



CENTUM VP

インストール手順

IM 33J01C10-01JA

IM 33J01C10-01JA
9版

はじめに

本書は、CENTUM VP をセットアップする手順を掲載しています。

本書の構成を次に示します。

- PART-A 概要
セットアップの概要について説明します。
- PART-B 新規セットアップ
CENTUM VP を新規にセットアップする際の手順について説明します。
- PART-C メンテナンス
CENTUM VP を運用していく中で必要となる項目について説明します。
- PART-D 他製品との接続
CENTUM VP を、他の当社製品と接続する際の方法や注意事項について説明します。

安全に使用するための注意事項

■ 本製品の保護、安全および改造に関する注意

- ・ 本製品によって制御されるシステムおよび本製品自体を保護し、安全に操作するために、本書に記載されている安全に使用するための注意事項に従ってください。指示事項に反する扱いをされた場合、横河電機株式会社（以下、当社といいます）は安全性の保証をいたしかねます。
- ・ ユーザーズマニュアルで指定していない方法で製品を使用した場合は、本製品で提供される保護機能が損なわれる可能性があります。
- ・ 本製品によって制御されるシステムおよび本製品そのものに保護または安全回路が必要な場合は、本製品外部に別途ご用意ください。
- ・ 本製品と組み合わせて使用する機器の仕様と設定については、必ず、機器の取扱説明書などで確認してください。
- ・ 本製品の部品または消耗品を交換する場合は、当社が指定する部品のみを使用してください。
- ・ 本製品および本製品の電源コードセットなどの付属品を、当社が指定する機器や用途以外に使用しないでください。
- ・ 本製品を改造することは、固くお断りいたします。
- ・ 本製品およびユーザーズマニュアルでは、安全に関する次の記号を使用しています。

 「注意」を示します。本製品においては、感電など、人体への危険や機器損傷の恐れがあることを示すとともに、ユーザーズマニュアルを参照する必要があることを示します。また、ユーザーズマニュアルにおいては、人体への危険や機器損傷を避けるための注意事項が記載されている箇所に、本記号を「注意」「警告」の用語と一緒に使用しています。

 「注意、高温表面」を示します。このマークの付いた機器は熱くなりますのでご注意ください。接触するとやけどなどの危険があります。

④ 「保護導体端子」を示します。感電防止のため、本製品を使用する前に、保護導体端子を必ず接地してください。

⊕ 「機能接地端子」を示します。「FG」と表示された端子も同じ機能を備えています。保護接地以外を目的とした接地端子です。本製品を使用する前に、機能接地端子を必ず接地してください。

～ 「AC 電源」を示します。

--- 「DC 電源」を示します。

| 「オン」を示します。電源スイッチなどの状態を示します。

○ 「オフ」を示します。電源スイッチなどの状態を示します。

■ ユーザーズマニュアルに対する注意

- ・ ユーザーズマニュアルは、最終ユーザまでお届けいただき、最終ユーザがお手元に保管して隨時参照できるようにしてください。
- ・ ユーザーズマニュアルをよく読んで、内容を理解したのちに本製品を操作してください。

- ・ ユーザーズマニュアルは、本製品に含まれる機能詳細を説明するものであり、お客様の特定目的に適合することを保証するものではありません。
- ・ ユーザーズマニュアルの内容については、将来予告なしに変更することがあります。
- ・ ユーザーズマニュアルの内容について万全を期していますが、もしご不審な点や誤り、記載もれなどお気付きのことがありましたら、当社またはお買い求め先代理店までご連絡ください。乱丁、落丁はお取り替えいたします。

■ 本製品の免責について

- ・ 当社は、保証条項に定める場合を除き、本製品に関するいかなる保証も行いません。
- ・ 本製品のご使用または使用不能から生じる間接損害については、当社は一切責任を負いかねますのでご了承ください。

■ ソフトウェア製品について

- ・ 当社は、保証条項に定める場合を除き、本ソフトウェアに関するいかなる保証も行いません。
- ・ 本製品の各ソフトウェアに対するライセンスは、ご使用になるコンピュータの台数に応じて適正にご購入ください。
- ・ バックアップ以外の目的で本ソフトウェアを複製することは、当社の知的所有権を侵害する行為であり、固くお断りいたします。
- ・ 本ソフトウェアが収められているソフトウェアメディアは、大切に保管してください。
- ・ 本ソフトウェアをリバースコンパイル、リバースアセンブリ、リバースエンジニアリング、その他の方法により人間が読み取り可能な形にすることは、固くお断りします。
- ・ 当社から事前の書面による承認を得ることなく、本ソフトウェアの全部または一部を譲渡、交換、転貸などによって第三者に使用させることは、固くお断りいたします。

ユーザーズマニュアル中の凡例

■ ユーザーズマニュアル中のシンボルマーク

ユーザーズマニュアルの本文中では、次の各種記号が使用されています。



死亡または重傷を招く可能性がある危険な状況を避けるための注意事項を記載しています。

警告



軽傷または物的損害を招く可能性がある危険な状況を避けるための注意事項を記載しています。

注意

重要 操作や機能を知る上で、注意すべき事柄を記載しています。

補足 説明を補足するための事柄を記載しています。

参照 参照先を示します。

オンラインマニュアルでは、緑色の参照先をクリックすると、該当箇所が表示されます。黒色の参照先は、該当箇所が表示されません。

■ ユーザーズマニュアル中の表記

ユーザーズマニュアル中の表記は、次の内容を示します。

● ユーザーズマニュアル全体を通して共通に使用されている表記

- 入力文字列

次の書体の文字列は、ユーザが実際の操作において入力する内容を示します。

例：

FIC100.SV=50.0

- ▼記号

本製品のエンジニアリングを行うウィンドウの定義項目に関する説明箇所であることを示します。

本製品のエンジニアリングを行うウィンドウのヘルプメニューから「ビルダ定義項目一覧」を選択したときに開くウィンドウを経由して、選択した項目の説明を表示できます。なお、複数の定義項目が併記されている場合には、複数の定義項目に関する説明箇所であることを示します。

例：

▼タグ名、ステーション名

- △記号

ユーザが入力する文字列で、空白文字（スペース）を示します。

例：

.AL△PIC010△-SC

- {} で囲った文字

ユーザが入力する文字列で、省略可能な文字列を示します。

例：

.PRATAG{△.シート名}

● キーまたはボタン操作を示すために使用されている表記

- ・ [] で囲った文字

キーまたはボタンの操作説明において [] で囲まれている文字は、キーボードのキー、オペレーションキーボードのキー、ウィンドウに表示されるボタン名、またはウィンドウに表示されるリストボックスの選択項目のいずれかを示します。

例：

機能を切り替えるには、[ESC] キーを押します。

● コマンド文やプログラム文などの書式説明の中で使用されている表記

コマンド文やプログラム文などの書式説明の中で使用されている表記は、次の内容を示します。

- ・ < >で囲った文字

ユーザが一定の規則に沿って任意に指定できる文字列を示します。

例：

#define <識別子> <文字列>

- ・ …記号

直前のコマンドや引数が繰り返し可能であることを示します。

例：

lmax (arg1, arg2, …)

- ・ [] で囲った文字

省略可能な文字列を示します。

例：

sysalarm <フォーマット文字列> [, <出力値>…]

- ・ | |で囲った文字

ユーザが複数候補から任意に選択できる文字列を示します。

例：

opeguide	<フォーマット文字列> [, <出力値>…]	
	OG,<素子番号>	

■ 図の表記

ユーザーズマニュアルに記載されている図は、説明の都合上、部分的に強調、簡略化、または省略されていることがあります。

ウィンドウの図では、機能理解や操作監視に支障を与えない範囲で、実際の表示と部品の表示位置や、大文字小文字など文字の種類が異なっている場合があります。

■ 入力文字

Windows では半角カタカナを使用できますが、本製品のソフトウェアへ入力する文字列には、半角カタカナを使用しないでください。

著作権および商標

■ 著作権

ソフトウェアメディアなどで提供されるプログラムおよびオンラインマニュアルなどの著作権は、当社に帰属します。

本製品を利用する目的でオンラインマニュアルの必要箇所をプリンタに出力することは可能ですが、全体の複製、または転載は著作権法で禁止されています。

したがって、オンラインマニュアルを電子的または上記出力を除く書面で複製したり、第三者に譲渡、販売、頒布（紙媒体、電子媒体、ネットワーク経由の配布など一切の方法を含みます）することを禁止します。また、無断でビデオ機器その他に登録、録画することも禁止します。

■ 商標

- CENTUM、ProSafe、Vnet/IP、PRM、Exaopc、Exaplog、Exapilot、Exaquantum、Exasmoc、Exarqe、Multivariable Optimizing Control/Robust Quality Estimation、StoryVIEW および FieldMate Validator は、横河電機株式会社の登録商標または商標です。
- 本製品で使用されている会社名、団体名、商品名およびロゴ等は、横河電機株式会社、各社または各団体の登録商標または商標です。

CENTUM VP インストール手順

IM 33J01C10-01JA 9 版

目 次

PART-A	概要.....	A-1
A1.	本書の読み方.....	A1-1
A2.	セットアップ作業の概要.....	A2-1
A2.1	セットアップの前に.....	A2-2
A2.2	新規セットアップ手順.....	A2-3
A2.2.1	CENTUM VP セットアップ手順.....	A2-4
A2.2.2	仮想化プラットフォーム上の CENTUM VP セットアップ手順.....	A2-6
A2.2.3	HIS のセットアップ手順.....	A2-8
A2.2.4	APCS のセットアップ手順.....	A2-9
A2.2.5	SIOS のセットアップ手順.....	A2-10
A2.2.6	GSGW のセットアップ手順.....	A2-11
A2.2.7	システム生成機能のみを搭載したコンピュータのセットアップ手順.....	A2-12
A2.2.8	AD サーバのみを搭載したコンピュータのセットアップ手順.....	A2-13
A2.2.9	HIS-TSE のセットアップ手順.....	A2-14
A2.2.10	ファイルサーバのセットアップ手順.....	A2-15
A2.2.11	ライセンス管理専用のコンピュータのセットアップ手順.....	A2-16
A2.2.12	コンピュータ切替型 UGS のセットアップ手順.....	A2-17
A2.2.13	UACS ステーションのセットアップ手順.....	A2-18
A2.3	メンテナンスに関する説明.....	A2-19
A3.	動作環境.....	A3-1

Blank Page

CENTUM VP インストール手順

IM 33J01C10-01JA 9 版

目 次

PART-B	新規セットアップをする.....	B-1
B1.	セットアップの準備をする.....	B1-1
B2.	Windows ドメイン環境の設定をする.....	B2-1
B2.1	ドメイン環境設定の概要.....	B2-2
B2.2	ドメインコントローラを構築する（Windows Server 2016/Windows Server 2012 R2）.....	B2-5
B2.3	ドメインコントローラを構築する（Windows Server 2008 R2/Windows Server 2008）.....	B2-7
B2.4	ドメインコントローラのセキュリティを設定する.....	B2-9
B2.5	ドメインユーザを作成する.....	B2-16
B2.6	クライアントコンピュータをドメインに参加させる.....	B2-21
B2.7	ドメインコントローラを冗長化する.....	B2-27
B2.8	Windows ドメイン環境での時刻同期を設定する.....	B2-28
B2.8.1	セキュリティを考慮した時刻同期をする.....	B2-29
B2.8.2	導入コストを抑えた時刻同期をする.....	B2-31
B3.	FCS/バス変換器/V ネットルータ/CGW/WAC ルータのハードウェアの設定をする.....	B3-1
B3.1	FCS の設定をする.....	B3-2
B3.2	バス変換器の設定をする.....	B3-5
B3.3	V ネットルータの設定をする.....	B3-11
B3.4	コミュニケーションゲートウェイユニットの設定をする.....	B3-13
B3.5	ワイドエリアコミュニケーションルータの設定をする.....	B3-15
B3.6	N-I/O のノードインターフェースユニットの設定.....	B3-17
B3.6.1	ノード番号設定ツールを使ってノード番号を設定する.....	B3-18
B3.6.2	メンテナンスポートの有効/無効の切り替え.....	B3-22
B4.	主なステーションやコンピュータのセットアップをする.....	B4-1
B4.1	ハードウェアの設定をする.....	B4-2
B4.2	Windows の設定をする.....	B4-7
B4.2.1	Windows 10 で設定する.....	B4-8
B4.2.2	Windows 7 で設定する.....	B4-14
B4.2.3	Windows Server 2016 で設定する.....	B4-23
B4.2.4	Windows Server 2012 R2 で設定する.....	B4-29
B4.2.5	Windows Server 2008 R2 で設定する.....	B4-36
B4.3	ネットワークの設定をする.....	B4-43
B4.3.1	制御バスドライバのインストールをする.....	B4-44
B4.3.2	Vnet/IP オープン通信ドライバのインストールをする.....	B4-46
B4.3.3	仮想マシンに Vnet/IP インタフェースパッケージをインストールする	B4-48
B4.3.4	Windows ネットワークの設定をする.....	B4-52
B4.3.5	CENTUM VP Small を使用する際の注意事項.....	B4-72
B4.3.6	コンピュータ切替型 UGS を使用する際の注意事項.....	B4-74

目次 B-2

B4.4	オペレーションキーボード用 USB ドライバのインストールをする.....	B4-79
B4.5	コンソール形 HIS の場合に必要な設定をする.....	B4-81
B4.6	CENTUM VP ソフトウェアのインストールをする	B4-87
B4.7	IT セキュリティを設定する.....	B4-96
B4.8	ライセンスの配布と反映をする.....	B4-103
B4.9	ユーザーアカウントを作成する.....	B4-104
	B4.9.1 標準モデル：スタンダードアロン管理のセキュリティ設定の場合.....	B4-105
	B4.9.2 従来モデルのセキュリティ設定の場合.....	B4-107
B4.10	ユーザごとの Windows 動作環境の設定をする.....	B4-109
	B4.10.1 Windows 10 で設定する	B4-110
	B4.10.2 Windows 7 で設定する.....	B4-118
	B4.10.3 Windows Server 2016 で設定する.....	B4-122
	B4.10.4 Windows Server 2012 R2 で設定する.....	B4-129
	B4.10.5 Windows Server 2008 R2 で設定する.....	B4-131
B4.11	ユーザ認証モードの設定をする.....	B4-136
	B4.11.1 CENTUM 認証モードの設定をする.....	B4-138
	B4.11.2 Windows 認証モードの設定をする.....	B4-140
	B4.11.3 ユーザ認証モードの注意事項.....	B4-148
B4.12	UPS (無停電電源装置) の設定をする.....	B4-149
B5.	リモート操作監視サーバ機能のセットアップをする.....	B5-1
B5.1	HIS-TSE サーバの設定をする.....	B5-4
	B5.1.1 Windows Server 2016 で設定する.....	B5-5
	B5.1.2 Windows Server 2008 R2 で設定する.....	B5-21
B5.2	HIS-TSE クライアントの設定をする.....	B5-43
B6.	ファイルサーバのセットアップをする.....	B6-1
B6.1	ファイルサーバ専用コンピュータのセットアップをする.....	B6-3
B6.2	HIS/システム生成機能/AD サーバのみを搭載したコンピュータにファイル サーバ機能を設定する.....	B6-11
B6.3	ファイルサーバとライセンス管理ステーションを兼用するコンピュータの セットアップをする.....	B6-12
B7.	ライセンス管理専用のコンピュータのセットアップをする.....	B7-1
B8.	仮想化環境のセットアップ.....	B8-1
B8.1	SIOS.....	B8-2
B8.2	HIS.....	B8-3
	B8.2.1 USB 機器を使用するための設定.....	B8-4
	B8.2.2 最大接続数制限の設定.....	B8-9
	B8.2.3 1 ユーザあたりのセッション制限の設定.....	B8-10
	B8.2.4 ピープの有効化.....	B8-11
	B8.2.5 ブザー設定.....	B8-12
B8.3	HIS-TSE.....	B8-13
	B8.3.1 USB 機器を使用するための設定.....	B8-14
	B8.3.2 仮想マシンのゲスト OS での設定.....	B8-15
	B8.3.3 最大接続数制限の設定.....	B8-18
	B8.3.4 1 ユーザあたりのセッション制限の設定.....	B8-19
	B8.3.5 アプリケーションと作業ディレクトリの設定.....	B8-20
	B8.3.6 HIS-TSE アンインストール.....	B8-21

CENTUM VP インストール手順

IM 33J01C10-01JA 9 版

目 次

PART-C	メンテナンス.....	C-1
C1. ライセンスの追加や割り付けの変更をする..... C1-1		
C1.1 ライセンスを追加する.....		C1-2
C1.2 ライセンスの割り付けを変更する.....		C1-3
C2. エンジニアリングデータ参照先を変更する..... C2-1		
C3. ドメイン環境をあとから構築する..... C3-1		
C4. CENTUM 認証モードから Windows 認証モードに変更をする.....		
.....		C4-1
C5. バックアップをとる..... C5-1		
C5.1 Windows 全体のバックアップ.....		C5-2
C5.2 VP プロジェクトのバックアップをとる.....		C5-3
C5.3 カスタムメニュー定義のバックアップをとる.....		C5-4
C5.4 CENTUM VP 操作監視機能用データベースのバックアップをとる.....		C5-5
C5.4.1 帳票のバックアップをとる.....		C5-6
C5.4.2 PICOT のバックアップをとる.....		C5-7
C5.5 CAMS for HIS コンフィグレータで定義したエンジニアリングデータのバックアップをとる.....		C5-8
C6. バージョンアップ／レビジョンアップやアップグレードをする.....		
.....		C6-1
C6.1 CENTUM CS 3000 から CENTUM VP R6 にバージョンアップする..... C6-2		
C6.1.1 バージョンアップをする.....		C6-3
C6.1.2 CS 3000 パッケージデータのバックアップとリストアをする.....		C6-8
C6.1.3 CAMS for HIS データのバックアップとリストアをする.....		C6-13
C6.2 CENTUM CS 1000 から CENTUM VP R6 へのアップグレードをする.....		
.....		C6-17
C6.2.1 アップグレードをする.....		C6-18
C6.2.2 CS 1000 パッケージデータのバックアップとリストア.....		C6-24
C6.3 CENTUM VP R4/R5 から R6 へのバージョンアップをする..... C6-29		
C6.4 CENTUM VP R6 のレビジョンアップをする..... C6-38		
C6.5 ライセンス管理専用のコンピュータのバージョンアップ／レビジョンアップをする..... C6-47		
C6.6 オペレーションキーボードを置き換える..... C6-49		
C6.7 制御バス用のカードを交換する..... C6-50		
C7. CENTUM VP ソフトウェアのアンインストールをする C7-1		
C7.1 主なステーションやコンピュータのアンインストールをする C7-2		
C7.1.1 CENTUM デスクトップ環境設定の解除をする.....		C7-3
C7.1.2 Windows の各種設定を復元する.....		C7-5
C7.1.3 CENTUM VP ソフトウェアをアンインストールする.....		C7-10

C7.2	ライセンス管理専用のコンピュータのアンインストールをする.....	C7-20
C8.	CENTUM VP ソフトウェアの再インストールをする.....	C8-1
C8.1	使用するコンピュータを変更しない場合.....	C8-2
C8.2	使用するコンピュータを変更する場合.....	C8-5
C9.	IT セキュリティ設定で注意すべきケース.....	C9-1
C9.1	CENTUM VP 標準モデルの VP プロジェクトに CENTUM CS 3000 R3 HIS を混在させる.....	C9-2
C9.2	CENTUM VP 標準モデルの VP プロジェクトに従来モデルの CENTUM VP HIS を混在させる.....	C9-4
C9.3	複数プロジェクト結合をする.....	C9-7
C9.3.1	標準モデルの CENTUM VP プロジェクトと従来モデルの CENTUM VP プロジェクトを結合する.....	C9-8
C9.3.2	CENTUM VP プロジェクトと CENTUM CS 1000/CS 3000 R3 プロジェクトを結合する.....	C9-12
C9.3.3	CENTUM VP プロジェクトと CENTUM CS プロジェクトを結合する.....	C9-16
C9.4	CENTUM VP R4 で IT セキュリティ設定をしたファイルサーバやドメインコントローラを使用する.....	C9-17
C10.	トラブルシューティング.....	C10-1
C10.1	Windows 関連のトラブルシューティング	C10-2
C10.1.1	ユーザーアカウント制御の注意事項.....	C10-3
C10.1.2	サーバーマネージャーの起動時にエラーが発生する.....	C10-4
C10.1.3	コントロールパネルのユーザーアカウントダイアログでユーザーアカウントが管理できない.....	C10-6
C10.1.4	コントロールパネルのプログラムと機能ウィンドウでインストールされた更新プログラムが表示されない.....	C10-7
C10.1.5	マイクロソフトの更新プログラムがインストールできない.....	C10-8
C10.1.6	.NET Framework のインストールに失敗する.....	C10-9
C10.1.7	システムがロックした.....	C10-10
C10.1.8	正常に動いていたコンピュータの動作が不安定になった.....	C10-11
C10.1.9	印刷順序がスプールされた順と一致しない.....	C10-12
C10.2	ネットワーク関連のトラブルシューティング	C10-14
C10.2.1	ネットワークケーブル配線時の注意事項.....	C10-15
C10.2.2	ドライバのインストールと削除に関するトラブル.....	C10-16
C10.3	CENTUM 製品関連のトラブルシューティング	C10-24
C10.3.1	実機 HIS の IP アドレスを変更してダウンロードした際にエラーが発生する.....	C10-25
C10.3.2	リモート操作監視サーバに接続できない.....	C10-26
C10.3.3	操作監視機能稼動中に AIP262 (USB インタフェース付き AUX ボード) の USB ケーブルがコンピュータから抜けた.....	C10-27
C10.3.4	スタートメニューの AD オーガナイザのショートカットが消えた.....	C10-28
C11.	バージョンアップ／レビジョンアップ時の注意事項.....	C11-1
C11.1	R4.01.33 へのバージョンアップ／レビジョンアップ	C11-2
C11.1.1	該当事項への対応作業.....	C11-6
C11.1.2	R4.01.00 互換機能サポートのレジストリ設定について	C11-8
C11.2	R4.01.60 へのバージョンアップ／レビジョンアップ	C11-9
C11.2.1	グラフィックビューのリンクについての注意事項.....	C11-10
C11.2.2	グラフィックにおける動作の選択.....	C11-11
C11.2.3	操作監視ウィンドウの表示枚数.....	C11-12
C11.2.4	複数モニタパッケージを使用している場合.....	C11-13
C11.2.5	ビューの更新周期.....	C11-15
C11.2.6	グラフィックのタグオブジェクトを示す枠の色.....	C11-16

目次 C-3

C11.2.7 グラフィックの押しボタンとソフトキーにガードが付いた場合の操作禁止枠の色.....	C11-17
C11.2.8 グラフィックビューでのコントロールの動作についての注意事項.....	C11-18
C11.3 R4.02.00 へのバージョンアップ／レビジョンアップ.....	C11-19
C11.4 R4.02.30 へのバージョンアップ／レビジョンアップ.....	C11-23
C11.5 R4.03.00 へのバージョンアップ／レビジョンアップ.....	C11-24
C11.6 R5.01.00 へのバージョンアップ.....	C11-26
C11.7 R5.01.10 へのバージョンアップ／レビジョンアップ.....	C11-31
C11.8 R5.02.00 へのバージョンアップ／レビジョンアップ.....	C11-32
C11.9 R5.03.00 へのバージョンアップ／レビジョンアップ.....	C11-33
C11.10 R5.03.20 へのバージョンアップ／レビジョンアップ.....	C11-37
C11.11 R5.04.00 へのバージョンアップ／レビジョンアップ.....	C11-39
C11.12 R5.04.20 へのバージョンアップ／レビジョンアップ.....	C11-40
C11.13 R6.01.00 へのバージョンアップ.....	C11-41
C11.14 R6.01.10 へのバージョンアップ／レビジョンアップ.....	C11-42
C11.15 R6.02.00 へのバージョンアップ／レビジョンアップ.....	C11-43
C11.16 R6.03.00 へのバージョンアップ／レビジョンアップ.....	C11-46
C11.17 R6.03.10 へのバージョンアップ／レビジョンアップ.....	C11-50
C11.18 R6.04.00 へのバージョンアップ／レビジョンアップ.....	C11-51
C11.19 R6.05.00 へのバージョンアップ／レビジョンアップ.....	C11-56
C11.20 R6.06.00 へのバージョンアップ／レビジョンアップ.....	C11-60
C11.21 R6.07.00 へのバージョンアップ／レビジョンアップ.....	C11-62

Blank Page

CENTUM VP インストール手順

IM 33J01C10-01JA 9 版

目 次

PART-D	他製品との接続.....	D-1
D1. 当社他製品との接続.....D1-1		
D1.1 CENTUM VP と ProSafe-RS.....D1-3		
D1.1.1	CENTUM VP - 操作監視基本機能と ProSafe-RS - SOE ビューアパッケージ..	D1-4
D1.1.2	CENTUM VP - 操作監視基本機能と ProSafe-RS - SOE OPC インタフェース パッケージ	D1-5
D1.1.3	CENTUM VP - システム生成機能と ProSafe-RS - CENTUM VP 統合パッケー ジ	D1-9
D1.1.4	CENTUM VP - システム生成機能と ProSafe-RS - 安全システムエンジニア リング・保守機能	D1-10
D1.1.5	CENTUM VP - エンジニアリングサーバ機能と ProSafe-RS - 安全システム エンジニアリング・保守機能	D1-11
D1.1.6	CENTUM VP - システム生成機能と ProSafe-RS - エンジニアリングサーバ 機能	D1-12
D1.2 CENTUM VP と PRM.....D1-13		
D1.2.1	CENTUM VP 操作監視基本機能と PRM サーバ	D1-14
D1.2.2	PRM サーバと CENTUM VP 操作監視基本機能	D1-16
D1.3 CENTUM VP と Exaopc.....D1-18		
D1.3.1	CENTUM VP - 操作監視基本機能と Exaopc サーバ	D1-19
D1.3.2	CENTUM VP - システム生成機能と Exaopc サーバ	D1-20
D1.4 CENTUM VP と Exapilot.....D1-21		
D1.4.1	CENTUM VP 操作監視基本機能と Exapilot サーバ	D1-22
D1.4.2	CENTUM VP 操作監視基本機能と Exapilot クライアント	D1-26
D1.4.3	CENTUM VP システム生成機能と Exapilot クライアント	D1-29
D1.5 CENTUM VP と Exaplog.....D1-30		
D1.5.1	CENTUM VP - 操作監視基本機能と Exaplog - イベント解析パッケージサー バ	D1-31
D1.6 CENTUM VP と Exaquantum.....D1-33		
D1.6.1	CENTUM VP - 操作監視基本機能と Exaquantum - PIMS サーバ	D1-34
D1.6.2	CENTUM VP - 操作監視基本機能と Exaquantum - Explorer クライアント	D1-38
D1.7 Multivariable Optimizing Control/Robust Quality Estimation と CENTUM VP.....D1-40		
D1.7.1	CENTUM VP 操作監視基本機能および APC クライアント	D1-41
D1.8 CENTUM VP と Exasmoc.....D1-43		
D1.8.1	CENTUM VP - 操作監視基本機能と Exasmoc クライアント	D1-44
D1.9 CENTUM VP と Exarqe.....D1-46		
D1.9.1	CENTUM VP - 操作監視基本機能と Exarqe クライアント	D1-47

Blank Page

CENTUM VP インストール手順

IM 33J01C10-01JA 9 版

目 次

付録

Appendix 1. 設定スイッチ.....	App.1-1
Appendix 2. Vnet/IP インタフェース管理ツール.....	App.2-1
Appendix 3. Windows 10 インストール時のカスタマイズ.....	App.3-1

Blank Page

A. 概要

ここでは、本書の読み方、CENTUM VP のセットアップ作業の種類と作業フロー、および動作環境について説明します。

Blank Page

A1. 本書の読み方

本書では、CENTUM VP ソフトウェアのセットアップ手順について説明します。Windows の OS、関連するサービスパック、Microsoft セキュリティパッチのインストール手順については、本書の記述範囲外です。

CENTUM VP ソフトウェアパッケージを各ステーションで使用するための各ステーションへのライセンス配布と有効化作業は、ライセンスマネージャと呼ばれるソフトウェアで実施します。ライセンスマネージャを使う作業については、ライセンス管理の IM に記述しています。本書では、セットアップの作業の流れを説明する中で、必要に応じてライセンス管理の IM を参照します。

また、システムのセキュリティ強化機能については、セキュリティガイドの IM を参照してください。

参照

Windows の OS、関連するサービスパック、Microsoft セキュリティパッチのインストール手順については、以下を参照してください。

Microsoft 社から提供されている情報

Microsoft セキュリティパッチについては、以下を参照してください。

マイクロソフト社セキュリティ・パッチに対する基本方針 (TI 33Y01B30-02)

各ステーションにライセンスを配布し有効にする作業については、以下を参照してください。

ライセンス管理 (IM 33J01C20-01JA) の「1.1.3 ライセンス管理の作業概要」

システムのセキュリティについては、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「1. 概要」

■ 本書の構成

本書の構成は次のようになっています。

- Part A : 概要
本書の読み方、CENTUM VP のセットアップ作業の種類とその作業フロー、および動作環境について説明します。
- Part B : 新規セットアップをする
各ステーションをセットアップする手順について説明します。
- Part C : メンテナンス
各ステーションの新規セットアップ後、それを運用していく中で必要となる作業について説明します。
- Part D : 他製品との接続
横河電機の ProSafe-RS、PRM、Exaopc などの他製品と接続して使用する方法について説明します。

■ セットアップ手順の説明について

Windows の設定やデバイスドライバのセットアップ手順は、Windows の OS 種別に依存しない場合、Windows 7 の例で示します。Windows の OS 種別に依存して、設定方法などが大きく異なる場合は、OS ごとに設定方法を示します。

Blank Page

A2. セットアップ作業の概要

ここでは、各ステーションのセットアップの前に知っておくべき事項や、セットアップ手順のワークフローなどについて説明します。

A2.1 セットアップの前に

ここでは、CENTUM VP ソフトウェアのインストールとライセンス付与の関係について説明します。

■ ソフトウェアパッケージのインストールとライセンス付与

CENTUM VP のソフトウェアパッケージを使用するには、CENTUM VP ソフトウェアをコンピュータにインストールしたあと、そのコンピュータに対して各ソフトウェアパッケージのライセンスを与える必要があります。

各コンピュータにソフトウェアパッケージをインストールするには、各コンピュータでインストーラと呼ばれるプログラムを使用します。ライセンスを与えるには、ライセンスマネージャと呼ばれるソフトウェアを使用します。ライセンスマネージャは、CENTUM VP ソフトウェアをインストールしたときに自動的にインストールされます。

ライセンスマネージャがインストールされたコンピュータのうち、システム内の各コンピュータのライセンス管理をするものをライセンス管理ステーションと呼びます。ライセンス管理ステーションから、ソフトウェアパッケージがインストールされた各コンピュータにライセンスを配布します。ライセンスを配布されたコンピュータでは、配布されたライセンスを反映することで、ソフトウェアパッケージが使用可能になります。

補足

ライセンスマネージャだけを単独でインストールし、ライセンス管理専用のコンピュータにすることもできます。

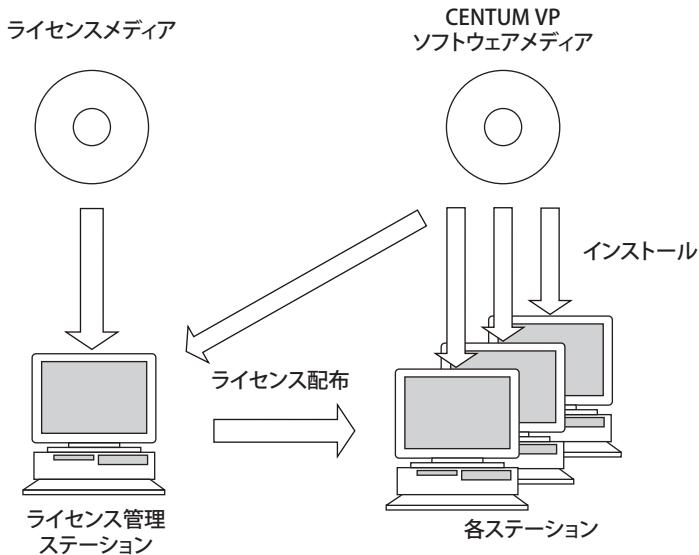


図 A2.1-1 ライセンスの配布

参照

ライセンスの詳細については、以下を参照してください。

ライセンスマネージャ (IM 33J01C20-01JA) の「1.1.3 ライセンス管理の作業概要」

A2.2 新規セットアップ手順

ここでは、フローチャートを使用して CENTUM VP 全体のセットアップおよび各ステーションやコンピュータのセットアップ手順を説明します。

説明するステーションやコンピュータの種類は次のとおりです。

- ・ ヒューマンインタフェースステーション (HIS)
- ・ APCS
- ・ システム統合 OPC ステーション (SIOS)
- ・ 汎用サブシステムゲートウェイ (GSGW)
- ・ システム生成機能のみを搭載したコンピュータ
- ・ オートメーションデザインサーバ (AD サーバ) のみを搭載したコンピュータ
- ・ リモート操作監視サーバー (HIS-TSE)
- ・ ファイルサーバ
- ・ ライセンス管理専用のコンピュータ
- ・ コンピュータ切替型 UGS
- ・ UACS ステーション
- ・ 仮想化プラットフォーム上の CENTUM VP 関連ステーションおよびコンピュータ

参照

ネットワーク切替型冗長化 UGS のセットアップ手順については、以下を参照してください。

統合ゲートウェイステーションリファレンス (IM 33J20C10-01JA) の「D2. ネットワーク切替型 UGS のシステム構築とメンテナンス」

仮想化プラットフォームについては、以下を参照してください。

仮想化プラットフォームセットアップ (IM 30A05B20-01JA) の「A. 概要」

■ 新規セットアップ後の作業

エンジニアリング開始前の準備として、次の作業が必要です。

- ・ オートメーションデザインプロジェクト (AD プロジェクト) の作成
- ・ VP プロジェクトの作成
- ・ VP プロジェクトの AD プロジェクトへの登録

参照

エンジニアリング開始前の準備については、以下を参照してください。

オートメーションデザインシート基本機能 (IM 33J10A10-01JA) の「B. エンジニアリングを開始する」

A2.2.1 CENTUM VP セットアップ手順

CENTUM VP セットアップ手順を次に示します。

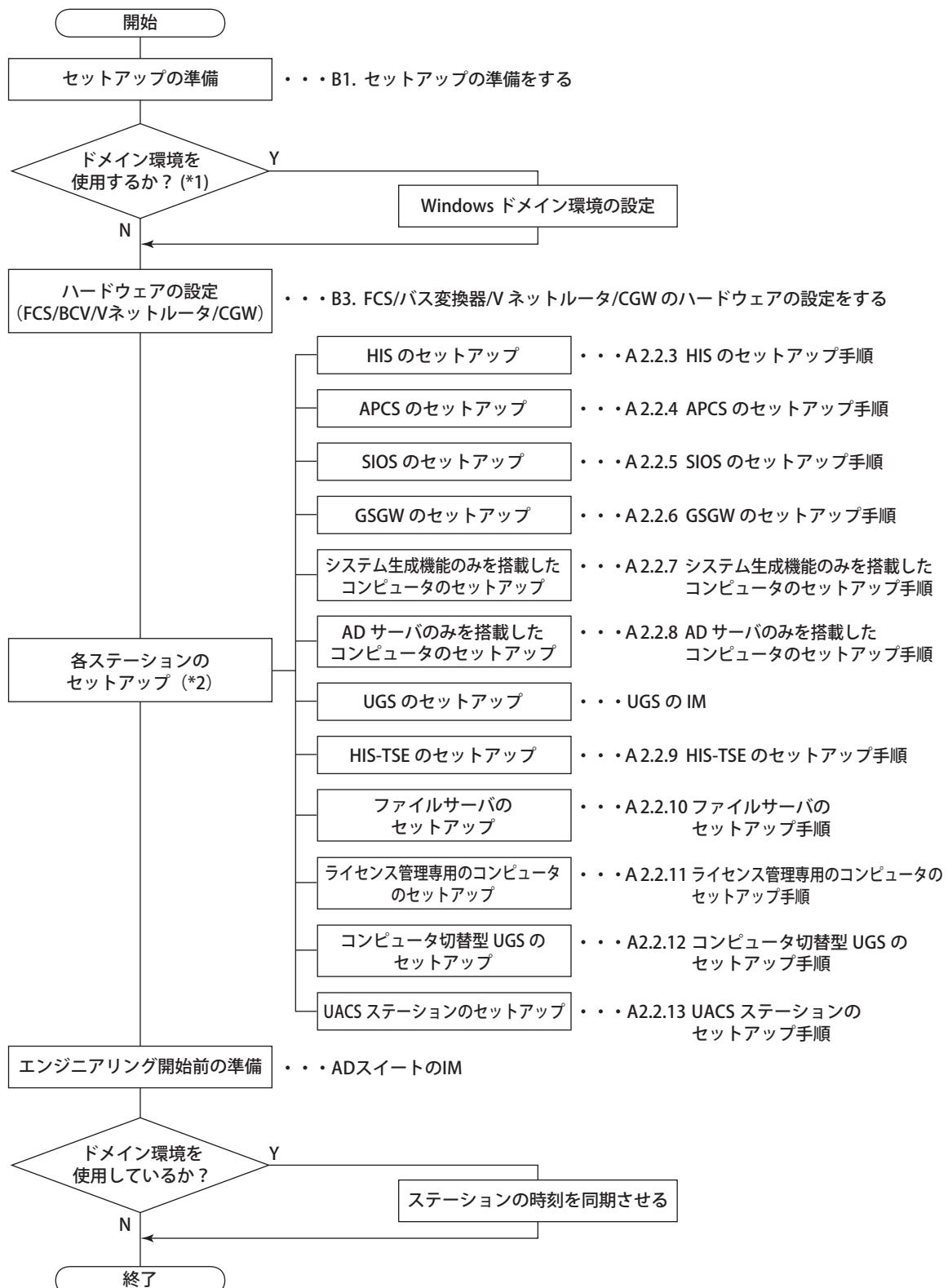


図 A2.2.1-1 CENTUM VP セットアップ手順

■ セットアップするステーションの順番

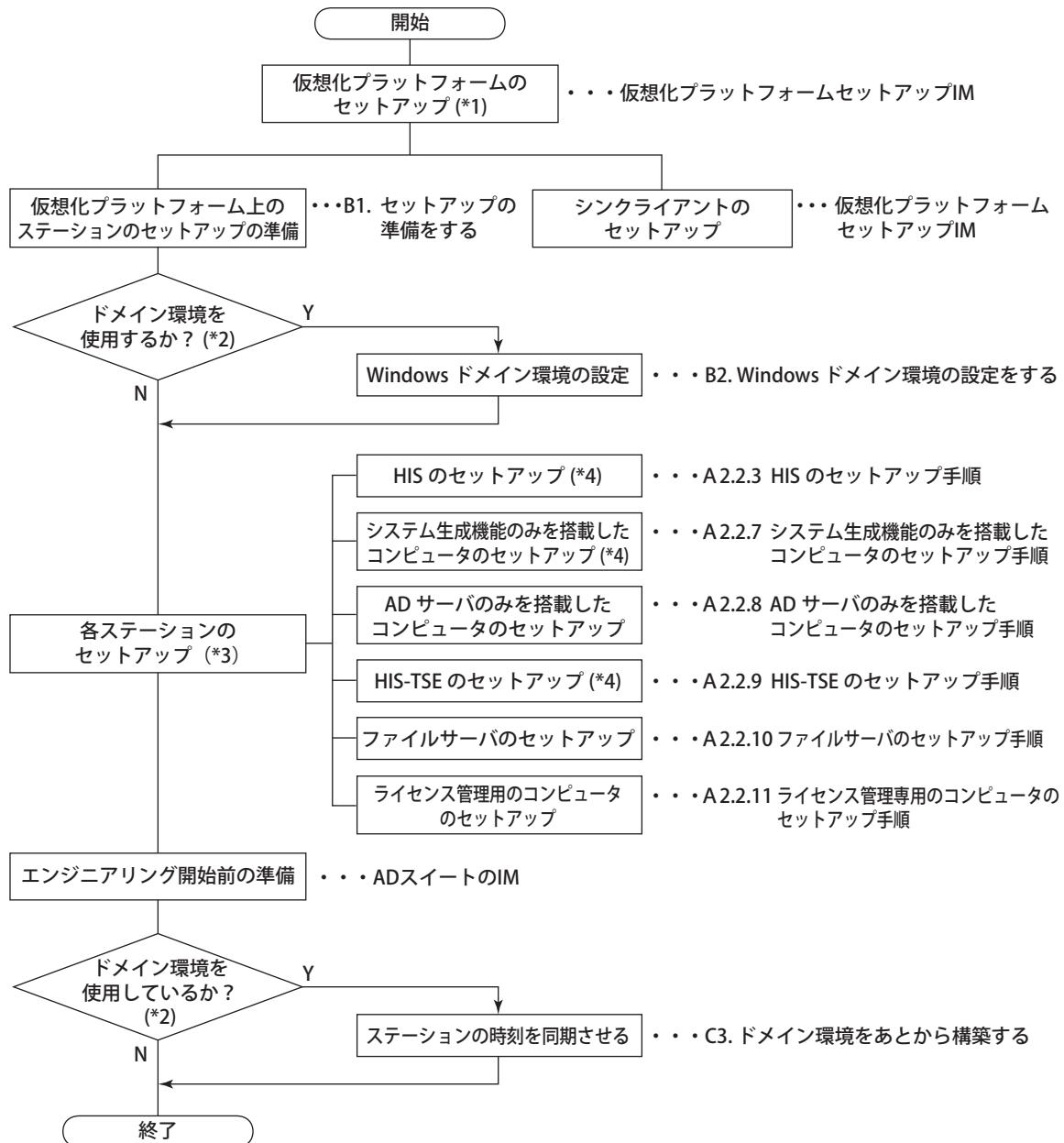
CENTUM VP のソフトウェアパッケージを使用するには、CENTUM VP ソフトウェアをコンピュータにインストールしたあと、そのコンピュータに対して各ソフトウェアパッケージの使用を許可するライセンスを与える必要があります。

そのため、ソフトウェアパッケージのライセンスを与えるコンピュータとなる、ライセンス管理ステーションと呼ばれるステーションを決めておき、そのステーションを最初にセットアップする必要があります。

その他のステーションは、IT セキュリティ設定まで終わったあと、ライセンス管理ステーションからライセンスが配布され、それを反映することで使用可能となります。

A2.2.2 仮想化プラットフォーム上の CENTUM VP セットアップ手順

仮想化プラットフォーム上の CENTUM VP セットアップ手順を次の図に示します。



*1: 仮想化ホストコンピュータを用意して、仮想化プラットフォームをインストールしてください。

*2: ドメイン環境はあとから構築することもできます。

*3: ライセンス管理ステーションとするものを最初にセットアップしてください。

*4: Vnet/IPインターフェースカードのセットアップは必要ありません。また、仮想化プラットフォーム上では、UPSは使用できません。

図 A2.2.2-1 仮想化プラットフォーム上の CENTUM VP のセットアップ手順

参照

ファイルサーバの構築手順については、以下を参照してください。

「A2.2.10 ファイルサーバのセットアップ手順」ページ A2-15

仮想化環境における追加手順については、以下を参照してください。

「B8. 仮想化環境のセットアップ」ページ B8-1

仮想化プラットフォームのインストール手順については、以下を参照してください。

仮想化プラットフォームセットアップ (IM 30A05B20-01JA)

■ ドメイン環境

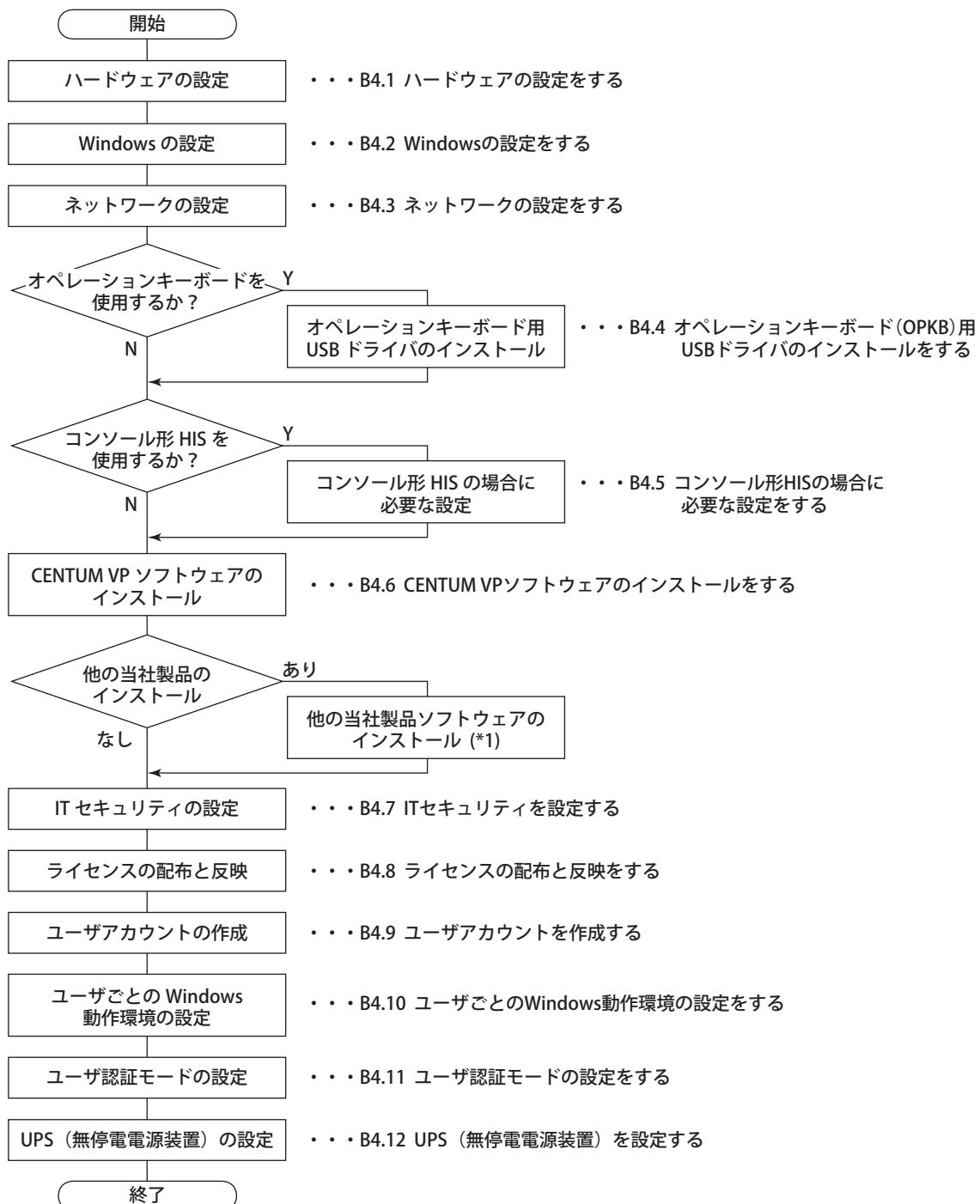
ドメインコントローラは既設の物理環境のコンピュータを使用することもできれば、仮想化プラットフォーム上で構築することもできます。

■ ライセンス管理コンピュータ

ライセンス管理コンピュータは既設の物理環境のコンピュータを使用することもできれば、仮想化プラットフォーム上で構築することもできます。

A2.2.3 HIS のセットアップ手順

HIS のセットアップ手順を次に示します。



*1: あとからインストールすることもできますが、その場合はITセキュリティ設定を再設定してください。

図 A2.2.3-1 HIS のセットアップ手順

A2.2.4 APCS のセットアップ手順

APCS のセットアップ手順を次に示します。

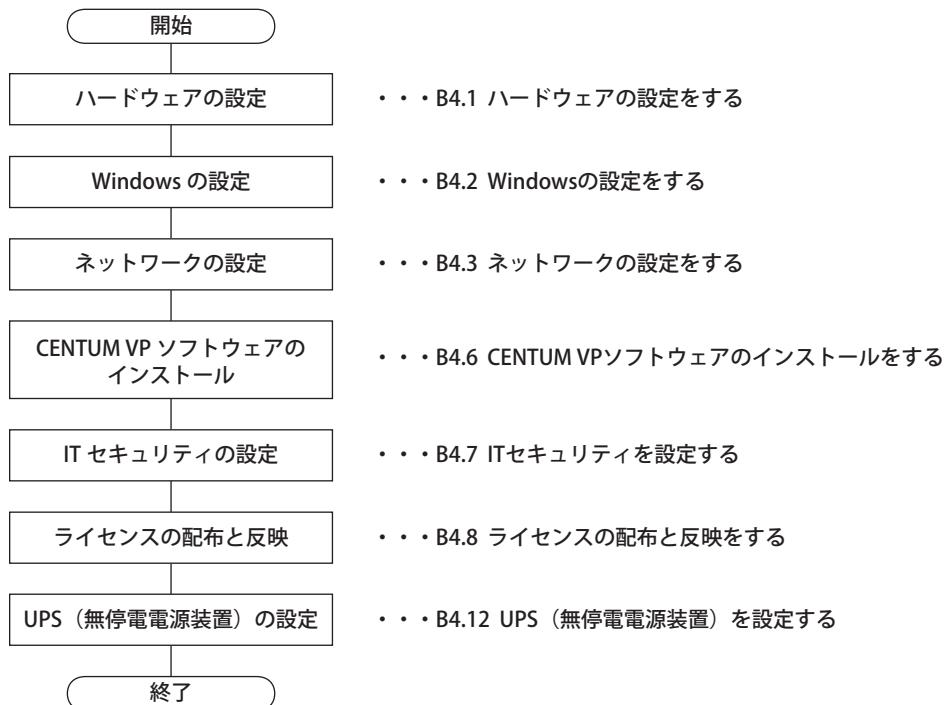


図 A2.2.4-1 APCS のセットアップ手順

A2.2.5 SIOS のセットアップ手順

SIOS のセットアップ手順を次に示します。

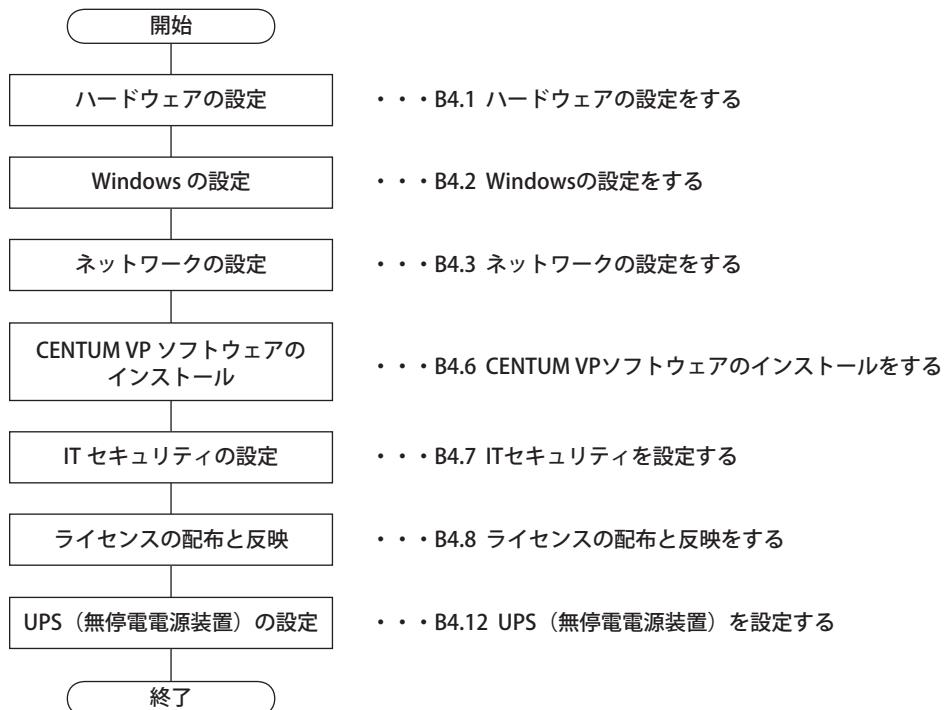


図 A2.2.5-1 SIOS のセットアップ手順

A2.2.6 GSGW のセットアップ手順

GSGW のセットアップ手順を次に示します。

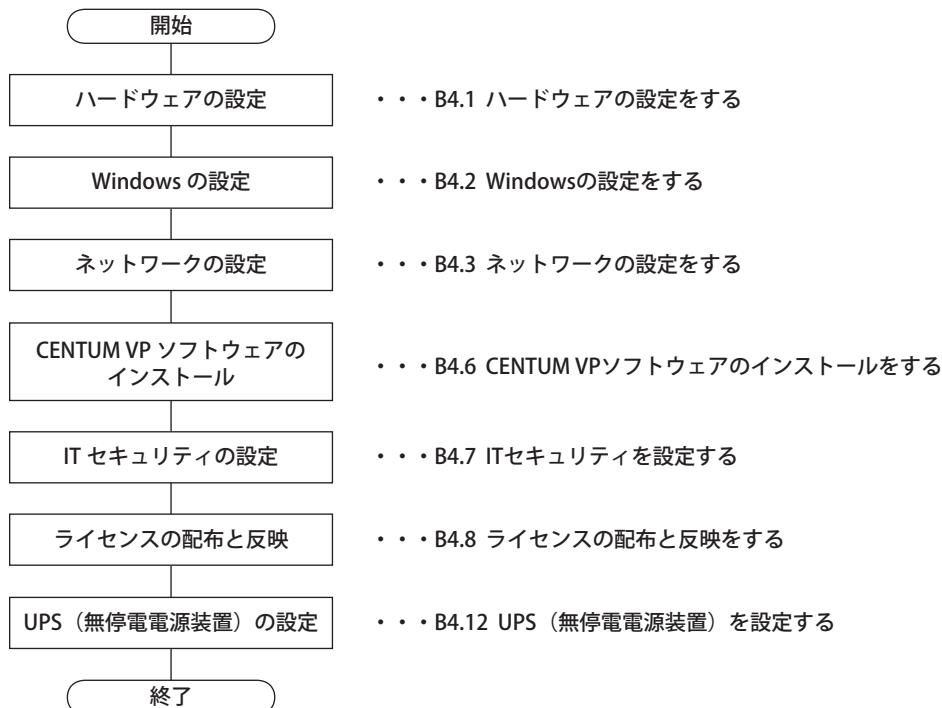
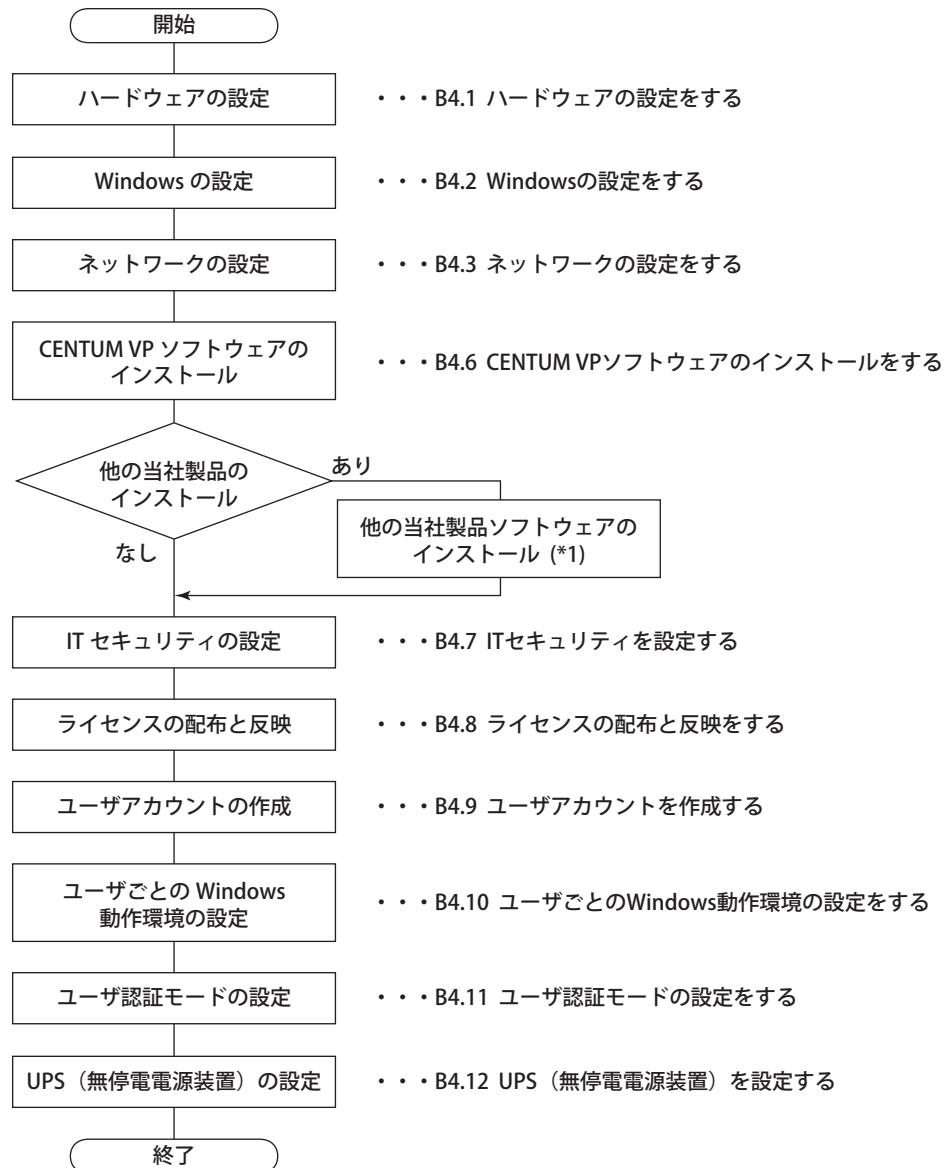


図 A2.2.6-1 GSGW のセットアップ手順

A2.2.7 システム生成機能のみを搭載したコンピュータのセットアップ手順

システム生成機能のみを搭載したコンピュータのセットアップ手順を次に示します。

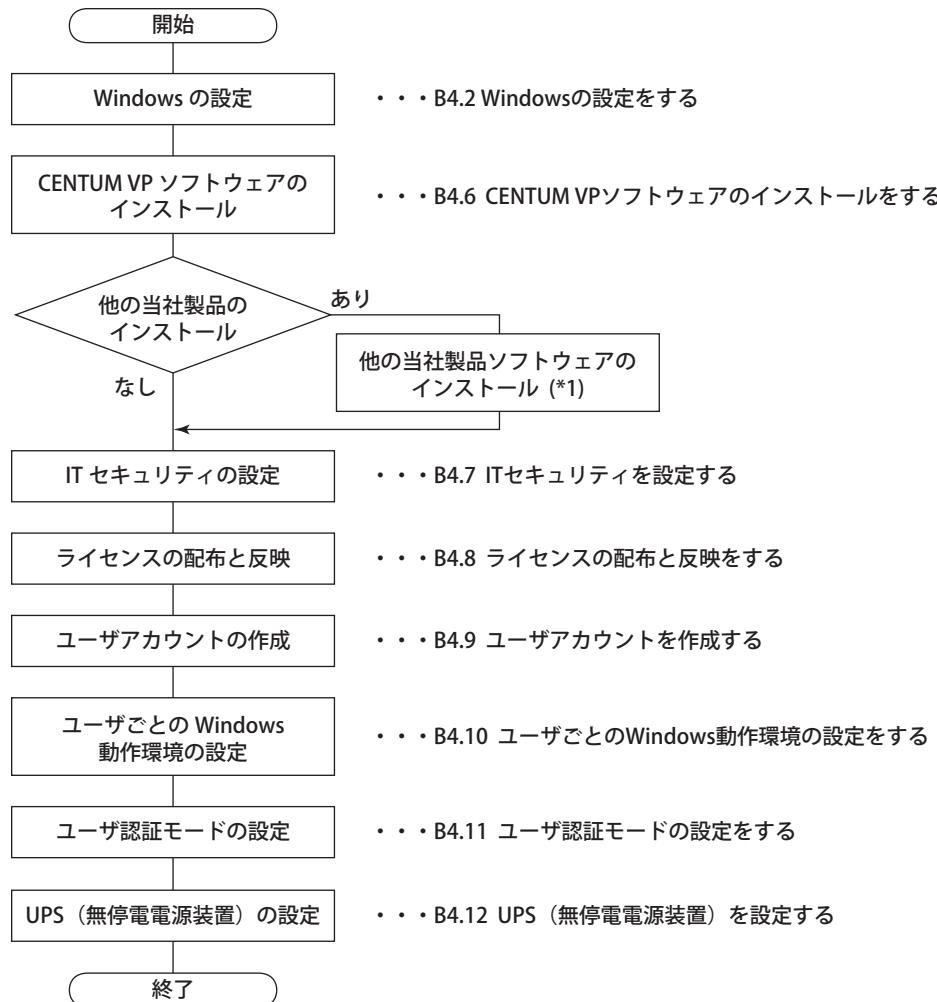


*1: あとからインストールすることもできますが、その場合はITセキュリティ設定を再設定してください。

図 A2.2.7-1 システム生成機能のみを搭載したコンピュータのセットアップ手順

A2.2.8 AD サーバのみを搭載したコンピュータのセットアップ手順

AD サーバのみを搭載したコンピュータのセットアップ手順を次に示します。

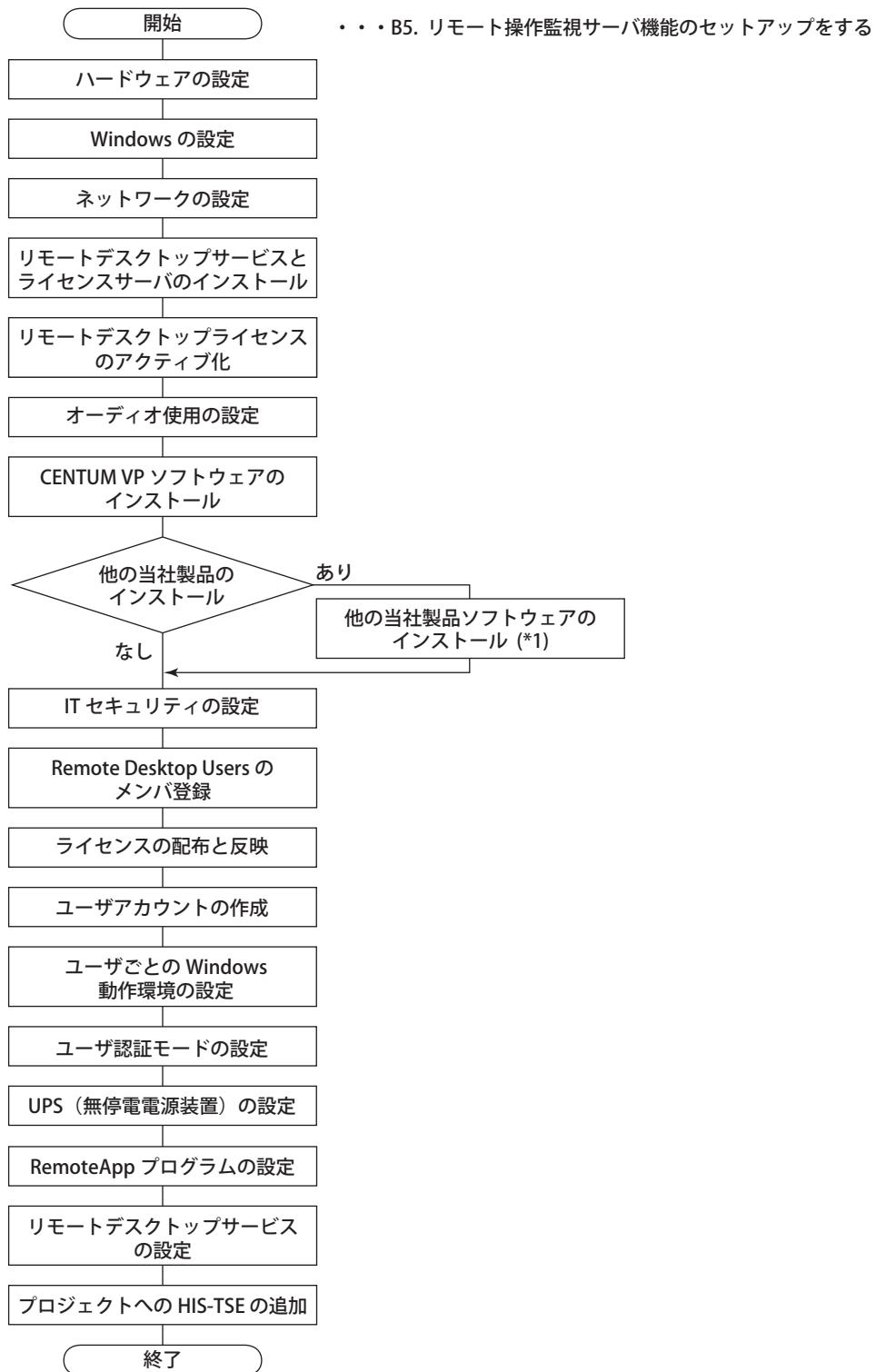


*1: あとからインストールすることもできますが、その場合はITセキュリティ設定を再設定してください。

図 A2.2.8-1 AD サーバのみを搭載したコンピュータのセットアップ手順

A2.2.9 HIS-TSE のセットアップ手順

HIS-TSE のセットアップ手順を次に示します。



*1: あとからインストールすることもできますが、その場合はITセキュリティ設定を再設定してください。

図 A2.2.9-1 HIS-TSE のセットアップ手順

A2.2.10 ファイルサーバのセットアップ手順

プロジェクトのデータを集中して管理したい場合などには、ファイルサーバを設置できます。ファイルサーバのセットアップ手順を次に示します。

補足

ここでフローチャートを使用して説明されている手順は、ファイルサーバ専用コンピュータのセットアップ手順です。

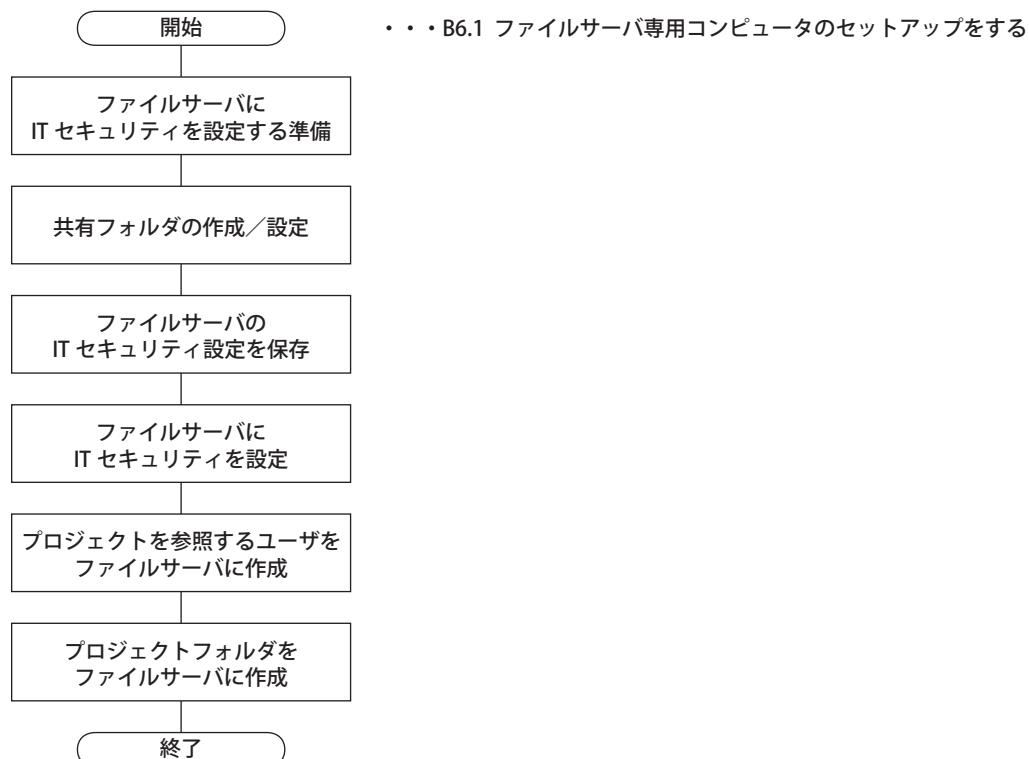


図 A2.2.10-1 ファイルサーバ専用コンピュータのセットアップ手順

参照

HIS やシステム生成機能のみを搭載したコンピュータにファイルサーバ機能をもたせる場合の手順については、以下を参照してください。

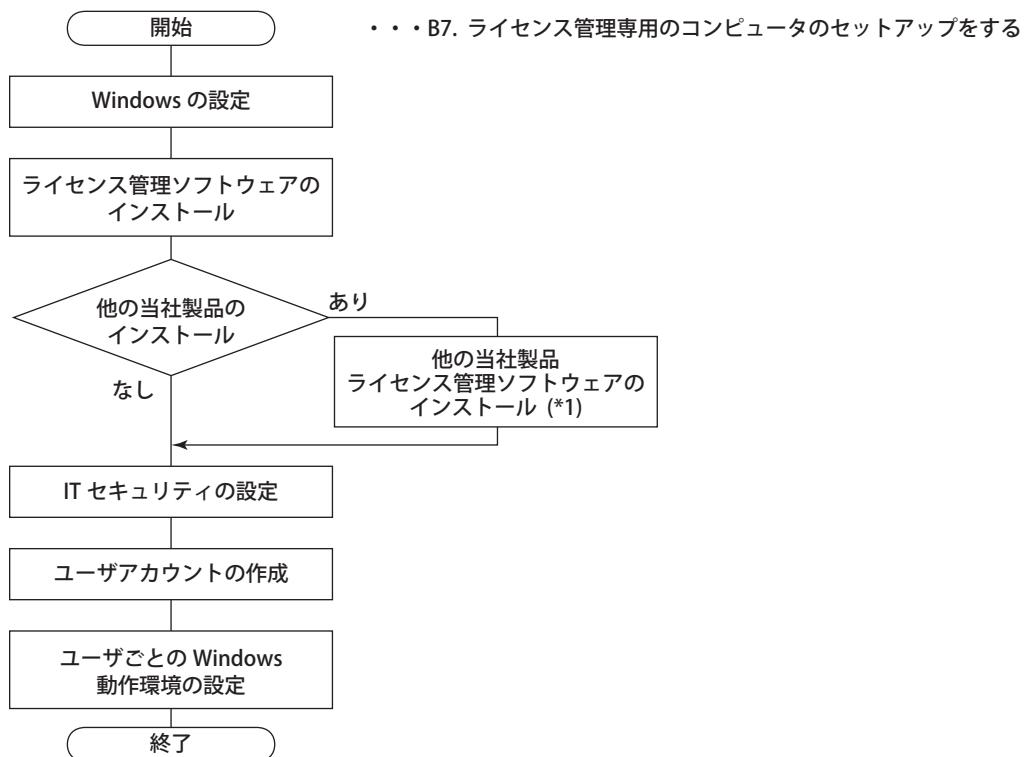
「B6.2 HIS/システム生成機能/AD サーバのみを搭載したコンピュータにファイルサーバ機能を設定する」
ページ B6-11

ファイルサーバとライセンス管理ステーションを兼用する場合の手順については、以下を参照してください。

「B6.3 ファイルサーバとライセンス管理ステーションを兼用するコンピュータのセットアップをする」
ページ B6-12

A2.2.11 ライセンス管理専用のコンピュータのセットアップ手順

システムの規模や運用方針に合わせて、ライセンス管理専用のコンピュータを設けられます。ライセンス管理専用のコンピュータのセットアップ手順を次に示します。



*1: あとからインストールすることもできますが、その場合はITセキュリティ設定を再設定してください。

図 A2.2.11-1 ライセンス管理専用のコンピュータのセットアップ手順

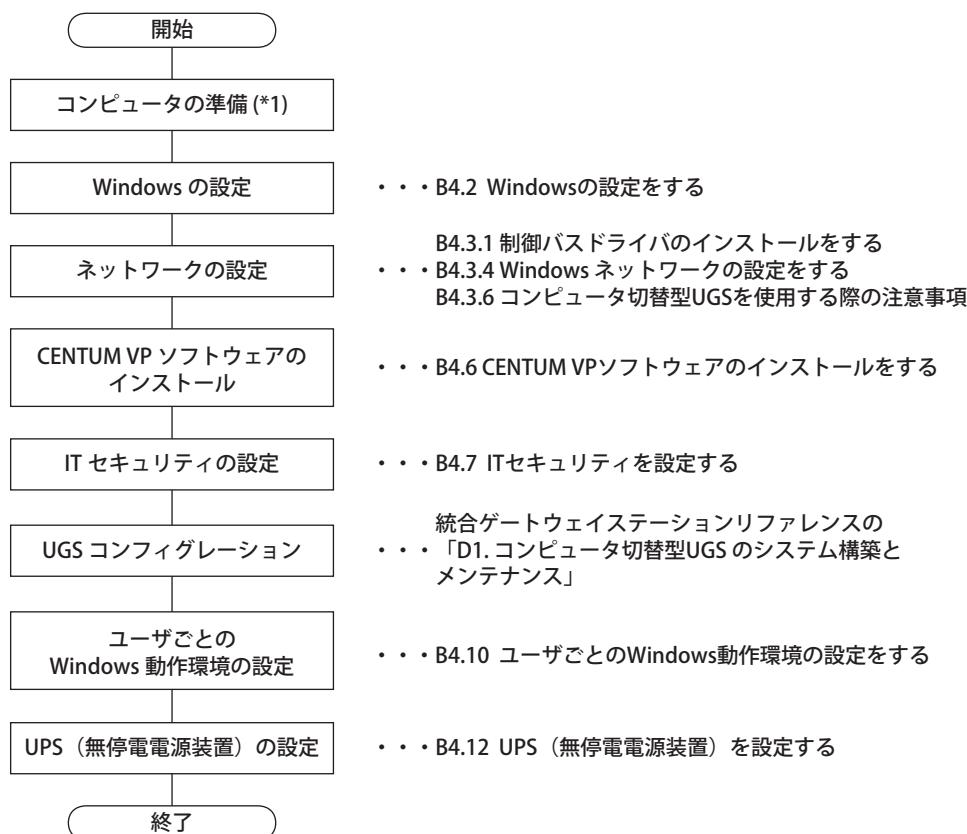
A2.2.12 コンピュータ切替型 UGS のセットアップ手順

重要

コンピュータ切替型 UGS のセットアップ作業に関する注意事項があります。

- コンピュータ切替型 UGS のセットアップのときは、CENTUM VP ソフトウェアのインストール前にコンピュータをドメイン参加させないでください。
- CENTUM VP ソフトウェアのインストール後のセキュリティ設定では、いったん従来モデルや標準モデル（スタンダードアロン管理）に設定してください。
- コンピュータをドメイン参加させたあとで、ドメイン管理または併用管理に変更してください。
- コンピュータ切替型 UGS をドメイン環境で使用する場合は、Windows Guest OS 側と PC 冗長化プラットフォーム側で Windows Domain 設定が必要となります。

コンピュータ切替型 UGS のセットアップ手順を次の図に示します。



*1: コンピュータ切替型UGS専用のコンピュータを用意して、PC冗長化プラットフォームをインストールしてください。冗長化構成の場合は、2台のコンピュータ切替型UGS専用のコンピュータを用意し、それぞれにPC冗長化プラットフォームをインストールしてください。

図 A2.2.12-1 コンピュータ切替型 UGS のセットアップ手順

補足

- コンピュータ切替型 UGS 専用のコンピュータについては、当社にお問い合わせください。
- 冗長化構成の場合は、「コンピュータの準備」の工程で、2台のコンピュータ切替型 UGS 専用のコンピュータに PC 冗長化プラットフォームをインストールしてください。「Windows の設定」以降は、稼動側となる1台目のコンピュータのみ作業を実施してください。「UGS コンフィグレーション」の工程で、待機側となる2台目のコンピュータを稼動側コンピュータに接続して等値化を行います。

A2.2.13 UACS ステーションのセットアップ手順

UACS ステーションのセットアップ手順を次に示します。

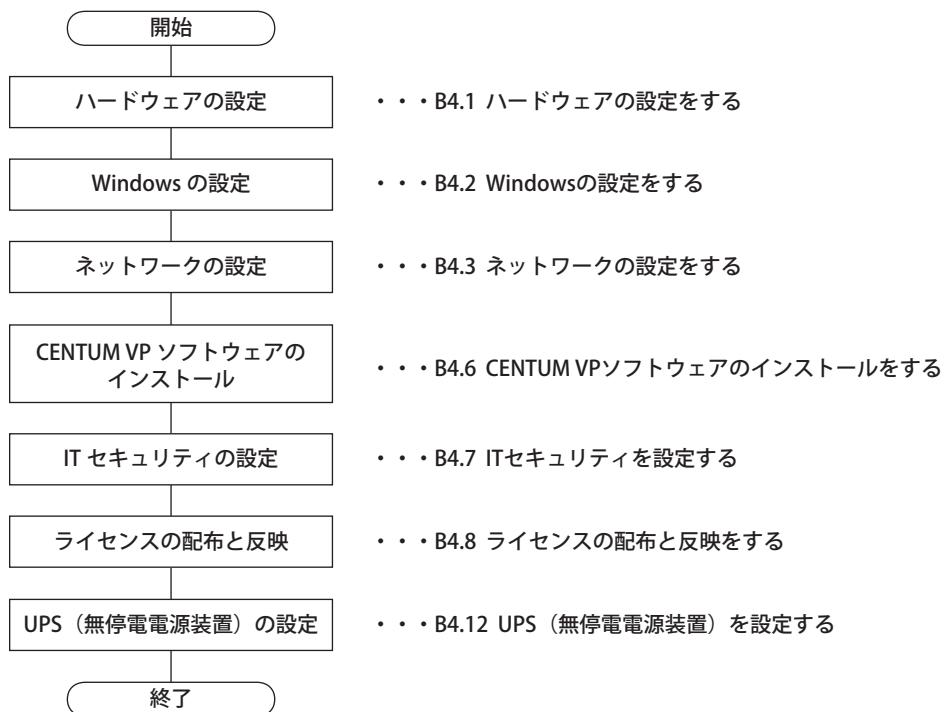


図 A2.2.13-1 UACS ステーションのセットアップ手順

A2.3 メンテナンスに関する説明

次に示すメンテナンス作業を実施するときには、Part C を参照してください。

- ・ライセンスの追加や割り付けを変更する
- ・ドメイン環境をあとから構築する
- ・バックアップをとる
- ・バージョンアップ/レビューションアップやアップグレードをする
- ・CENTUM VP ソフトウェアのアンインストールをする
- ・CENTUM VP ソフトウェアの再インストールをする
- ・バージョンアップ/レビューションアップ時の注意事項

Blank Page

A3. 動作環境

ここでは、CENTUM VP が動作するために必要なハードウェア環境、ソフトウェア環境などについて説明します。

■ ハードウェア環境

各ステーションやコンピュータが動作するために必要なハードウェア環境については、以下を参照してください。

参照

HIS のハードウェア環境については、以下を参照してください。

VP6H1100 操作監視基本機能 (GS 33J05D10-01JA)

GSGW のハードウェア環境については、以下を参照してください。

VP6B1250 汎用サブシステムゲートウェイパッケージ (GS 33J20F10-01JA)

SIOS のハードウェア環境については、以下を参照してください。

VP6B2100 システム統合 OPC クライアントパッケージ (GS 33J20D10-01JA)

APCS のハードウェア環境については、以下を参照してください。

VP6F1200 APCS 制御機能 (GS 33J15U10-01JA)

システム生成機能のみを搭載したコンピュータのハードウェア環境については、以下を参照してください。

VP6E5000 エンジニアリングサーバ機能 VP6E5100 エンジニアリング基本機能 (GS 33J10D10-01JA)

AD サーバのみを搭載したコンピュータのハードウェア環境については、以下を参照してください。

VP6E5000 エンジニアリングサーバ機能 VP6E5100 エンジニアリング基本機能 (GS 33J10D10-01JA)

ファイルサーバのハードウェア環境については、以下を参照してください。

「■ ファイルサーバの OS とハードウェア環境」ページ B6-1

UGS のハードウェア環境については、以下を参照してください。

- VP6B1500 統合ゲートウェイステーション基本機能 (GS 33J20C10-01JA)

- VP6B1600 統合ゲートウェイステーション (UGS2) 基本機能 (GS 33J20C20-01JA)

■ ソフトウェア環境

ソフトウェア環境について説明します。

● サポートする OS

- Windows 10 Enterprise 2016 LTSB (64 ビット) (*1)
- Windows 10 IoT Enterprise 2016 LTSB (64 ビット) (*1)
- Windows 10 Pro Semi-Annual Channel (64 ビット、32 ビット) (*2)
- Windows 7 Professional SP1 (64 ビット)
- Windows 7 Professional SP1 (32 ビット) (*2)
- Windows Server 2016 Standard (64 ビット)
- Windows Server 2012 R2 Standard (64 ビット) (*3)
- Windows Server 2008 R2 SP1 Standard (64 ビット)

*1: LTSB は機能更新がされず、セキュリティパッチと修正プログラムだけが提供されるモデルです。Windows 10 Enterprise LTSB は、他の Windows 10 のモデルとは機能的に違いがあるため注意してください。LTSB は、ボリュームライセンスだけで販売されます。

- *2: HIS 機能を搭載しない汎用コンピュータで、OPC クライアントアプリケーションを動作させる場合として使用できます。
- *3: コンピュータ切替型 UGS だけサポートします。また、CENTUM ソフトウェアが動作しないドメインコントローラやファイルサーバとして使用できます。

補足

Windows Server 2008 SP2 Standard Edition は、CENTUM ソフトウェアが動作しないドメインコントローラやファイルサーバとして使用できます。

重要

- Windows がプリインストールされたコンピュータでは、Windows の OS 以外にユーティリティなどがインストールされていることがあります。これらは CENTUM VP の動作に不要なだけではなく、動作に影響することもあります。Windows の OS を再インストールすることを推奨します。
- 本書では、OS インストール直後の初期状態から必要となる設定を記載しています。OS 内の機能追加や設定変更、OS 以外の機能のインストールなどは不用意に行わないでください。
- セキュリティパッチの適用は、お客様のセキュリティ対策方針に従って実施していくことが前提です。当社では、CENTUM VP システムにセキュリティパッチを適用することを推奨します。システムの運用開始前に必要なセキュリティパッチをすべて適用し、また運用開始後に発行されたセキュリティパッチも、できるだけ早い機会に適用することを推奨します。当社はセキュリティパッチ適用のサービスを提供していますので、より具体的な内容については、当社サービスまでお問い合わせください。
- Windows 10 Enterprise LTSB のコンピュータを使用する場合は、Windows 10 の OS インストール時にカスタマイズしてください。

参照

Windows 10 Enterprise LTSB のインストール時のカスタマイズ方法については、以下を参照してください。

「Appendix 3. Windows 10 インストール時のカスタマイズ」ページ App.3-1

仮想化プラットフォームが動作するハードウェアおよび仮想化プラットフォームの仮想マシンで動作する当社システム製品については、以下を参照してください。

IA システム製品仮想化プラットフォーム (GS 30A05B10-01JA)

● 共存できるソフトウェア

CENTUM VP は次のソフトウェアと共存できます。

これら以外のソフトウェアをインストールした場合、CENTUM VP の動作に影響する可能性があります。

表 A3-1 共存できるソフトウェア一覧

分類	ソフトウェア名称	バージョン (*1)	備考
表計算	Microsoft Excel (32 ビット) (*2)	2010 SP2、2013 SP1、2016	帳票パッケージ、FCS データ設定／収集パッケージ (PICOT) で使用 (*3)
ワープロ	Microsoft Word (32 ビット) (*2)	2010 SP2、2013 SP1、2016	AD スイートのモジュールベースエンジニアリングパッケージで 2013 SP1、または 2016 を使用
ソフトウェア開発	Microsoft Visual Studio	2017(*4)	
WWW ブラウザ	Microsoft Internet Explorer	11	オンラインマニュアル、セルフドキュメント、CAMS for HIS、UACS、および AD スイートの依存関係解析ツールで使用

次に続く

表 A3-1 共存できるソフトウェア一覧（前から続く）

分類	ソフトウェア名称	バージョン(*1)	備考
アプリケーション開発	.NET Framework (*5)	4.6.2 (*6)、4.7.1 (*7)	
UPS ソフトウェア	APC PowerChute Business Edition	8.0.1、9.0.1、9.1.1、9.2.1、9.5	
	APC PowerChute Network Shutdown (*8)	v4.1.0、v4.2.0	
	オムロン PowerAct Pro	4.8	
セキュリティ	横河標準アンチウイルスソフトウェア (*9)		
	エンドポイントセキュリティ対策用ホワイトリストティングソフトウェア (*10)		形名：SS1WL1C、SS1WL1S
ドキュメント閲覧	Adobe Acrobat Reader	DC、2017	Pro、Standard
	Adobe Acrobat	DC、2017	

*1: 「バージョン」の SP は、Service Pack を示します。

*2: Office 共有機能にある Visual Basic for Applications および VBA プロジェクトのデジタル証明書のインストールが必要です。

*3: Microsoft Excel を使用するときは、セキュリティ設定の変更が必要です。

*4: Microsoft Visual Studio 2017 は、Windows10 の Enterprise 2016 LTSB と IoT Enterprise 2016 LTSB では動作しません。

*5: .NET コンポーネントを作成するときは、ユーザプログラム開発環境を備えたコンピュータに、.NET Framework 4.6.2 開発者パックをあらかじめインストールしてください。その後、.NET コンポーネントの作成時に.NET Framework 4.6.2 を指定してください。.NET Framework 4.6.2 以外のバージョンを指定した場合、グラフィックビューで.NET コンポーネントが動作しません。

*6: Windows 10 Pro 以外は、.NET Framework 4.6.2 となります。

*7: .NET Framework 4.7.1 は、Windows 10 Pro では、プリインストールされています。

*8: コンピュータ切替型 UGS だけ共存可能です。

*9: McAfee 社製のアンチウイルスソフトウェア製品をベースにした、当社制御システム用に用意したアンチウイルスソフトウェアです。

*10: McAfee 社製のアプリケーションコントロールテクノロジーをベースにした、当社制御システム用に用意したホワイトリスト方式のソフトウェアです。Windows Server 2016 では動作しません。

補足

- CENTUM VP のマニュアルでは、Adobe Reader と Adobe Acrobat Reader を特に区別するとき以外は、両者の総称として、Adobe Reader と呼びます。
- 共存できるソフトウェアをインストールしたあとに、ライセンス認証と使用許諾の同意を行ってください。

参照

帳票パッケージで Microsoft Excel のセキュリティ設定を変更する手順については、以下を参照してください。

CENTUM VP オプション機能リファレンス (IM 33J05H10-01JA) の「2.1 帳票パッケージを使用するための設定を行う」

FCS データ設定／収集パッケージ (PICOT) で Microsoft Excel のセキュリティ設定を変更する手順については、以下を参照してください。

CENTUM VP オプション機能リファレンス (IM 33J05H10-01JA) の「3.1 PICOT の概要」の「■ PICOT を使用する際の注意事項」

● 帳票パッケージと Microsoft Excel のバージョンの関係

帳票パッケージを使用する場合、Microsoft Office 製品のサービスリリースのバージョンにより、動作が影響される場合があります。

複数のコンピュータで帳票を作成する場合は、Microsoft Excel のバージョンを統一してください。

参照

Microsoft Excel の旧バージョンで作成した帳票を Excel の新バージョンで使用する場合の手順については、以下を参照してください。

CENTUM VP オプション機能リファレンス (IM 33J05H10-01JA) の「2.3 帳票作成作業の流れ」の「■ 帳票の定義」

B. 新規セットアップをする

ここでは、各ステーションのセットアップをする手順について説明します。

Blank Page

B1. セットアップの準備をする

ここでは、セットアップの前に決定すべき項目や、セットアップの注意事項について説明します。

■ セットアップ前に決定すべき項目

セットアップ作業の前に決めておく事項を次に示します。

補足

コンピュータ切替型冗長化 UGS は、2 台のコンピュータで構成されますが、2 台で 1 つのステーションという定義となります。

● ドメイン番号／ステーション番号

ドメイン番号とは、1 つの制御バスに接続されたステーションのグループの番号です。1 から 16 の範囲で設定します。

ステーション番号は、各ステーションに付けられた番号です。各ドメイン内で、1 から 64 の範囲で設定します。

● コンピュータ名／ステーション名

コンピュータ名とは、Windows ネットワーク上の各コンピュータを識別するための名称です。Windows のコントロールパネルから設定できます。

ステーション名とは、CENTUM VP システムで制御バスアドレスより固有に付けられる名称です。

例： HISddss (HIS またはシステム生成機能のみを搭載したコンピュータ)

BCVOddss (SIOS)

FCSddss (GSGW または APCS)

BCVUddss (UGS)

STNddss (コンピュータ)

UACSddss (UACS ステーション)

(ddss : dd はドメイン番号、ss はステーション番号)

重要

すべてのステーションでコンピュータ名とステーション名を必ず一致させてください。コンピュータ名とステーション名が一致していない場合、CENTUM VP の動作の保証はできません。

● IP アドレス

各ステーションの制御バス、Ethernet それぞれの IP アドレスを決めてください。

Ethernet を敷設せずに Vnet/IP を使用する場合は、Vnet/IP オープン通信の IP アドレスも決めてください。

UACS 専用 Ethernet を使用する場合は、UACS 専用 Ethernet に接続するステーションの IP アドレスも決めてください。

● サブネットマスク

各ステーションの制御バス、Ethernet それぞれのサブネットマスクを決めてください。

Ethernet を敷設せずに Vnet/IP を使用する場合は、Vnet/IP オープン通信のサブネットマスクも決めてください。

UACS 専用 Ethernet を使用する場合は、UACS 専用 Ethernet のサブネットマスクも決めてください。

● 管理者アカウントとパスワード

コンピュータの管理者アカウントとパスワードを決定しておいてください。

ドメイン環境で使用する場合は、ドメインの管理者アカウントとパスワードを決定しておいてください。

● セキュリティモデルとユーザ管理方法

IT セキュリティツールで設定するセキュリティモデルとユーザ管理方法を決めておいてください。

重要

- IT セキュリティツールで設定する「セキュリティモデル」と「ユーザ管理方法」により、セットアップ作業手順の一部が異なってきますので、セットアップ作業を開始する前に、必ずシステム全体のセキュリティ設定に関する方針を決定してください。
- 従来モデルを選択した場合は、一部の環境で Windows OS に関する制限が発生します。そのため、標準モデルを選択することを推奨します。

参照

セキュリティについては、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「2. セキュリティモデル」

● ユーザ認証モード

セキュリティモデルとして標準モデルを使用する HIS とシステム生成機能のみを搭載したコンピュータの場合は、セットアップするコンピュータが所属する CENTUM プロジェクトを、どのような認証モードで運用するか決めておいてください。

参照

ユーザ認証モードについては、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「2.2.2 CENTUM VP のユーザ認証モード」

● ライセンスの割り付け

セットアップするコンピュータに、どのようにライセンスを割り付けるかを決めておいてください。

重要

CENTUM のシステムでは、ライセンス管理ステーションを 1 台決める必要があります。ライセンス管理ステーションは、HIS などのステーションが動作するコンピュータにセットアップできます。

各ステーションをセットアップする際には、ライセンス管理ステーションを最初にセットアップしてください。その後、各ステーションをセットアップしてください。各ステーションにインストールしたソフトウェアパッケージは、ライセンス管理ステーションからライセンスを配布し、反映すると、使用可能になります。

ライセンス管理ステーションを独立させたい場合は、ライセンス管理専用のコンピュータとしてセットアップすることもできます。

参照

ライセンスについては、以下を参照してください。

ライセンス管理 (IM 33J01C20-01JA) の「1.1 ライセンス管理」

■ セットアップするときの注意事項

セットアップするときの注意事項を次に示します。

● ディスクドライブの空き容量の確認

CENTUM VP ソフトウェアは、次に示す場所にインストールされます。

このインストール先のディスクドライブに十分な空き容量があることを確認してください。

- インストーラで指定するインストール先フォルダ（デフォルトでは<システムドライブ>¥CENTUMVP¥）

● Windows の設定変更

CENTUM VP ソフトウェアをインストールすることにより、次の Windows の設定が変更されます。

表 B1-1 Windows の設定変更

項目	設定	目的
ログオン時のアカウント名の表示	無効	ログオンアカウント名の漏洩を防止するため。
簡易ユーザ切り替え	無効	複数ユーザの同時ログオンには対応していないため。
Windows の自動更新	無効 (*1) (*2)	CENTUM VP のソフトウェアが動作するコンポーネントは連続運転を前提としているので、Windows の自動更新による再起動はさせないようにするため。

*1: Windows 10 と Windows Server 2016 の場合、Windows の自動更新は自動で無効化されません。CENTUM VP ソフトウェアのインストール前の設定で手動で無効にしてください。

*2: Windows Server Update Service (WSUS) を利用する場合は、CENTUM VP ソフトウェアのインストール後に、Windows の自動更新を手動で有効にしてから、WSUS の設定を行ってください。

参照

Windows の自動更新を手動で有効にする手順については、以下を参照してください。

「■ Windows Update を有効にする」ページ C7-7

● プロジェクト内のレビューションの混在

異なる CENTUM ソフトウェアレビューションで動作する FCS や HIS が混在する場合、システム生成機能が搭載されたコンピュータとライセンス管理ステーションは混在するレビューションの中で最新のレビューションにしてください。

● ユーザーアカウント制御ダイアログが表示されたら

インストール作業の途中で、その条件によってはユーザーアカウント制御ダイアログが表示されることがあります。

その場合は、[はい] または [続行]（アンインストール時は [はい] または [許可]）をクリックして、作業を続行してください。

● コントロールパネルの表示方法

セットアップ作業の中で、Windows のコントロールパネルを表示させることができます。本 IM では、Windows 7 の場合、コントロールパネルの表示方法として「カテゴリ」表示を選択してのメニュー選択方法を記載しています。

● Windows 更新プログラムのダウンロード（Windows 10）

Windows 更新プログラムのダウンロード条件は、次のとおりです。

- コンピュータの OS が Windows 10 Enterprise 2016 LTSB である。

- コンピュータを、システム生成機能を搭載した HIS、またはシステム生成機能を搭載したコンピュータにする予定である。

次に示す Windows 更新プログラムをダウンロードし、適用してください。適用しない場合、セルフドキュメント印字で目次が印刷されないことがあります。

- 2019年2月のサービススタック更新プログラム
- 2019年3月の更新プログラム

補足

- 本情報は、2019年3月時点のものです。最新情報は、エンドポイントセキュリティ対策サービスとして提供しています。エンドポイントセキュリティ対策サービスについては、当社にお問い合わせください。
- すでに適用済みの場合、インストールでエラーになることがあります、このエラーは無視してください。

● Windows 更新プログラムのダウンロード（Windows Server 2012 R2）

次に示す Windows 更新プログラムをダウンロードし、適用してください。適用しない場合、Windows Server 2012 R2 上の共有フォルダ、ファイルにアクセスするとエラーが発生して、アクセスできません。

- 2016年12月の Windows Server 2012 R2 用のサービススタック更新プログラム
- 2014年4月の Windows Server 2012 R2 Update
- 2014年11月の Windows Server 2012 のセキュリティ更新プログラム

補足

本情報は、2019年3月時点のものです。最新情報は、エンドポイントセキュリティ対策サービスとして提供しています。エンドポイントセキュリティ対策サービスについては、当社にお問い合わせください。

● Windows 更新プログラムのダウンロード（Windows 7 または Windows Server 2008 R2）

次に示す Windows 更新プログラムをダウンロードし、適用してください。適用しない場合、操作監視機能が起動しないことがあります。

- 2018年12月マンスリー品質ロールアップ

補足

本情報は、2019年3月時点のものです。最新情報は、エンドポイントセキュリティ対策サービスとして提供しています。エンドポイントセキュリティ対策サービスについては、当社にお問い合わせください。

● .NET Framework 開発者パックのダウンロード

.NET コンポーネントを作成するときは、ユーザプログラム開発環境を備えたコンピュータに、.NET Framework 4.6.2 開発者パックをあらかじめダウンロードしてください。

マイクロソフトのダウンロードセンターから開発者パックで検索して、入手してください。

● 他製品と接続するとき

CENTUM VP を当社の他製品と接続するときは、セキュリティ設定などの作業が必要となることがあります。

参照

他製品と接続するときの作業については、以下を参照してください。

「D. 他製品との接続」ページ D-1

● IT セキュリティ設定の初期データに関する注意事項

ファイルサーバやドメインコントローラでは、IT セキュリティ設定を適用する前の状態を初期データとして保存しておく必要があります。

ユーザ管理方式や IT セキュリティ設定項目の変更時に、保存しておいた初期データを使って、IT セキュリティ設定を適用する前の状態に戻してから、IT セキュリティ設定の再適用を行います。

ファイルサーバについては、セキュリティ設定の変更時に、ユーザ管理方式によって、次のような IT セキュリティ設定の保存データが必要になります。

- ・ 標準モデルでユーザ管理方式がスタンダードアロン管理の場合：
スタンダードアロンの状態で、IT セキュリティ設定の初回適用前に保存したデータ
- ・ 標準モデルでユーザ管理方式がドメイン管理／併用管理の場合：
ドメインに参加した後で、IT セキュリティ設定を適用する前に保存したデータ

参照

ファイルサーバ専用コンピュータの IT セキュリティ設定の保存については、以下を参照してください。

「■ 手順 6：IT セキュリティ設定の初期データを保存する」ページ B6-6

IT セキュリティを再適用する手順については、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「6.3.2 ファイルサーバやドメインコントローラの場合」

Blank Page

B2. Windows ドメイン環境の設定をする

ここでは、CENTUM VP を Windows ドメイン環境で使用する場合に必要な設定について説明します。Windows ドメイン環境は、あとから構築することもできます。

参照

Windows ドメイン環境をあとから構築する方法については、以下を参照してください。

「C3. ドメイン環境をあとから構築する」ページ C3-1

■ ドメインコントローラによる IT セキュリティ設定の統合管理

CENTUM VP では、ドメインコントローラで IT セキュリティ設定を統合管理できます。IT セキュリティ設定を統合管理するためには、すべてのクライアントで IT セキュリティを設定したあとに、ドメインコントローラで IT セキュリティ設定の統合管理の設定を行ってください。

参照

クライアントでの IT セキュリティの設定方法については、以下を参照してください。

「B4.7 IT セキュリティを設定する」ページ B4-96

IT セキュリティ設定の統合管理の設定については、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「6.9 アクティブディレクトリによる IT セキュリティ設定の統合管理」

B2.1 ドメイン環境設定の概要

ドメイン環境設定の概要を説明します。

ドメインコントローラは、停止するとシステム全体に影響が出るため、冗長化させることを推奨します。

■ 作業の流れ

Windows ドメイン環境の設定手順を次に示します。

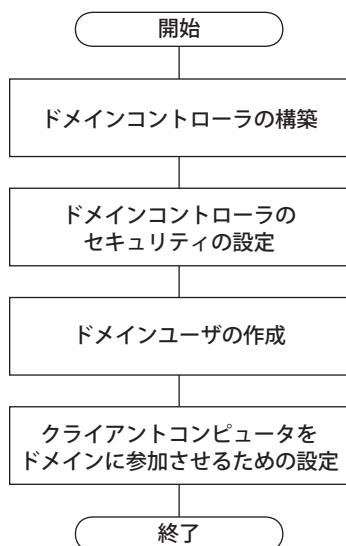


図 B2.1-1 Windows ドメイン環境の設定手順

■ 事前に決めておくこと

- ・ ドメイン名
- ・ ドメインコントローラの IP アドレス

■ 準備するもの

- ・ ドメインコントローラ用コンピュータ
- ・ CENTUM VP ソフトウェアメディア
セキュリティ設定に必要です。

■ 事前にドメインコントローラに設定しておくこと

- ・ IP アドレス
- ・ Administrator アカウントのパスワード

■ フォレストとドメインの機能レベルの設定

ドメインコントローラを構築するときにフォレストの機能レベルとドメインの機能レベルを設定する必要があります。そのときに設定する機能レベルは、新規にフォレストとドメインを構築する場合と、既存のフォレストとドメインにドメインコントローラを追加する場合で異なります。

● 新規にフォレストとドメインを構築する場合に設定する機能レベル

設定する機能レベルは、CENTUM VP がサポートするドメインコントローラ用サーバ OS で共通に設定できる最も低い機能レベルを設定してください。

例えば、CENTUM VP がサポートするドメインコントローラ用サーバが次の OS の場合、共通で設定できる最も低い機能レベルは、Windows Server 2008 です。

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012 R2
- Windows Server 2016

補足

将来的に機能レベルが低いサーバ OS がドメインコントローラとして追加される可能性を考慮して、最も低い機能レベルに設定してください。

● 既存フォレストとドメインにドメインコントローラを追加する場合に設定する機能レベル

この場合は、既存のフォレストとドメインの機能レベルが設定されます。そのため、既存のフォレストとドメインの機能レベルにより、ドメインコントローラのサーバ OS が制限されます。

既存のフォレストとドメインの機能レベルにより選択可能なサーバ OS の一覧を次の表に示します。

表 B2.1-1 既存のフォレストの機能レベルと CENTUM VP で選択可能なサーバ OS

既存のフォレストの機能レベル	CENTUM VP で選択可能なサーバ OS
Windows Server 2003	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2016
Windows Server 2008	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2016
Windows Server 2008 R2	Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2016
Windows Server 2012 R2	Windows Server 2012 R2 Windows Server 2016
Windows Server 2016	Windows Server 2016

表 B2.1-2 既存のドメインの機能レベルと CENTUM VP で選択可能なサーバ OS

既存のドメインの機能レベル	CENTUM VP で選択可能なサーバ OS
Windows Server 2003	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2016
Windows Server 2008	Windows Server 2008 Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2016
Windows Server 2008 R2	Windows Server 2008 R2 Windows Server 2012 R2 Windows Server 2016

次に続く

表 B2.1-2 既存のドメインの機能レベルと CENTUM VP で選択可能なサーバ OS (前から続く)

既存のドメインの機能レベル	CENTUM VP で選択可能なサーバ OS
Windows Server 2012 R2	Windows Server 2012 R2 Windows Server 2016
Windows Server 2016	Windows Server 2016

たとえば、既存のフォレストの機能レベルが Windows Server 2003 で、ドメインの機能レベルが Windows Server 2008 R2 の場合、CENTUM VP で選択可能なサーバ OS は Windows Server 2008 R2、Windows Server 2012 R2、および Windows Server 2016 です。

B2.2 ドメインコントローラを構築する（Windows Server 2016/Windows Server 2012 R2）

Windows Server 2016/Windows Server 2012 R2 でのドメインコントローラ構築手順を説明します。

■ 設定手順

1. サーバーマネージャーを起動してください。
2. 左側のペインで、[ダッシュボード] をクリックして、右ペインで [クイックスタート] をクリックしてから、[役割と機能の追加] をクリックしてください。
「役割と機能の追加ウィザード」が表示されます。
3. [次へ] をクリックしてください。
「インストールの種類の選択」が表示されます。
4. [役割ベースまたは機能ベースのインストール] を選択して、[次へ] をクリックしてください。
「対象サーバーの選択」が表示されます。
5. [サーバープールからサーバーを選択] を選択して、[サーバープール] 一覧から、自コンピュータを選択して、[次へ] をクリックしてください。
「サーバーの役割の選択」が表示されます。
6. [Active Directory ドメインサービス] を選択してください。
「機能追加の確認」ダイアログボックスが表示されます。
7. [機能の追加] をクリックしてください。
「サーバーの役割の選択」に戻ります。
8. [次へ] をクリックしてください。
「機能の選択」が表示されます。
9. 内容を確認して、[次へ] をクリックしてください。
「Active Directory ドメインサービス」が表示されます。
10. 内容を確認して、[次へ] をクリックしてください。
「インストールオプションの確認」が表示されます。
11. 内容を確認して、[インストール] をクリックしてください。
「インストール」が開始されます。インストールの完了後、「インストールの結果」が表示されます。
12. [このサーバーをドメインコントローラに昇格する] をクリックしてください。
「Active Directory ドメインサービス構成」ウィザードが表示されます。
13. 次の設定をして、[次へ] をクリックしてください。
 - ・ [新しいフォレストを追加する] を選択する。
 - ・ [ルートドメイン名] ボックスに、あらかじめ決めておいたドメイン名を「ドメイン名+.local」の形式で入力する
「ドメインコントローラオプション」が表示されます。
14. 次の設定をして、[次へ] をクリックしてください。
 - ・ [フォレストの機能レベル] で [Windows Server 2008] を選択する。
 - ・ [ドメインの機能レベル] で、[Windows Server 2008] を選択する。
 - ・ [ドメインネームシステム (DNS) サーバー] が選択されていることを確認する。
 - ・ ディレクトリサービス復元モードのパスワードを入力する。
「DNS オプション」が表示されます。
15. [次へ] をクリックしてください。

補足

ウィンドウに「権限のある親ゾーンが見つからないか」から始まる警告が表示されている場合でも、そのまま [次へ] をクリックしてください。

- 「追加オプション」が表示されます。
16. 自動的に入力される NetBIOS ドメイン名を確認して、[次へ] をクリックしてください。
「パス」が表示されます。
17. 次のフォルダのデフォルトのパスが表示されるので、必要に応じて変更して、[次へ] をクリックしてください。
- ・ データベースのフォルダ
 - ・ ログファイルのフォルダ
 - ・ SYSVOL フォルダ
- 「オプションの確認」が表示されます。
18. 内容を確認して、[次へ] をクリックします。
「前提条件のチェック」が表示されます。
19. チェックに合格していることを確認して、[インストール] をクリックしてください。
インストールが開始します。インストール完了後、コンピュータが自動的に再起動します。

B2.3 ドメインコントローラを構築する（Windows Server 2008 R2/Windows Server 2008）

Windows Server 2008 R2/Windows Server 2008 でのドメインコントローラ構築手順を説明します。

■ 設定手順

1. サーバーマネージャーを起動してください。
2. [サーバーマネージャー] – [役割] を選択して、[役割の追加] をクリックしてください。
「役割の追加ウィザード」が表示されます。
3. [次へ] をクリックしてください。
「サーバーの役割の選択」が表示されます。
4. [サーバーの役割] の [Active Directory ドメインサービス] を選択し、[次へ] をクリックしてください。
「Active Directory ドメインサービス」が表示されます。

補足

Windows Server 2008 R2 の場合、「Active Directory ドメインサービス」が表示される前に、役割の追加ウィザードが表示されます。[必要な機能を追加] をクリックしてください。

5. 内容を確認して、[次へ] をクリックしてください。
「インストールオプションの確認」が表示されます。
6. [インストール] をクリックしてください。
インストールが開始され、終了するとインストールの結果が表示されます。
7. [このウィザードを終了し、Active Directory ドメインサービスインストールウィザード (dcpromo.exe) を起動します。] をクリックしてください。
「Active Directory ドメインサービスインストールウィザード」が表示されます。
8. [次へ] をクリックしてください。
「オペレーティングシステムの互換性」が表示されます。
9. 内容を確認して、[次へ] をクリックしてください。
「展開の構成の選択」が表示されます。
10. [新しいフォレストに新しいドメインを作成する] を選択して、[次へ] をクリックしてください。
「フォレストルートドメイン名」が表示されます。
11. [フォレストルートドメインの FQDN] に、あらかじめ決めておいたドメイン名を「ドメイン名+.local」の形式で入力して [次へ] をクリックしてください。
「フォレストの機能レベルの設定」が表示されます。
12. [フォレストの機能レベル] で [Windows Server 2008] を選択し、[次へ] をクリックしてください。
「ドメインの機能レベルの設定」が表示されます。
13. [ドメインの機能レベル] で [Windows Server 2008] を選択し、[次へ] をクリックしてください。
「追加のドメインコントローラオプション」が表示されます。
14. [DNS サーバー] が選択されていることを確認して [次へ] をクリックしてください。
「データベース、ログファイル、および SYSVOL の場所」が表示されます。

補足

続行の確認のダイアログボックスが表示された場合は、[はい] をクリックしてください。

15. 「データベースのフォルダ」、「ログファイルのフォルダ」、および「SYSVOL フォルダ」を指定し、[次へ] をクリックしてください。
「ディレクトリサービス復元モード Administrator パスワード」が表示されます。
16. ディレクトリサービス復元モード Administrator パスワードを入力し、[次へ] をクリックしてください。
「概要」が表示されます。
17. 内容を確認して、[次へ] をクリックしてください。
Active Directory ドメインサービスの構成が開始され、終了すると「Active Directory ドメインサービスインストールウィザードの完了」が表示されます。
18. [完了] をクリックしてください。
設定を有効にするための再起動を促すダイアログが表示されます。
19. [再起動する] をクリックしてください。

B2.4 ドメインコントローラのセキュリティを設定する

標準モデルのセキュリティ設定を行うシステムの場合、ドメインコントローラでもITセキュリティツールを使用して、標準モデルのセキュリティ設定を行ってください。

補足

ユーザ環境のセキュリティポリシーにより、ドメインコントローラでITセキュリティツール実行しない場合は、ドメインのユーザグループを手動で作成してください。

参照

CENTUM VP で必要とするドメインのユーザグループについては、以下を参照してください。

- ・ CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「2.2.3 ユーザとグループの管理」の「■ Windows のユーザ管理とセキュリティモデルの組み合わせ」の「● タイプ 3：標準モデル／強固モードルードメイン管理」
- ・ CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「2.2.3 ユーザとグループの管理」の「■ Windows のユーザ管理とセキュリティモデルの組み合わせ」の「● タイプ 4：標準モデル／強固モードルー併用管理」

■ Microsoft Visual C++ 2017 再頒布可能パッケージのインストール

ITセキュリティツールを実行する前に Microsoft Visual C++ 2017 再頒布可能パッケージのインストールが必要です。

Microsoft Visual C++ 2017 再頒布可能パッケージをインストールするときは、次の手順に従ってください。

1. 管理者ユーザでドメインコントローラにログオンしてください。
2. CENTUM VP のソフトウェアメディアをドライブへ挿入してください。
3. エクスプローラで、<DVD ドライブ>:\CENTUM\INSTALL\vcredist_x86_2017\VC_redist.x86.exe をダブルクリックしてください。
4. ライセンス条項に同意して、インストールを実行してください。

■ ルート証明書の適用

Windows Server 2008 R2 に.NET Framework 4.6.2 をインストールする前に、ルート証明書の適用が必要です。

補足

Windows Server 2016、Windows Server 2012 R2 および Windows Server 2008 の場合、本作業は不要です。

参照

ルート証明書の適用方法については、以下を参照してください。

「■ ルート証明書を適用する」ページ B4-41

■ .NET Framework のインストール

ITセキュリティツールを実行する前に、次の.NET Framework をインストールする必要があります。

- ・ Windows Server 2008 R2 : .NET Framework 4.6.2
- ・ Windows Server 2008 : .NET Framework 4.5.2

補足

Windows Server 2016 と Windows Server 2012 R2 の場合、本作業は不要です。

.NET Framework をインストールするときは、次の手順に従ってください。

1. 管理者ユーザでドメインコントローラにログオンしてください。
2. CENTUM VP のソフトウェアメディアをドライブへ挿入してください。
3. エクスプローラで、次のファイルをダブルクリックしてください。
 - Windows Server 2008 R2 : <DVD ドライブ>:\CENTUM\INSTALL\DotNetFX462\NDP462-KB3151800-x86-x64-A11OS-ENU.exe
 - Windows Server 2008 : <DVD ドライブ>:\Microsoft\Runtime\DotNetFX452\NDP452-KB3026376-x86-x64-A11OS-ENU.exe
4. ライセンス条項に同意して、インストールを実行してください。

■ IT セキュリティツールを起動するまでの準備

1. 管理者ユーザでドメインコントローラにログオンしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [管理ツール] – [Active Directory ユーザーとコンピューター] を選択してください。
Active Directory ユーザーとコンピューターウィンドウが表示されます。
4. 左のペインの [Users] を右クリックして、[新規作成] – [グループ] を選択してください。
「新しいオブジェクト-グループ」ダイアログが表示されます。

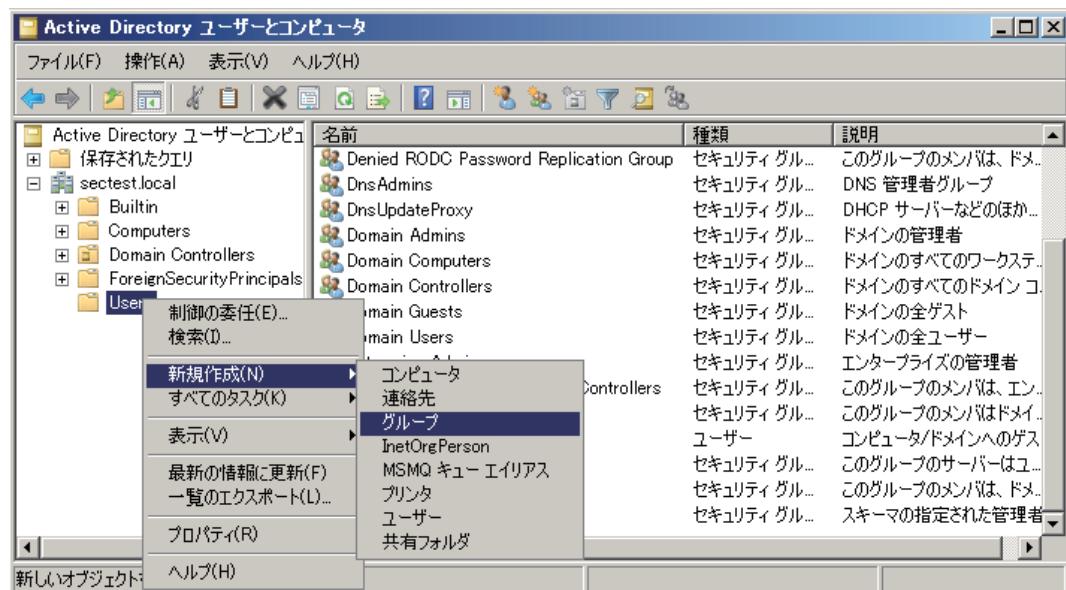


図 B2.4-1 Active Directory ユーザーとコンピュータ

5. [グループ名] に CTM_MAINTENANCE と入力し、[グループのスコープ] と [グループの種類] を選択して、[OK] をクリックしてください。



図 B2.4-2 新しいオブジェクト - グループ

6. 右のペインで [Users] に CTM_MAINTENANCE グループが作成されていることを確認してください。

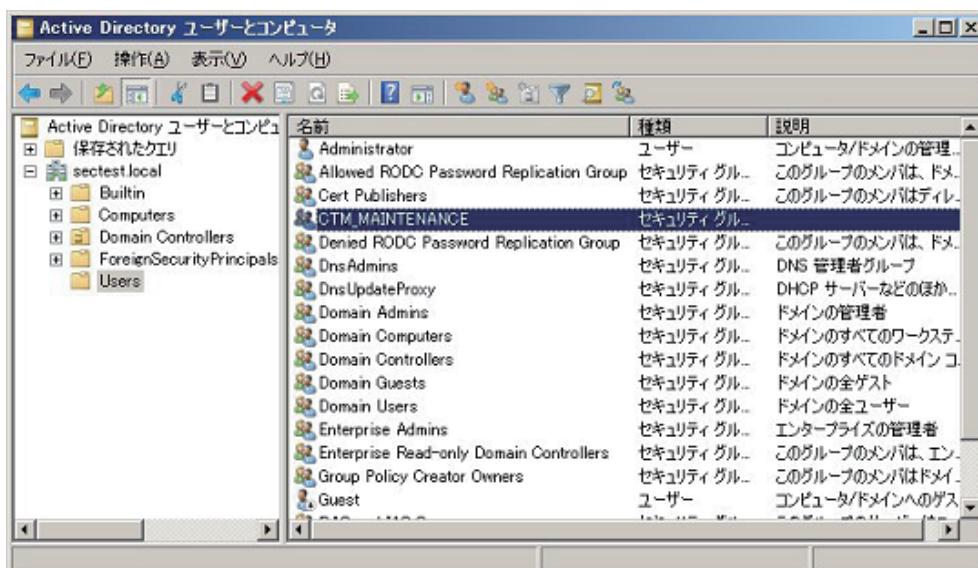


図 B2.4-3 Active Directory ユーザーとコンピュータ（グループの追加後）

7. ログオンしたユーザを CTM_MAINTENANCE と Domain Admins グループに所属させてください。

参照

ユーザをユーザグループに登録する方法については、以下を参照してください。

「■ ドメインユーザをドメイングループに登録する」ページ B2-17

■ IT セキュリティ設定の初期データを保存する

重要

- IT セキュリティ設定項目の変更時に、保存しておいた初期データを使って、IT セキュリティ設定を適用する前の状態に戻してから、IT セキュリティ設定の再適用を行います。そのため、ドメイン構築後、IT セキュリティツールを使ってはじめてセキュリティ設定を実施する前に、必ずセキュリティ設定を保存してください。
- 2 度目以降のセキュリティ設定では、基本的にセキュリティ設定の保存は不要です。しかし、次の場合はセキュリティ設定の初期データを保存し直してください。
 - R5.01～R6.03 の IT セキュリティツールでセキュリティの設定後、R6.04 以降の IT セキュリティツールで IT セキュリティバージョンを 2.0 に変更する場合
 - R4.03 以前の IT セキュリティツールでセキュリティの設定後、R5.01 以降の IT セキュリティツールで IT セキュリティバージョン、セキュリティモデル、または設定項目の選択状態を変更する場合
- セキュリティ設定の初期データを保存し直す場合は、IT セキュリティツールで以前に保存したセキュリティ設定を復元してください。その後、本手順によりセキュリティ設定を保存してください。以降はセキュリティ設定を初期化するときに、この保存し直したデータを使いますので、大切に保管してください。

IT セキュリティツールを実行する前のセキュリティ設定データを保存するには、次の手順に従ってください。

- Domain Admins とドメインの CTM_MAINTENANCE グループに所属するユーザでログオンしてください。
 - CENTUM VP のソフトウェアメディアをドライブへ挿入してください。
 - 自動再生ダイアログが表示された場合、[Launcher.exe の実行] をクリックしてください。
 - 自動再生ダイアログが表示されない場合、エクスプローラでソフトウェアメディアのトップフォルダにある Launcher.exe をダブルクリックしてください。インストールメニューが表示されます。
 - [IT セキュリティ設定 (ファイルサーバ/ドメインコントローラ用)] をクリックしてください。
- IT セキュリティツールが起動されます。

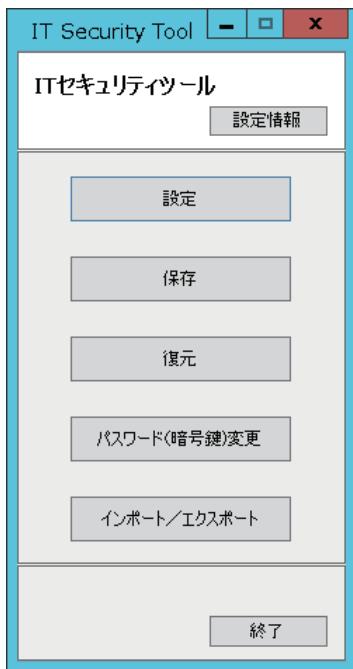


図 B2.4-4 IT セキュリティツールメニュー

4. [保存] をクリックしてください。
保存先の選択ページが表示されます。
5. 保存先を指定し、次の設定項目を入力してください。
 - ・ 識別名
 - ・ 対応製品
 - ・ 対応 OS
 - ・ ファイルバージョン

補足

[識別名] と [ファイルバージョン] は、必要に応じて入力してください。

6. [次へ] をクリックしてください。
アカウント初期パスワードの入力ページが表示されます。
7. 初期パスワードにするパスワードを入力して [次へ] をクリックしてください。
パスワード（暗号鍵）の入力ページが表示されます。

補足

本ツールで保存したアカウントを復元するときにこの初期パスワードが設定されます。保存したアカウントが復元時に存在しない場合は、アカウントを新規作成します。新規作成したアカウントの初期パスワードとして、このパスワードが設定されます。
新規作成されたアカウントが複数ある場合でも、初期パスワードはすべて同じになります。
設定したパスワードが復元する環境のパスワードポリシーを満たさない場合は、アカウント復元時にエラーとなります。
このパスワードはアカウントの初期パスワードとして設定されます。そのため、そのアカウントで初めてログオンするときにパスワード変更が求められます。

8. 保存データを暗号化するためのパスワードを入力して [次へ] をクリックしてください。
セキュリティ設定の保存が開始されます。

重要

- 本パスワード（暗号鍵）を紛失すると、保存したセキュリティ設定が復元できなくなります。パスワード（暗号鍵）の管理は、お客様側で正しく行ってください。
- パスワード（暗号鍵）は1文字以上です。
- パスワード（暗号鍵）に使用できる文字は大文字、小文字のアルファベットと数字、記号`~!@#\$%^&*()_-={}|\\:;`<>?,.です。
全角文字は使用できません。

- 保存が完了したら、[完了] をクリックしてください。
保存に失敗した場合、何に失敗したのかが表示されます。
- ITセキュリティツールメニューの [終了] をクリックしてください。

補足

保存に失敗した項目が表示された場合、当社窓口に連絡してください。

■ ITセキュリティを設定する

- ITセキュリティツールメニューから [設定] をクリックしてください。
確認ダイアログが表示されます。
- 前述の初期化用セキュリティ設定データを保存済みの場合は、[OK] をクリックしてください。
設定モデルの選択ページが表示されます。

補足

保存していない場合は、[キャンセル] をクリックしてメインメニューに戻り、セキュリティ設定を保存してください。

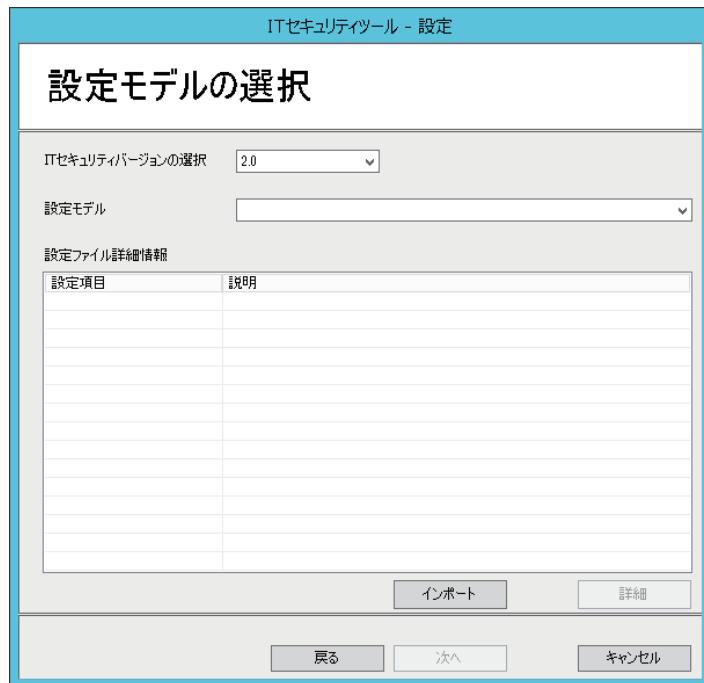


図 B2.4-5 設定モデルの選択

- [ITセキュリティバージョンの選択] で ITセキュリティバージョンを選択してください。
- [設定モデル] ドロップダウンリストから [ドメインコントローラ標準モデルドメイン／併用管理] を選択してください。
- [次へ] をクリックしてください。

設定内容の確認ページが表示されます。

補足

[詳細] をクリックした場合、設定項目の選択ページが表示されます。

6. 以降は、CENTUM VP ソフトウェアインストール後に続けて、IT セキュリティツールを実行する場合と同じ操作をしてください。

参照

IT セキュリティ設定をインポートする手順については、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「6.7 IT セキュリティ設定ファイルをインポート／エクスポートする」

CENTUM VP ソフトウェアインストール後の IT セキュリティ設定の操作については、以下を参照してください。

「B4.7 IT セキュリティを設定する」ページ B4-96

B2.5 ドメインユーザを作成する

ここでは、ドメインユーザを作成し、ドメイングループに登録する方法について説明します。

重要

ドメインで管理しているユーザの権限を変更する場合、その変更が即時には適用されないことがあります。その場合、ユーザの権限を変更したあとに、各コンピュータでログオンとログオフを2回繰り返してください。
ユーザから権限を削除した場合も同様です。

■ ドメインユーザを作成する

1. コントロールパネルを起動してください。
2. [システムとセキュリティ] – [管理ツール] – [Active Directory ユーザーとコンピューター] を選択してください。
Active Directory ユーザーとコンピューターウィンドウが表示されます。
3. 左のペインの [Users] を右クリックして、[新規作成] – [ユーザー] を選択してください。

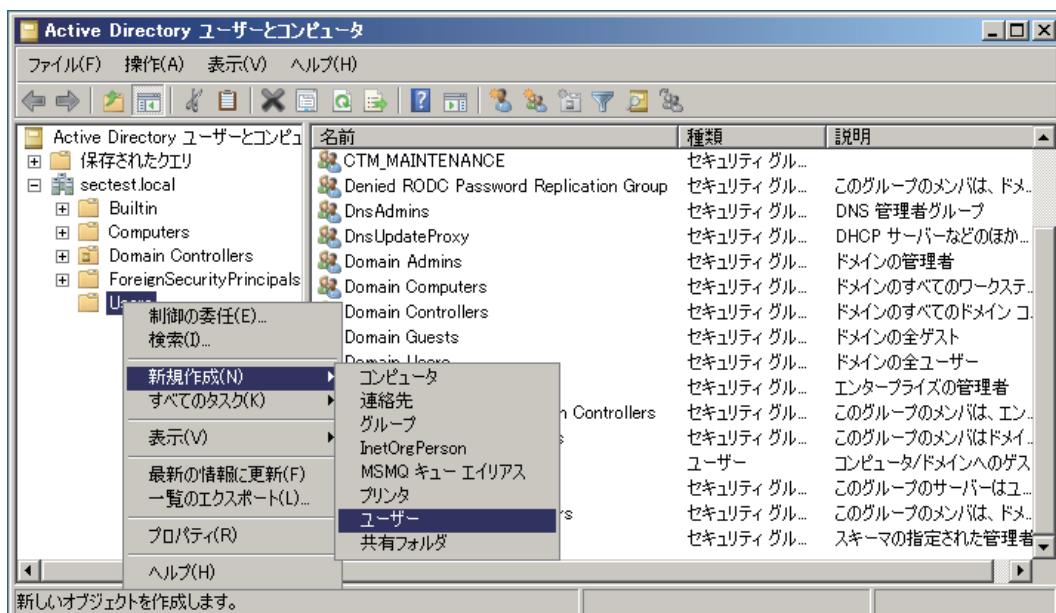


図 B2.5-1 Active Directory ユーザーとコンピュータ

4. 「新しいオブジェクト – ユーザー」が表示されます。必要事項を入力してください。

補足

[フルネーム] と [ユーザーログオン名] は必ず入力する必要があります。また、[ユーザーログオン名] を入力すると、自動的に下の [ログオン名] も入力されますが、変更可能です。

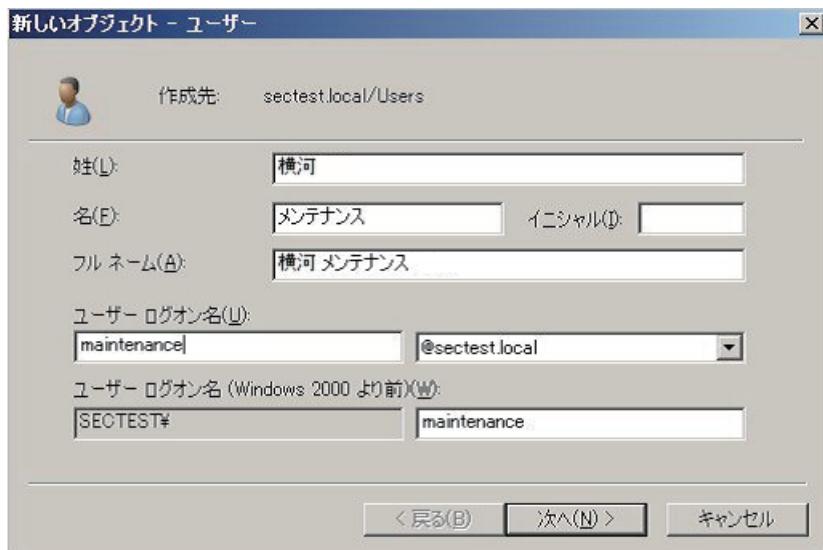


図 B2.5-2 新しいオブジェクト - ユーザー

5. [次へ] をクリックしてください。
パスワード入力のダイアログが表示されます。
6. パスワードを入力し、必要な項目のチェックボックスをオンにして、[次へ] をクリックしてください。
確認ダイアログが表示されます。
7. [完了] をクリックしてください。
8. [Users] を開いて、右のペインに新しいドメインユーザが追加されていることを確認してください。

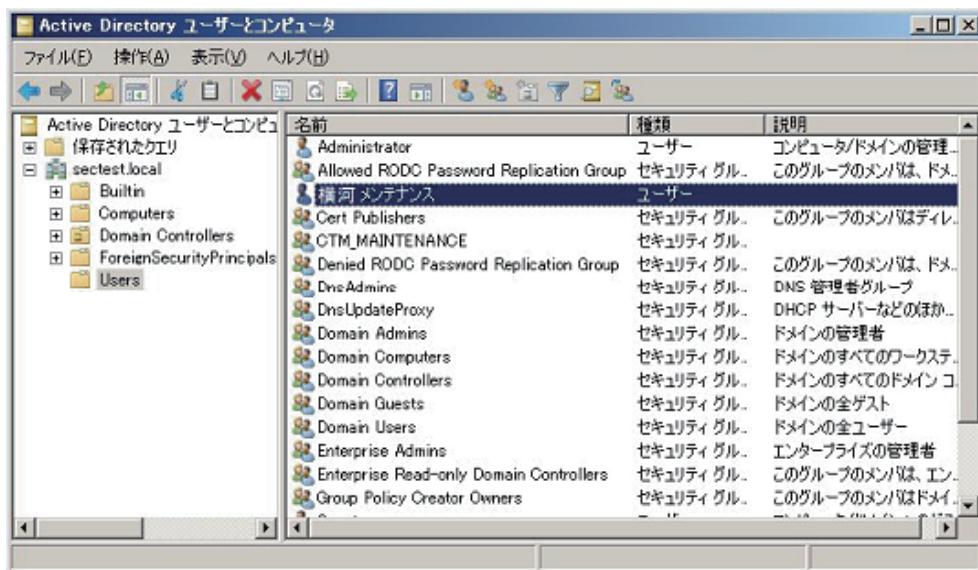


図 B2.5-3 Active Directory ユーザーとコンピュータ（登録の確認）

■ ドメインユーザをドメイングループに登録する

標準モデルのセキュリティを設定する場合は、ドメインユーザを、適切なドメイングループに登録してください。

ドメインコントローラで IT セキュリティツールを実行後は、次の CENTUM VP のドメイングループが作成されています。

- CTM_OPERATOR

- CTM_ENGINEER
- CTM_OPC
- CTM_ENGINEER_ADM
- ADS_MANAGER

補足

CTM_MAINTENANCE グループは、これまでの手順の中で、手動で作成してあります。

● ドメインユーザをドメイングループに登録する

ここでは、CTM_OPERATOR グループにドメインユーザ ("operator"ユーザ) を登録する例を説明します。

ここで説明は管理者権限が不要なユーザについて必要な操作です。

補足

管理者権限が必要なドメイングループに属するドメインユーザへの管理者権限設定方法については、この手順のあとに続く、「●管理者権限の設定」も行ってください。

1. Active Directory ユーザーとコンピュータウィンドウで、グループ権限を設定したいユーザをダブルクリックしてください。
選択したユーザのプロパティダイアログが表示されます。
2. [所属するグループ] タブを選択し、[追加] をクリックしてください。
グループの選択ダイアログが表示されます。
3. [詳細設定] をクリックしてください。
グループの選択ダイアログに詳細設定が表示されます。
4. [検索] をクリックしてグループを表示させ、CTM_OPERATOR グループを選択し、[OK] をクリックしてください。

補足

Windows Server 2008 の場合は、[今すぐ検索] をクリックしてグループを表示してください。

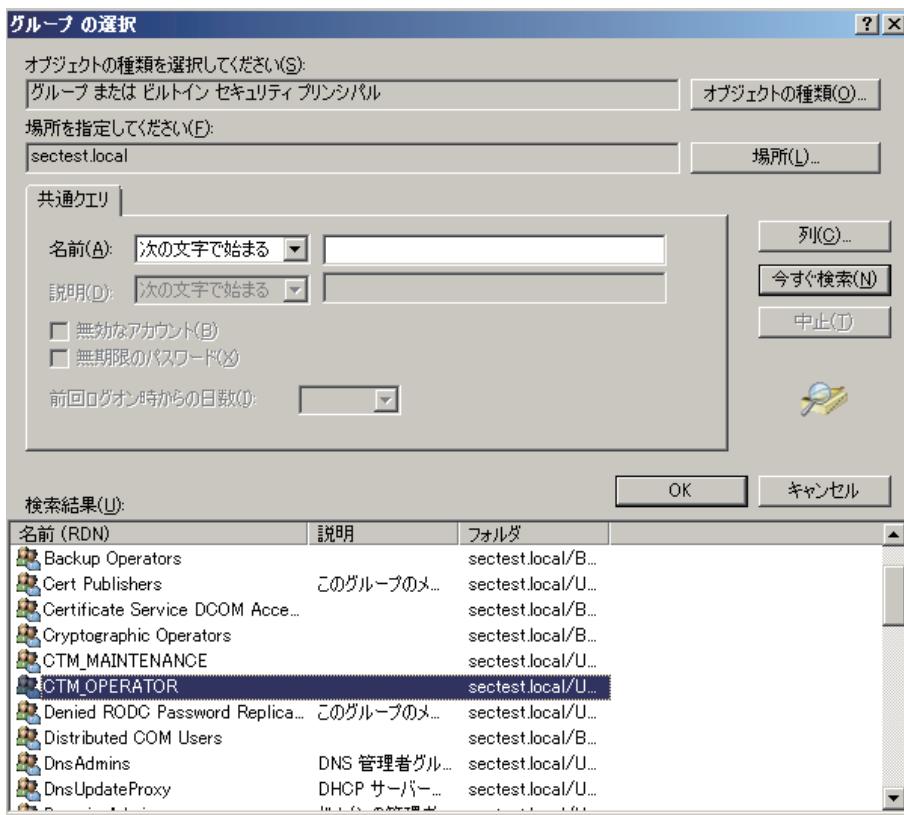


図 B2.5-4 グループの選択（検索結果）

5. グループの選択ダイアログで、CTM_OPERATOR が設定されていることを確認して、[OK] をクリックしてください。
6. CENTUM オペレータのプロパティダイアログで、[所属するグループ] リストに CTM_OPERATOR が表示されていることを確認してください。

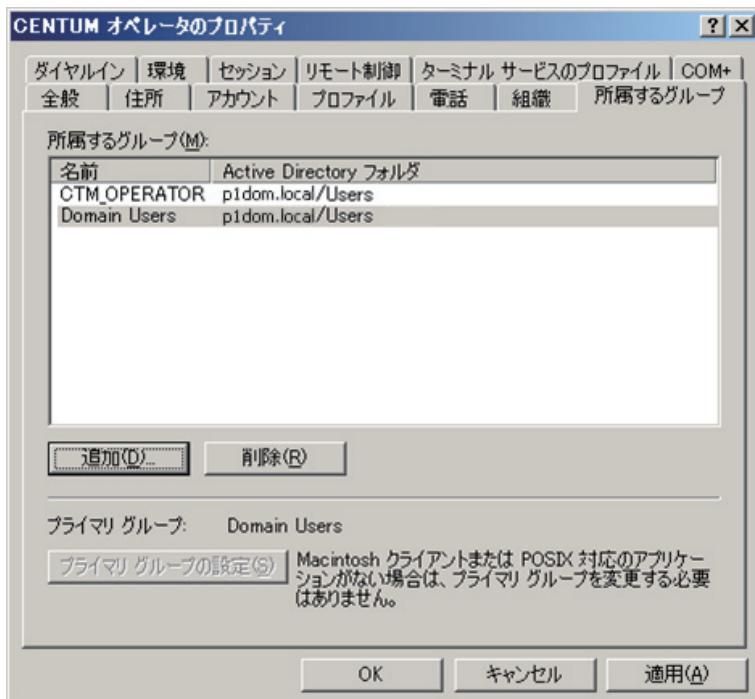


図 B2.5-5 ユーザに設定されているグループの表示

● 管理者権限の設定

管理者権限が必要なドメイングループに属するドメインユーザへの、管理者権限設定方法を説明します。

1. ドメインユーザを「Domain Admins」ユーザグループに所属させてください。
2. そのユーザのプロパティダイアログの「[所属するグループ]」タブで、[Domain Admins] を選択して「[プライマリグループの設定]」をクリックしてください。
ユーザのプライマリグループが Domain Admins に変更されます。
3. [Domain Users] を選択して、「[削除]」をクリックしてください。
4. 「[所属するグループ]」のリストから Domain Users が削除されたことを確認し、「[OK]」をクリックしてください。

B2.6 クライアントコンピュータをドメインに参加させる

クライアントコンピュータをドメインに参加させるには、ドメインコントローラ上にコンピュータアカウントが必要です。コンピュータアカウントの作成は、ドメインコントローラで作成する方法と、クライアントで作成する方法の2つがあります。

コンピュータアカウントをドメインコントローラ側で作成する場合、コンピュータアカウントを作成したあと、クライアント側の設定でクライアントコンピュータをドメインに参加させます。クライアント側から作成する場合、コンピュータアカウントの作成と、ドメインへの参加が同時に行えます。

ここでは、ドメインコントローラでコンピュータアカウントを作成して、クライアント側の設定でコンピュータをドメインに参加させる手順について説明します。クライアントコンピュータで設定する際、ドメインの管理者権限を持つアカウントの「ユーザ名」と「パスワード」が必要です。

■ クライアントコンピュータのセットアップ作業に関する注意事項

- ・ CENTUM VP をドメイン環境で使用する場合は、CENTUM VP ソフトウェアをインストールする前に、コンピュータをドメインに参加させてください。CENTUM VP ソフトウェアインストール後のセキュリティ設定では、標準モデルのドメイン管理または併用管理を選択してください。
- ・ 事前にコンピュータをドメインに参加させることができない場合は、CENTUM VP ソフトウェアインストール後のセキュリティ設定では、いったん従来モデルや標準モデル（スタンダードアロン管理）に設定してください。その後、コンピュータをドメインに参加させたあとで、ドメイン管理または併用管理に変更してください。
- ・ ドメインへ参加させたコンピュータへ CENTUM VP ソフトウェアをインストールするときに、ドメイングループに所属するユーザを使用する場合は、事前にドメインコントローラに CENTUM VP ソフトウェアインストール用の管理者ユーザを作成する必要があります。Domain Admins および CTM_MAINTENANCE のユーザグループに管理者用ユーザを登録しておいてください。
- ・ CENTUM VP ソフトウェアをインストール後、クライアントコンピュータの管理者ユーザを CTM_MAINTENANCE_LCL に登録してください。

参照

セキュリティモデルの変更については、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「6.3 IT セキュリティ設定を変更する」

■ コンピュータ切替型 UGS のセットアップ作業に関する注意事項

- ・ コンピュータ切替型 UGS のセットアップのときは、CENTUM VP ソフトウェアのインストール前にコンピュータをドメインに参加させないでください。
- ・ CENTUM VP ソフトウェアインストール後のセキュリティ設定では、いったん従来モデルや標準モデル（スタンダードアロン管理）に設定してください。
- ・ コンピュータをドメインに参加させたあとで、ドメイン管理または併用管理に変更してください。
- ・ コンピュータ切替型 UGS をドメイン環境で使用する場合は、Windows Guest OS 側と PC 冗長化プラットフォーム側で Windows Domain 設定が必要となります。

■ ドメインコントローラでの設定

1. コントロールパネルを起動してください。
2. [システムとセキュリティ] – [管理ツール] – [Active Directory ユーザーとコンピューター] を選択してください。
Active Directory ユーザーとコンピューターウィンドウが表示されます。
3. 左のペインの [Computers] を右クリックし、[新規作成] – [コンピューター] を選択してください。
「新しいオブジェクト – コンピューター」ダイアログが表示されます。

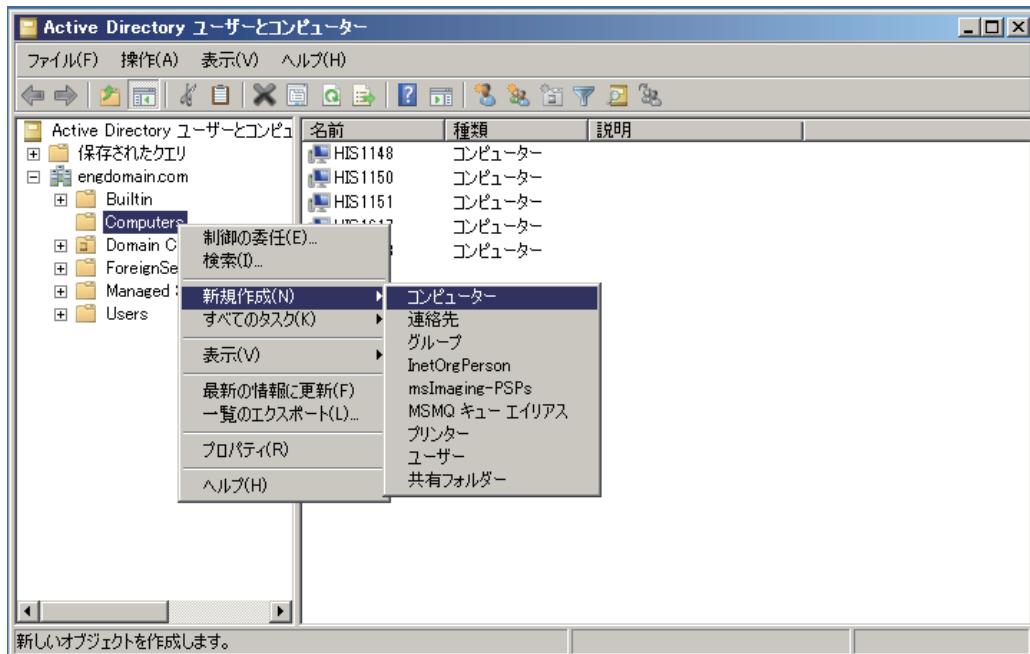


図 B2.6-1 Active Directory ユーザーとコンピューター（新規作成 – コンピューターの選択）

4. [コンピューター名] を入力して、[OK] をクリックしてください。

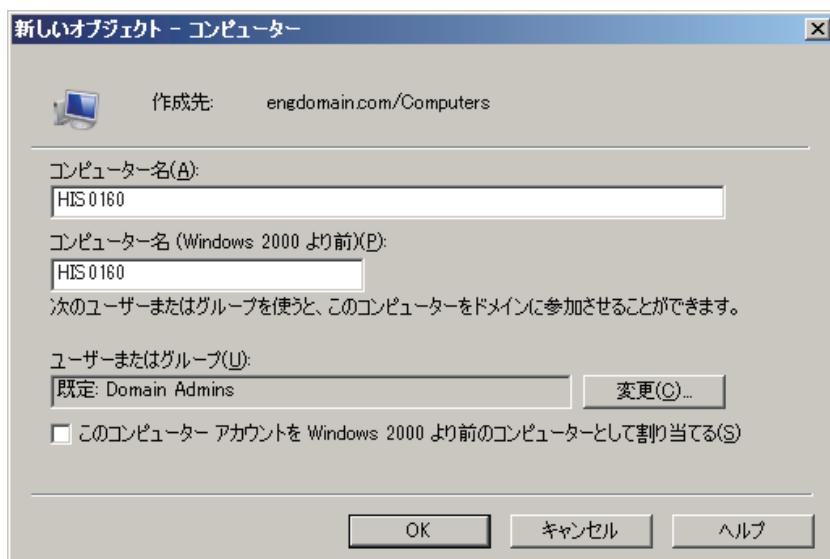


図 B2.6-2 新しいオブジェクト – コンピューター ダイアログ（コンピューター名入力）

5. [Computers] に新しいコンピュータが追加されていることを確認してください。

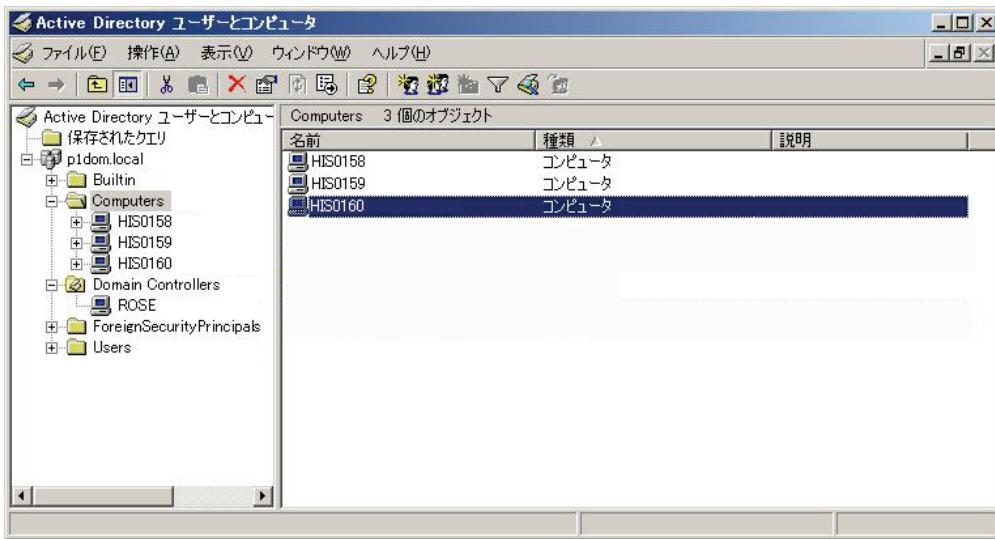


図 B2.6-3 Active Directory ユーザーとコンピュータ（コンピュータ追加の確認）

以上でドメインコントローラでの設定は終了です。このあと、クライアントコンピュータでの設定を行います。

参照

コンピュータ切替型 UGS をドメインに参加させるときの注意事項については、以下を参照してください。

統合ゲートウェイステーションリファレンス (IM 33J20C10-01JA) の「B8.4 コンピュータ切替型 UGS 構築時の注意事項」の「■ ドメインコントローラ設定での注意事項」

■ クライアントコンピュータでの設定 (Windows 10 の場合)

Windows 10 のコンピュータをドメインに参加させるときは、次の手順に従ってください。

1. コントロールパネルを起動してください。
2. [システムとセキュリティ] – [システム] を選択してください。
システムウィンドウが表示されます。
3. [設定の変更] をクリックしてください。
システムのプロパティダイアログが表示されます。
4. [コンピューター名] タブで、[変更] をクリックしてください。
コンピューター名／ドメイン名の変更ダイアログが表示されます。
5. コンピューター名／ドメイン名の変更ダイアログで [ドメイン] を選択し、ドメイン名を入力して [OK] をクリックしてください。
Windows セキュリティダイアログが表示されます。
6. ドメインの管理者権限を持つユーザのユーザ名とパスワードを入力し、[OK] をクリックしてください。

補足

ドメイン名が変更できないことを示すエラーメッセージダイアログが表示されることがあります。ドメインへの参加は成功していますので、[OK] をクリックして進んでください。

7. コンピューター名／ドメイン名の変更ダイアログで [OK] をクリックしてください。
8. 再起動の確認ダイアログで [今すぐ再起動する] をクリックし、コンピュータを再起動してください。

■ クライアントコンピュータでの設定 (Windows 7 の場合)

Windows 7 のコンピュータをドメインに参加させるときは、次の手順に従ってください。

1. コントロールパネルを起動してください。

2. [システムとセキュリティ] – [システム] – [システムの詳細設定] を選択してください。
システムのプロパティダイアログが表示されます。
3. [コンピューター名] タブを選択し、[変更] をクリックしてください。
コンピューター名／ドメイン名の変更ダイアログが表示されます。
4. コンピューター名／ドメイン名の変更ダイアログで [ドメイン] を選択し、ドメイン名を入力して [OK] をクリックしてください。

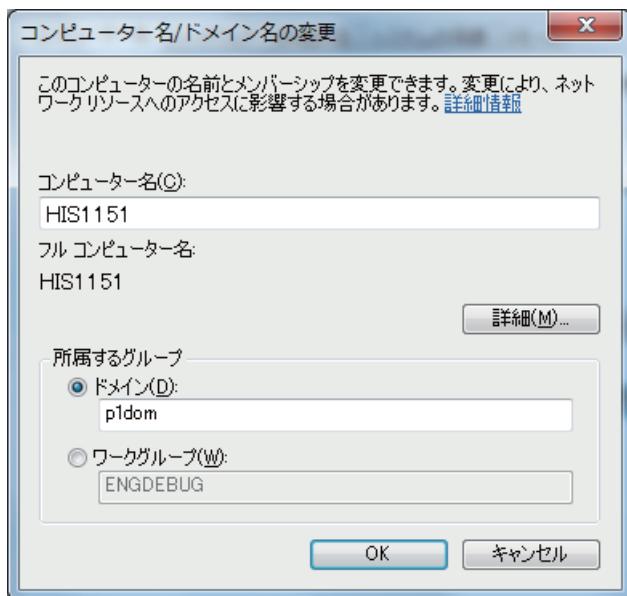


図 B2.6-4 コンピューター名／ドメイン名の変更ダイアログ

5. ダイアログが表示されるので、ドメインの管理者権限を持つユーザのユーザ名とパスワードを入力し、[OK] をクリックしてください。

補足

ドメイン名が変更できないことを示すエラーメッセージダイアログが表示されることがあります。ドメインへの参加は成功していますので、[OK] をクリックして進んでください。

6. コンピューター名／ドメイン名の変更ダイアログで [OK] をクリックしてください。
7. 再起動の確認ダイアログで [今すぐ再起動する] をクリックし、コンピュータを再起動してください。

■ クライアントコンピュータでの設定 (Windows Server 2016 の場合)

Windows Server 2016 のコンピュータをドメインに参加させるときは、次の手順に従ってください。

1. コントロールパネルを起動してください。
2. [システムとセキュリティ] – [システム] を選択してください。
システムウィンドウが表示されます。
3. [設定の変更] をクリックしてください。
システムのプロパティダイアログが表示されます。
4. [コンピューター名] タブで、[変更] をクリックしてください。
コンピューター名／ドメイン名の変更ダイアログが表示されます。
5. コンピューター名／ドメイン名の変更ダイアログで [ドメイン] を選択し、ドメイン名を入力して [OK] をクリックしてください。
Windows セキュリティダイアログが表示されます。

6. ドメインの管理者権限を持つユーザのユーザ名とパスワードを入力し、[OK] をクリックしてください。

補足

ドメイン名が変更できないことを示すエラーメッセージダイアログが表示されることがあります。ドメインへの参加は成功していますので、[OK] をクリックして進んでください。

7. コンピューター名/ドメイン名の変更ダイアログで、[OK] をクリックしてください。
8. 再起動の確認ダイアログで、[今すぐ再起動する] をクリックし、コンピュータを再起動してください。

■ クライアントコンピュータでの設定 (Windows Server 2012 R2 の場合)

Windows Server 2012 R2 のコンピュータをドメインに参加させるとときは、次の手順に従ってください。

1. コントロールパネルを起動してください。
2. [システムとセキュリティ] をクリックしてください。
3. [システム] をクリックしてください。
4. 画面左の [システムの詳細設定] をクリックしてください。
システムのプロパティダイアログが表示されます。
5. システムのプロパティダイアログで、[コンピューター名] タブを選択し、[変更] をクリックしてください。
コンピューター名／ドメイン名の変更ダイアログが表示されます。
6. コンピューター名／ドメイン名の変更ダイアログで [ドメイン] を選択し、ドメイン名を入力して [OK] をクリックしてください。
7. ダイアログが表示されるので、ドメインの管理者権限を持つユーザのユーザ名とパスワードを入力し、[OK] をクリックしてください。

補足

ドメイン名を変更できないことを示す、エラーメッセージダイアログが表示されることがあります。ドメインへの参加は成功していますので、[OK] をクリックして進んでください。

8. コンピューター名／ドメイン名の変更ダイアログで [OK] をクリックしてください。
9. 再起動の確認ダイアログで [今すぐ再起動する] をクリックし、コンピュータを再起動してください。

■ クライアントコンピュータでの設定 (Windows Server 2008 R2 の場合)

Windows Server 2008 R2 のコンピュータをドメインに参加させるとときは、次の手順に従ってください。

1. コントロールパネルを起動してください。
2. [システムとセキュリティ] – [システム] – [システムの詳細設定] を選択してください。
システムのプロパティダイアログが表示されます。
3. [コンピューター名] タブを選択し、[変更] をクリックしてください。
コンピューター名／ドメイン名の変更ダイアログが表示されます。
4. コンピューター名／ドメイン名の変更ダイアログで [ドメイン] を選択し、ドメイン名を入力して [OK] をクリックしてください。
5. ダイアログが表示されるので、ドメインの管理者権限を持つユーザのユーザ名とパスワードを入力し、[OK] をクリックしてください。

補足

ドメイン名が変更できないことを示すエラーメッセージダイアログが表示されることがあります。ドメインへの参加は成功していますので、[OK] をクリックして進んでください。

6. コンピューター名／ドメイン名の変更ダイアログで [OK] をクリックしてください。
7. 再起動の確認ダイアログで、[今すぐ再起動する] をクリックし、コンピュータを再起動してください。

B2.7 ドメインコントローラを冗長化する

ドメインコントローラが停止するとシステム全体に影響が出るため、ドメインコントローラを冗長化させることを推奨します。

■ 設定手順

1. 2台目となるドメインコントローラを、既存ドメインに追加してください。
2. ITセキュリティを設定してください。

参照

ITセキュリティ設定については、以下を参照してください。

「B2.4 ドメインコントローラのセキュリティを設定する」ページ B2-9

B2.8 Windows ドメイン環境での時刻同期を設定する

CENTUM VP を Windows ドメイン環境で使用する場合は、CENTUM VP システムで使用する各コンピュータの時刻とドメインコントローラの時刻を同期させる必要があります。CENTUM VP システムでは、制御バスを時刻マスタとする時刻同期サービスがあるため、Windows ドメイン環境設定をした場合は、ドメインコントローラをクライアントコンピュータの時刻に同期させる方法をとります。時刻を同期させる方法にはいくつかありますが、ここでは CENTUM VP として推奨する方法を、例を上げて説明します。

■ 時刻同期に関する注意事項

CENTUM VP ソフトウェアをインストールしたコンピュータは、Windows ドメインに参加しても、ドメインコントローラを時刻マスタとした時刻同期を行わないように自動的に設定されます。

B2.8.1 セキュリティを考慮した時刻同期をする

ファイアウォールまたは L3 スイッチを使用し、セキュリティを高めた上で設定する時刻同期方法について説明します。

■ 設定の概要

- SNTP サーバを導入し、ドメインコントローラと Vnet/IP システムは同一の SNTP サーバの時刻を参照するようにしてください。
- セキュリティ対策のため、ドメインコントローラと Vnet/IP システムから参照される SNTP サーバは、ファイアウォール (FW) または L3 スイッチ (L3SW) 経由で接続してください。
- Vnet/IP に接続したコンピュータは、ドメインコントローラの時刻を時刻マスタとした Windows サービスの W32Time を使用する時刻同期を行わないようにしてください。
- 機器を接続したあと、ドメインプロパティを設定してください。

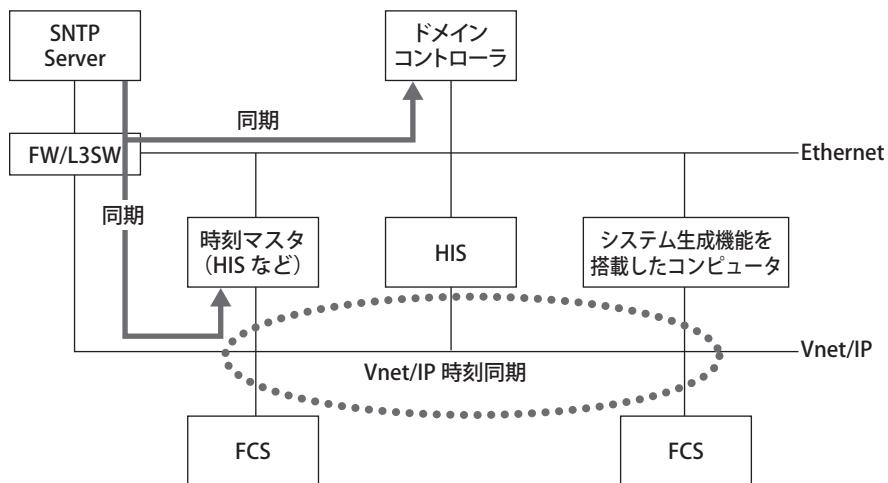


図 B2.8.1-1 セキュリティを考慮した時刻同期方法 (Vnet/IP)

● ドメインプロパティの設定方法

- システム生成機能を搭載したコンピュータで、システムビューを起動してください。
- 時刻同期を設定する Windows ドメイン内にある任意のステーションのフォルダを選択し、コンテキストメニューで [ファイル] – [ドメインプロパティ] を選択してください。
選択したステーションが属する Vnet/IP ドメインのプロパティダイアログが表示されます。
- 時刻グループの設定をしてください。

補足

0 を指定した場合、Vnet/IP ドメイン間の時刻同期は行われません。

- SNTP サーバ IP アドレスの設定をしてください。

補足

[バス 1 接続] テキストボックスには、バス 1 に接続する SNTP サーバの IP アドレスを指定します。空欄の場合、192.168.<ドメイン番号>.254 を指定したことになります。

[バス 2 接続] テキストボックスには、バス 2 に接続する SNTP サーバの IP アドレスを指定します。空欄の場合、192.168.<128 + ドメイン番号>.254 を指定したことになります。

5. [OK] をクリックしてください。

● Vnet/IP と V ネットを併用する場合

Vnet/IP と V ネットを併用する場合は、Vnet/IP ドメイン内で時刻同期設定をしたあと、次の設定も合わせて行ってください。

- V ネットルータのプロパティで Vnet/IP ドメインを時刻上位になるよう設定してください。
- V ネットドメインが複数存在する場合、バス変換器など中継器のプロパティ設定で、V ネットルータが接続された V ネットドメインが時刻上位となるようにしてください。

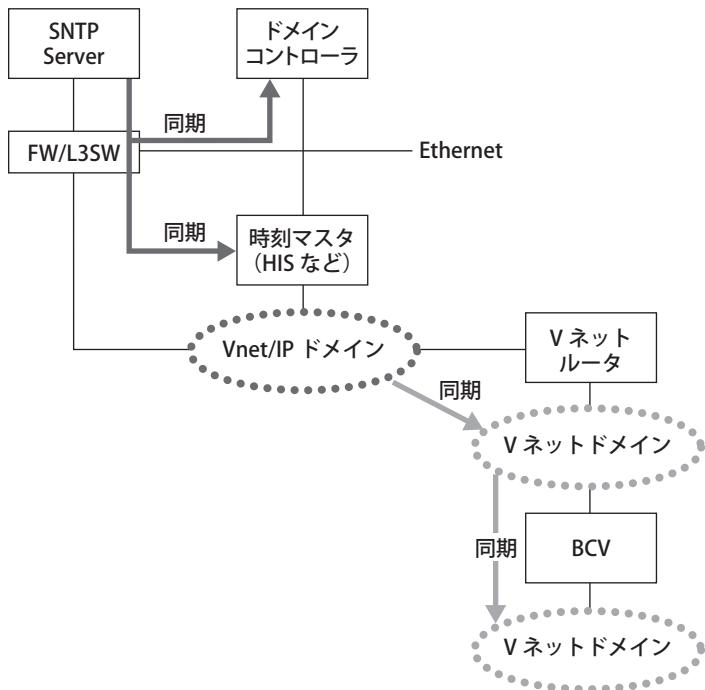


図 B2.8.1-2 セキュリティを考慮した時刻同期方法（Vnet/IP と V ネット併用）

参照

Vnet/IP ドメインの時刻同期設定方法については、以下を参照してください。

「● ドメインプロパティの設定方法」ページ B2-29

B2.8.2 導入コストを抑えた時刻同期をする

ファイアウォールや L3 スイッチを使用せず、導入コストを抑えた形で時刻を同期させる方法について説明します。

この場合の時刻同期方法には、次の種類があります。

- V ネット – UTC(協定世界時)に同期させない
- Vnet/IP – UTC(協定世界時)に同期させる
- Vnet/IP – UTC(協定世界時)に同期させない

■ V ネットの場合 – UTC(協定世界時)に同期させない

V ネットドメインに接続している任意の 1 台のステーションを SNTP サーバにしてください。V ネットドメイン内のコンピュータは、V ネット時刻同期機能で時刻同期されます。ドメインコントローラを SNTP サーバに時刻同期させると、全体が時刻同期されます。

補足

任意のステーションを SNTP サーバとした場合、システムの時刻は UTC (協定世界時) に合わせられているのではなく、SNTP サーバのハードウェアが持つ時刻を時刻マスタとしています。

- V ネットに接続したコンピュータでは、Windows サービスの W32Time を使用する時刻同期をさせないでください。W32Time を使用すると、ドメインコントローラの時刻に同期され、SNTP サーバと時刻同期ができません。
- ドメインコントローラでは、Windows サービスの W32Time を使用して、SNTP サーバと時刻同期させてください。
- V ネットが複数ドメインの場合、バス変換器など中継器のプロパティ設定で、ドメインコントローラが参照する HIS の V ネットドメインが時刻上位となるようにしてください。

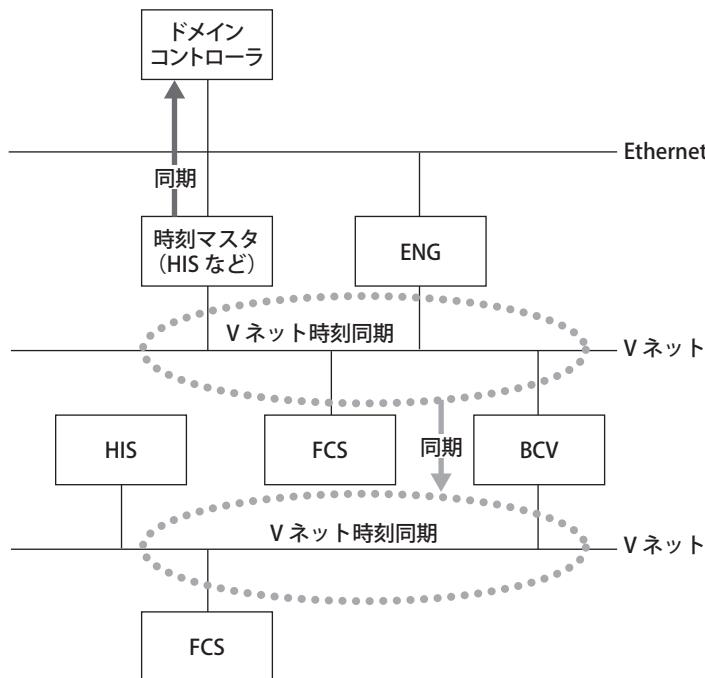


図 B2.8.2-1 導入コストを抑えた時刻同期方法（V ネット – UTC(協定世界時)に同期させない）

● 任意のステーションを SNTP サーバとする設定方法

1. SNTP サーバとするステーションに管理者ユーザでログオンしてください。
2. 次のコマンドを右クリックし [管理者として実行] を選択してください。

<CENTUM VP ソフトウェアメディアドライブ>:\CENTUM\TOOLS\BeNtpServer.cmd

補足

ITセキュリティ設定でソフトウェア制限ポリシーを適用している場合は、コマンドプロンプトを右クリックし[管理者として実行]を選択してください。その後、起動されたコマンドプロンプトからプログラムを実行してください。

- 表示されたウィンドウで、Enable NTP Server? (y/n/quit)のあとに、「y」を入力してください。

■ Vnet/IP の場合—UTC(協定世界時)に同期させる

- SNTP サーバを導入し、UTC と同期させてください。ドメインコントローラと Vnet/IP システムは、同一の SNTP サーバの時刻を参照させてください。
- Vnet/IP に接続したコンピュータでは、Windows サービスの W32Time を使用する時刻同期をさせないでください。W32Time を使用すると、ドメインコントローラの時刻に同期され、SNTP サーバと時刻同期ができません。

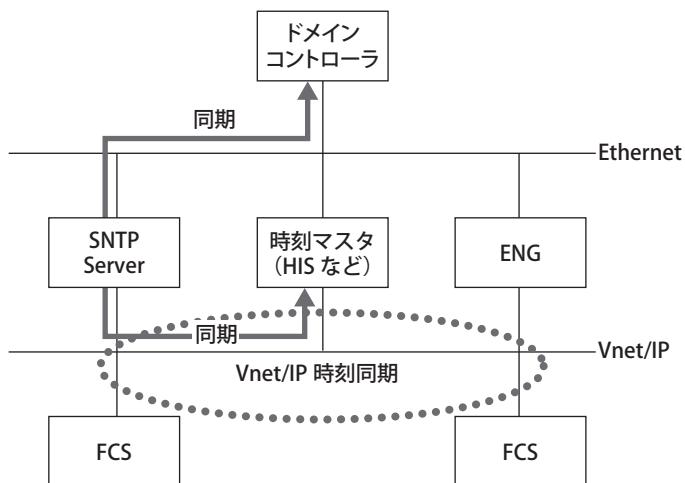


図 B2.8.2-2 導入コストを抑えた時刻同期方法（Vnet/IP—UTC(協定世界時)に同期させる）

参照

Vnet/IP ドメインの時刻同期設定方法については、以下を参照してください。

「● ドメインプロパティの設定方法」ページ B2-29

■ Vnet/IP の場合—UTC(協定世界時)に同期させない

Vnet/IP ドメインに接続している任意の 1 台のステーションを SNTP サーバにしてください。Vnet/IP ドメイン内のコンピュータは、Vnet/IP 時刻同期機能で時刻同期されます。ドメインコントローラを SNTP サーバに時刻同期させると、全体が時刻同期されます。

補足

任意のステーションを SNTP サーバとした場合、システムの時刻は UTC (協定世界時) に同期するのではなく、SNTP サーバのハードウェアが持つ時刻に同期されます。

- Vnet/IP に接続したコンピュータでは、Windows サービスの W32Time を使用する時刻同期をさせないでください。W32Time を使用すると、ドメインコントローラの時刻に同期され、SNTP サーバと時刻同期ができません。
- ドメインコントローラでは、Windows サービスの W32Time を使用して、SNTP サーバと時刻同期させてください。

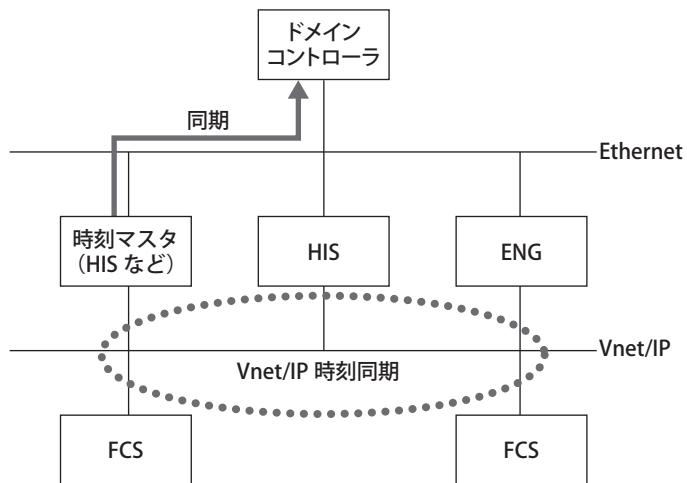


図 B2.8.2-3 導入コストを抑えた時刻同期方法（Vnet/IP—UTC(協定世界時)に同期させない）

● 任意のステーションを SNTP サーバとする設定方法

1. SNTP サーバとするステーションに管理者ユーザでログオンしてください。
2. 次のコマンドを右クリックし [管理者として実行] を選択してください。
 <CENTUM VP ソフトウェアメディアドライブ>:\CENTUM\TOOLS\BeNtpServer.cmd
 Enable NTP Server? (y/n/quit)のコマンドプロンプトが表示されます。

補足

ITセキュリティ設定でソフトウェア制限ポリシーを適用している場合は、コマンドプロンプトを右クリックし [管理者として実行] を選択してください。その後、起動されたコマンドプロンプトからプログラムを実行してください。

3. 「y」を入力し、[Enter] キーを押してください。

Blank Page

B3. FCS/バス変換器/N ネットルータ/CGW/WAC ルータのハードウェアの設定をする

ここでは、FCS/バス変換器/N ネットルータ/コミュニケーションゲートウェイユニット (CGW) /ワイドエリアコミュニケーションルータ (WAC ルータ) のハードウェア設定について説明します。ここで説明するハードウェアの設定は、ステーションセットアップのあとでも可能です。



ディップスイッチの設定などでカードの着脱を行う場合、静電気対策をしてください。

注意

参照

静電気対策については、以下を参照してください。

周辺機器 (IM 33J50B10-01JA) の「A6.1 静電気に対する注意事項」

B3.1 FCS の設定をする

ここでは、FCS に必要なハードウェアの設定について説明します。

■ プロセッサユニットをセットアップする

プロセッサユニットとは、制御ステーションにある、制御演算を行うユニットです。

プロセッサユニットには次の種類があります。

- CP471
- CP461
- CP401
- CP345
- CP703
- CP701

いずれのカードにも、ドメイン番号とステーション番号を設定するディップスイッチがあり、ステーションアドレスは、ドメイン番号とステーション番号の組み合わせで決まります。

ここでは、このディップスイッチの設定について説明します。

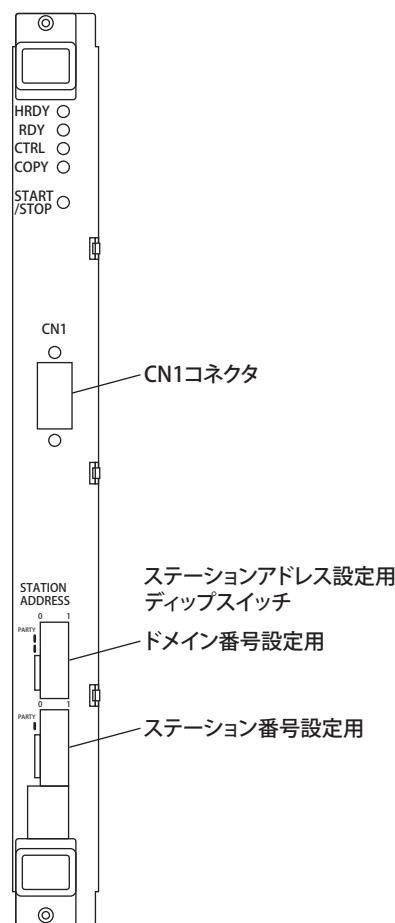


図 B3.1-1 ディップスイッチの位置 (CP345/CP703/CP701)

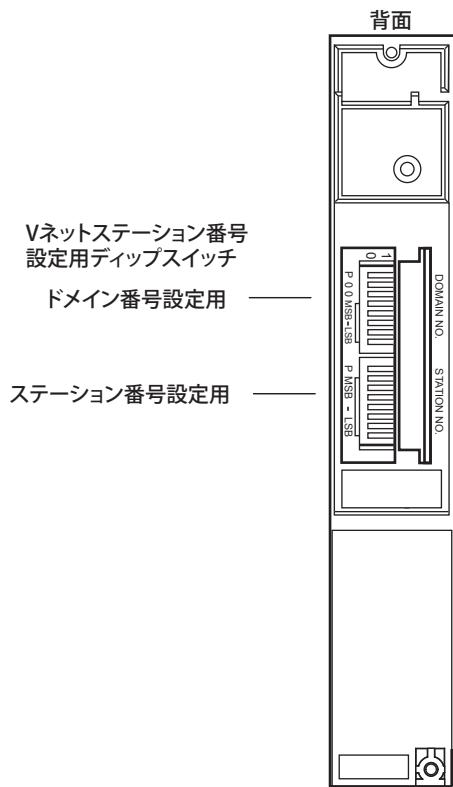
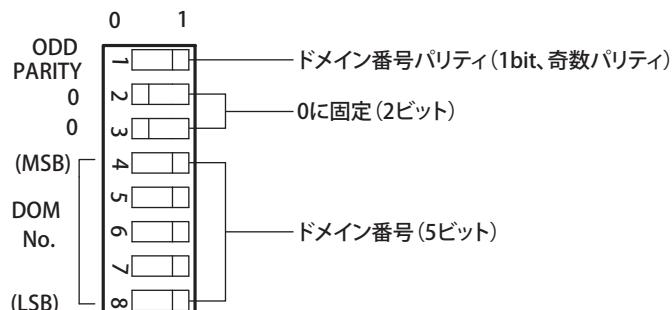


図 B3.1-2 ディップスイッチの位置 (CP471/CP461/CP401)

● ドメイン番号を設定する

ドメインとは、1系統の制御バスで結ばれるステーションの範囲のことです。ドメイン番号は1～16の範囲で設定してください。1系統のシステムでは1に設定します。



MSB : Most Significant Bit (最上桁のビット)
LSB : Least Significant Bit (最下桁のビット)

図 B3.1-3 ドメイン番号設定ディップスイッチ (CP401 の例)

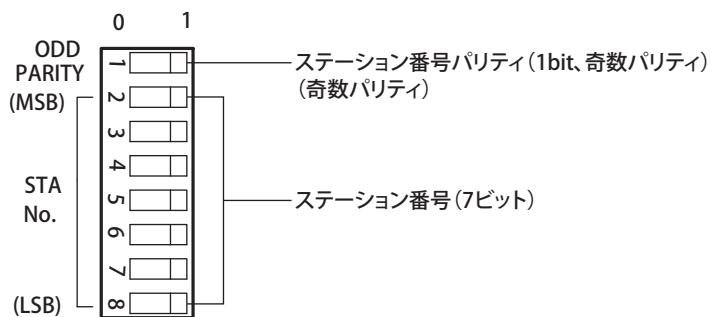
参照

ドメイン番号とそれに対応するディップスイッチの位置については、以下を参照してください。

「■ ドメイン番号と設定スイッチの位置」ページ App.1-1

● ステーション番号を設定する

ステーション番号は1～64の範囲で設定してください。



MSB : Most Significant Bit (最上桁のビット)

LSB : Least Significant Bit (最下桁のビット)

図 B3.1-4 ステーション番号設定ディップスイッチ

参照

ステーション番号とそれに対応するディップスイッチの位置については、以下を参照してください。

「■ ステーション番号と設定スイッチの位置」ページ App.1-1

B3.2 バス変換器の設定をする

ここでは、バス変換器（ABC11S、ABC11D）に必要なハードウェアの設定について説明します。

バス変換器で設定が必要なハードウェアは次のものです。

- ・ プロセッサカード
- ・ HF バス/RL バスインターフェースカード
- ・ V ネットインターフェースカード

■ プロセッサカードをセットアップする

プロセッサカードには、ドメイン番号とステーション番号を設定するディップスイッチがあり、ステーションアドレスはドメイン番号とステーション番号の組み合わせで決まります。

ここでは、このディップスイッチの設定について説明します。

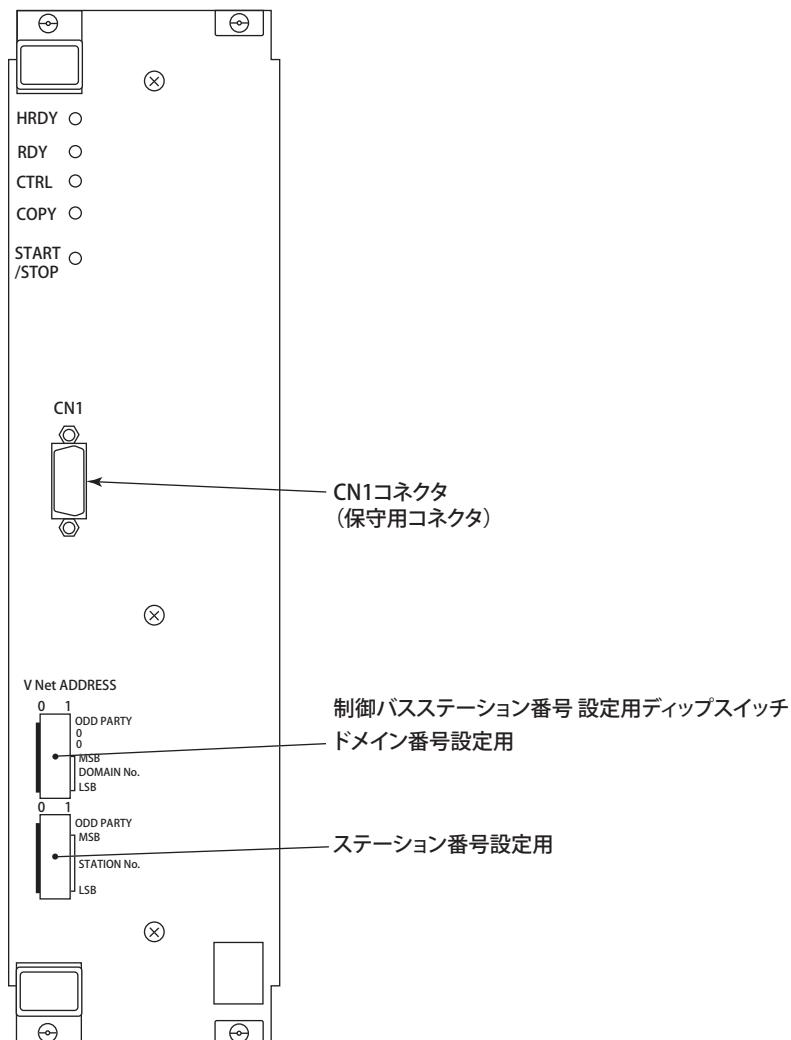
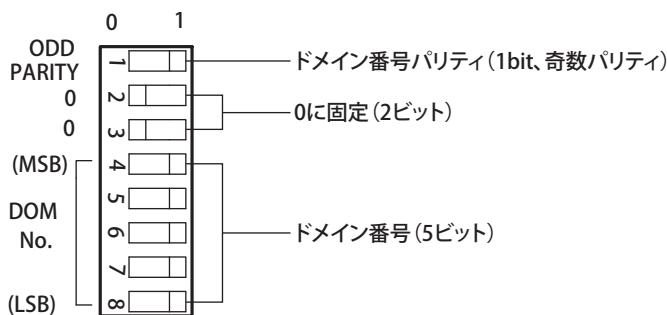


図 B3.2-1 ディップスイッチの位置

● ドメイン番号を設定する

ドメインとは、1 系統の制御バスで結ばれるステーションの範囲のことです。ドメイン番号は 1 ~ 16 の範囲で設定してください。1 系統のシステムでは 1 に設定します。



MSB : Most Significant Bit (最上桁のビット)
LSB : Least Significant Bit (最下桁のビット)

図 B3.2-2 ドメイン番号設定ディップスイッチ

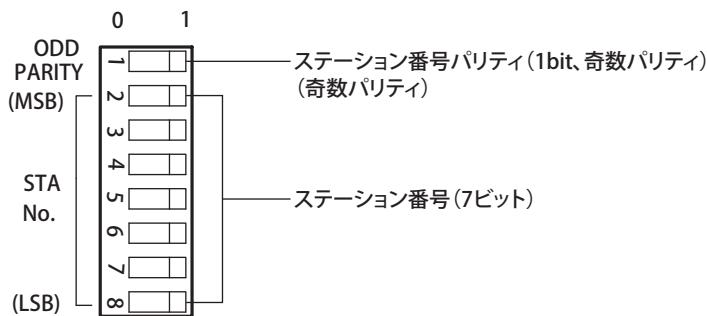
参照

ドメイン番号とそれに対応するディップスイッチの位置については、以下を参照してください。

「■ ドメイン番号と設定スイッチの位置」ページ App.1-1

● ステーション番号を設定する

ステーション番号は 1 ~ 64 の範囲で設定してください。



MSB : Most Significant Bit (最上桁のビット)
LSB : Least Significant Bit (最下桁のビット)

図 B3.2-3 ステーション番号設定ディップスイッチ

参照

ステーション番号とそれに対応するディップスイッチの位置については、以下を参照してください。

「■ ステーション番号と設定スイッチの位置」ページ App.1-1

■ HF バス/RL バスインターフェースカードをセットアップする

HF バス/RL バスインターフェースカードにはディップスイッチがあり、下位側のシステムでのステーション番号、またはユニット番号を設定します。

ここでは、このディップスイッチの設定について説明します。

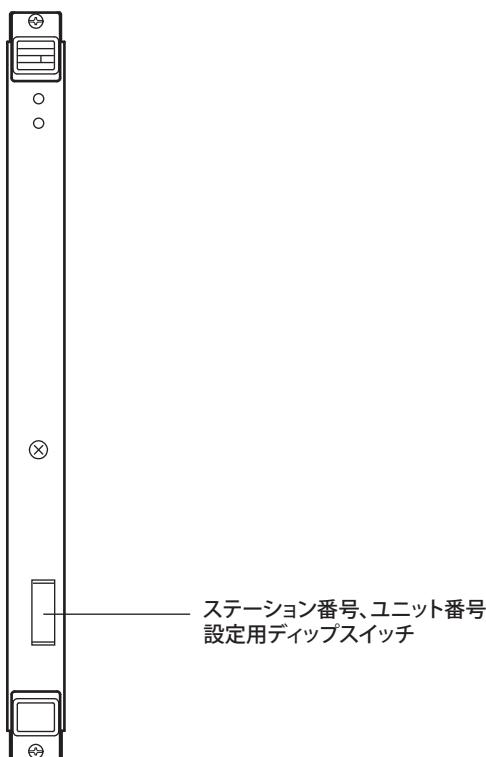
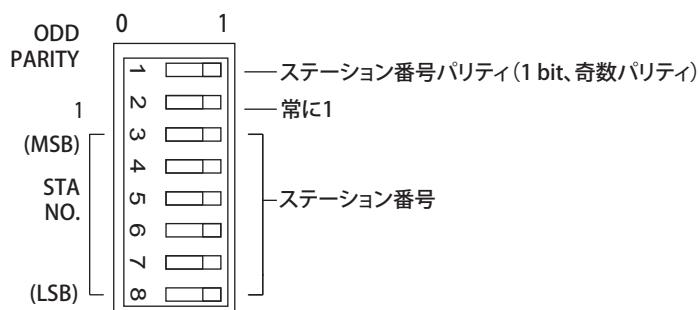


図 B3.2-4 ディップスイッチの位置

● ステーション番号を設定する

HFバスのステーション番号は1～32の範囲で設定してください。
ディップスイッチとステーション番号の対応は、次の表のとおりです。



MSB : Most Significant Bit (最上桁のビット)
LSB : Least Significant Bit (最下桁のビット)

図 B3.2-5 ステーション番号設定ディップスイッチ

- ・ ディップスイッチの設定
 - 0：上図の状態で、ディップスイッチを左側に倒すことを意味します。
 - 1：上図の状態で、ディップスイッチを右側に倒すことを意味します。

表 B3.2-1 ステーション番号と設定スイッチの位置

ステーション番号	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ビット番号1	1	1	0	1	0	0	1	1	0	0	1	0	1	1	0	1
ビット番号2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
ビット番号3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ビット番号4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
ビット番号5	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0

次に続く

表 B3.2-1 ステーション番号と設定スイッチの位置（前から続く）

ステーション番号	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
ビット番号 6	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0
ビット番号 7	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
ビット番号 8	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0

ステーション番号	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
ビット番号 1	0	0	1	0	1	1	0	0	1	1	0	1	0	0	1	1
ビット番号 2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
ビット番号 3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
ビット番号 4	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0
ビット番号 5	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0
ビット番号 6	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0
ビット番号 7	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0
ビット番号 8	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0

● ユニット番号を設定する

RL バスのユニット番号は 1 ~ 21 の範囲で設定してください。ディップスイッチとユニット番号の対応は、HF バスインターフェースカードのステーション番号の設定と同様です。

■ V ネットインターフェースカードをセットアップする

V ネットインターフェースカードは、次のシステム間を接続して通信させるためのインターフェースカードです。

- ・ CENTUM VP の V ネットと CENTUM VP の V ネット
- ・ CENTUM VP の V ネットと CS 3000 の V ネット
- ・ CENTUM VP の V ネットと CENTUM CS の V ネット
- ・ CENTUM VP の V ネットと CS 1000 の VL ネット

V ネットインターフェースカードにはディップスイッチがあり、ドメイン番号とステーション番号を設定します。

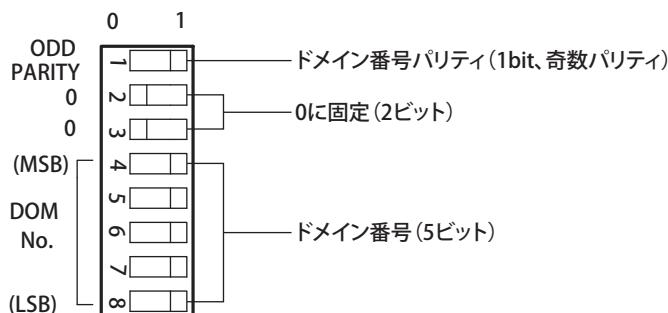
ここでは、このディップスイッチの設定について説明します。



図 B3.2-6 ディップスイッチの位置

● ドメイン番号を設定する

1～16 の範囲で下位側のドメイン番号を設定してください。
1 系統のシステムでは 1 に設定します。



MSB : Most Significant Bit (最上桁のビット)
LSB : Least Significant Bit (最下桁のビット)

図 B3.2-7 ドメイン番号設定ディップスイッチ

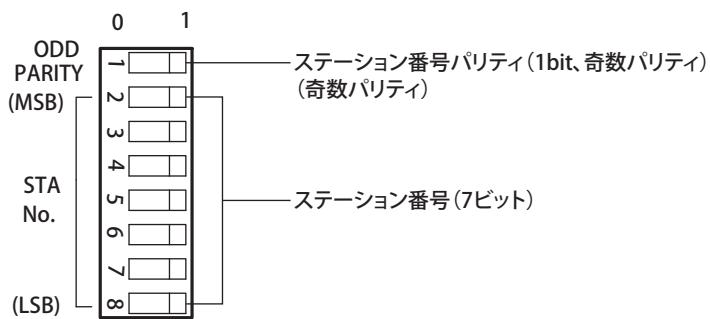
参照

ドメイン番号とそれに対応するディップスイッチの位置については、以下を参照してください。

「■ ドメイン番号と設定スイッチの位置」ページ App.1-1

● ステーション番号を設定する

1～64 の範囲で下位側のステーション番号を設定してください。
下位側が CS 1000 の場合は、1～24 の範囲でステーション番号を設定してください。



MSB : Most Significant Bit (最上桁のビット)

LSB : Least Significant Bit (最下桁のビット)

図 B3.2-8 ステーション番号設定ディップスイッチ

参照

ステーション番号とそれに対応するディップスイッチの位置については、以下を参照してください。

「■ ステーション番号と設定スイッチの位置」ページ App.1-1

B3.3 V ネットルータの設定をする

ここでは、V ネットルータ (AVR10D) に必要なハードウェアの設定について説明します。

■ V ネットルータの通信モジュールのセットアップをする

V ネットルータの通信モジュールには、ドメイン番号とステーション番号を設定するディップスイッチがあり、ステーションアドレスは、ドメイン番号とステーション番号の組み合わせで決まります。

ここでは、このディップスイッチの設定について説明します。

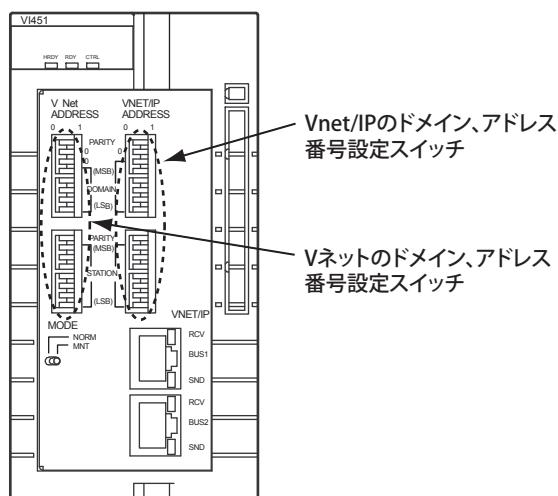
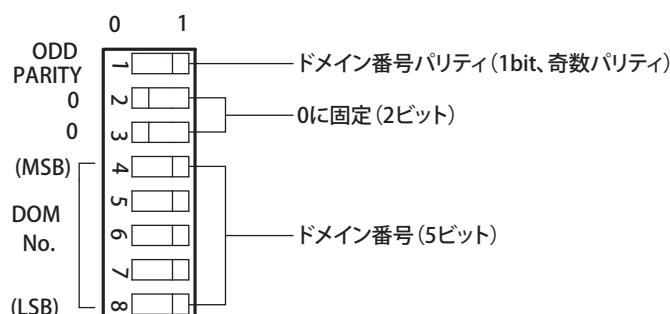


図 B3.3-1 ディップスイッチの位置

● ドメイン番号を設定する

ドメインとは、1 系統の制御バスで結ばれるステーションの範囲のことです。ドメイン番号は 1 ~ 16 の範囲で設定してください。1 系統のシステムでは 1 に設定します。



MSB : Most Significant Bit (最上桁のビット)
LSB : Least Significant Bit (最下桁のビット)

図 B3.3-2 ドメイン番号設定ディップスイッチ

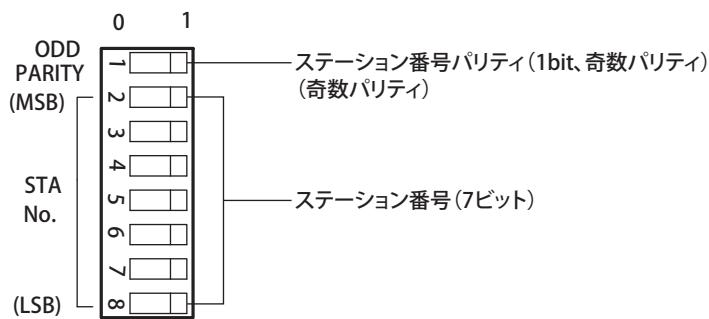
参照

ドメイン番号とそれに対応するディップスイッチの位置については、以下を参照してください。

「■ ドメイン番号と設定スイッチの位置」ページ App.1-1

● ステーション番号を設定する

ステーション番号は 1 ~ 64 の範囲で設定してください。



MSB : Most Significant Bit (最上桁のビット)
LSB : Least Significant Bit (最下桁のビット)

図 B3.3-3 ステーション番号設定ディップスイッチ

参照

ステーション番号とそれに対応するディップスイッチの位置については、以下を参照してください。

「■ ステーション番号と設定スイッチの位置」ページ App.1-1

B3.4 コミュニケーションゲートウェイユニットの設定をする

ここでは、コミュニケーションゲートウェイユニットに必要なハードウェアの設定について説明します。

■ コミュニケーションゲートウェイユニットのセットアップをする

コミュニケーションゲートウェイユニットには、ドメイン番号とステーション番号を設定するディップスイッチがあり、ステーションアドレスは、ドメイン番号とステーション番号の組み合わせで決まります。

ここでは、このディップスイッチの設定について説明します。

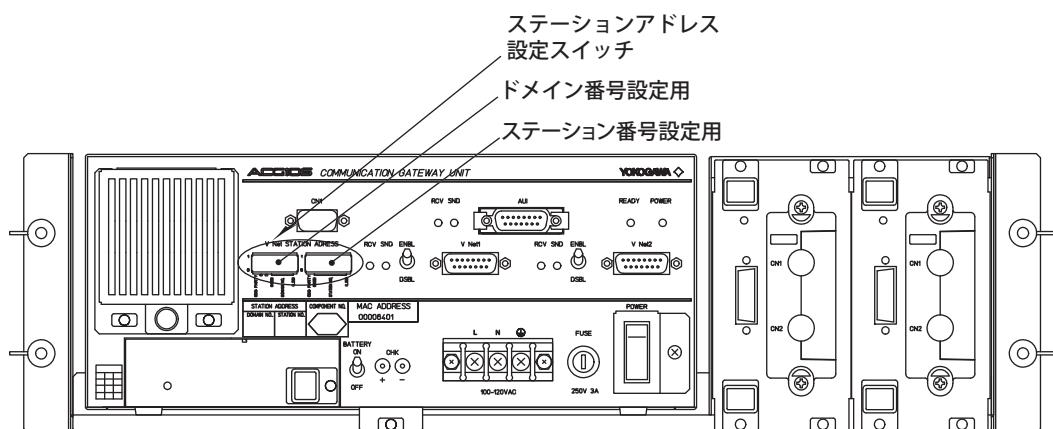
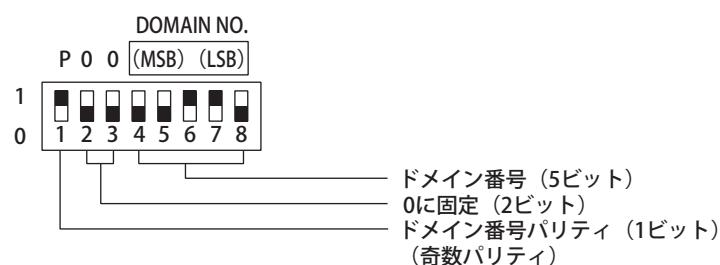


図 B3.4-1 ディップスイッチの位置

● ドメイン番号を設定する

ドメインとは、1系統の制御バスで結ばれるステーションの範囲のことです。ドメイン番号は1～16の範囲で設定してください。1系統のシステムでは1に設定します。



P (奇数パリティ) : ディップスイッチ8個の1側の数の和が奇数になるように設定
 MSB : Most Significant Bit (最上桁のビット)
 LSB : Least Significant Bit (最下桁のビット)

図 B3.4-2 ドメイン番号設定ディップスイッチ

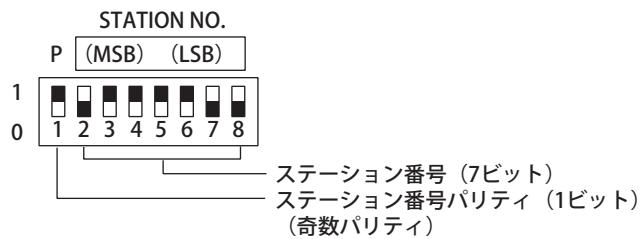
参照

ドメイン番号とそれに対応するディップスイッチの位置については、以下を参照してください。

「■ ドメイン番号と設定スイッチの位置」ページ App.1-1

● ステーション番号を設定する

ステーション番号は1～64の範囲で設定してください。



P (奇数パリティ) : ディップスイッチ8個の1側の数の和が奇数になるように設定
MSB : Most Significant Bit (最上桁のビット)
LSB : Least Significant Bit (最下桁のビット)

図 B3.4-3 ステーション番号設定ディップスイッチ

参照

ステーション番号とそれに対応するディップスイッチの位置については、以下を参照してください。

「■ ステーション番号と設定スイッチの位置」ページ App.1-1

B3.5 ワイドエリアコミュニケーションルータの設定をする

ここでは、ワイドエリアコミュニケーションルータ（AW810D）に必要なハードウェアの設定について説明します。

■ ワイドエリアコミュニケーションルータの通信モジュールのセットアップをする

ワイドエリアコミュニケーションルータの通信モジュールには、ドメイン番号とステーション番号を設定するディップスイッチがあり、ステーションアドレスは、ドメイン番号とステーション番号の組み合わせで決まります。

ここでは、このディップスイッチの設定について説明します。

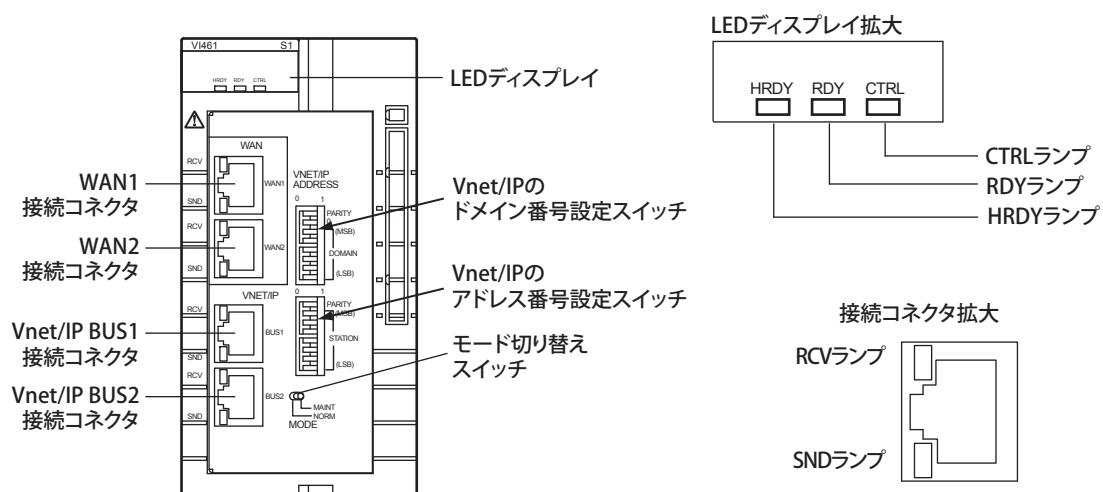
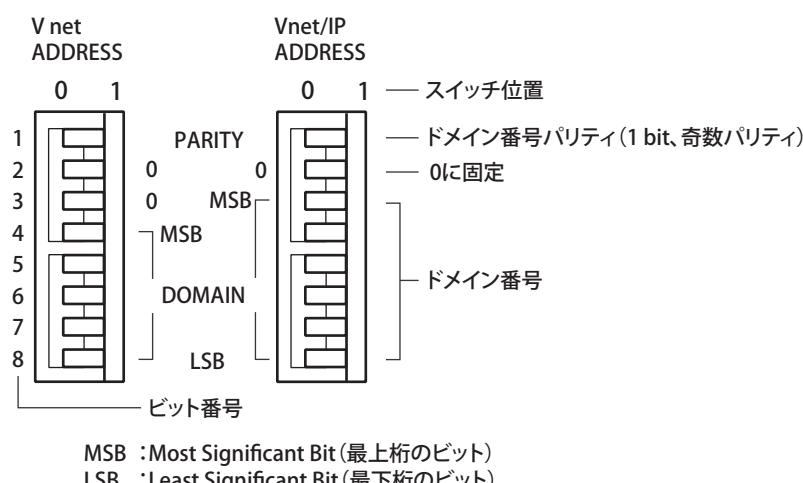


図 B3.5-1 ディップスイッチの位置

● ドメイン番号を設定する

ドメインとは、1系統の制御バスで結ばれるステーションの範囲のことです。ドメイン番号は1～16の範囲で設定してください。1系統のシステムでは1に設定します。



MSB :Most Significant Bit (最上桁のビット)
LSB :Least Significant Bit (最下桁のビット)

図 B3.5-2 ドメイン番号設定ディップスイッチ

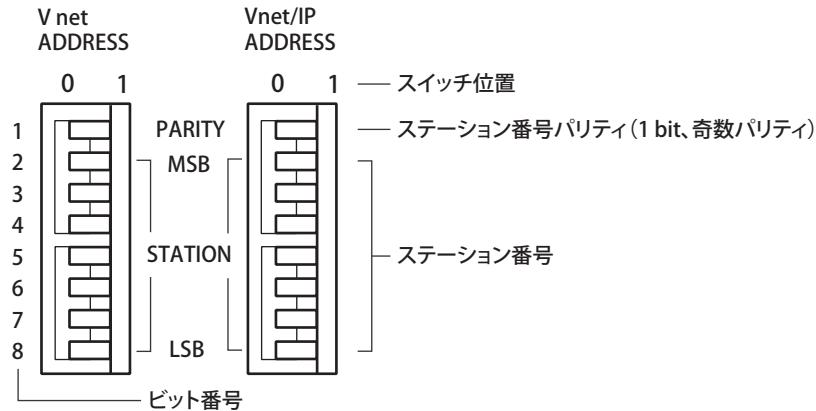
参照

ドメイン番号とそれに対応するディップスイッチの位置については、以下を参照してください。

「■ ドメイン番号と設定スイッチの位置」ページ App.1-1

● ステーション番号を設定する

ステーション番号は 1 ~ 64 の範囲で設定してください。



MSB :Most Significant Bit (最上桁のビット)

LSB :Least Significant Bit (最下桁のビット)

図 B3.5-3 ステーション番号設定ディップスイッチ

参照

ステーション番号とそれに対応するディップスイッチの位置については、以下を参照してください。

「■ ステーション番号と設定スイッチの位置」ページ App.1-1

B3.6 N-IO のノードインターフェースユニットの設定

N-IO のノードインターフェースユニットでは、ノードインターフェースユニットのメンテナンスポートとコンピュータを接続して、コンピュータ上のソフトウェアでノード番号の設定をします。ここでは、ノード番号を設定するためのツールとメンテナنسポートの有効/無効を切り替えるツールの説明をします。

B3.6.1 ノード番号設定ツールを使ってノード番号を設定する

N-IO ノードは、ノード番号設定ツールを使ってノード番号を設定します。ここでは、ノード番号設定ツールについて説明します。

■ ノード番号設定作業の概要

N-IO ノードのノードインターフェースユニットに実装されている N-ESB バスモジュールは、工場出荷時には、ノード番号が設定されていません。FCU と接続する前に、N-ESB バスモジュールにノード番号を設定する必要があります。

N-ESB バスモジュールのメンテナンスポートにコンピュータを接続して、コンピュータ上のソフトウェアを使ってノード番号を設定します。

ノード番号の設定に必要なソフトウェアは、CENTUM VP のインストールメディアに格納されています。

■ 準備する物

ノード番号設定作業をするために次のものが必要です。

● CENTUM VP のソフトウェアメディア

ノード番号の設定に必要な USB ドライバとノード番号設定ツールが含まれています。ノード番号設定作業をするコンピュータにこれらのソフトウェアをインストールします。

● コンピュータ

次の仕様を満たすコンピュータが必要です。

- ハードウェア
Windows 10、Windows 8.1、または Windows 7 のハードウェア要件に準拠します。
- ソフトウェア
Windows 10 Pro (64bit)
Windows 8.1 Professional (64bit、32bit)
Windows 7 Professional SP1 (64bit、32bit)

● USB ケーブル

N-ESB バスモジュール側のコネクタは MicroUSB Micro-B です。

■ ノード番号設定作業をするコンピュータ の準備

ノード番号設定作業に使用するコンピュータに必要なソフトウェアをインストールします。

● USB ドライバのインストール

1. CENTUM VP インストールメディアをコンピュータのドライブに挿入してください。
2. エクスプローラで、CENTUM VP インストールメディアの次のフォルダを表示してください。
<CENTUM VP ソフトウェアメディアドライブ>:CENTUM\NIO_TOOLS
3. フォルダの Setup.exe をダブルクリックして起動してください。
ユーザーアカウント制御のダイアログが表示されます。
4. [はい] をクリックしてください。
Setup 内容を確認するダイアログが表示されます。
5. [INSTALL] を選択して、[OK] をクリックしてください。
インストール開始を確認するダイアログが表示されます。

6. [OK] をクリックしてください。
7. Windows セキュリティダイアログが、表示された場合は、[インストール] をクリックしてください。
8. インストール終了を知らせるダイアログが表示されたら、[OK] をクリックしてください。

補足

- ・コンピュータの再起動を促すダイアログが表示されたら、[OK] をクリックし、コンピュータを再起動してください。
- ・USB ドライバのインストールは、コンピュータと N-ESB バスモジュールを接続したあとで、実施してもかまいません。

● ノード番号設定ツールのコピー

1. CENTUM VP のインストールメディアをコンピュータのドライブに挿入します。
2. エクスプローラで、CENTUM VP のソフトウェアメディア内の次のフォルダを表示してください。
<CENTUM VP ソフトウェアメディアドライブ>:CENTUM\NIO_TOOLS
3. フォルダ内の NodeNumSetting.exe をコンピュータ上の任意のフォルダにコピーしてください。

■ ノード番号の設定手順

ノード番号の設定手順を次に示します。

● 作業前の確認

設定作業をする前に N-ESB バスモジュールの STAT ランプが点灯していることを確認してください。

2台の N-ESB バスモジュールからすべての N-ESB バスケーブルを外して、バス通信が不可能な状態にしてください。

● N-ESB バスモジュールの取り外し

N-ESB バスモジュールにすでにノード番号が、設定されている場合は、2台ある N-ESB バスモジュールのうちの1台をノードインターフェースユニットから外してください。2台のうちのどちらを外してもかまいません。

ノード番号が、まだ設定されていない場合（ADRS ランプが点灯していない場合）は、N-ESB バスモジュールを外す必要はありません。

● コンピュータと N-ESB バスモジュールの接続

ノード番号設定作業に使うコンピュータの USB ポートと、ノードインターフェースユニット上の通電されている N-ESB バスモジュールのメンテナンスポートを、用意した USB ケーブルで接続します。

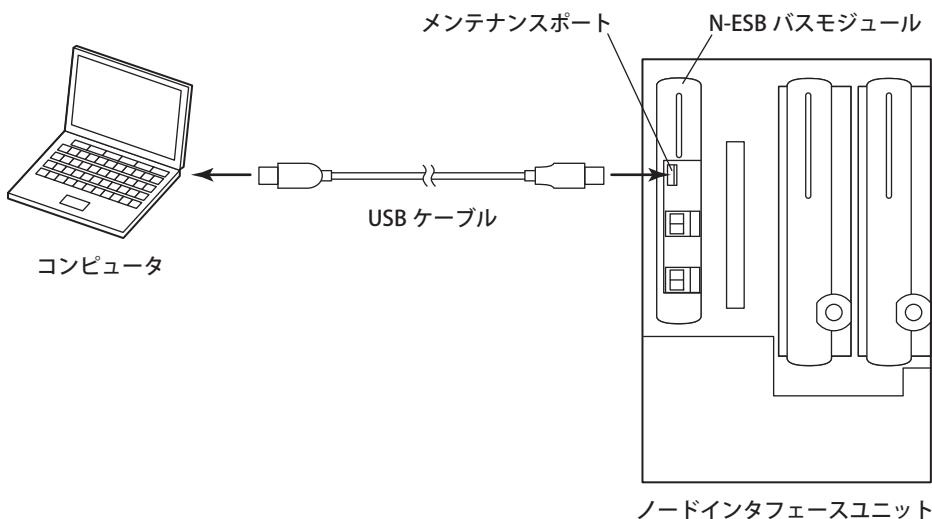


図 B3.6.1-1 コンピュータと N-ESB バスモジュールの接続

● ツールの操作

1. コンピュータ上で、NodeNumSetting.exe コマンドをダブルクリックして起動してください。
ノード番号設定ツールの画面が表示されます。

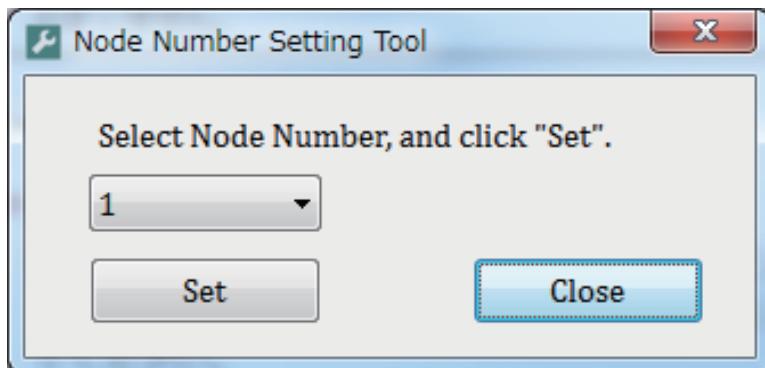


図 B3.6.1-2 ノード番号設定ツール

2. ノード番号を選択し、[Set] をクリックしてください。
現在、設定されているノード番号とこれから設定しようとしているノード番号を表示した確認ダイアログが表示されます。
3. [はい] をクリックしてください。
N-ESB バスモジュールにノード番号が設定されます。設定が完了したことを示すダイアログが表示されます。
4. N-ESB バスモジュールの ADRS ランプでノード番号を確認してください。

参照

ADRS ランプの位置とノード番号の読み取り方については、以下を参照してください。

入出力機器 Vol.2 (IM 33J62F10-01JA) の「2.4 N-ESB バスモジュール」の「■ N-ESB バスモジュールの構成と名称」

● もう片方の N-ESB バスモジュールのノード番号設定

最初に片方の N-ESB バスモジュールを外した場合は、外しておいた N-ESB バスモジュールに対して以下の操作をします。片方の N-ESB バスモジュールを外していない場合は、次の作業に進んでください。

1. 外しておいた N-ESB バスモジュールをノードインターフェースユニットに実装します。

実装していた N-ESB バスモジュールからノード番号がコピーされます。

2. N-ESB バスモジュールの ADRS ランプでノード番号を確認してください。

● ノード番号設定後の作業

1. ノード番号設定ツールを終了してください。
2. USB ケーブルを機器から外してください。
3. 2 台の N-ESB バスモジュールに全ての N-ESB バスケーブルを接続して、FCU との通信が可能な状態にしてください。

補足

N-ESB バスモジュールのメンテナンスポートは、出荷時には、有効に設定されています。運転に入る前に HIS から N-IO ノードセキュリティツールを使って無効にしてください。

参照

N-IO ノードセキュリティツールについては、以下を参照してください。

「B3.6.2 メンテナンスポートの有効/無効の切り替え」ページ B3-22

B3.6.2 メンテナンスポートの有効/無効の切り替え

N-ESB バスモジュールのメンテナンスポートは、工場出荷時には有効になっています。システムの運転中は、セキュリティの観点から無効にしてください。また、FieldMate Validator を使用するときは、メンテナンスポートを有効にし、使用後に無効にしてください。ここでは、メンテナンスポートの有効/無効を切り替えるツールについて説明します。

■ 機能の概要

メンテナンスポートの有効/無効の切り替えは、システム生成機能を搭載したコンピュータで動作する N-IO ノードセキュリティツールで行います。N-IO ノードセキュリティツールは以下の機能を持ちます。

- ・ メンテナンスポートの有効/無効の情報を取得できます。
- ・ 二重化された 2 枚の N-ESB バスモジュール一括で、メンテナンスポートの有効/無効を切り替えます。

■ ツールの操作方法

ここでは、ツールの操作方法を説明します。

● ツールの実行権限

ツールを実行できるユーザを次に示します。

表 B3.6.2-1 ツールを実行できるユーザ

セキュリティモデル	ツールを実行できるユーザ
標準モデル	次のグループに属するユーザ ・ CTM_ENGINEER、CTM_ENGINEER_LCL ・ CTM_ENGINEER_ADMIN、CTM_ENGINEER_ADMIN_LCL ・ CTM_MAINTENANCE、CTM_MAINTENANCE_LCL
従来モデル	CENTUM ユーザ

● ツールの起動

N-IO ノードセキュリティツールは、システム生成機能を搭載したコンピュータで起動します。起動方法を次に示します。

1. ツールの実行権限を持ったユーザでシステム生成機能を搭載したコンピュータにログオンしてください。
2. N-IO ノードセキュリティを起動してください。
コマンドプロンプトが開き、ドメイン番号とステーション番号の入力を要求されます。
3. ドメイン番号とステーション番号を入力します。
サブコマンドの入力待ち状態になります。

● サブコマンド

コマンドプロンプトでドメイン番号とステーション番号を指定した後は、次に示す形式でサブコマンドを実行します。

<サブコマンド>△[<ノード番号>]

次に示すサブコマンドがあります。

表 B3.6.2-2 サブコマンド

サブコマンド	説明
disable [Δ<ノード番号>]	メンテナンスポートを無効にします。ノード番号を省略した場合、ステーションに定義されている全 N-IO ノードに対してコマンドを実行します。この場合は、実行時に disable にするかどうかの確認メッセージが表示されます。
enable Δ<ノード番号>	メンテナンスポートを有効にします。ノード番号の指定は省略できません。
disp [Δ<ノード番号>]	メンテナンスポートの状態を表示します。ノード番号を省略した場合、ステーションに定義されている全 N-IO ノードに対してコマンドを実行します。
change	ドメイン番号とステーション番号を指定して、操作の対象とするステーションを変更します。
lo [Δ<ファイル名>]	コマンドの実行結果のファイル出力を開始します。すでに存在するファイルを指定した場合、ファイルの最後から実行結果を追加していきます。ファイル名を省略した場合、以下のファイルに実行結果が output されます。 <マイドキュメントフォルダ>\NioNodeSecurityLog\NioNodeSecurity_YYYYMMDD_hhmmss.log YYYYMMDD：西暦年月日 hhmmss：時分秒
lc	実行結果のファイル出力を終了します。
help	ヘルプを表示します。
quit または、q	コマンドを終了します。

● 実行結果の表示

disp、enable、disable サブコマンドを実行したときは、次の状態が表示されます。

表 B3.6.2-3 実行結果の表示

表示文字列	意味
DISABLED	メンテナンスポートが無効です。
ENABLED	メンテナンスポートが有効です。
MAINTENANCE	メンテナンスマードです。
FAIL	N-ESB バスモジュールが FAIL しています。

● エラーの表示

コマンドの実行でエラーが発生した場合のメッセージを次に示します。

表 B3.6.2-4 コマンド実行時のエラーメッセージ

メッセージ	意味
VHF Communication Error : v_sts 0x34 (エラーコード)	制御バスの通信エラー
Invalid Domain Number (指定されたドメイン番号)	ドメイン番号が正しくありません。
Invalid Station Number (指定されたステーション番号)	ステーション番号が正しくありません。
Invalid Node Address (指定されたノード番号)	ノード番号が正しくありません。
NIU Access Error : Node1 Left code = 0x3b1c (エラーコード)	NIU 通信エラー

■ コマンドの実行例

次に実行例を示します。

● コマンド起動の例

コマンド起動直後にドメイン番号 2、ステーション番号 8 のステーションを指定した例を次に示します。

C:\> NioNodeSecurityTool

Domain? 2

Station? 8
[02-08]001:

● N-IO ノードのノード番号を指定して無効を設定する例

2番のノードのメンテナンスポートを無効にします。

[02-08]002: disable 2

Node02 : DISABLED (Left : DISABLED Right : DISABLED)

● 全 N-IO ノードに無効を設定する例

メインコマンドの起動後、サブコマンドで定義されている全 N-IO ノードに対してメンテナンスポートを無効にします。

[02-08]003: disable

Disable All Nodes? y

Node01 : DISABLED (Left : DISABLED Right : DISABLED)

Node02 : DISABLED (Left : DISABLED Right : FAIL)

Node05 : DISABLED (Left : DISABLED Right : DISABLED)

Node06 : MAINTENANCE (Left : MAINTENANCE Right : MAINTENANCE)

● 全 N-IO ノードのメンテナンスポートの状態を表示する例

メインコマンドの起動後、サブコマンドで定義されている全 N-IO ノードのメンテナンスポートの状態を表示します。

[02-08]001: disp

Node01 : ENABLED (Left : ENABLED Right : ENABLED)

Node02 : ENABLED (Left : ENABLED Right : FAIL)

Node05 : ENABLED (Left : ENABLED Right : ENABLED)

Node06 : MAINTENANCE (Left : MAINTENANCE Right : MAINTENANCE)

● 対象とするステーションを変更する例

対象ステーションをドメイン番号 3、ステーション番号 9 のステーションに変更します。

[02-08]004: change

Domain? 3

Station? 9

[03-09]005:

■ 実行結果の確認

メンテナンスポートの有効/無効状態は、状態表示画面やシステムアラームメッセージで確認することもできます。

● 状態表示画面での確認

N-IO ノードの場合は、HIS の状態表示画面にメンテナンスポートの有効/無効の状態が表示されます。

参照

N-IO ノードの状態表示画面については、以下を参照してください。

操作監視リファレンス Vol.1 (IM 33J05A10-01JA) の「4.10 FFCS-C 状態表示ビュー」

● メッセージの発生

FCS 内のすべてのメンテナンスポートが無効である状態から、一つでも有効になった場合、メンテナンスポートが有効であることを示すメッセージが発生します。

FCS 内のすべてのメンテナンスポートが無効になった場合、メンテナンスポートが無効であることを示すメッセージが発生します。

参照

メッセージ内容の詳細については、以下を参照してください。

操作監視メッセージ (IM 33J05A30-01JA) の「2.5 制御ステーション状態変化関連メッセージ (メッセージ番号 0400...0496)」

Blank Page

B4. 主なステーションやコンピュータのセットアップをする

ここでは、これまでの新規セットアップ作業に続き、主なステーションやコンピュータとして必要なセットアップ作業の説明をします。

該当するステーションやコンピュータの種類は次のとおりです。

- HIS
- APCS
- SIOS
- GSGW
- UGS
- システム生成機能のみを搭載したコンピュータ
- AD サーバのみを搭載したコンピュータ
- UACS ステーション
- 仮想マシン

重要

CENTUM のシステムでは、ライセンス管理ステーションを 1 台決める必要があります。ライセンス管理ステーションは、HIS などのステーションと共に存させることができます。

各ステーションをセットアップする際には、ライセンス管理ステーションとするものを最初にセットアップしてください。その後、ライセンス適用ステーションにするものをセットアップし、ライセンス管理ステーションからライセンスを配布・反映すると、パッケージが使用可能となります。

ライセンス管理ステーションを、ライセンス管理専用のコンピュータとしてセットアップすることもできます。

補足

仮想化プラットフォームを用いて仮想化できる機能については、仮想化プラットフォームに関する GS および TI を参照してください。

参照

ライセンス管理専用のコンピュータのセットアップ方法については、以下を参照してください。

「B7. ライセンス管理専用のコンピュータのセットアップをする」ページ B7-1

■ 用意するもの

次のものを手元に用意してください。

- CENTUM VP R6 用ソフトウェアメディア
- CENTUM VP ライセンスマディア（ライセンス管理ステーションでのみ、ライセンス配布時に使用）

B4.1 ハードウェアの設定をする

ここでは、おもなステーションやコンピュータに必要なハードウェアの設定について説明します。

ただし、AD サーバ機能のみを搭載したコンピュータ、コンピュータ切替型 UGS、および仮想化ホストコンピュータでは、これらのハードウェアの設定は不要です。



デイップスイッチの設定などでカードを着脱する場合は、静電気対策をしてください。

注意

参照

静電気対策については、以下を参照してください。

周辺機器（IM 33J50B10-01JA）の「A6.1 静電気に対する注意事項」

■ 制御バスインターフェースカードをセットアップする

次の2種類の制御バスインターフェースカードがあります。機能は同じです。

- VF702 (PCI Express 用)
- VF701 (PCI バス用)

制御バスインターフェースカードには、ドメイン番号とステーション番号を設定するデイップスイッチがあります。ステーションアドレスは、ドメイン番号とステーション番号の組み合わせで決まります。

デイップスイッチは、ネットワーク設定の前に必ず設定してください。

ここでは、デイップスイッチの設定について説明します。デイップスイッチの位置は、VF702 と VF701 で同じです。

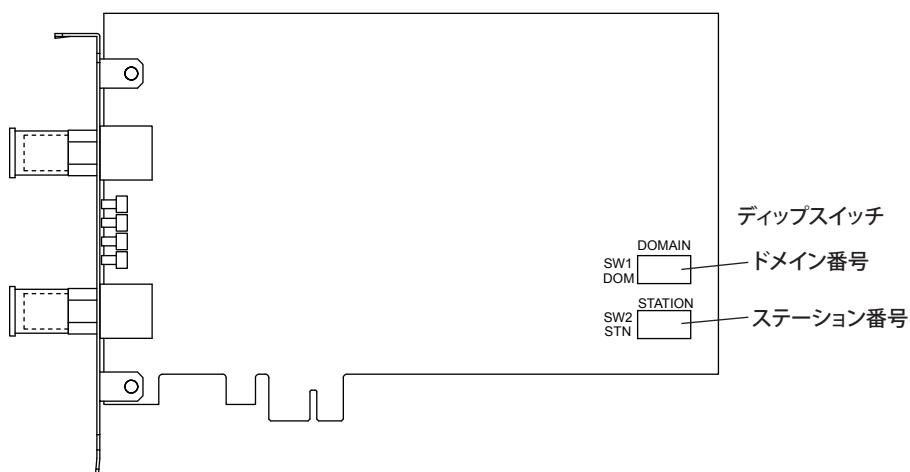
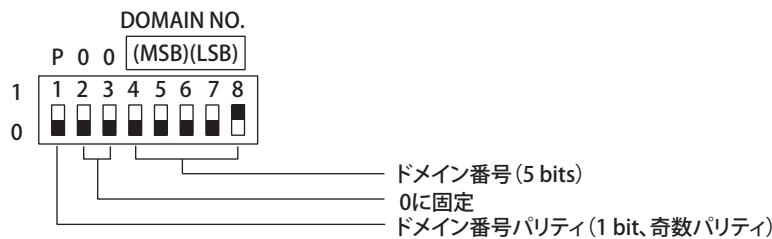


図 B4.1-1 デイップスイッチの位置

● ドメイン番号を設定する

ドメインとは、1系統の制御バスで結ばれるステーションの範囲のことです。ドメイン番号は1~16の範囲で設定してください。



MSB : Most Significant Bit (最上桁のビット)
LSB : Least Significant Bit (最下桁のビット)

図 B4.1-2 ドメイン番号設定ディップスイッチ

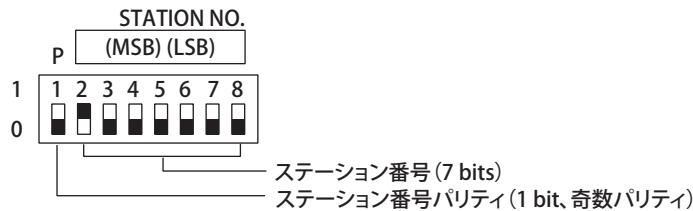
参照

ドメイン番号とそれに対応するディップスイッチの位置については、以下を参照してください。

「■ ドメイン番号と設定スイッチの位置」ページ App.1-1

● ステーション番号を設定する

ステーション番号は 1 ~ 64 の範囲で、64 から降順に設定することを推奨します。



MSB : Most Significant Bit (最上桁のビット)
LSB : Least Significant Bit (最下桁のビット)

図 B4.1-3 ステーション番号設定ディップスイッチ

参照

ステーション番号とそれに対応するディップスイッチの位置については、以下を参照してください。

「■ ステーション番号と設定スイッチの位置」ページ App.1-1

● 制御バスインターフェースカードの取り付けに関する注意事項

- VF702/VF701 カードは、Windows の設定が終了し、ネットワークの設定をする前に取り付けてください。
- VF702/VF701 カードを取り付けたあと、コンピュータを立ち上げたときに、制御バスドライバをインストールしてください。インストールの手順は、本書の説明に従ってください。

● 制御バスインターフェースカードの取り付け手順

VF702/VF701 カードにステーションアドレスを設定したあと、次の手順でコンピュータに取り付けます。

- コンピュータ本体の電源を OFF にしてください。安全のため電源プラグをコンセントから抜いてください。
- コンピュータ本体のカバーを外してください。
- スロットカバーを固定しているねじを外し、スロットカバーを外してください。
- VF702/VF701 をスロットに差し込み、固定してください。
- コンピュータ本体のカバーを取り付けてください。
- ステーションアドレスを VF702/VF701 に添付のシールに記入して、コンピュータ本体の前面または視認しやすい場所に貼ってください。

■ Vnet/IP インタフェースカードをセットアップする

Vnet/IP に接続するコンピュータには、Vnet/IP インタフェースカード（形名：VI702）を使用します。

VI702 は PCI Express 用です。

Vnet/IP インタフェースカードには、ドメイン番号とステーション番号を設定するディップスイッチと、動作モードを設定するディップスイッチがあります。ステーションアドレスは、ドメイン番号とステーション番号の組み合わせで決まります。

ディップスイッチは、ネットワーク設定の前に必ず設定してください。

ここでは、ディップスイッチの設定について説明します。

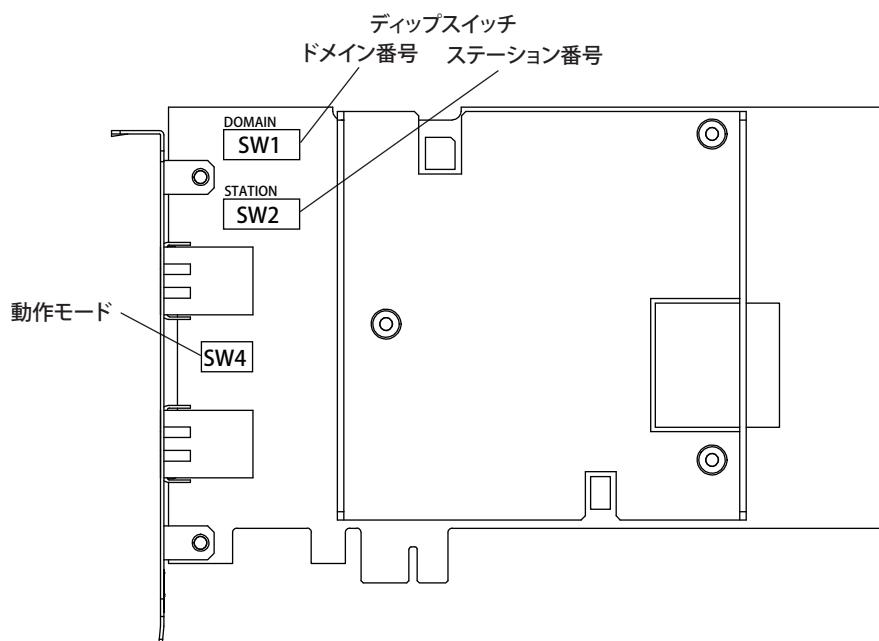
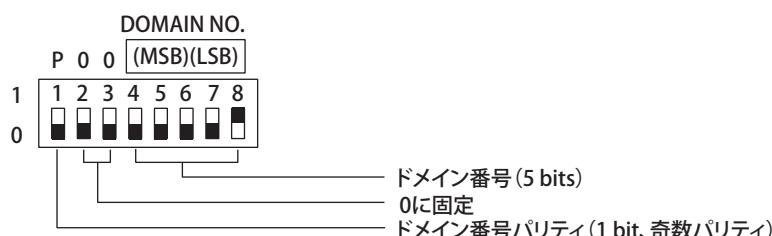


図 B4.1-4 ディップスイッチの位置

● ドメイン番号を設定する

ドメインとは、1 系統の制御バスで結ばれるステーションの範囲のことです。ドメイン番号は 1~16 の範囲で設定してください。



MSB : Most Significant Bit (最上桁のビット)

LSB : Least Significant Bit (最下桁のビット)

図 B4.1-5 ドメイン番号設定ディップスイッチ

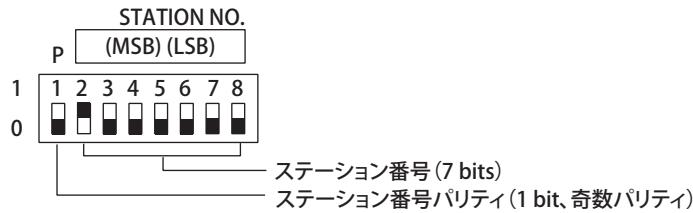
参照

ドメイン番号とそれに対応するディップスイッチの位置については、以下を参照してください。

「■ ドメイン番号と設定スイッチの位置」ページ App.1-1

● ステーション番号を設定する

ステーション番号は1～64の範囲で、64から降順に設定することを推奨します。



MSB : Most Significant Bit(最上桁のビット)
LSB : Least Significant Bit(最下桁のビット)

図 B4.1-6 ステーション番号設定ディップスイッチ

参照

ステーション番号とそれに対応するディップスイッチの位置については、以下を参照してください。

「■ ステーション番号と設定スイッチの位置」ページ App.1-1

● 動作モードスイッチ

プリント基板上のSW4は動作モードスイッチです。

このディップスイッチはすべてのビットがOFFの状態（工場出荷時）で使用してください。ディップスイッチの各ビットの意味は次のとおりです。

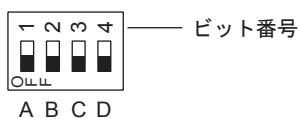


図 B4.1-7 動作モードスイッチ

表 B4.1-1 ディップスイッチの設定内容

	ディップスイッチ ON	ディップスイッチ OFF	備考
A (bit 1)	-	常に OFF	固定
B (bit 2)	100 Mbps	1 Gbps	通信スピード(デフォルト: OFF)
C (bit 3)	Force	Auto	ネゴシエーション設定(デフォルト: OFF)
D (bit 4)	-	常に OFF	固定

● Vnet/IP インタフェースカードの取り付けに関する注意事項

- Vnet/IP インタフェースカードは、Windows の設定が終了し、ネットワークの設定をする前に取り付けてください。
- Vnet/IP インタフェースカードを取り付けたあと、コンピュータを立ち上げたときに、ネットワークドライバをインストールしてください。インストールの手順は、本書の説明に従ってください。

● Vnet/IP インタフェースカードの取り付け手順

Vnet/IP インタフェースカードにステーションアドレスと動作モードを設定したあと、次の手順でコンピュータに取り付けます。

- コンピュータ本体の電源を OFFにしてください。安全のため電源プラグをコンセントから抜いてください。
- コンピュータ本体のカバーを外してください。

3. スロットカバーを固定しているねじを外し、スロットカバーを外してください。
4. Vnet/IP インタフェースカードをスロットに差し込み、固定してください。
5. コンピュータ本体のカバーを取り付けてください。
6. バス 1、バス 2 両方のケーブルを、Vnet/IP インタフェースカードとレイヤ 2 スイッチに接続してください。レイヤ 2 スイッチの電源を OFF にする必要はありません。
7. コンピュータの電源ケーブルをコンセントに接続し、コンピュータの電源を ON にしてください。
8. Vnet/IP インタフェースカードの RDY ランプが点灯することを確認してください。
9. ステーションアドレスを Vnet/IP インタフェースカードに添付のシールに記入して、コンピュータ本体の前面または視認しやすい場所に貼ってください。

B4.2 Windows の設定をする

当製品のソフトウェアをインストールする前に、コンピュータの Windows 設定を、推奨する状態に変更してください。

この設定は Windows の OS、サービスパックをインストールした状態から行います。

■ Windows の設定項目と各ステーションで必要な設定

当製品のソフトウェアをインストールする前に設定する Windows の設定項目は、ステーションの種類と OS によって異なります。実際の作業は、この表に基づいて行ってください。

表 B4.2-1 Windows 設定項目と各ステーションでの設定の要不要

Windows 設定項目	HIS	APCS	SIOS	GSGW	UGS	UACS ステーション	システム生成機能のみを搭載したコンピュータ	AD サーバのみを搭載したコンピュータ
ファイルシステム	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
パフォーマンス	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
仮想メモリ	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
電源管理	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
高速スタートアップの停止 (*1)	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Windows Defender(*2)	Yes	Yes	Yes	Yes	Yes (*3)	Yes	Yes	Yes
Windows Update (*4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ディスクデフラグ (*5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
パスワードの設定 (*6)	Yes	Yes	No	Yes	No (*7)	Yes	Yes	Yes
ルート証明書 (*8)	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
Windows 更新ログ ラム	Yes (*9)	Yes (*10)	Yes (*11)	Yes (*11)	Yes (*12)	No	Yes (*13)	Yes (*11)
DCOM の設定	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

*1: Windows 10 のみ

*2: Windows 10、Windows 7、Windows Server 2016、および Windows Server 2008 R2 のみ

*3: コンピュータ切替型 UGS では No です。

*4: Windows 10、および Windows Server 2016 のみ

*5: Windows 10、Windows 7、Windows Server 2016、および Windows Server 2012 R2 のみ

*6: Windows Server 2016、Windows Server 2012 R2、および Windows Server 2008 R2 のみ

*7: コンピュータ切替型 UGS では Yes です。

*8: Windows 7、および Windows Server 2008 R2 のみ

*9: Windows 7 または Windows Server 2008 R2 の場合は Yes です。Windows 10 でシステム生成機能を搭載する HIS は Yes です。それ以外は No です。

*10: Windows Server 2008 R2 の場合は Yes です。それ以外は No です。

*11: Windows 7 または Windows Server 2008 R2 の場合は Yes です。それ以外は No です。

*12: Windows Server 2012 R2 の場合は Yes です。それ以外は No です。

*13: Windows 10、Windows 7、または Windows Server 2008 R2 の場合は Yes です。それ以外は No です。

B4.2.1 Windows 10 で設定する

Windows 10 を使用するときは、次の設定方法に従ってください。

■ ファイルシステム

ファイルシステムは、NTFS 形式にしてください。FAT 形式になっている場合は、OS から再インストールを行い、パーティションを NTFS 形式にフォーマットし直してください。OS がインストールされていないパーティションについても、NTFS 形式にフォーマットしてください。

■ システムのパフォーマンス

システムのパフォーマンスは、次の方法で設定してください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [システム] – [システムの詳細設定] を選択してください。
システムのプロパティダイアログが表示されます。
4. [詳細設定] タブで、[パフォーマンス] の [設定] をクリックしてください。
パフォーマンスオプションダイアログが表示されます。
5. [視覚効果] タブで、[コンピュータに応じて最適なものを自動的に選択する] を選択してください。
6. [OK] をクリックしてください。

■ 仮想メモリ

仮想メモリは、カスタムサイズで設定することを推奨します。次の手順に従ってください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [システム] – [システムの詳細設定] を選択してください。
システムのプロパティダイアログが表示されます。
4. [詳細設定] タブで、[パフォーマンス] の [設定] をクリックしてください。
パフォーマンスオプションダイアログが表示されます。
5. [詳細設定] タブで、[次を最適なパフォーマンスに調整] の [プログラム] を選択し、[仮想メモリ] の [変更] をクリックしてください。
仮想メモリダイアログが表示されます。
6. [すべてのドライブのページングファイルのサイズを自動的に管理する] チェックボックスをオフにしてください。
7. [カスタムサイズ] を選択し、主記憶サイズの 1.5 倍となる値を、初期サイズと最大サイズに設定してください。
たとえば、主記憶サイズが 6 GB なら 9216 MB、8 GB なら 12288 MB としてください。
8. [設定] をクリックしたあと、[OK] をクリックしてください。

補足

設定終了後、再起動を促すダイアログが表示されることがあります。その場合は、ダイアログの指示に従い、再起動をしてください。

■ 電源管理

電源管理の設定方法を次に示します。説明の中には、コンピュータ構成により項目が表示されないものがあります。表示されない場合、機能自体が無効です。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [ハードウェアとサウンド] – [電源オプション] を選択してください。
電源オプションウィンドウが表示されます。
4. [お気に入りのプラン] の [高パフォーマンス] を選択し、その右の [プラン設定の変更] をクリックしてください。
プラン設定の編集ウィンドウが表示されます。

補足

[お気に入りのプラン] に [高パフォーマンス] がない場合、[追加のプランの表示] をクリックし、[高パフォーマンス] を選択して、その右の [プラン設定の変更] をクリックしてください。

5. [詳細な電源設定の変更] をクリックしてください。
電源オプションダイアログが表示されます。

補足

コンピュータの構成の違いによって、これ以降で説明される設定項目の中で、表示されないものがあります。その場合、その機能自体が無効であることを意味します。

6. [ハードディスク] の [次の時間が経過後ハードディスクの電源を切る] の設定を [なし] にしてください。
7. [スリープ] を、次のように設定してください。
 - [次の時間が経過後スリープする] :なし
 - [ハイブリッドスリープを許可する] :オフ
 - [次の時間が経過後休止状態にする] :なし
 - [スリープ解除タイマーの許可] :無効
8. [電源ボタンとカバー] の [電源ボタンの操作] の設定を [シャットダウン] にしてください。
9. [ディスプレイ] を、次のように設定してください。
 - [次の時間が経過後ディスプレイの電源を切る] :なし
 - [自動輝度調整を有効にする] :オフ
10. [OK] をクリックしてください。

補足

UPS の設定は当製品のソフトウェアのインストール後に行います。

■ 高速スタートアップの停止

制御バスドライバや Vnet/IP オープン通信ドライバをインストールする前に、高速スタートアップを停止してください。

高速スタートアップを停止するときには、次の手順に従ってください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [ハードウェアとサウンド] – [電源オプション] を選択してください。
電源オプションウィンドウが表示されます。
4. 左ペインで、[電源ボタンの動作の選択] をクリックしてください。
システム設定ウィンドウが表示されます。
5. [現在利用可能ではない設定を変更します] をクリックしてください。

6. [シャットダウン設定] に [高速スタートアップを有効にする (推奨)] チェックボックスが表示され、チェックボックスが選択されている場合は、チェックボックスをオフにしてください。

補足

[高速スタートアップを有効にする (推奨)] チェックボックスが表示されない場合は、本設定は不要です。

7. [変更の保存] ボタンをクリックしてください。
8. コンピュータを再起動してください。

重要

高速スタートアップを停止したあとに、必ず再起動してください。

■ Windows Defender

Windows Defender は、スパイウェアを検出、除去するソフトウェアです。

当製品では、この機能を利用しませんので、無効にすることを推奨します。

ドメイン環境の場合は、グループポリシーを利用して一括設定するなど、ドメインの管理運用方法により Windows Defender を無効にしてください。

ワークグループ環境の場合は、ローカルグループポリシーエディターで Windows Defender を無効化してください。

● ローカルグループポリシーエディターで Windows Defender を無効化する

次に設定方法を示します。

1. 管理者ユーザでサインインしてください。
2. コマンドプロンプトを起動してください。
3. gredit.msc と入力してください。
ローカルグループポリシーエディターが表示されます。
4. 左ペインで、[コンピューターの構成] – [管理用テンプレート] – [Windows コンポーネント] – [Endpoint Protection] を選択してください。
5. 右ペインで [Endpoint Protection を無効にする] をダブルクリックしてください。
Endpoint Protection を無効にするダイアログが表示されます。
6. [有効] を選択し、[OK] をクリックしてください。

■ Windows Update

Windows Update は、Windows を更新する機能です。

当製品では、次の理由により Windows Update を無効にする必要があります。

- Windows Update を有効にしていると当製品のソフトウェアのインストールに時間がかかる。
- 当製品のソフトウェアが動作するコンポーネントは連続運転を前提としているが、Windows Update を有効にしているとコンピュータが再起動してしまう。

補足

Windows Server Update Service (WSUS) を利用する場合は、当製品のソフトウェアのインストール後に、Windows の自動更新を手動で有効にしてから、WSUS の設定を行ってください。

Windows Update を無効にするときは、次の手順に従ってください。

1. 管理者ユーザでサインインしてください。
2. コマンドプロンプトを起動してください。
3. gredit.msc と入力してください。
ローカルグループポリシーエディターが表示されます。

4. 左ペインで、[コンピューターの構成] – [管理用テンプレート] – [Windows コンポーネント] – [Windows Update] を選択してください。
5. 右ペインで [自動更新を構成する] をダブルクリックしてください。
自動更新を構成するダイアログが表示されます。
6. [無効] を選択し、[OK] をクリックしてください。

参照

Windows Update を手動で有効にする手順については、以下を参照してください。

「■ Windows Update を有効にする」ページ C7-7

■ ドライブのデフラグと最適化

ドライブのデフラグツールは、コンピュータのハードディスク上の断片化したファイルを統合して、システムのパフォーマンスを向上させます。当製品ではパフォーマンスへの影響が大きいことが考えられますので、ディスクデフラグツールの定期的な実行を無効にすることを推奨します。

なお、システムのパフォーマンスが落ちていると感じた場合や点検時などには、必要に応じて手動でディスクデフラグツールを実行してください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [管理ツール] – [ドライブのデフラグと最適化] を選択してください。
ドライブの最適化ウィンドウが表示されます。
4. [設定の変更] をクリックしてください。
ドライブの最適化ダイアログが表示されます。
5. [スケジュールに従って実行する (推奨)] チェックボックスをオフにして [OK] をクリックしてください。

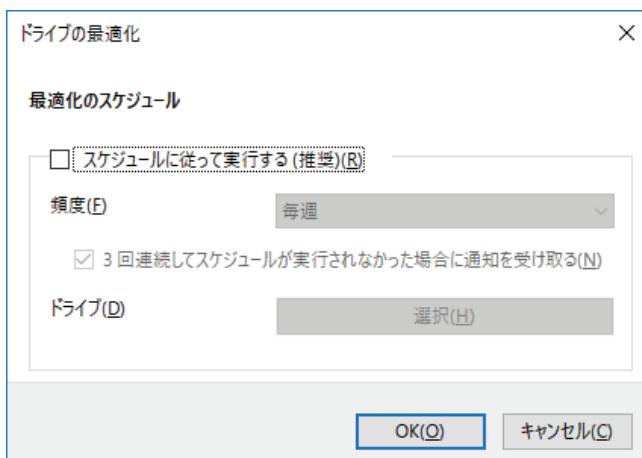


図 B4.2.1-1 ドライブの最適化ダイアログ

■ 自動クリーンアップタスクの無効化

更新プログラムを適用したときに、古くなったファイルを自動でクリーンアップする機能が追加されました。

自動クリーンアップの実行により、システムパフォーマンスが低下することがあるので、自動クリーンアップタスクの無効化を推奨します。

自動クリーンアップタスクを無効にするときは、次の手順に従ってください。

1. 管理者ユーザでサインインしてください。

2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [管理ツール] – [タスクスケジューラ] を選択してください。
タスクスケジューラウィンドウが表示されます。
4. 左ペインで、[タスクスケジューラ(ローカル)] – [タスクスケジューラライブラリ] – [Microsoft] – [Windows] – [Servicing] を選択してください。
5. 中央のペインで [StartComponentCleanup] を右クリックして、[無効] を選択してください。

■ Windows 更新プログラムのインストール

Windows 更新プログラムをダウンロードし、適用してください。

参照

Windows 更新プログラムのダウンロードについては、以下を参照してください。

「● Windows 更新プログラムのダウンロード (Windows 10)」ページ B1-3

■ DCOM の設定

DCOM の設定で既定の認証レベルが [なし] に設定されていると、再頒布モジュールなどのアプリケーションのインストールに失敗します。当製品をインストールするときは、既定の認証レベルを [接続] に設定してください。既定の認証レベルを [接続] にするときは、次の手順に従ってください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [管理ツール] – [コンポーネントサービス] を選択してください。

コンポーネントサービスウィンドウが表示されます。

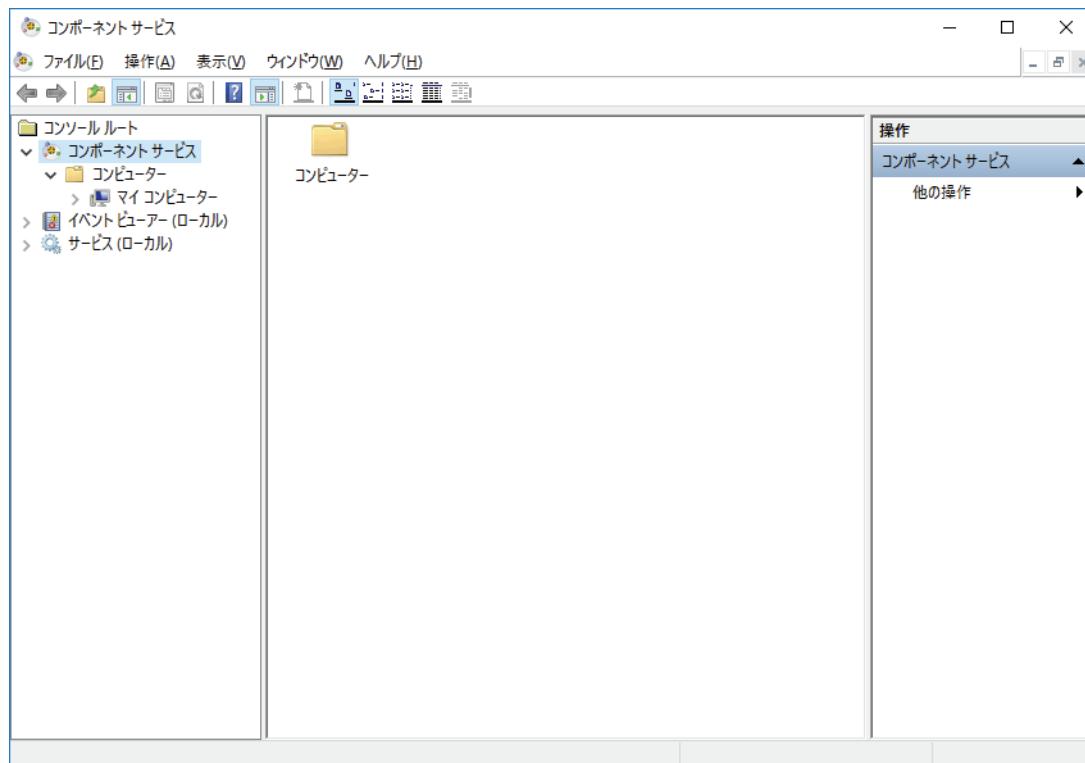


図 B4.2.1-2 コンポーネントサービスウィンドウ

4. [コンソールルート] – [コンポーネントサービス] – [コンピュータ] を選択してください。
5. [マイコンピュータ] を右クリックして、[プロパティ] を選択してください。
マイコンピュータのプロパティダイアログが表示されます。

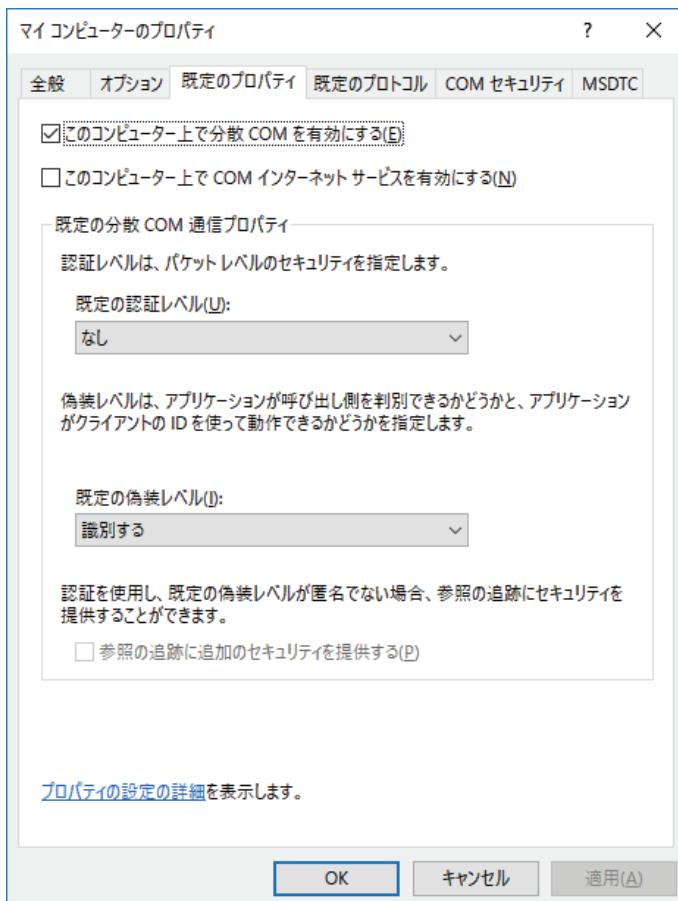


図 B4.2.1-3 マイコンピュータのプロパティダイアログ

6. [既定のプロパティ] タブを開き、[既定の認証レベル] のドロップダウンリストから [接続] を選択して、[OK] をクリックしてください。
7. コンピュータを再起動してください。

B4.2.2 Windows 7 で設定する

Windows 7 を使用するときは、次の設定方法に従ってください。

■ ファイルシステム

ファイルシステムは、NTFS 形式にしてください。FAT 形式になっている場合は、OS から再インストールを行い、パーティションを NTFS 形式にフォーマットし直してください。OS がインストールされていないパーティションについても、NTFS 形式にフォーマットしてください。

■ システムのパフォーマンス

システムのパフォーマンスは、次の方法で設定してください。

1. 管理者ユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [システム] – [システムの詳細設定] を選択してください。
システムのプロパティダイアログが表示されます。
4. [詳細設定] タブを選択し、[パフォーマンス] の [設定] をクリックしてください。
パフォーマンスオプションダイアログが表示されます。
5. [視覚効果] タブを選択し、[コンピュータに応じて最適なものを自動的に選択する] を選択してください。

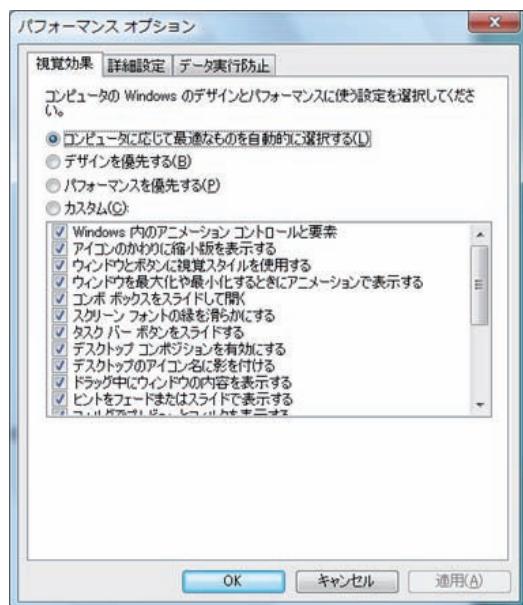


図 B4.2.2-1 パフォーマンスオプションダイアログ（視覚効果タブ）

6. [OK] をクリックしてください。

■ 仮想メモリ

仮想メモリは、カスタムサイズで設定することを推奨します。次の手順に従ってください。

1. 管理者ユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [システム] – [システムの詳細設定] を選択してください。

システムのプロパティダイアログが表示されます。

4. [詳細設定] タブを選択し、[パフォーマンス] の [設定] をクリックしてください。パフォーマンスオプションダイアログが表示されます。
5. [詳細設定] タブで、[次を最適なパフォーマンスに調整] の [プログラム] を選択し、[仮想メモリ] の [変更] をクリックしてください。
仮想メモリダイアログが表示されます。
6. [すべてのドライブのページングファイルのサイズを自動的に管理する] チェックボックスをオフにしてください。
7. [カスタムサイズ] を選択し、主記憶サイズの 1.5 倍となる値を、初期サイズと最大サイズに設定してください。
たとえば、主記憶サイズが 6GB なら 9216MB、8GB なら 12288MB としてください。

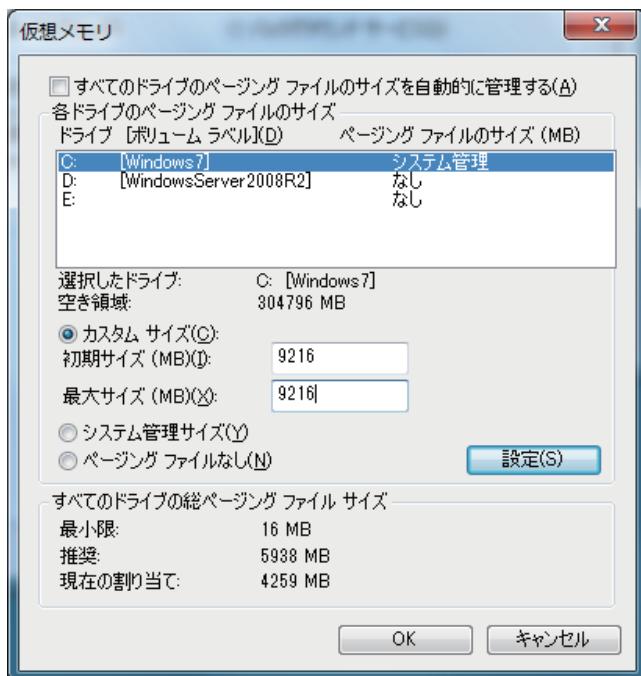


図 B4.2.2-2 仮想メモリダイアログ

8. [設定] をクリックしたあと、[OK] をクリックしてください。

補足

設定終了後、再起動を促すダイアログが表示されることがあります。その場合は、ダイアログの指示に従い、再起動をしてください。

■ 電源管理

電源管理の設定方法を次に示します。説明の中には、コンピュータ構成により項目が表示されないものがあります。表示されない場合、機能自体が無効です。

1. 管理者ユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. [ハードウェアとサウンド] – [電源オプション] を選択してください。
電源オプションダイアログが表示されます。
4. [お気に入りのプラン] の [高パフォーマンス] を選択し、その右の [プラン設定の変更] をクリックしてください。
プラン設定の変更ウィンドウが表示されます。

補足

[お気に入りのプラン] に [高パフォーマンス] がない場合、[追加のプランを表示します] をクリックし、[高パフォーマンス] を選択して、その右の [プラン設定の変更] をクリックしてください。

5. [詳細な電源設定の変更] をクリックしてください。
電源オプションダイアログに詳細設定が表示されます。

補足

コンピュータの構成の違いによって、これ以降で説明される詳細設定の項目の中で、表示されないものがあります。その場合、その機能自体が無効であることを意味します。

6. [ハードディスク] の [次の時間が経過後ハードディスクの電源を切る] の設定を [なし] にしてください。

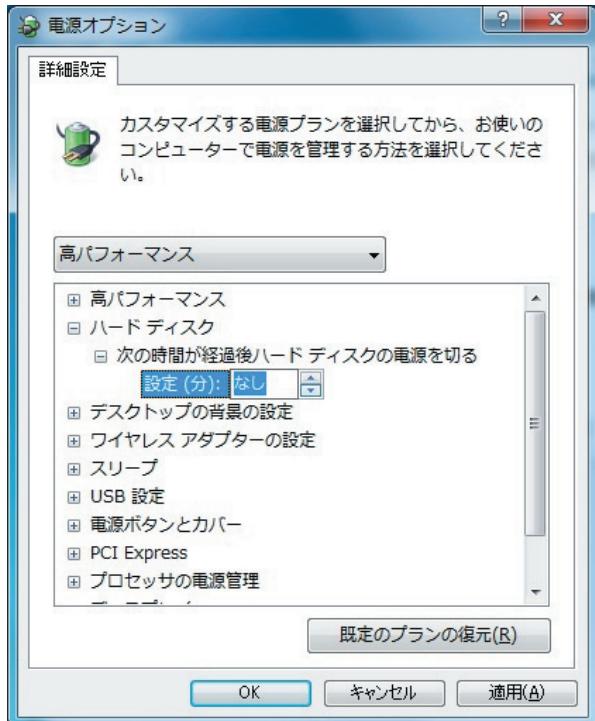


図 B4.2.2-3 電源オプション詳細設定

7. [スリープ] を、次のように設定してください。
- [次の時間が経過後スリープする] :なし
 - [ハイブリッドスリープを許可する] :オフ
 - [次の時間が経過後休止状態にする] :なし
 - [スリープ解除タイマーの許可] :無効

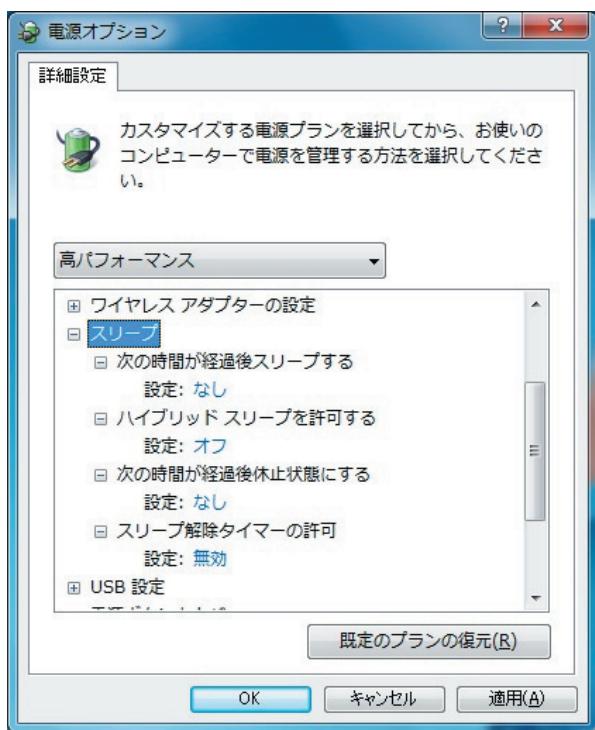


図 B4.2.2-4 電源オプション詳細設定

- [電源ボタンとカバー] の [電源ボタンの操作] の設定を [シャットダウン] にしてください。

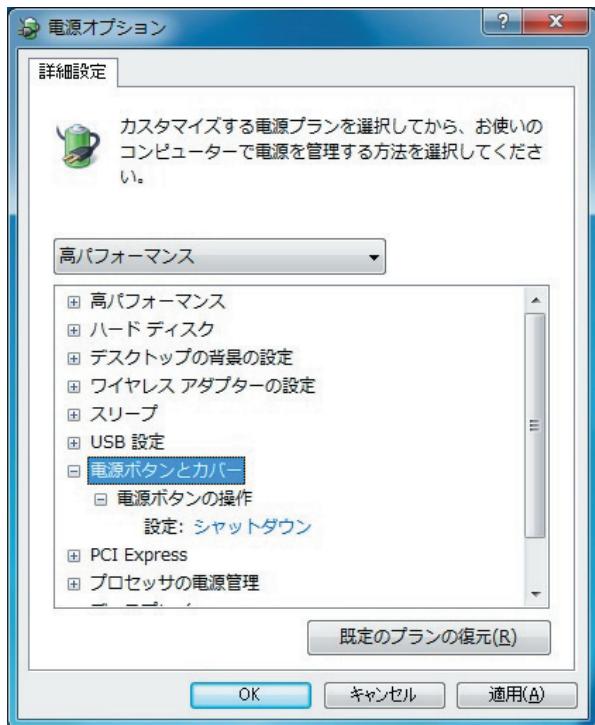


図 B4.2.2-5 電源オプション詳細設定

- [ディスプレイ] の [次の時間が経過後ディスプレイの電源を切る] の設定を [なし] にしてください。

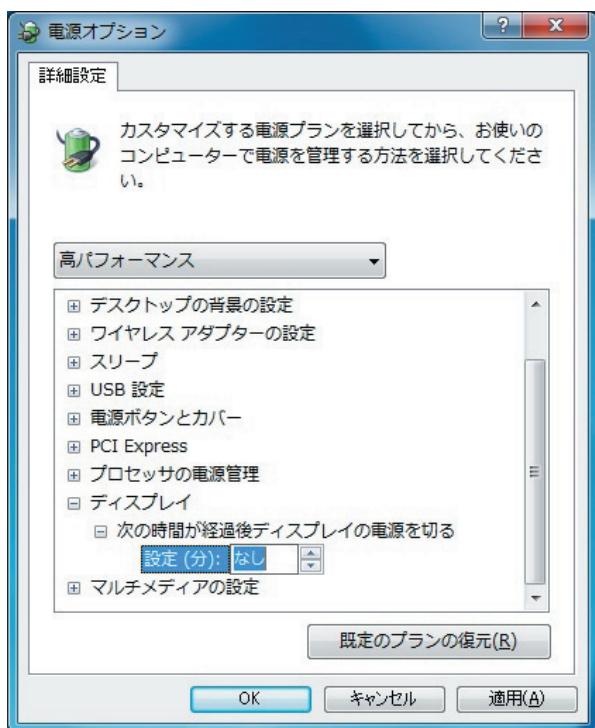


図 B4.2.2-6 電源オプション詳細設定

10. [OK] をクリックしてください。

補足

UPS の設定は、当製品のソフトウェアのインストール後に行います。

参照

UPS の設定については、以下を参照してください。

「B4.12 UPS（無停電電源装置）の設定をする」ページ B4-149

■ Windows Defender

Windows Defender は、スパイウェアを検出、除去するソフトウェアです。

当製品では、この機能を利用しませんので、無効にすることを推奨します。

ドメイン環境の場合は、グループポリシーを利用して一括設定するなど、ドメインの管理運用方法により Windows Defender を無効にしてください。

ワークグループ環境の場合は、次のいずれかの方法で Windows Defender を無効化してください。

- コントロールパネルで Windows Defender を無効化する
- ローカルグループポリシーエディターで Windows Defender を無効化する

補足

Windows Defender の [ツール] がグレーアウトされている場合、ローカルグループポリシーエディターで無効化してください。

● コントロールパネルで Windows Defender を無効化する

1. 管理者ユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. 表示方法で [大きいアイコン] か [小さいアイコン] を選択し、[Windows Defender] を選択してください。

Windows Defender ウィンドウが表示されます。

4. 上部に表示されている [ツール] をクリックしてください。
ツールと設定のウィンドウが表示されます。
5. [オプション] をクリックしてください。
オプションのウィンドウが表示されます。
6. 左側のメニューから [管理者] を選択し、[このプログラムを使用する] チェックボックスをオフにしてください。

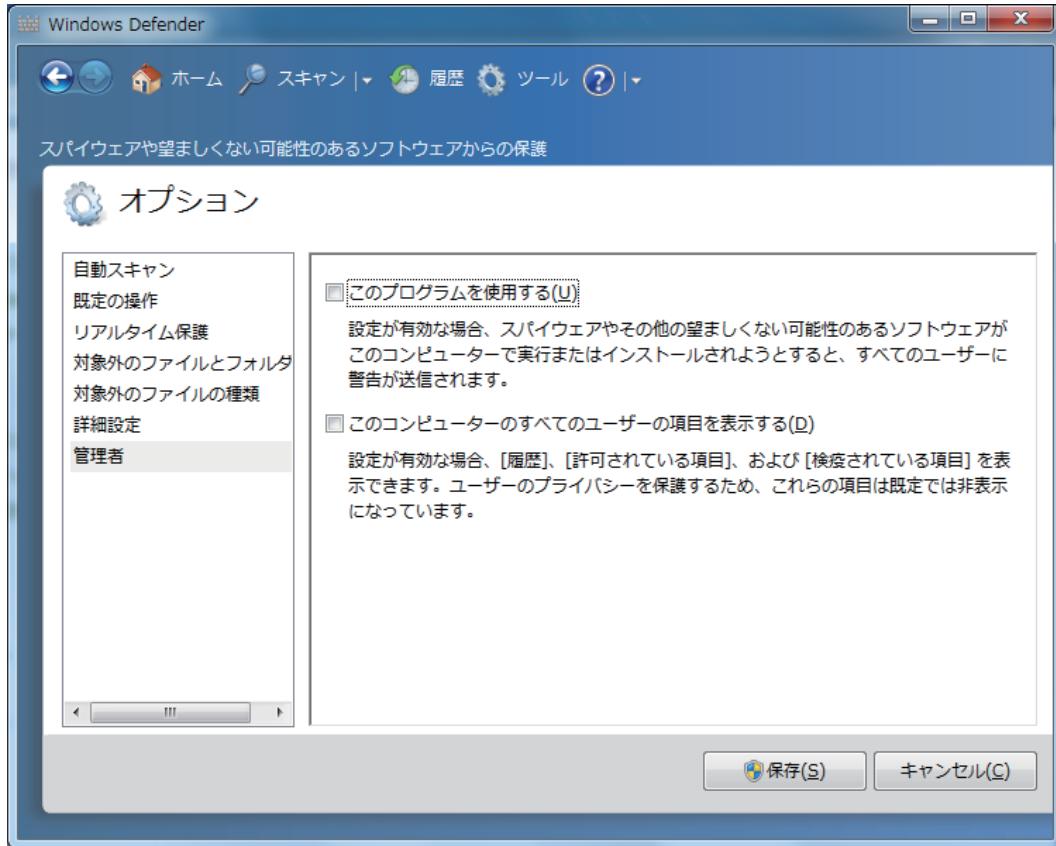


図 B4.2.2-7 オプション

7. [保存] をクリックしてください。
Windows Defender が無効になったことを示すダイアログが表示されます。
8. [x] ボタンをクリックしてください。

● ローカルグループポリシーエディターで Windows Defender を無効化する

補足

Windows Defender の [ツール] がグレーアウトされている場合、ローカルグループポリシーエディターで Windows Defender を無効化します。

次に設定方法を示します。

1. 管理者ユーザでログオンしてください。
2. コマンドプロンプトを起動してください。
3. `gpedit.msc` と入力してください。
ローカルグループポリシーエディターのウィンドウが表示されます。
4. [コンピューターの構成] – [管理用テンプレート] – [Windows コンポーネント] – [Windows Defender] を選択し、右側に表示されている [Windows Defender をオフにする] をダブルクリックしてください。
Windows Defender をオフにするダイアログが表示されます。

5. [有効] を選択し、[OK] をクリックしてください。

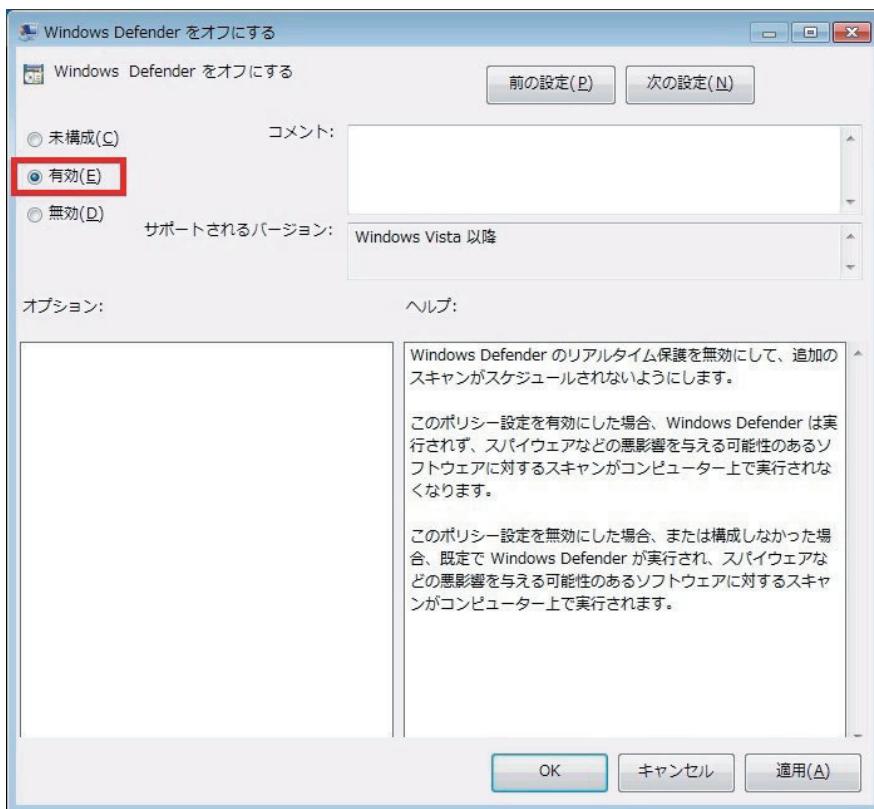


図 B4.2.2-8 Windows Defender をオフにする

■ ディスクデフラグ

ディスクデフラグツールは、コンピュータのハードディスク上の断片化したファイルを統合して、システムのパフォーマンスを向上させます。Windows 7では、ディスクデフラグツールを定期的（毎週水曜日 1:00）に実行するスケジュールが設定されています。当製品ではパフォーマンスへの影響が大きいことが考えられますので、ディスクデフラグツールの定期的な実行を無効にすることを推奨します。

なお、システムのパフォーマンスが落ちていると感じた場合や点検時などには、必要に応じて手動でディスクデフラグツールを実行してください。

1. 管理者ユーザでログオンしてください。
2. ディスクデフラグツールを起動してください。
3. [スケジュールの構成] をクリックしてください。
スケジュールの変更ダイアログが表示されます。
4. [スケジュールに従って実行する（推奨）] チェックボックスをオフにして [OK] をクリックしてください。

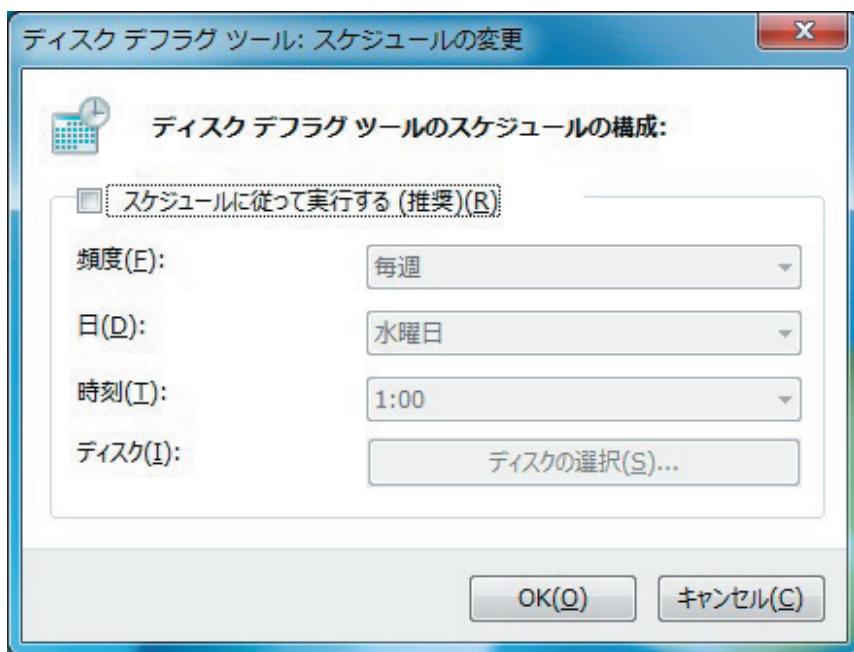


図 B4.2.2-9 スケジュールの変更ダイアログ

■ ルート証明書を適用する

Windows 7 には、.NET Framework 4.6.2 パッケージの証明書の検証に必要なルート証明書がデフォルトでは含まれていません。そのため、オフライン環境では.NET Framework 4.6.2 のインストールに失敗します。

.NET Framework 4.6.2 のインストールに必要となるルート証明書(Microsoft Root Certificate Authority 2011)を適用する必要があります。

ルート証明書を適用するときは、次の手順に従ってください。

1. CENTUM VP ソフトウェアをインストールする管理者ユーザでログオンしてください。

重要

本設定はユーザごとの設定です。CENTUM VP ソフトウェアのインストール時に.NET Framework 4.6.2 がインストールされますので、別の管理者ユーザではなく、CENTUM VP ソフトウェアをインストールする管理者ユーザでログオンしてください。

2. CENTUM VP のソフトウェアメディアをドライブに挿入してください。
3. コマンドプロンプトを起動してください。
4. certmgr.msc と入力してください。
certmgr が起動します。
5. 左ペインの「信頼されたルート証明機関」を右クリックして、[すべてのタスク] – [インポート] を選択してください。
証明書のインポートウィザードが表示されます。
6. [次へ] をクリックしてください。
「インポートする証明書ファイル」が表示されます。
7. [参照] をクリックして、次のファイルを指定してください。
<CENTUM VP ソフトウェアメディアドライブ>:\Microsoft\Certificates\MicrosoftRootCertificateAuthority2011.cer
8. [次へ] をクリックしてください。
「証明書ストア」が表示されます。

9. [証明書をすべて次のストアに配置する] を選択して、[次へ] をクリックしてください。
「証明書のインポートウィザードの完了」が表示されます。
10. [完了] をクリックしてください。
セキュリティ警告ダイアログが表示されます。
11. [はい] をクリックしてください。
証明書のインポートウィザードダイアログが表示され、証明書のインポートが完了します。

■ Windows 更新プログラムのインストール

Windows 更新プログラムをダウンロードし、適用してください。

参照

Windows 更新プログラムのダウンロード手順については、以下を参照してください。

「● Windows 更新プログラムのダウンロード (Windows 7 または Windows Server 2008 R2)」ページ
B1-4

B4.2.3 Windows Server 2016 で設定する

Windows Server 2016 を使用するときは、次の設定方法に従ってください。

■ ファイルシステム

ファイルシステムは、NTFS 形式にしてください。FAT 形式になっている場合は、OS から再インストールを行い、パーティションを NTFS 形式にフォーマットし直してください。OS がインストールされていないパーティションについても、NTFS 形式にフォーマットしてください。

■ システムのパフォーマンス

システムのパフォーマンスは、次の方法で設定してください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [システム] – [システムの詳細設定] を選択してください。
システムのプロパティダイアログが表示されます。
4. [詳細設定] タブで、[パフォーマンス] の [設定] をクリックしてください。
パフォーマンスオプションダイアログが表示されます。
5. [視覚効果] タブで、[コンピュータに応じて最適なものを自動的に選択する] を選択してください。
6. [OK] をクリックしてください。

■ 仮想メモリ

仮想メモリは、カスタムサイズで設定することを推奨します。次の手順に従ってください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [システム] – [システムの詳細設定] を選択してください。
システムのプロパティダイアログが表示されます。
4. [詳細設定] タブで、[パフォーマンス] の [設定] をクリックしてください。
パフォーマンスオプションダイアログが表示されます。
5. [詳細設定] タブで、[次を最適なパフォーマンスに調整] の [プログラム] を選択し、[仮想メモリ] の [変更] をクリックしてください。
仮想メモリダイアログが表示されます。
6. [すべてのドライブのページングファイルのサイズを自動的に管理する] チェックボックスをオフにしてください。
7. [カスタムサイズ] を選択し、主記憶サイズの 1.5 倍となる値を、初期サイズと最大サイズに設定してください。
たとえば、主記憶サイズが 6 GB なら 9216 MB、8 GB なら 12288 MB としてください。
8. [設定] をクリックしたあと、[OK] をクリックしてください。

補足

設定終了後、再起動を促すダイアログが表示されることがあります。その場合は、ダイアログの指示に従い、再起動をしてください。

■ 電源管理

電源管理の設定方法を次に示します。説明の中には、コンピュータ構成により項目が表示されないものがあります。表示されない場合、機能自体が無効です。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [ハードウェア] – [電源オプション] を選択してください。
電源オプションウィンドウが表示されます。
4. [お気に入りのプラン] の [高パフォーマンス] を選択し、その右の [プラン設定の変更] をクリックしてください。
プラン設定の編集ウィンドウが表示されます。

補足

[お気に入りのプラン] に [高パフォーマンス] がない場合、[追加のプランの表示] をクリックし、[高パフォーマンス] を選択して、その右の [プラン設定の変更] をクリックしてください。

5. [詳細な電源設定の変更] をクリックしてください。
電源オプションダイアログが表示されます。

補足

コンピュータの構成の違いによって、これ以降で説明される設定項目の中で、表示されないものがあります。その場合、その機能自体が無効であることを意味します。

6. [ハードディスク] の [次の時間が経過後ハードディスクの電源を切る] の設定を [なし] にしてください。
7. [スリープ] を、次のように設定してください。
 - [次の時間が経過後スリープする] :なし
 - [ハイブリッドスリープを許可する] :オフ
 - [次の時間が経過後休止状態にする] :なし
 - [スリープ解除タイマーの許可] :無効
8. [電源ボタンとカバー] の [電源ボタンの操作] の設定を [シャットダウン] にしてください。
9. [ディスプレイ] を次のように設定してください。
 - [次の時間が経過後ディスプレイの電源を切る] :なし
 - [自動輝度調整を有効にする] :オフ
10. [OK] をクリックしてください。

補足

UPS の設定は当製品のソフトウェアのインストール後に行います。

■ Windows Defender

Windows Defender は、スパイウェアを検出、除去するソフトウェアです。

当製品では、この機能を利用しませんので、無効にすることを推奨します。

ドメイン環境の場合は、グループポリシーを利用して一括設定するなど、ドメインの管理運用方法により Windows Defender を無効にしてください。

ワークグループ環境の場合は、ローカルグループポリシーエディターで Windows Defender を無効化してください。

● ローカルグループポリシーエディターで Windows Defender を無効化する

次に設定方法を示します。

1. 管理者ユーザでサインインしてください。

2. コマンドプロンプトを起動してください。
3. gredit.msc と入力してください。
ローカルグループポリシーエディターが表示されます。
4. 左ペインで、[コンピューターの構成] – [管理用テンプレート] – [Windows コンポーネント] – [Endpoint Protection] を選択してください。
5. 右ペインで [Endpoint Protection を無効にする] をダブルクリックしてください。
Endpoint Protection を無効にするダイアログが表示されます。
6. [有効] を選択し、[OK] をクリックしてください。

■ Windows Update

Windows Update は、Windows を更新する機能です。

当製品では、次の理由により Windows Update を無効にする必要があります。

- Windows Update を有効にしていると当製品のソフトウェアのインストールに時間がかかる。
- 当製品のソフトウェアが動作するコンポーネントは連続運転を前提としているが、Windows Update を有効にしているとコンピュータが再起動してしまう。

補足

Windows Server Update Service (WSUS) を利用する場合は、当製品のソフトウェアのインストール後に、Windows の自動更新を手動で有効にしてから、WSUS の設定を行ってください。

Windows Update を無効にするとときは、次の手順に従ってください。

1. 管理者ユーザでサインインしてください。
2. コマンドプロンプトを起動してください。
3. gredit.msc と入力してください。
ローカルグループポリシーエディターが表示されます。
4. 左ペインで、[コンピューターの構成] – [管理用テンプレート] – [Windows コンポーネント] – [Windows Update] を選択してください。
5. 右ペインで [自動更新を構成する] をダブルクリックしてください。
自動更新を構成するダイアログが表示されます。
6. [無効] を選択し、[OK] をクリックしてください。

参照

Windows Update を手動で有効にする手順については、以下を参照してください。

「■ Windows Update を有効にする」ページ C7-7

■ ドライブのデフラグと最適化

ドライブのデフラグツールは、コンピュータのハードディスク上の断片化したファイルを統合して、システムのパフォーマンスを向上させます。当製品ではパフォーマンスへの影響が大きいことが考えられますので、ディスクデフラグツールの定期的な実行を無効にすることを推奨します。

なお、システムのパフォーマンスが落ちていると感じた場合や点検時などには、必要に応じて手動でディスクデフラグツールを実行してください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [管理ツール] – [ドライブのデフラグと最適化] を選択してください。
ドライブの最適化ウィンドウが表示されます。
4. [設定の変更] をクリックしてください。

ドライブの最適化ダイアログが表示されます。

5. [スケジュールに従って実行する（推奨）] チェックボックスをオフにして [OK] をクリックしてください。

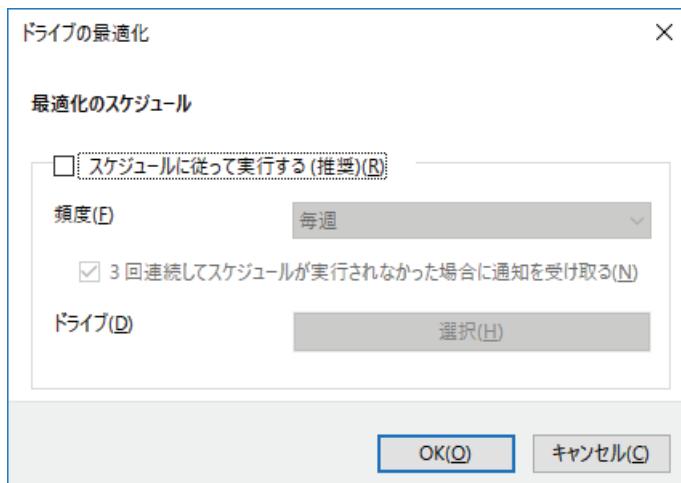


図 B4.2.3-1 ドライブの最適化ダイアログ

■ 自動クリーンアップタスクの無効化

更新プログラムを適用したときに、古くなったファイルを自動でクリーンアップする機能が追加されました。

自動クリーンアップの実行により、システムパフォーマンスが低下することがあるので、自動クリーンアップタスクの無効化を推奨します。

自動クリーンアップタスクを無効にするときは、次の手順に従ってください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [管理ツール] – [タスクスケジューラ] を選択してください。
タスクスケジューラウィンドウが表示されます。
4. 左ペインで、[タスクスケジューラ(ローカル)] – [タスクスケジューラライブラリ] – [Microsoft] – [Windows] – [Servicing] を選択してください。
5. 中央のペインで [StartComponentCleanup] を右クリックして、[無効] を選択してください。

■ パスワードの設定

Windows Server 2016 ではセキュリティが強化されているため、ユーザのパスワード設定で複雑さが求められる場合や、思いどおりに設定ができない場合があります。

このような場合には次の設定を行ってください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [管理ツール] – [ローカルセキュリティポリシー] を選択してください。
ローカルセキュリティポリシーウィンドウが表示されます。
4. 左のペインで [セキュリティの設定] – [アカウントポリシー] – [パスワードのポリシー] を選択してください。
ポリシーの一覧が表示されます。

5. 右のペインで [複雑さの要件を満たす必要があるパスワード] をダブルクリックしてください。
複雑さの要件を満たす必要があるパスワードのプロパティダイアログが表示されます。
6. [無効] を選択し、[OK] をクリックしてください。
7. [複雑さの要件を満たす必要があるパスワード] の設定が無効になっていることを確認してください。

■ DCOM の設定

DCOM の設定で既定の認証レベルが [なし] に設定されていると、再頒布モジュールなどのアプリケーションのインストールに失敗します。当製品をインストールするときは、既定の認証レベルを [接続] に設定してください。既定の認証レベルを [接続] にするときは、次の手順に従ってください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [管理ツール] – [コンポーネントサービス] を選択してください。

コンポーネントサービスウィンドウが表示されます。

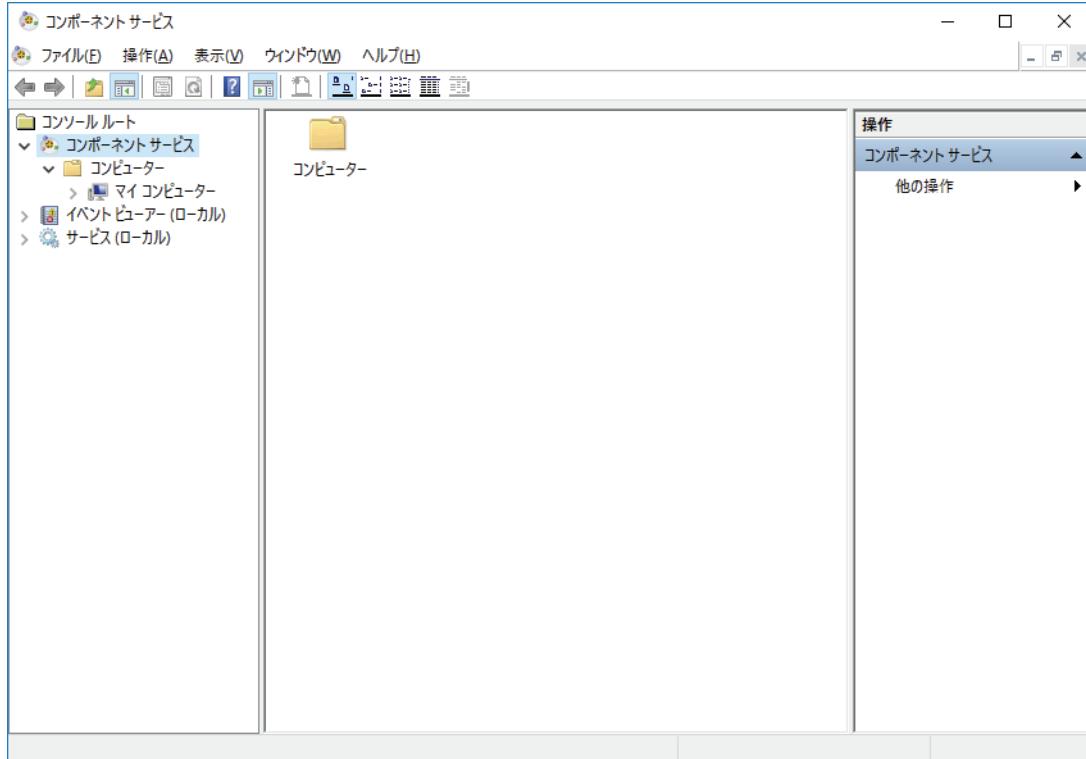


図 B4.2.3-2 コンポーネントサービスウィンドウ

4. [コンソールルート] – [コンポーネントサービス] – [コンピュータ] を選択してください。
5. [マイコンピュータ] を右クリックして、[プロパティ] を選択してください。
マイコンピュータのプロパティダイアログが表示されます。

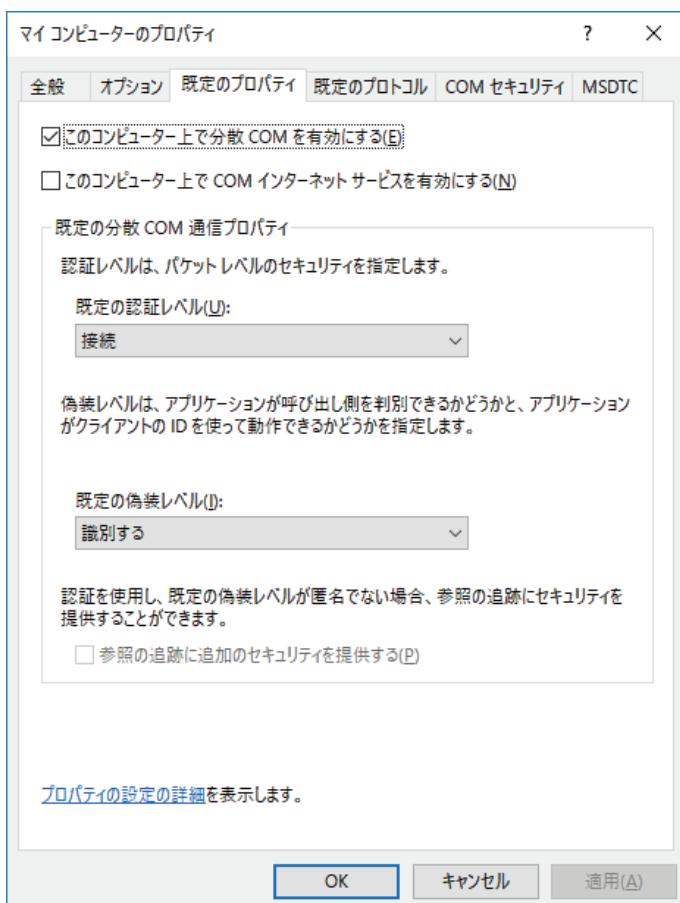


図 B4.2.3-3 マイコンピュータのプロパティダイアログ

6. [既定のプロパティ] タブを開き、[既定の認証レベル] のドロップダウンリストから [接続] を選択して、[OK] をクリックしてください。
7. コンピュータを再起動してください。

B4.2.4 Windows Server 2012 R2 で設定する

Windows Server 2012 R2 を使用するときは、次の設定方法に従ってください。

補足

Windows Server 2012 R2 は、コンピュータ切替型 UGS のみサポートです。

■ ファイルシステム

ファイルシステムは、NTFS 形式にしてください。FAT 形式になっている場合は、OS から再インストールを行い、パーティションを NTFS 形式にフォーマットし直してください。OS がインストールされていないパーティションについても、NTFS 形式にフォーマットしてください。

■ システムのパフォーマンス

システムのパフォーマンスは、次の方法で設定してください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] をクリックしてください。
4. [システム] をクリックしてください。
5. 画面左の [システムの詳細設定] をクリックしてください。
システムのプロパティダイアログが表示されます。
6. [詳細設定] タブを選択し、[パフォーマンス] の [設定] をクリックしてください。
パフォーマンスオプションダイアログが表示されます。
7. [視覚効果] タブを選択し、[パフォーマンスを優先する] を選択してください。
8. [OK] をクリックしてください。

■ 仮想メモリ

仮想メモリは、カスタムサイズで設定することを推奨します。次の手順に従ってください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] をクリックしてください。
4. [システム] をクリックしてください。
5. 画面左の [システムの詳細設定] をクリックしてください。
システムのプロパティダイアログが表示されます。
6. [詳細設定] タブを選択し、[パフォーマンス] の [設定] をクリックしてください。
パフォーマンスオプションダイアログが表示されます。
7. [詳細設定] タブで、[次を最適なパフォーマンスに調整] の [プログラム] を選択し、[仮想メモリ] の [変更] をクリックしてください。
仮想メモリダイアログが表示されます。
8. [すべてのドライブのページングファイルのサイズを自動的に管理する] チェックボックスをクリアしてください。
9. [カスタムサイズ] を選択し、主記憶サイズの 1.5 倍の値を初期サイズと最大サイズに設定してください。
たとえば、主記憶サイズが 6 GB なら 9216 MB、8 GB なら 12288 MB としてください。
10. [設定] をクリックしたあと、[OK] をクリックしてください。

補足

設定終了後、再起動を促すダイアログが表示されることがあります。その場合は、ダイアログの指示に従い、再起動をしてください。

■ 電源管理

電源管理の設定方法を次に示します。説明の中には、コンピュータ構成により項目が表示されないものがあります。表示されない場合、機能自体が無効です。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [ハードウェア] をクリックしてください。
4. [電源オプション] をクリックしてください。
電源オプションウィンドウが表示されます。
5. [お気に入りのプラン] の [高パフォーマンス] を選択し、その右の [プラン設定の変更] をクリックしてください。
プラン設定の編集ウィンドウが表示されます。

補足

[お気に入りのプラン] に [高パフォーマンス] がない場合、[追加のプランの表示] をクリックし、[高パフォーマンス] を選択して、その右の [プラン設定の変更] をクリックしてください。

6. [詳細な電源設定の変更] をクリックしてください。
電源オプションダイアログが表示されます。

補足

コンピュータの構成の違いによって、これ以降で説明される詳細設定の項目の中で、表示されないものがあります。その場合、その機能自体が無効であることを意味します。

7. [ハードディスク] の [次の時間が経過後ハードディスクの電源を切る] の設定を [なし] にしてください。
8. [スリープ] を、次のように設定してください。
 - [次の時間が経過後スリープする] : なし
 - [ハイブリッドスリープを許可する] : オフ
 - [次の時間が経過後休止状態にする] : なし
 - [スリープ解除タイマーの許可] : 無効
9. [電源ボタンとカバー] の [電源ボタンの操作] の設定を [シャットダウン] にしてください。
10. [ディスプレイ] の [次の時間が経過後ディスプレイの電源を切る] の設定を [なし] にしてください。
11. [OK] をクリックしてください。

■ ドライブのデフラグと最適化

ドライブのデフラグツールは、コンピュータのハードディスク上の断片化したファイルを統合して、システムのパフォーマンスを向上させます。当製品ではパフォーマンスへの影響が大きいことが考えられますので、ディスクデフラグツールの定期的な実行を無効にすることを推奨します。

なお、システムのパフォーマンスが落ちていると感じた場合や点検時などには、必要に応じて手動でディスクデフラグツールを実行してください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。

3. [システムとセキュリティ] – [管理ツール] – [ドライブのデフラグと最適化] を選択してください。
ドライブの最適化ウィンドウが表示されます。
4. [設定の変更] をクリックしてください。
ドライブの最適化ダイアログが表示されます。
5. [スケジュールに従って実行する (推奨)] のチェックボックスをクリアして [OK] をクリックしてください。

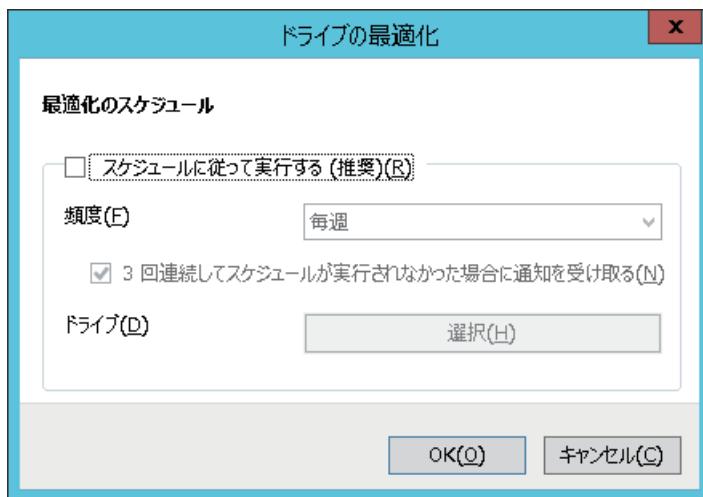


図 B4.2.4-1 ドライブの最適化ダイアログ

■ 自動クリーンアップタスクの無効化

更新プログラムを適用したときに、古くなったファイルを自動でクリーンアップする機能が追加されました。

自動クリーンアップの実行により、システムパフォーマンスが低下することがあるので、自動クリーンアップタスクの無効化を推奨します。

自動クリーンアップタスクを無効にするときは、次の手順に従ってください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [管理ツール] – [タスクスケジューラ] を選択してください。
タスクスケジューラウィンドウが表示されます。
4. 左ペインで、[タスクスケジューラ(ローカル)] – [タスクスケジューラライブラリ] – [Microsoft] – [Windows] – [Servicing] を選択してください。
5. 中央のペインで [StartComponentCleanup] を右クリックして、[無効] を選択してください。

■ パスワードの設定

Windows Server 2012 R2 ではセキュリティが強化されているため、ユーザのパスワード設定で複雑さが求められる場合や、思いどおりに設定ができない場合があります。

このような場合には次の設定を行ってください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [管理ツール] – [ローカルセキュリティポリシー] を選択してください。
ローカルセキュリティポリシーウィンドウが表示されます。

4. 左のペインで [セキュリティの設定] – [アカウントポリシー] – [パスワードのポリシー] を選択してください。
ポリシーの一覧が表示されます。
5. 右のペインで [複雑さの要件を満たす必要があるパスワード] をダブルクリックしてください。
複雑さの要件を満たす必要があるパスワードのプロパティダイアログが表示されます。
6. [無効] を選択し、[OK] をクリックしてください。
7. [複雑さの要件を満たす必要があるパスワード] の設定が無効になっていることを確認してください。

■ Windows 更新プログラムのインストール

用途に合わせて、Windows 更新プログラムをインストールしてください。

● ドメインコントローラ、ファイルサーバの場合

Windows 更新プログラムをダウンロードし、適用してください。

参照

Windows 更新プログラムのダウンロードについては、以下を参照してください。

「● Windows 更新プログラムのダウンロード (Windows Server 2012 R2)」ページ B1-4

● PC 冗長化プラットフォームを搭載したコンピュータの場合

PC 冗長化プラットフォームをインストールしたあとは、次に示す Windows 更新プログラムをダウンロードし、適用してください。

- 2014 年 11 月の Windows Server 2012 のセキュリティ更新プログラム
Windows 更新プログラムを適用するには、次の手順に従ってください。
 1. 管理者ユーザでサインインしてください。
 2. PC 冗長化プラットフォームインストールメディアをドライブに挿入してください。
 3. エクスプローラで、<DVD ドライブ>:\GuestOS\Win2012EvrR2\Updates を表示してください。
 4. [Windows8.1-KB2919442-x64.msu] をダブルクリックしてください。
Windows Update スタンドアロンインストーラダイアログが表示されます。
 5. [はい] をクリックしてください。
インストールを開始します。
 6. インストールが完了したら、[閉じる] をクリックしてください。
 7. [Windows8.1-KB2919355-x64.msu] をダブルクリックしてください。
Windows Update スタンドアロンインストーラダイアログが表示されます。
 8. [はい] をクリックしてください。
インストールを開始します。
 9. インストールが完了したら、[今すぐ再起動] をクリックして、コンピュータを再起動してください。
 10. [Windows8.1-KB2995730-x64.msu] をダブルクリックしてください。
Windows Update スタンドアロンインストーラダイアログが表示されます。
 11. [はい] をクリックしてください。
インストールを開始します。
 12. インストールが完了したら、[今すぐ再起動] をクリックして、コンピュータを再起動してください。

13. 2014 年 11 月の Windows Server 2012 のセキュリティ更新プログラムを適用してください。

補足

本情報は、2019 年 3 月時点のものです。最新情報は、エンドポイントセキュリティ対策サービスとして提供しています。エンドポイントセキュリティ対策サービスについては、当社にお問い合わせください。

● .NET Framework 4.6.2 のインストールの停止方法

Windows 更新プログラムをインストールする前に当製品のソフトウェアをインストールすると、.NET Framework 4.6.2 のインストールの途中で当製品のソフトウェアのインストールが停止します。その場合は、.NET Framework 4.6.2 のインストールを停止してから、Windows 更新プログラムをインストールする必要があります。

.NET Framework 4.6.2 のインストールを停止するときは、次の手順に従ってください。

1. タスクマネージャーを起動してください。

2. [詳細] タブで、[NDP462-KB3151800-x86-x64-AIOS-ENU.exe] を右クリックして、[タスクの終了] を選択してください。

.NET Framework 4.6.2 のインストールが停止して、当製品のソフトウェアのインストールも停止します。

■ DCOM の設定

DCOM の設定で既定の認証レベルが [なし] に設定されていると、再頒布モジュールなどのアプリケーションのインストールに失敗します。当製品をインストールするときは、既定の認証レベルを [接続] に設定してください。既定の認証レベルを [接続] にするときは、次の手順に従ってください。

1. 管理者ユーザでサインインしてください。

2. コントロールパネルを起動してください。

3. [システムとセキュリティ] – [管理ツール] – [コンポーネントサービス] を選択してください。

コンポーネントサービスウィンドウが表示されます。

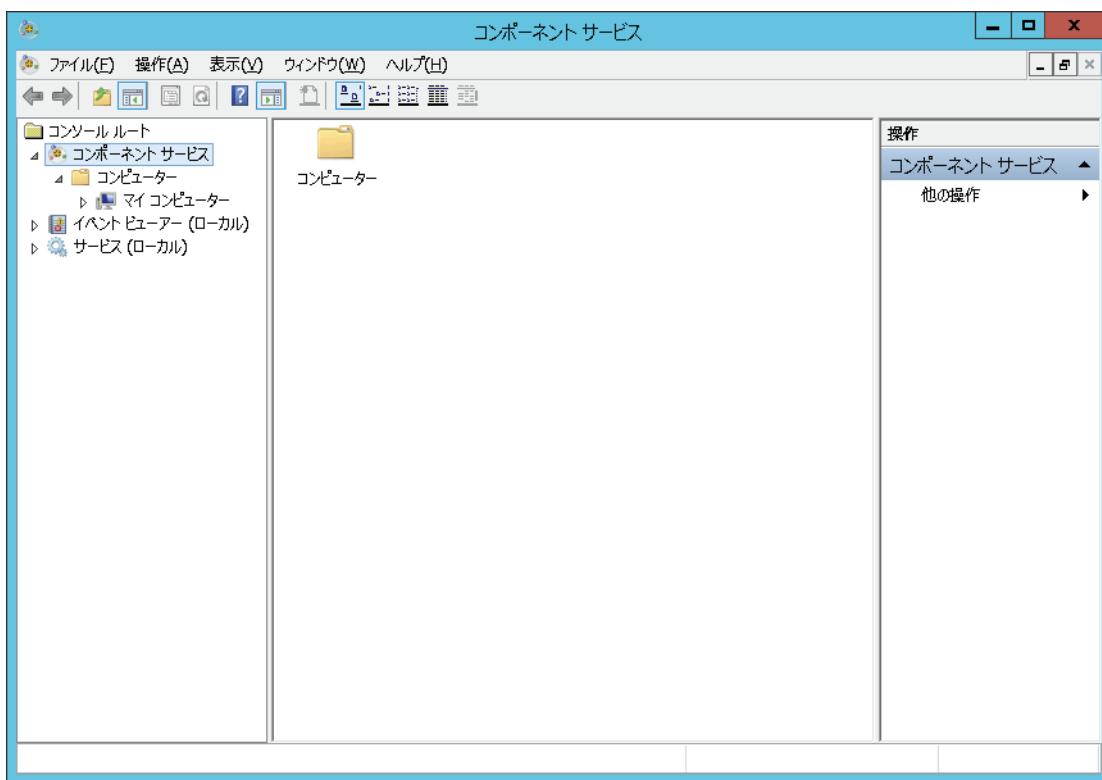


図 B4.2.4-2 コンポーネントサービスウィンドウ

4. [コンソールルート] – [コンポーネントサービス] – [コンピュータ] を選択してください。
5. [マイコンピュータ] を右クリックして、[プロパティ] を選択してください。
マイコンピュータのプロパティダイアログが表示されます。

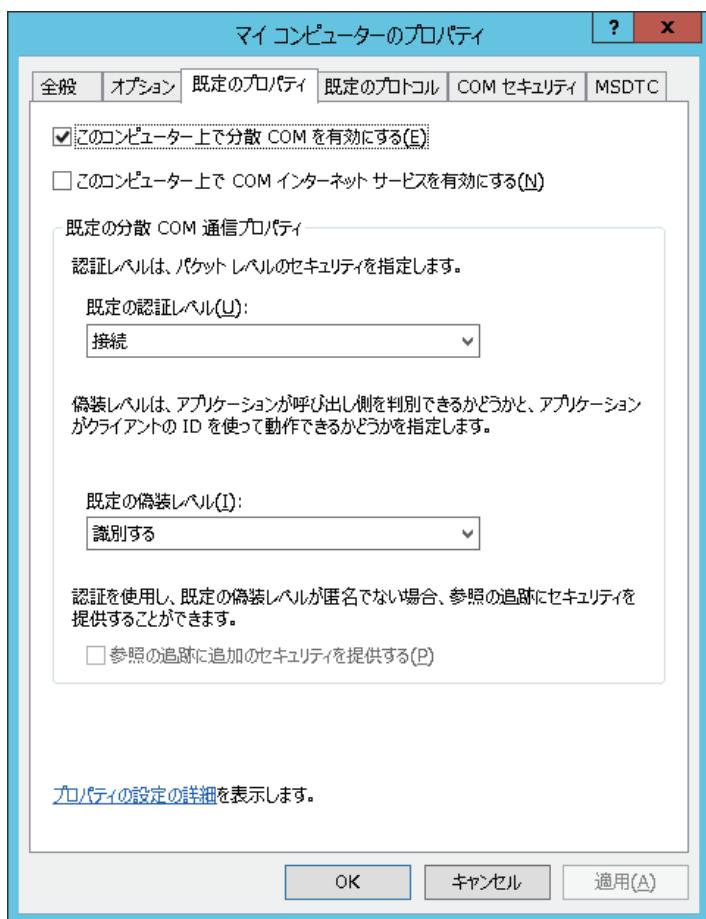


図 B4.2.4-3 マイコンピュータのプロパティダイアログ

6. [既定のプロパティ] タブを開き、[既定の認証レベル] のドロップダウンリストから [接続] を選択して、[OK] をクリックしてください。
7. コンピュータを再起動してください。

B4.2.5 Windows Server 2008 R2 で設定する

Windows Server 2008 R2 を使用するときは、次の設定方法に従ってください。

■ ファイルシステム

ファイルシステムは、NTFS 形式にしてください。FAT 形式になっている場合は、OS から再インストールを行い、パーティションを NTFS 形式にフォーマットし直してください。OS がインストールされていないパーティションについても、NTFS 形式にフォーマットしてください。

■ システムのパフォーマンス

システムのパフォーマンスは、次の方法で設定してください。

1. 管理者ユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [システム] – [システムの詳細設定] を選択してください。
システムのプロパティダイアログが表示されます。
4. [詳細設定] タブを選択し、[パフォーマンス] の [設定] をクリックしてください。
パフォーマンスオプションダイアログが表示されます。
5. [視覚効果] タブを選択し、[パフォーマンスを優先する] を選択してください。

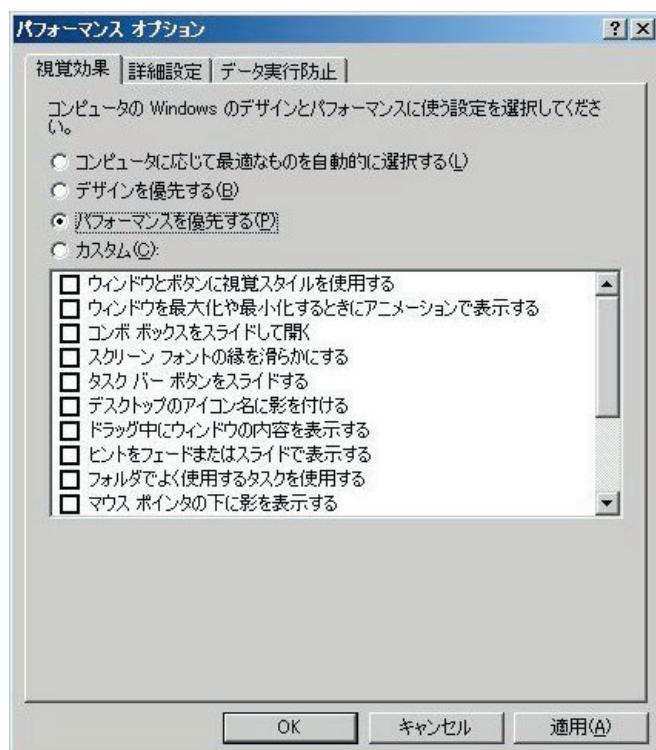


図 B4.2.5-1 パフォーマンスオプションダイアログ（視覚効果タブ）

6. [OK] をクリックしてください。

■ 仮想メモリ

仮想メモリは、カスタムサイズで設定することを推奨します。次の手順に従ってください。

1. 管理者ユーザでログオンしてください。

2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [システム] – [システムの詳細設定] を選択してください。
システムのプロパティダイアログが表示されます。
4. [詳細設定] タブを選択し、[パフォーマンス] の [設定] をクリックしてください。
パフォーマンスオプションダイアログが表示されます。
5. [詳細設定] タブで、[次を最適なパフォーマンスに調整] の [プログラム] を選択し、[仮想メモリ] の [変更] をクリックしてください。
仮想メモリダイアログが表示されます。
6. [すべてのドライブのページングファイルのサイズを自動的に管理する] チェックボックスをオフにしてください。
7. [カスタムサイズ] を選択し、主記憶サイズの 1.5 倍の値を初期サイズと最大サイズに設定してください。
たとえば、主記憶サイズが 6GB なら 9216MB、8GB なら 12288MB としてください。

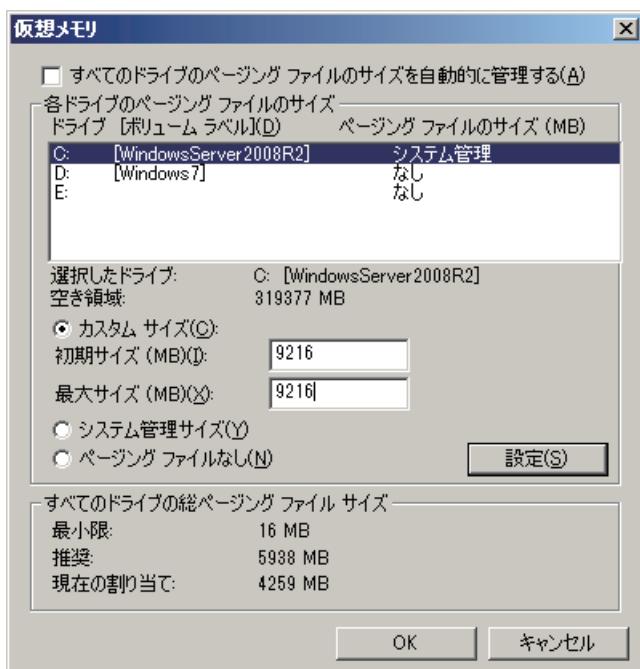


図 B4.2.5-2 仮想メモリダイアログ

8. [設定] をクリックしたあと、[OK] をクリックしてください。

補足

設定終了後、再起動を促すダイアログが表示されることがあります。その場合は、ダイアログの指示に従い、再起動をしてください。

■ 電源管理

電源管理の設定方法を次に示します。説明の中には、コンピュータ構成により項目が表示されないものがあります。表示されない場合、機能自体が無効です。

1. 管理者ユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. [ハードウェア] – [電源オプション] を選択してください。
電源オプションダイアログが表示されます。
4. [お気に入りのプラン] の [高パフォーマンス] を選択し、その右の [プラン設定の変更] をクリックしてください。
プラン設定の編集ウィンドウが表示されます。

補足

[お気に入りのプラン] に [高パフォーマンス] がない場合、[追加のプランを表示します] をクリックし、[高パフォーマンス] を選択して、その右の [プラン設定の変更] をクリックしてください。

5. [詳細な電源設定の変更] をクリックしてください。
電源オプションダイアログに詳細設定が表示されます。

補足

コンピュータの構成の違いによって、これ以降で説明される詳細設定の項目の中で、表示されないものがあります。その場合、その機能自体が無効であることを意味します。

6. [ハードディスク] の [次の時間が経過後ハードディスクの電源を切る] の設定を [なし] にしてください。

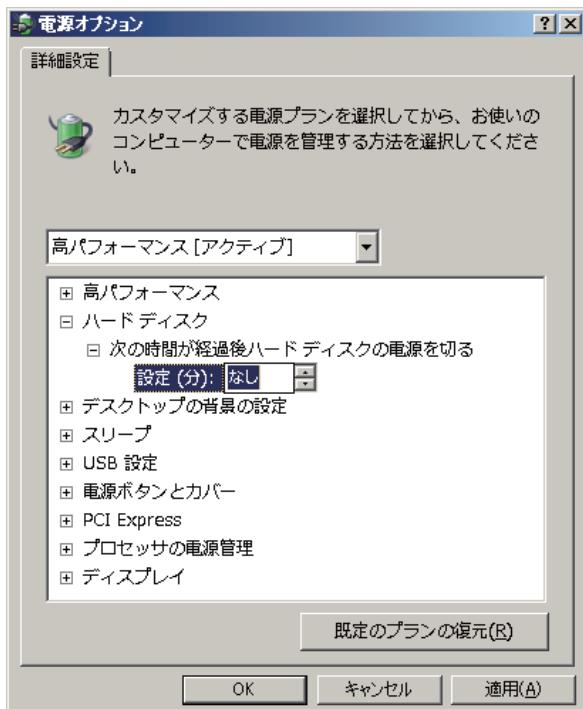


図 B4.2.5-3 電源オプション詳細設定

7. [スリープ] を、次のように設定してください。
 - [次の時間が経過後スリープする] : なし
 - [ハイブリッドスリープを許可する] : オフ
 - [次の時間が経過後休止状態にする] : なし
 - [スリープ解除タイマーの許可] : 無効

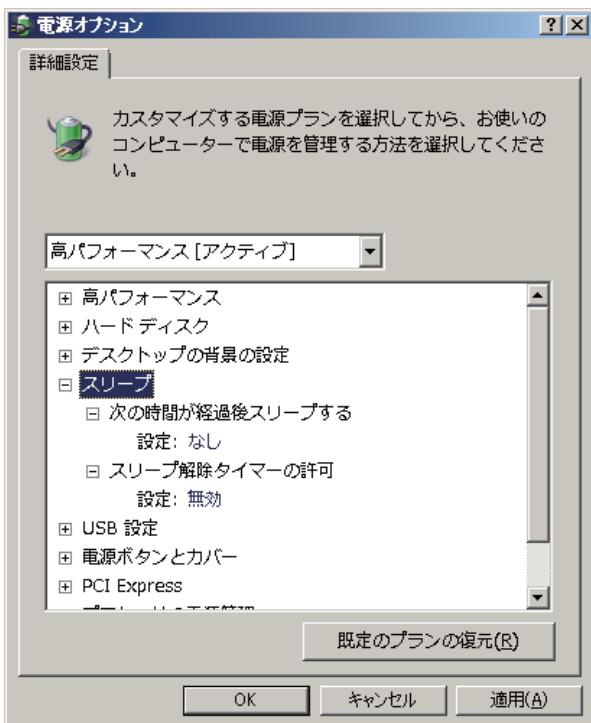


図 B4.2.5-4 電源オプション詳細設定

8. [電源ボタンとカバー] の [電源ボタンの操作] の設定を [シャットダウン] にしてください。

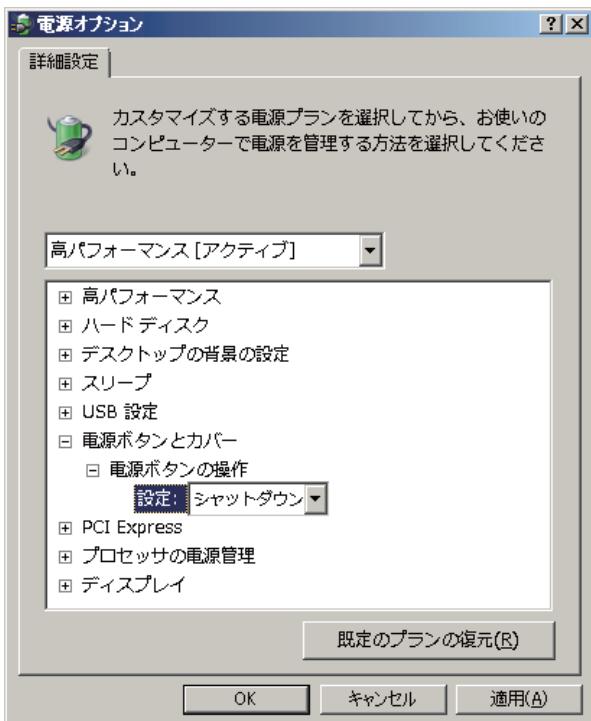


図 B4.2.5-5 電源オプション詳細設定

9. [ディスプレイ] の [次の時間が経過後ディスプレイの電源を切る] の設定を [なし] にしてください。

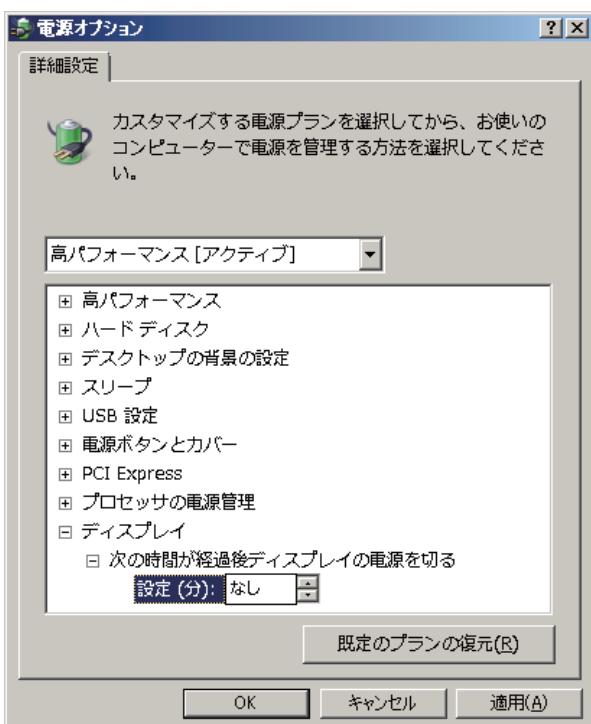


図 B4.2.5-6 電源オプション詳細設定

10. [OK] をクリックしてください。

補足

UPS の設定は、当製品のソフトウェアのインストール後に行います。

参照

UPS の設定については、以下を参照してください。

「B4.12 UPS（無停電電源装置）の設定をする」ページ B4-149

■ Windows Defender

Windows Defender は、スパイウェアを検出、除去するソフトウェアです。

当製品では、この機能を利用しませんので、無効にすることを推奨します。

ドメイン環境の場合は、グループポリシーを利用して一括設定するなど、ドメインの管理運用方法により Windows Defender を無効にしてください。

ワークグループ環境の場合は、ローカルグループポリシーエディターで Windows Defender を無効化してください。

● ローカルグループポリシーエディターで Windows Defender を無効化する

次に設定方法を示します。

1. 管理者ユーザでログオンしてください。
2. コマンドプロンプトを起動してください。
3. `gpedit.msc` と入力してください。
ローカルグループポリシーエディターが表示されます。
4. 左ペインで、[コンピューターの構成] – [管理用テンプレート] – [Windows コンポーネント] – [Windows Defender] を選択してください。
5. 右ペインで [Windows Defender をオフにする] をダブルクリックしてください。
Windows Defender をオフにするダイアログが表示されます。
6. [有効] を選択し、[OK] をクリックしてください。

■ パスワードの設定

Windows Server 2008 R2 ではセキュリティが強化されているため、ユーザのパスワード設定で複雑さが求められる場合や、思いどおりに設定ができない場合があります。

このような場合には次の設定を行ってください。

1. 管理者ユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [管理ツール] – [ローカルセキュリティポリシー] を選択してください。
ローカルセキュリティポリシーウィンドウが表示されます。
4. 左のペインで [セキュリティの設定] – [アカウントポリシー] – [パスワードのポリシー] を選択してください。
ポリシーの一覧が表示されます。
5. 右のペインで [複雑さの要件を満たす必要があるパスワード] をダブルクリックしてください。
複雑さの要件を満たす必要があるパスワードのプロパティダイアログが表示されます。
6. [無効] を選択し、[OK] をクリックしてください。
7. [複雑さの要件を満たす必要があるパスワード] の設定が無効になっていることを確認してください。

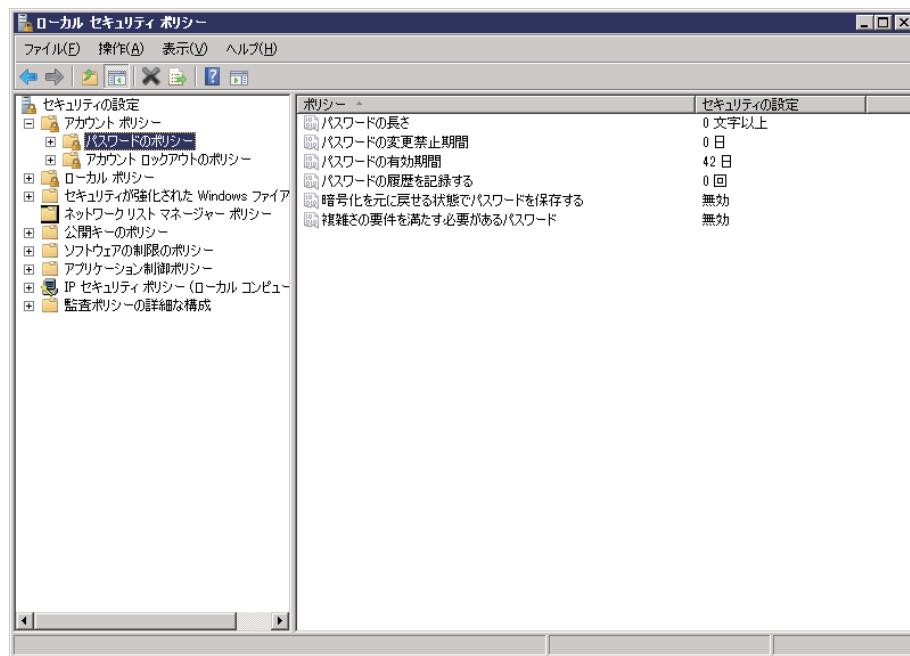


図 B4.2.5-7 ローカルセキュリティポリシー

■ ルート証明書を適用する

Windows Server 2008 R2 には、.NET Framework 4.6.2 パッケージの証明書の検証に必要なルート証明書がデフォルトでは含まれていません。そのため、オフライン環境では.NET Framework 4.6.2 のインストールに失敗します。

.NET Framework 4.6.2 のインストールに必要となるルート証明書(Microsoft Root Certificate Authority 2011)を適用する必要があります。

ルート証明書を適用するときは、次の手順に従ってください。

1. CENTUM VP ソフトウェアをインストールする管理者ユーザでログオンしてください。

重要

本設定はユーザごとの設定です。CENTUM VP ソフトウェアのインストール時に.NET Framework 4.6.2 がインストールされますので、別の管理者ユーザではなく、CENTUM VP ソフトウェアをインストールする管理者ユーザでログオンしてください。

2. CENTUM VP のソフトウェアメディアをドライブに挿入してください。
3. コマンドプロンプトを起動してください。
4. certmgr.msc と入力してください。
certmgr が起動します。
5. 左ペインの [信頼されたルート証明機関] を右クリックして、[すべてのタスク] – [インポート] を選択してください。
証明書のインポートウィザードが表示されます。
6. [次へ] をクリックしてください。
「インポートする証明書ファイル」が表示されます。
7. [参照] をクリックして、次のファイルを指定してください。
<CENTUM VP ソフトウェアメディアドライブ>:\Microsoft\Certificates\MicrosoftRootCertificateAuthority2011.cer
8. [次へ] をクリックしてください。
「証明書ストア」が表示されます。
9. [証明書をすべて次のストアに配置する] を選択して、[次へ] をクリックしてください。
「証明書のインポートウィザードの完了」が表示されます。
10. [完了] をクリックしてください。
セキュリティ警告ダイアログが表示されます。
11. [はい] をクリックしてください。
証明書のインポートウィザードダイアログが表示され、証明書のインポートが完了します。

■ Windows 更新プログラムのインストール

Windows 更新プログラムをダウンロードし、適用してください。

参照

Windows 更新プログラムのダウンロードについては、以下を参照してください。

「● Windows 更新プログラムのダウンロード (Windows 7 または Windows Server 2008 R2)」ページ
B1-4

B4.3 ネットワークの設定をする

制御バスを使用するには、制御バスドライバをインストールしてください。制御バスとして Vnet/IP を使用する場合は、Vnet/IP オープン通信ドライバもインストールしてください。

ここでは、制御バスドライバと Vnet/IP オープン通信ドライバのインストールについて説明します。

コンピュータ付属の Ethernet、または市販の Ethernet 通信カードを使用する場合は、付属のマニュアルを参照し、必要に応じて適切な Ethernet ドライバをインストールしてください。

仮想マシンの場合、Vnet/IP インタフェースパッケージがインストールされます。また、Vnet/IP オープン通信ドライバは、インストールしないでください。

B4.3.1 制御バスドライバのインストールをする

制御バスドライバのインストール手順は、Windows 10、Windows 7、Windows Server 2016、Windows Server 2012 R2、Windows Server 2008 R2 で基本的に共通です。ここでは、Windows 10 の手順を例にして、制御バスドライバのインストール方法について説明します。

■ インストール時の注意事項

制御バスにつながるコンピュータには、制御バスインターフェースカードまたは Vnet/IP インタフェースカードを実装してください。また、コンピュータには必ず制御バスドライバをインストールしてください。ドライバインストール時の注意事項を次に示します。

- ・ 制御バスドライバをインストールする前に、必ず、制御バスインターフェースカードまたは Vnet/IP インタフェースカードを実装してください。
ただし、テスト機能を使用するときは、これらのカードを実装していない場合でも、制御バスドライバをインストールしてください。この際に指定する各コンピュータの制御バスドライバの IP アドレスは、制御バスのアドレスである「ドメイン番号.ステーション番号」と同じものを設定し、さらに、拡張テスト機能を使用する場合には、接続するコンピュータの制御バスのアドレスが重複しないようにしてください。
- ・ Windows 10 の場合、制御バスドライバをインストールする前に、必ず、高速スタートアップが停止されていることを確認してください。停止されていない場合は、高速スタートアップを停止して、コンピュータを再起動してください。
- ・ 間違って、制御バスインターフェースカードまたは Vnet/IP インタフェースカードが実装されていない状態で制御バスドライバをインストールした場合、ドライバをアンインストールしてください。その後、カードを実装して、再度、ドライバをインストールしてください。
- ・ 制御バスインターフェースカードまたは Vnet/IP インタフェースカードの実装スロットを変更する場合、制御バスドライバをアンインストールしてから、実装スロットを変更してください。実装スロットを変更したあと、再度、ドライバをインストールしてください。
- ・ 制御バスインターフェースカードまたは Vnet/IP インタフェースカードを実装した状態で制御バスドライバをインストールしたあと、カードをコンピュータから外すときは、スロットから取り外す前にドライバをアンインストールしてください。

補足

- ・ 制御バスドライバをインストールする場合、コンピュータの再起動は基本的に不要ですが、インストール完了のダイアログ（要再起動）が表示されることがあります。その場合は、コンピュータを再起動してください。
- ・ 制御バスドライバをインストールしたあと、ネットワークの設定をしてください。
- ・ 制御バスドライバのインストール時に、制御バスインターフェースカードまたは Vnet/IP インタフェースカードが実装されていない場合は、カードなし用の制御バスドライバがインストールされます。カードを実装せずに FCS シミュレータを動作させる場合にこのドライバが使用されます。
- ・ カードなし用の制御バスドライバがインストールされたコンピュータを実運転で使用する場合は、制御バスドライバをアンインストールしたあと、制御バスインターフェースカードまたは Vnet/IP インタフェースカードを実装して、再度、制御バスドライバをインストールしてください。
- ・ コンピュータ切替型 UGS には、Vnet/IP インタフェースカードは不要です。ただし、専用のコンピュータを用意する必要があります。この場合も制御バスドライバをインストールしてください。

参照

Windows 10 で、高速スタートアップを停止する手順については、以下を参照してください。

「■ 高速スタートアップの停止」ページ B4-9

■ インストール手順

補足

制御バスドライバをインストールする前に他のデバイスの追加・削除を行うと、コンピュータの再起動を要求するメッセージが表示されることがあります。その場合は必ずコンピュータを再起動してください。

1. 管理者ユーザでログオンしてください。
2. CENTUM VP のソフトウェアメディアをドライブに挿入してください。
 - 自動再生ダイアログが表示された場合、[Launcher.exe の実行] をクリックしてください。
 - 自動再生ダイアログが表示されない場合、エクスプローラで CENTUM VP のソフトウェアメディアのトップフォルダにある Launcher.exe をダブルクリックしてください。
- インストールメニューが表示されます。
3. インストールメニューの [制御バスドライバ] をクリックしてください。Setup を確認するダイアログが表示されます。
4. [INSTALL] を選択して [OK] をクリックしてください。Setup の実行を確認するダイアログが表示されます。
5. [OK] をクリックしてください。

補足

- Windows セキュリティダイアログが表示された場合は、["Yokogawa Electric Corporation"からのソフトウェアを常に信頼する] チェックボックスをオンにして、[インストール] をクリックしてください。
- Windows セキュリティダイアログの [インストールしない] は、クリックしないでください。クリックすると、エラーが発生します。

6. インストール完了のダイアログが表示されたら、[OK] をクリックしてください。

B4.3.2 Vnet/IP オープン通信ドライバのインストールをする

制御バスとして Vnet/IP を使用する場合は、Vnet/IP オープン通信ドライバのインストールが必要です。さらに Ethernet を使用する場合は、Vnet/IP オープン通信ドライバを無効にします。

Vnet/IP オープン通信ドライバのインストール手順は、Windows 10、Windows 7、Windows Server 2016、Windows Server 2012 R2、Windows Server 2008 R2 で基本的に共通です。ここでは、Windows 10 の手順を例にして、Vnet/IP オープン通信ドライバのインストール方法について説明します。

コンピュータ切替型 UGS には、Vnet/IP オープン通信ドライバはインストールしないでください。

重要

Vnet/IP インタフェースカードが実装されている場合、Vnet/IP オープン通信を使用しなくても、Vnet/IP オープン通信ドライバのインストールを行う必要があります。

■ インストール時の注意事項

- Vnet/IP オープン通信ドライバをインストールする前に、必ず、Vnet/IP インタフェースカードを実装してください。カードが実装されていないと、インストールできません。
- Windows 10 の場合、Vnet/IP オープン通信ドライバをインストールする前に、必ず、高速スタートアップが停止されていることを確認してください。停止されていない場合は、高速スタートアップを停止して、コンピュータを再起動してください。
- Vnet/IP インタフェースカードの実装スロットを変更する場合、Vnet/IP オープン通信ドライバと制御バスドライバをアンインストールしてから、実装スロットを変更してください。実装スロットを変更したあと、再度、Vnet/IP オープン通信ドライバと制御バスドライバをインストールしてください。
- Vnet/IP オープン通信ドライバをインストールしたあと、Vnet/IP インタフェースカードをコンピュータから外すときは、スロットから取り外す前に Vnet/IP オープン通信ドライバをアンインストールしてください。

補足

- Vnet/IP オープン通信ドライバをインストールする場合、コンピュータの再起動は基本的に不要ですが、インストール完了のダイアログ（要再起動）が表示されたときは、コンピュータを再起動してください。
- Vnet/IP オープン通信ドライバをインストールしたあと、ネットワークの設定をしてください。

参照

Windows 10 で、高速スタートアップを停止する手順については、以下を参照してください。

「■ 高速スタートアップの停止」ページ B4-9

■ インストール手順

補足

Vnet/IP オープン通信ドライバをインストールする前に他のデバイスの追加・削除を行うと、コンピュータの再起動を要求するメッセージが表示されることがあります。その場合は必ずコンピュータを再起動してください。

1. 管理者ユーザでログオンしてください。
2. CENTUM VP のソフトウェアメディアをドライブに挿入してください。
 - 自動再生ダイアログが表示された場合、[Launcher.exe の実行] をクリックしてください。

- ・ 自動再生ダイアログが表示されない場合、エクスプローラで CENTUM VP のソフトウェアメディアのトップフォルダにある Launcher.exe をダブルクリックしてください。
- インストールメニューが表示されます。
3. インストールメニューの [Vnet/IP オープン通信ドライバ] をクリックしてください。Setup を確認するダイアログが表示されます。
 4. [INSTALL] を選択して [OK] をクリックしてください。
Setup の実行を確認するダイアログが表示されます。
 5. [OK] をクリックしてください。

補足

- ・ Windows セキュリティダイアログが表示された場合は、["Yokogawa Electric Corporation"からのソフトウェアを常に信頼する] チェックボックスをオンにして、[インストール] をクリックしてください。
- ・ Windows セキュリティダイアログの [インストールしない] は、クリックしないでください。クリックすると、エラーが発生します。

-
6. インストール完了のダイアログが表示されたら、[OK] をクリックしてください。

B4.3.3 仮想マシンに Vnet/IP インタフェースパッケージをインストールする

仮想化プラットフォームを使用するときは、Vnet/IP インタフェースパッケージを仮想マシンにインストールする必要があります。

Vnet/IP インタフェースパッケージをインストールするときは、次の手順に従ってください。

重要

- ・ 仮想化ホストコンピュータに Vnet/IP インタフェースカードを実装する必要はありません。
- ・ Vnet/IP インタフェースパッケージをインストールしたあと、仮想マシン上の Windows ネットワークの設定をしてください。

参照

仮想化については、以下を参照してください。

- ・ 仮想化プラットフォームセットアップ(IM 30A05B20-01JA)
- ・ 仮想化プラットフォーム計画・実装ガイド(TI 30A05B10-01JA)

■ Vnet/IP インタフェースパッケージをインストールするときの注意事項

Vnet/IP インタフェースパッケージをインストールするときは、次の事項に注意してください。

● 初回インストールするときの注意事項

IT セキュリティを適用する前に、Vnet/IP インタフェースパッケージをインストールしてください。IT セキュリティを適用したあとに、Vnet/IP インタフェースパッケージを初回インストールした場合は、再度 IT セキュリティを適用してください。

補足

IT セキュリティ適用後は、Vnet/IP インタフェースパッケージを再インストールしても、IT セキュリティを再適用する必要はありません。

● 再インストールするときの注意事項

Vnet/IP インタフェースパッケージを再インストールした場合、Vnet/IP インタフェースパッケージの実行ユーザのパスワードがリセットされます。パスワードを変更している場合は、再度設定してください。

■ 事前準備

次に示す Windows 更新プログラムをダウンロードし、適用してください。適用しない場合は、Windows 更新プログラムのインストールに失敗します。

- ・ 2019 年 2 月のサービススタック更新プログラム

さらに、次に示す Windows 更新プログラムをダウンロードし、適用してください。適用しない場合は、RIP Listener におけるシステムログ収集でエラーログが起ります。

- ・ 2019 年 3 月の累積的な更新プログラム

補足

本情報は、2019 年 3 月時点のものです。最新情報は、エンドポイントセキュリティ対策サービスとして提供しています。エンドポイントセキュリティ対策サービスについては、当社にお問い合わせください。

■ 手順 1：RIP Listener サービスを有効化する

Windows Server 2016 では、RIP Listener サービスがデフォルトで無効化されているため、RIP Listener サービスを有効化する必要があります。RIP Listener サービスを有効化するときは、次の手順に従ってください。

1. 仮想マシンのゲスト OS に、管理者ユーザでサインインしてください。
2. [コマンドプロンプト] を右クリックし、[管理者として実行] を選択してください。
3. 次のコマンドを実行してください。

```
dism /online /enable-feature /featurename:rasrip /all
```
4. [操作は正常に完了しました。] と表示されることを確認してください。
5. RIP Listener サービスが有効化されていることを次の手順で確認してください。
 - a. コントロールパネルを起動してください。
 - b. [システムとセキュリティ] – [管理ツール] – [サービス] を選択してください。
 サービスウィンドウが表示されます。
 - c. [RIP Listener] が存在し、その [スタートアップの種類] が [自動] になっていることを確認してください。

補足

DCOM の既定の認証レベルが「なし」の設定状態では、RIP Listener サービスを有効化できません。

参照

DCOM の既定の認証レベルを接続にする手順については、以下を参照してください。

「C10.1.2 サーバーマネージャーの起動時にエラーが発生する」ページ C10-4

■ 手順 2：Vnet/IP インタフェースパッケージをインストールする

Vnet/IP インタフェースパッケージをインストールするときは、次の手順に従ってください。

補足

Vnet/IP インタフェースパッケージをインストールする前に他のデバイスの追加や削除をすると、仮想マシンの再起動を要求するメッセージが表示されることがあります。その場合は必ず仮想マシンを再起動してください。

1. 仮想化ホストコンピュータのホスト OS に、管理者ユーザでサインインしてください。
2. CENTUM VP ソフトウェアメディアの ISO 形式ファイルを、仮想化ホストコンピュータのホスト OS 内の任意のフォルダにコピーしてください。
3. スタートメニューから、[サーバーマネージャー] を選択してください。
 サーバーマネージャーが起動します。
4. サーバーマネージャーのメニューバーから、[ツール] – [Hyper-V マネージャー] を選択してください。
 Hyper-V マネージャーが起動します。
5. Hyper-V マネージャーの左ペインで仮想化ホストコンピュータを選択してください。
 中央ペインに選択した仮想化ホストコンピュータ上の仮想マシンが表示されます。該当の仮想マシンを選択して、右クリックメニューで [接続] を選択してください。
 仮想マシン接続ウィンドウが表示されます。

補足

仮想マシン接続ウィンドウが全画面表示される場合があります。全画面表示されたときは、[元に戻す] をクリックして、全画面表示を解除してください。

6. 仮想マシン接続ウィンドウのメニューバーから、[メディア] – [DVD ドライブ] – [ディスクの挿入] を選択してください。
ファイルを開くダイアログが表示されます。
7. コピーした CENTUM VP ソフトウェアメディアの ISO 形式ファイルを指定してください。
選択した ISO 形式ファイルが仮想マシンにマウントされます。
 - ・ 自動再生ダイアログが表示された場合、[Launcher.exe の実行] をクリックしてください。
 - ・ 自動再生ダイアログが表示されない場合、エクスプローラで CENTUM VP のソフトウェアの ISO 形式ファイルが格納されているフォルダ下にある Launcher.exe をダブルクリックしてください。
 インストールメニューが表示されます。
8. インストールメニューの [制御バスドライバ] を選択してください。
Setup を確認するダイアログが表示されます。
9. [INSTALL] を選択して [OK] をクリックしてください。
Setup の実行を確認するダイアログが表示されます。
10. [OK] をクリックしてください。

補足

- ・ Windows セキュリティダイアログが表示された場合は、["Yokogawa Electric Corporation"からのソフトウェアを常に信頼する] チェックボックスをオンにして、[インストール] をクリックしてください。
- ・ Windows セキュリティダイアログの [インストールしない] は、クリックしないでください。クリックすると、エラーが発生します。

11. インストール完了のダイアログが表示されたら、[OK] をクリックしてください。

■ 手順 3：Vnet/IP インタフェースパッケージが管理するドメイン番号とステーション番号を設定する

Vnet/IP インタフェースパッケージのインストールが完了すると、Vnet/IP インタフェース管理ツールが表示されます。この Vnet/IP インタフェース管理ツールを使用して、Vnet/IP インタフェースパッケージが管理するドメイン番号とステーション番号を設定します。ドメイン番号とステーション番号を設定するときは、次の手順に従ってください。

補足

Vnet/IP インタフェースパッケージが管理しているドメイン番号とステーション番号は、あとで設定することもできます。ただし、設定を反映するには、仮想マシンの再起動が必要となります。

1. Vnet/IP インタフェース管理ツールの [Settings] タブを開いてください。
2. [Domain No] にドメイン番号を、[Station No] にステーション番号を入力して、[Save] ボタンをクリックしてください。

補足

ドメイン番号には 1 から 31 までの番号を、ステーション番号には 1 から 64 までの番号を設定できます。
拡張テスト機能パッケージ、FCS シミュレータパッケージをインストールして、他の HIS からリモート接続可能な FCS シミュレータを動作させる仮想マシンでは、ドメイン番号とステーション番号に、両方とも 0 を設定してください。
なお、ドメイン番号とステーション番号を 0 に設定し、テスト機能のみを使用する場合は、Vnet/IP インタフェースパッケージのライセンスは不要となります。

3. [CLOSE] ボタンをクリックして、仮想マシンを再起動してください。

参照

Vnet/IP インタフェース管理ツールについては、以下を参照してください。

「Appendix 2. Vnet/IP インタフェース管理ツール」ページ App.2-1

■ 手順 4：Vnet/IP インタフェースパッケージのライセンスを有効化する

Vnet/IP インタフェースパッケージを使用するためには、Vnet/IP インタフェースパッケージのライセンスを有効化する必要があります。CENTUM VP をインストールしたあとに、Vnet/IP インタフェースパッケージのライセンスの配布と反映をしてください。

B4.3.4 Windows ネットワークの設定をする

ネットワークドライバのインストール後、Windows ネットワークの設定が必要です。

ここでは、制御バス、Vnet/IP オープン通信、Ethernet、および UACS 専用 Ethernet の Windows ネットワークの設定について、Windows 7/Windows Server 2008 R2 での設定を基本として説明し、その他の OS については補足などで説明を加えていきます。

補足

コンピュータ切替型 UGS の場合は、「■手順 1:ローカルエリア接続の名称変更」から読んでください。

■ ケーブル配線の際の注意事項

ネットワーク接続の際、ケーブル配線したときに、ネットワークの場所の設定ダイアログが表示されることがあります。

補足

Windows 10 と Windows Server 2016 の場合は、ネットワークチャームバーが表示されることがあります。

参照

ネットワークの場所の設定ダイアログ、およびネットワークチャームバーについては、以下を参照してください。

「C10.2.1 ネットワークケーブル配線時の注意事項」ページ C10-15

■ 制御バス用のカードの確認

コンピュータに実装されている制御バス用のカードを確認してください。

● 制御バスインターフェースカードの場合

V ネットを使用したシステムでは、コンピュータに制御バスインターフェースカードを実装しています。この場合、制御バス通信と Ethernet 通信を使用するための Windows のネットワーク設定をしてください。

● Vnet/IP インタフェースカードの場合

Vnet/IP を使用したシステムでは、コンピュータに Vnet/IP インタフェースカードを実装しています。この場合、制御バス通信と Ethernet 通信、または制御バス通信と Vnet/IP オープン通信を組み合わせて使用します。使用するネットワーク構成に合わせて、必要な Windows のネットワーク設定をしてください。

補足

Vnet/IP のバス 2 で行う Ethernet 通信を Vnet/IP オープン通信と呼びます。

Vnet/IP オープン通信を使用するシステムでは、通常はバス 1 で制御バス通信を行い、バス 2 で Ethernet 通信を行います。バス 1 異常時は、バス 2 で制御バス通信と Ethernet 通信を行います。

■ Vnet/IP 使用時のネットワーク構成と Windows のネットワーク設定

Vnet/IP のネットワーク構成と、必要な Windows のネットワーク設定を示します。

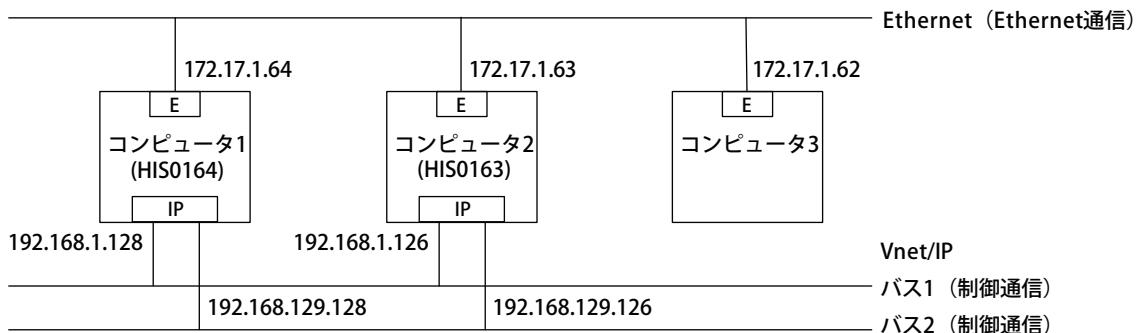


図 B4.3.4-1 ネットワーク構成とインターフェース（Vnet/IP と Ethernet を敷設する場合）

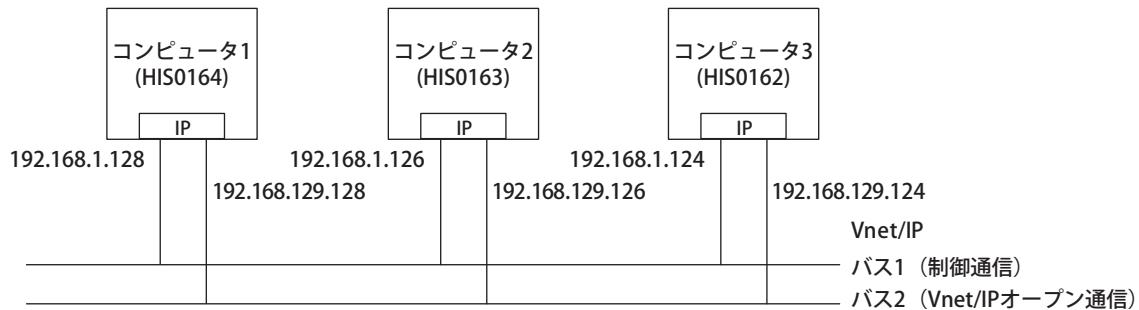


図 B4.3.4-2 ネットワーク構成とインターフェース（Vnet/IP のみ敷設する場合）

表 B4.3.4-1 ネットワーク構成と Windows で設定するネットワーク接続

ネットワーク構成	コンピュータ（図の例）	Windows で設定するネットワーク接続
Vnet/IP+Ethernet	Vnet/IP と Ethernet に接続（コンピュータ 1、コンピュータ 2）	制御バス通信、Ethernet 通信、Vnet/IP オープン通信(*1)
	Ethernet のみに接続（コンピュータ 3）	Ethernet 通信
Vnet/IP のみ	Vnet/IP に接続（バス 2 で Ethernet 通信を行う）（コンピュータ 1～コンピュータ 3）	制御バス通信、Vnet/IP オープン通信、Ethernet 通信(*2)

*1: Vnet/IP オープン通信ドライバをインストール後、デバイスを無効に設定します。

*2: Ethernet デバイスを無効に設定します。

■ Vnet/IP を使用する場合の注意事項

Vnet/IP のコンピュータでは、ネットワーク構成に合わせ、使用しないデバイスを無効にしてください。

● Vnet/IP と Ethernet を敷設する場合

重要 Vnet/IP と Ethernet を併用するシステムでは、Vnet/IP オープン通信を使用しません。この場合でも、Vnet/IP インターフェースカードを実装したコンピュータには Vnet/IP オープン通信ドライバをインストールし、ドライバを無効にする必要があります。

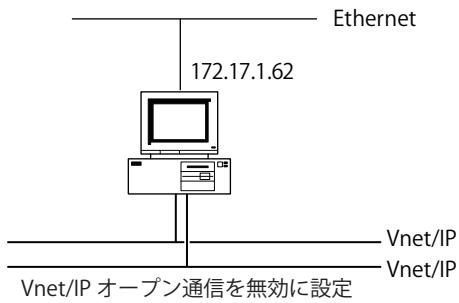


図 B4.3.4-3 Vnet/IP と Ethernet を敷設する場合

Vnet/IP インタフェースカードを実装したコンピュータでは、次の手順で Vnet/IP オープン通信ドライバを無効にしてください。

1. 管理者ユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [システム] – [デバイスマネージャー] を選択してください。
デバイスマネージャーが表示されます。
4. [ネットワークアダプタ] を表示してください。
5. [Vnet/IP Open Communication Driver (BUS2)] を選択し、ツールバーの無効ボタンをクリックしてください。

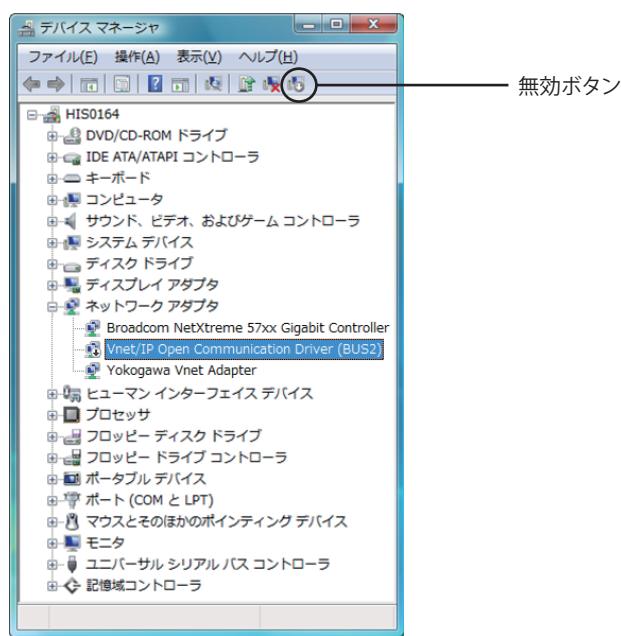


図 B4.3.4-4 Vnet/IP オープン通信ドライバの無効設定

● Vnet/IP のみ敷設する場合

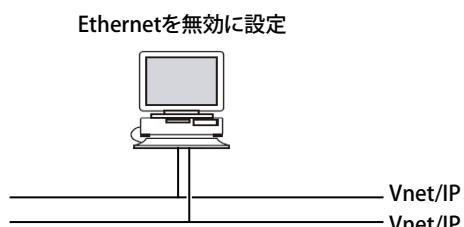


図 B4.3.4-5 Vnet/IP のみ敷設する場合

Vnet/IP のみ敷設するシステムのコンピュータでは、次の手段で Ethernet デバイスを無効にしてください。

1. 管理者ユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [システム] – [デバイスマネージャー] を選択してください。
デバイスマネージャーが表示されます。
4. [ネットワークアダプタ] を表示してください。
5. Ethernet デバイスを選択し、ツールバーの無効ボタンをクリックしてください。

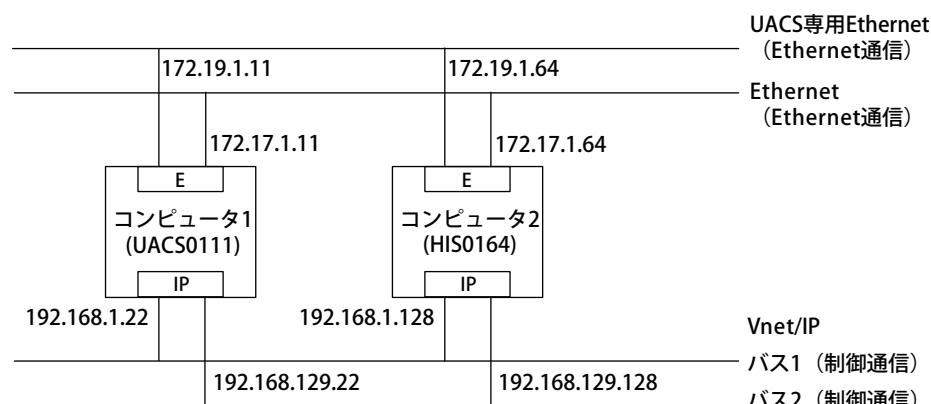
参照

Vnet/IP のバス 2 で Ethernet 通信を行える条件については、以下を参照してください。

統合生産制御システム CENTUM VP システム仕様書 (GS 33J01A10-01JA) の「■ ネットワーク仕様」の「● Ethernet」

■ UACS 専用 Ethernet を使用するときのネットワーク構成と Windows のネットワーク設定

UACS 専用 Ethernet を使用するときのネットワーク構成と、必要な Windows のネットワーク設定を示します。



E : Ethernetインターフェースカード、またはオンボードNIC

IP : Vnet/IPインターフェースカード

図 B4.3.4-6 ネットワーク構成とインターフェース

表 B4.3.4-2 ネットワーク構成と Windows で設定するネットワーク接続

コンピュータ（図の例）	Windows で設定するネットワーク接続
Vnet/IP と Ethernet と UACS 専用 Ethernet に接続（コンピュータ 1、コンピュータ 2）	制御バス通信、Ethernet 通信、Vnet/IP オープン通信 (*1)、UACS 専用 Ethernet 通信

*1: Vnet/IP オープン通信ドライバをインストール後、デバイスを無効に設定します。

■ 禁止事項

CENTUM VP では、次の機能を使用しないでください。

- ・ インターネット接続の共有 (ICS)
- ・ ブリッジ接続
- ・ ホームグループ

● インターネット接続の共有 (ICS)

Vnet、Ethernet、および VnetIPOpen（後述の手順で名称を設定する）のプロパティダイアログの共有タブにある [ネットワークのほかのユーザに、このコンピュータのインターネット接続をおしての接続を許可する] チェックボックスをオンにしないでください。

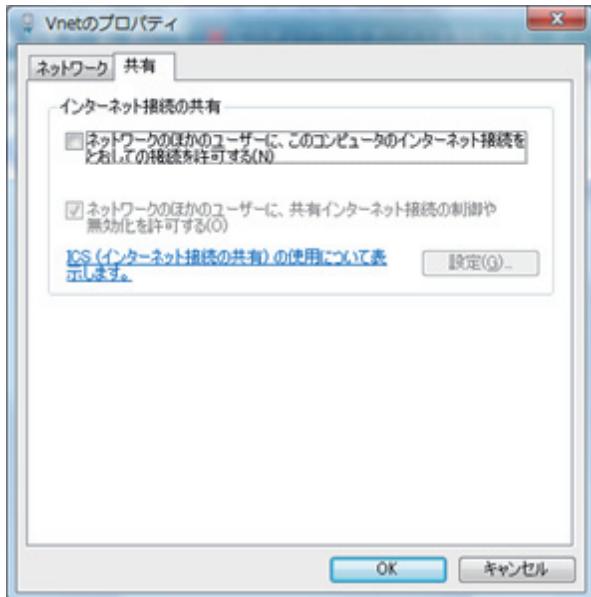


図 B4.3.4-7 Vnet のプロパティダイアログ（デフォルト）

補足

インターネット接続の共有 (ICS) は、1つのインターネット接続を家庭あるいは小規模オフィスネットワーク内のコンピュータ全体で共有させることが目的です。

● ブリッジ接続

ブリッジ接続は使用しないでください。ブリッジ接続を作成すると、ブリッジ接続を作成したコンピュータから制御バス通信ができないばかりか、制御バス通信全体が阻害される恐れがあります。万一作成した場合は削除してください。



図 B4.3.4-8 ネットワーク接続の禁止例（ブリッジを有効にした場合）

● ホームグループ（Windows 10、または Windows 7）

CENTUM VP では従来どおりワークグループ・ネットワーク環境のファイル共有機能を利用して、フォルダやプリンタの共有を行います。そのため、Windows 7 では、ネットワークの場所の設定ダイアログで、[ホームネットワーク] を選択せず、[パブリックネットワーク] を選択してください。Windows 10 では、ネットワークチャームバーで、[いいえ] を選択してください。

参照

ネットワークの場所の設定ダイアログ、およびネットワークチャームバーについては、以下を参照してください。

「C10.2.1 ネットワークケーブル配線時の注意事項」ページ C10-15

■手順 1：ローカルエリア接続の名称変更

インストール後のネットワークには、「ローカルエリア接続」という名前がつきます。ローカルエリア接続の名称変更を行うことでネットワークの識別がわかりやすくなります。

使用するネットワーク構成に合わせ、該当するローカルエリア接続の名称を変更してください。

1. コントロールパネルを起動してください。
2. [ネットワークとインターネット] – [ネットワークと共有センター] を選択してください。
ネットワークと共有センターウィンドウが表示されます。
3. [アダプターの設定の変更] を選択してください。
ネットワーク接続ウィンドウが表示されます。



図 B4.3.4-9 ネットワーク接続（名称の変更前）

補足

ここに表示されていない接続は、インストールに失敗したか、ドライバが正常に動作していません。正しく接続が表示されるように対処してください。

4. すべての [ローカルエリア接続] のアイコンを右クリックして [名前の変更] を選択し、名前を変更してください。

表 B4.3.4-3 ネットワーク接続名称の変更

ネットワーク種別	「ネットワーク接続」ウィンドウ上の表示	名称
Ethernet	各種 Ethernet 用ドライバ名	Ethernet
制御バス	Yokogawa Vnet Adapter	Vnet
Vnet/IP オープン通信	Vnet/IP Open Communication Driver (BUS2)	VnetIPOpen
UACS 専用 Ethernet	各種 Ethernet 用ドライバ名	UACSEthernet



図 B4.3.4-10 ネットワーク接続－V ネットの場合（名称の変更後）



図 B4.3.4-11 ネットワーク接続－Vnet/IP の場合（名称の変更後）

● ネットワークの種別を確認する方法

ネットワークの種別を確認するときは、次の手順に従ってください。

1. ネットワーク接続ウィンドウでネットワークを右クリックし、[プロパティ] を選択してください。
2. [ネットワーク] タブを開き、[構成] ボタンをクリックしてください。
3. 詳細設定タブを開き、[プロパティ] の [Hyper-V Network Adapter Name] を選択して、表示された [値] を確認してください。
仮想マシンを構築したときに設定したデバイス名が表示されます。

補足

手順 3 で確認する [値] については、仮想マシンを構築したエンジニアに確認してください。

参照

仮想マシンのネットワークの設定については、以下を参照してください。

「B4.3.7 仮想マシンを使用する際の注意事項」ページ B4-77

■ 手順 2：プロパティの設定

ネットワーク接続ごとのプロパティ設定で、使用する項目を設定します。

システムのネットワークに構成に合わせて、該当するプロパティを設定してください。

表 B4.3.4-4 ネットワーク接続ごとの使用項目一覧

項目	使用の有無 (*1)			
	Ethernet	VnetIPOpen	Vnet	UACSEthernet
Microsoft ネットワーク用クライアント	Yes	Yes	No	No
QoS パケットスケジューラ	Yes	Yes	No	No
Microsoft ネットワーク用ファイルとプリンタ共有	Yes	Yes	No	No
Microsoft Network Adapter Multiplexor Protocol (*2)	No	No	No	No
Microsoft LLDP プロトコルドライバー (*2)	Yes	Yes	No	No

次に続く

表 B4.3.4-4 ネットワーク接続ごとの使用項目一覧（前から続く）

項目	使用の有無 (*1)			
	Ethernet	VnetIPOpen	Vnet	UACSEthernet
Yokogawa Vnet Protocol	No	No	Yes	No
インターネットプロトコルバージョン 6 (TCP/IPv6)	No	No	No	No
インターネットプロトコルバージョン 4 (TCP/IPv4)	Yes	Yes	Yes (*3)	Yes
Link-Layer Topology Discovery Mapper I/O Driver	Yes	Yes	No	No
Link-Layer Topology Discovery Responder	Yes	Yes	No	No

*1: Yes:チェックボックスを選択
No:チェックボックスをクリア

*2: Windows 10 と Windows Server 2016 のみ

*3: コンピュータ切替型 UGS 用のコンピュータの場合は、[インターネットプロトコルバージョン 4 (TCP/IPv4)] を選択しないでください。

補足

表中の「Yokogawa Vnet Protocol」以外は、Windows で標準インストールされているものです。

参照

仮想マシンのネットワークアダプタの設定については、以下を参照してください。

「B4.3.7 仮想マシンを使用する際の注意事項」ページ B4-77

コンピュータ切替型 UGS 固有ネットワークの設定については、以下を参照してください。

「■ コンピュータ切替型 UGS 固有のネットワークの設定」ページ B4-74

● Vnet のプロパティ

- ネットワーク接続ウィンドウで [Vnet] を右クリックし、[プロパティ] を選択してください。
Vnet のプロパティウィンドウが表示されます。

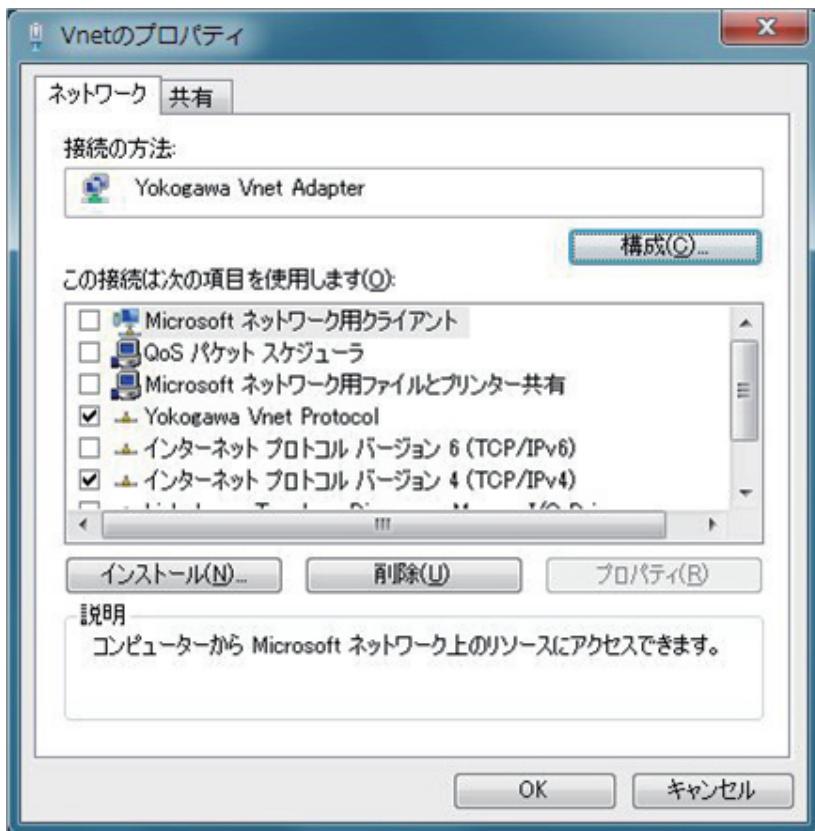


図 B4.3.4-12 Vnet のプロパティウィンドウ

- 「表 ネットワーク接続ごとの使用項目一覧」のとおり [Yokogawa Vnet Protocol] と [インターネットプロトコルバージョン 4 (TCP/IPv4)] のみチェックしてください。

重要

コンピュータ切替型 UGS 用のコンピュータの場合は、[インターネットプロトコルバージョン 4 (TCP/IPv4)] をチェックしないで、[Yokogawa Vnet Protocol] のみチェックしてください。

- 設定後、[OK] をクリックしてください。

● VnetIPOpen のプロパティ

- ネットワーク接続ウィンドウで [VnetIPOpen] を右クリックし、[プロパティ] を選択してください。
VnetIPOpen のプロパティウィンドウが表示されます。

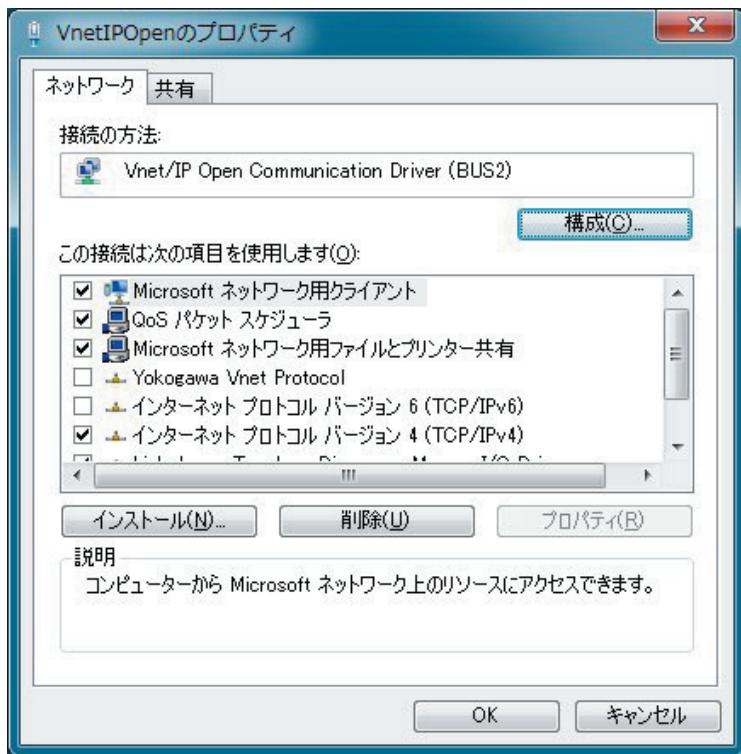


図 B4.3.4-13 VnetIPOpen のプロパティウィンドウ

2. 「表ネットワーク接続ごとの使用項目一覧」のとおり、[Yokogawa Vnet Protocol] と [インターネットプロトコルバージョン 6 (TCP/IPv6)] のチェックボックスをオフにしてください。
3. 設定後、[OK] をクリックしてください。

● Ethernet のプロパティ

1. ネットワーク接続ウィンドウで [Ethernet] を右クリックし、[プロパティ] を選択してください。
Ethernet のプロパティウィンドウが表示されます。

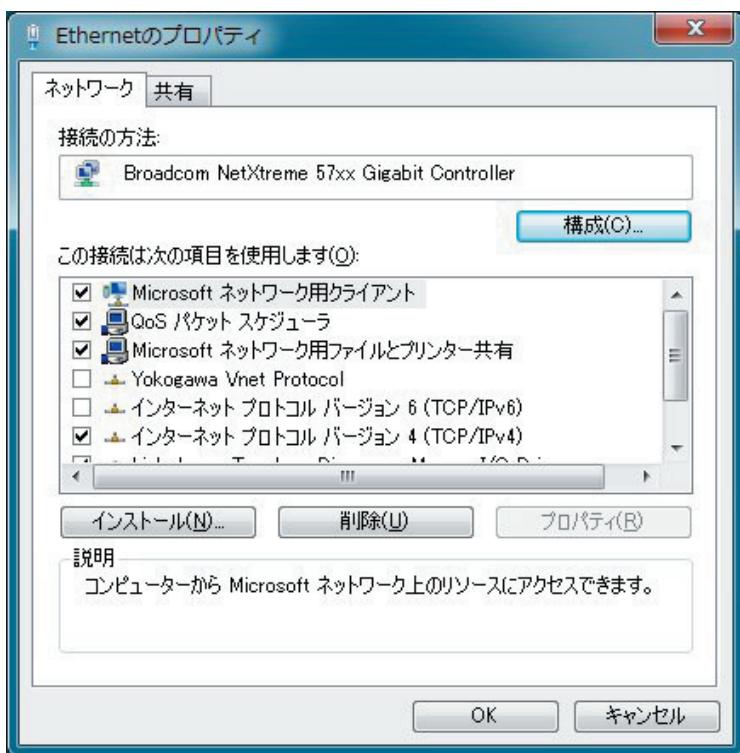


図 B4.3.4-14 Ethernet のプロパティウィンドウ

2. 「表 ネットワーク接続ごとの使用項目一覧」のとおり、[Yokogawa Vnet Protocol] と [インターネットプロトコルバージョン 6 (TCP/IPv6)] のチェックボックスをオフにしてください。
3. 設定後、[OK] をクリックしてください。

補足

コンピュータ切替型 UGS では、Ethernet のプロパティで、インターフェイスメトリックの設定も必要です。また、Windows 10 または Windows Server 2016 のコンピュータに、システム統合 OPC 機能に関連するソフトウェアをインストールする場合も、Ethernet のプロパティでインターフェイスメトリックの設定が必要です。

参照

インターフェイスメトリックの設定方法については、以下を参照してください。

「■ インターフェイスメトリックの設定」ページ B4-75

● UACSEthernet のプロパティ

1. ネットワーク接続ウィンドウで [UACSEthernet] を右クリックし、[プロパティ] を選択してください。
UACSEthernet のプロパティウィンドウが表示されます。
2. 「表 ネットワーク接続ごとの使用項目一覧」のとおり、[インターネットプロトコルバージョン 4 (TCP/IPv4)] チェックボックスを選択し、それ以外のチェックボックスをクリアしてください。
3. 次の手順に従ってインターフェイスメトリックを設定してください。
 - a. [インターネットプロトコルバージョン 4 (TCP/IPv4)] を選択して、[プロパティ] をクリックしてください。
インターネットプロトコルバージョン 4 (TCP/IPv4) のプロパティダイアログが表示されます。
 - b. [全般] タブをクリックしてください。
 - c. [詳細設定] をクリックしてください。

- TCP/IP 詳細設定ダイアログが表示されます。
- d. [IP 設定] タブをクリックしてください。
 - e. [自動メトリック] チェックボックスをクリアして、[インターフェイスメトリック] ボックスに 9999 を入力してください。
 - f. [OK] をクリックしてください。
4. [OK] をクリックしてください。

■ 手順 3：IP アドレスの設定

Windows では、ネットワークドライバをインストールすると、DHCP の使用がデフォルトで有効になります。しかし、CENTUM VP では DHCP を使用しないので、IP アドレスを設定します。ドメイン環境で使用する場合でも同様です。システムのネットワーク構成に合わせて、該当する IP アドレスを設定してください。

● Vnet の IP アドレス

重要

コンピュータ切替型 UGS では、本設定は不要です。

1. ネットワーク接続ウィンドウで Vnet のアイコンを右クリックし、[プロパティ] をクリックしてください。
Vnet のプロパティダイアログが表示されます。
2. [インターネット プロトコル バージョン 4 (TCP/IPv4)] を選択して [プロパティ] をクリックしてください。
インターネット プロトコル バージョン 4 (TCP/IPv4) のプロパティダイアログが表示されます。
3. [次の IP アドレスを使う] を選択し、IP アドレス、サブネットマスク、デフォルトゲートウェイを設定してください。通常は、ステーションアドレスによって決まる標準の値を設定してください。

補足

Vnet の標準の値を示します。

IP アドレス : 172.16. ドメイン番号.ステーション番号(*1)

サブネットマスク : 255.255.0.0

デフォルトゲートウェイ : 設定なし

*1: 既存の環境とネットワークアドレスが重複する場合、ネットワークアドレスは、172.16 以外の値を使用することもできます。

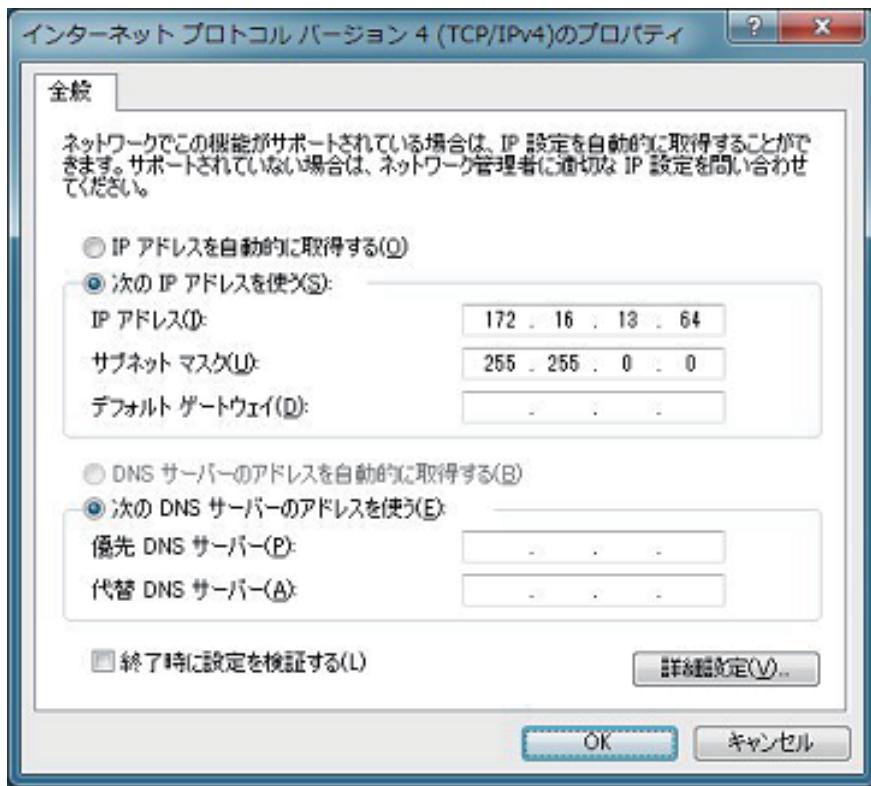


図 B4.3.4-15 IP アドレス設定例（Vnet）

4. 設定後、[OK] をクリックしてください。コンピュータの再起動は不要です。

● VnetIPOpen の IP アドレス

Vnet/IP を Ethernet と一緒に使用する場合には、この設定は不要です。

重要

コンピュータ切替型 UGS では、本設定は不要です。

- ネットワーク接続ウィンドウで VnetIPOpen のアイコンを右クリックし、[プロパティ] を選択してください。
VnetIPOpen のプロパティダイアログが表示されます。
- [インターネットプロトコルバージョン 4 (TCP/IPv4)] を選択して [プロパティ] をクリックしてください。
インターネットプロトコルバージョン 4 (TCP/IPv4) のプロパティダイアログが表示されます。
- [次の IP アドレスを使う] を選択し、IP アドレス、サブネットマスク、デフォルトゲートウェイについて次の値を設定してください。
 - 既存の環境でコンピュータを使用する場合、そのネットワーク環境で使用している値
 - 新規の環境でコンピュータを使用する場合、ステーションアドレスによって決まる標準の値

補足

VnetIPOpen のデフォルト値を示します。

IP アドレス : 192.168.<128 + ドメイン番号>.<129 + ステーション番号>(*1)

サブネットマスク : 255.255.255.0

デフォルトゲートウェイ : 他 Vnet/IP ドメインが存在する場合、L3SW の IP アドレスを設定

*1: 通常は標準の設定を使用してください。ただし、これ以外のアドレスを使用することもできます。

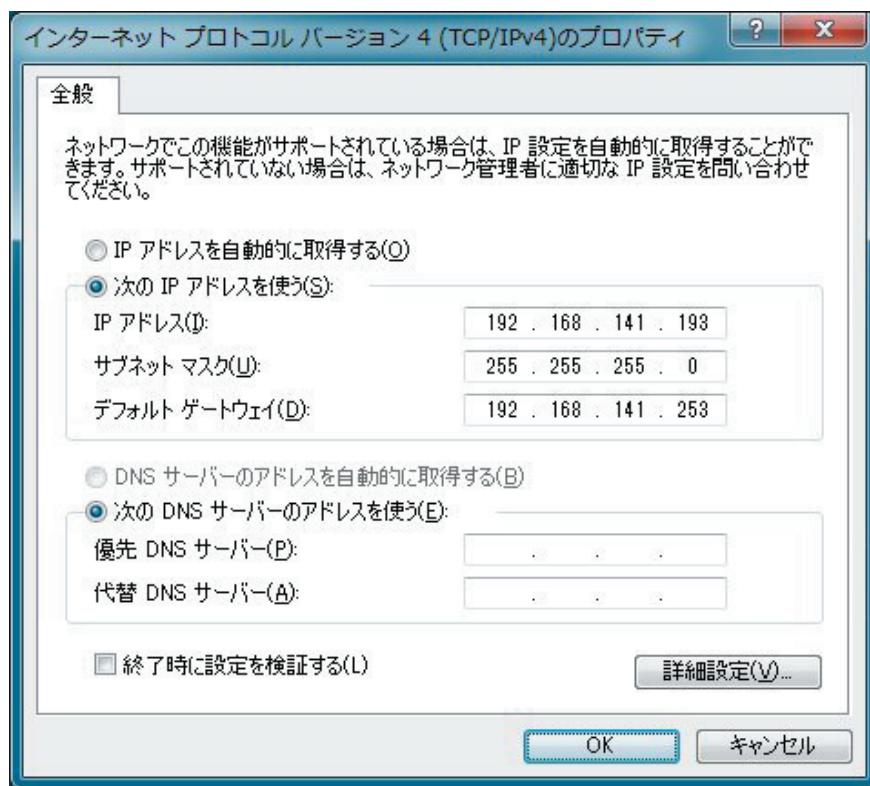


図 B4.3.4-16 IP アドレス設定例（Vnet/IP オープン通信）

4. 設定後、[OK] をクリックしてください。コンピュータの再起動は不要です。

参照

仮想マシンのネットワークの設定については、以下を参照してください。

「B4.3.7 仮想マシンを使用する際の注意事項」ページ B4-77

● Ethernet の IP アドレス

1. ネットワーク接続ウィンドウで Ethernet のアイコンを右クリックし、[プロパティ] を選択してください。
Ethernet のプロパティダイアログが表示されます。
2. [インターネットプロトコルバージョン 4 (TCP/IPv4)] を選択して [プロパティ] をクリックしてください。
インターネットプロトコルバージョン 4 (TCP/IPv4) のプロパティダイアログが表示されます。
3. [次の IP アドレスを使う] を選択し、IP アドレス、サブネットマスク、デフォルトゲートウェイについて次の値を設定してください。
 - 既存の環境でコンピュータを使用する場合、そのネットワーク環境で使用している値

- 新規の環境でコンピュータを使用する場合、ステーションアドレスによって決まる標準の値

補足

Ethernet の標準の値を示します。

IP アドレス : 172.17. ドメイン番号.ステーション番号(*1)

サブネットマスク : 255.255.0.0

デフォルトゲートウェイ : 設定なし

*1: 通常は標準の設定を使用してください。ただし、これ以外のアドレスを使用することもできます。

重要

- ワークグループ環境では、DNS サーバのアドレスと [詳細設定] から呼び出される設定は変更しないでください。
- Windows ドメイン環境では、Windows ドメインコントローラが参照する DNS サーバのアドレスを入力してください。
- コンピュータ切替型 UGS 用のコンピュータの場合は、[IP アドレスを自動的に取得する] を選択してください。DNS サーバについては、必要に応じて、IP アドレスを設定してください。

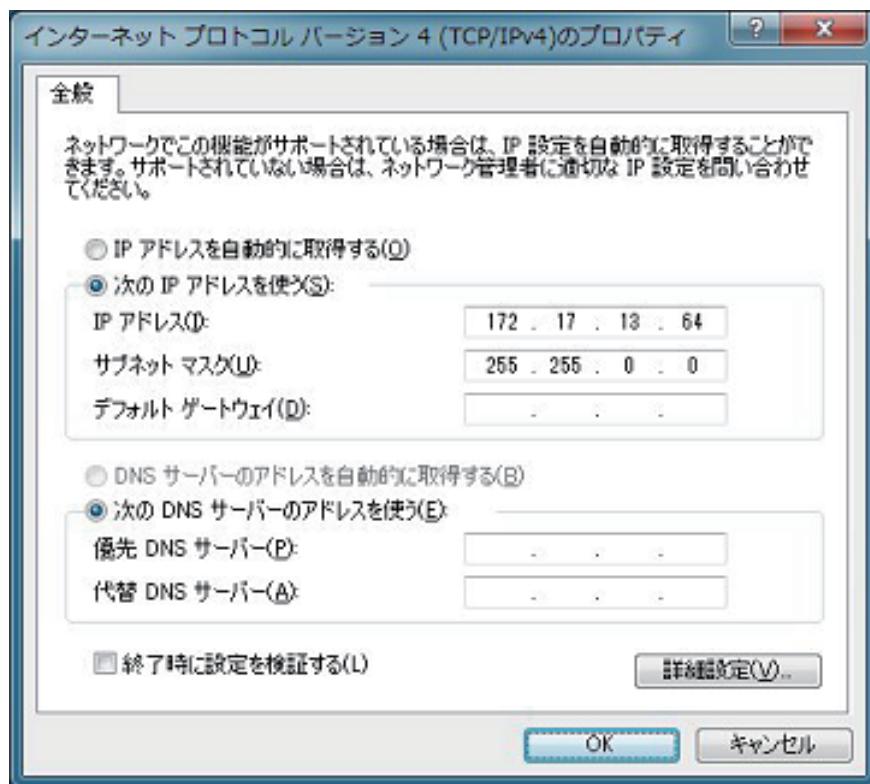


図 B4.3.4-17 IP アドレス設定例（Ethernet）

- 設定後、[OK] をクリックしてください。コンピュータの再起動は不要です。

重要

コンピュータ切替型 UGS を使用する場合は、Ethernet のネットワークアドレスに制限があります。

参照

コンピュータ切替型 UGS を使用する場合のネットワークアドレスの制限については、以下を参照してください。

PC冗長化プラットフォームはじめにお読みください (IM 30A05C10-01JA)

● デフォルトの IP アドレス以外を指定するときの注意事項

HIS にデフォルトの IP アドレス (172.17.dd.ss) 以外を指定する場合は、CENTUM VP ソフトウェアインストール後、CAMS for HIS を有効にする前に、システムビューの HIS のプロパティのネットワークタブの [Ethernet TCP/IP プロトコル] に実機 HIS の情報（ホスト名、IP アドレス、サブネットマスク）を正しく入力して、すべての HIS にプロジェクト共通部ダウンロードをしておく必要があります。

● UACSEthernet の IP アドレス

1. ネットワーク接続ウィンドウで UACSEthernet のアイコンを右クリックし、[プロパティ] を選択してください。
UACSEthernet のプロパティダイアログが表示されます。
2. [インターネットプロトコルバージョン 4 (TCP/IPv4)] を選択して [プロパティ] をクリックしてください。
インターネットプロトコルバージョン 4 (TCP/IPv4) のプロパティダイアログが表示されます。
3. [次の IP アドレスを使う] を選択し、IP アドレス、サブネットマスク、デフォルトゲートウェイについて次の値を設定してください。

IP アドレス : 172.19.ドメイン番号.ステーション番号

サブネットマスク : 255.255.0.0

デフォルトゲートウェイ : 設定なし

- DNS サーバの設定は不要です。
- 既存の環境とネットワークアドレスが重複する場合、ネットワークアドレスを、172.19 以外の値に変更してください。

4. 設定後、[OK] をクリックしてください。コンピュータの再起動は不要です。

■ 手順 4：バインドの設定

重要

Windows 10 または Windows Server 2016 の場合、本設定は不要です。

CENTUM VP では、Ethernet 通信と制御バス通信、Vnet/IP オープン通信と制御バス通信のように、ネットワークデバイスを複数使用するため、バインドの設定が必要です。使用するネットワーク構成に合わせて、該当するバインドを設定してください。

ネットワークカードの接続順位は、あとにインストールされたカードが優先されます。そのため、次の優先順位になるようにバインドの設定を変更する必要があります。

- Ethernet の順位を制御バス (Vnet) よりも高く設定してください。
- Vnet/IP オープン通信を使用する場合は、VnetIPOpen の順位を Vnet よりも高く設定してください。
- UACSEthernet の順位は、Vnet より低く設定してください。
- Vnet/IP オープン通信と Ethernet および UACSEthernet を併用する場合は、Ethernet、VnetIPOpen、Vnet、UACSEthernet の順に高く設定してください。

Ethernet と Vnet を使用する場合は、次の手順に従ってください。

1. ネットワーク接続ウィンドウの詳細設定メニューから [詳細設定] を選択してください。

詳細設定ダイアログが表示されます。

補足

詳細設定メニューが表示されないときは、Alt キーを押してください。

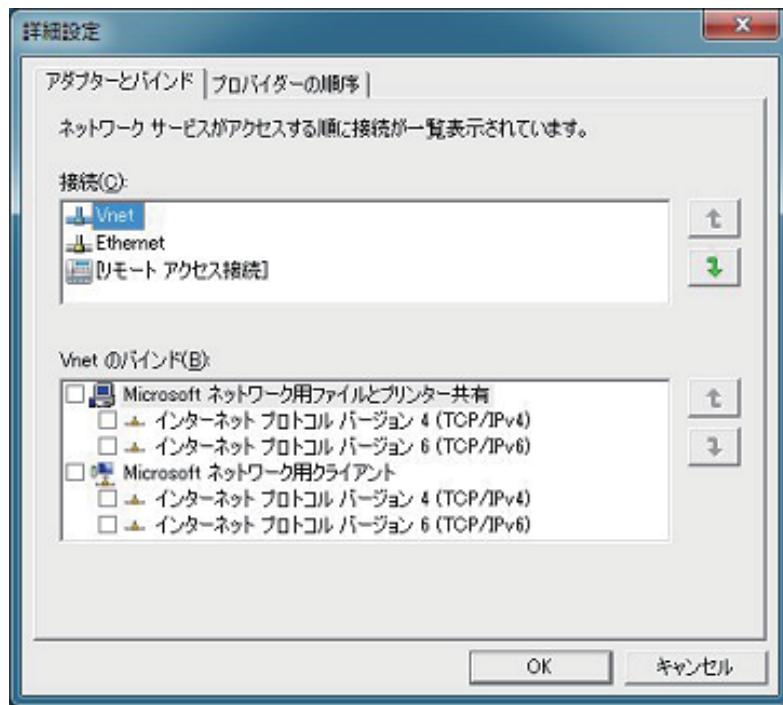


図 B4.3.4-18 詳細設定ダイアログ（バインドの設定が正しくない状態）

この図では、制御バス (Vnet) をあとからインストールしたので、制御バスが Ethernet よりも優先して接続されることになります。

2. Ethernet の順位を Vnet よりも高くするため、[接続] の右に表示されている矢印ボタンで順位を設定してください。

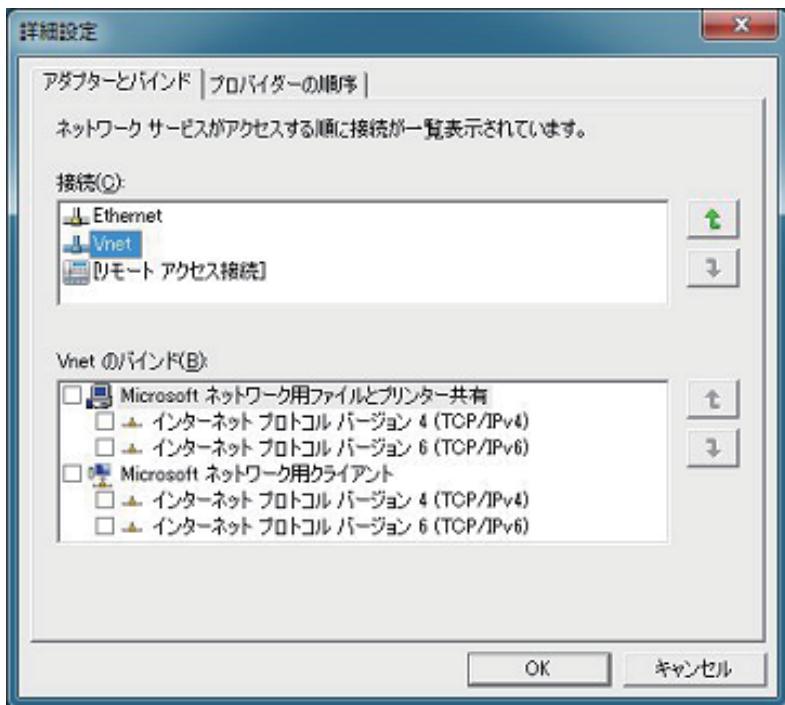


図 B4.3.4-19 詳細設定ダイアログ（バインドの順番が正しい状態）

3. [OK] をクリックしてください。
バインドの設定が終了します。

補足

バインドの設定を変更してもコンピュータの再起動は不要です。

重要

- ・[リモートアクセス接続] の順位は最低のまま変更しないでください。
- ・プロバイダーの順序タブは設定不要です。
- ・「接続」の下に表示される「Ethernet」、「Vnet」、「VnetIPOpen」、および「UACSEthernet」のバインドの設定を変更しないでください。

参照

コンピュータ切替型 UGS のバインドの優先順位については、以下を参照してください。

「■ コンピュータ切替型 UGS のバインド設定」ページ B4-74

■ 手順 5：コンピュータ名の変更

推奨する設定として、コンピュータ名と CENTUM VP システムでのステーション名同じにしてください。

1. コントロールパネルを起動してください。
2. [システムとセキュリティ] - [システム] - [システムの詳細設定] を選択してください。
システムのプロパティダイアログが表示されます。
3. コンピュータ名タブで [変更] をクリックしてください。
コンピュータ名／ドメイン名の変更ダイアログが表示されます。
4. ステーション名と同じコンピュータ名（大文字と小文字の区別はありません）を入力してください。

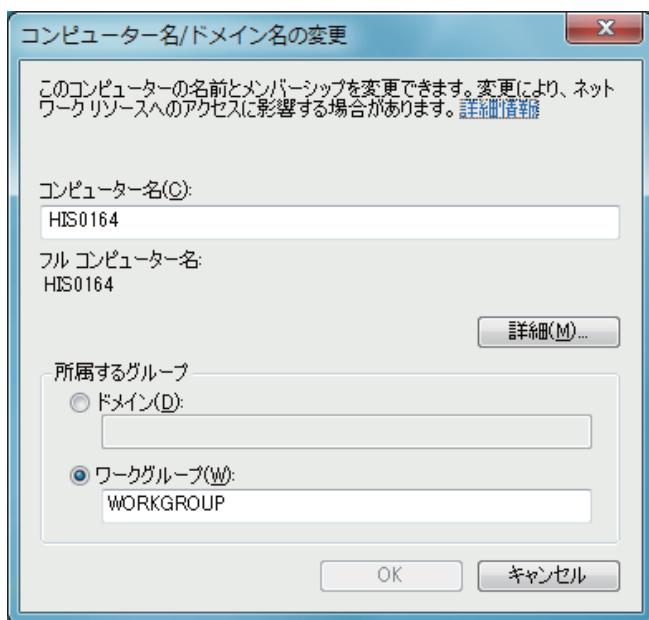


図 B4.3.4-20 コンピューター名／ドメイン名の変更ダイアログ

5. [OK] をクリックしてください。
コンピュータの再起動を促すダイアログが表示されます。
6. コンピュータを再起動してください。

重要

コンピュータ切替型 UGS の場合は、半角英数 13 文字まで。"- (ハイフン) "は使用可。
ただし、先頭文字は英文字を指定してください。
冗長化となるコンピュータに対して、同一のコンピュータ名を設定してください。

■ 手順 6：TCP/IP 設定を修復する

CENTUM VP ソフトウェアをインストールする前には、TCP/IP 設定不整合検出ツールを実行してください。不整合が検出された場合は、TCP/IP 設定不整合修復ツールを使用してください。

補足

過去に一度でも制御バスドライバまたは Vnet/IP オープン通信ドライバをアンインストールしたことがある場合、TCP/IPv4 の IP アドレス、サブネットマスク、デフォルトゲートウェイアドレスの設定がコンピュータを再起動するたびに消えてしまうことがあります。これは Windows OS の障害に起因するものです。

重要

コンピュータ切替型 UGS では、本設定は不要です。

● TCP/IP 設定不整合検出ツールの実行

1. エクスプローラで、CENTUM VP のソフトウェアメディア内の次の TOOLS フォルダを表示してください。
<CENTUM VP ソフトウェアメディアドライブ> : ¥CENTUM¥TOOLS

補足

TCP/IP 設定不整合修復ツールは、CENTUM VP をインストールすると、次のフォルダにもインストールされます。

<CENTUM VP インストール先フォルダ> ¥net¥tool

2. TcpipInconsistencyDetector.cmd を右クリックし、コンテキストメニューから [管理者として実行] を選択してください。
不整合の検出結果に応じて、メッセージが表示されます。
3. [OK] をクリックして、ツールを終了してください。
不整合が検出されない場合は、ネットワークは通常どおり使用可能です。
不整合が検出された場合、Windows は継続して動作しますが、ネットワーク接続が正しく動作しない可能性があります。TCP/IP 設定不整合修復ツールを実行し、その後 TCP/IP の設定を再度行ってください。

参照

TCP/IP 設定不整合修復ツールについては、以下を参照してください。

「● TCP/IP 設定不整合修復ツールの実行」ページ B4-71

● TCP/IP 設定不整合修復ツールの実行

重要

TCP/IP 設定不整合修復ツールを実行すると、コンピュータにインストールされているすべてのネットワークインターフェースカードの TCP/IP 設定がリセットされます。そのため、TCP/IP 設定不整合修復ツールを実行する前に、それぞれのネットワークインターフェースカードの TCP/IPv4 の設定について、次の情報を用意してください。

- IP アドレス
- サブネットマスク
- デフォルトゲートウェイアドレス

1. エクスプローラで、CENTUM VP のソフトウェアメディア内の次の TOOLS ディレクトリを表示してください。
<CENTUM VP ソフトウェアメディアドライブ>:\CENTUM\TOOLS

補足

TCP/IP 設定不整合修復ツールは、CENTUM VP をインストールすると、次のフォルダにもインストールされます。

<CENTUM VP インストール先フォルダ>\net\tool

2. TcpipInconsistencyRepair.cmd を右クリックし、コンテキストメニューから [管理者として実行] を選択してください。
不整合の検出結果に応じて、ダイアログが表示されます。
3. ネットワーク設定の不整合が検出されない場合は、[OK] をクリックして、ツールを終了してください。
ネットワークは通常どおり使用可能です。
4. 不整合を検出した場合は、[はい] を選択してください。
ネットワーク設定がリセットされ、コンピュータの再起動を要求するメッセージが表示されます。
5. [はい] を選択し、コンピュータを再起動してください。
6. コンピュータの再起動後、すべてのネットワークインターフェースカードについて、「インターネットプロトコルバージョン 4 (TCP/IPv4) のプロパティ」ウィンドウから、ネットワーク設定を再設定してください。

B4.3.5 CENTUM VP Small を使用する際の注意事項

CENTUM VP Small を使用する際は、次の点に注意してください。

■ CENTUM VP Small で V ネットをシングルとして使用するとき

CENTUM VP Small で、V ネットをシングルで使用する場合、次のコマンドを実行してネットワーク設定ツールを起動して、制御バスの設定を [シングル] にしてください。

<CENTUM VP インストールフォルダ>\Tool\CS3000\Tool\Network.exe

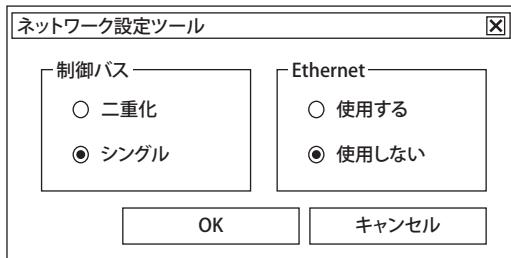


図 B4.3.5-1 ネットワーク設定ツール

■ CENTUM VP Small で Ethernet 接続を使用しないとき

V ネットのネットワークを利用して Ethernet の通信をするための設定です。

CENTUM VP Small で、Ethernet 接続を使用しない場合は、「■ CENTUM VP で V ネットをシングルとして使用する場合の設定」に記載されているネットワーク設定ツールの [Ethernet] の設定を [使用しない] にしてください。

また、V ネットのネットワークプロパティで設定を変更する必要があります。

次に V ネットのネットワークプロパティでの設定変更手順を示します。

1. 管理者ユーザでログオンしてください。

補足

すべてのアプリケーション（システムビューや操作監視機能なども含む）を起動しないでください。

2. コントロールパネルを起動してください。
3. [ネットワークとインターネット] – [ネットワークと共有センター] を選択してください。
ネットワークと共有センターウィンドウが表示されます。
4. [アダプターの設定変更] を選択してください。
ネットワーク接続ウィンドウが表示されます。
5. ネットワーク接続画面から、[Vnet] のアイコンを右クリックし、[プロパティ] を選択してください。
Vnet のプロパティダイアログが表示されます。

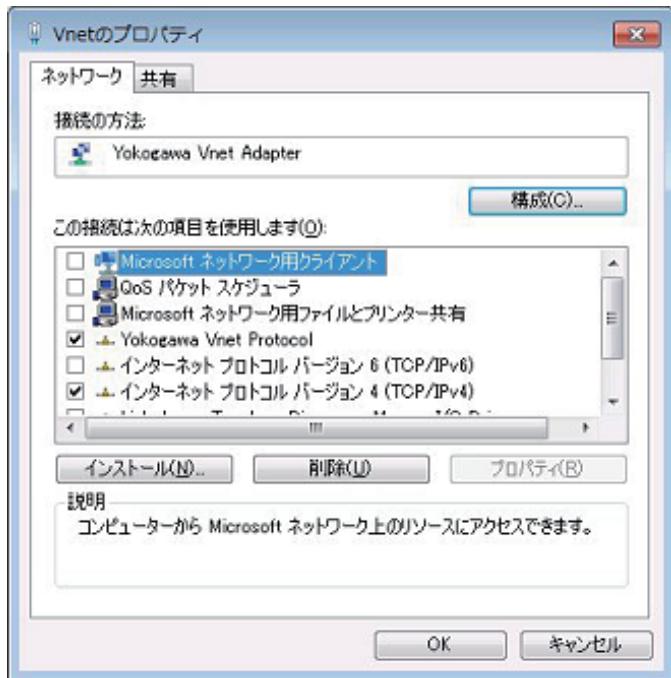


図 B4.3.5-2 Vnet のプロパティダイアログ

6. ネットワークタブの次の 4 つのチェックボックスをオンにしてください。
 - Microsoft ネットワーク用クライアント
 - Microsoft ネットワーク用ファイルとプリンタ共有
 - Link-Layer Topology Mapper I/O Driver
 - Link-Layer Topology Discovery Responder
7. [OK] をクリックして、コンピュータを再起動してください。

B4.3.6 コンピュータ切替型 UGS を使用する際の注意事項

コンピュータ切替型 UGS を使用する際は、次の点に注意してください。

■ コンピュータ切替型 UGS のバインド設定

コンピュータ切替型 UGS では、バインドの優先順位は、次のように設定してください。

重要 Windows Server 2016 の場合、本設定は不要です。

1. Ethernet および外部 Ethernet
2. Vnet
3. 冗長化制御ネットワーク

補足

- ・ Ethernet および外部 Ethernet の優先順位は、サブシステムとの通信の優先順位などを考慮して決定してください。
- ・ 冗長化制御ネットワークは、冗長化構成にしたときに使用します。

参照

バインドの設定方法については、以下を参照してください。

「■ 手順 4：バインドの設定」ページ B4-67

■ コンピュータ切替型 UGS 固有のネットワークの設定

コンピュータ切替型 UGS では、次の固有のネットワークを使用しています。

- ・ 冗長化制御ネットワーク
- ・ 外部 Ethernet ネットワーク 1～4

補足

- ・ コンピュータ切替型 UGS の構成によっては、外部 Ethernet ネットワーク 3、4 を使用しない場合があります。
- ・ 冗長化制御ネットワークは、冗長化構成にしたときに使用します。

コンピュータ切替型 UGS では、これらのネットワークの設定を変更して、[Yokogawa Vnet Protocol] を不使用とする必要があります。

ネットワークの設定を変更するときは、次の手順に従ってください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [ネットワークの状態とタスクの表示] をクリックしてください。
ネットワークと共有センターが表示されます。
4. 左ペインで、[アダプターの設定の変更] をクリックしてください。
ネットワーク接続ウィンドウが表示されます。
5. コンピュータ切替型 UGS 固有のネットワークのアイコンを右クリックし、[プロパティ] をクリックしてください。
プロパティダイアログが表示されます。
6. [Yokogawa Vnet Protocol] のチェックボックスをクリアしてください。
7. [OK] ボタンをクリックしてください。

補足

コンピュータ切替型 UGS 固有のネットワークのすべてに対して本操作を行ってください。

■ インターフェイスメトリックの設定

コンピュータ切替型 UGS では、Ethernet のプロパティでインターフェイスメトリックを設定する必要があります。

補足

Windows 10 または Windows Server 2016 のコンピュータに、システム統合 OPC 機能に関連するソフトウェアをインストールする場合も、インターフェイスメトリックを設定する必要があります。

インターフェイスメトリックを設定するときは、次の手順に従ってください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [ネットワークの状態とタスクの表示] をクリックしてください。
ネットワークと共有センターが表示されます。
4. 左ペインで、[アダプターの設定の変更] をクリックしてください。
ネットワーク接続ウィンドウが表示されます。
5. Ethernet のアイコンを右クリックし、[プロパティ] を選択してください。
プロパティダイアログが表示されます。
6. [インターネットプロトコルバージョン 4 (TCP/IPv4)] を選択して、[プロパティ] ボタンをクリックしてください。
インターネットプロトコルバージョン 4 (TCP/IPv4) のプロパティダイアログが表示されます。
7. [全般] タブで [詳細設定] ボタンをクリックしてください。
TCP/IP 詳細設定ダイアログが表示されます。
8. [IP 設定] タブで、[自動メトリック] チェックボックスをクリアして、[インターフェイスメトリック] ボックスに 1 を入力してください。

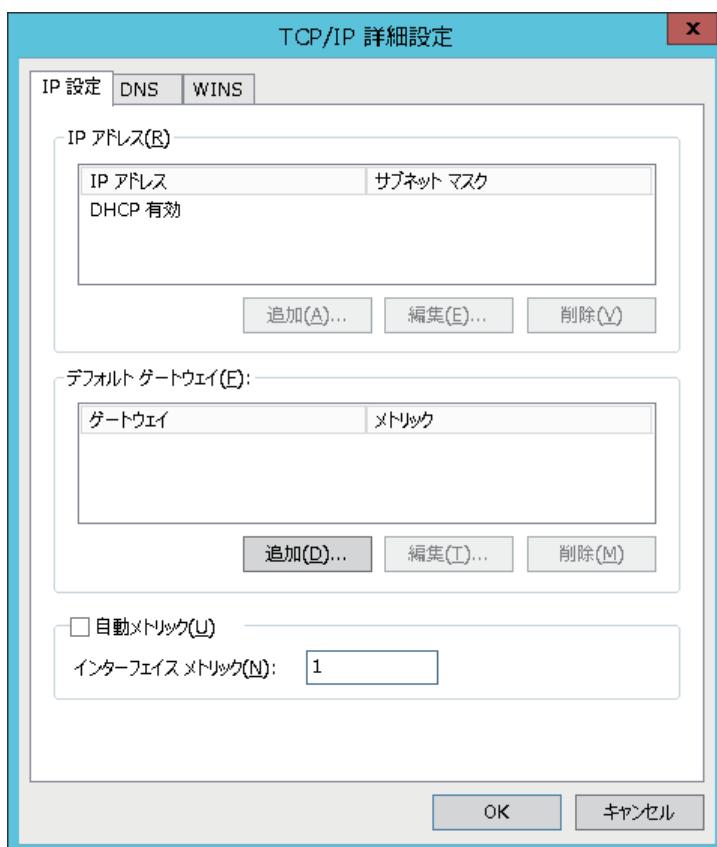


図 B4.3.6-1 TCP/IP 詳細設定ダイアログ

9. [OK] ボタンをクリックしてください。

B4.3.7 仮想マシンを使用する際の注意事項

仮想マシンを使用する際は、Ethernet、およびVnetの他に制御ネットワークとリモートUIネットワークの設定を行う必要があります。

■ ローカルエリア接続の名称変更

制御ネットワークとリモートUIネットワークに関するローカルエリア接続の名称は、次のように設定してください。

表 B4.3.7-1 ネットワーク接続名称の変更

ネットワーク種別	「ネットワーク接続」ウィンドウ上の表示 (*1)	名称 (*2)
制御ネットワーク 1	Microsoft Hyper-V Network Adapter #n	VnetIPBUS1
制御ネットワーク 2	Microsoft Hyper-V Network Adapter #n	VnetIPBUS2
リモート UI ネットワーク	Microsoft Hyper-V Network Adapter #n	RemoteUINetwork

*1: デフォルトの名称です。また、n=1,2,...となり、仮想NICの番号を示します。

*2: 必ず、この名称で設定してください。ただし、大文字、小文字の区別はしません。

● ネットワークの種別を確認する方法

ネットワークの種別を確認するときは、次の手順に従ってください。

- ネットワーク接続ウィンドウでネットワークを右クリックし、[プロパティ] を選択してください。
- [ネットワーク] タブを開き、[構成] ボタンをクリックしてください。
- 詳細設定タブを開き、[プロパティ] の [Hyper-V Network Adapter Name] を選択して、表示された「値」を確認してください。

仮想マシンを構築したときに設定したデバイス名が表示されます。

補足

手順3で確認する「値」については、仮想マシンを構築したエンジニアに確認してください。

■ プロパティの設定

ネットワーク接続ごとのプロパティ設定で、使用する項目を設定します。次の表に示すように、プロパティを設定してください。

表 B4.3.7-2 ネットワーク接続ごとの使用項目一覧

項目	使用の有無 (*1)		
	制御ネットワーク 1	制御ネットワーク 2	リモート UI ネットワーク
Microsoft ネットワーク用クライアント	No	No	Yes
QoS パケットスケジューラ	No	No	Yes
Microsoft ネットワーク用ファイルとプリンタ共有	No	No	No
Microsoft Network Adapter Multiplexor Protocol	No	No	No
Microsoft LLDP プロトコルドライバー	No	No	Yes
Yokogawa Vnet Protocol	No	No	No
インターネットプロトコルバージョン 6 (TCP/IPv6)	No	No	No
インターネットプロトコルバージョン 4 (TCP/IPv4)	Yes	Yes	Yes
Link-Layer Topology Discovery Mapper I/O Driver	No	No	Yes
Link-Layer Topology Discovery Responder	No	No	Yes

*1: Yes:チェックボックスをオン

No:チェックボックスをクリア

■ IP アドレスの設定

制御ネットワークに、IP アドレス、サブネットマスク、デフォルトゲートウェイを設定する必要はありません。それらは、Vnet/IP インタフェース管理ツールによって、Vnet/IP インタフェースパッケージが管理しているドメイン番号とステーション番号の設定値を元に、自動的に設定されます。リモート UI ネットワークの IP アドレス、サブネットマスク、デフォルトゲートウェイには、次の値を設定することを推奨します。

IP アドレス : 172.18.ドメイン番号.ステーション番号(*1)

サブネットマスク : 255.255.0.0

デフォルトゲートウェイ : 設定なし

*1: 既存の環境とネットワークアドレスが重複する場合、ネットワークアドレスは、172.18 以外の値を使用することもできます。

B4.4 オペレーションキーボード用 USB ドライバのインストールをする

USB 接続タイプのオペレーションキーボード（以降 OPKB と呼びます）を利用する場合、OPKB 用 USB ドライバが必要です。

以降の OPKB 用 USB ドライバのインストール手順は、Windows 10 をベースに説明しています。その他の OS については、手順や画面表示が異なる場合は、別途注意書きとして記載します。

OPKB 用 USB ドライバは CENTUM VP ソフトウェアのソフトウェアメディアに含まれています。

■ インストール手順

OPKB 用 USB ドライバのインストールについて説明します。

1. 管理者ユーザでログオンしてください。
2. 実行中のすべてのアプリケーションを終了してください。
3. OPKB を USB ポートに接続してください。

補足

AIP827 の場合は、OPKB の電源ケーブルも接続してください。

4. CENTUM VP のソフトウェアメディアをドライブに挿入してください。
 - ・ 自動再生ダイアログが表示された場合、[Launcher.exe の実行] をクリックしてください。
 - ・ 自動再生ダイアログが表示されない場合、エクスプローラでソフトウェアメディアのトップフォルダにある Launcher.exe をダブルクリックしてください。
 インストールメニューが表示されます。
5. [オペレーションキーボード用ドライバ] をクリックしてください。
Setup 内容を確認するダイアログが表示されます。
6. [INSTALL] を選択して、[OK] をクリックしてください。
インストール開始を確認するダイアログが表示されます。
7. [OK] をクリックしてください。

補足

- ・ Windows セキュリティダイアログが表示された場合は、["Yokogawa Electric Corporation"からのソフトウェアを常に信頼する] チェックボックスをオンにして、[インストール] をクリックしてください。
- ・ Windows セキュリティダイアログの [インストールしない] は、クリックしないでください。クリックすると、エラーが発生します。

8. インストール終了を知らせるダイアログが表示されたら、[OK] をクリックしてください。

補足

コンピュータの再起動を促すダイアログが表示された場合は、必ずコンピュータを再起動してください。

■ 8 ループ同時操作用オペレーションキーボード（形名：AIP831）を使用するときの注意事項

8 ループ同時操作用オペレーションキーボード（形名：AIP831）を使用するときは、AIP831 用のライセンスが必要になります。

参照

ライセンスの配布と反映については、以下を参照してください。

「B4.8 ライセンスの配布と反映をする」ページ B4-103

■ AIP830/AIP831 のサウンドスピーカーを使用する

本製品のサウンドデバイス名は [USB AUDIO DAC] です。AIP830/AIP831 のサウンドスピーカーを使用するときは、出力先にこのデバイスを指定してください。

なお、コンピュータに組み込まれているスピーカーが同じデバイス名で表示されることがあります。そのときは、コンピュータでサウンドを出力し、AIP830/AIP831 からのサウンド出力を確認してから使用してください。

B4.5 コンソール形 HIS の場合に必要な設定をする

コンソール形 HIS では、これまでの設定の他に、次のドライバのインストールと各種設定が必要です。

- RS-232C ドライバ
- RAS ドライバ
- オペレーションキーボードの設定
- タッチパネルの設定
- HIS の自動起動と自動ログオンの設定

補足

上記のドライバインストールをしたあと、コンピュータに接続している USB ケーブルの接続ポートを変更しないでください。USB ケーブルの接続ポートを変更すると、USB インタフェース付き AUX ボードに接続しているデバイスが動作しなくなります。

■ RS-232C ドライバのインストール

RS-232C ドライバは、コンソール HIS の 8 ループオペレーションキーボードを利用するためには必要です。

RS-232C ドライバのインストール手順について説明します。

重要

RS-232C ドライバをインストールするには、AUX ボードまたは USB インタフェース付き AUX ボードとコンピュータが接続されている必要があります。

- AUX ボード：コンピュータに実装したコンソール形 HIS 用インターフェース拡張カード（形名：AIP261）で接続
- USB インタフェース付き AUX ボード（形名：AIP262）：コンピュータの USB ポートで接続

1. 管理者ユーザでログオンしてください。
2. 実行中のすべてのアプリケーションを終了してください。
3. CENTUM VP のソフトウェアメディアをドライブに挿入してください。
 - 自動再生ダイアログが表示された場合、[Launcher.exe の実行] をクリックしてください。
 - 自動再生ダイアログが表示されない場合、エクスプローラでソフトウェアメディアのトップフォルダにある Launcher.exe をダブルクリックしてください。
 インストールメニューが表示されます。
4. [コンソール HIS 用 RS ドライバ] をクリックしてください。
PC インタフェースを選択するダイアログが表示されます。
5. インストールするドライバの PC インターフェースを選択して、[インストール] をクリックしてください。

補足

- USB インタフェース付き AUX ボードを、コンピュータの USB ポートで接続している場合は、「USB (AIP262)」を選択してください。
AUX ボードを、コンピュータに実装したコンソール形 HIS 用インターフェース拡張カードで接続している場合は、「PCI (AIP261)」を選択してください。
- 以降の手順では、PC インタフェースによってダイアログの表示が若干違うことがあります。ただし、手順の違いはありません。

- Setup 内容を確認するダイアログが表示されます。
6. [INSTALL] を選択して、[OK] をクリックしてください。
インストールを確認するダイアログが表示されます。

7. [OK] をクリックしてください。

補足

Windows セキュリティダイアログが表示された場合は、["Yokogawa Electric Corporation"からのソフトウェアを常に信頼する] チェックボックスをオンにして、[インストール] をクリックしてください。

8. インストール終了を知らせるダイアログが表示されたら、[OK] をクリックしてください。

補足

コンピュータの再起動を促すダイアログが表示されたら、[OK] をクリックし、コンピュータを再起動してください。

■ RS-232C ドライバの COM ポート番号の確認と再設定（Windows 10、Windows Server 2016）

次の条件をすべて満たす場合、RS-232C ドライバが正常な COM ポート番号に割り付けられているかを確認してください。

- ・ Windows 10 または Windows Server 2016 のコンピュータである
- ・ USB インタフェース付き AUX ボードを使用している

RS-232C ドライバが正常な COM ポート番号に割り付けられていない場合は、RS-232C ドライバの COM ポート番号を再設定してください。

ここでは、次の手順を説明します。

- ・ RS-232C ドライバの COM ポート番号の確認
- ・ RS-232C ドライバの COM ポート番号の再設定

● RS-232C ドライバの COM ポート番号を確認する

RS-232C ドライバの COM ポート番号を確認するときは、次の手順に従ってください。

1. 管理者ユーザでサインインしてください。
2. デバイスマネージャを起動してください。

補足

ユーザー アカウント制御ダイアログが表示された場合は、[はい] をクリックしてください。

3. [ポート (COM と LPT)] を展開して、[USB Serial Port Device (AIP262)] ドライバが 4つ表示されていることを確認してください。



図 B4.5-1 USB Serial Port Device (AIP262) ドライバ

4. 4つの [USB Serial Port Device (AIP262)] ドライバの右に(COM3)～(COM6)が表示されていることを確認してください。他の番号が表示されている場合は、RS-232C ドライバの COM ポート番号を再設定してください。
5. 4つの [USB Serial Port Device (AIP262)] ドライバの右に(COM3)～(COM6)が表示されているときは、各ドライバに COM ポート番号が正常に割り付いていることを確認します。

[USB Serial Port Device (AIP262)] ドライバごとに、次の手順を実施してください。

- a. [USB Serial Port Device (AIP262)] ドライバをダブルクリックしてください。
プロパティダイアログが表示されます。

- b. [詳細] タブの [プロパティ] ドロップダウンリストで、[ハードウェア ID] を選択してください。

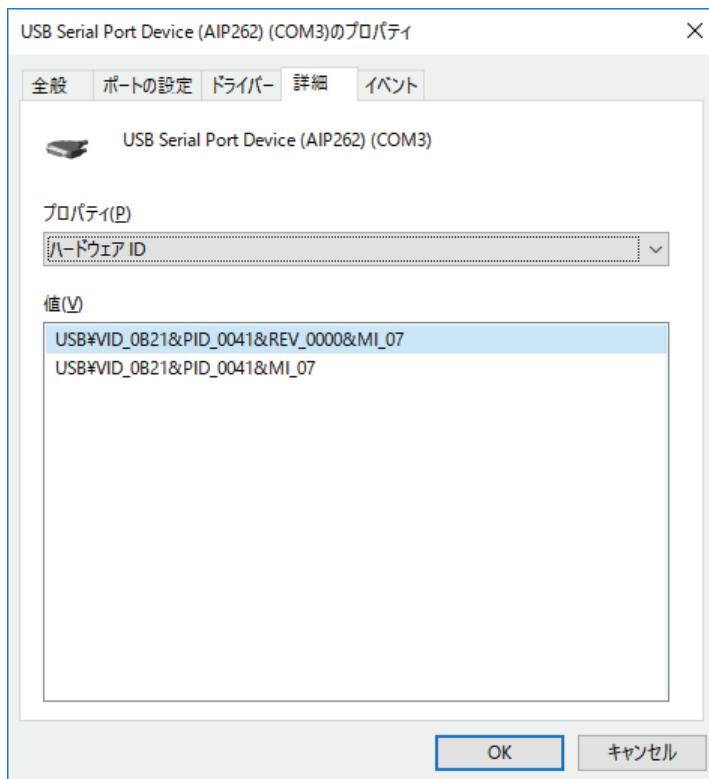


図 B4.5-2 ハードウェア ID

- c. [値] リストの上位の ID を確認して、COM ポート番号とハードウェア ID が次の表の対応となっているかを確認してください。対応していない場合は、RS-232C ドライバの COM ポート番号を再設定してください。

表 B4.5-1 COM ポート番号と対応するハードウェア ID

COM ポート番号	ハードウェア ID
COM3	USB\VID_0B21&PID_0041&REV_0000&MI_01
COM4	USB\VID_0B21&PID_0041&REV_0000&MI_03
COM5	USB\VID_0B21&PID_0041&REV_0000&MI_05
COM6	USB\VID_0B21&PID_0041&REV_0000&MI_07

● RS-232C ドライバの COM ポート番号を再設定する

RS-232C ドライバの COM ポート番号を再設定するときは、次の手順に従ってください。

1. 管理者ユーザでサインインしてください。
2. デバイスマネージャを起動してください。

補足

ユーザー アカウント制御ダイアログが表示された場合は、[はい] をクリックしてください。

3. 次の手順を繰り返すことにより、(COM3)～(COM6)と表示されているドライバの COM ポート番号を COM3～COM6 以外に変更してください。
 - a. ドライバをダブルクリックしてください。
プロパティダイアログが表示されます。
 - b. [ポート設定] タブの [詳細設定] ボタンをクリックしてください。
詳細設定ダイアログが表示されます。



図 B4.5-3 詳細設定ダイアログ

- c. [COM ポート番号] ドロップダウンリストで、COM3～COM6 以外の使用されていない COM ポート番号を選択して、[OK] ボタンをクリックしてください。
4. 次の手順を繰り返すことにより、4 つの [USB Serial Port Device (AIP262)] ドライバの COM ポート番号を再設定してください。
- [USB Serial Port Device (AIP262)] ドライバをダブルクリックしてください。プロパティダイアログが表示されます。
 - [詳細] タブの [プロパティ] ドロップダウンリストで、[ハードウェア ID] を選択してください。
 - [値] リストの上位の ID を確認してください。
 - [ポート設定] タブの [詳細設定] ボタンをクリックしてください。詳細設定ダイアログが表示されます。
 - [COM ポート番号] ドロップダウンリストで、次の COM ポート番号を選択してください。

表 B4.5-2 設定する COM ポート番号

ハードウェア ID	COM ポート番号
USB\VID_0B21&PID_0041&REV_0000&MI_01	COM3
USB\VID_0B21&PID_0041&REV_0000&MI_03	COM4
USB\VID_0B21&PID_0041&REV_0000&MI_05	COM5
USB\VID_0B21&PID_0041&REV_0000&MI_07	COM6

5. コンピュータを再起動してください。

■ RAS ドライバのインストール

RAS ドライバは、コンソール形 HIS 用の AUX ボードまたは USB インタフェース付き AUX ボードを使用するために必要です。

RAS ドライバのインストール手順について説明します。

重要

RAS ドライバをインストールするには、AUX ボードまたは USB インタフェース付き AUX ボードとコンピュータが接続されている必要があります。

- ・ AUX ボード：コンピュータに実装したコンソール形 HIS 用インターフェース拡張カード（形名：AIP261）で接続
- ・ USB インタフェース付き AUX ボード（形名：AIP262）：コンピュータの USB ポートで接続

1. 管理者ユーザでログオンしてください。
2. 実行中のすべてのアプリケーションを終了してください。
3. CENTUM VP のソフトウェアメディアをドライブに挿入してください。
 - ・ 自動再生ダイアログが表示された場合、[Launcher.exe の実行] をクリックしてください。
 - ・ 自動再生ダイアログが表示されない場合、エクスプローラでソフトウェアメディアのトップフォルダにある Launcher.exe をダブルクリックしてください。インストールメニューが表示されます。
4. [コンソール HIS 用 RAS ドライバ] をクリックしてください。
コンソールタイプと PC インターフェースを選択するダイアログが表示されます。
5. インストールするドライバのコンソールタイプと PC インターフェースを選択して、[インストール] をクリックしてください。

補足

- ・ USB インタフェース付き AUX ボードを、コンピュータの USB ポートで接続している場合は、「USB」を選択してください。
AUX ボードを、コンピュータに実装したコンソール形 HIS 用インターフェース拡張カードで接続している場合は、「PCI」を選択してください。
- ・ 以降の手順では、PC インターフェースによってダイアログの表示が若干違うことがあります。ただし、手順の違いはありません。

Setup 内容を確認するダイアログが表示されます。

6. [INSTALL] を選択して、[OK] をクリックしてください。
インストールを確認するダイアログが表示されます。
7. [OK] をクリックしてください。

補足

Windows セキュリティダイアログが表示された場合は、["Yokogawa Electric Corporation"からのソフトウェアを常に信頼する] チェックボックスをオンにして、[インストール] をクリックしてください。

8. インストール終了を知らせるダイアログが表示されたら、[OK] をクリックしてください。

補足

コンピュータの再起動を促すダイアログが表示されたら、[OK] をクリックし、コンピュータを再起動してください。

■ オペレーションキーボードの設定

コンソール形 HIS では、自動的にオペレーションキーボードを使用する設定になります。
接続ポートは COM4 です。

■ タッチパネルの設定

ソリッドスタイルコンソール形 HIS では、CENTUM VP ソフトウェアのインストール時に「タッチパネル設定」ダイアログが表示されます。ダイアログでは、タッチパネルを「使

用する／しない] を選択してください。2段積みモニタの場合、上段および下段のタッチパネルを [使用する／しない] を選択してください。
オープンスタイルコンソール形 HIS では、タッチパネルのセットアップが行われません。タッチパネル用ハードウェアに同梱の説明書に従って、別途セットアップをしてください。

■ HIS の自動起動と自動ログオンについて

コンソール形 HIS でエンジニアリングキーボードを接続しない場合、操作監視機能の自動起動（Windows の自動起動を含む）を有効にする設定を行ってください。理由は、Windows のログオンダイアログを表示させるための [Ctrl] + [Alt] + [Del] のキー入力とパスワードの入力がオペレーションキーボード（OPKB）ではできないからです。

参照

操作監視機能の自動起動（Windows の自動起動を含む）については、以下を参照してください。

「■ 操作監視機能の自動起動の設定」ページ B4-138

B4.6 CENTUM VP ソフトウェアのインストールをする

CENTUM VP のソフトウェアインストール手順について説明します。

■ インストールをする管理者ユーザ

次の表に示す管理者ユーザで実施してください。

CENTUM VP ソフトウェアをインストールすると、CTM_MAINTENANCE グループが作成され、インストールを実施したユーザは、自動的に CTM_MAINTENANCE グループに所属します。

表 B4.6-1 新規インストールを行う管理者ユーザ

従来モデル	設定しようとするセキュリティモデル／ユーザ管理方法	
	標準モデル	ドメイン管理／併用管理
Administrators ローカルグループに所属するローカルユーザ	Administrators ローカルグループに所属するローカルユーザ	<ul style="list-style-type: none"> • Domain Admins ドメイングループに所属するドメインユーザ • Administrators ローカルグループに所属するドメインユーザ • Administrators ローカルグループに所属するローカルユーザ(*1)

1: () : インストール中にドメインユーザのユーザ名とパスワードを入力する必要があります。

補足

ユーザ管理方法がドメイン管理／併用管理の場合は、コンピュータがドメインに参加した状態でインストールを実施してください。

参照

ドメイングループに所属する管理者ユーザの登録については、以下を参照してください。

「■ クライアントコンピュータのセットアップ作業に関する注意事項」ページ B2-21

■ インストール手順

CENTUM VP ソフトウェアのインストールは、HIS/システム生成機能/AD サーバのみを搭載したコンピュータにインストールする場合と、APCS/SIOS/GSGW/UGS/UACS ステーションにインストールする場合で、手順に違いがあります。

● HIS/システム生成機能/AD サーバのみを搭載したコンピュータにインストールする

1. 管理者ユーザでログオンしてください。
 2. 実行中のすべてのアプリケーション、アンチウィルスソフトウェアなどの常駐型プログラムを終了してください。
 3. CENTUM VP のソフトウェアメディアをドライブに挿入してください。
 - 自動再生ダイアログが表示された場合、[Launcher.exe の実行] をクリックしてください。
 - 自動再生ダイアログが表示されない場合、エクスプローラでソフトウェアメディアのトップフォルダにある Launcher.exe をダブルクリックしてください。
- インストールメニューが表示されます。

4. インストールメニューの [CENTUM VP ソフトウェアのインストール] をクリックしてください。
現在のログオンユーザに対して、以降のインストール作業で必要となる権限を付与するため、再起動を要求するダイアログが表示されます。

補足

Microsoft .NET Framework などの CENTUM VP に必要な Windows の再頒布モジュールがインストールされていない場合、それらのモジュールのインストールを促すダイアログが表示されます。

それらのモジュールをインストールする場合は、[インストール] をクリックしてください。[キャンセル] をクリックすると、CENTUM VP のインストールが中止されます。

CENTUM VP に必要なモジュールは次のとおりです。

- Microsoft .NET Framework 4.6.2
- MSXML 6.0 SP1
- Microsoft Visual C++ 2017 再頒布可能パッケージ
- OPCCOM ProxyStub

各モジュールのインストールが開始されると、ステータス欄の表示内容が変わります。また、インストール完了後、再起動を要求される場合があります。再起動を要求された場合、再起動後に CENTUM VP のインストールを継続してください。

重要

Windows Server 2012 R2 で、Microsoft .NET Framework 4.6.2 のインストールが途中で 5～10 分以上停止する場合は、Windows 更新プログラムがインストールされていない可能性があります。Microsoft .NET Framework 4.6.2 のインストールを停止して、Windows 更新プログラムをインストールしてください。

5. [OK] をクリックしてください。
再起動が始まります。
6. 同じユーザで再度ログオンしてください。
CENTUM VP ソフトウェアのインストールが開始され、ようこそダイアログが表示されます。
7. [次へ] をクリックしてください。
ユーザ情報とインストール先フォルダを入力するダイアログが表示されます。

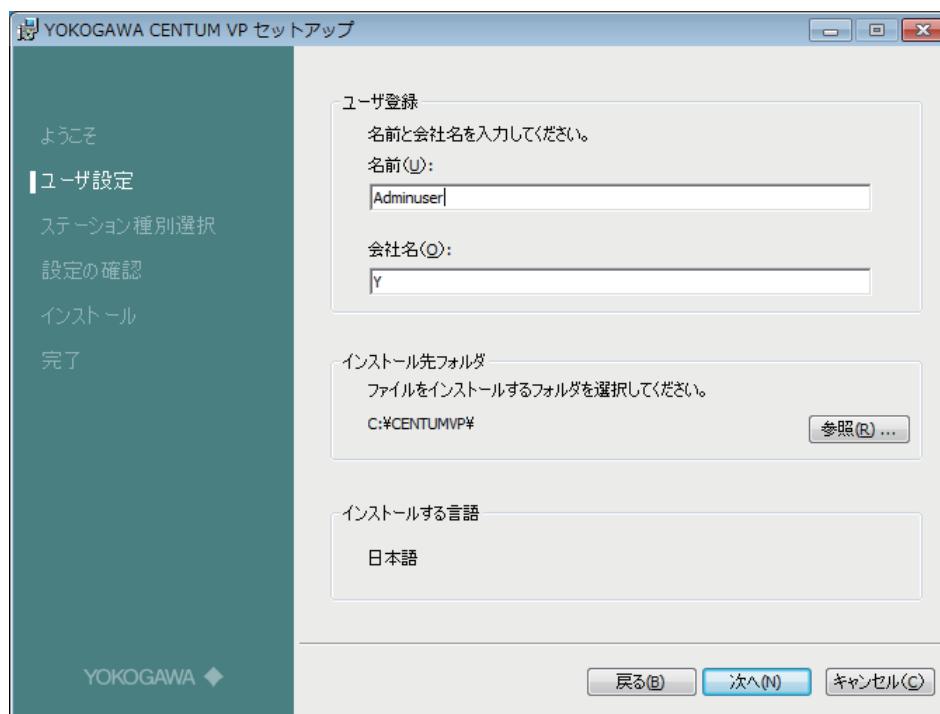


図 B4.6-1 CENTUM VP セットアップダイアログ（ユーザ設定）

補足

- 異なるバージョンのドライバがインストールされている場合は、それを示すダイアログが表示されます。内容を確認し、[OK] をクリックしてください。実際のドライバの更新は、CENTUM VP ソフトウェアのインストール後、ドライバのアンインストール、インストールをしてください。
- Vnet/IP インタフェースカードが実装されている場合、Vnet/IP オープン通信を使用しなくても、Vnet/IP オープン通信ドライバの更新をする必要があります。Ethernet に接続する場合は、Vnet/IP オープン通信ドライバを更新後、ドライバを無効にしてください。

8. 名前と会社名を入力してください。インストール先フォルダは、デフォルトの場所から変更する場合は、[参照] をクリックして指定してください。

補足

- 名前と会社名は、100 文字以内としてください。
- インストール先フォルダは、デフォルトでは、<システムドライブ>:\CENTUMVP\ になっています。フォルダを変更する場合は、50 文字以内で指定してください。
- インストールする言語は、システム言語が日本語の場合は日本語、それ以外の言語の場合は英語として自動決定されます。

9. [次へ] をクリックしてください。

ステーション種別の選択、データベースの参照先の入力、ステーションのコンソールタイプの選択をするダイアログが表示されます。

10. ステーション種別を選択してください。

補足

ステーション種別で選択する項目とインストールされるソフトウェアを次に示します。

表 B4.6-2 ステーション種別で選択する項目とインストールされるソフトウェア

ステーション種別	インストールされるソフトウェア
HIS/ENG/または汎用 PC (*1)	操作監視機能/システム生成機能/AD サーバなどに関連するソフトウェアをインストールする。
UGS	統合ゲートウェイステーション (UGS) に関連するソフトウェアをインストールする。
GSGW 汎用サブシステムゲートウェイ	汎用サブシステムゲートウェイ 機能に関連するソフトウェアをインストールする。
SIOS システム統合 OPC ステーション	システム統合 OPC 機能に関連するソフトウェアをインストールする。
APCS アドバンストプロセスコントロール ステーション	APCS 制御機能に関連するソフトウェアをインストールする。

*1: システムビューで HISddss、または、STNddss と定義するステーション。ただし、操作監視機能やシステム生成機能と共に存在しない AD サーバの場合、ステーション名は、コンピュータ名と同じになります。

11. データベースの参照先（プロジェクトデータベースが存在するコンピュータ名）を、15 文字以内で入力してください。システム生成機能のみを搭載したコンピュータや AD サーバ機能のみを搭載したコンピュータでは、この指定は不要です。

補足

- デフォルトでは、現在インストール中のコンピュータ名になっています。この設定は、あとから変更することもできます。その場合の手順は、「エンジニアリングデータ参照先を変更する。」の節に記載されています。
- プロジェクトデータベースが、システム生成機能を搭載した HIS やシステム生成機能を搭載したコンピュータにある場合は、コンピュータ名を 7 文字で入力してください。

12. ステーションのコンソールタイプを選択してください。

RAS ドライバをインストール済みの場合は、ドライバのインストール時に選択したコンソールタイプがデフォルトで表示されます。それ以外の場合は「PC」がデフォルトになっています。

- コンソールタイプで PC を選択した場合
ポート番号はデフォルトでは、空白になっています。
オペレーションキーボードを使用する場合は、オペレーションキーボードを接続する COM ポート番号を選択してください。
オペレーションキーボードを使用しない場合は、オペレーションキーボードを接続する COM ポート番号は空白のままとしてください。

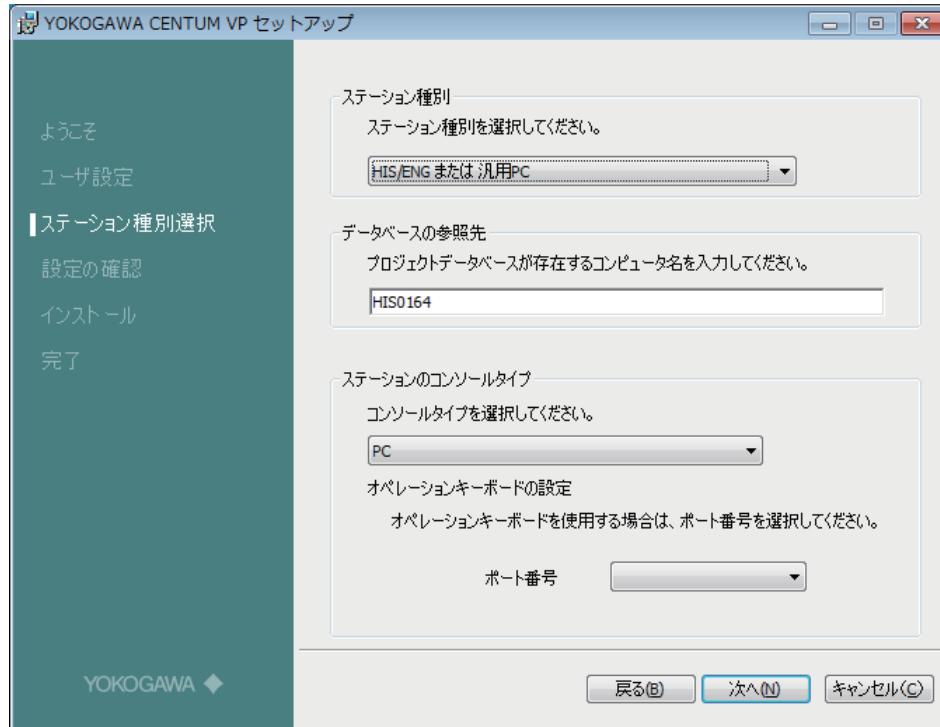


図 B4.6-2 CENTUM VP セットアップダイアログ（コンソールタイプで PC を選択した場合）

- コンソールタイプでソリッドスタイルコンソールを選択した場合
タッチパネル使用はデフォルトでは、上段・下段ともにチェックボックスがオフになっています。
2段積みモニタでタッチパネルの上段を使用する場合は、[タッチパネル（上段）を使用する。] チェックボックスをオンにしてください。
タッチパネルの下段を使用する場合は、[タッチパネル（下段）を使用する。] チェックボックスをオンにしてください。
シングルモニタでタッチパネルを使用する場合は、[タッチパネル（下段）を使用する。] チェックボックスをオンにしてください。[タッチパネル（上段）を使用する。] チェックボックスはオフのままにしてください。

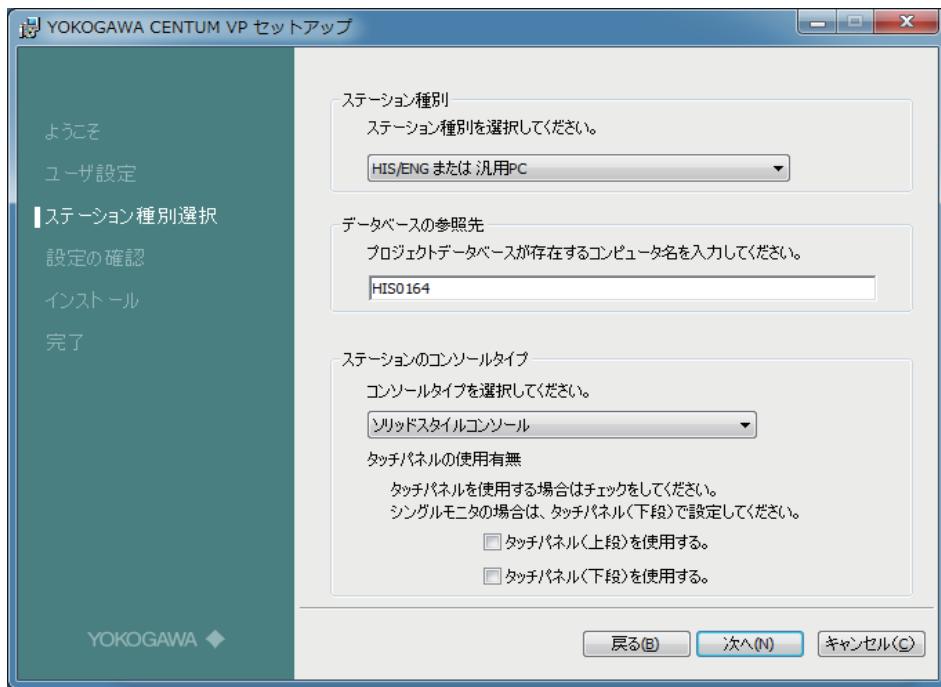


図 B4.6-3 CENTUM VP セットアップダイアログ（コンソールタイプでソリッドスタイルコンソールを選択した場合）

[次へ] をクリックすると、タッチパネルを使用しない設定になっている場合は次の確認ダイアログが表示されます。そのままインストールを続ける場合は [はい] を、設定画面に戻って再設定する場合は [いいえ] をクリックしてください。

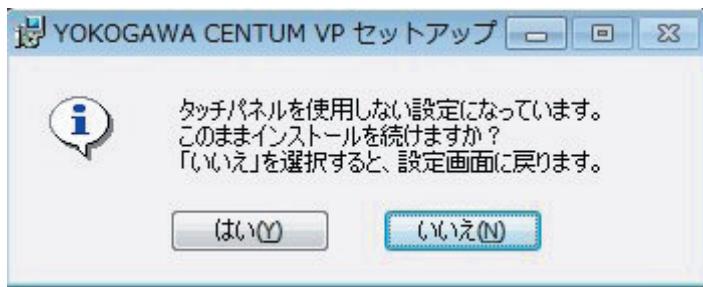


図 B4.6-4 タッチパネル使用の有無を確認するダイアログ

- ・ コンソールタイプでオープンスタイルコンソールを選択した場合
特に設定する項目はありません。

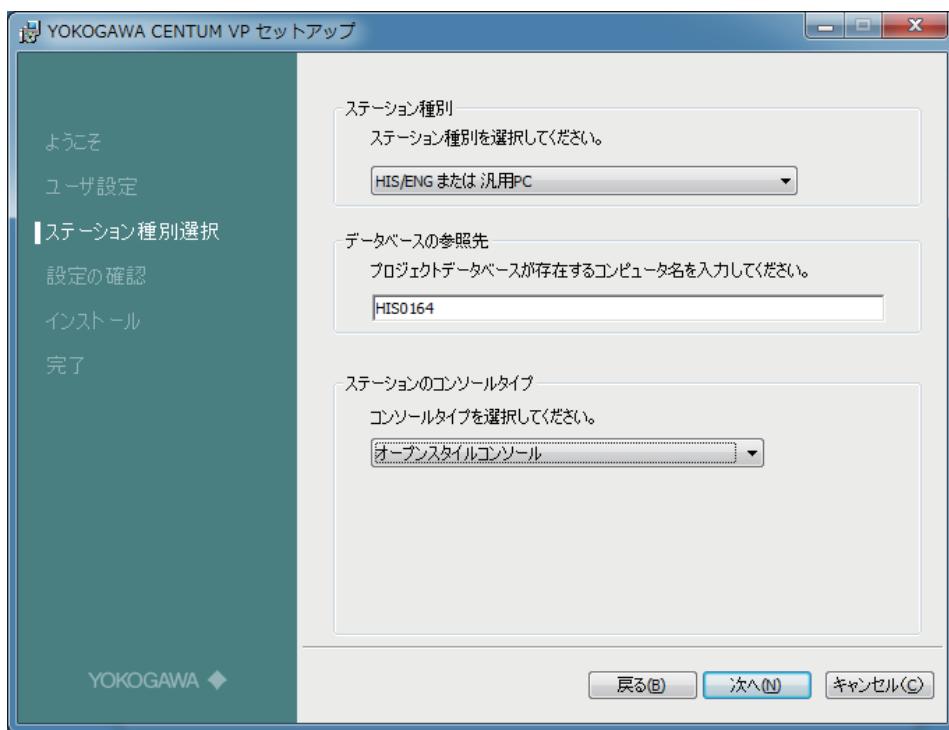


図 B4.6-5 CENTUM VP セットアップダイアログ（コンソールタイプでオープンスタイルコンソールを選択した場合）

13. [次へ] をクリックしてください。
インストール設定の確認ダイアログが表示されます。

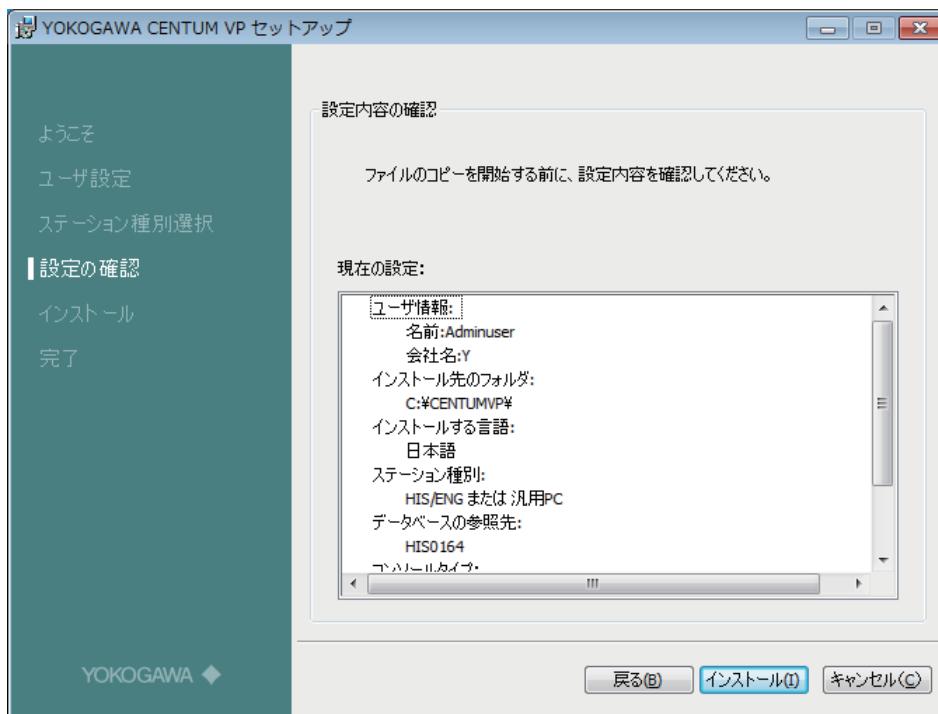


図 B4.6-6 CENTUM VP セットアップダイアログ（設定の確認）

14. インストールの設定内容の確認を行い、内容が正しければ [インストール] をクリックしてください。
CENTUM VP ソフトウェアのインストールが行われます。

補足

インストール中には、その進捗状況を知らせるダイアログが表示されます。インストールが完了するまでには、数分かかる場合があります。

15. インストール完了の画面が表示されたら、次のいずれかの操作を行ってください。

- ・ CENTUM VP のみインストールする場合、[はい、ITセキュリティの設定を行います] を選択して [終了] をクリックしてください。続けてITセキュリティツールが起動されます。
- ・ 続けて他の当社製品のインストールを行う場合は、[いいえ、続けて他製品のインストールを行います] を選択して [終了] をクリックし、インストールを終了してください。

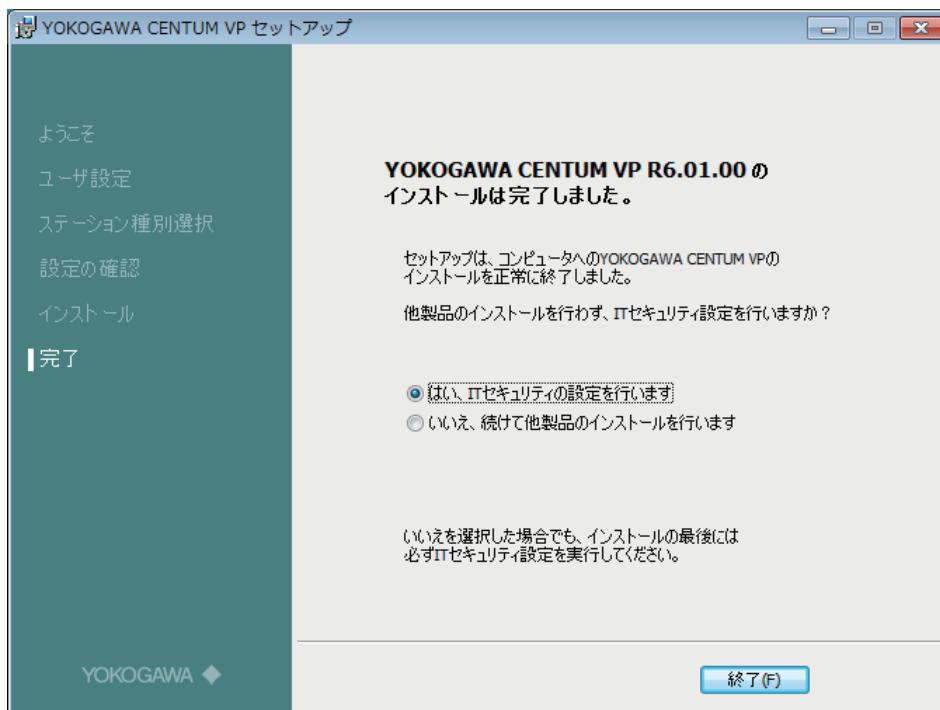


図 B4.6-7 CENTUM VP セットアップダイアログ（完了）

重要

他の当社製品のインストールを行った場合でも、インストール終了後に必ずITセキュリティの設定を行ってください。その場合、ITセキュリティ設定は、インストールされたすべての対象製品に対して一括実行されます。

ITセキュリティ設定を行わなかった場合、製品が正しく動作しません。

参照

Microsoft .NET Framework 4.6.2 のインストールを停止する方法については、以下を参照してください。

「● .NET Framework 4.6.2 のインストールの停止方法」ページ B4-33

Windows Server 2012 R2 で Windows 更新プログラムをインストールする方法については、以下を参照してください。

「■ Windows 更新プログラムのインストール」ページ B4-32

ITセキュリティの設定については、以下を参照してください。

「B4.7 ITセキュリティを設定する」ページ B4-96

● APCS/SIOS/GSGW/UGS/UACS ステーションにインストールする

1. 「●HIS/システム生成機能/AD サーバのみを搭載したコンピュータにインストールする」の手順 1 から 10 までを実行してください。
2. [次へ] をクリックしてください。
インストール設定の確認ダイアログが表示されます。
3. インストールの設定内容の確認を行い、内容が正しければ [インストール] をクリックしてください。
CENTUM VP ソフトウェアのインストールが行われます。

補足

インストール中には、その進捗状況を知らせるダイアログが表示されます。インストールが完了するまでには、数分かかる場合があります。

4. インストール完了の画面が表示されたら、次のいずれかの操作を行ってください。
 - CENTUM VP のみインストールする場合、[はい、IT セキュリティの設定を行います] を選択して [終了] をクリックしてください。続けて IT セキュリティツールが起動されます。
 - 続けて他の当社製品のインストールを行う場合は、[いいえ、続けて他製品のインストールを行います] を選択して [終了] をクリックし、インストールを終了してください。

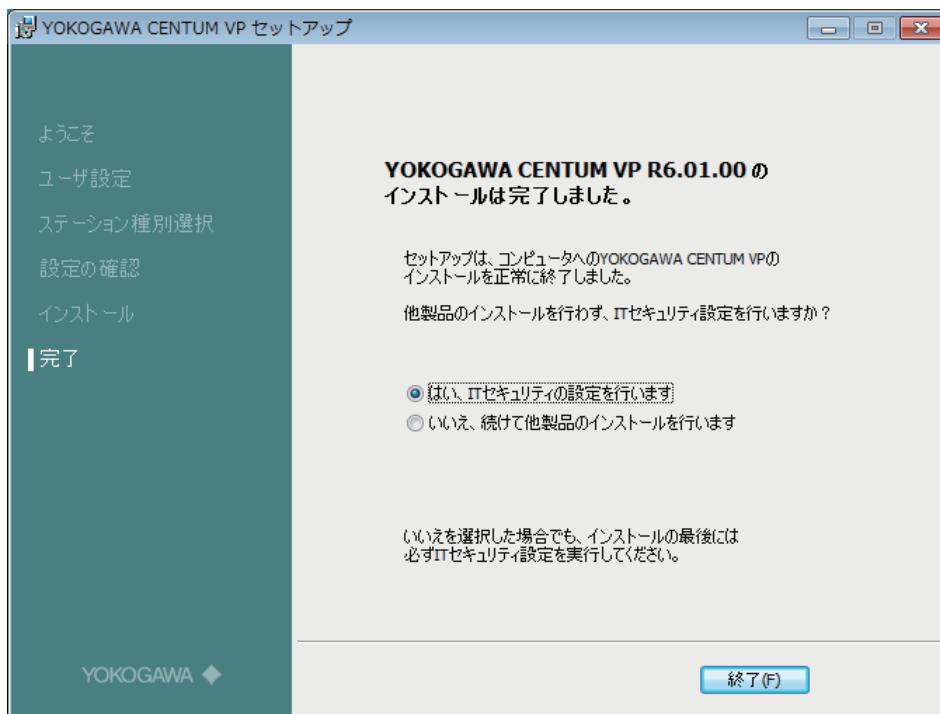


図 B4.6-8 CENTUM VP セットアップダイアログ（完了）

重要

他の当社製品のインストールを行った場合でも、インストール終了後に必ず IT セキュリティの設定を行ってください。その場合、IT セキュリティ設定は、インストールされたすべての対象製品に対して一括実行されます。

IT セキュリティ設定を行わなかった場合、製品が正しく動作しません。

参照

ITセキュリティの設定については、以下を参照してください。

「B4.7 ITセキュリティを設定する」ページ B4-96

B4.7 IT セキュリティを設定する

CENTUM VP では、ソフトウェアのインストール後に、Windows の IT セキュリティを強化するための設定を行う必要があります。

インストールの終了後、「[はい。IT セキュリティ設定を行います]」を選択した状態でインストーラを終了すると IT セキュリティツールが起動し、設定を行うことができます。

ここでは、IT セキュリティツールを使用してコンピュータの IT セキュリティを設定する手順について説明します。

重要

- IT セキュリティ設定のセキュリティモデルやユーザ管理方法は、システム全体で統一してください。異なるセキュリティモデルやユーザ管理方法に変更する場合、ファイルサーバを含むすべてのコンピュータで変更してください。
- コンピュータが故障した際にセキュリティの設定を復旧するため、セキュリティの設定をデフォルト以外の設定にした場合には、必ず IT セキュリティツールの「保存」機能で設定内容を保存しておいてください。
- 従来モデルを選択した場合は、一部の環境で Windows OS に関する制限が発生します。そのため、標準モデルを選択することを推奨します。
- IT セキュリティツール以外でカスタマイズされたセキュリティ設定は、IT セキュリティツールを実行すると、IT セキュリティツールが持つ設定情報で上書きされます。IT セキュリティツールの実行前と同じセキュリティ設定にしたい場合は、IT セキュリティツールの実行後に再度カスタマイズしてください。
なお、バージョンアップやレビューションアップをすると IT セキュリティツールが実行され、セキュリティ設定が上書きされるので、注意してください。

補足

- IT セキュリティ設定をドメインコントローラで統合管理する場合も、必ず各クライアントで IT セキュリティを設定してください。すべてのクライアントで IT セキュリティを設定したあとに、ドメインコントローラで IT セキュリティ設定を統合管理する設定を行ってください。
- コンピュータ切替型 UGS をドメイン環境で使用する場合は、CENTUM VP ソフトウェアインストール前にドメインに参加させないでください。その場合、CENTUM VP ソフトウェアインストール後の IT セキュリティ設定では、いったん従来モデルや標準モデル（スタンダードアロン管理）に設定してください。
- コンピュータ切替型 UGS をドメイン環境で使用する場合は、コンピュータ切替型 UGS をドメインに参加させたあとで、IT セキュリティ設定を標準モデルのドメイン管理または併用管理に変更してください。

参照

IT セキュリティ設定内容の詳細については、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「6.1 IT セキュリティツール」

ドメインコントローラで IT セキュリティ設定を統合管理する方法については、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「6.9 アクティブディレクトリによる IT セキュリティ設定の統合管理」

当社他製品の共存時の注意事項については、以下を参照してください。

「■ 他製品共存時の注意事項」ページ B4-101

IT セキュリティ設定で注意すべきケースについては、以下を参照してください。

「C9. IT セキュリティ設定で注意すべきケース」ページ C9-1

■ IT セキュリティツールを実行する

ここでは、IT セキュリティの設定を CENTUM VP ソフトウェアのインストール終了後に続けて行う場合の手順を説明します。

重要

次の当社製品のソフトウェアがインストールされていて、それらの製品が IT セキュリティバージョン 2.0 に対応していない場合は、IT セキュリティバージョンは 1.0 で変更できません。

- PRM
- ProSafe-RS
- Exaopc
- Exapilot
- Exaplog

IT セキュリティバージョン 2.0 に対応している場合は、IT セキュリティバージョンを維持することも、変更することもできます。

IT セキュリティツールを実行するときは、次の手順に従ってください。

1. CENTUM VP ソフトウェアインストール終了後、ダイアログが表示されます。[はい、IT セキュリティの設定を行います] を選択し、[終了] をクリックしてください。

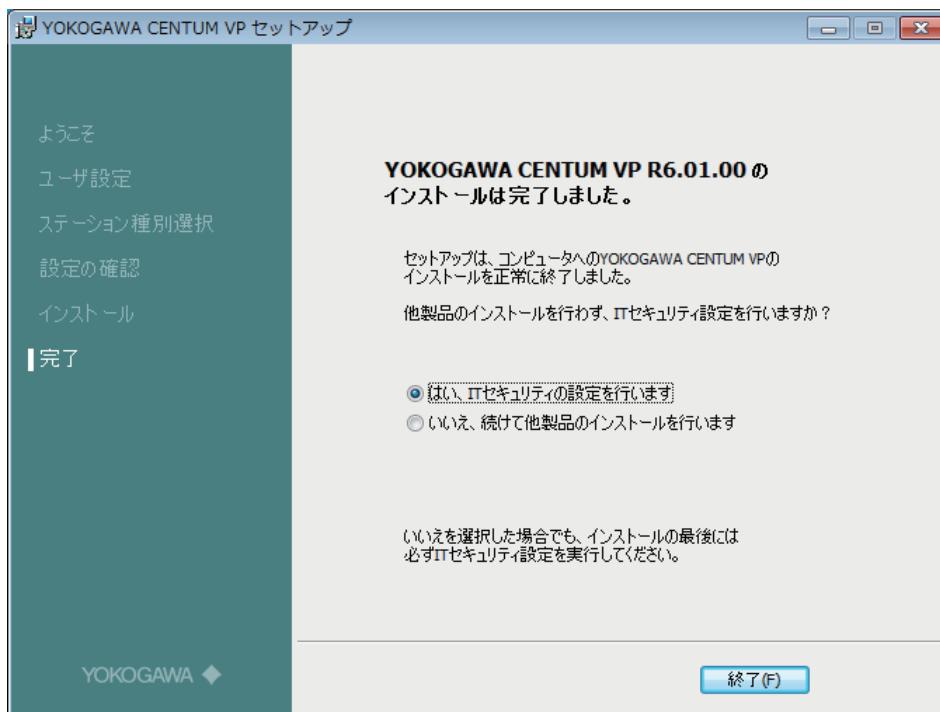


図 B4.7-1 CENTUM VP セットアップダイアログ（完了）

IT セキュリティツールが起動します。

補足

他製品をインストールしないにも関わらず、誤って [いいえ、続けて他製品のインストールを行います] を選択したまま [終了] をクリックした場合は、スタートメニューから IT セキュリティツールを起動して、メニューの [設定] をクリックしてください。IT セキュリティ設定のダイアログが表示されます。

他製品をインストールする場合は、インストール終了後にダイアログが表示されて IT セキュリティツールを起動できるので、スタートメニューから起動する必要はありません。

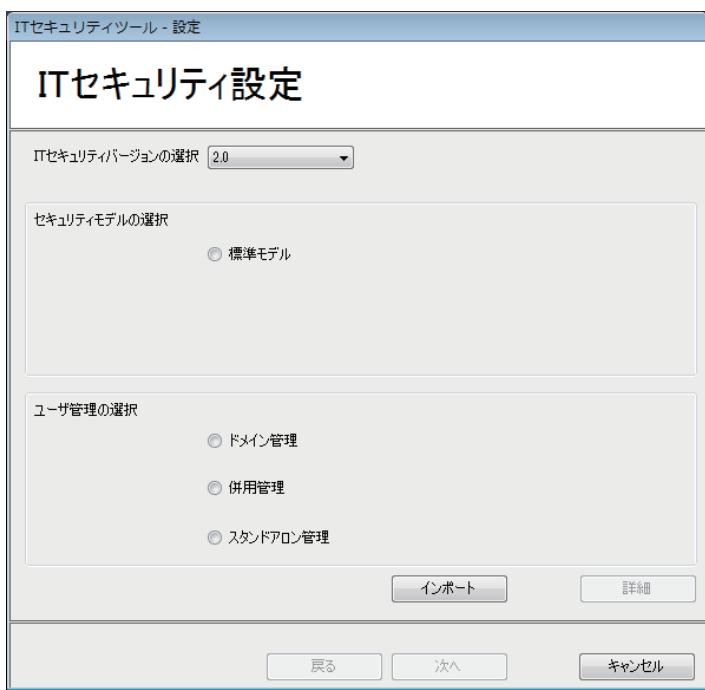


図 B4.7-2 IT セキュリティツール—設定

2. [IT セキュリティバージョンの選択] で IT セキュリティバージョンを選択してください。
3. [セキュリティモデルの選択] で [標準モデル] か [従来モデル] を選択してください。

補足

[IT セキュリティバージョンの選択] で [2.0] を選択した場合は、[標準モデル] だけ選択できます。

4. [ユーザ管理の選択] で [ドメイン管理]、[併用管理]、[スタンドアロン管理] のいずれかを選択してください。

補足

- ・ 従来モデルの場合、ユーザ管理はスタンドアロン管理のまま変更できません。
- ・ Windows ドメインに参加しているコンピュータで [スタンドアロン管理] を選択すると、警告メッセージが表示されます。[OK] をクリックして、処理を継続してください。

5. 個別の項目で設定変更する場合、次の手順を実行してください。

補足

- ・ IT セキュリティバージョンで 2.0 を選択している場合は、確認のダイアログが表示されます。そのまま設定する場合は、[はい] をクリックしてください。ただし、IT セキュリティバージョン 2.0 のみをサポートしている製品で IT セキュリティツールを実行する場合は、この確認ダイアログは表示されません。
- ・ 個別の項目の設定をしない場合は、[次へ] をクリックしてください。セキュリティ設定が行われます。設定が完了すると、セキュリティ情報の設定完了ページが表示されます。設定に失敗した項目があった場合、その内容が表示されます。その後、[今すぐ再起動する] チェックボックスをオンにして、[完了] をクリックしてください。IT セキュリティツールを終了すると、コンピュータは自動的に再起動されます。

- a. 個別の項目で設定変更する場合、[詳細] をクリックしてください。設定項目の選択ページが表示されます。

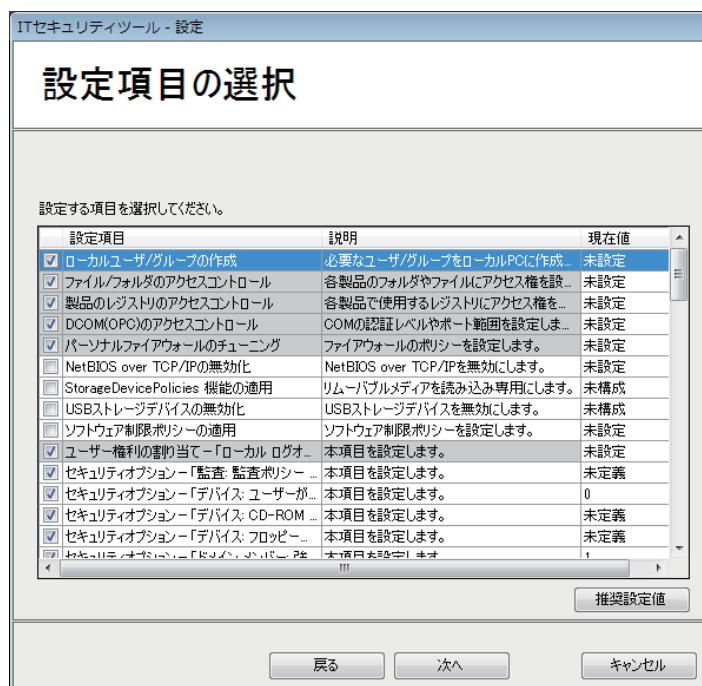


図 B4.7-3 設定項目の選択ページ (IT セキュリティバージョン 2.0 選択時)

- b. 変更する項目のチェックボックスをオン／オフしてください。

[現在値] では、該当する設定項目に、現在設定されている値が次の表の様に表示されます。

重要

ドメインコントローラから配布されたグループポリシーの設定値は表示されません。ローカルグループポリシーの設定値を表示します。

表 B4.7-1 現在値に表示される内容

表示内容	説明
実際の値	実際に設定されている値が表示されます。たとえば、[有効]、[無効]、[30]、[0] などが表示されます。(*1)
[未定義]	セキュリティオプション関連の設定項目で、値が設定されてない場合に表示されます。
[未構成]	グループポリシーの管理用テンプレートの設定項目で、値が設定されてない場合に表示されます。
[未設定]	1つの設定項目に複数の値を持つ項目で、IT セキュリティが 1 度も設定されていない場合に表示されます。
[設定済み]	1つの設定項目に複数の値を持つ項目で、IT セキュリティが 1 度でも設定されている場合に表示されます。

*1: セキュリティポリシーウィンドウで設定値が文字列で表示されている項目でも、OS 内部では設定値が数値で管理されている場合は、数値が表示されます。

補足

標準モデル選択時には設定を変更しないことを推奨します。

- c. [次へ] をクリックしてください。
設定内容の確認ページが表示されます。

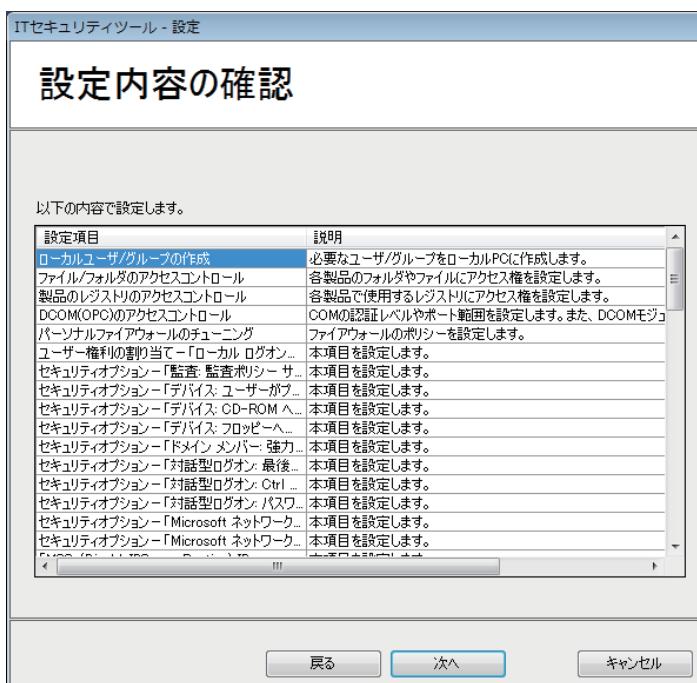


図 B4.7-4 設定内容の確認ページ (IT セキュリティバージョン 2.0 選択時)

補足

設定された内容が、セキュリティモデルのデフォルト値と異なっている場合、警告ダイアログが表示されます。

そのまま設定する場合は、[はい] をクリックしてください。[いいえ] をクリックすると、設定項目の選択ページに戻ります。

6. 設定内容を確認し、[次へ] をクリックしてください。

補足

過去に本ツールを用いてセキュリティ設定を行い、設定項目の選択ページを開かなかった場合、最後に設定したITセキュリティ設定が、そのまま設定されます。その設定内容と、選択されているセキュリティモデルのデフォルト設定が一致しないときには警告ダイアログが表示されます。

そのまま設定する場合は、[はい] をクリックしてください。

設定が完了するとセキュリティ情報の設定完了ページが表示されます。設定に失敗した項目があった場合、その内容が表示されます。

7. [今すぐ再起動する] チェックボックスをオンにして、[完了] をクリックしてください。

ITセキュリティツールを終了すると、コンピュータは自動的に再起動されます。

重要

設定に失敗した項目が表示された場合、当社窓口に連絡してください。

補足

セキュリティ設定終了後に「プログラム互換性アシスタント」ダイアログが表示されることがあります。設定は正しく行われていますので、[キャンセル] をクリックしてダイアログを閉じてください。

参照

IT セキュリティ設定をインポートする手順については、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「6.7 IT セキュリティ設定ファイルをインポート／エクスポートする」

IT セキュリティ設定の変更については、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「6.3 IT セキュリティ設定を変更する」

スタートメニューから呼び出せる CENTUM VP のアプリケーションのマッピングについては、以下を参照してください。

はじめにお読みください (IM 33J01A10-01JA) の「スタートメニューから呼び出せる CENTUM VP のアプリケーション」

● NetBIOS over TCP/IP を無効化した場合の注意事項

標準モデルを選んだ場合、NetBIOS over TCP/IP の無効化を設定することができます。ドメイン管理／併用管理の場合のデフォルトは NetBIOS over TCP/IP が無効になっています。この場合、名前解決のために次の設定をしてください。

1. エンジニアリングステーションのシステムビューから各 HIS のプロパティを開き、ネットワークタブのホスト名に、正しいホスト名を入力してください。
2. ネットワーク内の各ステーションの LMHOSTS ファイルに、次のように参照先ステーションの設定をしてください。
 - LMHOSTS の格納先

PATH : %Systemroot%\system32\drivers\etc

%Systemroot% は、Windows OS がインストールされたディレクトリで通常は、"C:\Windows"です。

- LMHOSTS ファイルの設定例

次の例は、HIS0124 (ホスト名=ステーション名) のプロジェクトファイルを参照させる場合の例です。

```
##### lmhosts
172.17.1.24 HIS0124 #PRE
```

表 B4.7-2 LMHOSTS ファイルの設定

ステーションの種類	LMHOSTS ファイルに設定する参照先ステーション
ライセンス管理ステーション	すべてのライセンス適用ステーション
HIS	ライセンス管理ステーションとプロジェクトファイルが存在しているコンピュータ
他ステーション	ライセンス管理ステーション

■ 他製品共存時の注意事項

CENTUM VP のコンピュータに IT セキュリティ設定対応の当社製品を共存させた場合の注意事項を説明します。

● 他製品をインストールしたあとに CENTUM VP ソフトウェアをインストールする場合

IT セキュリティバージョン 2.0 に対応していない他製品のインストール後に、CENTUM VP ソフトウェアをインストールするときは、IT セキュリティバージョンは 1.0 のみ選択できます。

IT セキュリティバージョン 2.0 に対応している他製品のインストール後に、CENTUM VP ソフトウェアをインストールするときは、IT セキュリティバージョンを維持することも、変更することもできます。

● CENTUM VP ソフトウェアをインストールしたあとに他製品をインストールする場合

CENTUM VP ソフトウェアのインストール時に IT セキュリティバージョン 2.0 の設定を行ったあと、IT セキュリティバージョン 2.0 に対応していない他製品のインストールで IT セキュリティ設定を行うときは、次の警告のダイアログボックスが表示されます。

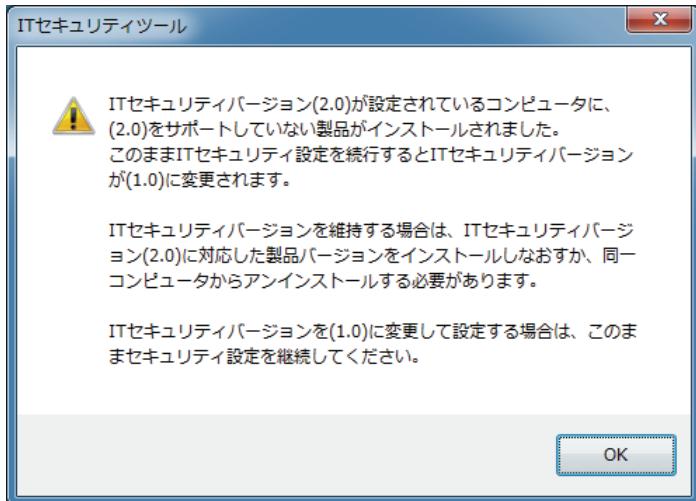


図 B4.7-5 警告のダイアログボックス

その場合は、IT セキュリティバージョンの指定を 1.0 に変更してください。

B4.8 ライセンスの配布と反映をする

ライセンスとは CENTUM VP のソフトウェアパッケージ使用権のことです。

各ステーションでパッケージを使用可能にするには、ライセンス管理ステーションからライセンス適用ステーションにライセンスを配布し、各ステーションでそれを反映する作業が必要です。この作業の結果、ソフトウェアを使用可能な状態にすることを、ソフトウェアパッケージの有効化と呼びます。

CENTUM VP システムでは、1 台のコンピュータをライセンス管理ステーションとし、他のコンピュータをライセンス適用ステーションとします。ライセンス管理ステーションは、HIS などのステーションと共に存させることができます。

参照

ライセンスの配布と反映については、以下を参照してください。

ライセンス管理 (IM 33J01C20-01JA) の「1.1.3 ライセンス管理の作業概要」

ライセンスのバージョンアップについては、以下を参照してください。

ライセンス管理 (IM 33J01C20-01JA) の「4. CENTUM VP R5 から R6、ProSafe-RS R3 から R4 へのライセンスの更新」

B4.9 ユーザアカウントを作成する

CENTUM VP を使用するユーザのアカウントを作成します。

IT セキュリティの標準モデルを選択した場合は、IT セキュリティツールにより、インストールされたフォルダ、レジストリなどに CENTUM VP のユーザグループでアクセス権が設定されます。そのため、作成したユーザを、エンジニア、保守員などの役割に応じた CENTUM VP のユーザグループに登録します。

ここでは、標準モデルのスタンドアロン管理および従来モデルのセキュリティ設定の場合の手順を説明します。

標準モデルのドメイン管理／併用管理の場合は、Windows のドメイン環境設定をする際に、ユーザアカウントを作成します。

参照

Windows ドメイン環境設定の際のユーザアカウント作成方法については、以下を参照してください。

「B2.5 ドメインユーザを作成する」ページ B2-16

■ CENTUM 認証モード指定時のユーザアカウント名の制限

- ・ 20 文字以内
- ・ スペース、タブなどの空白文字、半角カナ文字、漢字などのマルチバイトコードは使用しない

■ Windows 認証モード指定時のユーザアカウント名の制限

- ・ 16 文字以内
- ・ スペース、タブなどの空白文字、半角カナ文字、漢字などのマルチバイトコードは使用しない
- ・ 大文字のみ
- ・ ピリオドで終わることは不可

B4.9.1 標準モデル：スタンドアロン管理のセキュリティ設定の場合

スタンドアロン管理で標準モデルのセキュリティ設定を行う場合、コンピュータごとにユーザアカウントを作成します。

次にアカウント作成の手順を示します。

1. 管理者ユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [管理ツール] – [コンピューターの管理] を選択してください。
コンピューターの管理ウィンドウが表示されます。
4. ウィンドウ左側のツリービューで [システムツール] – [ローカルユーザーとグループ] – [ユーザー] を選択してください。
5. [操作] – [新しいユーザー] を選択してください。
新しいユーザーダイアログが表示されます。
6. ユーザアカウントを追加してください。(これ以降の手順では、"OPERATOR"というユーザアカウントを追加する例を示しています。)

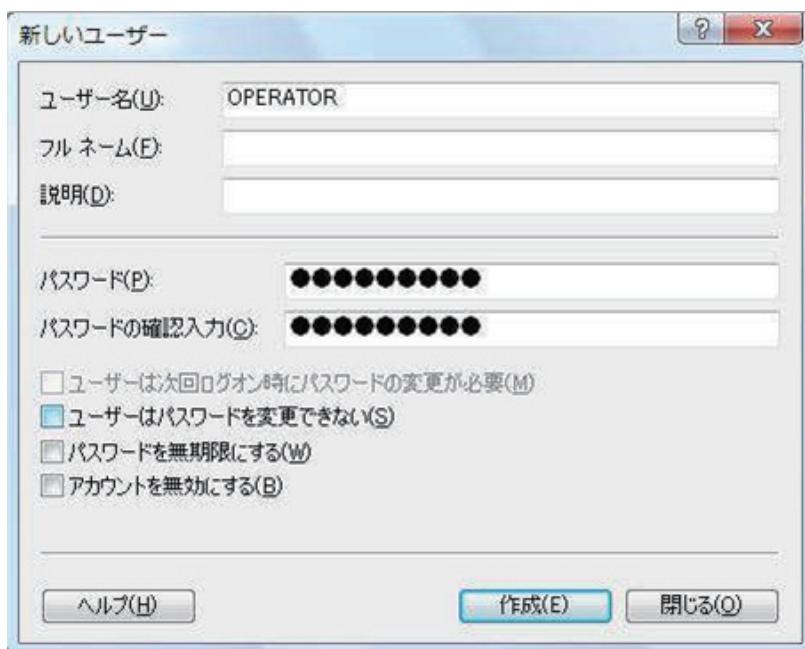


図 B4.9.1-1 新しいユーザーダイアログ

7. 新規に作成したユーザを右クリックして [プロパティ] を選択し、所属するグループタブの [追加] をクリックしてください。



図 B4.9.1-2 ユーザのプロパティ

8. 新規に追加したユーザを所属させる適切なグループを選択し、[OK] をクリックしてください。

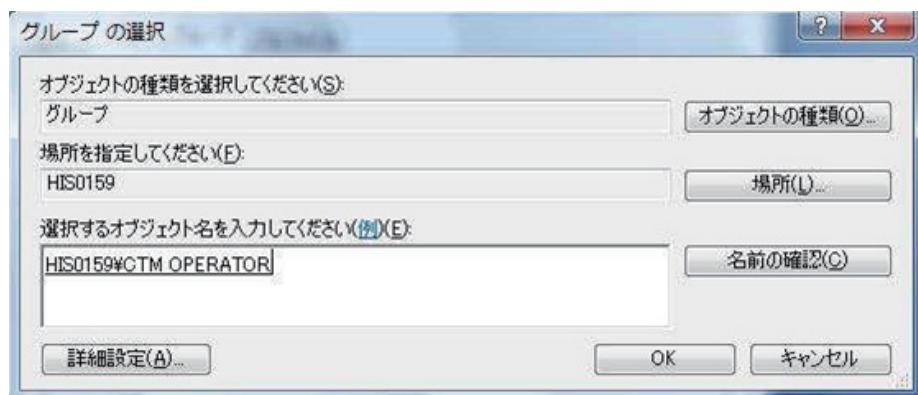


図 B4.9.1-3 グループの選択

補足

ユーザを管理者権限を持つグループ (CTM_MAINTENANCE、CTM_ENGINEER_ADMIN) に所属させる場合は、同時に Administrators グループにも所属させてください。

9. ユーザのプロパティダイアログで、選択したグループが [所属するグループ] に追加されたことを確認してください。

B4.9.2 従来モデルのセキュリティ設定の場合

アカウント名“CENTUM”が、IT セキュリティツールにより自動的に作成されています。デフォルトのパスワードは“Yokogawa1”が設定されていますので、初回のログオン時に適切なパスワードに変更してください。

また、エンジニアリング用として、専用のユーザアカウントを作成することができます。ユーザアカウントの作成手順については、スタンドアロン管理のコンピュータでユーザアカウントを作成する手順と同様です。ただし、従来モデルでは、Windows グループ CTM_ENGINEER は用意されていません。作成したユーザを Windows グループ CTM_ENGINEER に所属させる必要はありません。

参照

ユーザアカウントの作成手順については、以下を参照してください。

「B4.9.1 標準モデル：スタンドアロン管理のセキュリティ設定の場合」ページ B4-105

■ パスワードの有効期限の変更

従来モデルのセキュリティ設定の場合に作成されるアカウント“CENTUM”的パスワードの有効期限は無期限になっています。パスワードが期限切れになると HIS へのダウンロード、シーケンステーブルや SFC の状態表示ビューが正常に動作しなくなります。[パスワードを無期限にする] ことを推奨します。

次にパスワードを無期限にする手順を示します。

1. 管理者ユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [管理ツール] – [コンピューターの管理] を選択してください。
コンピューターの管理ウィンドウが表示されます。
4. [システムツール] の [ローカルユーザーとグループ] – [ユーザー] を選択してください。
5. CENTUM ユーザを選択し、プロパティを開いてください。



図 B4.9.2-1 CENTUM のプロパティ

6. [パスワードを無期限にする] チェックボックスをオンにして、[OK] をクリックしてください。

B4.10 ユーザごとの Windows 動作環境の設定をする

ユーザアカウントを作成後、ユーザごとに必要な Windows 動作環境の設定をしてください。

■ Windows の設定項目と各ステーションでの必要な設定

ユーザごとの Windows 設定項目は、ステーションの種類と OS によって異なります。実際の作業は、この表に基づいて行ってください。

表 B4.10-1 Windows 設定項目と各ステーションでの設定の要不要

Windows 設定項目	HIS	APCS	SIOS	GSGW	UGS	UACS ステーション	システム生成機能のみを搭載したコンピュータ	AD サーバのみを搭載したコンピュータ
Windows セキュリティセンター／アクションセンターの警告表示 (*1)	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes
画面のプロパティ(色)／デザイン／スクリーンセーバー／解像度	Yes	No	No	No	No	No	No	Yes
ディスプレイスケール	Yes	No	No	No	No (*2)	No	No	No
スクロール設定 (*3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
仮想デスクトップ (*3)	Yes (*4)	Yes (*5)	Yes (*4)	Yes (*4)				
Windows ファイアウォールのトラスト通知 (*6)	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes

*1: Windows 7、Windows Server 2008 R2、および Windows Server 2012 R2 のみ

*2: コンピュータ切替型 UGS では Yes です。

*3: Windows 10 と Windows Server 2016 のみ

*4: 仮想デスクトップを使用するかどうかに応じて、仮想デスクトップを使用する場合の設定、または仮想デスクトップを使用しない場合の設定を選択してください。

*5: 仮想デスクトップを使用しない場合の設定をしてください。

*6: Windows 10 かつ IT セキュリティモデルが従来モデルの場合に設定が必要です。

B4.10.1 Windows 10 で設定する

Windows 10 を使用するときは、次の設定方法に従ってください。

■ 画面のプロパティ

画面のプロパティの設定方法を次に示します。

1. 画面のプロパティを設定したいユーザーでサインインしてください。
2. コントロールパネルを起動してください。
3. 「デスクトップのカスタマイズ」 – 「個人用設定」を選択してください。
個人用設定ウィンドウが表示されます。



図 B4.10.1-1 個人用設定ウィンドウ

4. 「Windows の標準のテーマ」の「Windows」を選択してください。
5. 「デスクトップの背景」を選択してください。
Windows の設定ウィンドウが表示されます。

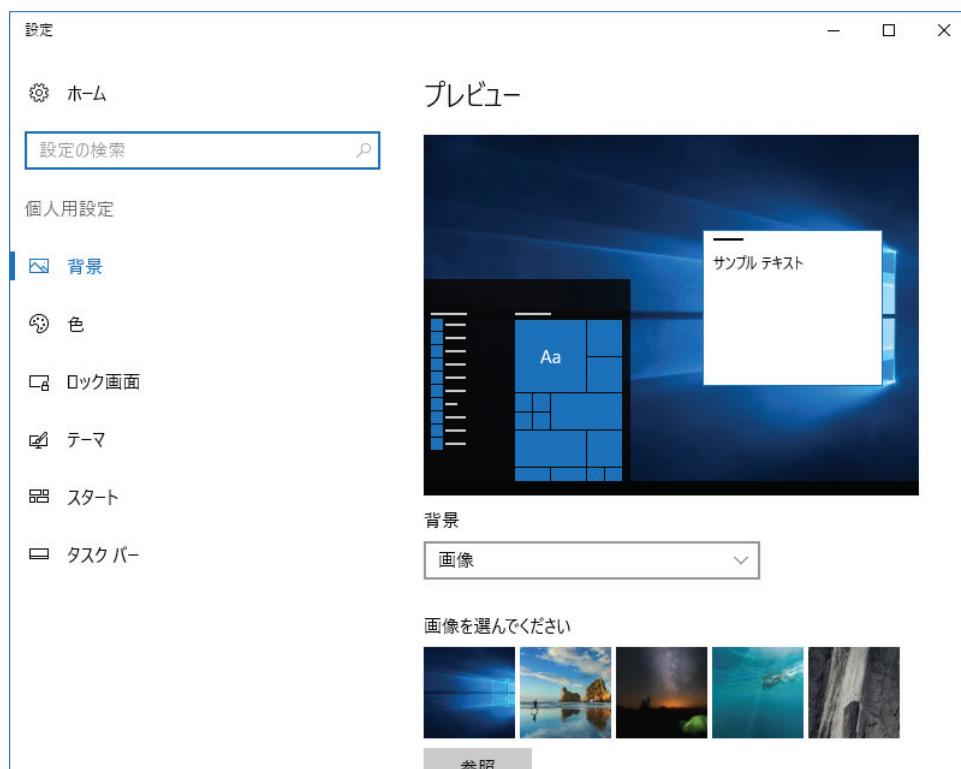


図 B4.10.1-2 設定ウィンドウ

6. [背景] ドロップダウンリストから [単色] を選択し、任意の背景色を選択してください。
7. [×] ボタンをクリックして、ウィンドウを終了してください。
個人用設定ウィンドウに戻ります。
8. [スクリーンセーバー] を選択してください。
スクリーンセーバーの設定ダイアログが表示されます。



図 B4.10.1-3 スクリーンセーバーの設定ダイアログ

9. [スクリーンセーバー] ドロップダウンリストから [(なし)] を選択して、[OK] をクリックしてください。
10. スタートメニューから Windows の設定ウィンドウを起動してください。
11. [システム] – [ディスプレイ] を選択してください。
12. 右ペインで [ディスプレイの詳細設定] をクリックしてください。
ディスプレイの詳細設定ページが表示されます。
13. 解像度を次のいずれかに設定して、[適用] をクリックしてください。
 - 通常モニタ : 1280 x 1024、1600 x 1200
 - ワイドモニタ : 1280 x 800、1440 x 900、1680 x 1050、1920x1080、1920 x 1200

■ ディスプレイスケール

ディスプレイスケールの設定方法を次に示します。

1. ディスプレイスケールを設定したいユーザでサインインしてください。
2. Windows の設定ウィンドウを起動してください。
3. [システム] – [ディスプレイ] を選択してください。
ディスプレイのカスタマイズページが表示されます。



図 B4.10.1-4 ディスプレイのカスタマイズページ

4. [テキスト、アプリ、その他の項目のサイズを変更する] のスライダーを調整して、100%にしてください。
5. [×] ボタンをクリックして、ウィンドウを終了してください。

■ 非アクティブウィンドウのスクロール設定

Windows 10 では、マウスホイールで、非アクティブウィンドウをスクロールできます。誤動作の原因になるので、この機能を停止します。

非アクティブウィンドウのスクロールを停止するときは、次の手順に従ってください。

1. 非アクティブウィンドウのスクロールを停止したいユーザでサインインしてください。
2. Windows の設定ウィンドウを起動してください。
3. [デバイス] を選択してください。
4. 左ペインで [マウスとタッチパッド] を選択してください。
マウスページが表示されます。



図 B4.10.1-5 マウスページ

5. [ホバーしたときに非アクティブウィンドウをスクロールする] をオフにしてください。
6. [×] ボタンをクリックして、ウィンドウを終了してください。

■ 仮想デスクトップ

Windows 10 では仮想デスクトップを使用できます。仮想デスクトップは、仮想的に複数のデスクトップを持つことができる機能です。複数のデスクトップを切り替えて、ディスプレイに表示できます。

当製品のソフトウェアを仮想デスクトップで使用することで、複数のデスクトップに別の操作監視ウィンドウを表示したり、操作監視ウィンドウと操作監視以外のウィンドウを別のデスクトップに表示したりできます。

当製品のソフトウェアを仮想デスクトップで使用する場合は、タスクバーにすべての仮想デスクトップのウィンドウを表示してください。

仮想デスクトップを使用しない場合は、タスクバーのタスクビューボタンを非表示にしてください。

重要

- ・ 仮想デスクトップで操作監視を行うときには注意事項があります。必ず注意事項を確認してください。
- ・ APCS、SIOS、GSGW、または UGS をセットアップする場合は、仮想デスクトップを使用しないでください。
- ・ ソリッドスタイルコンソールパッケージ、オープンスタイルコンソールパッケージ、8 ループ同時操作用パッケージ (AIP831 用) のソフトウェアを有効にしているときは、仮想デスクトップを使用できません。

参照

仮想デスクトップを使用するときの注意事項については、以下を参照してください。

操作監視リファレンス Vol.1 (IM 33J05A10-01JA) の「1. HIS 共通」の「■ Windows 10 と Windows Server 2016 の仮想デスクトップ」

● 仮想デスクトップを使用する場合の設定

仮想デスクトップを使用する場合は、タスクバーにすべての仮想デスクトップのウィンドウを表示してください。

タスクバーにすべての仮想デスクトップのウィンドウを表示するときは、次の手順に従ってください。

1. 仮想デスクトップを使用するユーザでサインインしてください。
2. Windows の設定ウィンドウを起動してください。
3. [システム] を選択してください。
4. 左ペインで [マルチタスク] を選択してください。
5. 右ペインの [仮想デスクトップ] の [タスクバーに次の場所で開いているウィンドウを表示する] ドロップダウンリストから「すべてのデスクトップ」を選択してください。

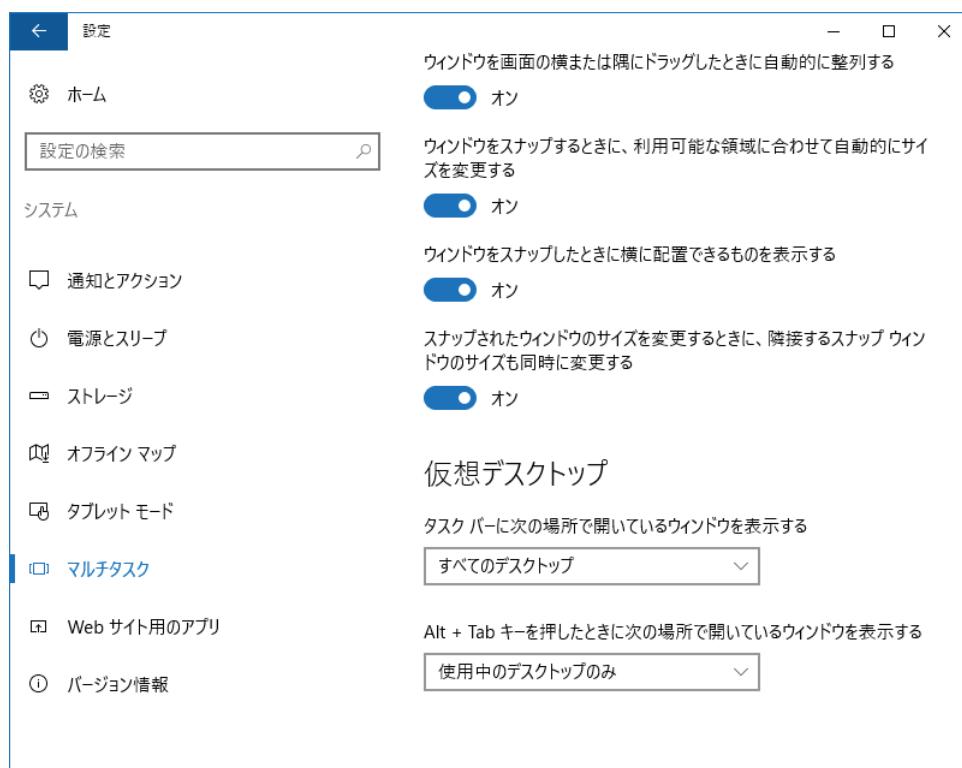


図 B4.10.1-6 設定ウィンドウ

6. [×] ボタンをクリックして、ウィンドウを終了してください。

● 仮想デスクトップを使用しない場合の設定

仮想デスクトップを使用しない場合は、タスクバーのタスクビューボタンを非表示にしてください。

重要

本操作をすると仮想デスクトップに対する操作ができなくなります。本操作をする前に仮想デスクトップが設定されていないことを確認してください。

タスクバーのタスクビューボタンを非表示にするときは、次の手順に従ってください。

1. 仮想デスクトップを使用しないユーザでサインインしてください。
2. デスクトップ下のタスクバーを右クリックし、[タスクビューボタンを表示] のチェックを外してください。



図 B4.10.1-7 タスクバーのコンテキストメニュー

■ Windows ファイアウォールのトースト通知に関する設定

IT セキュリティモデルが従来モデルの場合に、必要な設定です。

Windows ファイアウォールに関するトースト通知を抑制するときは、次の手順に従ってください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [Windows ファイアウォール] を選択してください。Windows ファイアウォールウィンドウが表示されます。
4. 左ペインで [Windows ファイアウォールの有効化または無効化] をクリックしてください。
5. プライベートネットワークの設定、パブリックネットワークの設定、ドメインネットワークの設定で、それぞれ [Windows ファイアウォールを無効にする] を選択してください。ただし、ドメインネットワークの設定は、ドメイン環境の場合のみ作業してください。
6. [OK] ボタンをクリックしてください。
7. Windows ファイアウォールに関するトースト通知を出さないようにしたいユーザでサインインし直してください。
8. コントロールパネルを起動してください。
9. [システムとセキュリティ] – [セキュリティとメンテナンス] を選択してください。セキュリティとメンテナスウィンドウが表示されます。
10. 左ペインで、[セキュリティとメンテナンスの設定を変更] をクリックしてください。
11. セキュリティメッセージの [ネットワークファイアウォール] のチェックボックスをクリアしてください。
12. [OK] ボタンをクリックしてください。

補足

- ・ [ネットワークファイアウォール] のチェックボックスがグレーアウトされている場合、有効になるまで数分お待ちください。
- ・ CENTUM デスクトップを設定したユーザでは、コントロールパネルを起動できません。設定を実施する場合は、CENTUM デスクトップを解除してから実施してください。
- ・ [Windows ファイアウォールを有効にする] というトースト通知が出たときは、このトースト通知をクリックせずに、上記の手順で対応してください。

B4.10.2 Windows 7 で設定する

Windows 7 を使用するときは、次の設定方法に従ってください。

■ Windows セキュリティセンター／アクションセンターの警告表示

Windows セキュリティセンターおよびアクションセンターは、コンピュータのセキュリティ保護に必要なすべての機能をまとめて管理します。

当製品のソフトウェアをインストールするコンピュータでは、Windows の自動更新を無効にすることを推奨しています。そのため、当製品のソフトウェアのインストール時に、Windows の自動更新が無効にされます。

Windows の自動更新が無効の場合は、Windows セキュリティセンターおよびアクションセンターから警告が通知されるため、警告表示を無効にする設定方法を示します。

重要

Windows の自動更新を有効にしたい場合は、当製品のソフトウェアのインストール後に、Windows の自動更新を手動で有効にする必要があります。その場合は、本設定は不要です。

補足

Windows セキュリティセンターおよびアクションセンターはクライアントセキュリティ監視サービスです。

1. Windows セキュリティセンターおよびアクションセンターの警告表示を無効にしたいユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. コントロールパネルの表示方法を小さいアイコンにしてください。
4. 表示される項目の中から、[通知領域アイコン] を選択してください。
通知領域アイコンウィンドウが表示されます。

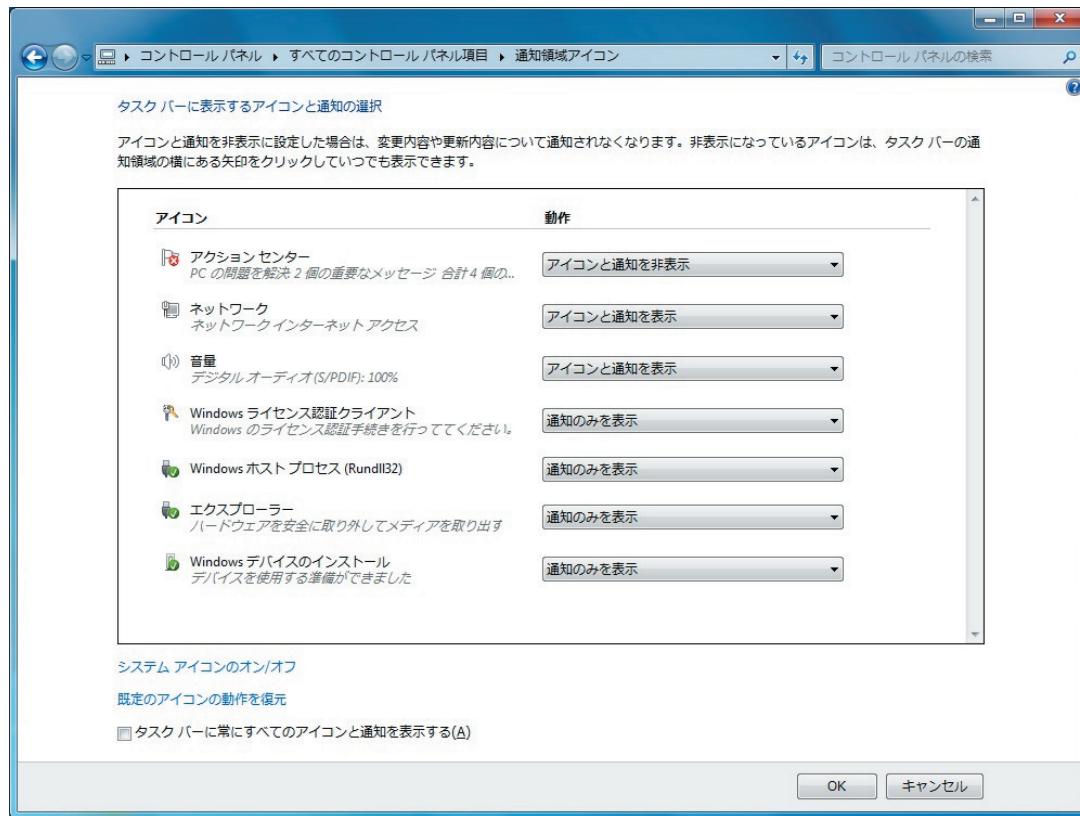


図 B4.10.2-1 通知領域アイコンウィンドウ

補足

アクションセンターの設定がグレーアウトされている場合、[タスクバーに常にすべてのアイコンと通知を表示する] をオフにしてください。このチェックボックスがオフであるにもかかわらず、グレーアウトされている場合は、有効になるまで数分お待ちください。

また、通知領域アイコンウィンドウにアクションセンターのアイコンが表示されていない場合、[システムアイコンのオン／オフ] をクリックし、表示されるウィンドウで [アクションセンター] の設定をオンにしてください。ここで設定がグレーアウトされている場合も、有効になるまで数分お待ちください。

- [アクションセンター] の設定を [アイコンと通知を非表示] として、[OK] をクリックしてください。

補足

ライセンス適用ステーションの場合、[LicenseAgent.TaskTray] の設定を [アイコンと通知を表示] としてください。

参照

Windows の自動更新を手動で有効にする手順については、以下を参照してください。

「■ Windows Update を有効にする」ページ C7-7

■ 画面のプロパティ

画面のプロパティの設定方法を次に示します。

- 画面のプロパティを設定したいユーザでログオンしてください。
- コントロールパネルを起動してください。
- [デスクトップのカスタマイズ] – [個人設定] を選択してください。
個人設定ウィンドウが表示されます。



図 B4.10.2-2 個人設定ウィンドウ

- [Aero テーマ] の [Windows 7] を選択してください。
- [個人設定] – [デスクトップの背景] を選択してください。
デスクトップの背景ウィンドウが表示されます。



図 B4.10.2-3 デスクトップの背景ウィンドウ

6. [画像の場所] の設定を [単色] にし、任意の色を選択して、[変更の保存] をクリックしてください。
7. [スクリーンセーバー] を選択してください。
スクリーンセーバーの設定ダイアログが表示されます。



図 B4.10.2-4 スクリーンセーバーの設定ダイアログ

8. [スクリーンセーバー] の設定を [(なし)] にして、[OK] をクリックしてください。
9. コントロールパネルを起動してください。
10. [デスクトップのカスタマイズ] – [ディスプレイ] – [解像度の調整] を選択してください。
画面の解像度選択ウィンドウが表示されます。
11. 解像度を次のいずれかに設定して、[OK] をクリックしてください。

- 通常モニタ：1280 x 1024、1600 x 1200
 - ワイドモニタ：1280 x 800、1440 x 900、1680 x 1050、1920 x 1080、1920 x 1200
12. [ディスプレイ] – [解像度の調整] – [詳細設定] を選択してください。
詳細設定ダイアログが表示されます。

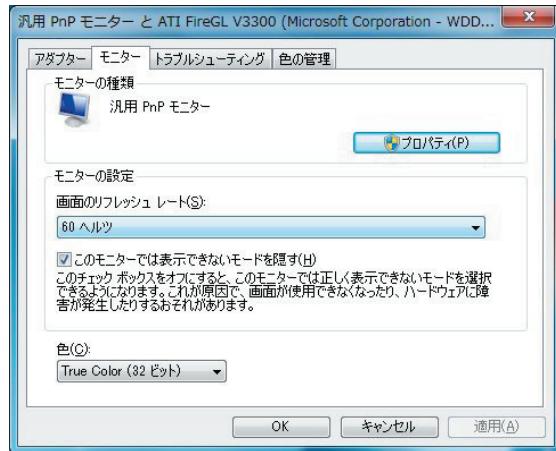


図 B4.10.2-5 詳細設定ダイアログ

13. [モニター] タブを選択して、[色] の設定を [True Color (32 ビット)] にして、[OK] をクリックしてください。

■ ディスプレイスケール

ディスプレイスケールの設定方法を次に示します。

- ディスプレイスケールを設定したいユーザでログオンしてください。
- コントロールパネルを起動してください。
- [デスクトップのカスタマイズ] – [ディスプレイ] を選択してください。
ディスプレイウィンドウが表示されます。

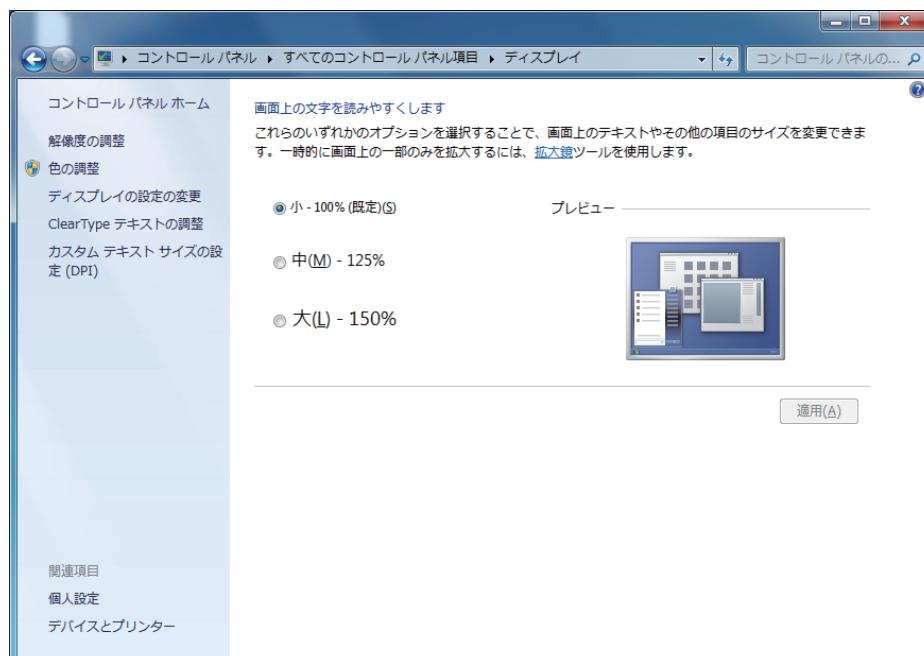


図 B4.10.2-6 ディスプレイウィンドウ

4. [小 – 100%] を選択してください。

B4.10.3 Windows Server 2016 で設定する

Windows Server 2016 を使用するときは、次の設定方法に従ってください。

■ 画面のプロパティ

画面のプロパティの設定方法を次に示します。

1. 画面のプロパティを設定したいユーザーでサインインしてください。
2. コントロールパネルを起動してください。
3. 「デスクトップのカスタマイズ」 – 「個人用設定」を選択してください。
個人用設定ウィンドウが表示されます。



図 B4.10.3-1 個人用設定ウィンドウ

4. [Windows の標準のテーマ] の [Windows] を選択してください。
5. [デスクトップの背景] を選択してください。
Windows の設定ウィンドウが表示されます。

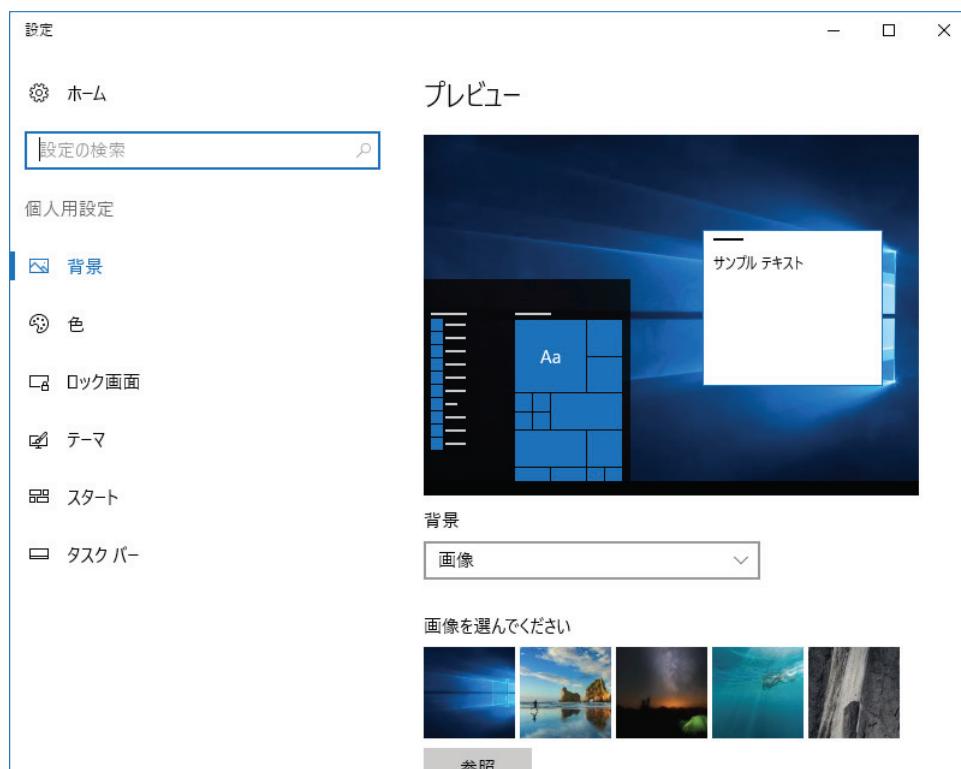


図 B4.10.3-2 設定ウィンドウ

6. [背景] ドロップダウンリストから [単色] を選択し、任意の背景色を選択してください。
7. [×] ボタンをクリックして、ウィンドウを終了してください。
個人用設定ウィンドウに戻ります。
8. [スクリーンセーバー] を選択してください。
スクリーンセーバーの設定ダイアログが表示されます。



図 B4.10.3-3 スクリーンセーバーの設定ダイアログ

9. [スクリーンセーバー] ドロップダウンリストから [(なし)] を選択して、[OK] をクリックしてください。
10. スタートメニューから Windows の設定ウィンドウを起動してください。
11. [システム] – [ディスプレイ] を選択してください。
12. 右ペインで [ディスプレイの詳細設定] をクリックしてください。
ディスプレイの詳細設定ページが表示されます。
13. 解像度を次のいずれかに設定して、[適用] をクリックしてください。
 - 通常モニタ : 1280 x 1024、1600 x 1200
 - ワイドモニタ : 1280 x 800、1440 x 900、1680 x 1050、1920x1080、1920 x 1200

■ ディスプレイスケール

ディスプレイスケールの設定方法を次に示します。

1. ディスプレイスケールを設定したいユーザでサインインしてください。
2. Windows の設定ウィンドウを起動してください。
3. [システム] – [ディスプレイ] を選択してください。
ディスプレイのカスタマイズページが表示されます。



図 B4.10.3-4 ディスプレイのカスタマイズページ

4. [テキスト、アプリ、その他の項目のサイズを変更する] のスライダーを調整して、100%にしてください。
5. [×] ボタンをクリックして、ウィンドウを終了してください。

■ 非アクティブウィンドウのスクロール設定

Windows Server 2016 では、マウスホイールで、非アクティブウィンドウをスクロールできます。誤動作の原因になるので、この機能を停止します。

非アクティブウィンドウのスクロールを停止するときは、次の手順に従ってください。

1. 非アクティブウィンドウのスクロールを停止したいユーザでサインインしてください。
2. Windows の設定ウィンドウを起動してください。
3. [デバイス] を選択してください。
4. 左ペインで [マウスとタッチパッド] を選択してください。
マウスページが表示されます。

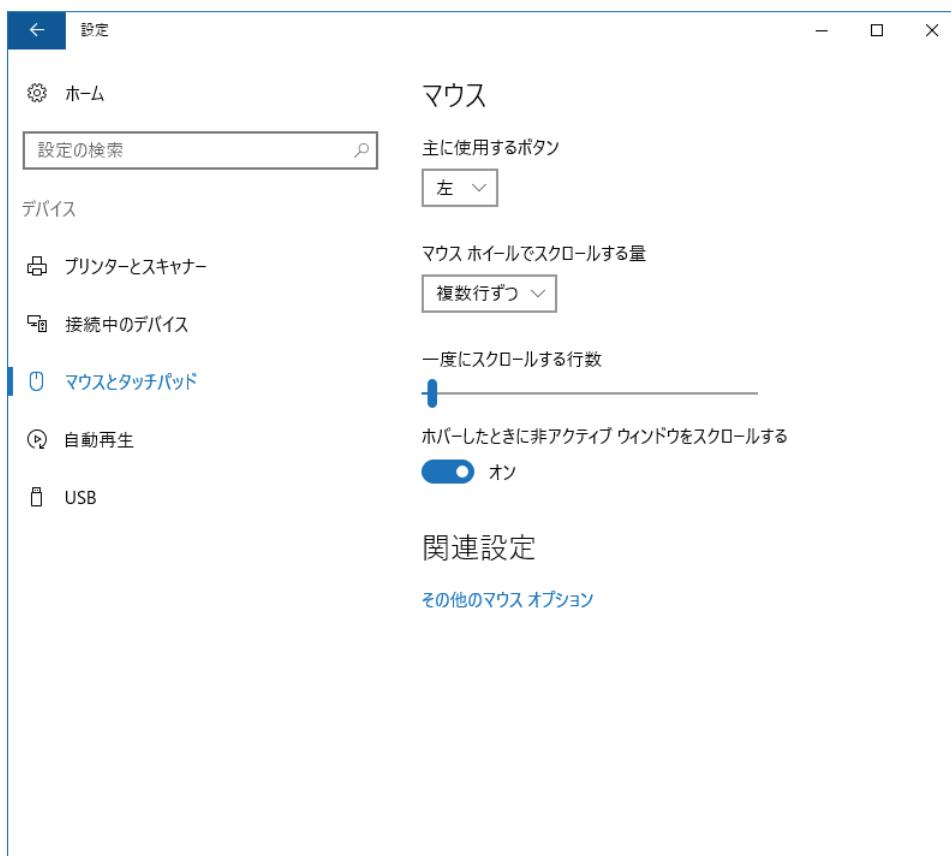


図 B4.10.3-5 マウスページ

5. [ホバーしたときに非アクティブウィンドウをスクロールする] をオフにしてください。
6. [×] ボタンをクリックして、ウィンドウを終了してください。

■ 仮想デスクトップ

Windows Server 2016 では仮想デスクトップを使用できます。仮想デスクトップは、仮想的に複数のデスクトップを持つことができる機能です。複数のデスクトップを切り替えて、ディスプレイに表示できます。

当製品のソフトウェアを仮想デスクトップで使用することで、複数のデスクトップに別の操作監視ウィンドウを表示したり、操作監視ウィンドウと操作監視以外のウィンドウを別のデスクトップに表示したりできます。

当製品のソフトウェアを仮想デスクトップで使用する場合は、タスクバーにすべての仮想デスクトップのウィンドウを表示してください。

仮想デスクトップを使用しない場合は、タスクバーのタスクビューボタンを非表示にしてください。

重要

- ・ 仮想デスクトップで操作監視を行うときには注意事項があります。必ず注意事項を確認してください。
- ・ APCS、SIOS、GSGW、または UGS をセットアップする場合は、仮想デスクトップを使用しないでください。
- ・ ソリッドスタイルコンソールパッケージ、オープンスタイルコンソールパッケージ、8 ループ同時操作用パッケージ (AIP831 用) のソフトウェアを有効にしているときは、仮想デスクトップを使用できません。

参照

仮想デスクトップを使用するときの注意事項については、以下を参照してください。

操作監視リファレンス Vol.1 (IM 33J05A10-01JA) の「1. HIS 共通」の「■ Windows 10 と Windows Server 2016 の仮想デスクトップ」

● 仮想デスクトップを使用する場合の設定

仮想デスクトップを使用する場合は、タスクバーにすべての仮想デスクトップのウィンドウを表示してください。

タスクバーにすべての仮想デスクトップのウィンドウを表示するときは、次の手順に従ってください。

1. 仮想デスクトップを使用するユーザでサインインしてください。
2. Windows の設定ウィンドウを起動してください。
3. [システム] を選択してください。
4. 左ペインで [マルチタスク] を選択してください。
5. 右ペインの [仮想デスクトップ] の [タスクバーに次の場所で開いているウィンドウを表示する] ドロップダウンリストから「すべてのデスクトップ」を選択してください。

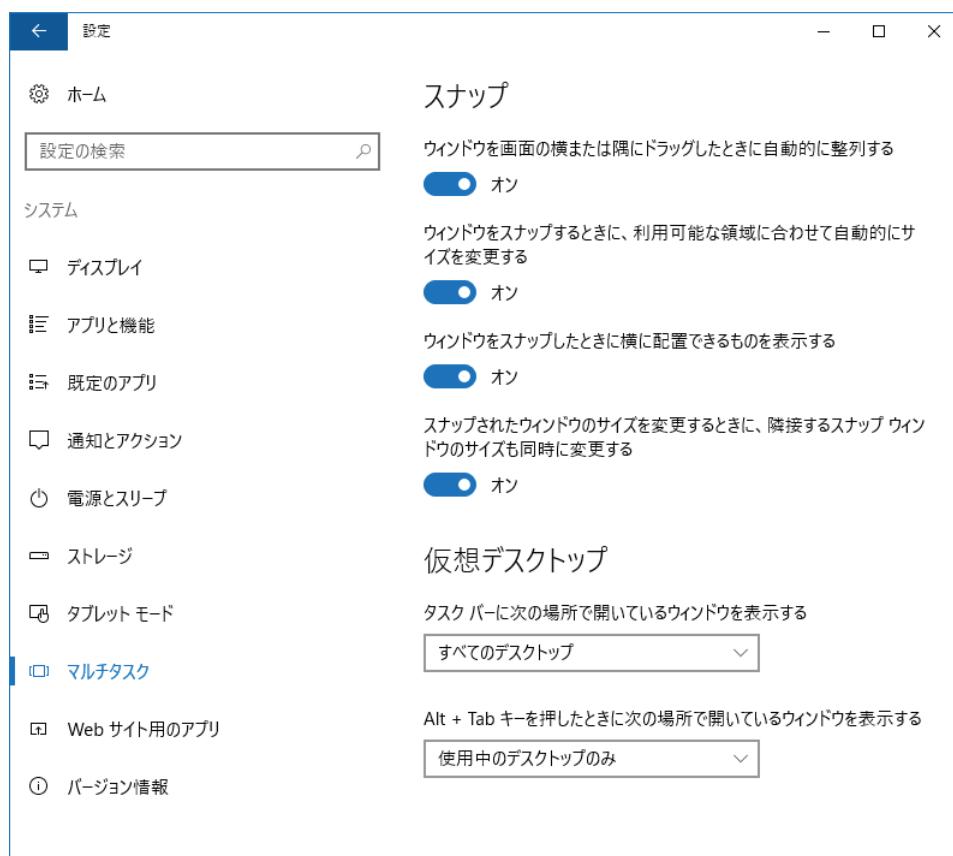


図 B4.10.3-6 設定ウィンドウ

6. [×] ボタンをクリックして、ウィンドウを終了してください。

● 仮想デスクトップを使用しない場合の設定

仮想デスクトップを使用しない場合は、タスクバーのタスクビュー ボタンを非表示にしてください。

重要

本操作をすると仮想デスクトップに対する操作ができなくなります。本操作をする前に仮想デスクトップが設定されていないことを確認してください。

タスクバーのタスクビューボタンを非表示にするときは、次の手順に従ってください。

1. 仮想デスクトップを使用しないユーザーでサインインしてください。
2. デスクトップ下のタスクバーを右クリックし、[タスクビューボタンを表示] のチェックを外してください。

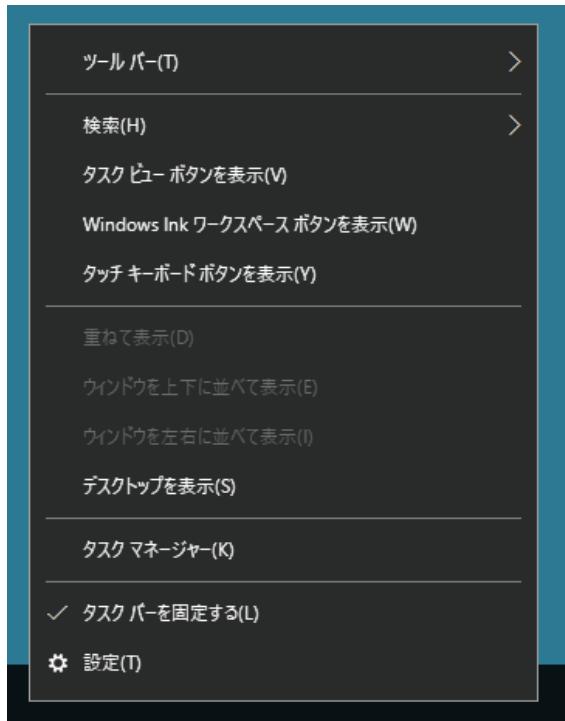


図 B4.10.3-7 タスクバーのコンテキストメニュー

B4.10.4 Windows Server 2012 R2 で設定する

Windows Server 2012 R2 を使用するときは、次の設定方法に従ってください。

補足

Windows Server 2012 R2 は、コンピュータ切替型 UGS のみサポートです。

■ Windows セキュリティセンター／アクションセンターの警告表示

Windows セキュリティセンター、およびアクションセンターは、コンピュータのセキュリティ保護に必要なすべての機能をまとめて管理します。

当製品のソフトウェアをインストールするコンピュータでは、Windows の自動更新を無効にすることを推奨しています。そのため、当製品のソフトウェアのインストール時に、Windows の自動更新が無効にされます。

Windows の自動更新が無効の場合は、Windows セキュリティセンターおよびアクションセンターから警告が通知されるため、警告表示を無効にする設定方法を示します。

重要

Windows の自動更新を有効にしたい場合は、当製品のソフトウェアのインストール後に、Windows の自動更新を手動で有効にする必要があります。その場合は、本設定は不要です。

補足

Windows セキュリティセンター、およびアクションセンターは、クライアントセキュリティ監視サービスです。

1. Windows セキュリティセンター、およびアクションセンターの警告表示を無効にしたいユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. コントロールパネルの表示方法を小さいアイコンにしてください。
4. 表示される項目の中から、[通知領域アイコン] を選択してください。
通知領域アイコンウインドウが表示されます。

補足

アクションセンターの設定がグレーアウトされている場合、[タスクバーに常にすべてのアイコンと通知を表示する] をオフにしてください。このチェックボックスがオフであるにもかかわらず、グレーアウトされている場合は、有効になるまで数分お待ちください。

また、通知領域アイコンウインドウにアクションセンターのアイコンが表示されていない場合、[システムアイコンのオン／オフ] をクリックし、表示されるウインドウで [アクションセンター] の設定をオンにしてください。ここで設定がグレーアウトされている場合も、有効になるまで数分お待ちください。

5. [アクションセンター] の設定を [アイコンと通知を非表示] として、[OK] をクリックしてください。

補足

ライセンス適用ステーションの場合、[LicenseAgent.TaskTray] の設定を [アイコンと通知を表示] としてください。

参照

Windows の自動更新を手動で有効にする手順については、以下を参照してください。

「■ Windows Update を有効にする」ページ C7-7

■ 画面のプロパティ

画面のプロパティの設定方法を次に示します。

1. 画面のプロパティを設定したいユーザでサインインしてください。

2. コントロールパネルを起動してください。
3. [ハードウェア] – [ディスプレイ] – [デスクトップ背景の変更] を選択してください。
デスクトップの背景ウィンドウが表示されます。
4. [画像の場所] の設定を [単色] にし、任意の色を選択して、[変更の保存] をクリックしてください。
5. [スクリーンセーバーの変更] を選択してください。
スクリーンセーバーの設定ダイアログが表示されます。
6. [スクリーンセーバー] の設定を [(なし)] にして、[OK] をクリックしてください。
7. コントロールパネルで [ハードウェア] – [ディスプレイ] – [解像度の調整] を選択してください。
画面の解像度ウィンドウが表示されます。
8. 解像度を 1024 x 768 に設定して、[OK] をクリックしてください。
9. [変更を維持する] をクリックしてください。

■ ディスプレイスケール

ディスプレイスケールの設定方法を次に示します。

1. ディスプレイスケールを設定したいユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [ハードウェア] – [ディスプレイ] を選択してください。
ディスプレイウィンドウが表示されます。
4. [すべてのディスプレイで同じ拡大率を使用する] のチェックボックスをオンにして、
[小–100%] を選択してください。

B4.10.5 Windows Server 2008 R2 で設定する

Windows Server 2008 R2 を使用するときは、次の設定方法に従ってください。

■ Windows セキュリティセンター／アクションセンターの警告表示

Windows セキュリティセンターおよびアクションセンターは、コンピュータのセキュリティ保護に必要なすべての機能をまとめて管理します。

当製品のソフトウェアをインストールするコンピュータでは、Windows の自動更新を無効にすることを推奨しています。そのため、当製品のソフトウェアのインストール時に、Windows の自動更新が無効にされます。

Windows の自動更新が無効の場合は、Windows セキュリティセンターおよびアクションセンターから警告が通知されるため、警告表示を無効にする設定方法を示します。

重要

Windows の自動更新を有効にしたい場合は、当製品のソフトウェアのインストール後に、Windows の自動更新を手動で有効にする必要があります。その場合は、本設定は不要です。

補足

Windows セキュリティセンターおよびアクションセンターはクライアントセキュリティ監視サービスです。

1. Windows セキュリティセンターおよびアクションセンターの警告表示を無効にしたいユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. コントロールパネルの表示方法を小さいアイコンにしてください。
4. 表示される項目の中から、[通知領域アイコン] を選択してください。
通知領域アイコンウィンドウが表示されます。

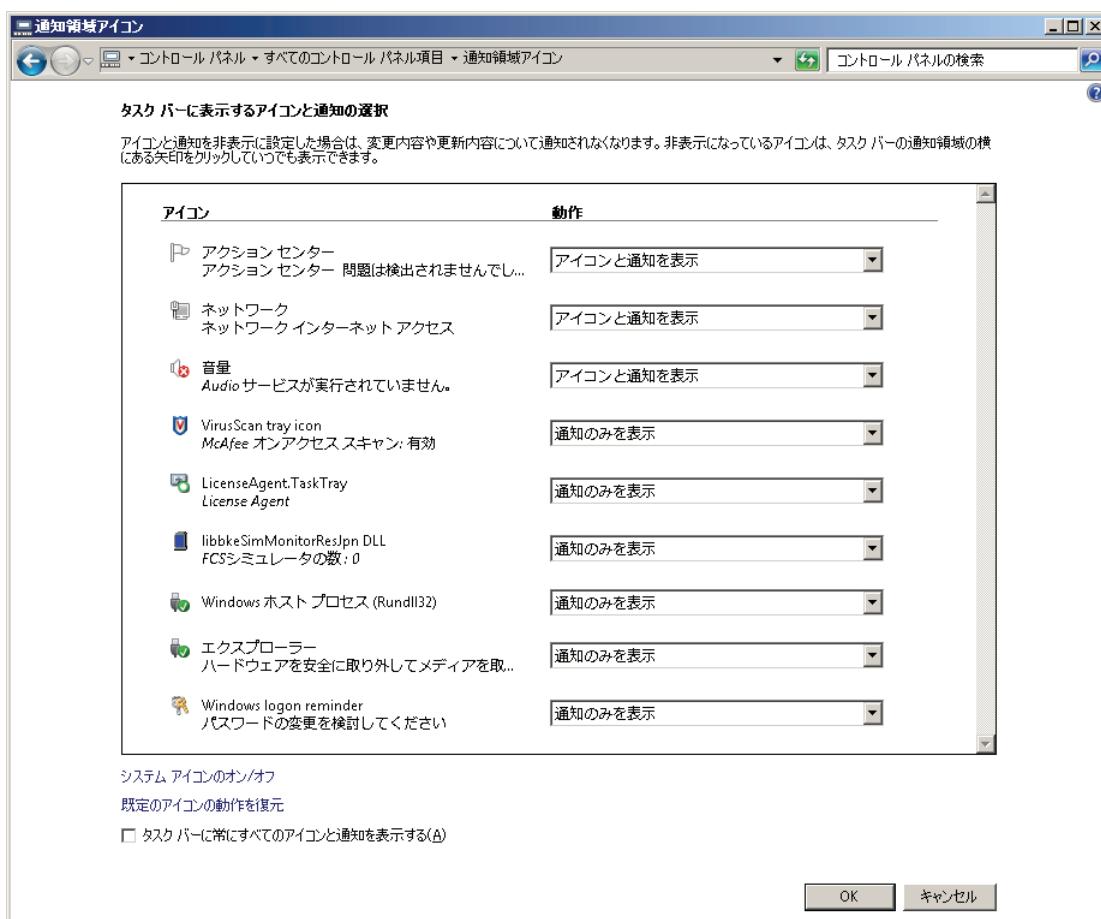


図 B4.10.5-1 通知領域アイコンウィンドウ

補足

アクションセンターの設定がグレーアウトされている場合、[タスクバーに常にすべてのアイコンと通知を表示する] をオフにしてください。このチェックボックスがオフであるにもかかわらず、グレーアウトされている場合は、有効になるまで数分お待ちください。

また、通知領域アイコンウィンドウにアクションセンターのアイコンが表示されていない場合、[システムアイコンのオン/オフ] をクリックし、表示されるウィンドウで [アクションセンター] の設定をオンにしてください。ここでの設定がグレーアウトされている場合も、有効になるまで数分お待ちください。

- [アクションセンター] の設定を [アイコンと通知を非表示] として、[OK] をクリックしてください。

補足

ライセンス適用ステーションの場合、[LicenseAgent.TaskTray] の設定を [アイコンと通知を表示] としてください。

参照

Windows の自動更新を手動で有効にする手順については、以下を参照してください。

「■ Windows Update を有効にする」ページ C7-7

■ 画面のプロパティ

画面のプロパティの設定方法を次に示します。

- 画面のプロパティを設定したいユーザでログオンしてください。
- コントロールパネルを起動してください。
- [ハードウェア] – [ディスプレイ] – [デスクトップ背景の変更] を選択してください。

デスクトップの背景ウィンドウが表示されます。

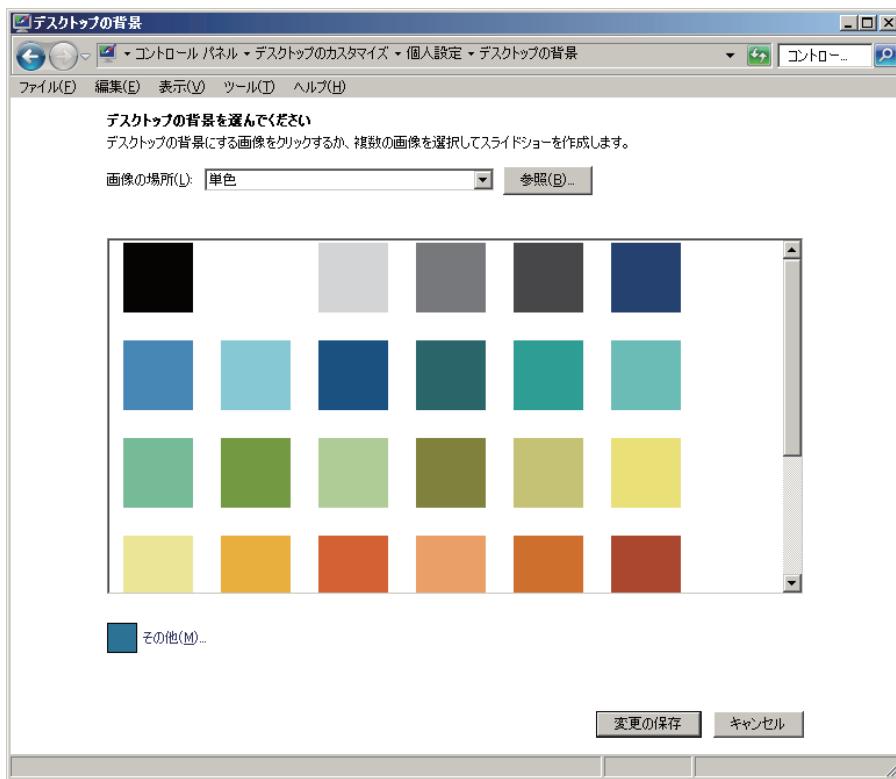


図 B4.10.5-2 デスクトップの背景ウィンドウ

4. [画像の場所] の設定を [単色] にし、任意の色を選択して、[変更の保存] をクリックしてください。
5. [スクリーンセーバー] を選択してください。
スクリーンセーバーの設定ダイアログが表示されます。



図 B4.10.5-3 スクリーンセーバーの設定ダイアログ

6. [スクリーンセーバー] の設定を [(なし)] にして、[OK] をクリックしてください。
7. コントロールパネルで [ハードウェア] – [ディスプレイ] – [解像度の調整] を選択してください。
画面の解像度ウィンドウが表示されます。

8. 解像度を次のいずれかに設定して、[OK] をクリックしてください。
 - ・ 通常モニタ：1280 x 1024、1600 x 1200
 - ・ ワイドモニタ：1280 x 800、1440 x 900、1680 x 1050、1920x1080、1920 x 1200
9. [変更を維持する] をクリックしてください。
10. [ディスプレイ] – [解像度の調整] – [詳細設定] を選択してください。
詳細設定ダイアログが表示されます。

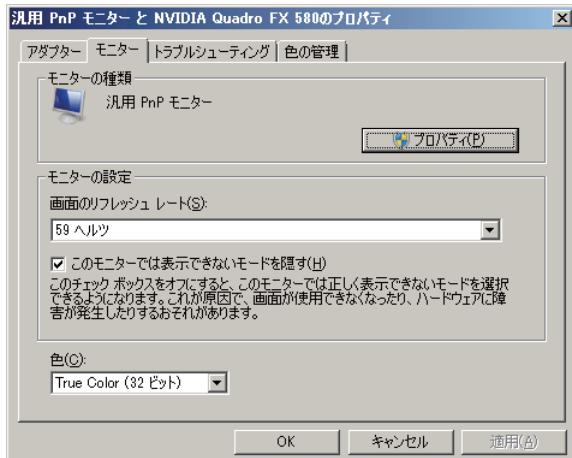


図 B4.10.5-4 詳細設定ダイアログ

11. [モニター] タブを選択して、[色] の設定を [True Color (32 ビット)] にして、[OK] をクリックしてください。

■ ディスプレイスケール

ディスプレイスケールの設定方法を次に示します。

1. ディスプレイスケールを設定したいユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. [ハードウェア] – [ディスプレイ] を選択してください。
ディスプレイウィンドウが表示されます。

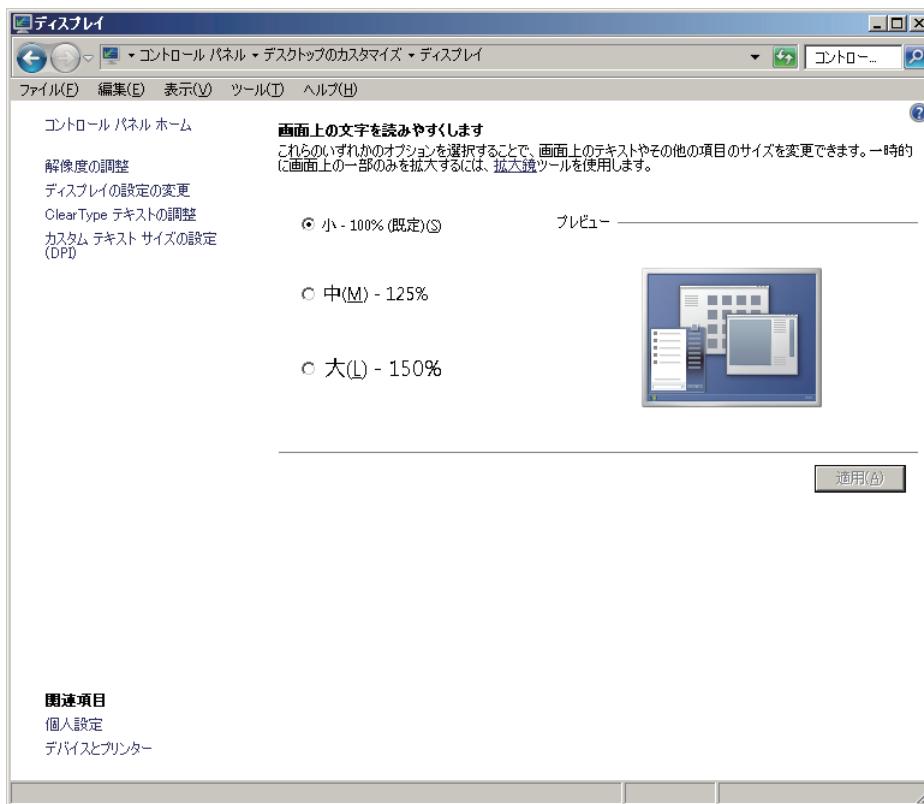


図 B4.10.5-5 ディスプレイウィンドウ

4. [小 - 100%] を選択してください。

B4.11 ユーザ認証モードの設定をする

ここでは、ユーザ認証モードの設定方法について説明します。

■ ユーザ認証モードについて

ITセキュリティ設定のセキュリティモデルで標準モデルを選択した場合、ユーザ認証モードを、次の2種類から選択できます。

- ・ CENTUM 認証モード
- ・ Windows 認証モード

デフォルトはCENTUM認証モードです。

セキュリティモデルとして従来モデルを選んだ場合は、ユーザ認証モードはCENTUM認証モード固定になります。

表 B4.11-1 用語の説明

用語	説明
Windows 認証モード	ユーザ認証を Windows の標準機能で行います。
CENTUM 認証モード	ユーザ認証を CENTUM 独自の方法で行います。R4.02までのユーザ認証と同一です。
HIS タイプシングルサインオン	ユーザ認証モードで Windows 認証モードを選択した場合に、選択できるユーザインのタイプの1つです。HISのユーザインダイアログを利用します。
Windows タイプシングルサインオン	ユーザ認証モードで Windows 認証モードを選択した場合に、選択できるユーザインのタイプの1つです。Windowsのログオンダイアログを利用します。
HIS グループユーザ	セキュリティビルダで管理し、操作監視機能でユーザイン・ユーザアウトするユーザを「HIS グループユーザ」と呼びます。
ENG グループユーザ	アクセス制限パッケージまたはFDA:21 CFR Part 11 対応パッケージを有効化している際の次のユーザを総称して「ENG グループユーザ」と呼びます。 <ul style="list-style-type: none"> ・システム生成機能を利用するシステムエンジニア ・処方機能を利用する処方エンジニア ・帳票機能を使用する帳票ユーザ
ENG グループユーザ 登録ビルダ	アクセス制限パッケージまたはFDA:21 CFR Part 11 対応パッケージを有効化している際の次のビルダを総称して「ENG グループユーザ登録ビルダ」と呼びます。 <ul style="list-style-type: none"> ・(システムエンジニアの) エンジニア登録ビルダ ・(処方エンジニアの) エンジニア登録ビルダ ・(帳票ユーザの) ユーザ登録ビルダ

参照

ユーザ認証モードについては、以下を参照してください。

- ・ CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「4.1 セキュリティを設定する前に考慮する項目」
- ・ 操作監視リファレンス Vol.1 (IM 33J05A10-01JA) の「1.1 HIS の起動、終了」

● ユーザ管理方法とパスワード

ユーザ管理方法とパスワードは、すべてのコンピュータで統一してください。

次はその注意事項です。

- ・ 同一プロジェクト内で R4.02 以前のソフトウェアパッケージをインストールしたコンピュータと混在させる場合：
ユーザ認証モードは、CENTUM 認証モードとしてください。

補足

R4.02 以前のソフトウェアパッケージをインストールしたコンピュータとは、次のパッケージのいずれかをインストールしたコンピュータを指します。

- ・ 操作監視基本機能 (LHS1100/LHM1101) およびこのパッケージの共存を必要とするオプションパッケージ
- ・ ビルダ基本機能 (LHS5100/LHM5100) およびこのパッケージの共存を必要とするオプションパッケージ
- ・ リモート操作監視サーバ機能 (LHS1150/LHM1150)
- ・ 帳票パッケージ (LHS6530)
- ・ CS Batch 3000 ビルダパッケージ (LHS5160)
- ・ CS Batch 3000 処方管理パッケージ (LHS5161)
- ・ CS Batch 3000 プロセス管理パッケージ (LHS6600/LHM6600)
- ・ アクセス制限パッケージ (LHS5110)
- ・ FDA:21 CFR Part 11 対応パッケージ (LHS5170)

-
- ・ R3.60 以前の Exaopc と Windows 認証モードの CENTUM をシステム内に混在させる場合 :

CENTUM 認証のパスワード管理を個別管理に変更したあとに、Windows 認証モードに変更してください。

CENTUM 認証時に設定したパスワードは、変更できません。

ユーザを追加した場合、追加したユーザは、パスワードなし認証となります。

Exaopc R3.60 が参照するプロジェクトファイルが存在するコンピュータは、CreateOPCProcess ツールを利用して、OPC_PROCESS ユーザを作成し、CTM_OPCT グループに登録してください。

- ・ Windows 認証モードを使用する場合 :

Windows ドメイン管理または、スタンドアロン管理のどちらかに統一してください。

1 つのプロジェクトで運用する Windows ドメインは 1 つにしてください。ただし、1 つの Windows ドメインで複数プロジェクトを運用することは可能です。(Windows ドメイン : プロジェクト = 1 : N)

B4.11.1 CENTUM 認証モードの設定をする

ここでは、CENTUM 認証モードの設定について説明します。

■ CENTUM 認証モードの設定

IT セキュリティ設定のセキュリティモデルで標準モデルを選択した場合、デフォルトの認証モードは CENTUM 認証モードになっています。

セットアップ後にプロジェクトを作成した際、プロジェクトのプロパティダイアログで、ユーザ認証方式欄にある [Windows ユーザと HIS グループユーザを連携させる] チェックボックスがオフになっていることを確認してください。

また、アクセス制限ユーティリティのアクセス制限タブで、[Windows ユーザと HIS グループユーザを連携させる] チェックボックスがオフになっていることを確認してください。

参照

HIS グループユーザの登録については、以下を参照してください。

エンジニアリングリファレンス Vol.1 (IM 33J10D10-01JA) の「2.2 プロジェクトの作成」の「■ プロジェクトの名前と位置」の「● ユーザ認証方式の設定」

ENG グループユーザの登録については、以下を参照してください。

FDA : 21CFR Part11 対応リファレンス (IM 33J10D21-01JA) の「4.3 エンジニア登録ビルダ」

■ 操作監視機能の自動起動の設定

CENTUM 認証モードで、Windows にログオンしたときに操作監視機能が自動的に起動するようにするには、HIS ユーティリティで次の設定をしてください。なお、コンピュータが制御バスに接続されていない場合は、操作監視機能の自動起動はできません。

1. 管理者ユーザでログオンしてください。
2. HIS ユーティリティを起動してください。
3. [ユーザ] タブを選択し、[設定] をクリックしてください。
ユーザ環境設定ダイアログが表示されます。
4. [追加] をクリックしてください。
ユーザの追加ダイアログが表示されます。

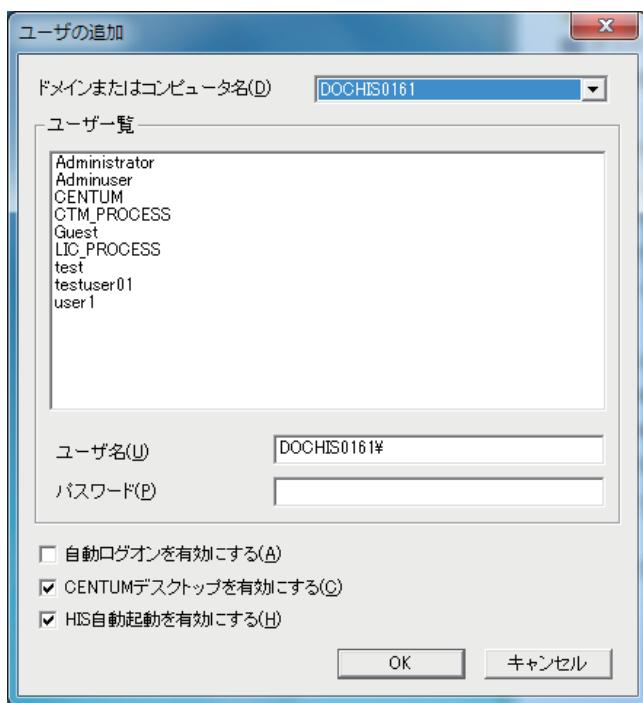


図 B4.11.1-1 ユーザの追加ダイアログ

5. [ドメインまたはコンピュータ名] のドロップダウンリストから、Windows ドメイン名またはローカルコンピュータ名を選択してください。
6. 設定を行いたいユーザ名を選択し、パスワードを入力してください。
7. [HIS 自動起動を有効にする] チェックボックスをオンにし、[OK] をクリックしてください。

補足

[OK] をクリックしたあと、「ログオンされたことが無いユーザを追加した場合は、終了までに時間がかかることがあります。」という警告メッセージが表示されます。

8. 他にもログオン時に操作監視機能を自動起動するユーザを追加する場合は、手順 5.～7.の操作を繰り返してください。
9. [OK] をクリックし、HIS ユーティリティを終了させてください。

B4.11.2 Windows 認証モードの設定をする

Windows 認証モードに関する設定について説明します。

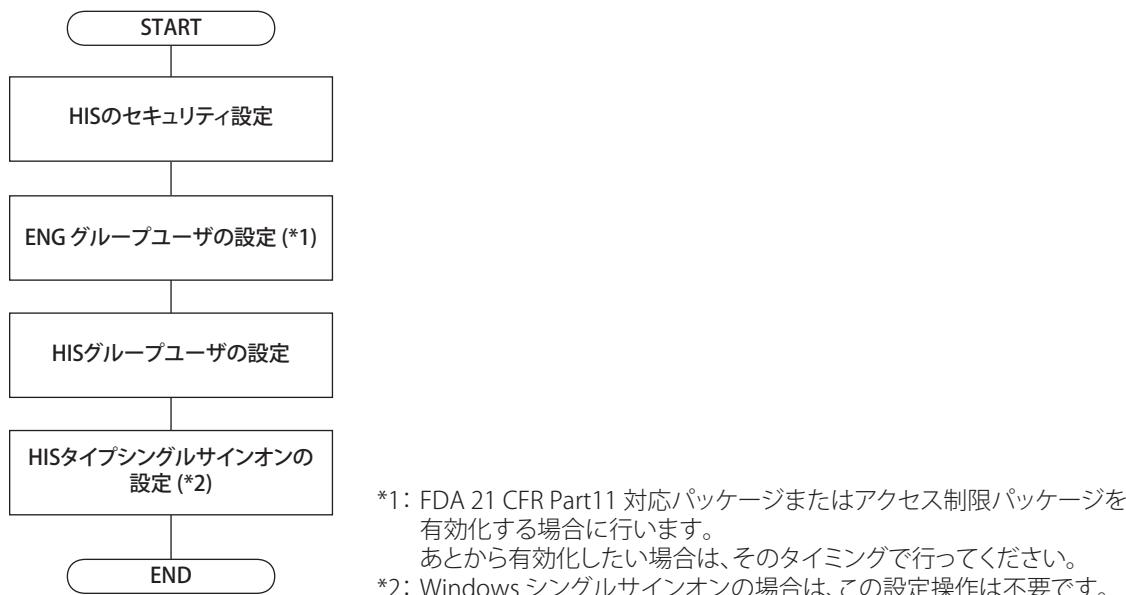


図 B4.11.2-1 作業の流れ

補足

HIS タイプシングルサインオンの場合、スタートメニューの権限は OFFUSER のときと同様です。ユーザインしても切り替わりません。
Windows タイプシングルサインオンの場合もスタートメニューの権限は、ログオンしたユーザの権限のままです。

参照

スタートメニューの権限については、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「3.1.1 ファイル／フォルダに対するアクセス許可」の「■ プログラムのアクセス許可」

■ HIS のセキュリティ設定

操作監視基本機能を有効化している場合に、各コンピュータで実施してください。

1. CTM_MAINTENANCE グループのユーザでログオンしてください。
2. HIS ユーティリティを起動してください。

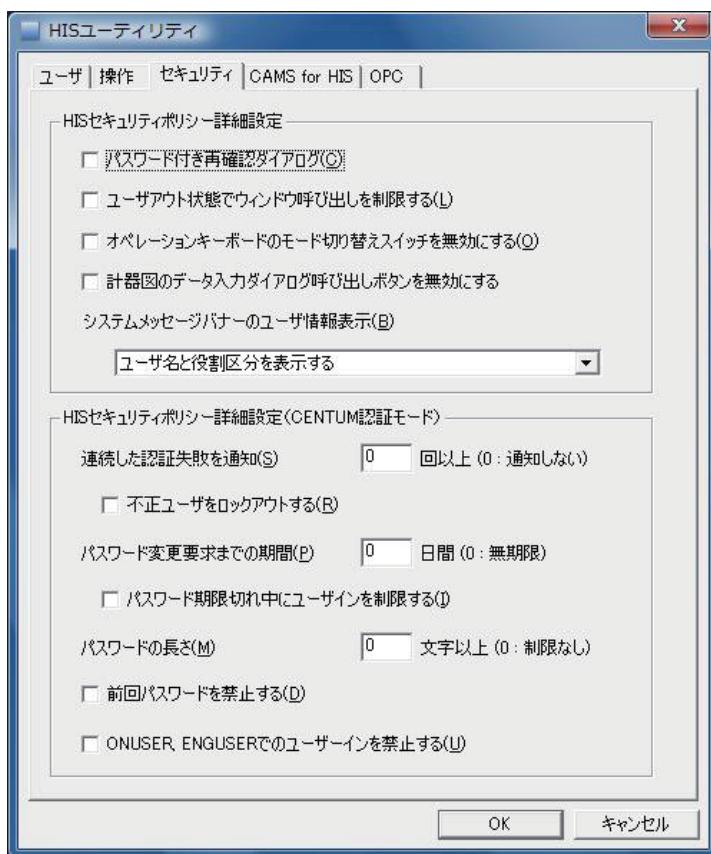


図 B4.11.2-2 セキュリティタブ

3. HIS の運用時のセキュリティポリシーに従って、セキュリティタブで、次のチェックボックスの設定をしてください。
 - ・ [パスワード付き再確認ダイアログ] チェックボックス
 - ・ [ユーザアウト状態でウィンドウ呼び出しを制限する] チェックボックス
 - ・ [オペレーションキーボードのモード切り替えスイッチを無効にする] チェックボックス
 - ・ [計器図のデータ入力ダイアログ呼び出しボタンを無効にする] チェックボックス

補足

Windows 認証モードのデフォルト設定では、セキュリティ強化の観点から OFFUSER の状態でウィンドウ呼び出しができません。ウィンドウ呼び出しを行う場合は、[ユーザアウト状態でウィンドウ呼び出しを制限する] チェックボックスをオフにしてください。

参照

上記チェックボックスについては、以下を参照してください。

エンジニアリングリファレンス Vol.1 (IM 33J10D10-01JA) の「3.1 ユーザ」

■ ENG グループユーザの設定

ENG グループユーザの設定をします。

● ユーザ環境設定

エンジニアリング基本機能、処方管理パッケージ、または帳票パッケージのうちのどれか 1 つ以上と、FDA 21 CFR Part11 対応パッケージまたはアクセス制限パッケージが有効化されている各コンピュータで実施してください。

1. CTM_MAINTENANCE または CTM_ENGINEER_ADM グループのユーザでログオンしてください。

2. アクセス制限ユーティリティを起動してください。
履歴管理とアクセス制限を行う対象を選択するための、設定対象選択ダイアログが表示されます。

補足

エンジニアリング基本機能、処方管理パッケージ、帳票パッケージのどれか1つだけが有効化されている場合、このダイアログは表示されません。有効化されているパッケージに対応したアクセス制限ユーティリティが起動されます。

3. アクセス制限ユーティリティをシステム生成機能用として起動する場合は、[エンジニアリング機能]を選択してください。処方管理機能用とする場合は [処方機能] を、帳票機能用とする場合は [帳票機能] を選択してください。
4. [OK] をクリックしてください。
アクセス制限ユーティリティが起動します。
5. 全般タブ内の [設定] をクリックしてください。
ユーザ環境設定ダイアログが表示されます。
6. 各ENGグループユーザーに関して、必要に応じて次の設定をしてください。
 - ・ 同一コンピュータに、操作監視基本機能がインストールされていない場合：自動ログオン設定とCENTUMデスクトップ設定

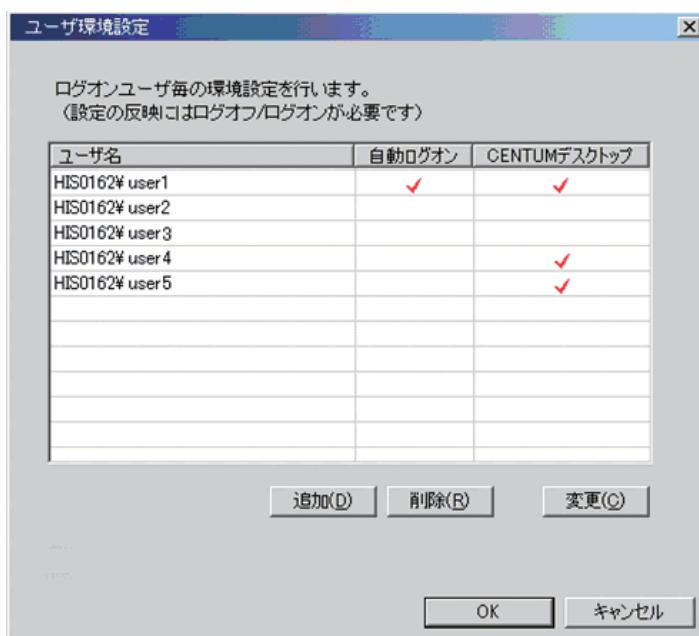


図 B4.11.2-3 ユーザ環境設定ダイアログ（操作監視基本機能がインストールされていない場合の例）

- ・ 同一コンピュータに、操作監視基本機能がインストールされている場合：自動ログオン設定、CENTUMデスクトップ設定、HIS起動設定

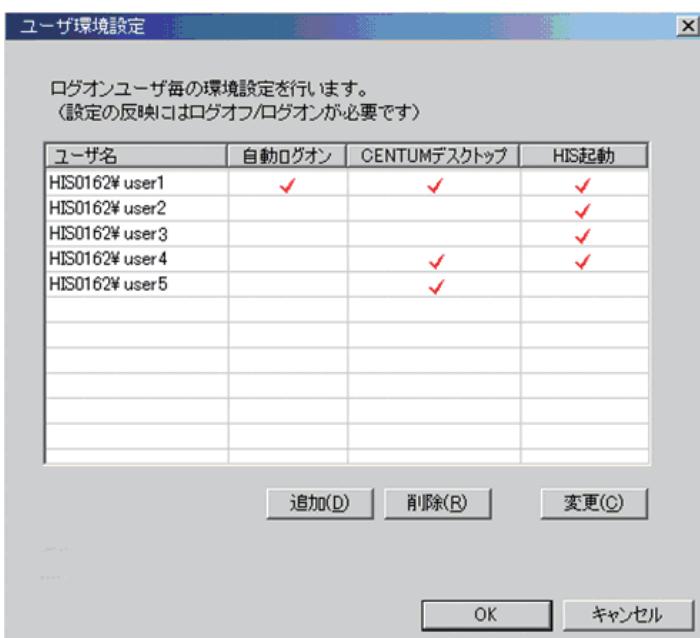


図 B4.11.2-4 ユーザ環境設定ダイアログ（操作監視基本機能がインストールされている場合の例）

補足

HIS グループユーザに関して、Windows 認証モードを選択している場合、次のダイアログが表示されます。設定項目は、[CENTUM デスクトップ設定] と [HIS 起動] の 2 つになります。

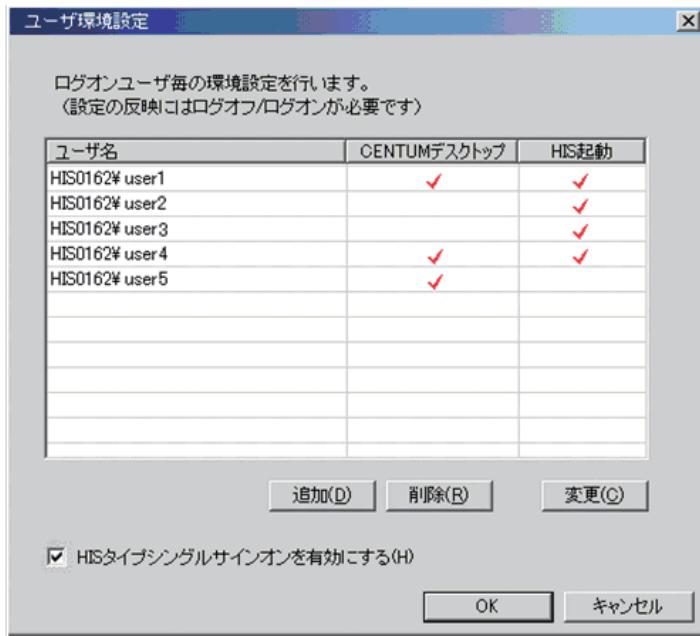


図 B4.11.2-5 ユーザ環境設定ダイアログ

参照

[HIS タイプシングルサインオンを有効にする] チェックボックスについては、以下を参照してください。

「■ HIS タイプシングルサインオンの設定」ページ B4-146

● ENG グループユーザのユーザ認証モードを Windows 認証モードに設定する

ENG グループユーザの管理を行うコンピュータで実施してください。

1. アクセス制限ユーティリティのアクセス制限タブを表示してください。
2. 設定対象に応じて次の操作を行ってください。

- ・ 設定対象選択ダイアログで [エンジニアリング機能] を選択していた場合、[Windows ユーザとシステムエンジニアを連携させる] チェックボックスをオンにしてください。
- ・ [処方機能] を選択していた場合は [Windows ユーザと処方エンジニアを連携させる] チェックボックスをオンにしてください。
- ・ [帳票機能] を選択していた場合は [Windows ユーザと帳票ユーザを連携させる] チェックボックスをオンにしてください。

● ENG グループユーザの登録

ENG グループユーザの管理を行うコンピュータで実施してください。

設定対象選択ダイアログで [帳票機能] を選択していた場合、「エンジニア登録ファイル」、「エンジニア登録ビルダ」、「エンジニア名」を「ユーザ登録ファイル」、「ユーザ登録ビルダ」、「ユーザ名」のそれぞれに読み替えてください。

1. 新規にエンジニア登録ファイルを作成するため、[既存ファイルを選択する] チェックボックスをオフしてください。
デフォルトのエンジニア登録ファイルが作成されます。
2. [参照先:] に、エンジニア登録ファイルを保存するフォルダを指定し、[OK] または [適用] をクリックしてください。
3. [編集...] をクリックして、エンジニア登録ビルダを起動してください。
4. [有効アカウント] タブを選択してください。
5. エンジニア名とエンジニアリンググループを設定してください。
6. 設定した内容を保存して、エンジニア登録ビルダを終了してください。
7. アクセス制限ユーティリティで [OK] をクリックしてください。

参照

エンジニア登録ビルダについては、以下を参照してください。

FDA : 21CFR Part11 対応リファレンス (IM 33J10D21-01JA) の「4.3 エンジニア登録ビルダ」

■ HIS グループユーザの設定

HIS グループユーザの設定をします。

● ユーザ環境設定

操作監視基本機能が有効化されている各コンピュータで実施してください。

HIS ユーティリティのユーザタブで、各 HIS グループユーザについて必要に応じたユーザ環境を設定してください。

1. CTM_MAINTENANCE グループのユーザでログオンしてください。
2. HIS ユーティリティを起動してください。
3. ユーザタブで、[設定] をクリックしてください。
ユーザ環境設定ダイアログが表示されます。

参照

ユーザ環境設定については、以下を参照してください。

「● ユーザ環境設定」ページ B4-141

● プロジェクトの新規作成

プロジェクトを作成・構築するコンピュータで実施してください。システムビューを使ってプロジェクトを新規作成します。

1. CTM_MAINTENANCE あるいは CTM_ENGINEER_ADM グループに属するユーザでログオンしてください。

2. システムビューを起動してください。
3. プロジェクトを新規作成してください。

補足

プロジェクトの作成は、CTM_ENGINEER グループに属するユーザで実行可能ですが、あとにユーザ認証モードを Windows 認証モードに設定するため、ここでは CTM_MAINTENANCE あるいは CTM_ENGINEER_ADMIN グループに属するユーザでログオンします。

参照

システムビューの操作については、以下を参照してください。

エンジニアリング基本操作 (IM 33J10D20-01JA) の「A1.5 システムビューの操作」

● プロジェクト構築

プロジェクトを作成・構築するコンピュータで実施してください。各種ビルダを使ってプロジェクトを構築します。

参照

各種ビルダを使ったプロジェクトの構築については、以下を参照してください。

エンジニアリング基本操作 (IM 33J10D20-01JA) の「A2. 新規システムのエンジニアリング」

● HIS グループユーザのユーザ認証モードを Windows 認証モードに設定

プロジェクトを作成・構築するコンピュータで実施してください。

1. プロジェクト作成・構築のために CTM_ENGINEER グループに属するユーザでログオンしている場合は、CTM_MAINTENANCE または CTM_ENGINEER_ADMIN グループに属するユーザでログオンし直してください。
2. プロジェクトを選択し、プロパティダイアログを表示してください。

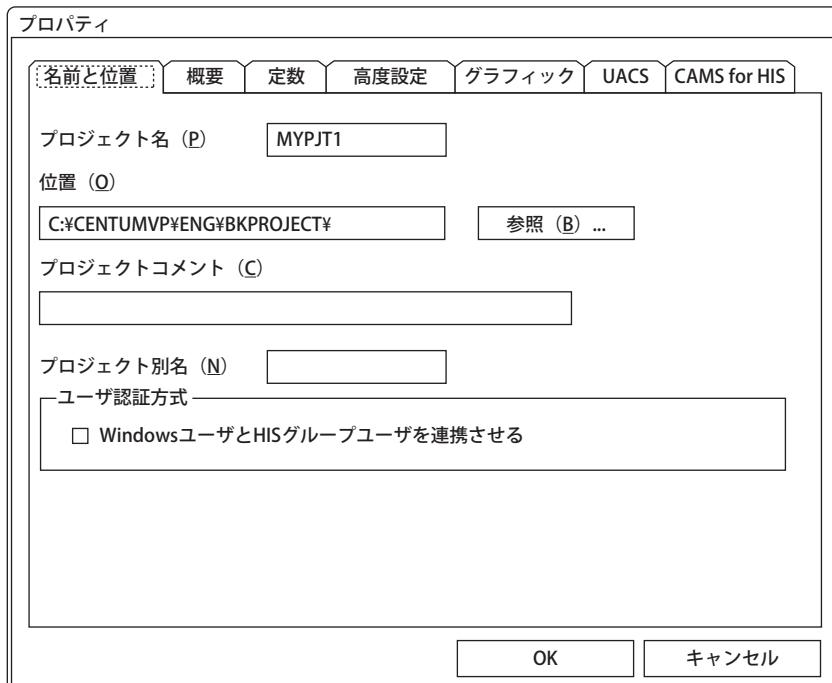


図 B4.11.2-6 プロジェクトのプロパティダイアログ

3. [名前と位置] タブを選択してください。
4. [Windows ユーザと HIS グループユーザを連携させる] チェックボックスをオンにしてください。

● HIS グループユーザの登録

プロジェクトを作成・構築するコンピュータで実施してください。

1. セキュリティビルダを起動してください。
2. [有効ユーザ] タブを選択してください。
3. ユーザ名を設定してください。
4. プロジェクト共通部をダウンロードしてください。

参照

セキュリティビルダについては、以下を参照してください。

エンジニアリングリファレンス Vol.1 (IM 33J10D10-01JA) の「3. セキュリティ」

● HIS の再起動

操作監視基本機能がインストールされている各コンピュータで、プロジェクトの作成・構築を行い、ユーザ認証モードを変更したあとに一度もプロジェクト共通部ダウンロードを実施していない場合、システムビューでプロジェクト 共通部ダウンロードを実施してください。

その後、HIS を再起動してください。

■ HIS タイプシングルサインオンの設定

操作監視基本機能が有効化されている各コンピュータで、HIS タイプシングルサインオンを利用したい場合に設定します。

● OFFUSER の Windows パスワード設定

HIS タイプシングルサインオンを利用したいコンピュータで実施してください。

1. 管理者ユーザでログオンしてください。
2. エクスプローラで下記のフォルダを表示してください。以下は C: ドライブの例です。
C:\Program Files (x86)\YOKOGAWA\IA\iPCS\Platform\SECURITY\PROGRAM
3. "Yokogawa.IA.iPCS.Platform.Security.OFFUSEREnabler.exe" をダブルクリックして実行してください。
OFFUSER のパスワードが "!centumvp123" に設定されます。

補足

IT セキュリティツールによって作成された OFFUSER は非公開の初期パスワードが設定されています。ここでは、OFFUSER の Windows 動作環境を設定するために、パスワードを一時的に変更します。

● OFFUSER の Windows 動作環境の設定

HIS タイプシングルサインオンを利用したいコンピュータで実施してください。

- OFFUSER でログオンして、Windows の動作環境の設定を行ってください。
ログオンに用いるパスワードは "!centumvp123" です。

補足

OFFUSER は、HIS タイプシングルサインオンで用いる Windows ユーザです。

参照

Windows の動作環境の設定については、以下を参照してください。

「B4.10 ユーザごとの Windows 動作環境の設定をする」ページ B4-109

● OFFUSER のパスワード初期化

HIS タイプシングルサインオンを利用したいコンピュータで実施してください。

1. 管理者ユーザでログオンしてください。

2. エクスプローラで、下記のフォルダを表示します。以下は C: ドライブの例です。
C:\Program Files (x86)\YOKOGAWAYIA\iPCS\Platform\SECURITY\PROGRAM
3. "Yokogawa.IA.iPCS.Platform.Security.OFFUSERDisabler.exe" をダブルクリックして実行してください。
OFFUSER のパスワードが初期化されます。

補足

ここでは、セキュリティの観点から OFFUSER のパスワードをふたたび非公開の初期パスワードに変更しています。

● HIS タイプシングルサインオンを有効にする

HIS タイプシングルサインオンを利用したいコンピュータで実施してください。

1. 管理者ユーザでログオンしてください。
2. HIS ユーティリティを起動してください。
3. [ユーザ] タブを選択し、[設定] をクリックしてください。
ユーザ環境設定ダイアログが表示されます。
4. [HIS タイプシングルサインオンを有効にする] チェックボックスをオンにしてください。

● OFFUSER の権限変更

プロジェクトを作成・構築するコンピュータで、OFFUSER の権限をデフォルトから変更する場合に実施してください。

1. 管理者ユーザでログオンしてください。
2. セキュリティビルダを起動してください。
3. [有効ユーザ] タブを選択してください。
4. OFFUSER の権限を編集してください。
5. システムビューで [プロジェクト共通部ダウンロード] を実施してください。

B4.11.3 ユーザ認証モードの注意事項

ここでは、ユーザ認証モードを使用する際の注意事項について説明します。

■ Window 認証モードで複数プロジェクト結合を使用する際の注意事項

Windows 認証モードの HIS タイプシングルサインオン環境で、複数プロジェクト機能を利用して、他のプロジェクトと結合する場合は、次の設定を行う必要があります。

● 相手側プロジェクトが CENTUM VP R4.03 より前で 標準モデルのセキュリティ設定をしている場合

相手側プロジェクトで、次の操作をしてください。

1. CENTUM VP ソフトウェアメディア中の次のプログラムを使用し、OFFUSER を作成してください。
¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS.Platform.Security.CreateOffuser.exe
2. プロジェクトデータベースフォルダのアクセス許可に OFFUSER を追加してください。

■ Window 認証モードで CENTUM データアクセスライブラリを使用する際の注意事項

Windows 認証モードの HIS タイプシングルサインオン環境で、CENTUM データアクセスライブラリを使用して複数プロジェクト結合で相手側プロジェクトへアクセスする場合は、次の設定を行う必要があります。

● 相手側プロジェクトが CENTUM VP で 標準モデルのセキュリティ設定をしている場合

相手側プロジェクトで、次の操作をしてください。

1. CENTUM VP ソフトウェアメディア中の次のプログラムを使用し、OFFUSER を作成してください。(相手側プロジェクトが CENTUM VP R4.03 より前の場合のみの作業)
¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS.Platform.Security.CreateOffuser.exe
2. 次の登録をしてください。
 - ・ スタンドアロン管理の場合 : CTM_OPC グループに OFFUSER を登録する
 - ・ ドメイン／併用管理の場合 : CTM_OPC_LCL グループに OFFUSER を登録する

B4.12 UPS (無停電電源装置) の設定をする

電源障害時などにコンピュータのデータを保護するため、コンピュータに無停電電源（以下、UPS）を接続し、ソフトウェアをインストールして各種の設定ができます。

CENTUM VP ソフトウェアが動作するコンピュータでは、UPS 管理ソフトウェアはユーザが自由に選択できます。CENTUM VP の標準機能ではありません。

CENTUM VP では、UPS ソフトウェア用に次のコマンドを提供しており、これによりコンピュータ電源障害発生をシステムアラームメッセージとして通知し、ソフトウェアを安全に停止できます。

- ・ システムアラームメッセージ出力コマンド
- ・ ソフトウェア機能停止コマンド

CENTUM VP 標準機能と UPS ソフトウェアとの組み合わせで実現される動作を次に示します。

表 B4.12-1 CENTUM VP 標準機能と UPS ソフトウェアとの組み合わせで実現される動作

異常要因	Windows 標準 UPS ソフトウェア	サードパーティソフトウェア (たとえば POWERCHUTE plus など)
電源障害によるバッテリへの切り替え時	設定不可	システムアラームメッセージ出力 (AC Fail)
電源回復時	設定不可	システムアラームメッセージ出力 (AC Recover)
システム・シャットダウン時	システムアラームメッセージ出力 (AC Fail Shutdown)	
システム・シャットダウン時	操作監視機能停止	
バッテリの交換必要時	設定不可	システムアラームメッセージ出力 (UPS Diagnose Error)

■ 設定の基本的な考え方

停電時の動作の基本的な考え方を次に示します。

ただし、この考え方がすべてのシステムに当てはまる訳ではありません。使用する電源事情やポリシーに従って、ソフトウェアの動作定義や設定時間は変更してください。また、管理ソフトウェアによっては実現できない機能があります。

- ・ 短い電源異常（瞬時停電など）時間では、コンピュータがシャットダウンしないように、UPS バッテリで動作が継続できるようにします。

補足

UPS バッテリでの動作継続時間は、1 分を目安とします。

このとき、電源異常が発生したことをコンピュータ使用者に通知するために、UPS 管理ソフトウェアにコマンド「BKHHisAcFail.exe」を実行させます。この結果、「AC Fail」のシステムメッセージが発生します。

- ・ 電源異常の継続時間が UPS バッテリでの動作継続時間を超えた場合、UPS 管理ソフトウェアにコマンド「BKHAcFailShut.exe」を実行させます。その結果、操作監視機能が正常にシャットダウンし、データの破壊などを防ぐことができます。このとき、「AC Fail Shutdown Execute」のシステムメッセージが発生します。
- ・ 上記の操作監視機能のシャットダウンの数分後に、Windows のシャットダウンを UPS 管理ソフトウェアから実行させます。このように Windows のシャットダウンを遅らせることにより、システム生成機能やアプリケーションなどを正常に終了させる時間を確保します。
- ・ Windows シャットダウンの数分後に、UPS の 2 次側電源出力を UPS 管理ソフトウェア用の設定により停止させます。

- 電源回復時には UPS にコマンド「BkHHisAcRecover.exe」を実行させます。その結果、「AC Recover」のシステムメッセージが発生します。

補足

UPS 側で、バッテリ交換を知らせるようなイベントのとき、「BKHUpSChk.exe」を実行させれば、「UPS Diagnose Error」のシステムアラームを発生させることができます。このアラームで、ユーザに UPS のログファイルを確認するよう喚起します。従って、UPS 管理ソフトウェア側でログが残るようにしておけば、電源異常発生時の解析に役立ちます。

● HIS 標準機能が提供するコマンド

表 B4.12-2 BKHHisAcFail.exe

パス	<CENTUM VP インストールフォルダ>\his\tool\BKHHisAcFail.exe
引数	なし
機能	システムアラームメッセージ AC Fail を出力する。

表 B4.12-3 BkHHisAcRecover.exe

パス	<CENTUM VP インストールフォルダ>\his\tool\BKHHisAcRecover.exe
引数	なし
機能	システムアラームメッセージ AC Recover を出力する。

表 B4.12-4 BKHAcFailShut.exe

パス	<CENTUM VP インストールフォルダ>\his\tool\BKHAcFailShut.exe
引数	なし
機能	システムアラームメッセージ AC Fail Shutdown を出力したあと、操作監視機能をシャットダウンする。

表 B4.12-5 BKHHisStop.exe

パス	<CENTUM VP インストールフォルダ>\his\tool\BKHHisStop.exe
引数	なし
機能	操作監視機能をシャットダウンする。

表 B4.12-6 BKHUpSChk.exe

パス	<CENTUM VP インストールフォルダ>\Fcs\tool\BKHUpSChk.exe
引数	なし
機能	システムアラームメッセージ UPS Diagnose Error を出力する。

● APCS/GSGW 標準機能が提供するコマンド

表 B4.12-7 BKFApcsAcFail.exe

パス	<CENTUM VP インストールフォルダ>\Fcs\tool\BKFApcsAcFail.exe
引数	なし
機能	システムアラームメッセージ AC Fail を出力する。

表 B4.12-8 BKFApcsAcRecover.exe

パス	<CENTUM VP インストールフォルダ>\Fcs\tool\BKFApcsAcRecover.exe
引数	なし
機能	システムアラームメッセージ AC Recover を出力する。

表 B4.12-9 BKFApcsAcFailShut.exe

パス	<CENTUM VP インストールフォルダ>\Fcs\tool\BKFApcsAcFailShut.exe
引数	なし
機能	システムアラームメッセージ AC Fail Shutdown を出力したあと、APCS/GSGW 制御機能をシャットダウンする。

● SIOS/UGS 標準機能が提供するコマンド

表 B4.12-10 BKVUpsAcFail.exe

パス	<CENTUM VP インストールフォルダ>\Eng\tool\BKVUpsAcFail.exe
引数	なし
機能	システムアラームメッセージ AC Fail を出力する。

表 B4.12-11 BKVUpsAcRecover.exe

パス	<CENTUM VP インストールフォルダ>\Eng\tool\BKVUpsAcRecover.exe
引数	なし
機能	システムアラームメッセージ AC Recover を出力する。

表 B4.12-12 BKVUpsDiagErr.exe

パス	<CENTUM VP インストールフォルダ>\Eng\tool\BKVUpsDiagErr.exe
引数	なし
機能	システムアラームメッセージ UPS Diagnose Error を出力する。

Blank Page

B5. リモート操作監視サーバ機能のセットアップをする

リモート操作監視サーバ機能を使うと、インターネット内にあるCENTUM VPがインストールされていないコンピュータからでも、CENTUM VPがインストールされたサーバーにアクセスして、CENTUM VPの操作監視機能を使用できるようになります。

リモート操作監視サーバ機能は、Windowsのリモートデスクトップサービス機能を使用します。

Windows Serverのリモートデスクトップサービスで動作する操作監視機能は、HIS-TSEと記述する場合があります。

参照

リモートデスクトップサービス機能の詳細設定については、以下を参照してください。

Microsoftの説明書

リモート操作監視サーバ機能については、以下を参照してください。

CENTUM VPオプション機能リファレンス (IM 33J05H10-01JA) の「7. リモート操作監視サーバ機能」

■用意するもの

サーバをセットアップする前に、次のものを手元に用意してください。

- CENTUM VP用ソフトウェアメディア

■インストールをする管理者ユーザ

次の表に示す管理者ユーザで実施してください。

インストールを実施したユーザは、自動的にCTM_MAINTENANCEグループに所属します。

表 B5-1 新規インストールを行う管理者ユーザ

設定しようとするセキュリティモデル／ユーザ管理方法		
従来モデル	標準モデル	
	スタンダードアロン管理	ドメイン管理／併用管理
Administratorsローカルグループに所属するローカルユーザ	Administratorsローカルグループに所属するローカルユーザ	<ul style="list-style-type: none"> Domain Admins ドメイングループに所属するドメインユーザ Administratorsローカルグループに所属するドメインユーザ Administratorsローカルグループに所属するローカルユーザ(*1)

*1: インストール中にドメインユーザのユーザ名とパスワードを入力する必要があります。

補足

ユーザ管理方法がドメイン管理／併用管理の場合は、コンピュータがドメインに参加した状態でインストールを実施してください。

■共存可能なパッケージの制限

HIS-TSEサーバでリモート操作監視サーバ機能と共に存在できないパッケージは、ライセンス配布時にエラーとなります。

表 B5-2 リモート操作監視サーバ機能との共存可否一覧

使用権形名	名称	共存	備考
VP6H1100	操作監視基本機能	Yes	
VP6H1120	ソリッドスタイルコンソールパッケージ	No	
VP6H1130	オープンスタイルコンソールパッケージ	No	
VP6H2411	Exaopc OPC インタフェースパッケージ (HIS 搭載用)	Yes	OPC サーバの機能自体も標準 HIS とは若干異なる。TSE 環境でのアプリケーションプログラムの動作確認が必須。
VP6H2412	CENTUM データアクセスライブラリ	Yes	作成したアプリケーションで個別に動作確認が必要
VP6H4000	操作監視タグ拡張パッケージ (100 万タグ対応)	Yes	
VP6H4100	ビルダ定義内容参照パッケージ	Yes	
VP6H4150	記録計出力パッケージ	No	
VP6H4190	ラインプリンタ出力パッケージ	No	
VP6H4200	ヒストリカルメッセージ統合パッケージ (FDA 対応)	No	
VP6H4410	制御ドローイング状態表示パッケージ	Yes	
VP6H4420	ロジックチャート状態表示パッケージ	Yes	
VP6H4450	複数プロジェクト結合パッケージ	Yes	
VP6H4600	複数モニタパッケージ	No	
VP6H4700	拡張アラームフィルタパッケージ	No	
VP6H6510	長期データ保管パッケージ	Yes	
VP6H6530	帳票パッケージ	No	クライアントコンピュータに帳票パッケージをインストールすることでリモート環境を構築可能。
VP6H6660	プロセス管理パッケージ	Yes	リモート操作監視サーバは、プロセス管理構成定義でクライアントステーションとする。
VP6H6710	FCS データ設定 / 収集パッケージ(PICOT)	No	
VP6E5000	エンジニアリングサーバ機能	Yes	同時 1 セッションのみ
VP6E5100	エンジニアリング基本機能	Yes	同時 1 セッションのみ
VP6E5110	アクセス制限パッケージ	Yes	同時 1 セッションのみ
VP6E5150	グラフィック作成パッケージ	Yes	同時 1 セッションのみ
VP6E5165	バッチビルダ	Yes	同時 1 セッションのみ
VP6E5166	処方管理パッケージ	Yes	同時 1 セッションのみ
VP6E5170	FDA : 21CFRpart11 対応パッケージ	Yes	同時 1 セッションのみ
VP6E5210	モジュールベースエンジニアリングパッケージ	Yes	同時 1 セッションのみ
VP6E5215	チューニングパラメータ管理パッケージ (モジュールベースエンジニアリング用)	Yes	同時 1 セッションのみ
VP6E5216	一括編集パッケージ (モジュールベースエンジニアリング用)	Yes	同時 1 セッションのみ
VP6E5250	変更管理パッケージ	Yes	同時 1 セッションのみ
VP6E5260	依存関係解析パッケージ	Yes	同時 1 セッションのみ
VP6E5420	テスト機能	No	
VP6E5425	拡張テスト機能	No	
VP6E5426	FCS シミュレータパッケージ	No	

次に続く

表 B5-2 リモート操作監視サーバ機能との共存可否一覧（前から続く）

使用権形名	名称	共存	備考
VP6E5427	HIS シミュレータパッケージ	No	
VP6A2505	UACS シミュレータパッケージ	No	
VP6E5450	複数プロジェクト結合機能ビルダ	Yes	同時 1 セッションのみ
VP6E5490	セルフドキュメントパッケージ	Yes	同時 1 セッションのみ
VP6C5495	電子ドキュメント	Yes	1 セッションあたり 2 個まで 1 コンピュータあたり 8 個まで

■ リモート操作監視サーバ機能のセットアップの注意事項

リモート操作監視サーバ機能のセットアップをするにあたっての注意事項を、次に示します。

● サーバーマネージャーのエラー

リモート操作監視サーバ機能をセットアップしたあと、サーバーマネージャーを立ち上げると、サーバーマネージャー内の表示がエラーになることがあります。

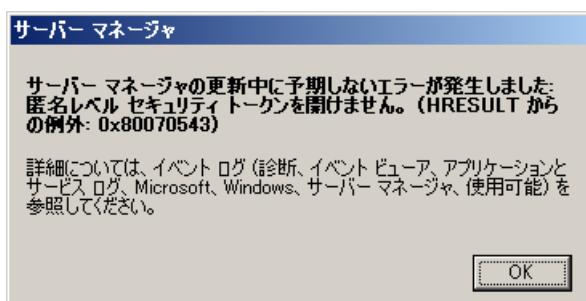


図 B5-1 サーバーマネージャーのエラーダイアログ

参照

サーバーマネージャー エラー時の対応については、以下を参照してください。

「C10.1.2 サーバーマネージャーの起動時にエラーが発生する」ページ C10-4

B5.1 HIS-TSE サーバの設定をする

リモート操作監視サーバ機能を使用するには、HIS-TSE サーバと HIS-TSE クライアントの両方で設定する必要があります。ここでは、HIS-TSE サーバの設定方法について説明します。

HIS-TSE サーバの設定を行う上で、バッチファイルを提供します。そのバッチファイルを使用する上での、次の注意事項があります。

- IT セキュリティにおいて、ソフトウェア制限ポリシーを設定している場合は、スタートメニューからコマンドプロンプト (cmd.exe) を右クリックして、[管理者として実行] を選択し、コマンドプロンプトを起動してください。起動されたコマンドプロンプトから必ずバッチファイルを実行してください。
- ドメイン環境で HIS-TSE 機能を実現している場合は、ドメインの Administrator でログオンし、バッチファイルを実行してください。

B5.1.1 Windows Server 2016 で設定する

Windows Server 2016 を使用するときは、次の設定方法に従ってください。

■ 手順 1：ハードウェアの設定をする

HIS-TSE サーバのハードウェアを設定してください。

参照

ハードウェア設定については、以下を参照してください。

「B4.1 ハードウェアの設定をする」ページ B4-2

■ 手順 2：Windows の設定をする

CENTUM VP ソフトウェアをコンピュータにインストールする前に行う Windows の設定をしてください。

補足

仮想メモリは、HIS セットアップ時と同サイズで設定してください。

参照

Windows の設定をする手順については、以下を参照してください。

「B4.2.3 Windows Server 2016 で設定する」ページ B4-23

■ 手順 3：ネットワークの設定をする

CENTUM VP のソフトウェアが動作するには、制御バスドライバが必要です。Vnet/IP を使用する場合は、Vnet/IP オープン通信ドライバも必要になります。

ここでは、制御バスドライバと Vnet/IP オープン通信ドライバのインストールをしてください。

コンピュータ付属の Ethernet、または市販の Ethernet 通信カードを使用する場合は、付属のマニュアルを参照し、必要に応じて適切な Ethernet ドライバをインストールしてください。

参照

ネットワークを設定する手順については、以下を参照してください。

「B4.3 ネットワークの設定をする」ページ B4-43

■ 手順 4：リモートデスクトップサービスをインストールする

リモートデスクトップサービスをインストールするときは、次の手順に従ってください。

1. サーバコンピュータに Administrator でサインインしてください。
2. CENTUM VP インストールメディアをコンピュータのドライブに挿入してください。
3. エクスプローラで、CENTUM VP インストールメディアの次のフォルダを開いてください。

<CENTUM VP ソフトウェアメディアドライブ> : ¥CENTUM¥HIS¥TSE

4. 1-InstallFeature.bat を右クリックして [管理者として実行] を選択してください。

リモートデスクトップサービスのインストールが終了するとサーバコンピュータが再起動します。

■ 手順 5：ライセンスサーバをインストールする

ライセンスサーバをインストールして、リモートデスクトップセッションホストの認証方法、リモートデスクトップライセンスマード、およびリモートデスクトップライセンスの検出スコープの構成を設定するときは、次の手順に従ってください。

補足

- ・ クライアントエクスペリエンスの構成の項目は、自動で次のとおりに設定されます。
 - ・ [オーディオおよびビデオ再生] : 有効
 - ・ [オーディオ録音リダイレクト] : 有効
 - ・ [リモートデスクトップセッションのデスクトップコンポジションを許可する] : 無効
- ・ システム内に複数のリモートデスクトップサーバが存在し、ライセンスサーバがリモートデスクトップサーバと同じ Windows Server 2016 を実行している場合、リモートデスクトップライセンスを共有できます。

1. サーバ 컴퓨터に Administrator でサインインしてください。
2. CENTUM VP インストールメディアをコンピュータのドライブに挿入してください。
3. エクスプローラで、CENTUM VP インストールメディアの次のフォルダを表示してください。
<CENTUM VP ソフトウェアメディアドライブ>:\CENTUM\HIS\TSE
4. 2-InstallLicense.bat を右クリックして [管理者として実行] を選択してください。
5. [Input for User Authentication:] ではリモートデスクトップセッションホストの認証方法を設定します。「ネットワークレベル認証を必要とする」を設定するために 1 を入力して、[Enter] キーを押してください。
6. [Input for Terminal Service Setting:] ではリモートデスクトップライセンスマードを設定します。次のどちらかの値を入力して、[Enter] キーを押してください。
 - ・ 接続デバイス数を選択する場合 : 2
 - ・ 接続ユーザー数を選択する場合 : 4
7. [Input for Discovery Scope:] ではリモートデスクトップライセンスの検出スコープの構成を設定します。次のどちらかの値を入力して、[Enter] キーを押してください。
 - ・ ワークグループを選択する場合 : 0
 - ・ ドメインを選択する場合 : 1

補足

サーバコンピュータをドメインで運用する場合、ドメインを選択します。

8. [Input for License Servers To Use:] では使用するライセンスサーバーを設定します。ライセンスサーバーのコンピュータ名もしくは IP アドレスを入力して、[Enter] キーを押してください。ライセンスサーバーがドメイン環境に設置されている場合は、コンピュータ名を「Fully Qualified Domain Name (FQDN)」として、ホスト名およびドメイン名などすべて省略せずに指定してください。

補足

ライセンスサーバーがリモートデスクトップサーバーと同居しているときは、自コンピュータ名もしくは IP アドレスを指定してください。

リモートデスクトップセッションホストの認証方法、リモートデスクトップライセンスマード、リモートデスクトップライセンスの検出スコープの構成、およびライセンスサーバーの設定内容がバッチファイルの画面に表示されます。

9. リモートデスクトップセッションホストの認証方法、リモートデスクトップライセンスマード、リモートデスクトップライセンスの検出スコープの構成、およびライセンスサーバーの設定内容を確認して、問題なければ、[To be continued?:] に y を入力

して[Enter]キーを押してください。設定が完了すると、[続行するには何かキーを押してください...]と表示されます。設定を変更する必要がある場合は [To be continued?]にnを入力して、再び2-InstallLicense.batを起動して、初めから設定し直してください。

■手順6：リモートデスクトップライセンスサーバの認証

リモートデスクトップライセンスサーバの認証については、次の手順に従ってください。

1. サーバコンピュータにAdministratorでサインインしてください。
2. コマンドプロンプトを起動してください。
3. licmgr.exeと入力してください。

RDライセンスマネージャーが表示されます。

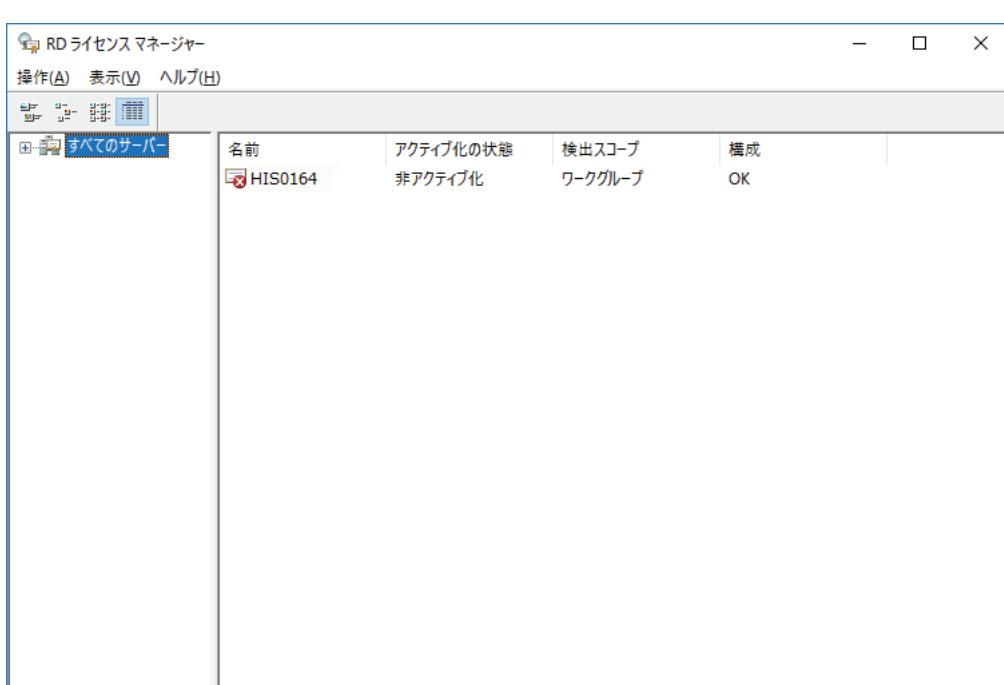


図 B5.1.1-1 RD ライセンスマネージャー

4. 認証するコンピュータを選択し、メニューバーから「操作」→「サーバーのアクティベーション」を選択してください。
サーバのアクティベーションウィザードが表示されます。
5. ウィザードの指示に従い、作業を行ってください。

補足

リモートデスクトップサービスのクライアントアクセスライセンス（RDS CAL）をインストールするには、最初にリモートデスクトップライセンスサーバーの認証の手続きを Microsoft に対して行う必要があります。ライセンスサーバーのアクティベーションが正常に完了したら、RDS CAL をインストールしてください。認証の手続きについては、Microsoft に問い合わせてください。

■手順7：オーディオ使用の設定をする

リモートデスクトップサービス接続時にオーディオを使用するためには、オーディオサービスの有効化、システムサウンドサービスの実行をする必要があります。

● オーディオサービスの有効化

1. コントロールパネルを起動してください。
2. 「システムとセキュリティ」→「管理ツール」→「サービス」を選択してください。
サービスウィンドウが表示されます。

3. [Windows Audio] をダブルクリックしてください。
Windows Audio のプロパティダイアログが表示されます。



図 B5.1.1-2 Window Audio のプロパティダイアログ

4. [スタートアップの種類] ドロップダウンリストボックスから [自動] を、[サービスの状態] では [開始] を選択し、[OK] をクリックしてください。
5. サービスウィンドウで、Windows Audio の状態が [実行中]、スタートアップの種類が [自動] になっていることを確認してください。

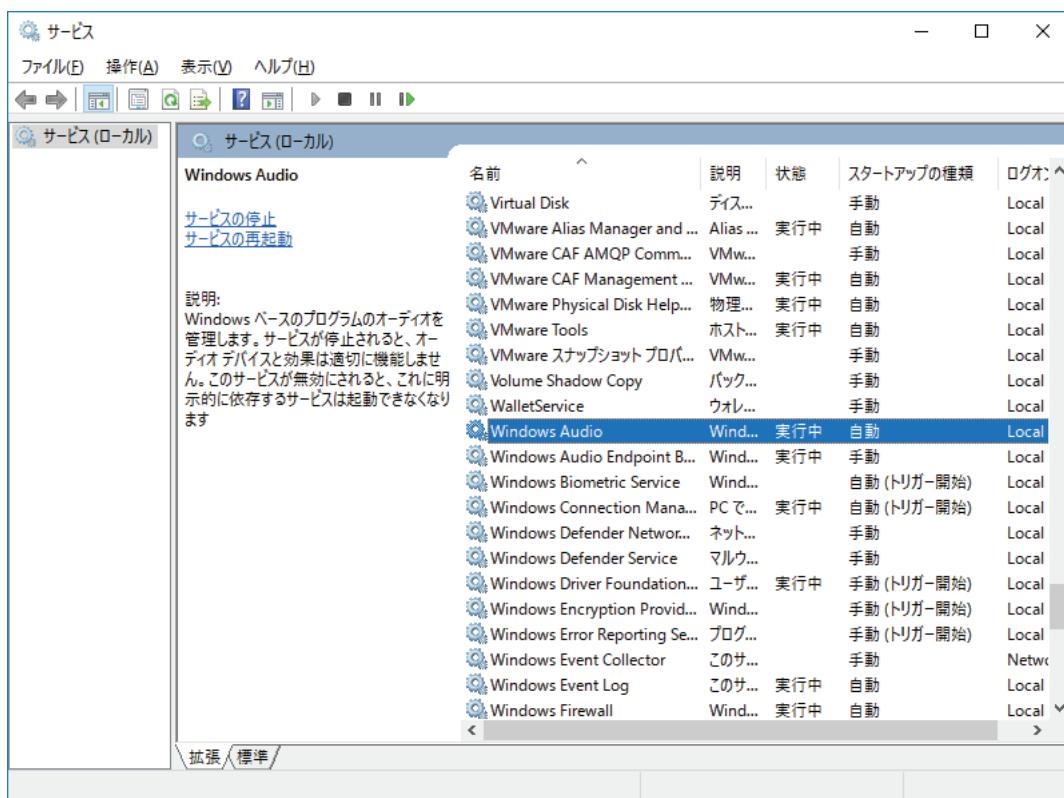


図 B5.1.1-3 サービス画面

● システムサウンドサービスの実行

1. コントロールパネルを起動してください。
2. [システムとセキュリティ] – [管理ツール] – [タスクスケジューラ] を選択してください。
タスクスケジューラ ウィンドウが表示されます。
3. [タスクスケジューラライブラリ] – [Microsoft] – [Windows] – [Multimedia] を選択してください。
4. [System Sound Service] を右クリックし、[有効] を選択してください。

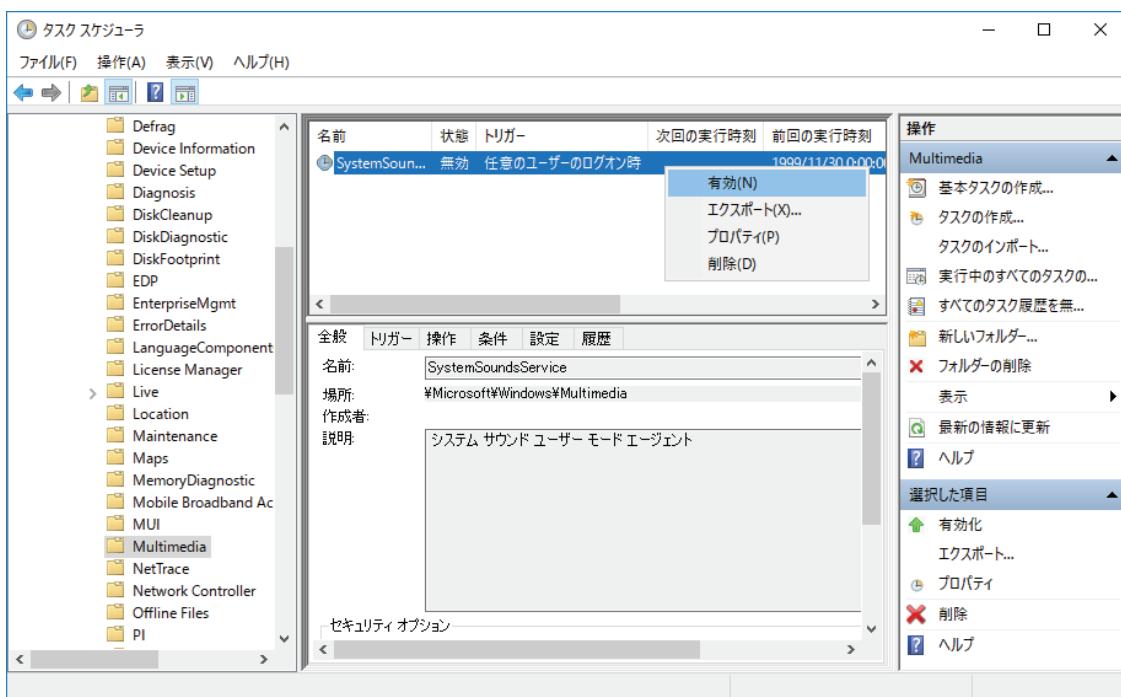


図 B5.1.1-4 タスクスケジューラウィンドウ – SystemSoundService の有効化

5. [System Sound Service] を右クリックし、[実行する] を選択してください。

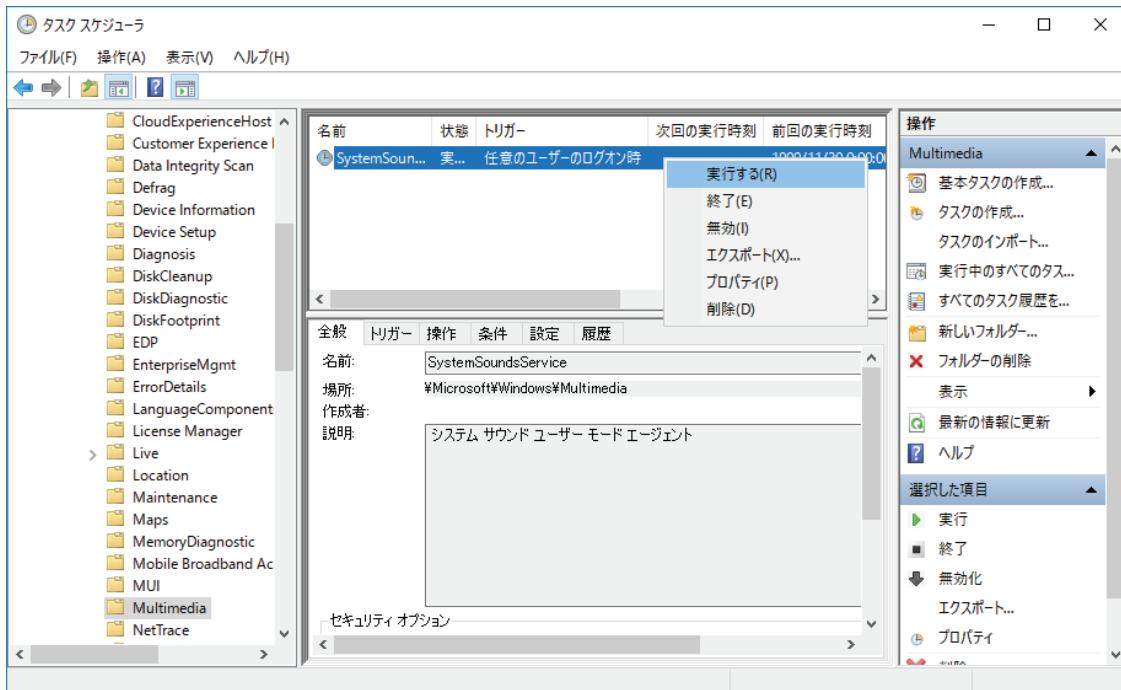


図 B5.1.1-5 タスクスケジューラウィンドウ – SystemSoundService の実行

■ 手順 8 : CENTUM VP ソフトウェアのインストールをする

リモート操作監視サーバのための CENTUM VP のインストールは、HIS と同様です。

参照

CENTUM VP ソフトウェアのインストールについては、以下を参照してください。

「B4.6 CENTUM VP ソフトウェアのインストールをする」ページ B4-87

■ 手順 9：IT セキュリティを設定する

CENTUM VP は、ソフトウェアのインストール後に、コンピュータの IT セキュリティを強化するための設定を行う必要があります。

参照

IT セキュリティを設定する手順については、以下を参照してください。

「B4.7 IT セキュリティを設定する」ページ B4-96

■ 手順 10：Remote Desktop Users のメンバ登録をする

IT セキュリティの設定後、リモートからログオンするユーザ、あるいはユーザグループを Remote Desktop Users グループに登録します。ここでは RemoteCentum ユーザを Remote Desktop Users グループに登録する手順を説明します。

1. サーバコンピュータに Administrator でログオンしてください。
サーバーマネージャーが表示されます。
2. [ツール] – [コンピュータの管理] を選択してください。
コンピュータの管理ウィンドウが表示されます。
3. [コンピュータの管理] – [ローカルユーザーとグループ] – [グループ] を選択してください。
グループの一覧が表示されます。
4. [Remote Desktop Users] を選択し、右クリックで [グループに追加] を選択してください。

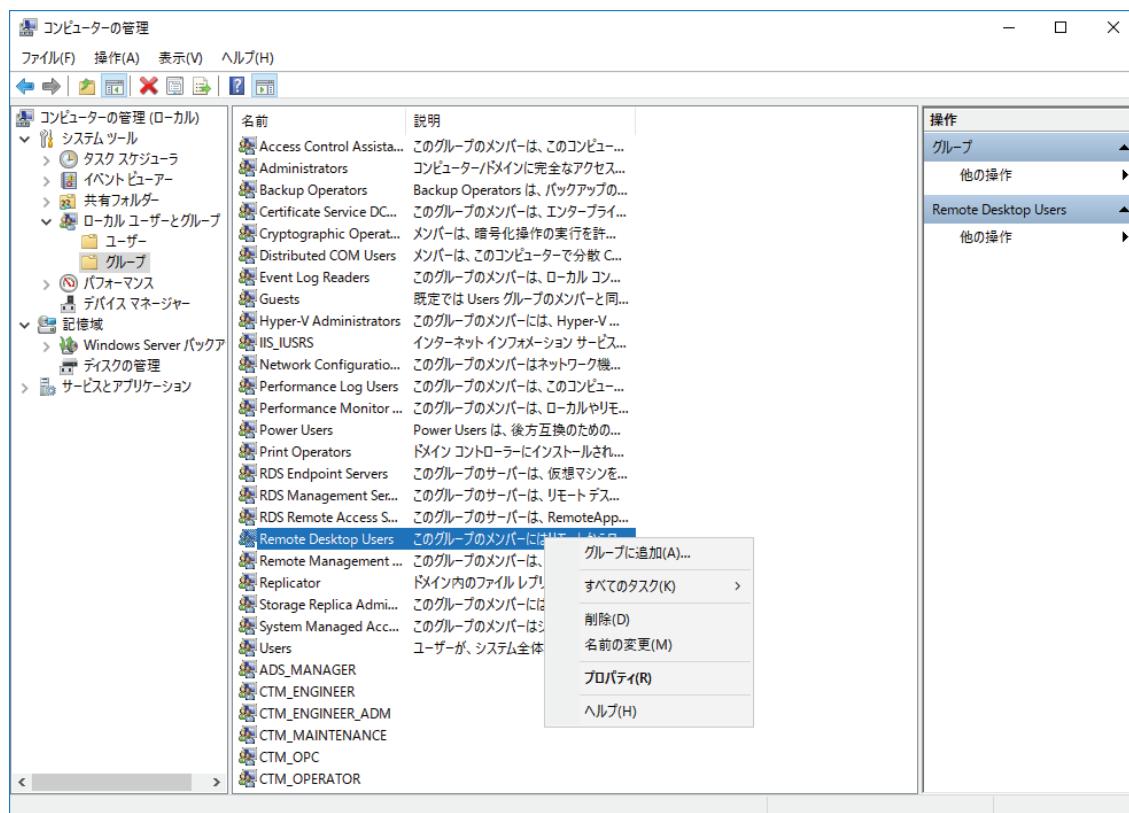


図 B5.1.1-6 コンピュータの管理ウィンドウ

Remote Desktop Users に所属するユーザの一覧が表示されます。

5. [全般] タブの [追加] をクリックしてください。
ユーザの選択ダイアログが表示されます。

6. [詳細設定] をクリックしてください。
詳細設定の欄が追加で表示されます。
7. [場所] をクリックしてください。
場所の一覧が表示されます。

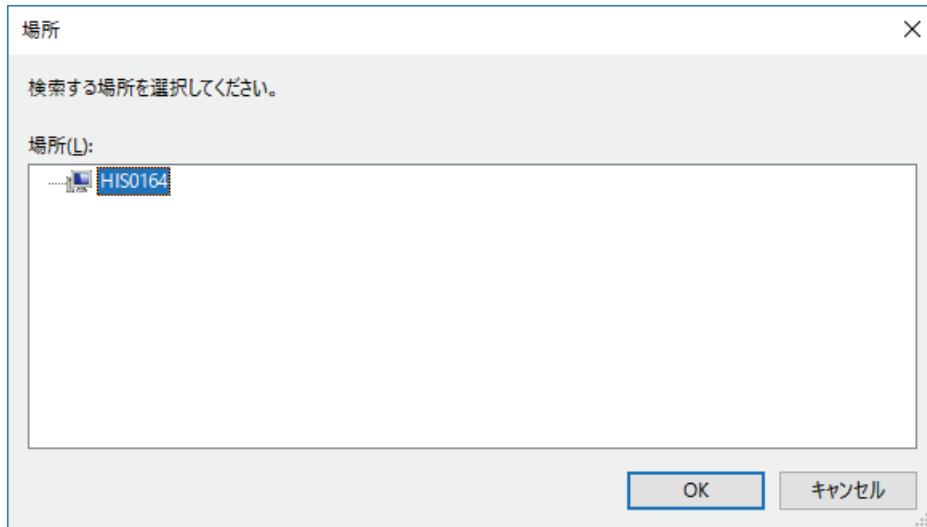


図 B5.1.1-7 場所の一覧

8. 追加したいユーザの所属するコンピュータ名またはドメイン名を選択し、[OK] をクリックしてください。
ユーザの選択ダイアログに戻ります。
9. [検索] をクリックしてください。
選択したコンピュータもしくはドメインに属するユーザの一覧が表示されます。

補足

場所の指定にドメイン名を選択したときは、ドメインの設定によってはユーザの一覧が表示されない場合があります。また、ドメインに所属するユーザ数が 10000 を超えるときには、すべてのユーザを一覧表示することができます。

この場合には、詳細設定ダイアログを [キャンセル] で閉じ、[選択するオブジェクト名] 欄にユーザ名を直接入力してください。

例： ドメインユーザを指定する場合 somedomain\RemoteCentum

ローカルユーザを指定する場合 HIS0164\RemoteCentum

10. 追加したいユーザである RemoteCentum を選択し、[OK] をクリックしてください。
グループに所属するメンバーに、RemoteCentum が追加されます。

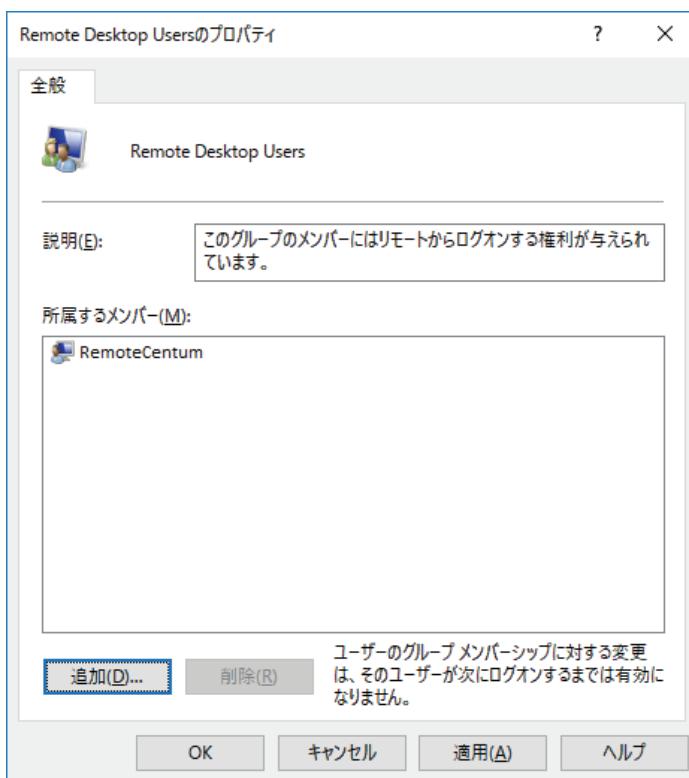


図 B5.1.1-8 Remote Desktop Users のプロパティ

11. [OK] をクリックしてください。

■ 手順 11：ライセンスの配布と反映をする

リモート操作監視サーバ機能に加え、必要なパッケージのライセンスを、ライセンス管理ステーションから配布し、反映してください。

参照

ライセンスの配布と反映をする手順については、以下を参照してください。

「B4.8 ライセンスの配布と反映をする」ページ B4-103

■ 手順 12：ユーザーアカウントを作成する

ユーザーアカウントの作成をする必要があります。

参照

ユーザーアカウントの作成については、以下を参照してください。

「B4.9 ユーザーアカウントを作成する」ページ B4-104

■ 手順 13：ユーザごとの Windows 動作環境の設定をする

ログオンユーザごとに Windows 動作環境の設定をする必要があります。

参照

ユーザごとの Windows 動作環境の設定をする手順については、以下を参照してください。

「B4.10 ユーザごとの Windows 動作環境の設定をする」ページ B4-109

■ 手順 14：ユーザ認証モードの設定をする

ユーザ認証モードの設定をする必要があります。

参照

ユーザ認証モードの設定手順については、以下を参照してください。

「B4.11 ユーザ認証モードの設定をする」ページ B4-136

■ 手順 15：UPS（無停電電源装置）の設定をする

UPS を使用する場合は、その設定をする必要があります。

参照

UPS（無停電電源装置）の設定をする手順については、以下を参照してください。

「B4.12 UPS（無停電電源装置）の設定をする」ページ B4-149

■ 手順 16：RemoteApp プログラムの設定をする

リモートで HIS-TSE サーバに接続するコンピュータから、CENTUM VP 操作監視機能を使用可能とするため、リモートデスクトップサービスの設定を行います。

● StartDesktop.bat の追加

HIS-TSE をデスクトップモードで利用する場合、この設定が必要になります。StartDesktop.bat を追加するときは、次の手順に従ってください。

1. サーバコンピュータに Administrator でサインインしてください。
2. CENTUM VP インストールメディアをコンピュータのドライブに挿入してください。
3. エクスプローラで、CENTUM VP インストールメディアの次のフォルダを開いてください。
<CENTUM VP ソフトウェアメディアドライブ> : ¥CENTUM¥HIS¥TSE
4. 3-AddStartDesktop.bat を右クリックして [管理者として実行] を選択してください。
5. CENTUM VP ソフトウェアがインストールされていることを確認して、[Have you installed CENTUM VP Software?] に *y* を入力して [Enter] キーを押してください。CENTUM VP ソフトウェアがインストールされていない場合は、*n* を入力して [ENTER] キーを押し、CENTUM VP をインストールしたあとに再びこの設定をしてください。

補足

CENTUM VP をインストールした場合、<CENTUM VP インストールフォルダ>¥program に StartDesktop.bat がインストールされます。CENTUM VP がインストールされていないと、この設定は動作しないため、StartDesktop.bat が存在することを確認してください。

● BKHBos.exe の追加

HIS-TSE をパネルモードで利用する場合、この設定が必要になります。BKHBos.exe を追加するときは、次の手順に従ってください。

1. サーバコンピュータに Administrator でサインインしてください。
2. CENTUM VP インストールメディアをコンピュータのドライブに挿入してください。
3. エクスプローラで、CENTUM VP インストールメディアの次のフォルダを開いてください。
<CENTUM VP ソフトウェアメディアドライブ> : ¥CENTUM¥HIS¥TSE
4. A1-AddBKHBos.bat を右クリックして [管理者として実行] を選択してください。
5. CENTUM VP ソフトウェアがインストールされていることを確認して、[Have you installed CENTUM VP Software?] に *y* を入力して [Enter] キーを押してください。CENTUM VP ソフトウェアがインストールされていない場合は、*n* を入力して [ENTER] キーを押し、CENTUM VP をインストールしたあとに再びこの設定をしてください。

補足

CENTUM VP をインストールした場合、<CENTUM VP インストールフォルダ>\program に BKHBos.exe がインストールされます。CENTUM VP がインストールされていないと、この設定は動作しないため、BKHBos.exe が存在することを確認してください。

■ 手順 17：リモートデスクトップサービスの設定をする

セッション制限、ネットワークアダプタを設定するときは、次の手順に従ってください。

補足

RDP-Tcp プロパティの項目は、自動で次のとおりに設定されます。

- ・ [全般] : [ネットワークレベル認証でリモートデスクトップを実行しているコンピュータからのみ接続を許可する] を有効にします。
- ・ [ログオン設定] : [次のログオン情報を常に使う] を有効し、ユーザに CENTUM を設定します。
- ・ [リモート制御] : [リモート制御を許可しない] を有効にします。
- ・ [クライアント設定] : [色の深度の最大数を制限する]、[オーディオ録音]、および [オーディオおよびビデオの再生] を無効にします。

1. サーバコンピュータに Administrator でサインインしてください。
2. CENTUM VP インストールメディアをコンピュータのドライブに挿入してください。
3. エクスプローラで、CENTUM VP インストールメディアの次のフォルダを開いてください。
<CENTUM VP ソフトウェアメディアドライブ>:\CENTUM\HIS\TSE
4. 4-TerminalServiceSetting.bat を右クリックして [管理者として実行] を選択してください。
5. [Input for Single Session Per User:] ではセッション制限に関する設定をします。次のどちらか値を入力して、[Enter] キーを押してください。
 - ・ IT セキュリティで従来モデル（常に CENTUM でサインイン）を使用する場合 : 0
 - ・ IT セキュリティで標準モデルを選択し、オペレータが個別名でサインインする運用の場合 : 1
6. [Select Network Adapter:] では HIS-TSE サーバと HIS-TSE クライアントの間の通信に使用するネットワークアダプタを指定します。使用できるネットワークアダプタの選択肢が表示されるので、該当するネットワークアダプタの値を入力して、[Enter] キーを押してください。

補足

[Yokogawa Vnet Adapter:1] は指定しないでください。

7. セッション制限、ネットワークアダプタの設定内容を確認して、問題なければ、[To be continued?:] に y を入力して [Enter] キーを押してください。設定が完了すると、[続行するには何かキーを押してください...] と表示されます。設定を変更する必要がある場合は [To be continued?:] に n を入力して、再び 4-TerminalServiceSetting.bat を起動して、初めから設定し直してください。

● 操作監視機能の自動起動設定

HIS-TSE をデスクトップモードで使用する場合、ローカルグループポリシーエディターの [接続時にプログラムを起動する] のポリシーにバッチファイルを設定しておくことで、HIS-TSE クライアントごとに設定を行わなくても、HIS-TSE サーバに接続しただけで、操作監視機能を自動的に起動できます。操作監視機能を自動的に起動させるときは、次の手順に従ってください。

1. サーバコンピュータに Administrator でサインインしてください。
2. コマンドプロンプトを起動してください。
3. gpedit.msc と入力してください。

ローカルグループポリシーエディターが表示されます。

4. 左ペインで、[コンピュータの構成] – [管理用テンプレート] – [Windows コンポーネント] – [リモートデスクトップサービス] – [リモートデスクトップセッションホスト] を選択して、[リモートセッション環境] をクリックしてください。
5. [接続時にプログラムを起動する] をダブルクリックしてください。
接続時にプログラムを起動するダイアログが表示されます。

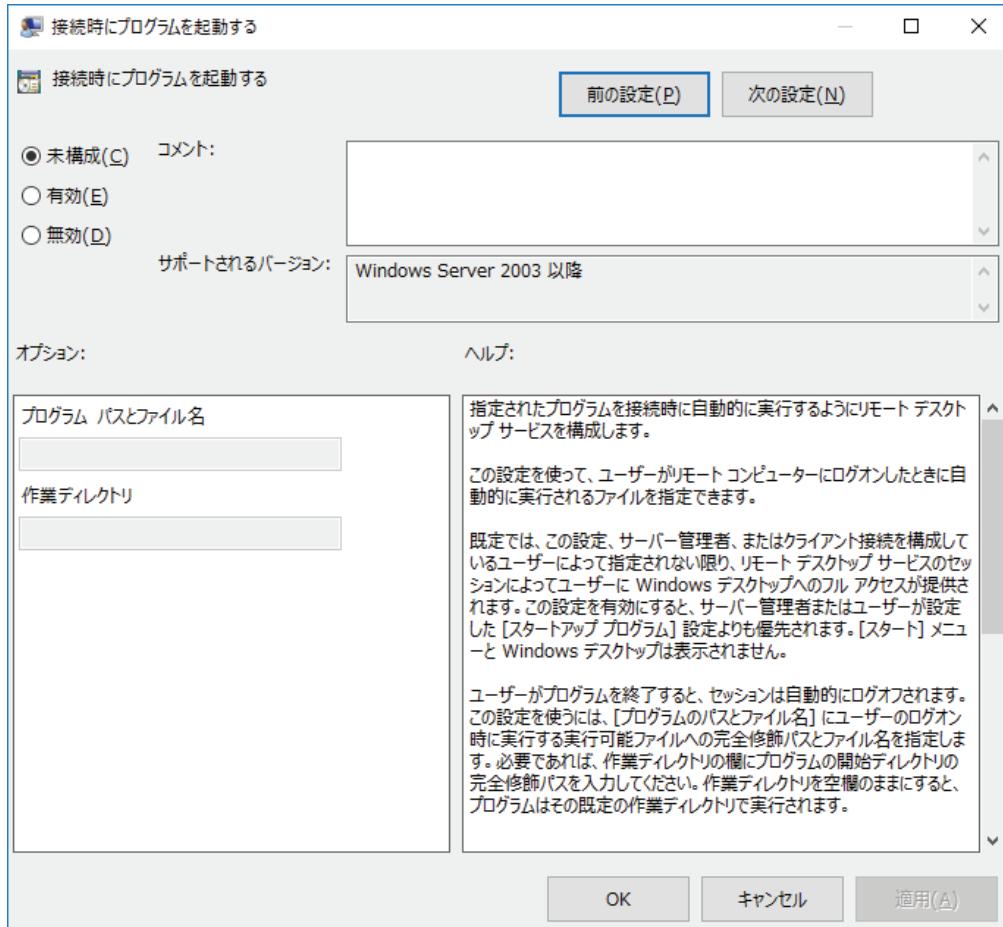


図 B5.1.1-9 接続時にプログラムを起動するダイアログ

6. [有効] を選択してください。
7. [プログラムパスとファイル名] に次のバッチファイルへのパスを入力してください。
<CENTUM VP インストールドライブ>:\CENTUMVP\Program\StartDesktop.bat
8. [作業ディレクトリ] に、次のパスを入力してください。
<CENTUM VP インストールドライブ>:\CENTUMVP\Program
9. [OK] ボタンをクリックしてください。

■手順 18：プロジェクトに HIS-TSE を追加する

1. システムビューで HIS-TSE を追加するプロジェクトを開いてください。
2. ステーションタイプに [HIS-TSE リモート操作監視サーバ機能搭載 HIS] を指定して、ステーションを追加してください。
3. 標準 HIS の場合と同様の操作で、[プロジェクト共通部ダウンロード]、[HIS ダウンロード]、[タグリストダウンロード] を実行してください。
4. リモート操作監視サーバを再起動してください。

参照

HIS 新規作成時のビルダ定義項目については、以下を参照してください。

エンジニアリングリファレンス Vol.1 (IM 33J10D10-01JA) の「2.4.2 HIS の新規作成」

■ 設定した項目を確認する

手順 5、手順 16、手順 17 の各バッチファイルで設定した項目を一覧表示で確認できます。設定した項目を確認するときは、次の手順に従ってください。

1. サーバコンピュータに Administrator でサインインしてください。
2. CENTUM VP インストールメディアをコンピュータのドライブに挿入してください。
3. エクスプローラで、CENTUM VP インストールメディアの次のフォルダを開いてください。
<CENTUM VP ソフトウェアメディアドライブ> : ¥CENTUM¥HIS¥TSE
4. A2-ConfirmSettings.bat を右クリックして [管理者として実行] を選択してください。設定した項目が次の形式で一覧表示されます。
設定項目[期待値]：設定値
5. 期待値と設定値が異なる場合、対象のバッチファイルを実行して再び設定し直してください。

参照

バッチファイルの実行方法については、以下を参照してください。

- ・ 「■ 手順 5：ライセンスサーバをインストールする」ページ B5-6
- ・ 「■ 手順 16：RemoteApp プログラムの設定をする」ページ B5-14
- ・ 「■ 手順 17：リモートデスクトップサービスの設定をする」ページ B5-15

● 各設定項目の期待値

各バッチファイルの設定項目の期待値を次の表に示します。

表 B5.1.1-1 各バッチファイルの設定項目の期待値

バッチファイル	設定項目	期待値	内容
2-InstallLicense.bat (手順 5)	User Authentication	1	リモートデスクトップセッションホストの認証方法の指定 [ネットワークレベル認証を必要とする] という設定
		0	リモートデスクトップセッションホストの認証方法の指定 [ネットワークレベル認証を必要としない] という設定
	Terminal Service Setting	2	リモートデスクトップライセンスマードの指定 [接続デバイス数] という設定
		4	リモートデスクトップライセンスマードの指定 [接続ユーザ数] という設定
	DisableCam	0 (固定値)	クライアントエクスペリエンス構成の指定 [オーディオおよびビデオ再生] が有効という設定
	DisableAudioCapture	0 (固定値)	クライアントエクスペリエンス構成の指定 [オーディオ録音リダイレクト] が有効という設定
	Allow Desktop Composition On Server	0 (固定値)	クライアントエクスペリエンス構成の指定 [デスクトップコンポジション] が無効という設定
	Discovery Scope	0	RD ライセンスの検出スコープの構成の指定 [このワークグループ] という設定
		1	RD ライセンスの検出スコープの構成の指定 [このドメイン] という設定
	License Servers To Use	ライセンスサーバーのコンピュータ名もしくはIPアドレス	使用するライセンスサーバーの指定

次に続く

表 B5.1.1-1 各バッチファイルの設定項目の期待値（前から続く）

バッチファイル	設定項目	期待値	内容
3-AddStartDesktop.bat (手順 16)	StartDesktop_CommandLineSetting	0 (固定値)	RemoteAPP プログラムの指定 [コマンドライン引数の許可] をしないという設定
	StartDesktop_Name	StartDesktop (固定値)	RemoteAPP プログラムの指定 バッチファイル名
	StartDesktop_Path	<CENTUM VP インストール フォルダ>\program\Start Desktop.bat (固定値)	RemoteAPP プログラムの指定 追加する RemoteApp プ ログラムのバッチファイルが格納されているファ イルパスを設定
	StartDesktop_ShowInTS WA	1 (固定値)	RemoteAPP プログラムの指定 [RemoteAPP プログラムを RD Web アクセスから 利用可能にする] が有効 という設定
A1-AddBKHBos.bat (手順 16)	BKHBos_CommandLineS etting	1 (固定値)	パネルモードで実行する ための指定 [コマンドライン引数を 許可] をするという設定
	BKHBos_Name	BKHBos (固定値)	パネルモードで実行する ための指定 RemoteAPP プログラム 名
	BKHBos_Path	<CENTUM VP インストール フォルダ>\program\BKHBos. exe (固定値)	パネルモードで実行する ための指定 追加した RemoteAPP プ ログラムが格納されてい るファイルパスを設定
	BKHBos_ShowInTSWA	1 (固定値)	パネルモードで実行する ための指定 [RemoteAPP プログラム は RD Web アクセスから 利用可能] が有効とい う設定

次に続く

表 B5.1.1-1 各バッチファイルの設定項目の期待値 (前から続く)

バッチファイル	設定項目	期待値	内容
4-TerminalServiceSetting.bat (手順 17)	Single Session Per User	0	ターミナルサービスの指定 [1 ユーザにつき 1 セッションに制限する] が無効という設定
		1	ターミナルサービスの指定 [1 ユーザにつき 1 セッションに制限する] が有効という設定
	Inherit Auto Logon	1 (固定値)	ターミナルサービスの指定 [ネットワークレベル認証でリモートデスクトップを実行しているコンピュータからのみ接続を許可する] が有効という設定
	Max Disconnection Time	60000 (固定値)	ターミナルサービスの指定 [切断されたセッションの終了] のタイムアウト値
	Shadow	0 (固定値)	ターミナルサービスのリモート制御の指定 [リモート制御を許可しない] が有効という設定
	Inherit Color Depth	1 (固定値)	ターミナルサービスのクライアントの指定 [色の深度の最大値を制限する] が無効という設定
	Max Monitors	1 (固定値)	ターミナルサービスのクライアントの指定 セッションごとのモニターの最大数
	Network Adapter	ネットワークアダプター番号	ターミナルサービスのネットワークアダプターの指定 選択したネットワークアダプターリストに対する認識番号
	Network Adapter List	ネットワークアダプターのリスト	ターミナルサービスのネットワークアダプターの指定 選択可能なネットワークアダプターの一覧

B5.1.2 Windows Server 2008 R2 で設定する

Windows Server 2008 R2 を使用するときは、次の設定方法に従ってください。

■ 手順 1：ハードウェアの設定をする

HIS-TSE サーバのハードウェアを設定してください。

参照

ハードウェア設定については、以下を参照してください。

「B4.1 ハードウェアの設定をする」ページ B4-2

■ 手順 2：Windows の設定をする

CENTUM VP ソフトウェアをコンピュータにインストールする前に行う Windows の設定をしてください。

補足

仮想メモリは、HIS セットアップ時と同サイズで設定してください。

参照

Windows の設定をする手順については、以下を参照してください。

「B4.2.5 Windows Server 2008 R2 で設定する」ページ B4-36

■ 手順 3：ネットワークの設定をする

CENTUM VP のソフトウェアが動作するには、制御バスドライバが必要です。Vnet/IP を使用する場合は、Vnet/IP オープン通信ドライバも必要になります。

ここでは、制御バスドライバと Vnet/IP オープン通信ドライバのインストールをしてください。

コンピュータ付属の Ethernet、または市販の Ethernet 通信カードを使用する場合は、付属のマニュアルを参照し、必要に応じて適切な Ethernet ドライバをインストールしてください。

参照

ネットワークを設定する手順については、以下を参照してください。

「B4.3 ネットワークの設定をする」ページ B4-43

■ 手順 4：リモートデスクトップサービスとライセンスサーバのインストールをする

1. サーバコンピュータに Administrator でログオンしてください。
サーバーマネージャーが表示されます。
2. [役割] – [役割の追加] を選択してください。
役割の追加ウィザードが表示されます。
3. 役割の追加ウィザードに書かれている条件を満たしていることを確認し、[次へ] をクリックしてください。
次の画面が表示されます。

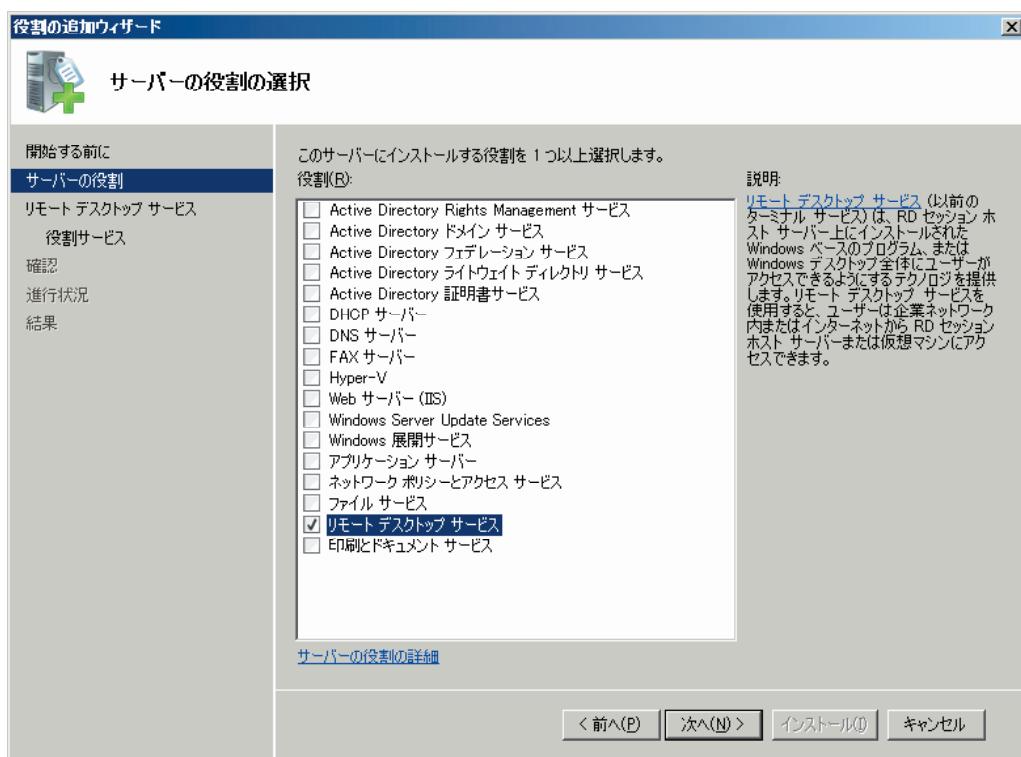


図 B5.1.2-1 役割の追加ウィザード—サーバーの役割の選択

4. [サーバーの役割の選択] リストから、[リモートデスクトップサービス] を選択し、[次へ] をクリックしてください。
5. 表示される画面のメッセージを確認後、[次へ] をクリックしてください。
役割サービスの選択ウィンドウが表示されます。

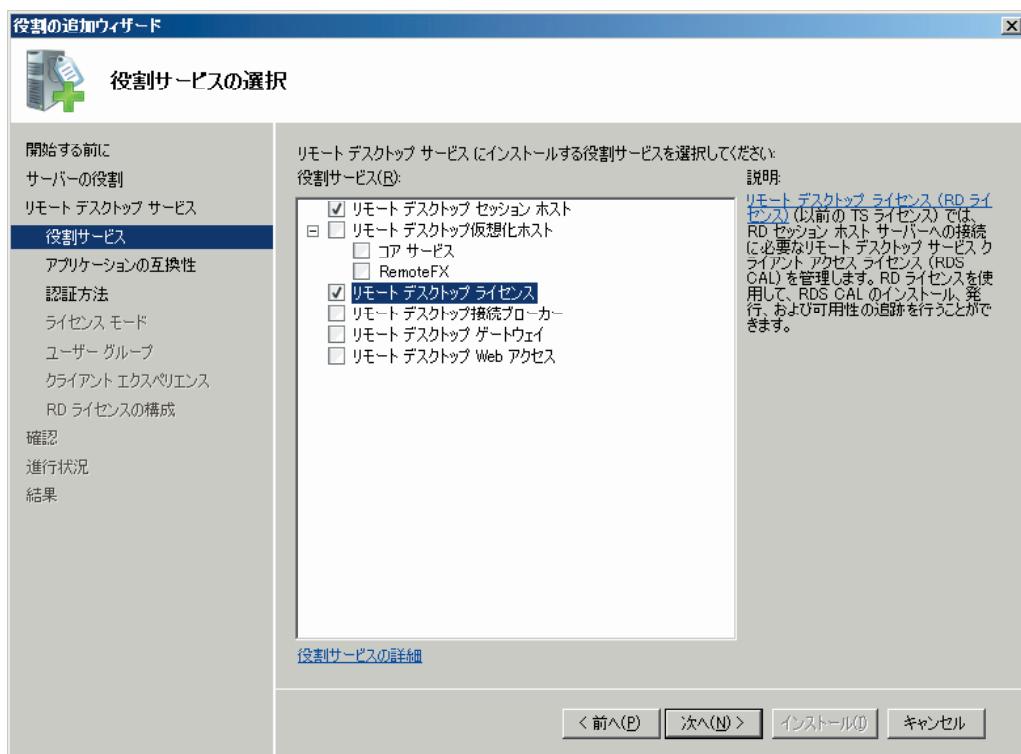


図 B5.1.2-2 役割の追加ウィザード—役割サービスの選択

6. [役割サービスの選択] リストから、[リモートデスクトップセッションホスト] と [リモートデスクトップライセンス] を選択し、[次へ] をクリックしてください。
互換性維持のためのアプリケーションのアンインストールと再インストールウィンドウが表示されます。

補足

複数のターミナルサーバがある場合、[リモートデスクトップライセンス] は共有できますので、必要に応じてチェックボックスをオンにしてください。すでに存在しているライセンスサーバに接続する場合、ライセンスサーバがリモートデスクトップサーバと同じ Windows Server 2008 R2 以降の OS を実行していることを確認してください。

7. 画面のメッセージを確認後、[次へ] をクリックしてください。
リモートデスクトップセッションホストの認証方法の指定ウィンドウが表示されます。

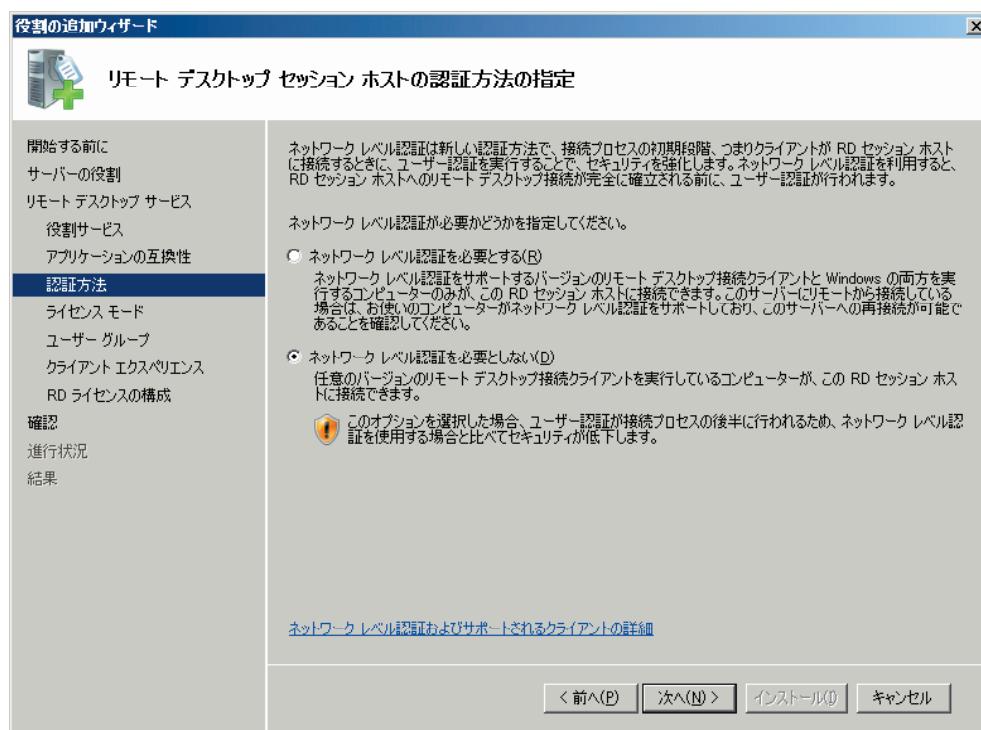


図 B5.1.2-3 役割の追加ウィザード—リモートデスクトップセッションホストの認証方法の指定

8. [ネットワークレベル認証を必要とする] を選択してください。
9. [次へ] をクリックしてください。
ライセンスマードの指定ウィンドウが表示されます。

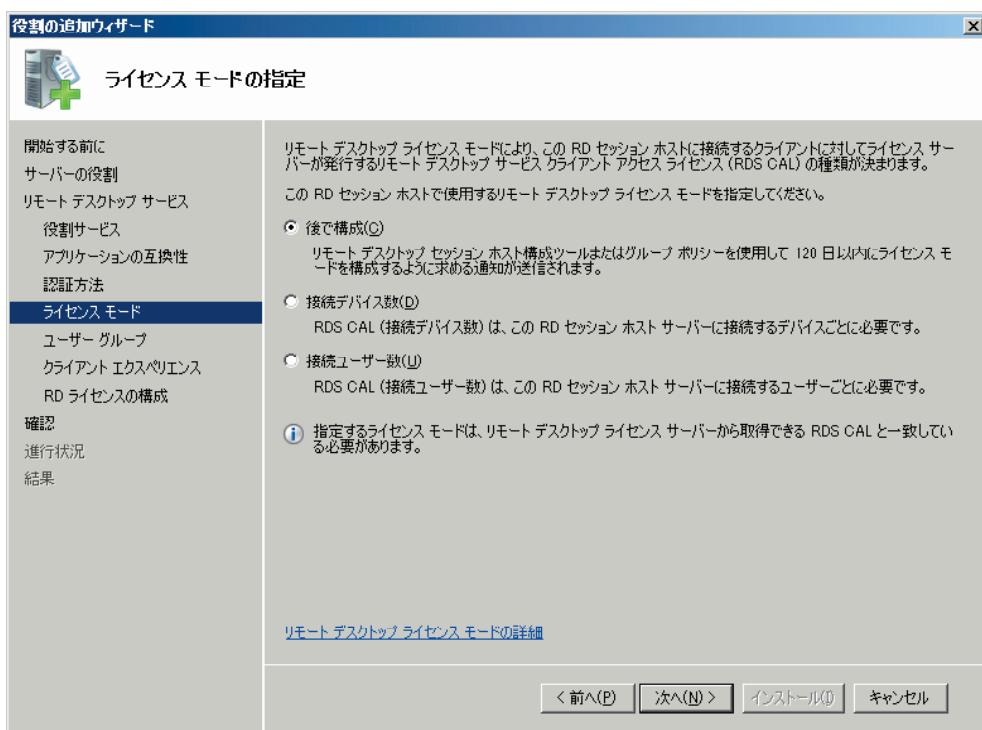


図 B5.1.2-4 役割の追加ウィザード—ライセンスマードの指定

10. このリモートデスクトップサーバで使用するリモートデスクトップライセンスマードを指定し、[次へ] をクリックしてください。

この RD セッションホストサーバへのアクセスが許可されたユーザーグループの選択ウィンドウが表示されます。

補足

ここで [後で構成] を選択したとしても、次のリモートデスクトップライセンスをアクティビ化する前には必ず設定が必要なため、ここでの設定を推奨します。

11. [次へ] をクリックしてください。

クライアントエクスペリエンスの構成ウィンドウが表示されます。

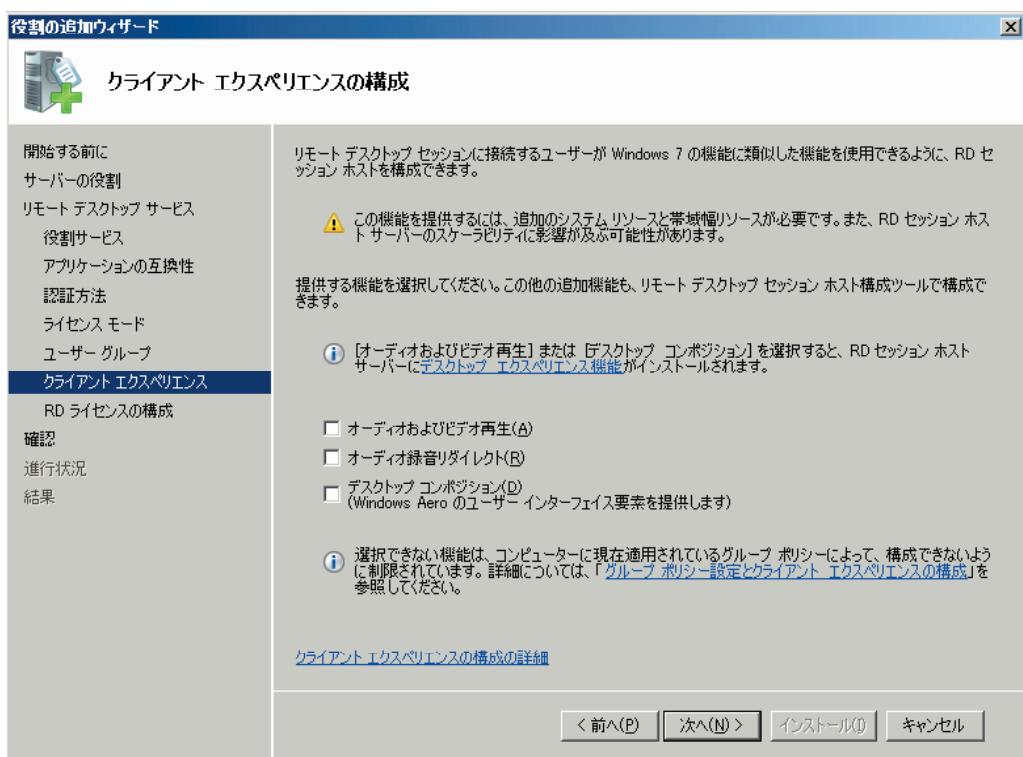


図 B5.1.2-5 役割の追加ウィザードークライアントエクスペリエンスの構成

補足

CETNUM VP のインストール後、リモートからログオンするユーザあるいはユーザグループを「Remote Desktop Users グループ」に登録する必要があります。

- すべての項目のチェックボックスをオフにし、[次へ] をクリックしてください。
RD ライセンスの検出スコープの構成ウィンドウが表示されます。

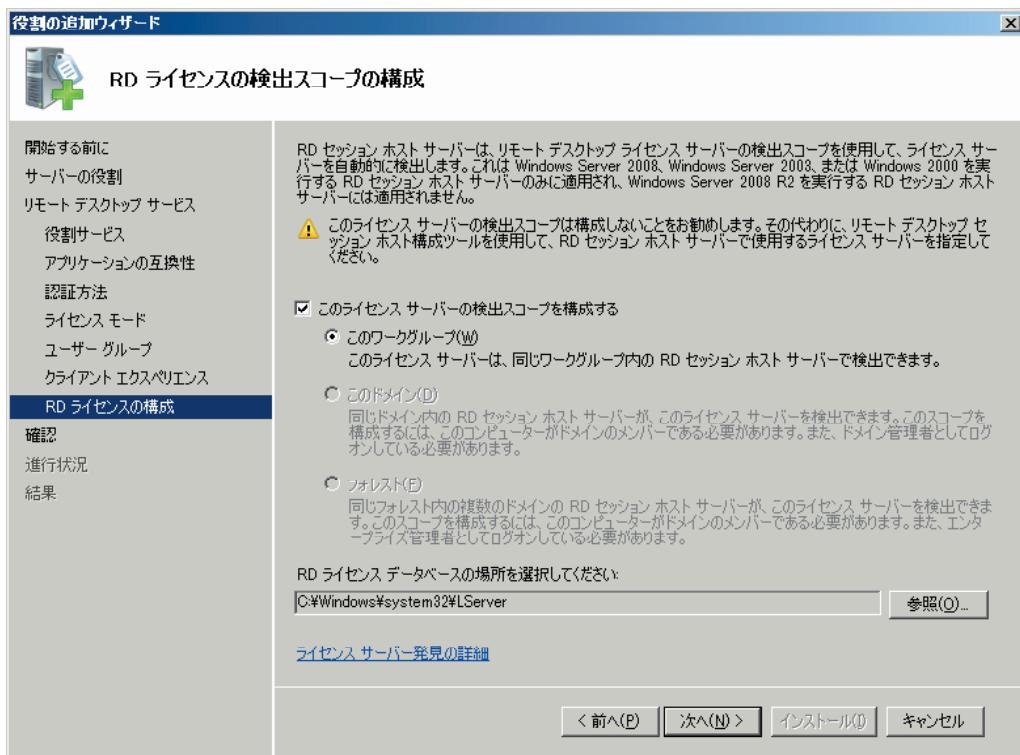


図 B5.1.2-6 役割の追加ウィザードーRD ライセンスの検出スコープの構成

13. [このライセンスサーバーの検出スコープを構成する] チェックボックスをオンにし、[このワークグループ] を選択し、[次へ] をクリックしてください（ドメイン管理で使用する場合は、[このドメイン] を選択してください）。
- インストールオプションの確認ウィンドウが表示されます。

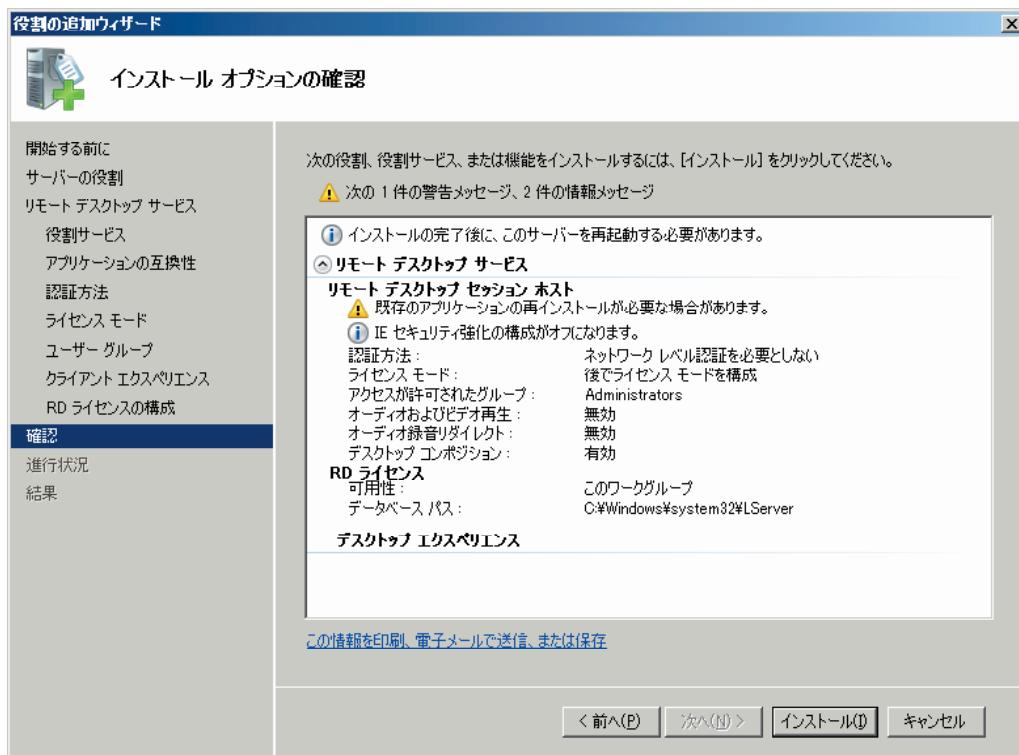


図 B5.1.2-7 役割の追加ウィザード—インストールオプションの確認

14. 画面の説明を確認し、[インストール] をクリックしてください。
インストールが開始され、終了するとインストールの結果ウィンドウが表示されます。
15. 表示内容を確認し、[閉じる] をクリックしてください。
再起動を確認するダイアログが表示されます。
16. [はい] をクリックし、コンピュータを再起動してください。
再起動が終了するとインストールの結果を示すウィンドウが表示されます。
17. 内容を確認して [閉じる] をクリックしてください。

■ 手順 5：リモートデスクトップライセンスサーバの認証

- リモートデスクトップライセンスサーバの認証については、次の手順に従ってください。
- [サーバーマネージャー] – [役割] – [リモートデスクトップサービス] – [RD セッションホストの構成] を選択してください。
次のウィンドウが表示されます。

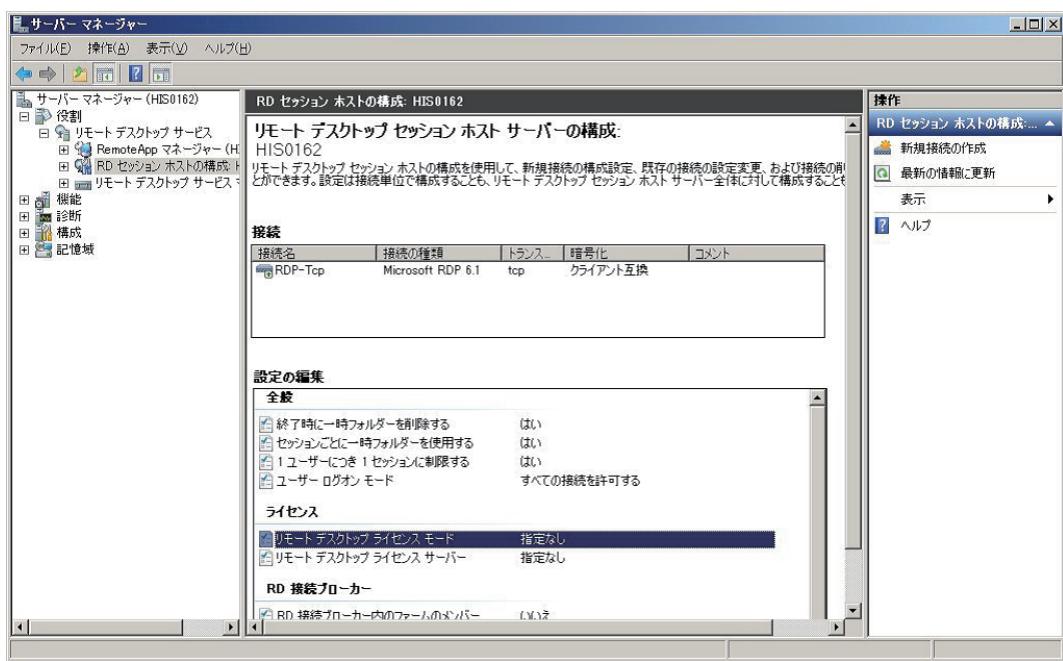


図 B5.1.2-8 RD セッションホストの構成

2. [設定の編集] 欄の [リモートデスクトップライセンスマード] をダブルクリックしてください。
ライセンスのプロパティが表示されます。

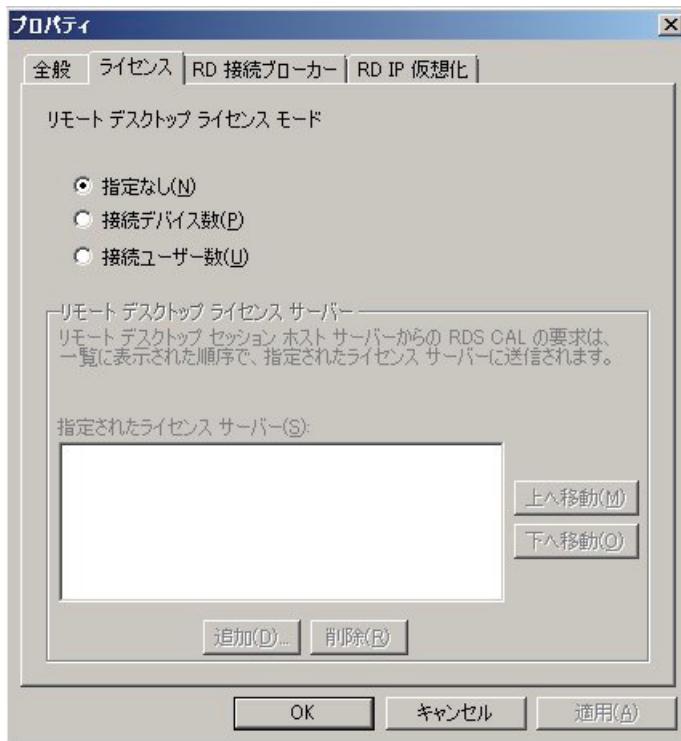


図 B5.1.2-9 プロパティダイアログ

3. 使用状況に合わせて設定をし、[OK] をクリックしてください。

補足

ライセンスサーバーの指定をしない場合、120 日後にアクセスができなくなります。

4. [サーバーマネージャー] – [役割] – [リモートデスクトップサービス] を選択してください。
次のウィンドウが表示されます。



図 B5.1.2-10 サーバーマネージャー

5. [詳細ツール] 欄の [リモートデスクトップライセンスマネージャー] をクリックしてください。
RD ライセンスマネージャーが起動します。

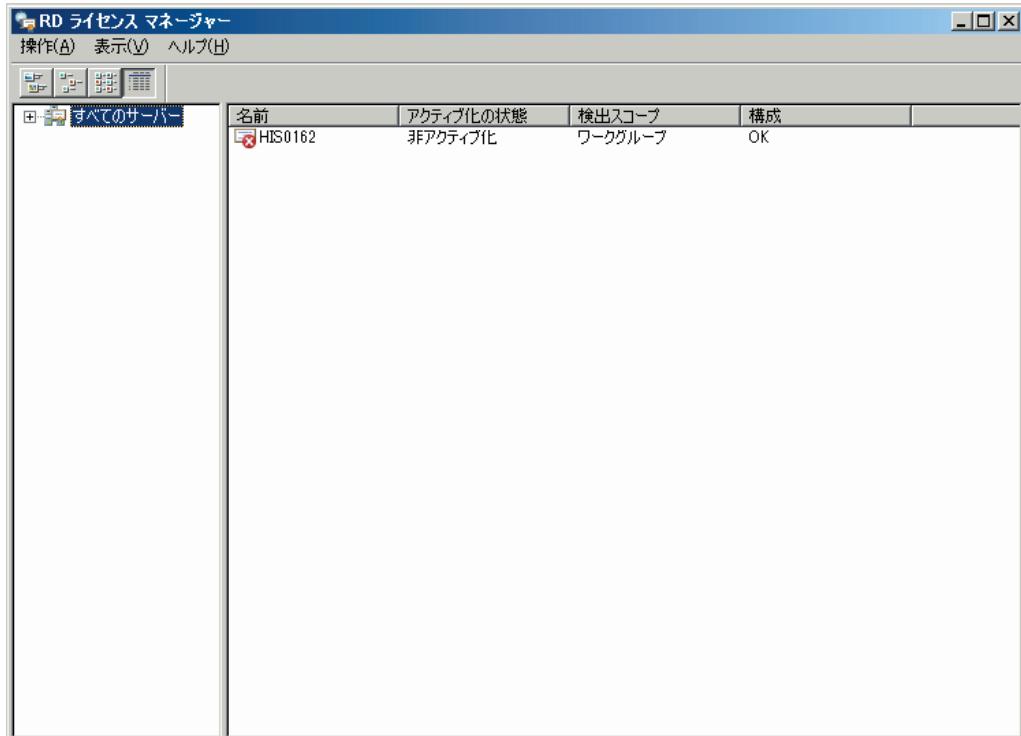


図 B5.1.2-11 RD ライセンスマネージャー

6. 認証するコンピュータを選択し、メニューバーから [操作] – [サーバーのアクティブ化] を選択してください。
サーバーのアクティブ化ウィザードが表示されます。
7. ウィザードの指示に従い、作業を行ってください。

補足

リモートデスクトップサービスのクライアントアクセスライセンス (RDS CAL) をインストールするには、最初にリモートデスクトップライセンスサーバーの認証の手続きを Microsoft に対して行う必要があります。ライセンスサーバーのアクティベーションが正常に完了したら、RDS CAL をインストールしてください。認証の手続きについては、Microsoft に問い合わせてください。

■ 手順 6：オーディオ使用の設定をする

リモートデスクトップサービス接続時にオーディオを使用するためには、オーディオサービスの有効化、システムサウンドサービスの実行をする必要があります。

● オーディオサービスの有効化

1. コントロールパネルを起動してください。
2. [システムとセキュリティ] – [管理ツール] – [サービス] を選択してください。
サービスウィンドウが表示されます。
3. [Windows Audio] をダブルクリックしてください。
Windows Audio のプロパティダイアログが表示されます。

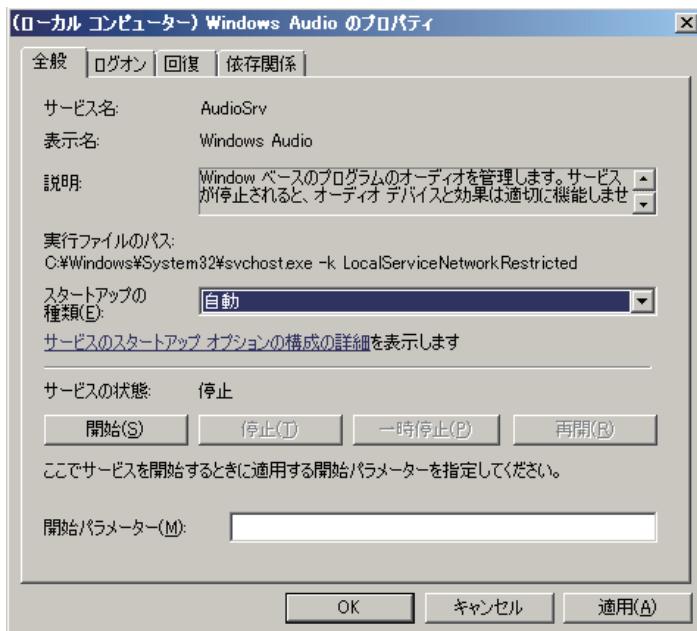


図 B5.1.2-12 Window Audio のプロパティダイアログ

4. [スタートアップの種類] ドロップダウンリストボックスから [自動] を、[サービスの状態] では [開始] を選択し、[OK] をクリックしてください。
5. サービスウィンドウで、Windows Audio の状態が「開始」、スタートアップの種類が「自動」になっていることを確認してください。

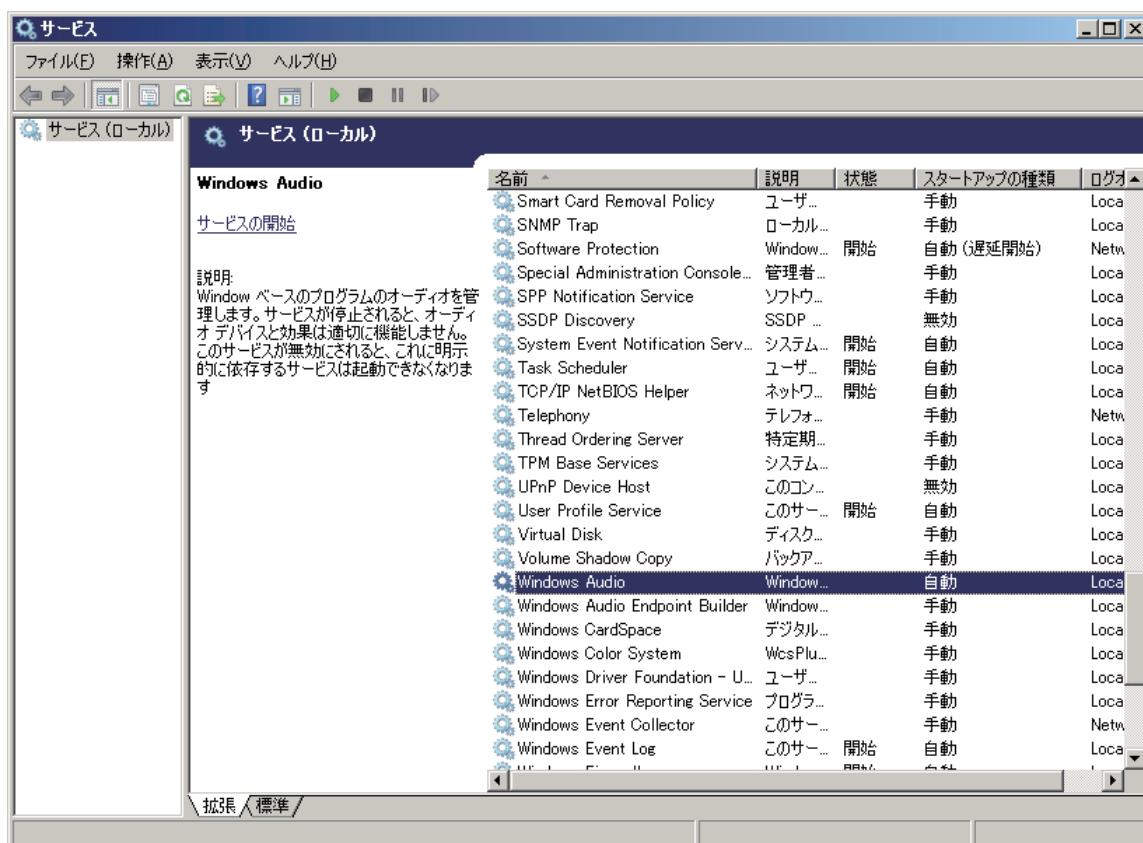


図 B5.1.2-13 サービス画面

● デスクトップエクスペリエンスのインストール

- [サーバーマネージャー] – [機能] を選択してください。
サーバーマネージャーが表示されます。
- [機能の概要] 欄の [機能の追加] をクリックしてください。
機能の追加ウィザードが表示されます。
- [デスクトップエクスペリエンス] チェックボックスをオンにしてください。
機能の追加を確認するダイアログが表示されます。
- [必要な機能を追加] をクリックしてください。
機能の追加ウィザードに戻ります。
- [次へ] をクリックしてください。
- インストールを行う項目に、「インクと手書きサービス インクサポート」と「デスクトップエクスペリエンス」があることを確認し、[インストール] をクリックしてください。
インストールが開始されます。
- インストール結果に、「インクと手書きサービス」と「デスクトップエクスペリエンス」が追加されていることを確認し、[閉じる] をクリックしてください。
コンピュータが再起動します。
- 再起動後、インストールの結果画面で「インクと手書きサービス」と「デスクトップエクスペリエンス」が正常にインストールされたことを確認し、[閉じる] をクリックしてください。

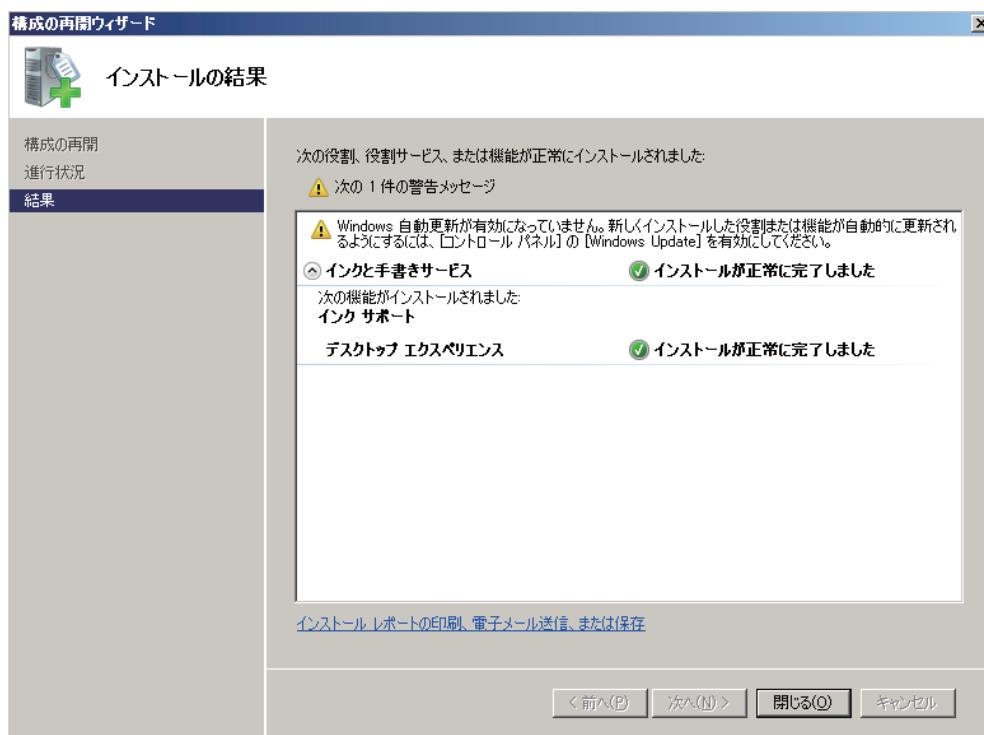


図 B5.1.2-14 インストールの結果－再起動後

● システムサウンドサービスの実行

1. コントロールパネルを起動してください。
2. [システムとセキュリティ] – [管理ツール] – [タスクスケジューラ] を選択してください。
タスクスケジューラウィンドウが表示されます。
3. [タスクスケジューラライブラリ] – [Microsoft] – [Windows] – [Multimedia] を選択してください。
4. [System Sound Service] を右クリックし、[有効] を選択してください。

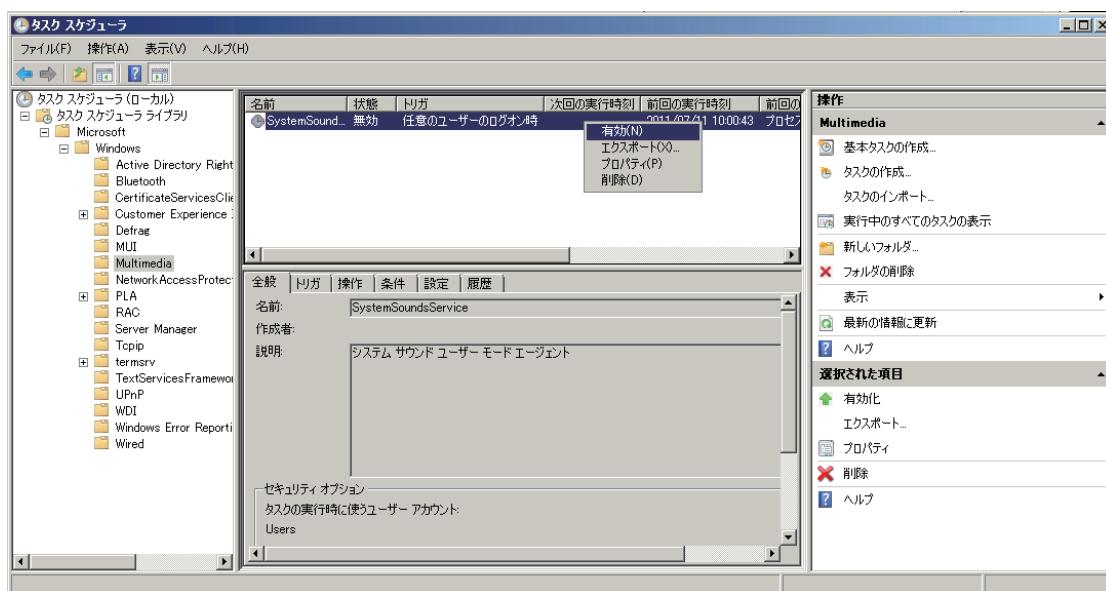


図 B5.1.2-15 タスクスケジューラウィンドウ－SystemSoundService の有効化

5. [System Sound Service] を右クリックし、[実行する] を選択してください。

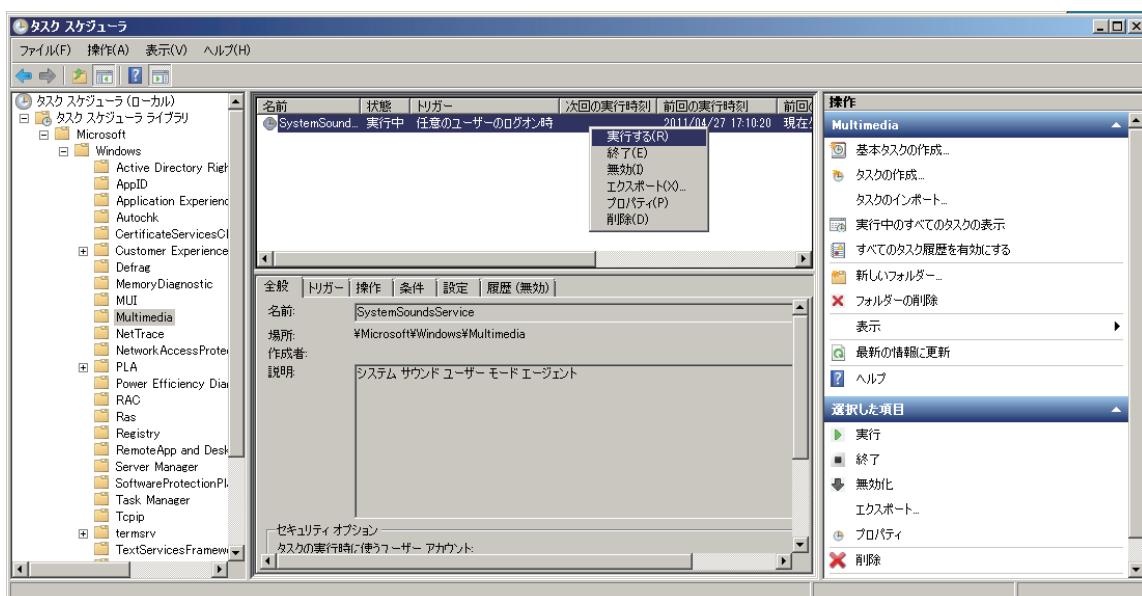


図 B5.1.2-16 タスクスケジューラウィンドウ –SystemSoundService の実行

■ 手順 7 : CENTUM VP ソフトウェアのインストールをする

リモート操作監視サーバのための CENTUM VP のインストールは、HIS と同様です。

参照

CENTUM VP ソフトウェアのインストールについては、以下を参照してください。

「B4.6 CENTUM VP ソフトウェアのインストールをする」ページ B4-87

■ 手順 8 : IT セキュリティを設定する

CENTUM VP では、ソフトウェアのインストール後に、コンピュータの IT セキュリティを強化するための設定を行う必要があります。

参照

IT セキュリティを設定する手順については、以下を参照してください。

「B4.7 IT セキュリティを設定する」ページ B4-96

■ 手順 9 : Remote Desktop Users のメンバ登録をする

IT セキュリティの設定後、リモートからログオンするユーザ、あるいはユーザグループを「Remote Desktop Users」グループに登録します。ここでは RemoteCentum ユーザを「Remote Desktop Users」グループに登録する手順を説明します。

1. サーバコンピュータに Administrator でログオンしてください。
サーバーマネージャーが表示されます。
2. [ツール] – [コンピュータの管理] を選択してください。
コンピュータの管理ウィンドウが表示されます。
3. [コンピュータの管理] – [ローカルユーザーとグループ] – [グループ] を選択してください。
グループの一覧が表示されます。
4. 「Remote Desktop Users」を選択し、右クリックで [グループに追加] を選択してください。

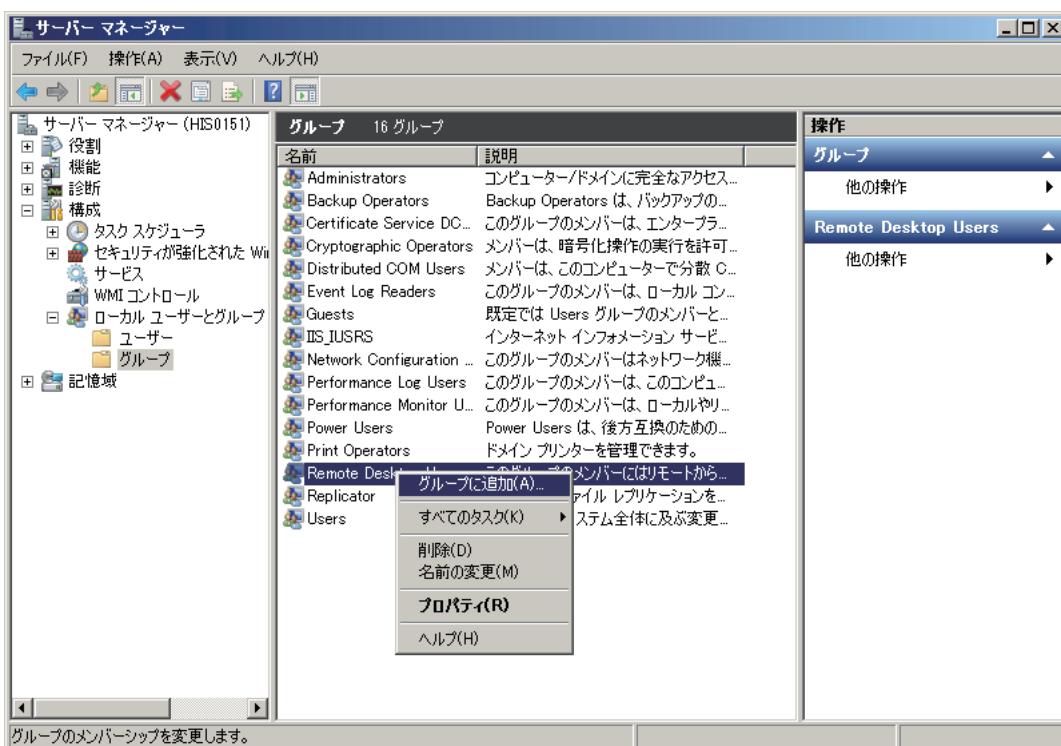


図 B5.1.2-17 コンピュータの管理ウィンドウ

Remote Desktop Users に所属するユーザの一覧が表示されます。

5. [全般] タブの [追加] をクリックしてください。
ユーザーの選択ダイアログが表示されます。
6. [詳細設定] をクリックしてください。
詳細設定の欄が追加で表示されます。
7. [場所] をクリックしてください。
場所の一覧が表示されます。

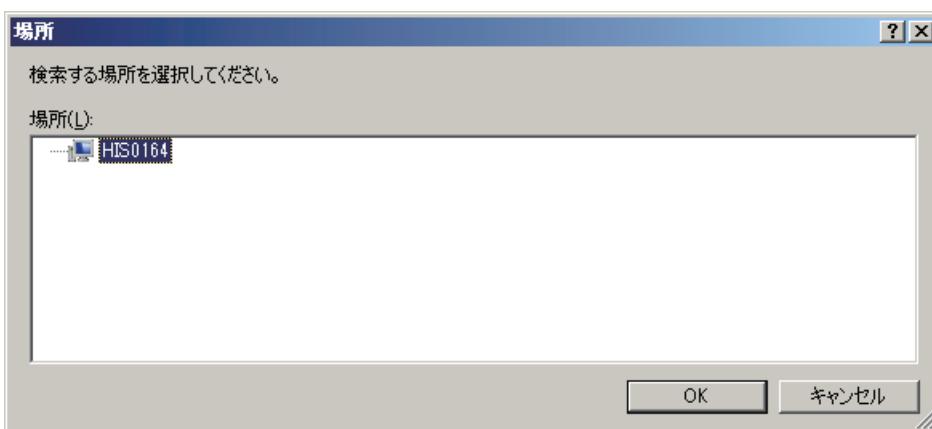


図 B5.1.2-18 場所の一覧

8. 追加したいユーザの所属するコンピュータ名またはドメイン名を選択し、[OK] をクリックしてください。
ユーザの選択ダイアログに戻ります。
9. [検索] をクリックしてください。
選択したコンピュータもしくはドメインに属するユーザの一覧が表示されます。

補足

場所の指定にドメイン名を選択したときは、ドメインの設定によってはユーザの一覧が表示されない場合があります。また、ドメインに所属するユーザ数が 10000 を超えるときには、すべてのユーザを一覧表示することができません。

この場合には、詳細設定ダイアログを [キャンセル] で閉じ、[選択するオブジェクト名] 欄にユーザ名を直接入力してください。

例： ドメインユーザを指定する場合 somedomain¥RemoteCentum

ローカルユーザを指定する場合 HIS0164¥RemoteCentum

- 追加したいユーザである RemoteCentum を選択し、[OK] をクリックしてください。グループに所属するメンバーに、RemoteCentum が追加されます。

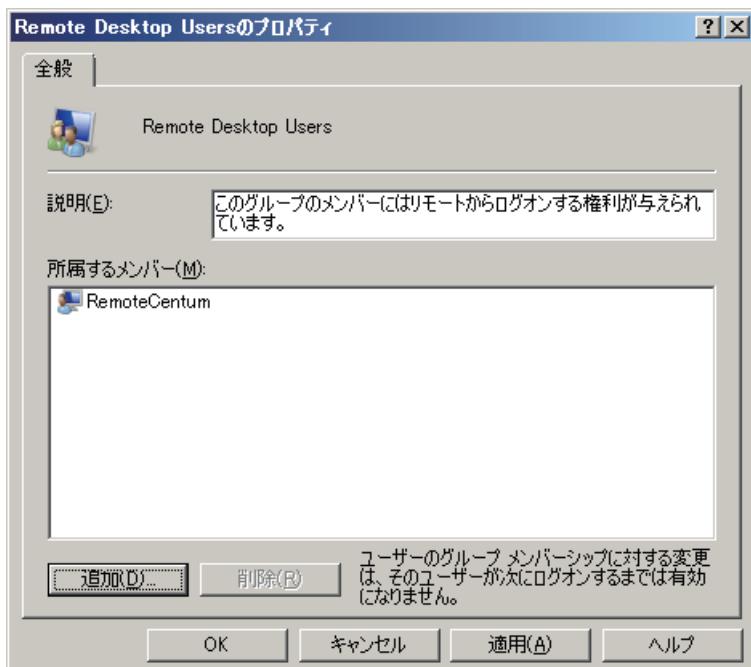


図 B5.1.2-19 Remote Desktop Users のプロパティ

- [OK] をクリックしてください。

■ 手順 10：ライセンスの配布と反映をする

リモート操作監視サーバ機能に加え、必要なパッケージのライセンスを、ライセンス管理ステーションから配布し、反映してください。

参照

ライセンスの配布と反映をする手順については、以下を参照してください。

「B4.8 ライセンスの配布と反映をする」ページ B4-103

■ 手順 11：ユーザアカウントを作成する

ユーザアカウントの作成をする必要があります。

参照

ユーザアカウントの作成については、以下を参照してください。

「B4.9 ユーザアカウントを作成する」ページ B4-104

■ 手順 12：ユーザごとの Windows 動作環境の設定をする

ログオンユーザごとに Windows 動作環境の設定をする必要があります。

参照

ユーザごとの Windows 動作環境の設定をする手順については、以下を参照してください。

「B4.10 ユーザごとの Windows 動作環境の設定をする」ページ B4-109

■ 手順 13：ユーザ認証モードの設定をする

ユーザ認証モードの設定をする必要があります。

参照

ユーザ認証モードの設定手順については、以下を参照してください。

「B4.11 ユーザ認証モードの設定をする」ページ B4-136

■ 手順 14：UPS（無停電電源装置）の設定をする

UPS を使用する場合は、その設定をする必要があります。

参照

UPS（無停電電源装置）の設定をする手順については、以下を参照してください。

「B4.12 UPS（無停電電源装置）の設定をする」ページ B4-149

■ 手順 15：RemoteApp プログラムの設定をする

リモートで HIS-TSE サーバに接続するコンピュータから、CENTUM VP 操作監視機能を使用可能とするため、リモートデスクトップサービスの設定を行います。

● StartDesktop.bat の追加

1. [サーバーマネージャー] – [役割] – [リモートデスクトップサービス] – [RemoteApp マネージャー] を選択してください。
サーバーマネージャーが表示されます。
2. [操作] 欄から、[RemoteApp プログラムの追加] をクリックしてください。
RemoteApp ウィザードが起動します。
3. ウィザードの内容を確認し、[次へ] をクリックしてください。
プログラム選択の画面が表示されます。
4. [参照] をクリックしてください。
プログラムの選択ウィンドウが表示されます。
5. StartDesktop.bat ファイルが存在するフォルダから、StartDesktop.bat を開いてください。
追加するプログラムを選択する画面で、[StartDesktop.bat] チェックボックスがオンになります。

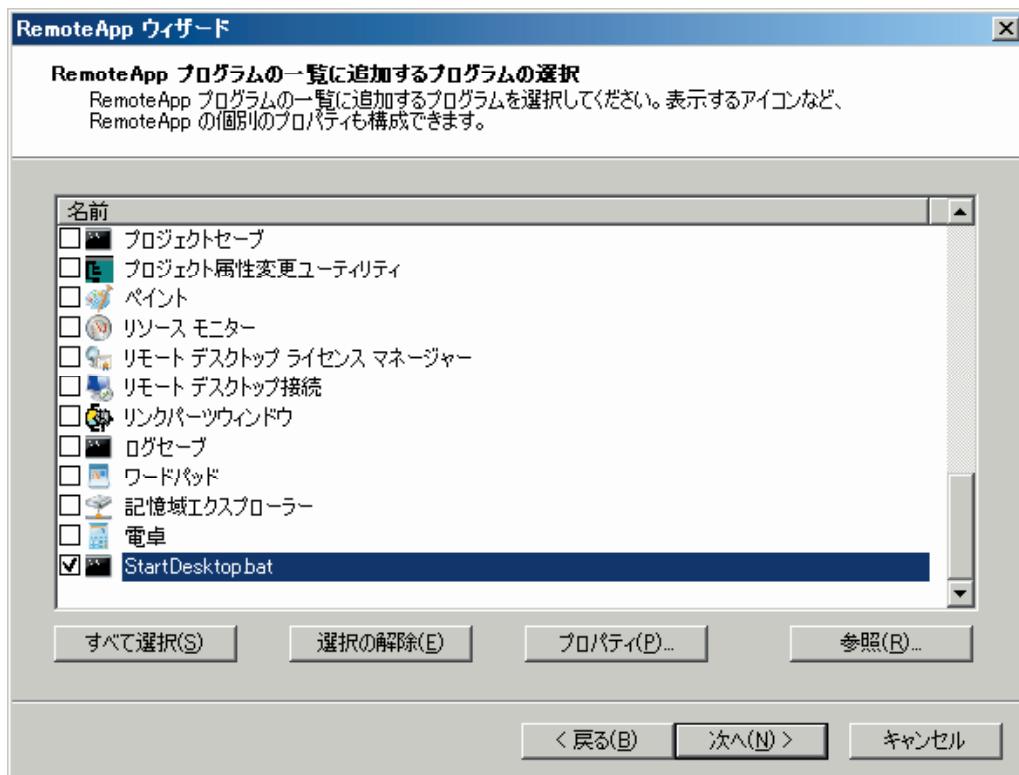


図 B5.1.2-20 RemoteApp ウィザード

補足

C:\CENTUMVP に CENTUM VP をインストールした場合は、c:\CENTUMVP\program フォルダに、StartDesktop.bat ファイルが存在します。

6. 確認したのち、[次へ] をクリックしてください。
設定の確認画面が表示されます。

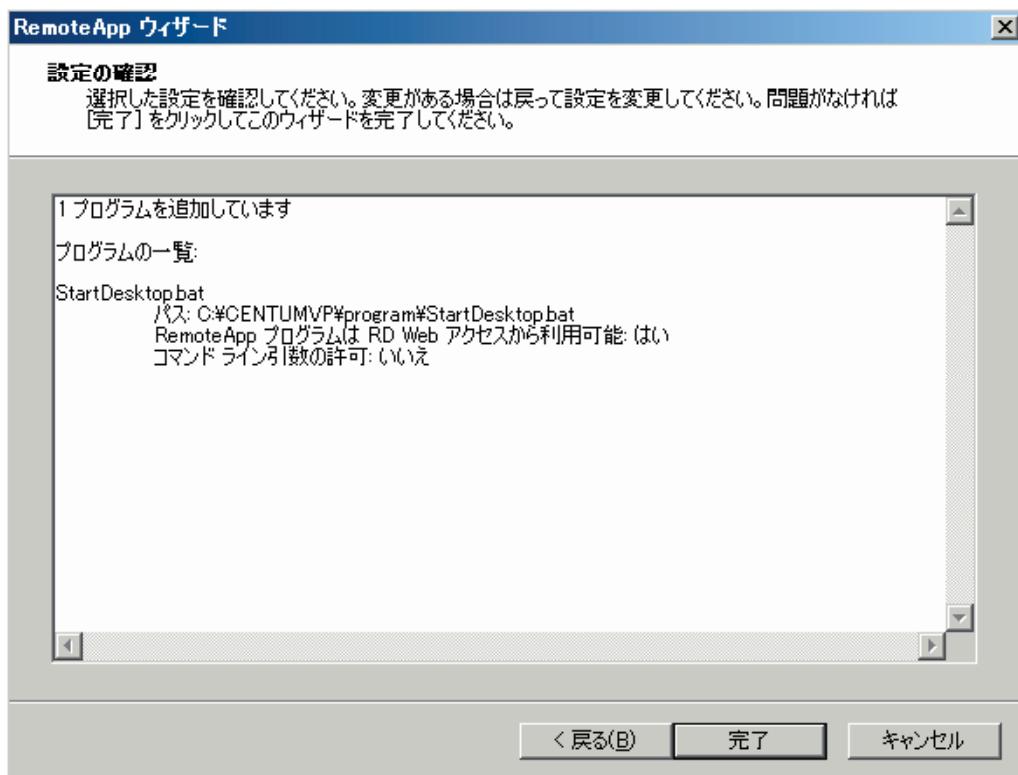


図 B5.1.2-21 RemoteApp ウィザード – 設定の確認

7. 設定内容が上記と同じになっていることを確認し、[完了] をクリックしてください。
8. RemoteApp マネージャーの RemoteApp プログラムテーブルに、StartDesktop.bat が追加されていることを確認してください。

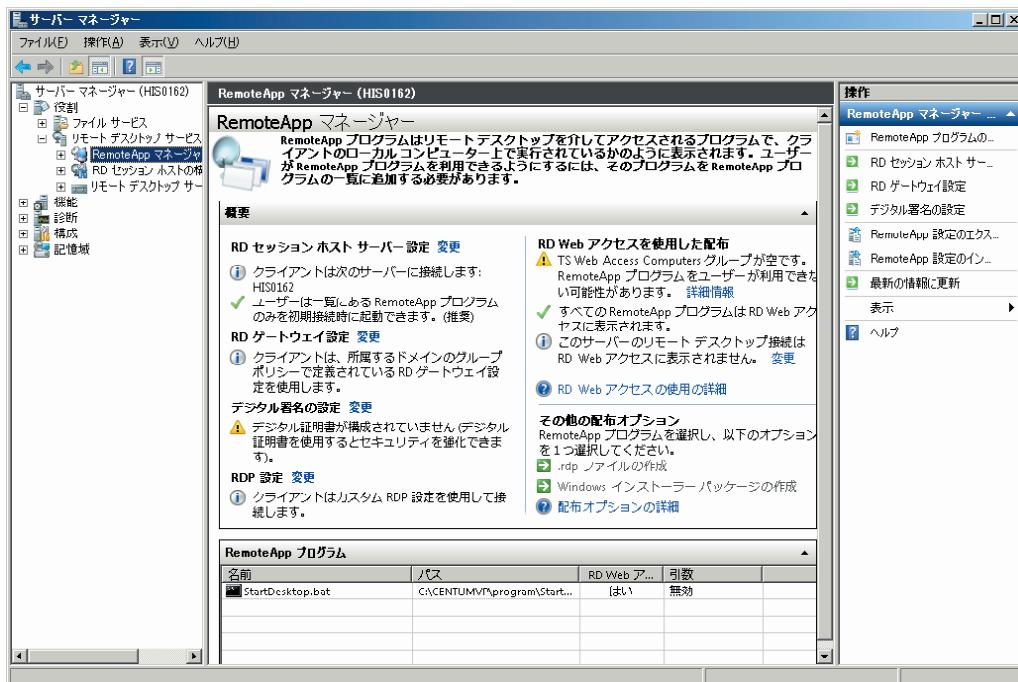


図 B5.1.2-22 サーバーマネージャー – RemoteApp マネージャー

● BKHBos.exe の追加

この設定は、パネルモードを使用する場合のみ必要です。

1. [サーバーマネージャー] - [役割] - [リモートデスクトップサービス] - [RemoteApp マネージャー] を選択してください。
サーバーマネージャーが表示されます。
2. [操作] 欄から、[RemoteApp プログラムの追加] をクリックしてください。
RemoteApp ウィザードが起動します。
3. ウィザードの内容を確認し、[次へ] をクリックしてください。
プログラム選択の画面が表示されます。
4. [参照] をクリックしてください。
プログラムの選択ウィンドウが表示されます。
5. BKHBos.exe ファイルが存在するフォルダから、BKHBos.exe を開いてください。
追加するプログラムを選択する画面で、[BKHBos.exe] チェックボックスがオンになります。

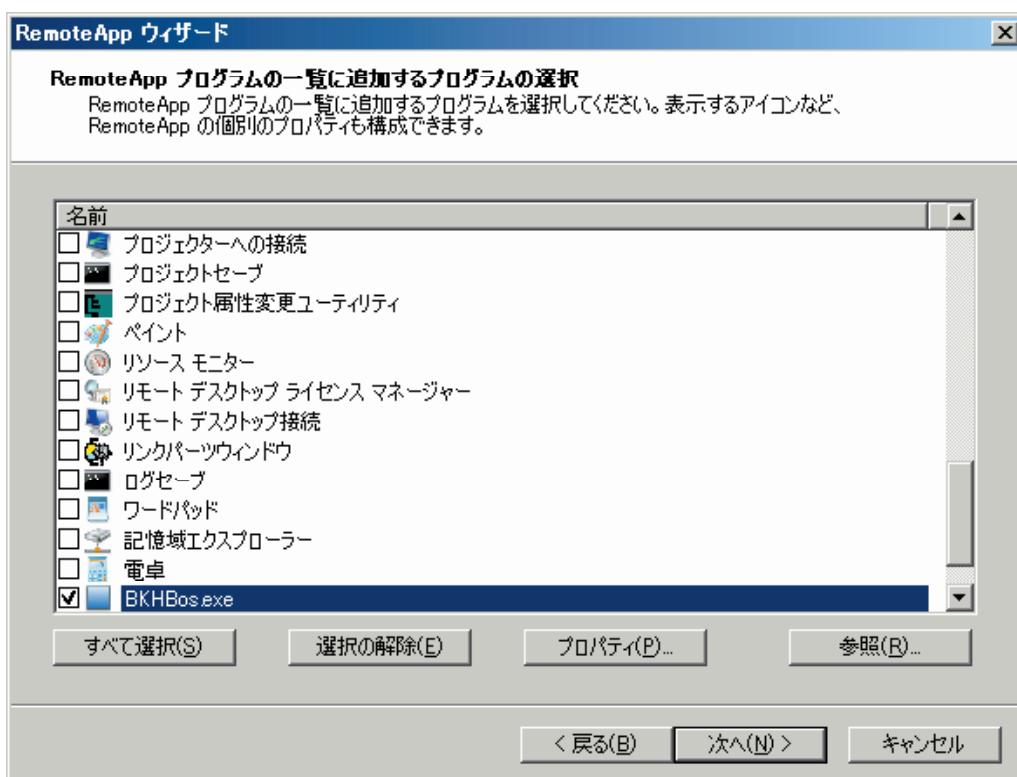


図 B5.1.2-23 RemoteAPP ウィザード

補足

C:\CENTUMVP に CENTUM VP をインストールした場合は、C:\CENTUMVP\program フォルダに、BKHBos.exe ファイルが存在します。

6. 確認したのち、[プロパティ] をクリックしてください。
BKHBOS.exe のプロパティダイアログが表示されます。
7. [コマンドライン引数] 欄で、[コマンドライン引数を許可する] を選択し、[OK] をクリックしてください。
操作続行の確認をするダイアログが表示されます。
8. [はい] をクリックしてください。
9. RemoteApp ウィザードで、[次へ] をクリックしてください。
設定の確認画面が表示されます。

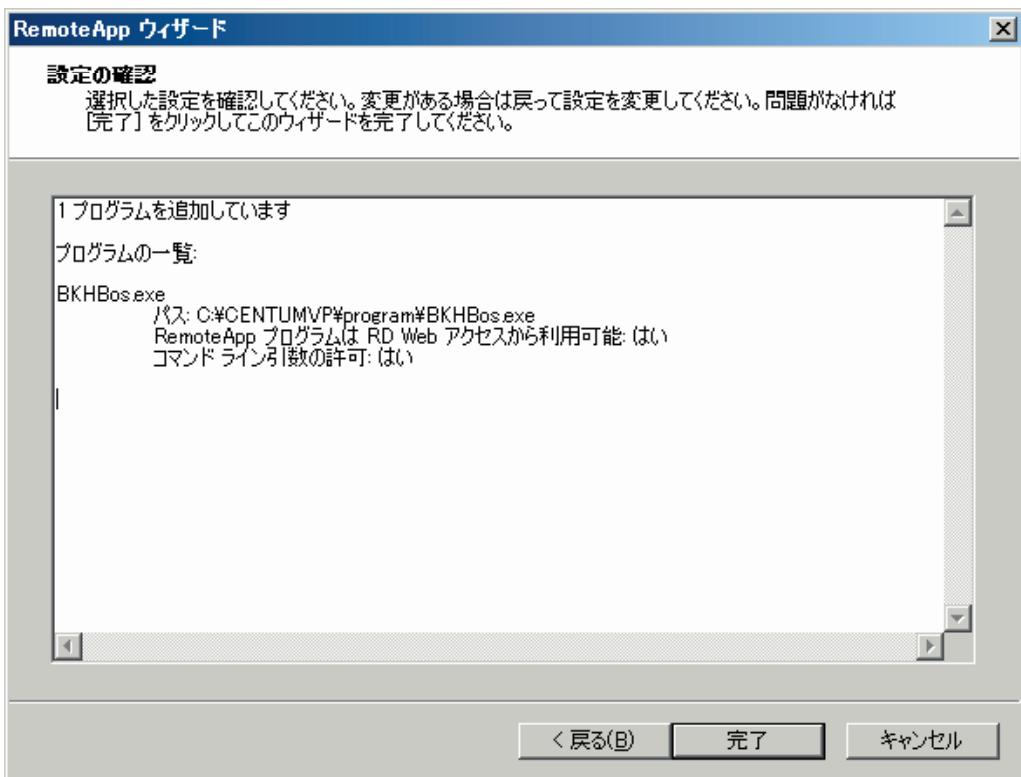


図 B5.1.2-24 RemoteAPP ウィザード – 設定の確認

10. 設定内容が上記画面と同じとなっていることを確認し、[完了] をクリックしてください。
11. RemoteApp マネージャーの RemoteApp プログラムテーブルに BKHBOS.exe が追加され、引数が「制限なし」になっていることを確認してください。



図 B5.1.2-25 サーバーマネージャー – RemoteAPP マネージャー

■ 手順 16：リモートデスクトップサービスの設定をする

1. サーバコンピュータに Administrator でログオンしてください。

- サーバーマネージャーが表示されます。
2. [サーバーマネージャー] – [役割] – [リモートデスクトップサービス] – [RD セッションホストの構成] を選択してください。
サーバーマネージャーが表示されます。
 3. [設定の編集] 欄で、[1 ユーザにつき 1 セッションに制限する] をダブルクリックしてください。
プロパティダイアログが表示されます。

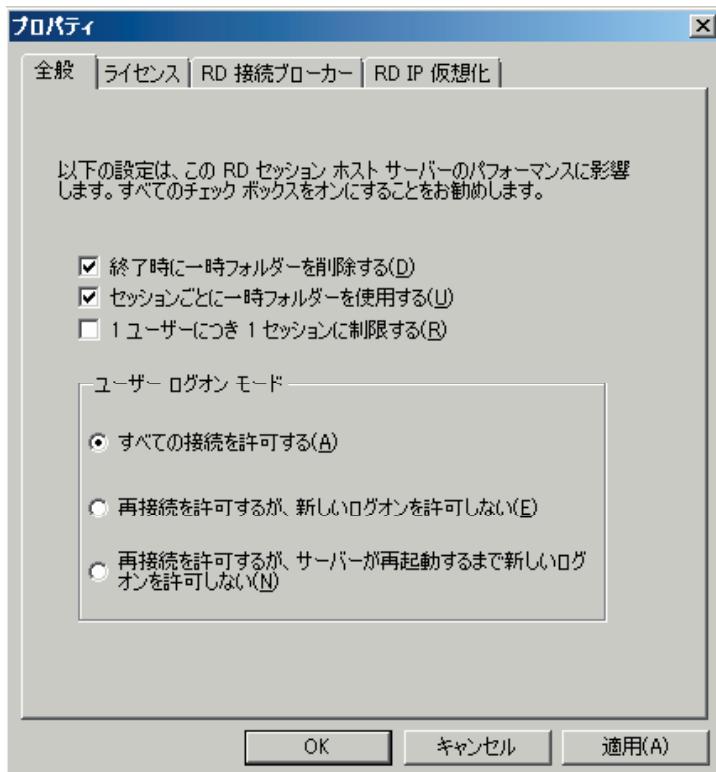


図 B5.1.2-26 プロパティダイアログ

4. 全般タブの、[1 ユーザにつき 1 セッションに制限する] チェックボックスを、条件に応じて、オン／オフしてください。
 - ・ IT セキュリティで従来モデル（常に CENTUM でログオン）を使用する場合には、オフにしてください。
 - ・ IT セキュリティで標準モデルを選択し、オペレータが個別名でログオンする運用の場合などは、オンにしてください。
5. ライセンスタブで、ライセンス使用状況に応じてリモートデスクトップサービスライセンスマード（接続ユーザー数／接続デバイス数）を設定してください。
6. [OK] をクリックしてください。
7. サーバーマネージャーで、[接続] 欄から [RDP-Tcp] を右クリックし、[プロパティ] を選択してください。
プロパティダイアログが表示されます。

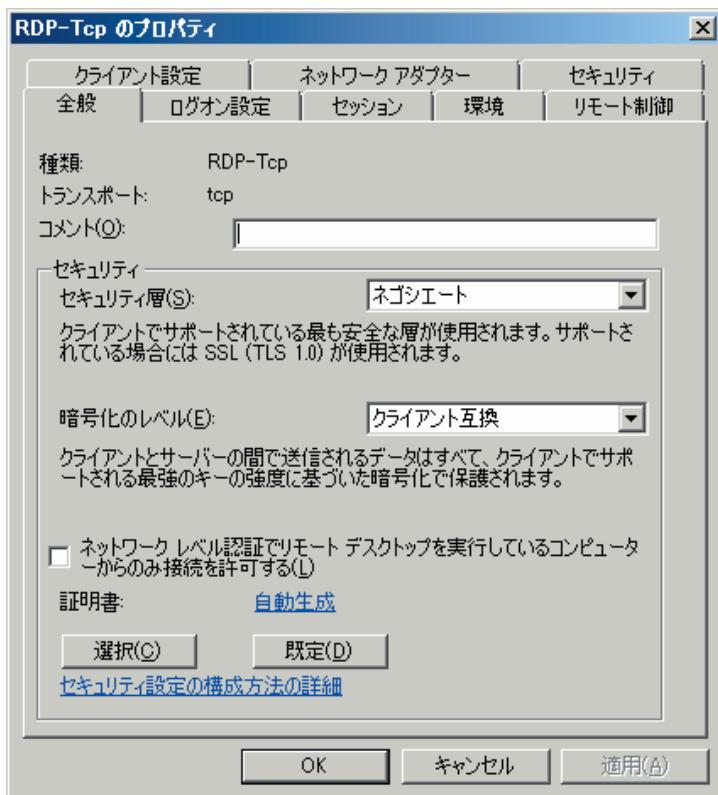


図 B5.1.2-27 RDP-Tcp のプロパティダイアログ

8. 全般タブで、[ネットワークレベル認証でリモートデスクトップを実行しているコンピューターからのみ接続を許可する] チェックボックスをオンにしてください。

補足

上記以外の項目は、デフォルトのままにしてください。

9. ログオン設定タブで、状況に応じて項目を設定してください。通常はデフォルトの[クライアントが提供したログオン情報を使用する] のままで問題ありません。

補足

接続するクライアントのアカウントを CENTUM ユーザに限定したい場合は、[次のログオン情報を常に使う] を選択し、[ユーザー名] に CENTUM と記述し、[パスワード] と [パスワード認証] をあらかじめ記述することにより、クライアントからは必ず CENTUM でログオンするように設定できます。たとえクライアントで他のアカウントでログオンするように設定しても、この設定はクライアントの設定よりも優先されるため、CENTUM でログオンします。パスワードを入力しないか、[常にパスワードの入力を求める] チェックボックスがオンの場合、クライアントからの接続時にログオンダイアログが表示され、そこでログオンユーザ名を書き替えることができるため、CENTUM 以外のユーザでもログオンが可能になります。

10. セッションタブで、[ユーザー設定よりも優先する] チェックボックスをオンにし、[切断されたセッションの終了] を「1分」にしてください。
11. 環境タブで、状況に応じて項目を設定してください。デフォルトのままでも問題ありません。

補足

HIS TSE をデスクトップモードでしか使用しない場合は、この設定で、HIS TSE サーバーに接続しただけで HIS が自動的に起動するようにできます。

「ログオン設定」と組み合わせると、クライアントプログラムから接続先を指定するだけで CENTUM ユーザでログオンし、HIS が自動的に起動することが可能です。

設定方法は次のとおりです。

1. [ユーザのログオン時に次のプログラムを開始する] のチェックボックスをオンにします。
2. [プログラムのパスとファイル名] に、StartDesktop.bat ファイルへのパスを記述します。
c:\CENTUMVP に、CENTUM VP をインストールした場合は、“c:\CENTUMVP\Program\StartDesktop.bat”とします。
3. [作業フォルダ] に、StartDesktop.bat ファイルが存在するフォルダを記述します。 c:\CENTUMVP に、CENTUM VP をインストールした場合は、“c:\CENTUMVP\Program”とします。

ダイアログの記述にもあるように、クライアントの設定よりも優先されるので、ここに記述するとデスクトップモードでしか起動しなくなります (StartDesktop.bat というバッチファイルは、デスクトップモードで起動するためのバッチファイルです)。

12. リモート制御タブで、[リモート制御を許可しない] を選択してください。
13. クライアント設定タブで、[色の深度] 欄の [色の深度の最大数を制限する] チェックボックスをオフにしてください。
14. 同じくクライアント設定タブでの [リダイレクト] 欄で、[オーディオ録音] と [オーディオおよびビデオの再生] をオフにしてください。
15. ネットワークアダプタータブで、HIS TSE サーバとクライアント間での通信に使用するネットワークアダプターを指定してください。「Yokogawa Vnet/VLnet adapter」は指定しないでください。
16. [OK] をクリックしてください。

■手順 17：プロジェクトに HIS-TSE を追加する

1. システムビューで HIS-TSE を追加するプロジェクトを開いてください。
2. ステーションタイプに [HIS-TSE リモート操作監視サーバ機能搭載 HIS] を指定して、ステーションを追加してください。
3. 標準 HIS の場合と同様の操作で、[プロジェクト共通部ダウンロード]、[HIS ダウンロード]、[タグリストダウンロード] を実行してください。
4. リモート操作監視サーバを再起動してください。

参照

HIS 新規作成時のビルダ定義項目については、以下を参照してください。

エンジニアリングリファレンス Vol.1 (IM 33J10D10-01JA) の「2.4.2 HIS の新規作成」

B5.2 HIS-TSE クライアントの設定をする

リモート操作監視サーバ機能を使用するには、HIS-TSE サーバと同時に、HIS-TSE クライアントの設定をする必要があります。

参照

HIS-TSE クライアントの設定については、以下を参照してください。

CENTUM VP オプション機能リファレンス (IM 33J05H10-01JA) の「7.1 HIS-TSE での操作監視」

Blank Page

B6. ファイルサーバのセットアップをする

ファイルサーバを設け、このコンピュータに置いたファイルを他のコンピュータから参照できます。

ファイルサーバには、システム生成機能のプロジェクトデータベースや、処方データベースを配置して、ネットワーク経由で参照、操作する構成をとることができます。

補足

履歴管理データベースは、専用でコンピュータを用意する必要があります。

ここでは、次の場合のファイルサーバのセットアップ方法を説明します。

- ・ ファイルサーバ専用コンピュータ
- ・ HIS/システム生成機能/AD サーバのみを搭載したコンピュータと兼用するファイルサーバ
- ・ ライセンス管理ステーションと兼用するファイルサーバ

参照

履歴管理データベース用サーバのセットアップについては、以下を参照してください。

FDA : 21CFR Part11 対応リファレンス (IM 33J10D21-01JA) の「4. ビルダのアクセス制限と履歴管理の設定」

■ 用意するもの

サーバをセットアップする前に、次のものを手元に用意してください。

- ・ CENTUM VP 用ソフトウェアメディア

■ ファイルサーバの OS とハードウェア環境

ファイルサーバとして使用できる OS とハードウェア環境を示します。

表 B6-1 ファイルサーバの OS とハードウェア環境

対応 OS	ハードウェア環境
Windows Server 2016 Standard Edition	プロセッサ：2 GHz 以上 メモリ：2 GB 以上 ハードディスク：32 GB 以上必須、50 GB 以上推奨 ドライブ：DVD-ROM ネットワークアダプタ：必須 ディスプレイ：Super VGA (800×600) 以上の解像度必須
Windows Server 2012 R2 Standard Edition	プロセッサ：2 GHz 以上 メモリ：2 GB 以上 ハードディスク：32 GB 以上必須、50 GB 以上推奨 ドライブ：DVD-ROM ネットワークアダプタ：必須 ディスプレイ：Super VGA (800×600) 以上の解像度必須
Windows Server 2008 R2 Standard Edition SP1	プロセッサ：2 GHz 以上 メモリ：2 GB 以上 ハードディスク：20 GB 以上必須、50GB 以上推奨 ドライブ：DVD-ROM ネットワークアダプタ：必須 ディスプレイ：Super VGA (800×600) 以上の解像度必須
Windows Server 2008 Standard Edition SP2	プロセッサ：2 GHz 以上 メモリ：2 GB 以上 ハードディスク：20 GB 以上必須、50 GB 以上推奨 ドライブ：DVD-ROM ネットワークアダプタ：必須 ディスプレイ：Super VGA (800×600) 以上の解像度必須

■ ファイルシステム

ファイルシステムは NTFS 形式にしてください。

B6.1 ファイルサーバ専用コンピュータのセットアップをする

ここでは、コンピュータをファイルサーバ専用として使用する場合のセットアップ方法について説明します。

■ セットアップする管理者ユーザ

ファイルサーバのセットアップは、次の表に示す管理者ユーザで実施してください。

表 B6.1-1 ファイルサーバをセットアップする管理者ユーザ

設定しようとするセキュリティモデル／ユーザ管理方法		
従来モデル	標準モデル	
	スタンドアロン管理	ドメイン管理／併用管理
Administrators ローカルグループに所属するローカルユーザ	Administrators ローカルグループと CTM_MAINTENANCE ローカルグループに所属するローカルユーザ	<ul style="list-style-type: none"> Domain Admins ドメイングループと CTM_MAINTENANCE ドメイングループに所属するドメインユーザ Administrators ローカルグループと CTM_MAINTENANCE ローカルグループに所属するドメインユーザ Administrators ローカルグループと CTM_MAINTENANCE ローカルグループに所属するローカルユーザ (*1)

*1: セットアップ中にドメインユーザのユーザ名とパスワードを入力する必要があります。

補足

ユーザ管理方法がドメイン管理／併用管理の場合は、コンピュータがドメインに参加した状態でセットアップを実施してください。

■ 手順 1: Microsoft Visual C++ 2017 再頒布可能パッケージのインストール

IT セキュリティツールを実行する前に Microsoft Visual C++ 2017 再頒布可能パッケージのインストールが必要です。

参照

Microsoft Visual C++ 2017 再頒布可能パッケージのインストール方法については、以下を参照してください。

「■ Microsoft Visual C++ 2017 再頒布可能パッケージのインストール」ページ B2-9

■ 手順 2：ルート証明書の適用

Windows Server 2008 R2 に.NET Framework 4.6.2 をインストールする前に、ルート証明書の適用が必要です。

補足

Windows Server 2016、Windows Server 2012 R2 および Windows Server 2008 では、本作業は不要です。

参照

ルート証明書の適用方法については、以下を参照してください。

「■ ルート証明書を適用する」ページ B4-41

■ 手順 3：.NET Framework のインストール

IT セキュリティツールを実行する前に、次の.NET Framework をインストールする必要があります。

- Windows Server 2008 R2 : .NET Framework 4.6.2

- Windows Server 2008 : .NET Framework 4.5.2

補足

Windows Server 2016 と Windows Server 2012 R2 の場合、本作業は不要です。

参照

.NET Framework のインストールのインストール方法については、以下を参照してください。

「■ .NET Framework のインストール」ページ B2-9

■ 手順 4：管理者ユーザを作成する

選択するセキュリティモデルに応じて、管理者ユーザを作成してください。

補足

従来モデルの場合は、すでに作成しているユーザでセットアップが可能なので、本作業は不要です。

● 標準モデルでスタンドアロン管理の場合

- Administrators グループに所属するユーザでログオンしてください。
- CTM_MAINTENANCE グループを作成してください。
- 管理者にしたいユーザを Administrators と CTM_MAINTENANCE グループに所属させてください。

補足

他の製品がコンピュータに共存している場合、その製品の MAINTENANCE グループにも所属している必要があります。たとえば、ProSafe-RS と共存する場合、PSF_MAINTENANCE にも所属させてください。

● 標準モデルでドメイン管理／併用管理の場合

ローカルグループのユーザを管理者とするときは、次の手順に従ってください。

補足

ドメイングループのユーザを管理者ユーザとして使用するときは、すでに作成済みなので本作業は必要ありません。

- Administrators グループに所属するユーザでログオンしてください。
- CTM_MAINTENANCE ローカルグループを作成してください。
- 管理者にしたいドメインユーザまたはローカルユーザを Administrators ローカルグループと CTM_MAINTENANCE ローカルグループに所属させてください。

補足

- 他の製品がコンピュータに共存している場合、その製品の MAINTENANCE グループにも所属している必要があります。たとえば、ProSafe-RS と共存する場合、PSF_MAINTENANCE にも所属させてください。
- IT セキュリティツールの実行後、作成した CTM_MAINTENANCE ローカルグループの名称は、CTM_MAINTENANCE_LCL に変更されます。

■ 手順 5：共有フォルダを作成／設定する

データベースを配置するフォルダのセキュリティを IT セキュリティツールで強化するには、対象フォルダに次の共有名を付ける必要があります。

共有名：CTM_PJTS_DBSF

重要

共有名が上記の名前に一致しない場合、IT セキュリティツールでセキュリティを強化できません。以降の手順に従ってセキュリティの強化を行うために、必ず上記の共有名を設定してください。

● 新規作成の場合

1. 管理者ユーザでログオンしてください。
2. Windows エクスプローラを起動し、プロジェクトフォルダを格納する任意のフォルダを作成してください。
3. 作成したフォルダのプロパティの共有タブで [詳細な共有] をクリックしてください。
4. [このフォルダーを共有する] を選択し、共有名を「CTM_PJTS_DBSF」としてください。
5. [アクセス許可] をクリックして [共有アクセス許可] の [Everyone] にフルコントロールを設定してください。

このアクセス許可設定は、IT セキュリティツール実行時に変更されます。

● すでにファイルサーバに共有フォルダを作成していた場合

IT セキュリティ設定を行う前に、そのフォルダに「CTM_PJTS_DBSF」という共有名を追加してください。IT セキュリティ設定の処理対象になりアクセス権の設定が行われます。従来設定されている共有名を削除する必要はありません。

重要

既存のファイルサーバで、「CTM_PJTS_DBSF」という共有名のフォルダを作成していて、別の目的に使用していた場合には、既存の共有名を別の共有名に変更してください。IT セキュリティ設定は、共有名「CTM_PJTS_DBSF」に対してアクセス権の設定を行うため、「CTM_PJTS_DBSF」が正しいフォルダに設定されていないと意図しない IT セキュリティ設定が行われます。

意図しないフォルダに IT セキュリティ設定が行われた場合、IT セキュリティ設定によって設定されたアクセス権を削除し、たとえば C:\Windows フォルダなどの設定を参考にして元来のアクセス権設定を行ってください。

■ 手順 6：IT セキュリティ設定の初期データを保存する

重要

- ・ IT セキュリティツールを使ってはじめてセキュリティ設定を実施する前に、必ずセキュリティ設定を保存してください。
- ・ ファイルサーバでは、IT セキュリティ設定を変更する際に、あらかじめ保存しておいた初期データを使って、セキュリティ設定を復元してから再適用を行います。そのため、次のような IT セキュリティ設定の保存データが必要になります。
 - ・ 標準モデルでユーザ管理方式がスタンダードアロン管理の場合：
スタンダードアロンの状態で、IT セキュリティ設定の初回適用前に保存したデータ
 - ・ 標準モデルでユーザ管理方式がドメイン管理／併用管理の場合：
ドメインに参加した後で、IT セキュリティ設定を適用する前に保存したデータ
- ・ 2 度目以降のセキュリティ設定では、基本的にセキュリティ設定の保存は不要です。しかし、次の場合はセキュリティ設定の初期データを保存し直してください。
 - ・ R5.01～R6.03 の IT セキュリティツールでセキュリティの設定後、R6.04 以降の IT セキュリティツールで IT セキュリティバージョンを 2.0 に変更する場合
 - ・ R4.03 以前の IT セキュリティツールでセキュリティの設定後、R5.01 以降の IT セキュリティツールで IT セキュリティバージョン、セキュリティモデル、または設定項目の選択状態を変更する場合
- ・ セキュリティ設定の初期データを保存し直す場合は、IT セキュリティツールで以前に保存したセキュリティ設定を復元してください。ドメインに参加したファイルサーバーの場合は、ドメインに参加したままとするかどうかによって、2 つの初期データのどちらで復元するかを決定してください。その後、本手順によりセキュリティ設定を保存してください。以降はセキュリティ設定を初期化するときに、この保存し直したデータを使いますので、大切に保管してください。

セキュリティ設定データを保存するには、次の手順に従ってください。

1. 管理者ユーザでログオンしてください。
2. CENTUM VP のソフトウェアメディアをドライブに挿入してください。
 - ・ 自動再生ダイアログが表示された場合、[Launcher.exe の実行] をクリックしてください。
 - ・ 自動再生ダイアログが表示されない場合、エクスプローラでソフトウェアメディアのトップフォルダにある Launcher.exe をダブルクリックしてください。インストールメニューが表示されます。
3. [IT セキュリティ設定（ファイルサーバ／ドメインコントローラ用）] をクリックしてください。
IT セキュリティツールが起動します。

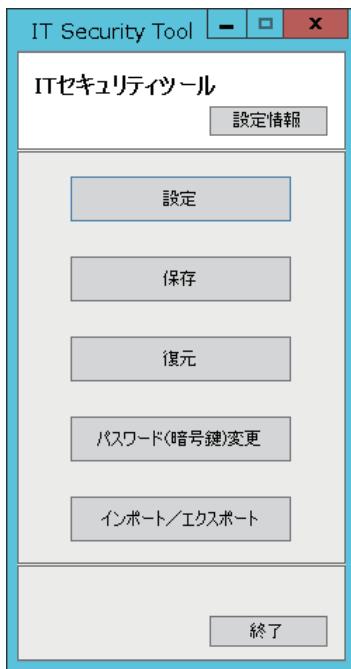


図 B6.1-1 IT セキュリティツールメニュー

補足

ファイルサーバをドメインに参加した状態で使用する場合、セキュリティ設定の初期データは、ドメインに参加した状態と、ドメインから脱退した状態の 2 種類必要です。

ドメインから脱退した初期データがない場合、一時的にドメインから脱退したあとで、セキュリティ設定を保存してください。

4. [保存] をクリックしてください。
保存先の選択ページが表示されます。
5. 保存先を指定し、次の設定項目を入力してください。
 - 識別名
 - 対応製品
 - 対応 OS
 - ファイルバージョン

補足

[識別名] と [ファイルバージョン] は、必要に応じて入力してください。

6. [次へ] をクリックしてください。
アカウント初期パスワードの入力ページが表示されます。
7. 初期パスワードにするパスワードを入力して [次へ] をクリックしてください。
パスワード（暗号鍵）の入力ページが表示されます。

補足

本ツールで保存したアカウントを復元するときにこの初期パスワードが設定されます。保存したアカウントが復元時に存在しない場合は、アカウントを新規作成します。新規作成したアカウントの初期パスワードとして、このパスワードが設定されます。

新規作成されたアカウントが複数ある場合でも、初期パスワードはすべて同じになります。

設定したパスワードが復元する環境のパスワードポリシーを満たさない場合は、アカウント復元時にエラーとなります。

このパスワードはアカウントの初期パスワードとして設定されます。そのため、そのアカウントで初めてログオンするときにパスワード変更が求められます。

8. 保存データを暗号化するためのパスワードを入力して [次へ] をクリックしてください。

セキュリティ設定の保存が開始されます。

重要

- ・ 本パスワード（暗号鍵）を紛失すると、保存したセキュリティ設定が復元できなくなります。パスワード（暗号鍵）の管理は、お客様側で正しく行ってください。
 - ・ パスワード（暗号鍵）は1文字以上です。
 - ・ パスワード（暗号鍵）に使用できる文字は大文字、小文字のアルファベットと数字、記号`~!@#\$%^&*()_+-={}|\\:;'<>>?,.:/です。
全角文字は使用できません。

- 保存が完了したら、[完了] をクリックしてください。
保存に失敗した場合、何に失敗したのかが表示されます。
 - IT セキュリティツールメニューの [終了] をクリックしてください。

補足

保存に失敗した項目が表示された場合、当社窓口に連絡してください。

■ 手順7：ファイルサーバにITセキュリティを設定する

1. ITセキュリティツールメニューから【設定】をクリックしてください。
確認ダイアログが表示されます。
 2. 前述の初期セキュリティ設定データを保存済みの場合は、[OK]をクリックしてください。

補足

保存していない場合は、[キャンセル] をクリックしてメインメニューに戻り、セキュリティ設定を保存してください。

設定モデルの選択ページが表示されます。

図 B6.1-2 設定モデルの選択

3. [ITセキュリティバージョンの選択]でITセキュリティバージョンを選択してください。

4. [設定モデル] ドロップダウンリストから、ファイルサーバ用の設定モデルを選択してください。
次の4つのモデルから選択します。

表 B6.1-2 ファイルサーバ用セキュリティモデル

設定モデル	説明
ファイルサーバ従来モデル (*1)	ユーザ管理方法に関係なく、ファイルサーバを従来モデルに設定するときに選択します。
ファイルサーバ標準モデルスタンダロン管理	ユーザ管理方法がスタンダロン管理でファイルサーバを標準モデルに設定するときに選択します。
ファイルサーバ標準モデルドメイン管理	ユーザ管理方法がドメイン管理でファイルサーバを標準モデルに設定するときに選択します。
ファイルサーバ標準モデル併用管理	ユーザ管理方法が併用管理でファイルサーバを標準モデルに設定するときに選択します。

*1: [IT セキュリティバージョンの選択] で [2.0] を選択した場合は、ファイルサーバ従来モデルは選択できません。

5. [次へ] をクリックしてください。
設定内容の確認ページが表示されます。

補足

ここで [詳細] をクリックした場合、設定項目の選択ページが表示されます。

6. 以降の操作は、CENTUM VP ソフトウェアインストール後の IT セキュリティ設定と同様にしてください。

参照

IT セキュリティ設定をインポートする手順については、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「6.7 IT セキュリティ設定ファイルをインポート／エクスポートする」

CENTUM VP ソフトウェアインストール後の IT セキュリティ設定の操作については、以下を参照してください。

「B4.7 IT セキュリティを設定する」ページ B4-96

■ 手順 8：プロジェクトを参照するユーザをファイルサーバに作成する

セキュリティモデルとユーザ管理方法に応じて、プロジェクトを参照するユーザをファイルサーバに作成します。

● 標準モデルでドメイン管理／併用管理の場合

ドメインコントローラで、プロジェクトを参照するアカウントを追加してください。すでに作成済みの場合、作業は必要ありません。

● 従来モデル、標準モデルスタンダロン管理の場合

ファイルサーバ上で次の作業を行ってください。

1. ユーザアカウントを作成してください。
このときユーザ名とパスワードは、プロジェクトを参照するコンピュータのものと一致させてください。
2. 作成したユーザを、ファイルサーバを参照するコンピュータと同一のユーザグループに登録してください。

補足

標準モデルの場合、次のユーザグループは、手順 7 で実行した IT セキュリティツールにより作成されています。

- CTM_OPERATOR
- CTM_ENGINEER
- CTM_OPC
- CTM_ENGINEER_ADM
- ADS_MANAGER

■ 手順 9：プロジェクトフォルダをファイルサーバに作成する

1. システム生成機能を持ったコンピュータから、手順 5 で作成した共有フォルダ「CTM_PJTS_DBASF」の下に CENTUM プロジェクトを作成してください。
2. ファイルサーバに管理者ユーザでログオンし、1.で作成した CENTUM プロジェクトフォルダを選択してください。
3. フォルダプロパティの共有タブで [詳細な共有] をクリックしてください。
4. [このフォルダーを共有する] のチェックボックスをオンにし、[共有名] ボックスに次の共有名を追加してください。
 - プロジェクトデータベースを共有する場合は、CS1000PJT
 - 処方ビルダのデータベースを共有する場合は、CTMRMNG履歴管理のデータベースの場合は共有名を付ける必要はありません。
5. [アクセス許可] をクリックして、アクセス許可ダイアログを表示してください。
6. [Everyone] にフルコントロールを設定してください。

B6.2 HIS/システム生成機能/AD サーバのみを搭載したコンピュータにファイルサーバ機能を設定する

HIS/システム生成機能/AD サーバのみを搭載したコンピュータとしてセットアップしたコンピュータを、ファイルサーバとして兼用させる場合の設定方法について説明します。

補足

システム生成機能のみを搭載したコンピュータの場合、プロジェクトデータベースはデフォルトでインストールフォルダ以下に置かれますが、これをインストールフォルダとは別の場所に置く場合の手順です。

1. コンピュータを HIS/システム生成機能/AD サーバのみを搭載したコンピュータとしてセットアップしてください。

補足

この時点では、IT セキュリティ設定をする必要はありません。

2. そのコンピュータに対して、共有フォルダの作成／設定をしてください。
3. IT セキュリティツールを起動し、IT セキュリティ設定をしてください。
4. プロジェクトフォルダをそのコンピュータの共有フォルダ以下に作成してください。

重要

ファイルサーバと HIS/システム生成機能/AD サーバのみを搭載したコンピュータを兼用する場合の IT セキュリティ設定では、インストールメニューの [IT セキュリティ設定(ファイルサーバ／ドメインコントローラ用)] を使用しないでください。

参照

HIS/システム生成機能/AD サーバのみを搭載したコンピュータの新規セットアップについては、以下を参照してください。

「B4. 主なステーションやコンピュータのセットアップをする」ページ B4-1

共有フォルダの設定については、以下を参照してください。

「■ 手順 5：共有フォルダを作成／設定する」ページ B6-4

プロジェクトを参照するユーザの作成については、以下を参照してください。

「■ 手順 8：プロジェクトを参照するユーザをファイルサーバに作成する」ページ B6-9

プロジェクトフォルダをファイルサーバに作成する方法については、以下を参照してください。

「■ 手順 9：プロジェクトフォルダをファイルサーバに作成する」ページ B6-10

B6.3 ファイルサーバとライセンス管理ステーションを兼用するコンピュータのセットアップをする

ファイルサーバとライセンス管理ステーションを兼用するコンピュータを、セットアップする設定方法について説明します。

■ 設定手順

1. ライセンス管理ソフトウェアのインストールをしてください。
2. インストール完了時のダイアログで、[いいえ、続けて他製品のインストールを行います] を選択し、[終了] をクリックしてください。
3. ファイルサーバの共有フォルダの設定をしてください。
4. ITセキュリティツールを起動し、ITセキュリティ設定をしてください。

重要

ファイルサーバとライセンス管理ステーションを兼用する場合のITセキュリティ設定では、インストールメニューの [ITセキュリティ設定（ファイルサーバ／ドメインコントローラ用）] を使用しないでください。

参照

ライセンス管理ソフトウェアのみのインストールについては、以下を参照してください。

「B7. ライセンス管理専用のコンピュータのセットアップをする」ページ B7-1

共有フォルダの設定については、以下を参照してください。

「■ 手順5：共有フォルダを作成／設定する」ページ B6-4

B7. ライセンス管理専用のコンピュータのセットアップをする

コンピュータにライセンス管理専用のコンピュータをインストールして、ライセンス管理ステーションとして使用できます。

ここでは、ライセンス管理専用のコンピュータのセットアップ手順について説明します。

■ 用意するもの

ライセンス管理専用のコンピュータをインストールする前に、次のものを手元に用意してください。

- CENTUM VP ソフトウェアメディア

■ インストールをする管理者ユーザ

ライセンス管理専用のコンピュータのインストールは、次の表に示す管理者ユーザで実施してください。

表 B7-1 ライセンス管理専用のコンピュータをインストールする管理者ユーザ

設定しようとするセキュリティモデル／ユーザ管理方法		
従来モデル	標準モデル	
	スタンドアロン管理	ドメイン管理／併用管理
Administrators ローカルグループに所属するローカルユーザ	Administrators ローカルグループに所属するローカルユーザ	<ul style="list-style-type: none"> Domain Admins ドメイングループに所属するドメインユーザ Administrators ローカルグループに所属するドメインユーザ Administrators ローカルグループに所属するローカルユーザ(*1)

*1: インストール中にドメインユーザのユーザ名とパスワードを入力する必要があります。

補足

ユーザ管理方法がドメイン管理／併用管理の場合は、コンピュータがドメインに参加した状態でインストールを実施してください。

■ ライセンス管理ステーションのセットアップ

ライセンス管理ステーションのセットアップ手順を説明します。

● Windows の設定

OS ごとに次の Windows 設定項目を行ってください。

- ファイルシステム： すべて
- 電源管理： すべて
- 高速スタートアップの停止： Windows 10
- Windows Defender： Windows 10、Windows 7
- Windows Update： Windows 10
- ディスクデフラグ： Windows 10、Windows 7
- ルート証明書： Windows 7、Windows Server 2008 R2

参照

Windows 設定項目ごとの設定手順については、以下を参照してください。

「B4.2 Windows の設定をする」ページ B4-7

● ライセンス管理ソフトウェアのインストール

ライセンス管理ソフトウェアをインストールするときは、次の手順に従ってください。

1. 管理者ユーザでログオンしてください。
2. CENTUM VP のソフトウェアメディアをドライブに挿入してください。
 - ・ 自動再生ダイアログが表示された場合、[Launcher.exe の実行] をクリックしてください。
 - ・ 自動再生ダイアログが表示されない場合、エクスプローラで CENTUM VP のソフトウェアメディアのトップフォルダにある Launcher.exe をダブルクリックしてください。
3. インストールメニューが表示されます。
4. [ライセンス管理ソフトウェアの単独インストール] をクリックしてください。
ようこそダイアログが表示されます。

補足

Microsoft .NET Framework などの CENTUM VP に必要な Windows の再頒布モジュールがインストールされていない場合、それらのモジュールのインストールを促すダイアログが表示されます。

それらのモジュールをインストールする場合は、[インストール] をクリックしてください。[キャンセル] をクリックすると、CENTUM VP のインストールが中止されます。

CENTUM VP に必要なモジュールは次のとおりです。

- ・ Microsoft .NET Framework 4.6.2
- ・ MSXML 6.0 SP1
- ・ Microsoft Visual C++ 2017 再頒布可能パッケージ
- ・ OPCCOM ProxyStub

各モジュールのインストールが開始されると、ステータス欄の表示内容が変わります。また、インストール完了後、再起動を要求される場合があります。再起動を要求された場合、再起動後に CENTUM VP のインストールを継続してください。

4. [次へ] をクリックしてください。
ユーザ設定ダイアログが表示されます。
5. ユーザ設定ダイアログで、名前と会社名を入力、インストール先フォルダを選択、インストールする言語を確認し、[次へ] をクリックしてください。
インストール設定の確認ダイアログが表示されます。
6. インストールの設定内容を確認し、[インストール] をクリックしてください。
ライセンス管理ソフトウェアのインストールが完了すると、インストール完了ダイアログが表示されます。
7. [はい、ITセキュリティの設定を行います] を選択し、[終了] をクリックしてください。
続けて IT セキュリティツールが起動されます。
8. IT セキュリティの設定をしてください。

補足

CENTUM VP インストール後に CENTUM VP の機能を削除し、ライセンス管理ソフトウェアのみをインストールする場合は、管理者ユーザでログオンし、CENTUM VP のアンインストールを行ってから、ライセンス管理ソフトウェアをインストールしてください。

重要

ライセンス管理専用のコンピュータで、他の製品のライセンス管理もする場合は、その製品のソフトウェアメディアから、ライセンス管理ソフトウェアのインストールが必要です。

参照

ユーザ設定ダイアログの設定内容については、以下を参照してください。

「B4.6 CENTUM VP ソフトウェアのインストールをする」ページ B4-87

ITセキュリティについては、以下を参照してください。

「B4.7 ITセキュリティを設定する」ページ B4-96

CENTUM VP ソフトウェアをアンインストールする方法については、以下を参照してください。

「C7.1.3 CENTUM VP ソフトウェアをアンインストールする」ページ C7-10

● ユーザアカウントの作成

ライセンスを管理するユーザのアカウントを作成します。

参照

ユーザアカウントの作成方法については、以下を参照してください。

「B4.9 ユーザアカウントを作成する」ページ B4-104

ライセンスを管理するユーザについては、以下を参照してください。

ライセンス管理（IM 33J01C20-01JA）の「1.2.2 ライセンスマネージャのユーザ権限」

● ユーザごとの Windows 動作環境の設定

OSごとに次のWindows設定項目を行ってください。

- ・ Windowsセキュリティセンター／アクションセンターの警告表示： すべて
- ・ スクロール設定： Windows 10
- ・ 仮想デスクトップ： Windows 10

参照

Windows設定項目ごとの設定手順については、以下を参照してください。

「B4.10 ユーザごとの Windows 動作環境の設定をする」ページ B4-109

Blank Page

B8. 仮想化環境のセットアップ^o

ここでは、仮想マシンで CENTUM VP 機能を動作させるために、必要な設定について説明します。

B8.1 SIOS

システムビューの SIOS ステーションプロパティ定義で設定した Ethernet IP アドレスと一致するネットワークカードのメトリック値を、最小値に設定してください。

また、仮想マシンにおけるネットワークのメトリック値を変更するときは、上記ネットワークカードのメトリック値を最小値に設定してください。

プラント情報ネットワークが上記ネットワークカードと別に存在する場合は、プラント情報ネットワークのメトリック値は、上記のネットワークカードの次に小さい値を設定してください。

参照

ネットワークのメトリック値変更については、以下を参照してください。

仮想化プラットフォームセットアップ (IM30A05B20-01JA) の「B1.4 システム製品をインストールしたあとの設定をする」の「■ ネットワークのメトリック値を変更する」

B8.2 HIS

ここでは、次の設定について説明します。

- ・ USB 機器を使用するための設定
- ・ 最大接続数制限の設定
- ・ 1 ユーザあたりのセッション制限の設定
- ・ ピープの有効化の設定
- ・ ブザー設定

B8.2.1 USB 機器を使用するための設定

USB 機器を使用するには、シンクライアント、仮想化ホストコンピュータ、仮想マシン、および仮想マシン上の HIS でそれぞれ設定を行ってください。

■ Windows OS のシンクライアントで設定する

Windows OS のシンクライアントである設定について説明します。

● オペレーションキーボード用 USB ドライバのインストール

USB 接続のオペレーションキーボードを使用する場合、シンクライアントに USB-DVD ドライブを接続し、オペレーションキーボード用 USB ドライバをインストールしてください。

参照

オペレーションキーボード用 USB ドライバのインストールについては、以下を参照してください。

「B4.4 オペレーションキーボード用 USB ドライバのインストールをする」ページ B4-79

オペレーションキーボード用 USB ドライバのアンインストールについては、以下を参照してください。

「■ OPKB 用 USB ドライバのアンインストール」ページ C7-17

● 接続設定ファイルへオペレーションキーボード関連の設定を追加する

仮想マシンへの接続設定ファイルへオペレーションキーボード関連の設定を追加するときは、次の手順に従ってください。

1. シンクライアントに、管理者ユーザでサインインしてください。
2. 仮想マシンへの接続設定を保存したファイルを右クリックして、[編集] を選択してください。
3. [オプションの表示] をクリックしてください。
4. [ローカルリソース] タブをクリックしてください。
5. [ローカルデバイスとリソース] で [詳細] ボタンをクリックしてください。
6. [その他のサポートされている RemoteFX USB デバイス] – [USB AUDIO DAC] チェックボックスを選択してください。
7. [その他のサポートされている RemoteFX USB デバイス] – [Yokogawa OPKB Device] チェックボックスを選択してください。
8. [全般] タブをクリックしてください。
9. [接続設定] で [保存] ボタンをクリックしてください。
10. リモートデスクトップ接続を閉じてください。

参照

仮想マシンへの接続設定ファイルの作成方法については、以下を参照してください。

仮想化プラットフォームセットアップ (IM30A05B20-01JA) の「C1.1.4 接続設定する」

■ 仮想化ホストコンピュータのホスト OS での設定

仮想化ホストコンピュータのホスト OS での設定について、説明します。

● ローカルグループポリシーの変更

ローカルグループポリシーを変更するときは、次の手順に従ってください。

1. 仮想化ホストコンピュータに、管理者ユーザでサインインしてください。

2. コマンドプロンプトを起動し、`gpedit.msc` と入力してください。

ローカルグループポリシーエディターが表示されます。

3. 左ペインで、[コンピュータの構成] – [管理用テンプレート] – [Windows コンポーネント] – [リモートデスクトップサービス] – [リモートデスクトップ接続のクライアント] を選択し、[RemoteFX USB デバイスリダイレクト] をクリックしてください。
4. 右ペインで、[サポートされている他の RemoteFX USB デバイスの、このコンピュータからの RDP リダイレクトを許可する] をダブルクリックしてください。
プロパティダイアログが表示されます。
5. [有効] を選択して、[RemoteFX USB リダイレクトのアクセス権] にて、[管理者とユーザー] を選択してください。
6. [OK] ボタンをクリックしてください。
7. 仮想化ホストコンピュータを再起動してください。

● Hyper-V の設定

Hyper-V 拡張セッションモードを利用するときは、次の手順に従ってください。

1. [スタート] – [サーバーマネージャー] を選択してください。
サーバーマネージャーが起動します。
2. [ツール] – [Hyper-V マネージャー] を選択してください。
Hyper-V マネージャーが起動します。
3. ホストコンピュータ名を右クリックして、[Hyper-V の設定] を選択してください。
4. [拡張セッションモードポリシー] の [拡張セッションモードを許可する] を選択して、[OK] ボタンをクリックしてください。

● オペレーションキーボード用 USB ドライバのインストール

USB 機器がオペレーションキーボード用 USB の場合のみ、この操作を実施してください。オペレーションキーボード用 USB ドライバをインストールするときは、次の手順に従ってください。

1. 仮想化ホストコンピュータに、オペレーションキーボードを接続してください。
2. 仮想化ホストコンピュータに、オペレーションキーボード用 USB ドライバをインストールしてください。

参照

オペレーションキーボード用 USB ドライバのインストールについては、以下を参照してください。

「B4.4 オペレーションキーボード用 USB ドライバのインストールをする」ページ B4-79

オペレーションキーボード用 USB ドライバのアンインストールについては、以下を参照してください。

「■ OPKB 用 USB ドライバのアンインストール」ページ C7-17

■ 仮想マシンのゲスト OS での設定

ここで説明する設定は、仮想化ホストコンピュータのホスト OS での設定後に行ってください。

● リモートデスクトップセッションホスト役割サービスのインストール

リモートデスクトップセッションホスト役割サービスをインストールするときは、次の手順に従ってください。

1. 仮想マシンのゲスト OS に、管理者ユーザでサインインしてください。
2. [スタート] – [サーバーマネージャー] を選択してください。
サーバーマネージャーが起動します。
3. [管理] – [役割と機能の追加] を選択してください。
役割と機能の追加ウィザードが表示されます。

4. 左ペインで [インストールの種類] を選択し、右ペインで [役割ベースまたは機能ベースのインストール] を選択してください。
5. 左ペインで [サーバーの選択] を選択し、右ペインで [サーバープールからサーバーを選択] を選択して、インストールするコンピュータを選択してください。
6. 左ペインで [サーバーの役割] を選択し、右ペインで [リモートデスクトップサービス] チェックボックスを選択してください。
7. 左ペインで [リモートデスクトップサービス] – [役割サービス] を選択し、右ペインで [リモートデスクトップセッションホスト] チェックボックスを選択してください。
ダイアログが表示されます。
8. ダイアログの [管理ツールを含める (存在する場合)] チェックボックスを選択して、[機能の追加] をクリックしてください。
9. 左ペインで [確認] を選択し、右ペインで [インストール] をクリックしてください。サービスのインストールが開始します。
10. インストールが完了したら、[閉じる] をクリックしてください。
11. 仮想マシンを再起動してください。

● リモートデスクトップライセンス役割サービスのインストール

リモートデスクトップライセンス役割サービスをインストールするときは、次の手順に従ってください。

1. 仮想マシンのゲスト OS に、管理者ユーザでサインインしてください。
2. [スタート] – [サーバーマネージャー] を選択してください。
サーバーマネージャーが起動します。
3. [管理] – [役割と機能の追加] をクリックしてください。
役割と機能の追加ウィザードが表示されます。
4. 左ペインで [インストールの種類] を選択し、右ペインで [役割ベースまたは機能ベースのインストール] を選択してください。
5. 左ペインで [サーバーの選択] を選択し、右ペインで [サーバープールからサーバーを選択] を選択して、インストールするコンピュータを選択してください。
6. 左ペインで [サーバーの役割] を選択し、右ペインで [リモートデスクトップサービス] – [リモートデスクトップライセンス] チェックボックスを選択してください。
7. ダイアログが表示された場合は、[管理ツールを含める (存在する場合)] チェックボックスを選択して、[機能の追加] をクリックしてください。
8. 左ペインで [確認] を選択し、右ペインで [インストール] をクリックしてください。サービスのインストールを開始します。
9. インストールが完了したら、[閉じる] をクリックしてください。

● リモートデスクトップライセンスサーバの指定

リモートデスクトップライセンスサーバを指定するときは、次の手順に従ってください。

1. 仮想マシンのゲスト OS に、管理者ユーザでサインインしてください。
2. コマンドプロンプトを起動し、`gpedit.msc` と入力してください。
ローカルグループポリシーエディターが表示されます。
3. 左ペインで、[コンピュータの構成] – [管理用テンプレート] – [Windows コンポーネント] – [リモートデスクトップサービス] – [リモートデスクトップセッションホスト] を選択し、[ライセンス] をダブルクリックしてください。
4. 右ペインで、[指定のリモートデスクトップライセンスサーバーを使用する] をダブルクリックしてください。
プロパティダイアログが表示されます。

5. [有効] を選択し、[使用するライセンスサーバー] にライセンスサーバのコンピュータ名または IP アドレスを入力してください。
6. [OK] ボタンをクリックしてください。
7. 右ペインで、[リモートデスクトップライセンスマードの設定] をダブルクリックしてください。
プロパティダイアログが表示されます。
8. [有効] を選択し、[RD セッションホストサーバーのライセンスマードを指定する] で [接続デバイス数] を選択してください。
9. [OK] ボタンをクリックしてください。

● リモートデスクトップライセンスサーバのアクティブ化

リモートデスクトップライセンスサーバのアクティブ化をするときは、次の手順に従ってください。

1. 仮想マシンのゲスト OS に、管理者ユーザでサインインしてください。
2. [スタート] – [サーバーマネージャー] を選択してください。
サーバーマネージャーが起動します。
3. [ツール] – [RD ライセンスマネージャー] を選択してください。
RD ライセンスマネージャーが起動します。
4. 左ペインでアクティブ化対象のコンピュータを選択し、メニューバーから [操作] – [サーバーのアクティブ化] を選択してください。
サーバーのアクティブ化ウィザードが表示されます。
5. ウィザードの指示に従い、サーバをアクティブ化してください。

● ローカルグループポリシーの変更

ローカルグループポリシーを変更するときは、次の手順に従ってください。

1. 仮想マシンのゲスト OS に、管理者ユーザでサインインしてください。
2. コマンドプロンプトを起動し、`gpedit.msc` と入力してください。
ローカルグループポリシーエディターが表示されます。
3. 左ペインで、[コンピュータの構成] – [管理用テンプレート] – [Windows コンポーネント] – [リモートデスクトップサービス] – [リモートデスクトップセッションホスト] を選択し、[デバイスとリソースのリダイレクト] をクリックしてください。
4. 右ペインで、[サポートされているプラグアンドプレイデバイスのリダイレクトを許可しない] をダブルクリックしてください。
プロパティダイアログが表示されます。
5. [無効] を選択して、[OK] ボタンをクリックしてください。
6. 仮想マシンを再起動してください。

● オペレーションキーボード用 USB ドライバのインストール

USB 機器がオペレーションキーボード用 USB の場合のみ、この操作を実施してください。
仮想マシンにオペレーションキーボード用 USB ドライバをインストールするときは、次の手順に従ってください。

1. 仮想化ホストコンピュータに、オペレーションキーボードを接続してください。
2. [スタート] – [サーバーマネージャー] を選択してください。
サーバーマネージャーが起動します。
3. [ツール] – [Hyper-V マネージャー] を選択してください。
Hyper-V マネージャーが起動します。
4. 右ペインで接続する仮想マシンを選択し、右クリックして [接続] を選択してください。

接続ダイアログが表示されます。

5. [オプションの表示] を選択してください。
6. [ローカルリソース] タブシートを開き、[ローカルデバイスとリソース] の [詳細] ボタンをクリックしてください。
7. [その他のサポートされている RemoteFX USB デバイス] – [Yokogawa OPKB Device] チェックボックスを選択し、[OK] ボタンをクリックしてください。
8. [接続] ボタンをクリックしてください。
9. 仮想マシンのデバイスマネージャを起動し、[ほかのデバイス->不明なデバイス] が表示されていることを確認してください。
10. オペレーションキーボードドライバをインストールしてください。

参照

オペレーションキーボード用 USB ドライバのインストールについては、以下を参照してください。

「B4.4 オペレーションキーボード用 USB ドライバのインストールをする」ページ B4-79

オペレーションキーボード用 USB ドライバのアンインストールについては、以下を参照してください。

「■ OPKB 用 USB ドライバのアンインストール」ページ C7-17

■ 仮想マシン上の HIS での設定

オペレーションキーボードを使用する場合は、仮想マシン上の HIS の HIS ユーティリティで、[操作] タブの [オペレーションキーボードの設定] を [USB] に設定してください。

参照

HIS ユーティリティについては、以下を参照してください。

操作監視リファレンス Vol.1 (IM 33J05A10-01JA) の「1.2 HIS ユーティリティで設定する項目」

B8.2.2 最大接続数制限の設定

仮想マシンのゲスト OS で、同時接続数の制限設定を行ってください。

最大接続数制限を設定するときは、次の手順に従ってください。

1. 仮想マシンのゲスト OS に、管理者ユーザでサインインしてください。
2. コマンドプロンプトを起動し、`gpedit.msc` と入力してください。
ローカルグループポリシーエディターが表示されます。
3. 左ペインで、[コンピュータの構成] – [管理用テンプレート] – [Windows コンポーネント] – [リモートデスクトップサービス] – [リモートデスクトップセッションホスト] – [接続] を選択してください。
4. 右ペインで、[接続数を制限する] をダブルクリックしてください。
プロパティダイアログが表示されます。
5. [有効] を選択して、[最大接続数] に 1 を設定してください。
6. [OK] ボタンをクリックしてください。
7. 仮想マシンを再起動してください。

B8.2.3 1 ユーザあたりのセッション制限の設定

仮想マシンのゲスト OS で、1 ユーザあたりのセッション数の設定を行ってください。

1 ユーザあたりのセッション制限を設定するときは、次の手順に従ってください。

1. 仮想マシンのゲスト OS に、管理者ユーザでサインインしてください。
2. コマンドプロンプトを起動し、`gpedit.msc` と入力してください。
ローカルグループポリシーエディターが表示されます。
3. 左ペインで、[コンピュータの構成] – [管理用テンプレート] – [Windows コンポーネント] – [リモートデスクトップサービス] – [リモートデスクトップセッションホスト] – [接続] を選択してください。
4. 右ペインで、[リモートデスクトップサービス ユーザーに対してリモートデスクトップサービスセッションを 1 つに制限する] をダブルクリックしてください。
プロパティダイアログが表示されます。
5. [無効] を選択し、[OK] ボタンをクリックしてください。
6. 仮想マシンを再起動してください。

B8.2.4 ビープの有効化

仮想マシンのゲスト OS で、ビープの有効化作業を実施してください。

■ オーディオサービスの有効化

参照

オーディオサービスの有効化の手順については、以下を参照してください。

「■ 手順 7：オーディオ使用の設定をする」ページ B5-7

■ システムサウンドサービスの実行

参照

システムサウンドサービスの実行の手順については、以下を参照してください。

「● システムサウンドサービスの実行」ページ B5-9

B8.2.5 ブザー設定

オペレーションキーボードを使用するときは、HIS 設定のブザータブで、[ブザ一切替え] の種別を [オペレーションキーボード] に設定してください。

オペレーションキーボードを使用しないときは、HIS 設定のブザータブで、[ブザ一切替え] の種別を [サウンド拡張] に設定してください。

B8.3 HIS-TSE

ここでは、次の設定について説明します。

- USB 機器を使用するための設定
- 仮想マシンのゲスト OS での設定
- 最大接続数制限の設定
- 1 ユーザあたりのセッション制限の設定
- アプリケーションと作業ディレクトリの設定

また、仮想化環境における HIS-TSE をアンインストールするための手順があります。

B8.3.1 USB 機器を使用するための設定

HIS-TSE で USB 機器を使用するためには、次の設定を実施してください。

- ・ シンクライアントでの設定
- ・ 仮想化ホストコンピュータのホスト OS での設定
- ・ 仮想マシンのゲスト OS での設定

参照

シンクライアントでの設定、および仮想化ホストコンピュータ上のホスト OS での設定の手順については、以下を参照してください。

- ・ 「■ Windows OS のシンクライアントで設定する」ページ B8-4
- ・ 「■ 仮想化ホストコンピュータのホスト OS での設定」ページ B8-4

B8.3.2 仮想マシンのゲスト OS での設定

ここで説明する設定は、仮想化ホストコンピュータのホスト OS での設定後に行ってください。

■ リモートデスクトップセッションホスト役割サービスのインストール

リモートデスクトップセッションホスト役割サービスをインストールするときは、次の手順に従ってください。

1. 仮想化ホストコンピュータのホスト OS に、管理者ユーザでサインインしてください。
2. CENTUM VP ソフトウェアメディアの ISO 形式ファイルを、仮想化ホストコンピュータのホスト OS 内の任意のフォルダにコピーしてください。
3. スタートメニューから、[サーバーマネージャー] を選択してください。
サーバーマネージャーが起動します。
4. サーバーマネージャーのメニューから、[ツール] – [Hyper-V マネージャー] を選択してください。
Hyper-V マネージャーが起動します。
5. Hyper-V マネージャーの左ペインで仮想化ホストコンピュータを選択してください。
中央ペインに選択した仮想化ホストコンピュータ上の仮想マシンが表示されます。
HIS-TSE サーバとなる仮想マシンを選択して、右クリックメニューで [接続] をクリックしてください。
仮想マシン接続ウィンドウが表示されます。

補足

仮想マシン接続ウィンドウが全画面表示される場合があります。全画面表示されたときは、[元に戻す] をクリックして、全画面表示を解除してください。

6. 仮想マシン接続ウィンドウのメニューバーから、[メディア] – [DVD ドライブ] – [ディスクの挿入] を選択してください。
ファイルを開くダイアログが表示されます。
7. コピーした CENTUM VP ソフトウェアメディアの ISO 形式ファイルを指定してください。
選択した ISO 形式ファイルが仮想マシンにマウントされます。
8. エクスプローラで、マウントされた CENTUM VP ソフトウェアメディアの次のフォルダを開いてください。
<マウントされたドライブ>:¥CENTUM¥HIS¥TSE
9. 1-InstallFeature.bat を右クリックして、[管理者として実行] を選択してください。
リモートデスクトップセッションホスト役割サービスがインストールされ、インストールが終了すると仮想マシンが再起動されます。

■ リモートデスクトップライセンス役割サービスのインストール、およびリモートデスクトップライセンスサーバの指定

リモートデスクトップライセンス役割サービスのインストール、およびリモートデスクトップライセンスサーバの指定については、次の手順に従ってください。

1. 仮想化ホストコンピュータのホスト OS に、管理者ユーザでサインインしてください。
2. CENTUM VP ソフトウェアメディアの ISO 形式ファイルを、仮想化ホストコンピュータのホスト OS 内の任意のフォルダにコピーしてください。
3. スタートメニューから、[サーバーマネージャー] を選択してください。
サーバーマネージャーが起動します。

4. サーバーマネージャーのメニューから、[ツール] – [Hyper-V マネージャー] を選択してください。
Hyper-V マネージャーが起動します。
5. Hyper-V マネージャーの左ペインで仮想化ホストコンピュータを選択してください。中央ペインに選択された仮想化ホストコンピュータ上の仮想マシンが表示されます。HIS-TSE サーバとなる仮想マシンを選択して、右クリックメニューで [接続] をクリックしてください。
仮想マシン接続ウィンドウが表示されます。

補足

仮想マシン接続ウィンドウが全画面表示される場合があります。全画面表示されたときは、[元に戻す] をクリックして、全画面表示を解除してください。

6. 仮想マシン接続ウィンドウのメニューから、[メディア] – [DVD ドライブ] – [ディスクの挿入] を選択してください。
ファイルを開くダイアログが表示されます。
7. コピーした CENTUM VP ソフトウェアメディアの ISO 形式ファイルを指定してください。
選択した ISO 形式ファイルが仮想マシンにマウントされます。
8. エクスプローラで、マウントされた CENTUM VP ソフトウェアメディアの次のフォルダを開いてください。
<マウントされたドライブ>:\CENTUM\HIS\TSE
9. 2-InstallLicense.bat を右クリックして、[管理者として実行] を選択してください。
10. [Input for User Authentication:] では、リモートデスクトップセッションホストの認証方法を設定します。「ネットワークレベル認証を必要とする」を設定するために 1 を入力して、[Enter] キーを押してください。
11. [Input for Terminal Service Setting:] では、リモートデスクトップライセンスマードを設定します。次のどちらかの値を入力して、[Enter] キーを押してください。
 - 接続デバイス数を選択する場合 : 2
 - 接続ユーザ数を選択する場合 : 4
12. [Input for Discovery Scope:] では、リモートデスクトップライセンスの検出スコープの構成を設定します。次のどちらかの値を入力して、[Enter] キーを押してください。
 - ワークグループを選択する場合 : 0
 - ドメインを選択する場合 : 1

補足

サーバコンピュータをドメインで運用する場合、ドメインを選択します。

13. [Input for License Servers To Use:] では、使用するライセンスマードを設定します。ライセンスマードのコンピュータ名もしくは IP アドレスを入力して、[Enter] キーを押してください。ライセンスマードがドメイン環境に設置されている場合は、コンピュータ名を「Fully Qualified Domain Name(FQDN)」として、ホスト名およびドメイン名などすべて省略せずに指定してください。

補足

ライセンスマードがリモートデスクトップサーバーと同居しているときは、自 PC のコンピュータ名もしくは自 PC の IP アドレスを指定してください。

14. リモートデスクトップセッションホストの認証方法、リモートデスクトップライセンスマード、リモートデスクトップライセンスの検出スコープの構成、およびライセンスマードの設定内容を確認して、問題がなければ、[To be continued?:] に y を入力して、[Enter] キーを押してください。

設定が完了すると、[続行するには何かキーを押してください...] と表示されます。設定を変更する必要がある場合は、[To be continued?:] に n を入力して、再び、2-InstallLicense.bat を起動して、初めから設定し直してください。

補足

ドメインコントローラのグループポリシーを設定している場合、2-InstallLicense.bat 実行時に使用するライセンスサーバーの設定でエラーとなります。しかし、ドメインコントローラのグループポリシーでライセンスサーバーの設定をしているので、使用上問題ありません。

■ リモートデスクトップライセンスサーバのアクティブ化

リモートデスクトップライセンスサーバをアクティブ化するときは、次の手順に従ってください。

1. HIS-TSE サーバとなる仮想マシンのゲスト OS に、管理者としてサインインしてください。
2. コマンドプロンプトを起動し、licmgr.exe と入力してください。
RD ライセンスマネージャが表示されます。
3. 左ペインで、[すべてのサーバー] を選択してください。
右ペインに、サーバコンピュータが表示されます。
4. 右ペインで、アクティブ化するコンピュータを選択し、メニューバーから [操作] - [サーバーのアクティブ化] を選択してください。
サーバのアクティブ化ウィザードが表示されます。
5. ウィザードの指示に従い、該当サーバコンピュータをアクティブ化してください。

■ ローカルグループポリシーの変更

参照

ローカルグループポリシーの変更については、以下を参照してください。

「● ローカルグループポリシーの変更」ページ B8-4

B8.3.3 最大接続数制限の設定

有効なリモート操作監視サーバ機能パッケージにより、設定値が異なります。

仮想マシンのゲスト OS で、同時接続数の制限設定を行ってください。

最大接続数制限を設定するときは、次の手順に従ってください。

1. 仮想マシンのゲスト OS に、管理者ユーザでサインインしてください。
2. コマンドプロンプトを起動し、`gpedit.msc` と入力してください。
ローカルグループポリシーエディターが表示されます。
3. 左ペインで、[コンピュータの構成] – [管理用テンプレート] – [Windows コンポーネント] – [リモートデスクトップサービス] – [リモートデスクトップセッションホスト] – [接続] を選択してください。
4. 右ペインで、[接続数を制限する] をダブルクリックしてください。
プロパティダイアログが表示されます。
5. [有効] を選択して、リモート操作監視サーバ機能（同時接続クライアント 4 台以下）のパッケージの場合は [最大接続数] に 4 を、リモート操作監視サーバ機能（同時接続クライアント 8 台以下）のパッケージの場合は [最大接続数] に 8 を設定してください。
6. [OK] ボタンをクリックしてください。
7. 仮想マシンを再起動してください。

B8.3.4 1 ユーザあたりのセッション制限の設定

仮想マシンのゲスト OS で、1 ユーザあたりのセッション数の設定を行ってください。

1 ユーザあたりのセッション制限を設定するときは、次の手順に従ってください。

1. 仮想マシンのゲスト OS に、管理者ユーザでサインインしてください。
2. コマンドプロンプトを起動し、`gpedit.msc` と入力してください。
ローカルグループポリシーエディターが表示されます。
3. 左ペインで、[コンピュータの構成] – [管理用テンプレート] – [Windows コンポーネント] – [リモートデスクトップサービス] – [リモートデスクトップセッションホスト] – [接続] を選択してください。
4. 右ペインで、[リモートデスクトップサービス ユーザーに対してリモートデスクトップサービスセッションを 1 つに制限する] をダブルクリックしてください。
プロパティダイアログが表示されます。
5. [未構成] を選択し、[OK] ボタンをクリックしてください。
6. 仮想マシンを再起動してください。

B8.3.5 アプリケーションと作業ディレクトリの設定

シンクライアントがThin OSの場合のみ、作業を実施してください。

アプリケーションと作業ディレクトリを設定するときは、次の手順に従ってください。

1. [接続マネージャ] を起動してください。
接続マネージャウィンドウが表示されます。
2. 接続したい仮想マシンに接続してください。
リモート接続ダイアログが表示されます。
3. ログオンタブの [アプリケーション] に、次の設定を行ってください。
 - デスクトップモードで起動する場合は、<CENTUM VP ソフトウェアをインストールしたフォルダ>:¥CENTUMVP¥Program¥Startdesktop.bat を実行してください。
 - パネルモードで起動する場合は、<CENTUM VP ソフトウェアをインストールしたフォルダ>:¥CENTUMVP¥Program¥BKHBoS.exe を指定し、更に続けて起動引数「-P」、機能文字列、引数を設定してください。
4. ログオンタブの [作業ディレクトリ] には、起動モードによらず、<CENTUM VP ソフトウェアをインストールしたフォルダ>:¥CENTUMVP¥Program を設定してください。
5. [OK] ボタンをクリックしてください。

B8.3.6 HIS-TSE アンインストール

環境設定で、リモートデスクトップ接続時に最初に実行するプログラムを設定したときは、次の手順に従ってください。

1. 仮想マシンのゲスト OS に、管理者ユーザでサインインしてください。
2. コマンドプロンプトを起動し、`gpedit.msc` と入力してください。
ローカルグループポリシーエディターが表示されます。
3. 左ペインで、[コンピュータの構成] – [管理用テンプレート] – [Windows コンポーネント] – [リモートデスクトップサービス] – [リモートデスクトップセッションホスト] – [リモートセッション環境] を選択してください。
4. 右ペインで、[接続時にプログラムを起動する] をダブルクリックしてください。
接続時にプログラムを起動するダイアログが表示されます。
5. [接続時にプログラムを起動する] 項目で [無効] を選択し、[OK] ボタンをクリックしてください。

Blank Page

C. メンテナンス

ここでは、各ステーションの新規セットアップ後、それを運用していく中で必要となる作業について説明します。

Blank Page

C1. ライセンスの追加や割り付けの変更をする

ここでは、新しいソフトウェアパッケージを追加する場合に必要な作業であるライセンスの追加とソフトウェアパッケージを移動するときに必要となるライセンス割り付けの変更について説明します。

C1.1 ライセンスを追加する

追加購入したライセンスをライセンス管理ステーションに読み込む手順は、新規の場合と同様です。

参照

追加購入したライセンスをライセンス管理ステーションに読み込む手順については、以下を参照してください。

ライセンス管理（IM 33J01C20-01JA）の「3.1 ライセンス管理ステーションへの追加ライセンスの読み込み」

C1.2 ライセンスの割り付けを変更する

ライセンス適用ステーションで新たに必要になったソフトウェアパッケージのライセンスは、ライセンス管理ステーションのライセンスマネージャで追加します。

また、ライセンス適用ステーションで不要になったソフトウェアパッケージのライセンスは、ライセンス管理ステーションのライセンスマネージャで削除します。

このような操作を、ライセンス割り付け状態の変更と呼びます。

参照

ライセンス割り付けの変更については、以下を参照してください。

ライセンス管理（IM 33J01C20-01JA）の「3.2 ライセンスの変更」

■ パッケージ無効化の準備

パッケージを有効な状態から無効化したときは、パッケージが有効なときに設定した内容は失われます。再度有効化したときには、必要な設定をもう一度やり直してください。

Blank Page

C2. エンジニアリングデータ参照先を変更する

CENTUM VP ソフトウェアインストール時に設定したエンジニアリングデータの参照先は、必要に応じてあとから変更できます。

■ 変更手順

エンジニアリングデータ参照先の変更は、次の手順に従ってください。

1. HIS の操作監視機能を起動してください。
2. ブラウザバーの名前入力ツールボックスで、[ウィンドウ名入力] ボックスに、「.SH」と入力してください。

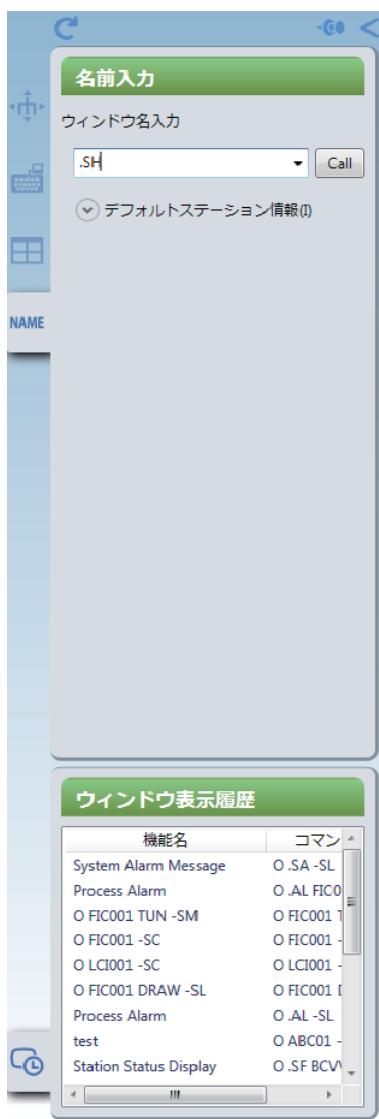


図 C2-1 ブラウザバー

3. [Call] をクリックしてください。
HIS 設定ウィンドウが表示されます。
4. [イコライズ] タブをクリックしてください。
5. [データベースの参照先] で、エンジニアリングデータの参照先を選択してください。

Blank Page

C3. ドメイン環境をあとから構築する

スタンダードアロン管理を主体としたシステムを構築したあと、ドメイン管理のシステムに変更する場合の手順について説明します。

■ 構築の流れ

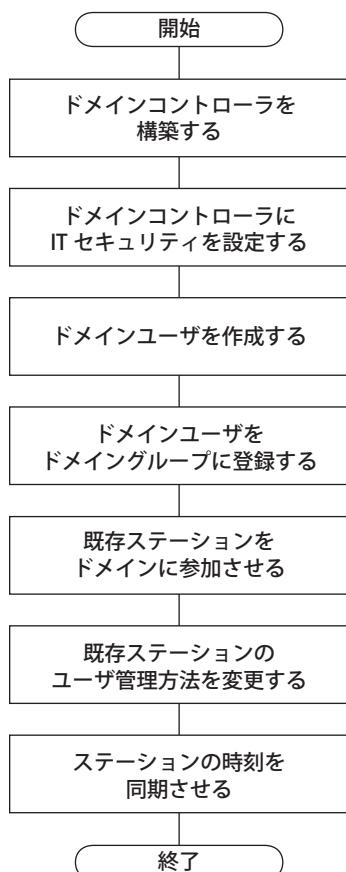


図 C3-1 ドメイン環境をあとから構築する流れ

■ 構築手順

1. ドメインコントローラにするコンピュータを用意し、ドメインコントローラを構築してください。
2. ITセキュリティの設定をしてください。
3. ドメインユーザを作成してください。
4. ドメインユーザをドメイングループに登録してください。
5. クライアントとなるステーションをドメインに参加させてください。
6. 既存ステーションのユーザ管理方法を、ドメイン管理または併用管理に変更してください。
7. ドメイン内のステーションの時刻を同期させてください。

参照

ドメインコントローラの構築については、以下を参照してください。

- ・ 「B2.2 ドメインコントローラを構築する（Windows Server 2016/Windows Server 2012 R2）」ページ B2-5
- ・ 「B2.3 ドメインコントローラを構築する（Windows Server 2008 R2/Windows Server 2008）」ページ B2-7

ドメインコントローラのITセキュリティ設定については、以下を参照してください。

「B2.4 ドメインコントローラのセキュリティを設定する」ページ B2-9

ドメインユーザの作成については、以下を参照してください。

「■ ドメインユーザを作成する」ページ B2-16

ドメインユーザのドメイングループへの登録方法については、以下を参照してください。

「■ ドメインユーザをドメイングループに登録する」ページ B2-17

クライアントコンピュータをドメインに参加させる方法については、以下を参照してください。

「B2.6 クライアントコンピュータをドメインに参加させる」ページ B2-21

ユーザ管理方法の変更については、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「6.3 ITセキュリティ設定を変更する」

ドメイン内のステーションの時刻を同期させる方法については、以下を参照してください。

「B2.8 Windows ドメイン環境での時刻同期を設定する」ページ B2-28

C4. CENTUM 認証モードから Windows 認証モードに変更をする

ここでは、CENTUM 認証モードから Windows 認証モードへ移行する手順について説明します。

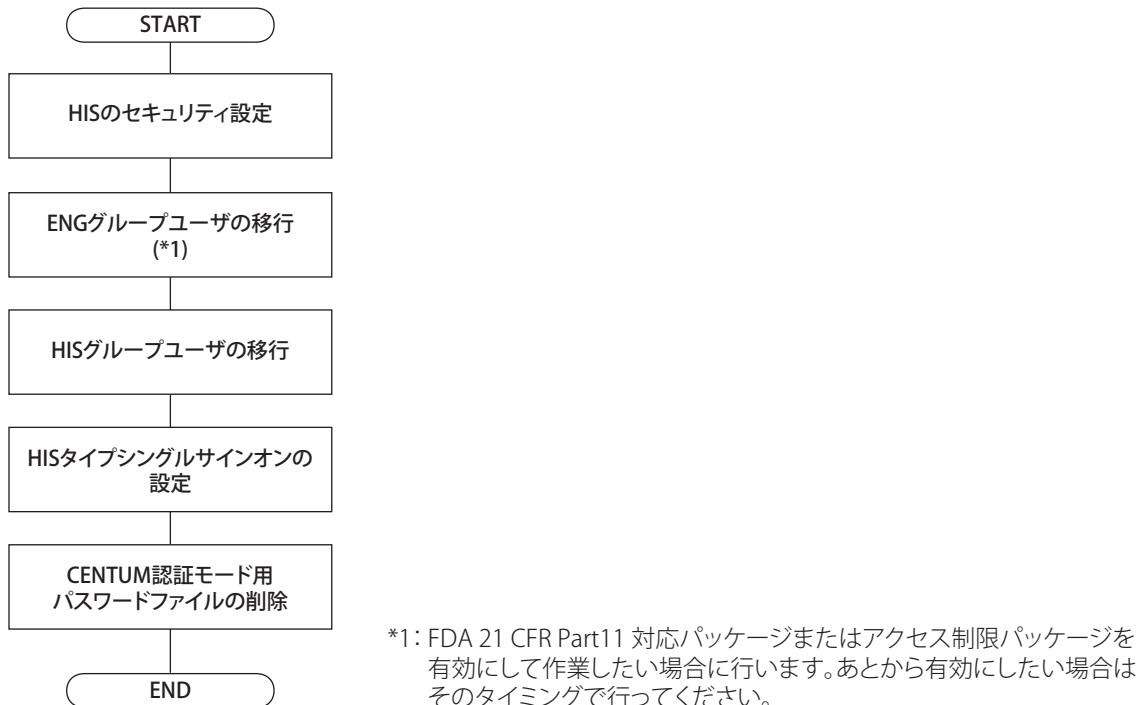


図 C4-1 作業の流れ

■ HIS のセキュリティ設定

操作監視基本機能を有効化している場合に、各コンピュータで実施してください。

参照

HIS のセキュリティ設定については、以下を参照してください。

「■ HIS のセキュリティ設定」ページ B4-140

■ ENG グループユーザの移行

エンジニアリング基本機能、処方管理パッケージ、または帳票パッケージのうちのどれか1つ以上と、FDA:21 CFR Part11 対応パッケージまたはアクセス制限パッケージが有効化されている場合に実施してください。FDA:21 CFR Part11 対応パッケージまたはアクセス制限パッケージの機能をあとで有効にする場合は、それらを有効化したあとに ENG グループユーザの移行を行ってください。

● ユーザ環境設定登録ユーザの削除

エンジニアリング基本機能、処方管理パッケージ、または帳票パッケージのうちのどれか1つ以上と、FDA:21 CFR Part11 対応パッケージまたはアクセス制限パッケージが有効化されている各コンピュータで実施してください。ENG グループユーザの移行前に、アクセス制限ユーティリティのユーザ環境設定に登録してあったユーザをすべて削除します。

重要

作業対象のコンピュータで操作監視基本機能が有効化されている場合、アクセス制限ユーティリティのユーザ環境設定と HIS ユーティリティのユーザ環境設定は同一の内容です。本作業より先に、HIS グループユーザの移行作業を完了している場合、本作業は実施しないでください。

1. CTM_MAINTENANCE または CTM_ENGINEER_ADM グループのユーザでログオンしてください。
2. アクセス制限ユーティリティを起動してください。
3. 全般タブ内の、[設定] をクリックしてください。
ユーザ環境設定ダイアログが表示されます。
4. ユーザを選択して [削除] をクリックしてください。
ユーザの削除ダイアログが表示されます。
5. 選択したユーザのパスワードを入力して、[OK] をクリックしてください。
6. 手順 4~5 を繰り返しすべてのユーザを削除してください。

● Windows ユーザの作成

エンジニア登録ビルダに登録済みのユーザに対応する Windows ユーザを、Windows ドメイン環境の場合はドメインに、スタンドアロン管理の場合は各コンピュータに作成してください。

補足

移行前の Windows アカウントが以下の条件を満たしていれば、そのまま利用可能です。

- ・ 移行前後のユーザ管理（ドメイン・スタンドアロン）が変わっていない。
- ・ IT セキュリティの標準モデルの適切なグループに属している。
- ・ ENG グループユーザとして登録してあるユーザと同じ名称である。

参照

Windows ユーザの作成手順については、以下を参照してください。

「B4.9.1 標準モデル：スタンドアロン管理のセキュリティ設定の場合」ページ B4-105

● ユーザの Windows 動作環境の設定

作成したユーザアカウントを利用してログオンするコンピュータで実施してください。

参照

Windows の動作環境の設定については、以下を参照してください。

「B4.10 ユーザごとの Windows 動作環境の設定をする」ページ B4-109

● ユーザ環境設定

作成したユーザアカウントを利用してログオンするコンピュータで実施してください。

参照

ユーザ環境設定については、以下を参照してください。

「● ユーザ環境設定」ページ B4-141

● ENG グループユーザのユーザ認証モードを Windows 認証モードに設定

ENG グループユーザの管理を行うコンピュータで実施してください。

参照

ENG グループユーザのユーザ認証モードを Windows 認証モードに設定する手順については、以下を参照してください。

「● ENG グループユーザのユーザ認証モードを Windows 認証モードに設定する」ページ B4-143

■ HIS グループユーザの移行

HIS グループユーザの移行をします。

● ユーザ環境設定登録ユーザの削除

操作監視基本機能が有効化されている各コンピュータで実施してください。移行前に、HIS ユーティリティのユーザ環境設定に登録してあったユーザをすべて削除します。

重要

作業対象のコンピュータで FDA:21 CFR Part11 対応パッケージまたはアクセス制限パッケージが有効化されている場合、アクセス制限ユーティリティのユーザ環境設定と HIS ユーティリティのユーザ環境設定は同一の内容です。本節の作業より先に、ENG グループユーザの移行作業を完了している場合、本作業は実施しないでください。

1. CTM_MAINTENANCE または CTM_ENGINEER_ADM グループのユーザでログオンしてください。
2. HIS ユーティリティを起動してください。
3. ユーザタブ内の、[設定] をクリックしてください。
ユーザ環境設定ダイアログが表示されます。
4. ユーザを選択して [削除] をクリックしてください。
ユーザの削除ダイアログが表示されます。
5. 選択したユーザのパスワードを入力して、[OK] をクリックしてください。
6. 手順 4~5 を繰り返してすべてのユーザを削除してください。

● Windows ユーザの作成

セキュリティビルダに登録済みのユーザに対応する Windows ユーザの作成は、Windows ドメイン環境の場合はドメインに、スタンドアロン管理の場合は各コンピュータに作成ください。

補足

移行前の Windows アカウントが以下の条件を満たしていれば、そのまま利用可能です。

- ・ 移行前後のユーザ管理（ドメイン・スタンドアロン）が変わっていない。
- ・ IT セキュリティの標準モデルの適切なグループに属している。
- ・ HIS グループユーザとして登録してあるユーザと同じ名称である。

参照

Windows ユーザの作成については、以下を参照してください。

「B4.9.1 標準モデル：スタンドアロン管理のセキュリティ設定の場合」ページ B4-105

● ユーザの Windows 動作環境の設定

作成したユーザアカウントを利用してログオンするコンピュータで実施してください。

参照

Windows の動作環境の設定については、以下を参照してください。

「B4.10 ユーザごとの Windows 動作環境の設定をする」ページ B4-109

● ユーザ環境設定

操作監視基本機能が有効化されている各コンピュータで実施してください。各 HIS グループユーザに関して設定を行います。

参照

ユーザ環境設定については、以下を参照してください。

「● ユーザ環境設定」ページ B4-141

● HIS グループユーザのユーザ認証モードを Windows 認証モードに設定

プロジェクトを作成・構築するコンピュータで実施してください。

参照

HIS グループユーザのユーザ認証モードを Windows 認証モードに設定する手順については、以下を参照してください。

「● HIS グループユーザのユーザ認証モードを Windows 認証モードに設定」ページ B4-145

● ONUSER、ENGUSER の削除

プロジェクトを作成・構築するコンピュータで実施してください。

重要

- プロジェクトのユーザ認証モードを変更してダウンロードしても、HIS を再起動するまではその HIS のユーザ認証モードは切り替わりませんが、セキュリティビルダ内の定義内容は切り替わります。
- CENTUM 認証モードから Windows 認証モードへ段階的に移行するときなど、一時的に CENTUM 認証モードで動作する HIS 端末を残したい場合、そこで使用するためのユーザはセキュリティビルダ内に残しておく必要があります。すべての HIS を Windows 認証モードに移行する場合に本作業を実施してください。

1. 管理者ユーザでログオンしてください。
2. セキュリティビルダを起動してください。
3. [有効ユーザ] タブを選択してください。
4. ONUSER、ENGUSER を削除してください。
5. システムビューで [プロジェクト共通部ダウンロード] を実施してください。

● HIS の再起動

操作監視基本機能が有効化されている各コンピュータで実施してください。

1. プロジェクトの作成・構築を行うコンピュータでユーザ認証モードを変更したあと、一度も [プロジェクト共通部ダウンロード] を実施していない場合は、[プロジェクト共通部ダウンロード] を実施してください。
2. HIS を再起動してください。

補足

プロジェクトのユーザ認証モードを変更してダウンロードしても、HIS を再起動するまではその HIS のユーザ認証モードは切り替わりません。

CENTUM 認証モードから Windows 認証モードへ段階的に移行するときなど、一時的に CENTUM 認証モードで動作する HIS 端末を残したい場合、その HIS は再起動しないでください。

■ HIS タイプシングルサインオンの設定

操作監視基本機能が有効化されている各コンピュータで HIS タイプシングルサインオンを利用したい場合に設定します。

参照

HIS タイプシングルサインオンの設定については、以下を参照してください。

「■ HIS タイプシングルサインオンの設定」ページ B4-146

■ CENTUM 認証モード用パスワードファイルの削除

HIS のパスワードファイルを共通管理していた場合、パスワードファイルを置いていたコンピュータで実施してください。

1. 共通管理用パスワードファイルを置いていたコンピュータに管理者でログオンします。

対象のコンピュータは、HIS 設定ウィンドウのイコライズタブの [データベースの参照] に設定してあるステーションです。

2. <プロジェクトトップフォルダ>\ETC\Password.odc を削除します。

補足

カレントプロジェクトのフォルダはプロジェクト属性変更ユーティリティで確認できます。

Blank Page

C5. バックアップをとる

予期せぬトラブルに備えて、定期的にシステムのバックアップをとることを推奨します。バックアップ対象フォルダを次の表に示します。

表 C5-1 バックアップ対象フォルダ

内容	フォルダ	バックアップをとるタイミング
Windows 全体	ハードディスク全体	システムを変更したときにバックアップをとってください（プログラムインストール後、セットアップ完了時など）。操作監視機能を含むすべてのアプリケーションを終了したあとに、バックアップ作業を行ってください。
オートメーションデザインマスターデータベース (ADMDB)	—	—
VP プロジェクト	プロジェクトフォルダ	システムビューを終了したあとに、バックアップ作業を行ってください。
カスタムメニュー定義	カスタムメニュー定義ファイルのフォルダ	—
CENTUM VP 操作監視機能用データベース	帳票、PICOT など機能ごとのフォルダ	—
CAMS for HIS コンフィグレータで定義したエンジニアリングデータ	—	—

IT セキュリティ設定の標準モデルを選択した場合は、CENTUM VP 関連フォルダにアクセス可能な権限を持つ管理者ユーザでログオンしてバックアップを実行してください。

参照

ADMDB のバックアップについては、以下を参照してください。

オートメーションデザインシート基本機能 (IM 33J10A10-01JA) の「C1.1.2 ADMDB のバックアップとリストア」

C5.1 Windows 全体のバックアップ^o

Windows 全体のバックアップについて説明します。

■ Windows 全体のバックアップをとる

市販のソフトウェアでバックアップをとり、ディスクの故障に備えてください。

■ Windows 修復ディスクを作成する

さまざまなアプリケーションをインストールすることで、Windows が立ち上がらなくなったりログオンできなくなることがあります。この場合、システム修復ディスクと起動ディスクがあれば、システムの状態をこれらのディスクが作成された時点に回復できます。

プログラムインストール後、ハードウェア変更後など、システムの状態を変更した場合には、システム修復ディスクと起動ディスクを作成するなどの対処をしてください。

参照

ディスク作成手順については、以下を参照してください。

Windows 関連の説明書や、Microsoft のホームページ

C5.2 VP プロジェクトのバックアップをとる

エンジニアリング作業を行ったあとは、必ずエンジニアリングデータのバックアップをとってください。

VP プロジェクトのバックアップ方法には、次の方法があります。

- ・ システムビューからのバックアップ
- ・ メンテナンスメニューからのバックアップ
- ・ AD プロジェクトへのバックアップ

補足

チューニングパラメータについては、あらかじめセーブしておくことを前提とします。

■ システムビューからのバックアップ

システムビューのツールバーから [ツール] – [バックアップ起動] を選択して、プロジェクトのバックアップをしてください。

参照

バックアップの詳細については、以下を参照してください。

エンジニアリングリファレンス Vol.1 (IM 33J10D10-01JA) の「2.6 プロジェクトデータのバックアップ」

■ メンテナンスメニューからのバックアップ

あらかじめ、バッチファイルにバックアップ内容を設定したあと、プロジェクトセーブを起動して、バックアップをしてください。

バックアップ方法の詳細、バックアップされる内容、およびバッチファイルの編集方法については、<CENTUM VP インストールフォルダ>\HIS\Tool にある PDF ファイルを参照してください。

バックアップ開始時にメッセージが outputされる場合、バッチファイルの編集が必要です。出力されたメッセージに従って作業をしてください。

重要

バックアップまたは、リストア作業をする前に、バックアップの場合はバックアップ先、リストアの場合はリストア先の旧フォルダを削除してください。

プロジェクトフォルダ内のファイルを上書きコピーすると、プロジェクトファイル内部の依存関係が壊れ、システムビューでの操作が行えなかったり、予期せぬエラーが発生することがあります。

■ AD プロジェクトへのバックアップ

ADMDB のバックアップ、または AD プロジェクトのエクスポートの前に、VP プロジェクトを AD プロジェクトにバックアップする必要があります。

参照

VP プロジェクトの AD プロジェクトへのバックアップについては、以下を参照してください。

オートメーションデザインシート基本機能 (IM 33J10A10-01JA) の「B1.5.1 VP プロジェクトを管理する」

C5.3 カスタムメニュー定義のバックアップをとる

コンテキストメニューで使用する「カスタムメニュー定義ファイル」を、他の媒体にコピーしてください。

■ カスタムメニュー定義ファイル

<CENTUM VP インストールフォルダ>\HIS\SPCONF\BKHMenuDef.xml
HIS メニューエディタにより編集済みの定義ファイルがここに保存されます。

補足

コンテキストメニューでは、次の定義ファイルを使用します。

- ・デフォルトメニュー定義ファイル
- ・カスタムメニュー定義ファイル

「デフォルトメニュー定義ファイル」は、インストーラでインストールされます。リビジョンアップの際には、無条件にインストーラにより上書きされます。

C5.4 CENTUM VP 操作監視機能用データベースの バックアップをとる

帳票や PICOT の機能ごとに、バックアップをとってください。

C5.4.1 帳票のバックアップをとる

帳票パッケージのコピーツールを使用して、帳票定義ファイルをリムーバブルメディアにコピーしてください。

C5.4.2 PICOT のバックアップをとる

Windows エクスプローラなどで、次のディレクトリ以下の内容を他の媒体にコピーしてください。

<CENTUM VP インストールフォルダ>\his\users\save\BKUPICOT

C5.5 CAMS for HIS コンフィグレータで定義したエンジニアリングデータのバックアップをとる

CAMS for HIS コンフィグレータのメニューバーから、バックアップツールを選択してください。

C6. バージョンアップ／レビジョンアップやアップグレードをする

ここでは、次の種類のバージョンアップやアップグレードの説明をします。

- CENTUM CS 3000 から CENTUM VP R6 へのバージョンアップ
- CENTUM CS 1000 から CENTUM VP R6 へのアップグレード
- CENTUM VP R4 または R5 から R6 へのバージョンアップ
- CENTUM VP R6 のレビジョンアップ

参照

バージョンアップ／レビジョンアップの際の注意事項については、以下を参照してください。

「C11. バージョンアップ／レビジョンアップ時の注意事項」ページ C11-1

■ バージョンアップ／レビジョンアップを実施する管理者ユーザ

同一コンピュータ上でのCENTUM VP ソフトウェアのバージョンアップやレビジョンアップは、次の表に示す管理者ユーザで実施してください。

表 C6-1 バージョンアップやレビジョンアップを実施する管理者ユーザ

設定しようとするセキュリティモデル／ユーザ管理方法		
従来モデル	標準モデル	
	スタンドアロン管理	ドメイン管理／併用管理
Administrators ローカルグループと CTM_MAINTENANCE ローカルグループに所属するローカルユーザ	Administrators ローカルグループと CTM_MAINTENANCE ローカルグループに所属するローカルユーザ	<ul style="list-style-type: none"> • Domain Admins ドメイングループと CTM_MAINTENANCE ドメイングループに所属するドメインユーザ • Administrators ローカルグループと CTM_MAINTENANCE_LCL ローカルグループに所属するドメインユーザ • Administrators ローカルグループと CTM_MAINTENANCE_LCL ローカルグループに所属するローカルユーザ (*1)

*1: インストール中にドメインユーザのユーザ名とパスワードを入力する必要があります。

補足

ユーザ管理方法がドメイン管理／併用管理の場合は、コンピュータがドメインに参加した状態でインストールを実施してください。

■ バージョンアップ／レビジョンアップやアップグレード後の作業

エンジニアリング開始前の準備として、次の作業が必要です。

- オートメーションデザインプロジェクト（AD プロジェクト）の作成
- 既存の VP プロジェクトの AD プロジェクトへの登録

参照

エンジニアリング開始前の準備については、以下を参照してください。

オートメーションデザインサイト基本機能 (IM 33J10A10-01JA) の「B. エンジニアリングを開始する」

C6.1 CENTUM CS 3000 から CENTUM VP R6 にバージョンアップする

CS 3000 と CENTUM VP の R6 では、動作保証している OS が違うため、動作保証している OS を搭載したコンピュータにソフトウェアを新規インストールして、その後、プロジェクトのデータベースを移行することが必要です。

C6.1.1 バージョンアップをする

■ バージョンアップの流れ

バージョンアップは次のような流れとなります。これに沿って、作業を行ってください。

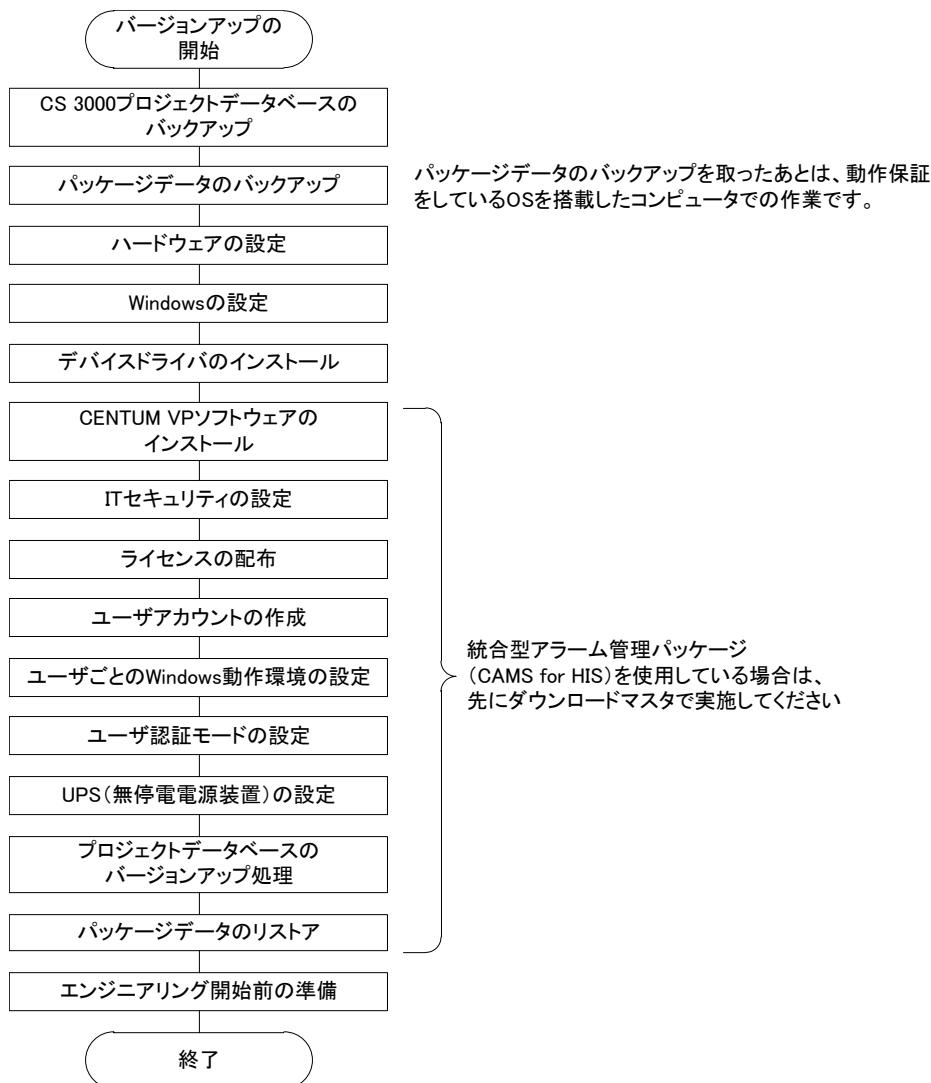


図 C6.1.1-1 バージョンアップインストールの手順

重要

CS 3000 プロジェクトレビューションアップ用プログラムのインストールおよび CENTUM VP ソフトウェアのインストールは、R6 での動作が保証されている OS で行ってください。その際は、先に Windows の設定を行ってください。

■ CS 3000 プロジェクトデータベースのバックアップ

既存の CS 3000 で、必要なプロジェクトデータベースをバックアップしてください。

参照

プロジェクトデータベースのバックアップについては、以下を参照してください。

「C5.2 VP プロジェクトのバックアップをとる」ページ C5-3

■ パッケージデータのバックアップ

既存の CS 3000 で使用しているパッケージで、保存が必要なデータをパッケージごとにバックアップしてください。

参照

パッケージデータのバックアップの詳細については、以下を参照してください。

「C6.1.2 CS 3000 パッケージデータのバックアップとリストアをする」ページ C6-8

■ ハードウェアの設定

ハードウェアの設定をしてください。

参照

ハードウェアの設定については、以下を参照してください。

「B4.1 ハードウェアの設定をする」ページ B4-2

■ Windows の設定

Windows の設定をしてください。

参照

Windows の設定については、以下を参照してください。

「B4.2 Windows の設定をする」ページ B4-7

■ デバイスドライバのインストール

制御バスドライバなどの通信用ドライバ、OPKB 用 USB ドライバなどのデバイスドライバをインストールしてください。

参照

デバイスドライバのインストール手順については、以下を参照してください。

- ・「B4.3 ネットワークの設定をする」ページ B4-43
- ・「B4.4 オペレーションキーボード用 USB ドライバのインストールをする」ページ B4-79
- ・「B4.5 コンソール形 HIS の場合に必要な設定をする」ページ B4-81

■ CENTUM VP ソフトウェアのインストール

CENTUM VP ソフトウェアをインストールしてください。

参照

CENTUM VP ソフトウェアのインストール手順については、以下を参照してください。

「B4.6 CENTUM VP ソフトウェアのインストールをする」ページ B4-87

■ IT セキュリティの設定

IT セキュリティの設定をしてください。

参照

IT セキュリティについては、以下を参照してください。

「B4.7 IT セキュリティを設定する」ページ B4-96

■ ライセンスの配布

ライセンスの配布をしてください。

バージョンアップの場合は、ライセンスメディアにパッケージリストが添付されます。このパッケージリストをライセンスマネージャにインポートすることで、ライセンス配布に必要なステーション構成定義と各ステーションへのパッケージ割り付け定義が生成できます。

参照

ライセンス配布については、以下を参照してください。

「B4.8 ライセンスの配布と反映をする」ページ B4-103

■ ユーザアカウントの作成

ユーザアカウントの作成をしてください。

参照

ユーザアカウントの作成については、以下を参照してください。

「B4.9 ユーザアカウントを作成する」ページ B4-104

■ ユーザごとの Windows 動作環境の設定

ユーザごとの Windows 動作環境の設定をしてください。

参照

ユーザごとの Windows 動作環境の設定については、以下を参照してください。

「B4.10 ユーザごとの Windows 動作環境の設定をする」ページ B4-109

■ ユーザ認証モードの設定

ユーザ認証モードの設定をしてください。

参照

ユーザ認証モードの設定については、以下を参照してください。

「B4.11 ユーザ認証モードの設定をする」ページ B4-136

■ UPS(無停電電源装置) の設定

UPS(無停電電源装置) の設定をしてください。

参照

UPS(無停電電源装置) の設定については、以下を参照してください。

「B4.12 UPS (無停電電源装置) の設定をする」ページ B4-149

■ プロジェクトデータベースのバージョンアップ

1. バージョンアップ前の CS 3000 プロジェクトデータベースを適切な場所にリストアしてください。
 2. プロジェクト属性変更ユーティリティを起動してください。
 3. プロジェクトデータベースをシステムビューに登録してください。
 4. システムビューを起動してください。
- プロジェクトデータベースのバージョンアップ処理が自動的に行われます。

重要

CS 3000 と CENTUM VP では、グラフィックの仕様が異なります。

CS 3000 のグラフィックファイルを、表示と動作の互換性を考慮して CENTUM VP R6 のグラフィックファイルに変換する場合は、そのための作業が必要です。

参照

プロジェクト属性変更ユーティリティについては、以下を参照してください。

エンジニアリングリファレンス Vol.1 (IM 33J10D10-01JA) の「2.3 プロジェクト属性変更ユーティリティ」

● HIS 変換ツール

プロジェクトに CS 3000 の HIS が含まれていると、CENTUM VP の HIS へのバージョンアップ処理が行われます。「HIS 変換ツール」が表示されますので、CENTUM VP の HIS に変換するステーションのチェックボックスをオンにし、CS 3000 の HIS のまま変換をしないステーションのチェックボックスはオフにしてください。

- CENTUM VP の HIS への変換時に、CS 3000 のグラフィックファイルは、ステーション単位で一括して CENTUM VP の最新のグラフィック形式に自動変換されます。
- HIS 変換ツールは、システムビューのツールメニューから [HIS 変換ツール] を選択することでも起動できます。

補足

HIS 変換ツールで VP HIS のステーションタイプにバージョンアップ後は、システムビューの HIS プロパティからステーションタイプの変更ができます。

参照

CS 3000 のグラフィックファイルを、表示と動作の互換性を考慮して CENTUM VP R6 のグラフィックファイルに変換する方法については、以下を参照してください。

グラフィック変換手順 (IM 33J01C40-01JA)

● グラフィックファイル変換ツール

CS 3000 グラフィックファイル単位で CENTUM VP グラフィックファイルに変換する場合に使用します。CENTUM VP のグラフィック形式に変換されたファイルは、CENTUM VP のグラフィックビルダでインポートして編集することができます。

グラフィックファイルの変換は、次の手順に従ってください。

1. グラフィックファイル変換ツールを起動してください。
2. 変換する CS 3000 グラフィックファイルまたはフォルダを追加してください。
3. 出力先フォルダを指定し、[変換] をクリックしてください。

変換状況を示すダイアログが表示されます。

補足

ファイル変換が終了すると、[ステータス] に正常に変換された場合は [成功] が表示され、エラーの場合は [失敗] が表示されます。

4. [閉じる] をクリックし、グラフィックファイル変換ツールを終了してください。

参照

CS 3000 のグラフィックファイルを、表示と動作の互換性を考慮して CENTUM VP R6 のグラフィックファイルに変換する方法については、以下を参照してください。

グラフィック変換手順 (IM 33J01C40-01JA)

■ バックアップしたパッケージデータのリストア

バックアップした、パッケージごとのデータをリストアしてください。

参照

パッケージごとのデータのリストアの手順については、以下を参照してください。

「C6.1.2 CS 3000 パッケージデータのバックアップとリストアをする」ページ C6-8

■ 計器図ハイライト機能に関する注意事項

CENTUM VP R5.03.00 から、計器図ハイライト機能が追加されています。この機能はオフにすることもできます。

参照

計器図ハイライト機能については、以下を参照してください。

操作監視リファレンス Vol.2 (IM 33J05A11-01JA) の「2.7 計器図ハイライト機能」

計器図ハイライト機能のオンオフについては、以下を参照してください。

操作監視リファレンス Vol.1 (IM 33J05A10-01JA) の「1.2 HIS ユーティリティで設定する項目」の「■ 操作タブシートでの設定項目」の「● 計器図ハイライト機能」

C6.1.2 CS 3000 パッケージデータのバックアップとリストアをする

ここでは、バックアップする必要があるデータとそのバックアップ方法、リストア方法について説明します。

■ バックアップとリストアが必要なデータ

パッケージごとにバックアップとリストアが必要なデータを、次に示します。
 バックアップとリストアが必要なデータには、CS 3000 稼動中にバックアップする必要があるものと、オフライン状態でバックアップするものがあります。
 バックアップはCS 3000 で行い、リストアはCENTUM VP に対して行います。

表 C6.1.2-1 CS 3000 稼動中にバックアップをとるデータ

パッケージ	名称	CENTUM VP R6 で該当するパッ ケージ	バックアップ／リストアするデータ
LHS1100 LHM1101	操作監視基本機能	VP6H1100	HIS 設定情報
LHS1150	リモート操作監視サーバ機能	VP6H1150	LHS1100 と同様です。
LHS4200	ヒストリカルメッセージ統合 パッケージ (FDA 対応)	VP6H4200	ヒストリカル統合サーバに格納されたデータ
LHS4700	拡張アラームフィルタパッケージ	VP6H4700	拡張アラームフィルタ定義データ
LHS6510	長期データ保管パッケージ	VP6H6510	長期データ
LHS6530	帳票パッケージ	VP6H6530	帳票定義データ
LHS5100 LHM5100	ビルダ基本機能 (*1)	VP6E5100	プロジェクトデータベース
LHS5150	グラフィック作成パッケージ	VP6E5150	プロジェクトデータベース
LHS5160	CS Batch 3000 ビルダ (*2)	VP6E5165	プロジェクトデータベース
LHS5161	CS Batch 3000 処方管理/パッケージ (*3)	VP6E5166	処方のデータベース
LFS1250	GSGW 汎用サブシステムゲート ウェイパッケージ	VP6F1250	OPC サーバ定義情報ファイルとアイテム定義情報ファイル

*1: CENTUM VP R6 では、エンジニアリング基本機能です。

*2: CENTUM VP R6 では、バッチビルダです。

*3: CENTUM VP R6 では、処方管理パッケージです。

表 C6.1.2-2 オフラインでバックアップをとるデータ

パッケージ	名称	CENTUM VP R6 で該当するパッ ケージ	バックアップ／リストアするデータ
LHS1100 LHM1101	操作監視基本機能	VP6H1100	HIS 関連データベース
LHS1150	リモート操作監視サーバ機能	VP6H1150	LHS1100 と同様です。

次に続く

表 C6.1.2-2 オフラインでバックアップをとるデータ（前から続く）

パッケージ	名称	CENTUM VP R6 で該当するパッ ケージ	バックアップ／リストアするデータ
LHS4800	統合型アラーム管理パッケージ (CAMS for HIS)	VP6H1100 (操作 監視基本機能) に含まれます。	<ul style="list-style-type: none"> ・メッセージモニタのデータ ・コンフィグレータのデータ ・稼動時データベース ・稼動時データベースのバックアップ ・ヒストリカルデータ ・疑似アラーム発生ツールのシナリオ ファイル ・ヒストリカルビューアのデータ ・OPC A&E サーバ接続設定 ・CAMS for HIS サーバ設定 ・等値化対象範囲設定
LHS6710 LHM6710	FCS データ設定／収集パッケージ (PICOT)	VP6H6710	定義データ
LHS5110	アクセス制限パッケージ	VP6E5110	定義データ
LHS5170	FDA:21 CFR Part 11 対応パッケージ	VP6E5170	履歴管理データベース

■ CS 3000 稼動中にバックアップするデータのバックアップとリストア

次のデータは、CS 3000 が稼動している状態でバックアップしてください。

バックアップするデータのコピーを作成しておき、各パッケージのインポート機能などを
を利用してリストアしてください。

重要

ビルダ基本機能、グラフィック作成パッケージ、CS Batch 3000 ビルダ、CS Batch 3000 処
方管理パッケージのデータは、プロジェクトデータベースのバックアップとリストアに含
められます。

● 操作監視基本機能－HIS 設定情報

- ・ バックアップ
HIS 設定ウィンドウのエクスポート機能で、HIS レジストリ情報をバックアップしてく
ださい。
- ・ リストア
HIS 設定ウィンドウのインポート機能で、バックアップしたファイルをインポートし
てください。

参照

HIS 設定ウィンドウのエクスポート、インポート機能については、以下を参照してください。

操作監視リファレンス Vol.1 (IM 33J05A10-01JA) の「4.3 HIS 設定ウィンドウ」の「■ HIS 設定ウィンド
ウの [インポート] と [エクスポート]」

● ヒストリカルメッセージ統合パッケージ

ヒストリカルメッセージ統合サーバに格納されたデータは、継承させることができます。
継承させるためには、各 HIS で、ヒストリカルメッセージ統合サーバに保管されたヒスト
リカルファイルのシーケンス番号を継続させるための作業をすること、ヒストリカルメ
ッセージの保管先を再設定することが必要です。

- ・ 各 HIS でのシーケンス番号のバックアップ
管理者ユーザでログオンし、次のコマンドを実行して操作監視機能を停止してく
ださい。

<CS 3000 インストールフォルダ>\his\tool\BKHHisStop.exe

エクスプローラで、次のファイルから最新のシーケンス番号のファイルをリムーバブルメディアに保存してください。

<CS 3000 インストールフォルダ>\Log\HISHIST\HISHISTnnnn-YYYYMMDD.log (nnnn : シーケンス番号)

- ヒストリカルメッセージ統合サーバでの作業

管理者ユーザでログオンし、保管した最新のシーケンス番号のファイルを、ヒストリカルメッセージ統合サーバの各 HIS に対応したフォルダにコピーしてください。

サーバ上のフォルダ : <共有名>\HisHist\HISddss (dd : ドメイン番号、 ss : ステーション番号)

補足

上記のサーバ保管先に HIS 名のフォルダが存在する HIS が、ヒストリカルメッセージ統合管理の対象です。交換前の HIS が故障などで最新ヒストリカルファイルの取得ができないときには、上記のサーバ保管先の該当 HIS フォルダを参照して、最新（最大）のシーケンス番号をメモしてください。このときには、最新ヒストリカルファイルのサーバ側への反映はできません。

- シーケンス番号のリストア

バージョンアップした HIS に管理者ユーザでログオンし、次のコマンドを実行して操作監視機能を停止してください。

<VP インストールフォルダ>\his\tool\BKHHisStop.exe

次の HISHIST 保存フォルダ内を空にしてください。

保存フォルダ : <VP インストールフォルダ>\Log\HISHIST

次のコマンドをコマンドプロンプトで実行してください。

<VP インストールフォルダ>\his\tool\SetSeqNo.bat<手順 2 でメモした最新シーケンス番号> (Δ : スペース)

HIS を再起動し、起動後に HISHIST フォルダ内にバックアップしたシーケンス番号+1 のヒストリカルファイルが 1 つ作成されていることを確認してください。

サーバ保管定義ファイル設定を実施し、ヒストリカルメッセージ統合サーバへ接続して、保管を開始してください。

参照

保管先の再設定については、以下を参照してください。

操作監視リファレンス Vol.2 (IM 33J05A11-01JA) の「8.1.1 ヒストリカルメッセージ保存ファイル保管先フォルダの設定」

● 拡張アラームフィルタパッケージ

- バックアップ

拡張アラームフィルタパッケージのアラームフィルタ 定義のエクスポート機能を使用して、フィルタ定義をバックアップしてください。

- リストア

拡張アラームフィルタパッケージのアラームフィルタ 定義のインポート機能を使用して、フィルタ定義をリストアしてください。

参照

アラームフィルタ定義のエクスポート、インポート機能の詳細については、以下を参照してください。

操作監視リファレンス Vol.2 (IM 33J05A11-01JA) の「7.5.3 拡張アラームフィルタウィンドウ」

● 長期データ保管パッケージ

- バックアップ

長期データ保管パッケージのアーカイブ操作で、保管データを外部記憶媒体にバックアップしてください。

また、次の BKHLogFile.txt ファイルもバックアップしてください。

¥¥<HIS名>¥LTDATA¥LOG¥BKHLogFile.txt

- リストア

バックアップした保管データは、長期データ保管パッケージのリトリーブ操作で、外部記憶媒体から HIS のハードディスクにリストアしてください。

また、BKHLogFile.txt ファイルもバックアップのときと同じ場所にリストアしてください。

参照

アーカイブ操作とリトリーブ操作の詳細については、以下を参照してください。

CENTUM VP オプション機能リファレンス (IM 33J05H10-01JA) の「4.2.4 アーカイブ操作とリトリーブ操作」

● 帳票パッケージ

- バックアップ

帳票パッケージのコピーツールを使用して、帳票定義ファイルをリムーバブルメディアにコピーしてください。

- リストア

帳票パッケージのコピーツールを使用して、リムーバブルメディアの帳票定義ファイルをリストア対象のコンピュータにコピーしてください。

参照

帳票定義データのコピーについては、以下を参照してください。

- CENTUM VP オプション機能リファレンス (IM 33J05H10-01JA) の「2.5.3 他コンピュータでの帳票印字」の「■ 他コンピュータへの帳票のコピー」
- CENTUM VP オプション機能リファレンス (IM 33J05H10-01JA) の「2.1 帳票パッケージを使用するための設定を行う」

● 汎用サブシステムゲートウェイパッケージのデータ

GSGW の次のフォルダにある定義ファイルをバックアップして、バージョンアップ後にリストアしてください。

- OPC サーバ定義情報ファイル：

<CS 3000 インストールフォルダ>¥apcs¥GPLSYBKEOPCSVDef.csv

- アイテム 定義情報ファイル：

<CS 3000 インストールフォルダ>¥apcs¥GPLSYBKEOPCITEMDef.csv

■ オフライン状態でバックアップするデータのバックアップとリストア

次のデータは、オフライン状態でバックアップしてください。

これらのデータを CS 3000 側でバックアップするとき、CS 3000 機能は完全に停止している必要があります。また、CENTUM VP 側でリストアするとき、CENTUM VP 機能が完全に停止している必要があります。

CENTUM VP のインストール後に、これらのデータを<CENTUM VP インストールフォルダ>以下の相対的に同じ場所にコピーしてください。コピー先フォルダに同名のファイルが存在する場合は、上書きしてください。

● 操作監視基本機能-HIS 関連データベース

1. コマンドプロンプトで次のコマンドを実行し、操作監視機能を停止してください。

<CS 3000 インストールフォルダ>¥his¥tool¥BKHHisstop.exe

2. 次の HIS 関連のファイルをバックアップ・リストアしてください。リストアの場合は、フォルダ名は<CENTUM VP インストールフォルダ>となります。

<CS 3000 インストールフォルダ>\his\database	: 音声メッセージなど
<CS 3000 インストールフォルダ>\his\recipe	: 処方・実行処方
<CS 3000 インストールフォルダ>\his\save	: 締切、スケジューラなど
<CS 3000 インストールフォルダ>\his\Trend	: トレンド
<CS 3000 インストールフォルダ>\his\spconf	: コンテキストメニューなど
<CS 3000 インストールフォルダ>\his\Media\User	: メディアデータ

補足

特注ソフトウェア関連のファイルは次のフォルダにあります。これらのファイルをバージョンアップ後にリストアして使用できるかどうかは、当社担当部署にご確認ください。

<CS 3000 インストールフォルダ>\his\spconf
<CS 3000 インストールフォルダ>\his\user

● 統合型アラーム管理パッケージ (CAMS for HIS)

CAMS for HIS データのバックアップは、CAMS for HIS 以外のパッケージデータのバックアップ作業が完了した後、CAMS for HIS を無効にした状態で行ってください。

CAMS for HIS データのリストアは、HIS 関連データベースのリストア作業が完了した後、CAMS for HIS を無効にした状態で行ってください。

参照

CAMS for HIS データのバックアップとリストアについては、以下を参照してください。

「C6.1.3 CAMS for HIS データのバックアップとリストアをする」ページ C6-13

● FCS データ設定／収集パッケージ (PICOT)

1. PICOT の停止

Windows タスクバーにある PICOT を開き、File メニューから [Exit] を選択してください。PICOT が停止されます。

2. 定義ファイルのバックアップとリストア

- バックアップ

本パッケージの次のフォルダにある定義ファイルをバックアップしてください。

<CS 3000 インストールフォルダ>\his\users\save\BKUPICOT

- リストア

バックアップしたファイルを次のフォルダにリストアしてください。

<CENTUM VP インストールフォルダ>\his\users\save\BKUPICOT

参照

定義ファイルの詳細については、以下を参照してください。

CENTUM VP オプション機能リファレンス (IM 33J05H10-01JA) の「3.2 PICOT の構成ファイルと処理の流れ」

● アクセス制限パッケージ、FDA:21 CFR Part 11 対応パッケージ

- バックアップ

アクセス制限ユーティリティで指定した「エンジニア登録ファイルの参照先」が CS 3000 インストールフォルダの下にある場合、そのフォルダ以下のファイルをバックアップしてください。その際、EngPassword2.odc というファイルのアクセス権に everyone の FULL コントロールを追加してください。

- リストア

ファイルを復元し、アクセス制限ユーティリティで再設定してください。

C6.1.3 CAMS for HIS データのバックアップとリストアをする

CAMS for HIS では等値化対象範囲内に、ダウンロードマスタとなる HIS と、それ以外の HIS が存在します。

どちらもデータ移行作業の手順は同じですが、データのリストアについては、先に CAMS for HIS ダウンロードマスタでの作業を完了させてください。その後で、CAMS for HIS ダウンロードマスタ以外の HIS に対して、同様の作業を実施してください。

ここでは、CAMS for HIS データのバックアップ方法、リストア方法について説明します。

参照

CAMS for HIS ダウンロードマスタについては、以下を参照してください。

統合型アラーム管理リファレンス (IM 33J05A21-01JA) の「A1. CAMS for HIS の概要」の「■ CAMS for HIS を使用したときのシステム構成」

■ CAMS for HIS データのバックアップ

CAMS for HIS データのバックアップ手順を、次に示します。

1. 等値化対象範囲内の、既存の CS 3000 の各 HIS に、管理者ユーザでログオンしてください。
2. HIS ユーティリティの CAMS for HIS タブシートで CAMS for HIS を無効にしてから、HIS を再起動してください。
3. 各 HIS で、次の CAMS フォルダにあるすべてのファイルをバックアップしてください。

<CS 3000 インストールフォルダ>\CAMS

補足

CAMS for HIS ヒストリカルデータが不要であれば、次のフォルダのファイルはバックアップ不要です。

<CS 3000 インストールフォルダ>\CAMS\hist

以上で、CAMS for HIS データのバックアップは終了です。

■ CAMS for HIS データのリストア前の作業

CAMS for HIS データのリストア作業を始める前に完了させておくべき作業について、手順を次に示します。

1. ダウンロードマスタとなる HIS に、CENTUM VP ソフトウェアをインストールしてください。
その後、IT セキュリティの設定、ライセンスの配布、ユーザーアカウントの作成、ユーザごとの Windows 動作環境の設定、ユーザ認証モードの設定、UPS(無停電電源装置)を設定してください。
2. 等値化対象範囲内のすべての HIS を、シャットダウンしてください。
3. ダウンロードマスタを起動してください。
4. CAMS for HIS データベース以外の、CS 3000 のパッケージデータをリストアしてください。
5. <CENTUM VP インストールフォルダ>に CAMS\hist フォルダ、および CAMS\hisis フォルダが存在している場合は、そのフォルダとフォルダ以下のすべてのファイルを削除してください。

以上で、CAMS for HIS データのリストア前の作業は終了です。

■ CAMS for HIS ダウンロードマスタでの、CAMS for HIS データのリストア

CAMS for HIS データのリストア作業は、先に CAMS for HIS ダウンロードマスタに対して実施してください。その後で、それ以外の HIS に対して作業を実施してください。

CAMS for HIS ダウンロードマスタでの、CAMS for HIS データのリストア手順を次に示します。

1. CAMS for HIS が無効になっていることを確認してから、バックアップした CAMS for HIS データベースから次のフォルダとファイルを、<CENTUM VP インストールフォルダ>の同じ場所にコピーしてください。

フォルダ：

CAMS¥Client	(CAMS for HIS メッセージモニタのデータ)
CAMS¥configurator	(CAMS for HIS コンフィグレータのデータ)
CAMS¥database	(CAMS for HIS 稼動時データベース)
CAMS¥defhist	(CAMS for HIS 稼動時データベースのバックアップ)
CAMS¥hist	(CAMS for HIS ヒストリカルデータ)
CAMS¥ScenarioFiles	(CAMS for HIS 擬似アラーム発生ツールのシナリオファイル)
CAMS¥Viewer	(CAMS for HIS ヒストリカルビューアのデータ)

ファイル：

CAMS¥CAMSCapture.bin	(OPC A&E サーバ接続設定)
CAMS¥ServerConfig.xml	(CAMS for HIS サーバ設定)
CAMS¥SystemScopeDefinition.bin	(等値化対象範囲設定)

2. コピーが終了したら、HIS ユーティリティの CAMS for HIS タブシートで CAMS for HIS を有効にしてから、HIS を再起動してください。

既存の CS 3000 のレビジョンが R3.08.50 より古い場合は、手順 3.～手順 4.を実行してください。R3.08.50 以降の場合は、手順 5.に移ってください。

3. バージョンアップ前に使用していた CAMS for HIS コンフィグレータを、起動します。コマンドプロンプトから、以下のコマンドを実行してください。

<CENTUM VP インストールフォルダ>\CAMS¥CAMSConfigurator.exe -o

4. 起動した CAMS for HIS コンフィグレータで、CAMS for HIS データベースをバックアップしてください。

5. エンジニアリング基本機能をインストールした HIS を、起動してください。

6. 既存の CS 3000 プロジェクトデータベースを、手順 5.で起動した HIS の、適切な場所にリストアしてください。

7. プロジェクト属性変更ユーティリティを起動してください。

8. プロジェクトデータベースを、システムビューに登録してください。

9. システムビューを起動してください。

プロジェクトデータベースのバージョンアップ処理が、自動的に行われます。

10. CAMS for HIS マイグレーションツールを起動してください。

11. 既存の CS 3000 の CAMS for HIS データベースを、マイグレーションツールで変換してください。

12. エンジニアリング基本機能をインストールした HIS で、システムビューを起動してください。

13. システムビューでダウンロードマスタを選択してから、[プロジェクト共通部ダウンロード] を実施してください。

以上で CAMS for HIS ダウンロードマスタでの、CAMS for HIS データのリストア作業は終了です。

参照

CAMS for HIS マイグレーションツールについては、以下を参照してください。

統合型アラーム管理リファレンス (IM 33J05A21-01JA) の「B3.6 マイグレーションツール」

■ CAMS for HIS ダウンロードマスター以外の HIS での、CAMS for HIS データのリストア

この作業は、CAMS for HIS ダウンロードマスターでのリストア作業が完了してから実施してください。

CAMS for HIS ダウンロードマスター以外の HIS での、CAMS for HIS データのリストア手順を次に示します。

1. ダウンロードマスター以外の各 HIS に、CENTUM VP ソフトウェアをインストールしてください。
その後、IT セキュリティの設定、ライセンスの配布、ユーザーアカウントの作成、ユーザごとの Windows 動作環境の設定、ユーザ認証モードの設定、UPS(無停電電源装置)を設定してください。
2. CAMS for HIS データベース以外の、CS 3000 のパッケージデータをリストアしてください。
3. <CENTUM VP インストールフォルダ>に CAMS¥hist フォルダ、および CAMS¥hisis フォルダが存在している場合は、そのフォルダとフォルダ以下のすべてのファイルを削除してください。
4. CAMS for HIS が無効になっていることを確認してから、バックアップした CAMS for HIS データベースから次のフォルダとファイルを、<CENTUM VP インストールフォルダ>の同じ場所にコピーしてください。

フォルダ：

CAMS¥Client	(CAMS for HIS メッセージモニタのデータ)
CAMS¥configurator	(CAMS for HIS コンフィグレータのデータ)
CAMS¥database	(CAMS for HIS 稼動時データベース)
CAMS¥defhist	(CAMS for HIS 稼動時データベースのバックアップ)
CAMS¥hist	(CAMS for HIS ヒストリカルデータ)
CAMS¥ScenarioFiles	(CAMS for HIS 擬似アラーム発生ツールのシナリオファイル)
CAMS¥Viewer	(CAMS for HIS ヒストリカルビューアのデータ)

ファイル：

CAMS¥CAMSCapture.bin	(OPC A&E サーバ接続設定)
CAMS¥ServerConfig.xml	(CAMS for HIS サーバ設定)
CAMS¥SystemScopeDefinition.bin	(等値化対象範囲設定)

5. データコピーが終了したら、HIS ユーティリティの CAMS for HIS タブシートで CAMS for HIS を有効にしてから、HIS を再起動してください。
6. エンジニアリング基本機能をインストールした HIS で、システムビューを起動してください。
7. システムビューでダウンロードマスター以外の HIS を選択してから、[プロジェクト共通部ダウンロード] を実施してください。

以上で CAMS for HIS ダウンロードマスター以外の HIS での、CAMS for HIS データのリストア作業は終了です。

■ すべての HIS で共通の作業

1. HIS ユーティリティの CAMS for HIS タブシートで、すべての HIS の CAMS for HIS が有効になっていることを確認してください。
2. すべての HIS で、CAMS for HIS インデックスファイル生成ツールを起動してください。

以上で、CAMS for HIS データのリストアは終了です。

参照

CAMS for HIS インデックスファイル生成ツールについては、以下を参照してください。

「■ CAMS for HIS ヒストリカルビューア検索改善」ページ C11-26

C6.2 CENTUM CS 1000 から CENTUM VP R6 への アップグレードをする

CS 1000 と CENTUM VP の R6 では、動作保証している OS が違うため、動作保証している OS を搭載したコンピュータにソフトウェアを新規インストールして、その後、プロジェクトのデータベースを移行することが必要です。

C6.2.1 アップグレードをする

ここでは、アップグレードの方法について説明します。

■ アップグレードの流れ

アップグレードは次のような流れとなります。これに沿って、作業を行ってください。

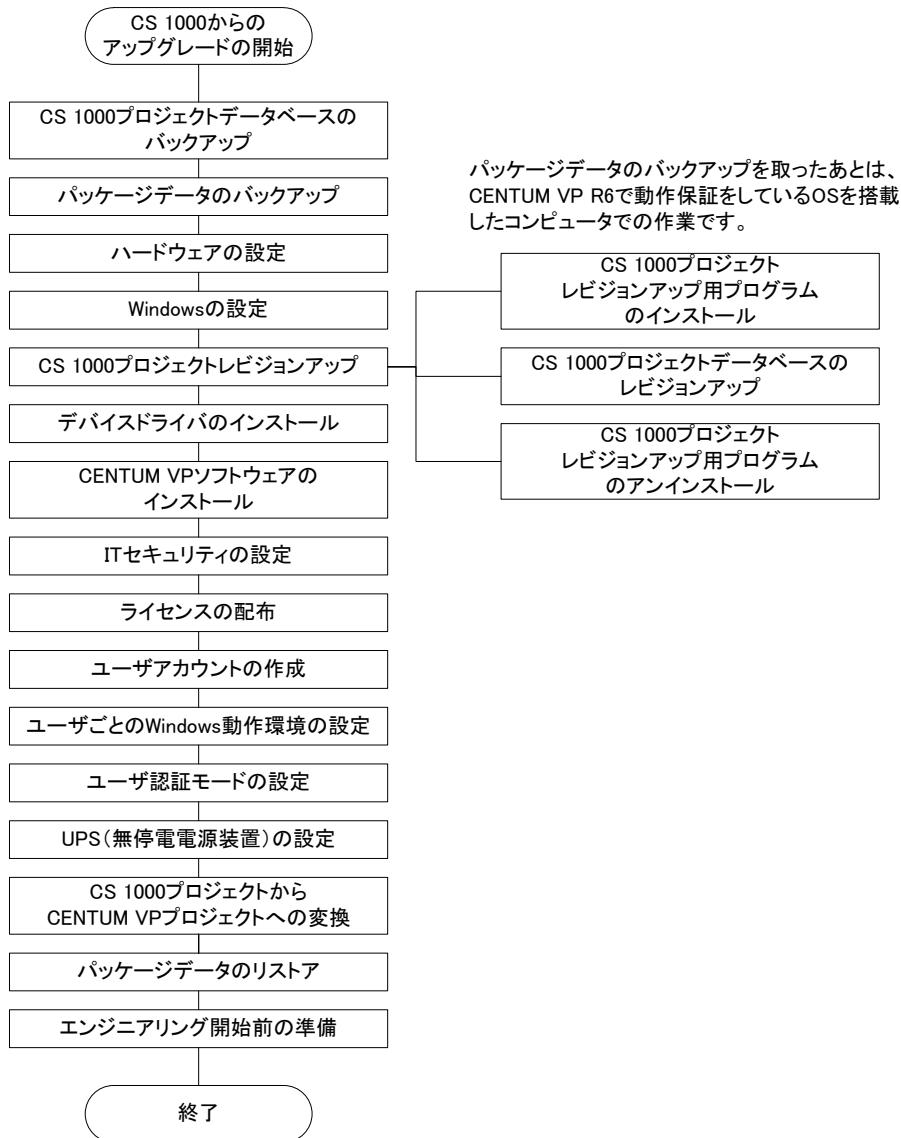


図 C6.2.1-1 バージョンアップの流れ

重要

- CS 1000 プロジェクトレビジョンアップ用プログラムのインストールおよび CENTUM VP ソフトウェアのインストールは、R6 での動作が保証されている OS で行ってください。その際は、先に Windows の設定を行ってください。
- CS 1000 プロジェクトデータベースのレビジョンアップが終了したら、CENTUM VP ソフトウェアのインストールをする前に、必ず CS 1000 プロジェクトレビジョンアップ用プログラムをアンインストールしてください。

■ CS 1000 プロジェクトデータベースのバックアップ

既存の CS 1000 で、必要なプロジェクトデータベースをバックアップしてください。

参照

プロジェクトデータベースのバックアップについては、以下を参照してください。

「C5.2 VP プロジェクトのバックアップをとる」ページ C5-3

■ パッケージデータのバックアップ

既存の CS 1000 で使用しているパッケージで、保存が必要なデータをパッケージごとにバックアップしてください。

アクセス制限の機能を有効にしている場合は無効に設定してください。

参照

パッケージデータのバックアップについては、以下を参照してください。

「C6.2.2 CS 1000 パッケージデータのバックアップとリストア」ページ C6-24

アクセス制限の設定については、以下を参照してください。

FDA : 21CFR Part11 対応リファレンス (IM 33J10D21-01JA) の「2.1 権限チェックとエンジニア認証」

■ ハードウェアの設定

ハードウェアの設定をしてください。

参照

ハードウェアの設定については、以下を参照してください。

「B4.1 ハードウェアの設定をする」ページ B4-2

■ Windows の設定

Windows の設定をしてください。

参照

Windows の設定については、以下を参照してください。

「B4.2 Windows の設定をする」ページ B4-7

■ CS 1000 プロジェクトレビューションアップ用プログラムのインストール

CENTUM VP にするコンピュータに、CS 1000 プロジェクトレビューションアップ用プログラムをインストールします。(*1)

*1: インストール用メディアは、CENTUM VP ソフトウェアと同じものを使用します。

補足

CS 1000 プロジェクトレビューションアップ用プログラムは、既存の CS 1000 プロジェクトデータベースを CENTUM VP 対応レビューションに、レビューションアップする機能のみ持っています。

1. 管理者ユーザでログオンしてください。
2. 実行中のすべてのアプリケーションを終了してください。
3. CENTUM VP のソフトウェアメディアを DVD-ROM ドライブに挿入してください。
 - ・ 自動再生ダイアログが表示された場合、[Launcher.exe の実行] をクリックしてください。
 - ・ 自動再生ダイアログが表示されない場合、エクスプローラでソフトウェアメディアのトップフォルダにある Launcher.exe をダブルクリックしてください。
 インストールメニューが表示されます。
4. インストールメニューの [CS 1000DB 変換ツールのインストール] をクリックしてください。
ようこそダイアログが表示されます。

補足

- CS 3000 または CENTUM VP ソフトウェアがインストールされている場合、エラーダイアログが表示されません。
- Microsoft .NET Framework などの CENTUM VP に必要な Windows の再頒布モジュールがインストールされていない場合、それらのモジュールのインストールを促すダイアログが表示されます。
それらのモジュールをインストールする場合は、[インストール] をクリックしてください。[キャンセル] をクリックすると、CENTUM VP のインストールが中止されます。
CENTUM VP に必要なモジュールは次のとおりです。
 - Microsoft .NET Framework 4.6.2
 - MSXML 6.0 SP1
 - Microsoft Visual C++ 2017 再頒布可能パッケージ
 - OPCCOM ProxyStub

各モジュールのインストールが開始されると、ステータス欄の表示内容が変わります。また、インストール完了後、再起動を要求される場合があります。再起動を要求された場合、再起動後に CENTUM VP のインストールを継続してください。

- [次へ] をクリックしてください。
インストール先フォルダを指定するダイアログが表示されます。
- インストール先フォルダを指定して、[次へ] をクリックしてください。
設定内容の確認ダイアログが表示されます。
- 設定内容を確認し、[インストール] をクリックしてください。
インストールが完了すると、インストールの完了を示すダイアログが表示されます。
- [終了] をクリックして、コンピュータを再起動してください。

■ CS 1000 プロジェクトデータベースのレビジョンアップ

- バージョンアップ前の CS 1000 プロジェクトデータベースを適切な場所にリストアしてください。
- プロジェクト属性変更ユーティリティを起動してください。
- プロジェクトデータベースをシステムビューに登録してください。
- システムビューを起動してください。
プロジェクトデータベースのレビジョンアップ処理が自動的に行われます。

参照

プロジェクト属性変更ユーティリティについては、以下を参照してください。

エンジニアリングリファレンス Vol.1 (IM 33J10D10-01JA) の「2.3 プロジェクト属性変更ユーティリティ」

■ CS 1000 プロジェクトレビジョンアップ用プログラムのアンインストール

CS 1000 プロジェクトレビジョンアップ用プログラムのアンインストールを、CENTUM VP ソフトウェアのアンインストールと同じ手順で行ってください。

参照

アンインストールの詳細手順については、以下を参照してください。

「C7.1.3 CENTUM VP ソフトウェアをアンインストールする」ページ C7-10

■ デバイスドライバのインストール

制御バスドライバなどの通信用ドライバ、OPKB 用 USB ドライバなどのデバイスドライバをインストールしてください。

参照

デバイスドライバのインストール手順については、以下を参照してください。

- ・「B4.3 ネットワークの設定をする」ページ B4-43
- ・「B4.4 オペレーションキーボード用 USB ドライバのインストールをする」ページ B4-79
- ・「B4.5 コンソール形 HIS の場合に必要な設定をする」ページ B4-81

■ CENTUM VP ソフトウェアのインストール

CENTUM VP ソフトウェアのインストールを、新規インストールと同じ手順で行ってください。

参照

CENTUM VP ソフトウェアのインストール手順については、以下を参照してください。

「B4.6 CENTUM VP ソフトウェアのインストールをする」ページ B4-87

■ IT セキュリティの設定

IT セキュリティの設定をしてください。

参照

IT セキュリティについては、以下を参照してください。

「B4.7 IT セキュリティを設定する」ページ B4-96

■ ライセンスの配布

ライセンスの配布をしてください。

アップグレードの場合は、ライセンスマネージャにパッケージリストが添付されています。このパッケージリストをライセンスマネージャにインポートすることで、ライセンス配布に必要なステーション構成定義と各ステーションへのパッケージ割り付け定義が生成できます。

参照

ライセンスの配布については、以下を参照してください。

「B4.8 ライセンスの配布と反映をする」ページ B4-103

■ ユーザアカウントの作成

ユーザアカウントの作成をしてください。

参照

ユーザアカウントの作成については、以下を参照してください。

「B4.9 ユーザアカウントを作成する」ページ B4-104

■ ユーザごとの Windows 動作環境の設定

ユーザごとの Windows 動作環境の設定をしてください。

参照

ユーザごとの Windows 動作環境の設定については、以下を参照してください。

「B4.10 ユーザごとの Windows 動作環境の設定をする」ページ B4-109

■ ユーザ認証モードの設定

ユーザ認証モードの設定をしてください。

参照

ユーザ認証モードの設定については、以下を参照してください。

「B4.11 ユーザ認証モードの設定をする」ページ B4-136

■ UPS(無停電電源装置) の設定

UPS(無停電電源装置) の設定をしてください。

参照

UPS(無停電電源装置) の設定については、以下を参照してください。

「B4.12 UPS (無停電電源装置) の設定をする」ページ B4-149

■ CS 1000 プロジェクトから CENTUM VP プロジェクトへの変換

変換ツールを使って、プロジェクトデータベースを CENTUM VP に変換します。

重要

CS 1000 と CENTUM VP では、グラフィックの仕様が異なります。

CS 1000 のグラフィックファイルを、表示と動作の互換性を考慮して CENTUM VP R6 のグラフィックファイルに変換する場合は、そのための作業が必要です。

● HIS 変換ツール

プロジェクトに CS 1000 の HIS が含まれていると、CENTUM VP の HIS へのバージョンアップ処理が行われます。「HIS 変換ツール」が表示されますので、CENTUM VP の HIS に変換するステーションのチェックボックスをオンにし、CS 1000 の HIS のまま変換をしないステーションのチェックボックスはオフにしてください。

- CENTUM VP の HIS への変換時に、CS 1000 のグラフィックファイルは、ステーション単位で一括して CENTUM VP の最新のグラフィック形式に自動変換されます。
- HIS 変換ツールは、システムビューのツールメニューから [HIS 変換ツール] を選択することでも起動できます。

参照

CS 1000 のグラフィックファイルを、表示と動作の互換性を考慮して CENTUM VP R6 のグラフィックファイルに変換する方法については、以下を参照してください。

グラフィック変換手順 (IM 33J01C40-01JA)

● グラフィックファイル変換ツール

CS 1000 グラフィックファイル単位で CENTUM VP グラフィックファイルに変換する場合に使用します。CENTUM VP のグラフィック形式に変換されたファイルは、CENTUM VP のグラフィックビルダでインポートして編集することができます。

グラフィックファイルの変換は、次の手順に従ってください。

1. グラフィックファイル変換ツールを起動してください。
2. 変換する CS 1000 グラフィックファイルまたはフォルダを追加してください。
3. 出力先フォルダを指定し、[変換] をクリックしてください。

変換状況を示すダイアログが表示されます。

補足

ファイル変換が終了すると、[ステータス] に正常に変換された場合は [成功] が表示され、エラーの場合は [失敗] が表示されます。

4. [閉じる] をクリックし、グラフィックファイル変換ツールを終了してください。

参照

CS 1000 のグラフィックファイルを、表示と動作の互換性を考慮して CENTUM VP R6 のグラフィックファイルに変換する方法については、以下を参照してください。

グラフィック変換手順 (IM 33J01C40-01JA)

■ バックアップしたパッケージデータのリストア

バックアップしたパッケージごとのデータをリストアしてください。

参照

パッケージデータのリストアの詳細については、以下を参照してください。

「C6.2.2 CS 1000 パッケージデータのバックアップとリストア」ページ C6-24

■ 計器図ハイライト機能に関する注意事項

CENTUM VP R5.03.00 から、計器図ハイライト機能が追加されています。この機能はオフにすることもできます。

参照

計器図ハイライト機能については、以下を参照してください。

操作監視リファレンス Vol.2 (IM 33J05A11-01JA) の「2.7 計器図ハイライト機能」

計器図ハイライト機能のオンオフについては、以下を参照してください。

操作監視リファレンス Vol.1 (IM 33J05A10-01JA) の「1.2 HIS ユーティリティで設定する項目」の「■ 操作タブシートでの設定項目」の「● 計器図ハイライト機能」

C6.2.2 CS 1000 パッケージデータのバックアップとリストア

ここでは、バックアップする必要があるデータとそのバックアップ方法、リストア方法について説明します。

■ バックアップとリストアが必要なデータ

パッケージごとにバックアップ／リストアが必要なデータを次に示します。

バックアップはCS 1000で行い、リストアはCENTUM VPに対して行います。

表 C6.2.2-1 CS 1000 パッケージデータのバックアップとリストア

CS 1000 の パッケージ	名称	CENTUM VP R6 で該当す るパッケー ジ	バックアップ／リ ストアするデータ
PHS1101	操作監視基本機能	VP6H1100	・ HIS 設定情報 ・ HIS 関連データベース
PHS4200	ヒストリカルメッセージ統合 パッケージ (FDA 対応)	VP6H4200	ヒストリカル統合 サーバに格納されたデータ
PHS4700	拡張アラームフィルタパッケ ージ	VP6H4700	拡張アラームフィルタ定義データ
PHS6510	長期データ保管パッケージ	VP6H6510	長期データ
PHS6530	帳票パッケージ	VP6H6530	帳票定義データ
PHS6710	FCS データ設定/収集パッケージ (PICOT)	VP6H6710	定義データ
PHS5100	ビルダ基本機能 (*1)	VP6E5100	プロジェクトデータベース
PHS5110	アクセス制限パッケージ	VP6E5110	定義データ
PHS5151	グラフィック作成パッケージ	VP6E5150	プロジェクトデータベース
PHS5160	CS Batch 1000 ビルダ(*2)	VP6E5165	プロジェクトデータベース
PHS5161	CS Batch 1000 処方管理パッ ケージ(*3)	VP6E5166	処方のデータベース
PHS5170	FDA:21 CFR Part 11 対応パッ ケージ	VP6E5170	履歴管理データベース

*1: CENTUM VP R6 では、エンジニアリング基本機能です。

*2: CENTUM VP R6 では、バッチビルダです。

*3: CENTUM VP R6 では、処方管理パッケージです。

■ CS 1000 稼動中にバックアップするデータのバックアップとリストア

次のデータは、CS 1000 が稼動している状態でバックアップしてください。

バックアップするデータのコピーを作成しておき、各パッケージのインポート機能などを利用してリストアしてください。

重要

ビルダ基本機能、グラフィック作成パッケージ、CS Batch 1000 ビルダ、CS Batch 1000 処方管理パッケージのデータは、プロジェクトデータベースのバックアップとリストアに含まれます。

● 操作監視基本機能－HIS 設定情報

1. HIS 設定情報のエクスポートとインポート

HIS 設定のエクスポート機能で、HIS レジストリ情報をバックアップしてください。

インストール後の HIS 設定情報のリストアでは、バックアップしたファイル（ファイル拡張子 : .reg）をテキストエディタで次のように編集してから、インポートしてください。

- 変更前 : HKEY_LOCAL_MACHINE\SOFTWARE\YOKOGAWA\BenKei\HIS\COMMON
- 変更後 : HKEY_LOCAL_MACHINE\SOFTWARE\YOKOGAWA\CS3K\HIS\COMMON

2. タグ監視点数の再設定

HIS 設定のステーションタブで、タグ監視点数を再設定してください。

参照

HIS 設定ウィンドウのエクスポート、インポート機能については、以下を参照してください。

操作監視リファレンス Vol.1 (IM 33J05A10-01JA) の「4.3 HIS 設定ウィンドウ」の「■ HIS 設定ウィンドウの [インポート] と [エクスポート]」

● ヒストリカルメッセージ統合パッケージ

ヒストリカルメッセージ統合サーバに格納されたデータは、継承させることができます。継承させるためには、各 HIS で、ヒストリカルメッセージ統合サーバに保管されたヒストリカルファイルのシーケンス番号を継続させるための作業をすること、ヒストリカルメッセージの保管先を再設定することが必要です。

- 各 HIS でのシーケンス番号のバックアップ

管理者ユーザでログオンし、次のコマンドを実行して操作監視機能を停止してください。

<CS 1000 インストールフォルダ>\his\tool\BKHHisStop.exe

エクスプローラで、次のファイルから最新のシーケンス番号のファイルをリムーバブルメディアに保存してください。

<CS 1000 インストールフォルダ>\Log\HISHIST\HISHISTnnnn-YYYYMMDD.log (nnnn : シーケンス番号)

- ヒストリカルメッセージ統合サーバでの作業

管理者ユーザでログオンし、保管した最新のシーケンス番号のファイルを、ヒストリカルメッセージ統合サーバの各 HIS に対応したフォルダにコピーしてください。

サーバ上のフォルダ : <共有名>\HisHist\HISddss (dd : ドメイン番号、 ss : ステーション番号)

補足

上記のサーバ保管先に HIS 名のフォルダが存在する HIS が、ヒストリカルメッセージ統合管理の対象です。交換前の HIS が故障などで最新ヒストリカルファイルの取得ができないときには、上記のサーバ保管先の該当 HIS フォルダを参照して、最新（最大）のシーケンス番号をメモしてください。このときには、最新ヒストリカルファイルのサーバ側への反映はできません。

- シーケンス番号のリストア

バージョンアップした HIS に管理者ユーザでログオンし、次のコマンドを実行して操作監視機能を停止してください。

<VP インストールフォルダ>\his\tool\BKHHisStop.exe

次の HISHIST 保存フォルダ内を空にしてください。

保存フォルダ : <VP インストールフォルダ>\Log\HISHIST

次のコマンドをコマンドプロンプトで実行してください。

<VP インストールフォルダ>\his\tool\SetSeqNo.bat<手順 2 でメモした最新シーケンス番号> (Δ : スペース)

HIS を再起動し、起動後に HISHIST フォルダ内にバックアップしたシーケンス番号+1 のヒストリカルファイルが 1 つ作成されていることを確認してください。

サーバ保管定義ファイル設定を実施し、ヒストリカルメッセージ統合サーバへ接続して、保管を開始してください。

参照

保管先の再設定については、以下を参照してください。

操作監視リファレンス Vol.2 (IM 33J05A11-01JA) の「8.1.1 ヒストリカルメッセージ保存ファイル保管先 フォルダの設定」

● 拡張アラームフィルタパッケージ

- ・ バックアップ

拡張アラームフィルタパッケージのアラームフィルタ 定義のエクスポート機能を使用して、フィルタ定義をバックアップしてください。

- ・ リストア

拡張アラームフィルタパッケージのアラームフィルタ 定義のインポート機能を使用して、フィルタ定義をリストアしてください。

参照

アラームフィルタ定義のエクスポート、インポート機能の詳細については、以下を参照してください。

操作監視リファレンス Vol.2 (IM 33J05A11-01JA) の「7.5.3 拡張アラームフィルタウィンドウ」

● 長期データ保管パッケージ

- ・ バックアップ

長期データ保管パッケージのアーカイブ操作で、保管データを外部記憶媒体にバックアップしてください。

また、次の BKHLogFile.txt ファイルもバックアップしてください。

¥¥<コンピュータ名>¥LTDATA¥LOG¥BKHLogFile.txt

- ・ リストア

バックアップした保管データは、長期データ保管パッケージのリトリーブ操作で、外部記憶媒体から HIS のハードディスクにリストアしてください。

また、BKHLogFile.txt ファイルもバックアップのときと同じ場所にリストアしてください。

参照

アーカイブ操作とリトリーブ操作の詳細については、以下を参照してください。

CENTUM VP オプション機能リファレンス (IM 33J05H10-01JA) の「4.2.4 アーカイブ操作とリトリーブ操作」

● 帳票パッケージ

- ・ バックアップ

帳票パッケージのコピーツールを使用して、帳票定義ファイルをリムーバブルメディアにコピーしてください。

- ・ リストア

帳票パッケージのコピーツールを使用して、リムーバブルメディアの帳票定義ファイルをリストア対象のコンピュータにコピーしてください。

参照

帳票定義データのコピーについては、以下を参照してください。

- ・ CENTUM VP オプション機能リファレンス (IM 33J05H10-01JA) の「2.5.3 他コンピュータでの帳票印字」の「■ 他コンピュータへの帳票のコピー」
- ・ CENTUM VP オプション機能リファレンス (IM 33J05H10-01JA) の「2.1 帳票パッケージを使用するための設定を行う」

■ オフライン状態でバックアップするデータのバックアップとリストア

次のデータは、CS 1000 インストールフォルダを削除する前に、バックアップしてください。

これらのデータを CS 1000 側でバックアップするとき、CS 1000 操作監視機能は完全に停止している必要があります。また、CENTUM VP 側でリストアするときは、CENTUM VP 操作監視機能が停止している必要があります。

CENTUM VP のインストール後に、これらのデータを<CENTUM VP インストールフォルダ>以下の相対的に同じ場所にコピーしてください。コピー先フォルダに同名のファイルが存在する場合は、上書きしてください。

● 操作監視機能－HIS 関連データベース

音声メッセージ定義、メディアデータ、コンテキストメニュー定義をバックアップ・リストアしてください。ただし、音声や右クリックのカスタマイズなどの機能のように、機能を利用しないと、その機能で使用するファイルが存在しない場合もあります。

1. コマンドプロンプトで次のコマンドを実行し、操作監視機能を停止してください。
<CS1000 インストールフォルダ>\his\tool\BKHHisstop.exe
2. 次の HIS 関連のファイルをバックアップし、リストアしてください。リストアの場合は、フォルダ名は<CENTUM VP インストールフォルダ>となります。

<CS1000 インストールフォルダ>\his\database\ops\MediaDef.odb：音声メッセージ定義ファイル

<CS1000 インストールフォルダ>\his\Media\User：メディアデータ（User フォルダ以下のファイル）

<CS1000 インストールフォルダ>\his\spconf\BKHMenuDef.xml：コンテキストメニュー定義ファイル

● FCS データ設定／収集パッケージ (PICOT)

1. PICOT の停止

Windows タスクバーにある PICOT を開き、File メニューから [Exit] を選択してください。PICOT が停止します。

2. 定義ファイルのバックアップとリストア

- バックアップ

本パッケージの次のフォルダにある定義ファイルをバックアップしてください。

<CS 1000 インストールフォルダ>\his\users\save\BKUPICOT

- リストア

バックアップしたファイルを以下のフォルダにリストアしてください。

<CENTUM VP インストールフォルダ>\his\users\save\BKUPICOT

参照

定義ファイルの詳細については、以下を参照してください。

CENTUM VP オプション機能リファレンス (IM 33J05H10-01JA) の「3.2 PICOT の構成ファイルと処理の流れ」

● アクセス制限パッケージ、FDA:21 CFR Part 11 対応パッケージ

- バックアップ

アクセス制限ユーティリティで指定した「エンジニア登録ファイルの参照先」が CS 1000 インストールフォルダの下にある場合、そのフォルダ以下のファイルをバック

アップしてください。その際、EngPassword2.odc というファイルのアクセス権に everyone の Full コントロールを追加してください。

- リストア
ファイルを復元し、アクセス制限ユーティリティで再設定してください。

C6.3 CENTUM VP R4/R5 から R6 へのバージョンアップをする

CENTUM VP R4/R5 と CENTUM VP R6 では、一部を除いて動作保証している OS が異なります。そのため、まず動作保証している OS を搭載した PC を用意し、そこにソフトウェアを新規インストールしてから、プロジェクトのデータベースを移行してください。

補足

既存の CENTUM プロジェクトが、動作保証している OS にインストールされている場合は、次の手順を省略できます。

- ・ CENTUM プロジェクトデータベースのバックアップ
- ・ パッケージデータのバックアップ
- ・ ハードウェアの設定

■ バージョンアップの流れ

バージョンアップは次のような流れとなります。これに沿って、作業を行ってください。

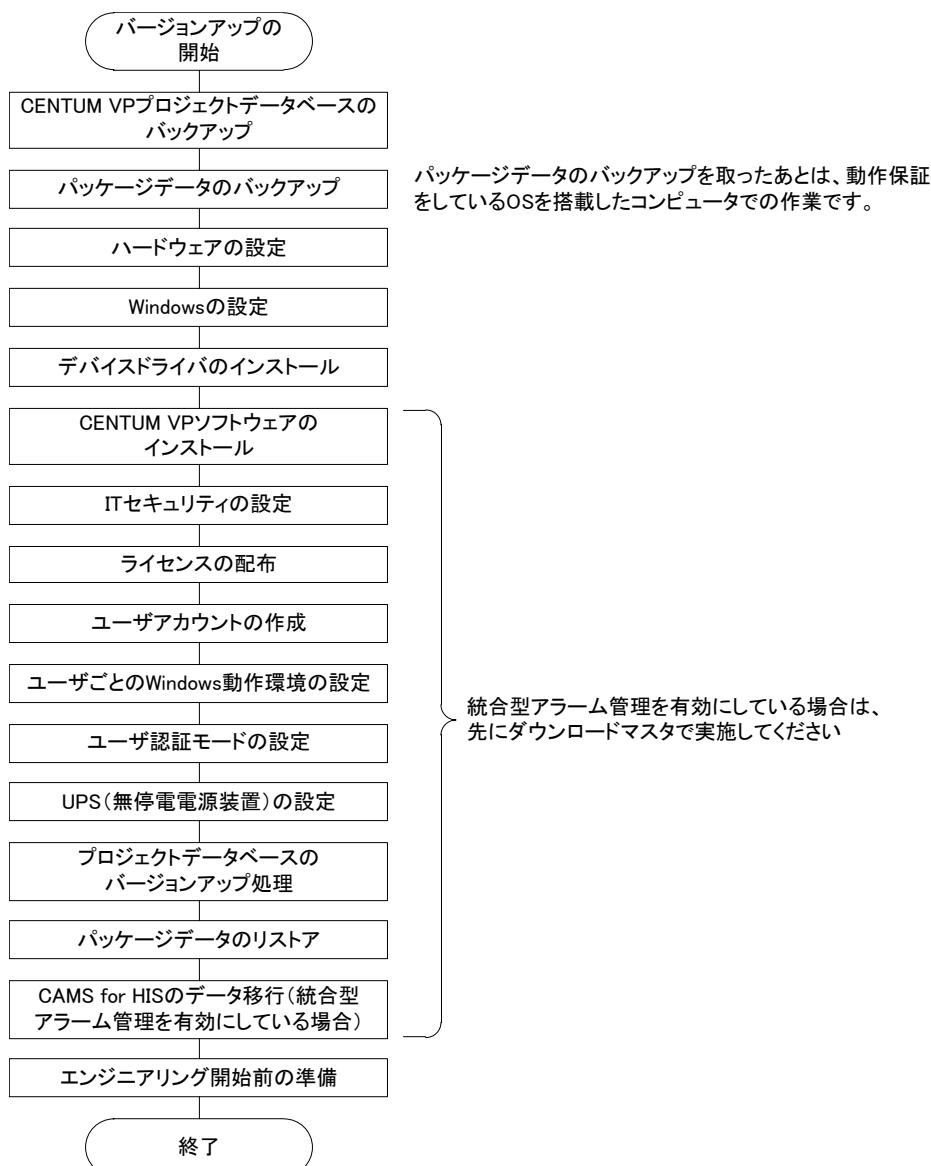


図 C6.3-1 バージョンアップの流れ

■ CENTUM プロジェクトデータベースのバックアップ

既存の CENTUM プロジェクトで、必要なプロジェクトデータベースをバックアップしてください。

既存の CENTUM プロジェクトが、動作保証している OS にインストールされている場合は、省略できます。

参照

プロジェクトデータベースのバックアップについては、以下を参照してください。

「C5.2 VP プロジェクトのバックアップをとる」ページ C5-3

■ パッケージデータのバックアップ

既存の CENTUM プロジェクトで使用しているパッケージで、保存が必要なデータをパッケージごとにバックアップしてください。

既存の CENTUM プロジェクトが、動作保証している OS にインストールされている場合は、省略できます。

■ ハードウェアの設定

ハードウェアの設定をしてください。

既存の CENTUM プロジェクトが、動作保証している OS にインストールされている場合は、省略できます。

参照

ハードウェアの設定については、以下を参照してください。

「B4.1 ハードウェアの設定をする」ページ B4-2

■ Windows の設定

Windows の設定をしてください。

参照

Windows の設定については、以下を参照してください。

「B4.2 Windows の設定をする」ページ B4-7

■ デバイスドライバのインストール

制御バスドライバなどの通信用ドライバ、OPKB 用 USB ドライバなどのデバイスドライバをインストールしてください。

既存の CENTUM プロジェクトが、動作保証している OS にインストールされている場合は、デバイスドライバの更新を実施してください。

参照

デバイスドライバのインストール手順については、以下を参照してください。

- ・「B4.3 ネットワークの設定をする」ページ B4-43
- ・「B4.4 オペレーションキーボード用 USB ドライバのインストールをする」ページ B4-79
- ・「B4.5 コンソール形 HIS の場合に必要な設定をする」ページ B4-81

■ デバイスドライバの更新

各ドライバの更新手順を次に示します。

● 制御バスドライバ

1. 制御バスドライバをアンインストールしてください。
2. 制御バスドライバをインストールしてください。
3. Windows ネットワークの設定をしてください。

参照

制御バスドライバのアンインストール方法については、以下を参照してください。

「■ 制御バスドライバのアンインストール」ページ C7-13

制御バスドライバのインストール方法については、以下を参照してください。

「B4.3.1 制御バスドライバのインストールをする」ページ B4-44

Windows ネットワークの設定方法については、以下を参照してください。

「B4.3.4 Windows ネットワークの設定をする」ページ B4-52

● Vnet/IP オープン通信ドライバ

1. Vnet/IP オープン通信ドライバをアンインストールしてください。
2. Vnet/IP オープン通信ドライバをインストールしてください。
3. Windows ネットワークの設定をしてください。

参照

Vnet/IP オープン通信ドライバのアンインストール方法については、以下を参照してください。

「■ Vnet/IP オープン通信ドライバのアンインストール」ページ C7-14

Vnet/IP オープン通信ドライバのインストール方法については、以下を参照してください。

「B4.3.2 Vnet/IP オープン通信ドライバのインストールをする」ページ B4-46

Windows ネットワークの設定方法については、以下を参照してください。

「B4.3.4 Windows ネットワークの設定をする」ページ B4-52

● RAS ドライバー AIP261/AIP262 カードを継続して使用する場合

1. RAS ドライバをアンインストールしてください。
2. RAS ドライバをインストールしてください。

参照

RAS ドライバのアンインストール方法については、以下を参照してください。

「■ RAS ドライバのアンインストール」ページ C7-18

RAS ドライバのインストール方法については、以下を参照してください。

「■ RAS ドライバのインストール」ページ B4-84

● RS-232C ドライバー AIP261/AIP262 カードを継続して使用する場合

1. RS-232C ドライバをアンインストールしてください。
2. RS-232C ドライバをインストールしてください。

参照

RS-232C ドライバのアンインストール方法については、以下を参照してください。

「■ RS-232C ドライバのアンインストール」ページ C7-18

RS-232C ドライバのインストール方法については、以下を参照してください。

「■ RS-232C ドライバのインストール」ページ B4-81

● オペレーションキーボード用 USB ドライバ

1. オペレーションキーボード用 USB ドライバをアンインストールしてください。

2. オペレーションキーボード用 USB ドライバをインストールしてください。

重要

オペレーションキーボード用 USB ドライバをインストールするときは、HIS を停止してから行ってください。また、オペレーションキーボード用 USB ドライバのインストールが完了すると、HIS は再起動します。

参照

オペレーションキーボード用 USB ドライバのアンインストール方法については、以下を参照してください。

「■ OPKB 用 USB ドライバのアンインストール」ページ C7-17

オペレーションキーボード用 USB ドライバのインストール方法については、以下を参照してください。

「B4.4 オペレーションキーボード用 USB ドライバのインストールをする」ページ B4-79

■ CENTUM VP ソフトウェアのインストール

CENTUM VP ソフトウェアをインストールしてください。

補足

CENTUM VP ソフトウェアのインストールは新規インストールの場合とほぼ同じですが、次の点に違いがあります。

- ・ CENTUM VP R4 の場合は、バージョンアップの確認ダイアログが表示される
バージョンアップの確認ダイアログが表示されたら、[次へ] をクリックしてください。
次の項目は、インストール済みの情報から収集するため、設定不要です。
 - ・名前
 - ・会社名
 - ・インストール先フォルダ
 - ・ステーション種別
 - ・データベースの参照先
 - ・ステーションのコンソールタイプ
- ・ カスタムフェースプレート更新ツールダイアログが表示される
CENTUM VP R4 で HIS にカスタムフェースプレートを設定している場合、そのカスタムフェースプレートは CENTUM VP R6 用のデータに自動的に変換されます。この変換処理は、インストールの完了直前に行われます。変換時にはプログレスバーが表示されます。
- ・ IT セキュリティ設定でソフトウェア制限ポリシーを適用している場合の起動方法
CENTUM VP R4 または R5 で、IT セキュリティ設定でソフトウェア制限ポリシーを適用している場合は、ソフトウェアメディアのトップフォルダにある Launcher.exe を右クリックして [管理者として実行] を選択して実行し、インストーラを起動してください。

参照

CENTUM VP ソフトウェアのインストール手順については、以下を参照してください。

「B4.6 CENTUM VP ソフトウェアのインストールをする」ページ B4-87

■ IT セキュリティの設定

IT セキュリティの設定をしてください。

参照

IT セキュリティについては、以下を参照してください。

「B4.7 IT セキュリティを設定する」ページ B4-96

■ ライセンスの配布

CENTUM VP R4 からのバージョンアップ時は、ライセンスを配布してください。CENTUM VP R5 からのバージョンアップ時は、ライセンスをバージョンアップしてから配布してください。

参照

ライセンス配布とバージョンアップについては、以下を参照してください。

「B4.8 ライセンスの配布と反映をする」ページ B4-103

■ ユーザアカウントの作成

ユーザアカウントの作成をしてください。

参照

ユーザアカウントの作成については、以下を参照してください。

「B4.9 ユーザアカウントを作成する」ページ B4-104

■ ユーザごとの Windows 動作環境の設定

ユーザごとの Windows 動作環境の設定をしてください。

参照

ユーザごとの Windows 動作環境の設定については、以下を参照してください。

「B4.10 ユーザごとの Windows 動作環境の設定をする」ページ B4-109

■ ユーザ認証モードの設定

ユーザ認証モードの設定をしてください。

参照

ユーザ認証モードの設定については、以下を参照してください。

「B4.11 ユーザ認証モードの設定をする」ページ B4-136

■ UPS(無停電電源装置) の設定

UPS(無停電電源装置) の設定をしてください。

参照

UPS(無停電電源装置) の設定については、以下を参照してください。

「B4.12 UPS (無停電電源装置) の設定をする」ページ B4-149

■ プロジェクトデータベースのバージョンアップ

システム生成機能のみを搭載したコンピュータの場合、システムビューを起動し、プロジェクトデータベースを開くとバージョンアップ処理が自動的に行われます。バージョンアップ処理中はグラフィックファイル更新ツールが自動的に起動されて、R4 のグラフィックファイルは最新のグラフィック形式に変換されます。

● グラフィックファイル更新ツールの留意事項

グラフィックファイル更新ツールでは、次の点に留意ください。

- ・ ユーザがグラフィックファイルをバージョンアップするステーションを選択できません。全ステーションが対象となります。
- ・ グラフィックファイルのバージョンアップの対象となるステーションは、R4.01.00 以降の HIS のみです。
- ・ グラフィックファイル更新ツールの実行を途中で取り消すことはできません。

● グラフィックファイル更新ツールの対象ファイル

次のファイルがバージョンアップの対象です。

- ・ R4.01.00～R4.03.00 のリビジョンで作成したグラフィックファイル

(ファイル拡張子 : edf)

- R4.01.00～R4.03.00 のレビューで作成した作業中グラフィックファイル
(ファイル拡張子 : wkf)
- R4.01.00～R4.03.00 のレビューで作成したリンクパーティファイル
(ファイル拡張子 : lpx)
- R4.01.00～R4.03.00 のレビューで作成したユーザ定義デフォルトファイル

補足

ファイル拡張子が sva のファイルについては、グラフィックファイルバージョンアップの対象外です。ただし、R4 以前で作成された sva ファイルやグラフィックファイルは、グラフィックビルダでインポートしたときに最新のグラフィック形式に変換されます。

■ バージョンアップに伴う、CAMS for HIS データの移行

CAMS for HIS では等値化対象範囲内に、ダウンロードマスターとなる HIS と、それ以外の HIS が存在します。

どちらもデータ移行作業の手順は同じですが、データのリストアについては、先に CAMS for HIS ダウンロードマスターでの作業を完了させてください。その後で、CAMS for HIS ダウンロードマスター以外の HIS に対して、同様の作業を実施してください。

ここでは、CAMS for HIS データのバックアップ方法、リストア方法について説明します。

参照

CAMS for HIS ダウンロードマスターについては、以下を参照してください。

統合型アラーム管理リファレンス (IM 33J05A21-01JA) の「A1. CAMS for HIS の概要」の「■ CAMS for HIS を使用したときのシステム構成」

● CAMS for HIS データのバックアップ

CAMS for HIS データのバックアップは、CAMS for HIS 以外のパッケージデータのバックアップ作業が完了した後、CAMS for HIS を無効にした状態で行ってください。

CAMS for HIS データのバックアップ手順を、次に示します。

1. 等値化対象範囲内の、既存の CENTUM プロジェクトの各 HIS に、管理者ユーザでログオンしてください。
2. HIS ユーティリティの CAMS for HIS タブシートで CAMS for HIS を無効にしてから、HIS を再起動してください。
3. 各 HIS で、次の CAMS フォルダにあるすべてのファイルをバックアップしてください。

<CENTUM インストールフォルダ>\CAMS

補足

CAMS for HIS ヒストリカルデータが不要であれば、次のフォルダのファイルはバックアップ不要です。

- <CENTUM インストールフォルダ>\CAMS\hist
- <CENTUM インストールフォルダ>\CAMS\hisis (存在する場合)

以上で、CAMS for HIS データのバックアップは終了です。

● CAMS for HIS データのリストア前の作業

CAMS for HIS データのリストアは、HIS 関連データベースのリストア作業が完了した後、CAMS for HIS を無効にした状態で行ってください。

CAMS for HIS データのリストア作業を始める前に完了させておくべき作業について、手順を次に示します。

1. ダウンロードマスターとなる HIS に、CENTUM VP ソフトウェアをインストールしてください。

その後、IT セキュリティの設定、ライセンスの配布、ユーザアカウントの作成、ユーザごとの Windows 動作環境の設定、ユーザ認証モードの設定、UPS(無停電電源装置)を設定してください。

2. 等値化対象範囲内のすべての HIS を、シャットダウンしてください。
3. ダウンロードマスタを起動してください。
4. CAMS for HIS データベース以外の、CENTUM プロジェクトのパッケージデータをリストアしてください。
5. <CENTUM VP インストールフォルダ>に CAMS¥hist フォルダ、および CAMS¥hisis フォルダが存在している場合は、そのフォルダとフォルダ以下のすべてのファイルを削除してください。

以上で、CAMS for HIS データのリストア前の作業は終了です。

● CAMS for HIS ダウンロードマスタでの、CAMS for HIS データのリストア

CAMS for HIS データのリストア作業は、先に CAMS for HIS ダウンロードマスタに対して実施してください。その後で、それ以外の HIS に対して作業を実施してください。

CAMS for HIS ダウンロードマスタでの、CAMS for HIS データのリストア手順を次に示します。

1. CAMS for HIS が無効になっていることを確認してから、バックアップした CAMS for HIS データベースから次のフォルダとファイルを、<CENTUM VP インストールフォルダ>の同じ場所にコピーしてください。

フォルダ：

CAMS¥Client	(CAMS for HIS メッセージモニタのデータ)
CAMS¥configurator	(CAMS for HIS コンフィグレータのデータ)
CAMS¥database	(CAMS for HIS 稼動時データベース)
CAMS¥defhist	(CAMS for HIS 稼動時データベースのバックアップ)
CAMS¥hist	(CAMS for HIS ヒストリカルデータ)
CAMS¥hisis	(存在する場合)
CAMS¥ScenarioFiles	(CAMS for HIS 摳似アラーム発生ツールのシナリオファイル)
CAMS¥Viewer	(CAMS for HIS ヒストリカルビューアのデータ)
CAMS¥Save	(アラーム設定値管理のデータ)

ファイル：

CAMS¥CAMSCapture.bin	(OPC A&E サーバ接続設定)
CAMS¥ServerConfig.xml	(CAMS for HIS サーバ設定)
CAMS¥SystemScopeDefinition.bin	(等値化対象範囲設定)

2. コピーが終了したら、HIS ユーティリティの CAMS for HIS タブシートで CAMS for HIS を有効にしてから、HIS を再起動してください。

既存の CENTUM プロジェクトのレビジョンが CS 3000 R3.08.50 より古い場合は、手順 3.～手順 4.を実行してください。CS 3000 R3.08.50 以降の場合は、手順 5.に移ってください。

3. バージョンアップ前に使用していた CAMS for HIS コンフィグレータを、起動します。コマンドプロンプトから、以下のコマンドを実行してください。
<CENTUM VP インストールフォルダ>\CAMS¥CAMSConfigurator.exe -o
4. 起動した CAMS for HIS コンフィグレータで、CAMS for HIS データベースをバックアップしてください。

5. エンジニアリング基本機能をインストールした HIS を、起動してください。
 6. 既存の CENTUM プロジェクトデータベースを、手順 5.で起動した HIS の、適切な場所にリストアしてください。
 7. プロジェクト属性変更ユーティリティを起動してください。
 8. プロジェクトデータベースを、システムビューに登録してください。
 9. システムビューを起動してください。
プロジェクトデータベースのバージョンアップ処理が、自動的に行われます。
既存の CENTUM プロジェクトの Revision が CENTUM VP R4.02 より古い場合は、手順 10.～手順 11.を実行してください。CENTUM VP R4.02 以降の場合は、手順 12.に移ってください。
 10. CAMS for HIS マイグレーションツールを起動してください。
 11. 既存の CENTUM プロジェクトの CAMS for HIS データベースを、マイグレーションツールで変換してください。
 12. エンジニアリング基本機能をインストールした HIS で、システムビューを起動してください。
 13. システムビューでダウンロードマスタを選択してから、[プロジェクト共通部ダウンロード] を実施してください。
- 以上で CAMS for HIS ダウンロードマスタでの、CAMS for HIS データのリストア作業は終了です。

参照

CAMS for HIS マイグレーションツールについては、以下を参照してください。

統合型アラーム管理リファレンス (IM 33J05A21-01JA) の「B3.6 マイグレーションツール」

● CAMS for HIS ダウンロードマスタ以外の HIS での、CAMS for HIS データのリストア

この作業は、CAMS for HIS ダウンロードマスタでのリストア作業が完了してから実施してください。

CAMS for HIS ダウンロードマスタ以外の HIS での、CAMS for HIS データのリストア手順を次に示します。

1. ダウンロードマスタ以外の各 HIS に、CENTUM VP ソフトウェアをインストールしてください。
その後、IT セキュリティの設定、ライセンスの配布、ユーザーアカウントの作成、ユーザごとの Windows 動作環境の設定、ユーザ認証モードの設定、UPS(無停電電源装置)を設定してください。
2. CAMS for HIS データベース以外の、CENTUM プロジェクトのパッケージデータをリストアしてください。
3. <CENTUM VP インストールフォルダ>に CAMS¥hist フォルダ、および CAMS¥hisis フォルダが存在している場合は、そのフォルダとフォルダ以下のすべてのファイルを削除してください。
4. CAMS for HIS が無効になっていることを確認してから、バックアップした CAMS for HIS データベースから次のフォルダとファイルを、<CENTUM VP インストールフォルダ>の同じ場所にコピーしてください。

フォルダ：

CAMS¥Client	(CAMS for HIS メッセージモニタのデータ)
CAMS¥configurator	(CAMS for HIS コンフィグレータのデータ)
CAMS¥database	(CAMS for HIS 稼動時データベース)

CAMS¥defhist	(CAMS for HIS 稼動時データベースのバックアップ)
CAMS¥hist	(CAMS for HIS ヒストリカルデータ)
CAMS¥hisis	(存在する場合)
CAMS¥ScenarioFiles	(CAMS for HIS 摂似アラーム発生ツールのシナリオファイル)
CAMS¥Viewer	(CAMS for HIS ヒストリカルビューアのデータ)
CAMS¥Save	(アラーム設定値管理のデータ)

ファイル：

CAMS¥CAMSCapture.bin	(OPC A&E サーバ接続設定)
CAMS¥ServerConfig.xml	(CAMS for HIS サーバ設定)
CAMS¥SystemScopeDefinition.bin	(等値化対象範囲設定)

5. データコピーが終了したら、HIS ユーティリティの CAMS for HIS タブシートで CAMS for HIS を有効にしてから、HIS を再起動してください。
6. エンジニアリング基本機能をインストールした HIS で、システムビューを起動してください。
7. システムビューでダウンロードマスター以外の HIS を選択してから、[プロジェクト共通部ダウンロード] を実施してください。

以上で CAMS for HIS ダウンロードマスター以外の HIS での、CAMS for HIS データのリストア作業は終了です。

● すべての HIS で共通の作業

1. HIS ユーティリティの CAMS for HIS タブシートで、すべての HIS の CAMS for HIS が有効になっていることを確認してください。

既存の CENTUM プロジェクトの Revision が CENTUM VP R5.01 より古い場合は、手順 2.を実行してください。

2. すべての HIS で、CAMS for HIS インデックスファイル生成ツールを起動してください。

以上で、CAMS for HIS データのリストアは終了です。

参照

CAMS for HIS インデックスファイル生成ツールについては、以下を参照してください。

「■ CAMS for HIS ヒストリカルビューア検索改善」ページ C11-26

C6.4 CENTUM VP R6 のリビジョンアップをする

すでに CENTUM VP R6 がインストールされているコンピュータをリビジョンアップする方法を説明します。

■ ソフトウェアのリビジョンアップ範囲

CENTUM VP のソフトウェアは、VP プロジェクトごとに同一のリビジョンである必要があります。CENTUM VP のソフトウェアをリビジョンアップする場合に、リビジョンアップが必要な範囲を以下の例に分けて、説明します。

- ・ VP プロジェクトが 1 つの場合
- ・ AD プロジェクトや VP プロジェクトが複数の場合
- ・ AD サーバとシステム生成機能を 1 つのコンピュータに共存させた場合

● VP プロジェクトが 1 つの場合のソフトウェアのリビジョンアップ範囲

VP プロジェクトが 1 つの場合のシステム構成例を次の図に示します。

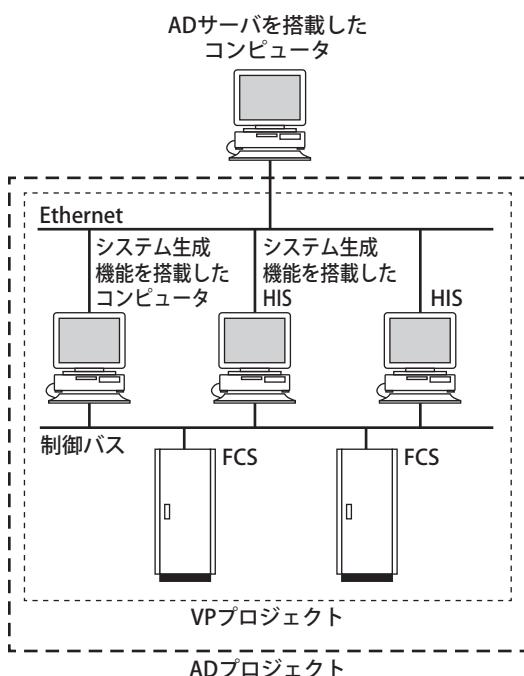


図 C6.4-1 VP プロジェクトが 1 つの場合のシステム構成例

図のようなシステム構成の場合は、CENTUM VP のソフトウェアをリビジョンアップするときには、AD サーバを搭載したコンピュータを含む、すべてのコンピュータや HIS のソフトウェアを同一リビジョンにリビジョンアップする必要があります。

● AD プロジェクトや VP プロジェクトが複数の場合のソフトウェアのリビジョンアップ範囲

AD サーバには、複数の AD プロジェクトを登録でき、1 つの AD プロジェクトには、複数の VP プロジェクトを登録できます。そして、VP プロジェクトには、システム生成機能を搭載したコンピュータや HIS が登録されます。

そのシステム構成の例を次の図に示します。

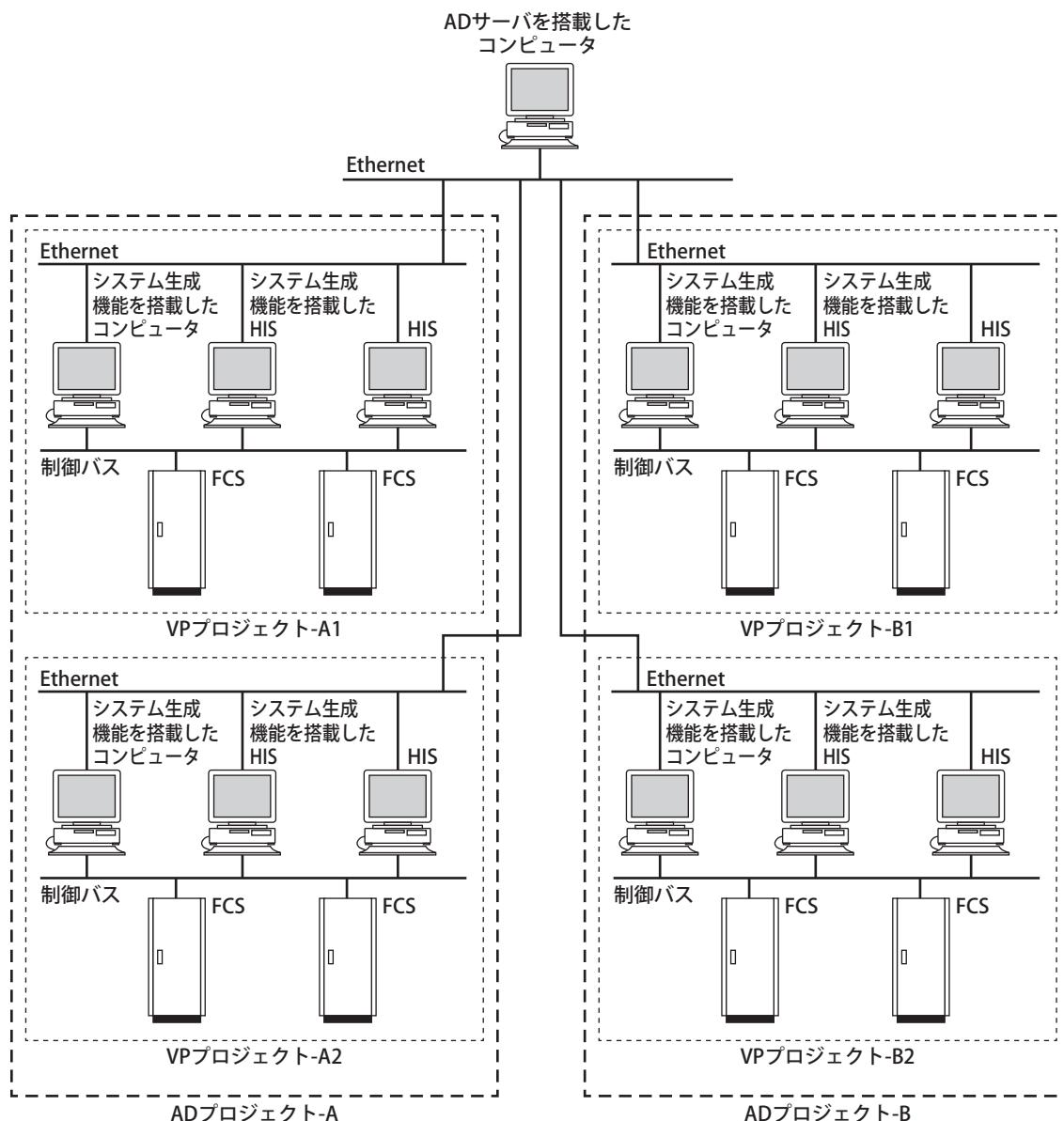


図 C6.4-2 AD プロジェクトや VP プロジェクトが複数の場合のシステム構成例

図のようなシステム構成の場合に CENTUM VP のソフトウェアをレビューションアップするときは、AD サーバを搭載したコンピュータを含む、すべてのコンピュータおよび HIS のソフトウェアを同一レビューションにレビューションアップすることを推奨します。

すべてのシステム生成機能を搭載したコンピュータや HIS のソフトウェアを同一レビューションにできない場合は、VP プロジェクトごとに同一のレビューションにしてください。その場合でも AD サーバについては、必ず最新レビューションにレビューションアップするようにしてください。

図を例にすると、以下のような構成を取ることができます。

- AD サーバ: 最新レビューション
- VP プロジェクト-A1 のコンピュータと HIS のソフトウェア: 最新レビューション
- VP プロジェクト-A2 のコンピュータと HIS のソフトウェア: 古いレビューション
- VP プロジェクト-B1 のコンピュータと HIS のソフトウェア: 古いレビューション
- VP プロジェクト-B2 のコンピュータと HIS のソフトウェア: 古いレビューション

重要

- このように複数のレビューションが混在する場合は、AD サーバを必ず最新のレビューションにレビューションアップしてください。
システム生成機能のレビューションより、AD サーバのレビューションが新しい場合は、AD オーガナイザを使用できますが、AD サーバのレビューションが古い場合は、AD オーガナイザを使用できません。
- 異なるレビューションの VP プロジェクトが混在する場合、新しいレビューションで追加された FCS の設定情報は古いレビューションの AD オーガナイザから閲覧できますが、編集できません。新しいレビューションで追加された FCS のステーションタイプに属するノードと入出力モジュールの設定情報は、古いレビューションの AD オーガナイザから閲覧も編集もできません。

● AD サーバとシステム生成機能を 1 つのコンピュータに共存させた場合のソフトウェアのレビューションアップ範囲

AD サーバとシステム生成機能を 1 つのコンピュータに共存させることもできます。

AD プロジェクトと VP プロジェクトが複数あり、AD サーバとシステム生成機能が 1 つのコンピュータに共存している場合のシステム構成の例を次に示します。

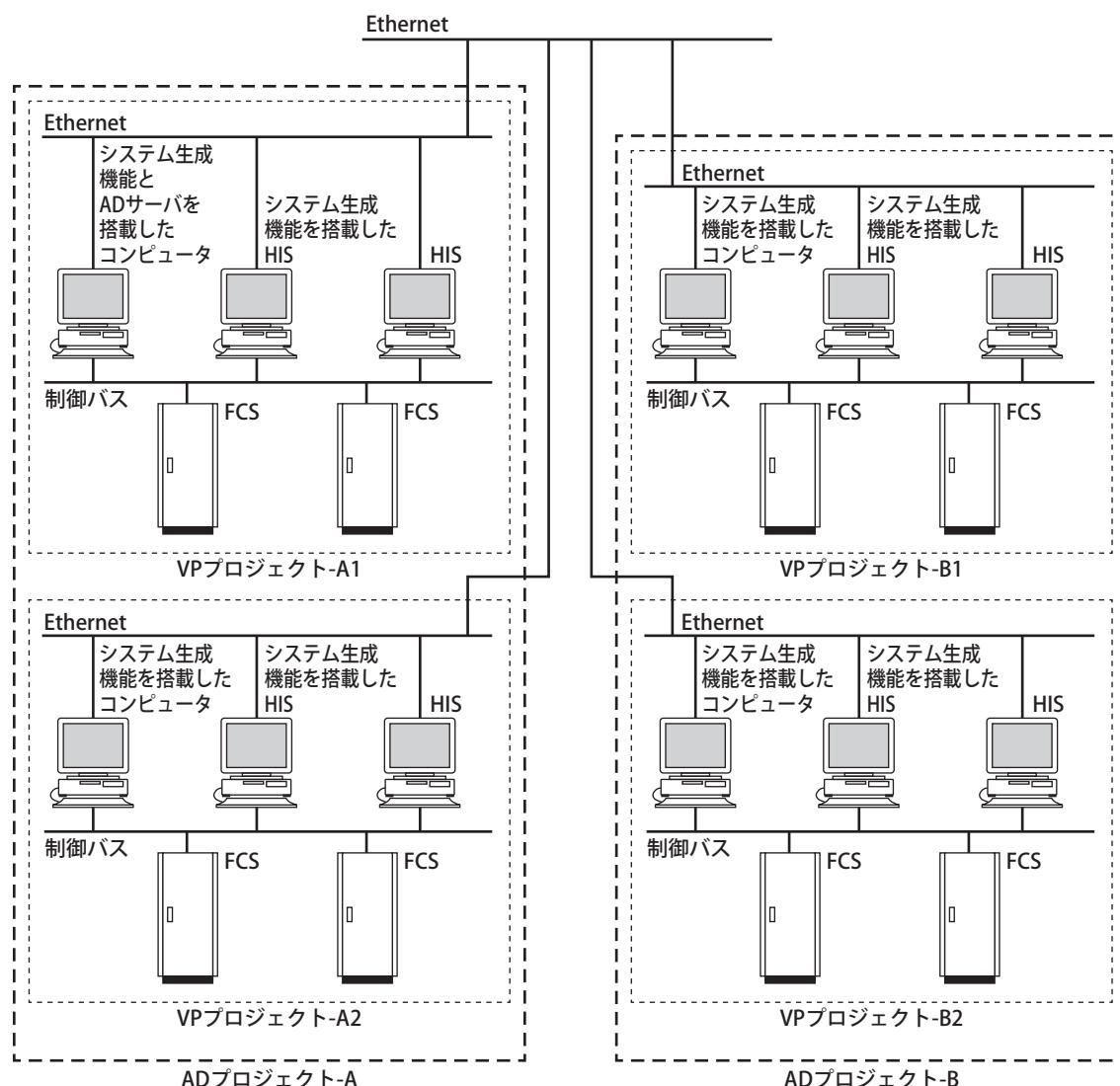


図 C6.4-3 AD サーバとシステム生成機能が 1 つのコンピュータに共存している場合のシステム構成例

図では、VP プロジェクト-A1 のコンピュータに AD サーバが搭載されています。

AD サーバとシステム生成機能が 1 つのコンピュータに共存している場合は、AD サーバとシステム生成機能を別のレビューションにすることできません。

図のようなシステム構成の場合に AD サーバを最新のレビューションにするためには、少なくとも VP プロジェクト-A1 のすべてのコンピュータと HIS のソフトウェアを最新レビューションにする必要があります。

VP プロジェクト-A1 のすべてのコンピュータと HIS をレビューションアップできない場合は、AD サーバを独立したコンピュータに移動して、最新レビューションにするか、または最新レビューションにする VP プロジェクトのコンピュータや HIS に AD サーバを移動するようにシステム構成を変更してください。

補足

AD サーバを移動するためには、移動元の AD サーバで ADMDB をバックアップして、移動先の AD サーバで ADMDB をリストアしてください。

重要

異なるレビューションの VP プロジェクトが混在する場合、新しいレビューションで追加された FCS の設定情報は古いレビューションの AD オーガナイザから閲覧できますが、編集できません。新しいレビューションで追加された FCS のステーションタイプに属するノードと入出力モジュールの設定情報は、古いレビューションの AD オーガナイザから閲覧も編集もできません。

参照

ADMDB のバックアップとリストアについては、以下を参照してください。

オートメーションデザインシート基本機能 (IM 33J10A10-01JA) の「C1.1.2 ADMDB のバックアップとリストア」

■ レビューションアップの流れ

すでに CENTUM VP ソフトウェアがインストールされているコンピュータをレビューションアップするときの流れを次に示します。

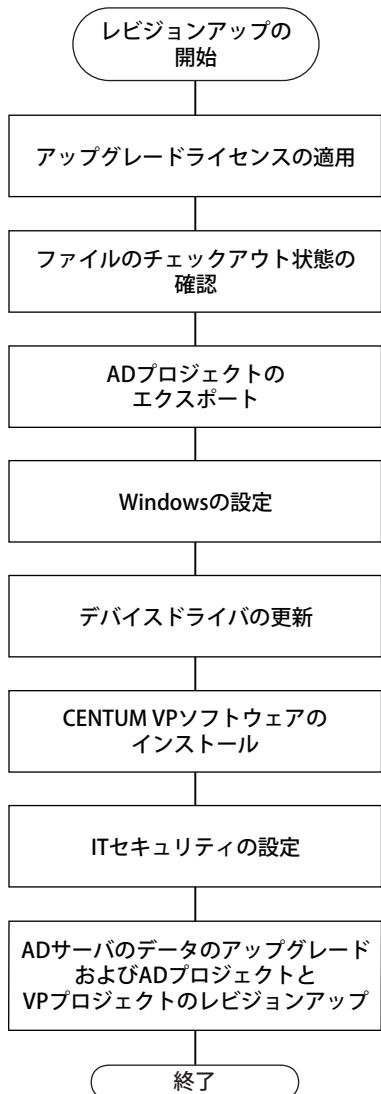


図 C6.4-4 レビューションアップの流れ

重要

CENTUM VP ソフトウェアをレビューションアップするときには、インストール済みのソフトウェアをアンインストールせずに、新しいレビューションのソフトウェアを上書きインストールしてください。

R6.04 以降の CENTUM VP ソフトウェアをアンインストールした場合、新しいレビューションの CENTUM VP ソフトウェアをインストールできません。その場合は、アンインストールした CENTUM VP ソフトウェアを再度インストールしたあと、新しいレビューションの CENTUM VP ソフトウェアを上書きインストールしてください。

■ アップグレードライセンスを適用する

R6.04 以降の CENTUM VP をレビューションアップするときは、アップグレードライセンスの配布と反映を実施してください。既にアップグレードライセンスが反映済みのときは、何もする必要はありません。

重要

新しいレビューションの CENTUM VP の発行日が、アップグレードライセンスの有効期限よりも前の日付であることも確認してください。

参照

アップグレードライセンスの配布と反映については、以下を参照してください。

ライセンス管理 (IM 33J01C20-01JA) の「5. アップグレードライセンスを操作する」の「■ アップグレードライセンスを配布、反映する」

■ ファイルのチェックアウト状態の確認

AD サーバのすべての AD プロジェクトで、すべてのファイルがチェックインされていることを確認してください。チェックアウト中のファイルがある場合は、AD オーガナイザでチェックイン、またはチェックアウトの取り消しをするか、ADS 管理ツールでチェックアウト状態を強制解除してください。

重要

チェックアウト中のファイルのチェックイン、またはチェックアウト取り消しは、CENTUM VP ソフトウェアのレビューションアップ前に必ず行ってください。CENTUM VP のソフトウェアのレビューションアップ後に、AD プロジェクトのレビューションアップを行います。チェックアウト中のファイルがある場合は、AD プロジェクトのレビューションアップがエラーとなります。

補足

レビューションアップ前に、修正中のファイルをジェネレーションする必要はありません。AD プロジェクトのファイルのマスタステータスやワークステータスは、レビューションアップの前後で変わりません。レビューションアップ前に修正したファイルをレビューションアップ後にジェネレーションできます。

参照

AD プロジェクトのファイルのチェックアウト状態を確認する方法については、以下を参照してください。

- ・ オートメーションデザインシート基本機能 (IM 33J10A10-01JA) の「C1.1.9 チェックアウト中ファイルに対するチェックアウト状態の強制解除」
- ・ オートメーションデザインシート基本機能 (IM 33J10A10-01JA) の「C1.3.7 チェックアウト中ファイルのチェックアウト状態を強制的に解除する」

■ AD プロジェクトのエクスポート

レビューションアップ作業のトラブル復旧のためのバックアップとして、AD プロジェクトをエクスポートします。

すべての VP プロジェクトを AD プロジェクトにバックアップしたあとで、すべての AD プロジェクトを、履歴情報を含めてエクスポートしてください。

参照

VP プロジェクトの AD プロジェクトへのバックアップについては、以下を参照してください。

オートメーションデザインシート基本機能 (IM 33J10A10-01JA) の「B1.5.1 VP プロジェクトを管理する」の「■ VP プロジェクトを操作する」の「● VP プロジェクトを AD プロジェクトにバックアップする」

AD プロジェクトのエクスポートについては、以下を参照してください。

オートメーションデザインシート基本機能 (IM 33J10A10-01JA) の「C1.3.4 AD プロジェクトをエクスポートする」

■ Windows の設定

Windows の設定手順を次に示します。

● ルート証明書の適用

Windows 7、または Windows Server 2008 R2 で、R6.03.10 以前からレビューションアップする場合は、ルート証明書を適用してください。

参照

Windows 7 のルート証明書の適用手順については、以下を参照してください。

「■ ルート証明書を適用する」ページ B4-21

Windows Server 2008 R2 のルート証明書の適用手順については、以下を参照してください。

「■ ルート証明書を適用する」ページ B4-41

● Windows 更新プログラムのインストール

次の条件をすべて満たす場合は、Windows 更新プログラムをダウンロードし、適用してください。

- ・ R6.04.00 以前からリビジョンアップする。
- ・ コンピュータの OS が Windows 7 または Windows Server 2008 R2 である。

参照

Windows 更新プログラムについては、以下を参照してください。

「● Windows 更新プログラムのダウンロード（Windows 7 または Windows Server 2008 R2）」ページ B1-4

■ デバイスドライバの更新

各ドライバの更新手順を次に示します。

● 制御バスドライバ

1. 制御バスドライバをアンインストールしてください。
2. 制御バスドライバをインストールしてください。
3. Windows ネットワークの設定をしてください。

参照

制御バスドライバのアンインストール方法については、以下を参照してください。

「■ 制御バスドライバのアンインストール」ページ C7-13

制御バスドライバのインストール方法については、以下を参照してください。

「B4.3.1 制御バスドライバのインストールをする」ページ B4-44

Windows ネットワークの設定方法については、以下を参照してください。

「B4.3.4 Windows ネットワークの設定をする」ページ B4-52

● Vnet/IP オープン通信ドライバ

1. Vnet/IP オープン通信ドライバをアンインストールしてください。
2. Vnet/IP オープン通信ドライバをインストールしてください。
3. Windows ネットワークの設定をしてください。

参照

Vnet/IP オープン通信ドライバのアンインストール方法については、以下を参照してください。

「■ Vnet/IP オープン通信ドライバのアンインストール」ページ C7-14

Vnet/IP オープン通信ドライバのインストール方法については、以下を参照してください。

「B4.3.2 Vnet/IP オープン通信ドライバのインストールをする」ページ B4-46

Windows ネットワークの設定方法については、以下を参照してください。

「B4.3.4 Windows ネットワークの設定をする」ページ B4-52

● Vnet/IP インタフェースパッケージ

仮想マシンを使用している場合のみ、次の作業を実施願います。

1. Vnet/IP インタフェースパッケージをアンインストールしてください。

2. Vnet/IP インタフェースパッケージをインストールしてください。
3. Windows ネットワークの設定をしてください。

参照

Vnet/IP インタフェースパッケージのアンインストール方法については、以下を参照してください。

「■ 仮想マシンの Vnet/IP インタフェースパッケージをアンインストールする」ページ C7-15

Vnet/IP インタフェースパッケージのインストール方法については、以下を参照してください。

「B4.3.3 仮想マシンに Vnet/IP インタフェースパッケージをインストールする」ページ B4-48

Windows ネットワークの設定方法については、以下を参照してください。

「B4.3.7 仮想マシンを使用する際の注意事項」ページ B4-77

● RAS ドライバー AIP261/AIP262 カードを継続して使用する場合

1. RAS ドライバをアンインストールしてください。
2. RAS ドライバをインストールしてください。

参照

RAS ドライバのアンインストール方法については、以下を参照してください。

「■ 仮想マシンの Vnet/IP インタフェースパッケージをアンインストールする」ページ C7-15

RAS ドライバのインストール方法については、以下を参照してください。

「■ RAS ドライバのインストール」ページ B4-84

● RS-232C ドライバー AIP261/AIP262 カードを継続して使用する場合

1. RS-232C ドライバをアンインストールしてください。
2. RS-232C ドライバをインストールしてください。

参照

RS-232C ドライバのアンインストール方法については、以下を参照してください。

「■ RS-232C ドライバのアンインストール」ページ C7-18

RS-232C ドライバのインストール方法については、以下を参照してください。

「■ RS-232C ドライバのインストール」ページ B4-81

● オペレーションキーボード用 USB ドライバ

1. オペレーションキーボード用 USB ドライバをアンインストールしてください。
2. オペレーションキーボード用 USB ドライバをインストールしてください。

重要

オペレーションキーボード用 USB ドライバをインストールするときは、HIS を停止してから行ってください。また、オペレーションキーボード用 USB ドライバのインストールが完了すると、HIS は再起動します。

参照

オペレーションキーボード用 USB ドライバのアンインストール方法については、以下を参照してください。

「■ OPKB 用 USB ドライバのアンインストール」ページ C7-17

オペレーションキーボード用 USB ドライバのインストール方法については、以下を参照してください。

「B4.4 オペレーションキーボード用 USB ドライバのインストールをする」ページ B4-79

■ CENTUM VP ソフトウェアのインストール

CENTUM VP ソフトウェアをインストールしてください。

補足

CENTUM VP ソフトウェアのインストールは新規インストールの場合とほぼ同じですが、次の点に違いがあります。

- ・次の項目は、インストール済みの情報から収集するため、設定不要です。
 - ・名前
 - ・会社名
 - ・インストール先フォルダ
 - ・ステーション種別
 - ・データベースの参照先
 - ・ステーションのコンソールタイプ
- ・CENTUM VP ソフトウェアのインストール後、パッケージの有効化処理中に、しばらくお待ちくださいという旨のダイアログが表示されます。

参照

CENTUM VP ソフトウェアのインストール手順については、以下を参照してください。

「B4.6 CENTUM VP ソフトウェアのインストールをする」ページ B4-87

● .NET Framework のインストール時の注意事項

IT セキュリティモデルの従来モデルが設定されているコンピュータに、CENTUM VP ソフトウェアをインストールするときに、.NET Framework のインストールに失敗する場合があります。その場合は、回避手順を実行してください。

参照

.NET Framework のインストールに失敗するときの回避手順については、以下を参照してください。

「C10.1.6 .NET Framework のインストールに失敗する」ページ C10-9

■ IT セキュリティの設定

IT セキュリティの設定をしてください。

参照

IT セキュリティについては、以下を参照してください。

「B4.7 IT セキュリティを設定する」ページ B4-96

■ AD サーバのデータのアップグレードおよび AD プロジェクトと VP プロジェクトのレビューションアップ

AD サーバのデータをアップグレードして、AD プロジェクトと VP プロジェクトをレビューションアップしてください。

参照

AD サーバのデータのアップグレードおよび AD プロジェクトと VP プロジェクトのレビューションアップについては、以下を参照してください。

オートメーションデザインシート基本機能 (IM 33J10A10-01JA) の「B2. レビューションアップ時のエンジニアリング開始方法」

C6.5 ライセンス管理専用のコンピュータのバージョンアップ/リビジョンアップをする

ここでは、ライセンス管理専用のコンピュータをバージョンアップ/リビジョンアップする方法を説明します。

■ バージョンアップ手順

1. Windows の設定を行ってください。
2. CENTUM VP のソフトウェアメディアを使用して、ライセンス管理ソフトウェアのインストールをしてください。

補足

ライセンス管理専用のコンピュータのバージョンアップの際のライセンス管理ソフトウェアインストールは、新規の場合とほぼ同じですが、次の項目は、インストール済みの情報から収集するため、設定不要です。

- ・ 名前
- ・ 会社名
- ・ インストール先フォルダ

3. ライセンスのバージョンアップを実施してください。
4. IT セキュリティの設定をしてください。
5. ユーザごとの Windows 動作環境を設定してください。

参照

Windows の設定については、以下を参照してください。

「● Windows の設定」ページ B7-1

ライセンス管理ソフトウェアのインストール手順については、以下を参照してください。

「B7. ライセンス管理専用のコンピュータのセットアップをする」ページ B7-1

ライセンスのバージョンアップ手順については、以下を参照してください。

ライセンス管理 (IM 33J01C20-01JA) の「4. CENTUM VP R5 から R6、ProSafe-RS R3 から R4 へのライセンスの更新」

IT セキュリティについては、以下を参照してください。

「B4.7 IT セキュリティを設定する」ページ B4-96

ユーザごとの Windows 動作環境の設定については、以下を参照してください。

「● ユーザごとの Windows 動作環境の設定」ページ B7-3

■ リビジョンアップ手順

1. R6.03.10 以前からのリビジョンアップの場合は、Windows の設定を行ってください。
2. CENTUM VP のソフトウェアメディアを使用して、ライセンス管理ソフトウェアのインストールをしてください。

補足

ライセンス管理専用のコンピュータのリビジョンアップの際のライセンス管理ソフトウェアインストールは、新規の場合とほぼ同じですが、次の項目は、インストール済みの情報から収集するため、設定不要です。

- ・ 名前
- ・ 会社名
- ・ インストール先フォルダ

3. IT セキュリティの設定をしてください。
4. R6.03.10 以前からのリビジョンアップの場合は、ユーザごとの Windows 動作環境を設定してください。

参照

Windows の設定については、以下を参照してください。

「● Windows の設定」ページ B7-1

ライセンス管理ソフトウェアのインストール手順については、以下を参照してください。

「B7. ライセンス管理専用のコンピュータのセットアップをする」ページ B7-1

IT セキュリティについては、以下を参照してください。

「B4.7 IT セキュリティを設定する」ページ B4-96

ユーザごとの Windows 動作環境の設定については、以下を参照してください。

「● ユーザごとの Windows 動作環境の設定」ページ B7-3

C6.6 オペレーションキーボードを置き換える

CENTUM VP R5.03.00 以降のバージョンでは、次のオペレーションキーボードが使用できます。

- ・ シングルループ操作用オペレーションキーボード（形名：AIP830）
- ・ 8 ループ同時操作用オペレーションキーボード（形名：AIP831）

現在使用しているオペレーションキーボードを AIP830/AIP831 に置き換える場合は、使用しているオペレーションキーボードによって必要な作業が異なります。

重要

ソリッドスタイルコンソールタイプのオペレーションキーボード、オープンスタイルコンソールタイプの 8 ループオペレーションキーボードからは、AIP830/AIP831 への置き換えはできません。また、オープンスタイルコンソールタイプの 1 ループオペレーションキーボードからは、AIP830 への置き換えのみ可能です。

■ USB オペレーションキーボード (AIP827)から AIP830 に置き換える

AIP827 から AIP830 に置き換えるときには、必要な作業はありません。オペレーションキーボードの入れ替えだけ行ってください。

■ USB オペレーションキーボード (AIP827)から AIP831 に置き換える

オペレーションキーボードの入れ替えをしたあと、AIP831 用のライセンスを配布／反映してください。

参照

ライセンスの配布と反映については、以下を参照してください。

「B4.8 ライセンスの配布と反映をする」ページ B4-103

■ オープンスタイルコンソールの 1 ループオペレーションキーボードから AIP830 に置き換える

1. オペレーションキーボードの入れ替えをしてください。
2. オペレーションキーボード用 USB ドライバのインストールをしてください。
3. HIS ユーティリティの [操作] タブで、[オペレーションキーボードの設定] – [接続 シリアルポート] – [USB] を選択してください。

参照

オペレーションキーボード用 USB ドライバのインストールについては、以下を参照してください。

「B4.4 オペレーションキーボード用 USB ドライバのインストールをする」ページ B4-79

C6.7 制御バス用のカードを交換する

CENTUM VP では、制御バス用のカードとして、制御バスインターフェースカードまたは Vnet/IP インタフェースカードを使用します。これらのカードを交換する際には、ドライバのアンインストールと再インストールが必要になります。

■ 制御バス用のカードの交換手順

制御バス用のカードを交換するときは、次の手順に従ってください。

1. カードを実装したまま、ドライバをアンインストールしてください。

補足

制御バスドライバと Vnet/IP オープン通信ドライバが両方インストールされている場合は、どちらもアンインストールしてください。

2. コンピュータの電源を OFF にし、カードを交換してください。
3. コンピュータの電源を ON にして、新たに実装したカードに必要なドライバをインストールしてください。

参照

ドライバのアンインストール方法については、以下を参照してください。

「C7.1.4 デバイスドライバのアンインストールをする」ページ C7-13

ドライバのインストール方法については、以下を参照してください。

「B4.3 ネットワークの設定をする」ページ B4-43

C7. CENTUM VP ソフトウェアのアンインストールをする

ここでは、CENTUM VP ソフトウェアや各デバイスドライバのアンインストール方法について説明します。アンインストールの手順は、次の 2 つの場合に分けて説明します。

- ・ 主なステーションやコンピュータのアンインストール
- ・ ライセンス管理専用のコンピュータのアンインストール

ただし、CENTUM VP ソフトウェアをアンインストールしても、プロジェクトデータベース、ユーザ設定情報、レジストリなどは削除されません。コンピュータにある CENTUM VP ソフトウェアを完全に削除したい場合は、OS から再インストールする必要があります。

C7.1 主なステーションやコンピュータのアンインストールをする

ここでは、主なステーションやコンピュータのアンインストールをする手順を説明します。

該当するステーションやコンピュータの種類は次のとおりです。

- HIS
- APCS
- SIOS
- GSGW
- UGS
- UAACS ステーション
- システム生成機能のみを搭載したコンピュータ
- AD サーバのみを搭載したコンピュータ
- 仮想化プラットフォーム上の CENTUM VP 関連ステーションおよびコンピュータ

重要

ProSafe-RS と同一のコンピュータに CENTUM VP をインストールしている場合は、CENTUM VP をアンインストールしないでください。機能が不要な場合はライセンスを削除してください。

C7.1.1 CENTUM デスクトップ環境設定の解除をする

操作監視基本機能、FDA : 21 CFR Part11 対応パッケージまたはアクセス制限パッケージが有効化されている場合、CENTUM VP のソフトウェアをアンインストールする前にユーザ環境設定画面のユーザ登録を削除し、[HIS タイプシングルサインオンを有効にする] チェックボックスをオフにしてください。

■ 解除手順

1. 管理者ユーザでログオンしてください。
2. HIS ユーティリティを起動してください。
3. ユーザタブで、[設定] をクリックしてください。
ユーザ環境設定ダイアログが表示されます。

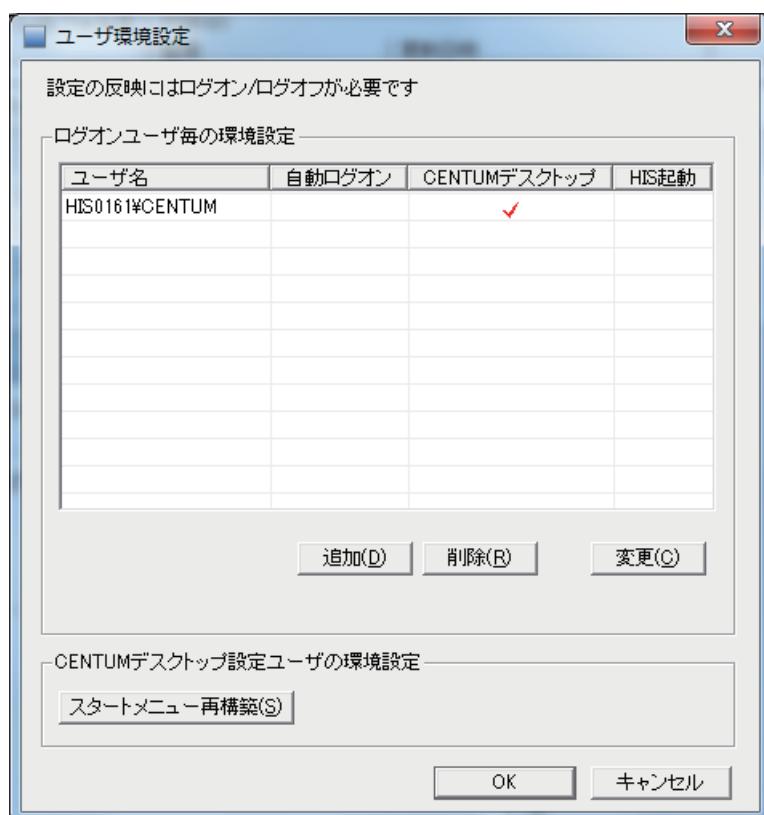


図 C7.1.1-1 ユーザ環境設定ダイアログ（ログオンユーザごとの環境設定）

4. ユーザを選択して [削除] をクリックしてください。
ユーザの削除ダイアログが表示されます。



図 C7.1.1-2 ユーザの削除ダイアログ

5. 選択したユーザのパスワードを入力して、[OK] をクリックしてください。
6. 4から5の手順を繰り返して、すべてのユーザを削除してください。

7. Windows 認証モードの場合、[HIS タイプシングルサインオンを有効にする] チェックボックスをオフにしてください。
8. [OK] をクリックして、ユーザ環境設定ダイアログと HIS ユーティリティダイアログを閉じてください。

C7.1.2 Windows の各種設定を復元する

CENTUM VP ソフトウェアをインストールしたときに、いくつかの Windows の設定を自動的に変更しています。CENTUM VP ソフトウェアのアンインストール時に、これらの Windows の設定を復元する方法について説明します。

重要

CENTUM VP 以外の当社製品（Prosafe-RS、PRM など）がインストールされていて、それらを引き続き使用する場合は、Windows 設定は復元しないでください。

■ ログオン時のアカウントアイコンを表示する

1. 管理者ユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [管理ツール] – [ローカルセキュリティポリシー] を選択してください。
ローカルセキュリティポリシーウィンドウが表示されます。
4. 左のペインの [ローカルポリシー] – [セキュリティオプション] を選択してください。
右のペインに [ポリシー] が表示されます。
5. [ポリシー] から [対話型ログオン：最後のユーザー名を表示しない] をダブルクリックしてください。
「対話型ログオン：最後のユーザー名を表示しないのプロパティ」ダイアログが表示されます。

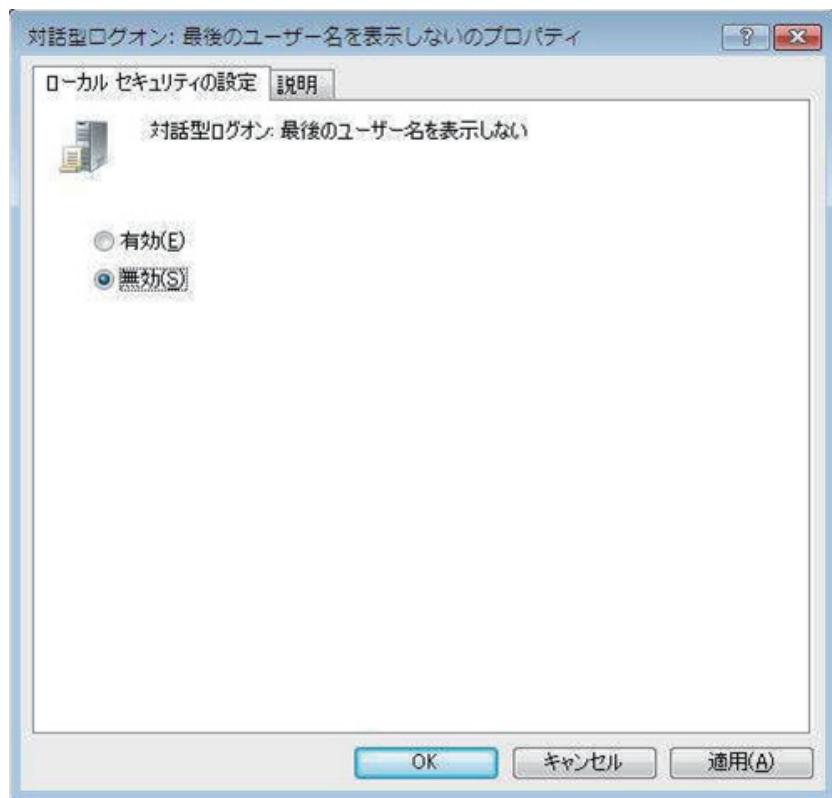


図 C7.1.2-1 対話型ログオン：最後のユーザー名を表示しないのプロパティ

6. [無効] を選択して、[OK] をクリックしてください。
7. コンピュータを再起動してください。

■ 簡易ユーザ切り替えを有効にする

1. 管理者ユーザでログオンしてください。
2. コマンドプロンプトを起動してください。
3. `gpedit.msc` と入力してください。
ローカルグループポリシーエディターが表示されます。
4. 左ペインで、[コンピュータの構成] – [管理用テンプレート] – [システム] – [ログオン] を選択して、[ユーザーの簡易切り替えのエントリポイントを非表示にする] をダブルクリックしてください。
「ユーザーの簡易切り替えのエントリポイントを非表示にする」のプロパティダイアログが表示されます。

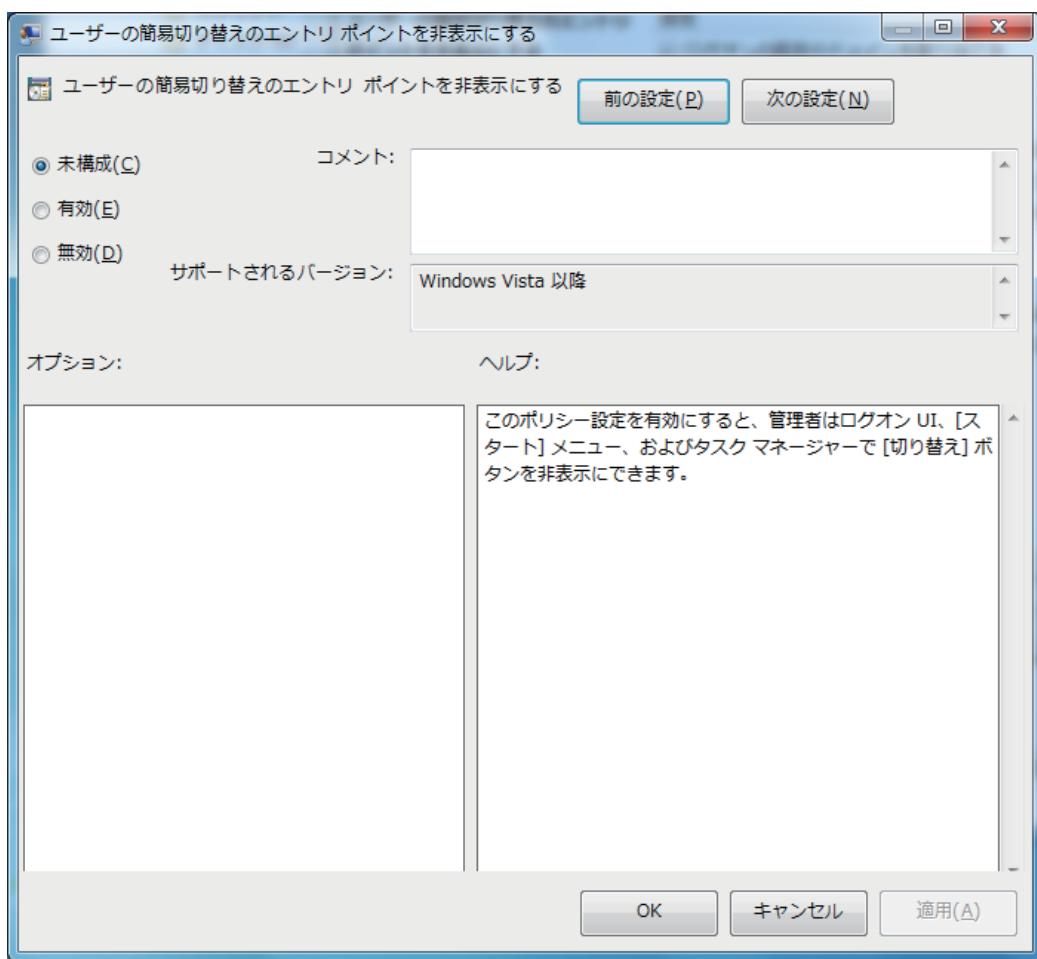


図 C7.1.2-2 ユーザーの簡易切り替えのエントリポイントを非表示にするのプロパティ

5. [無効] を選択して、[OK] をクリックしてください。
6. コンピュータを再起動してください。

■ Windows セキュリティセンターの警告表示を有効にする

Windows セキュリティセンターの警告表示を有効にする方法について説明します。
Windows セキュリティセンターの有効／無効はアカウントごとに設定します。

重要 Windows 10 では、警告表示が自動的に有効化されるので、本作業は不要です。

● Windows 7/Windows Server 2008 R2 の場合

1. アクションセンターの警告表示を有効にしたいユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. コントロールパネルの表示方法を小さいアイコンにしてください。
4. 表示される項目の中から、[通知領域アイコン] を選択してください。
通知領域アイコンダイアログが表示されます。

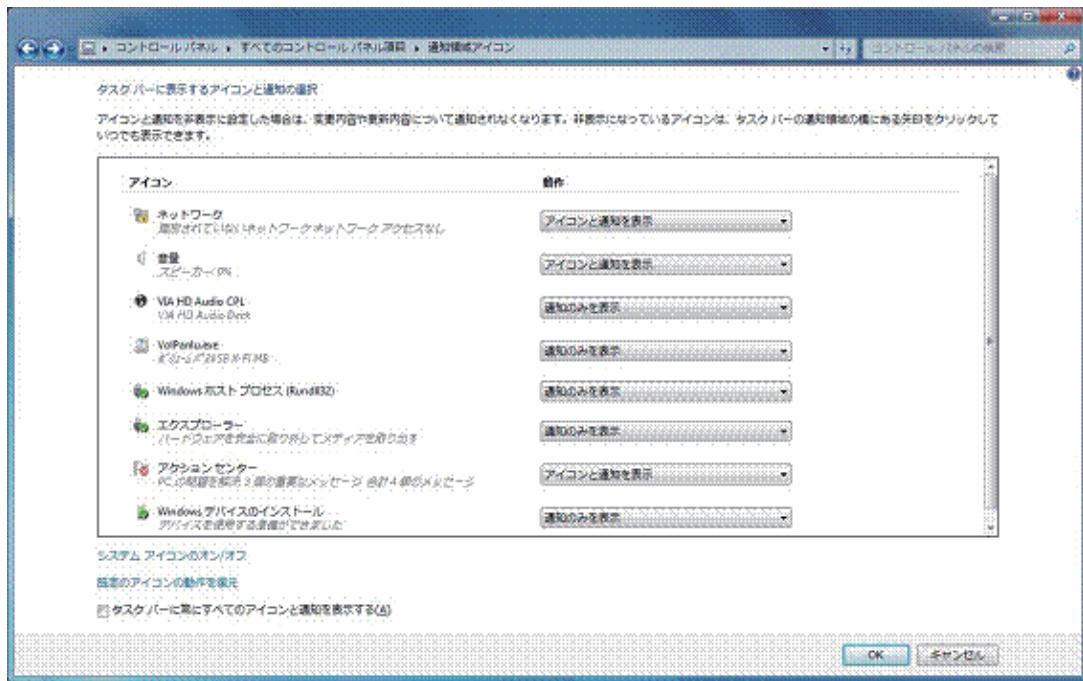


図 C7.1.2-3 通知領域アイコンダイアログ

5. [アクションセンター] の設定を [アイコンと通知を表示] としてください。

■ Windows Update を有効にする

Windows Update を有効にする方法を説明します。

● Windows 10 または Windows Server 2016 の場合

1. 管理者ユーザでサインインしてください。
2. コマンドプロンプトを起動してください。
3. `gpedit.msc` と入力してください。
ローカルグループポリシーエディターが表示されます。
4. 左ペインで、[コンピューターの構成] – [管理用テンプレート] – [Windows コンポーネント] – [Windows Update] を選択してください。
5. 右ペインで、[自動更新を構成する] をダブルクリックしてください。
自動更新を構成するダイアログが表示されます。
6. [有効] を選択して [OK] をクリックしてください。

● Windows 7 または Windows Server 2008 R2 の場合

1. 管理者ユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [Windows Update] を選択してください。
Windows Update ウィンドウが表示されます。

4. [設定の変更] をクリックしてください。
設定の変更ウィンドウが表示されます。

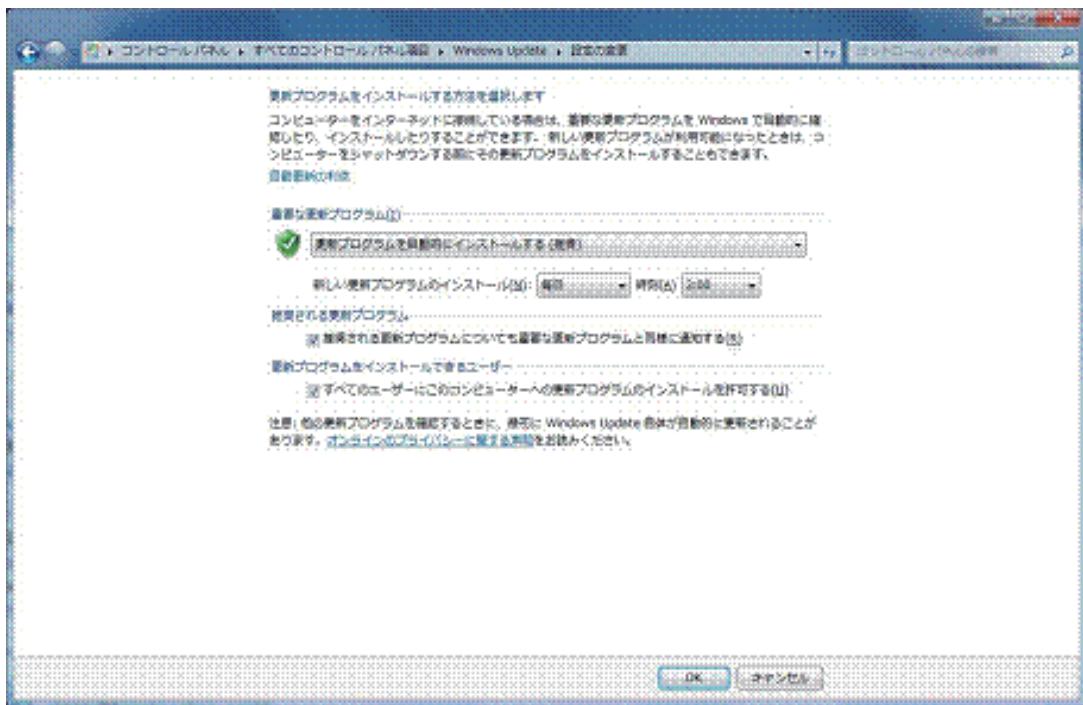


図 C7.1.2-4 設定の変更

5. [重要な更新プログラム] の設定を [更新プログラムを自動的にインストールする] を選択して、[OK] をクリックしてください。

■ Windows Defender を有効にする

Windows Defender は、Windows 10 および Windows 7 の標準プログラムで、スパイウェアなどの迷惑ソフトウェアやセキュリティ上の脅威からコンピュータを保護する目的で使用されます。

● Windows 10 または Windows Server 2016 の場合

1. 管理者ユーザでサインインしてください。
2. コマンドプロンプトを起動してください。
3. `gpedit.msc` と入力してください。
ローカルグループポリシーエディターが表示されます。
4. 左ペインで、[コンピューターの構成] – [管理用テンプレート] – [Windows コンポーネント] – [Endpoint Protection] を選択してください。

補足

Windows 10 IoT Enterprise 2016 LTSB では、[コンピューターの構成] – [管理用テンプレート] – [Windows コンポーネント] – [Windows Defender] を選択してください。

5. 右ペインで [Endpoint Protection を無効にする] をダブルクリックしてください。
Endpoint Protection を無効にするダイアログが表示されます。

補足

Windows 10 IoT Enterprise 2016 LTSB では、[Windows Defender を無効にする] をダブルクリックしてください。Windows Defender を無効にするダイアログが表示されます。

6. [未構成] を選択し、[OK] をクリックしてください。

● Windows 7 の場合

1. 管理者ユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. [表示方法] ドロップダウンリストで [大きいアイコン] か [小さいアイコン] を選択し、[Windows Defender] を選択してください。
このプログラムが無効となっていることを示すダイアログが表示されます。

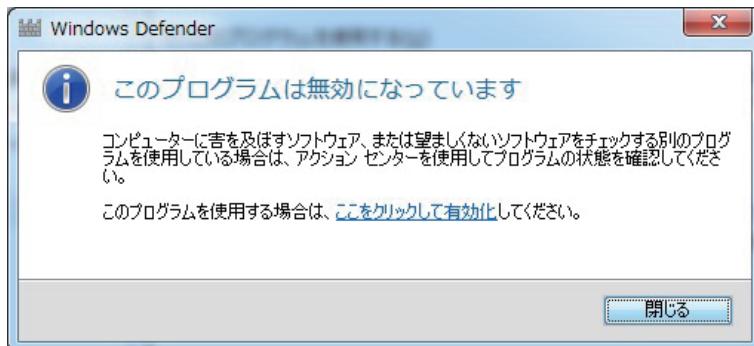


図 C7.1.2-5 Windows Defender

4. [ここをクリックして有効化してください] をクリックしてください。
Windows Defender が起動されます。
5. [×] をクリックして、Windows Defender ウィンドウを閉じてください。

C7.1.3 CENTUM VP ソフトウェアをアンインストールする

ここでは、CENTUM VP ソフトウェアをアンインストールする手順を説明します。

CENTUM VP ソフトウェアをアンインストールすると、ライセンス管理ソフトウェアもアンインストールされます。ただし、ライセンス管理データ、IT セキュリティツール、パッケージごとにカスタマイズした項目やプロジェクトデータなどは削除されません。

補足

IT セキュリティツールは、CENTUM VP だけではなく、当社の他の製品でも使用しています。そのため、CENTUM VP ソフトウェアをアンインストールしても、IT セキュリティツールのスタートメニュー、プログラム、およびファイルは削除されません。IT セキュリティツールをアンインストールするには、IT セキュリティツールを使用している製品を、すべてアンインストール後、IT セキュリティツールをアンインストールするコマンドを実行する必要があります。

■ ライセンスの削除と無効化の手順

コンピュータにライセンスが配布されている場合は、CENTUM VP ソフトウェアをアンインストールする前にライセンスを削除し、個々のパッケージを無効化する必要があります。

1. 管理者ユーザでログオンしてください。
2. 実行中のすべてのアプリケーションを終了してください。
3. 操作監視基本機能またはアクセス制限パッケージが有効化されていて、HIS 自動起動および自動ログオンが設定されている場合は、HIS ユーティリティで解除してください。
4. 有効化しているパッケージがあれば、ライセンスを削除することにより、それらを無効化してください。

参照

コンピュータのソフトウェアパッケージを無効化する方法については、以下を参照してください。

ライセンス管理 (IM 33J01C20-01JA) の「3.2.1 ライセンス割り付けの変更」の「■ ライセンス適用ステーションからライセンスを削除する」

■ アンインストール手順

CENTUM VP ソフトウェアのアンインストールは、パッケージを無効化（ライセンスの削除）をしたあと、次の手順に従ってください。

1. コントロールパネルを起動してください。
2. [プログラム] – [プログラムと機能] を選択してください。
プログラムと機能ウィンドウが表示されます。

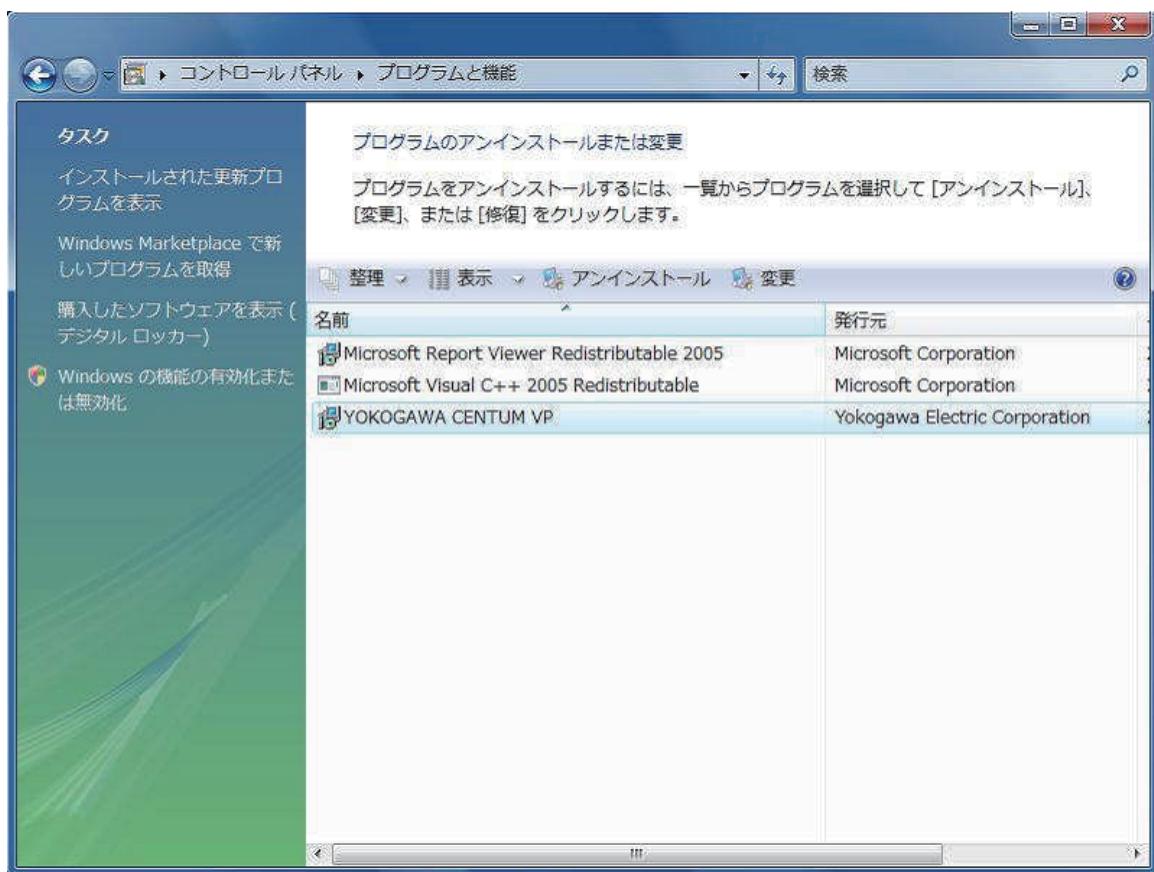


図 C7.1.3-1 プログラムと機能ウィンドウ

3. [YOKOGAWA CENTUM VP] を選択し、[変更] をクリックしてください。
ようこそダイアログが表示されます。
4. [次へ] をクリックしてください。
削除の確認ダイアログが表示されます。
5. [削除] をクリックしてください。
アンインストールが開始し、アンインストールの進捗状況を示すダイアログが表示されます。

補足

有効なライセンスが存在している場合は、アンインストールの続行を確認するダイアログが表示されます。[はい] を選択してアンインストールを続行してください。この時点で、ライセンスの無効化が行われます。ただし、ライセンス管理ステーションには、ライセンス情報はそのままの形で残ります。必要に応じて、ライセンス管理ステーションのライセンス情報を変更してください。

6. ユーザーアカウント制御ダイアログが表示されたら、[はい] または [許可] をクリックしてください。

補足

[はい] または [許可] をクリックせずにそのまま放置すると、ユーザーアカウント制御ダイアログが自動で閉じます。その後にアンインストール失敗のダイアログが表示され、アンインストールが中断されます。その場合は、再度アンインストールをしてください。

7. アンインストールが完了すると、アンインストール完了ダイアログが表示されるので、次のいずれかの操作をしてください。
 - すぐに再起動する場合は、[今すぐ再起動] を選択し、[終了] をクリックしてください。

- あとで再起動する場合は、[後で再起動] を選択し、[終了] をクリックしてください。

■ IT セキュリティツールのアンインストール手順

CENTUM VP ソフトウェアをアンインストールしても、IT セキュリティツールは削除されません。

IT セキュリティツールをアンインストールするには、次の手順に従ってください。

重要

次の当社製品がインストールされている場合、IT セキュリティツールは削除しないでください。

- PRM : R3.10 以降
- ProSafe-RS : R3.01 以降
- Exaopc : R3.70 以降
- Exapilot : R3.90 以降
- Exaplog : R3.40 以降

- 管理者ユーザでログオンしてください。
- CENTUM VP のソフトウェアメディアをドライブに挿入してください。
- 次のファイルを [管理者として実行] で起動してください。

<CENTUM VP ソフトウェアメディアドライブ>:\CENTUM\¥Security\DeleteITSecurity.cmd

C7.1.4 デバイスドライバのアンインストールをする

ここでは、デバイスドライバのアンインストール方法を説明します。

■ 制御バスドライバのアンインストール時の注意事項

制御バスドライバをアンインストールする前に、必ず制御バスドライバを無効にしてください。

制御バスドライバを無効化するには、次の手順に従ってください。

1. 管理者ユーザでサインインしてください。
2. コントロールパネルを起動してください。
3. [ネットワークとインターネット] – [ネットワークと共有センター] を選択してください。
ネットワークと共有センターウィンドウが表示されます。
4. [アダプターの設定の変更] を選択してください。
ネットワーク接続ウィンドウが表示されます。
5. [Yokogawa Vnet Adapter] を右クリックし、[無効にする] を選択してください。
接続の無効エラーダイアログが表示されます。
6. [OK] をクリックしてください。
7. コンピュータを再起動してください。
8. 手順 1 から 4 を実施してください。
9. ネットワーク接続ウィンドウで、制御バスドライバが無効化されていることを確認してください。

補足

制御バスドライバが無効化されていない場合は、再度、手順 2 から実施してください。

■ 制御バスドライバのアンインストール

制御バスドライバのアンインストールは、次の手順に従ってください。

1. 管理者ユーザでログオンしてください。
2. 実行中のすべてのアプリケーションを終了してください。
3. CENTUM VP のソフトウェアメディアをドライブに挿入してください。
 - ・ 自動再生ダイアログが表示された場合、[Launcher.exe の実行] をクリックしてください。
 - ・ 自動再生ダイアログが表示されない場合、エクスプローラでソフトウェアメディアのトップフォルダにある Launcher.exe をダブルクリックしてください。インストールメニューが表示されます。
4. [制御バスドライバ] をクリックしてください。
次のダイアログが表示されます。



図 C7.1.4-1 Setup 内容選択ダイアログ

5. [UNINSTALL] を選択して [OK] をクリックしてください。
アンインストールの実行を確認するダイアログが表示されます。
6. [OK] をクリックしてください。
アンインストールが始まります。
7. アンインストールが終了すると、アンインストール完了を知らせるダイアログが表示されるので、[OK] をクリックしてください。
8. コンピュータを再起動してください。

重要

ドライバのアンインストール後には、TCP/IP 設定不整合検出ツールを実行してください。不整合が検出された場合は、TCP/IP 設定不整合修復ツールを使用したあと、TCP/IP を再設定してください。

参照

TCP/IP 設定不整合検出ツールと TCP/IP 設定不整合修復ツールについては、以下を参照してください。

「■ 手順 6：TCP/IP 設定を修復する」ページ B4-70

■ Vnet/IP オープン通信ドライバのアンインストール

Vnet/IP オープン通信ドライバのアンインストールは、次の手順に従ってください。

1. 管理者ユーザでログオンしてください。
2. 実行中のすべてのアプリケーションを終了してください。
3. CENTUM VP のソフトウェアメディアをドライブに挿入してください。
 - ・ 自動再生ダイアログが表示された場合、[Launcher.exe の実行] をクリックしてください。
 - ・ 自動再生ダイアログが表示されない場合、エクスプローラでソフトウェアメディアのトップフォルダにある Launcher.exe をダブルクリックしてください。
 インストールメニューが表示されます。
4. [Vnet/IP オープン通信ドライバ] をクリックしてください。
次のダイアログが表示されます。



図 C7.1.4-2 Setup 内容選択ダイアログ

5. [UNINSTALL] を選択して [OK] をクリックしてください。
アンインストールの実行を確認するダイアログが表示されます。
6. [OK] をクリックしてください。
アンインストールが始まります。
7. アンインストールが終了すると、アンインストール完了を知らせるダイアログが表示されるので、[OK] をクリックしてください。
8. コンピュータを再起動してください。

重要

ドライバのアンインストール後には、TCP/IP 設定不整合検出ツールを実行してください。不整合が検出された場合は、TCP/IP 設定不整合修復ツールを使用したあと、TCP/IP を再設定してください。

参照

TCP/IP 設定不整合検出ツールと TCP/IP 設定不整合修復ツールについては、以下を参照してください。

「■ 手順 6：TCP/IP 設定を修復する」ページ B4-70

■ 仮想マシンの Vnet/IP インタフェースパッケージをアンインストールする

Vnet/IP インタフェースパッケージをアンインストールするときは、次の手順に従ってください。

補足

Vnet/IP ステーションと異なり、仮想マシンの場合、Vnet/IP インタフェースパッケージをアンインストールすると、その仮想マシンはすぐにステーション Fail になります。

● 手順 1：Vnet/IP インタフェースパッケージをアンインストールする

Vnet/IP インタフェースパッケージをアンインストールするときは、次の手順に従ってください。

1. 仮想マシンのゲスト OS に、管理者ユーザでサインインしてください。
2. 実行中のすべてのアプリケーションを終了してください。
3. 仮想マシンのゲスト OS からサインアウトしてください。
4. 仮想化ホストコンピュータのホスト OS に、管理者ユーザでサインインしてください。
5. CENTUM VP ソフトウェアメディアの ISO 形式ファイルを、仮想化ホストコンピュータのホスト OS 内の任意のフォルダにコピーしてください。
6. スタートメニューから、[サーバーマネージャー] を選択してください。

サーバーマネージャーが起動します。

7. サーバーマネージャーのメニューバーから、[ツール] – [Hyper-V マネージャー] を選択してください。

Hyper-V マネージャーが起動します。

8. Hyper-V マネージャーの左ペインで仮想化ホストコンピュータを選択してください。中央ペインに選択した仮想化ホストコンピュータ上の仮想マシンが表示されます。該当の仮想マシンを選択し、右クリックメニューで [接続] をクリックしてください。仮想マシン接続ウィンドウが表示されます。

補足

仮想マシン接続ウィンドウが全画面表示される場合があります。全画面表示されたときは、[元に戻す] をクリックして、全画面表示を解除してください。

9. 仮想マシン接続ウィンドウのメニューバーから、[メディア] – [DVD ドライブ] – [ディスクの挿入] を選択してください。

ファイルを開くダイアログが表示されます。

10. コピーした CENTUM VP ソフトウェアメディアの ISO 形式ファイルを指定してください。

選択した ISO 形式ファイルが仮想マシンにマウントされます。

- 自動再生ダイアログが表示された場合、[Launcher.exe の実行] をクリックしてください。
- 自動再生ダイアログが表示されない場合、エクスプローラで CENTUM VP のソフトウェアの ISO 形式ファイルが格納されているフォルダ下にある Launcher.exe をダブルクリックしてください。

インストールメニューが表示されます。

11. インストールメニューの [制御バスドライバ] をクリックしてください。

Setup の内容を選択するダイアログが表示されます。

12. [UNINSTALL] を選択して [OK] をクリックしてください。

アンインストールの実行を確認するダイアログが表示されます。

13. [OK] をクリックしてください。

アンインストールが始まります。

14. アンインストールが終了すると、アンインストール完了を知らせるダイアログが表示されるので、[OK] をクリックしてください。

15. 仮想マシンを再起動してください。

重要

ドライバのアンインストール後には、TCP/IP 設定不整合検出ツールを実行してください。不整合が検出された場合は、TCP/IP 設定不整合修復ツールを使用したあと、TCP/IP を再設定してください。

参照

TCP/IP 設定不整合検出ツールと TCP/IP 設定不整合修復ツールについては、以下を参照してください。

「■ 手順 6：TCP/IP 設定を修復する」ページ B4-70

● 手順 2：RIP Listener サービスを無効化する

RIP Listener サービスを無効化する手順について説明します。

重要

DCOM の [既定の認証レベル] が [なし] となっている場合に、RIP Listener サービスの無効化に失敗する場合があります。その場合は回避手順を実行してください。

Windows Server 2016 で RIP Listener サービスを無効化するときは、次の手順に従ってください。

1. 仮想マシンのゲスト OS に、管理者ユーザでサインインしてください。
2. スタートメニューから、[Windows システムツール] を選択してください。
Windows システムツールの一覧が表示されます。
3. [コマンドプロンプト] を右クリックし、[管理者として実行] を選択してください。
4. 次のコマンドを実行してください。

```
dism /online /disable-feature /featurename:rasrip
```
5. [操作は正常に完了しました。] と表示されることを確認してください。

参照

RIP Listener サービスの無効化に失敗するときの回避手順については、以下を参照してください。

「■ RIP Listener サービスの無効化に失敗する」ページ C10-22

■ OPKB 用 USB ドライバのアンインストール

オペレーションキーボード用ドライバのアンインストールは、次の手順に従ってください。

1. 管理者ユーザでログオンしてください。
2. 実行中のすべてのアプリケーションを終了してください。
3. オペレーションキーボードが USB ポートに接続され、オペレーションキーボードの電源が入っていることを確認してください。
4. CENTUM VP のソフトウェアメディアをドライブに挿入してください。
 - ・ 自動再生ダイアログが表示された場合、[Launcher.exe の実行] をクリックしてください。
 - ・ 自動再生ダイアログが表示されない場合、エクスプローラでソフトウェアメディアのトップフォルダにある Launcher.exe をダブルクリックしてください。
 インストールメニューが表示されます。
5. [オペレーションキーボード用ドライバ] をクリックしてください。
次のダイアログが表示されます。



図 C7.1.4-3 Setup 内容選択ダイアログ

6. [UNINSTALL] を選択して [OK] をクリックしてください。
アンインストールの実行を確認するダイアログが表示されます。
7. [OK] をクリックしてください。
アンインストールが始まります。

8. アンインストールが終了すると、アンインストール完了を知らせるダイアログが表示されるので、[OK] をクリックしてください。
9. コンピュータを再起動してください。

■ RS-232C ドライバのアンインストール

RS-232C ドライバのアンインストールは、次の手順に従ってください。

1. 管理者ユーザでログオンしてください。
2. 実行中のすべてのアプリケーションを終了してください。
3. CENTUM VP のソフトウェアメディアをドライブに挿入してください。
 - ・ 自動再生ダイアログが表示された場合、[Launcher.exe の実行] をクリックしてください。
 - ・ 自動再生ダイアログが表示されない場合、エクスプローラでソフトウェアメディアのトップフォルダにある Launcher.exe をダブルクリックしてください。インストールメニューが表示されます。
4. [コンソール HIS 用 RS ドライバ] をクリックしてください。
PC インターフェースを選択するダイアログが表示されます。
5. アンインストールするドライバの PC インターフェースを選択して、[インストール] をクリックしてください。
Setup 内容を確認するダイアログが表示されます。



図 C7.1.4-4 Setup 内容確認ダイアログ

6. [UNINSTALL] を選択して [OK] をクリックしてください。
アンインストールを確認するダイアログが表示されます。
7. [OK] をクリックしてください。
ドライバ削除が終了すると、アンインストール終了を知らせるダイアログが表示されます。
8. [OK] をクリックして、終了させてください。

■ RAS ドライバのアンインストール

RAS ドライバのアンインストールは、次の手順に従ってください。

1. 管理者ユーザでログオンしてください。
2. 実行中のすべてのアプリケーションを終了してください。
3. CENTUM VP のソフトウェアメディアをドライブに挿入してください。
 - ・ 自動再生ダイアログが表示された場合、[Launcher.exe の実行] をクリックしてください。

- 自動再生ダイアログが表示されない場合、エクスプローラでソフトウェアメディアのトップフォルダにある Launcher.exe をダブルクリックしてください。インストールメニューが表示されます。
4. [コンソール HIS 用 RAS ドライバ] をクリックしてください。
コンソールタイプと PC インタフェース選択のダイアログが表示されます。
5. アンインストールするドライバの PC インタフェースを選択して、[インストール] をクリックしてください。
Setup 内容を確認するダイアログが表示されます。



図 C7.1.4-5 Setup 内容選択ダイアログ

6. [UNINSTALL] を選択して [OK] をクリックしてください。
アンインストールを確認するダイアログが表示されます。
7. [OK] をクリックしてください。
ドライバ削除が終了すると、アンインストール終了を知らせるダイアログが表示されます。
8. [OK] をクリックしてください。
9. コンピュータを再起動してください。

C7.2 ライセンス管理専用のコンピュータのアンインストールをする

ここでは、ライセンス管理専用のコンピュータからライセンス管理ソフトウェアをアンインストールするための手順を説明します。

■ アンインストールの実行

ライセンス管理ソフトウェアのアンインストールは、次の手順に従ってください。

1. 管理者ユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. [プログラム] – [プログラムと機能] を選択してください。
プログラムと機能ウィンドウが表示されます。
4. プログラムのリストから [YOKOGAWA CENTUM VP] を選択し、[変更] をクリックしてください。
ようこそダイアログが表示されます。
5. [次へ] をクリックしてください。
削除の確認ダイアログが表示されます。
6. [削除] をクリックしてください。
アンインストールが開始され、アンインストールの進捗状況ダイアログが表示されます。
7. アンインストールが完了すると、アンインストール完了ダイアログが表示されるので、次のいずれかの操作をしてください。
 - ・ すぐに再起動する場合は、[今すぐ再起動] を選択し、[終了] をクリックしてください。
 - ・ あとで再起動する場合は、[後で再起動] を選択し、[終了] をクリックしてください。

C8. CENTUM VP ソフトウェアの再インストールをする

ここでは、CENTUM VP ソフトウェアの再インストールについて説明します。再インストールの方式には、使用するコンピュータを変更しない場合と、変更する場合があります。また、それぞれは、ライセンス適用ステーションとライセンス管理ステーションの再インストールに分かれます。

C8.1 使用するコンピュータを変更しない場合

CENTUM VP ソフトウェアとしてインストールされたファイルの破損や、誤ってファイルが削除されたような場合に、修復などの目的で再度インストールするための手順です。使用するコンピュータは変更しないという条件です。

上書きでの再インストールはできませんので、いったん CENTUM VP ソフトウェアをアンインストールして、もう一度 CENTUM VP ソフトウェアをインストールします。

■ ライセンス適用ステーションの再インストール

ここでは、ライセンス適用ステーションの再インストール手順について説明します。
ライセンス適用ステーションの再インストールの流れは、次のとおりです。

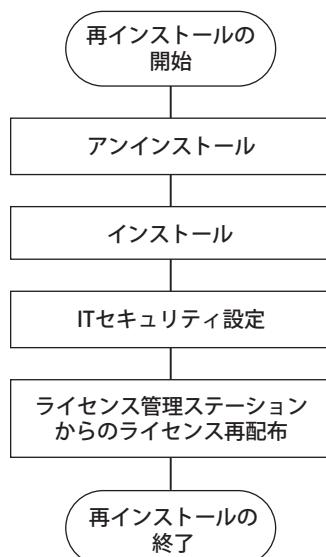


図 C8.1-1 ライセンス適用ステーションの再インストールの流れ

● CENTUM VP ソフトウェアのアンインストール

CENTUM VP ソフトウェアをアンインストールしてください。

参照

アンインストール手順については、以下を参照してください。

「C7.1.3 CENTUM VP ソフトウェアをアンインストールする」ページ C7-10

● CENTUM VP ソフトウェアのインストール

CENTUM VP ソフトウェアをインストールしてください。

参照

CENTUM VP ソフトウェアのインストール手順については、以下を参照してください。

「B4.6 CENTUM VP ソフトウェアのインストールをする」ページ B4-87

● IT セキュリティ設定

IT セキュリティ設定は、CENTUM VP ソフトウェアの新規インストールのときと同じです。

参照

セキュリティ設定については、以下を参照してください。

「B4.7 IT セキュリティを設定する」ページ B4-96

● ライセンス管理ステーションからのライセンスの再配布

ライセンス管理ステーションからライセンスの再配布をしてください。

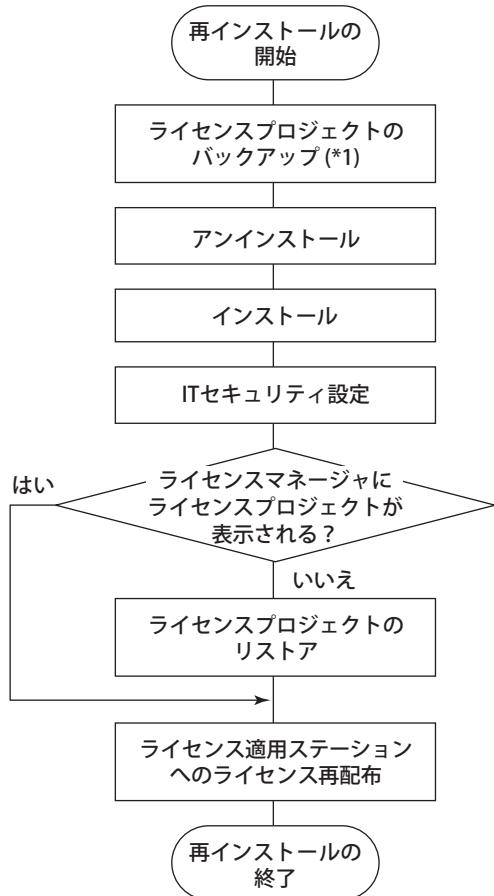
参照

ライセンス管理ステーションからのライセンスの再配布については、以下を参照してください。

ライセンス管理 (IM 33J01C20-01JA) の「3.4 ライセンス適用ステーションへのライセンス再配布」

■ ライセンス管理ステーションの再インストール

ここでは、ライセンス管理ステーションの再インストール手順について説明します。ライセンス管理ステーションには、CENTUM VP ソフトウェアをインストールしたコンピュータとライセンス管理専用のコンピュータがあります。ライセンス管理ステーションの種類に応じて、再インストール作業をしてください。



*1: ライセンスプロジェクトのバックアップがすでにある場合は、ここで作業は必要ありません。

図 C8.1-2 ライセンス管理ステーションの再インストールの流れ

● ライセンスプロジェクトのバックアップ

そのコンピュータで管理しているライセンスプロジェクトをバックアップしてください。

参照

ライセンスプロジェクトのバックアップの手順については、以下を参照してください。

ライセンス管理 (IM 33J01C20-01JA) の「3.6 ライセンスプロジェクトのバックアップとリストア」

● CENTUM VP ソフトウェアのアンインストール

CENTUM VP ソフトウェアをアンインストールしてください。ライセンス管理専用のコンピュータでは、ライセンス管理ソフトウェアをアンインストールしてください。

参照

CENTUM VP ソフトウェアをインストールしている場合のアンインストール手順については、以下を参照してください。

「C7. CENTUM VP ソフトウェアのアンインストールをする」ページ C7-1

ライセンス管理専用のコンピュータのアンインストール手順については、以下を参照してください。

「C7.2 ライセンス管理専用のコンピュータのアンインストールをする」ページ C7-20

● CENTUM VP ソフトウェアのインストール

CENTUM VP ソフトウェアをインストールしてください。ライセンス管理専用のコンピュータでは、ライセンス管理ソフトウェアをインストールしてください。

参照

ライセンス管理ソフトウェアのインストール手順については、以下を参照してください。

「B7. ライセンス管理専用のコンピュータのセットアップをする」ページ B7-1

● IT セキュリティ設定

IT セキュリティ設定は、CENTUM VP ソフトウェアの新規インストールのときと同じです。

参照

セキュリティ設定については、以下を参照してください。

「B4.7 IT セキュリティを設定する」ページ B4-96

● ライセンスプロジェクトのリストア

ライセンスマネージャを起動し、ライセンスプロジェクトが表示されるか確認してください。表示されない場合は、バックアップしたライセンスプロジェクトをリストアしてください。

参照

ライセンスプロジェクトのリストア手順については、以下を参照してください。

ライセンス管理 (IM 33J01C20-01JA) の「3.6 ライセンスプロジェクトのバックアップとリストア」の「■ ライセンスプロジェクトを別のライセンス管理ステーションにリストアする」

● ライセンス適用ステーションへのライセンスの再配布

ライセンス適用ステーションへのライセンスの再配布をしてください。

参照

ライセンス適用ステーションへのライセンスの再配布については、以下を参照してください。

ライセンス管理 (IM 33J01C20-01JA) の「3.4 ライセンス適用ステーションへのライセンス再配布」

C8.2 使用するコンピュータを変更する場合

CENTUM VP ソフトウェアをインストールしたコンピュータが故障した場合など、コンピュータを変更して再インストールするための手順です。

補足

ヒストリカルメッセージ統合パッケージで統合管理されている HIS であれば、変更後のコンピュータをヒストリカルメッセージ統合サーバに接続する前に、ヒストリカルファイルのシーケンス番号を継続させるための作業が必要です。

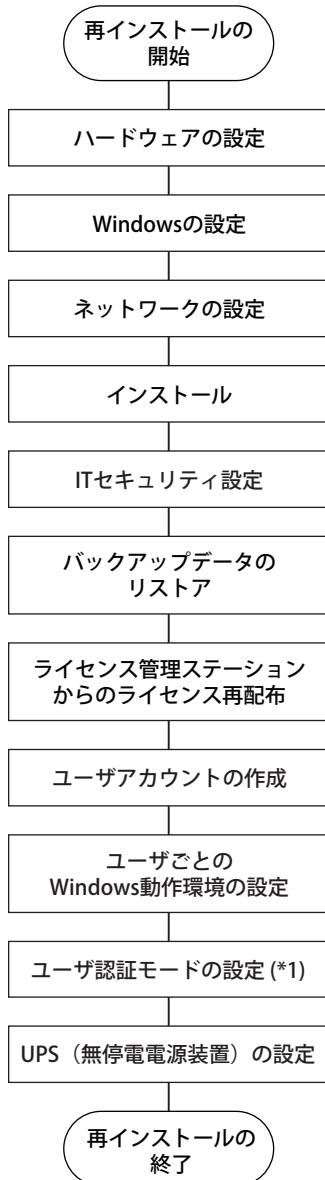
参照

ヒストリカルファイルのシーケンス番号継続については、以下を参照してください。

「● ヒストリカルメッセージ統合パッケージ」ページ C6-9

■ ライセンス適用ステーションの再インストール

ここでは、ライセンス適用ステーションの再インストール手順について説明します。
ライセンス適用ステーションの再インストールの流れは、次のとおりです。



*1: プロジェクトデータがリストアされていれば、この設定は不要です。

図 C8.2-1 ライセンス適用ステーションの再インストールの流れ

重要

新しいコンピュータのステーション名は、変更前のコンピュータで登録していたステーション名と同じ名前を登録してください。

● ハードウェアの設定

ハードウェアの設定をしてください。

参照

ハードウェアの設定については、以下を参照してください。

「B4.1 ハードウェアの設定をする」ページ B4-2

● Windows の設定

新しいコンピュータの Windows の設定をしてください。

参照

Windows の設定については、以下を参照してください。

「B4.2 Windows の設定をする」ページ B4-7

● ネットワークの設定

新しいコンピュータのネットワークの設定をしてください。

参照

ネットワークの設定については、以下を参照してください。

「B4.3 ネットワークの設定をする」ページ B4-43

● CENTUM VP ソフトウェアのインストール

CENTUM VP ソフトウェアを新しいコンピュータにインストールしてください。

参照

CENTUM VP ソフトウェアのインストール手順については、以下を参照してください。

「B4.6 CENTUM VP ソフトウェアのインストールをする」ページ B4-87

● IT セキュリティ設定

IT セキュリティ設定は、CENTUM VP ソフトウェアの新規インストールのときと同じです。

参照

セキュリティ設定については、以下を参照してください。

「B4.7 IT セキュリティを設定する」ページ B4-96

● バックアップデータのリストア

バックアップしておいたデータを、リストアしてください。

参照

バックアップデータについては、以下を参照してください。

「C5. バックアップをとる」ページ C5-1

● ライセンス管理ステーションからのライセンスの再配布

ライセンス管理ステーションからライセンスの再配布をしてください。

参照

ライセンス管理ステーションからのライセンスの再配布については、以下を参照してください。

ライセンス管理 (IM 33J01C20-01JA) の「3.4 ライセンス適用ステーションへのライセンス再配布」

● ユーザアカウントの作成

ユーザアカウントの作成をしてください。

参照

ユーザアカウントの作成については、以下を参照してください。

「B4.9 ユーザアカウントを作成する」ページ B4-104

● ユーザごとの Windows 動作環境の設定

ユーザごとの Windows 動作環境の設定をしてください。

参照

ユーザごとの Windows 動作環境の設定については、以下を参照してください。

「B4.10 ユーザごとの Windows 動作環境の設定をする」ページ B4-109

● ユーザ認証モードの設定

ユーザ認証モードの設定をしてください。
プロジェクトデータがリストアされていれば、この設定は不要です。

参照

ユーザ認証モードの設定については、以下を参照してください。

「B4.11 ユーザ認証モードの設定をする」ページ B4-136

● UPS(無停電電源装置) の設定

UPS(無停電電源装置) の設定をしてください。

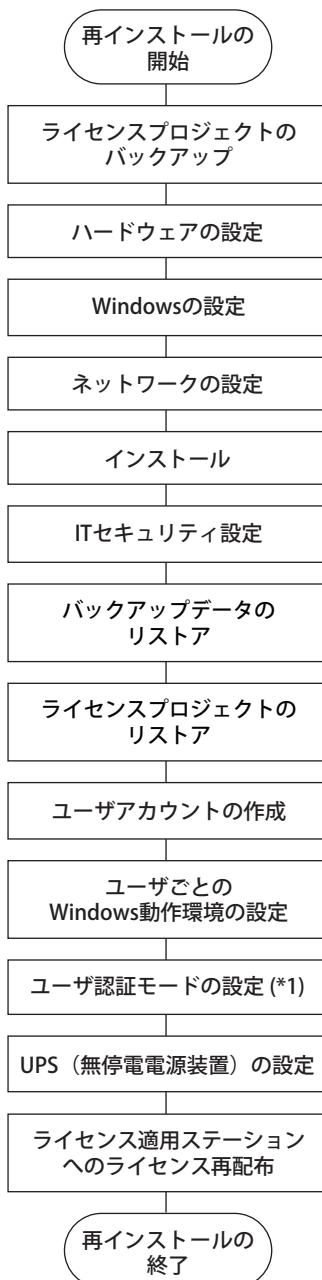
参照

UPS(無停電電源装置) の設定については、以下を参照してください。

「B4.12 UPS (無停電電源装置) の設定をする」ページ B4-149

■ ライセンス管理ステーションの再インストール

ライセンス管理ステーションには、CENTUM VP ソフトウェアをインストールしたコンピュータとライセンス管理専用のコンピュータがあります。ライセンス管理ステーションのタイプに応じて、再インストール作業を行ってください。



*1: プロジェクトデータがリストアされていれば、この設定は不要です。

図 C8.2-2 ライセンス管理ステーションの再インストールの流れ

重要

新しいコンピュータのステーション名は、変更前のコンピュータで登録していたステーション名と同じ名前を登録してください。

● ライセンスプロジェクトのバックアップ

変更前のコンピュータで管理しているライセンスプロジェクトをバックアップしてください。

参照

ライセンスプロジェクトのバックアップの手順については、以下を参照してください。

ライセンス管理（IM 33J01C20-01JA）の「3.6 ライセンスプロジェクトのバックアップとリストア」

● ハードウェアの設定

ハードウェアの設定をしてください。

参照

ハードウェアの設定については、以下を参照してください。

「B4.1 ハードウェアの設定をする」ページ B4-2

● Windows の設定

新しいコンピュータの Windows の設定をしてください。

参照

Windows の設定については、以下を参照してください。

「B4.2 Windows の設定をする」ページ B4-7

● ネットワークの設定

新しいコンピュータのネットワークの設定をしてください。

参照

ネットワークの設定については、以下を参照してください。

「B4.3 ネットワークの設定をする」ページ B4-43

● CENTUM VP ソフトウェアのインストール

CENTUM VP ソフトウェアを新しいコンピュータにインストールしてください。ライセンス管理専用のコンピュータでは、ライセンス管理ソフトウェアをインストールしてください。

参照

ライセンス管理ソフトウェアのみのインストール手順については、以下を参照してください。

「B7. ライセンス管理専用のコンピュータのセットアップをする」ページ B7-1

● IT セキュリティ設定

IT セキュリティ設定は、CENTUM VP ソフトウェアの新規インストールのときと同じです。

参照

セキュリティ設定については、以下を参照してください。

「B4.7 IT セキュリティを設定する」ページ B4-96

● バックアップデータのリストア

バックアップしておいたデータを、リストアしてください。

参照

バックアップデータについては、以下を参照してください。

「C5. バックアップをとる」ページ C5-1

● ライセンスプロジェクトのリストア

バックアップしてあるライセンスプロジェクトをリストアしてください。

参照

ライセンスプロジェクトのリストア手順については、以下を参照してください。

ライセンス管理 (IM 33J01C20-01JA) の「3.6 ライセンスプロジェクトのバックアップとリストア」の「■ ライセンスプロジェクトを別のライセンス管理ステーションにリストアする」

● ユーザアカウントの作成

ユーザアカウントの作成をしてください。

参照

ユーザアカウントの作成については、以下を参照してください。

「B4.9 ユーザアカウントを作成する」ページ B4-104

● ユーザごとの Windows 動作環境の設定

ユーザごとの Windows 動作環境の設定をしてください。

参照

ユーザごとの Windows 動作環境の設定については、以下を参照してください。

「B4.10 ユーザごとの Windows 動作環境の設定をする」ページ B4-109

● ユーザ認証モードの設定

ユーザ認証モードの設定をしてください。

プロジェクトデータがリストアされていれば、この設定は不要です。

参照

ユーザ認証モードの設定については、以下を参照してください。

「B4.11 ユーザ認証モードの設定をする」ページ B4-136

● UPS(無停電電源装置) の設定

UPS(無停電電源装置) の設定をしてください。

参照

UPS(無停電電源装置) の設定については、以下を参照してください。

「B4.12 UPS (無停電電源装置) の設定をする」ページ B4-149

● ライセンス適用ステーションへのライセンスの再配布

ライセンス適用ステーションへのライセンスの再配布をしてください。

参照

ライセンス適用ステーションへのライセンスの再配布については、以下を参照してください。

ライセンス管理 (IM 33J01C20-01JA) の「3.4 ライセンス適用ステーションへのライセンス再配布」

Blank Page

C9. IT セキュリティ設定で注意すべきケース

ここでは、IT セキュリティ設定をするにあたって、注意すべきケースの説明をします。

C9.1 CENTUM VP 標準モデルの VP プロジェクトに CENTUM CS 3000 R3 HIS を混在させる

CENTUM VP 標準モデルの VP プロジェクトに CENTUM CS 3000 R3 HIS を混在させるときの手順を説明します。

重要

- すべての HIS のユーザ認証モードを CENTUM 認証モードで統一してください。
- CENTUM CS 3000 R3 HIS に次のパッケージがインストールされているときは、CENTUM VP と混在をさせることができません。CENTUM CS 3000 R3 HIS を CENTUM VP にバージョンアップしてください。

LHS5100/LHM5100	: ビルダ基本機能
LHS5160	: CS Batch 3000 (バッチ管理パッケージ)
LHS5425	: 拡張テスト機能パッケージ
LHS5426	: FCS シミュレータパッケージ
LHS5427	: HIS シミュレータパッケージ
- このような構成の場合は、システム全体を CENTUM VP 標準モデルで統一した場合よりセキュリティ対策の効果が低下します。この構成を一時的なものととらえ、計画的に CENTUM VP 標準モデルに統一することを推奨します。

■ CENTUM CS 3000 R3 HIS から CENTUM VP を参照する

CENTUM CS 3000 R3 HIS から CENTUM VP の各種データを参照するために、CENTUM VP のコンピュータに CENTUM アカウントを作成してください。

● スタンドアロン管理

CENTUM VP のユーザ管理方法がスタンドアロン管理の場合、次の手順に従ってください。

- CENTUM VP のコンピュータで、CTM_OPC グループと CTM_OPERATOR グループに所属する CENTUM アカウントを作成してください。
ただし、次のコンピュータでは、CTM_OPC グループと CTM_ENGINEER グループに所属する CENTUM アカウントを作成してください。
 - 処方エンジニア登録ファイルがあるコンピュータ
 - 処方機能の履歴管理データベースがあるコンピュータ
- CENTUM CS 3000 R3 HIS と CENTUM VP で CENTUM アカウントのパスワードを一致させてください。

● ドメイン管理

CENTUM VP のユーザ管理方法がドメイン管理の場合は、併用管理に変更し、併用管理の手順を実施してください。

● 併用管理

CENTUM VP のユーザ管理方法が併用管理の場合、次の手順に従ってください。

- CENTUM VP のコンピュータで、CTM_OPC_LCL グループと CTM_OPERATOR_LCL グループに所属する CENTUM アカウントを作成してください。
ただし、次のコンピュータでは、CTM_OPC_LCL グループと CTM_ENGINEER_LCL グループに所属する CENTUM アカウントを作成してください。
 - 処方エンジニア登録ファイルがあるコンピュータ

- 処方機能の履歴管理データベースがあるコンピュータ
2. CENTUM CS 3000 R3 HIS と CENTUM VP で CENTUM アカウントのパスワードを一致させてください。

■ CENTUM VP から CENTUM CS 3000 R3 HIS を参照する

CENTUM VP から CENTUM CS 3000 R3 HIS の各種データを参照するために、CENTUM CS 3000 R3 HIS にユーザアカウントを作成してください。

● スタンドアロン管理

CENTUM VP のユーザ管理方法がスタンドアロン管理の場合、次の手順に従ってください。

1. CENTUM CS 3000 R3 HIS に、CENTUM VP コンピュータに登録されているすべてのユーザアカウントを登録してください。
2. CENTUM VP と CENTUM CS 3000 R3 HIS で、各ユーザアカウントのパスワードを一致させてください。
3. 管理者ユーザで CENTUM CS 3000 R3 HIS ヘログオンしてください。
4. 実行中のすべてのアプリケーションを終了させてください。
5. CENTUM VP のソフトウェアメディアを、ドライブにセットしてください。
インストールメニューが自動的に起動しますが、[閉じる] をクリックして終了させてください。
6. 次のコマンドを実行してください。

<CENTUM VP ソフトウェアメディアドライブ>:\CENTUM\SECURITY\yokogawa.IA.iPCS.Plat form.Security.CreateCentumProcess.exe

CTM_PROCESS アカウント作成ユーティリティが起動されて、CTM_PROCESS アカウントが作成されます。

● ドメイン管理

CENTUM VP のユーザ管理方法がドメイン管理の場合は、併用管理に変更し、併用管理の手順を実施してください。

● 併用管理

CENTUM VP のユーザ管理方法が併用管理の場合、次の手順に従ってください。

1. CENTUM CS 3000 R3 HIS に、ドメインに登録されているユーザアカウントと同じユーザ名のアカウントを登録してください。
2. CENTUM CS 3000 R3 HIS に、CENTUM VP コンピュータに登録されているすべてのローカルユーザのアカウントを登録してください。
3. ドメインユーザのアカウントと CENTUM VP コンピュータのローカルアカウント、CENTUM CS 3000 R3 HIS のローカルアカウントで、各ユーザアカウントのパスワードを一致させてください。
4. 管理者ユーザで CENTUM CS 3000 R3 HIS ヘログオンしてください。
5. 実行中のすべてのアプリケーションを終了させてください。
6. CENTUM VP のソフトウェアメディアを、ドライブにセットしてください。
インストールメニューが自動的に起動しますが、[閉じる] をクリックして終了させてください。
7. 次のコマンドを実行してください。

<CENTUM VP ソフトウェアメディアドライブ>:\CENTUM\SECURITY\yokogawa.IA.iPCS.Plat form.Security.CreateCentumProcess.exe

CTM_PROCESS アカウント作成ユーティリティが起動されて、CTM_PROCESS アカウントが作成されます。

C9.2 CENTUM VP 標準モデルの VP プロジェクトに従来モデルの CENTUM VP HIS を混在させる

CENTUM VP 標準モデルの VP プロジェクトに従来モデルの CENTUM VP HIS を混在させるときの手順を説明します。

重要

- ・すべての HIS のユーザ認証モードを CENTUM 認証モードで統一してください。
- ・次のパッケージが有効化されているコンピュータはセキュリティモデルを標準モデルにしてください。
 - ・エンジニアリングサーバ機能
 - ・エンジニアリング基本機能
 - ・バッチビルダ(VP Batch)
 - ・拡張テスト機能
 - ・FCS シミュレータパッケージ
 - ・HIS シミュレータパッケージ
- また、VP プロジェクトデータベースのあるコンピュータもセキュリティモデルを標準モデルにしてください。
- ・従来モデルの CENTUM VP HIS をドメインに参加させることもできます。
- ・このような構成の場合は、システム全体を CENTUM VP 標準モデルで統一した場合よりセキュリティ対策の効果が低下します。この構成を一時的なものととらえ、計画的に CENTUM VP 標準モデルに統一することを推奨します。

■ 従来モデルの CENTUM VP HIS から標準モデルのコンピュータを参照する

従来モデルの CENTUM VP HIS から標準モデルのコンピュータの各種データを参照するため、標準モデルのコンピュータに、従来モデルの CENTUM VP HIS のユーザアカウントを作成する必要があります。

ユーザアカウントを作成する手順は、ユーザ管理方法によって異なります。

● スタンドアロン管理

ユーザ管理方法がスタンドアロン管理の場合にユーザアカウント作成するときは、次の手順に従ってください。

1. 標準モデルのコンピュータで、従来モデルの CENTUM VP HIS で使用しているユーザを CTM_OPERATOR グループのユーザアカウントとして作成してください。ただし、処方機能を使用するユーザについては、CTM_ENGINEER グループのユーザアカウントとして作成してください。
2. 各コンピュータで、各ユーザアカウントのパスワードを統一してください。

● ドメイン管理

ユーザ管理方法がドメイン管理の場合にユーザアカウント作成するときは、次の手順に従ってください。

1. 従来モデルの CENTUM VP HIS をドメインに参加させてください。
さらに、従来モデルの CENTUM VP HIS が R4 の場合は、ドメインに参加させたあと、ドメインネットワークの Windows ファイアウォールを無効にしてください。
2. ドメインの CTM_OPERATOR グループに、従来モデルの CENTUM VP HIS 用のユーザアカウントを作成してください。

ただし処方機能を使用するユーザについては、CTM_ENGINEER グループのユーザアカウントとして作成してください。

補足

以降は、従来モデルの CENTUM VP HIS では、作成したドメインユーザのアカウントを使用してください。

● 併用管理

ユーザ管理方法が併用管理の場合にユーザアカウント作成するときは、次の手順に従ってください。

1. 従来モデルの CENTUM VP HIS をドメインに参加させてください。
さらに、従来モデルの CENTUM VP HIS が R4 の場合は、ドメインに参加させたあと、ドメインネットワークの Windows ファイアウォールを無効にしてください。
2. 次のどちらかを設定してください。
 - ・ 従来モデルの CENTUM VP HIS をドメインユーザで使用するときは、そのユーザをドメインの CTM_OPERATOR グループのユーザアカウントとして作成してください。
ただし、処方機能を使用するユーザは、CTM_ENGINEER グループのユーザアカウントとして作成してください。
 - ・ 従来モデルの CENTUM VP HIS をローカルユーザで使用するときは、そのユーザを標準モデルのすべてのコンピュータで、CTM_OPERATOR_LCL グループのユーザアカウントとして作成してください。
ただし、処方機能を使用するユーザは、CTM_ENGINEER_LCL グループのユーザアカウントとして作成してください。

■ 標準モデルのコンピュータから従来モデルの CENTUM VP HIS を参照する

標準モデルのコンピュータから従来モデルの CENTUM VP HIS の各種データを参照するため、従来モデルの CENTUM VP HIS に、標準モデルのコンピュータのユーザアカウントを作成する必要があります。

ユーザアカウントを作成する手順は、ユーザ管理方法によって異なります。

● スタンドアロン管理

ユーザ管理方法がスタンドアロン管理の場合にユーザアカウント作成するときは、次の手順に従ってください。

1. 従来モデルの CENTUM VP HIS で、標準モデルのコンピュータで使用しているユーザを作成してください。
2. 各コンピュータで、各ユーザアカウントのパスワードを統一してください。

● ドメイン管理

ユーザ管理方法がドメイン管理の場合は、従来モデルの CENTUM VP HIS をドメインに参加させれば、新規にユーザアカウントを作成する必要はありません。

さらに、従来モデルの CENTUM VP HIS が R4 の場合は、ドメインに参加させたあと、ドメインネットワークの Windows ファイアウォールを無効にしてください。

● 併用管理

ユーザ管理方法が併用管理の場合にユーザアカウントを作成するときは、次の手順に従ってください。

1. 従来モデルの CENTUM VP HIS をドメインに参加させてください。

さらに、従来モデルの CENTUM VP HIS が R4 の場合は、ドメインに参加させたあと、ドメインネットワークの Windows ファイアウォールを無効にしてください。

2. 従来モデルの CENTUM VP HIS に、標準モデルのコンピュータで使用しているローカルユーザのアカウントを作成してください。
3. 各コンピュータで、各ユーザアカウントのパスワードを統一してください。

C9.3 複数プロジェクト結合をする

複数プロジェクト結合を使用するときは、結合する相手システムによってセキュリティの設定方法が異なります。

重要

プロジェクト内のセキュリティモデルは、標準モデルまたは従来モデルに統一させてください。

C9.3.1 標準モデルの CENTUM VP プロジェクトと従来モデルの CENTUM VP プロジェクトを結合する

標準モデルの CENTUM VP プロジェクトと従来モデルの CENTUM VP プロジェクトを結合するときは、結合先のシステムに応じて設定が必要です。

補足

- ・ 標準モデルの CENTUM VP プロジェクトのユーザ認証モードは、Windows 認証モードまたは CENTUM 認証モードのどちらとすることも可能です。ただし、ユーザ認証モードはプロジェクト単位で統一させてください。
- ・ 従来モデルの CENTUM VP プロジェクトのコンピュータをドメインに参加させることもできます。

重要

このような構成の場合は、システム全体を CENTUM VP 標準モデルで統一した場合よりセキュリティ対策の効果が低下します。この構成を一時的なものととらえ、計画的に CENTUM VP 標準モデルに統一することを推奨します。

■ 従来モデルの CENTUM VP プロジェクトのコンピュータから、標準モデルの CENTUM VP のコンピュータを参照する

従来モデルの CENTUM VP プロジェクトのコンピュータから、標準モデルの CENTUM VP プロジェクトの各種データを参照するには、標準モデルの CENTUM VP プロジェクトのコンピュータに、従来モデルの CENTUM VP プロジェクトで使用しているユーザアカウントを作成してください。手順はユーザ管理方法によって異なります。

● スタンドアロン管理

ユーザ管理方法がスタンドアロン管理の場合にユーザアカウント作成するときは、次の手順に従ってください。

1. 従来モデルの CENTUM VP プロジェクトのコンピュータが接続する標準モデルの CENTUM VP プロジェクトのコンピュータを特定してください。
2. そのコンピュータで、従来モデルの CENTUM VP プロジェクトで使用しているすべてのユーザを CTM_OPERATOR グループのユーザアカウントとして作成してください。ただし次の条件を満たすコンピュータでは、CTM_ENGINEER グループのユーザアカウントとして作成してください。
 - ・ エンジニア登録ファイルや、処方エンジニア登録ファイルのあるコンピュータ
 - ・ システム生成機能のあるコンピュータ
 - ・ 処方機能の履歴管理データベースのあるコンピュータ
3. すべてのコンピュータで、ユーザアカウントのパスワードを統一してください。

参照

従来モデルの CENTUM VP プロジェクトのコンピュータが接続する標準モデルの CENTUM VP プロジェクトのコンピュータについては、以下を参照してください。

「■ プロジェクト結合時に接続先となるコンピュータ」ページ C9-11

● ドメイン管理

ユーザ管理方法がドメイン管理の場合にユーザアカウント作成するときは、次の手順に従ってください。

1. 従来モデルの CENTUM VP プロジェクトのコンピュータをドメインに参加させてください。
さらに、従来モデルの CENTUM VP HIS が R4 の場合は、ドメインに参加させたあと、ドメインネットワークの Windows ファイアウォールを無効にしてください。

2. ドメインの CTM_OPERATOR グループに、従来モデルの CENTUM VP プロジェクトのコンピュータ用ユーザアカウントを作成してください。
ただし、システム生成機能や処方機能を利用するユーザは、CTM_ENGINEER グループのユーザアカウントとして作成してください。

補足

以降は、従来モデルの CENTUM VP プロジェクトのコンピュータでは、作成したドメインユーザのアカウントを使用してください。

● 併用管理

ユーザ管理方法が併用管理の場合にユーザアカウント作成するときは、次の手順に従ってください。

1. 従来モデルの CENTUM VP プロジェクトのコンピュータをドメインに参加させてください。
さらに、従来モデルの CENTUM VP HIS が R4 の場合は、ドメインに参加させたあと、ドメインネットワークの Windows ファイアウォールを無効にしてください。
2. 次のどちらかを設定してください。
 - ・ 従来モデルの CENTUM VP プロジェクトのコンピュータをドメインユーザで使用するときは、そのユーザをドメインの CTM_OPERATOR グループのユーザアカウントとして作成してください。
ただし、システム生成機能や処方機能を利用するユーザは、CTM_ENGINEER グループのユーザアカウントとして作成してください。
 - ・ 従来モデルの CENTUM VP プロジェクトのコンピュータをローカルユーザで使用するときは、従来モデルの CENTUM VP プロジェクトのコンピュータが接続する標準モデルの CENTUM VP プロジェクトのコンピュータを特定してください。そのコンピュータに、従来モデルのコンピュータで使用するユーザを CTM_OPERATOR_LCL グループのアカウントとして作成してください。
ただし、次の条件を満たすコンピュータでは、CTM_ENGINEER_LCL グループのアカウントとして作成してください。
 - ・ 処方エンジニア登録ファイルのあるコンピュータ
 - ・ 処方機能の履歴管理データベースのあるコンピュータ

参照

従来モデルの CENTUM VP プロジェクトのコンピュータが接続する標準モデルの CENTUM VP プロジェクトのコンピュータについては、以下を参照してください。

「■ プロジェクト結合時に接続先となるコンピュータ」ページ C9-11

■ 標準モデルの CENTUM VP プロジェクトのコンピュータから、従来モデルの CENTUM VP のコンピュータを参照する

標準モデルの CENTUM VP プロジェクトのコンピュータから、従来モデルの CENTUM VP プロジェクトの各種データを参照するには、従来モデルの CENTUM VP プロジェクトのコンピュータに、標準モデルの CENTUM VP プロジェクトで使用しているユーザアカウントを作成してください。手順はユーザ管理方法によって異なります。

● スタンドアロン管理

ユーザ管理方法がスタンドアロン管理の場合にユーザアカウント作成するときは、次の手順に従ってください。

1. 標準モデルの CENTUM VP プロジェクトのコンピュータが接続する従来モデルの CENTUM VP プロジェクトのコンピュータを特定してください。

2. そのコンピュータで、標準モデルの CENTUM VP プロジェクトで使用しているすべてのユーザーアカウントを作成してください。標準モデルの CENTUM VP プロジェクトで Windows 認証モードを使用している場合は、OFFUSER も作成してください。
3. すべてのコンピュータで、ユーザーアカウントのパスワードを統一してください。

参照

標準モデルの CENTUM VP プロジェクトのコンピュータが接続する従来モデルの CENTUM VP プロジェクトのコンピュータについては、以下を参照してください。

「■ プロジェクト結合時に接続先となるコンピュータ」ページ C9-11

OFFUSER の作成方法については、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「6.10.7 CreateOffuser」

● ドメイン管理

ユーザ管理方法がドメイン管理の場合にユーザーアカウント作成するときは、次の手順に従ってください。

1. 従来モデルの CENTUM VP プロジェクトのコンピュータをドメインに参加させてください。
さらに、従来モデルの CENTUM VP HIS が R4 の場合は、ドメインに参加させたあと、ドメインネットワークの Windows ファイアウォールを無効にしてください。
2. 標準モデルの CENTUM VP プロジェクトで Windows 認証モードを使用している場合は、従来モデルの CENTUM VP プロジェクトのコンピュータで OFFUSER を作成してください。

参照

OFFUSER の作成方法については、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「6.10.7 CreateOffuser」

● 併用管理

ユーザ管理方法が併用管理の場合にユーザーアカウント作成するときは、次の手順に従ってください。

1. 従来モデルの CENTUM VP プロジェクトのコンピュータをドメインに参加させてください。
さらに、従来モデルの CENTUM VP HIS が R4 の場合は、ドメインに参加させたあと、ドメインネットワークの Windows ファイアウォールを無効にしてください。
2. 標準モデルの CENTUM VP プロジェクトで Windows 認証モードを使用している場合は、従来モデルの CENTUM VP プロジェクトのコンピュータで OFFUSER を作成してください。
3. 次のどちらかを設定してください。
 - 従来モデルの CENTUM VP プロジェクトのコンピュータをドメインユーザで使用するときは、そのユーザをドメインの CTM_OPERATOR グループのユーザアカウントとして作成してください。
ただし、システム生成機能や処方機能を利用するユーザは、CTM_ENGINEER グループのアカウントとして作成してください。
 - 従来モデルの CENTUM VP プロジェクトのコンピュータをローカルユーザで使用するときは、標準モデルの CENTUM VP プロジェクトのコンピュータが接続する従来モデルの CENTUM VP プロジェクトのコンピュータを特定してください。そのコンピュータに、標準モデルのコンピュータで使用するユーザを CTM_OPERATOR_LCL グループのアカウントとして作成してください。

ただし、次の条件を満たすコンピュータでは、CTM_ENGINEER_LCL グループのアカウントとして作成してください。

- ・ 処方エンジニア登録ファイルのあるコンピュータ
- ・ 処方機能の履歴管理データベースのあるコンピュータ

参照

OFFUSER の作成方法については、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「6.10.7 CreateOffuser」

標準モデルの CENTUM VP プロジェクトのコンピュータが接続する従来モデルの CENTUM VP プロジェクトのコンピュータについては、以下を参照してください。

「■ プロジェクト結合時に接続先となるコンピュータ」ページ C9-11

■ プロジェクト結合時に接続先となるコンピュータ

プロジェクト結合時には、DCOM (OPC) による接続や、共有フォルダによる接続が行われます。

DCOM (OPC)、または共有フォルダにより接続先となるコンピュータは、次の様なコンピュータがあります。

補足

なお、標準モデルから従来モデルに接続する場合も、従来モデルから標準モデルに接続する場合も接続先となるコンピュータの条件は同じです。

- ・ 自プロジェクトのシステム構成定義に存在する結合先プロジェクトの HIS
- ・ プロジェクトデータベースのあるコンピュータ
- ・ .SH HIS Setup ウィンドウの [メッセージサマリ参照先] で指定されたコンピュータ
- ・ 長期データ保管ファイルのあるコンピュータ
- ・ CAMS for HIS のヒストリカルデータの長期データ保管先にしてあるコンピュータ
- ・ ヒストリカルメッセージ保存ファイルの保管先に指定したコンピュータ
- ・ 処方管理とプロセス管理をプロジェクト間で共有する場合の処方管理データベースのあるコンピュータ
- ・ 帳票パッケージから指定した Exaopc OPC インタフェースパッケージ (HIS 搭載用) のあるコンピュータ
- ・ アクセス制限パッケージや FDA:21 CFR part 11 対応パッケージで、エンジニアリング機能、処方機能、および帳票機能の [連続した認証失敗を通知] の通知先に指定した Exaopc OPC インタフェースパッケージ (HIS 搭載用) のあるコンピュータ
- ・ アクセス制限パッケージや FDA:21 CFR part 11 対応パッケージのエンジニア登録ファイル、処方エンジニア登録ファイル、帳票のユーザセキュリティファイル、および各履歴管理データベースのあるコンピュータ

補足

システム構成定義に存在する接続先プロジェクトの HIS には、任意の HIS でログセーブを実行するときに接続します。

C9.3.2 CENTUM VP プロジェクトと CENTUM CS 1000/CS 3000 R3 プロジェクトを結合する

CENTUM VP プロジェクトと CENTUM CS 1000/CS 3000 R3 プロジェクトを結合するときは、結合先のシステムに応じて設定が必要です。

なお、CENTUM VP プロジェクトは標準モデルとします。

補足

- CENTUM VP プロジェクトのユーザ認証モードは、Windows 認証モードまたは CENTUM 認証モードのどちらとすることも可能です。ただし、ユーザ認証モードはプロジェクト単位で統一させてください。
- CENTUM CS 1000/CS 3000 R3 のコンピュータのユーザ管理方法は、常にスタンダードアロン管理にしてください。

重要

このような構成の場合は、システム全体を CENTUM VP 標準モデルで統一した場合よりセキュリティ対策の効果が低下します。この構成を一時的なものととらえ、計画的に CENTUM VP 標準モデルに統一することを推奨します。

■ CENTUM CS 1000/CS 3000 R3 プロジェクトのコンピュータから CENTUM VP プロジェクトのコンピュータを参照する

CENTUM CS 1000/CS 3000 R3 プロジェクトのコンピュータから、CENTUM VP プロジェクトの各種データを参照するには、CENTUM VP のコンピュータにユーザアカウントを作成してください。

● スタンダードアロン管理

CENTUM VP のユーザ管理方法がスタンダードアロン管理の場合、次の手順に従ってください。

1. CENTUM CS 1000/CS 3000 R3 プロジェクトのコンピュータが接続する CENTUM VP プロジェクトのコンピュータを特定してください。
2. そのコンピュータで、CTM_OPC グループと CTM_OPERATOR グループに所属する CENTUM アカウントを作成してください。
3. 次の条件を満たすコンピュータでは、システム生成機能、処方機能で使用しているユーザを CTM_OPC グループと CTM_ENGINEER グループに所属するアカウントとして作成してください。
 - エンジニア登録ファイルや、処方エンジニア登録ファイルがあるコンピュータ
 - システム生成機能があるコンピュータ
 - 処方機能の履歴管理データベースがあるコンピュータ
4. すべてのコンピュータで、ユーザアカウントのパスワードを統一してください。

参照

CENTUM CS 1000/CS 3000 R3 プロジェクトのコンピュータが接続する CENTUM VP プロジェクトのコンピュータについては、以下を参照してください。

「● CENTUM CS 1000/CS 3000 R3 プロジェクトのコンピュータから接続される CENTUM VP プロジェクトのコンピュータ」ページ C9-13

● ドメイン管理

CENTUM VP のユーザ管理方法がドメイン管理の場合は、併用管理に変更し、併用管理の手順を実施してください。

● 併用管理

CENTUM VP のユーザ管理方法が併用管理の場合、次の手順に従ってください。

1. CENTUM CS 1000/CS 3000 R3 プロジェクトのコンピュータが接続する CENTUM VP プロジェクトのコンピュータを特定してください。
2. そのコンピュータで、CTM_OPC グループと CTM_OPERATOR グループに所属する CENTUM アカウントを作成してください。
3. 次の条件を満たすコンピュータでは、システム生成機能、処方機能で使用しているユーザを CTM_OPC_LCL グループと CTM_ENGINEER_LCL グループに所属するアカウントとして作成してください。
 - ・ エンジニア登録ファイルや、処方エンジニア登録ファイルがあるコンピュータ
 - ・ システム生成機能があるコンピュータ
 - ・ 処方機能の履歴管理データベースがあるコンピュータ
4. すべてのコンピュータで、ユーザアカウントのパスワードを統一してください。

参照

CENTUM CS 1000/CS 3000 R3 プロジェクトのコンピュータが接続する CENTUM VP プロジェクトのコンピュータについては、以下を参照してください。

「● CENTUM CS 1000/CS 3000 R3 プロジェクトのコンピュータから接続される CENTUM VP プロジェクトのコンピュータ」ページ C9-13

● CENTUM CS 1000/CS 3000 R3 プロジェクトのコンピュータから接続される CENTUM VP プロジェクトのコンピュータ

プロジェクト結合時には、DCOM (OPC) による接続や、共有フォルダによる接続が行われます。

DCOM (OPC)、または共有フォルダにより接続先となるコンピュータは、次の様なコンピュータがあります。

- ・ プロジェクトデータベースのあるコンピュータ
- ・ .SH HIS Setup ウィンドウの [メッセージサマリ参照先] で指定されたコンピュータ
- ・ 長期データ保管ファイルのあるコンピュータ
- ・ CAMS for HIS のヒストリカルデータの長期データ保管先にしてあるコンピュータ
- ・ ヒストリカルメッセージ保存ファイルの保管先に指定したコンピュータ
- ・ 処方管理 CENTUM VP で行い、プロセス管理を CENTUM CS 3000 R3 で行っている場合の処方管理データベースのあるコンピュータ
- ・ 帳票パッケージから指定した Exaopc OPC インタフェースパッケージ (HIS 搭載用) のあるコンピュータ
- ・ アクセス制限パッケージや FDA:21 CFR part 11 対応パッケージで、エンジニアリング機能、処方機能、および帳票機能の [連続した認証失敗を通知] の通知先に指定した Exaopc OPC インタフェースパッケージ (HIS 搭載用) のあるコンピュータ
- ・ アクセス制限パッケージや FDA:21 CFR part 11 対応パッケージのエンジニア登録ファイル、処方エンジニア登録ファイル、帳票のユーザセキュリティファイル、および各履歴管理データベースのあるコンピュータ

■ CENTUM VP プロジェクトのコンピュータから CENTUM CS 1000/CS 3000 R3 プロジェクトを参照する

CENTUM VP プロジェクトのコンピュータから、CENTUM CS 1000/CS 3000 R3 プロジェクトの各種データを参照するには、CENTUM CS 1000/CS 3000 R3 のコンピュータにユーザアカウントを作成してください。

● スタンドアロン管理

CENTUM VP のユーザ管理方法がスタンドアロン管理の場合、次の手順に従ってください。

1. CENTUM VP プロジェクトのコンピュータが接続する CENTUM CS 1000/CS 3000 R3 プロジェクトのコンピュータを特定してください。
2. そのコンピュータで、CENTUM VP コンピュータに登録されているすべてのユーザーアカウントと、CTM_PROCESS アカウントを作成してください。

参照

ユーザアカウントと CTM_PROCESS アカウントの作成方法については、以下を参照してください。

「● スタンドアロン管理」ページ C9-3

CENTUM VP プロジェクトのコンピュータが接続する CENTUM CS 1000/CS 3000 R3 プロジェクトのコンピュータについては、以下を参照してください。

「● CENTUM VP プロジェクトのコンピュータから接続される CENTUM CS 1000/CS 3000 R3 プロジェクトのコンピュータ」ページ C9-14

● ドメイン管理

CENTUM VP のユーザ管理方法がドメイン管理の場合は、併用管理に変更し、併用管理の手順を実施してください。

● 併用管理

CENTUM VP のユーザ管理方法が併用管理の場合、次の手順に従ってください。

1. CENTUM VP プロジェクトのコンピュータが接続する CENTUM CS 1000/CS 3000 R3 プロジェクトのコンピュータを特定してください。
2. そのコンピュータで、ドメインユーザーのアカウント、CENTUM VP コンピュータに登録されているすべてのローカルユーザーのアカウント、および CTM_PROCESS アカウントを作成してください。

参照

ユーザアカウントと CTM_PROCESS アカウントの作成方法については、以下を参照してください。

「● 併用管理」ページ C9-3

CENTUM VP プロジェクトのコンピュータが接続する CENTUM CS 1000/CS 3000 R3 プロジェクトのコンピュータについては、以下を参照してください。

「● CENTUM VP プロジェクトのコンピュータから接続される CENTUM CS 1000/CS 3000 R3 プロジェクトのコンピュータ」ページ C9-14

● CENTUM VP プロジェクトのコンピュータから接続される CENTUM CS 1000/CS 3000 R3 プロジェクトのコンピュータ

プロジェクト結合時には、DCOM (OPC) による接続や、共有フォルダによる接続が行われます。

DCOM (OPC)、または共有フォルダにより接続先となるコンピュータは、次の様なコンピュータがあります。

- CENTUM VP プロジェクトのシステム構成定義上に存在する CENTUM CS 1000/CS 3000 R3 HIS
- プロジェクトデータベースのあるコンピュータ
- .SH HIS Setup ウィンドウの [メッセージサマリ参照先] で指定されたコンピュータ
- 長期データ保管ファイルのあるコンピュータ
- CAMS for HIS のヒストリカルデータの長期データ保管先にしてあるコンピュータ
- ヒストリカルメッセージ保存ファイルの保管先に指定したコンピュータ

- ・処方管理 CENTUM CS 3000 R3 で行い、プロセス管理を CENTUM VP で行っている場合の処方管理データベースのあるコンピュータ
- ・帳票パッケージから指定した Exaopc OPC インタフェースパッケージ（HIS 搭載用）のあるコンピュータ
- ・アクセス制限パッケージや FDA:21 CFR part 11 対応パッケージで、エンジニアリング機能、処方機能、および帳票機能の〔連続した認証失敗を通知〕の通知先に指定した Exaopc OPC インタフェースパッケージ（HIS 搭載用）のあるコンピュータ
- ・アクセス制限パッケージや FDA:21 CFR part 11 対応パッケージのエンジニア登録ファイル、処方エンジニア登録ファイル、帳票のユーザセキュリティファイル、および各履歴管理データベースのあるコンピュータ

補足

システム構成定義に存在する CENTUM CS 1000/CS 3000 R3 HIS には、他の HIS でログセーブを実行するときに接続します。

C9.3.3 CENTUM VP プロジェクトと CENTUM CS プロジェクトを結合する

CENTUM VP プロジェクトと CENTUM CS プロジェクトを結合するときは、CENTUM VP プロジェクトのセキュリティモデルは標準モデルとしてください。

重要

このような構成の場合は、システム全体を CENTUM VP 標準モデルで統一した場合よりセキュリティ対策の効果が低下します。この構成を一時的なものととらえ、計画的に CENTUM VP 標準モデルに統一することを推奨します。

■ CENTUM VP プロジェクトのコンピュータから CENTUM CS のプロジェクトデータベースを参照する

CENTUM VP から CENTUM CS のプロジェクトデータベースを参照する場合、特別な設定は必要ありません。

■ CENTUM CS のコンピュータから CENTUM VP のプロジェクトデータベースを参照する

CENTUM CS から CENTUM VP のプロジェクトデータベースを参照する場合は、CENTUM VP のプロジェクトデータベースがあるコンピュータで、ファイル管理サービス (BK FMS) を自動起動にする必要があります。

ファイル管理サービスを自動起動するときは、次の手順に従ってください。

1. 管理者ユーザでコンピュータにログオンしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [管理ツール] – [サービス] を選択してください。サービスウィンドウが表示されます。
4. BK FMS をダブルクリックしてください。BK FMS のプロパティが表示されます。
5. 全般タブで、[開始] をクリックしてください。BK FMS サービスが開始されます。
6. 全般タブの [スタートアップの種類] ドロップダウンリストで [自動] を選択してください。
7. [OK] をクリックしてください。

補足

BK FMS サービスのログオンアカウントは、CTM_PROCESS のままとしてください。

C9.4 CENTUM VP R4 で IT セキュリティ設定をしたファイルサーバやドメインコントローラを使用する

CENTUM VP R4 でセキュリティ設定をしたファイルサーバやドメインコントローラを使用する場合は、IT セキュリティ設定を再度行う必要があります。

■ 以前と同一のセキュリティ設定を行う場合

初期 IT セキュリティ保存データを使うことなく、R5 以降の IT セキュリティツールで、そのまま設定を行えます。

■ セキュリティ設定を変更する場合

1. R4 で IT セキュリティ設定をする前の初期 IT セキュリティ保存データを使い、IT セキュリティ設定が行われていない状態を復元してください。
2. R5 以降の IT セキュリティツールを適用してください。

参照

ファイルサーバ、ドメインコントローラのセキュリティ設定の復元については、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「6.5.2 ファイルサーバやドメインコントローラの場合」

Blank Page

C10. トラブルシューティング

ここでは、トラブル時に考えられる原因と対策について説明します。

C10.1 Windows 関連のトラブルシューティング

ここでは、Windows に関するトラブル対応について説明します。

C10.1.1 ユーザアカウント制御の注意事項

管理者ユーザ以外のアカウントでインストーラを起動しようとすると、次に示すダイアログが表示されます。[いいえ] をクリックしてから、管理者ユーザでログオンし直し、再度インストーラを起動してください。



図 C10.1.1-1 ユーザアカウント制御ダイアログ（管理者ユーザ以外の場合）

C10.1.2 サーバーマネージャーの起動時にエラーが発生する

サーバーマネージャーの起動時にエラーが表示される場合があります。

■ 発生条件

DCOM の [既定の認証レベル] が [なし] になっていると発生します。

補足

例えば、次のような場合に DCOM の [既定の認証レベル] が [なし] になっています。

- ・セキュリティモデルを従来モデルに設定している。
- ・他のコンピュータと通信するために DCOM の [既定の認証レベル] を [なし] に設定している。

■ 回避手順

次の手順で回避できます。ただし、次の手順を実行した場合、サーバーマネージャーを使った作業終了後に元の設定へ戻してください。

1. コントロールパネルを起動してください。
2. [システムとセキュリティ] – [管理ツール] – [コンポーネントサービス] を選択してください。
コンポーネントサービスウィンドウが表示されます。
3. [コンソールルート] – [コンポーネントサービス] – [コンピュータ] – [マイコンピュータ] を選択し、コンテキストメニューから [プロパティ] を選択してください。

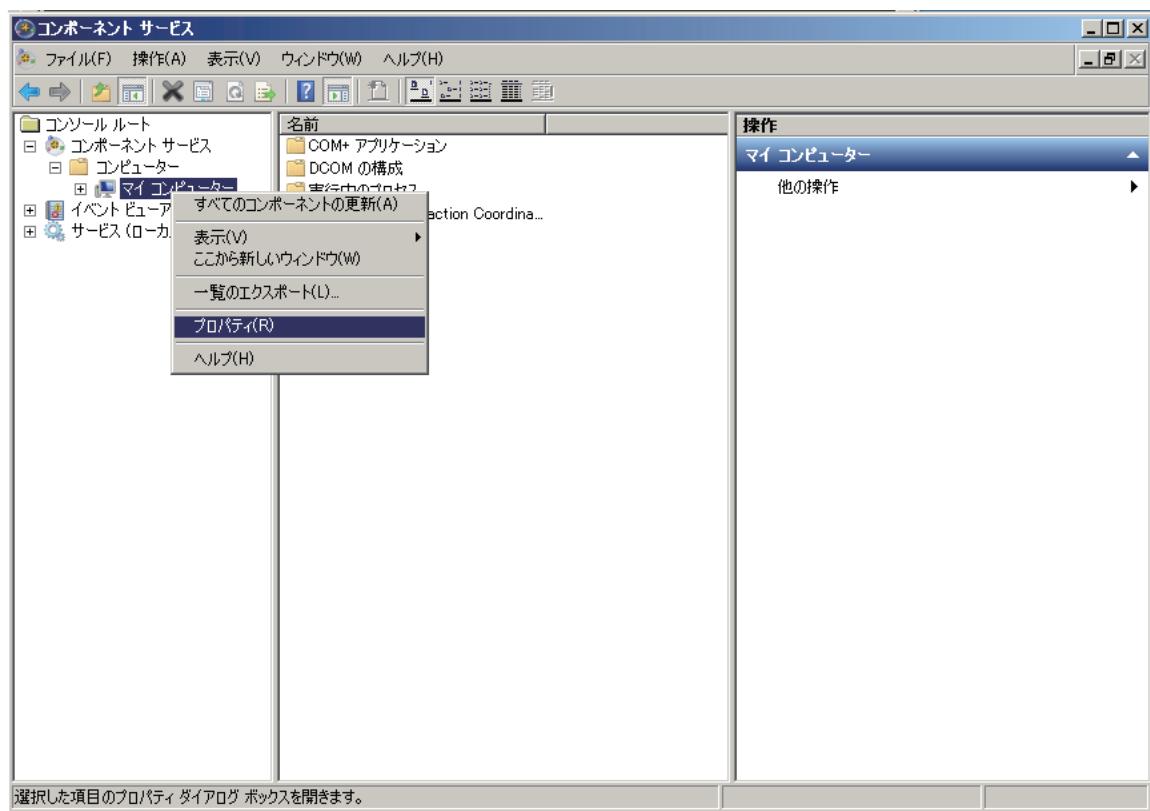


図 C10.1.2-1 コンポーネントサービス

マイコンピュータのプロパティダイアログが表示されます。

4. [既定の認証レベル] のドロップダウンリストから [接続] を選択して、[OK] をクリックしてください。

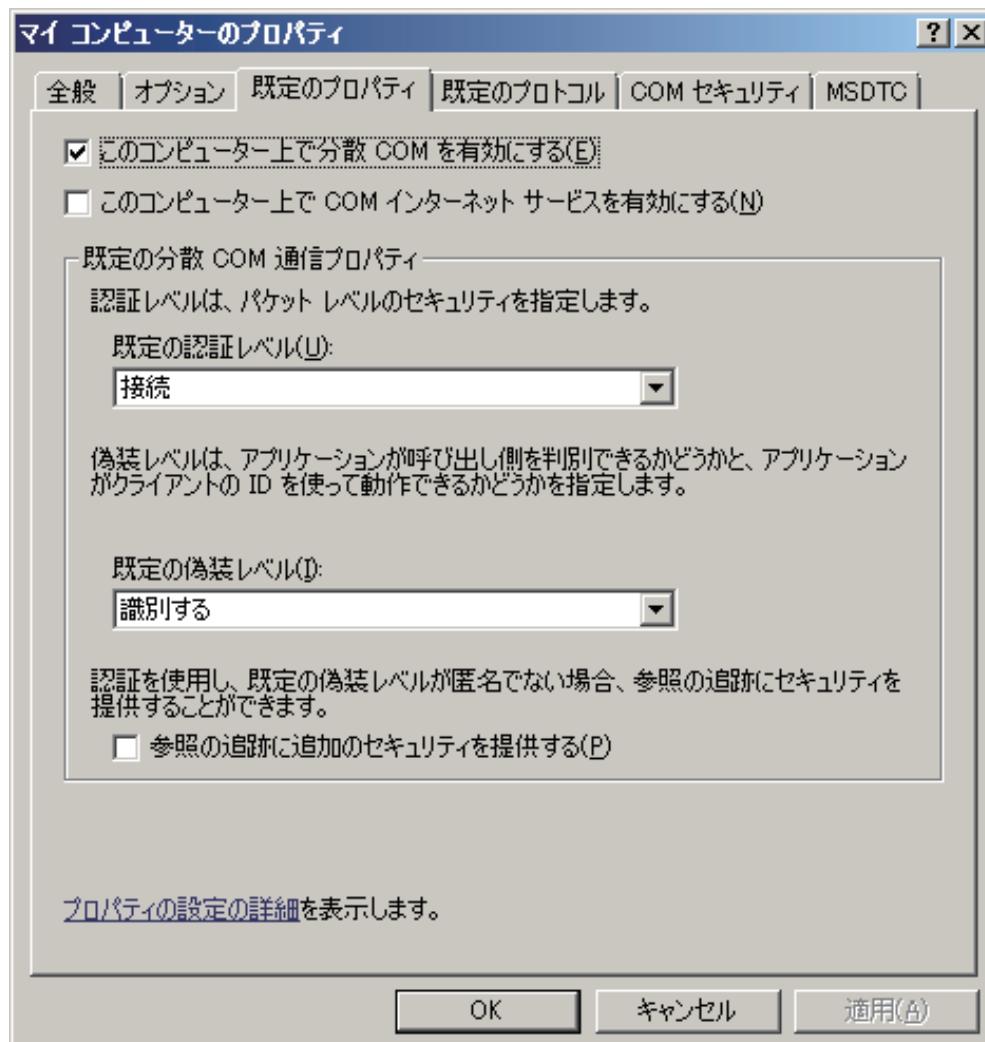


図 C10.1.2-2 マイコンピュータのプロパティ

C10.1.3 コントロールパネルのユーザーアカウントダイアログでユーザーアカウントが管理できない

コントロールパネルのユーザーアカウントダイアログで、ユーザの作成などの操作ができない場合があります。

■ 発生条件

DCOM の [既定の認証レベル] が [なし] になっていると発生します。

補足

例えば、次のような場合に DCOM の [既定の認証レベル] が [なし] になっています。

- セキュリティモデルを従来モデルに設定している。
- 他のコンピュータと通信するために DCOM の [既定の認証レベル] を [なし] に設定している。

■ 回避手順

次に回避手順を示します。

- コントロールパネルを起動してください。
- [システムとセキュリティ] – [管理ツール] – [コンピューターの管理] を選択してください。
コンピューターの管理ウィンドウが表示されます。
- 左ペインで [コンピューターの管理] – [システムツール] – [ローカルユーザーとグループ] を選択してください。
- 中央のペインで、ユーザの作成などの操作をしてください。

C10.1.4 コントロールパネルのプログラムと機能ウィンドウでインストールされた更新プログラムが表示されない

コントロールパネルのプログラムと機能ウィンドウで、インストールされた更新プログラムが表示されない場合があります。

■ 発生条件

DCOM の [既定の認証レベル] が [なし] になっていると発生します。

補足

例えば、次のような場合に DCOM の [既定の認証レベル] が [なし] になっています。

- セキュリティモデルを従来モデルに設定している。
- 他のコンピュータと通信するために DCOM の [既定の認証レベル] を [なし] に設定している。

■ 回避手順

次に回避手順を示します。

- 管理者ユーザでログオンしてください。
- コマンドプロンプトを起動してください。
- 次のコマンドを実行してください。

```
wmic qfe list full
```

インストールされた更新プログラムが出力されます。

補足

次のようにコマンドを入力すると、インストールされた更新プログラムを html 形式のファイルに出力できます。このファイルはコマンドを実行したフォルダに出力されます。

```
wmic qfe list full /format:htable > results.html
```

C10.1.5 マイクロソフトの更新プログラムがインストールできない

マイクロソフトの更新プログラムのインストール時にエラー 80070543 が発生し、インストールに失敗する場合があります。

■ 発生条件

DCOM の [既定の認証レベル] が [なし] になっていると発生します。

補足

例えば、次のような場合に DCOM の [既定の認証レベル] が [なし] になっています。

- セキュリティモデルを従来モデルに設定している。
- 他のコンピュータと通信するために DCOM の [既定の認証レベル] を [なし] に設定している。

■ 回避手段

次の手順で回避できます。

- DCOM の既定の認証レベルを [なし] から [接続] に変更してください。
- コンピュータを再起動してください。
- マイクロソフトの更新プログラムをインストールしてください。
- DCOM の既定の認証レベルを [接続] から [なし] に戻してください。
- コンピュータを再起動してください。

参照

DCOM の既定の認証レベルを変更する手順については、以下を参照してください。

「C10.1.2 サーバーマネージャーの起動時にエラーが発生する」ページ C10-4

C10.1.6 .NET Framework のインストールに失敗する

.NET Framework のインストールに失敗する場合があります。

■ 発生条件

DCOM の [既定の認証レベル] が [なし] になっていると発生します。

補足

例えば、次のような場合に DCOM の [既定の認証レベル] が [なし] になっています。

- セキュリティモデルを従来モデルに設定している。
- 他のコンピュータと通信するために DCOM の [既定の認証レベル] を [なし] に設定している。

■ 回避手段

次の手順で回避できます。

- DCOM の [既定の認証レベル] を [なし] から [接続] に変更してください。
- コンピュータを再起動してください。
- .NET Framework をインストールしてください。

参照

DCOM の既定の認証レベルを変更する手順については、以下を参照してください。

「C10.1.2 サーバーマネージャーの起動時にエラーが発生する」ページ C10-4

C10.1.7 システムがロックした

当社窓口に連絡してください。

C10.1.8 正常に動いていたコンピュータの動作が不安定になった

これまで正常に動いていたコンピュータ の動作が不安定になったときは、次の対応をしてください。

■ 原因

共存が許されていないソフトウェアをインストールした。

■ 対策

インストールした共存が許されていないソフトウェアをアンインストールしてください。

参照

共存可能なソフトウェアについては、以下を参照してください。

「● 共存できるソフトウェア」ページ A3-2

C10.1.9 印刷順序がスプールされた順と一致しない

一括セルフドキュメントなどで、プリンタに出力されたドキュメントの順序が印刷順序と異なる場合があります。

■ 原因

プリンタプロパティの詳細設定で【すぐに印刷データをプリンタに送る】に設定していると、多量の印刷要求がスプールされた場合に、あとから印刷要求のあったドキュメントが先に印刷されることがあります。

■ 対策

スプールされた順に印刷するためには、プリンタプロパティの詳細設定で【全ページ分のデータをスプールしてから、印刷データをプリンタに送る】に設定します。

次に、HP LaserJet 4050 Series PS を例にして、設定の手順を示します。これを参考に、使用しているプリンタの設定を変更してください。

- 管理者ユーザでログオンしてください。

補足

ネットワーク上の共有プリンタを使用している場合、そのプリンタのサーバマシンの管理者ユーザのアカウントでログオンしてください。

- コントロールパネルを起動してください。
- 【ハードウェアとサウンド】 – 【デバイスとプリンター】を選択してください。デバイスとプリンターウィンドウが表示されます。
- 使用するプリンタを選択し、右クリックして【プリンターのプロパティ】を選択してください。

使用するプリンタのプロパティのダイアログが表示されます。



図 C10.1.9-1 プリンタのプロパティ

- 【詳細設定】タブを選択して、【全ページ分のデータをスプールしてから、印刷データをプリンタに送る】を選択してください。

6. [スプールされたドキュメントを最初に印刷する] チェックボックスをオフにしてください。
7. [OK] をクリックしてください。
ダイアログが終了します。

C10.2 ネットワーク関連のトラブルシューティング

ここでは、ネットワークに関するトラブル対応について説明します。

C10.2.1 ネットワークケーブル配線時の注意事項

ネットワーク接続の際、Windows 7 の場合は、ケーブル配線したときに「ネットワークの場所の設定」ダイアログが表示されることがあります。この場合、[パブリックネットワーク] を選択してください。

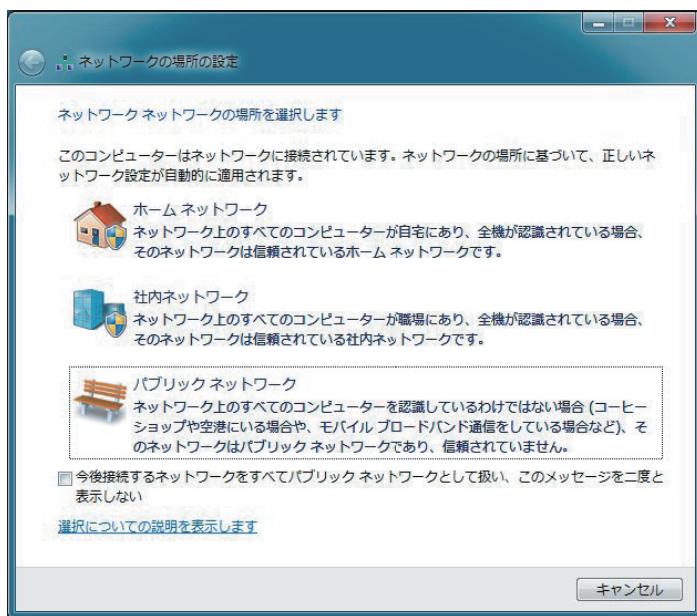


図 C10.2.1-1 「ネットワークの場所の設定」ダイアログ

Windows 10 と Windows Server 2016 の場合は、ケーブル配線したときに、デスクトップ右側からネットワークチャームバーが表示されることがあります。この場合、[いいえ] を選択してください。

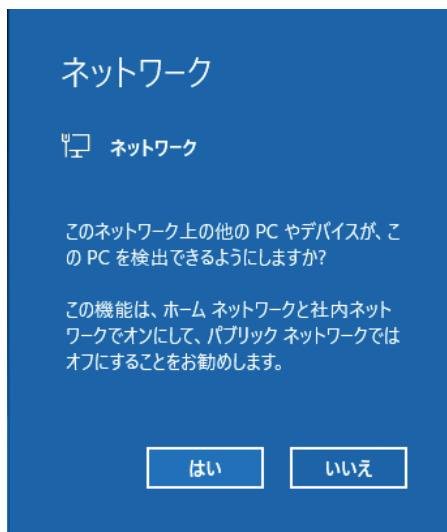


図 C10.2.1-2 ネットワークチャームバー

C10.2.2 ドライバのインストールと削除に関するトラブル

ネットワークドライバのインストールと削除に関するトラブルシューティングについて説明します。

重要

操作によっては管理者権限が必要な場合があり、「ユーザー アカウント制御」ダイアログが表示されることがあります。このときは [はい]、[続行]、または [許可] をクリックすることで操作を続行することができます（Administrator 権限を持つユーザの場合）。

■ インストール結果を確認する

ネットワークドライバが正しくインストールされているかどうか確認します。ドライバが正常に動作していない場合は、再度インストールしてください。

● 制御バスドライバのアダプタドライバの場合

制御バスドライバを追加すると、デバイスマネージャーの「ネットワークアダプタ」にアダプタドライバ「Yokogawa Vnet Adapter」が表示されます。

アダプタドライバが正常に起動しない場合、「！」マークがアダプタドライバのアイコンに表示されます。

デバイスマネージャーの表示方法は次のとおりです。

1. 管理者ユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. 「システムとセキュリティ」 – 「システム」 – 「デバイスマネージャー」を選択してください。

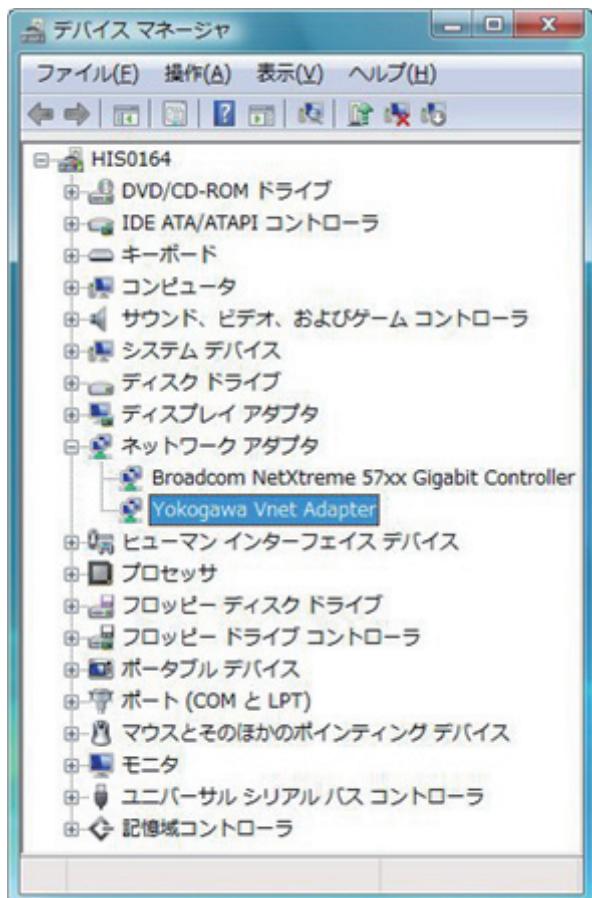


図 C10.2.2-1 アダプタドライバが正常に追加されている状態

● 制御バスドライバのプロトコルドライバの場合（Windows 10、Windows Server 2016）

制御バスドライバを追加すると、アダプタドライバと一緒にプロトコルドライバがインストールされます。

プロトコルドライバの動作状況は、コマンドプロンプトで確認できます。

プロトコルドライバの動作状況の確認方法は次のとおりです。

1. 一般ユーザ、または管理者ユーザでサインインしてください。
 2. コマンドプロンプトを起動してください。
 3. `sc query VLTDI` と入力して、[Enter] キーを押してください。
- プロトコルドライバの状態が表示されます。[STATE] が [RUNNING] となつていれば、正常に動作しています。

```
cmd コマンドプロンプト
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\$Users\$CENTUM>sc query VLTDI
SERVICE_NAME: VLTDI
    TYPE               : 1  KERNEL_DRIVER
    STATE              : 4  RUNNING
                           (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
    WIN32_EXIT_CODE    : 0  (0x0)
    SERVICE_EXIT_CODE : 0  (0x0)
    CHECKPOINT        : 0x0
    WAIT_HINT         : 0x0

C:\$Users\$CENTUM>
```

図 C10.2.2-2 プロトコルドライバが正常に動作している状態

● 制御バスドライバのプロトコルドライバの場合（Windows 7、Windows Server 2012 R2、Windows Server 2008 R2）

制御バスドライバを追加すると、アダプタドライバと一緒にプロトコルドライバがインストールされます。

プロトコルドライバ「Yokogawa Vnet Protocol」は、デバイスマネージャーの [プラグアンドプレイではないドライバー] に表示されます。

プロトコルドライバが正常に起動しない場合、「！」マークがプロトコルドライバのアイコンに表示されます。

プロトコルドライバの表示方法は次のとおりです。

1. 管理者ユーザでログオンしてください。
 2. コントロールパネルを起動してください。
 3. [システムとセキュリティ] – [システム] – [デバイスマネージャー] を選択してください。
- デバイスマネージャーが表示されます。
4. メニューバーの [表示] – [非表示デバイスの表示] を選択してください。
- [プラグアンドプレイではないドライバー] にプロトコルドライバ「Yokogawa Vnet Protocol」が表示されます。

補足

ドライバのインストール直後に「Yokogawa Vnet Protocol」ドライバが表示されない場合は、コンピュータを再起動してください。

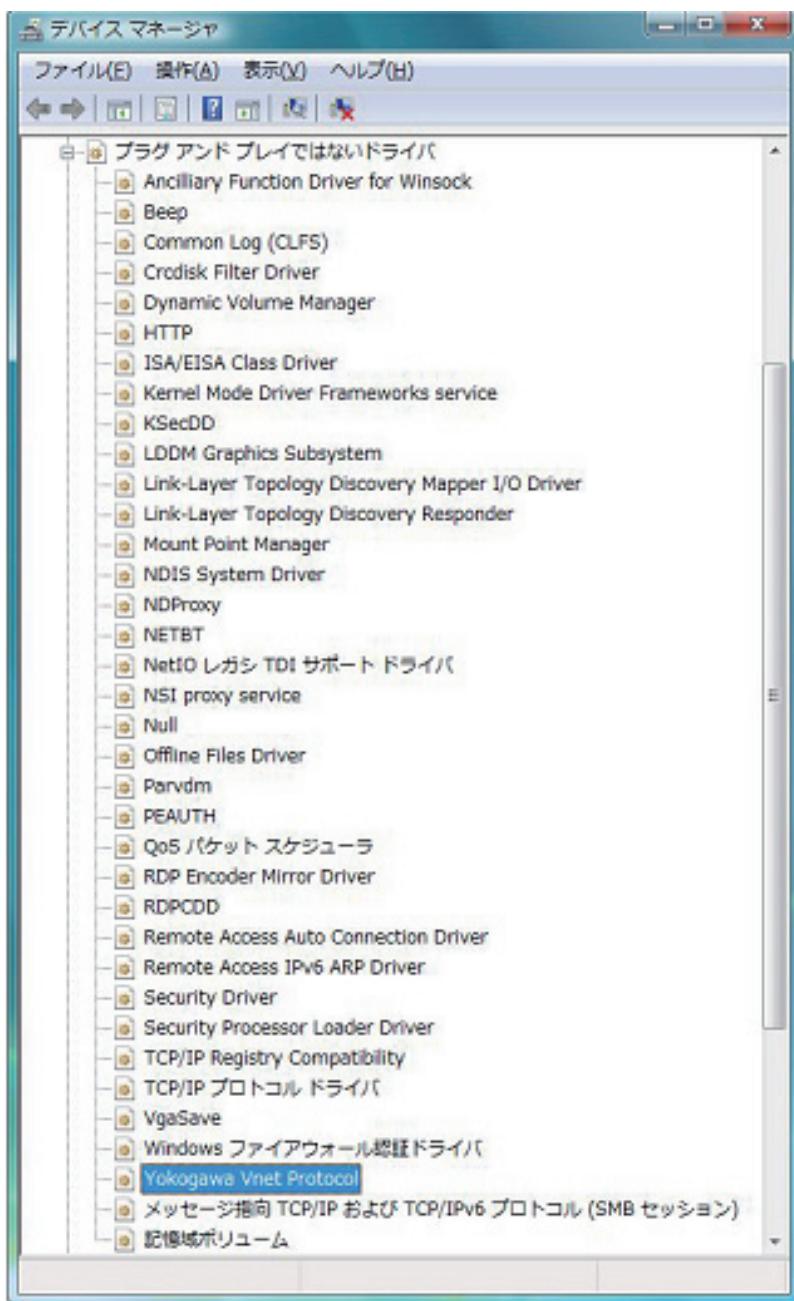


図 C10.2.2-3 プロトコルドライバが正常に動作している状態

● Vnet/IP オープン通信ドライバの場合

ドライバを追加すると、デバイスマネージャーのネットワークアダプタに「Vnet/IP Open Communication Driver (BUS2)」が表示されます。

ドライバが正常に起動しない場合、「！」マークがネットワークアダプタのアイコンに表示されます。

デバイスマネージャーの表示方法は次のとおりです。

1. 管理者ユーザでログオンしてください。
2. コントロールパネルを起動してください。
3. [システムとセキュリティ] – [システム] – [デバイスマネージャ] を選択してください。

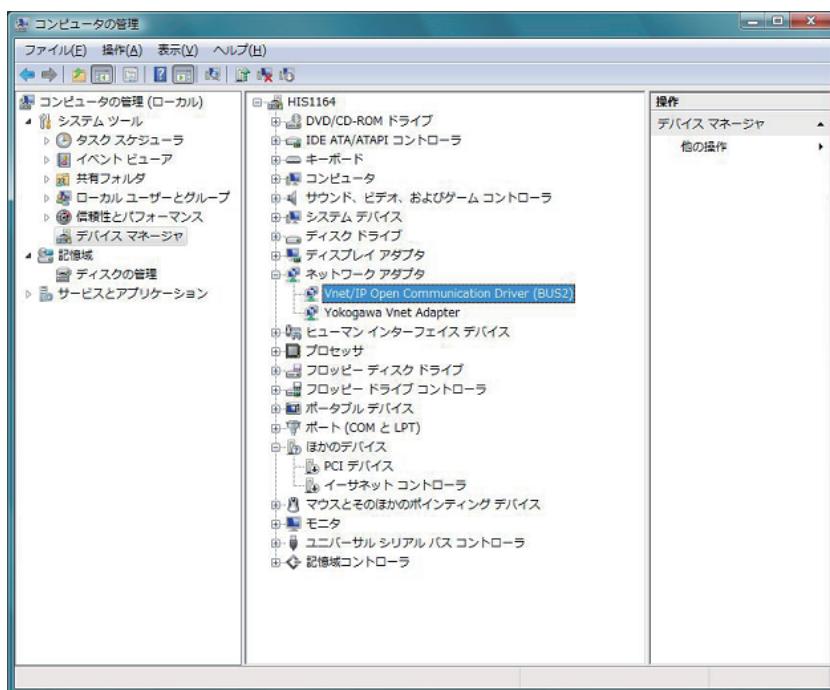


図 C10.2.2-4 アダプタドライバが正常に追加されている状態

■ 制御バスドライバのインストールに成功するが、ドライバが起動しない

制御バスドライバが正常に起動しない場合、バスの誤った接続やアドレス設定の間違いなどが考えられます。このときイベントビューアの「システム」ログに VLNIC のエラーが記録されます。

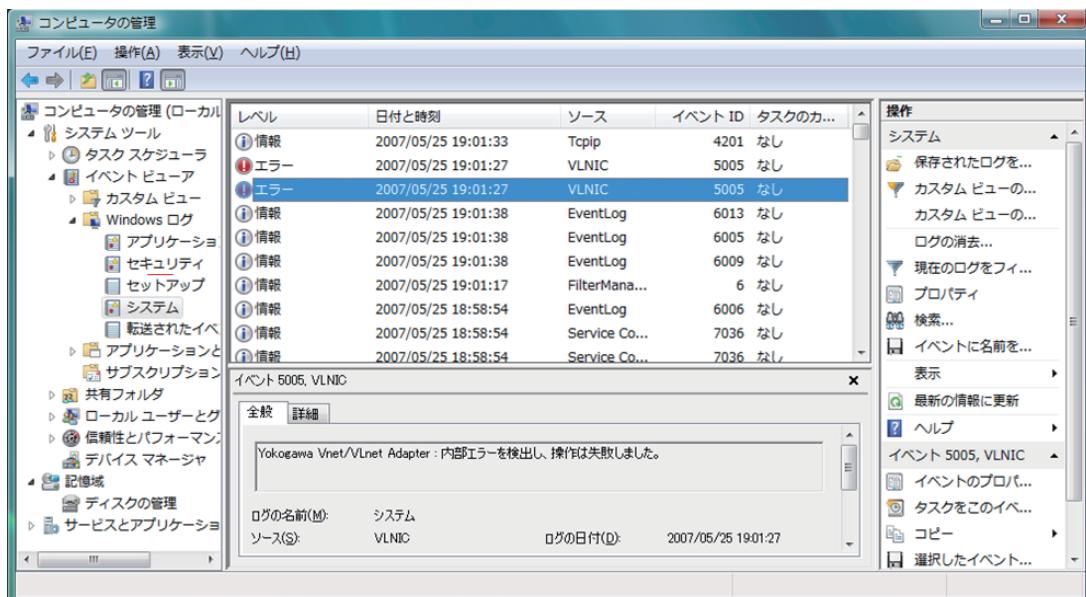


図 C10.2.2-5 VLNIC のエラーが記録されたイベントビューア（システム）

1. VLNIC のエラーをダブルクリックしてください。
イベントのプロパティが表示されます。

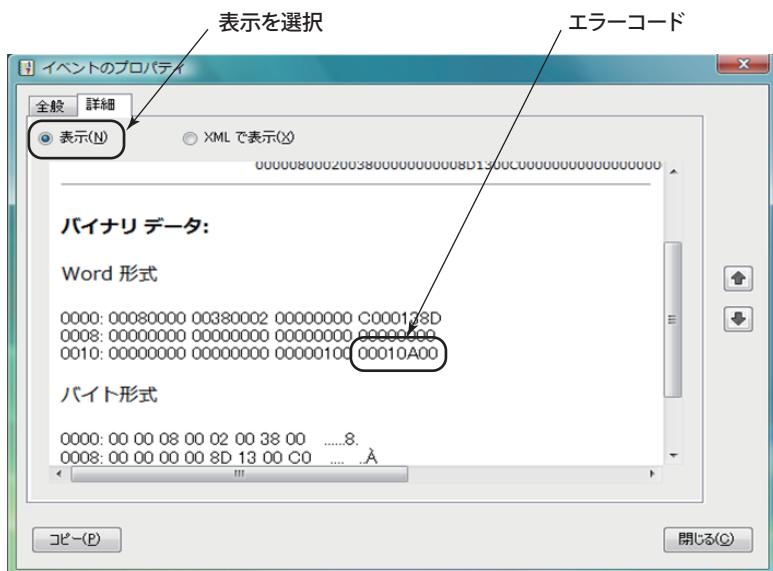


図 C10.2.2-6 イベントのプロパティ

2. 次の表よりエラーコードを調べ、バスの構成やアドレス設定の問題であれば、それらの設定が正しいことを確認し、コンピュータをシャットダウンしてください。その後、再度コンピュータを起動してください。

表 C10.2.2-1 ドライバ起動時発生するエラーコード

コード(*1)	意味
000101**	RAM パリティエラー (VF702/VF701/VI702 カードの故障)
000102**	RAM リード／ライトエラー (VF702/VF701/VI702 カードの故障)
000109**	アドレス重複エラー
00010a**	バス構成エラー (バスコネクタの接続の誤り)
00010b**	ディップスイッチステーション番号パリティエラー
00010c**	ディップスイッチドメイン番号パリティエラー
00010d**	ディップスイッチステーション番号不適合
00020013	ステーション番号不正 (バスコネクタの接続ミスの場合に検出されることがあります)

*1: コードの**は、VF702/VF701 で 00、VI702 では 2 衔の数になります。

そのほか、ドライバが起動しない場合は、制御バスインターフェースカードや Vnet/IP インタフェースカードが故障しているか、ほかのデバイスによる影響が考えられます。

制御バスインターフェースカードや Vnet/IP インタフェースカードを交換するか、ほかのデバイスをコンピュータから外してください。

- Vnet/IP オープン通信ドライバ削除後に Vnet/IP インタフェースカードをコンピュータから外さずにコンピュータを再起動した

Vnet/IP オープン通信ドライバ削除後に Vnet/IP インタフェースカードをコンピュータから外さずに再起動すると、Windows は Vnet/IP インタフェースカードを新規に追加されたデバイスだと判断し、ドライバのインストールに関するメッセージを通知します。このときの画面の指示は無視し、ドライバ追加の手順を実行しないでください。

■ インストーラの二重起動

インストーラの二重起動はできません。二重起動した場合は、警告ダイアログが表示されます。[OK] をクリックして、あとで起動したインストーラを終了してください。先に起動したインストーラの動作は継続されます。

■ ネットワークドライバインストール時にエラーメッセージが表示される —その1

ネットワークドライバインストール時に表示される「Windows セキュリティ」ダイアログで、[インストールしない] をクリックしたときに、エラーメッセージが表示された場合、次の操作をしてください。

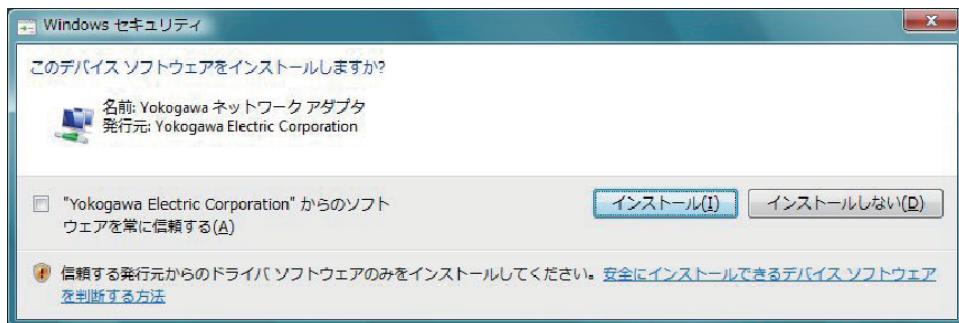


図 C10.2.2-7 Windows セキュリティダイアログ（ネットワークアダプタの場合）

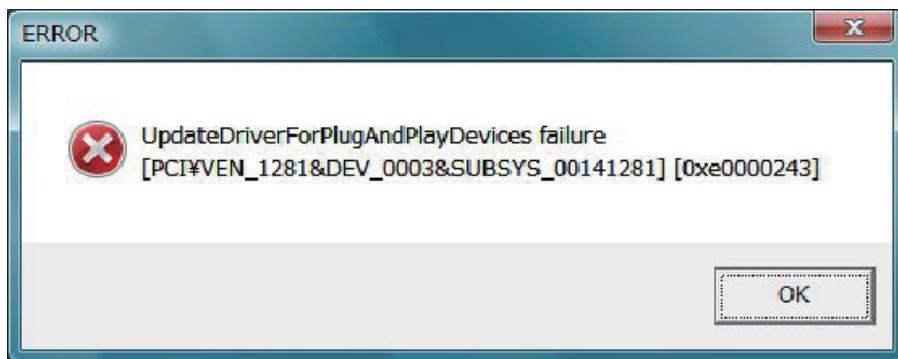


図 C10.2.2-8 エラーメッセージ（ネットワークアダプタの場合）

● 制御バスドライバの場合

- コンピュータを再起動後に、インストールメニューの [制御バスドライバ] をクリックしてください。
- 制御バスドライバを削除可能であれば削除し、コンピュータを再起動してください。
- 再度、ドライバをインストールしてください。

● Vnet/IP オープン通信ドライバの場合

再度インストーラを起動してください。

■ ネットワークドライバインストール時にエラーメッセージが表示される —その2

ネットワークドライバインストール時に表示される「Windows セキュリティ」ダイアログ（ネットワークプロトコルのインストール確認、ネットワークアダプタのインストール

確認) で、[インストールしない] をクリックしていないのにエラーメッセージが表示された場合、次の操作をしてください。

● 制御バスドライバの場合

1. コンピュータを再起動後にインストールメニューの [制御バスドライバ] をクリックしてください。
2. 次のいずれかの操作を行ってください。
 - ・ 制御バスドライバを削除可能であれば削除し、コンピュータを再起動してから再度ドライバをインストールしてください。
 - ・ 制御バスドライバの削除が不可能な場合は、コンピュータを再起動してから再度ドライバをインストールしてください。

● Vnet/IP オープン通信ドライバの場合

1. あらためてインストールメニューを起動し、[Vnet/IP オープン通信ドライバ]をクリックしてください。
2. 次のいずれかの操作をしてください。
 - ・ ドライバを削除可能であれば削除し、コンピュータを再起動してから再度ドライバをインストールしてください。
 - ・ ドライバの削除が不可能な場合は、コンピュータを再起動してから再度ドライバをインストールしてください。

■ ネットワークドライバインストール時にエラーメッセージが表示される —その3

これまで動いていた Ethernet が動作しなくなり、エラーが発生することがあります。

● 原因

- ・ ハードウェア、Ethernet アダプタカード、Ethernet ケーブルの接続ミス
- ・ ネットワークのバインドの設定の誤り
- ・ TCP/IP 通信の設定の誤り (IP アドレス、サブネットマスクなど)

● 対策

- ・ ハードウェア、Ethernet アダプタカード、Ethernet ケーブルのチェックしてください。
- ・ コントロールパネルの「ネットワークとダイヤルアップ接続」で設定をチェックしてください。

■ RIP Listener サービスの無効化に失敗する

RIP Listener サービスの無効化に失敗する場合があります。

● 発生条件

DCOM の [既定の認証レベル] が [なし] になっていると発生します。

補足

例えば、次のような場合に DCOM の [既定の認証レベル] が [なし] になっています。

- ・ セキュリティモデルを従来モデルに設定している。
- ・ 他のコンピュータと通信するために DCOM の [既定の認証レベル] を [なし] に設定している。

● 対策

次の手順で回避できます。

1. DCOM の [既定の認証レベル] を [なし] から [接続] に変更してください。
2. 対象の仮想マシンを再起動してください。
3. RIP Listener サービスをインストールまたはアンインストールしてください。

参照

DCOM の既定の認証レベルを変更する手順については、以下を参照してください。

「C10.1.2 サーバーマネージャーの起動時にエラーが発生する」ページ C10-4

C10.3 CENTUM 製品関連のトラブルシューティング

ここでは、CENTUM 製品に関するトラブル対応について説明します。

C10.3.1 実機 HIS の IP アドレスを変更してダウンロードした際にエラーが発生する

システムビューの HIS のプロパティからネットワークタブを選択し、[Ethernet TCP/IP ポートコル] にデフォルト以外を設定している場合、実機 HIS の IP アドレスを変更すると、ビルダからの HIS へのダウンロードがエラーになることがあります。この場合、次を実行してください。

1. ダウンロードエラーとなっている HIS に、管理者ユーザのアカウントで再度ログオンしてください。
2. 次のファイルをメモ帳などで開いて、コンピュータ名に対応した正しい IP アドレスに修正し、保存してください。
<CENTUM VP インストールフォルダ>\COMMON\ETC\lmhosts.cs
3. コンテキストメニューの [管理者として実行] でコマンドプロンプトを開き、次のコマンドを実行してください。
 - nbtstat -R (R は大文字) NetBIOS のキャッシュテーブル更新 (2.の修正を反映)
 - nbtstat -c (c は小文字) NetBIOS のキャッシュテーブル表示
4. 当該の HIS へプロジェクト共通項目をダウンロードできることを確認してください。
5. CTM_ENGINEER アカウントでログオンし、すべての HIS へプロジェクト共通項目をダウンロードしてください。

参照

すべての HIS へのプロジェクト共通項目のダウンロードの手順については、以下を参照してください。

エンジニアリング基本操作 (IM 33J10D20-01JA) の「A2.7 手順 7 定義した内容をダウンロードする」の「■ プロジェクト共通項目のダウンロード」

C10.3.2 リモート操作監視サーバに接続できない

リモート操作監視サーバ (HIS-TSE サーバ) に接続しようとしたときに、「クライアントをリモートコンピュータに接続できませんでした」というメッセージが表示されて接続できない場合、次の要因が考えられます。

- ネットワークカードのバインド順が Ethernet カードと制御バスインターフェースカードで逆になっている
コントロールパネルで、[ネットワークとインターネット] – [ネットワークと共有センター] を選択してください。ネットワークと共有センターウィンドウが表示されます。
[アダプターの設定の変更] を選択してください。ネットワーク接続ウィンドウが表示されます。
詳細設定メニューから [詳細設定] を選択してください。詳細設定ダイアログが表示されますので、Ethernet カードのバインドを先にしてください。

補足

詳細設定メニューが表示されないときは、Alt キーを押してください。

- リモートデスクトップサービス構成のネットワークアダプタの設定が不正
「リモートデスクトップサービス構成」の左側の [接続] を選択し、右側に表示される [RDP-Tcp] を右クリックして、[プロパティ] を選択してください。
「RDP-Tcp のプロパティ」ダイアログが表示されますので、「ネットワークアダプタ」タブの設定を Ethernet カードにしてください。
- HIS-TSE サーバがリモート接続を許可するようになっていない
[マイコンピュータ] を右クリックして [プロパティ] を選択してください。「システムのプロパティ」ダイアログが表示されます。リモートタブの [このコンピュータにユーザーがリモートで接続することを許可する] チェックボックスをオンにしてください。
- HIS-TSE サーバと HIS-TSE クライアントで Windows 更新プログラムの適用に違いがある
2018 年 3 月の Windows 更新プログラムの影響です。HIS-TSE サーバと HIS-TSE クライアントに、同じ Windows 更新プログラムを適用してください。同じ Windows 更新プログラムが適用できない場合は、HIS-TSE クライアントでローカルグループポリシーエディターの設定をしてください。
HIS-TSE クライアントのコマンドプロンプトで `gpedit.msc` と入力してローカルグループポリシーエディターを起動してください。左ペインで [コンピューターの構成] – [管理用テンプレート] – [システム] – [資格情報の委任] を選択し、右ペインの [暗号化オラクルの修復] で [有効] を選択し、[保護レベル] で [脆弱] を選択してください。

C10.3.3 操作監視機能稼動中に AIP262 (USB インタフェース付き AUX ボード) の USB ケーブルがコンピュータから抜けた

HIS が稼動中に、コンピュータ側または AUX ボード側の USB ポートから USB ケーブルが抜けた場合、システムアラームメッセージ（No.0241）が発生します。

この場合、USB ドライバのインストール時の接続ポートに USB ケーブルを再度接続し、コンピュータの再起動を行ってください。

保守時などで USB ケーブルを抜いたときには、必ずコンピュータ側接続ポートの元の位置に接続してください。

ドライバを前回インストールしたときのコンピュータ側接続ポートの位置が不明な場合は、コンピュータへのドライバの再インストールをしてください。

参照

ドライバの再インストールについては、以下を参照してください。

- ・「B4.4 オペレーションキーボード用 USB ドライバのインストールをする」ページ B4-79
- ・「B4.5 コンソール形 HIS の場合に必要な設定をする」ページ B4-81

C10.3.4 スタートメニューの AD オーガナイザのショートカットが消えた

1つのコンピュータに次の2つのライセンスが割り付けられている場合に、一方のライセンスを削除するとスタートメニューの AD オーガナイザのショートカットが削除されます。

- 論理 IO ポイント 4,000 以下の CENTUM VP エンジニアリング基本機能（形名：VP6E5100-V10N01 または VP6E5100-V10N02）
- ProSafe-RS 安全システムエンジニアリング・保守機能

この場合は、残っているライセンスを再配布することにより、スタートメニューに AD オーガナイザのショートカットが作成されます。ライセンスを再配布するときは次の手順に従ってください。

- ライセンスマネージャを起動してください。
- パッケージリストをエクスポートしてください。
- 対象ライセンス適用ステーションの該当ライセンスを削除してください。
- 対象ライセンス適用ステーションへライセンスを配布することで、ライセンスの削除を送信してください。
- 対象ライセンス適用ステーションで、ライセンスマネージャを起動して、ライセンスの変更を反映してください。
- ライセンスマネージャを起動してください。
- エクスポートしたパッケージリストをインポートしてください。
- 対象ライセンス適用ステーションへライセンスを配布してください。
- 対象ライセンス適用ステーションで、ライセンスマネージャを起動して、ライセンスの変更を反映してください。

参照

パッケージリストのエクスポートとインポートについては、以下を参照してください。

ライセンスマネージャ (IM 33J01C20-01JA) の「3.9.1 パッケージリストのインポートとエクスポート」

ライセンスの削除については、以下を参照してください。

ライセンスマネージャ (IM 33J01C20-01JA) の「3.2.1 ライセンス割り付けの変更」の「■ ライセンス適用ステーションからライセンスを削除する」

ライセンスの配布については、以下を参照してください。

ライセンスマネージャ (IM 33J01C20-01JA) の「3.2.2 変更されたライセンスの配布」

ライセンスの反映については、以下を参照してください。

ライセンスマネージャ (IM 33J01C20-01JA) の「3.2.3 変更されたライセンスの反映」

C11. バージョンアップ／レビューションアップ時の注意事項

ここでは、CENTUM VP をバージョンアップ／レビューションアップする場合の注意事項について説明します。

■ 本章の読み方

バージョンアップ／レビューションアップをする場合は、元となるバージョン／レビューションの次のバージョン／レビューションへの注意事項から順番に、最新レビューションまでのすべての注意事項を確認し、作業を行ってください。

たとえば R4.01.60 から R5.01.20 へバージョンアップする場合は、「C11.3 の R4.02.00 へのバージョンアップ／レビューションアップの注意事項」から「C11.8 の R5.01.20 へのバージョンアップ／レビューションアップの注意事項」まですべての作業を 1 つずつ行う必要があります。

C11.1 R4.01.33へのバージョンアップ／レビジョンアップ

R4.01.33へのバージョンアップ／レビジョンアップ時の注意事項について説明します。

■ グラフィックビューのデータ文字表示について

R4.01.33においてグラフィックビューのデータ文字表示を改善しました。その結果、バージョンアップすると、R4.01.33より前のレビジョンのときとデータ文字表示の表示位置が変わる場合があります。

CENTUM VP の R4.01.33 より前のレビジョンでは、グラフィックビューのデータ文字表示で表示データタイプにタグリストの指定をした場合、データ文字の表示桁数を 7 に固定していました。そのため、7 衡以上の桁数を持つデータ (SUM 値など) は、表示しきれずにアスタリスク表示 (******) になってしまいました。

R4.01.33 以降では、表示データタイプにタグリストの指定をした場合、タグリストから表示する桁数のデータを取り出して表示します。そのため、表示しきれないということはなくなります (以降の説明では、「R4.01.33 以降の本来の仕様」とします)。しかし、バージョンアップする前と、バージョンアップしたあとでは、表示桁数が固定から非固定になることで、表示位置が変わることがあります。

補足

表示桁数が 7 以外のデータを示します。

- 機能ブロックで共通の AFLS、AF、ALRM、AOFS、MODE、RAW、SUM、VN、BSTS
- 演算ブロックの RV、RVnn
- FUNC-VAR の Xnn、Ynn
- BDSET、BDSET-1C、BDSET-2、BDSET-2C、BDSET-1L、BDSET-2L、BDA、BDA-C の DTnn、DHnn、DLnn
- SEBOLP1～P3 の CHnn、DTnn
- SFC、UNIT のユーザ定義のデータアイテム

■ バージョンアップ後にデータ文字の表示位置が変わる場合

次に示す (条件 1) が成立し、(条件 2) は成立しない場合、バージョンアップ後に表示位置が変わります。

次のデータ文字表示タブは、データ文字表示のプロパティダイアログにあります。

(条件 1)

次の条件にすべて当てはまれば、成立となります。

- データ文字表示タブで、[拡張位置指定の使用] のチェックボックスがオンになっている
- データ文字表示タブで、[表示フォーマット] の [タイプ] で [タグリスト] が選択されている
- タグリストの表示桁数が 7 以外になっている

(条件 2)

次の条件のいずれかに当てはまれば、成立となります。

- データ文字表示タブで、[整列] に [左寄せ] が選択されており、[工業単位の表示] のチェックボックスがオフになっている
- データ文字表示タブで、[整列] に [左詰め] が選択されている
- データ文字表示タブで、[整列] に [両端寄せ] が選択されており、[工業単位の表示] のチェックボックスがオフになっている

■ バージョンアップ後にデータ文字の表示位置が変わる場合の対応

バージョンアップ後にデータ文字の表示位置が変わることへの対応として、R4.01.33より前のデータ文字表示の仕様（R4.01.00と同じ仕様）をレジストリで選択できます。

- レジストリ=0：R4.01.33以降の本来の仕様（デフォルトの設定です）
- レジストリ=1：R4.01.33より前の仕様（R4.01.00と同じ仕様）

次に、[拡張位置指定の使用]がオンになっている場合の表示を、次の分類で示します。

- R4.01.33より前の仕様と、R4.01.33以降でR4.01.33より前の仕様（R4.01.00と同じ仕様）を選択した場合（レジストリ=1）
- R4.01.33以降の本来の仕様を選択した場合（レジストリ=0）

重要

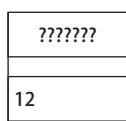
データ文字表示で表示データタイプにタグリストを指定した場合、表示桁数は実行時に決まります。

グラフィックビルダでデータ文字の定義をしたあと、タグリストの表示桁数が変更されるビルダ操作があった場合、データ文字の表示領域はグラフィックビルダでの定義時より大きくなる可能性があります。拡張位置指定の場合、表示領域は左基準で大きくなります。グラフィックビルダでの定義時は、これらのこと考慮して行ってください。

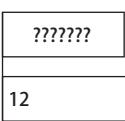
- R4.01.33より前の仕様
- R4.01.33以降で、R4.01.33より前の仕様を選択（レジストリ=1）(*1)

- R4.01.33以降の本来の仕様を選択（レジストリ=0）

左寄せ
左詰め



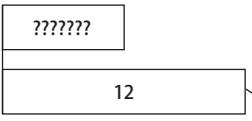
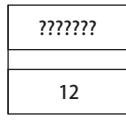
表示桁数 = 7(固定)



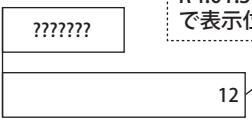
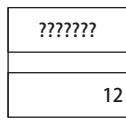
← 上段:ビルダでの設定

表示桁数 = 16の場合(タグリストに持っている表示桁数)

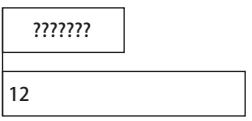
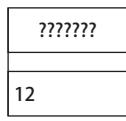
中央揃え



右寄せ
右詰め
中央詰め



両端寄せ



タグリスト指定しても7桁表示になる。
8桁以上のデータの場合、数字データでは
アスタリスク表示（*****）になり、
文字列データでは文字が切り捨てられて
表示される。

*1：レジストリ=1にすると、「拡張位置指定の使用」の
チェック有無にかかわらず、表示桁数=7になります。

図 C11.1-1 ビルダ設定時と実行時の位置の対応－工業単位なし

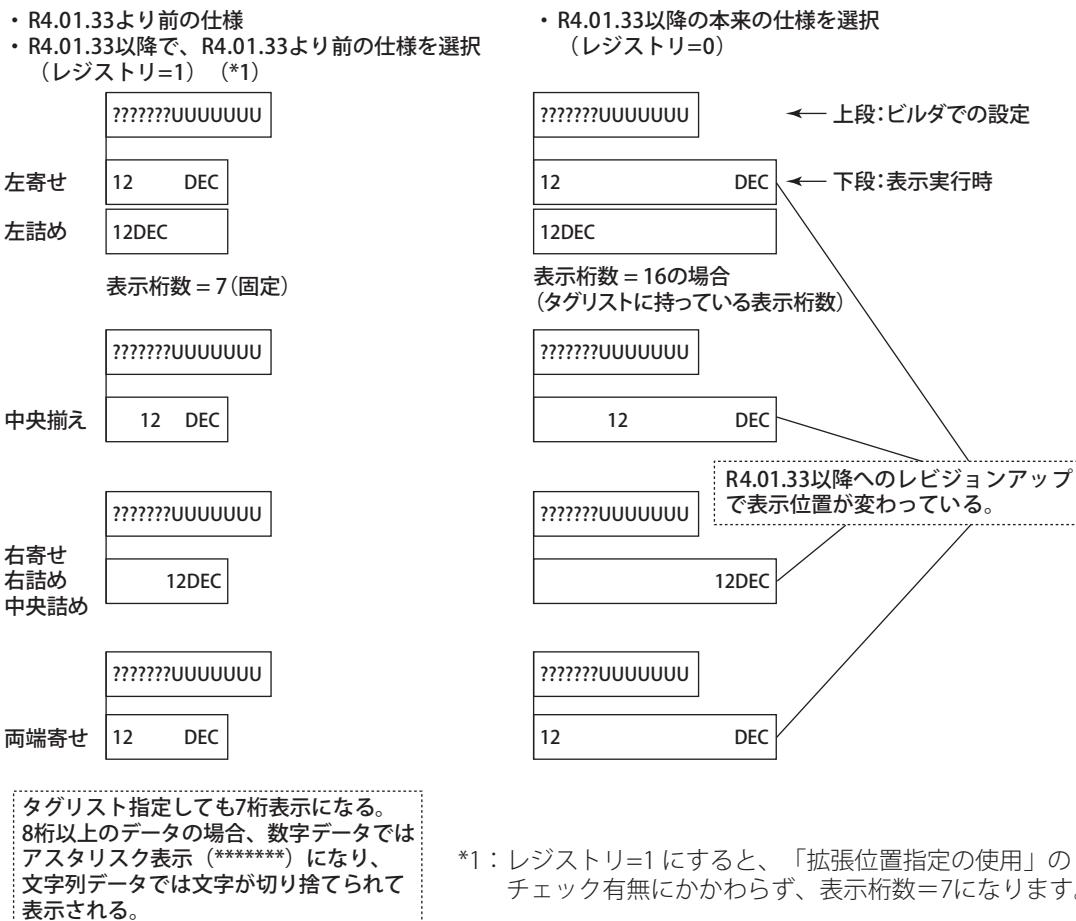


図 C11.1-2 ビルダ設定時と実行時の位置の対応－工業単位あり

参照

R4.01.00 互換機能サポートのレジストリ設定については、以下を参照してください。

「C11.1.2 R4.01.00 互換機能サポートのレジストリ設定について」ページ C11-8

■ データ文字表示についての各レビジョンでの問題点への対応方法

データ文字表示の表示桁数と表示位置の問題点についての対応方法を、次のとおり分けて次の表で示します。

- R4.01.33 より前のレビジョン (R4.01.00 の仕様) の場合
- R4.01.33 以降で、R4.01.33 以降の本来の仕様 (レジストリ=0) を選択した場合
- R4.01.33 以降で、R4.01.00 と同じ仕様 (レジストリ=1) を選択した場合

表 C11.1-1 各レビジョンでの問題点への対応方法

レビジョン	問題点	
	表示桁数： 7桁固定のため、8桁以上表示できない	表示位置： R4.01.33 より前のレビジョンと比べて、表示位置が変わる
R4.01.33 より前 (R4.01.00 の仕様)	タグリスト指定を使わずに他の方法で 対応してください。	— (該当しない)

次に続く

表 C11.1-1 各リビジョンでの問題点への対応方法（前から続く）

リビジョン	問題点	
	表示桁数： 7桁固定のため、8桁以上表示できない	表示位置： R4.01.33より前のリビジョンと比べて、表示位置が変わる
R4.01.33 以降 レジストリ=0 (R4.01.33 以降の 本来の仕様)	— (該当しない) 注：タグリストに持っている表示桁数 で表示します。	<ul style="list-style-type: none"> 稼動中のシステムやテスト済みシステムで、 ビルダ作業を今後行わない場合 (*1) R4.01.00 と同じ仕様（レジストリ=1）に設定 してください。 注：表示桁数は常時 7 桁になります。表示が 7 桁で問題ないか確認が必要です。 ビルダ作業が今後もある場合 [拡張位置指定の使用] チェックボックスをオ フにしてください。または、タグリスト指定 を使わずに他の方法で対応してください。
R4.01.33 以降 レジストリ=1 (R4.01.00 と同じ 仕様)	タグリスト指定を使わずに他の方法で 対応してください。	— (該当しない) 注：R4.01.00 の仕様になります。

*1：表示位置の問題の対応をすでに別途行っていて、グラフィックビルダでの設定の変更が困難なシステム
を含みます。

補足

現在エンジニアリング中のシステムについては、R4.01.33 以降の本来の仕様（レジストリ=0）に従い、データ
文字表示の設定をしてください。

データ文字表示に R4.01.00 と同じ仕様を採用するには、本リビジョンアップソフトウェア
のインストール後、R4.01.00 互換機能サポートのレジストリ設定についての手順を実行し
てください。

参照

R4.01.00 互換機能サポートのレジストリ設定については、以下を参照してください。

「C11.1.2 R4.01.00 互換機能サポートのレジストリ設定について」ページ C11-8

C11.1.1 該当事項への対応作業

次の事項に該当する場合に、その作業を実行してください。

■ 操作監視機能が動作するコンピュータの未使用 Ethernet カードについての対応

操作監視機能が動作するコンピュータに 2 枚以上の Ethernet カードを実装する場合、未使用の Ethernet カードについては、次の手順によりネットワークのプロパティに「無効」を設定してください。設定には管理者権限が必要です。

● Windows XP/Windows Server 2003 の場合

- スタートメニューから [コントロールパネル] – [ネットワーク接続] を選択してください。
ネットワーク接続ウィンドウが表示されます。
- 未使用の Ethernet を右クリックし、[無効にする] を選択してください。

● Windows Vista/Windows Server 2008 の場合

- スタートメニューから [コントロールパネル] – [ネットワークとインターネット] – [ネットワークと共有センター] を選択してください。
ネットワークと共有センターウィンドウが表示されます。
- [ネットワーク接続の管理] を選択してください。
ネットワーク接続ウィンドウが表示されます。
- 未使用の Ethernet を右クリックし、[無効にする] を選択してください。

■ Windows Server 2008 に HIS をインストールした場合の対応

Windows Server 2008 に操作監視機能をインストールした場合、次の設定をしてください。設定には管理者権限が必要です。

- スタートメニューから [コントロールパネル] – [システム] を選択してください。
システムのプロパティウィンドウが表示されます。
- [詳細設定] タブを選択し、[パフォーマンス] の [設定] をクリックしてください。
パフォーマンスオプションダイアログが表示されます。
- [詳細設定] タブを選択し、[プロセッサのスケジュール] の中の [プログラム] を選択してください。

■ プライマリダイレクトボタンのデザイン変更についての対応

チューニングウィンドウのツールバーにあるプライマリダイレクトボタンのデザインが次のとおり変更されます。



図 C11.1.1-1 デザイン変更

デザインの変更は、次のファイルをエクスプローラでダブルクリックすることで行えます。ボタンのデザインは次回にチューニングウィンドウを呼び出した際に変更されます。

- CENTUM VP R4.01.33 より前の旧デザインに戻す場合
<CENTUM VP インストールフォルダ>\his\tool\OldPRDIcon.reg
- 新デザインにする場合

<CENTUM VP インストールフォルダ>\his\tool\NewPRDIcon.reg

■ FIO のアナログ出力モジュール（電流出力のみ）についての対応

FIO のアナログ出力モジュール（電流出力のみ）について、IOM ビルダで次のとおり定義をしている場合、入出力モジュールへのダウンロードを実行してください。

- ・ [逆ぶれあり] としている
- ・ [OOP クリア] を「なし」としている

C11.1.2 R4.01.00 互換機能サポートのレジストリ設定について

R4.01.33 以降で、データ文字表示（拡張位置指定の使用、表示データタイプにタグリストを指定）に R4.01.00 と同じ仕様を採用するには、バージョンアップ作業後、システム内の各 HIS でデータ文字表示の仕様変更用レジストリを設定してください。

補足

ここでは、「R4.01.33 以降へのレビューションアップ時の注意事項」の「グラフィックのデータ文字表示で拡張位置指定の使用と表示データタイプにタグリストを指定してある場合、レビューションアップで表示位置が変わってしまうことがある」ことについての一つの対応策を説明しています。

重要

R4.01.00 と同じ仕様を採用すると表示桁数が 7 桁固定となります。7 桁を超えるデータ（SUM 値など）のとき、数字データではアスタリスク表示（*****）になったり、文字データでは文字の一部が表示されなくなったりします。
表示桁数が 7 桁を超えることがない、または 7 桁を超えて問題ないことを確認してください。

次にデータ文字表示の仕様変更用レジストリ設定の手順を示します。

R4.01.00 と同じ仕様を採用するには、管理者ユーザの権限で次を実行してください。

1. Windows エクスプローラで<CENTUM VP インストールフォルダ>HISYtool を開き、SetAdvancedAlignmentR40100CompatibleR40126.reg をダブルクリックしてください。
R4.01.00 と同じ仕様にするためのレジストリ=1 が設定されます。

補足

R4.01.33 以降の本来の仕様に戻すには、管理者ユーザの権限で次を実行してください。

Windows エクスプローラで<CENTUM VP インストールフォルダ>HISYtool を開いて、ResetAdvancedAlignmentR40100CompatibleR40126.reg をダブルクリックしてください。

R4.01.33 以降の本来の仕様にするためのレジストリ=0 が設定されます。

2. コンピュータを再起動してください。

補足

データ文字表示の仕様変更用レジストリ（IsNumberOfDigitTypeCheck）の設定データは、インストール時には前回値が保持されます。レビューションアップなどで再インストールしたとき、再設定する必要はありません。

C11.2 R4.01.60 へのバージョンアップ／リビジョンアップ

CENTUM VP R4.01.33 から R4.01.60 へのリビジョンアップをして R4.01.60 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R4.01.33 から R4.01.60 にリビジョンアップする場合です。

R4.01.33 より前のリビジョンから R4.01.60 にリビジョンアップ／バージョンアップする場合、これより前に説明した各リビジョン間でのリビジョンアップ／バージョンアップ時の注意も併せてお読みください。

C11.2.1 グラフィックビューのブリンクについての注意事項

R4.01.60 でグラフィックビューのブリンクの仕様が変わっています。

■ ブリンク仕様の違いの説明

グラフィックビューのオブジェクトがブリンク状態のとき、ブリンク OFF の瞬間(*1)でのオブジェクトの色の仕様が R4.01.60 で変更になります。

*1: オブジェクトがブリンク状態のときのブリンク OFF の瞬間とは、点滅動作のうちの「滅」の時点のことです。

- R4.01.60 より前のレビュー
ブリンク OFF の瞬間でのオブジェクトの色は、透明色です。
- R4.01.60 以降のレビュー
ブリンク OFF の瞬間でのオブジェクトの色は、キャンバス色です。

次に、R4.01.60 以降でのコンポーネントごとのブリンク OFF の瞬間ににおける表示の振る舞いを示します。

表 C11.2.1-1 R4.01.60 以降のブリンク OFF での表示の振る舞い

コンポーネント名	ブリンク OFF での表示の振る舞い	備考
線	ラインの色がキャンバス色になります。	
弧	ラインの色がキャンバス色になります。	
ポリライン	ラインの色がキャンバス色になります。	
ペンツール	ラインの色がキャンバス色になります。	閉じた描画の場合、塗りつぶしがキャンバス色になります。
矩形	塗りつぶしがキャンバス色になります。	塗りつぶしが透明の場合、ラインの色がキャンバス色になります。
フィルエリア	塗りつぶしがキャンバス色になります。	塗りつぶしが透明の場合、ラインの色がキャンバス色になります。
扇	塗りつぶしがキャンバス色になります。	塗りつぶしが透明の場合、ラインの色がキャンバス色になります。
橢円	塗りつぶしがキャンバス色になります。	塗りつぶしが透明の場合、ラインの色がキャンバス色になります。
円	塗りつぶしがキャンバス色になります。	塗りつぶしが透明の場合、ラインの色がキャンバス色になります。
マーカー	マーカーでハイライトしたところが透明になります。	
テキスト	テキストの色がキャンバス色になります。	
データ円バー	前景部がキャンバス色になります。	
データ矢印バー	矢印が透明になります。	
データ矩形バー	前景部がキャンバス色になります。	
データ文字	テキストの色がキャンバス色になります。	
押しボタン	背景部がキャンバス色になります。	

C11.2.2 グラフィックにおける動作の選択

CS 1000/CS 3000 で作成したグラフィックのコントロールに対し、次のような動作の選択ができます。

- ・ 透明が指定されたコントロールのモディファイ条件成立時の動作
- ・ テキストコントロールまたはデータ文字表示コントロールで、背景色に [透明] が指定され、モディファイ操作に [反転] が指定されている場合の動作
- ・ テキストコントロールまたはデータ文字表示コントロールで、モディファイ操作に [ブリンク] と [反転] が同時に指定されている場合の動作

この選択を行った場合、プロジェクト共通部をすべての HIS にダウンロードしてください。

参照

グラフィックにおける動作の選択については、以下を参照してください。

エンジニアリングリファレンス Vol.2 (IM 33J10D11-01JA) の「7.22.2 グラフィックにおける動作の選択」

C11.2.3 操作監視ウィンドウの表示枚数

バージョンアップすると、操作監視ウィンドウの表示枚数はデフォルトの設定になります。

表示枚数の設定を変更する場合は、システムの動作環境に見合った設定をしてください。

参照

操作監視ウィンドウの表示枚数の詳細については、以下を参照してください。

操作監視リファレンス Vol.2 (IM 33J05A11-01JA) の「10.5 複数モニタ環境の設定」の「■ HIS 設定ウィンドウの複数モニタに関する設定」の「● 画面操作モードとウィンドウ数に関する設定」

C11.2.4 複数モニタパッケージを使用している場合

複数モニタパッケージを使用している場合の注意事項を次に示します。

■ HIS 設定ウィンドウの設定

R4.01.60 より前のレビューにおいて、HIS 設定ウィンドウの次のいずれかの設定項目を変更している場合、バージョンアップしたとき、その設定項目には初期値が設定されます。必要に応じて設定を変更してください。

- ディスプレイタブシートの [操作画面モード] の [ウィンドウモード] の [コンテナウインドウ数] (*1)
- ディスプレイタブシートの [操作画面モード] の [フルスクリーンモード] の [ポップアップウインドウ数] (*2)

*1: 初期値=5 です。

*2: 初期値=2 です。

補足

ウインドウモードのコンテナウインドウ数と、フルスクリーンモードのポップアップウインドウ数は、R4.01.60 より前のレビューでは、1 台のモニタに対しての数として扱っていましたが、R4.01.60 以降では 1 台の HIS に対しての数として扱うようになりました。この違いの対応として、R4.01.60 以降へのレビューアップでは、これらの設定項目に初期値を設定しています。

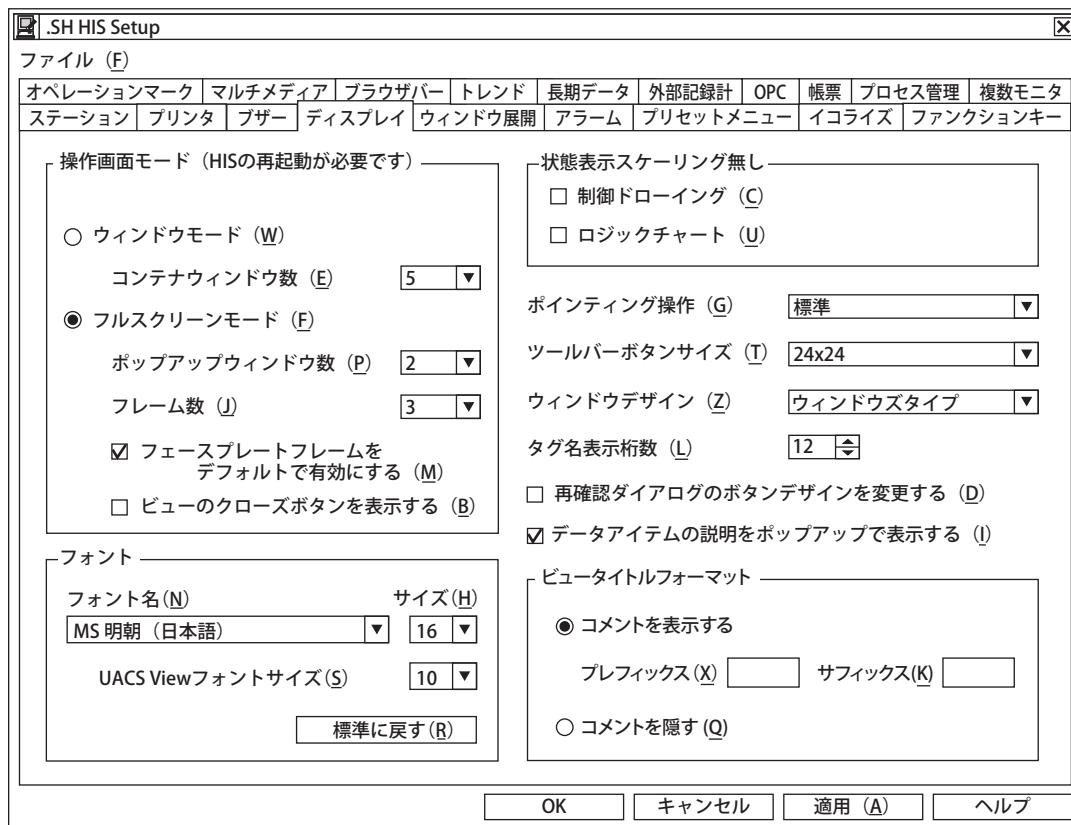


図 C11.2.4-1 HIS 設定ウィンドウのディスプレイタブシート

参照

コンテナウインドウ数または、ポップアップウインドウ数（操作画面モード）の設定については、以下を参照してください。

操作監視リファレンス Vol.1 (IM 33J05A10-01JA) の「4.3.4 ディスプレイタブシート」の「■ ディスプレイタブシートでの設定内容」

■ システムファンクションキーによるウィンドウコピーと同一画面の呼び出し

システムファンクションキーによるウィンドウコピー（CPYn）と、同一画面の呼び出しが変更になりました。

参照

ウィンドウコピー（CPYn）については、以下を参照してください。

操作監視リファレンス Vol.2 (IM 33J05A11-01JA) の「9.2.3 システムファンクションキーの実行を割り付ける場合の定義」の「■ 複数モニタパッケージが有効な場合のシステムファンクションキー」の「● ウィンドウコピー（CPYn） n=1~4」

同一画面の呼び出しへについては、以下を参照してください。

操作監視リファレンス Vol.2 (IM 33J05A11-01JA) の「10. 複数モニタ」の「■ 複数モニタの概要」の「● 同一画面の呼び出し」

C11.2.5 ビューの更新周期

ビューの更新周期が変更になりました。

参照

ビューの更新周期の詳細については、以下を参照してください。

操作監視リファレンス Vol.1 (IM 33J05A10-01JA) の「2.2 操作画面モード」の「■ ビューの更新周期の確定」

C11.2.6 グラフィックのタグオブジェクトを示す枠の色

グラフィックビルダで [タグオブジェクトを有効にする] を指定したコンポーネントを、グラフィックビューで選択すると、選択中であることを示す枠が表示されます。この枠の色は、R4.01.60 より前のレビューではオレンジでしたが、R4.01.60 以降は緑になります。

この枠の色は、R4.02.00 以降では、他の色にも変更できます。

参照

枠の色の変更については、以下を参照してください。

「● グラフィックのタグオブジェクトを示す枠の色」ページ C11-20

C11.2.7 グラフィックの押しボタンとソフトキーにガードが付いた場合の操作禁止枠の色

グラフィックの押しボタンとソフトキーにガードが付いた場合の操作禁止枠の色は、R4.01.60より前のレビューでは黒でしたが、R4.01.60以降は白になります。

C11.2.8 グラフィックビューでのコントロールの動作についての注意事項

グラフィックビルダで次のコントロールに、メニューダイアログの呼び出し、ウィンドウ呼び出し、などの機能設定がしてあるとき、該当する次の入力必須のパラメータが正しく設定されていない場合の、グラフィックビュー呼び出し時の動作を改善しました。これらのコントロールは表示されなくなります。

(該当コントロール)

- ・ 押しボタン
- ・ タッチターゲット
- ・ ソフトキー
- ・ オーバビュー

(該当入力必須のパラメータ)

- ・ 機能タブシート [メニューダイアログの呼び出し] におけるメニュー設定のラベル、またはデータ
- ・ 機能タブシート [ウィンドウ呼び出し] におけるパラメータ
- ・ 機能タブシート [計器指令操作] におけるデータ
- ・ 機能タブシート [ファイル名によるプログラムの実行] におけるプログラム名
- ・ 機能タブシート [データ入力ダイアログの呼び出し] におけるデータ
- ・ 機能タブシート [データアイテム依存のメニューダイアログ] におけるデータ
- ・ 機能タブシート [パネルセットの実行] におけるパネルセット名
- ・ 機能タブシート [その他] におけるパラメータ

C11.3 R4.02.00 へのバージョンアップ／リビジョンアップ

CENTUM VP R4.01.60 から R4.02.00 へのリビジョンアップをして R4.02.00 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R4.01.60 から R4.02.00 にリビジョンアップする場合です。

R4.01.60 より前のリビジョンから R4.02.00 にリビジョンアップ／バージョンアップする場合、これより前に説明した各リビジョン間でのリビジョンアップ／バージョンアップ時の注意も併せてお読みください。

■ ビルダ

ビルダに関する注意事項を次に示します。

● 伝送速度の設定

CENTUM VP R4.02.00 より、通信モジュールの ALR111/121 のプロパティダイアログで設定可能な伝送速度の指定が、38400 bps 以下に限定されます。

既存プロジェクトすでに 57600 bps 以上を選択しているプロジェクトでは、CENTUM VP R4.02.00 にリビジョンアップ後にモジュールのプロパティダイアログを開くと、設定値がチェックされ、範囲外であるとエラーになりますので、注意してください。

なお、既存プロジェクトで、すでに範囲外の値を設定している場合、プロパティダイアログを開かないかぎり、R4.02.00 以降でも、そのままの伝送速度で動作します。

● FF フェースプレートブロックと FCS 機能ブロックのデータ結合について

CENTUM VP R4.01.60 で、FF フェースプレートブロックと FCS 機能ブロックをデータ結合してジェネレーションを行うと、ワーニングが発生し、結合情報が失われた状態で FCS などにダウンロードされ、アプリケーションが正しく動作しません。

このような場合、R4.02 インストール作業のあとに、次の操作をしてください。

1. 制御ドローイングビルダを起動してください。
2. ワーニングが発生している結合の FF フェースプレートブロックのプロパティを開き、[OK] をクリックしてください。
制御ドローイング内に複数存在する場合は、いずれか 1 つのブロックに対してこの操作を実施してください。
3. 制御ドローイングビルダで、[ファイル] – [ダウンロード] を実行してください。
正しい結合情報が生成され、FCS、ALF111、機器に正しい情報がダウンロードされます。
4. すべての該当する制御ドローイングシートに対して、同じ操作を行ってください。

■ 操作監視機能

操作監視機能に関する注意事項を次に示します。

● グラフィックのデータ文字表示でのゼロリーディング

データ文字表示の表示フォーマットに次の設定をした場合、R4.01.00 ではゼロリーディングされませんでしたが、R4.02.00 からはゼロリーディングされます。

表 C11.3-1 グラフィックのデータ文字表示でのゼロリーディング

設定項目	設定パターン1	設定パターン2
拡張位置指定の使用	チェックなし	チェックなし
タイプ	数値、パーセント、16進	タグリスト（16進タイプ）
整列	指定なし	指定なし、右寄せ
ゼロリーディング	チェック	-

● グラフィックのタグオブジェクトを示す枠の色

グラフィックで、[タグオブジェクトを有効にする] を指定したコンポーネントを選択すると、選択中であることを示す枠が表示されます。R4.01.60 より前のリビジョンではこの枠の色がオレンジでしたが、R4.01.60 以降はデフォルトで緑色になります。

このタグオブジェクトを示す枠の色を別の色に変更するには、HIS ごとに次の手順で変更してください。また、複数の HIS に同じフレーム色を定義する場合、補足にある複数 HIS への設定の適用方法を参照してください。

- 管理者ユーザでログオンしてください。
- プログラムフォルダ C:\Program Files\YOKOGAWA\IA\iPCS\Products\CENTUMVP\Program\にある、ファイル Yokogawa.IA.iPCS.Platform.View.Graphic.Utility.FrameColorSettingTool.exe をダブルクリックしてください。
フレーム色を変更するツールが起動します。

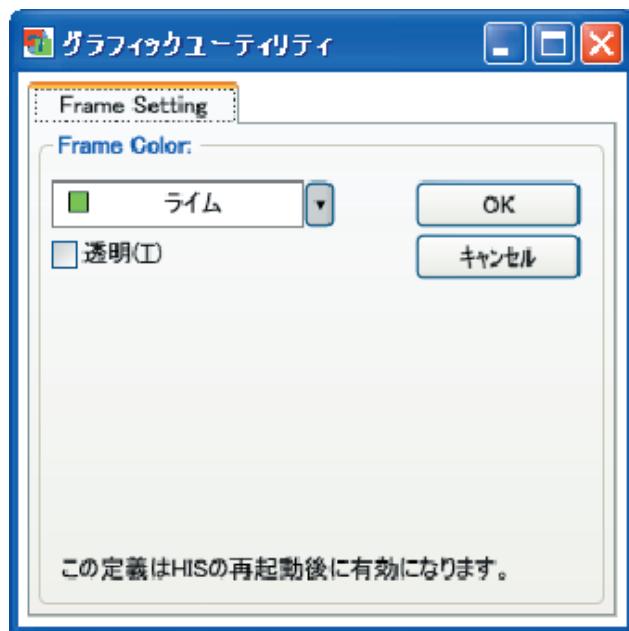


図 C11.3-1 グラフィックユーティリティ

選択色テキストボックスには現在選択されている色が表示されます。名前が付いている色を選択した場合、色の名前が表示されます。そうでない場合は、16進数で表示されます（例#FF123456）。このテキストボックスには直接入力できません。

- カラーピッカーボタンをクリックすると、カラーピッカーツールチップが表示されますので、色を選択してください。



図 C11.3-2 カラーピッカー

[他の色] を選択した場合、色の設定ダイアログが表示されます。



図 C11.3-3 色の設定ダイアログ

これによりカスタムカラーを選択することができます。

また、タグオブジェクトを示す枠の色を透明にするには、[透明] チェックボックスをオンにしてください。

4. 色の選択が終わったら、[OK] を選択してください。

これにより選択した色がファイルに保存され、次のメッセージが表示されます。

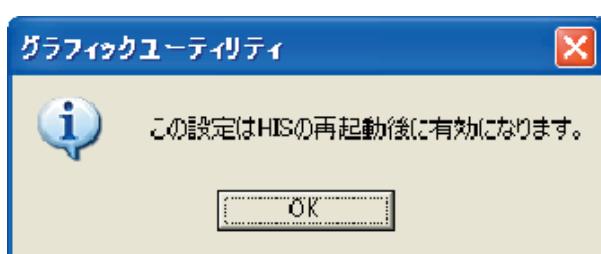


図 C11.3-4 再起動を確認するメッセージ

5. HIS を再起動してください。

補足

複数の HIS で同じ設定を使用する場合は、定義ファイルをコピーすることでも設定を反映できます。
定義ファイル：

<All Users Application data>\Yokogawa\IA\iPCSY\Products\CentumVP\Graphic\Config\UserConfig.xml
定義ファイルを同じフォルダ階層にコピーしたあと、HIS を再起動してください。

■ FCS 機能

FCS に関する注意事項を次に示します。

● CALCU 入出力データの正規化機能

R4.02.00 の仕様改訂における、仕様の変更点は次のとおりです。

表 C11.3-2 CALCU 入出力データの正規化機能

	R4.01.60	R4.02.00
非差分型データのリミット処理	正規化データとして 1-0 の範囲内に制限します。	正規化データとして±1 の範囲内に制限します。
CPV=RV の機能	機能しません。	機能します。
レンジ上下限値自身のデータ	演算式内で正規化データとして扱います。	演算式内で実量データとして扱います。

非差分型データのリミット処理および、CPV=RV の機能を R4.02.00 の仕様で動作させるためには、バージョンアップ後に FCS へのオフラインダウンロードが必要です。

レンジ上下限値自身のデータの扱いを R4.02.00 の仕様にするためには、バージョンアップ後の FCS へのオフラインダウンロードに加え、制御ドローイングビルダ (*1)からのダウンロード（ジェネレーション）が必要です。

*1：制御ドローイングビルダでの操作は、ビルダを起動してダウンロードするのみで編集は不要です。

■ 通信機能

通信機能に関する注意事項を次に示します。

● 制御バスドライバ

Windows Vista または Windows Server 2008 で CENTUM VP R4.02.00 以降の制御バスドライバを使用するためには、修正モジュール（KB971060）の適用が必要です。

修正モジュール（KB971060）は、CENTUM VP R4.02.00 以降の CENTUM VP インストーラで適用されます。

C11.4 R4.02.30 へのバージョンアップ／レビジョンアップ

CENTUM VP R4.02.00 から R4.02.30 へのレビジョンアップをして R4.02.30 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R4.02.00 から R4.02.30 にレビジョンアップする場合です。

R4.02.00 より前のレビジョンから R4.02.30 にレビジョンアップ／バージョンアップする場合、これより前に説明した各レビジョン間でのレビジョンアップ／バージョンアップ時の注意も併せてお読みください。

■ ユニットの移行条件について

R4.02.30 では、R4.02.30 より前のレビジョンで発生する次の問題点を解消しました。

- ユニットの移行条件に 8 文字の文字列長を持つデータアイテム名を定義している場合、FCS で移行条件の判定が正しく動作しません。
上記のような問題が発生するケースに該当する場合、問題を解消するために R4.02.30 のインストール作業のあとに次の操作をしてください。

● ユニットプロシージャ、またはユニット処方のダウンロード

前に述べた移行条件を含むユニットプロシージャ、またはユニット処方を次の方法でダウンロードします。

- 機能ブロック詳細ビルダでユニットプロシージャを定義している場合は、制御ドローリングビルダで該当するユニット計器を変更して（タグコメントを一度変更して元に戻す）、ダウンロードを実行してください。
- ユニットプロシージャを共有化している場合は、ユニットプロシージャビルダでダウンロードを実行してください。
- ニット処方プロシージャを使用している場合は、該当する処方を使用している実行中のバッチ、または予約済みのバッチがないかを確認してください。実行中バッチがある場合は、終了させてください。予約済みのバッチは削除してください。該当する処方を使った実行中および予約済みのバッチがないことを確認のうえ、処方プロシージャビルダで該当する処方をダウンロードしてください。

C11.5 R4.03.00 へのバージョンアップ／レビジョンアップ

CENTUM VP R4.02.30 から R4.03.00 へのレビジョンアップをして R4.03.00 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R4.02.30 から R4.03.00 にレビジョンアップする場合です。

R4.02.30 より前のレビジョンから R4.03.00 にレビジョンアップ／バージョンアップする場合、これより前に説明した各レビジョン間でのレビジョンアップ／バージョンアップ時の注意も併せてお読みください。

■ Windows 標準コントロールステンシルを削除

R4.03.00 から [Windows 標準コントロール] ステンシルは削除されました。

[Windows 標準コントロール] ステンシルにあった [ピクチャボックス] コントロールは、[基本図形] ステンシルに移動されました。すでに [Windows 標準コントロール] を使用しているユーザへの対応を次に示します。

- ・ [Windows 標準コントロール] ステンシルの [ボタン] を使用していた場合は、[ボタンとデータ表示コントロール] ステンシルの [押しボタン] を使用してください。
- ・ [ラベル] と [テキストボックス] を使用していた場合は、[基本図形] ステンシルの [テキスト] コンポーネントを使用してください。

[Windows 標準コントロール] ステンシルを使うことは推奨されませんが、次の方法で表示させることができます。リボン上のファイルタブで [ステンシルを開く] をクリックし、「ステンシルを開く」ダイアログボックスを表示したら、次のファイルを指定してください。

<Windows XP の場合>

C:\¥Documents and Settings¥All Users¥Data Application¥Yokogawa¥IA¥iPCS¥Products¥CentumVP¥Graphic¥WindowsControls.sdx

<Windows Vista の場合>

C:\¥ProgramData¥Yokogawa¥IA¥iPCS¥Products¥CentumVP¥Graphic¥Controls.sdx Windows

■ バッヂ関連画面についての注意事項

R4.03 からプロダクトオーバビュの使い勝手が替わりました。

参照

プロダクトオーバビュの詳細については、以下を参照してください。

バッヂ管理リファレンス (IM 33J05L10-01JA) の「7.2 プロダクトオーバビュ」

■ バッヂ関連画面の色変更

R4.03 からのバッヂ関連画面の表示色が変更になりました。

従来の黒背景に白文字から白系背景に黒文字に変更されました。

■ グラフィックウィンドウでのプロセスマネージメント確認操作

グラフィックウィンドウでのプロセスマネージメント確認操作は、セキュリティビルダで指定した操作監視範囲に該当機能ロックが含まれていた場合に可能でしたが、R4.03.00 からは、セキュリティビルダで指定した確認範囲に該当機能ロックが含まれている場合に可能になります。

■ グラフィックインターフェースの MoveCursor ファンクションを使用する場合の注意事項

R4.03.00 以降では、グラフィックビューがフォーカスされていない場合、MoveCursor ファンクションによるカーソルの移動は行われません。

■ HIS ヘデータベースをダウンロードする

R4.03.00 ヘリビジョンアップした場合、次の手順で、データベースを HIS ヘダウンロードしてください。

- システムビューから HIS ヘのプロジェクト共通部ダウンロードを実施する
システムビューにて、リビジョンアップした HIS を選択後、プロジェクト共通部ダウンロードを実施します。
なお、次の手順でも代替可能です。
- システムビューからすべての HIS ヘのプロジェクト共通部ダウンロードを実施する
システムビューにて、リビジョンアップした HIS が含まれるプロジェクトを選択後、プロジェクト共通部ダウンロードを実施します。

この操作により、プロジェクトに含まれるすべてのイコライズ対象ステーションに対して一度にダウンロードすることが可能です。

上記操作をいずれも実施しない場合は、FCS 状態表示ビューで次のボタンがグレーアウトされ、操作できません。

- チューニングパラメータセーブボタン
- IOM ロードボタン
- FCS 起動ボタン
- FCS 停止ボタン

■ FF フェースプレートブロックとのリモートカスケード接続について

CENTUM VP R4.02.00 で、FCS 機能ブロックの端子と FF フェースプレートブロックのデータアイテムを結合すると、ジェネレーションでワーニングが発生し、結合情報が失われた状態で FCS などにダウンロードされ、アプリケーションが正しく動作しません。また、この際にエラーメッセージなどは発生しませんので、ご注意ください。

このような場合、R4.03.00 インストール作業のあとに、次の操作をしてください。

- 制御ドローイングビルダを起動してください。
- ワーニングが発生している結合の FF フェースプレートブロックのプロパティを開き、[OK] をクリックしてください。

補足

制御ドローイング内に複数存在する場合は、いずれか 1 つのブロックに対してこの操作を実施してください。

- 制御ドローイングビルダで、[ファイル] – [ダウンロード] を実行してください。
正しい結合情報が生成され、FCS、ALF111、機器に正しい情報がダウンロードされます。
- すべての該当する制御ドローイングシートに対して、同じ操作を行ってください。

C11.6 R5.01.00 へのバージョンアップ[®]

CENTUM VP R4.03 から R5.01 へのバージョンアップをして R5.01 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R4.03 から R5.01 にバージョンアップする場合です。

R4.03 より前のレビューから R5.01 にバージョンアップする場合、これより前に説明した各レビュー間でのレビューアップ時の注意も併せてお読みください。

■ CENTUM データアクセスライブラリ

CENTUM VP R5.01 より前のレビューの CENTUM データアクセスライブラリを使用して作成された VB.NET アプリケーションで、CENTUM VP R5.01 以降でサポートされている OPC のセキュリティ機能を使用する場合は、CENTUM データアクセスライブラリを再配置する必要があります。

次の手順に従って、CENTUM データアクセスライブラリを再配置してください。

1. 既存の VB.NET アプリケーションのフォームに配置されている CENTUM データアクセスライブラリをフォームから削除してください。
2. ソリューションエクスプローラで、対象のプロジェクトの [My Project] ノードをダブルクリックしてください。
3. プロジェクトデザイナーで、[参照設定] タブをクリックしてください。
4. 参照設定ダイアログボックスで、AxInterop.libbkuCENTUM.dll と Interop.libbkuCENTUM.dll の参照をクリックしてください。
5. [削除] をクリックしてください。
6. フォームに CENTUM データアクセスライブラリを配置してください。
7. ソリューションエクスプローラで、対象のプロジェクトをクリックしてください。
8. [ビルド] メニューから対象のプロジェクトの [リビルド] をクリックし、対象プロジェクトのリビルドを実行してください。

重要

上記手順に従って CENTUM データアクセスライブラリの再配置を行うと、既存の VB.NET アプリケーションで CENTUM データアクセスライブラリに設定されていたプロパティの値が初期化されます。本作業を行う前に既存のプロパティの設定値を確認し再配置後に再度設定してください。

参照

配置方法については、以下を参照してください。

CENTUM データアクセスライブラリ (IM 33J05F10-01JA) の「2.2 ライブラリの利用」

■ CAMS for HIS ヒストリカルビューア検索改善

CENTUM VP R5.01.00 では、CAMS for HIS ヒストリカルビューアでの検索機能が大幅に改善されています。これは、R5.01.00 では内部で自動的にインデックスファイルを生成し、検索対象の絞り込みができるためです。R4.03.00 以前では、検索期間を指定しない場合、全ヒストリカルファイル（最大容量：20 GB）の検索を行うため、検索に時間がかかっていました。

そのため、次の操作を行うことにより、R4.03.00 以前に保管されたヒストリカルファイルにもインデックスファイルを作成し、R5.01.00 で実現された検索機能を使用できるようにします。

● 実施対象

R4.03.00 以前で CAMS for HIS を有効にしていた各 HIS が対象となります。

● 操作手順

R4.03.00 までのヒストリカルファイルに対してインデックスファイルを作成するには、次の手順に従ってください。

補足

インデックスファイル生成には、最大約 1 時間 30 分かかります（最大容量 20 GB のヒストリカルファイルが存在する場合）。なお、インデックスファイル生成中でも HIS の操作監視はできます。

1. 次のファイルを実行し、CAMS for HIS インデックス生成ツールを起動してください。

<CENTUM VP インストールフォルダ>\CAMSY\CAMSHistIndex.exe

CAMS for HIS インデックスファイル生成ツールダイアログが表示されます。

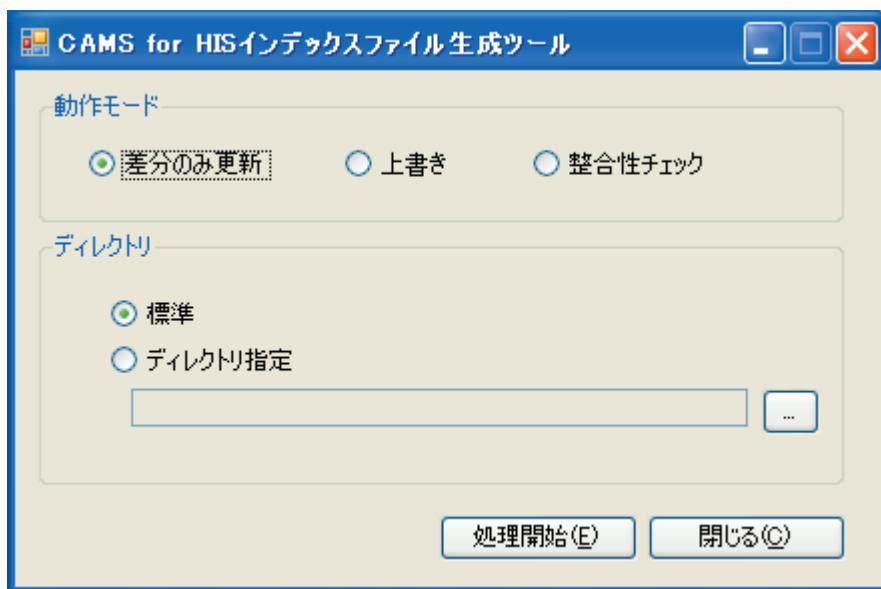


図 C11.6-1 CAMS for HIS インデックスファイル生成ツールダイアログ

2. 動作モードとディレクトリを指定してください。

表 C11.6-1 動作モードとディレクトリの詳細

項目名	内容
動作モード	差分のみ更新 既存のインデックスファイルが存在する場合、差分のみ更新します。存在しない場合は、新たにインデックスファイルを作成します。
	上書き 既存のインデックスファイルの有無にかかわらず、新たにインデックスファイルを作成します。
	整合性チェック 既存のインデックスファイルを読み込み、整合性をチェックします。
ディレクトリ	標準 CAMS for HIS 標準フォルダをインデックス生成処理対象にすることに選択します。
	ディレクトリ指定 長期保管フォルダをインデックス生成処理対象にすることに選択します。CamsHist という名称のフォルダのみ指定できます。

3. [処理開始] をクリックしてください。

確認ダイアログが表示されます。

4. [OK] をクリックしてください。
処理が始まり、処理状況を示すダイアログが表示されます。
5. 処理が完了すると完了ダイアログが表示されるので、[OK] をクリックしてください。

補足

インデックスファイル生成中にエラーが発生した場合は、エラー内容が次のファイルに出力されます。エラー内容を確認し、再度はじめからインデックスファイル生成を行ってください。

<CENTUM VP インストールフォルダ>\CAMSYLOG\LOGMNTLOG\CAMSHistIndex{0|1|2}.log

■ グラフィックファイル形式変更のための対応

CENTUM VP R5.01.00 は、グラフィックファイルのパフォーマンス向上のため、R4 からファイル形式を変更しています。そのため、HIS をバージョンアップしたあとは、HIS のダウンロードが必要です。

■ FCS のバージョンアップ

R5.01.00 の新機能を使用しない場合、R5.01.00 にバージョンアップしたシステム生成機能から FCS にオフラインダウンロードを実行することで、FCS のバージョンアップが完了します。また、オフラインダウンロードができない場合も、バージョンアップ以前の機能の範囲内であれば、次の機能は動作します。

- R5.01.00 にバージョンアップしたシステム生成機能を用いてのオンラインメンテナンスとチューニングパラメータセーブ
- R5.01.00 にバージョンアップした操作監視機能

● R5.01.00 での新機能を使用する場合

R5.01.00 で次の新機能を使用する場合には、そのための対応が必要です。

表 C11.6-2 新機能と FCS の対応

機能名	バージョンアップ前の FCS	
	R1, R2, R3	R4.01～R4.03
AFV30、AFV40 (FFCS-V)	—	×
CAL のプロセスアラーム通知	—	○
CAL 時の PRD モードへの変更	—	○

○：FCS に対して、オフラインダウンロードが必要です。

×：FCS を新規作成し、既存のエンジニアリングデータをすべてインポートしたあと、FCS にオフラインダウンロードが必要です。また、FCS のハードウェアの交換も必要です。

–：対象外

■ カスタムフェースプレートの表示

CENTUM VP R5.01.00 は、グラフィックファイルのパフォーマンス向上のため、R4 からファイル形式を変更しています。そのため、以前のリビジョンでカスタムフェースプレートを使用していて、R5.01.00 にバージョンアップした場合は、各 HIS でエクスプローラより次のコマンドをダブルクリックして、カスタムフェースプレートを更新してください。コピーしない場合、カスタムフェースプレートを R5.01.00 の HIS 上で表示できません。

<Program Files フォルダ (通常"C:\Program Files")>\YOKOGAWA\IA\iPCS\Products\CENTUMVP\Program\Yokogawa.IA.iPCS.CENTUMVP.HIS.Graphic.CustomFaceplateUpdtTool.exe

■ グラフィックビューの余白の色

以前のレビジョンでは、グラフィックビューの上下または左右にできる余白を白色で表示していました。R5.01.00 では、その余白をキャンバス背景色で表示します。

なお、以前と同様に余白を白色に戻したい場合、エクスプローラより次のコマンドを実行してください。

- 32 ビット OS の場合 (Windows Vista、Windows Server 2008)

<CENTUM VP インストールフォルダ>\his\tool\SetCanvasSpaceColorWhite.reg

- 64 ビット OS の場合 (Windows 7、Windows Server 2008 R2)

<CENTUM VP インストールフォルダ>\his\tool\SetCanvasSpaceColorWhite_64bit.reg

また、再度余白をキャンバス背景色にしたい場合は、次のコマンドを実行してください。

- 32 ビット OS の場合 (Windows Vista、Windows Server 2008)

<CENTUM VP インストールフォルダ>\his\tool\ResetCanvasSpaceColorWhite.reg

- 64 ビット OS の場合 (Windows 7、Windows Server 2008 R2)

<CENTUM VP インストールフォルダ>\his\tool\ResetCanvasSpaceColorWhite_64bit.reg

■ グラフィックのフォント幅

Windows の OS を、XP から Vista または Windows 7 に変更する場合、次のときにフォントの幅が違うことがあります。

- 存在しないフォントを指定しているとき

例：メイリオ

- 英文フォントで日本語を表示しているとき

例：Courier New

- 一部のプロポーショナルフォントでアルファベットを表示しているとき

例：Arial、Times New Roman

フォントの変更または文字の変更により、幅を調整してください。

■ グラフィックビルダのキャンバスにおけるタスクバーの高さ

Windows 7 のタスクバーの高さは、Windows XP/Vista より 10 ドット高くなります。そのため、タスクバーを常時表示して HIS を使用している場合、グラフィックなど HIS ウィンドウ表示領域の高さが狭くなり、画面にスクロールバーが表示されることがあります。

この場合は、Windows 7 のタスクバーのアイコンを小さくするか、タスクバーを自動的に隠す設定にしてください。

■ .NET コントロールと ActiveX コントロールの動作確認

Windows の OS を、Windows Vista または Windows 7 に変更する場合、ユーザが作成した.NET コントロール、ActiveX コントロールは動作確認が必要です。

■ オンラインマニュアルの表示

オンラインマニュアルの表示は、1 セッションに限定されます。

リモート操作監視サーバ機能で複数のセッションから表示しようとした場合は、1 セッションしか表示できない旨のダイアログが表示されます。別のセッションで表示されていないか（別のユーザがすでにオンラインマニュアルを使用していないか）をご確認ください。

■ グラフィックビューのタッチターゲット

CENTUM VP の R4 と R5 では、タッチターゲットを次のコントロールの上に重ねたときの動作に違いがあります。

- ・ タッチターゲット
- ・ 計器図コントロール
- ・ ユーザコントロール (ActiveX コントロール、Windows フォームコントロール)

R4 では上に配置されたタッチターゲットの機能条件が不成立の場合、下に配置されたコントロールの機能条件が成立していれば、その機能が実行されます。R5 では上に配置されたタッチターゲットの機能条件が不成立の場合、下に配置されたコントロールの機能条件が成立していても、その機能は実行されません。

タッチターゲットチェックツールで該当箇所を検索し、グラフィックファイルを修正してください。

● 対象となるタッチターゲットの検出方法

1. 次のファイルを実行して、タッチターゲットチェックツールを起動してください。
<ProgramFiles フォルダ>\YOKOGAWAYIA\iPCS\Products\CENTUMVP\Program\Yokogawa.IA.iPCS.CENTUMVP.ENG.UTY.TouchTargetCheckTool.exe
2. [参照] をクリックして、プロジェクトデータベースのトップフォルダを選択してください。
3. [チェック] をクリックして、検出を開始してください。
チェック完了後に、検出結果のダイアログが表示されます。該当箇所があるときは、その概要と詳細情報へのリンクがダイアログ内に表示されます。
 - ・ 検出結果の概要
<CENTUM VP インストールフォルダ>\Temp\Window\TouchTargetCheckTool\TouchTargetCheckSummary_yyyyMMdd_HHmmss.csv
yyyyMMdd : 西暦年月日
Hmmss : 時分秒
出力される情報は、次のとおりです。
 - ・ グラフィックファイル (.edf) のパス
 - ・ チェック結果 (成功／失敗)
 - ・ 検出したタッチターゲットの数
 - ・ エラーメッセージ (エラー発生時)
 - ・ 検出結果の詳細
<CENTUM VP インストールフォルダ>\Temp\Window\TouchTargetCheckTool\TouchTargetCheckDetails_yyyyMMdd_HHmmss.csv
yyyyMMdd : 西暦年月日
Hmmss : 時分秒
出力される情報は、次のとおりです。
 - ・ グラフィックファイル (.edf) のパス
 - ・ タッチターゲットのオブジェクト名
 - ・ 座標
 - ・ タッチターゲットがグループ化されているときは、そのグループ名
4. 検出結果に従って該当箇所を確認し、グラフィックファイルを修正してください。

C11.7 R5.01.10へのバージョンアップ／リビジョンアップ

CENTUM VP R5.01.00 から R5.01.10 へのリビジョンアップをして R5.01.10 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R5.01.00 から R5.01.10 にリビジョンアップする場合です。

R5.01.00 より前のリビジョンから R5.01.10 にリビジョンアップ／バージョンアップする場合、これより前に説明した各リビジョン間でのリビジョンアップ／バージョンアップ時の注意も併せてお読みください。

■ 基本処方のダウンロード

リビジョンアップ後に処方ビューから基本処方のダウンロードまたはマスタダウンロードをしてください。ダウンロードまたはマスタダウンロードを実施しないと、処方選択ダイアログでツリービューの階層が表示されません。

基本処方のダウンロードは、処方ビューの [ロード] メニューから [マスタダウンロード] または、[ダウンロード] を実施してください。

C11.8 R5.02.00 へのバージョンアップ／レビジョンアップ

CENTUM VP R5.01.20 から R5.02.00 へのレビジョンアップをして R5.02.00 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R5.01.20 から R5.02.00 にレビジョンアップする場合です。

R5.01.20 より前のレビジョンから R5.02.00 にレビジョンアップ／バージョンアップする場合、これより前に説明した各レビジョン間でのレビジョンアップ／バージョンアップ時の注意も併せてお読みください。

■ リモート操作監視サーバ機能のレビジョンアップ

CENTUM VP R5.02.00 より前のレビジョンでリモート操作監視サーバ機能を使用していて、OS が Windows Server 2008 であり、8 セッション接続ライセンスを使用する場合には、必要な仮想メモリサイズが確保されているか確認してください。

必要な仮想メモリサイズが確保されていないと、メモリ不足が発生し、リモートからの操作監視ができなくなることがあります。

参照

仮想メモリの必要サイズについては、以下を参照してください。

「■ 手順 2：Windows の設定をする」ページ B5-21

■ Vnet/IP バスステータス

Vnet/IP ファームウェアのレビジョンが Rev.13 以降のときは、バス異常時に表示される Vnet/IP バスステータスには、バス異常があったドメインに属する HIS のみのバス異常が表示されます。他ドメインの通信状態は含まれません。

C11.9 R5.03.00 へのバージョンアップ／リビジョンアップ

CENTUM VP R5.02.00 から R5.03.00 へのリビジョンアップをして R5.03.00 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R5.02.00 から R5.03.00 にリビジョンアップする場合です。

R5.02.00 より前のリビジョンから R5.03.00 にリビジョンアップ／バージョンアップする場合、これより前に説明した各リビジョン間でのリビジョンアップ／バージョンアップ時の注意も併せてお読みください。

■ UGS (統合ゲートウェイステーション)

UGS に関する注意事項を次に示します。

● OPC サーバコンピュータのアカウント設定

R5.03.00 の UGS と OPC DA サーバ、または OPC A&E サーバを接続するときは、接続先の OPC サーバコンピュータに UGS_PROCESS ユーザアカウントを作成してください。

参照

UGS と OPC DA サーバ、または OPC A&E サーバを接続する方法については、以下を参照してください。

統合ゲートウェイステーションリファレンス (IM 33J20C10-01JA) の「D2.4 シングル UGS の構築」の
「■ OPC DA サーバ、OPC A&E サーバ接続時のセキュリティ設定」

● HIS へのタグリストダウンロード

R5.03.00 へのバージョンアップアップ後、HIS に対して、全 UGS ステーションのタグリストのダウンロードを実施してください。

■ デバイスドライバの更新

CENTUM VP を R5.03.00 へリビジョンアップするときは、制御バスドライバや Vnet/IP オープン通信ドライバなどの各種デバイスドライバを更新してください。

参照

デバイスドライバの更新手順については、以下を参照してください。

「■ デバイスドライバの更新」ページ C6-30

■ FCS のバージョンアップ

R5.03.00 の新機能を使用しない場合、R5.03.00 にバージョンアップしたシステム生成機能から FCS にオフラインダウンロードを実行することで、FCS のバージョンアップが完了します。また、オフラインダウンロードができない場合も、バージョンアップ以前の機能の範囲内であれば、次の機能は動作します。

- R5.03.00 にバージョンアップしたシステム生成機能を用いてのオンラインメンテナンスとチューニングパラメータセーブ
- R5.03.00 にバージョンアップした操作監視機能

● R5.03.00 での新機能を使用する場合

R5.03.00 で新機能を使用する場合には、次に示す作業が必要です。

表 C11.9-1 新機能と必要な作業

機能名	システム生成機能のバージョンアップ	FCS の再作成および既存のエンジニアリングデータのインポート	FCS へのオフラインダウロード	操作監視機能のバージョンアップ	全 HIS に対するプロジェクト共通部のダウンロード
テスト機能 高速スキャン動作	Yes	No	No	No	No
OOP 中の出力モジュールへの出力値の書き込み	Yes	No	Yes	No	No
OOP 中の機能ブロックの出力トラッキング	Yes	No	Yes	Yes	No
SV を SVH～SVL の範囲外に設定不可とする	Yes	No	No	No	Yes
演算入力値の QST を演算出力値に伝達する	Yes	No	Yes	No	No
PRD モードのときの出力リミッタ	Yes	No	Yes	No	No
CPV のデータ制約レベルを PV と同じにする	Yes	No	No	No	Yes
サブシステム通信機能 二重化切り替え方式 ノード状態表示ダイアログの入出力モジュール状態表示	Yes	No	Yes	No	No
処方オペレーション付きユニット計器 ユニットオペレーション計器	Yes	Yes	Yes	Yes	Yes
ALP121	Yes	Yes	Yes	No	No

● CPV のデータ制約レベルを PV と同じにする

CENTUM VP R5.03 で、プロジェクト新規作成ダイアログの高度設定タブに本項目が追加されました。

本設定項目に関しては、R5.03 以降でプロジェクトを新規作成した場合と、既存のプロジェクトをレビューションアップした場合で、デフォルトの設定が異なります。複数プロジェクト結合でプロジェクト間の動作を同じにしたい場合は、必要に応じて設定を変更してください。

参照

本項目の詳細については、以下を参照してください。

エンジニアリングリファレンス Vol.1 (IM 33J10D10-01JA) の「2.2 プロジェクトの作成」の「■ プロジェクトに関する高度設定」の「● CPV のデータ制約レベルを PV と同じにする」

● OOP 中の機能ブロックの出力トラッキング

CENTUM VP R5.03 で、FCS 定数ビルダの高度設定項目タブシートに本項目が追加されました。

本設定項目に関しては、R5.03 以降のシステム生成機能で作成した FCS と、R5.03 より前のシステム生成機能で作成した FCS で、デフォルトの設定が異なります。FCS 間で動作を同じにしたいときは、必要に応じて設定を変更してください。

参照

本項目の詳細については、以下を参照してください。

エンジニアリングリファレンス Vol.1 (IM 33J10D10-01JA) の「2.10 OOP 中の機能ブロックの出力トラッキング：FFCS 系/KFCS2/LFCS2/RFC5」の「■ OOP 中の機能ブロックの出力トラッキング」

■ CENTUM データアクセスライブラリ

CENTUM VP R5.03 より前に CENTUM データアクセスライブラリを使用して作成したユーザアプリケーションを、R5.03 以降で使用するときには、移行作業をしてください。

● VB6 で作成したユーザアプリケーションの移行作業

VB6 で作成したユーザアプリケーションは、R5.03 以降の CENTUM データアクセスライブラリを使用できません。R5.03 以降の CENTUM データアクセスライブラリを使用するためには、VB6 で作成したユーザアプリケーションを VB.NET に移行する作業が必要です。VB6 で作成したユーザアプリケーションを VB.NET に移行する方法については、ユーザアプリケーションによって異なりますので本書では記述しません。

● VB.NET で作成したユーザアプリケーションの移行作業

開発用コンピュータ上で、次の手順に従って移行作業を行ってください。

1. R5.03 より前の CENTUM データアクセスライブラリへの参照を解除する
2. R5.03 以降の CENTUM データアクセスライブラリをセットアップする
3. R5.03 以降の CENTUM データアクセスライブラリを再配置する

各手順については、以降を参照してください。

● R5.03 より前の CENTUM データアクセスライブラリへの参照を解除する

R6.06 以降の環境に移行する手順と同じです。

参照

R5.03 より前の CENTUM データアクセスライブラリへの参照を解除する手順については、以下を参照してください。

CENTUM データアクセスライブラリ (IM 33J05F10-01JA) の「2.8.1 R5.03 より前に作成したユーザアプリケーションを R6.06 以降の環境に移行する」の「■ VB.NET で作成したユーザアプリケーションを移行する作業」の「● R5.03 より前の CENTUM データアクセスライブラリへの参照を解除する」

● R5.03 以降の CENTUM データアクセスライブラリをセットアップする

重要

本作業の実施後は、R5.03 より前の CENTUM データアクセスライブラリへの参照の解除ができなくなります。

必ず、参照の解除を実施したあと、本作業を行ってください。

HIS 上で開発作業を行っている場合、CENTUM VP システムのレビューを R5.03 以降に更新してください。

HIS 以外のコンピュータで開発作業を行っている場合、R5.03 以降のライブラリをセットアップしてください。

参照

HIS の CENTUM VP システムの更新については、以下を参照してください。

「C6. バージョンアップ／レビューションアップやアップグレードをする」ページ C6-1

HIS 以外のコンピュータでの CENTUM データアクセスライブラリのセットアップについては、以下を参照してください。

CENTUM データアクセスライブラリ (IM 33J05F10-01JA) の「2.1 HIS 以外のコンピュータへのライブラリの組み込み」

● R5.03 以降の CENTUM データアクセスライブラリを再配置する

1. フォームに新規の CENTUM データアクセスライブラリを配置してください。

2. フォーム上の CENTUM データアクセスライブラリのコントロール名称を、「● R5.03 より前の CENTUM データアクセスライブラリへの参照を解除する」で記録したコントロール名称に変更してください。
3. フォーム上の CENTUM データアクセスライブラリのプロパティ値を、「● R5.03 より前の CENTUM データアクセスライブラリへの参照を解除する」で記録したプロパティ値に変更してください。
4. 次のイベントを使用していた場合、イベントの再割り当てを行ってください。
 - MsgEvent イベント
 - ShutdownEvent イベント
5. ソリューションエクスプローラで、対象のプロジェクトをクリックしてください。
6. [ビルド] メニューから対象のプロジェクトの [リビルド] をクリックしてください。リビルドが実行されます。

参照

MsgEvent イベントについては、以下を参照してください。

CENTUM データアクセスライブラリ (IM 33J05F10-01JA) の「3.3.1 アラーム／メッセージの通知」の「■ MsgEvent イベント」

ShutdownEvent イベントについては、以下を参照してください。

CENTUM データアクセスライブラリ (IM 33J05F10-01JA) の「3.3.2 HIS のシャットダウンの通知」の「■ ShutdownEvent イベント」

C11.10 R5.03.20 へのバージョンアップ／レビジョンアップ

CENTUM VP R5.03.00 から R5.03.20 へのレビジョンアップをして R5.03.20 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R5.03.00 から R5.03.20 にレビジョンアップする場合です。

R5.03.00 より前のレビジョンから R5.03.20 にレビジョンアップ／バージョンアップする場合、これより前に説明した各レビジョン間でのレビジョンアップ／バージョンアップ時の注意も併せてお読みください。

■ プロジェクト内の各コンピュータへのデータベースダウンロード

R5.03.20 へバージョンアップ／レビジョンアップしたあとは、システムビューからプロジェクト内の各コンピュータへプロジェクト共通部をダウンロードしてください。

ダウンロードしたあとは、各コンピュータを再起動してください。

■ CAMS for HIS メッセージモニタ

CAMS for HIS メッセージモニタの次の項目に変更があります。

表 C11.10-1 変更内容

項目	R5.03.20	R5.03.20 より前	備考
One shot Shelf に Shelving されるメッセージの数	100 メッセージ／1 ユーザ	制限なし	最大値を超えてメッセージを Shelving しようとすると、誤操作メッセージが出来ます。バージョンアップ前に最大値を超えて Shelving していたときは、バージョンアップの際に最大値を超えたメッセージは、Shelf から削除されます。
Continuous Shelf に Shelving されるアラームソースの数	100 アラームソース／1 ユーザ	制限なし	最大値を超えてアラームソースを Shelving しようとすると、誤操作メッセージが出来ます。バージョンアップ前に最大値を超えて Shelving していたときは、バージョンアップの際に最大値を超えたアラームソースは、Shelf から削除されます。

■ CAMS for HIS 使用時のアラーム抑制機能の変更

Suppression およびアラーム抑制 (AOF) を実行したときの動作が変更されます。

参照

変更された動作の詳細については、以下を参照してください。

統合型アラーム管理リファレンス (IM 33J05A21-01JA) の「A6.1 CAMS for HIS メッセージモニタでメッセージを処理した結果は、その他の操作監視ウィンドウにどのように表示されるか」の「■ プロセスアラームメッセージを抑制したときの HIS の動作」

■ 複数プロジェクト結合をするとき

複数プロジェクト結合で下位側プロジェクトが R5.03.20 より前のレビジョンのときは、アラームエンジニアリング情報の共有ができません。上位側プロジェクトの OtherProject ノードで、下位プロジェクトのアラームエンジニアリング情報を定義してください。

参照

R5.03.20より前のCENTUM ソフトウェアを下位側プロジェクトにするときの操作については、以下を参照してください。

統合型アラーム管理リファレンス (IM 33J05A21-01JA) の「A7.1 CAMS for HIS を有効にしたときの、プロジェクトの結合形態」の「■ R5.03.20より前のCENTUM ソフトウェアを下位側プロジェクトにするときは」

C11.11 R5.04.00 へのバージョンアップ／レビジョンアップ

CENTUM VP R5.03.20 から R5.04.00 へのレビジョンアップをして R5.04.00 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R5.03.20 から R5.04.00 にレビジョンアップする場合です。

R5.03.20 より前のレビジョンから R5.04.00 にレビジョンアップ／バージョンアップする場合、これより前に説明した各レビジョン間でのレビジョンアップ／バージョンアップ時の注意も併せてお読みください。

■ FCS のバージョンアップ

R5.04.00 の新機能を使用しない場合、R5.04.00 にバージョンアップしたシステム生成機能から FCS にオフラインダウンロードを実行することで、FCS のバージョンアップが完了します。また、オフラインダウンロードができない場合も、バージョンアップ以前の機能の範囲内であれば、次の機能は動作します。

- R5.04.00 にバージョンアップしたシステム生成機能を用いてのオンラインメンテナンスとチューニングパラメータセーブ
- R5.04.00 にバージョンアップした操作監視機能

● R5.04.00 での新機能を使用する場合

R5.04.00 で新機能を使用する場合には、次に示す作業が必要です。

表 C11.11-1 新機能と必要な作業

機能名	システム生成機能のバージョンアップ	FCS の再作成および既存のエンジニアリングデータのインポート	FCS へのオフラインダウンロード	操作監視機能のバージョンアップ	全 HIS に対するプロジェクト共通部のダウンロード
プロセスアラームの検出遅延機能	Yes	No	Yes	No	No
IN 端子以外の入力が異常になった時の動作-XL 互換機能	Yes	No	Yes	No	No
DI がフェイルしたときの動作	Yes	No	Yes	No	No

C11.12 R5.04.20 へのバージョンアップ／レビジョンアップ

CENTUM VP R5.04.00 から R5.04.20 へのレビジョンアップをして R5.04.20 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

R5.04.00 より前のレビジョンから R5.04.20 にレビジョンアップ／バージョンアップする場合、これより前に説明した各レビジョン間でのレビジョンアップ／バージョンアップ時の注意も併せてお読みください。

■ ロジックチャートビュー用状態表示ファイルの再作成

R5.02.00～R5.04.00 からレビジョンアップした場合には、LC64-E が含まれる制御ドローリングの状態表示ファイルの再作成を行ってください。再作成をしないと、信号線の色が正しく表示されない場合があります。

● ロジックチャートビュー用状態表示ファイルの再作成手順

LC64-E が含まれる制御ドローリングファイルに対して作業をします。

1. システムビューから、[ツール] – [名称検索] を選択してください。
名称検索ツールが起動します。
2. ブロック形名に LC64-E を設定し、検索してください。
検索結果に LC64-E ブロックが存在する制御ドローリングファイルが表示されます。
3. 該当の制御ドローリングファイルを選択し、[ビルダ起動] ボタンをクリックしてください。
制御ドローリングビルダが展開されます。
4. 制御ドローリングビルダで、ツールバーの [作業中ファイル作成] ボタンをクリックしてください。
5. 制御ドローリングビルダを終了してください。
6. LC64-E ブロックが存在する制御ドローリングファイルについて、上記手順 3～5 を行ってください。
7. システムビューから、[FCS] – [一括ジェネレーション] を選択してください。
一括ジェネレーションツールが起動します。
8. 手順 4 で作成した作業中ファイルが表示されますので、[全選択] ボタンをクリックして、ジェネレーション対象とし、[開始] ボタンをクリックしてください。
状態表示ファイルが再作成されます。

補足

- ・ 状態表示ファイル再作成の作業は、エンジニアリングデータベースに対する作業であり、1台の HIS/ENG ステーションへの実施で十分です。他のステーションへの実施は不要です。
- ・ 状態表示ファイル再作成のみの作業では、チューニングパラメータセーブは不要です。

C11.13 R6.01.00 へのバージョンアップ[®]

CENTUM VP R5.04.20 から R6.01 へのバージョンアップをして R6.01 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R5.04.20 から R6.01 にバージョンアップする場合です。

R5.04.20 より前の Revision から R6.01 にバージョンアップする場合、これより前に説明した各 Revision 間での Revision アップ時の注意も併せてお読みください。

■ Suppression 実行時の復帰メッセージ出力指定

CENTUM VP R6.01 から CAMS for HIS で Suppression を実行した時に復帰メッセージを出力するかしないかの設定ができます。設定を変更した場合は、プロジェクト内の全 HIS にプロジェクト共通部ダウンロードを実施してください。

なお、新規プロジェクトを作成した時と過去のバージョンからバージョンアップした時の設定のデフォルト値は以下のようになります。バージョンアップの場合は、バージョンアップ前の復帰メッセージ出力動作を引き継ぎますので、新たに設定をし直す必要はありません。

表 C11.13-1 復帰メッセージ出力のデフォルト値

項目	デフォルト値
新規プロジェクト作成時	復帰メッセージを出力する
R5.03.00 以前からのバージョンアップ	復帰メッセージを出力する
R5.03.20 以降からのバージョンアップ	復帰メッセージを出力しない

C11.14 R6.01.10へのバージョンアップ／レビジョンアップ

CENTUM VP R6.01.00 から R6.01.10 へのレビジョンアップをして R6.01.10 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R6.01.00 から R6.01.10 にレビジョンアップする場合です。

R6.01.00 より前のレビジョンから R6.01.10 にバージョンアップ／レビジョンアップする場合、これより前に説明した各レビジョン間でのバージョンアップ／レビジョンアップ時の注意も併せてお読みください。

■ バージョンアップ／レビジョンアップやアップグレード後の作業の注意事項

VP プロジェクトの履歴管理のために、バージョンアップ／レビジョンアップやアップグレード後の作業として、既存の VP プロジェクトの AD プロジェクトへの登録が必要です。登録は、数十分かかります。この間、登録中の VP プロジェクトは修正できません。

C11.15 R6.02.00 へのバージョンアップ／レビジョンアップ

CENTUM VP R6.01.10 から R6.02.00 へのレビジョンアップをして R6.02.00 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R6.01.10 から R6.02.00 にレビジョンアップする場合です。

R6.01.10 より前のレビジョンから R6.02.00 にレビジョンアップ／バージョンアップする場合、これより前に説明した各レビジョン間でのレビジョンアップ／バージョンアップ時の注意も併せてお読みください。

■ 操作監視機能

操作監視機能に関する注意事項を、次に示します。

● HIS をレビジョンアップするときの注意事項

HIS を R6.01.10 以前から R6.02 にレビジョンアップしたあとに、システムビューから HIS を選択して、HIS ダウンロードを実行してください。

● トレンドブロック拡張

CS 3000 HIS 以外の HIS のレビジョンは、プロジェクト内で R6.02.00 に統一してください。また、R6.01.10 以前のレビジョンの HIS では、HIS プロパティの高度設定タブで、「トレンドブロックを拡張する（R6.02.00 以降）」のチェックボックスを選択しないでください。

● グラフィックビューのトレンドコントロール

CENTUM VP R6.02.00 では、グラフィックビューのトレンドコントールで他ステーショントレンドを表示できるようになりました。

それに伴い、レビジョンアップすることで、トレンドコントロールのトレンドポイントの表示が、自ステーショントレンドから他ステーショントレンドに変わることあります。

そのときは、同じプロセスデータのトレンドが表示されますが、次の様に表示内容が変わるので、注意してください。

- ・ トレンドの収集周期が変わる
 - ・ 他ステーショントレンドの収集元の HIS が停止するとトレンドが表示されなくなる
- これは、次の条件をすべて満たすときに発生します。
- ・ トレンドコントロールで自ステーショントレンドにない収集周期のプロセスデータを指定している
 - ・ 他ステーショントレンドに指定した収集周期のプロセスデータがある
- トレンドコントロールの表示を戻すときは、自ステーショントレンドにあるプロセスデータの収集周期となるよう、収集周期の設定を変更してください。

■ CAMS for HIS

CAMS for HIS に関する注意事項を、次に示します。

● HIS をレビジョンアップするときの注意事項

HIS をレビジョンアップするときは、次の点に注意してください。

- ・ プロジェクト共通部ダウンロード
- HIS を R6.01.10 以前から R6.02 にレビジョンアップしたあとに、システムビューから HIS に対してプロジェクト共通部ダウンロードを実行してください。
- ・ CAMS for HIS メッセージモニタのツールバーのカスタマイズ

HIS を R6.01.10 以前から R6.02 にリビジョンアップすると、ツールバーに [Suppression 一覧ウィンドウ] ボタンと [Shelving 一覧ウィンドウ] ボタンが追加されます。

R6.01.10 以前にすでにツールバーをカスタマイズしている場合は、カスタマイズの設定を引き継ぎつつ、これら 2 つのボタンが右側に追加されます。これらのボタンが不要な場合は、リビジョンアップ後に、ツールバーのカスタマイズでボタンを削除してください。

参照

ツールバーのカスタマイズについては、以下を参照してください。

統合型アラーム管理リファレンス (IM 33J05A21-01JA) の「B1.4.3 オペレータが CAMS for HIS メッセージモニタをカスタマイズする」の「■ ツールバータブシートで設定する項目」

● HIS のリビジョンが混在しているときの注意事項

HIS をリビジョンアップするときは、VP プロジェクトのすべての HIS をリビジョンアップする必要があります。しかし、すべてのリビジョンアップ作業が完了する前には、VP プロジェクトに複数のリビジョンの HIS が存在する場合があります。

そのような場合に、CAMS for HIS メッセージモニタをカスタマイズする必要があるときは、次の点に注意してください。

- ・ ダウンロードマスター

ダウンロードマスターは、必ず R6.02 の HIS としてください。R6.01.10 以前の HIS をダウンロードマスターとしているときは、CAMS for HIS コンフィグレータの CAMS for HIS メッセージモニタのカスタマイズ結果が R6.02 の HIS に反映されません。

補足

R6.02 以降にリビジョンアップする場合も、ダウンロードマスターは、必ず最新のリビジョンの HIS にしてください。

- ・ CAMS for HIS メッセージモニタのカスタマイズ
オペレータが CAMS for HIS メッセージモニタをカスタマイズする場合は、R6.02 の HIS でカスタマイズと変更反映を実行してください。R6.01.10 以前の HIS でカスタマイズと変更反映を実行しても、カスタマイズ結果が R6.02 の HIS に反映されません。
- ・ R6.01.10 以前の HIS でのツールバーのボタン表示
R6.01.10 以前の HIS のツールバーに、[Suppression 一覧ウィンドウ] ボタンと [Shelving 一覧ウィンドウ] ボタンは表示されません。

参照

CAMS for HIS のダウンロードマスターについては、以下を参照してください。

統合型アラーム管理リファレンス (IM 33J05A21-01JA) の「A1. CAMS for HIS の概要」の「■ CAMS for HIS を使用したときのシステム構成」

CAMS for HIS コンフィグレータについては、以下を参照してください。

統合型アラーム管理リファレンス (IM 33J05A21-01JA) の「B1.5 CAMS for HIS コンフィグレータ」

オペレータによる CAMS for HIS メッセージモニタのカスタマイズについては、以下を参照してください。

統合型アラーム管理リファレンス (IM 33J05A21-01JA) の「B1.4.3 オペレータが CAMS for HIS メッセージモニタをカスタマイズする」

● HIS のリビジョンを混在させる場合に、追加した HIS にダウンロードマスターを変更するときの手順

R6.01.10 以前の HIS のみが存在する等価化対象範囲に R6.02 の HIS を追加する場合は、ダウンロードマスターを R6.02 の HIS に変更する必要があります。

この場合に、設定済みの CAMS for HIS メッセージモニタのカスタマイズ結果を R6.02 のダウンロードマスターの HIS に引き継ぐときは、次の手順に従ってください。

1. R6.02 の HIS をシステムに追加して、すべての HIS にプロジェクト共通部ダウンロードを実行してください。
2. 既存の等値化対象範囲に R6.02 の HIS を追加して、すべての HIS を再起動してください。そのとき、R6.02 の HIS を最後に再起動してください。

補足

ダウンロードマスターは R6.01.10 以前の HIS のままとしてください。

3. 設定済みの CAMS for HIS メッセージモニタのカスタマイズ結果が R6.02 の HIS に反映されていることを確認してください。
4. R6.01.10 以前のダウンロードマスターの HIS で、ダウンロードマスターの設定を解除して、R6.02 の 1 台の HIS で、ダウンロードマスターの設定を行ってください。
5. ダウンロードマスターを解除した HIS、および新たにダウンロードマスターにした HIS を再起動してください。

補足

このときには HIS の再起動の順番に制約はありません。

6. R6.02 のダウンロードマスターの HIS で、必要に応じて、CAMS for HIS コンフィグレータにより CAMS for HIS メッセージモニタのカスタマイズとダウンロードを実行してください。

参照

等値化対象範囲とダウンロードマスターの設定については、以下を参照してください。

統合型アラーム管理リファレンス (IM 33J05A21-01JA) の「B1.3 CAMS for HIS を有効にするための設定」の「■ CAMS for HIS タブシートで設定する項目」

C11.16 R6.03.00 へのバージョンアップ／リビジョンアップ

CENTUM VP R6.02.00 から R6.03.00 へのリビジョンアップをして R6.03.00 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R6.02.00 から R6.03.00 にリビジョンアップする場合です。

R6.02.00 より前のリビジョンから R6.03.00 にリビジョンアップ／バージョンアップする場合、これより前に説明した各リビジョン間でのリビジョンアップ／バージョンアップ時の注意も併せてお読みください。

■ 操作監視機能

操作監視機能に関する注意事項を、次に示します。

● FFCS-C 状態表示ビュー

CENTUM VP R6.03 より前にエンジニアリングされた FFCS-C の状態表示ビューでは、FIO ノードのコンポーネント番号が表示されません。コンポーネント番号を表示させるときは、次の手順に従ってください。

- 対象 FIO を内蔵する FCS に、オフラインダウンロードを実行してください。
- システムビューのノードプロパティダイアログで、コンポーネント番号を入力し、オンラインダウンロードを行ってください。

■ CAMS for HIS

CAMS for HIS に関する注意事項を、次に示します。

● ユーザ定義属性を使用しているときの注意事項

R6.03.00 より前のリビジョンで、属性名を「モジュールベースエンジニアリング対象」としているユーザ定義属性を使用している場合は、R6.03.00 にリビジョンアップする前に属性名を変更してください。

属性名を変更せずにリビジョンアップした場合、その属性が CAMS for HIS アラームビルダに表示されなくなります。

参照

ユーザ定義属性を変更する方法については、以下を参照してください。

統合型アラーム管理リファレンス (IM 33J05A21-01JA) の「B1.2.4 CAMS for HIS アラームビルダ」の「■ ユーザ定義属性の追加」の「● ユーザ定義属性の変更」

● Shelving 履歴情報のデフォルト設定

CENTUM プロジェクトを R6.03.00 にリビジョンアップすると、プロジェクトのプロパティダイアログの CAMS for HIS タブシートで、[Shelving 履歴情報] チェックボックスがデフォルトで選択されます。

Shelving 履歴情報を使用しない場合は、リビジョンアップしたあとに、当該タブシートでチェックボックスをクリアしてください。その後で、システムビューから HIS に対して、プロジェクト共通部ダウンロードを再度、実行してください。

参照

Shelving 履歴情報については、以下を参照してください。

統合型アラーム管理リファレンス (IM 33J05A21-01JA) の「B1.1 アラームの警報動作などの定義」の「■ Shelving 履歴情報」

● R6.03.00 より前のプロジェクトの Shelving 履歴情報

R6.03.00 より前の CENTUM プロジェクトで発報された A&E メッセージには、Shelving 履歴情報が付加されません。

● シェルフ名の使用禁止文字

R6.03.00 以降の CAMS for HIS では、シェルフ名として使用できない文字があります。リビジョンアップ前に、シェルフ名に使用禁止文字が使われていないか確認してください。使用禁止文字が使われていた場合は、リビジョンアップする前か、リビジョンアップした後に、禁止文字が使用されているシェルフ名を変更してください。

参照

シェルフ名の使用禁止文字については、以下を参照してください。

統合型アラーム管理リファレンス (IM 33J05A21-01JA) の「B2.1 CAMS for HIS のビルダの設定項目」の「■ CAMS for HIS シェルフビルダの設定項目一覧」

● R6.03.00 にリビジョンアップする前にシェルフ名を変更する

使用禁止文字を変更するために、R6.03.00 にリビジョンアップする前にシェルフ名を変更するときは、次の手順に従ってください。

1. CAMS for HIS シェルフビルダを起動し、シェルフ名をエクスポートしてください。
CSV 形式の外部ファイルが作成されます。
 2. CSV ファイルを Microsoft Excel で表示させて、使用できない文字を削除、または別の文字に置換してから保存してください。
 3. CSV ファイルを CAMS for HIS シェルフビルダにインポートしてください。
 4. CAMS for HIS シェルフビルダで保存してください。
- 以降は、リビジョンアップの作業を実施してください。

参照

CAMS for HIS シェルフビルダについては、以下を参照してください。

統合型アラーム管理リファレンス (IM 33J05A21-01JA) の「B1.2.5 CAMS for HIS シェルフビルダ」

CAMS for HIS のビルダでのエクスポート手順については、以下を参照してください。

統合型アラーム管理リファレンス (IM 33J05A21-01JA) の「B1.2.1 ビルダの共通操作」の「■ エンジニアリング情報を定義するときの一般的な操作」の「● エクスポート」

CAMS for HIS のビルダでのインポート手順については、以下を参照してください。

統合型アラーム管理リファレンス (IM 33J05A21-01JA) の「B1.2.1 ビルダの共通操作」の「■ エンジニアリング情報を定義するときの一般的な操作」の「● インポート」

● R6.03.00 にリビジョンアップしたあとにシェルフ名を変更する

使用禁止文字を変更するために、R6.03.00 にリビジョンアップしたあとにシェルフ名を変更するときは、次の手順に従ってください。

1. CAMS for HIS シェルフビルダを起動してください。
メッセージタブシートに、WARNING メッセージが表示されます。
2. WARNING で指摘されたシェルフ名を変更し、保存してください。
3. システムビューから HIS に対して、プロジェクト共通部ダウンロードを実行してください。

参照

CAMS for HIS シェルフビルダについては、以下を参照してください。

統合型アラーム管理リファレンス (IM 33J05A21-01JA) の「B1.2.5 CAMS for HIS シェルフビルダ」

● HIS のリビジョンが混在しているときの、Shelving 解除の操作履歴の表示形式

リビジョンアップ作業中の期間など、VP プロジェクト内に複数のリビジョンの HIS が混在する状況では、新規起動する HIS と稼動中の HIS のリビジョンの組み合わせによって、Shelving 解除の操作履歴に Shelf 名が表示されない場合があります。Shelving 解除の操作履歴の表示形式を、次の表に示します。

表 C11.16-1 Shelving 解除の操作履歴の表示形式

新規起動する HIS	稼働中の HIS		
	R6.03.00	R4.03.00 以降、R6.03.00 より前	R4.03.00 より前
R6.03.00	Shelf 名を表示	Shelf 名を表示	Shelf 名は非表示
R6.03.00 より前	Shelf 名は非表示		

■ FCS 機能

FCS に関する注意事項を次に示します。

● FFCS-C 電流出力チャネルの出力読み返し機能のデフォルト値の変更

FFCS-C (A2FV50S、A2FV50D) の入出力モジュール (形名 : A2MMM843) の信号種別が電流出力、および電流出力 (HART 通信) であるチャネルにおいて、IOM ビルダのチャネル詳細設定で、定義項目「OOP 検出」のチェックボックスでチェックなしの場合、出力読み返し機能のデフォルト設定が、"Yes" (出力読み返しのチェックを行う) から"No" (出力読み返しのチェックを行わない) に変更となります。

「OOP 検出」なしで、かつ、「出力読み返しチェックを行う」で使用したい場合は、明示的にコマンドライン ORBE=Yes と設定してください。

なお、「OOP 検出」ありの場合は、ORBE=Yes となり「出力読み返しチェックを行う」がデフォルト値となります。

ORBE のデフォルト値を次の表に示します。

表 C11.16-2 ORBE のデフォルト値

	R6.03	R6.01 と R6.02
OOP 検出あり	Yes	Yes
OOP 検出なし	No	Yes

■ Exaopc

R3.74 以前の Exaopc が接続対象としている CENTUM VP システムを R6.03.00 へリビジョンアップする場合は、Exaopc を R3.75 以降にリビジョンアップしてください。

Exaopc を R3.75 以降にリビジョンアップしない場合は、次の様に動作します。

補足

接続対象のシステムには複数プロジェクト結合時の下位プロジェクトも含まれます。

● Exaopc DA サーバ

リビジョンが R3.70～R3.74 の Exaopc では、DA サーバのデータアクセスに影響を与える可能性があります。たとえば、システムに FFCS-R や FFCS-C を追加した場合に、DA サーバのデータアクセスの最大スループットが 4,000 アイテム ID/sec から 2,000 アイテム ID/sec に下がることがあります。

Exaopc の リビジョンが R3.74 の場合は、最大スループットを 4,000 アイテム ID/sec に固定することができます。詳細は Exaopc の IM の「データアクセスの最大スループット」に関する記述を参照ください。

● Exaopc A&E サーバ

新規に追加されたメッセージが A&E サーバから出力されません。

たとえば、R3.74 の Exaopc A&E サーバの場合は、R6.03.00 以降で追加されたコンピュータ切替型 UGS や FFCS-R のメッセージが、Exaopc A&E サーバから出力されません。

C11.17 R6.03.10 へのバージョンアップ／レビジョンアップ

CENTUM VP R6.03.00 から R6.03.10 へのレビジョンアップをして R6.03.10 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R6.03.00 から R6.03.10 にレビジョンアップする場合です。

R6.03.00 より前のレビジョンから R6.03.10 にレビジョンアップ／バージョンアップする場合、これより前に説明した各レビジョン間でのレビジョンアップ／バージョンアップ時の注意も併せてお読みください。

■ AD スイート

AD スイートに関する注意事項を次に示します。

● AD スイートをレビジョンアップするときのエンジニアリング手順

AD サーバのデータのアップグレードと VP プロジェクトのレビジョンアップは必要ありません。AD プロジェクトのレビジョンアップのみを実施してください。

参照

AD スイートをレビジョンアップするときのエンジニアリング手順については、以下を参照してください。

オートメーションデザインスイート基本機能 (IM 33J10A10-01JA) の「B2. レビジョンアップ時のエンジニアリング開始方法」

■ コンピュータ切替型 UGS

コンピュータ切替型 UGS に関する注意事項を次に示します。

● コンピュータ切替型 UGS を使用する場合のネットワークアドレスの制限

コンピュータ切替型 UGS を使用する場合は、Ethernet などのネットワークアドレスに制限があります。

参照

コンピュータ切替型 UGS を使用する場合のネットワークアドレスの制限については、以下を参照してください。

PC 冗長化プラットフォーム はじめにお読みください (IM 30A05C10-01JA)

C11.18 R6.04.00 へのバージョンアップ／レビジョンアップ

CENTUM VP R6.03.10 から R6.04.00 へのレビジョンアップをして R6.04.00 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R6.03.10 から R6.04.00 にレビジョンアップする場合です。

R6.03.10 より前のレビジョンから R6.04.00 にレビジョンアップ／バージョンアップする場合、これより前に説明した各レビジョン間でのレビジョンアップ／バージョンアップ時の注意も併せてお読みください。

■ IT セキュリティ

IT セキュリティに関する注意事項を次に示します。

● バージョンアップ／レビジョンアップのインストール時の IT セキュリティの設定

R6.04.00 で、IT セキュリティバージョンという設定が追加となり、新しく IT セキュリティバージョン 1.0 と IT セキュリティバージョン 2.0 が選択できるようになりました。

R6.03.10 以前の IT セキュリティ設定は IT セキュリティバージョン 1.0 に相当します。

バージョンアップ／レビジョンアップ時に IT セキュリティ設定を変更したくない場合は、IT セキュリティバージョン 1.0 を選択してください。なお、バージョンアップ／レビジョンアップのインストールでは、IT セキュリティバージョンのデフォルトが 1.0 です。

■ FCS

FCS に関する注意事項を次に示します。

● 機能ブロック SI-1ALM

機能ブロック SI-1ALM は、R6.04.00 での新機能です。SI-1ALM は、FFCS-V、FFCS-C、FFCS-R で使用できます。

● デジタル入出力モジュール A2MDV843

デジタル入出力モジュール A2MDV843 は、R6.04.00 での新ハードウェアです。A2MDV843 は、FFCS-C で使用できます。

● アダプタ A2SAM105H、A2SAM505H、A2SAT105

電流入力／電圧入力アダプタ A2SAM105H、電流出力／電圧出力アダプタ A2SAM505H、および mV／熱電対／測温抵抗体入力アダプタ A2SAT105 は、R6.04.00 から FFCS-C で使用できるようになりました。

● 新機能を使用するために必要な作業

R6.04.00 で FCS の新機能を使用するためには、次の作業が必要です。

表 C11.18-1 新機能を使用するために必要とする作業

機能名	システム生成機能のバージョンアップ	FCS の再作成および既存のエンジニアリングデータのインポート	FCS へのオフラインドウロード	操作監視機能のバージョンアップ	全 HIS に対するプロジェクト共通部のダウンロード
SI-1ALM	Yes	Yes	Yes	No	Yes

次に続く

表 C11.18-1 新機能を使用するために必要とする作業（前から続く）

機能名	システム生成機能のバージョンアップ	FCS の再作成および既存のエンジニアリングデータのインポート	FCS へのオフラインダウンロード	操作監視機能のバージョンアップ	全 HIS に対するプロジェクト共通部のダウンロード
A2MDV843	Yes	No	Yes	No	No
A2SAM105H、 A2SAM505H、 A2SAT105 (*1)	Yes	No	Yes	No	No

*1: FFCS-C に定義する場合

■ FDA:21 CFR Part11 対応パッケージ

FDA:21 CFR Part11 対応パッケージに関する注意事項を次に示します。

● エンジニア登録ファイルの格納場所を確認する

エンジニア登録ファイル、処方エンジニア登録ファイル、帳票のユーザセキュリティファイルが、C ドライブ直下にあった場合、管理者権限がないユーザが CENTUM 認証モードでログオンしようとすると、エラーダイアログボックスが表示されます。

また、エンジニア登録ファイル、処方エンジニア登録ファイル、帳票のユーザセキュリティファイルが次のフォルダ以下または当社製品のインストールフォルダ以下にあった場合、エラーメッセージが表示されることがあります。

- C:¥CENTUMVP
- C:¥Program Files (x86)¥Yokogawa
- C:¥Program Files¥Yokogawa
- C:¥Common Files¥Hilscher
- C:¥ProgramData¥Yokogawa

表示されるエラーメッセージを次に示します。

- ロックアウトの設定を取得できませんでした。
- パスワード情報が不正です。

パスワード情報にアクセスできるように管理者に依頼してください。

エンジニア登録ファイル、処方エンジニア登録ファイル、帳票のユーザセキュリティファイルの格納場所を確認するときは、次の手順に従ってください。

1. 次に示すいずれかのユーザで、Windows にログオンしてください。

表 C11.18-2 アクセス制限ユーティリティを起動可能なユーザ

セキュリティモデル	起動可能なユーザ
従来モデル	Administrators グループに所属するユーザ
標準モデル	Administrators グループと CTM_ENGINEER_ADMIN グループの両方に所属するユーザ Administrators グループと CTM_ENGINEER_ADMIN_LCL グループの両方に所属するユーザ Administrators グループと CTM_MAINTENACNE グループの両方に所属するユーザ Administrators グループと CTM_MAINTENACNE_LCL グループの両方に所属するユーザ

2. アクセス制限ユーティリティを起動してください。

履歴管理とアクセス制限を行う対象を選択するための、設定対象選択ダイアログボックスが表示されます。

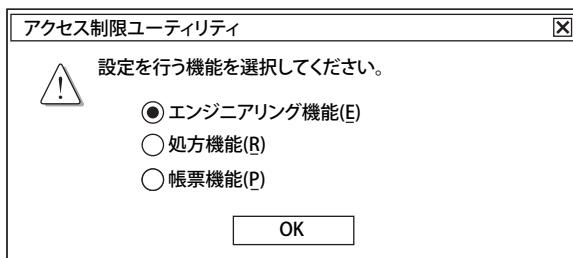


図 C11.18-1 設定対象選択ダイアログボックス

コンピュータにエンジニアリング基本機能、処方管理パッケージ、および帳票パッケージがすべて有効化されていれば、それぞれ別個の履歴管理とアクセス制限を行うことができます。どの機能に対してアクセス制限ユーティリティを起動するのかを、このダイアログボックスで指定してください。

エンジニアリング基本機能、処方管理パッケージ、または帳票パッケージのどれか1つだけが有効化されている場合、このダイアログボックスは表示されず、有効化されているパッケージに対応したアクセス制限ユーティリティが起動されます。

上記のパッケージがどれも有効化されていない場合は、履歴管理データベースビューが起動されます。

3. 設定対象選択ダイアログボックスが表示された場合、確認するファイルに従って、ラジオボタンを選択してください。
 - エンジニア登録ファイルの格納場所を確認するときは、[エンジニアリング機能]を選択してください。
 - 処方エンジニア登録ファイルの格納場所を確認するときは、[処方機能]を選択してください。
 - 帳票のユーザセキュリティファイルの格納場所を確認するときは、[帳票機能]を選択してください。
4. [OK] をクリックしてください。
アクセス制限ユーティリティが表示されます。
5. アクセス制限タブをクリックしてください。
6. 参照先のファイルのパス名を確認してください。
7. ファイルの格納先が不適切だった場合、エクスプローラを使って、次に示すファイルを適切なフォルダにコピーしてください。

表 C11.18-3 コピーするファイル名

移動対象	ファイル名	一緒にコピーするファイル名
エンジニア登録ファイル	EngSecurity.sva	EngPassword.odc
処方エンジニア登録ファイル	RcpSecurity.sva	RcpPassword.odc
帳票のユーザセキュリティファイル	RptSecurity.sva	RptPassword.odc

8. アクセス制限ユーティリティで、ファイルのパス名を変更してください。
9. [OK] をクリックしてください。
アクセス制限ユーティリティが終了します。

● 履歴管理データベースのトップフォルダを確認する

履歴管理データベース、処方の履歴管理データベース、帳票の履歴管理データベースのトップフォルダが、プロジェクトフォルダ以下にあった場合、システムビューでのプロジェクトプロパティ変更時にエラーメッセージが表示され、変更が失敗します。

また、履歴管理データベース、処方の履歴管理データベース、帳票の履歴管理データベースのトップフォルダが次のフォルダ以下または当社製品のインストールフォルダ以下にあった場合、エラーメッセージが表示されることがあります。

- C:\CENTUMVP
- C:\Program Files (x86)\Yokogawa
- C:\Program Files\Yokogawa
- C:\Common Files\Hilscher
- C:\ProgramData\Yokogawa

表示されるエラーメッセージを次に示します。

- 以下のプロジェクトの履歴管理データベースが不正です。

<プロジェクト名>

アクセスが拒否されました。err=0x5

履歴管理データベースにアクセスできるよう管理者に依頼してください。

- ファイル(FDA DB Connection File)を作成できません。

履歴管理データベースにアクセスできるよう管理者に依頼してください。

- 履歴ログの記録に失敗しました。

アクセスが拒否されました。err=0x5

履歴管理データベース、処方の履歴管理データベース、帳票の履歴管理データベースのトップフォルダを確認するときは、次の手順に従ってください。

1. 次のいずれかのユーザで、Windows にログオンしてください。

表 C11.18-4 アクセス制限ユーティリティを起動可能なユーザ

セキュリティモデル	起動可能なユーザ
従来モデル	Administrators グループに所属するユーザ
標準モデル	Administrators グループと CTM_ENGINEER_ADMIN グループの両方に所属するユーザ Administrators グループと CTM_ENGINEER_ADMIN_LCL グループの両方に所属するユーザ Administrators グループと CTM_MAINTENACNE グループの両方に所属するユーザ Administrators グループと CTM_MAINTENACNE_LCL グループの両方に所属するユーザ

2. アクセス制限ユーティリティを起動してください。

履歴管理とアクセス制限を行う対象を選択するための、設定対象選択ダイアログボックスが表示されます。

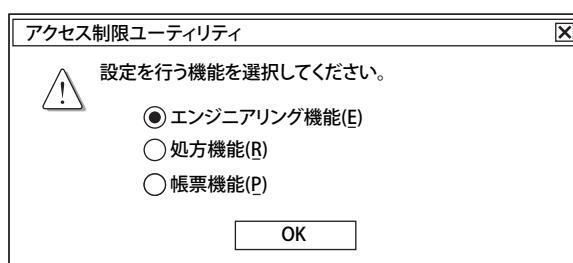


図 C11.18-2 設定対象選択ダイアログボックス

コンピュータにエンジニアリング基本機能、処方管理パッケージ、および帳票パッケージがすべて有効化されていれば、それぞれ別個の履歴管理とアクセス制限を行うことができます。どのアクセス制限ユーティリティを起動するのかを、このダイアログボックスで指定してください。

エンジニアリング基本機能、処方管理パッケージ、または帳票パッケージのどれか1つだけが有効化されている場合、このダイアログボックスは表示されず、有効化されているパッケージに対応したアクセス制限ユーティリティが起動されます。

上記のパッケージがどれも有効化されていない場合は、履歴管理データベースビューが起動されます。

3. 設定対象選択ダイアログボックスが表示された場合、確認するファイルに従って、ラジオボタンを選択してください。
 - ・ 履歴管理データベースのトップフォルダを確認するときは、[エンジニアリング機能] を選択してください。
 - ・ 処方の履歴管理データベースのトップフォルダを確認するときは、[処方機能] を選択してください。
 - ・ 帳票の履歴管理データベースのトップフォルダを確認するときは、[帳票機能] を選択してください。
4. [OK] をクリックしてください。
アクセス制限ユーティリティが表示されます。
5. 電子記録タブをクリックしてください。
6. 履歴管理 DB のフォルダ名のパスを確認してください。
7. フォルダのパスが不適切だった場合、エクスプローラを使って、トップフォルダ以下すべてを適切なフォルダにコピーしてください。
8. アクセス制限ユーティリティの履歴管理 DB の [変更] ボタンをクリックして、トップフォルダ名を変更してください。
9. [OK] をクリックしてください。
アクセス制限ユーティリティが終了します。

■ AD スイート

AD スイートに関する注意事項を次に示します。

● モジュールのファイル保存形式

既存のクラスモジュールやアプリケーションモジュールに、コメント付きシンボルを使用しているロジックチャート(LC-64/LC-64E)が存在する場合、R6.04 以降の AD オーガナイザで、そのクラスモジュールやアプリケーションモジュールに次のどちらかの操作を実行して、チェックインすると、R6.03 以前の AD オーガナイザでチェックアウトできなくなります。

- ・ 制御ドローイングビルダで保存を実行する
- ・ 制御ロジックエディタで、形名変更操作後、保存を実行する

これらの操作を実行した場合は、クラスモジュールやアプリケーションモジュールは新しいファイル形式で保存されます。

新しいファイル保存形式で保存されたクラスモジュールやアプリケーションモジュールでは、ロジックチャートの各素子のコメントを、制御ロジックエディタのタグリストエリアで編集できます。

補足

通常、クラスモジュールのパラメータで「[編集可]」を選択して、モジュール更新マネージャでクラスベースアプリケーションを更新した場合、クラスベースアプリケーションモジュールの該当するパラメータは、変更されません。

しかし、上記の新形式で保存されたクラスモジュールを用いて、R6.03 以前に作成したクラスベースアプリケーションモジュールを更新した場合、初回の更新のみクラスモジュールのロジックチャートの素子のコメントで「[編集可]」を選択していても、クラスベースアプリケーションモジュールのロジックチャートの素子のコメントが更新されます。

C11.19 R6.05.00 へのバージョンアップ／レビジョンアップ

CENTUM VP R6.04.00 から R6.05.00 へのレビジョンアップをして R6.05.00 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R6.04.00 から R6.05.00 にレビジョンアップする場合です。

R6.04.00 より前のレビジョンから R6.05.00 にレビジョンアップ／バージョンアップする場合、これより前に説明した各レビジョン間でのレビジョンアップ／バージョンアップ時の注意も併せてお読みください。

■ 操作監視機能

操作監視機能に関する注意事項を、次に示します。

● タグ重複チェックの自動実行

R6.05.00 より前の操作監視機能では、タグ重複チェックの自動実行の可否を、HIS 設定ウィンドウで設定しました。R6.05.00 では、自動実行の可否設定はなくなり、タグ重複を必ず自動でチェックするようになりました。タグ名の重複を検出すると、システムアラームメッセージが発報されます。

補足

- 重複しているタグ名を特定するときは、HIS 設定ウィンドウからタグ重複チェックを手動で実行してください。
- タグ名の長さは自動的にチェックされません。タグ名の長さをチェックするときは、HIS 設定ウィンドウからタグ重複チェックを手動で実行してください。

参照

タグ重複チェックの手動実行については、以下を参照してください。

操作監視リファレンス Vol.1 (IM 33J05A10-01JA) の「4.3.8 イコライズタブシート」の「■ イコライズタブシートでの設定内容」の「● タグ重複チェック」

■ AD スイート

AD スイートに関する注意事項を次に示します。

● 参照タグのパラメータを追加するときの注意事項

R6.05.00 では、クラスモジュールおよびアプリケーションモジュールの参照タグにパラメータを定義できます。R6.05.00 の AD オーガナイザで R6.04.00 以前のクラスモジュールを利用する場合、次の内容に注意してください。

R6.04.00 以前に定義されたクラスモジュールでは、参照タグのパラメータが含まれていません。そのため、そのクラスモジュールから作成されたクラスベースアプリケーションモジュールの参照タグにパラメータを追加したあとに、クラスベースアプリケーションモジュールを更新すると、参照タグのパラメータは削除されます。参照タグのパラメータを利用する場合、クラスモジュールに参照タグのパラメータを追加してからクラスベースアプリケーションモジュールを更新してください。

参照

アプリケーションモジュールの更新については、以下を参照してください。

オートメーションデザインスイートモジュールベースエンジニアリング (IM 33J10A15-01JA) の「D2.8 クラスモジュールを編集したあと、クラスベースアプリケーションモジュールを更新する」

● ドローイングモジュールの正当性チェック項目の変更

パフォーマンス向上のため、ドローイングモジュールの正当性チェック項目を変更しましたので、注意してください。

ドローイングモジュールの正当性チェックは、次のタイミングで自動的に実施されます。

- ・ ドローイングモジュール保存時
- ・ モジュールバインディング実行時
- ・ ドローイングモジュールチェックイン時

R6.05.00 では、ドローイングモジュールのチェックインまでにすべての項目の正当性チェックが実施されますが、作業途中に実施される正当性チェック項目を変更しました。そのため、正当性チェックで問題を検出するタイミングが、R6.04.00 以前から変わる場合がありますので、注意してください。

なお、[正当性チェック] ボタンによる手動での正当性チェックでは、すべての項目の正当性チェックを実施します。作業途中にすべての項目の正当性チェックを実施するときは、ツールバーの [正当性チェック] ボタンをクリックしてください。

■ バッチ

バッチに関する注意事項を次に示します。

● ユーザ定義コモンブロックの追加時の注意事項

R6.05.00 では、ユーザ定義コモンブロックを 951 個以上作成できるようになりました。ユーザ定義コモンブロックを 951 個以上作成する場合は、原則として、関連する VP プロジェクトのすべての HIS を R6.05.00 にリビジョンアップしてください。

それができない場合は、最低限必要な作業として、バッチサーバステーションの HIS とシステム生成機能を搭載する HIS を R6.05.00 にリビジョンアップしてください。

また、Exaopc OPC インタフェースパッケージ（HIS 搭載用）経由でバッチのデータを収集する場合は、Exaopc OPC インタフェースパッケージ（HIS 搭載用）が動作する HIS を R6.05.00 にリビジョンアップしてください。

補足

原則として、VP プロジェクトの HIS はすべて同一リビジョンにする必要があります。上記のような HIS のリビジョンが混在するような構成は一時的なものととらえ、計画的にすべての HIS を R6.05.00 にリビジョンアップしてください。

Exaopc OPC インタフェースパッケージ（HIS 搭載用）経由でバッチのデータを収集する場合は、さらに次の作業を行ってください。

1. OPC クライアントの設定の再実行

Exaopc OPC インタフェースパッケージ（HIS 搭載用）が動作する HIS とは別のコンピュータで OPC クライアントプログラムを動作させている場合、そのコンピュータで、OPC クライアントの設定を再度実行してください。

2. CENTUM データアクセスライブラリの組み込みの再実行

Exaopc OPC インタフェースパッケージ（HIS 搭載用）が動作する HIS とは別のコンピュータで CENTUM データアクセスライブラリを使用したユーザプログラムを動作させている場合、そのコンピュータで、CENTUM データアクセスライブラリの組み込みを再度実行してください。

● ユーザ定義コモンブロックの追加時のリビジョンアップ例

次の図のようなシステム構成の場合に、リビジョンアップが必要な HIS と作業が必要なコンピュータについて、説明します。

重要

原則、HIS をリビジョンアップする場合は、VP プロジェクトのすべての HIS をすべてリビジョンアップする必要があります。ここでは、それができない場合に、最低限必要なリビジョンアップ対象コンピュータを説明します。この構成は一時的なものととらえ、計画的にすべてのコンピュータをリビジョンアップしてください。

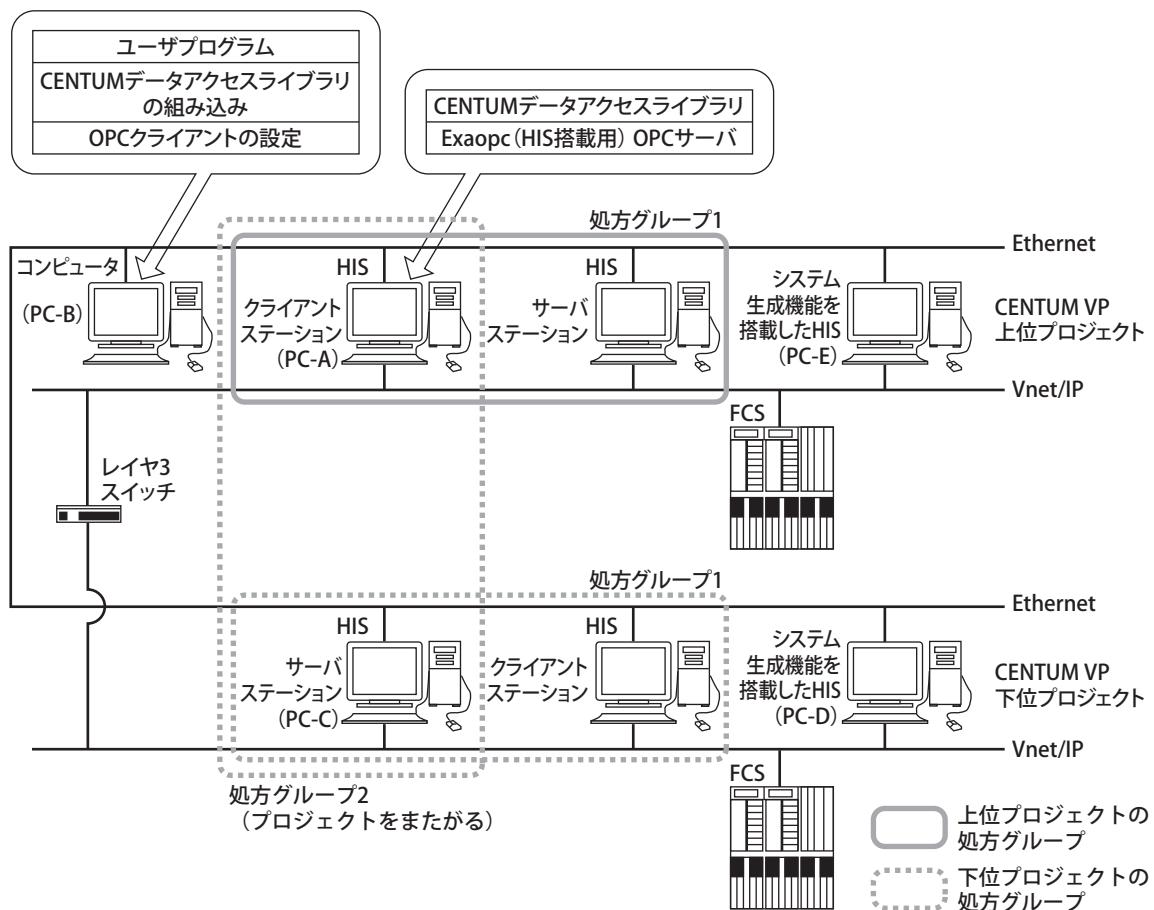


図 C11.19-1 システム構成

図のシステムは次の様な条件です。

- 下位プロジェクトの処方グループ 2 で、上位プロジェクトの HIS (PC-A) から下位プロジェクトの処方を操作監視している。
- 下位プロジェクトのクライアントステーションに指定されている上位プロジェクトの HIS (PC-A) で、Exaopc OPC インタフェースパッケージ (HIS 搭載用) が動作している。
- コンピュータ (PC-B) の CENTUM データアクセライブラリを使用したユーザプログラムは、HIS (PC-A) で動作する Exaopc OPC インタフェースパッケージ (HIS 搭載用) に接続して、GetRcpBlkList メソッドを使用してコモンブロック名一覧を取得している。

この図のシステムで、下位プロジェクトで 951 個以上のユーザ定義コモンブロックを作成した場合は、次の様な作業が最低限必要になります。

- 下位プロジェクトの CENTUM VP バッチサーバステーションの HIS (PC-C) を R6.05.00 にリビジョンアップしてください。このとき、下位プロジェクトのシステム生成機能を搭載した HIS (PC-D) も R6.05.00 にリビジョンアップしてください。
- 下位プロジェクトのクライアントステーションに指定されている、かつ、Exaopc OPC インタフェースパッケージ (HIS 搭載用) が動作する HIS (PC-A) を R6.05.00 にリビ

ジョンアップしてください。このとき、上位プロジェクトのシステム生成機能を搭載した HIS (PC-E) も R6.05.00 にリビジョンアップしてください。

3. コンピュータ (PC-B) で、OPC クライアントの設定を再度実行してください。その後、CENTUM データアクセスライブラリの組み込みを再度実行してください。

● OPC クライアントプログラムおよび CENTUM データアクセスライブラリを使用したユーザプログラムへの影響の確認

ユーザ定義コモンブロックを 951 個以上作成した場合、次に該当するプログラムの改造が必要ないか確認してください。

- CENTUM データアクセスライブラリの GetRcpBlkList メソッドで、コモンブロック名一覧を取得しているユーザプログラム
- Exaopc OPC インタフェースパッケージ (HIS 搭載用) の拡張バッチサーバの BrowseOPCItemIDs メソッドで、コモンブロック名一覧を取得している OPC クライアントプログラム

C11.20 R6.06.00 へのバージョンアップ／レビジョンアップ

CENTUM VP R6.05.00 から R6.06.00 へのレビジョンアップをして R6.06.00 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R6.05.00 から R6.06.00 にレビジョンアップする場合です。

R6.05.00 より前のレビジョンから R6.06.00 にレビジョンアップ／バージョンアップする場合、これより前に説明した各レビジョン間でのレビジョンアップ／バージョンアップ時の注意も併せてお読みください。

■ AD スイート

AD スイートに関する注意事項を次に示します。

● 通信入出力リストの P&ID グループの振る舞いに関する注意事項

R6.06.00 でプログラムグループ定義リストと通信グループ定義リストに [P&ID グループ] の欄が追加になりました。R6.06.00 以降にレビジョンアップしたときに、この [P&ID グループ] の欄は次のように設定されるので、必要に応じて P&ID グループを変更してください。

- シグナル定義リストに定義されている入出力点が属する P&ID グループが設定されている場合、その P&ID グループがプログラムグループ定義リストと通信グループ定義リストの [P&ID グループ] の欄に設定されます。
- プログラムグループ定義リストと通信グループ定義リストに属する入出力点がシグナル定義リストに定義されていない場合、プログラムグループ定義リストと通信グループ定義リストの [P&ID グループ] の欄は空欄になります。
- 異なる P&ID グループに属する入出力点が同じプログラムグループを利用している場合、プログラムグループ定義リストと通信グループ定義リストの [P&ID グループ] の欄は空欄になります。

■ HIS OPC／CENTUM データアクセスライブラリ

OPC サーバが動作する HIS がシステムにあり、その OPC サーバと通信するユーザーアプリケーションを使用している場合は、次の作業を実施してください。

ここでいうユーザーアプリケーションとは、CENTUM データアクセスライブラリを用いたアプリケーションを指します。

● OPC クライアントの開発環境で実施する作業

CENTUM データアクセスライブラリを用いたユーザーアプリケーションを開発するコンピュータで、次の作業を実施してください。なお、開発環境が HIS の場合、(1)と(2)の作業は不要です。

- CENTUM VP R6.06.00 のクライアントセットアップを実行してください。
- CENTUM データアクセスライブラリを利用している場合は、CENTUM VP R6.06.00 の CENTUM データアクセスライブラリを適用してください。
- CENTUM R6.05 までのシステムで使用していたユーザーアプリケーションは、Microsoft Visual Studio 2017 開発環境下でリビルドしてください。なお、ユーザーアプリケーションが .NET Framework アプリケーションの場合、指定する.NET Framework のバージョンは、4.6.2 としてください。

● OPC クライアントの実行環境で実施する作業

CENTUM データアクセスライブラリを用いたユーザアプリケーションを動作させているコンピュータで、次の作業を実施してください。なお、実行環境が HIS の場合、(1)と(2)の作業は不要です。また、開発環境と実行環境が同じ場合は、(3)の作業のみ実施してください。

1. CENTUM VP R6.06.00 のクライアントセットアップを実行してください。
2. CENTUM データアクセスライブラリを利用している場合は、CENTUM VP R6.06.00 の CENTUM データアクセスライブラリを適用してください。
3. CENTUM VP R6.05 まで使用していた CENTUM データアクセスライブラリを用いたユーザアプリケーションを、前述の「OPC クライアントの開発環境で実施する作業」で作成したユーザアプリケーションで置き換えてください。

■ アップグレードライセンス対応製品が複数共存している状態で、製品をレビジョンアップするときの手順

アップグレードライセンス対応製品である VP R6.04 以降の CENTUM VP と RS R4.03 以降の ProSafe-RS が同一コンピュータに共存するときは、次の手順に従ってレビジョンアップしてください。

1. 共存している製品のアップグレードライセンスをそれぞれ配布してください。
2. 各製品をレビジョンアップしてください。

C11.21 R6.07.00 へのバージョンアップ／レビジョンアップ

CENTUM VP R6.06.00 から R6.07.00 へのレビジョンアップをして、R6.07.00 で追加された新機能を用いる場合、機能によっては特殊な作業が必要になるものがあります。

次に述べる注意は R6.06.00 から R6.07.00 にレビジョンアップする場合です。

R6.06.00 より前のレビジョンから R6.07.00 にレビジョンアップ／バージョンアップする場合、これより前に説明した各レビジョン間でのレビジョンアップ／バージョンアップ時の注意事項も併せてお読みください。

■ PROFINET

R6.06 以前に作成した FCS に、PROFINET 通信モジュールである A2LP131 を新規に定義するときは、FCS を作り直してください。

参照

A2LP131 が稼動するためのハードウェア環境については、以下を参照してください。

PROFINET 通信モジュール（N-IO/FIO 用）(GS 33J60G90-01JA)

■ AVR10D の動作モードに関する注意事項

動作モードに「拡張モード」が追加され、新規プロジェクト作成時は「拡張モード」がデフォルトで設定されます。また、既存プロジェクトからバージョンアップ／レビジョンアップした場合、バージョンアップ／レビジョンアップ前の動作モードを引き継ぎます。

参照

AVR10D の動作モードについては、以下を参照してください。

通信機器リファレンス (IM 33J20B10-01JA) の「1.3 V ネットルータのエンジニアリング」の「■ 定数タブシート」の「● 動作モード」

■ AD スイート

AD スイートに関する注意事項を次に示します。

● AD スイートで FCS シーケンスライブラリをエンジニアリングする際の注意事項

CENTUM VP のソフトウェアレビジョンが R6.06.00 以前の VP プロジェクトを R6.07.00 以降にレビジョンアップした場合において、R6.06.00 以前に作成した FCS プロパティの「SEQ ライブラリを AD スイートで定義する」チェックボックスは、デフォルトでクリアされた状態になっています。クリアされた状態から選択状態への変更はいつでもできますが、一度選択した後は、変更できません。このチェックボックスを選択状態にすると、システムビューから起動された FCS シーケンスライブラリビルダは読み取り専用となり、FCS シーケンスライブラリの編集ができなくなります。

補足

R6.07.00 以降に新規作成した FCS プロパティの「SEQ ライブラリを AD スイートで定義する」チェックボックスは、デフォルトで選択された状態になっています。FCS 新規作成時のみ、クリアできます。

R6.06.00 以前に作成された FCS のシーケンスライブラリを、AD スイートでエンジニアリングするときは、次の手順に従ってください。

1. システムビューの FCS シーケンスライブラリビルダで、[ファイル] – [名前を付けて保存] を選択して、FCS シーケンスライブラリを別名保存してください。

補足

システムビューの FCS シーケンスライブラリビルダとは、次のビルダの総称です。

- ・ SEBOL ユーザ関数ビルダ
- ・ SFC ビルダ
- ・ ユニットプロシージャビルダ

-
2. FCS のプロパティで [SEQ ライブラリを AD スイートで定義する] チェックボックスを選択してください。
FCS シーケンスライブラリ削除確認メッセージが表示され、この FCS の FCS シーケンスライブラリが削除されます。
 3. 別名保存した FCS シーケンスライブラリを、AD プロジェクトにインポートしてください。

参照

FCS シーケンスライブラリの AD プロジェクトへのインポートについては、以下を参照してください。

オートメーションデザインスイートモジュールベースエンジニアリング (IM 33J10A15-01JA) の「D5.12 FCS シーケンスライブラリをインポートする」

FCS のプロパティの [SEQ ライブラリを AD スイートで定義する] については、以下を参照してください。

エンジニアリングリファレンス Vol.1 (IM 33J10D10-01JA) の「2.4.1 FCS の新規作成」の「■ SEQ ライブラリを AD スイートで定義する : FFCS-C/FFCS-V」

AD スイートにおける FCS シーケンスライブラリのエンジニアリングについては、以下を参照してください。

オートメーションデザインスイートモジュールベースエンジニアリング (IM 33J10A15-01JA) の「D5. AD オーガナイザで FCS シーケンスライブラリをエンジニアリングする」

Blank Page

D. 他製品との接続

CENTUM VP は、ProSafe-RS、PRM、Exaopc などの当社製品と接続して使用できます。

他製品と接続するときには、セキュリティ設定の変更が必要な場合があります。

ここでは、インストール作業の終了後に、各種製品を接続する方法についての情報と手順を説明します。

Blank Page

D1. 当社他製品との接続

ここでは、当社他製品を接続するときに必要な設定を説明します。

各接続ケースにはインテグレーションコードが割り当てられています。該当するインテグレーションコードで示された製品の組み合わせに対応した設定をしてください。

重要

- 当社製品間を接続するときは、各製品のセキュリティモデルとユーザ管理方法を統一してください。
- 接続する製品で、強固モデルが適用されている場合は、当社までお問い合わせください。

参照

セキュリティモデル、ユーザ管理方法、ユーザとグループ、セキュリティ設定については、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「1.概要」

■ インテグレーションコード

インテグレーションコードの構成は次のとおりです。

(第1パッケージコード) - (第2パッケージコード) - (インテグレーションタイプ) - (レビューション番号)

インテグレーションコードの各構成要素を、次の表に示します。

表 D1-1 インテグレーションコードの構成要素

構成要素	説明
パッケージコード	コンピュータに単独でインストールできるソフトウェアパッケージ単位に付けるコードです。 第1パッケージコードは製品1のパッケージコードを、第2パッケージコードは製品2のパッケージコードを指します。
インテグレーションタイプ	各種製品の接続形態を表します。 <ul style="list-style-type: none"> 01：同一のコンピュータにインストールした製品を個別に操作し、製品間で通信やファイル共有をしない。 02：別々のコンピュータにインストールした製品を個別に操作し、製品間で通信やファイル共有をする。 03：同一または別々のコンピュータにインストールした製品を操作し、製品間で通信やファイル共有をする。
レビューション番号	インテグレーションコードのレビューション番号です。 新しい製品のリリースで設定手順や接続方法が変更されると、この番号が更新されます レビューション番号は、01～99です。

重要

- インテグレーションタイプ 02 の組み合わせの製品は、同一のコンピュータにインストールできません。
- 各製品のユーザーズマニュアルには、他製品と接続するときに必要な設定が記載されています。しかし、製品によってリリース時期が異なるため、ユーザーズマニュアルの間に、接続のための設定情報が違ってくることがあります。常に最新の情報を得るために双方のユーザーズマニュアルを参照し、組み合わせる製品のバージョンとインテグレーションコードのレビューション番号を見て、新しい方の設定手順に従ってください。

● パッケージコード

CENTUM との連携に関するパッケージコードを、次の表に示します。

表 D1-2 パッケージコード

パッケージコード	製品	パッケージ
0101	CENTUM VP	CENTUM VP 操作監視基本機能 (*1)
0102	CENTUM VP	システム生成機能
0121	CENTUM VP	エンジニアリングサーバ機能
0196	CENTUM VP	プロジェクトデータベース
0201	ProSafe-RS	安全システム生成・保守パッケージ
0202	ProSafe-RS	SOE OPC インタフェースパッケージ
0203	ProSafe-RS	CENTUM VP/CS 3000 統合エンジニアリングパッケージ
0205	ProSafe-RS	エンジニアリングサーバ
0251	ProSafe-RS	SOE ビューアパッケージ
0302	PRM	統合機器管理サーバ
0401	Exaopc	Exaopc OPC インタフェースパッケージ
0601	Exapilot	Exapilot 運転効率向上支援パッケージ サーバ
0651	Exapilot	Exapilot 運転効率向上支援パッケージ クライアント
0701	Exaplog	Exaplog イベント解析パッケージ サーバ
0801	Exaquantum	PIMS サーバ
0851	Exaquantum	Explorer クライアント
0951	Exasmoc	Exasmoc クライアント
1051	Exarqe	Exarqe クライアント
1551	Multivariable Optimizing Control/Robust Quality Estimation	Multivariable Optimizing Control/Robust Quality Estimation パッケージクライアント (APC クライアント)

*1: オプション機能として、Exaopc OPC インタフェースパッケージ (HIS 搭載用) があります。統合型アラーム管理機能 (CAMS for HIS) は、操作監視基本機能に含まれます。

D1.1 CENTUM VP と ProSafe-RS

ここでは、CENTUM VP と ProSafe-RS を接続するときの設定について説明します。

重要 CENTUM VP と ProSafe-RS のソフトウェアを同一のコンピュータにインストールする場合は、CENTUM VP R6.06.00 以降と ProSafe-RS R4.04.00 以降のソフトウェアレビジョンの組み合わせで使用してください。

D1.1.1 CENTUM VP - 操作監視基本機能と ProSafe-RS - SOE ビューアパッケージ

CENTUM VP の操作監視基本機能と ProSafe-RS の SOE ビューアパッケージを接続すると、ProSafe-RS の SOE ビューアで CENTUM VP の HIS のヒストリカル情報を参照できます。

■ ProSafe-RS の SOE ビューアで CENTUM VP のヒストリカル情報を参照する

接続情報を次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

表 D1.1.1-1 接続情報

インテグレーションコード	0101-0251-03-04	
製品 1	CENTUM VP R5.01 以降 (*1) - 操作監視基本機能	
製品 2	ProSafe-RS R3.01 以降 (*1) - SOE ビューアパッケージ	
セキュリティモデル	従来モデル	標準モデル
ユーザ管理方法	-	スタンダードアロン管理 ドメイン管理／併用管理
必要な手順	なし	「●標準モデルの場合」を参照してください。

*1: CENTUM VP と ProSafe-RS のソフトウェアを同一のコンピュータにインストールする場合は、CENTUM VP R6.06.00 以降と ProSafe-RS R4.04.00 以降のソフトウェアレビジョンの組み合わせで使用してください。

● 標準モデルの場合

この設定は、ユーザ管理方法がスタンダードアロン管理の場合は、ProSafe-RS の SOE ビューアを使用するコンピュータで行ってください。ドメイン管理または併用管理の場合は、ドメインコントローラで行ってください。

- 同一のコンピュータにインストールした製品を連携させる場合
ProSafe-RS の SOE ビューアを使用するユーザアカウントを、CTM_OPERATOR グループに所属させてください。
- 別々のコンピュータにインストールした製品を連携させる場合
ProSafe-RS の SOE ビューアを使用するユーザアカウントを、CENTUM VP HIS が動作するコンピュータに登録してください。登録するユーザアカウントのユーザ名とパスワードは、ProSafe-RS の SOE ビューアを使用するユーザアカウントのユーザ名とパスワードと同一にする必要があります。また、登録したユーザアカウントを CTM_OPERATOR グループに所属させてください。

参照

ドメイン管理または併用管理でユーザアカウントを作成し、グループに所属させる方法については、以下を参照してください。

「B2.5 ドメインユーザを作成する」ページ B2-16

スタンダードアロン管理でユーザアカウントを作成し、グループに所属させる方法については、以下を参照してください。

「B4.9.1 標準モデル：スタンダードアロン管理のセキュリティ設定の場合」ページ B4-105

D1.1.2 CENTUM VP - 操作監視基本機能と ProSafe-RS - SOE OPC インタフェースパッケージ

CENTUM VP の Exaopc OPC インタフェースパッケージ (HIS 搭載用) と ProSafe-RS の SOE OPC インタフェースパッケージが、同じコンピュータにインストールされているときの設定を説明します。

両方のパッケージを搭載しているコンピュータが次のケースに該当するときは、ケースごとに記載された設定をすべて実施してください。

- 両方のパッケージを搭載しているコンピュータが、OPC 通信の OPC サーバコンピュータとして指定されている
- 両方のパッケージを搭載しているコンピュータで OPC クライアント機能を利用していている
- ドメイン管理または併用管理の場合で、両方のパッケージを搭載しているコンピュータが、ドメインに参加していない OPC クライアントコンピュータに OPC 通信の通信先サーバコンピュータとして指定されている

■ 両方のパッケージを搭載したコンピュータが、OPC 通信の通信先 OPC サーバコンピュータとして指定されているとき

接続情報を次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

表 D1.1.2-1 接続情報

インテグレーションコード	0101-0202-01-01		
製品 1	CENTUM VP R5.01 以降 - 操作監視基本機能		
製品 2	ProSafe-RS R3.01 以降 - ProSafe-RS SOE OPC インタフェースパッケージ		
セキュリティモデル	従来モデル	標準モデル	
ユーザ管理方法	-	スタンドアロン管理	ドメイン管理／併用管理
必要な手順	なし	「●標準モデルの場合」を参照してください。	

● 標準モデルの場合

OPC クライアントコンピュータで対象となる OPC クライアント機能を使用するユーザーアカウントを、OPC サーバコンピュータで CTM_OPC と PSF_OPC グループに所属させてください。

ドメイン管理または併用管理の場合は、この設定をドメインコントローラで実施してください。スタンドアロン管理の場合は、OPC クライアントコンピュータで OPC クライアント機能を使用するローカルユーザと同じ名称のユーザーアカウントを OPC サーバコンピュータに追加し、CTM_OPC と PSF_OPC グループに所属させてください。

参照

ドメイン管理または併用管理でユーザーアカウントを作成し、グループに所属させる方法については、以下を参照してください。

「B2.5 ドメインユーザを作成する」ページ B2-16

スタンドアロン管理でユーザーアカウントを作成し、グループに所属させる方法については、以下を参照してください。

「B4.9.1 標準モデル：スタンドアロン管理のセキュリティ設定の場合」ページ B4-105

● OPC クライアント機能を使用するユーザ

OPC クライアント機能を使用するユーザを、次の表に示します。

表 D1.1.2-2 OPC クライアント機能を使用するユーザ

OPC クライアント機能	ユーザ
帳票パッケージ	Windows のログオンユーザ
FDA:21 CFR Part 11 対応パッケージ	Windows のログオンユーザ
CENTUM VP 製品以外の OPC クライアント (*1)	OPC クライアント機能を使用するユーザ

*1: CENTUM データアクセスライブラリを利用して作成した機能も含みます。

■ 両方のパッケージを搭載したコンピュータで OPC クライアント機能を利用しているとき

接続情報を次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

表 D1.1.2-3 接続情報

インテグレーションコード	0101-0202-01-01		
製品 1	CENTUM VP R5.01 以降 - 操作監視基本機能		
製品 2	ProSafe-RS R3.01 以降 - ProSafe-RS SOE OPC インタフェースパッケージ		
セキュリティモデル	従来モデル	標準モデル	
ユーザ管理方法	-	スタンドアロン管理	ドメイン管理／併用管理
必要な手順	なし	「●標準モデルの場合」を参照してください。	

● 標準モデルの場合

OPC クライアント機能を使用するユーザアカウントを、CTM_OPC と PSF_OPC グループに所属させてください。

この設定は、ユーザ管理方法がスタンドアロン管理の場合は、OPC クライアントコンピュータで行ってください。ドメイン管理または併用管理の場合は、ドメインコントローラで行ってください。

参照

ドメイン管理または併用管理でユーザアカウントを作成し、グループに所属させる方法については、以下を参照してください。

「B2.5 ドメインユーザを作成する」ページ B2-16

スタンドアロン管理でユーザアカウントを作成し、グループに所属させる方法については、以下を参照してください。

「B4.9.1 標準モデル：スタンドアロン管理のセキュリティ設定の場合」ページ B4-105

● OPC クライアント機能を使用するユーザ

OPC クライアント機能を使用するユーザを、次の表に示します。

表 D1.1.2-4 OPC クライアント機能を使用するユーザ

OPC クライアント機能	ユーザ
帳票パッケージ	Windows のログオンユーザ
FDA:21 CFR Part 11 対応パッケージ	Windows のログオンユーザ

次に続く

表 D1.1.2-4 OPC クライアント機能を使用するユーザ (前から続く)

OPC クライアント機能	ユーザ
FCS データ設定／収集パッケージ (PICOT)	Windows のログオンユーザ
統合型アラーム管理機能 (CAMS for HIS)	OPC A&E サーバ接続設定をするときに指定したユーザ
CENTUM VP 製品以外の OPC クライアント (*1)	OPC クライアント機能を使用するユーザ

*1: CENTUM データアクセスライブラリを利用して作成した機能も含みます。

● FCS データ設定／収集パッケージ (PICOT) を使用しているとき

FCS データ設定／収集パッケージ (PICOT) を使用し、かつ HIS タイプシングルサインオンを使用するときは、次の設定を追加してください。

スタンドアロン管理の場合：当該コンピュータで OFFUSER を PSF_OPC グループに所属させてください。

ドメイン管理／併用管理の場合：当該コンピュータで OFFUSER を PSF_OPC_LCL グループに所属させてください。

■ 両方のパッケージを搭載したコンピュータが、ドメインに参加していない OPC クライアントコンピュータに OPC 通信の通信先サーバコンピュータとして指定されている

ドメイン管理または併用管理の場合で、両方のパッケージを搭載したコンピュータが、ドメインに参加していない OPC クライアントコンピュータに OPC 通信の通信先サーバコンピュータとして指定されているときの接続情報を、次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

表 D1.1.2-5 接続情報

インテグレーションコード	0101-0202-01-03
製品 1	CENTUM VP R5.01 以降 (*1) - 操作監視基本機能
製品 2	ProSafe-RS R3.01 以降 (*1) - ProSafe-RS SOE OPC インタフェースパッケージ
セキュリティモデル	標準モデル
ユーザ管理方法	ドメイン管理／併用管理
必要な手順	「●接続に必要な手順」を参照してください。

*1: CENTUM VP と ProSafe-RS のソフトウェアを同一のコンピュータにインストールする場合は、CENTUM VP R6.06.00 以降と ProSafe-RS R4.04.00 以降のソフトウェアレビジョンの組み合わせで使用してください。

● 接続に必要な手順

OPC クライアントコンピュータで OPC 通信を使用するローカルユーザと同じ名称のユーザアカウントを、OPC サーバコンピュータに追加し、CTM_OPC_LCL、PSF_OPC_LCL グループに所属させてください。

参照

スタンドアロン管理でユーザアカウントを作成し、グループに所属させる方法については、以下を参照してください。

「B4.9.1 標準モデル：スタンドアロン管理のセキュリティ設定の場合」ページ B4-105

ドメイン管理または併用管理でユーザアカウントを作成し、グループに所属させる方法については、以下を参照してください。

「B2.5 ドメインユーザを作成する」ページ B2-16

● OPC クライアント機能を使用するローカルユーザ

OPC クライアント機能を使用するローカルユーザを、次の表に示します。

表 D1.1.2-6 OPC クライアント機能を使用するローカルユーザ

OPC クライアント機能	ユーザ
帳票パッケージ	Windows のログオンユーザ
CENTUM VP 製品以外の OPC クライアント (*1)	OPC クライアント機能を使用するユーザ

*1: CENTUM データアクセスライブラリを利用して作成した機能も含みます。

D1.1.3 CENTUM VP - システム生成機能と ProSafe-RS - CENTUM VP 統合パッケージ

ProSafe-RS の CENTUM VP 統合パッケージを使用して、CENTUM VP と ProSafe-RS の統合システムを構築できます。

■ CENTUM VP と ProSafe-RS の統合システムを構築する

接続情報を次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

表 D1.1.3-1 接続情報

インテグレーションコード	0102-0203-03-04		
製品 1	CENTUM VP R5.01 以降 (*1) - システム生成機能		
製品 2	ProSafe-RS R3.01 以降 (*1) - CENTUM VP 統合パッケージ		
セキュリティモデル	従来モデル	標準モデル	
ユーザ管理方法	-	スタンドアロン管理	ドメイン管理／併用管理
必要な手順	なし	「●標準モデルの場合」を参照してください。	

*1: CENTUM VP と ProSafe-RS のソフトウェアを同一のコンピュータにインストールする場合は、CENTUM VP R6.06.00 以降と ProSafe-RS R4.04.00 以降のソフトウェアレビジョンの組み合わせで使用してください。

● 標準モデルの場合

- CENTUM VP プロジェクトが SCS Manager を使用するコンピュータにある場合：
ProSafe-RS の SCS Manager を使用するユーザアカウントを、CTM_ENGINEER と PSF_ENGINEER グループに所属させてください。
この設定は、ユーザ管理方法がスタンドアロン管理の場合は、SCS Manager を使用するコンピュータで行ってください。ドメイン管理または併用管理の場合は、ドメインコントローラで行ってください。
- CENTUM VP プロジェクトが SCS Manager を使用するコンピュータ以外のコンピュータにある場合：
スタンドアロン管理の場合は、SCS Manager を使用するユーザアカウントと同じ名称のユーザアカウントを、CENTUM VP プロジェクトが置いてあるコンピュータに作成し、CTM_ENGINEER グループに所属させてください。
ドメイン管理または併用管理の場合は、ドメインコントローラで、SCS Manager を使用するユーザアカウントを CTM_ENGINEER グループに所属させてください。

参照

ドメイン管理または併用管理でユーザアカウントを作成し、グループに所属させる方法については、以下を参照してください。

「B2.5 ドメインユーザを作成する」ページ B2-16

スタンドアロン管理でユーザアカウントを作成し、グループに所属させる方法については、以下を参照してください。

「B4.9.1 標準モデル：スタンドアロン管理のセキュリティ設定の場合」ページ B4-105

D1.1.4 CENTUM VP - システム生成機能と ProSafe-RS - 安全システムエンジニアリング・保守機能

CENTUM VP のシステム生成機能と ProSafe-RS の安全システムエンジニアリング・保守機能を接続して、ProSafe-RS の SCS シミュレータで SCS シミュレーションテストが実施できます。

■ SCS シミュレータで SCS シミュレーションテストを実施する

接続情報を次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

表 D1.1.4-1 接続情報

インテグレーションコード	0102-0201-03-04	
製品 1	CENTUM VP R5.01 以降 (*1) - システム生成機能	
製品 2	ProSafe-RS R3.01 以降 (*1) - 安全システムエンジニアリング・保守機能	
セキュリティモデル	従来モデル	標準モデル
ユーザ管理方法	-	スタンドアロン管理 ドメイン管理／併用管理
必要な手順	なし	「●標準モデルの場合」を参照してください。

*1: CENTUM VP と ProSafe-RS のソフトウェアを同一のコンピュータにインストールする場合は、CENTUM VP R6.06.00 以降と ProSafe-RS R4.04.00 以降のソフトウェアレビジョンの組み合わせで使用してください。

● 標準モデルの場合

ProSafe-RS の SCS Manager または CENTUM VP のシステムビューを使用するすべてのユーザーアカウントを CTM_ENGINEER と PSF_ENGINEER グループに所属させてください。この設定は、ユーザ管理方法がスタンドアロン管理の場合は、ProSafe-RS の SCS Manager とシステムビューを使用するコンピュータで行ってください。ドメイン管理または併用管理の場合は、ドメインコントローラで行ってください。

参照

スタンドアロン管理でユーザーアカウントを作成し、グループに所属させる方法については、以下を参照してください。

「B4.9.1 標準モデル：スタンドアロン管理のセキュリティ設定の場合」ページ B4-105

ドメイン管理または併用管理でユーザーアカウントを作成し、グループに所属させる方法については、以下を参照してください。

「B2.5 ドメインユーザを作成する」ページ B2-16

D1.1.5 CENTUM VP - エンジニアリングサーバ機能と ProSafe-RS - 安全システムエンジニアリング・保守機能

CENTUM VP のエンジニアリングサーバ機能と ProSafe-RS の安全システムエンジニアリング・保守機能を接続すると、AD スイートのクライアント機能と AD スイートのサーバ機能が連携し、I/O リストエンジニアリングや変更管理機能を使用できます。

■ CENTUM VP のエンジニアリングサーバを使用して ProSafe-RS の安全システムエンジニアリング・保守を実施する

接続情報を次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

表 D1.1.5-1 接続情報

インテグレーションコード	0121-0201-03-02		
製品 1	CENTUM VP R6.02 以降 (*1) - エンジニアリングサーバ機能		
製品 2	ProSafe-RS R4.01 以降 (*1) - 安全システムエンジニアリング・保守機能		
セキュリティモデル	従来モデル	標準モデル	
ユーザ管理方法	-	スタンダード管理	ドメイン管理／併用管理
必要な手順	「●従来モデルの場合」を参照してください。 「●標準モデルの場合」を参照してください。		

*1: CENTUM VP と ProSafe-RS のソフトウェアを同一のコンピュータにインストールする場合は、CENTUM VP R6.06.00 以降と ProSafe-RS R4.04.00 以降のソフトウェアレビジョンの組み合わせで使用してください。

● 従来モデルの場合

本機能を利用する Windows ユーザを AD スイートのクライアントコンピュータと AD スイートのサーバコンピュータに作成してください。

ADS 管理ツールを使って、当該 Windows ユーザをエンジニアリングサーバに登録してください。

● 標準モデルの場合

本機能を利用する Windows ユーザを AD スイートのクライアントコンピュータと AD スイートのサーバコンピュータに作成してください。

ユーザアカウントを CTM_ENGINEER と PSF_ENGINEER グループに所属させてください。ユーザ管理方法がスタンダード管理の場合は、CENTUM VP のエンジニアリングサーバを使用するコンピュータと ProSafe-RS の安全システムエンジニアリング・保守機能を使用するコンピュータでこの設定をしてください。

ドメイン管理または併用管理の場合は、ドメインコントローラで行ってください。

ADS 管理ツールを使って、当該 Windows ユーザをエンジニアリングサーバに登録してください。

D1.1.6 CENTUM VP - システム生成機能と ProSafe-RS - エンジニアリングサーバ機能

CENTUM VP のシステム生成機能と ProSafe-RS のエンジニアリングサーバ機能を接続すると、AD スイートのクライアント機能と AD スイートのサーバ機能が連携し、モジュールベースエンジニアリングや変更管理機能を使用できます。

■ ProSafe-RS のエンジニアリングサーバを使用して CENTUM VP のシステム生成を実施する

接続情報を次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

表 D1.1.6-1 接続情報

インテグレーションコード	0205-0102-03-02		
製品 1	ProSafe-RS R4.01 以降 (*1) - エンジニアリングサーバ機能		
製品 2	CENTUM VP R6.02 以降 (*1) - システム生成機能		
セキュリティモデル	従来モデル	標準モデル	
ユーザ管理方法	-	スタンダード管理	ドメイン管理／併用管理
必要な手順	「●従来モデルの場合」を参照してください。		

*1: CENTUM VP と ProSafe-RS のソフトウェアを同一のコンピュータにインストールする場合は、CENTUM VP R6.06.00 以降と ProSafe-RS R4.04.00 以降のソフトウェアレビジョンの組み合わせで使用してください。

● 従来モデルの場合

本機能を利用する Windows ユーザを AD スイートのクライアントコンピュータと AD スイートのサーバコンピュータに作成してください。

ADS 管理ツールを使って、当該 Windows ユーザをエンジニアリングサーバに登録してください。

● 標準モデルの場合

本機能を利用する Windows ユーザを AD スイートのクライアントコンピュータと AD スイートのサーバコンピュータに作成してください。

ユーザアカウントを CTM_ENGINEER と PSF_ENGINEER グループに所属させてください。ユーザ管理方法がスタンダード管理の場合は、CENTUM VP のシステム生成機能を使用するコンピュータと ProSafe-RS のエンジニアリングサーバを使用するコンピュータでの設定をしてください。

ドメイン管理または併用管理の場合は、ドメインコントローラで行ってください。

ADS 管理ツールを使って、当該 Windows ユーザをエンジニアリングサーバに登録してください。

D1.2 CENTUM VP と PRM

ここでは、CENTUM VP と PRM を接続するときの設定について説明します。

D1.2.1 CENTUM VP 操作監視基本機能と PRM サーバ

CENTUM VP 操作監視基本機能と PRM サーバを接続すると、PRM が CENTUM VP からメッセージを受信できるようになります。

CENTUM VP に、Exaopc OPC インタフェースパッケージ（HIS 搭載用）が必要です。

■ PRM が CENTUM VP R5 以降からメッセージを取得できるようにする

接続方法を次の表に示します。その後に、製品の接続に必要な手順を示します。

表 D1.2.1-1 接続情報

インテグレーションコード	0101-0302-02-03		
製品 1	CENTUM VP R5.01 以降の操作監視基本機能 (*1)		
製品 2	PRM R3.30 以降の統合機器管理サーバ		
セキュリティモデル	従来モデル	標準モデル	
ユーザ管理タイプ	—	スタンダードアロン管理	ドメイン管理／併用管理
必須手順	「● CENTUM VP R5.01 以降のコンピュータに従来モデルを適用している場合」を参照。	「● CENTUM VP R5.01 以降のコンピュータに標準モデルを適用している場合」を参照。	

*1: Exaopc OPC インタフェースパッケージ（HIS 搭載用）は、CENTUM VP 操作監視基本機能のオプション機能です。

● CENTUM VP R5.01 以降のコンピュータに従来モデルを適用している場合

CENTUM VP を実行しているコンピュータで、CreateInternalUserAccount ユーティリティを使用して PRMUSER アカウントを作成する必要があります。本ユーティリティは、PRM インストールメディアに収録されています。

PRMUSER アカウントを作成するときは、次の手順に従ってください。

- 管理者権限を持つユーザとしてログオンしてください。
- PRM インストールメディアを DVD ドライブに挿入してください。
- コマンドプロンプトウィンドウを開き、次のコマンドを実行してください。

```
<DVD ドライブ>:\PRM\Utility\CreateInternalUserAccount.exe -sm legacy
```

 PRMUSER アカウントが作成されます。
- HIS ユーティリティを起動してください。
- [OPC] タブをクリックしてください。
- [OPC サーバ接続時のログオン設定] セクションで、[変更] をクリックしてください。
 ログオン方式選択ダイアログボックスが表示されます。
- [OPC サーバへの接続時の自動ログオンを有効にする] を選択してください。
- [自動ログオンユーザ登録] または [互換動作 (R4.03 以前と互換)] を選択してください。
- [OK] をクリックしてください。

参照

HIS ユーティリティの OPC タブシートでのログオン方式の選択手順については、以下を参照してください。

CENTUM VP オプション機能リファレンス (IM 33J05H10-01JA) の「1.2 OPC に関するエンジニアリング」の「■ HIS ユーティリティ」

● CENTUM VP R5.01 以降のコンピュータに標準モデルを適用している場合

CENTUM VP を実行しているコンピュータで、CreateInternalUserAccount ユーティリティを使用して PRM_PROCESS と PRM_PROCESS2 のユーザーアカウントを作成する必要があります。本ユーティリティは、PRM インストールメディアに収録されています。

PRM_PROCESS と PRM_PROCESS2 のユーザーアカウントを作成するときは、次の手順に従ってください。

1. 管理者権限を持つユーザとしてログオンしてください。
2. PRM インストールメディアを DVD ドライブに挿入し、次のフォルダに移動してください。

<DVD ドライブ>:\PRM\Utility\SecuritySettingUtility

3. [CreateInternalUserAccount.exe] をダブルクリックしてください。

PRM_PROCESS と PRM_PROCESS2 のユーザーアカウントが作成され、自動で次のいずれかのグループに追加されます。

スタンダードアロン管理の場合： CTM_OPC

ドメイン管理の場合： CTM_OPC_LCL

併用管理の場合： CTM_OPC または CTM_OPC_LCL

4. HIS ユーティリティを起動してください。
5. [OPC] タブをクリックしてください。
6. [OPC サーバ接続時のログオン設定] セクションで、[変更] をクリックしてください。
ログオン方式選択ダイアログボックスが表示されます。
7. ログオン方式を選択してください。
8. [OK] をクリックしてください。

重要

[OPC サーバへの接続時に、ログオンを必要とする] を選択する場合、PRM サーバのコンピュータでメッセージ収集とアラーム配信ルールを設定するときは、ログオン詳細を指定してください。

参照

HIS ユーティリティの OPC タブシートでのログオン方式の選択手順については、以下を参照してください。

CENTUM VP オプション機能リファレンス (IM 33J05H10-01JA) の「1.2 OPC に関するエンジニアリング」の「■ HIS ユーティリティ」

D1.2.2 PRM サーバと CENTUM VP 操作監視基本機能

PRM サーバと CENTUM VP 操作監視基本機能を接続すると、CENTUM VP の統合型アラーム管理機能（CAMS for HIS）が PRM からメンテナンスマッセージを受信できるようになります。

CENTUM VP に、Exaopc OPC インタフェースパッケージ（HIS 搭載用）が必要です。

■ CAMS for HIS が PRM からメンテナンスマッセージを受信できるようにする

接続情報を次の表に示します。その後に、製品の接続に必要な手順を示します。

表 D1.2.2-1 接続情報

インテグレーションコード	0302-0101-02-02		
製品 1	統合機器管理サーバ		
製品 2	CENTUM VP R4.03 以降の操作監視基本機能(*1)		
セキュリティモデル	従来モデル	標準モデル	
ユーザ管理タイプ	一	スタンダードアロン管理	ドメイン管理／併用管理
必須手順	「● 従来モデルの場合」を参照	「● 標準モデルの場合」を参照	

*1: CAMS for HIS は操作監視基本機能に含まれています。

● 注意事項

- CAMS for HIS は、PRM から受信したメッセージを「設備」アラームタイプ（TypeOfAlarm）として分類します。ただし、PRM アドバンスト診断サーバパッケージがインストールされていて、PRM セットアップツールのアドバンスト診断ペインで [次の設定で HIS にメッセージを送信する] オプションが選択されている場合、メッセージは「ガイダンス」として分類されます。
- PRM クライアントと CAMS for HIS でメッセージを表示するには、アラーム管理ツールの 2 つのアラーム管理ルールを同じ条件に定義する必要があります。ただし、アクション定義の配信対象を、一方のルールでは「メンテナンス」に、もう一方のルールでは「オペレータ」に設定する必要があります。

● 従来モデルの場合

CENTUM VP の HIS ユーティリティで、CAMS for HIS の設定をしてください。

CAMS for HIS を設定するときは、次の手順に従ってください。

- 管理者権限を持つユーザとしてログオンして HIS ユーティリティを起動してください。
- HIS ユーティリティの [CAMS for HIS] タブで、[統合型アラーム管理を有効にする] チェックボックスを選択してください。
- [OPC A&E サーバ接続設定] をクリックしてください。
OPC A&E サーバ接続設定ダイアログボックスが表示されます。
- [OPC A&E サーバのコンピュータ名] ボックスに、PRM サーバのコンピュータ名を指定してください。
- [OPC A&E サーバプログラム ID] ボックスに、Yokogawa.ExaopcAEPRM.1 と入力してください。
- OPC A&E サーバ接続設定ダイアログボックスで、[OK] をクリックしてください。
- HIS ユーティリティで、[OK] をクリックしてください。

● 標準モデルの場合

CAMS for HIS を設定するときは、次の手順に従ってください。

1. PRM サーバのコンピュータで、ユーザアカウントを作成し、パスワードを設定してください。

ユーザアカウント名は、PRM_OPCT_USER にすることを推奨します。

2. 作成したユーザアカウントを、次のいずれかのグループに追加してください。

スタンダードアロン管理の場合： PRM_OPCT

ドメイン管理の場合： PRM_OPCT_LCL

併用管理の場合： PRM_OPCT または PRM_OPCT_LCL

重要

CENTUM HIS で PRM への OPC A&E サーバ接続を設定するときは、ここで設定したユーザ名と、CENTUM HIS ユーティリティで使用されるパスワードを指定してください。

3. CENTUM VP の HIS ユーティリティで CAMS for HIS を設定するには、次の手順を実行してください。

- a. 管理者権限を持つユーザとしてログオンして HIS ユーティリティを起動してください。

b. HIS ユーティリティの [CAMS for HIS] タブで、[統合型アラーム管理を有効にする] チェックボックスを選択してください。

- c. [OPC A&E サーバ接続設定] をクリックしてください。

OPC A&E サーバ接続設定ダイアログボックスが表示されます。

- d. [OPC A&E サーバのコンピュータ名] ボックスに、PRM サーバのコンピュータ名を指定してください。

- e. [OPC A&E サーバプログラム ID] ボックスに、Yokogawa.ExaopcAEPRM.1 と入力してください。

- f. [適用] をクリックしてください。

OPC A&E サーバのユーザ認証ダイアログボックスが表示されます。

- g. PRM サーバで作成したユーザの名前とパスワードを指定してください。

- h. [OK] をクリックしてください。

- i. OPC A&E サーバ接続設定ダイアログボックスで、[OK] をクリックしてください。

- j. HIS ユーティリティで、[OK] をクリックしてください。

D1.3 CENTUM VP と Exaopc

ここでは、CENTUM VP と Exaopc を接続するときの設定について説明します。

重要

接続する製品のセキュリティモデルとユーザ管理方法は統一することが原則です。しかし、CENTUM VP と Exaopc は、セキュリティモデルやユーザ管理方法が違っても接続できます。

D1.3.1 CENTUM VP - 操作監視基本機能と Exaopc サーバ

CENTUM VP の操作監視基本機能と Exaopc サーバを接続すると、OPC インタフェースを介してクライアントが CENTUM VP のデータを使用できるようになります。

■ CENTUM VP の操作監視基本機能と Exaopc を接続する

接続情報を次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

表 D1.3.1-1 接続情報

インテグレーションコード	0101-0401-02-01	
製品 1	CENTUM VP R5.01 以降 - 操作監視基本機能	
製品 2	Exaopc R3.70 以降 - Exaopc OPC インタフェースパッケージ サーバ	
セキュリティモデル	従来モデル	標準モデル
ユーザ管理方法	-	スタンドアロン管理 ドメイン管理／併用管理
必要な手順	NTPF100 Exaopc OPC インタフェースパッケージインストールマニュアル(IM 36J02A12-01)の「B1.6 CENTUM システムとの接続」を参照してください。	

表 D1.3.1-2 接続情報：セキュリティモデルが異なる場合 1

インテグレーションコード	0101-0401-02-01	
製品 1	CENTUM VP R5.01 以降 - 操作監視基本機能	
製品 2	Exaopc R3.70 以降 - Exaopc OPC インタフェースパッケージ サーバ	
セキュリティモデル	標準モデル (CENTUM VP) 従来モデル (Exaopc)	
ユーザ管理方法	スタンドアロン管理	ドメイン管理／併用管理
必要な手順	NTPF100 Exaopc OPC インタフェースパッケージインストールマニュアル(IM 36J02A12-01)の「B1.6 CENTUM システムとの接続」を参照してください。	

表 D1.3.1-3 接続情報：セキュリティモデルが異なる場合 2

インテグレーションコード	0101-0401-02-01	
製品 1	CENTUM VP R5.01 以降 - 操作監視基本機能	
製品 2	Exaopc R3.70 以降 - Exaopc OPC インタフェースパッケージ サーバ	
セキュリティモデル	従来モデル (CENTUM VP) 標準モデル (Exaopc)	
ユーザ管理方法	スタンドアロン管理	ドメイン管理／併用管理
必要な手順	なし	

D1.3.2 CENTUM VP - システム生成機能と Exaopc サーバ

CENTUM VP の拡張テスト機能は、Exaopc サーバと連携させることができます。

■ CENTUM VP の拡張テスト機能と Exaopc サーバを連携させる

接続情報を次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

表 D1.3.2-1 接続情報

インテグレーションコード	0102-0401-02-01		
製品 1	CENTUM VP R5.01 以降 - システム生成機能		
製品 2	Exaopc R3.70 以降 - インタフェースパッケージ サーバ		
セキュリティモデル	従来モデル	標準モデル	
ユーザ管理方法	-	スタンドアロン管理	ドメイン管理／併用管理
必要な手順	NTPF100 Exaopc OPC インタフェースパッケージインストールマニュアル(IM 36J02A12-01)の「B1.6 CENTUM システムとの接続」を参照してください。		

表 D1.3.2-2 接続情報：セキュリティモデルが異なる場合 1

インテグレーションコード	0102-0401-02-01		
製品 1	CENTUM VP R5.01 以降 - システム生成機能		
製品 2	Exaopc R3.70 以降 - インタフェースパッケージ サーバ		
セキュリティモデル	標準モデル (CENTUM VP) 従来モデル (Exaopc)		
ユーザ管理方法	スタンドアロン管理	ドメイン管理／併用管理	
必要な手順	NTPF100 Exaopc OPC インタフェースパッケージインストールマニュアル(IM 36J02A12-01)の「B1.6 CENTUM システムとの接続」を参照してください。		

表 D1.3.2-3 接続情報：セキュリティモデルが異なる場合 2

インテグレーションコード	0102-0401-02-01		
製品 1	CENTUM VP R5.01 以降 - システム生成機能		
製品 2	Exaopc R3.70 以降 - インタフェースパッケージ サーバ		
セキュリティモデル	従来モデル (CENTUM VP) 標準モデル (Exaopc)		
ユーザ管理方法	スタンドアロン管理	ドメイン管理／併用管理	
必要な手順	NTPF100 Exaopc OPC インタフェースパッケージインストールマニュアル(IM 36J02A12-01)の「B1.6 CENTUM システムとの接続」を参照してください。		

D1.4 CENTUM VP と Exapilot

ここでは、CENTUM VP と Exapilot を接続するときの設定について説明します。

D1.4.1 CENTUM VP 操作監視基本機能と Exapilot サーバ

CENTUM VP の操作監視基本機能と Exapilot サーバを接続して、Exapilot サーバが Exaopc OPC インタフェースパッケージ（HIS 搭載用）経由でデータを読み書きできます。接続する方法は、これらを同一のコンピュータ内で使用するか、別々のコンピュータで使用するかで違います。

Exapilot サーバは Exapilot クライアントの機能も含むため、CENTUM VP と Exapilot クライアントの接続でできることは、CENTUM VP と Exapilot サーバとの接続でも可能となります。そのため、CENTUM VP と Exapilot サーバを接続するときには、Exapilot クライアントでの接続の部分も合わせてお読みください。

■ 同一コンピュータ内で使用する

接続情報を次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

表 D1.4.1-1 接続情報

インテグレーションコード	0101-0601-03-02	
製品 1	CENTUM VP R4.03 以降 - 操作監視基本機能	
製品 2	Exapilot R3.95 以降 - 運転効率向上支援パッケージサーバ	
セキュリティモデル	従来モデル	標準モデル
ユーザ管理方法	-	スタンドアロン管理 ドメイン管理／併用管理
必要な手順	設定不要	「●両製品が標準モデルの場合」を参照してください。

重要

CENTUM VP R5.01 以降がインストールされたコンピュータに Exapilot サーバをインストールするときには、CENTUM デスクトップの再構築が必要な場合があります。

● 両製品が標準モデルの場合

両製品が標準モデルの場合は、次の手順に従ってください。

1. CENTUM VP が動作するコンピュータで、PLT_PROCESS アカウントを次のグループに所属させてください。
 - スタンドアロン管理の場合 : CTM_OPCT
 - ドメイン管理／併用管理の場合 : CTM_OPCL
2. Exapilot が動作するコンピュータで、CTM_PROCESS アカウントを次のグループに所属させてください。
 - スタンドアロン管理の場合 : PLT_OPCT
 - ドメイン管理／併用管理の場合 : PLT_OPCL

■ 別々のコンピュータで使用する

接続情報を次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

重要

接続する製品のセキュリティモデルとユーザ管理方法は統一することが原則です。しかし、CENTUM VP と Exapilot はセキュリティモデルやユーザ管理方法が違っても接続できます。

表 D1.4.1-2 接続情報

インテグレーションコード	0101-0601-03-02	
製品 1	CENTUM VP R4.03 以降 - 操作監視基本機能	
製品 2	Exapilot R3.95 以降 - 運転効率向上支援パッケージサーバ	
セキュリティモデル	従来モデル	標準モデル
ユーザ管理方法	-	スタンダードアロン管理 ドメイン管理／併用管理
必要な手順	「●両製品が従来モデルの場合」を参照してください。	「●両製品が標準モデルの場合」を参照してください。

表 D1.4.1-3 接続情報：セキュリティモデルが異なる場合 1

インテグレーションコード	0101-0601-03-02	
製品 1	CENTUM VP R4.03 以降 - 操作監視基本機能	
製品 2	Exapilot R3.95 以降 - 運転効率向上支援パッケージサーバ	
セキュリティモデル	標準モデル (CENTUM VP) 従来モデル (Exapilot)	
ユーザ管理方法	スタンダードアロン管理	ドメイン管理／併用管理
必要な手順	「●CENTUM VP が標準モデルで Exapilot が従来モデルの場合」を参照してください。	

表 D1.4.1-4 接続情報：セキュリティモデルが異なる場合 2

インテグレーションコード	0101-0601-03-02	
製品 1	CENTUM VP R4.03 以降 - 操作監視基本機能	
製品 2	Exapilot R3.95 以降 - 運転効率向上支援パッケージサーバ	
セキュリティモデル	従来モデル (CENTUM VP) 標準モデル (Exapilot)	
ユーザ管理方法	スタンダードアロン管理	ドメイン管理／併用管理
必要な手順	「●CENTUM VP が従来モデルで Exapilot が標準モデルの場合」を参照してください。	

補足

従来モデルのコンピュータと NetBIOS over TCP/IP を無効にした標準モデルのコンピュータを接続されるときは、名前解決のために追加の手順が必要です。次の 3 つの方法のいずれかを実施してください。

- ・ ドメインに参加させる
従来モデルのコンピュータを標準モデルのコンピュータと同じドメインに参加させる。
- ・ DNS を利用する
従来モデルのコンピュータを DNS サーバに登録し、また従来モデル／標準モデルの両コンピュータで DNS サーバを利用する。通常は、標準モデルのコンピュータが参加しているドメインコントローラを DNS サーバとして用いる。
- ・ hosts/lmhosts ファイルを用いる
従来モデルのコンピュータの hosts または lmhosts ファイルに、標準モデルのコンピュータのコンピュータ名と IP アドレスを登録する。標準モデルのコンピュータの hosts または lmhosts ファイルに従来モデルのコンピュータのコンピュータ名と IP アドレスを登録する。

● 両製品が従来モデルの場合

1. CENTUM VP が動作するコンピュータに、Exapilot サーバのプロセス実行アカウントを作成してください。
ユーザアカウント名のデフォルトは [EXA] です。パスワードも [EXA] としてください。

2. Exapilot が動作するコンピュータで、管理者権限を持つユーザで次のプログラムを実行し、CTM_PROCESS ユーザアカウントを作成してください。
 <CENTUM VP ソフトウェアメディアドライブ>: ¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS.Platform.form.Security.CreateCentumProcess.exe

● 両製品が標準モデルの場合

1. CENTUM VP が動作するコンピュータで、管理者権限を持つユーザアカウントを使用して次のプロセス実行アカウント作成ツールを実行し、PLT_PROCESS ユーザアカウントを作成してください。
 <Exapilot ソフトウェアメディアドライブ>: ¥TOOLS¥CreatePLTProcess.exe
2. CENTUM VP が動作するコンピュータで、作成したユーザアカウントをユーザ管理方法に応じて次のグループに所属させてください。

表 D1.4.1-5 ユーザ管理方法と所属させるグループ

CENTUM VP のユーザ管理方法	Exapilot のユーザ管理方法	所属させるグループ
スタンドアロン管理	スタンドアロン管理	CTM_OPC
ドメイン管理または併用管理	ドメイン管理または併用管理	CTM_OPC_LCL
スタンドアロン管理	ドメイン管理または併用管理	CTM_OPC
ドメイン管理または併用管理	スタンドアロン管理	CTM_OPC_LCL

3. Exapilot が動作するコンピュータで、管理者権限を持つユーザアカウントを使用して次のプロセス実行アカウント作成ツールを実行し、CTM_PROCESS ユーザアカウントを作成してください。
 <CENTUM VP ソフトウェアメディアドライブ>: ¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS.Platform.form.Security.CreateCentumProcess.exe
4. Exapilot が動作するコンピュータで、作成したユーザアカウントをユーザ管理方法に応じて次のグループに所属させてください。

表 D1.4.1-6 ユーザ管理方法と所属させるグループ

CENTUM VP のユーザ管理方法	Exapilot のユーザ管理方法	所属させるグループ
スタンドアロン管理	スタンドアロン管理	PLT_OPC
ドメイン管理または併用管理	ドメイン管理または併用管理	PLT_OPC_LCL
スタンドアロン管理	ドメイン管理または併用管理	PLT_OPC_LCL
ドメイン管理または併用管理	スタンドアロン管理	PLT_OPC

● CENTUM VP が標準モデルで Exapilot が従来モデルの場合

1. CENTUM VP が動作するコンピュータに Exapilot サーバのプロセス実行アカウントを作成し、CENTUM VP のユーザ管理方法に応じて次のグループに所属させてください。
 CENTUM VP がスタンドアロン管理 : CTM_OPC
 CENTUM VP がドメイン管理／併用管理 : CTM_OPC_LCL
 ユーザアカウント名のデフォルトは [EXA] です。パスワードも [EXA] としてください。
2. Exapilot が動作するコンピュータで、管理者権限を持つユーザアカウントを使用し、次のプロセス実行アカウント作成ツールを実行して CTM_PROCESS ユーザアカウントを作成してください。
 <CENTUM VP ソフトウェアメディアドライブ>: ¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS.Platform.form.Security.CreateCentumProcess.exe

● CENTUM VP が従来モデルで Exapilot が標準モデルの場合

1. CENTUM VP が動作するコンピュータで管理者権限を持つユーザアカウントを使用し、次のプロセス実行アカウント作成ツールを実行して PLT_PROCESS ユーザアカウントを作成してください。
<Exapilot ソフトウェアメディアドライブ>:¥TOOLS¥CreatePLTProcess.exe
2. Exapilot が動作するコンピュータで管理者権限を持つユーザアカウントを使用し、次のプロセス実行アカウント作成ツールを実行して CTM_PROCESS ユーザアカウントを作成してください。
<CENTUM VP ソフトウェアメディアドライブ>:¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS.Plat form.Security.CreateCentumProcess.exe
3. 作成したユーザアカウントを、Exapilot のユーザ管理方法に応じて次のグループに所属させてください。
Exapilot がスタンダロン管理： PLT_OP
Exapilot がドメイン管理／併用管理： PLT_OP_LCL

D1.4.2 CENTUM VP 操作監視基本機能と Exapilot クライアント

CENTUM VP の操作監視基本機能と Exapilot クライアントを接続して、次のことができます。

- CENTUM VP の HIS で、Exapilot の各種画面を操作する
- Exapilot の ActiveX コンポーネント/.NET コンポーネントを CENTUM VP のグラフィックで使用する

重要

これらの操作は、CENTUM VP 操作監視基本機能と Exapilot クライアントを同一のコンピュータで使用した場合にのみ、可能となります。

■ CENTUM VP の操作監視機能と Exapilot クライアントを接続する

接続情報を次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

表 D1.4.2-1 接続情報

インテグレーションコード	0101-0651-03-02		
製品 1	CENTUM VP R4.03 以降 - 操作監視基本機能		
製品 2	Exapilot R3.95 以降 - 運転効率向上支援パッケージ クライアント		
セキュリティモデル	従来モデル	標準モデル	
ユーザ管理方法	-	スタンダードアロン管理	ドメイン管理／併用管理
必要な手順	設定不要	「●両製品が標準モデルでスタンダードアロン管理の場合」を参照してください。	「●両製品が標準モデルでドメイン管理または併用管理の場合」を参照してください。

● 注意事項

CENTUM VP の操作監視基本機能と Exapilot クライアントを同一コンピュータ内で使用し、CENTUM VP の HIS を操作するユーザを切り替えるときは、次のことに注意してください。

- Windows ユーザのログオフとログオンを基本としているユーザ認証モードでは、Exapilot の Windows 認証モードを使用してください。
- ユーザインダイアログからの切り替えを基本としているユーザ認証モードでは、Exapilot 認証モードを使用してください。

表 D1.4.2-2 同一コンピュータ内で使用するときのユーザ認証モード

CENTUM VP	Exapilot	
	Windows 認証モード	Exapilot 認証モード
CENTUM 認証モード	使用可能(*1)	推奨
Windows 認証モード：HIS タイプ シングルサインオン	使用可能(*2)(*3)	推奨
Windows 認証モード：Windows タイプシングルサインオン	推奨 (*2)(*4)	使用可能

*1: Exapilot システムセキュリティウィンドウで Windows にログオンして HIS を操作するための Windows ユーザアカウントを登録し、Exapilot の操作に必要な権限を設定してください。

*2: HIS にユーザインするユーザを Exapilot のシステムセキュリティウィンドウに登録し、Exapilot の操作権限を設定してください。ただし、メッセージ通知機能の自動起動を設定するときは、Windows にログオンするユーザに操作権限を設定してください。また、自動起動ができるユーザは、Windows ログオンユーザである必要があります(HIS タイプシングルサインオンの Windows ログオンユーザは OFFUSER です)。

- *3: グラフィックに貼り付けられた Exapilot の ActiveX コンポーネント/.NET コンポーネントは OFFUSER で実行されるため、ActiveX コンポーネント/.NET コンポーネントを使用するときは、ローカルの OFFUSER を Exapilot のシステムセキュリティウィンドウに登録し、Exapilot の操作権限を設定してください。
- *4: グラフィックに貼り付けられた Exapilot の ActiveX コンポーネント/.NET コンポーネントは Windows にログオンしたユーザで実行されるため、ActiveX コンポーネント/.NET コンポーネントを使用するときは、Windows にログオンするユーザを Exapilot のシステムセキュリティウィンドウに登録し、Exapilot の操作権限を設定してください。

重要

- HIS タイプシングルサインオンを使用しているときは、Windows からログオフしないでください。
- Exapilot で使用する Windows ユーザ名は、CENTUM VP のルールに従ってください。

● 両製品が標準モデルでスタンドアロン管理の場合

1. Exapilot のサーバコンピュータに管理者権限を持つユーザアカウントでログオンし、CENTUM VP のユーザ認証モードに応じて次のユーザアカウントを作成してください。
 - CENTUM VP が CENTUM 認証モードの場合：
Exapilot の各種画面を操作する際に Windows にログオンするユーザアカウント
 - CENTUM VP が Windows 認証モードの場合：
Exapilot の各種画面を操作する際に CENTUM VP で HIS にユーザインするユーザアカウント
2. 作成したユーザアカウントを、PLT_OPERATOR グループに所属させてください。

● 両製品が標準モデルでドメイン管理または併用管理の場合

1. 次のユーザアカウントを、CENTUM VP のユーザ認証モードに応じて、PLT_OPERATOR_LCL グループに所属させてください。
 - CENTUM VP が CENTUM 認証モードの場合：
Exapilot の各種画面を操作する際に Windows にログオンするユーザアカウント
 - CENTUM VP が Windows 認証モードの場合：
Exapilot の各種画面を操作する際に CENTUM VP で HIS にユーザインするユーザアカウント

● HIS タイプシングルサインオンで運用するときのファンクションキー／プリセットメニューの設定

HIS タイプシングルサインオンで運用するとき、Exapilot のウィンドウを起動するには、CENTUM VP のファンクションキーまたはプリセットメニューにファイルを割り付けておく必要があります。これは、HIS タイプシングルサインオンでは常に OFFUSER で Windows にログオンされた状態となり、スタートメニューから Exapilot のウィンドウの起動ができないためです。

Exapilot の ActiveX コンポーネント/.NET コンポーネントを CENTUM VP のグラフィックで使用するための接続のときは、この設定は必要ありません。

表 D1.4.2-3 Exapilot のウィンドウ起動のために割り付けるファイル

スタートメニュー表示	ファイルパス(*1)
Exapilot 構築	%EXA%¥Program¥PLTBuilder.exe
Exapilot 運転	%EXA%¥Program¥PLTMonitor.exe
Exapilot イベント履歴表示	%EXA%¥Program¥PLTEventHistory.exe
ソフトウェア構成ビューア	%EXA%¥Program¥PMCSftView.exe

次に続く

表 D1.4.2-3 Exapilot のウィンドウ起動のために割り付けるファイル（前から続く）

スタートメニュー表示	ファイルパス(*1)
Exapilot イベント履歴管理	%EXA%\Program\PLTHistManager.exe
Exapilot オプション構成ビューア	%EXA%\Exapilot\tool\PLTOptInstall.exe
Exapilot セキュリティ	%EXA%\Program\PLTSecurity.exe
Exapilot ユーティリティ	%EXA%\Program\PLTUtility.exe
Exapilot セーブリストア	%EXA%\Program\PLTSaveRestore.exe
Exapilot 運転準備ツール	%EXA%\Program\PLTProcPrepare.exe
Exapilot 変数ビュー	%EXA%\Program\PLTVariable.exe
Exapilot メッセージ通知	%EXA%\Program\PLTMessageNotification.exe

*1: %EXA%はインストール先フォルダ名。デフォルトは「C:\EXA」

1. CENTUM VP のファンクションキー割り付けビルダを使って、ファンクションキーを割り付けてください。
2. HIS 設定ウィンドウで、プリセットメニューを設定してください。

D1.4.3 CENTUM VP システム生成機能と Exapilot クライアント

CENTUM VP のシステム生成機能と Exapilot クライアントで、Exapilot の ActiveX コンポーネント/.NET コンポーネントを配置した CENTUM VP のグラフィックを作成できます。

■ Exapilot の ActiveX コンポーネント/.NET コンポーネントを配置した CENTUM VP のグラフィックを作成する

接続情報を次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

表 D1.4.3-1 接続情報

インテグレーションコード	0102-0651-03-01		
製品 1	CENTUM VP R4.03 以降 - システム生成機能		
製品 2	Exapilot R3.90 以降 - 運転効率向上支援パッケージ サーバ		
セキュリティモデル	従来モデル	標準モデル	
ユーザ管理方法	-	スタンドアロン管理	ドメイン管理／併用管理
必要な手順	設定不要	「●両製品が標準モデルの場合」を参照してください。	

● 両製品が標準モデルの場合

次の手順に従ってください。

この手順は、ユーザ管理方法がスタンドアロン管理の場合は、CENTUM VP のグラフィックを作成するコンピュータで行ってください。ドメイン管理または併用管理の場合は、ドメインコントローラで行ってください。

1. 管理者権限を持つユーザでログオンしてください。
2. CENTUM VP のグラフィックを作成するユーザを、CTM_ENGINEER と PLT_OPERATOR グループに所属させてください。

D1.5 CENTUM VP と Exaplog

ここでは、CENTUM VP と Exaplog を接続するときの設定について説明します。

D1.5.1 CENTUM VP - 操作監視基本機能と Exaplog - イベント解析パッケージサーバ

CENTUM VP の操作監視基本機能と Exaplog のイベント解析パッケージサーバを接続すると、Exaplog が CENTUM VP の HIS からイベントデータを収集できます。接続する方法は、これらを同一コンピュータ内で使用するか、別々のコンピュータで使用するかで違います。

■ 同一コンピュータ内で使用する

CENTUM VP の操作監視基本機能と Exaplog のイベント解析パッケージサーバを同一コンピュータ内で使用するときは、機能を接続せずに個別で操作する場合も、製品間で通信やファイルを共有する場合も、接続のための設定は必要ありません。

■ 別々のコンピュータで使用する

CENTUM VP の操作監視基本機能と Exaplog のイベント解析パッケージサーバを別々のコンピュータで使用するときは、設定が必要になります。

接続情報を次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

重要

接続する製品のセキュリティモデルとユーザ管理方法は統一することが原則です。しかし、CENTUM VP と Exaplog は、セキュリティモデルとユーザ管理方法が違っても接続できます。

表 D1.5.1-1 接続情報

インテグレーションコード	0101-0701-03-02		
製品 1	CENTUM VP R5.01 以降 - 操作監視基本機能		
製品 2	Exaplog R3.40 以降 - イベント解析パッケージサーバ		
セキュリティモデル	従来モデル	標準モデル	
ユーザ管理方法	-	スタンドアロン管理	ドメイン管理／併用管理
必要な手順	「●両製品が従来モデルの場合」を参照してください。		

表 D1.5.1-2 接続情報：セキュリティモデルが異なる場合 1

インテグレーションコード	0101-0701-03-02		
製品 1	CENTUM VP R5.01 以降 - 操作監視基本機能		
製品 2	Exaplog R3.40 以降 - イベント解析パッケージサーバ		
セキュリティモデル	標準モデル (CENTUM VP) 従来モデル (Exaplog)		
スタンドアロン管理	スタンドアロン管理	ドメイン管理／併用管理	
必要な手順	「●CENTUM VP が標準モデルで Exaplog が従来モデルの場合」を参照してください。		

表 D1.5.1-3 接続情報：セキュリティモデルが異なる場合 2

インテグレーションコード	0101-0701-03-02		
--------------	-----------------	--	--

次に続く

表 D1.5.1-3 接続情報：セキュリティモデルが異なる場合 2（前から続く）

製品 1	CENTUM VP R5.01 以降 - 操作監視基本機能	
製品 2	Exaplog R3.40 以降 - イベント解析/パッケージサーバ	
セキュリティモデル 従来モデル (CENTUM VP)	従来モデル (CENTUM VP) 標準モデル (Exaplog)	
スタンドアロン管理	スタンドアロン管理	ドメイン管理／併用管理
必要な手順	「●CENTUM VP が従来モデルで Exaplog が標準モデルの場合」を参照してください。	

補足

従来モデルのコンピュータと NetBIOS over TCP/IP を無効にした標準モデルのコンピュータを接続させることは、名前解決のために追加の手順が必要です。次の 3つの方法のいずれかを実施してください。

- ・ ドメインに参加させる
従来モデルのコンピュータを標準モデルのコンピュータと同じドメインに参加させる。
- ・ DNS を利用する
従来モデルのコンピュータを DNS サーバに登録し、また従来モデル／標準モデルの両コンピュータで DNS サーバを利用する。通常は、標準モデルのコンピュータが参加しているドメインコントローラを DNS サーバとして用いる。
- ・ hosts/lmhosts ファイルを用いる
従来モデルのコンピュータの hosts または lmhosts ファイルに、標準モデルのコンピュータのコンピュータ名と IP アドレスを登録する。標準モデルのコンピュータの hosts または lmhosts ファイルに従来モデルのコンピュータのコンピュータ名と IP アドレスを登録する。

● 両製品が従来モデルの場合

CENTUM VP が動作するコンピュータに、exaplog ユーザアカウントを作成してください。exaplog ユーザアカウントのパスワードは、Exaplog サーバコンピュータの exaplog ユーザアカウントと同じにしてください。

● 両製品が標準モデルの場合

1. CENTUM VP が動作するコンピュータに、exaplog ユーザアカウントを作成してください。exaplog ユーザアカウントのパスワードは、Exaplog サーバコンピュータの exaplog ユーザアカウントと同じにしてください。
2. 作成した exaplog ユーザアカウントを、次のグループに所属させてください。
スタンドアロン管理 : CTM_OPERATOR
ドメイン管理または併用管理 : CTM_OPC_LCL

● CENTUM VP が標準モデルで Exaplog が従来モデルの場合

1. CENTUM VP が動作するコンピュータに、exaplog ユーザアカウントを作成してください。exaplog ユーザアカウントのパスワードは、Exaplog サーバコンピュータの exaplog ユーザアカウントと同じにしてください。
2. 作成した exaplog ユーザアカウントを、次のグループに所属させてください。

CENTUM VP がスタンドアロン管理 : CTM_OPERATOR

CENTUM VP がドメイン管理または併用管理 : CTM_OPC_LCL

● CENTUM VP が従来モデルで Exaplog が標準モデルの場合

CENTUM VP が動作するコンピュータに、exaplog ユーザアカウントを作成してください。exaplog ユーザアカウントのパスワードは、Exaplog サーバコンピュータの exaplog ユーザアカウントと同じにしてください。

D1.6 CENTUM VP と Exaquantum

ここでは、CENTUM VP と Exaquantum を接続するときの設定について説明します。

D1.6.1 CENTUM VP - 操作監視基本機能と Exaquantum - PIMS サーバ

CENTUM VP の操作監視基本機能と Exaquantum の PIMS サーバを接続すると、Exaquantum の PIMS サーバが、Exaopc OPC インタフェースパッケージ (HIS 搭載用) を経由して CENTUM VP の HIS や FCS からデータを収集できます。

■ Exaquantum が CENTUM VP の HIS や FCS からデータを収集する

CENTUM VP の操作監視基本機能と Exaquantum の PIMS サーバを別々のコンピュータで使用するときは、設定が必要になります。

接続情報を次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

重要

接続する製品のセキュリティモデルとユーザ管理方法は統一することが原則です。しかし、CENTUM VP と Exaquantum は、セキュリティモデルとユーザ管理方法が違っても接続できます。

表 D1.6.1-1 接続情報

インテグレーションコード	0101-0801-02-03		
製品 1	CENTUM VP R5.01 以降 - 操作監視基本機能		
製品 2	Exaquantum R2.70 以降 - PIMS サーバ		
セキュリティモデル	従来モデル	標準モデル	
ユーザ管理方法	-	スタンドアロン管理	ドメイン管理／併用管理
必要な手順	「●両製品が従来モデルの場合」を参照してください。	「●両製品が標準モデルの場合」を参照してください。	

表 D1.6.1-2 接続情報：セキュリティモデルが異なる場合 1

インテグレーションコード	0101-0801-02-03		
製品 1	CENTUM VP R5.01 以降 - 操作監視基本機能		
製品 2	Exaquantum R2.70 以降 - PIMS サーバ		
セキュリティモデル	標準モデル (CENTUM VP) 従来モデル (Exaquantum)		
スタンドアロン管理	スタンドアロン管理	ドメイン管理／併用管理	
必要な手順	「● CENTUM VP が標準モデルで Exaquantum が従来モデルの場合」を参照してください。		

表 D1.6.1-3 接続情報：セキュリティモデルが異なる場合 2

インテグレーションコード	0101-0801-02-03		
製品 1	CENTUM VP R5.01 以降 - 操作監視基本機能		
製品 2	Exaquantum R2.70 以降 - PIMS サーバ		
セキュリティモデル 従来モデル (CENTUM VP)	従来モデル (CENTUM VP) 標準モデル (Exaquantum)		
スタンドアロン管理	スタンドアロン管理	ドメイン管理／併用管理	

次に続く

表 D1.6.1-3 接続情報：セキュリティモデルが異なる場合 2（前から続く）

必要な手順	「●CENTUM VP が従来モデルで Exaquantum が標準モデルの場合」を参照してください。
-------	---

● 両製品が従来モデルの場合

1. CENTUM VP が動作するコンピュータに Quantumuser ユーザアカウントを作成し、Exaquantum の Quantumuser ユーザアカウントとパスワードを揃えてください。
2. Exaquantum が動作するコンピュータで、次のプロセス実行アカウント作成ツールを実行し、CTM_PROCESS ユーザアカウントを作成してください。
<CENTUM VP ソフトウェアメディアドライブ>:\CENTUM\SECURITY\Y\Yokogawa.IA.iPCS.Plat form.Security.CreateCentumProcess.exe
3. ログオン方式の設定をしてください。
 - ・互換動作とする場合：
CENTUM VP の動作するコンピュータの HIS ユーティリティの OPC タブで、ログオン方式を [互換動作 (R4.03 以前と互換)] に設定してください。また、Exaopc の動作するコンピュータで、OPC ゲートウェイセキュリティの [ログオンチェックを有効とする] をオフにしてください。
 - ・ログオンを必要とする場合：
CENTUM VP の動作するコンピュータの HIS ユーティリティの OPC タブで、ログオン方式を設定してください。また、Exaopc の動作するコンピュータで、CENTUM VP の設定に合わせて OPC ゲートウェイに OPC ログオン情報を設定してください。

● 両製品が標準モデルの場合

1. CENTUM VP が動作するコンピュータに、管理者ユーザでログオンしてください。
2. Exaquantum の前提条件ソフトウェア DVD (Disk 1) をドライブに挿入してください。
3. 次のコマンドを実行してください。
<DVD ドライブ>:\Misc\CPP2008\vcredist_x86.exe
Microsoft Visual C++ 2008 再頒布可能パッケージがインストールされます。
4. CENTUM VP が動作するコンピュータに、QTM_PROCESS ユーザアカウントを作成してください。
5. QTM_PROCESS ユーザアカウントを次のグループに所属させてください。
スタンダロン管理： CTM_OPCT
ドメイン管理／併用管理： CTM_OPCL
6. Exaquantum が動作するコンピュータで、次のプロセス実行アカウント作成ツールを使用して、CTM_PROCESS ユーザアカウントを作成してください。
<CENTUM VP ソフトウェアメディアドライブ>:\CENTUM\SECURITY\Y\Yokogawa.IA.iPCS.Plat form.Security.CreateCentumProcess.exe
7. CTM_PROCESS ユーザアカウントを次のグループに所属させてください。
スタンダロン管理： QTM_OPCT
ドメイン管理／併用管理： QTM_OPCL
8. ログオン方式の設定をしてください。
 - ・互換動作とする場合：
CENTUM VP の動作するコンピュータの HIS ユーティリティの OPC タブで、ログオン方式を [互換動作 (R4.03 以前と互換)] に設定してください。また、Exaopc の動作するコンピュータで、OPC ゲートウェイセキュリティの [ログオンチェックを有効とする] をオフにしてください。

- ・ ログオンを必要とする場合：

CENTUM VP の動作するコンピュータの HIS ユーティリティの OPC タブで、ログオン方式を設定してください。また、Exaopc の動作するコンピュータで、CENTUM VP の設定に合わせて OPC ゲートウェイに OPC ログオン情報を設定してください。

● CENTUM が標準モデルで Exaquantum が従来モデルの場合

1. CENTUM VP が動作するコンピュータに、Quantumuser ユーザアカウントを作成してください。

2. Quantumuser ユーザアカウントを次のグループに所属させてください。

スタンダロン管理： CTM_OPCT

ドメイン管理／併用管理： CTM_OPCLCL

3. Exaquantum が動作するコンピュータで、次のプロセス実行アカウント作成ツールを使用して、CTM_PROCESS ユーザアカウントを作成してください。

<CENTUM VP ソフトウェアメディアドライブ>:¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS_Platform.Security.CreateCentumProcess.exe

4. ログオン方式の設定をしてください。

- ・ 互換動作とする場合：

CENTUM VP の動作するコンピュータの HIS ユーティリティの OPC タブで、ログオン方式を [互換動作 (R4.03 以前と互換)] に設定してください。また、Exaopc の動作するコンピュータで、OPC ゲートウェイセキュリティの [ログオンチェックを有効とする] をオフにしてください。

- ・ ログオンを必要とする場合：

CENTUM VP の動作するコンピュータの HIS ユーティリティの OPC タブで、ログオン方式を設定してください。また、Exaopc の動作するコンピュータで、CENTUM VP の設定に合わせて OPC ゲートウェイに OPC ログオン情報を設定してください。

● CENTUM が従来モデルで Exaquantum が標準モデルの場合

1. CENTUM VP が動作するコンピュータに、管理者ユーザでログオンしてください。

2. Exaquantum の前提条件ソフトウェア DVD (Disk 1) をドライブに挿入してください。

3. 次のコマンドを実行してください。

<DVD ドライブ>:¥Misc¥CPP2008¥vcredist_x86.exe

Microsoft Visual C++ 2008 再頒布可能パッケージがインストールされます。

4. CENTUM VP が動作するコンピュータに、QTM_PROCESS ユーザアカウントを作成してください。

5. Exaquantum が動作するコンピュータで、次のプロセス実行アカウント作成ツールを使用して、CENTUM ユーザアカウントを作成してください。

<CENTUM VP ソフトウェアメディアドライブ>:¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS_Platform.Security.CreateCentumProcess.exe

6. CENTUM ユーザアカウントを次のグループに所属させてください。

スタンダロン管理： QTM_OPCT

ドメイン管理／併用管理： QTM_OPCLCL

7. ログオン方式の設定をしてください。

- ・ 互換動作とする場合：

CENTUM VP の動作するコンピュータの HIS ユーティリティの OPC タブで、ログオン方式を [互換動作 (R4.03 以前と互換)] に設定してください。また、Exaopc

の動作するコンピュータで、OPC ゲートウェイセキュリティの [ログオンチェックを有効とする] をオフにしてください。

- ・ ログオンを必要とする場合：

CENTUM VP の動作するコンピュータの HIS ユーティリティの OPC タブで、ログオン方式を設定してください。また、Exaopc の動作するコンピュータで、CENTUM VP の設定に合わせて OPC ゲートウェイに OPC ログオン情報を設定してください。

D1.6.2 CENTUM VP - 操作監視基本機能と Exaquantum - Explorer クライアント

CENTUM VP の操作監視基本機能と Exaquantum の Explorer クライアントを同一のコンピュータにインストールすると、CENTUM VP の HIS で Explorer クライアントが表示できます。

■ 同一コンピュータ内で使用する

接続情報を次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

表 D1.6.2-1 接続情報

インテグレーションコード	0101-0851-01-02		
製品 1	CENTUM VP R5.01 以降 - 操作監視基本機能		
製品 2	Exaquantum R2.60 以降 - Explorer クライアント		
セキュリティモデル	従来モデル	標準モデル	
ユーザ管理方法	-	スタンドアロン管理	ドメイン管理／併用管理
必要な手順	なし	「●標準モデルでスタンドアロン管理の場合」を参照してください。	「●標準モデルでドメイン管理または併用管理の場合」を参照してください。

● 前提条件

CENTUM VP の操作監視基本機能と Exaquantum Explorer クライアントを同一コンピュータ内で使用するときは、CENTUM VP の操作監視基本機能を先にインストールしてください。

● 標準モデルでスタンドアロン管理の場合

1. CENTUM VP の HIS で自動ログオン機能を使用しているときは、Exaquantum Explorer クライアントをインストールする前に、自動ログオン機能を解除してください。
2. インストールするユーザに HIS の自動起動の設定をしているときは、それを解除してください。
3. コンピュータを再起動し、管理者権限を持つユーザアカウントでログオンしてください。
4. Exaquantum の次のファイルを実行してください。
<Exaquantum ソフトウェアメディアドライブ>:\TOOLS\QTMPresetStdModel.bat
EXA_MAINTENANCE グループが作成され、EXA_MAINTENANCE グループにログオン中のユーザアカウントが登録されます。
5. 自動的にログオフされるので、再度 1 のユーザアカウントでログオンしてください。
6. CENTUM VP の HIS で、自動ログオン機能と HIS 自動起動の設定を元に戻してください。

● 標準モデルでドメイン管理または併用管理の場合

1. CENTUM VP の HIS で自動ログオン機能を使用しているときは、Exaquantum Explorer クライアントをインストールする前に、自動ログオン機能を解除してください。
2. インストールするユーザに HIS の自動起動の設定をしているときは、それを解除してください。
3. ドメインコントローラで、次のグループを作成してください。

EXA_MAINTENANCE

QTM_DATA_READ

QTM_DATA_WRITE

QTM_EXPLORER DESIGN

QTM_MAINTENANCE

QTM_OPC

4. Exaquantum インストール用のユーザアカウントを作成し、EXA_MAINTENANCE グループと Domain Admins グループに所属させてください。
5. Exaquantum の次のファイルを実行してください。
<Exaquantum ソフトウェアメディアドライブ>:\TOOLS\QTMPresetStdModelDom.bat
EXA_MAINTENANCE_LCL グループが作成され、このグループに、ログオン中のユーザアカウントが追加されます。
6. CENTUM VP の HIS で、自動ログオン機能と HIS 自動起動の設定を元に戻してください。

D1.7 Multivariable Optimizing Control/Robust Quality Estimation と CENTUM VP

ここでは、APC クライアントと CENTUM VP を接続するときの設定について説明します。

D1.7.1 CENTUM VP 操作監視基本機能および APC クライアント

CENTUM VP 操作監視基本機能と APC クライアントを同じコンピュータで使用できます。

■ 同じコンピュータでパッケージを使用する場合

APC クライアントと CENTUM VP は同じコンピュータで使用する場合は、接続のための設定は必要ありません。

● Multivariable Optimizing Control/Robust Quality Estimation と CENTUM VP が同一コンピュータにインストールされるときのユーザー認証モード

Multivariable Optimizing Control/Robust Quality Estimation と CENTUM VP が同一コンピュータにインストールされるときのユーザー認証モードと設定を、次の表に示します。

表 D1.7.1-1 Multivariable Optimizing Control/Robust Quality Estimation と CENTUM VP が同一コンピュータにインストールされるときのユーザー認証モード

CENTUM VP	Multivariable Optimizing Control/Robust Quality Estimation
CENTUM 認証モード	Windows ユーザーグループを APC Builder の割り付けパネルに追加してください。本グループに所属するユーザーは HIS を操作できます。
Windows 認証モード HIS タイプシングルサインオン	HIS サインオンユーザーを Windows ユーザーグループに追加してください、その Windows ユーザーグループを APC ビルダーの割り付けパネルに追加してください。
Windows 認証モード Windows タイプシングルサインオン	HIS サインオンユーザーを APC ビルダーの割り付けパネルに追加してください。

重要

- HIS タイプシングルサインオンを使用しているときに、Windows からログオフしないでください。
- Multivariable Optimizing Control/Robust Quality Estimation に登録する Windows ユーザー名は CENTUM VP のユーザー命名規則に従ってください。

参照

CENTUM VP ユーザー認証モードについては、以下を参照してください。

CENTUM VP セキュリティガイド (IM 33J01C30-01JA) の「2.2.2 CENTUM VP のユーザ認証モード」

● HIS タイプシングルサインオンで運用するときのファンクションキー／プリセットメニューの設定

HIS タイプシングルサインオンで運用するとき、Multivariable Optimizing Control/Robust Quality Estimation のウィンドウを起動するには、ファンクションキーまたはプリセットメニューにファンクションを割り付けてください。これは、HIS タイプシングルサインオンでは常に OFFUSER で Windows にログオンされた状態となり、[スタート] メニューから Multivariable Optimizing Control/Robust Quality Estimation のウィンドウの起動ができなくなるためです。

表 D1.7.1-2 Multivariable Optimizing Control/Robust Quality Estimation の各ウィンドウ起動のために割り付けるファイルパス一覧

スタートメニュー	ファイルパス
Builder	<インストールトップフォルダー>\Yokogawa\APC\Programs\Yokogawa.AP.C.HMI.Configuration.ThickClient.exe
Operation	<インストールトップフォルダー>\Yokogawa\APC\Programs\Yokogawa.AP.C.HMI.Runtime.ThickClient.exe

次に続く

表 D1.7.1-2 Multivariable Optimizing Control/Robust Quality Estimation の各ウィンドウ起動のために割り付けるファイルパス一覧（前から続く）

スタートメニュー	ファイルパス
Data Collection Tool	C:\Windows\System32\cmd.exe /k ""<インストールトップフォルダー>\Yokogawa\APC\Programs\DataCollectionTool.bat" "<インストールトップフォルダー>\Yokogawa\APC\Programs""
ソフトウェア構成ビューア	<インストールトップフォルダー>\Yokogawa\APC\Programs\PMCSftView.exe

- ファンクションキーの割り付け
CENTUM VP のファンクションキー割り付けビルダを使って、ファンクションキーを割り付けてください。
- プリセットメニューの設定
HIS 設定ウィンドウで、プリセットメニューを設定してください。

D1.8 CENTUM VP と Exasmoc

ここでは、CENTUM VP と Exasmoc を同一コンピュータ内で使用するときの設定について説明します。

D1.8.1 CENTUM VP - 操作監視基本機能と Exasmoc クライアント

CENTUM VP の操作監視基本機能と Exasmoc クライアントは、同一コンピュータ内で使用できます。

■ 同一コンピュータ内で使用する

接続情報を次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

表 D1.8.1-1 接続情報

インテグレーションコード	0101-0951-01-02		
製品 1	CENTUM VP R5.01 以降 - 操作監視基本機能		
製品 2	Exasmoc R4.03 - Exasmoc クライアント		
セキュリティモデル	従来モデル	標準モデル	
ユーザ管理方法	-	スタンダードアロン管理	ドメイン管理／併用管理
必要な手順	「●従来モデルの場合」を参照してください。	「●標準モデルでスタンダードアロン管理の場合」を参照してください。	「●標準モデルでドメイン管理または併用管理の場合」を参照してください。

● 前提条件

CENTUM VP の操作監視基本機能と Exasmoc クライアントを同一コンピュータ内で使用するときは、CENTUM VP の操作監視基本機能を先にインストールしてください。

● 従来モデルの場合

1. CENTUM VP の HIS で自動ログオン機能を使用しているときは、Exasmoc クライアントをインストールする前に、自動ログオン機能を解除してください。
2. コンピュータを再起動し、CENTUM VP のセキュリティ設定を行ったユーザアカウントでログオンして、Exasmoc をインストールしてください。
3. Exasmoc のツールを使用するユーザアカウントを、CENTUM VP の適切なグループに所属させてください。
4. 上記のユーザアカウントがログオンできるように、コンピュータを設定してください。
5. CENTUM VP の HIS で、ファンクションキーとプリセットメニューの設定をしてください。
6. CENTUM VP の HIS で、自動ログオン機能の設定を元に戻してください。

● 標準モデルでスタンダードアロン管理の場合

1. CENTUM VP の HIS で自動ログオン機能を使用しているときは、Exasmoc クライアントをインストールする前に、自動ログオン機能を解除してください。
2. コンピュータを再起動し、CENTUM VP のセキュリティ設定を行ったユーザアカウントでログオンして、Exasmoc をインストールしてください。
3. Exasmoc のツールを使用するユーザアカウントを、CENTUM VP の適切なグループに所属させてください。
4. 上記のユーザアカウントがログオンできるように、コンピュータを設定してください。
5. CENTUM VP の HIS で、ファンクションキーとプリセットメニューの設定をしてください。
6. CENTUM VP の HIS で、自動ログオン機能の設定を元に戻してください。

● 標準モデルでドメイン管理または併用管理の場合

1. CENTUM VP の HIS で自動ログオン機能を使用しているときは、Exasmoc クライアントをインストールする前に、自動ログオン機能を解除してください。
2. インストール用ユーザーアカウントとして、EXA_MAINTENANCE グループに所属しているユーザーアカウントを、CTM_MAINTENANCE グループに追加してください。
3. Exasmoc のツールを使用するユーザーアカウントを、CENTUM VP の適切なグループに所属させてください。
4. 上記のユーザーアカウントがログオンできるように、コンピュータを設定してください。
5. CENTUM VP の HIS で、ファンクションキーとプリセットメニューの設定をしてください。
6. CENTUM VP の HIS で、自動ログオン機能の設定を元に戻してください。

● ファンクションキーとプリセットメニューの設定をする

必要に応じて、Exasmoc の各ツールを CENTUM VP のファンクションキーまたはプリセットメニューに割り付けて、Exasmoc の各ツールが実行できるようにしてください。

ファンクションキーには、ファンクションキー割り付けビルダで、プリセットメニューには HIS 設定ウィンドウのプリセットメニューの [ファイル名によるプログラムの実行] で設定してください。

スタートメニューに登録されている Exasmoc の各ツールとパスの対応表は次のとおりです。

表 D1.8.1-2 スタートメニュー対応表

スタートメニューにある名称	パス
APC Builder	%ProgramFiles%\Yokogawa\IA\iPCS\Products\APC\Program\Yokogawa.IA.iPCS.APC.Builder.ScheduleBuilder.exe
APC HMI	%ProgramFiles%\Yokogawa\IA\iPCS\Products\APC\Program\Yokogawa.IA.iPCS.APC.WebHMI.ApcLocalClient.exe
Client Builder	%ProgramFiles%\Yokogawa\IA\iPCS\Products\APC\Program\Yokogawa.IA.iPCS.APC.Builder.ClientWindowBuilder.exe
Role Based Builder	%ProgramFiles%\Yokogawa\IA\iPCS\Products\APC\Program\Yokogawa.IA.iPCS.APC.Builder.RoleBasedBuilder.exe
インテグレーションビルダ	<Exa トップフォルダ>\Program\ZACItgBuilder.exe
ソフトウェア構成ビューア	<Exa トップフォルダ>\Program\PMCSftView.exe

D1.9 CENTUM VP と Exarqe

ここでは、CENTUM VP と Exarqe を同一コンピュータ内で使用するときの設定について説明します。

D1.9.1 CENTUM VP - 操作監視基本機能と Exarqe クライアント

CENTUM VP の操作監視基本機能と Exarqe クライアントは、同一コンピュータ内で使用できます。

■ 同一コンピュータ内で使用する

接続情報を次の表に示します。接続に必要な手順については、表の後ろの記載を参照してください。

表 D1.9.1-1 接続情報

インテグレーションコード	0101-1051-01-02		
製品 1	CENTUM VP R5.01 以降 - 操作監視基本機能		
製品 2	Exarqe R4.03 - Exarqe クライアント		
セキュリティモデル	従来モデル	標準モデル	
ユーザ管理方法	-	スタンドアロン管理	ドメイン管理／併用管理
必要な手順	「●従来モデルの場合」を参照してください。	「●標準モデルでスタンドアロン管理の場合」を参照してください。	「●標準モデルでドメイン管理または併用管理の場合」を参照してください。

● 前提条件

CENTUM VP の操作監視基本機能と Exarqe クライアントを同一コンピュータ内で使用するときは、CENTUM VP の操作監視基本機能を先にインストールしてください。

● 従来モデルの場合

1. CENTUM VP の HIS で自動ログオン機能を使用しているときは、Exarqe クライアントをインストールする前に、自動ログオン機能を解除してください。
2. コンピュータを再起動し、CENTUM VP のセキュリティ設定を行ったユーザーアカウントでログオンして、Exarqe をインストールしてください。
3. Exarqe のツールを使用するユーザーアカウントを、CENTUM VP の適切なグループに所属させてください。
4. 上記のユーザーアカウントがログオンできるように、コンピュータを設定してください。
5. CENTUM VP の HIS で、ファンクションキーとプリセットメニューの設定をしてください。
6. CENTUM VP の HIS で、自動ログオン機能の設定を元に戻してください。

● 標準モデルでスタンドアロン管理の場合

1. CENTUM VP の HIS で自動ログオン機能を使用しているときは、Exarqe クライアントをインストールする前に、自動ログオン機能を解除してください。
2. コンピュータを再起動し、CENTUM VP のセキュリティ設定を行ったユーザーアカウントでログオンして、Exarqe をインストールしてください。
3. Exarqe のツールを使用するユーザーアカウントを、CENTUM VP の適切なグループに所属させてください。
4. 上記のユーザーアカウントがログオンできるように、コンピュータを設定してください。
5. CENTUM VP の HIS で、ファンクションキーとプリセットメニューの設定をしてください。
6. CENTUM VP の HIS で、自動ログオン機能の設定を元に戻してください。

● 標準モデルでドメイン管理または併用管理の場合

1. CENTUM VP の HIS で自動ログオン機能を使用しているときは、Exarqe クライアントをインストールする前に、自動ログオン機能を解除してください。
2. インストール用ユーザーアカウントとして、EXA_MAINTENANCE グループに所属しているユーザーアカウントを、CTM_MAINTENANCE グループに追加してください。
3. Exarqe のツールを使用するユーザーアカウントを、CENTUM VP の適切なグループに所属させてください。
4. 上記のユーザーアカウントがログオンできるように、コンピュータを設定してください。
5. CENTUM VP の HIS で、ファンクションキーとプリセットメニューの設定をしてください。
6. CENTUM VP の HIS で、自動ログオン機能の設定を元に戻してください。

● ファンクションキーとプリセットメニューの設定をする

必要に応じて、Exarqe の各ツールを CENTUM VP のファンクションキーまたはプリセットメニューに割り付けて、Exarqe の各ツールが実行できるようにしてください。

ファンクションキーには、ファンクションキー割り付けビルダで、プリセットメニューには HIS 設定ウィンドウのプリセットメニューの [ファイル名によるプログラムの実行] で設定してください。

スタートメニューに登録されている Exarqe の各ツールとパスの対応表は次のとおりです。

表 D1.9.1-2 スタートメニュー対応表

スタートメニューにある名称	パス
APC Builder	%ProgramFiles%\Yokogawa\IA\iPCS\Products\APC\Program\Yokogawa.IA.iPCS.APC.Builder.ScheduleBuilder.exe
APC HMI	%ProgramFiles%\Yokogawa\IA\iPCS\Products\APC\Program\Yokogawa.IA.iPCS.APC.WebHMI.ApcLocalClient.exe
Client Builder	%ProgramFiles%\Yokogawa\IA\iPCS\Products\APC\Program\Yokogawa.IA.iPCS.APC.Builder.ClientWindowBuilder.exe
Role Based Builder	%ProgramFiles%\Yokogawa\IA\iPCS\Products\APC\Program\Yokogawa.IA.iPCS.APC.Builder.RoleBasedBuilder.exe
インテグレーションビルダ	<Exa トップフォルダ>\Program\ZACItgBuilder.exe
ソフトウェア構成ビューア	<Exa トップフォルダ>\Program\PMCSftView.exe

Appendix 1. 設定スイッチ

制御バスインターフェースカードと Vnet/IP インタフェースカードのプリント板にある設定スイッチで、ドメイン番号とステーション番号を設定できます。

■ ドメイン番号と設定スイッチの位置

表 Appendix 1-1 ドメイン番号と設定スイッチの位置

ドメイン番号	ディップスイッチビット番号							
	1	2	3	4	5	6	7	8
1	0	0	0	0	0	0	0	1
2	0	0	0	0	0	0	1	0
3	1	0	0	0	0	0	1	1
4	0	0	0	0	0	1	0	0
5	1	0	0	0	0	1	0	1
6	1	0	0	0	0	1	1	0
7	0	0	0	0	0	1	1	1
8	0	0	0	0	1	0	0	0
9	1	0	0	0	1	0	0	1
10	1	0	0	0	1	0	1	0
11	0	0	0	0	1	0	1	1
12	1	0	0	0	1	1	0	0
13	0	0	0	0	1	1	0	1
14	0	0	0	0	1	1	1	0
15	1	0	0	0	1	1	1	1
16	0	0	0	1	0	0	0	0

■ ステーション番号と設定スイッチの位置

制御バスインターフェースカードと Vnet/IP インタフェースカードのステーション番号と設定スイッチの位置を、次の表に示します。ディップスイッチを表のように設定することで、必要なステーション番号に合わせることができます。

表 Appendix 1-2 ステーション番号と設定スイッチの位置

ステーション番号	ディップスイッチビット番号							
	1	2	3	4	5	6	7	8
1	0	0	0	0	0	0	0	1
2	0	0	0	0	0	0	1	0
3	1	0	0	0	0	0	1	1
4	0	0	0	0	0	1	0	0
5	1	0	0	0	0	1	0	1
6	1	0	0	0	0	1	1	0
7	0	0	0	0	0	1	1	1
8	0	0	0	0	1	0	0	0
9	1	0	0	0	1	0	0	1
10	1	0	0	0	1	0	1	0

次に続く

表 Appendix 1-2 ステーション番号と設定スイッチの位置（前から続く）

ステーション 番号	ディップスイッチビット番号							
	1	2	3	4	5	6	7	8
11	0	0	0	0	1	0	1	1
12	1	0	0	0	1	1	0	0
13	0	0	0	0	1	1	0	1
14	0	0	0	0	1	1	1	0
15	1	0	0	0	1	1	1	1
16	0	0	0	1	0	0	0	0
17	1	0	0	1	0	0	0	1
18	1	0	0	1	0	0	1	0
19	0	0	0	1	0	0	1	1
20	1	0	0	1	0	1	0	0
21	0	0	0	1	0	1	0	1
22	0	0	0	1	0	1	1	0
23	1	0	0	1	0	1	1	1
24	1	0	0	1	1	0	0	0
25	0	0	0	1	1	0	0	1
26	0	0	0	1	1	0	1	0
27	1	0	0	1	1	0	1	1
28	0	0	0	1	1	1	0	0
29	1	0	0	1	1	1	0	1
30	1	0	0	1	1	1	1	0
31	0	0	0	1	1	1	1	1
32	0	0	1	0	0	0	0	0
33	1	0	1	0	0	0	0	1
·	·	·	·	·	·	·	·	·
60	1	0	1	1	1	1	0	0
61	0	0	1	1	1	1	0	1
62	0	0	1	1	1	1	1	0
63	1	0	1	1	1	1	1	1
64	0	1	0	0	0	0	0	0

Appendix 2. Vnet/IP インタフェース管理ツール

Vnet/IP インタフェース管理ツールを使用して、Vnet/IP インタフェースパッケージが管理するドメイン番号とステーション番号を設定できます。

■ ドメイン番号とステーション番号の変更手順

Vnet/IP インタフェースパッケージが管理しているドメイン番号とステーション番号を変更するときは、次の手順に従ってください。

1. 仮想マシンのゲスト OS に、管理者ユーザでサインインしてください。スタートメニューから、[YOKOGAWA Virtualization] – [VnetIP interface management tool] を選択してください。
2. Vnet/IP インタフェース管理ツールの [Settings] タブを開いてください。
3. [Domain No] にドメイン番号を、[Station No] にステーション番号を入力して、[Save] ボタンをクリックしてください。

補足

ドメイン番号には 1 から 31 までの番号を、ステーション番号には 1 から 64 までの番号を設定できます。
拡張テスト機能パッケージ、FCS シミュレータパッケージをインストールして、他の HIS からリモート接続可能な FCS シミュレータを動作させる仮想マシンでは、ドメイン番号とステーション番号に、両方とも 0 を設定してください。

なお、ドメイン番号とステーション番号を 0 に設定し、テスト機能のみを使用する場合は、Vnet/IP インタフェースパッケージのライセンスは不要となります。

4. [CLOSE] ボタンをクリックして、仮想マシンを再起動してください。

■ Vnet/IP インタフェースパッケージの稼動状態

[Monitor] タブで、次に示す情報を表示します。

- Vnet/IP インタフェースパッケージのバージョン情報
- Vnet/IP インタフェースパッケージの稼動状態
- ドメイン番号／ステーション番号
- Vnet/IP ファームウェア混在情報

● バージョン情報

Vnet/IP インタフェースパッケージのバージョン番号を表示します。

● 稼動状態

次に示す 5 つの稼動状態を表示します。

Stop : Vnet/IP インタフェースパッケージが停止状態を示す。

Starting : ドメイン番号、ステーション番号チェック中、コンフィグレーションの確認中という稼動状態前の起動状態を示す。

Waiting the license : ライセンス付与待ち状態を示す。

Working : 正常な状態を示す。

Stop(エラーメッセージ) : 停止状態を示す。

参照

エラーメッセージについては、以下を参照してください。

「■ エラーメッセージの対策」ページ App.2-2

● ドメイン番号／ステーション番号

ドメイン番号とステーション番号を表示します。

● Vnet/IP ファームウェア混在情報

Vnet/IP ファームウェアレビジョン情報を表示します。古いファームウェアを使用しているステーションが複数ある場合は、カンマで区切って表示します。

表示例： 06R, 13L

意味： ステーション番号 6 の右側、ステーション番号 13 の左側に実装された Vnet/IP ファームウェアが古い。

■ エラーメッセージの対策

Vnet/IP インタフェース管理ツールを使用する際に発生するエラーメッセージとその対策を説明します。

● Windows サービス登録不正

「Invalid Windows service registration」メッセージの発生条件と対策について説明します。

- ・ 発生条件

Vnet/IP インタフェースパッケージのサービスである「YVWNT_BKNET_Service」、「YVWNT_VnetIP_Stack_Service」、「YVWNT_VnetIP_Privileged_Service」のいずれかが Windows サービスに登録されていない、または Vnet/IP インタフェースパッケージのサービスが自動起動になっていない場合、メッセージが発生します。

- ・ 対策

Vnet/IP インタフェースパッケージを再インストールしてください。

参照

Vnet/IP インタフェースパッケージのインストール手順については、以下を参照してください。

「B4.3.3 仮想マシンに Vnet/IP インタフェースパッケージをインストールする」ページ B4-48

● BUS1 デバイスが見つからない

「BUS1 not found」メッセージの発生条件と対策について説明します。

- ・ 発生条件

制御ネットワーク 1 の名称が不正の場合、メッセージが発生します。

- ・ 対策

制御ネットワーク 1 の名称を VnetIPBUS1 に変更してください。

参照

制御ネットワーク 1 の名称については、以下を参照してください。

「■ ローカルエリア接続の名称変更」ページ B4-77

● BUS2 デバイスが見つからない

「BUS2 not found」メッセージの発生条件と対策について説明します。

- ・ 発生条件

制御ネットワーク 2 の名称が不正の場合、メッセージが発生します。

- ・ 対策

制御ネットワーク 2 の名称を VnetIPBUS2 に変更してください。

参照

制御ネットワーク 2 の名称については、以下を参照してください。

「■ ローカルエリア接続の名称変更」ページ B4-77

● ドメイン・ステーション番号が不正

「Invalid domain number or station number」メッセージの発生条件と対策について説明します。

- 発生条件

Vnet/IP インタフェースパッケージが管理しているドメイン番号とステーション番号が不正の場合、メッセージが発生します。

- 対策

Vnet/IP インタフェース管理ツールを使って、Vnet/IP インタフェースパッケージが管理しているドメイン番号とステーション番号を確認し、正しい値を設定してください。

参照

Vnet/IP インタフェースパッケージが管理するドメイン番号とステーション番号の設定方法については、以下を参照してください。

「■ ドメイン番号とステーション番号の変更手順」ページ App.2-1

● ドメイン・ステーション番号が他ステーションと重複

「Station of the specified domain number and station number already exists」メッセージの発生条件と対策について説明します。

- 発生条件

同一のドメイン番号とステーション番号が既に他のステーションで使用されている場合、メッセージが発生します。

- 対策

Vnet/IP インタフェース管理ツールを使って、Vnet/IP インタフェースパッケージが管理しているドメイン番号とステーション番号を確認し、正しい値を設定してください。

参照

Vnet/IP インタフェースパッケージが管理するドメイン番号とステーション番号の設定方法については、以下を参照してください。

「■ ドメイン番号とステーション番号の変更手順」ページ App.2-1

● IT セキュリティ設定未実行

「IT security not applied」メッセージの発生条件と対策について説明します。

- 発生条件

Vnet/IP インタフェースパッケージをインストール後、IT セキュリティを適用していない場合、メッセージが発生します。

- 対策

IT セキュリティを適用してください。

Blank Page

Appendix 3. Windows 10 インストール時のカスタマイズ

ここでは、Windows 10 Enterprise 2016 LTSB の OS インストール時のカスタマイズ方法を説明します。

補足

横河電機が提供する Windows 10 IoT Enterprise 2016 LTSB がインストールされたコンピュータでは、本カスタマイズを行う必要はありません。

■ Windows 10 インストール時のカスタマイズ手順

Windows 10 Enterprise 2016 LTSB のインストール中に、次の画面が表示されます。そのときに、[カスタマイズ] ボタンをクリックしてください。

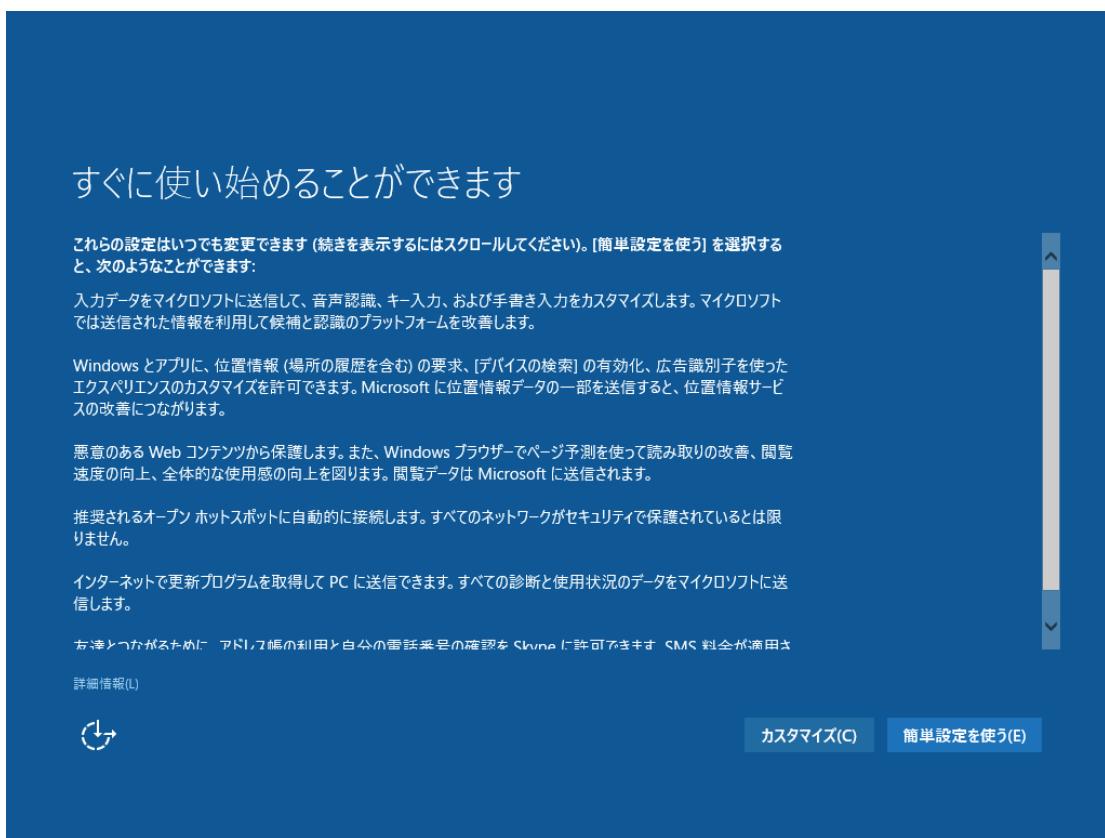


図 Appendix 3-1 Windows 10 インストール時の画面

設定のカスタマイズウィンドウで、すべての設定を [オフ] にしてください。

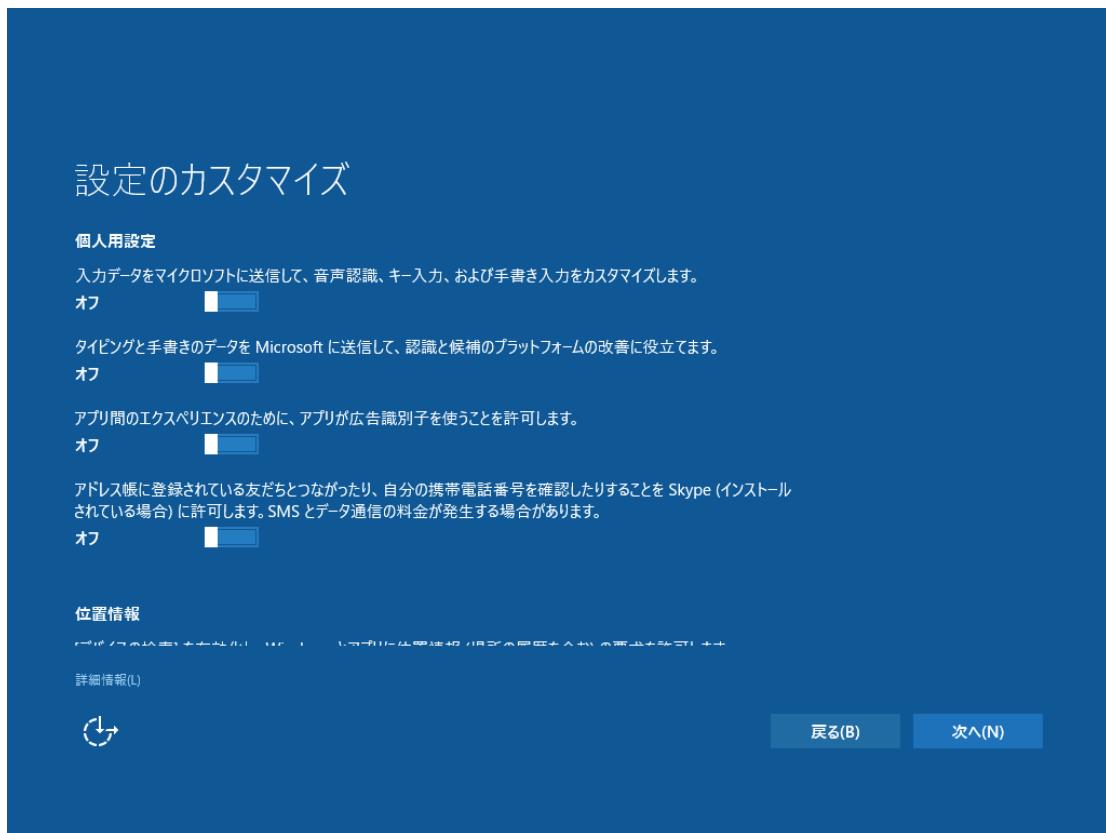


図 Appendix 3-2 設定のカスタマイズウィンドウ-1

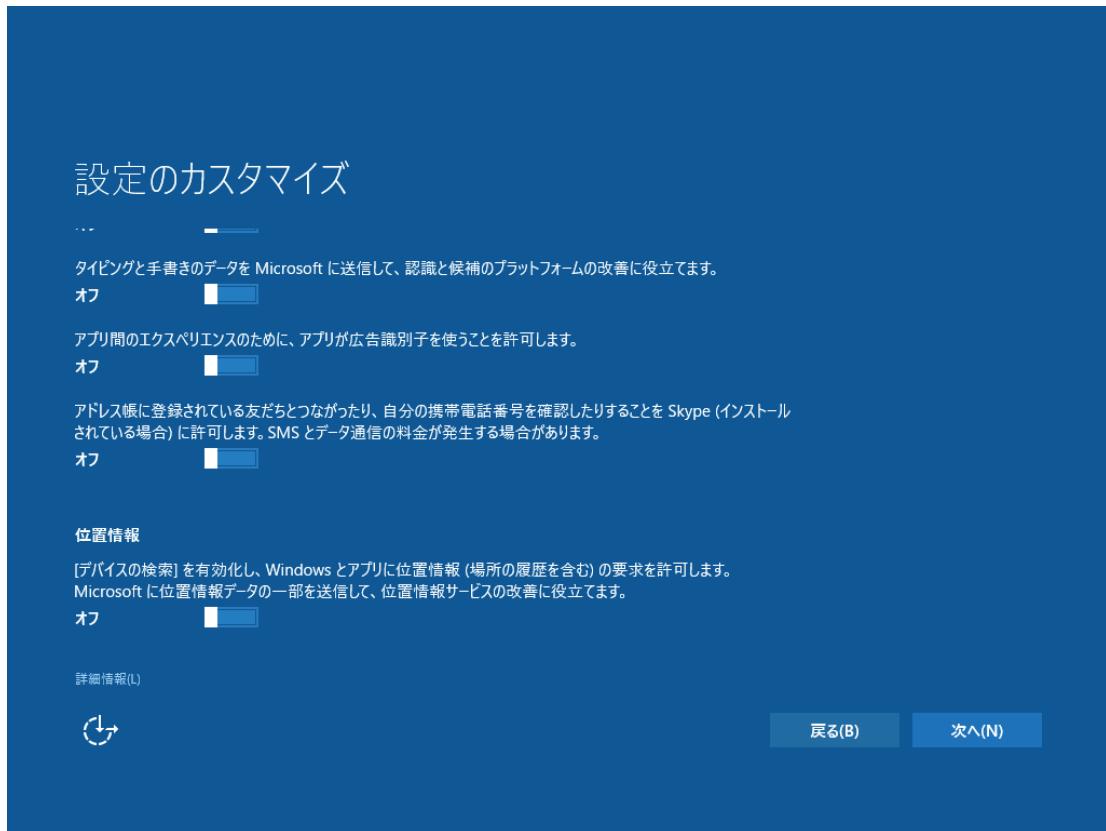


図 Appendix 3-3 設定のカスタマイズウィンドウ-2

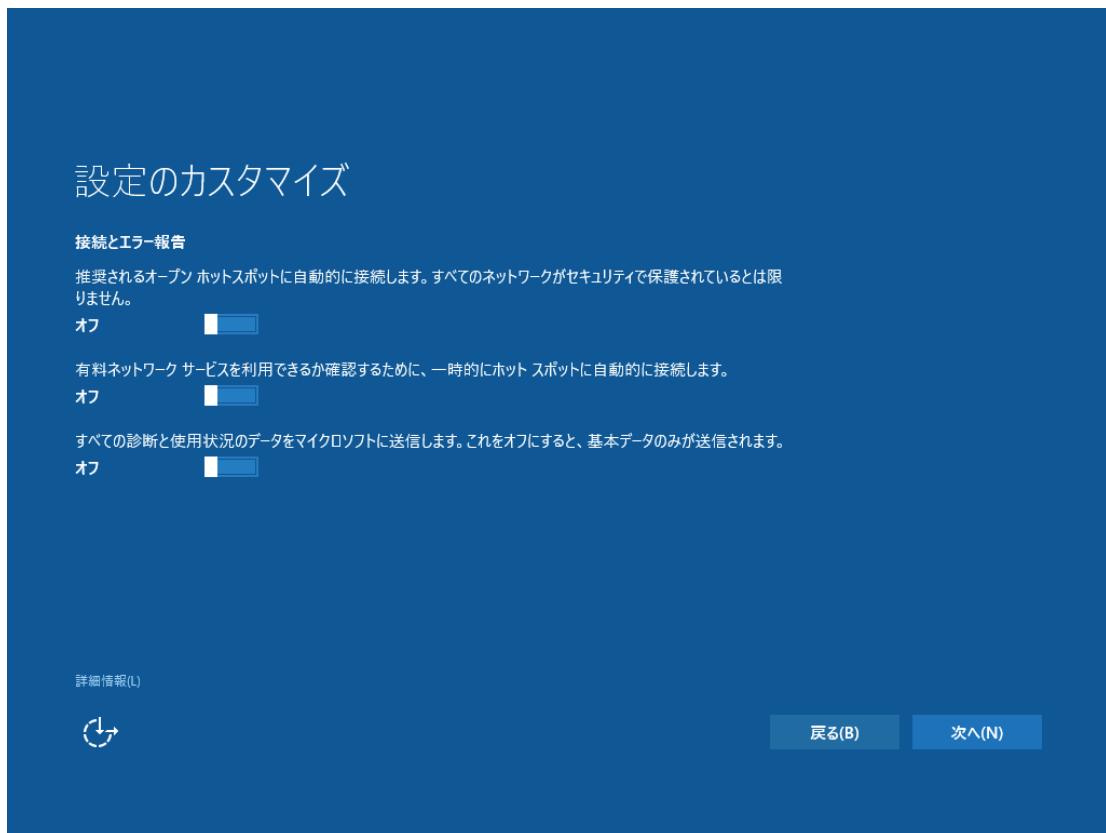


図 Appendix 3-4 設定のカスタマイズウィンドウ-3

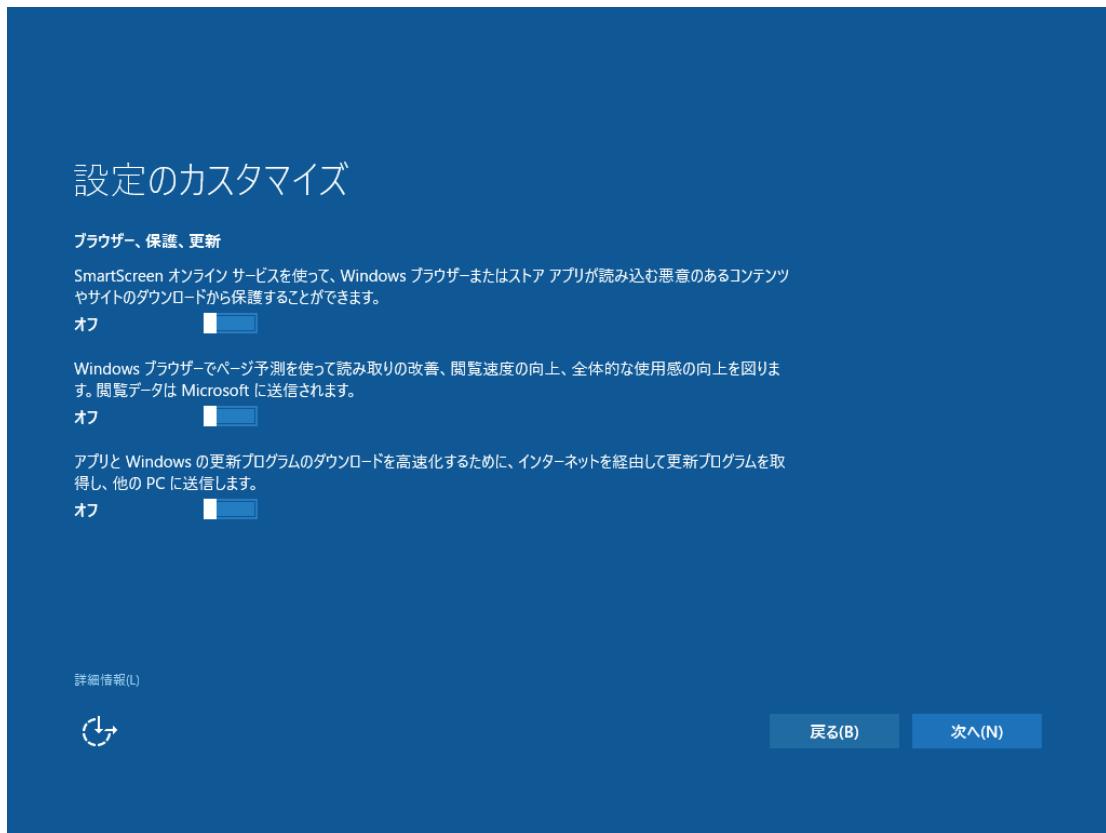


図 Appendix 3-5 設定のカスタマイズウィンドウ-4

[次へ] ボタンをクリックして、Windows 10 Enterprise 2016 LTSB のインストールを続けてください。

Blank Page

CENTUM VP インストール手順

IM 33J01C10-01JA 9 版

索引

B

BKHBos.exe B5-38

C

CENTUM CS 1000 から CENTUM VP R5 へのアップグレードをする C6-17
 CENTUM CS 3000 から CENTUM VP R5 にバージョンアップする C6-2
 CENTUM VP R4/R5 から R6 へのバージョンアップをする C6-29
 CENTUM VP Small B4-72
 CENTUM 認証モード B4-138
 レビジョンアップ時の注意事項 C11-1

E

ENG グループユーザ B4-141

H

HF バス／RL バスインターフェースカード B3-6
 HIS グループユーザ B4-144
 HIS タイプシングルサインオン B4-146,C4-4
 HIS の自動起動と自動ログオン B4-86

I

IP アドレス B1-1

O

OPKB 用 USB ドライバ C7-17

P

PICOT C5-7

R

RAS ドライバ B4-84,C7-18
 RemoteApp プログラム B5-14,B5-35
 RS-232C ドライバ B4-81,C7-18

S

StartDesktop.bat B5-35

T

TCP/IP B4-70

U

UPS (無停電源装置) B4-149

V

Vnet/IP オープン通信ドライバ B4-46,C7-14
 Vnet/IP インタフェースカード B4-4
 Vnet/IP オープン通信ドライバ B4-46,C7-14
 V ネットインターフェースカード B3-8
 V ネットルータ B3-11

W

Windows Defender B4-10,B4-18,B4-24
 Windows 認証モード B4-140,C4-1
 Windows ネットワークの設定 B4-52

ア

アンインストール C7-1

オ

オペレーションキーボード B4-85
 オペレーションキーボード (OPKB) 用 USB ドライバ B4-79

カ

仮想メモリ B4-8,B4-14,B4-23,B4-36
 管理者アカウントとパスワード B1-2

コ

コミュニケーションゲートウェイユニット B3-13
 コンソール形 HIS の設定 B4-81
 コンピュータ名／ステーション名 B1-1

ナ

再インストール C8-1
 サブネットマスク B1-1

セ

- 制御バスインターフェースカード B4-2
 制御バスドライバ B4-44,C7-13
 セキュリティポリシー B1-2

ソ

- ソフトウェア環境 A3-1

タ

- タッチパネル B4-85

チ

- 帳票 C5-6

テ

- ディスクデフラグ B4-11,B4-20,B4-25

ト

- ドメインコントローラ B2-7
 トラブルシューティング C10-1

ハ

- バス変換器 B3-5
 バックアップ C5-1
 ハードウェア環境 A3-1

フ

- ファイルシステム B4-8,B4-14,B4-23,B4-36
 プロセッサユニット B3-2

ユ

- ユーザーアカウント B4-104
 ユーザ認証モード B4-136

ラ

- ライセンス管理専用のコンピュータ B7-1
 ライセンスの配布と反映を行う B4-103
 ライセンスの割り付けを変更する C1-3
 ライセンスを追加する C1-2

リ

- リモート操作監視サーバ機能 B5-1

改訂情報

資料名称：CENTUM VP インストール手順

資料番号：IM 33J01C10-01JA

2019年8月／9版／R6.07以降

- A2.2 記述追加
- A2.2.1 記述追加
- A2.2.13 新規追加
- A3. 記述追加
- B1. 記述追加、記述変更
- B4. 記述追加
- B4.2 記述追加、記述変更
- B4.3 記述追加、記述変更
- B4.6 記述追加
- B4.7 記述追加、記述削除
- B4.10 記述追加
- B4.11.2 記述変更
- B5. 記述追加
- B5.1.1 記述変更
- B8.2.1 記述追加
- B8.3.2 記述変更
- C6.1.1 記述追加
- C6.1.2 記述削除
- C6.4 記述変更
- C7.1 記述追加
- C10.1.2 記述削除
- C10.1.3 記述削除
- C10.1.4 記述削除
- C10.1.5 記述削除
- C10.1.6 記述削除
- C10.2.2 記述削除
- C11.2.4 記述変更
- C11.21 新規追加
- D1.1.1 記述追加、記述変更
- D1.1.2 記述変更
- D1.1.3 記述変更
- D1.1.6 記述変更
- D1.2.1 記述変更
- D1.3.1 記述変更、記述削除
- D1.3.2 記述変更、記述削除

2018年8月／8版／R6.06

- A2.2 記述変更
- A2.2.2 新規追加

A3.	記述変更
B1.	記述追加
B2.6	記述追加
B4.	記述変更
B4.1	記述変更
B4.2	記述追加
B4.3	記述追加と変更
B4.7	記述変更
B4.10	記述追加と変更
B5.1	記述変更
B6.	記述変更
B8.	新規追加
C6.1.1	記述変更
C6.1.2	記述変更
C6.1.3	新規追加
C6.3	記述変更
C6.4	記述変更
C7.1	記述追加
C7.1.4	記述変更
C10.2	記述追加
C10.3.2	記述追加
C11.9	記述追加
C11.20	記述追加
D1.6.1	記述追加
Appendix 2.	記述変更

2017年11月／7版／R6.05

B1.	記述追加
B3.1	記述追加
B4.2	記述変更
B4.2.2	記述追加
B4.2.4	記述追加
C2.	記述変更
C6.1.2	記述追加
C6.4	記述追加
C7.1	記述追加
C10.1	記述変更
C11.15	記述追加・削除
C11.19	新規追加

2017年4月／6版／R6.04

全般	スタートメニューに関する記述変更
A2.2.10	記述変更
A3.	記述変更
B1.	記述変更

B2.全体	記述追加・変更
B3.6	記述追加
B4.全体	記述追加・変更
B5.全体	記述変更
B6.	記述追加
B6.1	記述変更
B7.	記述追加
C5.	記述変更
C5.2	記述変更
C6.3	記述追加
C6.4	記述追加
C6.5	記述追加
C7.1	記述変更
C9.	記述変更
C9.1	記述変更
C9.2	新規追加
C9.3	新規追加
C10.全体	記述変更
C10.1.7	新規追加
C10.3.4	新規追加
C11.18	新規追加
D1.	記述変更
D1.1.5	新規追加
D1.1.6	新規追加
Appendix 2.	新規追加

2016年9月／5版／R6.03.10

A2.2	記述変更
A3.	記述変更
B1.	記述追加
B2.5	記述追加
B4.	記述変更
B4.1	記述変更
B4.2	記述変更
B4.3	記述追加
B4.7	記述追加
B4.10	記述変更
C11.16	記述変更
C11.17	新規追加

2016年6月／4版／R6.03

A2.2	記述追加
A2.2.11	新規追加
A3.	記述変更
B2.5	新規追加

B3.6.2 記述変更
B4.1 記述変更
B4.2 記述追加
B4.2.3 新規追加
B4.3.1 記述追加
B4.3.2 記述追加
B4.3.3 記述追加
B4.3.5 新規追加
B4.6 記述追加
B4.10 記述追加
B4.10.3 新規追加
C6.4 記述追加
C6.7 新規追加
C10.1.7 新規追加
C11.16 新規追加
D1.1 記述追加
D1.1.1 記述変更
D1.1.3 記述変更
D1.1.4 記述変更
D1.2.1 記述変更

2015年12月／3版／R6.02

全般 媒体形名の記述削除
A3. 「● 共存できるソフトウェア」の記述変更
C6. 記述追加
C6.4 新規追加
C11.15 新規追加
D1. 「● パッケージコード」の記述追加
D1.7 新規追加

2015年4月／2版／R6.01.10

C11.14 新規追加

2015年3月／初版／R6.01

新規発行

■ お問い合わせについて

問い合わせ : <http://www.yokogawa.co.jp/dcs> より、お問い合わせフォームをご利用ください。

■ 著作者 横河電機株式会社

■ 発行者 横河電機株式会社

〒 180-8750 東京都武蔵野市中町 2-9-32

Blank Page
