



CENTUM VP セキュリティガイド

IM 33J01C30-01JA

IM 33J01C30-01JA

9 版

はじめに

本書は、CENTUM VP システムに IT (Information Technology) の観点からセキュリティを導入するためのガイドです。


CENTUM VP としてのセキュリティモデルや設定内容について記載しています。セキュリティモデルごとのセキュリティの内容について詳細を知りたい場合は、本書をお読みください。


本書は、CENTUM VP システムの構築、運用を検討するエンジニア向けに記載しています。

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、本製品外部に別途で用意ください。
- ・ 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。

⊕ 「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随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、記載もれなどお気づ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、本製品に関して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して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。

ユーザズマニュアル中の凡例

■ ユーザズマニュアル中のシンボルマーク

ユーザ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避けるための注意事項を記載しています。



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



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。



説明を補足するための事柄を記載しています。



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。

■ ユーザズマニュアル中の表記

ユーザズマニュアル中の表記は、次の内容を示します。

● ユーザ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

- ・ Δ 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：

`.ALΔPIC010Δ-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：

`.PRΔTAG{Δ.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 セキュリティガイド

IM 33J01C30-01JA 9 版

目 次

1.	概要.....	1-1
1.1	対処すべきセキュリティ脅威.....	1-2
1.2	セキュリティ対策.....	1-3
2.	セキュリティモデル.....	2-1
2.1	セキュリティモデルの概要.....	2-2
2.2	ユーザ／グループの管理.....	2-12
2.2.1	ユーザ管理の種類.....	2-13
2.2.2	CENTUM VP のユーザ認証モード.....	2-14
2.2.3	ユーザとグループの管理.....	2-17
2.2.4	ユーザ名とパスワードの規約.....	2-25
2.2.5	特別なユーザ.....	2-26
3.	セキュリティ対策の詳細.....	3-1
3.1	アクセスコントロール.....	3-2
3.1.1	ファイル／フォルダに対するアクセス許可.....	3-3
3.1.2	レジストリ構成とユーザ／グループ.....	3-7
3.1.3	DCOM (OPC) とユーザ／グループ.....	3-10
3.1.4	ローカルセキュリティとユーザ／グループ.....	3-11
3.2	パーソナルファイアウォールチューニング.....	3-12
3.3	不要な Windows サービスの停止.....	3-16
3.4	IT セキュリティバージョン 2.0/1.0 共通の IT 環境の設定項目.....	3-18
3.4.1	NetBIOS over TCP/IP の無効化.....	3-19
3.4.2	BIOS による HDD パスワード機能.....	3-20
3.5	IT セキュリティバージョン 2.0 におけるグループポリシー設定項目.....	3-21
3.5.1	ビルトイン Administrator アカウントの無効化またはユーザ名変更.....	3-22
3.5.2	ソフトウェア制限ポリシーの適用.....	3-23
3.5.3	StorageDevicePolicies 機能の適用.....	3-25
3.5.4	USB ストレージデバイスの無効化.....	3-26
3.5.5	パスワードポリシーの適用.....	3-27
3.5.6	監査ポリシーの詳細な構成.....	3-28
3.5.7	アカウントロックアウトポリシーの適用.....	3-30
3.5.8	ユーザ権利の割り当て.....	3-31
3.5.9	セキュリティオプション.....	3-32
3.5.10	管理用テンプレート.....	3-34
3.5.11	ユーザ構成-管理用テンプレート.....	3-42
3.6	IT セキュリティバージョン 1.0 におけるグループポリシー設定項目.....	3-43
3.6.1	ビルトイン Administrator アカウントの無効化またはユーザ名変更.....	3-44
3.6.2	直前ログオンユーザ名の非表示.....	3-45
3.6.3	ソフトウェア制限ポリシーの適用.....	3-46
3.6.4	AutoRun の制限の適用.....	3-47
3.6.5	StorageDevicePolicies 機能の適用.....	3-48

3.6.6	USB ストレージデバイスの無効化.....	3-49
3.6.7	LAN Manager 認証レベルの変更.....	3-50
3.6.8	パスワードポリシーの適用.....	3-51
3.6.9	監査ポリシーの適用.....	3-52
3.6.10	アカウントロックアウトポリシーの適用.....	3-53
4.	セキュリティ機能の選定.....	4-1
4.1	セキュリティを設定する前に考慮する項目.....	4-2
4.2	モデルケース.....	4-5
5.	運用上の注意事項.....	5-1
5.1	Windows のアカウント管理.....	5-2
5.1.1	共通アカウント管理.....	5-3
5.1.2	個別アカウント管理.....	5-4
5.1.3	共通アカウント管理／個別アカウント管理で共通な注意事項.....	5-5
5.2	関連プログラム.....	5-6
5.3	システム導入時および運用時のセキュリティに関する注意事項.....	5-7
6.	セキュリティ設定のためのユーティリティ	6-1
6.1	IT セキュリティツール.....	6-2
6.2	IT セキュリティツールを実行する.....	6-4
6.3	IT セキュリティ設定を変更する.....	6-5
6.3.1	CENTUM VP ソフトウェアをインストールしたコンピュータの場合.....	6-6
6.3.2	ファイルサーバやドメインコントローラの場合.....	6-9
6.4	IT セキュリティ設定を保存する.....	6-13
6.4.1	CENTUM VP ソフトウェアをインストールしたコンピュータの場合.....	6-14
6.4.2	ファイルサーバやドメインコントローラの場合.....	6-17
6.5	IT セキュリティ設定を復元する.....	6-18
6.5.1	CENTUM VP ソフトウェアをインストールしたコンピュータの場合.....	6-19
6.5.2	ファイルサーバやドメインコントローラの場合.....	6-21
6.6	セキュリティ設定ファイルのパスワードを変更する.....	6-22
6.6.1	CENTUM VP ソフトウェアをインストールしたコンピュータの場合.....	6-23
6.6.2	ファイルサーバやドメインコントローラの場合.....	6-25
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.....	6-26
6.8	IT セキュリティツールで設定した情報を参照する.....	6-28
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.....	6-29
6.9.1	グループポリシーオブジェクトを作成する.....	6-30
6.9.2	組織単位にグループポリシーオブジェクトを適用する.....	6-32
6.10	その他のユーティリティ	6-34
6.10.1	CreateCentumProcess.....	6-35
6.10.2	CreateUgsProcess.....	6-36
6.10.3	CreateLicenseProcess.....	6-37
6.10.4	CreateAdsProcess.....	6-38
6.10.5	CreateAdsAgent.....	6-39
6.10.6	CreateRDCProcess.....	6-40
6.10.7	CreateOffuser.....	6-41
6.10.8	YVWNETCreateVNTUser.....	6-42
6.10.9	ChangeOffuserPassword.....	6-44
6.10.10	OFFUSEREnabler.....	6-45
6.10.11	OFFUSERDisabler.....	6-46
6.10.12	StorageDeviceCTL.....	6-47
6.10.13	ITSecuritySettingItemExport.....	6-49

CENTUM VP セキュリティガイド

IM 33J01C30-01JA 9 版

目次

付録

Appendix 1. IT セキュリティ設定項目	App.1-1
Appendix 1.1 IT セキュリティバージョン 2.0	App.1-2
Appendix 1.1.1 CENTUM VP ソフトウェアをインストールしたコンピュータの場合.	App.1-3
Appendix 1.1.2 ファイルサーバやドメインコントローラの場合	App.1-12
Appendix 1.2 IT セキュリティバージョン 1.0	App.1-25
Appendix 1.2.1 CENTUM VP ソフトウェアをインストールしたコンピュータの場合.	App.1-26
Appendix 1.2.2 ファイルサーバやドメインコントローラの場合	App.1-28

1. 概要

本書は、本製品にセキュリティ対策を実施し、運用するためのガイドです。
セキュリティ対策を実施し、運用することで、現存するセキュリティ脅威と将来想定されるセキュリティ脅威から本製品を保護します。
本書で紹介するセキュリティモデルは、あくまでも本製品の一般的な構成を基に検討したセキュリティモデルです。実際のシステムに適用する場合は、エンジニアリング方法や運用方法を考慮した上で適用してください。

■ 本書で使用されるセキュリティに関連した用語

セキュリティに関連した用語を次に示します。

表 1-1 セキュリティ関連の用語

用語	説明
IT セキュリティ	現在から将来にわたって、サイバーテロなどのセキュリティ脅威に対して防御および対処するために、IT 環境から考慮したセキュリティ対策
ユーザ認証モード	Windows のユーザと CENTUM VP で使用するユーザのユーザ管理方法を規定する機能。Windows 認証モードと CENTUM 認証モードの 2 つのモードが存在する
CENTUM 認証モード	ユーザ認証モードの 1 つ。Windows 側の機能から独立して、CENTUM VP のユーザ管理およびアクセス制御を行うモード
Windows 認証モード	ユーザ認証モードの 1 つ。Windows のユーザと CENTUM VP で使用するユーザを連携して動作させるモードのこと。HIS へユーザインするタイプとして、Windows タイプシングルサインオンと HIS タイプシングルサインオンの 2 つのタイプが存在する
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。HIS のユーザインダイアログを利用するタイプ
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。Windows のログオンダイアログを利用するタイプ
ケルベロス（Kerberos）認証	Windows ドメインのデフォルトの認証方式。Windows ドメイン環境のような、サーバや PC が混在する環境において、1 度の認証で全システムが利用できるようなシングルサインオン環境に適する
パーソナルファイアウォール	PC やドメインコントローラ上で動作するファイアウォール。Windows 標準のファイアウォール以外も含む
二要素認証	指紋認証とパスワード認証の両方とも用いるなど、2 種類の認証方法で認証を行うことです。パスワード認証を 2 回行うなどの、同様な認証方法を 2 回実施することは二要素認証と呼ばれません。
セキュリティ区画	許可された者しかアクセスできないように管理された物理的、または論理的な区画です。セキュリティ区画内の施設や設備には特別な管理が要求され、他の区画とは明確に分離されています。

1.1 対処すべきセキュリティ脅威

本製品のセキュリティが対処すべきセキュリティ脅威について説明します。

■ セキュリティ脅威

CENTUM VP がさらされるセキュリティ脅威には、次のようなものがあります。

1. ネットワーク経由の攻撃
企業内ネットワークなどから、CENTUM VP システムに対して権限を持たない者がネットワーク経由で CENTUM VP システムへ影響を及ぼす脅威。また、その結果 CENTUM VP システムの重要なデータが漏えいする脅威。
2. HIS やシステム生成機能を搭載した PC を操作しての直接攻撃
CENTUM VP システムに対して権限を持たない者が HIS やシステム生成機能を搭載した PC を直接操作して、システムへ影響を及ぼし、重要なデータが持ち出される脅威。
3. HIS やシステム生成機能を搭載した PC やデータの盗難
HIS やシステム生成機能を搭載した PC やデータが持ち出され、解析される脅威。

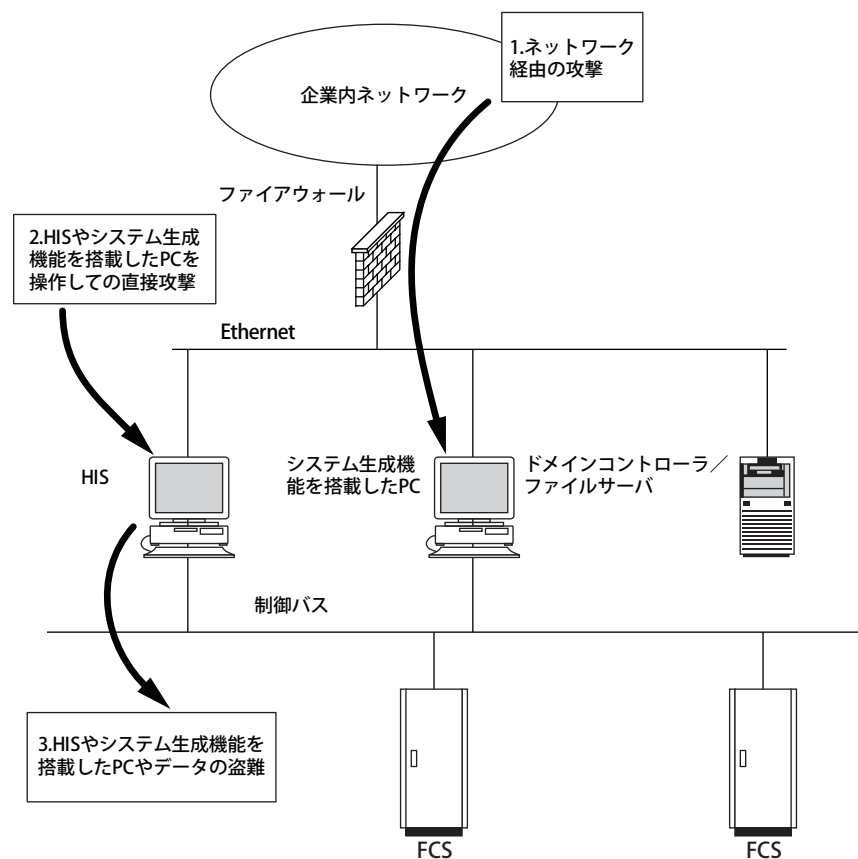


図 1.1-1 セキュリティ脅威

1.2 セキュリティ対策

セキュリティ脅威に対するセキュリティ対策について説明します。本製品で必要なセキュリティ対策の項目を洗い出し、その中からセキュリティ強度に応じて、必要なセキュリティ対策の項目を選びます。

■ セキュリティ対策と対処するセキュリティ脅威

セキュリティ脅威に対処するため、Microsoft 社で発行される各 OS 向けセキュリティガイドや、一般的なビジネスネットワーク環境で適用されているセキュリティ対策を、本製品用に最適化しました。セキュリティ対策がカバーする範囲によって、IT セキュリティバージョン 2.0 と IT セキュリティバージョン 1.0 の 2 種類があります。次に、それぞれについて説明します。

- IT セキュリティバージョン 2.0
IT セキュリティバージョン 1.0 を見直し、より多くのセキュリティ対策を含みます。セキュリティモデルとしては、標準モデル、強固モデルに対応しています。
- IT セキュリティバージョン 1.0
CENTUM VP R6.03 までのセキュリティ対策です。セキュリティモデルとしては、従来モデル、標準モデル、強固モデルに対応しています。

IT セキュリティバージョン 2.0 と IT セキュリティバージョン 1.0 は、同じプロジェクト内に混在できます。

このセキュリティ対策によって対処されるセキュリティ脅威を、セキュリティバージョン別に示します。

[1]：ネットワーク経由の攻撃

[2]：HIS やシステム生成機能を搭載したコンピュータを操作しての直接攻撃

[3]：HIS やシステム生成機能を搭載したコンピュータ／データの盗難

表 1.2-1 セキュリティ脅威に対処するセキュリティ対策-IT セキュリティバージョン 2.0

セキュリティ対策	セキュリティ脅威への対処		
	[1]	[2]	[3]
パスワードのポリシー「パスワードの長さ」	Yes	Yes	No
パスワードのポリシー「パスワードの変更禁止期間」	Yes	Yes	No
パスワードのポリシー「パスワードの有効期間」	Yes	Yes	No
パスワードのポリシー「パスワードの履歴を記録する」	Yes	Yes	No
パスワードのポリシー「暗号化を元に戻せる状態でパスワードを保存する」を無効に設定する	Yes	Yes	No
パスワードのポリシー「複雑さの要件を満たす必要があるパスワード」	Yes	Yes	No
ファイル／フォルダのアクセスコントロール	Yes	Yes	No
製品のレジストリのアクセスコントロール	Yes	Yes	No
DCOM(OPC)のアクセスコントロール	Yes	Yes	No
パーソナルファイアウォールのチューニング	Yes	No	No
パーソナルファイアウォール「ユニキャスト応答の許可」を無効に設定する	Yes	No	No
不要な Windows サービスの停止	Yes	No	No
アカウントロックアウトのポリシー「アカウントのロックアウトのしきい値」	Yes	Yes	No

次に続く

表 1.2-1 セキュリティ脅威に対処するセキュリティ対策-IT セキュリティバージョン 2.0（前から続く）

セキュリティ対策	セキュリティ脅威への対処		
	[1]	[2]	[3]
アカウントロックアウトのポリシーー「ロックアウトカウンターのリセット」	Yes	Yes	No
アカウントロックアウトのポリシーー「ロックアウト期間」	Yes	Yes	No
NetBIOS over TCP/IP の無効化	Yes	No	No
StorageDevicePolicies 機能の適用	No	Yes	Yes
USB ストレージデバイスの無効化	No	Yes	Yes
ソフトウェア制限ポリシーの適用	Yes	Yes	No
ユーザー権利の割り当てー「ネットワーク経由でのアクセス」	Yes	No	No
ユーザー権利の割り当てー「ドメインにワークステーションを追加」	Yes	Yes	No
ユーザー権利の割り当てー「ローカルログオンを許可」	No	Yes	No
ユーザー権利の割り当てー「ローカルログオンを拒否」	No	Yes	No
セキュリティオプションー「監査：監査ポリシーサブカテゴリの設定（Windows Vista 以降）を強制して、監査ポリシーカテゴリの設定を上書きする」	Yes	Yes	No
セキュリティオプションー「デバイス：ユーザーがプリンタードライバをインストールできないようにする」	No	Yes	No
セキュリティオプションー「デバイス：CD-ROM へのアクセスを、ローカルログオンユーザーだけに制限する」	Yes	No	No
セキュリティオプションー「デバイス：フロッピーへのアクセスを、ローカルログオンユーザーだけに制限する」	Yes	No	No
セキュリティオプションー「ドメインコントローラー：Server Operators がタスクのスケジュールを割り当てるのを許可する」を無効に設定する	No	Yes	No
セキュリティオプションー「ドメインコントローラー：コンピューターアカウントのパスワードの変更を拒否する」を無効に設定する	No	Yes	No
セキュリティオプションー「ドメインメンバー：強力な（Windows 2000 かそれ以降のバージョン）セッションキーを必要とする」	Yes	No	No
セキュリティオプションー「対話型ログオン：セッションがロックされているときにユーザーの情報を表示する」をユーザー情報は表示しないに設定する	No	Yes	No
セキュリティオプションー「対話型ログオン：最後のユーザー名を表示しない」	No	Yes	No
セキュリティオプションー「対話型ログオン：Ctrl + Alt + Del を必要としない」を無効に設定する	No	Yes	No
セキュリティオプションー「対話型ログオン：コンピューターの非アクティブ状態の上限」	No	Yes	No
セキュリティオプションー「対話型ログオン：パスワードが無効になる前にユーザーに変更を促す」	Yes	Yes	No
セキュリティオプションー「Microsoft ネットワークサーバー：クライアントが同意すれば、通信にデジタル署名を行う」	Yes	No	No
セキュリティオプションー「Microsoft ネットワークサーバー：サーバー SPN ターゲット名検証レベル」	Yes	No	No
「MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)」	Yes	No	No
「MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)」を無効に設定する	Yes	No	No

次に続く

表 1.2-1 セキュリティ脅威に対処するセキュリティ対策-IT セキュリティバージョン 2.0（前から続く）

セキュリティ対策	セキュリティ脅威への対処		
	[1]	[2]	[3]
「MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)」	Yes	No	No
セキュリティオプション「ネットワークアクセス：SAM アカウントの匿名の列挙を許可しない」	Yes	No	No
セキュリティオプション「ネットワークアクセス：SAM アカウントおよび共有の匿名の列挙を許可しない」	Yes	No	No
セキュリティオプション「ネットワークアクセス：ネットワーク認証のためにパスワードおよび資格情報を保存することを許可しない」	Yes	No	No
セキュリティオプション「ネットワークセキュリティ：NTLM で Local System によるコンピューター ID の使用を許可する」	Yes	No	No
セキュリティオプション「ネットワークセキュリティ：Local System による NULL セッションフォールバックを許可する」を無効に設定する	Yes	No	No
セキュリティオプション「ネットワークセキュリティ：ログオン時間を経過した場合はユーザを強制的にログオフさせる」	No	Yes	No
セキュリティオプション「ネットワークセキュリティ：LAN Manager 認証レベル」	Yes	No	No
セキュリティオプション「ネットワークセキュリティ：NTLM SSP ベース（セキュア RPC を含む）のクライアント向け最小セッションセキュリティ」	Yes	No	No
セキュリティオプション「ネットワークセキュリティ：NTLM SSP ベース（セキュア RPC を含む）のサーバー向け最小セッションセキュリティ」	Yes	No	No
セキュリティオプション「シャットダウン：システムのシャットダウンにログオンを必要としない」を無効に設定する	No	Yes	No
セキュリティオプション「ユーザーアカウント制御：ビルトイン Administrator アカウントのための管理者承認モード」	No	Yes	No
セキュリティオプション「ユーザーアカウント制御：管理者承認モードでの管理者に対する昇格時のプロンプトの動作」	No	Yes	No
監査ポリシーの詳細な構成「資格情報の確認の監査」	Yes	Yes	No
監査ポリシーの詳細な構成「コンピューターアカウントの管理の監査」	Yes	Yes	No
監査ポリシーの詳細な構成「その他のアカウント管理イベントの監査」	Yes	Yes	No
監査ポリシーの詳細な構成「セキュリティグループの管理の監査」	Yes	Yes	No
監査ポリシーの詳細な構成「ユーザーアカウントの管理の監査」	Yes	Yes	No
監査ポリシーの詳細な構成「プロセス作成の監査」	Yes	Yes	No
監査ポリシーの詳細な構成「ディレクトリサービスのアクセス」	Yes	Yes	No
監査ポリシーの詳細な構成「ディレクトリサービスの変更の監査」	Yes	Yes	No
監査ポリシーの詳細な構成「アカウントロックアウトの監査」	Yes	Yes	No
監査ポリシーの詳細な構成「ログオフの監査」	Yes	Yes	No

次に続く

表 1.2-1 セキュリティ脅威に対処するセキュリティ対策-IT セキュリティバージョン 2.0（前から続く）

セキュリティ対策	セキュリティ脅威への対処		
	[1]	[2]	[3]
監査ポリシーの詳細な構成－「ログオンの監査」	Yes	Yes	No
監査ポリシーの詳細な構成－「その他のログオン／ログオフイベントの監査」	Yes	Yes	No
監査ポリシーの詳細な構成－「特殊なログオンの監査」	Yes	Yes	No
監査ポリシーの詳細な構成－「リムーバブル記憶域の監査」	Yes	Yes	No
監査ポリシーの詳細な構成－「監査ポリシーの変更の監査」	Yes	Yes	No
監査ポリシーの詳細な構成－「認証ポリシーの変更の監査」	Yes	Yes	No
監査ポリシーの詳細な構成－「フィルタリングプラットフォームポリシーの変更の監査」	Yes	Yes	No
監査ポリシーの詳細な構成－「MPSSVC ルールレベルポリシーの変更の監査」	Yes	Yes	No
監査ポリシーの詳細な構成－「その他のポリシー変更イベントの監査」	Yes	Yes	No
監査ポリシーの詳細な構成－「重要な特権の使用の監査」	Yes	Yes	No
監査ポリシーの詳細な構成－「IPsec ドライバー」	No	Yes	No
監査ポリシーの詳細な構成－「その他のシステムイベントの監査」	Yes	Yes	No
監査ポリシーの詳細な構成－「セキュリティ状態の変更の監査」	Yes	Yes	No
監査ポリシーの詳細な構成－「セキュリティシステムの拡張の監査」	Yes	Yes	No
監査ポリシーの詳細な構成－「システムの整合性の監査」	Yes	Yes	No
個人用設定－「ロック画面カメラを有効にできないようにする」	No	Yes	No
個人用設定－「ロック画面スライドショーを有効にできないようにする」	No	Yes	No
WLAN 設定－「推奨されるオープンホットスポット、連絡先によって共有されたネットワーク、有料サービスを提供するホットスポットに Windows が自動的に接続することを許可する」	Yes	No	No
SCM－「Enable LSA Protection」	Yes	Yes	No
SCM－「Lsass.exe audit mode」	Yes	Yes	No
グループポリシー－「レジストリポリシーの処理を構成する」	Yes	Yes	No
インターネット通信の設定－「プリンタードライバーの HTTP 経由でのダウンロードをオフにする」	Yes	No	No
インターネット通信の設定－「イベントビューアーの 'Event.asp' リンクをオフにする」	Yes	No	No
インターネット通信の設定－「Web 発行およびオンライン注文ウィザードのインターネットダウンロードをオフにする」	Yes	No	No
インターネット通信の設定－「HTTP 経由の印刷をオフにする」	Yes	No	No
インターネット通信の設定－「検索コンパニオンの内容ファイルの更新をオフにする」	Yes	No	No
インターネット通信の設定－「ファイルおよびフォルダーの 'Web に発行' タスクをオフにする」	Yes	No	No
インターネット通信の設定－「Windows カスタマーエクスペリエンス向上プログラムをオフにする」	Yes	No	No
インターネット通信の設定－「Windows Messenger カスタマーエクスペリエンス向上プログラムをオフにする」	Yes	No	No

次に続く

表 1.2-1 セキュリティ脅威に対処するセキュリティ対策-IT セキュリティバージョン 2.0（前から続く）

セキュリティ対策	セキュリティ脅威への対処		
	[1]	[2]	[3]
ログオンー「ネットワークの選択の UI を表示しない」	Yes	Yes	No
ログオンー「ドメインに参加しているコンピューターに接続しているユーザーを列挙しない」	No	Yes	No
ログオンー「レガシの実行の一覧を処理しない」	No	Yes	No
ログオンー「一度だけ実行するコマンドの一覧を処理しない」	No	Yes	No
ログオンー「ドメインに参加しているコンピューターのローカルユーザーを列挙する」を無効に設定する	No	Yes	No
ログオンー「ロック画面のアプリ通知をオフにする」	No	Yes	No
軽減策オプションー「信頼されていないフォントのブロック」	Yes	Yes	No
リモートプロシージャコールー「RPC エンドポイントマッパークライアント認証を有効にする」	Yes	Yes	No
ユーザープロファイルー「広告 ID を無効にする」	Yes	No	No
アプリのプライバシーー「Windows アプリでアカウント情報にアクセスする」	Yes	No	No
アプリのプライバシーー「Windows アプリで通話履歴にアクセスする」	Yes	No	No
アプリのプライバシーー「Windows アプリで連絡先にアクセスする」	Yes	No	No
アプリのプライバシーー「Windows アプリでメールにアクセスする」	Yes	No	No
アプリのプライバシーー「Windows アプリで位置情報にアクセスする」	Yes	No	No
アプリのプライバシーー「Windows アプリでメッセージングにアクセスする」	Yes	No	No
アプリのプライバシーー「Windows アプリでモーションにアクセスする」	Yes	No	No
アプリのプライバシーー「Windows アプリでカレンダーにアクセスする」	Yes	No	No
アプリのプライバシーー「Windows アプリでカメラにアクセスする」	Yes	No	No
アプリのプライバシーー「Windows アプリでマイクにアクセスする」	Yes	No	No
アプリのプライバシーー「Windows アプリで信頼済みデバイスにアクセスする」	Yes	No	No
アプリのプライバシーー「Windows アプリで無線を制御する」	Yes	No	No
アプリのプライバシーー「Windows アプリでデバイスと同期する」	Yes	No	No
アプリ実行時ー「ホストされているコンテンツから Windows ランタイム API でアクセスする Windows ストアアプリを起動できないようにする」	Yes	No	No
自動再生のポリシーー「自動再生機能をオフにする」	No	Yes	No
自動再生のポリシーー「ボリューム以外のデバイスの自動再生を許可しない」	No	Yes	No
データの収集とプレビュービルドー「利用統計情報の許可」	Yes	No	No
データの収集とプレビュービルドー「フィードバックの通知を表示しない」	Yes	No	No
イベントログサービス（アプリケーション）ー「ログファイルの最大サイズ（KB）を指定する」	Yes	Yes	No

次に続く

表 1.2-1 セキュリティ脅威に対処するセキュリティ対策-IT セキュリティバージョン 2.0（前から続く）

セキュリティ対策	セキュリティ脅威への対処		
	[1]	[2]	[3]
イベントログサービス（セキュリティ）－「ログファイルの最大サイズ（KB）を指定する」	Yes	Yes	No
イベントログサービス（システム）－「ログファイルの最大サイズ（KB）を指定する」	Yes	Yes	No
エクスプローラー－「破損後のヒープ終了をオフにする」	No	Yes	No
ホームグループ－「コンピューターがホームグループに参加できないようにする」	Yes	No	No
OneDrive－「OneDrive をファイル記憶域として使用できないようにする」	Yes	No	No
OneDrive－「ドキュメントを既定で OneDrive に保存する」 (既定でローカルコンピューターにドキュメントを保存する)	Yes	No	No
リモートデスクトップ接続のクライアント－「パスワードの保存を許可しない」	Yes	No	No
デバイスとリソースのリダイレクト－「ドライブのリダイレクトを許可しない」	Yes	No	No
セキュリティ－「接続するたびにパスワードを要求する」	Yes	No	No
セキュリティ－「セキュリティで保護された RPC 通信を要求する」	Yes	No	No
セキュリティ－「リモート接続にネットワークレベル認証を使用したユーザー認証を必要とする」	Yes	No	No
セッションの時間制限－「アクティブでアイドル状態になっているリモートデスクトップサービスセッションの制限時間を設定する」	Yes	No	No
PC 設定の同期－「アプリを同期しない」	Yes	No	No
PC 設定の同期－「スタート設定を同期しない」	Yes	No	No
Windows エラー報告－「OS が生成するエラー報告のためにメモリダンプを自動送信する」を無効に設定する	Yes	No	No
Windows ログオンのオプション－「システムによる再起動後に自動的に前回の対話ユーザーでサインインする」を無効に設定する	No	Yes	No
通知－「ロック画面のトースト通知をオフにする」	No	Yes	No
ビルトイン Administrator アカウントの無効化またはユーザー名変更	Yes	Yes	No
BIOS による HDD パスワード機能	No	No	Yes

表 1.2-2 セキュリティ脅威に対処するセキュリティ対策-IT セキュリティバージョン 1.0

セキュリティ対策	セキュリティ脅威への対処		
	[1]	[2]	[3]
アクセスコントロール	Yes	Yes	No
パーソナルファイアウォールチューニング	Yes	No	No
不要な Windows サービスの停止	Yes	No	No
ビルトイン Administrator アカウントの無効化またはユーザー名変更	Yes	Yes	No
直前のログオンユーザー名の非表示	Yes	Yes	No
ソフトウェア制限ポリシーの適用	Yes	Yes	No
AutoRun の制限の適用	No	Yes	No
StorageDevicePolicies 機能の適用	No	Yes	Yes
USB ストレージデバイスの無効化	No	Yes	Yes

次に続く

表 1.2-2 セキュリティ脅威に対処するセキュリティ対策-IT セキュリティバージョン 1.0（前から続く）

セキュリティ対策	セキュリティ脅威への対処		
	[1]	[2]	[3]
NetBIOS over TCP/IP の無効化	Yes	No	No
LAN Manager の認証レベルの変更	Yes	No	No
パスワードポリシーの適用	Yes	Yes	No
監査ポリシーの適用	Yes	Yes	No
アカウントロックアウトポリシーの適用	Yes	Yes	No
BIOS による HDD パスワード機能	No	No	Yes

2. セキュリティモデル

本製品では、システム構成や運用に対して柔軟に対応するために、要求されるセキュリティ強度に応じて、従来モデル、標準モデル、強固モデルの3種類のセキュリティモデルを提供します。セキュリティモデルには、必要なセキュリティ対策の項目が組み込まれています。

2.1 セキュリティモデルの概要

ここではセキュリティモデルの特徴、セキュリティモデルと対応するセキュリティ対策との関係について説明します。

■ セキュリティモデルの特徴

セキュリティモデルの従来モデル、標準モデル、強固モデルのそれぞれの特徴を説明します。

- ・ 従来モデル
セキュリティを強化しないモデル。セキュリティ対策が行われていない当社製品と接続する場合、このモデルを使用します。
- ・ 標準モデル
本製品の運用や他システム（Exaopc、ProSafe-RS など）との連携を重視して、「ネットワーク経由の攻撃」、「HIS やシステム生成機能を搭載したコンピュータを操作しての直接攻撃」に対処できるようにしたモデル。「HIS やシステム生成機能を搭載したコンピュータやデータの盗難」への対処に関しては、本製品の性格上、脅威が低いと考えられるので、標準モデルでは対応していません。
- ・ 強固モデル
セキュリティ脅威に対してすべて対策を行うモデル。すべてのセキュリティ対策を行うと、運用などに影響が発生する可能性があります。必須項目以外は、各システムの性格に合わせて対策を講じてください。

重要 強固モデルを使用する場合は、当社にご相談ください。

■ セキュリティモデルとセキュリティ対策

CENTUM VP のセキュリティ対策として、IT セキュリティツールが提供されます。IT セキュリティツールでは、各コンピュータごとにセキュリティ対策を実施できます。

ドメイン環境下で統合したセキュリティ対策を実施したい場合は、当社が提供するグループポリシーオブジェクト（以降、本章では GPO と呼びます）を併せて利用できます。

重要 GPO ファイルによるセキュリティ対策を行う場合でも、事前に IT セキュリティツールでセキュリティの設定を行っておく必要があります。また、GPO ファイルによるセキュリティの設定は、IT セキュリティツールでのセキュリティ設定よりも優先されます。

IT セキュリティツールを使用したセキュリティの設定では、IT セキュリティツールのバージョンの違い、セキュリティモデルの違いによって、設定が異なるセキュリティ対策項目があります。また、IT セキュリティバージョン 2.0 では、セキュリティ脅威に対処する目的以外に、製品の仕様を整合させるために設定するセキュリティ対策項目があります。

参照 セキュリティ対策については、以下を参照してください。

「3. セキュリティ対策の詳細」ページ 3-1

GPO ファイルの作成については、以下を参照してください。

「6.9.1 グループポリシーオブジェクトを作成する」ページ 6-30

GPO ファイルの適用については、以下を参照してください。

「6.9.2 組織単位にグループポリシーオブジェクトを適用する」ページ 6-32

● セキュリティ脅威に対応するためのセキュリティ対策

IT セキュリティバージョン 2.0 における、セキュリティ脅威に対応するためのセキュリティ対策項目と設定を次の表に示します。

GPO ファイルでの設定欄の「設定あり／設定なし」は、各セキュリティ対策項目に対して、当社が提供しているグループポリシーに基づいて作成した GPO ファイルで設定されるか否かを表しています。

- ・ 設定あり
当社が採用したセキュリティ対策が、GPO ファイルに定義されています。
- ・ 設定なし
そのセキュリティ対策項目に対しては、GPO ファイルに定義されていません。

IT セキュリティツールでの設定欄の「適用する／適用しない」は、各セキュリティ対策項目に対して IT セキュリティツールで設定されるか否かを、セキュリティモデルごとに表しています。

- ・ 適用する
当社が採用したセキュリティ対策が、IT セキュリティツールで設定されます。
- ・ 適用しない
当社が採用しないと判断したセキュリティ対策のため、IT セキュリティツールでは設定されません。

補足

IT セキュリティツールで提供されるセキュリティ対策項目には、その設定値をユーザが変更できる項目と変更できない項目があります。変更できる項目については、付録を参照してください。

表 2.1-1 IT セキュリティバージョン 2.0 におけるセキュリティ対策

セキュリティ対策	GPO ファイルでの設定	IT セキュリティツールでの設定	
		標準モデルの場合	強固モデルの場合
パスワードのポリシー「パスワードの長さ」	設定あり	適用しない	適用する
パスワードのポリシー「パスワードの変更禁止期間」	設定あり	適用しない	適用する
パスワードのポリシー「パスワードの有効期間」	設定あり	適用しない	適用する
パスワードのポリシー「パスワードの履歴を記録する」	設定あり	適用しない	適用する
パスワードのポリシー「暗号化を元に戻せる状態でパスワードを保存する」を無効に設定する	設定あり	適用しない	適用する
パスワードのポリシー「複雑さの要件を満たす必要があるパスワード」	設定あり	適用しない	適用する
ファイル/フォルダのアクセスコントロール (*1)	設定なし	適用する	適用する
製品のレジストリのアクセスコントロール (*1)	設定なし	適用する	適用する
DCOM(OPC)のアクセスコントロール (*1)	設定なし	適用する	適用する
パーソナルファイアウォールのチューニング (*2)	設定なし	適用する	適用する
パーソナルファイアウォール「ユニキャスト応答の許可」を無効に設定する (*3)	設定なし	適用する	適用する
不要な Windows サービスの停止 (*2)	設定なし	適用しない	適用する
アカウントロックアウトのポリシー「アカウントのロックアウトのしきい値」	設定あり	適用しない	適用する
アカウントロックアウトのポリシー「ロックアウトカウンターのリセット」	設定あり	適用しない	適用する
アカウントロックアウトのポリシー「ロックアウト期間」	設定あり	適用しない	適用する
NetBIOS over TCP/IP の無効化 (*1)	設定なし	適用する (*4)	適用する (*4)
StorageDevicePolicies 機能の適用	設定あり	適用する	適用する

次に続く

表 2.1-1 IT セキュリティバージョン 2.0 におけるセキュリティ対策（前から続く）

セキュリティ対策	GPO ファイル での設定	IT セキュリティツールでの設定	
		標準モデルの場合	強固モデルの場合
USB ストレージデバイスの無効化	設定あり	適用する	適用する
ソフトウェア制限ポリシーの適用	設定なし	適用する	適用する
ユーザー権利の割り当てー「ネットワーク経由でのアクセス」	設定なし	適用する (*5) (*6)	適用する (*5) (*6)
ユーザー権利の割り当てー「ドメインにワークステーションを追加」	設定なし	適用する (*5)	適用する (*5)
ユーザー権利の割り当てー「ローカルログオンを許可」	設定なし	適用する (*6)	適用する
ユーザー権利の割り当てー「ローカルログオンを拒否」	設定なし	適用する	適用する
セキュリティオプションー「監査：監査ポリシーサブカテゴリの設定（Windows Vista 以降）を強制して、監査ポリシーカテゴリの設定を上書きする」	設定あり	適用する	適用する
セキュリティオプションー「デバイス：ユーザーがプリンタードライバをインストールできないようにする」	設定あり	適用する	適用する
セキュリティオプションー「デバイス：CD-ROM へのアクセスを、ローカルログオンユーザーだけに制限する」	設定あり	適用する	適用する
セキュリティオプションー「デバイス：フロッピーへのアクセスを、ローカルログオンユーザーだけに制限する」	設定あり	適用する	適用する
セキュリティオプションー「ドメインコントローラー：Server Operators がタスクのスケジュールを割り当てるのを許可する」を無効に設定する	設定なし	適用する (*5)	適用する (*5)
セキュリティオプションー「ドメインコントローラー：コンピューターアカウントのパスワードの変更を拒否する」を無効に設定する	設定なし	適用する (*5)	適用する (*5)
セキュリティオプションー「ドメインメンバー：強力な（Windows 2000 かそれ以降のバージョン）セッションキーを必要とする」	設定あり	適用する	適用する
セキュリティオプションー「対話型ログオン：セッションがロックされているときにユーザーの情報を表示する」をユーザー情報は表示しないに設定する	設定あり	適用しない	適用する
セキュリティオプションー「対話型ログオン：最後のユーザー名を表示しない」	設定あり	適用する	適用する
セキュリティオプションー「対話型ログオン：Ctrl + Alt + Del を必要としない」を無効に設定する	設定あり	適用する	適用する
セキュリティオプションー「対話型ログオン：コンピューターの非アクティブ状態の上限」	設定なし	適用する (*6)	適用する (*6)
セキュリティオプションー「対話型ログオン：パスワードが無効になる前にユーザーに変更を促す」	設定あり	適用する	適用する
セキュリティオプションー「Microsoft ネットワークサーバー：クライアントが同意すれば、通信にデジタル署名を行う」	設定あり	適用する	適用する
セキュリティオプションー「Microsoft ネットワークサーバー：サーバー SPN ターゲット名検証レベル」	設定あり	適用する	適用する
「MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)」	設定なし	適用する	適用する
「MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)」を無効に設定する	設定なし	適用する	適用する
「MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)」	設定なし	適用する	適用する

次に続く

表 2.1-1 IT セキュリティバージョン 2.0 におけるセキュリティ対策（前から続く）

セキュリティ対策	GPO ファイル での設定	IT セキュリティツールでの設定	
		標準モデルの場合	強固モデルの場合
セキュリティオプション「ネットワークアクセス：SAM アカウントの匿名の列挙を許可しない」	設定あり	適用する	適用する
セキュリティオプション「ネットワークアクセス：SAM アカウントおよび共有の匿名の列挙を許可しない」	設定あり	適用する	適用する
セキュリティオプション「ネットワークアクセス：ネットワーク認証のためにパスワードおよび資格情報を保存することを許可しない」	設定あり	適用する	適用する
セキュリティオプション「ネットワークセキュリティ：NTLM で Local System によるコンピューター ID の使用を許可する」	設定あり	適用する	適用する
セキュリティオプション「ネットワークセキュリティ：Local System による NULL セッションフォールバックを許可する」を無効に設定する	設定あり	適用する	適用する
セキュリティオプション「ネットワークセキュリティ：ログオン時間を経過した場合はユーザを強制的にログオフさせる」	設定なし	適用する (*5)	適用する (*5)
セキュリティオプション「ネットワークセキュリティ：LAN Manager 認証レベル」	設定あり	適用する	適用する
セキュリティオプション「ネットワークセキュリティ：NTLM SSP ベース（セキュア RPC を含む）のクライアント向け最小セッションセキュリティ」	設定あり	適用する	適用する
セキュリティオプション「ネットワークセキュリティ：NTLM SSP ベース（セキュア RPC を含む）のサーバー向け最小セッションセキュリティ」	設定あり	適用する	適用する
セキュリティオプション「シャットダウン：システムのシャットダウンにログオンを必要としない」を無効に設定する	設定あり	適用する	適用する
セキュリティオプション「ユーザーアカウント制御：ビルトイン Administrator アカウントのための管理者承認モード」	設定あり	適用する	適用する
セキュリティオプション「ユーザーアカウント制御：管理者承認モードでの管理者に対する昇格時のプロンプトの動作」	設定あり	適用する	適用する
監査ポリシーの詳細な構成「資格情報の確認の監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成「コンピューターアカウントの管理の監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成「その他のアカウント管理イベントの監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成「セキュリティグループの管理の監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成「ユーザーアカウントの管理の監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成「プロセス作成の監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成「ディレクトリサービスのアクセス」	設定なし	適用する (*5)	適用する (*5)
監査ポリシーの詳細な構成「ディレクトリサービスの変更の監査」	設定なし	適用する (*5)	適用する (*5)
監査ポリシーの詳細な構成「アカウントロックアウトの監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成「ログオフの監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成「ログオンの監査」	設定あり	適用する	適用する

次に続く

表 2.1-1 IT セキュリティバージョン 2.0 におけるセキュリティ対策（前から続く）

セキュリティ対策	GPO ファイル での設定	IT セキュリティツールでの設定	
		標準モデルの場合	強固モデルの場合
監査ポリシーの詳細な構成－「その他のログオン／ログオフイベントの監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成－「特殊なログオンの監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成－「リムーバブル記憶域の監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成－「監査ポリシーの変更の監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成－「認証ポリシーの変更の監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成－「フィルタリングプラットフォームポリシーの変更の監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成－「MPSSVC ルールレベルポリシーの変更の監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成－「その他のポリシー変更イベントの監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成－「重要な特権の使用の監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成－「IPsec ドライバー」	設定なし	適用する (*5)	適用する (*5)
監査ポリシーの詳細な構成－「その他のシステムイベントの監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成－「セキュリティ状態の変更の監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成－「セキュリティシステムの拡張の監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成－「システムの整合性の監査」	設定あり	適用する	適用する
個人用設定－「ロック画面カメラを有効にできないようにする」	設定あり	適用する	適用する
個人用設定－「ロック画面スライドショーを有効にできないようにする」	設定あり	適用する	適用する
WLAN 設定－「推奨されるオープンホットスポット、連絡先によって共有されたネットワーク、有料サービスを提供するホットスポットに Windows が自動的に接続することを許可する」(*7)	設定あり	適用する	適用する
SCM－「Enable LSA Protection」(*7)	設定あり	適用しない	適用する
SCM－「Lsass.exe audit mode」(*7)	設定あり	適用しない	適用する
グループポリシー－「レジストリポリシーの処理を構成する」	設定あり	適用する	適用する
インターネット通信の設定－「プリンタードライバーの HTTP 経由でのダウンロードをオフにする」	設定あり	適用する	適用する
インターネット通信の設定－「イベントビューアーの 'Event.asp' リンクをオフにする」	設定あり	適用する	適用する
インターネット通信の設定－「Web 発行およびオンライン注文ウィザードのインターネットダウンロードをオフにする」	設定あり	適用する	適用する
インターネット通信の設定－「HTTP 経由の印刷をオフにする」	設定あり	適用する	適用する
インターネット通信の設定－「検索コンパニオンの内容ファイルの更新をオフにする」	設定あり	適用する	適用する
インターネット通信の設定－「ファイルおよびフォルダーの 'Web に発行' タスクをオフにする」	設定あり	適用する	適用する
インターネット通信の設定－「Windows カスタマーエクスペリエンス向上プログラムをオフにする」	設定あり	適用する	適用する

次に続く

表 2.1-1 IT セキュリティバージョン 2.0 におけるセキュリティ対策（前から続く）

セキュリティ対策	GPO ファイル での設定	IT セキュリティツールでの設定	
		標準モデルの場 合	強固モデルの場 合
インターネット通信の設定－「Windows Messenger カスタマーエクスペリエンス向上プログラムをオフにする」	設定あり	適用する	適用する
ログオン－「ネットワークの選択の UI を表示しない」	設定あり	適用する	適用する
ログオン－「ドメインに参加しているコンピューターに接続しているユーザーを列挙しない」	設定あり	適用する	適用する
ログオン－「レガシの実行の一覧を処理しない」	設定あり	適用しない	適用する
ログオン－「一度だけ実行するコマンドの一覧を処理しない」	設定あり	適用しない	適用する
ログオン－「ドメインに参加しているコンピューターのローカルユーザーを列挙する」を無効に設定する	設定あり	適用する	適用する
ログオン－「ロック画面のアプリ通知をオフにする」	設定あり	適用する	適用する
軽減策オプション－「信頼されていないフォントのブロック」	設定あり	適用する	適用する
リモートプロシージャコール－「RPC エンドポイントマッパークライアント認証を有効にする」	設定あり	適用しない	適用する
ユーザープロファイル－「広告 ID を無効にする」	設定あり	適用する	適用する
アプリのプライバシー－「Windows アプリでアカウント情報にアクセスする」	設定あり	適用する	適用する
アプリのプライバシー－「Windows アプリで通話履歴にアクセスする」	設定あり	適用する	適用する
アプリのプライバシー－「Windows アプリで連絡先にアクセスする」	設定あり	適用する	適用する
アプリのプライバシー－「Windows アプリでメールにアクセスする」	設定あり	適用する	適用する
アプリのプライバシー－「Windows アプリで位置情報にアクセスする」	設定あり	適用する	適用する
アプリのプライバシー－「Windows アプリでメッセージングにアクセスする」	設定あり	適用する	適用する
アプリのプライバシー－「Windows アプリでモーションにアクセスする」	設定あり	適用する	適用する
アプリのプライバシー－「Windows アプリでカレンダーにアクセスする」	設定あり	適用する	適用する
アプリのプライバシー－「Windows アプリでカメラにアクセスする」	設定あり	適用する	適用する
アプリのプライバシー－「Windows アプリでマイクにアクセスする」	設定あり	適用する	適用する
アプリのプライバシー－「Windows アプリで信頼済みデバイスにアクセスする」	設定あり	適用する	適用する
アプリのプライバシー－「Windows アプリで無線を制御する」	設定あり	適用する	適用する
アプリのプライバシー－「Windows アプリでデバイスと同期する」	設定あり	適用する	適用する
アプリ実行時－「ホストされているコンテンツから Windows ランタイム API でアクセスする Windows ストアアプリを起動できないようにする」	設定あり	適用する	適用する
自動再生のポリシー－「自動再生機能をオフにする」	設定あり	適用する	適用する
自動再生のポリシー－「ボリューム以外のデバイスの自動再生を許可しない」	設定あり	適用する	適用する
データの収集とプレビュービルド－「利用統計情報の許可」	設定あり	適用する	適用する

次に続く

表 2.1-1 IT セキュリティバージョン 2.0 におけるセキュリティ対策（前から続く）

セキュリティ対策	GPO ファイル での設定	IT セキュリティツールでの設定	
		標準モデルの場合	強固モデルの場合
データの収集とプレビュービルド – 「フィードバックの通知を表示しない」	設定あり	適用する	適用する
イベントログサービス（アプリケーション） – 「ログファイルの最大サイズ（KB）を指定する」	設定あり	適用する	適用する
イベントログサービス（セキュリティ） – 「ログファイルの最大サイズ（KB）を指定する」	設定あり	適用する	適用する
イベントログサービス（システム） – 「ログファイルの最大サイズ（KB）を指定する」	設定あり	適用する	適用する
エクスプローラー – 「破損後のヒープ終了をオフにする」	設定あり	適用する	適用する
ホームグループ – 「コンピューターがホームグループに参加できないようにする」	設定あり	適用する	適用する
OneDrive – 「OneDrive をファイル記憶域として使用できないようにする」	設定あり	適用する	適用する
OneDrive – 「ドキュメントを既定で OneDrive に保存する」（既定でローカルコンピューターにドキュメントを保存する）	設定あり	適用する	適用する
リモートデスクトップ接続のクライアント – 「パスワードの保存を許可しない」	設定あり	適用する	適用する
デバイスとリソースのリダイレクト – 「ドライブのリダイレクトを許可しない」 (*3)	設定あり (*8)	適用する	適用する
セキュリティ – 「接続するたびにパスワードを要求する」	設定なし	適用する (*6)	適用する (*6)
セキュリティ – 「セキュリティで保護された RPC 通信を要求する」	設定あり	適用する	適用する
セキュリティ – 「リモート接続にネットワークレベル認証を使用したユーザー認証を必要とする」	設定あり	適用する	適用する
セッションの時間制限 – 「アクティブでアイドル状態になっているリモートデスクトップサービスセッションの制限時間を設定する」	設定なし	適用する (*6)	適用する (*6)
PC 設定の同期 – 「アプリを同期しない」	設定あり	適用する	適用する
PC 設定の同期 – 「スタート設定を同期しない」	設定あり	適用する	適用する
Windows エラー報告 – 「OS が生成するエラー報告のためにメモリダンプを自動送信する」を無効に設定する	設定あり	適用する	適用する
Windows ログオンのオプション – 「システムによる再起動後に自動的に前回の対話ユーザーでサインインする」を無効に設定する	設定あり	適用する	適用する
通知 – 「ロック画面のトースト通知をオフにする」	設定あり	適用する	適用する
ビルトイン Administrator アカウントの無効化またはユーザー名変更	設定なし	適用しない	IT セキュリティツールでは設定できません。手動で設定してください。
BIOS による HDD パスワード機能 (*1)	設定なし	適用しない	IT セキュリティツールでは設定できません。手動で設定してください。

*1: グループポリシーの影響を受けません。

*2: グループポリシーで制御可能ですが、IT セキュリティツールでは、個別に設定します。

*3: UGS では設定しません。

*4: ネットワーク接続名称が「UACSEthernet」の場合、セキュリティモデル、およびユーザ管理に関係なく NetBIOS over TCP/IP の無効化を設定します。

- *5: ドメインコントローラで設定します。
- *6: UACS ステーションで設定します。
- *7: Active Directory を使用した統合管理で設定値を変更する場合、この項目は、「有効」もしくは「無効」のいずれかを選択してください。
- *8: Active Directory を使用した統合管理のために提供する、UGS 用の YOKOGAWA GPO ファイルには、この項目はありません。

補足

IT セキュリティバージョン 2.0 では、各ステーションや、ファイルサーバ、ドメインコントローラによるセキュリティ設定項目が異なります。

● 製品の仕様に整合させるためのセキュリティ対策

IT セキュリティバージョン 2.0 における、製品の仕様に整合させるためのセキュリティ対策項目と設定を次の表に示します。

GPO ファイルでの設定欄の「設定あり／設定なし」は、各セキュリティ対策項目に対して、当社が提供しているグループポリシーに基づいて作成した GPO ファイルで設定されるか否かを表しています。

- ・ 設定あり
当社が採用したセキュリティ対策が、GPO ファイルに定義されています。
- ・ 設定なし
そのセキュリティ対策項目に対しては、GPO ファイルに定義されていません。

IT セキュリティツールでの設定欄の「適用する／適用しない」は、各セキュリティ対策項目に対して IT セキュリティツールで設定されるか否かを、セキュリティモデルごとに表しています。

- ・ 適用する
当社が採用したセキュリティ対策が、IT セキュリティツールで設定されます。
- ・ 適用しない
当社が採用しないと判断したセキュリティ対策のため、IT セキュリティツールでは設定されません。

表 2.1-2 IT セキュリティバージョン 2.0 における製品の仕様に整合させるために設定するセキュリティ対策

セキュリティ対策	GPO ファイルでの設定	IT セキュリティツールでの設定	
		標準モデルの場合	強固モデルの場合
ユーザー権利の割り当てー「グローバルオブジェクトの作成」	設定なし	適用する	適用する
ユーザー権利の割り当てー「バッチジョブとしてログオン」	設定なし	適用する	適用する
ユーザー権利の割り当てー「サービスとしてログオン」	設定なし	適用する	適用する
「MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments)」	設定なし	適用する	適用する
セキュリティオプションー「ネットワークアクセス：Everyone のアクセス許可を匿名ユーザーに適用する」	設定なし	適用する	適用する
セキュリティオプションー「ネットワークセキュリティ：次回のパスワード変更時に LAN Manager のハッシュ値を保存しない」	設定なし	適用する	適用する
監査ポリシーの詳細な構成ー「RPC イベントの監査」	設定あり	適用する	適用する
監査ポリシーの詳細な構成ー「生成されたアプリケーションの監査」	設定あり	適用する	適用する
プロセス作成の監査ー「プロセス作成イベントにコマンドラインを含める」を無効に設定する	設定あり	適用する	適用する
インターネット通信の設定ー「ストアへのアクセスをオフにする」	設定あり	適用する	適用する

次に続く

表 2.1-2 IT セキュリティバージョン 2.0 における製品の仕様に整合させるために設定するセキュリティ対策 (前から続く)

セキュリティ対策	GPO ファイルでの設定	IT セキュリティツールでの設定	
		標準モデルの場合	強固モデルの場合
ビデオとディスプレイの設定ー「ディスプレイをオフにする (バッテリー使用時)」	設定あり	適用する (*1)	適用する (*1)
ビデオとディスプレイの設定ー「ディスプレイをオフにする (電源接続時)」	設定あり	適用する (*1)	適用する (*1)
クラウドコンテンツー「Windows のヒントを表示しない」	設定あり	適用する	適用する
クラウドコンテンツー「Microsoft コンシューマーエクスペリエンスを無効にする」	設定あり	適用する	適用する
データの収集とプレビュービルドー「プレリリースの機能または設定を無効にする」	設定あり	適用する	適用する
データの収集とプレビュービルドー「Insider ビルドに関するユーザーコントロールの切り替え」	設定あり	適用する	適用する
検索ー「Cortana を許可する」を無効に設定する	設定あり	適用する	適用する
検索ー「Web を検索したり [検索] に Web の検索結果を表示したりしない」	設定あり	適用する	適用する
検索ー「従量制課金接続を使用して Web を検索したり [検索] に Web の検索結果を表示したりしない」	設定あり	適用する	適用する
ソフトウェア保護プラットフォームー「KMS クライアントオンライン AVS 検証を無効にする」	設定あり	適用する	適用する
ストアー「更新プログラムの自動ダウンロードおよび自動インストールをオフにする」	設定あり	適用する	適用する
ストアー「Windows 8 コンピューターでの更新プログラムの自動ダウンロードをオフにする」	設定あり	適用する	適用する
ストアー「最新バージョンの Windows への更新プログラム提供をオフにする」	設定あり	適用する	適用する
ストアー「ストアアプリケーションをオフにする」	設定あり	適用する	適用する
Endpoint Protectionー「Endpoint Protection を無効にする」	設定あり	適用する	適用する

*1: UACS ステーションでは、未定義に設定します。

● セキュリティ脅威に対応するためのセキュリティ対策

IT セキュリティバージョン 1.0 における、セキュリティ脅威に対応するためのセキュリティ対策項目と設定を次の表に示します。

GPO ファイルでの設定欄の「設定あり／設定なし」は、各セキュリティ対策項目に対して、当社が提供しているグループポリシーに基づいて作成した GPO ファイルで設定されるか否かを表しています。

- ・ 設定あり
当社が採用したセキュリティ対策が、GPO ファイルに定義されています。
- ・ 設定なし
そのセキュリティ対策項目に対しては、GPO ファイルに定義されていません。

IT セキュリティツールでの設定欄の「適用する／適用しない」は、各セキュリティ対策項目に対して IT セキュリティツールで設定されるか否かを、セキュリティモデルごとに表しています。

- ・ 適用する
当社が採用したセキュリティ対策が、IT セキュリティツールで設定されます。
- ・ 適用しない
当社が採用しないと判断したセキュリティ対策のため、IT セキュリティツールでは設定されません。

補足

IT セキュリティツールで提供されるセキュリティ対策項目には、その設定値をユーザが変更できる項目と変更できない項目があります。変更できる項目については、付録を参照してください。

表 2.1-3 IT セキュリティバージョン 1.0 におけるセキュリティ対策

セキュリティ対策	GPO ファイルでの設定	IT セキュリティツールでの設定		
		従来モデル	標準モデル	強固モデル
アクセスコントロール (*1)	設定なし	適用しない	適用する	適用する
パーソナルファイアウォールのチューニング	設定なし	適用しない	適用する	適用する
不要な Windows サービスの停止	設定なし	適用しない	適用しない	適用する
ビルトイン Administrator アカウントの無効化またはユーザー名変更	設定なし	適用しない	適用しない	IT セキュリティツールでは設定できません。手動で設定してください。
直前のログオンユーザー名の非表示	設定あり	適用する	適用する	適用する
ソフトウェア制限ポリシーの適用	設定なし	適用しない	適用する	適用する
AutoRun の制限の適用	設定あり	適用する	適用する	適用する
StorageDevicePolicies 機能の適用	設定あり	適用しない	適用する	適用する
USB ストレージデバイスの無効化	設定あり	適用しない	適用する	適用する
NetBIOS over TCP/IP の無効化	設定なし	適用しない (*2)	適用する (*2)	適用する (*2)
LAN Manager の認証レベルの変更	設定あり	適用しない	適用する	適用する
パスワードポリシーの適用	設定あり	適用しない	適用しない	適用する
監査ポリシーの適用	設定あり	適用しない	適用しない	適用する
アカウントロックアウトポリシーの適用	設定あり	適用しない	適用しない	適用する
BIOS による HDD パスワード機能 (*1)	設定なし	適用しない	適用しない	IT セキュリティツールでは設定できません。手動で設定してください。

*1: グループポリシーの影響を受けません。

*2: ネットワーク接続名称が「UACSEthernet」の場合、セキュリティモデル、およびユーザ管理に関係なく NetBIOS over TCP/IP の無効化を設定します。

2.2 ユーザ／グループの管理

ここでは、Windows のユーザ管理と本製品との関係について、説明します。アクセスコントロールは、ここで説明するユーザ／グループ単位で設定します。

2.2.1 ユーザ管理の種類

Windows には、ユーザを管理する方法として、スタンドアロン管理とドメイン管理の 2 つの方法があります。

本製品では、スタンドアロン管理とドメイン管理を併用する、併用管理というユーザ管理の方法もあります。

表 2.2.1-1 ユーザ管理方法

ユーザ管理の種類	必要な構成	運用	特徴
スタンドアロン管理	本製品で構築されたシステムのための構成	すべての HIS やシステム生成機能を搭載した PC 単位で利用ユーザアカウントを登録して運用します。	<ul style="list-style-type: none"> ドメインコントローラが不要なシンプルな構成です。 PC 単位のアカウント管理が必要になるので、ユーザアカウントのメンテナンス時は全 PC のメンテナンスが必要になり、大規模システムには不向きです。 PC の管理者権限と本製品のメンテナンス権限の分離ができません。
ドメイン管理	本製品で構築されたシステム以外にドメインコントローラの構築が必要	ドメインコントローラへ利用ユーザのアカウントを登録し、運用します。	<ul style="list-style-type: none"> ユーザの一元管理ができ、人為的なミスを軽減できます。 PC の管理者権限と本製品のメンテナンス権限の分離ができます。
併用管理	本製品で構築されたシステム以外にドメインコントローラの構築が必要	通常運用は、ドメイン管理と同様に運用します。	<ul style="list-style-type: none"> ドメインコントローラが利用不能な場合でも、PC 単位でのアカウント管理を行うことで、継続して運用が可能です。 PC の管理者権限と本製品のメンテナンス権限の分離ができません。

補足

併用管理は、通常、ドメイン管理でユーザを管理します。必要なときにはスタンドアロン管理でユーザを管理できます。例として、次のようなケースです。

通常はドメイン管理を利用して中央の管理部門がユーザ作成の管理を行っています。しかし、現場の責任者が、任意のユーザに対して権限が設定できる特定の PC を設置したいときに、併用管理でユーザを管理します。

2.2.2 CENTUM VP のユーザ認証モード

CENTUM VP のユーザ認証には、Windows 認証モードと CENTUM 認証モードの 2 つがあります。これらを総称して、ユーザ認証モードと言います。

- ・ Windows 認証モード
ユーザ認証を Windows 機能で行う方法です。
- ・ CENTUM 認証モード
ユーザ認証を CENTUM VP 独自の機能で行う方法です。

重要 セキュリティモデルが標準モデル、および強固モデルのいずれかの場合だけ、Windows 認証モードは使用できます。

ユーザ認証を必要とする CENTUM VP のユーザを次の 2 つに分類します。

- ・ HIS グループユーザ
操作監視機能を利用するユーザです。ユーザは、セキュリティビルダで登録します。
- ・ 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 対応パッケージをインストール時に登録されるシステムエンジニア、処方エンジニアおよび帳票ユーザの総称。ユーザとユーザを管理するビルダについて、次に示します。

表 2.2.2-1 ユーザとユーザを管理するビルダ

ユーザ		ユーザを管理するビルダ		説明
HIS グループユーザ		セキュリティビルダ		操作監視機能を利用するユーザ
ENG グループユーザ	システムエンジニア	ENG グループユーザ登録ビルダ (*1)	システムエンジニアのエンジニア登録ビルダ	システムビューや、システムビューから起動される各種ビルダでエンジニアリングするエンジニア
	処方エンジニア		処方エンジニアのエンジニア登録ビルダ	処方機能を利用するエンジニア
	帳票ユーザ		帳票ユーザのユーザ登録ビルダ	帳票機能を利用するユーザ

*1: 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および帳票ユーザのユーザ登録ビルダの総称。

ユーザ認証モードが Windows 認証モードの場合、操作監視機能やビルダを操作するときの認証機能が Windows ユーザを使用した認証になります。

ユーザ認証モードは、次の単位で設定します。

- ・ HIS グループユーザ：プロジェクト単位（複数プロジェクト結合の場合もプロジェクト単位）
- ・ ENG グループユーザ：エンジニア登録ファイル、ユーザ登録ファイル単位

■ ユーザ認証モードを設定する際の注意事項

ユーザ管理とパスワードを CENTUM VP システムで統一するために、次の設定としてください。

- ・ 同一プロジェクト内で R4.02 以前の HIS が混在する場合は、プロジェクトを CENTUM 認証モードとしてください。
- ・ Windows 認証モード時のユーザ管理は、ドメイン管理（併用管理）かスタンドアロン管理かどちらかに統一してください。

- ・ 1 つまたは複数のプロジェクトが連携できる Windows ドメインは 1 つです。
(Windows ドメイン：プロジェクト = 1 : N)

■ HIS グループユーザのユーザ認証

HIS グループユーザの場合、ユーザ認証モードの影響範囲はプロジェクト単位です。

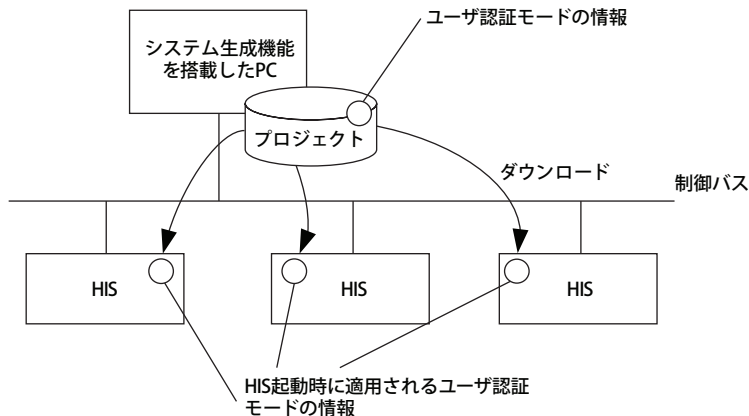


図 2.2.2-1 ユーザ認証モードの影響範囲 (HIS グループユーザ)

ユーザ認証モードは、システムビューのプロジェクトプロパティで設定します。設定後にダウンロードが必要です。ダウンロードしたユーザ認証モード (CENTUM 認証モードまたは Windows 認証モード) の情報は、次のように使用されます。

- ・ HIS のセキュリティモデルが標準モデルのとき、HIS に記憶され、次回の HIS 起動時にダウンロードされたユーザ認証モードが反映されます。
- ・ HIS のセキュリティモデルが標準モデルの場合、操作監視機能が動作している現在のユーザ認証モードと異なっていると、システムアラームが発生します。HIS の再起動でユーザ認証モードが変わります。
- ・ HIS のセキュリティモデルが従来モデルの場合、ダウンロードしたユーザ認証モードが Windows 認証モードになっていると、システムアラームが発生します。HIS の再起動をしても、CENTUM 認証モードのままです。この場合は IT セキュリティツールを使って、HIS のセキュリティモデルを標準モデルにするか、CENTUM 認証モードに戻してください。

重要

HIS が再起動するまでは、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、ダウンロードされたものになります。ユーザを削除した場合、そのユーザは使用できません。

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 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。

● シングルサインオン

HIS グループユーザのユーザ認証モードが Windows 認証モードの場合、1 度のユーザ認証で HIS を利用可能にすることができます。これをシングルサインオンと言います。シングルサインオンには、次の 2 つがあります。

- ・ Windows タイプシングルサインオン
Windows ログオンダイアログでログオンすると、自動的に操作監視機能にユーザインします。他のユーザにユーザインすることで、ユーザを切り替えられます。ユーザアウトすると、Windows ログオンで使用したユーザに戻ります。

- ・ HIS タイプ シングルサインオン

PC を起動すると、Windows に OFFUSER（初期ユーザ）で自動的にログオンし、操作監視機能を起動します。この状態では、CENTUM デスクトップが適用されます。

補足

CENTUM 認証モードで操作監視機能にユーザインする場合、HIS グループユーザに共有利用目的の匿名ユーザを使用できます。Windows 認証モードでシングルサインオンすると、この匿名ユーザが排除されるため、オペレーションのトレーサビリティが向上し、セキュアな運用の促進効果があります。

■ ENG グループユーザのユーザ認証

ENG グループユーザの場合、ユーザ認証モードの影響範囲はエンジニア登録ファイルまたはユーザ登録ファイル単位です。

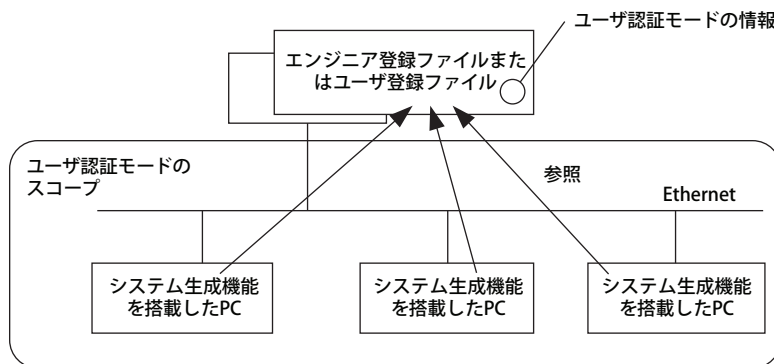


図 2.2.2-2 ユーザ認証モードの影響範囲（ENG グループユーザ）

ユーザ認証モードは、アクセス制限ユーティリティで設定します。
ユーザ認証モードの情報は即時反映され、ユーザ認証のタイミングで使われます。

2.2.3 ユーザとグループの管理

ユーザとグループについて説明します。

■ Windows のユーザ管理とセキュリティモデルの組み合わせ

Windows のユーザ管理と、セキュリティモデルの組み合わせで、4 つのユーザ／グループ作成タイプが存在します。

- ・ タイプ 1：従来モデル
- ・ タイプ 2：標準モデル／強固モデルースタンドアロン管理
- ・ タイプ 3：標準モデル／強固モデルードメイン管理
- ・ タイプ 4：標準モデル／強固モデルー併用管理

補足

IT セキュリティのセキュリティモデルに関係なく、CENTUM VP のインストーラで、CTM_MAINTENANCE が作成され、CENTUM VP のインストールユーザがメンバとして追加されます。
また、ユーザ管理がドメイン管理の場合や併用管理の場合は、ドメインの CTM_MAINTENANCE を利用してください。

重要

- ・ ユーザ／グループを作成するときに、CENTUM VP システムで予約されている次のグループ名を使用しないでください。
 - ・ CTM_HISIS
 - ・ ADS_SERVICE
 - ・ ADS_SERVICE_LCL
- ・ システム生成機能进行操作するためには、IT セキュリティの設定だけではなく、AD プロジェクトのセキュリティも設定してください。

参照

AD プロジェクトのセキュリティについては、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「C1.1.6 AD プロジェクトに対するアクセスコントロール」

● タイプ 1：従来モデル

IT セキュリティツールを実行すると、次の表に示されるユーザが自動で作成されます。

表 2.2.3-1 従来モデル

ユーザ名／グループ名	種別	作成場所	所属するグループ	説明
CENTUM	ユーザ	ローカル PC	Users	CS 3000 と同様に、システムをインストールすると作成されるユーザ。ただし、初期パスワードは、「Yokogawa1」で、初回ログオン時にパスワード変更を要求される。
CTM_PROCESS	ユーザ	ローカル PC	Users	CENTUM VP のプロセス (Windows サービス) を実行させるためのユーザで、Windows へのログオン権限はないユーザ。
UGS_PROCESS	ユーザ	ローカル PC	Administrators	CENTUM VP のプロセス (Windows サービス) を実行させるためのユーザで、Windows へのログオン権限はないユーザ。UGS にのみ作成され、UGS 関連のプロセスを実行する。

次に続く

表 2.2.3-1 従来モデル（前から続く）

ユーザ名／グループ名	種別	作成場所	所属するグループ	説明
LIC_PROCESS	ユーザ	ローカル PC	Users	ライセンス管理機能のプロセス (Windows サービス) を実行させるためのユーザで、Windows へのログオン権限はないユーザ。
ADS_PROCESS	ユーザ	ローカル PC	Users	オートメーションデザインサーバのプロセス (Windows サービス) を実行させるためのユーザで、Windows へのログオン権限はないユーザ。
RDC_PROCESS	ユーザ	ローカル PC	Users	コンピュータ切替型 UGS 機能用のプロセス (Windows サービス) を実行させるためのユーザで、Windows へのログオン権限はないユーザ。
PSF_PROCESS	ユーザ	ローカル PC	Users	エンジニアリングサーバ機能ライセンスがある場合に作成されるユーザで、プロジェクトのバックアップ時に使用される。
ADS_AGENT	ユーザ	ローカル PC	<ul style="list-style-type: none"> Users Performance Monitor Users 	ステーション情報の管理プロセスを実行するためのユーザで、Windows へのログオン権限はないユーザ。

重要

これらのユーザは、CENTUM VP の用途以外には使用しないでください。

参照

オートメーションデザインサーバについては、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「A. オートメーションデザインスイート概要」

● タイプ 2：標準モデル／強固モデルースタンドアロン管理

IT セキュリティツールを実行すると、次の表に示されるユーザ／グループが自動で作成されます。

表 2.2.3-2 標準モデル／強固モデルースタンドアロン管理

ユーザ名／グループ名	種別	作成場所	所属するグループ	説明
CTM_OPERATOR	グループ	ローカル PC	Users (*1)	オペレータ用ユーザのグループ。
CTM_ENGINEER	グループ	ローカル PC	Users (*1)	システムビューなどを使い、CENTUM VP のエンジニアリングを行うユーザのグループ。
CTM_ENGINEER_ADM	グループ	ローカル PC	Administrators (*1)	システムビューなどを使い、CENTUM VP のエンジニアリングを行うユーザのグループで、CTM_ENGINEER より強い権限を持ったグループ。
CTM_OPC	グループ	ローカル PC	Users (*1)	他プログラムが CENTUM VP と連携するために使用するグループ。たとえば、CENTUM VP と OPC 通信を行うときに使用される。
CTM_MAINTENANCE	グループ	ローカル PC	Administrators (*1)	システム構築時の SE やメンテナンス担当者など、CENTUM VP のメンテナンスを行うユーザのグループ。

次に続く

表 2.2.3-2 標準モデル／強固モデル—スタンドアロン管理（前から続く）

ユーザ名／グループ名	種別	作成場所	所属するグループ	説明
ADS_MANAGER	グループ	ローカル PC	Users(*1)	オートメーションデザインスイート管理ツールを使い、CENTUM VP のオートメーションデザインサーバの管理を行うためのグループ。
OFFUSER	ユーザ	ローカル PC	Users	Windows 認証モードの HIS タイプ シングルサインオンの自動ログオンに利用されるユーザ。Windows 環境の権限は、必要最低限の設定となる。
CTM_PROCESS	ユーザ	ローカル PC	Users	CENTUM VP のプロセス（Windows サービス）を実行させるためのユーザで、Windows へのログオン権限はないユーザ。
UGS_PROCESS	ユーザ	ローカル PC	Administrators	CENTUM VP のプロセス（Windows サービス）を実行させるためのユーザで、Windows へのログオン権限はないユーザ。UGS にのみ作成され、UGS 関連のプロセスを実行する。
LIC_PROCESS	ユーザ	ローカル PC	Users	ライセンス管理機能のプロセス（Windows サービス）を実行させるためのユーザで、Windows へのログオン権限はないユーザ。
ADS_PROCESS	ユーザ	ローカル PC	Users	オートメーションデザインサーバのプロセス（Windows サービス）を実行させるためのユーザで、Windows へのログオン権限はないユーザ。
RDC_PROCESS	ユーザ	ローカル PC	<ul style="list-style-type: none"> Users CTM_OPC 	コンピュータ切替型 UGS 機能用のプロセス（Windows サービス）を実行させるためのユーザで、Windows へのログオン権限はないユーザ。
PSF_PROCESS	ユーザ	ローカル PC	Users	エンジニアリングサーバ機能ライセンスがある場合に作成されるユーザで、プロジェクトのバックアップ時に使用される。
ADS_AGENT	ユーザ	ローカル PC	<ul style="list-style-type: none"> Users Performance Monitor Users CTM_OPC 	ステーション情報の管理プロセスを実行するためのユーザで、Windows へのログオン権限はないユーザ。

*1: 作成されるグループに所属するユーザは、[所属するグループ] 欄に記載のグループにも所属させてください。

重要

- これらのユーザとグループは、CENTUM VP の用途以外には使用しないでください。
- セキュリティモデルを変更した場合、確認なしで、既存ユーザグループが削除されたり、その名称が変更されたりすることがあります。

参照

オートメーションデザインサーバについては、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「A. オートメーションデザインスイート概要」

● タイプ 3：標準モデル／強固モデルードメイン管理

IT セキュリティツールを実行すると、次の表に示されるユーザ／グループが自動で作成されます。

表 2.2.3-3 標準モデル／強固モデルードメイン管理

ユーザ名／グループ名	種別	作成場所	所属するグループ	説明
CTM_OPERATOR	グループ	ドメインコントローラ	Domain Users (*1)	オペレータ用ユーザのグループ。
CTM_ENGINEER	グループ	ドメインコントローラ	Domain Users (*1)	システムビューなどを使い、CENTUM VP のエンジニアリングを行うユーザのグループ。
CTM_ENGINEER_ADM	グループ	ドメインコントローラ	Domain Admins (*1)	システムビューなどを使い、CENTUM VP のエンジニアリングを行うユーザのグループで、CTM_ENGINEER より強い権限を持ったグループ。
CTM_OPC	グループ	ドメインコントローラ	Domain Users (*1)	他プログラムが CENTUM VP と連携するために使用するグループ。たとえば、CENTUM VP と OPC 通信を行うときに使用される。
CTM_OPC_LCL	グループ	ローカル PC	Users (*1)	権限的には、CTM_OPC と同様で、EXA パッケージの組み込みユーザなど、ドメイン管理に対応できないユーザ向けの補助的なグループで通常の運用では利用しない。
CTM_MAINTENANCE	グループ	ドメインコントローラ	Domain Admins (*1)	システム構築時の SE やメンテナンス担当者など、CENTUM のメンテナンスを行うユーザのグループ。
CTM_MAINTENANCE_LCL	グループ	ローカル PC	Administrators (*1)	権限的には、CTM_MAINTENANCE と同様で、ドメイン環境が異常な場合に利用する緊急用グループ。通常の運用では利用しない。CENTUM VP をドメイン環境で構築完了後、各 PC の管理者ユーザ（ローカルユーザ）を、このグループに追加する。
ADS_MANAGER	グループ	ドメインコントローラ	Domain Users (*1)	オートメーションデザインスイート管理ツールを使い、CENTUM VP のオートメーションデザインサーバの管理を行うためのグループ。
OFFUSER	ユーザ	ローカル PC	Users	Windows 認証モードの HIS タイプシングルサインオンの自動ログオンに利用されるユーザ。Windows 環境の権限は、必要最低限の設定となる。
CTM_PROCESS	ユーザ	ローカル PC	Users	CENTUM VP のプロセス（Windows サービス）を実行させるためのユーザで、Windows へのログオン権限はないユーザ。
UGS_PROCESS	ユーザ	ローカル PC	Administrators	CENTUM VP のプロセス（Windows サービス）を実行させるためのユーザで、Windows へのログオン権限はないユーザ。UGS にのみ作成され、UGS 関連のプロセスを実行する。
LIC_PROCESS	ユーザ	ローカル PC	Users	ライセンス管理機能のプロセス（Windows サービス）を実行させるためのユーザで、Windows へのログオン権限はないユーザ。

次に続く

表 2.2.3-3 標準モデル／強固モデル—ドメイン管理（前から続く）

ユーザ名／グループ名	種別	作成場所	所属するグループ	説明
ADS_PROCESS	ユーザ	ローカル PC	Users	オートメーションデザインサーバのプロセス（Windows サービス）を実行させるためのユーザで、Windows へのログオン権限はないユーザ。
RDC_PROCESS	ユーザ	ローカル PC	<ul style="list-style-type: none"> Users CTM_OPC_LCL 	コンピュータ切替型 UGS 機能用のプロセス（Windows サービス）を実行させるためのユーザで、Windows へのログオン権限はないユーザ。
PSF_PROCESS	ユーザ	ローカル PC	Users	エンジニアリングサーバ機能ライセンスがある場合に作成されるユーザで、プロジェクトのバックアップ時に使用される。
ADS_AGENT	ユーザ	ローカル PC	<ul style="list-style-type: none"> Users Performance Monitor Users CTM_OPC_LCL 	ステーション情報の管理プロセスを実行するためのユーザで、Windows へのログオン権限はないユーザ。

*1: 作成されるグループに所属するユーザは、[所属するグループ] 欄に記載のグループにも所属させていただきます。

重要

- これらのユーザとグループは、CENTUM VP の用途以外には使用しないでください。
- セキュリティモデルを変更した場合、確認なしで、既存ユーザグループが削除されたり、その名称が変更されたりすることがあります。

参照

オートメーションデザインサーバについては、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「A. オートメーションデザインスイート概要」

● タイプ 4：標準モデル／強固モデル—併用管理

IT セキュリティツールを実行すると、次の表に示されるユーザ／グループが自動で作成されます。

表 2.2.3-4 標準モデル／強固モデル—併用管理

ユーザ名／グループ名	種別	作成場所	所属するグループ	説明
CTM_OPERATOR	グループ	ドメインコントローラ	Domain Users (*1)	オペレータ用ユーザのグループ。
CTM_OPERATOR_LCL	グループ	ローカル PC	Users (*1)	スタンドアロン管理を行う PC で使用されるオペレータ用ユーザのグループ。
CTM_ENGINEER	グループ	ドメインコントローラ	Domain Users (*1)	システムビューなどを使い、CENTUM VP のエンジニアリングを行うユーザのグループ。
CTM_ENGINEER_LCL	グループ	ローカル PC	Users (*1)	スタンドアロン管理を行う PC で使用される、システムビューなどを使い、CENTUM VP のエンジニアリングを行うユーザのグループ。

次に続く

表 2.2.3-4 標準モデル／強固モデル併用管理（前から続く）

ユーザ名／グループ名	種別	作成場所	所属するグループ	説明
CTM_ENGINEER_ADM	グループ	ドメインコントローラ	Domain Admins (*1)	システムビューなどを使い、CENTUM VP のエンジニアリングを行うユーザのグループで、CTM_ENGINEER より強い権限を持ったグループ。
CTM_ENGINEER_ADM_LCL	グループ	ローカル PC	Administrators (*1)	スタンドアロン管理を行う PC で使用される、CENTUM VP のエンジニアリングを行うユーザのグループで、CTM_ENGINEER より強い権限を持ったグループ。
CTM_OPC	グループ	ドメインコントローラ	Domain Users (*1)	他プログラムが CENTUM VP と連携するために使用するグループ。たとえば、CENTUM VP と OPC 通信を行うときに使用される。
CTM_OPC_LCL	グループ	ローカル PC	Users (*1)	権限的には、CTM_OPC と同様で、EXA パッケージの組み込みユーザなど、ドメイン管理に対応できないユーザ向けの補助的なグループで通常の運用では利用しない。
CTM_MAINTENANCE	グループ	ドメインコントローラ	Domain Admins (*1)	システム構築時の SE やメンテナンス担当者など、CENTUM VP のメンテナンスを行うユーザのグループ。
CTM_MAINTENANCE_LCL	グループ	ローカル PC	Administrators (*1)	権限的には、CTM_MAINTENANCE と同様で、ドメイン環境が異常な場合に利用する緊急用グループ。通常の運用では利用しない。CENTUM VP をドメイン環境で構築完了後、各 PC の管理者ユーザ（ローカルユーザ）を、このグループに追加する。
ADS_MANAGER	グループ	ドメインコントローラ	Domain Users (*1)	オートメーションデザインスイート管理ツールを使い、CENTUM VP のオートメーションデザインサーバの管理を行うためのグループ。
ADS_MANAGER_LCL	グループ	ローカル PC	Users (*1)	スタンドアロン管理を行う PC で使用されるオートメーションデザインスイート管理ツールを使い、CENTUM VP のオートメーションデザインサーバの管理を行うためのグループ。
OFFUSER	ユーザ	ローカル PC	Users	Windows 認証モードの HIS タイプシングルサインオンの自動ログオンに利用されるユーザ。Windows 環境の権限は、必要最低限の設定となる。
CTM_PROCESS	ユーザ	ローカル PC	Users	CENTUM VP のプロセス（Windows サービス）を実行させるためのユーザで、Windows へのログオン権限はないユーザ。
UGS_PROCESS	ユーザ	ローカル PC	Administrators	CENTUM VP のプロセス（Windows サービス）を実行させるためのユーザで、Windows へのログオン権限はないユーザ。UGS にのみ作成され、UGS 関連のプロセスを実行する。
LIC_PROCESS	ユーザ	ローカル PC	Users	ライセンス管理機能のプロセス（Windows サービス）を実行させるためのユーザで、Windows へのログオン権限はないユーザ。

次に続く

表 2.2.3-4 標準モデル／強固モデル－併用管理（前から続く）

ユーザ名／グループ名	種別	作成場所	所属するグループ	説明
ADS_PROCESS	ユーザ	ローカル PC	Users	オートメーションデザインサーバのプロセス（Windows サービス）を実行させるためのユーザで、Windows へのログオン権限はないユーザ。
RDC_PROCESS	ユーザ	ローカル PC	<ul style="list-style-type: none"> Users CTM_OPC_LCL 	コンピュータ切替型 UGS 機能用のプロセス（Windows サービス）を実行させるためのユーザで、Windows へのログオン権限はないユーザ。
PSF_PROCESS	ユーザ	ローカル PC	Users	エンジニアリングサーバ機能ライセンスがある場合に作成されるユーザで、プロジェクトのバックアップ時に使用される。
ADS_AGENT	ユーザ	ローカル PC	<ul style="list-style-type: none"> Users Performance Monitor Users CTM_OPC_LCL 	ステーション情報の管理プロセスを実行するためのユーザで、Windows へのログオン権限はないユーザ。

*1: 作成されるグループに所属するユーザは、[所属するグループ] 欄に記載のグループにも所属させてください。

重要

- これらのユーザとグループは、CENTUM VP の用途以外には使用しないでください。
- セキュリティモデルを変更した場合、確認なしで、既存ユーザグループが削除されたり、その名称が変更されたりすることがあります。

参照

オートメーションデザインサーバについては、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「A. オートメーションデザインスイート概要」

■ Vnet/IP インタフェースパッケージが追加するユーザとユーザグループ

Vnet/IP インタフェースパッケージをインストールすると、次の表に示されるユーザやユーザグループが自動で作成されます。

LIC_PROCESS 以外のユーザやユーザグループは、Vnet/IP インタフェースパッケージだけで使用されます。CENTUM VP のソフトウェアには影響を与えません。

表 2.2.3-5 追加されるユーザとグループ

ユーザ名／グループ名	種別	作成場所	所属するグループ	説明
VNT_ALL	グループ	ローカル PC	-	Vnet/IP インタフェースパッケージのディレクトリを読み書き可能なユーザグループです。Windows にサインインできるユーザを、このグループに所属させないでください。
VNT_VNET_VVIF	グループ	ローカル PC	-	Vnet/IP インタフェースパッケージのプロセス（Windows サービスなど）の実行に必要なユーザグループです。Windows にサインインできるユーザを、このグループに所属させないでください。
VNT_NVP_CMDIF	グループ	ローカル PC	-	
VNT_NVP_MNGIF	グループ	ローカル PC	-	

次に続く

表 2.2.3-5 追加されるユーザとグループ（前から続く）

ユーザ名／グループ名	種別	作成場所	所属するグループ	説明
VNT_COMMON	ユーザ	ローカル PC	VNT_ALL	Vnet/IP インタフェースパッケージのディレクトリを読み書き可能なユーザです。Windows へのサインイン権限はありません。
VNT_NVP_CORE	ユーザ	ローカル PC	<ul style="list-style-type: none"> • VNT_VNET_WVI • VNT_NVP_CM • VNT_NVP_MN • VNT_NVP_GIF • VNT_ALL • Performance Monitor Users 	Vnet/IP インタフェースパッケージのプロセス（Windows サービスなど）を実行させるためのユーザです。Windows へのサインイン権限はありません。
VNT_BKNET	ユーザ	ローカル PC	<ul style="list-style-type: none"> • VNT_VNET_WVI • VNT_NVP_MN • VNT_GIF • VNT_ALL 	
LIC_PROCESS	ユーザ	ローカル PC	<ul style="list-style-type: none"> • VNT_ALL • Users 	LIC_PROCESS ユーザは、ライセンスマネージャに対応した製品共通のユーザです。ライセンス反映などに使用されます。Vnet/IP インタフェースパッケージインストール時に、LIC_PROCESS が存在しなければ LIC_PROCESS ユーザの作成と設定が行われます。

重要

Vnet/IP インタフェースパッケージをインストールしたときに自動的に作成されるユーザやユーザグループは、ローカル PC でのみ有効です。ドメインコントローラで管理しないでください。また、Windows にサインインできるユーザを、これらのグループに所属させないでください。

2.2.4 ユーザ名とパスワードの規約

Windows 機能にはユーザ名とパスワードの規約があります。これに伴い、HIS グループユーザと ENG グループユーザのユーザ名とパスワードにも規約があります。次の規約に従って、HIS グループユーザ、ENG グループユーザ、および Windows 認証モード時の Windows ユーザを作成してください。

■ ユーザ名

ユーザ名の規約は次のとおりです。

表 2.2.4-1 ユーザ名

項目	詳細
文字数	16 文字以内
文字種	アルファベット、数字および記号 ! # \$ % () - . ^ _ { } ~ が使用できます。 全角は使用できません。
制約	大文字のみ。 先頭文字はアルファベットと数字および記号 ^ _ { } ~ が使用できます。 ピリオドで終わるものは許されません。

補足 HIS グループユーザや ENG グループユーザでは大文字しか使用できません。Windows ユーザでは大文字や小文字の使用が可能ですが、区別はされないため、大文字を使用してください。

■ パスワード

パスワードの規約は次のとおりです。

表 2.2.4-2 パスワード

項目	詳細
文字数	HIS グループユーザ、および ENG グループユーザのパスワードは、半角英数 32 文字までです。 Windows 認証モード時の Windows ユーザのパスワードは、63 文字以内です。
文字種	アルファベット、数字および次の記号が使用できます。 ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~ スペース
制約	運用時に Windows で設定したパスワードポリシーが適用されます。

補足 HIS グループユーザは、HIS ユーティリティでパスワードポリシーを設定します。
ENG グループユーザは、アクセス制限ユーティリティでパスワードポリシーを設定します。

2.2.5 特別なユーザ

Windows 認証モードの場合に、Windows ユーザと連携する特別な HIS グループユーザと ENG グループユーザについて説明します。

■ ローカル認証用ユーザ

ローカル認証用ユーザとして、次のユーザ名を使用できます。

_ (アンダースコア) で始まるユーザ名

Windows 認証モードのときに、ユーザが使用している PC でユーザ認証を行います。このユーザは、ドメイン管理時や併用管理時にドメインコントローラがダウンしているときなどの緊急時に用いるユーザです。通常では使用しません。また、スタンドアロン管理時には、作成する必要はありません。

操作監視機能のユーザインダイアログでこのユーザを使用した場合は、次の条件でシステムアラームが通知されます。

- ・ ドメイン管理中であり、かつドメインコントローラへのアクセスができるとき
これは、正常にドメイン上の認証処理が可能にもかかわらず、緊急時用のローカルユーザを使用した場合に相当します。セキュリティ上の問題があるため、システムアラームとして警告を出します。

■ OFFUSER

Windows 認証モードでの OFFUSER には、次のような特徴があります。

- ・ Windows 認証モードの HIS タイプシングルサインオンで、自動ログオンに利用されるユーザとしてのみ使用されます。
- ・ ドメイン管理、スタンドアロン管理にかかわらず、ローカルユーザとして作成されます。
- ・ 初期パスワードは、32 文字で非公開です。(パスワードは変更可能です。ただし、CENTUM VP システムとして、同一パスワードにする必要があります。)

3. セキュリティ対策の詳細

ここでは、セキュリティ対策の詳細について、セキュリティタイプごとに説明します。

3.1 アクセスコントロール

本製品のユーザの権限を必要最低限にすることにより、本製品内の重要なデータへの不正アクセスおよび漏えい、改ざん、破壊に対処します。Windows のアクセスコントロール機能を利用して、ファイル／フォルダ、レジストリ、DCOM モジュール、およびローカルセキュリティポリシーに対するアクセス許可をコントロールします。

アクセスコントロールはユーザ／グループ単位で行います。ユーザは、そのユーザに許可された権限、または所属するグループに許可された権限だけ利用できます。

3.1.1 ファイル／フォルダに対するアクセス許可

本製品では、ファイルやフォルダに対してファイル単位やフォルダ単位でアクセスコントロールできます。ユーザ／グループごとに実行、読み取り、書き込み、削除などのアクセス許可を設定し、各ユーザの利用できる権限を制限します。本製品では、フォルダ単位でアクセス許可を設定します。

補足

フォルダのアクセス許可とは異なる設定が必要なファイルに対しては、個別のアクセス許可を設定します。

■ 対象フォルダ

おもなアクセスコントロール対象のフォルダを次に示します。

表 3.1.1-1 対象フォルダ

対象フォルダ	内容
<CENTUM VP インストールフォルダ>	CENTUM VP がインストールされたフォルダ
<ProgramFiles32> (*1) ¥Yokogawa¥IA¥iPCS¥Platform¥License	ライセンス管理プログラムの実行に必要なファイルがインストールされるフォルダ
<ProgramFiles32> (*1) ¥Yokogawa¥IA¥iPCS¥Platform¥Program	ライセンス管理プログラムなどがインストールされるフォルダ
<ProgramFiles32> (*1) ¥Yokogawa¥IA¥iPCS¥Platform¥SECURITY	IT セキュリティツールなどがインストールされるフォルダ
<ProgramFiles32> (*1) ¥Yokogawa¥IA¥iPCS¥Platform¥PC-Redundancy¥Tool	コンピュータ切替型 UGS 用管理ツールがインストールされるフォルダ
<ProgramFiles32> (*1) ¥Yokogawa¥IA¥iPCS¥Platform¥PC-Redundancy¥Agent	コンピュータ切替型 UGS 関連プログラムがインストールされるフォルダ
<ProgramFiles32> (*1) ¥Yokogawa¥IA¥iPCS¥Products¥CENTUMVP	CENTUM VP のプログラムで、Program Files 側にインストールされたフォルダ
<ProgramFiles32> (*1) ¥Yokogawa¥IA¥iPCS¥Products¥ADSuite	オートメーションデザインサーバやモジュールベースエンジニアリングに関連したプログラムがインストールされるフォルダ
<ProgramFiles64> (*2) ¥Yokogawa¥IA¥iPCS¥Platform¥PC-Redundancy¥Agent	コンピュータ切替型 UGS 関連プログラムがインストールされるフォルダ
<ProgramFiles64> (*2) ¥Yokogawa¥IA¥iPCS¥Products¥ADSuite	オートメーションデザインサーバやモジュールベースエンジニアリングに関連したプログラムがインストールされるフォルダ
<ProgramFiles64> (*2) ¥Yokogawa¥IA¥iPCS¥Products¥CENTUMVP	CENTUM VP のプログラムで、Program Files 側にインストールされたフォルダ
<ProgramFiles64> (*2) ¥Yokogawa¥IA¥iPCS¥Products¥CIMAgent	ステーション情報の管理プロセスに関連したプログラムがインストールされるフォルダ
<ProgramFiles32> (*1) ¥Yokogawa¥IA¥iPCS¥Products¥Platform	ログサーバなどがインストールされるフォルダ
<ProgramData> (*3) ¥Yokogawa¥IA¥iPCS¥Platform¥License	ライセンス管理データなどがインストールされるフォルダ
<ProgramData> (*3) ¥Yokogawa¥IA¥iPCS¥Platform¥Security	IT セキュリティツールの設定ファイルなどがインストールされるフォルダ
<ProgramData> (*3) ¥Yokogawa¥IA¥iPCS¥Platform¥PC-Redundancy¥Agent	コンピュータ切替型 UGS 関連データなどがインストールされるフォルダ
<ProgramData> (*3) ¥Yokogawa¥IA¥iPCS¥Products¥CentumVP	CENTUM VP のログなどが作成されるフォルダ
<ProgramData> (*3) ¥Yokogawa¥IA¥iPCS¥Products¥Platform	オンラインマニュアルの管理データなどが作成されるフォルダ

次に続く

表 3.1.1-1 対象フォルダ（前から続く）

対象フォルダ	内容
<ProgramData> (*3) ¥Yokogawa¥IA¥iPCS¥Products¥ChronusENG	オートメーションデザインサーバやモジュールベースエンジニアリングに関連したデータがインストールされるフォルダ
<ProgramData> (*3) ¥Yokogawa¥IA¥iPCS¥Products¥CIMAgent	ステーション情報の管理プロセスに関連したデータがインストールされるフォルダ
<ProgramData> (*3) ¥Yokogawa¥IA¥iPCS¥Products¥AccessRef¥CTM-PSF	CENTUM VP で扱うデータがインストールされるフォルダ
<ProgramFiles32> (*1) ¥Yokogawa¥PROFIBUS_Configurator	PROFIBUS-DP コンフィグレータや PROFINET コンフィグレータがインストールされたフォルダ
<ProgramData> (*3) ¥Yokogawa¥SYCONnet	PROFIBUS-DP コンフィグレータや PROFINET コンフィグレータのデータファイルが格納されているフォルダ
<ProgramFiles32> (*1) ¥Common Files¥Hilscher	PROFIBUS-DP コンフィグレータや PROFINET コンフィグレータに関連したファイルが格納されているフォルダ
<ProgramFiles32> (*1) ¥Common Files¥Hilscher GmbH	PROFIBUS-DP コンフィグレータや PROFINET コンフィグレータに関連したファイルが格納されているフォルダ
<windir> (*4) ¥system32	Windows 用メンテナンスツールがインストールされているフォルダ (*5)
<windir> (*4) ¥SysWOW64 (*6)	Windows 用メンテナンスツールがインストールされているフォルダ (*5)
<プロジェクトデータ>	CENTUM VP 用プロジェクトファイルが格納されているフォルダ
CTM_PJTS_DBSF	ファイルサーバ、HIS、またはシステム生成機能を搭載した PC に作成する共有フォルダ。 HIS またはシステム生成機能を搭載した PC については、プロジェクトデータをデフォルト以外のフォルダに置く場合に作成する。
<ProgramFiles64> (*2) ¥Yokogawa¥IA¥iPCS¥Platform¥VnetIPSoftStack	Vnet/IP インタフェースパッケージ関連のファイルやデータが格納されているフォルダ
<ProgramData> (*3) ¥Yokogawa¥IA¥iPCS¥Platform¥VnetIPSoftStack	Vnet/IP インタフェースパッケージ関連のファイルやデータが格納されているフォルダ
<ProgramData> (*3) ¥Yokogawa¥IA¥iPCS¥Products¥AccessRef¥VnetIPSoftStack	Vnet/IP インタフェースパッケージ関連のファイルやデータが格納されているフォルダ

- *1: <ProgramFiles32> は、次のフォルダを表します。システムドライブが、C ドライブの例です。
Windows 10、Windows 7、Windows Server 2016、Windows Server 2012 R2、および Windows Server 2008 R2 の場合は、
C:¥Program Files (x86)
Windows Server 2008 の場合は、
C:¥Program Files
- *2: <ProgramFiles64> は、次のフォルダを表します。システムドライブが、C ドライブの例です。
Windows 10、Windows 7、Windows Server 2016、Windows Server 2012 R2、および Windows Server 2008 R2 の場合は、
C:¥Program Files
- *3: <ProgramData> は、次のフォルダを表します。システムドライブが、C ドライブの例です。
C:¥ProgramData
- *4: <windir> は、次のフォルダを表します。システムドライブが、C ドライブの例です。
C:¥Windows
- *5: フォルダ内の一部のファイルに対して、アクセス許可が設定されます。
- *6: Windows 10、Windows 7、Windows Server 2016、Windows Server 2012 R2、および Windows Server 2008 R2 の場合のみ。

■ プログラムのアクセス許可

CENTUM VP の各機能（プログラム）に、ユーザ／グループごとのアクセス許可を設定し、各ユーザの利用できる機能を制限します。

次に、スタートメニューに登録されるプログラムの実行に対するアクセス許可の設定状況をユーザ／グループ別に示します。アクセスが許可されているユーザ／グループのみプログラムを実行できます。

ただし、HIS 本体はスタートメニューからは起動しません。

補足

スタートメニューに登録される以外の拡張子が exe、com、bat、cmd、または vbs のプログラムについても、ユーザやグループごとに実行に対するアクセス許可を設定しています。

表 3.1.1-2 スタートメニューから起動するプログラムのアクセス許可

スタートメニューの項目	ユーザ／グループ (*1)									
	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
HIS 本体 (*2)	Yes	Yes	Yes	No	Yes	No	No	No	No	No
HIS ユーティリティ	No	No	No	No	Yes	No	No	No	No	No
アクセス制限ユーティリティ	No	No	Yes	No	Yes	No	No	No	No	No
グラフィックビルダ	Yes (*3)	Yes	Yes	No	Yes	No	No	No	No	No
グラフィック互換性チェックツール	No	Yes	Yes	No	Yes	No	No	No	No	No
システムビュー	No	Yes	Yes	No	Yes	No	No	No	No	No
ソフトウェア構成ビューア	No	Yes	Yes	No	Yes	No	No	No	No	No
ヒストリカル統合ビューア	No	Yes	Yes	No	Yes	No	No	No	No	No
フィールドバス関連ファイルコピーツール	No	Yes	Yes	No	Yes	No	No	No	No	No
プロジェクト属性変更ユーティリティ	No	Yes	Yes	No	Yes	No	No	No	No	No
リンクパーツウィンドウ	No	Yes	Yes	No	Yes	No	No	No	No	No
Device Panel	No	Yes	Yes	No	Yes	No	No	No	No	No
処方ビュー	No	Yes	Yes	No	Yes	No	No	No	No	No
帳票パッケージ	No	Yes	Yes	No	Yes	No	No	No	No	No
コマンドプロンプト	Yes	Yes	Yes	No	Yes	No	No	Yes	No	No
プロジェクトセーブ	No	Yes	Yes	No	Yes	No	No	No	No	No
ログセーブ	Yes	Yes	Yes	No	Yes	No	No	Yes	No	No
N-IO ノードセキュリティ	No	Yes	Yes	No	Yes	No	No	No	No	No
CAMS for HIS コンフィグレータ	No	Yes	Yes	No	Yes	No	No	No	No	No
CAMS for HIS マイグレーションツール	No	Yes	Yes	No	Yes	No	No	No	No	No
CAMS for HIS 擬似アラーム発生ツール	No	Yes	Yes	No	Yes	No	No	No	No	No
UACS マイグレーションツール	No	Yes	Yes	No	Yes	No	No	No	No	No
UACS ユーティリティ	No	No	No	No	Yes	No	No	No	No	No
AD オーガナイザ	No	Yes	Yes	No	Yes	No	No	No	Yes	No
ADS 管理ツール	No	No	No	No	No	No	No	Yes	Yes	No
依存関係解析	No	Yes	Yes	No	Yes	No	No	No	Yes	No
SIOS 統計情報収集ユーティリティ	No	No	No	No	Yes	No	No	No	No	No

次に続く

表 3.1.1-2 スタートメニューから起動するプログラムのアクセス許可（前から続く）

スタートメニューの項目	ユーザ／グループ(*1)									
	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]
License Manager	Yes	Yes	Yes	No	Yes	No	Yes	No	No	No
IT セキュリティツール	No	No	No	No	Yes	No	No	No	No	No
Redundancy Management Tool	(*4)									
Vnet/IP interface management tool	(*5)									

*1: ユーザ／グループ

- [1] : CTM_OPERATOR/CTM_OPERATOR_LCL/OFFUSER
- [2] : CTM_ENGINEER/CTM_ENGINEER_LCL
- [3] : CTM_ENGINEER_ADM/CTM_ENGINEER_ADM_LCL
- [4] : CTM_OPC/CTM_OPC_LCL
- [5] : CTM_MAINTENANCE/CTM_MAINTENANCE_LCL
- [6] : CTM_PROCESS/UGS_PROCESS
- [7] : LIC_PROCESS
- [8] : ADS_MANAGER/ADS_MANAGER_LCL
- [9] : ADS_PROCESS
- [10] : RDC_PROCESS/PSF_PROCESS/ADS_AGENT

*2: スタートメニューから起動しない機能

*3: HIS でビルダ参照パッケージ（オプション）を利用する場合、グラフィックビルダが必要なため

*4: <ProgramFiles32>のアクセス許可に従って実行可否が決まります。

*5: Vnet/IP インタフェース管理ツールが起動します。Administrators グループ、または Users グループに所属するユーザが実行できます。Administrators グループに属するユーザは、V ネットステーションアドレスの設定と、Vnet/IP インタフェースパッケージのモニタができます。Users グループに属するユーザは、Vnet/IP インタフェースパッケージのモニタのみできます。

重要

Administrators グループに所属する CTM_ENGINEER_ADM、CTM_ENGINEER_ADM_LCL、CTM_MAINTENANCE、CTM_MAINTENANCE_LCL のユーザは、操作監視機能およびテスト機能を起動できません。ただし、ビルトイン Administrator アカウントは例外で、操作監視機能およびテスト機能を起動できます。

3.1.2 レジストリ構成とユーザ／グループ

本製品が使用するレジストリへのアクセスを制御することで改ざんや破壊を防止します。

■ レジストリの分類

アクセスコントロール対象のレジストリは、3 種類あります。

表 3.1.2-1 レジストリの分類

名称	内容
CENTUM 関連	CENTUM 関連のレジストリです。
DCOM 関連	DCOM 通信（OPC）関連のレジストリです。
PROFIBUS-DP コンフィグレータおよび PROFINET コンフィグレータ関連	PROFIBUS-DP コンフィグレータおよび PROFINET コンフィグレータ関連のレジストリです。

■ 対象キー

アクセスコントロール対象のレジストリキーを次に示します。

表 3.1.2-2 CENTUM 関連のレジストリキー

名称	対象キー	内容
CENTUM Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\YOKOGAWA]	CENTUM VP をインストール時に作成されるレジストリ
CS3000 Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\YOKOGAWA\CS3000]	CENTUM VP のプログラムで利用されるレジストリ
CentumProductInfo Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\YOKOGAWA\CentumProductInfo]	CENTUM VP のプロダクト情報が格納されるレジストリ
CENTUMVP Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\YOKOGAWA\CENTUMVP]	インストーラで利用されるレジストリ
CS3K Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\YOKOGAWA\CS3K]	インストーラで利用されるレジストリ
VHFD Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\YOKOGAWA\VHFD]	制御バスに関するレジストリ
PKGCOM Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\YOKOGAWA\PKGCOM]	Exa に関するレジストリ

表 3.1.2-3 DCOM 関連のレジストリキー

名称	対象キー	内容
OpcEnum Registry	[HKEY_CLASSES_ROOT\AppID\{13486D44-4821-11D2-A494-3CB306C10000}]	OpcEnum 用 DCOM 関連レジストリ
OPC Alarms Registry	[HKEY_CLASSES_ROOT\AppID\{21FF9972-DE40-11D1-B324-00A024770B10}]	Yokogawa CSHIS OPC Alarms 用 DCOM 関連レジストリ
BKCLcs Registry	[HKEY_CLASSES_ROOT\AppID\{79142CD2-0ABE-11D4-8F5C-0060B0C3BE1F}]	BKCLcs 用 DCOM 関連レジストリ
CS Batch Server Registry	[HKEY_CLASSES_ROOT\AppID\{A232A362-E94E-11D1-AB29-0060B0174D72}]	Yokogawa CS Batch Server 用 DCOM 関連レジストリ
CS DCOM Server Registry	[HKEY_CLASSES_ROOT\AppID\{b75cd3f2-a692-11d2-a06e-006008ab9b09}]	Yokogawa CS DCOM Server 用 DCOM 関連レジストリ
OPC Server Registry	[HKEY_CLASSES_ROOT\AppID\{E6C32641-F1CF-11d0-B0E4-080009CCD384}]	Yokogawa CSHIS OPC Server 用 DCOM 関連レジストリ
OPC HDA Server Registry	[HKEY_CLASSES_ROOT\AppID\{FCF966F4-D7E8-11D1-9702-00C04FBC25BF}]	Yokogawa CSHIS OPC HDA Server 用 DCOM 関連レジストリ
Exaopc HDA Server Registry	[HKEY_CLASSES_ROOT\AppID\{6CE76D12-D100-11D2-9804-00C04FBC25BF}]	Yokogawa Exaopc HDA Server 用 DCOM 関連レジストリ

表 3.1.2-4 PROFIBUS-DP コンフィグレータおよび PROFINET コンフィグレータ関連のレジストリキー

名称	対象キー
PROFIBUS Configurator Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Hilscher GmbH]
PROFIBUS International Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\PROFIBUS International]
PROFIBUS DTMs Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Yokogawa\DTMs]
PROFIBUS GenericSlaveDTM Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Yokogawa\GenericSlaveDTM]
PROFIBUS Sycon_net Registry	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Yokogawa\SyCon_net]

■ レジストリのアクセス許可

レジストリに対するアクセス許可を示します。

表 3.1.2-5 CENTUM 関連のレジストリに対するアクセス許可

レジストリの項目	ユーザ／グループ (*1)													
	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]
CENTUM Registry	-	-	-	-	-	-	-	-	F	F	-	-	--	-
CS3000 Registry	F	F	F	F	F	F	F	-	R	F	-	-	-	-
CentumProductInfo Registry	-	-	-	-	F	-	-	-	F	F	-	-	-	-
CENTUMVP Registry	-	-	-	-	F	-	-	-	F	F	-	-	-	-
CS3K Registry	F	F	F	F	F	F	F	F	R	F	-	-	-	-
VHFD Registry	F	F	F	F	F	F	F	-	R	F	-	-	-	-
PKGCOM Registry	-	F	-	-	F	F	-	-	-	F	-	-	-	-

*1: ユーザ／グループ

- [1]: CTM_OPERATOR/CTM_OPERATOR_LCL/OFFUSER
- [2]: CTM_ENGINEER/CTM_ENGINEER_LCL
- [3]: CTM_ENGINEER_ADM/CTM_ENGINEER_ADM_LCL
- [4]: CTM_OPC/CTM_OPC_LCL
- [5]: CTM_MAINTENANCE/CTM_MAINTENANCE_LCL
- [6]: CTM_PROCESS
- [7]: UGS_PROCESS
- [8]: LIC_PROCESS
- [9]: Everyone
- [10]: SYSTEM
- [11]: SERVICE
- [12]: ADS_MANAGER/ADS_MANAGER_LCL
- [13]: ADS_PROCESS
- [14]: RDC_PROCESS/PSF_PROCESS/ADS_AGENT

アクセス許可の種類
 F: フルコントロール
 R: 読み取り
 -: 権限なし

表 3.1.2-6 DCOM 関連のレジストリに対するアクセス許可

レジストリの項目	ユーザ／グループ (*1)													
	[1] (*2)	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]
OpcEnum Registry	F	F	F	F	F	F	-	-	-	F	R	-	-	-
OPC Alarms Registry	F	F	F	F	F	F	-	-	-	F	R	-	-	-
BKCLcs Registry	F	F	F	F	F	F	-	-	-	F	R	-	-	-
CS Batch Server Registry	F	F	F	F	F	F	-	-	-	F	R	-	-	-
CS DCOM Server Registry	F	F	F	F	F	F	-	-	-	F	R	-	-	-

次に続く

表 3.1.2-6 DCOM 関連のレジストリに対するアクセス許可 (前から続く)

レジストリの項目	ユーザ／グループ(*1)													
	[1] (*2)	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]
OPC Server Registry	F	F	F	F	F	F	-	-	-	F	R	-	-	-
OPC HDA Server Registry	F	F	F	F	F	F	-	-	-	F	R	-	-	-
Exaopc HDA Server Registry	F	F	F	F	F	F	-	-	-	F	R	-	-	-

*1: ユーザ／グループ

- [1]: CTM_OPERATOR/CTM_OPERATOR_LCL/OFFUSER
- [2]: CTM_ENGINEER/CTM_ENGINEER_LCL
- [3]: CTM_ENGINEER_ADM/CTM_ENGINEER_ADM_LCL
- [4]: CTM_OPC/CTM_OPC_LCL
- [5]: CTM_MAINTENANCE/CTM_MAINTENANCE_LCL
- [6]: CTM_PROCESS
- [7]: UGS_PROCESS
- [8]: LIC_PROCESS
- [9]: Everyone
- [10]: SYSTEM
- [11]: SERVICE
- [12]: ADS_MANAGER/ADS_MANAGER_LCL
- [13]: ADS_PROCESS
- [14]: RDC_PROCESS/PSF_PROCESS/ADS_AGENT

アクセス許可の種類

F: フルコントロール

R: 読み取り

-: 権限なし

*2: OFFUSER の場合、アクセス許可は R となります。

表 3.1.2-7 PROFIBUS-DP コンフィグレータおよび PROFINET コンフィグレータ関連のレジストリに対するアクセス許可

レジストリの項目	ユーザ／グループ(*1)											
	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]
PROFIBUS Configurator Registry	-	F	F	-	F	-	-	-	F	-	-	-
PROFIBUS International Registry	-	F	F	-	F	-	-	-	F	-	-	-
PROFIBUS DTMs Registry	-	F	F	-	F	-	-	-	F	-	-	-
PROFIBUS GenericSlaveDTM Registry	-	F	F	-	F	-	-	-	F	-	-	-
PROFIBUS Sycon_net Registry	-	F	F	-	F	-	-	-	F	-	-	-

- *1: [1]: CTM_OPERATOR/CTM_OPERATOR_LCL/OFFUSER
 [2]: CTM_ENGINEER/CTM_ENGINEER_LCL
 [3]: CTM_ENGINEER_ADM/CTM_ENGINEER_ADM_LCL
 [4]: CTM_OPC/CTM_OPC_LCL
 [5]: CTM_MAINTENANCE/CTM_MAINTENANCE_LCL
 [6]: CTM_PROCESS/UGS_PROCESS
 [7]: LIC_PROCESS
 [8]: Everyone
 [9]: SYSTEM
 [10]: ADS_MANAGER/ADS_MANAGER_LCL
 [11]: ADS_PROCESS
 [12]: RDC_PROCESS/PSF_PROCESS/ADS_AGENT
- アクセス許可の種類
 F: フルコントロール
 -: 権限なし

3.1.3 DCOM（OPC）とユーザ／グループ

CENTUM VP と DCOM 通信を行う他パッケージ（サードパーティパッケージを含む）を考慮して、DCOM コンポーネントにアクセスコントロールを設定します。

■ 全体設定

PC 全体に関する設定は、次のとおりです。

- ・ 従来モデル
既定の認証レベル：なし
- ・ 標準モデルまたは強固モデル
既定の認証レベル：接続

■ DCOM コンポーネント個別設定

CENTUM VP がインストールした DCOM コンポーネントに対して、次の [1] から [9] のユーザ／グループすべてにローカル／リモートからの OPC の実行権限を設定します。

OFFUSER は、ローカルからの実行権限を設定します。

- [1] : CTM_OPERATOR/CTM_OPERATOR_LCL
- [2] : CTM_ENGINEER/CTM_ENGINEER_LCL
- [3] : CTM_ENGINEER_ADM/CTM_ENGINEER_ADM_LCL
- [4] : CTM_OPC/CTM_OPC_LCL
- [5] : CTM_MAINTENANCE/CTM_MAINTENANCE_LCL
- [6] : CTM_PROCESS/UGS_PROCESS
- [7] : SYSTEM
- [8] : ADS_MANAGER/ADS_MANAGER_LCL
- [9] : ADS_PROCESS

PSF_PROCESS については、DCOM コンポーネントに対する権限を設定しません。

3.1.4 ローカルセキュリティとユーザ／グループ

各ユーザ／グループに、Windows 標準以外の次のローカルセキュリティポリシーを設定します。

表 3.1.4-1 ローカルセキュリティポリシーの許可状況

ポリシー	ユーザ／グループ(*1)													
	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]	[13]	[14]
グローバルオブジェクトの作成	No	No	No	No	No	No	Yes	Yes	No	No	No	No	No	No
プログラムのデバッグ	No	No	Yes	Yes	No	Yes	Yes	No	No	No	No	No	No	No
バッチジョブとしてログオン	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes	No
サービスとしてログオン	No	No	No	No	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
ローカルでログオンを拒否する	Yes(*2)	No	No	No	No	No	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
ローカルログオンを許可(*3)	No	No	Yes	Yes	No	Yes	No	No	No	No	No	No	No	No

*1: ユーザ／グループ

- [1] : OFFUSER
- [2] : CTM_OPERATOR/CTM_OPERATOR_LCL
- [3] : CTM_ENGINEER/CTM_ENGINEER_LCL
- [4] : CTM_ENGINEER_ADM/CTM_ENGINEER_ADM_LCL
- [5] : CTM_OPC/CTM_OPC_LCL
- [6] : CTM_MAINTENANCE/CTM_MAINTENANCE_LCL
- [7] : CTM_PROCESS
- [8] : UGS_PROCESS
- [9] : LIC_PROCESS
- [10] : ADS_MANAGER/ADS_MANAGER_LCL
- [11] : ADS_PROCESS
- [12] : RDC_PROCESS/ADS_AGENT
- [13] : PSF_PROCESS
- [14] : VNT_COMMON、VNT_NVP_CORE、VNT_BKNET

*2: ファイルサーバのみ

*3: このポリシーは、UACS ステーションのみで有効で、UACS ステーション以外は、影響はありません。UACS ステーションでは、Administrators およびこの表で Yes のグループに所属しているユーザアカウントでのみログオンできます。

補足

PSF_PROCESS については、各ローカルセキュリティポリシーに対する許可が与えられていません。

3.2 パーソナルファイアウォールチューニング

ネットワークからの各 PC への接続を必要最低限にすることにより、権限を持たない者からの攻撃に対処します。

■ 例外設定タイプ

CENTUM VP の機能が動作するように、必要な通信ポートを例外として設定します。パーソナルファイアウォールの例外設定を、次に示します。

表 3.2-1 例外設定タイプ

名称	内容
CENTUM 関連	CENTUM 関連のプログラムが通信するための通信ポート
Vnet/IP インタフェースパッケージ関連	Vnet/IP インタフェースパッケージが使用する通信ポート
DCOM 通信関連	DCOM 通信（OPC 通信を含む）を利用したプログラムが通信するポート
ファイル共有関連	Windows のファイル共有機能が使用する通信ポート
Windows 関連	Windows 機能（ファイル共有機能を除く）が使用する通信ポート
コンピュータ切替型 UGS 関連	コンピュータ切替型 UGS 機能が使用する通信ポート

■ CENTUM 関連例外設定

CENTUM 関連例外設定について、次に示します。

表 3.2-2 CENTUM 関連例外設定

サービス名／ 実行ファイル名	プロトコル：ポート番号	パッケージ名または機能名	備考
BKHOdeq.exe	TCP:20109	操作監視基本機能	CENTUM CS と通信する場合は必要
BKHOdeq.exe	TCP:20171	操作監視基本機能	なし
BKHTTrGthr.exe	TCP:20110	操作監視基本機能	なし
BKHLongTerm.exe	TCP:20183	操作監視基本機能	なし
MnsServer.exe	UDP:34301	操作監視基本機能	なし
BKBCopyD.exe	TCP:20111	プロセス管理パッケージ	なし
BKBBDFH.exe	TCP:20174	プロセス管理パッケージ	なし
BKBRECP.exe	TCP:20177	プロセス管理パッケージ	なし
BKBBDFH.exe	TCP:20178	プロセス管理パッケージ	なし
BKBRECP.exe	TCP:20179	プロセス管理パッケージ	なし
BKESimmgr.exe	TCP:34205	拡張テスト機能パッケージ FCS シミュレータパッケージ HIS シミュレータパッケージ UACS シミュレータパッケージ	なし
BKFSim_vhfd.exe	TCP:20010～20013 UDP:20010～20013	拡張テスト機能パッケージ FCS シミュレータパッケージ HIS シミュレータパッケージ UACS シミュレータパッケージ	なし
リモートデスクトップサービス	TCP:3389	リモート操作監視機能サーバ 統合ゲートウェイステーション (UGS2) 基本機能	なし

次に続く

表 3.2-2 CENTUM 関連例外設定 (前から続く)

サービス名／ 実行ファイル名	プロトコル：ポート番号	パッケージ名または機能名	備考
BKHFms.exe	TCP:20181	複数プロジェクト結合パッケージ	CENTUM VP システム内の 1 台の PC で設定があればよい。
BKHFms.exe	TCP:20101	複数プロジェクト結合パッケージ	なし
BKHFms.exe	TCP:20102	複数プロジェクト結合パッケージ	なし
BKHFms.exe	TCP:20105	複数プロジェクト結合パッケージ	なし
BKFApcsMng.exe	TCP:20184	APCS 制御機能	APCS/GSGW
BKVMngService.exe	TCP:34333	SIOS	SIOS 関連
CAMSServer.exe	TCP:8819 TCP:8820 UDP:8819	統合型アラーム管理機能	CAMS
CAMSLogSvr.exe	UDP:8820	統合型アラーム管理機能	CAMS
Yokogawa.IA.iPCS.CENTUMVP.HIS.AlarmSetpoint.Ul.exe	TCP:34419	操作監視基本機能	なし
Yokogawa.IA.iPCS.Platform.License.LicenseManager.Service.exe	TCP:34417	ライセンス管理機能	なし
Yokogawa.IA.iPCS.CENTUMVP.UGS.Facade.Service.exe	TCP:38000	UGS	なし
Yokogawa.IA.iPCS.CENTUMVP.UGS.ENG.FileTransferServiceDispatcher.exe	TCP:38010~38012	UGS	なし
Yokogawa.IA.iPCS.CENTUMVP.UGS.FB.Host.exe	TCP:40111 TCP:40113~40115	UGS	なし
Yokogawa.IA.iPCS.CENTUMVP.UGS.System.Service.exe	TCP:38020 TCP:40112 TCP:40116	UGS	なし
Yokogawa.IA.iPCS.CENTUMVP.UGS.Vnet.Host.exe	TCP:40117	UGS	なし
Yokogawa.IA.iPCS.CENTUMVP.UGS.DataSync.Host.exe	TCP: 38030	UGS	なし
durm_udp.exe	UDP:1099	UGS	なし
opxdas.exe	TCP:135	UGS	なし
eqpmdc.exe	TCP:502	UGS	なし
eqpfcx.exe	TCP:1090	UGS	なし
eqpabc.exe	TCP:44818	UGS	なし
IIS (FTP)	TCP:38040	UGS	UGS 冗長化機能 (ネットワーク切替型)
Yokogawa.IA.iPCS.CENTUMVP.HIS.HISIS.HISInfService.exe	TCP:34420	操作監視基本機能	なし
Yokogawa.IA.iPCS.ChronusENG.Services.Service.exe	ユーザ指定可能 デフォルト TCP:34473	オートメーションデザインサーバ	なし

次に続く

表 3.2-2 CENTUM 関連例外設定（前から続く）

サービス名／ 実行ファイル名	プロトコル：ポート番号	パッケージ名または機能名	備考
Yokogawa.IA.iPCS.ChronusENG.CIMAgent.exe	ユーザ指定可能 デフォルト TCP:34497	CENTUM VP のステーション	ライセンスに影響されない
UACS.Client.ClientManager.exe	UDP:34568 UDP:34569	UACS UACS シミュレータパッケージ	
UACS.Kernel.exe	UDP:34570 UDP:34571 TCP:34572 TCP:34573 TCP:34574 TCP:34575	UACS UACS シミュレータパッケージ	
UACS.HistoricalServer.exe	TCP:34580 TCP:34581	UACS UACS シミュレータパッケージ	
UACS.HealthChecker.exe	TCP:34582 TCP:34583	UACS UACS シミュレータパッケージ	

■ Vnet/IP インタフェースパッケージ関連例外設定

Vnet/IP インタフェースパッケージの例外設定について、次に示します。

表 3.2-3 Vnet/IP インタフェースパッケージ関連例外設定

パッケージ名	プロトコル：ポート番号	備考
Vnet/IP インタフェースパッケージ	UDP:520 UDP:5313 UDP:9940	Vnet/IP インタフェースパッケージで使用する、左記 UDP ポートでの送受信を有効に設定する

■ DCOM 通信関連例外設定

DCOM 通信関連例外設定について、次に示します。

表 3.2-4 DCOM 通信関連例外設定

サービス名／ 実行ファイル名	プロトコル：ポート番号	想定パッケージ名	備考
DCOM サービス	TCP:135	OPC 通信を利用するプログラム	OPC 通信を利用するとき に必要
DCOM サービス	TCP:20501～20550	OPC 通信を利用するプログラム	OPC 通信を利用するとき に必要

■ ファイル共有関連例外設定

ファイル共有関連例外設定について、次に示します。

表 3.2-5 ファイル共有関連例外設定

サービス名／実行ファイル名	プロトコル：ポート番号	機能名	備考
ファイルとプリンタの共有	TCP:139 UDP:137 UDP:138	NetBIOS	-
ファイルとプリンタの共有	TCP:445	Direct Hosting	NetBIOS を無効にした場合、 HOSTS ファイルや DNS への登録など、別途名前解決の手段が必要
ファイルとプリンタの共有	UDP:5355	LLMNR	-

■ Windows 関連例外設定

Windows 関連例外設定について、次に示します。

表 3.2-6 Windows 関連例外設定

サービス名／実行ファイル名	プロトコル：ポート番号	サーバ／ステーション
ICMP 有効化 (*1)	ICMP	ドメインコントローラ ファイルサーバ CENTUM VP ステーション
ケルベロス (Kerberos) 認証	TCP:88 UDP:88	ドメインコントローラ
LDAP(Active Directory)	TCP:389 UDP:389	ドメインコントローラ
DNS	TCP:53 UDP:53	ドメインコントローラ
Windows Time	UDP:123	UGS
ネットワーク探索	UDP:137 UDP:138 UDP:5355 UDP:3702 UDP:1900 TCP:2869 TCP:5358 TCP:5357 UDP:3702	CENTUM VP ステーション

*1: OS によっては、ICMPv4 と ICMPv6 の場合があります。

■ 注意事項

ドメイン環境では、ドメインコントローラのグループポリシーによって、この設定がドメインコントローラに設定されている情報で上書きされる場合があります。このような場合は、ドメインコントローラに設定されている情報を変更してください。

参照

ドメインコントローラで、クライアントコンピュータのセキュリティポリシーを一括して管理する設定については、以下を参照してください。

「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」 ページ 6-29

■ ユニキャスト応答の許可

IT セキュリティバージョン 2.0 からユニキャスト応答の許可を「無効」に設定します。マルチキャストやブロードキャストを使うアプリケーションは、応答を受信することができません。

補足

UGS では設定しません。

3.3 不要な Windows サービスの停止

不要な Windows サービスを停止することにより、権限を持たない者からの攻撃に対処し、セキュリティを強化できます。Windows サービスの脆弱性が悪用されると、本製品内のユーザ情報などが取得される場合や、本製品内の重要なデータが、漏えい、改ざん、または破壊される可能性があります。最悪の場合、攻撃者にドメインの管理者権限を取得される恐れがあります。

■ 不要な Windows サービス

IT セキュリティバージョン 2.0、IT セキュリティバージョン 1.0 における停止が可能な Windows サービスを次に示します。

表 3.3-1 Windows サービスの中の停止可能なサービス-IT セキュリティバージョン 2.0

サービス	Windows OS (*1)					
	10	7	2016	2012 R2	2008 R2	2008
Delivery Optimization (*2)	Yes (*3)	-	-	-	-	-
DHCP Client (*2)	No	Yes (*3)	No	Yes (*3) (*4)	Yes (*3)	Yes (*3)
Diagnostic Policy Service (*2)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)
Connected User Experiences and Telemetry (*2)	Yes (*3)	-	Yes (*3)	-	-	-
dmwappushsvc (*2)	Yes (*3)	-	Yes (*5)	-	-	-
Downloaded Maps Manager (*2)	Yes (*3)	-	Yes (*3)	-	-	-
IP Helper (*2)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)
IPsec Policy Agent (*2)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*3)
Offline Files (*2)	Yes (*5)	Yes (*3)	Yes (*7)	-	-	Yes (*5)
Program Compatibility Assistant Service (*2)	Yes (*3)	Yes (*3)	Yes (*3)	-	-	-
Remote Registry (*6)	Yes (*7)	Yes (*5)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)
Shell Hardware Detection (*8)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)	Yes (*3)
WebClient (*8)	Yes (*5)	Yes (*5)	-	-	-	-
Windows Error Reporting Service (*2)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*3)
Windows プッシュ通知システムサービス (*2)	Yes (*3)	-	Yes (*3)	-	-	-

*1: 10 : Windows 10

7 : Windows 7

2016 : Windows Server 2016

2012 R2 : Windows Server 2012 R2

2008 R2 : Windows Server 2008 R2

2008 : Windows Server 2008

Yes : 停止が可能なサービス

No : 停止してはいけないサービス

- : OS に存在しないサービス

*2: 本製品内では不要なサービスです。

*3: OS の初期状態で「スタートアップの種類」が「自動」であるため、IT セキュリティツールで「スタートアップの種類」を「無効」にする Windows サービス。

*4: コンピュータ切替型 UGS では、DHCP Client サービスを利用します。

*5: OS の初期状態で「スタートアップの種類」が「手動」であるため、IT セキュリティツールでは何もしない Windows サービス。

- *6: 機能的に利用しておらず、セキュリティ的にも問題があるので不要なサービスです。
 *7: OS の初期状態で「スタートアップの種類」が「無効」であるため、IT セキュリティツールでは何もしない Windows サービス。
 *8: 機能的に利用しておらず不要なサービスです。

表 3.3-2 Windows サービスの中の停止可能なサービス-IT セキュリティバージョン 1.0

サービス	Windows OS (*1)					
	10	7	2016	2012 R2	2008 R2	2008
DHCP Client (*2)	No	Yes (*6)	No	Yes (*6) (*3)	Yes (*6)	Yes (*6)
Windows Error Reporting Service (*4)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*6)
IP Helper (*4)	Yes (*6)	Yes (*6)	Yes (*6)	Yes (*6)	Yes (*6)	Yes (*6)
IPsec Policy Agent (*4)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*5)	Yes (*6)
Offline Files (*4)	Yes (*5)	Yes (*6)	Yes (*8)	-	-	Yes (*5)
Remote Registry (*7)	Yes (*8)	Yes (*5)	Yes (*6)	Yes (*6)	Yes (*6)	Yes (*6)
Shell Hardware Detection (*9)	Yes (*6)	Yes (*6)	Yes (*6)	Yes (*6)	Yes (*6)	Yes (*6)
WebClient (*9)	Yes (*5)	Yes (*5)	-	-	-	-

*1: 10 : Windows 10

7 : Windows 7

2016 : Windows Server 2016

2012 R2 : Windows Server 2012 R2

2008 R2 : Windows Server 2008 R2

2008 : Windows Server 2008

Yes : 停止が可能なサービス

No : 停止してはいけないサービス

- : OS に存在しないサービス

*2: 本製品内では DHCP サービスを利用しないので不要なサービスです。

*3: コンピュータ切替型 UGS では、DHCP Client サービスを利用します。

*4: 本製品内では不要なサービスです。

*5: OS の初期状態で「スタートアップの種類」が「手動」であるため、IT セキュリティツールで何もしない Windows サービス。

*6: OS の初期状態で「スタートアップの種類」が「自動」であるため、IT セキュリティツールで「スタートアップの種類」を「無効」にする Windows サービス。

*7: 機能的に利用しておらず、セキュリティ的にも問題があるので不要なサービスです。

*8: OS の初期状態で「スタートアップの種類」が「無効」であるため、IT セキュリティツールでは何もしない Windows サービス。

*9: 機能的に利用しておらず不要なサービスです。

■ 注意事項

ドメイン環境では、ドメインコントローラのグループポリシーによって、この設定がドメインコントローラに設定されている情報で上書きされる場合があります。このような場合は、ドメインコントローラに設定されている情報を変更してください。

参照

ドメインコントローラで、クライアントコンピュータのセキュリティポリシーを一括して管理する設定については、以下を参照してください。

「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」 ページ 6-29

3.4 IT セキュリティバージョン 2.0/1.0 共通の IT 環境の設定項目

ここでは、IT セキュリティバージョン 2.0/1.0 共通の IT 環境の設定項目について説明します。セキュリティ機能の導入に際しては、個々のシステムの状況に応じて適用できない場合も想定されますので、導入前に個別に導入の可否を検討してください。

3.4.1 NetBIOS over TCP/IP の無効化

NetBIOS を利用することにより、攻撃者が、ターゲットコンピュータ上で動作するサービス一覧やユーザー一覧を取得できる可能性があるため、NetBIOS を無効化することを推奨します。

■ 設定値

ネットワーク接続名称が「UACSEthernet」の場合、「NetBIOS over TCP/IP を無効にする」が設定されます。

■ 注意事項

NetBIOS over TCP/IP の無効化を実施するときは、次の点に注意してください。

- ・ コンピュータ名とステーション名を一致させてください。
- ・ DNS、または HOSTS ファイルで、コンピュータ名の名前解決をできるようにしてください。

3.4.2 BIOS による HDD パスワード機能

本機能はほとんどの PC に装備されている機能で、HDD を制御する ATA コマンドを利用した HDD を保護する機能です。通常の BIOS パスワード設定では、PC からハードディスクを外して、他の PC に接続すれば、HDD の中身を参照することができます。HDD パスワードは、HDD そのものにロックをかけるので、HDD を取り出して別のコンピュータに接続してもデータを読み出せません。もし、PC が盗難された場合でも、盗難にあった PC から本製品の重要なデータが漏えいする恐れがありません。HDD パスワードは、忘れてしまうと復旧不可能であり、また、PC 起動時には必ず入力が必要となるので、導入には細心の注意を払ってください。

本機能の有無および設定方法に関しては、PC メーカーにお問い合わせください。

3.5 IT セキュリティバージョン 2.0 におけるグループポリシー設定項目

ここでは、IT セキュリティバージョン 2.0 におけるグループポリシー設定項目について説明します。セキュリティ機能の導入に際しては、個々のシステムの状況に応じて適用できない場合も想定されますので、導入前に個別に導入の可否を検討してください。

3.5.1 ビルトイン Administrator アカウントの無効化またはユーザ名変更

Windows のインストール時に作成されるビルトインアカウントは、パスワードクラックなどの対象となりやすいので、ビルトイン Administrator アカウントを無効化してください。また、コンピュータ切替型 UGS の PC 冗長化プラットフォームには、あらかじめ管理作業、および保守作業用のアカウントがそれぞれ用意されています。これについてもユーザ名変更を推奨します。

■ 注意事項（ビルトイン Administrator アカウントを無効化する場合）

ビルトイン Administrator アカウントを無効化するときは、次の点に注意してください。

- ・ 管理者権限を持つユーザを作成したあと、ビルトイン Administrator アカウントの無効化を行ってください。
- ・ 管理者権限を持つユーザ名に、管理者を意味する root、su、admin などの単語が含まれないようにしてください。
- ・ 管理者権限を持つユーザは、運用上必須ですので確実に管理してください。
- ・ ドメイン環境では、ドメインコントローラのグループポリシーによって、この設定がドメインコントローラに設定されている情報で上書きされる場合があります。このような場合は、ドメインコントローラに設定されている情報を変更してください。

参照

ドメインコントローラで、クライアントコンピュータのセキュリティポリシーを一括して管理する設定については、以下を参照してください。

「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」ページ 6-29

■ コンピュータ切替型 UGS の PC 冗長化プラットフォームのユーザ名を変更する場合の注意事項

コンピュータ切替型 UGS の PC 冗長化プラットフォームには、デフォルトで「ADMINISTRATOR」と「PATCHUSER」の2つの管理者権限のユーザ名が用意されています。これらについてユーザ名を変更することを推奨します。ユーザ名は、冗長化管理ツールで変更できます。

補足

- ・ ADMINISTRATOR
冗長化管理ツールで PC 冗長化プラットフォームのメンテナンスサーバに接続し、管理作業を行うためのユーザです。
- ・ PATCHUSER
PC 冗長化プラットフォームにログオンし、パッチを適用するなどの保守作業を行うユーザです。

ユーザ名を変更するときは、次の点に注意してください。

- ・ 変更するユーザ名に、管理者を意味する「root」、「su」、および「admin」などの単語が含まれないようにしてください。
- ・ 管理作業や保守作業に必要なユーザ名となりますので、確実に管理してください。

参照

冗長化管理ツールでユーザ名を変更する方法については、以下を参照してください。

統合ゲートウェイステーションリファレンス（IM 33J20C10-01JA）の「D1.2.1 冗長化運転の設定—稼働側 UGS」の「■ アカウント設定」

3.5.2 ソフトウェア制限ポリシーの適用

ソフトウェア制限ポリシーは、プログラムの実行を制限する機能で、次のタイプで実行を制限できます。

- ・ パスの規則
- ・ ハッシュの規則
- ・ 証明書の規則
- ・ インターネットゾーンの規則

本製品では、パスの規則を利用し、利用者に対して、指定されたプログラム以外は実行できない環境を提供します。もし、有害なプログラムがテンポラリフォルダなどにコピーされても、不正に実行されることを防止します。

IT セキュリティツールで対応するタイプは、パスの規則です。この制限を行った場合、他製品と共存する際に他製品が動作しないことがあります。

■ 設定値

パスの規則に CENTUM VP のパスの規則を追加します。

具体的には、次のパスを追加します。

- ・ %ALLUSERSPROFILE%\Microsoft\Windows\Templates (*1)
- ・ %ALLUSERSPROFILE%\Templates
- ・ %ALLUSERSPROFILE%\Yokogawa\IA\iPCS\Products\ChronusENG\Data\Projects (*2)
- ・ %localappdata%\Microsoft\OneDrive*\FileSyncConfig.exe (*3)
- ・ %ProgramFiles% (*4)
- ・ %ProgramFiles(x86)% (*5)
- ・ %ProgramW6432% (*6)
- ・ %ProgramFiles%\Yokogawa\IA\iPCS\Platform\Security\PROGRAM
- ・ %ProgramFiles(x86)%\Yokogawa\IA\iPCS\Platform\Security\PROGRAM
- ・ %SystemRoot% (*7)
- ・ CENTUM VP インストールフォルダ (*8)

また、次のルールを削除します。

- ・ [専用ファイルの種類のプロパティ] から「lnk」と「mdb」を削除します。

*1: %ALLUSERSPROFILE%は、次のことを表します。システムドライブが、C ドライブの例です。
C:\ProgramData

*2: オートメションデザインマスターデータベースを保管する位置がデフォルトの場合

*3: Windows 10 のみ

*4: %ProgramFiles%は、次のことを表します。システムドライブが、C ドライブの例です。
C:\Program Files

*5: %ProgramFiles(x86)%は、次のことを表します。システムドライブが、C ドライブの例です。
C:\Program Files(x86)

*6: %ProgramW6432%は、次のことを表します。システムドライブが、C ドライブの例です。
C:\Program Files

*7: %SystemRoot%は、次のことを表します。システムドライブが、C ドライブの例です。
C:\Windows

*8: CENTUM VP インストールフォルダは、次のことを表します。システムドライブが、C ドライブの例です。
C:\CENTUMVP (デフォルト値)

■ 注意事項

本機能は、IT セキュリティツールにて設定できますが、ドメイン環境では、ドメインコントローラのグループポリシーによって、この設定がドメインコントローラに設定されている情報で上書きされる場合があります。このような場合は、ドメインコントローラに設定されている情報を変更してください。

参照

ドメインコントローラで、クライアントコンピュータのセキュリティポリシーを一括して管理する設定については、以下を参照してください。

「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」 ページ 6-29

● ソフトウェア制限ポリシーを適用した場合のツールや機能に関する注意事項

ソフトウェア制限ポリシーを適用した場合、次のツールは利用できません。

- ・ フィールドバスエンジニアリングツール
- ・ 機器管理ツール

テスト機能を利用し、FCS シミュレータを動作させる場合は、ソフトウェア制限ポリシーを適用すると、次の機能を有効にできません。

- ・ APCS のユーザカスタムアルゴリズム
- ・ プラント訓練システム (Exatif)
- ・ オフサイトブロック、拡張形スイッチ計器ブロック、またはバルブパターンモニタ

● ソフトウェア制限ポリシーを適用した場合の注意事項

ソフトウェア制限ポリシーを適用した場合には、次の注意事項があります。

- ・ 本製品のソフトウェア、またはサードパーティソフトウェアを、外部記憶メディアを使用してインストールする場合、管理者権限を持つユーザで PC にログオンし、セットアッププログラムを右クリックして「管理者として実行」を選択して実行してください。
- ・ 実行したいプログラムの拡張子が、bat、cmd、reg、または vbs の場合は、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」を選択して、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プログラムを実行してください。
- ・ Microsoft Excel、GSGW や SIOS に使用する OPC サーバ、またはサードパーティソフトウェアは、%ProgramFiles%または%ProgramFiles(x86)%にインストールしてください。
- ・ ディスプレイドライバ用アップデートプログラムは、C ドライブ直下にインストールされることがあります。ドライバをアップデートする場合、管理者権限を持つユーザで PC にログオンし、アップデートプログラムを右クリックして「管理者として実行」を選択して実行してください。
- ・ プロジェクトバックアップファイルを解凍する場合は、C ドライブ直下など製品インストールフォルダとは無関係の場所に解凍用の一時フォルダを作成し、そこにプロジェクトバックアップファイルである PJT.exe を格納してください。その後、PJT.exe ファイルを右クリックし、「管理者として実行」を選択して実行してください。
- ・ OPC クライアントをインストールする場合、管理者権限を持つユーザで PC にログオンし、OPC クライアントセットアッププログラムを右クリックして「管理者として実行」を選択して実行してください。
- ・ ユーザが作成した ActiveX コントロールは、<CENTUM VP インストールフォルダ>%this%users 以下に格納してください。

● ソフトウェア制限ポリシーを適用する前の注意事項

ソフトウェア制限ポリシーを適用する前に、次の点に注意してください。

- ・ Microsoft Excel、GSGW や SIOS に使用する OPC サーバ、ユーザが作成した ActiveX コントロールまたはサードパーティソフトウェアは、ソフトウェア制限ポリシーとして追加するパスの下フォルダにインストールしてください。ソフトウェア制限ポリシーとして追加するパスのフォルダ以外にインストールされている場合は、再インストールしてください。

3.5.3 StorageDevicePolicies 機能の適用

Windows の StorageDevicePolicies 機能を利用することにより、USB 接続による外部記憶メディアを読み取り専用のデバイスとして扱うことができます。本機能を利用することにより、不正なユーザによるデータの持ち出しを防止できます。また、本製品が提供する StorageDeviceCTL を利用することにより、利用者に対して一時的に書き込み権限を設定することも可能です。

参照

StorageDeviceCTL については、以下を参照してください。

「6.10 その他のユーティリティ」 ページ 6-34

■ 設定値

設定値は、次のとおりです。

表 3.5.3-1 設定値

ポリシー	設定値
リムーバブルディスク：書き込みアクセス権の拒否	有効

■ 注意事項

StorageDevicePolicies 機能を適用するときは、次の点に注意してください。

- ・ 本機能を Windows Server 2008 R2 に適用した場合、一時的な書き込み権限を設定する目的で StorageDeviceCTL を使用できません。読み取り専用状態を解除するためには、IT セキュリティツールを使い、詳細設定において [StorageDevicePolicies 機能の適用] チェックボックスをオフにして、再度実行する必要があります。また、本機能を適用しないで、外部記憶メディアを使ったデータ持ち出しを禁止するには、USB ポートにふたをかぶせるなどのセキュリティ対策が必要です。
- ・ ドメイン環境では、ドメインコントローラのグループポリシーによって、この設定がドメインコントローラに設定されている情報で上書きされる場合があります。このような場合は、ドメインコントローラに設定されている情報を変更してください。

参照

ドメインコントローラで、クライアントコンピュータのセキュリティポリシーを一括して管理する設定については、以下を参照してください。

「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」 ページ 6-29

3.5.4 USB ストレージデバイスの無効化

本機能により、USB メモリなどの USB ストレージデバイスが使用できなくなります。本機能を利用することにより、不正なユーザによるデータの持ち出しを防止できます。また、本製品が提供する StorageDeviceCTL を利用することにより、利用者に対して一時的に書き込み権限を設定することも可能です。

参照

StorageDeviceCTL については、以下を参照してください。

「6.10 その他のユーティリティ」 ページ 6-34

■ 設定値

設定値は、次のとおりです。

表 3.5.4-1 設定値

ポリシー	設定値
フロッピードライブ：実行アクセス権の拒否	有効
フロッピードライブ：読み取りアクセス権の拒否	有効
フロッピードライブ：書き込みアクセス権の拒否	有効
リムーバブルディスク：実行アクセス権の拒否	有効
リムーバブルディスク：読み取りアクセス権の拒否	有効
リムーバブルディスク：書き込みアクセス権の拒否	有効
WPD デバイス：読み取りアクセス権の拒否	有効
WPD デバイス：書き込みアクセス権の拒否	有効

■ 注意事項

USB ストレージデバイスの無効化をするときは、次の点に注意してください。

- ・ 本機能を Windows Server 2008 R2 に適用した場合、一時的な書き込み権限を設定する目的で StorageDeviceCTL を使用できません。無効化を解除するためには、IT セキュリティツールを使い、詳細設定において「USB ストレージデバイスの無効化」チェックボックスをオフにして、再度実行する必要があります。また、本機能を適用しないで、外部記憶メディアを使ったデータ持ち出しを禁止するには、USB ポートにふたをかぶせるなどのセキュリティ対策が必要です。
- ・ ドメイン環境では、ドメインコントローラのグループポリシーによって、この設定がドメインコントローラに設定されている情報で上書きされる場合があります。このような場合は、ドメインコントローラに設定されている情報を変更してください。

参照

ドメインコントローラで、クライアントコンピュータのセキュリティポリシーを一括して管理する設定については、以下を参照してください。

「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」 ページ 6-29

3.5.5 パスワードポリシーの適用

設定されたパスワードにより、ユーザ認証に対するセキュリティ強度が大きく変わります。パスワードポリシーを適用して、最低限のパスワード強度を確保することを推奨します。

■ 設定値

設定値は次のとおりです。

表 3.5.5-1 設定値

ポリシー	設定値
パスワードの長さ	12 文字以上
パスワードの変更禁止期間	1 日
パスワードの有効期間	70 日
パスワードの履歴を記録する	2 回
複雑さの要件を満たす必要があるパスワード	有効
暗号化を元に戻せる状態でパスワードを保存する	無効

■ 注意事項

パスワードポリシーを適用するときは、次の点に注意してください。

- ・ パスワードポリシーを厳しくすることにより、利用者のパスワード管理に対する負担が増加すると同時に、運用管理者が利用者のパスワードを管理する負担も増大します。
- ・ ドメイン環境では、ドメインコントローラのグループポリシーによって、この設定がドメインコントローラに設定されている情報で上書きされる場合があります。このような場合は、ドメインコントローラに設定されている情報を変更してください。

参照

ドメインコントローラで、クライアントコンピュータのセキュリティポリシーを一括して管理する設定については、以下を参照してください。

「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」 ページ 6-29

3.5.6 監査ポリシーの詳細な構成

アカウントログオン状況やセキュリティに関するイベントを収集することにより、システムの異常状態の早期検知と、セキュリティに関する問題が発生した場合の事故原因のトレースに有効なデータとなります。IT セキュリティバージョン 2.0 では、より詳細な監査ポリシーを設定できます。次に、各設定項目について説明します。

■ アカウントログオン

設定値は、次のとおりです。

表 3.5.6-1 設定値

ポリシー	設定値
資格情報の確認の監査	成功、失敗双方のチェックボックスをオン

■ アカウントの管理

設定値は、次のとおりです。

表 3.5.6-2 設定値

ポリシー	設定値
コンピューターアカウントの管理の監査	成功のチェックボックスをオン
その他のアカウント管理イベントの監査	成功、失敗双方のチェックボックスをオン
セキュリティグループの管理の監査	成功、失敗双方のチェックボックスをオン
ユーザーアカウントの管理の監査	成功、失敗双方のチェックボックスをオン

■ 詳細追跡

設定値は、次のとおりです。

表 3.5.6-3 設定値

ポリシー	設定値
プロセス作成の監査	成功のチェックボックスをオン
RPC イベントの監査	成功、失敗双方のチェックボックスをオフ (*1)

*1: ドメインコントローラとファイルサーバの場合、成功と失敗双方のチェックボックスがオンです。

■ DS アクセス

本設定は、ドメインコントローラ専用です。

設定値は、次のとおりです。

表 3.5.6-4 設定値

ポリシー	設定値
ディレクトリサービスアクセスの監査	成功、失敗双方のチェックボックスをオン
ディレクトリサービスの変更の監査	成功、失敗双方のチェックボックスをオン

■ ログオン／ログオフ

設定値は、次のとおりです。

表 3.5.6-5 設定値

ポリシー	設定値
アカウントロックアウトの監査	成功のチェックボックスをオン
ログオフの監査	成功のチェックボックスをオン
ログオンの監査	成功、失敗双方のチェックボックスをオン
その他のログオン/ログオフイベントの監査	成功、失敗双方のチェックボックスをオン
特殊なログオンの監査	成功のチェックボックスをオン

■ オブジェクトアクセス

設定値は、次のとおりです。

表 3.5.6-6 設定値

ポリシー	設定値
生成されたアプリケーションの監査	成功、失敗双方のチェックボックスをオフ (*1)
リムーバブル記憶域の監査	成功、失敗双方のチェックボックスをオン

*1: ドメインコントローラとファイルサーバの場合は、成功と失敗双方のチェックボックスがオンです。

■ ポリシーの変更

設定値は、次のとおりです。

表 3.5.6-7 設定値

ポリシー	設定値
監査ポリシーの変更の監査	成功、失敗双方のチェックボックスをオン
認証ポリシーの変更の監査	成功、失敗双方のチェックボックスをオン
フィルタリングプラットフォームポリシーの変更の監査	成功、失敗双方のチェックボックスをオン
MPSSVC ルールレベルポリシーの変更の監査	成功、失敗双方のチェックボックスをオン
その他のポリシー変更イベントの監査	成功、失敗双方のチェックボックスをオン

■ 特権の使用

設定値は、次のとおりです。

表 3.5.6-8 設定値

ポリシー	設定値
重要な特権の使用の監査	成功、失敗双方のチェックボックスをオン

■ システム

設定値は、次のとおりです。

表 3.5.6-9 設定値

ポリシー	設定値
その他のシステムイベントの監査	成功、失敗双方のチェックボックスをオン
セキュリティ状態の変更の監査	成功、失敗双方のチェックボックスをオン
セキュリティシステムの拡張の監査	成功、失敗双方のチェックボックスをオン
システムの整合性の監査	成功、失敗双方のチェックボックスをオン
IPsec ドライバー (*1)	成功、失敗双方のチェックボックスをオン

*1: 本設定はドメインコントローラ専用の設定

3.5.7 アカウントロックアウトポリシーの適用

オンラインクラッキングなどの攻撃から、本製品を守るために有効な機能です。

■ 設定値

設定値は次のとおりです。

表 3.5.7-1 設定値

ポリシー	設定値
アカウントのロックアウトのしきい値	10 回ログインに失敗
ロックアウトカウンターのリセット	15 分後
ロックアウト期間	15 分

補足

コンピュータ切替型 UGS の PC 冗長化プラットフォームのアカウントロックアウトポリシーの設定値は、上の表と同じです。なお、コンピュータ切替型 UGS の PC 冗長化プラットフォームのアカウントロックアウトポリシーは、常に設定されています。このアカウントロックアウトポリシーは、冗長化管理ツールで使用するユーザ認証に用いるものです。

■ 注意事項

アカウントロックアウトポリシーを適用するときは、次の点に注意してください。

- ・ 本機能を適用した場合、ログイン失敗を繰り返すと、設定されたロックアウトカウンターのリセット時間まで、そのユーザでログインできなくなります。
- ・ ドメイン環境では、ドメインコントローラのグループポリシーによって、この設定がドメインコントローラに設定されている情報で上書きされる場合があります。このような場合は、ドメインコントローラに設定されている情報を変更してください。
- ・ コンピュータ切替型 UGS を Windows ドメインに参加させる場合は、ドメインコントローラの「アカウントのロックアウトのしきい値」を「20 回ログインに失敗」に設定してください。

参照

ドメインコントローラで、クライアントコンピュータのセキュリティポリシーを一括して管理する設定については、以下を参照してください。

「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」 ページ 6-29

3.5.8 ユーザ権利の割り当て

ある特定の操作に対して、操作可能なユーザ／グループを設定します。

■ 設定値

設定値は、次のとおりです。

表 3.5.8-1 設定値

ポリシー	削除するグループ	追加するグループ
ネットワーク経由でのアクセス (*1)(*2)	登録されているアカウントすべて (*1)(*2)	Administrators (*1) (*2) Authenticated Users (*1) (*2) Enterprise Domain Controllers (*1)
ドメインにワークステーションを 追加 (*1)	Authenticated User	Administrators

*1: ドメインコントローラで設定します。

*2: UACS ステーションで設定します。

3.5.9 セキュリティオプション

個別のセキュリティ項目に対して、有効か無効かを設定します。

■ 設定値

設定値は、次のとおりです。

表 3.5.9-1 設定値

ポリシー	設定値
監査：監査ポリシーサブカテゴリの設定(Windows Vista 以降)を強制して、監査ポリシーカテゴリの設定を上書きする	有効
デバイス：ユーザーがプリンタードライバーをインストールできないようにする	有効
デバイス：CD-ROM へのアクセスを、ローカルログオンユーザーだけに制限する	有効
デバイス：フロッピーへのアクセスを、ローカルログオンユーザーだけに制限する	有効
ドメインコントローラー：Server Operators がタスクのスケジュールを割り当てるのを許可する (*1)	無効
ドメインコントローラー：コンピューターアカウントのパスワードの変更を拒否する (*1)	無効
ドメインメンバー：強力な(Windows 2000 かそれ以降のバージョン)セッションキーを必要とする	有効
対話型ログオン：セッションがロックされているときにユーザの情報を表示する	ユーザーの表示名、ドメインおよびユーザー名
対話型ログオン：最後のユーザー名を表示しない	有効
対話型ログオン：Ctrl + Alt + Del を必要としない	無効
対話型ログオン：コンピューターの非アクティブ状態の上限 (*2)	有効 900 秒
対話型ログオン：パスワードの期限が切れる前にユーザーに通知する	有効 14 日間
Microsoft ネットワークサーバー：クライアントが同意すれば、通信にデジタル署名を行う	有効
Microsoft ネットワークサーバー：サーバー SPN ターゲット名検証レベル	有効 クライアントによって提供される場合は受け入れる
MSS: (AutoReboot) Allow Windows to automatically restart after a system crash (recommended except for highly secure environments)	無効
MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)	有効 Highest protection, source routing is completely disabled
MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)	無効
MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	有効 3
ネットワークアクセス：SAM アカウントの匿名の列挙を許可しない	有効
ネットワークアクセス：SAM アカウントおよび共有の匿名の列挙を許可しない	有効

次に続く

表 3.5.9-1 設定値（前から続く）

ポリシー	設定値
ネットワークアクセス：ネットワーク認証のためにパスワードおよび資格情報を保存することを許可しない	有効
ネットワークアクセス：Everyone のアクセス許可を匿名ユーザーに適用する	無効
ネットワークセキュリティ：NTLM で Local System によるコンピューター ID の使用を許可する	有効
ネットワークセキュリティ：ログオン時間を経過した場合はユーザーを強制的にログオフさせる (*1)	有効
ネットワークセキュリティ：LocalSystem による NULL セッションフォールバックを許可する	無効
ネットワークセキュリティ：LAN Manager 認証レベル	有効 NTLMv2 応答のみ送信
ネットワークセキュリティ：NTLM SSP ベース(セキュア RPC を含む)のクライアント向け最小セッションセキュリティ	有効 ・ NTLMv2 セッションセキュリティが必要 ・ 128 ビット暗号化が必要 双方のチェックボックスをオン
ネットワークセキュリティ：NTLM SSP ベース(セキュア RPC を含む)のサーバー向け最小セッションセキュリティ	有効 ・ NTLMv2 セッションセキュリティが必要 ・ 128 ビット暗号化が必要 双方のチェックボックスをオン
ネットワークセキュリティ：次のパスワード変更時に LAN Manager のハッシュ値を保存しない	有効
シャットダウン：システムのシャットダウンにログオンを必要としない	無効
ユーザーアカウント制御：ビルトイン Administrator アカウントのための管理者承認モード	有効
ユーザーアカウント制御：管理者承認モードでの管理者に対する昇格時のプロンプトの動作	有効 セキュリティで保護されたデスクトップで同意を要求する

*1: ドメインコントローラで設定します。

*2: UACS ステーションで設定します。

■ 注意事項

セキュリティオプションで設定する MSS:で始まる 4 つの設定項目は、Windows Server 2008 以降の OS ではローカルグループポリシー管理エディタでは表示されません。gpresult コマンドを実行して、適用確認してください。

3.5.10 管理用テンプレート

グループポリシーにおける管理用テンプレートについて説明します。

■ 個人用設定（コントロールパネル）

● 設定値

設定値は、次のとおりです。

表 3.5.10-1 設定値

ポリシー	設定値
ロック画面カメラを有効にできないようにする	有効
ロック画面スライドショーを有効にできないようにする	有効

■ WLAN 設定（ネットワーク）

● 設定値

設定値は、次のとおりです。

表 3.5.10-2 設定値

ポリシー	設定値
推奨されるオープンホットスポット、連絡先によって共有されたネットワーク、有料サービスを提供するホットスポットに Windows が自動的に接続することを許可する	無効

■ プロセス作成の監査（システム）

● 設定値

設定値は、次のとおりです。

表 3.5.10-3 設定値

ポリシー	設定値
プロセス作成イベントにコマンドラインを含める	無効

補足

本設定を有効にすると、各プロセスのコマンドライン情報がプロセス作成の監査イベント 4688 "新しいプロセスの作成"の一部として、テキスト形式でセキュリティイベントログに記録されます。たとえば CreateCentumProcess ツールを使ってパスワードを設定した場合、引数で指定したパスワードがイベントログに記録されます。

■ グループポリシー（システム）

● 設定値

設定値は、次のとおりです。

表 3.5.10-4 設定値

ポリシー	設定値
レジストリポリシーの処理を構成する	グループポリシーオブジェクトが変更されていなくても処理する、のチェックボックスをオン

■ インターネット通信の管理（システム）

● 設定値

設定値は、次のとおりです。

表 3.5.10-5 設定値

ポリシー	設定値
ストアへのアクセスをオフにする	有効
プリンタードライバの HTTP 経由でのダウンロードをオフにする	有効
イベントビューアーの'Event.asp'リンクをオフにする	有効
Web 発行およびオンライン注文ウィザードのインターネットダウンロードをオフにする	有効
HTTP 経由の印刷をオフにする	有効
検索コンパニオンの内容ファイルの更新をオフにする	有効
ファイルおよびフォルダーの'Web に発行'タスクをオフにする	有効
Windows カスタマーエクスペリエンス向上プログラムをオフにする	有効
Windows Messenger カスタマーエクスペリエンス向上プログラムをオフにする	有効

■ ログオン（システム）

● 設定値

設定値は、次のとおりです。

表 3.5.10-6 設定値

ポリシー	設定値
ネットワークの選択の UI を表示しない	有効
ドメインに参加しているコンピューターに接続しているユーザーを列挙しない	有効
ドメインに参加しているコンピューターのローカルユーザーを列挙する	無効
ロック画面のアプリ通知をオフにする	有効

■ 軽減策オプション（システム）

● 設定値

設定値は、次のとおりです。

表 3.5.10-7 設定値

ポリシー	設定値
信頼されていないフォントのブロック	有効 信頼されていないフォントをブロックしてイベントログに記録する

● 注意事項

この設定を有効にすると、%Windir%\Font（通常は C:\Windows\Font）にインストールされていないフォントは使用できなくなります。その場合は、使用するフォントを当該フォルダにインストールしてください。フォントを右クリックして [Install] を選択すれば、インストールできます。

■ 電源の管理（システム）

● 設定値

設定値は、次のとおりです。

表 3.5.10-8 設定値

ポリシー	設定値
ディスプレイをオフにする（バッテリー使用時）(*1)	有効 0
ディスプレイをオフにする（電源接続時）(*1)	有効 0

*1: UACS ステーションでは、未定義に設定します。

■ ユーザープロファイル（システム）

● 設定値

設定値は、次のとおりです。

表 3.5.10-9 設定値

ポリシー	設定値
広告 ID を無効にする	有効

■ アプリのプライバシー（Windows コンポーネント）

● 設定値

設定値は、次のとおりです。

表 3.5.10-10 設定値

ポリシー	設定値
Windows アプリでアカウント情報にアクセスする	有効 強制的に拒否
Windows アプリで通話履歴にアクセスする	有効 強制的に拒否
Windows アプリで連絡先にアクセスする	有効 強制的に拒否
Windows アプリでメールにアクセスする	有効 強制的に拒否
Windows アプリで位置情報にアクセスする	有効 強制的に拒否
Windows アプリでメッセージングにアクセスする	有効 強制的に拒否
Windows アプリでモーションにアクセスする	有効 強制的に拒否

次に続く

表 3.5.10-10 設定値（前から続く）

ポリシー	設定値
Windows アプリでカレンダーにアクセスする	有効 強制的に拒否
Windows アプリでカメラにアクセスする	有効 強制的に拒否
Windows アプリでマイクにアクセスする	有効 強制的に拒否
Windows アプリで信頼済みデバイスにアクセスする	有効 強制的に拒否
Windows アプリで無線を制御する	有効 強制的に拒否
Windows アプリでデバイスと同期する	有効 強制的に拒否

■ アプリ実行時（Windows コンポーネント）

● 設定値

設定値は、次のとおりです。

表 3.5.10-11 設定値

ポリシー	設定値
ホストされているコンテンツから Windows ランタイム API でアクセスする Windows ストアアプリを起動できないようにする	有効

● 注意事項

Web コンテンツから Windows ランタイム API で直接アクセスする Windows ストアアプリが、起動できなくなります。

■ 自動再生のポリシー（Windows コンポーネント）

外部メディアから自動的にプログラムを実行されることを防止します。本設定は、USB メモリを介してコンピュータに感染するウィルス(USB ワーム)の対策に有効な手段です。

● 設定値

設定値は、次のとおりです。

表 3.5.10-12 設定値

ポリシー	設定値
自動再生機能をオフにする	有効 すべてのドライブ
ボリューム以外のデバイスの自動再生を許可しない	有効

● 注意事項

- ・ ドライブの自動起動機能を無効にした場合は、本製品のソフトウェアメディアを挿入しても、インストールメニューは立ち上がりません。
- ・ HIS セットを利用した場合はセキュリティモデルに関係なく、すべてのドライブの自動再生機能をオフにします。これは USB ワーム対策としての措置です。
- ・ ドメイン環境では、ドメインコントローラのグループポリシーによって、この設定がドメインコントローラに設定されている情報で上書きされる場合があります。このような場合は、ドメインコントローラに設定されている情報を変更してください。

参照

ドメインコントローラで、クライアントコンピュータのセキュリティポリシーを一括して管理する設定については、以下を参照してください。

「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」 ページ 6-29

■ クラウドコンテンツ（Windows コンポーネント）**● 設定値**

設定値は、次のとおりです。

表 3.5.10-13 設定値

ポリシー	設定値
Windows のヒントを表示しない	有効
Microsoft コンシューマーエクスペリエンスを無効にする	有効

■ データの収集とプレビュービルド（Windows コンポーネント）**● 設定値**

設定値は、次のとおりです。

表 3.5.10-14 設定値

ポリシー	設定値
利用統計情報の許可	有効 0-セキュリティ [Enterprise のみ]
プレリリースの機能または設定を無効にする	無効
フィードバックの通知を表示しない	有効
Insider ビルドに関するユーザーコントロールの切り替え	無効

■ イベントログサービス（Windows コンポーネント）**● 設定値**

設定値は、次のとおりです。

表 3.5.10-15 設定値

ポリシー	設定値
ログファイルの最大サイズ(KB)を指定する	有効 32768KB

■ エクスプローラー（Windows コンポーネント）**● 設定値**

設定値は、次のとおりです。

表 3.5.10-16 設定値

ポリシー	設定値
破損後のヒープ終了をオフにする	無効

■ ホームグループ (Windows コンポーネント)

● 設定値

設定値は、次のとおりです。

表 3.5.10-17 設定値

ポリシー	設定値
コンピューターがホームグループに参加できないようにする	有効

■ OneDrive (Windows コンポーネント)

● 設定値

設定値は、次のとおりです。

表 3.5.10-18 設定値

ポリシー	設定値
OneDrive をファイル記憶域として使用できないようにする	有効
ドキュメントを既定で OneDrive に保存する(既定でローカルコンピューターにドキュメントを保存する)	有効

■ リモートデスクトップサービス (Windows コンポーネント)

● 設定値

設定値は、次のとおりです。

表 3.5.10-19 設定値

ポリシー	設定値
パスワードの保存を許可しない	有効
ドライブのリダイレクトを許可しない (*1)	有効
接続するたびにパスワードを要求する (*2)	有効
セキュリティで保護された RPC 通信を要求する	有効
リモート接続にネットワークレベル認証を使用したユーザー認証を必要とする	有効
アクティブでアイドル状態になっているリモートデスクトップサービスセッションの制限時間を設定する (*2) (*3)	有効 1h

*1: UGS では設定しません。

*2: UACS ステーションで設定します。

*3: リモートデスクトップ接続した状態で、設定時間の間、無操作のとき、リモートデスクトップ接続が切断されます。

■ 検索 (Windows コンポーネント)

● 設定値

設定値は、次のとおりです。

表 3.5.10-20 設定値

ポリシー	設定値
Cortana を許可する	無効
Web を検索したり[検索]に Web の検索結果を表示したりしない	有効
従量制課金接続を使用して Web を検索したり[検索]に Web の検索結果を表示したりしない	有効

■ ソフトウェア保護プラットフォーム（Windows コンポーネント）

● 設定値

設定値は、次のとおりです。

表 3.5.10-21 設定値

ポリシー	設定値
KMS クライアントオンライン AVS 検証を無効にする	有効

■ ストア（Windows コンポーネント）

● 設定値

設定値は、次のとおりです。

表 3.5.10-22 設定値

ポリシー	設定値
Windows 8 コンピューターでの更新プログラムの自動ダウンロードをオフにする	有効
更新プログラムの自動ダウンロードおよび自動インストールをオフにする	有効
最新バージョンの Windows への更新プログラム提供をオフにする	有効
ストアアプリケーションをオフにする	有効

■ PC 設定の同期（Windows コンポーネント）

● 設定値

設定値は、次のとおりです。

表 3.5.10-23 設定値

ポリシー	設定値
アプリを同期しない	有効
スタート設定を同期しない	有効

■ Endpoint Protection（Windows コンポーネント）

● 設定値

設定値は、次のとおりです。

表 3.5.10-24 設定値

ポリシー	設定値
Endpoint Protection を無効にする	有効

■ Windows エラー報告（Windows コンポーネント）

● 設定値

設定値は、次のとおりです。

表 3.5.10-25 設定値

ポリシー	設定値
OS が生成するエラー報告のためにメモリダンプを自動送信する	無効

■ Windows ログオンのオプション（Windows コンポーネント）

● 設定値

設定値は、次のとおりです。

表 3.5.10-26 設定値

ポリシー	設定値
システムによる再起動後に自動的に対話ユーザーでサインインする	無効

3.5.11 ユーザ構成-管理用テンプレート

■ 通知（タスクバーとスタートメニュー）

● 設定値

設定値は、次のとおりです。

表 3.5.11-1 設定値

ポリシー	設定値
ロック画面のトースト通知をオフにする	有効

3.6 IT セキュリティバージョン 1.0 におけるグループポリシー設定項目

ここでは、IT セキュリティバージョン 1.0 におけるグループポリシー設定項目について説明します。セキュリティ機能の導入に際しては、個々のシステムの状況に応じて適用できない場合も想定されますので、導入前に個別に導入の可否を検討してください。

3.6.1 ビルトイン Administrator アカウントの無効化またはユーザ名変更

IT セキュリティバージョン 2.0 における注意事項と同じです。

参照

ビルトイン Administrator アカウントの無効化またはユーザ名変更における注意事項については、以下を参照してください。

「3.5.1 ビルトイン Administrator アカウントの無効化またはユーザ名変更」 ページ 3-22

3.6.2 直前ログオンユーザ名の非表示

最後にログオンしたユーザ名をログオンダイアログに表示しないことにより、システム内での有効ユーザ名の漏えいを防止します。

■ 注意事項

直前ログオンユーザ名を非表示にするときは、次の点に注意してください。

- ・ ログオン時には、毎回、ユーザ名の入力が必要となります。
- ・ ドメイン環境では、ドメインコントローラのグループポリシーによって、この設定がドメインコントローラに設定されている情報で上書きされる場合があります。このような場合は、ドメインコントローラに設定されている情報を変更してください。

参照

ドメインコントローラで、クライアントコンピュータのセキュリティポリシーを一括して管理する設定については、以下を参照してください。

「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」 ページ 6-29

3.6.3 ソフトウェア制限ポリシーの適用

IT セキュリティバージョン 2.0 における設定事項、および注意事項と同じです。

参照

ソフトウェア制限ポリシーの適用における設定事項については、以下を参照してください。

「■ 設定値」 ページ 3-23

ソフトウェア制限ポリシーの適用における注意事項については、以下を参照してください。

「■ 注意事項」 ページ 3-23

3.6.4 AutoRun の制限の適用

DVD-ROM などがドライブに挿入されてメディアから自動的にプログラムを実行させることを防止します。本設定は、USB メモリを介してコンピュータに感染するウィルス（USB ワーム）の対策に有効な手段です。

■ 設定値

すべてのドライブの自動起動機能を無効にします。

■ 注意事項

AutoRun の制限を行うときは、次の点に注意してください。

- ・ 本製品のソフトウェアのメディアを挿入しても、インストールメニューは立ち上がりません。
- ・ ドメイン環境では、ドメインコントローラのグループポリシーによって、この設定がドメインコントローラに設定されている情報で上書きされる場合があります。このような場合は、ドメインコントローラに設定されている情報を変更してください。

3.6.5 StorageDevicePolicies 機能の適用

IT セキュリティバージョン 2.0 における注意事項と同じです。

参照

StorageDevicePolicies 機能の適用における注意事項については、以下を参照してください。

「■ 注意事項」 ページ 3-25

3.6.6 USB ストレージデバイスの無効化

IT セキュリティバージョン 2.0 における注意事項と同じです。

参照

USB ストレージデバイスの無効化における注意事項については、以下を参照してください。

「■ 注意事項」 ページ 3-26

3.6.7 LAN Manager 認証レベルの変更

Windows は、下位互換のために LM 認証、NTLM 認証、NTLMv2 認証の認証方法を持っています。

本製品環境下では、NTLMv2 認証の使用を推奨します。LM 認証は、パスワード処理（ハッシュ処理）が非常に脆弱なため、推奨しません。

■ 設定値

設定値は、次のとおりです。

表 3.6.7-1 設定値

ポリシー	設定値
LAN Manager 認証レベルの変更	NTLMv2 応答のみを送信する
LM 認証のパスワードデータを保管しない	有効
RPC を含むクライアントベースの NTLM SSP 最小のセキュリティセッション	NTLMv2 セッションセキュリティが必要 128 ビット暗号化が必要
RPC を含むサーバーベースの NTLM SSP 最小のセキュリティセッション	NTLMv2 セッションセキュリティが必要 128 ビット暗号化が必要
Everyone のアクセス許可を匿名ユーザーに適用する	無効

■ 注意事項

- ・「RPC を含むクライアントベースの NTLM SSP 最小のセキュリティセッション」と「RPC を含むサーバーベースの NTLM SSP 最小のセキュリティセッション」は、すべての端末で同時に設定してください。
- ・ドメイン環境では、ドメインコントローラのグループポリシーによって、この設定がドメインコントローラに設定されている情報で上書きされる場合があります。このような場合は、ドメインコントローラに設定されている情報を変更してください。

参照

ドメインコントローラで、クライアントコンピュータのセキュリティポリシーを一括して管理する設定については、以下を参照してください。

「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」 ページ 6-29

3.6.8 パスワードポリシーの適用

設定されたパスワードにより、ユーザ認証に対するセキュリティ強度が大きく変わります。パスワードポリシーを適用して、最低限のパスワード強度を確保することを推奨します。

参照

パスワードポリシーの適用における注意事項については、以下を参照してください。

「■ 注意事項」 ページ 3-27

■ 設定値

設定値は次のとおりです。

表 3.6.8-1 設定値

ポリシー	設定値
パスワードの長さ	12 文字以上
パスワードの変更禁止期間	1 日
パスワードの有効期間	90 日
パスワードの履歴を記録する	24 パスワード数 (25 種類以上のパスワードが必要となります。)
複雑さの要件を満たす必要があるパスワード	有効
暗号化を元に戻せる状態でパスワードを保存する	無効

3.6.9 監査ポリシーの適用

アカウントログオン状況やセキュリティに関するイベントを収集することにより、システムの異常状態の早期検知と、セキュリティに関する問題が発生した場合の事故原因のトレースに有効なデータとなります。適切な監査ポリシーを設定することを推奨します。

■ 設定値

設定値は次のとおりです。

表 3.6.9-1 設定値

ポリシー	設定値
アカウントログオンイベントの監査	成功、失敗双方のチェックボックスをオン
アカウント管理の監査	成功、失敗双方のチェックボックスをオン
オブジェクトアクセスの監査	失敗のチェックボックスをオン
システムイベントの監査	成功、失敗双方のチェックボックスをオン
ディレクトリサービスのアクセスの監査	成功、失敗双方のチェックボックスをオン
プロセス追跡の監査	成功のチェックボックスをオン
ポリシーの変更の監査	成功、失敗双方のチェックボックスをオン
ログオンイベントの監査	成功、失敗双方のチェックボックスをオン
特権使用の監査	成功、失敗双方のチェックボックスをオン

■ 注意事項

監査ポリシーを適用するときは、次の点に注意してください。

- ・ 収集するイベントの種類を増加させると、システムのパフォーマンスに影響します。
- ・ 収集イベントの種類やシステムの運用により発生イベント数が異なります。システムの運用状態に合った、イベントの収集サイズを決定してください。
- ・ ドメイン環境では、ドメインコントローラのグループポリシーによって、この設定がドメインコントローラに設定されている情報で上書きされる場合があります。このような場合は、ドメインコントローラに設定されている情報を変更してください。

参照

ドメインコントローラで、クライアントコンピュータのセキュリティポリシーを一括して管理する設定については、以下を参照してください。

「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」ページ 6-29

3.6.10 アカウントロックアウトポリシーの適用

IT セキュリティバージョン 2.0 における設定事項、および注意事項と同じです。

参照

アカウントロックアウトポリシーの適用における設定事項については、以下を参照してください。

「■ 設定値」 ページ 3-30

アカウントロックアウトポリシーの適用における注意事項については、以下を参照してください。

「■ 注意事項」 ページ 3-30

4. セキュリティ機能の選定

セキュリティを設定するには、さまざまな項目を考慮する必要があります。ここでは、考慮する項目とセキュリティを設定する際に参考となるモデルケースを説明します。

4.1 セキュリティを設定する前に考慮する項目

ここでは、考慮すべき項目を説明します。

■ セキュリティ機能を決定する上で考慮が必要な項目

次の項目について、運用を考慮した上で、決定する必要があります。

なお、これらの項目については、本製品のソフトウェアのインストールを開始する前に決定しておいてください。

- ・ IT セキュリティバージョン
- ・ セキュリティモデル
- ・ Windows のユーザ管理方法
- ・ ユーザ認証モード

● IT セキュリティバージョンの選択

セキュリティ対策の設定範囲によって、次のいずれかを選択します。

表 4.1-1 IT セキュリティバージョンの選択

IT セキュリティバージョン	選択基準
2.0	CENTUM VP R6.03 までのセキュリティ対策に比べ、より多くのセキュリティポリシーを含みます。また、グループポリシーにおける管理用テンプレートが、セキュリティ設定対象に含まれます。 IT セキュリティバージョン 2.0 から、従来モデルは提供されません。
1.0	CENTUM VP R6.03 までのセキュリティ対策です。

● セキュリティモデルの選択

セキュリティモデルを次の 3 つから選択します。

表 4.1-2 セキュリティモデルの選択

セキュリティモデル	選択基準
従来モデル	R6.03 までの CENTUM プロジェクトからバージョンアップ、またはレベジョンアップする際に IT セキュリティ設定を変更したくない場合や、Windows のユーザを複数人で共有するときなどに選択します。 従来モデルは、IT セキュリティバージョン 1.0 でのみ選択可能です。本モデルを選択すると、情報漏えいやワームおよびウィルスからの攻撃に弱くなります。
標準モデル（推奨）	特別な理由がないかぎり、本セキュリティモデルを選択することを推奨します。 本製品の運用や他システムとの連携を考慮して、システムに対して必要最低限のセキュリティを設定したモデルです。
強固モデル	標準モデルより強固なセキュリティが必要な場合に選択します。 導入に関しては、当社にご相談ください。

● Windows のユーザ管理方法

Windows のユーザ管理は、システム 規模やシステム 構成により、次の 3 つから選択します。

表 4.1-3 ユーザ管理の選択

ユーザ管理の方法	選択基準
スタンドアロン管理	比較的規模の小さなシステムでの利用に適しています。この方式を選択した場合、システム内のユーザとパスワードをすべての PC で一致させる必要があります。

次に続く

表 4.1-3 ユーザ管理の選択（前から続く）

ユーザ管理の方法	選択基準
ドメイン管理	システム内でユーザの一元管理を行う場合に適しています。この方式を選択した場合、システムの構築にあたり、専用のドメインコントローラを新規に立ち上げることを推奨します。
併用管理	ドメインコントローラによるユーザの一元管理に加え、特定ユーザに対して個別の PC へのアクセスを許可する場合などに適しています。

● ユーザ認証モード

運用状況やセキュリティポリシーに合わせて、次のいずれかを選択します。

表 4.1-4 ユーザ認証モードの選択

ユーザ認証モード	選択基準
CENTUM 認証モード	R4.03 より前のレビジョンと同様の管理方法です。Windows のユーザと CENTUM のユーザを別に管理する場合に選択します。
Windows 認証モード	Windows のユーザと操作監視やシステムの構築のためのユーザを連携して管理する場合に選択します。 厳格なセキュリティが必要な場合に適しています。

Windows 認証モードを選択すると、1 度のユーザ認証で HIS を操作することが可能になります。これをシングルサインオンといいます。

シングルサインオンには、次の 2 つがあります。HIS やシステム生成機能を搭載した PC 単位で、次のタイプを選択することができます。

表 4.1-5 シングルサインオンの選択

タイプ	特長
Windows タイプシングルサインオン	ユーザを切り替えるには、Windows をログオフし、別のユーザ名でログオンします。
HIS タイプシングルサインオン	常時操作監視に使用される HIS での使用に適しています。 ユーザを切り替えるには、Windows をログオフせずに、ユーザインダイアログを使用します。 したがって、操作監視機能に関する権限は切り替わりますが、Windows の権限（例：スタートメニューなど）は、自動ログオンに利用されるユーザ（OFFUSER）のままです。 なお、Windows をログオフした場合は、PC を再起動し、ログオン状態にしてください。

■ セキュリティを設定する上での注意事項

セキュリティを設定する上での注意事項を次に示します。

表 4.1-6 セキュリティを設定する上での注意事項

セキュリティ機能	考慮項目
スクリーンセーバ機能	Windows 認証モードの HIS タイプシングルサインオンを選択した場合、スクリーンセーバ機能の「パスワードによる保護機能」は利用できません。
CTM_PROCESS/ UGS_PROCESS/LIC_PROCESS/ RDC_PROCESS/OFFUSER のパスワード	CTM_PROCESS/UGS_PROCESS/LIC_PROCESS/RDC_PROCESS/OFFUSER (*1) のパスワードを変更する場合は、ユーザ管理方法に関係なく、CTM_PROCESS/UGS_PROCESS/LIC_PROCESS/RDC_PROCESS/OFFUSER (*1) が存在するすべてのコンピュータのパスワードを一致させる必要があります。
オペレーションキーボードのユーザ切り替え機能	ユーザ認証モードで、Windows 認証モードを利用して、ユーザ単位のアクセスコントロールを検討している場合、オペレーションキーボードのユーザ切り替え機能を利用するとユーザの権限を一時的に昇格できユーザ単位のアクセスコントロールに不向きです。利用する場合は、考慮して利用してください。
ファイルサーバ／ドメインコントローラに IT セキュリティを設定する場合	ファイルサーバ／ドメインコントローラに対して、IT セキュリティツールを利用する場合、NET Framework 3.0 以上 (*2) をインストールする必要があります。

- *1: OFFUSER は、Windows 認証モードの HIS タイプシングルサインオンで動作させる場合のみ対応が必要となります。
- *2: CENTUM VP インストールメディアには、.NET Framework3.5 SP1 が含まれています。

4.2 モデルケース

モデルケースとして、次のケースの推奨設定を示します。

- ・ CENTUM VP を新規で導入するケース
- ・ プロジェクトデータベースをファイルサーバに置くケース
- ・ CENTUM VP システム内のみでユーザの一元管理を行うケース
- ・ 複数の CENTUM VP システムでユーザの一元管理を行うケース
- ・ IT セキュリティ未対応の当社製品がシステムに含まれているケース
- ・ セキュリティを優先したシステムを構築するケース
- ・ IT セキュリティバージョン 1.0 相当の当社製品がシステムに含まれているケース

■ CENTUM VP を新規で導入するケース（HIS 台数が少なく、ユーザの一元管理が不要な場合）

表 4.2-1 CENTUM VP を新規で導入するケース

セキュリティ機能	推奨設定
IT セキュリティバージョンの選択	2.0
セキュリティモデル	標準モデル
Windows のユーザ管理	スタンドアロン管理
ユーザ認証モード	Windows 認証モード
ソフトウェア制限ポリシー	不適用
スクリーンセーバ機能	[パスワードによる保護機能] を無効にする。
CTM_PROCESS/OFFUSER のパスワード変更機能	対応不要
オペレーションキーボードのユーザ切り替え機能	ユーザ切り替え機能を有効にする。
ファイルサーバ	ファイルサーバを構築した場合の IT セキュリティは標準モデル（スタンドアロン管理）を適用
ドメインコントローラ	不要

■ プロジェクトデータベースをファイルサーバに置くケース

表 4.2-2 プロジェクトデータベースをファイルサーバに置くケース

セキュリティ機能	推奨設定
IT セキュリティバージョンの選択	2.0
セキュリティモデル	標準モデル
Windows のユーザ管理	スタンドアロン管理
ユーザ認証モード	Windows 認証モード
ソフトウェア制限ポリシー	適用
スクリーンセーバ機能	[パスワードによる保護機能] を無効にする。
CTM_PROCESS/OFFUSER のパスワード変更機能	対応不要
オペレーションキーボードのユーザ切り替え機能	ユーザ切り替え機能を有効にする。
ファイルサーバ	標準モデル（スタンドアロン管理）
ドメインコントローラ	不要

■ CENTUM VP システム内のみでユーザの一元管理を行うケース

表 4.2-3 CENTUM VP システム内のみでユーザの一元管理を行うケース

セキュリティ機能	推奨設定
IT セキュリティバージョンの選択	2.0
セキュリティモデル	標準モデル
Windows のユーザ管理	ドメイン管理
ユーザ認証モード	Windows 認証モード
ソフトウェア制限ポリシー	適用
スクリーンセーバ機能	[パスワードによる保護機能] を無効にする。
CTM_PROCESS/OFFUSER のパスワード変更機能	対応不要
オペレーションキーボードのユーザ切り替え機能	ユーザ切り替え機能を無効にする。
ファイルサーバ	10 台以上の HIS やシステム生成機能が搭載された PC が存在する場合は構築します。構築した場合の IT セキュリティは標準モデル（ドメイン・併用管理）を適用。
ドメインコントローラ	新規に構築（IT セキュリティは、標準モデル（ドメイン・併用管理）の適用）

■ 複数の CENTUM VP システムでユーザの一元管理を行うケース

表 4.2-4 複数の CENTUM VP システムでユーザの一元管理を行うケース

セキュリティ機能	推奨設定
IT セキュリティバージョンの選択	2.0
セキュリティモデル	標準モデル
Windows のユーザ管理	併用管理
ユーザ認証モード	Windows 認証モード
ソフトウェア制限ポリシー	適用
スクリーンセーバ機能	[パスワードによる保護機能] を無効にする。
CTM_PROCESS/OFFUSER のパスワード変更機能	対応不要
オペレーションキーボードのユーザ切り替え機能	ユーザ切り替え機能を無効にする。
ファイルサーバ	10 台以上の HIS やシステム生成機能が搭載された PC が存在する場合は構築します。構築した場合の IT セキュリティは標準モデル（ドメイン・併用管理）を適用
ドメインコントローラ	既存サーバの再利用（IT セキュリティは、標準モデル（ドメイン・併用管理）の適用、または導入ユーザのセキュリティポリシーに順ずる。）

■ IT セキュリティ未対応の当社製品がシステムに含まれているケース

表 4.2-5 IT セキュリティ未対応の当社製品がシステムに含まれているケース

セキュリティ機能	推奨設定
IT セキュリティバージョンの選択	1.0(*1)
セキュリティモデル	従来モデル
Windows のユーザ管理	スタンドアロン管理
ユーザ認証モード	CENTUM 認証モード
ソフトウェア制限ポリシー	不適用

次に続く

表 4.2-5 IT セキュリティ未対応の当社製品がシステムに含まれているケース（前から続く）

セキュリティ機能	推奨設定
スクリーンセーバ機能	[パスワードによる保護機能] を無効にする。
CTM_PROCESS/OFFUSER のパスワード変更機能	対応不要
オペレーションキーボードのユーザ切り替え機能	ユーザ切り替え機能を有効にする。
ファイルサーバ	10 台以上の HIS やシステム生成機能が搭載された PC が存在する場合は構築します。IT セキュリティは従来モデルを適用
ドメインコントローラ	不要

*1: セキュリティモデルとして従来モデルを選択するためには、IT セキュリティバージョンを 1.0 にしてください。

■ セキュリティを優先したシステムを構築するケース

セキュリティを優先したシステムを構築する場合は、運用を十分に考慮して、検討してください。

表 4.2-6 セキュリティを優先したシステムを構築するケース

セキュリティ機能	推奨設定
IT セキュリティバージョンの選択	2.0
セキュリティモデル	強固モデル
Windows のユーザ管理	ドメイン管理
ユーザ認証モード	Windows 認証モード
ソフトウェア制限ポリシー	適用
スクリーンセーバ機能	[パスワードによる保護機能] を有効にする。
CTM_PROCESS/OFFUSER のパスワード変更機能	対応必要
オペレーションキーボードのユーザ切り替え機能	ユーザ切り替え機能を無効にする。
ファイルサーバ	強固モデル（ドメイン・併用管理）
ドメインコントローラ	新規に構築（IT セキュリティは、強固モデル（ドメイン・併用管理）の適用）

5. 運用上の注意事項

本製品の運用を行う上でのセキュリティに関する注意事項を説明します。

5.1 Windows のアカウント管理

Windows のアカウント管理は、セキュリティ機能を導入する前に構築されたシステムで、よく利用されているユーザアカウントを共有した運用を考慮して、共通アカウント管理と個別アカウント管理の 2 つのアカウント管理を想定しています。

■ 共通アカウント管理と個別アカウント管理

共通アカウント管理と個別アカウント管理の違いを示します。

表 5.1-1 共通アカウント管理と個別アカウント管理

アカウント管理方法	運用形態	運用上の利便性		セキュリティ強度	
共通アカウント管理	1 つの Windwos アカウントを複数のユーザで共有する運用形態。	高い	セキュリティ機能を導入する前に構築されたシステムと同等の操作性。	低い	匿名性が高く不利。
個別アカウント管理	1 ユーザに 1 つの Windows アカウントを配布する運用形態。	低い	要員交代時に Windows ログオフ／ログオンが必要になり、従来の運用に比べ煩雑。	高い	ユーザごとのアクセス管理ができ有利。

5.1.1 共通アカウント管理

共通アカウント管理は、セキュリティ機能を導入する前に構築されたシステムのアカウント管理と同様なので、運用上の利便性は高いです。しかし、セキュリティ上の観点からみると匿名性が高くセキュリティ強度が低くなるので、要員教育や運用環境のセキュリティにも十分に配慮して運用してください。

■ アカウントの使用

共通アカウントで運用する場合、権限者ごとにグループ分けを行い、グループ内で共通アカウントを利用する運用を推奨します。権限者ごとにグループ分けを行うことにより、本製品に対して権限を持たない者の操作を防止することができます。事故発生時のトレースに関しても利用者グループを絞り込むことが可能となるので、すべてのユーザで共通アカウントを利用した場合より有効なトレースデータになると考えられます。

■ パスワード管理

セキュリティを考慮すると、パスワードは定期的に変更することを推奨します。パスワード変更を定期的に行うことにより、パスワードクラッキング攻撃に対処できます。共通アカウントで運用する場合は、共通アカウントを利用するメンバが変更されたタイミングでもパスワード変更することを推奨します。パスワード変更することにより、旧関係者からの不正アクセスを防止します。

■ 自動ログオン機能

自動ログオン機能を利用する場合、自動ログオン機能に設定するユーザは、CTM_OPERATOR グループに属しているアカウントを設定することを推奨します。他ユーザグループに所属しているアカウントを設定した場合、CENTUM VP システムに対して権限を持たない者によって不用意にシステム生成機能などを利用されることが想定されます。

5.1.2 個別アカウント管理

個別アカウント管理は、PC の使用者を特定することにより、アカウントに対する権限を必要最低限にすることができます。また、事故発生時にも使用者を特定できるため、有効なトレースが可能となります。ただし、個別アカウント管理は、要員交代時に Windows のログオフ／ログオンの作業が発生するなど、従来の運用と異なる点もあるので、導入時には十分な考慮が必要です。

■ アカウントメンテナンス

ユーザに権限の変更が生じた場合、すみやかにアカウント権限を変更することを推奨します。

すみやかなアカウントメンテナンスを行うことにより、以前に権限を持っていたユーザからの不正アクセスや攻撃者からの予期しない攻撃に対処できます。

たとえば、対象ユーザが退職した場合はアカウントを削除する、メンテナンス担当者の担当範囲に変更があった場合は、所属グループを変更するなどの作業が考えられます。

■ パスワード管理

セキュリティを考慮し、パスワードは定期的に変更することを推奨します。パスワード変更を定期的に行うことにより、パスワードクラッキング攻撃に対処します。

5.1.3 共通アカウント管理／個別アカウント管理で共通な注意事項

共通アカウント管理／個別アカウント管理のいずれにも共通する注意事項を列挙します。

■ システム監視

システム監視を定期的に行うことを推奨します。監視を定期的に行うことにより、システムの異常を早期に発見でき、事故の予兆や事故の早期発見につながります。なお、異常が発見された場合は、ネットワーク管理者または有識者に相談してすみやかに適切な対応を行ってください。

■ スタンドアロン管理によるアカウント管理

アカウントをスタンドアロン管理で管理する場合、ユーザが利用する PC およびプロジェクトデータベースが存在するシステム 生成機能を搭載した PC のすべてに、同一ユーザのアカウントを作成する必要がある、登録されたアカウントのパスワードも統一する必要があります。なお、パスワード変更を行う場合も、同一アカウントが登録されている全 PC を、共通の新しいパスワードへ変更する必要があります。

■ ドメイン管理によるアカウント管理

ドメインコントローラと本製品の各 PC の時刻が大きく異なる（デフォルト値は、5 分以上）場合、ドメイン環境下での認証機能が正常に動作しません。ドメインコントローラと各 PC との時間のずれには注意してください。

■ CTM_MAINTENANCE グループ

CTM_MAINTENANCE は、メンテナンスのためのグループで管理者権限を含む非常に強力な権限を持ちます。通常運用時は、CTM_MAINTENANCE に所属するアカウントは、無効なアカウントとして扱い、利用のタイミングでアカウントを有効化する運用が望ましいです。また、アカウントを有効にするタイミングでアカウントに対して有効期限を設定する運用なども、セキュリティ的には有効な手段です。

■ OPC 利用可能ユーザ

OPC 利用可能ユーザは、DCOM 機能をリモートサイトで利用できるので、システムへの影響を低減するために、OPC 利用可能ユーザの登録に関しては、必要最低限にすることが望ましいです。また、対象ユーザがプログラムのみの利用の場合、ログオン権限を削除することも有効な手段です。

■ Windows の管理者権限があるグループのユーザの作成方法に関して

CTM_ENGINEER_ADM/CTM_ENGINEER_ADM_LCL/CTM_MAINTENANCE/
CTM_MAINTENANCE_LCL に所属するユーザを作成する場合、所属するグループのほかに、Administrators グループ、または Domain Admins グループのいずれかにも所属している必要があります。

5.2 関連プログラム

関連プログラムとして、次について説明します。

- ・ Windows のセキュリティパッチ
- ・ アンチウィルスソフトウェア

■ Windows のセキュリティパッチ

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ただくことが前提です。

当社では、本製品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。

0-day attack で注視されるように、ソフトウェアにセキュリティ上の脆弱性（セキュリティホール）が発見（公表）されてから、その脆弱性を悪用する攻撃が行われるまでの期間が短くなってきています。

また、本製品に対して、セキュリティパッチやサービスパックを適用した場合、既存のセキュリティ設定（ファイアウォールの設定やローカルセキュリティ設定）が変更される場合があります。セキュリティパッチやサービスパックを適用した場合、従来のセキュリティ設定が有効であることを確認してください。

■ アンチウィルスソフトウェア

本製品内の PC、ドメインコントローラに関しては、当社が検証済みのアンチウィルスソフトウェアをインストールして運用することを推奨します。アンチウィルスソフトウェアの適用については、当社サービスまでお問い合わせください。

アンチウィルスソフトウェアの検索エンジンやパターンファイルを更新した場合、PC の再起動が必要となったり、PC の動作に予期せぬ影響を及ぼしたりする可能性があります。更新の場合は、テスト用の PC など事前に動作確認を行うなど、十分に留意してください。

5.3 システム導入時および運用時のセキュリティに関する注意事項

ここでは、システムを導入する時、および運用する時のセキュリティに関する一般的な注意事項を説明します。

■ HIS やシステム生成機能を搭載した PC へリモートアクセスする場合

HIS-TSE などを利用して HIS やシステム生成機能を搭載した PC にリモートアクセスする場合には、接続時の認証に、Windows の機能を利用した 二要素認証を導入できます。

■ セキュリティ区画への立ち入り通知

本製品を、セキュリティ区画に設置した場合、ログインする前の利用者に対して、次の方法で、今後の操作はセキュリティ区画へ立ち入る作業であることを通知できます。通知が必要であれば、設定してください。

通知方法は、Windows のコントロールパネルのローカルセキュリティポリシーで、[ローカルポリシー] – [セキュリティオプション] を選択したのち、次のポリシーを設定してください。

- ・ [対話型ログオン：ログオン時のユーザへのメッセージのタイトル]
- ・ [対話型ログオン：ログオン時のユーザへのメッセージのテキスト]

■ 脆弱性が疑われる事象を発見した場合

本製品を使用中に、当社製品の脆弱性が疑われる事象を発見した場合は、当社にご連絡ください。

6. セキュリティ設定のためのユーティリティ

ここでは、セキュリティ設定のための IT セキュリティツールとその他のユーティリティについて説明します。

6.1 IT セキュリティツール

IT セキュリティツールは、当社製品向けのセキュリティ設定ツールです。本製品がインストールされているコンピュータにセキュリティ対策を実施するには、このツールを使用する必要があります。

IT セキュリティツールは、選択した IT セキュリティバージョン、セキュリティモデル、およびユーザ管理方法に基づいて、コンピュータのセキュリティ設定を自動的に適用します。

重要

- ・ HIS/ENG をファイルサーバに変更する場合など、コンピュータの役割を変更するときは、OS の再インストールから行ってください。
- ・ HIS/ENG に対してファイルサーバ用の IT セキュリティを設定した場合など、コンピュータに対して異なる IT セキュリティを設定してしまったときは、OS の再インストールから行ってください。

■ IT セキュリティツールの機能概要

IT セキュリティツールの機能について、次の表で説明します。

表 6.1-1 IT セキュリティツールの機能

機能	説明
設定情報	IT セキュリティツールによって設定されたセキュリティ設定の概要を表示します。
設定	「IT セキュリティバージョン」の選択により、セキュリティモデル、ユーザ管理の設定を行います。
保存	OS のセキュリティ設定を保存します。保存時に、パスワード（暗号鍵）で暗号化します。
復元	保存したセキュリティ設定から OS のセキュリティ設定を復元します。
パスワード（暗号鍵）変更	保存したセキュリティ設定のパスワード（暗号鍵）を変更します。パスワード（暗号鍵）を定期的に変更したいときなどに利用します。
インポート/エクスポート	IT セキュリティツールで設定した情報をファイルにエクスポートします。また、エクスポートされたファイルをインポートします。

IT セキュリティバージョン 2.0 を選択している場合は、セキュリティモデルは標準モデルのみ選択可能です。また、ユーザ管理は、ドメイン管理、併用管理、スタンドアロン管理のいずれか選択可能です。

IT セキュリティバージョン 1.0 を選択している場合は、セキュリティモデルは、標準モデル、従来モデルのいずれか選択可能です。また、ユーザ管理は、ドメイン管理、併用管理、スタンドアロン管理のいずれか選択可能です。

IT セキュリティ設定画面のデフォルト表示は、新規インストール時や他のレビジョンからのレビジョンアップで異なります。

■ IT セキュリティバージョン

IT セキュリティバージョンは、各セキュリティモデルのセキュリティ設定の強化、設定範囲の拡張度合いによって分類されます。

● IT セキュリティバージョン 2.0

IT セキュリティバージョン 1.0 を見直し、より多くのセキュリティ対策を含みます。

● IT セキュリティバージョン 1.0

CENTUM VP R6.03 までのセキュリティ対策です。

■ セキュリティモデル

セキュリティモデルは、設定されるセキュリティ強度に応じて、次のモデルから選択します。

● 標準モデル

ユーザ認証によるアクセス制限、DCOM 設定、ファイアウォールを有効化し、システムへの直接攻撃を防ぐことができます。

補足

標準モデルよりさらにセキュリティを強化したい場合には、強固モデルを使用できます。強固モデルを使用する場合は、当社にご相談ください。

● 従来モデル

セキュリティを強化しないモデルです。CENTUM CS 3000 R3 以前との互換性、および IT セキュリティツールを使用しない他の当社製品との統合を重視する場合は、このモデルを使用します。このモデルを選択すると、Windows のファイアウォールは無効になるため、情報漏洩、ワーム、およびウイルスに対するこのモデルの脆弱性に伴う影響を考慮する必要があります。

■ ユーザ管理

標準モデルのセキュリティ設定には、ユーザ管理方法の違いによって、次の 3 つのタイプがあります。従来モデルで選択できるユーザ管理方法は、スタンドアロン管理のみです。

● ドメイン管理

Windows ドメインコントローラでユーザとグループのアカウントを管理する場合に選択してください。

● スタンドアロン管理

Windows ドメインコントローラを使用せず、コンピュータごとにユーザとグループのアカウントを管理する場合に選択してください。この場合、ユーザアカウントはコンピュータごとに作成しますが、関連する全コンピュータのグループとユーザの管理を一致させる必要があります。

● 併用管理

併用管理とは、ドメイン管理とスタンドアロン管理を併用するユーザ管理方法です。主たるユーザ管理はドメイン管理で行いますが、通常運用時にもワークグループ管理のような運用が想定される場合に併用管理を使用します。利便性は向上しますが、ドメイン管理を使用する場合に比べて、ローカルコンピュータの管理者権限でできることが増えるため、セキュリティは低くなります。

6.2 IT セキュリティツールを実行する

参照

IT セキュリティツール実行については、以下を参照してください。

CENTUM VP インストール手順 (IM 33J01C10-01JA) の「B4.7 IT セキュリティを設定する」の「■ IT セキュリティツールを実行する」

6.3 IT セキュリティ設定を変更する

一度、設定したセキュリティ設定の変更について説明します。
設定の変更には、次のものがあります。

- ・ セキュリティモデルの変更
- ・ IT セキュリティバージョンの変更
- ・ ユーザ管理方法の変更
- ・ 個別設定項目の変更

重要 IT セキュリティ設定を変更する前に、現在のセキュリティ設定をバックアップしてください。

参照 セキュリティ設定のバックアップについては、以下を参照してください。
「6.4 IT セキュリティ設定を保存する」 ページ 6-13

6.3.1 CENTUM VP ソフトウェアをインストールしたコンピュータの場合

本製品のソフトウェアをインストールしたコンピュータの場合の変更手順を説明します。

■ 注意事項

本製品のソフトウェアをインストールしたコンピュータで、IT セキュリティ設定を変更する場合の注意事項を説明します。

● 旧 IT セキュリティ対応製品と共存している場合のモデル変更

旧 IT セキュリティ対応製品と共存している場合のセキュリティモデル変更は、旧 IT セキュリティ対応製品の MAINTENANCE 権限が必要となります。他製品の MAINTENANCE と CTM_MAINTENANCE の両方に属しているユーザで、セキュリティモデル変更を行ってください。セキュリティモデル変更の際は、まず旧 IT セキュリティ対応製品のセキュリティモデルを変更し、その後 CENTUM VP のセキュリティモデルを変更してください。

旧 IT セキュリティ対応製品のバージョンは、次のとおりです。

- ・ CENTUM VP R5.01 より前
- ・ PRM R3.10 より前
- ・ ProSafe-RS R3.01 より前
- ・ Exaopc R3.70 より前
- ・ Exapilot R3.90 より前
- ・ Exaplog R3.40 より前

これらの製品と共存している場合の IT セキュリティバージョンは、1.0 です。IT セキュリティバージョンの確認は、現在の IT セキュリティ設定情報ダイアログで確認できます。

参照

現在の IT セキュリティ設定情報ダイアログを呼び出す操作については、以下を参照してください。

「6.8 IT セキュリティツールで設定した情報を参照する」 ページ 6-28

● ユーザ認証モードが Windows 認証モードで、従来モデルに変更

従来モデルに変更する前のシステム構成で、ユーザ認証モードが Windows 認証モードで運用されていた場合、CENTUM 認証モードに変更してください。

参照

CENTUM 認証モードの設定については、以下を参照してください。

CENTUM VP インストール手順 (IM 33J01C10-01JA) の「B4.11.1 CENTUM 認証モードの設定をする」

● ユーザ認証モードが Windows 認証モードで、ユーザ管理を変更

ユーザ管理をスタンドアロン管理からドメイン管理／併用管理やドメイン管理／併用管理からスタンドアロン管理に変更した場合は、Windows 認証モードで動作させる設定が再度必要となります。

参照

Windows 認証モードの設定については、以下を参照してください。

CENTUM VP インストール手順 (IM 33J01C10-01JA) の「C4. CENTUM 認証モードから Windows 認証モードに変更をする」

● ユーザ管理の変更を伴わない場合

コンピュータのドメイン参加、不参加の状態は、現状のまま IT セキュリティ設定を実施してください。

● **従来モデル／標準モデル（スタンドアロン管理）から標準モデル（併用管理／ドメイン管理）に変更**

IT セキュリティ設定をする前に、コンピュータをドメインに参加させてください。

● **標準モデル（併用管理／ドメイン管理）から従来モデル／標準モデル（スタンドアロン管理）に変更**

IT セキュリティ設定をする前に、コンピュータをドメインから離脱させてください。

● **IT セキュリティバージョンのみを変更**

IT セキュリティバージョンの変更操作以外の追加手順はありません。

● **IT セキュリティバージョンとセキュリティモデル／ユーザ管理を同時に変更**

実行中のアプリケーションをすべて終了してください。

重要

IT セキュリティ設定を行う前に、現在の IT セキュリティ設定をバックアップしてください。

■ **IT セキュリティ設定を変更できるユーザ**

IT セキュリティ設定を変更するには、セキュリティモデル、ユーザ管理方法によって必要な権限を持ったユーザで実施する必要があります。

表 6.3.1-1 IT セキュリティ設定を変更できるユーザ

現在のセキュリティモデル／ユーザ管理方法		設定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
従来モデル		ローカルの Administrators グループかつローカルの CTM_MAINTENANCE グループに属するローカルユーザ	ドメインの Domain Admins グループかつドメインの CTM_MAINTENANCE グループに属するドメインユーザ (*1)
			ローカルの Administrators グループかつローカルの CTM_MAINTENANCE グループに属するローカルユーザ (*1) (*2)
			ローカルの Administrators グループかつローカルの CTM_MAINTENANCE グループに属するドメインユーザ (*1)
標準モデル	スタンドアロン管理	ローカルの Administrators グループかつローカルの CTM_MAINTENANCE_LCL グループに属するローカルユーザ (*3)	ローカルの Administrators グループかつローカルの CTM_MAINTENANCE グループに属するローカルユーザ (*1) (*2)
			ローカルの Administrators グループかつローカルの CTM_MAINTENANCE グループに属するドメインユーザ (*1)
			ローカルの Administrators グループかつローカルの CTM_MAINTENANCE_LCL グループに属するドメインユーザ (*1)
	併用管理／ドメイン管理		ドメインの Domain Admins グループかつドメインの CTM_MAINTENANCE グループに属するドメインユーザ (*1)
			ローカルの Administrators グループかつローカルの CTM_MAINTENANCE グループに属するローカルユーザ (*1) (*2)
			ローカルの Administrators グループかつローカルの CTM_MAINTENANCE_LCL グループに属するドメインユーザ (*1)

*1: コンピュータがドメインに参加した状態でログオンしてください。

*2: 実行中に、ドメイン管理者のユーザ名、パスワードの入力が必要です。

*3: IT セキュリティ設定を変更する前に、コンピュータをドメインから離脱させてください。

■ 変更手順

1. IT セキュリティ設定を変更するユーザでログオンしてください。
2. 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ください。
3. [設定] をクリックしてください。
4. 変更したいセキュリティモデル、ユーザ管理方法を選択してください。
以降は、通常の IT セキュリティの設定と同じです。

参照

IT セキュリティツールの実行については、以下を参照してください。

CENTUM VP インストール手順 (IM 33J01C10-01JA) の「B4.7 IT セキュリティを設定する」の「■ IT セキュリティツールを実行する」

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」

6.3.2 ファイルサーバやドメインコントローラの場合

ファイルサーバ専用コンピュータやドメインコントローラの場合の変更手順を説明します。

重要

ファイルサーバ、ドメインコントローラで IT セキュリティ設定を変更するには、IT セキュリティが設定されない状態で保存されたセキュリティ設定データを用意してください。

■ ファイルサーバの IT セキュリティを変更できるユーザ

ファイルサーバにおける IT セキュリティ設定を変更するには、セキュリティモデル、ユーザ管理方法によって必要な権限を持ったユーザで実施する必要があります。

表 6.3.2-1 セキュリティ設定を変更できるユーザ

現在のセキュリティモデル／ユーザ管理方法		設定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 併用管理／ドメイン管理
従来モデル		ローカルの Administrators グループに属するローカルユーザ	ドメインの Domain Admins グループかつドメインの CTM_MAINTENANCE グループに属するドメインユーザ (*1)
			ローカルの Administrators グループかつローカルの CTM_MAINTENANCE グループに属するローカルユーザ (*1) (*2)
			ローカルの Administrators グループかつローカルの CTM_MAINTENANCE グループに属するドメインユーザ (*1)
標準モデル	スタンドアロン管理	ローカルの Administrators グループかつローカルの CTM_MAINTENANCE グループに属するローカルユーザ	ローカルの Administrators グループかつローカルの CTM_MAINTENANCE グループに属するローカルユーザ (*2) (*3)
			ローカルの Administrators グループかつローカルの CTM_MAINTENANCE グループに属するドメインユーザ (*2) (*3)
	併用管理／ドメイン管理	ローカルの Administrators グループかつローカルの CTM_MAINTENANCE_LCL グループに属するローカルユーザ (*4)	ドメインの Domain Admins グループかつドメインの CTM_MAINTENANCE グループに属するドメインユーザ (*1)
			ローカルの Administrators グループかつローカルの CTM_MAINTENANCE_LCL グループに属するローカルユーザ (*1) (*2)
			ローカルの Administrators グループかつローカルの CTM_MAINTENANCE_LCL グループに属するドメインユーザ (*1)

*1: コンピュータがドメインに参加した状態でログオンしてください。

*2: 実行中にドメインユーザのユーザ名とパスワードの入力が必要です。

*3: ドメインに参加していない状態で実施する作業とドメインに参加したあとで実施する作業があります。

*4: IT セキュリティ設定を変更する前に、コンピュータをドメインから離脱させてください。

■ ドメインコントローラの IT セキュリティを変更できるユーザ

ドメインコントローラの IT セキュリティを変更する場合、ドメインの Domain Admins グループかつドメインの CTM_MAINTENANCE グループに属するドメインユーザでログオンしてください。

■ 変更手順

変更手順には、次の 3 種類があります。

- ・ 基本手順
- ・ ファイルサーバで標準モデル（スタンドアロン管理）から標準モデル（併用管理・ドメイン管理）に変更する手順
- ・ ファイルサーバで標準モデル（併用管理・ドメイン管理）から標準モデル（スタンドアロン管理）に変更する手順

● セキュリティ設定変更の基本手順

1. セキュリティ設定を変更するユーザでログインしてください。
2. 本製品のソフトウェアメディアからインストールメニューを起動し、[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、IT セキュリティツールを起動してください。
3. [復元] をクリックしてください。
4. IT セキュリティ設定前のセキュリティ設定が保存されたファイルを選択し、セキュリティ設定の復元をしてください。
ファイルサーバについては、現在、ドメインに参加していないのであれば、スタンドアロンの状態で保存した初期化データを使用します。ドメインに参加している場合は、ドメイン参加後に保存した初期化データを使用します。
5. 復元が終わったら、コンピュータを再起動してください。
6. ファイルサーバで、ドメインへの参加状態を変更する場合、参加、離脱作業をしてください。
7. 再度、インストールメニューを起動し、[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、IT セキュリティツールを起動してください。
8. [設定] をクリックしてください。
9. 目的のセキュリティモデル、ユーザ管理を選択してください。
以降は、初回のセキュリティ設定と同じです。

参照

インストールメニューの起動方法については、以下を参照してください。

CENTUM VP インストール手順（IM 33J01C10-01JA）の「B4.6 CENTUM VP ソフトウェアのインストールをする」

CENTUM VP ソフトウェアをインストールしないでファイルサーバ、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。

「6.5.2 ファイルサーバやドメインコントローラの場合」 ページ 6-21

CENTUM VP ソフトウェアをインストールしていないファイルサーバの初回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。

CENTUM VP インストール手順（IM 33J01C10-01JA）の「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」

CENTUM VP ソフトウェアをインストールしていないドメインコントローラの初回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。

CENTUM VP インストール手順（IM 33J01C10-01JA）の「B2.4 ドメインコントローラのセキュリティを設定する」

● ファイルサーバで標準モデル（スタンドアロン管理）から標準モデル（併用管理・ドメイン管理）に変更する場合

この変更の場合、ファイルサーバをドメインに参加させたあとはセキュリティ関連の設定が変更されるため、あらためて、セキュリティ設定を保存する必要があります。次の手順に従って、作業してください。

1. ローカルの Administrators グループかつローカルの CTM_MAINTENANCE グループに属する管理者ユーザでログインしてください。

2. 本製品のソフトウェアメディアからインストールメニューを起動してください。
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、IT セキュリティツールを起動してください。
4. 初回設定前（コンピュータがドメインに参加していないとき）に保存しておいたデータを復元してください。
5. 再起動後、コンピュータをドメインに参加させてください。
6. 手順 1 と同じ管理者ユーザでログオンしてください。
7. インストールメニューを起動し、[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。
8. [保存] をクリックしてください。
9. ドメイン参加後の初期化データとしてセキュリティ設定を保存してください。
10. IT セキュリティツールのメニューで、[設定] をクリックしてください。
11. ファイルサーバの目的のモデル・ユーザ管理を選択し、実行してください。
12. IT セキュリティ適用後、コンピュータを再起動してください。

● ファイルサーバで標準モデル（併用管理・ドメイン管理）から標準モデル（スタンドアロン管理）に変更する場合

この変更の場合、ドメイン離脱のタイミングが基本の手順と異なります。

1. ローカルの Administrators グループかつローカルの CTM_MAINTENANCE_LCL グループに属する管理者ユーザでログオンしてください。
2. コンピュータをドメインから離脱させてください。
3. コンピュータを再起動し、手順 1 で示した管理者ユーザでログオンしてください。
4. 本製品のソフトウェアメディアからインストールメニューを起動してください。
5. [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、IT セキュリティツールを起動してください。
6. [復元] をクリックし、初回設定前（コンピュータをドメインに参加させる前）に保存しておいたデータを復元してください。
7. コンピュータを再起動してください。
8. 手順 1 と同じ管理者ユーザでログオンしてください。
9. 本製品のソフトウェアメディアからインストールメニューを起動してください。
10. [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）] から IT セキュリティツールを起動してください。
11. [設定] をクリックし、ファイルサーバの標準・スタンドアロンを選択し、実行してください。
12. IT セキュリティ適用後、コンピュータを再起動してください。

■ IT セキュリティバージョンの変更手順

ファイルサーバやドメインコントローラで、IT セキュリティバージョン 1.0 から IT セキュリティバージョン 2.0 へ変更する場合は、次の手順に従ってください。

1. 本製品のソフトウェアメディアからインストールメニューを起動して、IT セキュリティツールを起動してください。
2. [復元] をクリックして、運用開始前に IT セキュリティツールの保存機能で保存した初期状態を復元してください。復元が終わったら、コンピュータを再起動してください。
3. 手順 1 を実施してください。
以降、手順 4～手順 5 は、IT セキュリティツールで実施してください。
4. [保存] をクリックして、復元した状態を保存してください。

5. [設定] をクリックして、任意のセキュリティモデルを設定してください。

6.4 IT セキュリティ設定を保存する

保存機能でローカルコンピュータのセキュリティ設定を保存できます。

ここで保存した IT セキュリティ設定は、必要に応じて IT セキュリティツールの復元機能で復元させることができます。

■ セキュリティ設定を保存できるユーザ

IT セキュリティ設定を保存するには、セキュリティモデルやユーザ管理方法によって、必要な権限を持ったユーザで実施する必要があります。

表 6.4-1 セキュリティ設定を保存できるユーザ

現在の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	併用管理／ドメイン管理
ローカルの Administrators グループに属するユーザ	ローカルの Administrators グループかつローカルの CTM_MAINTENANCE グループに属するユーザ	ローカルの Administrators グループかつローカルの CTM_MAINTENANCE_LCL グループに属するユーザ
		ドメインの Domain Admins グループかつドメインの CTM_MAINTENANCE グループに属するユーザ

■ セキュリティ設定を保存したファイル

セキュリティ設定を保存すると、拡張子が .hed と .csf の 2 つのファイルが作成されます。復元時には、これら 2 つのファイルが共に必要になります。

6.4.1 CENTUM VP ソフトウェアをインストールしたコンピュータの場合

本製品のソフトウェアをインストールしたコンピュータでの保存手順を説明します。

■ 保存手順

1. 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ください。
2. 「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。

図 6.4.1-1 保存先の選択

3. 保存先を指定し、その他必要事項を入力してください。
「識別名」と「ファイルバージョン」は、オプション入力項目です。
4. 「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。

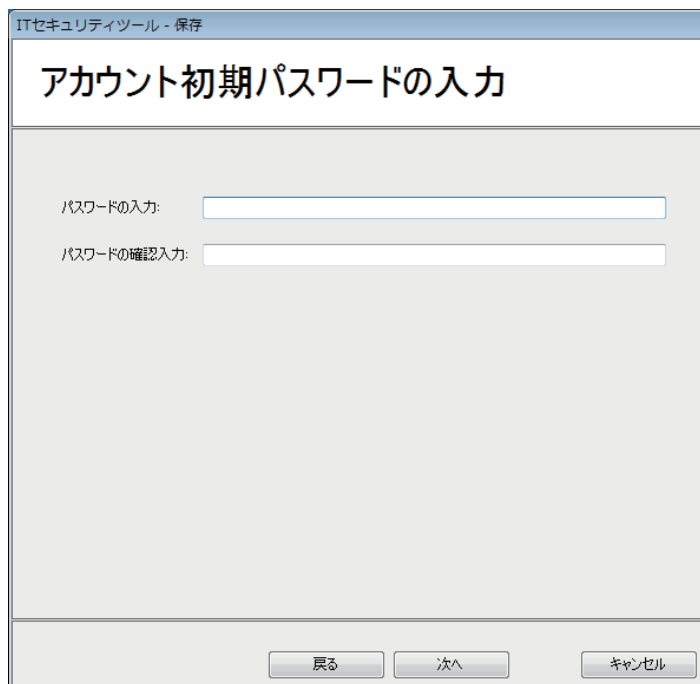


図 6.4.1-2 アカウント初期パスワードの入力

5. 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。

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。復元時に保存したアカウントが存在しない場合は、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時のパスワードポリシーを満たさないときは、アカウント復元時にエラーとなります。

アカウントに初期パスワードとして、このパスワードが設定されるため、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の変更が求められます。

保存データを暗号化するためのパスワードを入力するページが表示されます。

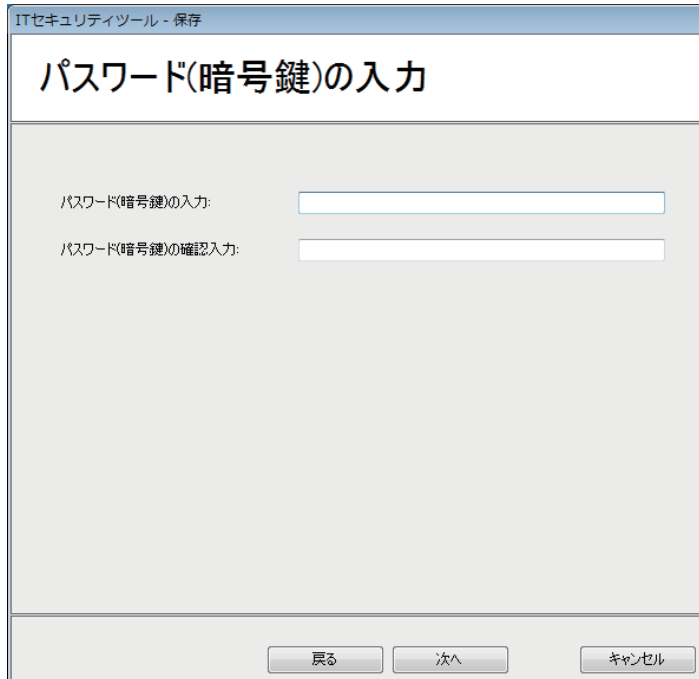


図 6.4.1-3 パスワード（暗号鍵）の入力

6. 暗号鍵を入力して「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。
全角は使用できません。

7. 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。
8. 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。

重要

保存に失敗した項目が表示された場合、当社窓口にご連絡してください。

参照

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」

6.4.2 ファイルサーバやドメインコントローラの場合

ファイルサーバ専用コンピュータやドメインコントローラで IT セキュリティ設定を保存するには、本製品のソフトウェアメディアからインストールメニューを起動し、[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、IT セキュリティツールを起動します。以降は、本製品のソフトウェアをインストールしたコンピュータの場合と同じです。

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保存できません。ローカルグループポリシーの設定値を保存します。

参照

インストールメニューの起動方法については、以下を参照してください。

CENTUM VP インストール手順（IM 33J01C10-01JA）の「B4.6 CENTUM VP ソフトウェアのインストールをする」

6.5 IT セキュリティ設定を復元する

ローカルコンピュータのセキュリティ設定を、保存機能を使って保存したセキュリティ設定に復元します。

■ 復元前の準備

復元データのユーザ管理方法に合わせて、ドメインの参加、離脱を行います。従来モデル、標準モデルのスタンドアロン管理の場合は、ドメインを離脱してください。標準モデルのドメイン管理や併用管理の場合は、ドメインに参加してください。

■ セキュリティ設定を復元できるユーザ

IT セキュリティ設定を復元するには、セキュリティモデルやユーザ管理方法によって、必要な権限を持ったユーザで実施する必要があります。

表 6.5-1 セキュリティ設定を復元できるユーザ

復元データの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	併用管理／ドメイン管理
ローカルの Administrators グループに属するユーザ	ローカルの Administrators グループかつローカルの CTM_MAINTENANCE グループに属するユーザ	ローカルの Administrators グループかつローカルの CTM_MAINTENANCE_LCL グループに属するユーザ (*1)
		ドメインの Domain Admins グループかつドメインの CTM_MAINTENANCE グループに属するユーザ

*1: CTM_MAINTENANCE_LCL グループがローカルに存在しない場合（復元作業前のセキュリティモデルとユーザ管理方法が、従来モデル、または標準モデルでスタンドアロン管理の場合）は、下の欄のグループに所属するユーザで実施してください。

6.5.1 CENTUM VP ソフトウェアをインストールしたコンピュータの場合

本製品のソフトウェアをインストールしたコンピュータでの復元手順を説明します。

重要

IT セキュリティツールの保存機能でコンピュータのセキュリティ設定を保存した場合は、保存状態と同一のユーザ管理状態に復元する必要があります。

■ 復元手順

1. 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ください。
2. [復元] をクリックしてください。
設定ファイルの選択ページが表示されます。

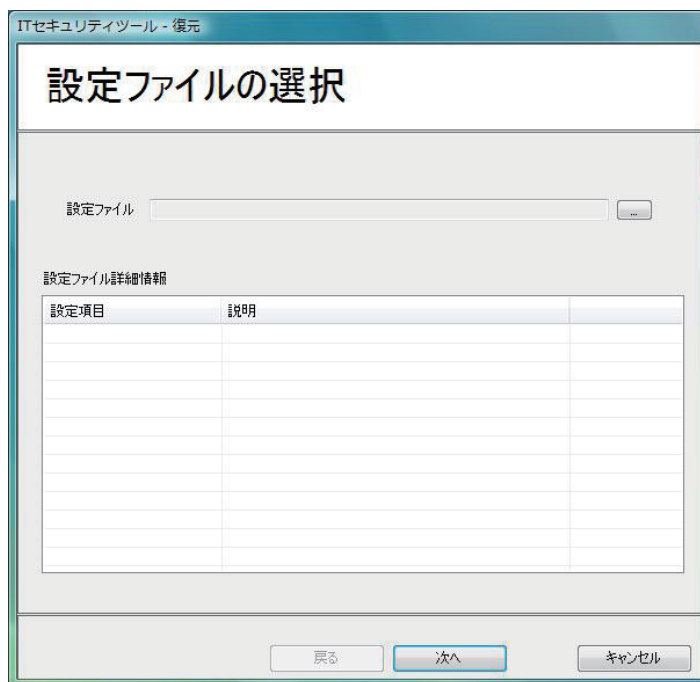


図 6.5.1-1 設定ファイルの選択

3. [設定ファイル] 欄の横にある [...] をクリックしてください。
開くダイアログが表示されます。
4. 復元に使用する設定ファイルを選択し、[開く] をクリックしてください。

補足

保存時に作成したファイルのうち拡張子が.hed のファイルを選択します。

選択したファイルを読み込むためのパスワード（暗号鍵）を入力するダイアログが表示されます。

5. 保存時に設定したパスワード（暗号鍵）を入力し、[OK] をクリックしてください。
選択したファイルが復元できると、設定ファイルの選択ページに詳細情報が表示されます。
6. [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。

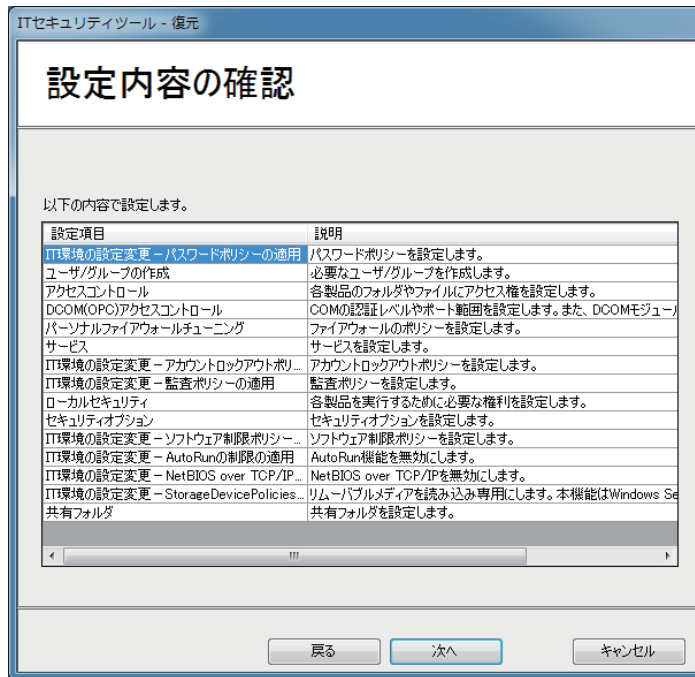


図 6.5.1-2 設定内容の確認

補足

ここに表示されている項目は、保存されたセキュリティ設定を復元する際にアクセスする項目を表しています。説明欄の表示は、すべて設定する方向の記述となっていますが、この内容が、そのまま設定される訳ではありません。項目ごとに、設定する、設定しないの属性を持っていますが、画面には表示されませんので注意してください。

7. 設定内容を確認し、[次へ] をクリックしてください。
設定が完了すると完了ページが表示されます。

補足

設定に失敗した項目がある場合、何に失敗したのかが表示されます。

8. [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。
9. [終了] をクリックして、IT セキュリティツールを終了してください。

重要

設定に失敗した項目が表示された場合、当社窓口にご連絡してください。

参照

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」

6.5.2 ファイルサーバやドメインコントローラの場合

ファイルサーバ専用コンピュータやドメインコントローラで IT セキュリティ設定を復元するには、本製品のソフトウェアメディアからインストールメニューを起動し、[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、IT セキュリティツールを起動します。以降は、本製品のソフトウェアをインストールしたコンピュータの場合と同じです。

参照

インストールメニューの起動方法については、以下を参照してください。

CENTUM VP インストール手順（IM 33J01C10-01JA）の「B4.6 CENTUM VP ソフトウェアのインストールをする」

6.6 セキュリティ設定ファイルのパスワードを変更する

IT セキュリティツールで使用する、セキュリティ設定ファイルのパスワード（暗号鍵）を変更できます。

6.6.1 CENTUM VP ソフトウェアをインストールしたコンピュータの場合

本製品のソフトウェアをインストールしたコンピュータでのパスワード変更手順を説明します。

パスワードを変更するときは、同じファイル名の.hed と.csf の2つのファイルを1セットとして扱います。パスワードの変更対象として「1セット」、または「複数セット」のどちらかを選択します。「複数セット」を選択した場合は、指定したフォルダのすべてのファイルのパスワードが変更されます。

■ 変更手順

1. CTM_MAINTENANCE グループに属するユーザでログオンし、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ください。
2. [パスワード（暗号鍵）変更] をクリックしてください。
セキュリティ情報バックアップファイルの選択ページが表示されます。

図 6.6.1-1 バックアップファイルの選択

3. 変更対象を選択するときは、次の手順に従います。
 - 1セットを変更する場合の手順
[変更対象] で [1セット] を選択し、変更対象ファイルセットと、変更後のファイルセットを出力するフォルダを選択してください。変更対象ファイルセットとして.hed ファイルを選択してください。
 - 複数セットを変更する場合の手順
[変更対象] で [複数セット] を選択し、変更対象ファイルセットが保存されているフォルダと、変更後のファイルセットを出力するフォルダを選択してください。
4. [次へ] をクリックしてください。
パスワード（暗号鍵）の変更ページが表示されます。

図 6.6.1-2 パスワード（暗号鍵）の変更

5. 旧パスワードと新しいパスワードを入力し、[次へ] をクリックしてください。
パスワード（暗号鍵）の変更が完了すると完了ページが表示されます。
6. [完了] をクリックしてください。
7. 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。

参照

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」

6.6.2 ファイルサーバやドメインコントローラの場合

ファイルサーバ専用コンピュータやドメインコントローラでの、セキュリティ設定ファイルのパスワード変更手順を説明します。

■ 変更手順

1. CTM_MAINTENANCE グループに属するユーザでログオンしてください。
2. 本製品のソフトウェアメディアからインストールメニューを起動し、[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、IT セキュリティツールを起動してください。
以降は、本製品のソフトウェアをインストールしたコンピュータと同じです。

参照

インストールメニューの起動方法については、以下を参照してください。

CENTUM VP インストール手順（IM 33J01C10-01JA）の「B4.6 CENTUM VP ソフトウェアのインストールをする」

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 セキュリティツールで設定した設定項目をエクスポート、インポートすることができます。IT セキュリティツールには、セキュリティ設定の保存機能、および復元機能がありますが、OS 依存の設定項目については、異なる OS への復元ができません。異なる OS への設定の場合は、エクスポート／インポート機能を使用します。

■ エクスポート手順-IT セキュリティツール

1. CTM_MAINTENANCE グループに属するユーザでログオンしてください。
2. 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ください。

補足

ファイルサーバやドメインコントローラの場合、本製品のソフトウェアメディアからインストールメニューを起動し、[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、IT セキュリティツールを起動してください。

3. メインメニュー画面の [インポート/エクスポート] をクリックしてください。
設定項目選択状態のインポート/エクスポートダイアログが表示されます。
4. 「操作の選択」で [エクスポート] を選択してください。
「ファイルの選択」のテキストボックスに、エクスポート先のデフォルトファイル名が表示されます。デフォルトファイル以外のファイル名にする場合は、直接ファイル名を変更するかテキストボックスの右にあるボタンを押してファイルを直接指定してください。

補足

ファイルの拡張子には、xml を指定してください。xml 形式以外の拡張子を指定した場合、ファイル名の末尾に拡張子「.xml」が自動的に付加されます。

5. [実行] をクリックしてください。
指定したファイルに情報が書き込まれ、設定項目選択状態のインポート/エクスポートダイアログは閉じます。

参照

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」

■ エクスポート手順-ITSecuritySettingItemExport.exe

R6.04 より前に設定した IT セキュリティ設定の状態をエクスポートするには、ITSecuritySettingItemExport ツールを使用してください。

1. CTM_MAINTENANCE グループに属するユーザでログオンしてください。
2. 本製品のソフトウェアメディアの ¥¥CENTUM¥SECURITY¥ITSecuritySettingItemExport.exe を選択してください。
3. 次の固定フォルダにファイルがエクスポートされます。

C:¥ProgramData¥Yokogawa¥IA¥iPCS¥Platform¥Security¥Config¥DisplaySelectInfo.xml

■ インポート手順-IT セキュリティツール

1. CTM_MAINTENANCE グループに属するユーザでログオンしてください。
2. 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ください。

補足

ファイルサーバやドメインコントローラの場合、本製品のソフトウェアメディアからインストールメニューを起動し、[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、IT セキュリティツールを起動してください。

3. メインメニュー画面の [インポート/エクスポート] をクリックしてください。
設定項目選択状態のインポート/エクスポートダイアログが表示されます。
4. 「操作の選択」で [インポート] を選択してください。
「ファイルの選択」のテキストボックスに、インポートするファイル名を直接入力するか、テキストボックスの右にあるボタンを押してファイルを直接指定してください。
5. [実行] をクリックしてください。
指定したファイルを読み込み、設定項目選択状態のインポート/エクスポートダイアログは閉じます。
6. メインメニュー画面の [設定] をクリックしてください。
インポートした内容で設定され、IT セキュリティ設定の画面が表示されます。

参照

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」

6.8 IT セキュリティツールで設定した情報を参照する

IT セキュリティツールで設定したコンピュータのセキュリティ情報を表示します。
表示される内容は、次の 3 つです。

- ・ IT セキュリティツール情報
IT セキュリティツールのバージョンや著作権、発行元の情報を表示します。
- ・ IT セキュリティ設定基本情報
IT セキュリティツールによって設定されたセキュリティモデル、ユーザ管理、IT セキュリティバージョンを表示します。
- ・ IT セキュリティ設定状況
IT セキュリティツールを起動したコンピュータにインストールされている YOKOGAWA 製品の IT セキュリティ設定状況を表示します。
ITSecuritySettingCompleted 以下に IT セキュリティ設定が完了した製品を列挙します。
InstallCompleted 以下に IT セキュリティ設定が未適用の製品を列挙します。

■ 起動手順

1. CTM_MAINTENANCE グループに属するユーザでログオンしてください。
2. 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ください。

補足

ファイルサーバやドメインコントローラの場合、本製品のソフトウェアメディアからインストールメニューを起動し、[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、IT セキュリティツールを起動してください。

3. [設定情報] ボタンをクリックしてください。
現在の IT セキュリティ設定情報ダイアログが表示されます。

参照

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」

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

Windows のアクティブディレクトリには、コンピュータやユーザの IT 環境を一元管理するための、グループポリシーという仕組みがあります。このグループポリシーを利用して、IT セキュリティ設定のためのインポート用ファイルを提供することで、ドメインに属するクライアントコンピュータのセキュリティポリシーを一括して管理できます。次の設定をしてください。

- ・ ドメインコントローラ上に、セキュリティポリシーを実現するためのグループポリシーオブジェクトを作成する
- ・ アクティブディレクトリを使ってドメインコントローラ上に組織単位を構築し、グループポリシーオブジェクトを適用する

補足

Windows Server 2008 によるアクティブディレクトリを用いたグループポリシーの統合管理では、グループポリシーの項目のひとつである「監査ポリシーの詳細な構成」の設定値を管理したり、クライアントに適用することはできません。また、Windows Server 2008 がクライアントの場合は、アクティブディレクトリから「監査ポリシーの詳細な構成」を設定することはできません。

6.9.1 グループポリシーオブジェクトを作成する

ドメインコントローラ上で、セキュリティポリシーを実現するためのグループポリシーオブジェクトを作成するには、次の手順に従ってください。

1. 本製品のインストールメディアを、ドメインコントローラのドライブに挿入してください。
2. エクスプローラで次のファイルを表示し、ドメインコントローラの任意のフォルダにコピーしてください。コピー先フォルダは、ドメイン管理者がアクセスできるフォルダにしてください。
<ソフトウェアメディアドライブ>:\CENTUM\SECURITY\GPOFiles\xxx\CTM_Standard_xxx.zip
 - ・ xxx が 2.0 の場合; IT セキュリティバージョン 2.0 の標準モデル相当のファイル
 - ・ xxx が 1.0 の場合; IT セキュリティバージョン 1.0 の標準モデル相当のファイル
3. コピーしたファイルをダブルクリックしてください。
インポート用ファイルが展開されます。
4. コントロールパネルを起動してください。
5. [管理ツール] - [グループポリシー管理] を選択してください。
グループポリシーの管理ダイアログが表示されます。
6. 左のペインの [グループポリシーオブジェクト] を右クリックして、[新規] を選択してください。
新しい GPO ダイアログが表示されます。
7. 次に示す設定をしてください。
 - ・ 定義項目 [名前] には、任意の名前を入力
 - ・ 定義項目 [ソーススタター GPO] には、[(なし)] を選択
8. [OK] をクリックしてください。
新しいグループポリシーオブジェクトが作成されます。
9. 新しいグループポリシーオブジェクトを右クリックして、[設定のインポート] を選択してください。
[設定のインポートウィザードの開始] が表示されます。
10. [次へ] をクリックしてください。
バックアップを促すダイアログが表示されます。
11. 新規作成したグループポリシーオブジェクトのためのバックアップは実行せずに、[次へ] をクリックしてください。
[バックアップの場所] が表示されます。
12. [バックアップフォルダー] に、インポート対象フォルダの親フォルダを選択して、[次へ] をクリックしてください。
選択した親フォルダ以下に置かれている、インポート可能なグループポリシー一覧が表示されます。

補足

グループポリシーオブジェクトの設定情報を確認する場合は、[設定の表示] をクリックしてください。Microsoft Internet Explorer に、情報が表示されます。

13. グループポリシーを選択し、[次へ] をクリックしてください。
インポート対象のグループポリシーオブジェクトに、セキュリティプリンシパルや UNC パスの参照が含まれているか、を確認するダイアログが表示されます。

補足

確認ダイアログには、次のメッセージが表示されます。

「スキャンの結果:

バックアップはセキュリティプリンシパルまたは UNC パスの参照を含んでいません。続行するには、[次へ] をクリックしてください。」

14. [次へ] をクリックしてください。

[設定のインポートウィザードの完了] ダイアログが表示されます。

15. [完了] をクリックしてください。

グループポリシーオブジェクトのインポートを開始します。

16. インポートが完了したら、[グループポリシーの管理] でインポートしたポリシーを確認してください。

コントロールパネルを起動し、[管理ツール] – [グループポリシー管理] を選択して [グループポリシーの管理] を表示させ、左のペインで目的のグループポリシーを右クリックして [表示] を選択してください。

以上で、グループポリシーオブジェクトの作成は終了です。このあとドメインコントローラ上に組織単位を構築し、グループポリシーオブジェクトを適用します。

6.9.2 組織単位にグループポリシーオブジェクトを適用する

ドメインコントローラ上で、組織単位にグループポリシーオブジェクトを適用するには、次の手順に従ってください。

1. 管理者アカウントで、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. [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が表示されます。
4. 左のペインで組織単位を作成するドメインコントローラを右クリックして、[新規作成] - [組織単位] を選択してください。
新しいオブジェクト - 組織単位が表示されます。
5. 次に示す設定をしてください。
 - ・ 定義項目 [名前] には、任意の組織単位名を入力
 - ・ [間違えて削除されないようコンテナを保護する] をチェック
6. [OK] をクリックしてください。
新しい組織単位が作成されます。
7. 必要に応じて、組織単位の階層構造を構築してください。手順 4 から手順 6 を繰り返すことで作成することができます。
8. Active Directory ユーザーとコンピューターの左のペインで [Computers] を選択し、表示されるコンピューター一覧から各組織単位に所属させるコンピューターを選択して、目的の組織単位にドラッグアンドドロップしてください。その際、オブジェクトを移動させることについての警告メッセージが表示されますが、[はい] をクリックして処理を継続してください。

補足

1 つの組織単位に属するコンピューターは、同じグループポリシーを適用するコンピューターに限定してください。この後の手順で、組織単位に対してグループポリシーを適用するため、1 つの組織単位に異なる IT セキュリティレベルのコンピューターが属さないようにしてください。

また、統合ゲートウェイステーションは、次のステーションと同じ組織単位に属さないようにしてください。

- ・ HIS
- ・ APCS
- ・ 汎用サブシステムゲートウェイステーション
- ・ システム統合 OPC ステーション
- ・ ライセンス管理

以上で、組織単位の構築は終了です。このあと組織単位にグループポリシーオブジェクトを適用します。

■ 組織単位を削除する手順

新しく組織単位を作成するときに、[新しいオブジェクト - 組織単位] ダイアログで「間違えて削除されないようコンテナを保護する」をチェックしている場合は、その組織単位を削除しようとするときメッセージが表示されます。このような組織単位を削除するときは、次の操作をしてください。

1. コントロールパネルを起動してください。
2. [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] が表示されます。
3. 削除する組織単位を右クリックして [プロパティ] を選択し、さらに [オブジェクト] タブシートを選択してください。[オブジェクト] タブシートが表示されないときは、[Active Directory ユーザーとコンピューター] で [表示] - [拡張機能] を選択すれば、表示されるようになります。

4. 「間違って削除されないようにコンテナを保護する」のチェックを外し、さらに [OK] をクリックしてください。
この組織単位が削除できるようになります。
 5. 組織単位を削除してください。
- 以上で、組織単位の削除は終了です。

■ 組織単位にグループポリシーオブジェクトを適用する手順

次の操作をしてください。

1. コントロールパネルを起動してください。
 2. [管理ツール] – [グループ ポリシー管理] を選択してください。
[グループ ポリシーの管理] が表示されます。
 3. 左のペインで [グループ ポリシー オブジェクト] を選択し、表示されるオブジェクト一覧から各組織単位に適用するグループポリシーオブジェクトを選択して、目的の組織単位にドラッグアンドドロップしてください。
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。
[グループ ポリシー管理コンソール] が表示され、ここで適用されたグループポリシーオブジェクトを変更した場合は、他の組織単位にも共有されることが示されます。
 5. [OK] をクリックしてください。
 6. ドメインコントローラを再起動してください。
- 以上で、グループポリシーオブジェクトの適用は終了です。

補足

ドメインコントローラを再起動しない場合でも、OS のグループポリシー確認機能が実行されるタイミングで、グループポリシーオブジェクトが更新されます。

● 組織単位に適用したグループポリシーオブジェクトを解除する手順

組織単位に適用したグループポリシーオブジェクトを解除しても、グループポリシーオブジェクト自体は削除されません。

次の操作をしてください。

1. コントロールパネルを起動してください。
 2. [管理ツール] – [グループ ポリシー管理] を選択してください。
[グループ ポリシーの管理] が表示されます。
 3. 左のペインで組織単位を選択し、解除するグループポリシーオブジェクトを右クリックして [削除] を選択してください。
確認メッセージが表示されます。
 4. [OK] をクリックしてください。
- 以上で、組織単位に適用したグループポリシーオブジェクトの解除は終了です。

6.10 その他のユーティリティ

IT セキュリティツール以外のユーティリティを説明します。

6.10.1 CreateCentumProcess

CTM_PROCESS ユーザを作成します。また、CTM_PROCESS ユーザのパスワードを変更できます。

■ 詳細説明

CreateCentumProcess は、プロジェクトデータベースを配置するファイルサーバや、他パッケージと連携する場合に、連携する PC 側で利用するツールです。このツールを実行すると、CTM_PROCESS ユーザが作成され、自動的にパスワードが設定されます。ユーザがパスワードを管理したい場合は、オプションで任意のパスワードを指定できます。

■ 起動方法

CreateCentumProcess を起動するには、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、コマンドプロンプトから次のコマンドを実行してください。

```
<ソフトウェアメディアドライブ>:¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS.Platform.Security.CreateCentumProcess.exe
```

CTM_PROCESS ユーザが存在しない場合はユーザが作成され、自動的にパスワードが設定されます。このとき、CTM_PROCESS ユーザ用として登録されている Windows サービスのパスワードも設定されます。

CTM_PROCESS ユーザがすでに存在する場合は、設定されているパスワードが初期パスワードに変更されます。

補足

任意のパスワードを設定する場合、次のコマンドを実行してください。

```
<ソフトウェアメディアドライブ>:¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS.Platform.Security.CreateCentumProcess.exe -p (任意のパスワード)
```

任意のパスワードは、127 文字以下にしてください。パスワードなしは、指定できません。CTM_PROCESS ユーザが存在しない場合はユーザが作成され、指定した任意のパスワードが設定されます。このとき、CTM_PROCESS ユーザ用として登録されている Windows サービスのパスワードも変更されます。

CTM_PROCESS ユーザが存在する場合は、設定されているパスワードが任意のパスワードに変更されます。

重要 パスワードを変更するときの注意点を次に示します。

- CENTUM VP、連携する他のパッケージ、およびファイルサーバなどの CTM_PROCESS ユーザが存在するすべての PC について、同一のパスワードになるように変更してください。
- すでに存在する CTM_PROCESS ユーザのパスワードを変更したときは、PC を再起動してください。

6.10.2 CreateUgsProcess

UGS_PROCESS ユーザを作成します。また、UGS_PROCESS ユーザのパスワードを変更できます。

■ 詳細説明

CreateUgsProcess は、UGS と通信する OPC サーバが存在する場合に、OPC サーバが動作している PC 側で利用するツールです。このツールを実行すると、UGS_PROCESS ユーザが作成され、自動的にパスワードが設定されます。ユーザがパスワードを管理したい場合は、オプションで任意のパスワードを指定できます。

■ 起動方法

CreateUgsProcess を起動するには、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、コマンドプロンプトから次のコマンドを実行してください。

```
<ソフトウェアメディアドライブ>:¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS.Platform.Security.CreateUgsProcess.exe
```

UGS_PROCESS ユーザが存在しない場合はユーザが作成され、自動的にパスワードが設定されます。このとき、UGS_PROCESS ユーザ用として登録されている Windows サービスのパスワードも設定されます。

UGS_PROCESS ユーザがすでに存在する場合は、設定されているパスワードが初期パスワードに変更されます。

補足

任意のパスワードを設定する場合、次のコマンドを実行してください。

```
<ソフトウェアメディアドライブ>:¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS.Platform.Security.CreateUgsProcess.exe -p (任意のパスワード)
```

任意のパスワードは、127 文字以下にしてください。パスワードなしは、指定できません。UGS_PROCESS ユーザが存在しない場合はユーザが作成され、指定した任意のパスワードが設定されます。このとき、UGS_PROCESS ユーザ用として登録されている Windows サービスのパスワードも変更されます。

UGS_PROCESS ユーザが存在する場合は、設定されているパスワードが任意のパスワードに変更されます。

重要 パスワードを変更するときの注意点を次に示します。

- ・ UGS および UGS と通信する OPC サーバの UGS_PROCESS ユーザが存在するすべての PC について、同一のパスワードになるように変更してください。
- ・ すでに存在する UGS_PROCESS ユーザのパスワードを変更したときは、PC を再起動してください。

6.10.3 CreateLicenseProcess

LIC_PROCESS ユーザを作成します。また、LIC_PROCESS ユーザのパスワードを変更できます。

■ 詳細説明

CreateLicenseProcess は、プロジェクトデータベースを配置するファイルサーバや、ProSafe-RS と連携する場合に、連携する PC 側で利用するツールです。このツールを実行すると、LIC_PROCESS ユーザが作成され、自動的にパスワードが設定されます。ユーザがパスワードを管理したい場合は、オプションで任意のパスワードを指定できます。

■ 起動方法

CreateLicenseProcess を起動するには、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、コマンドプロンプトから次のコマンドを実行してください。

```
<ソフトウェアメディアドライブ>:¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS.Platform.License.CreateLicenseProcess.exe
```

LIC_PROCESS ユーザが存在しない場合はユーザが作成され、自動的にパスワードが設定されます。このとき、LIC_PROCESS ユーザ用として登録されている Windows サービスのパスワードも設定されます。

LIC_PROCESS ユーザがすでに存在する場合は、設定されているパスワードが初期パスワードに変更されます。

補足

任意のパスワードを設定する場合、次のコマンドを実行してください。

```
<ソフトウェアメディアドライブ>:¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS.Platform.License.CreateLicenseProcess.exe -p (任意のパスワード)
```

任意のパスワードは、127 文字以下にしてください。パスワードなしは、指定できません。LIC_PROCESS ユーザが存在しない場合はユーザが作成され、指定した任意のパスワードが設定されます。このとき、LIC_PROCESS ユーザ用として登録されている Windows サービスのパスワードも変更されます。

LIC_PROCESS ユーザが存在する場合は、設定されているパスワードが任意のパスワードに変更されます。

重要

パスワードを変更するときの注意点を次に示します。

- ・ CENTUM VP、ProSafe-RS、およびファイルサーバなどの LIC_PROCESS ユーザが存在するすべての PC について、同一のパスワードになるように変更してください。
- ・ すでに存在する LIC_PROCESS ユーザのパスワードを変更したときは、PC を再起動してください。

6.10.4 CreateAdsProcess

ADS_PROCESS ユーザを作成します。また、ADS_PROCESS ユーザのパスワードを変更できます。

■ 詳細説明

CreateAdsProcess は、オートメーションデザインマスターデータベースを配置するオートメーションデザインサーバで利用するツールです。このツールを実行すると、ADS_PROCESS ユーザが作成され、自動的にパスワードが設定されます。ユーザがパスワードを管理したい場合は、オプションで任意のパスワードを指定できます。

■ 起動方法

CreateAdsProcess を起動するには、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、コマンドプロンプトから次のコマンドを実行してください。

<ソフトウェアメディアドライブ>:¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS.ChronusENG.Security.CreateAdsProcess.exe

ADS_PROCESS ユーザが存在しない場合はユーザが作成され、自動的にパスワードが設定されます。このとき、ADS_PROCESS ユーザ用として登録されている Windows サービスのパスワードも設定されます。

ADS_PROCESS ユーザがすでに存在する場合は、設定されているパスワードが初期パスワードに変更されます。

補足

任意のパスワードを設定する場合、次のコマンドを実行してください。

<ソフトウェアメディアドライブ>:¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS.ChronusENG.Security.CreateAdsProcess.exe -p (任意のパスワード)

任意のパスワードは、127 文字以下にしてください。パスワードなしは、指定できません。ADS_PROCESS ユーザが存在しない場合はユーザが作成され、指定した任意のパスワードが設定されます。このとき、ADS_PROCESS ユーザ用として登録されている Windows サービスのパスワードも変更されます。

ADS_PROCESS ユーザが存在する場合は、設定されているパスワードが任意のパスワードに変更されます。

重要

パスワードを変更するときの注意点を次に示します。

- ・ オートメーションデザインマスターデータベースを配置するオートメーションデザインサーバの ADS_PROCESS ユーザが存在するすべての PC について、同一のパスワードになるように変更してください。
- ・ すでに存在する ADS_PROCESS ユーザのパスワードを変更したときは、PC を再起動してください。

参照

オートメーションデザインサーバについては、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「A. オートメーションデザインスイート概要」

6.10.5 CreateAdsAgent

ADS_AGENT ユーザのパスワードを変更できます。

■ 詳細説明

CreateAdsAgent は、CENTUM VP をインストールした PC で利用するツールです。このツールを実行すると、ADS_AGENT ユーザに対して、任意のパスワードを設定できます。

補足

このツールの実行については、当社サービスまでお問い合わせください。

■ 起動方法

CreateAdsAgent を起動するには、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、コマンドプロンプトから次のコマンドを実行してください。

<ソフトウェアメディアドライブ>: ¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS.ChronusENG.Security.CIM.CreateAdsAgent.exe -p (任意のパスワード)

任意のパスワードは、127 文字以下にしてください。パスワードなしは、設定できません。

このコマンドを実行すると、ADS_AGENT ユーザ用として登録されている Windows サービスのパスワードも、同じパスワードに変更されます。

補足

任意のパスワードを設定しないでコマンドを実行した場合は、デフォルトのパスワードが設定されます。

重要

パスワードを変更するときの注意点を次に示します。

- ・ ADS_AGENT ユーザが存在するすべての PC について、同一のパスワードになるように変更してください。
- ・ すでに存在する ADS_AGENT ユーザのパスワードを変更したときは、PC を再起動してください。

6.10.6 CreateRDCProcess

RDC_PROCESS ユーザを作成します。また、RDC_PROCESS ユーザのパスワードを変更できます。

■ 詳細説明

CreateRDCProcess は、コンピュータ切替型 UGS で利用するツールです。このツールを実行すると、RDC_PROCESS が作成され、自動的にパスワードが設定されます。ユーザがパスワードを管理したい場合は、オプションで任意のパスワードを指定できます。

■ 起動方法

CreateRDCProcess を起動するには、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、コマンドプロンプトから次のコマンドを実行してください。

<ソフトウェアメディアドライブ>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.Redundancy.CreateRDCProcess.exe

RDC_PROCESS が存在しない場合はユーザが作成され、自動的にパスワードが設定されます。

RDC_PROCESS がすでに存在する場合は、設定されているパスワードが初期パスワードに変更されます。

補足

任意のパスワードを設定する場合、次のコマンドを実行してください。

<ソフトウェアメディアドライブ>:\CENTUM\SECURITY\Yokogawa.IA.iPCS.Platform.Redundancy.CreateRDCProcess.exe -p (任意のパスワード)

任意のパスワードは、127 文字以下にしてください。パスワードなしは、指定できません。RDC_PROCESS が存在しない場合はユーザが作成され、指定した任意のパスワードが設定されます。

RDC_PROCESS が存在する場合は、設定されているパスワードが任意のパスワードに変更されます。

重要

パスワードを変更するときの注意点を次に示します。

- RDC_PROCESS のパスワードを変更するときは、RDC_PROCESS が存在するすべてのコンピュータで同一のパスワードになるようにパスワードの変更を行ってください。RDC_PROCESS が存在するコンピュータ間で RDC_PROCESS のパスワードが異なっていると、システムが正常に動作しないことがあります。
- すでに存在する RDC_PROCESS のパスワードを変更したときは、コンピュータを再起動してください。
- RDC_PROCESS のパスワードを変更すると、RDC_PROCESS で登録されている Windows サービスのパスワードも変更されます。

6.10.7 CreateOffuser

OFFUSER を作成します。また、OFFUSER のパスワードを変更できます。このツールは、CENTUM VP の HIS 以外の他システムの PC、ファイルサーバ、および CS 3000 の HIS で実行します。

重要

CENTUM VP の HIS で、OFFUSER のパスワードを変更したい場合は、ChangeOffuserPassword を使用してください。

CENTUM VP の HIS で CreateOffuser を使用すると、OFFUSER でログオンできなくなります。この場合、次のいずれかの方法で復旧できます。

- ・ CENTUM VP の HIS にインストールされている ChangeOffuserPassword を使用して、パスワードを変更する。
- ・ ローカルセキュリティポリシーの「ローカルでログオンを拒否する」に登録されている OFFUSER を削除する。

■ 詳細説明

CreateOffuser を実行すると、OFFUSER が作成され、自動的にパスワードが設定されます。ユーザがパスワードを管理したい場合は、オプションで任意のパスワードを指定できます。

■ 起動方法

CreateOffuser を起動するには、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、コマンドプロンプトから次のコマンドを実行してください。

```
<ソフトウェアメディアドライブ>:¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS.Platform.Security.CreateOffuser.exe
```

OFFUSER が存在しない場合はユーザが作成され、自動的にパスワードが設定されます。

OFFUSER がすでに存在する場合は、設定されているパスワードが初期パスワードに変更されます。

補足

任意のパスワードを設定する場合、次のコマンドを実行してください。

```
<ソフトウェアメディアドライブ>:¥CENTUM¥SECURITY¥Yokogawa.IA.iPCS.Platform.Security.CreateOffuser.exe -p (任意のパスワード)
```

任意のパスワードは、127 文字以下にしてください。パスワードなしは、指定できません。OFFUSER が存在しない場合はユーザが作成され、指定した任意のパスワードが設定されます。

OFFUSER が存在する場合は、設定されているパスワードが任意のパスワードに変更されます。

重要

パスワードを変更するときの注意点を次に示します。

- ・ CENTUM VP、連携する他パッケージ、およびファイルサーバなどの OFFUSER が存在するすべての PC について、同一のパスワードになるように変更してください。
- ・ すでに存在する OFFUSER のパスワードを変更したときは、PC を再起動してください。

6.10.8 YWVNETCreateVNTUser

YWVNETCreateVNTUser は、Vnet/IP インタフェースパッケージを実行するユーザのパスワードを変更するユーティリティです。次に示すユーザのパスワードを変更できます。

- VNT_COMMON
- VNT_NVP_CORE
- VNT_BKNET

重要

- パスワードを変更する際は、事前に、CENTUM VP ソフトウェアメディアの ISO 形式ファイルを用意してください。
- パスワードを変更するには、Vnet/IP インタフェースパッケージがインストールされている必要があります。パスワードを変更する際は、事前に、Vnet/IP インタフェースパッケージがインストールされていることを確認してから行ってください。
- パスワードを変更したときは、仮想マシンを再起動してください。

■ 起動方法

YWVNETCreateVNTUser を起動するには、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、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。
6. YWVNETCreateVNTUser を起動する仮想マシンを右クリックし、[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] ボタンをクリックして、全画面表示を解除してください。

7. 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。
8. 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。
9. 仮想マシン接続ウィンドウで、[スタート] - [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。
10. [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。
11. コマンドプロンプトから次のコマンドを実行してください。
<マウントしたドライブ>:\¥CENTUM¥security¥ywvnetcreatevntuser.exe -u ユーザ名 -p 任意のパスワード

任意のパスワードは、127 文字以下にしてください。パスワードなしは、指定できません。

12. 仮想マシンを再起動してください。

重要

- Vnet/IP インタフェースパッケージがインストールされている状態で、本ユーティリティを起動してください。Vnet/IP インタフェースパッケージがインストールされていない状態で、本ユーティリティでパスワードを変更した場合は、Vnet/IP インタフェースパッケージのインストールからやり直してください。
 - パスワード変更後に Vnet/IP インタフェースパッケージを再インストールすると、変更したパスワードがリセットされます。パスワードを再度変更してください。
-

6.10.9 ChangeOffuserPassword

OFFUSER のパスワードを変更できます。このツールは、CENTUM VP の HIS で実行します。

■ 詳細説明

ユーザが OFFUSER のパスワードを管理したい場合、ChangeOffuserPassword を使用して、任意のパスワードを指定して実行すると、指定されたパスワードが設定されます。

■ 起動方法

ChangeOffuserPassword を起動するには、次の手順に従ってください。

1. 管理者権限を持つユーザでログオンしてください。
2. 次のコマンドを実行してください。

システムドライブが C ドライブの例です。

```
C:¥Program Files (x86)¥Yokogawa¥IA¥iPCS¥Platform¥SECURITY¥PROGRAM¥Yokogawa.IA.iPCS.Platform.Security.ChangeOffuserPassword.exe -p (任意のパスワード)
```

任意のパスワードは、127 文字以下にしてください。パスワードなしは、指定できません。設定されているパスワードが任意のパスワードに変更されます。OFFUSER が存在しない場合は、OFFUSER が作成されます。

補足

設定されているパスワードを初期パスワードに変更する場合、次のコマンドを実行してください。システムドライブが C ドライブの例です。

```
C:¥Program Files (x86)¥Yokogawa¥IA¥iPCS¥Platform¥SECURITY¥PROGRAM¥Yokogawa.IA.iPCS.Platform.Security.ChangeOffuserPassword.exe
```

重要

パスワードを変更するときの注意点を次に示します。

- ・ CENTUM VP、連携する他パッケージ、およびファイルサーバなどの OFFUSER が存在するすべての PC について、同一のパスワードになるように変更してください。
- ・ すでに存在する OFFUSER のパスワードを変更したときは、PC を再起動してください。

6.10.10 OFFUSEREnabler

OFFUSER のパスワードを一時的に、「!centumvp123」に変更します。

■ 詳細説明

管理者権限を持つユーザで、OFFUSEREnabler を実行すると OFFUSER のパスワードを、「!centumvp123」に変更して OFFUSER で Windows へログオンできるようにします。また、OFFUSER のパスワードを初期パスワード（非公開）に戻すために、作業を行ったあとで OFFUSERDisabler コマンドを実行してください。標準モデルまたは強固モデルを適用している PC では、コマンドを実行するのに CTM_MAINTENANCE 権限が必要となります。

■ 起動方法

起動方法は次のとおりです。

1. 管理者権限を持つユーザでログオンしてください。
2. エクスプローラで次のプログラムフォルダを開いてください。
システムドライブが C ドライブの例です。

`C:¥Program Files (x86)¥Yokogawa¥IA¥iPCS¥Platform¥SECURITY¥PROGRAM¥`

3. フォルダ内の次のファイルをダブルクリックしてください。
`Yokogawa.IA.iPCS.Platform.Security.OFFUSEREnabler.exe`

6.10.11 OFFUSERDisabler

OFFUSER のパスワードを初期化します。

■ 詳細説明

管理者権限を持つユーザで、OFFUSERDisabler を実行すると OFFUSER のパスワードを初期化し、初期パスワード（非公開）に変更します。

標準モデルまたは強固モデルを適用している PC では、コマンドを実行するのに CTM_MAINTENANCE 権限が必要となります。

■ 起動方法

起動方法は次のとおりです。

1. 管理者権限を持つユーザでログオンしてください。
2. エクスプローラで次のプログラムフォルダを開いてください。
システムドライブが C ドライブの例です。

C:\Program Files (x86)\Yokogawa\IA\iPCS\Platform\Security\PROGRAM\

3. フォルダ内の次のファイルをダブルクリックしてください。
Yokogawa.IA.iPCS.Platform.Security.OFFUSERDisabler.exe

6.10.12 StorageDeviceCTL

StorageDeviceCTL は、次の無効化を一時的に解除するツールです。

- ・ StorageDevicePolicies 機能の適用によって設定された、書き込み権限の無効化
- ・ USB ストレージデバイスの無効化

■ 詳細説明

StorageDevicePolicies 機能や USB ストレージデバイスの無効化によって、ストレージデバイス（USB メモリなど）に対する書き込みができないときに、書き込み権限が必要なタイミングで StorageDeviceCTL を実行すると、実行中のみ書き込みが可能となります。

本ツールの起動後に、USB ストレージデバイスを PC に挿入し、書き込み作業を行います。本ツールの実行には、CTM_MAINTENANCE 権限が必要となります。

なお、本ツールは StorageDevicePolicies 機能や USB ストレージデバイスの無効化を設定した PC に対してのみ利用してください。

重要

- ・ 必ず本ツールの起動後に、ストレージデバイスを認識させてください。
- ・ Windows Server 2008 R2 で、StorageDevicePolicies 機能の適用や USB ストレージデバイスの無効化を行っている場合、本ツールでは解除できません。
- ・ 本製品がインストールされていない PC で、OS が Windows Server 2008 の場合、本ツールを起動したときに、サービス停止の確認ダイアログが表示されることがあります。ダイアログが表示された場合は、ダイアログ内の「閉じる」をクリックしてください。

■ 起動方法

StorageDeviceCTL を起動するには、次の手順に従ってください。

1. エクスプローラで次のプログラムフォルダを開いてください。
システムドライブが C ドライブの例を示します。

C:\Program Files (x86)\Yokogawa\IA\iPCS\Platform\SECURITY\PROGRAM\

2. フォルダ内の次のファイルをダブルクリックしてください。

Yokogawa.IA.iPCS.Platform.Security.StorageDeviceCTL.exe

起動直後は、タスクバーにのみタスクが表示されます。



図 6.10.12-1 タスクバー

3. USB ストレージデバイスを PC に挿入してください。
4. USB ストレージデバイスに対して、必要なデータの読み込み／書き込みを行ってください。
5. USB ストレージデバイスを取り外してください。

補足

USB ストレージデバイスを取り外す場合は、タスクトレイから「ハードウェアの安全な取り外し」アイコンを右クリックして、「USB Flash Disk の取り出し」を選択して、デバイスの停止を行ってください。

6. タスクバーから「StorageDeviceCTL」をクリックして、「WriteStop」をクリックしてください。

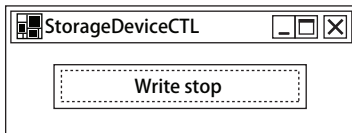


図 6.10.12-2 StorageDeviceCTL ダイアログ

StorageDeviceCTL が終了し、ふたたび USB ストレージデバイスが無効になります。

参照

StorageDevicePolicies 機能については、以下を参照してください。

「3.5.3 StorageDevicePolicies 機能の適用」 ページ 3-25

USB ストレージデバイスの無効化については、以下を参照してください。

「3.5.4 USB ストレージデバイスの無効化」 ページ 3-26

6.10.13 ITSecuritySettingItemExport

R5.01 以降、R6.03 までの IT セキュリティツールで設定したセキュリティモデル、ユーザ管理、設定項目の変更、IT セキュリティバージョンをファイルに出力します。

■ 詳細説明

出力される内容は、実行環境で最後に IT セキュリティを設定した時の状態です。

出力されたファイルを IT セキュリティツールでインポートすると、出力した環境で設定した IT セキュリティツールの各選択状態を再現できます。

■ 起動方法

ITSecuritySettingItemExport を起動するには、次の手順に従ってください。

1. 管理者権限を持つユーザでログオンしてください。
2. 本製品のソフトウェアメディアをドライブに挿入し、コマンドプロンプトから次のコマンドを実行してください。
＜ソフトウェアメディアドライブ＞: ¥CENTUM¥SECURITY¥ITSecuritySettingItemExport.exe
3. 実行後、ファイルが自動生成されて確認ダイアログが表示されますので、[OK] ボタンをクリックして、ファイルを保存してください。

重要

- ・ 本ツールは YOKOGAWA のシステム 製品がインストールされているコンピュータのみ使用可能です。製品のインストールを行わず、IT セキュリティツールでセキュリティ設定を行うファイルサーバやドメインコントローラでは使用できません。
- ・ 本ツールを実行するアカウントは、製品のメンテナンスグループに属する必要があります。
- ・ 本ツールで出力されるフォルダ、ファイル名は固定となります。すでにコンピュータ上で存在する場合は、上書きされます。
- ・ 本ツールで出力されるフォルダ、ファイルにアクセスできない場合は、アクセス違反のエラーメッセージが表示されます。

Appendix 1. IT セキュリティ設定項目

IT セキュリティバージョン 2.0、および IT セキュリティバージョン 1.0 における、セキュリティ設定項目について説明します。

Appendix 1.1 IT セキュリティバージョン 2.0

IT セキュリティバージョン 2.0 における、セキュリティ設定項目とその設定項目のデフォルト値、および設定変更の可否について説明します。ただし、OS やステーションの種類によってセキュリティ設定項目が表示されないことがあります。

Appendix 1.1.1 CENTUM VP ソフトウェアをインストールしたコンピュータの場合

本製品ソフトウェアをインストールしたコンピュータにおける、セキュリティモデルとユーザ管理方式の組み合わせごとの、セキュリティ設定項目の一覧を示します。

■ 標準モデル、スタンドアロン管理環境下でのセキュリティ設定項目

標準モデル、スタンドアロン管理という組み合わせ環境下でのセキュリティ設定を、次に示します。

表 Appendix 1.1.1-1 標準モデル-スタンドアロン管理

設定項目	チェックボックスのデフォルト状態	設定変更の可否
ローカルユーザ／グループの作成	オン	変更不可
ファイル／フォルダのアクセスコントロール	オン	変更不可
製品のレジストリのアクセスコントロール	オン	変更不可
DCOM(OPC)のアクセスコントロール	オン	変更不可
パーソナルファイアウォールのチューニング	オン	変更不可
パーソナルファイアウォールー「ユニキャスト応答の許可」を無効に設定する (*1)	オン	変更可
NetBIOS over TCP/IP の無効化	オフ	変更可
StorageDevicePolicies 機能の適用	オフ	変更可
USB ストレージデバイスの無効化	オフ	変更可
ソフトウェア制限ポリシーの適用	オフ	変更可
ユーザー権利の割り当てー「ネットワーク経由でのアクセス」 (*2)	オン	変更可
ユーザー権利の割り当てー「ローカルログオンを許可」 (*2)	オン	変更可
ユーザー権利の割り当てー「ローカルログオンを拒否」	オン	変更不可
セキュリティオプションー「監査：監査ポリシーサブカテゴリの設定 (Windows Vista 以降) を強制して、監査ポリシーカテゴリの設定を上書きする」	オン	変更可
セキュリティオプションー「デバイス：ユーザーがプリンタードライバをインストールできないようにする」	オン	変更可
セキュリティオプションー「デバイス：CD-ROM へのアクセスを、ローカルログオンユーザーだけに制限する」	オン	変更可
セキュリティオプションー「デバイス：フロッピーへのアクセスを、ローカルログオンユーザーだけに制限する」	オン	変更可
セキュリティオプションー「ドメインメンバー：強力な (Windows 2000 かそれ以降のバージョン) セッションキーを必要とする」	オン	変更可
セキュリティオプションー「対話型ログオン：最後のユーザー名を表示しない」	オン	変更不可
セキュリティオプションー「対話型ログオン：Ctrl + Alt + Del を必要としない」を無効に設定する	オン	変更可
セキュリティオプションー「対話型ログオン：コンピューターの非アクティブ状態の上限」 (*2)	オン	変更可
セキュリティオプションー「対話型ログオン：パスワードが無効になる前にユーザーに変更を促す」	オン	変更可
セキュリティオプションー「Microsoft ネットワークサーバー：クライアントが同意すれば、通信にデジタル署名を行う」	オン	変更可
セキュリティオプションー「Microsoft ネットワークサーバー：サーバー SPN ターゲット名検証レベル」	オン	変更可

次に続く

表 Appendix 1.1.1-1 標準モデル-スタンドアロン管理（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
「MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)」	オン	変更可
「MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)」を無効に設定する	オン	変更可
「MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)」	オン	変更可
セキュリティオプション「ネットワークアクセス：SAM アカウントの匿名の列挙を許可しない」	オン	変更可
セキュリティオプション「ネットワークアクセス：SAM アカウントおよび共有の匿名の列挙を許可しない」	オン	変更可
セキュリティオプション「ネットワークアクセス：ネットワーク認証のためにパスワードおよび資格情報を保存することを許可しない」	オン	変更可
セキュリティオプション「ネットワークセキュリティ：NTLM で Local System によるコンピューター ID の使用を許可する」	オン	変更可
セキュリティオプション「ネットワークセキュリティ：Local System による NULL セッションフォールバックを許可する」を無効に設定する	オン	変更可
セキュリティオプション「ネットワークセキュリティ：LAN Manager 認証レベル」	オン	変更不可
セキュリティオプション「ネットワークセキュリティ：NTLM SSP ベース（セキュア RPC を含む）のクライアント向け最小セッションセキュリティ」	オン	変更可
セキュリティオプション「ネットワークセキュリティ：NTLM SSP ベース（セキュア RPC 含む）のサーバー向け最小セッションセキュリティ」	オン	変更可
セキュリティオプション「シャットダウン：システムのシャットダウンにログオンを必要としない」を無効に設定する	オン	変更可
セキュリティオプション「ユーザーアカウント制御：ビルトイン Administrator アカウントのための管理者承認モード」	オン	変更可
セキュリティオプション「ユーザーアカウント制御：管理者承認モードでの管理者に対する昇格時のプロンプトの動作」	オン	変更可
監査ポリシーの詳細な構成「資格情報の確認の監査」	オン	変更可
監査ポリシーの詳細な構成「コンピューターアカウントの管理の監査」	オン	変更可
監査ポリシーの詳細な構成「その他のアカウント管理イベントの監査」	オン	変更可
監査ポリシーの詳細な構成「セキュリティグループの管理の監査」	オン	変更可
監査ポリシーの詳細な構成「ユーザーアカウントの管理の監査」	オン	変更可
監査ポリシーの詳細な構成「プロセス作成の監査」	オン	変更可
監査ポリシーの詳細な構成「アカウントロックアウトの監査」	オン	変更可
監査ポリシーの詳細な構成「ログオフの監査」	オン	変更可
監査ポリシーの詳細な構成「ログオンの監査」	オン	変更可
監査ポリシーの詳細な構成「その他のログオン/ログオフイベントの監査」	オン	変更可
監査ポリシーの詳細な構成「特殊なログオンの監査」	オン	変更可
監査ポリシーの詳細な構成「リムーバブル記憶域の監査」	オン	変更可
監査ポリシーの詳細な構成「監査ポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成「認証ポリシーの変更の監査」	オン	変更可

次に続く

表 Appendix 1.1.1-1 標準モデル-スタンドアロン管理（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
監査ポリシーの詳細な構成－「フィルタリングプラットフォームポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「MPSSVC ルールレベルポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「その他のポリシー変更イベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「重要な特権の使用の監査」	オン	変更可
監査ポリシーの詳細な構成－「その他のシステムイベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「セキュリティ状態の変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「セキュリティシステムの拡張の監査」	オン	変更可
監査ポリシーの詳細な構成－「システムの整合性の監査」	オン	変更可
個人用設定－「ロック画面カメラを有効にできないようにする」	オン	変更可
個人用設定－「ロック画面スライドショーを有効にできないようにする」	オン	変更可
WLAN 設定－「推奨されるオープンホットスポット、連絡先によって共有されたネットワーク、有料サービスを提供するホットスポットに Windows が自動的に接続することを許可する」	オン	変更可
グループポリシー－「レジストリポリシーの処理を構成する」	オン	変更可
インターネット通信の設定－「プリンタードライバーの HTTP 経由でのダウンロードをオフにする」	オン	変更可
インターネット通信の設定－「イベントビューアーの'Event.asp'リンクをオフにする」	オン	変更可
インターネット通信の設定－「Web 発行およびオンライン注文ウィザードのインターネットダウンロードをオフにする」	オン	変更可
インターネット通信の設定－「HTTP 経由の印刷をオフにする」	オン	変更可
インターネット通信の設定－「検索コンパニオンの内容ファイルの更新をオフにする」	オン	変更可
インターネット通信の設定－「ファイルおよびフォルダーの'Web に発行'タスクをオフにする」	オン	変更可
インターネット通信の設定－「Windows カスタマーエクスペリエンス向上プログラムをオフにする」	オン	変更不可
インターネット通信の設定－「Windows Messenger カスタマーエクスペリエンス向上プログラムをオフにする」	オン	変更不可
ログオン－「ネットワークの選択の UI を表示しない」	オン	変更可
ログオン－「ドメインに参加しているコンピューターに接続しているユーザーを列挙しない」	オン	変更可
ログオン－「ドメインに参加しているコンピューターのローカルユーザーを列挙する」を無効に設定する	オン	変更可
ログオン－「ロック画面のアプリ通知をオフにする」	オン	変更可
軽減策オプション－「信頼されていないフォントのブロック」	オン	変更可
ユーザープロファイル－「広告 ID を無効にする」	オン	変更可
アプリのプライバシー－「Windows アプリでアカウント情報にアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリで通話履歴にアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリで連絡先にアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリでメールにアクセスする」	オン	変更可

次に続く

表 Appendix 1.1.1-1 標準モデル-スタンドアロン管理（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
アプリのプライバシー「Windows アプリで位置情報にアクセスする」	オン	変更可
アプリのプライバシー「Windows アプリでメッセージングにアクセスする」	オン	変更可
アプリのプライバシー「Windows アプリでモーションにアクセスする」	オン	変更可
アプリのプライバシー「Windows アプリでカレンダーにアクセスする」	オン	変更可
アプリのプライバシー「Windows アプリでカメラにアクセスする」	オン	変更可
アプリのプライバシー「Windows アプリでマイクにアクセスする」	オン	変更可
アプリのプライバシー「Windows アプリで信頼済みデバイスにアクセスする」	オン	変更可
アプリのプライバシー「Windows アプリで無線を制御する」	オン	変更可
アプリのプライバシー「Windows アプリでデバイスと同期する」	オン	変更可
アプリ実行時「ホストされているコンテンツから Windows ランタイム API でアクセスする Windows ストアアプリを起動できないようにする」	オン	変更可
自動再生のポリシー「自動再生機能をオフにする」	オン	変更可
自動再生のポリシー「ボリューム以外のデバイスの自動再生を許可しない」	オン	変更可
クラウドコンテンツ「Windows のヒントを表示しない」	オン	変更可
クラウドコンテンツ「Microsoft コンシューマーエクスペリエンスを無効にする」	オン	変更可
データの収集とプレビュービルド「利用統計情報の許可」	オン	変更可
データの収集とプレビュービルド「プレリリースの機能または設定を無効にする」	オン	変更可
データの収集とプレビュービルド「フィードバックの通知を表示しない」	オン	変更可
データの収集とプレビュービルド「Insider ビルドに関するユーザーコントロールの切り替え」	オン	変更可
イベントログサービス（アプリケーション）「ログファイルの最大サイズ（KB）を指定する」	オン	変更可
イベントログサービス（セキュリティ）「ログファイルの最大サイズ（KB）を指定する」	オン	変更可
イベントログサービス（システム）「ログファイルの最大サイズ（KB）を指定する」	オン	変更可
エクスプローラー「破損後のヒープ終了をオフにする」	オン	変更可
ホームグループ「コンピューターがホームグループに参加できないようにする」	オン	変更可
OneDrive「OneDrive をファイル記憶域として使用できないようにする」	オン	変更可
OneDrive「ドキュメントを既定で OneDrive に保存する」（既定でローカルコンピューターにドキュメントを保存する）	オン	変更可
リモートデスクトップ接続のクライアント「パスワードの保存を許可しない」	オン	変更可
デバイスとリソースのリダイレクト「ドライブのリダイレクトを許可しない」（*1）	オン	変更可
セキュリティ「接続するたびにパスワードを要求する」（*2）	オン	変更可

次に続く

表 Appendix 1.1.1-1 標準モデル-スタンドアロン管理（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
セキュリティ「セキュリティで保護された RPC 通信を要求する」	オン	変更可
セキュリティ「リモート接続にネットワークレベル認証を使用したユーザー認証を必要とする」	オン	変更可
セッションの時間制限「アクティブでアイドル状態になっているリモートデスクトップサービスセッションの制限時間を設定する」(*2)	オン	変更可
検索「Cortana を許可する」を無効にする	オン	変更可
ソフトウェア保護プラットフォーム「KMS クライアントオンライン AVS 検証を無効にする」	オン	変更可
PC 設定の同期「アプリを同期しない」	オン	変更可
PC 設定の同期「スタート設定を同期しない」	オン	変更可
Windows エラー報告「OS が生成するエラー報告のためにメモリダンプを自動送信する」を無効に設定する	オン	変更不可
Windows ログオンのオプション「システムによる再起動後に自動的に前回の対話ユーザーでサインインする」を無効に設定する	オン	変更可
通知「ロック画面のトースト通知をオフにする」	オン	変更可

*1: UGS では、チェックボックスの状態は「オフ」となり、変更不可となります。

*2: UACS ステーションのみ対象となります。

■ 標準モデル、ドメイン管理／併用管理環境下でのセキュリティ設定項目

標準モデル、ドメイン管理／併用管理という組み合わせ環境下でのセキュリティ設定を、次に示します。

表 Appendix 1.1.1-2 標準モデル-ドメイン管理／併用管理

設定項目	チェックボックスのデフォルト状態	設定変更の可否
ローカルユーザ／グループの作成	オン	変更不可
ドメインユーザ／グループの作成	オン	変更不可
ファイル／フォルダのアクセスコントロール	オン	変更不可
製品のレジストリのアクセスコントロール	オン	変更不可
DCOM(OPC)のアクセスコントロール	オン	変更不可
パーソナルファイアウォールのチューニング	オン	変更不可
パーソナルファイアウォール「ユニキャスト応答の許可」を無効に設定する (*1)	オン	変更可
NetBIOS over TCP/IP の無効化	オン	変更可
StorageDevicePolicies 機能の適用	オフ	変更可
USB ストレージデバイスの無効化	オフ	変更可
ソフトウェア制限ポリシーの適用	オフ	変更可
ユーザー権利の割り当て「ネットワーク経由でのアクセス」(*2)	オン	変更可
ユーザー権利の割り当て「ローカルログオンを許可」(*2)	オン	変更可
ユーザー権利の割り当て「ローカルログオンを拒否」	オン	変更不可
セキュリティオプション「監査：監査ポリシーサブカテゴリの設定（Windows Vista 以降）を強制して、監査ポリシーカテゴリの設定を上書きする」	オン	変更可
セキュリティオプション「デバイス：ユーザーがプリンタードライバをインストールできないようにする」	オン	変更可

次に続く

表 Appendix 1.1.1-2 標準モデル-ドメイン管理／併用管理（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
セキュリティオプション－「デバイス：CD-ROM へのアクセスを、ローカルログオンユーザーだけに制限する」	オン	変更可
セキュリティオプション－「デバイス：フロッピーへのアクセスを、ローカルログオンユーザーだけに制限する」	オン	変更可
セキュリティオプション－「ドメインメンバー：強力な（Windows 2000 かそれ以降のバージョン）セッションキーを必要とする」	オン	変更可
セキュリティオプション－「対話型ログオン：最後のユーザー名を表示しない」	オン	変更不可
セキュリティオプション－「対話型ログオン：Ctrl + Alt + Del を必要としない」を無効に設定する	オン	変更可
セキュリティオプション－「対話型ログオン：コンピューターの非アクティブ状態の上限」(*2)	オン	変更可
セキュリティオプション－「対話型ログオン：パスワードが無効になる前にユーザーに変更を促す」	オン	変更可
セキュリティオプション－「Microsoft ネットワークサーバー：クライアントが同意すれば、通信にデジタル署名を行う」	オン	変更可
セキュリティオプション－「Microsoft ネットワークサーバー：サーバー SPN ターゲット名検証レベル」	オン	変更可
「MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)」	オン	変更可
「MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)」を無効に設定する	オン	変更可
「MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)」	オン	変更可
セキュリティオプション－「ネットワークアクセス：SAM アカウントの匿名の列挙を許可しない」	オン	変更可
セキュリティオプション－「ネットワークアクセス：SAM アカウントおよび共有の匿名の列挙を許可しない」	オン	変更可
セキュリティオプション－「ネットワークアクセス：ネットワーク認証のためにパスワードおよび資格情報を保存することを許可しない」	オン	変更可
セキュリティオプション－「ネットワークセキュリティ：NTLM で Local System によるコンピューター ID の使用を許可する」	オン	変更可
セキュリティオプション－「ネットワークセキュリティ：Local System による NULL セッションフォールバックを許可する」を無効に設定する	オン	変更可
セキュリティオプション－「ネットワークセキュリティ：LAN Manager 認証レベル」	オン	変更不可
セキュリティオプション－「ネットワークセキュリティ：NTLM SSP ベース（セキュア RPC を含む）のクライアント向け最小セッションセキュリティ」	オン	変更可
セキュリティオプション－「ネットワークセキュリティ：NTLM SSP ベース（セキュア RPC を含む）のサーバー向け最小セッションセキュリティ」	オン	変更可
セキュリティオプション－「シャットダウン：システムのシャットダウンにログオンを必要としない」を無効に設定する	オン	変更可
セキュリティオプション－「ユーザーアカウント制御：ビルトイン Administrator アカウントのための管理者承認モード」	オン	変更可
セキュリティオプション－「ユーザーアカウント制御：管理者承認モードでの管理者に対する昇格時のプロンプトの動作」	オン	変更可
監査ポリシーの詳細な構成－「資格情報の確認の監査」	オン	変更可

次に続く

表 Appendix 1.1.1-2 標準モデル-ドメイン管理／併用管理（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
監査ポリシーの詳細な構成－「コンピューターアカウントの管理の監査」	オン	変更可
監査ポリシーの詳細な構成－「その他のアカウント管理イベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「セキュリティグループの管理の監査」	オン	変更可
監査ポリシーの詳細な構成－「ユーザーアカウントの管理の監査」	オン	変更可
監査ポリシーの詳細な構成－「プロセス作成の監査」	オン	変更可
監査ポリシーの詳細な構成－「アカウントロックアウトの監査」	オン	変更可
監査ポリシーの詳細な構成－「ログオフの監査」	オン	変更可
監査ポリシーの詳細な構成－「ログオンの監査」	オン	変更可
監査ポリシーの詳細な構成－「その他のログオン/ログオフイベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「特殊なログオンの監査」	オン	変更可
監査ポリシーの詳細な構成－「リムーバブル記憶域の監査」	オン	変更可
監査ポリシーの詳細な構成－「監査ポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「認証ポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「フィルタリングプラットフォームポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「MPSSVC ルールレベルポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「その他のポリシー変更イベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「重要な特権の使用の監査」	オン	変更可
監査ポリシーの詳細な構成－「その他のシステムイベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「セキュリティ状態の変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「セキュリティシステムの拡張の監査」	オン	変更可
監査ポリシーの詳細な構成－「システムの整合性の監査」	オン	変更可
個人用設定－「ロック画面カメラを有効にできないようにする」	オン	変更可
個人用設定－「ロック画面スライドショーを有効にできないようにする」	オン	変更可
WLAN 設定－「推奨されるオープンホットスポット、連絡先によって共有されたネットワーク、有料サービスを提供するホットスポットに Windows が自動的に接続することを許可する」	オン	変更可
グループポリシー－「レジストリポリシーの処理を構成する」	オン	変更可
インターネット通信の設定－「プリンタードライバの HTTP 経由でのダウンロードをオフにする」	オン	変更可
インターネット通信の設定－「イベントビューアーの'Event.asp'リンクをオフにする」	オン	変更可
インターネット通信の設定－「Web 発行およびオンライン注文ウィザードのインターネットダウンロードをオフにする」	オン	変更可
インターネット通信の設定－「HTTP 経由の印刷をオフにする」	オン	変更可
インターネット通信の設定－「検索コンパニオンの内容ファイルの更新をオフにする」	オン	変更可
インターネット通信の設定－「ファイルおよびフォルダーの'Web'に発行'タスクをオフにする」	オン	変更可
インターネット通信の設定－「Windows カスタマーエクスペリエンス向上プログラムをオフにする」	オン	変更不可

次に続く

表 Appendix 1.1.1-2 標準モデル-ドメイン管理／併用管理（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
インターネット通信の設定－「Windows Messenger カスタマーエクスペリエンス向上プログラムをオフにする」	オン	変更不可
ログオン－「ネットワークの選択の UI を表示しない」	オン	変更可
ログオン－「ドメインに参加しているコンピューターに接続しているユーザーを列挙しない」	オン	変更可
ログオン－「ドメインに参加しているコンピューターのローカルユーザーを列挙する」を無効に設定する	オン	変更可
ログオン－「ロック画面のアプリ通知をオフにする」	オン	変更可
軽減策オプション－「信頼されていないフォントのブロック」	オン	変更可
ユーザープロファイル－「広告 ID を無効にする」	オン	変更可
アプリのプライバシー－「Windows アプリでアカウント情報にアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリで通話履歴にアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリで連絡先にアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリでメールにアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリで位置情報にアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリでメッセージングにアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリでモーションにアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリでカレンダーにアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリでカメラにアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリでマイクにアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリで信頼済みデバイスにアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリで無線を制御する」	オン	変更可
アプリのプライバシー－「Windows アプリでデバイスと同期する」	オン	変更可
アプリ実行時－「ホストされているコンテンツから Windows ランタイム API でアクセスする Windows ストアアプリを起動できないようにする」	オン	変更可
自動再生のポリシー－「自動再生機能をオフにする」	オン	変更可
自動再生のポリシー－「ボリューム以外のデバイスの自動再生を許可しない」	オン	変更可
クラウドコンテンツ－「Windows のヒントを表示しない」	オン	変更可
クラウドコンテンツ－「Microsoft コンシューマーエクスペリエンスを無効にする」	オン	変更可
データの収集とプレビュービルド－「利用統計情報の許可」	オン	変更可
データの収集とプレビュービルド－「プレリリースの機能または設定を無効にする」	オン	変更可
データの収集とプレビュービルド－「フィードバックの通知を表示しない」	オン	変更可
データの収集とプレビュービルド－「Insider ビルドに関するユーザーコントロールの切り替え」	オン	変更可

次に続く

表 Appendix 1.1.1-2 標準モデル-ドメイン管理／併用管理（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
イベントログサービス（アプリケーション）－「ログファイルの最大サイズ（KB）を指定する」	オン	変更可
イベントログサービス（セキュリティ）－「ログファイルの最大サイズ（KB）を指定する」	オン	変更可
イベントログサービス（システム）－「ログファイルの最大サイズ（KB）を指定する」	オン	変更可
エクスプローラー－「破損後のヒープ終了をオフにする」	オン	変更可
ホームグループ－「コンピューターがホームグループに参加できないようにする」	オン	変更可
OneDrive－「OneDrive をファイル記憶域として使用できないようにする」	オン	変更可
OneDrive－「ドキュメントを既定で OneDrive に保存する」（既定でローカルコンピューターにドキュメントを保存する）	オン	変更可
リモートデスクトップ接続のクライアント－「パスワードの保存を許可しない」	オン	変更可
デバイスとリソースのリダイレクト－「ドライブのリダイレクトを許可しない」（*1）	オン	変更可
セキュリティ－「接続するたびにパスワードを要求する」（*2）	オン	変更可
セキュリティ－「セキュリティで保護された RPC 通信を要求する」	オン	変更可
セキュリティ－「リモート接続にネットワークレベル認証を使用したユーザー認証を必要とする」	オン	変更可
セッションの時間制限－「アクティブでアイドル状態になっているリモートデスクトップサービスセッションの制限時間を設定する」（*2）	オン	変更可
検索－「Cortana を許可する」を無効に設定する	オン	変更可
ソフトウェア保護プラットフォーム－「KMS クライアントオンライン AVS 検証を無効にする」	オン	変更可
PC 設定の同期－「アプリを同期しない」	オン	変更可
PC 設定の同期－「スタート設定を同期しない」	オン	変更可
Windows エラー報告－「OS が生成するエラー報告のためにメモリダンプを自動送信する」を無効に設定する	オン	変更不可
Windows ログオンのオプション－「システムによる再起動後に自動的に前回の対話ユーザーでサインインする」を無効に設定する	オン	変更可
通知－「ロック画面のトースト通知をオフにする」	オン	変更可

*1: UGS では、チェックボックスの状態は「オフ」となり、変更不可となります。

*2: UACS ステーションのみ対象となります。

Appendix 1.1.2 ファイルサーバやドメインコントローラの場合

ファイルサーバ、またはドメインコントローラにおける、セキュリティモデルとユーザ管理方式の組み合わせごとの、セキュリティ設定項目の一覧を示します。

■ ファイルサーバにおける標準モデル、スタンドアロン管理環境下でのセキュリティ設定項目

ファイルサーバにおける標準モデル、スタンドアロン管理という組み合わせ環境下でのセキュリティ設定を、次に示します。

表 Appendix 1.1.2-1 ファイルサーバ：標準モデル-スタンドアロン管理

設定項目	チェックボックスのデフォルト状態	設定変更の可否
ローカルユーザ／グループの作成	オン	変更不可
ファイル／フォルダのアクセスコントロール	オン	変更不可
パーソナルファイアウォールのチューニング	オン	変更不可
パーソナルファイアウォール「ユニキャスト応答の許可」を無効に設定する	オン	変更可
NetBIOS over TCP/IP の無効化	オフ	変更可
StorageDevicePolicies 機能の適用	オフ	変更可
USB ストレージデバイスの無効化	オフ	変更可
ユーザー権利の割り当て「ローカルログオンを拒否」	オン	変更不可
セキュリティオプション「監査：監査ポリシーサブカテゴリの設定（Windows Vista 以降）を強制して、監査ポリシーカテゴリの設定を上書きする」	オン	変更可
セキュリティオプション「デバイス：ユーザーがプリンタードライバをインストールできないようにする」	オン	変更可
セキュリティオプション「デバイス：CD-ROM へのアクセスを、ローカルログオンユーザーだけに制限する」	オン	変更可
セキュリティオプション「デバイス：フロッピーへのアクセスを、ローカルログオンユーザーだけに制限する」	オン	変更可
セキュリティオプション「ドメインメンバー：強力な（Windows 2000 かそれ以降のバージョン）セッションキーを必要とする」	オン	変更可
セキュリティオプション「対話型ログオン：最後のユーザー名を表示しない」	オン	変更可
セキュリティオプション「対話型ログオン：Ctrl + Alt + Del を必要としない」を無効に設定する	オン	変更可
セキュリティオプション「対話型ログオン：パスワードが無効になる前にユーザーに変更を促す」	オン	変更可
セキュリティオプション「Microsoft ネットワークサーバー：クライアントが同意すれば、通信にデジタル署名を行う」	オン	変更可
セキュリティオプション「Microsoft ネットワークサーバー：サーバー SPN ターゲット名検証レベル」	オン	変更可
「MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)」	オン	変更可
「MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)」を無効に設定する	オン	変更可

次に続く

表 Appendix 1.1.2-1 ファイルサーバ：標準モデル-スタンドアロン管理（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
「MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)」	オン	変更可
セキュリティオプション－「ネットワークアクセス：SAM アカウントの匿名の列挙を許可しない」	オン	変更可
セキュリティオプション－「ネットワークアクセス：SAM アカウントおよび共有の匿名の列挙を許可しない」	オン	変更可
セキュリティオプション－「ネットワークアクセス：ネットワーク認証のためにパスワードおよび資格情報を保存することを許可しない」	オン	変更可
セキュリティオプション－「ネットワークセキュリティ：NTLM で Local System によるコンピューター ID の使用を許可する」	オン	変更可
セキュリティオプション－「ネットワークセキュリティ：Local System による NULL セッションフォールバックを許可する」を無効に設定する	オン	変更可
セキュリティオプション－「ネットワークセキュリティ：LAN Manager 認証レベル」	オン	変更不可
セキュリティオプション－「ネットワークセキュリティ：NTLM SSP ベース（セキュア RPC を含む）のクライアント向け最小セッションセキュリティ」	オン	変更可
セキュリティオプション－「ネットワークセキュリティ：NTLM SSP ベース（セキュア RPC を含む）のサーバー向け最小セッションセキュリティ」	オン	変更可
セキュリティオプション－「シャットダウン：システムのシャットダウンにログオンを必要としない」を無効に設定する	オン	変更可
セキュリティオプション－「ユーザーアカウント制御：ビルトイン Administrator アカウントのための管理者承認モード」	オン	変更可
セキュリティオプション－「ユーザーアカウント制御：管理者承認モードでの管理者に対する昇格時のプロンプトの動作」	オン	変更可
監査ポリシーの詳細な構成－「資格情報の確認の監査」	オン	変更可
監査ポリシーの詳細な構成－「コンピューターアカウントの管理の監査」	オン	変更可
監査ポリシーの詳細な構成－「その他のアカウント管理イベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「セキュリティグループの管理の監査」	オン	変更可
監査ポリシーの詳細な構成－「ユーザーアカウントの管理の監査」	オン	変更可
監査ポリシーの詳細な構成－「プロセス作成の監査」	オン	変更可
監査ポリシーの詳細な構成－「RPC イベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「アカウントロックアウトの監査」	オン	変更可
監査ポリシーの詳細な構成－「ログオフの監査」	オン	変更可
監査ポリシーの詳細な構成－「ログオンの監査」	オン	変更可
監査ポリシーの詳細な構成－「その他のログオン/ログオフイベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「特殊なログオンの監査」	オン	変更可

次に続く

表 Appendix 1.1.2-1 ファイルサーバ：標準モデル-スタンドアロン管理（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
監査ポリシーの詳細な構成－「生成されたアプリケーションの監査」	オン	変更可
監査ポリシーの詳細な構成－「リムーバブル記憶域の監査」	オン	変更可
監査ポリシーの詳細な構成－「監査ポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「認証ポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「フィルタリングプラットフォームポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「MPSSVC ルールレベルポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「その他のポリシー変更イベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「重要な特権の使用の監査」	オン	変更可
監査ポリシーの詳細な構成－「その他のシステムイベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「セキュリティ状態の変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「セキュリティシステムの拡張の監査」	オン	変更可
監査ポリシーの詳細な構成－「システムの整合性の監査」	オン	変更可
個人用設定－「ロック画面カメラを有効にできないようにする」	オン	変更可
個人用設定－「ロック画面スライドショーを有効にできないようにする」	オン	変更可
WLAN 設定－「推奨されるオープンホットスポット、連絡先によって共有されたネットワーク、有料サービスを提供するホットスポットに Windows が自動的に接続することを許可する」	オン	変更可
グループポリシー－「レジストリポリシーの処理を構成する」	オン	変更可
インターネット通信の設定－「プリンタードライバの HTTP 経由でのダウンロードをオフにする」	オン	変更可
インターネット通信の設定－「イベントビューアーの 'Event.asp' リンクをオフにする」	オン	変更可
インターネット通信の設定－「Web 発行およびオンライン注文ウィザードのインターネットダウンロードをオフにする」	オン	変更可
インターネット通信の設定－「HTTP 経由の印刷をオフにする」	オン	変更可
インターネット通信の設定－「検索コンパニオンの内容ファイルの更新をオフにする」	オン	変更可
インターネット通信の設定－「ファイルおよびフォルダーの 'Web に発行' タスクをオフにする」	オン	変更可
インターネット通信の設定－「Windows カスタマーエクスペリエンス向上プログラムをオフにする」	オン	変更不可
インターネット通信の設定－「Windows Messenger カスタマーエクスペリエンス向上プログラムをオフにする」	オン	変更不可
ログオン－「ネットワークの選択の UI を表示しない」	オン	変更可
ログオン－「ドメインに参加しているコンピューターに接続しているユーザーを列挙しない」	オン	変更可
ログオン－「ドメインに参加しているコンピューターのローカルユーザーを列挙する」を無効に設定する	オン	変更可

次に続く

表 Appendix 1.1.2-1 ファイルサーバ：標準モデル-スタンドアロン管理（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
ログオン－「ロック画面のアプリ通知をオフにする」	オン	変更可
軽減策オプション－「信頼されていないフォントのブロック」	オン	変更可
ユーザープロファイル－「広告 ID を無効にする」	オン	変更可
アプリのプライバシー－「Windows アプリでアカウント情報にアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリで通話履歴にアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリで連絡先にアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリでメールにアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリで位置情報にアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリでメッセージングにアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリでモーションにアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリでカレンダーにアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリでカメラにアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリでマイクにアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリで信頼済みデバイスにアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリで無線を制御する」	オン	変更可
アプリのプライバシー－「Windows アプリでデバイスと同期する」	オン	変更可
アプリ実行時－「ホストされているコンテンツから Windows ランタイム API でアクセスする Windows ストア アプリを起動できないようにする」	オン	変更可
自動再生のポリシー－「自動再生機能をオフにする」	オン	変更可
自動再生のポリシー－「ボリューム以外のデバイスの自動再生を許可しない」	オン	変更可
クラウドコンテンツ－「Windows のヒントを表示しない」	オン	変更可
クラウドコンテンツ－「Microsoft コンシューマーエクスペリエンスを無効にする」	オン	変更可
データの収集とプレビュービルド－「利用統計情報の許可」	オン	変更可
データの収集とプレビュービルド－「プレリリースの機能または設定を無効にする」	オン	変更可
データの収集とプレビュービルド－「フィードバックの通知を表示しない」	オン	変更可
データの収集とプレビュービルド－「Insider ビルドに関するユーザーコントロールの切り替え」	オン	変更可
イベントログサービス（アプリケーション）－「ログファイルの最大サイズ（KB）を指定する」	オン	変更可
イベントログサービス（セキュリティ）－「ログファイルの最大サイズ（KB）を指定する」	オン	変更可

次に続く

表 Appendix 1.1.2-1 ファイルサーバ：標準モデル-スタンドアロン管理（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
イベントログサービス（システム）－「ログファイルの最大サイズ（KB）を指定する」	オン	変更可
エクスプローラー－「破損後のヒープ終了をオフにする」	オン	変更可
ホームグループ－「コンピューターがホームグループに参加できないようにする」	オン	変更可
OneDrive－「OneDrive をファイル記憶域として使用できないようにする」	オン	変更可
OneDrive－「ドキュメントを既定で OneDrive に保存する」（既定でローカルコンピューターにドキュメントを保存する）	オン	変更可
リモートデスクトップ接続のクライアント－「パスワードの保存を許可しない」	オン	変更可
デバイスとリソースのリダイレクト－「ドライブのリダイレクトを許可しない」	オン	変更可
セキュリティ－「セキュリティで保護された RPC 通信を要求する」	オン	変更可
セキュリティ－「リモート接続にネットワークレベル認証を使用したユーザー認証を必要とする」	オン	変更可
検索－「Cortana を許可する」を無効に設定する	オン	変更可
ソフトウェア保護プラットフォーム－「KMS クライアントオンライン AVS 検証を無効にする」	オン	変更可
PC 設定の同期－「アプリを同期しない」	オン	変更可
PC 設定の同期－「スタート設定を同期しない」	オン	変更可
Windows エラー報告－「OS が生成するエラー報告のためにメモリダンプを自動送信する」を無効に設定する	オン	変更不可
Windows ログオンのオプション－「システムによる再起動後に自動的に前回の対話ユーザーでサインインする」を無効に設定する	オン	変更可
通知－「ロック画面のトースト通知をオフにする」	オン	変更可

■ ファイルサーバにおける標準モデル、ドメイン管理／併用管理環境下でのセキュリティ設定項目

ファイルサーバにおける標準モデル、ドメイン管理／併用管理という組み合わせ環境下でのセキュリティ設定を、次に示します。

表 Appendix 1.1.2-2 ファイルサーバ：標準モデル-ドメイン管理／併用管理

設定項目	チェックボックスのデフォルト状態	設定変更の可否
ローカルユーザ／グループの作成	オン	変更不可
ドメインユーザ／グループの作成	オン	変更不可
ファイル／フォルダのアクセスコントロール	オン	変更不可
パーソナルファイアウォールのチューニング	オン	変更不可
パーソナルファイアウォール－「ユニキャスト応答の許可」を無効に設定する	オン	変更可
NetBIOS over TCP/IP の無効化	オン	変更可
StorageDevicePolicies 機能の適用	オフ	変更可
USB ストレージデバイスの無効化	オフ	変更可
ユーザー権利の割り当て－「ローカルログオンを拒否」	オン	変更不可

次に続く

表 Appendix 1.1.2-2 ファイルサーバ：標準モデル-ドメイン管理／併用管理（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
セキュリティオプション－「監査：監査ポリシーサブカテゴリの設定（Windows Vista 以降）を強制して、監査ポリシーカテゴリの設定を上書きする」	オン	変更可
セキュリティオプション－「デバイス：ユーザーがプリンタードライバーをインストールできないようにする」	オン	変更可
セキュリティオプション－「デバイス：CD-ROM へのアクセスを、ローカルログオンユーザーだけに制限する」	オン	変更可
セキュリティオプション－「デバイス：フロッピーへのアクセスを、ローカルログオンユーザーだけに制限する」	オン	変更可
セキュリティオプション－「ドメインメンバー：強力な（Windows 2000 かそれ以降のバージョン）セッションキーを必要とする」	オン	変更可
セキュリティオプション－「対話型ログオン：最後のユーザー名を表示しない」	オン	変更可
セキュリティオプション－「対話型ログオン：Ctrl + Alt + Del を必要としない」を無効に設定する	オン	変更可
セキュリティオプション－「対話型ログオン：パスワードが無効になる前にユーザーに変更を促す」	オン	変更可
セキュリティオプション－「Microsoft ネットワークサーバー：クライアントが同意すれば、通信にデジタル署名を行う」	オン	変更可
セキュリティオプション－「Microsoft ネットワークサーバー：サーバー SPN ターゲット名検証レベル」	オン	変更可
「MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)」	オン	変更可
「MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)」を無効に設定する	オン	変更可
「MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)」	オン	変更可
セキュリティオプション－「ネットワークアクセス：SAM アカウントの匿名の列挙を許可しない」	オン	変更可
セキュリティオプション－「ネットワークアクセス：SAM アカウントおよび共有の匿名の列挙を許可しない」	オン	変更可
セキュリティオプション－「ネットワークアクセス：ネットワーク認証のためにパスワードおよび資格情報を保存することを許可しない」	オン	変更可
セキュリティオプション－「ネットワークセキュリティ：NTLM で Local System によるコンピューター ID の使用を許可する」	オン	変更可
セキュリティオプション－「ネットワークセキュリティ：Local System による NULL セッションフォールバックを許可する」を無効に設定する	オン	変更可
セキュリティオプション－「ネットワークセキュリティ：LAN Manager 認証レベル」	オン	変更不可
セキュリティオプション－「ネットワークセキュリティ：NTLM SSP ベース（セキュア RPC を含む）のクライアント向け最小セッションセキュリティ」	オン	変更可
セキュリティオプション－「ネットワークセキュリティ：NTLM SSP ベース（セキュア RPC を含む）のサーバー向け最小セッションセキュリティ」	オン	変更可

次に続く

表 Appendix 1.1.2-2 ファイルサーバ：標準モデル-ドメイン管理／併用管理（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
セキュリティオプション－「シャットダウン：システムのシャットダウンにログオンを必要としない」を無効に設定する	オン	変更可
セキュリティオプション－「ユーザーアカウント制御：ビルトイン Administrator アカウントのための管理者承認モード」	オン	変更可
セキュリティオプション－「ユーザーアカウント制御：管理者承認モードでの管理者に対する昇格時のプロンプトの動作」	オン	変更可
監査ポリシーの詳細な構成－「資格情報の確認の監査」	オン	変更可
監査ポリシーの詳細な構成－「コンピューターアカウントの管理の監査」	オン	変更可
監査ポリシーの詳細な構成－「その他のアカウント管理イベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「セキュリティグループの管理の監査」	オン	変更可
監査ポリシーの詳細な構成－「ユーザーアカウントの管理の監査」	オン	変更可
監査ポリシーの詳細な構成－「プロセス作成の監査」	オン	変更可
監査ポリシーの詳細な構成－「RPC イベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「アカウントロックアウトの監査」	オン	変更可
監査ポリシーの詳細な構成－「ログオフの監査」	オン	変更可
監査ポリシーの詳細な構成－「ログオンの監査」	オン	変更可
監査ポリシーの詳細な構成－「その他のログオン/ログオフイベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「特殊なログオンの監査」	オン	変更可
監査ポリシーの詳細な構成－「生成されたアプリケーションの監査」	オン	変更可
監査ポリシーの詳細な構成－「リムーバブル記憶域の監査」	オン	変更可
監査ポリシーの詳細な構成－「監査ポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「認証ポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「フィルタリングプラットフォームポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「MPSSVC ルールレベルポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「その他のポリシー変更イベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「重要な特権の使用の監査」	オン	変更可
監査ポリシーの詳細な構成－「その他のシステムイベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「セキュリティ状態の変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「セキュリティシステムの拡張の監査」	オン	変更可
監査ポリシーの詳細な構成－「システムの整合性の監査」	オン	変更可
個人用設定－「ロック画面カメラを有効にできないようにする」	オン	変更可
個人用設定－「ロック画面スライドショーを有効にできないようにする」	オン	変更可

次に続く

表 Appendix 1.1.2-2 ファイルサーバ：標準モデル-ドメイン管理／併用管理（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
WLAN 設定－「推奨されるオープンホットスポット、連絡先によって共有されたネットワーク、有料サービスを提供するホットスポットに Windows が自動的に接続することを許可する」	オン	変更可
グループポリシー－「レジストリポリシーの処理を構成する」	オン	変更可
インターネット通信の設定－「プリンタードライバーの HTTP 経由でのダウンロードをオフにする」	オン	変更可
インターネット通信の設定－「イベントビューアーの 'Event.asp' リンクをオフにする」	オン	変更可
インターネット通信の設定－「Web 発行およびオンライン注文ウィザードのインターネットダウンロードをオフにする」	オン	変更可
インターネット通信の設定－「HTTP 経由の印刷をオフにする」	オン	変更可
インターネット通信の設定－「検索コンパニオンの内容ファイルの更新をオフにする」	オン	変更可
インターネット通信の設定－「ファイルおよびフォルダーの 'Web' に発行'タスクをオフにする」	オン	変更可
インターネット通信の設定－「Windows カスタマーエクスペリエンス向上プログラムをオフにする」	オン	変更不可
インターネット通信の設定－「Windows Messenger カスタマーエクスペリエンス向上プログラムをオフにする」	オン	変更不可
ログオン－「ネットワークの選択の UI を表示しない」	オン	変更可
ログオン－「ドメインに参加しているコンピューターに接続しているユーザーを列挙しない」	オン	変更可
ログオン－「ドメインに参加しているコンピューターのローカルユーザーを列挙する」を無効に設定する	オン	変更可
ログオン－「ロック画面のアプリ通知をオフにする」	オン	変更可
軽減策オプション－「信頼されていないフォントのブロック」	オン	変更可
ユーザープロファイル－「広告 ID を無効にする」	オン	変更可
アプリのプライバシー－「Windows アプリでアカウント情報にアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリで通話履歴にアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリで連絡先にアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリでメールにアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリで位置情報にアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリでメッセージングにアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリでモーションにアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリでカレンダーにアクセスする」	オン	変更可
アプリのプライバシー－「Windows アプリでカメラにアクセスする」	オン	変更可

次に続く

表 Appendix 1.1.2-2 ファイルサーバ：標準モデル-ドメイン管理／併用管理（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
アプリのプライバシー「Windows アプリでマイクにアクセスする」	オン	変更可
アプリのプライバシー「Windows アプリで信頼済みデバイスにアクセスする」	オン	変更可
アプリのプライバシー「Windows アプリで無線を制御する」	オン	変更可
アプリのプライバシー「Windows アプリでデバイスと同期する」	オン	変更可
アプリ実行時「ホストされているコンテンツから Windows ランタイム API でアクセスする Windows ストア アプリを起動できないようにする」	オン	変更可
自動再生のポリシー「自動再生機能をオフにする」	オン	変更可
自動再生のポリシー「ボリューム以外のデバイスの自動再生を許可しない」	オン	変更可
クラウドコンテンツ「Windows のヒントを表示しない」	オン	変更可
クラウドコンテンツ「Microsoft コンシューマーエクスペリエンスを無効にする」	オン	変更可
データの収集とプレビュービルド「利用統計情報の許可」	オン	変更可
データの収集とプレビュービルド「プレリリースの機能または設定を無効にする」	オン	変更可
データの収集とプレビュービルド「フィードバックの通知を表示しない」	オン	変更可
データの収集とプレビュービルド「Insider ビルドに関するユーザーコントロールの切り替え」	オン	変更可
イベントログサービス（アプリケーション）「ログファイルの最大サイズ（KB）を指定する」	オン	変更可
イベントログサービス（セキュリティ）「ログファイルの最大サイズ（KB）を指定する」	オン	変更可
イベントログサービス（システム）「ログファイルの最大サイズ（KB）を指定する」	オン	変更可
エクスポローラー「破損後のヒープ終了をオフにする」	オン	変更可
ホームグループ「コンピューターがホームグループに参加できないようにする」	オン	変更可
OneDrive「OneDrive をファイル記憶域として使用できないようにする」	オン	変更可
OneDrive「ドキュメントを既定で OneDrive に保存する（既定でローカルコンピューターにドキュメントを保存する）」	オン	変更可
リモートデスクトップ接続のクライアント「パスワードの保存を許可しない」	オン	変更可
デバイスとリソースのリダイレクト「ドライブのリダイレクトを許可しない」	オン	変更可
セキュリティ「セキュリティで保護された RPC 通信を要求する」	オン	変更可
セキュリティ「リモート接続にネットワークレベル認証を使用したユーザー認証を必要とする」	オン	変更可
検索「Cortana を許可する」を無効に設定する	オン	変更可
ソフトウェア保護プラットフォーム「KMS クライアントオンライン AVS 検証を無効にする」	オン	変更可
PC 設定の同期「アプリを同期しない」	オン	変更可

次に続く

表 Appendix 1.1.2-2 ファイルサーバ：標準モデル-ドメイン管理／併用管理（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
PC 設定の同期－「スタート設定を同期しない」	オン	変更可
Windows エラー報告－「OS が生成するエラー報告のためにメモリダンプを自動送信する」を無効に設定する	オン	変更不可
Windows ログオンのオプション－「システムによる再起動後に自動的に前回の対話ユーザーでサインインする」を無効に設定する	オン	変更可
通知－「ロック画面のトースト通知をオフにする」	オン	変更可

■ ドメインコントローラにおける標準モデル環境下でのセキュリティ設定項目

ドメインコントローラにおける標準モデル環境下でのセキュリティ設定を、次に示します。

表 Appendix 1.1.2-3 ドメインコントローラ：標準モデル

設定項目	チェックボックスのデフォルト状態	設定変更の可否
ドメインユーザ／グループの作成	オン	変更不可
ファイル／フォルダのアクセスコントロール	オン	変更可
DCOM(OPC)のアクセスコントロール	オン	変更不可
パーソナルファイアウォールのチューニング	オン	変更不可
パーソナルファイアウォール－「ユニキャスト応答の許可」を無効に設定する	オン	変更可
NetBIOS over TCP/IP の無効化	オン	変更可
StorageDevicePolicies 機能の適用	オフ	変更可
USB ストレージデバイスの無効化	オフ	変更可
ユーザー権利の割り当て－「ネットワーク経由でのアクセス」	オン	変更可
ユーザー権利の割り当て－「ドメインにワークステーションを追加」	オン	変更可
セキュリティオプション－「監査：監査ポリシーサブカテゴリの設定（Windows Vista 以降）を強制して、監査ポリシーカテゴリの設定を上書きする」	オン	変更可
セキュリティオプション－「デバイス：ユーザーがプリンタードライバをインストールできないようにする」	オン	変更可
セキュリティオプション－「デバイス：CD-ROM へのアクセスを、ローカルログオンユーザーだけに制限する」	オン	変更可
セキュリティオプション－「デバイス：フロッピーへのアクセスを、ローカルログオンユーザーだけに制限する」	オン	変更可
セキュリティオプション－「ドメインコントローラ：Server Operators がタスクのスケジュールを割り当てるのを許可する」を無効に設定する	オン	変更可
セキュリティオプション－「ドメインコントローラ：コンピューターアカウントのパスワードの変更を拒否する」を無効に設定する	オン	変更可
セキュリティオプション－「ドメインメンバー：強力な（Windows 2000 かそれ以降のバージョン）セッションキーを必要とする」	オン	変更可
セキュリティオプション－「対話型ログオン：最後のユーザー名を表示しない」	オン	変更可

次に続く

表 Appendix 1.1.2-3 ドメインコントローラ：標準モデル（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
セキュリティオプション－「対話型ログオン：Ctrl + Alt + Del を必要としない」を無効に設定する	オン	変更可
セキュリティオプション－「対話型ログオン：パスワードが無効になる前にユーザーに変更を促す」	オン	変更可
セキュリティオプション－「Microsoft ネットワークサーバ：クライアントが同意すれば、通信にデジタル署名を行う」	オン	変更可
セキュリティオプション－「Microsoft ネットワークサーバ：サーバー SPN ターゲット名検証レベル」	オン	変更可
「MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)」	オン	変更可
「MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)」を無効に設定する	オン	変更可
「MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)」	オン	変更可
セキュリティオプション－「ネットワークアクセス：SAM アカウントの匿名の列挙を許可しない」	オン	変更可
セキュリティオプション－「ネットワークアクセス：SAM アカウントおよび共有の匿名の列挙を許可しない」	オン	変更可
セキュリティオプション－「ネットワークアクセス：ネットワーク認証のためにパスワードおよび資格情報を保存することを許可しない」	オン	変更可
セキュリティオプション－「ネットワークセキュリティ：NTLM で Local System によるコンピューター ID の使用を許可する」	オン	変更可
セキュリティオプション－「ネットワークセキュリティ：Local System による NULL セッションフォールバックを許可する」を無効に設定する	オン	変更可
セキュリティオプション－「ネットワークセキュリティ：ログオン時間を経過した場合はユーザーを強制的にログオフさせる」	オン	変更可
セキュリティオプション－「ネットワークセキュリティ：LAN Manager 認証レベル」	オン	変更不可
セキュリティオプション－「ネットワークセキュリティ：NTLM SSP ベース（セキュア RPC を含む）のクライアント向け最小セッションセキュリティ」	オン	変更可
セキュリティオプション－「ネットワークセキュリティ：NTLM SSP ベース（セキュア RPC を含む）のサーバー向け最小セッションセキュリティ」	オン	変更可
セキュリティオプション－「シャットダウン：システムのシャットダウンにログオンを必要としない」を無効に設定する	オン	変更可
セキュリティオプション－「ユーザーアカウント制御：ビルトイン Administrator アカウントのための管理者承認モード」	オン	変更可
セキュリティオプション－「ユーザーアカウント制御：管理者承認モードでの管理者に対する昇格時のプロンプトの動作」	オン	変更可
監査ポリシーの詳細な構成－「資格情報の確認の監査」	オン	変更可
監査ポリシーの詳細な構成－「コンピューターアカウントの管理の監査」	オン	変更可

次に続く

表 Appendix 1.1.2-3 ドメインコントローラ：標準モデル（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
監査ポリシーの詳細な構成－「その他のアカウント管理イベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「セキュリティグループの管理の監査」	オン	変更可
監査ポリシーの詳細な構成－「ユーザーアカウントの管理の監査」	オン	変更可
監査ポリシーの詳細な構成－「プロセス作成の監査」	オン	変更可
監査ポリシーの詳細な構成－「RPC イベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「ディレクトリサービスアクセスの監査」	オン	変更可
監査ポリシーの詳細な構成－「ディレクトリサービスの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「アカウントロックアウトの監査」	オン	変更可
監査ポリシーの詳細な構成－「ログオフの監査」	オン	変更可
監査ポリシーの詳細な構成－「ログオンの監査」	オン	変更可
監査ポリシーの詳細な構成－「その他のログオン/ログオフイベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「特殊なログオンの監査」	オン	変更可
監査ポリシーの詳細な構成－「生成されたアプリケーションの監査」	オン	変更可
監査ポリシーの詳細な構成－「リムーバブル記憶域の監査」	オン	変更可
監査ポリシーの詳細な構成－「監査ポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「認証ポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「フィルタリングプラットフォームポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「MPSSVC ルールレベルポリシーの変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「その他のポリシー変更イベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「重要な特権の使用の監査」	オン	変更可
監査ポリシーの詳細な構成－「IPsec ドライバー」	オン	変更可
監査ポリシーの詳細な構成－「その他のシステムイベントの監査」	オン	変更可
監査ポリシーの詳細な構成－「セキュリティ状態の変更の監査」	オン	変更可
監査ポリシーの詳細な構成－「セキュリティシステムの拡張の監査」	オン	変更可
監査ポリシーの詳細な構成－「システムの整合性の監査」	オン	変更可
個人用設定－「ロック画面カメラを有効にできないようにする」	オン	変更可
個人用設定－「ロック画面スライドショーを有効にできないようにする」	オン	変更可
ログオン－「ネットワークの選択の UI を表示しない」	オン	変更可
自動再生のポリシー－「ボリューム以外のデバイスの自動再生を許可しない」	オン	変更可
イベントログサービス（アプリケーション）－「ログファイルの最大サイズ（KB）を指定する」	オン	変更可

次に続く

表 Appendix 1.1.2-3 ドメインコントローラ：標準モデル（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
イベントログサービス（セキュリティ）－「ログファイルの最大サイズ（KB）を指定する」	オン	変更可
イベントログサービス（システム）－「ログファイルの最大サイズ（KB）を指定する」	オン	変更可
エクスポーラー－「破損後のヒープ終了をオフにする」	オン	変更可
セキュリティ－「セキュリティで保護された RPC 通信を要求する」	オン	変更可
ストア－「更新プログラムの自動ダウンロードおよび自動インストールをオフにする」	オン	変更可
ストア－「Windows 8 コンピューターでの更新プログラムの自動ダウンロードをオフにする」	オン	変更可
ストア－「最新バージョンの Windows への更新プログラム提供をオフにする」	オン	変更可
ストア－「ストアアプリケーションをオフにする」	オン	変更可
PC 設定の同期－「アプリを同期しない」	オン	変更可
PC 設定の同期－「スタート設定を同期しない」	オン	変更可
Windows エラー報告－「OS が生成するエラー報告のためにメモリダンプを自動送信する」を無効に設定する	オン	変更可
Windows ログオンのオプション－「システムによる再起動後に自動的に前回の対話ユーザーでサインインする」を無効に設定する	オン	変更可

Appendix 1.2 IT セキュリティバージョン 1.0

IT セキュリティバージョン 1.0 における、セキュリティ設定項目とその設定項目のデフォルト値、および設定変更の可否について説明します。ただし、OS によってセキュリティ設定項目が表示されないことがあります。

Appendix 1.2.1 CENTUM VP ソフトウェアをインストールしたコンピュータの場合

本製品ソフトウェアをインストールしたコンピュータにおける、セキュリティモデルとユーザ管理方式の組み合わせごとの、セキュリティ設定項目の一覧を示します。

■ 従来モデル環境下でのセキュリティ設定項目

従来モデル環境下でのセキュリティ設定を、次に示します。

表 Appendix 1.2.1-1 従来モデル

設定項目	チェックボックスのデフォルト状態	設定変更の可否	備考
ローカルユーザ／グループの作成	オン	変更不可	なし
ファイル／フォルダアクセスコントロール	オン	変更不可	Everyone フルコントロールのアクセス許可を追加します。 Windows フォルダの一部のツールについては、親フォルダのアクセス許可に戻します。
製品のレジストリのアクセスコントロール	オン	変更不可	Everyone フルコントロールのアクセス許可を追加します。
DCOM (OPC) アクセスコントロール	オン	変更不可	Everyone フルコントロールのアクセス許可を追加します。
パーソナルファイアウォールチューニング	オン	変更不可	パーソナルファイアウォールを無効化します。
ローカルセキュリティ	オン	変更不可	Everyone グループのアクセスを許可します。
IT 環境の設定変更－直前のログオンユーザ名の非表示	オン	変更可	なし
IT 環境の設定変更－AutoRun の制限の適用	オン	変更可	なし

参照

ユーザ／グループの作成については、以下を参照してください。

「■ Windows のユーザ管理とセキュリティモデルの組み合わせ」 ページ 2-17

■ 標準モデル、スタンドアロン環境下でのセキュリティ設定項目

標準モデル、スタンドアロン管理という組み合わせ環境下でのセキュリティ設定を、次に示します。

表 Appendix 1.2.1-2 標準モデル-スタンドアロン管理

設定項目	チェックボックスのデフォルト状態	設定変更の可否
ローカルユーザ／グループの作成	オン	変更不可
ファイル／フォルダアクセスコントロール	オン	変更不可
製品のレジストリのアクセスコントロール	オン	変更不可
DCOM (OPC) アクセスコントロール	オン	変更不可
パーソナルファイアウォールチューニング	オン	変更不可
ローカルセキュリティ	オン	変更不可
IT 環境の設定変更－LAN Manager の認証レベルの変更	オン	変更可
IT 環境の設定変更－直前のログオンユーザ名の非表示	オン	変更可

次に続く

表 Appendix 1.2.1-2 標準モデル-スタンドアロン管理（前から続く）

設定項目	チェックボックスのデフォルト状態	設定変更の可否
IT 環境の設定変更－AutoRun の制限の適用	オン	変更可
IT 環境の設定変更－NetBIOS over TCP/IP の無効化	オフ	変更可
IT 環境の設定変更－StorageDevicePolicies 機能の適用	オフ	変更可
IT 環境の設定変更－USB ストレージデバイスの無効化	オフ	変更可
IT 環境の設定変更－ソフトウェア制限ポリシーの適用	オフ	変更可

参照

ユーザ／グループの作成については、以下を参照してください。

「■ Windows のユーザ管理とセキュリティモデルの組み合わせ」 ページ 2-17

■ 標準モデル、ドメイン管理／併用管理環境下でのセキュリティ設定項目

標準モデル、ドメイン管理／併用管理という組み合わせ環境下でのセキュリティ設定を、次に示します。

表 Appendix 1.2.1-3 標準モデル-ドメイン管理／併用管理

設定項目	チェックボックスのデフォルト状態	設定変更の可否
ローカルユーザ／グループの作成	オン	変更不可
ドメインユーザ／グループの作成	オン	変更不可
ファイル／フォルダアクセスコントロール	オン	変更不可
製品のレジストリのアクセスコントロール	オン	変更不可
DCOM（OPC）アクセスコントロール	オン	変更不可
パーソナルファイアウォールチューニング	オン	変更不可
ローカルセキュリティ	オン	変更不可
IT 環境の設定変更－LAN Manager の認証レベルの変更	オン	変更可
IT 環境の設定変更－直前のログオンユーザ名の非表示	オン	変更可
IT 環境の設定変更－AutoRun の制限の適用	オン	変更可
IT 環境の設定変更－NetBIOS over TCP/IP の無効化	オン	変更可
IT 環境の設定変更－StorageDevicePolicies 機能の適用	オフ	変更可
IT 環境の設定変更－USB ストレージデバイスの無効化	オフ	変更可
IT 環境の設定変更－ソフトウェア制限ポリシーの適用	オフ	変更可

参照

ユーザ／グループの作成については、以下を参照してください。

「■ Windows のユーザ管理とセキュリティモデルの組み合わせ」 ページ 2-17

Appendix 1.2.2 ファイルサーバやドメインコントローラの場合

ファイルサーバ、またはドメインコントローラにおける、セキュリティモデルとユーザ管理方式の組み合わせごとの、セキュリティ設定項目の一覧を示します。

■ ファイルサーバにおける従来モデル環境下でのセキュリティ設定項目

ファイルサーバにおける従来モデル環境下でのセキュリティ設定を、次に示します。

表 Appendix 1.2.2-1 ファイルサーバ：従来モデル

設定項目	チェックボックスのデフォルト状態	設定変更の可否	備考
ローカルユーザ／グループの作成	オン	変更不可	CTM_PROCESS を作成します。
ファイル／フォルダアクセスコントロール	オン	変更不可	Windows フォルダについては、親フォルダのアクセス許可に戻します。 Project フォルダについては、Everyone フルコントロールのアクセス許可を追加します。
パーソナルファイアウォールチューニング	オン	変更不可	パーソナルファイアウォールを無効化します。
ローカルセキュリティ	オン	変更不可	Everyone グループのアクセスを許可します。

■ ファイルサーバにおける標準モデル、スタンドアロン管理環境下でのセキュリティ設定項目

ファイルサーバにおける標準モデル、スタンドアロン管理という組み合わせ環境下でのセキュリティ設定を、次に示します。

表 Appendix 1.2.2-2 ファイルサーバ：標準モデル-スタンドアロン管理

設定項目	チェックボックスのデフォルト状態	設定変更の可否
ローカルユーザ／グループの作成	オン	変更不可
ファイル／フォルダアクセスコントロール	オン	変更不可
パーソナルファイアウォールチューニング	オン	変更不可
ローカルセキュリティ	オン	変更不可
IT 環境の設定変更－監査ポリシーの適用	オン	変更可
IT 環境の設定変更－LAN Manager の認証レベルの変更	オン	変更可
IT 環境の設定変更－AutoRun の制限の適用	オン	変更可
IT 環境の設定変更－NetBIOS over TCP/IP の無効化	オフ	変更可
IT 環境の設定変更－StorageDevicePolicies 機能の適用	オフ	変更可
IT 環境の設定変更－USB ストレージデバイスの無効化	オフ	変更可

参照

ユーザ／グループの作成については、以下を参照してください。

「■ Windows のユーザ管理とセキュリティモデルの組み合わせ」 ページ 2-17

■ ファイルサーバにおける標準モデル、ドメイン管理／併用管理環境下でのセキュリティ設定項目

ファイルサーバにおける標準モデル、ドメイン管理／併用管理という組み合わせ環境下でのセキュリティ設定を、次に示します。

表 Appendix 1.2.2-3 ファイルサーバ：標準モデル-ドメイン管理／併用管理

設定項目	チェックボックスのデフォルト状態	設定変更の可否
ローカルユーザ／グループの作成	オン	変更不可
ドメインユーザ／グループの作成	オン	変更不可
ファイル／フォルダアクセスコントロール	オン	変更不可
パーソナルファイアウォールチューニング	オン	変更不可
ローカルセキュリティ	オン	変更不可
IT 環境の設定変更－監査ポリシーの適用	オン	変更可
IT 環境の設定変更－LAN Manager の認証レベルの変更	オン	変更可
IT 環境の設定変更－AutoRun の制限の適用	オン	変更可
IT 環境の設定変更－NetBIOS over TCP/IP の無効化	オン	変更可
IT 環境の設定変更－StorageDevicePolicies 機能の適用	オフ	変更可
IT 環境の設定変更－USB ストレージデバイスの無効化	オフ	変更可

参照

ユーザ／グループの作成については、以下を参照してください。

「■ Windows のユーザ管理とセキュリティモデルの組み合わせ」 ページ 2-17

■ ドメインコントローラにおける標準モデル、ドメイン管理／併用管理環境下でのセキュリティ設定項目

ドメインコントローラにおける標準モデル、ドメイン管理／併用管理という組み合わせ環境下でのセキュリティ設定を、次に示します。

表 Appendix 1.2.2-4 ドメインコントローラ：標準モデル-ドメイン管理／併用管理

設定項目	チェックボックスのデフォルト状態	設定変更の可否
ドメインユーザ／グループの作成	オン	変更不可
ファイル／フォルダアクセスコントロール	オン	変更可
DCOM (OPC) アクセスコントロール	オン	変更不可
パーソナルファイアウォールチューニング	オン	変更不可
IT 環境の設定変更－監査ポリシーの適用	オン	変更可
IT 環境の設定変更－LAN Manager の認証レベルの変更	オン	変更可
IT 環境の設定変更－AutoRun の制限の適用	オン	変更可
IT 環境の設定変更－NetBIOS over TCP/IP の無効化	オン	変更可
IT 環境の設定変更－StorageDevicePolicies 機能の適用	オフ	変更可
IT 環境の設定変更－USB ストレージデバイスの無効化	オフ	変更可

補足

ユーザ／グループの作成では、ドメインに作成するもののみ作成されます。

参照

ユーザ／グループの作成については、以下を参照してください。

「■ Windows のユーザ管理とセキュリティモデルの組み合わせ」 ページ 2-17

改訂情報

資料名称 : CENTUM VP セキュリティガイド

資料番号 : IM 33J01C30-01JA

2019 年 8 月 / 9 版 / R6.07 以降

- 2.1 「● セキュリティ脅威に対応するためのセキュリティ対策」に UACS ステーションの脚注を追記
- 3.1.1 「■ 対象フォルダ」に PROFINET コンフィグレータ追記
「■ プログラムのアクセス許可」に UACS マイグレーションツール追記
- 3.1.2 「■ レジストリの分類」に PROFINET コンフィグレータ追記
「■ 対象キー」に PROFINET コンフィグレータ追記
「■ レジストリのアクセス許可」に PROFINET コンフィグレータ追記
- 3.1.4 UACS ステーションにおけるローカルセキュリティポリシーを追記
- 3.4.1 「■ 設定値」追記
- 3.5.10 「■ リモートデスクトップサービス (Windows コンポーネント)」に UACS ステーションの脚注を追記
- 付録 1.1.1 「■ 標準モデル、スタンドアロン管理環境下でのセキュリティ設定項目」に UACS ステーションの脚注を追記
「■ 標準モデル、ドメイン管理 / 併用管理環境下でのセキュリティ設定項目」に UACS ステーションの脚注を追記

2018 年 8 月 / 8 版 / R6.06

- 1.2 「● セキュリティ脅威に対応するためのセキュリティ対策」に UACS ステーションの脚注を追記
- 2.1 「■ セキュリティモデルとセキュリティ対策」の表と記述を変更
- 2.2.3 「■ Windows のユーザ管理とセキュリティモデルの組み合わせ」の記述削除
「■ Vnet/IP インタフェースパッケージが追加するユーザとユーザグループ」を追加
- 3.1.1 「■ 対象フォルダ」の「表 対象フォルダ」にオートメーションデザインスイート関連のフォルダを追加
「■ 対象フォルダ」の「表 対象フォルダ」に Vnet/IP インタフェースパッケージ関連のフォルダを追加
「■ 対象フォルダ」の「表 対象フォルダ」の脚注に Windows Server 2016 の記述追加
「■ プログラムのアクセス許可」の「表 スタートメニューから起動するプログラムのアクセス許可」に Vnet/IP インタフェース管理ツールを追加
- 3.1.4 「表 ローカルセキュリティポリシーの許可状況」に Vnet/IP インタフェースパッケージ関連のユーザ / ユーザグループを追加
- 3.2 「■ Vnet/IP インタフェースパッケージ関連例外設定」を追加
- 3.3 「■ 不要な Windows サービス」の「表 サービスの中の停止可能なサービス-IT セキュリティバージョン 2.0」に Windows Server 2016 の列を追加
「■ 不要な Windows サービス」の「表 サービスの中の停止可能なサービス-IT セキュリティバージョン 1.0」に Windows Server 2016 の列を追加
- 3.5.2 「● ソフトウェア制限ポリシーを適用した場合の注意事項」の記述変更
- 3.5.6 「■ 詳細追跡」に記述追加
「■ オブジェクトアクセス」に記述追加
- 3.5.9 「■ 設定値」の「表 設定値」に記述追加
- 6.1 記述追加
- 6.6.1 「■ 変更手順」の図を変更、および記述を変更
- 6.6.2 「■ 変更手順」の記述削除
- 6.7 「■ エクスポート手順-IT セキュリティツール」の記述削除、および補足を追加
「■ エクスポート手順-IT SecuritySettingItemExport.exe」の記述削除
「■ インポート手順-IT セキュリティツール」の記述削除
- 6.8 「■ 起動手順」の記述削除

- 6.9.1 記述変更
- 6.10 節構成の見直し
- 6.10.8 「CreateVNTUser」を追加
- 付録 1.1.1 表を変更
- 付録 1.1.2 表を変更

2017 年 11 月／7 版／R6.05

- 2.1 「表 セキュリティモデルに対応するセキュリティ対策-IT セキュリティバージョン 2.0」の記述変更
- 2.2.3 「表 従来モデル」に記述追加
「表 標準モデル／強固モデルースタンドアロン管理」に記述追加
「表 標準モデル／強固モデルードメイン管理」に記述追加
「表 標準モデル／強固モデルー併用管理」に記述追加
- 3.1.1 「表 対象フォルダ」に記述追加
「表 スタートメニューから起動するプログラムのアクセス許可」に記述追加
- 3.1.2 「表 CENTUM 関連のレジストリに対するアクセス許可」に記述追加
「表 DCOM 関連のレジストリに対するアクセス許可」に記述追加
「表 PROFIBUS-DP コンフィグレータ関連のレジストリに対するアクセス許可」に記述追加
- 3.1.4 「表 ローカルセキュリティポリシーの許可状況」に記述追加
- 3.2 「表 CENTUM 関連例外設定」に記述追加
- 3.5.5 「表 設定値」の記述変更
- 3.5.7 「表 設定値」の記述変更
「■ 注意事項」の記述変更
- 3.6.8 「表 設定値」の記述変更
- 6.10 記述追加
「■ CreateAdsAgent」新規作成

2017 年 4 月／6 版／R6.04

- 1.2 システムセキュリティ強化に伴う IT セキュリティバージョン対応
- 2.1 システムセキュリティ強化に伴う IT セキュリティバージョン対応
- 3. システムセキュリティ強化に伴う IT セキュリティバージョン対応
- 4. システムセキュリティ強化に伴う IT セキュリティバージョン対応
- 6. 構成変更
- 付録 新規追加

2016 年 9 月／5 版／R6.03.10

- 2.2.3 ユーザ名 RDC_PROCESS の説明を変更
- 3.1.1 「■ 対象フォルダ」の記述変更
- 3.2 「■ 例外設定タイプ」の記述変更
「■ CENTUM 関連例外設定」の記述変更
「■ UGS 冗長化機能（コンピュータ切替型）冗長化プラットフォームの設定」を削除
- 3.3 「■ 不要な Windows サービス」の記述変更
- 3.4.1 記述変更
「■ UGS 冗長化機能（コンピュータ切替型）冗長化プラットフォームのユーザ名を変更する場合の注意事項」を「■ コンピュータ切替型 UGS の PC 冗長化プラットフォームのユーザ名を変更する場合の注意事項」にタイトル変更、および記述変更
- 3.4.11 「■ 設定値」の記述変更
「■ 注意事項」に記述追加

6.2 「■ CreateRDCProcess」の「● 詳細説明」の記述変更

2016 年 6 月／4 版／R6.03

- 2.2.3 ユーザ名に RDC_PROCESS を追加
- 3.1.1 UGS 冗長化関連のフォルダとユーザ名／グループ名を追加
- 3.1.2 OS に Windows Server 2012 R2 を追加、およびユーザ名に RDC_PROCESS を追加
- 3.1.4 ユーザ名に RDC_PROCESS を追加
- 3.2 UGS 冗長化機能の記述を追加
- 3.3 OS に Windows Server 2012 R2 を追加
- 3.4.1 UGS 冗長化機能の記述を追加、および OS に Windows Server 2012 R2 を追加
- 3.4.3 OS に Windows Server 2012 R2 を追加
- 3.4.11 UGS 冗長化機能の記述を追加
- 6.2 RDC_PROCESS の記述を追加

2015 年 12 月／3 版／R6.02

- 3.1.1 ADSuite フォルダ名称の変更
- 6.2 CreateAdsProcess の重要事項に追記

2015 年 4 月／2 版／R6.01.10

- 2.2.3 記述を変更

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
