

情報種別: 秘密(統合開発セキュリティ基盤サービス関係者限り)
会社名: NTT DATA GROUP CORP.
情報所有者: IT マネジメント室

統合開発セキュリティ基盤 アクセス中継サービス 利用マニュアル(グループ会社向け)

第 1.3 版

2024 年 4 月 1 日
株式会社 NTT データグループ IT マネジメント室

改訂履歴

版数	改訂日	改定項目	改定内容	改定理由
1.0	2021/07/05	初版公開	第 1.0 版を公開	
1.01	2021/08/23	1.1. サービス概要	軽微な修正	
1.2	2023/07/11	1.1.1 中継デスクトップ 1.1.2 ファイル中継	イメージ図の修正	
1.2	2023/07/11	3.2.1 グループ共用セキュリティ基盤経由でのアクセス	補足説明を追記	
1.3	2024/04/01	1.1. サービス概要 3.1. インスタンス情報の確認 3.7.[ファイル中継] 個別権限付与申請 3.8.[ファイル中継] 大容量ストレージ時利用申請 3.6.監査ログの確認	申請フォーマットの名称変更 ファイル中継機能利用申請フォーマットについての記載を削除 3.1.1・3.1.2 の項番を追加。 3.7・3.8.の項番を追加 3.6.1・3.6.2 の項番を追加	
1.3	2024/04/01	全般	株式会社エヌ・ティ・ティ・データ再編に伴う情報種別および一部表記の変更	

本マニュアルは著作権上の保護を受けています。本マニュアルの一部あるいは全部について、著者からの許諾を得ずに、いかなる方法においても無断で複写、複製することは禁じられています。

その他、本書に掲載されている商品名、会社名などは各会社の商標または登録商標です。

本文中では、TM、(R)マークは表示していません。

本マニュアルに記載されている事柄は、将来予告なしに変更することがあります。

目次

第 1 章 はじめに	1
1.1. サービス概要.....	1
1.1.1. 中継デスクトップ.....	1
1.1.2. ファイル中継.....	3
1.2. 前提条件	4
1.2.1. 利用者	4
1.2.2. 利用条件.....	4
1.2.3. 推奨環境.....	5
第 2 章 サービスの申請方法	6
2.1. 接続する開発 LAN による事前準備・前提.....	6
2.2. 利用開始申請.....	6
2.3. 利用終了申請.....	11
第 3 章 サービスの利用方法	14
3.1. インスタンス情報の確認.....	14
3.1.1. 中継デスクトップの場合	14
3.1.2. ファイル中継の場合.....	16
3.2. 中継デスクトップの利用.....	17
3.2.1. グループ共用セキュリティ基盤経由でのアクセス.....	17
3.3. ファイル中継の利用	19
3.4. インスタンス再起動	20
3.5. インスタンス強制停止.....	20
3.6. 監査ログ確認.....	20
3.6.1. 中継デスクトップの場合	21
3.6.2. ファイル中継の場合.....	22
3.7. [ファイル中継] 個別権限付与申請	23
3.8. [ファイル中継] 大容量ストレージ時利用申請	24

第 1 章 はじめに

本書では、統合開発セキュリティ基盤(UDS)のサービスの 1 つである、アクセス中継サービス(以降、UDS アクセス中継)の概要・利用方法について記載する。本章では、本サービスの概要について説明する。

1.1. サービス概要

本サービスは、本来各プロジェクトで相互接続してはならない利用会社イントラネット(グループ共用セキュリティ基盤)と開発 LAN について、それらの 2 つのネットワーク間を安全に接続し、特定の方法でイントラネットから開発 LAN に入る、イントラネットと開発 LAN 間でファイル授受を可能にする、というサービスである。

開発 LAN は、「統合開発セキュリティ基盤」(UDS)に接続可能である。

本サービスでは、役割に応じて以下 2 つのインスタンスがあり、G 会社の利用者は中継デスクトップ、ファイル中継を払い出すことができる。

- 中継デスクトップ
- ファイル中継

それぞれの機能概要について、以降の項にて示す。

1.1.1. 中継デスクトップ

中継デスクトップとは、利用会社イントラネットからリモートデスクトップ接続が可能な Windows デスクトップ環境である。デスクトップには開発環境への SSH 接続、X-NET/統合開発クラウドのサービス利用等可能なブラウザが用意されている。

ログイン可能な人数に制限があるため、主に少人数開発向けの機能である。

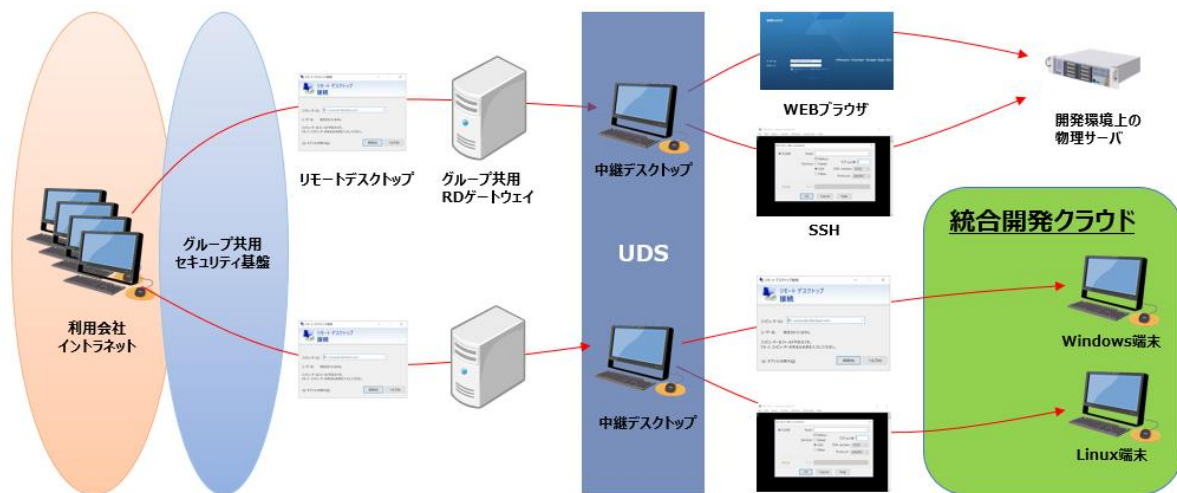


図 1 中継デスクトップの利用イメージ

中継デスクトップで提供される機能、明示的に制限される機能は以下の通りである。

- 中継デスクトップが提供する機能

- リモートデスクトップクライアント
- SSH ターミナル
- Web ブラウザ利用
- アクセスログ閲覧
- インスタンスの再起動・強制停止

- 中継デスクトップ上で制限される機能

- クリップボード共有
- ローカルデバイスのアタッチ
- 各種アプリケーションのインストール・OS 設定変更等
- SMB のアクセス制限(WindowsXP/WindowsServer2003R2 以前のアクセス不可)

中継デスクトップは SMB の接続を制限しているため、ファイルの送受信はできない。

中継デスクトップは以下のようなケースで有効である。

- **統合開発クラウド評価利用のためのアクセス環境**

- PJ適用のため統合開発クラウドの機能確認などを主な目的とした場合は、中継デスクトップを利用すると簡単に統合開発クラウドのサービスを利用可能なアクセス環境が準備できる。

- **小規模開発プロジェクトでの開発環境**

- 数人の開発メンバーによる小規模なプロジェクトであれば 1~2 台の中継デスクトップを申請すれば、すぐにアクセス環境を準備できる。

- **開発 LAN 上でのインフラ環境等の開発が主でアプリケーション開発がない**

- IDE 等が必要なく SSH 接続が出来ればよい場合、中継デスクトップには TeraTerm や Putty は用意されているので、払い出してすぐ利用ができる。

1.1.2. ファイル中継

イントラネット、開発 LAN 間でのファイルを中継するための、一時的にデータ格納が可能な領域を提供する。イントラネット(グループ共有セキュリティ基盤)上の Windows 端末から、また開発 LAN 側の Windows 端末から、ファイル共有(SMB プロトコル)でアクセスし、ファイルの配置・取得が可能である。

中継デスクトップでは、クリップボード共有やファイル共有機能は制限されているため、ファイル中継機能を介してイントラネット、開発 LAN 間でのデータの授受を行う。

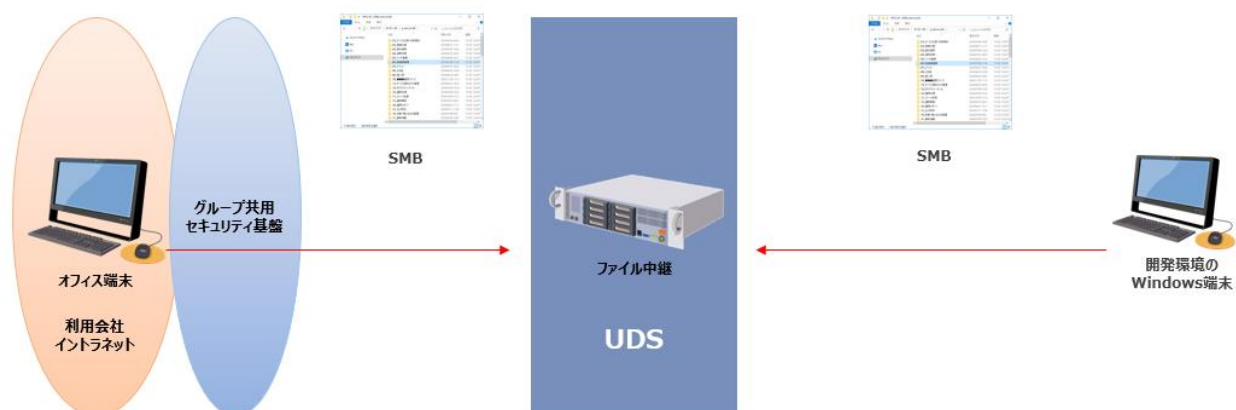


図 2 ファイル中継の利用イメージ

ファイル中継インスタンスで提供される機能、制限されている機能は以下の通りである。

- **ファイル中継上で提供する機能**
 - イン트라ネット(グループ共用セキュリティ基盤)、開発 LAN からの SMB2.0 以上によるファイル共有
 - アクセスログの保存・閲覧
 - インスタンスの再起動・強制停止
- **ファイル中継上で制限されている機能**
 - ファイル中継へのリモートデスクトップ接続
 - SMB2.0 未満のアクセス制限(WindowsXP/WindowsServer2003R2 以前のアクセス不可)

また、ファイル中継環境内の D ドライブにあるファイルは、メンテナンスのファイル削除処理が実行されるタイミングで削除される。(フォルダは削除されない)。E ドライブにあるファイル、フォルダは削除されない。
そのため、永続的にファイルを保管する用途には使用できない点に注意する必要がある。

1.2. 前提条件

UDS アクセス中継サービスを利用するための前提条件を説明する。

1.2.1. 利用者

本サービスの利用者は下記の通りとする。

- 「NTT データグループ協定」及び「NTT データグループ運営費に関する契約」を締結した G 会社
- ・グループ共用セキュリティ基盤契約済の会社

1.2.2. 利用条件

本サービスの利用条件は下記の通りとする。

- 利用は国内からのみであること。
- UIM に、利用者全員のアカウントが登録済みであること。
- UIM に、テナント管理者全員の UIM アカウントが登録されているプロジェクトグループを登録済みであること。
- 「NTT データグループ協定」及び「NTT データグループ運営費に関する契約」を締結していること。
- 海外拠点、非居住者が利用する場合は輸出管理申請が完了していること。
- アクセスする「すべての拠点」で、CAL(クライアントアクセスライセンス)または UAF(マイクロソフト包括ライセンス)を保持していること。

- 換金性の高い情報は取り扱わないこと。

1.2.3. 推奨環境

UDS アクセス中継サービスを利用するクライアント OS は下記のバージョン以上を推奨している。また、Windows 以外の OS からの接続は推奨しない。

- Windows 10 以上（クライアント OS）
- Windows Server 2016 以上（サーバ OS）

第 2 章 サービスの申請方法

本章では、UDS アクセス中継サービスを利用するための各インスタンス払出し申請の方法について説明する。

2.1. 接続する開発 LAN による事前準備・前提

UDS アクセス中継サービスの各インスタンスは、必ず 2 つのネットワーク「イントラネット(グループ共用セキュリティ基盤)」と、「開発 LAN」に接続する。各インスタンスの払出し時に、どの開発 LAN(UDS NW) に接続するかを選択することができる。

払い出す UDS アクセス中継サービスの開発 LAN 側のネットワークを、「統合開発セキュリティ基盤」(UDS)に接続するため、事前に以下の条件を満たす必要がある。

① 接続先の UDS ネットワークが既に存在していること

接続先の UDS ネットワークの実体が存在しない場合、UDS アクセス中継サービスの払出しはできない。そのため、事前に統合開発クラウドダッシュボードより、UDS 申請を起案する必要がある。

新規の UDS ネットワーク払出しの申請については [UDS 電子申請クイックスタートマニュアル](https://uds-portal.x-network.jp/uds/doc/01_manual/08_manual_quickstart_group.xlsx)を参照すること。

https://uds-portal.x-network.jp/uds/doc/01_manual/08_manual_quickstart_group.xlsx

② UDS アクセス中継サービス申請から、既存のセグメントまたは新規にセグメントを登録して払い出すことが可能 (詳細は 2.2. 利用開始申請に記載)

2.2. 利用開始申請

UDS アクセス中継サービス利用開始にあたっての申請方法について以下に説明する。

UDS アクセス中継サービスのサービスインスタンスには 3 つの種類(「中継デスクトップ」、「RD ゲートウェイ」、「ファイル中継」)が存在するが、申請書は 1 種類で共通となる。申請書 1 件につき 1 インスタンスを払い出すことができる。

※G 会社向けは「RD ゲートウェイ」のサービスは提供しておりません。

以下に UDS アクセス中継サービスのインスタンスを払出すための申請方法を示す。

1. ダッシュボードトップ画面の左メニューから「新規契約の申請」を選択する。

統合開発セキュリティ基盤 アクセス中継サービス 利用マニュアル



2. カテゴリから「UDS アクセス中継サービス申請」を選び、「申請/処理開始」アイコンを押下する。

	UDS：関連作業申請
	UDS：端末セキュリティ管理サービス申請
	UDS：リモートアクセスサービス申請
	UDS：ネットワーク接続サービス申請
	UDS：セキュアインターネットアクセスサービス申請
	UDS：インターネットメールセキュリティサービス申請
	UDS基本申請
	UDSアクセス中継サービス申請

3. UDS アクセス中継サービス申請画面から、以下の必須項目を選択・入力する。

・事前確認

事前確認

- ☐ 開発環境（もしくは検証用途）として利用すること。(*)
商用サービスを提供する本番環境として利用してはならない。
また、他の利用者の利用に支障を及ぼす可能性のある、性能や可用性などの非機能要件に対する検証（負荷試験など）は実施してはならない。
- ☐ 統合開発セキュリティ基盤PJグループIDが作成済みであること。(*)
- ☐ ネットワーク経路が確保されていること。(*)
アクセス元端末がNOANETに接続可能であること。

内容を確認し、チェックを入れる。

・基本情報

統合開発セキュリティ基盤 アクセス中継サービス 利用マニュアル

基本情報

グループ会社プライム案件での利用

☐ グループ会社プライム案件で利用する。

グループ会社名

① 利用サービス(*)

② メンテナンスタイミング(*)

③ インスタンスタイプ(*)

④ クラスタ(*)

自動

※ 各インスタンスタイプのスペック情報は以下の表を参照してください。

インスタンスタイプ

利用サービス

CPU(コア)

メモリ(GB)

B1

中継デスクトップ 12人用

4

8

B2

中継デスクトップ 24人用

8

12

G1

RDゲートウェイ

4

8

F1

ファイル中継(中継領域50GB)

4

8

⑤ ログイン認証用PJグループID(*)

pgr

⑥ 監査ログ参照用PJグループID(*)

pgr

利用終了

☐ UDSアクセス中継サービスの利用を終了します。

① 利用サービス

利用サービスに応じて以下のみ選択できる

- 中継デスクトップ
- ファイル中継

② メンテナンスタイミング

インスタンス再起動を含むメンテナンスタイミングを指定する。ここで指定した時間帯は、利用者は当該インスタンスへのログインや、再起動等を行うことができない

③ インスタンスタイプ

同画面上のインスタンスタイプ スペック表を参照し、利用サービスに必要なスペックを指定する(中継デスクトップ(B1または B2)、ファイル中継(F1)が選択できる)

④ クラスタ

インスタンスのデータを格納する物理クラスタを指定する。特に要件が無い場合は「自動」を選択すると、インスタンス払出し時にいずれかのクラスタが選択される

⑤ ログイン認証用PJグループID

統合開発セキュリティ基盤のワークフローシステムにおけるプロジェクト ID を指定する。ここで指定したグループにユーザが所属するか否かで、各サービスの認可(ログイン可否)が決定される。

⑥ 監査ログ参照用PJグループID

統合開発セキュリティ基盤のワークフローシステムにおけるプロジェクト ID を指定する。ここで指定したグループにユーザが所属するか否かで、各インスタンスの監査ログの閲覧可否が決定される。

統合開発セキュリティ基盤 アクセス中継サービス 利用マニュアル

・接続情報

インスタンスを接続するネットワークを選択する。

接続情報

接続するネットワーク(*)

UDS.pgrtest

● 利用中のアドレスレンジから選択

○ 新規でアドレスレンジを登録

※ 利用中のIPアドレスレンジが存在しない、または払出可能なIPアドレスレンジが存在しない場合は、新規でアドレスレンジを登録してください。

※ 接続するネットワークは後から変更できないためご注意ください。

※ 同一ネットワークに接続したサービス・テナントに限り、相互通信可能です。
(異なるネットワークに接続したサービス・テナント同士は相互通信できません)

※ 本プルダウンには払出し途中のUDSネットワーク(統合開発セキュリティ基盤申請)は表示されません。

※ 接続したいUDSネットワークが払出し途中の場合、払出し完了まで本申請の起案はお待ちください。

開発LAN側IP払出し元(*)

エラー! 参照元が見つかりません。で事前に指定したIPアドレスレンジから、本サービスで利用するIPアドレスレンジを指定する場合は、ラジオボタン「利用中のアドレスレンジから選択」を指定し、開発 LAN 側 IP 払出し元から既存の IP アドレスレンジを選択可能。

新規にセグメントを払い出す場合は「新規でアドレスレンジを登録」ラジオボタンを指定し、「UDS アクセス中継サービスに割り振る IP アドレスレンジ(CIDR 形式)」欄に直接セグメントを入力する。

○ 利用中のアドレスレンジから選択

● 新規でアドレスレンジを登録

※ 利用中のIPアドレスレンジが存在しない、または払出可能なIPアドレスレンジが存在しない場合は、新規でアドレスレンジを登録してください。

UDSアクセス中継サービスに
割り振る
IPアドレスレンジ(CIDR形式)

ネットワーク内のIP利用状況一覧

申請に伴う確認項目

申請に伴う確認項目

☐

統合開発クラウドの利用規約に同意します。 (*)

☐

最大料金について同意します。(下記の最大料金確認ボタンを押下することでチェック可能になります) (*)

最大料金確認

本申請及び、同一ダッシュボードから申請中のUDSアクセス中継サービスが全て承認された場合、ダッシュボード内のUDSアクセス中継サービス利用料金が最大で以下ようになります。

内容を確認し、チェックを入れる。

4. 返却情報

統合開発セキュリティ基盤 アクセス中継サービス 利用マニュアル

返却情報

UDSアクセス中継サービスID		クラスタ	
UDSアクセス中継サービスのIPアドレス(NOANET側)		UDSアクセス中継サービスのIPアドレス(開発LAN側)	

処理

「処理」を押下する。

※NOA-NET 側＝イントラネット側

5. 申請確認画面

申請/処理開始 [申請]

フロー

案件名 *	UDSアクセス中継サービス申請
申請/処理開始者	
申請/開始基準日	2019/07/12
担当組織 *	NTT DATA
優先度	通常
コメント	

申請

申請/処理開始 ウィンドウが表示されるので、表示されている内容を確認し「申請」を押下する。

6. 申請受付完了確認メール

申請受付のメールが自動送信されるので、記載されている申請番号と識別子を確認する。

7. 申請中の状況確認

統合開発クラウド

サービスを契約する

- 新規契約の申請
- 既存契約確認・変更申請
- 申請中の状況
- 対処が必要な申請
- 申請履歴

サービスを使う

- 利用できるサービス
- 開発環境のPPを調べる
- 構成情報確認

ダッシュボードトップ

お知らせ

2019.05.08	公開testタイトル
2018.10.25	【仕様変更】開発BXO管理ポータル テナント名仕様
2018.10.25	画像表示テスト
2018.09.10	【テスト】お知らせのテスト
2018.08.10	【お知らせ】ポータル画面リニューアルに伴い、皆

ダッシュボードトップ画面の左メニューから「申請中の状況」を選択する。

項番7で確認した申請番号が申請中案件にあることを確認する。進行状況を確認する場合は「申請状態・履歴」アイコンを押下する。

8. 申請フロー完了メール

申請フロー完了のメールが自動送信され、サービスが利用可能になる。

2.3. 利用終了申請

UDS アクセス中継サービス利用終了にあたっての申請方法について以下に説明する。

1. ダッシュボードトップ画面の左メニューから「既存契約確認・変更申請」を選択する。



2. カテゴリから「UDS アクセス中継サービス申請」を選び、「申請/処理開始」アイコンを押下する。

	UDS：関連作業申請
	UDS：端末セキュリティ管理サービス申請
	UDS：リモートアクセスサービス申請
	UDS：ネットワーク接続サービス申請
	UDS：セキュアインターネットアクセスサービス申請
	UDS：インターネットメールセキュリティサービス申請
	UDS基本申請
	UDSアクセス中継サービス申請

3. UDS アクセス中継サービス申請画面から、基本情報-利用終了 のチェックを入れる。

統合開発セキュリティ基盤 アクセス中継サービス 利用マニュアル

基本情報

グループ会社プライム案件での利用

☐ グループ会社プライム案件で利用する。

グループ会社名

利用サービス(*)

メンテナンスタイミング(*)

インスタンスタイプ(*)

クラスタ(*)

自動

※ 各インスタンスタイプのスペック情報は以下の表を参照してください。

インスタンスタイプ	利用サービス	CPU(コア)	メモリ(GB)
B1	中継デスクトップ 12人用	4	8
B2	中継デスクトップ 24人用	8	12
G1	RDゲートウェイ	4	8
F1	ファイル中継(中継領域50GB)	4	8

ログイン認証用PJグループID(*)

pgr

監査ログ参照用PJグループID(*)

pgr

利用終了

☐ UDSアクセス中継サービスの利用を終了します。

4. 返却情報 の内容を確認し、「処理」を押下する。

返却情報

UDSアクセス中継サービスID

クラスタ

UDSアクセス中継サービスのIPアドレス(NOANET側)

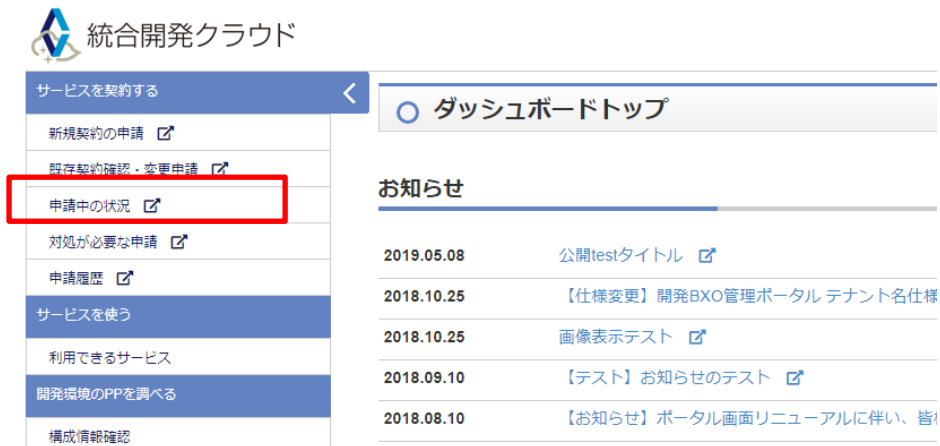
UDSアクセス中継サービスのIPアドレス(開発LAN側)

処理

5. 申請受付完了確認メール

申請受付のメールが自動送信されるので、記載されている申請番号と識別子を確認する。

6. 申請中の状況確認



ダッシュボードトップ画面の左メニューから「申請中の状況」を選択する。

項番5で確認した申請番号が申請中案件にあることを確認する。進行状況を確認する場合は「申請状態・履歴」アイコンを押下する。

7. 申請フロー完了メール

申請フロー完了のメールが自動送信され、サービスが利用終了される。

第 3 章 サービスの利用方法

本章では、払い出し済みの統合開発セキュリティ基盤 アクセス中継サービスに対して、実際にログイン・制御等を行う手順について説明する。

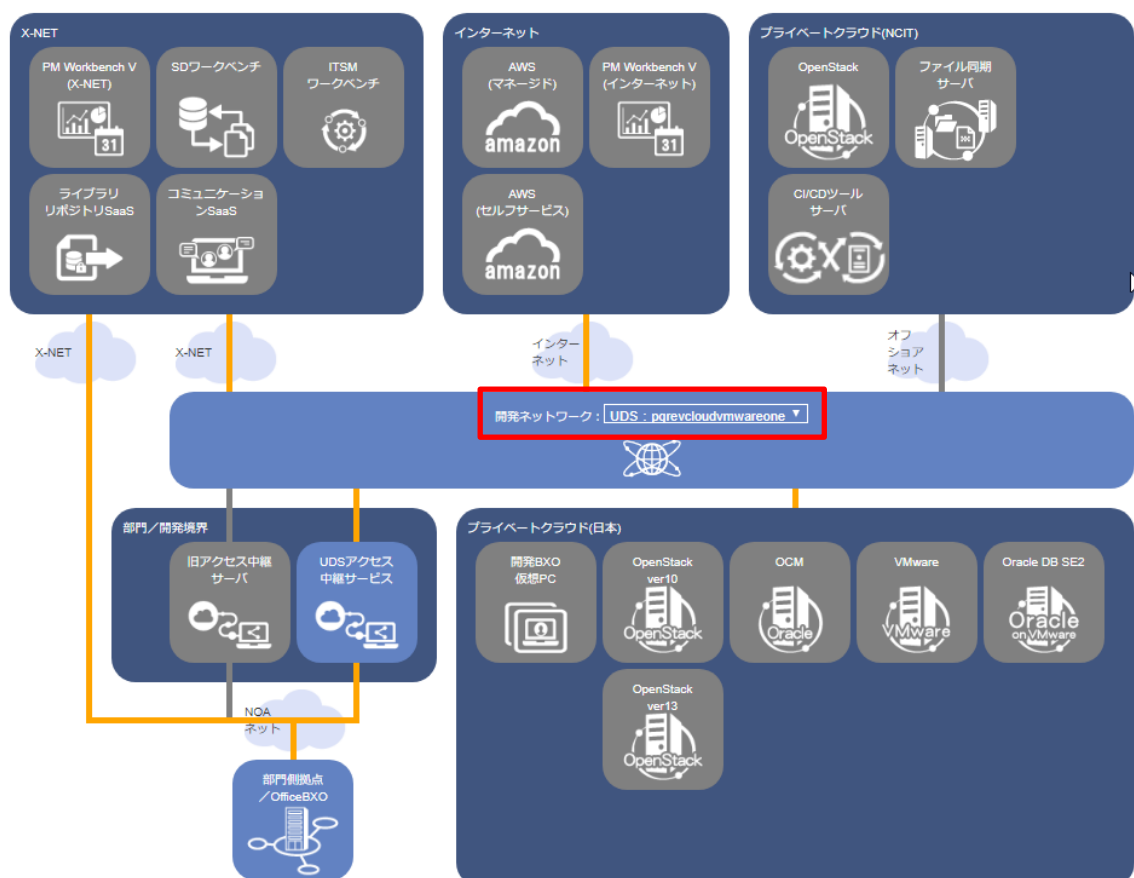
3.1. インスタンス情報の確認

払い出されたアクセス中継サービスのインスタンス情報を確認する手順を以下に説明する。

3.1.1. 中継デスクトップの場合

1. ダッシュボードトップ画面で、払い出した UDS アクセス中継サービスが接続されたネットワークを選択する

利用できるサービス



UDSアクセス中継サービス のアイコンが活性化されていれば押下する。

※活性化していなければ払出しが完了していない可能性がある。

2. 現在払い出されているUDSアクセス中継サービスの一覧が表示されるので対象のインスタンスIDを押下する。



3. インスタンス情報画面がポップアップするので、以下の情報を確認する。(利用サービスによっては表示されない情報がある)

インスタンスID : harsbs0008 (中継デスクトップ)

認証・認可情報

RDPログイン可能グループ: pgrarstest

監査ログ参照可能グループ: pgrevccloudvmwareone

※ ご自身が当該グループに所属しているかは、WorkflowSystem(グループ管理者検索)から確認してください。
※ グループメンバの追加は、グループの管理者または副管理者にて、WorkflowSystem(申請管理)より「新規申請」プロジェクトグループメンバ追加申請」を選択して申請してください。

利用区分	ログインID	パスワード
NTTデータ社員	JAPAN\氏名コード	X-UIMで設定
NTTデータ協働者	JAPAN\IU*****	X-UIMで設定
社外ユーザ	GUEST\g*****	WorkflowSystemで設定

アクセス情報(NOANET側)

RDPアドレス: 10.201.0.8

監査ログパス: \\10.201.0.8\Archives

アクセス情報(開発LAN側)

RDPアドレス: 192.168.15.5

メンテナンス情報

メンテナンスタイミング: 金曜日22時～土曜日6時

クラスタ: Cluster1B

状態: 取得中... 再起動 強制停止

3.1.2. ファイル中継の場合

1. ダッシュボードトップ画面で、「既存契約確認・変更申請」を選択する。



サービスを契約する

新規契約の申請

既存契約確認・変更申請

申請中の状況

対処が必要な申請

申請履歴

サービスを使う

利用できるサービス

使い方に困ったら

問い合わせ方法

FAQ

2. 申請したファイル中継の UDS アクセス中継サービス申請の「詳細」を選択する。

完了案件							
変更申請	カテゴリ	識別子	最終更新日	申請者	親申請番号	詳細	
	UDSアクセス中継サービス申請						
	UDSアクセス中継サービス申請						
	UDSアクセス中継サービス申請						
	UDSアクセス中継サービス申請						
	UDSアクセス中継サービス申請						

3. 申請書内の「返却情報」から「UDS アクセス中継サーバ用スタティック NAT 後 IP アドレス」の項目を確認する。

返却情報

UDSアクセス中継サービスID

クラスタ

UDSアクセス中継サービスのIPアドレス(NOANET側)

UDSアクセス中継サービスのIPアドレス(開発LAN側)

UDSアクセス中継サービスのFQDN (NOANET側/セキュアFAT側共通)

UDSアクセス中継サーバ用スタティックNAT後IPアドレス

3.2. 中継デスクトップの利用

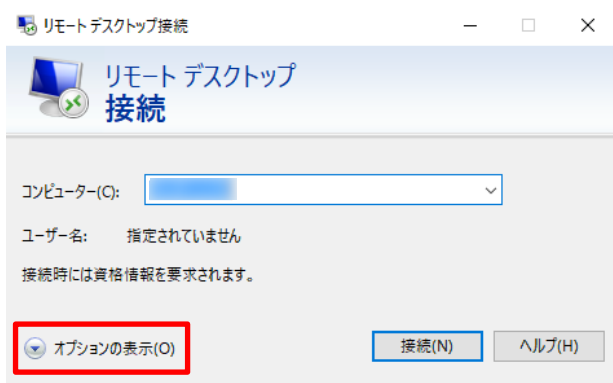
中継デスクトップへのリモートデスクトップ接続方法を以下に説明する。

3.2.1. グループ共有セキュリティ基盤経由でのアクセス

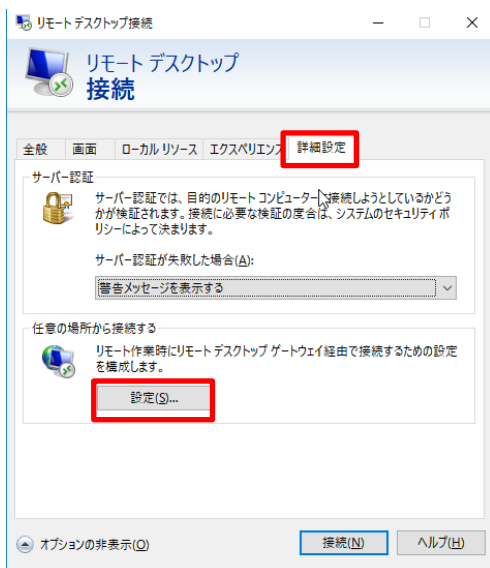
グループ共有セキュリティ基盤経由で中継デスクトップへ接続する場合は、以下の手順を行う。

※グループ共有セキュリティ基盤、インターネット Web アクセスサービス利用環境の場合は、プロキシサーバの例外設定に `[*.x-network.jp;]` が必要です。

1. ファイル名を指定して実行 → `mstsc` を実行し、リモートデスクトップを起動し、「オプションの表示」を展開する。



2. 詳細設定タブを展開し、「設定」を押下する。



統合開発セキュリティ基盤 アクセス中継サービス 利用マニュアル

3. 接続設定から以下の内容を設定して、「OK」を押下する。

・次の RD ゲートウェイサーバー設定を使用する を選択

-サーバ名(以下のグループ共用 RD ゲートウェイを使用する):

harsgg0001.x-network.jp

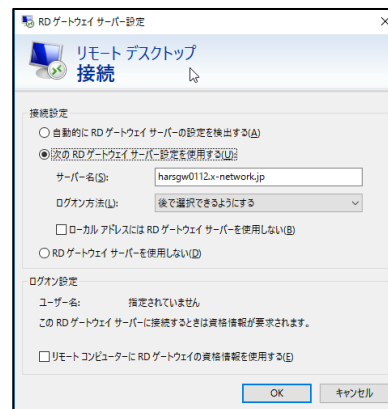
harsgg0002.x-network.jp

harsgg0003.x-network.jp

harsgg0004.x-network.jp

harsgg0005.x-network.jp

※グループ共用 RD ゲートウェイは共用サービスのため、
別途申請は必要ございません。



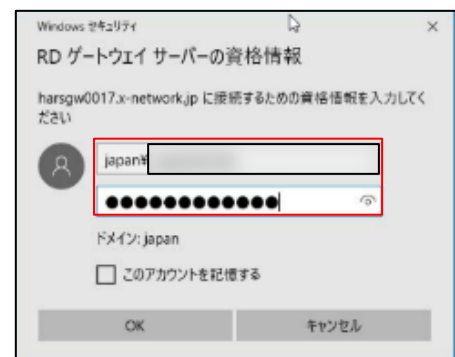
・ローカルアドレスには RD ゲートウェイサーバーを使用しない のチェックをはずす

4. 全般タブから、対象の中継デスクトップ RDP アドレスを入力し、「接続」を押下する。

5. RD ゲートウェイサーバーの資格情報の入力画面がポップアップするので、以下の情報を入力し、「OK」を押下する。

アカウント:japan¥UIM のログイン ID

パスワード: UIM ログイン時のパスワード



6. 中継デスクトップインスタンスのログイン画面で、以下の情報を入力する。

アカウント:japan¥UIM のログイン ID

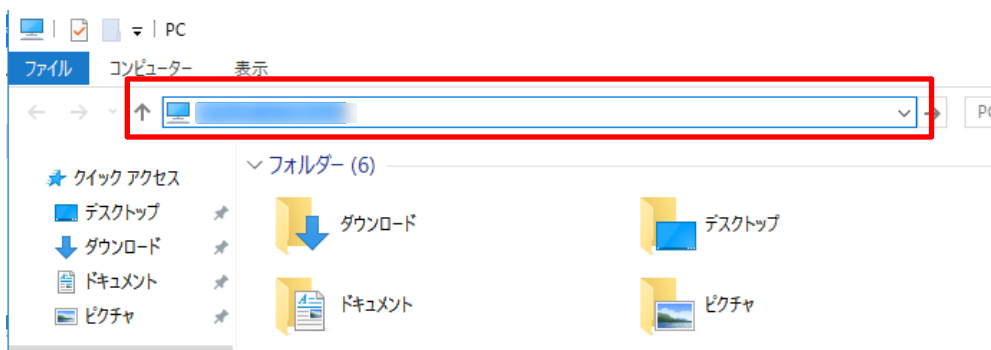
パスワード: UIM ログイン時のパスワード

7. 対象の中継デスクトップインスタンスへログインしたことを確認する。

3.3. ファイル中継の利用

ファイル中継サービスのファイル転送手順を以下に説明する。

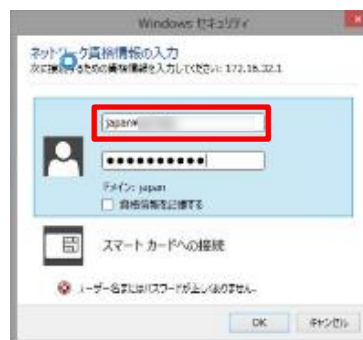
1. ファイル転送を行うファイル中継インスタンスの情報画面を3. 1. 2.の手順で開く。
2. 「UDS アクセス中継サーバ用スタティック NAT 後 IP アドレス」の項目を確認する。
3. 操作端末のエクスプローラで「¥¥<確認した IP アドレス>¥share」を入力し、Enterを押下する。



4. ネットワーク資格情報の入力画面がポップアップするので、以下の情報を入力し、「OK」を押下する。

アカウント:japan¥UIM のログイン ID

パスワード:UIM ログイン時のパスワード

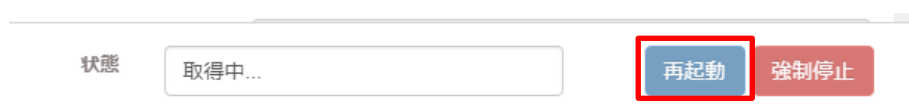


5. 共有フォルダ(share)にアクセス出来ることを確認する。

3.4. インスタンス再起動

インスタンス障害や手動メンテナンスなどの要請に応じて、ユーザが手動で再起動を行うための手順を以下に説明する。

1. 再起動を行う対象のインスタンスの情報画面を3. 1. 1 項番2、3の手順で開く。
2. 画面下部にある「再起動」を押下する。



状態を確認して、停止→起動 となることを確認する。

3.5. インスタンス強制停止

ウイルス感染などの緊急時に、インスタンスを外部から即時停止したい場合に、下記の手順で強制的に停止することができる。
本手順で強制停止したインスタンスは、恒久的に使用できなくなる。

外部から手動でインスタンス強制停止を行うための手順を以下に説明する。

1. 強制停止を行う対象のインスタンスの情報画面を3. 1. 1 項番2、3の手順で開く。
2. 画面下部にある「強制停止」を押下する。



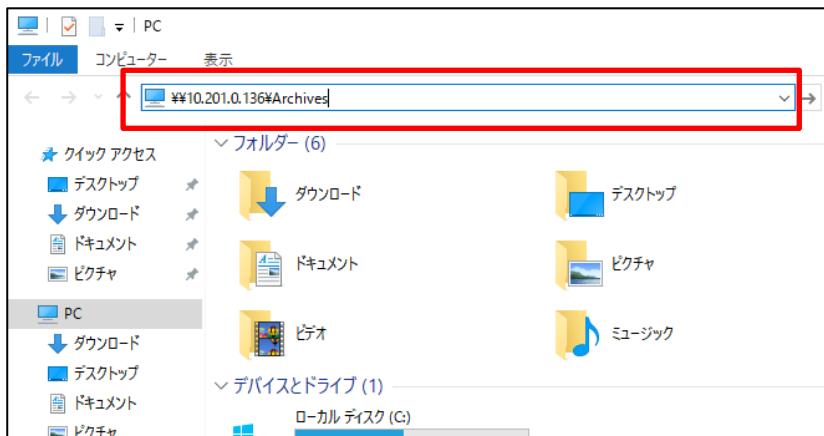
状態を確認して、停止 となることを確認する。

3.6. 監査ログ確認

各アクセス中継サービスのセキュリティイベントログにアクセスする手順を以下に説明する。

3.6.1. 中継デスクトップの場合

1. 監査ログ確認を行う対象のインスタンスの情報画面を3. 1. 1 項番2、3の手順で開く。
2. アクセス情報 から監査ログパスを確認する。
3. 項番 2 で確認した監査ログパスを操作端末のエクスプローラで入力し、Enterを押下する。



4. ネットワーク資格情報の入力画面がポップアップするので、以下の情報を入力し、「OK」を押下する。

アカウント:japan¥UIM のログイン ID

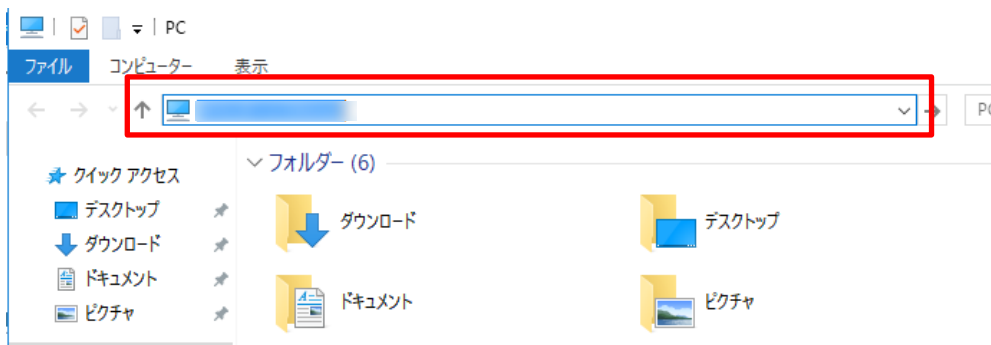
パスワード:UIM ログイン時のパスワード



5. 監査ログを格納したフォルダ (archive) にアクセス出来ることを確認する。

3.6.2. ファイル中継の場合

1. ファイル転送を行うファイル中継インスタンスの情報画面を3. 1. 2.の手順で開く。
2. 「UDS アクセス中継サーバ用スタティック NAT 後 IP アドレス」の項目を確認する。
3. 操作端末のエクスプローラで「¥¥<確認した IP アドレス>¥archive」を入力し、Enterを押下する。



4. ネットワーク資格情報の入力画面がポップアップするので、以下の情報を入力し、「OK」を押下する。

アカウント:japan¥UIM のログイン ID

パスワード: UIM ログイン時のパスワード



5. 監査ログを格納したフォルダ (archive) にアクセス出来ることを確認する。

3.7. [ファイル中継] 個別権限付与申請

複数プロジェクトでファイル中継インスタンスを共用する場合など、共有フォルダ

¥¥[ファイル共有パス]¥Share¥

配下に、個別に異なる権限を付与したい場合、個別権限付与申請によって権限付与が可能。

申請の事前に

¥¥[ファイル共有パス]¥Share¥

直下に個別権限を付与したいフォルダを作り、そのフォルダ名 (share の直下のみ、2 階層以上下のフォルダは指定不可) を下記フォーマットに記載し、統合開発クラウドヘルプセンタ、または OI ヘルプデスク宛てに申請を行う。

フォルダが事前に存在していない場合、申請は受理されない。

(下記フォーマットの赤字部分を変更して申請すること)

=====個別権限付与申請フォーマットここから=====

下記の通りファイル中継インスタンスの共有フォルダに個別権限の付与を希望します。

■対象のファイル中継インスタンス

harsft0000

■独自権限グループを付与したいディレクトリ(作成済みフォルダに限る)

¥¥[ファイル共有パス]¥Share¥xxxxxx

■独自権限のグループ

pgrXXXXX

■付与希望日(必ずしも希望通りにならない可能性があります)

YYYY/MM/DD

=====個別権限付与申請フォーマットここまで=====

3.8. [ファイル中継] 大容量ストレージ一時利用申請

標準のファイル中継のストレージでは不足する場合（VM イメージ等の大容量ファイルをやり取りする場合等）、1TB のボリュームを別途 2 週間付与することができる。

下記フォーマットに記載し、統合開発クラウドヘルプセンタ、または OI ヘルプデスク宛てに申請を行う。

（下記フォーマットの赤字部分を変更して申請すること）

=====大容量ストレージ一時利用申請フォーマットここから=====

下記の通り、ファイル中継インスタンスへの大容量ストレージ一時付与を希望します。

■対象のファイル中継インスタンス

harsft0000

■貸与開始希望日（必ずしも希望通りにならない可能性があります）

YYYY/MM/DD

=====大容量ストレージ一時利用申請フォーマットここまで=====

通常、申請から2～3営業日を目安に作業が可能。

一時付与された大容量ストレージは、ファイル中継の利用者権限にて、

¥¥[ファイル共有パス]¥buffer

でアクセス可能となる。

本パスは、付与から 14 日後に自動的に削除される。

ファイル中継機能の仕様上、個別権限が付与されたファイルは

メンテナンスのファイル削除処理が実行されるタイミングで削除される。

※他 VM との負荷分散のため、メンテナンスのタイミングで必ずしもファイル削除処理が実行されるとは限らない。