情 報 種 別：G外秘
会　社　名：株式会社NTTデータ
情報所有者：ITマネジメント室

NTT DATA
Trusted Global Innovator

【別紙】統合開発セキュリティ基盤サービス サービス仕様書（グループ会社版）1.0版

株式会社NTTデータ
ITマネジメント室

改訂履歴

版数	発行日	改訂履歴
1.0	2021年6月4日	初版

Index

用語の定義(1/2)

項番	用語	略称	意味
1	NTTデータ	NTTデータ	株式会社NTTデータ。
2	グループ会社	G会社	NTTデータの国内グループ会社。
3	統合開発セキュリティ基盤	UDS	NTTデータが提供する開発環境向けの拠点間閉域ネットワーク接続、及びインターネット接続環境を提供するサービスの総称。
4	サービス利用プロジェクト	プロジェクト/PJ	統合開発セキュリティ基盤サービスを利用するNTTデータ、グループ会社、業務委託先の協力会社及び開発環境へアクセスするお客様の総称。
5	プロジェクト管理者	PJ管理者	サービス利用プロジェクトにおいて、プロジェクトを管理する立場にある利用会社の管理職以上の社員。プロジェクト毎に1名。
6	プロジェクト副管理者	PJ副管理者	サービス利用プロジェクトにおいて、PJ管理者の役割を代行する立場にある利用会社の社員、協働者。プロジェクト毎に1～20名。
7	プロジェクト利用者	利用者	統合開発セキュリティ基盤サービスを利用するNTTデータグループ会社の社員、協働者、お客様、業務委託先社員及び業務委託先協働者。
8	ワークフローシステム	—	統合開発セキュリティ基盤サービスを利用するプロジェクトを管理するためのシステム。
9	プロジェクトグループ	PJグループ	統合開発セキュリティ基盤サービスを利用する単位。PJ管理者、PJ副管理者、利用者が所属するグループ。 ワークフローシステムで作成する。
10	プロジェクトメンバ	メンバ	PJグループに登録されている利用者のこと。ワークフローシステムでは利用者をメンバと呼称する。
11	統合開発クラウド	—	NTTデータが提供する統合開発クラウドは開発プロジェクトに提供するNTTデータ及びグループ会社向け統合開発環境である。 ※提供元組織は異なります。
12	オフショアネットワーク	オフショアNW	NTTデータが提供するオフショア拠点を結ぶネットワーク回線。オフショア拠点での開発で利用する。 ※提供元組織は異なります。

用語の定義(2/2)

項番	用語	略称	意味
13	UDS提供元	—	サービス提供元（NTTデータ）
14	イントラネット	—	主にグループ会社の社内情報システムやインターネット上のサービスの利用を目的として、端末等（仮想環境含む）が接続されたネットワーク。
15	サービス利用プロジェクト管理内ネットワーク	管理内NW	以下要件を満たすことができるネットワークをいう。 • サービス利用プロジェクト業務にのみ利用する閉じられたネットワークであり、且つ、他のネットワーク（インターネット、他社社内ネットワーク、他委託先会社ネットワーク等）へ接続できないこと。 • 当該ネットワークにおいて、別紙「統合開発セキュリティ基盤利用時における開発LANに求めるセキュリティ要件について（グループ会社版）」のセキュリティ対策が実施されていること。 • 当該ネットワークにおいて、セキュリティ面や運用面等の問題が発生した場合、当該ネットワーク管理者に是正を指示できること。
16	サービス利用プロジェクト管理外ネットワーク	管理外NW	UDS提供元が求める要件を満たすことができないネットワーク。次のネットワークをいう。 サービス利用プロジェクトのネットワークのうち、サービス利用プロジェクト管理内ネットワークの要件を満たすことができないネットワーク。
17	開発LAN	—	サービス利用プロジェクト管理内ネットワークのうち、統合開発セキュリティ基盤サービス（UDS）にアクセス可能な部分をいう。主にシステム開発を目的とする。 開発LANは、グループ会社のイントラネット及びインターネット等のサービス利用プロジェクト管理外ネットワークとは接続できません。 開発LANから接続可能なネットワークは、別紙「統合開発セキュリティ基盤利用時における開発LANに求めるセキュリティ要件について（グループ会社版）」をご確認ください。
18	業務委託先LAN	—	グループ会社から業務委託を受けた会社社内にあり、かつ、サービス利用プロジェクト管理内ネットワークの要件を満たすネットワークをいう。
19	オフショアネットワーク接続LAN	—	サービス利用プロジェクト管理内ネットワークのうち、オフショアネットワークに接続している海外の業務委託先LANをいう。

1. はじめに

開発環境におけるセキュリティリスクへの脅威

これまでの経緯と現状

NTTデータグループでは2014年に、セキュリティ対策基準(※)を制定し、仕組みとして『グループ共用セキュリティ基盤』を整備。しかしながら、本ルールと仕組みの対象は、**オフィスネットワークのみ**であり、システム開発に利用する**開発環境は対象外**であった。

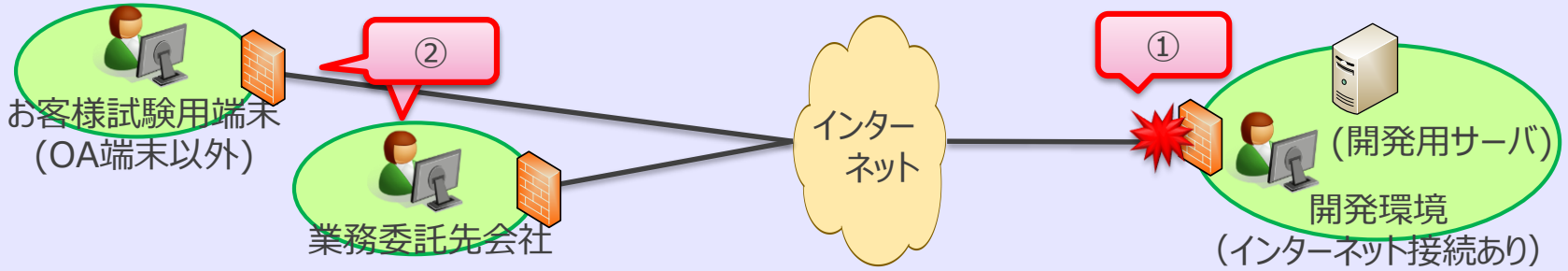
一方、セキュリティリスクは、開発環境にも存在し、お客様の情報を扱う(お客様への納品物含む)といった点において、開発環境も同様であり、(特にインターネット接続ありの開発環境は)**標的型攻撃対策ガイドライン**に沿って、各組織にて対策されている。

※ **標的型攻撃対策ガイド**、初動対応ガイドの順守

<リスク例>

① **不正侵入検知等のセキュリティ対策が不足。**
→ ネットワークに対する不正侵入や標的型攻撃による情報漏えいのリスク

② **(クラウド上のシステムを含む)アカウントの棚卸などが適切に実施されていない。**
→ プロジェクトを離れた元利用者(お客様やベンダ含む)が容易に情報入手可能



1.1. 背景と目的(2/3)

統合開発クラウドへの接続による開発環境の提供

これまで各個別のプロジェクトで構築していた開発環境を、一元的にプライベート/パブリッククラウド上で提供することにより、**デリバリ向上(短納期)とコスト削減を目的**とした、**「統合開発クラウド」**の提供。統合開発セキュリティ基盤では、統合開発クラウドへのアクセスラインを提供。

営業フェーズ：事前検証 → 受注判定 企画会議 → 開発フェーズ：ED / ID / M/UT / IT / ST → 終了判定 → 維持フェーズ：維持

ワンストップ

統合開発クラウド

1 開発環境サービス

システム基盤構築

- デリバリサービス
  - スタック
  - パッケージソフトウェア
- プライベートクラウドサービス
  - OpenStack
  - VM (New)
- パブリッククラウドサービス
  - AWS
  - Azure 等
- (New) 開発端末管理サービス

2 開発支援サービス

アプリケーション開発／プロジェクト管理

- 開発ツール
  - Jenkins
  - DaaS
- 管理ツール
  - PM/ITSM ワークベンチ
- プロフェッショナルサービス
  - 第三者チェック
  - まかせいのう
  - 他

3 開発ネットワークサービス

powered by 統合開発セキュリティ基盤サービス

1.1. 背景と目的(3/3)

目的

1 NTTデータグループ開発環境の**セキュリティレベルの向上**

- 「標的型攻撃対策ガイドライン」に沿ったセキュリティ機能を提供。
- 開発LANに対しては、これまでインターネットと接続しなければ利用できなかった各種サービス(例：セキュリティパッチの取得等)をセキュアに提供。

2 **コスト低減**と**デリバリ向上**

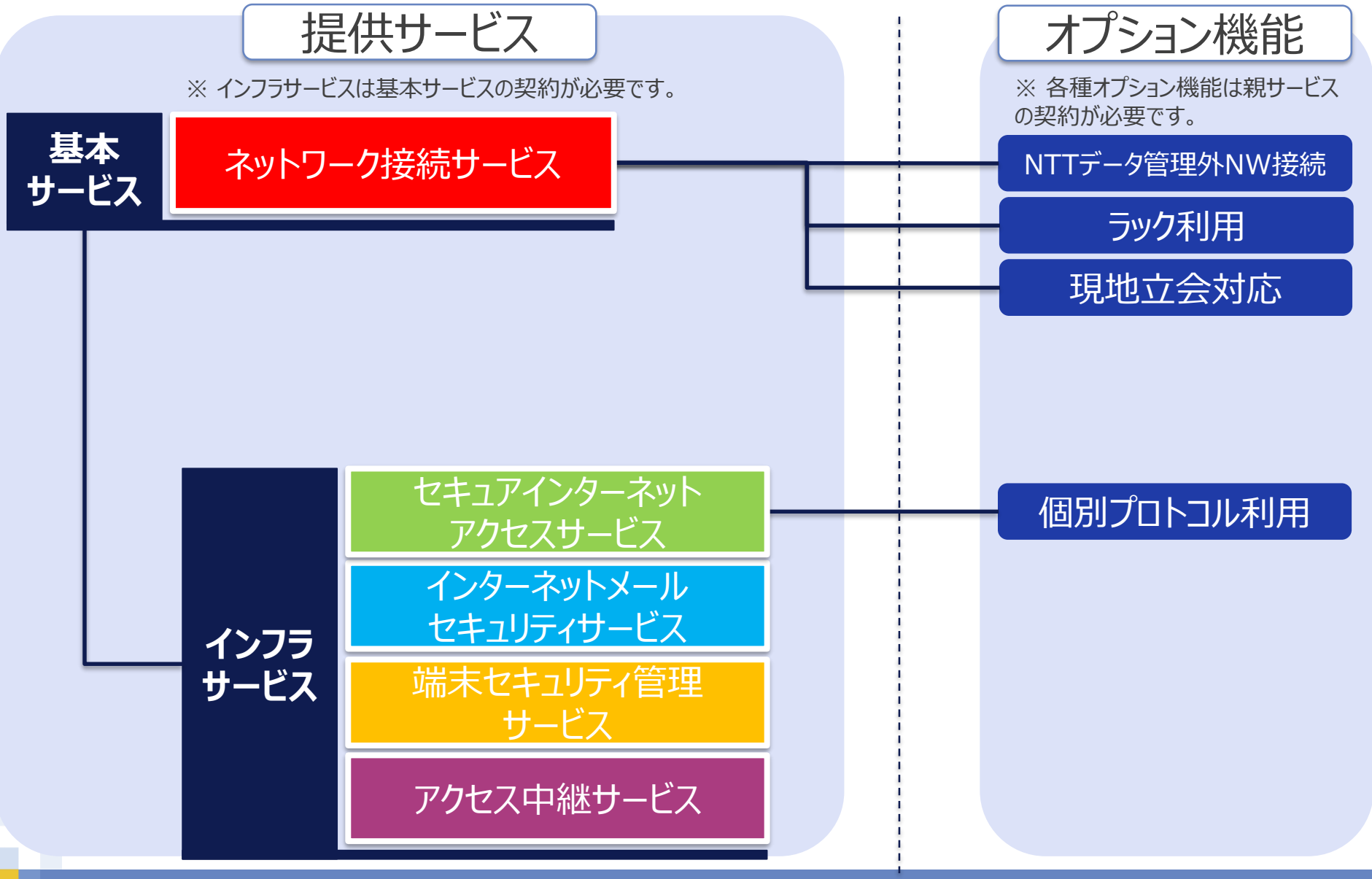
- 共通した仕組みを提供することで、個別のプロジェクトで構築運用していたコストを低減。
- さらに、サービスとして提供することで、比較的短期の開発であっても長期にわたってインフラを維持する必要がなく、プロジェクトの固定費が低減。
- サービス提供により、個別に環境を準備していた際のリードタイムを削減し迅速に開発インフラを整備することが可能。

3 **クラウド開発環境の活用**

- 統合開発クラウドへのアクセス経路を提供。
  ※ 統合開発クラウドのご説明は本資料では割愛

2. 統合開発セキュリティ基盤とは

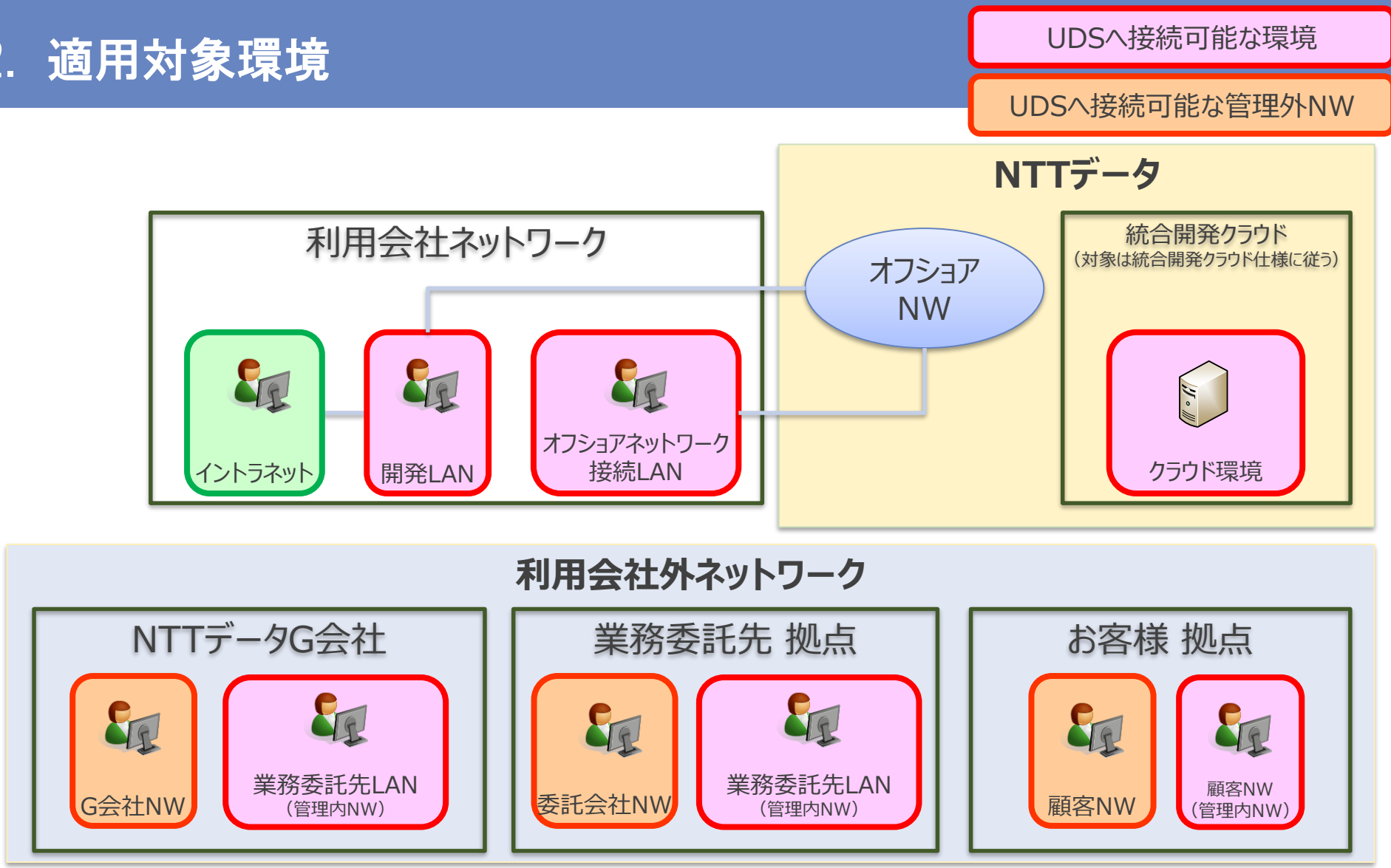
2.1. 提供サービスの立付(1/2)



2.1. 提供サービスの立付(2/2)

	サービス	提供機能	オプション
基本サービス	**ネットワーク接続サービス**	• **開発環境をさまざまな手段で接続し相互アクセスする中継ハブ** • 管理外NWへアクセス • 統合開発クラウドへのアクセス経路	• NTTデータ管理外NW接続 • ラック利用 • 現地立会対応
インフラサービス	**セキュアインターネットアクセスサービス**	• **インターネットWebアクセス（http/https）** • 出口/入口対策（FW、IDS、URLフィルタ、ユーザ認証） • インターネットとのDNS連携	• 個別プロトコル利用
	インターネットメールセキュリティサービス	• **インターネット側とのメール中継（メールボックスサーバはPJ側で準備）** • メールセキュリティチェック（メールフィルタ、ウィルススキャン、SPAMフィルタ）	
	端末セキュリティ管理サービス	• **セキュリティパッチ適用状況のモニタリング** • 無許可の無線LAN接続制限 • 小型可搬媒体利用制限 • **セキュリティパッチ・ウィルスパターンファイルのダウンロード**	
	アクセス中継サービス	• 利用会社イントラネットから開発LANに安全に入るための中継装置としての機能を提供する。	

2.2. 適用対象環境



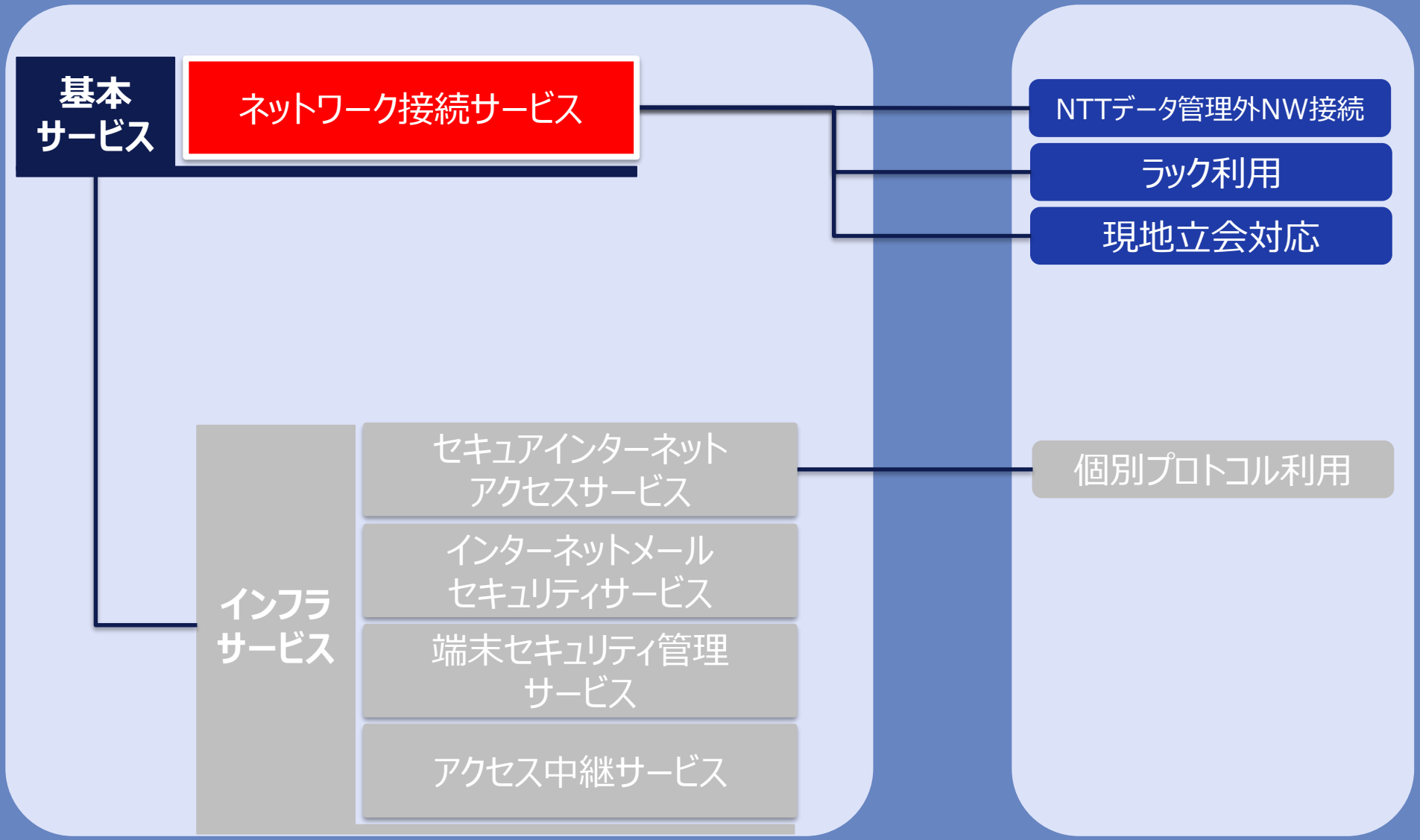
※ 開発環境の接続方法は、「3. ネットワーク接続サービス」に後述します。
※ 本サービス仕様書で記載しているクラウド環境は、統合開発クラウド提供するサービスをさします。

2.3. UDSサービスの全体像

統合開発セキュリティ基盤は、各種開発環境（開発LAN等）を対象に、セキュアインフラサービスの提供と、統合開発クラウドへのアクセスを実現します。

NTT DATA

3. ネットワーク接続サービス

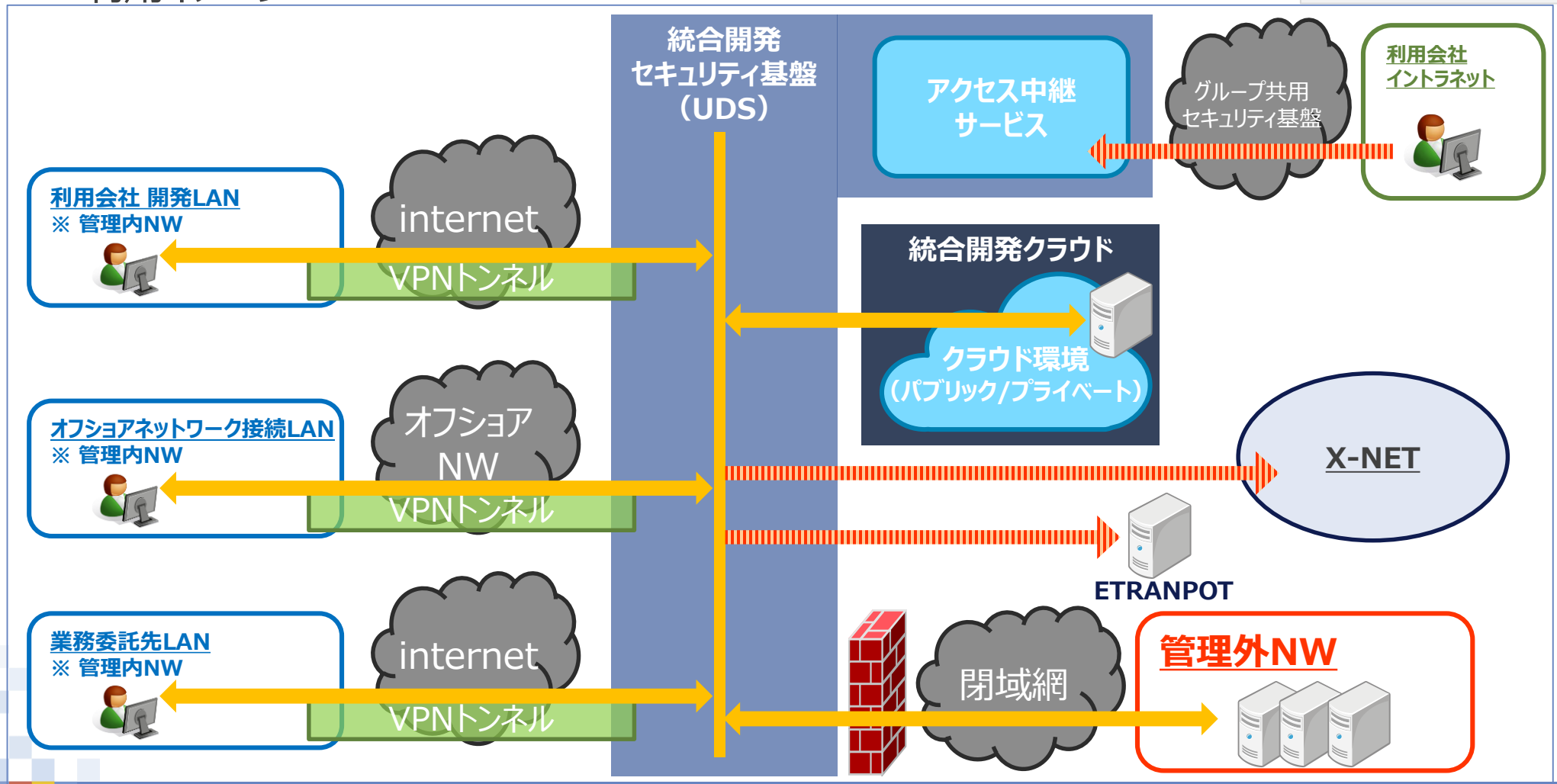


NTT DATA

3.1. ネットワーク接続サービス概要

NW

- サービス概要
  統合開発セキュリティ基盤を介して開発環境を相互にアクセス可能とするサービスを提供します。
- 利用イメージ



NTT DATA

3.2. ネットワーク接続機能（基本機能）

NW

ネットワーク接続サービスは、以下の接続形態を提供します。

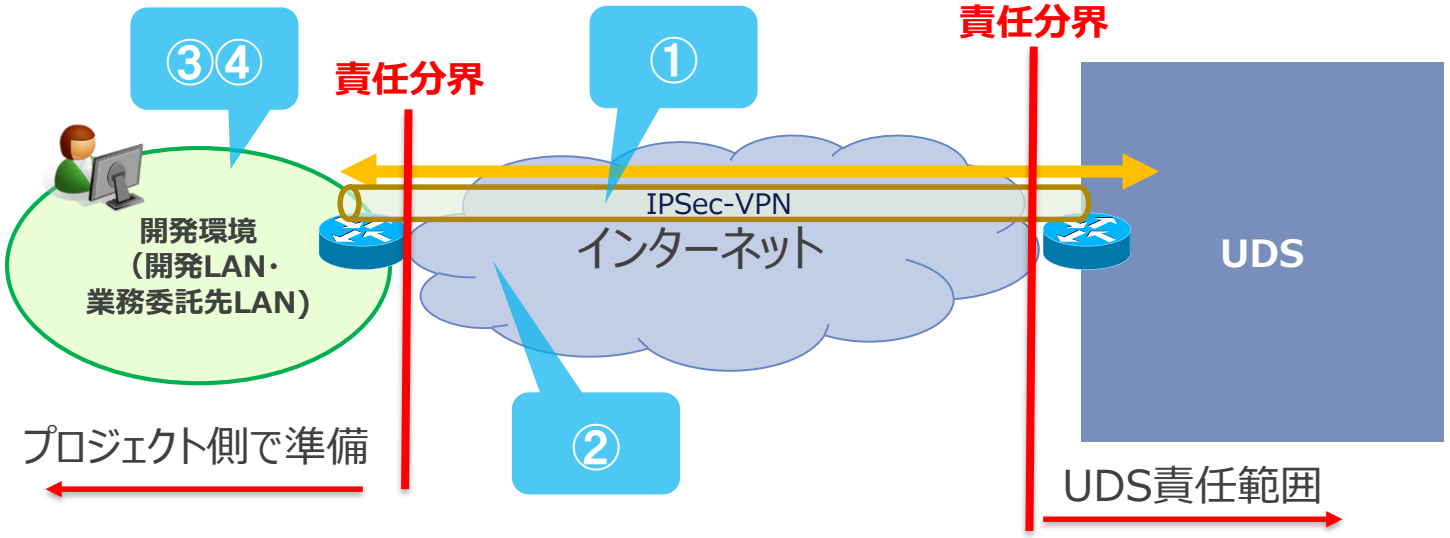
サービス区分	接続形態	主な接続対象の環境	概説
通常サービス	インターネット経由接続	開発LAN 業務委託先LAN	インターネット経由で、開発環境をUDSへ接続する。
	オフショアNW経由接続	オフショアネットワーク接続LAN	オフショアNWを利用し、開発環境をUDSへ接続する。
	専用線・閉域網経由接続	業務委託先LAN	専用線・閉域網経由で、開発環境をUDSへ接続する。
	プライベートクラウド接続	統合開発クラウドが提供する、プライベートクラウド	UDS接続している開発環境から統合開発クラウドが提供するプライベートクラウドを利用する。 グループ共用セキュリティ基盤上からアクセス中継サービスを経由して、統合開発クラウドが提供するプライベートクラウドを利用する。
	パブリッククラウド接続	統合開発クラウドが提供する、パブリッククラウド	UDS接続している開発環境から統合開発クラウドが提供するパブリッククラウドを利用する。 グループ共用セキュリティ基盤上からアクセス中継サービスを経由して、統合開発クラウドが提供するパブリッククラウドを利用する。
	XNET接続	-	UDSを経由してXNETを利用する。
オプション機能	専用線・閉域網経由接続	管理外NW（顧客NW、インターネットが接続したLAN など）	専用線・閉域網経由で、管理外NWをUDSへ接続する。

- 各利用会社への環境提供数は**10個**とします。
- 本サービスを用いた負荷試験（大量のトラフィックを流す等）は**禁止**です。
  特定のPJにて、大量の通信が発生していることを検知した場合、ネットワークを遮断する措置を取る場合があります。
- 各接続形態の詳細は次ページ以降をご参照ください。

3.2.1. 接続形態(1/5)

NW

インターネット経由接続



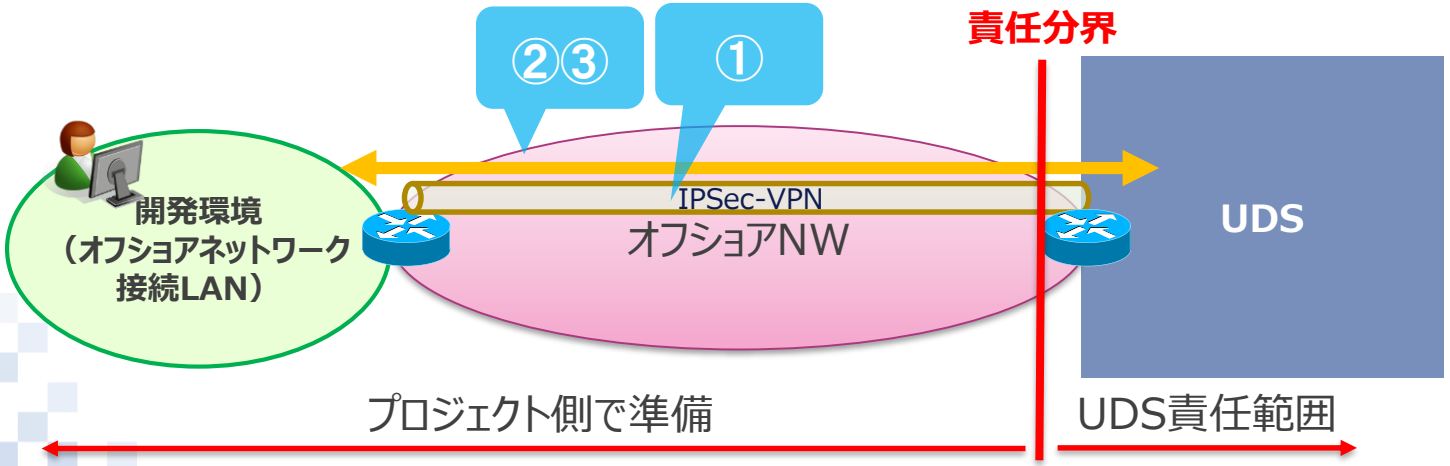
① VPNで接続となります。

② 静的グローバルアドレスを提供するインターネット回線が必要です。（VPNトンネル用）

③ 管理内NWの開発環境であれば利用会社拠点以外（他G会社、顧客、開発委託会社）でも接続可能です。

④ UDSへ接続する開発環境には、管理外NW（インターネット、顧客NW等）が接続していないことが条件です。

オフショアNW経由接続



① VPNで接続となります。

② オフショアNWと接続している拠点が対象です。

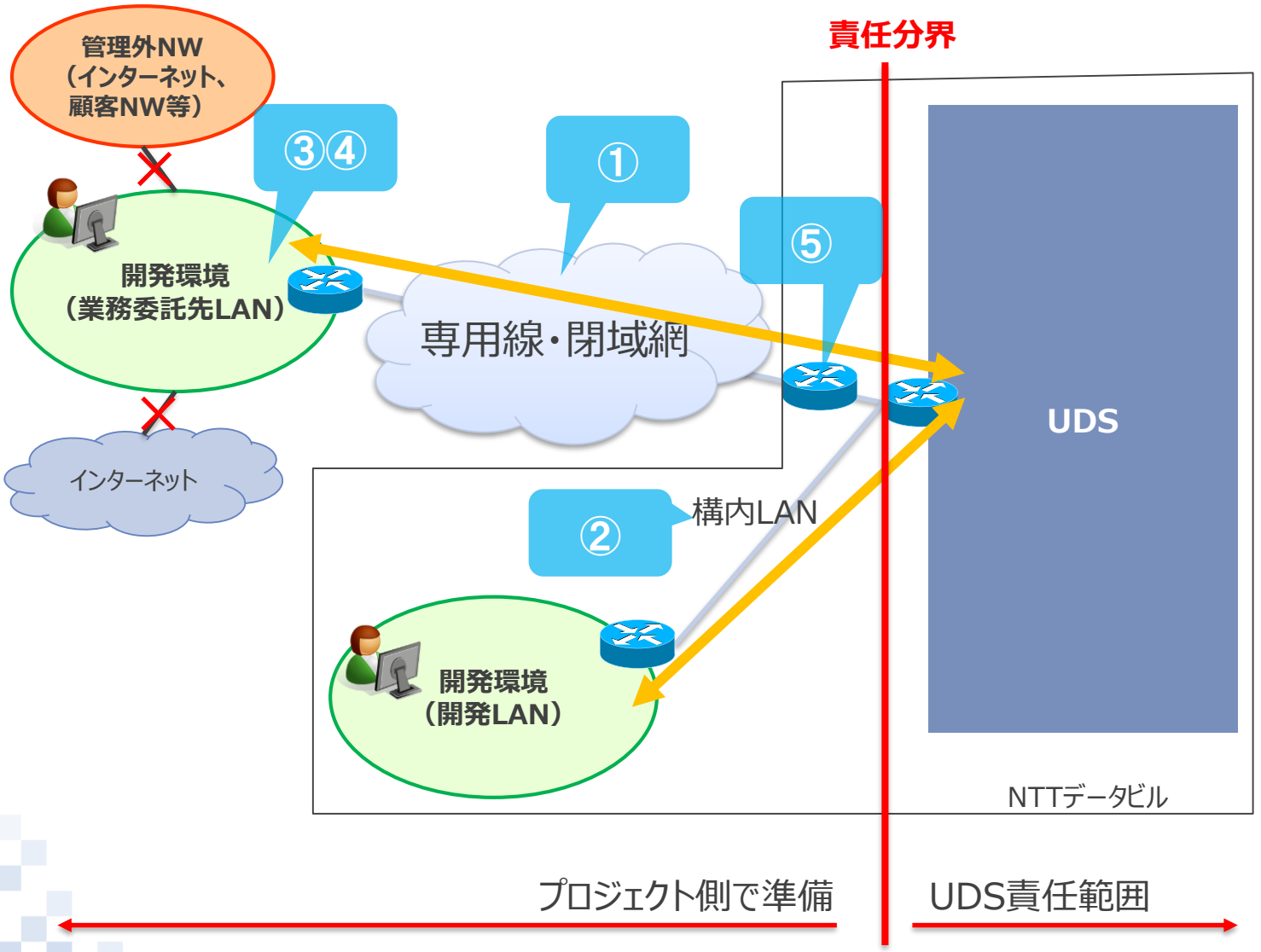
③ オフショアNW利用料は別途必要です。

NTT DATA

3.2.1. 接続形態(2/5)

NW

専用線・閉域網経由接続



① 業務委託先LANを専用線・閉域網経由で接続できます。（回線敷設先はUDSセンタ設備を設置しているNTTデータビル）

② NTTデータビルの開発LANを接続する場合は、統合セキュリティ基盤まで専用線を敷設することで接続できます。

③ 管理内NWの開発環境であれば利用会社拠点以外（他のG会社、顧客、開発委託会社）でも接続可能です。

④ UDSへ接続する開発環境には、管理外NW（インターネット、顧客NW等）が接続していないことが条件です。

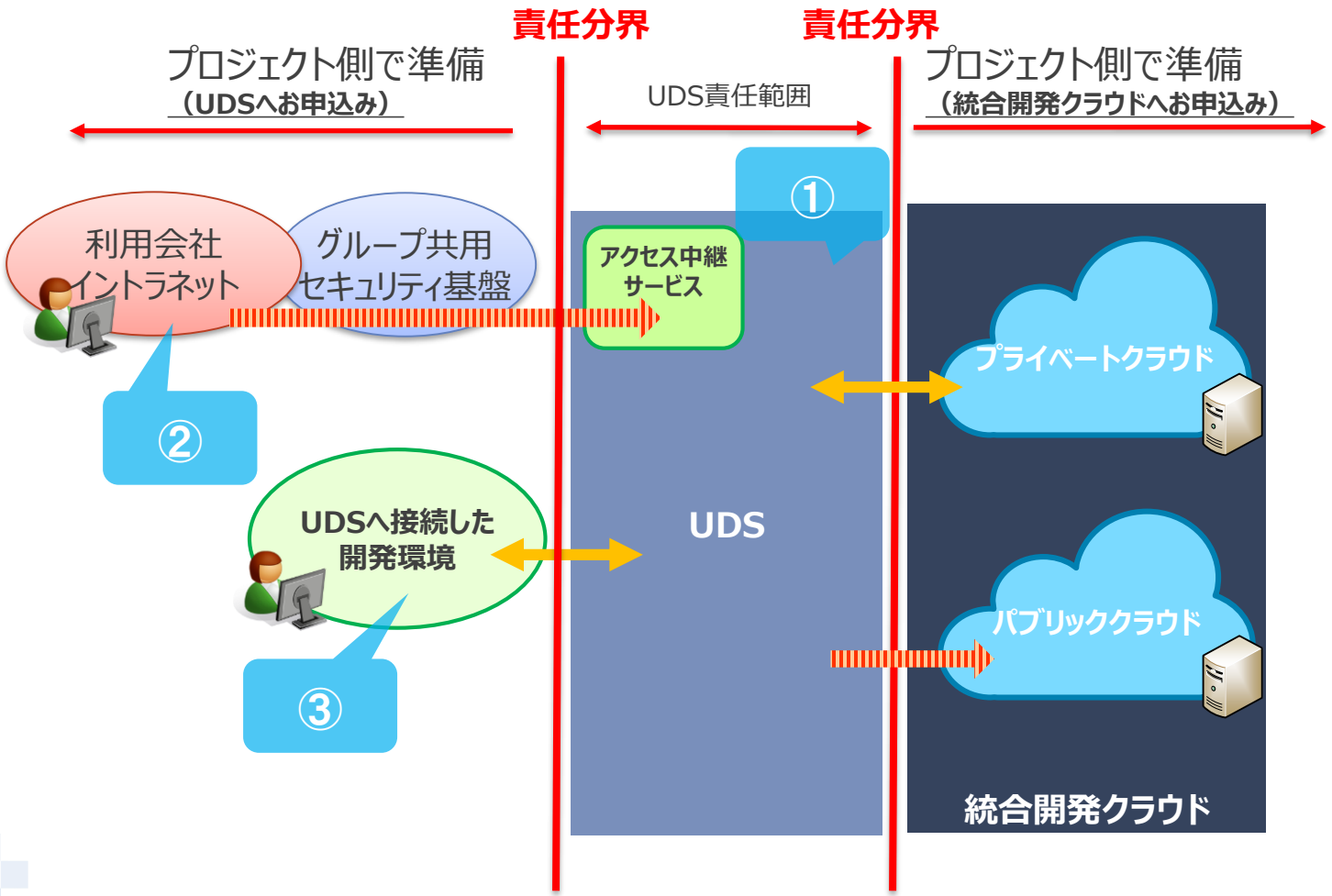
⑤ プロジェクト側でNW機器の設置場所を用意できない場合は、UDS提供元管理ラックを有償でご利用いただくことが可能です。**【オプション機能】**

NTT DATA

3.2.1. 接続形態(3/5)

NW

統合開発クラウド　プライベートクラウド・パブリッククラウド接続



① 開発LANから統合開発クラウドが提供するプライベートクラウド・パブリッククラウドへ接続する場合、UDSのお申込みが必要です。

② 利用会社イントラネットからアクセス中継サービスを経由しプライベートクラウド・パブリッククラウドへアクセス可能です。

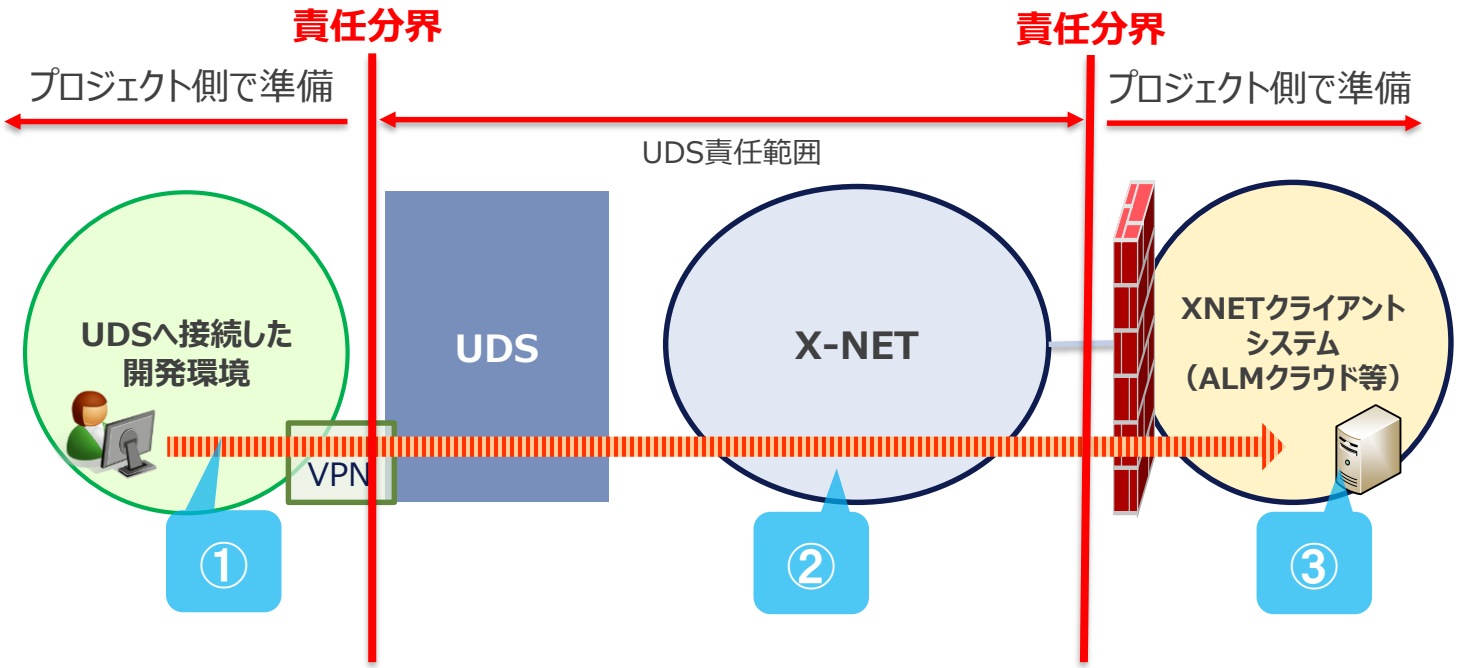
③ UDSへ接続した開発環境よりプライベートクラウド・パブリッククラウドへアクセス可能です。

NTT DATA

3.2.1. 接続形態(4/5)

NW

X-NET接続



① UDSを経由してX-NETへ接続することが可能です。

② ダッシュボードのUDS申請にてX-NET申請が集約されておりますので、X-NET接続申請書の提出は不要です。

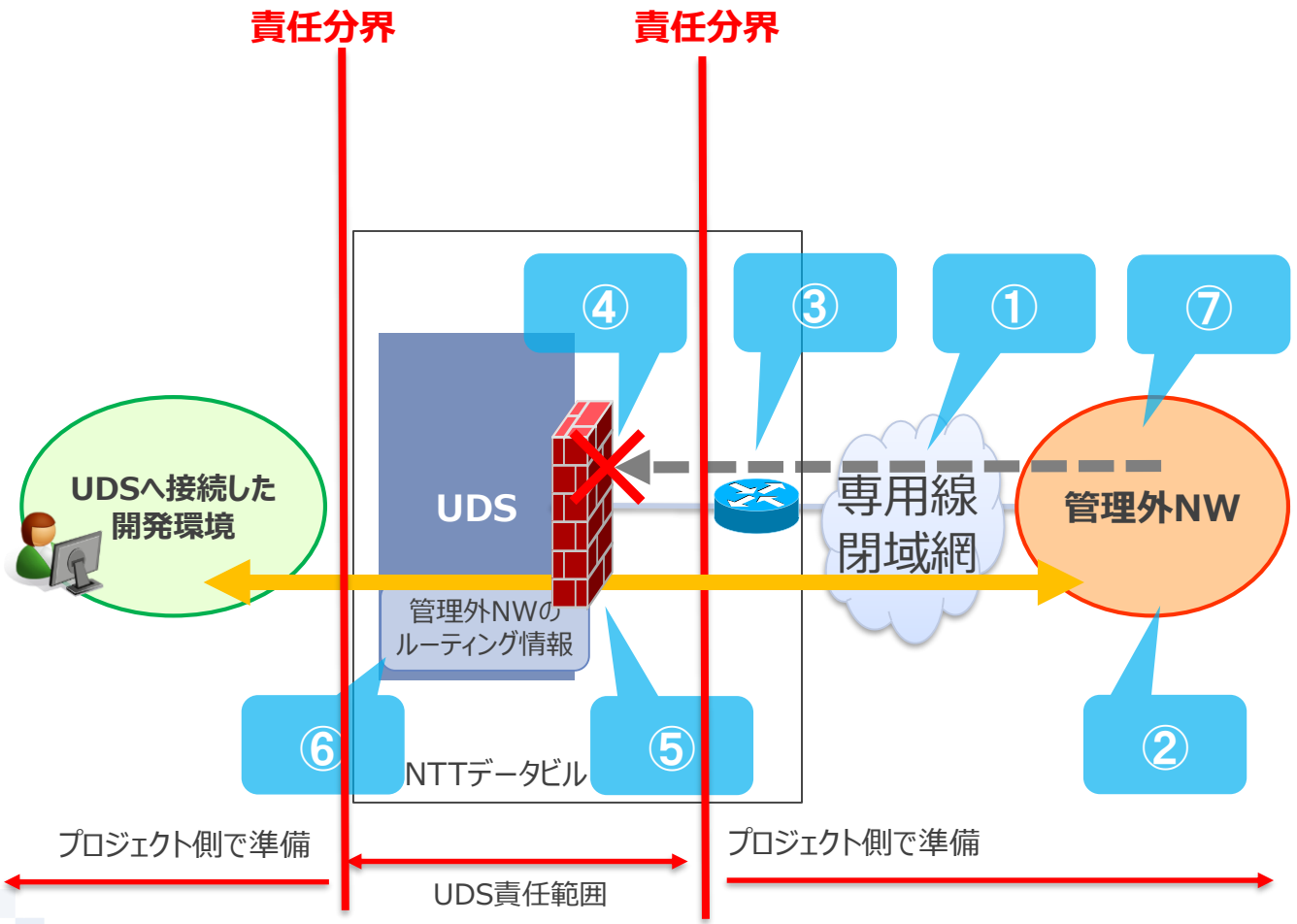
③ X-NETクライアントシステム（ALMクラウド等）の利用についてはPJ側で個別にお申込みが必要です。

NTT DATA

3.2.1. 接続形態(5/5)

NW

NTTデータ管理外NW接続【オプション機能】



① 管理外NWを専用線・閉域網経由で接続することができます。（回線敷設先はUDSセンタ設備を設置しているNTTデータビル）

② 管理外NWからUDSの各インフラサービス及び、X-NET、ETRANPOTはご利用できません。

③ プロジェクト側でNW機器の設置場所を用意できない場合は、UDS提供元管理ラックを有償でご利用いただくことが可能です。**【オプション機能】**

④ 管理外NWからの通信制御はUDS側のFWで行います。（FWは冗長/シングルを選択可。）通信制御の条件は下記の通りです。

- a. プロトコルと送信元/送信先アドレスのand条件で通信許可設定を行います。アドレス、プロトコルともにanyは認められません。
- b. 管理外NWを送信元とする通信で、送信元IPアドレスがグローバルIPアドレスとなる通信は通信許可設定を行うことができません。
- c. 送信元IPアドレスにアクセス中継サービスは指定できません。
- d. UDS基盤用のIPアドレス（下表）を含む通信許可設定はできません。

⑤ 通信許可設定を行った通信内の不正なアクセスはIPS(侵入防止システム)で検知・遮断します。

⑥ 管理外NWに存在するセグメントと通信できるよう、UDSへルーティング情報を登録。

⑦ UDS基盤用のIPアドレス（下表）が管理外NWに存在する場合、あるいは、PJの開発環境側のIPアドレスと管理外NWに同一セグメントが存在する場合、IPアドレスの変更もしくはPJ側機器でNAT設定を実施する必要があります。

163.135.0.0/16	10.15.240.0/21
202.217.39.64/26	10.44.0.0/16
202.217.50.0/23	10.100.0.0./16
202.217.52.0/24	10.120.0.0/16
203.182.132.0/22	10.177.192.0/18
	10.228.0.0/17

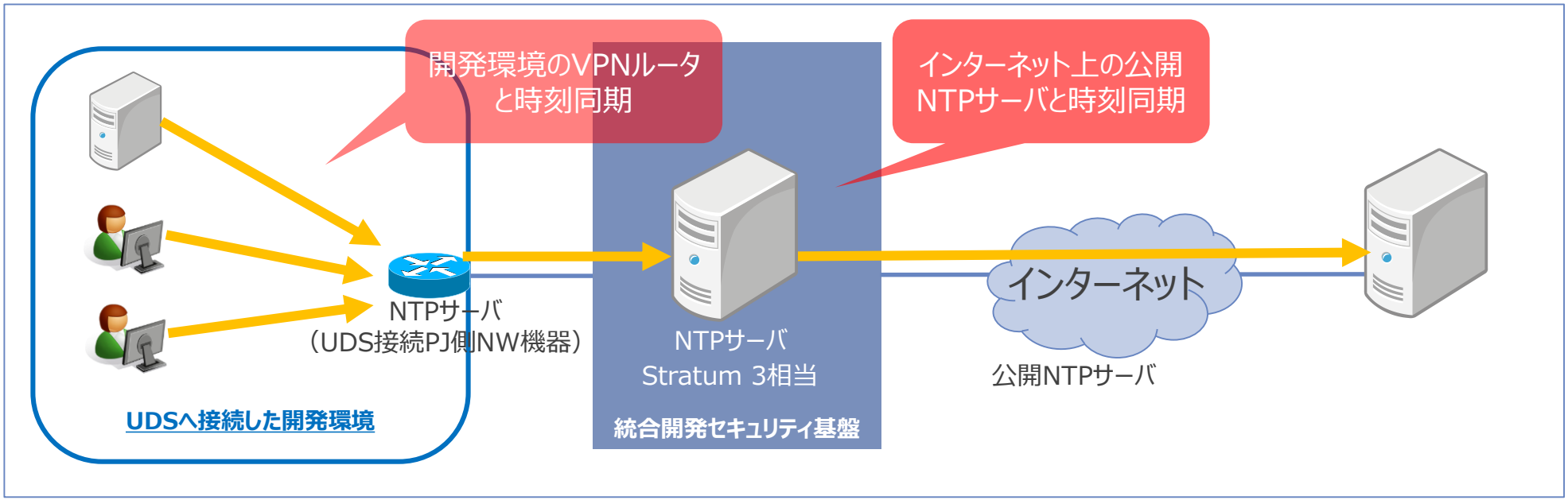
NTT DATA

3.3. NTP機能

NW

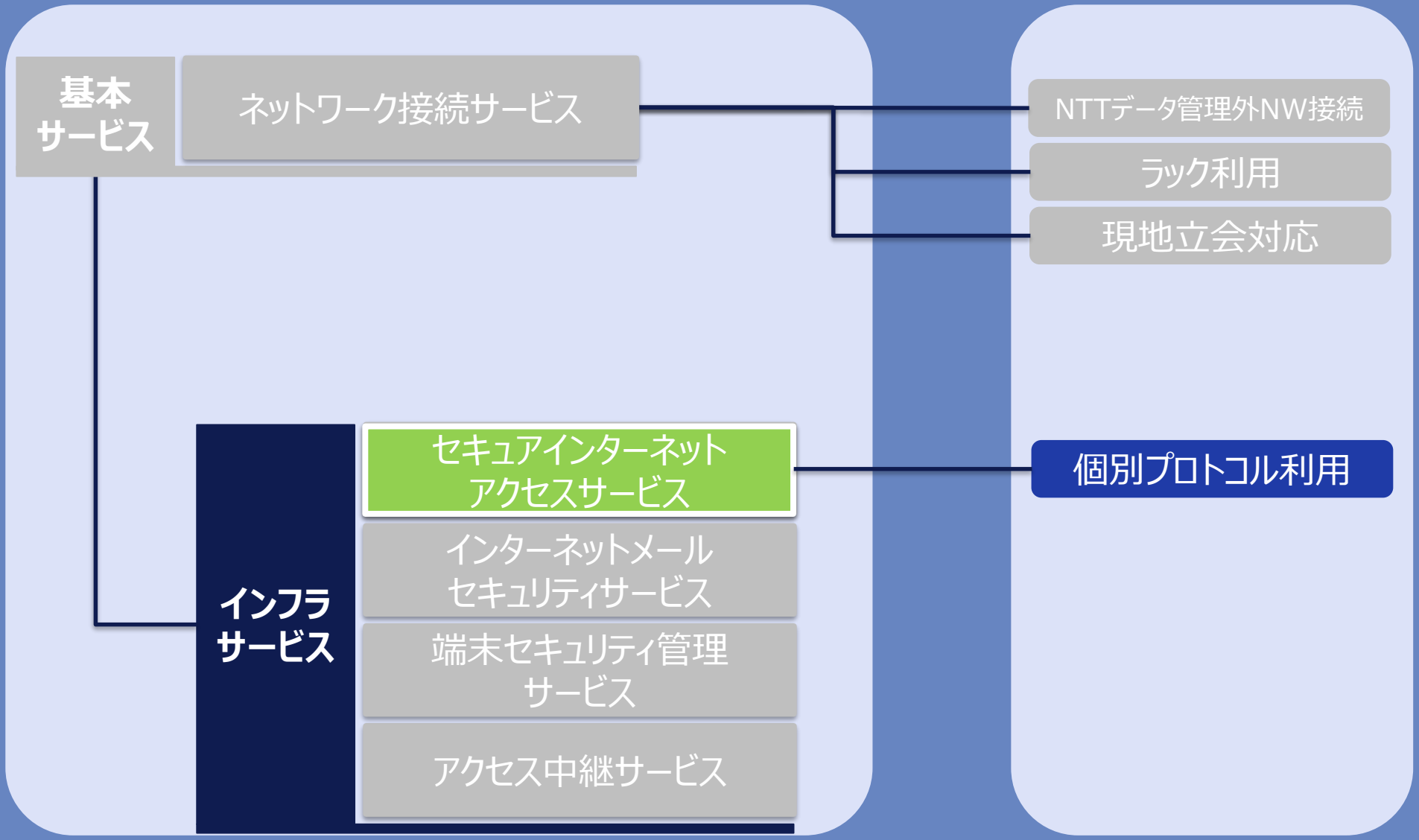
- サービス概要
  - ・統合開発セキュリティ基盤へ接続した開発環境を対象に時刻同期サービスを提供します。
  - ・参照先は　開発環境内の機器 → UDS接続用PJ側NW機器 → UDS NTPサーバ となります。

- 利用イメージ



NTT DATA

4. セキュアインターネットアクセスサービス



4.1. セキュアインターネットアクセスサービス概要

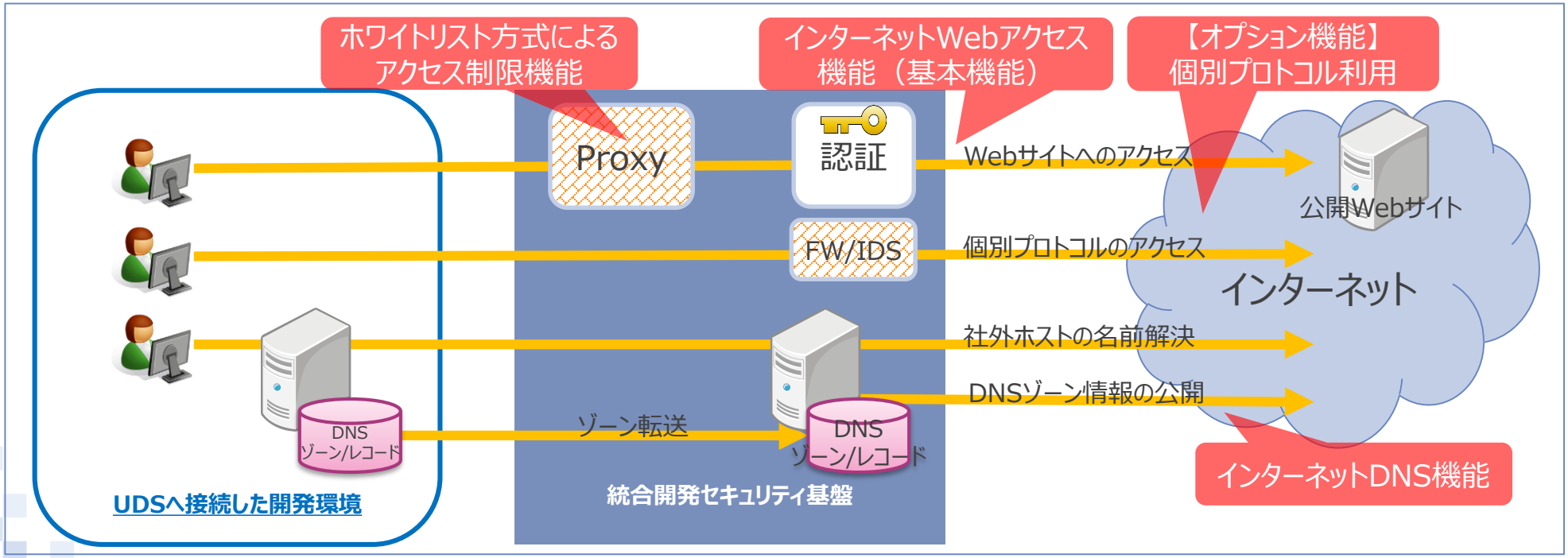
IWA

- サービス概要

  統合開発セキュリティ基盤へ接続した開発環境を対象に以下の機能を提供します。

  - インターネット上のWebサイトへの接続機能
  - ホワイトリスト方式によるアクセス制限機能
  - インターネットとのDNS連携機能
  - オプション機能として、個別プロトコルでインターネットへの接続機能

- 利用イメージ



NTT DATA

4.2. インターネットWebアクセス機能（基本機能）

IWA

No	分類	サービス仕様
1	前提条件	• プロジェクトごとにサービスの利用要否を検討し、サービスを利用する場合は申請を行ってください。 • 利用者をワークフローシステムへ登録してください。 • 認証不要サイト(共通)(※)については、本サービスのお申込みがない場合でもアクセス可能です。 ※Windows, Adobe, Java, Symantec, TrendMicro の Update 用サイト
2	基本動作	• プロキシサーバを経由し、インターネット上のWebサイトにアクセスします。 • アクセス可能なプロトコルはhttp,httpsのみアクセス可能です。 ※ http,https以外のプロトコルを利用する場合は、**個別プロトコル利用サービス**が必要です。（本表No.6参照） • アクセス時にはWebプロキシ認証を適用します。認証後はコンテンツフィルタ機能の定義に従いWebサイトのみアクセスが可能です。 ※ コンテンツフィルタ機能については「4.3. コンテンツフィルタ機能」を参照
3	認証	• ユーザ認証では、ワークフローシステムへ登録したアカウントを入力します。
4	アカウントポリシー	• ユーザ認証が連続で失敗すると、アカウントがロックアウトされます。
5	その他	• 推奨Webブラウザは、各OSの最新バージョンのInternet Explorerです。 • 利用プロジェクトの設置したProxy経由でUDS Proxyを利用する多段Proxy構成はサポート対象外となります。 また、UDS Proxyを経由してインターネット上に利用プロジェクトの設置したProxyを利用する多段Proxy構成は禁止です。 • インターネット向けのすべての通信はIDS(侵入検知システム)で監視します。(※) • 不正な通信が検知された場合、利用プロジェクトへ問合せを行う場合があります。 ※　Web閲覧だけでなく、全ての通信が監視対象となります。 • 本サービスを用いた負荷試験は禁止です。
6	**【オプション機能】** 個別プロトコル利用サービス	• http,https以外のプロトコルでインターネット上のホストと通信する場合は、本オプション機能をお申込みください。 • アクセスの際、ID/PWの認証要求はありません。 • 通信元、通信先のIPアドレスを指定する必要があります。※通信元、通信先IPアドレスにアクセス中継サービスは指定できません。 • 通信元IPアドレスはグローバルIPへNAPTし、アクセスします。（10ホスト単位で1グローバルIPにNAPT） • すべての通信はIDSの監視対象となります。 • サービス利用料については、「9.1. サービス利用料」をご参照ください。

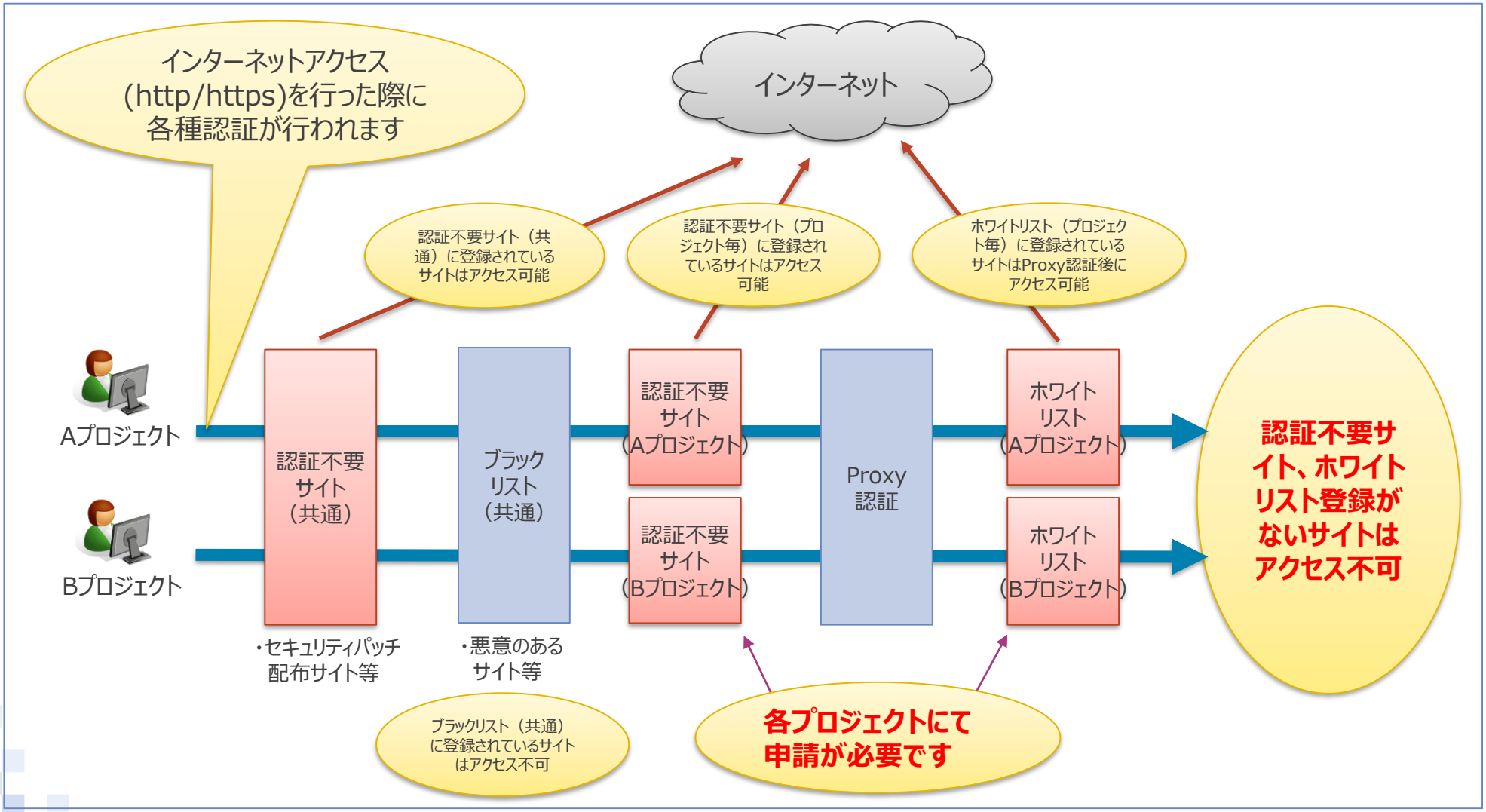
4.3. コンテンツフィルタ機能(1/2)

IWA

No	分類	サービス仕様
1	前提条件	• コンテンツフィルタ機能は、プロジェクト毎に適用されます。 • ホワイトリスト申請をしない場合は共通の認証不要サイト(共通)(※1)のみにアクセスが可能です。 ※1 Windows, Adobe, Java, Symantec, TrendMicro の Update 用サイト • NTTデータ 情報セキュリティ推進室が指定するブラックリスト(※2)に該当するサイトへのアクセスはできません。 ※2 ブラックリストの内容は公開されていません。 • **統合開発セキュリティ基盤では調査目的で検索サイト等を利用する用途は想定していません。**検索サイト等を利用する場合は利用会社イントラネットからの利用をご検討ください。
2	基本動作	• **プロジェクトごとに、開発業務に必要なWebサイトのみにアクセス可能とします。(ホワイトリスト方式)** • Webコンテンツのダウンロード時にマルウェアスキャンを行います。マルウェアが検出された場合、当該コンテンツおよびファイルは削除され、利用者にマルウェア検知のメッセージが表示されます。（ただしhttpsの場合は暗号化されているためマルウェアスキャンがされません。）
3	ホワイトリスト	• 業務上アクセスが必要なWebサイトは、利用プロジェクトの申請に基づき、ホワイトリストを設定します。 • ホワイトリスト登録可否の審査基準は、**プロジェクト管理者の承認**です。登録申請を行うWebサイトについては**プロジェクト側で必要性を確認の上**申請してください。 • ホワイトリストは、プロジェクト単位での登録となります。特定ユーザ、特定セグメント等の適用条件を設定することはできません。
4	認証不要	• Proxyからの認証要求に応答できない通信は認証不要サイトに登録します。 • 業務上アクセスが必要なWebサイトの申請、登録単位、登録審査についてはホワイトリストと同様です。
5	制限事項	• 情報漏洩防止およびマルウェア感染防止の観点から、本サービスによるVPN接続の利用は禁止です。

NTT DATA

- フィルター条件



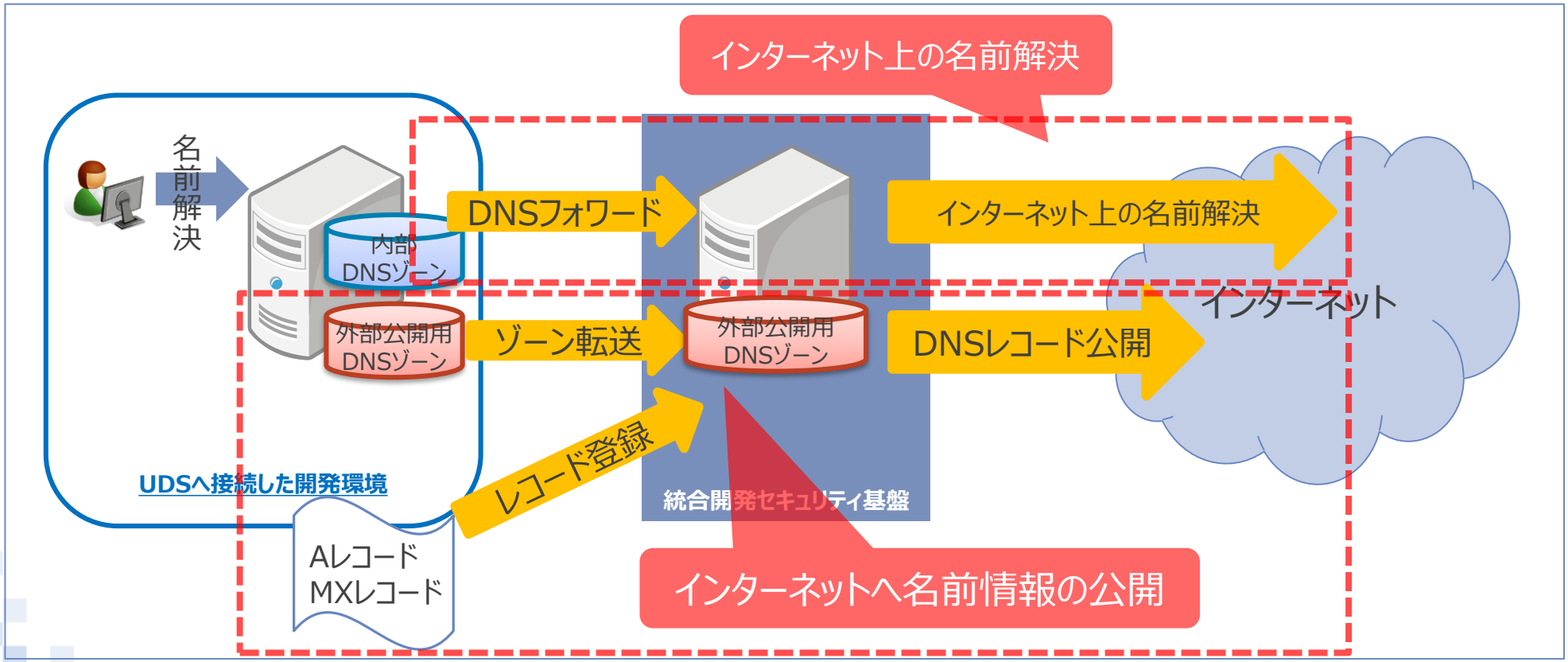
4.4. インターネットDNS機能(1/2)

IWA

- サービス概要
  - ✓ インターネット上の名前解決
  - ✓ インターネットへ名前情報の公開

※ **PJ開発LANの内部向け名前解決機能は提供しません**ので、必要に応じてPJ側でDNSサーバを準備してください。

- 利用イメージ



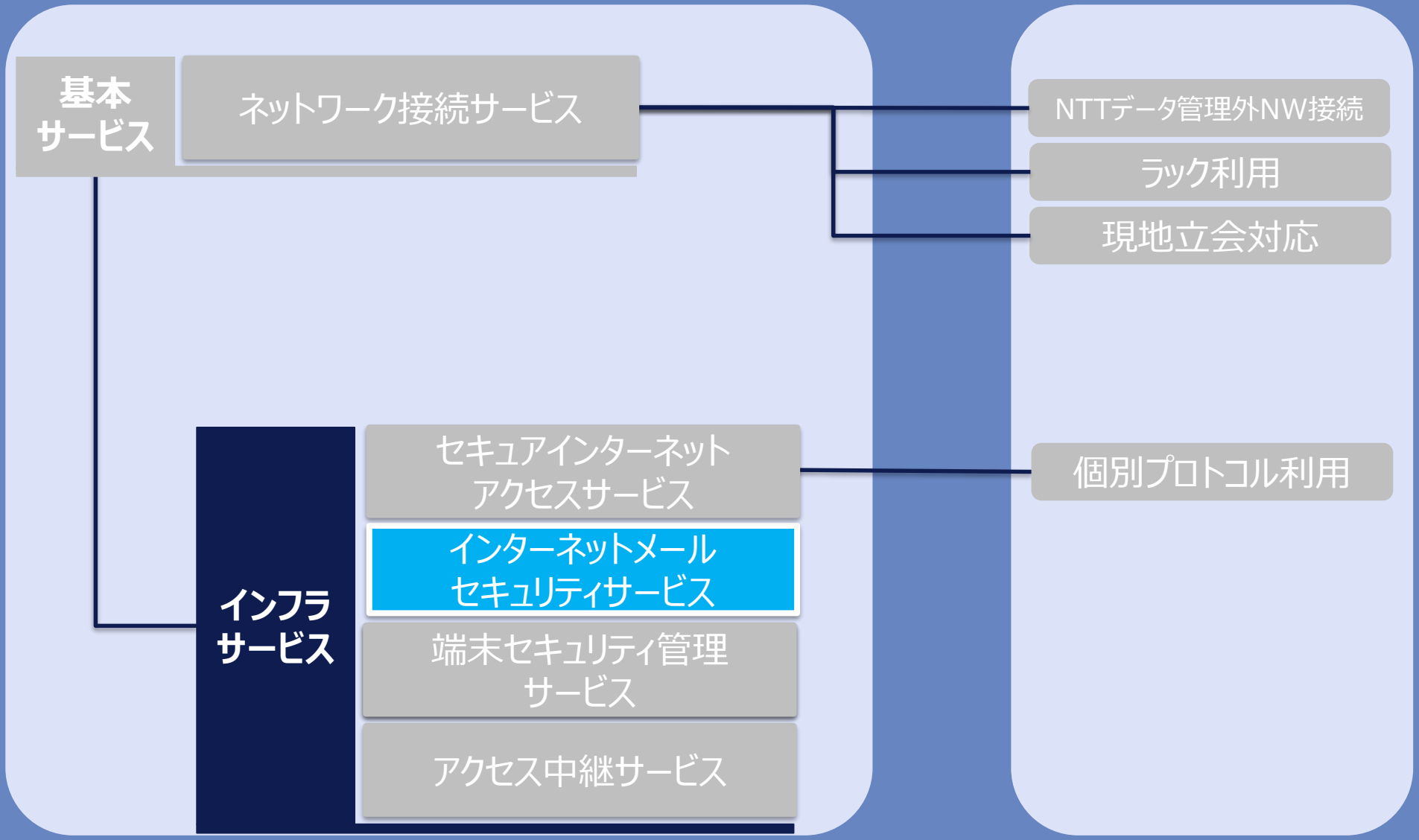
NTT DATA

4.4. インターネットDNS機能(2/2)

IWA

No	用途	サービス仕様
1	インターネット上のホストの名前解決	インターネットアクセスの際の名前解決を行います。
2		各プロジェクトで開発LAN上に構築したDNSサーバから、名前解決のフォワード先として利用できます。
3		開発LANのDNSクライアントは、名前解決に利用するDNSサーバとして、極力開発LANのDNSサーバを指定してください。
4	インターネットへ公開するホストの名前解決	ホスト数（Aレコード数）が10以下の場合は、直接ホスト登録を受け付けます。
5		各プロジェクトで開発LAN上に構築したDNSサーバから、本DNSサーバにゾーン転送を受けます。
6		コンテンツサーバとして登録可能なドメインは、利用会社が契約して保持しているドメインに限ります。
7		IPv6には対応しておりません。

5. インターネットメールセキュリティサービス

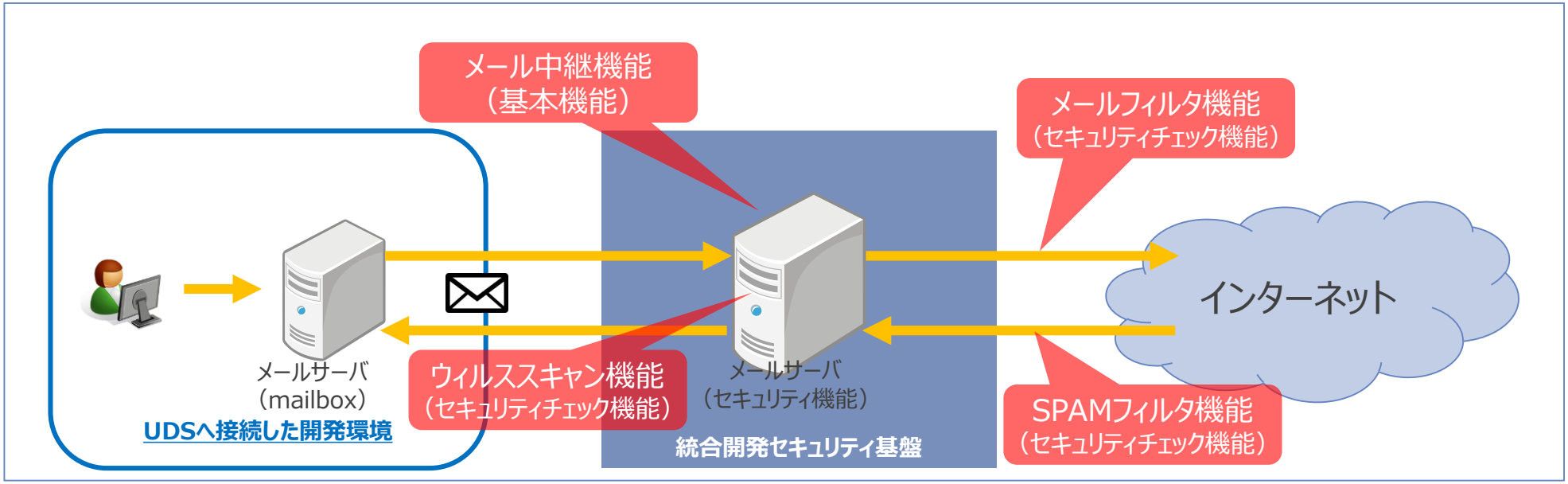


5.1. インターネットメールセキュリティサービス概要

Mail

- サービス概要
  - インターネット側とのメール中継機能
  - 各種メールセキュリティチェック機能（メールフィルタ、ウィルススキャン、SPAMフィルタ）

- 利用イメージ



NTT DATA

5.2. インターネットメールセキュリティ機能(基本機能)(1/2)

Mail

No	機能	概説
1	前提条件	メールサーバ（メールボックス）は統合開発セキュリティ基盤上では提供致しません。必ずPJ側で準備する必要があります。
2	利用可能ドメイン	インターネット側とメール中継する場合、利用会社ドメインの一部サブドメイン（※）、または、PJ独自のドメインの利用が可能です。 ※利用会社ドメインの一部サブドメインを利用する場合、予め以下についてご留意ください。 ・ グループ共用セキュリティ基盤サービスの提供するメールアーカイブ機能にて開発環境のメールデータが参照可能となります。 ・ 利用会社からグループ共用セキュリティ基盤へメール中継ログの提供を依頼した場合、開発環境のメール中継ログが含まれます。
		以下のドメインに当てはまり、かつWhois未登録のドメインのメールを利用する場合は、本サービスを利用することが出来ません。 ・ すでに本サービスで利用されているドメインと重複する場合 ・ すでにWhois登録されているドメインと重複する場合 ・ *.nttdata.co.jpに該当するドメイン ・ 利用会社以外のNTTデータグループ会社で利用されているドメインと重複する場合
3	DNS公開	• PJ独自に利用するメールドメインの中継情報は、DNSで公開する必要があります。 • メールドメインの中継情報の公開にインターネットプロバイダのDNS等を利用することが可能です。 • PJ側で中継情報をDNS公開する手段がない場合は、UDSのセキュアインターネットアクセスサービスをご契約頂き、インターネットDNS機能を利用し公開情報として登録（MXレコード）してください。 • メール送信専用で本サービスをご利用いただく場合はドメインの登録は必須ではございません。
4	メーリングリストの利用	外部メンバが含まれているメーリングリストの利用には対応しておりません。
5	ログ提供	メール中継ログを保管し、プロジェクト管理者の要求に応じて提供します。提供するログの範囲は、メールアドレスのドメイン単位とします。

5.2. インターネットメールセキュリティ機能(基本機能)(2/2)

Mail

No	機能	送受信区分	概説
6	メールフィルタ	送信	添付ファイル付きの送信をすべて遮断します。一度に100件を超える宛先への送信を遮断します。
7	ウィルススキャン	受信	中継するメールに対して、マルウェアチェックを実施します。また、指定された拡張子(5.3参照)を含む添付ファイル付きの受信を遮断します。
8	スパムフィルタ	受信	スパムメール情報に基づきスパムメールを判定し、スパムメールを隔離します。
			スパムと誤判定されたメールについて、利用プロジェクトの申請に基づき送信元ホワイトリストを適用し、受信可能とします。
9	その他	-	情報漏洩防止の観点から送信可能なメール容量は一通あたり4MB(※)とし、受信可能なメール容量は一通あたり10MB(※)となります。 ※4MB/10MBはエンコード後の容量のため、実質は3MB/7.5MB程度となります。
10			社外へのメール配信にて、対向のメール転送サービス（MTA）の不良等でメールが配信できない場合には再送処理を行います。 3時間を超えて対向のMTAへメールが配信できない場合には、配信不能通知が送信者へ通知されます。

5.3. 削除対象となる添付ファイルの拡張子一覧

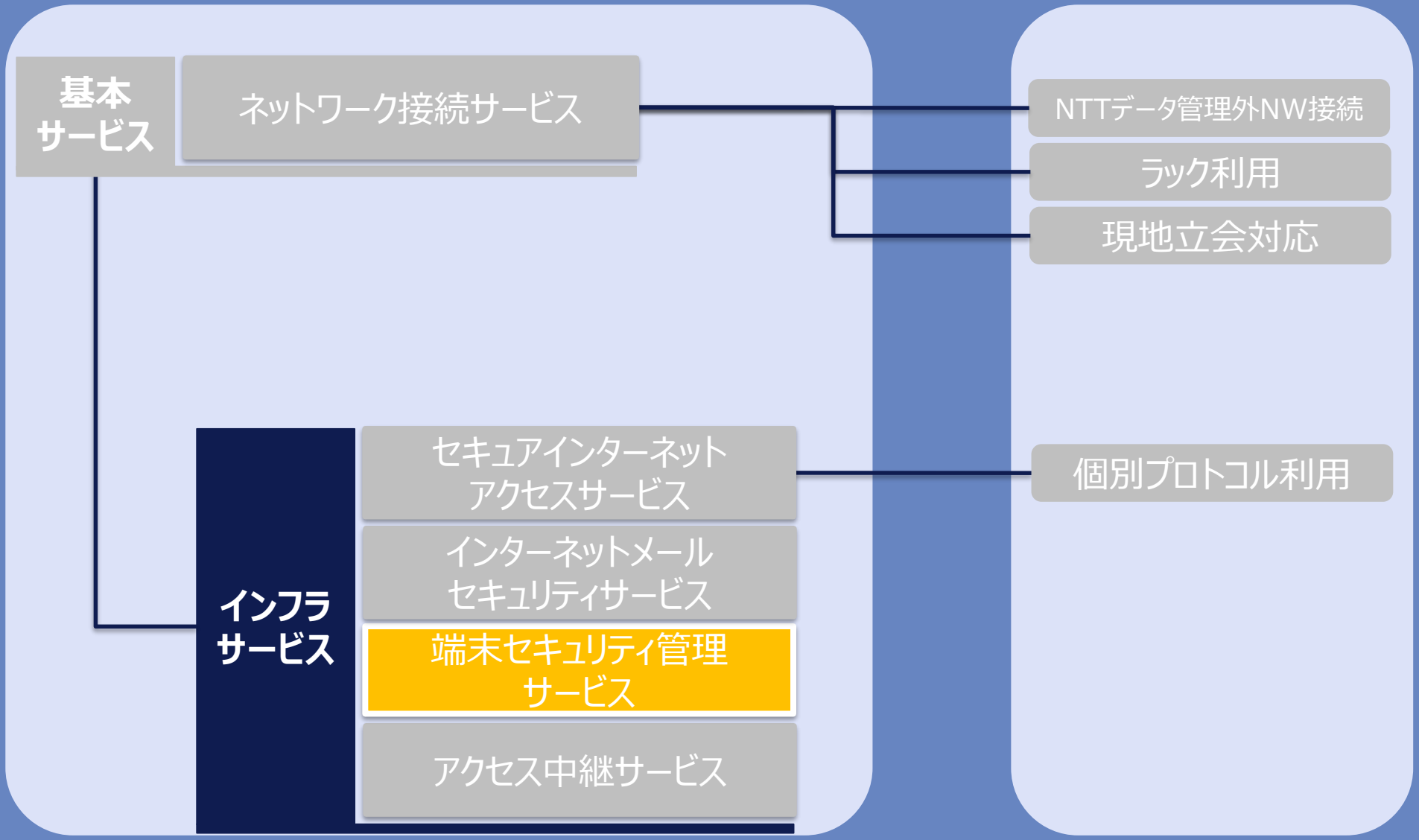
Mail

項番	拡張子	概要
1	.bat	MS-DOSバッチファイル
2	.cmd	Windows NTコマンドスクリプト
3	.com	MS-DOS アプリケーション
4	.cpl	コントロール パネル
5	.exe	アプリケーション
6	.fon	フォント ファイル
7	.hlp	ヘルプ ファイル
8	.hta	HTML Application
9	.ini	構成設定
10	.js	JScript スクリプト ファイル
11	.jse	JScript 符号化スクリプト ファイル
12	.lnk	ショートカット
13	.msi	Windows Installer Package
14	.msp	Windows Installer Patch
15	.pif	MS-DOS プログラムへのショートカット
16	.reg	レジストリファイル
17	.scf	Windows Explorer Command
18	.scr	スクリーン セーバー
19	.sct	Windows Script Component

項番	拡張子	概要
20	.url	インターネット ショートカット
21	.vb	VBScript ファイル
22	.vbe	VBScript 符号化スクリプト ファイル
23	.vbs	VBScript スクリプト ファイル
24	.wsc	Windows Script Component
25	.wsf	Windows スクリプト ファイル
26	.wsh	Windows スクリプト ホスト設定ファイル
27	.avi	ビデオ クリップ
28	.mp3	MP3 形式サウンド
29	.mpeg	MPEG ムービー
30	.mpg	MPEG ムービー
31	.ra	RealAudio
32	.ram	RealOne Player プレゼンテーション
33	.rm	RealMedia
34	.wmv	Windows Media オーディオ/ビデオ ファイル
35	.docm	Microsoft Office Word(マクロ有効文書)
36	.cab （※）	Cab形式で圧縮されたファイル
37	.svg （※）	ベクター形式の画像フォーマット

※インターネット→UDSへ接続した開発環境

6. 端末セキュリティ管理サービス



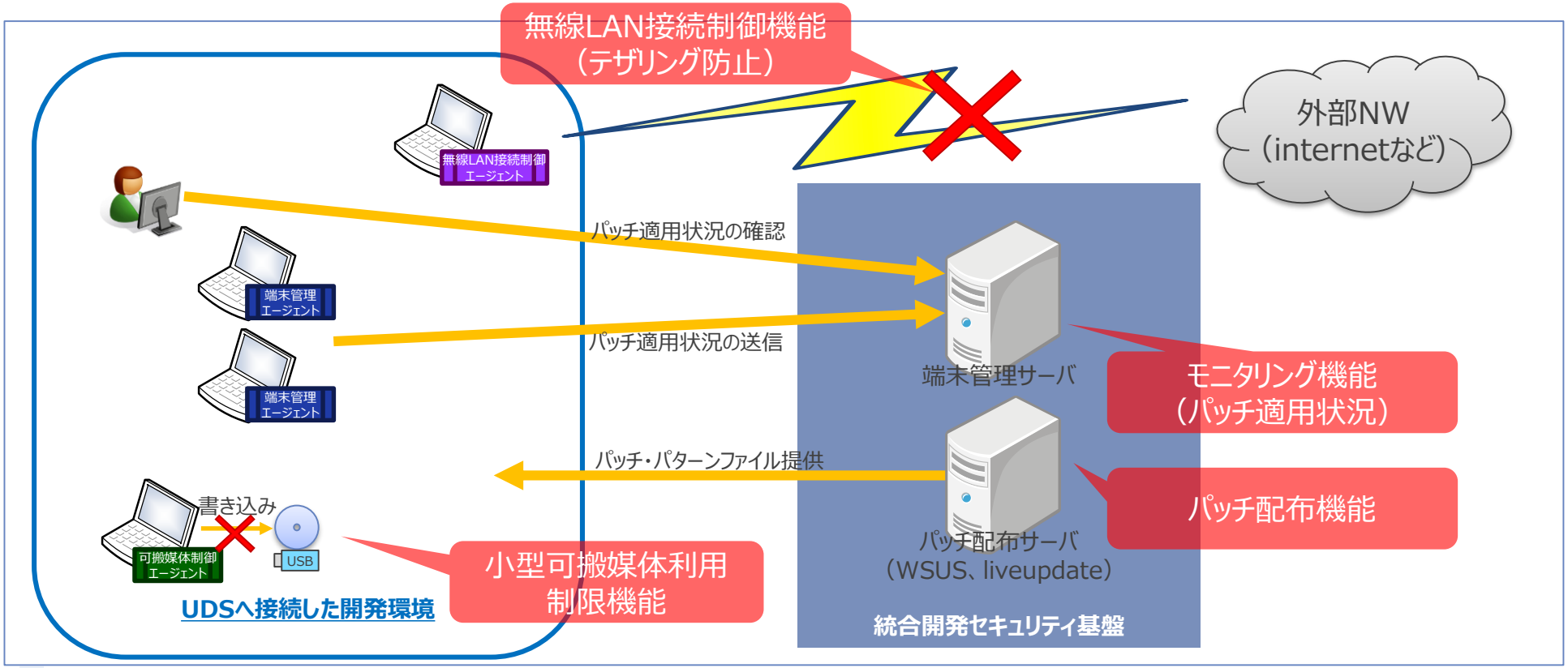
6.1. 端末セキュリティ管理サービス概要

SCS

- サービス概要

  開発LANの端末を対象に、モニタリング機能(パッチ適用状況の閲覧)及び、小型可搬媒体制御機能、テザリング防止機能を提供する。

- 利用イメージ



NTT DATA

6.2. 端末セキュリティ管理機能（基本機能）

SCS

No	機能名称	サービス仕様
1	モニタリング	Windows端末のセキュリティ対策状況をモニタリング可能な仕組みを提供します。
		モニタリング周期は、各プロジェクトにて設定できます。
		PJ管理者から登録したプロジェクト毎に対策状況が閲覧できるインターフェースを提供します。モニタリング可能な範囲は、プロジェクトグループ単位とします。
2	小型可搬媒体利用制限	Windows端末における小型可搬媒体（※）の利用を制限する機能を提供します。 （※）USBストレージクラスとして認識される媒体（例：USBメモリ、外付HDD、スマートフォン等）
		当該端末からの小型可搬媒体による情報持ち出しを制限します。
		同機能の解除およびエージェントアンインストールが可能な機能を提供します。
		各種ログがプロジェクト管理者にて閲覧可能な仕組みを提供します。閲覧可能なログの範囲は、プロジェクトグループ単位とします。
		端末利用ユーザと端末管理者間で申請ファイルとパスワードの授受を行うことで利用許可します。ファイル連携機能等は本サービスでは提供しませんので、利用プロジェクトでご用意ください。
3	テザリング防止	プロジェクトで利用している無線LANのテザリング利用を防止する機能を提供します。ただし、プロジェクトで開発LANを使用する場合は、プロジェクト毎に許可する無線LAN（※SSID）を指定する必要があります。 プロジェクト内のWindows　PCの、テザリングを含む無線LANを無効化する機能を提供します。 プロジェクトのネットワークで無線LANを提供している場合、例外SSIDに設定することで、接続が可能になります。 例外接続するプロジェクトの無線LANは端末管理システムに接続できる必要があります。
		同機能の解除およびエージェントアンインストールが可能な機能を提供します。
		各種ログがPJ管理者にて閲覧可能な仕組みを提供します。閲覧可能なログの範囲は、プロジェクトグループ単位とします。
		端末利用ユーザと端末管理者間で申請ファイルとパスワードの授受を行うことで利用許可します。ファイル連携機能等は本サービスでは提供しませんので、利用プロジェクトでご用意ください。
		システム故障時は、無線LAN接続が不可となる場合があります。この場合は、有線LANに切り替えてご利用ください。

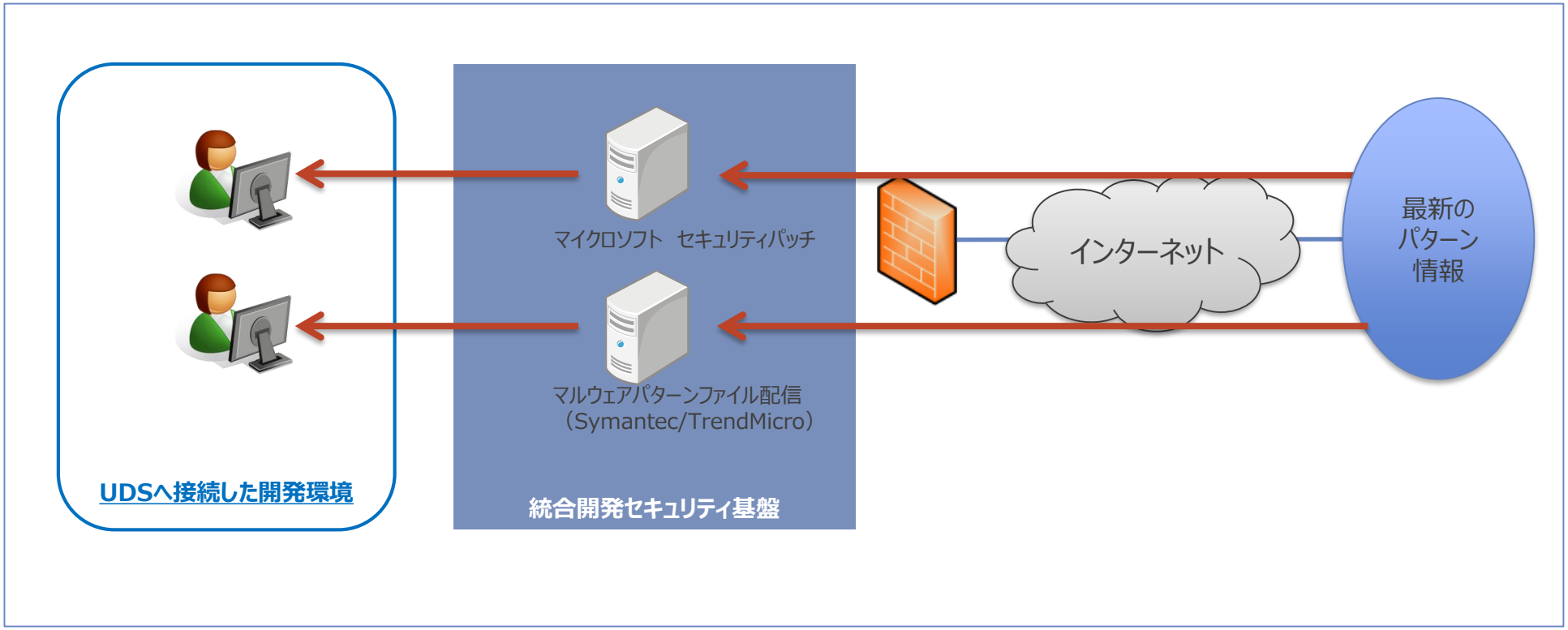
6.3. セキュリティパッチ提供機能(1/2)

SCS

- サービス概要

  開発LANなどの端末に対してセキュリティパッチ適用状況等を管理する仕組みを提供します。

- 利用イメージ



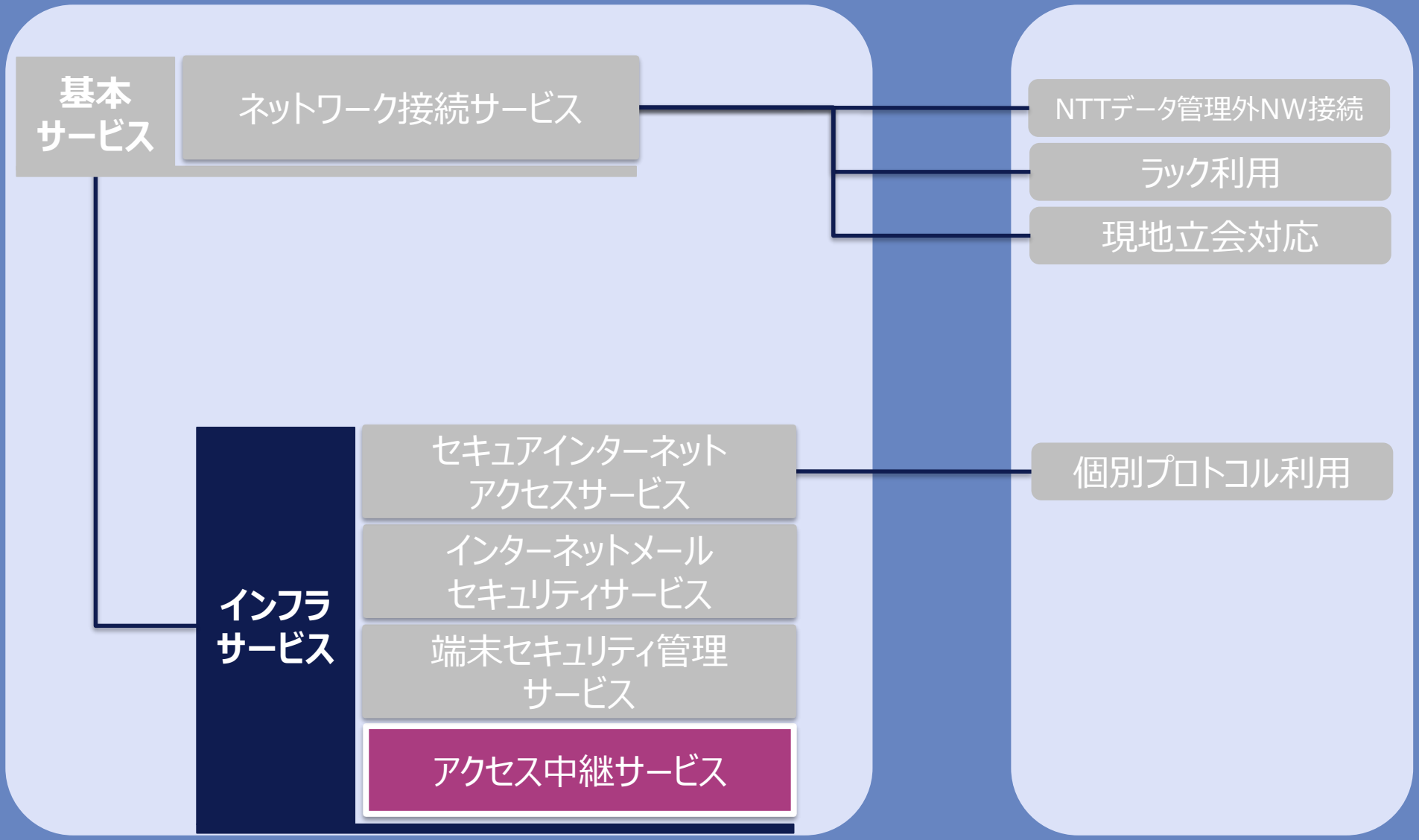
NTT DATA

6.3. セキュリティパッチ提供機能(2/2)

SCS

No	分類	サービス仕様
1	マイクロソフト製品	マイクロソフト社のセキュリティパッチ配信サービスを提供します。
2		対象OSは、サポート期間のOSを対象とします。
3		Office製品は、サポート期間の製品を対象とします。
4		端末からの取得を可能とするものであり、配信サービスからのPush型配信は行いません。
5		上記以外のソフトウェアやリポジトリへのアクセスは、インターネットアクセスにおけるホワイトリストにて対応します。 （別途セキュアインターネットアクセスサービスをご利用いただく必要があります）
6	マルウェア対策製品	マルウェア対策ソフトの最新定義ファイル配信サービスを提供します。
7		配信する対象のマルウェア対策ソフトは、Symantec製品およびTrendmicro製品とします。 最新の対応ソフトウェアはサポートサイトをご覧ください。
8		端末からの取得を可能とするものであり、配信サービスからのPush型配信は行いません。
9		上記以外の対策ソフトやリポジトリへのアクセスは、インターネットアクセスにおけるホワイトリストにて対応します。 （別途セキュアインターネットアクセスサービスをご利用いただく必要があります）
10		開発LANで利用されるマルウェア対策ソフトのソフトウェアライセンスについては、本サービスで提供するものではありません。プロジェクト側での購入が必要となります。

7. アクセス中継サービス



7.1. アクセス中継サービス概要

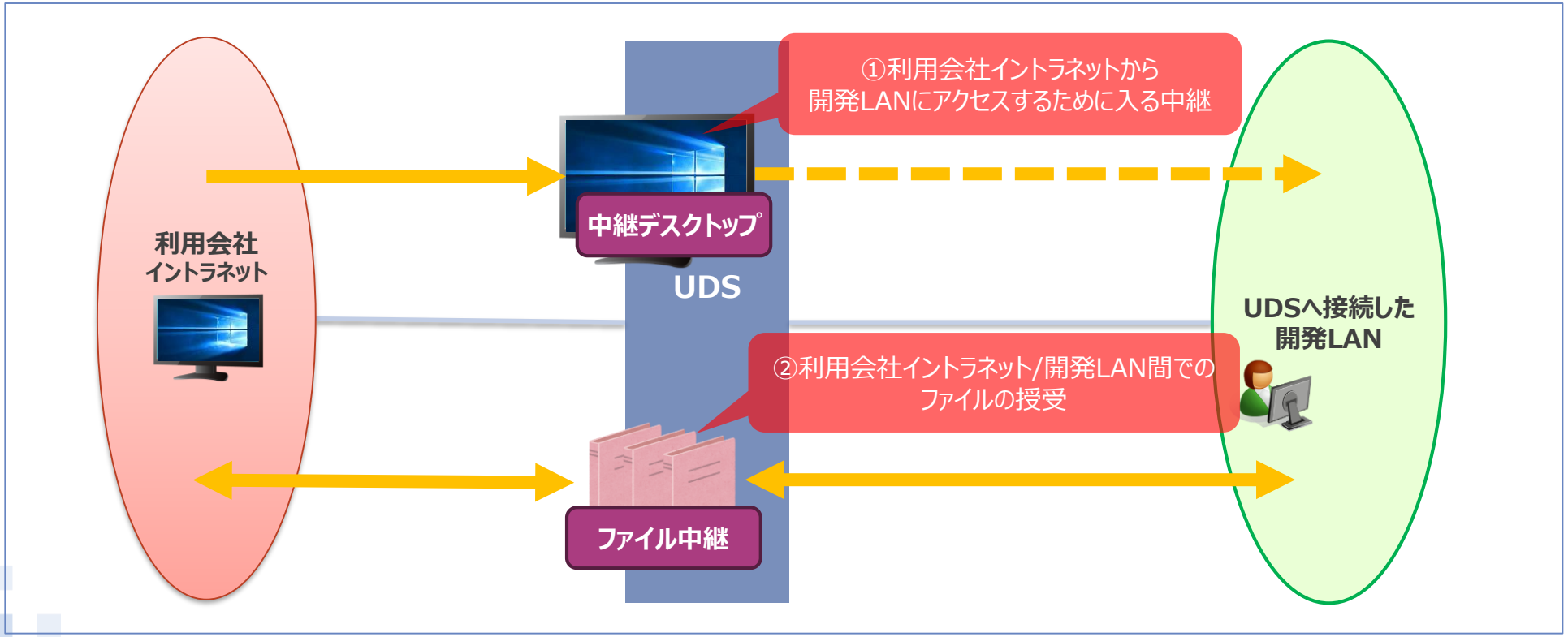
ARS

- サービス概要

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)から開発LANに安全に入るための中継装置としての機能を提供します。

- 利用会社イントラネットから開発LANにアクセスするための中継するデスクトップ機能
- 利用会社イントラネット/開発LAN間でのファイルの授受を可能にするファイル中継機能【UDS導入時のみの限定提供】

- 利用イメージ



NTT DATA

7.2. アクセス中継機能(基本機能)

ARS

No	分類	説明
1	前提条件	• 対象者 1. NTTデータ社員・協働者 2. 国内NTTデータグループ会社社員・協働者 3. ワークフローシステムにて登録された社外ユーザ • 利用可能な拠点 1. グループ共用セキュリティ基盤で接続した国内グループ会社社内ネットワーク • サービス利用にあたっては、申請が必要となります。
2	中継デスクトップ	• グループ共用セキュリティ基盤からUDS内の開発環境へ接続するための中継デスクトップ環境を提供します。 • 中継デスクトップ環境上から開発環境内の端末やサーバへリモートデスクトップあるいはSSHで接続することが可能です。 ※本機能は、インスタンス1台あたり小規模人数（～十数名程度）での利用を想定しております。
3	ファイル中継	• グループ共用セキュリティ基盤とUDS内の開発環境間でファイルを中継するための一時的なファイル格納領域を提供します。 ※本サービスは一時的なデータ受け渡しを目的としたサービスのため、データはバックアップされません。また、定期的にデータは削除されるため、ファイルサーバの代替としての使用はできません。 ※本サービスはUDS導入時のみの限定提供サービスです。継続利用は出来ません。 ※本サービスの申請方法は【別紙1】ファイル中継機能一時利用申請をご参照ください。

7.3. 中継デスクトップ機能(1/4)

ARS

No	分類	小分類	説明
1	基本動作	-	• グループ共用セキュリティ基盤からUDS内の開発環境へ接続するための中継デスクトップ環境を提供します。 • 中継デスクトップ環境上から開発環境内の端末やサーバへリモートデクストップあるいはSSHで接続することが可能です。 ※本機能は、インスタンス1台あたり小規模人数（～十数名程度）での利用を想定しております。
2	機能	中継デスクトップ環境	• 中継デスクトップ環境では以下のソフトウェアが利用可能です。 1. リモートデスクトップクライアント 2. SSH接続クライアント(Teraterm, Putty) 3. Webブラウザ(IE, Firefox) • MS Office製品やAdobe Reader等は提供されません。 • アプリケーションの追加インストールはできません。
3		サーバ管理	• 統合開発クラウドの開発ダッシュボード画面より、以下のサーバ管理機能を提供します。 1. 新規払い出し 2. ステータス確認 3. 再起動 4. 利用終了・削除 5. 強制停止(強制停止後は、該当サーバ再度起動することができません。) • 強制停止は、サーバに対するマルウェア感染等が確認された場合に利用する機能です。強制停止したサーバは二度と利用することができません。
4		ログ閲覧・ダウンロード	• 各ユーザのログインおよびログアウトに関するログを閲覧およびダウンロード可能です。 • ログの閲覧およびダウンロードは、払出し時に設定する監査者グループに属するユーザのみが利用可能です。 • 監査者グループには、UDSワークフローシステムで作成したプロジェクトグループを指定します。
5	接続元環境	NW	• 中継デスクトップ環境へのリモートデスクトップ接続は、以下の環境からのみ可能です。 1. グループ共用セキュリティ基盤利用会社からの接続(※) ※グループ会社社内ネットワークにて、後述の通信要件を満たしている必要があります。 • 開発LANから中継デスクトップ環境へのリモートデスクトップ接続はできません。

7.3. 中継デスクトップ機能(2/4)

ARS

No	分類	小分類	説明
6	接続元環境	端末	• 接続元となる端末は、下記いずれかの要件を満たす必要があります。 1. 利用会社シンクライアント端末 2. Microsoftサポート期間内のWindowsOSであり、かつWindowsUpdate等のセキュリティ対策が適切に実施されている端末およびサーバ • すべての環境において動作を保証するものではありません。端末の機種等によっては、サービスを利用できない場合あります。問合せおよび調査については、可能な範囲での対応となります。
7	接続元通信要件	中継デスクトップ環境	• デスクトップ環境へ接続するためには、下記の通信要件を満たす必要があります。 1. ポート番号3389/TCP、3389/UDP
8		ログ閲覧・ダウンロード	• ログ閲覧・ダウンロードを実施するためには、下記の通信要件を満たす必要があります。 1. ポート番号445/TCP 2. SMB2.0以上のプロトコルによる接続
9	接続先環境	NW	• 中継デスクトップ環境からの接続先は、以下に限定されます。 1. 開発LAN(統合開発クラウド、開発BXOを含む) • 中継デスクトップ環境からグループ共用セキュリティ基盤へリモートデスクトップ接続することはできません。 • 中継デスクトップ環境から管理外NWへ接続することはできません。開発LAN上の端末を経由して接続する必要があります。 • 中継デスクトップからセキュアインターネットアクセスサービスを介したインターネットへの通信はできません。
10		端末	• リモートデスクトップ接続先については、下記の要件を満たす必要があります。 1. Microsoftサポート期間内のWindowsOSであり、かつWindowsUpdate等のセキュリティ対策が適切に実施されている端末およびサーバ • 上記要件を満たさない環境へのリモートデスクトップ接続を禁止するものではありませんが、上記要件を満たさない環境については問合せ等のサポートを受けることができません。 • SSH接続については、接続先環境に関する制約事項はありません。 • すべての環境において動作を保証するものではありません。接続先の環境によっては、接続できない場合あります。問合せおよび調査については、可能な範囲での対応となります。

NTT DATA

7.3. 中継デスクトップ機能(3/4)

ARS

No	分類	小分類	説明
11	接続先 通信要件	-	• リモートデスクトップ接続およびSSH接続ともに任意のポートに接続することができます。 • 通信で利用するポートについて、開発LAN内で通信許可されている必要があります。
12	セキュリティ	認証	• 中継デスクトップ環境へのログイン時に、認証が行われます。 • ユーザ認証では、ワークフローシステムへ登録したアカウントを入力します。 • 払出し申請時に指定したUDSワークフローシステムのプロジェクトグループに含まれている利用者のみが利用可能です。
13		マルウェア 対策	• ファイルアクセス時にリアルタイムでマルウェアスキャンが実施されます。 • マルウェア発見時には中継デスクトップを停止し、該当する中継デスクトップ環境は恒久的に使用不能となります。また、事前登録済みの利用者メールアドレスへ通知します。
14		パッチ適用	• WindowsUpdate等のセキュリティパッチは自動的に適用されます。利用者がパッチを手動適用する必要はありません。
15		制限事項	• セキュリティ確保のため、中継デスクトップ環境では以下の制約があります。 1. クリップボード共有は行えません。 2. ローカルデバイスへのアタッチは行えません。 3. アプリケーションのインストール・アンインストールはできません。 4. OSおよびアプリケーションの設定変更はできません。 5. 切断状態が180分継続すると、自動的にサインアウトされます。 6. 不審・疑わしき振る舞いを発見した場合、サービス提供側から中継デスクトップ環境を強制的に停止・恒久的に使用不能する場合があります。
16	性能	同時接続数	• B1タイプ、B2タイプの2種類のインスタンスを提供します。 • 1台あたりの最大同時接続数は、B1タイプで12、B2タイプで24となります。

NTT DATA

7.3. 中継デスクトップ機能(4/4)

ARS

No	分類	小分類	説明
17	拡張	-	• 1ネットワークセグメント(/24～/28)毎に最大13～253台まで各環境を払出しが可能です。 • 構成できるネットワークセグメント数は、最大5セグメントです。 • 構成できるネットワークセグメント数は、各プロジェクトが統合開発クラウドで作成済のテナント数により変動するため、5セグメントを下回る場合があります。
18	可用性	-	• 中継デスクトップ環境のサーバ単体について可用性の保証はありません。複数台のサーバを払出すことを推奨します。 • 中継デスクトップ環境のサーバ単体について故障が発生した場合、再起動・新規払出し等によりユーザ自身で対処を実施します。 • 払出し申請時にクラスタを指定可能です。複数のクラスタを払い出すことで、クラスタダウン時の代替手段を利用者側で確保可能です。 • 複数払出したサーバの内、どのサーバに接続するかは利用者が指定する必要があります。
19	バックアップ	中継デスクトップ環境	• 中継デスクトップ環境上のデータは保証されず、バックアップ等はされません。一時的な保管用途として利用します。
20		ログ	• ログは90日間保存します。 • ログ容量が一定容量を超過した場合は古いログから予告なく削除を行う場合があります。
21	メンテナンス	-	• アクセス中継サービス全体として定義されたメンテナンス時間と、環境払出し時に利用者が指定する個別メンテナンス時間枠にてメンテナンスを実施します。 • サービスの利用状況等に応じて、選択可能なメンテナンス時間枠の設定は変更されます。 • メンテナンス時は、OS再起動等が行われるため、サービスをご利用いただけません。
22		ユーザプロファイル	• 30日以上利用されていないユーザプロファイルは自動的に削除されます。

NTT DATA

7.4. ファイル中継機能(1/3)

ARS

No	分類	小分類	説明
-	前提条件	-	• 本サービスはUDS導入時において、一時的に大容量ファイル転送が必要な場合に14日間の期間限定で提供します。 • 本サービスを用いたファイル転送時に大量のトラフィックを流す場合には以下条件を順守する必要があります。 <利用条件> 1.時間帯：平日20:00～8:00 2.帯域上限：300Mbps
	留意事項	-	• 本サービスの利用においては以下留意事項を了承する必要があります。 <留意事項> 1.サービス提供元で問題を検知した場合、速やかに作業を停止してください。 2.メンテナンス等によって接続が一時的に利用できなくなる可能性があります。 3.複数プロジェクト様が同時に大量トラフィックを流す作業を行わないよう、日時を調整させていただく場合があります。 大量トラフィックを流す作業を予定されている場合は、利用申請時に予め作業予定をご連絡ください。
1	基本動作	-	• グループ共用セキュリティ基盤とUDS内の開発環境間でファイルを中継するための一時的なファイル格納領域を提供します。 ※本サービスは一時的なデータ受け渡しを目的としたサービスのため、データはバックアップされません。また、定期的にデータは削除されるため、ファイルサーバの代替としての使用はできません。
2	機能	ファイル格納領域	• 50GBのファイル格納領域に加えて、利用開始後14日間限定で1TBの大容量ストレージを提供します。
3		サーバ管理	• 統合開発クラウドの開発ダッシュボード画面より、以下のサーバ管理機能を提供します。 1. 新規払い出し 2. ステータス確認 3. 再起動 4. 利用終了・削除 5. 強制停止(強制停止後は、該当サーバ再度起動することができません。) • 強制停止は、サーバに対するマルウェア感染等が確認された場合に利用する機能です。強制停止したサーバは二度と利用することができません。

7.4. ファイル中継機能(2/3)

ARS

No	分類	小分類	説明
4	機能	ログ閲覧・ダウンロード	• 各ユーザのログインおよびログアウトに関するログを閲覧およびダウンロード可能です。 • ログの閲覧およびダウンロードは、払出し時に設定する監査者グループに属するユーザのみが利用可能です。 • 監査者グループは、UDSワークフローシステムで作成したプロジェクトグループを指定します。
5	接続元環境	NW	• ファイル中継環境への接続元となる端末およびサーバは、以下の環境からのみ可能です。 1. 利用会社イントラネットからの接続 2. 開発LAN(統合開発クラウド、開発BXOを含む)からの接続 • 管理外NWから接続することはできません。
6	接続元通信要件	端末	• ファイル中継環境への接続元となる端末およびサーバは、下記いずれかの要件を満たす必要があります。 1. Microsoftサポート期間内のWindowsかつ、Windowsアップデート等のセキュリティ対策が適切に実施されている端末およびサーバ • 上記要件を満たさない端末からの接続を禁止するものではありませんが、上記要件を満たさない環境については問合せ等のサポートを受けることができません。 • すべての環境において動作を保証するものではありません。端末の機種等によっては、サービスを利用できない場合があります。問い合わせおよび調査については、可能な範囲での対応となります。
7		-	• ファイル中継環境へ接続するためには、下記の通信要件を満たす必要があります。 1. ポート番号445/TCP 2. SMB2.0以上のプロトコルによる接続
8	セキュリティ	認証	• ユーザ認証では、ワークフローシステムへ登録したアカウントを入力します。 • 払出し申請時に指定されたワークフローシステムのプロジェクトグループに含まれている利用者がファイル中継機能を利用可能です。
9		フォルダアクセス権限	• デフォルトでは、申請時に指定したプロジェクトグループのメンバがルートフォルダ(Shareフォルダ)配下のすべてのフォルダにアクセス可能です。 • ルートフォルダ直下のサブフォルダについてのみ、指定したプロジェクトグループにのみ閲覧権限を付与するアクセス制御が可能です。

7.4. ファイル中継機能(3/3)

ARS

No	分類	小分類	説明
10	セキュリティ	マルウェア対策	• ファイルアクセス時にリアルタイムでマルウェアスキャンが実施されます。 • マルウェア発見時には中継デスクトップを停止し、該当する中継デスクトップ環境は恒久的に使用不能となります。また、事前登録済みの利用者メールアドレスへ通知します。
11		パッチ適用	• WindowsUpdate等のセキュリティパッチは自動的に適用されます。利用者がパッチを手動適用する必要はありません。
12		制限事項	• 不審・疑わしき振る舞いを発見した場合、サービス提供側から本機能を強制的に停止・恒久的に使用不能する場合があります。
13	性能	同時接続数	• 同時接続数の上限は設けられていません。 • 同時接続数は利用者の利用状況によって変動します。
14	可用性	-	• ファイル中継環境のサーバ単体について可用性の保証はありません。 • ファイル中継環境のサーバ単体について故障が発生した場合、再起動によりユーザ自身で対処を実施します。 再起動後も事象が解消しない場合はOIヘルプデスクまでお問い合わせください。 • 払出し申請時にクラスタを指定可能です。
15	バックアップ	ファイル中継環境	• ファイル中継環境上のデータは保証されず、バックアップ等はされません。一時的な保管用途として利用します。
16	メンテナンス	-	• アクセス中継サービス全体として定義されたメンテナンス時間と、環境払出し時に利用者が指定する個別メンテナンス時間枠にてメンテナンスを実施します。 • メンテナンス時は、OS再起動等が行われるため、サービスをご利用いただけません。
17		ファイル削除	• ファイル中継環境内のファイルは、環境払出し時に利用者が指定する個別メンテナンス時間枠のファイル削除処理のタイミングで削除されます。（フォルダは残ります。） • サービスの利用状況等に応じて、選択可能なメンテナンス時間枠の設定は変更されます。 • 1TBの大容量ストレージは、削除の対象外となります。

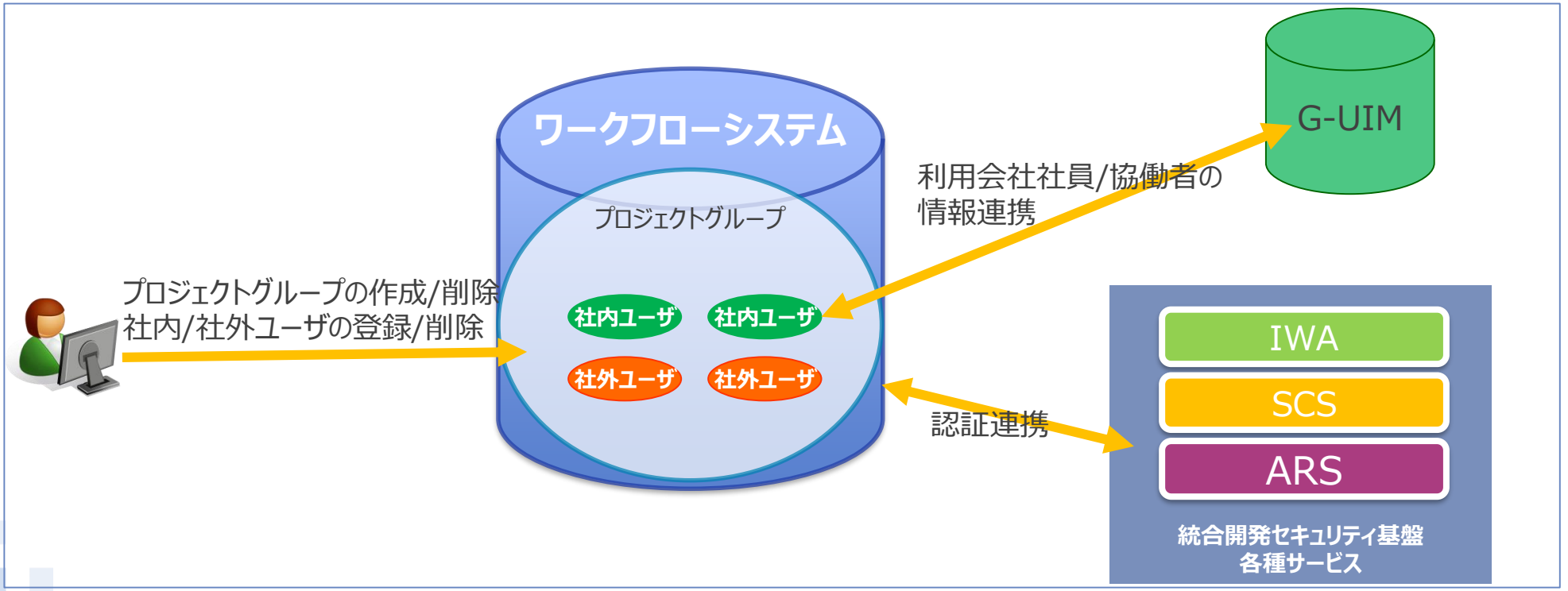
8. アカウントの管理（ワークフローシステム）

8.1. ワークフローシステム概要

- システム概要

ワークフローシステムは、UDSや統合開発クラウドを利用する為の、アカウントや権限管理を行うためのシステムです。
利用会社社員/協働者のアカウント情報はG-UIMより連携されます。
※利用会社以外のNTTデータグループ会社社員/協働者のアカウントは、
利用会社の協働者としてG-UIMへ登録するか、社外ユーザとして登録する必要があります。

- 利用イメージ



8.2. ワークフローシステムの機能

<table>
<tr><th>No</th><th>業務区分</th><th>機能</th></tr>
<tr><td>1</td><td>プロジェクトグループの管理</td><td>プロジェクトグループの作成・変更・削除を行います。プロジェクトグループには、管理者、副管理者を登録必要があります。
※　プロジェクト管理者は利用会社社員管理職のみ設定可（1名）、プロジェクト副管理者は利用会社社員/協働者を設定可（20名）</td></tr>
<tr><td>2</td><td>認証/認可制御</td><td>作成したプロジェクトグループへメンバを登録することで、統合開発セキュリティ基盤、統合開発クラウドが提供する各種サービスを利用することが可能です。
ユーザ認証では、以下のID/PWを入力します。
<table>
<tr><th colspan="2">ユーザ区分</th><th>ID</th><th>Pass</th></tr>
<tr><td>社内ユーザ</td><td>利用会社社員/協働者</td><td>japan¥GWNet利用者ID_会社識別子</td><td>GWNetログイン時のパスワード</td></tr>
<tr><td>社外ユーザ</td><td>上記以外の利用者
（協力会社やお客様）</td><td>guest¥ワークフローシステムで登録したID</td><td>ワークフローシステムで設定したパスワード</td></tr>
</table>
なお、本システムを利用した権限情報をPJ側のシステム等へ連携することはできません。
アカウントを利用するサービスは下記の通りです。
◆統合開発セキュリティ基盤
• セキュアインターネットアクセスサービスにおけるproxyのユーザ認証
• 端末セキュリティ管理サービスにおけるエージェントの認証
• アクセス中継サービスにおける認証/認可制御
◆統合開発クラウド（※）
• パブリッククラウド利用における認証/認可制御
※ 詳細は、統合開発クラウドへお問い合わせください。</td></tr>
<tr><td>3</td><td>メンバ/権限の管理</td><td>プロジェクトグループへ登録できるアカウントは、社内ユーザ（G-UIMに登録がある利用会社社員/協働者）ならびに社外ユーザ（ワークフローシステムで登録したG-UIMにアカウントが存在しないユーザ）になります。
以下、メンバ/権限管理における留意点です。
• 社内ユーザは、G-UIMに登録されているアカウント情報を利用します。
• 社外ユーザは、ワークフローシステムでアカウントを作成します。作成時、所属するプロジェクトグループを指定する必要があります。また、アカウント作成に当たり、必ずお客様の個人情報管理担当元と統合開発セキュリティ基盤の個人情報取り扱いについて同意していただく必要があります。
• 同一の社外ユーザが複数プロジェクトグループへ所属することはできません。プロジェクトグループごとに個別にアカウントを作成する必要があります。</td></tr>
</table>

上記業務を実行できるアクターについては、利用マニュアルをご参照ください。

9. 料金体系

9.1. サービス利用料(1/2)

UDSサービスを契約すると下表の月額利用料が発生します。

サービス区分	プラン		月額利用料		備考
基本サービス	NW接続 ①＋② ※ ②接続ポイント数は利用人数が21名以上場合に適用	①利用人数	1名～20名部分	¥1,400/人	カウント方法は、UDSへ接続した環境を利用している人数
			21名～50名部分	¥800/人	
			51名～150名部分	¥600/人	
			151名～300名部分	¥400/人	
			301名～439名部分	¥200/人	
			440名以上	¥200,000（一律）	
		②接続ポイント数	¥10,000/接続ポイント		UDSへ接続する環境数
インフラサービス	セキュアインターネットアクセス		¥100/人		インターネットへアクセスする人数
	メールセキュリティ		¥90/メールアドレス		利用するメールアドレス数
	端末セキュリティ管理		¥170/台		エージェントを導入する端末数
	アクセス中継		¥1,500/GB		払出し済みインスタンスの予約メモリ量
オプション機能	NW接続	NTTデータビル ラック利用	¥10,000/Unit		インチラックにおける1.75インチ分の高さ数
		NTTデータ管理外NW接続	冗長構成：¥37,000 シングル構成：¥25,000		
		NTTデータビル 現地立会対応	￥40,000/回		ネットワーク接続サービス利用開始時の初回立会は除く
	セキュアインターネットアクセス	個別プロトコル利用	¥10,000/グローバルIPアドレス		通信元のグローバルIPアドレス数、開発端末10台毎に1グローバルIPアドレスにNAPTする仕様

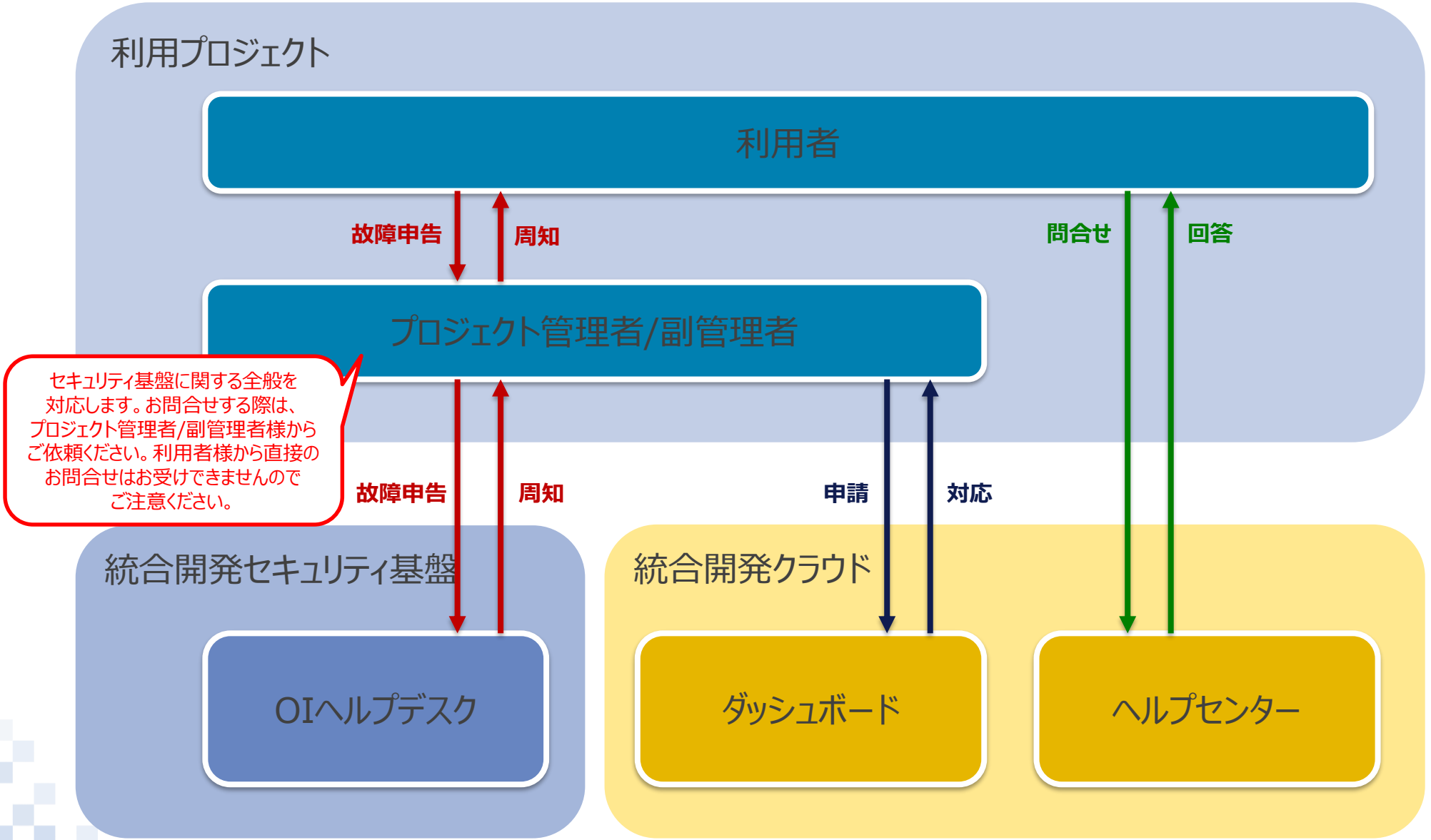
※ 利用者数が100名の接続ポイント2つの場合、基本サービスの月額利用料は
{(20名×1400)＋(30名×800)＋(50名×600)}+{2×10000}＝82000 ＋ 20000＝102000円 となります。

9.1. サービス利用料(2/2)

No	項目	関連プラン	説明
1	利用料金	-	• 月額利用料は、**基本サービス利用料**と**インフラサービス利用料**と**オプション機能利用料**の合算となります。 • UDS導入に伴い発生する各種費用（機器、回線、稼働等）はPJ側での負担となります。
2	課金開始	-	• UDS各種サービス申請が**完了した翌月**から課金開始となります。
3	請求処理	-	• 各月1日時点で完了している統合開発クラウドダッシュボード上のお申込み内容に基づいて請求額を決定します。 • **四半単位（6月、9月、12月、3月）**に請求処理を行います。
4	課金仕様	NW接続	• 接続ポイントは以下をカウントし、合計が接続ポイント数となります。 ・利用会社イントラネット（アクセス中継サービスを経由） ・パブリッククラウド（統合開発クラウド提供） ・UDSへ接続した開発環境数（統合開発クラウド提供のNCIT版プライベートクラウド含む）
5		アクセス中継	• 払出し済みインスタンスの**予約メモリ量の合計32GBまでは無償**となります。 ※ 予約メモリ量の合計が48GBの場合、48GB-32GB=16GB分に対して料金が発生します。
6		NTTデータ管理外NW接続	• 構成するFWスペックにより利用料金は変動します。 • 本紙に記載されている料金プランは、おおよそ500人未満の利用を想定したFWスペックとなります。 • 利用人数が500名を超える場合や、通常よりも通信料が多いことが想定される等、個別要件がある場合はご相談ください。別途見積もりします。
7		NTTデータビル現地立会対応	• 立会費用は、四半期に発生した回数分の費用を合計し、月額利用料の請求処理に合わせて行います。
8	その他	NTTデータビル現地立会対応	• NTTデータビルにあるUDS提供元管理ラックの開け閉めが必要な場合にUDS提供元担当者の立会が必要です。 具体的なケースは下記の通り。 ・PJ拠点の追加に伴い、回線を引き込み及び、回線受けのNW機器をラックへ追加設置する。 ・ラックに設置しているPJ側のNW機器で障害が発生しオンサイト対応を行う。 ・ラックに設置しているPJ側のNW機器撤去作業を行う。 • PJ担当者の立会は必須です。

10. 運用仕様

10.1. 運用体制



10.2. サービスレベル

- 運用サービス一覧

項目	サービス時間(JST)	内容
お問合せ	平日　9:00-12:00 13:00-17:00	プロジェクト管理者/副管理者からのサービスの利用方法に関する問合せ、故障申告を受け付けます。
申請対応	平日　9:00-12:00 13:00-17:00	プロジェクト管理者/副管理者からの申請を受け付けます。申請内容については次頁の「申請一覧」を参照ください。
サービス監視	24時間365日	サービス提供の維持に必要な項目を監視致します。 上記には、利用プロジェクトが個別に管理する機器は含みません。
故障対応	平日 9:00～17:00	システム異常を検知した場合、復旧対応、および利用者（UDS申請における申請責任者/連絡先メーリングリスト）通知を行います。 ※ NTTデータの基幹システムと設備を共有しておりますので、故障対応方針も準じます。
定期/緊急 メンテナンス	-	定期メンテナンスを実施します。（実施日時はサポートサイトに掲載） セキュリティ対応等により緊急メンテナンスを実施する場合があります。メンテナンスによりサービスが一時中断する際には、UDS申請における申請責任者/連絡先メーリングリストに通知します。

- 故障時対応方針

時間帯(JST)	復旧目標時間
平日 9：00～17：00	故障検知から3時間以内を目標 オンサイト対応が必要な場合は、機器設置拠点に到着してから3時間以内を目標
上記以外の時間帯 (土日祝日含む)	翌営業日開始時刻(9:00)から3時間以内を目標

11. 導入までの流れ

11.1. 導入までの流れ

① UDSの仕様が開発要件に沿うものであるかをご確認ください。
② PJの開発環境をどういった形でUDSへ接続するかをご検討ください。
③ UDSへ接続するための回線や機器をご準備ください。
④ ワークフローシステムでプロジェクトグループ登録を行い、利用申込みと、統合開発クラウドのダッシュボードよりUDS申請を実施してください。
⑤ PJ側の設定を行い、UDSとの疎通確認を実施してください。

※ 過去の導入実績より、②、③、⑤に時間を要する傾向がございますので、余裕をもってご対応ください。（リードタイムとして1～2ヵ月程度を想定してください）
※ 手続きの詳細・各種上限値については、統合開発セキュリティ基盤サポートサイトをご確認ください。
https://uds-portal.x-network.jp/uds/

11.2. 利用申込み方法

- G会社プライム案件では、
「01_【別紙01】統合開発セキュリティ基盤_利用申込書」または、
「02_【別紙02】統合開発セキュリティ基盤_利用終了申込書」をOIヘルプデスクへ送付し、
サービスのお申込みを行います。

- サービスお申し込み完了後、統合開発クラウドダッシュボードよりUDS各種サービスの申請手続きが可能となります。

- UDS各種サービスの申請一覧は次ページをご参照ください。

11.3. 申請一覧(1/2)

サービス区分	発生するケース	必要な申請
UDS全般	UDSを新規で利用開始する。	・[統合開発クラウドダッシュボード] UDS基本申請
	UDSのサービス利用数増減する。	
	UDSの利用を終了する。	
ネットワーク接続サービス	UDSへ接続するポイント数が増減する。	・[統合開発クラウドダッシュボード] UDS：ネットワーク接続サービス申請
	UDS利用開始後、ITMラックをレンタルしており、PJ側理由でオンサイト対応をする。	・[統合開発クラウドダッシュボード] UDS：関連作業申請
	UDS利用開始後、ITMラックをレンタルしており、専用線・閉域網経由接続している拠点の増減に伴う回線引込を行う。	
セキュアインターネットアクセスサービス	セキュアインターネットアクセスサービスの利用を開始する。	・[統合開発クラウドダッシュボード] UDS：セキュアインターネットアクセスサービス申請
	セキュアインターネットアクセスサービスのサービス利用人数が増減する。	
	インターネット上のサイトでアクセスできるサイトが追加/削除する。	
	インターネット上のサイトで認証なしでアクセスできるサイトが追加/削除する。	
	インターネット上のサイトでhttp/https以外のプロトコルでアクセスする。	
	プロジェクト側で用意したDNSサーバで管理するDNSゾーンの情報をインターネットに公開する。	
	ホストの名前情報をインターネットに公開する。	
	セキュアインターネットアクセスサービスの利用を終了する。	
インターネットメールセキュリティサービス	インターネットメールセキュリティサービスの利用を開始する。	・[統合開発クラウドダッシュボード] UDS：インターネットメールセキュリティサービス申請
	インターネットメールセキュリティサービスのメールアドレス数が増減する。	
	プロジェクトで保有しているメールドメインやメールサーバを本サービスへ登録する。	
	スパムと誤判されたメールについて、受信を許可する送信元のドメインを登録する。	
	インターネットメールセキュリティサービスの利用を終了する。	

11.3. 申請一覧(2/2)

サービス区分	発生するケース	必要な申請
インターネットメールセキュリティサービス	中継サーバのメールログ提供依頼。（最大過去1年分となります。）	・[統合開発クラウドダッシュボード] UDS：関連作業申請
端末セキュリティ管理サービス	端末セキュリティ管理サービスの利用を開始する。	・[統合開発クラウドダッシュボード] UDS：端末セキュリティ管理サービス申請
	端末セキュリティ管理サービスの端末数が増減する。	
	開発端末に各エージェントを導入する。	
	端末セキュリティ管理サービスの利用を終了する。	
アクセス中継サービス	アクセス中継サービスの利用を開始する。	・[統合開発クラウドダッシュボード] UDSアクセス中継サービス申請
	アクセス中継サービスの利用を終了する。	

12. その他

12.1. 標的型攻撃対策ガイドラインとの対比(1/3)

標的型攻撃対策ガイドラインより転載

1.1. 本ガイドラインについて

NTTデータグループ各社が取り扱う情報システム(※1)に対して、標的型攻撃対策を実施する際のガイドラインである。

本ガイドラインでは、NTTデータで実施している標的型攻撃対策をモデルケースとして提示している。情報システムへの技術的攻撃、オフィス環境における端末対策、運用ルール、社員教育対策など、対策全般を解説する。

標的型攻撃対策ガイドラインにて定められている対策モデルは、以下の4観点に大別される。

No	観点	説明
1	入口対策	インターネットとの接続点において、インターネットからの攻撃を防ぐ対策。標的型攻撃対策では攻撃手段に主にメールを用いるので、メールサーバにおけるセキュリティ対策が重要となる。
2	内部対策	ユーザが操作する端末をはじめとして、社内に設置されるコンピュータが不正プログラムに感染することを防ぐ対策。OS・アプリケーションのセキュリティパッチの最新化やウイルス対策ソフトの適切な設定が標的型攻撃に有効な対策となる。攻撃者は、端末以外には、Active Directoryサーバをはじめとして共通利用されるサーバ類への攻撃を行うことが想定されるため、それらのサーバ類への対策を行うことは特に重要となる。
3	出口対策	社内に不正プログラムが潜入した場合に、不正プログラムから攻撃者への通信を防御・検知する対策。ファイアウォール、Proxyサーバの適切な設定や、ネットワーク機器のログ監視が重要となる。
4	教育・啓発活動	標的型攻撃への社員の対応力を向上させる活動。教育・訓練等を通して、不審なメールの見分け方や、攻撃を受けた場合の初動対応力の向上を行う。

12.1. 標的型攻撃対策ガイドラインとの対比(2/3)

標的型攻撃対策ガイドラインの対策項目(※1)と統合開発セキュリティ基盤で提供予定のサービスの紐付けを示す。

標的型攻撃ガイドラインにおける対策の目次			対策カテゴリ	統合開発セキュリティ基盤	
				サービス提供	提供サービス
入口対策	4.1.1	メールサーバのセキュリティ対策 ウイルス対策ソフト(メールサーバ用)	システム	○	インターネットメールセキュリティサービス
		メール添付ファイの拡張子規制	システム	○	インターネットメールセキュリティサービス
		スパムメールフィルタ	システム	○	インターネットメールセキュリティサービス
		メールサーバのログ設定	システム	○	インターネットメールセキュリティサービス
		メールアーカイブ	システム	–	—
	4.1.2	ファイアウォール	システム	○	セキュアインターネットアクセスサービス
	4.1.3	侵入検知・防止システム(IDS、IPS)	システム	○	セキュアインターネットアクセスサービス
	4.1.4	(オプション)侵入検知・防止システム(サンドボックス)	システム	–	—
内部対策	4.2.1	ソフトウェアのバージョンの更新	システム	○	端末セキュリティ管理サービス
		セキュリティ更新プログラム情報の収集、周知	運用	–	—
		サポート期限切れ製品情報の把握、周知	運用	–	—
	4.2.2	ウイルス対策ソフト	システム	○	端末セキュリティ管理サービス (ソフトライセンスは含まず)
		(オプション)ふるまい検知型ウイルス対策ソフト	システム	–	—
	4.2.3	バージョン管理ソリューション	システム	○	端末セキュリティ管理サービス (クライアント環境が対象)
	4.2.4	メールクライアントのプレビューア機能の無効化	運用	–	(クライアント設定)
	4.2.5	情報漏えい対策ソリューション	システム	○	端末セキュリティ管理サービス

※1 「標的型攻撃対策ガイドライン　4.　対策編」

12.1. 標的型攻撃対策ガイドラインとの対比(3/3)

標的型攻撃ガイドラインにおける対策の目次			対策カテゴリ	統合開発セキュリティ基盤	
				サービス提供	提供サービス
内部対策	4.2.6	管理者権限の適切な管理	システム	○	(プロジェクト管理のサーバは対象外 ※2)
	4.2.7	ファイル共有の適切な管理	システム	○	アクセス中継サービス (プロジェクト管理のサーバは対象外 ※2)
	4.2.8	開発/運用環境における端末利用ルール	運用	–	—
	4.2.9	ネットワークセグメント間の適切なアクセス制御の実施	システム	○	ネットワーク接続サービス(※3)
	4.2.10	ADサーバをはじめとするWindowsサーバのログ取得と保存	システム	○	(プロジェクト管理のサーバは対象外 ※2)
	4.2.11	ローカル管理者のパスワード設定ルール	運用	–	–
	4.2.12	WindowsClientイベントログ	システム	–	–
出口対策	4.3.1	ファイアウォール	システム	○	セキュアインターネットアクセスサービス
	4.3.2	Proxyサーバ	システム	○	セキュアインターネットアクセスサービス
	4.3.3	URLフィルタリング	システム	○	セキュアインターネットアクセスサービス
	4.3.4	DNSサーバのログ設定	システム	○	セキュアインターネットアクセスサービス
	4.3.5	侵入検知・防止システム(IDS、IPS)	システム	○	ネットワーク接続サービス セキュアインターネットアクセスサービス
	4.3.6	ログ運用(ログ監視)	システム	–	(ログ監視サービスは提供対象外)
		(オプション)ログ分析	運用	–	–
	4.3.7	インターネット上の情報収集	運用	–	–
教育・啓発活動			運用	–	–
コンテンジェシープランの策定			運用	–	–

※2 開発LAN内で運用されているAD(Active Directory)サービス等は、統合開発セキュリティ基盤サービスの対象外
※3 インターネット～統合開発セキュリティ基盤、統合開発セキュリティ基盤～各開発LAN間におけるアクセス制御

12.3. UDS導入のサポート体制

サービス利用申し込み、UDSのサービス導入、サービス仕様に関するお問合せやご相談は、以下の窓口までご連絡ください。

UDS導入に関するお問合せ先
ITマネジメント室 統合開発セキュリティ基盤 導入推進担当
Mail：ide-desk@am.nttdata.co.jp

【別紙1】ファイル中継機能一時利用申請(1/2)

申請の事前に、UDSネットワークを指定したファイル中継インスタンスの払い出しを行い
下記フォーマットに記載し、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)
========ファイル中継機能一時利用申請フォーマットここから========
件名:【G会社プライム】【UDS:アクセス中継サービス】ファイル中継機一時利用申請
本文:
下記の通り、ファイル中継インスタンスの一時利用を希望します。
■利用UDSのPJグループID
pgr****
■対象のファイル中継インスタンス
harsft****
========ファイル中継機能一時利用申請フォーマットここまで========

通常、申請から5営業日を目安に対応可能です。

【別紙1】ファイル中継機能一時利用申請(2/2)

対応完了後、申請されたインスタンスの利用期間を連絡致しますので
必ず利用期間内に下記フォーマットに記載しファイル中継機能一時利用終了申請を行ってください。

(下記フォーマットの赤字部分を変更して申請すること)
========ファイル中継機能一時利用終了申請フォーマットここから========
件名:【G会社プライム】【UDS:アクセス中継サービス】ファイル中継機一時利用終了申請
本文:
下記の通り、ファイル中継インスタンスの一時利用終了を希望します。
■利用UDSのPJグループID
pgr****
■対象のファイル中継インスタンス
harsft****
========ファイル中継機能一時利用終了申請フォーマットここまで========

※留意事項※

1. 本申請は、1プロジェクトあたり1回限りとなります。
2. 複数プロジェクトからの申請が重なった場合、ご利用をお待ちいただく可能性があります。
3. 申請されたインスタンス分のメモリ量は、払い出しを行った翌月1日AM5:00に予約メモリ量としてカウントされます。
   翌月1日AM5:00までに利用終了を完了いただければ対象インスタンス分の課金は発生しません。

NTT DATA

Trusted Global Innovator