警察庁　御中

共通基盤システムにおける調査研究

最終報告書

2025 年 3 月 14 日

株式会社 NTT データ

目次

エグゼクティブサマリ

1. 目的

警察庁の共通基盤システムのリプレースに向けて、令和５年度に実施した調査研究おいて策定した将来的な共通基盤システムのあるべき姿に向けたロードマップに対し、セキュリティ面のあるべき姿、ネットワーク最適化、仮想化ソフトウェアについて検討し、提言する。

2. 調査項目

本調査研究において定めた方針および整理した要件に基づいて、共通基盤システムのセキュリティ面のあるべき姿、ネットワークの最適化について現状整理と次期および将来的な姿について検討した。また、仮想化ソフトウェアについては、警察庁要件の確認を行ったうえで、仮想化の市場動向を踏まえた比較・整理を行い、実機検証にてシステム移行における影響調査を実施した。本調査研究の結果を踏まえ、次期共通基盤システムへの移行を推進する。

なお、本調査研究の内容は以下のとおりである。

調査項目	調査対象
セキュリティ	・在宅勤務および執務室からのアプリケーション開発 ・開発の対象、工程 ・セキュリティリスク、対策 ・シンクライアント環境 ・開発環境要件 ・業務の配置方針 ・クラウド ・LAN間データ交換装置の市場調査、実機検証、製品構成 ・セキュリティ要件、製品構成 ・ゼロトラストセキュリティの導入計画、運用高度化
ネットワーク	・業務毎の通信傾向、最適な通信帯域 ・QoS設計 ・トラフィック優先度 ・IPアドレスリソース管理 ・名前解決 ・データセンタ運営
仮想化ソフトウェア	・仮想環境要件 ・市場動向 ・移行方式 ・システム移行における影響、実機検証 ・コンテナ

3. 共通基盤システムにおける将来的なセキュリティ面のあるべき姿

検討

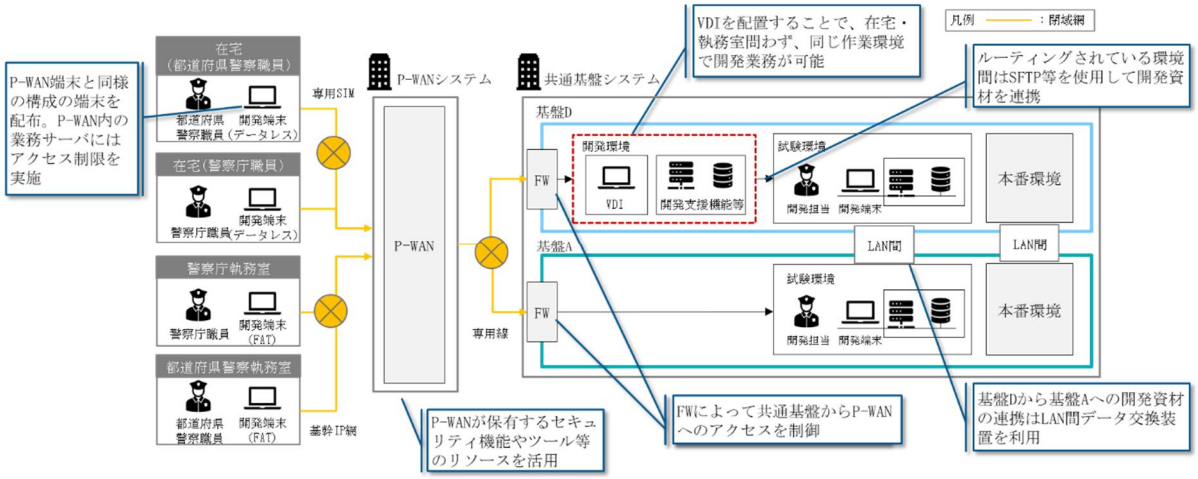
・在宅勤務および執務室でのアプリケーション開発において、セキュリティリスクを考慮したうえでの開発のあり方について検討する。

・LAN 間データ交換装置について製品の比較検討を行う。

・ゼロトラストモデルでのセキュリティ対策を段階的に進めるための計画を提案する。

結論

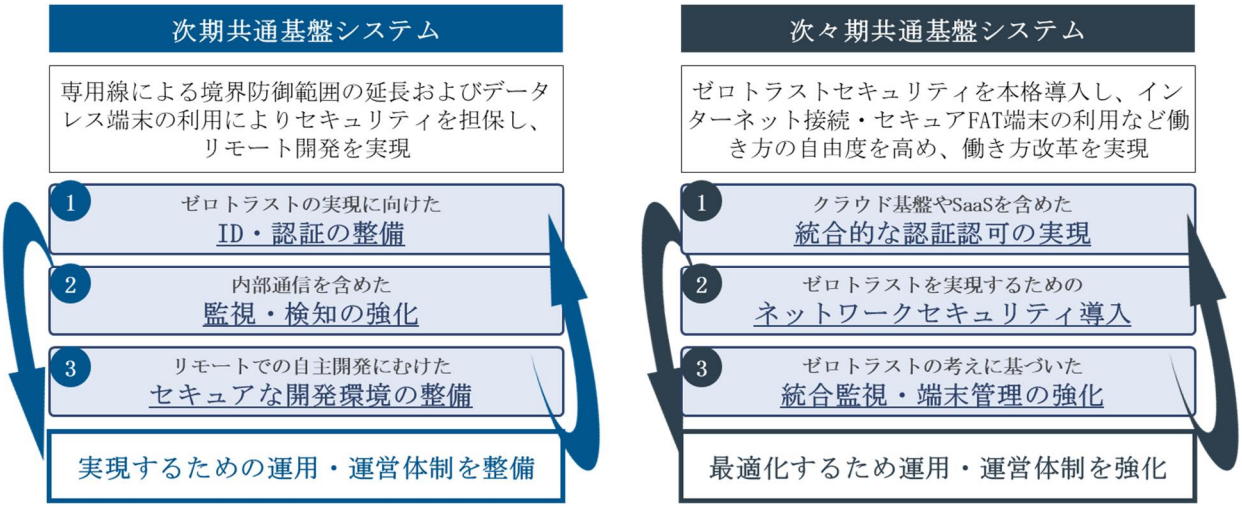
・次期共通基盤システムで実現するアプリケーション開発については、P-WAN を経由し開発環境の VDI にアクセスする方式を推奨案とした。全体像については以下のとおりである。



・LAN 間データ交換装置および、代替としてデータ転送のいずれかの方式での分離を実現できる製品について広く市場調査したうえで机上での比較を行い、更に実機検証において比較を実施した。比較結果は以下のとおりである。

比較観点	比較		製品名	
	機能項目		製品①（物理分離型製品）	製品②（論理分離型製品）
セキュリティ	片方向・データ転送機能	共通	逆方向への転送を防ぐ仕組みを有していることを確認	
		転送可能時間の指定	転送可能時間の指定可	特定日時の指定は不可
	認証・認可機能	共通	利用者の制限、ファイルの転送許可・不可の設定があることを確認	
	ログ出力	共通	いつ・誰が・何のファイルを転送したかログが残ることを確認	
		ログローテーション	PowerShell等作り込みが必要	固定で1日1回ローテーション可能
	ファイル無害化機能	ファイル無害化	ファイル無害化はOP対応で可	
		アンチウィルス	アンチウィルスは送信端末に別途導入が必要	アンチウィルスはOP対応で可
データ転送性能	データ収集間隔	最小設定値	1秒(設定可)	10秒
	データ転送速度(単体)	転送対象 100MB×10ファイル	105秒 実測値：9.52MB/秒(USB2.0) 理論値：25MB/秒(USB3.0)	25秒 40MB/秒(GbE)
	同時接続・並列転送	全般	同時接続・並列転送 可	同時接続・並列転送 不可
拡張容易性	スケールアウト	全般	○可能 柔軟に構成が可能	△制限あり ファイルサーバ(端末)を両端に1対1で配置が必要
利用者利便性	複数データ交換	同一端末		
		複数端末		
	制限事項の確認	制限事項		

・次期および次々期の共通基盤システムにおいて、セキュリティ対策の強化とセキュリティ運用の高度化を段階的に実施する。それぞれの段階での重点方針について以下のとおり整理した。



4. 共通基盤システムにおけるネットワークの最適化

検討

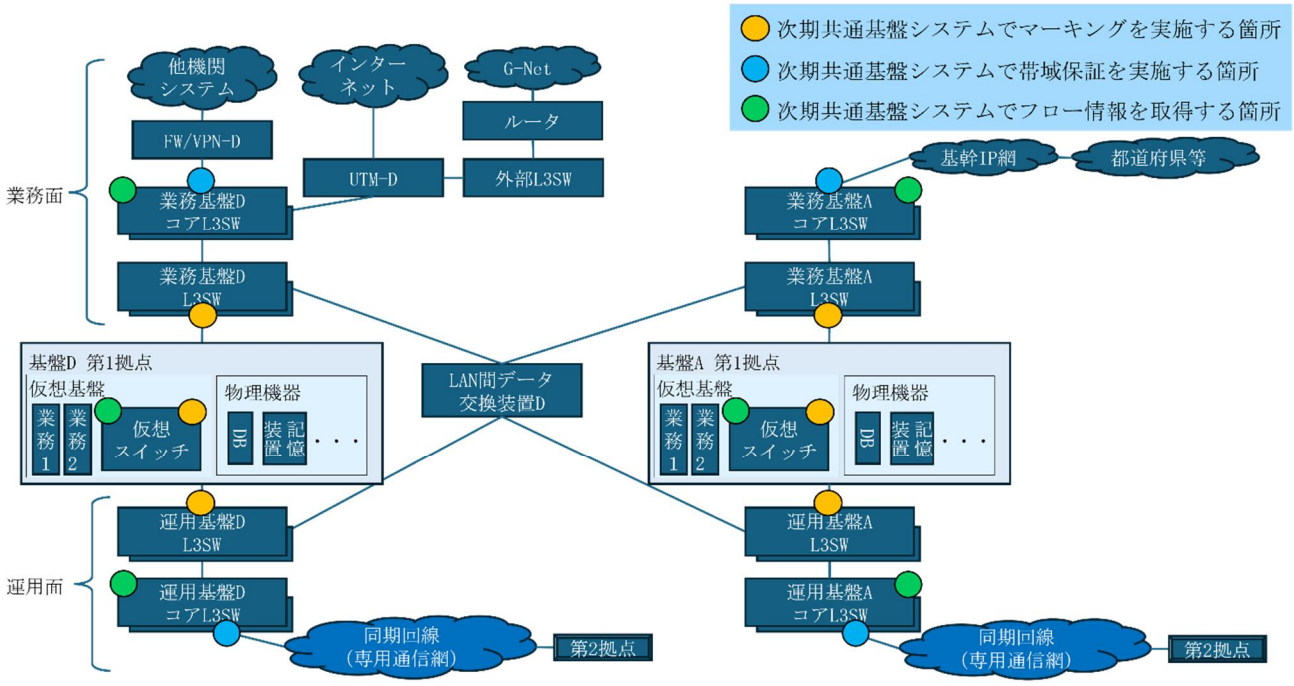
・将来的なトラフィック増加によるネットワーク輻輳に対処するため、適切な通信傾向分析、QoS 設計並びに動的に QoS を制御する手法について検討する。

・IP アドレスの管理および利用方法についてあるべき姿について検討する。

結論

次期共通基盤システムでは以下を推奨案とした。

・下図の箇所にて、フローの取得、マーキング、帯域保証を実装する。



・コア L3 スイッチでフロー情報を取得し、ネットワークの可視化／通信傾向の分析を行う。

・動的に QoS を制御する手法として、スイッチのバッファ割り当て自動調整機能、WRED 機能を活用する。
・IP アドレス管理システムである IPAM を導入し、IP アドレスの管理について現状のファイル運用から IPAM による運用に切り替える。
・内部通信におけるホスト名と IP アドレスの名前解決方法について、現状の Hosts ファイルを用いた方式から DNS を用いた方式に切り替える。

5. 共通基盤システムにおける仮想化ソフトウェアの比較検討

検討

広く世の中の技術や市場動向を調査し比較検討する。また、バージョンが異なる仮想化ソフトウェア間および異なる仮想化ソフトウェア間のシステム移行について、実機検証を実施する。

結論

広く市場動向において机上調査を実施し、仮想化アセスメントを実施のうえで対象を絞り、詳細比較として実機検証を行った。3 製品の比較結果は以下のとおりである。

比較観点	製品名		
	製品①	製品②	製品③
全般	仮想マシン、テンプレートイメージの作成・利用、スナップショット作成など運用のために必要な機能が利用可能		
移行性	移行ツールでIP保持や変更での移行が可能		移行ツールでIP保持での移行が可能 IP変更は仮想マシン移行後、手動またはファミリー製品などを利用し移行可能
バックアップ	スナップショットやブロック差分を利用した他社バックアップ製品と連携したバックアップが可能	グループ化の単位でスナップショットをスケジュールに基づいて行い、リカバリポイントを管理するような高度な管理が製品の機能で可能	スナップショットでバックアップ管理、リストアが可能　スナップショットと他社製品を利用したバックアップやVMのクローンが可能
モニタリング	確認したいメトリック、指標を個別に選択し、ダッシュボード画面で確認可能		
可用性	フェイルオーバの機能を有し故障時に正常に動作することを確認		
基盤への適合性	移行経路の帯域制御、閉域環境での動作が可能		他社NW製品と連携し帯域制御が可能 閉域環境での動作が可能
システム無停止移行	可能	停止を伴う	停止を伴う
システム固有の制約	クラスタウェアはIP変更ができず停止を伴う（アンインストール・移行・再インストールが必要） RDM方式を採用しているシステムはストレージ装置での移行・バックアップリストアが必要（移行時、停止時間が長時間化する可能性）		
リスクへの対応	大きな影響なく移行対応可能		
運用性	VerUpや運用保守作業に応じた作り込みが必要	VerUp前にプリアップデート可能など、ノーコードで自動化可能	VerUpや運用保守作業に応じた作り込みが必要（ファミリー製品などで対応）
その他	ー	ー	ライセンス改定もありライセンス単価が安価

1. はじめに

1.1. 本資料の位置づけ

本資料は、令和 6 年度「共通基盤システムにおける調査研究」（以下、「本調査研究」という。）において実施した作業およびその成果の全体概要を取りまとめたものである。

第 2 章では、本調査研究が実施された背景および目的について示す。

第 3 章では、共通基盤システムにおける将来的なセキュリティ対策のあるべき姿を示す。

第 4 章では、共通基盤システムにおけるネットワークの通信傾向分析手法および最適化手法について示す。

第 5 章では、共通基盤システムに適した仮想化ソフトウェア比較検討結果およびシステム移行における影響調査結果を示す。

2. 本調査研究の背景・目的

2.1. 本調査研究の背景

警察庁では、令和５年度に「共通基盤システムのリプレースに関する調査研究」において、共通基盤システムにおけるハードウェア構成の最適化や共通機能の機能要件の見直し、ソフトウェア製品の選定等のコスト削減および業務プログラムの移行等について検討を行い、共通基盤システムの方針やあるべき姿に向けてロードマップを策定した。

これを踏まえて、次期共通基盤システムにおけるセキュリティ要件や、ネットワークの最適化、共通基盤システムに適した仮想化ソフトウェア製品選定等、将来的な共通基盤システムのあるべき姿を具体化して検討する必要がある。

本調査研究においては、将来的な共通基盤システムの在り方の観点から、以下の 3 項目を調査した。

1. 共通基盤システムにおける将来的なセキュリティ面のあるべき姿
2. 共通基盤システムにおけるネットワークの最適化
3. 共通基盤システムにおける仮想化ソフトウェアの比較検討

2.2. 本調査研究の目的

2.1 で記述した調査項目について、本調査に対する目的を示す。

1. 共通基盤システムにおける将来的なセキュリティ面のあるべき姿

セキュリティを担保しつつ、警察職員の働き方改革に資する指針を明確にすることを目的とする。将来的な運用業務を見据えたアプリケーション開発の全体像およびゼロトラストモデルにおけるセキュリティ対策の検討を行う。また、現行の LAN 間データ交換装置の課題である拡張性を考慮し、実機検証を踏まえた製品検討を行う。

2. 共通基盤システムにおけるネットワークの最適化

共通基盤システムにおける将来的なネットワーク管理の最適化に向けた方針整理を目的とする。現行共通基盤における業務毎の通信状況の把握手法の検討、将来的なトラフィック増加に伴うネットワーク輻輳に対する適切な QoS 設計を行う。また、大規模基盤における運用性・セキュリティ性を考慮した最適な IP アドレス管理手法の検討を行う。

3. 共通基盤システムにおける仮想化ソフトウェアの比較検討

次期共通基盤システムに適した仮想化ソフトウェア選定のための情報収集および整理を目的とする。システム規模および警察庁の特性、市場動向を踏まえ、複数の観点から仮想化ソフトウェア製品の調査を行う。また、実機検証によるシステム移行の影響調査を行い、各製品の比較・評価を行う。

3. 共通基盤システムにおける将来的なセキュリティ面のあるべき姿

3.1. 在宅勤務および執務室でのアプリケーション開発

現行共通基盤におけるアプリケーション開発工程について、開発工程毎に対応する主要なタスクと取り扱う情報を整理したうえで、次期共通基盤システムにおけるアプリケーション開発において、在宅環境および執務室から作業可能な範囲を検討した。

また、端末および端末周辺・通信経路・接続先環境における脅威の観点として、マルウェア・紛失や盗難・重要情報の窃取・不正アクセスについてのセキュリティリスクを考慮し、セキュリティ対策を整理したうえで開発のあり方を検討した。同様に、入口・出口・内部でのセキュリティ脅威の侵入経路について考慮し、対策を検討した。

3.1.1. 次期共通基盤システムにおけるアプリケーション開発工程

現行共通基盤システムのアプリケーション開発は、外部委託ベンダでの作業が主となっており、基本的に警察庁データセンタ内の開発端末で作業を実施する。今後の共通基盤システムでの自主開発を想定した場合、在宅環境および執務室から作業可能な範囲を広げることで、開発業務の働き方の柔軟性拡大や、警察全体での IT 人材の活用を可能にする。

図表 3-1「在宅環境および執務室から作業可能な範囲」

在宅環境および執務室から作業可能な範囲

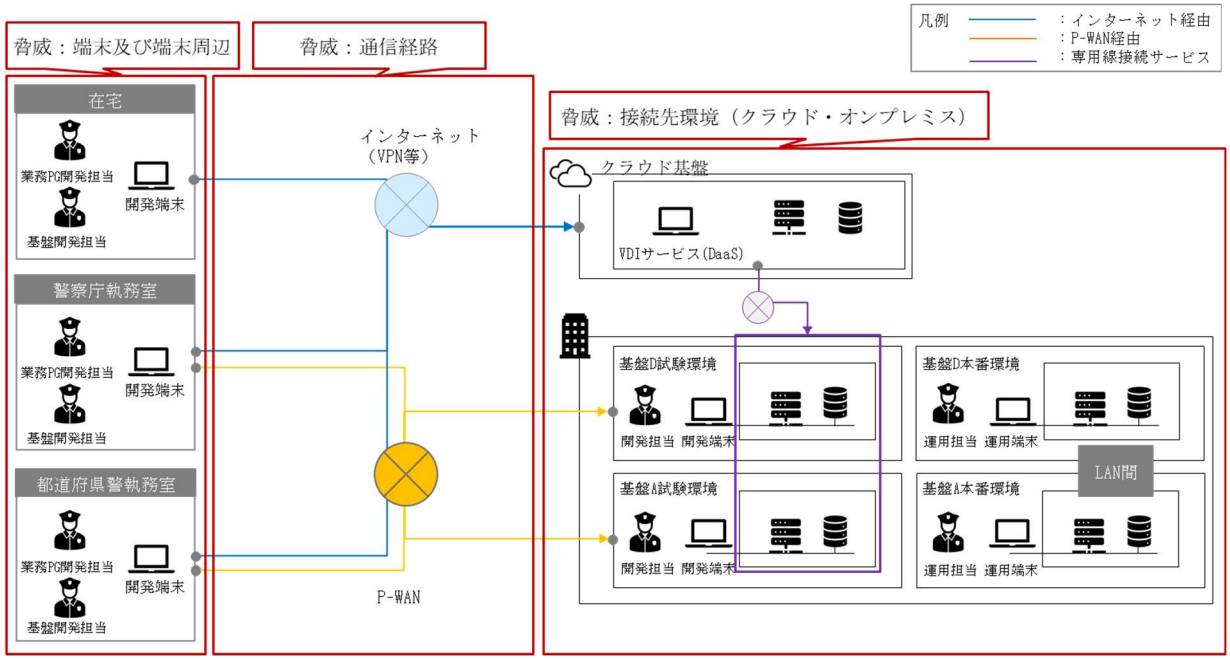
	企画・要件定義	概要・詳細設計	製造・単体テスト・内部結合テスト	外部結合テスト・総合テスト	受入テスト	移行・リリース
警察庁職員・都道府県警察職員（業務プログラム側）	業務要件の整理 要件定義書の作成	各種設計書作成 テスト計画書作成	コーディング テスト実施 不具合修正	テスト実施 不具合修正	警察要件への適合確認	移行作業 リリース作業
警察庁職員（基盤担当）	インフラ要件の整理 要件定義書の作成	各種設計書作成 テスト計画書作成 開発環境構築	試験環境・本番環境構築	試験実施支援	警察要件への適合確認	本番切り替え作業

3.1.2. 在宅環境および執務室からのアプリケーション開発におけるセキュリティリスク

在宅環境および執務室から接続先環境である開発環境へのアクセスについて、脅威の対象として大きく分けると、「端末および端末周辺」「通信経路」「接続先環境」の 3 つとなり、脅威の観点ごとに整理を実施した。

※「P-WAN」は以降において「警察庁 WAN」または「警察庁 WAN システム」を表す。

図表 3-2「セキュリティリスク（イメージ）」



在宅勤務および執務室からのアプリケーション開発におけるセキュリティリスクとして、特に危惧されるのは情報漏洩である。脅威の対象として当てた 3 つの焦点「端末および端末周辺」「通信経路」「接続先環境」に対し、脅威の観点「マルウェア」、「紛失・盗難」、「重要情報の搾取」「不正アクセス」の 4 点に対し整理を実施した。

図表 3-3「端末および端末周辺における脅威」

脅威の観点	脅威の概要
マルウェア	セキュリティ対策ソフトの未導入・未更新によるマルウェア感染
	偽サイトへのアクセスによるマルウェア感染
	メールに添付された偽リンクやファイルへのアクセスによるマルウェア感染
	USB記憶デバイス経由によるマルウェア感染
紛失・盗難	端末の紛失・盗難
	紙媒体の紛失・盗難
	閉域網接続用ネットワークデバイスの紛失・盗難
重要情報の窃取	のぞき見による重要情報の窃取
	画面の撮影・スクリーンショットによる重要情報の窃取
不正アクセス	端末や自宅NW機器の設定不備による端末への不正アクセス
	公に認知されていない脆弱性を悪用した不正アクセス

図表 3-4「通信経路における脅威」

脅威の観点	脅威の概要
マルウェア	偽サイトへのアクセスによるマルウェア感染
重要情報の窃取	通信の傍受による重要情報の窃取
不正アクセス	なりすましによる不正アクセス

図表 3-5「接続先環境における脅威」

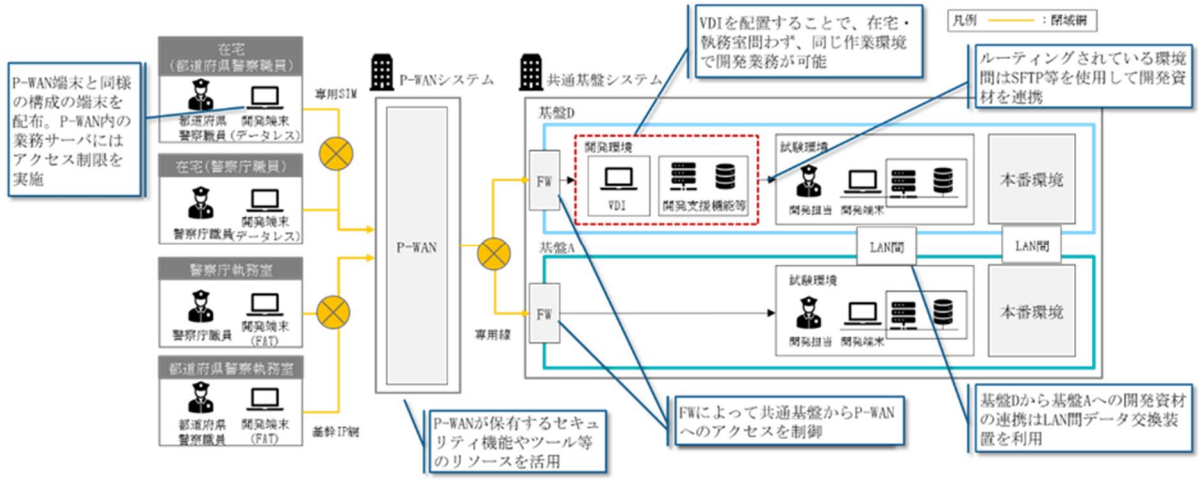
脅威の観点	脅威の概要
マルウェア	セキュリティパッチの更新漏れによるマルウェア感染
重要情報の窃取	通信の傍受による重要情報の窃取
	ファイルやデータの流出による重要情報の窃取
	ソースコードに含まれた重要情報の窃取
	意図しない情報の外部公開による重要情報の窃取（クラウド）
不正アクセス	認証情報の管理不備による不正アクセス
	アクセス制御の不備による不正アクセス
	システム設定の不備による不正アクセス
	ネットワーク内のラテラルムーブメント（横移動）による不正アクセス（侵入拡大）

次期共通基盤システムで在宅環境および執務室からアプリケーション開発を行うために、要件・リスク・対応案の整理を実施した。また、P-WAN における在宅勤務の要件を合わせて検討した結果、次期共通基盤システムのアプリケーション開発環境の前提条件として、以下 3 点とした。

- ✓ 在宅の端末にはデータを残さないこと
- ✓ P-WAN には、閉域網を使用してアクセスすること
- ✓ オープンネットワークにつながるシステムへアクセスする場合は VDI 経由を必須とすること

次期共通基盤システムにおける開発環境への接続経路は、P-WAN を経由して、開発環境の VDI にアクセスする方式を想定する。P-WAN を経由することで、既存の P-WAN リソースを活用し、リモートでのアプリケーション開発を実現することが可能である。また、開発環境を VDI 上に構築することで、在宅環境および執務室ともに同じ作業環境を利用して開発することが可能である。

図表 3-6「次期共通基盤システムで実現するアプリケーション開発環境」



なお、警察庁による自主開発の拡大、さらに都道府県警察を含めた開発者の急な増加の可能性も考慮し、クラウドを活用した段階的な開発環境の拡張を行う想定である。

具体的には、クラウド環境の仮想デスクトップ上で利用するアプリケーションはオンプレミスと

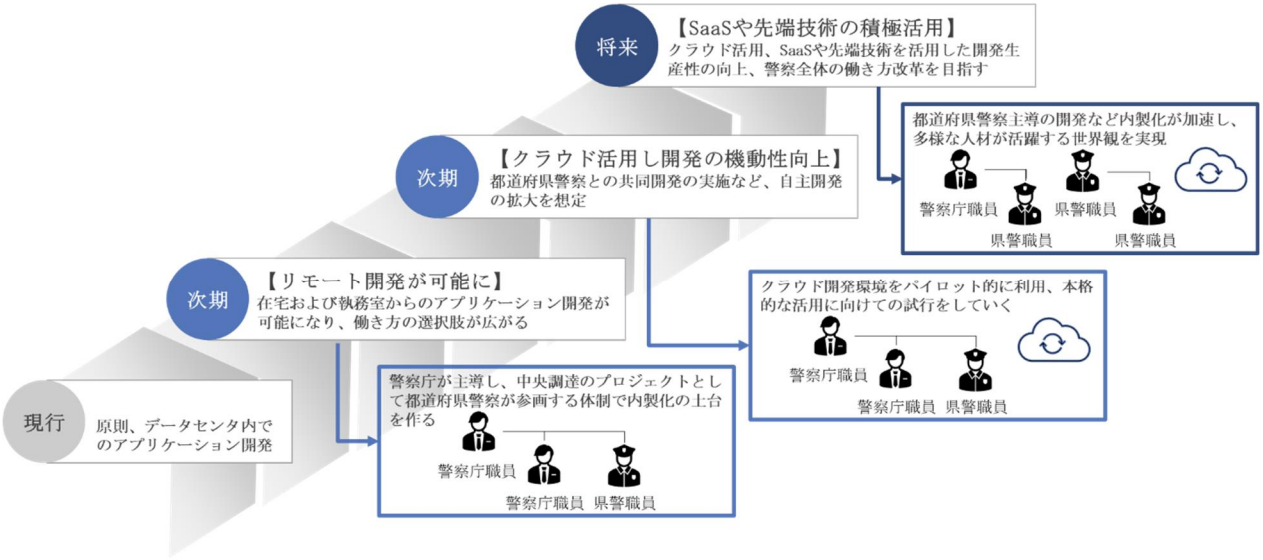
同様とし、認証や開発業務で必要なサーバは原則オンプレミス環境に構築したリソースを活用する想定である。ただし、開発支援ツールのサーバがリソース不足となった場合は、将来に向けた拡張がしやすいようにクラウド環境に拡張を行うものとする。

3.1.3. 将来的な警察のアプリケーション開発の姿

警察におけるアプリケーション開発として、次期共通基盤システムでは、警察庁が主幹となり都道府県警察と協働体制をとって自主開発を開始する。そして拡張可能な基盤としてクラウドを活用することで開発環境の提供に要する時間を短縮でき、開発の機動力向上が見込める。リスクが少ない開発環境からクラウド利用を開始することで、将来的なクラウド活用を見据える。

そして、将来的な共通基盤システムでは、警察庁だけでなく各都道府県警察も主導する体制で警察における自主開発が加速し、国民の声や政府動向に対して迅速に対応可能なシステム開発やサービス提供の実現を目指す。

図表 3-7「将来的な警察のアプリケーション開発の姿（イメージ）」



3.2. LAN 間データ交換装置に関する調査

本調査研究では、現行共通基盤システムにおいて、LAN 間データ交換装置が同時に複数ファイルの転送があった場合に負荷分散が難しい点について、コスト面・装置の仕様面および性能面での調査を行い、比較・実機検証のうえで最適な製品構成を検討した。

3.2.1. LAN 間データ交換装置に関する机上調査

現行の共通基盤システムでは、LAN 間データ交換装置は内部向け基盤と外部向け基盤間のデータ連携部分をネットワークから独立させて実現する装置と定義されている。LAN 間データ交換装置および、代替としてデータ転送のいずれかの方式でネットワークからの独立を実現できる製品について、市場調査し 16 製品のリストアップを行った結果、インターネットや TCP 通信等の手段が前提となる製品を除外し、以下のとおり机上調査対象は 4 製品とした。

図表 3-8「LAN 間データ交換装置および類似製品の市場動向」

No	製品名	分類	特徴	調査/除外
1	製品A	物理分離	ネットワーク分離環境で安全かつ効率的なデータ受け渡しを実現可能	調査対象
2	製品B	物理分離	ネットワークを分離し、エアギャップ（物理遮断技術）による連接技術で、情報漏えいを防止するとともに利便性を確保	調査対象
3	製品C	論理分離	ネットワーク分離環境で「自分から自分」へのファイル受け渡しをシンプルかつ安全に行うことが可能	調査対象
4	製品D	論理分離	ネットワーク分離における安全なファイル共有が可能	調査対象

机上調査対象である 4 製品に対し、共通基盤システムで求められる要件や現行製品の特徴を踏まえ、警察庁が重視する観点をセキュリティ・データ転送性能・スケーラビリティとして比較観点を整理した。これらの比較観点を踏まえ、比較調査を実施した結果は以下のとおりである。将来的な採用可能性を考慮し、分離方式として物理分離型、論理分離型の各 1 製品を選出した。

図表 3-9「LAN 間データ交換装置の机上調査・比較」

比較観点	比較	製品名			
	機能項目	製品A	製品B	製品C	製品D
セキュリティ	片方向・データ転送機能	○	○	○	○
	認証・認可機能	○	○	○	○
	ログ出力	○	○	○	○
	自動削除	○	○	定期削除を設定	定期削除を設定
	ファイル無害化	○OP	○	○OP	○OP
データ転送性能	データ転送速度	25MB/Sec(USB3.0)	1.4MB/Sec	非公開	非公開
	データ収集間隔(最小値)	10秒	60秒	10秒	60秒
	データサイズ(最大)	15GB～	20GB	1TB未満	2GB
	同時接続・並列転送	○	○	○	○
スケーラビリティ	拡張性	○	○	△実機検証で確認	×
	分離方式(物理・論理)	物理分離	物理分離	論理分離	論理分離
	オンプレミス/クラウド	オンプレミス	オンプレミス	オンプレミス	オンプレミス

3.2.2. LAN 間データ交換装置の実機検証

LAN 間データ交換装置において、実機検証を行う際の検証項目を整理した。まずセキュリティの確保ができることを実機で検証するための検証項目は以下のとおりである。

図表 3-10「実機検証項目-セキュリティ」

重視する観点	機能例	概要	確認内容
片方向へのデータ転送能力	ネットワーク上ファイルの一方向のみのデータ転送	端末上から参照できるファイルサーバ上のファイルを転送できるか	送信側、受信側の両方でファイルサーバ参照ができること 不要な参照を制御可能ができること
	転送可能時間の指定	転送可能な日、時間帯など制限をかけることができるか	日時、時間帯をポリシー制御可能ができること
	逆方向へのデータ転送阻止	論理設定変更によるファイル送受を逆方向から実施できないようになっているか	逆方向のファイル転送は物理変更がしないとできないこと
認証・認可機能	特定利用者のみの許可	転送した利用者の特定ができるようになっているか	転送の利用者を特定できること 転送の認可処理ができること
	特定ファイルの転送許可・不可設定	転送可能なファイル種別を指定しフィルタリングできるか	ファイル種別の許可不許可ができること
ログ出力	送受ログの内容	いつ・誰が・何のファイルをといった監査に必要な情報が送受ログにあるか	送受ログからいつ・誰が・何のファイルなどの情報が確認できること
	ログの可視性	可視性を持ったログが出力されるか	送受ログの形式が一般的なものであること 抽出、ソートが可能なフォーマットで生成されていること
	ログローテーション	長期保存や、ログの保存漏れがないようにログローテーションを設定可能か	保存期間、ログローテーション機能があること

同様に、データ転送性能・スケーラビリティの確保を実機で確認するための検証項目、また利用者が違和感なく利用できるかを実機で確認するための検証項目は以下のとおりである。

図表 3-11「実機検証項目-データ転送性能・スケーラビリティ・利用者利便性」

重視する観点	機能例	概要	確認内容
データ転送性能	データ転送速度	ネットワーク環境下でパスを増やすと転送スループットが増えるか	データ交換機器を複数セットおいて、同時転送が可能か確認する。
	データサイズ・形式依存の排除	大容量ファイルや特定のデータ形式により転送パスに偏りが生じないか	同じ容量の異なるファイル形式で転送を行い、転送速度に変化はないか 容量の異なるファイルで転送速度の差がないか
	同時接続・並列転送能力	同時に複数の接続や転送を安全・効率的に行えるか	同時転送でファイルはロックされ、同じファイルを取り合うことはないか
スケーラビリティ	拡張性	並列構成への拡張（スケールアウト）が容易にできるか	単一の場合と複数セットする場合で異なる追加設定があるか 追加が容易にできるか
	可用性	エラー・障害時のデータ転送の再開が可能か	エラーを起こし、速やかに復旧（データ転送の再開）が可能か
利用者利便性	同一端末からの複数データ交換	同一端末から複数のデータ交換をした場合に、複数パスに自動で振り分けられるか	自動振り分けできるか
	複数端末からの複数データ交換	複数端末からデータ交換をした場合に、複数パスに自動で振り分けられるか	自動振り分けできるか
	制限事項の確認	データ転送パスが単式の場合と複式の場合で利用上の制限事項がないか	単一の場合と複数セットの制限事項の整理

これらの検証項目を踏まえ、机上調査で選定した 2 製品を対象に、実機検証を実施した。セキュリティ・データ転送性能・スケーラビリティ・利用者利便性について、確認した結果は以下のとおりである。

図表 3-12「LAN 間データ交換装置の実機検証結果・比較」

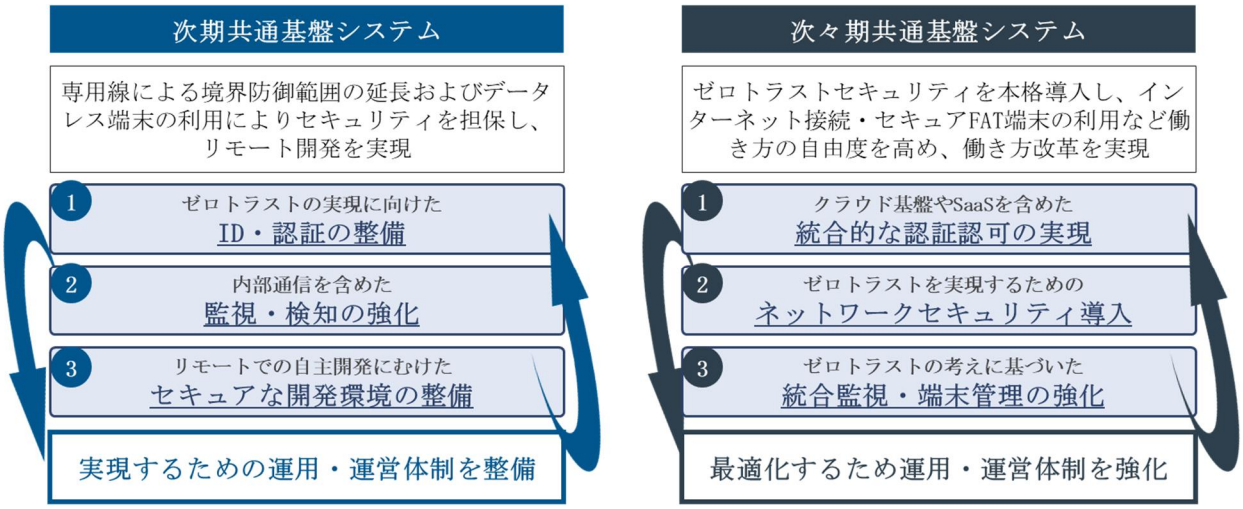
比較観点	比較		製品名	
	機能項目		製品①（物理分離型製品）	製品②（論理分離型製品）
セキュリティ	片方向・データ転送機能	共通	逆方向への転送を防ぐ仕組みを有していることを確認	
		転送可能時間の指定	転送可能時間の指定可	特定日時の指定は不可
	認証・認可機能	共通	利用者の制限、ファイルの転送許可・不可の設定があることを確認	
	ログ出力	共通	いつ・誰が・何のファイルを転送したかログが残ることを確認	
		ログローテーション	PowerShell等作り込みが必要	固定で1日1回ローテーション可能
	ファイル無害化機能	ファイル無害化	ファイル無害化はOP対応で可	
		アンチウィルス	アンチウィルスは送信端末に別途導入が必要	アンチウィルスはOP対応で可
データ転送性能	データ収集間隔	最小設定値	1秒(設定可)	10秒
	データ転送速度(単体)	転送対象 100MB×10ファイル	105秒 実測値：9.52MB/秒(USB2.0) 理論値：25MB/秒(USB3.0) ※1	25秒 40MB/秒(GbE)
	同時接続・並列転送	全般	同時接続・並列転送 可	同時接続・並列転送 不可
拡張容易性	スケールアウト	全般	○可能 柔軟に構成が可能	△制限あり ファイルサーバ(端末)を両端に1対1で配置が必要
利用者利便性	複数データ交換	同一端末		
		複数端末		
	制限事項の確認	制限事項		

※1 今回、実機検証機の都合上、USB2.0 機器にて実測を行ったが、実際に利用する場合は USB3.0 機器を想定しており、その場合の転送性能は向上する想定であるため理論値も記載

3.3. ゼロトラストセキュリティの導入計画検討

柔軟な働き方の実現のためには、利用する端末や働く場所などの自由度を高めることが重要な一方で、自由度が高まった中でもセキュリティレベルを担保するための対策を検討する必要がある。これまでの境界防御の考え方から、境界に脅威が侵入する前提での対策が必要となるため、次期および次々期の共通基盤システムにおいて、セキュリティ対策の強化とセキュリティ運用の高度化を段階的に実現していく。

図表 3-13「ゼロトラストセキュリティ導入に向けたステップ」



3.3.1. 次期および次々期の共通基盤システムで優先すべきセキュリティ対策

ゼロトラストセキュリティは、「全ての通信を保護し、セッション単位で認証を実施する」「認証は複数のインプットを基に動的ポリシーによる認証を実施する」を設計指針の主旨としている。

次期共通基盤システムでは境界防御を維持しつつ、エンドポイントや ID アクセス管理に重点を置き対策を実施していく。また、監視ポイントの増加に備え、運用・運営の体制を整備しつつ、段階的にセキュリティ運用の自動化を進めていくことが必要である。

次々期共通基盤システムでは、選択可能な働き方実現のためのセキュリティ担保として、外部および内部脅威のリスクを考慮し、優先度の再設定を実施した。

今後、共通基盤システムの利用者の増大や、監視ポイントの増加に合わせて、セキュリティ運用の高度化が必須となる。その実現には、セキュリティ対策だけでなく共通基盤システムにおける CSIRT/SOC といったセキュリティ専門チームの体制整備および拡充といった運用体制の強化が重要となる。

図表 3-14「セキュリティ対策強化の優先度についての考え方」

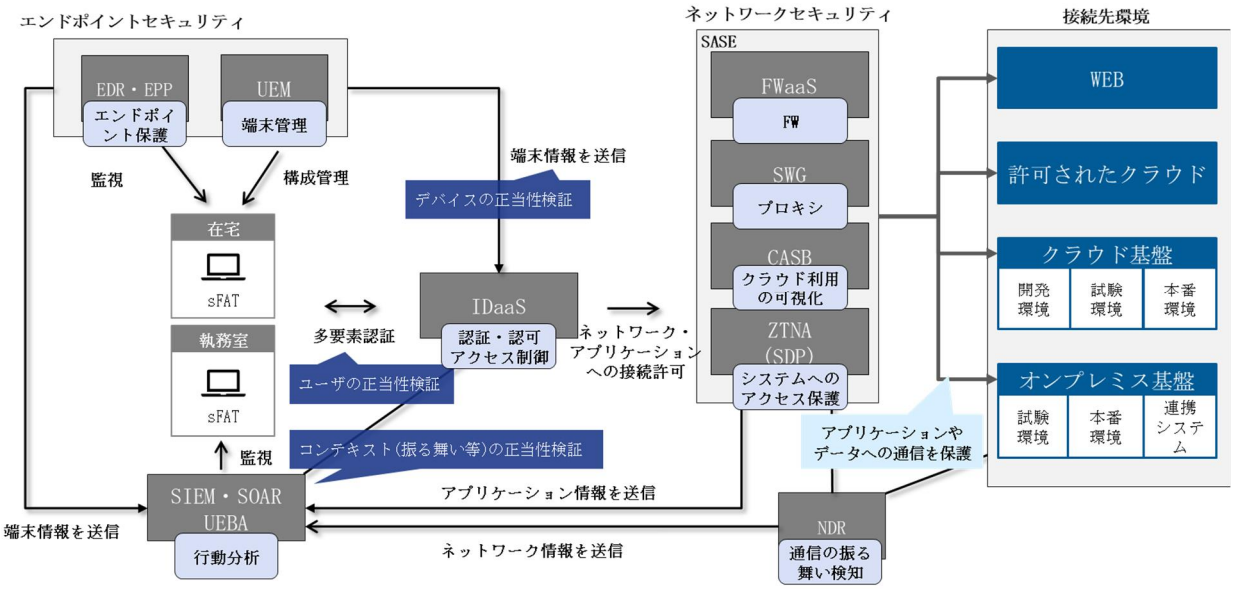
カテゴリ	次期共通基盤システム		次々期共通基盤システム	
	優先度	理由	優先度	理由
エンドポイント セキュリティ	高	マルウェア・ランサムウェアなどのエンドポイントへのリスク対策としてEDRを中心とした振る舞い検知が必要なため	最高	インターネット接続によるエンドポイントへの脅威リスクが増加する想定、EDR(XDR)を中心とした振る舞い検知など総合的な対策を実施する必要があり、ゼロトラストセキュリティ環境下でのアクセス可否判断の中核を担うため
端末管理	中	執務室から持ち出ししない、またはP-WAN専用線利用を前提とした境界内での利用を想定しているため	高	ゼロトラストセキュリティ環境下では「端末の安全性」を常に評価し、リスクの高い端末からのアクセスを制限する設計が必要となるため
ネットワーク セキュリティ	中	現行でもFW/IPS等を導入済みで境界防御を維持するが、内部セグメンテーション強化や振る舞い検知など、運用負荷を考慮しつつ組合せおよび段階的な取り組みにより強化をしていくことが望ましいため	最高	ゼロトラストセキュリティ環境下では「ネットワークを信用しない」前提として、マイクロセグメンテーションやSASEなどのネットワークセキュリティの強化、また振る舞い検知による対策が優先して必要なため
サーバセキュリティ	中	EDRを中心とした振る舞い検知の対策は実施しつつ、現行の境界防御を維持するため	高	オンプレミス環境としての境界防御は維持しつつ、EDRを中心とした振る舞い検知の対策は必要なため
クラウドセキュリティ	中	次期でのクラウド活用は、閉域環境内かつ開発環境としての利用想定のため（境界内としてサーバセキュリティと同様）	最高	本番環境としてクラウドを活用想定、かつパブリッククラウドの場合はクラウド特有の対策が優先して必要なため ※プライベートクラウドの場合、サーバセキュリティと同等（高）の想定
データセキュリティ	中	EDRを中心とした振る舞い検知の対策は実施しつつ、現行の境界防御を維持するため	最高	インターネット接続、セキュアFAT端末利用を想定し、データが移動する想定とした場合、漏洩対策・権限管理・暗号化の強化が優先して必要であるため
IDアクセス管理	高	境界内におけるIDのライフサイクル管理、アクセス制御は重要かつ次々期におけるセキュリティ対策の根幹となるため	最高	ゼロトラストセキュリティ環境下においてIDの統合管理、認証認可の整備が根幹となり、優先して対策が必要なため
ログ収集・管理	高	内部通信も含む統合ログ基盤整備により、リアルタイム監視やインシデント分析の実施が推奨されるため	最高	クラウド/SaaSを含めた横断的なログ収集を前提とした統合ログ基盤の整備が継続して必要なため
運用自動化	中	監視対象の拡大および統合ログ基盤の整備が優先、セキュリティに関する運用・運営体制の整備とともにSOAR等を用いたセキュリティ運用の自動化を段階的に進めていくことが推奨されるため	高	ゼロトラストセキュリティ環境下ではポリシーの動的変更の頻度が増え、かつ監視ポイントの増加を考慮すると、運用・運営体制の整備とともに自動化は必要なため

3.3.2. 将来的な共通基盤システムにおけるセキュリティ対策のあるべき姿

将来的な共通基盤システムでは、セキュア FAT 端末の利用やインターネット経由でのアクセスなど、働き方の選択肢が広がる一方で脅威については増加が考えられる。また、近年更に高度化しているサイバー攻撃への対策の検討も必要である。

具体的には、次々期以降での共通基盤システムは、ネットワークセキュリティ、データセキュリティの強化が更に重要となる。そして、適切な認証を受けた端末とそのユーザだけが、許可されたデータやアプリケーションにアクセス可能となる「ゼロトラストセキュリティ」の実現が必要不可欠となる。

図表 3-15「将来的な共通基盤システムにおけるセキュリティ対策のあるべき姿（イメージ）」



4. 共通基盤におけるネットワークの最適化

4.1. 業務毎に通信傾向を分析し最適な通信帯域を把握

ネットワークの可視化／通信傾向の分析には、SNMP やフロー情報を活用する方法がある。現行システムの通信分析の結果、フロー情報を用いることで業務単位での通信状況を把握でき、バーストトラフィックを発生させる業務サーバの特定など、通信トラブルの原因究明に有効であると確認した。また、頻繁に通信状況を把握する必要がある業務については、IP アドレスやネットワークアドレスをグループ化し、フロー情報を用いた解析装置（コレクタ）に登録することで、通信帯域の使用状況や負荷の大きい機器を容易に特定できる。

フロー情報を取得するには、解析対象のネットワーク機器からデータを収集する必要がある。ネットワーク構成やコスト面を考慮し、各コア L3 スイッチの WAN 側を最適なフロー情報の推奨取得箇所とする。コア L3 スイッチのフロー情報を利用して、WAN 経由の通信や WAN 回線輻輳時の原因分析が可能となる。WAN 通信は LAN 間通信より通信遅延が発生しやすいため、WAN 通信の解析重要度が高いと判断した。

図表 4-1「フローの取得箇所案」

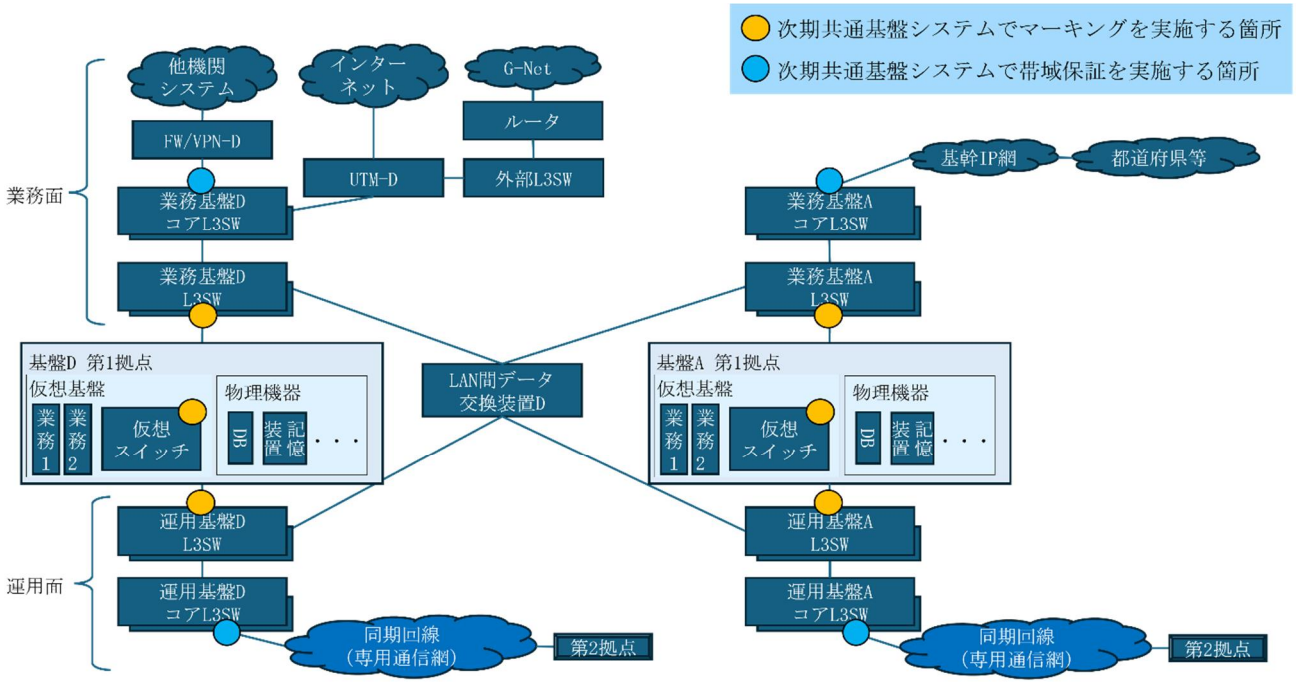
	主な調査目的	取得場所	利点	課題
推奨案	WAN 回線のバースト原因	WAN 接続用スイッチ（各コア L3SW）	回線を圧迫している対象の IP アドレスや通信内容(TCP/UDP のポート番号など）を特定でき、迅速な解析が可能	WAN 通信に特化した分析となるため、LAN 内の詳細な通信状況は把握しにくい
	業務単位の輻輳状況	エッジスイッチ（各基盤 L3SW、仮想スイッチ）	WAN に影響を与えていないが、負荷の大きい通信を特定し、業務単位での影響分析が可能	取得対象が増えるため、管理負担や機器負荷が高まり、コストが増加する可能性がある

4.2. 適切な QoS 設計および動的にトラフィックの優先度を変更する手法

将来的なトラフィック増加に伴いネットワークの輻輳が発生した場合、重要な通信の品質確保が困難となる可能性が懸念される。この課題に対処するため、パケットのマーキングや帯域保証を含む QoS 設計について検討した。

次図のとおり、マーキング、帯域保証の実装を推奨する。

図表 4-2「次期基盤における QoS 全体像」



重要度の高い通信を適切に識別するため、エッジ相当スイッチのダウンリンクポートおよび仮想スイッチにおいてパケットのマーキングを実施する。また、識別された重要通信の安定性を確保するため、コア相当スイッチのアップリンクポートにおいて帯域保証を適用し、一定の帯域を割り当てることで、輻輳時における影響を最小限に抑える。これにより、ネットワーク全体の品質向上と、重要通信の確実な保護が可能となる。

さらに、輻輳時におけるネットワークの安定性を向上させるため、QoS 補助機能として動的にパケットの優先度を制御する機能について検討を行った。

以下の機能を搭載する機器の導入を推奨する。

図表 4-3「QoS 補助機能」

機能名	動作
バッファ割り当て自動調整機能	必要に応じて追加のバッファを動的に割り当て、パケットドロップの発生を抑制し、安定した通信を維持することが可能となる。
WRED (Weighted Random Early Detection)	バッファが許容量に達する前に、優先度に応じたパケットドロップを段階的に実施する。優先度ごとに閾値が設定されており、バッファの使用率が上昇すると優先度の低い通信から順次破棄されるため、重要な通信への影響を最小限に抑えることが可能となる。

4.3. IP アドレスに係るリソース管理について管理手法、割り当てルールの提示

大規模な基盤の IP アドレスリソースをファイルベースで管理する場合、データの整合性の維持や情報アクセス管理において、大きな運用負荷が伴う。そのようなケースでは、「IPAM（ IP Address Management)」といった概念のシステムを導入することで、以下の点を実現し、運用性およびセキュリティ性を向上させることができる。

- 利用していない/利用しているアドレス空間を容易に確認できる仕組み
- 管理対象のオブジェクト（サブネットなど）ごとに ReadOnly や ReadWrite などのアクセス権限制御
- 管理情報変更に関するイベントの自動ログ記録
- 管理情報変更時の承認フローの仕組み
- 単一コンソールからの一元管理

次期基盤では IPAM を導入し、以下のポリシーで IP アドレスの割り当てや棚卸の運用をすることを推奨案とした。

- 全基盤の IP アドレスを IPAM で一元管理する。ファイルでの管理は原則行わない。
- IPAM の利用ユーザを定義する。不要なユーザは登録しない。
- ネットワークごとにユーザ権限（Read/Write/閲覧不可）を定義する。
- 設定変更は承認制とし、設定変更内容のチェックのフローを導入する。

IP アドレスリソース管理において、IP アドレスとホスト名のマッピング手法も検討する必要がある。現行基盤のホスト名と IP アドレスを紐づける名前解決の仕組みについて、基盤内部の通信においては Hosts ファイルを用いた名前解決を利用している。基盤の拡張や変更が多く発生する場合、Hosts ファイル運用のメリットより DNS 運用のメリットの方が大きくなるため、次期共通基盤システムの内部通信のホスト・IP アドレスの名前解決の仕組みは DNS を用いた方式を推奨
案とした。

DNS 運用の主なメリットは以下となる。

- 名前解決参照先を一元管理可能であるため、管理や作業負荷が軽減される。
- 各ホストの変更処理が発生しなくなるため、変更作業時のトラブル発生が起きにくくなる。

現行基盤の内部通信の名前解決パターンについて調査し、DNS 運用の方式を採用しても問題ないことを確認した。

5. 共通基盤システムにおける仮想化ソフトウェアの比較検討

5.1. 仮想化ソフトウェアの市場動向調査

仮想化ソフトウェアについて、広く市場における 14 製品の情報収集を行い、警察庁の要件・規模を踏まえ、ノックアウトとなる 10 製品について除外した。

具体的には以下の観点でノックアウトファクターとなりうる製品について除外した。

- ✓ 対応範囲（サーバ仮想化/デスクトップ仮想化）
- ✓ 対応 OS（Linux/Windows）
- ✓ 機能充足性
- ✓ 保守サポート
- ✓ 実績
- ✓ 企業体力

机上調査対象の 4 製品について、仮想化アセスメントを実施し、詳細比較を行った。警察庁要件を踏まえた仮想化基盤としての適性度を減点方式で評価し、評価結果をサマリとして整理した。結果は以下のとおりである。

図表 5-1「仮想化アセスメント机上評価・比較」

候補	製品名	適性度	評価概要
1	製品A	★★★★☆ (4.5)	第一、第二サイトの仮想化基盤や、ネットワーク基盤を同製品で運用しているため、次期の仮想マシンの払い出し、セキュリティ、及びそれらの管理を一元的に行い続けるためには同製品が運用としては最適である。また、次期共通基盤への移行性も高い。 ただし、同製品がコア課金となるため、割当再検討や価格低減策が行われない場合、高額となる可能性がある。
2	製品B	★★★★☆ (4.0)	3Tierではなく HCI構成となりホスト上のオーバーヘッドが多少あるものの、大規模仮想基盤の実績も多く、サポートの信頼も高い。また日本語ナレッジも多い。 一方、サービスポータルの実績もあるが、現行のフローと近いイメージで実現できるかは検討が必要。性能面は、クラスタを組むノード数、さばけるIOPS数などもツールでサイジング可能。
3	製品C	★★★☆☆ (3.0)	同製品の採用によりコストメリットが出てくる可能性がある。アーキテクチャが同製品機能を使ったIaaS基盤に変わるため、仮想ネットワークやHA等の要件を十分に満たすことができるかは検証が必要。また、ミドルウェアも利用製品の動作環境を確認する必要がある。
4	製品D	★★☆☆☆ (2.5)	警察庁ではLinux OSが多く使われているものの、同製品は大規模LinuxOS集約の事例が少ない。一部の機能や3rd Party製品を活用・カスタマイズし、仮想マシンの払い出しポータルを構成している大規模仮想基盤の事例はあるが、ゲストの大半がWindows ServerやWindows 10,11 である場合が多い。

候補 1～3 の 3 製品を実機検証対象とした。

5.2. システム移行における仮想化ソフトウェアの影響調査

仮想化ソフトウェアの移行における課題の洗い出しを行い、移行方式および移行主幹（自主/委託）を考慮した移行方式の整理を行った。移行方式においては、仮想化ソフトウェア 3 製品それぞれで複数パターンを検討し、一般的に想定される環境上の制約、警察庁の要件を考慮したうえで、もっとも現実的な 2 パターンまたは 3 パターンを実機検証で行う移行方式とした。

仮想化ソフトウェア 3 製品について、警察庁の課題および要件に沿って検証観点の整理を行った。

重視する観点は以下のとおりである。

図表 5-2「仮想化ソフトウェアにおける移行検証観点」

重視する観点	機能例	概要
基盤への適合性	利用する帯域・通信経路上の制御	通信経路上の転送帯域の制御が可能か
	セキュリティ上の制約確認	本機能導入による既存システムへの影響、セキュリティ上の制約がないか
システム無停止移行	最小の停止で行う移行	短時間停止の時間がどれぐらいか、移行ができるか
システム固有の試験	停止中の仮想マシンの移行	停止中の仮想マシンを移行させることができるか
	移行対象OSが新規ハードウェアで起動することの確認	OSが移行先の新規仮想ハードウェアで起動し問題ないか
	システムが利用する固有ハードウェアIDの移行可否確認	MACアドレス・システムボードのUUIDを変更なく移行が必要となるアプリケーションへの対応可能か
リスクへの対応	移行中の管理サーバ/仮想ソフトウェア/移行ソフトウェア再起動	基盤単体障害における移行影響があるか、どういった対処となるか
	移行中のOS再起動（利用者によるもの）	システム利用者の操作による移行影響があるか
	移行後に不具合が出た場合の切り戻し	想定外の事象による移行中止において、サービス再開することが可能か

また、実機検証および運用を考慮したデモを実施した。他仮想化ソフトウェアへの移行についても専用ツールで移行が可能なことを実機検証デモにおいて警察庁職員に参加いただき確認を行った。

なお、既存仮想環境から他仮想化ソフトウェア環境への移行後に既存のシステム運用からの変更点や変更に伴って必要となる作業を洗い出した。具体的には以下のとおりである。

図表 5-3「他仮想化ソフトウェアへの移行における仮想基盤としての運用で重視する観点」

重視する観点	機能例	概要
リソース構成（仮想環境）管理	仮想環境作成(Linux/Windows)	テンプレートから仮想環境を作成できることを確認する
	仮想環境コンソールアクセス機能	CLI、GUI等を通じて作成された仮想環境のコンソール機能があるか確認
	仮想環境(Linux/Windows)への接続	リモート接続(SSH etc)でOSへ接続ができることを確認する
	仮想環境テンプレートイメージの登録/削除機能を確認する	仮想環境を作成するためのテンプレートイメージを作成・管理できるかを確認する
	仮想環境タイプの定義済み機能	タスクサイズや目的毎に仮想環境のリソースサイズ（CPU、メモリ、ディスク）を事前に定義できるかを確認する
	仮想環境のリソース追加	仮想環境再起動を必要とせずにリソース設定ができること、適用には再起動が必要であることを確認する(vCPUソケット、メモリ、ディスク追加、NIC追加等)
	仮想環境の一時停止と解除機能	未使用の仮想環境を一時停止し、アクティブな仮想環境がリソースを最大限活用できるか確認する
	仮想環境スナップショット作成機能	現在の状態のスナップショット作成及びリストアができることを確認する
	仮想環境のクローン作成	既存の仮想環境からクローンを作成できることを確認する
ボリューム / バックアップ管理	テンプレートイメージとして作成する機能	作成した仮想環境をテンプレートイメージ として再利用できるか確認する
	スナップショットから新しい仮想環境を作成する機能	障害発生時にデータを回復するために、 作成されたスナップショットを使用して新しい仮想環境を作成できるか確認する
モニタリング	環境に関する詳細モニタリング機能	管理画面で各パフォーマンス指標に関す る情報モニタリング機能を確認する（CPU、 メモリ、ディスク、ネットワーク等）
可用性	仮想環境のホストフェイルオーバー機能	安定したサービスを提供するためのホスト障害時に仮想環境のフェイルオーバー機能があることを確認する

既存の仮想化ソフトウェアにおいて、異なるバージョン間における移行検証を実施し、バージョンが異なる仮想化ソフトウェア間で仮想マシンを無停止もしくは一時停止で移行可能であることを実機検証で実施した。

異なる仮想化ソフトウェア間の移行検証においても、2 製品を対象として、既存仮想化ソフトウェアから仮想マシンを一時停止で移行可能であることを確認した。また、既存の仮想化ソフトウェ

アから他仮想化ソフトウェア環境への移行後に運用性が確保できることを実機環境で検証した。

仮想化ソフトウェア 3 製品においての共通した課題として、クラスタウェアの利用による制約およびアプリケーションに対し物理ストレージとして見せる手法を用いた機能について制約があることがわかった。アプリケーションに対し物理ストレージとして見せる手法を用いた機能については、今後の移行を考慮すると、採用するべきではなく、今後も必要な場合は慎重に検討を行う必要がある。

なお、実機検証結果について、仮想化ソフトウェアごとに比較観点のポイントを整理した結果は以下のとおりである。

図表 5-4「仮想化ソフトウェアの実機検証結果・比較」

比較観点	製品名		
	製品①	製品②	製品③
全般	仮想マシン、テンプレートイメージの作成・利用、スナップショット作成など運用のために必要な機能が利用可能		
移行性	移行ツールでIP保持や変更での移行が可能		移行ツールでIP保持での移行が可能 IP変更は仮想マシン移行後、手動またはファミリー製品などを利用し移行可能
バックアップ	スナップショットやブロック差分を利用した他社バックアップ製品と連携したバックアップが可能	グループ化の単位でスナップショットをスケジュールに基づいて行い、リカバリポイントを管理するような高度な管理が製品の機能で可能	スナップショットでバックアップ管理、リストアが可能　スナップショットと他社製品を利用したバックアップやVMのクローンが可能
モニタリング	確認したいメトリック、指標を個別に選択し、ダッシュボード画面で確認可能		
可用性	フェイルオーバの機能を有し故障時に正常に動作することを確認		
基盤への適合性	移行経路の帯域制御、閉域環境での動作が可能		他社NW製品と連携し帯域制御が可能 閉域環境での動作が可能
システム無停止移行	可能	停止を伴う	停止を伴う
システム固有の制約	クラスタウェアはIP変更ができず停止を伴う（アンインストール・移行・再インストールが必要） RDM方式を採用しているシステムはストレージ装置での移行・バックアップリストアが必要（移行時、停止時間が長時間化する可能性）		
リスクへの対応	大きな影響なく移行対応可能		
運用性	VerUpや運用保守作業に応じた作り込みが必要	VerUp前にプリアップデート可能など、ノーコードで自動化可能	VerUpや運用保守作業に応じた作り込みが必要（ファミリー製品などで対応）
その他	ー	ー	ライセンス改定もありライセンス単価が安価

6. 提言

共通基盤システムの将来像として、先進技術を活用した業務高度化の継続的な推進が重要である。これを実現するためには、アジリティ向上を目指したマイクロサービス化等のアプリケーションレイヤの再検討、柔軟性および拡張性を考慮した基盤構成の検討が必要である。