令和７年度

警察情報システムの合理化・高度化に係る調査研究

調査研究報告書（概要版）

2026 年 3 月 19 日

株式会社三菱総合研究所

目　　次

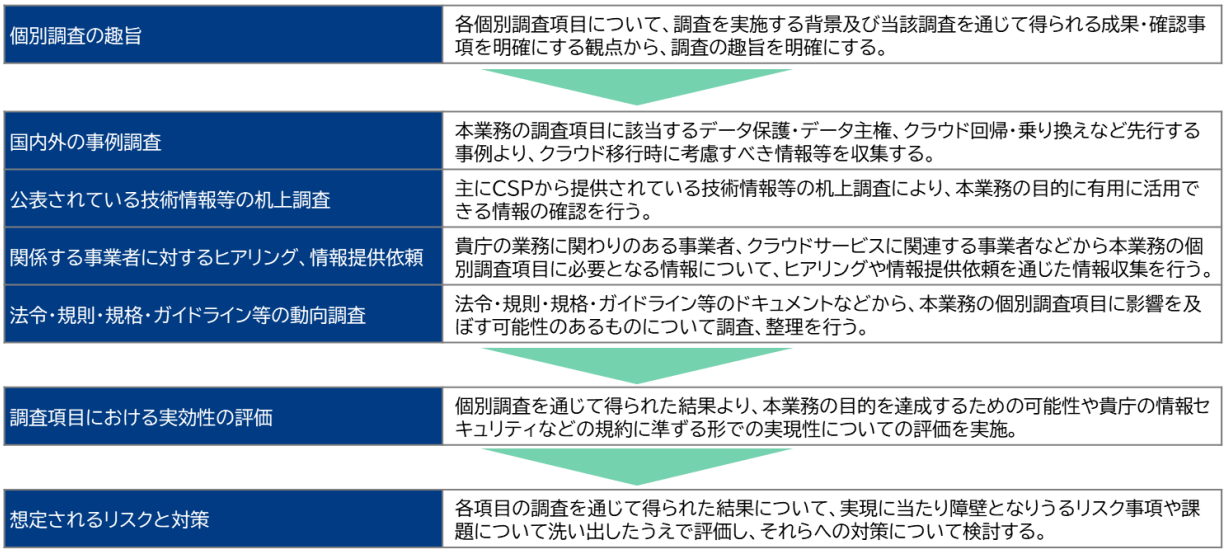
第 1 章　はじめに

1.1　本調査研究の目的

警察情報システムの合理化・高度化に係る調査研究（以下「本業務」という。）は、将来的な警察情報システムの最適化・運用負荷の軽減等を実現するために、現在オンプレミス環境にて整備・運用している警察情報システムのうち、特に基幹システムである警察共通基盤システムをクラウド環境へ移行する際の費用対効果、想定される技術・運用上の課題及び懸念事項について整理・分析を行い、今後の検討の基礎資料とすることを目的とする。

1.2　本調査研究の流れ

本業務の調査対象となる項目について、事例、技術情報、関係事業者等へのヒアリング・情報提供依頼等を通じて情報収集し、それらの情報を元に警察共通基盤システムの最適化に向けた評価・分析を図表 1.2-1 の流れで実施した。



図表 1.2-1　調査研究の流れ

1.3　用語について

本業務において使用する用語の解説を別紙に示す。

第 2 章　クラウドサービスの特徴

個別調査の前段として、本業務において利用するクラウドサービスの定義やクラウドサービスの形態について、以下のとおり整理する。

2.1　クラウドサービスの定義

本業務におけるクラウドサービスについては、NIST（米国国立標準技術研究所）による定義に基づいて、以下の 3 点に分類し、図示したものが図表 2.1-1 である。

- プライベートクラウド

  特定のユーザー専用に構築されたクラウド環境のこと

  自組織でリソースを管理・運用するオンプレミス型と、第三者の事業者がリソースを管理・運用するホスティング型で分類できる

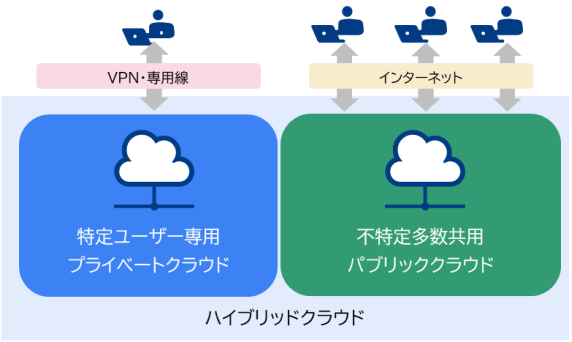
- パブリッククラウド

  インターネットを介して、不特定多数のユーザーが、CSP が用意したリソースを共有する形態のクラウド環境のこと

- ハイブリッドクラウド

  複数の異なる利用形態同士を組み合わせたクラウド環境のこと

	プライベートクラウド	パブリッククラウド	ハイブリッドクラウド
利用主体	特定ユーザー	不特定多数のユーザー	構成ごとに異なる
インフラ所有者	自社またはクラウド事業者	クラウド事業者	構成ごとに異なる



図表 2.1-1　クラウドサービスの種別

警察共通基盤システムのクラウド環境への移行の検討において、上記のクラウドサービスの他にオンプレミス環境も加えた。プライベートクラウドについては設置場所、所有により特徴も異なるところ、本業務においても区別して検討対象とした。図表 2.1-2 において、特徴的な項目については赤文字にて表記した。

凡例：○＝特性を満たす 、△＝限定的に特性を満たす、 ×＝特性を満たさない

	特性	詳細	オンプレミス	プライベートクラウド(オンプレミス型)	プライベートクラウド(ホスティング型)	パブリッククラウド
NISTが定義する特性	オンデマンドセルフサービス	人を介さずセルフでリソースを利用する	△ (設計次第)	△ (設計次第)	○	○
	幅広いネットワークアクセス	ネットワーク経由でコンピューティング能力を利用可能	×	○	○	○
	リソースの共有	論理的にテナント分離を行い、物理的なリソースを共有する	△ (自組織内)	○	○	○
	スピーディな拡張性	需要に応じてリソースをスケールアウト/スケールインさせる	△ (自組織リソースの上限まで)	△ (自組織リソースの上限まで)	○ (事業者側リソースの上限まで)	○ (世界規模のCSPは無制限に近い)
	サービスが計測可能	サービスの利用状況を可視化する	△ (設計次第)	△ (設計次第)	○	○
NIST定義外で追加	マネージドサービス等、CSP固有機能が活用可能		×	×	△ (事業者による)	○
	物理的なハードウェア設置場所		自組織内	自組織内	事業者側 (専用区画)	事業者側 (海外CSPを含むため、海外へのデータ移転可能性に留意)
	システム基盤の管理主体		自組織	自組織	事業者	事業者

図表 2.1-2　クラウドサービス種別ごとの特性

また、近年では NIST が定義する特性だけでは分類が難しいクラウドサービスも提供されており、代表的な２サービスとして以下の２点について検討対象とした

① パブリッククラウドのサービスを顧客側のオンプレミス環境に拡張して提供するサービス（本業務において『**オンプレミス拡張型クラウド**』と呼ぶ）

② パブリッククラウドのサービスをパートナー企業のクラウド環境に拡張、サービスをカスタマイズして提供するサービス（本業務において『**CSP 再提供型クラウド**』と呼ぶ）

それぞれの特性を図表 2.1-3 のとおり整理した。特徴的な項目については赤文字にて表記した。

凡例：〇＝特性を満たす 、△＝限定的に特性を満たす、 ×＝特性を満たさない

特性			①オンプレミス拡張型クラウド	②CSP再提供型クラウド
NISTが定義する特性	オンデマンドセルフサービス	人を介さずセルフでリソースを利用する	〇	〇
	幅広いネットワークアクセス	ネットワーク経由でコンピューティング能力を利用可能	〇	〇
	リソースの共有	論理的にテナント分離を行い、物理的なリソースを共有する	〇	〇
	スピーディな拡張性	需要に応じてリソースをスケールアウト/スケールインさせる	△ （自組織リソースの上限まで）	〇 （パートナー企業のクラウドサービスのリソースの上限まで）
	サービスが計測可能	サービスの利用状況を可視化する	〇	〇
NIST定義外で追加	マネージドサービス等、CSP固有機能が活用可能		△ （一部制限有）	△ （一部制限有）
	物理的なハードウェア設置場所		自組織内	事業者側 （国内SIer想定）
	システム基盤の管理主体		自組織だが、マネージドサービス機能等は事業者管理	事業者 （国内SIer想定）

図表 2.1-3 オンプレミス拡張型クラウドと CSP 再提供型クラウドの特性比較

2.2　クラウドサービスのメリット・デメリット

クラウドサービスの利用形態におけるメリット・デメリットについて、現行の警察共通基盤システムの運用環境でもあるオンプレミス環境も含めた比較を図表 2.2-1 に示す。それぞれについて、メリットを赤字、デメリットを青字、その他の特徴を黒字で表記した。

観点	パブリッククラウド	プライベートクラウド（ホスティング型）	オンプレミス
初期コスト	• ハードウェアが不要 • IaCによる環境構築の自動化が可能	• 専有環境が必要	• ハードウェアへの初期投資が必要
ランニングコスト	• 変動性が高い（従量課金） • 従量課金体系による、処理量が少ない時間帯のコスト低減 • マネージドサービス活用による運用保守費用削減の可能性有 • 個々のシステムをマルチクラウド構成化することによるコスト増大リスク	• 従量課金も部分的にあり得るが、専有環境の固定費が必要となることが多い • 事業者によりマネージドサービスが活用できれば、運用保守費削減の可能性有	• 安定性が高い（ハードウェアの償却コスト） • ピーク時の需要に合わせて設計するため、通年で安定稼働するシステムの場合はコストメリットが出やすい一方で、需要変動が大きいシステムの場合はハードウェアのコストが高額になるデメリットがある。
導入スピード	• 速い傾向（マネージドサービス、IaC、CI/CDの活用等）	• 中間（契約、構築、ネットワーク接続等が必要）	• 遅い傾向（調達や、設置・構築の物理的な作業発生）
技術革新対応力	• 新機能が随時追加される（分析やAIの機能等）	• 新機能が随時追加されるが、事業者による	• 新技術導入には個別対応が必要で、基盤更改時の対応となることが多い
柔軟性、拡張性	• 従量制課金により、短期間利用や、リソース増強が比較的容易 • オートスケーリングにより、負荷に応じて自動的にリソースを増強/削減することが可能	• パブリッククラウドほど柔軟ではなく、申請や作業が必要なケースがある	• 増強に物理的な増設が必要
可用性、災害復旧（DR）	• 複数拠点（データセンター）へのレプリケーションが可能	• 2拠点での構成も可能だが、事業者による	• 2拠点の構成を作る必要があり、費用や期間が必要
運用負荷	• マネージドサービス活用により低減可能	• ハードウェアについては事業者が運用するが、OS以上の運用は事業者のサービス設計による	• 全て自組織での運用が必要
障害対応	• クラウド側の障害はCSPの責任で対応 • 責任分界点を定義することが必要であり、CSP責任による障害の影響を被る可能性がある	• クラウド側の障害はCSPの責任で対応 • 責任分界点を定義することが必要であり、CSP責任による障害の影響を被る可能性がある	• 全て自組織で対応が必要 • 自組織外の責任範囲で障害事業が発生しない
監査/証跡	• ログ取得と保管のサービスが機能として提供される	• 事業者によっては機能があるが、保管等は設計が必要なケースもある	• ログの取得や保管について、自組織での設計が必要
ネットワーク遅延	• 距離や経路により遅延するリスク	• 距離や経路により遅延するリスク	• LAN内で完結しやすく、物理的に1か所に構築すれば遅延リスクは小さい
セキュリティ	• 責任共有モデルによりクラウド自体のセキュリティはCSPが責任を負う。マネージドサービスも活用することで、クラウド利用者はクラウドの設定、アプリケーション、運用といった部分のセキュリティ対策に注力できる。 • クラウドで提供されるサービスを活用することで、ゼロトラストセキュリティや暗号化といった対策を実装しやすい。	• 環境やネットワークを分離しやすく、統制が取りやすい • 左記のパブリッククラウドの特徴も該当し得るが、グローバルで事業展開する大手パブリッククラウドほど充実した機能が提供されるかは事業者による	• リソースを自組織で管理するため、統制が取りやすい • 自由度は高いが、自社での適切な設計と運用が必要
データ保護/主権	• 国内法以外の法令及び規制が適用されるリスク	• 国内に閉じて事業展開やDCを活用するCSPであれば国内法が適用されるが、国外の企業との資本関係や国外での事業展開に注意を要する	• 物理的に国内、自組織内で管理できる場合、国内法が適用される
ベンダーロックイン	• 特にマネージドサービスによりCSPにロックインされデータ移行性が担保されないリスク	• 事業者や構成に依存する	• 特定のハードウェア等に依存するリスクはあるが、汎用的な基盤や技術を採用すれば回避しやすい

図表 2.2-1　クラウドサービスの利用形態におけるメリット・デメリット

それぞれの利用形態における特徴を把握したうえで、クラウドサービスを選定することにより全体最適を図ることができると考えるため、この観点を踏まえた検討が必要となる。

第 3 章　警察共通基盤システムの現状

3.1　現行警察共通基盤システムの環境

現行の警察共通基盤システムは、オンプレミス環境でシステム基盤を整備し、その基盤上で個別業務プログラムの開発、運用を実施している。また、主系及び待機系のシステムをそれぞれ第一サイト及び第二サイトの遠隔地に配置し、災害時等においても業務継続を可能とするシステム構成としている。

過去の調査研究事業の報告なども踏まえ、警察共通基盤システムの最適化に向け、以下の事項の検討を実施する必要があると考える。

<u>クラウドサービスの利活用</u>

警察情報の機微性の高さから、警察情報システムは基本的にオンプレミス環境で運用されてきたが、各国の状況も参考にしつつ、機密レベルに応じたデータの保護・主権を確保した上で、クラウドサービスの利活用について検討する必要があるのではないか。

警察共通基盤システム上の機能・プログラムの見直し

警察共通基盤システムが提供する共通機能や、個別の業務プログラムで実現する機能等については、これまでも適宜見直しを行ってきているところ、更に中長期的な視点から見直しを図ることで、これまで以上にコスト・運用を最適化することができないか。

適切な非機能要件の設定

業務要件を担保するために導入された専用のハードウェアについて、現在の技術レベルを踏まえて見直したり、複数のシステムで共用するなど、共通基盤システム全体を俯瞰した上で更なる最適化ができないか。

維持コストの抑制

維持コストの更なる抑制ができないか。特に待機系は業務継続の観点から不可欠なものの、抜本的な構成の見直しを図ることで、業務継続の目的を維持したまま、コストの抑制ができるのではないか。

以上のような観点から、警察共通基盤システムの最適化に向けて、クラウドサービスの導入の実現可能性について、個別調査を実施した。

第 4 章　個別調査

警察共通基盤システムの課題の解決には多様な手法が考えられるところ、本業務では特にクラウドサービスの導入によって解決できる課題に焦点をおくこととし、本章では、クラウドサービスの導入の前後に生じる課題や検討を要する事項を個別調査した結果を述べる。

4.1　クラウドにおけるデータ保護・データ主権に関する調査

警察共通基盤システムにおいて取り扱われるデータのうち、特に機微性の高い情報については、喪失・消失を防止するための措置に加え、不正な取得や利用を防ぐ観点から、データの適切な保護及び主権の確保が求められる。本調査では、クラウドサービスの導入可能性を検討するにあたり、取り扱うデータの適切な保護及び主権の確保を前提として、以下の観点から調査を実施した。

1. データ保護及びデータ主権の観点から、各国におけるデータ取扱いに関する政策、基準、法令等の動向について調査
2. 各国における機密区分の整理を踏まえ、取り扱いデータの区分方法についての調査・比較・評価

本項目の調査結果を踏まえ、クラウドサービスの利用も視野に入れた非機能要件を整理し、将来的な警察共通基盤システムのあるべき姿を検討するための基礎資料とする。

4.1.1　国内・海外における動向調査

クラウドにおけるデータ保護・データ主権に関連する検討事項、国内及び海外における事例について以下の観点より動向調査を行った。

- クラウドに関するセキュリティ認証
- 米国の警察・関連分野におけるクラウド政策と基準
  - Clarifying Lawful Overseas Use of Data Act (CLOUD Act)
  - Federal Risk and Authorization Management Program (FedRAMP)
  - Criminal Justice Information Services (CJIS) Security Policy
  - DoD The Cloud Computing Security Requirements Guide (CC SRG)
  - Joint Warfighting Cloud Capability (JWCC)
- EU の警察・関連分野におけるクラウド政策と基準
  - Europol におけるデータ管理規則
  - NIS2 (Directive (EU) 2022/2555)
  - ENISA EUCS (European Cybersecurity Certification Scheme for Cloud Services)
  - EU データ法 (Data Act)
  - Cloud Sovereignty Framework
- ドイツの警察・関連分野におけるクラウド政策と基準
  - Programm Polizei 20/20
  - Cloud Computing Compliance Criteria Catalogue (C5)
  - Verschlusssachen
- オーストラリアの警察・関連分野におけるクラウド政策と基準
  - Protective Security Policy Framework (PSPF)
  - Information Security Manual (ISM)
  - Whole-of-Government Cloud Computing Policy
  - Hosting Certification Framework (HCF)

諸外国においては、日本が掲げる「クラウド・バイ・デフォルト」に類似した動きが先行して見られる。諸外国は、機密性の高い情報に応じた技術面・運用面の要件を定めることで、クラウドサービスの利用を全面的に否定せず、条件付きで活用できる枠組みを整えている。

その背景には、情報の特性に応じた規則やガイドラインが存在し、日本の ISMAP とは別体系の枠組みが各国に設けられている点が挙げられる。

すなわち、諸外国においては、データ保護やデータ主権を適切に確保しながら、クラウドサービスを効果的に利用する政策が採用されていると言える。

4.1.1.1　国際的なクラウドに関するセキュリティ認証について

ISO/IEC 27017 は、クラウドに特化した情報セキュリティの技術的・組織的な管理策を定義する国際規格である。具体的には、ISMS (ISO/IEC 27001) をベースに、クラウドサービス提供者及び利用者の双方に対する固有のセキュリティ管理策を追加したものである。

ISO/IEC 27017 は、CSP 及びクラウドサービスカスタマの双方に対するセキュリティガイドラインを提供する。本規格では、従来の ISMS の管理策に対し、クラウド特有の脅威（仮想環境の保護、クラウド資産の返却など）に対応する追加の管理策を定めている。特に、クラウドにおける責任共有モデルを明文化し、プロバイダと顧客のどちらがどのセキュリティ領域を担保すべきかの境界線を定義している。

公共分野では、米国の FedRAMP のように「標準化された評価・認可・継続監視」を政府横断で再利用する設計が進み、EU では EUCS のような域内統一認証の検討が続く。

ドイツは BSI C5 を監査（ISAE 3000 等）ベースの枠組みとして位置付けている。

オーストラリアは HCF で政府調達におけるホスティング/クラウドの適合枠組みを運用し、ISM/PSPF 等の運用基準と接続している。

4.1.1.2　米国の警察・関連分野におけるクラウド政策と基準

米国は、政府横断のクラウド統制を FedRAMP で標準化し、セキュリティ評価・認可・継続監視を共通化することで、重複審査を抑えつつ政府利用クラウドの統制水準を揃える方向で整備している。

この上に、防衛分野では DoD のクラウド要件（Impact Level 等）を用いて情報の影響度に応じた段階的統制を設計し、法執行分野では CJIS のような分野固有要件で人的・技術的統制を上乗せする考え方が提示されている。

加えて、CLOUD Act は、米国の管轄下にある事業者に対して、データの所在にかかわらず「保有・管理下（possession/custody/control）」のデータを適法手続に基づき提出させ得る点を明確化し、域外データ取得の制度前提を与えている。

結果として、機微情報のクラウド利用では、域外法の影響を前提に、鍵管理（事業者が平文で提出できない状態の担保）や運用アクセス、監査証跡、インシデント対応の時間要件等を、統制の階層（FedRAMP＋分野要件）として組み立てる方向が読み取れる。

警察においては、FBI の CJIS Security Policy 等により犯罪情報への人的適格性審査やアクセス統制を要求している。

4.1.1.3　EU の警察・関連分野におけるクラウド政策と基準

EU は、EU 域外の大手 CSP への依存低減とデジタル主権確立を背景に、警察・防衛を含む公的分野でのクラウド利用について、法制度・認証・調達を組み合わせた統制強化を進めている。

警察分野では Europol 規則と独立監督（EDPS/欧州データ保護監察官等）を通じ、データ処理の目的限定、データ主体分類、保存・消去、監督・是正の枠組みを整備する方向が示されている。

サイバーセキュリティ面では、EU 全域のサイバーセキュリティ要件の標準化を目指す NIS2 において、デジタルインフラ分野において CSP 事業者に対しリスク管理措置と報告義務を求めており、EU 全域での耐障害性を底上げする制度構造となっている。

クラウド認証では EUCS の検討が継続し、制度統一と主権論点（域外法・支配、透明性等）

の扱いを巡る議論が続く。さらに欧州委員会は 2025 年 11 月 19 日に Digital Omnibus（デジタル・オムニバス）立法提案を公表し、既存のデジタル法制群の整合・簡素化により、企業・行政等のコンプライアンス負担を下げつつ競争力を高める「技術的改正パッケージ」と位置付けている。

特に EU データ法（Data Act）は、欧州データ戦略の中核をなす規則であり、コネクテッド製品及び関連サービスが生成するデータへの公正なアクセスと利用を促進し、データの経済的価値を高めることを目的とする。ユーザー（企業及び消費者）は、当該製品・サービスの利用によって生成されるデータにアクセスし、一定条件の下で第三者と共有できる。

Data Act は 2024 年 1 月 11 日に発効し、2025 年 9 月 12 日から適用された。Data Governance Act と並んで欧州データ戦略を支える制度であり、Data Governance Act がデータ共有の仲介・ガバナンスを扱うのに対し、Data Act はデータへのアクセス、利用、共有、ならびにデータ処理サービス（クラウドサービスやエッジサービスをいう。以下同じ。）間の乗換えに関するルールを定める。

Data Act に関する流れを整理したものが図表 4.1-1 である。

時期	出来事	概要
2020年2月	欧州データ戦略の発表	欧州のデータ経済に関する包括的な戦略目標の策定。
2022年2月	データ法案の提案	欧州委員会による規則案の公表。
2023年11月	欧州議会および理事会での採択	修正協議を経て、EUの立法機関により正式に承認。
2024年1月11日	発効	発効後、対応に係る猶予期間を設ける。
2025年9月12日	適用開始	猶予期間が終了し、対象企業に対する実質的な義務の適用が開始。
～2027年1月12日	乗換え手数料の廃止	乗換えに直接結びつく実費相当の減額手数料のみ認められる。2027年1月12日以降は、乗換え手数料を課してはならない。

図表 4.1-1 Data Act 発行・適用の流れ

また、データ処理サービス間の乗り換えを容易にし、ベンダーロックインを排除するための規定を設けている。CSP は、ユーザーが他のプロバイダへ移行する際の技術的、商業的、及び運用上の障壁を取り除く義務を負う。また、移行期間を経過した後は、データ移行に伴う乗り換え手数料の請求が全面的に禁止される。これらの事項を整理したものが、図表 4.1-2 である。

分類	概要
契約条件の透明化	乗り換えプロセス、データ移行にかかる期間、サポート内容を契約書に明記すること。
手数料の段階的撤廃	適用開始後、乗り換えに伴う手数料を実費のみに制限し、最終的には完全無料化すること。
相互運用性の確保	機能的同等性や相互運用性を確保するための技術的措置を行うこと。
域外データ移転の制限	第三国の政府機関による EU 域内非個人データへの違法なアクセス・移転要求に対し、技術的・組織的・契約的措置を求める。

図表 4.1-2 ベンダーロックインを排除するための規定

警察・防衛を含む公共部門が民間のクラウドサービスを利用する場合には、第三国政府による EU 域内非個人データへのアクセス要求への対応が重要な論点となる。

また、データ処理サービスの提供者に対し、EU 法または加盟国法と抵触する第三国政府アクセスや移転要求を防ぐため、合理的な技術的・法的・組織的措置を講じることを求

めている。

また、公的緊急事態への対応など必要性が認められる場合には、公共部門等が一定条件の下で民間企業の保有データの提供を求めることができる。この提供の求めは、目的限定・必要性・補充性を前提とする例外的枠組みであり、警察・防衛機関による一般的な自由取得権を定めるものではない。これらの事項を整理したものが図表 4.1-3 である。

観点	関連条項	クラウドシステムへの影響
国家安全保障の保護	第1条	Data Act は加盟国のpublic security、defence、national securityに関する権限を損なわない。したがって、これらの領域は一般のデータ流通ルールとは切り分けて解釈する必要がある。
域外アクセスの遮断	第7章(第32条) 第6章(第28条)	EU域内で保持される非個人データについて、EU法または加盟国法と抵触する第三国政府アクセス・移転を防止するため、クラウド事業者に技術的・組織的・法的措置が求められる。透明性情報の開示義務も課される。
民間保有データの提供	第5章(第15条)	緊急事態対応や、法律で明示された公的利益任務の遂行に必要な場合、公共部門等は必要性を示したうえで、一定条件の下で民間保有データの提供を求めることができる。

図表 4.1-3　Data Act によるクラウドシステムへの影響

4.1.1.4　デジタル・オムニバス法案の概要

2025 年 11 月 19 日、欧州委員会は、EU のデジタル関連ルールを簡素化し、企業の事務・コンプライアンス負担を軽減するための一連の措置を公表した。欧州委員会はこれを一般に「Digital Package」と説明しており、その中核となる立法提案が「Digital Omnibus」及び「Digital Omnibus on AI」である。

本提案は、単一の包括的新法を新設するものではなく、既存の複数の EU デジタル関連法令を横断的に改正するオムニバス方式を採る。具体的には、①GDPR、NIS2、Data Act 等を改正し、関連法案の一部を整理・統合する「Digital Omnibus」と、②AI Act を中心に改正する「Digital Omnibus on AI」の 2 本の規則案から構成される。

本提案の背景には、EU の競争力強化と規制簡素化を求める政策方針がある。欧州委員会は、企業が行政・コンプライアンス対応に費やす時間を減らし、イノベーションや成長に振り向けられるようにすることを目的としており、2029 年までに企業の行政コストを最大 50 億ユーロ削減できるとしている。他方で、欧州委員会は、簡素化は基本権、データ保護、安全性、公平性といった高い保護水準を維持したまま進めるとしている。

直近の状況としては、2026 年 2 月 5 日に欧州議会にて報告があり、複数の修正案が提出されている。また、2026 年 2 月 11 日には EDPB と EDPS が共同意見を発表し、特に個人データの定義変更に反対している。現時点では立法手続きの途中段階となっている。

①　GDPR（一般データ保護規則）に関する変更点

GDPR については、定義や通知実務等の一部を明確化・簡素化する改正が提案されている。

- 個人データの定義については、EU 司法裁判所の判例を踏まえ、ある主体にとって当該自然人を識別するために合理的に利用され得る手段がない場合、当該情報は個人データではないことを明確化する改正が提案されている。
- 個人データ侵害の通知義務については、現行の 72 時間から 96 時間へ延長する提案が盛り込まれている。また、NIS2 の単一エントリーポイント経由で通知を行う仕組

みも提案されており、サイバー事故報告の重複負担軽減が意図されている。

- さらに、EDPB による共通通知テンプレートや、高リスクとなり得る事案の共通リスト、EU レベルの DPIA 対象処理リスト等の導入も提案されており、加盟国間の解釈のばらつきを減らす方向性が示されている。

② データ関連法（Data Act、Data Governance Act）の統合

重複していたデータ関連法制の整理が行われた。

- 欧州委員会提案では、FFDR(Free Flow of Non-personal Data Regulation/EU 域内での非個人データの自由流通規則）、DGA(Data Governance Act)、Open Data Directive（政府や公共機関が保有するデータを民間や市民が利用できるようにする制度）についても、関連する規定などを Data Act へ取り込むこととされている。

③ AI 法（AI Act）に関する変更点（Digital Omnibus on AI）

2024 年に成立し、2024 年 8 月 1 日に発効した AI Act について、実施段階での負担軽減と運用円滑化を目的とする修正案が提示された。

- 高リスク AI システムに関する義務については、整合規格、共通仕様、欧州委員会ガイドライン等の支援措置の利用可能性に連動して適用開始時期を決める仕組みが提案された。欧州委員会の決定後、Annex III 型の高リスク AI には 6 か月後、Annex I 型には 12 か月後に適用開始とされ、最終的な期限はそれぞれ 2027 年 12 月 2 日及び 2028 年 8 月 2 日とされている。
- これまで SME 向けに設けられていた一部の簡素化措置は、SMC にも拡張される。具体的には、簡易な技術文書様式、任意の支援ツール、制裁適用時の配慮などについて、SME だけでなく SMC も対象とする提案が含まれる。
- 加えて、実地試験の柔軟化、AI リテラシー義務の見直し、高リスクに該当しないと判断した AI システムの登録負担軽減、中央集権的な監督の一部強化なども提案されている。

4.1.1.5 ドイツの警察・関連分野におけるクラウド政策と基準

ドイツは、政府利用クラウドのベースラインとして BSI C5 を位置付け、監査（ISAE 3000 等に基づく報告）を通じて透明性と統制の説明責任を担保する方向で整理されている。

警察分野では Programm Polizei 20/20 等を通じ、州ごとに分断された警察 IT の統合・標準化と情報共有の効率化を図る政策文脈が示され、全国規模でのデータ利活用基盤の整備が構想されている。

ドイツにおける機密情報（Verschlusssachen）は、BMI（連邦内務省）が定めた機密情報管理制度に関する規則である VSA(Verschlusssachenanweisung)に基づく取扱いが行われる。公共機関での利用のみに限定された情報である VS-NfD 等の VS 文脈でのクラウド利用については、BSI/連邦情報セキュリティ庁が Leitfaden für den Einsatz von Cloud-Lösungen

im VS-Kontext der Bundesverwaltung（連邦行政における VS 文脈でのクラウドソリューション利用のためのガイド）を公表している。

また、人物審査（要員統制）の制度的枠組みとして SÜG(Sicherheitsüberprüfungsgesetz)が存在し、安全保障上機微な活動を行う要員の審査手続と、機密事項の保護を定めている。

さらに、機密情報向け暗号製品等の承認・運用条件に関しては、BSI の承認製品一覧（BSI-Schrift 7164: Liste der zugelassenen IT-Sicherheitsprodukte und -systeme）が公開されており、承認を受けた製品を用いることで、その製品が承認された等級までの機密情報を処理・伝送することが可能である。

4.1.1.6 オーストラリアの警察・関連分野におけるクラウド政策と基準

オーストラリアは、政府データの保護を目的に、調達段階の認証（HCF）と運用段階の基準（ISM/PSPF）を接続し、政府利用クラウドの統制を整備している。

HCF は、政府顧客が主権性・セキュリティ要件を満たすホスティング／クラウドサービスを選定するための枠組みとして公式サイト上で運用が示され、認証済みサービスの活用を通じて政府データの保護水準を揃える設計となっている。

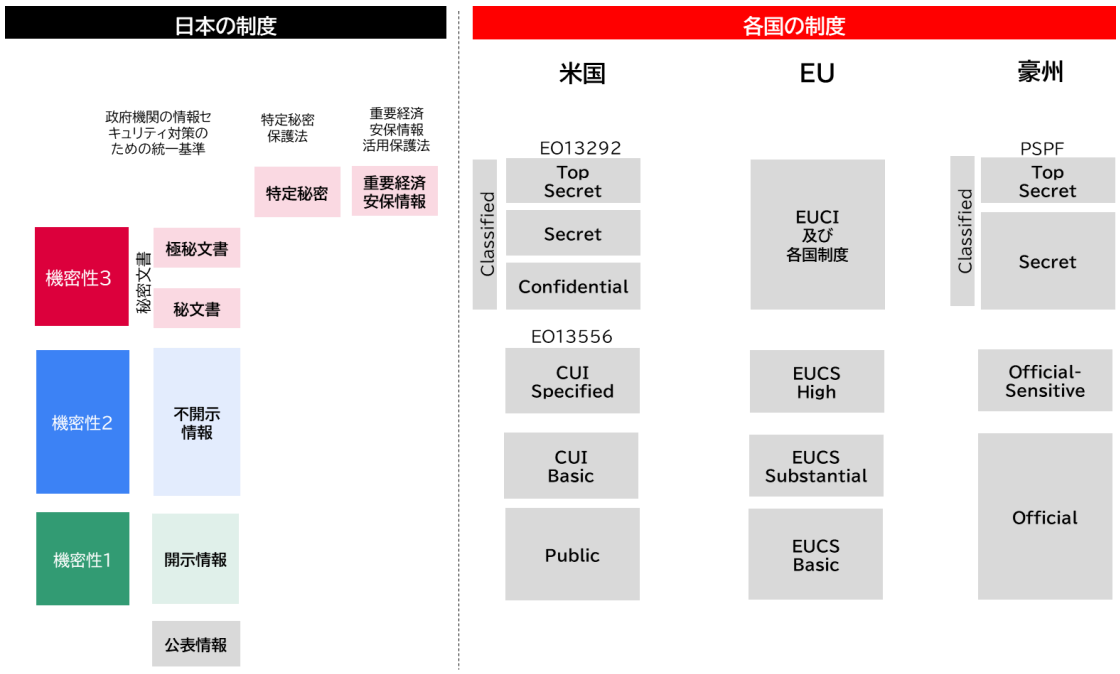
技術・運用の具体指針は ASD（オーストラリア信号局）の定めた Information Security Manual（ISM）が担い、PSPF は政府全体の保護安全保障の最低基準として、組織・人・情報・物理等の領域を横断する要求を与える。

さらに、DTA（DX 庁）は Whole-of-Government Cloud Computing Policy を公表し、2026 年 7 月 1 日の発効予定として APS 横断でクラウド移行とガバナンスを統一し、レガシー刷新と安全なクラウド活用を促進する方針を明確化している。

4.1.1.7 日本と各国の情報の機密区分に関する比較

日本と各国における情報の機密区分の比較は以下のとおり。日本における「機密性 3」以上の情報（例：「Secret」等）に対して制度上の区分が設けられていると同時に、日本における「機密性 2」に相当する情報についても、区分がある制度が存在する。

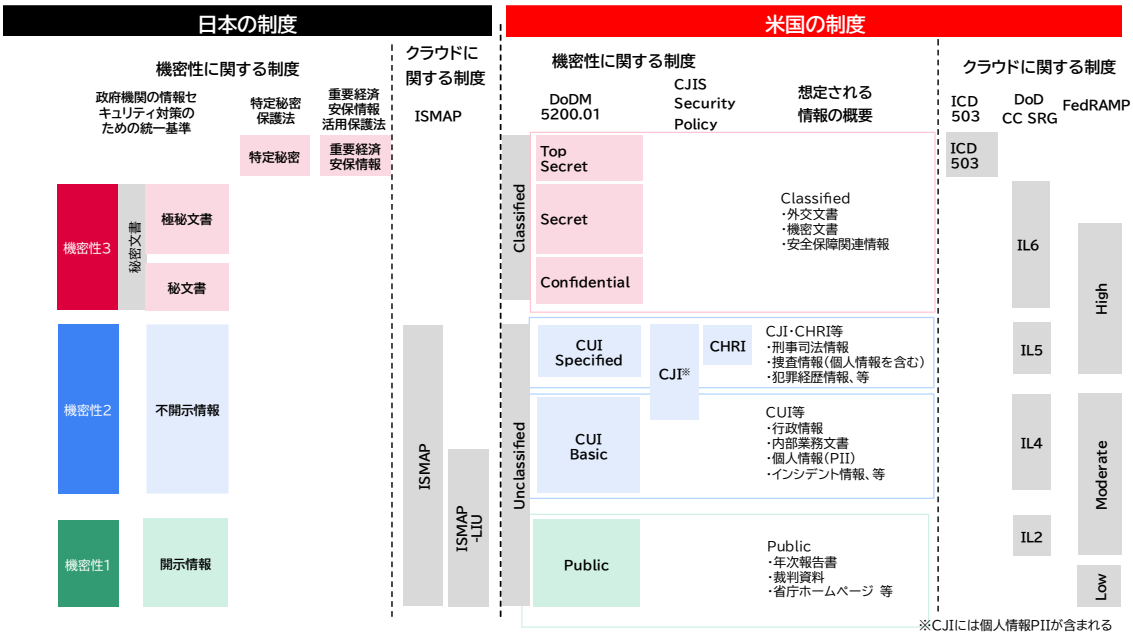
日本と各国の情報の機密区分の比較を図示したものが図表 4.1-4 である。



図表 4.1-4　日本と各国における情報機密の区分に関する比較

このうち、日本における機密性と米国における情報の機密性、クラウドの利用等に係る施策を比較する。特に DoD IL4、5 及び CJI/CHRI（犯罪に関する情報）の取り扱いについては、日本の機密性 2 よりも詳細な区分が存在することがわかる。

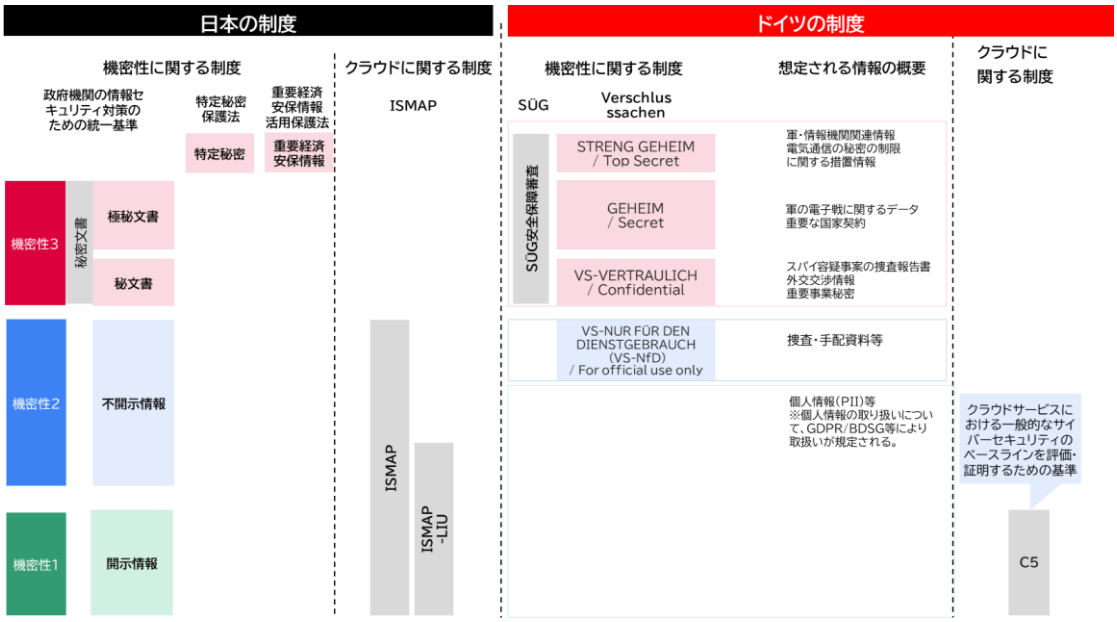
図表 4.1-5 は、日本と米国における情報機密の区分及びクラウドの利用に関する施策の比較を図示したものである。



図表 4.1-5　日本と米国における情報機密の区分及びクラウドの利用に関する施策の比較

同様に、日本における機密性とドイツにおける情報の機密性、クラウドの利用等に係る施策を比較する。特に機密性の高い情報における区分が定義されており、機密性 2 に該当する情報の一部等に管理要件が求められている。

図表 4.1-6 は、日本とドイツにおける情報機密の区分及びクラウドの利用に関する施策の比較を図示したものである。



図表 4.1-6　日本とドイツにおける情報機密の区分及びクラウドの利用に関する施策の比較

4.1.2　実効性の評価

海外動向の調査結果及び日本の機密区分と比較した結果、諸外国の枠組みと同等水準となる、警察が取り扱う情報の重要度に応じた技術面・運用面での要件等を備えた、新たな分類区分を提案する。

本項では、警察庁が取り扱う情報のうち、従来「機密性 2」として一括して整理されてきた領域について、その内実の差異を明確化し、クラウド利用を含むシステムの設計・調達・運用判断に資する新たな Tier1～Tier5 の区分として再整理することを目的とする。

日本の警察及び政府全体では、デジタル化の進展や捜査手法の高度化に伴い、取り扱う情報の量、種類、流通経路が大きく拡大している。他方、警察庁におけるクラウドサービスの活用は、捜査情報の機微性、証拠保全責任、国外法令の影響、インシデント発生時の対応といった観点から、これまで慎重かつ限定的に進められてきた経緯がある。

こうした中で、警察分野では同じ「機密性 2」に分類される情報であっても、実際に求められる統制水準には大きな幅が存在していた。しかし、従来の区分ではその差異を制度上十分に表現できず、結果として安全側に倒した一律の制約、すなわちオンプレミスを前提とした運用が生じやすかった。

4.1.1 で整理した各国動向をみても、諸外国では情報区分とクラウド要件が階層的に接続されており、日本の「機密性 2」に相当する層についても、情報の性質や漏えい時の影響に応じて複数段階に分けて統制している例が多い。特に米国では、日本の機密性 2 に近い領域を複

数のレイヤーに分割し、それぞれに対応するシステム要件を設定している。

このため本報告書では、従来「機密性 2」に包含されていた領域を、捜査関連性、秘匿性、運用主体、ネットワーク要件、国外法令の影響等の観点から再整理し、機密性の高い方から Tier5〜Tier1 の 5 段階に区分する枠組みを提案する。これは制度上の情報の機密区分そのものを新設する趣旨ではなく、警察庁が取り扱う情報の性質に応じて、要求すべき統制要件を具体化し、設計・調達・運用の判断を再現可能にするための整理である。

本整理では、特に Tier3 を一つの境界として位置づける。Tier3 は、捜査に関連し得る情報を扱うことを前提とした技術面・運用面の要件を備えた Tier 区分であり、国内データ所在、テナント分離、運用主体の信頼性確保など、一定以上の統制を前提とする。一方で、厳格な物理分離や完全専用構成までは必ずしも要求しない。このため、従来はオンプレミス前提とされがちであった領域についても、条件付きでクラウドの活用が検討できる余地がある。

これに対し Tier4 以上は、秘文書に相当する機密情報を取り扱うことを想定した水準であり、完全分離構成、国内事業者主導の運用、運用要員の信頼性確保、サプライチェーンリスクへの対応など、より強固な統制を要求する領域として整理する。したがって、本提案は単にクラウド利用の可否を二分するものではなく、どのような構成、運用、契約条件を満たせば当該情報を取り扱えるのかを、説明可能な形で示す。

また、本整理の重要な意図の一つは、ISMAP 等の政府横断的なクラウド制度と、警察固有のリスク認識との関係を明確にすることにある。ISMAP は政府情報システム全体の信頼性確保を目的とした枠組みであるが、警察が取り扱う捜査情報や機密情報については、ISMAP 適合のみでは十分とは言えない場合がある。そこで本整理では、ISMAP を基準としつつ、さらに追加の統制が必要となる領域を Tier として可視化する。

なお、本報告書では、機密性 3 相当の情報については、原則としてオンプレミス又はそれに準ずる環境での利用を前提とし、機密性 2 相当の情報については、その性質に応じてクラウドサービスの利用を検討対象とする考え方を採る。主要 CSP においても、外国法への対抗措置、専用リージョン、接続先を限定した環境等の提供が進んでおり、今後はガバメントクラウドとの関係や制度整備の進展も踏まえつつ、利用可能性を個別に判断していくことが考えられる。

図表 4.1-7 は、以上の考え方に基づき、各 Tier の想定対象となる情報の性質と、それを取り扱うシステムに求められる統制の方向性を整理したものである。後続のマッピング図及び要件整理図は、この Tier 区分を前提として構成したものである。

Tier	機密性	想定される情報例	想定される統制(制度面・運用面)	想定される統制(技術面)
5	機密性3 (極秘文書)以上	・極秘文書 ・特定秘密文書 ・重要経済安全保障情報	特定機密保護法、重要経済安保情報保護活用法、に基づく運用	
4	機密性3 (秘文書)	・秘文書、等	物理隔離・テナント分離、運用拠点の所在地(NOC/SOC国内完結等)、物理監査権	閉域網・外部持出しの制限、処理中データの保護、暗号化鍵の自律管理(HYOK)
3	機密性2	・捜査情報 ・犯罪経歴情報、等	**米国CLOUD法対応(開示請求への対抗)**、経済安全保障法(クラウドプログラムの安定供給の確保への適合)	自律運用性(キルスイッチへの対応等)、運用者の国籍・身元(クリアランス)
2		・行政情報 ・個人情報、等	データの所在地、サプライチェーン(懸念国排除、SBOM)、**諸外国基準適合(例:FedRAMP Moderate〜)**	耐量子計算機暗号(PQC対応)
1	機密性1	開示情報等	外部委託先の管理(再委託先開示)、**ISMAP適合** 透明性の確保(アクセスログ開示)、**準拠法・管轄(日本法・東京地裁)**、**知的財産・所有権(目的外利用禁止)**、**諸外国基準適合(例:FedRAMP Low〜)**	ロックイン対策(移行可能性の担保、消去証明)、データ削除・廃棄、アクセス制御

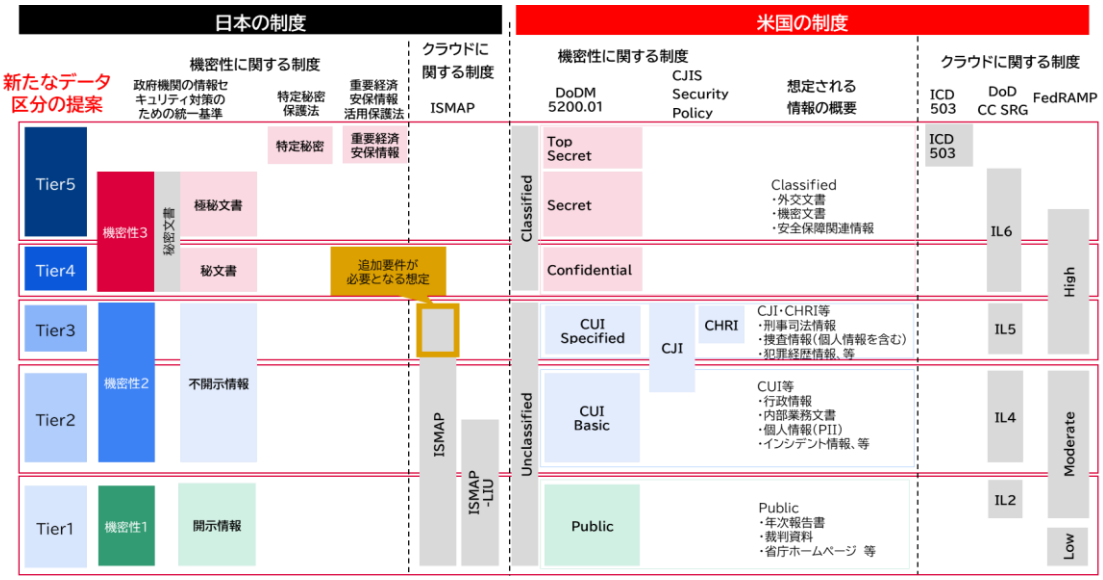
図表 4.1-7 各 Tier の想定対象と取り扱うシステムに求められる統制の方向性

日本における機密性と米国における情報の機密性、クラウドの利用等に係る施策に対しては、図表 4.1-3 のように、マッピングすることを提案する。

米国側の制度は、単一の機密区分だけでなく、政府横断の認可枠組み（例：FedRAMP）、国防分野の段階的要件（Impact Level 等）、法執行分野の分野固有要件（CJIS 等）が重層的に存在し、同じ「非機密（Unclassified）」領域でも、取り扱う情報の性質に応じて要求水準が細分化されている。

このため、以下の対応図は、制度上の完全な等価性を主張するものではなく、警察庁の Tier 整理に対して、米国の代表的な枠組みがどの階層で参照され、どの種別の統制（評価・監査、アクセス統制、インシデント対応、監査証跡等）に影響し得るかを把握するための整理である。

Tier2、3 の区分において、米国における IL4、5 相当の情報を扱うクラウドサービスが複数存在する状況を踏まえ、警察庁における IL4 と IL5 に相当する区分を設けることにより、情報の機密性に応じた基盤の選択が可能となる。



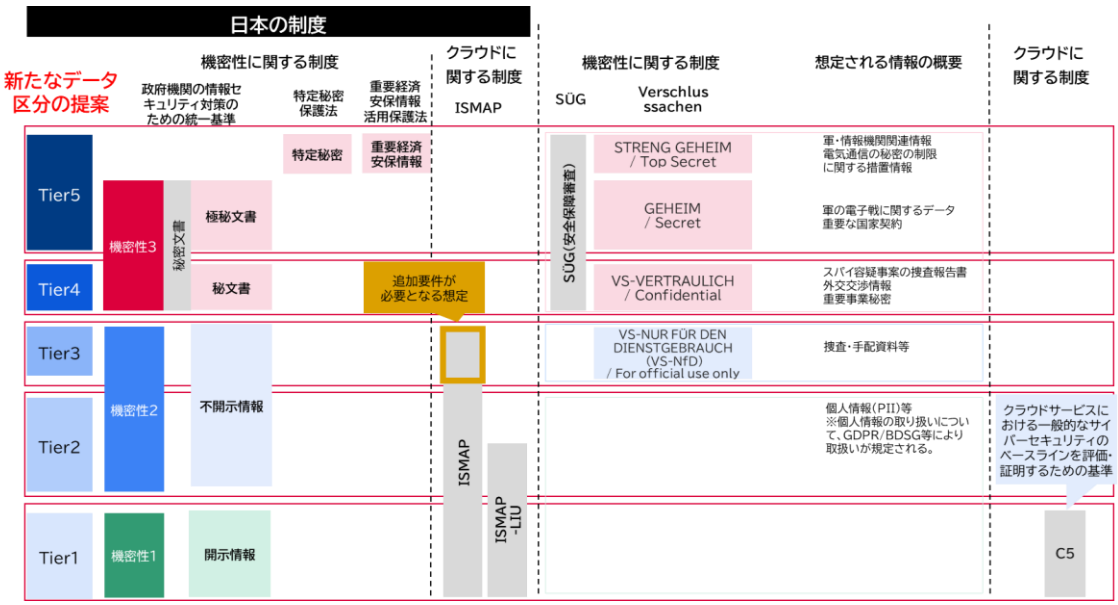
図表 4.1-8 各 Tier と日本及び米国の情報機密区分との対応

ドイツは、連邦行政における機密情報（Verschlusssachen）の取扱いを VSA 等で規定し、特に VS-NfD を含む VS 文脈でのクラウド利用については、行政向けガイドや要員統制（SÜG）等と接続しながら、運用上の前提条件を整理している。

このため、ドイツの機密区分と Tier の単純な名称対応を示すものではなく、VS 文脈でのクラウド利用を成立させるために必要となる前提（運用主体、要員適格性、承認製品の利用、ネットワーク要件等）が、Tier のどの水準で顕在化するかを読み替えるための整理である。

特に、Tier2～Tier3 の境界を、日本では機密性 2 とされる情報のうち、例えば要配慮個人情報のような機微性の高い情報としての管理が求められる区分である。Tier3～Tier4 の境界を追加の人員要件等が含まれる区分として扱い、当該境界以降で求められる統制の要素を、後段の要件整理へ接続することを意図している。

ドイツにおける情報の機密性等に対するマッピングは図表 4.1-9 のとおりとなる。Tier3 以上（犯罪に関する情報の取り扱い等）における機密区分を定めており、警察庁における Tier2 と Tier3 の区分を設けることにより、情報の機密性に応じた基盤の選択が可能となる。



図表 4.1-9 各 Tier と日本及びドイツの情報機密区分との対応

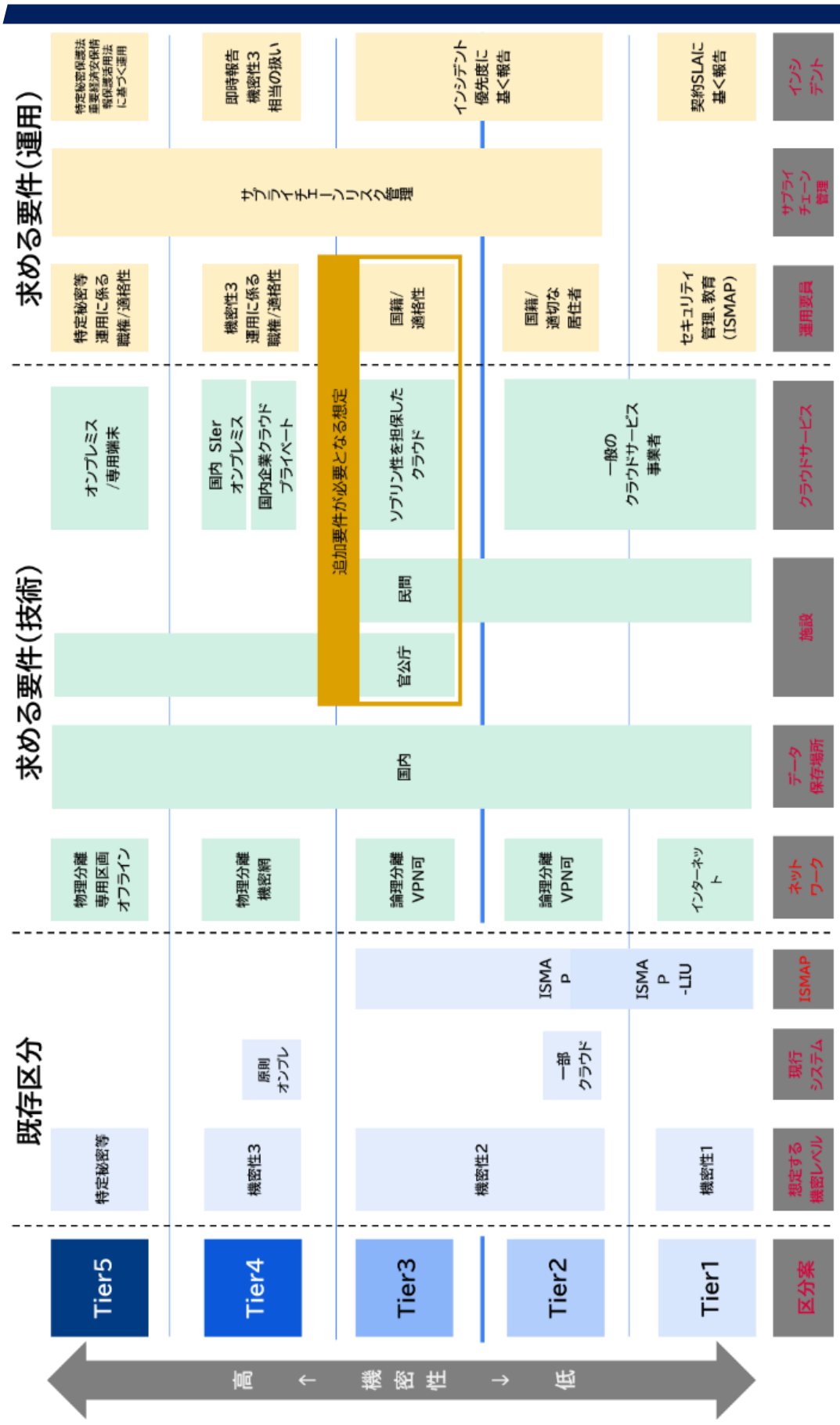
前掲の Tier 整理及び各国制度との対応関係は、あくまで設計・調達判断の「前提」を示したものである。ここから先は、Tier を実務で使える形にするため、「どの種類の情報がどの Tier に該当し得るか」及び「当該 Tier を扱うシステムに求めるべき統制要件が何か」を、警察行政の業務対象データに即して具体化する。

Tier	機密性	対象データ	想定する統制	ネットワーク	データの保存場所	施設	事業者	要員	インシデント
5	機密性3（極秘文書）以上	・極秘文書 ・特定秘密文書 ・重要経済安全保障情報	• 特定機密保護法 • 重要経済安保情報保護活用法に基づく運用	物理分離 専用区画 オフライン	国内	官公庁	オンプレミス /専用端末	• 特定秘密等運用に係る職権/適格性 • サプライチェーン管理	特定秘密保護法 重要経済安保情報保護活用法に基づく運用
4	機密性3（秘文書）	・秘文書等	• 物理的隔離・テナント分離 • 閉域網・外部持ち出し制限 • 使用中データの保護 • 暗号化鍵の自律管理 • 運用拠点の所在地 • 物理監査権	物理分離 機密網	国内	官公庁	国内SIer オンプレミス プライベートクラウド	• 機密性3運用に係る職権/適格性 • サプライチェーン管理	即時報告 機密性3相当の取り扱い
3	機密性2	・捜査情報 ・犯罪経歴情報等	• 米国CLOUD法対応 • 経済安全保障法 • 自律運用性 • 運用者の国籍・身元	論理分離 /VPN可	国内	官公庁 /民間	ソブリン性を担保したクラウド	• 国籍・適格性の限定 • サプライチェーン管理	優先度に基く報告
2		・行政情報 ・個人情報等	• 耐量子計算機暗号 • サプライチェーン	論理分離 /VPN可	国内	民間	一般の クラウドサービス	• 国籍・適切な居住者 • サプライチェーン管理	優先度に基く報告
1	機密性1	開示情報等	• 外部委託先の管理 • データの所在地 • ロックイン対策 • ISMAP適合 • アクセス制御 • データ削除・廃棄 • 透明性の確保、 • 準拠法・管轄 • 知的財産・所有権	インターネット 接続可能	国内	民間	一般の クラウドサービス	• セキュリティ管理体制の維持、教育（ISMAP）	契約SLA に基く報告

図表 4.1-10 各 Tier に該当する情報及びシステムに求めるべき統制要件の整理

図表 4.1-11 は、Tier の概念整理を、要件としての要求事項へ落とし込むための整理である。クラウド利用の検討では、クラウド基盤の機能だけでなく、運用体制・契約条件・監査可能性を含む「統制の実装可能性」が成否を左右する。

そのため、各 Tier について、技術要件（分離、暗号、ログ等）と運用要件（要員統制、運用主体、インシデント対応、証跡管理等）を組み合わせた要件案を示す。



図表 4.1-11 各 Tier における技術要件と運用要件の案

併せて、想定する統制のうち、Tier ごとに実施すべき内容を図表 4.1-12 のとおり整理する。

Tier	機密性	想定する統制	具体的な統制の内容案
5	機密性3（極秘文書）以上	特定機密保護法 重要経済安保情報保護活用法等に基づく運用	左記制度等で指定される各種要件を踏まえた運用が想定される。
4	機密性3（秘文書）	物理的隔離・テナント分離	他テナントと物理的にサーバーやストレージを共有しない専有環境（エアギャップ環境等）の構築が想定される。
		閉域網・外部持出しの制限	インターネット境界を持たない閉域網での運用と、外部へのデータ持ち出しの物理的な遮断を組み合わせた運用が想定される。
		処理中データの保護	コンフィデンシャル・コンピューティング等による、メモリ処理中におけるデータの暗号化状態の維持等の検討が想定される。一方で、実装コストに対し、実装の必要性が上回るか、検討が必要となる。
		暗号化鍵の自律管理（HYOK）	クラウド事業者がアクセスできない、庁内のハードウェア・セキュリティ・モジュール（HSM）を用いた暗号化鍵の生成と保管が想定される。 これ以下のTierでも、情報の性質に応じて、必要な鍵管理の検討が必要となる場合がある。
		運用拠点の所在地（NOC/SOC国内完結）	ネットワーク監視拠点（NOC）およびセキュリティ監視拠点（SOC）を日本国内に限定し、国外からの運用アクセスを完全遮断することが想定される。
		物理監査権	監査人または庁担当者がデータセンターに直接立ち入り、物理的セキュリティ対策を現地確認できる権利の契約明記が想定される。
3	機密性2	米国CLOUD法対応（開示請求への対抗）	外国政府等からのデータ開示要求に対して法的に対抗し、庁の許可なくデータを開示しない契約上のスキーム確立が想定される。
		経済安全保障法適合	クラウドプログラムの安定供給確保のため、インフラ基盤における特定国依存のサプライチェーンリスク排除に関する仕組みの検討が想定される。
		自律運用性	緊急時にクラウド事業者本国の制御から切り離し、システムを物理的または論理的に庁の判断で遮断・停止しても問題なく運用可能な機能の実装が想定される。
		運用者の国籍・身元（クリアランス）	データセンターやインフラ運用に直接アクセス可能な要員に対する、日本国籍の要件化と事前の身元調査の実施が想定される。
2		耐量子計算機暗号（PQC対応）	データの保存期間に応じ、将来的な暗号解読リスクに備えた、NISTが標準化を進める耐量子計算機暗号アルゴリズムへの移行計画の提示と段階的実装が想定される。
		サプライチェーン（懸念国排除、SBOM）	ソフトウェア構成一覧等の提出義務化と開発・運用プロセスにおける懸念国製コンポーネントの排除の検討が想定される。
		諸外国基準適合	各国制度 Moderateレベル（例：FedRAMP、C5）等の動向に合わせた基準の更新が想定される。
1	機密性1	データの所在地	データ主権要件（参考：BSI C5等）に準ずる、データの保存先およびバックアップ先を日本国内リージョンに限定することが想定される。
		アクセス制御（特権ID、承認フロー）	最小特権の原則に基づくロールベースのアクセス制御と、特権ID利用時における多段の承認プロセスのシステム化が想定される。
		外部委託先の管理（再委託先開示）	クラウド事業者が利用する再委託先の開示と、変更時の事前通知および承認プロセスの検討が想定される。
		ロックイン対策（移行可能性の担保）	標準形式でのデータエクスポート機能の提供と、NIST SP 800-88等に準拠した確実なデータ消去の実行が必要になる。 他環境への移行時の手数料等についても、各国の動きを注視し、適切に契約を行うことが想定される。
		ISMAP適合	日本政府のクラウドセキュリティ評価制度であるISMAP（若しくはISMAP-LIU）に準ずる管理基準を継続的に維持する必要がある。
		データ削除・廃棄	契約終了時または利用終了時に、システム上から確実かつ自動的に該当データが論理削除される仕組みの提供が想定される。
		透明性の確保（アクセスログ開示）	セキュリティインシデント発生時のアクセスログおよび監査ログの抽出・提供機能が想定される。
		準拠法・管轄（日本法）	契約に関する法的紛争が生じた場合の準拠法を日本法とし、第一審の専属的合意管轄を国内裁判所とする法的拘束力のある条項の記載が想定される。
		知的財産・所有権（目的外利用禁止）	データやシステム利用履歴を、事業者がAIの学習モデル構築など本来の目的以外に利用することの明示的な禁止する条項の記載が想定される。
		諸外国基準適合	各国制度 Moderateレベル（例：FedRAMP、C5）等の動向に合わせた基準の更新が想定される。

図表 4.1-12 Tier ごとに実施すべき内容案

4.1.3 今後の検討事項について

今後は、本整理で定義した Tier 区分を参考として、警察が取り扱う情報を体系的に棚卸しし、各情報がどの Tier に該当するかを具体的に整理することが必要である。その上で、情報の性質と求められる統制水準に応じて、対象システムごとの基盤構成、運用主体、接続方式、契約条件を段階的に具体化していく必要がある。

特に、クラウド活用の具体的な検討対象となり得るのは、Tier2 又は Tier3 に該当する情報を取り扱う基盤である。これらの領域について、従来のように一律にオンプレミスを前提とするのではなく、運用効率化、コスト最適化、開発・運用負荷の低減といったクラウドの利点を活かしつつ、データ所在、テナント分離、運用主体の信頼性確保、国外法令リスクへの対応等の要件を満たす構成を検討することが必要と考えられる。

- Tier3 相当のデータを扱う基盤の提案
  - ネットワーク主権や運用要員に関する国外依存リスクを排除する観点から、国内クラウド、国内プライベートクラウド、又はそれに準ずる構成を主軸とする。

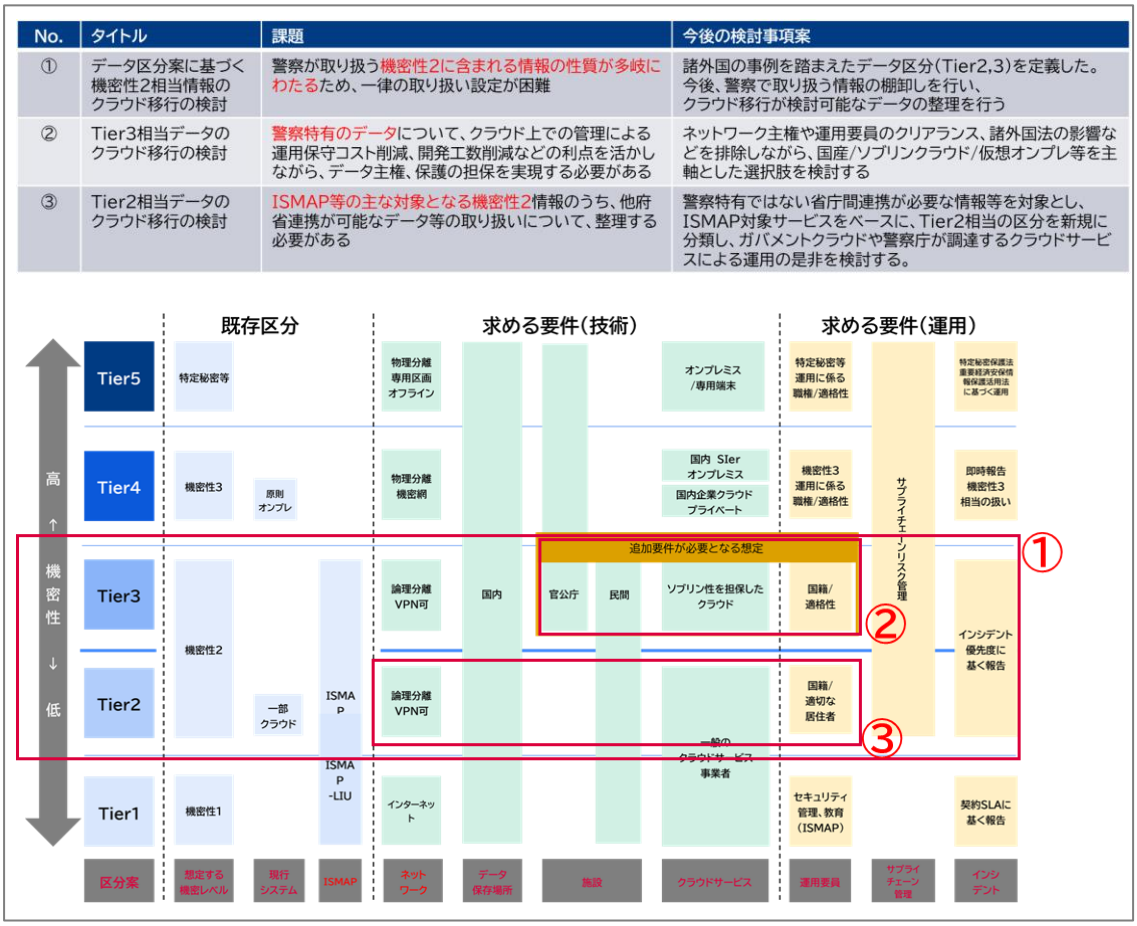
- 警察固有の管理が必要な情報については、警察自らが関与する運用体制を前提としたクラウドサービスを活用する。

➢ Tier2 相当のデータを扱う基盤の提案

- ISMAP 対象となる一般行政系システムとの連携も見据え、他府省との共同利用や、政府全体としてのクラウド基盤を活用する。
- ただしその場合、従来の ISMAP 区分に加え、警察用途を考慮した Tier2 相当の内部区分を設け、CSP による運用を前提とした場合の要件を明確化する。

図表 4.1-13 は今後の検討事項を整理したものである。

No.	タイトル	課題	今後の検討事項案
①	データ区分案に基づく機密性2相当情報のクラウド移行の検討	警察が取り扱う機密性2に含まれる情報の性質が多岐にわたるため、一律の取り扱い設定が困難	諸外国の事例を踏まえたデータ区分(Tier2,3)を定義した。今後、警察で取り扱う情報の棚卸しを行い、クラウド移行が検討可能なデータの整理を行う
②	Tier3相当データのクラウド移行の検討	警察特有のデータについて、クラウド上での管理による運用保守コスト削減、開発工数削減などの利点を活かしながら、データ主権、保護の担保を実現する必要がある	ネットワーク主権や運用要員のクリアランス、諸外国法の影響などを排除しながら、国産/ソブリンクラウド/仮想オンプレ等を主軸とした選択肢を検討する
③	Tier2相当データのクラウド移行の検討	ISMAP等の主な対象となる機密性2情報のうち、他府省連携が可能なデータ等の取り扱いについて、整理する必要がある	警察特有ではない省庁間連携が必要な情報等を対象とし、ISMAP対象サービスをベースに、Tier2相当の区分を新規に分類し、ガバメントクラウドや警察庁が調達するクラウドサービスによる運用の是非を検討する。



図表 4.1-13 Tier2,3 に相当する情報における今後の検討事項

中長期的には、AI 活用やデータ利活用の高度化を見据え、匿名化・仮名化を前提としたデータ活用の可能性、データ連携時の責任分界、相互運用性の確保、ベンダーロックイン回避のための調達・契約要件についても、段階的に検討を進める必要がある。これにより、現行業務を安全にクラウドへ移行するだけでなく、現在警察庁でも検討を開始している分析基盤や共通データ活用基盤への発展可能性もあわせて確保できるものと考える。

基盤の検討においてはコスト高騰や技術障壁に対する対抗策が重要となる。EU Data Act 等の動向を踏まえ、調達要件に相互運用性確保やクラウドからの移行時の費用の低減に係る規定を含むと同時に、調達、運用、移行等に関する FinOps 実装推進が必要となる。

4.2　オンプレミス環境への回帰又はクラウドサービスの乗換え

4.2.1　本個別調査の趣旨

クラウド環境に移行する際に想定される懸念に、クラウド環境に移行したシステムが十分なメリットを得られなかった場合、情勢の変化等によりクラウドを利用し続けることが困難となった場合等において、「クラウドサービスに移行したシステムをオンプレミス環境に回帰する」あるいは「異なるクラウドサービスへの乗換えを実施する」といったことが可能か、という点が挙げられる。そのため、本調査項目では、その際の実現性と留意すべき事項について整理する。

4.2.2　動向調査

国内外の官公庁、自治体を中心にオンプレミス環境への回帰、クラウドサービスの乗換え事例についての文献調査を実施した。公開情報を確認できた件数は多くないものの、それらの情報からオンプレミス環境への回帰、クラウドサービスの乗換えに至った経緯等を整理した。また、併せてデジタル庁が公開している GCAS ガイド、システム移行ガイド等の情報も参考に、影響を整理した。

4.2.3　実現性の評価

オンプレミス環境への回帰、クラウドサービスの乗換えについて、デジタル庁が公開しているシステム移行ガイドの R1/Replatform 及び R2/Rebuild を対象として評価を行った。（R3/Repurchase は移行ではなく再設計となる。）

それぞれの機能における、オンプレミス環境への回帰、クラウドサービスの乗換えの調査結果及び留意事項を整理したものを図表 4.2-1 に示す。

カテゴリ		回帰・乗り換えの致命的な阻害要因 （△：検証すべき要因あり、□：コスト観点での懸念のみあり、ー：阻害要因無し）	
データベース	RDB	△	クラウド移行する際に、現行システムDBでの非機能要件の確認、クラウドサービス固有機能の必要性（コスト削減効果含む）、暗号鍵管理の評価を行い、オンプレミスや他CSPでの再現の可能性やそのコストを検証したい。また、データ廃棄方法について、各CSPが提供する方法がデータ保護の要件を満たしているか確認が必要。
ストレージ	オブジェクトストレージ	△	暗号鍵管理の評価を行い、オンプレミスや他CSPでの再現の可能性やそのコストを検証したい。 データ廃棄方法について、各CSPが提供する方法がデータ保護の要件を満たしているか確認が必要。
ネットワーク	仮想ネットワーク	□	再設計・再構築による費用増の可能性は残るが、回帰や乗換えが不可能になる致命的な課題が出るとは想定されない。
	CDN	ー	考慮不要になる可能性が高いと想定する。 ※日本国内のみの利用を想定しているため技術課題としてはない認識
	DNS	□	本案件では日本国内のみ利用を想定しているため、技術課題はない認識。クラウド固有機能部分に対する再設計やHW保守等による費用増の可能性は残るが、回帰や乗換えが不可能になる致命的な課題が出るとは想定されない。
	負荷分散	□	再設計による費用増の可能性は残るが、回帰や乗換えが不可能になる致命的な課題が出るとは想定されない。
API		□	再設計・再構築による費用増の可能性は残るが、回帰や乗換えが不可能になる致命的な課題が出るとは想定されない。
コンピュート	仮想マシン（VM）	□	VM周辺の再設計やデータ移行について考慮は必要となるが、回帰や乗換えが不可能になる致命的な課題が出るとは想定されない。
	サーバレス/FaaS	□	FaaSの特性であるイベント駆動や並列実行を前提に設計する部分の再設計は必要となる可能性はあるが、回帰や乗換えが不可能になる致命的な課題が出るとは想定されない。
	コンテナ	□	コンテナ自体の周辺部分に関する考慮は必要となるが、回帰や乗換えが不可能になる致命的な課題が出るとは想定されない。
運用		□	クラウドの利便性の裏返しであるが、運用機能を一からオンプレミスで実装すると対応コストが大きくなる懸念がある。また運用負荷の増加による工数増加も留意が必要である。
CI/CD		□	再設計は必要となる可能性はあるが、回帰や乗換えが不可能になる致命的な課題が出るとは想定されない
セキュリティ		□	セキュリティ機能を一からオンプレミスで実装すると対応コストが大きくなる懸念がある。またオンプレ回帰においては、運用負荷の増加による工数増加も留意が必要である。

図表 4.2-1　オンプレ回帰・クラウド乗換時の阻害要因

4.2.4　想定されるリスクと対策

オンプレミス環境への回帰及びクラウドサービスの乗換えを行う場合には、Kubernetes（コンテナを管理し、複数のサーバ上での自動配置・運用を行うソフトウェア）やPostgreSQLといった、オンプレミス・クラウド間、クラウドサービス間で比較的互換性の高い製品・サービスを利用することにより、オンプレミス環境への回帰・クラウドサービスの乗換えの難易度や移行コストを一定程度抑制することが可能であると見込まれるものの、原則再設計が必要になるためそれなりの期間やコストを要するものと考えられる。

また、オンプレミス環境への回帰・クラウドサービスの乗換え時の残存データの削除の観点においては、CSPによって条件が異なることが明らかとなった。ガバメントクラウドに採択されたCSPにおいては、原則完全削除を実現しているところであるが、削除までに要する期間、完全削除の証跡の提示の可否などについてはCSPによって異なる。そのため、調達前等に予め条件を確認し、残存データが完全に削除されることが担保されるクラウドサービスを選択することを提案する。

4.3　オンプレミス・クラウド間のシームレスな接続と通信遅延の最小化

現行警察共通基盤システムは、オンプレミス環境で運用されていることから同一構内通信により安定した高速通信を可能としているが、将来的にオンプレミス及びクラウドサービスの双方を活用するハイブリッドクラウド構成を想定する場合、専用線接続、VPN接続等外部の回線を通じて通信を行う必要があり、その際に通信遅延の要因となるものとして新たに、オンプレミス及びクラウド環境間の接続距離、通信の暗号化による遅延を考慮する必要があり、これらの影響について整理した。

4.3.1　本個別調査の趣旨

警察共通基盤システムをオンプレミスとクラウドを跨ぐハイブリッドクラウド構成とする場合、下記のような観点で、オンプレミスとクラウド間の通信遅延の実態を調査し、警察庁のシステムの通信要件を満たすことができるかを検討する必要がある。

1. オンプレミスとクラウド間の接続方式における通信遅延
2. 接続方式・暗号化方式による通信性能・セキュリティの評価

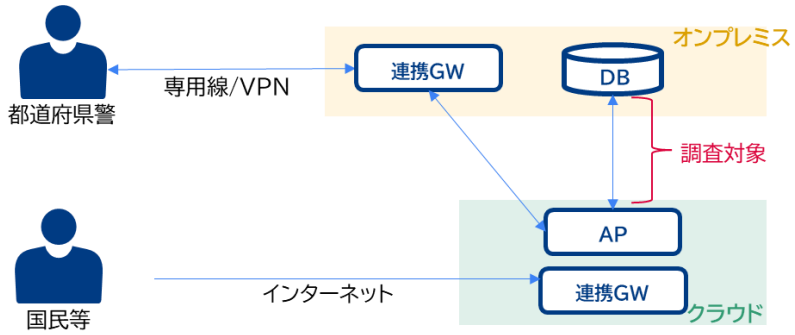
本個別調査においては、ハイブリッドクラウド化によるオンプレミスとクラウド間の通信遅延を調査し、警察庁のシステムにおいて留意すべき事項を明らかにする。

4.3.2　動向調査(論文調査等)

国内外において、通信遅延の机上及び通信遅延の実測値の検証を実施した論文等の調査及び実存するクラウドサービスの環境を利用した実測値のテスト等を実施した。

4.3.3　前提となるクラウド構成

4.3節において、オンプレミスとクラウド間の通信遅延の調査対象とする構成を図表4.3-1のとおりとする。



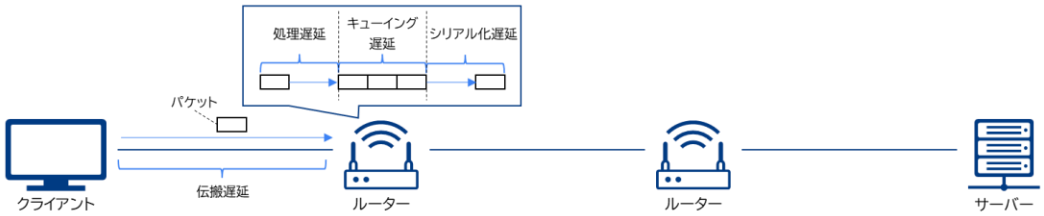
図表 4.3-1 通信遅延調査の対象

ハイブリッドクラウド構成を前提として、業務システムを利用した際に、検索処理等の応答速度に最も影響が出ると考えられる構成であるデータを格納するデータベース(DB)をオンプレミス側に、業務アプリケーションを配置するアプリケーションサーバ/Web サーバ(AP)をクラウドサービス側に配置するハイブリッド構成を想定し、オンプレミスとクラウド間の往復通信遅延（RTT：Round Trip Time）を算出した。

4.3.4 遅延要因の整理

一般的なネットワークの遅延の要因は主に図表 4.3-2 の 4 分類となるが、本調査では処理遅延と伝番遅延に着目して遅延の評価を行った。

分類	概要	対策
処理遅延	• パケットのヘッダの書き換えや暗号化処理等、ルーティングやスイッチング処理を行い、パケットをキューに入れるまでにかかる時間	• 高性能な通信機器の使用 • 処理が軽いプロトコルやソフトウェアではなくハードウェアで処理(ハードウェアアクセラレーション)できるプロトコルの使用
キューイング遅延	• キューに格納されたパケットやフレームが送信されるまでにかかる時間	• QoS(Quality of Service)制御により、重要なパケットを優先的に送信
シリアル化遅延	• NIC(Network Interface Card)がパケットやフレームを送信し始めてから送信し終わるまでにかかる時間	• 十分な帯域を用意することで、ほとんど無視できる • イーサネットフレーム(1518 byte)を1 Gbpsの回線で送信する場合: $\frac{1518}{1\times10^9/8} = 0.012$ ms
伝搬遅延	• 光、電気信号が物理的に伝搬するのにかかる時間	• データの送信元、送信先をなるべく近くに配置



図表 4.3-2 通信遅延の要因となるポイント

パケット暗号化等による処理遅延は実測値として暗号化無しの場合と比較し 0.04～0.08ms 程度、通信距離による伝搬遅延は東京－大阪間を想定した 600km の場合において、RTT は 8ms 程度であった。都道府県警からの業務利用による通信を想定すると、連携 GW - AP - DB - AP - 連携 GW と、オンプレミスとクラウドの間で最低 4 回の通信が発生するため、トータルで 32ms(8ms×4)の通信遅延が発生すると想定される。

4.3.5　想定されるリスクと対策

調査を行った結果、オンプレミスとクラウドサービスを跨ぐことに起因する通信遅延の要因はなく、拠点間接続距離、暗号化方式といった一般的なネットワークの構成による通信遅延に関しては、警察共通基盤システムにおける目標レスポンスタイムと比較すると影響はほぼ無いと判断する。ただし、第一サイトー第二サイト間で active-active 構成とするなど大幅なシステム変更を実現する場合は、その要件に合わせた検討が必要となる。

その他リスクとして、オンプレミスとクラウド間の通信回線を一本のみとした場合、光ファイバの断線等、通信障害によりシステムが停止する可能性がある。そのため、別経路での専用線を 2 本用意する等、冗長構成を採用することで可用性および継続性を高めることが必要と考える。

4.4　ガバメントクラウドを採択した場合におけるコストメリットの試算

4.4.1　ガバメントクラウドを選択した場合におけるコストメリットの試算

ガバメントクラウドに移行することで得られる金銭的コストのメリットを把握するために図表 4.4-1 のとおり整理した。

No	ドキュメント名	発行元	概要	本調査で活用可能な内容
1	継続的運用経費削減（FinOps）ガイド	デジタル庁	• ガバメントクラウドの運用開始後に、組織のIT部門・実務部門・財務部門が連携してクラウド利用料の継続的な管理と削減を目指す取り組みをまとめた文書 • 契約時ではなく本番運用後のコスト削減が重要であり、コスト構造の可視化や職員主体の削減計画、運用保守費の明細化で削減余地を探る必要性が示されている	• 利用中に実際のコストを把握し、改善・削減する方法が示されており、継続的に無駄を減らす運用が可能になる
2	ガバメントクラウド技術マニュアル	デジタル庁	• ガバメントクラウド利用組織がガバメントクラウドを利用する際の利用方法および技術的な特徴・要素・制約事項を理解することを目的とした文書 • クラウド最適化手法やシステム移行ガイド等、ガバメントクラウドに関する様々な個別マニュアルがまとめられている	• ガバメントクラウドにおけるアーキテクチャ・セキュリティ・コスト最適化等の全般的な情報が提供されており、設計・運用に必要な判断が可能になる
3	ガバメントクラウド利用における推奨構成（令和7年6月6日更新）	デジタル庁	• ガバメントクラウド利用者向けに、ガバメントクラウド利用時の推奨システム構成と設計・運用上の考慮事項を整理した技術指針を示す文書（AWS/Azure/Google Cloud/OCI） • イニシャル・ランニングコスト削減の観点から、Auto Scalingや長期継続割引の活用、コスト配分タグ管理、回線共同利用等による最適化が示されている	• ガバメントクラウド利用時の推奨構成が提供されており、迅速・柔軟・高セキュリティかつコスト効率の高いシステムを構築することが可能になる
4	令和5年度 ガバメントクラウド早期移行団体検証事業 早期移行団体への調査 検証結果	デジタル庁	• 令和5年度に実施された「ガバメントクラウド早期移行団体検証事業」の検証結果であり、ガバメントクラウド利用組織のクラウド移行に関する契約・申込・費用分担・回線導入・移行プロセス等の課題と改善点を整理し、後続組織向けの有益情報を提供することを目的とした文書 • 標準準拠システム移行前後の運用効率やランニングコストに関する比較検証項目が含まれており、運用工数や費用の増減理由の検証が行われている	• ガバメントクラウド移行後の運用管理およびシステム導入工数などのコスト増減情報が得られる • 移行プロセスにおける「つまずきやすいポイント」や望ましい導入プロセスの検証があり、ガバメントクラウド移行時のリスク軽減が期待できる
5	地方公共団体標準準拠システムのガバメントクラウド移行に係る手順書 第3.0 版	デジタル庁	• ガバメントクラウド利用組織が標準準拠システムをガバメントクラウドへ移行するための手順書であり、計画策定・予算化・契約・移行・運用開始までの具体的な作業手順を示した文書 • ガバメントクラウド移行において、試算するべきイニシャルコスト及び移行後発生するランニングコストが記載されている	• 移行手続きや作業の段取りが体系的に整理されているため、ガバメントクラウドへの移行を円滑に進めることが可能になる
6	地方公共団体標準準拠システムのガバメントクラウドの利用について 第3.0 版	デジタル庁	• ガバメントクラウド利用組織がガバメントクラウドを用いて標準準拠システムを運用する際の契約・責任分界・利用方式等の基本ルールを示した文書	• 利用組織、デジタル庁、クラウド事業者等の責任・役割範囲が明確化されており、ガバメントクラウドの契約関係を理解することが可能になる
7	ガバメントクラウド概要解説（全編）	デジタル庁	• ガバメントクラウドの概要が記されており、ガバメントクラウドの全体像や特徴などを理解することを目的とした文書	• ガバメントクラウドの特徴、制約等がまとめられており、ガバメントクラウドの全体像を理解することが可能になる

図表 4.4-1　ガバメントクラウド関連ドキュメントからの収集情報

4.4.2　実効性の評価

前項で収集した情報から以下のコスト削減となる要素を抽出した。

- クラウド利用料においてコスト削減ができる可能性が高い項目
  - インスタンスサイズの最適化
  - ストレージ容量の最適化
  - システム稼働時間の最適化
- 運用工数においてコスト削減ができる可能性が高い項目
  - 運用監視のマネージドサービス化
  - インフラ構築の自動化

期待されるメリット

- CSP が提供している CPU、メモリ等のリソースの柔軟性、構築の自動化、マネージドサービス等提供サービスを活用することにより、クラウドサービス活用時における運用経費が最適化されることが見込まれる。
- CSP が提供するコンテナ、マネージドサービス等を利用することにより、バージョンアップ時におけるプログラム改修時の影響範囲が縮小化され、オンプレミスと比較しコスト削減につながることが見込まれる。

第 5 章　費用対効果の試算

5.1　クラウド利用におけるコストの考え方

オンプレミス環境のシステムをクラウド環境へ移行する場合、個別業務プログラムの開発・改修が新たに発生するため、オンプレミス環境を継続することと比較すると主に開発・改修に係る役務コストが一時的に増加することが想定される。一方で、CSP が提供しているサービスを有効に活用することで、クラウド環境への移行後の運用コストを逓減することができ中長期的にはトータルコストの抑制も想定される。

第５章においては、オンプレミス環境で運用している警察共通基盤システムのクラウド環境への移行に関し、整備経費・運用経費等、システム開発・運用フェーズまでのライフサイクルを通じて要する経費を試算し、オンプレミス環境での運用を継続する場合の経費と比較することで、費用対効果の程度を確認する。

5.2　費用対効果の試算

5.2.1　費用対効果試算の前提

コスト試算に必要となる情報のうち、クラウドへの移行方法、使用する回線の種別や既存システムの維持運用コストといった不確定な条件により、現時点における試算が困難であったことから、以下の項目を含む、前提・仮定を置いたうえで費用対効果の試算を行った。

- 試算対象は、警察共通基盤システムの基盤の整備・運用に係る経費、個別業務プログラムに係る開発経費を対象とした。

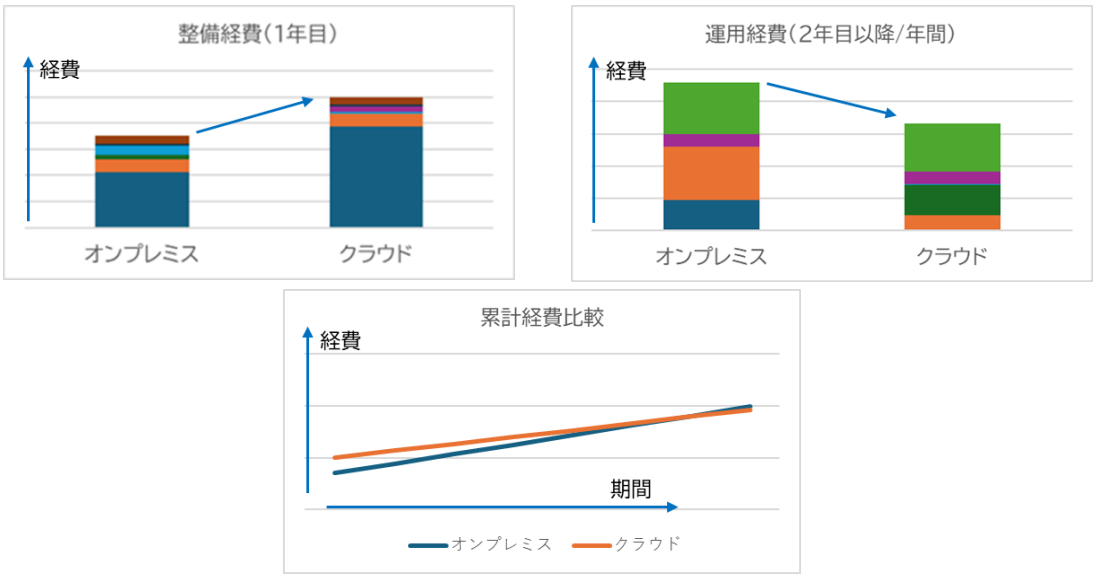
・ 令和２年度～令和６年度に調達を行った警察共通基盤システムの整備・運用経費を比較元の現行警察共通基盤システムのコストとした。
・ 比較対象期間は７年とし、オンプレミスの再構築及びクラウド移行したシステムについて初年度に整備経費を一括計上、２年目以降は運用経費を１年ごとに計上し、比較・試算を行った。
・ クラウド環境への移行先については、デジタル庁のクラウド化方針のうち R2/Rebuild であるクラウドシフトを目指すところであるが、本調査業務において業務アプリケーションのコンテナ化等の試算に至らなかったため、R1/Replatform での移行を前提とした。

5.2.2 試算結果

令和２年度～令和６年度までの警察共通基盤システムおける調達実績を元にオンプレミスでの再構築の場合、及びクラウド移行の場合の所要経費を試算した。

費用対効果の試算の結果、整備経費については、オンプレミス環境を継続する場合と比して、クラウド環境に移行する場合がより多くの費用を要すると見込むものの、運用フェーズにおいてはクラウド化することによるコスト抑制効果が働くことで中長期的に見ると、図表 5.2-1 の所要経費イメージのとおりオンプレミス環境を継続した場合の経費と逆転することが見込まれる。

＜所要経費イメージ＞



図表 5.2-1 中長期的に発生する経費のイメージ

5.2.3　為替レート・物価変動の影響

コストに関する試算、比較を行う際には将来的な価格変動要素について、予測もしくは想定可能なものについては考慮に入れておくべき必要がある。ここでは為替レート及び物価において将来的な変動要素となることを想定し前提を置きつつ変動時の影響について、5.2.2 にて行ったクラウド構成におけるコスト試算結果を現時点におけるコストの基準とし、為替レート・物価が変動する前提をおいたうえでコストに与える影響を試算した。なお、為替レート及び物価変動について、当然のことながら今後の経済情勢・動向により値は変動することとなるため、クラウド環境へ移行した後にあっても、コスト最適化に関する取り組みを継続的に行うことが重要であると考える。

5.3　実効性の評価と留意事項

費用対効果について試算した結果を以下のとおり整理した。

- 多くの前提や仮定を置いた試算結果ではあるが、傾向として CPU やメモリといったハードウェアリソースについてはクラウド環境に移行することにより、逓減する効果が見込まれる。
- ネットワーク経費については接続拠点数や利用する回線の種別により変動することはあるが、増額の要因となることが考えられる。
- 個別業務プログラムの移行については、オンプレミス環境での R2～6 年度の開発経費がクラウド移行後でも必要となるコストと仮定して積算している状況ではあるが、この想定で試算すると運用開始後、7 年目以降より総経費に対する効果が現れ始めると考えられる。

また、今回の試算においては仮定や前提条件を置いたうえで実施したものとなるため、今後、より精緻に試算を行うにあたっては以下の事項についても考慮する必要がある。

- マネージドサービスや IaC 等のクラウドサービスならではのツールやサービスを活用することにより構築・運用の更なる効率化が見込まれる。したがって、これらの活用を踏まえたデータ保護・主権を確保できる技術動向と併せて関連事業者、CSP などから、技術的な情報、経費に関する情報を幅広く収集することが必要と考える。
- また、オンプレミス環境を継続する場合においても、単に現行踏襲するのではなく、個別業務プログラムのコンテナ化といった最適化を検討するなど、コスト最適化に資する見直しも必要考える。
- 個別業務プログラムのコンテナ化を含めた全体の見直しを実施することにより、プログラムの改修及び改修後の運用の効率化を実現することができる可能性があるため、業務プログラム毎に実現可能性を検討する。
- 今回の試算は自治体の業務システムにおける、システム構成を参考とした試算となり、ハードウェア、ソフトウェア構成比率が警察共通基盤システムと異なると考えられる。
- 本章の試算においては、次にあげるような経費区分を試算対象より除外しているため、より精緻な試算に当たってはこれらの経費区分を考慮した費用対効果の算出を行うことが必要となる。

試算除外項目：電気料金、データセンター設備経費(監視カメラ、入退室管理)、媒体保管・搬送費、個別業務プログラムの改修経費 等

第 6 章　今後の方向性・ロードマップ

本業務は、警察共通基盤システムの費用の最適化や運用負荷の軽減等の観点から、警察共通基盤システムにおけるクラウドサービスの活用の可能性を検討するため、オンプレミス環境下にあるシステムをクラウド環境に移行した場合の費用対効果、想定される技術的・運用上の課題及び懸念事項について整理・分析を行い、今後の警察共通基盤システムの維持・発展に最適な方針の検討に資する基礎資料となることを目的としたものである。

本章では、本業務の結果を踏まえ、警察共通基盤システムの今後の維持及び発展に向けた方向性について整理する。具体的には、まず現行システムの課題認識を踏まえた今後の方向性を示した上で、本調査により得られた知見を整理するとともに、それらを踏まえた実現に向けた取組の方向性について取りまとめる。

6.1　本調査結果を踏まえた警察共通基盤システムの方向性

警察共通基盤システムは、これまでオンプレミス環境を前提として構築・運用されてきたが、近年のクラウド技術の進展やデータ利活用ニーズの高度化、並びにシステム運用コストの最適化に対する要請の高まりを踏まえると、今後のシステム更改に向けては、従来の構成や運用方式を前提としない形での検討が求められている。

現行システムの構成及び運用状況を踏まえて、警察共通基盤システムの維持及び発展に向けて今後検討を進めるべき方向性として、第３章に示したとおり以下の４点として整理した。

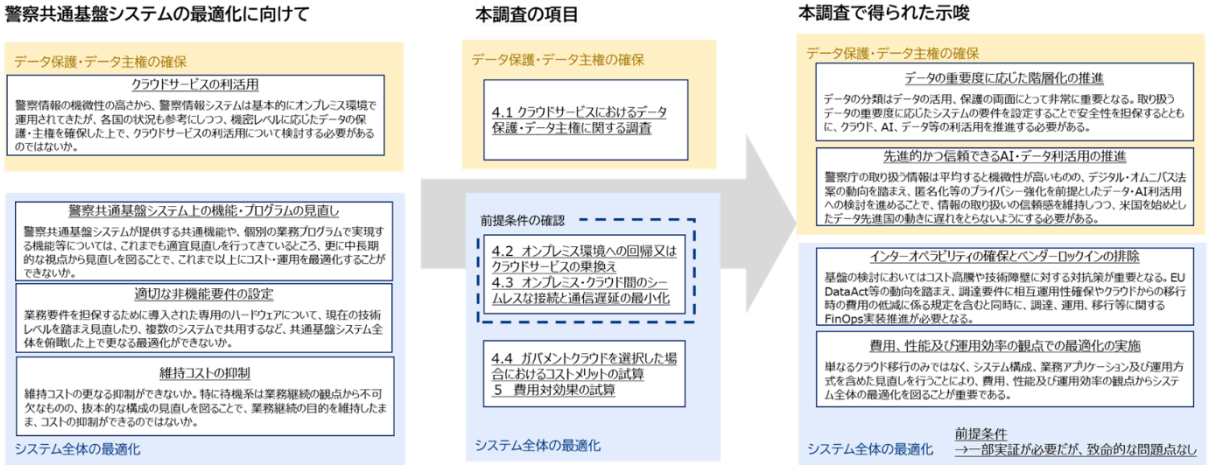
- **クラウドサービスの利活用**
- **警察共通基盤システム上の機能・プログラムの見直し**
- **適切な非機能要件の設定**
- **維持コストの抑制**

これらの方向性は大きく以下の二つの観点を踏まえて整理できる。第一に、**『クラウドサービスの活用を検討するに当たり、取り扱うデータの特性を踏まえつつ、データの保護及び主権を適切に確保すること（「データ保護・データ主権の確保」）』**である。第二に、**『限られた資源の中で持続的なシステム運用を実現する観点から、システム構成、アプリケーション構造及び運用方式の見直し等を図ること（「システム全体の最適化」）』**である。

こうした背景を踏まえ、本業務では既に示した「クラウド環境におけるデータ保護及びデータ主権」（データ保護・データ主権の確保）並びに、「オンプレミス環境への回帰又はクラウドサービス乗換え」、「オンプレミス環境とクラウド環境のシームレスな接続及び通信遅延の最小化」及び「費用対効果の試算」（システム全体の最適化）の４点について調査・整理を行い、警察共通基盤システムが今後取り組むべき事項として、以下の示唆を得た。

- データの重要度に応じた階層化の推進
- 先進的かつ信頼できる AI・データ利活用の推進
- インターオペラビリティの確保とベンダーロックインの排除
- 費用、性能及び運用効率の観点での最適化の実施

図表 6.1-1 はこれらの整理と示唆を図示したものである。



図表 6.1-1 本調査の概要と得られた示唆

6.2 各調査項目の結果及び得られた示唆

本節では、第４章及び第５章に示した各種調査の中で得られた示唆を、『データ保護・データ主権の確保』及び『システム全体の最適化』の２つの観点から整理する。

6.2.1 データ保護・データ主権の確保に係る観点

データ保護及びデータ主権に関する各国の動向及び技術動向を整理した結果、データの重要度に応じた適切な管理を行うことにより、安全性を確保しつつクラウド、AI 及びデータ利活用を推進できる可能性があることが確認された。また、データの重要度を踏まえた適切な管理を行うことで、データ保護とデータ利活用の両立を図る上で重要であることが示された。（4.1.1 項参照）

これらの調査結果を踏まえ、本調査ではデータ保護・データ主権の確保の観点から、「データの重要度に応じた階層化の推進」及び「先進的かつ信頼できる AI・データ利活用の推進」の２点を主要な示唆として整理した。

データの重要度に応じた階層化の推進

データの分類は、データの活用及び保護の双方の観点から極めて重要な要素である。特に機密情報等については、当該データの重要度に応じて必要な保護水準を適切に設定することにより、安全性を担保しつつ、クラウド、AI 及びデータの利活用を推進することが求められる。

本調査では、米国 DoD の IL、EU の CSA といった海外事例を参考に、機密性に加えて漏洩時の影響度などを踏まえた、データの重要度に応じた新たな情報区分の考え方を整理するとともに、各区分に対して想定される要件案の検討を行った。これらは今後のデータ管理の在り方

を検討するための参考となる整理として位置付けられるものであり、実際の情報区分及び管理要件については、今後の制度及び運用の検討状況を踏まえつつ適切に設定していくことが重要である。具体的には、今回の提案した情報区分を区切る要件である、運用要員に対する適格性、機器の設置場所（官公庁内か否か）、NW 構成の要件の設定が挙げられる。（詳細は 4.1.2 項参照）

このような整理も踏まえ、データの重要度に応じた適切な管理を行うことで、安全性を確保しながらクラウド、AI 及びデータの利活用を推進し、データ連携の円滑化や国民へのサービス提供における機動性の確保を図ることが期待される。

先進的かつ信頼できる AI・データ利活用の推進

警察共通基盤システムが取り扱う情報は、平均すると機微性の高いものが多いものの、近年のデータ利活用技術の進展や政策動向を踏まえると、適切な安全対策を前提とした AI 及びデータ利活用の検討を進めることが重要である。

本調査では、デジタル・オムニバス法案等の動向を踏まえ、データの重要度に応じた情報区分の考え方を整理するとともに、各区分に対して想定される要件案の検討を行った。

こうした整理を前提として、匿名化等のプライバシー強化措置を講じた上でのデータ及び AI の利活用について検討を進めることで、情報の取り扱いに対する信頼性を維持しつつ、行政サービスの高度化や業務効率化を図るとともに、米国や EU をはじめとするデータ利活用先進国の動向に遅れをとらない形でのデータ利活用の推進が期待される。

6.2.2　システム全体の最適化に係る観点

第４章及び第５章に示した各種調査の結果から、単なるクラウド移行のみではなく、システム構成、個別業務プログラム及び運用方式も含めた見直しを行うことにより、費用、性能及び運用効率の観点からシステム全体の最適化を図ることが重要であると考える。

これらの調査結果を踏まえ、本調査では「システム全体の最適化」の観点から、「インターオペラビリティの確保とロックインの排除」及び「費用、性能及び運用効率の観点での最適化の実施」の２点を主要な示唆として整理した。

インターオペラビリティの確保とベンダーロックインの排除

4.1.3 項で述べたとおり、クラウドにおけるデータ保護・データ主権に関する調査の中では、データ保護・データ主権の確保の重要性だけでなく、データ保護・データ主権の確保の達成を前提とした上での費用面における示唆も得られた。

本調査では、データの重要度に応じた情報区分の考え方を整理するとともに、各区分に対する要件案の検討を行った。こうした整理を踏まえつつ、基盤の調達及び運用においては、EU Data Act 等の国際的な制度動向も参考としながら、調達要件においてシステム間の相互運用性の確保を求めるとともに、クラウドサービスから外部へデータを移転する際の料金の規定についても適切に整理することが重要となる。

また、クラウドサービスの利用に伴うコストについては、調達、運用及び移行の各段階にお

いて継続的に把握及び管理を行い、コスト構造の透明性を確保するとともに、サービスの選択や構成の見直しを適切に行うことにより、長期的に持続可能なシステム基盤の実現を図ることが求められる。

費用、性能及び運用効率の観点での最適化の実施

費用対効果に係る調査（5章）では、クラウドサービスの利用の検討においては、既存システムの単純な移行にとどまらず、マネージドサービスの活用やインフラ構成をプログラムにより管理する手法（IaC）の導入といったクラウドスマート化を推進するとともに、業務プログラムのコンテナ化・更なるマイクロサービス化等を含めたシステム構成及び運用方式の見直しを検討し、費用面、運用面での最適化の検討が重要であるという結果を得た。

また、クラウドサービスを利用するに当たって留意すべき、オンプレ回帰・クラウド乗り換え時の障害（4.2.3項及び4.2.4項参照）及び通信遅延（4.3.5項参照）についても調査を行い、いずれも致命的な問題はないものの、性能要件である処理要件等については実際に採用を想定する基盤を用いた実証することが望ましいと考える。

こうした結果から、システム全体の最適化として、費用、性能及び運用効率の観点での最適化を実施することを提案する。

6.3 今後の取組の方向性

本節では、前節までに整理した調査結果及び得られた示唆を踏まえ、警察共通基盤システムの将来的な更改及び基盤整備を進めるに当たって検討すべき取組の方向性について整理する。

本調査では、警察共通基盤システムの今後の方向性を検討する上で、主として「データ保護・データ主権の確保」及び「システム全体の最適化」の二つの観点が重要であることを確認した。

このため、本節ではこれら二つの観点から、警察共通基盤システムの今後の具体的な検討事項を、令和９年度の次期システムリリース以後の次期システムにおける増設時での実施を検討する短期的な取組事項と次々期システムを見据えた中長期的な取組事項に分けて整理する。

6.3.1 データ保護・データ主権の確保に係る取組

本調査では、クラウド環境におけるデータ保護及びデータ主権に関する制度及び技術動向を整理した結果、米国DoDのIL、EUのCSAといった海外事例を参考に、データの重要度に応じて適切な保護水準を設定することにより、安全性を確保しながらクラウド、AI及びデータ利活用を推進することが可能であることが確認された。

一方で、警察共通基盤システムにおいては機微性の高い情報を取り扱うことから、データの重要度を踏まえた適切な管理及びシステム構成の検討が必要である。

このため、今後の検討においては、まず本システムが取り扱うデータの重要度を整理するとともに、データ保護・データ主権を確保するシステム基盤の技術動向を把握し、情報区分に応じたシステム構成の検討及び実証検証を段階的に進めていくことが望まれる。

上記を踏まえ、以下に今後の取組事項案を示す。

- データの重要度の整理
- データ保護・データ主権を確保するシステム基盤の動向調査
- システム基盤の構成の検討
- システム基盤部分の実証

データの重要度の整理

警察共通基盤において適切なデータ保護を実現するためには、まず本システムが取り扱うデータの特性及び機密性を整理し、データの重要度に応じた分類を明確化することが重要である。具体的には各個別業務プログラムで利用している主要なデータを洗い出したうえで、それぞれのデータの重要度を今回整理した情報区分等を踏まえて、濃淡をつけたうえで整理することが考えられる。

本取組は次期システムの増設に合わせて実施可能な取組と想定されるため、先行して実施する取組として位置づけられる。

この整理を行うことにより、各データの保護に求められる要件やシステム構成の検討における前提条件を明確化するとともに、今後のシステム基盤の検討やデータ利活用の方針検討の基礎とすることができる。

データ保護・データ主権を確保するシステム基盤の動向調査

近年、クラウドサービスをはじめとするシステム基盤の技術は急速に進展しており、データ保護やデータ主権を担保するための機能やサービスも多様化している。従って、データの重要度の整理で判明した、警察共通基盤システムが扱う情報の重要度とそれに応じた要件を満たすサービスについて改めて確認することが必要である。

本取組は新たな情報区分を踏まえたシステム更改に資する検討であるため、次々期システムを見据えた取組として位置づけられる。

なお、この調査は以下に示すシステム基盤の構成の検討と密接に関連するため、一体的に取り組むことが望ましい。

システム基盤の構成の検討

重要度に応じたデータの保護を実現するためには、その利用形態も踏まえたシステム構成の検討が必要となる。従って、前述の「データの重要度の整理」「データ保護・データ主権を確保するシステム基盤の動向調査」の整理結果を踏まえて、データ保護・主権を確保できる警察共通基盤システムの構成案を検討する必要がある。

本取組は新たな情報区分を踏まえたシステム更改に資する検討であるため、次々期システムを見据えた取組として位置づけられる。

なお、本調査で提案した情報区分に応じたシステム基盤の分割案については後述する。(※)

システム基盤部分の実証

システム基盤の構成を決定するに当たっては、通信遅延、可用性、性能等の非機能要件が業務運用に与える影響を事前に確認することが重要である。本調査において、業務要件として致命的な影響がないことは確認しているが、上述で作成されたシステムの構成案を踏まえて、利用が想定されるシステム基盤を利用した、小規模な系での通信遅延及び性能要件等に係る実証を行うことが望ましい。

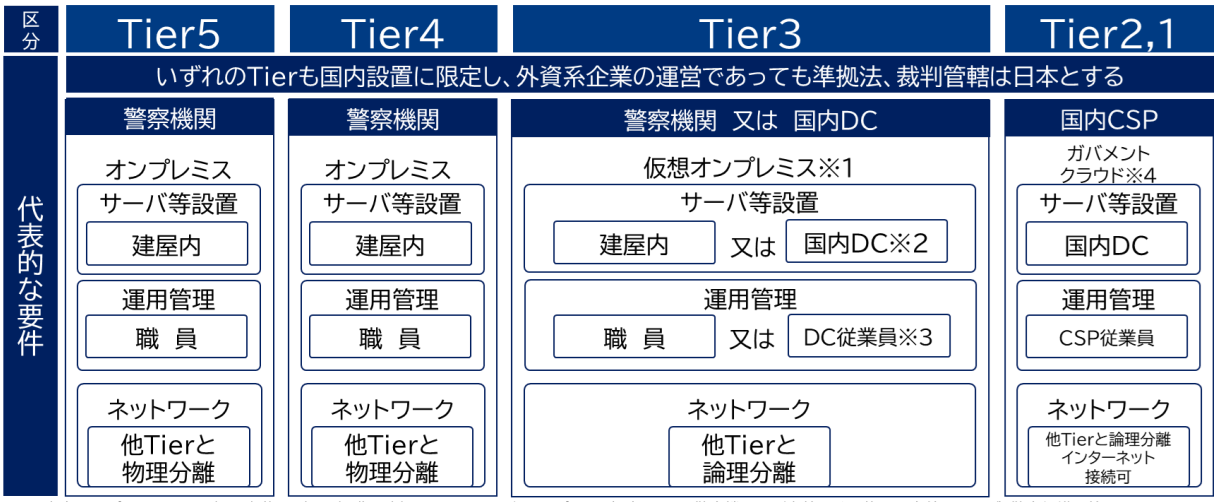
本取組は新たな情報区分を踏まえたシステム更改に資する検討であるため、次々期システムを見据えた取組として位置づけられる。

※本調査結果を踏まえたシステム基盤の分割案について

本調査において整理した情報区分（Tier）では、運用要員に求められる適格性に加えて、Tier2 と Tier3、Tier3 と Tier4 の違いはそれぞれ以下のように整理される。なお、Tier1 と Tier2 の要件の違いとなるサプライチェーンマネジメントは警察庁の方針として、Tier1 においても必要となるため、本検討部分において、Tier1 と Tier2 は一体として考える。また、警察共通基盤システムではインターネットによる外部連携システムも存在するため、インターネットとの接続要件についても以下に整理する。

- Tier2 と Tier3：Tier3 はサーバ設置場所が他のシステムと施設内で独立している、加えてネットワーク要件として、インターネットとの接続が許容されない。
- Tier3 と Tier4：Tier4 は施設として官公庁の施設にのみが許容。また、ネットワーク要件として、他 Tier と物理分離されている。

各 Tier の代表的な要件の差分を整理したものが図表 6.3-1 である。



※1 仮想オンプレミスとは、データ主権とデータ保護を確保していることが、オンプレミス相当であり、警察機関の所有管理する施設の内外を問わず、警察組織の管理や統制が機能し、自律的な運用が可能と認められるものを言う。
※2 専用ラック等DC内で独立していることが必要
※3 国内DCの従業員は、システム運用管理を行うため、日本国籍を有し、警察情報システムを扱うのに適切と認められる者であり、機器の異常の有無やOS、データベース等のミドルウェアのアップデート作業等を行う要員をいう。
※4 Tier2の場合は、ガバメントクラウド。Tier1の場合は、パブリッククラウドとする。

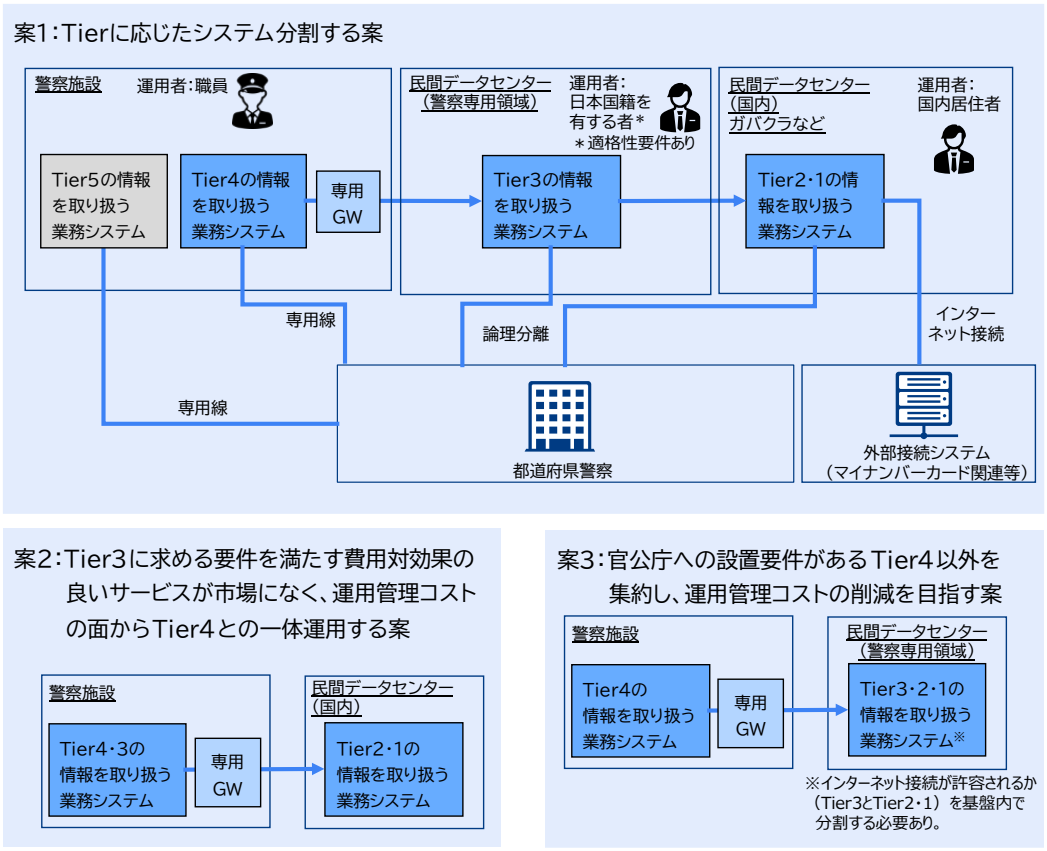
図表 6.3-1 Tier に応じたシステムに求められる要件差分の概要

これらの前提に加え、本調査において整理した情報区分（Tier）を踏まえたシステム構成基盤の想定案を図表 6.3-2 に示す。（案 2、案 3 については、業務システムの所在地と業務システム間の連携に絞って記した。また Tier5 の情報は独立して扱う必要があることから、警察共通基盤システムに係る検討では対象外とすることとする。）

情報の Tier ごとにシステム基盤を分割した場合は案 1 となるが、環境を複数用意することによる運用管理負荷の増加や適切なサービスが市場にないことなどによって、基盤を集約する方が合理的であると考えられ、案 2, 案 3 が候補となる。案 3 については、インターネットでの外部連携システムが存在するため、基盤内でインターネット接続が許容の是非でセグメントを分割する必要がある点に留意する必要があるが、より多くの基盤を警察施設外に出すことが可能となることから、運用管理コストの削減を図ることができる。

こうした分割案の決定に当たっては、各 Tier の情報がどの程度あるのか、基盤の分割による運用管理コストの見積等を踏まえて決定することが望ましい。

なお、こうした分割案の実現に当たっては、一度に対象となる業務システムを全てデータセンター等に移行するのではなく、一部の業務システムから試行的に移行し、業務への影響等を精査しつつ、移行の対象となる業務システム全体を段階的に移行していくことが望ましいと考える。



図表 6.3-2 情報 Tier に基づいたシステム基盤の分割案

6.3.2　システム全体の最適化

本調査では、クラウドサービスの活用による費用対効果を最大化するためには、単なるインフラ環境の移行ではなく、システム構成及び個別業務プログラムの見直しを含めた総合的な最適化が重要であることが確認された。

特に、EU Data Act 等で示された、クラウドサービス間の移行や他の環境への移転に伴う技術的及び経済的な障壁の低減を図る方針は、クラウドサービスの特性を踏まえたシステムアーキテクチャの見直しや運用方式の改善を進めることの重要性を高めている。

こうした背景を踏まえて、今後の検討においては、次期システムの構築・運用の中で実施可能な取組を進めるとともに、将来的なシステム更改を見据えたシステム構成及び運用方式の見直しについて検討を進めることが望まれる。

上記を踏まえ、以下に今後の取組事項案を示す。

- **オンプレミス拡張型クラウドの活用の検討**
- **個別業務プログラムの見直し**
- **クラウドスマート化の検討**
- **データの階層化を踏まえたシステム構成案に対する見積の精査**

オンプレミス拡張型クラウドの活用の検討

オンプレミス拡張型クラウドは、現行のシステム構成、各種要件を大きく変更せずに利用できるサービスと想定され、活用することでコンピューティングリソースの見直しや稼働時間調整といったコストメリットを受けられることが想定されるため、活用の検討が望ましい。特に開発環境や検証環境等の非本番環境において特に有効に活用できる可能性がある。

本取組は次期システムの増設のタイミングでも早期に実施可能な取組と想定され、効果やシステム構成案によっては次々期システムに向けても継続した活用も想定される。

個別業務プログラムの見直し

コンテナ技術の活用やマイクロサービス化等によりアプリケーション構成を柔軟化することは、クラウドサービスの利用に関わらず、システムの拡張性や運用効率を向上させることが期待され、クラウドサービスとの親和性も高く、検討することが望ましい。警察共通基盤システムでは既にアプリケーション基盤の分割など行われている状況であるため、更なる柔軟化が可能かという観点での見直し可能なものがあると考える。

本取組は次期システムの増設のタイミングでも早期に実施可能な取組と想定されるが、データの重要度を踏まえたシステム構成を目指す次々期システムに向けても継続した実施が想定される。

クラウドスマート化の検討

システム全体の最適化、特に費用面での最適化にあたっては、CSP が提供するマネージドサービスや自動化技術を適切に活用することが重要となる。EU データ法に代表される昨今のクラウドサービス間の移行や他の環境への移転に伴う技術的及び経済的な障壁の低減を図る方

針を踏まえると、技術的な観点でのインターオペラビリティの確保の動向を引き続き伺う必要はあるものの、従前はロックインの要素となることが危惧されてきたクラウドサービスの特性を活かしたシステム運用について検討を進めることが重要である。

本取組は次期システムの増設のタイミングでも早期に実施可能な取組と想定されるが、データの重要度を踏まえたシステム構成を目指す次々期システムに向けても継続した実施が想定される。

データの階層化を踏まえたシステム構成案に対する見積の精査

今後のシステム更改に向けては、クラウドサービス及び関連技術の動向や費用構造を踏まえた調達条件の整理を行うことが重要である。ここまでに記載した取り組みの結果を踏まえたシステムの各種要件に対して、事業者より見積を取得し、精査することで、データ保護・データ主権の確保とシステム全体の最適化を両立したシステム構成案を決定することが重要である。

本取組は新たな情報区分を踏まえたシステム更改に資する検討であるため、次々期システムを見据えた取組として位置づけられる。

6.3.3　ロードマップ案

6.3.1 及び 6.3.2 において整理した取組事項について、今後の検討及び実施の進め方を示すためのロードマップ案を図表 6.3-3 に示す。

項目	実施する内容	スケジュール
データの重要度の整理	各個別業務プログラムで利用している主要なデータを洗い出したうえで、それぞれのデータの機密レベルを今回整理したTier等を踏まえて、より濃淡をつけたうえで整理する。	次期システム増設▼ 次々期システム更改▼
データ保護を担保するシステム基盤の動向調査	データ保護・主権を担保できる技術動向、導入事例等の調査、警察共通基盤システムへの適用可能性の調査を行う。	
システム基盤の構成の検討	データ保護・主権を確保できる警察共通基盤システムの構成案を検討する。	
システム基盤部分の実証検証	システム基盤の構成の検討で作成された構成案を踏まえた処理要件等非機能要件にかかる実証を行い、業務影響がないことを確認する。	
オンプレミス拡張型クラウドの活用の検討	第二サイトも含め、データ保護・主権を貴庁で担保しつつ、コスト削減、運用効率化に寄与する機器、サービスの適用を検討する。	継続実施も検討
個別業務プログラムの見直し	警察共通基盤システムにおいて利用している個別業務プログラムについて、更なるマイクロサービスやコンテナへの移行余地がないか検討を行う。	
クラウドスマート化の検討	データ保護・データ主権を確保しつつ、マネージドサービスの活用やITインフラの設定・管理の自動化等を中心としたクラウドスマート化を検討する。	部分的な実施を想定
データの階層化を踏まえたRFPの実施	システム基盤の構成の検討で作成された構成案を踏まえて詳細な見積もりを取得し、費用対効果を精査する。	

データ保護・データ主権の確保　先行して実施　次々期システムに向けて実施

システム全体の最適化　先行して実施　次々期システムに向けて実施

図表 6.3-3　ロードマップ案

（別紙）

警察情報システムの合理化・高度化に係る調査研究 用語集

用語	説明	備考
A～Z		
CSP	＜調達仕様書記載内容を抜粋＞ クラウドサービスを提供する事業者の総称。	Cloud Service Provider
DR	地震・火災・サイバー攻撃などの災害や障害により停止したITシステムや業務を、迅速に復旧し事業継続を図るための対策や仕組みを指す。	Disaster Recovery
FinOPS	クラウド利用におけるコスト（費用）を可視化・管理・最適化するための運用・管理の考え方	Financial Operations
GCAS	政府機関がガバメントクラウドを安全かつ統一的に利用するための共通アクセス基盤。利用者認証や接続管理などを集約し、各省庁が個別に同様の仕組みを構築する負担を軽減することを目的としている。	Government Cloud Assistant Service
GDPR	GDPRはEUの一般データ保護規則で、EU居住者の個人データを扱う企業に目的明示や同意、削除請求対応、越境移転の管理などを義務付ける。域外企業にも適用される。	General Data Protection Regulation
GSS	政府機関が共通的に利用することを前提とした業務・情報システムやサービスの総称。共通業務を標準化・集約することで、効率化とコスト削減を図る。	Government Solution Service
IaaS	サーバやネットワーク、ストレージなどのIT基盤をサービスとして提供するクラウドサービスの形態。	Infrastructure as a Service
IaC	サーバーやネットワークなどのインフラ構成をコードで定義・管理する手法。自動化により再現性や効率、品質を高める。	Infrastructure as Code
IPsec	IPネットワーク上で送受信される通信を暗号化・認証し、安全に保護するための通信方式。	Internet Protocol Security
ISMAP	政府が利用するクラウドサービスのセキュリティ水準を評価・登録する制度。ISMAPに登録されたクラウドサービスのみが、原則として政府調達で利用可能となる。	Information system Security Management and Assessment Program
Kubernetes	業務アプリケーションを小さな実行単位（コンテナ）に分けて、サーバーで動かす際に、配置・起動・増減・復旧などを自動で管理してくれる基盤	
PaaS	アプリケーションを動かすためのOS・ミドルウェア等の実行環境や開発基盤を提供するクラウドサービスの形態。	Platform as a Service
SaaS	クラウドサービスプロバイダが提供する業務アプリケーションを利用するクラウドサービスの形態。	Software as a Service
SLA	サービスの品質や稼働率、サポート内容などを定めた合意事項。	Service Level Agreement
SOC2レポート	CSPにおいて、自社のシステムや運用が適切な内部統制・セキュリティ管理の下で行われていることを、第三者（監査人）が評価し、その結果をまとめた報告書	System and Organization Controls 2 Report
TLS	インターネット上で送受信されるデータを暗号化し、第三者による盗聴や改ざんを防ぐための通信保護技術。	Transport Layer Security
VPN	インターネットなどの公衆ネットワーク上に、論理的に分離された安全な通信経路を仮想的に構築する仕組み。	Virtual Private Network
あ行		
暗号アルゴリズム	情報を第三者に読まれたり改ざんされたりしないよう、あらかじめ決められた計算のルールに従ってデータを変換・保護する仕組み。	
オンプレミス	企業や組織が自社の施設（社内のサーバールームやデータセンター）内に、情報システムの機器やソフトウェアを設置・保有し、運用・管理する形態。	
オンプレミス拡張型クラウド	クラウド事業者が顧客拠点に専用設備を設置し、クラウドと同様の機能を提供・遠隔運用する形態のサービス。	（例）AWS Outpost、Azure stack 、Oracle Cloud@Customer
か行		
ガバメントクラウド	＜調達仕様書記載内容を抜粋＞ デジタル庁が整備する国と公共情報システム整備運用者が協同して利用することができるクラウド環境のことをいう。	
クラウドネイティブ	最初からクラウド環境での利用を前提に、クラウドの特性を最大限活かすよう設計・開発・運用されるシステムやアプリケーションの考え方。	
コンテナ	アプリケーションと、その実行に必要なプログラムや設定をひとまとめにし、OS上で独立したプロセスとして動作させる仕組み。	
さ行		
生成AI	文章や画像、プログラムコードなどを自動的に生成する人工知能技術。	
ソブリンクラウド	データやシステムの管理について、特定の国や組織の主権・法制度を確保できるクラウドサービスの形態。	
た行		
耐量子計算機暗号（PQC）	計算・解析能力の高い量子コンピュータでも解読されにくいことを前提に設計された暗号技術。	
データ主権	データが保存・処理される国や地域の法令・規制が、そのデータの取扱いに適用されるという考え方。	

（別紙）

警察情報システムの合理化・高度化に係る調査研究 用語集

用語	説明	備考
は行		
ハイブリッドクラウド	オンプレミス環境とクラウド環境を組み合わせ、役割分担しながら一体的に利用する構成・運用形態。複数のクラウドサービスを組み合わせたマルチクラウドを含める場合もあるが、本調査研究においては含めないこととする。	
パブリッククラウド	CSPが提供する共通のクラウド基盤を、インターネット等を通じて複数の利用者が利用する形態。	
プライベートクラウド	特定の組織や利用者だけが利用することを前提に構築・運用されるクラウドサービスの形態。	
米国クラウド法（Cloud Act）	米国の捜査当局が、犯罪捜査などの目的で、米国企業が管理するデータの提出を求めることを可能にした米国の法律	
ま行		
マネージドサービス	＜調達仕様書記載内容を抜粋＞ CSPが、インフラやミドルウェア等の運用や保守を代行し、クラウドサービスの利用者に提供するサービスのことをいう。	
マルチクラウド	複数のCSPが提供するクラウドサービスを、目的に応じて併用する利用形態	
や・ら・わ行		
ランサムウェア	コンピュータやサーバ内のデータを利用できない状態にし、元に戻すことと引き換えに対価（金銭等）を要求する悪意のあるソフトウェア。	