地方公共団体情報セキュリティポリシーに関する
ガイドラインの改定方針

総 務 省

令和６年７月

総務省自治行政局

デジタル基盤推進室

自己紹介

総務省自治行政局
住民制度課デジタル基盤推進室　課長補佐

ほり　しま　ゆづき
堀　島　佑　月

＜主な経歴＞

平成27年（2015年）　総務省入省、千葉県市町村課
～地方交付税関係、市町村からの問合せ対応　等～

平成29年（2017年）　行政管理局行政情報システム企画課

令和２年（2020年）　情報流通行政局地域通信振興課
～地域情報化アドバイザー関係、自治体AIガイドブック　等～

令和４年（2022年）　内閣官房内閣人事局

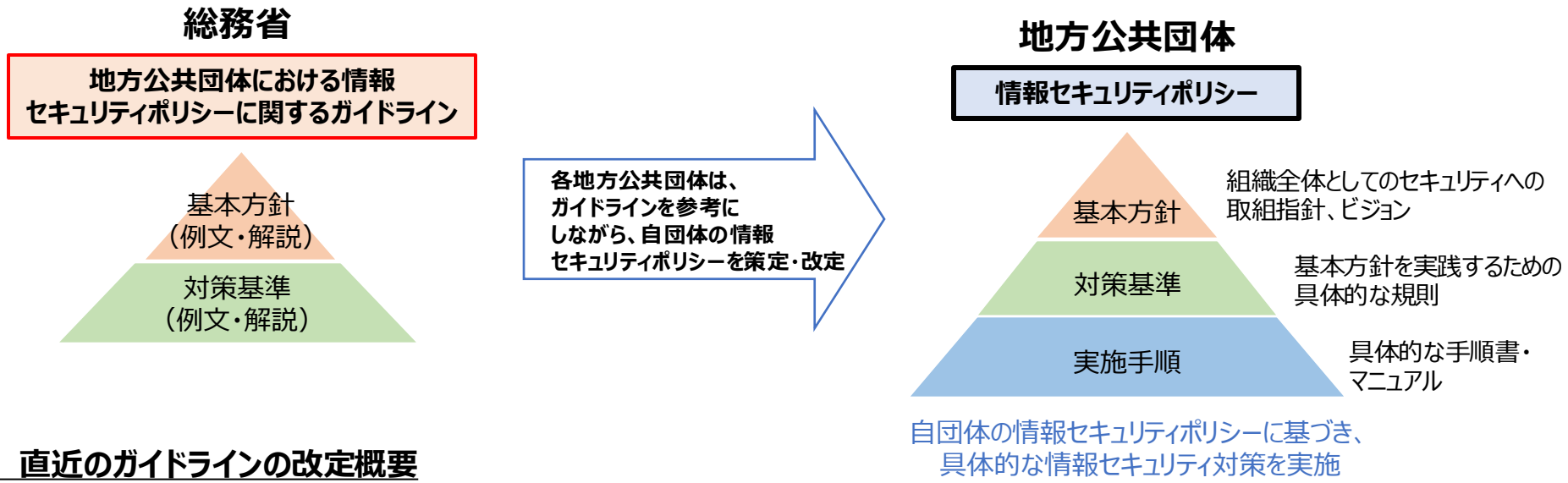
令和５年（2023年）　現職

1. ガイドラインの概要

「地方公共団体における情報セキュリティポリシーに関するガイドライン」について

１．概要

各自治体のセキュリティー対策の指針として総務省が策定し助言。国における情報セキュリティ対策の動向やデジタル化の動向等を踏まえながら、有識者検討会での議論を経て、**年度ごとに改定を実施**。



２．直近のガイドラインの改定概要

改定時期	改定内容・理由
平成27年３月	「行政手続における特定の個人を識別するための番号の利用等に関する法律（マイナンバー法）」、「サイバーセキュリティ基本法」の成立等の内容を反映
平成30年９月	平成27年の日本年金機構における情報流出事案を受け、総務省から地方公共団体へ要請を行った「三層の対策」等の情報セキュリティの抜本的強化策の内容を反映
令和２年12月	「三層の対策」の効果や課題、新たな時代の要請を踏まえ、セキュリティの確保と効率性・利便性向上の両立の観点から、情報セキュリティ対策の見直しを実施し、その内容を反映
令和４年３月	令和３年７月の「政府機関等のサイバーセキュリティ対策のための統一基準群」の改定や地方公共団体のデジタル化の動向を踏まえた内容を反映
令和５年3月	標準準拠システム等のクラウドサービスの利用を想定し、クラウドサービスを利用する際の具体的な情報セキュリティ対策の内容を第4編（特則）に反映

■ ガイドラインは、**学識経験者、自治体職員、システム調達契約や個人情報保護法に知見を有する弁護士が構成員となっている検討会で議論**。

検討会構成員（※令和６年３月時点）

石井　夏生利	中央大学国際情報学部教授
井上 茂	港区芝地区総合支所区民課長
上原 哲太郎	立命館大学情報理工学部教授
大高 利夫	藤沢市総務部情報システム課
岡村 久道	弁護士 国立情報学研究所客員教授
佐々木 良一	東京電機大学名誉教授兼 同大学サイバーセキュリティ研究所客員教授　【座長】
澁谷 展由	弁護士 弁護士法人琴平綜合法律事務所
庄司 昌彦	武蔵大学社会学部メディア社会学科教授
髙橋 邦夫	合同会社KUコンサルティング 代表社員 (元豊島区役所ＣＩＳＯ、一関市、北区等のCIO補佐官)
三輪 信雄	総務省最高情報セキュリティアドバイザー
山崎 晋一	横浜市デジタル統括本部企画調整部担当課長

（オブザーバ）デジタル庁、総務省サイバーセキュリティ統括官室、地方公共団体情報システム機構

（参考）ガイドラインの構成

- 地方公共団体が情報セキュリティポリシー（基本方針・対策基準）を策定、改定する際に、「第2編」の例文を参照し、活用することが可能な構成としている。
- 対策基準の例文の詳細な解説は、「第2編」の例文の構成と対応した内容で「第3編」に記載。
- クラウドサービス上で業務システムを利用する場合には、クラウドサービスの特性を踏まえた情報セキュリティ対策を考慮する必要があることから、「第4編」を特則として定めている。

編	項目	本編の主な内容	補足
第１編	総則	• ガイドラインの目的 • 地方公共団体における情報セキュリティとその対策 • 情報セキュリティ管理プロセス • 本ガイドラインの構成 • 対策レベルの設定 • クラウドサービスに関する留意点	• 情報セキュリティポリシーを策定するための前提となる事項を記載。 • 情報セキュリティポリシーの策定や改定のプロセス、クラウドサービスの留意点等を記載。
第２編	地方公共団体における情報セキュリティポリシー（例文）	• 情報セキュリティ基本方針（例文） • 情報セキュリティ対策基準（例文）	• 地方公共団体の基本方針、対策基準に定める文案の参考として、例文を記載。
第３編	地方公共団体における情報セキュリティポリシー（解説）	• 情報セキュリティ基本方針（解説） • 情報セキュリティ対策基準（解説）	• 第２編の例文と同様の構成で、具体的なセキュリティ対策の考え方を記載。
第４編	地方公共団体の情報システムのクラウド利用等に関する特則（例文・解説）	• 本編の目的 • 本編におけるクラウドサービスの範囲 • 本編における対策基準の構成 • 情報セキュリティ対策	• 標準準拠システム等のクラウド利用を行う場合に必要となる情報セキュリティ対策（対策基準）を、本編と同様の構成で例文と解説の形式で記載。
第５編	付録	• 権限・責任等一覧表	• 総務省セキュリティポリシーガイドラインで求められる役割を一覧で記載。

○「地方公共団体における情報セキュリティポリシーに関するガイドライン」（令和５年３月28日改定）

https://www.soumu.go.jp/menu_news/s-news/01gyosei07_050328.html

２．ネットワークモデルについて

「三層の対策」概要（従来型のαモデル）

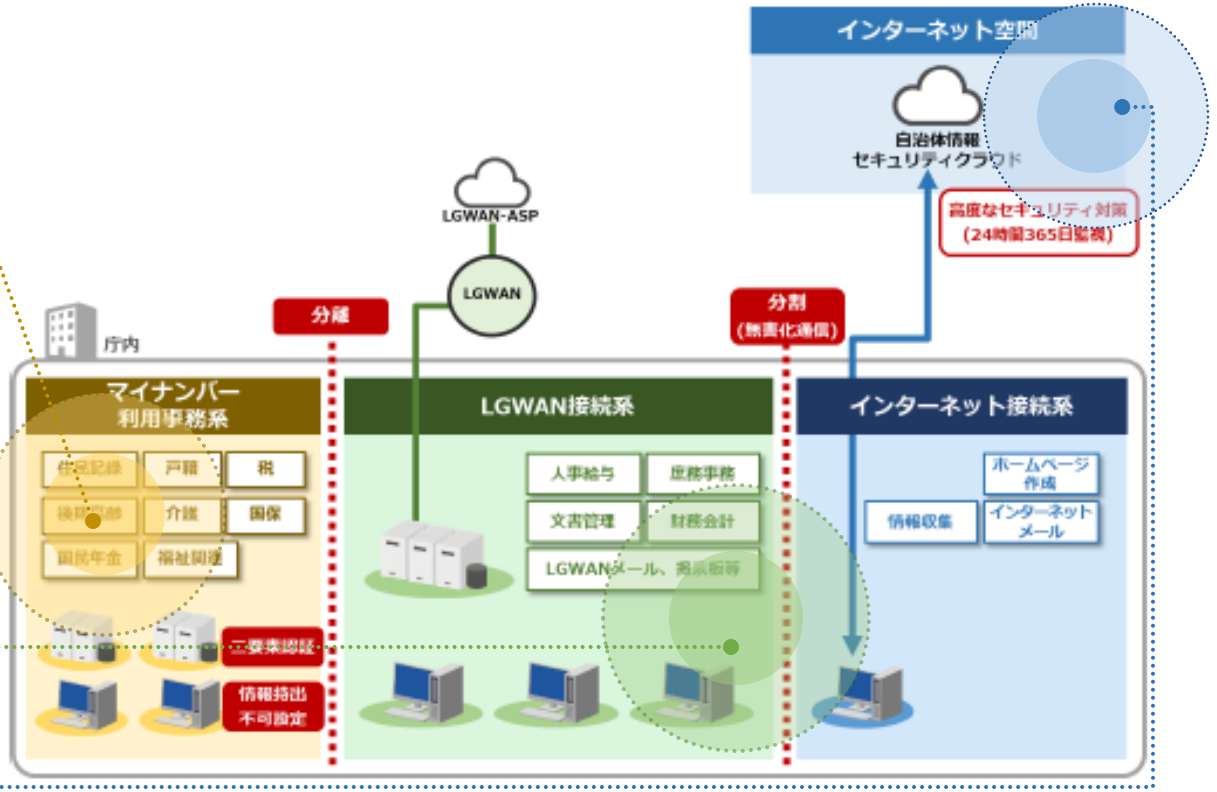
- 複雑・巧妙化しているサイバー攻撃の脅威により、地方公共団体の行政に重大な影響を与えるリスクが想定されるため、情報システムにおいては、機密性はもとより、可用性や完全性の確保にも十分配慮した、情報システム全体の強靭性の向上が求められる。
- **<u>情報システム全体の強靭性の向上を「三層の対策」により実現する</u>**。

三層の対策

1 マイナンバー利用事務系では、端末からの情報の持ち出し不可設定等を講じ、住民情報の流出を徹底して防止

2 LGWAN接続系とインターネット接続系を分割し、LGWAN環境のセキュリティを確保

3 都道府県と市区町村が協力して、自治体情報セキュリティクラウドを構築し、高度なセキュリティ対策を実施



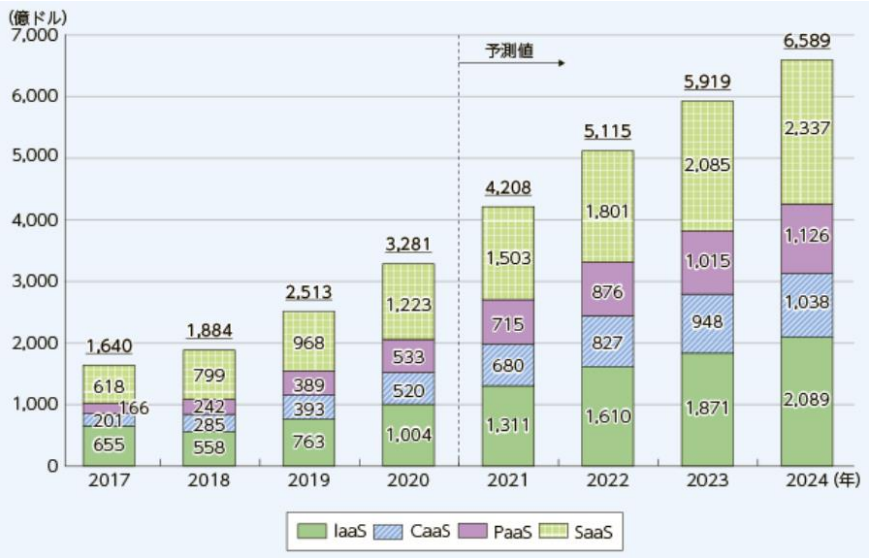
三層の構えによる自治体情報システム例（図表21）

クラウドサービスの増加

✓　Microsoft 365をはじめ、インターネット経由で利用することが必要なクラウドサービスが増加している。

＜情報通信白書　令和４年版（抜粋）＞

世界のパブリッククラウドサービス市場は、
2020年は35兆315億円（前年比27.9%増）となっている。

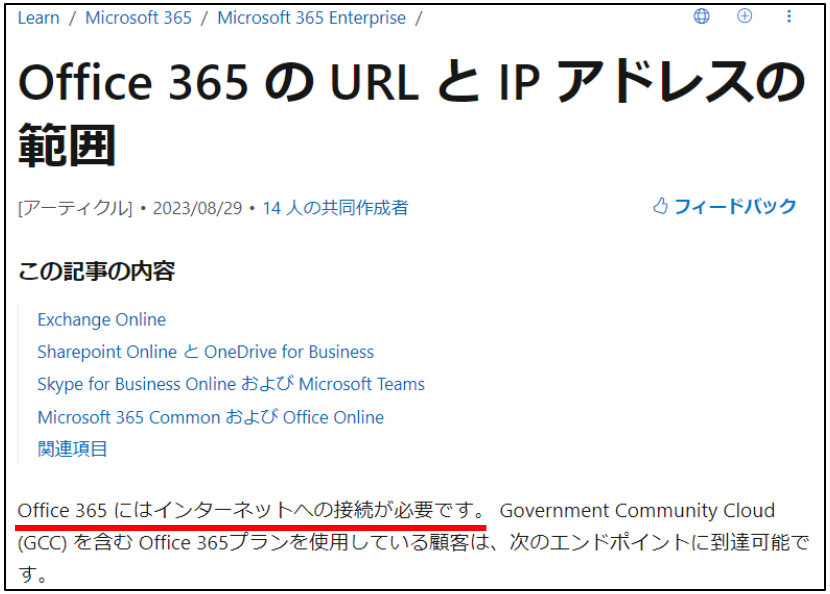


図表3-6-8-1　世界のパブリッククラウドサービス市場規模（売上高）の推移及び予測

- IaaS（Infrastructure as a Service）：インターネット経由でハードウェアやICTインフラを提供
- CaaS（Cloud as a Service）：クラウド上で他のクラウドのサービスを提供
- PaaS（Platform as a Service）：インターネット経由でアプリケーションを実行するためのプラットフォームを提供
- SaaS（Software as a Service）：インターネット経由でソフトウェアパッケージを提供

＜Microsoft 365の例＞

- Microsoft 365には、Word、Excel、PowerPointなどのOfficeアプリケーション、Web会議、ビジネスチャット、ファイル共有などのツールが含まれている。
- Microsoft 365の中の、メール（Outlookから接続して使うクラウドサービスであるExchange Online）やWeb会議（Teams）等のコミュニケーションサービス群であるOffice 365の通信要件は、右のMicrosoftのHPにおいて公開されており、**インターネットへの接続が必要**とされている。
- Word、Excel、PowerPointなどのOfficeアプリケーションについても、認証は一部インターネットへの接続が必要とされている。


Learn / Microsoft 365 / Microsoft 365 Enterprise /

Office 365 の URL と IP アドレスの範囲

[アーティクル] • 2023/08/29 • 14 人の共同作成者　フィードバック

この記事の内容

Exchange Online
Sharepoint Online と OneDrive for Business
Skype for Business Online および Microsoft Teams
Microsoft 365 Common および Office Online
関連項目

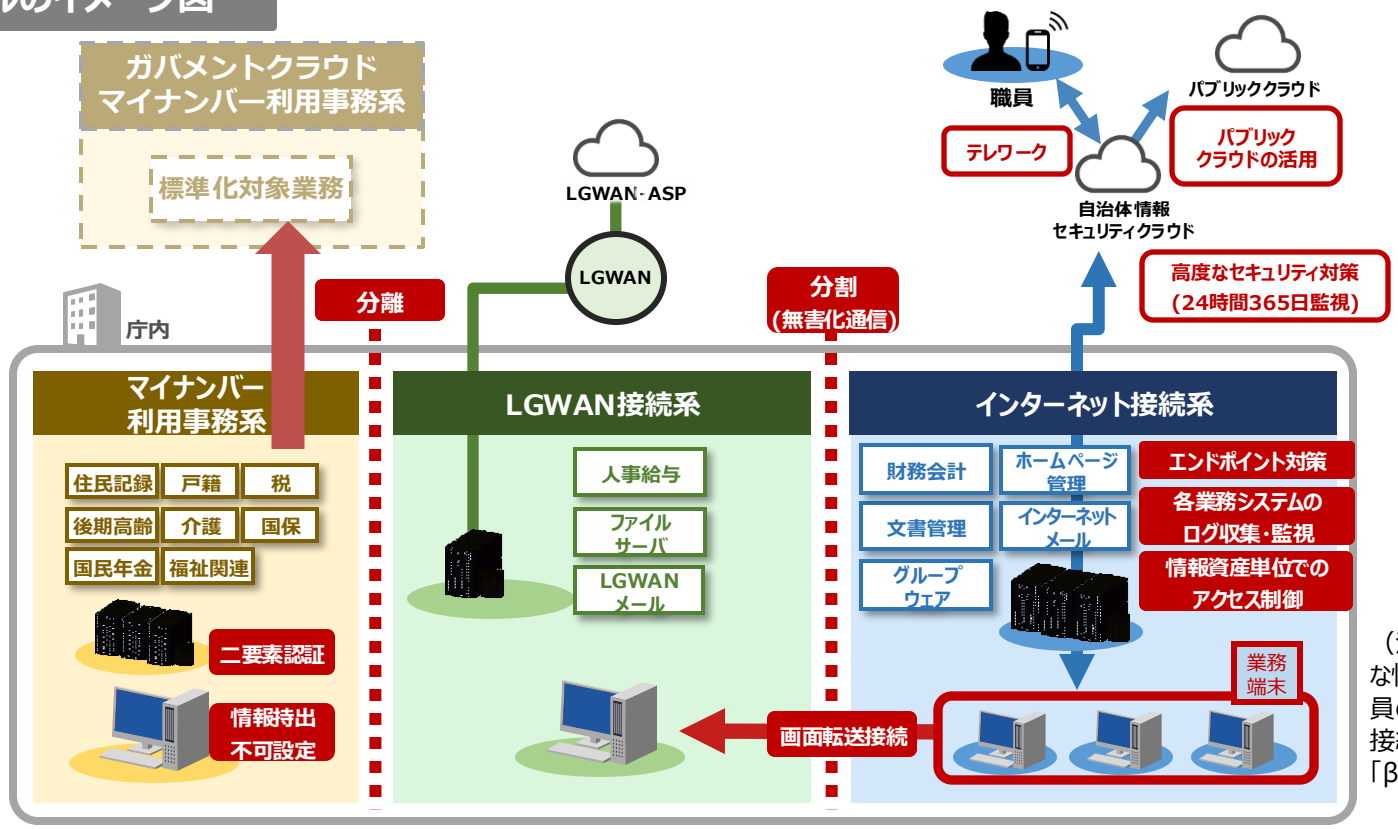
Office 365 にはインターネットへの接続が必要です。 Government Community Cloud (GCC) を含む Office 365プランを使用している顧客は、次のエンドポイントに到達可能です。

（URLは以下のとおり）
https://learn.microsoft.com/ja-jp/microsoft-365/enterprise/urls-and-ip-address-ranges

β´モデルについて

- ✓ 地方公共団体の業務で広く活用されているサービスがクラウド上で提供されるようになっており、インターネットと接続可能な領域に業務環境を配置する必要性が高まっていることを受け、インターネット接続系に業務端末・業務システムを配置したβ´モデルに対するニーズが高まっている。
- ✓ インターネット接続系の業務端末に対するエンドポイント対策、各業務システムのログ収集・監視など、従来の境界型防御にとどまらない追加のセキュリティ対策を行うことが求められる。

β´モデルのイメージ図



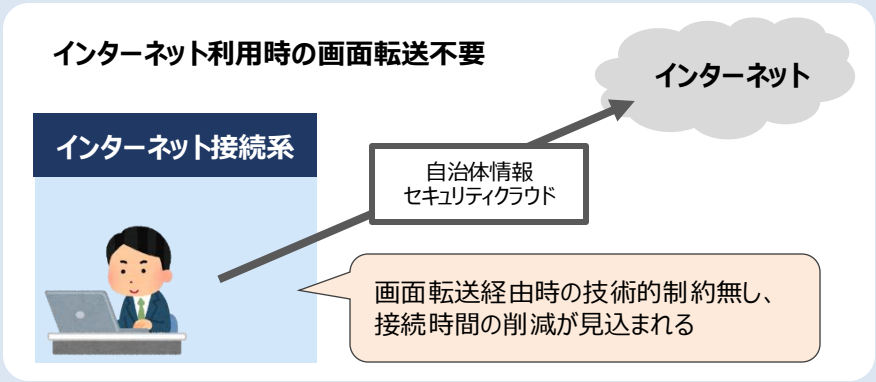
（注）βモデルのうち、重要な情報資産(入札情報や職員の情報等)をインターネット接続系に配置する場合は「β´モデル」としている。

※β´モデルの採用には、技術的対策に加え、緊急時即応体制の整備等の組織的・人的対策の確実な実施が条件

β´モデルのメリット（利便性）

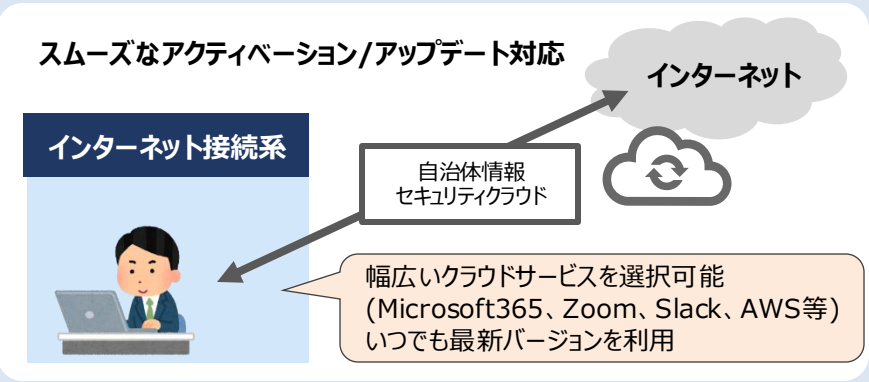
インターネットへの直接接続

- インターネット上のサイト、サービス、オンライン会議等を画面転送(VDI)経由ではなく一般のブラウザ（Microsoft Edge、Google Chrome等）で利用可能



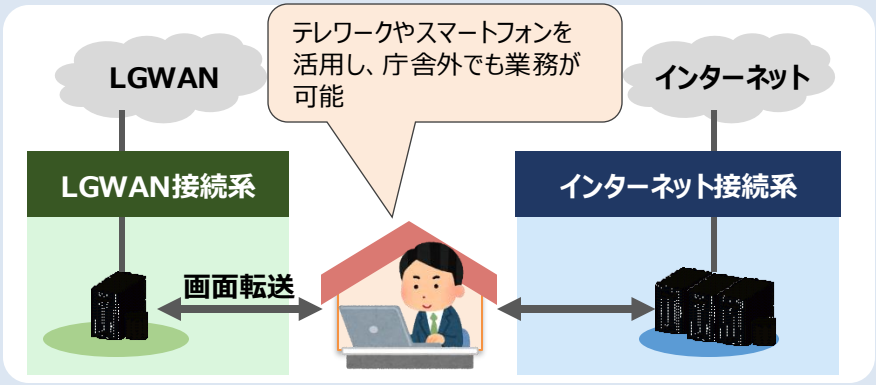
最新かつ多様なクラウドサービスの活用

- クラウドサービス利用時のアクティベーション(認証)がスムーズ
- 最新の資産、定義体ファイル等に随時更新可能
- ソフトウェアのアップデート対応自体が不要になる場合も



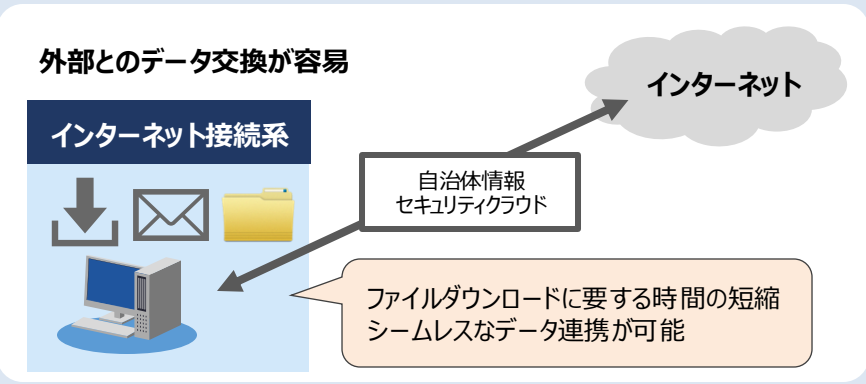
庁内/庁外用端末の統合

- 業務端末を集約し、効率の良い業務環境を実現
- バージョン管理や端末貸出し対応の負荷軽減
- テレワーク規模拡大により働き方改革にも貢献



同一セグメントでの業務完了

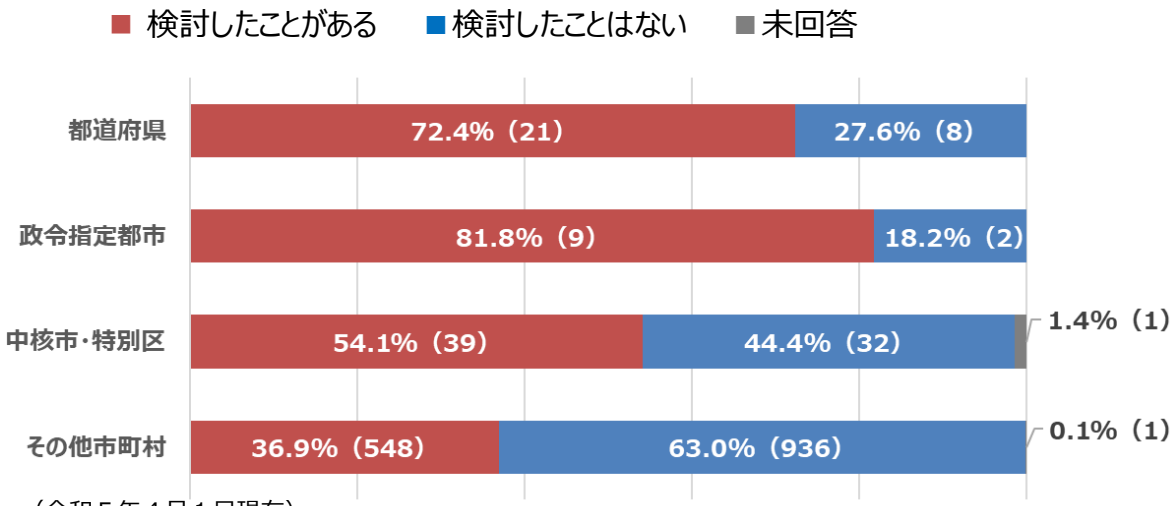
- 外部とのファイル交換やメールの送受信を同一セグメントで実施
（通常はファイルをLGWAN接続系に取り込む必要が無いため、無害化処理が不要となる※無害化処理を残す場合有り）



αモデルの団体がβ・β‘モデル移行を断念している理由

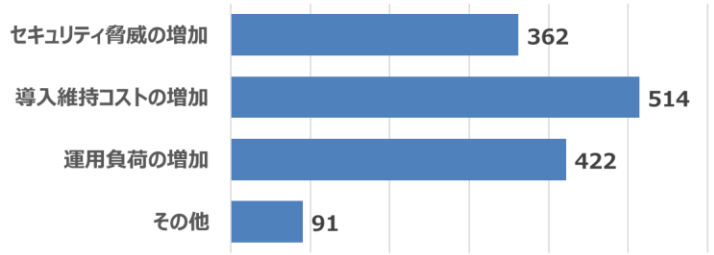
- ✓ **<u>αモデルの団体のうち、政令指定都市では約８割、都道府県では約７割、中核市・特別区でも半数以上がβモデル・β‘モデル移行を検討したことがある</u>**が移行に至っていない。
- ✓ 移行を断念する理由として、「導入・維持コストの増加」、「運用負荷増加」、「セキュリティ脅威の増加」が挙げられていた。他に、「移行のタイミング」や「情報資産の棚卸し」についても挙げられている。

α団体のうち移行を検討した割合（自治体分類別）



（令和５年４月１日現在）

β・β‘モデル移行の断念理由



（令和５年４月１日現在）

β・β‘モデル移行の断念理由：その他の意見

移行のタイミング

- 各システムの更改時期がことなるため、調整が難しい
- 標準化システムと改修タイミングが重なるため
- 次期端末入替のタイミングで移行したい
- 庁舎移転にあわせモデル移行することを検討する

外部監査

- 外部監査は小規模団体には対応困難なため
- 外部監査の対応する事務処理コストが大きいため

情報資産の棚卸

- 住民情報を多く扱う性質上、βモデルに向くのか判断が付かない
- LGWAN-ASPで業務を集約しており、インターネット接続系に業務システムが簡単に移行できない
- 情報システム機器等の配置や構成の根本的な見直しが必要となる

人材・スキル不足

- 職員のセキュリティ意識不足、β‘移行の舵取りできる人材不足

3. β‘モデル移行に係る支援

β'モデル移行に向けた手順書

✓ β'モデル導入を検討する自治体が、計画的に円滑に移行を進められるように、作業項目やフェーズ毎に想定される主な作業手順、自治体の事例を移行手順書として提示。

手順１．全体分析

（１）ネットワーク・業務システムの現状把握
（２）LGWAN接続系に残す業務システム等の検討
（３）LGWAN接続系に残す業務システム等の利用方法の検討

手順２．β´モデルに移行した場合のネットワークの設計及び関連システムの整備

（１）β´モデルのネットワーク設計
（２）既存システムの改修に係る影響範囲の特定と対応方針の検討
（３）β´モデル移行に合わせて行う施策の整理と検討

手順３．移行プロセスの検討と移行作業

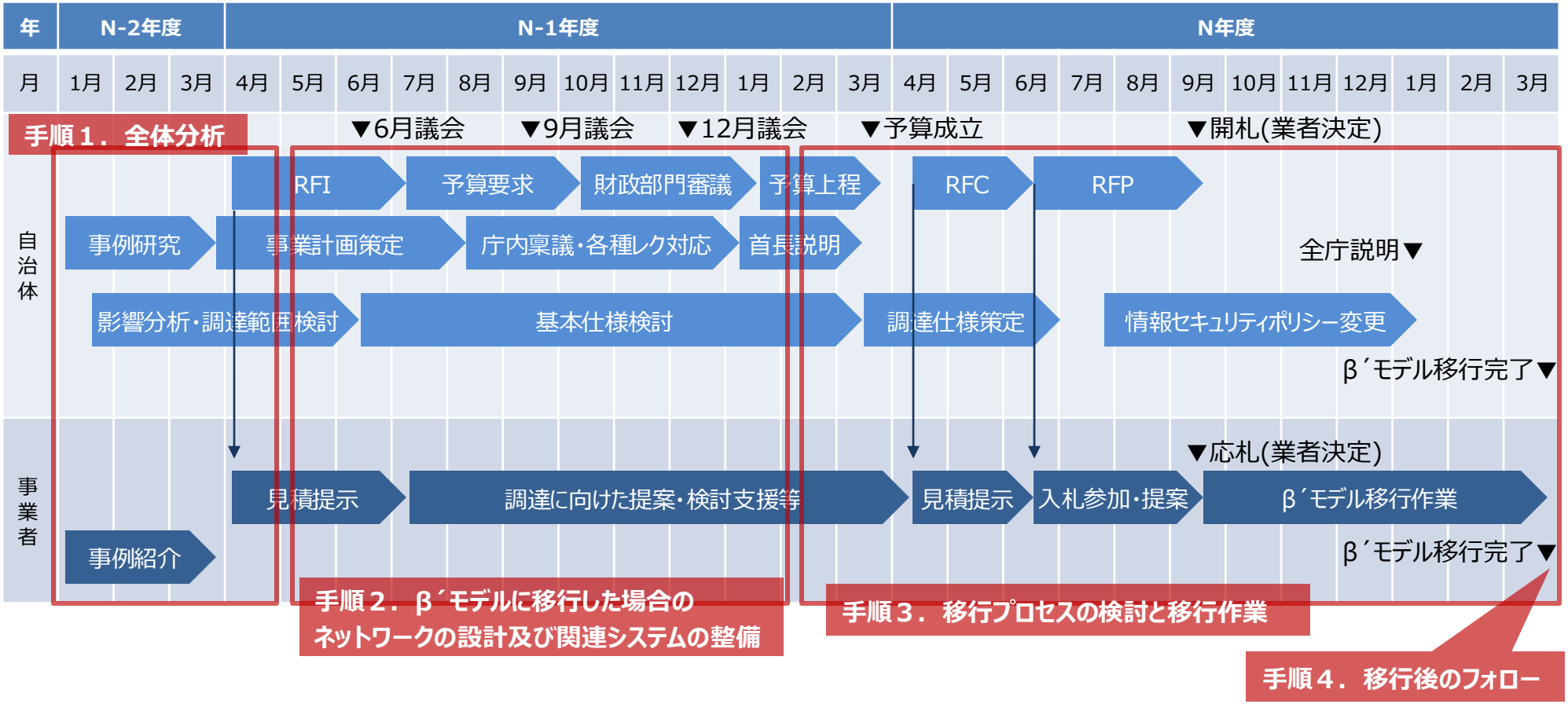
（１）移行プロセスの検討
（２）移行作業及び進捗管理
（３）各利用者に対する説明・周知

手順４．移行後のフォロー

（１）移行作業の前段のテストにおいて発生する技術課題等の対応
（２）実運用後の通信不可等の事象等への対応
（３）実運用における質疑応答等をもとにしたＦＡＱ等の速やかな作成展開等

移行プロジェクト推進における全体スケジュール（例）

・β ‘モデル移行までの予算化および予算化後の作業プロセスについて、スケジュールを記載。
（職員数：10,000人規模）



手順書のアプローチ

β´モデル移行時に課題とされる事項に対し、先行事例(既にβ´モデルへの移行を完了された団体)に基づき、検討時の参考となるよう、本書にて情報を整理し、解説する。

検討に係るノウハウ・人材不足	β´モデル移行に向けた事業計画策定の基本的な考え方、移行プロセスについて、先行事例を参考に記載する。
セキュリティ対策の強化	ガイドラインにおいて、β´モデルに必要とされるセキュリティ対策において、地方公共団体でしばしば課題として聞かれる要件について、システム構成の設計時、製品選定時の考慮ポイントを解説し、先行事例を参考として記載する。
移行に係るコスト増加	コスト低減に資する工夫、踏まえるべき観点等を先行事例から参考として記載する。
適切な移行時期の見極め	先行団体が選択した移行タイミング、判断根拠から、踏まえるべき観点を整理の上、参考として記載する。

移行に係るコスト低減について

（１）コスト低減に係る施策・アイデア（例）

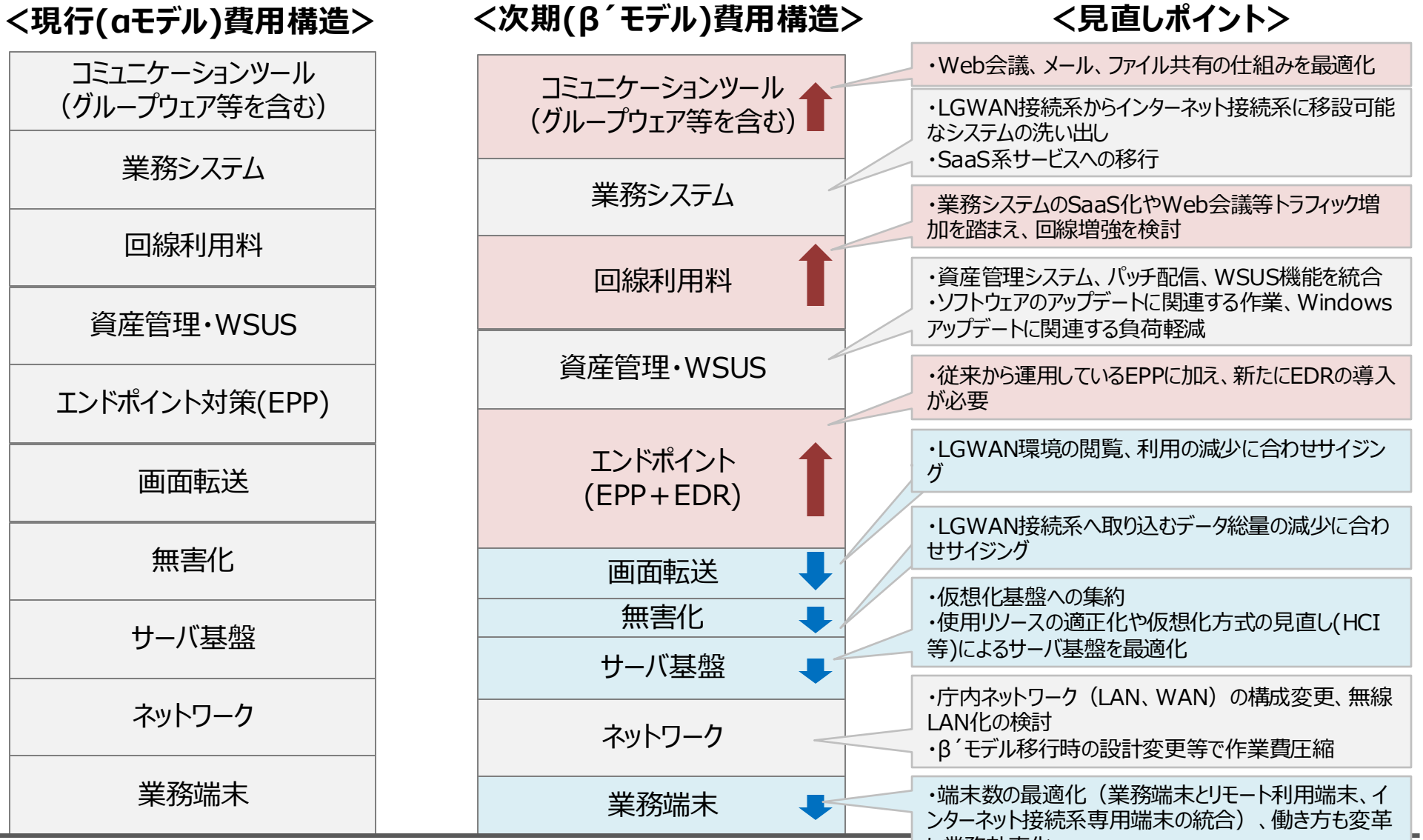
・共同利用での調達や**自治体情報セキュリティクラウドが提供するオプション機能などを有効活用**する。
・各セキュリティ機能単位で別々に調達、導入することも可能だが、**同一メーカーで包括的にセキュリティ機能を安価に実装できる場合がある**。ただし、この場合は将来に渡って、ベンダロックインとならないよう配慮する必要がある。
・LGWAN接続系に極力業務システムを残さない設計思想に基づくことで、**LGWAN接続系を閲覧するための画面転送(仮想端末)の数を最小化させ、トータルでのコスト低減を実現する**ことが可能。
※例）全職員分→LGWANを日常的に使う人数のみにライセンス数を削減可能
・画面転送の実装においては、様々な方式を選択肢に入れることでコスト低減となる可能性がある。

（２）費用対効果の試算にあたって

・**事業計画は、働き方改革（クラウドサービスの利活用、コミュニケーション基盤の刷新、テレワークの拡大等）を目的とし、ネットワークモデルの変更はその手段として位置付ける**ものが多い。
・先行自治体の例では、β´モデル移行後のメリットについて、**定量的な試算**も見られた。
※例）インターネット閲覧時における、起動時間等の削減
起動時間 × 全職員数 × 年間勤務日 × 平均時給/60分 ＝ 人件費削減　（机上の計算）
・β´モデルに移行した自治体の実施後庁内アンケートなどでは、**利便性の向上や働き方が大きく改善した**との回答もあった。(移行前は十分にイメージできなかった業務効率化も、実際に移行した後はメリットとして実感される場合がある)
・インターネットサービスの活用についても、より利用しやすい環境に変わることで、**職員が自ら創意工夫し、「移行前には想定していなかった効果が得られた」といった声も聞かれた**。

【参考】αモデル→β'モデル移行時の費用構造イメージ

- ✓ β´モデル移行におけるコストの増大については、現状の環境における予算配分に見直しにより一部費用をまかなえる可能性がある。
- ✓ 現在の業務システム状況の把握にあたっては、各原課へのヒアリング等が必要となる。



※各予算項目の大きさは相対的な金額規模を表すものではありません。

手順書のアプローチ

β´モデル移行時に課題とされる事項に対し、先行事例(既にβ´モデルへの移行を完了された団体)に基づき、検討時の参考となるよう、本書にて情報を整理し、解説する。

検討に係るノウハウ・人材不足	β´モデル移行に向けた事業計画策定の基本的な考え方、移行プロセスについて、先行事例を参考に記載する。
セキュリティ対策の強化	ガイドラインにおいて、β´モデルに必要とされるセキュリティ対策において、地方公共団体でしばしば課題として聞かれる要件について、システム構成の設計時、製品選定時の考慮ポイントを解説し、先行事例を参考として記載する。
移行に係るコスト増加	コスト低減に資する工夫、踏まえるべき観点等を先行事例から参考として記載する。
適切な移行時期の見極め	先行団体が選択した移行タイミング、判断根拠から、踏まえるべき観点を整理の上、参考として記載する。

適切な移行時期の見極めについて

- 移行のタイミングは各団体の調達サイクルや取り巻く環境により異なることが想定される。これまでにβ´モデル移行を実施した先行自治体の事例から、想定される６つの移行タイミングについて例示する。
- 環境変更の検討には一定の期間が必要であるため、予め相当期間を見積っておくことも重要である。

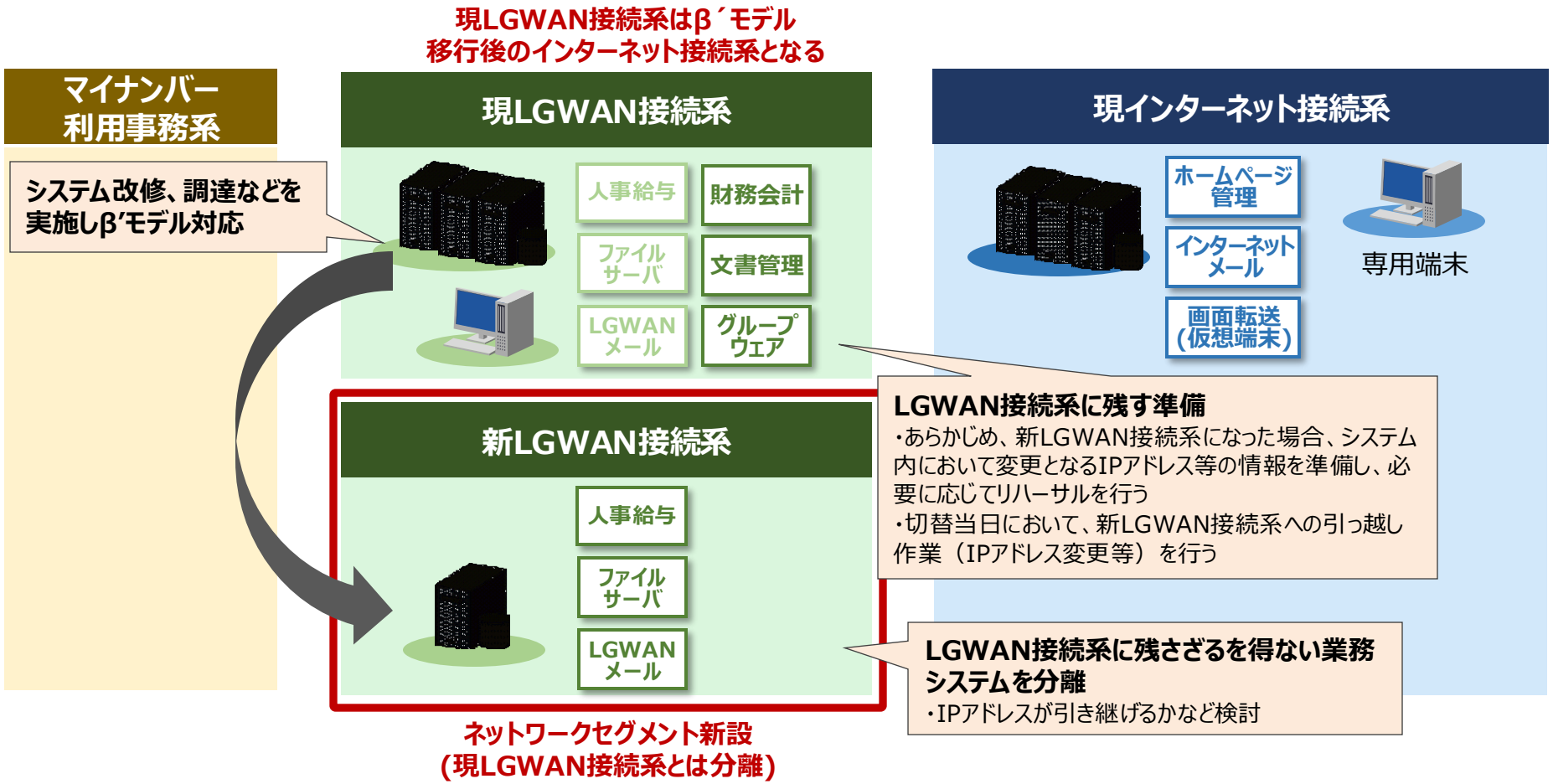
移行タイミング	想定される概要
庁内ネットワーク更改時	• 次期庁内ネットワーク更新に合わせ、ネットワークモデルの検討を行い、β´モデル移行するケース。 • 庁内無線LAN化、庁舎建て替え等を機会に庁内ネットワークの見直しが発生する場合もある。 ※β´モデルに移行するタイミングにおいて、比較的多いケースと考えられる。
セキュリティ強靭化システム（画面転送/無害化等）更改時	• 三層分離を実施する際に導入した仮想環境、無害化システム等の更新時にβ´モデルに移行するケース。 • 現状αモデルでインターネットをVDIで閲覧している場合に、β´モデルに移行することでVDIライセンスの大幅な削減が可能となる等、VDI更新が機会となる可能性がある。 ※β´モデルに移行するタイミングにおいて、比較的多いケースと考えられる。
業務端末更改時	• 端末更新を機にインターネット接続系に業務端末を配置するケース、あるいはモバイルワークシフトに合わせて庁内ネットワークも見直すケース。 • LGWAN接続系とインターネット接続系で端末分離している場合、端末調達を機に台数の最適化を行いインターネット接続系に集約することも想定される。
統合仮想基盤更新時	• 業務システムやセキュリティ関連システムが同一のインフラ基盤上で稼働している場合で、仮想基盤の更改時にβ´モデルに移行するケース。 • メリットとして、業務システム環境設定がネットワーク変更と同時に行える点が考えられる。
クラウドサービス接続時	• クラウドサービス（グループウェア、Web会議、コミュニケーション基盤、クラウドストレージ等）の利用開始時期に合わせ、β´モデルへの移行を実施するケース。
新たに移行日を設定	• 既存システムの調達サイクルは意識せず、最短で移行可能な時期を設定する場合や、業務影響が最小化されるタイミングを見計らって移行するケースなどが考えられる。

移行ステップ１

先行事例で多くみられる移行ステップについて、そのプロセスを参考として解説する。

ステップ１．新LGWAN接続系を構築

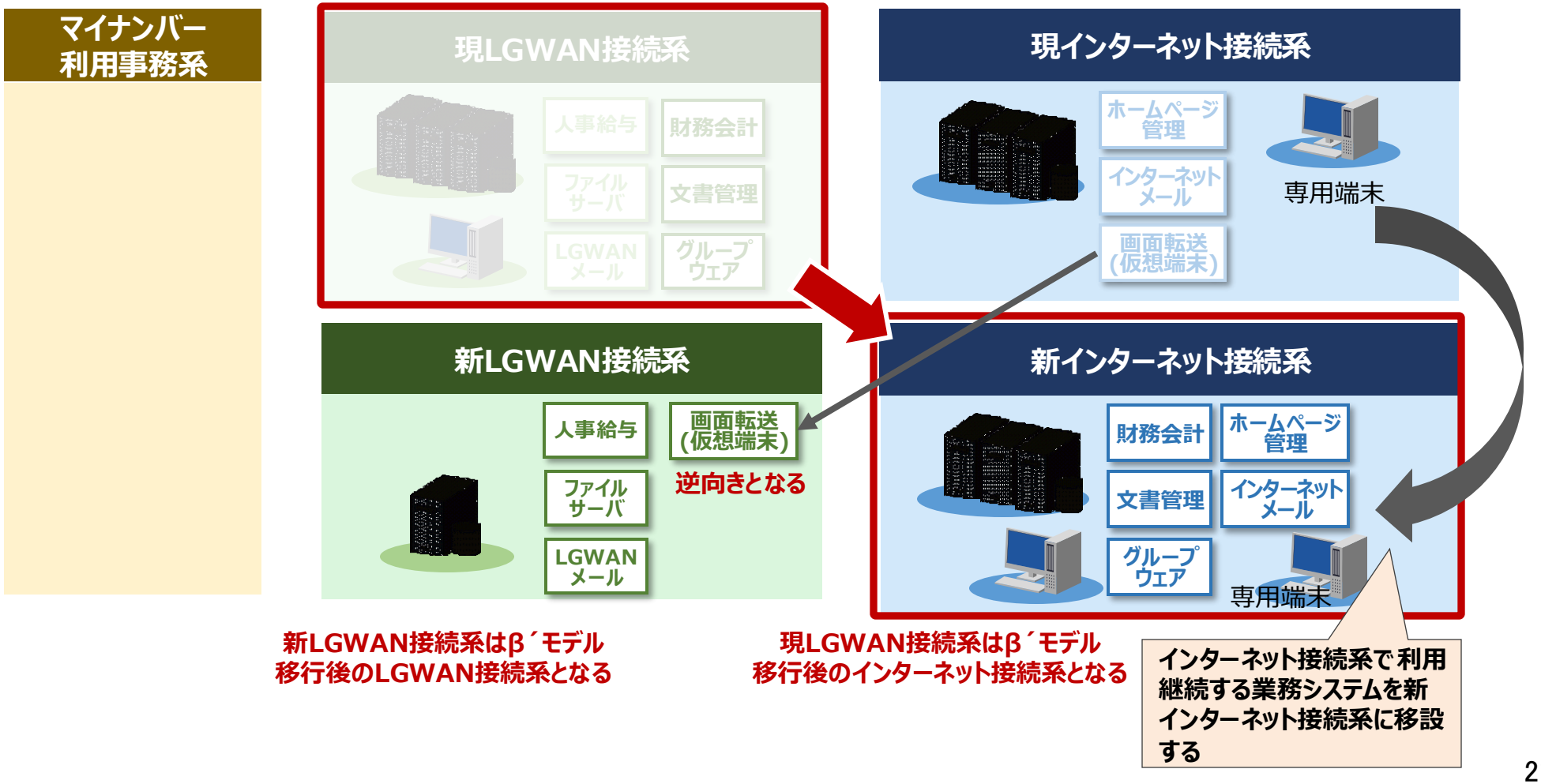
・β´モデル移行後は、現LGWAN接続系のIPアドレス体系をインターネット接続系に読み替える前提の計画
・新LGWAN接続系(β´モデル移行後のLGWAN接続系)を新設し、LGWAN接続系に残すシステムを配置する



移行ステップ２

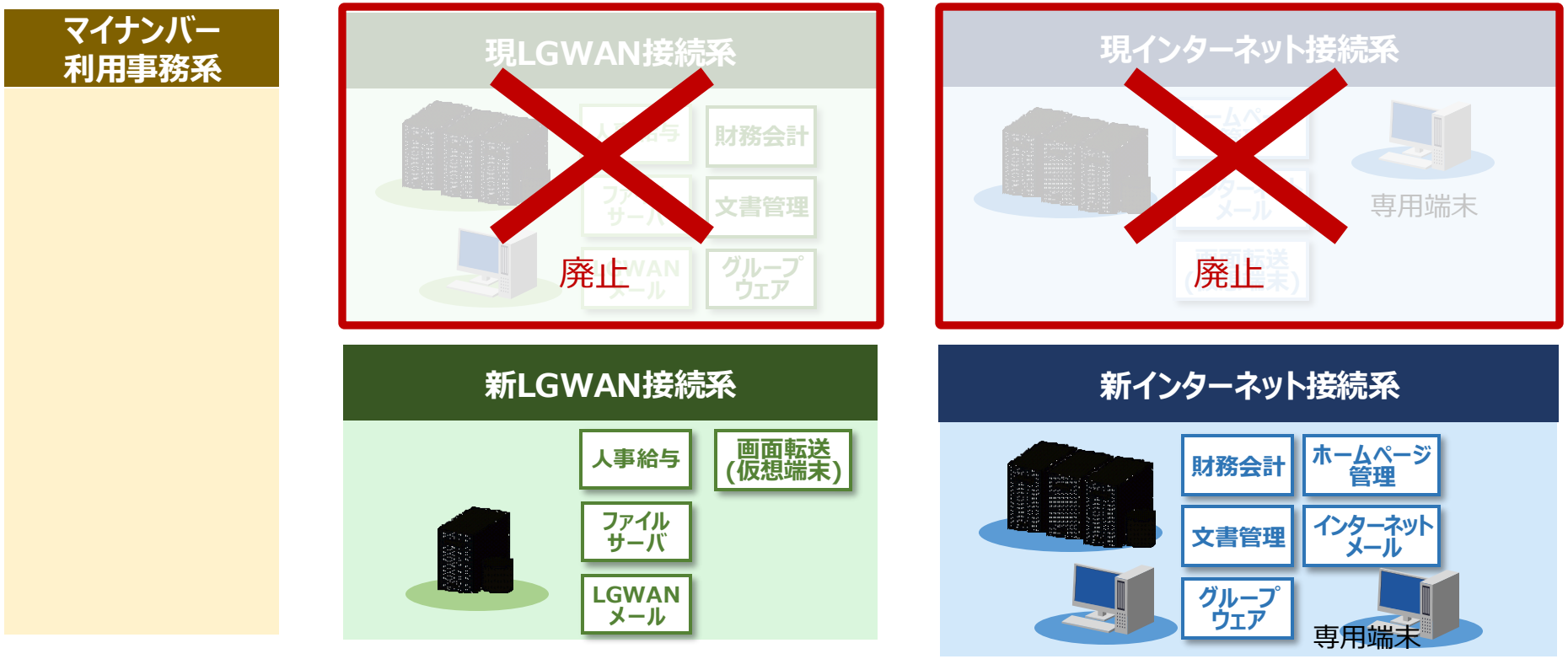
ステップ２．現LGWAN接続系を新インターネット接続系に移行

・引っ越し後（ほぼ同じタイミング）において、旧LGWAN接続系のIPアドレス体系を、インターネット接続系の体系として変更し、動作確認を実施。
・前行程のステップ１とステップ２は、時系列ではほぼ同一のアクションとなる場合が多い。



ステップ３．現LGWAN接続系及び現インターネット接続系の廃止

・現LGWAN接続系及び現インターネット接続系を廃止し、マイナンバー利用事務系、新LGWAN接続系、新インターネット接続系の３系統となる。
・マイナンバー利用事務系は変更対象とはならない。



β′モデル団体の例（三重県）

項目	内容
区分（都道府県市町村）	都道府県
団体の規模（職員数）	約23,000人
移行方式	一括移行（業務端末および業務システムを一度に移行）
EDR共同の実施有無	実施中
β´モデル移行の目的	・徹底的な業務効率化、生産性の向上（※） ・データ利活用による新サービス創出 取組１：クラウドシフトによるコミュニケーションの活性化 取組２：ゼロトラストと柔軟な働き方の実現 取組３：データドリブンの実現に向けた活用の推進 ※インターネット利用に係る業務の効率化（画面転送、無害化処理の見直し）。職員の業務環境が大幅に改善されることに伴い、住民への情報提供、回答も迅速化し、行政サービス向上となる。

- **工夫した点**

＜人材のスキル面＞
・ネットワークに関するノウハウを持つ人材の確保
＜委託事業者の活用＞
・既存ネットワークの設計ノウハウを生かした再設計
＜セキュリティ対策＞
・EPP,EDRによるエンドポイント対策
・（追加要素）SASEの導入によりゼロトラストの考え方に基づいたテレワーク環境の導入
・インターネットアクセスに関し、αモデル時は仮想端末経由であったが、β´モデル時は端末直接接続に変更となっている。ただし、同じProxy経由でのアクセスとしたため、都道府県セキュリティクラウド側の設定変更が生じなかった。庁内に設置したProxyの設定変更（端末からの直接アクセスを許可）とスペック増強は必要であった。
＜予算申請＞
・予算当局への丁寧な説明

β'モデル団体の例（団体B）

項目	内容
区分（都道府県市町村）	市町村
団体の規模（職員数）	約700人
移行方式	一括移行（業務端末および業務システムを一度に移行）
EDR共同の実施有無	未実施
移行のきっかけ （業務の課題、市民からの期待等）	既存のネットワーク機器サポート終了に伴うネットワーク更改が必須となり、同時期に国のセキュリティポリシーに関するガイドラインが改定されたことにより、新たなセキュリティ強化モデルの検討が可能となったため。

- **工夫した点**

＜人材のスキル面＞
・当自治体職員は数年おきの異動が想定されるため、新規配属された職員でも、基礎的な対応はできるように、運用に関するドキュメントを納品前に職員のチェックを行った。
・ユーザー目線に立ち、研修開催だけでなく、グループウエア等に適宜、利用に関する情報を掲載した。
＜委託事業者の活用＞
・一般的な設計構築委託や新規製品の説明にとどまらず、新規製品のテスト、当自治体においての向き・不向き、実運用上懸念される課題について、ほぼ毎週打合せを行い、業者のノウハウを職員に浸透させるようにした。
＜セキュリティ対策＞
・特段新たなものはなく、一般的なセキュリティ対策の積み上げ。セキュリティクラウドによる外部からのデータのチェック、端末管理ソフトによる許可されたUSBメモリ以外の利用制限、イントラネット側への許可された端末のみの接続制限、週毎のウイルス対策ソフトの定時スキャン等）。金額面、運用面を考慮し、セキュリティクラウドで提供されるEDRを導入した。
＜予算申請＞
・内部情報ネットワークの更改が必須の状況下において、国のセキュリティポリシーに関するガイドライン改定によりβ、β´モデルの検討が可能となったことから、αモデル継続とβ又はβ´モデル採用との比較検証を行い、特に国が今後目指す方向性や導入に係るコスト増を上回る運用メリット等の説明を綿密に行った。

4. 中間報告の概要

中間報告のポイント（要点）

- 政府統一基準の改定や地方公共団体におけるクラウドサービス利用拡大を踏まえ、令和６年３月にガイドラインの改定の方向性を中間報告として提示。
- 主に「**クラウドサービスの利用に対する対応**」、「**業務委託先管理の強化**」、「**サイバーレジリエンスの強化等**」の３つの観点が盛り込まれている。

1. クラウドサービスの利用に対する対応

- Web会議等の目的で、LGWAN接続系の業務端末からインターネット経由で、特定のクラウドサービスを安全に利用するための対策（アクセス制御等）をα'モデルとして規定。

2.業務委託先管理の強化

- 業務委託契約時、業務委託の実施期間中、終了後に取るべき対策について、地方公共団体で実施すべき対策・委託先に求めるべき対策をそれぞれ規定。

3.サイバーレジリエンスの強化等

- サイバー攻撃を受けることを念頭においた対策の強化として、バックアップ等の要件を追記。
- 昨今のサービス不能攻撃(DDoS攻撃)を踏まえた対策について記載。
- ゼロトラストアーキテクチャを実現する機能の一部と考えられる「動的なアクセス制御」に関する記載。
- 機器・ソフトウェアの利用時の対策の強化

現時点における改定案の構成

- ✓ **政府統一基準群の改定**に伴い、**第１編から第４編に至るまで、多くの項目について改定予定**。
- ✓ 第３編「３.情報システムの全体の強靭性の向上」において、**αモデルでローカルブレイクアウトを行いクラウドサービスを利用する際のセキュリティ要件**を追記予定。

第１編　総則
- 第1章　本ガイドラインの目的等
- 第2章　地方公共団体における情報セキュリティとその対策
- 第3章　情報セキュリティの管理プロセス
  - 1. 策定及び導入
  - 2. 運用
  - **3. 評価・見直し**（変更）

第２編・第3編　地方公共団体における情報セキュリティポリシー（例文・解説）
- 第1章　情報セキュリティ基本方針
  - **8. 情報セキュリティポリシーの見直し**（変更）
- 第2章　情報セキュリティ対策基準
  - 1. 組織体制
  - 2. 情報資産の分類と管理
  - **3. 情報システム全体の強靭性の向上**（変更）（α'モデル追記）
  - 4. 物理的セキュリティ
    - 4.1 サーバ等の管理、 4.2 管理区域（情報システム室等）の管理
    - **4.3 通信回線及び通信回線装置の管理**（変更）
    - 4.4 職員等の利用する端末や電磁的記録媒体等の管理
  - 5. 人的セキュリティ
    - 5.1 職員等の遵守事項、 5.2 研修・訓練
    - **5.3 情報セキュリティインシデントの報告**（変更）
    - 5.4 ID及びパスワード等の管理
  - 6. 技術的セキュリティ
    - **6.1 コンピュータ及びネットワークの管理**（変更）
    - **6.2 アクセス制御**（変更）
    - **6.3 システム開発、導入、保守等**（変更）
    - 6.4 不正プログラム対策、 6.5 不正アクセス対策
    - **6.6 セキュリティ情報の収集**（変更）
  - 7. 運用
    - **7.1 情報システムの監視**（変更）
    - 7.2 情報セキュリティポリシーの遵守状況の確認～ 7.6 懲戒処分等
  - **8. 業務委託と外部サービス（クラウドサービス）の利用**（見出し変更）
    - **8.1 業務委託**（変更）
    - **8.2 情報システムに関する業務委託**（新規作成）
    - **8.3 外部サービス（クラウドサービス）の利用（機密性２以上の情報を取り扱う場合）**（変更）
    - **8.4 外部サービス（クラウドサービス）の利用（機密性２以上の情報を取り扱わない場合）**（変更）
  - 9. 評価・見直し
    - **9.1 監査**（変更）
    - 9.2 自己点検
    - **9.3 情報セキュリティポリシー及び関係規程等の見直し**（変更）

第4編　地方公共団体におけるクラウド利用等に関する特則
- 第1章　本編の目的について
- 第2章　本編におけるクラウドサービスの範囲について
- 第3章　本編における対策基準の構成について
- 第4章　情報セキュリティ対策について
  - 1. 組織体制～ 7. 運用
  - **8. 業務委託と外部サービス（クラウドサービス）の利用**（見出し変更）
  - 9. 評価・見直し

中間報告のポイント（クラウドサービスの利用に対する対応①）

「第２編 第２章 情報セキュリティ対策基準（解説）3. 情報システム全体の強靭性の向上」を参照

改定箇所	主な記載内容
α'モデルの規定	● 主に外部のクラウドサービスの利用を目的として、LGWAN接続系から接続先にローカルブレイクアウトする構成として、α'モデルを規定。 ● 本モデルの採用を検討する際に、留意すべき観点として、以下を記載。 • **地方公共団体は、その保有する情報資産を守るにあたり、自ら責任を持ってセキュリティを確保すべきものであることを改めて認識する**ことが重要 • **利用可能なクラウドサービスは、ISMAP管理基準を満たし、ISMAPクラウドサービスリストに登録されているサービス**とする。ただし、利用するクラウドサービスがISMAP登録サービスであっても、当該サービスのローコードツール等を用いて、**地方公共団体自身の責任で個々のサービスを設計、構築する場合は、セキュリティについても個別に検討し、必要な対策を実施する必要**がある • **接続先制限やアクセス制御、テナントアクセス制御等の技術的対策が必要**となる。また、テナントアクセス制御を適切に行うため、接続先のクラウドサービスにおける設定に誤りがないか、定期的な確認に加え、アップデートに伴う仕様変更の際の確認を行うことが必要。 ● α'モデルを利用する場合においては、**利用するクラウドサービスのサービス範囲に応じて、セキュリティ対策を検討する必要がある**ため、以下の通り、**最も基本的な３つのケースについてセキュリティ要件を規定**。 • **（ア）認証・ウイルス定義体の取得のみの場合** • **（イ）コミュニケーションツールを利用するが、ファイルを内部に取り込まない場合** • **（ウ）コミュニケーションツールを利用し、外部とファイル送受信を行う場合** ※セキュリティ要件はサービス利用範囲を踏まえて、個別に検討する必要があり、最終的には地方公共団体の責任でもって実施すること

資産ベースのリスク分析（α'モデルの分析）について

- ✓ リクスアセスメントは、**「制御システムのセキュリティリスク分析ガイド　第２版　～セキュリティ対策におけるリスクアセスメントの実施と活用～」（2023年３月IPA）に沿って実施**。
- ✓ 上記ガイドに記載されている、資産ベースのリスク分析は、保護すべき制御システムを構成する資産群を明確化し、各資産に対するシステム構成上及び運用管理上に想定される脅威について、各資産の重要度と、その脅威の発生可能性と受容可能性（脆弱性）の相乗値によって、資産のリスクを評価するリスク分析手法である。
- ✓ なお本リスクアセスメントは、情報処理安全確保支援士が、その倫理綱領に従い、公正な立場で実施したものである。

資産ベースのリスク分析の流れ

順番	作業の概要
①	**資産の定義とその重要度を定義する** 分析対象の資産を、物理的なまとまりや論理的な機能単位（サーバ、端末、装置等）の観点で定義すると共に、各資産の重要度を定義する。
②	**各資産に対する脅威とそのレベルを定義する** 脅威レベルの判断基準を定義し、その基準を基に、各資産に対して、資産の機能、ネットワーク構成や利用環境等を考慮して、想定される脅威とその脅威レベル（それが実行される可能性）を定義する。
③	**資産の各脅威に対する脆弱性を評価する** 各脅威に対するセキュリティ対策の各資産における対策状況（対策レベル）を評価することにより、当該脅威に対する脆弱性を評価する。
④	**各資産の脅威に対するリスク値を算定する** ①と②③の相乗値によって、各資産の各脅威に対するリスク値を算定する。

出典：「制御システムのセキュリティリスク分析ガイド第２版」（2023年３月　IPA）
https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

（参考）対策レベルとリスク値

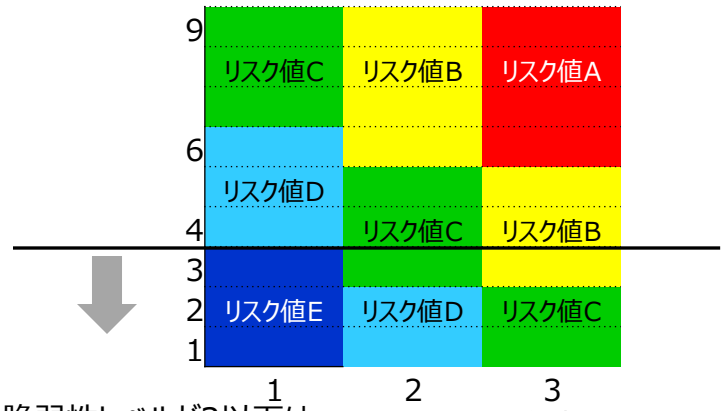
- ✓ 脅威レベルが最も高い3（脅威が発生しやすい）であっても、十分な対策により脆弱性が１であれば、脅威レベル×脆弱性レベル＝3となり安全である。
- ✓ 対策が不十分で脆弱性が3であっても、脅威レベルが最も低い1(脅威が発生しにくい）であれば、脅威レベル×脆弱性レベル＝3となり安全である。

対策レベルと脆弱性レベルの対応

対策レベル	判断基準	脆弱性レベル
3	当該脅威（攻撃手段）において、複数の「防御」「検知／被害把握」可能な対策項目を多層で実施しており、攻撃が成功する可能性は低い。（即ち、○が二つ以上）	1
2	当該脅威（攻撃手段）において、「防御」「検知／被害把握」可能な対策項目を実施している。 即ち、○が一つ以上ついているが、十分とは言えないため、攻撃が成功する可能性は中程度である。	2
1	当該脅威（攻撃手段）において、「防御」「検知／被害把握」可能な対策項目を実施していない。 即ち、○が一つもついておらず、攻撃が成功する可能性は高い。	3

リスク値

脅威レベル×脆弱性レベル



脅威レベル×脆弱性レベルが3以下は対策の効果があり、安全と考える対象とする

リスク値	意味
A	リスクが非常に高い。
B	リスクが高い。
C	リスクが中程度。
D	リスクが低い。
E	リスクが非常に低い。

資産の重要度

評価値	評価基準
3	・資産が失われた、もしくは不正に操作された場合、事業上の被害大となる。 －システムの停止が業務停止につながる
2	・資産が失われた、もしくは不正に操作された場合、事業上の被害中となる。 －システムの停止による業務停止が限定される
1	・資産が失われた、もしくは不正に操作された場合、事業上の被害小となる。 －システムの停止が業務間停止につながらない

（参考）リスクアセスメント結果（α'モデルと自治体情報セキュリテイクラウドのローカルブレイクアウト比較）

- ✓ 自治体情報セキュリテイクラウドは、インターネットとの通信において、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施しており、既にガイドラインで規定されているローカルブレイクアウトを実施した場合も、アクセス先のクラウドサービスの通信は同様に保護される。
- ✓ 想定したα'モデルの技術的対策を実施した場合と、自治体情報セキュリテイクラウドにおけるローカルブレイクアウトを実施した場合のリスク値に差がなく（＝自治体セキュリティクラウドのローカルブレイクアウトと同様のセキュリティレベルが担保される）、かつ、**<u>３以下であり安全性が確保された水準</u>**であった。

１．α'モデルのローカルブレイクアウトのリスクアセスメント結果＜資産ベース＞

脅威 ＼ 資産	LGWAN接続系の各資産
重要度	
外部（インターネット経由）不正アクセス	資産別に脅威に対するリスクを対策と資産の重要度から評価
外部（インターネット経由）からのメール、Webアクセスによるマルウェア感染	
高負荷攻撃	
プロセス不正実行	
侵入した攻撃者、マルウェアの内部拡散	
通信データ改ざん	

⇒ リスク値が全て**<u>脅威レベル×脆弱性レベル≦3</u>**であり、対策が十分に行われており、安全だと判断する。

２．自治体情報セキュリテイクラウドのローカルブレイクアウトのリスクアセスメント結果＜資産ベース＞

脅威 ＼ 資産	LGWAN接続系やインターネット接続系の各資産
重要度	
外部（インターネット経由）不正アクセス	資産別に脅威に対するリスクを対策と資産の重要度から評価
外部（インターネット経由）からのメール、Webアクセスによるマルウェア感染	
高負荷攻撃	
プロセス不正実行	
侵入した攻撃者、マルウェアの内部拡散	
通信データ改ざん	

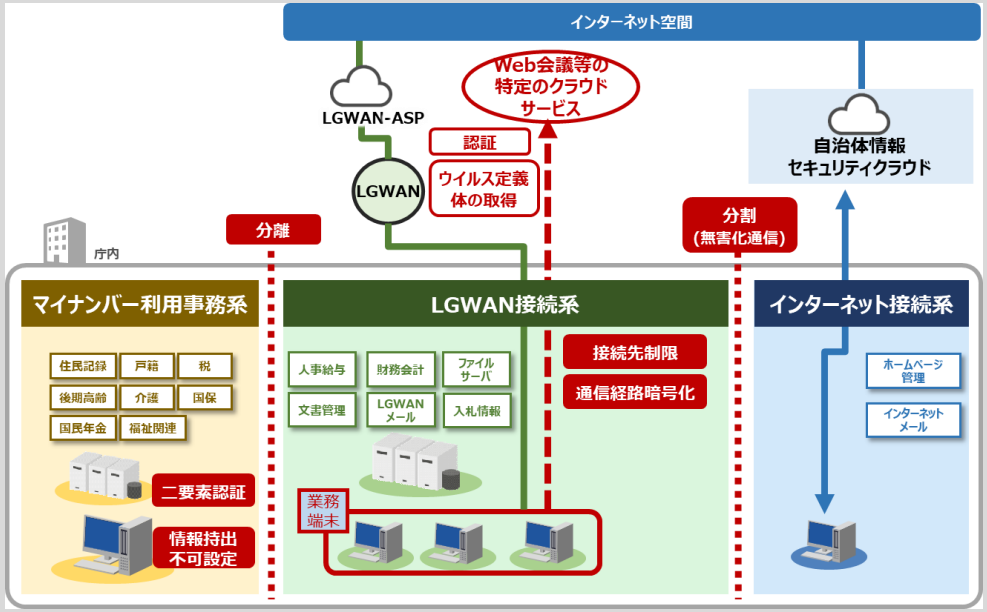
⇒ リスク値が全て**<u>脅威レベル×脆弱性レベル≦3</u>**であり、対策が十分に行われており、安全だと判断する。

α'モデルの対策（クラウドサービスのライセンス認証・認可のみの場合）（ア）

＜クラウドサービスの利用条件＞

- アプリケーションを利用するためのライセンスの認証・認可でクラウドサービスにアクセスする
- 各団体専用領域（テナント）を保有しない
- Web会議システム、メールなどのアプリケーションを利用しない

イメージ図



※各セキュリティ対策の性質に着目しセキュリティ対策を講じる場所を抽象化して表記している。また、すべての対策を網羅していないため、厳密な図とはなっていない。

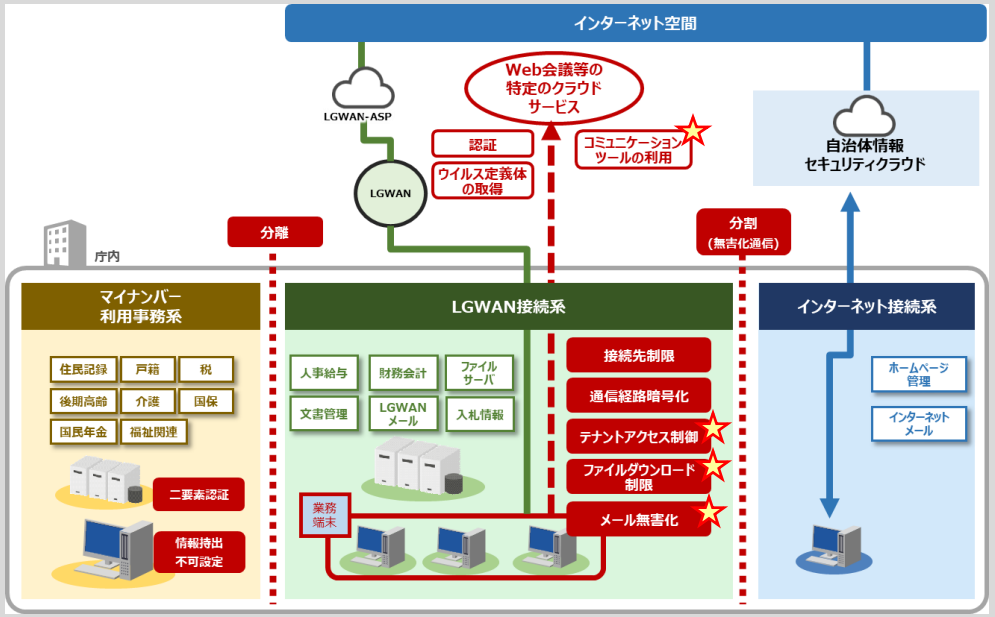
対策区分	セキュリティ対策	概要
技術的対策	接続先のクラウドサービスの証明書による認証	・接続先のクラウドサービスが本物であるか否か、正当性を確認する。
	マルウェア対策ソフト	・パターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。LGWAN接続系に配置する端末、業務サーバで対応が必要となる。
	パッチ適用	・脆弱性を修正するパッチを速やかに適用し、脆弱性を解消するLGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、接続系のスイッチ・無線APで対応が必要となる。
	接続先制限	・LGWAN接続系から外部へのアクセス先をLGWAN-ASP及び利用が許可されたクラウドサービスのみに限定する。
	権限管理	・不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、管理者、ユーザの権限関連する属性に応じて適切に管理する。LGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、LGWAN接続系のスイッチ・無線APで対応が必要となる。
	DDoS対策	・サービス不能攻撃の一つであるDDoS（Distributed Denial of Service）攻撃による被害を最小化するために、DDoS対策機器の導入やDDoS対策サービスの利用によって、高負荷攻撃への耐性を向上させる。負荷分散装置（ロードバランサ）による耐性向上を含む。
	通信路暗号化	・通信路上の盗聴・改ざんによる被害を最小化するために、暗号技術を用いて通信路上のデータを暗号化する。通信路上のデータ漏えいが発生しても、暗号化により攻撃者にとって無意味なものとする。
組織的・人的対策	手続・規定	・クラウドサービスを利用開始する場合の申請、承認等に係る規定を整備するとともに、運用を徹底しなければならない。
	組織・人的な対応	・以下の組織的・人的対策に加え、本ガイドラインの「５.人的セキュリティ」記載の組織的・人的対策を確実に実施する。 職員等が毎年度最低1回は情報セキュリティ研修を受講可能となる研修計画の策定 ・職員等の実践的サイバー防御演習（CYDER）の受講 ・演習等を通じたサイバー攻撃情報やインシデント等への対策情報の共有 ・本ガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し

α'モデルの対策（コミュニケーションツールを利用するがファイルを内部に取り込まない場合）（イ）

＜クラウドサービスの利用条件＞

- Web会議システム、団体外の組織を自テナントの**Web会議に招待し、会議を行うがLGWAN接続系へのファイルのダウンロードは制限する**
  ※**外部団体のテナントにアクセスする場合**(外部団体から招待されたWeb会議に参加し、ファイル交換をする等）は、**インターネット接続系の端末からアクセスする**
- 団体外の組織と**ファイル管理システムを通じ、ファイルの共有を行うが、LGWAN接続系にファイルのダウンロードは制限**する
- メール、団体外の組織からのメール受信あり

イメージ図



※各セキュリティ対策の性質に着目しセキュリティ対策を講じる場所を抽象化して表記している。また、すべての対策を網羅していないため、厳密な図とはなっていない。

対策区分	セキュリティ対策	概要
技術的対策	クラウドサービスからファイルダウンロード制限	・クラウドサービス上から業務端末へのファイルダウンロードを制限する。
	接続先のクラウドサービスの証明書による認証	・接続先のクラウドサービスが本物であるか否か、正当性を確認する。
	マルウェア対策ソフト	・パターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。LGWAN接続系に配置する端末、業務サーバで対応が必要となる。
	パッチ適用	・脆弱性を修正するパッチを速やかに適用し、脆弱性を解消するLGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、スイッチ・無線APで対応が必要となる。
	接続先制限	・LGWAN接続系から外部へのアクセス先をLGWAN-ASP及び利用が許可されたクラウドサービスのみに限定する。
	ローカルブレイクアウトテナントアクセス制御	・利用するクラウドサービスへのアクセスを自らの団体が利用するテナントのみに制限する。
	メール無害化/ファイル無害化	・ファイルからテキストのみを抽出、ファイルを画像PDFに変換、サニタイズ処理、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェアで危険因子の有無を確認するなどの方法を用いて、危険因子が無いことを確認した上で、LGWAN接続系にインターネットからファイルを取り込む。なお、**本対策におけるファイル無害化とは、インターネットメールに添付されたファイルの無害化を指す**。 ※詳細は、情報セキュリティ対策基準（解説）３．情報システム全体の強靭性の向上(２)LGWAN接続系①LGWAN接続系とインターネット接続系の分割を参照。
	権限管理	・不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、管理者、ユーザの権限関連する属性に応じて適切に管理する。LGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、LGWAN接続系のスイッチ・無線APで対応が必要となる。
	アクセス制御	・不正アクセス（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、権限に応じた認証・認可に基づき、アクセスの許可または拒否を行う。LGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、スイッチ・無線APで対応が必要となる。
	IDS/IPS	・ネットワーク上の通信パケットを収集・解析し、不正な通信の検知及び遮断を行う。
	DDoS対策	・サービス不能攻撃の一つであるDDoS（Distributed Denial of Service）攻撃による被害を最小化するために、DDoS対策機器の導入やDDoS対策サービスの利用によって、高負荷攻撃への耐性を向上させる。負荷分散装置（ロードバランサ）による耐性向上を含む。
	通信路暗号化	・通信路上の盗聴・改ざんによる被害を最小化するために、暗号技術を用いて通信路上のデータを暗号化する。通信路上のデータ漏えいが発生しても、暗号化により攻撃者にとって無意味なものとする。
組織的・人的対策	（クラウドサービスのライセンス認証・認可のみの場合と同じ）	

α'モデルの対策（外部とファイル送受信を行う場合）（ウ）

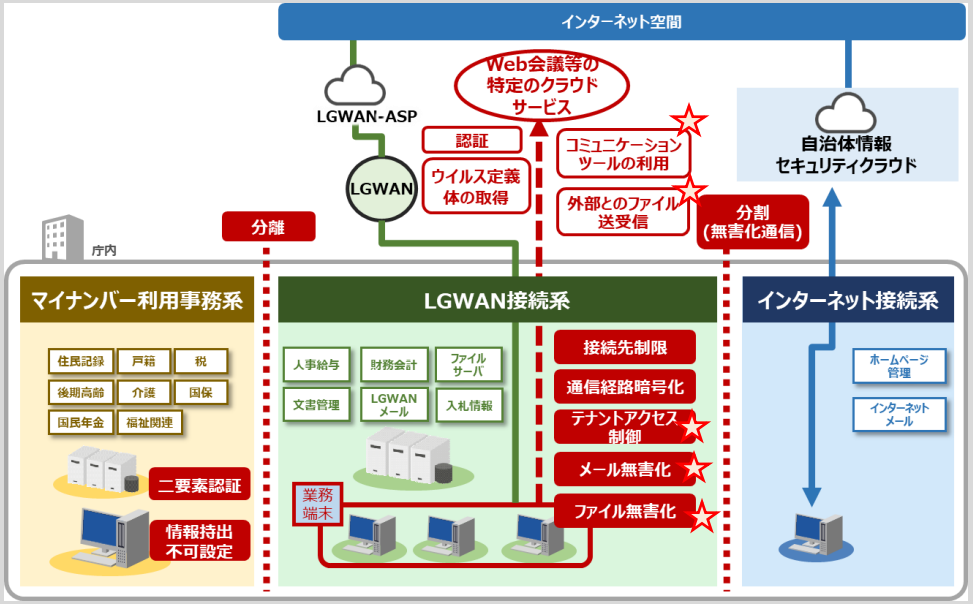
<クラウドサービスの利用条件>

- Web会議システム、団体外の組織を自テナントの**Web会議に招待し、会議を行う**

※**外部団体のテナントにアクセスする場合**(外部団体から招待されたWeb会議に参加し、ファイル交換をする等）は、**インターネット接続系の端末からアクセスする**

- 団体外の組織と**Web会議システムを通じ、ファイルの共有を行う**
- 団体外の組織と**ファイル管理システムを通じ、ファイルの共有を行う**
- メール、団体外の組織からのメール受信あり

イメージ図



※各セキュリティ対策の性質に着目しセキュリティ対策を講じる場所を抽象化して表記している。また、すべての対策を網羅していないため、厳密な図とはなっていない。

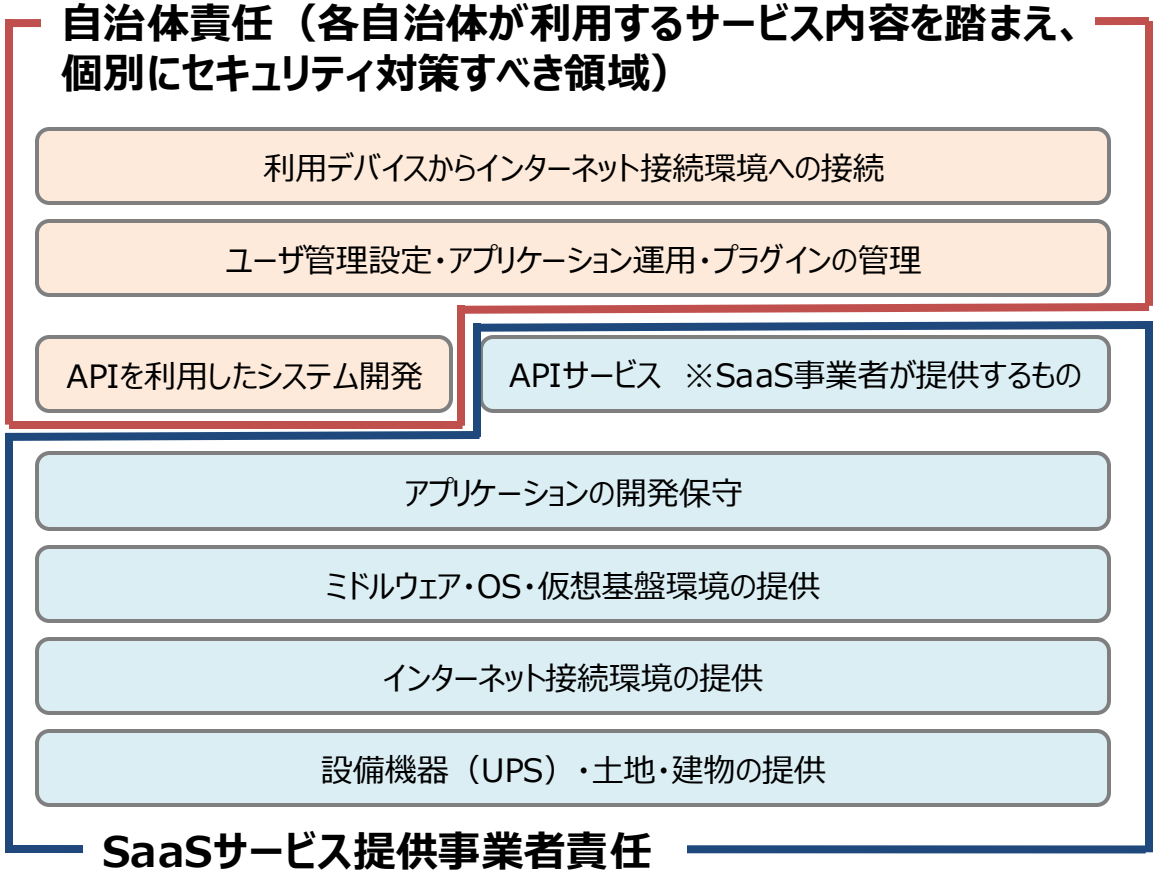
対策区分	セキュリティ対策	概要
技術的対策	接続先のクラウドサービスの証明書による認証	・接続先のクラウドサービスが本物であるか否か、正当性を確認する。
	マルウェア対策ソフト	・パターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。LGWAN接続系に配置する端末、業務サーバで対応が必要となる。
	パッチ適用	・脆弱性を修正するパッチを速やかに適用し、脆弱性を解消するLGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、接続系のスイッチ・無線APで対応が必要となる。
	接続先制限	・LGWAN接続系から外部へのアクセス先をLGWAN-ASP及び利用が許可されたクラウドサービスのみに限定する。
	ローカルブレイクアウトテナントアクセス制御	・利用するクラウドサービスへのアクセスを自らの団体が利用するテナントのみに制限する。
	メール無害化/ファイル無害化	・ファイルからテキストのみを抽出、ファイルを画像PDFに変換、サニタイズ処理、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェアで危険因子の有無を確認するなどの方法を用いて、危険因子が無いことを確認した上で、LGWAN接続系にインターネットからファイルを取り込む。 ※詳細は、情報セキュリティ対策基準（解説）３．情報システム全体の強靭性の向上(２)LGWAN接続系①LGWAN接続系とインターネット接続系の分割を参照。
	権限管理	・不正行為（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、管理者、ユーザの権限関連する属性に応じて適切に管理する。LGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、スイッチ・無線APで対応が必要となる。
	アクセス制御	・不正アクセス（例：無許可の重要コマンド発行や重要データ読み書き）を防止するために、権限に応じた認可に基づき、アクセスの許可または拒否を行う。LGWAN端末、LGWAN業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、LGWAN接続系のスイッチ・無線APで対応が必要となる。
	IDS/IPS	・ネットワーク上の通信パケットを収集・解析し、不正な通信の検知及び遮断を行う。
	DDoS対策	・サービス不能攻撃の一つであるDDoS（Distributed Denial of Service）攻撃による被害を最小化するために、DDoS対策機器の導入やDDoS対策サービスの利用によって、高負荷攻撃への耐性を向上させる。負荷分散装置（ロードバランサ）による耐性向上を含む。くす
	通信路暗号化	・通信路上の盗聴・改ざんによる被害を最小化するために、暗号技術を用いて通信路上のデータを暗号化する。通信路上のデータ漏えいが発生しても、暗号化により攻撃者にとって無意味なものとする。
組織的・人的対策	（クラウドサービスのライセンス認証・認可のみの場合と同じ）	

ISMAP登録サービスの利用に係る留意点

- ✓ ISMAP登録サービスであっても、**自治体自身の責任で個々のサービスのセキュリティについて個別に検討し、必要な対策を実施する必要がある**。
- ✓ 例えば、SaaSサービスの中には、ローコードツール（必要最小限のソースコードを書くことによりアプリケーション等を開発する手法）によりシステム構築が可能になるものがあるが、そのような場合は自治体自身の責任で、セキュリティ機能を構築する必要がある。

●例：ISMAPに登録されている、あるローコードツールに係る責任分界

※サービスごとに責任範囲が異なるため注意が必要



多くのクラウドサービスでユーザ側が設定することになっている領域があり、設定内容により脆弱な状態になり得るため、個別に対策が必要である。

※　サービス範囲は多様であるため、ガイドラインで一律に対策を示すことは困難であるが、例示として、以下の対策が考えられる。

- アクセス制御（ID・PWのみ、多要素認証など）
- 回線暗号化
- データの暗号化
- 権限昇格の防止
- データ消去

ISMAP登録されている場合でも、以下の点が事前に確認が必要である

- 言明対象の範囲を詳細に確認する。（表題のみで許可は判断できない）
- データが保存されるリージョンが海外か国内かを確認し、情報資産の機密性に応じて選定する

※　ガイドライン第３編第８章8.2.（１）外部サービスに係る規定（外部サービス利用判断基準）の整備及び8.2.（２）外部サービスの選定②の解説にも記載

ガイドライン改定案（見え消し）①

改定案：対策基準（解説）

第2章
3.情報システム全体の強靭性の向上
（２）LGWAN接続系
①LGWAN接続系とインターネット接続系の分割
（略）
②LGWAN-ASPとの接続
（略）

③主に外部のクラウドサービスの利用を目的として、LGWAN接続系から接続先にローカルブレイクアウトする構成として、α’モデルが考えられる。

本モデルの採用を検討する際に、留意すべき観点は以下のとおりである。

まず、地方公共団体は、その保有する情報資産を守るにあたり、自ら責任を持ってセキュリティを確保すべきものであることを改めて認識することが重要である。

○サイバーセキュリティ基本法（平成26年法律第104号）
（地方公共団体の責務）
第五条　**地方公共団体は**、基本理念にのっとり、国との適切な役割分担を踏まえて、**サイバーセキュリティに関する自主的な施策を策定し、及び実施する責務を有する**。

LGWAN接続系に配置された業務端末から、インターネット接続により直接外部のクラウドサービスを活用することが可能となるため、外部からの脅威が増加することになる。その結果、LGWAN接続系に設置された業務システムの停止や重要な情報資産の漏えいなどに加え、LGWANへ脅威が侵入した場合は、更なる被害の拡大に繋がる恐れもある。このようなインシデントが発生した場合、上記のとおり、保有する情報資産を守る立場にあり、セキュリティ確保の責務を有する地方公共団体が責任を負うことになるため、セキュリティ対策に万全を期す必要がある。

このため、本モデルにおいて利用可能なクラウドサービスは、ISMAP管理基準を満たし、ISMAPクラウドサービスリストに登録されているサービスとする。

なお、ISMAPに登録されたクラウドサービスを基盤として構築されたことをもって、その構築されたサービスを、ISMAP登録サービスとして扱ってはならないことに留意する。ただし、セキュリティ関連サービス（ウィルス定義ファイルやIPアドレス、URLドメインリスト等の更新をインターネット経由で提供するサービス）については、更新情報の配信ツールであるため、
・行政文書や行政文書に相当する情報を扱わないこと
・利用するクラウドサービスの接続先のURLを確認の上、当該接続先のみに接続を制限すること
・信頼できる機関が発行した証明書を用いた認証の実施により、サービス提供元の真正性が担保されていること（この対策だけではなく、上記のURLを用いた接続先制限も併せて実施すること）
を条件に、ISMAPクラウドサービスリストに登録されていないクラウドサービスについても、利用を認めるものとする。

また、地方公共団体においては、採用したクラウドサービスへのみ、安全につなぐ（＝採用したクラウドサービス以外の通信を確実に遮断する）ことが重要となるため、接続先制限やアクセス制御、テナントアクセス制御等の技術的対策が必要となる。このようなテナントアクセス制御を適切に行うため、接続先のクラウドサービスにおける設定に誤りがないか、定期的な確認に加え、アップデートに伴う仕様変更の際の確認を行うことが必要であり、設定や確認作業等を外部に委託する場合は、そのサービスの品質が保証されるよう、契約で担保する必要がある（第２編、第３編8.1. 業務委託参照）。

ガイドライン改定案（見え消し）②

改定案：対策基準（解説）

【仕様変更による事故事例】

・クラウドサービスの設定ミスにより、不適切なアクセス権限をデータに付与していた。それにより新しい機能がリリースされた際に、意図しない情報が外部から参照できる状態になってしまった。

以下の「Salesforce の製品の設定不備による意図しない情報が外部から参照される可能性について 」（2021年1月29日内閣官房内閣サイバーセキュリティセンター（NISC））参照）。
https://www.nisc.go.jp/pdf/policy/infra/salesforce20210129.pdf

・「クラウドサービス利用・提供における適切な設定のためのガイドライン」（2022年 10 月総務省）に以下のとおり事例を記載している。

Ⅱ．２ 設定不備の要因と対策

Ⅱ．2．１ 設定不備の事例と要因分析

事例１

クラウドサービス提供事業者が、提供している SaaS の機能変更を行った。これに伴い、当該 SaaS のユーザーアクセスに関する設定について、結果的にデフォルトでセキュリティレベルが下がってしまった。利用企業側はこれに気づかず、低いセキュリティレベルのまま利用し続けた結果、機密情報が大量に流出した。

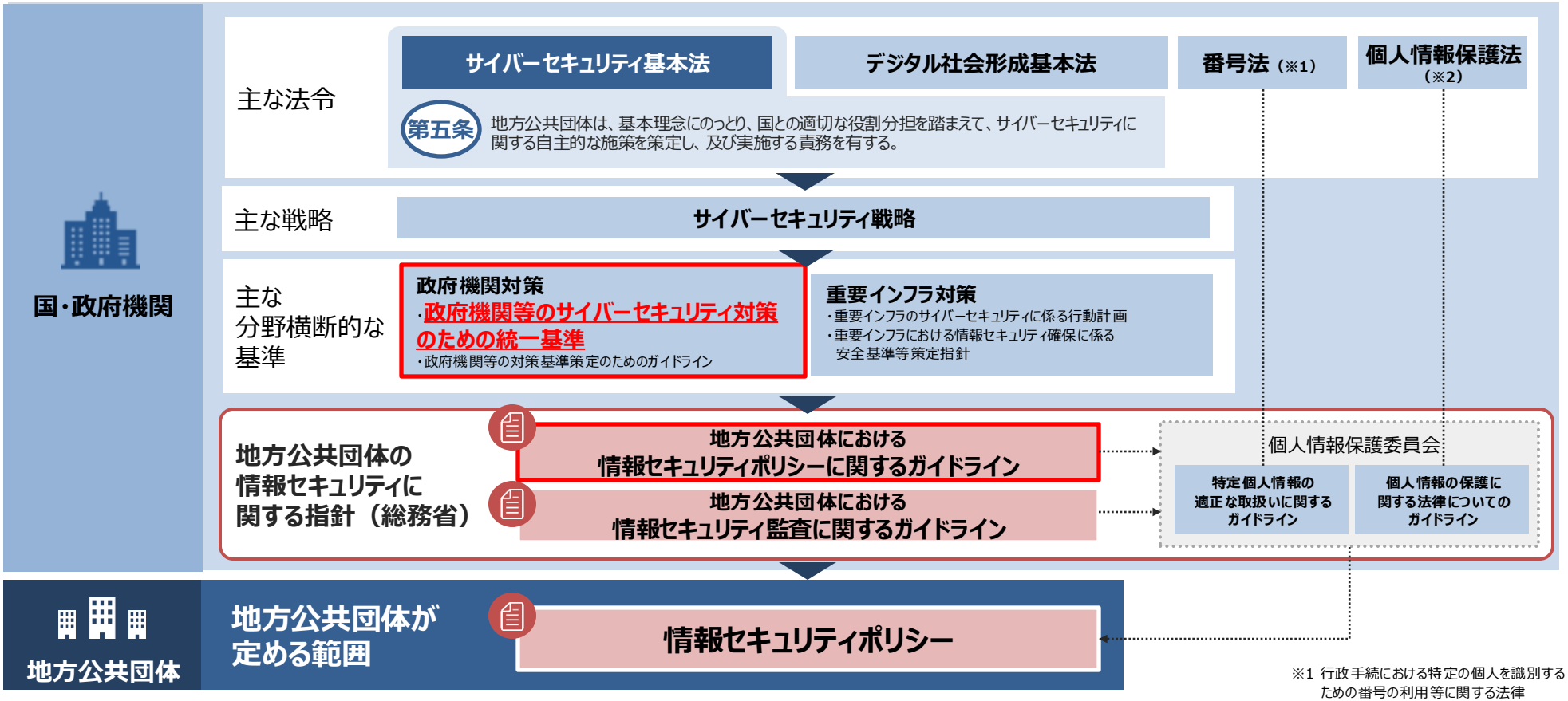
事例３

ある企業の業務委託先が、サーバからクラウドサービスへのデータ移行を行う際に、ストレージの設定を公開設定としていた。これにより長期間機密情報が公開されている状態になった。

（https://www.soumu.go.jp/main_content/000843318.pdf）

政府統一基準について

- ✓ サイバーセキュリティ基本法の枠組みの中で、政府統一基準において国・政府機関に必要なセキュリティ対策を規定することとされている。
- ✓ 国・政府機関のセキュリティ対策を踏まえ、地方公共団体の情報セキュリティに関する指針を策定する必要があることから、統一基準の改定内容を、ガイドラインに反映させている。



※1 行政手続における特定の個人を識別するための番号の利用等に関する法律

※2 個人情報の保護に関する法律

中間報告のポイント（業務委託先管理の強化）

「第２編 第２章 情報セキュリティ対策基準（例文）8. 業務委託と外部サービス（クラウドサービス）の利用」を参照

「第３編 第２章 情報セキュリティ対策基準（解説）8. 業務委託と外部サービス（クラウドサービス）の利用」を参照

- **政府統一基準の改定を踏まえ**、委託先に提供した情報の適切な保護について、委託先に求めるべき対策を規定。

改定ポイント	主な記載内容
委託先に提供した情報の保護	● 委託先に提供した情報が適切に保護されるよう、**業務委託契約時、業務委託の実施期間中、終了後に取るべき対策について、地方公共団体で実施すべき対策・委託先に求めるべき対策をそれぞれ規定**。 • 委託事業者への**提供を認める情報**及び**委託する業務の範囲を判断する基準**、**委託事業者の選定基準**を含む**運用規程を整備**すること。 • 業務委託の実施までに、委託する業務内容の特定や委託事業者の選定条件を含む仕様の策定、仕様に基づく委託事業者の選定、情報セキュリティ要件を明記した契約の締結を実施し、委託の前提条件として、仕様に準拠した提案、契約の締結、**委託事業者において重要情報を取り扱う場合の秘密保持契約（NDA）の締結を委託事業者に求めなければならない**。 • 業務委託の実施期間において、**情報の適正な取扱いのための情報セキュリティ対策、契約に基づく情報セキュリティ対策の履行状況の定期的な報告等の実施を委託事業者に求めなければならない**。 • 業務委託の終了に際して、**業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告**を含む検収の受検、提供を受けた情報を含め、**委託業務において取り扱った情報の返却、廃棄又は抹消等の実施**を委託事業者に求めなければならない。

中間報告のポイント（サイバーレジリエンスの強化等）

「第２編 第２章 情報セキュリティ対策基準（例文）４. 物理的セキュリティ」を参照
「第２編 第２章 情報セキュリティ対策基準（例文）６. 技術的セキュリティ」を参照
「第２編 第２章 情報セキュリティ対策基準（例文）７. 運用」を参照

- **政府統一基準の改定を踏まえ**、「サイバー攻撃を受けることを念頭においた情報システムの防御・復旧やバックアップに係る対策の強化」「サービス不能攻撃に対する対策強化」「動的アクセス制御の実装」「機器・ソフトウェアの利用時の対策の強化」について規定。

改定ポイント	主な記載内容
サイバー攻撃を受けることを念頭においた情報システムの防御・復旧やバックアップに係る対策の強化	● **サーバ機器と通信機器に関するバックアップ**についての要件を記載。 ● **アクセス権限は必要最小限の範囲で適切に設定**することに加え、**不要なアクセス権限が付与されていないか定期的に確認**するよう記載。
サービス不能攻撃(DDoS攻撃)に対する対策強化	● 昨今のサービス不能攻撃(DDoS攻撃)を踏まえ、ネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施する旨を記載。 ・ インターネット等の外部ネットワークを接続する場合は、**不正アクセス等のリスクを低減するためのネットワーク構成等を構築する**必要がある。 ・ 通信回線装置を設定する際は、当該通信回線装置を提供している提供者が提示している**推奨設定や業界標準、ベストプラクティス等を参照し、通信回線装置の各種設定を行い、設定の不備等がないようにする**必要がある。 ● 「監視を含むセキュリティ機能」の例として、主体認証機能、アクセス制御機能、権限の管理、ログの取得・管理等を記載。 ● 情報システムの監視に係る運用管理機能について、監視するイベントや実装の仕組みの具体的例示を記載。
動的アクセス制御の実装	● **ゼロトラストアーキテクチャを実現する機能の一部と考えられる「動的なアクセス制御」**に関し、実装する場合に特に必要な対策について、参考として記載。
機器・ソフトウェアの利用時の対策の強化	● 機器及びソフトウェアの調達において、それらの選定基準の一つとして、**情報システムの開発時のみならず、運用開始後も不正な変更が加えられない管理**がなされ、その管理を確認可能な運用規定を整備するよう記載。 ● アプリケーション・コンテンツの開発時の対策として、既知の種類のウェブアプリケーションの脆弱性を排除するよう記載。

５．今後の動き

地方自治法改正の概要（情報システム・セキュリティ関係）

○　地制調答申において、これまでの地方自治を基盤としつつ、**事務の種類に応じて、他の地方公共団体や国等と連携・協力し、デジタル技術を最適化された形で効果的に活用**することが重要であるとともに、国・地方公共団体等のネットワークを通じた相互接続がますます進展する中で、**地方公共団体のサイバーセキュリティ対策の実効性を担保**することが必要との提言があったことを踏まえ、以下の改正を行う。

現行制度

○　現在の地方自治法には、情報システムについての**規定は置かれていない**。

○　サイバーセキュリティについては、総務省において**技術的助言**として「地方公共団体における情報セキュリティポリシーに関するガイドライン」を示すとともに、各地方公共団体はこれを踏まえ、個々の判断でセキュリティポリシーを定めている。

改正概要

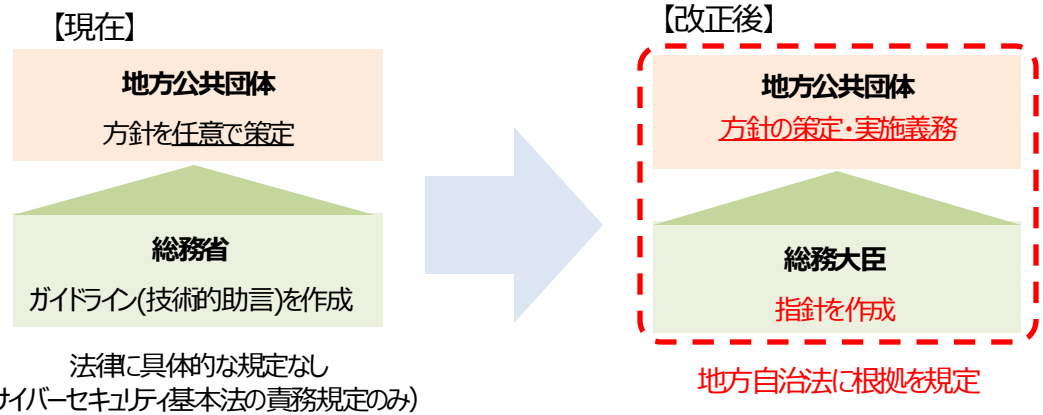
○　地方公共団体は、**事務の種類・内容に応じ**、**情報システムを有効に利用**するとともに、**他の地方公共団体又は国と協力**し、**その利用の最適化を図るよう努める**。

○　地方公共団体は、サイバーセキュリティの確保、個人情報の保護※など、**情報システムの適正な利用を図るために必要な措置**を講じなければならない。

○　**サイバーセキュリティの確保**について、地方公共団体の議会及び長その他の執行機関は、**方針を定め、必要な措置を講じる**。**総務大臣は、方針の策定等について指針を示す**。

※　個人情報については、漏えい防止等の安全管理措置を講じるなど、引き続き、個人情報保護法に基づき適切に対応することが求められる。

《地方公共団体におけるサイバーセキュリティ対策》



地方自治法

第二条　地方公共団体は、法人とする。
⑭　地方公共団体は、その事務を処理するに当つては、住民の福祉の増進に努めるとともに、最少の経費で最大の効果を挙げるようにしなければならない。
⑮　地方公共団体は、常にその組織及び運営の合理化に努めるとともに、他の地方公共団体に協力を求めてその規模の適正化を図らなければならない。

（**情報システムの利用に係る基本原則**）
第二百四十四条の五　普通地方公共団体は、第二条第十四項及び第十五項の規定の趣旨を達成するため、その事務を処理するに当たつて、情報システムを有効に利用するとともに、事務の種類及びその内容に応じて、他の普通地方公共団体又は国と協力して当該事務の処理に係る情報システムの利用の最適化を図るよう努めなければならない。
２　普通地方公共団体は、その事務の処理に係る情報システムの利用に当たつて、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。次条第一項において同じ。）の確保、個人情報の保護その他の当該情報システムの適正な利用を図るために必要な措置を講じなければならない。

（**サイバーセキュリティを確保するための方針等**）
第二百四十四条の六　**普通地方公共団体の議会及び長その他の執行機関は**、その事務の処理に係る情報システムの利用に当たつての**サイバーセキュリティを確保するための方針を定め、及びこれに基づき必要な措置を講じなければならない**。
２　普通地方公共団体の議会及び長その他の執行機関は、**前項の方針を定め、又はこれを変更したときは**、遅滞なく、**これを公表しなければならない**。
３　総務大臣は、普通地方公共団体に対し、第一項の方針（政令で定める執行機関が定めるものを除く。）の策定又は変更について、指針を示すとともに、必要な助言を行うものとする。
４　総務大臣は、前項の指針を定め、又は変更しようとするときは、国の関係行政機関の長に協議しなければならない。

（**普通地方公共団体に関する規定の準用**）
第二百九十二条　**地方公共団体の組合については**、法律又はこれに基づく政令に特別の定めがあるものを除くほか、都道府県の加入するものにあつては都道府県に関する規定、市及び特別区の加入するもので都道府県の加入しないものにあつては市に関する規定、その他のものにあつては町村に関する**規定を準用する**。

地方公共団体における情報セキュリティポリシーに関するガイドライン　情報セキュリティ基本方針（例文）

1．目的
　本基本方針は、本市が保有する情報資産の機密性、完全性及び可用性を維持するため、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2．定義
（略）

3．対象とする脅威
情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。
（１） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等
（２） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等
（３） 地震、落雷、火災等の災害によるサービス及び業務の停止等
（４） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等
（５） 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4．適用範囲
（１） 行政機関の範囲
　本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局、消防本部及び地方公営企業とする。
（２） 情報資産の範囲
本基本方針が対象とする情報資産は、次のとおりとする。
①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体
②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）
③情報システムの仕様書及びネットワーク図等のシステム関連文書

5．職員等の遵守義務
　職員、非常勤職員及び臨時職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

6．情報セキュリティ対策
上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。
（１） 組織体制
　本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。
（２） 情報資産の分類と管理
　本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。
（３） 情報システム全体の強靭性の向上
　情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。
（略）

（４） 物理的セキュリティ
　サーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。
（５） 人的セキュリティ
　情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。
（６） 技術的セキュリティ
　コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。
（７） 運用
　情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。
（８） 業務委託と外部サービスの利用
　業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる。
　外部サービスを利用する場合には、利用に係る規定を整備し対策を講じる。
　ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。
（９） 評価・見直し
　情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

7．情報セキュリティ監査及び自己点検の実施
　情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8．情報セキュリティポリシーの見直し
情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

9．情報セキュリティ対策基準の策定
　上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

10．情報セキュリティ実施手順の策定
　情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。
　なお、情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

国・地方ネットワークの将来像及び実現シナリオに関する検討会

設置趣旨・目的

「デジタル社会の実現に向けた重点計画」（令和５年６月９日閣議決定）において、
「**国・地方を通じたデジタル基盤に関して、全体最適かつ効率的なネットワーク構成となるよう、強固なセキュリティ基盤の具備、ユーザー利便性の向上、安定的な運用体制、強靭性の確保の観点も念頭に、将来像及び実現シナリオについて、具体的に検討を進めることとする**」とされているところ、
「国・地方ネットワークの将来像及び実現シナリオに関する検討会」をデジタル庁に設置し、総務省の協力を得ながら、総合的な観点から各分野における有識者の意見を伺いつつ検討を深める。

「デジタル社会の実現に向けた重点計画」（令和５年６月９日閣議決定）第３-２　各分野における基本的な施策
１．（１）② イ 安全性と利便性の両立を追求するネットワーク環境
インフラの検討は、技術的・環境的な変化や地方公共団体の課題を踏まえ、不断に進める。国・地方を通じたデジタル基盤に関して、全体最適かつ効率的なネットワーク構成となるよう、強固なセキュリティ基盤の具備、ユーザー利便性の向上、安定的な運用体制、強靭性の確保の観点も念頭に、将来像及び実現シナリオについて、具体的に検討を進めることとする。
特に、地方公共団体のセキュリティについては、ガバメントクラウドやSaaS等のクラウドサービスの利活用、職員の効率的な働き方の実現、新しい住民サービスの迅速な提供等を可能にするため、「地方公共団体における情報セキュリティポリシーに関するガイドライン」を継続的に見直す。具体的には、現行のいわゆる「三層の対策」について、地方公共団体の意見も聞きながら、抜本的な見直しを行うとともに、将来的には、政府情報システムと歩調を合わせつつ、ゼロトラストアーキテクチャの考えに基づくネットワーク構成に対応するよう検討を行う。

構成員メンバー

◆構成員

立命館大学情報理工学部 教授	上原 哲太郎
情報セキュリティ大学院大学 学長	後藤 厚宏
青森大学ソフトウェア情報学部 教授	下條 真司
武蔵大学社会学部 教授　◎座長	庄司 昌彦
KUコンサルティング 代表	高橋 邦夫
IPAサイバー技術研究室 室長	登 大遊
デジタル庁 統括官付審議官	阿部 知明
デジタル庁 統括官付審議官	藤田 清太郎
総務省 大臣官房審議官 （地方行政・個人番号制度、地方公務員制度、選挙担当）	三橋 一彦
地方公共団体情報システム機構　総合行政ネットワーク全国センター長	菊池 善信

◆準構成員

デジタル庁 ﾁｰﾌｱｰｷﾃｸﾄ	本丸 達也
デジタル庁 ﾁｰﾌｸﾗｳﾄﾞｵﾌｨｻｰ	山本 教仁
デジタル庁 ﾁｰﾌｲﾝﾌｫﾒｰｼｮﾝｾｷｭﾘﾃｨｵﾌｨｻｰ	坂 明
デジタル庁 ﾈｯﾄﾜｰｸｴﾝｼﾞﾆｱ	大江 将史
デジタル庁 ﾈｯﾄﾜｰｸｴﾝｼﾞﾆｱ	関谷 勇司
デジタル庁 ｾｷｭﾘﾃｨｱｰｷﾃｸﾄ	満塩 尚史
デジタル庁 統括官付参事官	古川 易史
デジタル庁 統括官付参事官付企画官	羽田 翔
総務省 自治行政局デジタル基盤推進室長	名越 一郎

◆オブザーバー

宮城県 企画部デジタルみやぎ推進課長	橋本 崇
兵庫県神戸市 デジタル戦略部課長	金高 裕一
長崎県佐世保市 総務部DX推進室 主査	峯 雅徳
兵庫県伊丹市 総合政策部デジタル戦略室主幹	高科 恵美
埼玉県美里町 総合政策課長	萩原 和幸
鹿児島県肝付町 デジタル推進課 課長補佐	中窪 悟
エヌ・ティ・ティ・コミュニケーションズ株式会社 ビジネスソリューション本部 ソリューションサービス部　担当部長	山内 一郎
KDDI株式会社 コア技術統括本部　技術企画本部　副本部長	丸田 徹
日本電気株式会社 ガバメントプラットフォーム統括部 統括部長代理	伊藤 晋
日本電信電話株式会社 研究企画部門　IOWN推進室 技術ディレクタ	川島 正久
一般社団法人行政情報システム研究所　システム事業部長	稲垣 浩
総務省　情報流通行政局情報通信政策課長	田邊 光男
経済産業省　商務情報政策局ソフトウェア・情報サービス戦略室長	渡辺 琢也

✓ 境界型防御に依拠しない「三層の対策」の見直しに取り組む。

国・地方ネットワークの将来像及び実現シナリオに関する検討会　報告書【概要②】

Ⅲ 2030年頃の国・地方ネットワークの将来像

2030年の姿

- 国民・住民に、**国・地方の行政サービスを、柔軟かつセキュア、安定的に提供可能**
- **国・地方のネットワーク基盤の共用化**が行われ、**ネットワークの効率性が向上**
- 国・地方の職員が、セキュリティを確保しつつ、**一人一台のPCで効率的に業務ができ、テレワーク等の柔軟な働き方が可能**

シンプルかつ柔軟なネットワーク

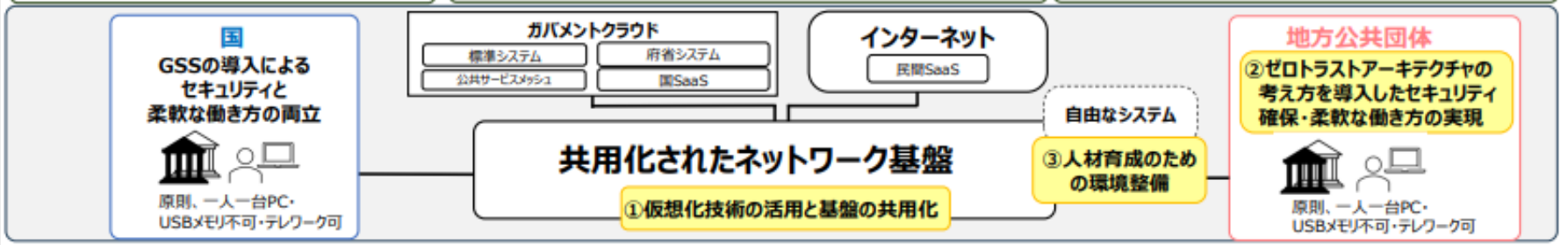
・**仮想化ネットワーク技術の活用**により、シンプルかつ柔軟なネットワークを構築

災害時のレジリエンスの確保

・大規模災害等にも対応し得る**強靭性・冗長性を確保**
（例：地上回線＋衛星回線の活用、国と地方ネットワークの相互運用等）

セキュリティの確保と利便性の向上

・強固なセキュリティ・柔軟なサービス構成には、**「ゼロトラストアーキテクチャ」の考え方が有効**



①仮想化技術の活用と基盤の共用化

・国は、冗長化された共用可能な回線等を全国に整備し、仮想化技術を用い、柔軟で可用性の高い論理ネットワークを効果的・効率的に整備

・国・地方での平時のコスト効率向上、レジリエンスの確保、地方の負担軽減のため、仮想化技術を活用しつつ、**国・地方の適切な役割分担の下、国が主体的に整備するネットワーク基盤の共用化**を検討（※）

（※）GSSが国の地方機関向けに全国に整備しているネットワークや拠点について、国・地方のネットワーク基盤としての活用を検討。
その際、新技術（Beyond5G等）の活用や費用負担の在り方等も検討

②ゼロトラストアーキテクチャの考え方の導入

・国は、ゼロトラストアーキテクチャの考え方を導入したGSSに、原則移行し、柔軟な働き方とセキュリティの両立を実現。ユーザー数増加に対応するため、保守・運用体制を強化

・地方のネットワーク上のシステムについて、**デジタル庁・総務省が調査・分析・検証を実施**（※）した上で、**ゼロトラストアーキテクチャの考え方に基づきセキュリティを強化**

（※）ゼロトラストアーキテクチャの考え方の導入に当たって必要な要件等の整理、概念実証（PoC）による技術面、運用管理体制面、コスト面等に係る課題の洗い出しとその解決策の検討などを実施予定

③人材育成のための環境整備

・行政職員による基礎的なデジタル能力の修得、システムの構築・運用に必要な技術研鑽、官民の技術者・研究者との交流、革新的技術の創出等を実現できる、人材育成環境としての**「自由なシステム」**（※）を整備

（※）行政人材によって自律的に発達するデジタル人材育成サイクルを支える仕組みや実験用ネットワーク等。他のデジタル人材に係る施策とも連携して官民人材を発掘・育成

- LGWANが担っている重要情報のやり取りを行う機能(※)の在り方は引き続き検討　(※)マイナンバー制度による情報連携、J-アラート等
- 地方の強固なセキュリティ・さらなる利便性向上に向け、J-LIS・IPAによる共同研究・実証実験を推進
- ガバメントクラウド上のデータの保護のため、より一層低コストかつ安全な方法について、暗号技術を含む多角的な観点からの調査研究を実施

今後の進め方

- 本報告書について、地方の意見を丁寧に伺った上で、**可能なものから速やかに上記実証等を実施**
- 標準化に取り組む地方の負担やネットワーク更改時期等を考慮した上で、新たなネットワークへの移行は、**分散・段階的に実施**

ご清聴ありがとうございました