資料６－１

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４月

総務省自治行政局

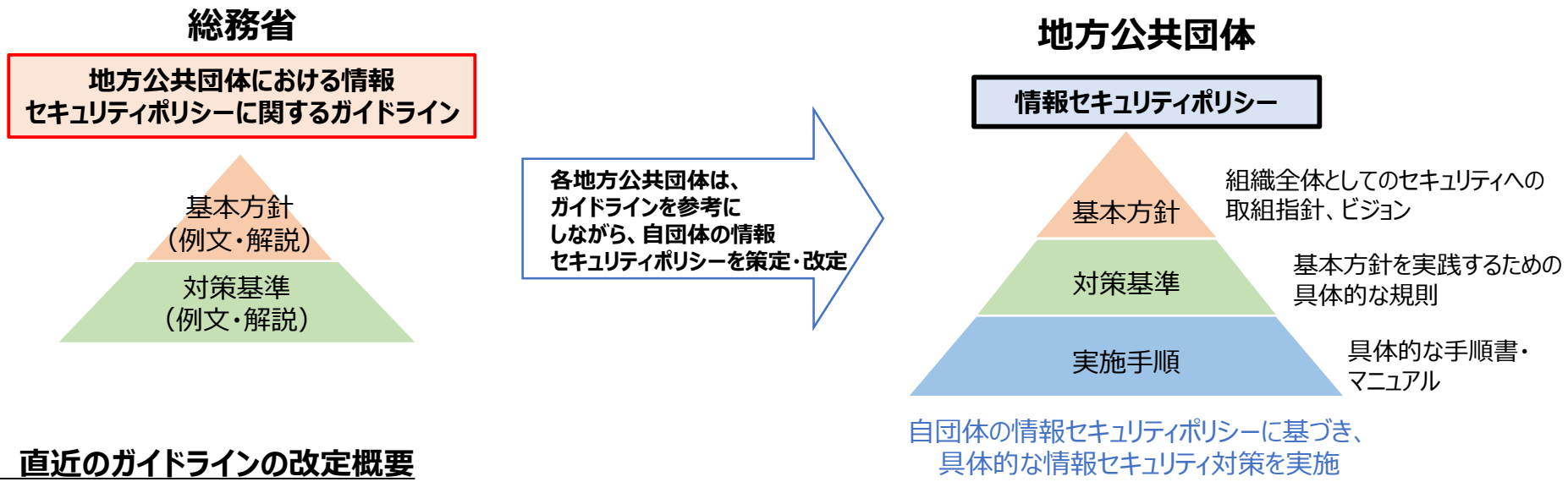
デジタル基盤推進室

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．地方公共団体の状況

「三層の対策」概要（従来型のαモデル）

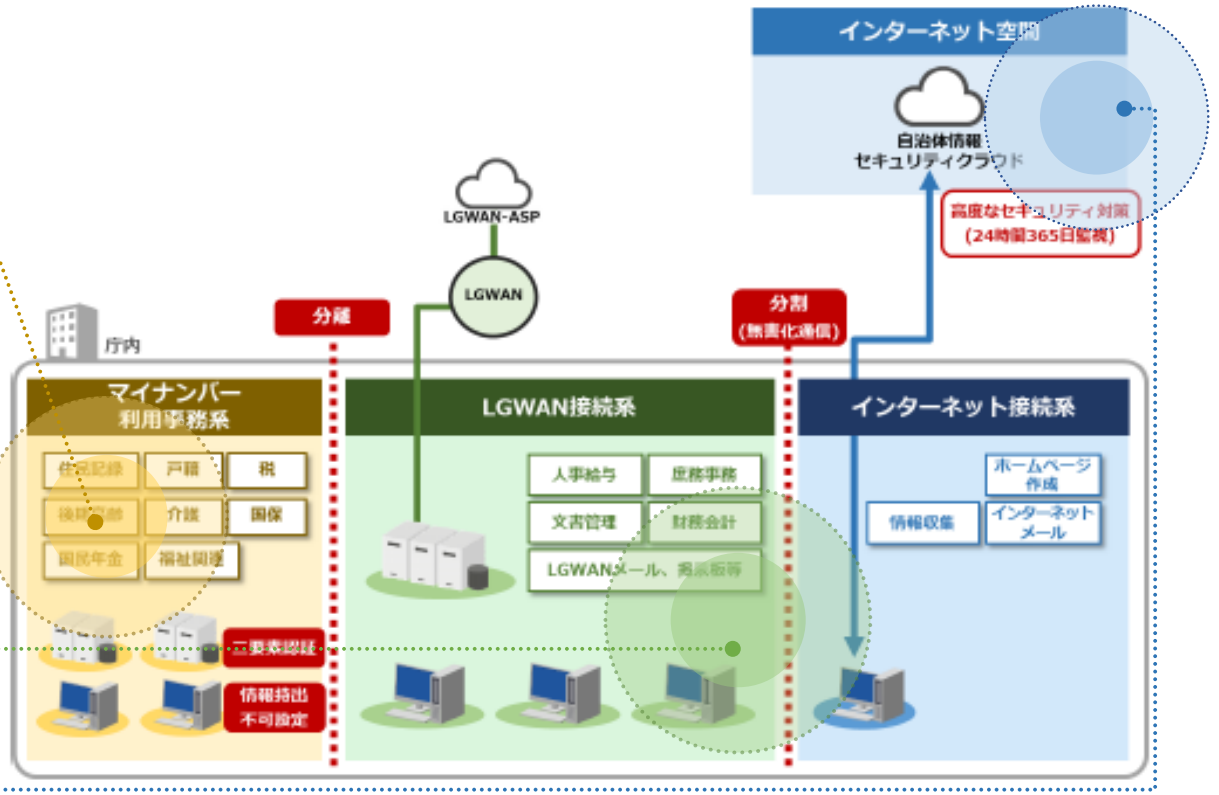
- 複雑・巧妙化しているサイバー攻撃の脅威により、地方公共団体の行政に重大な影響を与えるリスクが想定されるため、情報システムにおいては、機密性はもとより、可用性や完全性の確保にも十分配慮した、情報システム全体の強靭性の向上が求められる。
- **<u>情報システム全体の強靭性の向上を「三層の対策」により実現する</u>**。

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



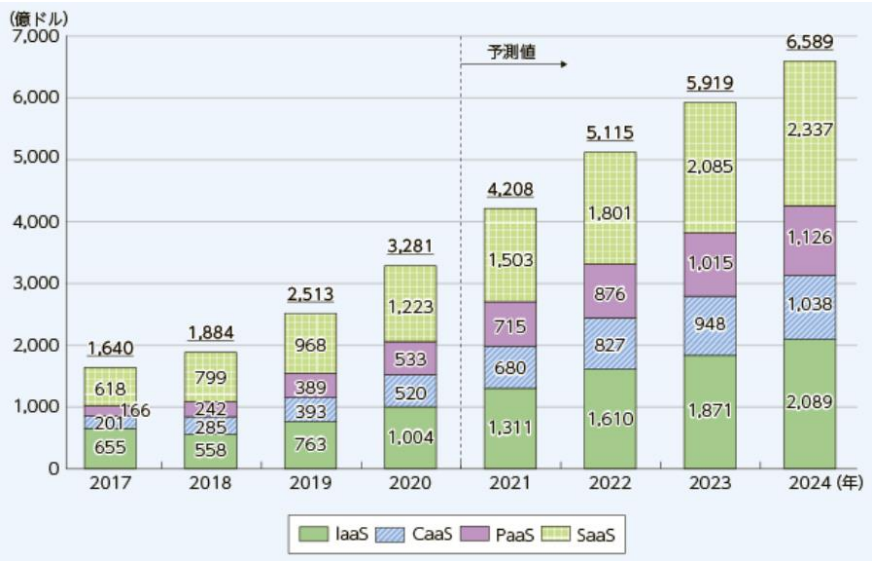
三層の構えによる自治体情報システム例（図表21）

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。

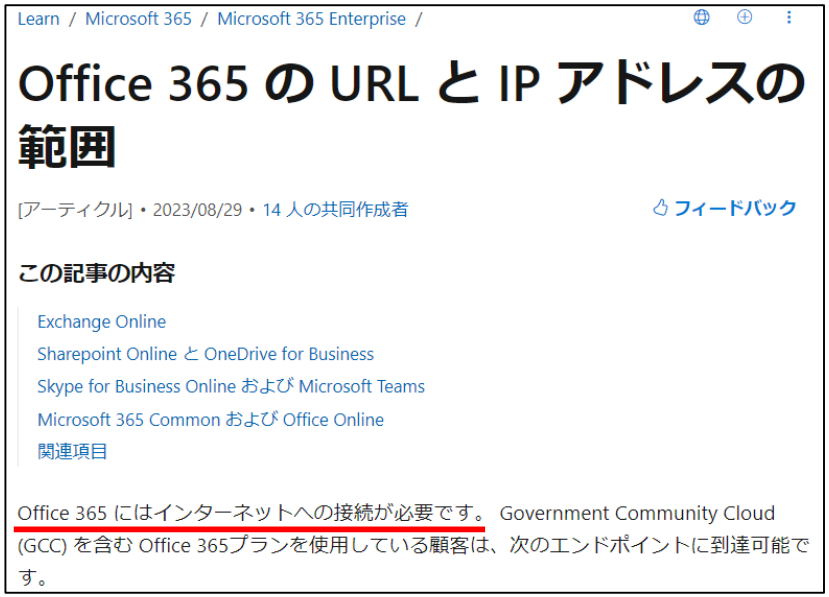


図表3-6-8-1　世界のパブリッククラウドサービス市場規模（売上高）の推移及び予測

- 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

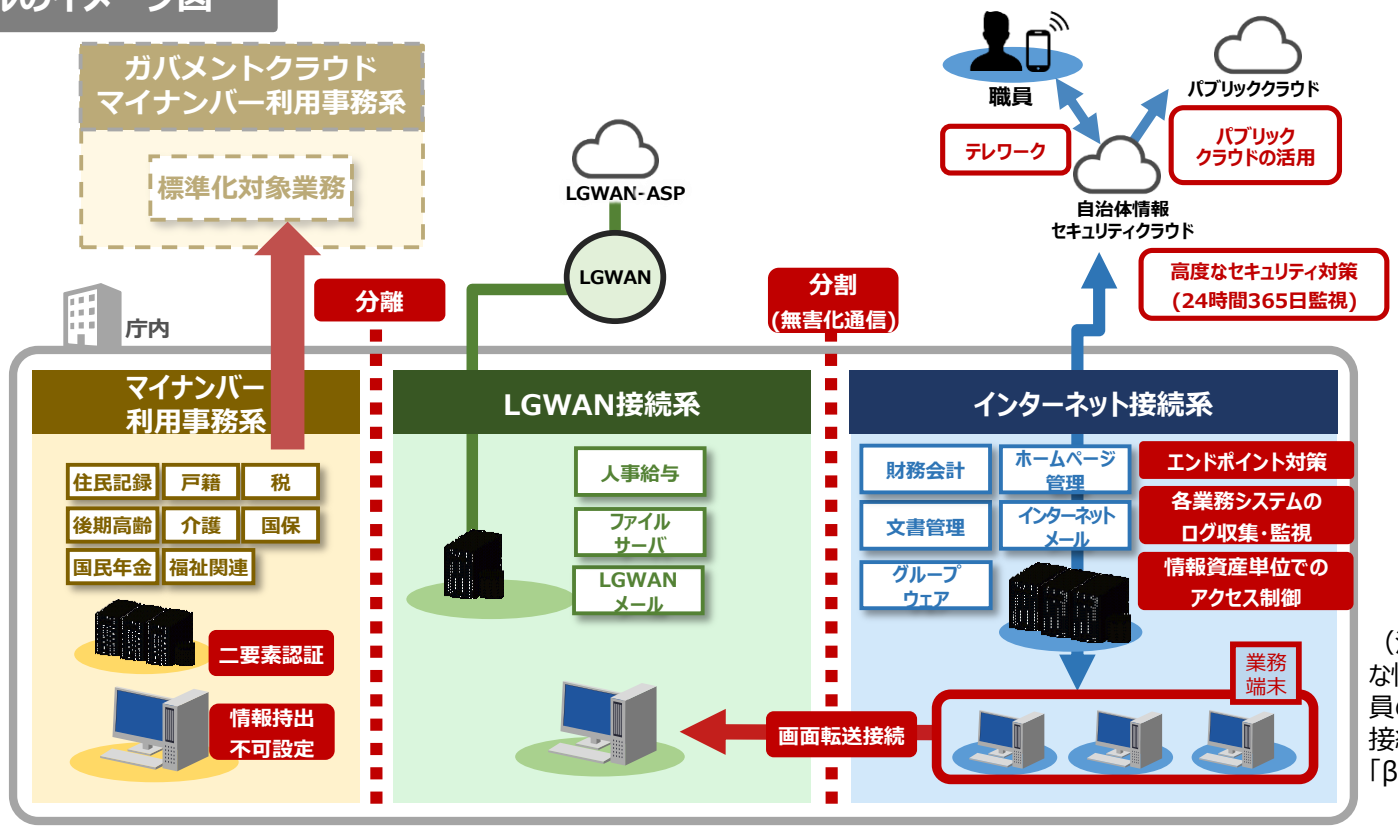
Office 365 にはインターネットへの接続が必要です。 Government Community Cloud (GCC) を含む Office 365プランを使用している顧客は、次のエンドポイントに到達可能です。

（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



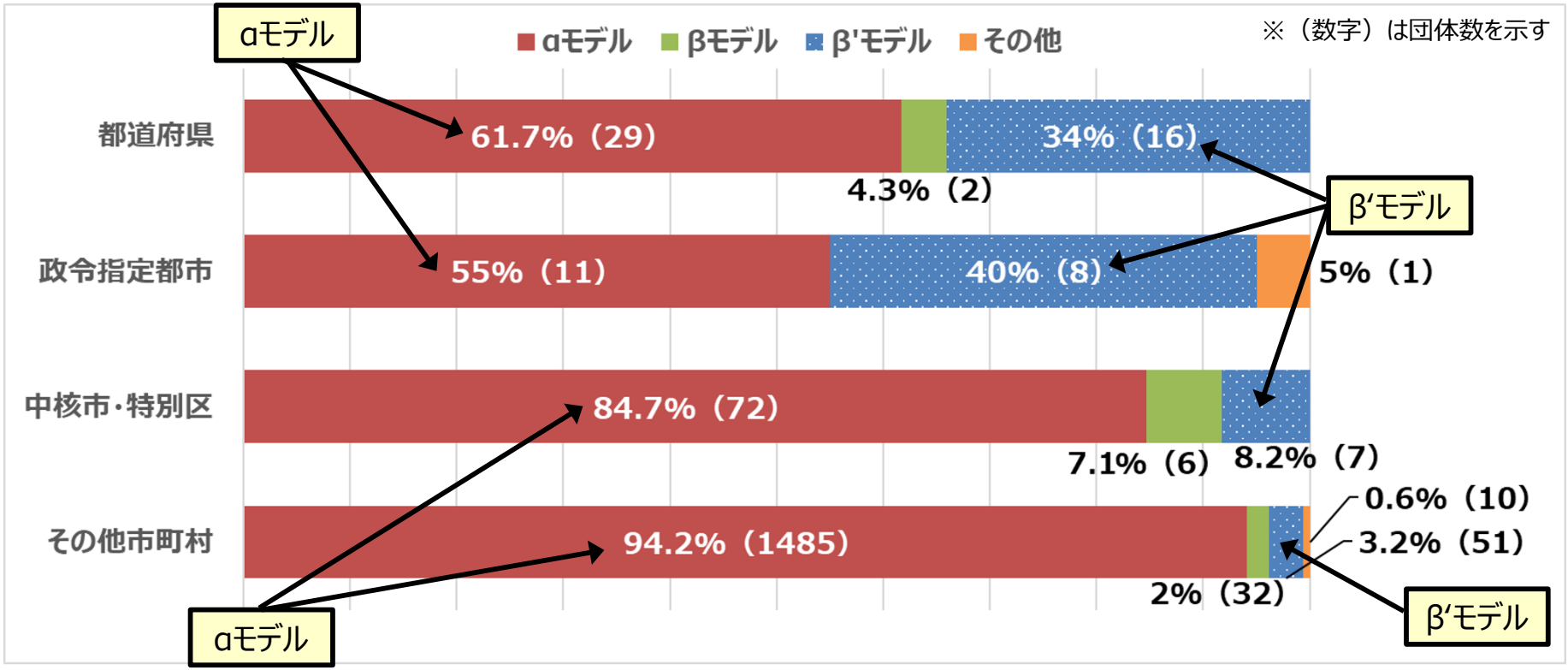
（注）βモデルのうち、重要な情報資産(入札情報や職員の情報等)をインターネット接続系に配置する場合は「β'モデル」としている。

※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

「三層の対策」の状況（自治体分類別）

- ✓ 回答のあった1,730団体のうち、**都道府県は約３割、政令指定都市は約４割がβ'モデル団体**である。
- ✓ 一方、**中核市・特別区は８割以上、その他市町村は９割以上が従来型のαモデル団体**であった。

回答数	都道府県 47団体	政令指定都市 20団体	中核市・特別区 85団体	その他市町村 1578団体
合計	1730団体			

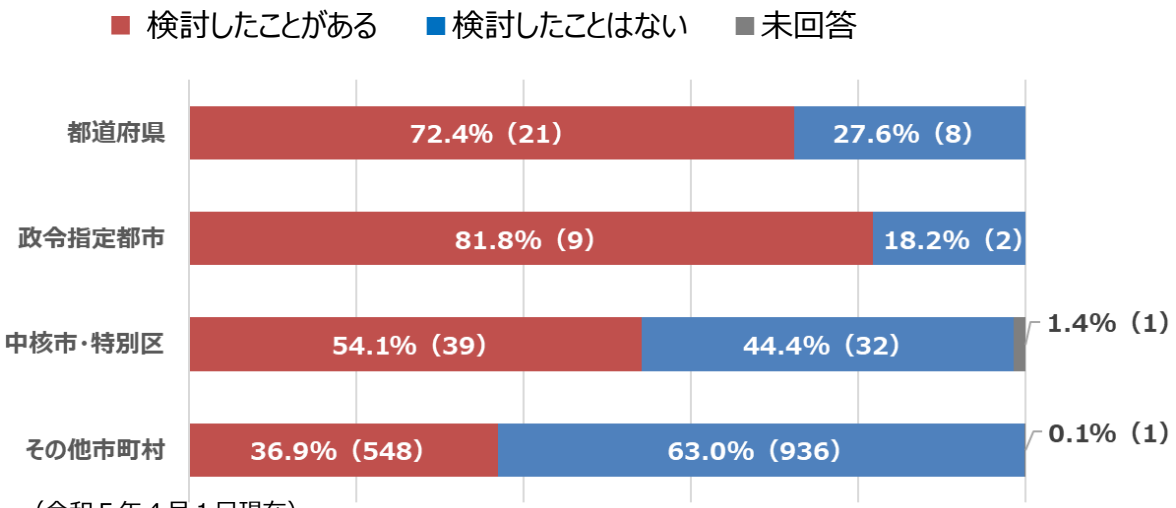


（令和５年４月１日現在）

αモデルの団体がβ・β‘モデル移行を断念している理由

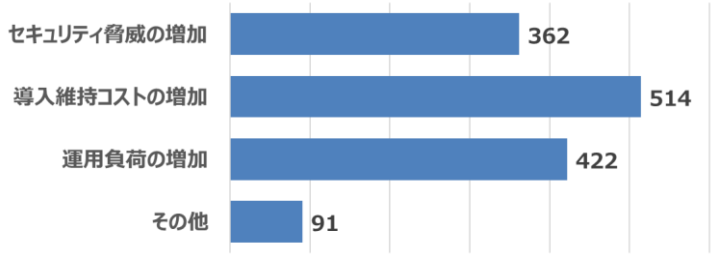
- ✓ **αモデルの団体のうち、政令指定都市では約８割、都道府県では約７割、中核市・特別区でも半数以上がβ・β‘移行を検討したことがある**が移行に至っていない。
- ✓ 移行を断念する理由として、「導入・維持コストの増加」、「運用負荷増加」、「セキュリティ脅威の増加」が挙げられていた。他に、「移行のタイミング」や「情報資産の棚卸し」についても挙げられている。

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

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。

検討の方向性

✓ αモデル採用団体のうち、β‘移行を希望している団体は一定数存在しているものの断念している場合が多い。
✓ β‘モデルに移行した団体から、β’移行にあたっての工夫点が共有されている。

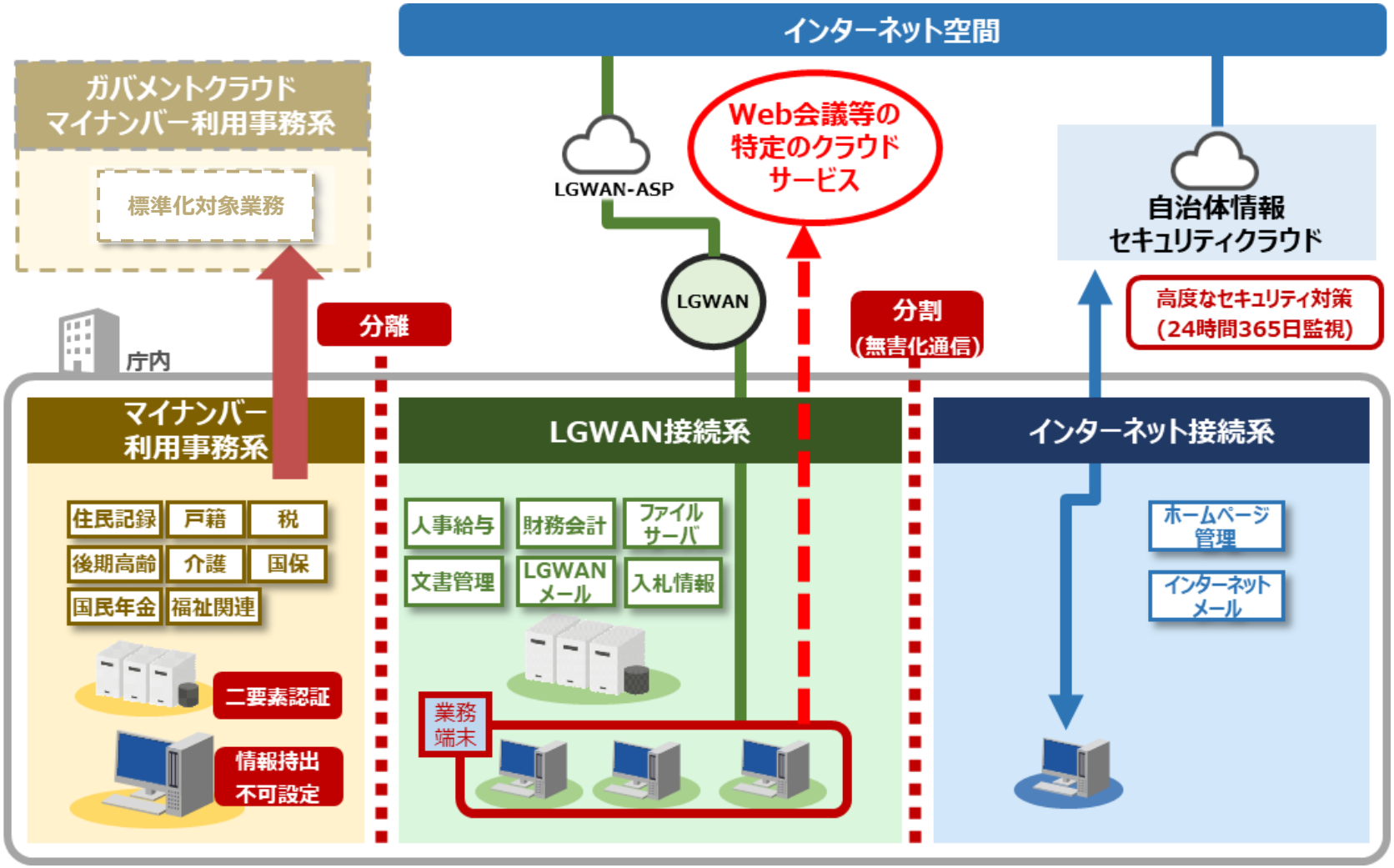
β‘移行の事例や移行にあたっての工夫を横展開することで、
β’モデルへの移行を推進

✓ 他方、政令指定都市以外の市町村の大多数が、業務環境がインターネットから分割されたαモデルの状態で、インターネットに接続しクラウドサービスを利用する必要があると考えられる。

セキュリティ対策を徹底の上、LGWAN接続系から
Web会議等の特定のクラウドサービスに対して
直接接続を行うモデル（α‘モデル）を提示

α´モデルについて　～LGWAN接続系からローカルブレイクアウト～

- ✓　LGWAN接続系から外部のクラウドサービスに接続（ローカルブレイクアウト）するための、必要なセキュリティ対策をガイドライン上で規定する必要がある。
- ✓　**<u>α'モデルのリスク評価を行い</u>**、評価結果を踏まえてガイドラインに必要なセキュリティ対策を規定する。



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、既にβ'モデルに移行している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

３．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

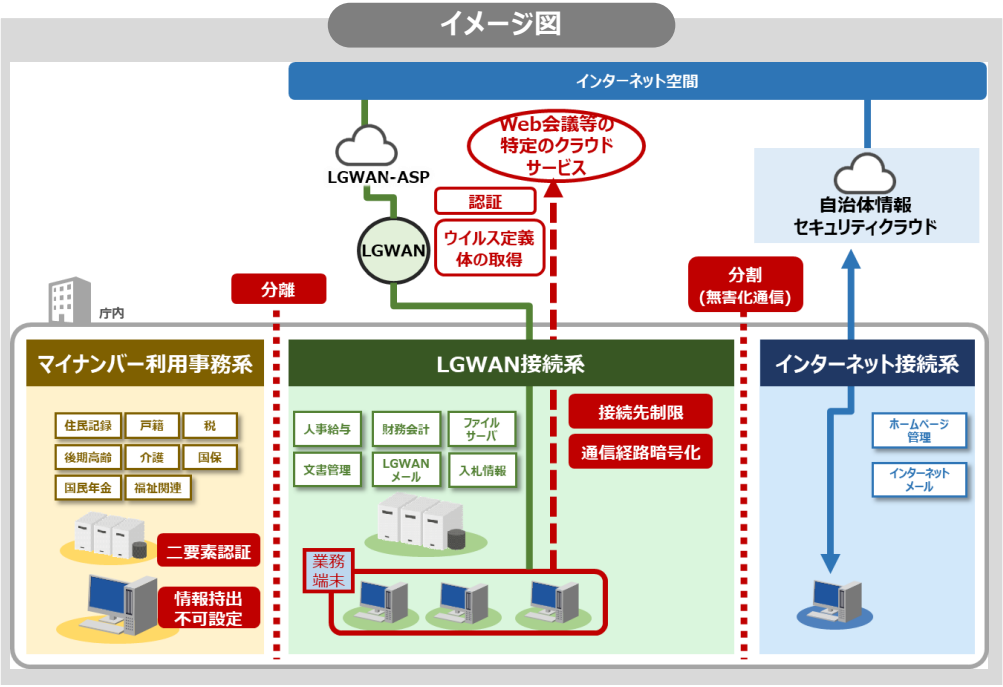
順番	作業の概要
①	**資産の定義とその重要度を定義する** 分析対象の資産を、物理的なまとまりや論理的な機能単位（サーバ、端末、装置等）の観点で定義すると共に、各資産の重要度を定義する。
②	**各資産に対する脅威とそのレベルを定義する** 脅威レベルの判断基準を定義し、その基準を基に、各資産に対して、資産の機能、ネットワーク構成や利用環境等を考慮して、想定される脅威とその脅威レベル（それが実行される可能性）を定義する。
③	**資産の各脅威に対する脆弱性を評価する** 各脅威に対するセキュリティ対策の各資産における対策状況（対策レベル）を評価することにより、当該脅威に対する脆弱性を評価す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

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）①

<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



※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。

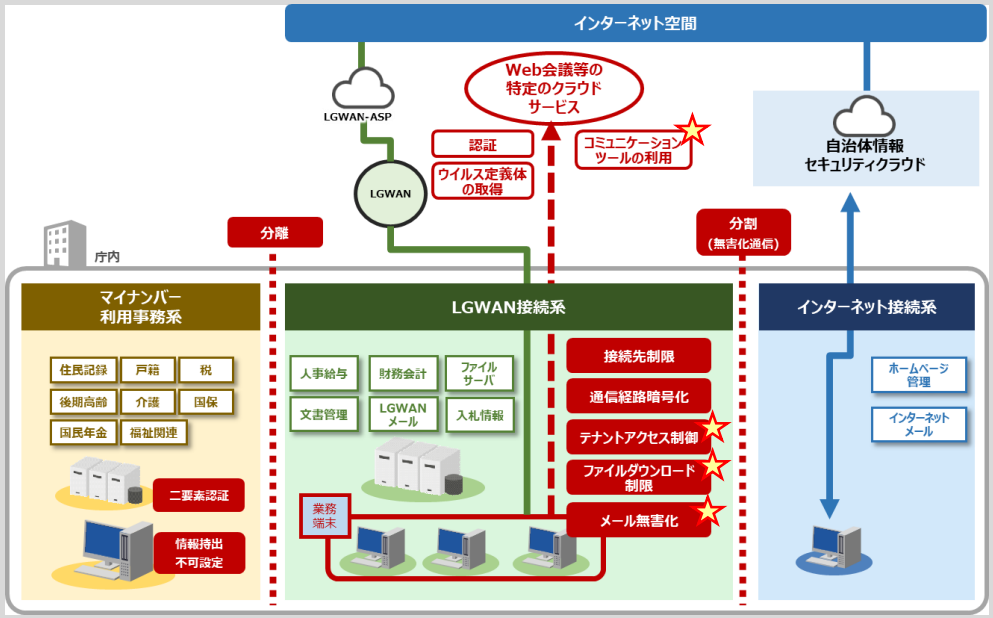
対策区分	セキュリティ対策	概要
技術的対策	接続先のクラウドサービスの証明書による認証	・接続先のクラウドサービスが本物であるか否か、正当性を確認する。
	マルウェア対策ソフト	・パターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。LGWAN接続系に配置する端末、業務サーバで対応が必要となる。
	パッチ適用	・脆弱性を修正するパッチを速やかに適用し、脆弱性を解消するLGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、接続系のスイッチ・無線APで対応が必要となる。
	接続先制限	・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）①

<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）①

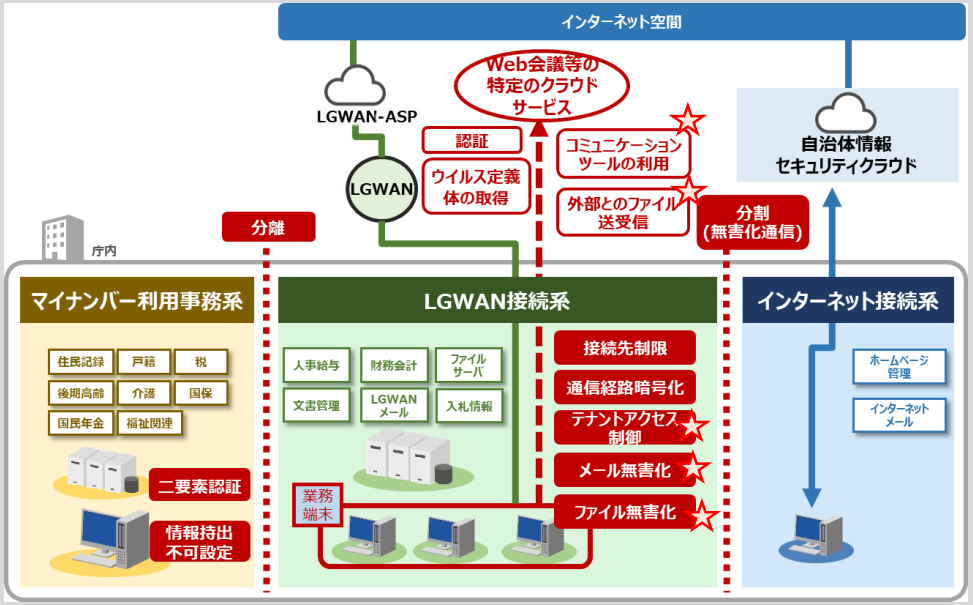
<クラウドサービスの利用条件>

- 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

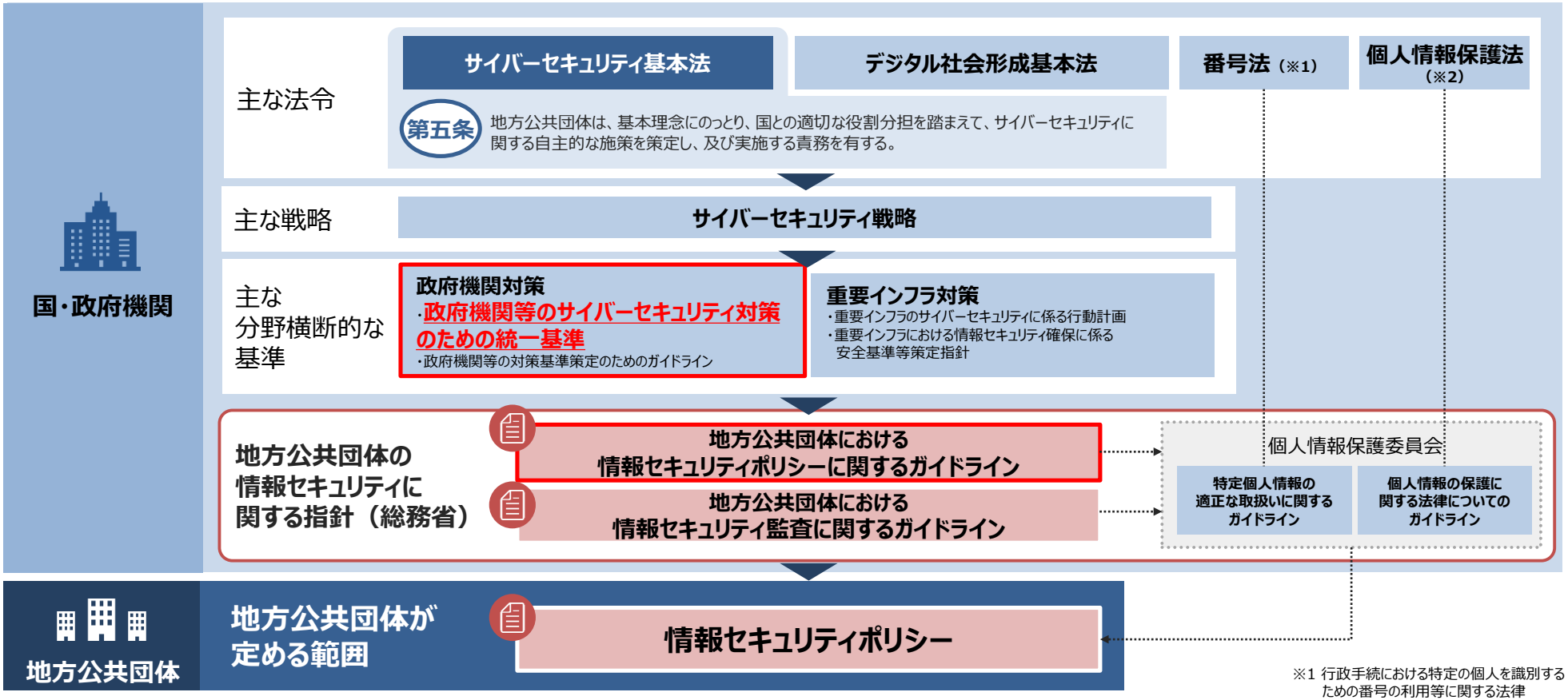


※各セキュリティ対策の性質に着目しセキュリティ対策を講じる場所を抽象化して表記している。また、すべての対策を網羅していないため、厳密な図とはなっていない。

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）	

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。

今後のスケジュール

✓　中間報告の内容や、令和５年度から６年度にかけて継続して議論した結果を踏まえ、ガイドラインの改定を6月下旬～７月に実施。

３月13日	検討会
３月末	**中間報告　公表**
４～６月中旬	検討会
６月下旬～７月	**改定・公表**