資料２－１

# 地方公共団体のセキュリティ対策に係る国の動きと地方公共団体の状況について

総務省

令和５年10月10日

総務省自治行政局

デジタル基盤推進室

# 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の改定等に係る検討会について

✓ 総務省では、「地方公共団体情報システム標準化基本方針」（令和４年10月 閣議決定）を踏まえ、地方公共団体の標準準拠システム等のクラウド利用に関する情報セキュリティ対策について、令和５年３月に「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」（以下「ガイドライン」という）の改定を行ったところである。
✓ 「デジタル社会の実現に向けた重点計画」や、NISC政府統一基準で新しく示されたセキュリティ対策等の動きを踏まえ、昨年度に引き続き、地方公共団体の情報セキュリティ対策について見直しを行うことが必要である。
✓ 昨今の背景を踏まえ、検討項目を６つ設定する。

| 背景 |
| --- |
| ✓ デジタル社会の実現に向けた重点計画<br>（「三層の対策」の見直し、ゼロトラストアーキテクチャー） |
| ✓ 地方公共団体向けサービスのクラウド化 |
| ✓ NISC政府統一基準で新たにゼロトラストアーキテクチャについて規定 |
| ✓ ガイドライン上の機密性分類と政府機関の機密性分類の違い |
| ✓ コンビニ交付サービスにおける証明書誤交付問題 |
| ✓ マイナンバー利用事務系と他の領域との画面転送に関する実施の要望 |

## 検討項目

1 β'モデル 移行のための支援方策の検討

2 LGWAN接続系のローカルブレイクアウト（α'モデル）の検討

3 令和５年度NISC政府統一基準群改定に関する対応

4 ガイドライン上の機密性分類と政府機関の機密性分類の考え方の違いや具体例の追記

5 情報システムの品質管理の推進に関する対応

6 マイナンバー利用事務系と他の領域との画面転送要件の検討

1　β’モデル 移行のための支援方策の検討/

2　LGWAN接続系のローカルブレイクアウト（α ’ モデル）の検討

# 「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)

- ✓ 重点計画において、**地方公共団体の意見を踏まえた「三層の対策」の見直し**と**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への対応が掲げられている。
- ✓ **地方公共団体の状況を把握**しつつ、NISCの統一基準の中で政府機関等のセキュリティ対策として新たに示された**ゼロトラストアーキテクチャの考え方**を踏まえる必要がある。

第３－２ 各分野における基本的な施策

１． 国民に対する行政サービスのデジタル化

（１）国・地方公共団体・民間を通じたトータルデザイン

② 実装に向けた取組

イ 安全性と利便性の両立を追求するネットワーク環境

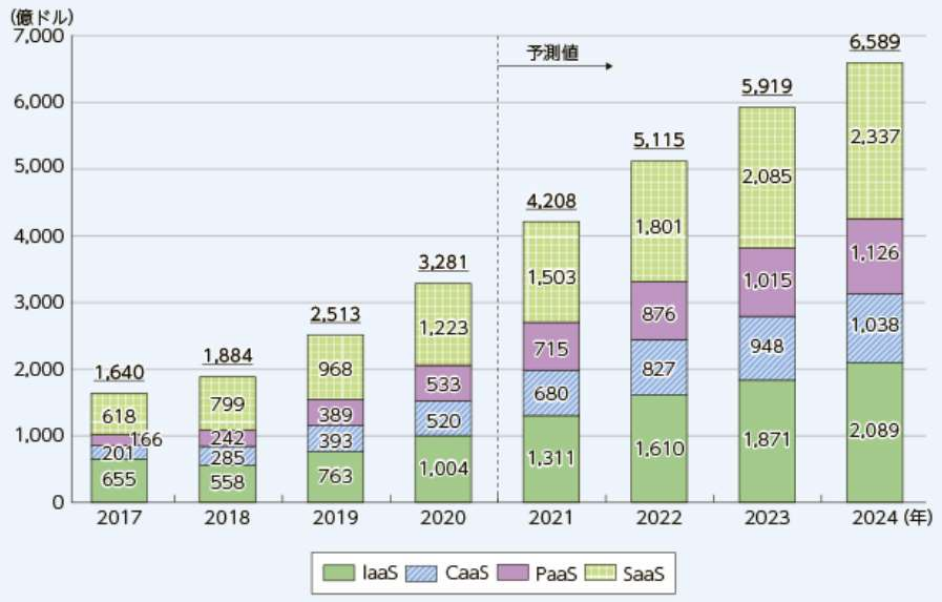
インフラの検討は、技術的・環境的な変化や地方公共団体の課題を踏まえ、不断に進める。国・地方を通じたデジタル基盤に関して、全体最適かつ効率的なネットワーク構成となるよう、強固なセキュリティ基盤の具備、ユーザー利便性の向上、安定的な運用体制、強靱性の確保の観点も念頭に、将来像及び実現シナリオについて、具体的に検討を進めることとする。特に、地方公共団体のセキュリティについては、ガバメントクラウドやSaaS等のクラウドサービスの利活用、職員の効率的な働き方の実現、新しい住民サービスの迅速な提供等を可能にするため、**「地方公共団体における情報セキュリティポリシーに関するガイドライン」を継続的に見直す**。**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**。

# 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。**

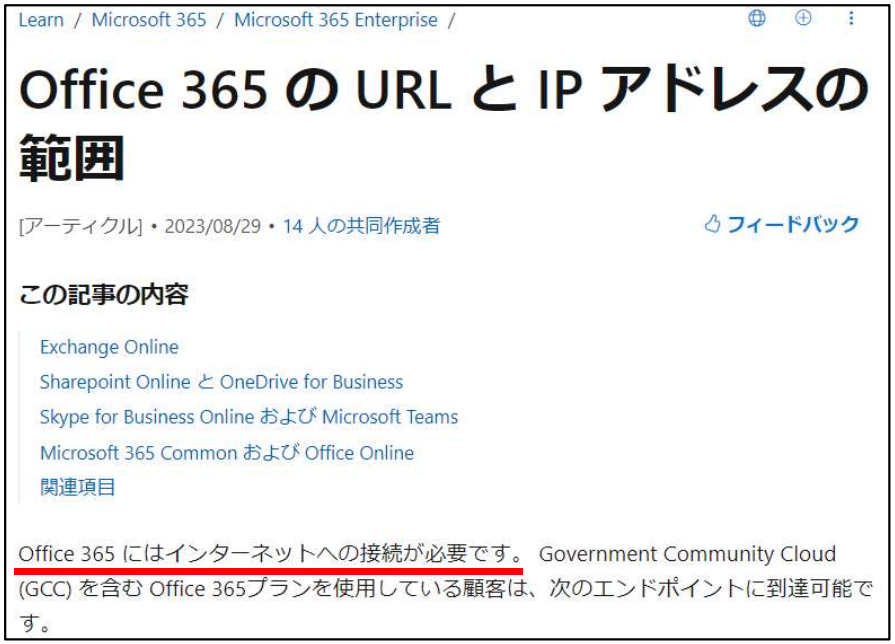



図表3-6-8-1　世界のパブリッククラウドサービス市場規模（売上高）の推移及び予測

- 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

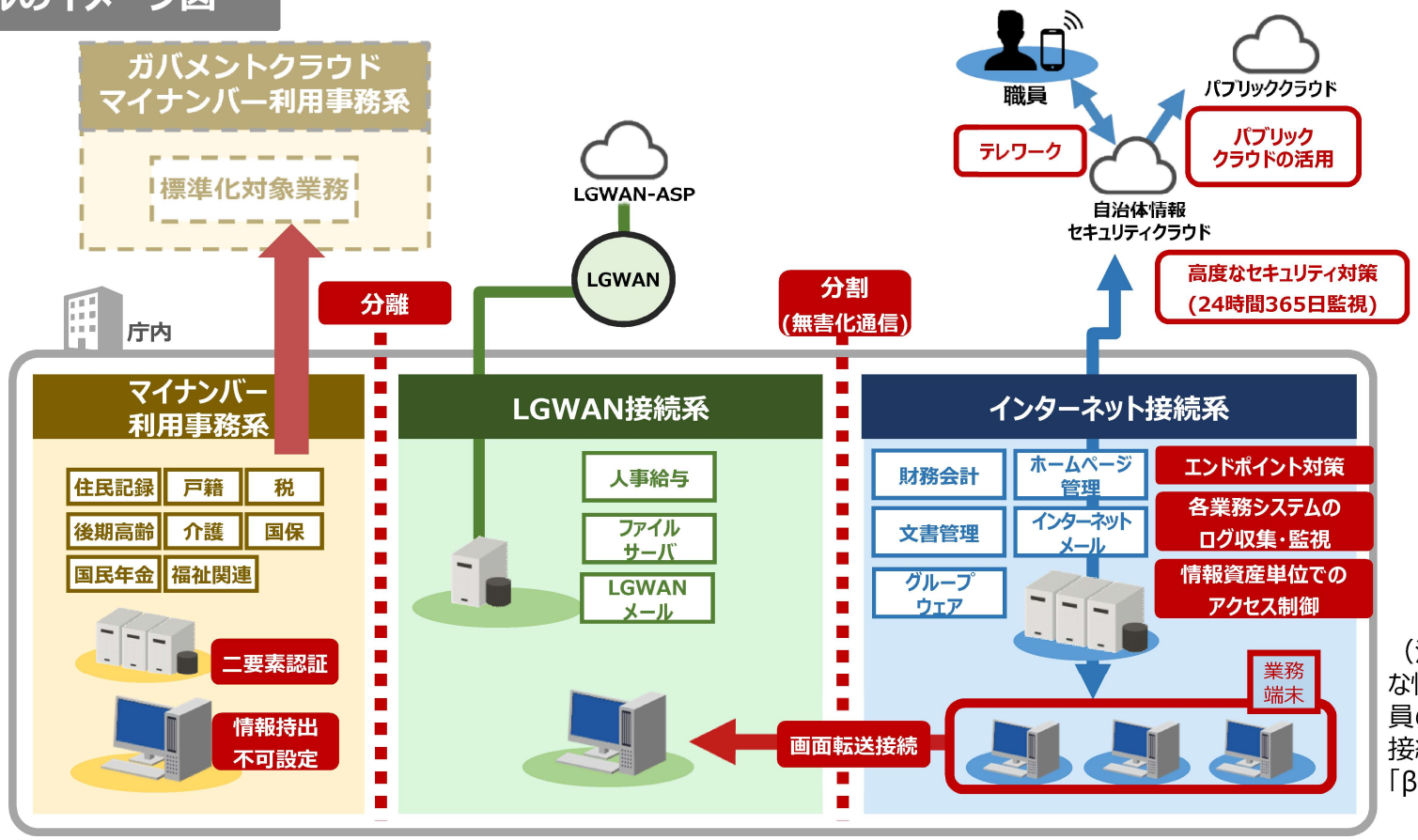
Office 365 にはインターネットへの接続が必要です。 Government Community Cloud (GCC) を含む Office 365プランを使用している顧客は、次のエンドポイントに到達可能です。

（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



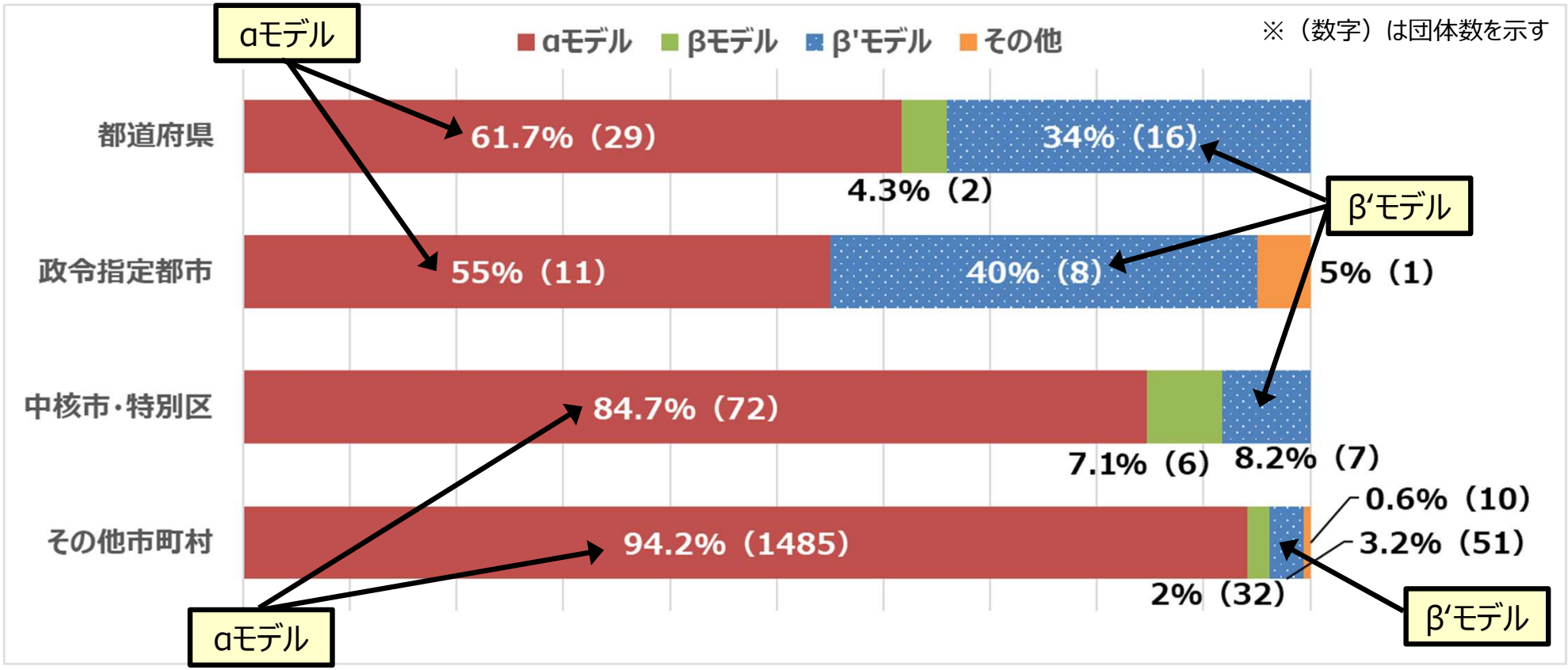

（注）βモデルのうち、重要な情報資産(入札情報や職員の情報等)をインターネット接続系に配置する場合は「β'モデル」としている。

※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<br>47団体 | 政令指定都市<br>20団体 | 中核市・特別区<br>85団体 | その他市町村<br>1578団体 |
|---|---|---|---|---|
| 合計 | 1730団体 | | | |

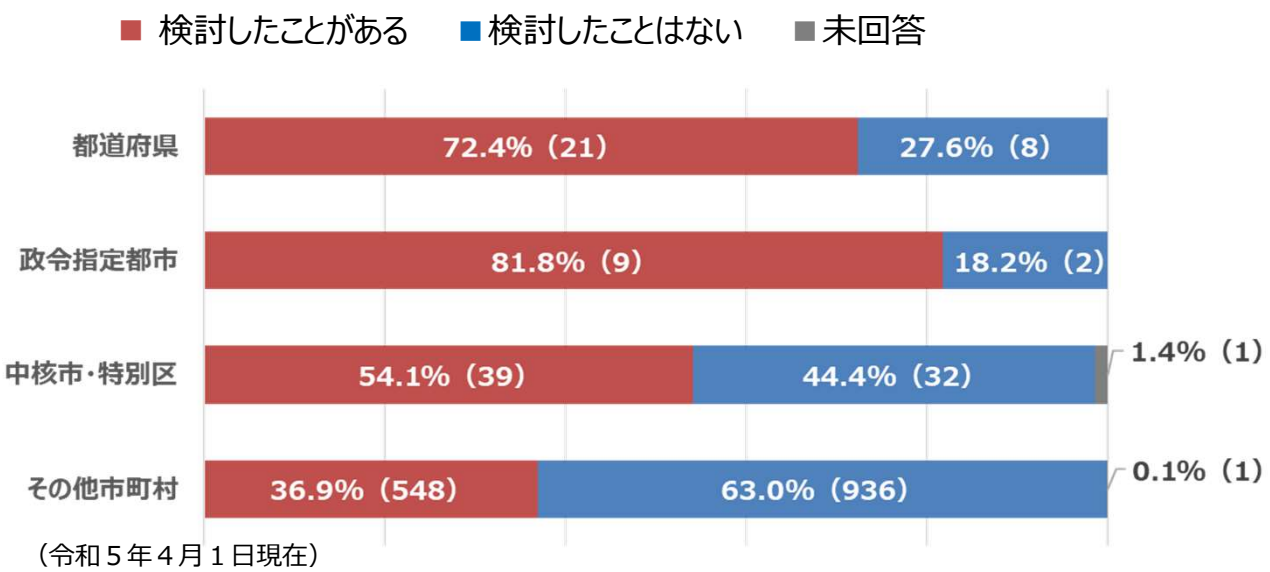



（令和５年４月１日現在）

# αモデルの団体がβ・β‘モデル移行を断念している理由

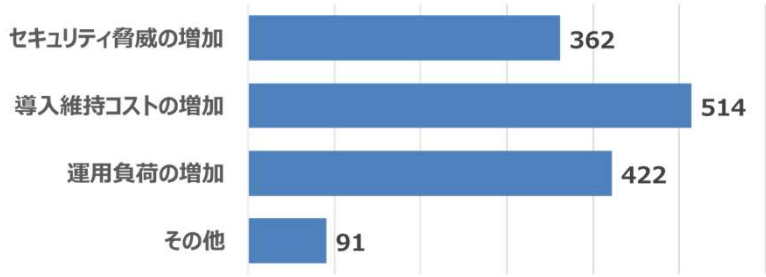
- ✓ **<u>αモデルの団体のうち、政令指定都市では約８割、都道府県では約７割、中核市・特別区でも半数以上がβ・β‘移行を検討したことがある</u>**が移行に至っていない。
- ✓ 移行を断念する理由として、「導入・維持コストの増加」、「運用負荷増加」、「セキュリティ脅威の増加」が挙げられていた。他に、「移行のタイミング」や「情報資産の棚卸し」についても挙げられている。

## 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

# αモデルからβ'モデルへ移行した際の工夫点

✓ αモデルからβ'モデルのネットワーク構成に移行した82団体における工夫点は以下のとおり。

## 人材のスキル面

### 専門職員の確保

- 庁内公募（ネットワーク知識）
- 長期に情報担当課に勤務する職員（常駐SEを含む）が存在
- 他団体との意見交換・聴取
- 行政（ICT）枠の職員採用
- 外部研修への参加

### 全職員の知識・スキル向上

- 段階に分けて経営層や管理職、全職員に周知
  - ✓ 目指すべきβ'モデルの明確化（ネットワーク・システム構成および利用者視点での変更点　など）
  - ✓ β'への移行方針の策定（移行体制・役割分担の整理、スケジュール、費用　など）
  - ✓ 説明用のコンテンツの準備（コンテンツ、操作手順　など）
  - ✓ 職員への周知、イントラ掲載（朝会、研修会およびFAQの充実　など）

## 委託事業者の活用

### 有識者の確保

- β'モデルに知見のある事業者の人員確保
- 庁内NW管理事業者との調整

### 構想検討の支援

- 設計業務の外部委託以外に中立的な立場でのアドバイスをもらうためにコンサルタントを契約した
- 責任分界点を意識した
- 既設ネットワーク導入業者等を選定し設計業務を外部委託した

### 技術的な支援

- 技術的な観点で、既存の構成から現実的な移行を実現するために既存の委託事業者へ外部委託
  （EDR、VDI、セキュアブラウザなどの検討項目を提示）

### 委託事業者との検討期間（一例）

- ２年間（定期的な検討会）

## セキュリティ対策面

### EDR（エンドポイント）

- 県のセキュリティクラウドの活用

### ログ管理・監視

- 資産管理ソフトとEDRの連携（監視運用の設計も含む）

### メール対策

- メール無害化の継続
  （インターネットから受信するメールは引き続き無害化の構成）

### その他

- 庁内システムへの通信要件の再精査
- Webフィルタリング
- シンクライアントの導入
- AI振る舞い検知
- 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

# 今後の方向性

✓ 団体のネットワーク環境に応じた支援を検討することとしてはいかがか。

✓ 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‘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。

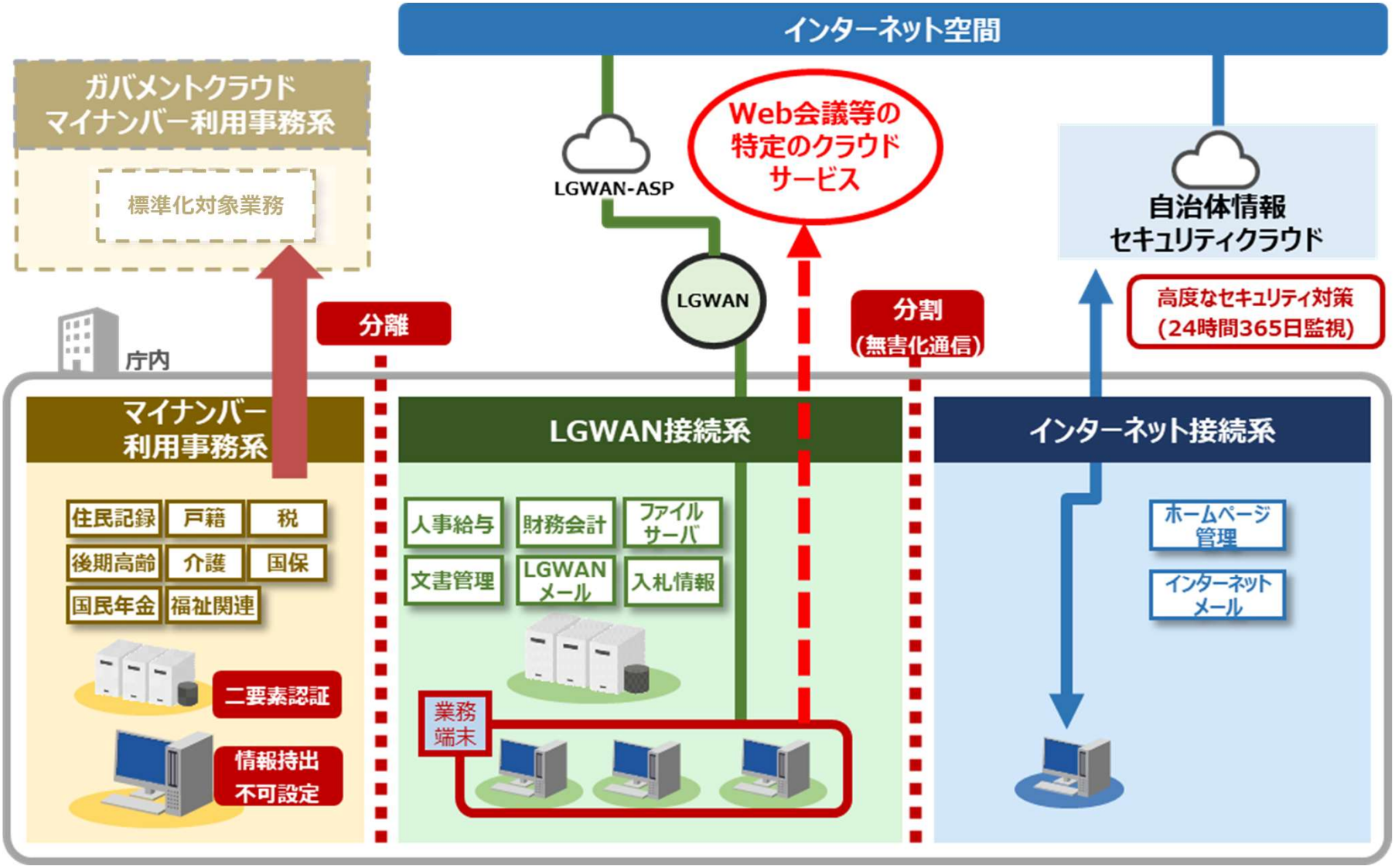
**β‘移行の事例や移行にあたっての工夫を横展開することで、**
**β’モデルへの移行を推進してはいかがか。**

✓ 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）を検討してはいかがか。**

# 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～

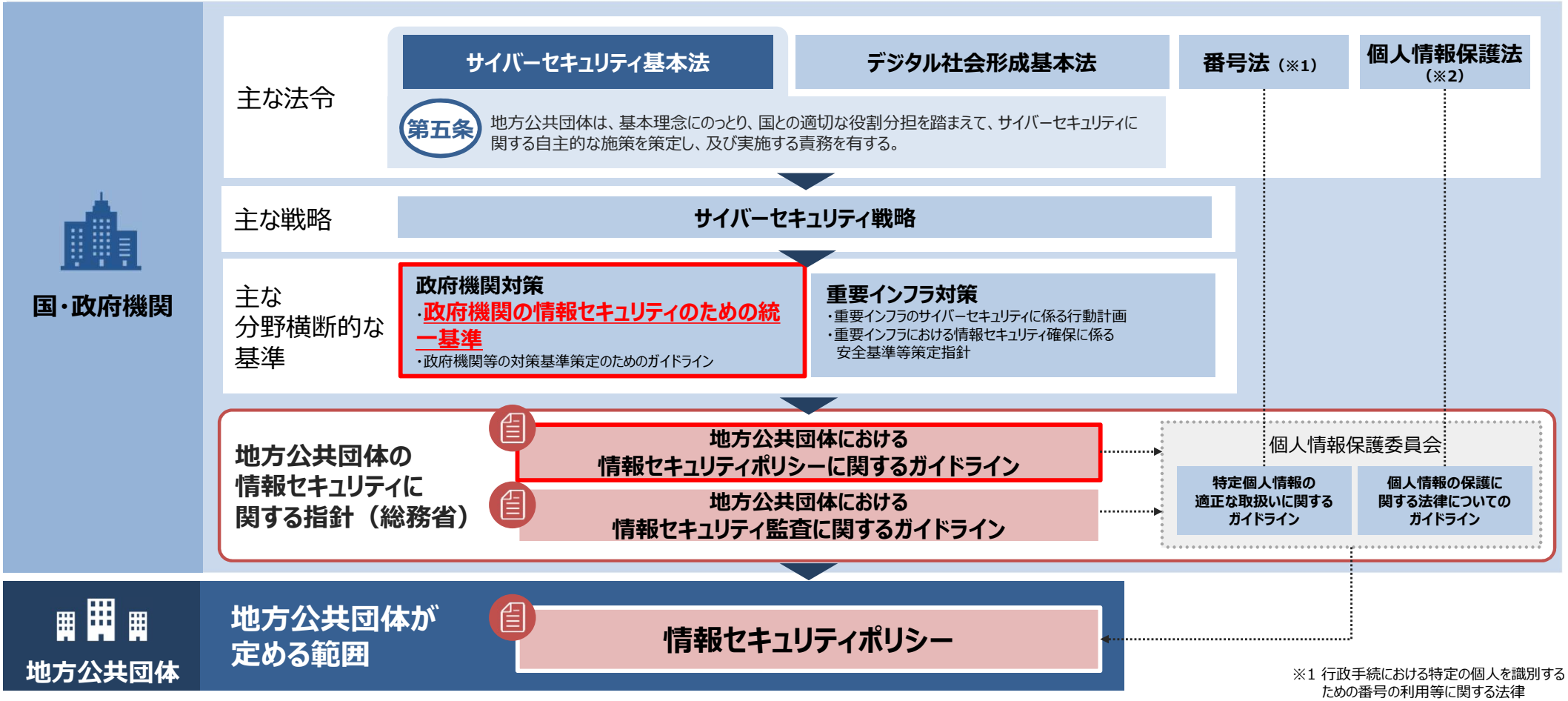
- ✓　LGWAN接続系から外部のクラウドサービスに接続（ローカルブレイクアウト）するための、必要なセキュリティ対策をガイドライン上で規定する必要がある。
- ✓　**<u>α'モデルのリスク評価を行い</u>**、評価結果を踏まえてガイドラインに必要なセキュリティ対策を規定する。



# ３　令和５年度NISC政府統一基準群改定に関する対応

# NISC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、NISCの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

# 【参考】政府統一基準群の見直しについて

✓ NISCの統一基準の改定ポイントは大きく以下の５つあり、ガイドラインに反映させるのが望ましいのではないか。

## １．情報セキュリティに関するサプライチェーン対策の強化

- 業務委託における政府の情報を保護するため、米国NISTのサプライチェーン対策を参考に、情報へのアクセス制御、ログの取得・監視などの委託先に担保させるべき情報セキュリティ対策を契約に含めるとともに、委託期間を通じた実施を求める。

## ２．クラウドサービスの利用拡大を踏まえた対策の強化

- 独立行政法人等へのISMAP拡大や、ISMAP-LIU運用開始等を踏まえ、要機密情報を取り扱う場合のクラウドサービスはISMAPクラウドサービスリストから選定することを明記する。
- 要機密情報を取り扱わない場合においても、適切な主体認証やアクセス制御の管理などのクラウドサービスを安全に利用するための対策を講ずる。また、調達行為を伴わないクラウドサービスを利用する場合には、「調達行為を伴わないSNS等の外部サービスの利用等に関する申合せ」に基づき、講ずべき措置についてNISCに助言を求める。

## ３．ソフトウェア利用時の対策の強化

- 機器等調達時のIT調達申し合わせに基づく対応を必須のものとして明記する。また、重要なソフトウェアについて、設定手順の整備、設定の定期的な確認、教育の実施など、運用時の情報セキュリティ水準を維持するための対策を講ずる。
- 従来の対策に加え、サーバ装置や端末等の運用開始時において、脆弱性診断の実施などソフトウェアの脆弱性対策を強化する。

## ４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

- 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に係る対策や情報システムの復旧のための対策を講ずる。
- 昨今のサービス不能攻撃（DDoS攻撃）を踏まえ、専用の対策装置やサービスの導入、サーバ装置や通信回線等の冗長化などの対策や、サービス不能攻撃を受けることを想定した監視方針の策定や脅威情報の収集等の対策を講ずる。
- クラウドサービスの利用の拡大に対応するため、常時診断・対応型セキュリティアーキテクチャを実装することを念頭に、情報資産等へのアクセスを常時診断・検証して、アクセスを許可又は拒否する新たな技術的手法を講じる際に必要な対策を規定（※）。 ※ゼロトラストアーキテクチャに該当。

## ５．組織横断的な情報セキュリティ対策の強化と情報システムの重要度に応じた対策の確保

- 監査等から得られた組織横断的に改善が必要な事項について、進捗状況を定期的にCISOに報告し、CISOは監査結果に基づく改善進捗を把握・組織の統制を図る。
- 所管独法等の情報セキュリティ対策を支援するため、府省庁側に必要な体制を整備する。独法等は専門的知見を要する事項等について所管省庁等へ助言を求める。
- 情報システムの重要度より高度な対策情報システムの重要度の考え方を導入。全ての情報システムに求める必須の対策に加えて、基幹業務システムなどより重要度の高い情報システムについては、リアルタイムにログ分析を行う機能の導入などの高度な対策を求める。

# 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（令和５年度）の改定内容

- ✓ NISC政府統一基準にて、新たにゼロトラストアーキテクチャについて規定された。
- ✓ 最新の政府統一基準の内容を踏まえた見直しを実施することが望ましいのではないか。

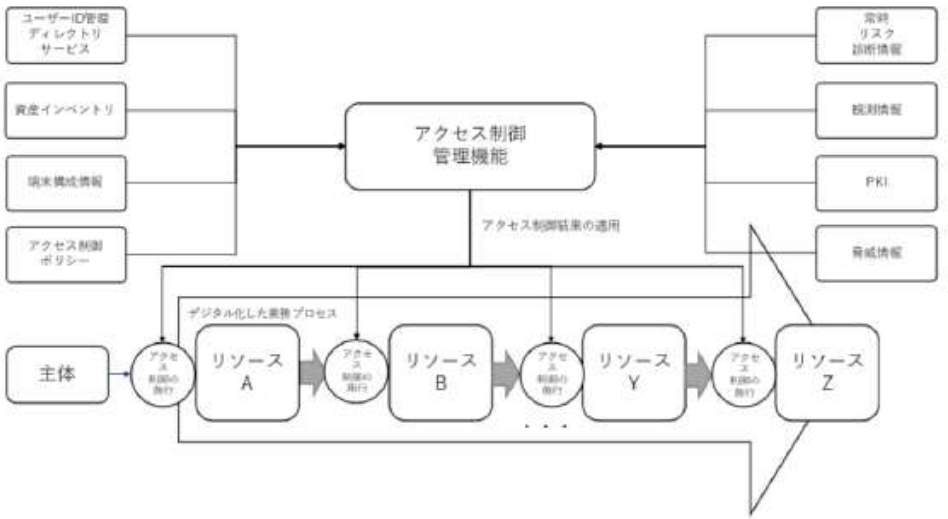
## 7.3 ゼロトラストアーキテクチャー（改定のポイント）

NISC

「7.3 ゼロトラストアーキテクチャ」

- 「ゼロトラストアーキテクチャ」は、組織内外を問わずネットワークは常に侵害されているものであるとの前提のもと、情報資産を保護し、情報セキュリティリスクの最小化を図るための情報セキュリティ対策における論理的・構造的な考え方である。
- 本節では、ゼロトラストアーキテクチャに基づく情報資産の保護策の１つであり、アクセス制御の仕組みを実現する機能の一部と考えられる動的アクセス制御（※）を実装する場合に特に必要となる対策事項を規定する。

※「動的なアクセス制御」とは、特定のアクセスに対して、セッションが確立してない操作ごとに、都度、アクセス元の信用情報を動的に評価し、アクセス先が信用できる状態であるかを検証したうえで、特定のリスクが検出された場合には追加の認証を求めることや、アクセスを拒否する等のアクセス制御を行うことを想定している。




ゼロトラストアーキテクチャ概念図
（出典）ゼロトラストアーキテクチャ適用方針（デジタル庁）

■改定のポイント

- 複数の情報システム間で横断的な対策の企画・推進・運用に関する事務の責任者として、情報システムセキュリティ責任者を選任（7.3.1(1)）
- 動的なアクセス制御の導入方針を定めるにあたり、動的アクセス制御の対象とする情報システムと対象とする情報システムのリソース（ユーザーアカウント、機器等）を識別（7.3.1(2)）
- 動的なアクセス制御の実装にあたり、リソースの信頼情報の変化に応じた動的なアクセス制御のポリシーを作成し、動的なアクセス制御のポリシーに基づき、動的なアクセス制御を行う（7.3.1(3)）
- 動的なアクセス制御の運用に際し、アクセスパターンの変化に応じて、再度リスク評価を行い、動的なアクセス制御のポリシーを見直す。また、リソースの信頼情報の収集により検出されたリスクへ対処を行う。（7.3.2）

# ４　ガイドライン上の機密性分類と政府機関の機密性分類の考え方の違いや具体例の追記

# 「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」における機密性の記載

✓ **政府統一基準において**、最も機密性に配慮すべき情報である機密性３情報に含まれるのは、国家安全保障に係る極秘文書及び秘文書であり、**個人情報は、機密性２情報に含まれる**。

| | |
|---|---|
| 機密性３情報 | 国の行政機関における業務で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成23年４月１日内閣総理大臣決定。以下 「文書管理ガイドライン」という。） に定める秘密文書※としての取扱いを要する情報 |
| 機密性2情報 | 国の行政機関における業務で取り扱う情報のうち、**行政機関の保有する情報の公開に関する法律（平成11年法律第42号。以下「情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報**であって、「機密性３情報」以外の情報 |
| 機密性1情報 | 国の行政機関における業務で取り扱う情報のうち、情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報 |

※秘密文書とは（第10）
極秘文書　秘密保全の必要が高く、その漏えいが国の安全、利益に損害を与えるおそれのある情報を含む行政文書
秘文書　　極秘文書に次ぐ程度の秘密であって、関係者以外には知らせてはならない情報を含む極秘文書以外の行政文書

◎行政機関の保有する情報の公開に関する法律（平成11年法律第42号）
第五条　行政機関の長は、開示請求があったときは、開示請求に係る行政文書に次の各号に掲げる情報（以下「不開示情報」という。）のいずれかが記録されている場合を除き、開示請求者に対し、当該行政文書を開示しなければならない。

一　個人に関する情報（事業を営む個人の当該事業に関する情報を除く。）であって、当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項をいう。次条第二項において同じ。）により特定の個人を識別することができるもの（他の情報と照合することにより、特定の個人を識別することができることとなるものを含む。）又は特定の個人を識別することはできないが、公にすることにより、なお個人の権利利益を害するおそれがあるもの。

# 総務省「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」における機密性の記載

- ✓ 現行の総務省ガイドラインにおいて、以下のとおり機密性の分類がなされているが、各分類の具体的な例は示されていない。
- ✓ 令和２年８月18日付総行情第111号別添において、ガイドラインにおける機密性３情報の例として個人情報が挙げられており、**個人情報は、ガイドラインにおいて最も機密性に配慮すべき情報として扱われている**といえる。

| | |
|---|---|
| 機密性３情報 | 行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産 |
| 機密性2情報 | 行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産 |
| 機密性1情報 | 機密性２又は機密性３の情報資産以外の情報資産 |

（注）
機密性３情報の例・・・住民の個人情報、職員の個人情報、施設設計情報や入札予定価格など非公開情報
機密性２情報の例・・・政策検討に関する情報
※令和２年８月１８日付総行情第111号
「新型コロナウィルスへの対応等を踏まえたLGWAN接続系のテレワークセキュリティ要件について」の別添で地方公共団体に通知

# 背景及び今後の方向性

- ✓　現行の総務省ガイドラインの機密性分類について、どのような情報を想定しているかの具体的な記載がないため、政府機関等における機密性の分類との違いがわかりにくい。
- ✓　**政府機関等における機密性３情報に相当する情報を扱う情報システムは、ガバメントクラウドの利用対象外**で、機密性２情報（個人情報含む）に相当する情報を扱う情報システムについては、ガバメントクラウドの利用を原則とされている（※）ため、総務省ガイドラインと政府機関等統一基準の違いを知らず、「個人情報を扱う地方公共団体の情報システムは、ガバメントクラウドの利用ができないのではないか」と混乱するケースが発生した。
- ✓　地方公共団体では、税や住民基本台帳、生活保護等の業務があるため、個人情報を業務で使用する頻度が政府機関よりも圧倒的に多く、情報漏えい等のリスクも大きいと考えられる。

- ✓　**現行の総務省ガイドラインの考え方を変えず、個人情報を最も機密性に配慮すべき情報（機密性３情報）として扱うことが望ましいのではないか。**
- ✓　**具体例の追記や政府機関の分類との相違を明記する必要があると考えられる。**

※「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」（令和４年12月28日デジタル社会推進会議幹事会決定）

# ５　情報システムの品質管理の推進に関する対応

# 背景及び今後の方向性

✓　コンビニ交付サービス等の証明書発行サーバにおいて、誤ったプログラム処理が生じたことにより、別人の証明書が交付される事案が発生した（※）　。

**サービスの品質確保や個人情報保護の観点から、一連の事案で顕在化した課題に対応するための対策を、具体例を交えつつ記載してはいかがか。**

## ○コンビニ交付サービス等において別人の証明書が交付された事案

| 団体 | ① | ② | ③ | ④ | ⑤ |
|---|---|---|---|---|---|
| **原因** | 証明書発行サーバに交付申請が集中した際に、**誤ったプログラム処理が生じ**、証明書データの取り違えが発生 | 証明書発行サーバの印刷処理と同サーバに対する住民基本台帳システムからの住民票データの反映処理が同時に行われた際に、**誤ったプログラム処理が生じ**、証明書データの取り違えが発生 | 証明書発行サーバと戸籍システムの間の当該自治体固有の連携システムにおいて、２名の同時申請が行われた場合に、**誤ったプログラム処理が生じ**、証明書データの取り違えが発生 | 庁内証明書交付サービスとコンビニから同時に交付申請があった場合に、サーバにおいて**誤ったプログラム処理が生じ**、証明書データの取り違えが発生 | 庁内証明書交付サービスにおいて、住所変更等の手続後、システム更新中に申請があった場合に、サーバにおいて**誤ったプログラム処理が生じ**、証明書データの取り違えが発生 |
| **延べ件数<br>事案発生日** | 10件<br>R5年3月27日 | 2件<br>R5年3月22日、4月18日 | 1件<br>R5年5月2日 | 1件<br>R5年3月27日 | 1件<br>R5年6月28日 |
| **誤交付した証明書** | • 住民票の写し<br>• 住民票記載事項<br>• 印鑑登録証明書 | • 住民票の写し<br>• 印鑑登録証明書 | • 戸籍全部事項証明書 | • 戸籍全部事項証明書の一部 | • 住民票の写し |
| **その後の対応** | • プログラムを修正<br>• 3月31日付け事務連絡で総務省から自治体に運用監視の徹底を要請 | • プログラムを修正<br>• 5月2日付け事務連絡で自治体に証明書発行サーバの運用管理を委託している事業者への点検を依頼 | • プログラムを修正<br>• 5月10日付け事務連絡で関連システムを含めて誤交付が生じうる仕組みとなっていないか至急点検するよう要請 | • システムを停止<br>• 5月22日付け通知で、証明書発行サーバ及びこれと連携する印鑑登録等の各業務システムの総点検の徹底を要請 | • プログラムを修正（適用漏れしていた修正プログラムを適用）<br>• ベンダーにおいてシステム利用団体の再点検を実施 |

※参考資料「コンビニ交付サービスにおける住民票等誤交付事案に対する個人情報の保護に関する法律に基づく行政上の対応について」（令和５年９月 20 日個人情報保護委員会）参照。

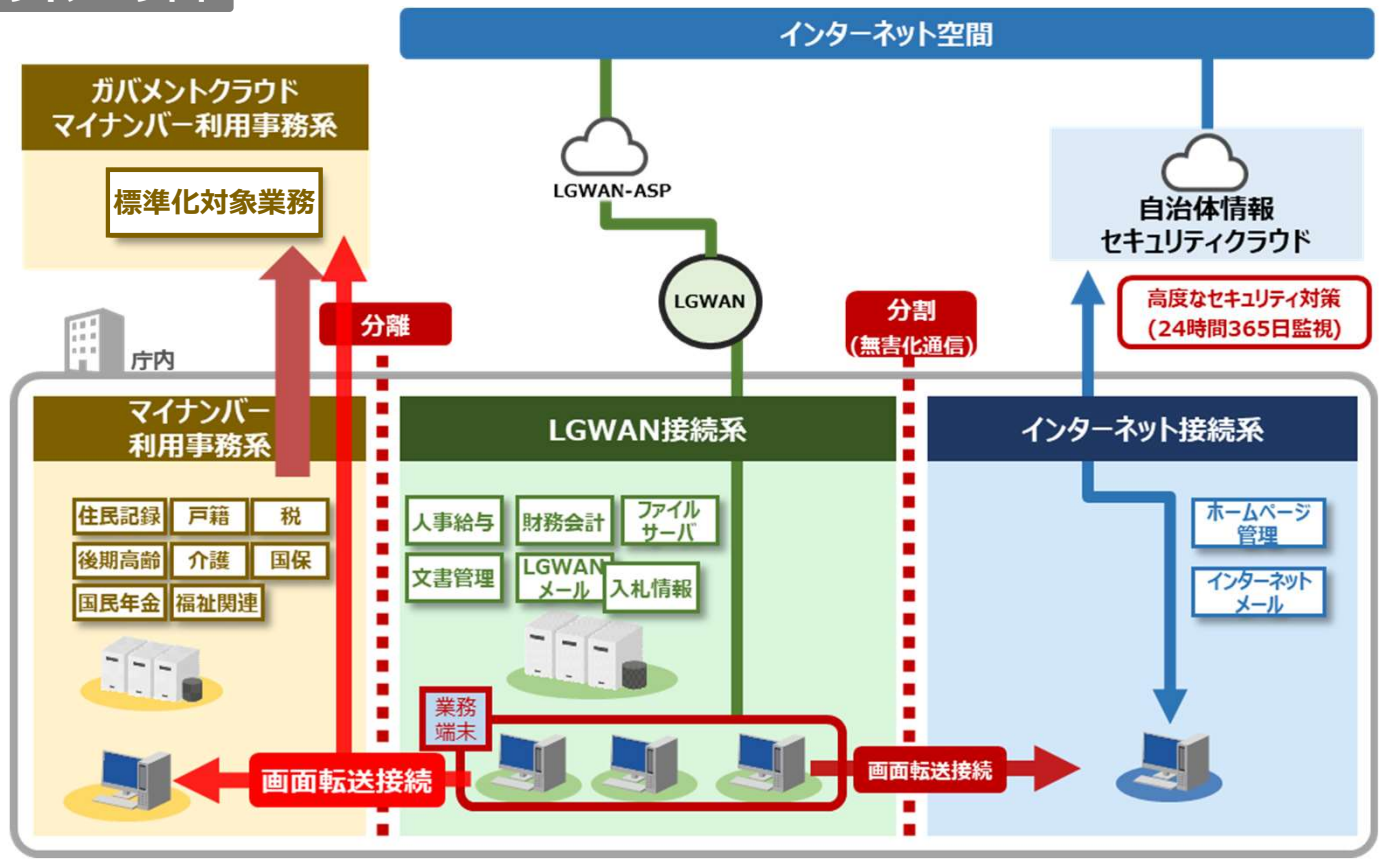
# ６　マイナンバー利用事務系と他の領域との画面転送要件の検討

# 画面転送のイメージ

✓ 複数の団体から、利便性向上の観点でマイナンバー利用事務系と他の領域との画面転送実施の要望がある。
✓ 三層分離の根本的な見直しにつながるため、慎重な検討が必要となる。

✓ **<u>２年間かけて検討</u>**することとし、**<u>１年目（今年度）は、次年度に評価を実施する上で、リスク評価の手法（どのようなケースを想定すべきか等）について検討する</u>**こととしてはいかがか。
✓ ２年目にリスク評価及び評価結果を踏まえ、必要なセキュリティ対策を記載することとしてはいかがか。

**αモデルのイメージ図**




※ マイナンバー利用事務系の業務システムがガバメントクラウドにリフトされる点を考慮する必要がある。
※ ネットワークモデル（α、β、β´）によって、画面データ転送先のセグメントが異なる。右図はαモデルの場合となる。

# 令和５年度のガイドライン改定の進め方について（イメージ）

- ✓ 以下のようなスケジュールで、検討会や地方公共団体への意見照会等を行い、ガイドライン改定を実施。
- ✓ LGWAN接続系のローカルブレイクアウト（α′モデル）の検討については、リスク評価を行う必要性から、今年度第３回目に改定案の提示を予定。

| イベント等 | 10月 | 11～12月 | 1月 | 2月～ |
|---|---|---|---|---|
| 検討会（年度の中での回数を記載） | 第１回<br>（10月10日） | 第２回 | 第３回 | 第４回 |
| 方向性・論点の整理 | → | α´モデル以外 | α´モデル | |
| ガイドライン改定案の提示 | | ★ | ★ | |
| 地方公共団体への意見照会・意見反映 | | | → | |
| ガイドライン修正案の提示 | | | | ★ |
| パブリックコメントの実施・意見反映 | | | | → |
| ガイドライン改定、公表 | | | | 改定・公表 |

# （参考）自治体情報システムの標準化・共通化、LGWAN更改のスケジュール

| 事項 | | 2023年度 | 2024年度 | 2025年度 |
|---|---|---|---|---|
| 自治体情報システムの標準化・共通化 | 地方自治体の取組 | 全20業務の基幹業務システムについて標準準拠システムへの移行 | | |
| | ベンダの取組 | 標準準拠システムの開発 | 標準準拠システムへの移行作業 | |
| | デジタル庁の取組 | ガバメントクラウドの調達、提供 | | |
| | | ガバメントクラウド実証事業等によるベストプラクティスの横展開 | | |
| | | 適合確認試験等の実施<br>データ要件・連携要件、共通機能等に係る制度改正への対応 | | |
| | | 標準準拠システムへの移行支援<br>（全国の約34,000システムが対象） | | |
| | 制度所管省庁の取組 | 標準仕様書に係る制度改正等への対応 | | |
| LGWANの更改 | 現行LGWAN | 2025年度末まで運用 | | |
| | 次期LGWAN | 設計・構築 | 運用開始 | |

移行