

# 次期LGWANの検討状況（セキュリティ関係）

令和5年2月21日

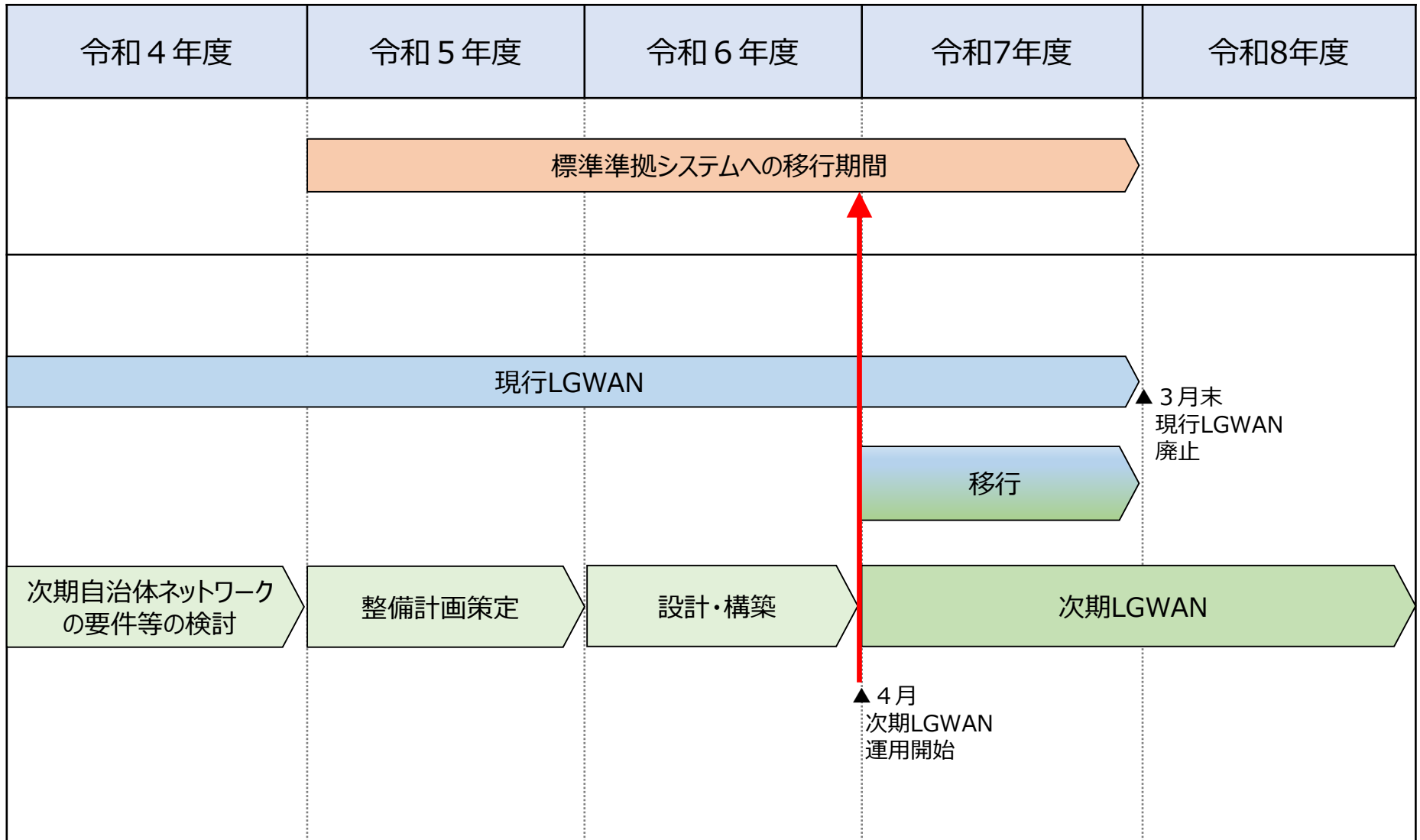
地方公共団体情報システム機構

---

# 1 次期LGWANの検討について

---

# LGWAN更改に関する全体スケジュール



# 次期LGWANに関する検討会について

## <目的>

次期LGWANに求める要件等について、自治体の観点からの議論・検討を行うため、「次期LGWANに関する検討会」を設置。

## <委員>

佐々木 良一（座長）	東京電機大学 名誉教授 兼 東京電機大学 サイバーセキュリティ研究所 客員教授
安藤 昌弘	神奈川県 総務局 デジタル戦略本部室 情報システム担当課長
中後 康	滋賀県 総合企画部 DX推進課 課長
山縣 敦子	大阪府 スマートシティ戦略部 戦略推進室 地域戦略推進課 課長
北村 卓司	香川県 政策部 デジタル戦略総室情報システム課 専門監
甲斐 慎一郎	宮崎県 総合政策部 デジタル推進課 課長
安藤 篤哉	仙台市 まちづくり政策局デジタル戦略推進部 情報システム課 課長
吉岡 幹仁	神戸市 企画調整局 デジタル戦略部情報システム担当 課長
倉島 恭一	杉並区 政策経営部 情報管理課情報システム担当 課長
植村 道広	都城市 総務部 情報政策課 課長
萩原 和幸	美里町 総合政策課 副課長兼まち創生係長
阿部 知明	デジタル庁審議官 デジタル社会共通機能グループ 次長
湯本 博信	デジタル庁審議官 戦略・組織グループ 特命担当次長
三橋 一彦	総務省 大臣官房審議官

## <オブザーバ>

浅見 良雄	地方公共団体情報システム機構 理事（非常勤）
上杉 卓志	地方公共団体情報システム機構 理事（非常勤）
崎山 雅子	地方公共団体情報システム機構 理事（非常勤）

## <開催状況>

- 第1回：令和4年11月9日(水)
- 第2回：令和4年12月7日(水)
- 第3回：令和5年2月1日(水)

# 利便性向上に関する検討部会について

## <目的>

次期LGWANにおける「セキュリティ確保と利便性向上の両立」の重要性に鑑み、次期LGWANにおける利便性向上について利用者視点に立った検討を行うため、「次期LGWANに関する検討会」（以下、「検討会」という。）の下に、「利便性向上に関する検討部会」（以下、「検討部会」という。）を設置。

検討部会の検討結果等は、検討会に報告し、検討会において、セキュリティ確保との両立、コスト等の観点を踏まえ、検討する予定。

## <委員>

須藤 修（座長）	中央大学国際情報学部 教授
工藤 早苗	合同会社m sプランナーズ 代表
後藤 省二	株式会社地域情報化研究所 代表取締役社長
板垣 和幸	秋田県 総務部 税務課 副主幹
橘 昌尚	新潟県 知事政策局 東京事務所 所長代理
村上 暢章	愛媛県 企画振興部デジタル戦略局 スマート行政推進課 主幹
鈴木 充	名古屋市 財政局税務部税務システム推進課 システム企画係長
平田 祐子	中野区 区民部 産業振興課長（兼務）区民部マイナンバーカード活用推進担当課長
齋藤 理栄	深谷市 市民生活部 収税課 主査
野崎 洋平	上里町 総合政策課 主査

## <開催状況>

第1回：令和4年12月28日(水)

第2回：令和5年1月25日(水)

## 次期LGWANの論点等（叩き台）

---

[次期LGWANに求められる要件（自治体のニーズ）]

### ① セキュリティ確保と利便性向上の両立

ア 小規模自治体を含む全ての自治体のセキュリティの確実な確保

イ LGWAN接続系でパブリッククラウド上のサービス（電子契約サービスを含む）の利用を容易に

### ② 一層の安定運用

### ③ LGWAN-ASP等の利用

[ 次期LGWANの論点 ]

### ○ ガバメントクラウド接続への対応（政府と要調整）

ア 自治体とガバメントクラウド上の標準準拠システムとの効率的な接続の仕組み

イ 自治体の基幹業務の円滑な実施に必要な回線帯域を低コストで確保、柔軟な帯域拡張等

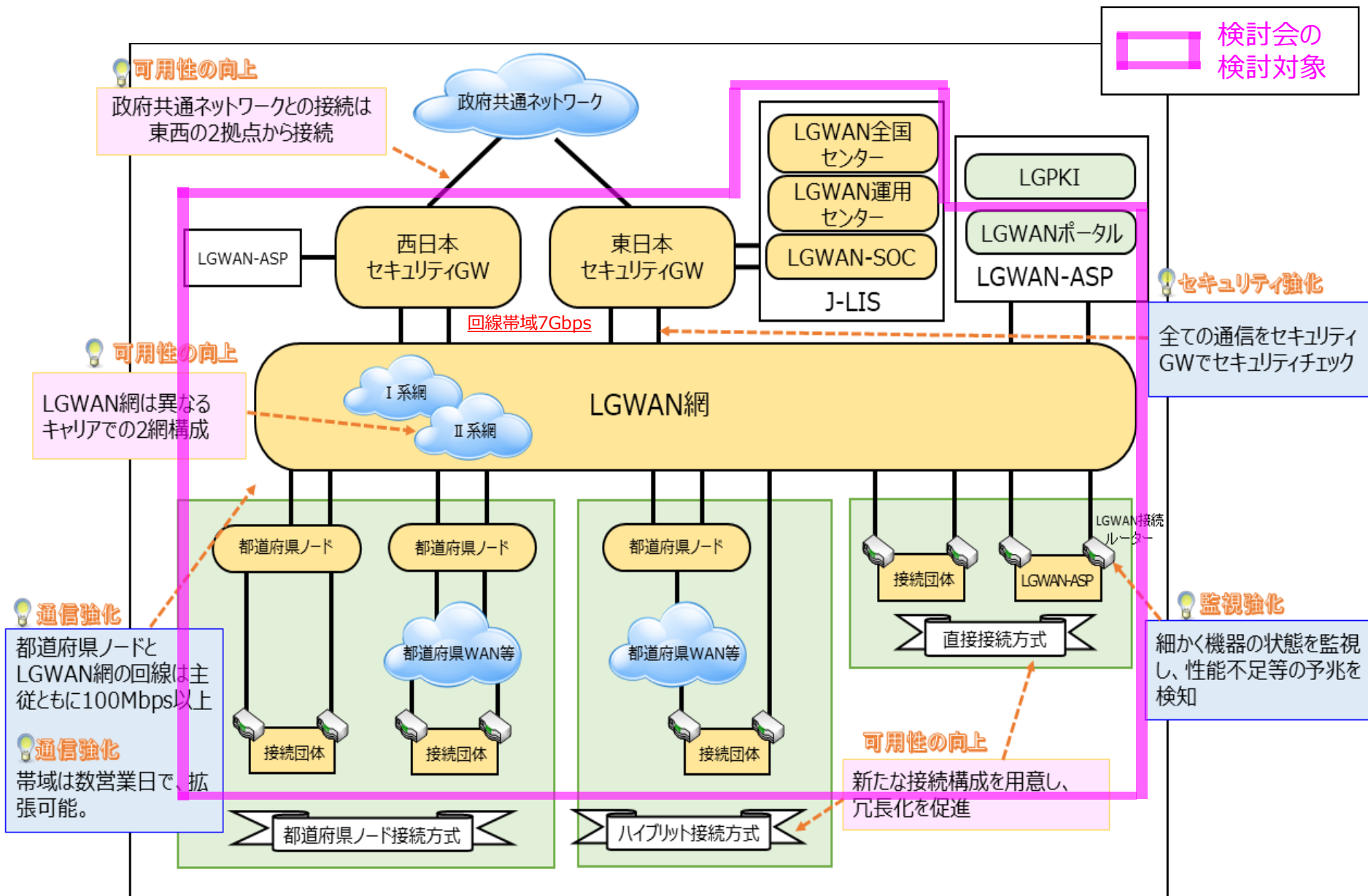
- ・ バックボーン 50Gbps超
- ・ アクセス回線 人口規模に応じて10Mbps～1Gbps

---

## 2 現行LGWANのセキュリティ対策

---

# 現行LGWANのイメージ図





# 現行LGWANにおけるセキュリティ対策

## ①閉域ネットワーク

- 閉域・境界防御によりインターネット等外部からの脅威を防御しています。

## ②ファイアウォールによる防御

- セキュリティゲートウェイにおいてLGWANの各種サーバ群をファイアウォールによって侵入の脅威から防御しています。

## ③通信経路の暗号化による盗聴防止

- LGWANの通信経路を暗号化し、盗聴防止策としています。

## ④侵入検知機能（IDS：Intrusion detection System）

- セキュリティゲートウェイにおいて地方公共団体間、都道府県ノード間での直接通信を制限し、全ての通信を侵入検知機能（IDS）で監視することで、不正アクセスの検知を行っています。

## ⑤SOC（Security Operation Center）の設置

- 専門家による24時間365日のセキュリティ監視を行っています。

## ⑥公開鍵暗号方式（PKI※）による組織認証の実施

- 認証技術による情報の「盗聴」「改ざん」「なりすまし」「事後否認」を防止しています。

※ PKI: Public Key Infrastructure 公開鍵暗号方式の仕組みを利用したインターネット上で安全にやりとりを行うセキュリティのインフラ（基盤）のことです。

# 外部サービスを利用する場合のセキュリティ対策

LGWAN-ASPが外部のサービスの中継する場合、主に以下のセキュリティ対策（要件）を求めている。

## ① IPリーチャビリティの遮断

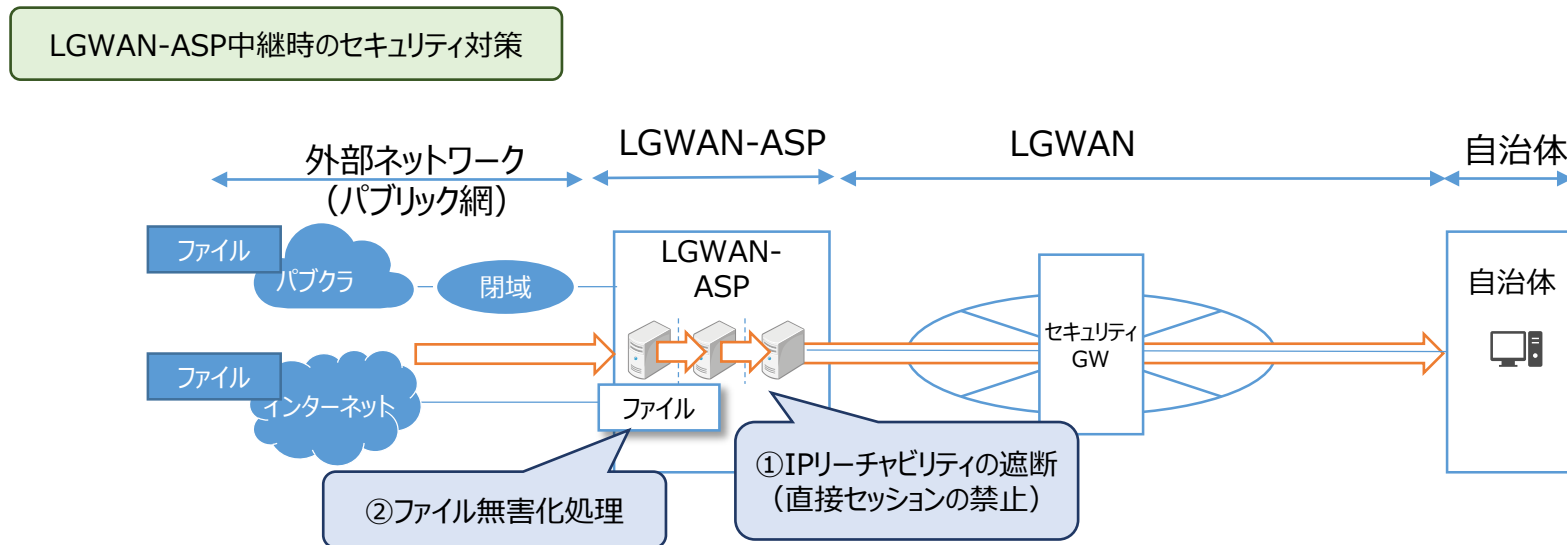
- インターネットなどパブリック網から切り離されており、直接セッションを認めない。

## ② ファイル無害化处理

- インターネットからLGWANへファイルを受け渡す場合には、テキスト化又は画像化して送信すること。
- LGWAN-ASPがクリーンな環境で表組みなどの体裁を整えて（ファイルを再構成し、悪意の可能性があるデータ領域を除去して）送信することは可。

※ LGWAN-ASPが中継・無害化を行っているサービスの例

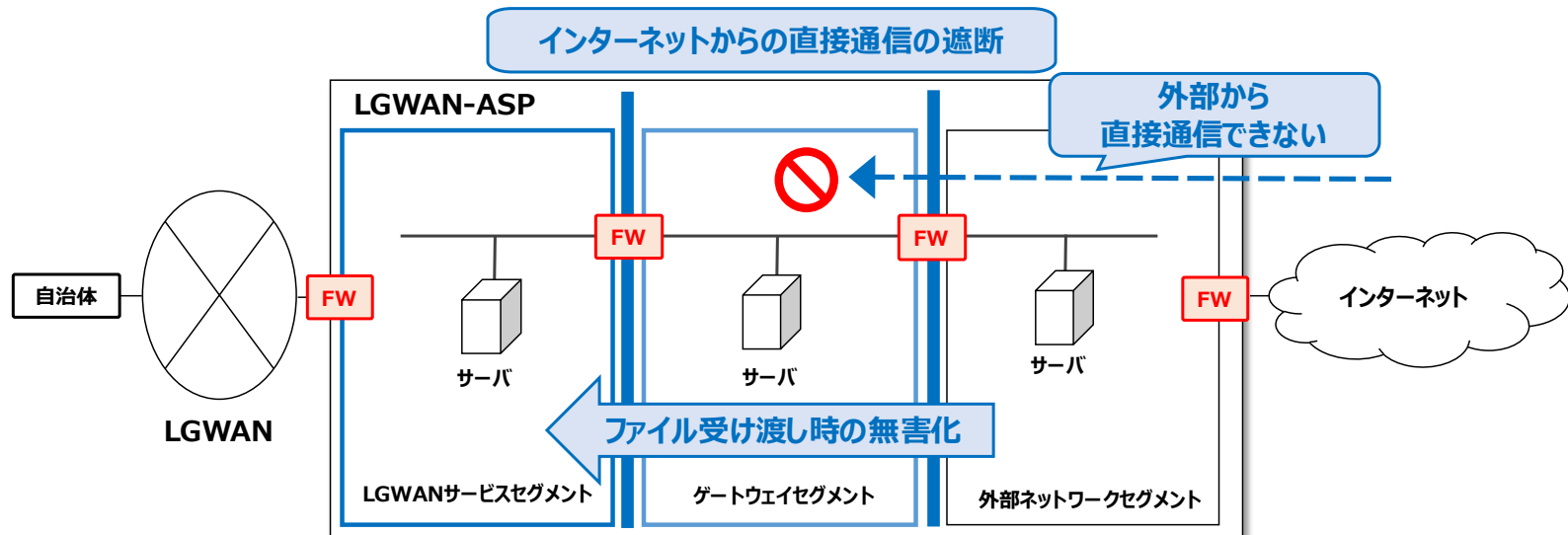
BOX、Kintone、salesforce、Slack、ServiceNow、Cisco AMP 等



# LGWAN及び三層の対策の効果

- 自治体では、「三層の対策」として、庁内ネットワークを番号利用事務系、LGWAN接続系、インターネット接続系に分離・分割
- LGWANは、自治体の庁内LANを相互に接続する行政専用の閉域ネットワーク
- 閉域性確保のため、インターネットと接続する場合には、中継するLGWAN-ASP(※)において、セグメントを分け、インターネットからの直接通信の遮断とともに、インターネット側からファイルを受け渡す際に、無害化(安全なファイルへの再構成)を実施
  - (※) 民間企業等がASP(アプリケーションサービスプロバイダ)として、LGWANを通じて自治体に提供する各種行政事務サービス
- 実際のセキュリティインシデントにおいて、これらの対策の効果が発揮され、セキュリティが確保

## 【LGWAN-ASPでの対策】

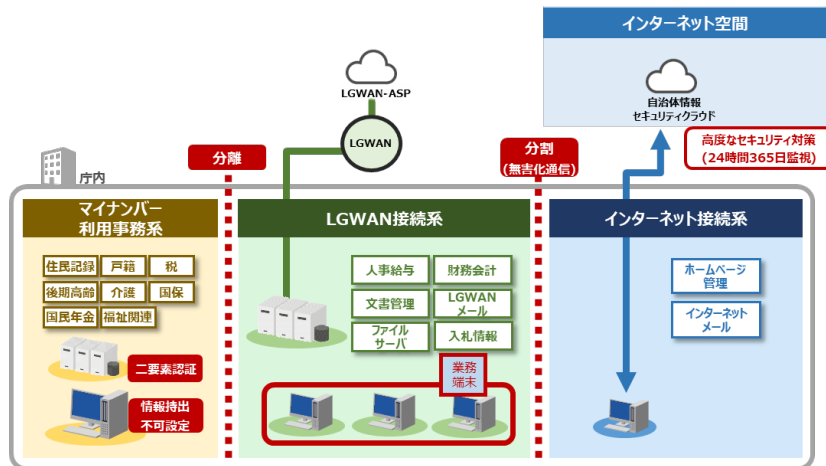


# 自治体ネットワークモデル（三層対策）について

- 自治体の三層対策は、3つの強靱性向上モデル（αモデル、βモデル、β'モデル）が定義されている。
- αモデルが主たる業務端末を「LGWAN接続系」に配置するのに対し、βモデル（β'モデル）は「インターネット接続系」に主たる業務端末を配置する。
- 先進的に検討を進めている団体は、すでにβモデル又はβ'モデルに移行をしている状況。  
→本検討会では主にαモデルを念頭に、LGWANの利便性向上について検討

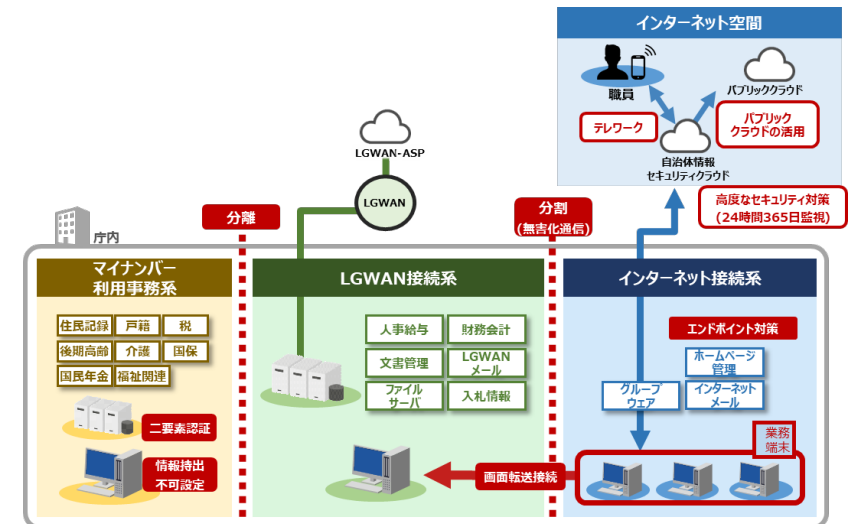
## αモデル

- ・ 主たる業務端末をLGWAN接続系に配置
- ・ LGWAN-ASPサービスや庁内システムを業務に利用



## βモデル（β'モデル）

- ・ 業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末・システムを配置
- ・ インターネット上のサービスを業務に利用



(注) βモデルのうち、重要な情報資産をインターネット接続系に配置する場合は「β'モデル」

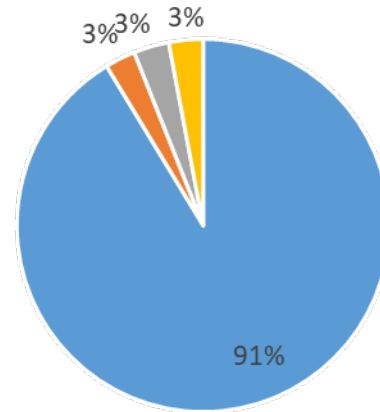
セキュリティリスクを考慮し、EDR等の技術的対策に加え、緊急時即応体制の整備等の組織的・人的対策の確実な実施が条件

# 自治体ネットワークモデル（ $\alpha, \beta, \beta'$ ）の状況

(団体数)

	$\alpha$ モデル	$\beta$ モデル	$\beta'$ モデル	その他
都道府県	36	0	8	3
市町村	1597	47	47	50
合計	1633	47	55	53

総務省調査データ（2022年3月）をLGWAN全国センターにて加工



■  $\alpha$ モデル ■  $\beta$ モデル ■  $\beta'$ モデル ■ その他

---

### 3 次期LGWANの検討状況（セキュリティ関係）

---

# LGWANのセキュリティ及び利便性に関する自治体のニーズ

---

## (第1回／第2回次期LGWAN検討会における主な意見)

- 広帯域で、様々な用途に対応できる複数論理ネットワークを提供すべき。
- 電子契約サービスの利用について、次期LGWANを待たずに検討してもらいたい。
- WEB会議のサービス提供を検討してほしい。
- 回線帯域について、十分に検討してほしい。

# LGWANのセキュリティ及び利便性に関する自治体のニーズ

## (第1回／第2回利便性向上に関する検討部会における主な意見)

- 特に小規模自治体では、自力でのセキュリティ確保や安定運用は困難であり、自治体としては、信頼しているLGWANがなくなると困る。
- 小規模自治体としてはLGWANのような共通基盤で一定のセキュリティを確保する必要がある。
- 手続の起点となる住民や自治体職員がデジタルで完結したと認識したときがデジタル完結であり、自治体業務に関する様々なシステム・ネットワークのシームレスな接続が必要。LGWANは、その役割を果たしており、自治体にとって不可欠。ガバメントクラウドに搭載された業務システムとその他の業務システム、マイナポータルを経由するものとしなないもの等、全体を考え、シームレスな接続によりデジタルで完結したと認知できるようにすべき。
- インターネットを安全に使うという視点で進める必要。
- LGWAN経由で利用可能なローコード開発ツールであっても利用できない機能（例：kintoneのプラグイン）があり、これを利用できるようにしてほしい。
- LGWANの役割を明確にすべき。全てをLGWANで叶えようとするのではなく、インターネットに任せる部分は任せ、それぞれの回線がそれぞれの役割を果たすべき。
- パブリッククラウドサービス上のサービスを利用する場合に、プロキシサービス（LGWAN-ASP）を介すると料金が高くなるので、プロキシサービスを介さずに利用したい。
- LGWAN-ASPは、いろいろなサービスがあるがコストが高い。



## 次期LGWANにおけるセキュリティ対策の考え方（検討案）

### <LGWANのセキュリティについて>

- 現行LGWANでは、閉域・境界防御により自治体のセキュリティを共同で確保。「三層の対策」と相俟って、セキュリティインシデント発生時にセキュリティを確保した実績あり。
- 自治体からは「特に小規模自治体では、自力でのセキュリティ確保や安定運用は困難であり、自治体としては、信頼しているLGWANがなくなると困る。」「小規模自治体にとってはLGWANのような共通基盤で一定のセキュリティを確保する必要。」との意見。

### <自治体におけるゼロトラスト導入について>

- ゼロトラストではすべてのアクセスに対し、セッション単位で認証・認可を行う。アクセス可否の決定に当たっては様々な情報を収集し、それをもとにアクセス要求の信頼性を動的に判断。
- 自治体で導入する場合には、各自治体において、庁内のすべてのユーザ/デバイスや情報資産の棚卸、各々に対する動的なポリシーの定義付けなど、専門的知見を要する煩雑な作業が必要。
- また、常時監視、動的制御が必要であり、すべてのユーザやデバイスの挙動、全情報資産へのアクセスなど、膨大なログ管理が必要。ログ監視・分析、インシデント検知時の対応など、高度なセキュリティ技術を持った専門の組織体制も必要。
- さらに、実装に要する費用が高額。
- 自治体でのゼロトラスト導入は、こうした技術面や費用面の課題があり、自治体の実情を考慮すると、現時点では特に小規模自治体で対応が困難。  
→次期自治体ネットワークについて、ゼロトラスト導入を前提にすることは困難。

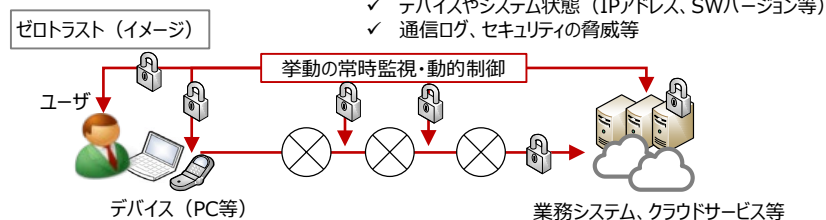
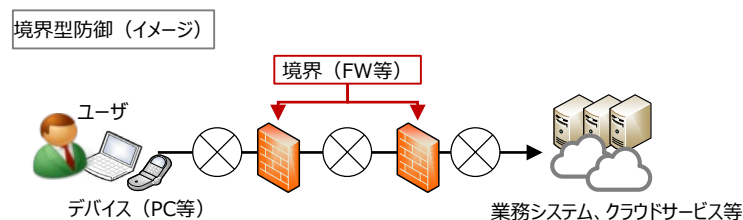


- セキュリティの脅威が高まる中、小規模自治体を含む全自治体のセキュリティを共同で確保するため、**次期LGWANでも閉域・境界防御を継続**。  
※なお、自治体におけるゼロトラスト導入は、自治体のセキュリティ対策における今後の検討課題。

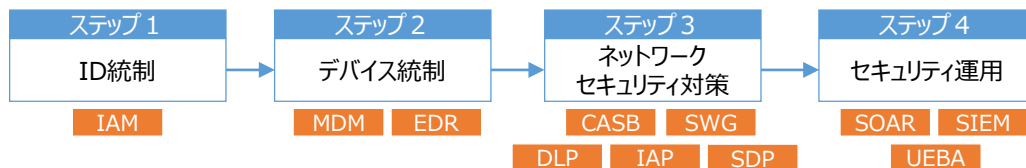
# ゼロトラストセキュリティ

- 米国では政府機関のセキュリティ対策にゼロトラストアーキテクチャの採用を決定。ゼロトラストは世界的な潮流になりつつある。現行LGWANでは現状重大なセキュリティインシデントは発生していないものの、セキュリティの脅威は日々複雑化しており、次期LGWANにおいても**ゼロトラストに留意**した検討が必要。
- ゼロトラストとは、「**内部ネットワークやデバイスからのアクセスを暗黙に信頼せず、常にアクセスの信頼性を検証することで企業の情報資産やIT資産を保護すること**」に焦点をあてたセキュリティの考え方。「信頼がない」アクセスは境界内であっても許可されない点が、境界型防御と異なる。
- **ユーザの挙動やデバイス・システムの状態、通信ログやセキュリティの脅威等の情報を収集**。当該情報をもとに、ユーザからのアクセス要求に関する**ポリシーの適合を厳格にチェック**（PDP）し、ポリシーに従って都度**動的なアクセス制御**（PEP）を行う。

※PDP : Policy Decision Point PEP : Policy Enforcement Point



- なお、現状では、ゼロトラスト全体をカバーできる単一のソリューションは存在しない。例えば、EDRやCASB、SWGなど様々な構成要素を組み合わせて実装する必要。また、それらの構成要素には実装の順序があり、技術面や費用面双方を鑑みたうえで順を追って導入することが重要となる。



■ : ゼロトラストにおける主な構成要素

IAM	IDアクセス管理	IAP	ID認識型プロキシ
MDM	モバイルデバイス管理	SDP	ソフトウェア定義ペリメータ
EDR	エンドポイント検知・対応	SIEM	セキュリティ情報イベント管理
CASB	クラウドアクセスセキュリティ	UEBA	振る舞い解析
SWG	セキュアWEBゲートウェイ	SOAR	セキュリティ運用自動化
DLP	データ漏洩防止		

# ゼロトラスト導入に係る課題

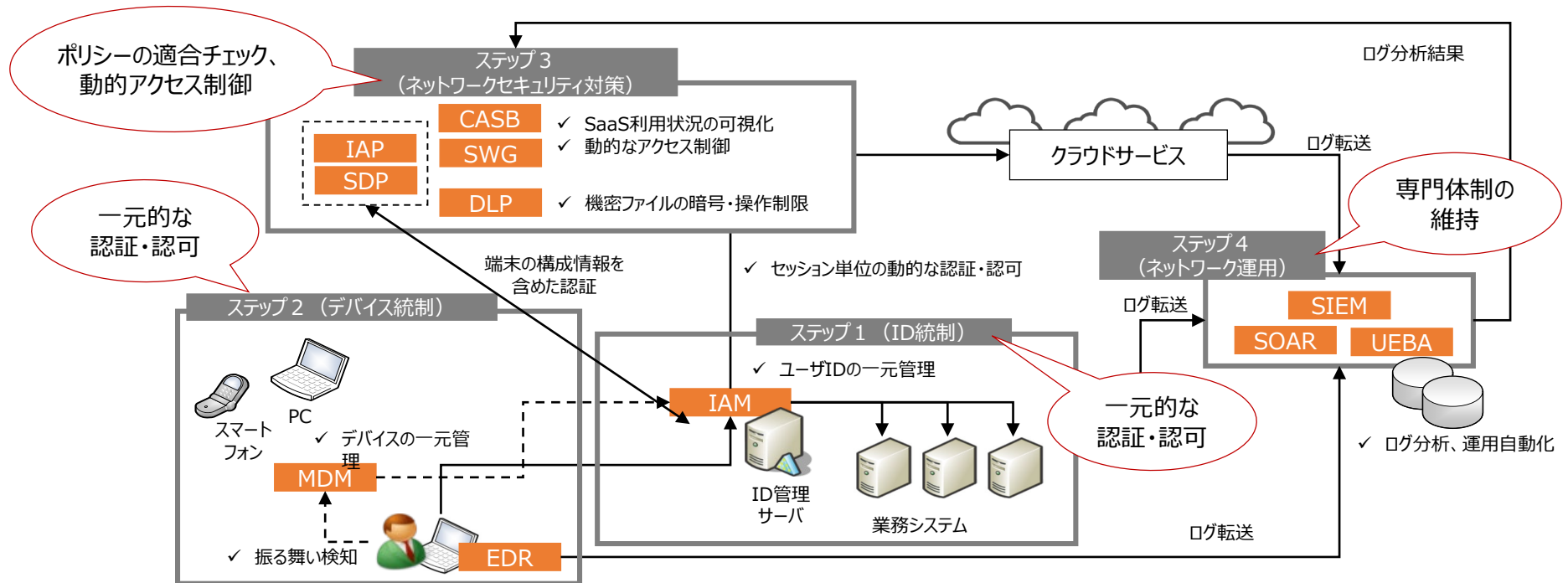
## <技術面の課題>

- 全IT資産の棚卸や動的なポリシー定義など煩雑な作業が発生。専門的な知見も必要。
- 常時監視、動的制御が必要であり、すべてのユーザやデバイスの挙動、全情報資産へのアクセスなどによる膨大なログ管理が必要となることや、ログ監視・分析、インシデント検知時の対応など、高度なセキュリティ技術を持った専門の組織体制が必要。

## <費用面の課題>

- ゼロトラストは様々なソリューションを組み合わせる必要があるため、かつ**非常に高額**であり、特に小規模**自治体**にとって**負担が大きい**。

※代表的なソリューションにおいては年間1,930億円のコストが発生。(ユーザ数:100万人とした場合の参考値)

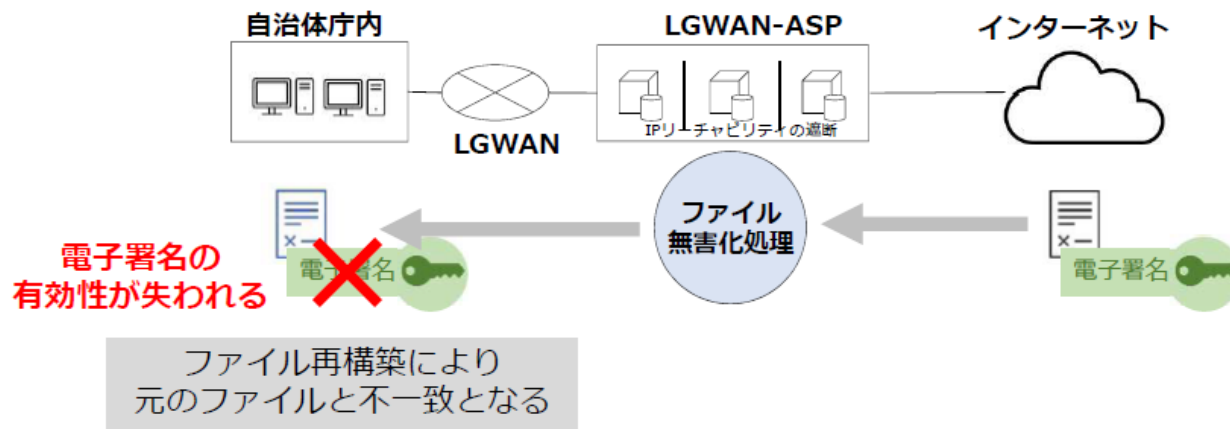


## 電子契約に関する要望

- 電子契約について、LGWANにファイルを取り込む際に無害化処理を行い、原本性が損なわれるとともに電子署名が無効になる。
- 電子契約サービス事業者から、「電子署名付き電子契約文書に対して、LGWAN-ASPでの無害化処理の対象外としていただけないか。」との要望。

### 電子署名付きファイルへの影響

LGWAN-ASPにおける無害化処理により、ファイルは再構成される。この再構成により、オリジナルのファイルとは異なるファイルとなるため、電子署名の有効性が失われる。



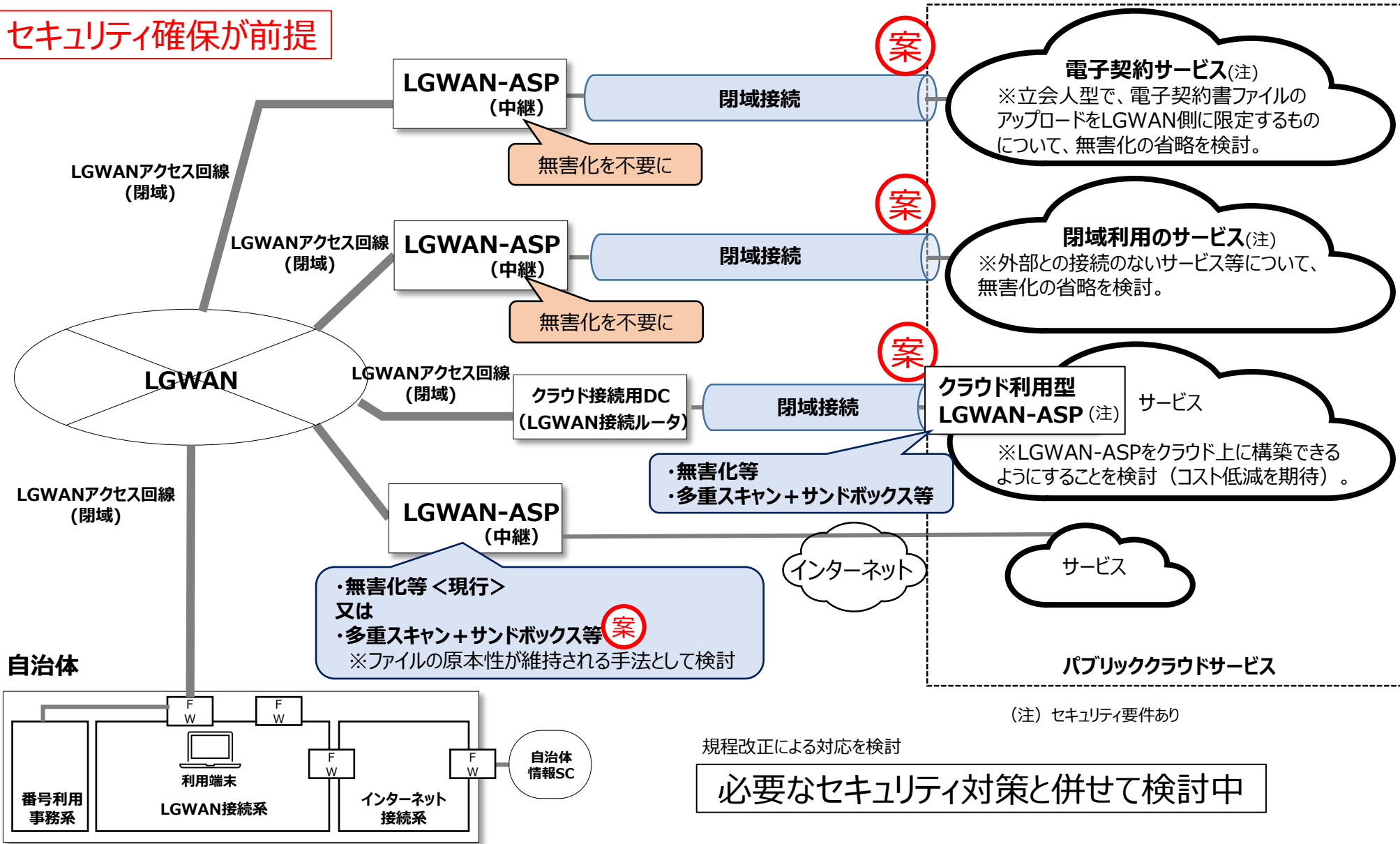
## LGWANの利便性向上について（検討案）

---

- LGWANの利便性向上に関する自治体のニーズは、パブリッククラウド上のサービスを使いやすくしてほしいというものが主。
- LGWANは、小規模自治体を含む全自治体のセキュリティを共同で確保するもの。セキュリティ確保を前提とし、その枠の中で利便性向上策を検討。
- 次スライドの検討案について、必要なセキュリティ対策と併せて検討中。これらは、次期LGWANを待たず、規程改正により、可能なものから順次対応することを検討する。

# LGWANの利便性向上（クラウド上のサービスの利用拡大）（検討案）

セキュリティ確保が前提



※併せて、LGWAN-ASPの参入促進策(ホスティングサービスとの連携等)を検討。

## 第3回次期LGWAN検討会における主な意見

- 次期LGWANでは、ゼロトラストの方向には行かないことになると思うが、次々期では避けられず、ゼロトラスト導入について、いつから検討を開始するのか、自治体への説明が必要。
- ゼロトラストは、0か1かではなく、段階的な導入も含め検討してもらいたい。  
→ゼロトラストは、自治体のセキュリティ対策に関わるものであり、総務省やデジタル庁と連携して検討していく。  
(事務局)
- 電子契約サービスの利用について、次期LGWANを待たずに検討してもらいたい。
- 示された利便性向上策は、画期的なことであり、有益と考える。一方で、セキュリティレベルが下がるのではないかと懸念がある。対応策のセキュリティ基準をどう定めるかが論点。また、定期的にセキュリティ対策をチェックする仕組みも必要。



### <座長によるまとめ>

- セキュリティ確保については、本検討会としては、次期LGWANにおいても閉域・境界防御を維持する方向で整理したい。
- LGWANの利便性向上については、対応策について、セキュリティ面やコスト面を更に詰める必要がある。次期LGWANを待たずに規程改正で対応できるとのことなので、J-LISでどんどん検討を進めてもらいたい。
- ゼロトラストの段階的な導入についても、引き続き検討してもらいたい。