資料１

前回の検討会と
地方公共団体への意見照会を踏まえた対応

総 務 省

令和６年３月13日

総務省自治行政局

デジタル基盤推進室

地方公共団体への意見照会の実施概要

✓　都道府県・市区町村に対し、２段階に分けて意見照会を実施することで、各検討項目ごとに確認期間を確保できるように配慮。

政府統一基準改定に伴う変更	
期間	令和６年１月13日　～　令和６年１月22日　※NISCとの合同説明会開催後に実施。
提示資料	政府統一基準（令和５年度版）の改定に係るセキュリティポリシーガイドラインの文書案

α'モデルのローカルブレイクアウトに関するセキュリティ要件についての意見照会	
期間	令和６年２月２日　～　令和６年２月９日
提示資料	第１１回検討会資料１（一部抜粋）

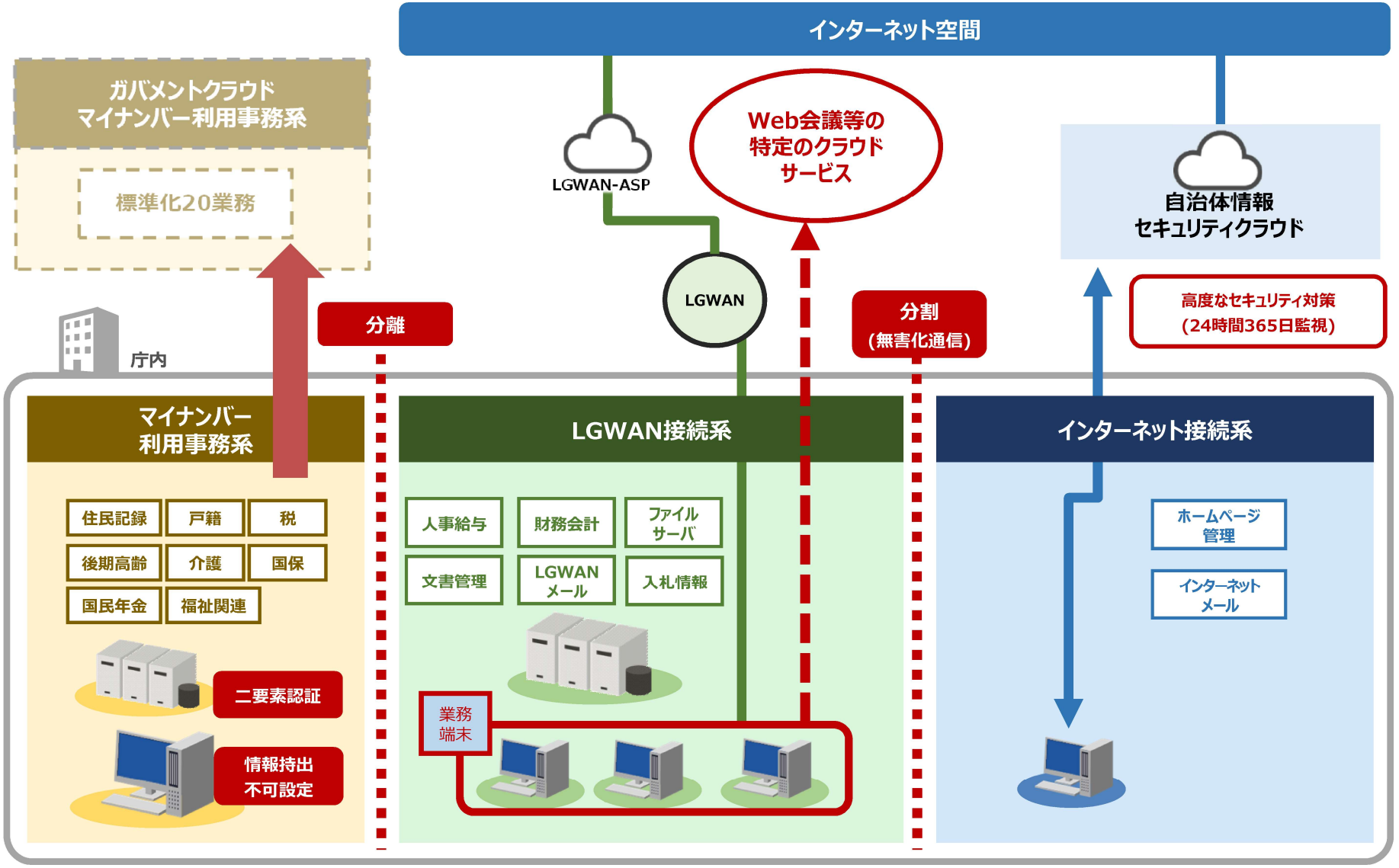
	政府統一基準	α'モデル
都道府県	14団体	10団体
市区町村	36団体	45団体
計	50団体	55団体

１．LGWAN接続系のローカルブレイクアウト（α’モデル）の検討

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～

ガイドライン改定の方向性

- 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。
- α'モデルのリスク評価を行い、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。



リスクアセスメント概要（前回提示）

✓ 第三者認証制度による接続先の安全性担保、インターネット回線の利用を視野に入れてリスク評価を実施することとしてはいかがか。
✓ パブリッククラウドのサービス範囲に応じ、それぞれのケースを想定したセキュリティ対策を検討してはいかがか。

リスク評価の観点

✓ SaaS型サービスセキュリティは、ユーザ（自治体）側で完全に制御することが難しいため（※）、利用するパブリッククラウドの安全性を担保する方策が必要となる。
→ **ISMAPに登録されているサービス等、第三者認証により安全性が担保された接続先にのみ接続先を認める**方向性。

※例えば、ゲートウェイ機器をSaaSのデータセンターに自由に設置できないことなどが考えられる。

✓ 接続に用いる回線について、パブリッククラウドのサービス特性、帯域確保（特にWeb会議で利用する場合）および導入維持コストの観点を踏まえ、安全性を確保する必要がある。
→ **インターネット回線の利用を視野に入れた接続構成**にて検討。

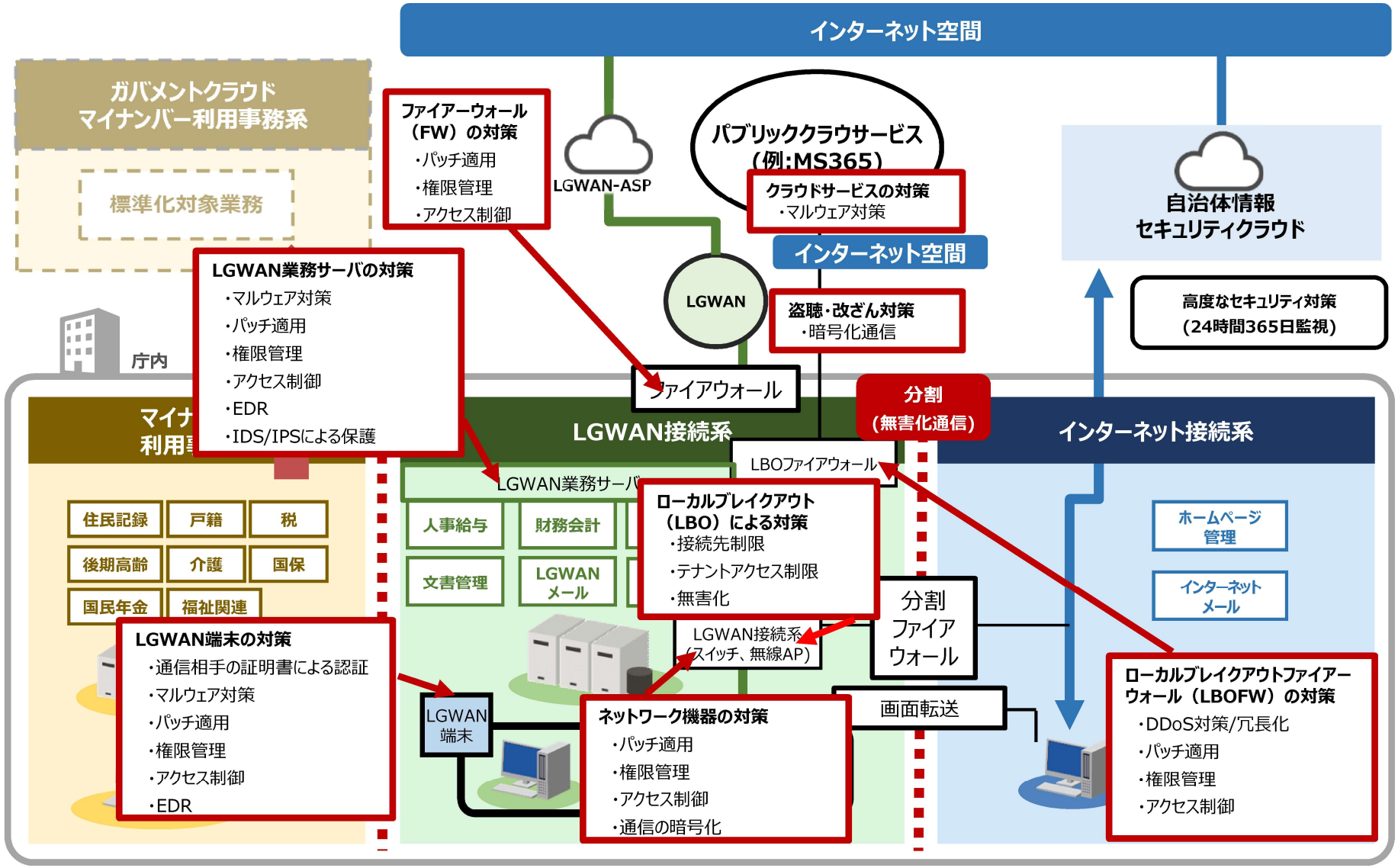
✓ 利用するパブリッククラウドのサービス範囲に応じ、セキュリティリスクが異なる。
→ 認証のみ実施する場合と、外部とファイル送受信が発生する場合ではセキュリティリスクが異なるため、コストの観点から、**それぞれのケースを想定したセキュリティ対策を検討**。

認証等	コミュニケーションツールの利用	外部とファイル送受信が発生
＜例＞ ■ 認証・認可 ■ ウイルス定義ファイル配信	＜例＞ ■ 認証・認可 ■ ウイルス定義ファイル配信 ■ Web会議、チャット	＜例＞ ■ 認証・認可 ■ Web会議、チャット ■ ファイル送受信等

小 → セキュリティリスク → 大

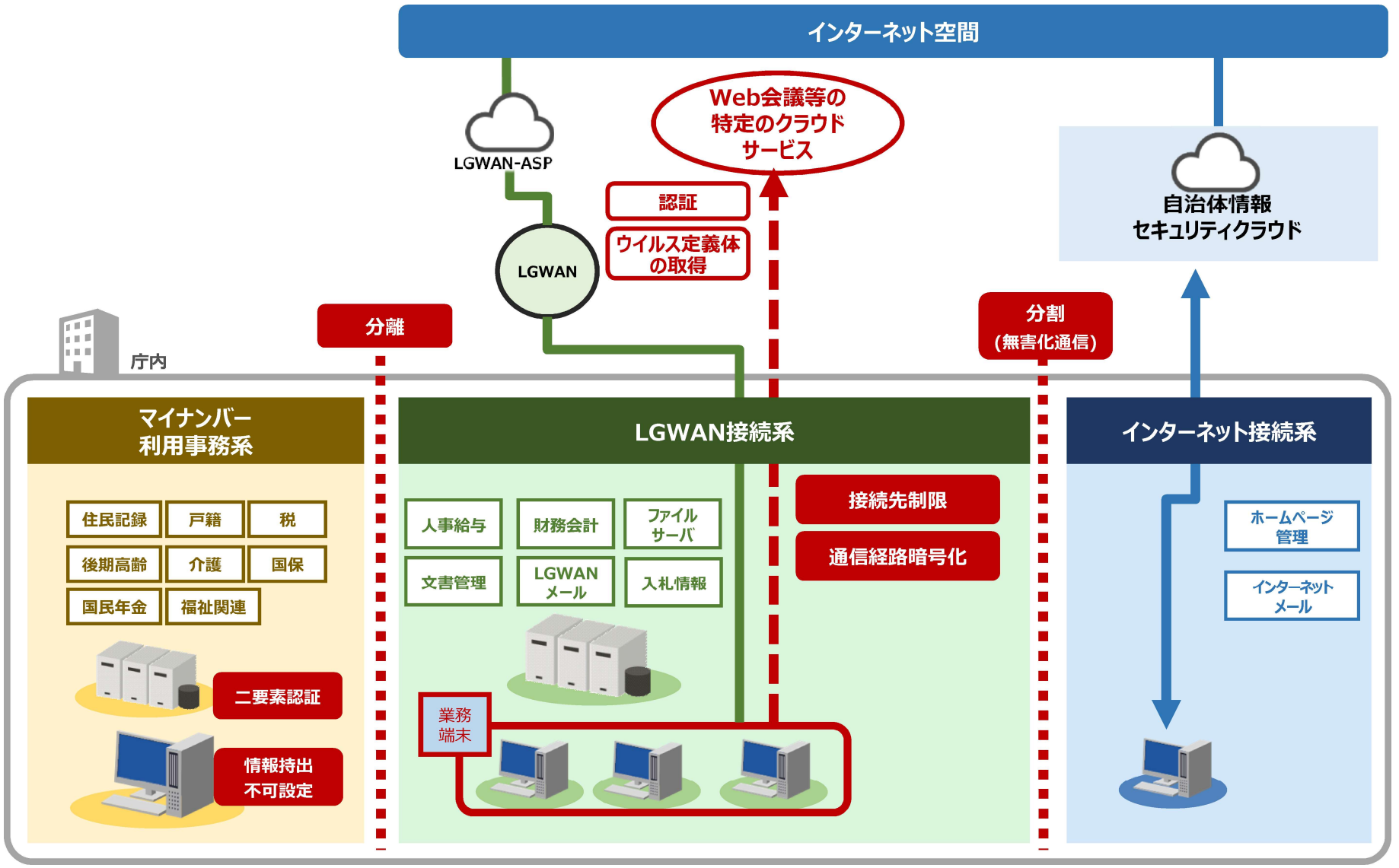
α'モデルの技術的対策

✓ 最もリスクの大きい、外部とファイル送受信を行う場合に必要な対策を以下に示す。



α'モデルの技術的対策（認証・ウイルス定義体の取得のみの場合）のイメージ図

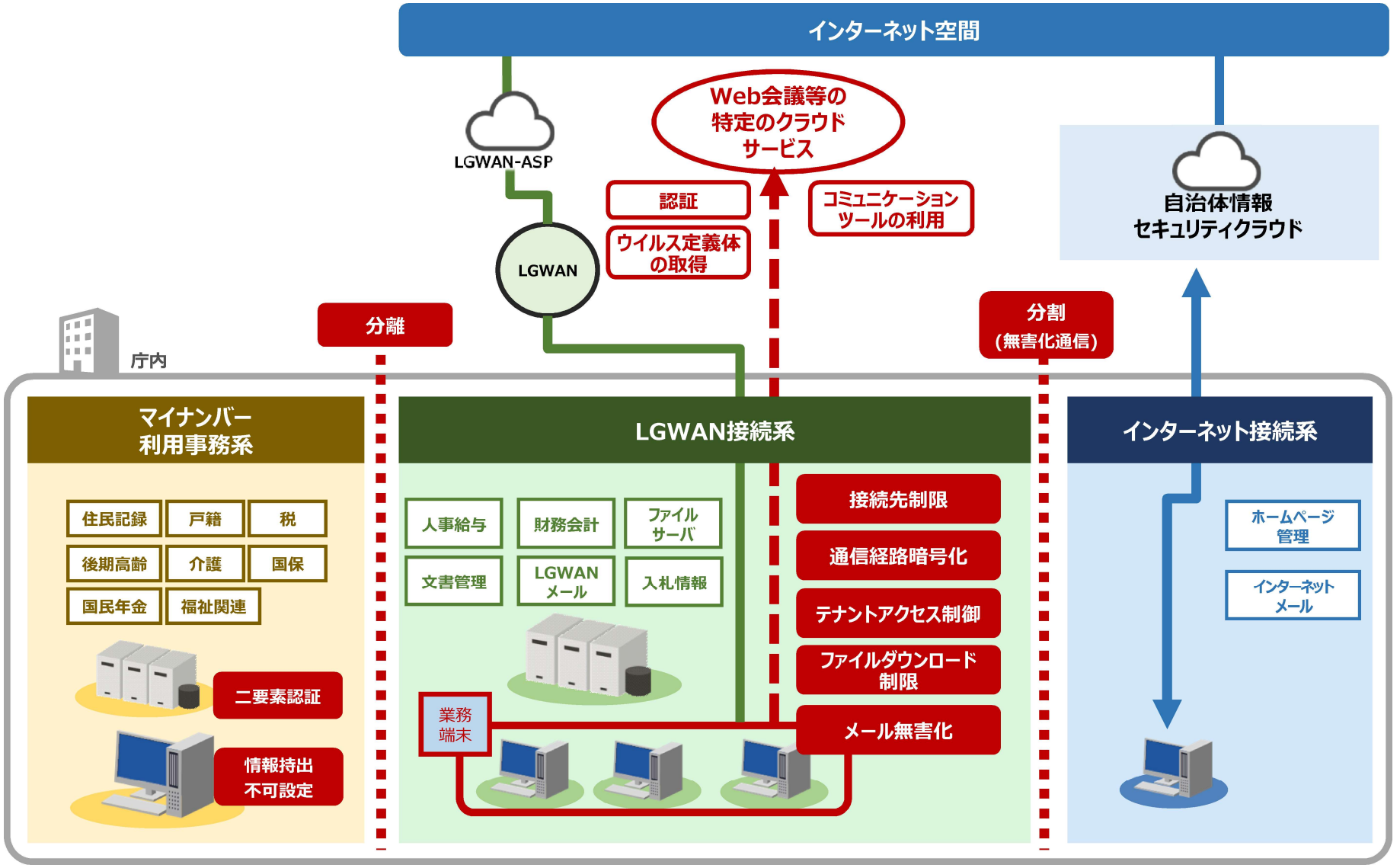
✓ 認証・ウイルス定義体の取得のみの場合におけるセキュリティ対策のネットワーク構成イメージは以下の通り。



※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。

α'モデルの技術的対策（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）のイメージ図

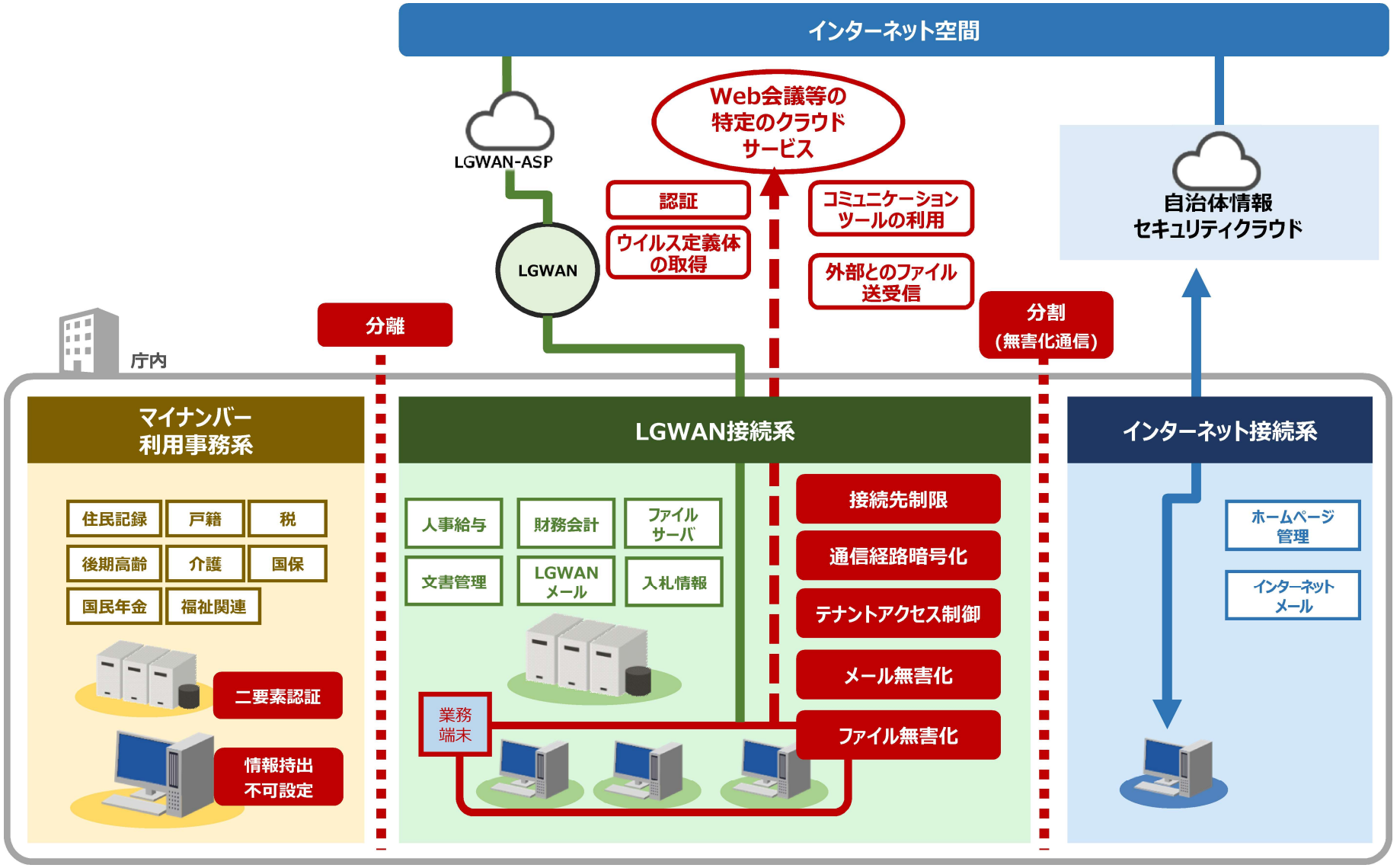
✓ コミュニケーションツールを利用するが、ファイルを内部に取り込まない場合におけるセキュリティ対策のネットワーク構成イメージは以下の通り。



※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。

α'モデルの技術的対策（外部とファイル送受信を行う場合）のイメージ図

✓ 外部とファイル送受信を行う場合におけるセキュリティ対策のネットワーク構成イメージは以下の通り。



※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。

前回いただいたご意見 ①

- ✓ **地方公共団体は、自ら責任を持ってセキュリティを確保すべきであることを明示すべきであり、その旨を強調すべき**との意見があった。
- ✓ **クラウドサービスの設定確認は、サービスのアップデートの際にも行う必要がある**旨を明記すべきとの意見があった。

検討項目	視点	発言要旨
LGWAN接続系のローカルブレイクアウト（α′モデル）	責任の所在	• **インシデントが発生した際、自治体の責任になるということを改めて留意する必要がある**。難しい話であればあるほど、最終的な判断が自治体側ではできず、自治体側が業者に頼んだ時点、クラウドに頼んだ時点、あるいは自治体ガイドラインやISMAPに載っている時点で手離れしてしまう可能性がある。

ガイドライン改定の方向性

- ➢ **情報セキュリティの確保は自治体の責任となることを改めて明記**する。

検討項目	視点	発言要旨
LGWAN接続系のローカルブレイクアウト（α′モデル）	品質の確保	• 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、定期的な確認を行うことが必要と書いてあるが、定期的だけでは足りない場合として、アップデートに伴う仕様変更で齟齬が生じたことがあるため、その点も明記をしてほしい。

ガイドライン改定の方向性

- ➢ クラウドサービスのアップデートに伴う仕様変更があった際も、設定の確認が必要なことを記載する。
- ➢ クラウドサービスのアップデートによる仕様変更に伴う事故事例を記載する。

前回いただいたご意見 ②

✓ α'の外部監査に関連して、自治体が外部監査を委託する際の参考となるように、**外部監査を実施する組織や監査メンバーの資格を詳細に記載すべきではないかという意見があった**。

検討項目	視点	発言要旨
LGWAN接続系のローカルブレイクアウト（α'モデル）	外部監査	• 外部監査の実施について、適正に外部監査を実施するため、「地方公共団体における情報セキュリティ監査に関するガイドライン」の「監査人の実績等」に具体的な資格を明記すべきと思う。特に監査メンバーについてはより具体的なものが望ましい。

ガイドライン改定の方向性

➢ 外部監査を実施する監査人として、以下の資格が考えられうるため、「地方公共団体における情報セキュリティ監査に関するガイドライン」に参考として記載する。

【独立行政法人 情報処理推進機構】
（https://www.ipa.go.jp/index.html）

・システム監査技術者

・情報処理安全確保支援士

【特定非営利活動法人　日本セキュリティ監査協会】
（https://www.jasa.jp/）

・公認情報セキュリティ監査人

【ISACA】
（https://engage.isaca.org/japanesechapters/aboutus）

・公認情報システム監査人

・公認情報セキュリティマネジャー

【一般財団法人 日本要員認証協会】（https://www.jrca-jsa.or.jp/）

・ISMS審査員

【特定非営利活動法人 日本システム監査人協会】
（https://www.saaj.or.jp/）

・公認システム監査人

【国際情報システムセキュリティ認証コンソーシアム】
（https://japan.isc2.org/）

・公認情報システムセキュリティ専門家

前回いただいたご意見 ③

✓ セキュリティ対策の記載についても意見があり、自治体が混乱しないよう、書き方に留意する。

検討項目	視点	発言要旨
LGWAN接続系のローカルブレイクアウト（α'モデル）	対策の明確化	• βモデルβ´モデルのように、α'モデルでも、どのような対策を確実に実施しなければならないのかを明確にする必要がある。
	マルウェア対策ソフト	• 「パターンマッチング方式、不審な動作を行うことが含まれていることを検出するヒューリスティック方式を行う」と書かれているが、「及び」なのか「または」なのかを明確にすることで、混乱を避けられるのではないかと思う。 • マルウェア対策ソフトは、検知方式というよりは他の様々な要因で性能が決まるところがあり、どの製品であれば問題ないのかという判断がとても難しい製品である。現状、Windows標準でマルウェア対策ができてしまうということもあり、書き方には注意をした方が良い。 • α'モデルにおいて、マルウェア対策ソフトが必須となっているが、提供会社によって製品によって良し悪しがあると思う。一定のセキュリティ認証をパスしたソフトを使うということを義務付けることなのか、そこまでは求めないのか、IPAセキュリティリスク分析ガイドでの記載はどのようになっているのか、国際的なサイバーセキュリティの水準からするとどうなのか。
	パッチ適用	• 自治体では、パソコンはパッチ適用しているが、ネットワーク機器はパッチ未適用という部分が散見される。自治体に分かりやすく周知していただくためにも、具体的な製品名を出すわけにはいかないかもしれないが、運用の中で組み込んでいく旨も出してほしい。

ガイドライン改定の方向性

- α'モデル３パターンのそれぞれについて、必須のセキュリティ対策を表形式で記載する。
- マルウェア対策ソフトの概要の記載を「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。」に修正する。

地方公共団体への意見照会結果：主な意見と対応①（α‘モデル関係）

【意見】

✓　ISMAPに登録されているクラウドサービスに限定した場合、サービス選定の幅が狭まり、本来業務効率化・最適化に必要とされるサービスが利用できないことが想定されるため、選定基準の条件緩和をしてほしい。

✓　ISMAPに登録されているサービスや第三者認証等により安全性が担保された接続先にのみ接続を認める」とすべきではないか。

【対応】

✓　LGWAN接続系から直接クラウドサービスに接続する構成であることを踏まえ、クラウドサービスの安全性を確保するため、ISMAP登録サービスであることを条件とする。

＜改定案＞

第３編 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。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。

セキュリティ関連サービスについて

- ✓ α'モデルの利用条件として「接続先のクラウドサービスの証明書による認証」をあげているが、これと同様に、**セキュリティ関連サービスと連携するセキュリティ対策ソフトも、そのサービス提供元が本物であることを証明書により認証**されている場合があり、この**真正性確保を条件に、ISMAPクラウドサービスリストに登録されていないサービスについても利用可**とする。
- ✓ また、α'モデルによる利用が想定される、行政文書や行政文書に相当するやりとりが保存されるファイル管理やメール機能を有するクラウドサービスとは異なり、**セキュリティ関連サービスはウィルス定義ファイル、URLドメインリスト等の更新情報の配信ツールであるため、ISMAP登録サービスの利用の制限から除くものとする**。

＜改定案＞

第３編 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。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（＝許可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。
（略）

地方公共団体への意見照会結果：主な意見と対応②　（α'モデル関係）

【意見】

✓ 「LGWAN接続系にインターネット接続系からファイルを取り込む。」とあるが、ローカルブレイクアウトした場合であっても組織外からのデータについては、LGWAN接続系への直接のファイルの取込は認めず、インターネット接続系から無害化の上、ダウンロードすることを前提としていると考えてよろしいか。

【対応】

✓ 「LGWAN接続系にインターネットからファイルを取り込む。」の誤記のため、修正する。

＜改定案＞

第３編 第2章3.情報システム全体の強靭性の向上
(２)LGWAN接続系
（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。
（略）
（イ）α'モデル：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（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）
本モデルにおいては、以下の図表に記載された対策を講じなければならない。

対策区分	セキュリティ対策	概要
		（略）
技術的対策	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。
		（略）

図表28 α'モデル（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）における必須のセキュリティ対策について

（ウ）α'モデル：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（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）
本モデルにおいては、以下の図表に記載された対策を講じなければならない。

対策区分	セキュリティ対策	概要
		（略）
技術的対策	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。
		（略）

図表30 α'モデル（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）における必須のセキュリティ対策について

地方公共団体への意見照会結果：主な意見と対応③ （α'モデル関係）

【意見】

✓ 「通信相手の証明書による認証」とは、LGWAN端末を証明書で認証するのか、LGWAN端末が、LBO接続先のサーバ等を証明書で認証するのかが不明確なので、明記して頂きたい。

【対応】

✓ 「接続先のクラウドサービス」に修正する。

＜改定案＞

第３編 第2章3.情報システム全体の強靭性の向上

（２）LGWAN接続系

（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。

（略）

（ア）α'モデル：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（認証・ウイルス定義体の取得のみの場合）

本モデルにおいては、以下の図表に記載された対策を講じなければならない。

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。

（略）

図表26 α'モデル（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）における必須のセキュリティ対策について

（略）

（イ）α'モデル：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（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）

本モデルにおいては、以下の図表に記載された対策を講じなければならない。

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。

（略）

図表28 α'モデル（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）における必須のセキュリティ対策について

（略）

（ウ）α'モデル：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（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）

本モデルにおいては、以下の図表に記載された対策を講じなければならない。

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。

（略）

図表30 α'モデル（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）における必須のセキュリティ対策について

地方公共団体への意見照会結果：主な意見と対応④　（α'モデル関係）

【意見】

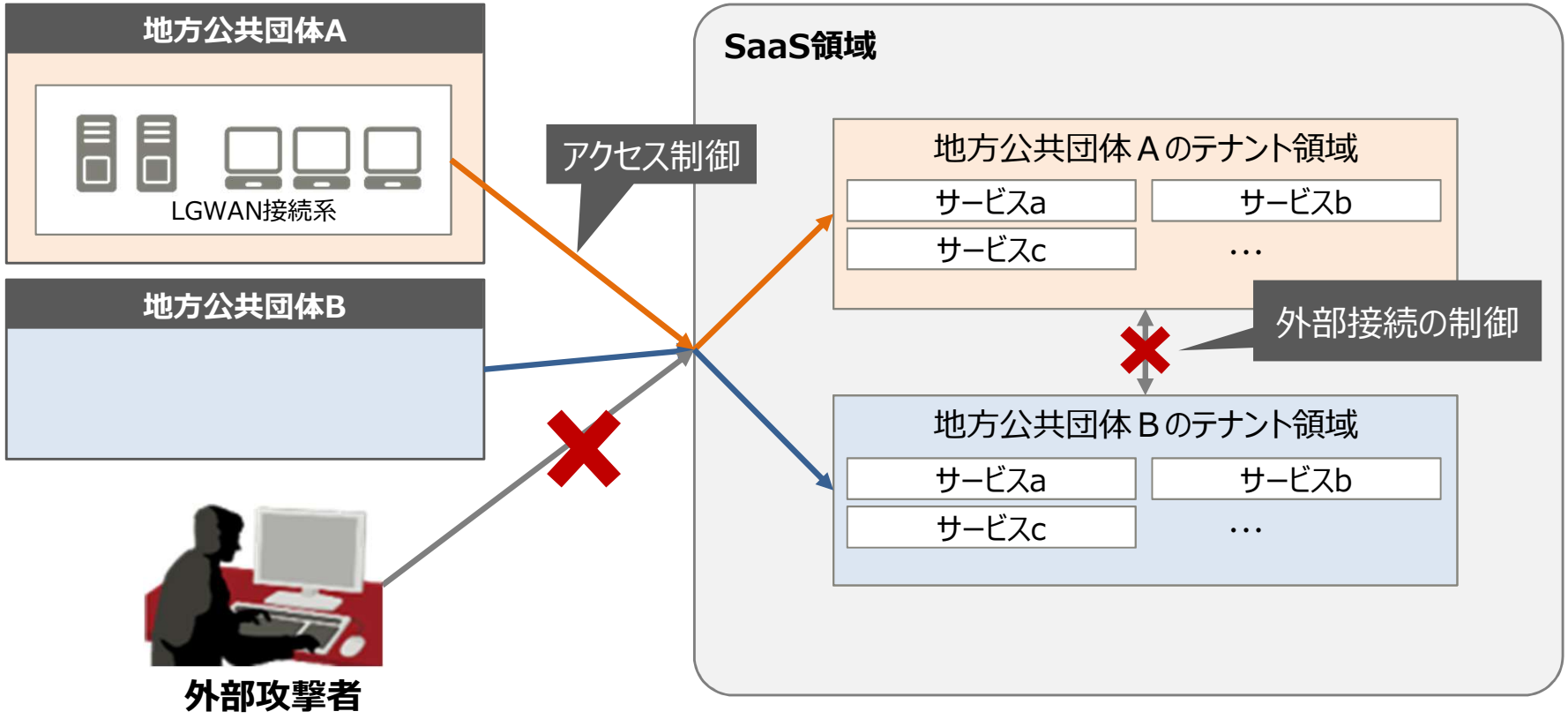
✓　自団体のファイル管理やグループウェアの専用テナントを利用し、かつ外部から専用テナントへのアクセスを制限している場合は、そのテナント内には内部からアップロードしたファイルのみ保管されることになるため、無害化等の制限の対象外としていただきたい。

【対応】

✓　今後、関係事業者からテナントの閉域性を担保する考え方について聴取した上、対応を検討する。

クラウドサービス(SaaS)におけるテナントの考え方

- テナントとは、クラウドサービスを利用する団体に割り当てられた専用の管理領域であり、基本的に、アクセス制御を設定することにより、許可された団体／団体の職員のみが利用可能な領域を指す。



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。
（略）
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。

ISMAPの記載に伴いアクセス制限の記載を修正

自治体が自ら責任をもって臨むことを記載（２箇所）

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）。

サービスアップデート時の対応

ISMAPの登録されているクラウドサービスであることが前提であることを明記

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ため、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
（略）

事故事例を記載

事故事例を記載

ガイドライン改定案（見え消し）③

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
③
（前ページからの続き）

（略）

さらに、クラウドサービスへのアクセス状況やアプリケーションの利用状況についてログを取得し、状態監視を行うなど適切なセキュリティ対策を講じるとともに、セキュリティインシデント発生時の対応手順をあらかじめ用意する必要がある（第４編　情報セキュリティインシデントの報告　参照）。この点を、第２編、第３編の8.3.及び8.4.の外部サービス(クラウドサービス)の利用で規定している各事項と合わせて、留意すること。
α’モデルを採用する場合は、従来モデル（αモデル）と比較してインターネットからのリスクが増加し、より高度なセキュリティ対策の確実な実施が必要になることから、その実施について事前に外部による確認を実施し、その確認の報告書を地方公共団体情報システム機構に提出することとする。また、その後も定期的に外部監査を実施することとし、その監査報告書を地方公共団体情報システム機構に提出することとする。なお、外部による事前確認や外部監査を行う者については、監査の対象となる情報資産に直接関与しない者であることが望ましい。

第2章
9.評価・見直し
9.1.監査
（略）
(２)監査を行う者の要件
（略）
（注２）監査業務を事業者に請け負わせる場合には、経済産業省が定める「情報セキュリティサービス基準」及び当該基準を満たすと認められた企業を記載した「情報セキュリティサービス基準適合サービスリスト」（うちセキュリティ監査サービスに係る部分）を活用することも考えられる。
参考：経済産業省「情報セキュリティサービス審査登録制度」（https://www.meti.go.jp/policy/netsecurity/shinsatouroku/touroku.html）

外部監査の記載は本レベルとし、監査資格については経済産業省の情報セキュリティサービスの適合性などを踏まえ、参考情報を9項に追記

ガイドライン改定案（見え消し）④

改定案：対策基準（解説）

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（ア）～（ウ）のとおり、利用範囲の異なる３つのケースを想定し、それぞれにセキュリティ対策を記載する。ただし、利用するクラウドサービスは多様であり、すべてのケースを想定することは困難であるため、α’モデルを採用する場合は、地方公共団体ごとのサービス利用範囲を踏まえて、個別に検討する必要がある。今回示す３つのケースは昨今の動向を踏まえた、最も基本的なケースであり、セキュリティ対策は、最終的には地方公共団体の責任でもって実施するとともに、記載しているセキュリティ対策以外の対策の導入も考えられることに留意すること。

クラウドサービスを利用した際のセキュリティリスクを低減するための対応として、（ア）～（ウ）に示されたもの以外の技術的対策の導入する場合は、定量的な分析によりリスクが低減されることを確認すること。

（ア）α’モデル：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（認証・ウイルス定義体の取得のみの場合）

本モデルは以下のクラウドサービス利用の構成である。

- 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

本モデルにおいては、以下の図表に記載された対策を講じなければならない。

自治体意見：通信相手の明確化

必須のセキュリティ対策を表形式にて記載

マルウェア対策ソフトの概要を修正

ネットワーク機器のパッチ適用

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

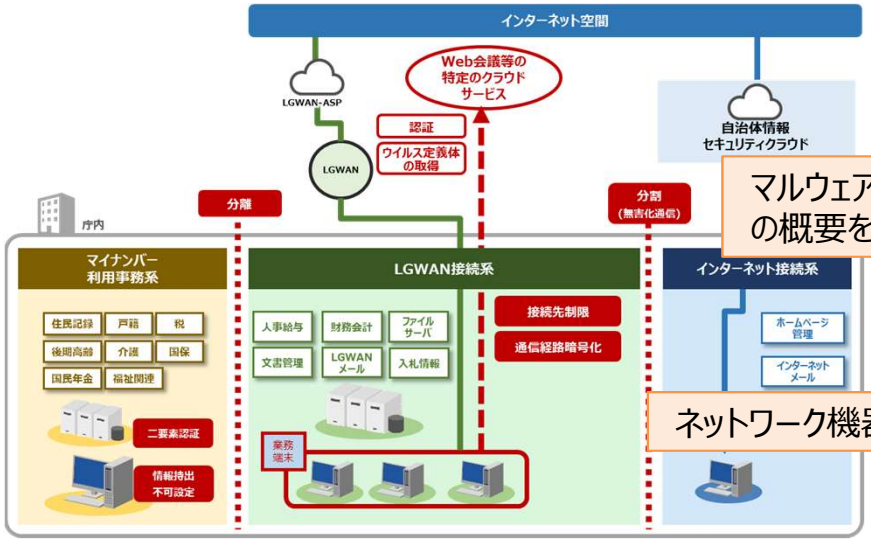
図表26　α’モデル（認証・ウイルス定義体の取得のみの場合）における必須のセキュリティ対策について

α’モデル（認証・ウイルス定義体の取得のみの場合）については、以下の対策も有効である。

・システムに対するDDoS攻撃発生時の継続稼働を保証するため、あるいは障害状態からの早期回復を実現するための、構成要素の冗長化

ガイドライン改定案（見え消し）⑤

改定案：対策基準（解説）



図表26 α’モデル（認証・ウイルス定義体の取得のみの場合）イメージ図
※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。

（イ）α’モデル：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（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）

本モデルは以下のクラウドサービス利用の構成である。

- 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

本モデルにおいては、以下の図表に記載された対策を講じなければならない。

自治体意見：通信相手の明確化

必須のセキュリティ対策を表形式にて記載

マルウェア対策ソフトの概要を修正

ネットワーク機器のパッチ適用

自治体意見：誤字修正

利用サービスを明記

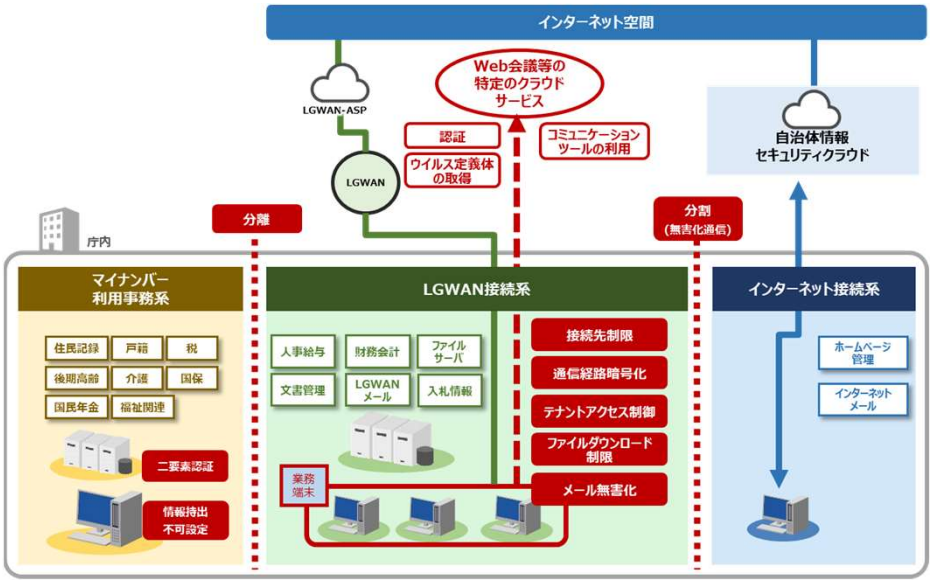
対策区分	セキュリティ対策	概要
技術的対策	クラウドサービスからファイルダウンロード制限	・クラウドサービス上から業務端末へのファイルダウンロードを制限する。
	接続先のクラウドサービスの証明書による認証	・接続先のクラウドサービスが本物であるか否か、正当性を確認する。
	マルウェア対策ソフト	・パターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。LGWAN接続系に配置する端末、業務サーバで対応が必要となる。
	パッチ適用	・脆弱性を修正するパッチを速やかに適用し、脆弱性を解消するLGWAN接続系に配置する端末、業務サーバ、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	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

図表28 α’モデル（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）における必須のセキュリティ対策について

ガイドライン改定案（見え消し）⑥

改定案：対策基準（解説）

α’モデル（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）については、以下の対策も有効である。
・システムに対するDDoS攻撃発生時の継続稼働を保証するため、あるいは障害状態からの早期回復を実現するための、構成要素の冗長化
・クラウドサービス上でのマルウェア対策
・未知の不正プログラムへの対策（エンドポイント対策）



図表28 α’モデル（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）イメージ図
※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。

（ウ）α’モデル：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（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）

本モデルは以下のクラウドサービス利用の構成である。

- 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

本モデルにおいては、以下の図表に記載された対策を講じなければならない。

ガイドライン改定案（見え消し）⑦

改定案：対策基準（解説）

自治体意見：通信相手の明確化

必須のセキュリティ対策を表形式にて記載

マルウェア対策ソフトの概要を修正

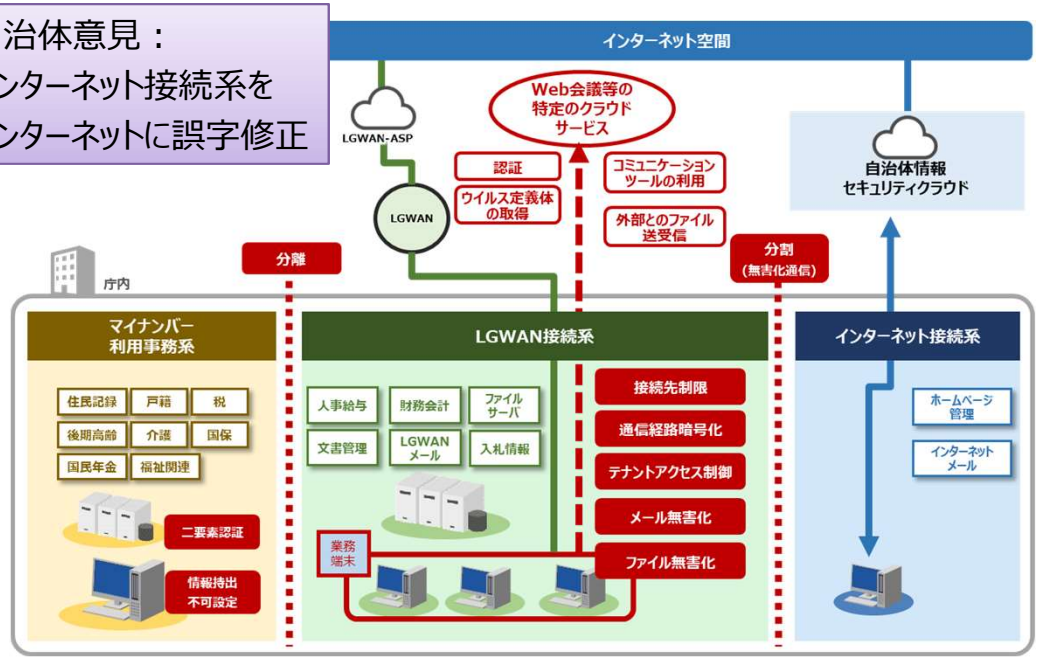
対策区分	セキュリティ対策	概要
技術的対策	接続先のクラウドサービスの証明書による認証	・接続先のクラウドサービスが本物であるか否か、正当性を確認する。
	マルウェア対策ソフト	・パターンマッチング方式や、不審な動作を行うコードが含まれていることを検出する振る舞い検知などにより、不正プログラム対策を行う。LGWAN接続系に配置する端末、業務サーバで対応が必要となる。
	パッチ適用	・脆弱性を修正するパッチを速やかに適用し、脆弱性を解消するLGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、接続系のスイッチ・無線APで対応が必要となる。
	接続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

図表30　α’モデル（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）における必須のセキュリティ対策について

α’モデル（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）については、以下の対策も有効である。
・システムに対するDDoS攻撃発生時の継続稼働を保証するため、あるいは障害状態からの早期回復を実現するための、構成要素の冗長化
・クラウドサービス上でのマルウェア対策
・未知の不正プログラムへの対策（エンドポイント対策）

ネットワーク機器のパッチ適用

自治体意見：
インターネット接続系を
インターネットに誤字修正



図表30 α’モデル（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）イメージ図
※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。

２．令和５年度政府統一基準改定に関する対応

地方公共団体への意見照会結果：主な意見と対応①（政府統一基準改定関係）

【意見】

✓ ISMAP同様、参考とすべき認証の１つと位置付ける「ISMAP-LIU」について、「対象とする範囲が限定的なことに加え」とあるが、「対象とする範囲が限定的なこと」についての説明をガイドライン等に補足してほしい。

【対応】

✓ 「政府情報システムのためのセキュリティ評価制度（ISMAP）」（令和４年11月１日NISC、デジタル庁、総務省、経済産業省）の記載を参照し、「SMAP-LIUは、『ISMAPが対象とするクラウドサービス』のうち、セキュリティ上のリスクの小さな業務・情報の処理に用いるSaaSサービスに対する仕組みであり、また情報システムの調達においては、業務・情報の影響度に応じたセキュリティを確保すべきとの考え方から、影響度が低いと評価される業務、情報に用いられるSaaSを対象とする制度として策定されている」旨を追記する。

＜現行ガイドライン＞

第３編 第２章 ８.業務委託と外部サービスの利用 8.2.外部サービスの利用（機密性２以上の情報を取り扱う場合）

【解説】
（２）外部サービスの選定
⑦（略）
参考：国際規格
「ISO/IEC27017（安全なクラウドサービス利用のための分野ISMS規格）」

＜改定案＞

第３編 第２章 ８.業務委託と外部サービス（クラウドサービス）の利用 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）

【解説】
（３）クラウドサービスの選定
⑦（略）
参考：国際規格
「ISO/IEC27017（安全なクラウドサービス利用のための分野別ISMS規格）」
参考：ISMAP及びISMAP-LIU
「ISMAP 政府情報システムのためのセキュリティ評価制度」
（https://www.ismap.go.jp/csm）
参考：ISMAPとISMAP-LIUの違い
内閣サイバーセキュリティセンター（NISC）
「政府情報システムのためのセキュリティ評価制度（ISMAP）（令和４年11月１日NISC、デジタル庁、総務省、経済産業省）」
（https://www.nisc.go.jp/policy/group/general/ismap.html）
※〔ISMAPとISMAP-LIUの比較〕参照
ISMAP-LIUは、「ISMAPが対象とするクラウドサービス」のうち、セキュリティ上のリスクの小さな業務・情報の処理に用いるSaaSサービスに対する仕組みであり、また情報システムの調達においては、業務・情報の影響度に応じたセキュリティを確保すべきとの考え方から、影響度が低いと評価される業務、情報に用いられるSaaSを対象とする制度として策定されている。

（参考）クラウドサービスの位置づけについて

ガイドライン改定において、「外部サービス（クラウドサービス）」とした背景は以下の通りとなる。
- ✓ NISC統一基準では「外部サービス」が再整理され「クラウドサービス」としている。
- ✓ 全体的な「クラウドサービス」への変更は自治体内で混乱する可能性があるとの委員からの意見から、章タイトルの「外部サービス」は残しつつ、「（クラウドサービス）」を併記している。

なお、自治体からの意見として、「外部サービス」から「クラウドサービス」への変更に関する意図についての質問があったため、以下に位置づけを再掲する。

第10回検討会資料再掲

政府統一基準群の主な改定内容

- ✓ 「業務委託」から「情報システムに関する業務委託」を切り出し、必要な対策を上乗せで規定する。
- ✓ 従来の「外部サービス」を「クラウドサービス」、「機関等向けに情報システムの一部の機能を提供するサービス※」に分離し、ISMAP原則利用の考え方に基づいた対策へと改定する。 ※業務委託に分類される。

＜改定前の分類＞

4.1 業務委託

4.2 外部サービス

4.2.1 要機密情報を取り扱う場合

4.2.2 要機密情報を取り扱わない場合

●外部サービスの例

クラウドサービス、Web会議サービス、検索サービス、翻訳サービス、地図サービス、 SNS

ホスティングサービス、インターネット回線接続サービス

＜改定後の分類＞

4.1.1 業務委託 ※全ての「業務委託」に適用

4.1.2 情報システムに関する業務委託 ※「情報システムに関する業務委託」について上乗せで適用

(1) 共通的対策
(2) 構築の場合の対策
(3) 運用・保守の場合の対策
(4)機関等向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

●情報システムに関する業務委託の例
情報システムの開発及び構築業務、アプリケーション・コンテンツの開発業務、情報システムの運用業務

4.2 クラウドサービス ※ISMAP原則利用

4.2.1、4.2.2 要機密情報を取り扱う場合

4.2.3 要機密情報を取り扱わない場合

●**クラウドサービスの例**
仮想サーバ、ストレージ、ハイパーバイザー等提供サービス（IaaS）、
データベースや開発フレームワーク等のミドルウェア等提供サービ（PaaS）、
Web会議サービス、ソーシャルメディア、検索サービス、翻訳サービス、地図サービス

地方公共団体への意見照会結果：主な意見と対応②（政府統一基準改定関係）

【意見】

✓ 「第３編　第２章　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」の解説「（注６）また、内部通信回７７線に接続した機器等に対して」の「７７」は誤記ではないか。

【対応】

✓ 誤記となるため、「内部通信回線に接続した」に修正する。

＜現行ガイドライン＞

第３編 第２章 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

【解説】

（８）ネットワークの接続制御、経路制御等

ネットワーク上では、フィルタリング、ルーティング、侵入検知システム等が機能しているが、これらの機能を十分活用するため、ハードウェア及びソフトウェアの設定を適正に行うよう注意する必要がある。

（略）

さらに、仮想ネットワークを構築する場合には、仮想ネットワークと物理ネットワークとの対応関係、仮想ネットワークの運用設定方針及び設定承認方針並びに庁内設備をクラウドサービスに移行する場合の注意事項等について確認し、適正な対策を講じる必要がある。

＜改定案 ＞

第３編 第２章 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

【解説】

（８）ネットワークの接続制御、経路制御等

ネットワーク上では、フィルタリング、ルーティング、侵入検知システム等が機能しているが、これらの機能を十分活用するため、ハードウェア及びソフトウェアの設定を適正に行うよう注意する必要がある。

（略）

さらに、仮想ネットワークを構築する場合には、仮想ネットワークと物理ネットワークとの対応関係、仮想ネットワークの運用設定方針及び設定承認方針並びに庁内設備をクラウドサービスに移行する場合の注意事項等について確認し、適正な対策を講じる必要がある。

（注６）インターネット等の外部ネットワークである通信回線から内部通信回線に接続された機器等に対して行われるリモートメンテナンスについては、職員等が業務アプリケーション等のみへアクセスできるリモートアクセスとは違い、インターネット等の外部ネットワークから内部通信回線へのアクセスが前提となることを想定している。

（略）

また、内部通信回線に接続した機器等に対してインターネット等の外部ネットワークから直接接続して行うリモート監視についても同様の情報セキュリティを確保するための措置を行うことが重要である。