資料１

各検討項目の改定方針

総 務 省

令和６年２月１日

総務省自治行政局

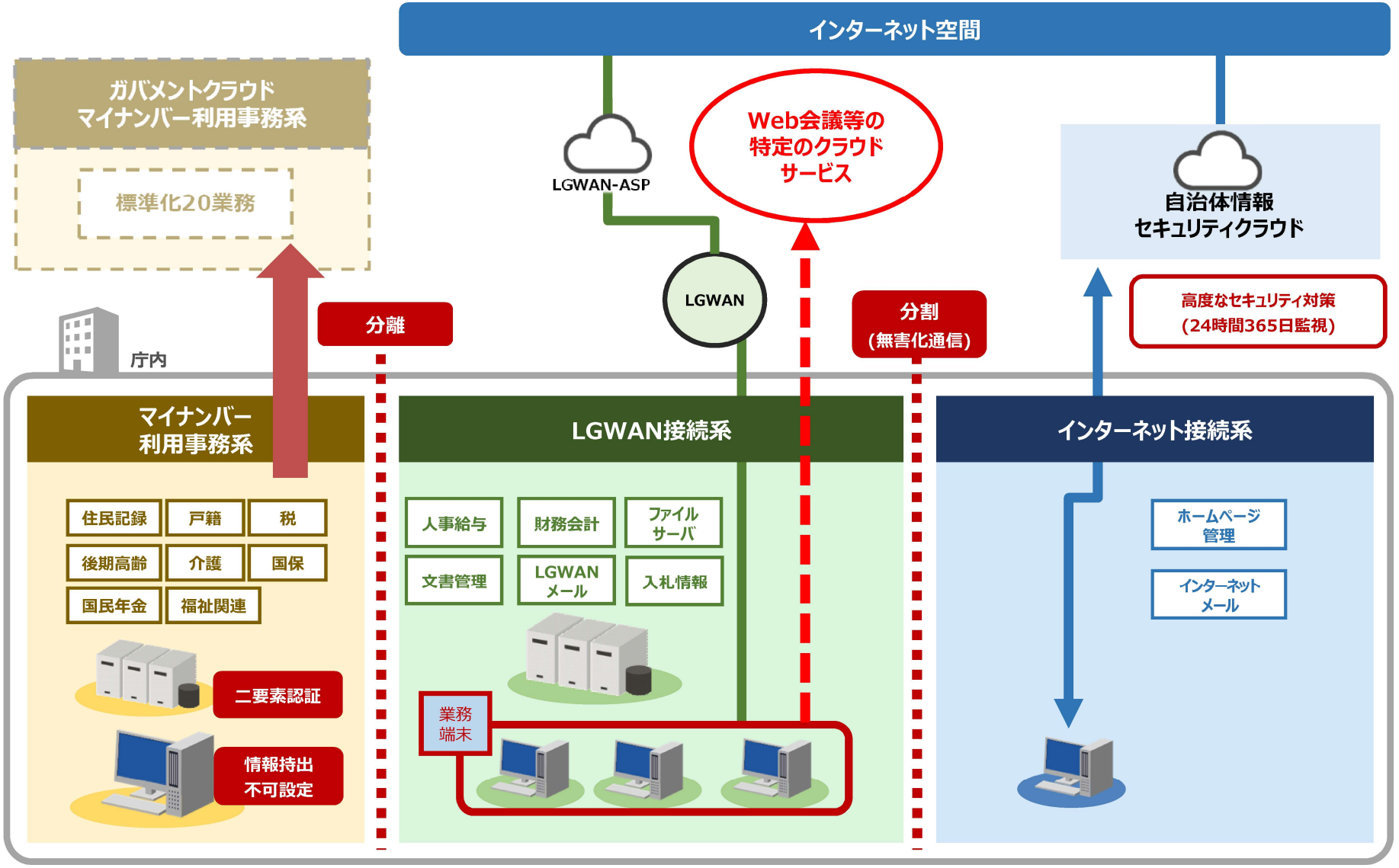
デジタル基盤推進室

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**。

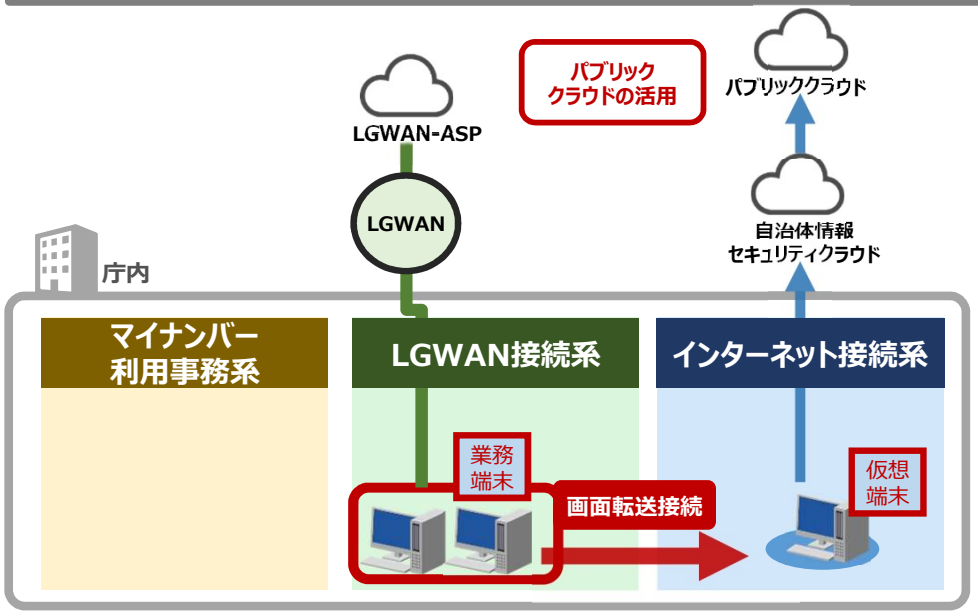
認証等	コミュニケーションツールの利用	外部とファイル送受信が発生
＜例＞ ■ 認証・認可 ■ ウイルス定義ファイル配信	＜例＞ ■ 認証・認可 ■ ウイルス定義ファイル配信 ■ Web会議、チャット	＜例＞ ■ 認証・認可 ■ Web会議、チャット ■ ファイル送受信等

小 → セキュリティリスク → 大

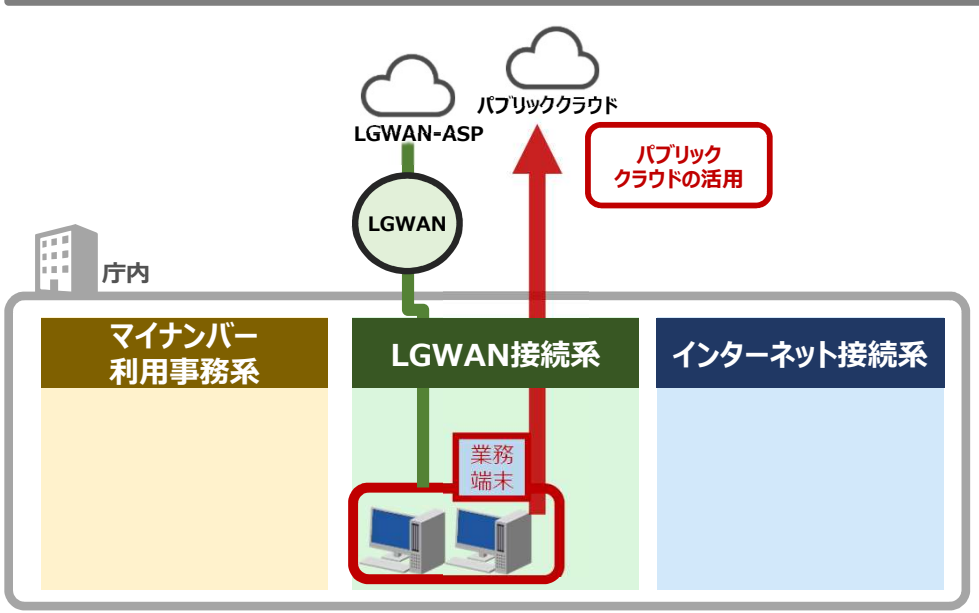
リスクアセスメント概要（前回提示）

✓現行ガイドラインで認められている都道府県セキュリティクラウド経由のローカルブレイクアウトを比較対象とし、LGWAN接続系からのローカルブレイクアウトのセキュリティリスクを分析する。

都道府県セキュリティクラウド経由のローカルブレイクアウト



LGWAN接続系からのローカルブレイクアウト



現行ガイドラインにおけるローカルブレイクアウトの記載

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

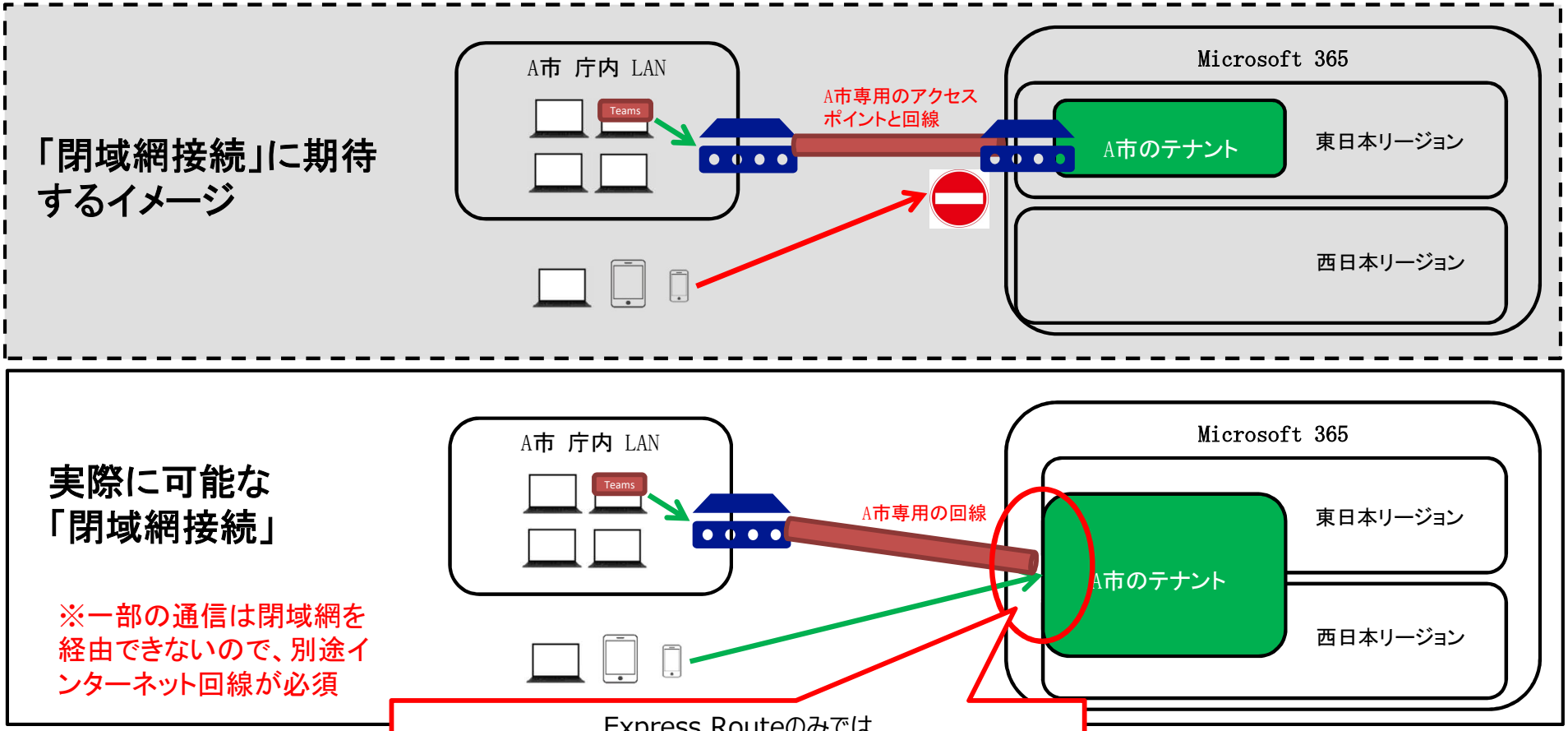
（３）インターネット接続系

自治体情報セキュリティクラウド構成団体からのクラウドサービスの利用増加等に伴うトラフィック増加に対応するため、ローカルブレイクアウトを行う場合には、その実施可否について、セキュリティ上のリスクを勘案し、都道府県、市区町村で協議の上、慎重に判断する必要がある。ローカルブレイクアウトを行う場合は、原則として、都道府県側の設定により、実施することとする。その場合、当該ルートを狙った攻撃等のリスクの増加を十分に理解した上で、例えば、信頼できる事業者が提供する特定のクラウドサービスのみローカルブレイクアウトを認める、構成団体と１対１で紐づく通信元IP・ポート番号と通信先IP・ポート番号をもとに通信をポリシーベースルーティングで振り分ける、ログイン状況やアプリケーションの利用状況の監視を行うなどといった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。

（参考）Microsoft 365への接続回線について（日本マイクロソフト社より）

✓ 自治体からのニーズが大きいパブリッククラウドサービスが、**インターネット回線での接続を前提**としている。

- Microsoft 365（M365）は、世界中どこからでも快適にサービスを利用することと、データセンターレベルの障害でもサービスを継続して提供（東日本リージョン、西日本リージョンでデータを冗長化）することを可能とするため、**インターネット回線での接続を前提**としている。
- M365 を利用する際に、ExpressRoute と呼ばれる専用線サービスを利用することは可能だが、**当該専用線サービス は、あくまでもパフォーマンス向上を目的とした帯域を保証する環境で費用を要する**上に、**外部からの接続を遮断するものではない**。
- さらに、**認証などの一部の通信は、閉域網を経由できない**ため、別途インターネット回線を自治体側で用意する必要がある、



資産ベースのリスク分析について

- ✓ 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'モデルにおけるクラウドサービス、接続回線の利用条件

＜α'モデルの基本的なコンセプト＞
✓ 許可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）
✓ セキュリティリスクの観点として、クラウドサービスの利用形態およびサービス内容を踏まえた安全性確保が重要である。
✓ 外部とのファイル交換、メールの送受信等が発生する場合は、無害化等必要な対策を実施する。

(1) 利用するクラウドサービスの選定

・**ISMAPに登録されているクラウドサービスに限定する**
※ただし、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。

(2) クラウドサービスの利用条件

・**各団体専用領域（テナント）があり、当該団体職員のみが該当テナントにアクセスを許可する制御を行う。**
・クラウドサービスで利用するアプリケーションは以下を想定する。
  - Web会議システム(Micosoft社の例：Teams)
  - ファイル管理システム(Micosoft社の例：SharePoint、OneDrive)
  - メール(Micosoft社の例：Exchange)　※団体外部の組織からのメール受信することを想定している
・団体外部の組織から招待されたWeb会議は、インターネット接続系の業務端末で利用することを想定している。仮に当該Web会議をLGWAN接続系からブレイクアウトし、LGWAN接続系の業務端末から利用する場合は、ファイルの流出、流入に対する制御の設定等対策を実施する必要がある。特にファイルの流入が想定される場合は、ファイル無害化等の対策を講じる必要がある。

(3) 接続回線

・自治体からのニーズが大きいパブリッククラウドサービスが、インターネット回線での接続を前提としていることから、**インターネット回線が利用されることを前提とする。**

脅威に対するセキュリティ対策の考え方

脅威（攻撃手法）	考えられる主な対策 （太字は現在実施されていない対策または強化する対策）
外部（インターネット経由）不正アクセス ーインターネット経由で機器に侵入し、攻撃を実行する。	・権限管理 ・アクセス制御 ・パッチ適用
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 ー攻撃対象機器にマルウェア（不正プログラム）を感染・動作させる。	・通信相手の証明書による認証 ・マルウェア対策ソフト ・パッチ適用 **・LBOテナントアクセス制御** **・接続先制限** ・メール無害化/ファイル無害化 ・EDR
高負荷攻撃 ーインターネット経由のDDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。 または容量以上の通信トラフィックを発生させ、輻輳状態とする。	・DDoS対策 ・冗長化
プロセス不正実行 ー侵入したマルウェアが攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	・権限管理 ・アクセス制御 ・EDR
侵入した攻撃者、マルウェアの内部拡散 ー侵入したマルウェアが内部ネットワークの機器を探索し、残存する脆弱性やファイル共有等を利用し、通信可能な機器、システムに侵入を広げ、攻撃する。 または、マルウェアに感染したファイルがWeb会議等で共有され拡散する。	・マルウェア対策ソフト ・パッチ適用 ・IDS/IPS ・権限管理 **・LBOテナントアクセス制御** **・接続先制限** ・EDR
通信データ改ざん ーネットワーク上を流れる情報を改ざんする。	・通信路暗号化 ・通信相手の証明書による認証

※ローカルブレイクアウトとは直接関係のない物理的な脅威等は対象外とする。

（参考）対策レベルとリスク値

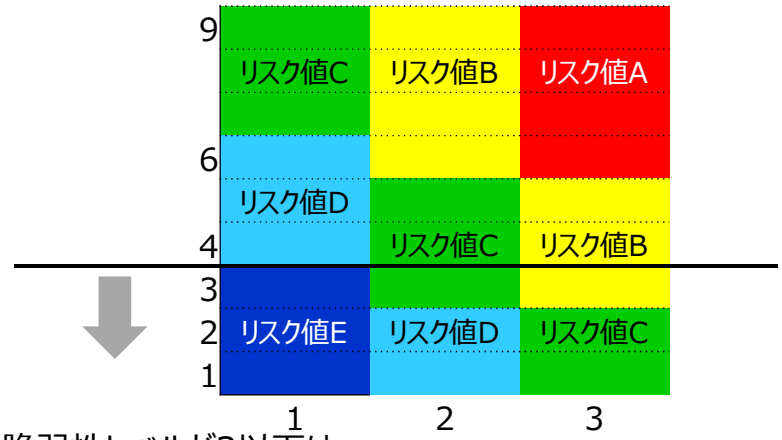
- ✓ 脅威レベルが最も高い3（脅威が発生しやすい）であっても、十分な対策により脆弱性が１であれば、脅威レベル×脆弱性レベル＝3となり安全である。
- ✓ 対策が不十分で脆弱性が3であっても、脅威レベルが最も低い1(脅威が発生しにくい）であれば、脅威レベル×脆弱性レベル＝3となり安全である。

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

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、**３以下であり安全性が確保された水準**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**脅威レベル×脆弱性レベル≦3**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**脅威レベル×脆弱性レベル≦3**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）

＜前提条件＞

（１）利用するクラウドサービス

・ ISMAPに登録されているクラウドサービス

（２）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

●技術的対策（案）

対策を実施しなくてもリスクアセスメント結果において、リスク値が３以下となった対策は推奨とする。

技術的対策	対策の定義	必須	推奨
LGWAN接続系での対策			
通信相手の証明書による認証	通信相手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	マルウェアを検知・除去する。パターンマッチング方式、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。	○	
冗長化	ローカルブレイクアウトファイアウォールに対するDDoS攻撃発生時の継続稼働を保証するために、あるいは障害状態からの早期回復を実現するために、システムの重要構成要素を多重化し、冗長構成とする。		○
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。	○	

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

＜前提条件＞

（１）利用するクラウドサービス

・ISMAPに登録されているクラウドサービス

（２）クラウドサービスの利用条件

・**各団体専用領域（テナント）があり、当該団体職員のみが該当テナントにアクセスを許可する**制御が可能

・**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。**

・クラウドサービスで利用するアプリケーションは以下のとおり

- **Web会議システム**(例： Teams)
- **ファイル管理システム**(例： SharePoint、OneDrive)
- **メール**(例：Exchange)

なお、メールは、インターネット接続系のメール利用を前提とするが、災害時にインターネット接続系のメール利用不可となった時を考慮し、クラウドサービスでのメール利用も想定する。

・クラウドサービスの**Web会議やメールで取り扱うファイルのマルウェア検査が可能**（例：Defender)

・ファイルはクラウドサービス上での共有、編集を可能とし、**PCにはダウンロードさせない設定**が可能

●技術的対策（案）※次項に続く

対策を実施しなくてもリスクアセスメント結果において、リスク値が３以下となった対策は推奨とする。

技術的対策	対策の定義	必須	推奨
クラウドサービス上での対策			
マルウェア対策	クラウドサービス上でWeb会議やインターネットメールで取り扱うファイルのマルウェア検査を行う。		○
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。	○	
LGWAN接続系での対策			
通信相手の証明書による認証	通信相手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	マルウェアを検知・除去する。パターンマッチング方式、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。	○	

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取り込まない場合）②

●技術的対策（案）※次項からの続き

技術的対策	対策の定義	必須	推奨
LGWAN接続系での対策			
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接続系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。（※）	○	
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。	○	
未知の不正プログラム対策（エンドポイント対策）	従来のパターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動の端末を監視・検出・特定する。また、異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施する。さらにインシデント発生要因の詳細な調査を実施する。LGWAN接続系に配置する端末、業務サーバにて対応が必要。		○
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。	○	
冗長化	ローカルブレイクアウトファイアウォールに対するDDoS攻撃発生時の継続稼働を保証するために、あるいは障害状態からの早期回復を実現するために、システムの重要構成要素を多重化し、冗長構成とする。		○
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。	○	

α'モデルの対策（外部とファイル送受信を行う場合）①

＜前提条件＞

（１）利用するクラウドサービス

- ISMAPに登録されているクラウドサービス

（２）クラウドサービスの利用条件

- **各団体専用領域（テナント）があり、当該団体職員のみが該当テナントにアクセスを許可する**制御が可能
- クラウドサービスで利用するアプリケーションは以下のとおり
  - **Web会議システム**(例：　Teams)
  - **ファイル管理システム**(例：　SharePoint、OneDrive)
  - **メール**(例：Exchange)

    なお、メールは、インターネット接続系のメール利用を前提とするが、災害時にインターネット接続系のメール利用不可となった時を考慮し、クラウドサービスでのメール利用も想定する
- クラウドサービスのWeb会議やメールで取り扱う**ファイルのマルウェア検査が可能**（例：Defender)

●技術的対策（案）※次項に続く

対策を実施しなくてもリスクアセスメント結果において、リスク値が３以下となった対策は推奨とする。

技術的対策	対策の定義	必須	推奨
クラウドサービス上での対策			
マルウェア対策	クラウドサービス上でWeb会議やインターネットメールで取り扱うファイルのマルウェア検査を行う。		○
LGWAN接続系での対策			
通信相手の証明書による認証	通信相手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	マルウェアを検知・除去する。パターンマッチング方式、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。	○	

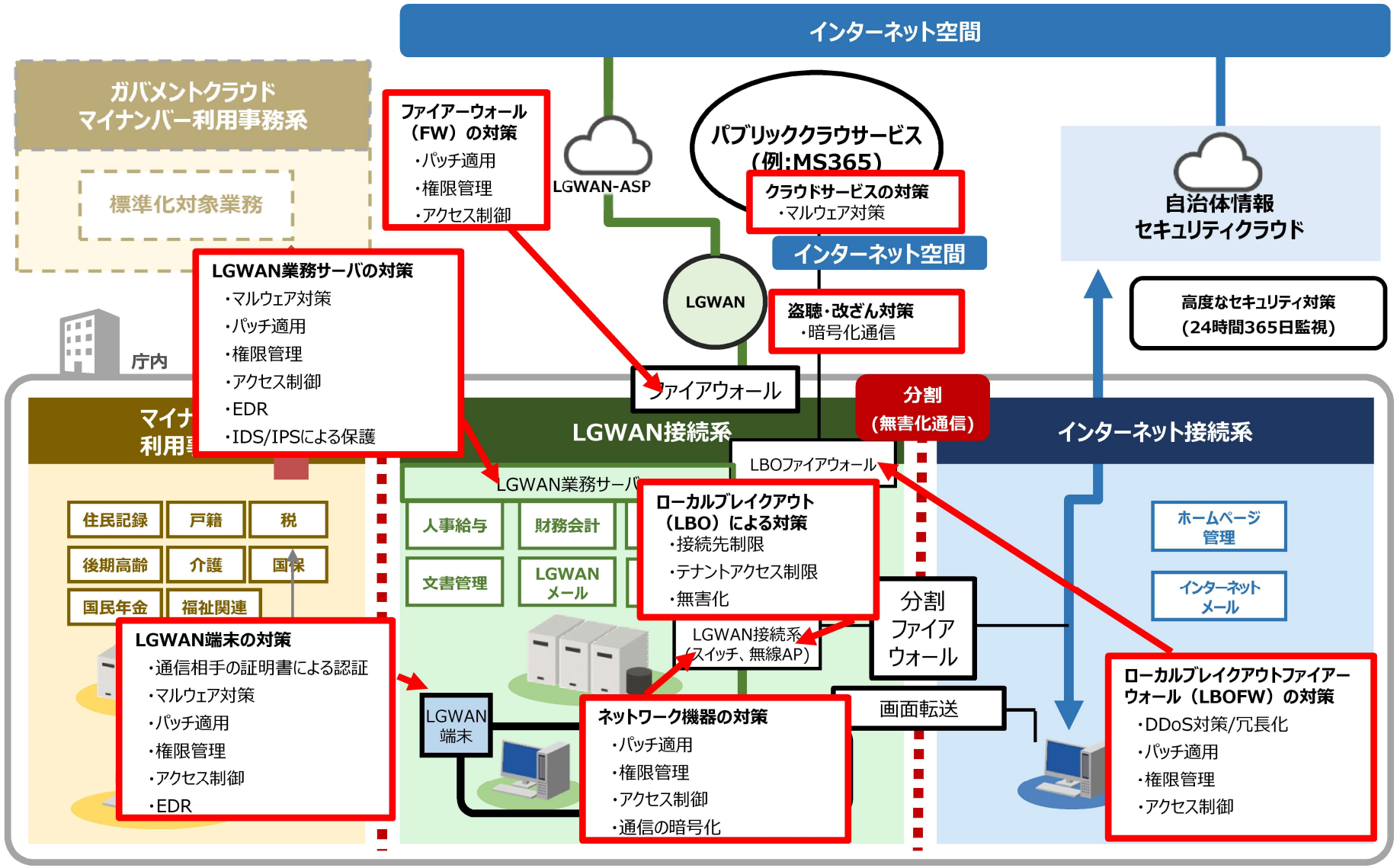
α'モデルの対策（外部とファイル送受信を行う場合）②

●技術的対策（案）※次項からの続き

技術的対策	対策の定義	必須	推奨
LGWAN接続系での対策			
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接続系からファイルを取り込む。（※）	○	
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。 ※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。	○	
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。	○	
未知の不正プログラム対策（エンドポイント対策）	従来のパターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動の端末を監視・検出・特定する。また、異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施する。さらにインシデント発生要因の詳細な調査を実施する。LGWAN接続系に配置する端末、業務サーバにて対応が必要。		○
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。	○	
冗長化	ローカルブレイクアウトファイアウォールに対するDDoS攻撃発生時の継続稼働を保証するために、あるいは障害状態からの早期回復を実現するために、システムの重要構成要素を多重化し、冗長構成とする。		○
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。	○	

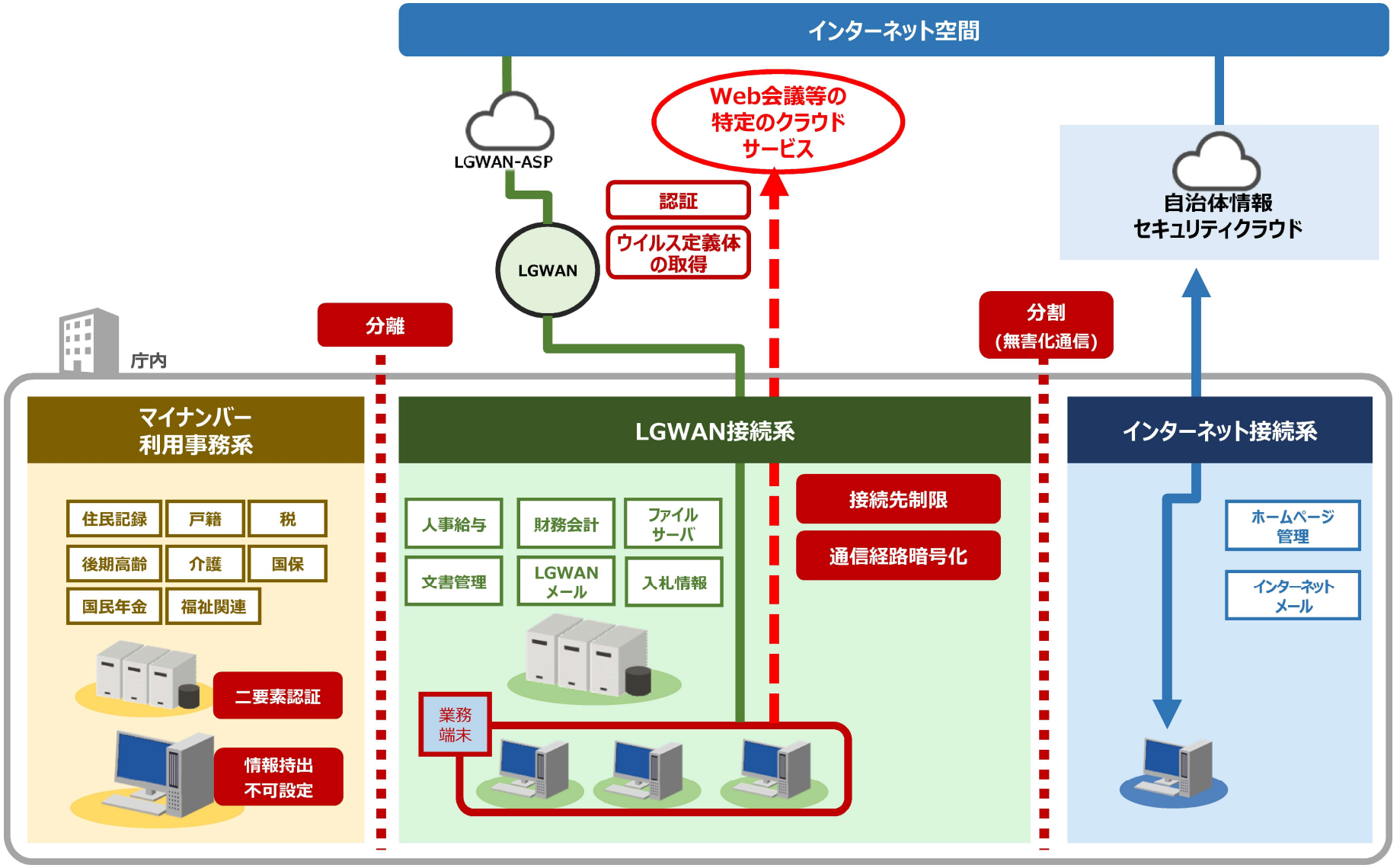
a'モデルの技術的対策

✓ 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

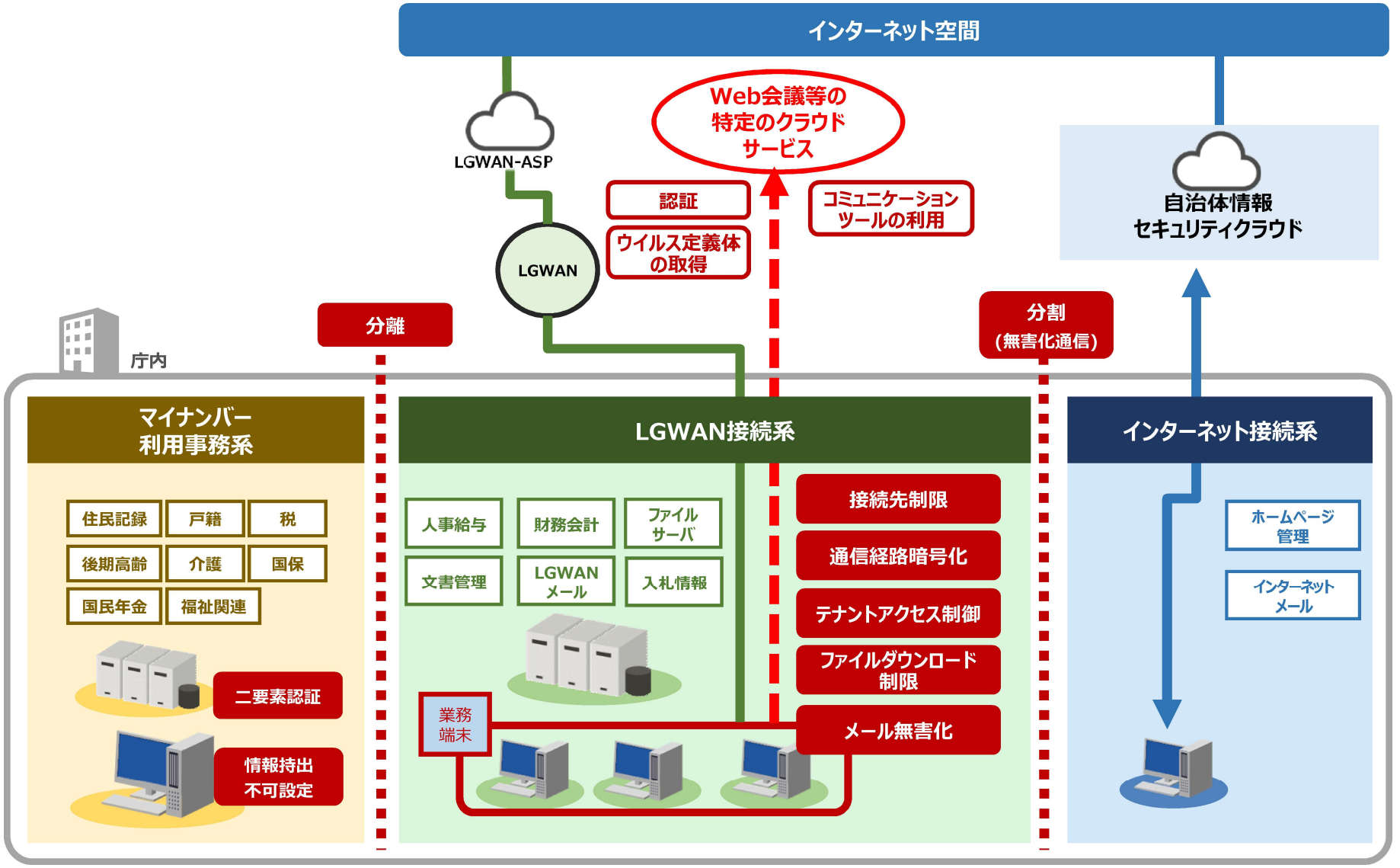
✓ 認証・ウイルス定義体の取得のみの場合におけるセキュリティ対策のネットワーク構成イメージは以下の通り。



※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

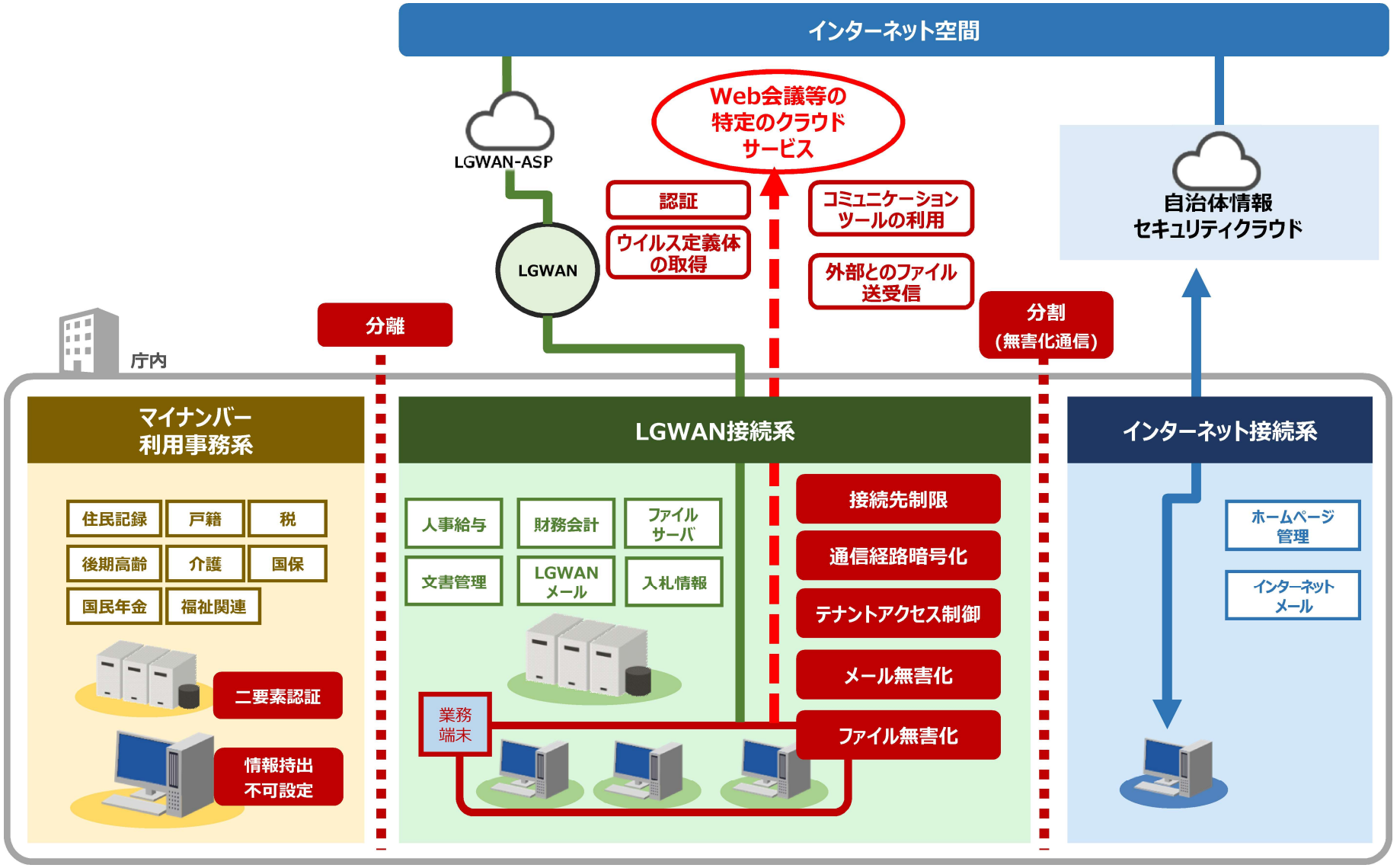
✓ コミュニケーションツールを利用するが、ファイルを内部に取り込まない場合におけるセキュリティ対策のネットワーク構成イメージは以下の通り。



※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。

α'モデルの組織的・人的対策（案）

技術的対策		対策の定義	必須	推奨
組織的・人的対策				
	手続き・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	○	

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。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。

・　特に、本モデルを採用する地方公共団体においては、許可したクラウドサービス（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）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。

・　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）。

・　また、クラウドサービスの利用形態およびサービス内容を踏まえた安全性確保が重要であり、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点に留意が必要である。
特に、外部とのデータ通信、ファイル交換、メールの送受信等が発生する場合は、利用者の多要素認証やデータの暗号化、無害化等の必要な対策を実施することが必要である。

第１編　総則
第1章 本ガイドラインの目的等
本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は、各地方公共団体が保有する情報資産を守るにあたって自ら責任を持って確保すべきものであり、情報セキュリティポリシーも各地方公共団体が組織の実態に応じて自主的に策定するものである。

○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**。

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
③
（前ページからの続き）

・　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。

β モデル又はβ’モデルを採用する場合について、同様の規程がある。

【解説】

３．情報システム全体の強靭性の向上

(３) インターネット接続系

β モデル又はβ’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、インターネット接続系とLGWAN 接続系を完全に分離する場合を除き、**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**。

ガイドライン改定案（見え消し）②

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。

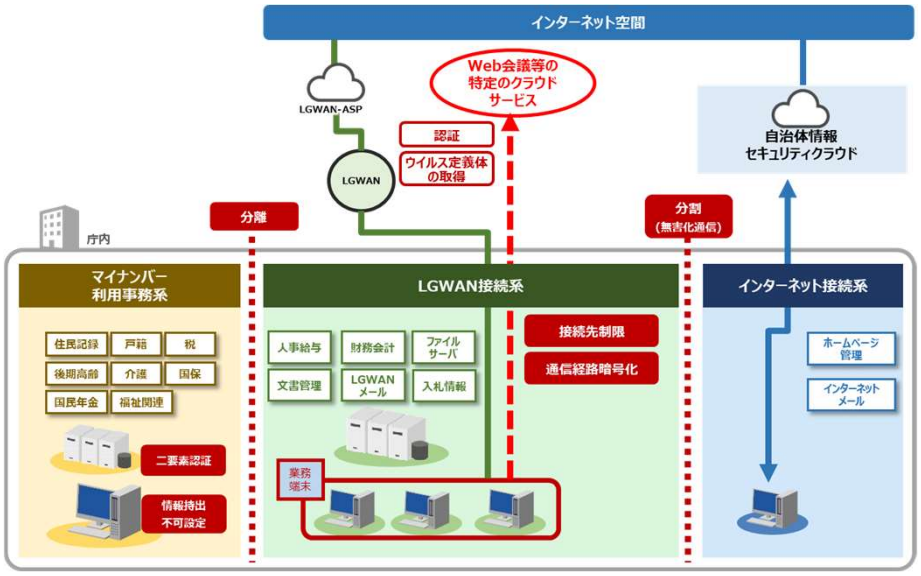
対策区分	セキュリティ対策	概要
技術的対策	通信相手の証明書による認証	・通信相手が本物であるか否か、正当性を確認する。
	マルウェア対策ソフト	・マルウェアを検知・除去する。パターンマッチング方式、不審な動作を行うコードが含まれていることを検出する振る舞い検知を行う。LGWAN接続系に配置する端末、業務サーバで対応が必要となる。
	パッチ適用	・脆弱性を修正するパッチを速やかに適用し、脆弱性を解消するLGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、接続系のスイッチ・無線APで対応が必要となる。
	接続先制限	・LGWAN接続系から外部へのアクセス先を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	手続き・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25　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）②

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。

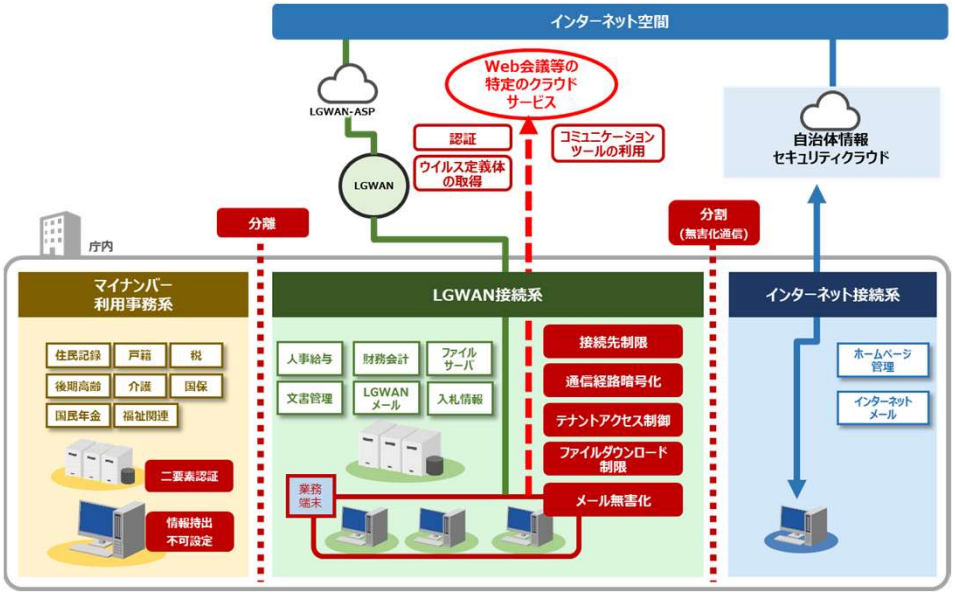
対策区分	セキュリティ対策	概要
技術的対策	クラウドサービスからファイルダウンロード制限	・クラウドサービス上から業務端末へのファイルダウンロードを制限する。
	通信相手の証明書による認証	・通信相手が本物であるか否か、正当性を確認する。
	マルウェア対策ソフト	・マルウェアを検知・除去する。パターンマッチング方式、不審な動作を行うコードが含まれていることを検出する振る舞い検知を行う。LGWAN接続系に配置する端末、業務サーバで対応が必要となる。
	パッチ適用	・脆弱性を修正するパッチを速やかに適用し、脆弱性を解消するLGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレ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接続系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にて対応が必要となる。
	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	手続き・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27　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）③

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。

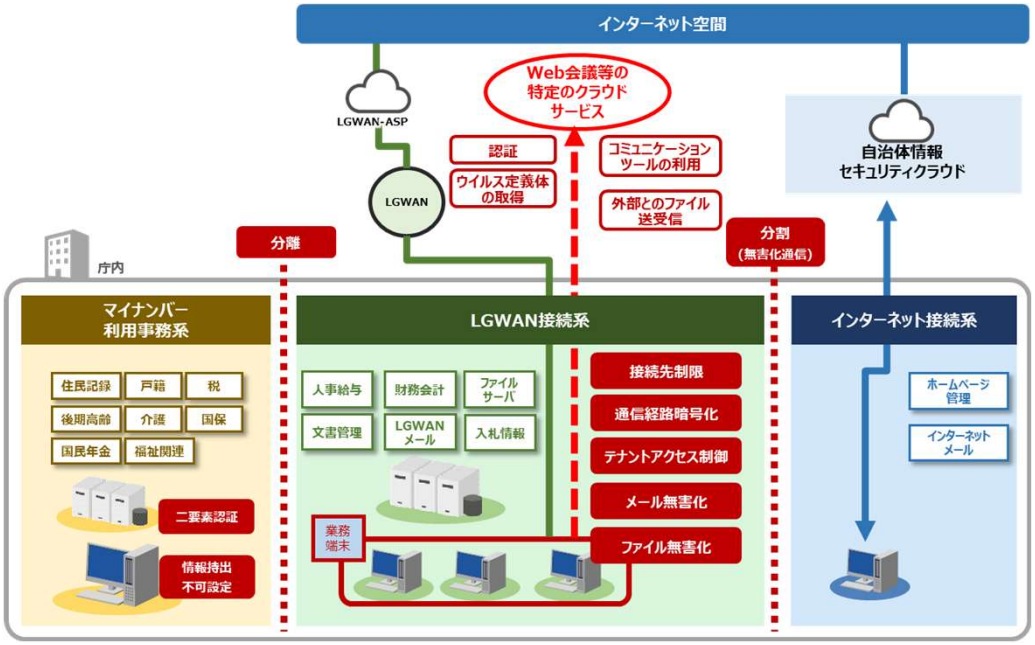
対策区分	セキュリティ対策	概要
技術的対策	通信相手の証明書による認証	・通信相手が本物であるか否か、正当性を確認する。
	マルウェア対策ソフト	・マルウェアを検知・除去する。パターンマッチング方式、不審な動作を行うコードが含まれていることを検出する振る舞い検知を行う。LGWAN接続系に配置する端末、業務サーバで対応が必要となる。
	パッチ適用	・脆弱性を修正するパッチを速やかに適用し、脆弱性を解消するLGWAN接続系に配置する端末、業務サーバ、ファイアウォール、ローカルブレイクアウトファイアウォール、接続系のスイッチ・無線APで対応が必要となる。
	接続先制限	・LGWAN接続系から外部へのアクセス先を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接続系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	手続き・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29 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

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（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）



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。

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

前回いただいたご意見

✓ 前回の検討会では、**通信先の特定は必要条件ではあるが、セキュリティ対策として十分とはいえない**ことに留意すべきなどの意見をいただいた。
✓ これまでいただいたご指摘を踏まえ、リスクアセスメントの対象となるセキュリティ要件を今後検討する。

観点１：ネットワークモデルと接続先のセグメント

α/α'モデル団体が、マイナンバー利用事務系又はLGWAN接続系に画面転送接続する場合に加え、β/β'モデルの団体が、マイナンバー利用事務系又はインターネット接続系に画面転送接続する場合についてもセキュリティリスクを分析。

観点２：接続要件

画面転送で使用される通信に関し、特定通信*（マイナンバー利用事務系からインターネットに接続する場合に**最低限必要な、接続先特定のための通信**）を実施した場合のセキュリティリスクを分析。

(*)通信経路の限定（MACアドレス、IPアドレス）に加えて、アプリケーションプロトコル（ポート番号）のレベルでの限定等を行う。

観点３：端末仮想化の方式

VDI、SBC、セキュアブラウザの３方式についてセキュリティリスクを分析。

観点４：業務運用

個人情報保護法や番号法上問題がないように対策を検討する必要がある。

検討項目	発言要旨
画面転送	• リスク観点の接続要件の中に特定通信とあるが、IPアドレスの限定かつポート番号の限定だけでいいと読めてしまうことが気になる。「特定通信さえすればよい」とならないようご注意いただきたい。 • β'モデルを採用した自治体ではマイナンバー利用事務系との通信を必要としないのではないか。リスクアセスメントの前にニーズがあるか調べた方がよいと思う。 • 観点４は、リスクアセスメントに関する観点というよりは、どのような運用であれば問題ないか検討していただきたい。