資料２－３

【サイバーセキュリティ対策室提出資料】
今年度のガイドライン改定の方向性と機密性の整理について

総務省

令和８年１１月４日
サイバーセキュリティ対策室

三層対策について

公表資料

○ 2015年度の日本年金機構の個人情報流出を受けて、地方公共団体には「三層対策」の実施を要請。

新たな自治体情報セキュリティ対策の抜本的強化に向けて（H27年度報告）

〈三層の構えで万全の自治体情報セキュリティ対策の抜本的強化を〉

1．マイナンバー利用事務系（既存住基、税、社会保障など）においては、**原則として、他の領域との通信をできないように**した上で、端末からの情報持ち出し不可設定や端末への二要素認証の導入等を図ることにより、住民情報の流出を徹底して防ぐこと。

2．マイナンバーによる情報連携に活用されるＬＧＷＡＮ環境のセキュリティ確保に資するため、財務会計などＬＧＷＡＮを活用する業務用システムと、Ｗｅｂ閲覧やインターネットメールなどのシステムとの通信経路を分割すること。なお、両システム間で通信する場合には、ウイルスの感染のない無害化通信を図ること（**LGWAN接続系とインターネット接続系の分割**）。

3．インターネット接続系においては、都道府県と市区町村が協力してインターネット接続口を集約した上で、**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講じること。

ガイドラインで求めている主要なセキュリティ対策について

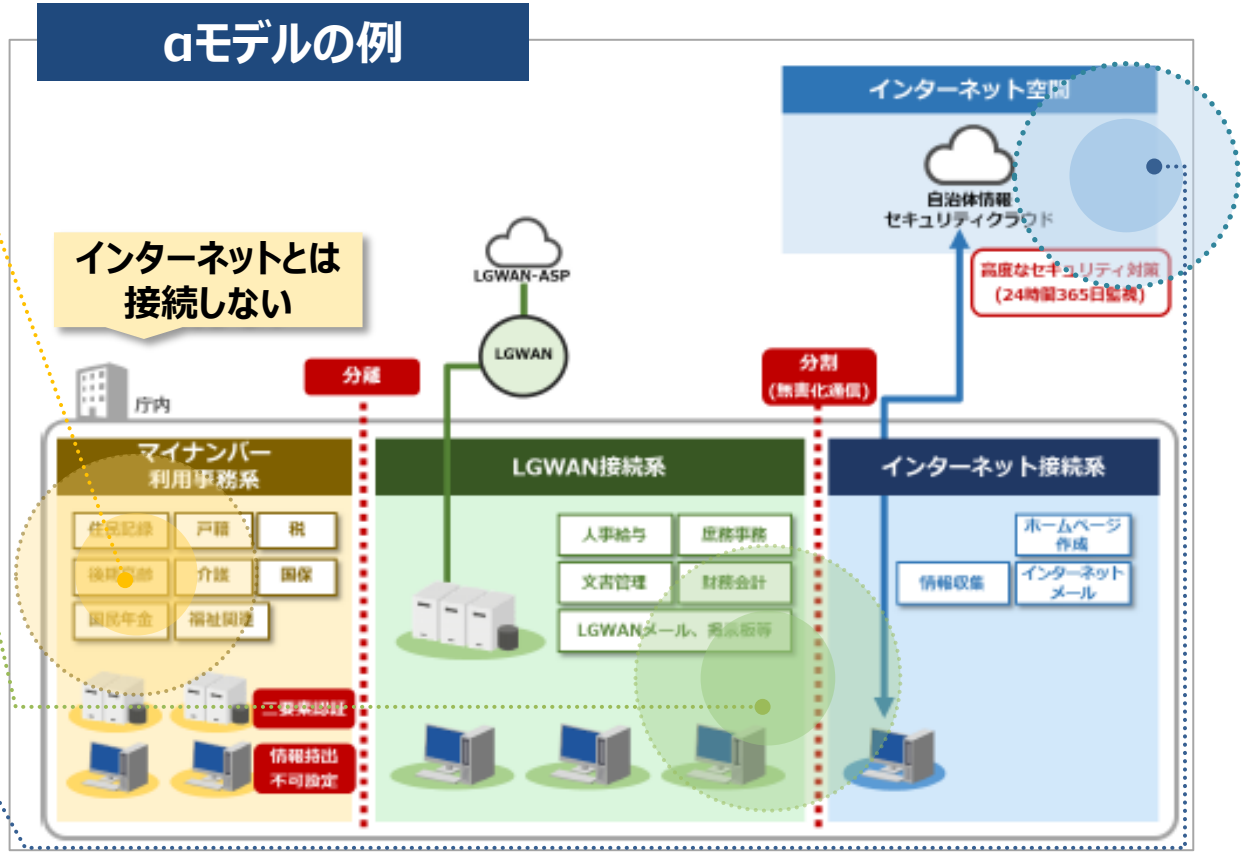
公表資料

- 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。
- 地方公共団体の情報システムをマイナンバー利用事務系、LGWAN接続系、インターネット接続系の３つに分けて防御を実施するとともに、都道府県が自治体情報セキュリティクラウドを構築して、インターネットからのサイバー攻撃の脅威等から効率的に防御。

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



βモデルとβ′モデルについて

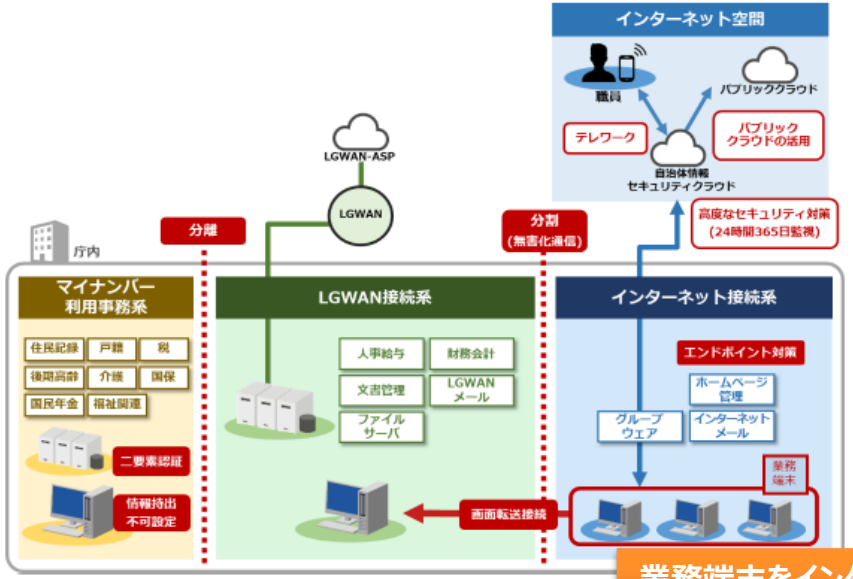
公表資料

■ 令和2年度ガイドライン改定により、利便性を高めるため、**高度なセキュリティ対策を実施することを条件に**、インターネット接続系に業務端末を配置するβモデルとβ′モデルを示している。

βモデル(重要な情報資産配置なし)

業務効率性・利便性：中　**必要な対策のレベル：中**

- インターネット接続系に主たる業務端末を配置
- 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



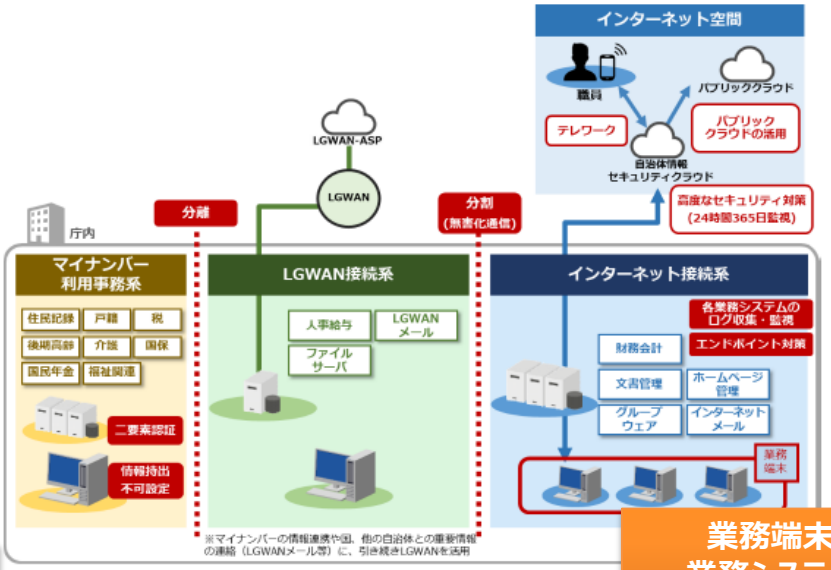
βモデルイメージ図

業務端末をインターネット接続系に配置

β′モデル(重要な情報資産配置あり)

業務効率性・利便性：高　**必要な対策のレベル：高**

- βモデルに加え、文書管理、財務会計等の業務システム（マイナンバー利用事務系を除く。）をインターネット接続系に配置
- βモデルの技術的対策、組織的、人的対策の確実な実施の条件に加え、情報資産単位でのアクセス制御、組織的なセキュリティ対策基準の遵守、セキュリティの継続的な検知・モニタリング体制の構築が条件



β′モデルイメージ図

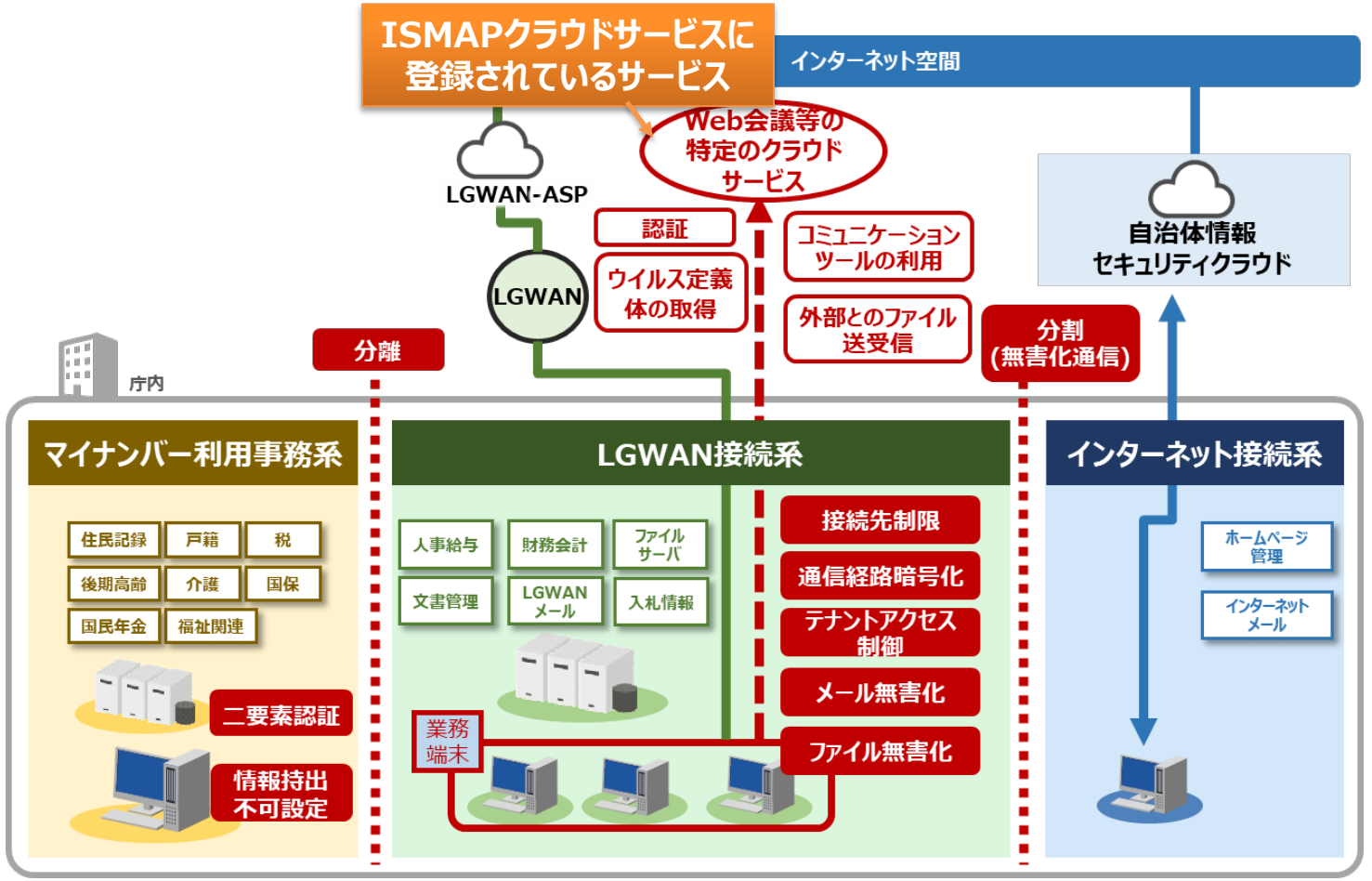
業務端末と業務システムをインターネット接続系に配置

LGWAN接続系からのローカルブレイクアウト（α'モデル）

公表資料

■ 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モデルの状態であり、インターネットに接続しWeb会議等の特定のクラウドサービスを利用する必要が生じている。

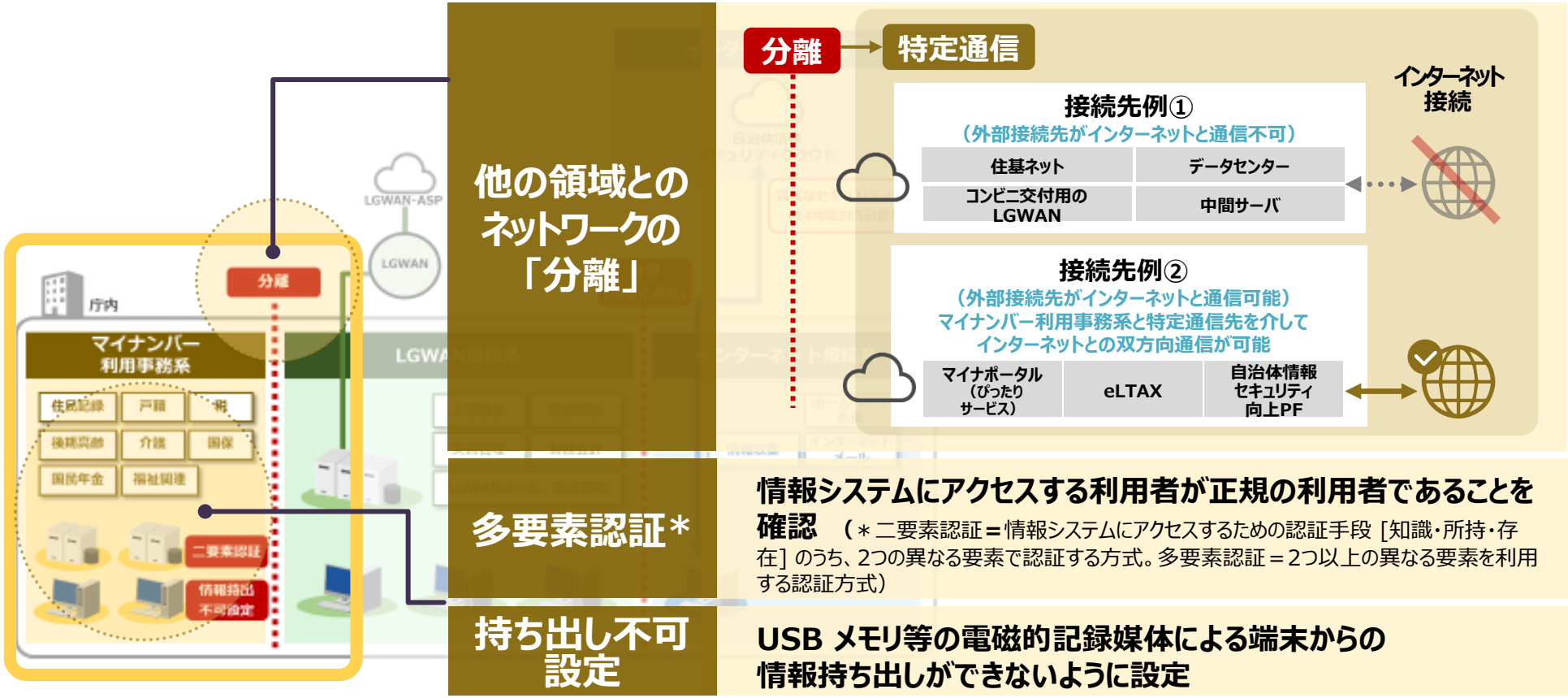
セキュリティ対策を徹底の上、LGWAN接続系からWeb会議等の特定のクラウドサービスに対して直接接続を行うモデル（α'モデル）を検討（令和6年10月改定で追加）



マイナンバー利用事務系と特定通信について

公表資料
（一部編集）

○ ガイドライン上、住民情報の流出を防ぐ必要があることから、他の領域（LGWAN接続系及びインターネット接続系）との通信をできないようにする必要がある。
○ マイナンバー利用事務系と外部接続先の通信が必要な場合は、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）のレベルでの限定を行う必要があり、これらの通信を「**特定通信**」と定義。



総務省ガイドライン図表22

公表資料

機密性 高 → 低

分類	分類基準	情報資産	パブリッククラウドサービス（※１）の範囲
自治体機密性３A	行政事務で取り扱う情報資産のうち、「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）に定める秘密文書に相当する文書	＜例＞ ・「行政文書の管理に関するガイドライン」上の極秘文書、秘文書に相当する文書（統一基準における機密性３情報に相当する情報） ・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	「行政文書の管理に関するガイドライン」、統一基準の規定に則って取り扱うものとする（なお、上記ガイドラインにおいては、極秘文書について、インターネットに接続していない電子計算機又は媒体等に保存することが求められている（※２）） ISMAP登録サービスは利用可（8.3で規定されるアクセス制御、機密性保護のための暗号化等が必要） ※統一基準改定に合わせて、8.3でクラウドサービスの利用について規定
自治体機密性３B	行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	＜例＞ ・データベースや台帳形式になった住民情報を含む個人情報ファイル及びこれに準ずる情報 （住民記録システム、税務システム、国民健康保険システム、生活保護システム、農業委員会台帳システム、貸付金償還システム等に保存される住民の個人情報）	
自治体機密性３C	行政事務で取り扱う情報資産のうち、自治体機密性３B以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	＜例＞ ・職員としての属性に基づく個人情報 ・オンライン申請の処理等により、システム処理上一時的にインターネット上に保管されるデータ ・文書管理システムの決裁文書として保存されている個人情報 ・施設設計情報や入札予定価格など非公開情報	
自治体機密性２	行政事務で取り扱う情報資産のうち、自治体機密性３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	＜例＞ ・政策検討に関する情報	可 （8.3で規定されるアクセス制御、機密性保護のための暗号化等が必要）
自治体機密性１	自治体機密性２又は機密性３の情報資産以外の情報資産	＜例＞ ・将来公表する予定の文書（白書の案等） ・公表された情報	可

注）自治体機密性３C情報については、情報資産単位でのアクセス制御、業務システムログ管理の実施等、β'モデルにおいてインターネット接続系に求められている対策を実施することで、インターネット接続系における取扱いが可能。

※１　クラウド事業者が提供するサーバやネットワークなどのインフラを、仮想化技術により複数のユーザで共用し、個々のユーザが、システムの運用体系を完全に制御することが難しいサービスを想定している。

※２　「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 令和７年２月14 日一部改正）第10 秘密文書等の管理