資料１

自治体情報セキュリティ対策の経緯について

総務省

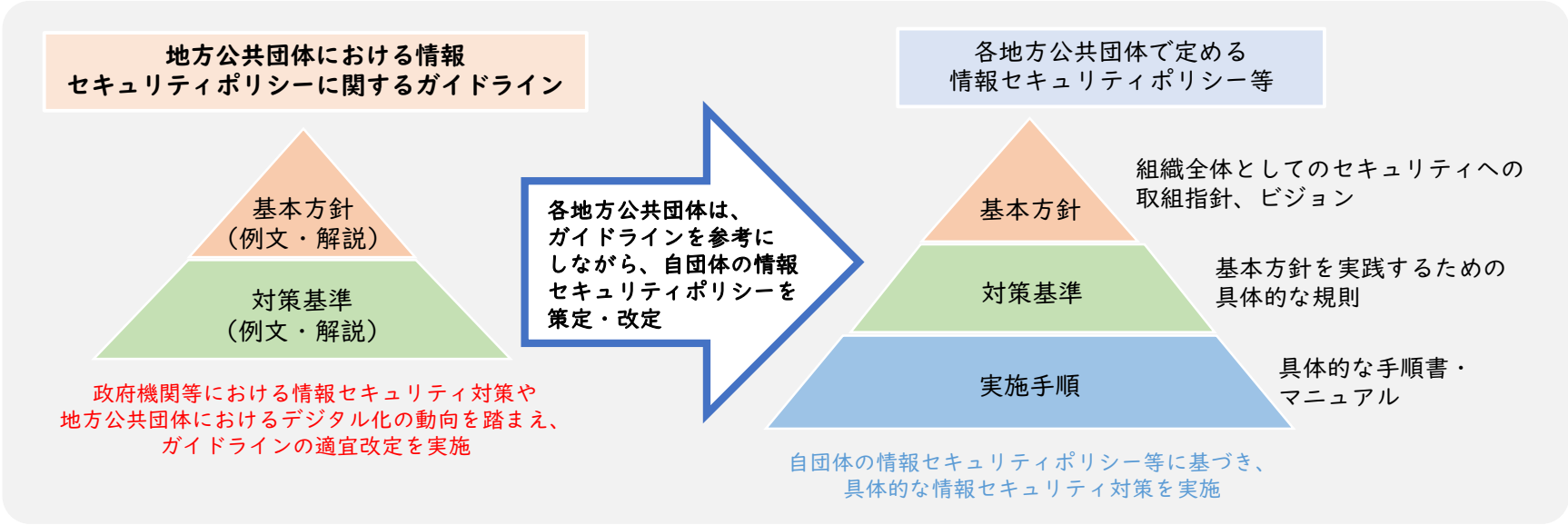
2021年９月27日

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

「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」について

総務省における自治体の情報セキュリティ対策への支援

総務省は、地方公共団体の情報セキュリティ対策を支援するため、平成13年度に自治体情報セキュリティ対策の指針として「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」を策定し、その後も、政府機関等における情報セキュリティ対策の動向や地方公共団体におけるデジタル化の動向等を踏まえながら適宜ガイドラインの改定を実施してきた。



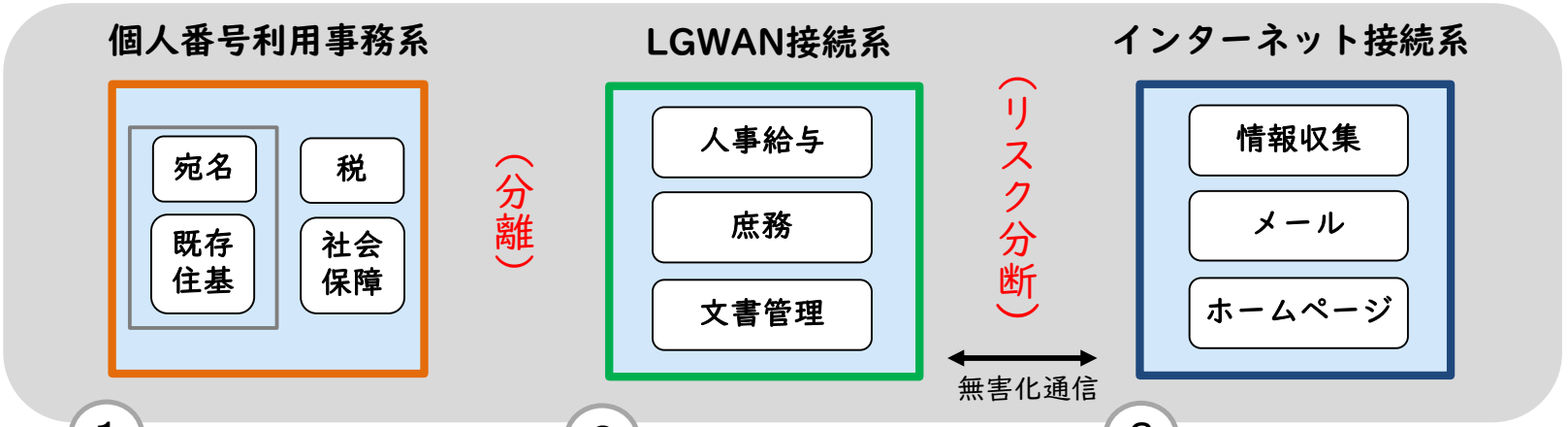
これまでの主なガイドライン改定

改定時期	改定内容・理由
平成15年3月	①外部委託に関する管理、②情報セキュリティ監査、③無線LAN等の新たな技術動向等を踏まえた記述等の追加
平成27年３月	「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（マイナンバー法）」、 「サイバーセキュリティ基本法」等の成立や新たな対策技術の動向、政府の情報セキュリティ政策の改定を踏まえて一部改定
平成30年９月	平成27年の日本年金機構における情報流出事案を受け、総務省から自治体へ要請を行った「三層の対策」等の 自治体情報セキュリティの抜本的強化策の内容を反映（「三層の対策」の詳細は次頁）

「三層の対策」概要

「三層の対策」によるセキュリティ対策の強化について（2015年～）

市町村におけるネットワーク構成（イメージ）



1 個人番号利用事務系では、端末からの情報持ち出し不可設定等を図り、住民情報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

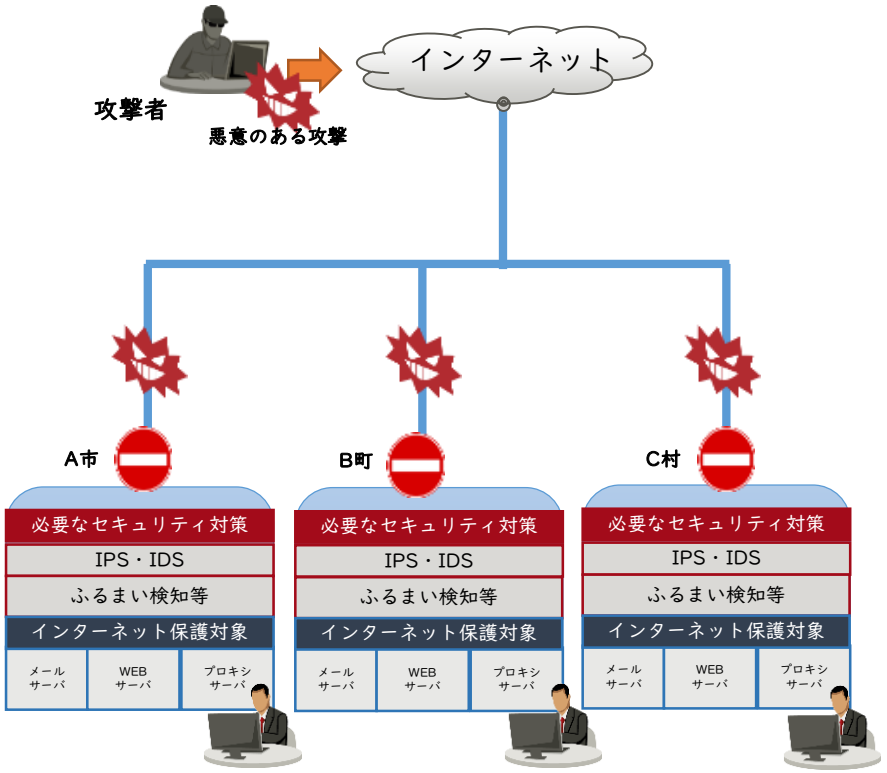
3 都道府県と市区町村が協力して、自治体情報セキュリティクラウドを構築し、高度なセキュリティ対策を実施

対策要請の経緯

2015.5　年金機構の情報漏えい事案発覚後、有識者による「自治体情報セキュリティ対策検討チーム」を設置
2015.11　検討チームより自治体の対策内容（「三層の対策」）について報告
2015.12　総務大臣通知により自治体に「三層の対策」を要請
2016.2　自治体が「三層の対策」に取り組むための補助金を創設（H27年度補正予算）
2017.7　自治体による「三層の対策」への対応完了

自治体情報セキュリティクラウドについて

導入前イメージ

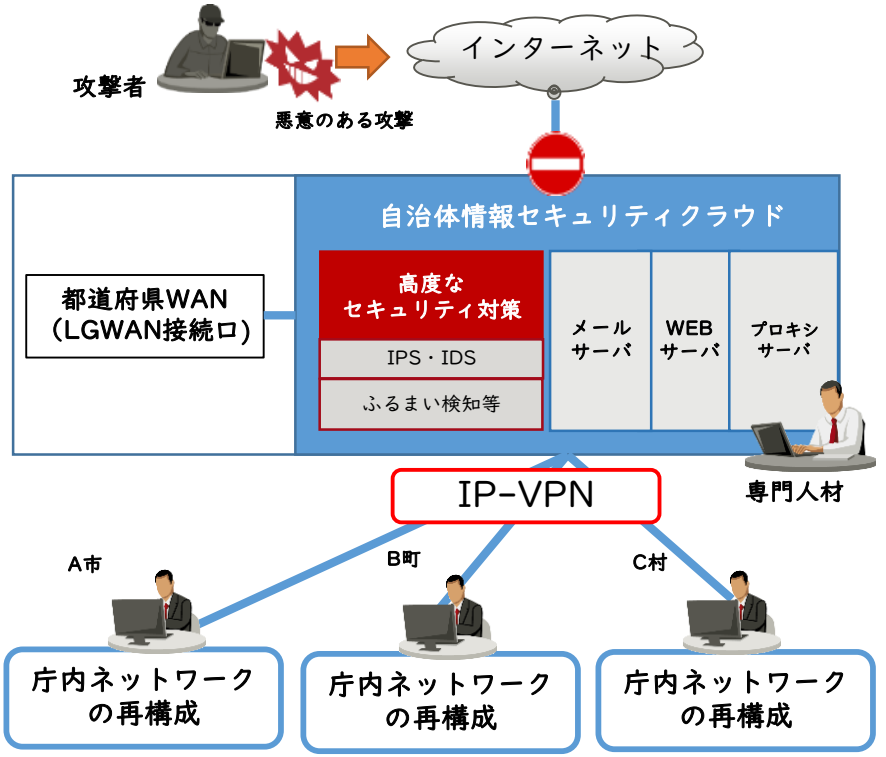


課題

- 各自治体ごとに監視水準にバラツキ
- 不正接続など必要なセキュリティ対策におけるコストが甚大
- プロキシログ等の分析するスキルを持った職員の不足
- 個々の自治体のインシデント情報の共有化に時間を要する

導入後イメージ

全都道府県で運用開始（2017年７月～）
→2021年度末に更新の自治体が多い



特色

- 全国的に必要な監視水準を確保・維持
- サーバの共同利用によりコスト減
- セキュリティ専門人材によるプロキシログ等の分析
- 自治体システム側からLGWANへの不適切なアクセス等の監視
- 都道府県相互でインシデント情報の共有化が可能

令和2年度のガイドライン改定までの経緯

「三層の対策」により短期間で自治体の情報セキュリティ対策を抜本的に強化し、
インシデント数の大幅な減少を実現

一方で、

① ユーザビリティへの影響

- 自治体内の情報ネットワークの分離・分割による事務効率の低下
  例：マイナンバー利用事務系のシステムへのデータの取込み、
  インターネットメールの添付ファイルの取得など

② 新たな時代の要請

- 行政アプリケーションを自前調達方式からサービス利用式へ
  （政府における「クラウド・バイ・デフォルト」原則）
- 行政手続を紙から電子へ（デジタル手続法を受けた行政手続のオンライン化）
- 働き方改革 (テレワーク等のリモートアクセス)
- サイバー攻撃の増加、サイバー犯罪における手口の巧妙化　　等

「三層の対策」の効果や課題、新たな時代の要請を踏まえ、効率性・利便性を向上させた新たな自治体情報セキュリティ対策を検討会 (※) において検討し、**令和２年５月に「三層の対策」の見直しを公表**

上記とりまとめを踏まえ、「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」及び「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」を改定（令和２年12月28日）

令和2年度のガイドライン改定の概要

➢ 主な改定ポイント

１．マイナンバー利用事務系の分離の見直し

住民情報の流出を徹底して防止する観点から他の領域との分離は維持しつつ、国が認めた特定通信（例：eLTAX、ぴったりサービス）に限り、インターネット経由の申請等のデータの電子的移送を可能とし、ユーザビリティの向上や行政手続のオンライン化に対応

２．LGWAN接続系とインターネット接続系の分割の見直し

効率性・利便性の高いモデルとして、インターネット接続系に業務端末・システムを配置した新たなモデル（βモデル）を提示（ただし、採用には人的セキュリティ対策の実施が条件）

３．リモートアクセスのセキュリティ

業務で取り扱う情報の重要性に合わせて、LGWAN接続系のテレワークについての基本的な考え方、リスク及びセキュリティ要件とともに、想定されるモデルを記載

４．LGWAN接続系における庁内無線LANの利用

LGWAN接続系において庁内無線LANを利用する場合のセキュリティ要件を記載

５．情報資産及び機器の廃棄

神奈川県におけるHDD流出事案を踏まえ、情報システム機器の廃棄等について、情報の機密性に応じた適切な手法等を整理

６．クラウドサービスの利用

クラウドサービスを利用するにあたっての注意点（サービスレベルの検討の必要性、バックアップを含めた必要なサービスレベルを保証させる契約締結等）を記載

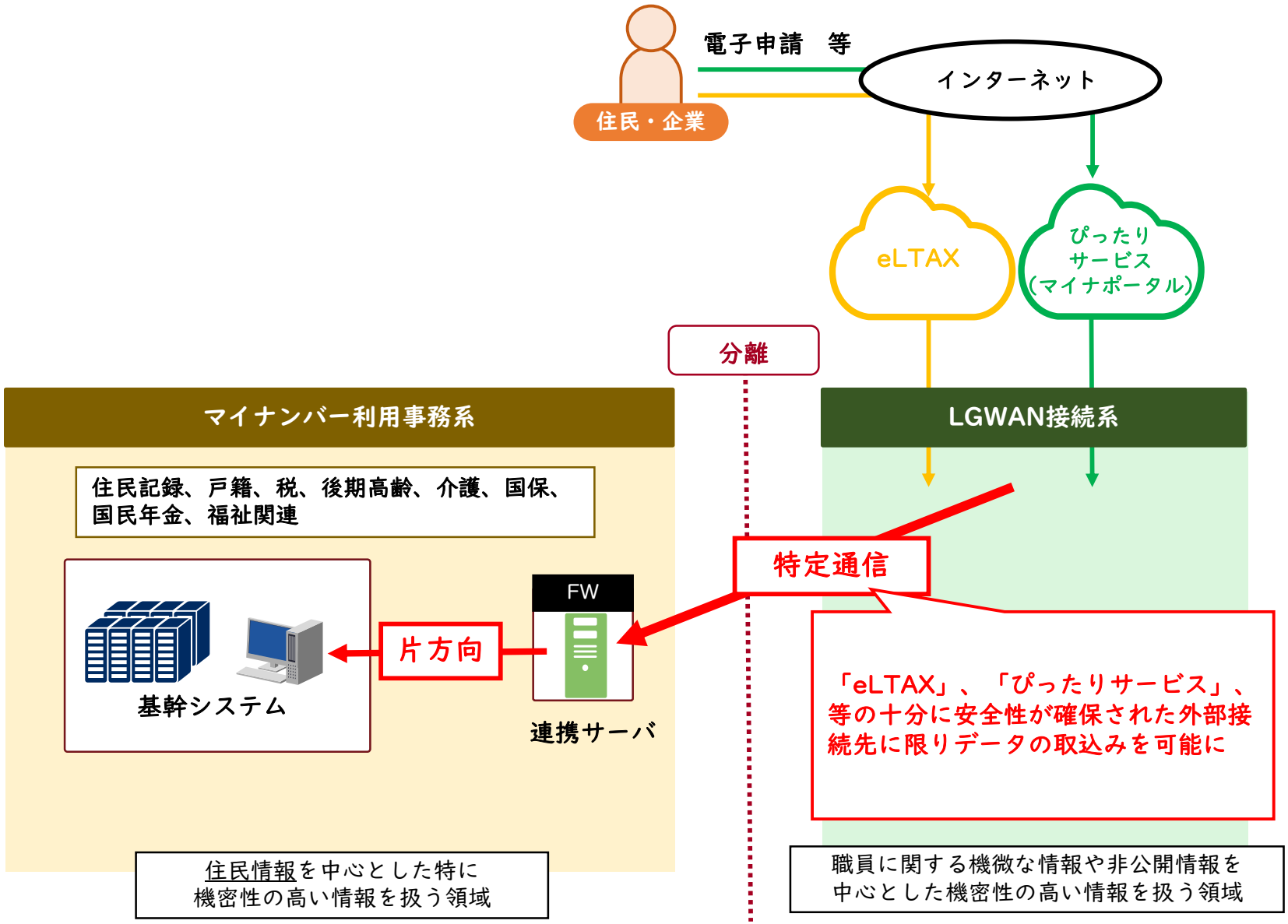
７．研修、人材育成

各自治体の情報セキュリティ体制・インシデント即応体制の強化について記載

※　その他、平成30年の「政府機関等の情報セキュリティ対策のための統一基準」の改定の内容を反映

マイナンバー利用事務系の分離の見直し

➢ ユーザビリティの向上及び行政手続のオンライン化に対応



LGWAN接続系とインターネット接続系の分割の見直し

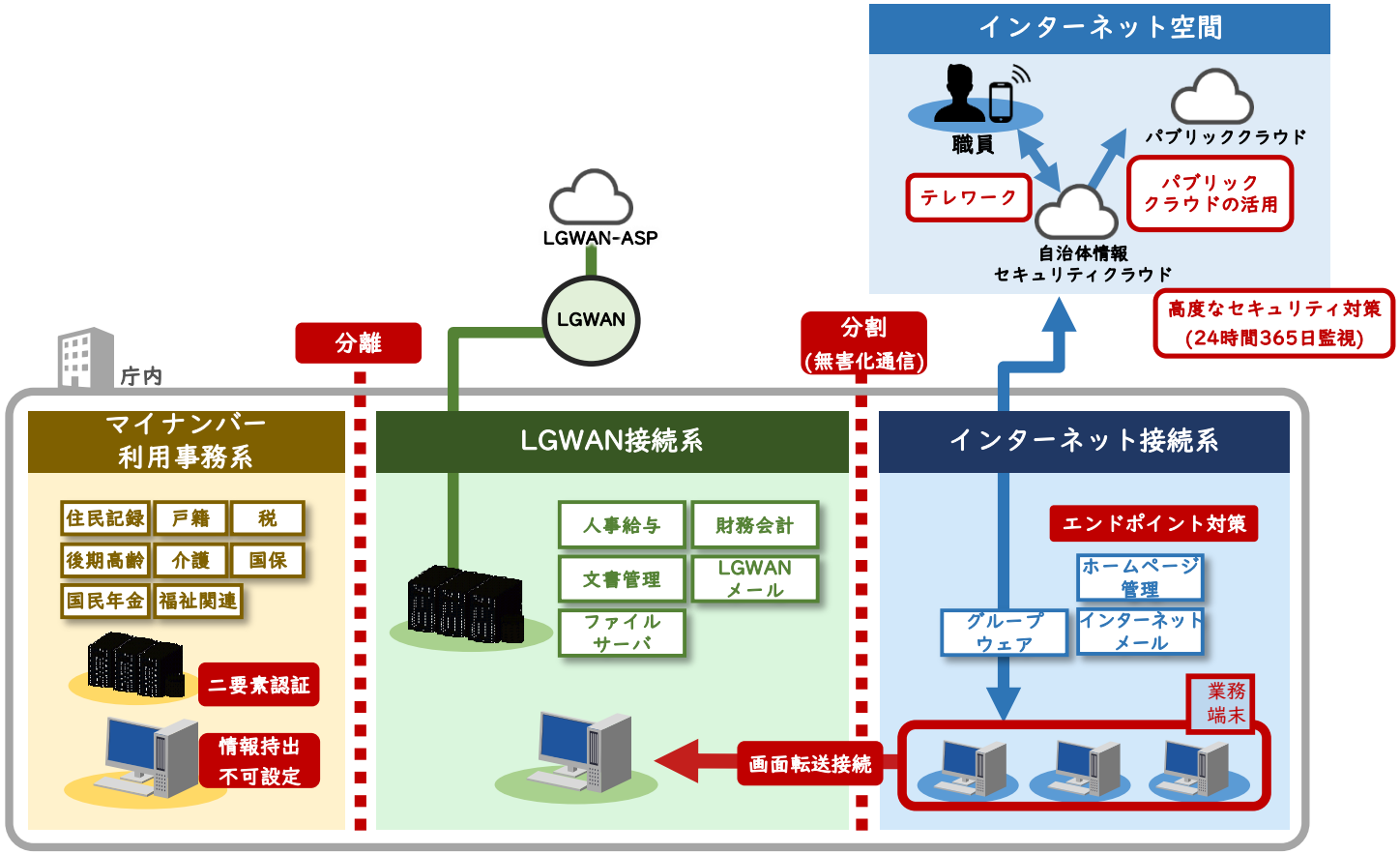
αモデル、βモデル、β’モデルの特徴比較

		αモデル (従来モデル) 業務効率性・利便性：現行と同じ（低） 必要な対策のレベル：現行と同じ（低）	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	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
モデルの特徴		・これまでの「三層の対策」による強靭化モデルを強化・改善	・業務システムをLGWAN接続系に残しつつ、業務端末をインターネット接続系に移行し、画面転送によりLGWAN接続系業務システムを利用	・βモデルに加え、文書管理、人事給与、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移行し、業務の効率性を改善
業務端末		LGWAN接続系	インターネット接続系	インターネット接続系
主なセキュリティ対策	主な技術的対策	・無害化処理 ・インターネット接続系の画面転送	・無害化処理 ・LGWAN接続系の画面転送 ・未知の不正プログラム対策（エンドポイント対策） ・業務システムログ管理 ・脆弱性管理	・無害化処理 ・LGWAN接続系の画面転送 ・未知の不正プログラム対策（エンドポイント対策） ・業務システムログ管理 ・情報資産単位でのアクセス制御 ・脆弱性管理
	主な組織的・人的対策	・インシデント対応チーム（CSIRT）の設置及び役割の明確化 ・啓発や訓練を通じた各自治体の職員のセキュリティ・リテラシーの向上 ・実践的サイバー防御演習（CYDER）の確実な受講 ・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の推進 ・自治体情報セキュリティポリシー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	左記対策の確実な実施に加えて、 ・組織的なセキュリティ対策基準の遵守 ・住民に関する情報はインターネット接続系に保存させない規定の整備	左記対策の確実な実施に加えて、 ・セキュリティの継続的な検知・モニタリング体制の整備 ・情報セキュリティ研修、標的型攻撃訓練、セキュリティインシデント訓練の受講

LGWAN接続系とインターネット接続系の分割の見直し

βモデル

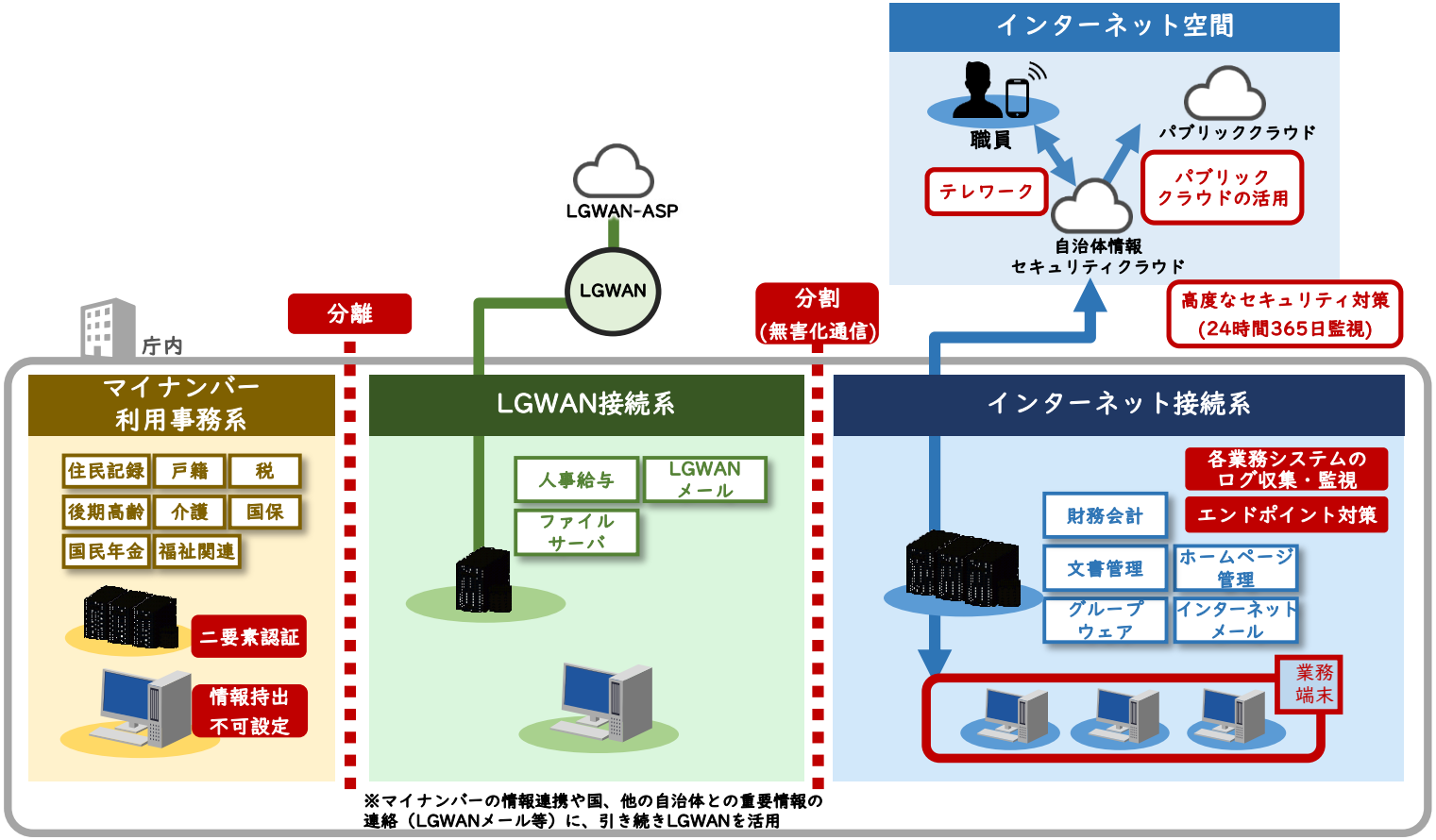
業務システムをLGWAN接続系に残しつつ、業務端末をインターネット接続系に移行し、画面転送によりLGWAN接続系業務システムを利用



LGWAN接続系とインターネット接続系の分割の見直し

β’ モデル

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移行し、業務の効率性を改善



【参考】国等の情報セキュリティ関連文書と自治体ガイドラインの関係