資料１

地方公共団体情報セキュリティ対策の経緯について

総務省

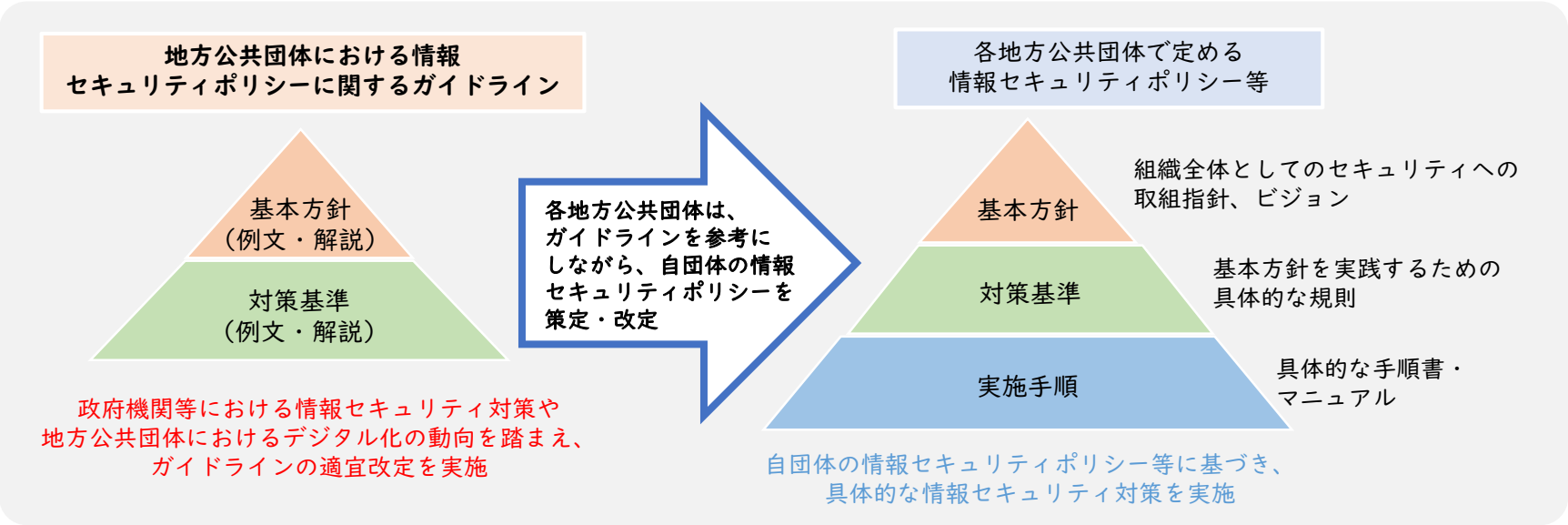
令和４年６月２日

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(第４回)

「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」の概要

総務省における地方公共団体の情報セキュリティ対策に対する支援

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



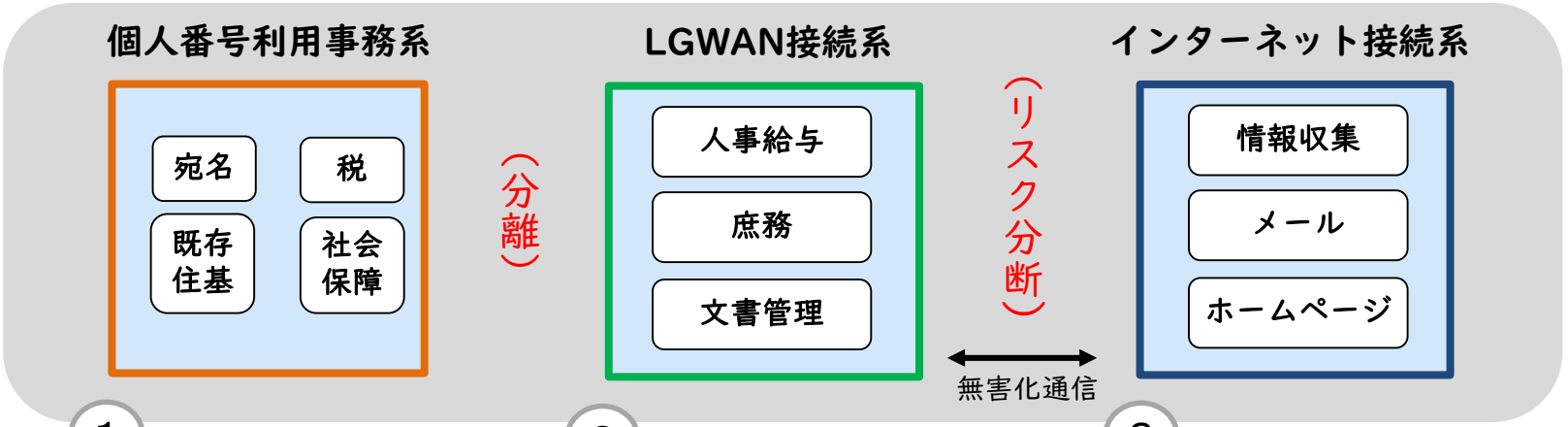
直近のガイドライン改定

改定時期	改定内容・理由
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」の成立等の内容を反映
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、総務省から地方公共団体へ要請を行った 「三層の対策」等の情報セキュリティの抜本的強化策の内容を反映
令和２年12月	「三層の対策」の効果や課題、新たな時代の要請を踏まえ、セキュリティの確保と効率性・利便性向上の 両立の観点から、情報セキュリティ対策の見直しを実施し、その内容を反映
令和４年３月	令和３年７月の「政府機関等の情報セキュリティ対策のための統一基準群」の改定や 地方公共団体のデジタル化の動向を踏まえた内容を反映

「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（平成27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

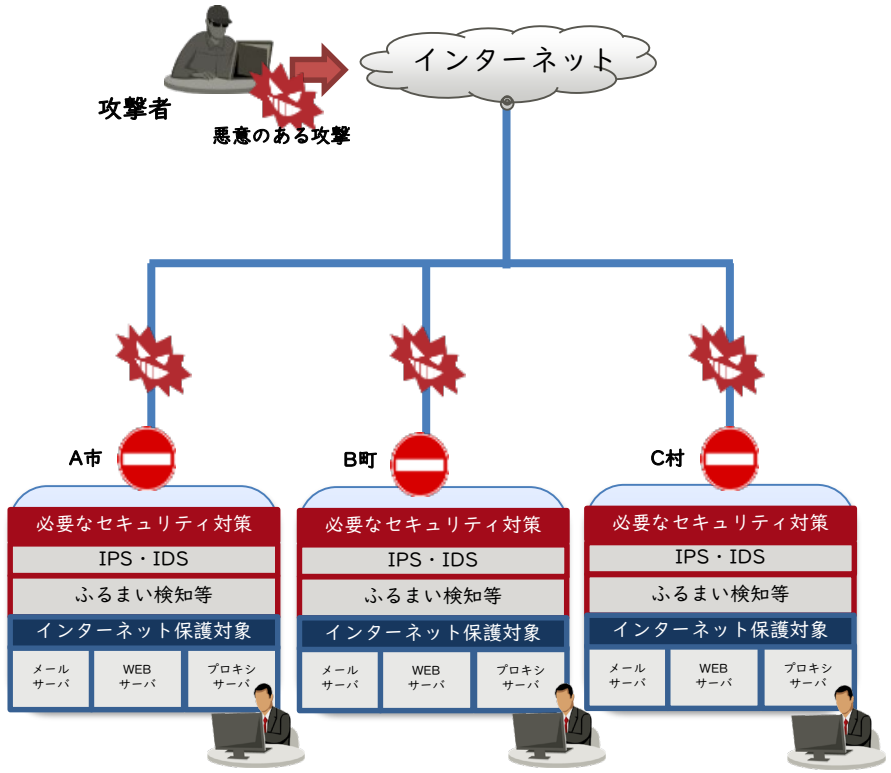
3 都道府県と市区町村が協力して、自治体情報セキュリティクラウドを構築し、高度なセキュリティ対策を実施

対策要請の経緯

H27.5　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
H27.11　検討チームより地方公共団体の対策内容（「三層の対策」）について報告
H27.12　総務大臣通知により地方公共団体に「三層の対策」を要請
H28.2　地方公共団体が「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）
H29.7　地方公共団体による「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

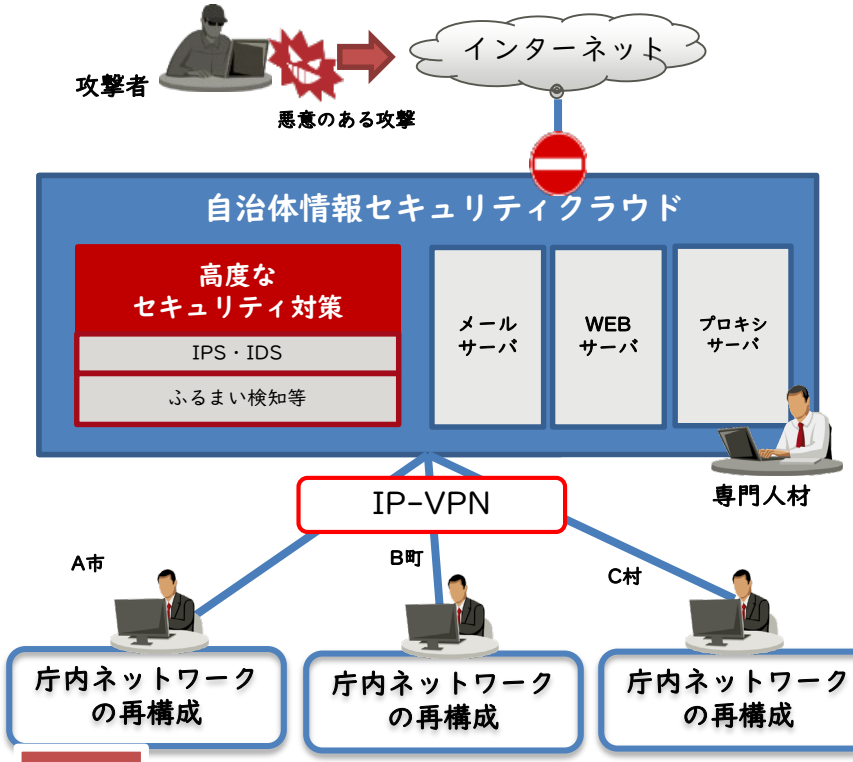


課題

- 各地方公共団体ごとに監視水準にバラツキがある
- 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
- プロキシログ等を分析するスキルを持った職員の不足
- 個々の地方公共団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（平成２９年７月～）
→令和３～４年度に多くの自治体が
次期自治体情報セキュリティクラウドに移行



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
- 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（eLTAX、マイナポータル）に限り、インターネット経由の申請等のデータのダウンロード（片方向）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、採用には追加の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記載

６．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

令和3年度のガイドライン改定の概要

ガイドライン改定の経緯

令和３年７月の「政府機関等の情報セキュリティ対策のための統一基準群」の改定及び地方公共団体におけるデジタル化の動向を踏まえ、令和４年３月に改定

➢ 主な改定ポイント

Ⅰ.業務委託・外部サービス利用時の情報資産の取扱い

- 業務委託・外部サービスを再定義した上で、取り扱う情報に応じて適切なセキュリティ対策の実施を記載
- 外部サービス利用時のライフサイクルに渡るセキュリティ要件や利用承認手続に関する規定を記載
- 今後のクラウドサービスの活用を見据えて、第三者認証制度や監査報告書をクラウドサービス選定の指標・基準等として、積極的に活用するよう記載を見直し

２.情報セキュリティ対策の動向を踏まえた記載の充実

- 不正プログラム対策製品やソフトウェア等を導入するだけではなく、監視体制やCSIRTとの連携等の組織的な対応が必要であること等を記載

３.多様な働き方を前提とした情報セキュリティ対策

- テレワーク実施場所等の運用面に関するセキュリティ対策を記載
- 支給以外の端末（BYOD）利用時の情報セキュリティ対策として、支給以外の端末に情報を保存させない対策や電子証明書等を用いて庁内ネットワークへ接続する端末を制限する対策を記載
- Web会議に関する対策を記載

４.マイナンバー利用事務系から外部接続先へのデータのアップロード

- 国が認めた特定通信（eLTAX、マイナポータル）に限り、必要な情報セキュリティ対策を徹底した上で、マイナンバー利用事務系から外部接続先へのデータのアップロード（双方向）を可能とするよう記載を見直し