サイバーセキュリティセミナー'25 in 東北

地方公共団体において求められる サイバーセキュリティについて

２０２５年１１月２７日

総務省地域情報化アドバイザー

情報セキュリティ大学院大学客員研究員

小田 信治

議題

01	地方公共団体のセキュリティにおける昨今のインシデント事例を踏まえた対策について
02	国の動向を踏まえた今後の対応について

自己紹介

＜現在の職務・所属等＞

- セキュリティ専門家として政府機関に勤務中（非常勤国家公務員）
- 総務省地域情報化アドバイザー
- 情報セキュリティ大学院大学客員研究員
- 東京都豊島区個人情報保護審議会委員
- 一般社団法人オープンガバメントコンソーシアム セキュリティ分科会主査

令和7年度：３団体支援
セキュリティポリシー改定（議会含む）等の支援

＜経歴＞大手ITベンダー所属

- 地方公共団体に対する情報システムの構築（住民情報システム、内部情報システム、ネットワーク等）
- 国の地方公共団体に対する情報システム、情報セキュリティ関連における施策立案等の支援業務
- 地方公共団体対する情報セキュリティコンサル業務

＜主な資格＞

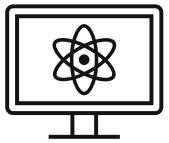
- 情報処理安全確保支援士（国家資格）
- CISSP (Certified Information System Security Professional)
- CCSP（Certified Cloud Security Professional)
- AWS Certified Solutions Architect - Professional
- AWS Certified Security - Specialty
- ITコーディネータ　等

総務省
- 「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」、「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」の執筆
  （平成30年9月版～令和5年3月版）
- 「地方公共団体におけるICT部門の業務継続計画（BCP）策定に関するガイドライン」の執筆（令和6年3月版）

1. 地方公共団体のセキュリティに関する昨今のインシデント事例を踏まえた対策について

地方公共団体におけるインシデント（１）

地方公共団体は、実際にサイバー攻撃の被害にあっているのか？



ランサムウェアの被害　「情報セキュリティ１０大脅威 ２０２５」１位

赤穂市教育委員会（兵庫県）	
発生日	２０２４年１２月２７日
概要	市教育員会のサーバがランサムウェアに感染し校務系システムに支障が出る事態になった。
影響	データ暗号化による業務停止、個人情報流出の痕跡は確認できていない。
備考	加東市教育委員会（兵庫県）においても学校関連のサーバや教職員のＰＣがランサムウェアに感染し、業務が停止した事例あり（２０２３年）。

（出展）https://www.city.ako.lg.jp/koushitsu/hishokouhou/documents/r6_news_report_252.pdf
（出展）https://www.kobe-np.co.jp/news/sougou/202305/0016407882.shtml

地方公共団体におけるインシデント（２）

地方公共団体は、実際にサイバー攻撃の被害にあっているのか？

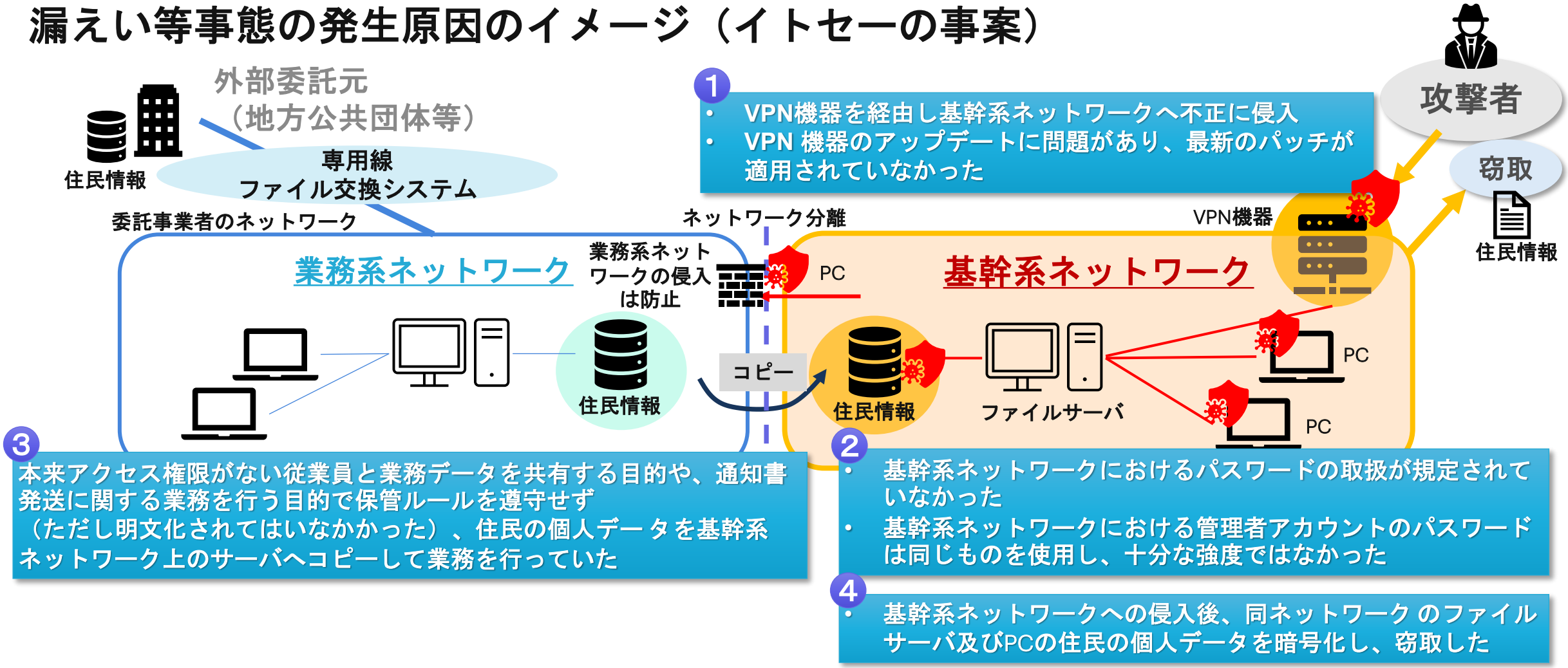
サプライチェーンや委託先を狙った攻撃　「情報セキュリティ１０大脅威 ２０２５」２位

和歌山市、豊田市、徳島県等の複数の地方公共団体	
発生日	２０２４年５月２６日
概要	地方公共団体の委託先（株式会社イトセー）のサーバがランサムウェアに感染した。
影響	委託元の住民情報が大量に漏えいした。 （和歌山市約１５万人　→委託元が契約期間過ぎても情報を廃棄していなかった） （個人情報保護委員会の発表によると行政機関等委託分５６６,５６１人が漏えい）
備考	２０２５年度においては、卒業アルバムを制作している事業者からの情報漏えい事案あり。

（出展）https://www.city.wakayama.wakayama.jp/_res/projects/default_project/_page_/001/058/774/070303.pdf
（出展）https://www.ppc.go.jp/files/pdf/250319_houdou.pdf
（出展）https://www.ishikura.co.jp/news/386

地方公共団体におけるインシデント（２）

漏えい等事態の発生原因のイメージ（イトセーの事案）



以下を参考に筆者が作成

（参考）個人情報保護委員会「株式会社イセトーに対する個人情報の保護に関する法律に基づく行政上の対応について」令和7年3月19日，
https://www.ppc.go.jp/files/pdf/250319_houdou.pdf

地方公共団体におけるインシデント（３）

地方公共団体は、実際にサイバー攻撃の被害にあっているのか？

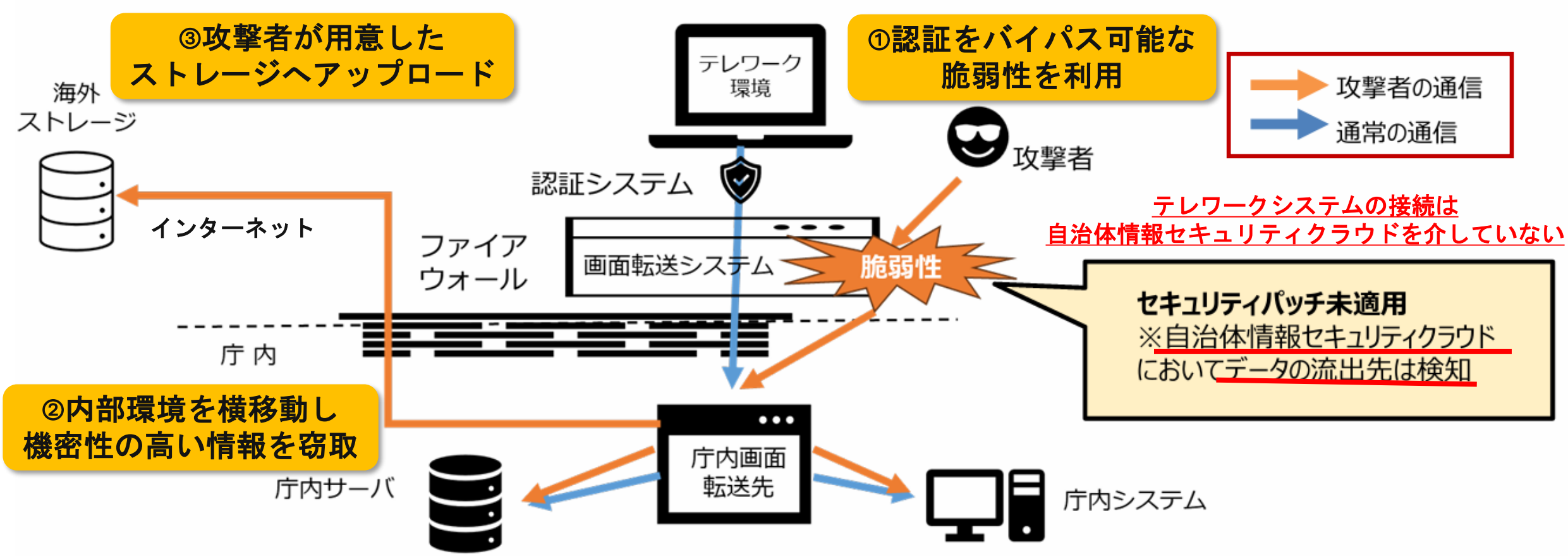
システムの脆弱性を突いた攻撃　「情報セキュリティ１０大脅威 ２０２５」３位

Ａ団体（団体名は未公表）	
発生日	２０２４年（日付は未公表）
概要	テレワークシステム（仮想デスクトップ（VDI）方式で庁内ネットワークに接続し業務を行うもの）が脆弱性を突く攻撃を受け、攻撃者が職員3名のアカウントになりすましてVDIにログインする不正アクセスが行われた。
影響	テレワークシステムのログに不正アクセス時に外部のオンラインストレージ等にアクセスしてデータのアップロードが行われた形跡があり、情報漏洩が発覚した。
備考	総務省の「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」において本事案が取り上げられ、対策について言及している。

（出展）https://www.soumu.go.jp/main_content/000992128.pdf

地方公共団体におけるインシデント（３）

システムの脆弱性を突いた攻撃のイメージ（Ａ団体）



（出展）総務省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16回),資料2,p2（一部加筆）
https://www.soumu.go.jp/main_sosiki/kenkyu/chiho_security_r03/02gyosei02_04000202.html

地方公共団体におけるインシデント（３）

不正アクセスによる被害（岡山県）（２０２５年１１月６日）

不正アクセスにより停止していた個別ホームページの再開等について（最終報）

不正アクセスにより公開を停止しておりました個別ホームページにて、下記のとおり安全に再開するための対応を講じた上で、再開等しましたのでお知らせいたします。
なお、調査結果概要は下記のとおりです。

記

１　不正アクセス事案の調査結果概要

・10月９日から13日にサーバー内のソフトウェアが攻撃され、マルウェアへの感染、７サイトのファイル改ざん（他サイトへの誘導コードの埋め込み）が確認された。
・不正アクセスを受けたサーバー内には個人情報は保有しておらず、個人情報の流出は確認されておりません。
・原因の特定には至っておりませんが、ソフトウェアの更新が徹底出来ていなかったことが、攻撃された一因と考えております。

２　安全に再開するための対応

・セキュリティ対策を総点検し、ソフトウェアの最新版へのアップデートの徹底等を再確認するとともに、セキュリティ対策の強化を行いました。
・不正アクセスの監視強化に加え、セキュリティ対策の定期確認を徹底します。
・岡山県警察に相談し、改ざんに関する捜査をお願いしています。

【参考】再開・閉鎖したホームページ

・晴れの国おかやまＰＲサイト（公聴広報課）
　https://8092-okayama.jp
・岡山　私のみらい発見カフェ（中山間・地域振興課）：イベント終了により閉鎖
　https://8092-okayama.jp/kansaimtg2025
・公共交通利用促進キャンペーン（交通政策課）
　https://8092-okayama.jp/public-transportation/2025
・こどもまんなかマナーアップ県民運動（子ども未来課）
　https://8092-okayama.jp/otasukemomosuke
・企業版子育て支援ポータルサイト　ハレまる。（子ども未来課）
　https://8092-okayama.jp/haremaru-portal
・ももっこアプリ利用促進キャンペーン（子ども未来課）
　https://8092-okayama.jp/momocco_campaign
・晴れ恋♡晴れ婚プロジェクト（縁むすび応援室）
　https://8092-okayama.jp/harekoi_harekon
・おかやま結婚応援パスポート（縁むすび応援室）
　https://8092-okayama.jp/kekkon_pp

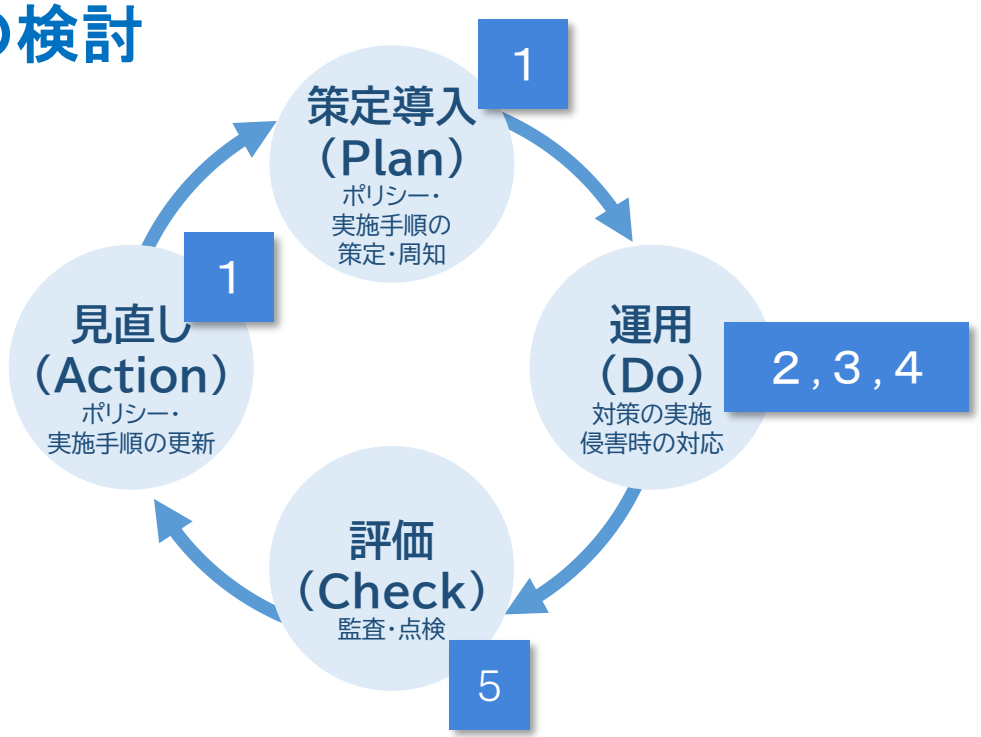
（出展）https://www.pref.okayama.jp/uploaded/life/1006527_9708920_misc.pdf

地方公共団体におけるインシデント事例からの考察

必要な対策とは何か

1. 規定の整備と明文化（定期的なセキュリティポリシーの改定）
2. 情報資産を把握し、保有する情報資産の脆弱性管理を徹底
3. 教育・訓練・啓発による人的な対策を実施
4. 委託先に関するセキュリティ要件を定め、遵守状況を確認
5. 情報セキュリティ監査による評価、改善の検討

情報セキュリティマネジメント（PDCA）サイクルにそった運用が重要



委託事業者の対する対応について

課題

1. 何をもって委託事業者を信頼すれば良いのか不明である
2. 要件が厳しいと委託事業を受託してもらえない
3. 必要なセキュリティ要件とは何かよくわからない

考えられる対応

1. ISMSやプライバシーマーク等は必須の要件

2. 住民情報を取扱う場合は、特に住民に対する説明責任が伴うため、委託事業者とコミュニケーションを十分に行う（委託事業者側も個人情報取扱事業者となり、法的責任が生じる）→共同調達も選択肢ではないか

3. 総務省から「外部委託先に関するセキュリティ要件のチェックシート」が発出されているので参考にする（契約時・契約期間中に委託事業者からチェックシートを提示させる）

ランサムウェアに対する対策について

今すぐ確認を実施！１１項目のチェック（総務省セキュリティポリシーガイドライン対策基準解説より筆者が作成）

項番	αモデルにおける確認項目（共通項目＋αモデルによる事前対策）	確認欄
1	自治体情報セキュリティクラウドを介してインターネットを利用しているか。また、ネットワークの分離や分割が正しく設定できているか。	□
2	導入している各機器やOS・ソフトウェア等の資産管理を行い、脆弱性に関する最新の情報を漏れなく収集しているか。収集した情報に基づき修正パッチの適用などを速やかに実施する仕組みとなっているか。	□
3	パスワードを第三者に推測されないようなものに設定し、システム・機器ごとに異なるものを設定されているか。また、デフォルト値での設定がされていないか。	□
4	ランサムウェアによる犯罪の手口とその対策に関する注意喚起と啓発を組織的に行っているか。	□
5	端末のOS からアクセスできないネットワークから切り離されたオフラインのディスクや媒体等へバックアップデータが保管されているか。	□
6	システムのバックアップが取得できているか。	□
7	バックアップから復旧可能なことや復旧手順を定期的に確認しているか。バックアップからの復元にあたってはランサムウェア感染前の復旧ポイントの特定手法や復元したバックアップにマルウェアが残存していないかの確認を復旧手順に含められているか。	□
8	必要の無い通信や不要サービスの設定がされていることはないか、各種設定の情報を確認できているか。	□
9	メールやファイル無害化の設定が正しく実施されているか定期的に確認しているか。また、無害化を行う機器やソフトウェアの脆弱性を速やかに修正されているか。	□
１０	端末におけるウイルス対策ソフトの導入と定義ファイルの更新、OS 等の修正プログラム等の更新がされているか。また、定義ファイルや修正プログラム等は速やかに更新が実施されているか。	□
１１	OS 等の権限において、最小権限の設定がされているか。	□

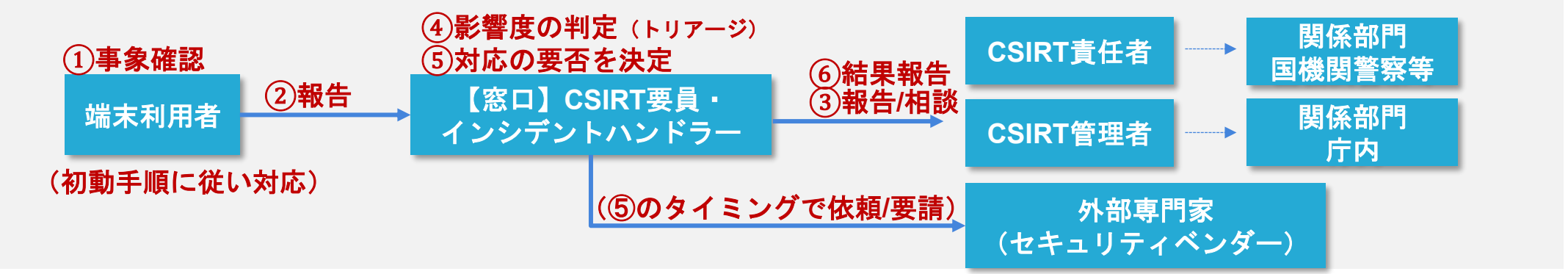
インシデント発生時の対応について

緊急時対応計画の内容（役割・フロー等）を確認し、定期的に訓練を行う

●対応例（主管課の端末がランサムウエアに感染した場合）

1. 主管部門の運用する端末にて、ランサムウェア感染により表示される脅迫文を確認
   （端末利用者はネットワークから端末の切り離しを実施、電源はオンのまま）

   初動対応は別途手順を用意し組織内に周知する
2. 端末利用者からCSIRTの連絡窓口へ事象を報告（連絡窓口を事前に共有しておく）
3. CSIRT要員又はインシデントハンドラーからCSIRT管理者へ事象を報告
4. CSIRT要員又はインシデントハンドラーは事実確認の実施の上、影響度を判定【トリアージ】
5. CSIRT要員又はインシデントハンドラーは、インシデントハンドリングを実施
   【対応方針の検討⇒証拠保全⇒封じ込め⇒根絶】
   ※本ケースではランサムウェア感染の原因や影響調査は外部専門家（セキュリティベンダー）へ依頼
6. CSIRT要員又はインシデントハンドラーからCSIRT管理者、CSIRT責任者へ対応結果を報告
   – （影響度に応じてCISOが住民等への報告を実施）



2. 国の動向を踏まえた今後の対応について

地方自治法の改正（第二百四十四条の六）令和８年４月１日施行

自治法上の基本方針の策定と公表が義務となる

（サイバーセキュリティを確保するための方針等）

1. 普通地方公共団体の議会及び長その他の執行機関は、それぞれその管理する情報システムの利用に当たつての**サイバーセキュリティを確保するための方針を定め、及びこれに基づき必要な措置を講じなければならない**。

「議会」、「地方公共団体の長」、「執行機関」が対象

2. 普通地方公共団体の議会及び長その他の執行機関は、前項の方針を定め、又はこれを変更したときは、遅滞なく、これを**公表しなければならない**。

令和８年４月までに「方針」の公表が義務化

3. 総務大臣は、普通地方公共団体に対し、第一項の方針（政令で定める執行機関が定めるものを除く。）の策定又は変更について、**指針を示すとともに、必要な助言を行う**ものとする。

総務省から「大臣指針（案）」が令和７年４月に発出済

4. 総務大臣は、前項の指針を定め、又は変更しようとするときは、国の関係行政機関の長に協議しなければならない。

総務省セキュリティポリシーガイドラインの改定

令和６年度に２回の改定が実施された（令和６年１０月と令和７年３月）

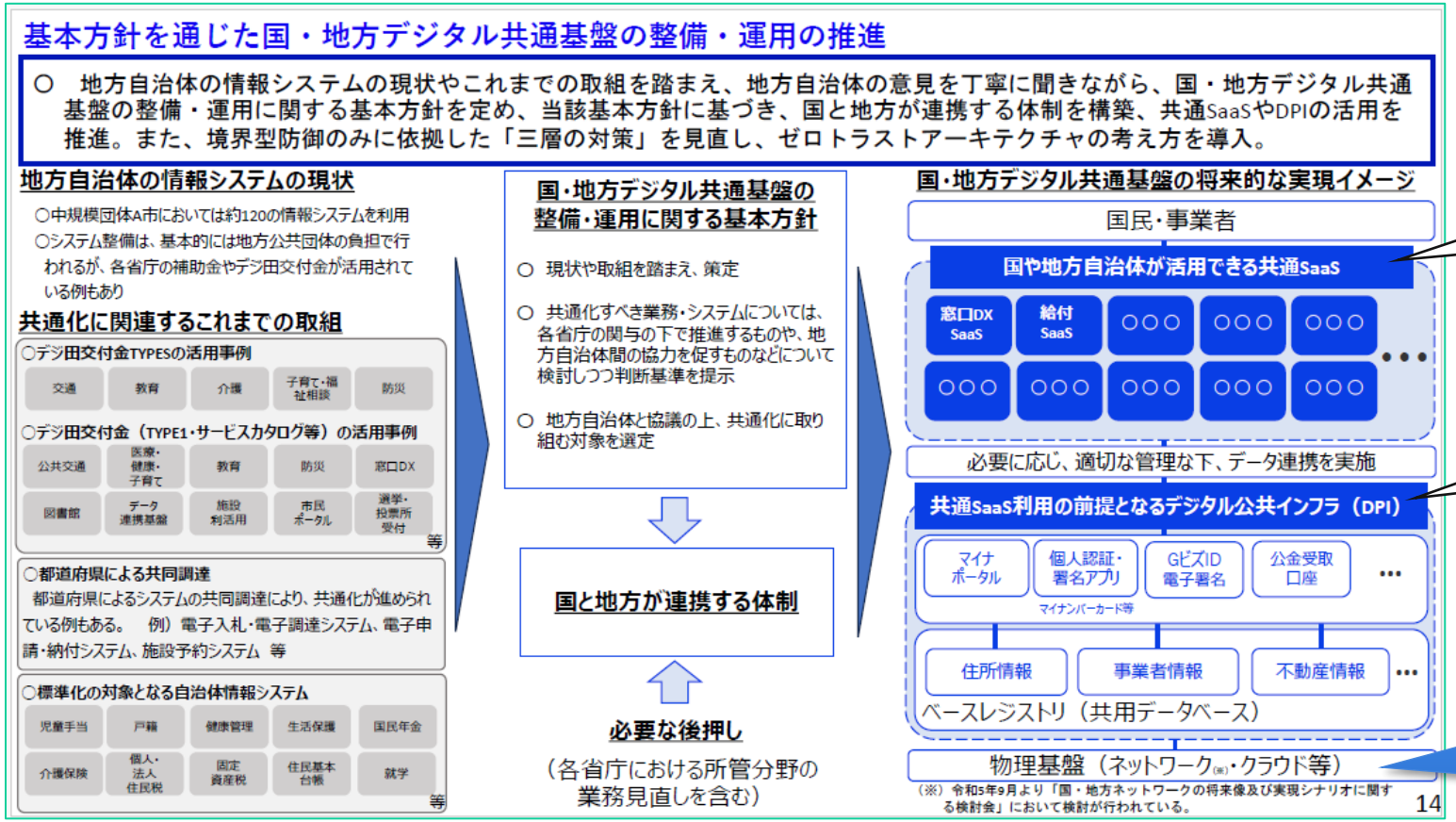
＜主な対策基準【例文】の改定内容＞ 令和６年１０月改定

- **情報資産の分類の見直し**
  - （対策基準２「情報資産の分類と管理」において、新たに自治体情報機密性３Ａ、自治体機密性３Ｂ、自治体機密性３Ｃという分類がされた）
- **外部委託に関する分類の見直し**
  - （対策基準８.２「情報システムに関する業務委託」が追加）
- **機器･ソフトウェア利用時の対策の強化**
  - （対策基準６.３（１）「機器等の調達に係る運用規程の整備」が追加、主にサプライチェーンリスクに関する事項）
- **サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化**
  - （対策基準６.技術的セキュリティの項目に「アクセス権限の最小権限の設定」「通信回線装置における適切なセキュリティ対策の実施」「監視機能の実装」等が追加）

対策基準【解説】のおいて、α'モデルが追加された。さらに、マイナンバー利用事務系における画面転送に関する内容やマイナンバー利用事務系における無線LANの利用に関する内容が追加された。

デジタル庁の各種政策

国・地方デジタル共通基盤の整備・運用
（「国・地方デジタル共通基盤の整備・運用に関する基本方針」）



アプリケーションレイヤ

システムの
共通化（SaaS）

プラットフォームレイヤ

Digital public
infrastructure

ネットワークレイヤ

**共用化された
ネットワーク基盤
２０３０年頃の国・地方
ネットワークの将来像**

（出展）デジタル行財政改革会議 第5回 資料1,p14 （一部加筆）
https://www.cas.go.jp/jp/seisaku/digital_gyozaikaikaku/kaigi5/kaigi5_siryou1.pdf

Ⅲ　2030年頃の国・地方ネットワークの将来像

2030年の姿

- 国民・住民に、**国・地方の行政サービスを、柔軟かつセキュア、安定的に提供可能**
- **国・地方のネットワーク基盤の共用化**が行われ、**ネットワークの効率性が向上**
- 国・地方の職員が、セキュリティを確保しつつ、**一人一台のPCで効率的に業務ができ、テレワーク等の柔軟な働き方が可能**

シンプルかつ柔軟なネットワーク

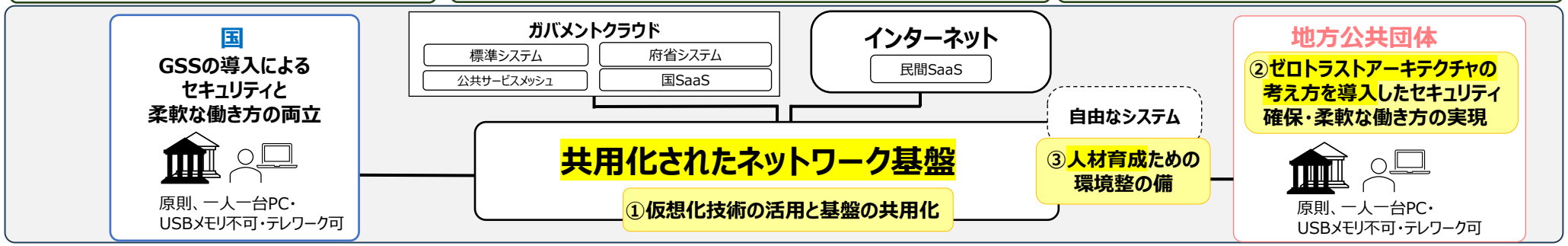
・**仮想化ネットワーク技術の活用**により、シンプルかつ柔軟なネットワークを構築

災害時のレジリエンスの確保

・大規模災害等にも対応し得る**強靭性・冗長性を確保**
（例：地上回線＋衛星回線の活用、国と地方ネットワークの相互運用等）

セキュリティの確保と利便性の向上

・強固なセキュリティ・柔軟なサービス構成には、**「ゼロトラストアーキテクチャ」の考え方が有効**



①仮想化技術の活用と基盤の共用化

- 国は、冗長化された共用可能な回線等を全国に整備し、仮想化技術を用い、柔軟で可用性の高い論理ネットワークを効果的・効率的に整備
- 国・地方での平時のコスト効率向上、レジリエンスの確保、地方の負担軽減のため、仮想化技術を活用しつつ、**国・地方の適切な役割分担の下、国が主体的に整備するネットワーク基盤の共用化**を検討（※）

（※）GSSが国の地方機関向けに全国に整備しているネットワークや拠点について、国・地方のネットワーク基盤としての活用を検討。
その際、新技術（Beyond5G等）の活用や費用負担の在り方等も検討

②ゼロトラストアーキテクチャの考え方の導入

- 国は、ゼロトラストアーキテクチャの考え方を導入したGSSに、原則移行し、柔軟な働き方とセキュリティの両立を実現。ユーザー数増加に対応するため、保守・運用体制を強化
- 地方のネットワーク上のシステムについて、**デジタル庁・総務省が調査・分析・検証を実施**（※）した上で、**ゼロトラストアーキテクチャの考え方に基づきセキュリティを強化**

（※）ゼロトラストアーキテクチャの考え方の導入に当たって必要な要件等の整理、概念実証（PoC）による技術面、運用管理体制面、コスト面等に係る課題の洗い出しとその解決策の検討などを実施予定

③人材育成のための環境整備

- 行政職員による基礎的なデジタル能力の修得、システムの構築・運用に必要な技術研鑽、官民の技術者・研究者との交流、革新的技術の創出等を実現できる、人材育成環境としての**「自由なシステム」**（※）を整備

（※）行政人材によって自律的に発達するデジタル人材育成サイクルを支える仕組みや実験用ネットワーク等。他のデジタル人材に係る施策とも連携して官民人材を発掘・育成

- LGWANが担っている重要情報のやり取りを行う機能(※)の在り方は引き続き検討　(※)マイナンバー制度による情報連携、J-アラート等
- 地方の強固なセキュリティ・さらなる利便性向上に向け、J-LIS・IPAによる共同研究・実証実験を推進
- ガバメントクラウド上のデータの保護のため、より一層低コストかつ安全な方法について、暗号技術を含む多角的な観点からの調査研究を実施

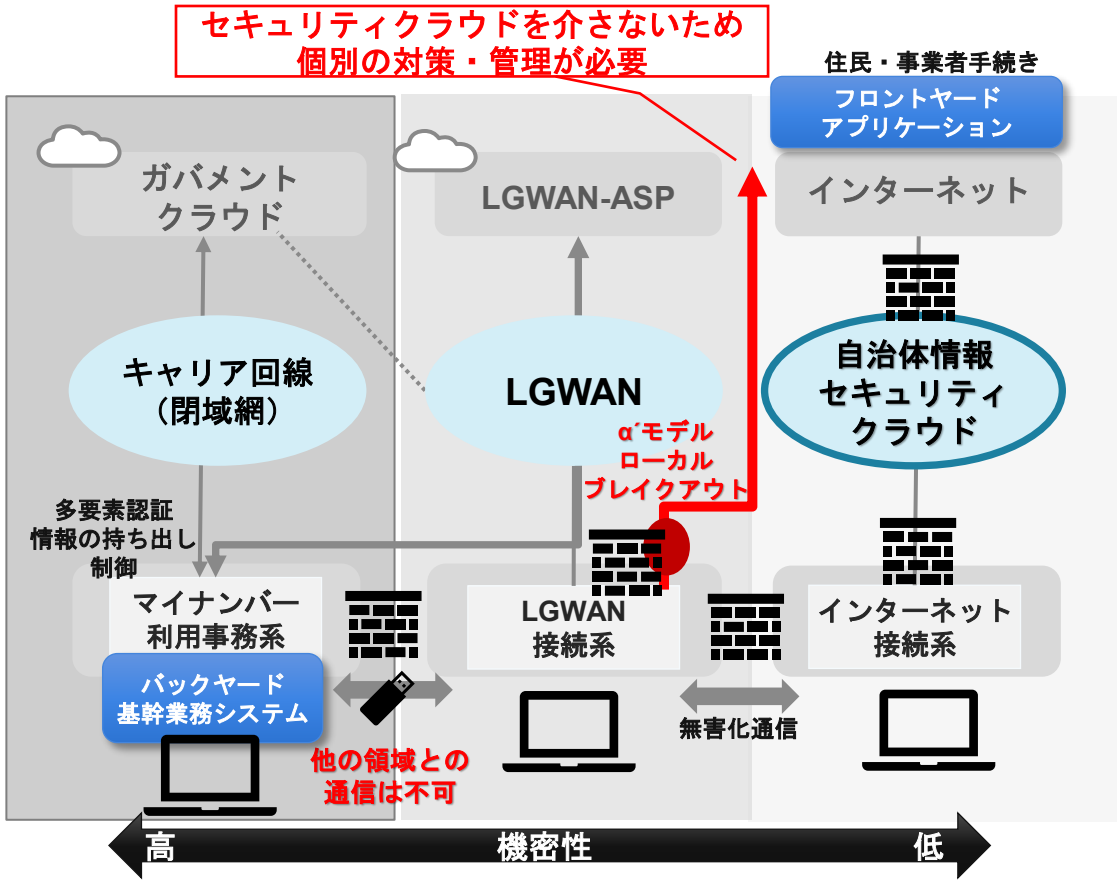
今後の進め方

- 本報告書について、地方の意見を丁寧に伺った上で、**可能なものから速やかに上記実証等を実施**
- 標準化に取り組む地方の負担やネットワーク更改時期等を考慮した上で、新たなネットワークへの移行は、**分散・段階的に実施**

三層の対策とゼロトラストアーキテクチャ（筆者の意見）

「三層の対策」は、マイナンバー利用事務系をインターネットからの脅威と情報漏えいを徹底的に防ぐための<u>リスク回避型アプローチ</u>

オンプレミスベースの情報システムを中心としたネットワーク・セキュリティの考え方



特徴

- 各領域単位でネットワーク回線を利用
- <u>「多層防御」と「境界型」セキュリティをベースとした分かり易い運用</u>
- マイナンバー利用事務系における確実なセキュリティを維持する手段

課題

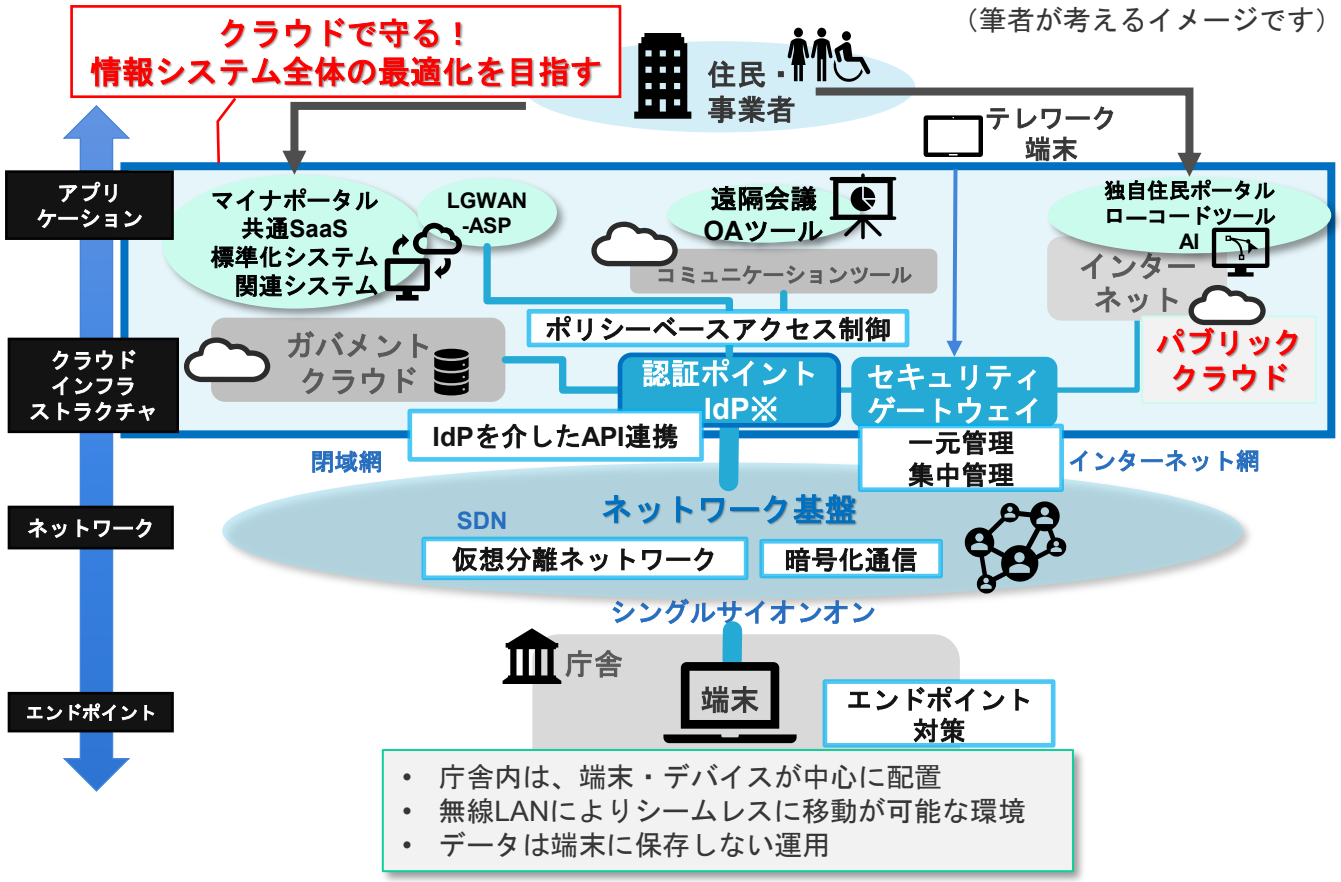
- ネットワーク領域を分離・分割しているため、<u>記憶媒体を利用したデータの受渡しが必要</u>であり、リアルタイムなデータ処理が出来ず、<u>住民へのタイムリーなサービスが困難</u>
- 各領域から<u>ブレイクアウト接続</u>する場合、接続ポイント単位でセキュリティ対策が必要となり、<u>一元的、集中的なセキュリティ対策が困難</u>。脆弱性のある接続点が有る場合、セキュリティ侵害が容易に行えるリスクが発生

三層の対策とゼロトラストアーキテクチャ（筆者の意見）

「ゼロトラストアーキテクチャ」は、ＤＸを推進するためクラウドテクノロジーを駆使したリスク低減型アプローチ

クラウドの利活用を中心としたネットワーク・セキュリティの考え方

一般的なゼロトラストアーキテクチャのイメージをベースに地方公共団体の構成をマッピング
（筆者が考えるイメージです）



※Identify Provider（IDプロバイダー）

特徴

- クラウドテクノロジーによりセキュリティを一元管理し運用を効率化
- 業務システムをクラウドで運用することで、より効果が発揮
- 認証ポイントを介してセキュアかつシームレスなデータ連携を実現し、DXの推進に寄与

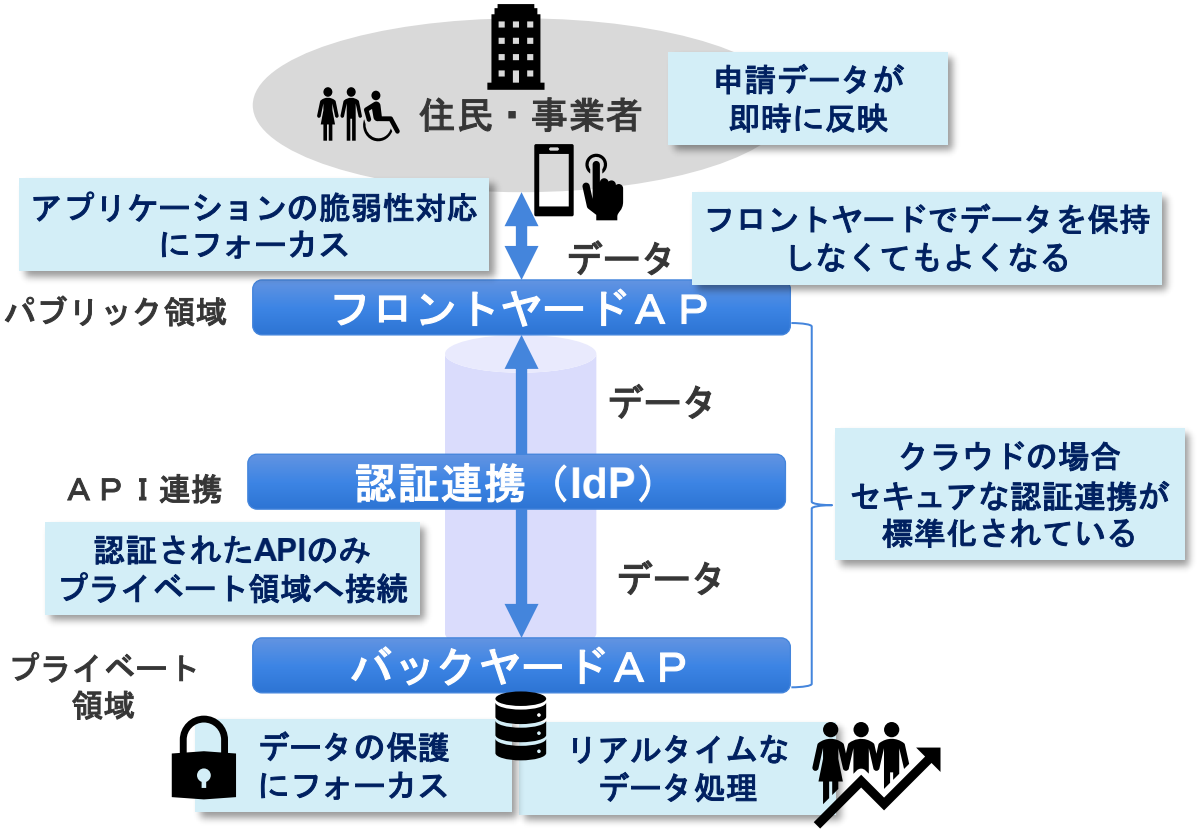
課題

- 業務システムがオンプレミスベースのものとクラウドサービスのものと混在した場合、各々のセキュリティ対策が必要
- 正規ユーザのIDやパスワードを利用され不正アクセスされるケースを想定し、クライアント証明書を利用した認証や生体認証※※等の不正アクセス対策が重要

※※WebAuthn（公開鍵暗号方式を基盤としFIDO2対応等の生体認証と連携してパスワードを使用せずに安全な認証を実現するための技術）

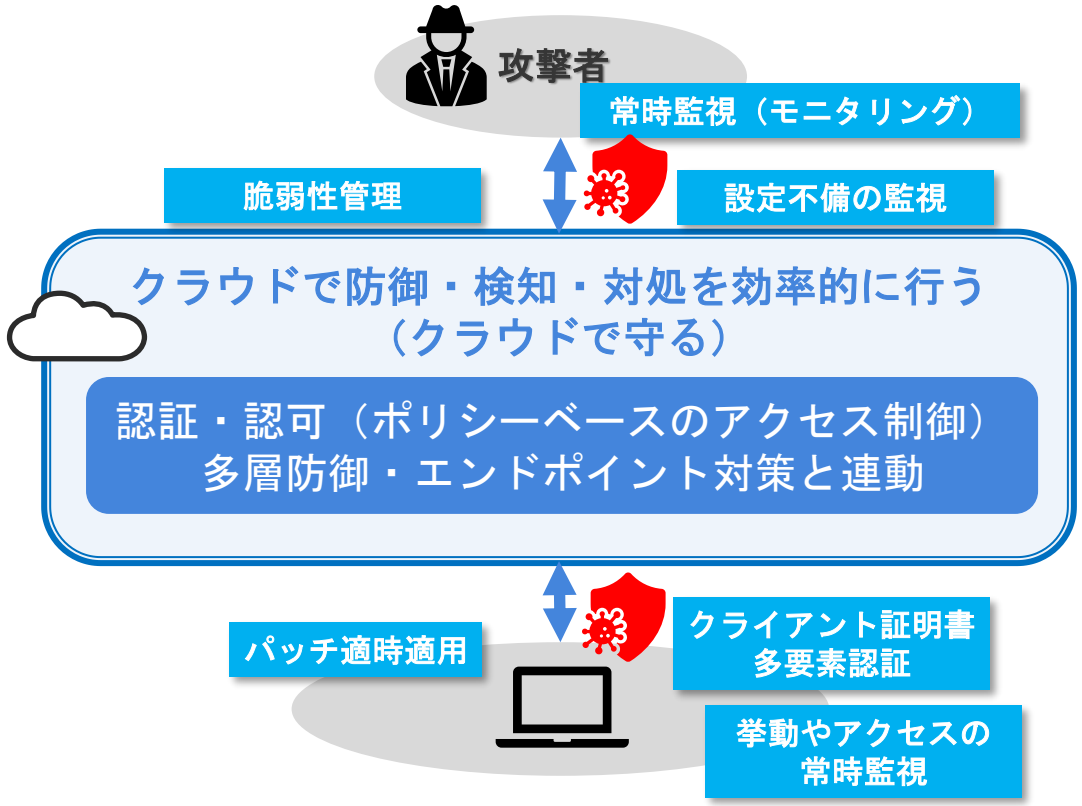
ゼロトラストアーキテクチャの利点

① フロントヤード（住民ポータル）とバックヤード（住民情報系システム）との<u>シームレスなデータ連携を実現</u>し、DXの推進につながる。



業務システム間が
ＡＰＩによってセキュアに連携

② クラウドテクノロジーを活用することで、<u>一元的かつ集中的にセキュリティをコントロール</u>することが出来、セキュリティを高めるとともに、情報システム全体の最適化を促進する。



リモートからの不正アクセス
内部からの不正アクセス等を検知・ブロック

ゼロトラストアーキテクチャの採用における重要となるポイント

セキュアなデータ連携やAPI連携を行うには、**アクセス制御ポリシーの設計**が重要であり、技術的な知見が必要となる。

リスク低減型アプローチであるため、CSIRTにおける対応や職員のリテラシー等、**組織的・人的対策**も重要となる。

三層の対策とはセキュリティの概念が異なるので、**目的（DXの推進・情報システム全体の最適化）を明確**にした上で、手段としてゼロトラストアーキテクチャを採用し、その**具体的な実装方法を正確に理解**することが必要となる。

ゼロトラストアーキテクチャはクラウドテクノロジーを軸としているため、**業務システムをクラウド化**することでより効果が発揮（クラウドで一元管理）する。

今後の進め方

国の動向を注視する（正確な情報を収集）

⇒ **地域情報化アドバイザーの活用**（県や広域での情報共有を）

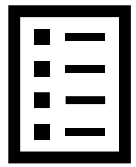
（αモデルからゼロトラストアーキテクチャへの移行は、国から示されるのか）

（α´モデルやβ´モデルにおいて部分的なポリシーベースのアクセス制御を実装し様子を見る）

DX計画と整合したクラウド戦略を検討する（情報システム全体の最適化）

⇒ 国のドキュメントは、各省庁・担当別に発出される

自組織の状況に合わせて**全体計画を取り纏める**

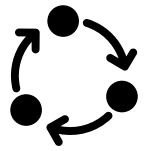


セキュリティの基本を徹底的に実践し、組織に浸透させる

⇒ ゼロトラストアーキテクチャ製品やソリューションの検討の前に

「基本」が出来ているのか振り返る

まずは、**情報セキュリティマネジメントの確立！**を



ご清聴ありがとうございました

＜総務省地域アドバイザー＞

地域情報化アドバイザー | 地域情報化アドバイザーを活用しよう！
https://www.r-ict-advisor.jp/