資料２

第22回　地方公共団体における情報セキュリティポリシーガイドラインの改定等に係る検討会

令和7年度
国・地方ネットワークの将来像の実現に向けた検証事業

2026/6/8　　デジタル庁　省庁業務サービスグループ／デジタル社会共通機能グループ　国・地方ネットワーク班

デジタル庁
Digital Agency

令和７年度 国・地方ネットワークの将来像の実現に向けた検証事業

令和７年度　国・地方ネットワークの将来像の実現に向けた検証事業　概要①

背景

現行の地方の行政ネットワークの課題解消に向け、「国・地方ネットワークの将来像及び実現シナリオに関する検討会報告書」(令和６年５月31日公表) 及び「デジタル社会の実現に向けた重点計画」(令和７年６月13日閣議決定) に基づき、以下(1)(2)の２つの検証・検討を実施。

検証観点・検証方式

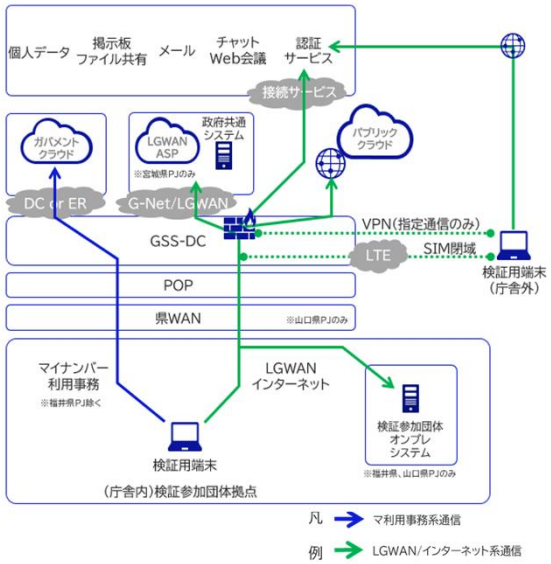
(1)既存の国のGSS環境を一括のパッケージで自治体において試用する検証
(GSS試用型検証)

○ 国が整備・運用するGSS（ガバメントソリューションサービス）は高セキュリティ、高品質、低遅延等を実現。

○ GSS環境*を自治体で試用し、実現性、業務利便性や運用負荷を含めた導入効果等の観点を検証。

※ オフィスソフトウェア、コミュニケーションツール、ネットワークや業務用PC端末、セキュリティ対策等を含めた標準的な業務実施環境

R7年度 GSS試用型検証（イメージ）



(2) 自治体内のネットワーク上のシステムにゼロトラストアーキテクチャの考え方を導入する際の効果や課題等を検証 (自治体提案型検証)

○ 自治体の提案する方法に基づき、自治体内のネットワーク上のシステムにゼロトラストアーキテクチャの考え方の導入ができるか検証。

○ 各自治体に応じて対策すべきと考えているセキュリティ上のリスク・脅威やクラウド利用の程度等の将来像が異なるため、それらに応じたリスク対策方針をもとに検証環境を構築。その上で、業務利便性、セキュリティ対策レベルの向上具合、コスト等の観点を検証。

R7年度 検証事業（イメージ）

令和７年度　国・地方ネットワークの将来像の実現に向けた検証事業　概要②

(1) 既存の基盤として、国の業務実施環境を一括パッケージで自治体において試用して検証 (GSS試用型検証)

プロジェクト	検証内容	R7検証環境における検証結果
共通検証	• **将来的に職員数減になることを見据え、庁舎外（テレワークなど）からのリモート接続やBYOD端末（スマホ・タブレット）からの業務実施可否を確認** • 一人一台のGSS端末での業務利用において、**マイナンバー情報等機微な情報に対する情報漏洩対策の確認** • 不正アクセスに対するアカウントや閉域SIMの無効化、端末紛失に対するリモートワイプ等、**障害時におけるGSSの機能性の確認** **※ ID管理や端末監視等は、既存のGSS運用体制の中で実施**	• **場所を問わない働き方の実現・業務利便性の向上に資する** • 自治体に求められるゼロトラストセキュリティ機能は網羅。マイナンバー系とLGWAN・インターネット系の**論理分離で現行業務の実施は可能**。ただし、**機微な情報に対する情報漏洩対策は一定程度有効であるものの、その検知精度に懸念** • アカウントや閉域SIMの無効化、端末紛失に対するリモートワイプ等、**障害時対応は可能** **※ 対象となるIDや端末は30程度**
宮城県（代表） 名取市	• 東日本大震災の経験をもとに、**大規模災害における様々なシナリオ**（専用線・モバイル網がともに利用できなくなり、衛星回線経由で通信するケース等）**を想定した業務環境を確保できるか確認** • GSSに移行するにあたっての過渡期対応として、GSS G-Netを経由したLGWAN-ASPへの接続検証	• **統一的な業務実施環境により、災害時の相互運用性が確保** • **衛星回線の利用は屋上での電源環境が準備できず検証できなかった**が、モバイルルーター経由では接続可能。ただし、自治体において事前にLANケーブルや電源の敷設等、**衛星機器設備の設置場所の調査・確保が不可欠** • GSS G-Net経由でLGWAN-ASPサービスを問題なく利用可能
福井県（代表） 鯖江市 高浜町	• **現在オンプレミス環境の地場ソフトフェア**（建シリーズ）がガバクラ上に構築されていく将来を見据え、GSS環境においてアプリ審査を経たうえで**導入可否を検証**（利用者はGSS端末にインストール；サーバーはガバクラ上で構築） • 検証事業者として地元企業（江守情報）が参画し、自治体業務における利用検証を支援	• アプリ審査の過程において、**脆弱性が指摘された**。他方、**審査側の運用体制と審査に係る所要期間に懸念** • **運用体制が一元化されることにより、検証環境構築時の接続不備解消に時間を要した**ことから、障害時の原因切り分け・復旧対応の煩雑化に懸念
山口県（代表） 岩国市	• **GSS NWに移行した場合における県WAN**（やまぐち情報スーパーネットワーク(YSN)）**の必要性を検証** • 自治体ではオンプレミス環境下にあるシステムが未だ多く存在することから、**GSS NWからLGWAN・インターネット接続系を経由したオンプレミス環境下にあるシステムへの接続検証**、及び従来の三層の対策において物理分離されていた業務を一台端末で実施可能か検証	• 県域でのコスト最適化・運用一元化、トラフィック分散等の観点から、各自治体による直接接続ではなく**県WAN経由による接続が有用** • **GSS NWからオンプレミス環境下にあるシステムへは接続可能**であり、従来の三層の対策において物理分離されていた環境へ一台端末でアクセス可能

令和７年度　国・地方ネットワークの将来像の実現に向けた検証事業　概要③

(2) 自治体の提案する方法に基づき、自治体へのゼロトラストアーキテクチャの考え方の導入を検証 (自治体提案型検証)

プロジェクト	検証内容	R7検証環境における検証結果
北海道（代表） 室蘭市、登別市、石狩市、栗山町、鷹栖町、洞爺湖町、音更町	【リモートブラウザ分離(RBI)ベースのゼロトラスト環境の導入の実現性】 ・スマート北海道（Prisma Access等をベースとしたゼロトラスト環境）を構築し検証 ・インターネット接続系においても、従来のVDI（仮想デスクトップ環境）ではなく**導入コストが比較的安価なRBI（web閲覧の隔離）によるリモートアクセス**を検証	・スマート北海道によるゼロトラスト環境の構築は**技術的に可能** ・**ただし、マイナンバー情報等機微な情報に対する情報漏洩対策の検知精度に課題あり** ・**リソースの現状把握が不十分な団体や、専門人材の確保等の運用体制に対する懸念**
岐阜県坂祝町（代表） 愛知県名古屋市 愛知県長久手市	【一般的なセキュリティソリューションを利用した接続】 ・**民間企業でも利用されている一般的なサービス（Zscaler等）を用いる形で、職員の運用負担に配慮したシステム構成にて検証**	・**現行以上のセキュリティレベルを技術的には確保することが可能** ・単独自治体で運用する場合、**情報システム担当職員の負荷増加を懸念**
福岡県北九州市（代表） 山口県下関市 福岡県大牟田市	【オンプレミス環境が残存することを前提とした段階的移行のあり方】 ・北九州市が独自に提唱している「次世代自治体デジタル共通基盤（LGSS）」において、仮想化共用ネットワーク基盤等を構築し検証 ・**Cisco Secure Accessを活用したゼロトラスト環境を構築しつつ、マイナンバー利用事務系については、既存の境界型防御を活用して検証**	・**仮想端末を介しての接続が解消されるとともに、端末切替えの手間が軽減され、業務利便性が向上** ・現行システムごとに分散しているID管理を見直し、ID管理のモダン化を図る上で、**ID管理やセキュリティ監視等の運用においては専門知識が必要**
鹿児島県肝付町（代表） 北海道札幌市 京都府舞鶴市 和歌山県すさみ町	【Google製品を利用したゼロトラスト環境の導入の実現性】 ・肝付町モデル（Chrome Enterprise等をベースとしたゼロトラスト環境）を参考に、**Google Workspaceを基本業務環境としてゼロトラストアーキテクチャの考え方を導入できるか検証** ・既存システムを疑似的にモダン化するサービス（Cameyo）を活用 ・既存システムからの移行フェーズに着目し、現状のセキュリティレベルが異なる自治体への横展開・運用の課題を検証	・自治体規模や導入フェーズを問わず技術的には導入可能 ・**専門人材も含めた運用体制の差**が横展開を阻害するため、支援体制の構築が必要 ・コスト構造が機器購入からサービス利用にシフトするため、**為替変動や物価上昇による将来的なライセンス費用の高騰への懸念**

検証参加プロジェクトの意見

(1)既存の国の業務実施環境を一括のパッケージで自治体において試用する検証（GSS試用型検証）

導入により期待される効果

業務利便性の向上

・コミュニケーションツールの統一化による、他自治体はじめ外部機関との円滑な情報共有
・情報共有・文書管理ツールの統一化による、円滑なファイル共有や共同作業の迅速化
・仮想化技術やクラウドの活用による、場所を選ばない働き方の実現

災害時のレジリエンス確保

・統一的な基盤、通信・認証方式による災害時の相互運用性の確保（他自治体職員による即時の業務参加・応援体制の立上げ、切れ目のない住民支援が期待）
・避難所や自宅等の庁舎外から安全に業務継続ができ、行政機能を維持することが期待

セキュリティ対策への有効性

・全国一律のセキュリティ対策による、セキュリティ水準の平準化・高度化
・セキュリティの維持や管理等ができる高度なITインフラ人材の確保、人件費軽減

懸念・課題

導入に向けた全般的な懸念・課題

・一律で設定されるセキュリティ基準に適合するための既存導入アプリの対応
・情報共有・文書管理ツールの編集権限等、事前の運用ルールの検討
・現行の自治体セキュリティクラウド要件の要否と代替可能性の検討
※　庁舎外からマイナンバー利用事務系への接続可否に関する意見は二分
（セキュリティ上、庁舎外からは接続すべきでない⇔
テレワーク需要や災害時対策として庁舎外からも接続できるようにすべき）

自治体業務・環境の特殊性

・窓口業務で必要となる既存の共用端末・専用端末の取扱いの検討
・既存の旧来システムや特定クライアント依存アプリの取扱いの検討
・市域の狭さや業務拠点の少なさによる、リモートワーク・テレワークへの需要の差と、それに伴う庁舎外からのネットワーク構成やBYOD端末*の対応の検討

*業務利用を認める私物端末

運用体制・コスト

・運用体制の一元化により、個々の自治体が把握できる情報が限定されることによる障害復旧対応の煩雑化
・障害発生時における共用基盤の運用主体と自治体間の役割分担の明確化や、対応フローの検討
・導入・運用コストに対する懸念（国が導入を主導した場合、国が導入・運用コストを負担すべき、という意見も存在）

(2) 自治体内のネットワーク上のシステムにゼロトラストアーキテクチャの考え方を導入する際の効果や課題等を検証 (自治体提案型検証)

導入により期待される効果

セキュリティの高度化

・標的型攻撃等による内部ネットワークでの感染拡大や、外部への不正送信による情報窃盗等、近年頻発している脅威に対するリスク軽減
・端末の窃盗や不正接続によるリスクの抑止・低減

業務利便性の向上

・セキュアな状態で出張窓口を開設したり、庁舎外において業務を完結させることが可能になり、移動時間の削減等が期待
・VDI接続や複数回のログイン等が不要となり、端末切替の煩雑さが改善することによる業務効率化
・ファイル転送等が不要となり、円滑なデータ連携が可能
・クラウドの活用が促進され、業務効率化や、災害やインシデント発生時の業務継続性の向上に寄与

懸念・課題

導入に向けた全般的な懸念・課題

・導入に向けた自治体職員のセキュリティに対する意識醸成・変革の必要性（変化を望まない管理職層や、 DX推進部門と対面業務が主体の現場部門との意識の差が存在）
・ID管理、IT資産管理が部局・業務ごとに分かれ、各システムの担当者が個別に設定を行っており、一元的な把握や取組の実施が困難

※ 三層の対策の見直しに賛同する意見もある一方で、マイナンバー利用事務系の今後の取扱いについては意見が二分
（１つのネットワークに統合しないと業務利便性が十分に向上しない⇔
実機検証において情報漏洩防止機能では十分に特定個人情報の漏洩防止ができない等の懸念があり、マイナンバー利用事務系は分離しておくべき）

運用体制・コスト

・サイバー攻撃やテクノロジーの最新化を踏まえたポリシー設定の見直しやログ監視分析等、専門的な運用作業に対応できる専門人材の不足
・高度なセキュリティ対策であるため導入コストへの懸念（財政措置等の検討を求める意見が存在）
・為替変動や物価上昇に伴う、将来的なライセンス料・サービス利用料の高騰への懸念

ゼロトラストアーキテクチャの考え方の導入の必要性

ゼロトラストアーキテクチャの考え方の導入の必要性

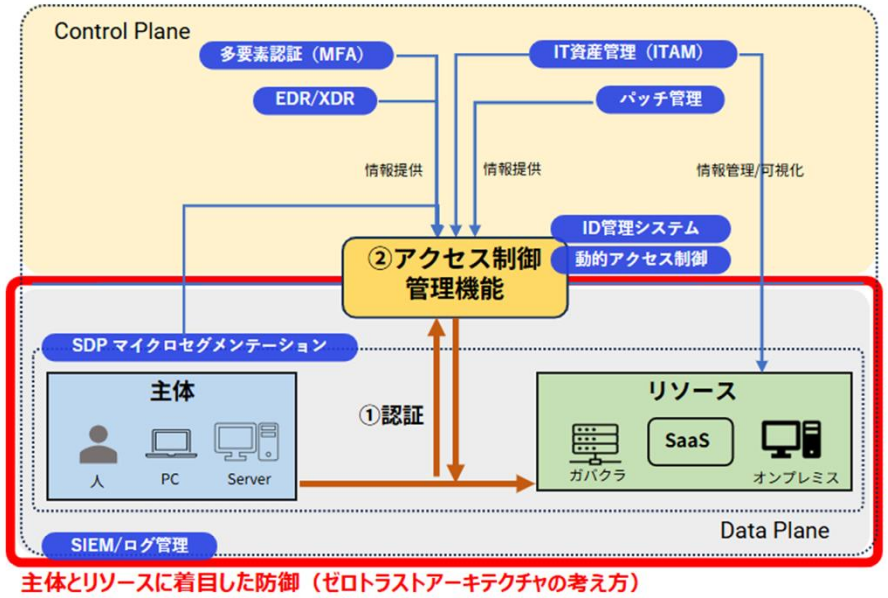
近年のセキュリティ動向や自治体の現状

- 近年のランサムウェア攻撃に至る高度なサイバー攻撃の増加
- 自治体におけるリモートワーク・テレワークの普及やクラウドサービス利用の促進

境界型防御のみに依拠しない、**ゼロトラストアーキテクチャの考え方の導入**が必要

ゼロトラストアーキテクチャは、境界だけに依存せず、ネットワーク内外を問わず全てのアクセスを適切に制御する考え方

➡ ゼロトラストアーキテクチャの考え方の導入により、より高いセキュリティと柔軟な働き方の両立を実現できる



主体とリソースに着目した防御（ゼロトラストアーキテクチャの考え方）

庁舎内外等の場所にとらわれず、以下①②により、庁舎内外の主体やリソースを守る動的な制御
① 主体がリソースにアクセスする際に都度認証
② 認証をするために必要なルールを事前に定める

（NIST SP800-207、ゼロトラストアーキテクチャ適用方針を参考にデジタル庁にて作成）

自治体におけるゼロトラストアーキテクチャの考え方の導入にあたって

令和７年度の検証事業において確認されたこと

- 各自治体においてIDやIT資産管理の状況は千差万別であるが、自治体内において、その把握が十分に行えていない状況
- 自治体によって、想定する将来的に実現したい働き方の像や、対策すべきセキュリティ上のリスク・脅威、及びそれに伴い備えるべきセキュリティ要件も異なるところ、各自治体において、そのような現状分析が十分に行えていない状況
- 自治体においてはゼロトラストアーキテクチャの考え方に関する知見が不足しており、自治体職員のセキュリティに対する意識醸成・意識変革が必要な状況

自治体がゼロトラストアーキテクチャの考え方を導入するにあたっては、まずは以下４点を必要最低限の要素としていくべきではないか

Identity（ID・認証管理）	職員がシステムを利用する際には、多要素認証（MFA）を必須とするとともに、管理者権限を持つ特権IDについては、作成、変更、停止、廃止まで含めて厳格にライフサイクルを管理する。
Device（端末管理）	全ての業務用端末を一元的に管理し、セキュリティ更新プログラムの適用、端末内データの暗号化、必要な設定の統一化を自動的に実施できるようにする。
Validation（検証・有効性評価）	アクセス要求の都度、IdentityやDeviceの状態に基づき、利用者本人であることや利用端末の安全性等を確認し、その操作が事前に定義されたポリシーに適合しているかを動的に判定する。 その際、一度認証された利用者に対して永続的な権限を与え続けるのではなく、業務上必要な情報や機能に限定してアクセスを認めること（最小権限の原則）に基づき、都度必要なリソースのみに許可する仕組みを維持する。
Telemetry（ログ・事跡管理）	当初から高度な分析を前提とするのではなく、まずは有事の際に「誰が、いつ、何を行ったか」を確認し、説明できるよう、必要な記録を保全・集約できる状態を確保する。

今後の進め方

令和８年度（2026年度）～

国・地方ネットワークの将来像の実現に向けた検証事業　2.0億円　（令和７年度補正予算）

○ **GSS環境のうちネットワーク基盤のみを対象とした共用化も含め、その対象範囲や技術的な実現可能性、効率的な導入方法等について更なる分析・検討**

①基盤の共用化の対象範囲の検討

・GSSネットワーク基盤のみの共用化に関する技術面等の実現可能性の検証

・候補となる実現案の機能・コスト・運用体制・自治体メリット等の比較検討

②GSS環境への移行の実現可能性や移行に向けた、更なる検討

移行に向けた自治体の現行環境の調査や移行プロセスを通じた課題の洗い出しや移行モデル・スケジュールの検討

○ **自治体におけるゼロトラストアーキテクチャの考え方の導入に向けた、更なる検討**

自治体が円滑に導入できるよう、情報資産等の現状把握の方法も含めたポリシー設定や調達仕様書作成の参考となる参照手順書案の作成

【参考】以下の点についても取り組んでいく必要がある。

・「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」の改定の検討

（検証自治体から出た課題例）インターネット接続と分離に関する要件の緩和、無害化処理の義務付けの緩和、持ち出し端末に関する手続における例外措置の創設　等

・ゼロトラスト基盤の共同調達・共同運用等、効率的な運用方法やコスト負担のあり方に関する検討

令和９年度（2027年度）～

○ 将来像案の具体化、自治体への意見照会

○ 将来像の実現に向けた環境整備

令和12年度（2030年度）～

○ 将来像への移行開始

参考資料

【参考】ゼロトラストアーキテクチャに関連するサイバーセキュリティ関連文書

No.	文書名	発行主体	概要
1	DS-210 ゼロトラストアーキテクチャ適用方針	デジタル庁	ゼロトラストアーキテクチャを適用するための基本方針及び導入時の留意事項
2	デジタル社会推進標準ガイドライン群	デジタル庁	サービス・業務改革並びにこれらに伴う政府情報システムの整備及び管理についての手続・手順や、各種技術標準等に関する共通ルールや参考ドキュメントをまとめたガイドライン群 ※上記DS-210も本ガイドライン群に含まれる
3	NIST SP 800-207 Zero Trust Architecture	NIST （米国国立標準技術研究所）	ゼロトラストアーキテクチャの基本概念と構成要素を示した文書
4	NIST SP 1800-35 Implementing a Zero Trust Architecture	NIST	NIST SP 800-207を踏まえて、ゼロトラストアーキテクチャの具体的な実装方法、ユースケース、ベストプラクティス等を示した実践ガイド
5	①JIS Q 27001/27002 ②JIS Q 27017	JIS （日本産業規格）	①JIS Q 27001は、組織が情報セキュリティを体系的に管理するために満たすべき要求事項を定め、JIS Q 27002は、当該要求事項を実現するための具体的な管理策の選択・実装・運用に関する指針を示した規格であり、両者は相互に補完関係にある ②クラウドサービスを利用・提供する場合に必要となる、クラウド向けの情報セキュリティ管理策を示した規格
6	①NIST SP 800-53 Rev.5 ②NIST SP 800-53B	NIST	①組織及び情報システムに適用し得るセキュリティ及びプライバシー管理策を体系的に示した文書 ②①に記載された管理策を前提に、情報システムや組織の特性に応じて参照すべき管理策のベースラインを示した文書
7	Cybersecurity Framework（CSF）2.0	NIST	組織がサイバーセキュリティ対策を整理し、リスク管理の優先順位を定めるために参照すべき共通的な指針
8	CIS Critical Security Controls for Effective Cyber Defense	CIS （米国インターネット・セキュリティ・センター）	組織が代表的なサイバー攻撃に対処するに当たって 、優先的に実施すべき実務上有効なセキュリティ対策を示した文書
9	Zero Trust Maturity Model v2	CISA （米国サイバーセキュリティ・社会基盤安全保障庁）	ゼロトラストに移行する際に参照できるロードマップの一つであり、成熟度段階に沿って移行を進めるための参照モデル
10	Zero Trust Implementation Guidelines	NSA （米国国家安全保障局）	ゼロトラストの実装を促進するための具体的かつ段階的な実行指針
11	NIST Special Publication 800-37 Revision 2	NIST	情報システム及び組織における、セキュリティ及びプライバシーのリスクを管理するための、統制がとれ、構造化された、柔軟なプロセスを提供するリスクマネジメントフレームワーク（RMF）を解説
12	NIST Cybersecurity White Paper NIST CSWP 20	NIST	ゼロトラスト移行に必要な計画・役割・検討観点を 上記No.11において解説されているRMF工程に対応づけた設計・実装の道筋

【参考】ゼロトラストアーキテクチャ適用方針

ゼロトラストアーキテクチャ適用方針	説明	ソリューションカテゴリ（例）
①リソースを識別し、特定できる状態にする	組織内のハードウェア・ソフトウェア・クラウド資産を一元管理し、可視化する。	IT資産管理（ITAM） 構成管理データベース（CMDB）　等
②主体の身元確認・当人認証を実施する	ユーザーやデバイスの認証を強化し、アクセスの正当性を保証する。	ID管理（IAM） 多要素認証（MFA）　等
③ネットワークを保護する	境界に依存せず、動的にアクセスを制御するネットワーク保護技術。	SDP（Software Defined Perimeter） マイクロセグメンテーション ZTNA（Zero Trust Network Access）（VPN代替）　等
④リソースの状態を確認する	デバイスやアプリケーション、クラウド環境のセキュリティ状態を監視・評価する。	エンドポイントセキュリティ EDR（Endpoint Detection and Response） パッチ管理　等
⑤アクセス制御ポリシーで評価しアクセス管理をする	ユーザー属性やコンテキストに基づいてアクセスを許可・拒否する。	ポリシーベースアクセス制御（PBAC） 動的アクセス制御　等
⑥リソースとアクセスを観測する	ログや行動分析により、異常検知やインシデント対応を行う。	SIEM（Security Information and Event Management） ログ管理 UEBA（User and Entity Behavior Analytics） XDR（Extended Detection and Response）　等

※「ゼロトラストアーキテクチャ適用方針」（デジタル庁）を元にデジタル庁国・地方ネットワークチームにて作成