

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

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

目次

はじめに	1
I 現状と課題	2
(1) 行政ネットワーク高度化の現状	2
(2) 行政ネットワークが直面している課題	5
(3) 行政ネットワーク構築・運用に係る課題	6
II 2030年頃の国・地方ネットワークの在り方	8
(1) ネットワークアーキテクチャ	8
(2) セキュリティの確保と利便性の向上	9
III 新たな国・地方のネットワークの将来像とそれを実現するための方策	11
(1) 仮想化技術の活用と基盤の共用化	11
(2) ゼロトラストアーキテクチャの考え方の導入	13
(3) 情報資産の扱い	14
(4) 役割分担・運用管理体制の在り方	15
(5) 移行プロセスの考え方	15
(6) 行政デジタル人材育成・発掘・技術創成・国際競争力確立のための環境整備	16
おわりに（今後の進め方）	19
参考資料1（構成員名簿）	20
参考資料2（検討スケジュール）	23
参考資料3（「デジタル社会の実現に向けた重点計画」抜粋）	24

はじめに

デジタル技術を活用し、国・地方の行政サービスを国民・住民に柔軟かつセキュアに提供すること、大規模災害や高度化するサイバー攻撃を想定したレジリエンスを確保すること、さらに行政部門の生産性を向上させ職員の働き方改革も実現していくことは、国・地方共通の課題である。

この点、国・地方のシステムが置かれた環境は変革期にある。すなわち、システムの構築・運用にあたっては、運用面の負荷軽減、共通化を通じた費用低減、セキュリティ向上等の観点から、これまでのオンプレミスから、国・地方を通じた共通基盤であるガバメントクラウドでの構築・運用を目指すこととされている。加えて、今後、ガバメントクラウドには国や地方の基幹系システムだけでなく、公共サービスメッシュをはじめ国・地方間でデータ連携を円滑に行うための情報連携基盤の整備が一層進むことも想定される。そのため、国・地方のシステムのアーキテクチャーを考える際には、ガバメントクラウドに各種システムが構築されることを念頭に置く必要がある。

しかしながら、時代のニーズに応えるシステムを構築しても、そのシステムと国・地方の行政機関を接続するネットワークがなければ、サービスを提供できない。このことを踏まえると、国・地方のネットワークは、これからの時代の重要なデジタルインフラであると言える。

これまでの国・地方のネットワークは、マイナンバー制度導入など時代の要請にも対応しつつ、それぞれ独自の成り立ち・発展をしてきた。今後、国・地方の更なる連携強化やコスト効率化、サービスレベルの向上を実現するためには、中長期の視点で全体最適となる「国・地方を通じたデジタル基盤」としてのネットワークの将来像を描く必要がある。

そのため、「デジタル社会の実現に向けた重点計画」（令和5年6月9日閣議決定。以下「重点計画」という。）に基づき、令和5年9月12日に「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」をデジタル庁に設置し、総務省の協力を得ながら、強固なセキュリティ基盤具備、ユーザー利便性の向上、安定的な運用体制、強靱性の確保の観点も念頭に、将来像及び実現シナリオについて検討を進めてきた。

本書は、その結果を報告書としてとりまとめたものである。

I 現状と課題

(1) 行政ネットワーク高度化の現状

① 国のネットワークの統合

国においては、重点計画に基づき、行政機関における生産性やセキュリティの向上を図りつつ、テレワーク等柔軟な働き方を促進できるよう、ゼロトラストアーキテクチャを採用したガバメントソリューションサービス（以下「GSS」という。）が、デジタル庁によって各府省庁に順次提供されている。

GSSは、政府共通の標準的な業務実施環境（業務用PCやネットワーク環境）を提供するサービスであり、

- ・冗長化された GSS ダークファイバ、GSS データセンター等のデジタルインフラや、
- ・GSS ネットワーク全国網、GSS ネットワークモバイル・衛星網、各省庁に整備する Wi-Fi 主体のエンタープライズネットワーク等のアクセスサービス

を組み合わせて、各種アプリサービスが提供されている。

また、こうした各種サービスは、機能化（モジュール化）され、仮想化ネットワーク技術の活用によって、各省庁の様々なニーズに応じた導入を可能としており、柔軟で可用性の高いネットワークの整備が効果的・効率的に進められている。

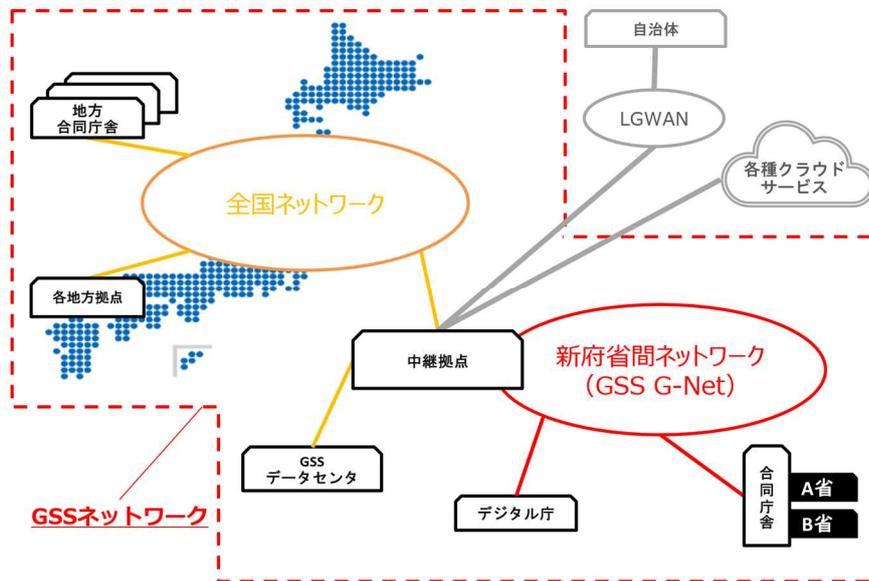
なお、GSS ネットワークは、ネットワークの設計・構築において内製化にも取り組んでおり、細分化したタスク的作業を中心に事業者の活用を行っていることが、低コスト・高パフォーマンスで高い柔軟性を有するネットワークの実現に寄与している。

GSS が提供する標準的な業務環境は、ゼロトラストアーキテクチャの考え方にに基づき、従来の境界型防御（ファイアウォール、侵入防止システム（IPS）、閉域ネットワーク等）に加えて、端末防御等を導入することで、原則、職員一人一アカウント、一台 PC 端末により、柔軟な働き方とセキュリティの両立を実現している。各府省庁のネットワークは、重点計画に基づき、2022 年以降のネットワーク更改等を契機に、原則、GSS へ移行することとされており、現在、デジタル庁、人事院、農林水産省、個人情報保護委員会、こども家庭庁、宮内庁、消費者庁、内閣府及びカジノ管理委員会が移行を行い、働き方改革や業務の効率化を実現した。また、内閣法制局、金融庁、総務省、環境省、法務省、国税庁等においても、GSS 導入に向けた準備が進められている。

広域ネットワークとしては、GSS 移行済みの本省拠点と地方支分部局等の地方拠点を結ぶ独自の全国広域ネットワークが整備・運用されており、また、2023 年 10 月の利用機関での一斉リハーサルを経て、同年末に旧来の府省間ネットワークが廃止され、GSS が提供する広帯域、高品質、低コストかつ高セキュリティな「政府共通ネットワーク」（以下「GSS G-Net」という。）への移行が完了している。

さらに、マイナポータル等ガバメントクラウド上の国のシステムについて、安全かつ費用対効果が高く、スケールアップが容易な閉域アクセスネットワークが整備され、各府省庁や地方公共団体等の各拠点からの接続が実現されている。

現在の国のネットワーク（GSS）のイメージ



② 地方のネットワーク

地方公共団体に係るネットワークに関しては、

- ・J-LIS（地方公共団体情報システム機構）が整備している、地方公共団体間や地方公共団体と政府機関間の通信を可能にしている総合行政ネットワーク（LGWAN）を中心としたネットワーク
 - ・都道府県が整備している、LGWAN から都道府県までの足回り回線や、都道府県内の通信網（都道府県 WAN）などの都道府県内のネットワーク
 - ・市区町村が整備している、LGWAN や都道府県 WAN から市区町村までの足回り回線や、市区町村内の機関同士の通信網などの市区町村内のネットワーク
- 等に分けられ、複数の整備主体により構成されている。

加えて、これらの他にも、国・都道府県から市区町村に対し、連携する事務ごとに物理的に独立したネットワーク整備を求められる場合があり、ネットワークが複雑になっている。

また、インターネット空間へは、情報セキュリティ対策が施された自治体情報セキュリティクラウドを通じて接続される。

そして、地方のネットワークのうち LGWAN は、地方の自主的かつ独自の取組として成り立ち・発展を遂げてきたところ、地方公共団体間、地方公共団体と政府機関間のメールの送受信に加え、マイナンバー制度に導入に際して、国と地方との情報連携の要としての役割も求められることとなり、

- ・マイナンバー制度による情報連携（税情報や社会保障の給付状況等）

- ・地方税の電子申告の受付、国税庁から地方公共団体への申告情報の提供
- ・マイナンバーカードを活用した各種証明書のコンビニ交付
- ・防災・人命に係る緊急情報（J-アラート）等の情報をやり取りに利用されている。

また、令和6年10月頃から運用開始を予定している第五次 LGWAN では、ガバメントクラウド接続機能を追加することとしている。

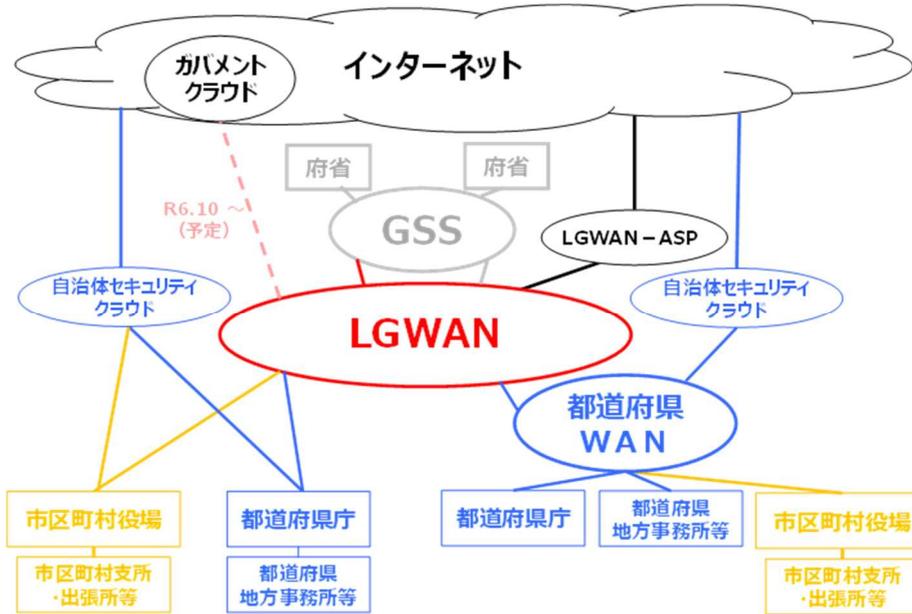
こうした情報をセキュアにやり取りするために、LGWAN は、ファイアウォールの設置、通信経路の暗号化による盗聴防止、侵入検知機能、専門家による 24 時間 365 日のセキュリティ監視等により、不正な侵入を未然に防止し、高度な安全性を確保するとともに、ネットワーク・機器の冗長化、障害発生時の早期復旧等により、安定的な運用を図っている。

なお、コスト面では、都道府県の負担金等により運営されているが、地方公共団体間の回線を集約することにより、コスト削減を図っている。

地方公共団体内のネットワークについては、2015 年の日本年金機構における情報漏えい事案を受け、マイナンバー制度による情報連携の開始が迫る中、住民情報を多く扱う地方公共団体の情報システム全体の強靭性を短期間で全国一律に向上させるため、「三層の対策」が講じられた。

その後、システムのクラウド化、行政手続オンライン化、働き方改革等の新たな時代の要請に対応するため、「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」の改定が順次行われ、各地方公共団体の判断に基づき採用しうる、より利便性の高いモデル（インターネット接続系に業務端末・システムを配置し、民間クラウドサービス利用やテレワーク等による業務効率化を図る $\beta \cdot \beta'$ モデル）の提示、LGWAN 接続系でのテレワーク・無線 LAN の利用など、業務効率と情報セキュリティ対策の両立を図るための対策が講じられるとともに、各地方公共団体において独自にセキュリティ強化や業務利便性向上に向けた取組も進められている。

現在の地方公共団体ネットワークのイメージ



③ ガバメントクラウドの展開

重点計画において、各府省庁の情報システムにおけるクラウドサービスの利用の検討に当たっては、原則としてデジタル庁が整備したガバメントクラウドの活用を検討することとし、クラウド化等を進める場合には、情報システム構築の迅速性・柔軟性の向上、可用性を始めとする高いセキュリティの実現、コスト効率の向上など、これにより得られる効果の追求を図るとされている。

また、地方公共団体は、2025 年度末（原則）までに標準化基準（標準化法第 6 条第 1 項及び第 7 条第 1 項に規定する標準化のために必要な基準をいう。）に適合する基幹業務システム（以下「標準準拠システム」という。）への移行を目指すにあたり、標準準拠システムにおいて、ガバメントクラウドを利用することは、標準化法第 10 条により努力義務とされている。

(2) 行政ネットワークが直面している課題

① 国と地方の共通の課題

行政機能の広範囲にコンピュータ・システムが活用されている現在においては、行政ネットワークには、昨今の大規模災害や高度化するサイバー攻撃を想定したレジリエンスの確保が求められている。また、少数のネットワークシステムやクラウドシステムへの集中により、クラウド事故や国家レベルのサイバー攻撃が発生した場合に、日本の行政全体が麻痺するリスクを緩和するため、集中と分散との調和を実現できるネットワークの実現も、ますます重要な課題となりつつある。

また、高度化するサイバー攻撃に対して、ネットワーク上には境界の外部/内部を問わず脅威が存在するといった前提に立ち、セキュリティを担保し、利便性を両立すること

も重要である。

②国のネットワークの課題

国においては、(1)①のとおり、各府省庁ネットワークの GSS への移行を進めており、各省庁によって異なる様々なニーズや実情を適切に把握しつつ、各省庁の GSS 移行を円滑に進めることが必要である。

また、GSS は、現在、対象ユーザー数約 3 万 5 千人、全国の拠点が約 1,300 拠点まで拡大しており、2024 年度に移行作業を開始した総務省、法務省、国税庁等の GSS 移行により、対象ユーザー数が約 9 万 9 千人、拠点数が約 1,800 拠点更に増加する見込みである。加えて、多くの職員や地方機関を抱える厚生労働省や国土交通省等についても移行に向けた協議が進められており、今後、更なる拠点数の増加やユーザー数の増加が見込まれている。

また、GSS は、政府機関の情報共有や業務連携に不可欠な GSS G-Net を提供するとともに、多数のガバメントクラウド上の国の重要システム（今後、国税などの大規模システムの移行も予定）への各府省庁拠点等からのアクセスを提供している。

こうした中、利用府省庁やユーザー数の増加に対応したネットワークの整備・強化とともに、サービスを確実かつ安定的に提供することができるよう、保守・運用体制を整備することが必要である。

③地方公共団体のネットワークの課題

地方公共団体内のネットワークでは、I(1)②のとおり、境界型防御を中心とした「三層の対策」が採られており、住民情報を多く扱う地方公共団体の情報システム全体の強靱性の向上が図られている。

この「三層の対策」は、物理的にネットワークが分離されていることで高いセキュリティを確保しているが、一方で、高度化するサイバー攻撃に備えて財政面での負担を考慮しつつ、更なるセキュリティ強化が必要である。

また、I(1)②のとおり、「三層の対策」後、業務効率と情報セキュリティ対策の両立を図るための取組が進められているが、例えば、マイナンバー利用事務系は、物理的にネットワークが分離されているが、境界を跨いでデータのやり取りが発生するなど、業務の利便性の面で引き続き課題がある。

このほか、地方公共団体と外部とのネットワークに関しては、国や都道府県から市区町村に対し、連携する事務ごとに物理的に独立した専用回線や専用端末が供給される場合があり、管理・運用が複雑になっている。

(3) 行政ネットワーク構築・運用に係る課題

国及び地方公共団体においては、行政ネットワークの企画設計、構築運用、セキュリティ対策の各段階を主導できるネットワーク等のシステム・インフラストラクチャの最

低限の知識を有する人材が不足しており、その人材育成が急務である。

また、当該人材不足に起因し、ベンダ依存体質によるコスト増や、ベンダロックイン、クラウドロックインなどの課題がある。

加えて、民間ベンダ側でも同様に人材不足が進行しており、行政ネットワークの構築・運用におけるブラックボックス依存が今後さらに進行するおそれがある。ブラックボックス化が過度に進行し、行政人材が行政のコンピュータ・システムの内容を確実に監理することができない状態となると、システムへの外部的脅威の侵入の間隙が広がるリスクがある。そこで、これを予防・改善するための行政人材育成と内製化能力の回復が、重要である。さらに、システムの内製化を進める場合、属人化により運用の持続可能性が損なわれるリスクや、引き継ぎができず外注化する場合のコスト増加のリスク等についても配慮する必要がある。

(参考) ゼロトラストアーキテクチャとその動向

ゼロトラストアーキテクチャは、ネットワーク上には外部/内部を問わず脅威が存在するといった前提に立ち、「トラスト・ゾーン（システムの内側の特権領域）を極小化する」といった概念である。物理的閉域性のみ依存する境界型モデルにおいては、トラスト・ゾーンが広大であり、全面的な防御が困難となる中、当該ゼロトラストアーキテクチャに沿ったシステムが、高いセキュリティの実現に有効である。具体的には、トラスト・ゾーンの極小化の実現の手段の一手法として、ユーザー、デバイス、アプリケーション等の細分化されたレイヤにおいて『都度必要なアクションに対して必要なレベルの認証を行い、問題なければ適切なアクセス権を認可する』といった検証を厳密に行うこと等が有効であり、国が整備するGSSでは境界型防御と端末防御等を組み合わせて導入が進められている。

II 2030年頃の国・地方ネットワークの在り方

2030年頃の国・地方のネットワークの在り方としては、国と地方公共団体や地方公共団体間の重要な行政情報処理における国家レベルの高水準なセキュリティの実現、ユーザーの利便性の向上、安定的な運用体制、強靱性が確保されたものを旨とする。

(1) ネットワークアーキテクチャ

① シンプルかつ柔軟なネットワーク

まず、ネットワークアーキテクチャとしては、シンプルかつ柔軟なネットワークが望ましい。

具体的には、共用可能な物理回線（複数種類の組み合わせ）や機器を実現し、設定における正確性や第三者検証を踏まえた安全性、長期的運用可能性、技術のオープン性、ベンダロックインの予防を担保した上で論理的に分離された仮想化ネットワーク技術を用いれば、シンプルかつ柔軟で性能及び拡張性の高いネットワークを構築することが可能となる。

それにより、結果としてユーザー目線でも簡単に操作ができ、利便性が高まるネットワークになると考えられる。

② 災害時のレジリエンス確保

I(2)①のとおり行政ネットワークにはレジリエンスの確保が求められているが、将来像でも、大規模災害等にも対応し得る強靱性と冗長性を確保する必要がある。

例えば、レジリエンス確保のために、ネットワークインフラに関するリスク分析等の現状調査を実施した上で、地上回線（固定網、携帯網）だけでなく地理的特性も配慮した衛星回線等の活用や、III(1)②で後述するような災害時の国と地方ネットワークの相互運用、インシデント対応体制（CSIRT）を含む災害時の体制の整備、平時・非常時それぞれの運用シナリオの策定及びそれに基づく訓練の実施も考えられ、検討が必要である。

③ LGWAN が担っている機能

LGWAN は、I(1)②のとおり、住民生活に密接に関わる情報をやり取りし、今後はガバメントクラウドとの接続を担うこととされており、2030年頃においても、重要情報のやり取りを担う機能は引き続き重要である。

一方、こうした機能を担うネットワークの姿としては、狭い帯域で重要情報のやり取りのみを担うネットワークとする案や、広い帯域でインターネットへの接続機能も担うネットワークとする案、更なる仮想化や IPv6 に対応したネットワークとする案なども考えられる。

詳細については、国の GSS の取組や新技術の動向も参考に、地方公共団体のコスト負担にも配慮しつつ、更なるセキュリティ確保と利便性向上が十分に図られるよう、地方

が主体となって引き続き検討する必要がある。

なお、検討に当たっては、III(5)で後述するように、強固なセキュリティを確保しつつ、更なる利便性向上を実現するための、新技術・概念・方式に係る J-LIS と IPA が連携して推進する共同研究・実証実験の成果も参考とすることが適当である。

④新技術の動向や既存施設の活用を踏まえた柔軟な対応

新たな技術であるオール・フォトニクス・ネットワークや Beyond 5G(6G)の活用による超高速大容量ネットワークの構築及び地域の既存インフラや公共インフラ（ダークファイバ含む）の有効利用による柔軟なネットワーク構成を目指すべきである。

なお、このようなネットワークを目指すにあたっては、行政主体（国・地方）の人材育成を推進し、通信事業者と対等に対話できる程度の知識・水準を実現した上で、通信事業者と必要に応じて協調しつつ、行政主体自らが柔軟で革新的なネットワーク設計・実装を常に試行錯誤し実証実験のできる環境の実現を目指す必要がある。

(2) 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及び柔軟なサービス構成を確保するためには、『トラスト・ゾーンをできる限り極小化する』という考え方である「ゼロトラストアーキテクチャ」が有効である。その一手法として、都度のアクションや対象データに対して「実効性ある認証」、「アクセス制御」、「ログの記録確実化」、「暗号化」等をソフトウェア的に実装する方法が有効である。

具体的な手法は以下のとおりである。

- (ア) リソースを識別し、特定できる状態にする（実効性ある認証）
- (イ) 主体の身元確認・本人認証を実施する（実効性ある認証）
- (ウ) ネットワーク上の脅威から保護する（実効性ある認証、アクセス制御、エンド・ツー・エンドの暗号化）
- (エ) リソースの状態を確認する（アクセス制御）
- (オ) アクセス制御ポリシーで評価し、アクセス管理をする（アクセス制御）
- (カ) リソースとアクセスを観測する（ログの記録確実化）

上記に加え、攻撃者がシステム特権領域へのアクセス権限を不正に取得し、ユーザーデータにアクセスできる状態になっても、リソースの機密性・完全性を保護するために、データを暗号化し、かつ、その暗号鍵を特権領域から隔離することは特に重要である。

※実効性ある認証

例外なく全てを識別し、身元や属性情報を確認し、認証すること

アクセス制御

認証した結果とリソースの状況に応じて判断し、アクセスを許可すること

ログの記録確実化

アクセスした結果を確実に記録し、セキュリティインシデントを発見し、また、事後的な状況分析を可能とすること

III 新たな国・地方のネットワークの将来像とそれを実現するための方策

2030年頃の国・地方のネットワークの姿としては、例えば、

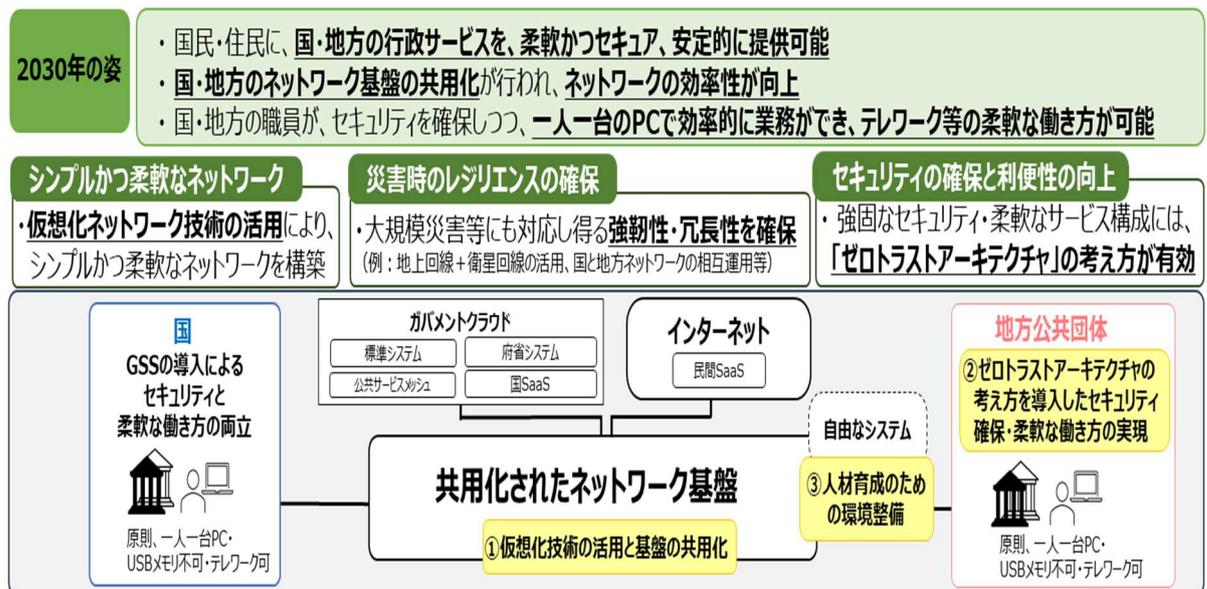
- ・国民・住民に、国・地方の行政サービスを、柔軟かつセキュア、安定的に提供可能であること
- ・国・地方のネットワーク基盤の共用化が行われ、効率性が向上すること
- ・国・地方の職員が、セキュリティを確保しつつ、一人一台のPCで効率的に業務ができ、テレワーク等の柔軟な働き方が可能であること

を目指す必要がある。

また、IIのとおり、2030年頃の国・地方のネットワークの在り方は、シンプルかつ柔軟であること、災害時のレジリエンスが確保されていること、セキュリティの確保と利便性の向上を実現すること等が求められる。

以下に、2030年頃の国・地方のネットワークの将来像のイメージとそれを実現するための方策を示す。

国・地方のネットワークの将来像イメージ



(1) 仮想化技術の活用と基盤の共用化

平時のサービス展開のコスト効率向上、非常時のレジリエンスの確保を目的として、以下のような仮想化技術の活用を検討すべきである。

- ① 現在、国の GSS においては、冗長化された共用可能な物理回線や共用のネットワーク機器（拠点ゲートウェイ機器等）を全国に整備し、その上で、仮想化ネットワーク技術を活用して GSS G-Net や各府省庁 LAN などの論理ネットワークを構築している。これにより、これまで各府省庁が個別最適の考え方で整備していたネットワーク環境の重複を排除し、コスト削減を行うとともに、各府省庁のニーズに応じた柔軟なサービス提供を実現している。
- ② 他方、地方のネットワークについては、国の課題と必ずしも同じではないが、国・地方でノウハウやリソースを共用する観点や円滑な情報連携の実現の観点も踏まえつつ、GSS の例と同様に、地方を主体として、(a) 地方公共団体間の相互のネットワーク、(b) 地方公共団体の庁舎とその地方公共団体が契約するガバメントクラウドとの間のネットワーク及び(c)地方が国のネットワークに接続するための地方のネットワークの仮想化を検討すべきである。
- ③ さらに、国・地方のネットワークインフラへの重複投資の排除等による効率化、ネットワーク機器や運用ポリシー等の標準化による相互運用性の確保、国・地方共同での人材確保・育成など、国・地方での戦略的なネットワーク整備を国・地方が対等な関係で相互に協力しながら実現できるよう、地方の意見も聞きながら、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すべきである。
- （※国・地方のネットワーク基盤の共用化の方法としては、例えば、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することが考えられる。また、その際、新技術（オール・フォトリクス・ネットワークや Beyond 5G(6G)等）の活用についても検討することが考えられる。）
- ただし、検討に当たっては、同一の物理ネットワーク上で国・地方の様々な重要情報が行き交うことになることから、個人情報保護、セキュリティ、業務継続性等に万全の配慮がなされる必要があり、運用主体の在り方、責任分界及び共用化範囲等の運用面、費用負担の在り方等の財源面、技術面、法令面並びに人材育成面について留意が必要である。加えて、国と地方のチェック・アンド・バランス（権力抑制・均衡）の観点から、両者において一定水準のネットワーク人材が確保されるよう、国・地方のネットワーク人材の双方を育成することが必要である。
- また、ネットワーク基盤を共用化することで、例えば、災害・障害発生時等に国又は地方のネットワークのいずれかが不通となった場合に、相互乗り入れが可能になることも考えられる一方、どちらも不通になることも考えられるため、レジリエンス確保の観点から併せて検討が必要である。

(2) ゼロトラストアーキテクチャの考え方の導入

① 国においては、I(1)①のとおり、GSS 導入済みの各府省庁では、ゼロトラストアーキテクチャの考え方（ネットワーク上には外部/内部を問わず脅威が存在するといった前提に立ち、「トラスト・ゾーン（システムの内側の特権領域）を極小化する」という考え方をいう。以下同じ。）に基づき、従来の境界型防御に加えて、端末防御等を導入することで柔軟な働き方とセキュリティの両立を実現している。このため、重点計画に基づき、ネットワーク更改等を契機に、原則、ゼロトラストアーキテクチャの考え方を導入した GSS への移行を着実に進めるべきであり、各省庁によって異なる様々なニーズや実情を適切に把握しつつ、必要に応じ GSS が提供するサービスの見直しや拡充を行うことも含め、円滑な移行に向けた準備を計画的に進めることが必要である。また、I(2)②のとおり、利用府省庁やユーザー数の増加に対応するため、保守・運用体制を強化することが必要である。

② 地方のネットワークについても、国とのセキュアで円滑なデータ連携を実現する観点からは、ネットワーク設計の基本的な考え方をそろえることが望ましく、また、高いセキュリティの確保と利便性の向上を実現する手段としても、ゼロトラストアーキテクチャの考え方を導入することが有効である。このため、個人番号利用事務系や LGWAN 接続系を含めた地方公共団体内の庁内の閉域的なネットワークについても、境界内部に脅威が存在しうることを前提として、ゼロトラストアーキテクチャの考え方をサーバーやソフトウェアに確実に実装していくことが重要である。すなわち、ゼロトラストアーキテクチャの考え方を導入している GSS の取組を参考に、境界型防御だけに依拠するのではなく、閉域網内部のシステムにおいてもゼロトラストアーキテクチャの考え方を徹底して、より高いセキュリティやテレワーク等柔軟な働き方の実現を目指すべきである。

また、利便性向上のため、庁内の複数ネットワークへの単一の端末からの高速・快適・低遅延な同時アクセスのために、物理的なネットワーク分離をやめて、1 台のコンピュータ上で複数のセグメントに接続し、各セグメントのアプリケーション領域を相互に安全に隔離するとともに、異なるセグメントのアプリケーション間のデータのやりとりを容易・快適にする等の仮想化技術(論理ネットワーク、VM、コンテナ等の新技術)を一層活用していくことが考えられる。

そして、ゼロトラストアーキテクチャの考え方の実装に向けては、

- (i) 総合行政主体である地方公共団体は、国の各府省庁と比べ、業務分野が幅広く、守るべき住民情報を多く扱っていること、
- (ii) ゼロトラストアーキテクチャの考え方を既存の製品、ソリューション、ライブラリ等に依存して実装する場合は、これらが比較的新しく、ゼロトラストアーキテク

ャの考え方に正確に沿っておらず、ブラックボックス的性質を有する製品などトラスト・ゾーンの極小化に反する製品を導入することで、かえってセキュリティリスクが高まることも起こり得ること、

- (iii)ゼロトラストアーキテクチャの考え方の導入には、既存のサーバーやアプリケーションに確実に認証等の処理を実装するか、あるいは、新たにシステムやアプリケーションを開発する必要がある、それに対応できる内製人材の育成あるいは外注費用がかかるといったコストが生じるが、地方公共団体の状況によっては、短期間ですべてのシステムにゼロトラストアーキテクチャの考え方を実装することは困難であること

を考慮する必要がある。

そのため、技術動向や運用管理体制も含めた費用対効果、地方独自の実情も踏まえ、今後、地方の意見を十分に聞きながら、デジタル庁及び総務省においてゼロトラストアーキテクチャの考え方の導入に向けた調査・分析・検証（※）を実施することで、上記を含めた考慮事項に係る懸念点の解消を目指し、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」で詳細な検討を行うのが適当である。

（※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することが考えられる。）

(3) 情報資産の扱い

- ① 国の情報資産の扱いについては、「政府機関等のサイバーセキュリティ対策のための統一基準（令和5年度版）」（令和5年7月4日サイバーセキュリティ戦略本部決定。以下「統一基準」という。）の第1部 1.2 情報の格付の区分・取扱制限にて示されている。「政府情報システムにおけるクラウドサービスの利用に係る基本方針」の2章基本方針では、「クラウド・バイ・デフォルト原則」が記され、政府情報システムはクラウドサービスの利用を第一候補として検討を行うものとしている。クラウドサービスの利用にあたっては、統一基準の 4.2.1 クラウドサービスの選定（要機密情報を取り扱う場合）において、原則、「政府情報システムのためのセキュリティ評価制度（以下「ISMAP」という。）」で定める ISMAP 等クラウドサービスリストからクラウドサービスを選定することとしている。
- ② 地方公共団体の情報資産の扱いについては、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」に記載されているが、国の取扱いを踏まえ、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、ガバメントクラウド上の取り扱いを含め情報資産の分類の考え方を整理し、地方公共団体に参考として提示する。

- ③ ガバメントクラウド上に保管されるデータのセキュリティ(機密性または完全性のいずれかの確保が必要なもの)の一層の確保のため、(ア) 行政主体自らの機微な情報、及び(イ) 国民・住民の個人情報に係るプライバシー権等の法的権利を、クラウド特権領域に係る侵害から保護し、国や地方公共団体が適切に情報資産を管理する手法の一つとして BYOK (Bring Your Own Key。クラウド上に保存されるデータを、ユーザー自らが用意した鍵により暗号化・復号化し、かつ、その鍵は当該クラウド上に決して保存しない手法。)をはじめとする暗号鍵管理手法は、必須となりつつある。

そこで、ガバメントクラウド上のユーザーデータの機密性を保護するために、ユーザーが自ら生成した鍵を用いて、ユーザーデータを透過的に暗号化・復号できるようにすることにより、行政側が、ガバメントクラウド上のデータの管理権を確保する必要がある。すなわち、クラウド事業者がユーザーの許可なくユーザーデータにアクセスできないようにすべきである。

デジタル庁において、現在利用可能なデータ保護の方法に加え、将来を含めたガバメントクラウドの様々な利用形態を想定し、より一層低コストかつ安全な方法について、最新の暗号技術を含む多角的な観点からの継続的な調査研究を行いながら、検討する。

(4) 役割分担・運用管理体制の在り方

国においては、デジタル庁が主体となり GSS ネットワークの構築・運用を進めていくが、各省庁の GSS 移行を着実に実施するとともに、ユーザー数増に対応したネットワークの整備を強化していく必要がある。

他方、地方公共団体において、ネットワーク構築・運用を進めるにあたっては、地方公共団体の負担増にならないよう配慮しながら、運用主体、国のネットワークとの責任分界、各行政主体の役割分担について、III(1)の仮想化技術の活用による国・地方のネットワークの共用化の視点も考慮し、国と地方が協調して、さらに検討する。

運用開始後の管理体制について、ゼロトラストアーキテクチャの実装に必要な ID や端末の管理、システムの安定的な運用を支える体制、CSIRT を含む災害時の体制の整備、平時・非常時それぞれの運用シナリオの策定、それに基づく訓練の実施、運用に対する評価プロセスの確立が重要である。

また、国から地方公共団体に対し、IT や DX に関する最新技術や動向等について情報発信するなどして、国は地方公共団体のネットワーク構築を担当者のみならず幹部層を含めサポートする。

(5) 移行プロセスの考え方

国においては、ネットワーク更改等を契機に、各府省庁と順次協議を行いながら GSS による標準業務環境への統合を進めている。

地方においては、LGWAN の強固なセキュリティを確保しつつ、さらなる利便性向

上を実現するため、自治体テレワークシステム for LGWAN の共同実現の前例を基礎として、J-LIS や地方公共団体によって自ら運用可能な新技術・概念・方式に係る共同研究・実証実験を、J-LIS と IPA が連携して推進することが考えられる。

また、地方公共団体のⅢで示した将来の新たなネットワーク移行においては、上記の地方における強固なセキュリティと利便性向上の両立のための研究・実証や、Ⅲ(2)②にあ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十分な調査・分析・検証等を踏まえつつ、地方公共団体の負担増にならないよう、移行に伴うイニシャルコストを明らかにした上で、分散・段階的な移行について検討が必要である。

(6) 行政デジタル人材育成・発掘・技術創成・国際競争力確立のための環境整備

Ⅲ(2)のとおり、ゼロトラストアーキテクチャの考え方の導入を見据え、システムの安定的な運用やインシデント等に的確に対応できる人材や、システムやネットワークのアーキテクチャを考えながら適切に機器・サービスの選定・調達ができる人材の確保もますます重要になると予想される。

このように、行政ネットワークの構築・運用に資する専門人材の確保が課題となる中、人材の確保や育成及び人事評価が重要であることに鑑み、例えば、国と地方公共団体の職員の交流・コミュニティの形成、研修機会の提供、国及び地方公共団体への専門人材の積極的な登用、資格取得の奨励、成果を上げた職員への評価制度の見直しを進めるべきである。また、職員の専門性を高めるため専門人材を登用した際の人事ローテーションについて、関連部署間の異動など一般職員と異なる仕組みで行うことも考えられる。

さらに、行政のデジタル人材の不足が進展する中、以下のような取組が必要である。

- ・コンピュータ、ネットワーク、セキュリティ、クラウド等のデジタル要素に関する基礎的・基本的な知識を実践的に学ぶことができる機会や環境の確保
- ・高度に複雑化した現行の行政デジタルシステムのブラックボックスの内側を含めて、システム全体を本質的に理解できる行政デジタル人材の増加
- ・異なる主体、プラットフォーム、ネットワーク上で成長してきた各種行政デジタルシステム間の効率的な連携に資する人材や新技術の形成
- ・行政職員自らシステムを試作・改良する慣習やリスク受容性がありデジタル変化に対応できるシステム試行錯誤環境の整備と、デジタル人材のための人事上の適切な配慮
- ・国の安定した統治や国民・地域住民の権利を保障する高いセキュリティと、高い利便性の両立とを現実化することができる人材の育成と新たな技術の醸成

これらの取組を進めるに当たっては、以下の「自由なシステム」と呼ばれる方策を推進することが必要である。

- (a) 「厳格なシステム」 / 「自由なシステム」の区別

主に外注主義・計画主義で運用されている、停止が許容されず、厳格な開発・運用・管理が必要な性質を有する各種現用システムおよびそれらの開発・動作環境のことを、総称して、「厳格なシステム」と呼ぶ。これと対比し、行政職員自らが技術研鑽目的で自作システムを試作したり、新しい企画に基づいて新たなシステムを一人または少数グループで開発したりする場合における、開発・実験環境およびそれによって作った自作システム類を総称して、「自由なシステム」と呼ぶ。

「自由なシステム」は、創造的な生態系である。目前に必要な基礎的・基本的デジタルリテラシの修得にも利用可能とするとともに、より長期的視点にも立ち、新技術創成、国家レベルの高いセキュリティの実現、コンピュータ領域に留まらない経営的・戦略的能力を有する人材育成、国際競争力強化等をより大きな目的とする。そのために、官民の技術者や研究者が適切な自律性及び高い自由度をもって業務革新を試行することのできる場と、そこに自然に形成される人的・ネットワーク的・コンピュータ的・ソフトウェア的生態系を実現することを目指す。

(b) 「自由なシステム」による人材育成の全国の行政機関共同での実現

各行政機関がそれぞれ「自由なシステム」の考え方に基づく環境を実現することは負担が大きいため、共同で整備することが望ましい。この手法は、各行政機関に点在している行政デジタル人材間の連携や互助を自然に促す点でも有益である。そこで、「自由なシステム」は、複数の行政主体の行政職員たちが共用できるだけでなく、各人材が共同して組み立てていくことができ、その上で、各人材が各種システムを内製したり試験提供したりすることが容易に可能な仕組みを目指す。

(c) 国・地方の複数の行政機関間での連携・協調

国の複数の行政機関等と、複数の地方公共団体等との間で、コンピュータやネットワークに関する人的交流を深め、信頼関係を醸成し、技術を高め合えば、国・地方の互いの協力関係がさらに高まり、さまざまな施策や IT プロジェクトの実施の上で円滑に連携することで、質の高い行政サービスの実現を目指す。

(d) 民間との連携や将来を担う地域若手人材の育成

外部の知見を取り入れたり、行政職員が創成した技術成果を社会還元したりするためには、民間人材との交流が重要である。また、2030～2040年頃において優秀な行政人材として入庁してくれる可能性や、あるいは国際的な競争力を持つデジタル産業を創業する可能性がある、潜在的能力が突出した地域若手人材（現在は子どもである。）の発掘育成と交流も、極めて重要である。官民の優秀な人材が行政機関のレガシーなシステムの課題に触れ、これを根本的に解決できる新技術を生み出す契機ともなる。そこで、「自由なシステム」は、民間人材に対して可能な限りオープンな体制とするとともに、地域人材の発掘・育成に熱意がある自治体主体の施策にも活用できることが必要である。

(e) リスク対処と受容の仕組みの実現

行政職員が発案したシステムを試作したり、職員が高度なセキュリティ能力を修得

したり、従来の限界を超えるネットワークやクラウド技術等の実現を目指したりするためには、試作中の段階から、行政機関のユーザーはもちろん、一般ユーザーを対象に公開したり、インターネット上で運用したりする必要がある。また、(d)により、民間や地域若手人材の参画を許容する必要がある。「自由なシステム」においては、このような必要な行為に付随して発生する各種リスクを受容し、対処できる仕組みを実現することを目指す。そのための手法として、「自由なシステム」は、行政の既存の「厳格なシステム」との隔離を徹底し、互いに影響が及ばないようにする。

(f) スモールスタート原則

歴史的にみると、良いコンピュータやネットワーク技術創成には、大規模な計画主義は逆効果な場合が多く、むしろ小規模・低コストで開始され、段階的に発展する場合の方が効果的であり、自由な発想や創造性が高まる可能性が高い。そこで、「自由なシステム」の方針としては、当初は目立たずにスモールスタートし、一定の能力を有する国・地方の有志が共同で運営を行ないつつ、次第に多数の人材が集まり、成果が継続的・自律的に出現する、自然的拡大を目指す。

なお、現在、政府においては、「デジタル田園都市国家構想」におけるデジタル専門人材派遣制度など他の政策パッケージの中でも、デジタル人材の確保・育成に向けた取組が進められており、こうした施策と連携して、行政ネットワークを担う人材の育成・確保にしっかりと取り組むことも重要である。

おわりに（今後の進め方）

本報告書で示した 2030 年頃の国・地方のネットワークの将来像については、今後、地方公共団体の意見も丁寧に伺いながら、実現するための取組を着実に進める必要がある。

具体的には、国として国・地方のネットワークの将来像に係る方向性を示し、

- ・ゼロトラストアーキテクチャの考え方の導入に向けた調査・分析・検証（Ⅲ(2)②）
- ・人材育成のための「自由なシステム」の実証環境整備（Ⅲ(6)）
- ・地方における強固なセキュリティと利便性向上の両立のための研究・実証（Ⅲ(5)）

等について、可能なものから速やかに実施する必要がある。そして、地方公共団体の意見も丁寧に伺いつつ、トライアル&エラーを行いながら将来像の実現に向けて詳細な検討を進め、国・地方の新たなネットワークへの移行を実現するとともに、安定的かつ持続的な運用管理体制も構築する必要がある。

他方、現在、国では、ネットワーク更改等を契機に、各府省庁と順次協議を行いながら GSS による標準業務環境への統合を進めており、地方公共団体においては、2025 年度末（原則）までに標準準拠システムへの移行を進めている。加えて、GSS や LGWAN は、2030 年頃に更改時期を迎えることが想定される。

そのため、本検討会では、国・地方・各事業者の負担やリソースの不足、行政ネットワークの更改時期を考慮して、国・地方のネットワークの将来像を 2030 年頃と設定している。今後、国・地方の新たなネットワークへの移行プロセスを具体化する際も、ネットワーク更改時期等を踏まえた分散・段階的な移行を検討するなど、配慮が必要である。

最後に、今回とりまとめた国・地方のネットワークの将来像は、これまで独自の成り立ち・発展をしてきた行政ネットワークについて、全体最適を目指す前例のない取組であり、実現の過程では、新たなハードルが多く生じることが予想される。

しかしながら、国・地方の更なる連携強化やコスト効率化、サービスレベルの向上を実現するためには、「国・地方を通じたデジタル基盤」としてのネットワークは欠くことのできないものであり、今後、国・地方の緊密な連携・対話の下、両者の叡智を結集し、粘り強く実現に向けて取り組んでいくことを期待する。

参考資料1（構成員名簿）

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

構成員名簿（令和6年4月23日時点）

【座長】

しやうじ まきひこ
庄司 昌彦 武蔵大学社会学部 教授

【構成員】

うえはら てつたろう
上原 哲太郎 立命館大学情報理工学部 教授

ごとう あつひろ
後藤 厚宏 情報セキュリティ大学院大学 学長

しもじょう しんじ
下條 真司 青森大学ソフトウェア情報学部 教授

たかほし くにお
高橋 邦夫 KU コンサルティング 代表

のぼり だいゆう
登 大遊 IPA サイバー技術研究室 室長

あべ ともあき
阿部 知明 デジタル庁 統括官付審議官

ふじた せいたろう
藤田 清太郎 デジタル庁 統括官付審議官

みはし かずひこ
三橋 一彦 総務省 大臣官房審議官

（地方行政・個人番号制度、地方公務員制度、選挙担当）

きくち よしのぶ
菊池 善信 地方公共団体情報システム機構 総合行政ネットワーク全国センター長

（※敬称略）

【準構成員】

ほんまる たつや
本丸 達也

デジタル庁 チーフアーキテクト

やまもと のりひと
山本 教仁

デジタル庁 チーフクラウドオフィサー

さか あきら
坂 明

デジタル庁 チーフインフォメーションセキュリティオフィサー

おおい えまきふみ
大江 将史

デジタル庁 ネットワークエンジニア

せきや ゆうじ
関谷 勇司

デジタル庁 ネットワークエンジニア

みつしお なおふみ
満塩 尚史

デジタル庁 セキュリティアーキテクト

ふるかわ やすし
古川 易史

デジタル庁 統括官付参事官

はだ かける
羽田 翔

デジタル庁 統括官付参事官付企画官

なごし いちろう
名越 一郎

総務省 自治行政局デジタル基盤推進室長

(※敬称略)

【オブザーバー】

橋本 崇

宮城県 企画部デジタルみやぎ推進課長

金高 裕一

兵庫県神戸市 デジタル戦略部課長

峯 雅徳

長崎県佐世保市 総務部 DX 推進室 主査

高科 恵美

兵庫県伊丹市 総合政策部デジタル戦略室主幹

萩原 和幸

埼玉県美里町 総合政策課長

中窪 悟

鹿児島県肝付町 デジタル推進課 課長補佐

山内 一郎

エヌ・ティ・ティ・コミュニケーションズ株式会社

ビジネスソリューション本部 ソリューションサービス部 担当部長

丸田 徹

KDDI 株式会社 コア技術統括本部 技術企画本部 副本部長

伊藤 晋

日本電気株式会社 ガバメントプラットフォーム統括部 統括部長代理

川島 正久

日本電信電話株式会社 研究企画部門 IOWN 推進室 技術ディレクタ

稲垣 浩

一般社団法人行政情報システム研究所 システム事業部長

田邊 光男

総務省 情報流通行政局情報通信政策課長

渡辺 琢也

経済産業省 商務情報政策局ソフトウェア・情報サービス戦略室長

(※敬称略)

参考資料2 (検討スケジュール)

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

検討スケジュール

令和5年	9月12日	第1回検討会
	11月2日	第2回検討会
	12月21日	第3回検討会
令和6年	2月6日	第4回検討会
	3月18日	第5回検討会
	4月23日	第6回検討会

参考資料3（「デジタル社会の実現に向けた重点計画」抜粋）

「デジタル社会の実現に向けた重点計画」（令和5年6月9日閣議決定）（抄）

第3-2 各分野における基本的な施策

1 国民に対する行政サービスのデジタル化

（1）国・地方公共団体・民間を通じたトータルデザイン

② 実装に向けた取組

イ 安全性と利便性の両立を追求するネットワーク環境

インフラの検討は、技術的・環境的な変化や地方公共団体の課題を踏まえ、不断に進める。国・地方を通じたデジタル基盤に関して、全体最適かつ効率的なネットワーク構成となるよう、強固なセキュリティ基盤の具備、ユーザー利便性の向上、安定的な運用体制、強靱性の確保の観点も念頭に、将来像及び実現シナリオについて、具体的に検討を進めることとする。

特に、地方公共団体のセキュリティについては、ガバメントクラウドやSaaS等のクラウドサービスの利活用、職員の効率的な働き方の実現、新しい住民サービスの迅速な提供等を可能にするため、「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」を継続的に見直す。具体的には、現行のいわゆる「三層の対策」について、地方公共団体の意見も聞きながら、抜本的な見直しを行うとともに、将来的には、政府情報システムと歩調を合わせつつ、ゼロトラストアーキテクチャの考えに基づくネットワーク構成に対応するよう検討を行う。