新たなコミュニケーション基盤の整備にかかる

基本計画書

（必要箇所のみ抜粋）

令和３年３月

目次

本計画書の趣旨

県では、デジタル技術を駆使して行政事務を効率化し、県民・企業などへの効果的・効率的な行政サービスの提供や、職員の生産性向上を実現する「スマート自治体」への転換をめざしている。

現在、AI・RPA やペーパーレス化のほか、コロナ禍におけるテレワーク・Web 会議の導入を推進しており、さらに今後は、コロナ後の新常態を見据え、申請などのオンライン化やクラウドサービスの利用など、新たなデジタル技術を活用した行政サービスの創出（DX＝デジタル・トランスフォーメーション）にも取り組むこととしている。

こうした状況にある一方で、現在の情報基盤については、情報セキュリティ対策の抜本的強化（いわゆる「三層の対策（三層分離）」）や、全庁ネットワークシステムへ接続する業務端末の環境などに起因する利便性・効率性の低下を招いている状況であり、DX の推進に向けて、コミュニケーション基盤としてのあり方を抜本的に見直す必要が生じている。

そこで、情報セキュリティを確保しつつ、ネットワークシステム環境の見直しや、データ活用をはじめとしたデジタル技術の先進的な利活用、新しい働き方の実現などを可能にする新たなコミュニケーション基盤の整備に向けた考え方を、基本計画としてとりまとめた。

第1章　基本計画策定の背景

1.　環境の変化（国・他県の動向）

1.1　　国の動向

政府は、2020 年（令和 2 年）12 月 25 日、デジタル化改革の推進に向け、「デジタル社会の実現に向けた改革の基本方針」及び「2020 年改定版デジタル・ガバメント実行計画」を閣議決定した。

また、総務省は同日、「デジタル・ガバメント実行計画」における自治体のデジタル社会構築に向けた施策を定めた「自治体 DX 推進計画」を策定した。

1.1.1　　デジタル社会の実現に向けた改革の基本方針

(1)　位置付け

デジタル社会の将来像、IT 基本法の見直しの考え方、デジタル庁（仮称）設置の考え方などについて、政府としての方針を示すものである。

(2)　概要

- 「デジタルの活用により、一人ひとりのニーズに合ったサービスを選ぶことができ、多様な幸せが実現できる社会」を、デジタル改革がめざすデジタル社会のビジョンに掲げ、「誰一人取り残さない、人に優しいデジタル化」を進める。
- ビジョンに掲げるデジタル社会形成の実現に向けて、「図 1-1-1　デジタル社会形成に向けた 10 の基本原則」に示す 10 の基本原則を大方針として施策を展開することとしている。
- 新たな社会課題に的確に対応し、社会のデジタル化を強力に進めるため、施策の策定に係る方針などを定める IT 基本法の全面的な見直しを行う。
- デジタル社会の形成に関する施策を迅速かつ重点的に推進する新たな司令塔としてデジタル庁（仮称）の設置 (注) とその方針を示す。
  注：2021 年（令和 3 年）2 月 9 日、デジタル庁（仮称）を創設することを柱としたデジタル改革関連法案が閣議決定・国会提出された。このうち、「デジタル庁設置法案」は、9 月にデジタル庁を創設し、デジタル改革の司令塔として各省庁への勧告権など強力な権限を持たせるとともに、国の情報システムを統括させるなどとしている。
- また、「デジタル社会形成基本法案」は、2000 年（平成 12 年）に制定された IT 基本法にかわるもので、デジタル社会の形成に関し、基本理念及び施策の策定に係る基本方針、国・地方公共団体及び事業者の責務、デジタル庁の設置並びに重点計画の作成について定めている。

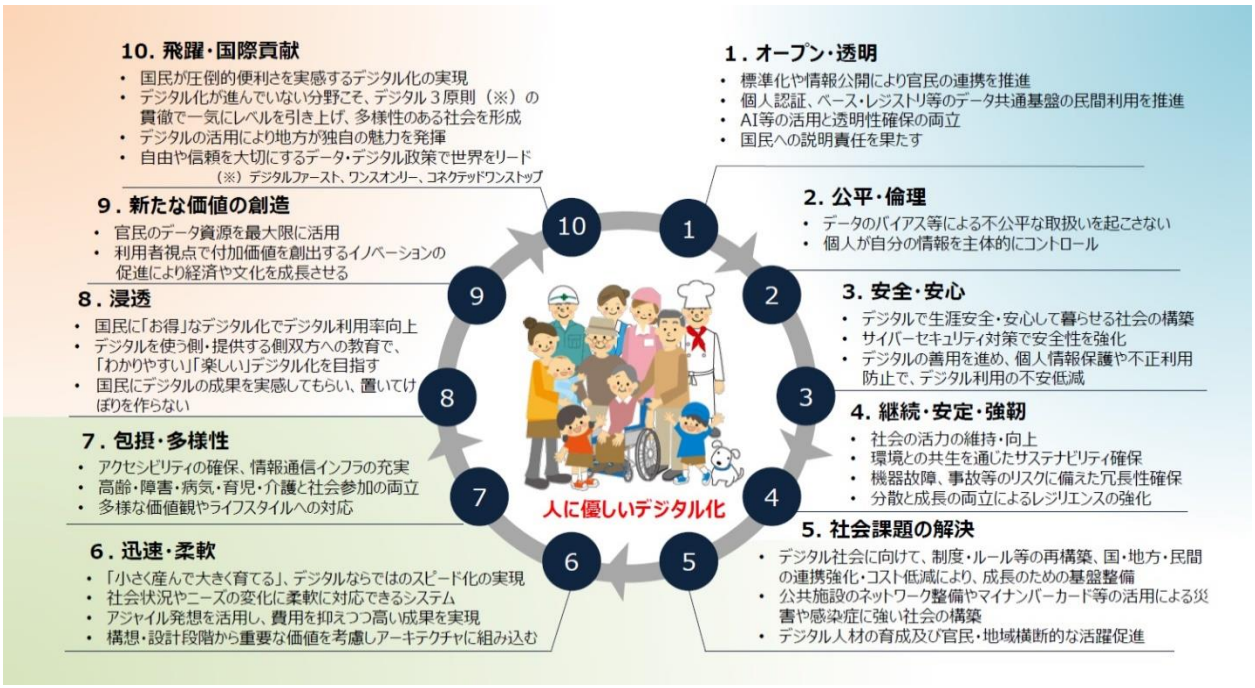


図 1-1-1　デジタル社会形成に向けた 10 の基本原則

1.1.2　デジタル・ガバメント実行計画

(1)　位置付け

デジタル手続法に基づく、ICT を利用して行われる手続などに係る国の行政機関などの情報システムの整備に関する計画である。2019 年（令和元年）12 月に閣議決定され前計画に対し、その後の取り組みの進展や、新型コロナウイルス感染症への対応で明らかになった課題をふまえ、デジタル・ガバメント推進のための取り組みを加速するとともに、計画的かつ実効的に進めていくために改定された（計画期間：2020 年（令和 2 年）12 月～2026 年（令和 8 年）3 月）。

(2)　概要

・ 実行計画は次の 7 項目の課題について取り組みを進めていく。

「サービスデザイン・業務改革（BPR）の徹底」

「国・地方デジタル化指針」

「デジタル・ガバメント実現のための基盤の整備」

「一元的なプロジェクト管理の強化等」

「行政手続のデジタル化、ワンストップサービス推進等」

「デジタルデバイド対策・広報等の実施」

「地方公共団体におけるデジタル・ガバメントの推進」

・「国・地方デジタル化指針」は、デジタル政府・デジタル社会の基盤となる、マイナンバー制度及び国と地方のデジタル基盤の抜本的な改善に係る取組及びその工程表からなる。
・この取り組みは、地方のシステムの標準化・共通化・クラウド化、情報連携基盤（「公共サービスメッシュ」）の構築、利便性の高い国民・民間事業者向けポータルサイトなどの構築（「民間タッチポイント」）、システムのクラウド化と連動したネットワーク構造の抜本的な見直しなどとして示され、2025 年（令和 7 年）へ向けたシステム・ネットワークのトータルデザインが描かれている。

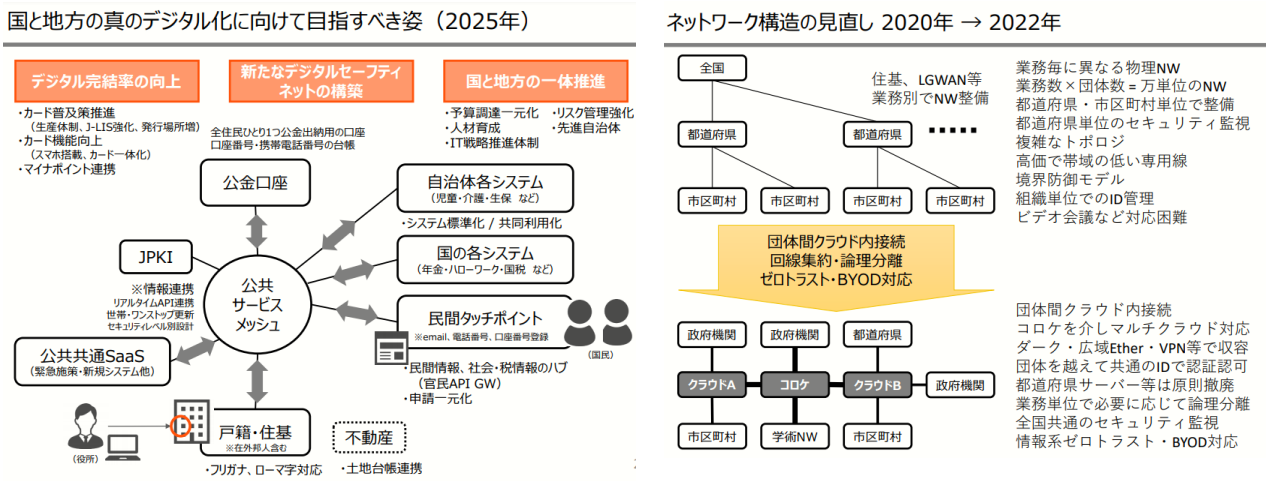


図 1-1-2　2025 年へ向けたシステム・ネットワークのトータルデザイン

1.1.3　自治体 DX 推進計画

(1)　位置付け

「デジタル・ガバメント実行計画」における自治体の情報システムの標準化・共通化など、自治体が重点的に取り組むべき事項を具体化するとするとともに、総務省及び関係省庁による支援策などをとりまとめた計画である。（計画期間：2021 年（令和 3 年）1 月～2026 年（令和 8 年）3 月）

(2)　概要

・「(仮称)Gov-Cloud」の活用に向けた 6 つの重点取組事項を示している。
「自治体の情報システムの標準化・共通化」
「マイナンバーカードの普及促進」
「自治体の行政手続のオンライン化」
「自治体の AI・RPA の利用促進」

「テレワークの推進」
「セキュリティ対策の徹底」

・「(仮称)Gov-Cloud」は、国が整備・運用することとしている、共通的な基盤・機能を提供する複数のクラウドサービス（IaaS、PaaS、SaaS）の利用環境である。これにより、業務改革（BPR）、業務・データの標準化などを前提に、各情報システムを構築することで、迅速な構築及び柔軟な拡張、最新のセキュリティ対策、技術革新対応力や可用性の向上、コストの大幅低減の実現をめざしている。

・「(仮称)Gov-Cloud」の活用イメージ、及び自治体の情報システムの標準化・共通化のスケジュールが、「図 1-1-3 「(仮称)Gov-Cloud」の活用イメージ」並びに「図 1-1-4 自治体の情報システムの標準化・共通化のスケジュール」のとおり示されている。

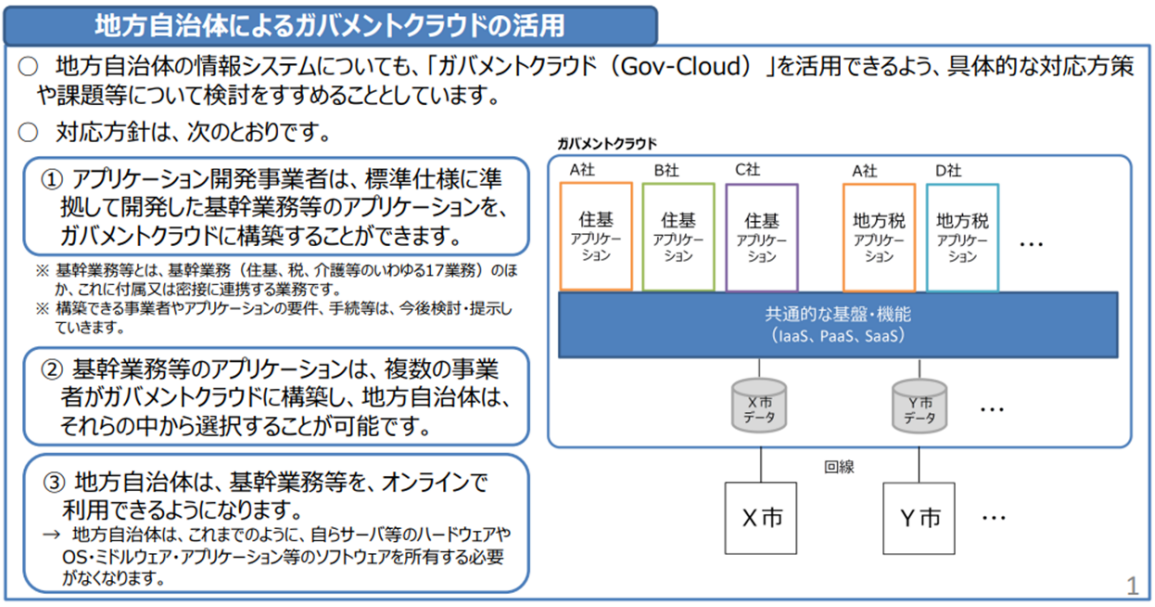


図 1-1-3 「(仮称)Gov-Cloud」の活用イメージ

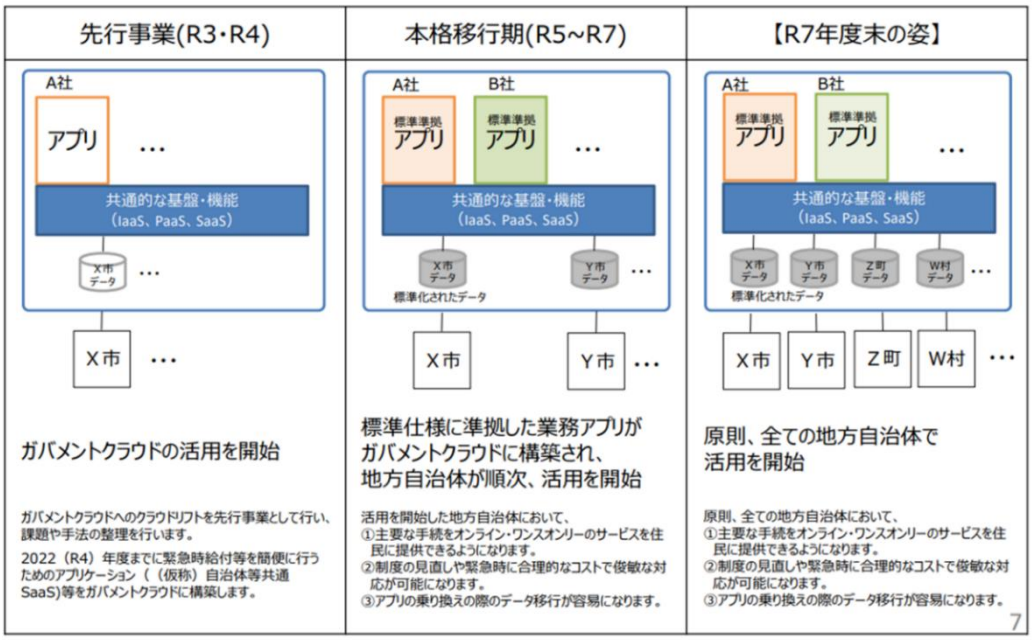


図 1-1-4　自治体の情報システムの標準化・共通化のスケジュール

1.2 他県の動向

（省略）

2. 県の現状と課題

2.1 「アフターコロナの新常態」を見据えたスマート改革の推進

県は、2019 年度（令和元年度）にスマート改革を開始し、2020 年度（令和 2 年度）には、「Smart Government」「Smart Workstyle」「Smart Solutions」という 3 つの「S」を柱に、全庁的なスマート改革を進めている。

2.1.1 背景・目的

今後、県内でも人口減少が見込まれ、少ない職員で県民からのニーズに応え続けるためには、業務効率化と生産性の向上が不可欠である。また、新型コロナウイルスの感染拡大により、世の中の考え方・働き方は大きく変わり、「アフターコロナの新常態（ニュー・ノーマル）」が現れ出ている。このような社会情勢の中、感染拡大の防止を進めつつ、収束後の「新常態」を見据え、県の変革を進めることが必要となっている。また、県がこの変革を率先して進めることにより、県全体に変革の機運を波及させることも狙いとしている。

2.1.2 スマート改革の現状

県は、業務削減や効率化により職員の生産性を向上させつつ、県民サービスの向上も図ることで、住民・民間団体など多様な主体・市町にとって便利な県庁をめざす改革（Smart Government）、在宅勤務など柔軟な働き方を実現する改革（Smart Work Style）、そして、テクノロジーを活用し、これまで解決できなかった社会課題の解決を進める改革（Smart Solutions）の「3S」に取り組んでいるところである。

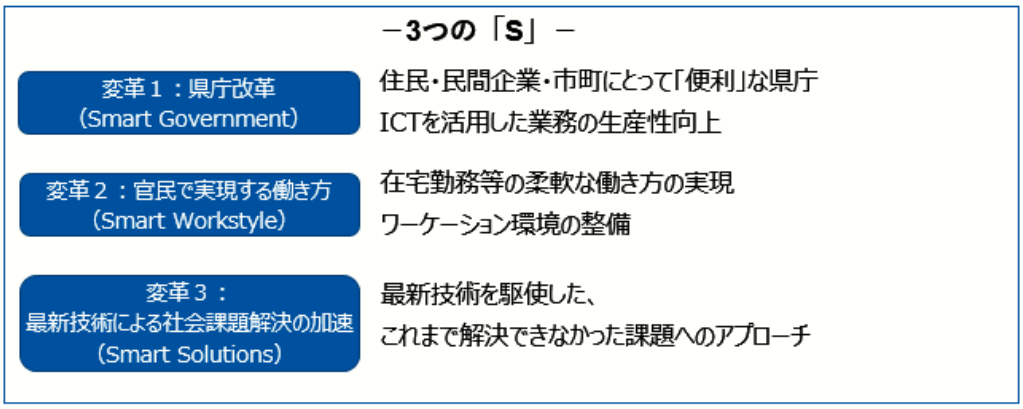


図 1-2-1 県が取組む「スマート改革」の概要

2.1.3 スマート改革を推進する DX

「スマート改革」の推進に向けては、組織経営を含む課題認識を明確にした上でデジタル技術を効果的に取り入れ、県民目線に立った、付加価値の高いサービスを生み出していく DX が不可欠である。

DX には、「デジタル技術の活用」はもちろんのこと、これらの活用を可能とする「人材の育成」「ルールの整備」が必要な要素である。

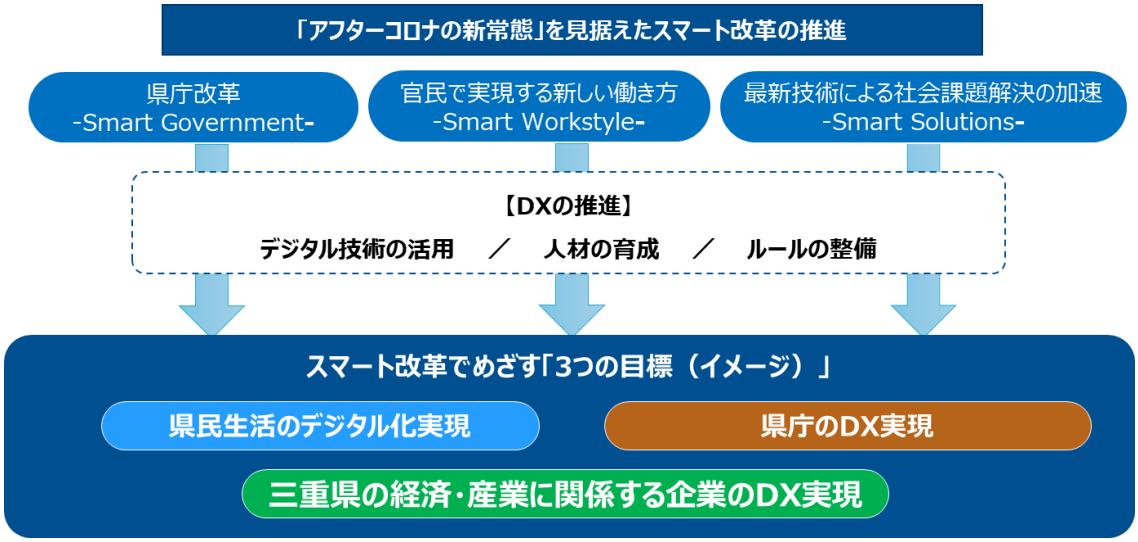


図 1-2-2 スマート改革推進の基盤となる DX

2.2 スマート改革でめざす「3 つの目標（イメージ）」と解決すべき課題

本計画では、スマート改革でめざす目標を、職員の生産性向上や多様な働き方を実現する「県庁の DX」、企業のビジネスモデル変革や新サービスの創造を実現する「三重県の経済・産業に関係する企業の DX」、そして最終目標となる「県全体の DX（＝県民生活のデジタル化）」の 3 つとしてイメージしている。

最終目標である「県全体の DX（＝県民生活のデジタル化）」を実現していくためには、「県庁の DX」を推進していくことが前提となり、本計画では、その推進基盤の整備を、国の「デジタル・ガバメント実行計画」「自治体 DX 推進計画」の計画期間にあわせて、2025 年度（令和 7 年度）までに実現していく必要があるとしている。

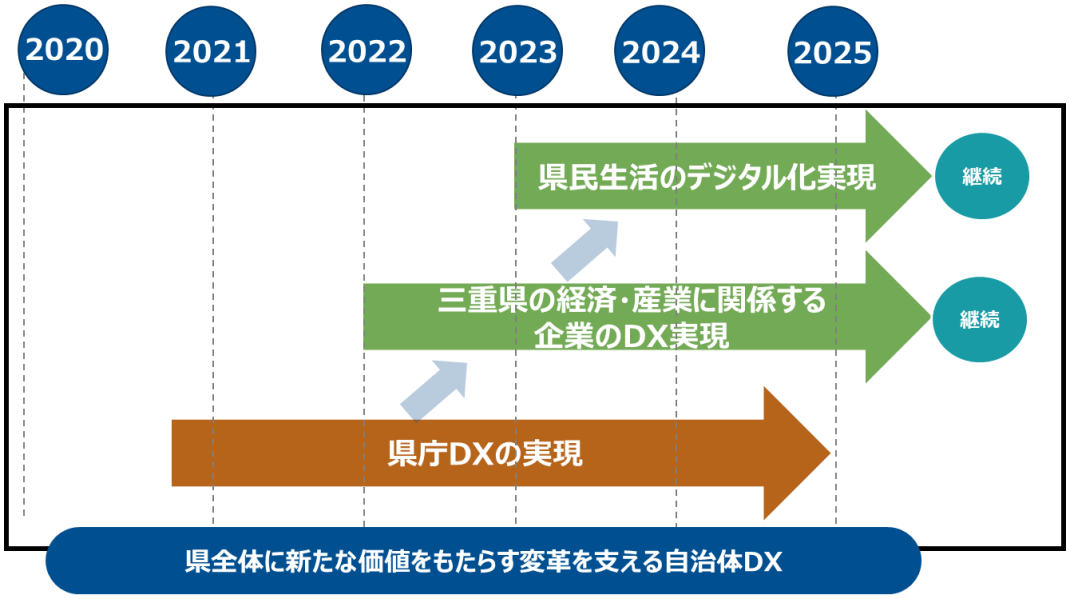


図 1-2-3 段階的なスマート改革推進

2.2.1 「県庁の DX」と課題

「県庁の DX」は、デジタル技術を活用して、業務効率化による生産性向上や、多様な働き方を推進することで、職員が企画立案業務や県民サービスの提供などの業務に注力できる状態をめざすものであり、この取り組みを支える執務環境等に関する課題を以下に挙げる。

(1) 執務環境等の見直し検討・実施

メールやグループウェア等の業務システム・アプリケーションについては大部分がオンプレミス方式であり、テレワークの推進など、新たな時代の要請に対応するため、クラウドサービスを活用する、執務環境等の見直し検討・実施に取り組む必要がある。

(2) 最適な強靭化モデルの見直し検討・実施

「三層の対策」強靭化モデルにより一定のセキュリティ強化が図られた一方で、LGWAN 接続系とインターネット接続系が分割されていることに伴う、利便性の低下や業務の非効率化を招いている状況にある。テレワークの推進など、新たな時代の要請に対応するため、早急に強靭化モデルの見直し検討・実施に取り組む必要がある。

(3) セキュリティ対策の強化

執務環境等や強靭化モデルの見直し検討・実施を進めていくためには、情報セキュリティ対策の強化は避けて通れない。特に、クラウドサービスの活用やテレワーク環境についてのセキュリティ対策は十分な検討と見直しが必要である。

2.2.2 三重県の経済・産業に関係する企業の DX（企業の DX）※参考

企業の DX は、「県庁の DX」の考え方と同様、企業がデジタル技術を活用して、ビジネスモデルの変革や新たなサービスの創出など、既存の価値観や枠組みを根底から覆すような革新的なイノベーションをもたらしている状態である。

2.2.3 県全体の DX（県民生活のデジタル化）※参考

「県庁の DX」と「企業の DX」が推進されることにより、市町を含めた、県域全体での行政手続や防災、医療・福祉、教育、さらには、民間サービスに至る様々な場面で付加価値の高いサービス提供が行われ、県民は、いつでもどこでも、簡単にこれらのサービスを利用できる日常になっている。

3. 課題解決に向けて

3.1 課題解決に向けての対策

「県全体の DX（県民生活のデジタル化）」には、最終的に、県や市町、企業等による、質の高いサービス提供を可能とする、共通プラットフォーム基盤の共同利用化などの枠組みが必要であると考える。

本計画では、その前提となる「県庁の DX」を推進する、県庁の「新たなコミュニケーション基盤」の整備に主眼を置いており、共同利用化の枠組みに関する具体的な検討を行うものではない。ただし、すべての県民が、いつでも・どこでも簡単に様々な官民のサービスを利用することができる、県全体の共通プラットフォームが将来的には不可欠であると考える。

なお、「県庁の DX」を推進する「新たなコミュニケーション基盤」に求められる対策については次の 3 つと考える。

- フレキシブルなコミュニケーション、多様な働き方を可能にするクラウドサービスの活用
- クラウドサービスの活用等に対応するネットワーク環境の見直し
- エンドポイントである職員を守る、強固な情報セキュリティ対策の実施

第2章　新たなコミュニケーション基盤の基本事項

1.　基本方針（基本的な考え方）

「新たなコミュニケーション基盤」の基本方針（基本的な考え方）を整理する前に、前章で触れた、「県全体の DX（県民生活のデジタル化）」に必要と考えられる、県や市町、企業等による共通プラットフォームのイメージを説明する。

計画では、クラウド利用をベースとした、だれでも・いつでも・どこからでも安全かつ柔軟にアクセスができる「三重県デジタルプラットフォーム（仮称）」（以下、「デジタルプラットフォーム」）として定義する。

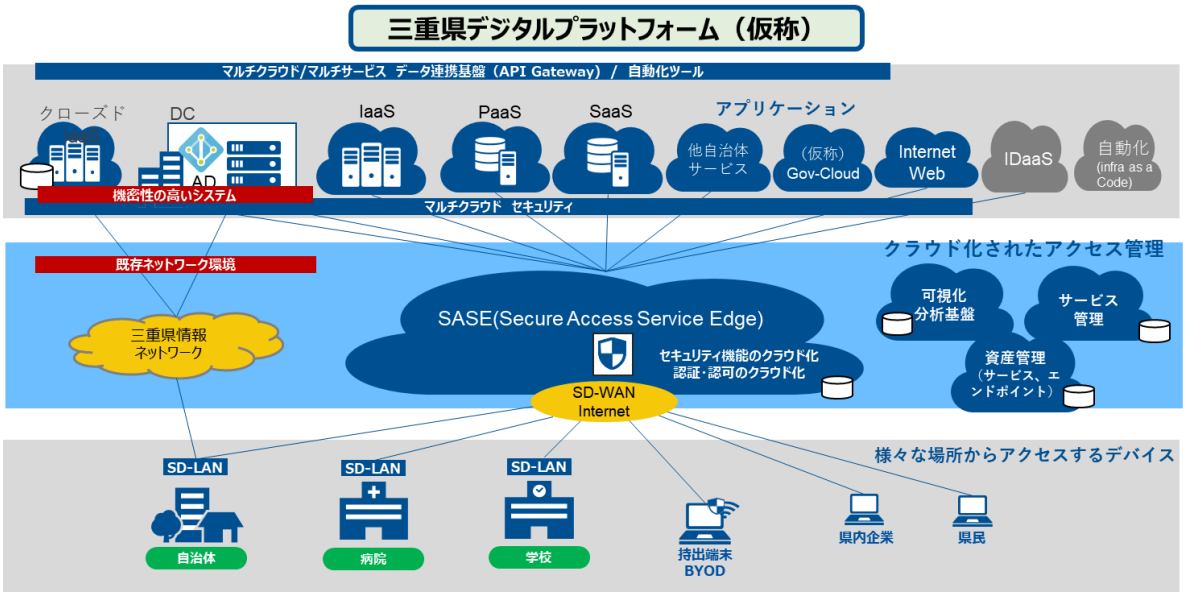


図 2-1-1　デジタルプラットフォーム概観（イメージ）

デジタルプラットフォームは、利用者がインターネットを介してどこからでも接続するという柔軟性と、クラウドベースの様々なサービスを自治体や企業が使い分けることが必要となるため、後述する「ゼロトラストネットワーク」と「SASE」による統合ネットワークシステムが考えられる。

1.1　ゼロトラストネットワーク

コロナ禍において、多くの企業や自治体がテレワークにシフトしたが、現在のテレワークで欠かせない技術となっているのが VPN（Virtual Private Network）である。

VPN は、ネットワークを流れる通信を暗号化して、仮想的に組織ネットワークに接続する技術のことである。しかし、コロナ禍で多くの企業等が一斉に VPN を使い始めたことにより、VPN が生産性の低下や、セキュリティリスクを高める可能性が問題視された。

具体的には、多くの利用者が VPN を使うことで、VPN のエンドポイント（受け口）の帯域容量が不足して応答が非常に遅くなったり、国内 900 以上の企業等で VPN 装置の欠陥をつかれた不正アクセスを受けたニュースが話題になったところである。

こうした VPN への不安が指摘される中で注目を浴びているのがゼロトラストネットワークの概念である。“すべての通信が信頼できない”という前提に立ち、ネットワークに接続するすべての利用者が誰で、どこから、どんな端末から通信し、どのデータにアクセスするのかといった情報に基づいて、組織ネットワークへのアクセス可否を決定することで、安全を確保する仕組みである。

現在、多くの IT ベンダがゼロトラスト関連の製品開発に取り組んでいる。

なお、現段階では、レガシーシステムへのアクセスは VPN を引き続き活用し、ゼロトラストを適用すべき部分から段階的に取り入れるなど、双方を併用する方法が現実的であると考える。

1.2 SASE（サシー、サージー）

ゼロトラストネットワークは“何も信頼しない”という前提で境界型防御を脱却する概念であり、それを実現するために必要なソリューション（セキュリティとネットワークを）を一元管理したフレームワークのひとつが SASE（サシー、サージー）である。SASE はコスト削減や業務効率化などのメリットももたらす。今後の情報セキュリティ対策のあり方を具現化するには、SASE をゼロトラストネットワークの構築に役立てるべきと考える。

ただし、SASE は最近登場したアプローチであるため、今のところ単一の SASE ソリューションは提供されていない。そのため、セキュリティを強化するためには、SASE のアプローチをセキュリティポリシーのベースとして、製品やソリューションの選定に役立てていく必要がある。

県のネットワークシステムについて、クラウドシフトを前提としたゼロトラストネットワークへの移行に着手した次の段階として、すべての県民の利便性向上に向けて、市町や企業などの関係者がデータ・システムを共通的に利用する枠組み（プラットフォーム化）をめざすことが重要となり、その際に中心となる技術が SASE であると考える。

SASE は Gartner が提唱しているアーキテクチャで、Security Access Service Edge の略であり、中心をデータセンターやオンプレからクラウドへ移行し、統合的な WAN 機能や統合的なネットワークセキュリティ機能を組み合わせる新しいアーキテクチャとして、近年注目されている技術である。

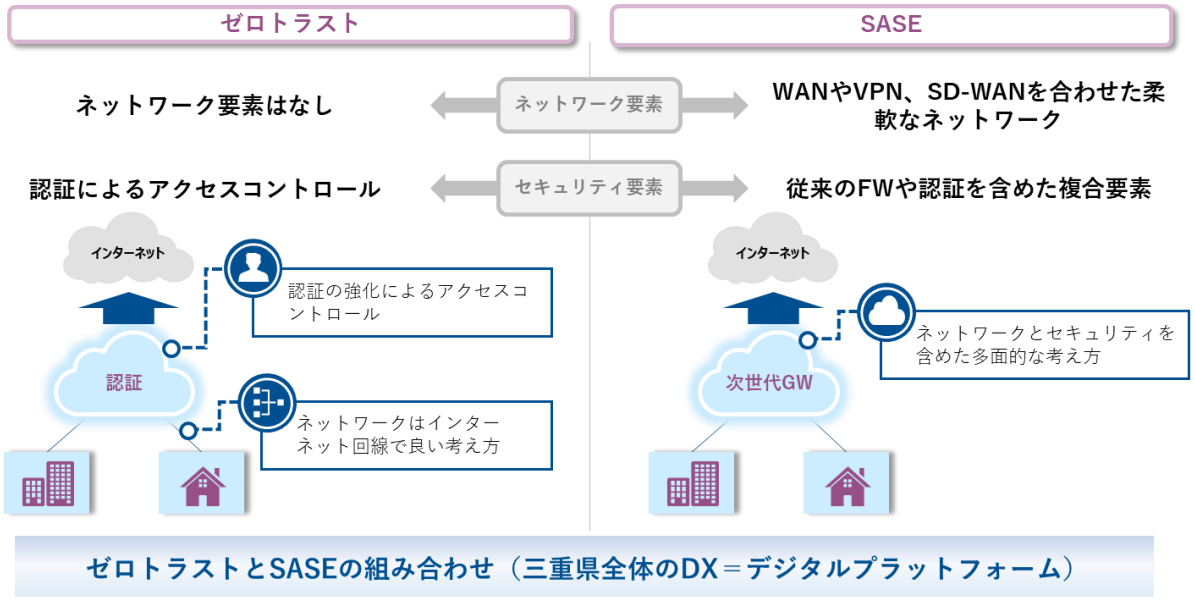


図 2-1-2　ゼロトラストネットワークと SASE の違い

1.3　整備の考え方

新たなコミュニケーション基盤は、庁内外の利用者がいつでもどこでもつながることができる、クラウド利活用を前提とした基盤である。当該整備は、その前提に基づき、段階的にクラウドシフトしながら、庁外利活用に必要なセキュリティ対策を図るよう進めることとする。

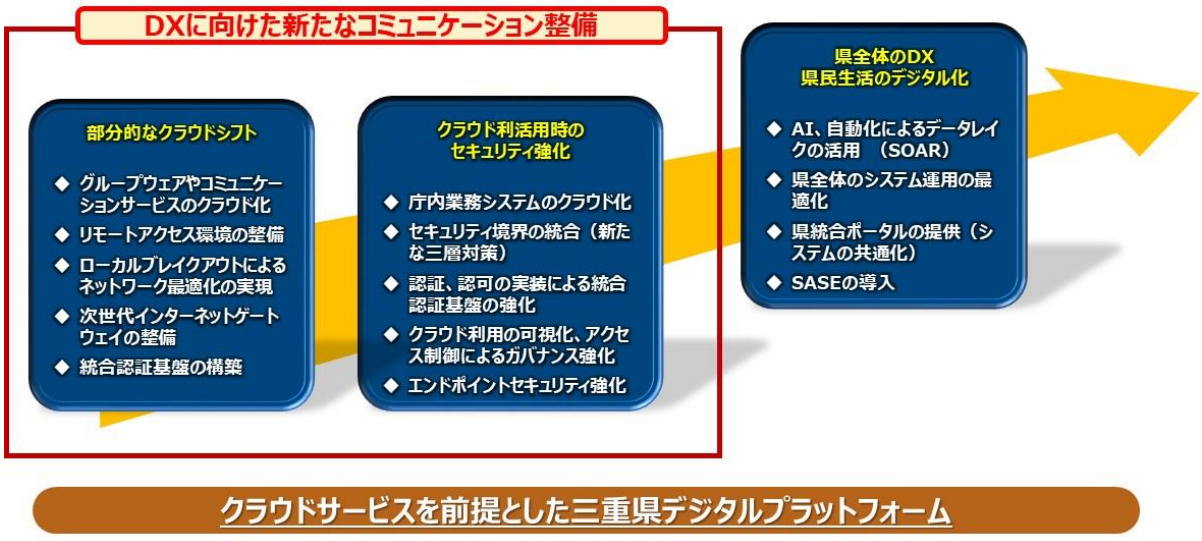


図 2-1-3　新しいコミュニケーション基盤整備の進め方

2. 整備の基本的事項

2.1 基本的事項

新たなコミュニケーション基盤は、次に掲げる 3 つの基本事項に基づき整備する。

2.1.1 クラウドサービスを前提とした職場環境の整備

働く場所や時間にとらわれない新しい働き方を可能とする、職員同士のコミュニケーションやデータ共有の仕組みを構築する。

2.1.2 強靭化モデル（三層の対策（三層分離））の抜本的な見直し

クラウドサービスの利用が前提となり、どこからでも業務を行うことが可能な環境が構築される。そのため、現行の三層の対策（三層分離）を抜本的に見直し、境界型の従来のセキュリティ対策からゼロトラストネットワークモデルへシフトする。

2.1.3 新たな情報セキュリティ対策（エンドポイントセキュリティ）

働く場所や時間にとらわれず業務を行うために必要なセキュリティ対策として、ゼロトラストモデルへのシフトとともに、エンドポイントである業務端末を守る仕組みを導入する。

3. 新たなコミュニケーション基盤の概要

DX の実現に向けた、新たなコミュニケーション基盤を整備するにあたり、その目的と必要な方策について検討を進めてきた。クラウドの利活用を前提とした職員間のコミュニケーション、全庁的な情報共有・活用の促進、セキュリティ対策の強化など、県庁の DX を推進する「新たなコミュニケーション基盤」の整備により、既存概念にとらわれず新たな価値を創造できる行政経営の環境が実現する。

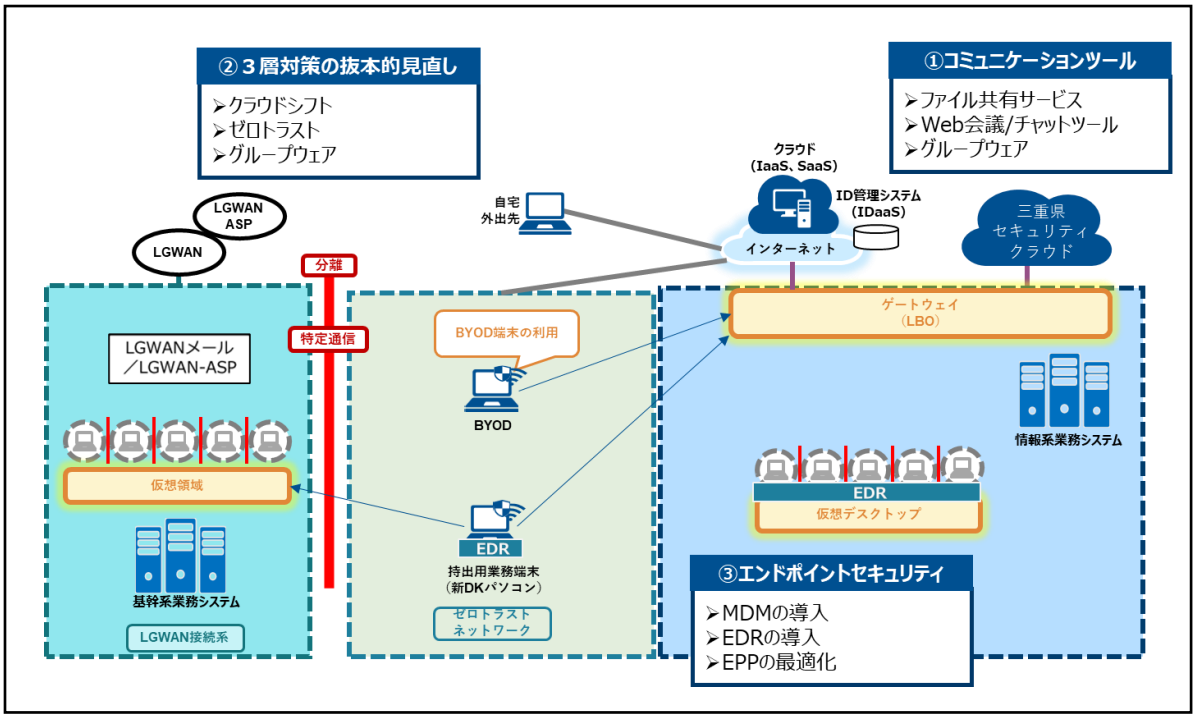


図 2-3-1 新たなコミュニケーション基盤概要図

第3章　具体的な方策

1.　クラウドサービスを前提とした職場環境の整備

今後、テレワークの推進などにより、場所や時間にとらわれない職場環境のあり方が重要になっていくことから、どのような環境であっても、業務効率性や生産性を高めていくことができるツールやアプリケーションの充実を図る。

1.1　　職員、関係者間のコミュニケーションの活性化

テレワークは、自宅や出張先などで業務を行うことが前提となるため、テレワーク先の職員と庁内の職員、さらには県民・企業・市町などの関係者とのコミュニケーションが可能となる環境を確保する。

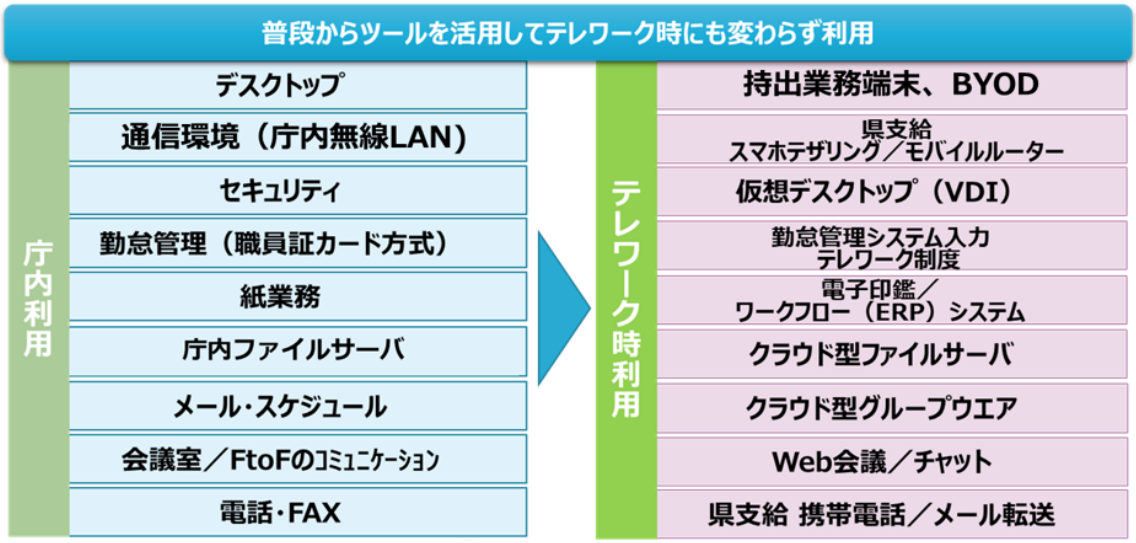


図 3-1-1　生産性向上につながる環境ツール例

1.1.1　　Web 会議／チャットシステム

テレワークでは、コミュニケーションを活性化するツールが必要であり、具体的には、Web 会議及びチャットツールの導入が有効である。

特に Web 会議については、機能や操作性、セキュリティ面とともに、映像・音声面で一定の品質を確保できることが重要であるため、利用者が集中した場合でも問題なく利用できるよう、ネットワーク環境の安定性も求められる。

また、これらのツールは、グループウェアやメール、ファイル管理等とも連携が可能で、職員が一体的に利用できることも重要な要素となる。

・ システム概要図

システムの概要を以下に示す。

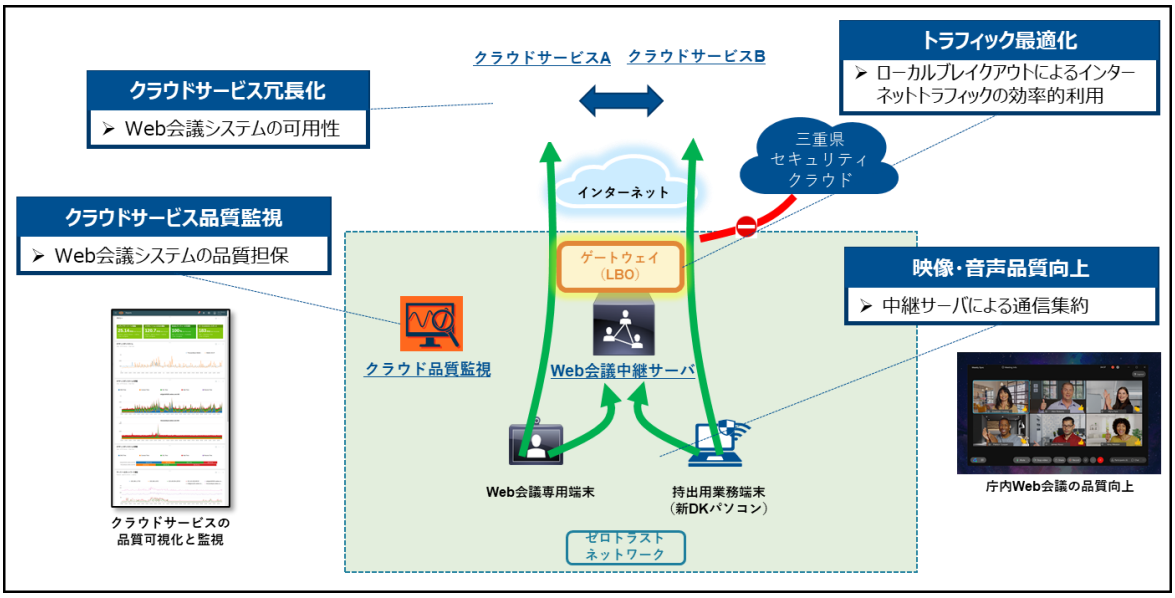


図 3-1-2 Web 会議システム概要図

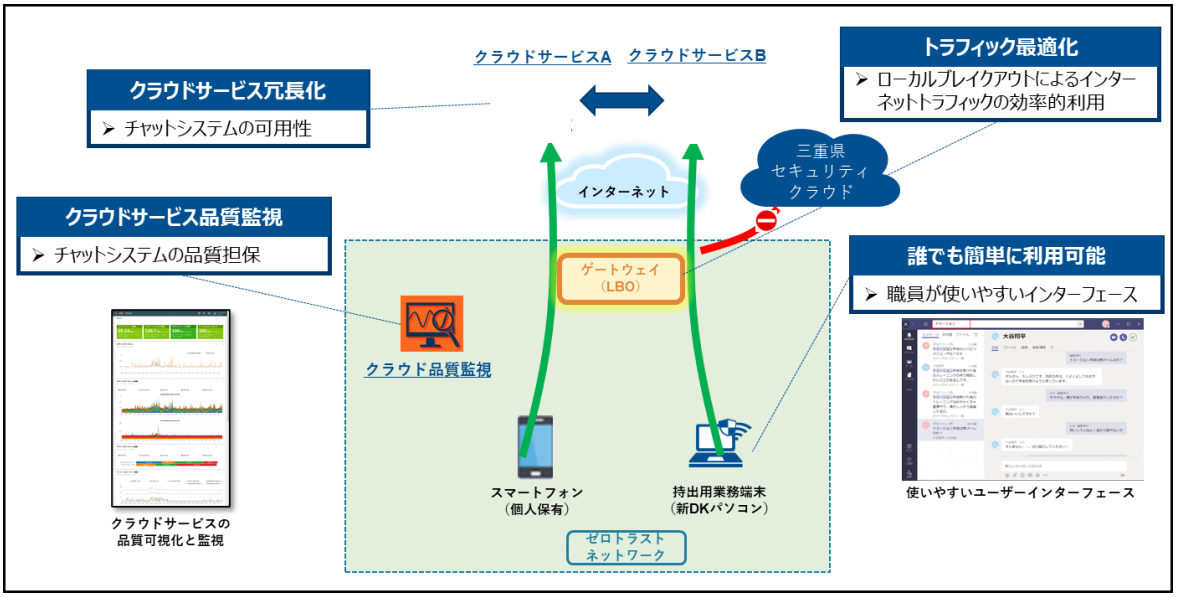


図 3-1-3 チャットシステム概要図

・ 機能要件

機能要件を以下に示す。

表 3-1-1 Web 会議／チャットシステムの機能要件

機能要件	
基本仕様	自治体への導入実績が多数あり、安定的に稼働しているシステムであること。 多くの OS やデバイスにも対応していること。 庁内 ID サーバ（将来的には IDaaS）との連携により認証を行うこと。
機能	クラウドサービスで提供されるシステムとして、職員同士が業務端末やスマートデバイス（将来的な BYOD の利用検討も視野）により、Web 会議やチャットができること。 （Web 会議の主な機能） 音声・ビデオ会議／テキストチャット／スケジュール設定／録音・録画／ミュート／投票／モバイルデバイス対応／在籍確認（プレゼンス）／デスクトップ・アプリケーション共有／ファイル共有・送受信／ホワイトボード／イベント対応 （チャットの主な機能） チャット（グループチャット／ダイレクトチャット／メンション）／検索／ファイル（アップロード・ダウンロード・プレビュー）／ビデオ通話

・ 可用性要件

可用性の要件を以下に示す。

表 3-1-2 Web 会議／チャットシステムの可用性要件

可用性要件	
クラウドサービス障害検知	クラウドサービスの障害発生時に、個々の利用ユーザに障害情報が送信されることはない。また、障害がすぐに報告されることは少なく、時間が経過されてから障害がアナウンスされることがあるため、利用しているクラウドサービスに対する監視機能を導入すること。
SLA（Service Level Agreement）	ベンダもしくはメーカが SLA を明示しているクラウドサービスを採用すること。また、品質面においても、導入ベンダもしくはメーカは、クラウド評価基準や各種認定（ISO、FISC、ISMAP）を有していること。

可用性要件	
システム冗長化	クラウドサービスであっても、トラブルが発生する可能性はオンプレミスでシステムを構築するのと同様である。そのため、クラウドサービスが利用できない時の代替手法（バックアップ）を準備することが重要である。相互互換性を事前に調査してクラウドサービスを選定すること。

・ 品質要件

Web 会議の品質要件を以下に示す。

表 3-1-3 Web 会議の品質要件

品質要件	
庁内環境の改善	庁内における業務端末からの接続については、Proxy サーバを経由した通信フローとする場合、通信遅延が発生する可能性がある。この点においては Proxy サーバを利用しない通信での利用を推奨する。なお、Proxy サーバを利用しない場合は、ファイアウォールなどによる外部からの攻撃防御も考慮すること。
庁内会議通信の最適化	Web 会議はクラウドサービスが基本ではあるが、庁内で利用する会議においてもインターネットを経由して通信をするのは、帯域の効率性が非常に悪い。そのため、庁内のみで利用する Web 会議は、オンプレミスで構築する中継サーバで通信を集約できることが望ましい。
ネットワーク品質の改善	Web 会議の品質要件は、主にパケットロス 1%以下、ジッター30msec 以下、遅延 150msec 以下といわれている。安定運用を確保するため、定常的にこれらを測定して、条件内に収まるよう品質を保持する。

表 3-1-4 Web 会議の映像・音声品質要件

品質要件	
音声の改善	音声については、業務端末側のスピーカーや、利用しているイヤホン及びマイクの品質に大きく左右される。Bluetooth イヤホンマイクは利便性は高いが、周囲の電波状況（干渉）により音声品質が劣化することもあるため、有線イヤホンマイクを利用することが望ましい。
会議専用環境の整備	コミュニケーションシステムは基本的にスマートデバイスや PC で利用するケースが多いが、知事レクや部長級会議等の重要性の高い会議については、密閉性の高い個々の会議室に専用装置を設置した上で Web 会議を行

品質要件	
	うことが望ましい。専用装置のネットワーク接続については、電波状況によっては品質が劣化する WiFi ではなく、有線による接続が望ましい。

1.2 データ共有、共同利用等による業務効率化

職員の業務効率化と生産性向上には、組織が保有するあらゆる情報（データ）の共有・活用が、安全かつスムーズに行えていることが重要な要素であり、さらに、庁内だけでなく、テレワーク等でもこれら情報へのアクセスが支障なく行え、活用できる必要がある。

1.2.1 グループウェア等の情報共有システム

テレワークの推進をふまえ、現在、庁内（LGWAN 接続系）ネットワーク内に整備・運用している情報共有システム（メールやスケジュール等のグループウェア）は、クラウドサービスに移行していくことが効果的である。

また、クラウドサービスを活用することにより、業務端末・専用端末だけでなく、一定のセキュリティ対策を講じることで、職員のスマートデバイス（ノート PC、タブレット、スマートフォン等）など各種端末からもアクセスが可能になる。

・ システム概要図

システムの概要を以下に示す。

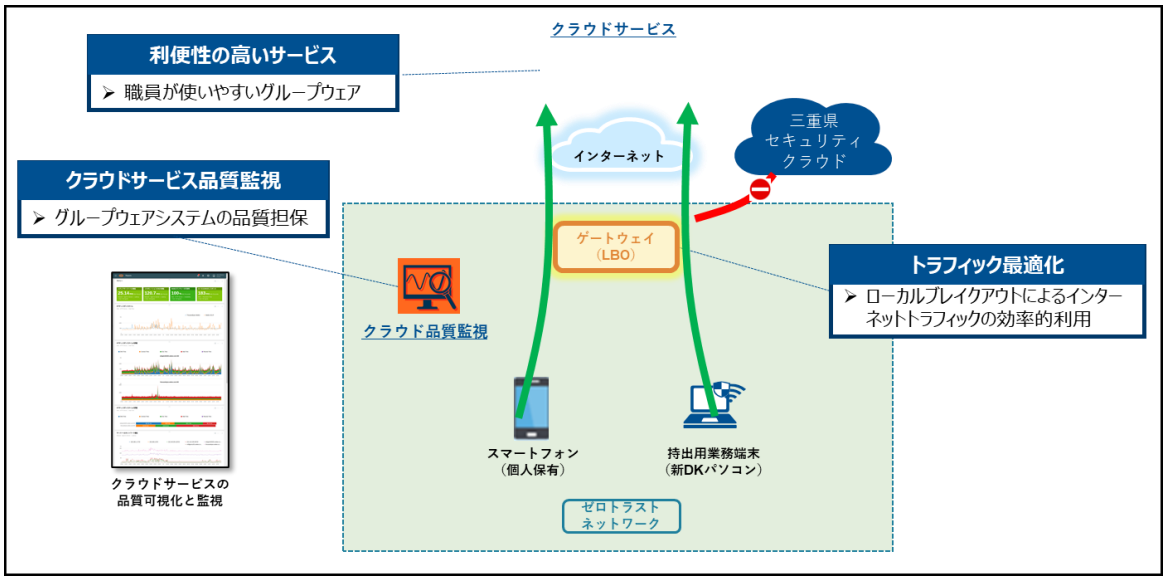


図 3-1-4 情報共有システム概要図

・ 機能要件

情報共有システムの機能要件を以下に示す。

表 3-1-5 情報共有システムの機能要件

機能要件	
基本仕様	自治体への導入実績が多数あり、安定的に稼働しているシステムであること。 多くの OS やデバイスにも対応していること。 庁内 ID サーバ（将来的には IDaaS）との連携により認証を行うこと。 二要素認証に対応していること。
機能	クラウドサービスで提供される情報共有システムとして、メールやスケジュール機能を有すること。メールについては、利用しているすべてのドメインが設定できること。 なお、本システムと各種コミュニケーションツールが連携して、スケジュールから会議を開催できること。 保管されているデータは、暗号化やアクセス制限などによりセキュリティを確保すること。
スマートデバイス対応	個人が保有しているスマートデバイスから、インターネットを経由して、安全にクラウドサービス側のグループウェアを閲覧できる機能を有すること。

・ 可用性要件

可用性要件については、Web 会議／チャットシステムと同等とする。

1.2.2 ファイル共有システム

情報資産の一元管理によるファイル活用・共同作業など、安全かつスムーズな情報活用を可能にするため、ファイルストレージのクラウドサービスを導入することが効果的である。

また、テレワーク時でも、庁内と同様にファイルの操作（閲覧やアップロード、ダウンロード、編集等）が行える必要がある。ただし、情報保護・セキュリティの観点から、利用者の属性に応じたダウンロードの制限や認証等の機能を必須とすること。

・ システム概要図

システムの概要を以下に示す。

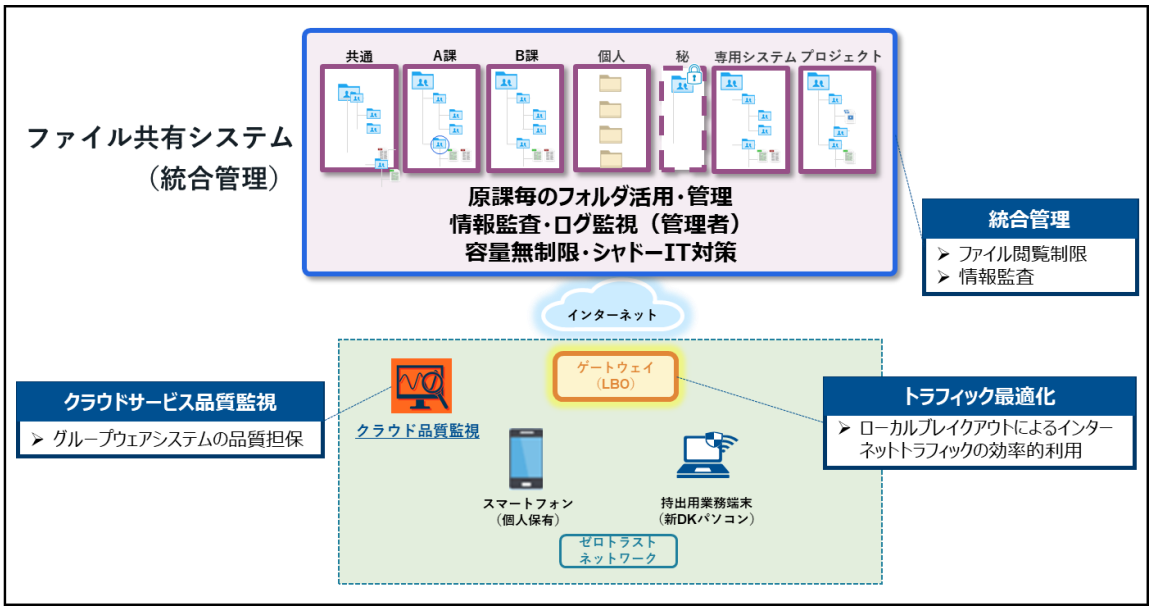


図 3-1-5 ファイル共有システム概要図

- 機能要件

システムの機能要件を以下に示す。

表 3-1-6 ファイル共有システムの機能要件

機能要件	
基本仕様	ファイル共有システムとして、自治体への導入実績が多数あり、安定的に稼働しているシステムであること。 多くの OS やデバイスにも対応していること。 庁内 ID サーバ（将来的には IDaaS）との連携により認証を行うこと。
機能	クラウドサービスで提供されるファイル共有システムとして、庁内の職員及び部局が利用できるファイルサーバ機能を有すること。 利便性を高めるため、現状のファイルサーバと同様、Windows 端末からエクスプローラーで閲覧可能であること。 保管されているデータは、暗号化やアクセス制限などによりセキュリティを確保すること。

・ 可用性要件

可用性要件については、Web 会議／チャットシステムと同等とする。

2. 強靭化モデル（三層の対策（三層分離））の抜本的な見直し

国の要請に基づき実施した「三層の対策（三層分離）」は、インターネット接続環境と LGWAN 環境を分断して、庁内の業務端末から直接インターネット接続を行えなくすることで、マイナンバー情報を含む庁内のセキュリティを確保する考え方である。一方で、今後、クラウドサービスへの移行を推進する、近年の国の方針に対応していくと、テレワークを含む業務端末が、庁内のシステムと外部（クラウドサービス）とを行き来することになるため、利便性の低下とともに、従来の境界型といわれる庁内監視の考え方だけではセキュリティ対策も不十分となる。

こうした状況から、早急に「三層の対策（三層分離）」を見直し、ゼロトラストネットワークをベースとした新たな強靭化モデルにシフトする必要がある。

表 3-2-1 境界型とゼロトラスト比較表

評価項目	三層の対策（境界型）	ゼロトラストネットワーク
セキュリティ対策の手法	多層防御	都度評価
庁外からの脅威	境界での防御	端末個々に防御
庁内からの脅威	無防備	拡散させない
業務系アプリケーションの利用	庁内ネットワークからのみ	どこからでも
利用できる端末	庁内で許可・管理されたデバイスのみ利用可能	BYOD を含めた様々なデバイスが利用可能
端末の管理	情報システム管理者で集中管理	職員が個々に管理
職員の利用できる場所	庁内の限定された場所	どこからでも

2.1 ゼロトラストネットワークへの移行

従来の、庁内にシステム基盤（データセンターやサーバ等）を設置する構成から、グループウェア／メール／ファイル共有等はクラウドサービス（IaaS や SaaS 等）を活用し、庁内ネットワークはゼロトラストネットワークへシフトする。今までの“庁内は安全である“という前提では、境界の外のやり取りを守れなくなる現状をふまえ、「すべてのトラフィックを信頼しないことを前提として検査・ログ取得を行う」、ゼロトラストネットワークへ移行する。

・ システム概要図

システムの概要を以下に示す。

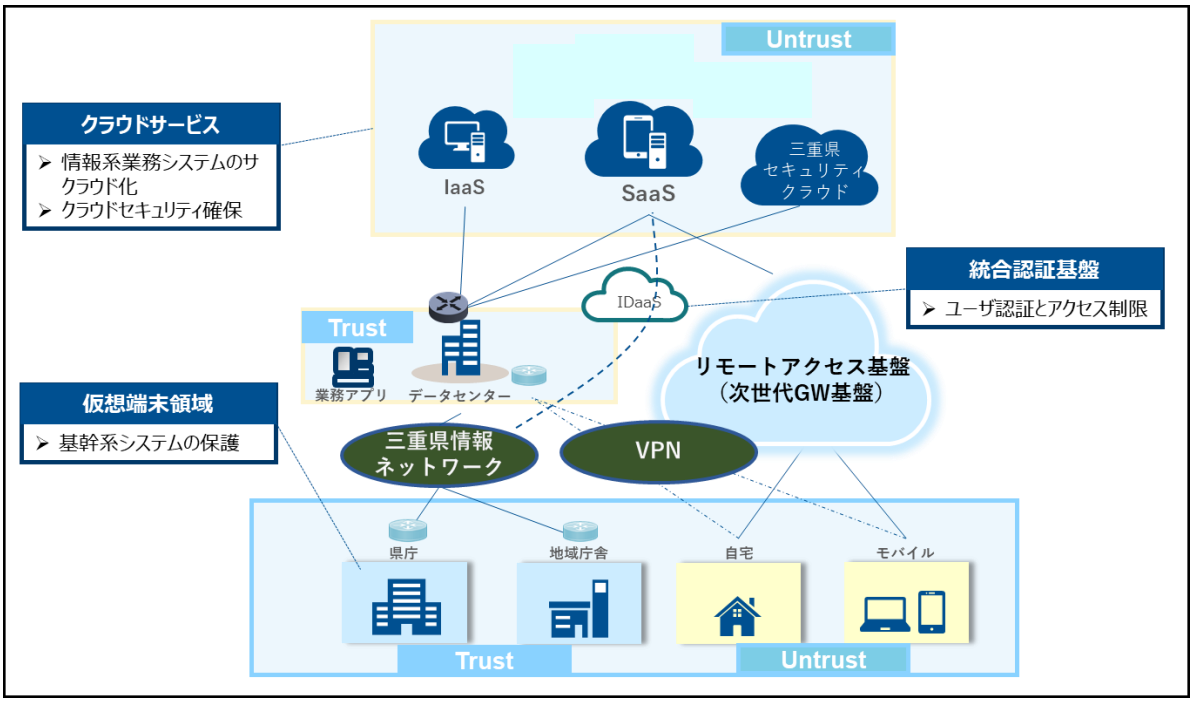


図 3-2-1　ゼロトラストネットワーク概要図

・ 構成要素

構成要素を以下に示す。

表 3-2-2　ゼロトラストネットワーク構成要素表

構成要素	詳細
ネットワーク機器	クラウドサービスを利用するためのインターネット回線を冗長化として導入すること。 庁内ネットワークと接続するためのファイアウォール及び L3 スイッチを導入すること。ファイアウォールについては SWG と連携して動作すること。 BYOD や業務端末を利用できるように、全庁に無線ネットワーク環境を整備すること。 業務端末を持ち出した場合にインターネット接続を行うための SIM 回線を導入すること。
SWG： Secure Web Gateway	URL フィルタやアプリケーションフィルタ、アンチウイルス、サンドボックスなどの機能をクラウド型で提供するサービス。アクセス先の URL や IP アドレスからその安全性を評価し、安全でないと評価された場合にはアクセスを遮断する。

構成要素	詳細
IAM： Identity and Access Management	「正しい個人を、正しい理由で、正しいリソースに、正しい回数アクセスさせる」ための情報セキュリティならびビジネス上の管理運用体系。 （ID アクセス制御機能） ID 作成・管理／アクセス管理／サービス／フェデレーション（シングルサインオン）
LBO： local breakout	特定のクラウドサービス向けのトラフィックについては、自治体情報セキュリティクラウド経由のインターネットを使わず、各拠点から直接アクセスするネットワーク構成とする。 各拠点に置いたルーターなどで通信内容を識別し、あらかじめ登録されたクラウドサービスであればインターネット回線、そうでなければ閉域回線とトラフィックを振り分ける。

2.2 仮想領域による基幹系業務システムの保護

県では、基幹系業務システムをはじめ、大部分のシステム・サーバが庁内ネットワーク内に存在しているため、クラウド活用及びゼロトラストネットワークと境界型のセキュリティ対策を行う、ハイブリッドな強靭化モデルを運用する必要がある。

・ 要求機能

要求機能を以下に示す。

表 3-2-3 仮想領域構成要素表

構成要素	詳細
基本仕様	企業・自治体への導入実績が多数あり、安定的に稼働しているシステムであること。 庁内 ID サーバとの連携により認証を行うこと。
中継サーバ	業務端末から仮想領域への接続を中継するサーバ。
仮想領域	業務端末上で仮想領域を構成し、基幹系業務システムのデータが外部に持ち出されないように制限を行う。 仮想デスクトップ方式または、大規模なサーバ基盤を不要とするアプリケーションラッピング方式など、コストや動作アプリケーション(※) の検証を行いながら最適な方式を採用すること。

構成要素	詳細
	（※）Office 製品など一般的に利用するアプリケーションや LGWAN 接続系から利用するシステムが仮想領域で動作できること。

・ システム概要図

システムの概要を以下に示す。

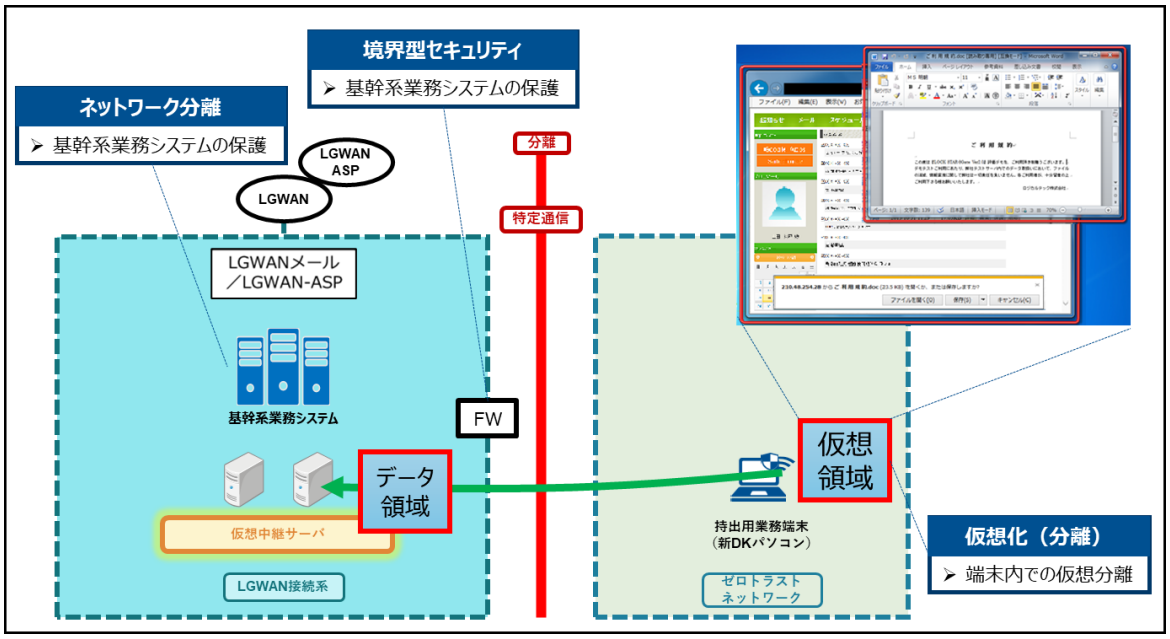


図 3-2-2 仮想化領域による基幹系システム保護概要図

3. エンドポイントセキュリティ対策

ゼロトラストネットワークをベースとした「強靭化モデル」の場合、エンドポイントとなる業務端末が常にインターネット側からの脅威にさらされることになる。サイバー攻撃・犯罪における手口の巧妙化など、セキュリティ上の脅威が増大している現状をふまえ、インターネットに接続する業務端末のセキュリティ対策となるエンドポイントセキュリティを強化する必要がある。

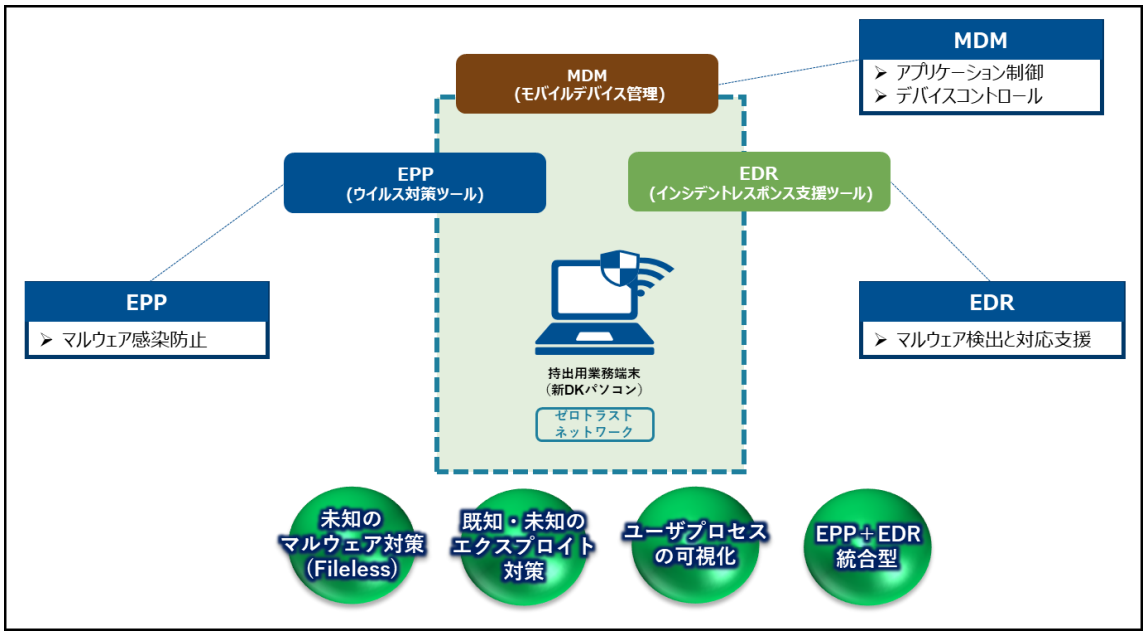
3.1 業務端末のセキュリティ向上

業務端末を管理対象として、遠隔で操作するための MDM（Mobile Device Management）を導入する。また、インターネットからの攻撃による不審挙動検知及び対応支援を行うため、EDR（Endpoint Detection and Response）を導入する。EDR は EPP（Endpoint Protection Platform）と連動して使うことで、セキュリティをより強化できるため、EPP の導入も同時に実施する。

・ システム概要図

システムの概要を以下に示す。

図 3-3-1 エンドポイントセキュリティ対策概要図



・ 要求機能

要求機能を以下に示す。

表 3-3-1 エンドポイント構成要素表

構成要素	機能
EDR : Endpoint Detection and Response	ユーザが利用するパソコンやサーバにおける不審な挙動を検知し、迅速な対応を支援するソリューション。具体的には、パソコンやサーバの状況及び通信内容などを監視し、異常、あるいは不審な挙動があれば管理者に通知する。
EPP : Endpoint Detection and Response	ユーザが利用するパソコンやサーバにおいて、既知ウイルスやマルウェアから保護するソリューション。いくつかの検知技術を組み合わせることでウイルスを検知し、自動的に取り除く。
SOC : Security Operation Center	EDR にて検知されたインシデントの分析を行い、その対策を支援する体制を整備すること。
MDM : Mobile Device Management	業務で使用するスマートフォンなどのモバイルデバイスのシステム設定などを統合的・効率的に管理するツール。

4. 採用製品の検討

ゼロトラストネットワークについては、他自治体においても検討が進んでいるものの、導入並びに運用の実績が少ない。そのため、採用する製品はゼロトラストネットワーク一式としての採用ではなく、導入実績がある個別システムを組み合わせた検討を行う必要がある。

5. ロードマップ（推進計画）

新たなコミュニケーション基盤については、現行システムの更新時期等を見据えて、効果的・公立的に整備することが望ましい。2021 年度（令和 3 年度）には庁内メールシステム・ID 管理システム（ユーザ認証システム）の更新、2022 年度（令和 4 年度）にはグループウェア、インターネット接続環境の更新に着手する必要があることから、これに合わせた最短のスケジュールとして、2021 年度（令和 3 年度）から 2022 年度（令和 4 年度）にかけて整備し、2023 年度（令和 5 年度）から運用できるロードマップとした。

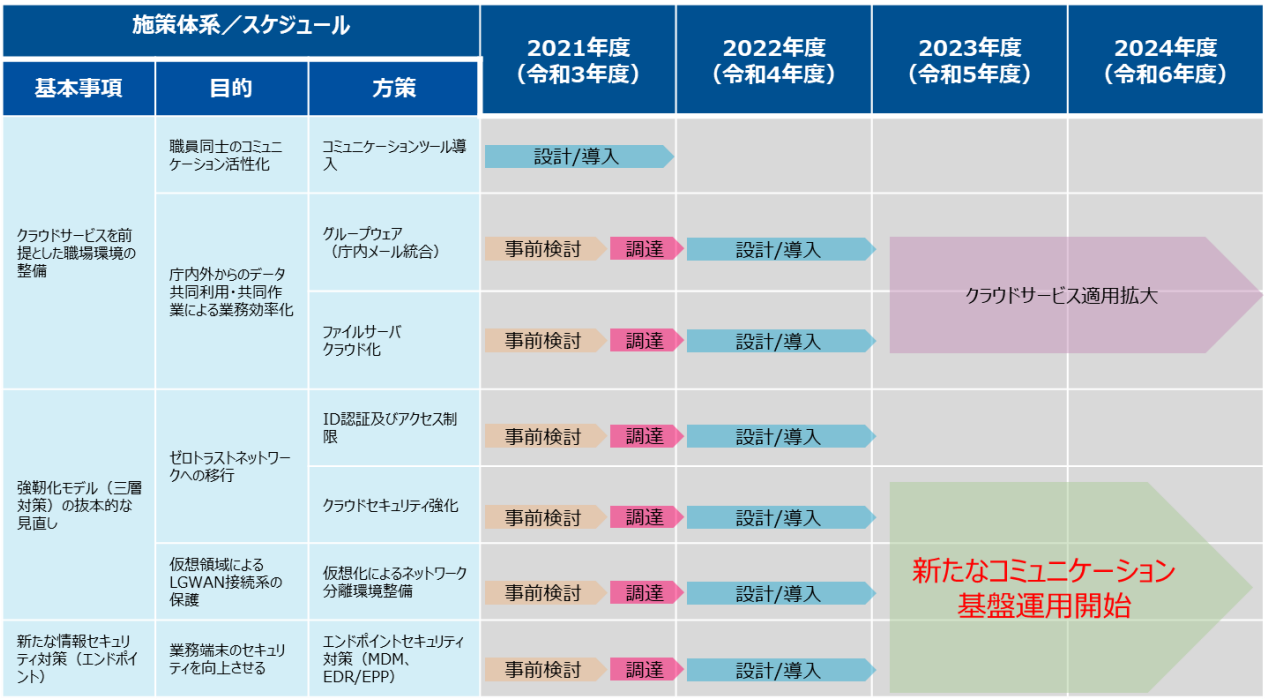


図 3-5-1 推進計画（ロードマップ）

第4章　今後の課題

1.　庁内システムのクラウド移行の促進

これまでの県における全庁ネットワークシステムは、オンプレミスによるシステムインフラを中心とした構成で調達を進めてきた。

クラウドサービスは、リソースの迅速な配備と柔軟な増減が可能で、自動化された運用による高度な信頼性や複数地域へのリソース配置による可用性の確保、サービスが提供する管理機能等を活用することによる運用負荷の低減が期待されるため、DX を抜本的に進めるためには、本サービスの積極的な利用に取り組むべきである。

新たなコミュニケーション基盤の整備とともに、今後、現行の各情報システムの更新時期に合わせて、クラウドサービスへの移行を段階的に進めていく必要がある。

2.　継続的な PDCA 推進体制の構築

弊社は、新情報ネットワークの基本計画（平成 30 年度）策定のタイミングで過去 5 年間を振り返り、現行ネットワークの課題整理や、新ネットワークのあるべき姿を実現するための設計及び構築計画の立案を行った。しかしながら、今回の新型コロナウイルス感染症への対策のように、計画策定時の想定を超える事態に迅速かつ適切に対応できるよう、課題の抽出と改善策の検討（PDCA サイクルにおいて、実行の結果を確認する C（評価）と評価結果を受けて改善活動を行う A（改善）にあたる取り組み）を継続的に行う仕組みが非常に重要であると考える。

弊社では、コロナ禍において、新たなテレワークやコミュニケーションシステムの導入に寄与してきたところであるが、本計画でめざす新たなコミュニケーション基盤の整備に向けて、PDCA サイクルの P（計画）、D（実行）の後に、実行の結果を確認する C（評価）と評価結果を受けて改善活動を行う A（改善）を行う枠組みを日常的な運用業務の中に組込むことを提言する。