【資料２】

新たなコミュニケーション基盤の整備に係る情報提供依頼（RFI）詳細

「新たなコミュニケーション基盤」については、令和３年３月に基本計画（【資料３】「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」）を策定しているが、本資料は、基本計画を踏まえ、基盤整備にかかる基本方針、基本事項、具体的取組等の想定（案）を整理したものであり、決定事項ではない。

１　基本方針

（１）めざす姿（理想状態）

「誰とでも、いつでも、どこでも、どんなアプリケーションでも、どんなデバイスでもつながる」職場環境の実現

（２）基本的な考え方

①職員エクスペリエンスの向上

企業において、顧客満足度の向上には社員のエクスペリエンス（職場で得られる経験価値）の向上が必要不可欠といわれているように、県においても、デジタル技術を取り入れ、より働きやすい職場環境を作ることで職員エクスペリエンスの向上につなげる。

②働き方の多様化

クラウドサービスをはじめとするデジタル技術を活用して、職員を「時間」や「場所」という制約から開放し、ワークライフバランスの実現や生産性の向上など、本当の意味での働き方改革を実現する。

③生産性の向上

業務をデジタル化することで情報連携がスピーディになり、作業効率の改善につながるほか、ビジネスチャットなどのコミュニケーションツールの導入により、全庁的なコミュニケーションの活性化と新たなイノベーションの創造につなげる。

（３）セキュリティの確保

コミュニケーション基盤の整備にあたり、前提となるのはセキュリティの確保である。庁内ネットワークは安全、外部は危険と見なし、外部からの通信を制限する従来の「境界防御」の考え方から、クラウドシフトは、情報資産の多くを、危険と見なしていた外部に保管する考え方に移行することとなり、今後、セキュリティの確保に向けた対策の発想を根本から変える必要がある。

２　整備の基本事項

（１）国の強靭化対策である「三層の対策」の見直し（イメージ等は４ページ）

【課題】利便性の低下・業務の非効率化（インターネット接続等）
【課題】業務端末等執務環境の制約（専用端末の活用等）
【課題】シャドーIT 対策（LINE での業務情報のやり取り等）
→（対応）

- 現在の「αモデル」から業務効率性・利便性の高い「β’モデル」に移行する
- テレワーク専用エリアとして「テレワークエリア」を新設する

- 業務システムは、移行が困難なものを除き、インターネット接続系に移行する
- 個人番号利用事務系及び「テレワークエリア」の端末を除き、全ての業務端末をインターネット接続系に移行する
- 業務システム・業務端末のエンドポイントセキュリティの強化を図る
- 「テレワークエリア」では約 2,000 台 (※1) の業務端末を活用する

（※１）テレワークエリアの端末
全職員数約 6,800 人うち、約 2,000 人が、業務端末を活用してテレワークエリアにおいてテレワークを実施する想定。

（２）各システムのクラウドシフト

【課題】庁内システム（オンプレミス）の操作性・利便性に対する改善要望

→（対応）

- オンプレミスで運用している、メール（職員間限定の庁内メール、通常のインターネットメール）やグループウェアをクラウドサービスの統合ツール（Google Workspace や Microsoft365 等）に移行する
- ビジネスチャット等の新たなツールの活用についても推進する
- 上記以外の庁内システムについても、クラウドサービスまたは別サービスへの移行に向けて積極的に検討を行う

実装する機能	整備により置換できる既存システム
（１）クラウドサービスの活用 ・統合ツールの導入 ※メール、グループウェア、チャット等 ※Google Workspace や MS365	・庁内メール ・インターネットメール ・グループウェア ・業務端末の OS 及び Office 関連
（２）三層対策の見直し ・ネットワークの構成変更 ・テレワーク環境の整備 ・業務端末のテレワーク通信費	・インターネット接続環境 ・在宅勤務システム (※2)
（４）エンドポイントセキュリティ ・ネットワークセキュリティ ・EPP/EDR ・認証基盤の一元化	

（※２）在宅勤務システム
コロナ禍での在宅勤務を推進するため、令和 2 年 6 月に緊急導入（試行運用中）。
職員は自宅(私有)端末から庁内ネットワークにリモートデスクトップ接続を行う。
最大同時接続は 1,300 台（人）。
・使用ツール（サービス）：VPN＋Soliton Secure Desktop

（参考）モバイルワークシステム
その他、専用端末（貸出端末）を活用したモバイルワークシステムを庁内ネットワークの整備運用（令和 7 年 12 月まで運用）の中で運用している。
・使用ツール（オンプレ）：VPN+仮想デスクトップ（最大 500 台同時接続）

（3）セキュリティ対策（例）

①認証機能のクラウド活用

- メールやチャット、ストレージなど、SaaS（Software as a Service）を使う際は、個々に ID とパスワードを設定して本人認証を行う。
- アクセス時は VPN から庁内の認証システムを経由する形が多いが、通信経路が増え、サービスが増えると操作も煩雑になることから、認証機能のクラウド集約等、ID とパスワードに依存するのではなく、多要素認証や条件付きアクセスなどの補強も要検討。

②通信経路とエンドポイントの保護

- サイバー攻撃が巧妙化している現状では、不審なサイトへの接続やマルウェアによる被害の危険性は絶えず存在する。
- 正式に許可していないクラウドサービスが使われる「シャドーIT」も課題であり、職員とデバイスを守る手段として、CASB や EPP／EDR が有効と考える。

（経路上の保護：CASB（Cloud Access Security Broker））

- CASB（キャスビー）は、県とクラウドとの間にコントロールポイントを設置して、利用状況を可視化、制御するシステム・サービスである。
- 許可した通信は行動をモニターし、情報流出につながるような動きがあればブロックするほか、未許可のクラウドサービスに対しては、接続される前に遮断する。

（エンドポイント保護：EPP／EDR）

- 境界防御の限界に対するソリューションとして、PC やスマートデバイス、サーバなど、ネットワークを構成するエンドポイントの単位でガードを固めるシステムやサービスを併用して活用する。

（セキュア PC）

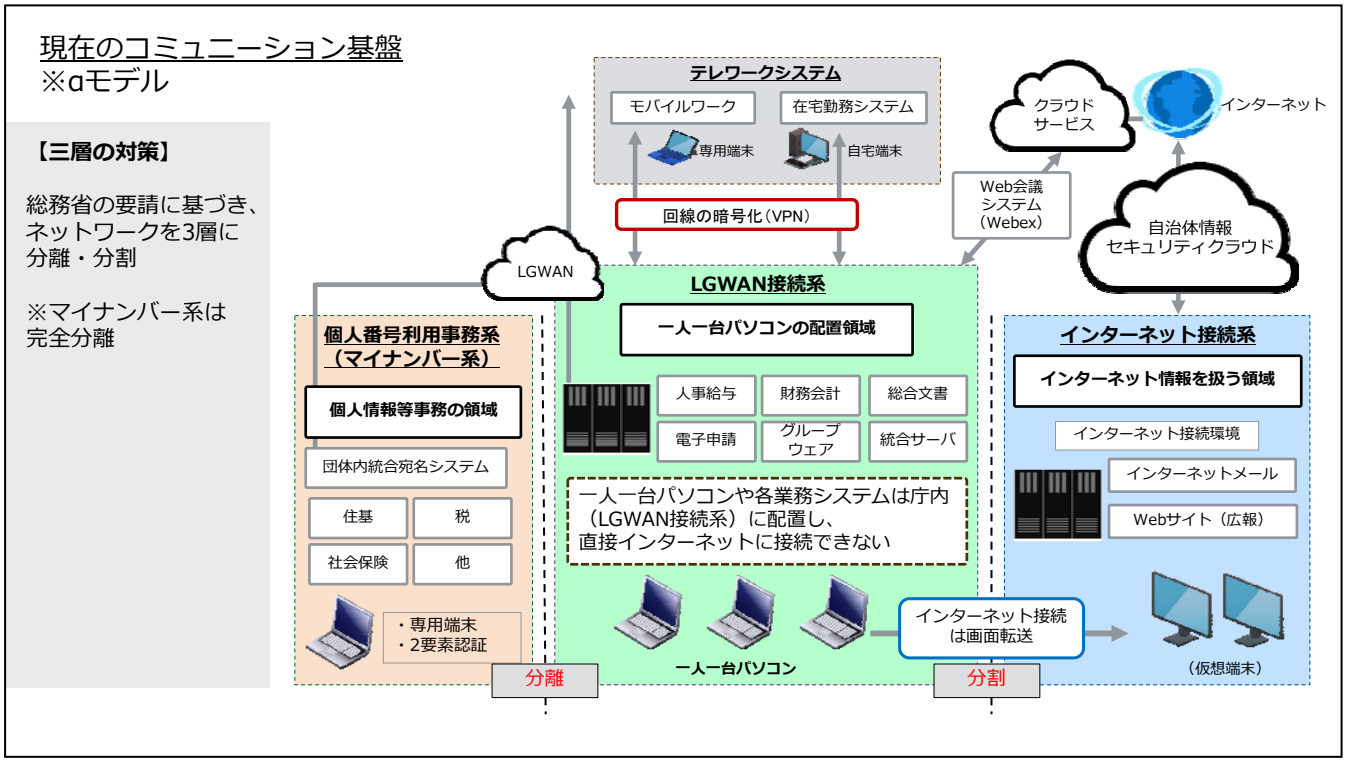
- 端末側のセキュリティ対策の 1 つであり、安全面を重視すれば、端末にプログラムやデータを保存しないシンクライアント型が有利だが、インターネット接続と庁内システムの経由が前提になるため、ファットクライアントに比べ機能と使い勝手は劣る。
- 高度なセキュリティ機能を搭載し、情報は一時的に保存できるなど、オフライン時のデメリットを軽減できるより高機能のセキュア PC を導入する事例も増えてきている。

③コンテンツセキュリティ

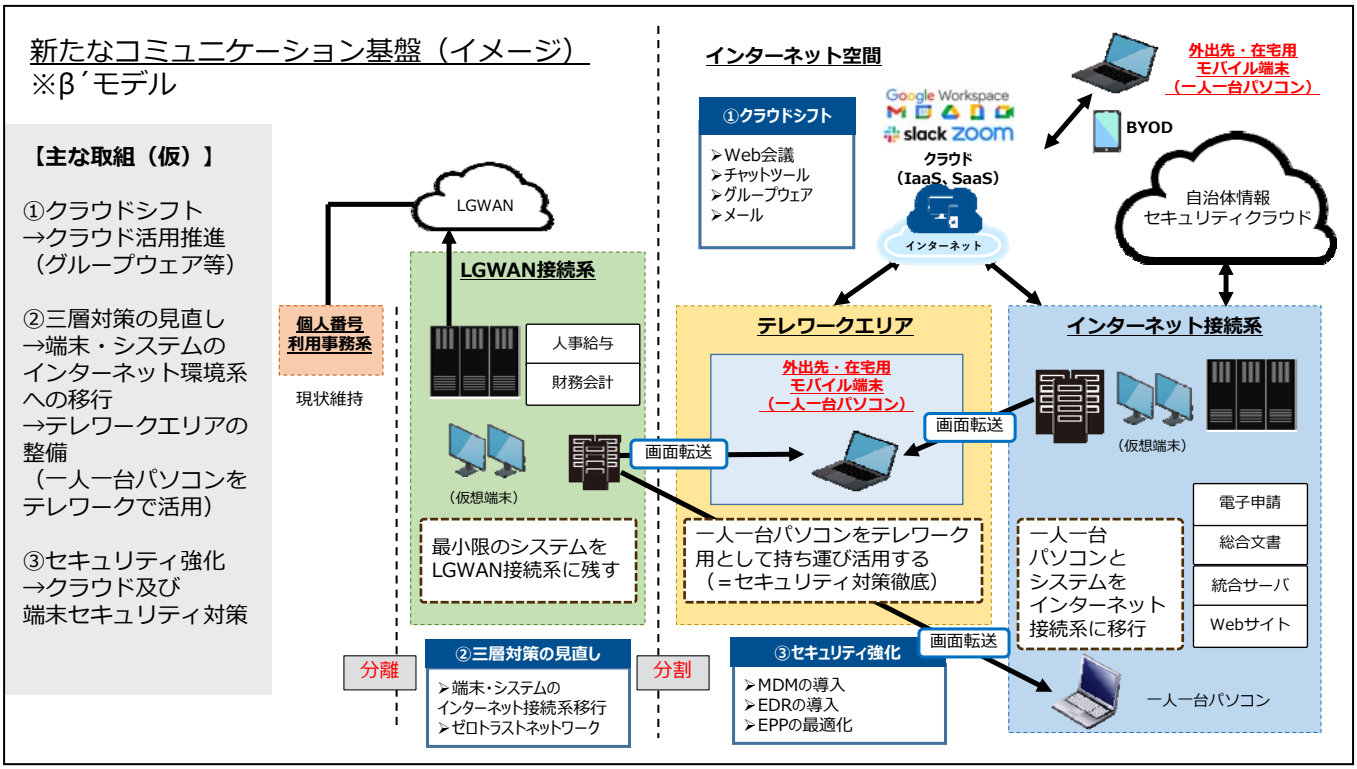
- データ流出は組織に大きなダメージを与えるため、例えばメールの誤送信対策、ファイルサーバの運用ミスなどを避ける体制の整備が必要である。
- 例えばメールの誤送信対策として、コンテンツをクラウド側で一元管理し、ファイルはセキュアなストレージに置いて、共有を許可した相手に URL だけを伝えるようにすれば、誤送信によるファイル拡散のリスクはなくなる。
- ストレージの容量も課題であり、増え続けるデータの扱いに苦慮し、個別にサーバ（NAS）を立ててやり繰りする所属も多く、大容量かつセキュアなクラウドストレージを活用することで、容量制限故にできなかったコンテンツの一元管理、版管理の負担軽減、検索時間の短縮などにより職員の生産性は上がり、維持管理のコストも削減できる。

3　整備の具体的取組

（現状：α モデル）



（整備イメージ：β´モデル）



（1）クラウドサービスの活用

①統合ツールの導入

Google Workspace やMicrosoft365 などクラウドサービスで提供されている統合ツールを導入する。

これらサービスにはメールやスケジュール、Web 会議（※3）、ビジネスチャット、ファイルストレージ等が含まれており、現行のメールやグループウェア等のオンプレミス（自主構築）の後継としていく（全職員約 6,800 人が使用）。

また、現段階の検討状況においては、個人所有端末（スマートフォン、タブレット含む）からも、統合ツール等のサービスに限り使用できることを想定している。

（※3）Web 会議

現在、県では、Zoom（Zoom ビデオコミュニケーションズ）と Webex（シスコシステムズ）のクラウドサービスを使用している。

今後登場する新たなサービスの動向や、本基盤の整備に向けた検討を踏まえながら、使用する Web 会議の考え方（組み合わせ等）についても随時検討していくこととなる。

（2）「三層の対策」の見直し

①ネットワークの構成変更

現行の「三層の対策」を見直し、業務端末（※4）や庁内の大部分のシステムを、現在の LGWAN 接続系からインターネット接続系に配置場所を変更し、パブリッククラウドの利用等、インターネット接続の利用増を見据えた県情報ネットワークの機器（ファイアウォール・プロキシサーバ等）の増強・構成変更を行う。

（※4）業務端末（一人一台パソコン等）

正規職員が使用する業務端末（一人一台パソコン）が約 5,700 台、非正規職員が使用する業務端末が約 1,100 台でノートパソコン型。

現在、LGWAN 接続系に配置し、令和元年度から令和 2 年度にかけて、一人一台パソコン約 1,800 台をモバイル型（13.3 インチ）に更新したところである。

②テレワーク環境の整備

新たに整備した「テレワークエリア」の端末（外出先での端末を想定）からインターネット接続系及び LGWAN 接続系を利用するための仮想デスクトップ環境を整備する。現段階では、「テレワークエリア」から、LGWAN 接続系への接続は 500 台程度、インターネット接続系への接続は 2 ,000 台程度を想定。

ただし、VPN と仮想デスクトップの組み合わせについては、VPN の脆弱性問題のほか、オンプレミスで整備する仮想基盤のフレキシブルな変更が困難なことから、セキュアかつ利便性に優れた新たな方式があれば検討を行うこととする。

③業務端末のテレワーク通信費

テレワークエリアで活用する端末（2,000 台想定）の通信費（現状においてはインターネット VPN を使用）。

（3）セキュリティ

①ネットワークセキュリティ

例えばクラウドサービスを活用した認証の一元化により、職員の利便性とともに、多要素認証や条件付きアクセスなどを用いた安全性の向上を図る。

また、近年、新たな概念として取り入れられはじめている SASE（総合脅威管理）の採用も検討する。

②エンドポイントセキュリティ（EPP/EDR）

エンドポイント対策として主流とされる EPP と EDR を実装する。

EPP はマルウェアや攻撃メールなど外部からの脅威を遮断するシステムや技術、一方の EDR はガードをすり抜けた攻撃を検知し、封じ込めるためのソリューションで、役割分担は異なるため、両者の採用を検討する。

また、本基盤の整備にあわせて、自宅（私有）端末を活用している現行の在宅勤務システムは原則廃止を想定しているが、整備後、引き続き個人端末（スマートフォン、タブレット含む）から統合ツール等のサービスに限り使用できる想定とするなど、これらを可能とする効果的なセキュリティ対策を検討する（※5）。

（※5）個人端末の活用

個人端末から統合ツールへの接続は、利便性向上を図るため、庁内ネットワーク経由ではなく、直接サービスに接続できることを想定（全職員 6,800 人）

③認証基盤の一元化

クラウドサービスを活用した認証の一元化（例：IDaaS : Identity as a Service）により、職員の利便性とともに、多要素認証や条件付きアクセスなどを用いた安全性の向上を図る。