地方公共団体向けβ'モデル移行に向けた手順書

総 務 省

令和６年３月29日

総務省自治行政局

デジタル基盤推進室

目次

１．はじめに

本書の目的

- 総務省は、平成27年の日本年金機構における情報流出事案を受け、平成27年11月に取りまとめられた「自治体情報セキュリティ対策検討チーム」の報告を踏まえ、地方公共団体に対して情報セキュリティの抜本的強化策である「三層の対策」を講じるよう要請。

- 「三層の対策」の効果や課題、新たな時代の要請を踏まえ、セキュリティの確保と効率性・利便性向上の両立の観点から、情報セキュリティ対策の見直しを実施し、その内容を「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(令和2年版)」に反映した。業務端末をLGWAN接続系に配置するαモデル（従来モデル）に加え、**利便性を高めるため、高度なセキュリティ対策を実施することを条件に、インターネット接続系に配置するβモデルとβ'モデルを示した**。

- 社会全体のデジタル化の進展とともに急速なクラウドサービスの普及が広がっており、デジタル化を進めるための様々な場面でインターネット接続が必須なクラウドサービスを業務で利用する需要も高まっている。地方公共団体においても、クラウドサービスをインターネット接続可能なβ´モデルは多様な働き方を前提としたセキュリティ対策となり得る。
- 自治体から、「β'モデルへ移行したいが具体的な手順が分からない」「作業イメージがつかない」等の意見が出ている。

目的

本手順書において以下を示すことで、β'モデル導入を検討する自治体が、計画的に円滑に移行を進められるようにする。

- **作業項目やフェーズ毎に想定される主な作業手順等**
- **既にβ'モデルに移行している自治体の事例**

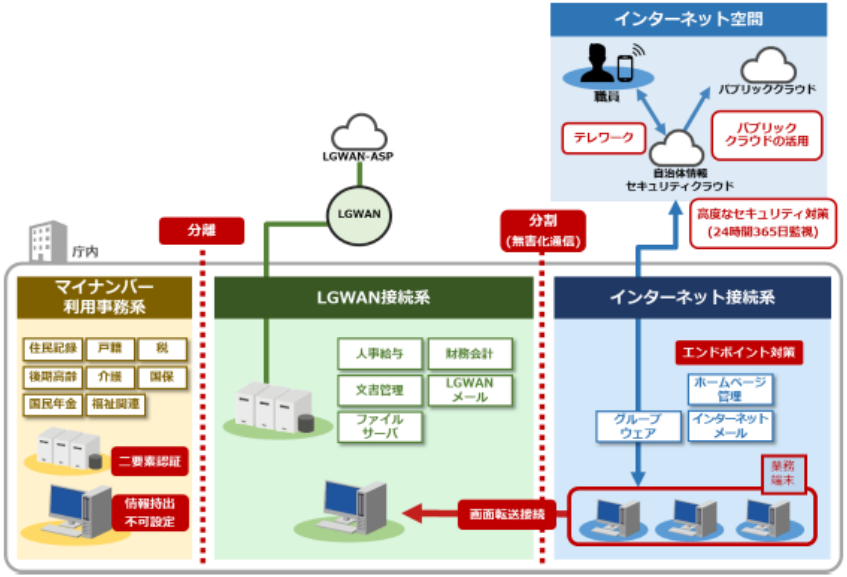
（ご参考）βモデル、β´モデル

令和２年度ガイドライン改定により、業務端末をLGWAN接続系に配置するαモデル（従来モデル）に加え、利便性を高めるため、高度なセキュリティ対策を実施することを条件に、インターネット接続系に業務端末を配置するβモデルとβ'モデルを示している。

βモデル(重要な情報資産配置なし)

業務効率性・利便性：中　**必要な対策のレベル：中**

- インターネット接続系に主たる業務端末を配置
- セキュリティリスクを考慮し、EDR等の技術的対策に加え、緊急時即応体制の整備等の組織的、人的対策の確実な実施が条件

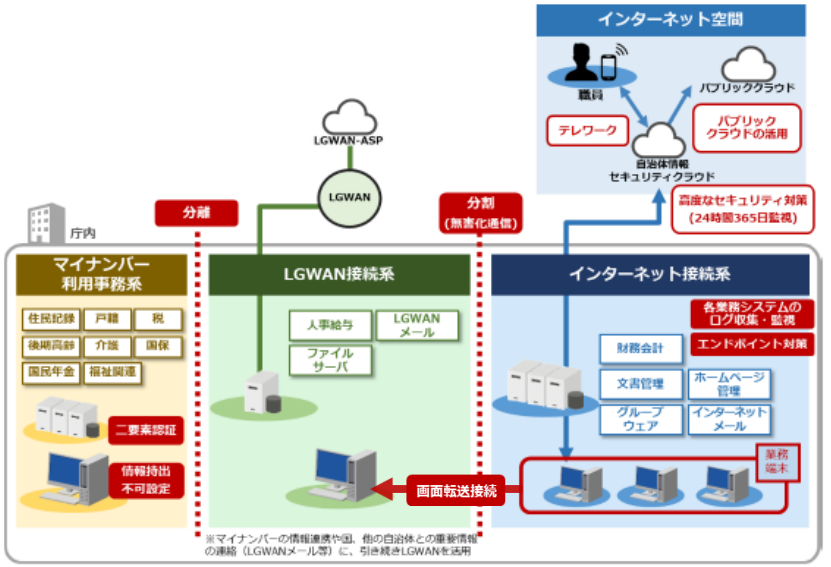


βモデルイメージ図（図表28）

β'モデル(重要な情報資産配置あり)

業務効率性・利便性：高　**必要な対策のレベル：高**

- βモデルに加え、文書管理、人事給与、財務会計等の業務システム（マイナンバー利用事務系を除く。）をインターネット接続系に配置
- βモデルの技術的対策、組織的、人的対策の確実な実施の条件に加え、情報資産単位でのアクセス制御、組織的なセキュリティ対策基準の遵守、セキュリティの継続的な検知・モニタリング体制の構築が条件

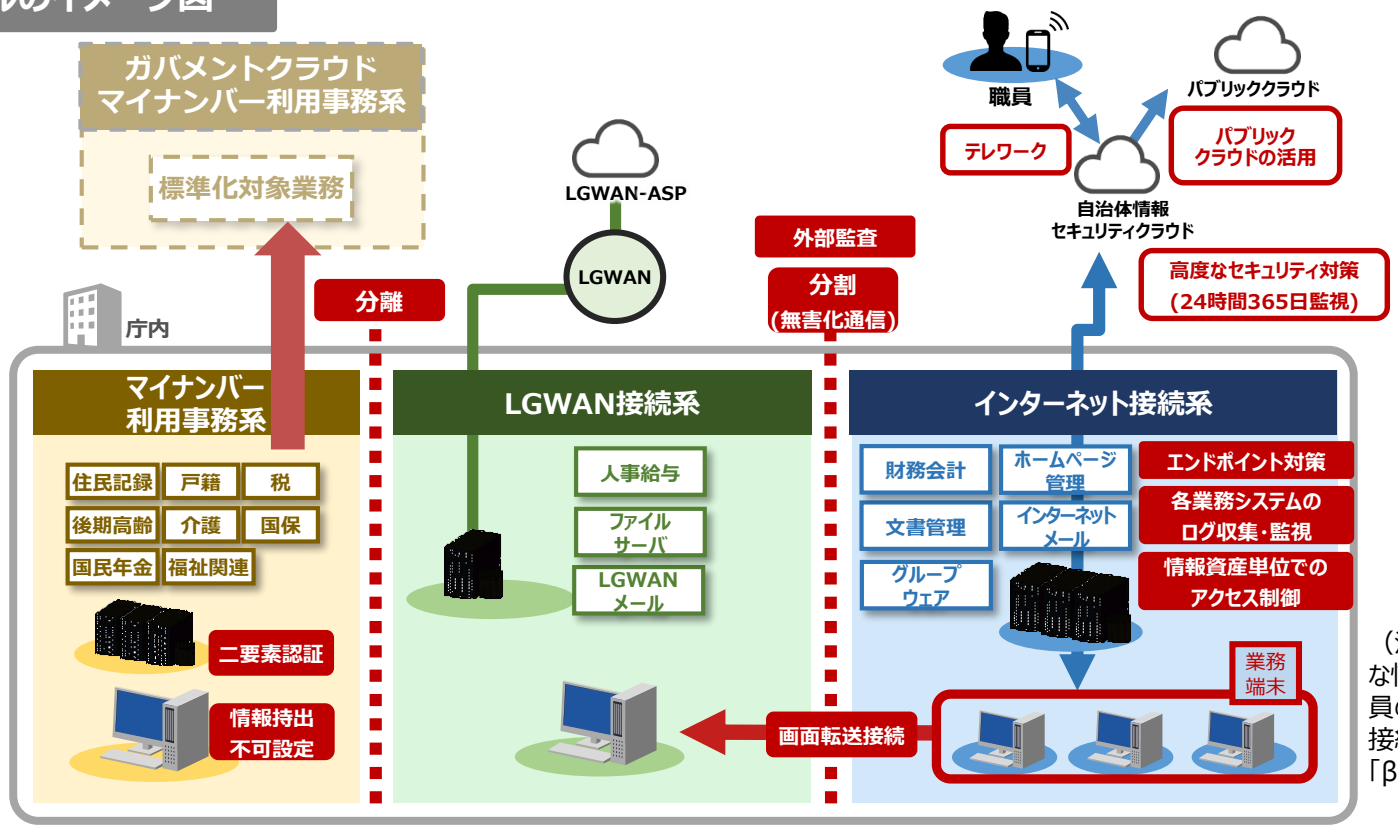


β'モデルイメージ図（図表30）

β´モデルについて

- ✓ 地方公共団体の業務で広く活用されているサービスがクラウド上で提供されるようになっており、インターネットと接続可能な領域に業務環境を配置する必要性が高まっていることを受け、インターネット接続系に業務端末・業務システムを配置したβ´モデルに対するニーズが高まっている。
- ✓ インターネット接続系の業務端末に対するエンドポイント対策、各業務システムのログ収集・監視など、従来の境界型防御にとどまらない追加のセキュリティ対策を行うことが求められる。

β´モデルのイメージ図



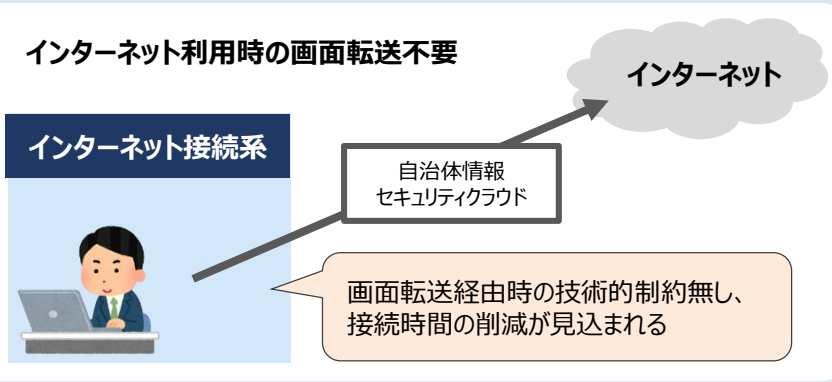
（注）βモデルのうち、重要な情報資産(入札情報や職員の情報等)をインターネット接続系に配置する場合は「β'モデル」としている。

※β´モデルの採用には、技術的対策に加え、緊急時即応体制の整備等の組織的・人的対策の確実な実施が条件

β´モデルのメリット（インターネットサービスの利用拡大）

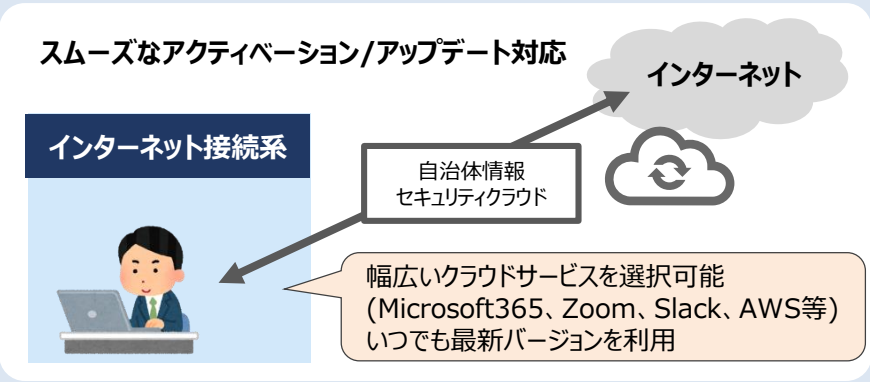
インターネットへの直接接続

- インターネット上のサイト、サービス、オンライン会議等を画面転送(VDI)経由ではなく一般のブラウザ（Microsoft Edge、Google Chrome等）で利用可能



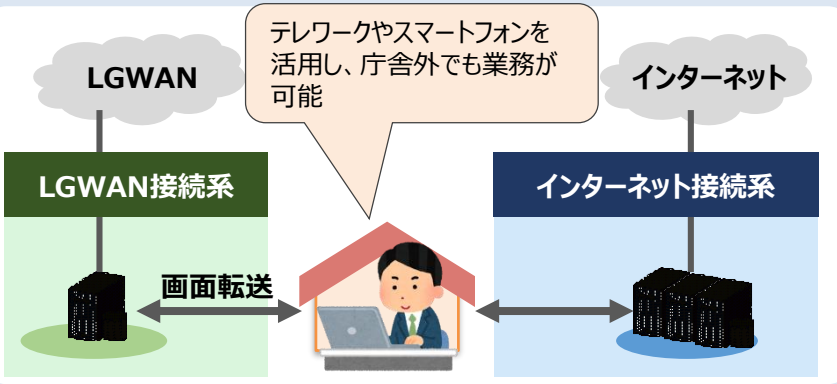
最新かつ多様なクラウドサービスの活用

- クラウドサービス利用時のアクティベーション(認証)がスムーズ
- 最新の資産、定義体ファイル等に随時更新可能
- ソフトウェアのアップデート対応自体が不要になる場合も



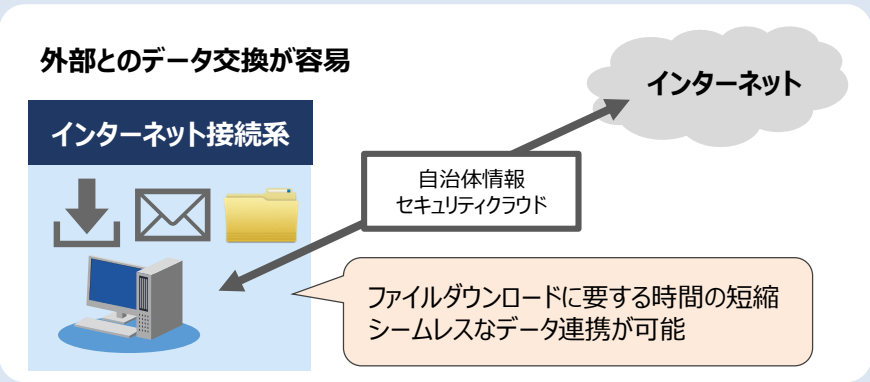
庁内/庁外用端末の統合

- 業務端末を集約し、効率の良い業務環境を実現
- バージョン管理や端末貸出し対応の負荷軽減
- テレワーク規模拡大により働き方改革にも貢献



同一セグメントでの業務完了

- 外部とのファイル交換やメールの送受信を同一セグメントで実施
（通常はファイルをLGWAN接続系に取り込む必要が無いため、無害化処理が不要となる※無害化処理を残す場合有り）



β´モデルのメリット（βモデルとの比較）

画面転送システムの規模縮小

- αモデルは、インターネットへの閲覧はほぼ全職員が必要となるため、LGWAN接続系からインターネット接続系への画面転送の必要数は大規模となる。
- βモデルは、グループウェアのみインターネット系に移行するため、その他のLGWAN接続系業務に残った業務システム利用において画面転送が必要であり、インターネット接続系からLGWAN接続系への画面転送必要数は中規模となる。

<βモデル>

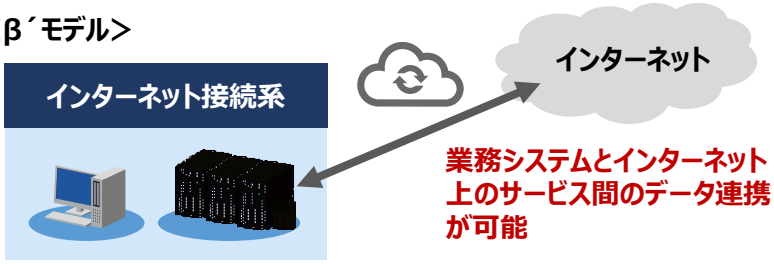
- β´モデルは、グループウェア以外の業務システムもインターネット系に移行するため、インターネット接続系で完結できる業務が増えることにより、インターネット接続系からLGWAN接続系への画面転送必要数は小規模となる。

<β´モデル>

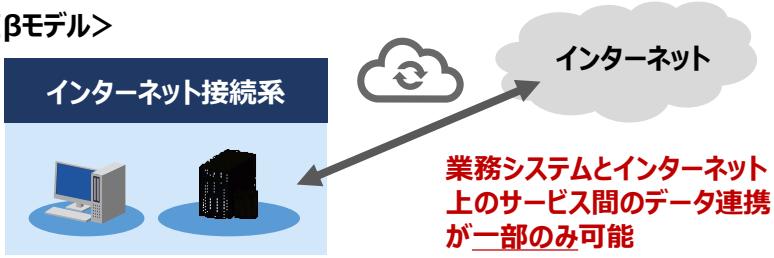
最新かつ多様なクラウドサービスの活用

- インターネット接続系に配置した業務システムについては、インターネットがシームレスに接続されるため、アクティベーションや資産アップデートが可能となる。一方、βモデルはインターネット接続系に配置した一部の業務システムのみがその対象となる。

<β´モデル>



<βモデル>



βモデル採用の理由

・業務システムをインターネット接続系に配置した場合のセキュリティリスクを考慮し、業務端末のみを移行する。

・最終的にβ´モデルへの移行を試みる場合でも、庁内スケジュール等を考慮し、段階的に移行する場合は、一時的に業務端末のみインターネット接続系に配置する(βモデル)場合がある。

自治体アンケートに基づくβ´モデル移行における主な課題

検討に係るノウハウ・人材不足

- ネットワーク変更に伴う影響範囲を把握し、あるべきシステム構成・事業計画を立案するにあたり、技術的スキルや人員確保が必要となる

・情報システム機器等の配置や構成の根本的な見直しなるため、それなりの検討期間と体制確保が必要
・β'モデル移行の舵取りできる人材不足
・LGWAN-ASPで業務を集約しており、インターネット接続系に業務システムが簡単に移行できない　等

セキュリティ対策の強化

- セキュリティ脅威の増加に対する適切な対策群の検討及びそのために必要な情報資産の洗い出し

・住民情報を多く扱う性質上、β'モデルに向くのか判断が付かない
・業務端末や業務システムが外部脅威に晒されるため、αモデルに比べ情報漏洩対策の更なる強化と徹底が必要
・職員のセキュリティ意識不足が心配　等

移行に係るコスト増加

- ネットワーク移行に伴う経費や関連システムの設定変更、新たなセキュリティ対策に必要な経費について、コスト増となる

・導入維持コストの増加が心配
・EDRなどの追加セキュリティ対策、クラウド利用に伴う回線費用の増加など現行予算より大幅な増額となる見込み　等

適切な移行時期の見極め

- 全庁的な業務環境見直しを伴うものであり、仮想基盤やアクティブディレクトリなど全庁共通システム群も関連する場合が多く、適切な移行タイミングを設定するのが難しい

・各システムの更改時期がことなるため、調整が難しい
・標準化システムと改修タイミングが重なるため
・次期端末入替のタイミングで移行したい
・庁舎移転にあわせモデル移行することを検討する　等

２．移行プロジェクト推進にあたって

本書のアプローチ

β´モデル移行時に課題とされる事項に対し、先行事例(既にβ´モデルへの移行を完了された団体)に基づき、検討時の参考となるよう、本書にて情報を整理し、解説する。

検討に係るノウハウ・人材不足	β´モデル移行に向けた事業計画策定の基本的な考え方、移行プロセスについて、先行事例を参考に記載する。
セキュリティ対策の強化	ガイドラインにおいて、β´モデルに必要とされるセキュリティ対策において、地方公共団体でしばしば課題として聞かれる要件について、システム構成の設計時、製品選定時の考慮ポイントを解説し、先行事例を参考として記載する。
移行に係るコスト増加	コスト低減に資する工夫、踏まえるべき観点等を先行事例から参考として記載する。
適切な移行時期の見極め	先行団体が選択した移行タイミング、判断根拠から、踏まえるべき観点を整理の上、参考として記載する。

本書のアプローチ

β´モデル移行時に課題とされる事項に対し、先行事例(既にβ´モデルへの移行を完了された団体)に基づき、検討時の参考となるよう、本書にて情報を整理し、解説する。

検討に係るノウハウ・人材不足	β´モデル移行に向けた事業計画策定の基本的な考え方、移行プロセスについて、先行事例を参考に記載する。
セキュリティ対策の強化	ガイドラインにおいて、β´モデルに必要とされるセキュリティ対策において、地方公共団体でしばしば課題として聞かれる要件について、システム構成の設計時、製品選定時の考慮ポイントを解説し、先行事例を参考として記載する。
移行に係るコスト増加	コスト低減に資する工夫、踏まえるべき観点等を先行事例から参考として記載する。
適切な移行時期の見極め	先行団体が選択した移行タイミング、判断根拠から、踏まえるべき観点を整理の上、参考として記載する。

本書で扱う移行ステップの考え方について

■ 本書で扱う移行プロセスは、過去のβ´モデル移行実施団体の事例から、最も採用数が多いと思われる方式を採用する。本移行プロセスは下記３ステップを前提としており、次ページから詳細を記載。

ステップ１：新LGWAN接続系を構築
ステップ２：現LGWAN接続系を新インターネット接続系に移行
ステップ３：現LGWAN接続系及び現インターネット接続系の廃止
※他の移行方式については、本書では取り扱わないものとする。

■ β´モデルへの移行方法の検討において、業務端末／業務システム等のIPアドレス体系をどの程度維持できるかが重要な観点となる。IPアドレスが変更された場合、IPアドレスを参照しているあらゆるシステムの設定変更が生じるため、影響が大きくなる。効率的な移行方式の選定にあたっては、いかにIPアドレス体系に手を加えないかに配慮し設計することが望ましい。業務端末／業務システム等を複数回に分割して移行する場合は、移行対象機器から順にIPアドレスを変更することになり、IPアドレス体系の維持が難しくなることに留意する。

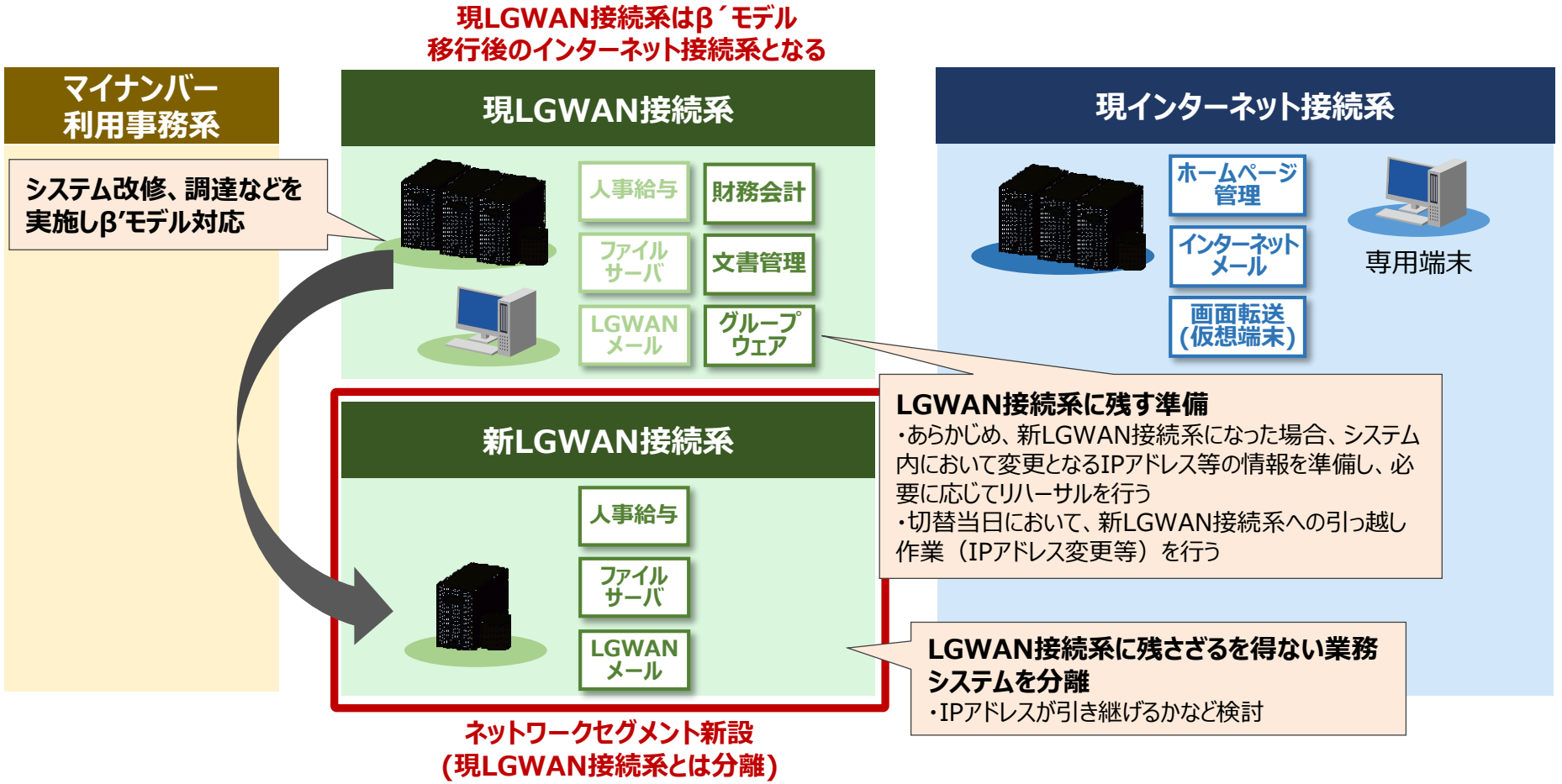
なお、LGWAN接続系の業務端末を残したまま、新規に業務端末をインターネット接続系に配備する場合は、IPアドレスを移行する必要なく、インターネット接続系のIPアドレス体系を拡張することで対応可能なケースも想定される。上記の、本書で扱う移行プロセス（３ステップ）以外の方式が効率的なケースも考えられるため、各団体の更新スケジュールや各種計画等を踏まえ、移行方式を検討することが望ましい。

移行ステップ１

先行事例で多くみられる移行ステップについて、そのプロセスを参考として解説する。

ステップ１．新LGWAN接続系を構築

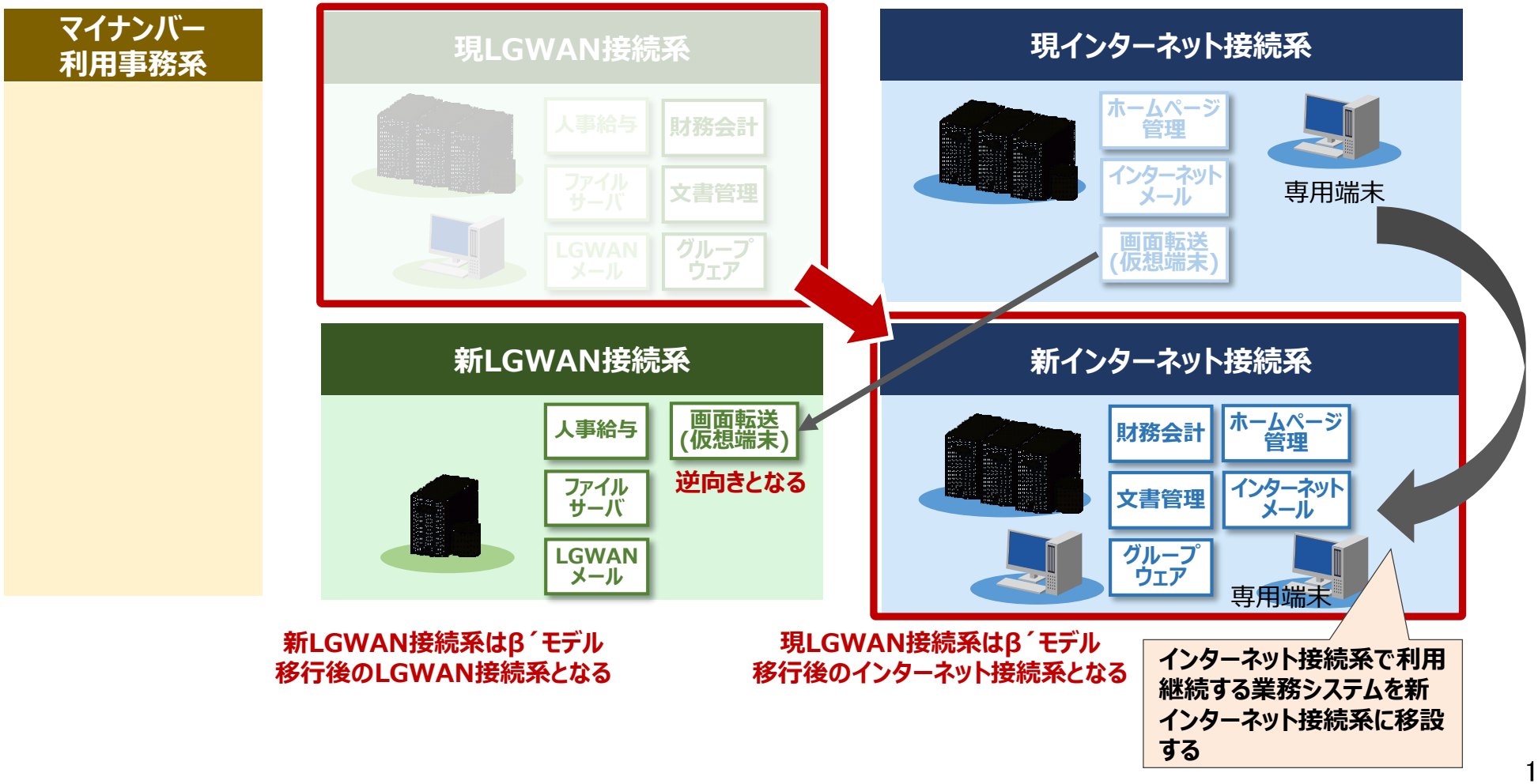
・β´モデル移行後は、現LGWAN接続系のIPアドレス体系をインターネット接続系に読み替える前提の計画
・新LGWAN接続系(β´モデル移行後のLGWAN接続系)を新設し、LGWAN接続系に残すシステムを配置する



移行ステップ２

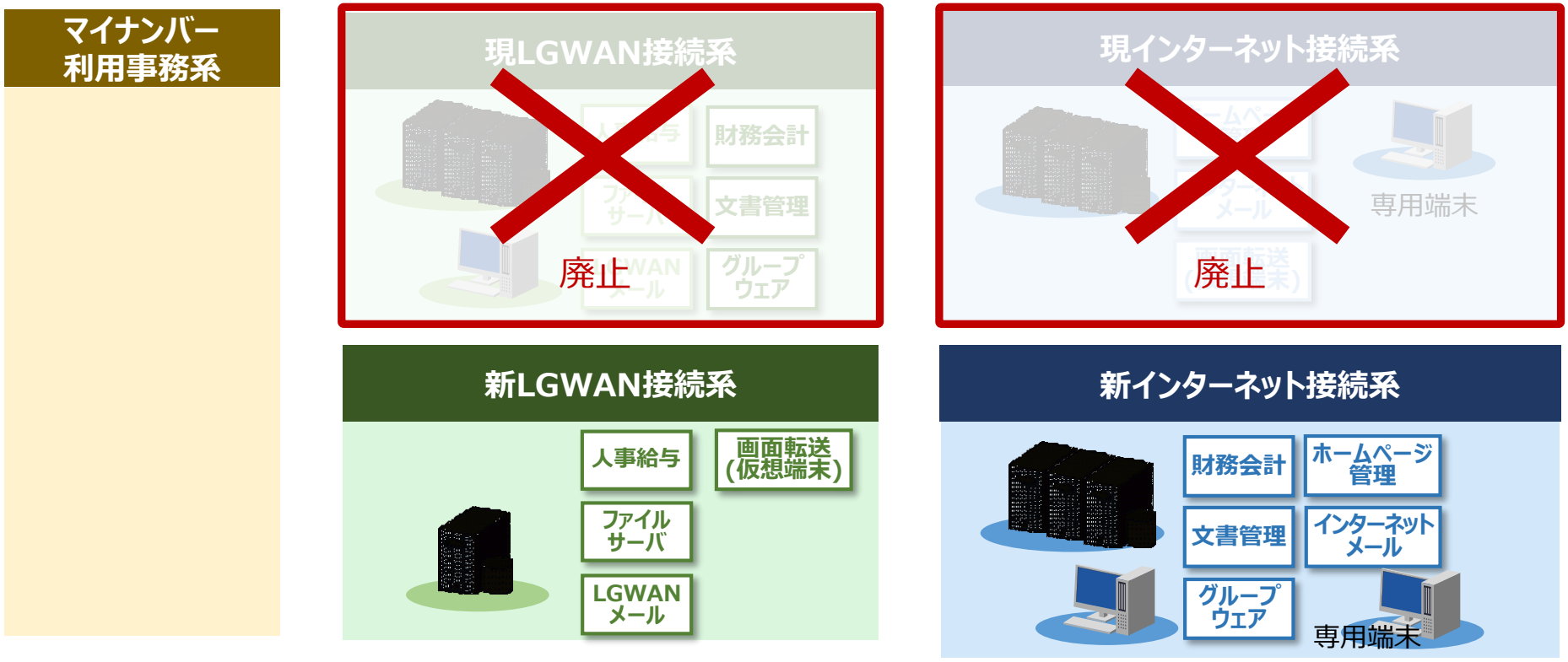
ステップ２．現LGWAN接続系を新インターネット接続系に移行

・引っ越し後（ほぼ同じタイミング）において、旧LGWAN接続系のIPアドレス体系を、インターネット接続系の体系として変更し、動作確認を実施。
・前行程のステップ１とステップ２は、時系列ではほぼ同一のアクションとなる場合が多い。



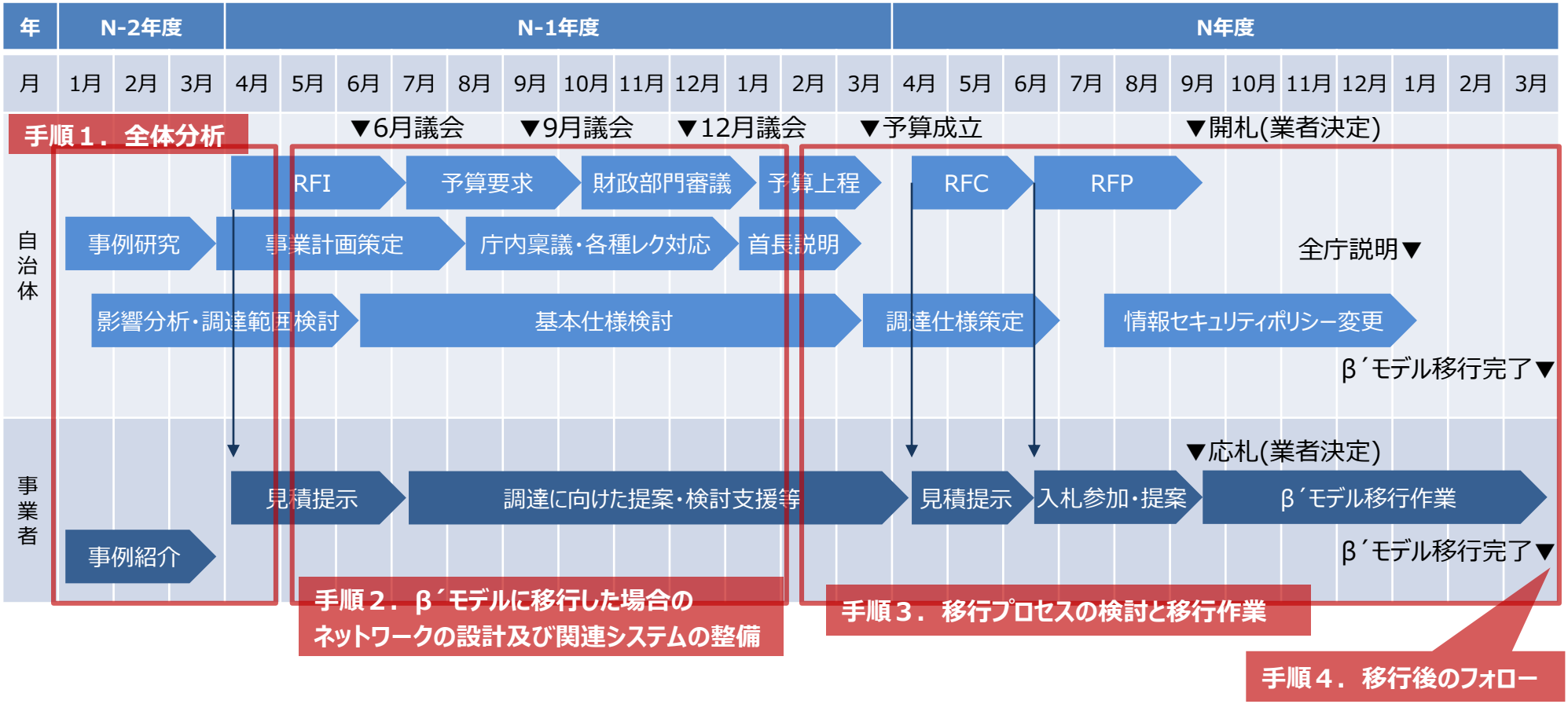
ステップ３．現LGWAN接続系及び現インターネット接続系の廃止

・現LGWAN接続系及び現インターネット接続系を廃止し、マイナンバー利用事務系、新LGWAN接続系、新インターネット接続系の３系統となる。
・マイナンバー利用事務系は変更対象とはならない。



移行プロジェクト推進における全体スケジュール（例）

・β ‘モデル移行までの予算化および予算化後の作業プロセスについて、スケジュールを記載しています。
（職員数：10,000人規模）



β´モデルへの移行手順（１）

手順１．全体分析

（１）ネットワーク・業務システムの現状把握

・業務システムが配置されるネットワークセグメントを可視化する。
・次期ネットワークモデルの設計に活用するため、業務システムの利用形態、規模の現状把握を行う。この際、業務システムを所管している部門にヒアリングを行う必要があり、参考情報として、次葉にて具体的な調査フォーマットの例を記載する。
・マイナンバー利用事務系、LGWAN接続系、インターネット接続系以外の独自ネットワークを調査する。
※文部科学省や厚生労働省が策定するガイドラインの適用対象となっているネットワークは本移行プロセスの対象には含まれない。

（２）LGWAN接続系に残す業務システム等の検討

・上記（１）において、LGWAN接続系に配置した業務システム等のうち、どのシステムがインターネット接続系に移行することができるか確認、整理する。

（３）LGWAN接続系に残す業務システム等の利用方法の検討

・上記（２）においてインターネット接続系に移行できない業務システムに対する利用方法等を確認、整理する。
※インターネットに配置した業務端末から仮想環境でLGWAN接続系を利用する等が考えられる。
仮想環境における業務システムの利用の技術的可否（例：VDIのみ可能、 SBCでも可能等）、
利用環境数も含む

（ご参考）現状把握に用いる調査表フォーマット例

業務システムの利用に関する現状把握を行うため、下記フォーマットを作成し、庁内各部局に照会をかけ棚卸しを行う必要がある。データ入力された調査表は業務システムの移行パターンの選定等に用いる。

＜調査表フォーマット例＞

	所有組織名				業務システム名	接続セグメント	ソフトウェア名	導入事業者	導入維持経費	契約開始日	契約終了日
	所管課	担当者名	連絡先【メール】	連絡先【電話番号】					【単位:円／税込】		
例	情報政策課	○○　○○	xxxxx@lg.jp	xxx-xxx-xxxx	●●システム	LGWAN接続系	△△	A株式会社	55,000,000	2025/04/01	2029/03/31
1											
2											
3											

利用端末			サーバ基盤（環境）						必要リソース（※調達仕様）			
台数	仮想OS	OS	稼働環境	製品メーカー	台数	仮想OS	OS	データベース	CPUコア数／1台	メモリ容量【GB】	ハードディスク種別	容量【GB】
25	無し	Windows 10	オンプレミス（庁内）	X社	1	Hyper-V	Windows Server 2019	Oracle	2	900	SSD	900

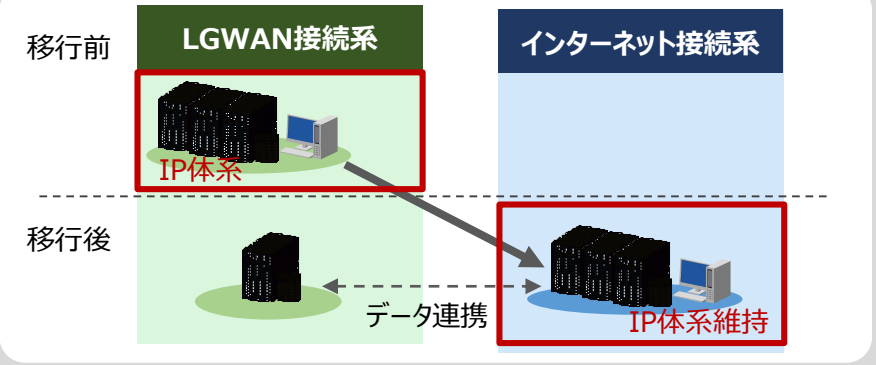
接続方法	保有する情報資産の機密性分類	次期ネットワークモデル(β´モデル)移行後のご希望				次期ネットワークモデル(β´モデル)移行後、インターネット接続系に設置した場合、運用に支障が生じる場合はその理由を記載下さい。 その他補足説明、現状課題、ご要望等がございましたら、自由に記載ください。
		移行希望時期	移行後の設置セグメント	インターネット経由での運用保守希望の有無	「有」の場合の理由	
ブラウザ（chrome）	機密性2	2030/04/01	インターネット接続系	有	サーバ障害時の復旧時間短縮化	

業務システムの代表的な移行パターン

β´モデル移行における業務システムの代表的な移行パターンとして、以下の３つが考えられる。p12～15に記載した移行ステップの検討において、全ての移行パターンについて考慮する必要がある。

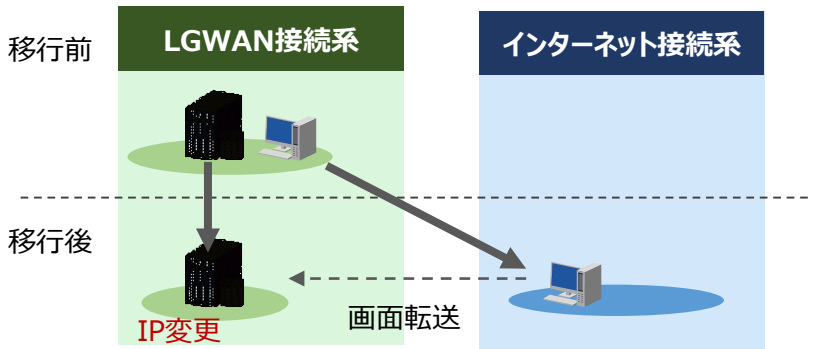
①LGWAN接続系からインターネット接続系へ転換

- 業務システム(および業務端末)は、IPアドレス体系を引き継いだまま、インターネット接続系へ転換するケースを前提とした場合、設定変更は生じない
- 連携先システムについても、転換後も変化が生じない限り、設定変更は発生しない想定



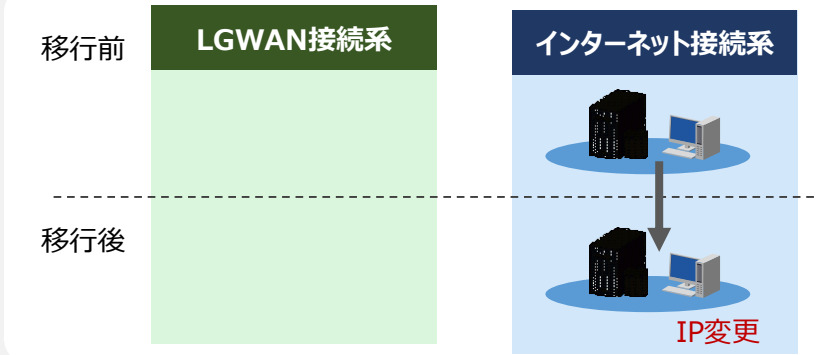
②LGWAN接続系にありLGWAN接続系に残す

- ①を前提とする場合、業務システムは、IPアドレスの設定変更が発生する
- 業務端末はインターネット接続系に配置転換されるため、画面転送を経由したシステム利用となる。画面転送利用が不可の場合は独自端末を準備するなどの対応が必要となる



③インターネット接続系にありインターネット接続系で利用

- ①を前提とする場合、インターネット接続系の業務システムは、IPアドレスの設定変更が発生する場合がある
- セキュリティ対策強化が必要となるため、OSパッチ適用、β´モデル転換後の動作確認作業が必要となる



手順１の具体的な進め方とポイント

全庁アンケートの作成	✓ 各部局・課室が調達／管理している業務システム、業務端末、ネットワーク等について、現状調査をするため、アンケートを作成する。 ✓ アンケート依頼時には、現状のネットワークと次期ネットワーク移行計画の概要、β´モデルのメリットや移行プロジェクト推進方針を分かりやすく解説した資料を作成し、調査目的として発出する。適宜、説明会などを開催し、関係部署における理解の向上や疑問点の解消に努めることが肝要である。 **＜ポイント＞** ① β´モデル移行にあたっては、インターネット接続に業務システムを配置することを基本的な方針として、意思表示することが重要である（LGWAN接続系に残す／インターネット接続系に移行する、という選択肢が与えられた場合、LGWAN接続系に残したい＝現状維持したい、という回答が多くなることが想定され、移行コスト、検討課題が増えるため）。あくまで、「業務システムをインターネット接続系に配置した場合、支障が生じる場合はアンケートに記入下さい」とする） ② β´モデルでは、住民に関する情報をインターネット接続系に保存させない規定を整備する必要があるため、住民情報の定義を踏まえ、業務システムが保有する情報資産の機密性分類を把握する必要がある。
全庁アンケート結果を踏まえた検討	✓ 全庁アンケートの収集を行い、出された課題に対する解決策の検討を行う。 **＜ポイント＞** LGWAN接続系に残す必要がある／残したい業務システムについては、インターネット接続系に移行できない理由を把握の上、個別に検討する。例えば、LGWAN-ASPやLGWANメールなど、LGWANの利用を前提とした業務であることが移行が困難な理由として考えられる。

β´モデルへの移行手順（２）

手順２．β´モデルに移行した場合のネットワークの設計及び関連システムの整備

（１）β´モデルのネットワーク設計

・次期ネットワークモデルとして目指す姿を明確にし、ネットワーク構成図として具体的に記述する。
　※LGWAN接続系に配置する業務端末/システム、インターネット接続系に配置する業務端末/システム
・都道府県セキュリティクラウドとの関係性を考慮し、インターネットとの通信、アクセス制御の仕組みを検討
・各業務システムにおける技術的確認、合意形成を行う

（２）既存システムの改修に係る影響範囲の特定と対応方針の検討

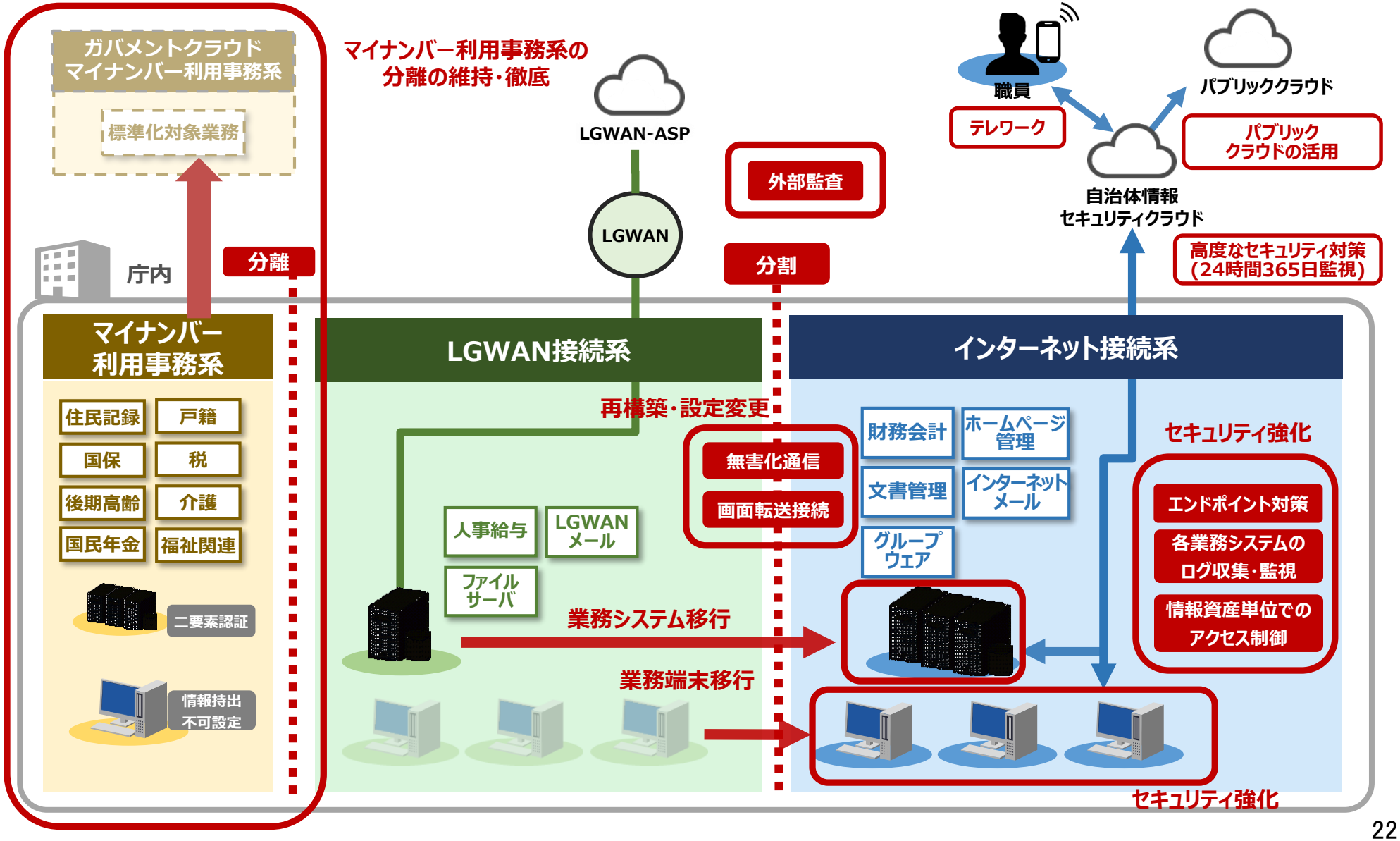
・インターネット接続系に移行するシステムに対する改修等の確認、費用算出、スケジュール等調整
・LGWAN接続系に配置するシステムに対する改修等の確認、費用算出、スケジュール等調整
・各業務システムにおける改修費用等の負担元の明確化
　※改修例）庁内ネットワーク改修、グループウェア改修、ファイルサーバ改修、認証基盤改修　等

（３）β´モデル移行に合わせて行う施策の整理と検討

・β´モデルでの移行事業の中で、クラウドサービスとの接続、無線LANの導入、テレワークの拡大、コミュニケーション基盤の刷新等の施策も同時に実施する場合がある。中でもクラウドサービス利用はβ´モデル移行の目的の一つとして位置付けられることが多く、クラウドサービスの本格利用開始にあたっては、接続回線の増強やアクセス制御に係るネットワーク機器の増強が必要になる可能性がある。
(ブレイクアウト/増加するセッションに対応したプロキシ等の明確化、出先レベルでブレイクアウトを実現する場合のFWログの取得・保管の必要性)
・外部監査の実施について、事業者選定※、監査方法、監査対象、スケジュール等の検討が必要
※事業者選定基準：IPA情報セキュリティサービス基準適合サービスリスト−情報セキュリティ監査サービス

β´モデルのネットワーク設計に係るイメージ図

・移行を目指すβ´モデルを構成図として可視化し、必要なセキュリティ対策群及び想定される影響範囲を明記する。
・主な対応事項として、「機器の配置転換」「各種設定変更」「セキュリティ強化」が挙げられる。



（ご参考）既存システムの改修に係る影響範囲の特定と対応方針の検討

既存資産に与える影響として、既存ネットワークの改修やLGWAN接続系システム利用のための環境整備、インフラ環境の拡張・改修等があり、回収修や整備、拡張時に考慮すべき内容を以下に例示する。

既存資産に与える影響	検討課題
既存ネットワークの改修	• ネットワーク構成変更、インターネット閲覧環境（DNS、プロキシ等）の設定変更 • β´の構成に必要なネットワーク機器新設（ファイアウォール、スイッチ等） • LAN敷設、無線LAN導入の設定変更
LGWAN接続系システム利用のための環境整備	• LGWAN接続系に設置する資源を利用するために必要なシステムを構築する(専用端末の配備含む) • インターネット接続系の業務端末からLGWAN-ASPサービスを利用するための仕組み、また同サービスで受信したデータをインターネット接続系に転送する仕組み(画面転送、ファイル転送、無害化処理)等
認証基盤/資産管理システム等改修	• 新ネットワーク構成への移行に伴う認証基盤/資産管理システムの改修 • インターネット接続系では業務端末の増加に対し、LGWAN接続系では減少に対し、それぞれAD設定変更 • 業務端末の移設に伴い端末向け配信システム(WSUS、ウイルス定義体配信)および端末管理系の設定変更
グループウェアシステム改修(主にメール運用設定を指す)	• インターネット接続系に業務端末を移設することに伴うメール送信システムの構成変更、インターネットから受信するメール受信システムの構成変更、LGWANへ送信するメールを無害化するための構成変更 • 無害化前のファイルをブラウザ上で送信する用途のためにWebメーラーの再構築　等
ファイルサーバ改修	• インターネット接続系に業務端末を移設することに伴うファイルサーバの整備(運用ルール整備も重要) • 情報セキュリティ管理の観点から各セグメントにそれぞれ設置し、アクセス制御を徹底する。また、セグメント間を越えてデータをやりとりする場合は無害化等を必須とし、クラウドストレージとは用途を区別する
インフラ環境拡張・改修(統合仮想基盤/物理サーバの設定変更)	• 新たなネットワーク構成となることに伴い、各セグメントに配置するシステムを上位L3スイッチに接続 • インターネット接続系に移設される業務システムが業務端末と通信できるよう仮想サーバのスイッチの設定変更 • 既存のIP体系に改修を加えないよう、IPアドレス/VLANの変更とせずスイッチ設定変更で回避するのも有効

β´モデルへの移行手順（３）

手順３．移行プロセスの検討と移行作業

（１）移行プロセスの検討

・業務端末/各業務システムの移設、既存システムの改修、セキュリティ対策を含めた全体スケジュールの整理、合意を行う。
・事前の調査では洗出しきれない潜在的な通信フローも想定される為、可能であればリハーサル等テスト移行の複数計画や、切替予備日の設定など、安全な移行を目指す事が重要である。

（２）移行作業及び進捗管理

・移行プロセスはいくつかのステップに分けて、一定期間をかけて段階的に完了する場合が多い。従って、各業務システム側の改修等の進捗管理や設定値の変更や軌道修正も含めた技術調整対応が必要となる。
※必要に応じて移行プロジェクト課題管理が必要

（３）各利用者に対する説明・周知

・広く庁内システムの利用者に関わる構成変更であり、十分かつ丁寧な説明が必要となる。
・業務端末の設置されるネットワークセグメントが変更になる点、セキュリティ対策が強化される点、LGWAN接続系に配置されるシステムを仮想環境で閲覧することなど、運用変更になる箇所は特に事前の説明が重要。

移行方法と考慮すべき観点

移行パターン選択時において、「セキュリティの観点」と「業務継続の観点」から留意すべき事項を以下に示す。

端末移行	**＜セキュリティの観点＞** ・端末がインターネット接続系に移設された時点で、β´セキュリティ要件への準拠が必要 （セキュリティパッチの適用、EDR、ログ管理、人的対策等） ・端末内に保存されている情報資産が、インターネット接続系に移設された時点で、庁内で規定している情報セキュリティポリシー要件への準拠が必要。 自治体によっては情報セキュリティポリシーの改定含め、実態との整合性を検討する必要がある。 （重要性分類に基づいた情報資産の規定等） **＜業務継続の観点＞** ・端末がインターネット接続系に移設された時点で、LGWAN接続閲覧用の仮想環境が必要 ・端末がインターネット接続系に移設された時点で、LGメールのルート変更が必要 ・新たな業務環境での職員研修が必要
業務システム移行	**＜セキュリティの観点＞** ・業務システムがインターネット接続系に移設された時点で、β´セキュリティ要件への準拠が必要 （セキュリティパッチの適用、ログ管理、人的対策等） **＜業務継続の観点＞** ・業務システムがインターネット接続系とLGWAN接続系で分かれる(期間がある)場合、ネットワークセグメント間のデータ連携を構築する必要がある

- 移行を複数回実施することは、αモデルとβ´モデルの併存を意味するため、両モデルを利用するユーザ向けの環境構築や研修を実施しなければならない

移行方法と考慮すべき観点

仮想基盤	**＜セキュリティの観点＞** ・異なるネットワークセグメント間の論理分割を継続 ・情報資産レベルに応じたセキュリティ対策 **＜業務継続の観点＞** ・端末移行、業務システム移行と仮想基盤更新は同時に行うことで、手戻りのない移行プロジェクトを実施できる可能性があるため、検討範囲に含まれる場合がある。一方、IPアドレスを変更する場合は、インフラレイヤーの立ち上げとIPアドレス体系変更を同時に実施できるためメリットが出るが、IPアドレス変更を伴わない場合、同時実施のメリットはあまりない可能性も考えられる。 ・むしろ業務システム移行と仮想基盤更新を同時に行うことにより、障害時の切り分けが困難になるため、業務システム移行先に完了させ、安定稼働と業務継続性の確保を確認したのち、仮想基盤を刷新する進め方も有効と考えられる。

仮想基盤の単純更新であれば特に問題はないが、例えば、インフラの基盤をマルチクラウド構成とする場合、検討期間と人的リソースが必要となる。業務システム別に、情報資産レベル、アプリケーションの更新頻度、イベントによる一時的な負荷集中の有無、高い可用性が求められる業務か、クラウドサービス利用に対応可能なアプリケーションであるかどうか等を検討し、対象範囲を定義していく必要がある。

（ご参考）移行時に検討すべき項目

セキュリティ対策の強化、既存システムの改修も含め、移行時に移行計画として策定することが望ましい項目を以下に例示する。計画策定時の参考とされたい。

項番	検討項目（例）	検討内容（例）
1	インターネット/LGWANにおけるサイト閲覧移行計画	• インターネット接続系/LGWAN接続系におけるファイル交換システムをβ´モデルへ移行する。 • β´モデル移行後、インターネット接続系は移行前LGWAN接続系からプロキシサーバやPACファイル配信環境を移行して利用する。 • β´モデル移行後、LGWAN接続系は新設する移行後LGWAN接続系にプロキシサーバやPACファイル配信環境を新規構築して利用する。
2	インターネット接続系/LGWAN接続系におけるファイル交換移行計画	• インターネット接続系/LGWAN接続系におけるファイル交換システムをβ´モデルへ移行する。 • β´モデル移行後、現在使用しているファイル交換システムは既存流用を検討し、流用が難しい場合は既存を廃止し、新たに構築する。 • β´モデル移行後も既存のサンドボックス型セキュリティ製品を継続利用するなど検討する。
3	インターネット/LGWANにおけるメール送受信移行計画	• インターネット/LGWANにおけるメール送受信システムをβ´モデルへ移行する。 • β´モデル移行後の環境では、インターネット向けのメールの添付ファイルは誤送信抑止サーバで分離する。インターネット接続系に構築したメールシステムからLGWANに向けたメール発信については、LGWAN接続系を経由するため、メール無害化サーバにて無害化処理を実施する。
4	端末統制基盤におけるID連携移行計画	• 端末統制基盤をβ´モデルへ移行する。 • β´モデル移行後の環境では、移行後インターネット利用事務接続系に存在する一般事務用端末及び業務システムは移行後インターネット利用事務接続系データセンターサーバにて認証し、移行後LGWAN接続系に存在する一般事務用端末、VDI、業務システムは移行後LGWAN接続系データセンターサーバにて認証する。 • β´モデル移行後の環境では、移行後インターネット利用事務接続系に存在する職員認証システムのデータをユーザー情報連携システムへ連携連携されたデータを基にLGWAN接続系及びインターネット接続系の各データセンターサーバに対してユーザーの追加/登録/削除を実施する。 • ユーザー情報連携システムから各データセンターサーバへは必要な通信のみ許可する。
5	重要な情報資産へのアクセス移行計画	• β´モデルへ移行後も継続してLGWAN-ASPシステム等の重要な情報資産へのアクセスを可能とする。

（ご参考）移行時に検討すべき項目

項番	検討項目（例）	検討内容（例）
6	LGWAN接続用仮想環境の移行計画	• LGWAN接続系のサイト閲覧を行う仮想環境を新規構築する。 • 現行のインターネット接続用仮想環境（VDI、SBC等）システムはインターネット接続系の操作が一般事務用端末から可能となるため、廃止とする。 • LGWAN接続系の操作は一般事務用端末がインターネット接続系に配置されたことにより、間接的に操作する手段が必要となるため、LGWAN接続系に新たに仮想環境システムを構築する。
7	EPPシステム移行・EDR導入計画	• 既存のEPPシステムをβ´モデルへ移行する。 • インターネット接続系に配置される一般事務端末、サーバに未知の不正プログラム対策（Endpoint Detection and Response（以下、「EDR」））を導入する。 • 必要に応じてEDRを活用した情報セキュリティ専門人材によるインシデントの早期検知や対処サービス（SOC）の検討を行う。
8	全庁仮想化基盤/バックアップシステム移行計画	• サーバ仮想化基盤/バックアップシステムをβ´モデルへ移行する。 • 移行後LGWAN接続系及び移行後インターネット利用事務接続系に配置される仮想マシンを収容できるよう、必要に応じてサーバ仮想化基盤のネットワーク設定を変更する。 • β´モデル移行後に新規構築が必要となる仮想マシンを見据え、外部データセンター設置のサーバ用仮想化基盤にサーバを増強する。
9	庁内ネットワーク移行計画	• 庁内ネットワークをβ´モデルへ移行する。 • インターネット接続系は、UTM及びコアスイッチの設定変更により、移行前インターネット利用事務接続系及び移行前LGWAN接続系を配置し、ネットワーク種別名として移行後インターネット利用事務接続系とする。 • LGWAN接続系は、新規にネットワークを構築し、ネットワーク種別名として移行後LGWAN接続系とする。また、UTM及びコアスイッチの設定により、インターネット接続系と論理分離する。 • β´モデルへの移行に伴うインターネット通信量の増加を考慮し、ネットワーク経路や機器構成、WAN回線を見直すこととする。なお、インターネット(セキュリティクラウド)への接続口は、現在外部データセンターとなっているが、外部データセンターへの変更を前提として検討すること。
10	外部監査実施計画	• 外部監査を実施する。 • 監査事業者を選定する。※ ・監査方法を検討する。（資料確認ベース、オンサイトベース等） ・スケジュールを検討する。（監査実施期間、J-LISへの報告時期等） ・必要に応じて庁内セキュリティポリシーの改定を検討する。 ※選定基準：IPA情報セキュリティサービス基準適合サービスリスト-情報セキュリティ監査サービス

β´モデルへの移行手順（４）

手順４．移行後のフォロー

（１）移行作業の前段のテストにおいて発生する技術課題等の対応

・クラウド利用のアクセス回線の増強
・インターネット接続系に設けたプロキシ等の増強

（２）実運用後の通信不可等の事象等への対応

・ネットワーク機器の設定変更
・EDR運用開始後の誤検知に対するチューニング及び端末に導入したEDRエージェントのバージョンアップに係る資産配信ルートの設定や調整

（３）実運用における質疑応答等をもとにしたＦＡＱ等の速やかな作成展開等

・文書管理やファイルサーバの利用における情報資産管理の規定作成、周知
・新たに導入する画面転送や無害化の利用方法に対する操作マニュアルの作成、周知
・受付窓口の明確化
※インシデントを効率的に管理し、解決する仕組みとして、ITSM（インシデント管理）を活用することも有効
・職員のリテラシー向上を目的とした、インシデント訓練、セキュリティ研修等の継続的な開催。

（ご参考）移行プロジェクト推進における留意事項

- 業務システム関係の検討整理等は、事業者と調整をして実現していく形になるため、通常のシステム構築と同様(進捗・課題・品質の各要素に配慮して進める）になるが、相手先が幅広になるため、各業務システム側においても、β´モデル移行の意味や仕組みを正しく理解していることや、その趣旨に沿った対応をしているかを注視してくことへの配慮が必要かと思われる。

- β移行においての、一般ユーザへの周知等については、とても丁寧に行う必要があり、そのための資料作成においてあいまいな点を排除して作成することを考慮していくべきと考えられる。移行作業自体におけるあいまいな点も、可能な限り明確に設計することで、現場の混乱を最小限に抑えられる。

- β´モデル移行のタイミングにおいては、庁内ネットワークの更新と同時に行う事例が多く見られた。次期庁内ネットワークの構成検討においては、β´モデルに向けた見直しのみならず、無線LAN導入や、テレワーク端末の増設、コミュニケーション基盤の刷新、ゼロトラストアーキテクチャの導入など、新たな取り組みも包括した計画も多く確認された。β´モデル移行にあわせ、これらの構成変更の要素も考慮し、最適なシステム構成を包括的に検討していく必要がある。

本書のアプローチ

β´モデル移行時に課題とされる事項に対し、先行事例(既にβ´モデルへの移行を完了された団体)に基づき、検討時の参考となるよう、本書にて情報を整理し、解説する。

検討に係るノウハウ・人材不足	β´モデル移行に向けた事業計画策定の基本的な考え方、移行プロセスについて、先行事例を参考に記載する。
セキュリティ対策の強化	ガイドラインにおいて、β´モデルに必要とされるセキュリティ対策において、地方公共団体でしばしば課題として聞かれる要件について、システム構成の設計時、製品選定時の考慮ポイントを解説し、先行事例を参考として記載する。
移行に係るコスト増加	コスト低減に資する工夫、踏まえるべき観点等を先行事例から参考として記載する。
適切な移行時期の見極め	先行団体が選択した移行タイミング、判断根拠から、踏まえるべき観点を整理の上、参考として記載する。

● β'モデルの基本的なコンセプト

○セキュリティ対策における防御の限界

- メールやインターネット経由のマルウェア等の感染を防ぐため、サンドボックスを用いた振る舞い検知などの対策が必要であるが、マルウェア等の侵入を完全に防ぐことができず、防御による対策だけでは限界がある。

○検知と対処・復旧の重要性

- 業務端末がマルウェア等に感染してしまった場合に、外部への情報漏えいを防ぐため、エンドポイントでの対策や通信のログ管理・監視、通信経路のアクセス制御といった早期検知や対処、復旧の仕組みを構築することが重要となる。

○組織的対策・人的対策の整備

- インターネット接続系に業務端末を設置することによって、αモデルと比較して業務情報の漏えい等のリスクが高まり、脅威に対する組織的・人的対策の整備が求められる。
- 不審なメールに注意し、添付ファイルを開かない、URLにアクセスしないといった運用を徹底することで防御につながるため、セキュリティ教育の実施によるリテラシー向上などの人的な対策が必要となる。また、インシデント発生時の対応や自治体間での情報共有のためのCSIRTの運用が重要となる。

○自治体セキュリティクラウドとの連携

- 自治体セキュリティクラウド（SOC）との連携により、情報セキュリティ専門人材によるインシデントの早期検知や対処、自治体間での情報共有が期待できる。

β´モデルにおいて対策を強化すべき事項

● **業務端末及び業務システムをインターネット接続系に移行することにより新たに発生するリスクを考慮する。**

No	考慮すべきリスク(**黄色背景は追加項目**)	考えられる主な対策 **(現在実施されていない対策または強化する対策　赤字必須　青字オプション)**	対策場所
1	インターネット接続系にある業務端末が乗っ取られ、画面転送接続経由でLGWAN接続系の情報を不正に閲覧・操作される	・ネットワーク監視・防御 ・脆弱性対策（**資産管理※**、パッチ適用等） ・ウイルス対策(パターンマッチング) **・ログ管理（SIEM※※等）** **・未知の不正プログラム対策（エンドポイント対策）**	・各自治体による対応
2	インターネット接続系にある業務端末に不正なリモートアクセスをして重要情報を不正に閲覧・操作される	「地方公共団体における業務の効率性・利便性向上策の検討に係るWG」より ・**端末認証、端末の持ち出し管理**など	・各自治体による対応
3	サイバー攻撃の検知漏れにより、インターネット接続系に不正に侵入される	・ネットワーク監視・防御 **・SOCの強化**	・セキュリティクラウドによる対応
4	標的型メールの添付ファイルからのマルウェア感染による機密情報の漏えい（Emotet等）	・ネットワーク監視・防御 ・メールセキュリティ（サンドボックス） ・脆弱性対策（**資産管理※**、パッチ適用等） ・ウイルス対策(パターンマッチング) **・ファイル暗号化** ・アクセス制御（アクセス権の局所化） **・未知の不正プログラム対策（エンドポイント対策）** **・DLP※※**	・ゲートウェイ対策はセキュリティクラウド ・内部メールサーバ、グループウェア等のセキュリティ対策は、各自治体での対応
5	標的型メールの添付ファイルからのランサムウェア感染によるグループウェアやメール利用停止（WannaCry等）	・ネットワーク監視・防御 ・メールセキュリティ（サンドボックス） ・脆弱性管理（**資産管理※**、パッチ適用等） ・ウイルス対策(パターンマッチング) ・アクセス制御（アクセス権の局所化） **・未知の不正プログラム対策（エンドポイント対策）** ・バックアップ	・ゲートウェイ対策はセキュリティクラウド ・端末のセキュリティ対策は、各自治体での対応
6	端末、サーバ、ソフトウェア等の脆弱性を悪用し、不正なコードが実行される	・ネットワーク監視・防御 ・脆弱性対策（**資産管理※**、パッチ適用等） ・ウイルス対策 **・未知の不正プログラム対策（エンドポイント対策）** **・業務システムログ管理（ログ収集、監視）**	・ゲートウェイ対策はセキュリティクラウド ・業務システムサーバ等のセキュリティ対策は、各自治体による対応
7	職員が組織に許可されていないクラウドサービスに機密情報を不正にアップロードする	**・シャドーIT管理※※**	・セキュリティクラウドまたは各自治体による対応

※OSやソフトウェアのバージョンなどを漏れなく管理することで、脆弱性の所在の効率的な把握を可能とし、ゼロデイ攻撃等のソフトウェアの脆弱性を狙った攻撃に迅速に対応できる。
※※SIEM：サーバーやネットワーク機器、セキュリティ関連機器及び各種アプリケーション等から集められたログ 情報を分析し、異常を検知した場合に管理者に通知する仕組みのこと。
DLP：機密性２以上の情報等の紛失や庁外への漏えいを防止・阻止するための装置やソフトウェアまたはその仕組みのこと。
シャドーIT：庁内で用いられる情報システム、機器やソフトウェアなどのうち、職員等の判断で導入・使用され、情報システム部門による把握や管理が及んでいないもののこと。
なお、SIEM、DLPは対策例であり、これに限定するものではない。これらの対策の機能の趣旨に沿うものであれば、当該リスクの対策になりうる。

セキュリティ対策の強化について

ガイドラインでは、β´モデルにおける「技術的対策」および「組織的・人的対策」で必要な要件が以下の通り定められている。対策群を実施する上での考慮ポイントを次葉にて記載する。

対策区分	セキュリティ対策	概要
技術的対策	無害化処理	・ファイルからテキストのみを抽出、ファイルを画像PDFに変換、サニタイズ処理、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェアで危険因子の有無を確認するなどの方法を用いて、危険因子が無いことを確認した上で、LGWAN接続系にインターネット接続系からファイルを取り込む。
	LGWAN接続系の画面転送	・インターネット接続系の業務端末からLGWAN接続系のサーバや端末を利用する場合は、仮想化されたリモートデスクトップ形式で接続する。 ・LGWAN接続系からインターネット接続系へのデータ転送(クリップボートのコピー&ペースト等)は禁止とする。ただし、LGWANメールやLGWAN-ASPから取り込み、業務で必要となるデータの転送については、中継サーバやファイアウォール等を設置し、通信ポート、IPアドレス、MACアドレス等で通信先を限定することで可能とする。
	未知の不正プログラム対策（エンドポイント対策）	・従来のパターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動の端末を監視・検出・特定する。また、異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施する。さらにインシデント発生要因の詳細な調査を実施する。
	業務システムログ管理	・インシデントの兆候検知や、インシデント発生後の調査に使用するため、業務システムのログの収集、分析、保管を実施する。
	情報資産単位でのアクセス制御	・情報資産の機密性レベルに応じて業務システム単位でのアクセス制御を行う。文書を管理するサーバ等は課室単位でのアクセス制御を必須とし、係単位でのアクセス制御は推奨とする。
	脆弱性管理	・OSやソフトウェアのバージョンなどを漏れなく資産管理し、脆弱性の所在を効率的に把握する。また、深刻度に応じて修正プログラムを適用し、ゼロデイ攻撃等のソフトウェアの脆弱性を狙った攻撃に迅速に対応する。
組織的・人的対策	セキュリティの継続的な検知・モニタリング体制の整備	・標的型攻撃訓練や研修等の職員等の受講状況や結果を確認し、セキュリティ対策の浸透状況や効果を測定する。測定した結果をもとに改善につなげていく。
	組織的なセキュリティ対策基準の遵守	・インターネット接続系とLGWAN接続系を完全に分離する場合を除き、必要なセキュリティ対策が実施されていることについて、事前に内部及び外部による確認を実施し、外部による確認の報告書を地方公共団体情報システム機構に提出する。また、その後も定期的に内部監査及び外部監査を実施することとし、外部監査の監査報告書を地方公共団体情報システム機構に提出する。
	住民に関する情報をインターネット接続系に保存させない規定の整備	・住民の名簿など、住民の個人情報をインターネット接続系に保存しない規定を整備するとともに、運用を徹底する。
	情報セキュリティ研修、標的型攻撃訓練、セキュリティインシデント訓練の受講	・職員等は情報セキュリティ研修、標的型攻撃訓練を年1回以上受講する。また、情報システム管理者、情報システム担当者はセキュリティインシデントが発生した場合の訓練を年１回以上受講する。
	本ガイドライン対策基準（例文）「１．組織体制　（９）CSIRTの設置・役割」「５.人的セキュリティ」記載の組織的・人的対策の必須事項の確実な実施に加え、以下の対策を実施する。 ・職員等が毎年度最低1回は情報セキュリティ研修を受講可能となる研修計画の策定 ・演習等を通じたサイバー攻撃情報やインシデント等への対策情報の共有 ・職員等の実践的サイバー防御演習（CYDER）の受講 ・本ガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し	

セキュリティ対策の強化について

ガイドライン*を補完する内容として、セキュリティ対策群を実装する上での考慮ポイントを記載する。

対策区分	セキュリティ対策	考慮ポイント
技術的対策	無害化処理 LGWAN接続系の画面転送	・利便性の向上、コスト削減の可能性について検討(インターネット接続系に端末と業務システムを設置する場合、インターネット接続系とLGWAN接続系の通信は特定の事務に限定できるため、両セグメント間の通信頻度を極小化、通信で使用する業務端末の数を減らせる可能性がある)。
	未知の不正プログラム対策（エンドポイント対策）	・自治体情報セキュリティクラウドのオプションとして利用するケースと、各団体が個別に導入するケースがある。 ・テレワーク端末やLGWAN接続系の端末に導入する意義にも触れられている。 ・製品選定にあたっては、既存EPPとの関連性、エージェントがクライアントに与える影響、コスト等を総合的に判断する。 ・EDRにおけるSOCは、求める要件を満たすものであるか十分な仕様の整理が必要(EDR付随のSOCのみではインシデントや照会対応が不十分なケースも考えられるので注意)。
	業務システムログ管理	・ユーザを起点としたアプリケーションの操作ログを指す。特定のユーザが職員のマイナンバー情報を繰り返し閲覧している、落札情報のCSVデータを夜間に大量出力している等の情報漏えいに繋がる挙動を登録しておき、兆候検知できる仕組みを構築する。 ・セキュリティリスク低減の観点から、ログ収集ソフト等で収集した情報をSIEMでビジュアライズ、専門人材がログ解析をインシデントの予兆検知や早期発見に活かす必要がある。その際、統合的なSOCが効果的な場合がある。
	情報資産単位でのアクセス制御	・機密性レベルに応じ、各セグメントに配置された情報資産と取扱状況の現状把握が必要。 ・業務システムはアプリケーション側でアクセス制御を行っている場合が多いが、ダウンロードしたファイル、共有ストレージに保存されたデータのアクセス制御にも配慮することが望ましい。
	脆弱性管理	・情報部門管理外(所管課調達)の端末の把握やテレワーク端末、自治体支給外端末(BYOD)も含めた統合管理、ガバナンスの強化が求められる。 ・ウイルス感染から復旧(安全宣言)までの時間を最小化するため、効率的な資産管理と運用を検討する。
組織的・人的対策	住民に関する情報をインターネット接続系に保存させない規定の整備	・住民情報β´モデル移行時をインターネット接続系に保存しないため、LGWAN接続系に住民情報を格納するファイルサーバを構築し、該当情報をβ´モデル移行時までに移管する必要がある。 ・β´モデル運用時、外部から住民情報を取得する場合/どうしてもインターネット接続系で住民情報のデータを扱う必要がある場合は、然るべきセキュリティ責任者の承認を得た上で、一時的な取扱いとし、使用終了後は速やかに削除あるいはLGWAN接続系に移設する等の対策を講じる。

(*)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

本書のアプローチ

β´モデル移行時に課題とされる事項に対し、先行事例(既にβ´モデルへの移行を完了された団体)に基づき、検討時の参考となるよう、本書にて情報を整理し、解説する。

検討に係るノウハウ・人材不足	β´モデル移行に向けた事業計画策定の基本的な考え方、移行プロセスについて、先行事例を参考に記載する。
セキュリティ対策の強化	ガイドラインにおいて、β´モデルに必要とされるセキュリティ対策において、地方公共団体でしばしば課題として聞かれる要件について、システム構成の設計時、製品選定時の考慮ポイントを解説し、先行事例を参考として記載する。
移行に係るコスト増加	コスト低減に資する工夫、踏まえるべき観点等を先行事例から参考として記載する。
適切な移行時期の見極め	先行団体が選択した移行タイミング、判断根拠から、踏まえるべき観点を整理の上、参考として記載する。

移行に係るコスト低減について

（１）コスト低減に係る施策・アイデア（例）

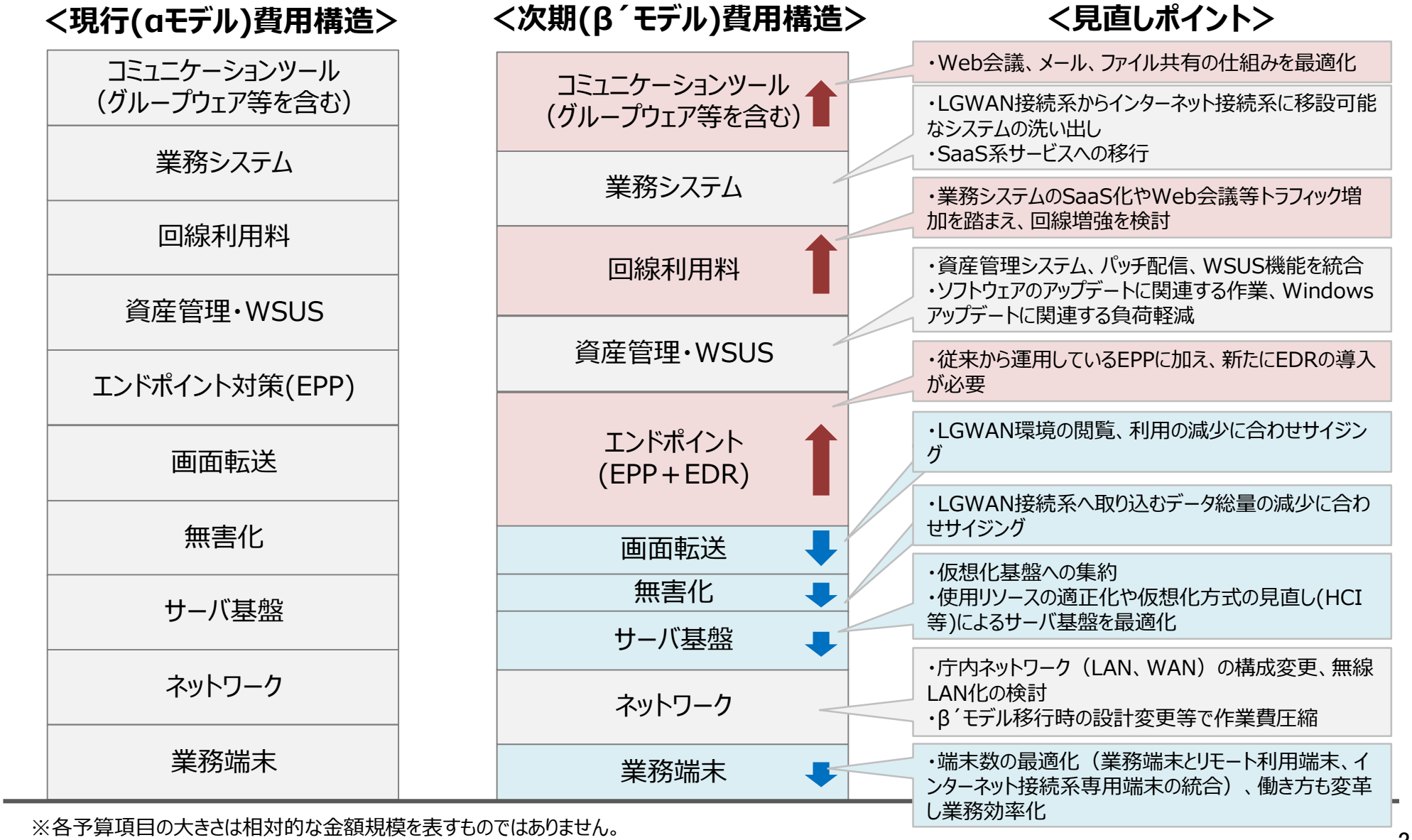
・共同利用での調達や自治体情報セキュリティクラウドが提供するオプション機能などを有効活用する。
・各セキュリティ機能単位で別々に調達、導入することも可能だが、同一メーカーで包括的にセキュリティ機能を安価に実装できる場合がある。ただし、この場合は将来に渡って、ベンダロックインとならないよう配慮する必要がある。
・LGWAN接続系に極力業務システムを残さない設計思想に基づくことで、LGWAN接続系を閲覧するための画面転送(仮想端末)の数を最小化させ、トータルでのコスト低減を実現することが可能。
※例）全職員分→LGWANを日常的に使う人数のみにライセンス数を削減可能
・画面転送の実装においては、様々な方式を選択肢に入れることでコスト低減となる可能性がある。

（２）費用対効果の試算にあたって

・事業計画は、働き方改革（クラウドサービスの利活用、コミュニケーション基盤の刷新、テレワークの拡大等）を目的とし、ネットワークモデルの変更はその手段として位置付けるものが多い。
・先行自治体の例では、β´モデル移行後のメリットについて、定量的な試算も見られた。
※例）インターネット閲覧時における、起動時間等の削減
起動時間 × 全職員数 × 年間勤務日 × 平均時給/60m ＝ 人件費削減　（机上の計算）
・β´モデルに移行した自治体の実施後庁内アンケートなどでは、利便性の向上や働き方が大きく改善したとの回答もあった。(移行前は十分にイメージできなかった業務効率化も、実際に移行した後はメリットとして実感される場合がある)
・インターネットサービスの活用についても、より利用しやすい環境に変わることで、職員が自ら創意工夫し、「移行前には想定していなかった効果が得られた」といった声も聞かれた。

【参考】αモデル→β′モデル移行時の費用構造イメージ

β´モデル移行におけるコストの増大については、現状の環境における予算配分に見直しにより一部費用をまかなえる可能性があり、費用構造の考え方について、参考として記載する。現在の業務システム状況の把握にあたっては、各原課へのヒアリング等が必要となる。



※各予算項目の大きさは相対的な金額規模を表すものではありません。

本書のアプローチ

β´モデル移行時に課題とされる事項に対し、先行事例(既にβ´モデルへの移行を完了された団体)に基づき、検討時の参考となるよう、本書にて情報を整理し、解説する。

検討に係るノウハウ・人材不足	β´モデル移行に向けた事業計画策定の基本的な考え方、移行プロセスについて、先行事例を参考に記載する。
セキュリティ対策の強化	ガイドラインにおいて、β´モデルに必要とされるセキュリティ対策において、地方公共団体でしばしば課題として聞かれる要件について、システム構成の設計時、製品選定時の考慮ポイントを解説し、先行事例を参考として記載する。
移行に係るコスト増加	コスト低減に資する工夫、踏まえるべき観点等を先行事例から参考として記載する。
適切な移行時期の見極め	先行団体が選択した移行タイミング、判断根拠から、踏まえるべき観点を整理の上、参考として記載する。

適切な移行時期の見極めについて

・移行のタイミングは各団体の調達サイクルや取り巻く環境により異なることが想定される。これまでにβ´モデル移行を実施した先行自治体の事例から、想定される６つの移行タイミングについて例示する。
・移行時期の設定にあたっては、ネットワークモデル変更に影響を与えるシステム群の調達時期を踏まえ、極力二重投資とならないよう配慮することが求められる。環境変更の検討には一定の期間が必要であるため、予め相当期間を見積っておくことも重要である。

移行タイミング	想定される概要
庁内ネットワーク更改時	• 次期庁内ネットワーク更新に合わせ、ネットワークモデルの検討を行い、β´モデル移行するケース。 • 庁内無線LAN化、庁舎建て替え等を機会に庁内ネットワークの見直しが発生する場合もある。 ※β´モデルに移行するタイミングにおいて、比較的多いケースと考えられる。
セキュリティ強靭化システム（画面転送/無害化等）更改時	• 三層分離を実施する際に導入した仮想環境、無害化システム等の更新時にβ´モデルに移行するケース。 • 現状αモデルでインターネットをVDIで閲覧している場合に、β´モデルに移行することでVDIライセンスの大幅な削減が可能となる等、VDI更新が機会となる可能性がある。 ※β´モデルに移行するタイミングにおいて、比較的多いケースと考えられる。
業務端末更改時	• 端末更新を機にインターネット接続系に業務端末を配置するケース、あるいはモバイルワークシフトに合わせて庁内ネットワークも見直すケース。 • LGWAN接続系とインターネット接続系で端末分離している場合、端末調達を機に台数の最適化を行いインターネット接続系に集約することも想定される。
統合仮想基盤更新時	• 業務システムやセキュリティ関連システムが同一のインフラ基盤上で稼働している場合で、仮想基盤の更改時にβ´モデルに移行するケース。 • メリットとして、業務システム環境設定がネットワーク変更と同時に行える点が考えられる。
クラウドサービス接続時	• クラウドサービス（グループウェア、Web会議、コミュニケーション基盤、クラウドストレージ等）の利用開始時期に合わせ、β´モデルへの移行を実施するケース。
新たに移行日を設定	• 既存システムの調達サイクルは意識せず、最短で移行可能な時期を設定する場合や、業務影響が最小化されるタイミングを見計らって移行するケースなどが考えられる。

（ご参考）αモデルからβ'モデルへ移行した際の工夫点

✓ αモデルからβ'モデルのネットワーク構成に移行した82団体における工夫点は以下のとおり。

人材のスキル面

専門職員の確保

- 庁内公募（ネットワーク知識）
- 長期に情報担当課に勤務する職員（常駐SEを含む）が存在
- 他団体との意見交換・聴取
- 行政（ICT）枠の職員採用
- 外部研修への参加

全職員の知識・スキル向上

- 段階に分けて経営層や管理職、全職員に周知
  - ✓ 目指すべきβ'モデルの明確化（ネットワーク・システム構成および利用者視点での変更点　など）
  - ✓ β'への移行方針の策定（移行体制・役割分担の整理、スケジュール、費用　など）
  - ✓ 説明用のコンテンツの準備（コンテンツ、操作手順　など）
  - ✓ 職員への周知、イントラ掲載（朝会、研修会およびFAQの充実　など）

委託事業者の活用

有識者の確保

- β'モデルに知見のある事業者人員
- 庁内NW管理事業者　など

構想検討の支援

- 設計業務の外部委託以外に中立的な立場でのアドバイスをもらうためにコンサルタントを契約した
- 責任分界点を意識した
- 既設ネットワーク導入業者等を選定し設計業務を外部委託した

技術的な支援

- 技術的な観点で、既存の構成から現実的な移行を実現するために既存の委託事業者へ外部委託
  （EDR、VDI、セキュアブラウザなどの検討項目を提示）

委託事業者との検討期間（一例）

- ２年間（定期的な検討会）

セキュリティ対策面

EDR（エンドポイント）

- 県のセキュリティクラウドの活用

ログ管理・監視

- 資産管理ソフトとEDRの連携（監視運用の設計も含む）

メール対策

- メール無害化の継続
  （インターネットから受信するメールは引き続き無害化の構成）

その他

- 庁内システムへの通信要件の再精査
- Webフィルタリング
- シンクライアントの導入
- AI振る舞い検知
- 端末管理ソフトによる許可されたUSBメモリ以外の利用制限

３．モデルケース

モデルケース１（三重県）

（１）基礎情報

項目	内容
区分（都道府県市町村）	都道府県
団体の規模（職員数）	約23,000人
移行方式	一括移行（業務端末および業務システムを一度に移行）
EDR共同の実施有無	実施中
β´モデル移行の目的	・徹底的な業務効率化、生産性の向上（※） ・データ利活用による新サービス創出 取組１：クラウドシフトによるコミュニケーションの活性化 取組２：ゼロトラストと柔軟な働き方の実現 取組３：データドリブンの実現に向けた活用の推進 ※インターネット利用に係る業務の効率化（画面転送、無害化処理の見直し）。職員の業務環境が大幅に改善されることに伴い、住民への情報提供、回答も迅速化し、行政サービス向上となる。

（２）移行にかかった期間、体制、費用等の概要

項目	内容
移行にかかった作業期間	約６カ月
プロジェクトに携わった自治体職員	11人
プロジェクトに携わった人数（外部委託を含む）	17人
総合的な費用	・基盤整備（β´モデル移行作業費およびセキュリティ監査作業）：移行費用（4年総額） 約1億円 ・庁内ネットワーク更新およびクラウドサービス利用経費も含めた総事業費は約23億円（6年総額）※上記基盤整備を含む

モデルケース１（三重県）

（３）移行時の苦労話や工夫したい点、移行して良かった点について

- **苦労した点**

・一括移行・段階移行等の移行方式検討
・リソース増強に関わる検討（インターネット接続系のサーバリソース増加等）
・情報セキュリティポリシーガイドラインに規定されているセキュリティ対策の実装に係る検討
・既存資産に与える影響の分析及び構築（既存ネットワークの再設計、庁内仮想基盤、ファイルサーバ、認証基盤等の再設定）
・端末や業務システムの移行に伴う新たなIPネットワーク体系の検討及び構築

- **工夫した点**

＜人材のスキル面＞
・ネットワークに関するノウハウを持つ人材の確保
＜委託事業者の活用＞
・既存ネットワークの設計ノウハウを生かした再設計
＜セキュリティ対策＞
・EPP,EDRによるエンドポイント対策
・（追加要素）SASEの導入によりゼロトラストの考え方に基づいたテレワーク環境の導入
・インターネットアクセスに関し、αモデル時は仮想端末経由であったが、β´モデル時は端末直接接続に変更となっている。ただし、同じProxy経由でのアクセスとしたため、都道府県セキュリティクラウド側の設定変更が生じなかった。庁内に設置したProxyの設定変更（端末からの直接アクセスを許可）とスペック増強は必要であった。
＜予算申請＞
・予算当局への丁寧な説明

- **移行後の新たな課題**

・セキュリティ脅威の増加
・ネットワークセグメント間の通信に係る制約（ネットワーク分離・ネットワーク分割等）

モデルケース２（団体B）

（１）基礎情報

項目	内容
区分（都道府県市町村）	市町村
団体の規模（職員数）	約700人
移行方式	一括移行（業務端末および業務システムを一度に移行）
EDR共同の実施有無	未実施
移行のきっかけ （業務の課題、市民からの期待等）	既存のネットワーク機器サポート終了に伴うネットワーク更改が必須となり、同時期に国のセキュリティポリシーに関するガイドラインが改定されたことにより、新たなセキュリティ強化モデルの検討が可能となったため。

（２）移行にかかった期間、体制、費用等の概要

項目	内容
移行にかかった期間	検討期間を含め、約２年間
プロジェクトに携わった自治体職員	約７人
プロジェクトに携わった人数 （外部委託を含む）	約５０人
総合的な費用	移行費用：約２億５千万円 運用経費（5年総額）：約２８億円 ※ネットワーク構築費、ネットワーク機器、運用保守費、クラウドサービス利用料（コミュニケーション　ツール等）、クラウド接続回線、外部監査等が含まれる。

モデルケース２ （団体B）

（３）移行時の苦労話や工夫したい点、移行後の課題について

- **苦労した点**

・内部検討の際、三層分理からの説明が必要となり、各セキュリティモデルの運用イメージを持ってもらうことに苦労した。
・コロナ禍の影響を受けて半導体不足による機器類調達が不安視される中でのβ´モデル移行への設計構築であり、予算措置、プロポーザルからの契約締結に期間的な余裕がほとんどなかった。
・運用開始当初は、効率性が高まったものの大きな変更を伴うβ´モデルでの業務運用について、情報システム部門への問い合わせ等が大幅に増大した。

- **工夫した点**

＜人材のスキル面＞
・当自治体職員は数年おきの異動が想定されるため、新規配属された職員でも、基礎的な対応はできるように、運用に関するドキュメントを納品前に職員のチェックを行った。
・ユーザー目線に立ち、研修開催だけでなく、グループウエア等に適宜、利用に関する情報を掲載した。
＜委託事業者の活用＞
・一般的な設計構築委託や新規製品の説明にとどまらず、新規製品のテスト、当自治体においての向き・不向き、実運用上懸念される課題について、ほぼ毎週打合せを行い、業者のノウハウを職員に浸透させるようにした。
＜セキュリティ対策＞
・特段新たなものはなく、一般的なセキュリティ対策の積み上げ。セキュリティクラウドによる外部からのデータのチェック、端末管理ソフトによる許可されたUSBメモリ以外の利用制限、イントラネット側への許可された端末のみの接続制限、週毎のウイルス対策ソフトの定時スキャン等）。金額面、運用面を考慮し、セキュリティクラウドで提供されるEDRを導入した。
＜予算申請＞
・内部情報ネットワークの更改が必須の状況下において、国のセキュリティポリシーに関するガイドライン改定によりβ、β´モデルの検討が可能となったことから、αモデル継続とβ又はβ´モデル採用との比較検証を行い、特に国が今後目指す方向性や導入に係るコスト増を上回る運用メリット等の説明を綿密に行った。

（３）移行時の苦労話や工夫したい点、移行後の課題について

- **移行後の新たな課題**

・セキュリティ脅威の増加
・導入維持コストの増加（セキュリティ対策費用等）
・不具合発生時の責任分界点の分析、判断（業務運用の変更やシステム改修、クラウドサービス利用開始に伴い、一時的に問合せが増加したり、インシデント発生時の障害切り分けが難しくなること等が考えられる）