資料１

各検討項目の改定方針

総務省

令和５年12月19日

総務省自治行政局

デジタル基盤推進室

β′モデル 移行のための支援方策の検討/
LGWAN接続系のローカルブレイクアウト（α′モデル）の検討

今後の方向性（前回提示）

✓ 団体のネットワーク環境に応じた支援を検討することとしてはいかがか。

✓ αモデル採用団体のうち、β‘移行を希望している団体は一定数存在しているものの断念している場合が多い。
✓ β‘に移行した団体から、β’移行にあたっての工夫点が共有されている。

β‘移行の事例や移行にあたっての工夫を横展開することで、
β’モデルへの移行を推進してはいかがか。

✓ 他方、政令指定都市以外の市町村の大多数が、業務環境がインターネットから分割されたαモデルの状態で、インターネットに接続しクラウドサービスを利用する必要があると考えられる。

セキュリティ対策を徹底の上、LGWAN接続系から
Web会議等の特定のクラウドサービスに対して
直接接続を行うモデル（α‘モデル）を検討してはいかがか。

前回いただいたご意見

- ✓ β′モデルについて、移行推進に賛同する意見をいただいた一方、**導入等に係るコストを勘案した支援策が必要**との意見をいただいた。
- ✓ また、国の方策をそのまま取り入れるのではなく、**個人情報の漏えいを防ぐことを重視すべき**との意見をいただいた。
- ✓ コストや安全性を考慮し、β‘モデルの事例や移行手順を示すことが重要なのではないか。

検討項目	視点	発言要旨
β‘モデルの移行/ゼロトラストアーキテクチャ	β′モデルのコスト	• 小規模自治体では、**β′モデルへの移行を検討したことがないとあるが、どのようにすれば検討してもらえるかを研究する必要がある**。おそらく**移行・導入コストや移行を検討するコストが大きく見えている**と思う。 • αからβに移行することによってセキュリティを緩める方向になることから、後ろ向きになってしまう地方公共団体が出るのは明らかである。また**β′モデルは、運用コストが高い**ため、小規模自治体には、β′に移ろうという気が起こらない場合も少なくない。β′モデルの推進ありきにならないように議論を進めてほしい。
	将来像	• 令和２年にβ′モデルが出た時に、将来的にはインターネットに接続するシステムか、保護すべきシステムかの２層に分けていくことを目指していると思っている。そのため、**β′モデルに多くの地方自治体を誘導するということに対して賛成**である。 • 政府が示す、**インシデントが起こることを前提に被害を最小限に抑えるというゼロトラストの考え方に従うと、個人情報は漏れる前提といった問いが生じる**。そのため、**政府が示すものをそのまま採用することは危険**である。

前回いただいたご意見

- ✓ LGWAN接続系のローカルブレイクアウト（α'モデル）について、接続先やファイル添付等、安全性の観点からの意見をいただいた。
- ✓ **第三者認証を活用することで、接続先のクラウドサービスの安全性を担保**し、**ファイル添付を視野に入れたリスクアセスメントを実施**することが重要なのではないか。
- ✓ なお、帯域確保のためのコストの観点と、LGWAN-ASPとしてサービスを提供するか否かは事業者の判断になることを踏まえ、LGWANからローカルブレイクアウトをする方策を検討する必要がある。

検討項目	発言要旨
LGWAN接続系のローカルブレイクアウト（α'モデル）の検討	• αモデルにおけるローカルブレイクアウトについて、**接続先がどこかが重要**であり、ローカルブレイクアウトの接続先を限定することが必要である。 • 業務で使用しているコミュニケーションツール等は、特定の通信を止めると使えなくなることが分かっており、GAFAMの通信先であっても安全とは限らない（インターネットに直接繋いでいるリスクとあまり大差がない）ため、気を付けなくてはならない。 • 更にクラウドサービスの利用が進むとクラウドサービスに対するデータの流れを含めた監視も考える必要がある。 • ローカルブレイクアウトは、接続先以外との通信がないため安全という考え方であるが、**アップロードやコミュニケーションツール上でファイル添付ができるため管理は必要**である。 • ローカルブレイクアウトは、**地方公共団体にてなし崩し的に推進されていることに危機感を持っている**。まずLGWANという仕組みを活かして改善していくという方法があるのではないか。

β'モデルやα'モデルを提示する意義

- ✓ ガイドラインでインターネット利用に係る適切なセキュリティ対策を提示しない場合、**自治体の独自判断で、外部サービスの利用などが行われるケースが多くなる**と考えられる。
- ✓ **β'モデルやα'モデルの形で、パブリッククラウドサービスを安全に利用するための必要なセキュリティ対策を示すことが重要なのではないか。**

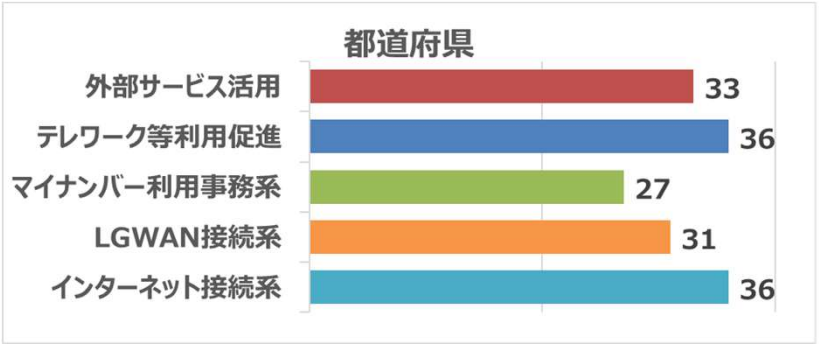
地方公共団体へのアンケート結果

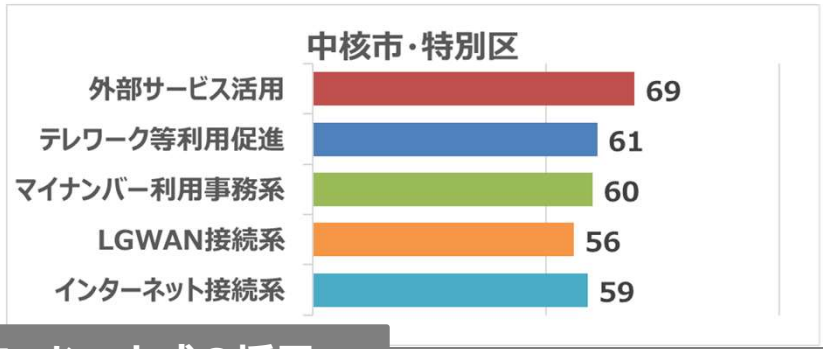
外部サービスの利用、テレワーク利用促進、インターネット接続系の利便性向上など、インターネット利用に係るニーズが増えている。

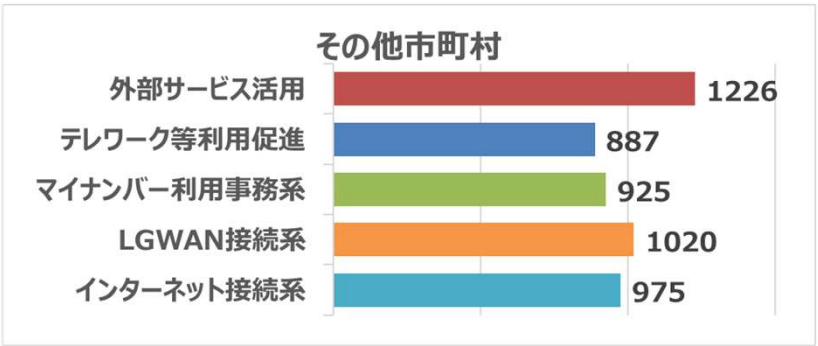
回答数	都道府県 47団体	政令指定都市 20団体	中核市・特別区 85団体	その他市町村 1578団体

※ 未回答２　※ 未回答16

- グループウェア、市民向けポータル、電子申請等の外部サービスを活用
- テレワーク等の利用促進（場所を選ばない働き方への移行等）
- マイナンバー利用事務系セグメントにおける利便性向上（画面転送、電子決裁、端末の持ち運び・持ち出し、認証等）
- LGWAN接続系セグメントにおける利便性向上（無害化通信、画面転送、認証等）
- インターネット接続系セグメントにおける利便性向上（画面転送、暗号化、認証等）







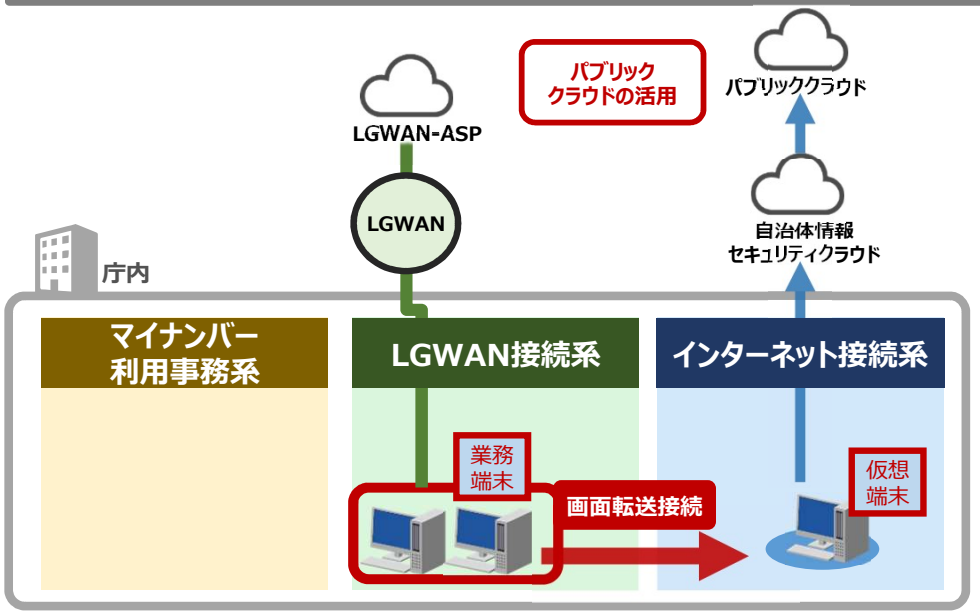
ガイドラインに規定されていない方式の採用

- α'モデルに必要なセキュリティ対策は、本検討会で対策案を検討する予定だが、既に複数の団体が、LGWAN接続系からローカルブレイクアウトを実施しパブリッククラウドサービスを利用している旨が民間事業者のHPにおいて掲載。
- 前回検討会でも、「なし崩し的に推進されていることに危機感を持っている」との指摘があった。

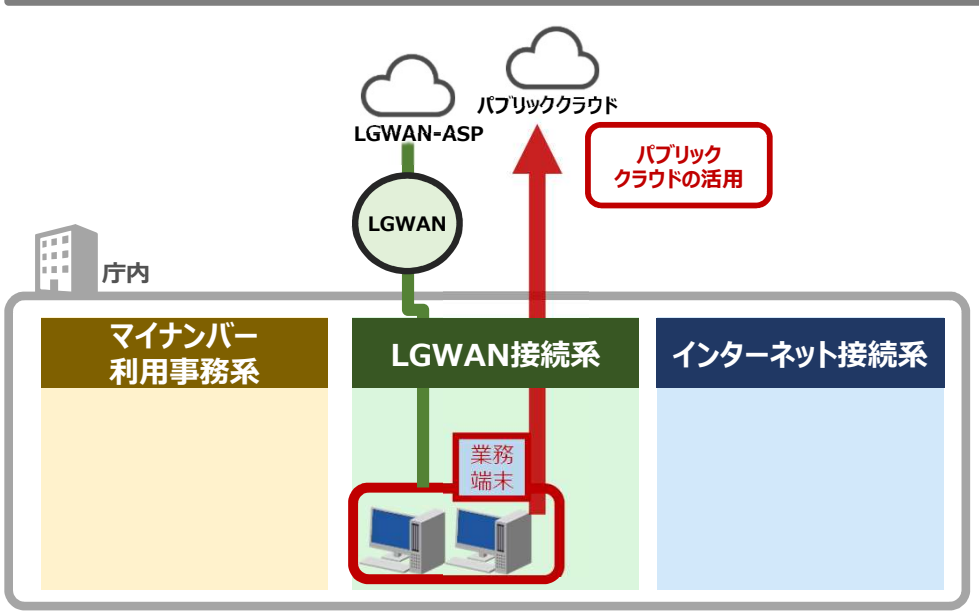
リスクアセスメント概要

✓現行ガイドラインで認められている都道府県セキュリティクラウド経由のローカルブレイクアウトを比較対象とし、LGWAN接続系からのローカルブレイクアウトのセキュリティリスクを分析する。

都道府県セキュリティクラウド経由のローカルブレイクアウト



LGWAN接続系からのローカルブレイクアウト



現行ガイドラインにおけるローカルブレイクアウトの記載

第2章 情報セキュリティ対策基準（解説）

3．情報システム全体の強靭性の向上

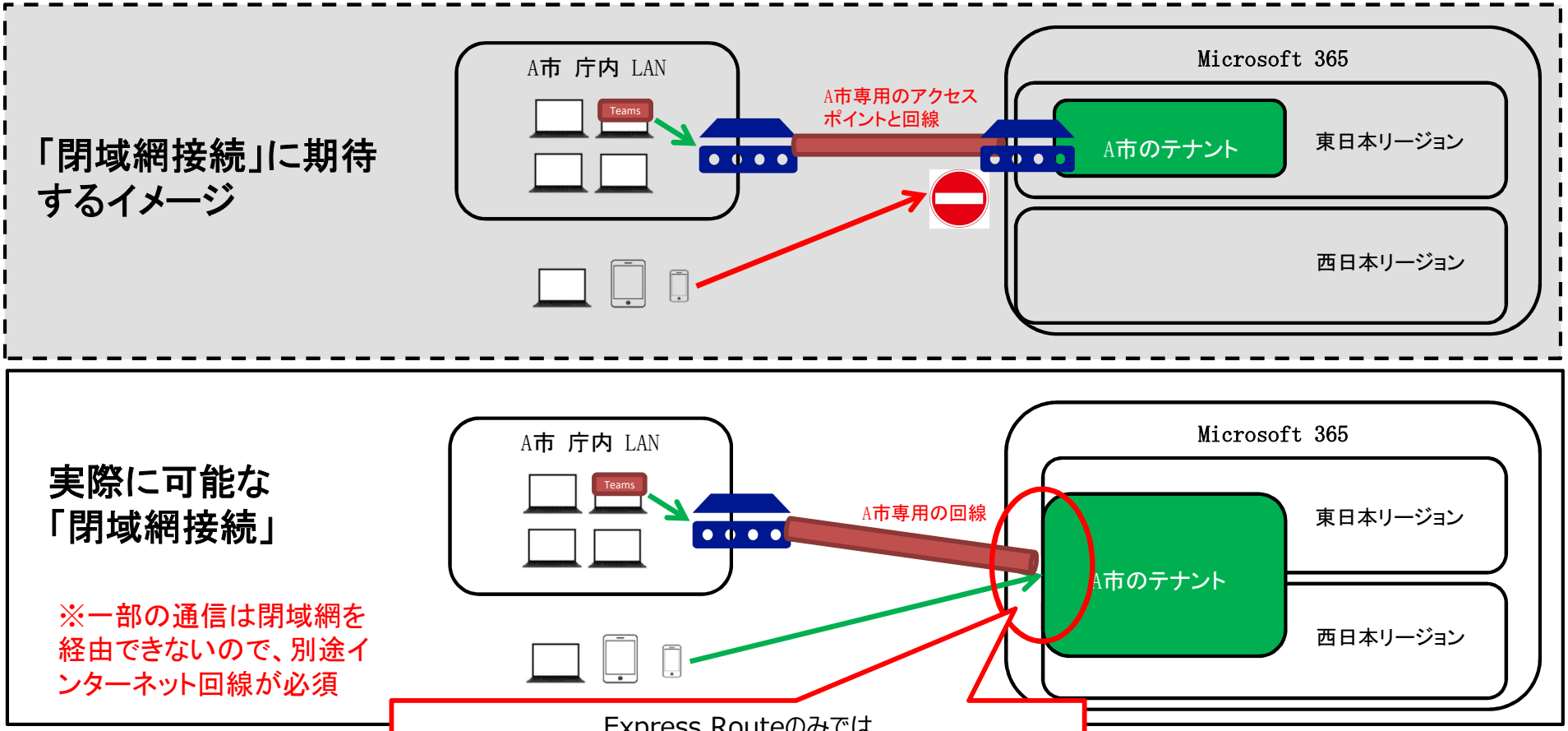
（3）インターネット接続系

自治体情報セキュリティクラウド構成団体からのクラウドサービスの利用増加等に伴うトラフィック増加に対応するため、ローカルブレイクアウトを行う場合には、その実施可否について、セキュリティ上のリスクを勘案し、都道府県、市区町村で協議の上、慎重に判断する必要がある。ローカルブレイクアウトを行う場合は、原則として、都道府県側の設定により、実施することとする。その場合、当該ルートを狙った攻撃等のリスクの増加を十分に理解した上で、例えば、信頼できる事業者が提供する特定のクラウドサービスのみローカルブレイクアウトを認める、構成団体と１対１で紐づく通信元 IP・ポート番号と通信先 IP・ポート番号をもとに通信をポリシーベースルーティングで振り分ける、ログイン状況やアプリケーションの利用状況の監視を行うなどといった適切なセキュリティ対策を講じるとともに、セキュリティインシデント発生時の対応手順をあらかじめ用意する必要がある。

参考：Microsoft 365への接続回線について（日本マイクロソフト社より）

✓ 自治体からのニーズが大きいパブリッククラウドサービスが、**インターネット回線での接続を前提**としている。

- Microsoft 365（M365）は、世界中どこからでも快適にサービスを利用することと、データセンターレベルの障害でもサービスを継続して提供（東日本リージョン、西日本リージョンでデータを冗長化）することを可能とするため、**インターネット回線での接続を前提**としている。
- M365 を利用する際に、ExpressRoute と呼ばれる専用線サービスを利用することは可能だが、**当該専用線サービス は、あくまでもパフォーマンス向上を目的とした帯域を保証する環境で費用を要する**上に、**外部からの接続を遮断するものではない**。
- さらに、**認証などの一部の通信は、閉域網を経由できない**ため、別途インターネット回線を自治体側で用意する必要がある、



リスクアセスメント概要

- ✓ 第三者認証制度による接続先の安全性担保、インターネット回線の利用を視野に入れてリスク評価を実施することとしてはいかがか。
- ✓ パブリッククラウドのサービス範囲に応じ、 それぞれのケースを想定したセキュリティ対策を検討してはいかがか。

リスク評価の観点

- ✓ SaaS型サービスセキュリティは、ユーザ（自治体）側で完全に制御することが難しいため（※）、利用するパブリッククラウドの安全性を担保する方策が必要となる。
  - → **ISMAPに登録されているサービス等、第三者認証により安全性が担保された接続先にのみ接続先を認める**方向性。

※例えば、ゲートウェイ機器をSaaSのデータセンターに自由に設置できないことなどが考えられる。

- ✓ 接続に用いる回線について、パブリッククラウドのサービス特性、帯域確保（特にWeb会議で利用する場合）および導入維持コストの観点を踏まえ、安全性を確保する必要がある。
  - → **インターネット回線の利用を視野に入れた接続構成**にて検討。
- ✓ 利用するパブリッククラウドのサービス範囲に応じ、セキュリティリスクが異なる。
  - → 認証のみ実施する場合と、外部とファイル送受信が発生する場合ではセキュリティリスクが異なるため、コストの観点から、**それぞれのケースを想定したセキュリティ対策を検討**。

認証等	コミュニケーションツールの利用	外部とファイル送受信が発生
＜例＞ ■ 認証・認可 ■ ウイルス定義ファイル配信	＜例＞ ■ 認証・認可 ■ ウイルス定義ファイル配信 ■ Web会議、チャット	＜例＞ ■ 認証・認可 ■ Web会議、チャット ■ ファイル送受信等

小 → セキュリティリスク → 大

ガイドライン上の機密性分類と政府機関の機密性分類の考え方の違いや具体例の追記

背景及び今後の方向性（前回提示）

- ✓　現行の総務省ガイドラインの機密性分類について、どのような情報を想定しているかの具体的な記載がないため、政府機関等における機密性の分類との違いがわかりにくい。
- ✓　**政府機関等における機密性３情報に相当する情報を扱う情報システムは、ガバメントクラウドの利用対象外**で、機密性２情報（個人情報含む）に相当する情報を扱う情報システムについては、ガバメントクラウドの利用を原則とされている（※）ため、総務省ガイドラインと政府機関等統一基準の違いを知らず、「個人情報を扱う地方公共団体の情報システムは、ガバメントクラウドの利用ができないのではないか」と混乱するケースが発生した。
- ✓　地方公共団体では、税や住民基本台帳、生活保護等の業務があるため、個人情報を業務で使用する頻度が政府機関よりも圧倒的に多く、情報漏えい等のリスクも大きいと考えられる。

- ✓　**現行の総務省ガイドラインの考え方を変えず、個人情報を最も機密性に配慮すべき情報（機密性３情報）として扱うことが望ましいのではないか。**
- ✓　**具体例の追記や政府機関の分類との相違を明記する必要があると考えられる。**

※「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」（令和４年12月28日デジタル社会推進会議幹事会決定）

前回いただいたご意見

- ✓ 前回の検討会では、**個人情報の取扱いについて多くの意見をいただいた**。
  - ➢ 機密性の分類における**個人情報の取扱いが、インターネット経由でクラウドサービスを利用する妨げにならないように**検討が必要。
  - ➢ 個人情報について、**住民の情報が台帳形式になっているものと、それ以外（特に職員の個人情報）は分ける**。
  - ➢ 「自治体」を機密性分類の前に付けるなど、ラベリングで区別。
- ✓ 多くの意見をいただいたことを踏まえ、**本検討会では改定の方向性を示す**こととし、**次回改定案を提示する**こととする。

検討項目	視点	発言要旨
機密性の分類	個人情報の分類	• 総務省では、令和２年の通知で「住民の個人情報、職員の個人情報等の非公開情報」と記載しているが、地方公共団体の実情は、住民の個人情報が必ずしも非公開とはなっていない。また従来の使い方としては、職員の個人情報はLGWAN接続系に置かれ、住民の個人情報はマイナンバー利用事務系に置かれる等、分けている。 • 機微性が高い情報は管理方法が異なるため、総務省ガイドラインに、**すべての個人情報を機密性３にすると記載してしまうと、範囲が広くなりすぎてしまうということを懸念**している。 • 個人情報は機密性が高いためクラウドサービス利用ができない等、地方公共団体の中では思考停止になっているところがある。**人事情報と一般的な住民情報を分けることや、文部科学省のガイドラインを参考にする等、個人情報を一律に機密性３としないことも大事ではないか**。 • 今後、ガイドラインで例示するとのことだが、台帳は機密性３だと考えているが、電子申請のトランザクションデータのように個々に発生するものは機密性２に該当するのではないか等、**クラウドサービスの利用促進を妨げないような例示が必要**。 • 個人情報の考え方にて、**全住民を集めている台帳と住民から個別に申請が来る情報、住民情報では、長時間使うシステムと短時間で終わるシステム等で考え方を変えることにより、クラウドサービスをより活用できる**と思うため、ガイドラインに記載されていると良いのではないか。 • 個人情報だから大事という思考停止的な発想ではなく、**使われ方がもたらすリスクを考えた上で重要性が高いと判断すべき**と考える。ただし、ガバメントクラウドの利用対象外なのか否かで取り扱いが変わってくるため、地方公共団体の現場で困らないようにより具体的に方向性を示すべきではないか。
	分類の名称	• 機密性のラベリングについて、NISCと地方公共団体で同じラベリングをしているが、内容が異なるため、同じ言葉を使うと現場に混乱を招くことが懸念される。そのため、**例えば「自治体」を「機密性３情報」の頭あるいは間に付ける等で、ラベリングを区別しやすくすればよいのではないか**。

現行の政府機関と地方公共団体における機密性範囲の違いについて

✓ 現状は、国とガイドラインで、機密性分類における個人情報の位置づけが異なっている。

国の行政機関
（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（統一基準））

機密性３

国の行政機関における業務で取り扱う情報のうち、行政文書の管理に関するガイドライン（平成23年４月１日内閣総理大臣決定）に定める**秘密文書（※１）としての取扱いを要する情報**

※１　秘密文書とは
- **極秘文書**　**秘密保全の必要が高く、その漏えいが国の安全、利益に損害を与えるおそれのある情報**を含む行政文書
- **秘文書**　**極秘文書に次ぐ程度の秘密**であって、関係者以外には知らせてはならない情報を含む極秘文書以外の行政文書

機密性２

国の行政機関における業務で取り扱う情報のうち、**行政機関の保有する情報の公開に関する法律（平成11年法律第42号。以下「情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報（※２）**であって、「機密性３情報」以外の情報

※２　情報公開法第５条第１号に、**個人に関する情報**が掲げられている。

機密性１

国の行政機関における業務で取り扱う情報のうち、情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報

「政府情報システムにおけるクラウドサービスの適切な利用に係る基本方針」（令和４年12月28日デジタル社会推進会議幹事会決定。以下「クラウドサービス基本方針」という）の適用対象外

ガバメントクラウドの利用が原則とされている（クラウドサービス基本方針の適用対象）

地方公共団体（本ガイドライン）

機密性３

行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産（※３）

※３　令和２年８月１８日付総行情第111号の別添で**住民の個人情報**、**職員の個人情報**、施設設計情報や入札予定価格など非公開情報を例示

機密性２

行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、**直ちに一般に公表することを前提としていない**情報資産（※４）

※４　令和２年８月１８日付総行情第111号の別添で**政策検討に関する情報**を例示

機密性１

機密性２又は機密性３の情報資産以外の情報資産

現行のガイドラインにおける機密性３情報の取扱い

✓ 機密性２以上の情報資産は公表しないことを鑑み、基本的に同じ取扱制限を設けている。
✓ β'モデルでは、**機密性３情報に相当する情報がインターネット接続系に配置**されると規定されている一方で、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の整備や運用の徹底等を規定。
※ 自治体から、β'モデルでは、**機密性３に分類される住民の個人情報が、文書管理システムに保存される形でインターネット接続系に置かれるため、矛盾が生じている**との意見があった。

機密性による情報資産の分類

分類	分類基準	取扱制限
機密性３	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	・支給端末以外の端末での作業の原則禁止（機密性３の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性２	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
機密性１	機密性２又は機密性３の情報資産以外の情報資産	―

（３）インターネット接続系
（β´モデルを採用する場合）業務の効率性・利便性の向上を目的として、**インターネット接続系**に主たる業務端末と入札情報や職員の情報等**重要な情報資産を配置**する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

図表29 β'モデルにおける必須のセキュリティ対策について

対策区分	セキュリティ対策	概要
技術的対策	～（略）～	
組織的・人的対策	～（略）～	～（略）～
	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。
	～（略）～	～（略）～

住民の個人情報が含まれるエクセル表が、そのままの状態でインターネット接続系のファイル共有サーバに保存されないようにすること等が目的

β'であれば、職員のマイナンバーは、条件付でインターネット接続系に保存可

（注11）**β'モデルで取り扱う重要な情報資産とは、機密性３に該当する秘密情報に相当する機密性を要する情報資産を想定**する。なお、**インターネット接続系に職員のマイナンバー情報を配置する場合には、情報の取扱いに十分留意し、アクセス制御等のセキュリティ対策を適正に実施する必要がある**。

自治体における個人情報の取扱い

✓ 自治体における個人情報の取扱いについて調査（※）した結果を踏まえると、**職員や外部有識者の個人情報、オンライン申請等の処理上一時的に保管する個人情報**は、**インターネット接続系で取り扱われる場合も想定し、ガイドラインに記載する必要があると考えられる**。※都道府県2団体、特別区1団体、市町村3団体（政令市、中核市以外）聞き取り

情報の形式／性質	区分	情報の種類	扱う情報システム等	設置セグメント
基本４情報等を束ねたリスト（台帳）	住民の個人情報	氏名、性別、住所、各種資格情報、住民のマイナンバー等	住民記録システム、税務システム、国民健康保険システム、生活保護システム等	主にマイナンバー利用事務系 ※ただし自治体によっては、**選挙人名簿管理システム、学齢簿システム等をLGWAN接続系に配置している場合がある**
		氏名、性別、住所等	文書管理システム（決裁文書に住民情報）	主にLGWAN接続系 ※ただし**β'モデル団体は、文書管理システムをインターネット系に配置している場合がある**。
	職員の個人情報	氏名、性別、住所、所属、職位等級、職員のマイナンバー等	人事給与システム、庶務事務システム等	主にLGWAN接続系 ※ただし**β'モデル団体は、左記の人事給与システム、庶務事務システム、財務会計システムをインターネット系に配置している場合がある**。
	外部有識者、CISOアドバイザーなどのリスト	氏名、口座等	財務会計システム、ファイル共有サーバ（エクセル表による管理）等	
	各種名簿情報	氏名、住所、口座、各種資格情報等	農業委員会台帳システム、戦没者台帳システム、貸付金償還システム、許認可・免許管理システム、ファイル共有サーバ（エクセル表による管理）等	
上記以外	システム処理上**一次的に保管する情報**	氏名、性別、住所等	電子申請システム、施設予約システム等	主にLGWAN接続系
	外部とのデータ授受等により**一時的に保管する情報**	イベントの運営者や出席者リスト等	ファイル共有サーバ（エクセル表による管理）	**主にインターネット接続系**

ガイドラインの改定の方向性①

ガイドライン改定の方向性

◆ 機密性分類の名称

- 国の分類との混同を避けるため、名称を「**自治体機密性**」とした上で、自治体機密性３については、**個人情報の種類を考慮した上でA~Cの３段階に分類**し、それぞれについて具体例を明示してはいかがか。

◆ 分類基準の見直し

- 個人情報保護法の安全管理措置との整合性をとる形で、分類基準を見直してはいかがか。

個人情報の保護に関する法律についてのガイドライン （行政機関等編） （令和 4 年 9 月一部改正 個人情報保護委員会）

5-3-1 安全管理措置

(1) 行政機関の長等の安全管理措置義務

行政機関の長等は、保有個人情報の漏えい、滅失又は毀損（以下「漏えい等」という。）の防止その他の保有個人情報の安全管理のため、必要かつ適切な措置（以下「安全管理措置」という。）を講じなければならない（法第 66 条第 1 項）。

（ 略 ）

求められる安全管理措置の内容は、保有個人情報の**漏えい等が生じた場合に本人が被る権利利益の侵害の大きさを考慮**し、**事務又は業務の規模及び性質、保有個人情報の取扱状況（取り扱う保有個人情報の性質及び量を含む。）、保有個人情報を記録した媒体の性質等に起因するリスクに応じて、必要かつ適切な内容**としなければならない。

◆ 利用可能なクラウドサービスの範囲

- **標準化対象業務システムのガバメントクラウドへの移行が努力義務とされていることを受けて、ガバメントクラウドでは、標準化対象業務システムが取り扱っている自治体機密性３情報を、基本的には扱うことが可能である旨を記載**してはいかがか。
- ガバメントクラウド以外のパブリッククラウドサービスで、自治体機密性３情報を扱う場合には、**原則ISMAPに登録されているクラウドサービスを使用する**ものとしてはいかがか。

ガイドラインの改定の方向性②

ガイドライン改定の方向性

- 自治体の意見を踏まえ、β'モデルの業務システムにおける個人情報の取扱いについて、矛盾が生じないようにセキュリティ対策の説明を修正してはいかがか。

改定案：対策基準(解説)

図表27･29　β･β'モデルにおける必須のセキュリティ対策について

対策区分	セキュリティ対策	概要
技術的対策	～（略）～	～（略）～
	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、保管を実施する方法
	～（略）～	～（略）～
組織的･人的対策	～（略）～	～（略）～
	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（業務システムに保存されている場合は除く）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。
	～（略）～	～（略）～

（注11）β'モデルで取り扱う重要な情報資産とは、自治体機密性３に該当する秘密情報に相当する機密性を要する情報資産を想定する。なお、インターネット接続系に職員のマイナンバー情報を配置する場合には、情報の取扱いに十分留意し、アクセス制御等のセキュリティ対策を適正に実施する必要がある。

情報システムの品質管理の推進に関する対応

背景及び今後の方向性（前回提示）

✓　コンビニ交付サービス等の証明書発行サーバにおいて、誤ったプログラム処理が生じたことにより、別人の証明書が交付される事案が発生した（※）　。

サービスの品質確保や個人情報保護の観点から、一連の事案で顕在化した課題に対応するための対策を、具体例を交えつつ記載してはいかがか。

○コンビニ交付サービス等において別人の証明書が交付された事案

団体	①	②	③	④	⑤
原因	証明書発行サーバに交付申請が集中した際に、**誤ったプログラム処理が生じ**、証明書データの取り違えが発生	証明書発行サーバの印刷処理と同サーバに対する住民基本台帳システムからの住民票データの反映処理が同時に行われた際に、**誤ったプログラム処理が生じ**、証明書データの取り違えが発生	証明書発行サーバと戸籍システムの間の当該自治体固有の連携システムにおいて、２名の同時申請が行われた場合に、**誤ったプログラム処理が生じ**、証明書データの取り違えが発生	庁内証明書交付サービスとコンビニから同時に交付申請があった場合に、サーバにおいて**誤ったプログラム処理が生じ**、証明書データの取り違えが発生	庁内証明書交付サービスにおいて、住所変更等の手続後、システム更新中に申請があった場合に、サーバにおいて**誤ったプログラム処理が生じ**、証明書データの取り違えが発生
延べ件数 事案発生日	10件 R5年3月27日	2件 R5年3月22日、4月18日	1件 R5年5月2日	1件 R5年3月27日	1件 R5年6月28日
誤交付した証明書	• 住民票の写し • 住民票記載事項 • 印鑑登録証明書	• 住民票の写し • 印鑑登録証明書	• 戸籍全部事項証明書	• 戸籍全部事項証明書の一部	• 住民票の写し
その後の対応	• プログラムを修正 • 3月31日付け事務連絡で総務省から自治体に運用監視の徹底を要請	• プログラムを修正 • 5月2日付け事務連絡で自治体に証明書発行サーバの運用管理を委託している事業者への点検を依頼	• プログラムを修正 • 5月10日付け事務連絡で関連システムを含めて誤交付が生じうる仕組みとなっていないか至急点検するよう要請	• システムを停止 • 5月22日付け通知で、証明書発行サーバ及びこれと連携する印鑑登録等の各業務システムの総点検の徹底を要請	• プログラムを修正（適用漏れしていた修正プログラムを適用） • ベンダーにおいてシステム利用団体の再点検を実施

※参考資料「コンビニ交付サービスにおける住民票等誤交付事案に対する個人情報の保護に関する法律に基づく行政上の対応について」（令和５年９月 20 日個人情報保護委員会）参照。

前回いただいたご意見

- ✓ 自治体の負担軽減の観点から意見をいただいた。
- ✓ **品質管理は、情報システム全般に求められる**ところ、**契約やリリース前のテスト等に係る留意事項をより詳細に記載**することで、地方公共団体が整備・運用する情報システム全般の品質管理を推進し、大規模なインシデントの防止を図ることとしてはいかがか。

検討項目	発言要旨
情報システムの品質管理	• 小規模の地方公共団体は、契約や契約後の管理はベンダーに任せきりになりがちで、職員自らが管理するリソースは不足していると考える。そのため、**契約上の注意点や契約した後にベンダーへの要求事項を具体的に**分かるようなガイドラインの記載を検討する必要がある。 • コンビニ交付サービスに関する事案に対する対策として、サービス選定をする際、J-LISの受入れに関する基準を明確にする等、**地方公共団体への負荷が軽減される仕組みを考えていくことが必要**である。 • コンビニ交付については、J-LIS等がどこのパッケージソフトであれば大丈夫である等の保証する形がとれると、地方公共団体としてはコンビニ交付サービスを利用しやすくなるのではないか。

「コンビニ交付サービスにおける住民票等誤交付事案に対する個人情報の保護に関する法律に基づく行政上の対応について」（令和５年９月 20 日個人情報保護委員会）

✓　今年９月に公表された、個人情報保護委員会の指導文書で、事業者との契約に関係する一般的な留意事項として、以下が規定されている。

- 事業者は、**テスト工程において、不具合を想定したテスト計画を行い、不具合を摘出して修正**すること。
- 地方公共団体は、**契約書において**、具体的に誤交付を防止するための技術的安全管理措置に関する取り決めを明記。
- 事業者は、**各地方公共団体に当該システムの利用を継続するか否かの判断を促すための材料を提供**すること。

第３ 問題点の検討

４ その他

⑴ 誤交付の直接的原因となったプログラム不具合について

本件のプログラム不具合は事前に想定可能な内容であり、富士通Japan は、**地方公共団体にプログラムを納品するまでの間のテスト工程において、当該不具合を想定したテスト計画を行うことで、当該不具合を摘出し修正する**ことを、各地方公共団体から期待される立場にあった。

⑵ 証明書交付サービス全般について

ア 本件で発覚した安全管理措置及び委託先の監督に不備に関する問題点は、**誤交付が実際に発生した地方公共団体のみならず、同サービスを利用する全ての地方公共団体に関係するもの**である。同種システムを用いて証明書交付事務を実施している地方公共団体においては、本件を機に、その特定個人情報又は保有個人情報の取扱い状況を改めて確認し、自ら窓口で住民に証明書を交付するのと同様に、システムを利用した際にも、誤交付を防止するための技術的安全管理措置が講じられているか、**契約書において、具体的に誤交付を防止するための技術的安全管理措置に関する取り決めを明記しているか**等を、改めて確認すべきである。

イ 富士通Japan においては、本件を機に総点検等を行い、組織的な再発防止を検討していると認められるところ、これまで、一つのシステム不具合が発生した後、類似の不具合の有無に関する調査等を組織的・網羅的に実行できず、**各地方公共団体に当該システムの利用を継続するか否かの判断を促すための材料を提供してこなかったことが、本件事態の影響を拡大させた**との批判は免れない。

「マイナンバーカード等に係る各種事案に対する個人情報保護委員会の対応について」

（令和５年12月６日個人情報保護委員会）

- ✓ 今年12月の個人情報保護委員会の公表資料で、コンビニエンスストアでの住民票等誤交付事案に関する富士通Japan株式会社における改善策の実施状況について記載。
- ✓ 富士通Japan株式会社は、各事案の修正プログラムを全て適用し、高負荷時の動作における動作検証等の他、処理中の中間データへの申請番号の付与、証明書の要求から証明書の作成にかけて、処理電文間で取り扱うデータの比較の実施といった、**異常検出機能の開発**を行う予定であることが記載。

住民票等誤交付事案に関する富士通Japan株式会社における改善策の実施状況について

別紙１

- 個人情報保護委員会は、コンビニエンスストアでの住民票等誤交付事案に関して、富士通Japan株式会社（以下「富士通Japan」という。）に対し、令和５年９月20日に指導を行い、同年10月31日までに改善策の実施状況について報告するよう求めていた。
- 今回富士通Japanから報告を受けた改善策の実施状況に関して、現時点において一定の取組が認められるものであった。
- 当委員会としては、今後も、改善策が確実に実施されることを、引き続き注視していく。

	指導事項	改善策の実施状況
１．技術的安全管理措置		
	証明書を交付する事務の実施にあたり、自社システムを利用するのであれば、当該システムの使用に伴う誤交付を防止するための技術的安全管理措置を適切に講ずること。	■類似の誤交付トラブルの横展開確認 令和５年６月17日までにトラブルの横展開確認を実施済みで、各事案の修正プログラムを全て適用、証明書発行プログラムの初期化漏れに関するロジック確認、高負荷時の動作における動作検証を完了。 ■異常検出機能の開発 自社システムの安全性向上のため、令和６年１月を目処に、以下の異常検出機能を開発予定。 ⑴コンビニ交付サービス内において、申請から証明書出力までの一貫性を保証するため、処理中の中間データに申請番号を付与し、取り違えを防止する機能 ⑵コンビニ交付サービスの手続中に、住民票の異動等のデータ更新があった場合の取り違えを防止するため、証明書の要求から証明書の作成にかけて、処理電文間で取り扱うデータを比較することにより正当性を保証する（エラー検知時は申請をリトライするよう促す）機能

✓　地方公共団体が、ベンダとの契約締結時に、契約不適合責任に関する民法の規律をふまえつつ、問題発生時に適切に権利を確保できる契約条項とするための検討を行うことができるようにするため、**民法上の要件を解説に記載してはいかがか**。
※　なお、契約上請求権が適切に確保されれば、問題発生時に訴訟に至らずとも、協議により解決する蓋然性も高まる。

＜契約不適合に基づく請求権が認められるための民法上の要件＞

請求権 （民法条文：売買関係/請負関係）	契約不適合があった場合に請求できる内容	請求手段が認められるための民法の要件
追完請求 （562Ⅰ,566/ 559,637）	買主（発注者）は、売主（請負者）に対し、**目的物の修補、代替物の引渡し又は不足分の引渡しによる履行の追完の請求が可能**。ただし、売主（請負者）は、買主（発注者）に不相当な負担を課するものでないときは、買主（発注者）が請求した方法と異なる方法による履行の追完が可能	① 種類・品質・数量の契約不適合 ② **①を知ってから1年以内に請求　※1**
代金減額請求 （563Ⅰ・Ⅱ,566/ 559,637）	買主（発注者）が相当の期間を定めて履行の追完の催告をし、その期間内に履行の追完がないとき又は追完されないことが明らかなとき等に、買主（発注者）は、**その不適合の程度に応じて代金の減額を請求する**ことが可能	① 種類・品質・数量の契約不適合 ② 追完されない（563Ⅰ）／追完されないことが明らか等（563Ⅱ） ③ **①を知ってから1年以内に請求　※1**
解　除 （564,541,542,566/ 559,637）	当事者の一方がその債務を履行しない場合において、相手方が相当の期間を定めてその履行の催告をし、**その期間内に履行がないとき又は追完されないことが明らかなとき等に、相手方は、契約の解除が可能**（軽微なものは除く）	① 種類・品質・数量の契約不適合 ② 履行催告（541）／履行されないことが明らか等（542） ③ **①を知ってから1年以内に請求　※1**
損害賠償請求 （564,415,566/ 559,637）	債務者がその債務の本旨に従った履行をしないとき又は**債務の履行が不能であるときは、債権者は、これによって生じた損害の賠償を請求する**ことが可能（契約その他の債務の発生原因及び取引上の**社会通念に照らして**債務者の責めに帰することができない事由によるものであるときは除く）	① 種類・品質・数量の契約不適合 ② 不履行が契約その他の債務の発生原因及び取引上の**社会通念に照らして債務者の責めに帰することができない事由に該当しない場合** ③ 損害発生　④ **①を知ってから1年以内に請求　※1**

※1　「～情報システム・モデル取引・契約書～（受託開発（一部企画を含む）、保守運用）＜第二版＞」（IPA・経産省。2020年12月）　では、（外部設計書についての契約不適合責任を負うのは）「確定後〇ヶ月／〇年以内【であって、かつ甲（ユーザ）が当該契約不適合を知った時から〇ヶ月以内】）」という権利行使期間を契約上規定するひな型が提案されている。

例：　システム開発・保守について、ベンダ（売主/請負者）の義務として個人情報漏えい防止のための技術的安全管理措置を講じることを民法上の請負契約の中で定めたにも関わらず、ベンダが当該措置を取らず、自治体（買主/発注者）が当該措置を取られていなかったこと（契約不適合）を知ったとき（具体的には、**自治体がシステムを調べた結果、本来取られるべき措置がとられていなかったことが判明**したとき）
→　自治体が、**1年以内に請求**を行い、契約不適合があったことを立証できれば**追完請求**を、追完されなければ**代金減額請求**を、履行されなければ**解除をすることが可能**となりうる。
→　**国の指針等（個人情報保護委員会の報告書など）でベンダが技術的安全管理措置をとるべきとされていれば**、措置が取られていないことについて**「社会通念に照らして債務者の責めに帰することができない事由によるものではない」という要件も原則として満たす**ため、自治体が併せて損害発生の立証ができれば、損害賠償請求を認められうる。

※2　上記の例は、システム開発・保守の請負契約の他、アプリケーションの売買契約を念頭に置いている。アジャイル開発を行う場合には「請負契約より…準委任契約の方が、その性質上…馴染み易い」という考え方が「 ～情報システム・モデル取引・契約書 ＜アジャイル開発版＞～ 」（2021年10月６日更新　IPA・経産省）p8で示されている。

ガイドライン改定の方向性①

✓　業務委託についての、契約項目に係る例文及び解説に、個人情報漏えい防止のための技術的安全管理措置に関する取り決めや、コンビニ交付事案の原因等について新たに規定。

現行ガイドラインにおける「業務委託」に関する規定

第３編　解説　第２章
8. 業務委託と外部サービスの利用
8.1．業務委託
（１）委託事業者の選定基準
（２）**契約項目**
（３）確認・措置等

✓ 業務委託を行う場合には、業務委託実施前の対策として、必要に応じて「提供されるサービスレベルの保証」を明記した契約を締結しなければならない、とされている。
✓ 個人情報保護法上の、**技術的安全管理措置に関する取り決めについては規定されていない**。

ガイドライン改定の方向性

- 「コンビニ交付サービスにおける住民票等誤交付事案に対する個人情報の保護に関する法律に基づく行政上の対応について」（令和５年９月20 日）の内容を踏まえ、**個人情報漏えい防止のための技術的安全管理措置に関する取り決めを契約書に明記**するよう、例文に追記し、**コンビニ交付サービスの事案の原因や個人情報保護委員会の指導内容について解説に追記する**。
- 上記に関連し、**契約不適合に関する民法における考え方について、解説に追記**する。

ガイドライン改定案（見え消し）①

現行：対策基準（例文）

8.1. 業務委託
(2)契約項目

重要な情報資産を取扱う業務を委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。
・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
・提供されるサービスレベルの保証
（略）

改定案：対策基準(例文)

8.1. 業務委託
(2) 業務委託実施前の対策

NISC統一基準の改定に伴うもの

業務委託実施前の対策
①情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、以下を全て含む事項を実施しなければならない。
（ア）委託する業務内容の特定
（イ）委託事業者の選定条件を含む仕様の策定
（ウ）仕様に基づく委託事業者の選定
（エ）情報セキュリティ要件を明記した契約の締結（契約項目）
重要な情報資産を取扱う業務を委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ等に係る要件を明記した契約を締結しなければならない。
・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
・個人情報漏えい防止のための技術的安全管理措置に関する取り決め
・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
・提供されるサービスレベルの保証
（略）

ガイドライン改定案（見え消し）②

現行：対策基準（解説）

8.1.業務委託
(2)契約項目

委託事業者に起因する情報漏えい等の事案を防ぐため、各団体で実施する場合と同様の対策を当該委託事業者に実施させるよう必要な要件を契約等に定める必要が
ある。以下に示す項目について、委託する業務の内容に応じて明確に要件を規定する
ことが必要である。
①（略）
②（略）
③提供されるサービスレベルの保証
通信の速度及び安定性、システムの信頼性の確保等の品質を維持するために、必要に応じて、サービスレベルを保証させる。

（略）

（注１０）業務の内容に応じて規定する要件の詳細については、「非機能要求グレード（地方公共団体版）利用ガイド」（平成26年3月　地方自治情報センター）を参照されたい。

コンビニ交付サービス等の証明書発行サーバにおける具体的な事例を入れる。

改定案：対策基準(解説)

（注９）業務の内容に応じて規定する要件の詳細については、「非機能要求グレード（地方公共団体版）利用ガイド」（平成26年3月　地方自治情報センター）を参照されたい。
（注１０）個人情報漏えい防止のための技術的安全管理措置に関する取り決めについては、以下の参考事例を踏まえ、検討を行うことが望ましい。

<参考：コンビニ交付サービス等における事例>
コンビニ交付サービス等の証明書発行サーバにおいて、誤ったプログラム処理が生じたことにより、別人の証明書が交付される事案が発生した。各地方公共団体において、発生した事態の内容及び件数の内訳は、下表のとおりである。

事態の内容	漏えい発生日（令和５年）	発生件数（本人数）
住民票（個人番号あり）の写しを別人に誤交付※１	３月 27 日	１件（１名）
住民票（個人番号なし）の写しを別人に誤交付※１	３月 27 日	５件（11 名）
住民票記載事項証明書を別人に誤交付※１	３月 27 日	２件（４名）
印鑑登録証明書を別人に誤交付※１	３月 27 日	２件（２名）
住民票（個人番号なし）の写しを別人に誤交付※１	３月 22 日	１件（３名）
印鑑登録証明書を別人に誤交付	４月 18 日	１件（１名）
戸籍証明書を別人に誤交付	５月２日	１件（１名）
戸籍証明書を別人に誤交付※１	３月 27 日	１件（１名）
住民票（個人番号なし）の写しを別人に誤交付	６月 28 日	１件（１名）

※１　発生当時、地方公共団体の個人情報の取扱いには、個人情報保護法の規律が適用されない[2]。

[2] 個人情報保護法の改正（令和５年４月１日に施行）により、その適用範囲が拡大し、地方公共団体における個人情報の取扱いについても、個人情報保護法の規律が適用されることとなった。

いずれの事案においても、委託事業者が開発したプログラムの不具合に起因し、そのプログラムを用いて証明書の交付事務を行っていた地方公共団体において、保有個人情報の漏えいが発生したものである。

ガイドライン改定案（見え消し）②続き

現行：対策基準（解説）

改定案：対策基準(解説)

各不具合の原因詳細は様々であるが、共通して、エラーが生じた際の処理において、想定不足及び不要な処理の混入により、前後の申請者の証明書を取り違えて印刷を行うという不具合が生じており、当該不具合を開発及びテスト工程では検出できず、運用途中に改修されることはなく、本件各誤交付に至っている。
本事例における技術的安全管理措置として、以下の対応が実施されている。
・類似の誤交付トラブルの点検及び異常検出機能の開発
※参考文書１
『個人情報保護委員会　コンビニ交付サービスにおける住民票等誤交付事案に対する個人情報の保護に関する法律に基づく行政上の対応について（令和５年９月20日）』
https://www.ppc.go.jp/files/pdf/230920_01_houdou.pdf
※参考文書２
『マイナンバーカード等に係る各種事案に対する 個人情報保護委員会の対応について（令和５年12月６日）』
https://www.ppc.go.jp/files/pdf/231206_houdou.pdf

ガイドライン改定案（見え消し）③

現行：対策基準（解説）

8.1. 業務委託
(1) 委託事業者の選定基準
(2) 契約項目
(3) 確認・措置等

（略）

8.1.業務委託の解説部分の最後に、契約不適合に関する民法の考え方についての解説を入れる。

改定案：対策基準(解説)

8.1. 業務委託

NISC統一基準の改定に伴うもの

(1) 業務委託に係る規定の整備
(2) 業務委託実施前の対策
(3) 業務委託実施期間中の対策
(4) 業務委託終了時の対策
①業務委託の終了時に実施すべき対策
（ア）（略）
（イ）「情報が確実に返却、廃棄又は抹消されたことの確認」について、委託事業者ともあらかじめ具体的な確認手段を定め、合意しておくことが望ましい。情報が完全に廃棄又は抹消されたことを確認することが困難な場合は、確認書を委託事業者に提出させるなどの方法も考慮する必要がある。

＜参考：契約不適合に基づく請求権が認められるための民法上の要件＞

請求手段 （民法条文：売買関係/請負関係）	契約不適合があった場合に請求できる内容	請求手段が認められるための民法の要件
追完請求 （562Ⅰ,566/559,637）	買主（発注者）は、売主（請負者）に対し、目的物の修補、代替物の引渡し又は不足分の引渡しによる履行の追完の請求が可能。ただし、売主（請負者）は、買主（発注者）に不相当な負担を課するものでないときは、買主（発注者）が請求した方法と異なる方法による履行の追完が可能	①　種類・品質・数量の契約不適合 ②　①を知ってから1年以内に請求 ※
代金減額請求 （563Ⅰ・Ⅱ,566/559,637）	買主（発注者）が相当の期間を定めて履行の追完の催告をし、その期間内に履行の追完がないとき又は追完されないことが明らかなとき等に、買主（発注者）は、その不適合の程度に応じて代金の減額を請求することが可能	①　種類・品質・数量の契約不適合 ②　追完されない（563Ⅰ）／追完されないことが明らか等（563Ⅱ） ③　①を知ってから1年以内に請求 ※
解　除 （564,541,542,566/559,637）	当事者の一方がその債務を履行しない場合において、相手方が相当の期間を定めてその履行の催告をし、その期間内に履行がないとき又は追完されないことが明らかなとき等に、相手方は、契約の解除が可能（軽微なものは除く）	①　種類・品質・数量の契約不適合 ②　履行催告（541）／履行されないことが明らか等（542） ③　①を知ってから1年以内に請求 ※
損害賠償請求 （564,415,566/559,637）	債務者がその債務の本旨に従った履行をしないとき又は債務の履行が不能であるときは、債権者は、これによって生じた損害の賠償を請求することが可能（契約その他の債務の発生原因及び取引上の社会通念に照らして債務者の責めに帰することができない事由によるものであるときは除く）	①　種類・品質・数量の契約不適合 ②　不履行が契約その他の債務の発生原因及び取引上の社会通念に照らして債務者の責めに帰することができない事由に該当しない場合 ③　損害発生 ④　①を知ってから1年以内に請求 ※

※　「～情報システム・モデル取引・契約書～（受託開発（一部企画を含む）、保守運用）＜第二版＞」（2020年12月 IPA・経産省）では、（外部設計書についての契約不適合責任を負うのは）「確定後○ヶ月／○年以内【であって、かつ甲（ユーザ）が当該契約不適合を知った時から○ヶ月以内】）」という権利行使期間を契約上規定するひな型が提案されている。

ガイドライン改定案（見え消し）③続き

現行：対策基準（解説）	改定案：対策基準(解説)
	例として、以下のようなケースが考えられる。 ＜例＞ システム開発・保守について、ベンダ（売主/請負者）の義務として個人情報漏えい防止のための技術的安全管理措置を講じることを民法上の請負契約の中で定めたにも関わらず、ベンダが当該措置を取らず、自治体（買主/発注者）が当該措置を取られていなかったこと（契約不適合）を知ったとき（具体的には、自治体がシステムを調べた結果、本来取られるべき措置がとられていなかったことが判明したとき） →　地方公共団体が、1年以内に請求を行い、契約不適合があったことを立証できれば追完請求を、追完されなければ代金減額請求を、履行されなければ解除をすることが可能となりうる。 →　国の指針等（個人情報保護委員会の報告書など）でベンダが技術的安全管理措置をとるべきとされていれば、措置が取られていないことについて「社会通念に照らして債務者の責めに帰することができない事由によるものではない」という要件も原則として満たすため、自治体が併せて損害発生の立証ができれば、損害賠償請求を認められうる。 上記の例は、システム開発・保守の請負契約の他、アプリケーションの売買契約を念頭に置いている。ジャイル開発を行う場合には「請負契約より…準委任契約の方が、その性質上…馴染み易い」という考え方が「～情報システム・モデル取引・契約書＜アジャイル開発版＞～」（2021年10月６日更新　IPA・経産省）p8で示されている。 なお、契約上請求権が適切に確保されれば、問題発生時に訴訟に至らずとも、協議により解決する蓋然性も高まる。

ガイドライン改定の方向性②

✓ 技術的セキュリティに関する解説に、不具合の考慮やテスト計画の策定・実施や、セキュリティ機能に関する判断のための情報の開示を、事業者に求められるような方策を追記する。

現行ガイドラインにおける「技術的セキュリティ」に関する規定

第３編　解説　第２章

6. 技術的セキュリティ

6.3.　システム開発、導入、保守等業務委託

【趣旨】
システム開発、導入、保守等において、技術的なセキュリティ対策が十分に実施されていない場合は、プログラム上の欠陥（バグ）によるシステム障害等により業務に重大な支障が生じるおそれがある。

（１）情報システムの調達
（２）情報システムの開発
（３）情報システムの導入
（４）システム開発・保守に関連する資料等の整備・保管
（５）情報システムにおける入出力データの正確性の確保

②情報システム管理者は、故意又は**過失により情報が改ざんされる又は漏えいするおそれがある場合**に、**これを検出するチェック機能を組み込むように情報システムを設計しなければならない**。

③情報システム管理者は、**情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない**。

ガイドライン改定の方向性

- 地方公共団体は、**システム調達、開発、導入、保守等業務委託全般**において、**業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載する**ことに加え、委託先の監督を適切に行い、当該機能を**確実に検証するテスト計画の策定・実施を行う必要がある**ことを、**例文に追記**する。

- また、**適切なセキュリティ機能及びテスト仕様をどのように実現するかの判断に資する情報を、事業者から適時に得られるような方策**を、地方公共団体が講ずることができるようにするため、以下について解説に追記する。
  - RFI（調達前の情報収集）やRFP（提案要請）の段階でセキュリティに関する対応状況について開示を求め、委託事業者選定の際の参考にする。
  - 開発、運用・保守の各工程における、機密性の高い情報の漏えいを防止する観点で、安全管理措置に係る対応状況について、委託先に定期的に報告を求めるような契約を締結する。

ガイドライン改定案（見え消し）④

現行：対策基準（例文）

6.3.システム開発、導入、保守等

（１） 機器等及び情報システムの調達
①統括情報セキュリティ責任者及び情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。

（２）（略）
（３） 情報システムの導入
① （略）
② テスト
（ア）情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。
（イ）情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。
（ウ）情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。
（エ）情報システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

改定案：対策基準(例文)

6.3.システム開発、導入、保守等

（１）（略）
（２） 機器等及び情報システムの調達
①統括情報セキュリティ責任者及び情報システム管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記しなければならない。また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載しなければならない。

NISC統一基準の改定に伴うもの

（４）情報システムの導入
① （略）
② テスト
（ア）情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。
（イ）情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。
（ウ）情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。
（エ）情報システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。
（オ）情報システム管理者は、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮したテスト計画を策定し、確実に検証が実施されるよう、必要かつ適切に委託事業者の監督を行わなければならない。

ガイドライン改定案（見え消し）⑤

現行：対策基準（解説）

6.3.システム開発、導入、保守等

【趣旨】
システム開発、導入、保守等において、技術的なセキュリティ対策が十分に実施されていない場合は、プログラム上の欠陥（バグ）によるシステム障害等により業務に重大な支障が生じるおそれがある。このことから、システム開発、導入、保守のそれぞれの段階における対策を規定する。なお、本規定にはシステムの更新又は統合時の十分な検証等も含まれる。

改定案：対策基準(解説)

6.3.システム開発、導入、保守等

【趣旨】
システム開発、導入、保守等において、技術的なセキュリティ対策が十分に実施されていない場合は、プログラム上の欠陥（バグ）によるシステム障害等により業務に重大な支障が生じるおそれがある。このことから、システム開発、導入、保守のそれぞれの段階における対策を規定する。なお、本規定にはシステムの更新又は統合時の十分な検証等も含まれる。
また、地方公共団体が適切に技術的なセキュリティ機能やテスト仕様等を検討できるよう、委託事業者に対して、判断に資する情報を適時開示するよう求めることが必要である。具体的には以下が考えられる。
・RFI（調達前の情報収集）やRFP（提案要請）の段階でセキュリティに関する対応状況について開示を求め、委託事業者選定の際の参考にする。
・開発、運用・保守の各工程における、機密性の高い情報の漏えいを防止する観点で、安全管理措置に係る対応状況について、委託先に定期的に報告を求めるような契約を締結する。

マイナンバー利用事務系と他の領域との画面転送要件の検討

前回いただいたご意見

✓　リスクアセスメントで安全性を確認し、慎重に検討を進めるべきとの意見や、どこまでの対策が必要なのかを明記すべきとの意見をいただいた。

✓　当初の方針のとおり、**2年間の期間を設けてリスクアセスメントを実施**し、実施可否を含め慎重に検討する。

検討項目	発言要旨
画面転送	• マイナンバー利用事務系の画面転送は、**リスクアセスメントを実施し安全性を確認した上で対応しないと問題があり**、何か起こった時の影響が大きいと考える。リスクアセスメントを実施することを前提に、**少し時間を掛けてもよいので安全性を確認してからやるべきである**。 • マイナンバー利用事務系と接続が可能なインターネット系サービスについては、ガイドライン上でeLTAXかマイナポータルが限定と挙がっているが、限定的にするか、**どこまで対策を講じていれば可能であるかを明記**すると良いのではないか。

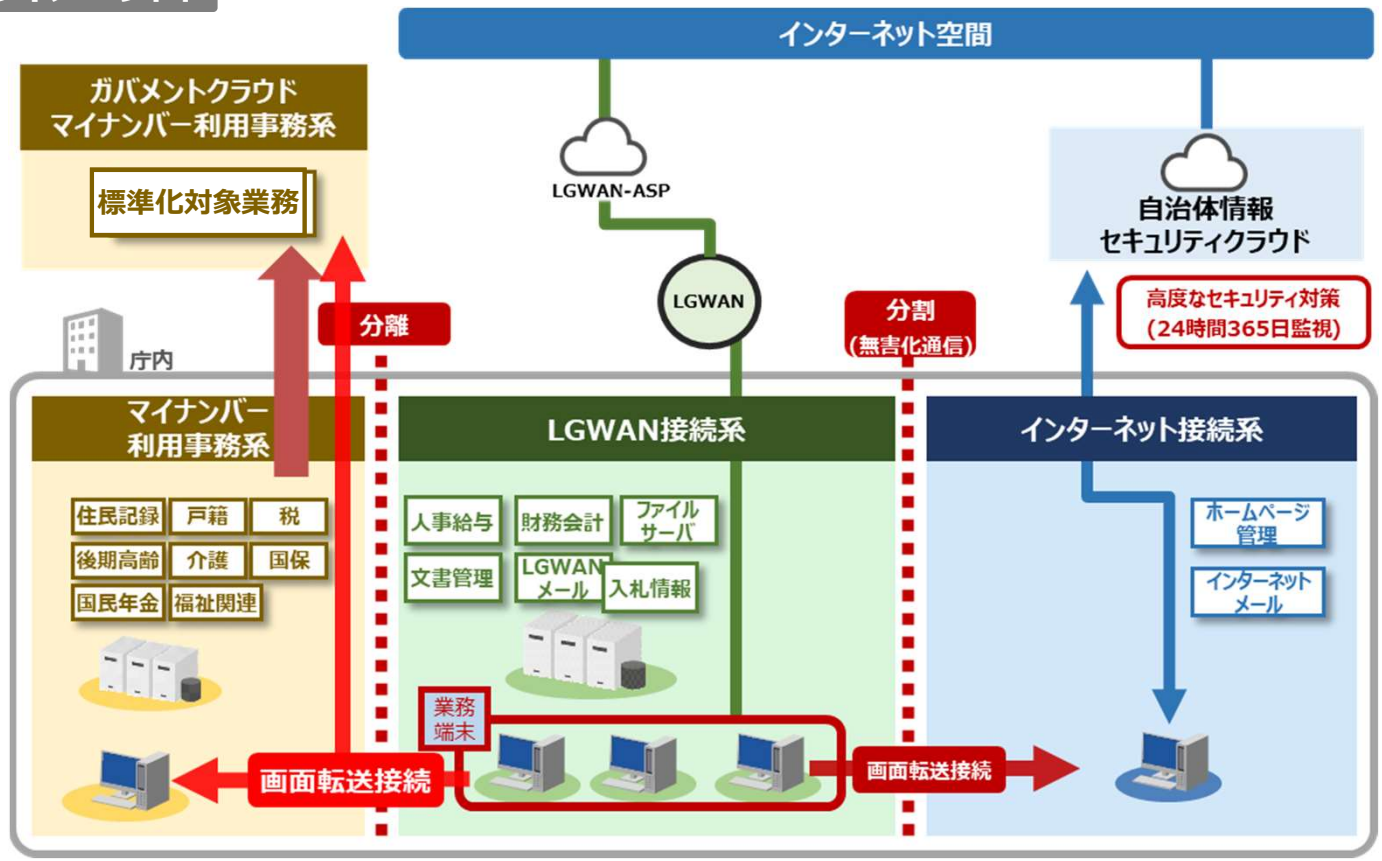
画面転送のイメージ

✓ 複数の団体から、利便性向上の観点でマイナンバー利用事務系と他の領域との画面転送実施の要望がある。
✓ 三層分離の根本的な見直しにつながりうるため、慎重な検討が必要となる。

✓ **２年間かけて検討**することとし、**１年目（今年度）は、次年度に評価を実施する上で、リスク評価の手法（どのようなケースを想定すべきか等）について検討する**こととしてはいかがか。
✓ ２年目にリスク評価及び評価結果を踏まえ、必要なセキュリティ対策を記載することとしてはいかがか。

αモデルのイメージ図

※ マイナンバー利用事務系の業務システムがガバメントクラウドにリフトされる点を考慮する必要がある。
※ ネットワークモデル（α、β、β´）によって、画面データ転送先のセグメントが異なる。右図はαモデルの場合となる。



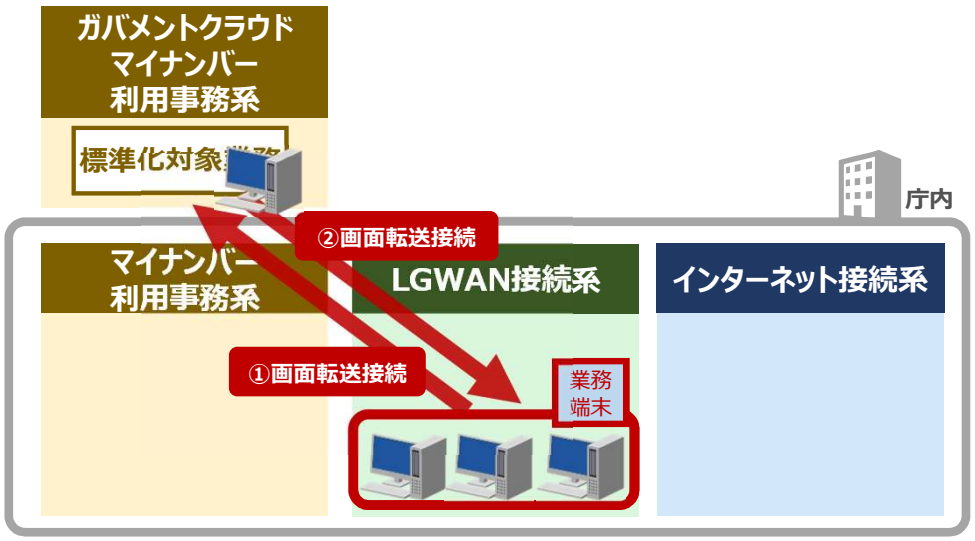
画面転送の方式の検討に必要な観点

✓ マイナンバー利用事務系と他セグメント間の通信について、画面転送を新たに**特定通信**（マイナンバー利用事務系からインターネットに接続する場合に**最低限必要な、接続先特定のための通信**）の方式で実施した場合のセキュリティリスクを評価し、実施可否および実施する場合の接続要件やセキュリティ対策基準を明確にする。

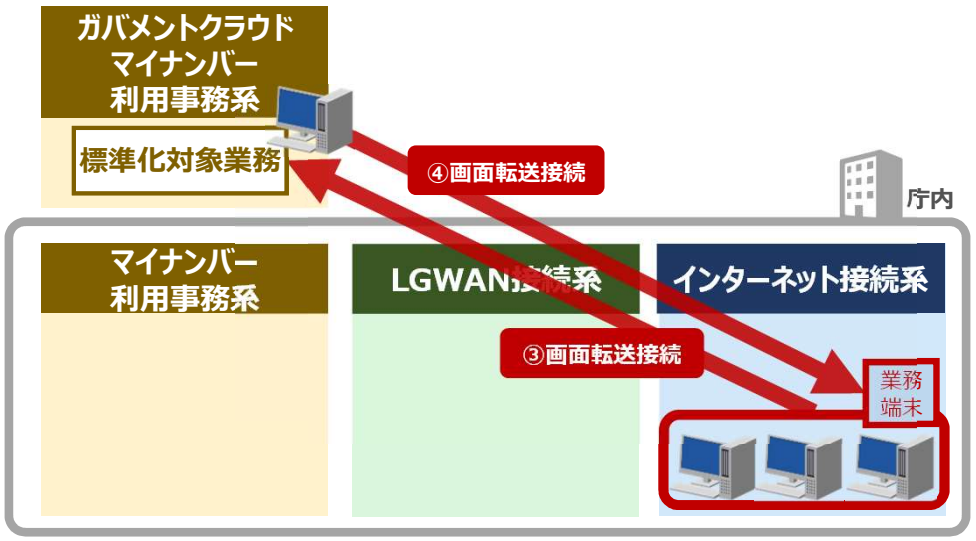
観点１：ネットワークモデルと接続先のセグメント

✓ 以下の４つのパターンについて、セキュリティリスクを分析する。
- ①α/α´モデルの団体が、マイナンバー利用事務系に画面転送接続する場合
- ②α/α´モデルの団体が、LGWAN接続系に画面転送接続する場合
- ③β/β´モデルの団体が、マイナンバー利用事務系に画面転送接続する場合
- ④β/β´モデルの団体が、インターネット接続系に画面転送接続する場合

α/α´モデルの接続構成



β/β´モデルの接続構成



※インターネット接続系の端末にマイナンバー利用事務系の画面転送を実施する事例がある

画面転送の方式の検討に必要な観点

観点２：接続要件

- ✓ 画面転送で使用される通信に関し、特定通信＊（マイナンバー利用事務系からインターネットに接続する場合に**最低限必要な、接続先特定のための通信**）を実施した場合のセキュリティリスクを分析する
- ✓ 特にパブリッククラウドサービスとして、画面転送を利用する場合は、閉域を担保する構成とする等、画面転送の通信が発生するセグメントのネットワークを踏まえた接続要件を検討する。

(*)通信経路の限定（MACアドレス、IPアドレス）に加えて、アプリケーションプロトコル（ポート番号）のレベルでの限定等を行う。

観点３：端末仮想化の方式

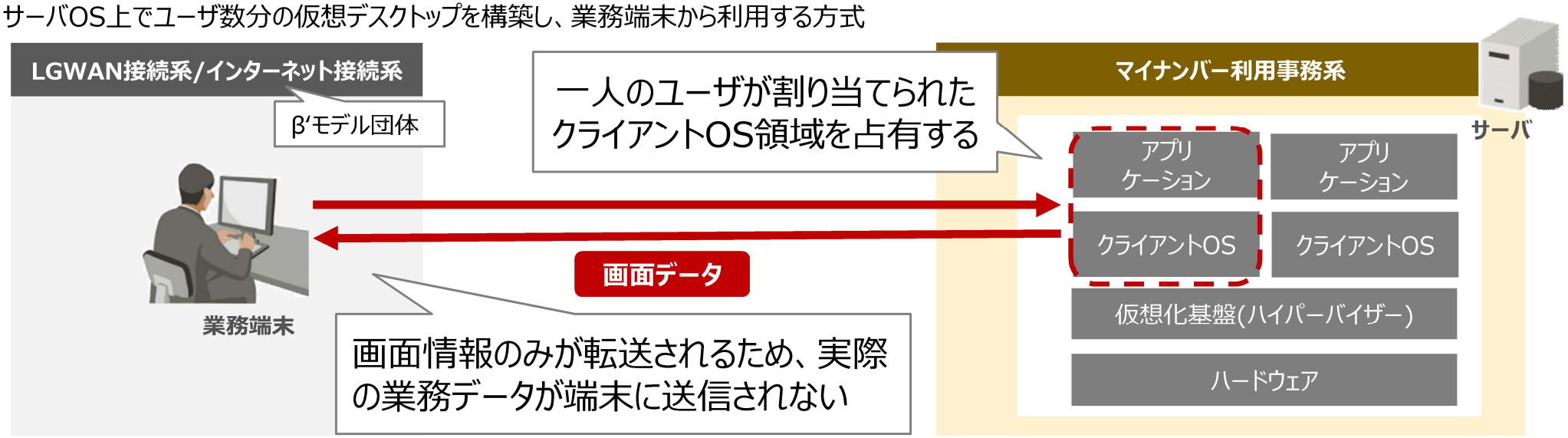
- ✓ 画面転送で利用が想定されるされる端末仮想化の各方式について、セキュリティリスクを分析する

方式	概要
VDI （Virtual Desktop Infrastructure）	サーバOS上でユーザ数分の仮想デスクトップを構築し、業務端末から利用する
SBC （Server Based Computing）	サーバOS上でマルチユーザーに対応した仮想環境を構築し、複数台の端末で共有する
セキュアブラウザ	サーバOSをセッション単位で仮想化
	接続端末上で分離された領域を確保し、その領域内でWeb上のドキュメントやデータを表示することで、セキュアにWeb閲覧を行う

（ご参考）端末仮想化の方式の例

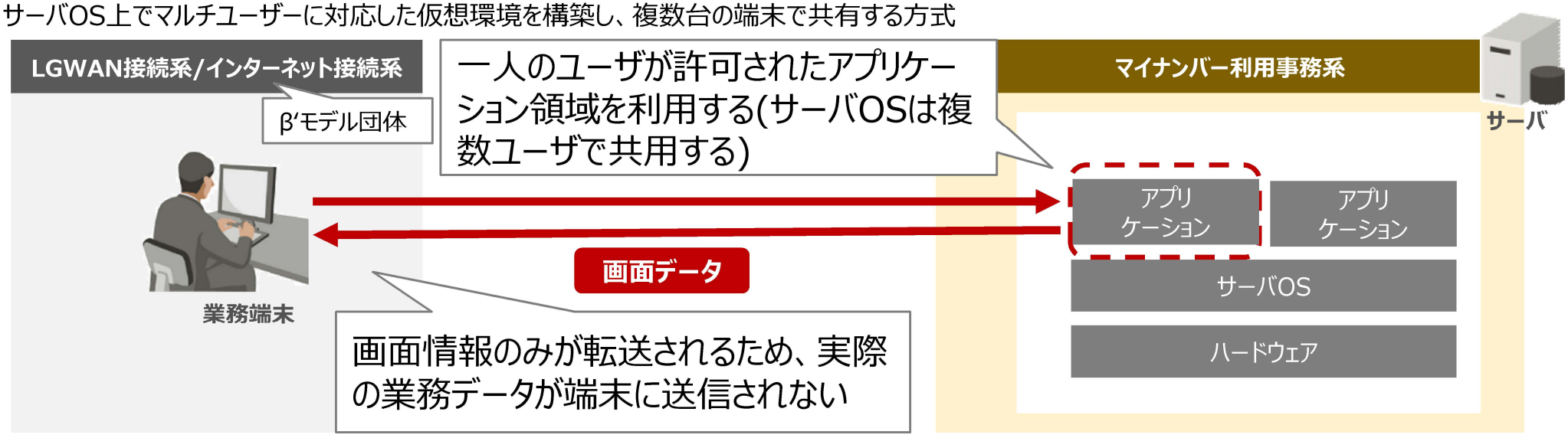
VDI（Virtual Desktop Infrastructure）方式

・サーバOS上でユーザ数分の仮想デスクトップを構築し、業務端末から利用する方式



SBC（Server Based Computing）方式

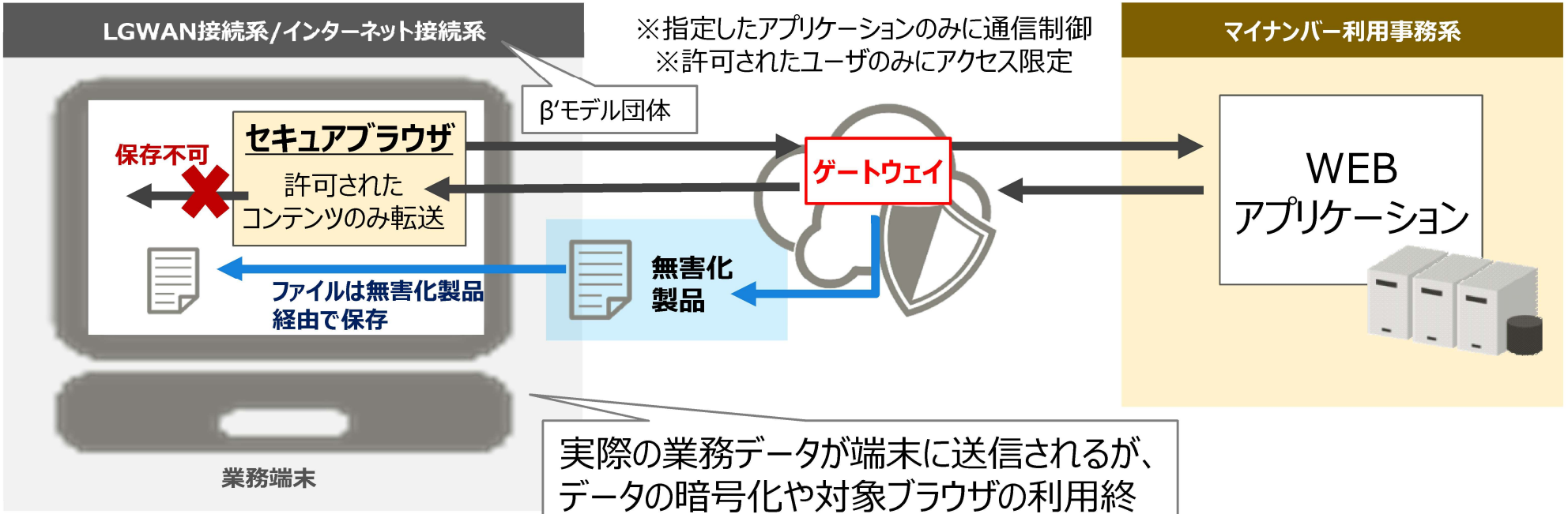
・サーバOS上でマルチユーザーに対応した仮想環境を構築し、複数台の端末で共有する方式



（ご参考）端末仮想化の方式の例

セキュアブラウザ方式

・接続端末上で分離された領域を確保し、その領域内でWeb上のドキュメントやデータを表示することで、セキュアにWeb閲覧を行う方式

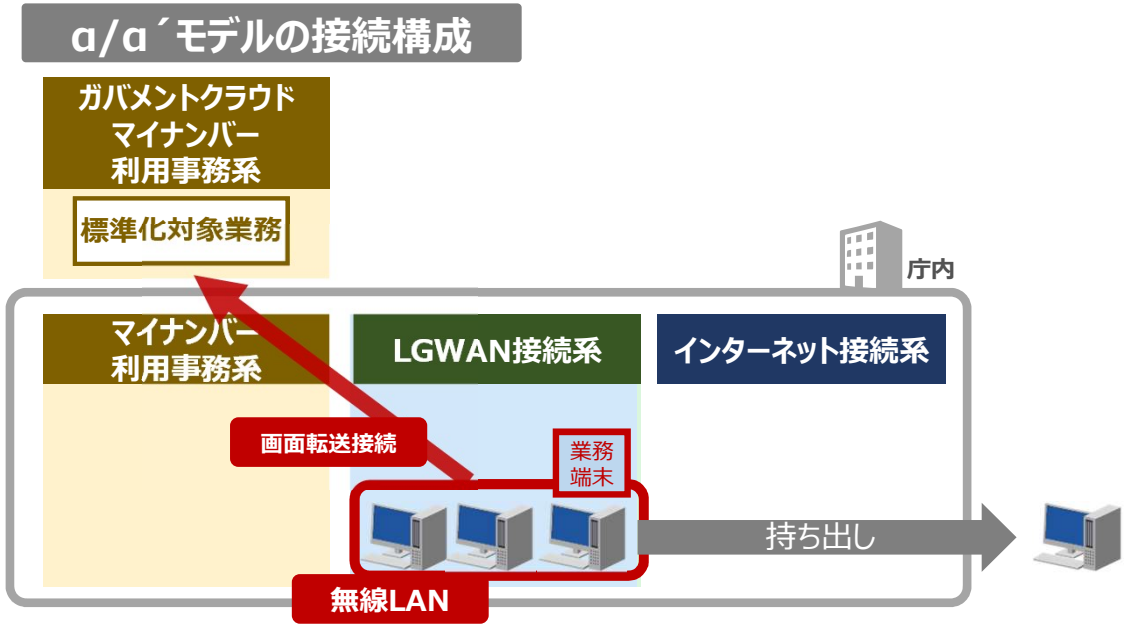


実際の業務データが端末に送信されるが、データの暗号化や対象ブラウザの利用終了時に領域データを削除するなどでセキュリティを担保

画面転送の方式の検討に必要な観点

観点４：業務運用

- ✓ マイナンバー利用事務系の画面転送を実施する業務端末が無線LAN化されていた場合、持ち運び可能な端末でマイナンバー関連事務が実施できる状態となる。本来、マイナンバー利用事務系の端末は無線LANが認められていないため、当該構成について、運用状況を想定したリスク分析を行う必要がある。
- ✓ **<u>個人情報保護法や番号法上問題がないように</u>**対策を検討する必要がある。



令和５年度のガイドライン改定の進め方について（イメージ）

- ✓ 以下のようなスケジュールで、検討会や地方公共団体への意見照会等を行い、ガイドライン改定を実施。
- ✓ 統一基準の改定対応は、NISCと共同で１月に自治体向け説明会を実施し、その後自治体を対象に意見照会を行う予定。