資料２

検討項目①
電磁的記録媒体を使用しないデータ連携について

総 務 省

令和７年　６月２３日

総務省自治行政局住民制度課

サイバーセキュリティ対策室

USBメモリの紛失による主な個人情報漏洩事案

- 近年、USBメモリの紛失による個人情報の漏洩事案が複数発生。
- 特に令和４年度のA市の事案は、**全住民の住民基本台帳の情報が漏洩**したものであり、報道でも大きく取り上げられた。
- したがって、**電磁的記録媒体を使用しないデータ連携の検討は、情報漏洩を防止する観点で非常に意味がある**。

◆ A市の事案（令和４年度）

○概要

住民税非課税世帯等に対する臨時特別給付金の支給事務の受託者の、再々委託先の従業員が、個人情報を含むUSBメモリを紛失。

【流出した個人情報】

・全市民の住民基本台帳の情報（46万517人分）
・住民税に係る税情報（36万573件）
・非課税世帯等臨時特別給付金の対象世帯情報（R3年度分　7万4,767世帯分、R4年度分　7,949世帯分）
・生活保護受給世帯と児童手当受給世帯の口座情報（生保　1万6,765件、児手　6万9,261件）

◆ B町の事案（令和５年度）

○概要

職員が、個人情報を含むUSBメモリを紛失。

【流出した個人情報】

・新型コロナワクチン接種済者等約1万3,400人分（転出、死亡者含む。）　の住所、氏名、生年月日、性別、接種履歴等

◆ C町の事案（令和５年度）

○概要

職員が、個人情報を含むUSBメモリを紛失。

【流出した個人情報】

・個人情報を含むデータ（4,138名、4,740 件の口座情報、口座振替額）

現行のガイドラインにおけるUSBメモリに係る規定

■　ガイドラインでは、ネットワークが分離されていることを踏まえ、**マイナンバー利用事務系に係る電磁的記録媒体（USBメモリ等）の使用について明示的に規定**している。

３．情報システム全体の強靭性の向上
【例文】
（１）マイナンバー利用事務系
②情報のアクセスおよび持ち出しにおける対策
（イ）情報の持ち出し不可設定
原則として、**USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない**。

【解説】
（イ）情報の持ち出し不可設定
納付書など**大量帳票のアウトソーシングや指定金融機関に対する口座振替情報の提供等の電磁的記録媒体の利用が止むを得ない場合**においては、管理者権限を持つ職員によってその都度限定を解除する又は管理者権限を持つ職員のみに許可する設定とすることを例外として取り扱わなければならない。
USB メモリ等の電磁的記録媒体による端末からの情報持ち出しを行う場合は、次の手段により実施しなければならない。
（略）

まずは、電磁的記録媒体の利用を含めマイナンバー利用事務系におけるデータの受け渡しをどのようにガイドラインで規定しているかについて次頁以降で整理する。

ガイドラインの規定①

■　マイナンバー利用事務系から、**LGWAN接続系やインターネット接続系とのデータの受け渡しが発生する場合**（「**パターン①**」とする）については、以下の２つをガイドラインで規定。

- 指定金融機関からの外部データを、LGWAN-ASPにより受信し、マイナンバー利用事務系に取り込む場合
- 委託事業者等へ、インターネットを利用したクラウドサービスで重要な情報資産を運搬する場合

パターン①

第３編　３．情報システム全体の強靭性の向上
【解説】
（１）①マイナンバー利用事務系と他の領域との分離
（注３）**指定金融機関から税などの口座引落済みデータ（消し込みデータ）等の外部データを受信**し、**マイナンバー利用事務系へ取り込みを行う場合**は、**LGWAN-ASP等を利用して受信**しなければならない。マルウェア感染しているファイルをマイナンバー利用事務系に取り込んでしまうことを防止するため、以下の手順で取り込むことが考えられる。

- 予め指定された職員等が、他の職員等の立ち合い又は操作が監視カメラで記録される管理区画等において、LGWAN接続系端末でウイルスチェックを実施
- 他の用途で使用されることのない専用の電磁的記録媒体に保存
- システム管理責任者による電磁的記録媒体接続禁止の一時的解除
- マイナンバー利用事務系端末でウイルスチェックを実施後に取り込む

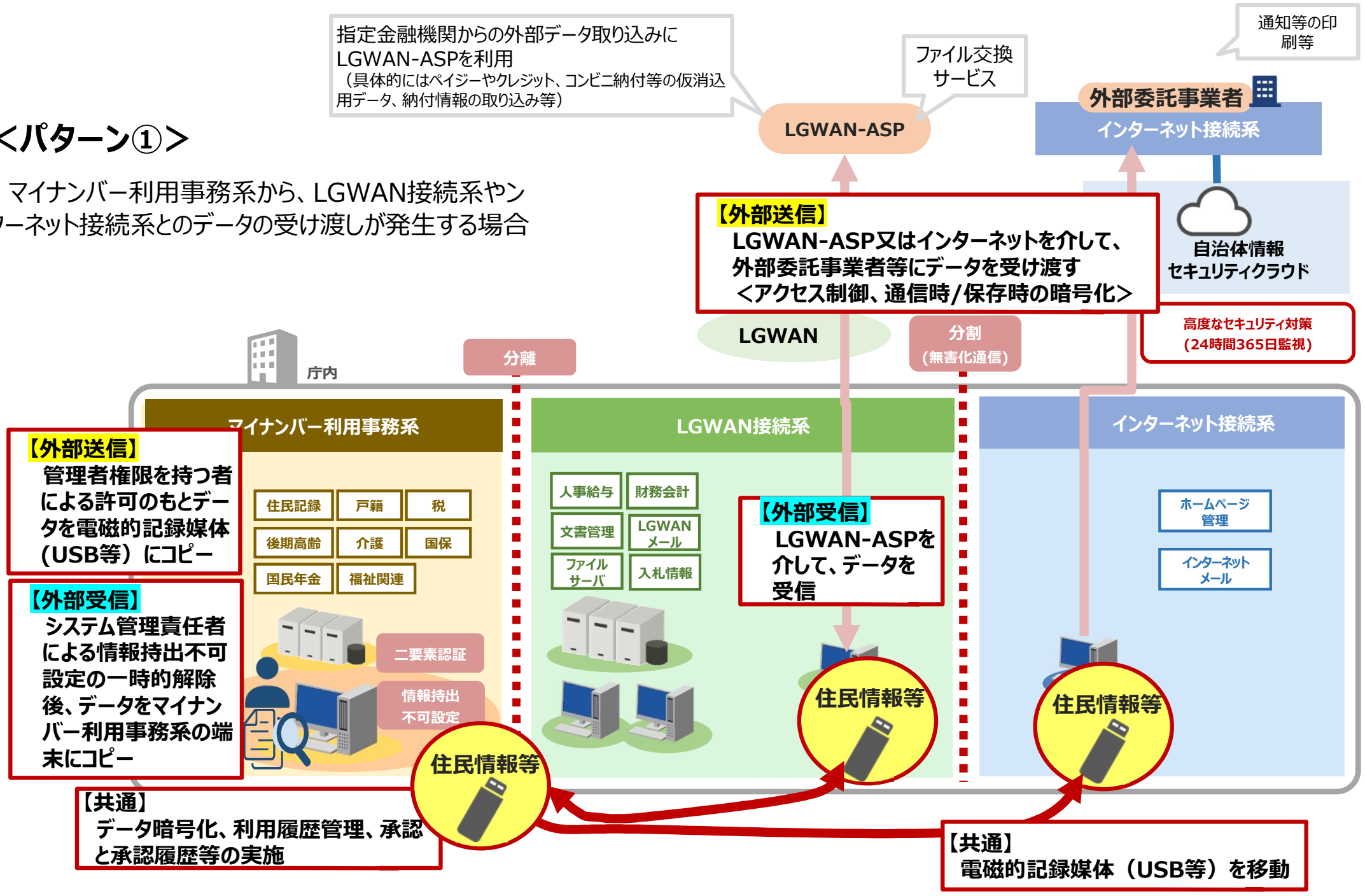
マイナンバー利用事務系とは明記されていないが、過去に、臨時特別給付金支給事務の委託事業者が、全住民の住民基本台帳の情報が保存されたUSBを紛失した事案を踏まえ、規定した内容であり、**マイナンバー利用事務系に係るデータのやりとりの方式として規定**。

第３編　２．情報資産の分類と管理（Ｐiii -33・34）
【解説】
（２）③情報の作成～⑩情報資産の廃棄
（注８）（略）**インターネットを利用したクラウドサービス等で委託事業者等へ重要な情報資産を運搬する場合**は、**アクセス制御等のシステム設定が適切にされている**か、重要な情報資産を**暗号化して保存**しているか、インターネットを利用した**クラウドサービスと接続する通信が暗号化**されているか等を確認する必要がある。また、委託事業者等に重要な情報資産が運搬された後の情報の管理を徹底することも重要となる。

データの受け渡しのイメージ図①（aモデルの場合）

＜パターン①＞

マイナンバー利用事務系から、LGWAN接続系やインターネット接続系とのデータの受け渡しが発生する場合



ガイドラインの記載②

■　マイナンバー利用事務系から直接外部とデータをやりとりする場合（「パターン②」とする）については、専用回線の設置、専用端末の管理区域内の設置等を求めた上で、電磁的記録媒体の使用を必須としている。

パターン②

第３編　３．情報システム全体の強靭性の向上（Ｐiii -40）

【解説】

（１）①マイナンバー利用事務系と他の領域との分離

（注１）現在、国等の公的機関が構築したインターネットに接続されたシステム等で十分に安全性が確保された外部接続先との通信としてeLTAX、マイナポータル、自治体情報セキュリティ向上プラットフォームが考えられる。（略）

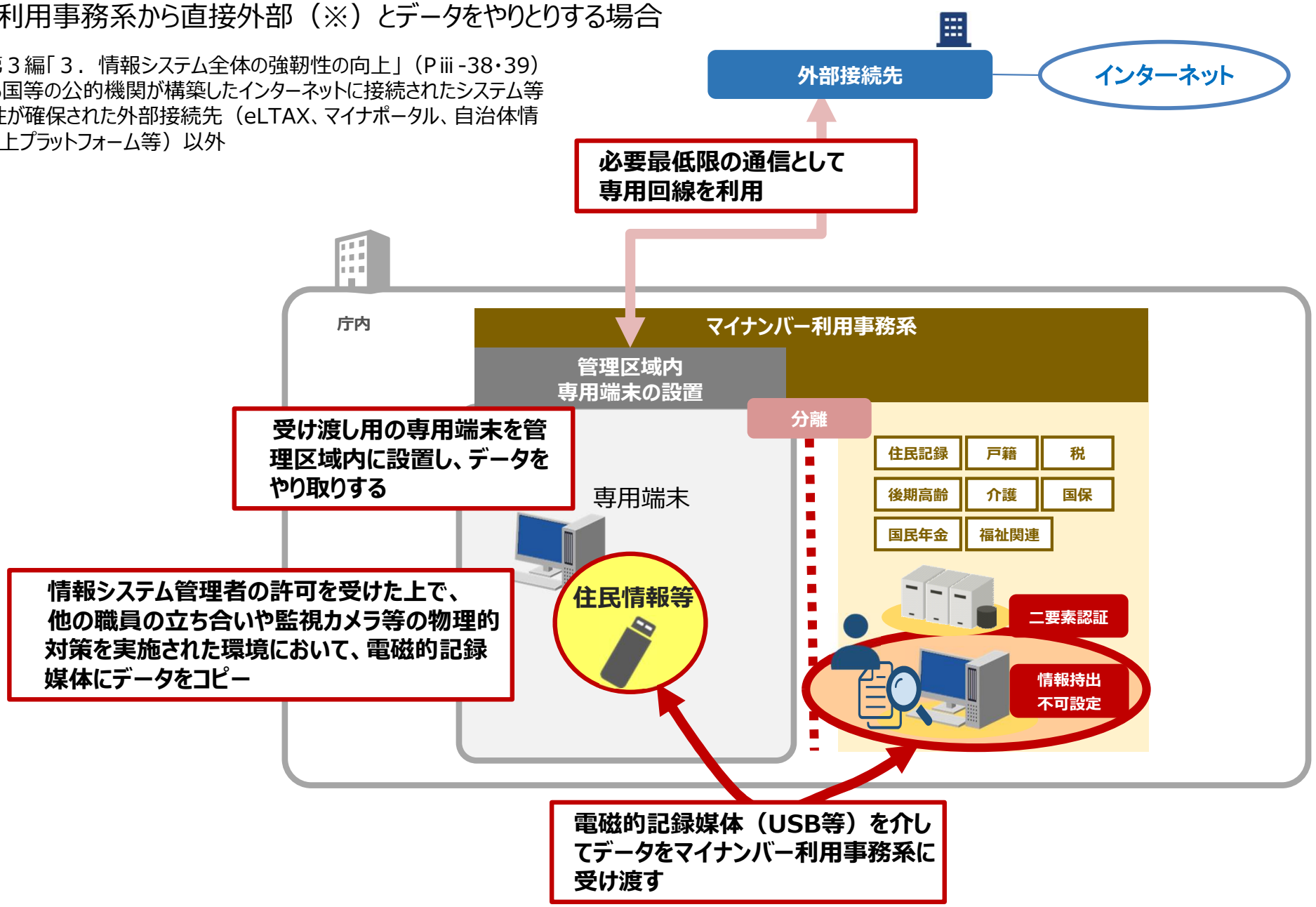
（注２）**（注１）の接続先以外の外部接続先については**、止むを得ず**インターネットとデータをやり取りする場合**は、**専用回線を新たに設置**し、必要最小限の通信とし、外部のネットワークと通信する**専用の端末を管理区域内に設置**した上で、**電磁的記録媒体を経由したデータのやり取りを行わなければならない**。その際には情報システム管理者の許可を受けた上で、電磁的記録媒体の接続禁止設定を一時的に解除し、他の職員の立ち合い又は監視カメラで撮影された状態で、管理区域内において作業を行うなどの取扱いを行わなければならない。　（略）

データの受け渡しのイメージ図②

＜パターン②＞

マイナンバー利用事務系から直接外部（※）とデータをやりとりする場合

※　ガイドライン第３編「３．情報システム全体の強靭性の向上」（Ｐiii -38・39）（注１）にある国等の公的機関が構築したインターネットに接続されたシステム等で十分に安全性が確保された外部接続先（eLTAX、マイナポータル、自治体情報セキュリティ向上プラットフォーム等）以外



ガイドラインの記載③

■　マイナンバー利用事務系のデータを、電磁記録媒体の形で外部の委託事業者に運搬する場合（「パターン③」とする）については、機密情報を運搬する専用のサービスを利用し、安全な運搬措置を行うことを必須としている。

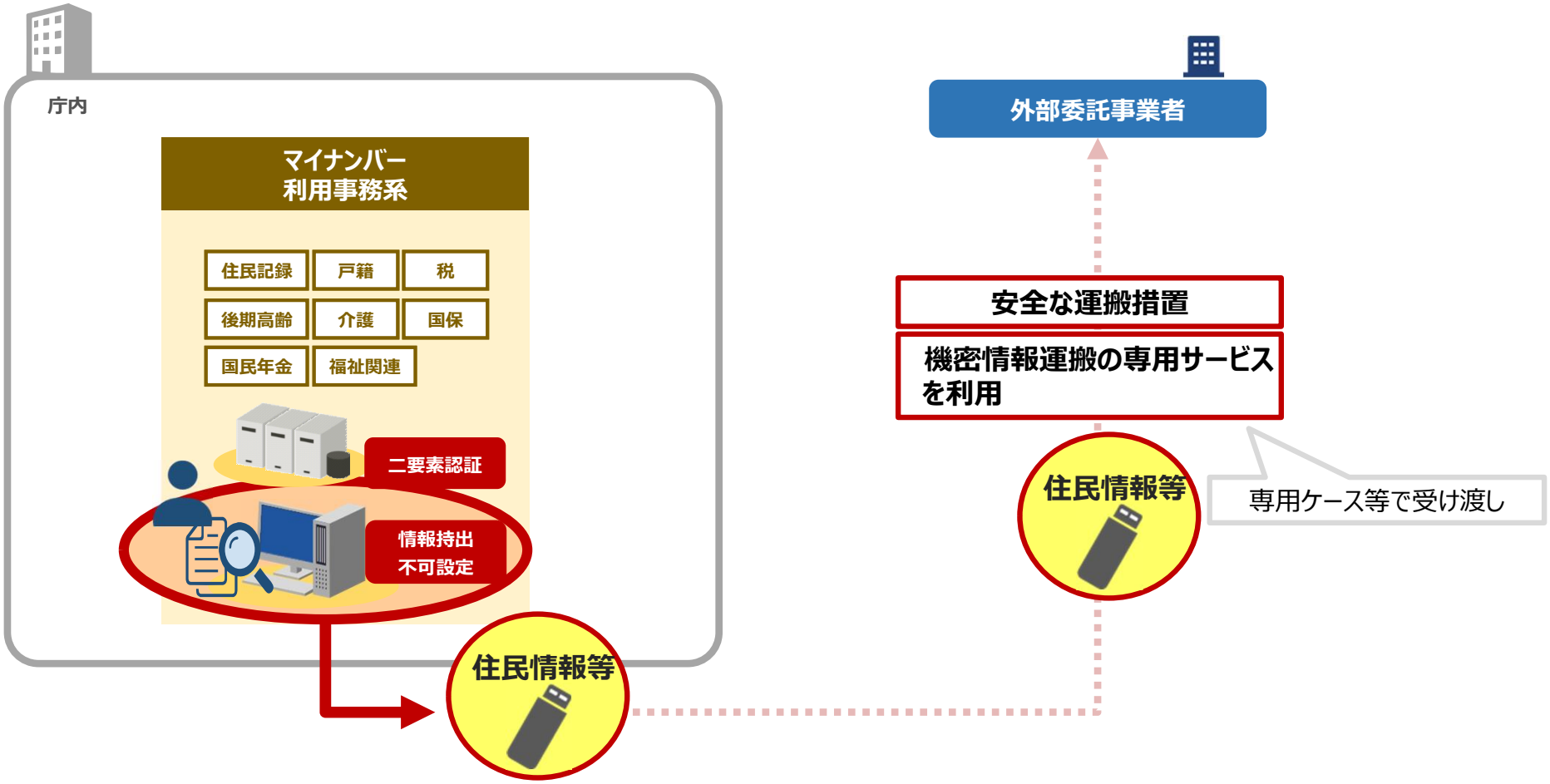
パターン③

第３編　2. 情報資産の分類と管理（Ｐiii -33）
【解説】
（２）③情報の作成～⑩情報資産の廃棄
（注８）委託事業者等の**外部へ重要な情報資産を電磁的記録媒体で運搬する場合**は、機密情報を運搬する**専用のサービスを利用**するなど**安全な運搬措置を行う**こと。（略）

データの受け渡しのイメージ図③（aモデルの場合）

＜パターン③＞

マイナンバー利用事務系のデータを、電磁記録媒体の形で外部の委託事業者に運搬する場合



今後の進め方

■ 現行のガイドラインでは、パターン①②③のような形でのデータのやりとりを規定。

■ パターン①は、主たるデータのやりとりが**「マイナンバー利用事務系と庁内の他の領域とのデータのやりとり」**であり、パターン②③は、**「マイナンバー利用事務系と外部との直接のデータのやりとり」**となる。

■ ただし、**地方公共団体の実務の効率的な運用のため止むを得ず、総務省のガイドラインに示したパターン①②③以外の方法で、データの受け渡しを行っている可能性がある**。

■ そこで、以下のように地方公共団体の業務の実情に沿った検討を行うこととしてはいかがか。

（ア） どのような業務で実際にデータの受け渡しが発生しているか、**複数の規模の異なる地方公共団体にヒアリングを実施し、頻度や業務負荷が多いデータの受け渡しのパターンを抽出**。

(イ) (ア)で抽出したパターンについて、電磁的記録媒体を利用しない方式を検討する方針を**全団体に照会**

(ウ) **(イ)の照会結果を踏まえ、必要に応じて新たな方式を検討**する。

(エ) (ウ)までで検討した方式についてリスク分析を実施し、必要なセキュリティ対策を含めガイドラインに規定する。

■ 今年度は、上記（ア）から（ウ）までを実施（※）し、地方公共団体の業務の実情を踏まえた方式を検討することに注力することとしてはいかがか。（※可能であれば（ア）～（エ）までをすべて実施する）

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【概要②】

Ⅲ　2030年頃の国・地方ネットワークの将来像

2030年の姿

- 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**
- **国・地方のネットワーク基盤の共用化**が行われ、**ネットワークの効率性が向上**
- 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**

シンプルかつ柔軟なネットワーク

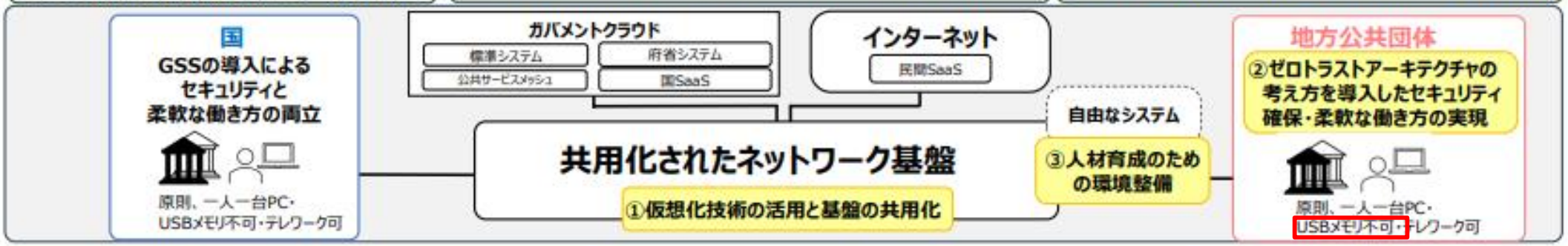
・**仮想化ネットワーク技術の活用**により、シンプルかつ柔軟なネットワークを構築

災害時のレジリエンスの確保

・大規模災害等にも対応し得る**強靭性・冗長性を確保**
（例：地上回線＋衛星回線の活用、国と地方ネットワークの相互運用等）

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・柔軟なサービス構成には、**「ゼロトラストアーキテクチャ」の考え方が有効**



①仮想化技術の活用と基盤の共用化

- 国は、冗長化された共用可能な回線等を全国に整備し、仮想化技術を用い、柔軟で可用性の高い論理ネットワークを効果的・効率的に整備
- 国・地方での平時のコスト効率向上、レジリエンスの確保、地方の負担軽減のため、仮想化技術を活用しつつ、**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（※）

（※）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。
その際、新技術（Beyond5G等）の活用や費用負担の在り方等も検討

②ゼロトラストアーキテクチャの考え方の導入

- 国は、ゼロトラストアーキテクチャの考え方を導入したGSSに、原則移行し、柔軟な働き方とセキュリティの両立を実現。ユーザー数増加に対応するため、保守・運用体制を強化
- 地方のネットワーク上のシステムについて、**デジタル庁・総務省が調査・分析・検証を実施**（※）した上で、**ゼロトラストアーキテクチャの考え方に基づきセキュリティを強化**

（※）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予定

③人材育成のための環境整備

- 行政職員による基礎的なデジタル能力の修得、システムの構築・運用に必要な技術研鑽、官民の技術者・研究者との交流、革新的技術の創出等を実現できる、人材育成環境としての**「自由なシステム」**（※）を整備

（※）行政人材によって自律的に発達するデジタル人材育成サイクルを支える仕組みや実験用ネットワーク等。他のデジタル人材に係る施策とも連携して官民人材を発掘・育成

- LGWANが担っている重要情報のやり取りを行う機能(※)の在り方は引き続き検討　(※)マイナンバー制度による情報連携、J-アラート等
- 地方の強固なセキュリティ・さらなる利便性向上に向け、J-LIS・IPAによる共同研究・実証実験を推進
- ガバメントクラウド上のデータの保護のため、より一層低コストかつ安全な方法について、暗号技術を含む多角的な観点からの調査研究を実施

今後の進め方

- 本報告書について、地方の意見を丁寧に伺った上で、**可能なものから速やかに上記実証等を実施**
- 標準化に取り組む地方の負担やネットワーク更改時期等を考慮した上で、新たなネットワークへの移行は、**分散・段階的に実施**