資料　1

令和５年度の検討を踏まえた
改定方針

総 務 省

令和６年７月22日

総務省自治行政局

デジタル基盤推進室

令和５年度の各検討項目について

- ✓ 令和５年度は以下の項目について議論し、方向性が固まったLGWAN接続系のローカルブレイクアウト（α’モデル）と、令和５年度NISC政府統一基準群改定に関する対応について、早期に自治体の事務に資する観点から、中間報告としてとりまとめ、公表済み。
- ✓ 残りの検討項目については、今年度改めて議論。

検討項目

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

→ 中間報告として３月に公表済み

令和５年度NISC政府統一基準群改定に関する対応

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

情報システムの品質管理の推進に関する対応

→ **昨年度の検討結果を踏まえ今回検討**

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

→ 「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」の報告書を踏まえ、一人一台端末が可能となるよう今年度も引き続き検討

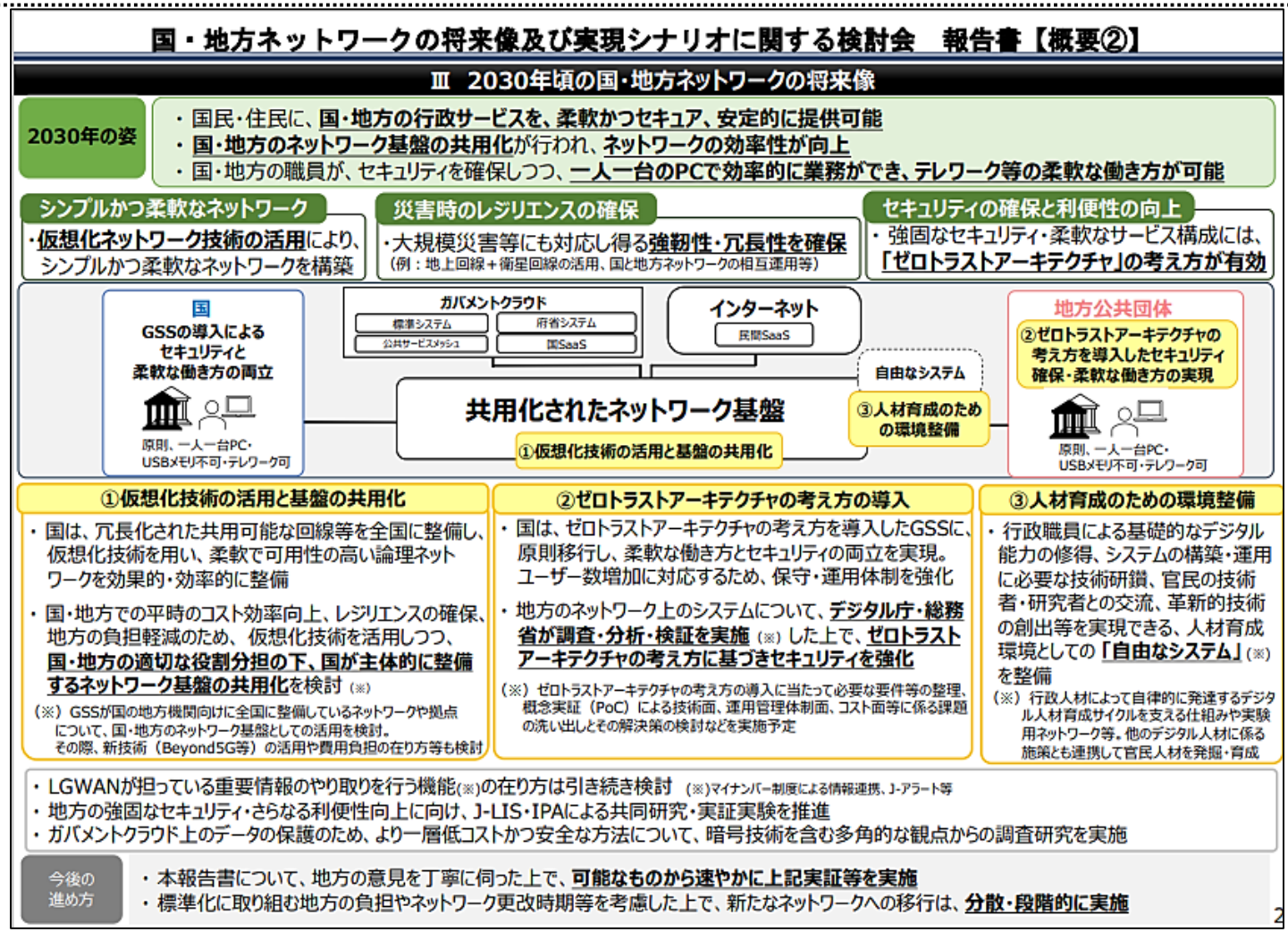
◎デジタル社会の実現に向けた重点計画（2024年（令和６年）６月21日） 重点施策一覧（抄）

○[No.1-73] 中長期の視点で全体最適となる「国・地方を通じたデジタル基盤」としてのネットワークの実現

- 今後、国・地方の更なる連携強化やコスト効率化、セキュリティ強化、サービスレベルの向上を実現するため、**「2030年頃の国・地方のネットワークの将来像」の実現に向け、以下の取組を着実に進める**。
- 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の検討
- **地方のネットワーク上のシステムへのゼロトラストアーキテクチャの考え方の導入に向けた調査・分析・検証**
- 行政職員がシステムの構築・運用に必要な技術研鑽等が可能な人材育成環境の整備

等について、可能なものから速やかに実施する。あわせて、将来像への移行プロセスの具体化、安定的かつ持続的な運用管理体制、**情報セキュリティポリシーガイドライン（注）等について更なる検討を行う**。

（注）「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」（総務省）



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

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

ガイドラインの改定の方向性（昨年度提示）

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。

（参考）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等①

○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（2022 年（令和４年）12 月 28 日デジタル社会推進会議幹事会決定）

１.２ 適用対象

本方針は、デジタル・ガバメント推進標準ガイドラインが適用されるサービス・業務改革並びにこれらに伴う**政府情報システムの整備及び管理に関する事項に適用するものとする**。ただし、**特定秘密**（特定秘密の保護に関する法律（平成 25 年法律第 108 号）第３条第１項に規定する特定秘密をいう。）及び行政文書の管理に関するガイドライン（内閣総理大臣決定。初版平成 23 年４月１日。）に掲げる秘密文書中**極秘文書に該当する情報を扱う政府情報システムについては、本方針の全部を適用対象外**とする。

また、**安全保障、公共の安全・秩序の維持といった機微な情報及び当該情報になり得る情報を扱う政府情報システムについては**、別添を除いて**本方針の全部を適用対象外**とする。（略）

３.１ クラウドサービスの選択

クラウドサービスの利用についてはガバメントクラウドを原則とするが、**ガバメントクラウドを利用しない場合については**、セキュリティの観点より、**ISMAPに登録されたものを原則として選定**する。 （略）

別添） **安全保障、公共の安全・秩序の維持といった機微な情報及び当該情報になり得る情報**[2] **をクラウドで扱う上での基準については**、経済財政運営と改革の基本方針及びデジタル社会の実現に向けた重点計画（令和４年６月決定）で明記された方針に沿って、セキュリティの観点から個別の措置を講ずる必要があること等を踏まえ、基本的かつ共通的な内容を**「安全保障等の機微な情報等に係る政府情報システムの取扱い」として定めた**ため、当該文書を参照されたい。

---

2 行政文書の管理に関するガイドライン（内閣総理大臣決定。初版平成 23 年４月１日。）に掲げる秘密文書中**秘文書に該当する情報及びそれに準ずる情報**のこと。（略）

○デジタル社会の実現に向けた重点計画（2023年（令和５年） ６月９日閣議決定）

５． デジタル社会を支えるシステム・技術

（１） 国の情報システムの刷新

⑤ ガバメントクラウドの整備

各府省庁の情報システムにおけるクラウドサービスの利用の検討に当たっては、原則としてデジタル庁が整備したガバメントクラウドの活用を検討することとし、クラウド化等を進める場合には、情報システム構築の迅速性・柔軟性の向上、可用性を始めとする高いセキュリティの実現、コスト効率の向上など、これにより得られる効果の追求を図る。

（参考）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等②

○デジタル・ガバメント推進標準ガイドライン　－サービス・業務改革並びに政府情報システムの整備及び管理について－（令和５年3月31日デジタル社会推進会議幹事会決定）

第２章 標準ガイドライン群の整備について

１．体系

1) **デジタル・ガバメント推進標準ガイドライン**

サービス・業務改革並びにこれらに伴う政府情報システムの整備及び管理に関して、その手続・手順に関する基本的な方針及び事項並びに政府内の各組織の役割等を定める体系的な政府の共通ルールである。**「標準ガイドライン」と略称**する。

第３章 適用

１．適用対象

標準ガイドラインは、**政府情報システムに適用する**ものとする。また、各府省が所管する政府情報システムに標準ガイドラインを適用するに当たり、情報の取扱いに重大な懸念があると判断する場合はデジタル庁に遅滞なく相談し所要の調整をするものとする。標準ガイドライン附属文書の適用対象は、それぞれに定めるところによる。

○標準ガイドライン群用語集（最終改定：2023年3月31日）

政府情報システム　**各府省がサービス・業務を実施するために用いる情報システム**のこと。

○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/令和４年２月７日 全部改正）

第10 秘密文書等の管理

２　特定秘密以外の公表しないこととされている情報が記録された行政文書のうち秘密保全を要する行政文書（特定秘密である情報を記録する行政文書を除く。以下「秘密文書」という。）の管理

(1)　**秘密文書は、次の種類に区分**し、指定する。

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

昨年度いただいたご意見

✓ 前回の検討会では、個人情報保護法、ネットワークセグメント、ISMAP登録サービスの利用等の観点からご意見をいただいた。

検討項目	視点	発言要旨
機密性の分類	ネットワークセグメント	• 自治体によっては、マイナンバー利用事務系ではなくLGWAN接続系で業務を行っているものもあるため、マイナンバー利用事務系の情報はあくまでも機密性３Bの例であるということを明確にし、**機密性３Bはマイナンバー利用事務系の情報のみが該当すると誤解されないような表現を考えた方がよい**。
	個人情報保護法関係	• 機密性３Bのところに「機微な住民情報」とあるが、「機微な」という記載は、個人情報保護法の要配慮個人情報を想起することが多いと思われる。「機微な」を削除した方がよい。 • マイナンバー利用事務系の「住民情報」とは何を指すのか、やや定義の揺らぎが生じてくるのではないかと疑問に思っている。個人情報ファイルだと言い切って書いてしまってもよい。
	ISMAP登録サービスの利用	• ISMAPに登録されているサービスの中には、一般に広く公開するようなシステムを構築できるものもあり、そのようなサービスに機密性３Bの情報を乗せることで、**利用形態によっては機密性３Bの情報がインターネットに公開されてしまうシステムを構築することが出来てしまうため、その配慮が必要**。 • ISMAPに登録されているサービスの中には、利用方法によっては情報漏えいに繋がる可能性のあるものもある。**ISMAPの登録だけではなく、当該サービスがどのような管理策を取っているかまで確認が必要**。
	その他	• 自治体機密性３Cに関しては、ファイルサーバ等に市民から集めた一部の個人情報を置くことがあるため、システム化されていないファイルサーバであっても暗号化やアクセス制御が徹底されていれば、住民情報を含んだファイルをインターネット接続系に配置しても良いと、という表現があると望ましい。 • 自治体機密性３Bと機密性３Cの差別化を図るために、**個人情報の中で「３B以外の」と明記すると、混乱を避けられるのではないかと思う**。

自治体機密性３Bと３C

- ✓ 自治体機密性３Bの例について、**「マイナンバー利用事務系」など、特定のネットワークセグメントを表す用語を用いず**、**個人情報保護法上の用語の使用についても検討**する。
- ✓ 自治体機密性３Cの例について、過去の検討会意見を踏まえ、職員の属性に基づく個人情報などを記載するのが望ましいと考えられる。

分類	分類基準	情報資産の例/ インターネット接続系への配置
自治体 機密性３B	行政事務で取り扱う情報資産のうち、**漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき**情報資産	**<例>** ・ **住民情報（基本４情報等）を束ねたリストやこれに準ずる情報** （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、農業委員会台帳システム、貸付金償還システム、許認可・免許管理システム等に保存される住民の個人情報） <インターネット接続系への配置> β'モデルにおいても、住民記録システム等をインターネット接続系を置くことは想定していないため**不可**
自治体 機密性３C	行政事務で取り扱う情報資産のうち、**自治体機密性３B以上に相当する機密性は要しない**が、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	**<例>** ・ **職員としての属性に基づく個人情報** ・ オンライン申請の処理等により**システム処理上、一時的にインターネット上に保管されるデータ** ・ 文書管理システムの決裁文書として保存されている個人情報 ・ 施設設計情報や入札予定価格など非公開情報 <インターネット接続系への配置> β'で求められている、**情報資産単位でのアクセス制御、業務システムログ管理の実施等を条件として可**

- ３Bはマイナンバー利用事務系ではなく**LGWAN接続系で業務を行っているものもあるため、マイナンバー利用事務系の情報のみが該当すると誤解されない**ような表現が必要。
- **（個人情報保護法上の）個人情報ファイル**だと言い切って書いてしまってもよいのではないか。

- 職員の人事情報と、一般的な住民情報は分けるべき（10/10検討会）
- 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**住民の台帳**よりも機密性が低いのではないか。（10/10検討会）

- システム化されていないファイルサーバであっても暗号化やアクセス制御が徹底されていれば、住民情報を含んだファイルをインターネット接続系に配置しても良いと、という表現があると望ましい。

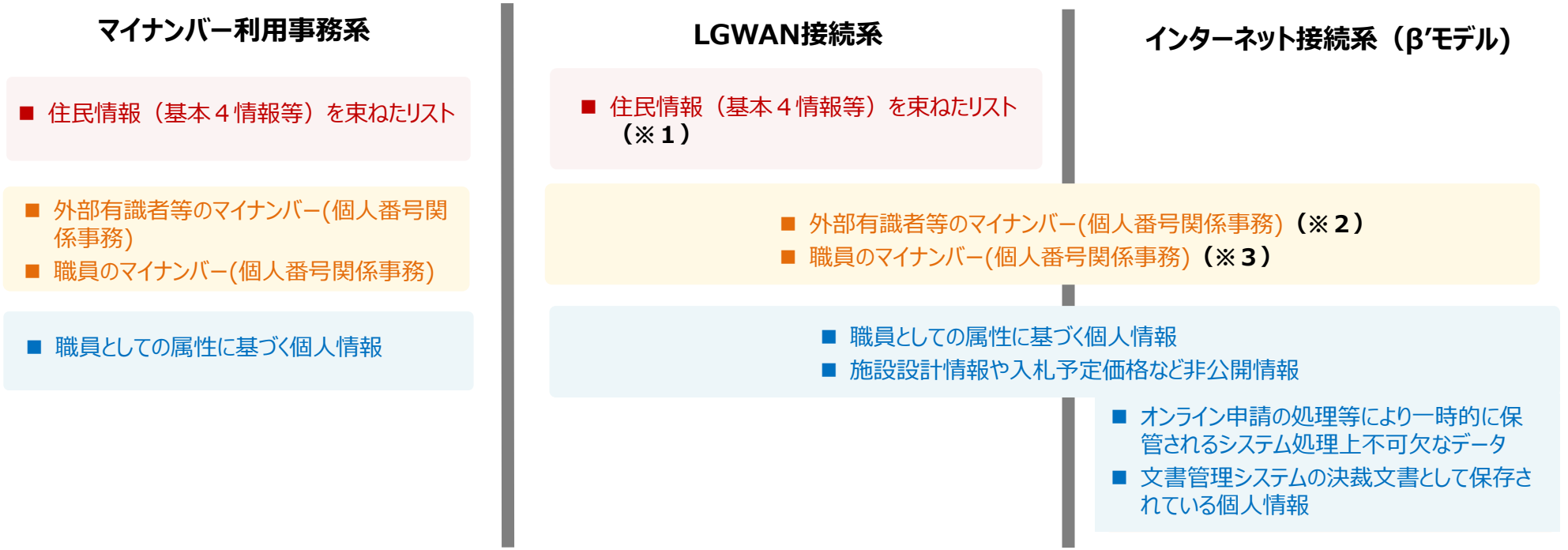
  → ファイルサーバのセキュリティ要件の定義のためには**リスクアセスメントが必要**

個人情報の中で**「３Ｂ以外の」と明記する**と、混乱を避けられるのではないか

ネットワークセグメントと情報資産の対応関係

✓ 各ネットワークセグメントと情報資産（一部）の対応関係は、以下の図のようになると考えられる。
✓ **「台帳」のような大量の住民情報（基本４情報等）を束ねたリスト**は、住民基本台帳のように、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、また扱われる業務の規模が大きいと考えられるため、**インターネット接続系に置かない**ものとし、**自治体機密性３Bに分類するのが望ましい**のではないか。

赤字：住民情報（基本４情報等）を束ねたリスト　橙字：マイナンバー　青字：その他



※１：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、農業委員会の台帳等をLGWAN接続系に配置している場合がある。
※２：源泉徴収票に印字等を実施するため、外部有識者、CISOアドバイザー、操作研修講師等のマイナンバーをマイナンバー利用事務系以外で保持している場合がある。
※３：現行のガイドラインでは、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。」と注書きで規定。

個人情報保護法上の用語との整理

- ✓ 個人情報保護法や、個人情報保護委員会の各種ガイドラインによると以下のとおり整理が可能。
- ✓ 住民情報（基本４情報等）を束ねたリストとして想定しているものは、個人情報保護法上の**「台帳形式になった住民情報を含む個人情報ファイル」**と記載することが可能。

個人情報ファイル（法第60条第２項）

保有個人情報を含む情報の集合物で、以下のもの。

① **一定の事務の目的を達成するため**に**特定の保有個人情報を電子計算機を用いて検索することができるように体系的に構成したもの**

② ①のほか、**一定の事務の目的を達成するため**に**氏名、生年月日、その他の記述等により特定の保有個人情報を容易に検索することができるように体系的に構成したもの**

- ✓ 住民情報（基本４情報等）を束ねたリストは、個人情報ファイルに該当すると考えられる。
- ✓ 公表されている個人情報ファイル簿から、「住民基本台帳システム」、「自動車税システム」等が個人情報ファイルであることがわかる。

個人情報ファイル簿（法第75条）

個人情報ファイルについて、**ファイルの名称、利用目的、記録項目等を記載した帳簿**

公表義務が課されており、個人情報そのものではない。

要配慮個人情報（法第２条第３項）

本人の**人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実**その他本人に対する**不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するもの**として政令で定める記述等が含まれる個人情報

- ✓ 実態としては、要配慮個人情報は個人情報ファイルの中で記載されると考えられる。
- ✓ 行政事務で取り扱う頻度の多さ、業務の規模の観点では、住民の個人情報ファイルを例として明示することが望ましいと考えられる。

個人情報データベース等（法第16条）

個人情報を含む情報の集合物であって、利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定めるものを除いた以下のもの。

① 特定の個人情報を電子計算機を用いて検索することができるように 体系的に構成したもの

② ①のほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの

例：電子メールソフトに保管されているメールアドレス帳、インターネットサービスに係るログ情報の電子ファイル(ユーザーIDと個人情報を容易に照合することができる場合）※個人情報の保護に関する法律についてのガイドライン（通則編）（令和5年12月一部改正）

- ✓ 行政事務の目的を達成するための、住民情報（基本４情報等）を束ねたリストは、個人情報ファイルに該当すると考えられる。
- ✓ 法第４章及び第８章において個人情報データベース等を事業の用に供している者として定義されている個人情報取扱事業者には、行政機関は含まれない（法第16条第２項）

（参考）個人情報保護法

○個人情報の保護に関する法律（平成十五年法律第五十七号）

（定義）

第二条　この法律において「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。

３　この法律において「**要配慮個人情報**」とは、**本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報**をいう。

（定義）

第十六条　この章及び第八章において「**個人情報データベース等**」とは、個人情報を含む情報の集合物であって、次に掲げるもの（利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定めるものを除く。）をいう。

一　特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの

二　前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの

２　**この章及び第六章から第八章までにおいて「個人情報取扱事業者」とは、個人情報データベース等を事業の用に供している者をいう。ただし、次に掲げる者を除く**。

一　国の機関

二　地方公共団体

三　独立行政法人等

四　地方独立行政法人

（定義）

第六十条　（略）

２　この章及び第八章において「**個人情報ファイル**」とは、保有個人情報を含む情報の集合物であって、次に掲げるものをいう。

一　一定の事務の目的を達成するために特定の保有個人情報を電子計算機を用いて検索することができるように体系的に構成したもの

二　前号に掲げるもののほか、一定の事務の目的を達成するために氏名、生年月日、その他の記述等により特定の保有個人情報を容易に検索することができるように体系的に構成したもの

（参考）個人情報保護法

○個人情報の保護に関する法律（平成十五年法律第五十七号）

（個人情報ファイルの保有等に関する事前通知）

第七十四条　行政機関（会計検査院を除く。以下この条において同じ。）が個人情報ファイルを保有しようとするときは、当該行政機関の長は、あらかじめ、個人情報保護委員会に対し、次に掲げる事項を通知しなければならない。通知した事項を変更しようとするときも、同様とする。

一　個人情報ファイルの名称

二　当該機関の名称及び個人情報ファイルが利用に供される事務をつかさどる組織の名称

三　個人情報ファイルの利用目的

四　個人情報ファイルに記録される項目（以下この節において「記録項目」という。）及び本人（他の個人の氏名、生年月日その他の記述等によらないで検索し得る者に限る。次項第九号において同じ。）として個人情報ファイルに記録される個人の範囲（以下この節において「記録範囲」という。）

五　個人情報ファイルに記録される個人情報（以下この節において「記録情報」という。）の収集方法

六　**記録情報に要配慮個人情報が含まれるときは、その旨**

七　記録情報を当該機関以外の者に経常的に提供する場合には、その提供先

（略）

九　第七十六条第一項、第九十条第一項又は第九十八条第一項の規定による請求を受理する組織の名称及び所在地

十　第九十条第一項ただし書又は第九十八条第一項ただし書に該当するときは、その旨

（個人情報ファイル簿の作成及び公表）

第七十五条　行政機関の長等は、政令で定めるところにより、当該行政機関の長等の属する行政機関等が保有している**個人情報ファイルについて、それぞれ前条第一項第一号から第七号まで、第九号及び第十号に掲げる事項その他政令で定める事項を記載した帳簿**（以下この章において「**個人情報ファイル簿**」という。）を作成し、公表しなければならない。

ISMAP登録サービスの利用に係る留意点

- ✓ ISMAP登録サービスであっても、**自治体自身の責任で個々のサービスのセキュリティについて個別に検討し、必要な対策を実施する必要がある**。
- ✓ 例えば、SaaSサービスの中には、ローコードツール（必要最小限のソースコードを書くことによりアプリケーション等を開発する手法）によりシステム構築が可能になるものがあるが、そのような場合は自治体自身の責任で、セキュリティ機能を構築する必要がある。

●例：ISMAPに登録されている、あるローコードツールに係る責任分界

※サービスごとに責任範囲が異なるため注意が必要

自治体責任（各自治体が利用するサービス内容を踏まえ、個別にセキュリティ対策すべき領域）

- 利用デバイスからインターネット接続環境への接続
- ユーザ管理設定・アプリケーション運用・プラグインの管理
- APIを利用したシステム開発
- APIサービス　※SaaS事業者が提供するもの

SaaSサービス提供事業者責任

- アプリケーションの開発保守
- ミドルウェア・OS・仮想基盤環境の提供
- インターネット接続環境の提供
- 設備機器（UPS）・土地・建物の提供

多くのクラウドサービスでユーザ側が設定することになっている領域があり、設定内容により脆弱な状態になり得るため、個別に対策が必要である。

※　サービス範囲は多様であるため、ガイドラインで一律に対策を示すことは困難であるが、例示として、以下の対策が考えられる。

- アクセス制御（ID・PWのみ、多要素認証など）
- 回線暗号化
- データの暗号化
- 権限昇格の防止
- データ消去

ISMAP登録されている場合でも、以下の点が事前に確認が必要である

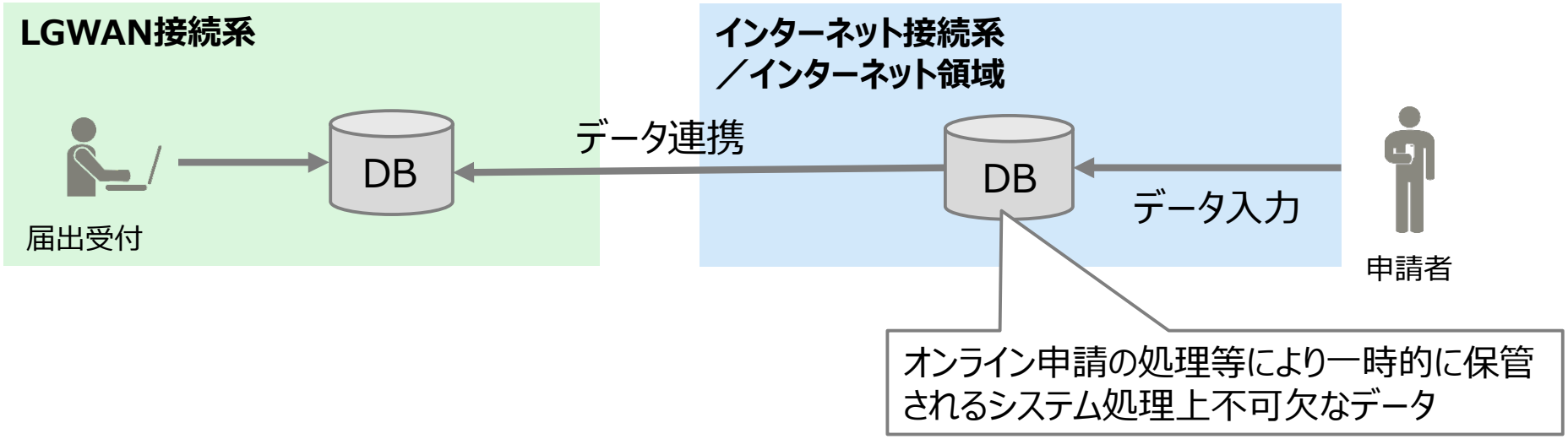
- 言明対象の範囲を詳細に確認する。（表題のみで許可は判断できない）
- データが保存されるリージョンが海外か国内かを確認し、情報資産の機密性に応じて選定する

※　ガイドライン第３編第８章8.2.（１）外部サービスに係る規定（外部サービス利用判断基準）の整備及び8.2.（２）外部サービスの選定②の解説にも記載

（参考）一時的にインターネット上に保管されるデータ

- ✓ インターネットから申請を受け付ける場合は、インターネット領域でシステム処理が必要であり、一時的に申請データがインターネット上に存在する状態になる。
- ✓ 外部からサイバー攻撃を受けた場合に漏えいするリスクを鑑み、自治体機密性３C以上の情報に求められる対策が必要と考えられる。

●例：汎用的電子申請システム、施設予約システム等



※上図は、データの流れを簡略化して示したものであり、データ連携やセキュリティ確保に係る構成は簡略化されている。

国と地方公共団体における機密性分類

国

（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（政府統一基準））

ガバメントクラウドの利用対象外 ※1

機密性３

秘密文書

（極秘文書、秘文書）

機密性２

情報公開法上の**不開示情報**

（個人情報を含む）

ガバメントクラウドの利用が原則 ※1

機密性１

情報公開法上の**開示情報等**

※１　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）

地方公共団体

（現行ガイドライン）

機密性３

秘密文書

（住民の個人情報　等）

機密性２

直ちに一般に公表することを前提としていない情報

（政策検討に関する情報　等）

機密性１

機密性２又は機密性３の情報以外の情報

（ガイドライン改定(案)）

自治体機密性３

A　**秘密文書**　（極秘文書、秘文書）

B　**漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、**事務又は業務の規模や性質上、取扱いに非常に留意すべき情報
（住民記録システム、税務システム等に保存される住民の個人情報）

C　自治体機密性３B以上に相当する機密性は要しないが、**基本的に公表することを前提としていない**情報
（職員の属性に基づく個人情報、入札予定価格）

自治体機密性２

自治体機密性３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

（政策検討に関する情報　等）

自治体機密性１

行政事務で取り扱う情報のうち、自治体機密性２以上に相当する機密性は要しない情報

ガイドラインの改定の方向性

機密性 高 → 低

分類	分類基準	情報資産	パブリッククラウドサービス（※１）の範囲
自治体 機密性３A	行政事務で取り扱う情報資産のうち、「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）に定める秘密文書に相当する文書	＜例＞ ・「行政文書の管理に関するガイドライン」上の**極秘文書、秘文書に相当する文書**（統一基準における機密性３情報に相当する情報） **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	「行政文書の管理に関するガイドライン」、統一基準の規定に則って取り扱うものとする（なお、上記ガイドラインにおいては、極秘文書について、**インターネットに接続していない**電子計算機又は媒体等に保存することが求められている（※２））
自治体 機密性３B	行政事務で取り扱う情報資産のうち、**漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき**情報資産	＜例＞ ・**データベースや台帳形式になった住民情報を含む個人情報ファイル及びこれに準ずる情報** （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、農業委員会台帳システム、貸付金償還システム等に保存される住民の個人情報）	ISMAP登録サービスは利用可（8.3で規定される**アクセス制御、機密性保護のための暗号化等**が必要） ※統一基準改定に合わせて、8.3でクラウドサービスの利用について規定
自治体 機密性３C	行政事務で取り扱う情報資産のうち、**自治体機密性３B以上に相当する機密性は要しないが、基本的に公表することを前提としていない**もので、業務の規模や性質上、取扱いに留意すべき情報資産	＜例＞ ・**職員としての属性に基づく個人情報** ・オンライン申請の処理等により、**システム処理上一時的にインターネット上に保管されるデータ** ・文書管理システムの決裁文書として保存されている個人情報 ・施設設計情報や入札予定価格など非公開情報	
自治体 機密性２	行政事務で取り扱う情報資産のうち、自治体機密性３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	＜例＞ ・政策検討に関する情報	可 （8.3で規定されるアクセス制御、機密性保護のための暗号化等が必要）
自治体 機密性１	自治体機密性２又は機密性３の情報資産以外の情報資産	＜例＞ ・将来公表する予定の文書（白書の案等） ・公表された情報	可

注）自治体機密性３C情報については、β'モデルで求められている、情報資産単位でのアクセス制御、業務システムログ管理の実施等を条件としてインターネット接続系における利用が可能。

※１　クラウド事業者が提供するサーバやネットワークなどのインフラを、仮想化技術により複数のユーザで共用し、個々のユーザが、システムの運用体系を完全に制御することが難しいサービスを想定している。
※２「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、令和４年２月7日 全部改定）第10 秘密文書等の管理

自治体機密性２以上の情報を取り扱う場合に必要な対策

✓ 現行のガイドラインにおける、不正なアクセスを防止するための**アクセス制御**、機密性保護のための**暗号化**を改定後も求める予定。

政府統一基準

4.2.2 クラウドサービスの利用（要機密情報を取り扱う場合）
遵守事項
(1) クラウドサービスの利用に係る運用規程の整備
(a)統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用規程として整備すること。
(b) 統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規程として整備すること。
（略）
(2) クラウドサービスの利用に係るセキュリティ要件の策定
（略）
(b) クラウドサービス管理者は、クラウドサービスを利用する目的、対象とする業務等の業務要件及びクラウドサービスで取り扱われる情報の格付等に基づき、(1)各項で整備した基本方針としての運用規程に従い、クラウドサービスの利用に係るセキュリティ要件を策定すること。

(3) クラウドサービスを利用した情報システムの導入・構築時の対策
(c) クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備すること。
(ア)クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順
（略）
(4) クラウドサービスを利用した情報システムの運用・保守時の対策
(a) クラウドサービス管理者は、(1)(b)で定めた運用規程を踏まえて、クラウドサービスに係る運用・保守を適切に実施すること。また、運用・保守時に実施状況を定期的に確認・記録すること。
（略）

セキュリティ要件について、アクセス制御、暗号化等については現行のガイドラインのまま具体的に記載（統一基準では「基本対策事項」に記載）

改定案：対策基準(例文)

8.3.外部サービス(クラウドサービス)の利用（機密性２以上の情報を取り扱う場合）
【例文】
（２）クラウドサービスの利用に係る運用規程の整備
①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを導入・構築する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。
②統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、クラウドサービスを利用して情報システムを運用・保守する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。
（略）
（６） クラウドサービスを利用した情報システムの導入・構築時の対策
①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、以下を含むクラウドサービスを利用して情報システムを構築する際のセキュリティ対策を規定しなければならない。
（ア）不正なアクセスを防止するためのアクセス制御
（イ）取り扱う情報の機密性保護のための暗号化
（略）
③クラウドサービス管理者は、クラウドサービスの情報セキュリティ対策を実施するために必要となる文書として、クラウドサービスの運用開始前までに以下の全ての実施手順を整備しなければならない。
（ア）クラウドサービスで利用するサービスごとの情報セキュリティ水準の維持に関する手順
（略）
（７） クラウドサービスを利用した情報システムの運用・保守時の対策
①統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方を踏まえ、以下を含むクラウドサービスを利用して情報システムを運用する際のセキュリティ対策を規定しなければならない。
（略）
（エ）不正アクセスを防止するためのアクセス制御
（オ）取り扱う情報の機密性保護のための暗号化
（略）

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。

（参考）セキュリティインシデントに関する判例

✓ 原告のウェブサイトにおける商品のウェブ受注システムの導入を、被告（情報システムの保守事業者）に委託したが、納入された当該受注システムに不正アクセスがあり、顧客のクレジットカード情報を含む個人情報（約7,000件）が流出した。

✓ 判決では、**当時の技術水準に沿ったセキュリティ対策を施したプログラムを提供することが黙示的に合意されていた**ことを理由に、**被告が、個人情報の漏洩を防ぐために必要なセキュリティ対策を施したプログラムを提供すべき債務を負っている**との判断が出された。

✓ 最終的に原告の請求の一部である損害賠償請求が認められた。

◎ウェブサイトによる商品の受注システムを利用した顧客のクレジットカード情報が流出した事故につき、システムの設計、製作、保守等の受託業者の債務不履行に基づく謝罪・問合せ等の顧客対応費用、売上損失等の損害賠償責任が肯定された事例（東京地判平 26.1.23 判時 2221号）

- **経済産業省は**、平成18年2月20日、「個人情報保護法に基づく個人データの安全管理措置の徹底に係る注意喚起」と題する文書において、SQLインジェクション攻撃によってデータベース内の大量の個人データが流出する事案が相次いで発生していることから、独立行政法人情報処理推進機構(以下「IPA」という。)が紹介する**SQLインジェクション対策の措置を重点的に実施することを求める旨の注意喚起をしていた**。
- **IPAは**、平成19年4月、「大企業・中堅企業の情報システムのセキュリティ対策～脅威と対策」と題する文書において、ウェブアプリケーションに対する代表的な攻撃手法としてSQLインジェクション攻撃を挙げ、SQL文の組み立てにバインド機構を使用し、又はSQL文を構成する全ての変数に対しエスケープ処理を行うこと等により、**SQLインジェクション対策をすることが必要である旨を明示していた**。
- これらの事実に照らすと、**被告は**、平成21年2月4日の本件システム発注契約締結時点において、本件データベースから**顧客の個人情報が漏洩することを防止するために、SQLインジェクション対策として、バインド機構の使用又はエスケープ処理を施したプログラムを提供すべき債務を負っていたということができる**。
- **被告は**、情報処理システムの企画、ホームページの制作、業務システムの開発等を行う会社として、**プログラムに関する専門的知見を活用した事業を展開し、その事業の一環として本件ウェブアプリケーションを提供**しており、**原告もその専門的知見を信頼して本件システム発注契約を締結したと推認でき、被告に求められる注意義務の程度は比較的高度なものと認められる**ところ、SQLインジェクション対策がされていなければ、**第三者がSQLインジェクション攻撃を行うことで本件データベースから個人情報が流出する事態が生じ得ることは被告において予見が可能**であり、かつ、経済産業省及びIPAが、ウェブアプリケーションに対する代表的な攻撃手法としてSQLインジェクション攻撃を挙げ、バインド機構の使用又はSQL文を構成する全ての変数に対するエスケープ処理を行うこと等のSQLインジェクション対策をするように注意喚起をしていたことからすれば、**その事態が生じ得ることを予見することは容易であったといえる**。

※「判例研究 情報システム障害・事故における IT 事業者の責任」（弁護士法人 内田・鮫島法律事務所 伊藤 雅浩）より作成

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。

今後の方針

今年度の主な検討項目

✓　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等を踏まえ、今年度は主に以下を検討する予定。

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

（一人一台端末・USBメモリ不可）

■　マイナンバー利用事務系への画面転送

■ ネットワーク系統をまたいだデータ連携の在り方

→ 昨年度～今年度検討

（今年度に本格的にリスクアセスメントを実施）

令和６年地方分権改革に関する提案

（マイナンバー利用事務系への無線ＬＡＮ接続等を可能とする具体的対策の明示）

■　マイナンバー利用事務系における無線LAN利用

→ 今年度から検討開始