サイバーセキュリティセミナー'24 in 東北

2030年を見据えた
自治体情報セキュリティ

2024年12月11日

合同会社KUコンサルティング
髙橋　邦夫

自治体職員からフリーのコンサルタントに転身して7年目

元々は豊島区役所職員

文部科学省セキュリティポリシーガイドライン改訂検討会座長

総務省情報セキュリティポリシーガイドライン改訂検討会委員

総務省地域情報化アドバイザー

総務省テレワークマネージャー

文部科学省学校DX戦略アドバイザー

文部科学省教育情報化推進アドバイザー

他にもデジタル庁・経済産業省・厚生労働省・J-LISなどの委員を務める

令和6年度契約自治体：一関市・さいたま市・春日部市・船橋市・北区・荒川区・江東区・箕輪町・飯島町・常滑市・堺市・宇和島市

平成27年：情報化促進貢献個人等表彰「総務大臣賞」
令和4年：情報通信月間記念式典「総務大臣表彰」
令和6年：情報セキュリティ大学院大学「情報セキュリティ文化賞」

先の国会で自治体セキュリティが審議

地方自治法改正案の概要（情報システム・セキュリティ関係）

○ 地制調答申において、これまでの地方自治を基盤としつつ、**事務の種類に応じて、他の地方公共団体や国等と連携・協力し、デジタル技術を最適化された形で効果的に活用**することが重要であるとともに、国・地方公共団体等のネットワークを通じた相互接続がますます進展する中で、**地方公共団体のサイバーセキュリティ対策の実効性を担保**することが必要との提言があったことを踏まえ、以下の改正を行う。

現行制度

○ 現在の地方自治法には、情報システムについての**規定は置かれていない**。

○ サイバーセキュリティについては、総務省において**技術的助言**として「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」を示すとともに、各地方公共団体はこれを踏まえ、個々の判断でセキュリティポリシーを定めている。

改正概要

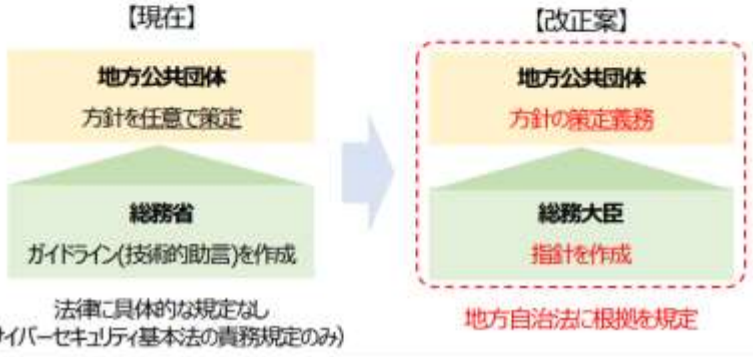
○ 地方公共団体は、**事務の種類・内容に応じ**、**情報システムを有効に利用**するとともに、**他の地方公共団体又は国と協力**し、**その利用の最適化を図るよう努める**。

○ 地方公共団体は、サイバーセキュリティの確保、個人情報の保護※など、**情報システムの適正な利用を図るために必要な措置**を講じなければならない。

○ **サイバーセキュリティの確保**について、地方公共団体の議会及び長その他の執行機関は、**方針を定め、必要な措置を講じる**。**総務大臣は、方針の策定等について指針を示す**。

※ 個人情報については、漏えい防止等の安全管理措置を講じるなど、引き続き、個人情報保護法に基づき適切に対応することが求められる。

《地方公共団体におけるサイバーセキュリティ対策》



（参考）現行の総務省ガイドラインで示している基本方針における記載事項の例

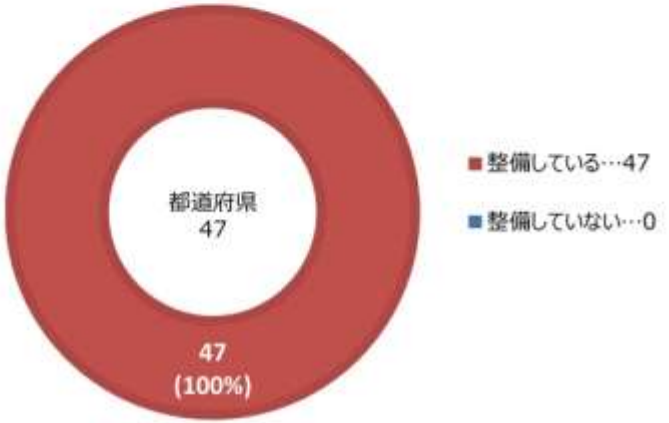
項目	情報セキュリティ対策の内容
組織体制	セキュリティ対策を推進する全庁的な組織体制を確立
物理的セキュリティ	サーバ、情報システム室、通信回線及び職員等のPC等の管理について物理的な対策を講じる
人的セキュリティ	職員等が遵守すべき事項を定めるとともに、十分な教育・啓発を行う等の人的な対策を講じる
技術的セキュリティ	コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる
業務委託	セキュリティ要件を明記した契約を締結の上、委託事業者における対策の実施を確認

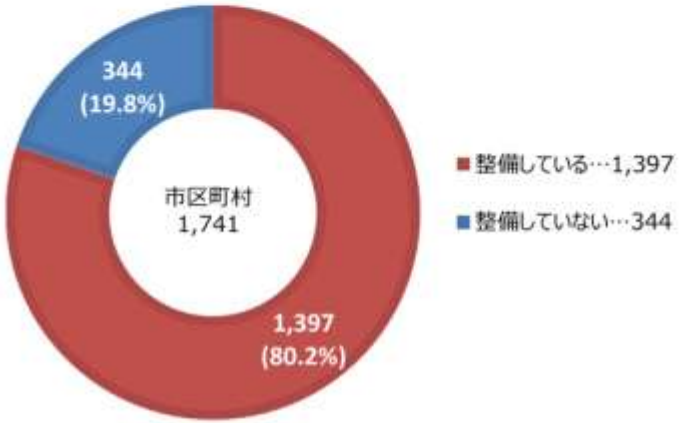
（３）情報セキュリティ対策

①　組織体制・規程類の整備

1　CSIRT（情報セキュリティインシデントに対処するための体制）の整備

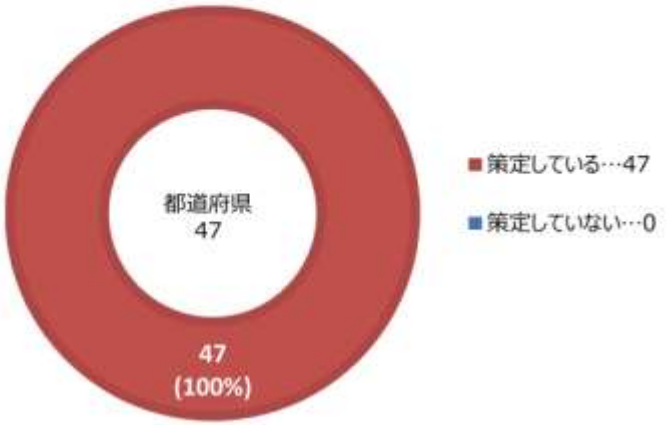
都道府県では全団体、市区町村では1,397団体（80.2%）が整備している。

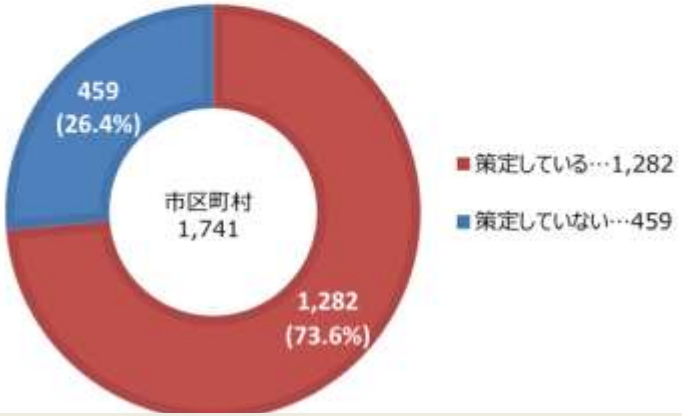




2　緊急時対応計画（情報セキュリティに関する事故及び障害等が発生した場合の体制と対応手順）の策定

都道府県では全団体、市区町村では1,282団体（73.6%）が緊急時対応計画を策定している。





「自治体DX・情報化推進概要」令和5年度調査結果より

CSIRTについては必ずしも自治体規模に比例ではない

（2）人口段階別（市および特別区。指定都市を除く。）　（　）内数字は%

	団体数	CSIRT(情報セキュリティインシデントに対処するための体制）を整備している
50万人以上	15	14(93.3)
40万～50万人未満	21	19(90.5)
30万～40万人未満	29	27(93.1)
20万～30万人未満	47	41(87.2)
10万～20万人未満	149	133(89.3)
5万～10万人未満	246	201(81.7)
5万人未満	288	243(84.4)
合　計	795	678(85.3)

（3）人口段階別（町村）　（　）内数字は%

	団体数	CSIRT(情報セキュリティインシデントに対処するための体制）を整備している
5万人以上	2	2(100.0)
4万～5万人未満	18	11 (61.1)
3万～4万人未満	45	31 (68.9)
2万～3万人未満	78	64 (82.1)
1万～2万人未満	264	213 (80.7)
5千～1万人未満	230	182 (79.1)
5千人未満	289	230 (79.6)
合　計	926	733 (79.2)

（2）人口段階別（市および特別区。指定都市を除く。）　（　）内数字は%

	団体数	情報セキュリティ対策の監査・点検			
		情報セキュリティについて内部監査のみを実施している	情報セキュリティについて外部監査のみを実施している	情報セキュリティについて内部監査及び外部監査を実施している	情報セキュリティポリシー等の遵守状況について、自己点検を実施している
50万人以上	15	7(46.7)	1(6.7)	6(40.0)	12(80.0)
40万～50万人未満	21	8(38.1)	2(9.5)	11(52.4)	16(76.2)
30万～40万人未満	29	19(65.5)	1(3.4)	7(24.1)	22(75.9)
20万～30万人未満	47	27(57.4)	2(4.3)	9(19.1)	32(68.1)
10万～20万人未満	149	68(45.6)	14(9.4)	22(14.8)	102(68.5)
5万～10万人未満	246	104(42.3)	23(9.3)	32(13.0)	139(56.5)
5万人未満	288	130(45.1)	9(3.1)	17 (5.9)	140(48.6)
合　計	795	363(45.7)	52(6.5)	104(13.1)	463(58.2)

（3）人口段階別（町村）　（　）内数字は%

	団体数	情報セキュリティ対策の監査・点検			
		情報セキュリティについて内部監査のみを実施している	情報セキュリティについて外部監査のみを実施している	情報セキュリティについて内部監査及び外部監査を実施している	情報セキュリティポリシー等の遵守状況について、自己点検を実施している
5万人以上	2	0 (0.0)	0 (0.0)	2(100.0)	1(50.0)
4万～5万人未満	18	7(38.9)	2(11.1)	2 (11.1)	8(44.4)
3万～4万人未満	45	18(40.0)	2 (4.4)	1 (2.2)	23(51.1)
2万～3万人未満	78	30(38.5)	4 (5.1)	3 (3.8)	39(50.0)
1万～2万人未満	264	108(40.9)	13 (4.9)	6 (2.3)	137(51.9)
5千～1万人未満	230	110(47.8)	6 (2.6)	7 (3.0)	115(50.0)
5千人未満	289	121(41.9)	9 (3.1)	11 (3.8)	139(48.1)
合　計	926	394(42.5)	36 (3.9)	32 (3.5)	462(49.9)

「自治体DX・情報化推進概要」令和4年度調査結果より

高橋が支援している自治体監査の例（特別区）

情報セキュリティ及び特定個人情報の安全管理措置に係る外部・内部監査報告書

令和５年度情報セキュリティ及び特定個人情報の安全管理措置に係る外部・内部監査の結果を下記のとおり報告します。

対象所属及び日程		監査日時		監査対象所属	主な監査対象範囲
	外部監査	11月1日（水）	午前	子どもわくわく課	情報資産の取扱い（個人情報含む） わくわく☆ひろば入退室管理システム 委託先の監督
			午後	保健予防課	情報資産の取扱い（個人情報含む） 予防接種に関する事務（利用事務） 新型コロナ患者管理システム 委託先の監督
		11月9日（木）	午前	高齢福祉課	情報資産の取扱い（個人情報含む） 老人福祉法施行事務（利用事務） 地域包括支援センターシステム 委託先の監督
	内部監査	10月17日（火）	午後	長寿支援課	情報資産の取扱い（個人情報含む） 委託先の監督
		10月19日（木）	午前	生涯学習・学校地域連携課	
		10月24日（火）	午前	リサイクル清掃課	情報資産の取扱い（個人情報含む）

年に6課
全部で80課
あるので10
年に1回も当
たらない

高橋が支援している自治体の例（町人口1万人未満）

ウ　監査実施

監 査 日　令和５年10月27日（金）

監査対象　住民税務課・教育委員会事務局

監査項目　[redacted]町情報セキュリティポリシー及びシステム利用実施手順書への適合

監 査 人　（合）KUコンサルティング

エ　情報セキュリティ自己点検実施（別添：セキュリティ自己点検結果集計表）

点検期間　令和６年２月９日（金）～２月29日(木)まで

実施方法　ガルーン内　ワークフローで個々に入力申請

対 象 者　庁内システムを使用する全職員

実施状況　156名/165名(94.55%)

オ　監査報告（別添：監査報告書）

令和５年３月25日（金）

指摘事項の改善確認後、監査報告書を提出

カ　情報セキュリティインシデントの報告

令和５年度　０件発生

(2)　令和６年度情報セキュリティ業務計画

年に2課
全部で10課
なので5年毎
に監査実施

自治体情報セキュリティ強靭化の背景

情報セキュリティ対策は時代と共に変遷
自治体向けガイドラインも同様に改定

2000年：政府機関のセキュリティポリシー策定
2001年：総務省自治体対象のガイドライン策定
2006年：総務省ガイドライン全面改訂
2015年：マイナンバー制度を踏まえて一部改訂

日本年金機構
情報漏えい

2016年：抜本的強化（強靭化）
2018年：強靭化策を踏まえた改定
2022年：直近の改定（ガバメントクラウド対応）

自治体情報セキュリティ強靭化の背景

日本年金機構の情報漏えい事故とは

2015年5月に日本年金機構宛に多数のマルウエア付のメールが届く　→　２名の職員が開封

＝＞　ファイル共有サーバにあった125万件の年金情報がインターネット上の中継サーバに送信された

ウイルス対策ソフトでは検知されないウイルス

標的型攻撃メールから逃れることは難しい

自治体情報セキュリティ強靭化の背景

一番の問題は重要情報の保管場所にあった

日本年金機構で年金情報は専用ネットワーク
＝＞　個人情報を扱う作業は専用システム（基幹系）
＝＞　使い勝手の良い事務処理用ネットワーク（情報系）に無断で年金情報を移管していた

多くの自治体も当時は基幹系と情報系の二層
＝＞　基幹系は旧ホストコンピューターの業務
＝＞　情報系では事務処理のほか個人情報も扱う
＝＞　他にも単独で個人情報を扱うネットワークも

自治体情報セキュリティ強靭化の背景

特定個人情報を流出させるわけにはいかない

総務省が当初発出した通知は「二層の徹底」
＝＞　新たに始まるマイナンバーの扱いは基幹系で
＝＞　情報系でマイナンバーを扱うことを禁じる通知

自治体側からの猛烈な反発
＝＞　マイナンバーを扱う業務には情報系もある
＝＞　限られた部署に配置してある基幹系のPCを
　　多くの部署に配置するのは大きな負担

自治体情報セキュリティ強靭化の背景

短期間でリスクを減らすため三層に分離

✖　特定個人情報を基幹系に移す
＝＞　当時多くの自治体で人事給与は情報系
＝＞　民生委員や消防団員の情報も情報系

○　業務システム移行よりインターネットを分離
＝＞　そもそもの脅威であるインターネットを分離する
＝＞　基幹系はそのままで情報系を2つに分ける
＝＞　インターネットとの接点は都道府県が監視

「三層の対策」概要（従来型のαモデル）

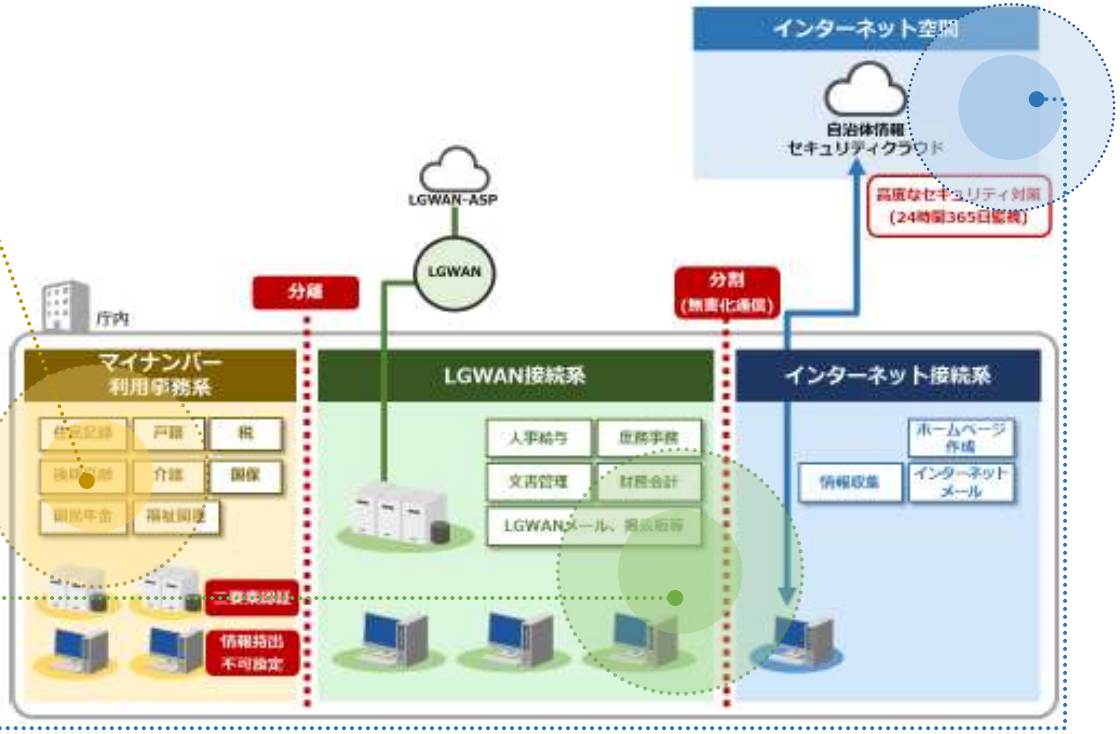
- 複雑・巧妙化しているサイバー攻撃の脅威により、地方公共団体の行政に重大な影響を与えるリスクが想定されるため、情報システムにおいては、機密性はもとより、可用性や完全性の確保にも十分配慮した、情報システム全体の強靭性の向上が求められる。
- **<u>情報システム全体の強靭性の向上を「三層の対策」により実現する</u>**。

三層の対策

1 マイナンバー利用事務系では、端末からの情報の持ち出し不可設定等を講じ、住民情報の流出を徹底して防止

2 LGWAN接続系とインターネット接続系を分割し、LGWAN環境のセキュリティを確保

3 都道府県と市区町村が協力して、自治体情報セキュリティクラウドを構築し、高度なセキュリティ対策を実施



三層の構えによる自治体情報システム例（図表21）

「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改定検討会」資料より

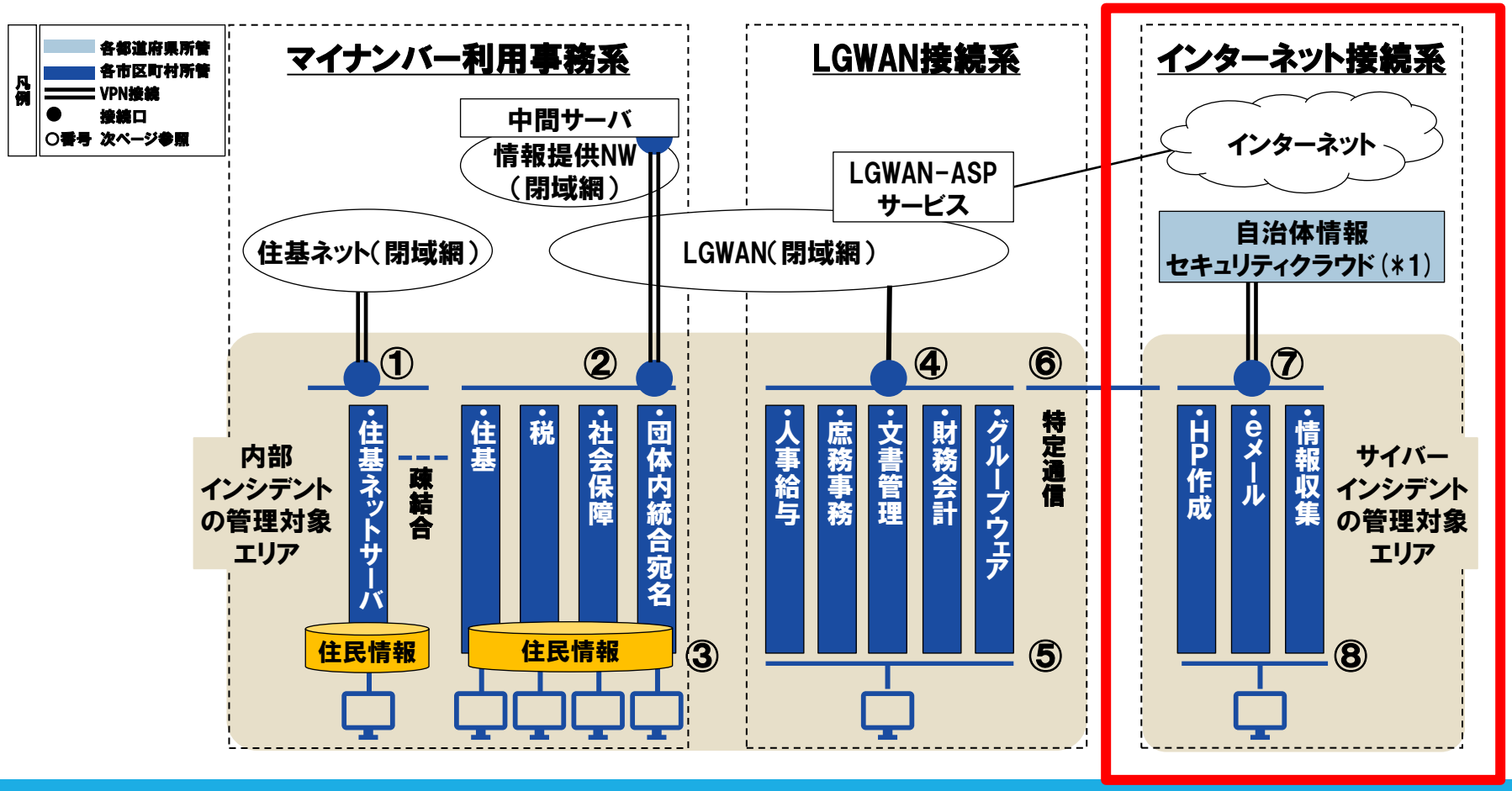
完全防御は幻想
検知後にどう対応するか

- 「防御」は時間稼ぎ
- いかに攻撃（被害）を見つけるか
- 見つけた後、どう動くか（報告・連携）

「起きた」とき、組織の内外で様々な連携が必要となる。

■ インターネット接続系

- 公開系のホームページがサイバー攻撃（DDoS、SQLインジェクション等）を受けることもある。
- 業務データは残さない前提でも、漏洩により影響が生じる情報が全くない状況が常に保たれていると言えるか

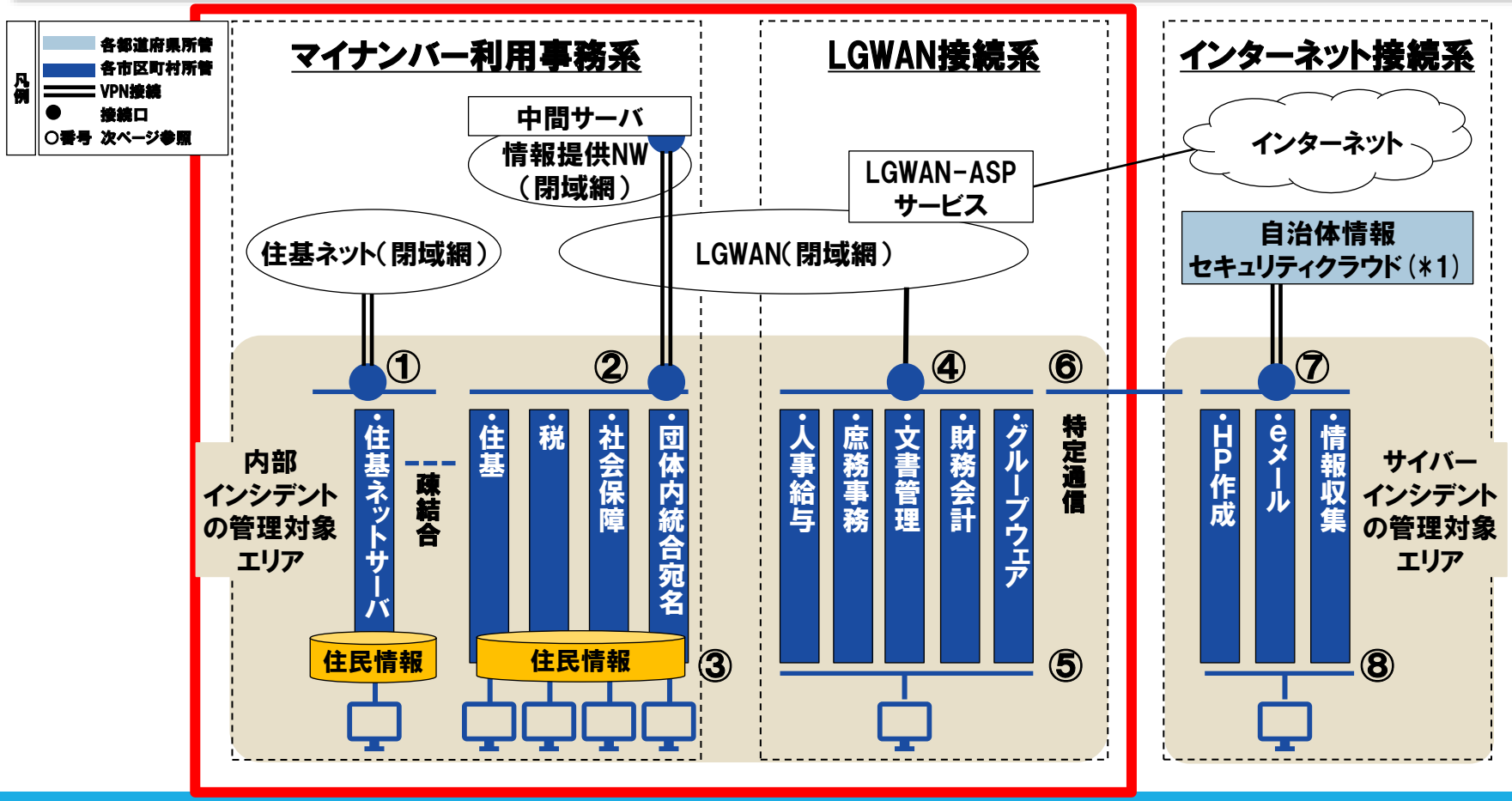


■ LGWAN接続系

インターネット接続系とは分割され、無害化通信によるファイルの切り離しが行われているが、データ通信が全く発生しない訳ではない（ファイル転送や媒体によるデータの移出入はある）

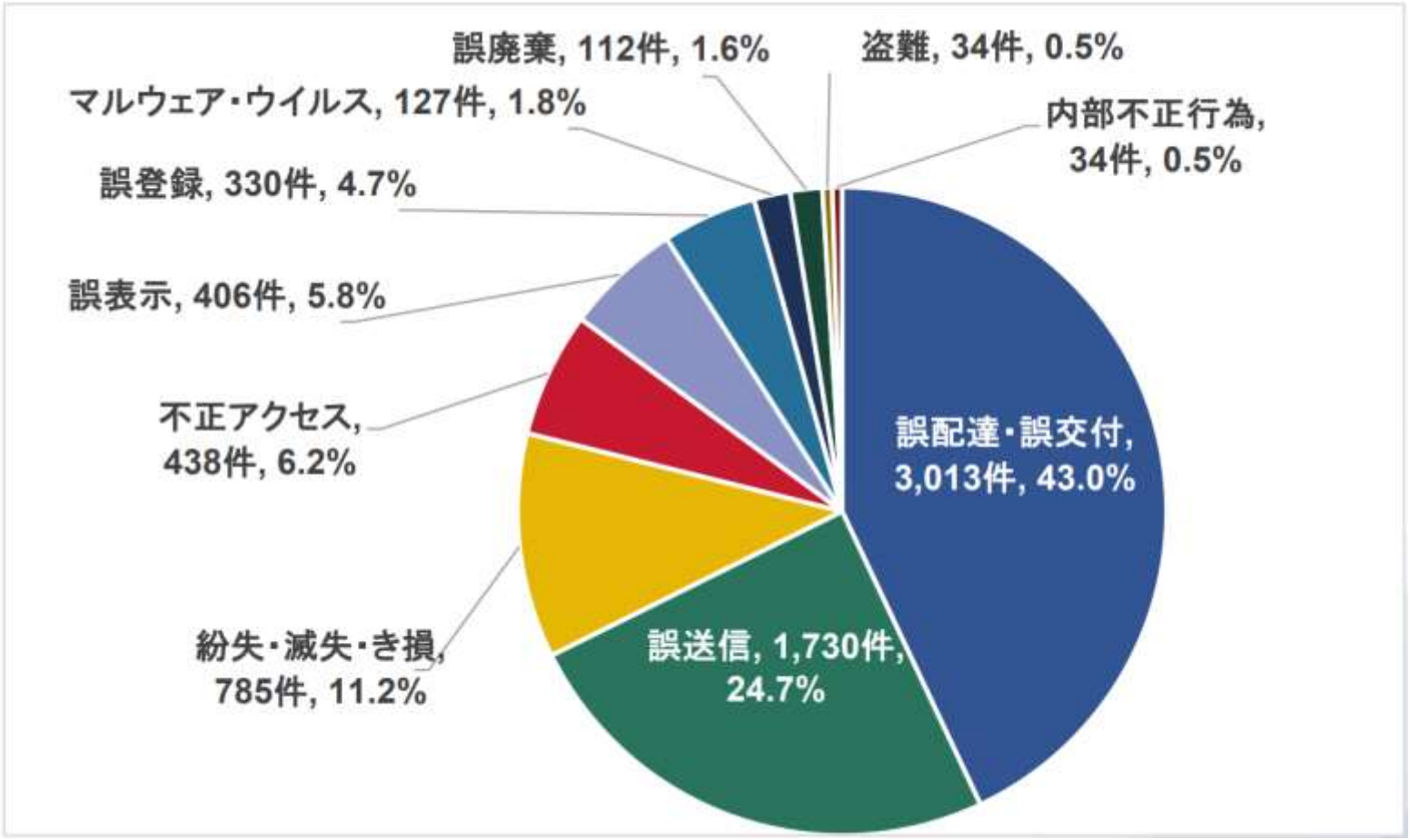
■ マイナンバー利用事務系

- 外部ネットワークからの攻撃に対して強固であっても、媒体によるデータの移出入やクラウドサービス利用など、別の経路からの情報漏えいやマルウェア感染、データ滅失等の可能性は十分有り得る。
- 扱っている情報の性質上、セキュリティインシデント発生時は即時対応が求められる。



内部職員の「過失」による事故は依然として多い

- 個人情報の漏えいに関しては、メール誤送信や紛失等、人為的ミスによる漏えいが依然として多い



JIPDEC プライバシーマーク推進センター「2022年度 個人情報の取扱いにおける事故報告集計結果」より

内部職員の「過失」による事故は依然として多い

（注１３）一般的に情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、発生した情報セキュリティインシデントを正確に把握・分析し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とするための機能を有する体制を CSIRT と呼ぶ。CSIRT の持つ機能や在り方は組織によって様々であるが、まずは、地方公共団体においては情報セキュリティに関する統一的な窓口の機能を有する体制を整えることが重要である。

※「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（令和6年10月版）」より引用

サイバー攻撃に限らず、情報セキュリティの統一的な窓口として求められる自治体「CSIRT」

CSIRT構築･運用の流れ

フェーズ１　CSIRTの設置

① 検討チームの立ち上げ

② 設置に向けた検討

③ 設置作業の実施

フェーズ２　CSIRT運用の準備

① 必要な情報の確認

② 監視連絡体制等の整備

③ 訓練の実施

必要な情報の確認　～常に最新の状態を維持するもの～

必要な情報	内容
インシデントに係る注意喚起情報	J-LISが注意喚起等の緊急連絡を掲載する「情報セキュリティ支援サイト」(LGWAN)を毎日確認する。 また、同情報を配信するLASCセキュリティ情報提供メール（J-LISからの情報提供メール）に自団体のPoCメールアドレスを登録する。
インシデントへの対応の連絡先	人事異動や組織改編、外部委託事業者や外部の専門家の変更等、必要に応じて見直し、最新の状態を保つ。
外部委託事業者への依頼内容	インシデント発生に際して、外部委託事業者（システムベンダー等）に依頼できる作業内容と責任の範囲を確認、明文化。
関連する規程類	インシデント対応に係る実施手順、団体内部及び外部機関への報告様式類等、インシデント対応時に参照、利用する可能性のある規程類が最新版か確認。
業務システム・ネットワークの構成	組織全体の業務システム・ネットワーク概要図、体制図を整備。個別のシステム構成図、ネットワーク構成図についても、常に最新化されていることを確認、把握しておく。
ログ	重要情報へのアクセス履歴、その他システムログ等の証跡が適切に取得され、保全されていることを確認する。

総務省ガイドラインは5年度連続で改定中

2020年12月（一部改定）
＝＞「クラウド・バイ・デフォルト原則」、行政手続のオンライン化、働き方改革、サイバー攻撃増加

2022年3月（一部改定）
＝＞「デジタル改革関連法」、「地方公共団体情報システムの標準化に関する法律」

2023年3月（一部改定）
＝＞ ガバメントクラウドの運用開始、情報システム標準化（先行自治体での移行）

2024年3月（中間報告）※後述

2024年10月（一部改定）※後述

※国のクラウドバイデフォルト原則に合わせて改定

クラウド活用のメリットはアジャイル開発

✖　データセンターの資源を使ってコスト削減
＝＞　ランニングコストはオンプレミス以上に掛かる
＝＞　「クラウドに預けたから保守不要」は間違い

○　俊敏にシステムを変更できることが長所
＝＞　想定以上の負荷に柔軟に対応可能
＝＞　余剰資産を抱える必要がない
＝＞　可用性と完全性を高める効果あり

令和5年度のガイドライン改定検討項目

中間報告

併せて改定

背景	検討項目
✓ デジタル社会の実現に向けた重点計画 （「三層の対策」の見直し、ゼロトラストアーキテクチャー） ✓ 地方公共団体向けサービスのクラウド化	1 β'モデル 移行のための支[illegible]策の検討 2 LGWAN接続系のロー[illegible]ブレイクアウト（α'モデル）の検討
✓ NISC政府統一基準で新たにゼロトラストアーキテクチャについて規定	3 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違い	4 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
✓ コンビニ交付サービスにおける証明書誤交付問題	5 情報システムの品質管理の推進に関する対応
✓ マイナンバー利用事務系と他の領域との画面転送に関する実施の要望	6 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

次回検討

現行の政府機関とガイドラインの機密性分類の対応関係

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**秘密文書としての取扱いを要する情報**

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（※１）**であって、「機密性３情報」以外の情報

※１　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「政府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（注）（政府クラウドサービス基本方針の適用対象）

注）政府クラウドサービス基本方針
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。

✓　前回提示した分類基準の見直しの案と国の機密性分類の対応関係は以下のとおり。

地方公共団体（本ガイドライン）

自治体機密性３

A　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

B　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**

C　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

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（※２）

※２　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

自治体機密性１

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

「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改定検討会」資料より

今般の「三層の対策」の見直し

現対策の効果や課題、新たな時代の要請を
踏まえて常に見直しを行う

✖　完璧なセキュリティ対策を考案する
＝＞　セキュリティ技術は日進月歩で変化する
＝＞　川の水も対策の低い個所から決壊する

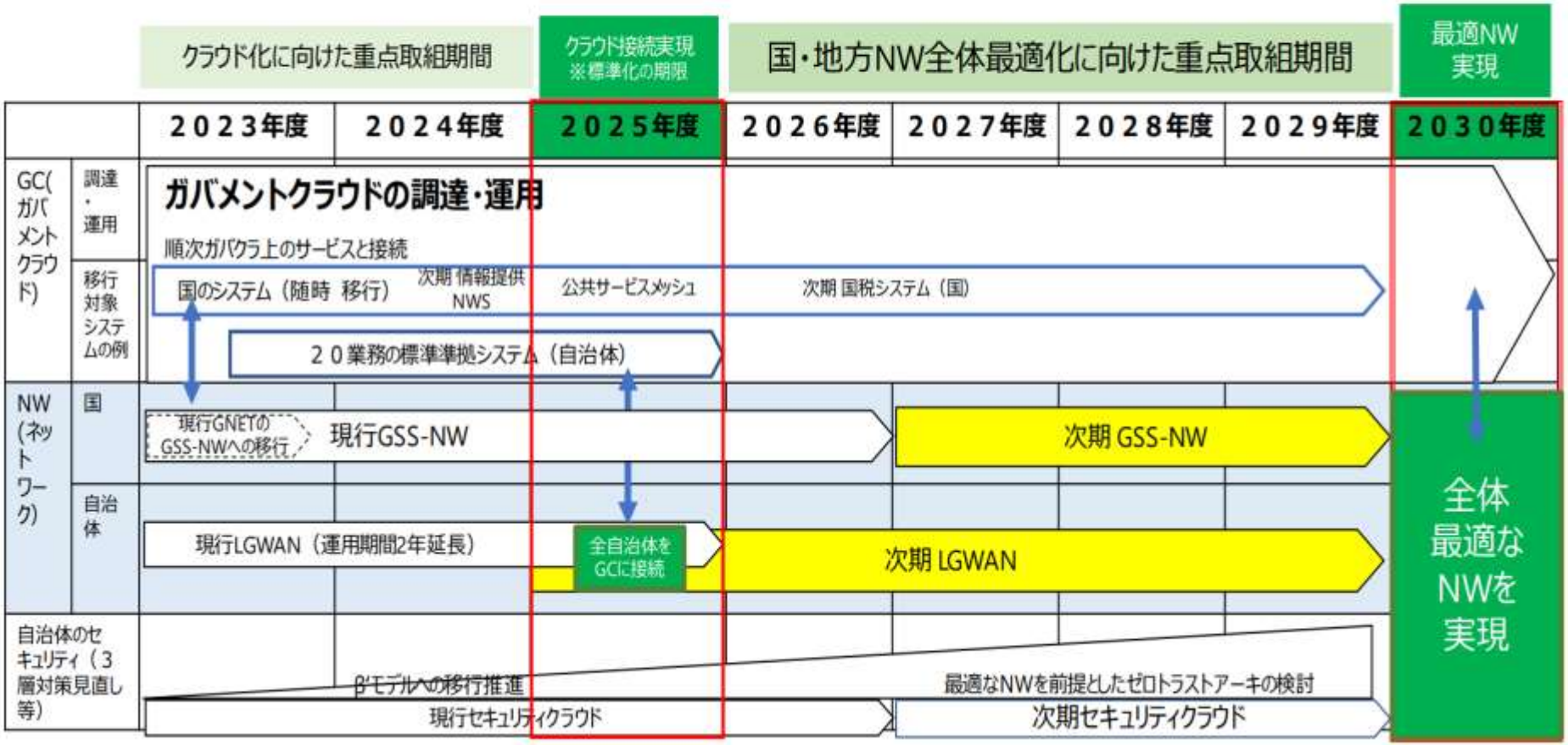
○　情報セキュリティは定期的な見直しが必要
＝＞　PDCAを回すことで、一段向上する
＝＞　見直しの際には「情報活用」も視野に入れる
＝＞　目指すのは自治体のビジョンを達成すること

デジタル庁の検討会が報告書を提出

デジタル庁検討会のスケジュール感

全体最適の観点から望ましいネットワークの将来スケジュール（２０３０頃までに想定されるスケジュール）

資料３



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

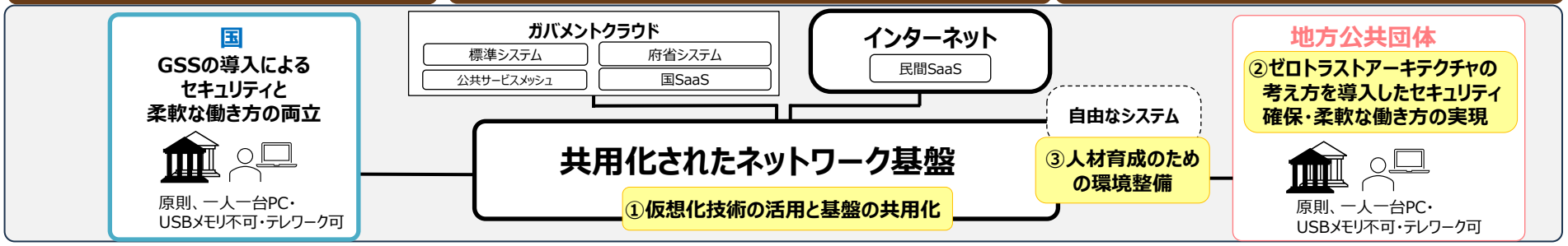
・**仮想化ネットワーク技術の活用**により、シンプルかつ柔軟なネットワークを構築

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**

デジタル庁の検討会の報告書とは

目指すべき将来像・実現イメージ（2030年頃）

２０３０年頃をターゲットとした段階的な実現イメージ

●国・自治体共通事項

（ゼロトラスト）

- 境界型防御に加え、業務システムからID管理やデバイス管理を分離させたシステム環境を整備し、適切な人が適切なデータにアクセスできるようにすることで、論理分離によるセキュリティ担保の手法で最新化することにより、セグメンテーションの概念を考慮する。これにより、情報の重要性に応じた制限のもとインターネットサービスが柔軟に利用可能になり、テレワークなど柔軟で効率的な働き方が実現する。また、職員が使用する端末の統制、ネットワークの監視、統合的なログ監視によってセキュアな環境も同時に実現可能となる。

（ネットワーク）

- 国において導入済みのゼロトラストの概念を、地方ネットワークにも導入し、国と地方でインフラの共有や冗長性の確保、相互接続可能なネットワークを実現する。
- 国・地方のネットワークが災害時に相互に乗り入れすることで、それぞれの業務継続が図られるよう連携する。

（インターネットセキュリティ）

- インターネット上のサービス利用が進み、インターネットセキュリティ対策が更に重要となることから、国と地方共通のポリシー（ネットワーク防御を拡張し、IDやデバイス等のアイデンティティ管理も行う）のもとセキュリティの機能を備えること。

（ガバメントクラウド）

- 国及び地方自治体のシステムがガバメントクラウド上に構築されて、ガバメントクラウド内のセキュアな環境でデータ連携が可能になる。
- ガバメントクラウド上に構築された公共サービスメッシュにより、標準化基準に適合している自治体は、円滑なデータ連携が可能となりデータを活用した住民サービスが実現しやすくなる。行政機関同士の情報連携についても、高い性能や低コストで安全に対応できる。

（デジタルマーケットプレイス）

- 事業者がデジタルサービスを登録するカタログサイトを設け、国及び地方自治体がそのカタログサイトから最適なサービス（SaaS）を選択できるようになる。国及び地方自治体は、迅速にSaaSを調達可能になり、よりアジャイルなソフトウェア導入が可能になる。

（新技術の積極的な導入と人材の育成）

- 2030年頃に導入可能な新技術を積極的に導入するとともに、運用体制の構築等に必要な人材を育成する。

本年6月のデジタル行財政改革会議

国・地方デジタル共通基盤の整備・運用に関する基本方針の概要

１．基本的な考え方

問題意識

急激な人口減少による担い手不足に対応するため、デジタル技術の活用による公共サービスの供給の効率化と利便性の向上が必要

目指す姿

① システムは共通化、政策は地方公共団体の創意工夫という最適化された行政

② 即時的なデータ取得により社会・経済の変化等に柔軟に対応。有事の際に状況把握等の支援を迅速に行うことができる強靱な行政

③ 規模の経済やコストの可視化及び調達の共同化を通じた負担の軽減により、国・地方を通じ、トータルコストが最小化された行政

【タテの改革】
各府省庁による所管分野の国・地方を通じたBPRとデジタル原則の徹底

【ヨコの改革】
DPIの整備・利活用と共通SaaS利用の推進

２．取組の方向性

共通化すべき業務・システムの基準

① 国民・住民のニーズ（利用者起点）に即しているか
② 効果の見込みがあるか
③ 実現可能性があるか

共通化は、国と地方の協力の枠組みの下で進め、原則として地方に義務付けを行うものでなく、地方の主体的な判断により行われるもの。

(a)喫緊の課題である20業務の標準化に引き続き注力し、(b)基準に合致するものは共通化を進め、(c)基準に合致しないものであっても都道府県の共同調達による横展開の推進等に取り組む

費用負担の基本的考え方

ⅰ）共通SaaS
- 国が共通化に関する調査、初期段階における実証、標準的な仕様書の作成等に要する費用を負担
- 地方公共団体が利用料等を負担することが原則

ⅱ）デジタル公共インフラ（DPI）
※認証基盤（マイナンバーカード等）、ベース・レジストリ等
国が主導して開発・運用・保守を行うことが適当

ⅲ）物理／仮想基盤（クラウド、ネットワーク）
- 原則として費用は整備主体が負担
- 利用者は、運用・保守費用等について応分の負担

デジタル人材の確保

ⅰ）共通SaaS・DPIの整備・活用のための体制の強化
デジタル庁を中心に、専門人材の確保や、各省と地方公共団体との調整を行う行政人材の配置を推進

ⅱ）地方公共団体における人材確保
- 令和７年度中に、全ての都道府県で都道府県を中心に市町村と連携した地域DX推進体制を構築し、人材プール機能を確保
- 総務省において、都道府県間の連携も促進しながら、デジタル庁と連携し、支援を強化

自治体情報セキュリティで大事なこと

情報のデジタル化はセキュリティレベル向上

報道がなされている事件・事故はアナログ
＝＞　多くが人為的ミスか紙・媒体での情報漏えい

情報をデジタル化することで、対策が増える
＝＞　誰が、いつ、どこから情報を見たのかが判明
＝＞　暗号化・パスワードなど複数の方法で守れる
（許された者だけが情報にアクセス）

本人の情報は本人が確認できる（守れる）

自治体DX推進と情報セキュリティ

DXを進めることで、セキュリティレベルを上げる

○　業務改革と情報セキュリティはセット
＝＞　セキュリティ事故、事件を防ぐため手法を変える
＝＞　複数の人間がチェックする体制は限界に

○　人でなくても出来ることをDXで実現する
＝＞　人間が介在することでミスは発生する
＝＞　AIやRPAを利用して極力人の介在を減らす
＝＞　そもそも作業が必要か、自動化することが大事

シャドーITをなくすことも自治体DXの肝

ご清聴ありがとうございました。
ご参考になれば幸いです。

合同会社KUコンサルティング
髙橋邦夫