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

令和８年度

自治行政局 住民制度課

サイバーセキュリティ対策室

本資料の位置づけ

- 本資料は地方公共団体の情報政策部門に新たに着任された方や異動されてきた方が、情報セキュリティの基本を理解するために、最初に確認することを想定して作成しています。

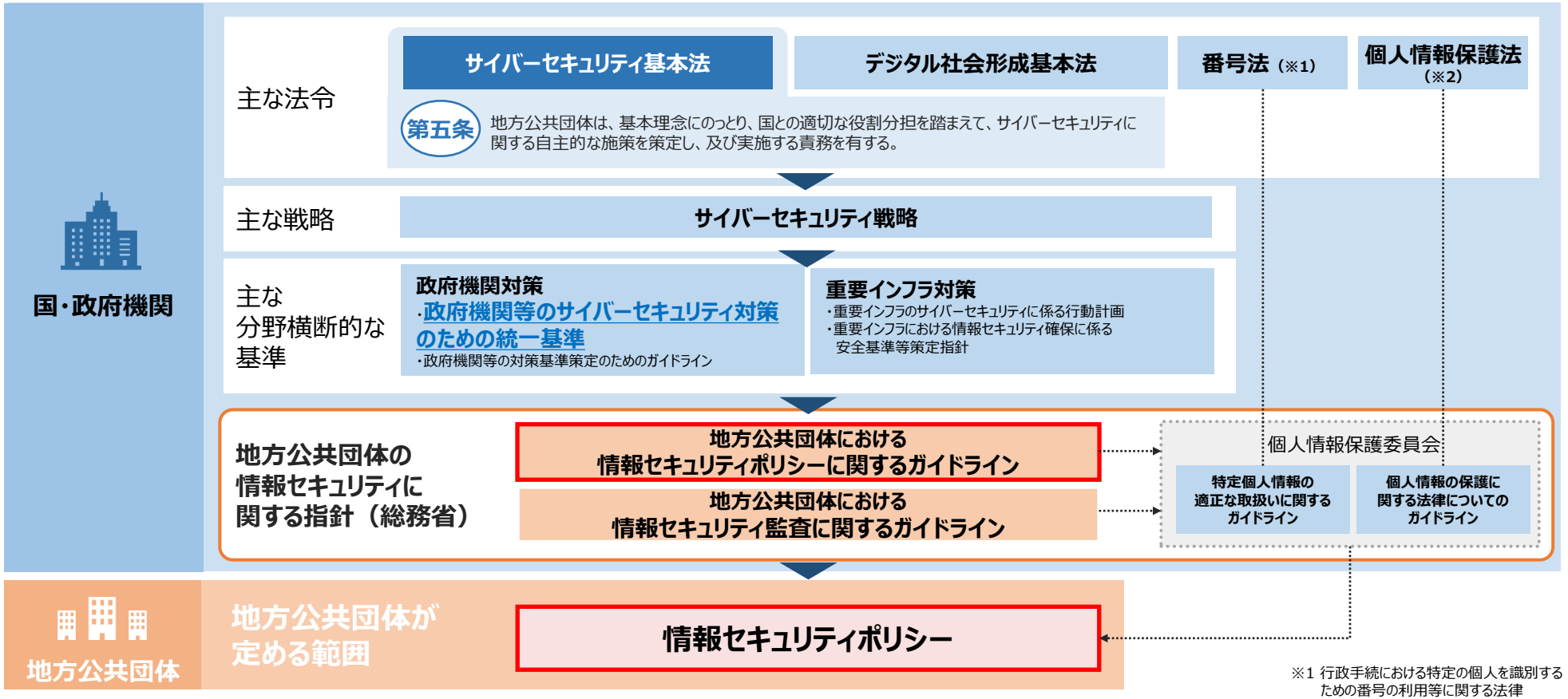
- これにより、「地方公共団体における情報セキュリティポリシーに関するガイドライン」（以下「総務省セキュリティポリシーガイドライン」という。）の内容を効率的に理解し、また、地方公共団体における研修資料等としても活用することで、職員等の理解や情報セキュリティの意識の向上に寄与しようとするものです。

- なお、本資料は「総務省セキュリティポリシーガイドライン」の概要を理解するためのものであるため、詳細は本文を参照してください。また、各地方公共団体が定めた情報セキュリティポリシーを確認した上で、情報セキュリティを維持するための行動をとるようお願いします。

ガイドラインの概要

サイバーセキュリティに関する国と地方の関係

- サイバーセキュリティ基本法の枠組みの中で、「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」（以下「政府統一基準」という。）において国・政府機関に必要なセキュリティ対策を規定することとされている。
- 国・政府機関と整合性のとれたセキュリティ対策を地方公共団体にも提示する必要があることから、政府統一基準の改定内容を、総務省**「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」**に反映させている。

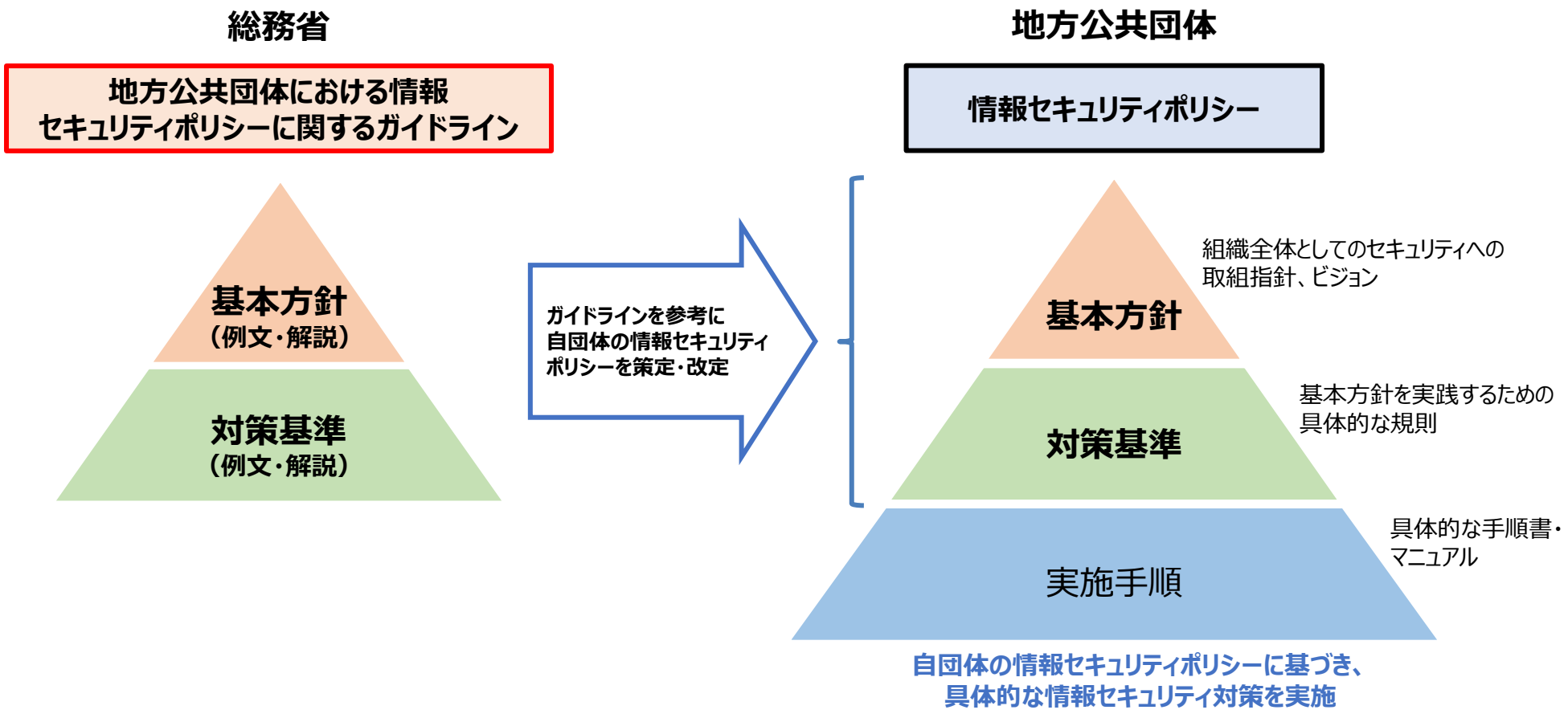


※1 行政手続における特定の個人を識別するための番号の利用等に関する法律

※2 個人情報の保護に関する法律

「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」について

■ 「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」（以下「ガイドライン」という。）は各地方公共団体のセキュリティ対策の指針として総務省が策定し助言。国における情報セキュリティ対策の動向やデジタル化の動向等を踏まえながら、**有識者検討会（学識経験者、自治体職員、システム調達契約や個人情報保護法に知見を有する弁護士が構成員となっている検討会）での議論を経て、年度ごとに改定を実施**。



※ 改正地方自治法に規定されている総務大臣の指針や各地方公共団体の方針は、上図の基本方針に相当

ガイドラインの構成

- 地方公共団体が情報セキュリティポリシー（基本方針・対策基準）を策定、改定する際に、「第2編」の例文を参照し、活用することが可能な構成となっている。
- 基本方針・対策基準の例文の詳細な解説は、「第2編」の例文の構成と対応した内容で「第3編」に記載。
- クラウドサービス上で業務システムを利用する場合には、クラウドサービスの特性を踏まえた情報セキュリティ対策を考慮する必要があることから、「第4編」を特則として定めている。

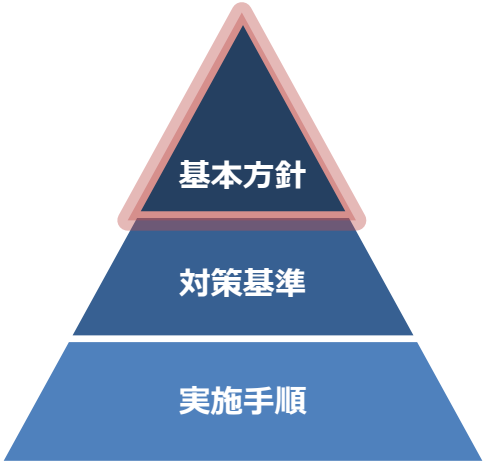
編	項目	本編の主な内容	補足
第１編	総則	• ガイドラインの目的 • 地方公共団体における情報セキュリティとその対策 • 情報セキュリティ管理プロセス • 本ガイドラインの構成 • 対策レベルの設定 • クラウドサービスに関する留意点	• 情報セキュリティポリシーを策定するための前提となる事項を記載。 • 情報セキュリティポリシーの策定や改定のプロセス、クラウドサービスの留意点等を記載。
第２編	地方公共団体における情報セキュリティポリシー（例文）	• 情報セキュリティ基本方針（例文） • 情報セキュリティ対策基準（例文）	• 地方公共団体の基本方針、対策基準に定める文案の参考として、例文を記載。
第３編	地方公共団体における情報セキュリティポリシー（解説）	• 情報セキュリティ基本方針（解説） • 情報セキュリティ対策基準（解説）	• 第２編の例文と同様の構成で、具体的なセキュリティ対策の考え方を記載。
第４編	地方公共団体の情報システムのクラウド利用等に関する特則（例文・解説）	• 本編の目的 • 本編におけるクラウドサービスの範囲 • 本編における対策基準の構成 • 情報セキュリティ対策	• 標準準拠システム等のクラウド利用を行う場合に必要となる情報セキュリティ対策（対策基準）を、本編と同様の構成で例文と解説の形式で記載。
第５編	付録	• 権限・責任等一覧表	• 総務省セキュリティポリシーガイドラインで求められる役割を一覧で記載。

○「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８年３月27日改定）計422頁
https://www.soumu.go.jp/main_content/001064410.pdf

基本方針

- サイバーセキュリティを確保するための方針の策定及びこれに基づく措置の実施が義務付けられ（地方自治法第244条の6第1項）、方針の策定又は変更について、総務大臣が指針を示すこととされた（同条第3項）。
- 大臣指針の地方公共団体が策定する方針の内容に関する箇所においては、「ガイドラインにおいて、基本方針の策定例及び解説を示しているところであり、ガイドラインを十分に参照し、各執行機関等におけるネットワーク構成等の個別の事情に即して方針（基本方針）を策定することが重要である。」と示されている。
- **基本方針**は、地方公共団体が情報セキュリティ対策の**基本的な考え方を示す**もの。全ての情報システムに共通する**具体的な情報セキュリティに関する対策**は、基本方針の各項の内容を踏まえて**対策基準**に定める。

基本方針の主な規定内容は右の表のとおり



項目	主な規定内容
1. 目的	地方公共団体が実施する情報セキュリティ対策について基本的な事項を策定
2. 定義	基本方針で使用する文言の定義
3. 対象とする脅威	不正アクセス、サイバー攻撃、委託先管理の不備等の脅威を例示
4. 適用範囲	基本方針を適用する部局、対象の情報資産
5. 職員等の遵守義務	情報セキュリティの重要性について認識、ポリシーを遵守
6. 情報セキュリティ対策	脅威から情報資産を保護するための対策
7. 情報セキュリティ監査及び自己点検の実施	情報セキュリティポリシーの遵守状況を検証するための監査及び自己点検の実施
8. 情報セキュリティポリシーの見直し	情報セキュリティの新たに対策が必要になった場合の情報セキュリティポリシーの見直しの必要性
9. 情報セキュリティ対策基準の策定	基本方針に基づく具体的な遵守事項及び判断基準等を策定
10. 情報セキュリティ実施手順の策定	対策基準に基づく具体的な手順等を策定

■ 情報セキュリティ対策基準の構成

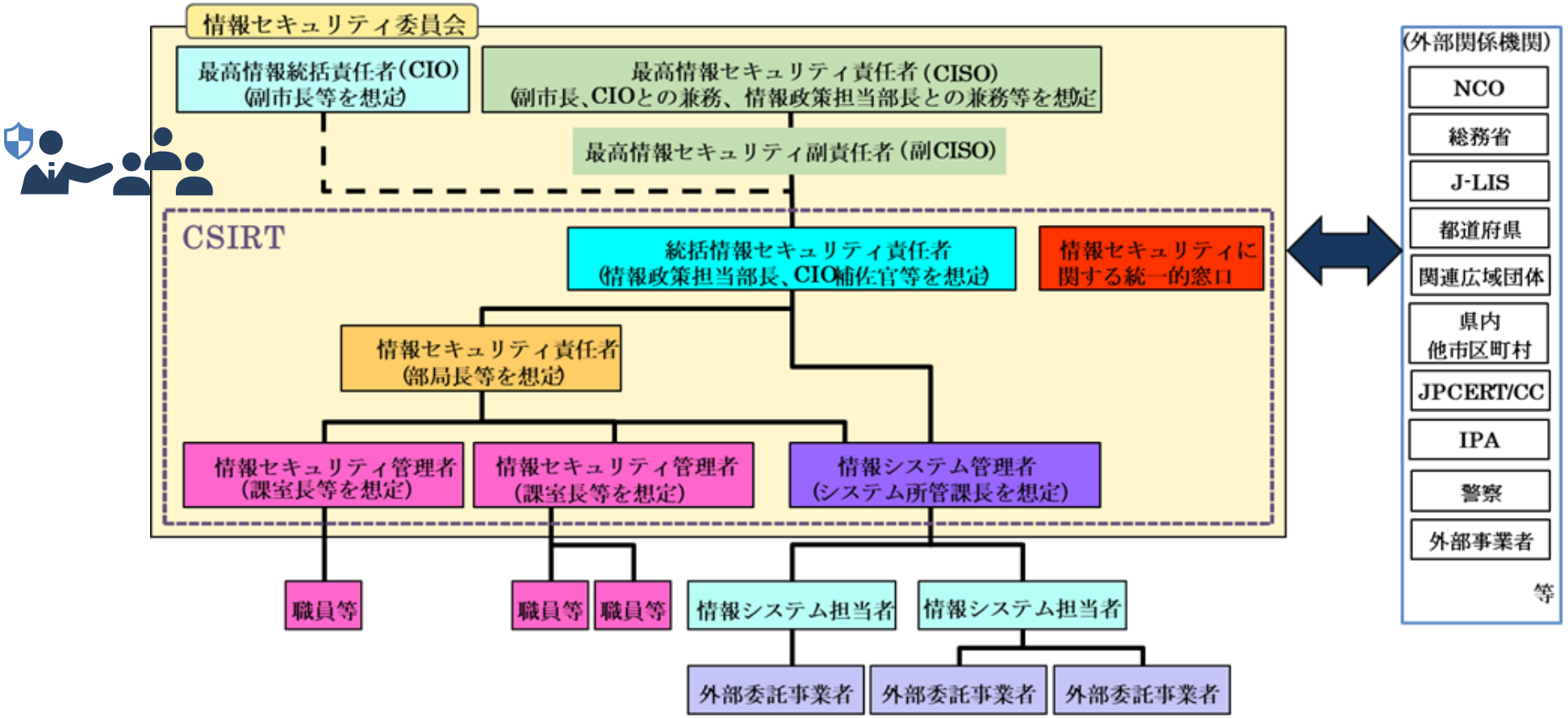
1. 組織体制
2. 情報資産の分類と管理
3. 情報システム全体の強靭性の向上
4. 物理的セキュリティ
5. 人的セキュリティ
6. 技術的セキュリティ
7. 運用
8. 業務委託と外部サービス（クラウドサービス）の利用
9. 評価・見直し

セキュリティを維持するためには、対策基準１から９まで実施することを求めている

1. 組織体制

「第3編 第2章 情報セキュリティ対策基準（解説）1. 組織体制」を参照

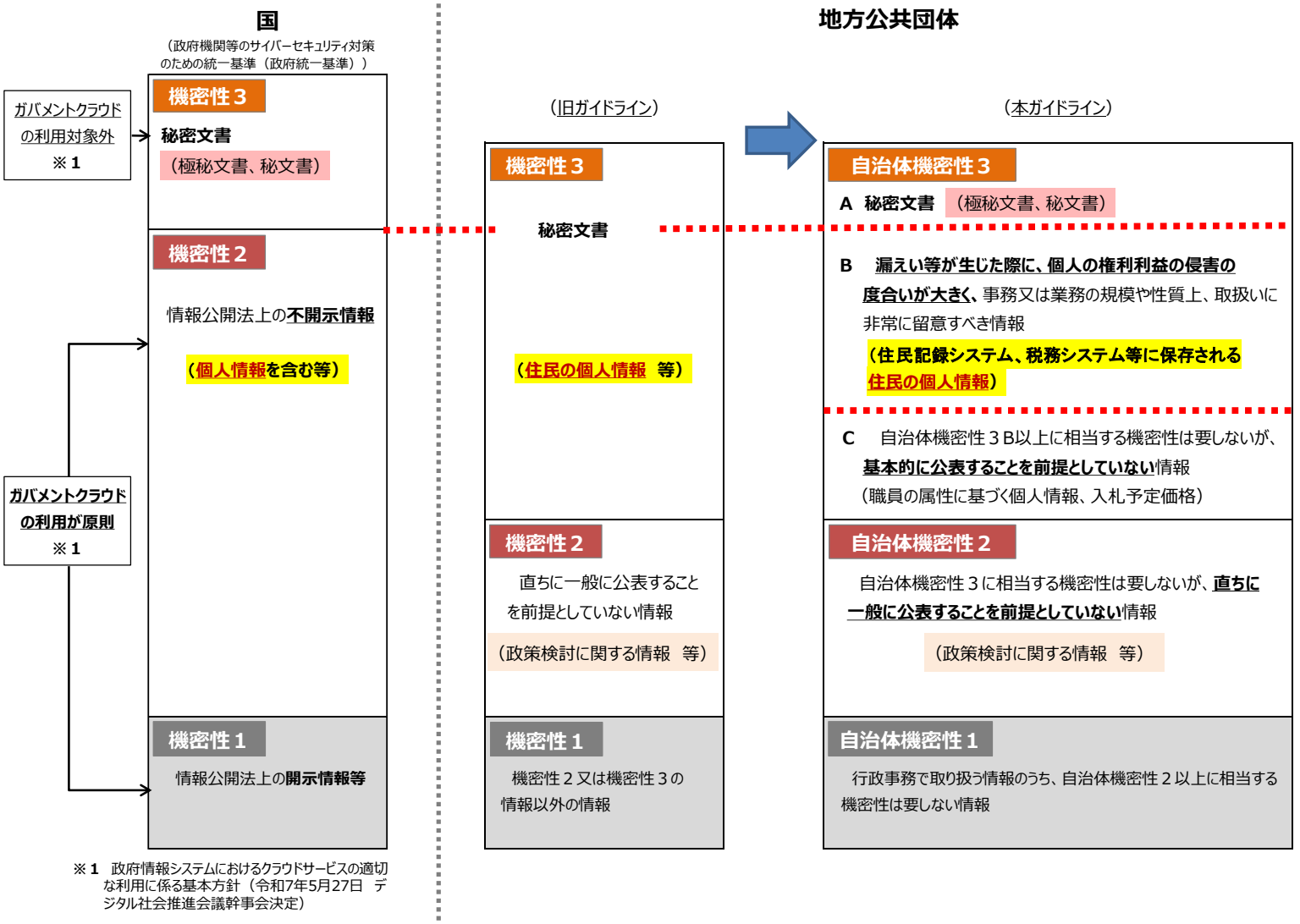
- 組織として、情報セキュリティ対策を確実に実施するには、情報セキュリティ対策に取り組む十分な組織体制を整備し、一元的に情報セキュリティ対策を実施する必要がある。
- 最高情報セキュリティ責任者（CISO）は、**情報セキュリティインシデントに対処するための体制（CSIRT）を整備**し、役割を明確化する必要がある。



2. 情報資産の分類と管理

「第3編 第2章 情報セキュリティ対策基準（解説）2. 情報資産の分類と管理」を参照

■ 機密性・完全性・可用性に基づく情報資産の分類と分類に応じた取扱いを定めた上で、情報資産の管理責任を明確にし、情報資産のライフサイクルに応じて取るべき管理方法を規定。



3. 情報システム全体の強靭性の向上

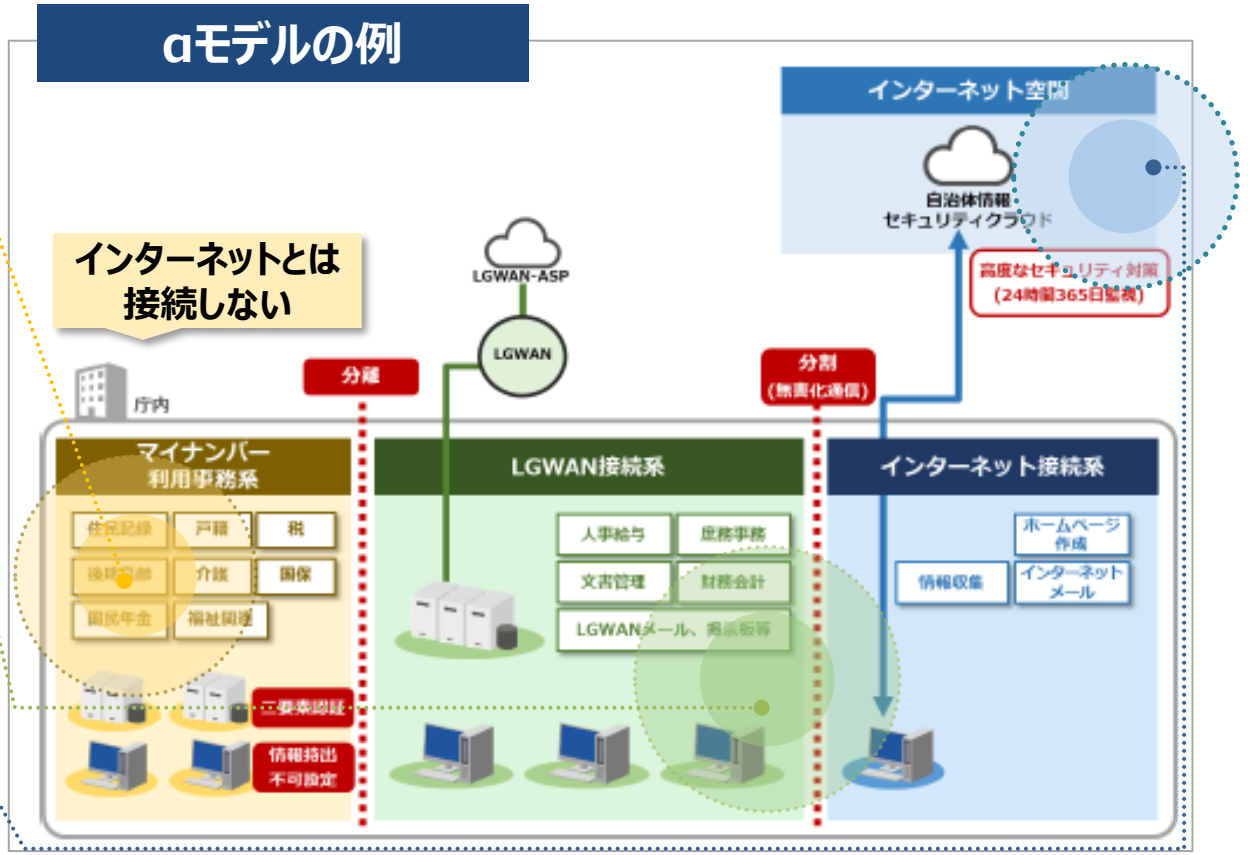
「第3編 第2章 情報セキュリティ対策基準（解説）3. 情報システム全体の強靭性の向上」を参照

- 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。
- 情報システム全体の強靭性の向上は、「三層対策」により実現。

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

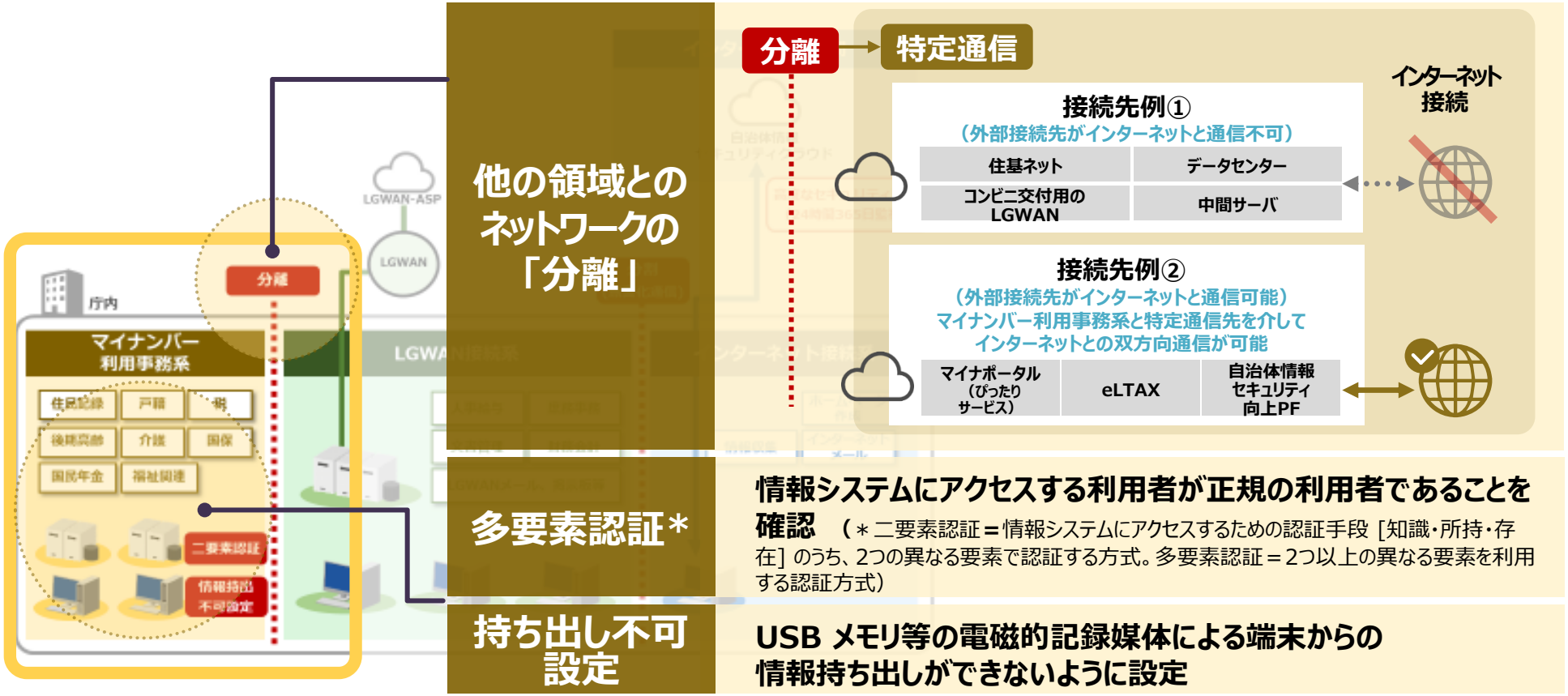
2 LGWAN接続系とインターネット接続系を分割し、LGWAN環境のセキュリティを確保

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



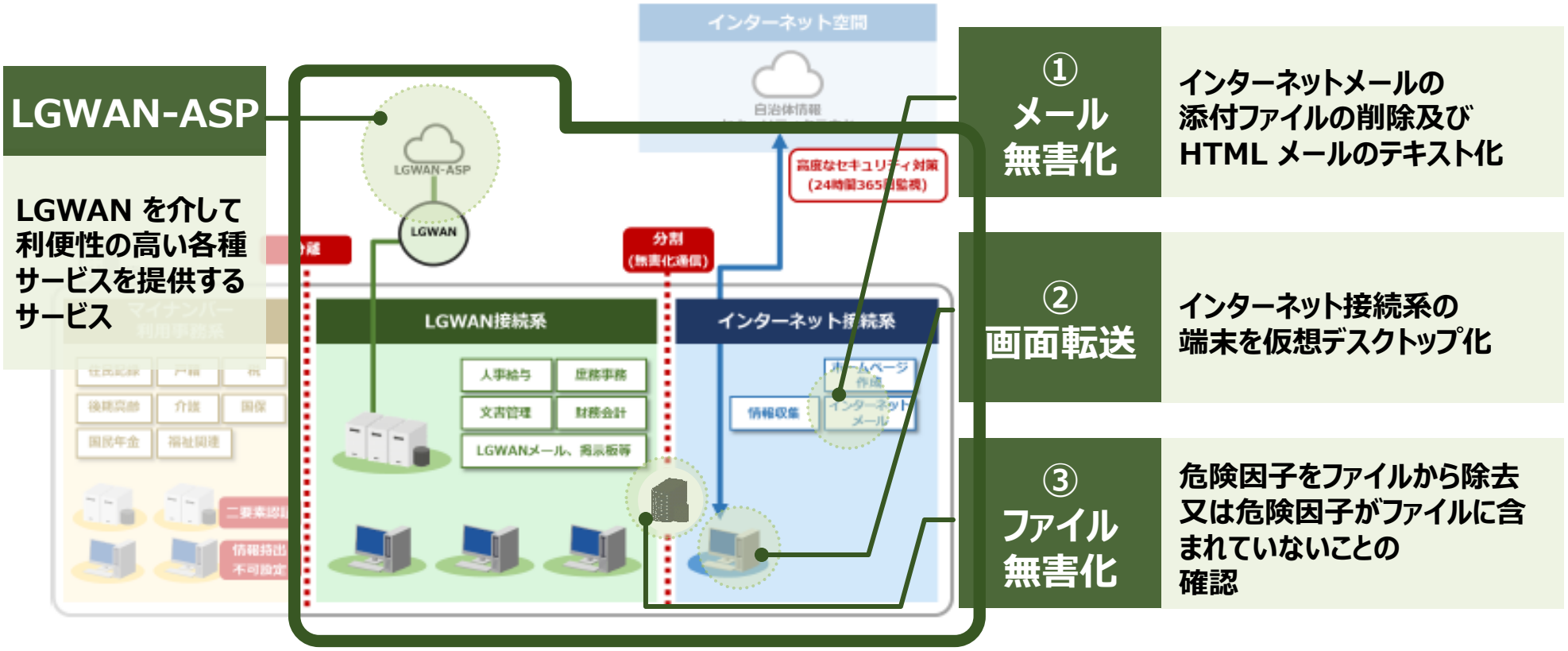
マイナンバー利用事務系

住民情報の流出を防ぐ必要があることから、他の領域（LGWAN接続系及びインターネット接続系）との通信をできないようにする必要があります。マイナンバー利用事務系と外部接続先の通信が必要な場合は、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）のレベルでの限定を行う必要があり、これらの通信を「**特定通信**」と定義。

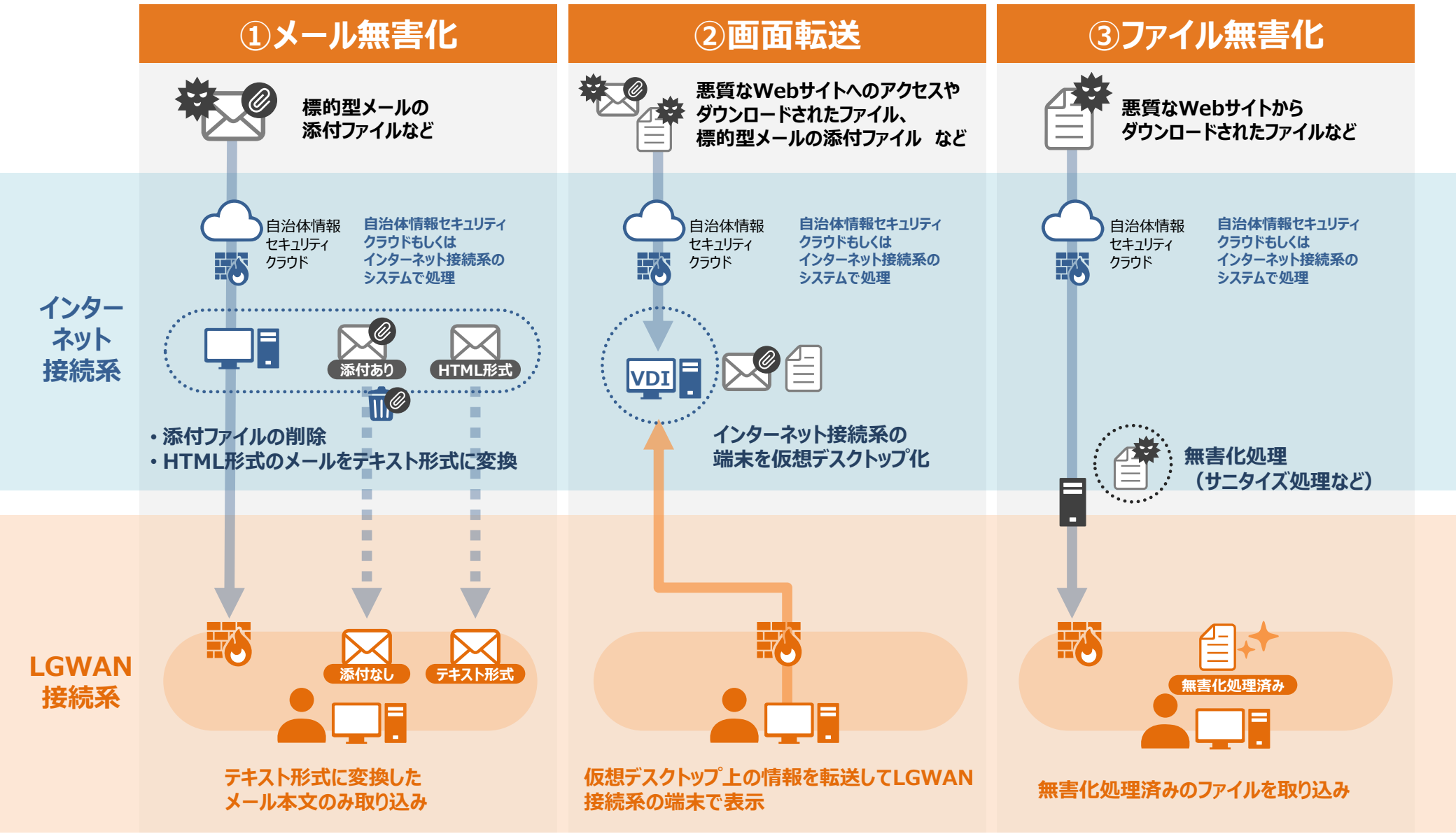


LGWAN接続系

- 一旦両環境間の通信環境を分離した上で、必要な通信だけを許可することを「分割」と呼ぶ。
- 「分割」した上でインターネット接続系と通信する場合は、「**無害化通信**」を実施する。「無害化通信」には、３つの方式が定められている。
  - インターネット環境で受信したインターネットメールの本文のみをLGWAN接続系に転送するメールテキスト化方式（メール無害化）
  - インターネット接続系の端末から、LGWAN 接続系の端末へ画面を転送する方式（画面転送）
  - 危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式（ファイル無害化）

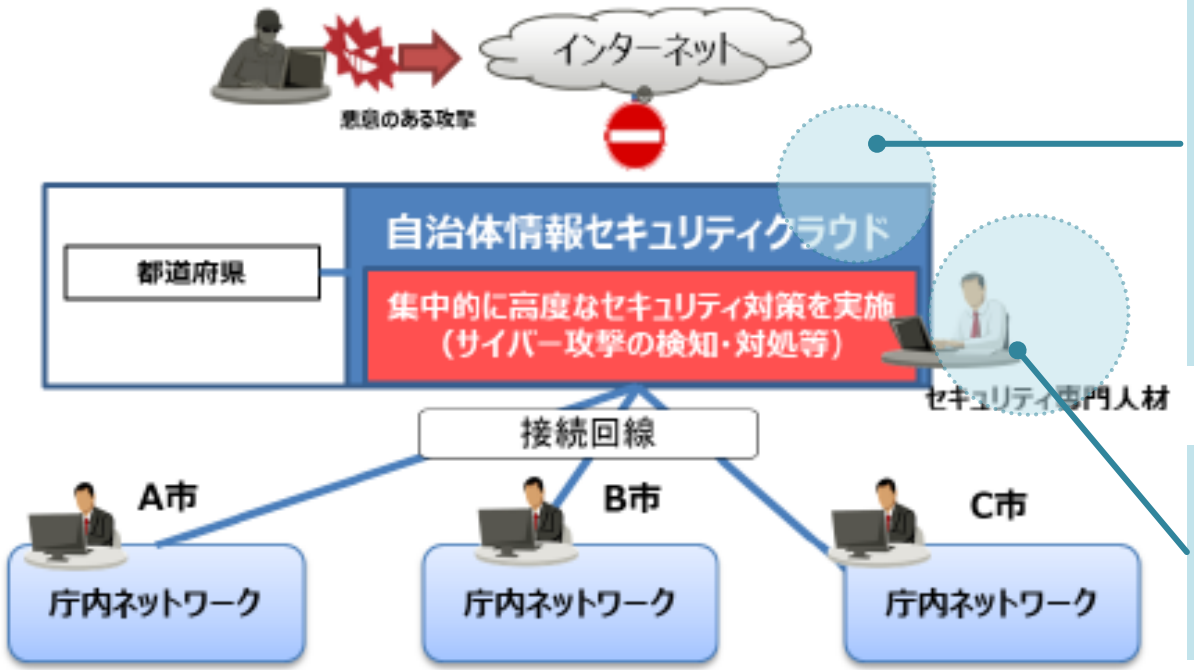


無害化通信の3つの方式



インターネット接続系

- インターネットからの脅威に対応するために、情報セキュリティインシデントの早期発見と対処及びLGWAN への不適切なアクセスの監視等の情報セキュリティ対策を講じる必要がある。
- 都道府県及び市区町村のインターネットとの通信を集約する「**自治体情報セキュリティクラウド**」に参加し、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進する。



通信パケットの監視及び破棄、通信ポートの制御、不正なプログラムの検知、不審なメールの検知及び遮断、不審なURL へのアクセス遮断、ログ監視、コンテンツの改ざん検知等の機能を持った高度な情報セキュリティ対策機能を持つ

情報セキュリティ専門人材による高水準なセキュリティ運用監視

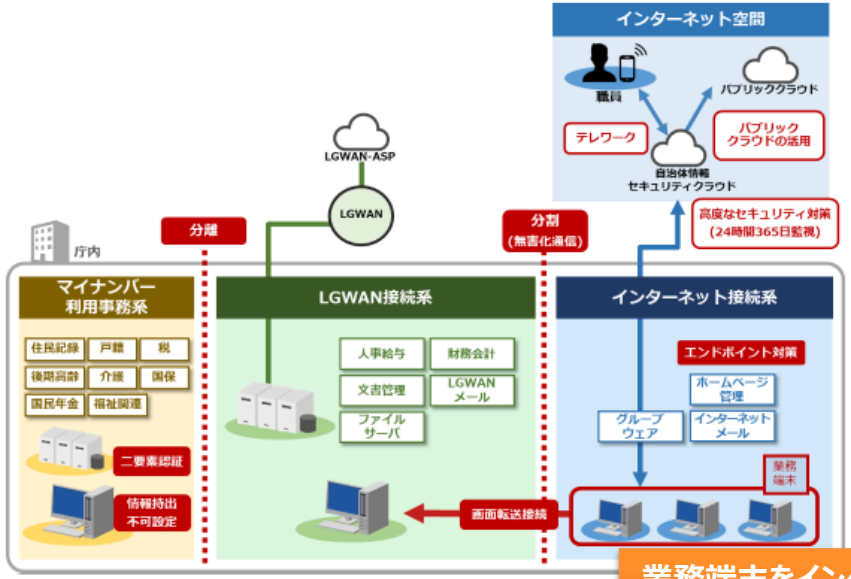
βモデルとβ′モデル

■ 令和2年度ガイドライン改定により、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



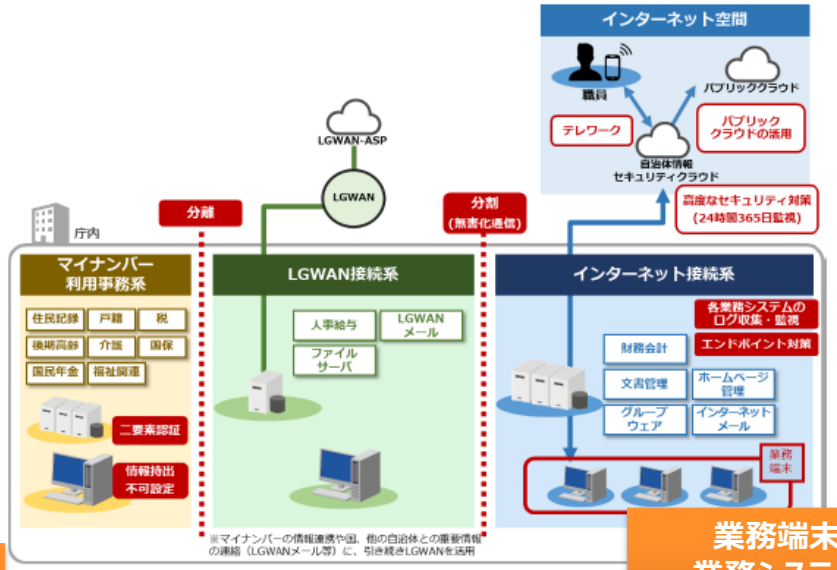
βモデルイメージ図

業務端末をインターネット接続系に配置

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、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



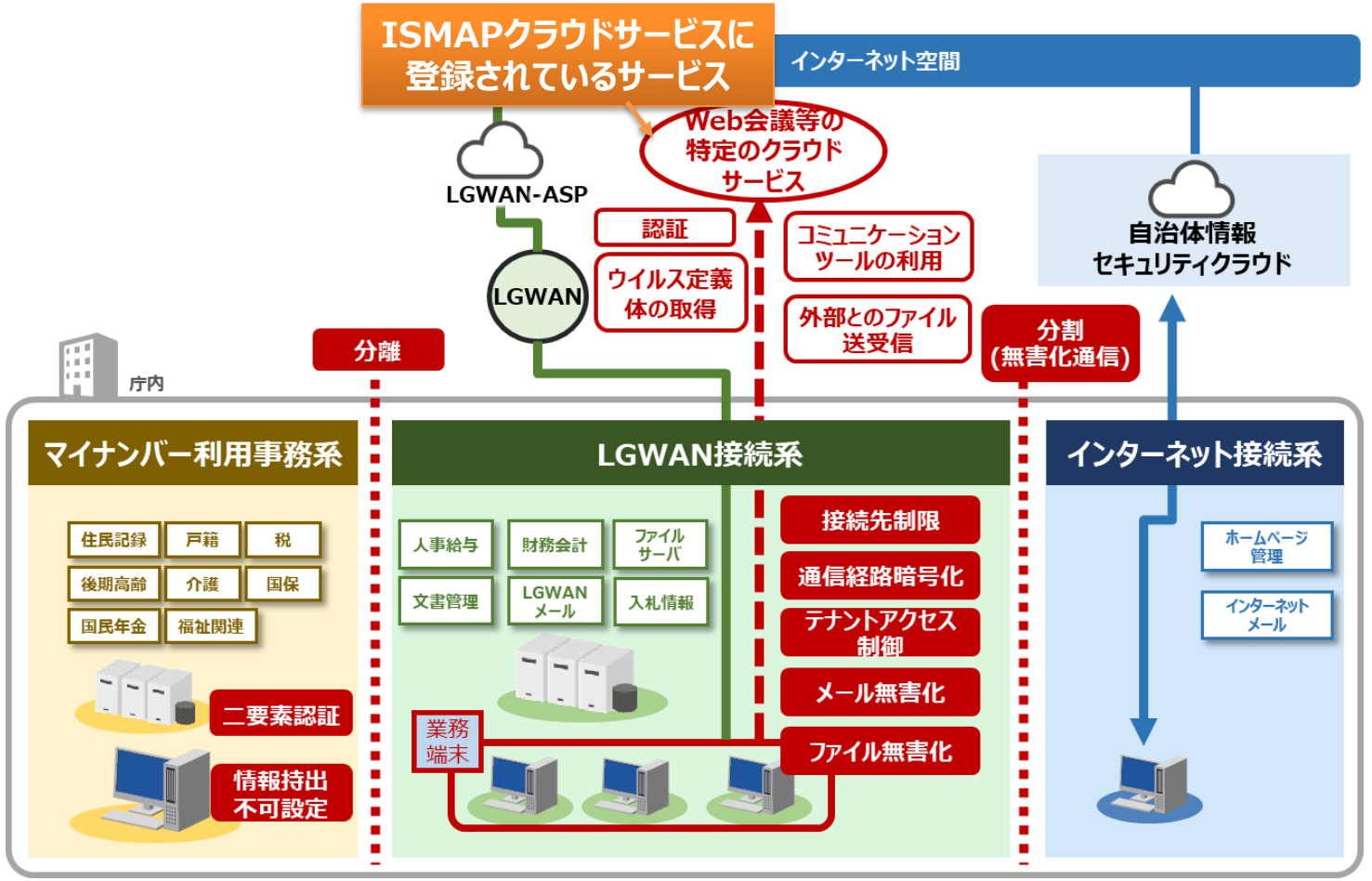
β′モデルイメージ図

業務端末と業務システムをインターネット接続系に配置

LGWAN接続系からのローカルブレイクアウト（α'モデル）

■ 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モデルの状態であり、インターネットに接続しWeb会議等の特定のクラウドサービスを利用する必要が生じている。

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（令和6年10月改定で追加）



4. 物理的セキュリティ

「第3編 第2章 情報セキュリティ対策基準（解説）4. 物理的セキュリティ」を参照

- サーバ等のハードウェアや通信回線・装置の管理が不十分な場合、情報システム全体への悪影響や業務継続への支障が生じるおそれがあるため、設置・保守・廃棄を含む物理的セキュリティ対策を規定。
- 情報システム室の重要設備や職員が利用する端末・記録媒体についても、盗難や紛失、情報漏えいを防止するため、入退室管理や機器の搬入出、持ち出し・持ち込みに関するルールを規定。

情報の機密性に応じた機器の廃棄等の方法（図表41 抜粋）

分類	抹消方法	廃棄等の方法	
(1) マイナンバー利用事務系の領域において住民情報を保存する記録媒体 ※マイナンバー利用事務系：社会保障、地方税、防災、戸籍事務等に関する情報システム及びデータ **(2) 自治体機密性２以上に該当する情報を保存する記録媒体** （上記(1) に該当するものを除く。） **記録媒体がHDD･SSDの場合は、破壊か除去か抹消方法の選択が可能**	**破壊** **リユース不可**	HDD	当該媒体を**細断、変形するなど**して情報を記録している内部の円盤を物理的に破壊する必要がある。HDDの場合、筐体に対して不適当なサイズの円盤を組み込んでいるものが存在しており、**穿孔**する際は、円盤を確実に損傷するため多点方式で最下層の円盤まで損傷を与えることができる**専用破壊装置を利用**する必要がある。
		SSD	当該媒体を**切断するなど**して情報を記録している**内部のメモリチップを破壊**する方法が例として挙げられる。HDD向けの一般的な物理的破壊方法では、裁断の細かさ等の点からフラッシュメモリ媒体を完全には破壊できないため、**専用の破壊装置を使用**し、メモリチップを破壊する必要がある。
		USBメモリ	
		光学媒体	• **メディアシュレッダー**や**メディアクラッシャー**等の機器にて記録層を破壊
	除去 **リユース可** **(消磁の場合はリユース不可の場合あり)**	HDD	• **暗号化消去** • ATA コマンドの「**SECURITY ERASE UNIT**」コマンドを「**Enhanced Erase mode**」で使用 • SCSIコマンドの「**SCSI SANITIZE**」コマンドや「**SCSI Format**」コマンドを使用 • **消磁**
		SSD	• **暗号化消去** • ATA コマンドの「**BLOCK ERASE**」コマンドを使用 • SCSIコマンドの「**SCSI SANITIZE**」コマンドや「**SCSI Format**」コマンドを使用 • NVMe（PCIe）コマンドの「**NVM Express Format**」コマンドや「**NVM Express SANITIZE**」コマンドを使用

5. 人的セキュリティ

「第3編 第2章 情報セキュリティ対策基準（解説）5. 人的セキュリティ」を参照

- 職員等による情報資産の不正利用や不適切な取扱いは、ウイルス感染や情報漏えいなどの重大な被害につながるおそれがあるため、情報セキュリティポリシーの遵守、業務外利用の禁止、ID・パスワードや認証情報等の適正管理など、遵守すべきルールを明確に定める必要がある。
- 対策の実効性を確保するには、幹部を含む全職員がその重要性や最新の脅威を理解することが不可欠である。あわせて、インシデント発生時に迅速な報告を行い、被害拡大防止と早期復旧を図るための報告義務を規定。

職員の遵守事項

- 情報セキュリティポリシー等の遵守
- 業務以外での目的での使用の禁止
- モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限
- 支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用
- 持ち出し及び持ち込みの記録
- パソコンやモバイル端末におけるセキュリティ設定変更の禁止
- 机上の端末等の管理
- 退職時等の遵守事項

定期的な研修・訓練
セキュリティ意識向上

研修計画の立案及び実施

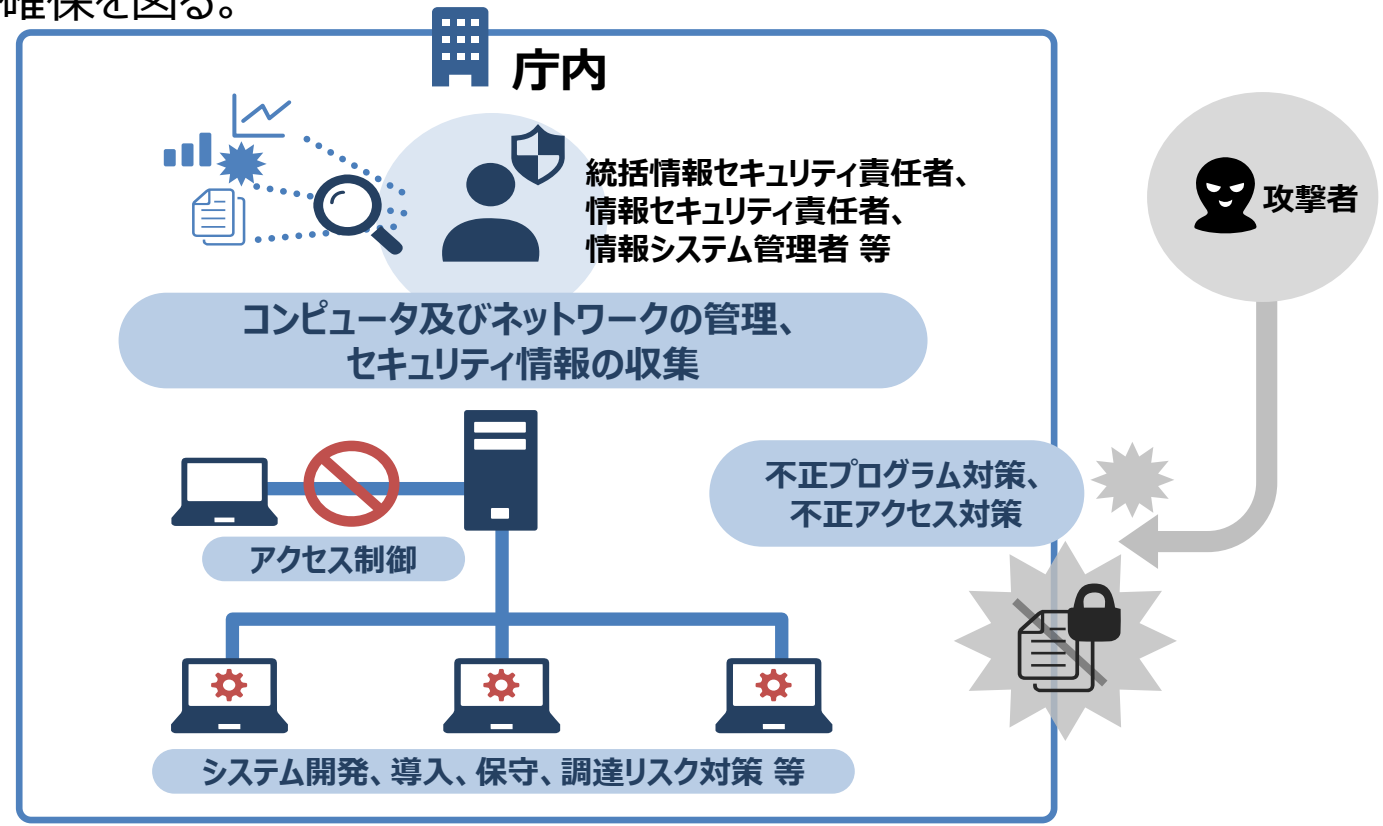
緊急時対応訓練

（CIDER　実践的サイバー防御演習）
（インシデント発生時CSIRT対応訓練支援）

6. 技術的セキュリティ

「第3編 第2章 情報セキュリティ対策基準（解説）6. 技術的セキュリティ」を参照

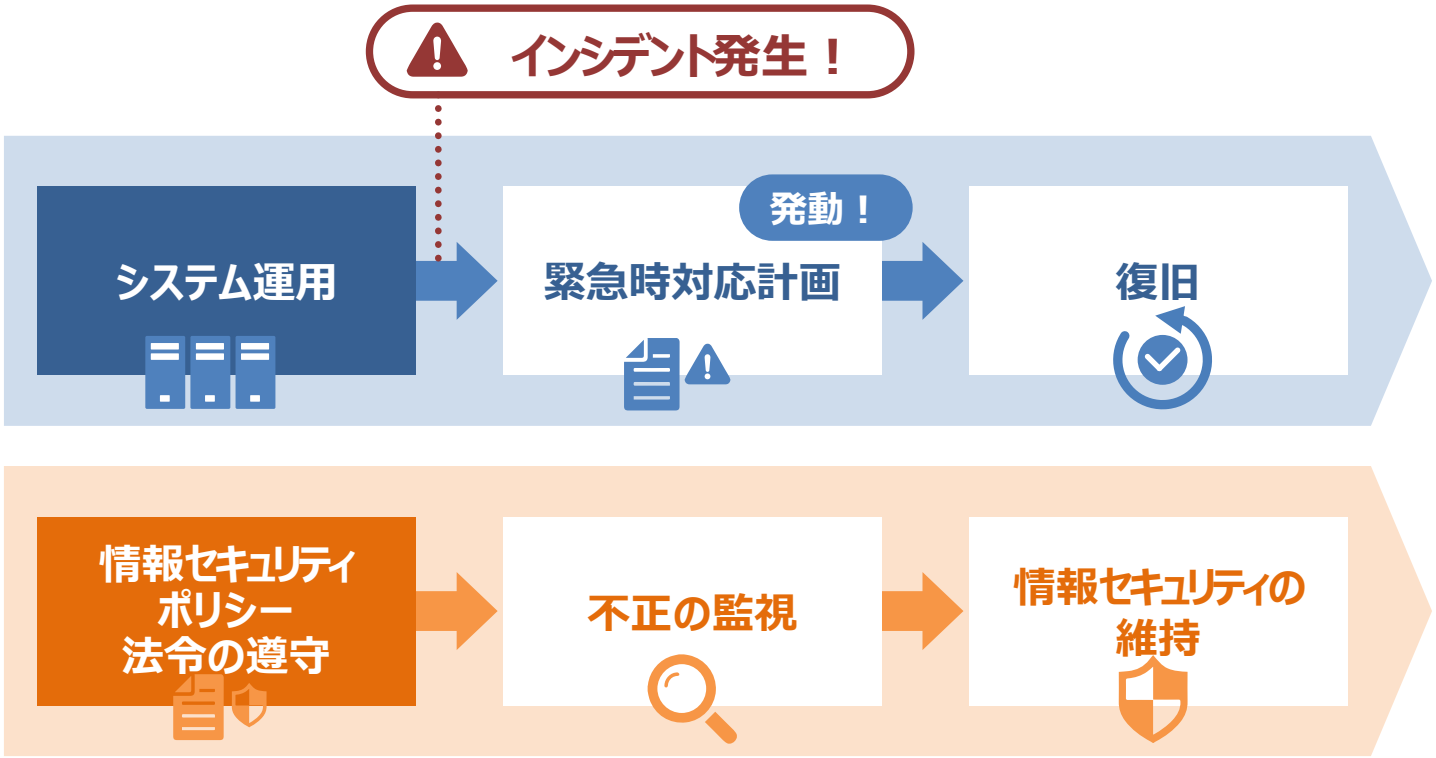
- ネットワークや情報システムの管理が不十分な場合、サイバー攻撃や不正利用による情報漏えいなどの重大な被害が生じるおそれがある。このため、ログ管理やバックアップ、無許可ソフトウェアの使用禁止、構成変更の制限などの技術的対策と、権限に応じたアクセス制御を規定する。
- 開発・導入・保守の各段階で適切な対策（調達リスク対策等）を講じることにより、脆弱性や不正プログラム、不正アクセスへの対応を徹底し、攻撃時の対応手順や情報共有を含め、継続的な情報セキュリティの確保を図る。



7. 運用

「第3編 第2章 情報セキュリティ対策基準（解説）7. 運用」を参照

- 情報システムへの攻撃や不正利用、内部不正を防止するため、ネットワーク監視等により稼働状況を常時把握するとともに、情報セキュリティポリシーの遵守状況を確認し、問題発生時の対応を明確に定める。
- インシデントや障害、ポリシー違反が発生した際に備え、被害拡大防止と迅速な復旧を目的とした緊急時対応計画を策定する。加えて、例外措置や関係法令、懲戒処分の規定を整備し、法令・規定遵守の徹底と違反防止を図る。



8. 業務委託と外部サービス（クラウドサービス）の利用

「第3編 第2章 情報セキュリティ対策基準（解説）8. 業務委託と外部サービス（クラウドサービス）の利用」を参照

- 情報システムやアプリケーションの開発・運用・保守を外部事業者に委託する場合、委託先のセキュリティ対策を直接管理できないため、所定の基準に適合した対策を確実に実施させるよう、要求事項を調達仕様書等に明記し、契約条件とする必要がある。
- 委託事業者による意図しないシステム変更や、開発・運用・保守の各段階での脆弱性混入を防止するため、委託業務特有の対策も契約上明確化する。
- クラウドサービスの利用に際しては、基盤を含む情報流通全体を考慮した総合的なセキュリティ対策を講じる。

業務委託

- 業務委託する場合は、委託する業務の範囲や、委託先の責任範囲等を明確化し、契約を締結。
- 「外部委託先に関するセキュリティ要件のチェックシート」に基づいて委託先事業者のセキュリティ要件の遵守状況を確認。

外部サービス（クラウド）の利用

- **自治体機密性2以上の情報を取り扱う場合**
  クラウドサービスの利用にあたっては、自組織のガバナンスやセキュリティ確保を十分に考慮し、クラウドサービス提供者との役割・責任分担を明確にした上で、選定基準やセキュリティ要件を満たしていることを確認する必要がある。一方、不特定多数向けに画一的な規約のみで提供され、個別のセキュリティ対応やデータ取扱いを求められないクラウドサービスについては、自治体機密性2以上の情報に必要なセキュリティ要件を満たすことが一般に困難であるため、原則として当該情報を取り扱うことはできない。
- **自治体機密性2以上の情報を取り扱わない場合**
  自治体機密性2以上の情報を取り扱わない場合であっても、約款その他の提供条件等から、利用に当たってのリスクが許容できることを確認する。

9. 評価・見直し

「第3編 第2章 情報セキュリティ対策基準（解説）9. 評価・見直し」を参照

- 情報セキュリティポリシーの実施状況を確認するため、専門的かつ客観的な監査を行うことが重要であり、その体制や方法を明確に規定する必要がある。
- 自己点検・評価は職員の意識向上や改善点の把握に有効であり、監査結果とあわせて活用することで、脅威や技術の変化に対応したポリシーや関連規程の定期的な見直しにつなげる。

監査

- 被監査部門から独立した監査人が公平な立場で客観的に監査。
- 情報システムの運用や保守を業務委託している場合は、委託先事業者に対する監査を行う場合も。
- 監査項目の例は、「総務省セキュリティ監査ガイドライン」を参照。

自己点検

- 専門的な監査人のアサインが困難な場合は、自己点検を定期に実施することも有効。

情報セキュリティポリシー及び関係規定等の見直し

監査や自己点検の結果を反映

情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に、評価を行い、必要がある場合、改善を実施。

ガイドラインの改定の経緯

改定時期	主な改定内容
平成30年９月	平成27年の日本年金機構における情報流出事案を受け、総務省から地方公共団体へ要請を行った「**三層の対策**」等の情報セキュリティの抜本的強化策の内容を反映
令和２年12月	「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、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モデルを提示するなど新たな対応策を追加（β・β'モデル）**
令和４年３月	令和３年７月の「政府機関等の情報セキュリティ対策のための統一基準群」の改定や、地方公共団体のデジタル化の動向を踏まえた内容を反映
令和５年3月	標準準拠システム等のクラウドサービスの利用を想定し、**クラウドサービスを利用する際の具体的な情報セキュリティ対策の内容を第4編（特則）に反映**
令和６年10月	Web会議等の目的で、業務端末からインターネット経由で、特定のクラウドサービスを安全に利用するための対策**（α'モデル）**や、政府統一基準の改定内容に沿った業務委託時における対策、地方公共団体が取り扱う個人情報の重要性を鑑みて、個人情報を自治体機密性３分類に分類することを追加
令和７年３月	令和６年６月の「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」を踏まえた**マイナンバー利用事務系に係る画面転送の方式**やLGWAN接続系・マイナンバー利用事務系における無線LAN利用の要件等について新たに規定
令和８年3月	地方自治法の一部を改正する法律(令和６年法律第65号)により総務大臣が指針を示すこととされガイドラインとの重複箇所を一部見直すとともに、**リユースを踏まえ機器の廃棄・データ消去に関する規定の見直し**やUSBメモリ等の利用に関するリスクへの対処を反映

令和8年3月のガイドライン改定のポイントについて

1.地方自治法改正に伴う対応

■ 令和６年の地方自治法の改正に伴い、大臣指針案が令和７年４月１日付で発出されており、ガイドライン第1編総則において記載内容が重複する箇所等について削除等を実施。

2. 機器の廃棄・データ消去について

■ 「政府機関等の対策基準策定のためのガイドライン」を参考にマイナンバー利用事務系の領域において住民情報を保存する記録媒体における機器の物理的破壊について、機器のリユース（再利用）が困難になることやコスト等の課題があることから、物理破壊以外の方法を追加。また、データ消去作業の職員の立ち合いを行う範囲を明確化。

3. USBメモリ等の利用におけるリスクへの対処

■ 「政府機関等の対策基準策定のためのガイドライン」を参考に総務省のガイドラインで不足している対策について追記。

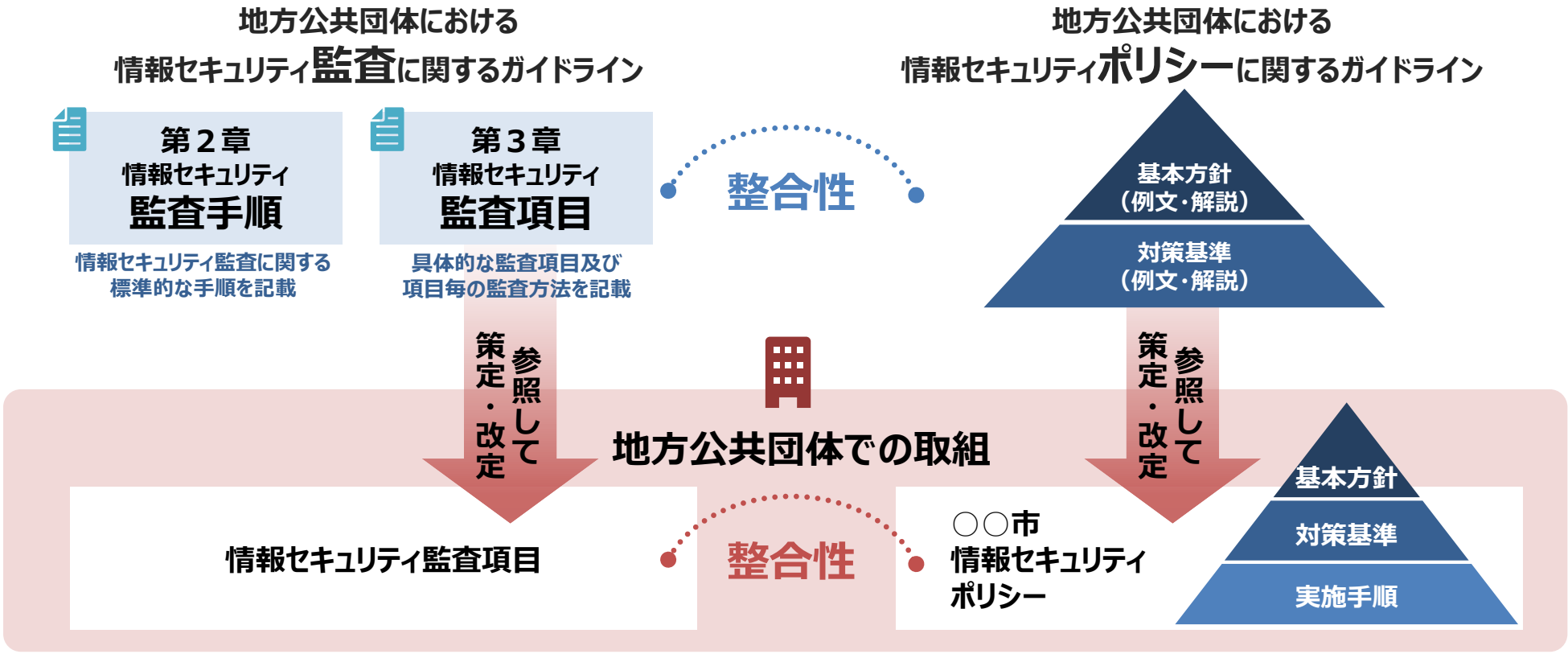
4.その他

■ 「政府機関等の対策基準策定のためのガイドラインの一部改定（令和７年９月）」を踏まえ、DNS設定情報を悪用する攻撃等について追記。

※ 上記2・3については第3編 対策基準（解説）を改定。
※ 地方公共団体における情報セキュリティ監査に関するガイドラインについては時点更新と形式修正のみ。

監査ガイドライン（1）

- 地方公共団体においては、「地方公共団体における情報セキュリティ監査に関するガイドライン」（以下「監査ガイドライン」という。）を参照して監査項目を策定し、監査を実施する必要がある。
- β・β'モデルやα'モデルを採用する場合、外部監査を実施し、監査報告書をJ-LIS（地方公共団体情報システム機構）へ提出する必要がある。



監査ガイドライン (2)

監査ガイドライン「第3章情報セキュリティ監査項目」を参照

- 監査ガイドラインの監査項目は、ガイドラインの例文の番号に対応するように構成。
- 当該監査項目で求められる内容の詳細は、総務省セキュリティポリシーガイドラインの例文・解説参照。

項目			No.	必須	監査項目	監査資料の例	監査実施の例	情報セキュリティポリシーガイドラインの例文の番号	関連するJISQ27002番号	留意事項
1. 組織体制		(1)組織体制、権限及び責任	1	○	**ⅰ)組織体制、権限及び責任** CISOによって、情報セキュリティ対策のための組織体制、権限及び責任が定められ、文書化されている。	□情報セキュリティポリシー □権限・責任等一覧	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、情報セキュリティ対策に係る権限、責任、連絡体制、兼務の禁止が文書化され、正式に承認されているか確かめる。	1.(1)～(6)、(8)	5.2 5.4	
		(2)情報セキュリティ委員会	2	○	**ⅰ)情報セキュリティ委員会の設置** CISOによって、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する機関(情報セキュリティ委員会)が設置されている。	□情報セキュリティポリシー □情報セキュリティ委員会設置要綱	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、情報セキュリティポリシー等、情報セキュリティに関する重要な事項を決定する機関(情報セキュリティ委員会)が設置されているか確かめる。	1.(7)①	―	・情報セキュリティに関する意思決定機関として情報セキュリティ委員会以外に庁議や幹部会議等を位置づけることも可能である。
			3		**ⅱ)情報セキュリティ委員会の開催** 情報セキュリティ委員会が毎年度開催され、情報セキュリティ対策の改善計画を策定し、その実施状況が確認されている。	□情報セキュリティポリシー □情報セキュリティ委員会設置要綱 □情報セキュリティ委員会議事録	監査資料のレビューと統括情報セキュリティ責任者又は情報セキュリティ責任者へのインタビューにより、情報セキュリティ委員会が毎年度開催され、リスク情報の共有や情報セキュリティ対策の改善計画を策定し、その実施状況が確認されているか確かめる。	1.(7)②	―	
		(3)CSIRTの設置・役割	4	○	**ⅰ)CSIRTの設置・役割の明確化** CSIRTが設置され、部局の情報セキュリティインシデントについてCISOへの報告がされている。また、CISOによって、CSIRT及び構成する要員の役割が明確化されている。	□情報セキュリティポリシー □CSIRT設置要綱	監査資料のレビューと統括情報セキュリティ責任者へのインタビューにより、CSIRTが設置されており、規定された役割に応じて情報セキュリティインシデントのとりまとめやCISOへの報告、報道機関等への通知、関係機関との情報共有等を行う統一的な窓口が設置されているか確かめる。また、監査資料のレビューとCISO又は構成要員へのインタビューにより、CSIRTの要員構成、役割などが明確化されており、要員はそれぞれの役割を理解しているか確かめる。	1.(9)	5.5 5.6 5.24 5.25 5.26 6.8	
2		(1)情報			ⅰ)情報資産の分類に関わる基準	□情報セキュリティポリ	監査資料のレビューと統括情報セキュリティ責任者又は情報セキュリティ責	2.(1)	5.12	

情報セキュリティ監査項目例（監査ガイドラインから抜粋）