資料１

地方公共団体情報セキュリティポリシーに関する ガイドラインの概要及び直近の改定内容

総 務 省

令和５年10月10日

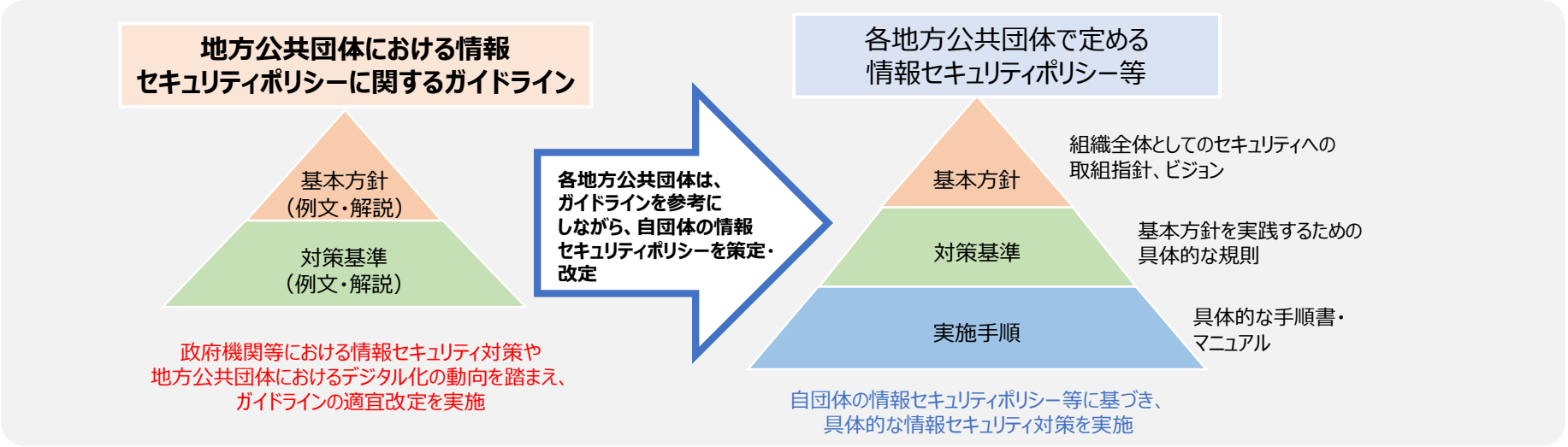
総務省自治行政局

デジタル基盤推進室

地方公共団体における情報セキュリティポリシーガイドラインについて

総務省における地方公共団体の情報セキュリティ対策に対する支援

総務省は、地方公共団体の情報セキュリティ対策を支援するため、平成13年度に情報セキュリティ対策の指針として「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」を策定し、その後も、政府機関等における情報セキュリティ対策の動向や地方公共団体におけるデジタル化の動向等を踏まえながら適宜ガイドラインの改定を実施



直近のガイドライン改定

改定時期	改定内容・理由
平成27年３月	「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（マイナンバー法）」、「サイバーセキュリティ基本法」の成立等の内容を反映
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、情報セキュリティ対策の見直しを実施し、その内容を反映
令和４年３月	令和３年７月の「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

総務省セキュリティポリシー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している。
- 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」に記載した。
- 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５年３月28日改定）

https://www.soumu.go.jp/menu_news/s-news/01gyosei07_050328.html

「三層の対策」概要

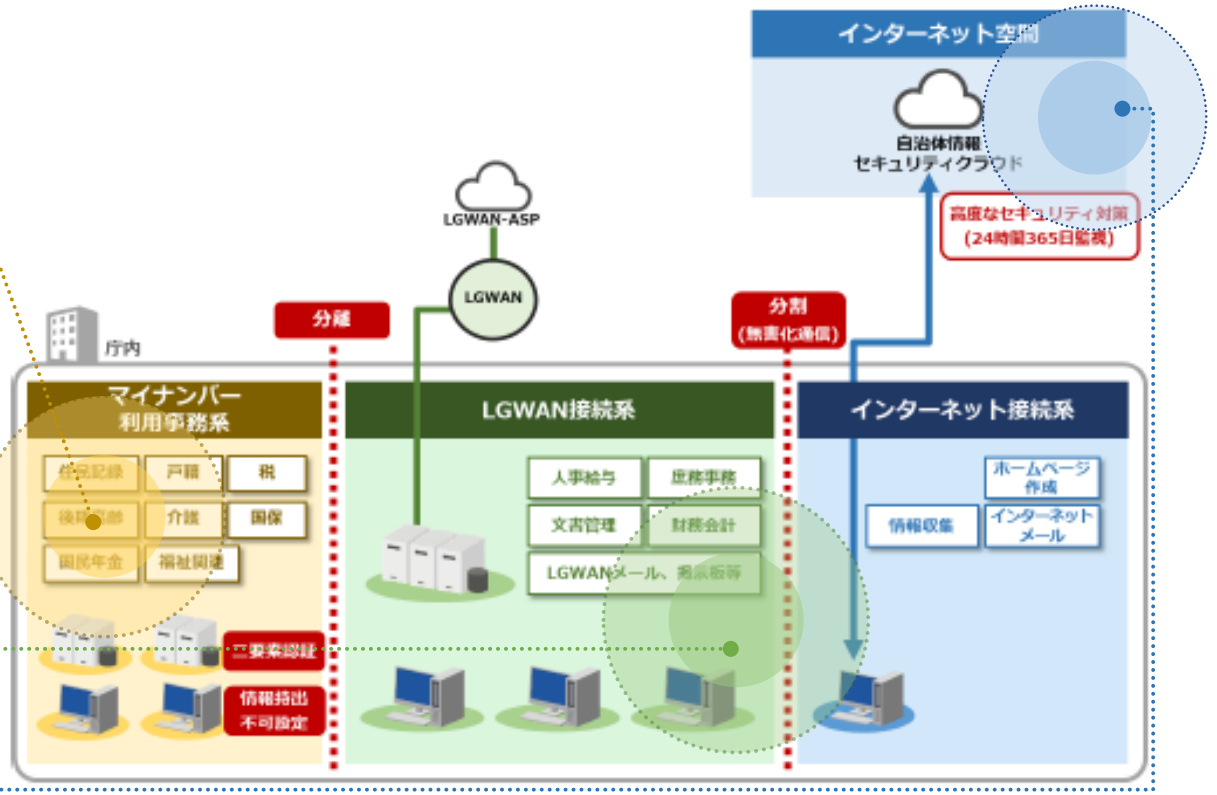
- 複雑・巧妙化しているサイバー攻撃の脅威により、地方公共団体の行政に重大な影響を与えるリスクが想定されるため、情報システムにおいては、機密性はもとより、可用性や完全性の確保にも十分配慮した、情報システム全体の強靭性の向上が求められる。
- **<u>情報システム全体の強靭性の向上を「三層の対策」により実現する</u>**。

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

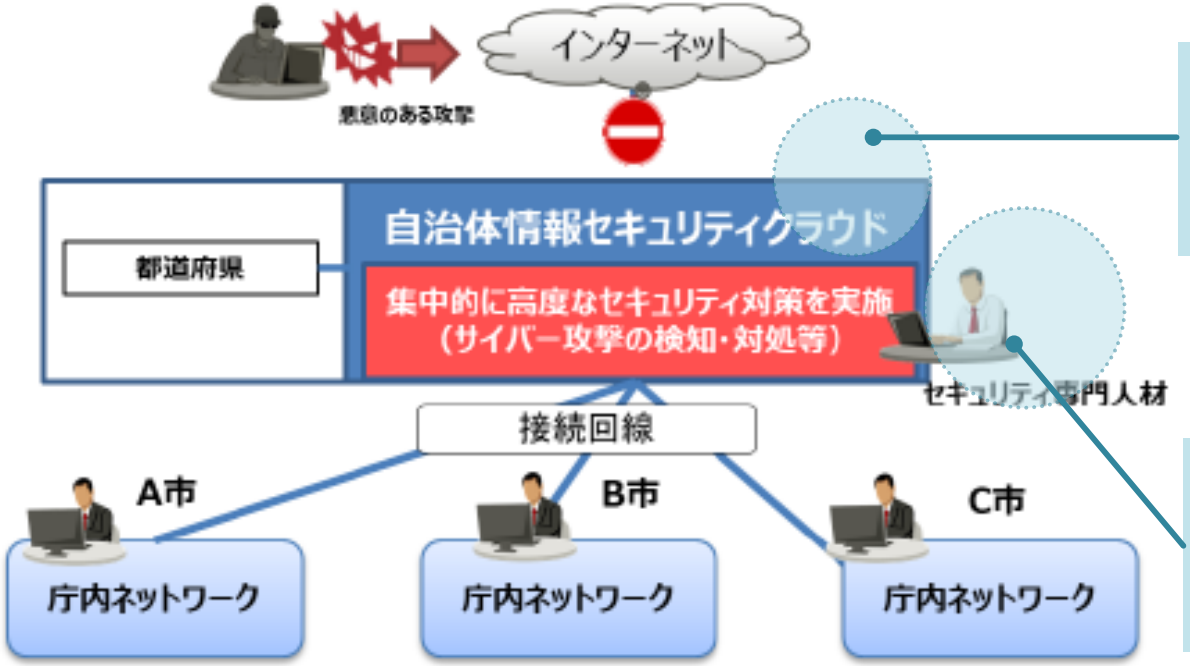
3 都道府県と市区町村が協力して、自治体情報セキュリティクラウドを構築し、高度なセキュリティ対策を実施



三層の構えによる自治体情報システム例（図表21）

自治体情報セキュリティクラウドについて

- 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。
- **自治体情報セキュリティクラウドとは、都道府県と市区町村がWebサーバー等を集約し、監視及びログ分析・解析をはじめ高度なセキュリティ対策を実施するもの**。
- 次期自治体情報セキュリティクラウドにおいては、**国が標準要件として、最低限満たすべき事項（必須要件）及び各都道府県の要求水準に応じて導入を検討する事項（オプション要件）を提示**し、民間ベンダにクラウドサービスの開発・提供を依頼することにより、セキュリティ水準の確保とコストの抑制を図った。



インターネット通信の監視
インシデントの予防（ファイアウォール等のゲートウェイ対策、メールセキュリティ対策、Webサーバセキュリティ対策等）　等

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

自治体情報セキュリティクラウド（図表25）

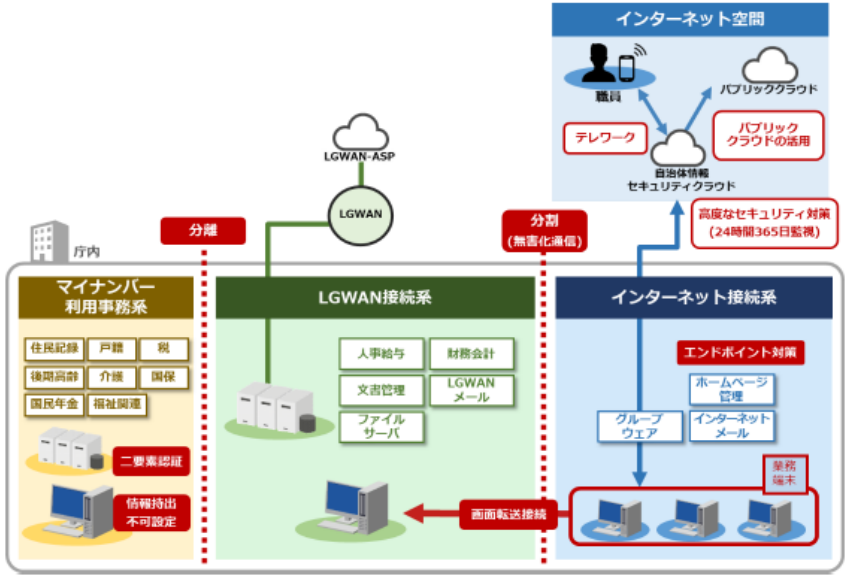
βモデルとβ′モデル

令和２年度ガイドライン改定により、業務端末をLGWAN接続系に配置するαモデル（従来モデル）に加え、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

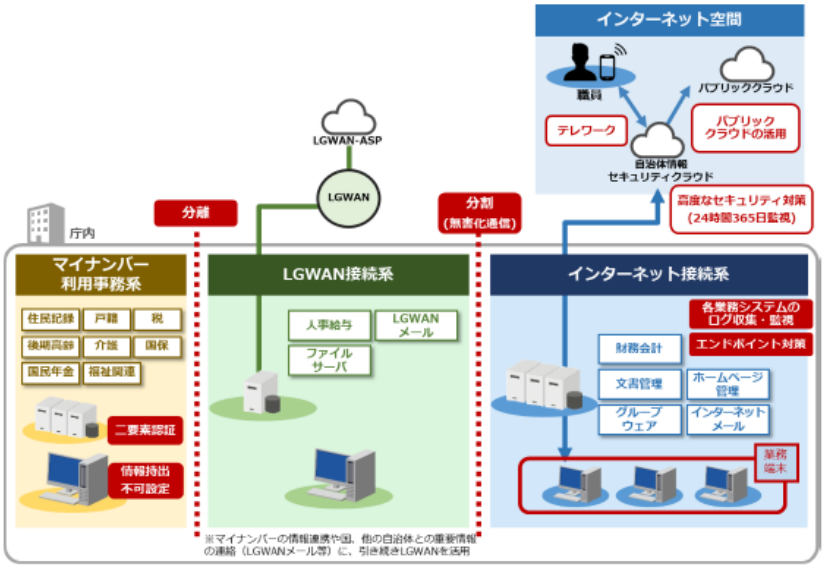


βモデルイメージ図（図表28）

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（図表30）

令和４年度（令和5年3月改定）の改定のポイント（要点）

- 「総務省セキュリティポリシーガイドライン」は、主に「**標準準拠システム等のクラウドサービスの利用**」、「**業務委託先管理の強化**」、「**昨今のサイバー攻撃の動向を踏まえた対策**」の３つの観点により、令和５年３月に改定を実施した。
- 特にクラウドサービスはサービスモデルが多岐にわたるため、セキュリティ要件確認の際の、クラウドサービスの特性を鑑みた留意事項（ISMAP等の取得、機密性の高い情報が国内のデータセンターに保存されるか）や、ガバメントクラウド等を利用する際に対応すべきセキュリティ対策をガイドラインで定めた。

1. クラウドサービスの利用に対する対応

- 「第１編 総則」に、クラウドサービス利用に関するメリットや留意点等を記載。
- 「第４編 特則」に、標準準拠システム等のクラウド利用を行う場合の具体的な情報セキュリティ対策（セキュリティポリシーの例文・解説）を新規作成。

2.業務委託先管理の強化

- 業務委託先の情報の取扱いに当たり、「最小限の権限」、「複数人による確認」等を徹底する旨を記載。
- 委託事業者に対し、最新版の従事者名簿の提出を求め、定期的な確認を記載。
- 委託事業者の従業員が地方公共団体の情報セキュリティポリシー等を理解するための研修を記載。
- 運用面の支援として、「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」を新規作成。

3. 昨今のサイバー攻撃に対する対策

- Emotet等への対策として、マクロの実行禁止、メールの監査ログの取得、SOC による常時監視等を記載。
- ランサムウェア等への対策として、導入しているOSやソフトウェアの脆弱性管理やデータ、システムのバックアップ等を記載。
- フィッシング等への対策として、 Webサービスにログイン時の多要素認証等の設定の有効化等を記載。

令和４年度の改定のポイント（クラウドサービスの利用に対する対応①）

- 第１編 総則には、クラウドサービスの特性に応じた留意点として、「情報セキュリティ要求事項の確認」、「第三者認証の取得状況の確認」、「機密性の高い情報の国内データセンターへの保存」等を確認する旨を示している。
- また、クラウドサービス利用時には、リスク評価を実施し、受容が困難な場合のリスク低減策の検討等の必要性を示している。

第１編 総則	主な記載内容
1. クラウドサービスにおけるサービスモデルと責任の分担	● **クラウドサービスのモデルに応じて、クラウドサービス事業者の責任の範囲が異なり、留意が必要**なため、各モデル（IaaS、PaaS、SaaS）の特徴や一般的な管理主体の例を記載。
2. クラウドサービスの特性における留意事項	● クラウドサービスの特性に伴い、次の事項に留意が必要であることを記載。 ・ **第三者認証の確認の際には、ISMAP等の取得状況を確認**すること ・ **機密性が高い情報は、国内のデータセンターに保存されることを確認**する必要があること ・ **自組織の情報セキュリティの要求事項を満たすか評価**すること ・ 情報セキュリティ対策の評価の際には、クラウドサービス事業者の公開情報等を参考にすること
3. クラウドサービスを利用する際に関係する複数のステークホルダー	● クラウドサービスを利用する際に複数のステークホルダーが存在する場合は、**役割と責任の範囲を明確**にし、契約締結が必要であることを記載。 ● クラウドサービスのサプライチェーンの構成に応じた複数のステークホルダーとの契約関係、責任の範囲の例を記載。
4. クラウドサービスを利用する際のリスクの検討	● クラウドサービスの**リスク評価及び結果に応じた対応の確認**をクラウドサービスの利用前に実施する必要があることを記載。 ● ライフサイクルにおける管理、自組織の運用体制、自組織の情報セキュリティポリシーや業務継続に適しているか等の検討が必要であることを記載。

令和４年度の改定のポイント（クラウドサービスの利用に対する対応②）

- 第４編 特則には、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を、本編と同様の構成で、例文と解説として示している。
- また、ガバメントクラウド及びガバメントクラウドと同等の情報セキュリティの水準が維持可能なクラウドサービスは、原則としてインターネット接続は禁止だが、例外的に接続が可能となる場合（修正プログラムの適用、ソフトウェアのアクティベーションの実施及び管理コンソール接続）を示している。

第４編 特則	主な記載内容
第１章 本編の目的について	● 今後、地方公共団体においては、ガバメントクラウドの利用を中心として、マイナンバー利用事務系の標準準拠システム等のクラウドサービスの利用が浸透することが想定されるため、本編においては、**クラウドサービス上で標準準拠システム・関連システム等の業務システム（以下「標準準拠システム等」という。）を整備及び運用する場合の考え方とその対策基準**を記載。 ● **地方公共団体においては、クラウドサービス上での標準準拠システム等の整備及び運用を開始するまでに、本編に示された対策基準（例文及び解説）の内容を参考に情報セキュリティポリシーの見直しを行う必要がある**ことを記載。
第２章 本編における クラウドサービスの範囲について	● **ガバメントクラウド及びガバメントクラウドと同等の情報セキュリティの水準が維持可能なクラウドサービスについては、**特段の場合（**修正プログラムの適用、ソフトウェアのアクティベーションの実施及び管理コンソール接続**）に例外的に**インターネット接続を可能**とすることを記載。 ● 本編は、標準準拠システム等をガバメントクラウドにおいて利用することを前提とした情報セキュリティの対策基準を記載。
第３章 本編における対策基準の構成について	● 本編の構成は、地方公共団体が参照しやすいようにガイドラインの対策基準において規定されている項目に沿って、クラウドサービスの提供や利用に関する情報セキュリティの国際規格（JIS Q 27017）のクラウドサービスの利用者に求められる事項を参考にし、**クラウドサービス上で標準準拠システム等を整備及び運用する場合の具体的な対策基準について、例文と解説**を記載。
第４章 情報セキュリティ対策について	● **対策基準に追加する例文と解説**を記載。 ※詳細は、以降のスライドに記載。

令和４年度の改定のポイント（業務委託先管理の強化）

「第３編 第２章 情報セキュリティ対策基準（解説） 8.1. 業務委託」を参照

- 業務委託先における情報漏えい等を防ぐため、地方公共団体による管理をより強化する観点から、特に運用面に関する必要なセキュリティ対策を示している。
- 委託事業者がセキュリティ要件を遵守していることを地方公共団体が確認できるようにするため、「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」を作成した。

業務委託先の管理 改定ポイント	主な記載内容
業務委託先の情報の取扱いの徹底	● 業務委託を行う場合、情報資産の分類に応じた情報のライフサイクル管理の徹底が必要である旨を記載。 ● **業務委託先が重要な情報資産を取り扱う場合**においては、情報セキュリティの原則である**「最小限の権限」、「複数人による確認」等を徹底**する旨を記載。 ● また、USBメモリのような物理的なデータ移動ではなく、外部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の確認事項を記載。
委託事業者の従事者の確認	● **管理区域内に入室する際**は、入室者に対して**身分証の提示を求め、従事者名簿と突合**することや職員の随行、監視カメラ等によって入室者を確認する旨を記載。 ● 従事者の変更があった際は、委託事業者に対し、**最新版の名簿の提出**を求めるとともに、従事者名簿の提出時に身分証明書の確認や面談により本人確認を行う旨を記載。 ● 委託事業者から名簿の提出がない場合であっても定期的（年1回程度）に従事者が変更されていないか確認する旨を記載。
委託事業者の研修	● **委託事業者の従業員が地方公共団体の情報セキュリティポリシー等を理解**することが重要であり、業務委託先の従業員に地方公共団体が主催する研修等に参加させることや、研修を合同で行うことも有効である旨を記載。
運用面の支援	● 委託事業者がセキュリティ要件を遵守していることを地方公共団体が確認するため、**「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、委託事業者がセキュリティ要件を遵守しているか確認**する必要がある旨を記載。

令和４年度の改定のポイント（昨今のサイバー攻撃に対する対策）

「第３編 第２章 情報セキュリティ対策基準（解説） 6.4 不正プログラム対策」を参照

- 昨今、感染被害が確認されているEmotetを始め、ランサムウェア、フィッシング等の特徴と対策をガイドラインに示している。
- 事前対策としては、導入しているOSやソフトウェアのアップデート、パスワード設定の見直しを行い、被害を低減するための対策としては、データだけでなく、システムも含めたバックアップを取得し、復旧手順をあらかじめ作成し、定期的に確認することが有効と記載。

サイバー攻撃対策 改定ポイント	主な記載内容
Emotet等への対策	● Emotetへの感染を予防し、被害を最小限にとどめるための対策として**「組織内への注意喚起の実施」、「信頼できないWord文書やExcelファイルにおいてマクロの実行禁止」、「メールの監査ログの取得や定期的な確認」**等を記載。
ランサムウェア等への対策	● ランサムウェアに感染しないための事前対策として**「導入しているOSやソフトウェアのアップデート」、「パスワード設定の見直し」**、被害を受けた際の影響を低減するための対策として**「データのバックアップ」**等を記載。 ● なお、「データのバックアップ」については、バックアップを含め暗号化されてしまう可能性があるため、**端末のOS からアクセスできない、ネットワークから切り離されたオフラインのディスクや媒体等へ保管**する検討も必要となる旨を記載。 ● また、可用性を担保する対策としては、**対象となるデータだけではなく、システムのバックアップを取る**ことが有効である旨を記載。 ● その際、有事の際に早急に対応できるようバックアップから復旧可能なことや**復旧手順を定期的に確認する**旨を記載。
フィッシング等への対策	● 対策として、**「メールやSMSに添付されているURLは安易にクリックせず、ウェブサイトにアクセスする際は、あらかじめ登録しているURLからアクセスする」、「Webサービスにログインする場合に、多要素認証等の設定が可能な場合、有効化する」**等を記載。