資料2

NISC政府統一基準（令和５年度）の改定に係る対応について

総 務 省

令和５年12月19日

総務省自治行政局

デジタル基盤推進室

令和5年度における政府統一基準群の見直しについて

✓ 改定ポイントは大きく以下の５つ。

１．情報セキュリティに関するサプライチェーン対策の強化

- 業務委託における政府の情報を保護するため、米国NISTのサプライチェーン対策を参考に、情報へのアクセス制御、ログの取得・監視などの委託先に担保させるべき情報セキュリティ対策を契約に含めるとともに、委託期間を通じた実施を求める。

２．クラウドサービスの利用拡大を踏まえた対策の強化

- 独立行政法人等へのISMAP拡大や、ISMAP-LIU運用開始等を踏まえ、要機密情報を取り扱う場合のクラウドサービスはISMAPクラウドサービスリストから選定することを明記する。
- 要機密情報を取り扱わない場合においても、適切な主体認証やアクセス制御の管理などのクラウドサービスを安全に利用するための対策を講ずる。また、調達行為を伴わないクラウドサービスを利用する場合には、「調達行為を伴わないSNS等の外部サービスの利用等に関する申合せ」に基づき、講ずべき措置についてNISCに助言を求める。

３．ソフトウェア利用時の対策の強化

- 機器等調達時のIT調達申し合わせに基づく対応を必須のものとして明記する。また、重要なソフトウェアについて、設定手順の整備、設定の定期的な確認、教育の実施など、運用時の情報セキュリティ水準を維持するための対策を講ずる。
- 従来の対策に加え、サーバ装置や端末等の運用開始時において、脆弱性診断の実施などソフトウェアの脆弱性対策を強化する。

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

- サイバー攻撃を受けることを念頭においた情報システムの防御に係る対策や情報システムの復旧のための対策を講ずる。
- 昨今のサービス不能攻撃（DDoS攻撃）を踏まえ、専用の対策装置やサービスの導入、サーバ装置や通信回線等の冗長化などの対策や、サービス不能攻撃を受けることを想定した監視方針の策定や脅威情報の収集等の対策を講ずる。
- クラウドサービスの利用の拡大に対応するため、常時診断・対応型セキュリティアーキテクチャを実装することを念頭に、情報資産等へのアクセスを常時診断・検証して、アクセスを許可又は拒否する新たな技術的手法を講じる際に必要な対策を規定（※）。 ※ゼロトラストアーキテクチャに該当。

５．組織横断的な情報セキュリティ対策の強化と情報システムの重要度に応じた対策の確保

- 監査等から得られた組織横断的に改善が必要な事項について、進捗状況を定期的にCISOに報告し、CISOは監査結果に基づく改善進捗を把握・組織の統制を図る。
- 所管独法等の情報セキュリティ対策を支援するため、府省庁側に必要な体制を整備する。独法等は専門的知見を要する事項等について所管省庁等へ助言を求める。
- 情報システムの重要度より高度な対策情報システムの重要度の考え方を導入。全ての情報システムに求める必須の対策に加えて、基幹業務システムなどより重要度の高い情報システムについては、リアルタイムにログ分析を行う機能の導入などの高度な対策を求める。

統一基準による改定箇所（案）

✓ 第１編から第４編に至るまで、多くの項目について改定予定。

第１編　総則
- 第1章　本ガイドラインの目的等
- 第2章　地方公共団体における情報セキュリティとその対策
- 第3章　情報セキュリティの管理プロセス
  - 1. 策定及び導入
  - 2. 運用
  - **3. 評価・見直し（変更）**

第２編・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（例文・解説）
- 第1章　情報セキュリティ基本方針
  - **8. 情報セキュリティポリシーの見直し（変更）**
- 第2章　情報セキュリティ対策基準
  - 1. 組織体制
  - **2. 情報資産の分類と管理（変更）**
  - **3. 情報システム全体の強靭性の向上（変更）**
  - 4. 物理的セキュリティ
  - 4.1 サーバ等の管理、 4.2 管理区域（情報システム室等）の管理
  - **4.3 通信回線及び通信回線装置の管理（変更）**
  - 4.4 職員等の利用する端末や電磁的記録媒体等の管理
  - 5. 人的セキュリティ
  - 5.1 職員等の遵守事項、 5.2 研修・訓練
  - **5.3 情報セキュリティインシデントの報告（変更）**
  - 5.4 ID及びパスワード等の管理
  - 6. 技術的セキュリティ
  - **6.1 コンピュータ及びネットワークの管理（変更）**
  - **6.2 アクセス制御（変更）**
  - **6.3 システム開発、導入、保守等（変更）**
  - 6.4 不正プログラム対策、 6.5 不正アクセス対策
  - **6.6 セキュリティ情報の収集（変更）**
  - 7. 運用
  - **7.1 情報システムの監視（変更）**
  - 7.2 情報セキュリティポリシーの遵守状況の確認～
  - 7.6　懲戒処分等
  - **8. 業務委託と外部サービス（クラウドサービス）の利用　（見出し変更）**
  - **8.1 業務委託（変更）**
  - **8.2 情報システムに関する業務委託（新規作成）**
  - **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）（変更）**
  - **8.4 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わない場合）（変更）**
  - 9. 評価・見直し
  - **9.1 監査（変更）**
  - 9.2 自己点検
  - **9.3 情報セキュリティポリシー及び関係規程等の見直し（変更）**

第4編　地方公共団体におけるクラウド利用等に関する特則
- 第1章　本編の目的について
- 第2章　本編におけるクラウドサービスの範囲について
- 第3章　本編における対策基準の構成について
- 第4章　情報セキュリティ対策について
  - 1. 組織体制～
  - 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　（見出し変更）**
  - 9. 評価・見直し

１．情報セキュリティに関するサプライチェーン対策の強化

1 外部委託に関する分類の見直し

政府統一基準群の主な改定内容

- ✓ 「業務委託」から「情報システムに関する業務委託」を切り出し、必要な対策を上乗せで規定する。
- ✓ 従来の「外部サービス」を「クラウドサービス」、「機関等向けに情報システムの一部の機能を提供するサービス※」に分離し、ISMAP原則利用の考え方に基づいた対策へと改定する。 ※業務委託に分類される。

<改定前の分類>

4.1 業務委託

4.2 外部サービス

4.2.1 要機密情報を取り扱う場合

4.2.2 要機密情報を取り扱わない場合

●外部サービスの例

クラウドサービス、Web会議サービス、検索サービス、翻訳サービス、地図サービス、SNS

ホスティングサービス、インターネット回線接続サービス

<改定後の分類>

4.1.1 業務委託 ※全ての「業務委託」に適用

4.1.2 情報システムに関する業務委託 ※「情報システムに関する業務委託」について上乗せで適用

(1) 共通的対策
(2) 構築の場合の対策
(3) 運用・保守の場合の対策
(4)機関等向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

●情報システムに関する業務委託の例
情報システムの開発及び構築業務、
アプリケーション・コンテンツの開発業務、
情報システムの運用業務

4.2 クラウドサービス ※ISMAP原則利用

4.2.1、4.2.2 要機密情報を取り扱う場合

4.2.3 要機密情報を取り扱わない場合

●**クラウドサービスの例**
仮想サーバ、ストレージ、ハイパーバイザー等提供サービス（IaaS）、
データベースや開発フレームワーク等のミドルウェア等提供サービ（PaaS）、
Web会議サービス、ソーシャルメディア、検索サービス、翻訳サービス、地図サービス

１．情報セキュリティに関するサプライチェーン対策の強化

ガイドライン改定の方向性

- **業務委託は「業務委託」と「情報システムに関する業務委託」に区分して記載**

業務委託の中に情報システムに関す業務委託や情報システムの一部の機能を提供するサービスとの関係性を明確にしてはいかがか。

政府統一基準

4.1.1 業務委託

「業務委託」とは、機関等の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委託」「準委任」「請負」といった契約形態を問わず、全てを含むものとする。
ただし、当該業務において機関等の情報を取り扱わせる場合に限る。

（例）
- 業務運用支援業務（統計、集計、データ入力、媒体変換等）の委託
- プロジェクト管理支援業務の委託
- 調査・研究業務（調査、研究、検査等）の委託

4.1.2 情報システムに関する業務委託

（例）
- 情報システムの開発及び構築業務の委託
- アプリケーション・コンテンツの開発業務の委託
- 情報システムの運用業務の委託
- ウェブサイトの運用業務の委託
- 本市内でのみ利用される共通基盤システム（情報システムのリソースやソフトウェアの一部又は全部を共有する基盤を提供する情報システム）の運用業務（ホスティング型プライベートクラウド）

4.1.2(4)本市向けに情報システムの一部の機能を提供するサービス

（例）
- ホスティングサービス
- インターネット回線接続サービス

改定案：対策基準(趣旨)

8.1. 業務委託

「業務委託」とは、本市の業務の一部又は全部について、契約をもって外部の者に実施させることをいう。「委託」「準委任」「請負」といった契約形態を問わず、全てを含むものとする。
ただし、当該業務において本市の情報を取り扱わせる場合に限る。

（例）
- 業務運用支援業務（統計、集計、データ入力、媒体変換等）の委託
- プロジェクト管理支援業務の委託
- 調査・研究業務（調査、研究、検査等）の委託

8.2. 情報システムに関する業務委託

（例）
- 情報システムの開発及び構築業務の委託
- アプリケーション・コンテンツの開発業務の委託
- 情報システムの運用業務の委託
- ウェブサイトの運用業務の委託
- 本市内でのみ利用される共通基盤システム（情報システムのリソースやソフトウェアの一部又は全部を共有する基盤を提供する情報システム）の運用業務（ホスティング型プライベートクラウド）

8.2.(4)本市向けに情報システムの一部の機能を提供するサービス

（例）
- ホスティングサービス
- インターネット回線接続サービス

１．情報セキュリティに関するサプライチェーン対策の強化

➢ **業務委託は「業務委託」と「情報システムに関する業務委託」に区分して記載**

政府統一基準

（新設）

4.1.2 情報システムに関する業務委託
【遵守事項】

(1) 情報システムに関する業務委託における共通的対策
(a)情報システムセキュリティ責任者は、情報システムに関する業務委託の実施までに、委託先の選定条件に情報システムに機関等の意図せざる変更が加えられないための対策に係る選定条件を加え、仕様を策定すること。
(2) 情報システムの構築を業務委託する場合の対策
(a)情報システムセキュリティ責任者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託先に求めること。
(ア)情報システムのセキュリティ要件の適切な実装
(イ)情報セキュリティの観点に基づく試験の実施
(ウ)情報システムの開発環境及び開発工程における情報セキュリティ対策
(3) 情報システムの運用・保守を業務委託する場合の対策
(a)情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託先に実施を求めること。
(b) 情報システムセキュリティ責任者は、情報システムの運用・保守を業務委託する場合は、委託先が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託先に速やかな報告を求めること。
（続く）

改定案：対策基準(例文)

8.2. 情報システムに関する業務委託
【例文】

（１） 情報システムに関する業務委託における共通的対策
情報システム管理者は、情報システムに関する業務委託の実施までに、情報システムに本市の意図せざる変更が加えられないための対策に係る選定条件を委託事業者の選定条件に加え、仕様を策定しなければならない。
（２） 情報システムの構築を業務委託する場合の対策
情報システム管理者は、情報システムの構築を業務委託する場合は、契約に基づき、以下を全て含む対策の実施を委託事業者に求めなければならない。
①情報システムのセキュリティ要件の適切な実装
②情報セキュリティの観点に基づく試験の実施
③情報システムの開発環境及び開発工程における情報セキュリティ対策
（３） 情報システムの運用・保守を業務委託する場合の対策
①情報システム管理者は、情報システムの運用・保守を業務委託する場合は、情報システムに実装されたセキュリティ機能が適切に運用されるための要件について、契約に基づき、委託事業者に実施を求めなければならない。
②情報システム管理者は、情報システムの運用・保守を業務委託する場合は、委託事業者が実施する情報システムに対する情報セキュリティ対策を適切に把握するため、当該対策による情報システムの変更内容について、契約に基づき、委託先に速やかな報告を求めなければならない。
（続く）

１．情報セキュリティに関するサプライチェーン対策の強化

➢ **業務委託は「業務委託」と「情報システムに関する業務委託」に区分して記載**

政府統一基準

（新設）

4.1.2 情報システムに関する業務委託

【遵守事項】

(続き)

(4) 機関等向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、機関等外の一般の者が機関等向けに要機密情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託先の選定条件に業務委託サービスに特有の選定条件を加えること。

(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定すること。

(c) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、委託先の信頼性が十分であることを総合的・客観的に評価し判断すること。

(d) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は業務委託サービスを利用する場合には、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当該サービスの利用申請を行うこと。

(e) 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は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定すること。

(f) 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は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名すること。

改定案：対策基準(例文)

8.2. 情報システムに関する業務委託

【例文】

(続き)

（４） 本市向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

①情報システム管理者又は情報セキュリティ管理者は、外部の一般の者が本市向けに重要情報を取り扱う情報システムの一部の機能を提供するサービス（クラウドサービスを除く。）（以下「業務委託サービス」という。）を利用するため、情報システムに関する業務委託を実施する場合は、委託事業者の選定条件に業務委託サービスに特有の選定条件を加えなければならない。

②情報システム管理者又は情報セキュリティ管理者は、業務委託サービスに係るセキュリティ要件を定め、業務委託サービスを選定しなければならない。

③情報システム管理者又は情報セキュリティ管理者は、委託事業者の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。

④情報システム管理者又は情報セキュリティ管理者は業務委託サービスを利用する場合には、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当該サービスの利用申請を行わなければならない。

⑤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は、業務委託サービスの利用申請を受けた場合は、当該利用申請を審査し、利用の可否を決定しなければならない。

⑥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は、業務委託サービスの利用申請を承認した場合は、承認済み業務委託サービスとして記録し、業務委託サービス管理者を指名しなければならない。

１．情報セキュリティに関するサプライチェーン対策の強化

2　業務委託に関し、委託先に実施を求める対策を具体化

政府統一基準群の主な改定内容

✓ 業務委託における政府の情報を保護するため、米国NISTのサプライチェーン対策を参考に、情報へのアクセス制御、ログの取得・監視などの委託先に担保させるべき情報セキュリティ対策（※）を契約に含めることを求める。

（※）NISTのSP800-171を参考に、以下の８類型の対策を規定
①インシデント等への対処能力の確立・維持、②アクセス主体の識別とアクセス制御、③ログの取得・監視、④機器等の物理的保護、
⑤要員への周知と統制、⑥資産管理・リスク評価、⑦システムの完全性の保護、⑧セキュリティ対策の検証・評価・見直し

ガイドライン改定の方向性

➢ 委託先に提供した情報が適切に保護されるよう、業務委託契約時、業務委託の実施期間中、終了後に取るべき対策について、地方公共団体で実施すべき対策・委託先に求めるべき対策をそれぞれ規定する。

業務委託に係る規定の整備 → 業務委託実施前の対策 → 業務委託実施期間中の対策 → 業務委託終了時の対策

１．情報セキュリティに関するサプライチェーン対策の強化

➢ 委託先に提供した情報が適切に保護されるよう、**業務委託契約時、業務委託の実施期間中、終了後に取るべき対策について、地方公共団体で実施すべき対策・委託先に求めるべき対策をそれぞれ規定**

業務委託に係る規定の整備 ＞ 業務委託実施前の対策 ＞ 業務委託実施期間中の対策 ＞ 業務委託終了時の対策

政府統一基準

4.1.1 業務委託
【例文】　（赤字が改定部分）
(1)　業務委託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、業務委託に係る以下の内容を全て含む運用規程を整備すること。
(ア)委託先への提供を認める情報及び委託する業務の範囲を判断する基準（以下本款において「委託判断基準」という。）
(イ)委託先の選定基準
(2)　業務委託実施前の対策

（新設）
(a)情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の実施までに、以下を全て含む事項を実施すること。
(ア)委託する業務内容の特定
(イ)委託先の選定条件を含む仕様の策定
(ウ)仕様に基づく委託先の選定
(エ)契約の締結
(オ)委託先に要機密情報を提供する場合は、秘密保持契約（NDA）の締結

（新設）
(b)情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の実施までに、委託の前提条件として、以下を全て含む事項の実施を委託先に求めること。
(ア)仕様に準拠した提案
(イ)契約の締結
(ウ)委託先において要機密情報を取り扱う場合は、秘密保持契約（NDA）の締結

改定案：対策基準(例文)

8.1.業務委託
【例文】
(1)　業務委託に係る運用規程の整備
統括情報セキュリティ責任者は、業務委託に係る以下の内容を全て含む運用規程を整備しなければならない。
①委託事業者への提供を認める情報及び委託する業務の範囲を判断する基準（以下「委託判断基準」という。）
②委託事業者の選定基準
(2)　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。
（略）
（オ）委託事業者に重要情報を提供する場合は、秘密保持契約（NDA）の締結
②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、委託の前提条件として、以下を全て含む事項の実施を委託事業者に求めなければならない。
（ア）仕様に準拠した提案
（イ）契約の締結
（ウ）委託事業者において重要情報を取り扱う場合は、秘密保持契約（NDA）の締結　（続く）

１．情報セキュリティに関するサプライチェーン対策の強化

➢ 委託先に提供した情報が適切に保護されるよう、**業務委託契約時、業務委託の実施期間中、終了後に取るべき対策について、地方公共団体で実施すべき対策・委託先に求めるべき対策をそれぞれ規定**

業務委託に係る規定の整備 ｜ 業務委託実施前の対策 ｜ 業務委託実施期間中の対策 ｜ 業務委託終了時の対策

政府統一基準

4.1.1 業務委託
【例文】
（続き）
（新設）
(3) 業務委託実施期間中の対策
(a)情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の実施期間において以下を全て含む対策を実施すること。
(ア)委託判断基準に従った要保護情報の提供
(イ)契約に基づき委託先に実施させる情報セキュリティ対策の履行状況の定期的な確認
(ウ)委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

(b)情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の実施期間において以下を全て含む対策の実施を委託先に求めること。
(ア)情報の適正な取扱いのための情報セキュリティ対策
(イ)契約に基づき委託先が実施する情報セキュリティ対策の履行状況の定期的な報告
(ウ)委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処。
（続く）

改定案：対策基準(例文)

8.1. 業務委託
【例文】
（続き）

（３） 業務委託実施期間中の対策
①情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、以下を全て含む対策を実施しなければならない。
（ア）委託判断基準に従った重要情報の提供
（イ）契約に基づき委託事業者に実施させる情報セキュリティ対策の履行状況の定期的な確認及び措置の実施
（ウ）統括情報セキュリティ責任者へ措置内容の報告（重要度に応じてCISOに報告）
（エ）委託した業務において、情報セキュリティインシデントの発生若しくは情報の目的外利用等を認知した場合又はその旨の報告を職員等より受けた場合における、委託事業の一時中断などの必要な措置を含む、契約に基づく対処の要求

②情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、以下を全て含む対策の実施を委託事業者に求めなければならない。
（ア）情報の適正な取扱いのための情報セキュリティ対策
（イ）契約に基づき委託事業者が実施する情報セキュリティ対策の履行状況の定期的な報告
（ウ）委託した業務において、情報セキュリティインシデントの発生又は情報の目的外利用等を認知した場合における、委託事業の一時中断などの必要な措置を含む対処
（続く）

１．情報セキュリティに関するサプライチェーン対策の強化

➢ 委託先に提供した情報が適切に保護されるよう、**業務委託契約時、業務委託の実施期間中、終了後に取るべき対策について、地方公共団体で実施すべき対策・委託先に求めるべき対策をそれぞれ規定**

業務委託に係る規定の整備 | 業務委託実施前の対策 | 業務委託実施期間中の対策 | 業務委託終了時の対策

政府統一基準

（新設）

4.1. 業務委託
4.1.1 業務委託

(4) 業務委託終了時の対策
(a) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、業務委託の終了に際して以下を全て含む対策を実施すること。
(ア) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収
(イ) 委託先に提供した情報を含め、委託先において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認
(b) 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、契約に基づき、業務委託の終了に際して以下を全て含む対策の実施を委託先に求めること。
(ア) 業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検
(イ) 提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

改定案：対策基準(例文)

8.1. 業務委託
【例文】

（４） 業務委託終了時の対策
①情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、以下を全て含む対策を実施しなければならない。
（ア）業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの確認を含む検収
（イ）委託事業者に提供した情報を含め、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認
②情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、以下を全て含む対策の実施を委託事業者に求めなければならない。
（ア）業務委託の実施期間を通じてセキュリティ対策が適切に実施されたことの報告を含む検収の受検
（イ）提供を受けた情報を含め、委託業務において取り扱った情報の返却、廃棄又は抹消

２．クラウドサービスの利用拡大を踏まえた対策の強化

２．クラウドサービスの利用拡大を踏まえた対策の強化

政府統一基準群の主な改定内容

- ✓ 独立行政法人等へのISMAP拡大や、ISMAP-LIU運用開始等を踏まえ、要機密情報を取り扱う場合のクラウドサービスはISMAPクラウドサービスリストから選定することを明記。
  （調達したい機能を有したクラウドサービスが登録されていない場合など、やむを得ずISMAPクラウドサービスリスト以外から選定する場合は、CISOの責任において、ISMAP制度で求めている要求事項や管理基準を満たしていることを確認）
- ✓ 要機密情報を取り扱わない場合においても、適切な主体認証やアクセス制御の管理などのクラウドサービスを安全に利用するための対策を講ずる。また、調達行為を伴わないクラウドサービスを利用する場合には、「調達行為を伴わないSNS等の外部サービスの利用等に関する申合せ」に基づき、講ずべき措置についてNISCに助言を求める。

ISMAP-LIUについて

ISMAPが対象とするクラウドサービスのうち、セキュリティ上のリスクの小さな業務・情報の処理に用いるSaaSサービスに対する仕組みであり、また情報システムの調達においては、業務・情報の影響度に応じたセキュリティを確保すべきとの考え方から、影響度が低いと評価される業務、情報に用いられるSaaSを対象とする制度として趣旨が広く理解されるよう、名称は、ISMAP for Low-Impact Use（通称：ISMAP-LIU） とする。

※出典：『ISMAP-LIUについて』（令和４年１１月１日 NISC、デジタル庁、総務省、経済産業省）

外部委託に関する分類の見直し

政府統一基準群の主な改定内容

- ✓ クラウドサービスに一般的なSaaSが含まれることを用語定義において明記し、従来の「外部サービス」を「クラウドサービス」、「機関等向けに情報システムの一部の機能を提供するサービス※」に分離し、ISMAP原則利用の考え方に基づいた対策へと改定する。
- ✓ 「機器等の調達」に関する規定を集約して記載する。

<改定前の分類>

4.1 業務委託

4.2 外部サービス

4.2.1 要機密情報を取り扱う場合

4.2.2 要機密情報を取り扱わない場合

●外部サービスの例

クラウドサービス、Web会議サービス、検索サービス、翻訳サービス、地図サービス、SNS

ホスティングサービス、インターネット回線接続サービス

<改定後の分類>

4.1.1 業務委託 ※全ての「業務委託」に適用

4.1.2 情報システムに関する業務委託 ※「情報システムに関する業務委託」について上乗せで適用

(1) 共通的対策
(2) 構築の場合の対策
(3) 運用・保守の場合の対策
(4)機関等向けに情報システムの一部の機能を提供するサービスを利用する場合の対策

●情報システムに関する業務委託の例
情報システムの開発及び構築業務、
アプリケーション・コンテンツの開発業務、
情報システムの運用業務

4.2 クラウドサービス ※ISMAP原則利用

4.2.1、4.2.2 要機密情報を取り扱う場合

4.2.3 要機密情報を取り扱わない場合

●**クラウドサービスの例**
仮想サーバ、ストレージ、ハイパーバイザー等提供サービス（IaaS）、
データベースや開発フレームワーク等のミドルウェア等提供サービ（PaaS）、
Web会議サービス、ソーシャルメディア、検索サービス、翻訳サービス、地図サービス

4.3 機器等の調達 ※サプライチェーン・リスク対応の明確化

●機器の例
情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称

政府統一基準における「クラウドサービス」の定義 ※下線部が改定により追加
「クラウドサービス」とは、事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。クラウドサービスの例としては、SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）等がある。なお、統一基準におけるクラウドサービスは、機関等外の一般の者が一般向けに情報システムの一部又は全部の機能を提供するクラウドサービスであって、当該サービスにおいて機関等の情報が取り扱われる場合に限るものとする。

２．クラウドサービスの利用拡大を踏まえた対策の強化

ガイドライン改定の方向性

➢ **「外部サービス」の名称を「外部サービス（クラウドサービス）」に修正し、クラウドサービスの例示を見直す**

政府統一基準

4.2.1 クラウドサービスの選定（要機密情報を取り扱う場合）
【趣旨】

＜外部サービスクラウドサービスの例＞
・仮想サーバ、ストレージ、ハイパーバイザー等提供サービス（IaaS）
・データベースや開発フレームワーク等のミドルウェア等提供サービス（PaaS）
・Ｗｅｂ会議サービス
・ソーシャルメディア
・検索サービス、翻訳サービス、地図サービス

全ての文言を外部サービス(クラウドサービス）に変更すると読みにくくなるため、以下「クラウドサービス」としてはいかがか。

【例文】
クラウドサービスの選定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、以下を全て含むクラウドサービス（要機密情報を取り扱う場合）の選定に関する運用規程を整備すること。
(ア)クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下4.2節において「クラウドサービス利用判断基準」という。）
(イ)クラウドサービスの選定基準
(ウ)クラウドサービスの利用申請の許可権限者と利用手続
(エ)クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

改定案：対策基準(趣旨、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）
【趣旨】

＜クラウドサービスの例＞
・仮想サーバ、ストレージ、ハイパーバイザー等提供サービス（IaaS）
□ データベースや開発フレームワーク等のミドルウェア等提供サービス（PaaS）
・Web会議サービス
・SNS（ソーシャルメディア）
・検索サービス、翻訳サービス、地図サービス

【例文】

（１） クラウドサービスの選定に係る運用規程の整備
統括情報セキュリティ責任者は、機密性２以上の情報を取り扱う場合、以下を含む外部サービス（クラウドサービス、以下「クラウドサービス」という。）の利用に関する規定を整備すること。
①クラウドサービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下8.3節において「クラウドサービス利用判断基準」という。）
②クラウドサービス提供者の選定基準
③クラウドサービスの利用申請の許可権限者と利用手続
④クラウドサービス管理者の指名とクラウドサービスの利用状況の管理

２．クラウドサービスの利用拡大を踏まえた対策の強化

➢ 統一基準の遵守事項で「セキュリティ要件を策定」となっている部分については、現行のガイドラインのまま、内容を具体的に記載。

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）

２．クラウドサービスの利用拡大を踏まえた対策の強化

ガイドライン改定の方向性

- **なお、「第４編　地方公共団体におけるクラウド利用等に関する特則」におけるクラウドサービスは、情報システムの標準化に伴うガバメントクラウド利用を念頭においた記載であることを明確にする。**

現行：第４編

第Ⅰ章 本編の目的について

（略）

このような状況を踏まえ、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示す。

対策基準の内容については、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、「クラウドサービスの利用に関する情報セキュリティの国際規格（JIS Q 27017：JIS Q27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の規範）」の内容を参考にしている。

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）の内容を参考にセキュリティポリシーの見直しを行う必要がある。

ガイドラインの記載事項とガバメントクラウドに関する対応については、デジタル庁が示すガバメントクラウドに関するドキュメント類の記載内容等を踏まえ、本ガイドラインの補足資料として、本編の対策基準との対応表を掲載し、適時更新を行う。

現行の第４編は、左記マーカー部分で示す通り、**標準準拠システムをガバメントクラウド上で利用することを念頭においた本編の対策基準が記載されている**ため、改定しないこととしてはいかがか。

２．クラウドサービスの利用拡大を踏まえた対策の強化

ガイドライン改定の方向性

- ISMAPについては、登録事業者側の費用負担増加に伴いサービス継続が困難となる可能性等を鑑み、引き続き、要機密情報を取扱う外部サービスのうちクラウドサービス選定時の参考とすべき認証の１つとする
- ISMAP-LIUについては、**対象とする範囲が限定的**なことに加え、**地方公共団体自身による影響度評価の実施など、地方公共団体側に負担が伴う**ことから、ISMAP同様、参考とすべき認証の１つと位置付ける

政府統一基準

4.2.1 クラウドサービスの選定（要機密情報を取り扱う場合）

【解説】
（2）クラウドサービスの選定
クラウドサービスの選定においては、原則としてISMAP 等クラウドサービスリストから選定する必要がある。やむを得ずISMAP 等クラウドサービスリスト以外のクラウドサービスを選定する場合は、ISMAP の原則利用の考え方に基づき、最高情報セキュリティ責任者の責任において、ISMAP 制度で求めている要求事項や管理基準を満たしていることを確認する必要がある。

改定案：対策基準(解説)

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）
【解説】
（３）クラウドサービスの選定
⑦情報セキュリティ責任者は、クラウドサービスに対する情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、クラウドサービス及び当該サービスの委託先の信頼性が十分であることを総合的・客観的に評価し判断しなければならない。
（略）
このような評価に当たって、クラウドサービス提供者が利用者に提供可能な第三者による監査報告書や認証等を取得している場合には、その監査報告書や認証等を利用する必要がある。
なお、選定条件となる認証には、ISO/IEC27017によるクラウドサービス分野におけるISMS認証の国際規格がある。
また、ISMAP又はISMAP-LIUの管理基準を満たすことの確認やISMAP又はISMAP-LIUクラウドサービスリスト等のほか、日本セキュリティ監査協会のクラウド情報セキュリティ監査やクラウドサービス提供者等のセキュリティに係る内部統制の保証報告書であるSOC報告書（Service Organization Control Report）を活用することを推奨する。クラウドサービス利用時のセキュリティ対策や内部統制に関する報告書等については、以下を参照されたい。
（続く）

2．クラウドサービスの利用拡大を踏まえた対策の強化

ガイドライン改定の方向性

- ISMAPについては、登録事業者側の費用負担増加に伴いサービス継続が困難となる可能性等を鑑み、引き続き、要機密情報を取扱う外部サービスのうちクラウドサービス選定時の参考とすべき認証の１つとする
- ISMAP-LIUについては、**対象とする範囲が限定的**なことに加え、利用する団体（地方公共団体）自身による影響度評価の実施など、地方公共団体側に負担が伴う可能性があることから、ISMAP同様、参考とすべき認証の１つと位置付ける

政府統一基準

4.2.1 クラウドサービスの選定（要機密情報を取り扱う場合

【解説】
（続き）

参考：サイバーセキュリティ対策推進会議・各府省情報化統括責任者（CIO）連絡会議決定「政府情報システムのためのセキュリティ評価制度（ISMAP）の利用について」（令和２年６月30 日）（https://www.nisc.go.jp/policy/group/general/ismap.html）

参考：ISMAP クラウドサービスリスト（https://www.ismap.go.jp/csm?id=cloud_service_list）

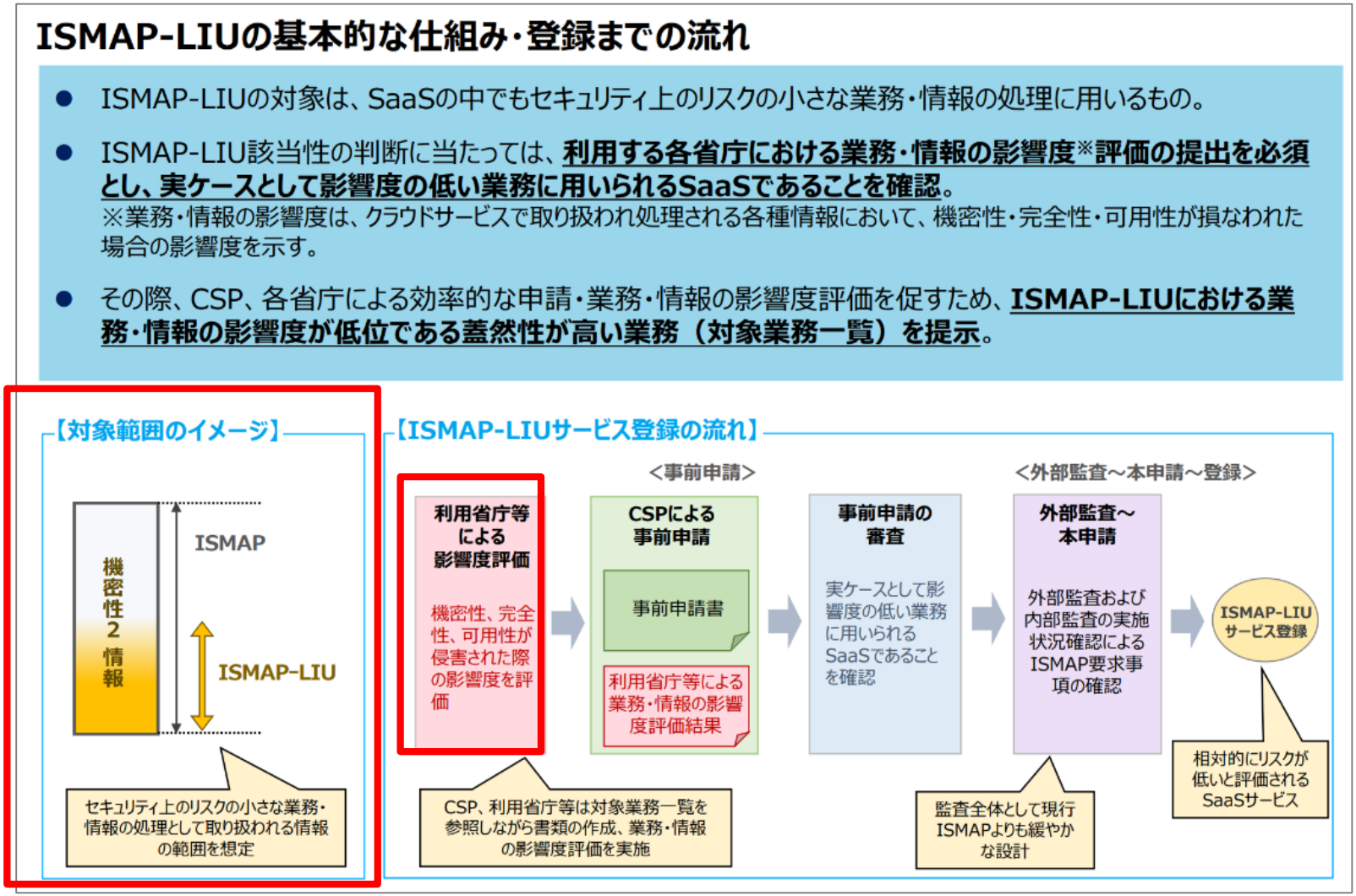
改定案：対策基準(解説)

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）
【解説】
（続き）

参考：国際規格
「ISO/IEC27017（安全なクラウドサービス利用のための分野別ISMS規格）」
参考：ISMAP及びISMAP-LIU
「ISMAP　政府情報システムのためのセキュリティ評価制度」（https://www.ismap.go.jp/csm）
参考：日本セキュリティ監査協会
「クラウド情報セキュリティ管理基準」（https://jcispa.jasa.jp/documents/）
「クラウド情報セキュリティ監査制度規程」（https://jcispa.jasa.jp/cloud_security/jcispa_regulation/）
参考：日本公認会計士協会「受託業務のセキュリティ・可用性・処理のインテグリティ・機密保持に係る内部統制の保証報告書（日本公認会計士協会IT委員会実務指針第7 号）」（https://jicpa.or.jp/specialized_field/45_8.html）
参考：米国公認会計士協会「Service Organization Control (SOC) Reports」（https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html）

（参考）ISMAP-LIUについて

- ✓ **ISMAP-LIUの対象は、セキュリティ上のリスクの小さな業務・情報処理**とされており、ISMAPの代わりにはなり得ない。
- ✓ ISMAP-LIU登録にあたっては、事前申請において、**利用する各省庁における業務・情報の影響度評価が必須**とされており、仮にガイドラインでISMAP-LIUを必須とした場合、利用者である地方公共団体で、同様の影響度評価の実施が必要になると考えられる。



※出典：『ISMAP-LIUについて』（令和４年１１月１日 NISC、デジタル庁、総務省、経済産業省）

３．機器・ソフトウェアの利用時の対策の強化

3．機器・ソフトウェア利用時の対策の強化

政府統一基準群の主な改定内容

- ✓ サプライチェーンリスクの明確化のため、「機器等の調達」に関する規定を集約して記載する。
- ✓ 機器等調達時のIT調達申し合わせに基づく対応を必須のものとして明記。また、重要なソフトウェア(※)について、設定手順の整備、設定の定期的な確認、教育の実施など、運用時の情報セキュリティ水準を維持するための対策を講ずる。
  （※）端末やサーバ装置の制御、統合的な主体認証管理、資産管理、ネットワーク監視など、情報システムを制御する上でセキュリティ上の重要な機能を有しているソフトウエアをいう
- ✓ 従来の対策に加え、サーバ装置や端末等の運用開始時において、脆弱性診断の実施などソフトウェアの脆弱性対策を強化する。

4.3 機器等の調達

●用語の定義
用語定義：「機器等」とは、情報システムの構成要素（サーバ装置、端末、通信回線装置、複合機、特定用途機器等、ソフトウェア等）、外部電磁的記録媒体等の総称をいう。

＜情報システムの基盤を管理又は制御するソフトウェアの例＞
・端末やサーバ装置、通信回線装置等を制御するソフトウェア
・統合的な主体認証を管理するソフトウェア
・ネットワークを制御・管理するソフトウェア
・資産を管理するソフトウェア
・監視に関連するソフトウェア
・情報システムのセキュリティ機能として使用するソフトウェア

6.5.1 情報システムの基盤を管理又は制御するソフトウェア

●ソフトウェア導入時の対策
ソフトウェア自体を保護するための措置を講ずること、ソフトウェアの情報セキュリティ水準の維持に関する手順の整備、ソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順の整備

●ソフトウェア運用時の対策
ソフトウェアのセキュリティを維持するための対策、脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策

権限設定やアクセス制御、セキュリティ設定が適切であるか定期的な確認（脆弱性対策）

3．機器・ソフトウェア利用時の対策の強化

ガイドライン改定の方向性

➢ 機器及びソフトウェアの調達においては、それらの選定基準の一つとして、情報システムの開発時のみならず、運用開始後も不正な変更が加えられない管理がなされ、その管理を地方公共団体が確認できるよう記載を見直す。

政府統一基準

（新設）

4.3. 機器等の調達
4.3.1 機器等の調達
遵守事項

(1)機器等の調達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、機器等の選定基準を運用規程として整備すること。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられない管理がなされ、その管理を機関等が確認できることを加えること。
(b)統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

改定案：対策基準(例文)

（新設）

6.3. システム開発、導入、保守等
【例文】

（1） 機器等の調達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、機器等の選定基準を運用規程として整備しなければならない。必要に応じて、選定基準の一つとして、機器等の開発等のライフサイクルで不正な変更が加えられないような対策を講じなければならない。
②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、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備しなければならない。
（2） 機器等及び情報システムの調達
（略）

「機器等の選定基準」、「必要に応じて」、「不正な変更が加えられないような対策」を具体的に示すため【解説】に説明を追加してはいかがか。

- 選定基準としては、開発工程において信頼できる品質保証体制が確立されていること、**設置時や保守時のサポート体制**が確立されていること、**利用マニュアル・ガイダンスが適切に整備されている**こと、**脆弱性検査等のテストの実施**が確認できること、**ISO等の国際標準に基づく第三者認証**が活用可能な場合は活用すること等が考えられる。
- 取り扱う情報の分類及び取扱制限、利用する組織の特性や利用環境等に応じて想定されるリスクを考慮し、その適用要否を判断した上で、選定基準を整備。
- 不正な変更が行われないような対策としては、機器等の製造工程における不正行為の有無について、**定期的な監査**を行っていること、機器等の**製造環境にアクセス可能な従業員が適切に制限され、定期点検が行われている**こと、**各製造工程の履歴が記録されている**などの厳格な管理されていることが考えられる。

3．機器･ソフトウェア利用時の対策の強化

ガイドライン改定の方向性

- サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を、定期的及び適時に確認することを記載する。

→ アプリケーション･コンテンツの開発時の対策についても記載。

政府統一基準

（新設）

6.6.1 アプリケーション・コンテンツの作成・運用時の対策
【遵守事項】

(3)アプリケーション・コンテンツの開発時の対策

(a)情報システムセキュリティ責任者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講ずること。

改定案：対策基準(例文)

6.3. システム開発、導入、保守等
【例文】

（３）情報システムの開発

④アプリケーション・コンテンツの開発時の対策
情報システム管理者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。

【解説】に脆弱性の排除や脆弱性診断についての説明を追加してはいかがか。

- **脆弱性を排除したウェブアプリケーションを実装する方法**の詳細については、**独立行政法人情報処理推進機構（IPA）による「安全なウェブサイトの作り方」やOWASPのASVS（Application Security Verification Standard：アプリケーションセキュリティ検証標準）を参照**することも考えられる。
- **開発者の気付かない脆弱性が存在してしまう可能性があるため、脆弱性対策の状況を確認するために脆弱性診断を行う**ことが考えられる。
- 脆弱性診断には、ソースコード診断、ウェブアプリケーション診断等の種類があり、必要に応じて脆弱性診断を使い分けて実施する必要がある。

3．機器･ソフトウェア利用時の対策の強化

➢ サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を、定期的及び適時に確認することを記載する。

政府統一基準

（新設）

6.5.1 情報システムの基盤を管理又は制御するソフトウェア
【遵守事項】

(1) 情報システムの基盤を管理又は制御するソフトウェア導入時の対策
(a) 情報システムセキュリティ責任者は、情報セキュリティの観点から情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置を講ずること。
(b) 情報システムセキュリティ責任者は、利用するソフトウェアの特性を踏まえ、以下の全ての実施手順を整備すること。
(ア) 情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順
(イ) 情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順
（続く）

改定案：対策基準(例文)

6.3. システム開発、導入、保守等
【例文】

（５） 情報システムの基盤を管理又は制御するソフトウェア導入時の対策
①情報システム管理者は、情報セキュリティの観点から情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバ装置、通信回線装置等及びソフトウェア自体を保護するための措置を講じなければならない。【推奨事項】
②利用するソフトウェアの特性を踏まえ、以下の全ての実施手順を整備しなければならない。
（ア）情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準の維持に関する手順
（イ）情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順
（続く）

追加のツール等を導入して、端末やサーバ等を保護する必要があり、財政面での負担が発生するため推奨事項としてはいかがか。

3．機器･ソフトウェア利用時の対策の強化

- サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を、定期的及び適時に確認することを記載する。

政府統一基準

（新設）
6.5.1 情報システムの基盤を管理又は制御するソフトウェア
【遵守事項】

(2) 情報システムの基盤を管理又は制御するソフトウェア運用時の対策
(a) 情報システムセキュリティ責任者は、情報システムの基盤を管理又は制御するソフトウェアを運用・保守する場合は、以下の全てのセキュリティ対策を実施すること。
(ア) 情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するための対策
(イ) 脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策

6.2.1 サーバ装置
【遵守事項】
(2) サーバ装置の運用時の対策
(a) 情報システムセキュリティ責任者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行うこと。

改定案：対策基準(例文)

6.3. システム開発、導入、保守等
【例文】

（６） 情報システムの基盤を管理又は制御するソフトウェア運用時の対策
①情報システム管理者は、情報システムの基盤を管理又は制御するソフトウェアを運用・保守する場合は、以下の全てのセキュリティ対策を実施しなければならない。【推奨事項】
（ア）情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するための対策
（イ）脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策

追加のツール等を導入して、端末やサーバ等を保護する必要があり、財政面での負担が発生するため推奨事項としてはいかがか。

②情報システム管理者は、利用を認めるソフトウェアについて、定期的な確認による見直しを行わなければならない。

3． 機器･ソフトウェア利用時の対策の強化

➢ サーバ装置、端末及び通信回線装置上で利用するソフトウェアにおける脆弱性対策の状況を、定期的及び適時に確認することを記載する。

政府統一基準

6.1　端末
6.1.1 端末
遵守事項
(1) 端末の導入時の対策

(e) 情報システムセキュリティ責任者は、端末において利用するソフトウェアに関連する公開された脆弱性について対策を実施すること。（新設）

6.2　サーバ装置
6.2.1 サーバ装置
遵守事項
(1) サーバ装置の導入時の対策

(f) 情報システムセキュリティ責任者は、サーバ装置において利用するソフトウェアに関連する公開された脆弱性について対策を実施すること。（新設）

6.4　通信回線
6.4.2　通信回線装置
遵守事項
(1) 通信回線装置の導入時の対策

(d)情報システムセキュリティ責任者は、通信回線装置において利用するソフトウェアに関連する公開された脆弱性について対策を実施すること。（新設）

改定案：対策基準(例文)

6.6. システム開発、導入、保守等
【例文】

(1)　セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等
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、サーバ装置、端末及び通信回線装置等におけるセキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

統一基準で追記された「公開された脆弱性への対応」については、現行ガイドラインで既に記載されているため、サーバ装置、端末及び通信回線装置等の対象を追加するに留めてはいかがか。

＜該当箇所＞
6.6.
（1）セキュリティホールに関する情報の収集･共有及びソフトウェアの更新等
（2）不正プログラム等のセキュリティ情報の収集･周知
（3）情報セキュリティに関する情報の収集及び共有

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

1 サイバー攻撃を受けることを念頭においた情報システムの防御・復旧やバックアップに係る対策の強化

政府統一基準群の主な改定内容

✓ サイバー攻撃を受けることを念頭においた情報システムの防御に係る対策や情報システムの復旧のための対策を講ずる。
（情報システムへの監視機能やクラウドサービスの管理者権限を有する主体などの厳格な主体認証が必要な場合における多要素主体認証の導入、情報セキュリティインシデント発生に備えた情報システムの復旧手順の整備や適切なバックアップの取得、バックアップ要件・復旧手順の見直しなど）

現行ガイドラインにおける「情報システムの防御・復旧に係る対策」の記載

第２編　例文　第２章

6.1.　コンピュータ及びネットワークの管理

（２）バックアップの実施

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、業務システムのデータベースやファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

6.2. アクセス制御等

（１）アクセス制御等

①アクセス制御

統括情報セキュリティ責任者又は情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

③特権を付与されたID の管理等

（ア）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、管理者権限等の特権を付与されたID を利用する者を必要最小限にし、当該ID のパスワードの漏えい等が発生しないよう、当該ID 及びパスワードを厳重に管理しなければならない。

7.3.　侵害時の対応等

（１）緊急時対応計画の策定

CISO 又は情報セキュリティ委員会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、緊急時対応計画を定めておき、セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

ガイドライン改定の方向性

- 基本的に、必要な対策群が記載されており、更に強化が必要な項目については、地方公共団体の導入費用等も考慮しながら記載を見直す。

→ サーバ装置と通信回線装置について記載。

政府統一基準

6.2.1 サーバ装置
【遵守事項】
(1) サーバ装置の導入時の対策

(g) 情報システムセキュリティ責任者は、要安定情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得すること。（新設）

6.4.2 通信回線装置
【遵守事項】
(2) 通信回線装置の運用時の対策

(b) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管すること。（新設）

改定案：対策基準(例文)

6.1. コンピュータ及びネットワークの管理
【例文】

(2)バックアップの実施
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、業務システムのデータベースやファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。
②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、重要な情報を取り扱うサーバ装置については、適切な方法でサーバ装置のバックアップを取得しなければならない。
③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、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管しなければならない。

【解説】にバックアップについての説明を追加してはいかがか。
- 許容される停止時間等を踏まえる。
- OS やアプリケーションなどを含むサーバ装置全体をバックアップする方法やサーバ装置の複製をバックアップとして用意しておく方法などが存在する。

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

ガイドライン改定の方向性

- 基本的に、必要な対策群が記載されており、更に強化が必要な項目については、地方公共団体の導入費用等も考慮し記載を見直す。

→ 権限の管理に関し、アクセス制限について追記。

政府統一基準

7.1.3 権限の管理
【遵守事項】

(1)権限の管理
(a)情報システムセキュリティ責任者は、主体から対象に対するアクセスの権限を**必要最小限の範囲で適切に設定するよう、措置を講ずること。**
(略)
(c)**情報システムセキュリティ責任者は、主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認すること。**
（続く）

（赤字が改定部分）

「不要なアクセス権限が付与されていないか定期的に確認」について、以下を【解説】に記載してはいかがか。

- 特に管理者権限を付与した主体については、管理者権限の付与が不要になった時点で権限を変更するなどの対策を実施する必要がある。
- 保守やメンテナンスなどを実施するため、特定の主体に対して一時的に付与した権限については、必要な作業等が終了したら確実に権限の付与を削除する必要がある。

改定案：対策基準(例文)

6.2. アクセス制御
【例文】

（1）アクセス制御等
①アクセス制御
統括情報セキュリティ責任者又は情報システム管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように**必要最小限の範囲で適切に設定する等**、システム上制限しなければならない。
②利用者IDの取扱い
（ア）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、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者IDの取扱い等の方法を定めなければならない。
（イ）職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。
（ウ）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、利用されていないIDが放置されないよう、人事管理部門と連携し、点検しなければならない。
（エ）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、主体から対象に対する不要なアクセス権限が付与されていないか定期的に確認しなければならない。
（続く）

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

➢　基本的に、必要な対策群が記載されており、更に強化が必要な項目については、地方公共団体の導入費用等も考慮し記載を見直す。

→　管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置について記載。

政府統一基準

7.1.3 権限の管理
【遵守事項】
（続き）
(ｌ)権限の管理

(ｂ)情報システムセキュリティ責任者は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講ずること。

改定案：対策基準(例文)

6.2.　アクセス制御
【例文】
（続き）
（ｌ）アクセス制御等
③特権を付与されたIDの管理等
（ア）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、管理者権限等の特権を付与されたIDを利用する者を必要最小限にし、当該IDのパスワードの漏えい等が発生しないよう、当該ID及びパスワードを厳重に管理しなければならない。
（イ）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、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講じなければならない。
（ウ）～（キ）　（略）

「内部からの不正操作や誤操作を防止するための措置」を具体的に示すため、以下の内容を【解説】に記載してはいかがか。

・　権限管理を行う情報システムのうち、内部からの不正操作や誤操作を防ぐための特に強固な権限管理が必要な情報システムについては、ある処理に対し、**複数名による主体認証操作がなければ、その処理自体を完遂できない「デュアルロック機能」や「ワークフロー機能」を導入することが考えられる**。

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

➢ 基本的に、必要な対策群が記載されており、更に強化が必要な項目については、地方公共団体の導入費用等も考慮し記載を見直す。

政府統一基準

8.1.3　テレワーク
【解説】

自治体の費用負担を考慮し、多要素認証方式を用いた主体認証については、推奨事項の形で【解説】に記載してはいかがか。

(2)（b）「リモートアクセスに対し多要素主体認証を行うこと」について
　リモートアクセスにおけるアクセスポイントは、インターネットとの接点になるため、外部からの攻撃にさらされる可能性が高い。悪意のある者に容易に侵入されることのないよう多要素主体認証を導入する必要がある。
　例えば、インターネットVPN 等の公衆回線網である機関等外通信回線を利用する場合は、VPN 回線装置等のアクセスポイントはインターネットとの接点を有することが考えられるため、多要素主体認証方式を用いて主体認証を行う機能を設ける必要がある。また、IP-VPN 等の閉域網をベースとしたインターネットと接点を有していない場合であっても、アクセス元が機関等外通信回線である場合は、機関等の管理外の端末等が接続される可能性があり、なりすましによる不正アクセス等の脅威が考えられるため、多要素主体認証方式を用いて主体認証を行う機能を設ける必要がある。
　なお、侵入を許してしまった場合に備えて、認証を受けた後でも、適宜再認証が必要となるようシステムを構築することが望ましい。

改定案：対策基準(解説)

6.2.　アクセス制御
【解説】

（２）職員等による外部からのアクセス等の制限
外部から庁内ネットワークや情報システムに接続を認める場合は、外部から攻撃を受けるリスクが高くなることから、本人確認手段の確保、通信途上の盗聴を防御するために、原則、安全な通信回線サービスを利用しなければならない。
（略）
なお、マイナンバー利用事務系は、住民情報等の特に重要な情報資産が大量に配置されており、情報漏えいリスクが高いこと等を踏まえ、テレワークの対象外としなければならない。
外部からのアクセス（リモートアクセス）におけるアクセスポイントは、インターネットとの接点になるため、外部からの攻撃にさらされる可能性が高い。悪意のある者に容易に侵入されることのないよう「利用者の本人確認を行う機能」として、多要素認証を導入することが考えられる。例えば、インターネットVPN等の公衆回線網である外部の通信回線を利用する場合は、VPN回線装置等のアクセスポイントはインターネットとの接点を有することが考えられるため、多要素認証方式を用いて主体認証を行う機能を設けることが望ましい。また、IP-VPN等の閉域網をベースとしたインターネットと接点を有していない場合であっても、アクセス元が外部の通信回線である場合は、地方公共団体の管理外端末等が接続される可能性があり、なりすましによる不正アクセス等の脅威が考えられるため、多要素認証方式を用いて主体認証を行う機能を設けることが望ましい。なお、侵入を許してしまった場合に備えて、認証を受けた後でも、適宜再認証が必要となるようシステムを構築することも考えられる。

2 サービス不能攻撃

政府統一基準群の主な改定内容

✓ 昨今のサービス不能攻撃(DDoS攻撃)を踏まえ、専用の対策装置やサービスの導入、サーバ装置や通信回線等の冗長化などの対策や、サービス不能攻撃を受けることを想定した監視方針の策定や脅威情報の収集等の対策を講ずる。

現行ガイドラインにおける「サービス不能攻撃（DDoS攻撃）に対する対策」の記載

✓ ガイドラインが対象とする脅威に含まれており、情報セキュリティ対策基準の解説にて、情報システムの可用性確保の対策として、情報システムを構成する機器の装備している機能による対策の実施等が例示されている。また、都道府県情報セキュリティクラウドの標準要件において、DDoS攻撃を想定した機能について記載している。

第２編　例文　第２章

6.5.　不正アクセス対策

（６）サービス不能攻撃

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、外部からアクセスできる情報システムに対して、第三者からサービス不能攻撃を受け、利用者がサービスを利用できなくなることを防止するため、情報システムの可用性を確保する対策を講じなければならない。

次期自治体情報セキュリティクラウド要件シート（令和２年８月１８日「次期自治体情報セキュリティクラウドの標準要件について」）

対策手段	要件概要・目的	要件補足事項及び推奨事項
CDN	住民への継続的な情報発信のために、Webサイトを公開するWebサーバの負荷分散をする	・DDoS対策機能、WAF機能をオプションとして用意されていることが望ましい

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

ガイドライン改定の方向性

- 基本的に、必要な対策群が記載されており、更に強化が必要な項目については、現行の自治体情報セキュリティクラウドとの関係性を踏まえながら、地方公共団体の導入費用等も考慮し記載を見直す。

→ ネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施する旨を記載。

政府統一基準

6.4.2 通信回線装置
【遵守事項】

(ｉ)通信回線装置の導入時の対策

(ｃ)情報システムセキュリティ責任者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施すること。（新設）

改定案：対策基準(例文)

4.3.　通信回線及び通信回線装置の管理
【例文】

①統括情報セキュリティ責任者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。
②統括情報セキュリティ責任者は、情報システムのセキュリティ要件として策定した情報システムのネットワーク構成に関する要件内容に従い、通信回線装置に対して適切なセキュリティ対策を実施しなければならない。
③～⑤　（略）

「適切なセキュリティ対策を実施」の内容について、以下を【解説】に記載してはいかがか。

・ インターネット等の外部ネットワークを接続する場合は、**不正アクセス等のリスクを低減するためのネットワーク構成**等を構築する必要がある。
・ 通信回線装置を設定する際は、当該通信回線装置を提供している提供者が提示している**推奨設定や業界標準、ベストプラクティス等を参照し、通信回線装置の各種設定を行い、設定の不備等がないようにする**必要がある。

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

ガイドライン改定の方向性

- 基本的に、必要な対策群が記載されており、更に強化が必要な項目については、現行の自治体情報セキュリティクラウドとの関係性を踏まえながら、地方公共団体の導入費用等も考慮し記載を見直す。

→ 通信回線装置が動作するために必要なソフトウェアに関する事項ついて記載。

政府統一基準

6.4.1 通信回線
【遵守事項】
(２)機関等外通信回線の接続時の対策
(b) 情報システムセキュリティ責任者は、機関等内通信回線と機関等外通信回線との間及び機関等内通信回線内の不正な通信の有無を監視するための措置を講ずること。

6.4.2 通信回線装置
【遵守事項】
(１)通信回線装置の導入時の対策
(b) 情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順を定めること。
(2) 通信回線装置の運用時の対策
(c) 情報システムセキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講ずること。

（赤字が改定部分）

改定案：対策基準(例文)

4.3.　通信回線及び通信回線装置の管理
【例文】
（続き）
⑥統括情報セキュリティ責任者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように、不正な通信の有無を監視する等の十分なセキュリティ対策を実施しなければならない。
⑦統括情報セキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアに関する事項を含む実施手順を定めなければならない。また、必要なソフトウェアの状態等を調査し、認識した脆弱性等について対策を講じなければならない。
⑧統括情報セキュリティ責任者は、可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

通信回線装置が動作するために必要な「ソフトウェアに関する事項」を具体的に示すため、以下のような説明を【解説】に追加してはいかがか。

- 通信回線装置で使用するソフトウェアについて、バージョンを含めて定めておくことが望ましい。
- 通信回線装置の更新ソフトウェアの提供を受けた際は、修正された脆弱性についての影響度と緊急度を判断し、影響度や緊急度に応じて更新ソフトウェアを適用するまでの時間をできるだけ短くするなどの対策を検討する必要がある。

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

ガイドライン改定の方向性

- 基本的に、必要な対策群が記載されており、更に強化が必要な項目については、現行の自治体情報セキュリティクラウドとの関係性を踏まえながら、地方公共団体の導入費用等も考慮し記載を見直す。

→ 監視を含むセキュリティ機能について記載。

政府統一基準

（新設）

5.2.3. 情報システムの運用・保守

【遵守事項】

(ｌ) 情報システムの運用・保守時の対策

(a) 情報システムセキュリティ責任者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用すること。

(d) 情報システムセキュリティ責任者は、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講ずること。

(e) 情報システムセキュリティ責任者は、要安定情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をすること

改定案：対策基準(例文)

7.1.　情報システムの監視

【例文】

（１）　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及び情報システム管理者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用しなければならない。

②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、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。

③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、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。

「監視を含むセキュリティ機能」の例として、以下を【解説】に記載してはいかがか。

・主体認証機能
・アクセス制御機能
・権限の管理
・ログの取得・管理
・暗号・電子署名
・監視機能

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

➢ 基本的に、必要な対策群が記載されており、更に強化が必要な項目については、現行の自治体情報セキュリティクラウドとの関係性を踏まえながら、地方公共団体の導入費用等も考慮し記載を見直す。

→ 監視に係る運用管理機能について記載。

政府統一基準

（新設）

7.1.6. 監視機能

【遵守事項】

(1)監視機能の導入・運用

(a) 情報システムセキュリティ責任者は、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装すること。

(b) 情報システムセキュリティ責任者は、情報システムの運用において、情報システムに実装された監視機能を適切に運用すること。

(c) 情報システムセキュリティ責任者は、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直すこと。

6.2.1. サーバ装置

【遵守事項】

(2)サーバ装置の運用時の対策

(c) 情報システムセキュリティ責任者は、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講ずること。

改定案：対策基準(例文)

7.1. 情報システムの監視

【例文】

（２） 情報システムの監視機能

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、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装しなければならない。

②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、情報システムの運用において、情報システムに実装された監視機能を適切に運用しなければならない。

③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、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を定期的に見直さなければならない。

④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、サーバ装置上での情報セキュリティインシデントの発生を監視するため、当該サーバ装置を監視するための措置を講じなければならない。

「監視機能を実装」を具体的に示すため、以下の内容を【解説】に記載してはいかがか。

- 監視するイベントとしては、通信回線を通してなされる不正アクセス又は不正侵入並びにC&Cサーバ等への不正な通信、情報システムの管理者・運用者又は利用者の誤操作若しくは不正操作、サーバ装置等機器の動作、許可されていない者の要管理対策区域への立入り等があり得る。
- 職員等による情報窃取等の不正な動作を監視し、これらの不正な動作を検知・防止する内部脅威対策機能を備えたDLPの仕組みの導入を検討してもよい。

3 動的アクセス制御の実装について

政府統一基準群の主な改定内容

✓ クラウドサービスの利用の拡大に対応するため、常時診断・対応型セキュリティアーキテクチャを実装することを念頭に、情報資産等へのアクセスを常時診断・検証して、アクセスを許可又は拒否する新たな技術的手法を講じる際に必要な対策を規定する。

○ 7.3　ゼロトラストアーキテクチャ

・「ゼロトラストアーキテクチャ」は、組織内外を問わずネットワークは常に侵害されているものであるとの前提のもと、情報資産を保護し、情報セキュリティリスクの最小化を図るための情報セキュリティ対策における論理的・構造的な考え方である。

・ゼロトラストアーキテクチャに基づく情報資産の保護策の１つであり、アクセス制御の仕組みを実現する機能の一部と考えられる動的アクセス制御（※）を実装する場合に特に必要となる対策事項を規定する。

※「動的なアクセス制御」とは、特定のアクセスに対して、セッションが確立してない操作ごとに、都度、アクセス元の信用情報を動的に評価し、アクセス先が信用できる状態であるかを検証したうえで、特定のリスクが検出された場合には追加の認証を求めることや、アクセスを拒否する等のアクセス制御を行うことを想定している。

- 複数の情報システム間で横断的な対策の企画・推進・運用に関する事務の責任者として、情報システムセキュリティ責任者を選任。
- 動的なアクセス制御の導入方針を定めるにあたり、動的アクセス制御の対象とする情報システムと対象とする情報システムのリソース（ユーザーアカウント、機器等）を識別。
- 動的なアクセス制御の実装にあたり、リソースの信頼情報の変化に応じた動的なアクセス制御のポリシーを作成し、動的なアクセス制御のポリシーに基づき、動的なアクセス制御を行う。
- 動的なアクセス制御の運用に際し、アクセスパターンの変化に応じて、再度リスク評価を行い、動的なアクセス制御のポリシーを見直す。また、リソースの信頼情報の収集により検出されたリスクへ対処を行う。

現行ガイドラインにおける「アクセス制御」の記載

- ✓ 例文にて、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない、とされている。
- ✓ 解説にて、β´モデルを採用する場合の必須セキュリティ対策として規定されている。
- ✓ いずれも、静的なアクセス制御に関する記載となっている。

第２編　例文　第２章

6. 技術的セキュリティ

6.2.　アクセス制御

アクセス制御、職員等による外部からのアクセス等の制限、自動識別の設定、ログイン時の表示等、認証情報の管理、特権（管理者権限等）による接続時間の制限について規定

第３編　解説　第２章

３．情報システム全体の強靭性の向上

(中略)

(３) インターネット接続系③　【解説】

β′モデルを採用する場合の必須のセキュリティ対策

対策区分	セキュリティ対策	概要
技術的対策	情報資産単位でのアクセス制御	・情報資産の機密性レベルに応じて業務システム単位でのアクセス制御を行う。文書を管理するサーバ等は課室単位でのアクセス制御を必須とし、係単位でのアクセス制御は推奨とする。

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

ガイドライン改定の方向性

➢ **ゼロトラストアーキテクチャを実現する機能の一部と考えられる「動的なアクセス制御」**に関し、**実装する場合に特に必要な対策について、解説編に参考として記載する**。

政府統一基準

（新設）

7.3.1.動的なアクセス制御の実装時の対策

【目的・趣旨】

従来、組織内ネットワーク上の情報資産の保護においては、インターネット等の機関等外通信回線と組織内ネットワークである機関等内通信回線との境界にファイアウォール等を設置し防御を行い、組織内のネットワークに一定の信頼を置く「境界モデル」の対策が一般的であった。クラウドサービスの普及や、テレワークによる業務システム環境の変化等により、組織内の情報資産を取り巻く脅威は変化しており、このような新たな環境における脅威に対して境界モデルによる防御だけでは十分なセキュリティ対策の実施は困難になりつつある。特に、境界内部に設置されたサーバ装置等の情報資産について、境界での対策を過信しており、内部に侵入された際の横断的侵害（横方向の侵害やラテラルムーブメントとも呼称される）への情報セキュリティ対策が不足している可能性がある。

（続く）

改定案：対策基準(解説)

3．情報システム全体の強靭性の向上

【解説】

（５）ゼロトラストアーキテクチャ

「デジタル社会の実現に向けた重点計画」(令和５年６月９日閣議決定)において、ゼロトラストアーキテクチャの考えに基づくネットワーク構成への対応が掲げられている。
また、内閣官房内閣サイバーセキュリティセンター（NISC）の政府統一基準では以下のとおり、ゼロトラストアーキテクトについて紹介されている。

＜参考：政府機関の情報セキュリティ対策のための統一基準＞

従来、組織内ネットワーク上の情報資産の保護においては、インターネット等の外部通信回線と組織内ネットワークである内部通信回線との境界にファイアウォール等を設置し防御を行い、組織内のネットワークに一定の信頼を置く「境界モデル」の対策が一般的であった。クラウドサービスの普及や、テレワークによる業務システム環境の変化等により、組織内の情報資産を取り巻く脅威は変化しており、このような新たな環境における脅威に対して境界モデルによる防御だけでは十分なセキュリティ対策の実施は困難になりつつある。

特に、境界内部に設置されたサーバ装置等の情報資産について、境界での対策を過信しており、内部に侵入された際の横断的侵害（横方向の侵害やラテラルムーブメントとも呼称される）への情報セキュリティ対策が不足している可能性がある。

（続く）

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

政府統一基準

（新設）

7.3.1. 動的なアクセス制御の実装時の対策

【目的・趣旨】
（続き）

ゼロトラストアーキテクチャは、組織内外を問わずネットワークは常に侵害されているものであるとの前提のもと、情報資産を保護し、情報セキュリティリスクの最小化を図るための情報セキュリティ対策における論理的・構造的な考え方である。また、ゼロトラストアーキテクチャは中長期的な政府情報システムに係るライフサイクル全体にわたって適用されるものであり、特定の実装やソリューションを指すものではない。
ゼロトラストアーキテクチャに基づく情報資産の保護策の１つとして、情報資産へのアクセスの要求ごとに、アクセスする主体や、アクセス元・アクセス先となる機器、ソフトウェア、サービス、ネットワークなどの状況を継続的に認証し、認可する仕組みが考えられる。本款では、このような仕組みを実現する機能の一部と考えられる「動的なアクセス制御」を実装する場合に特に必要な対策について記載する。

【遵守事項】
(1) 動的なアクセス制御における責任者の設置
(a) 統括情報セキュリティ責任者は、複数の情報システム間で動的なアクセス制御を実装する場合は、複数の情報システム間で横断的な対策の企画・推進・運用に関する事務の責任者として、情報システムセキュリティ責任者を選任すること。
（続く）

改定案：対策基準(例文)

3. 情報システム全体の強靭性の向上
（５）ゼロトラストアーキテクチャ
【解説】
（続き）

ゼロトラストアーキテクチャは、組織内外を問わずネットワークは常に侵害されている ものであるとの前提のもと、情報資産を保護し、情報セキュリティリスクの最小化を図るための情報セキュリティ対策における論理的・構造的な考え方である。また、ゼロトラストアーキテクチャは中長期的な情報システムに係るライフサイクル全体にわたって適用されるものであり、特定の実装やソリューションを指すものではない。
ゼロトラストアーキテクチャに基づく情報資産の保護策の１つとして、情報資産へのアクセスの要求ごとに、アクセスする主体や、アクセス元・アクセス先となる機器、ソフトウェア、サービス、ネットワークなどの状況を継続的に認証し、認可する仕組みが考えられる。本款では、このような仕組みを実現する機能の一部と考えられる「動的なアクセス制御」を 実装する場合に特に必要な対策について記載する。

①動的なアクセス制御における責任者の設置
統括情報セキュリティ責任者は、複数の情報システム間で動的なアクセス制御を実装する場合は、複数の情報システム間で横断的な対策の企画・推進・運用に関する事務の責任者として、情報システム管理者を選任すること。
（続く）

４．サイバーレジリエンスの強化や脅威・技術動向を踏まえての対策の強化

政府統一基準

（新設）

7.3.1. 動的なアクセス制御の実装時の対策

【遵守事項】
（続き）

(2) 動的なアクセス制御の導入方針の検討
(a) 情報システムセキュリティ責任者は、動的なアクセス制御を導入する場合、動的アクセス制御の対象とする情報システムのリソースを識別し、動的なアクセス制御の導入方針を定めること。
(3) 動的なアクセス制御の実装時の対策
(a) 情報システムセキュリティ責任者は、動的なアクセス制御の実装に当たり、リソースの信用情報の変化に応じて動的にアクセス制御を行うためのアクセス制御ポリシー（以下「アクセス制御ポリシー」という。）を作成すること。
(b) 情報システムセキュリティ責任者は、アクセス制御ポリシーに基づき、動的なアクセス制御を行うこと。

改定案：対策基準(例文)

3. 情報システム全体の強靭性の向上
（５）ゼロトラストアーキテクチャ
【解説】
（続き）

②動的なアクセス制御の導入方針の検討
情報システム管理者は、動的なアクセス制御を導入する場合、動的アクセス制御の対象とする情報システムのリソースを識別し、動的なアクセス制御の導入方針を定めること。
③動的なアクセス制御の実装時の対策
・情報システムセキュリティ責任者は、動的なアクセス制御の実装に当たり、リソースの信用情報の変化に応じて動的にアクセス制御を行うためのアクセス制御ポリシーを作成すること。
・情報システムセキュリティ責任者は、アクセス制御ポリシーに基づき、動的なアクセス制御を行うこと。

５．組織横断的な情報セキュリティ対策の強化と情報システムの重要度に応じた対策の確保

５．組織横断的な情報セキュリティ対策の強化と情報システムの重要度に応じた対策の確保

政府統一基準群の主な改定内容

✓ 監査等から得られた組織横断的に改善が必要な事項について、進捗状況を定期的にCISOに報告し、CISOは監査結果に基づく改善進捗を把握・組織の統制を図る。

ガイドライン改定の方向性

➢ 監査報告書の指摘事項に対する改善計画が完了していない場合について、CISOに対する進捗状況の定期的な報告を規定する。

政府統一基準

2.3.2　情報セキュリティ監査
【遵守事項】

(３) 情報セキュリティインシデントに係る情報共有
(a) 最高情報セキュリティ責任者は、監査報告書の内容を踏まえ、指摘事項に対する改善計画の策定等を統括情報セキュリティ責任者及び情報セキュリティ責任者に指示すること。**また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示すること。**
(b) 統括情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、機関等内で横断的に改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告すること。**また、措置が完了していない改善計画は、定期的に進捗状況を最高情報セキュリティ責任者に報告すること。**
(c) 情報セキュリティ責任者は、最高情報セキュリティ責任者からの改善の指示のうち、自らが担当する組織のまとまりに特有な改善が必要な事項について、必要な措置を行った上で改善計画を策定し、措置結果及び改善計画を最高情報セキュリティ責任者に報告すること。**また、措置が完了していない改善計画は、定期的に進捗状況を最高情報セキュリティ責任者に報告すること。**

（赤字が改定部分）

改定案：対策基準(例文)

9.1. 監査
【例文】

(７) 監査結果への対応
①CISOは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処（改善計画の策定等）を指示しなければならない。また、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。
②CISOは、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。**また、**庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処**（改善計画の策定等）**を指示しなければならない。**なお、措置が完了していない改善計画は、定期的に進捗状況の報告を指示しなければならない。**

６．過去に改定されなかった箇所の反映

６．過去に改定されなかった箇所の反映

ガイドライン改定の方向性

- 黒塗りを施した報告書が閲覧可能であった事案が発生したことを受けて、外部公開する際の黒塗りの手順について追記してはいかがか。

政府統一基準

3.1.1 情報の取扱い
(5)情報の提供・公表
(d)「不用意な情報漏えい」について
【遵守事項】

情報の提供や公表に当たっては、情報漏えいを防ぐため、文書の作成者名、組織名その他の記録に使用できる「プロパティ」や、文書の作成履歴、PDF ファイルの「しおり」等に残留した不要な情報を除去する必要がある。
また、ソフトウェアを用いて文書の特定の部分（提供・公表不可の情報が記載された部分）の情報を黒塗りして提供・公表する場合があるが、当該文書を入手した者が編集ソフト等を用いて黒塗り部分の情報の閲覧を試みる場合があるため、黒塗りされた部分の情報の削除や置換を行うなど、適切に措置する必要がある。

改定案：対策基準(解説)

2. 情報資産の分類と管理
(2) 情報資産の管理
③情報の作成～⑩情報資産の廃棄
【解説】

（注9）情報の提供や公表に当たっては、情報漏えいを防ぐため、文書の作成者名、組織名その他の記録に使用できる「プロパティ」や、文書の作成履歴、PDFファイルの「しおり」等に残留した不要な情報を除去する必要がある。 また、ソフトウェアを用いて文書の特定部分（提供・公表不可の情報が記載された部分）の情報を黒塗りして提供・公表する場合があるが、当該文書を入手した者が編集ソフト等を用いて黒塗り部分の情報の閲覧を試みる場合があるため、黒塗りされた部分の情報の削除や置換を行うなど、適切に措置する必要がある。

6．過去に改定されなかった箇所の反映

ガイドライン改定の方向性

- ドメイン管理に係るガイドラインについて、古いバージョンを参照元としていたため、最新版に更新する。

現行：対策基準（解説）

6.3. システム開発、導入、保守等
(5)情報システムにおける入出力データの正確性の確保
【解説】

(注12)庁外の者が地方公共団体の名前をタイトルに掲げるなどし、地方公共団体のウェブサイトと誤解されかねないウェブサイトを構築することがあり、これを完全に防ぐことは困難である。このため、以下を例とする対策を実施する必要がある。
・正規のウェブサイトが検索サイトで上位に表示されるよう検索エンジン最適化の措置を実施する
・情報システム管理者は、庁外に提供するウェブサイトに関連するキーワードで定期的にウェブサイトを検索し、不審なサイトが検索結果に表示された場合は、検索サイト事業者に報告するなどの対策を実施する
・以前利用していたドメイン（旧ドメイン）を運用停止する場合は、第三者に再取得され元のWebサイトへのアクセスを利用し、詐欺サイト等へ誘導されることのないようドメインを一定期間保持する。また、旧ドメインへのアクセスがあった際に後継となるサイト（後継サイトがない場合は終了を告知したページや団体トップページ等）へHTTP応答コード301を用いた転送を行うことで、旧ドメインが検索サイトの上位に表示される機会をできるだけなくすことが望ましい。詳細は「ドメイン管理ガイド(2.0版)」（平成28年12月1日 内閣官房情報通信技術（IT）総合戦略室）を参照されたい。

改定案：対策基準(解説)

6.3. システム開発、導入、保守等
（8）情報システムにおける入出力データの正確性の確保
【解説】

（注12）庁外の者が地方公共団体の名前をタイトルに掲げるなどし、地方公共団体のウェブサイトと誤解されかねないウェブサイトを構築することがあり、これを完全に防ぐことは困難である。このため、以下を例とする対策を実施する必要がある。
・正規のウェブサイトが検索サイトで上位に表示されるよう検索エンジン最適化の措置を実施する
・情報システム管理者は、庁外に提供するウェブサイトに関連するキーワードで定期的にウェブサイトを検索し、不審なサイトが検索結果に表示された場合は、検索サイト事業者に報告するなどの対策を実施する
・以前利用していたドメイン（旧ドメイン）を運用停止する場合は、第三者に再取得され元のウェブサイトへのアクセスを利用し、詐欺サイト等へ誘導されることのないようドメインを一定期間保持する。また、旧ドメインへのアクセスがあった際に後継となるサイト（後継サイトがない場合は終了を告知したページや団体トップページ等）へHTTP応答コード301を用いた転送を行うことで、旧ドメインが検索サイトの上位に表示される機会をできるだけなくすことが望ましい。詳細は「**Webサイト等の整備及び廃止に係るドメイン管理ガイドライン**」（平成30年3月30日 **各府省情報化統括責任者（CIO）連絡会議決定**）を参照されたい。