資料２－２

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10月10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。

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．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

＜政府統一基準改定に至った背景＞
委託先が運用するファイル共有ツールへの不正アクセスにより、当該事業者に委託していた政府機関等の情報が流出する事案が発生。サプライチェーンの複雑化に伴い、委託先などのサプライチェーンの脆弱な部分を起点としたサイバー攻撃によるリスクが増大している。

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。
- ✓ 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。　※業務委託に分類される
- ✓ 「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。

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

現行ガイドラインにおける外部委託及び外部サービスの分類

- ✓ 「業務委託」と「情報システムに関する業務委託」は区分されていない。
- ✓ クラウドサービス、ホスティングサービスは外部サービスに含まれており、SaaS・IaaS・PaaSはクラウドサービスの構成要素として例示されている。
- ✓ 情報セキュリティで取り扱う機器について、明確な区分で章立てがされていない。

	用語の定義		具体例
業務委託	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		➢ 情報システムの開発、構築及び運用業務 ➢ アプリケーション・コンテンツの開発業務 ➢ 業務運用支援業務（統計、集計、データ入力、媒体変換等） ➢ プロジェクト管理支援業務 ➢ 調査・研究業務（調査、研究、検査等）
外部サービス	機関等外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	要機密情報を取り扱う場合	➢ クラウドサービス ※構成要素：SaaS、PaaS、IaaS ➢ Ｗｅｂ会議サービス ➢ ＳＮＳ（ソーシャルネットワーキングサービス） ➢ 検索サービス、翻訳サービス、地図サービス ➢ ホスティングサービス
		要機密情報を取り扱わない場合	

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」に区分して記載するのはいかがか。
- ➢ **「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**こととしてはいかがか。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。

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

現行ガイドラインにおける「業務委託」に関する規定

第２編　例文　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、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、委託事業者において必要なセキュリティ対策が確保されていることを確認し、必要に応じて契約に基づき措置を講じる、とされている。

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のはいかがか。

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

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

＜政府統一基準改定に至った背景＞
クラウドサービスの利用が拡大し、調達時から開発、運用、廃棄に至るまでの一連のプロセスにおいてセキュリティ強化が求められており、広報等で利用するSNS等のクラウドサービスについても、安全に利用するための対策（適切な主体認証やアクセス制御等）を確認していくことが必要である。

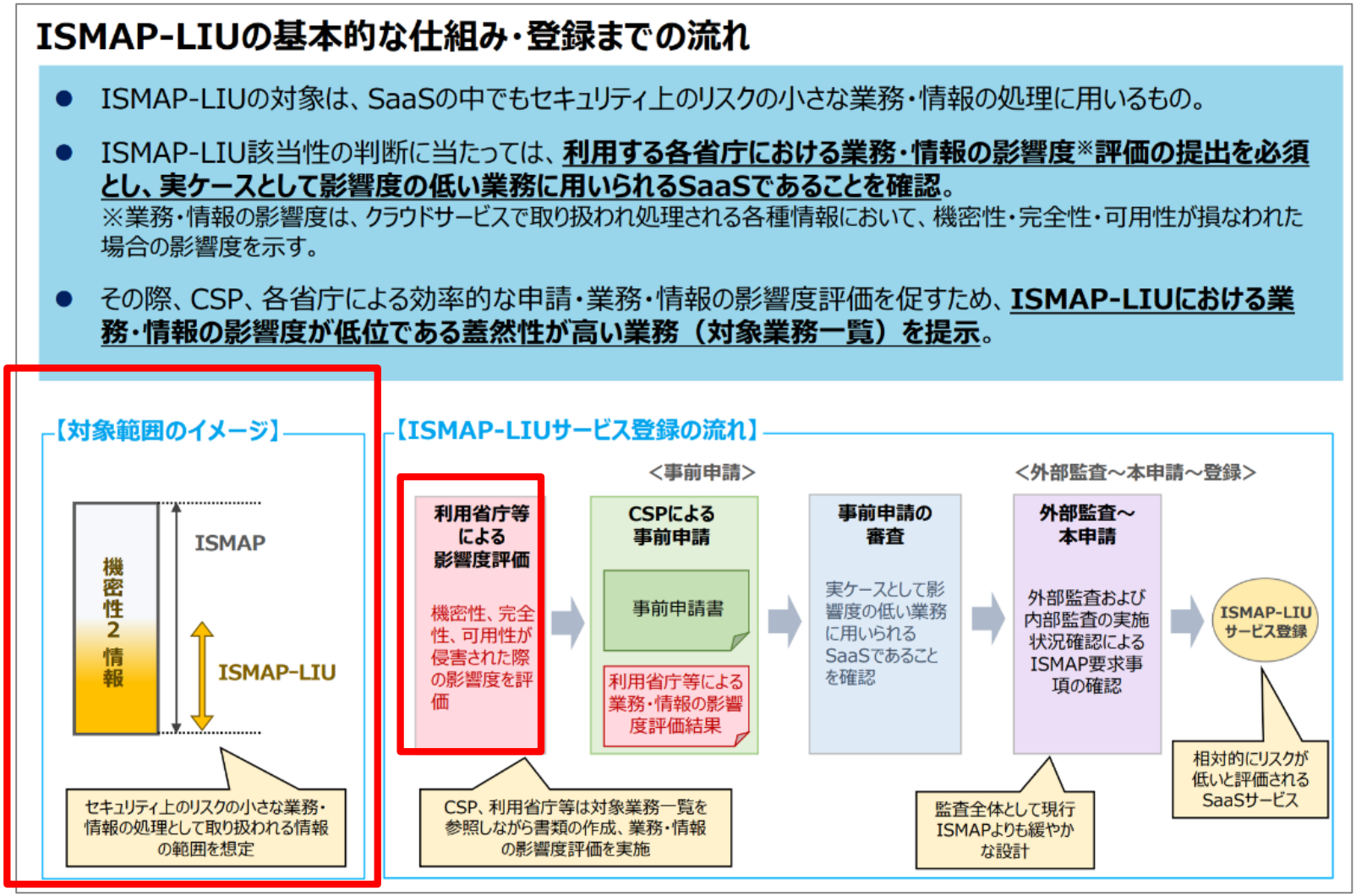
政府統一基準群の主な改定内容

- ✓ 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）

（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）

２．クラウドサービスの利用拡大を踏まえた対策の強化

ガイドラインにおける「ISMAP」に関する記載

第１編　総則　第４章

3.2. クラウドサービスの特性における留意事項

（中略）

●第三者認証

クラウドサービスを評価する場合に、第三者認証を活用することが考えられる。第三者認証は、ISMS（ISO/IEC27001）に加え、ISMAP又はクラウドサービスにおける第三者認証（ISO/IEC2701710、ISO/IEC2701811等）12の取得を確認する必要がある。また、事業継続の観点からは ISO22301（事業継続マネジメントシステムに関する国際規格）の取得を確認することが望ましい。

第３編　解説　第２章

8.2. 外部サービスの利用（機密性２以上の情報を取り扱う場合）

（中略）

（２）外部サービスの選定

（中略）

なお、選定条件となる認証には、ISO/IEC 27017 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 の管理基準を満たすことの確認やISMAP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外部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。

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つとするのはいかがか。
- 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つと位置付けるのはいかがか。

３．ソフトウェア利用時の対策の強化

3．ソフトウェア利用時の対策の強化

＜政府統一基準改定に至った背景＞
ソフトウェア設定不備に起因する情報漏えいインシデントや、正規のネットワーク監視ソフトウェアのアップデートを通じた攻撃など、ソフトウェアを標的としたサイバー攻撃が複雑化・巧妙化しており、米国でも、政府機関等のソフトウェア利用時のセキュリティ対策の強化が図られている。

政府統一基準群の主な改定内容

- ✓ 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．ソフトウェア利用時の対策の強化

現行ガイドラインにおける「ソフトウェア利用」に関する規定

第２編　例文　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

（１）情報システムの調達

(中略)

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、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

（２）情報システムの開発

(中略)

③システム開発に用いるハードウェア及びソフトウェアの管理

（ア）情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。

（イ）情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。

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のはいかがか。
- また、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のはいかがか。

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

＜政府統一基準改定に至った背景＞
昨今、ランサムウェア被害も多く発生しており、政府機関等においても、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が必要である。また、サービス不能攻撃（DDoS攻撃）が多く観測されており、ウェブサイト障害につながるおそれがある。

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に係る対策」の記載

第２編　例文　第２章
7．運用
7.1．情報システムの監視
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、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。

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
（中略）
③特権を付与されたIDの管理等

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の記載はない。

第４編　特則　第４章
6．技術的セキュリティ
〇アクセス制御
（中略）
⑦クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、クラウドサービスにアクセスさせなければならない。

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

現行ガイドラインにおける「情報システムの復旧に係る対策」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。

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。

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検討するのはいかがか。

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

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検討するのはいかがか。

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。

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

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。

ガイドライン改定の方向性

- ➢ **<u>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」</u>**に関し、**<u>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</u>**のはいかがか。

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

＜政府統一基準改定に至った背景＞

- 組織全体での情報システム等の資産管理、リスクの評価と対応、継続的な見直し・改善について、PDCAサイクルを通じた定着、組織横断的な課題の横展開など、ガバナンスの強化が求められている。
- 情報システムを取り巻く脅威動向や、インシデント発生時の業務影響度、社会的影響、取り扱う情報、機関等の組織特性等によって、通常のシステムと比してより高度な情報セキュリティ対策が必要となる情報システムが存在するため、高度な情報セキュリティ対策が要求される情報システムを判別するための基準（情報システムの分類基準）が必要となっている。

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。
- ✓ 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。

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のはいかがか。
- ➢ 現行の総務省ガイドラインにおいて、「三層の対策」により、住民の個人情報やマイナンバー等極めて重要な情報資産について、ネットワーク分離を行い、その他情報資産においても、外部接続の有無等に応じて追加的対策を設けている。従って、「三層の対策」によりネットワーク分離を行う対象を定め、対策の強弱を設けることで、情報システムの分類が一定程度なされていると考えられる。さらに、統一基準に沿って新たに情報システムの分類を設ける場合、既存の分類との関係性が不明確であり、地方公共団体の混乱を招く恐れがあることから、新たに情報システムの分類を設けない方向で検討を進めるのはいかがか。

政府共通利用型システムについて

＜政府統一基準改定に至った背景＞

- これまで統一基準では、政府共通プラットフォームを念頭に置いた「基盤となる情報システム」について、セキュリティ上留意すべき事項等を運用指針及びガイドラインにおいて示してきた。
- 他省庁が整備したシステムの利用が広がっていること、また、システムの利用形態が従来の定義には収まりきれないことから「政府共通利用型システム」として新たに定義した上で、当該システムの管理機関と利用機関の責任分界やそれぞれに必要となる対策等について、節を新設して整理した。

政府統一基準群の主な改定内容

- ✓ 「政府共通利用型システム」の管理機関は、管理機関と利用機関の責任分界、平常時及び非常時の協力・連携体制、非常時の具体的対応策を網羅した情報セキュリティ対策に関する運用管理規程を整備する。
- ✓ 利用機関は、管理機関が定める運用管理規程に基づき体制を整備、その他利用側でのセキュリティ対策を実施する。
- ✓ 提供を受ける機器等を直接利用する利用機関は、利用管理者を定め、運用規程の整備、提供を受けた機器等を把握するために必要な文書の整備、その他機器等の直接利用側でのセキュリティ対策を実施する。

政府共通利用型システムとは

他の機関等含め共通的に利用することを目的として、一つの機関等が管理・運用する情報システムであって、
①他の機関等が整備する情報システムに対し、同情報システムと連携して、情報システムのセキュリティ機能を提供する情報システム
②他の機関等に機器等を提供し、他の機関等の職員等が利用する情報システム
をいう。

ガイドライン改定の方向性

- ➢ NISCによると、「政府共通利用型システム」の例として、デジタル庁が、他の機関等（デジタル庁以外の機関等）に機器等を提供し、他の機関等の職員等が利用する情報システムであるGSS（ガバメントソリューションサービス）や、複数省庁の情報システムにセキュリティ機能（主体認証機能）を提供する「職員認証サービス（GIMA）」などが考えられる。このことを踏まえ、地方公共団体については、上記①②の定義に該当するサービスが全国的に使用されている例が確認されていないことから、今回の改定時に反映しないこととしてはどうか。
  ※　NISCによると、統一基準の対象外の組織**（具体的には地方公共団体など）**のみである場合は、政府共通利用型システムに該当しないと整理している。