資料１－１

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 月版)
（ICT 総合推進課・抜粋）

平成 13 年 3 月 30 日 策 定

令和 5 年 3 月２８ 日 改 定

総 務 省

第４章

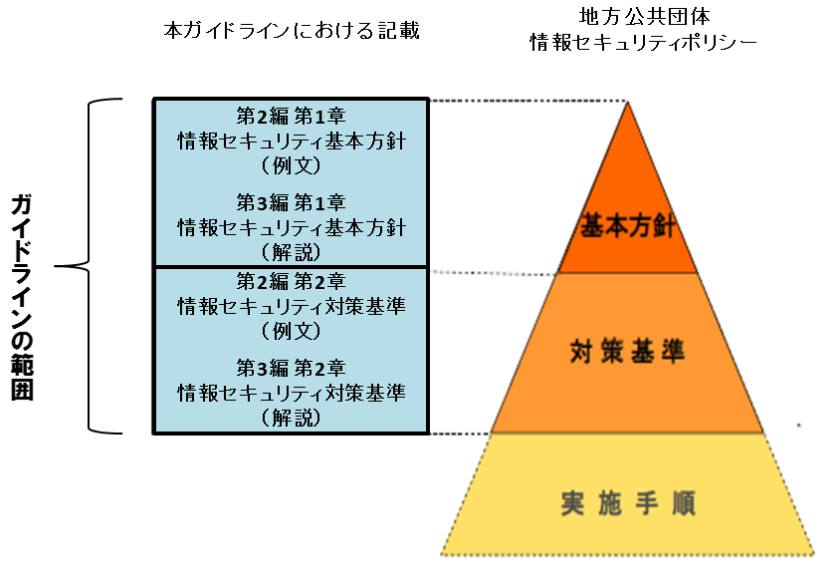
本ガイドラインの構成と対策レベルの設定及びクラウドサービスに関する留意点

（目次）

第4章　本ガイドラインの構成と対策レベルの設定及びクラウドサービスに関する留意点

1.　本ガイドラインの構成

本ガイドラインの構成は図表 9 のとおり、第 2 編 第 1 章が「情報セキュリティ基本方針」の例文、第 3 編 第 1 章が「情報セキュリティ基本方針」に関する解説、第 2 編 第 2 章が「情報セキュリティ対策基準」の例文、第 3 編 第 2 章が「情報セキュリティ対策基準」に関する解説となっている。



図表 9　本ガイドラインの構成と地方公共団体情報セキュリティポリシーの対応関係

2.　本ガイドラインにおける対策レベルの設定

地方公共団体において扱う情報資産の重要性や取り巻く脅威の大きさによって、必要とされる対策は一様でないことから、本ガイドラインでは、特段の理由がない限り対策を講じることが望まれる事項に加え、各地方公共団体において、その事項の必要性の有無を検討し、必要と認められる時に選択して実施することが望ましいと考えられる対策事項については、推奨事項として示している。推奨事項の項目を情報セキュリティポリシーに記載するか否かの判断は地方公共団体の裁量に委ねるが、記載した場合は遵守する必要があることに留意されたい。

各地方公共団体においては、組織の実態に合わせ、必要に応じて推奨事項も含めて、情報セキュリティポリシーを策定することが期待される。

3. 本ガイドラインにおけるクラウドサービスに関する全般的な留意点について

3.1. 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

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（2022年9月30日デジタル社会推進会議幹事会決定）において、クラウドサービスの利用メリットとして、「効率性の向上」、「セキュリティ水準の向上」、「技術革新対応力の向上」、「柔軟性の向上」、「可用性の向上」、といった５つのメリットがあるとしている。さらに、オンプレミス環境からクラウドサービスへ移行するだけでなく、クラウドサービスが保有するサービス（マネージドサービス）を活用することによって、環境構築の自動化や運用の自動化が可能となり、サーバ構築に伴うコストや手作業に係る工数を大きく削減することが可能となると記している。ただし、各クラウドサービス事業者が提供するクラウドサービスには、様々なサービスが存在するため、これらのメリットを享受できるサービスかどうかは、地方公共団体がそのサービスの内容や信頼性について慎重に検討を行い、見極める必要がある。そして、クラウドサービスの特性を十分に理解し、その利用の判断を行う必要がある。

以下にクラウドサービスの特徴[4]を示す。

- オンデマンド・セルフサービス
  クラウドサービス利用者は、必要に応じて自動的にコンピューティングリソースを設定し、利用が可能
- ブロードネットワークアクセス
  標準的なネットワークの仕組みを利用してアクセスが可能
- リソースプーリング
  利用者の需要に応じて、動的にクラウドサービス事業者のコンピューティングリソースが割り当てられる。物理的な所在場所に制約されない。
- スピーディな拡張性
  コンピューティングリソースの能力は、伸縮自在であり、場合によっては、自動で割り当て及び提供される。需要に応じてスケールアウト／スケールイン[5]可能
- 計測可能
  サービスの利用に応じて、従量課金・従量請求となる。

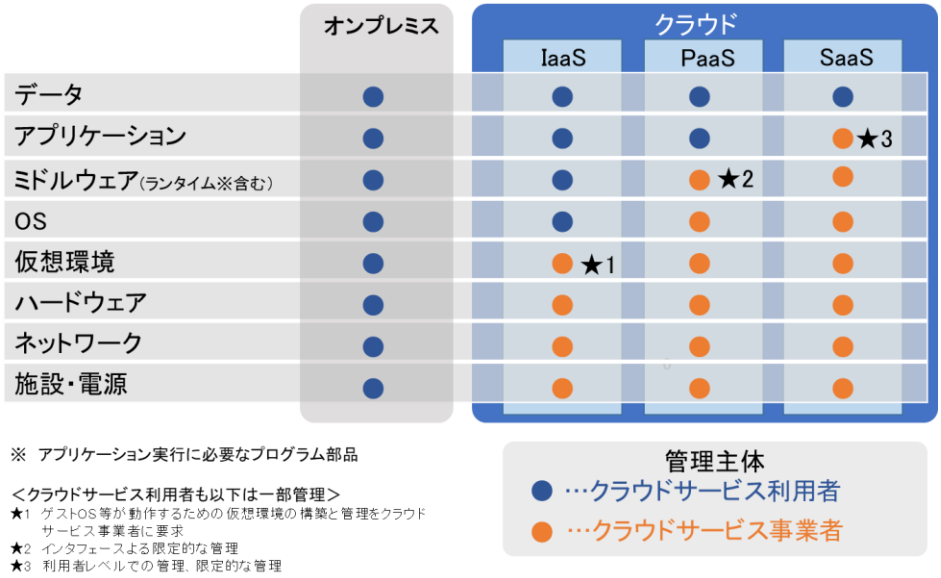
また、クラウドサービスは、様々なサービスモデルが存在する。例えば、NIST SP800-145では、次の３つのサービスモデルを定義している。これらのサービスモデルにより、クラウドサービス事業者の責任の範囲が異なる事に留意する。

[4] 米国国立標準技術研究所(NIST)では、情報セキュリティに関する研究や、各種文書・ガイドラインの発行している。クラウドサービスの特徴については、NIST Special Publication 800-145を参照。
[5] コンピューティングリソースを負荷状況に応じて自動で増減できること。

- IaaS（Infrastructure as a Service）クラウド上のネットワーク、CPU、メモリ、ストレージなどのコンピューティングリソースを利用するサービスとして提供されるインフラストラクチャであり、利用者には演算機能、ストレージ、ネットワークその他の基礎的コンピューティングリソースが提供される。
- PaaS（Platform as a Service）クラウド上の OS やミドルウェアなどのプラットフォームを利用するサービスであり、利用者には演算機能、ストレージ、ネットワークその他の基礎的コンピューティングリソースが提供される。
- SaaS（Software as a Service） クラウド上のソフトウェア／アプリケーションを利用するサービスであり、利用者には CSP[6]のインフラストラクチャ上で稼動している ASP[7]由来のアプリケーションが提供される。

なお、クラウドサービスの各サービスモデルにおけるクラウドサービス利用者とクラウドサービス事業者の責任に関する一般的な考え方については、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版） Ⅰ． ６．クラウドサービス事業者とクラウドサービス利用者の責任」に記載されている。

また、SaaS 型の場合、API（アプリケーション・プログラム・インタフェース）等で複数の SaaS 事業者間で水平連携している場合がある。これらの責任の分担に関する考え方は、総務省「クラウドサービス利用・提供における適切な設定のためのガイドライン」(2022 年 10 月)「Ⅱ．１．３ 環境の設定における留意すべきパターン ４．連携したクラウドサービスを提供する場合」に記載されているため、参考にされたい。



図表 10　クラウドサービス事業者の責任に関する一般的な考え方

[6] 各クラウドサービスを提供するサービス事業者である CSP（クラウドサービスプロバイダ）を指す。
[7] 各クラウドサービスを提供するサービス事業者である ASP（アプリケーションサービスプロバイダ）を指す。

サービスモデル区分	サービスモデルの特徴
IaaS／PaaS	・主にクラウドサービス上に、情報システムをクラウドサービス利用者が実装し、運用するケースに利用される。 ・組織のセキュリティ要求事項に対する評価が、比較的し易い。（ISMAP[8]におけるサービスリストの登録、第三者認証の取得や外部機関による監査報告書を開示可能なクラウドサービス提供事業者が多い。）
SaaS	・情報システムそのものをクラウドサービス事業者がサービスとして提供する。クラウドサービス利用者は、主にデータ、利用者 ID の管理（Identity and Access Management）に注力できる。 ・多種多様なサービスが存在する。 ・組織のセキュリティ要求事項に対する評価が、比較的難しい。（ISMAP におけるサービスリストの登録、第三者認証の取得や外部機関による監査報告書を開示可能な地方公共団体向けのアプリケーションサービスを提供しているクラウドサービス事業者が少ないため、そのサービスの情報セキュリティ対策の実態を確認することが難しい。）

図表 11　クラウドサービスの各サービスモデルの特徴

3.2. クラウドサービスの特性における留意事項

クラウドサービスは、一般向けに提供される汎用的なサービスをベースとしている。クラウドサービス利用者は、そうした汎用的なサービスを利用することで、情報システムの運用の効率化を図ることが出来る。ただし、以下のような特性とそれに伴う留意事項がある。

- 責任分担／責任共有

  図表 10 で示したとおり、クラウドサービス事業者とクラウドサービス利用者の責任が分担されクラウドサービスを利用することになる。このように、クラウドサービスのサービスモデルにより、各情報資産の管理における役割があるものの、クラウドサービスを利用して運用する情報システムのセキュリティ確保の責任は、一義的にクラウドを利用する側が負うものである。クラウドサービスの利用者は、利用するクラウドサービスについて、ユーザーとして適切な設定を行うことが当然に求められることに加えて、情報システム全体について、そのセキュリティリスクを分析し、適切な対策を行うことが求められる。そのため、利用するクラウドサービスが組み込まれる情報システムのセ

[8] 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

キュリティリスクを適切に把握した上で、クラウドサービスが提供するセキュリティ機能やセキュリティに係る提供情報を踏まえ、情報システム全体のセキュリティ対策を実施するとともに、セキュリティ確保についての最終的な責任を負わなければならない。したがって、クラウドサービスを利用する前に、そのクラウドサービスが、クラウドサービス利用者の組織における情報セキュリティの要求事項を満たすのか、評価を行い、クラウドサービスを利用する際のリスクの対応について、十分な検討が必要となる。

- 情報の非対称性

  クラウドサービスは、一般向けに提供される汎用的なサービスをベースにしているため、その詳細な情報は、クラウドサービス事業者が保有している。クラウドサービスにおける情報セキュリティ対策の状況等を評価する場合は、クラウドサービス利用者が、必要に応じて能動的にクラウドサービス事業者が公開している情報を得る必要がある。場合によっては、秘密保持契約書を締結し、監査報告書を入手して、情報セキュリティ対策の状況を確認する必要がある。また、一般社団法人日本クラウド産業協会(ASPIC)がクラウドサービス情報開示認定機関として、クラウドサービスのサービスモデル別に安全性・信頼性に係る情報開示認定制度[9]を実施しており、これらの情報も参考になる。

- 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/IEC27017[10]、ISO/IEC27018[11]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。SaaS 型のクラウドサービスでは、SasS 型のクラウドサービス自体の第三者認証に加え、プラットフォームとして利用している IaaS やデータセンターにおける第三者認証の取得状況について確認が必要となる場合がある点に留意する。また、第三者認証は、クラウドサービスにおける信頼の目安であり、サービスの品質を保証するものではないことに留意する。なお、サービスの品質の保証やクラウドサービス事業者の責任範囲は、契約（サービスレベル合意書：SLA[13]）において定める必要がある。

- データの保護、プライバシー

  クラウドサービスの各サービスモデルにおいて共通していることは、クラウ

[9] https://www.aspicjapan.org/nintei/index.html
[10] ISO/IEC 27002 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
[11] PII プロセッサ（個人識別情報委託先）としてパブリッククラウド内で個人情報を保護するための実施基準
[12] 国際標準の第三者認証以外では、JASA クラウドセキュリティ推進協議会 CS ゴールドマークがある。
https://jcispa.jasa.jp/cs_mark_co/cs_mark_co/
[13] Service Level Agreement の略

ドサービス利用者は、データの保護に関する対応が必要となることである。データが使用されている場合、データが転送されている場合、データが保存されている場合、各々において、機密性に応じたデータを保護する仕組みの検討等[14]が必要となる。また、クラウドサービスにおけるデータの保存場所が海外にある場合、その国の安全保障上の要請があれば、データの提出が求められる国内法が存在するケースがある。そのため、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[15]する必要があるが、SaaS 型の場合は、海外のプラットフォームを利用している場合があるため、最終的なデータの所在となる地域については、留意が必要である。なお、海外の IaaS／PaaS 型のサービスであっても日本国内の利用においては、国内のデータセンターのみで運用している場合があるため、クラウドサービス事業者が公開している情報やクラウドサービスを取り扱う事業者（クラウドサービス販売者）へ問合せをするなど十分に確認を行う。

3.3. 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

地方公共団体が利用するクラウドサービスは、複数のステークホルダーが存在する場合がある。地方公共団体は、これらのステークホルダーの役割と責任の範囲を把握し、明確にした上で、クラウドサービスを利用する際に必要となる契約を締結する。本編では、関係するステークホルダーについて、次のとおり定義する。

	項目	説明	備考
1	クラウドサービス利用者	クラウドサービスを利用する組織（地方公共団体）	クラウドサービス事業者等と利用における契約を行う。
2	クラウドサービス事業者 ・クラウドサービスプロバイダ（CSP） ・アプリケーションサービスプロバイダ（ASP）	クラウドサービスを提供する組織 ・クラウドサービスにおけるインフラストラクチャを提供する組織 ・クラウドサービスにおけるアプリケーションを提供する組織	CSP と ASP が一つの組織である場合もあれば、異なる組織の場合もある。

[14] 本ガイドライン第４編（３．情報システム全体の強靭性の向上（１）マイナンバー利用事務系④マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱いの解説）も参照されたい。
[15] 本ガイドライン第３編第８章 8.2.（１）外部サービスに係る規定（外部サービス利用判断基準）の整備及び 8.2.（２）外部サービスの選定②の解説も参照されたい。

	項目	説明	備考
3	クラウドサービス販売者	クラウドサービスを販売（契約代行）する組織	クラウドサービス事業者と同じ組織である場合もあれば、異なる場合もある。
4	クラウドサービス構築者	クラウドサービスを活用して情報システムを構築する組織	クラウドサービス事業者と同じ組織の場合もあれば、異なる場合もある。
5	クラウドサービス運用委託事業者	クラウドサービス上で構築された情報システムの運用保守等を支援する組織	クラウドサービス事業者又はクラウドサービス構築者と同じ組織である場合もあれば、異なる場合もある。

図表 12　クラウドサービスを利用する際に関係するステークホルダー

また、クラウドサービスは、複数のクラウドサービスを利用してサービスを提供している（以下「サプライチェーン」という。）場合があるが、このような場合、クラウドサービス全体の情報セキュリティレベルは、サプライチェーン（を構成する複数のクラウドサービス）のうち最も低いレベルのものに一致する特徴がある。これらの考え方とサプライチェーンのパターンの例については、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン（第３版）Ⅰ．７．サプライチェーン」に記載されている。ここでは、その記載内容に基づき、地方公共団体の情報システムにおけるクラウドサービスのサプライチェーンの一例を示す。（この例では、クラウドサービス事業者は、クラウドサービス販売者・クラウドサービス構築者・クラウドサービス運用委託事業者を兼ねている前提としている。）

- クラウドサービスのサプライチェーン例（クラウドサービス事業者 A 社は、住民向け健診予約システムをクラウドサービス事業者 B 社のプラットフォームを利用し開発、提供している。地方公共団体は、クラウドサービス事業者A社とサービス利用契約を締結している。）

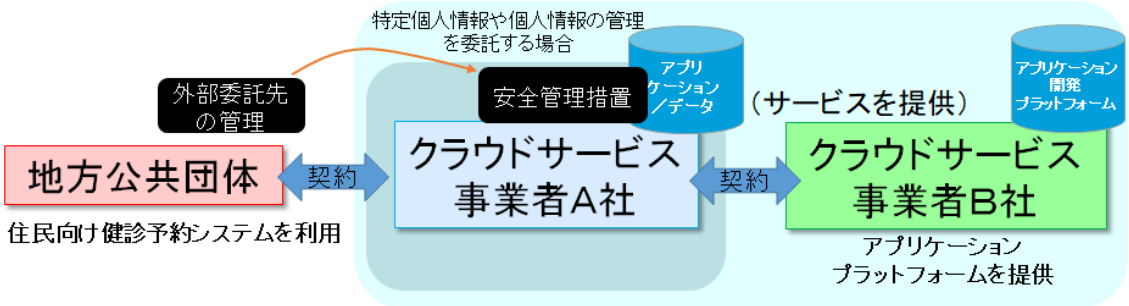
図表 13　クラウドサービスのサプライチェーン例の構成
（特定個人情報を扱わない場合）

- クラウドサービス事業者 A 社は、地方公共団体との契約者であることから、地方公共団体との契約に基づき、提供するクラウドサービス全体の管理責任を負う。
- クラウドサービス事業者 B 社は、クラウドサービス事業者 A 社との契約に基づきクラウドサービス事業者 B 社の管理責任の一部をクラウドサービス事業者 A 社に委譲する。クラウドサービス事業者 A 社は、クラウドサービス事業者 B 社との契約に基づきクラウドサービス事業者 B 社の管理責任の一部を引き継ぐ。
- 提供しているクラウドサービスにおいて、クラウドサービス事業者 B 社の管理範囲に帰する問題が発生した場合は、クラウドサービス事業者 A 社とクラウドサービス事業者 B 社との契約に基づき、対処する。

＜特定個人情報を扱う事業者に委託する場合の例＞

地方公共団体は、特定個人情報や個人情報を業務で利用している場合があり、特定個人情報については、番号法で安全管理措置[16]が定められている。

この例において、特定個人情報をクラウドサービスで扱う場合は、次のようなケースが考えられる。



図表 14　クラウドサービスのサプライチェーン例の構成
（特定個人情報を扱う場合）

[16] 番号法による安全管理措置の内容については、個人情報保護委員会「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）」に示されている。

- 特定個人情報を扱う情報システムをクラウドサービスで利用し、その業務運用をクラウドサービス事業者 A 社に委託する場合は、地方公共団体及びクラウドサービス事業者 A 社は、安全管理措置を行う。
- また、地方公共団体は、クラウドサービス事業者 A 社の委託先の管理が必要となる。なお、クラウドサービス事業者 B 社がプラットフォームの提供だけを実施しており、特定個人情報を取り扱わないことになっている場合は、地方公共団体の委託先にはならない[17]。

このように、クラウドサービスにおいては、複数のステークホルダーが存在することになるが、各クラウドサービス事業者が提供するクラウドサービスによって、その内容が異なるため、利用するクラウドサービスの構成を確認し、その役割と責任分担の範囲を明確にする必要がある。

3.4. クラウドサービスを利用する際のリスクの検討

クラウドサービスを利用する地方公共団体は、クラウドサービスの特徴とそのリスクを理解し、クラウドサービスを利用する前に、これらのリスクに対する対応可否を確認しなければならない。そして、地方公共団体は、必要となる情報セキュリティ対策について、情報資産のライフサイクル[18]（作成・入手・利用・保管・送信・運搬・提供・公表・廃棄等）の全般を通して行わなければならない。

とりわけ、クラウドサービス利用の前に最低限検討すべき事項の例を以下に示す。

- クラウドサービスを利用する場合における取り扱う情報資産の内容とライフサイクルにおける管理について
- クラウドサービスを利用する場合の自組織の運用体制について
- 利用を予定しているクラウドサービスが、自組織の情報セキュリティポリシーや業務（事業）継続に適しているかについて
- クラウドサービスの障害時に業務（事業）への影響が大きい場合は、業務（事業）継続計画を策定し、万が一の場合の対応の可否について

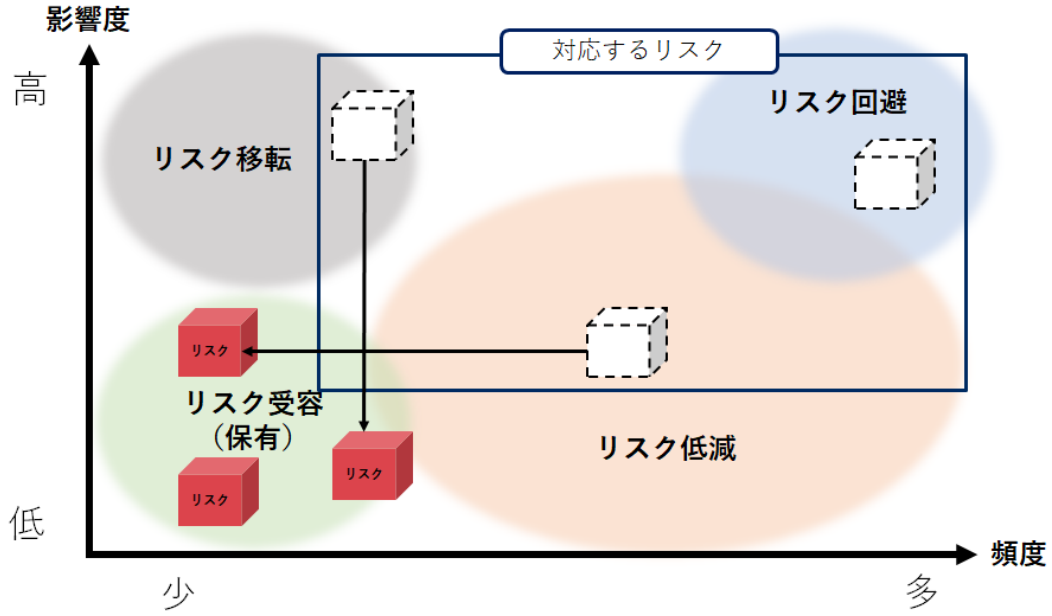
クラウドサービスで提供されるサービスの内容（機能等）とそのコストの検討と合わせて、上記内容を検討し、クラウドサービスにおける業務影響度合いとリスクの発生頻度を評価[19]する。そして、必要に応じてリスク低減等を行い、リスクが受容できるレベルに到達するよう対策を行う必要がある。このように、最終的なクラウドサービスの利用の判断は、地方公共団体が自ら実施する必要がある。

---

[17] 個人情報保護委員会 QA（Q7-53, A7-53）https://www.ppc.go.jp/all_faq_index/faq1-q7-53/

[18] 本ガイドライン第４編第４章 2.（２）情報資産の管理の解説も参照されたい。

[19] リスク回避：リスクの発生要因を無くすことでリスク自体を無くす（例：重要な情報については他のクラウドサービスやその他の方法を検討する）
リスク低減：セキュリティ対策することでリスクの発生頻度を下げる（例:情報資産の暗号化や通信経路の二重化等）
リスク移転：リスクを他者に移転する（例：サイバー保険への加入等））
リスク受容（保有）：許容範囲内のリスクであるため、新たなセキュリティ対策（リスク対応）はしない



図表 15　リスクの検討と対応イメージ

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）

（目次）

第１章

情報セキュリティ基本方針
（例文）

（目次）

第1章　情報セキュリティ基本方針（例文）

1.　目的

本基本方針は、本市が保有する情報資産の機密性、完全性及び可用性を維持するため、本市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定めることを目的とする。

2.　定義

（1）　ネットワーク

コンピュータ等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（2）　情報システム

コンピュータ、ネットワーク及び電磁的記録媒体で構成され、情報処理を行う仕組みをいう。

（3）　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（4）　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（5）　機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

（6）　完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（7）　可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく、情報にアクセスできる状態を確保することをいう。

（8）　マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

（9）　LGWAN 接続系

LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。

（１０）　インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

（１１）　通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安

全が確保された通信だけを許可できるようにすることをいう。

（１２） 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着が無い等、安全が確保された通信をいう。

3. 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（１） 不正アクセス、ウイルス攻撃、サービス不能攻撃等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（２） 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（３） 地震、落雷、火災等の災害によるサービス及び業務の停止等

（４） 大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（５） 電力供給の途絶、通信の途絶、水道供給の途絶等のインフラの障害からの波及等

4. 適用範囲

（１） 行政機関の範囲

本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局、消防本部及び地方公営企業とする。

（２） 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）

③情報システムの仕様書及びネットワーク図等のシステム関連文書

5. 職員等の遵守義務

職員、非常勤職員及び臨時職員等（以下「職員等」という。）は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティ実施手順を遵守しなければならない。

6. 情報セキュリティ対策

上記３の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

（１） 組織体制

本市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

（２） 情報資産の分類と管理

本市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

（３） 情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

①マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

②LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、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した上で、自治体情報セキュリティクラウドの導入等を実施する。

（４） 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パソコン等の管理について、物理的な対策を講じる。

（５） 人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

（６） 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。

（７） 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

（８） 業務委託と外部サービスの利用

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。

外部サービスを利用する場合には、利用に係る規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、利用するソーシャルメディアサービスごとの責任者を定める。

（９） 評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

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、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8. 情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティに関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

9. 情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策基準を策定する。

10. 情報セキュリティ実施手順の策定

情報セキュリティ対策基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティ実施手順は、公にすることにより本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。

（注）情報セキュリティ基本方針は、基本的事項を規定する形式で作成する必要がある。また、宣言書形式での情報セキュリティポリシー基本方針の作成は任意とする。これらの形式の詳細は「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）」の「第１章　情報セキュリティ基本方針（解説）」を参照されたい。

第２章

情報セキュリティ対策基準
（例文）

（目次）

第2章　情報セキュリティ対策基準（例文）

本対策基準は、情報セキュリティ基本方針を実行に移すための、本市における情報資産に関する情報セキュリティ対策の基準を定めたものである。

1. 組織体制

（1） 最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「CISO」という。）

①副市長を CISO とする。CISO は、本市における全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

②CISO は、必要に応じ、情報セキュリティに関する専門的な知識及び経験を有した専門家を最高情報セキュリティアドバイザーとして置き、その業務内容を定めるものとする。【推奨事項】

③CISO 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：Computer Security Incident Response Team、以下「CSIRT」という。）を整備し、役割を明確化する。

④CISO は、CISO を助けて本市における情報セキュリティに関する事務を整理し、CISO の命を受けて本市の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者（以下「副 CISO」という。）１人を必要に応じて置く。

⑤CISO は、本対策基準に定められた自らの担務を、副 CISO その他の本対策基準に定める責任者に担わせることができる。

（2） 統括情報セキュリティ責任者

①情報政策担当部長を CISO 直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は、CISO 及び副 CISO を補佐しなければならない。

②統括情報セキュリティ責任者は、本市の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③統括情報セキュリティ責任者は、本市の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

④統括情報セキュリティ責任者は、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。

⑤統括情報セキュリティ責任者は、本市の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セキュリティ侵害のおそれがある場合に、CISO の指示に従い、CISO

が不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。

⑥統括情報セキュリティ責任者は、本市の共通的なネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。

⑦統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、CISO、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

⑧統括情報セキュリティ責任者は、緊急時には CISO に早急に報告を行うとともに、回復のための対策を講じなければならない。

⑨統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて CISO にその内容を報告しなければならない。

（3）情報セキュリティ責任者

①内部部局の長、行政委員会事務局の長、消防長及び地方公営企業の局長を情報セキュリティ責任者とする。

②情報セキュリティ責任者は、当該部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。

③情報セキュリティ責任者は、その所管する部局等において所有している情報システムにおける開発、設定の変更、運用、見直し等を行う統括的な権限及び責任を有する。

④情報セキュリティ責任者は、その所管する部局等において所有している情報システムについて、緊急時等における連絡体制の整備、情報セキュリティポリシーの遵守に関する意見の集約並びに職員、非常勤職員及び臨時職員等（以下「職員等」という。）に対する教育、訓練、助言及び指示を行う。

（4） 情報セキュリティ管理者

①内部部局の課室長、内部部局の出張所等出先機関の長、行政委員会事務局の課室長、消防本部の課室長及び地方公営企業の課室長を情報セキュリティ管理者とする。

②情報セキュリティ管理者は、その所管する課室等の情報セキュリティ対策に関する権限及び責任を有する。

③情報セキュリティ管理者は、その所掌する課室等において、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セキュリティ侵害のおそれがある場合には、情報セキュリティ責任者、統括情報セキュリティ責任者及び CISO へ速やかに報告を行い、指示を仰がなければならない。

（５） 情報システム管理者

①各情報システムの担当課室長等を当該情報システムに関する情報システム管理者とする。

②情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

③情報システム管理者は、所管する情報システムにおける情報セキュリティに関する権限及び責任を有する。

④情報システム管理者は、所管する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

（６） 情報システム担当者

情報システム管理者の指示等に従い、情報システムの開発、設定の変更、運用、更新等の作業を行う者を情報システム担当者とする。

（７） 情報セキュリティ委員会

①本市の情報セキュリティ対策を統一的に実施するため、情報セキュリティ委員会において、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。

②情報セキュリティ委員会は、毎年度、本市における情報セキュリティ対策の改善計画を策定し、その実施状況を確認しなければならない。【推奨事項】

（８） 兼務の禁止

①情報セキュリティ対策の実施において、止むを得ない場合を除き、承認又は許可の申請を行う者とその承認者又は許可者は、同じ者が兼務してはならない。

②情報セキュリティ監査の実施において、止むを得ない場合を除き、監査を受ける者とその監査を実施する者は、同じ者が兼務してはならない。

（９） CSIRT の設置・役割

①CISO は、CSIRT を整備し、その役割を明確化しなければならない。

②CISO は、CSIRT に所属する職員等を選任し、その中から CSIRT 責任者を置かなければならない。また、CSIRT 内の業務統括及び外部との連携等を行う職員等を定めなければならない。

③CISO は、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。

④CISO による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供しなければならない。

⑤情報セキュリティインシデントを認知した場合には、CISO、総務省、都道府県等へ報告しなければならない。

⑥情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。

⑦情報セキュリティに関して、関係機関や他の地方公共団体の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部署、委託事業者等との情報共有を行わなければならない。

2. 情報資産の分類と管理

（1） 情報資産の分類

本市における情報資産は、機密性、完全性及び可用性により、次のとおり分類し、必要に応じ取扱制限を行うものとする。

機密性による情報資産の分類

分類	分類基準	取扱制限
機密性３	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	・支給以外の端末での作業の原則禁止（機密性３の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性２	行政事務で取り扱う情報資産のうち、秘密文書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	
機密性１	機密性２又は機密性３の情報資産以外の情報資産	－

完全性による情報資産の分類

分類	分類基準	取扱制限
完全性２	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、電子署名付与 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
完全性１	完全性２の情報資産以外の情報資産	－

可用性による情報資産の分類

分類	分類基準	取扱制限
可用性２	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	・バックアップ、指定する時間以内の復旧 ・電磁的記録媒体の施錠可能な場所への保管
可用性１	可用性２の情報資産以外の情報資産	－

（２） 情報資産の管理

①管理責任

（ア）情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。

（イ）情報セキュリティ管理者は、情報資産が複製又は伝送された場合には、複製等された情報資産も（１）の分類に基づき管理しなければならない。

②情報資産の分類の表示

職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適正な管理を行わなければならない。

③情報の作成

（ア）職員等は、業務上必要のない情報を作成してはならない。

（イ）情報を作成する者は、情報の作成時に（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

（ウ）情報を作成する者は、作成途上の情報についても、紛失や流出等を防止しなければならない。また、情報の作成途上で不要になった場合は、当該情報を消去しなければならない。

④情報資産の入手

（ア）庁内の者が作成した情報資産を入手した者は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

（イ）庁外の者が作成した情報資産を入手した者は、（１）の分類に基づき、当該情報の分類と取扱制限を定めなければならない。

（ウ）情報資産を入手した者は、入手した情報資産の分類が不明な場合、情報セキュリティ管理者に判断を仰がなければならない。

⑤情報資産の利用

（ア）情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。

（イ）情報資産を利用する者は、情報資産の分類に応じ、適正な取扱いをしなければならない。

（ウ）情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑥情報資産の保管

（ア）情報セキュリティ管理者又は情報システム管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。

（イ）情報セキュリティ管理者又は情報システム管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じなければならない。

（ウ）情報セキュリティ管理者又は情報システム管理者は、利用頻度が低い電磁的記録媒体や情報システムのバックアップで取得したデータを記録する電磁的記録媒体を長期保管する場合は、自然災害を被る可能性が低い地域に保管しなければならない。【推奨事項】

（エ）情報セキュリティ管理者又は情報システム管理者は、機密性２以上、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及

び耐湿を講じた施錠可能な場所に保管しなければならない。

⑦情報の送信

電子メール等により機密性２以上の情報を送信する者は、必要に応じ、パスワード等による暗号化[1]を行わなければならない。

⑧情報資産の運搬

（ア）車両等により機密性２以上の情報資産を運搬する者は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

（イ）機密性２以上の情報資産を運搬する者は、情報セキュリティ管理者に許可を得なければならない。

⑨情報資産の提供・公表

（ア）機密性２以上の情報資産を外部に提供する者は、必要に応じパスワード等による暗号化を行わなければならない。

（イ）機密性２以上の情報資産を外部に提供する者は、情報セキュリティ管理者に許可を得なければならない。

（ウ）情報セキュリティ管理者は、住民に公開する情報資産について、完全性を確保しなければならない。

⑩情報資産の廃棄等

（ア）情報資産の廃棄やリース返却等を行う者は、情報を記録している電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置しなければならない。

（イ）情報資産の廃棄やリース返却等を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。

（ウ）情報資産の廃棄やリース返却等を行う者は、情報セキュリティ管理者の許可を得なければならない。

3. 情報システム全体の強靭性の向上

（１） マイナンバー利用事務系

①マイナンバー利用事務系と他の領域との分離

[1] 電子メール等により情報を送信する場合の暗号化に用いるパスワードについては、本ガイドライン第３編第２章 2.（２）情報資産の管理の解説（注６）も参照されたい。

①統括情報セキュリティ責任者が違反を確認した場合は、統括情報セキュリティ責任者は当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

②情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者及び当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。

③情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨を CISO 及び当該職員等が所属する課室等の情報セキュリティ管理者に通知しなければならない。

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

①情報セキュリティ管理者は、委託事業者の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。

②情報セキュリティ管理者は、情報セキュリティマネジメントシステムの国際規格の認証取得状況、情報セキュリティ監査の実施状況等を参考にして、委託事業者を選定しなければならない。【推奨事項】

（2） 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要件を明記した契約を締結しなければならない。

・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
・委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
・提供されるサービスレベルの保証
・委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法
・委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び委託事業者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・市による監査、検査

・市による情報セキュリティインシデント発生時の公表
・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

（３） 確認・措置等

情報セキュリティ管理者は、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定期的に確認し、必要に応じ、(２)の契約に基づき措置を実施しなければならない。また、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じて CISO に報告しなければならない。

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）

（１） 外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は、以下を含む外部サービス（機密性２以上の情報を取り扱う場合）の利用に関する規定を整備すること。

①外部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 8.2 節において「外部サービス利用判断基準」という。)

②外部サービス提供者の選定基準

③外部サービスの利用申請の許可権限者と利用手続

④外部サービス管理者の指名と外部サービスの利用状況の管理

（２） 外部サービスの選定

①情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。

②情報セキュリティ責任者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めること。

（ア）外部サービスの利用を通じて本市が取り扱う情報の外部サービス提供者における目的外利用の禁止

（イ）外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制

（ウ）外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、本市の意図しない変更が加えられないための管理体制

（エ）外部サービス提供者の資本関係・役員等の情報、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供並びに調達仕様書による施設の場所やリージョンの指定

（オ）情報セキュリティインシデントへの対処方法

（カ）情報セキュリティ対策その他の契約の履行状況の確認方法
（キ）情報セキュリティ対策の履行が不十分な場合の対処方法
③情報セキュリティ責任者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含めること。
④情報セキュリティ責任者は、外部サービスの利用を通じて本市が取り扱う情報の格付等を勘案し、必要に応じて以下の内容を外部サービス提供者の選定条件に含めること。
（ア）情報セキュリティ監査の受入れ
（イ）サービスレベルの保証
⑤情報セキュリティ責任者は、外部サービスの利用を通じて本市が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて本市の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めること。
⑥情報セキュリティ責任者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本市に提供し、本市の承認を受けるよう、外部サービス提供者の選定条件に含めること。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断すること。
⑦情報セキュリティ責任者は、取り扱う情報の格付及び取扱制限に応じてセキュリティ要件を定め、外部サービスを選定すること。また、外部サービスのセキュリティ要件としてセキュリティに係る国際規格等と同等以上の水準を求めること。【推奨事項】
⑧情報セキュリティ責任者は、外部サービスの特性を考慮した上で、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めること。
⑨　統括情報セキュリティ責任者は、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、外部サービス提供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すること。

（３）外部サービスの利用に係る調達・契約

①情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者の選定基準及び選定条件並びに外部サービスの選定時に定めたセキュリティ要件を調達仕様に含めること。

②情報セキュリティ責任者は、外部サービスを調達する場合は、外部サービス提供者及び外部サービスが調達仕様を満たすことを契約までに確認し、調達仕様の内容を契約に含めること。

（４） 外部サービスの利用承認

①情報セキュリティ責任者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行うこと。

②利用申請の許可権限者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。

③利用申請の許可権限者は、外部サービスの利用申請を承認した場合は、承認済み外部サービスとして記録し、外部サービス管理者を指名すること。

（５） 外部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、外部サービスの特性や責任分界点に係る考え方等を踏まえ、以下を含む外部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すること。

（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

（ウ）開発時におけるセキュリティ対策

（エ）設計・設定時の誤りの防止

②外部サービス管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録すること。

（６） 外部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、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部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すること。

（ア）外部サービス利用方針の規定

（イ）外部サービス利用に必要な教育

（ウ）取り扱う資産の管理

（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

（カ）外部サービス内の通信の制御

（キ）設計・設定時の誤りの防止

（ク）外部サービスを利用した情報システムの事業継続

②情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏ま

え、外部サービスで発生したインシデントを認知した際の対処手順を整備すること。

③外部サービス管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録すること。

（７） 外部サービスを利用した情報システムの更改・廃棄時の対策

①統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスの利用を終了する際のセキュリティ対策を規定すること。

（ア）外部サービスの利用終了時における対策

（イ）外部サービスで取り扱った情報の廃棄

（ウ）外部サービスの利用のために作成したアカウントの廃棄

②外部サービス管理者は、前項において定める規定に対し、外部サービスの利用終了時に実施状況を確認・記録すること。

8.3. 外部サービスの利用（機密性２以上の情報を取り扱わない場合）

（１） 外部サービスの利用に係る規定の整備

統括情報セキュリティ責任者は、以下を含む外部サービス（機密性２以上の情報を取り扱わない場合）の利用に関する規定を整備すること。

（ア）外部サービスを利用可能な業務の範囲

（イ）外部サービスの利用申請の許可権限者と利用手続

（ウ）外部サービス管理者の指名と外部サービスの利用状況の管理

（エ）外部サービスの利用の運用手順

（２） 外部サービスの利用における対策の実施

①職員等は、利用するサービスの約款、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した上で機密性２以上の情報を取り扱わない場合の外部サービスの利用を申請すること。また、承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講ずること。

②情報セキュリティ責任者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。また、承認した外部サービスを記録すること。

9. 評価・見直し

9.1. 監査

（１） 実施方法

CISO は、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じ