資料３

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）

（目次）

第１章

情報セキュリティ基本方針
（解説）

（目次）

第1章　情報セキュリティ基本方針（解説）

地方公共団体における情報セキュリティ対策の基本的な考え方を示すものが情報セキュリティ基本方針である。地方公共団体としての基本的な取り組み事項として、セキュリティ対策を実施する目的、対象とする脅威、情報セキュリティポリシーが適用される行政機関や情報資産の範囲、職員等の義務、必要な情報セキュリティ対策の実施、情報セキュリティ対策基準の策定及び情報セキュリティ実施手順の策定等について、情報セキュリティ基本方針に示すものである。必要に応じて住民や外部機関に対して公開することが望ましい。

1.　目的

【例文】

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。

（解説）

ここでは、なぜ、情報セキュリティが必要なのか、情報セキュリティ対策を取り組む必要性について定めている。情報セキュリティとは、地方公共団体の情報資産を「機密性」、「完全性」、「可用性」に関わる脅威から保護することであり、これを目的としている。「機密性」、「完全性」、「可用性」については、情報セキュリティ基本方針の例文　「２．定義」に定義している。

2.　定義

【例文】

（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。

（解説）

情報セキュリティ基本方針及び情報セキュリティ対策基準で使用する情報セキュリティに関わる用語について、定義している。

3. 対象とする脅威

【例文】

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、外部委託管理の不備、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

（解説）

情報資産の「機密性」、「完全性」、「可用性」を脅かす脅威を明確にしている。

例文には、昨今、想定される脅威の例を挙げている。

4. 適用範囲

【例文】

（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

（解説）

情報セキュリティ対策について限られたリソースで最大限の効果が発揮できる様に、情報セキュリティポリシーを適用する行政機関及び情報資産の範囲を明確にして、対策の範囲を決める必要がある。

なお、教育委員会や市立病院等においては、「行政系ネットワーク」（マイナンバー利用事務系及び LGWAN 接続系）とは別に、「教育学習に利用するネットワーク」（校務系、学習系、校務外部接続系等）や「医療情報系ネットワーク」がある。これらのネットワークについては、セキュリティポリシーに関する対策基準のガイドラインが監督官庁において策定されている場合があり、その場合は本ガイドラインの対象外とするが、これらのネットワークが「行政系ネットワーク」（マイナンバー利用事務系及び LGWAN 接続系）

と分割されていない場合は、本ガイドラインが適用されるので注意が必要である。

実際には、各団体の実情に応じて適用させる行政機関を決定することになるが、それぞれの行政機関によって情報セキュリティ対策を進める必要があることに変わりはない。そのため、基本的に全ての行政を司る執行機関を対象とすることが望ましい。

情報セキュリティポリシーの対象とする情報資産の範囲と情報資産の例は下表に示す通りであるが、文書で対象としているのは、ネットワーク、情報システムで取り扱うデータを印刷した文書及びシステム関連文書である。これら以外の文書は、情報資産に含めていないが、文書管理規程等により適正に管理しなければならない。

文書一般を情報資産に含めなかったのは、従来電子データ等の管理と文書の管理が、一般に異なる部署、制度によって行われてきた経緯、実態を踏まえたものである。しかしながら、情報資産の重要性自体は、電子データ等と文書の場合で異なるものでないことから、情報セキュリティ対策が進んだ段階では、全ての文書を情報セキュリティポリシーの対象範囲に含めることが望ましい。

情報資産の種類	情報資産の例
①ネットワーク	通信回線、ルータ等の通信機器等
②情報システム	サーバ、パソコン、モバイル端末、汎用機、複合機、オペレーティングシステム、ソフトウェア等
③①・②に関する施設・設備	コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル等
④電磁的記録媒体	サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体、USB メモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等の外部電磁的記録媒体等
⑤ネットワーク及び情報システムで取り扱う情報	ネットワーク、情報システムで取り扱うデータ等（これらを印刷した文書を含む。）
⑥システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等

図表 10　情報資産の種類と例

5. 職員等の遵守義務

【例文】

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。

（解説）

職員等は、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に対する誤った認識や、遵守しなかったことで情報セキュリティインシデントが発生し、情報システム停止や情報漏えいといった重大事故につながる可能性があるため、情報セキュリティ対策を実施するにあたり、内容を十分理解し、それらを遵守する必要がある。

また、情報セキュリティポリシーの策定を行う者や、セキュリティ上の職責を担う者は、情報セキュリティポリシーを定めるだけではなく、職員等に対して十分に教育や啓発を行うことが望ましい。

なお、「職員等」とは、例示された者を含む全ての職員が該当するものである。

6. 情報セキュリティ対策

【例文】

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、外部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） 外部委託~~サービスの利用~~

外部委託する場合には、外部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、外部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。

~~約款による~~外部サービスを利用する場合には、利用にかか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。

（解説）

情報セキュリティ対策の基本方針について記載する。例文では、組織体制、情報資産の分類と管理方法、情報システム全体の強靭性の向上、物理的セキュリティ、人的セキュリ

ティ、技術的セキュリティ、運用、外部委託~~サービスの利用~~及び評価・見直しにおける情報セキュリティ基本方針を記載している。

7. 情報セキュリティ監査及び自己点検の実施

【例文】
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。

（解説）

情報セキュリティ上のリスクは、常に変化している。地方公共団体における情報セキュリティ対策もその変化に対応する必要がある。そのため、常に最新の情報セキュリティ関連の情報を収集する体制が必要であり、収集した情報を参考にして、現在の情報セキュリティポリシーの内容に不足している項目がないかどうかを評価しなければならない。

評価のためには、日常的に職員等へのモニタリングを行い、地方公共団体の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が運用の中で遵守されているかについて、職員等や外部の組織によって定期的又は必要に応じて確認しなければならないことを明確にしている。この際に、情報セキュリティポリシーが現場の状況に適合しているか、最新の法令や組織の現状を踏まえ、情報セキュリティポリシーに不備や不足はないか、なども考慮する必要がある。

8. 情報セキュリティポリシーの見直し

【例文】
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。

（解説）

情報セキュリティの監査及び自己点検の結果並びに内部及び外部の環境の変化から、定期的又は必要に応じて情報セキュリティポリシーを見直さなければならないことを明確にしている。情報セキュリティは、マネジメントの実施サイクル（PDCA サイクル）によって、実態に沿った内容になっているかを常にチェックし、絶えず見直し、改善を図る必要がある。

9. 情報セキュリティ対策基準の策定

【例文】

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。

(解説)

情報セキュリティ基本方針「６．情報セキュリティ対策」、「７．情報セキュリティ監査及び自己点検」及び「８．情報セキュリティポリシーの見直し」で示した情報セキュリティ対策について、遵守事項及び判断基準を定める必要がある。遵守事項及び判断基準は本ガイドラインの情報セキュリティ対策基準に記載している。情報セキュリティ対策基準は、公にすると、サイバー攻撃を受けるリスクがあるため、必要に応じて非公開にすることも考えられる。

10. 情報セキュリティ実施手順の策定

【例文】

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。

(解説)

情報セキュリティ対策基準を策定するとともに、その対策基準に対して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必要がある。情報セキュリティ実施手順は、公にすると、サイバー攻撃を受けるリスクが高くなってしまうため、非公開にする必要がある。

11. 宣言書の形式

(解説)

情報セキュリティ基本方針の記載形式には、地方公共団体が実施する情報セキュリティ対策の基本的事項を規定し、宣言書形式にしても良い。

冒頭で情報セキュリティ対策に取り組む必要性や理念を記載し、全庁的な推進体制、情報セキュリティ対策基準及び情報セキュリティ実施手順の策定、主要な情報セキュリティ対策の実施、職員等の情報セキュリティポリシー遵守義務等を規定している。

地方公共団体の長又は最高情報セキュリティ責任者が、情報セキュリティ対策に積極的に取り組むことを対外的に宣言することができる。

【宣言書の形式例】

情報セキュリティ基本方針（宣言書）

今日、インターネットをはじめとする情報通信ネットワークや情報システムの利用は生活、経済、社会のあらゆる面で拡大している。一方で、個人情報の漏えい、不正アクセスや新たな攻撃手法による情報資産の破壊・改ざん、操作ミス等によるシステム障害等が後を絶たない。また、自然災害によるシステム障害や疾病を起因とするシステム運用の機能不全にも備える必要がある。

本市は、市民の個人情報や行政運営上重要な情報など~~の重要な情報~~を多数取り扱っている。また、電子自治体の構築が進み、多くの業務が情報システムやネットワークに依存している。したがって、これらの情報資産を様々な脅威から防御することは、市民の権利、利益を守るためにも、また、行政の安定的、継続的な運営のためにも必要不可欠である。また、本市には、地域全体の情報セキュリティ基盤を強化していく役割も期待されている。

これらの状況を鑑み、本市における情報資産に対する安全対策を推進し、市民からの信頼を確保し、さらに地域に貢献するため、以下に積極的に取り組むことを宣言する。

（１） 情報セキュリティ対策に取り組むための全庁的な体制を確立する。

（２） 情報セキュリティ対策の基準として情報セキュリティ対策基準を策定し、その実行のための手順等を盛り込んだ実施手順を策定する。

（３） 本市の保有する情報資産を適正に管理する。

（４） 情報セキュリティ対策の重要性を認識させ、当該対策を適正に実施するために、職員等に対して必要な教育を実施する。

（５） 情報セキュリティインシデントが発生した場合又はその予兆があった場合に速やかに対応するため、緊急時対応計画を定める。

（６） 情報セキュリティ対策の実施状況の監査及び自己点検等を通して、定期的に対策の見直しを実施する。

（７） 全ての職員等は、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基本方針、情報セキュリティ対策基準及び情報セキュリティ実施手順を遵守する。

（８） 地域全体の情報セキュリティの基盤を強化するため、地域における広報啓発や注意喚起、官民の連携・協力等に積極的に貢献する。

令和〇〇年〇〇月〇〇日

〇〇市長（又は、最高情報セキュリティ責任者）

第２章

情報セキュリティ対策基準
（解説）

（目次）

第2章　情報セキュリティ対策基準（解説）

1.　組織体制

【趣旨】

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。このことから、情報セキュリティ対策のための組織体制、権限及び責任を規定する。

【例文】

（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、本ガイドラインに定められた自らの担務を、副 CISO その他の本ガイドライン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、や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、や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、外部の事業者等との情報共有を行わなければならない。

（解説）

各地方公共団体においては、図表 11 のような組織体制を構築して、以下のような情報セキュリティ対策に取り組むことを想定している。

・CISO・CSIRT の設置
・インシデント連絡ルートの多重化
・緊急時対応計画の見直し、緊急時対応訓練の実施及び要員へ適切な教育の実施
・標的型攻撃への対策

（注１）情報セキュリティ対策を確実に実施するには、組織体制を整備するとともに、必要な予算、人員などの資源を確保することが重要である。

（注２）情報セキュリティポリシーにおいて、誰がどのような権限及び責任を持っているのかを容易に把握できるよう一覧表で整理しておくことが望ましい。

（注３）情報セキュリティインシデントの発生時の連絡ルートは多重化することが望ましい。

（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。）

CISO は、地方公共団体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や情報セキュリティに関する権限及び責任を有する。

例文では、CISO が、情報資産の管理や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こととしているが、小規模の地方公共団体などにおいては、情報通信技術の活用による住民の利便性の向上及び行政運営改善等に関するものを統括する最高情報統括責任者（CIO：Chief Information Officer、以下「CIO」という。）

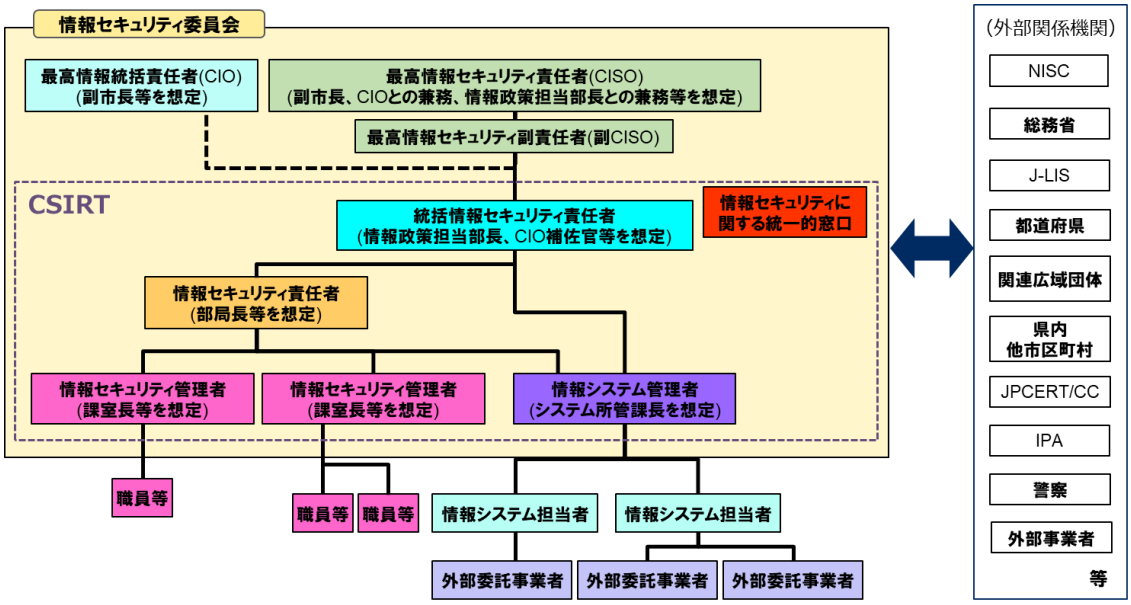
との兼務や情報政策担当部長との兼務など、柔軟な対応が必要となる。

また、適正に情報セキュリティ対策を講じていくには専門知識を必要とするため、内部の職員のみならず、情報セキュリティに関する外部の専門家を最高情報セキュリティアドバイザー（CISO の補佐）として置くことが望ましい。また、情報セキュリティインシデントに備える体制として CSIRT を設置する必要がある。

（注４）CISO 及び CIO は、副知事、副市長等、庁内を全般的に把握でき、部局間の調整や取りまとめを行うことができる上位の役職者をあてることが望ましい。

副 CISO は、CISO からの委任（CISO が自ら行うべき重要事項を除き、事務を任せること。任命及び監督の責任は、CISO に残る。）に基づき、CISO を助けて、市等の情報セキュリティ対策に係る事務を総括整理する役割を担う。

このため、情報セキュリティ対策について一定程度の専門性を有するとともに、CISO を助け、組織全体として整合性の取れた方針等の策定、人的資源及び予算等の計画的で持続可能な投入等を実施していく役割が求められる。



図表 11　情報セキュリティ推進の組織体制例

（２）　統括情報セキュリティ責任者

統括情報セキュリティ責任者は、地方公共団体のネットワークや情報システムの開発、設定の変更、運用、見直し等の権限及び責任を有するほか、情報セキュリティ対策に関する権限及び責任を有する。統括情報セキュリティ責任者は、情報通信技術に関する高度な専門的知識を有する者をあて、CISO の直属とすべきである。

CISO が不在の場合には、統括情報セキュリティ責任者がその権限を CISO に代わって行使できるよう、権限の委譲についても規定しておく。また、情報セキュリ

ティインシデント発生時等の緊急時には、統括情報セキュリティ責任者が中心となり、被害の拡大防止、事態の回復のための対策実施、再発防止策の検討を行う必要がある。

（注５）統括情報セキュリティ責任者には、具体的には情報政策担当部長、CIO 補佐官等が考えられる。

（３） 情報セキュリティ責任者

情報セキュリティ責任者は、各部局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。

（注６）情報セキュリティ責任者には、内部部局の長、各行政委員会事務局の長、消防長及び各地方公営企業の管理者をあてることが想定される。

（４） 情報セキュリティ管理者

情報セキュリティ管理者は、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。

情報セキュリティ管理者は、システムの利用現場の担当者であり、所管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又はセキュリティ侵害のおそれがある状況に直面する可能性が高い。そのため、このような場合を想定し、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 に対する報告義務を定める。

（注７）情報セキュリティ管理者には、内部部局の課室長、内部部局の出張所等出先機関の長、各行政委員会事務局の課室長、消防本部の課室長及び各地方公営企業の課室長をあてることが想定される。

（５） 情報システム管理者

情報システム管理者は、個々の情報システムの開発、設定の変更、運用、見直し等の権限及び責任を有するほか、所管する情報システムに対する情報セキュリティ対策に関する権限及び責任を負う。

個々の情報システムに関する情報セキュリティ実施手順の維持・管理は、情報システム管理者が行う。

（注８）情報システム管理者には、各情報システムの担当課室長等をあてることが想定される。

（６） 情報システム担当者

情報システム担当者とは、情報システム管理者の指示等に従う職員で、開発、設定の変更、運用、更新等の作業を行う。

（７） 情報セキュリティ委員会

情報セキュリティに関する重要事項を決定する機関として、情報セキュリティ委員会を設置する。情報セキュリティ委員会は、リスク情報の共有、情報セキュリティポリシーの決定等、情報セキュリティに関する重要な事項を決定する。

（注９）情報セキュリティ委員会の構成員は、CISO、CIO、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

理者等が想定され、定期的及び必要に応じて CISO が構成員を招集し、開催する。

（注１０）小規模の地方公共団体等においては、情報化推進委員会が情報セキュリティ委員会を兼ねるなど、地方公共団体の実情に応じた柔軟な運営が必要である。

（注１１）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付けることも可能である。

（８） 兼務の禁止

情報セキュリティ対策に係る組織において、申請者と承認者が同一であることや監査人と被監査部門の者が同一である場合は、承認や監査の客観性が担保されないため、兼務の禁止を定める。

「やむを得ない場合」とは、例えば、統括情報セキュリティ責任者のみに認められた承認について、統括情報セキュリティ責任者が申請する場合や小規模団体で代替する者がいない場合などをいう。

（９） CSIRT の設置・役割

情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、発生状況のとりまとめ、CISO・CIO への報告、報道機関等への通知・公表、関係機関との情報共有など、情報セキュリティインシデントに関するコミュニケーションの核となる体制を、危機管理等の既存の枠組み等を活用するなどして構築する必要がある。CISO は、コミュニケーションの核となる体制として CSIRT を整備し、その役割を明確化する必要がある。

CSIRT は、報告された事案について、その状況を確認し、情報セキュリティインシデントであるかの評価を行う。その結果、情報セキュリティインシデントであると評価した場合、統括情報セキュリティ責任者は、CISO に速やかに報告する。CSIRT は、被害の拡大防止等を図るため、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、応急措置の実施及び復旧に係る指示、勧告及び助言を行う。CSIRT は、CISO、総務省、都道府県等に報告し、情報システムの停止を含む必要な措置を講じる。CSIRT は、情報セキュリティインシデントに関する対処の内容を記録する必要がある。

また、CSIRT は、職員等に対して情報セキュリティインシデントの予防や啓発のための活動等を行うことが望ましい。

（注１２）CSIRT の設置においては、役割を明確にする必要があるため、以下を参考に構築や役割の明確化を実施することが望ましい。

・「情報セキュリティインシデント対応ハンドブック（令和 2 年 3 月版）」（地方公共団体情報システム機構）

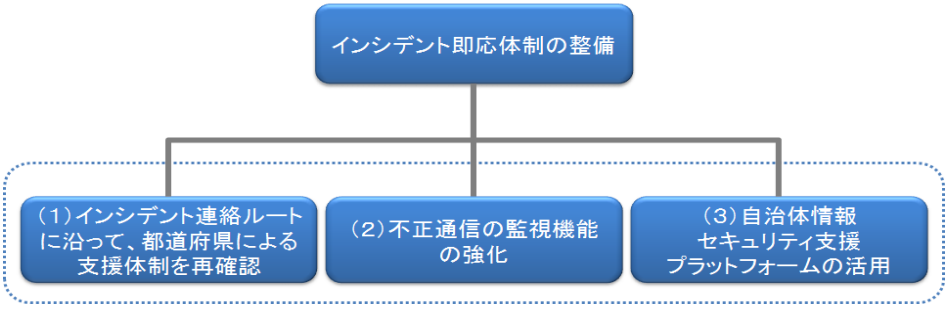
・「小規模自治体のための CSIRT 構築の手引き」（地方公共団体情報システム機構）

また、地方公共団体情報システム機構（自治体 CEPTOAR 事務局）等の関係機関や他の地方公共団体における同様の窓口機能、外部の事業者、有識者及び専門家等と連携して体制を強化するとともに、有事の際においても専門家との連携ができるようにしておくことが望ましい。

（注１３）一般的に情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、発生した情報セキュリティインシデントを正確に把握・分析し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とするための機能を有する体制を CSIRT と呼ぶ。CSIRT の持つ機能や在り方は組織によって様々であるが、まずは、地方公共団体においては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体制を整えることが重要である。

（注１４）情報セキュリティインシデントに関しては、単独で対応することが困難なケースもあること、また同様の被害拡大防止、発生の予防が重要であることから、インシデント即応体制は図表 12 の３つの視点から整備することが必要である。都道府県は、各都道府県内の市区町村における情報セキュリティインシデント発生時において、国への連絡を行うとともに、当該市区町村の情報セキュリティインシデント対応の支援を実施することが期待される。平常時から、都道府県と管内市区町村との間の連絡を密にして、各都道府県において、都道府県 CSIRT と市区町村 CSIRT の連携体制を構築しておくことが望ましい。

都道府県においては、自らの対策の充実とともに、市区町村に対する初動対応の支援体制の強化及び自治体情報セキュリティクラウドの構築等により、各市区町村における必要な情報セキュリティ水準の確保に努めることが望ましい。



図表 12　インシデント即応体制の整備例

（注１５）情報セキュリティインシデント発生時の連絡ルートは、インシデントの検知元により連絡ルートが異なるため注意すること。報告の際は、原則 LGWAN を利用すること。

（a）内閣官房内閣サイバーセキュリティセンター（NISC）が検知したイン

シデントの連絡ルート

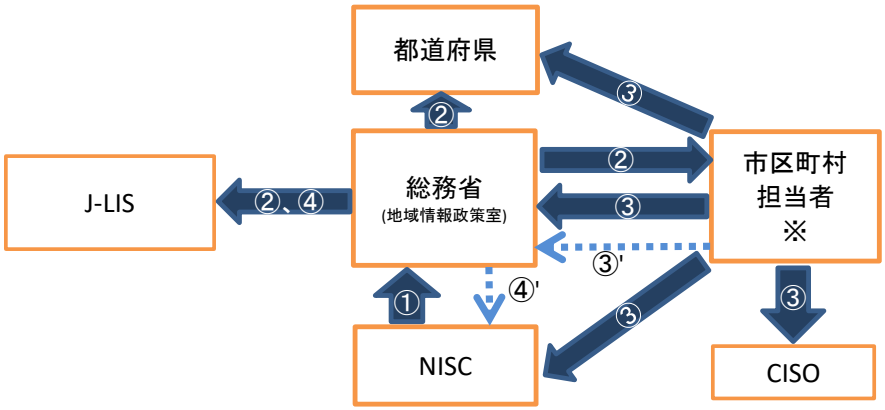
①NISC は、総務省に情報提供を行う。

②総務省は、インシデントが発生した自治体及び当該団体が所在する都道府県に情報提供を行う。また、必要に応じて J-LIS に情報提供する。

※サイバー攻撃（と考えられる事案を含む）に係るものについては全て情報提供を行う。

③インシデントが発生した市区町村（指定都市を含む）は、対応状況について速やかに都道府県、総務省、NISC 及び市区町村内 CISO に報告する。（都道府県においてインシデントが発生した場合も同様）

④総務省は、③の内容を必要に応じて J-LIS に情報提供する。

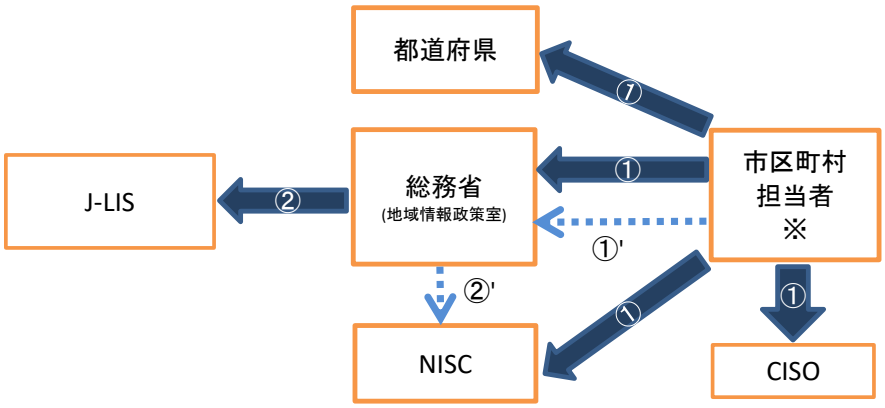


図表 13　NISC が検知したインシデントの連絡フロー

(b) 各地方公共団体が検知したインシデントの連絡ルート

①インシデントが発生した市区町村（指定都市を含む）は、対応状況について速やかに都道府県、総務省、NISC 及び市区町村内 CISO に報告する。（都道府県においてインシデントが発生した場合も同様）

②総務省は、必要に応じて J-LIS に情報提供する。



図表 14　各地方公共団体が検知したインシデントの連絡フロー

2. 情報資産の分類と管理

【趣旨】

情報資産を保護するには、まず情報資産を分類し、分類に応じた管理体制を定める必要がある。情報資産の管理体制が不十分な場合、情報の漏えい、紛失等の被害が生じるおそれがある。そこで、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する。

【例文】

（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、暗号化又はパスワード設定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、暗号化又はパスワードの設定を行う等、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、必要に応じ暗号化又はパスワードの設定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

（ア）情報資産の廃棄を行う者は、情報を記録している電磁的記録媒体が不要になった場合、記録されている情報の機密性に応じ、電磁的記録媒体の情報を復元できないように処置した上で廃棄しなければならない。

（イ）情報資産の廃棄を行う者は、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。

（解説）

（１） 情報資産の分類

情報資産について、機密性、完全性及び可用性を踏まえ、被害を受けた場合に想定される影響の大きさをもとに分類を行い、必要に応じ取扱制限を定める必要がある。

（注１）情報資産の分類は、機密性、完全性及び可用性に基づき、分類することが望ましいが、職員の理解度等に応じ、以下のような重要性に基づき分類することもあり得る。

重　要　性　分　類
Ⅰ　個人情報及びセキュリティ侵害が住民の生命、財産等へ重大な影響を及ぼす情報。
Ⅱ　公開することを予定していない情報及びセキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報。
Ⅲ　外部に公開する情報のうち、セキュリティ侵害が、行政事務の執行等に微妙な影響を及ぼす情報。
Ⅳ　上記以外の情報。

（２） 情報資産の管理

①管理責任

情報資産の管理は、その情報資産に係る実務に精通している者が行う必要があり、本ガイドラインでは、情報資産の管理責任者を情報セキュリティ管理者（課室長等）と想定している。

（注２）管理に当たっては、重要な情報資産について台帳を作成することが望ましい。これにより、情報資産の所在、分類、管理責任が明確になる。また、情報資産の管理について、管理者不在の状態や二重管理にならないように留意することが重要である。

②情報資産の分類の表示

（注３）情報システムについて、当該情報システムに記録される情報の分類を規定等により明記し、当該情報システムを利用する全ての者に周知する方法もある。

（注４）機密性２以上、完全性２、可用性２の情報資産についてのみ表示を行い、表示のない情報資産は、機密性１、完全性１、可用性１とする運用もある。

③情報の作成～⑩情報資産の廃棄

情報資産の取扱いについて遵守すべき事項は、情報のライフサイクルに着目し定める。情報のライフサイクルには、作成、入手、利用、保管、送信、運搬、提供、公表、廃棄等の局面がある。これらの局面ごとに、情報資産の分類に応じ取扱制限を定める。また、情報のライフサイクルの局面、情報資産の分類及び分類に応じた取扱制限については、定期的又は必要に応じて見直すことが重要である。なお、庁外の者が提供するアプリケーション・コンテンツに関する情報を告知する場合は、アプリケーション・コンテンツのリンク先の URL やドメイン名の有効性や管理する組織名等の必要情報を明記するなどの対策を講じることが必要である。

（注５）情報の提供、行政手続、意見募集等の行政サービスのためにアプリケーション・コンテンツを提供する場合は、利用者端末の情報セキュリティ水準の低下を招いてしまうことを避けるため、アプリケーション・コンテンツの作成に係る規定の整備やセキュリティ要件の策定等の情報セキュリティ対策を講じておく必要がある。

（注６）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、あらかじめ受信者と合意した文字列を用いるか、あるいは、電子メールで送信せずに電話などの別手段を用いて伝達することが望ましい。

3. 情報システム全体の強靭性の向上

【趣旨】

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、各地方公共団体においては、機密性はもとより、可用性や完全性の確保にも十分配慮された攻撃に強い情報システムが望まれる。

【例文】

（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

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(MAC アドレス、IP アドレス)及び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わなければならない。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、インターネット等から LGWAN-ASP を経由してマイナンバー利用事務系にデータの取り込みを可能とする。

②情報のアクセス及び持ち出しにおける対策

（ア）情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。また、業務毎に専用端末を設置することが望ましい。

（イ）情報の持ち出し不可設定

原則として、USB メモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

（2） LGWAN 接続系

①LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は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できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

（ア）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

（イ）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

（ウ）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

（３） インターネット接続系

①インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、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等の監視等の情報セキュリティ対策を講じなければならない。

②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するとともに、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しなければならない。

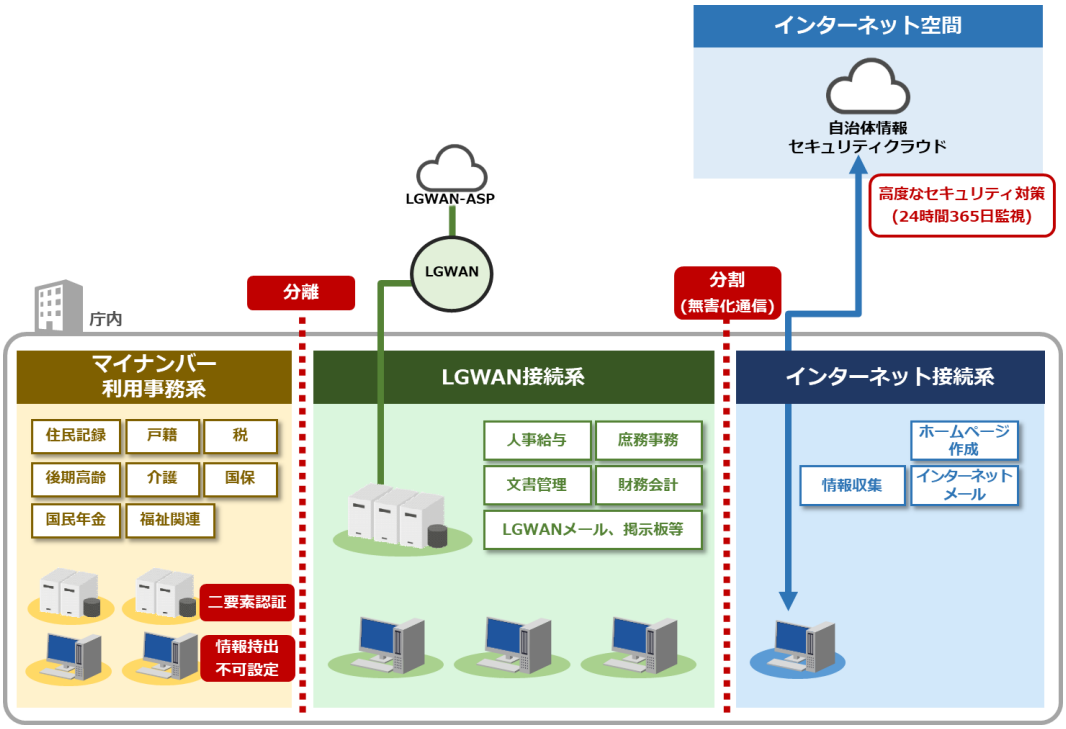
③（β モデルを採用する場合）業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末を置き、入札情報や職員の情報等重要な情報資産を LGWAN 接続系に配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

（β´モデルを採用する場合）業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末と入札情報や職員の情報等重要な情報資産を配置する場合、必要な情報セキュリティ対策を講じた上で、対策の実施について事前に外部による確認を実施し、配置後も定期的に外部監査を実施しなければならない。

（解説）

情報システム全体の強靭性の向上を図るため、情報セキュリティ対策の抜本的強化が必要であり、これを実現させる手法を「三層の構え」という。

三層の構えによる情報セキュリティ対策の詳細については、「新たな自治体情報セキュリティ対策の抜本的強化に向けて」（平成 27 年 11 月 24 日自治体情報セキュリティ対策検討チーム報告）及び「新たな自治体情報セキュリティ対策の抜本的強化について」（平成 27 年 12 月 25 日総行情第 77 号　総務大臣通知）等を参照されたい。



図表 15　三層の構えによる自治体情報システム例

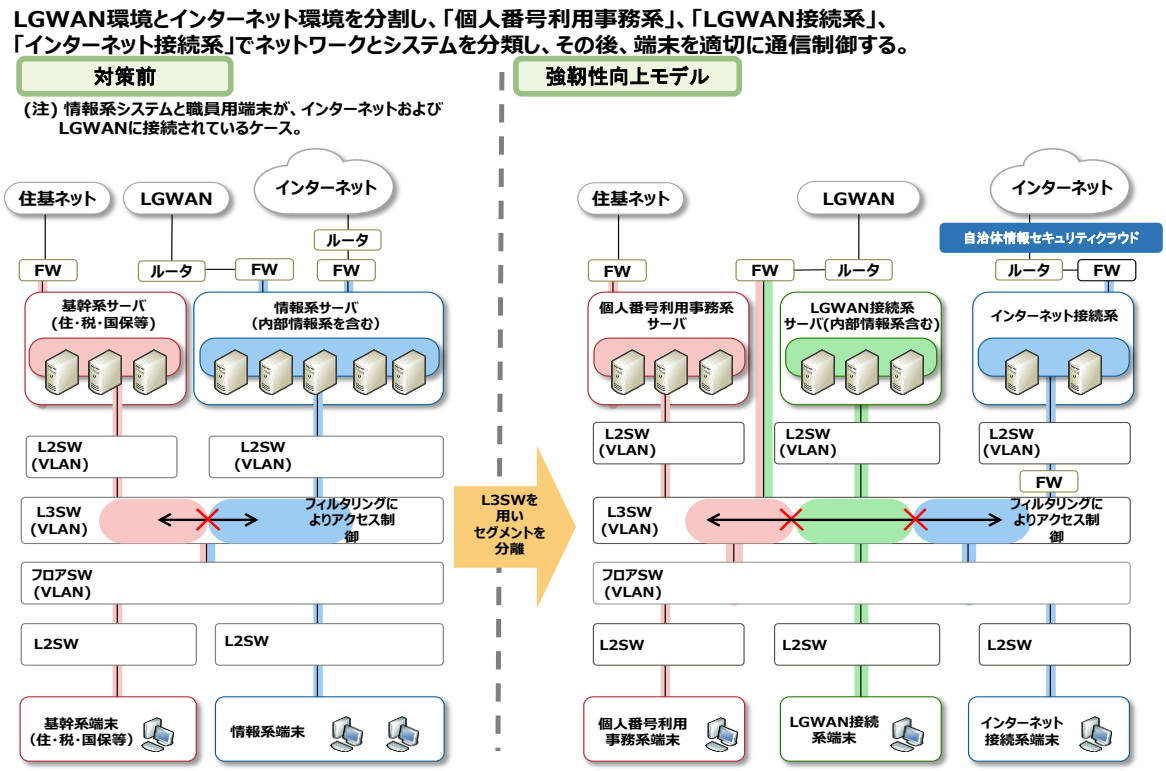
（1）　マイナンバー利用事務系

①マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系においては、住民情報の流失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しなければならない。統合パッケージシステムを利用している場合であっても、マイナンバー利用事務系と LGWAN 接続系との端末は分けなければならない。総合窓口を実施している場合等、業務毎に専用端末を設置することが難しい場合には、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を図り、利用状況をチェックする運用体制などを整備した上で実施することが望ましい。

マイナンバー利用事務系と LGWAN 接続系のサーバが仮想化基盤上にあり、物理的なサーバに共存している場合は、各系統の通信について、分離を徹底することが重要であることから、通信が分離されていることの確認を行わなければならない。

なお、地方公共団体が共同で利用するデータセンターに構築しているネットワークについても、庁内ネットワークとして同様の措置を行わなければならない。



図表 16　強靭性向上モデルにおけるネットワーク再構成の一つのイメージ

マイナンバー利用事務系と外部との通信の必要がある場合は、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わなければならない。これらの限定を行った通信を特定通信という。

特定通信を行う際は、以下の点に留意しなければならない。

（ア）・L2SW/L3SW による通信経路限定、ファイアウォールによる通信プロトコル限定等を行うことで通信を制限すること。

（イ）・その他外部ネットワークとの通信が発生する場合は専用回線サービス（IP-VPN や SSL-VPN など仮想技術を利用した通信を含む）を検討すること。

（ウ）・特定通信は、マイナンバー利用事務系が、住民基本台帳ネットワーク、中間サーバ連携、コンビニ交付や LGWAN-ASP サービスなど接続先が信頼される特定先との通信のことであり、マイナンバー利用事務系は、LGWAN 接続系やインターネット接続系と特定通信として接続してはならない。

特定通信となる外部接続の例として、住民基本台帳ネットワークシステム、マイナンバー制度における中間サーバ連携や住民票の写し等のコンビニ交付用の LGWAN 接続、データバックアップセンターや共同利用／クラウドセンター等、十分に情報セキュリティが確保された通信先との限定的な接続がある。また、特定

通信を行う外部接続先についても、インターネット等と接続されていてはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、LGWAN-ASP を経由してマイナンバー利用事務系にデータの取り込みを可能とする。

（注１）現在、国等の公的機関が構築したインターネットに接続されたシステム等で十分に安全性が確保された外部接続先との通信として eLTAX、ぴったりサービス（内閣府が整備するぴったりサービス（サービス検索・電子申請システム）に LGWAN-ASP を経由して接続する方式に限る。）、自治体情報セキュリティ向上プラットフォームが考えられる。これらの外部接続先から LGWAN-ASP を経由してマイナンバー利用事務系にデータを取り込む場合、特定通信を行う際の留意点に加え、以下の対策が必要である。

・~~（ア）~~外部接続先とは、連携サーバを設置して通信を行うこととする。外部接続先の LGWAN-ASP からのデータやファイルは、連携サーバを介してマイナンバー利用事務系へ転送（片方向）する。また、ファイアウォールやプロキシサーバ等でマイナンバー利用事務系から LGWAN-ASP に直接通信する経路が許可されないよう設定する。

・~~（イ）~~ファイアウォールや連携サーバで外部接続先との通信を制限（FQDN 指定）することで通信先を限定する。

・~~（ウ）~~許可されていないマイナンバー利用事務系の端末から LGWAN-ASP サービスへ接続することがないよう、ファイアウォールや連携サーバで通信を制限する。

・~~（エ）~~マイナンバー利用事務系のサーバ、端末については、ウイルス対策ソフトを導入し、最新の定義ファイルを常時更新する。また、OS の修正プログラムについては、マイナンバー利用事務系のシステムへの影響の大きさを踏まえ、更新を行う。端末については適時、修正プログラムを適用する。

・~~（オ）~~住民の情報を扱う場合は、外部接続先とは TLS プロトコルを利用し、認証、暗号化、改ざんの検知等の対策を実施する。これらの対策に加え、ファイアウォール及び連携サーバの通信の履歴等を取得することが望ましい。

（注２）（注１）の接続先以外の外部接続先については、やむを得ずインターネットとデータをやり取りする場合は、専用回線を新たに設置し、必要最小限の通信とし、外部のネットワークと通信する専用の端末を管理区域内に設置した上で、電磁的記録媒体を経由したデータのやり取りを行わなければならない。その際には情報システム管理者の許可を受けた上で、電磁的記録媒体の接続禁止設定を一時的に解除し、他の職員の立ち合い又は監視カメラで撮影された状態で、管理区域内において作業を行うなどの取扱いを行わなければ

ならない。

（注３）指定金融機関から税などの口座引落済みデータ（消し込みデータ）等の外部データを受信し、マイナンバー利用事務系へ取り込みを行う場合は、LGWAN-ASP 等を利用して受信しなければならない。マルウェア感染しているファイルをマイナンバー利用事務系に取り込んでしまうことを防止するため、以下の手順で取り込むことが考えられる。

・~~（ア）~~予め指定された職員等が、他の職員等の立ち合い又は操作が監視カメラで記録される管理区画等において、LGWAN 接続系端末でウイルスチェックを実施

・~~（イ）~~他の用途で使用されることのない専用の電磁的記録媒体に保存

・~~（ウ）~~システム管理責任者による電磁的記録媒体接続禁止の一時的解除

・~~（エ）~~マイナンバー利用事務系端末でウイルスチェックを実施後に取り込む

②情報のアクセス及び持ち出しにおける対策

（ア）情報のアクセス対策

認証手段には「知識」「所持」「存在」の種類が存在する。認証の種類と手段及び情報システムが正規の利用者かどうかを判断する手段を以下に示す。

種類	認証の手段
知識	正規の利用者“だけが知っている情報（知識)”をその人が知っているか否かで判断する
所持	正規の利用者“だけが持っているモノ（所持品)”をその人が持っているか否かで判断する
存在	正規の利用者の“身に備わっている特徴（利用者自身の存在)”でその人か否かを判断する

図表 17　認証の種類と手段

認証手段の概要と具体例		利点	欠点
「知識」を利用する手段	● パスワード ● パスフレーズ ● 暗証番号 ● ピクチャーパスワード	●運用コストが安い ●特別な装置が不要で、非常に簡便	● 複雑すぎる「知識」は記憶できない ● 簡単な「知識」さえあれば、正規の利用者でなくても、「知識」を推定して正規の利用者になりすますことができる ●「知識」忘失の恐れがある
「知識」と「所持」を併用	● IC カードと暗証番号の併用 ● ワンタイムパスワードトークンとパスワード（暗証番号）の併用 ● SIM カード（携帯電話／スマートフォンの固有番号）とパスワードの併用	● 「知識」と「所持」を併用することで、「知識」だけ、あるいは「所持」だけに頼るよりも安全性が高い	● カードやトークン等が必要で運用コストが高い ● カードやトークン等の盗難・紛失の恐れがある ● 「知識」忘失の恐れがある
「所持」を利用する手段	● IC カード ● USB トークン ● SIM カード（携帯電話／スマートフォンの固有番号）	●「知識」に頼らず、安全性を向上できる	● カードやトークン等が必要で運用コストが高い ● カードやトークン等の盗難・紛失の恐れがある ● 正規の利用者でなくても、何らかの手段（例えば盗難や偽造）でカードやトークン等を「所持」することができれば、情報システムは正規の利用者と誤認する

認証手段の概要と具体例		利点	欠点
「存在」を利用する手段	●バイオメトリックス認証（指紋、声紋、静脈等）	●「知識」や「所持」に頼らず、安全性を向上できる ●偽造がかなり困難 ●盗難・紛失の恐れがない	●特別な装置が必要で、運用コストが高い ●システム・装置によって認証精度に大きなばらつきがある ●認証データは本人固有の生体情報を基にして作られるため、万が一、認証データの漏えいや偽造が発生しても、認証データ自体を変えることができない
	●リスクベース認証（行動パターン、キーボードを使う時の癖など）	●行動パターンや癖などをまねるのは難しい ●完全に一致する行動パターンや癖が現れるのもかえって不自然と判断可能 ●盗難・紛失の恐れがない	●完全な利用者認証にはならない。“リスクベース”とは、行動パターンやキーボードを使う時の癖がいつもと違うことを検出した時に、“他人が利用しているかもしれない＝リスクの検知”と判断して、別の利用者認証を要求する、という意味 ●状態監視が常時必要なので、運用コストが比較的高い

図表 18　情報システムが正規の利用者かどうかを判断する認証手段

（注４）接続する端末を特定するために MAC アドレスの管理を行うことが望ましい。

（イ）情報の持ち出し不可設定

納付書など大量帳票のアウトソーシングや指定金融機関に対する口座振替情報の提供等の電磁的記録媒体の利用が止むを得ない場合においては、管理者権限を持つ職員によってその都度限定を解除する又は管理者権限を持つ職員のみに許可する設定とすることを例外として取り扱わなければならない。

USB メモリ等の電磁的記録媒体による端末からの情報持ち出しを行う場合は、次の手段により実施しなければならない。

・端末には利用許可された媒体のみ接続可能とすること。
・データは暗号化しパスワードを設定すること。
・利用媒体は、全て管理し利用履歴を残せること。
・データの受け渡しには、必ず情報セキュリティ管理者の承認と承認記録を残せること。

（２） LGWAN 接続系

①LGWAN 接続系とインターネット接続系の分割

分割とは、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できるようにすることをいう。

（ア）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

LGWAN 接続系へインターネットメールを転送する際には、インターネットメールの転送に必要な特定サーバ間以外の通信を遮断するとともに、LGWAN 環境とインターネット環境は SMTP 以外の Web 通信を始めとするプロトコルを遮断し、インターネットメールの添付ファイルの削除及び HTML メールのテキスト化を行う。

（イ）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

インターネット接続系の端末を仮想デスクトップ化し、LGWAN 接続系の端末から添付ファイルも含むメールの閲覧を可能とする。

（ウ）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

危険因子が埋め込まれたファイルを LGWAN 接続系に取り込んだ場合、脆弱性を突いた悪意あるコード等が実行される恐れがある。インターネット接続系から LGWAN 接続系にファイルを取り込む際は、以下のような手法により、危険因子をファイルから除去又は危険因子がファイルに含まれていないことの確認を行った上で、取り込まなければならない。（いずれかの手法のみ又は複数の手法を組み合わせて採用することが考えられる。）

・ファイルからテキストのみを抽出

・ファイルを画像 PDF に変換

・サービス等を活用してサニタイズ処理（ファイルを一旦分解した上で危険因子を除去した後、ファイルを再構築し、分解前と同様なファイル形式に復元する）

・インターネット接続系において内容を目視で確認するとともに、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェア等で危険因子が含まれていないことを確認

なお、上記のいずれか又は複数の手法による対策を実施した場合であっても、マルウェア等の除去が完全に保証されるものではないため、LGWAN 接続系において以下のようなセキュリティ対策を実施しなければならない。

・OS 等の修正プログラムの適時適用（自治体情報セキュリティ向上プ

ラットフォームの利用等）

・アンチウイルスソフトウェアの最新化（定義ファイルのアップデート等）

・業務に必要なファイルやメール等の定期的なバックアップの実施

また、上記の LGWAN 接続系における対策に加え、業務システムの停止を狙ったマルウェアの感染を防ぐ対策として、LGWAN 接続系端末にアプリケーションホワイトリストを設定し、実行できるアプリケーションの制限等を行うことを強く推奨する。

（注５）サニタイズ処理等を実現する手法は多岐にわたるため、適正な製品を選定し導入することが望ましい。

（注６）仮想デスクトップであれば、デスクトップ仮想方式、アプリケーション仮想方式など実現方法は問わない。なお、許可する通信は、画面転送用のプロトコルのみとし、その他の通信はすべて遮断し、インターネット接続系から LGWAN 接続系へマルウェア感染を防ぐ必要がある。

（３） インターネット接続系

①インターネット接続系で実施する情報セキュリティ対策の内容は具体的には以下のものがある。

（ア）サーバ等の監視

Web サーバ、メールリレーサーバ、プロキシサーバ、外部 DNS サーバのログの監視を行う。

（イ）情報セキュリティ機器の導入

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機器を導入する。

（ウ）情報セキュリティ運用監視

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を行う。

②自治体情報セキュリティクラウドの導入等による情報セキュリティ対策では、以下のような情報セキュリティレベルの向上とコスト削減が期待される。

・各市区町村において必要な情報セキュリティレベルの確保・向上

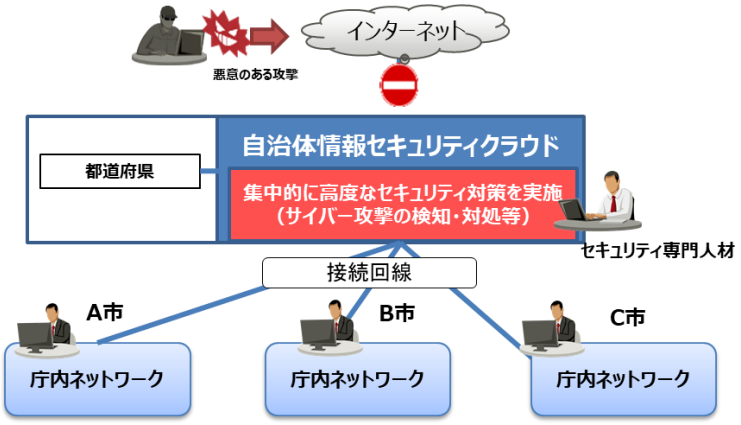
・情報セキュリティ専門人材によるインシデントの早期発見と対処

・機器・運用の共同利用によるコスト削減

（注７）都道府県及び市区町村のインターネットとの通信を監視するため、業務

に支障のない稼働が望まれる。情報セキュリティインシデントに対し迅速かつ適正に対応するために、セキュリティの専門人材が 24 時間 365 日有人で集中監視と分析を行う監視機能を持つ SOC（Security Operation Center）を設置し、インシデントの予兆を含め早期検知を図らなければならない。

（注８）「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」（令和 2 年 8 月 18 日総行情 109 号　総務省自治行政局地域情報政策室長通知）における標準要件等に基づき自治体情報セキュリティクラウドを導入しなければならない。なお、都道府県とは別に、市区町村において独自に自治体情報セキュリティクラウドの調達を行った場合は、市区町村の調達した自治体情報セキュリティクラウドが標準要件に基づいた機能を有すること及び運用がなされていることについて、定期的に外部監査を受けなければならない。



図表 19　自治体情報セキュリティクラウド

③業務の効率性・利便性の向上を目的として、インターネット接続系に主たる業務端末・システムを配置する場合、以下のモデルが考えられる。

・β モデル：インターネット接続系に主たる業務端末を置き、入札情報や職員の情報等重要な情報資産は LGWAN 接続系に配置する方式・・・（ア）

・β’モデル：インターネット接続系に主たる業務端末と入札情報や職員の情報等重要な情報資産を配置する方式・・・（イ）

（注９）β’モデルで取り扱う重要な情報資産とは、機密性~~レベル~~３に該当する秘密情報に相当する機密性を要する情報資産を想定する。なお、インターネット接続系に職員のマイナンバー情報を配置する場合には、情報の取扱いに十分留意し、アクセス制御等のセキュリティ対策を適正に実施する必要がある。

これらのモデルは、クラウドサービスの活用、テレワーク、民間事業者とのやり取り等でメリットがある一方、インターネットからのリスクも増加することとなる。ま

た、サイバー攻撃の高度化・複雑化により、自治体情報セキュリティクラウド側でのファイアウォールや IPS/IDS 等の防御による対策だけでは、マルウェアの侵入等を防ぐことが困難となっている。

このため、特に、これらのモデルを採用する自治体においては、インターネット接続系に配置する情報の重要性を踏まえ、各端末（エンドポイント）でのセキュリティ対策や不正な挙動等を検知し、早期対処する仕組みを構築する必要がある。早期検知のための仕組みの構築には EDR（Endpoint Detection and Response）ソフトウェア等の導入が有効である。EDR ソフトウェア等は、従来のパターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動の端末を監視・検出・特定する。また、異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施する。さらに、インシデント発生要因の詳細な調査を実施することで、検知、復旧等の早期対処を可能とする。

さらにまた、情報資産単位でのアクセス制御、監視体制や CSIRT など緊急時即応体制の整備、個々の職員のリテラシー向上など人的セキュリティ対策が必須となる。

また、β モデル又は β’モデルを採用する場合は、従来モデル（α モデル）と比較してインターネットからのリスクが増加し、より高度なセキュリティ対策の確実な実施が必要になることから、インターネット接続系と LGWAN 接続系を完全に分離する場合を除き、その実施について事前に外部による確認を実施し、その確認の報告書を地方公共団体情報システム機構に提出することとする。また、その後も定期的に外部監査を実施することとし、その監査報告書を地方公共団体情報システム機構に提出することとする。なお、外部による事前確認や外部監査を行う者については、監査の対象となる情報資産に直接関与しない者であることが望ましい。

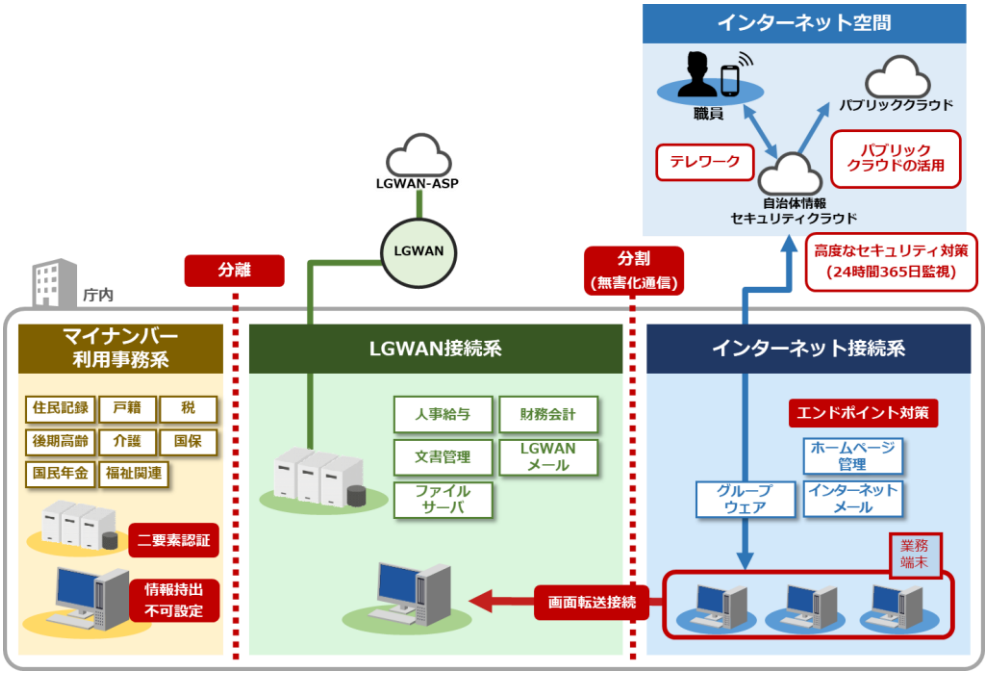
具体的には、以下の（ア）、（イ）のとおり、対策を実施しなければならない。

（ア）β モデル：インターネット接続系に主たる業務端末を置き、入札情報や職員の情報等重要な情報資産は LGWAN 接続系に配置する方式

本モデルは、業務システムを LGWAN 接続系に残しつつ、業務端末及びグループウェア等をインターネット接続系に配置し、画面転送により LGWAN 接続系業務システムを利用できるようにしたモデルである。本モデルにおいては、以下の図表に記載された対策を講じなければならない。

対策区分	セキュリティ対策	概要
技術的対策	無害化処理	・ファイルからテキストのみを抽出、ファイルを画像PDFに変換、サニタイズ処理、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェアで危険因子の有無を確認するなどの方法を用いて、危険因子が無いことを確認した上で、LGWAN接続系にインターネット接続系からファイルを取り込む。
	LGWAN接続系の画面転送	・インターネット接続系の業務端末からLGWAN接続系のサーバや端末を利用する場合は、仮想化されたリモートデスクトップ形式で接続する。 ・LGWAN接続系からインターネット接続系へのデータ転送(クリップボートのコピー&ペースト等)は禁止とする。ただし、LGWANメールやLGWAN-ASPから取り込み、業務で必要となるデータの転送については、中継サーバやファイアウォール等を設置し、通信ポート、IPアドレス、MACアドレス等で通信先を限定することで可能とする。
	未知の不正プログラム対策 （エンドポイント対策）	・従来のパターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動の端末を監視・検出・特定する。また、異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施する。さらにインシデント発生要因の詳細な調査を実施する。
	業務システムログ管理	・インシデントの兆候検知や、インシデント発生後の調査に使用するため、LGWAN接続系の業務システムのログの収集、分析、保管を実施する。
	脆弱性管理	・OSやソフトウェアのバージョンなどを漏れなく資産管理し、脆弱性の所在を効率的に把握する。また、深刻度に応じて修正プログラムを適用し、ゼロデイ攻撃等のソフトウェアの脆弱性を狙った攻撃に迅速に対応する。
組織的・人的対策	組織的なセキュリティ対策基準の遵守	・インターネット接続系とLGWAN接続系を完全に分離する場合を除き、必要なセキュリティ対策が実施されていることについて、事前に外部による確認を実施し、その確認の報告書を地方公共団体情報システム機構に提出する。また、その後も定期的に外部監査を実施することとし、その監査報告書を地方公共団体情報システム機構に提出する。
	住民に関する情報をインターネット接続系に保存させない規定の整備	・住民の名簿など、住民の個人情報をインターネット接続系に保存しない規定を整備するとともに、運用を徹底する。
	本ガイドライン対策基準（例文）「１．組織体制　（９）CSIRTの設置・役割」「５.人的セキュリティ」記載の組織的・人的対策の必須事項の確実な実施に加え、以下の対策を実施する。 ・職員等が毎年度最低1回は情報セキュリティ研修を受講可能となる研修計画の策定 ・職員等の実践的サイバー防御演習（CYDER）の受講 ・演習等を通じたサイバー攻撃情報やインシデント等への対策情報の共有 ・本ガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し	

図表 20　β モデルにおける必須のセキュリティ対策について



図表 21　β モデルイメージ図

（イ）β’モデル：インターネット接続系に主たる業務端末と重要な情報資産を配置する方式

本モデルは、β モデルと同様に業務端末及びグループウェア等をインターネット接続系に配置し、さらに入札情報や職員の情報等重要な情報資産をインターネット接続系に配置するモデルである。本モデルにおいては、以下の図表に記載された対策を講じなければならない。

対策区分	セキュリティ対策	概要
技術的対策	無害化処理	・ファイルからテキストのみを抽出、ファイルを画像PDFに変換、サニタイズ処理、未知の不正プログラムの検知及びその実行を防止する機能を有するソフトウェアで危険因子の有無を確認するなどの方法を用いて、危険因子が無いことを確認した上で、LGWAN接続系にインターネット接続系からファイルを取り込む。
	LGWAN接続系の画面転送	・インターネット接続系の業務端末からLGWAN接続系のサーバや端末を利用する場合は、仮想化されたリモートデスクトップ形式で接続する。 ・LGWAN接続系からインターネット接続系へのデータ転送(クリップボートのコピー&ペースト等)は禁止とする。ただし、LGWANメールやLGWAN-ASPから取り込み、業務で必要となるデータの転送については、中継サーバやファイアウォール等を設置し、通信ポート、IPアドレス、MACアドレス等で通信先を限定することで可能とする。
	未知の不正プログラム対策 （エンドポイント対策）	・従来のパターンマッチング型の検知に加えて、セキュリティ専門家によるマネージドサービスの運用により、エンドポイントのアクティビティを監視し、未知及び既知のマルウェア等による悪意ある活動を示す異常な挙動の端末を監視・検出・特定する。また、異常な挙動を検出した際にプロセスを停止し、ネットワークから論理的な隔離を実施する。さらにインシデント発生要因の詳細な調査を実施する。
	業務システムログ管理	・インシデントの兆候検知や、インシデント発生後の調査に使用するため、業務システムのログの収集、分析、保管を実施する。
	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。
	脆弱性管理	・OSやソフトウェアのバージョンなどを漏れなく資産管理し、脆弱性の所在を効率的に把握する。また、深刻度に応じて修正プログラムを適用し、ゼロデイ攻撃等のソフトウェアの脆弱性を狙った攻撃に迅速に対応する。
組織的・人的対策	セキュリティの継続的な検知・モニタリング体制の整備	・標的型攻撃訓練や研修等の職員等の受講状況や結果を確認し、セキュリティ対策の浸透状況や効果を測定する。測定した結果をもとに改善につなげていく。
	組織的なセキュリティ対策基準の遵守	・インターネット接続系とLGWAN接続系を完全に分離する場合を除き、必要なセキュリティ対策が実施されていることについて、事前に外部による確認を実施し、その確認の報告書を地方公共団体情報システム機構に提出する。また、その後も定期的に外部監査を実施することとし、その監査報告書を地方公共団体情報システム機構に提出する。
	住民に関する情報をインターネット接続系に保存させない規定の整備	・住民の名簿など、住民の個人情報をインターネット接続系に保存しない規定を整備するとともに、運用を徹底する。
	情報セキュリティ研修、標的型攻撃訓練、セキュリティインシデント訓練の受講	・職員等は情報セキュリティ研修、標的型攻撃訓練を年1回以上受講する。また、情報システム管理者、情報システム担当者はセキュリティインシデントが発生した場合の訓練を年１回以上受講する。
	本ガイドライン対策基準（例文）「１．組織体制　（９）CSIRTの設置・役割」「５.人的セキュリティ」記載の組織的・人的対策の必須事項の確実な実施に加え、以下の対策を実施する。 ・職員等が毎年度最低1回は情報セキュリティ研修を受講可能となる研修計画の策定 ・職員等の実践的サイバー防御演習（CYDER）の受講 ・演習等を通じたサイバー攻撃情報やインシデント等への対策情報の共有 ・本ガイドライン等の見直しを踏まえた情報セキュリティポリシーの見直し	

図表 22 β’モデルにおける必須のセキュリティ対策について

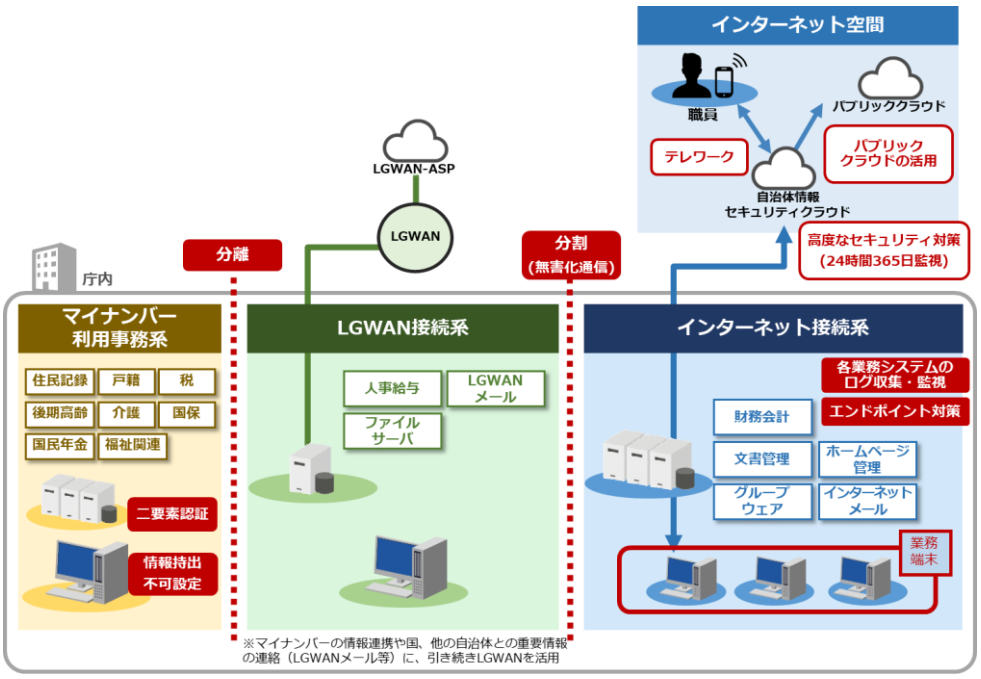
また、β’モデルについては、定期的な脆弱性診断、プラットフォーム診断等の実施が有効である。加えて、情報漏えいに対する対策として、以下の対策も有効である。

・万一ファイルが外部に漏えいしても解読できないよう、データベースやファイル

の暗号化

・組織が定義したポリシーに従ってデータへの操作を監視・制限し情報の流出を防止（Data Loss Prevention）

・組織が許可していない外部接続先のサービスへのアクセスを監視、遮断



図表 23 β'モデルイメージ図

（注１０）未知の不正プログラムへの対策（エンドポイント対策）

未知の不正プログラム対策として、OS のプロセスやメモリ、レジストリへの不正なアクセスや書き込みを監視し、不正プログラムの可能性がある処理を検知した場合には、不正プログラムの実行を防止するとともに、これを隔離する方式があり、不審な挙動を示す端末のホスト名や IP アドレスなどの情報をログとして取得し、管理者へ通知する必要がある。なお、製品の導入だけでは未知の不正プログラムの対策とはならない。監視体制や CSIRT との連携等組織的な対策と合わせて検討が必要となることに留意する必要がある。

（４） その他のセキュリティ対策

①プリンタ・複合機の情報セキュリティ対策

プリンタ・複合機は、必要に応じてマイナンバー利用事務系、LGWAN 接続系、インターネット接続系のネットワーク毎に設置されることが望ましい。共有する場合においてもマイナンバー利用事務系又は LGWAN 接続系について、インターネット接続系と共有することは認められない。共有する場合には、１台のプリン

タ・複合機にネットワーク毎に専用の LAN ポートを設け、他の領域と分離された通信を保証することが望ましい。それが困難である場合には、ネットワークの一方を LAN ポートに、もう一方は USB ポートにプリンタサーバを繋ぐなどの方法を検討する必要がある。

②本庁・支所・出先機関間でのネットワーク通信

本庁、支所、出先機関でマイナンバー利用事務系と LGWAN 接続系を構築するネットワークは、原則としてインターネット回線ではなく閉域網を利用すること。インターネット回線を利用する場合、VPN 通信等を用いて、通信元と通信先が特定されており、通信経路が限定されるようにすること。

③修正プログラム及びパターンファイルの更新

マイナンバー利用事務系及び LGWAN 接続系では、OS・アプリケーションの修正プログラム及びウイルス対策ソフトのパターンファイルの更新等においても、インターネットに接続して利用してはならない。LGWAN-ASP 等を利用して修正プログラム等を取得し適用することが望ましい。WSUS のファイル更新サーバ及びウイルス対策ソフトのパターンファイル更新サーバ等についても、マイナンバー利用事務系及び LGWAN 接続系からのインターネット接続は認められない。

④自動交付機による証明交付

自動交付機による証明交付をしている場合、個人番号利用事務の範囲に限定しているのであれば自動交付機をマイナンバー利用事務系と分離する必要はない。

⑤VPN 接続による外部との通信

遠隔での情報システム保守により、マイナンバー利用事務系及び LGWAN 接続系について VPN 接続による通信を許可する場合は、特定通信としての設定がされており、かつ IP－VPN 等の閉域網又は LGWAN で接続されなければならない。

⑥J-ALERT 等の LGWAN 接続系とインターネット接続系の双方への接続が必要な情報システムへの対応

J-ALERT 等の LGWAN 接続系とインターネット接続系の双方への接続が必要な情報システムがある場合は、ファイアウォールを設置し、さらに特定通信としなければならない。あるいはデータベースのみを共用し、情報システムは LGWAN 接続系とインターネット接続系の各系統で別に設置する方法で実現してもよい。

⑦インターネットメールによる障害通報

インターネット接続系についてはインターネットメールを利用してシステム障害通報を行ってもよい。マイナンバー利用事務系及び LGWAN 接続系については、特定サーバ間通信に限定した上で、LGWAN-ASP を活用することが望ましい。

⑧アクセス記録を外部に提供する又は他団体からアクセス記録を受領する際、アクセス記録に個人情報が含まれる場合は、個人情報保護条例及び情報セキュリティ管理関係の規程に従わなければならない。

4. 物理的セキュリティ

4.1. サーバ等の管理

【趣旨】

サーバ等のハードウェアは、情報システムの安定的な運用のために適正に管理する必要があり、管理が不十分な場合、情報システム全体に悪影響が及んだり、業務の継続性に支障が生じるおそれがある。このことから、サーバ等の設置や保守・管理、配線や電源等の物理的セキュリティ対策を規定する。

【例文】

（1） 機器の取付け

情報システム管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じなければならない。

（2） サーバの冗長化

①情報システム管理者は、重要情報を格納しているサーバ、セキュリティサーバ、住民サービスに関するサーバ及びその他の基幹サーバを冗長化し、同一データを保持しなければならない。【推奨事項】

②情報システム管理者は、メインサーバに障害が発生した場合に、速やかにセカンダリサーバを起動し、システムの運用停止時間を最小限にしなければならない。【推奨事項】

（3） 機器の電源

①情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。

②情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じなければならない。

（4） 通信ケーブル等の配線

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、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置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、主要な箇所の通信ケー

ブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応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、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。

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、自ら又は情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

（５） 機器の定期保守及び修理

①情報システム管理者は、可用性２のサーバ等の機器の定期保守を実施しなければならない。

②情報システム管理者は、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管理者は、外部の事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

（６） 庁外への機器の設置

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、庁外にサーバ等の機器を設置する場合、CISO の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（７） 機器の廃棄等

情報システム管理者は、機器を廃棄、リース返却等をする場合、機器内部の記憶装置から、全ての情報を消去の上、復元不可能な状態にする措置を講じなければならない。

（解説）

（１） 機器の取付け

情報システムで利用する機器は、温度、湿度等に敏感であることから、室内環境を整えることが必要である。

（注１）機器の排気熱が、特定の場所に滞留しないよう室内の空気を循環させることにも注意する必要がある。熱が機器周辺に滞留すると機器内部が高温になり、緊急停止する場合がある。

（２） サーバの冗長化

サーバ等の機器が緊急停止した場合にも、業務を継続できるようにするために、

バックアップシステムを設置することが有効である。

（注２）ハードウェアやソフトウェアが二重に必要となるほか、運用面でデータの同期化等が必要となり、多額の費用を要するので、これらの費用とサーバ等の緊急停止による損失の可能性を検討した上で、冗長化を行うか否かを判断する必要がある。

（３） 機器の電源

何らかの要因で電力供給が途絶し、機器が緊急停止した場合には、情報システムの機能が損なわれるおそれがある。これを避けるために、機器が適正に停止するまでの間電力を供給する予備電源を設ける必要がある。

（注３）予備電源は、パソコン等に接続する小型の UPS（無停電電源装置）、蓄電池設備による給電を行うものや、自家発電機等様々な種類がある。また、これらの予備電源が緊急時に機能した場合に、現状どのくらい給電が行えるかを把握しておくべきである。例えば、1 年前には、蓄電池設備により 30 分程度の電源供給ができていたものが、サーバの増設等により 15 分程度しか供給できなくなっている場合もある。このために、施設管理部門から予備電源が給電可能な時間等について定期的に確認しておくことが必要である。

（４） 通信ケーブル等の配線

執務室に通信ケーブル等を配線する場合に、ケーブルを剥き出しにしたままにしておくと、踏まれるなどして損傷する可能性が高くなる。配線収納管等を利用し、通信ケーブル等の損傷を防ぐ必要がある。

（５） 機器の定期保守及び修理

情報システムの安定的な運営のためには、定期的に保守を行うことが不可欠である。また、機器を修理に出す場合には、できる限り故障した部品を特定し、情報を消去できる場合は消去を行った上で引き渡すことにより、修理業者から情報が漏えいする可能性を低くしなければならない。内容を消去できないときは、守秘義務契約を締結するほか、秘密保持に関する体制や運用などが適正であることを確認しなければならない。

（６） 庁外への機器の設置

庁外にサーバ等の機器を設置する場合には、十分なセキュリティ対策が実施されているか、定期的に確認する必要がある。

（注４）外部委託事業者のデータセンターに、システム機器等を設置している場合は、定期的に物理的なセキュリティ状況を確認する必要がある。外部委託事業者を定期的に訪問し、定期報告では把握しきれない設置室内の状況の変化、当該外部委託事業者の要員の変化等を把握する。地方公共団体職員によるデータセンター内部への立入りがデータセンターのセキュリティポリシーに違反する等、外部委託事業者を訪問できない場合は、訪問調査に代えて第三者による情報セキュリティ監査報告書、外部委託事業者の内部監査部門による情報

セキュリティ監査報告書等によって確認する。

（7） 機器の廃棄等

情報システム機器が不要になった場合やリース返却等を行う場合には、機器内部の記憶装置からの情報漏えいのリスクを軽減する観点から、情報を復元困難な状態にする措置を徹底する必要がある。この場合、一般的に入手可能な復元ツールの利用によっても復元が困難な状態とすることが重要であり、OS 及び記憶装置の初期化（フォーマット等）による方法は、ハードディスク等の記憶演算子にはデータの記憶が残った状態となるため、適当でないことに留意が必要である。また、原則として、以下の表に記載されている方法により、記録されている情報の機密性に応じて、情報システム機器の廃棄等を行わなければならない。なお、運用にあたっては、「情報システム機器の廃棄等時におけるセキュリティの確保について」（令和 2 年 5 月 22 日総行情第 77 号　総務省自治行政局地域情報政策室長通知）を参照されたい。

分類	機器の廃棄等の方法	確実な履行を担保する方法
（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憶媒体 ※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	当該媒体を分解・粉砕・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすることが適当である。 なお、対象となる機器について、リース契約により調達する場合においても、リース契約終了後、当該機器の記憶媒体については、物理的に破壊を行う。この場合、予め仕様に明記のうえ、機器の廃棄方法を契約において明記することが望ましい。	職員が左記措置の完了まで立ち会いによる確認を行うほか、庁舎内において後述（3）で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、委託事業者等が物理的な破壊を実施し、当該破壊の完了証明書により確認する。当該完了証明書については、破壊の証拠写真が添付されるとともに、その提出期限が定められていることが望ましい。
（2）機密性２以上に該当する情報を保存する記憶媒体（上記（1）に該当するものを除く。）	一般的に入手可能な復元ツールの利用を超えた、いわゆる研究所レベルの攻撃からも耐えられるレベルで抹消を行うことが適当である。 具体的には、①物理的な方法による破壊、②磁気的な方法による破壊、③OS 等からのアクセスが不可能な領域も含めた領域のデータ消去装置又はデータ消去ソフトウェアによる上書き消去、④ブロック消去、⑤暗号化消去のうちいずれかの方法を選択することが適当である。	庁舎内において後述（3）で記述する情報の復元が困難な状態までデータの消去を行った上で、委託事業者等に引き渡しを行い、抹消措置の完了証明書により確認する方法など適切な方法により確認を行う。
（3）機密性１に該当する情報を保存する記憶媒体	一般的に入手可能な復元ツールの利用によっても復元が困難な状態に消去することが適当である。 具体的には、（2）に記述した方法①～⑤のほか、OS 等からアクセス可能な全てのストレージ領域をデータ消去装置又はデータ消去ソフトウェアにより上書き消去する方法がある。 OS 及び記憶装置の初期化（フォーマット等）による方法は、HDD の記憶演算子にはデータの記憶が残った状態となるため、適当ではない	庁舎内において消去を実施し、職員が作業完了を確認する方法など適切な方法により確認を行う。
※上記（1）は、オンプレミスの場合を想定したもの（ハウジングやプライベートクラウドを含む）		

図表 24　情報の機密性に応じた機器の廃棄等の方法

4.2. 管理区域(情報システム室等)の管理

【趣旨】

情報システム室等は、重要な情報資産が大量に保管又は設置されており、特に厳格に管理する必要がある。情報システム室等が適正に管理されていない場合には、盗難、損傷等により重大な被害が発生するおそれがあり、このことから、情報システム室等の備えるべき要件や入退室管理、機器等の搬入出に関する対策を規定する。

ただし、対策によっては建物の改修を必要とするなど多額の費用を要するものもある。対策の実施に当たっては、費用対効果を考慮して行う必要がある。

【例文】

（1） 管理区域の構造等

①管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。

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、管理区域を地階又は1階に設けてはならない。また、外部からの侵入が容易にできないように無窓の外壁にしなければならない。【推奨事項】

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、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

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、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

⑤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、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部を全て塞がなければならない。【推奨事項】

⑥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、管理区域に配置する消火薬剤や消防用設備等が、機器及び電磁的記録媒体等に影響を与えないようにしなければならない。

（2） 管理区域の入退室管理等

①情報システム管理者は、管理区域への入退室を許可された者のみに制限し、IC カード、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行わなければならない。

②職員等及び外部委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。

③情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じ

て立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

④情報システム管理者は、機密性２以上の情報資産を扱うシステムを設置している管理区域について、当該情報システムに関連しない、または個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしなければならない。

（３） 機器等の搬入出

①情報システム管理者は、搬入する機器等が、既存の情報システムに与える影響について、あらかじめ職員又は委託した業者に確認を行わせなければならない。

②情報システム管理者は、情報システム室の機器等の搬入出について、職員を立ち会わせなければならない。

(解説)

（１） 管理区域の構造等

情報システムの安定的な運営等のために、情報システム室や保管庫（磁気テープ等の保管庫）である管理区域の管理方法について定める。管理区域内には精密機器が多いことから、火災、水害、埃、振動、温度、湿度等への対策を講じる必要がある。

また、地方公共団体においては、多くの住民等の出入りがあることから、管理区域には施錠等を施し、監視カメラや認証機能等を活用して不正な者の入室を防止することが重要である。

（注１）IC カード等で扉を自動開閉制御している場合、サーバ室内で発生した火災等により、自動制御の扉が故障し開閉ができず、室内にいる要員が閉じ込められてしまう危険性がある。このような事態を回避するため、手動で扉を開閉できるように、平時から管理区域を管理している情報システム管理者が、自動扉開閉制御を解除するスイッチの場所を入室権限のある職員等に周知しておくことが必要である。鍵等による立入り防止措置についても、同様である。

（注２）管理区域に配置する消火薬剤は、発泡性のものを避けるべきである。また、情報システム機器等に水がかかる位置にスプリンクラーを設置してはならない。

（注３）情報システム室内では機器等をサーバラックに固定した上で、管理権限の異なる複数のシステムが同一の室内に設置されている場合は、他システムの管理者による不正操作を回避するため、サーバラックの施錠管理を行うことが必要である。

（２） 管理区域の入退室管理等

管理区域は情報資産の分類に応じて厳格な管理が行われなければならない。リスク評価を行って許可する範囲を検討し、入室できる者は許可された者のみに制限す

る。また、外部からの訪問者が管理区域に入室する場合、職員が付き添うとともに、訪問者であることを明示したネームプレートを着用させるなど外見上訪問者であることが分かるようにしておくべきである。また、情報漏えい等を回避するため、不要な電子計算機、モバイル端末、電磁的記録媒体等を管理区域に持ち込ませないことが重要である。

（注４）入退室の記録簿は、業者名、訪問者名等を記録する場合が多い。これらの記録簿に個人情報を記述している場合は、紛失等が生じないように保管することが必要である。

（３） 機器等の搬入出

搬入出に伴い外部の者が管理区域に立入る場合は、同行、立会いを行い、相手の行動を監視する必要がある。

（注５）同行、立会いについては、原則として非常勤職員や臨時職員等ではなく、職員が行う必要がある。

4.3. 通信回線及び通信回線装置の管理

【趣旨】

ネットワーク利用における通信回線及び通信回線装置が適正に管理されていない場合は、ネットワークそれ自体のみならず、ネットワークに接続している情報システム等に対しても損傷や不正アクセス等が及ぶおそれがある。このことから、外部ネットワーク接続等の通信回線及び通信回線装置の管理にセキュリティ対策を規定する。

【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、外部へのネットワーク接続を必要最低限に限定し、できる限り接続ポイントを減らさなければならない。

③統括情報セキュリティ責任者は、行政系のネットワークを総合行政ネットワーク（LGWAN）に集約するように努めなければならない。

④統括情報セキュリティ責任者は、機密性２以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化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十分なセキュリティ対策を実施しなければならない。

⑥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。

（解説）

庁内の通信回線は、施設管理部門が敷設・管理を行っていることが多く、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、ネットワークに関する工事を行う場合、施設管理部門と連携して実施する必要がある。庁舎内の通信回線敷設図、結線図等は、外部への漏えい等がないよう、厳重に管理しなければならない。

また、外部のネットワークへの不必要な接続は情報セキュリティ上の危険性が高まることから、接続は必要最低限のものに限定し、特に行政系のネットワークは、安全性の高い総合行政ネットワークに集約するように努めることが必要である。

通信回線として利用する回線は、当該システムで取り扱う情報資産の重要性に応じて、適正なセキュリティ機能を備えたものを選択することが必要であり、通信回線の性能低下や異常によるサービス停止を防ぐために、通信回線や通信回線装置を冗長構成にした

り、回線の種類を変えて複数の回線を構築しておくことが望ましい。また、庁内から外部に敷設する通信回線の管路についても、例えば異なる通信事業者による複数の経路で構築しておくと、災害発生時の復旧にかかる時間が短縮されるなどの効果が期待される。

（注１）図面管理を外部委託事業者に依頼する場合でも、当該外部委託事業者で紛失する場合に備えて、各地方公共団体で、控えを保管しておくことが必要である。

4.4. 職員等の利用する端末や電磁的記録媒体等の管理

【趣旨】

職員等が利用するパソコン、モバイル端末及び電磁的記録媒体等が適正に管理されていない場合は、不正利用、紛失、盗難、情報漏えい等の被害を及ぼすおそれがある。このことから、これらの被害を防止するために、職員等の利用するパソコン、モバイル端末及び電磁的記録媒体等の盗難及び情報漏えい防止策、持ち出し・持ち込み等に関する対策を規定する。

【例文】

①情報システム管理者は、盗難防止のため、執務室等で利用するパソコンのワイヤーによる固定、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じなければならない。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。

②情報システム管理者は、情報システムへのログインに際し、パスワード、スマートカード、或いは生体認証等複数の認証情報の入力を必要とするように設定しなければならない。

③情報システム管理者は、端末の電源起動時のパスワード（BIOS パスワード、ハードディスクパスワード等）を併用しなければならない。【推奨事項】

④情報システム管理者は、マイナンバー利用事務系では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証）を行うよう設定しなければならない。

⑤情報システム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についてもデータ暗号化機能を備える媒体を使用しなければならない。【推奨事項】

⑥情報システム管理者は、モバイル端末の庁外での業務利用の際は、上記対策に加え、遠隔消去機能を利用する等の措置を講じなければならない。【推奨事項】

（解説）

執務室等からパソコン、モバイル端末及び電磁的記録媒体等が盗難され、情報が漏えいする事例は多く、盗難を防止するための物理的措置が必要である。

また、各団体が保有しているパソコン、モバイル端末及び電磁的記録媒体等が盗難等に遭った場合でも、指紋又は顔等を用いた生体認証、パスワード等の設定、暗号化により使用できないようにしておくことで、情報が不正使用等される可能性を減らすことができる。特に、パソコン起動時のパスワード機能の利用と、電磁的記録媒体の暗号化の併用が情報の漏えいに対する有効な防止対策になる。また、次のパソコンの不正利用を防止するためのパスワード機能及び暗号化機能を活用することが必要である。

①ログインパスワード

OS やソフトウェアにログインする際に使用するパスワードであり、ログインパスワードによって、パソコンの多くの機能の不正利用を防御できる。

②多要素認証の利用

取り扱う情報の重要度等に応じて「知識」「所持」「存在」を利用する認証の手段のうち、二つ以上を併用する多要素認証を行うことによりセキュリティ機能が強化されることになる。多要素認証の詳細は、「３．情報システム全体の強靭性の向上」を参照されたい。

③電源起動時のパスワード（BIOS パスワード）

パソコンを起動したときに、OS が起動する前に入力するパスワードであり、この BIOS パスワードの設定をしておくことで、オペレーティングシステムが自動起動しない。

④電源起動時のパスワード（ハードディスクパスワード）

ハードディスクパスワードを設定しておけば、不正利用を防御できる。ただし、ハードディスクパスワードについては、失念すると解除が不可能になる場合があるために留意する必要がある。

⑤セキュリティチップの暗号化機能

セキュリティチップを搭載したパソコン、モバイル端末及び電磁的記録媒体の場合は、暗号鍵が当該チップに記録されているために、ハードディスクの暗号化機能を利用することによって、ハードディスク装置を抜き取られても不正利用を防御できる。

⑥モバイル端末のセキュリティ

モバイル端末を庁外で業務利用する場合は、端末の紛失・盗難対策として、前述のように普段からパスワードによる端末ロックを設定しておくことが必要である。また、紛失・盗難に遭った際は、遠隔消去（リモートワイプ）や自己消去機能により、モバイル端末内のデータを消去する対策も有効である。

なお、USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順を定めなければならない。

（注１）USB メモリ等の外部電磁的記録媒体を用いた情報の取扱いに関する利用手順には、以下の事項を含めることが望ましい。

・職員等は支給された外部電磁的記録媒体、又は本項に規定する利用手順において定められた外部電磁的記録媒体を用いた情報の取扱いの遵守を契約により外部の組織との間で取り決めた外部の組織から受け取った外部電磁的記録媒体を使用すること。

・外部の組織から受け取った外部電磁的記録媒体は、情報を運搬する目的に限って使用することとし、当該外部電磁的記録媒体から情報を読み込む場合及びこ

れに情報を書き出す場合の安全確保のために必要な措置を講ずること。

（注２）特にセキュリティ機能を強化する必要がある場合には、パスワードの流用等による悪用を防止するため、認証のために一度しか使えないワンタイムパスワードを使用することも考えられる。

（注３）ディスク装置を持たない形態のシンクライアント端末は、端末から情報が漏えいする可能性が非常に低くなることから、情報漏えい防止にも有効であり、導入する地方公共団体も出ている。ただし、シンクライアント端末の場合、サーバ、ネットワークに障害が生じると、業務ができなくなる可能性があることから、その場合の対応、特に災害時等の対応も考慮した上で導入を行う必要がある。

（注４）パソコン、モバイル端末、通信機器、ケーブル等からは、微弱電磁波が流れている。これらから流れる電磁波から、指向性の高いアンテナを利用して、情報を盗聴することが技術的には可能である。このため、機密性の非常に高い情報を取り扱う企業等では、電磁波により重要情報が外部に漏えいすることを防止する対策を実施することがある。この電磁波盗聴対策は、シールドルーム工事等、多額の費用を要するため、盗聴された場合のリスクを考慮した上で、実施の可否を判断する必要がある。

（注５）モバイル端末の遠隔消去（リモートワイプ）機能は、モバイル端末に電源が入っており、かつ通信状態が良好な場合にしか効果が期待できない点に留意する必要がある。このことから、本機能とあわせて、データを暗号化する等、漏えいしても内容が知られることのない仕組みを合わせて導入することが有効である。

5. 人的セキュリティ

5.1. 職員等の遵守事項

【趣旨】

職員等が情報資産を不正に利用したり、適正な取扱いを怠った場合、コンピュータウイルス等の感染、情報漏えい等の被害が発生し得る。このことから、情報セキュリティポリシーの遵守や情報資産の業務以外の目的での使用の禁止等、職員等が情報資産を取り扱う際に遵守すべき事項を明確に規定する。職員だけでなく、非常勤職員、臨時職員及び外部委託事業者等についても、遵守事項を定めなければならない。

情報漏えい事案の多くが、職員等の過失又は故意による規定違反から生じており、職場の実態等を踏まえつつ、職員等の遵守事項を適正に定めるとともに、規程の実効性を高める環境を整備することが重要である。

【例文】

（１） 職員等の遵守事項

①情報セキュリティポリシー等の遵守

職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。

②業務以外の目的での使用の禁止

職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。

③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

（ア）CISO は、機密性２以上、可用性２、完全性２の情報資産を外部で処理する場合における安全管理措置を定めなければならない。

（イ）職員等は、本市のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ管理者の許可を得なければならない。

（ウ）職員等は、外部で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。

④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

（ア）職員等は、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を原則業務に利用してはならない。ただし、支給以外の端末の業務利用の可否判断をCISO が行った後に、業務上必要な場合は、統括情報セキュリティ責任者の定め

る実施手順に従い、情報セキュリティ管理者の許可を得て利用することができる。

（イ）職員等は、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を用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置に関する規定を遵守しなければならない。

⑤持ち出し及び持ち込みの記録

情報セキュリティ管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管しなければならない。

⑥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

職員等は、パソコンやモバイル端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

⑦机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

⑧退職時等の遵守事項

職員等は、異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を漏らしてはならない。

（２） 非常勤及び臨時職員等への対応

①情報セキュリティポリシー等の遵守

情報セキュリティ管理者は、非常勤及び臨時職員等に対し、採用時に情報セキュリティポリシー等のうち、非常勤及び臨時職員等が守るべき内容を理解させ、また実施及び遵守させなければならない。

②情報セキュリティポリシー等の遵守に対する同意

情報セキュリティ管理者は、非常勤及び臨時職員等の採用の際、必要に応じ、情報セキュリティポリシー等を遵守する旨の同意書への署名を求めるものとする。

③インターネット接続及び電子メール使用等の制限

情報セキュリティ管理者は、非常勤及び臨時職員等にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

（３） 情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び実施手

順を閲覧できるように掲示しなければならない。

（４） 外部委託事業者に対する説明

情報セキュリティ管理者は、ネットワーク及び情報システムの開発・保守等を外部委託事業者に発注する場合、外部委託事業者から再委託を受ける事業者も含めて、情報セキュリティポリシー等のうち外部委託事業者が守るべき内容の遵守及びその機密事項を説明しなければならない。

（解説）

（１） 職員等の遵守事項

情報セキュリティを確保するために、情報セキュリティポリシー及び実施手順に定められている事項等、全ての職員が遵守すべき事項について定めたものである。

情報セキュリティ管理者は、異動、退職等により業務を離れる場合、職員等が利用している情報資産を返却させる。また ID についても、速やかに利用停止等の措置を講じる必要がある。

①モバイル端末の持ち出し及び外部における情報処理作業

情報の漏えいは、不正なモバイル端末の持ち出しや移動中にモバイル端末が盗難に遭うなどしたことが原因で発生する場合が多い。重要な情報資産を使って外部で作業する場合には、庁内の安全対策に加え、安全管理に関して追加的な措置を定めた上で、モバイル端末の持ち出しや外部での作業の実施については許可制とするのが適正である。

（注１）モバイル端末の持ち出しを許可した場合にも、モバイル端末は常に携行することを職員等に周知する必要がある。特に交通機関（電車、バス、自家用車等）による移動時の携行に際しては、紛失、盗難等に留意する必要がある。

（注２）共用しているモバイル端末の持ち出しでは、管理者が不明確になりやすく、その結果として所在不明になりやすいので特に注意する必要がある。

（注３）持ち出し専用パソコンによる情報の持ち出しにおいては、万一当該パソコンを紛失した場合に、記録されている情報を容易に特定するため、日常においては当該パソコンに情報を記録しないようにし、持ち出し時においては持ち出し情報が必要最小限であるかどうか確認を行った上で情報を記録し、返却時においては情報の完全削除をするといった運用を行う必要がある。

（注４）テレワーク等におけるセキュリティ対策については、「6.2. アクセス制御」を併せて参照されたい。

②支給以外のパソコンやモバイル端末等の業務利用

自宅や庁外等での情報処理作業においては支給された端末を使用することとし、支給以外の端末の使用は原則禁止とする。

やむを得ず支給以外の端末を使用する場合は、以下のような対策を実施することが必要である。

・統括情報セキュリティ責任者の定める実施手順に従い、情報セキュリティ管理者の許可を得る
・支給以外の端末のコンピュータウイルスチェックが実施されていることやファイル共有ソフトウェアの導入がされていないことを情報セキュリティ管理者が確認する
・パスワードによる端末ロック機能や遠隔消去機能などの要件を満たしていることを情報セキュリティ管理者が確認する
・機密性３の情報資産については支給以外の端末での作業を禁止とする
・支給以外の端末のセキュリティに関する教育を受けた者のみ使用を許可する
・無許可で行政情報等を記録、持ち出す行為を禁止する
・業務利用する必要がなくなった場合は、支給以外のパソコンやモバイル端末等から業務に関係する情報を削除する

（注５）支給以外の端末の利用申請内容については、以下を含めること。

・申請者の氏名、所属、連絡先
・利用する端末の契約者の名義（スマートフォン等の通信事業者と契約を行う端末の場合）
・利用する端末の製造企業名、機種名、OS の種類及びバージョン
・利用目的、取り扱う情報の概要、機密性２以上の情報の利用の有無等
・主要な利用場所
・利用する主要な通信回線サービス
・利用する期間

さらに、支給以外の端末から庁内ネットワークに接続を行う可能性がある場合は、情報漏えいを防ぐため、以下のような利用者が端末に情報を保存できないようにするための機能又は端末に保存される情報を暗号化するための機能を設ける~~対策を講じる~~必要がある。

・シンクライアント等の仮想デスクトップ技術を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者は専用のシンクライアントアプリケーションを利用端末にインストールし、業務用システムへリモートアクセスする。
・セキュアブラウザ等を活用した、端末に情報を保存させないリモートアクセス環境を構築する。利用者はセキュアブラウザを利用端末にインストールし、業務用システムへリモートアクセスする。
・ファイル暗号化等のセキュリティ機能を持つアプリケーションを導入する。
・端末に、ハードディスク等の電磁的記録媒体全体を自動的に暗号化する機能を設ける。

・上記のいずれの機能も使用できない場合は、端末にファイルを暗号化する機能を設ける。
・ハードディスク等の電磁的記録媒体に保存されている情報を遠隔からの命令等により暗号化消去する機能を設ける。
~~・シンクライアント環境やセキュアブラウザを使用する~~
~~・ファイル暗号化機能を持つアプリケーションでの接続のみを許可する~~

また、支給以外のパソコン、モバイル端末及び電磁的記録媒体を情報システム室に持ち込むことは禁止する。

その他、職員等が講じるべき以下の事項を含む利用時の実施手順に係る安全管理措置をあらかじめ定め、情報セキュリティ管理者は職員に安全管理措置を講じさせなければならない。

・パスワード等による端末ロックの常時設定
・OS やアプリケーションの最新化
・不正プログラム対策ソフトウェアの導入及び定期的な不正プログラム検査の実施（不正プログラム対策ソフトウェアを指定する場合は当該ソフトウェアの導入も含める）
・端末内の機密性２以上の~~要機密~~情報の外部サーバ等へのバックアップの禁止（安全管理措置として定める場合は職務上取り扱う情報のバックアップ手順を別途考慮する必要がある）
・市等提供の業務専用アプリケーションの利用（専用アプリケーションを提供する場合のみ）

また、以下を例とする禁止事項を遵守させなければならない。

・端末、OS、アプリケーション等の改造行為
・安全性が確認できないアプリケーションのインストール及び利用
・利用が禁止されているソフトウェアのインストール及び利用
・許可されない通信回線サービスの利用（利用する回線を限定する場合）
・第三者への端末の貸与

③持ち出し及び持ち込みの記録

庁内のパソコン、モバイル端末及び電磁的記録媒体の持ち出しや業務利用を許可された支給以外のパソコン、モバイル端末及び電磁的記録媒体の持ち込みについては現状把握や資産管理のためこれを記録する必要がある。

（注６~~５~~）記録簿に記録を作成する場合は、持ち出しの項目として、所属課室名、名前、日時、持出物、個数、用途、持出の場所、返却日、管理者の確認等を設ける。

（注７~~６~~）持ち込みの項目としては、所属課室名、名前、日時、持込物、個数、用途、持込の場所、持ち帰り日、管理者の確認等を設ける。

（２） 非常勤及び臨時職員等への対応

情報セキュリティ管理者は、非常勤職員等の採用時に情報セキュリティポリシー

等のうち守るべき内容を理解させ、必要に応じて情報セキュリティポリシーの遵守の同意書への署名を求める。また、パソコンやモバイル端末の機能は、非常勤職員等の業務内容に応じて、不必要な機能については制限することが適正である。

（３） 情報セキュリティポリシー等の掲示

職員等が情報セキュリティポリシーを遵守する前提として、イントラネット等に掲示する方法により、職員等が常に最新の情報セキュリティポリシー及び実施手順を閲覧できるようにしなければならない。

（４） 外部委託事業者に対する説明

外部委託事業者の内部管理が不十分であることから、情報の漏えい等が発生する事例は多い。したがって、各地方公共団体が事業者（外部委託事業者から再委託を受けた事業者を含む。）等に情報システムの開発及び運用管理を委託する場合、情報セキュリティ管理者は、契約の遵守を求め、委託の業務範囲に従って、情報セキュリティポリシー及び実施手順に関する事項を説明する必要がある。

なお、外部委託については、「8. ~~1.~~ 外部委託」を参照のこと。

5.2. 研修・訓練

【趣旨】

情報セキュリティを適正に確保するためには、情報セキュリティ対策の必要性と内容を幹部を含め全ての職員等が十分に理解していることが必要不可欠である。情報セキュリティに関する情報セキュリティインシデントの多くが、職員等の規定違反に起因している。情報セキュリティの向上は、利便性の向上とは、必ずしも相容れない場合があり、職員等の意識として業務優先で情報セキュリティ対策の軽視につながることもある。また、情報セキュリティに関する脅威や技術の変化は早く、職員等には常に最新の状況を理解させることが必要である。

また、実際に情報セキュリティインシデントが発生した場合に的確に対応できるようにするため、緊急時に対応した訓練を実施しておくことが必要である。

これらのことから、職員等に情報セキュリティに関する研修・訓練を行うことを規定する。

【例文】

（1） 情報セキュリティに関する研修・訓練

CISO は、定期的に情報セキュリティに関する研修・訓練を実施しなければならない。

（2） 研修計画の策定及び実施

①CISO は、幹部を含め全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、情報セキュリティ委員会の承認を得なければならない。

②研修計画において、職員等は毎年度最低１回は情報セキュリティ研修を受講できるようにしなければならない。【推奨事項】

③新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

④研修は、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及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

⑤情報セキュリティ管理者は、所管する課室等の研修の実施状況を記録し、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対して、報告しなければならない。

⑥統括情報セキュリティ責任者は、研修の実施状況を分析、評価し、CISO に情報セ

キュリティ対策に関する研修の実施状況について報告しなければならない。

⑦CISO は、毎年度１回、情報セキュリティ委員会に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

（３） 緊急時対応訓練

CISO は、緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

（４） 研修・訓練への参加

幹部を含めた全ての職員等は、定められた研修・訓練に参加しなければならない。

（解説）

（１） 情報セキュリティに関する研修・訓練

情報セキュリティに関する研修・訓練を実施する責任は CISO にあり、研修・訓練を定期的に行わなければならない。

（２） 研修計画の立案及び実施

CISO は、幹部を含めた全ての職員等が、情報セキュリティの重要性を認識し、情報セキュリティポリシーを理解し、実践するために、研修及び訓練を定期的かつ計画的に実施する必要がある。

（注１）研修計画には、研修内容や受講対象者のほか、e-ラーニング、集合研修、説明会等の実施方法、時期、日程、講師等を盛り込む。

（注２）部外の研修等に、職員等を参加させることも有益である。

情報セキュリティポリシーを運用する際、多くの部分は組織の責任者及び利用者の判断や行動に依存している。したがって、全ての職員等を対象に研修を行う必要がある。情報セキュリティに関する環境変化は早いことから、毎年度最低１回は研修を受講するようにすることが望ましい。

研修内容は、毎回同じ内容ではなく、情報セキュリティ監査の結果や庁内外での情報セキュリティインシデントの発生状況等を踏まえ、継続的に更新することや職員等が具体的に行動すべき事項を考慮することが望ましい。

新規採用の職員等に対しては、採用時に情報セキュリティ研修を行うことによって、情報セキュリティの大切さを深く認識させることができる。

また、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及び職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じた研修を実施することが必要である。これは不正アクセスから情報資産を防御することはもとより、不正プログラムの

感染、侵入、内部者による情報の漏えい、外部への攻撃等を防ぐ観点からも重要である。

研修受講を確実にするため、CISO に、毎年度１回、情報セキュリティ委員会に対して職員等の研修の実施状況を報告させなければならない。

また、CISO は、研修計画を通じて将来の情報セキュリティを担う人材の育成や要員の管理を行うとともに、地方公共団体の長によるメールでの周知等、研修効果を向上させる施策を講じることが望ましい。

なお、外部の専門家や内部の職員を最高情報セキュリティアドバイザー等として登用している場合は、それらの専門家等を内部教育に有効活用することも考えられる。

（３） 緊急時対応訓練

実際に情報の漏えい等の情報セキュリティインシデントが発生した場合に、即応できる態勢を構築しておくため、緊急時を想定した訓練を定期的に実施しなければならない。

（注３）参考として受講が望まれる訓練等を以下に示すので、計画的な受講を推進されたい。

・実践的サイバー防御演習（CYDER）: NICT ナショナルサイバートレーニングセンター主催

・小規模自治体のための CSIRT 構築の手引きに関する説明会：地方公共団体情報システム機構主催

・インシデント対応訓練（基礎/高度）：地方公共団体情報システム機構主催

・分野横断的演習：NISC 主催（地方公共団体情報システム機構同時開催）

（４） 研修・訓練への参加

幹部を含めた全ての職員に対し、研修・訓練に参加させることが情報セキュリティ確保にとって必要であることから、義務規定を設ける。

（注４）教育・訓練の実施後、理解度試験等を行い、その有効性を評価し、次回の研修・訓練の改善に活用すれば、より効果を上げることができる。

（注５）啓発や訓練を通じた各自治体の職員等のセキュリティ・リテラシーの向上として、地方公共団体情報システム機構主催の以下の研修等があるので、積極的に活用いただき、受講を推進されたい。また、自治体情報セキュリティクラウドに関して、都道府県が主催する演習・研修がある場合は、それらも積極的に受講する必要がある。

・リモートラーニングによるデジタル人材育成のための基礎研修~~セキュリティリモートラーニングによる情報セキュリティ研修~~（e ラーニング）

・情報セキュリティ対策セミナー/情報セキュリティマネジメントセミナー（オンライン~~集合~~研修）

・専門 e ラーニング（専門・ICT 基礎/専門・ICT 中級）

5.3. 情報セキュリティインシデントの報告

【趣旨】

情報セキュリティインシデントやその発生の予防が重要なことは言うまでもないが、完全な予防は事実上困難であることから、実際に情報セキュリティインシデントを認知した場合に、責任者に報告を速やかに行うことにより、被害の拡大を防ぎ、早期に回復を図れるようにしておく必要がある。このことから、情報セキュリティインシデントを認知した場合の報告義務について規定する。

なお、報告に対する対応については、「7.3. 侵害時の対応等」による。

【例文】

（1） 庁内での情報セキュリティインシデントの報告

①職員等は、情報セキュリティインシデントを認知した場合、速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない。

②報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

③情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、CISO 及び情報セキュリティ責任者に報告しなければならない。

（2） 住民等外部からの情報セキュリティインシデントの報告

①職員等は、本市が管理するネットワーク及び情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けた場合、情報セキュリティ管理者に報告しなければならない。

②報告を受けた情報セキュリティ管理者は、速やかに統括情報セキュリティ責任者及び情報システム管理者に報告しなければならない。

③情報セキュリティ管理者は、当該情報セキュリティインシデントについて、必要に応じて CISO 及び情報セキュリティ責任者に報告しなければならない。

④CISO は、情報システム等の情報資産に関する情報セキュリティインシデントについて、住民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない。【推奨事項】

（3） 情報セキュリティインシデント原因の究明・記録、再発防止等

①CSIRT は、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

②CSIRT は、情報セキュリティインシデントであると評価した場合、CISO に速や

かに報告しなければならない。

③CSIRT は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。

④CSIRT は、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、CISO に報告しなければならない。

⑤CISO は、CSIRT から、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

（解説）

（１） 庁内からの情報セキュリティインシデントの報告

職員等は、情報セキュリティインシデントを認知した場合に、自らの判断でその情報セキュリティインシデントの解決を図らずに速やかに管理者に報告し、その指示を仰ぐことが必要である。その情報セキュリティインシデントによる被害を拡大しないためにも、報告ルート及びその方法を事前に定めておく必要がある。

（注１）CSIRT は、情報セキュリティインシデント発生時の対処手順のうち、意思決定の判断基準、判断に応じた対応内容、緊急時の意思決定方法等をあらかじめ定めておく必要がある。

（注２）CSIRT は、自組織~~本市~~において発生した情報セキュリティインシデントについて、報告・連絡を受ける情報セキュリティに関する統一的な窓口を設置し、情報セキュリティインシデント発生が報告された際に、CISO、総務省、都道府県等への報告手順を定めておく必要がある。

（注３）情報セキュリティインシデント発生時の報告ルートは、団体の意思決定ルートと整合性を図ることが重要である。

（２） 住民等外部からの情報セキュリティインシデントの報告

住民からの報告が契機となって、重大な情報セキュリティインシデントの発見につながる場合等も想定されることから、当該報告、連絡を受ける窓口を設置する。

（注４）住民からの報告に対しては、適正に処理し、必要に応じ対応した結果について、報告を行った住民等に通知する必要がある。

（３） 情報セキュリティインシデント原因の究明・記録、再発防止等

CSIRT は、報告された情報セキュリティインシデントについて評価を行い、情報セキュリティインシデントであると評価した場合は、CISO に速やかに報告することが必要である。さらに、被害の拡大防止等を図るための応急措置の実施及び復旧に係

る指示又は勧告を行う必要がある。

CSIRT は、情報セキュリティインシデントの原因を究明し、効果的な再発防止策を検討するために、情報セキュリティインシデントを引き起こした部門の情報セキュリティ管理者は、情報セキュリティインシデントの発生から対応までの記録を作成し、保存しておく必要がある。

（注５）他部門も含めて同様の情報セキュリティインシデントの再発を防止するために全庁横断的に再発防止策を検討する必要がある。再発防止処置の策定については、「7.3. 侵害時の対応　（２）④再発防止措置の策定」を参照されたい。

5.4. ID 及びパスワード等の管理

【趣旨】

情報システムを利用する際の ID 及びパスワード、生体認証に係る情報等の認証情報及びこれを記録した媒体（IC カード等）の管理が適正に行われない場合は、情報システム等を不正に利用されるおそれがある。このことから、ID 及びパスワード等の管理に関する遵守事項を規定する。

認証情報等は、人的な原因により漏えいしやすい情報である。情報システム管理者からの認証情報等の発行から職員等での管理に至るまで、人的な原因で情報が漏えいするリスクを最小限にとどめる必要がある。

【例文】

（1） IC カード等の取扱い

①職員等は、自己の管理する IC カード等に関し、次の事項を遵守しなければならない。

（ア）認証に用いる IC カード等を、職員等間で共有してはならない。

（イ）業務上必要のないときは、IC カード等をカードリーダ又はパソコン等の端末のスロット等から抜いておかなければならない。

（ウ）IC カード等を紛失した場合には、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報し、指示に従わなければならない。

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、IC カード等の紛失等の通報があり次第、当該 IC カード等を使用したアクセス等を速やかに停止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、IC カード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

（2） ID の取扱い

職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。

①自己が利用している ID は、他人に利用させてはならない。

②共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

（3） パスワードの取扱い

職員等は、自己の管理するパスワードに関し、次の事項を遵守しなければならない。

①パスワードは、他者に知られないように管理しなければならない。

②パスワードを秘密にし、パスワードの照会等には一切応じてはならない。
③パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。
④パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。
⑤複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。
⑥仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。
⑦サーバ、ネットワーク機器及びパソコン等の端末にパスワードを記憶させてはならない。
⑧職員等間でパスワードを共有してはならない（ただし、共有 ID に対するパスワードは除く）。

（解説）

（１） IC カード等の取扱い

認証のため、IC カードや USB トークン等の媒体を利用する場合は、情報のライフサイクルに着目し、利用、保管、返却、廃棄等の各段階における取扱い方法を定めておくことが必要である。

（２） ID の取扱い

ID の利用は本人に限定することを規定する。

（３） パスワードの取扱い

パスワードの秘密を担保するため、想像しにくいパスワード設定（例えば、大文字及び小文字を組み合わせる、数字、アルファベット及び記号を組み合わせる等）、パスワードの共有禁止などを定める。

（注１）複数のシステムを取り扱う等により、複数の異なるパスワードが必要となる場合があるが、全てを覚えることの困難性から、安易なパスワードを数個使い回すといった運用が起こる可能性がある。

パスワードのメモを作成し、机上、キーボード、ディスプレイ周辺等にメモを置くことは禁止する必要があるが、特定の場所に施錠して保存する等により他人が容易に見ることができないような措置を講じていれば、メモの存在がパスワードの効果を削ぐものではないため、メモの作成を禁止するものではない。

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

【趣旨】

ネットワークや情報システム等の管理が不十分な場合、不正利用による情報システム等へのサイバー攻撃、情報漏えい、損傷、改ざん、重要情報の詐取、内部不正等の被害が生じるおそれがある。このことから、情報システム等の不正利用を防止し、また不正利用に対する証拠の保全をするために、ログの管理やシステム管理記録の作成、バックアップ、無許可ソフトウェアの導入禁止、機器構成の変更禁止等の技術的なセキュリティ対策を規定する。

【例文】

（１） 文書サーバの設定等

①情報システム管理者は、職員等が使用できる文書サーバの容量を設定し、職員等に周知しなければならない。

②情報システム管理者は、文書サーバを課室等の単位で構成し、職員等が他課室等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

③情報システム管理者は、住民の個人情報、人事記録等、特定の職員等しか取り扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一課室等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

（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、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。

（３） 他団体との情報システムに関する情報等の交換

情報システム管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、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の許可を得なければならない。

（４） システム管理記録及び作業の確認

①情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成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、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理しなければならない。

③統括情報セキュリティ責任者、情報システム管理者又は情報システム担当者及び契約により操作を認められた外部委託事業者がシステム変更等の作業を行う場合は、2名以上で作業し、互いにその作業を確認しなければならない。

（5） 情報システム仕様書等の管理

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、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適正に管理しなければならない。

（6） ログの取得等

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、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存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、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理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、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

（7） 障害記録

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、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適正に保存しなければならない。

（8） ネットワークの接続制御、経路制御等

①統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

②統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

（９） 外部の者が利用できるシステムの分離等

情報システム管理者は、電子申請の汎用受付システム等、外部の者が利用できるシステムについて、必要に応じ他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

（１０） 外部ネットワークとの接続制限等

①情報システム管理者は、所管するネットワークを外部ネットワークと接続しようとする場合には、CISO 及び統括情報セキュリティ責任者の許可を得なければならない。

②情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、庁内の全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

③情報システム管理者は、接続した外部ネットワークの瑕疵によりデータの漏えい、破壊、改ざん又はシステムダウン等による業務への影響が生じた場合に対処するため、当該外部ネットワークの管理責任者による損害賠償責任を契約上担保しなければならない。

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、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

⑤情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、統括情報セキュリティ責任者の判断に従い、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（１１） 複合機のセキュリティ管理

①統括情報セキュリティ責任者は、複合機を調達する場合、当該複合機が備える機能及び設置環境並びに取り扱う情報資産の分類及び管理方法に応じ、適正なセキュリティ要件を策定しなければならない。

②統括情報セキュリティ責任者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策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は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消する又は再利用できないようにする対策を講じなければならない。

（１２） IoT 機器を含む特定用途機器のセキュリティ管理

統括情報セキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を講じなければならない。

（１３） 無線 LAN 及びネットワークの盗聴対策

①統括情報セキュリティ責任者は、無線 LAN の利用を認める場合、解読が困難な暗号化及び認証技術の使用を義務付けなければならない。

②統括情報セキュリティ責任者は、機密性の高い情報を取り扱うネットワークについて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

（１４） 電子メールのセキュリティ管理

①統括情報セキュリティ責任者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行わなければならない。

②統括情報セキュリティ責任者は、大量のスパムメール等の受信又は送信を検知した場合は、メールサーバの運用を停止しなければならない。

③統括情報セキュリティ責任者は、電子メールの送受信容量の上限を設定し、上限を超える電子メールの送受信を不可能にしなければならない。

④統括情報セキュリティ責任者は、職員等が使用できる電子メールボックスの容量の上限を設定し、上限を超えた場合の対応を職員等に周知しなければならない。

⑤統括情報セキュリティ責任者は、システム開発や運用、保守等のため庁舎内に常駐している外部委託事業者の作業員による電子メールアドレス利用について、外部委託事業者との間で利用方法を取り決めなければならない。

⑥統括情報セキュリティ責任者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監視等によりシステム上措置を講じなければならない。【推奨事項】

（１５） 電子メールの利用制限

①職員等は、自動転送機能を用いて、電子メールを転送してはならない。

②職員等は、業務上必要のない送信先に電子メールを送信してはならない。

③職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。

④職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。

⑤職員等は、ウェブで利用できる電子メール、ネットワークストレージサービス等を使用してはならない。

（１６） 電子署名・暗号化

①職員等は、情報資産の分類により定めた取扱制限に従い、外部に送るデータの機密性又は完全性を確保することが必要な場合には、CISO が定めた電子署名、暗号化又はパスワード設定等、セキュリティを考慮して、送信しなければならない。

②職員等は、暗号化を行う場合に CISO が定める以外の方法を用いてはならない。また、CISO が定めた方法で暗号のための鍵を管理しなければならない。

③CISO は、電子署名の正当性を検証するための情報又は手段を、署名検証者へ安全に提供しなければならない。

（１７） 無許可ソフトウェアの導入等の禁止

①職員等は、パソコンやモバイル端末に無断でソフトウェアを導入してはならない。

②職員等は、業務上の必要がある場合は、統括情報セキュリティ責任者及び情報システム管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報セキュリティ管理者又は情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。

③職員等は、不正にコピーしたソフトウェアを利用してはならない。

（１８） 機器構成の変更の制限

①職員等は、パソコンやモバイル端末に対し機器の改造及び増設・交換を行ってはならない。

②職員等は、業務上、パソコンやモバイル端末に対し機器の改造及び増設・交換を行う必要がある場合には、統括情報セキュリティ責任者及び情報システム管理者の許可を得なければならない。

（１９） 無許可でのネットワーク接続の禁止

職員等は、統括情報セキュリティ責任者の許可なくパソコンやモバイル端末をネットワークに接続してはならない。

（２０） 業務以外の目的でのウェブ閲覧の禁止

①職員等は、業務以外の目的でウェブを閲覧してはならない。

②統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、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。

（２１）Web 会議サービスの利用時の対策

①統括情報セキュリティ責任者は、Web 会議を適切に利用するための利用手順を定めなければならない。

②職員等は、本市の定める利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

③職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。

④職員等は、外部から Web 会議に招待される場合は、本市の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

（２２）ソーシャルメディアサービスの利用

①情報セキュリティ管理者は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

(ア)本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理 Web サイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

(イ)パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（IC カード等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること。

②機密性２以上の情報はソーシャルメディアサービスで発信してはならない。

③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なければならない。

④アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。

⑤可用性２の情報の提供にソーシャルメディアサービスを用いる場合は、本市の自己管理 Web サイトに当該情報を掲載して参照可能とすること。

（解説）

（１） 文書サーバの設定等

文書サーバは、複数の課室等で共用している場合が多いため、職員等が利用可能な容量を取り決める必要がある。また、複数の課室等で利用している場合には、アクセス制御を行う必要がある。

（注１）土木部門等では、静止画像を業務で利用するために大容量の蓄積容量を使用し、共用の文書サーバでは容量不足が生じ、専用のディスク装置を執務室等に設置している場合がある。このような場合には、専用のディスク装置に備

わったセキュリティ機能を有効に活用するほか、物理的セキュリティ対策を実施する必要がある。

（2） バックアップの実施

緊急時に備え、ファイルサーバ等に記録される情報について、バックアップを取ることが必要である。

（注２）バックアップを行う場合には、データの保全を確保するため、バックアップ処理の成否の確認、災害等による同時被災を回避するためバックアップデータの別施設等への保管、システムを正常に再開するためのリストア手順の策定及びリストアテストによる検証が必要である。

（注３）バックアップはシステムの重要度に応じて、バックアップの取得間隔や遠隔地へのバックアップ保管の有無を決定しなければならない。

（3） 他団体との情報システムに関する情報等の交換

他団体との間で情報システムに関する情報及びソフトウェアを交換する場合は、その用途等を明確にして目的外利用や紛失、改ざん等が起こらないようにしなければならず、相手方の団体との間で当該内容を明記した合意文書を取り交わす等の対策を実施することが望ましい。

（4） システム管理記録及び作業の確認

情報システムに対して行った日常の運用作業については、記録を残しておくことが必要である。特に、システム変更等の作業を行った場合は、情報システムの現状を正確に把握するため、当該作業内容を記録し、詐取、改ざん等のないよう適正に管理しておくことが必要である。

また、システム変更等の作業を行う場合は、2 人以上で確認を行い、設定ミス、プログラムバグ等によるシステム障害のリスクを減らさなければならない。

（5） 情報システム仕様書等の管理

情報システム及びネットワークに関する文書は、悪意を持つ者に攻撃材料として使われるおそれがあることから、機密性３相当の文書として扱い、業務上必要のある者以外が閲覧したり、紛失等が生じないように管理する必要がある。

（6） ログの取得等

ログ（アクセスログ、システム稼動ログ、障害時のシステム出力ログ）及び障害対応記録は、第三者等による不正侵入や不正操作等の情報セキュリティインシデントを検知するための重要な材料となる。また、情報システムに係る情報セキュリティの上の問題が発生した場合には、当該ログ等は、事後の調査の過程で、問題を解明するための重要な材料となる。したがって、情報システムにおいては、仕様どおりにログ等が取得され、また、改ざんや消失等が起こらないよう、ログ等が適正に保存されなければならない。目的や取得する機器の明確化のほか、取得後において定期的又は必要に応じて確認をしなければならない。また、ログは１年以上保管することが望まし

い。なお、ログの保管期間については、システムが遵守すべき法令等によって定められている場合があるため、関係法令等を確認の上、決定する必要がある。

（注４）保管期限を設定し、期限が切れた場合は、これらの記録を確実に消去する必要がある。

（７） 障害記録

システム障害への対応を決める際、過去に起きた類似障害が参考になるので、障害記録を適正に保存しておく必要がある。

（注５）障害記録のデータベース化を図るなど、障害対応を決める場合に活用できるように保管しておくことが重要である。

（８） ネットワークの接続制御、経路制御等

ネットワーク上では、フィルタリング、ルーティング、侵入検知システム等が機能しているが、これらの機能を十分活用するため、ハードウェア及びソフトウェアの設定を適正に行うよう注意する必要がある。また、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

なお、クラウドサービスを利用し、住民情報等の重要な情報を外部のデータセンターとやり取りする場合は、VPN 接続による通信経路の暗号化や本人認証等の高度なセキュリティ対策を実施する必要がある。さらに、仮想ネットワークを構築する場合には、仮想ネットワークと物理ネットワークとの対応関係、仮想ネットワークの運用設定方針及び設定承認方針並びに庁内設備をクラウドサービスに移行する場合の注意事項等について確認し、適正な対策を講じる必要がある。

（９） 外部の者が利用できるシステムの分離等

電子申請受付システム、庁舎を訪問した住民等に対する庁舎案内システムなど、外部の者が利用できるシステムは、不正アクセス等を防御するため、必要に応じ、他のシステムのネットワークと切り離すなどの措置が必要である。

（１０） 外部ネットワークとの接続制限等

インターネットに接続し、公開しているウェブサーバ等が、外部から攻撃を受けた場合に、庁内ネットワークへの侵入を可能な限り阻止するために、庁内と外部ネットワークの境界にファイアウォールを設置する必要がある。

（注６）このほか、非武装セグメントを設け公開サーバを接続すると有効である。また、非武装セグメントに接続している公開サーバについて、不要なポートの閉鎖、不要なサービスの無効化、エラーメッセージの簡略化(攻撃者に対して、システムの技術情報を過度に表示し、与えない対策)を実施することによって、防御能力を高めることができる。

（１１） 複合機のセキュリティ管理

（注７）プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器を「複合機」という。複合機は、庁内ネットワークや公

衆電話網等の通信回線に接続して利用されることが多く、その場合には、ウェブによる管理画面を始め、ファイル転送、ファイル共有、リモートメンテナンス等多くのサービスが動作するため、様々な脅威が想定されることに注意が必要である。

（１２） IoT 機器を含む特定用途機器のセキュリティ管理

テレビ会議システム、IP 電話システム、ネットワークカメラシステム、入退管理システム、施設管理システム、環境モニタリングシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている又は電磁的記録媒体を内蔵しているものを「特定用途機器」という。これらの機器についても当該機器の特性や取り扱う情報、利用方法、通信回線の接続形態等により想定される脅威に注意が必要である。例えば、テレビ会議システム、IP 電話システム等は組織等 LAN を経由してインターネットに接続されて利用されることが想定され、その場合外部からの攻撃対象となり得る。これらの IoT 機器等の脆弱性がサイバー攻撃の標的となることが懸念される。また、内蔵電磁的記録媒体を備える場合は、運用終了時に内蔵電磁的記録媒体に残された情報が漏えいするおそれがある。そのため、特定用途機器の特性に応じて、以下の対策を講じる必要がある。

・特定用途機器について、認証情報を初期設定から変更した上で、適切に管理する。
・特定用途機器にアクセスする主体に応じて必要な権限を割り当て、管理する。
・特定用途機器が備える機能のうち利用しない機能を停止する。
・インターネットと通信を行う必要のない特定用途機器については、当該特定用途機器をインターネットやインターネットに接点を有する情報システムに接続しない。
・特定用途機器がインターネットを介して外部と通信する場合は、ファイアウォール等の利用により適切に通信制御を行う。
・特定用途機器のソフトウェアに関する脆弱性の有無を確認し、脆弱性が存在する場合は、バージョンアップやセキュリティパッチの適用、アクセス制御等の対策を講ずる。
・特定用途機器に対する不正な行為、無許可のアクセス等の意図しない事象の発生を監視する。
・特定用途機器を廃棄する場合は、特定用途機器の内蔵電磁的記録媒体に保存されている全ての情報を抹消する。

（注８）IoT 機器に関するセキュリティ対策については、「IoT セキュリティガイドライン ver 1.0」（平成 28 年 7 月　IoT 推進コンソーシアム 総務省 経済産業省）を参照されたい。

（１３） 無線 LAN 及びネットワークの盗聴対策

無線 LAN を利用する場合は、解読が困難な暗号化及び認証技術を使用し、アクセ

スポイントへの不正な接続を防御する必要がある。特に、LGWAN 接続系で無線 LAN を利用する場合は、盗聴及びなりすましアクセスポイント（AP）などによる情報漏えいや不正アクセスに対して、認証サーバを利用した WPA2/WPA3 エンタープライズによる認証（IEEE802.1X 認証）を採用する等、セキュリティ対策を実施しなければならない。遵守すべきセキュリティ要件は、「庁内無線 LAN のセキュリティ要件について」を参照されたい。なお、マイナンバー利用事務系においては、無線 LAN は利用しないこととしなければならない。

（注９）暗号化方式の１つである WEP（Wired Equivalent Privacy）/WPA（Wi-Fi Protected Access）については、既に脆弱性が公知となっているため、暗号強度が確認されている暗号方式（WPA2/WPA3）を採用しなければならない。

（注１０）アクセスポイントの管理者パスワードを適切に設定（強固な ID・パスワードの設定、アクセスポイント単位での管理など）を行うとともに、無線端末間の通信が行われないよう適切な設定を行わなければならない。また、無線 LAN の不正利用調査を行い、探査ツール等を用い、無許可のアクセスポイントや使用されていないアクセスポイントが設置されていないことを点検することも有益である。

（１４） 電子メールのセキュリティ管理

メールサーバに対するセキュリティ対策等、電子メールのセキュリティ管理について定める。外部からの電子メール受信及び外部への電子メール送信においてなりすましを防ぐため、メールサーバのセキュリティ対策として電子署名を用いた DKIM（DomainKeys Identified Mail）や SPF（Sender Policy Framework）等の対策を実施するとともに、DMARC（Domain-based Message Authentication, Reporting & Conformance）も実施しなければならない。また、インターネットを介して通信する電子メールの盗聴及び改ざんの防止のため、SMTP によるサーバ間通信を TLS ~~(SSL)~~ による保護や、S/MIME 等の電子メールにおける暗号化及び電子署名の技術の利用等、電子メールのサーバ間通信の暗号化の対策を講ずることも考えられる。

加えて、電子メールの不正な中継を行わないようにメールサーバを設定しなければならない。外部へ情報を持ち出すために電子メールが用いられることを考慮し、フィルタリングソフトウェア等による監視を実施することが望ましい。

中継処理の禁止は、メールサーバが踏み台となり他のサーバに攻撃を行うことを防止するために必要がある。

職員等が電子メールの送信等により情報の外部への不正な持ち出しをしていないか監視するためには、フィルタリングソフトウェア等を利用する。

（注１１）上司など指定した職員に同報しなければ、送信できないように設定し、外部への持ち出しを牽制する方法もある。

（注１２）電子メールの送信に使われる通信方式の１つである SMTP（Simple Mail Transfer Protocol）では、差出人のメールアドレスを誰でも自由に名乗ることができるため、送信者のアドレス詐称（なりすまし）が容易にできる問題がある。このため、電子メールのなりすまし対策として、「送信ドメイン認証技術」を採用しなければならない。なお、送信ドメイン認証技術については、「送信ドメイン認証技術導入マニュアル」（迷惑メール対策推進協議会）を参照されたい。

（注１３）職員等は、庁外に電子メールにより情報を送信する場合は、当該電子メールのドメイン名にあらかじめ指定された「lg.jp」ドメイン名を使用することが望ましい。ただし、当該庁外の者にとって、当該職員等が既知の者である場合は除く。

（１５） 電子メールの利用制限

職員等が電子メールを利用する際の取扱いについて規定したものである。不正な情報の持ち出しを防止する観点から、電子メールの自動転送を禁止する。

プロバイダーが提供するサービスである、電子メールやオンラインストレージサービスに対しては、外部への不正な情報の持ち出し等に利用される場合があることから、適正なセキュリティ対策を講じる必要がある。

複数の送信先に電子メールを送る場合、他の送信先の電子メールアドレスが分からないようにするには、宛先や CC ではなく、BCC に送信先を入力する方法がある。

（注１４）受信した電子メールをテキスト形式で表示するメールソフトの機能を有効化することによって、マルウェア感染の可能性の低減を図ることができる。

（１６） 電子署名・暗号化

職員等が自由に暗号方法を利用すると、暗号鍵を紛失した場合に、復号が困難になり、データ自体が完全に破壊されたのと同じ状態になってしまうため、暗号方法は組織として特定の方法を定める必要がある。

その方法について情報システム管理者は、 暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を参照した上で、情報システム及び電子署名のアルゴリズム並びにそれを使用した安全なプロトコル及びその運用方法について、定めなければならない。

また、署名検証者が電子署名を検証するための電子証明書を信頼できる機関からダウンロードできる環境を整備したり、電子署名の付与を行う情報システム管理者から電磁的記録媒体等で入手できる体制を整備する必要がある。暗号化された情報の復号又は電子署名の付与に用いる鍵の管理手順として、鍵のライフサイクルを考慮した管理手順を策定することが望ましい。

なお、電子署名を行うに当たっては、地方公共団体組織認証基盤(LGPKI：Local

Government Public Key Infrastructure）の利用など、目的に応じた適切な公開鍵基盤を使用するように定めること。

（１７） 無許可ソフトウェアの導入等の禁止

インターネットからソフトウェアをダウンロードし、パソコンやモバイル端末に導入すると、不正プログラムの感染、侵入の可能性が高まることや、導入済みのソフトウェアに不具合が発生する場合もあり、許可を得ない導入は禁止する必要がある。また、不正にコピーしたソフトウェアは、ライセンス違反や著作権法違反となることから、明確に禁止しなければならない。なお、許可を得てインターネットからソフトウェアをダウンロードする場合においても、提供元のサイト等の信頼性が確保できることを確認した上で入手する必要がある。

（注１５）あらかじめ、一定のソフトウェアを指定して、その範囲では個別の許可を不要とする運用もあり得る。

（１８） 機器構成の変更の制限

職員等が、メモリ増設等の際に静電気を発生させるなど、パソコンを故障させたり、ネットワーク全体にも悪影響を及ぼす可能性があり、許可を得ない構成変更は禁止する必要がある。

（１９） 無許可でのネットワーク接続の禁止

セキュリティ上、ネットワークとの接続には適正な管理が必要であることから、無許可での接続を禁止する。あわせて、接続が許可されたものであることを確認するための措置を講じるとともに、許可手続を定める必要がある。（支給以外の端末を接続する場合も同様とする。）

（注１６）庁外の通信回線に接続した支給以外の端末を庁内の通信回線に接続することの許可手続として、以下を含む手続を規定し、職員等に遵守させること。

・利用時の許可申請手続

・手続内容（利用者、目的、利用する情報、端末等）

・利用期間満了時の手続

・庁内通信回線への接続時の手続（端末の事前検疫等）

・許可権限者（情報セキュリティ管理者）による手続内容の記録

（注１７~~６~~）特に、庁内で無線 LAN を使用している場合に、職員等や外部委託事業者がパソコンやモバイル端末等を持込み、無許可でアクセスポイントへ接続する行為を禁止する必要がある。

（２０） 業務以外の目的でのウェブ閲覧の禁止

業務外の外部サイトを閲覧している場合、不正プログラムの感染、侵入の可能性が高まるため、業務以外の目的でのウェブ閲覧は禁止しなければならない。また、閲覧先サイトのサーバにドメイン名等の組織を特定できる情報がログとして残ることにより、外部から指摘を受けるようなことがあってはならない。統括情報セキュリティ

責任者は、業務外での閲覧を発見した場合は、情報セキュリティ管理者に通知し、対応を求めなければならない。

（２１） Web 会議サービスの利用時の対策

職員等は、Web 会議サービスの利用に当たり、以下の情報セキュリティ対策を実施する必要がある。

・支給する端末を利用すること。

・許可された Web 会議サービスを利用すること。

・利用する Web 会議サービスのソフトウェアが、最新の状態であることを確認すること。

・機密性２以上の情報を取り扱う場合は、可能な限りエンドツーエンド（E2E）の暗号化を行うこと。

・機密性２以上の情報を取り扱う場合は、Web 会議サービスの議事録作成機能、自動翻訳機能及び録画機能等、E2E の暗号化を利用できなくなる機能を可能な限り使用しないこと。

・音声を扱う場合は、ヘッドホンを使用するなど、内容が周囲に漏れないよう注意すること。

また、職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう以下の情報セキュリティ対策を講ずる必要がある。

・会議室にアクセスするためのパスワード等をかける。

・会議の参加者に会議室にアクセスするためのパスワード等を通知する際は、第三者に知られないよう安全な方法で通知する。

・待機室を設けて参加者と確認できた者だけを会議室に入室させる。

・なりすましや入れ替わりが疑われるなどの不審な参加者を会議室から退室させる。

（注１８）Web 会議サービスを利用する場合、Web 会議サービスのソフトウェアで録画等を防止する設定を行っていても、ビデオカメラで撮影されれば会議内容は保存されるため、会議内容は会議の参加者に保存されることを前提として、会議で取り扱う情報を確認する必要がある。

（２２） ソーシャルメディアサービスによる情報発信

①情報セキュリティ責任者は、ソーシャルメディアの閲覧者の信頼を確保し、その情報セキュリティ水準の低下を招かないよう、以下を含む対策を手順として定めること。

（ア）アカウント運用ポリシー（ソーシャルメディアポリシー）を策定し、ソーシャルメディアのアカウント設定における自由記述欄又はソーシャルメディアアカウントの運用を行っている旨の表示をしている自組織の Web サイト上のページに、アカウント運用ポリシーを掲載する。特に、専ら情報発信に用いる場合には、

その旨をアカウント運用ポリシーに明示する。

（イ）URL 短縮サービスは、利用するソーシャルメディアサービスが自動的に URL を短縮する機能を持つ場合等、その使用が避けられない場合を除き、原則使用しない。

②情報セキュリティ責任者は、自組織のアカウントによる情報発信が実際のものであると認識できるようにするためのなりすまし対策として、以下を含む対策を手順として定めること。

（ア）自組織からの情報発信であることを明らかにするために、自組織のドメイン名を用いて管理している Web サイト内において、利用するソーシャルメディアのサービス名と、そのサービスにおけるアカウント名又は当該アカウントページへのハイパーリンクを明記するページを設けること。

（イ）自組織からの情報発信であることを明らかにするために、アカウント名やアカウント設定の自由記述欄等を利用し、自組織が運用していることを利用者に明示すること。

（ウ）運用しているソーシャルメディアのアカウント設定の自由記述欄において、当該アカウントの運用を行っている旨の表示をしている自組織の Web サイト上のページの URL を記載すること。

（エ）ソーシャルメディアの提供事業者が、アカウント管理者を確認しそれを表示等する、いわゆる「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合には、可能な限りこれを取得すること。

③情報セキュリティ責任者は、第三者が何らかの方法で不正にログインを行い、偽の情報を発信するなどの不正行為を行う、いわゆる「アカウント乗っ取り」を防止するために、ソーシャルメディアのログインパスワードや認証方法について、以下を含む管理手順を定めること。

（ア）パスワードを適切に管理すること。具体的には、ログインパスワードには十分な長さと複雑さを持たせた容易に推測されないものを設定するとともに、パスワードを知る担当者を限定し、パスワードの使い回しをしないこと。

（イ）二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用すること。

（ウ）ソーシャルメディアへのログインに利用する端末を紛失した又は当該端末が盗難に遭った場合は、当該端末を悪用され、アカウント乗っ取りの可能性があるため、当該端末の管理を厳重に行うこと。

（エ）ソーシャルメディアへのログインに利用する端末が不正アクセスされた場合、当該端末が不正に遠隔操作される又は、当該端末に保存されたパスワードが窃取される可能性がある。これらを防止するため、少なくとも端末には最新のセキュリティパッチの適用や不正プログラム対策ソフトウェアを導入するなど、

適切なセキュリティ対策を実施すること。

④情報セキュリティ責任者は、なりすましや不正アクセスを確認した場合の対処として、以下を含む対処手順を定めること。

（ア）自己管理 Web サイトに、なりすましアカウントが存在することや当該ソーシャルメディアを利用していないこと等の周知を行い、また、信用できる機関やメディアを通じて注意喚起を行うこと。

（イ）アカウント乗っ取りを確認した場合には、被害を最小限にするため、ログインパスワードの変更やアカウントの停止を速やかに実施し、自己管理 Web サイト等で周知を行うとともに、自組織のエスカレーションルールに従い報告すること。

6.2.　アクセス制御

【趣旨】

情報システム等がアクセス権限のない者に利用できる状態にしておくと、情報漏えいや情報資産の不正利用等の被害が発生し得る。そこで、アクセス制御を業務内容、権限ごとに明確に規定しておく必要がある。また、不用意なアクセス権限付与による不正アクセスを防ぐために、アクセス権限の管理は統括情報セキュリティ責任者及び情報システム管理者に集約することが重要である。

このことから、利用者登録や特権管理等を用いた情報システムへのアクセス制御、ログイン手順、接続時間の制限等不正なアクセスを防止する手段について規定する。

また、働き方改革実行計画（平成 29 年 3 月 28 日　働き方改革実現会議決定）により、柔軟な働き方に対応しやすい環境整備が求められているところ、職員等が業務を遂行する上で、必ずしも勤務庁舎に出勤する必要はなく、自宅やサテライトオフィス等から遠隔で業務を遂行する形態への対応が求められることとなった。また、大規模感染症の感染予防対策として、勤務庁舎への出勤が抑制されるような状況下では、大半の職員等が勤務庁舎以外から業務を遂行できるようにテレワーク環境の整備が必要となり、その実施に必要な対策についても解説する。

【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、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。

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の特権を代行する者は、統括情報セキュリティ責任者及び情報システム管理者が指名し、CISO が認めた者でなければならない。

（ウ）CISO は、代行者を認めた場合、速やかに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及び情報システム管理者に通知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、特権を付与された ID 及びパスワードの変更について、外部委託事業者に行わせてはならない。

（オ）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、特権を付与された ID 及びパスワードについて、職員等の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

（カ）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、特権を付与された ID を初期設定以外のものに変更しなければならない。

（２） 職員等による外部からのアクセス等の制限

①職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、統括情報セキュリティ責任者及び当該情報システムを管理する情報システム管理者の許可を得なければならない。

②統括情報セキュリティ責任者は、内部のネットワーク又は情報システムに対する外部からのアクセスを、アクセスが必要な合理的理由を有する必要最小限の者に限定しなければならない。

③統括情報セキュリティ責任者は、外部からのアクセスを認める場合、システム上利用者の本人確認を行う機能を確保しなければならない。

④統括情報セキュリティ責任者は、外部からのアクセスを認める場合、通信途上の盗聴を防御するために暗号化等の措置を講じなければならない。

⑤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、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

⑥職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状

況等を確認し、情報セキュリティ管理者の許可を得るか、もしくは情報セキュリティ管理者によって事前に定義されたポリシーに従って接続しなければならない。

⑦統括情報セキュリティ責任者は、公衆通信回線（公衆無線 LAN 等）の庁外通信回線を庁内ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者の ID、パスワード及び生体認証に係る情報等の認証情報並びにこれを記録した媒体（IC カード等）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

（3） 自動識別の設定

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、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。【推奨事項】

（4） ログイン時の表示等

情報システム管理者は、ログイン時におけるメッセージ、ログイン試行回数の制限、アクセスタイムアウトの設定及びログイン・ログアウト時刻の表示等により、正当なアクセス権を持つ職員等がログインしたことを確認することができるようシステムを設定しなければならない。

（5） 認証情報の管理

①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、職員等の認証情報を厳重に管理しなければならない。認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

②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、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させなければならない。

③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、認証情報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。

（6） 特権による接続時間の制限

情報システム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

（解説）

（１） アクセス制御

管理者権限（サーバ等の全ての機能を利用できる権限）等の特権は、全ての機能を利用可能にするので、利用者登録を厳格に行うとともに、特権で利用する ID 及びパスワードを厳重に管理する必要がある。

情報システムの管理者とデータベースの管理者を別にすることが望ましい。データベースに対するアクセス管理、データの暗号化、脆弱性対策の実施と、管理権限の不適切な付与の検知について措置を講じることが望ましい。

アクセス制御の要件を定めるにあたっては、必要に応じて、以下を例とするアクセス制御機能の要件を定めることが望ましい。

a)利用時間や利用時間帯によるアクセス制御

b)同一主体による複数アクセスの制限

c)IP アドレスによる端末の制限

d)ネットワークセグメントの分割によるアクセス制御

（注１）外部委託事業者が利用する場合にも、ID 及びパスワードの利用については、全て統括情報セキュリティ責任者及び情報システム管理者が管理しなければならない。

（注２）管理者権限等の特権の悪用を防ぐために、「セキュア OS」（これまでの OS では対応できなかったアクセス制御を実施し、セキュリティ強化を図る機能）を利用することが考えられる。セキュア OS は、「強制アクセス制御」及び「最小特権」の機能に特徴がある。

強制アクセス制御	特権の操作に対しても、情報へのアクセス制御を実施させる機能
最小特権	特権の ID を利用できる者でも、強制アクセス制御機能で必要最小限のアクセスしか認めない機能

（注３）ファイルベースでのアクセス制御を行うことも考えられる。その場合には、ファイルに記録された情報へのアクセスを制御するサーバにおいて主体認証を受けたユーザのみが、暗号化されたファイルに記録された情報に対し、与えられた権限の範囲でアクセス可能とすることをアクセス制御機能の要件とすることが望ましい。

（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。その際、通信する情報の機密性に応じて、ファイル暗号化、通信経路の暗号化、専用回線の利用等の必要な措置を実施することが求められる。また、接続に当たっては許可制とし、許可は必要最小限の者に限定しなければならない。

職員等がテレワークにより庁内ネットワークや情報システムに接続を認める場合、情報資産の重要性を踏まえて対象となる資産を明確化し、テレワーク等で扱うことができる情報資産やテレワーク実施時の情報セキュリティ対策について規則を整備するとともに、外部からの不正な通信、マルウェアによる情報漏えいを防ぐためにアクセス制御等の技術的対策を行うことが求められる。また、なりすまし、情報漏えい及び盗難・紛失といったリスク等を踏まえ、取り扱う情報の重要度を勘案しつつ、適切なセキュリティ対策を講じる必要がある。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。

（LGWAN 接続系のテレワークを認める場合のセキュリティ対策について）

LGWAN 接続系の情報資産には、職員の個人情報等重要な情報資産が配置されている。テレワークにおいては、情報資産の重要性を踏まえ、取り扱う情報資産を明確にする必要がある。また、取り扱う情報の重要性に応じて、テレワークの実施可否の規則を整備するとともに、アクセス制御等の技術的対策を行わなければならない。なお、大量又は機微な住民情報を扱う業務がある場合、庁舎と同等の物理的な対策がなされたサテライトオフィスでの場合を除き、テレワークの対象外とすることが適当である。

また、以下のリスクとセキュリティ対策の方向性のとおり、適切なセキュリティ対策を行わなければならない。

リスク		概要	対策の方向性
①なりすまし		悪意のある第三者の ID・パスワードの窃取等により、庁内システムが不正アクセスされるリスク	許可された端末・職員のみ可能となるよう認証の仕組みの整備
②漏えい（盗聴・改ざん等）	通信	インターネット上で、悪意のある第三者に通信内容を傍受されるリスク	通信回線は、閉域網を使用する等、安全な接続方式を採用
	データ	不正アクセスにより、データを窃取／改ざんされるリスク	端末内での業務データ非保持（端末仮想化等）、端末データの暗号化等、第三者による端末の操作・データ窃取の防止や被害拡大を防ぐ仕組みの整備

③盗難/紛失	端末の盗難・紛失により、情報漏洩するリスク	盗難／紛失時に端末内の情報をリモートで管理できる仕組みの整備
④不正利用	利用者が故意又は過失により、システムを不正に利用することに起因するリスク 例）権限を持たない第三者による不正なアクセスフリーソフト等許可されていないアプリケーションに起因したウイルス感染	権限に応じた情報へのアクセス制限、ポリシーの一元管理 業務に不要なアプリケーション導入の制限 操作ログの収集・管理
⑤不正持出し	利用者が故意又は過失により、不正なデータ持ち出しを行うリスク 例）外部記録媒体などを用いたデータ不正持ち出し	端末に対する記録媒体の接続制限
⑥脆弱性・マルウェア	OS やソフトウェアの脆弱性を利用した攻撃により、端末がウイルスに感染するリスク 感染端末がセキュリティホールとなり、庁内のサーバや端末等に不正アクセスやウイルス感染を引き起こすリスク	端末の OS／ソフトウェアの適切なプログラム更新、パターンファイルの最新化 ネットワークのセキュリティ対策の実施
※上記リスクのうち①～③がリモートアクセス特有のリスク		

図表 25　テレワークにおけるリスクと対策の方向性

具体的には、以下のモデルを採用し、各モデルを導入する際は、「新型コロナウィルスへの対応等を踏まえた LGWAN 接続系のテレワークセキュリティ要件について」（令和 2 年 8 月 18 日総行情第 111 号　総務省自治行政局地域情報政策室長通知）にある技術要件を遵守しなければならない。

インターネット回線を使用しないモデル：

・閉域 SIM による接続サービスを利用するモデル

インターネット回線を使用するモデル：

・LGWAN-ASP サービスを利用して庁内にある LGWAN 接続系の端末に接続するモデル

・インターネット接続系を経由して LGWAN 接続系の端末に接続するモデル

（注４）テレワークのセキュリティ対策については、「テレワークセキュリティガイドライン（第５~~4~~版）」（令和３~~平成 30~~年５~~4~~月　総務省）を併せて参照されたい。

（注５）持ち込んだモバイル端末を確認するシステムとして、検疫システムがある。検疫システムとは、OS のパッチやコンピュータウイルス対策ソフトウェアのパターンファイルが最新でない、不正プログラムが侵入しているなど、十分な

セキュリティ対策が実施されていないモバイル端末を庁内ネットワークに接続させないシステムである。モバイル端末を庁内に持ち帰った場合等に、検疫システムによる確認を義務付けることにより、様々な脅威の発生を防止する。

（注６）庁外から庁内のネットワークや情報システムにアクセスする際に公衆無線 LAN 等の庁外通信回線を利用することは原則禁止であるが、やむを得ず利用する場合は、統括情報セキュリティ責任者の許可を得た上で、必要最小限の範囲のみのアクセスとする。さらに、ログを取得し、不正なアクセスがないかを定期的に確認することが求められる。

（注７）画面ののぞき見や盗聴を防止できるような環境を選定することで情報の漏えい対策につながる。また、テレワーク実施時の離席時の端末等の盗難に注意する。

（注８）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、テレワーク実施時の情報セキュリティ対策を確実に実施させるため、テレワーク実施前及び実施後に、端末に情報を保存させない等のチェックすべき項目を定め、職員等に当該チェックを実施させること。

（３） 自動識別の設定

ネットワークに不正な機器の接続を防止するために、電子証明書による端末認証や、接続する機器の IP アドレス、MAC アドレス等の認証情報を利用し制限する必要がある。

（４） ログイン時の表示等

ソフトウェアに、ログイン試行回数の制限や、直近に使用された日時が表示される機能等がある場合は、それらを有効に活用し、不正にパソコン等の端末が利用されないようにする必要がある。

（５） 認証情報の管理

認証機能として、指紋又は顔等を利用した生体認証、スマートカードを利用した認証及びパスワード認証等が存在する。認証の機能は、ソフトウェアにより様々な認証機能があるために、これらの機能を有効に利用することが求められる。認証機能を利用するにあたり、認証情報を不正利用から保護する必要があり、オペレーティングシステム等で認証に関する設定のセキュリティ強化を行わなければならない。認証情報の管理について、以下の点に注意する必要がある。

①パスワード認証を利用する際は情報システム間で同一パスワードの使い回しを行ってはならない。

②スマートカードを利用する際は紛失時に直ちにそのカードを無効化する等の処置を講じなければならない。

③利用者が認証情報を変更する際に、以前に設定した認証情報の再設定を防止す

る機能を実装することが望ましい。

④利用者が情報システムを利用する必要がなくなった場合は、ID の無効化や認証情報の廃棄等、当該利用者の ID や認証情報の不正な利用を防止するための措置を講じなければならない。

利用するパスワードの機能は、「5.4. ID 及びパスワード等の管理」に記載されているパスワードの取扱いに従い、パスワードを設定する必要がある。

（6） 特権による接続時間の制限

管理者権限等の特権を利用している際に、システムにログインしたままで端末を放置しておくと、他者に不正利用されるおそれがあることから、システムの未使用時には自動的にネットワーク接続を終了するなどの措置を講じる必要がある。

6.3. システム開発、導入、保守等

【趣旨】

システム開発、導入、保守等において、技術的なセキュリティ対策が十分に実施されていない場合は、プログラム上の欠陥（バグ）によるシステム障害等により業務に重大な支障が生じるおそれがある。このことから、システム開発、導入、保守のそれぞれの段階における対策を規定する。なお、本規定にはシステムの更新又は統合時の十分な検証等も含まれる。

【例文】

（1） 情報システムの調達

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、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記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、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

①システム開発における責任者及び作業者の特定

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を特定しなければならない。また、システム開発のための規則を確立しなければならない。

②システム開発における責任者、作業者の ID 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 ID を管理し、開発完了後、開発用 ID を削除しなければならない。

（イ）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のアクセス権限を設定しなければならならない。

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。

（3） 情報システムの導入

①開発環境と運用環境の分離及び移行手順の明確化

（ア）情報システム管理者は、システム開発、保守及びテスト環境とシステム運用環境を分離しなければならない。【推奨事項】

（イ）情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。

（ウ）情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実に行い、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。

（エ）情報システム管理者は、導入するシステムやサービスの可用性が確保されていることを確認した上で導入しなければならない。

②テスト

（ア）情報システム管理者は、新たに情報システムを導入する場合、既に稼働している情報システムに接続する前に十分な試験を行わなければならない。

（イ）情報システム管理者は、運用テストを行う場合、あらかじめ擬似環境による操作確認を行わなければならない。

（ウ）情報システム管理者は、個人情報及び機密性の高い生データを、テストデータに使用してはならない。

（エ）情報システム管理者は、開発したシステムについて受け入れテストを行う場合、開発した組織と導入する組織が、それぞれ独立したテストを行わなければならない。

（４） システム開発・保守に関連する資料等の整備・保管

①情報システム管理者は、システム開発・保守に関連する資料及びシステム関連文書を適正に整備・保管しなければならない。

②情報システム管理者は、テスト結果を一定期間保管しなければならない。

③情報システム管理者は、情報システムに係るソースコードを適正な方法で保管しなければならない。

（５） 情報システムにおける入出力データの正確性の確保

①情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力を除去する機能を組み込むように情報システムを設計しなければならない。

②情報システム管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計しなければならない。

③情報システム管理者は、情報システムから出力されるデータについて、情報の処理が正しく反映され、出力されるように情報システムを設計しなければならない。

（６） 情報システムの変更管理

情報システム管理者は、情報システムを変更した場合、プログラム仕様書等の変更履歴を作成しなければならない。

（７） 開発・保守用のソフトウェアの更新等

情報システム管理者は、開発・保守用のソフトウェア等を更新又はパッチの適用をする場合、他の情報システムとの整合性を確認しなければならない。

（８） システム更新又は統合時の検証等

情報システム管理者は、システム更新・統合時に伴うリスク管理体制の構築、移行基準の明確化及び更新・統合後の業務運営体制の検証を行わなければならない。

（解説）

（１） 情報システムの調達

情報システムを調達する場合は、当該情報システムで取り扱う情報の重要性に応じて、情報システムのライフサイクルで必要となるセキュリティ機能を洗い出し、調達要件に含める必要がある。例えば、アクセス制御の機能、パスワード設定機能、ログ取得機能、データの暗号化等である。

（注１）情報機器及びソフトウェア等の情報セキュリティ機能の評価に当たっては、第三者機関による客観的な評価である、ISO/IEC15408 に基づく IT セキュリティ評価及び認証制度による認証の取得の有無を評価項目として活用することも考えられる。また、構築する情報システムに重要な情報セキュリティ要件があると認められた場合には、第三者機関による当該情報システムのセキュリティ設計仕様書（ST: Security Target）の ST 評価・ST 確認を活用することも考えられる。「IT セキュリティ評価及び認証制度（JISEC）」については、独立行政法人情報処理推進機構のサイトを参照のこと。

（注２）情報システム管理者は、システム調達、開発、導入を行うに当たっては、CISO の許可を得て実施することが望ましい。また、情報システム管理者は、情報システムのライフサイクル全般にわたって情報セキュリティの維持が可能な体制の確保を、CISO に求めることが望ましい。

CISO は体制の確保に際し、CIO の協力を得ることが必要な場合は、CIO に当該体制の全部又は一部の整備を求めることが望ましい。

（注３）情報システムの利用を満足できるものにするためには、情報システムが当

該利用に足りる十分な処理能力と記憶容量を持つことが必要である。また、処理能力と記憶容量の使用状況を監視し、将来的に必要とされる能力・容量を予測して、ハードディスクの増強等適正な措置を講じることが望まれる。

（注４）情報システムは可用性の観点から、冗長性を組み入れることを考慮することが望ましい。ただし、冗長性を組み入れることにより、情報システムの完全性、機密性に対するリスクが生じる可能性があるため、この点についても考慮すること。

・機密性を高める対策例

サーバを二重化することにより場合によっては機密性の高い情報が二カ所に保存されることになるため、修正プログラムの適用やソフトウェアの最新化、不要なサービスの停止といったセキュリティの確保を二重化した双方のサーバに同時・同等に実施する。

・完全性を高める対策例

二重化したサーバ内の情報の整合性を確保するために、双方のサーバ内のデータの突合確認や誤り訂正機能の実装などの対策を実施する。

（注５）IT 製品の調達において、その製品に他の供給者から供給される構成部品やソフトウェアが含まれる場合には、そのサプライチェーン全体に適正なセキュリティ慣行を伝達し、サプライチェーンの過程において意図せざる変更が加えられないよう、直接の供給者に要求することが必要である。また、提供された IT 製品が機能要件として取り決められたとおりに機能すること、構成部品やソフトウェアについてはその供給元が追跡可能であることを保証させることが望ましい。

（注６）調達する情報システムに応じた要件の詳細については、「非機能要求グレード（地方公共団体版）利用ガイド」（平成 26 年 3 月　地方自治情報センター）「IT 製品の調達におけるセキュリティ要件リスト」（平成 30 年 2 月 28 日　経済産業省）を参照されたい。

（注７）オンラインでの申請及び届出等の手続を提供するシステムについては、住民が情報システムのアクセス主体になることにも留意し、オンライン手続におけるリスクを評価した上で、認証に係る要件を策定する必要がある。

なお、オンライン手続におけるリスク評価等に関しては、「政府機関等の対策基準策定のためのガイドライン」（平成 30 年 7 月 25 日　内閣官房内閣サイバーセキュリティセンター）を参照されたい。

（２）　情報システムの開発

①　システム開発における責任者及び作業者の特定

システム開発においては、その責任の所在や実施体制を把握する観点から、責任者と作業者を特定する必要がある。また、システム開発の方針、手順等の規則を決

定し、開発に適用する必要がある。

（注８）システム開発において、作業進捗が悪い場合等に、要員の投入が逐次行われるケースがあるが、これらのことが、要員の調整等に不備が生じるケースがある。特に、業務~~外部~~委託でシステム開発を行う場合等は、その理由を明確にして、要員の変更や増減の許可をする必要がある。

② システム開発における管理者及び作業者の ID の管理

システム開発において、開発用の ID は、管理がずさんになりやすい傾向があることから、適正な管理が必要である。

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

外部委託事業者が選定した開発用ソフトウェアについて、一般的に利用が知られていないソフトウェアは、その理由を確認する必要がある。また、利用することとしたソフトウェア以外のソフトウェアは削除することとする。

（３） 情報システムの導入

① 開発環境と運用環境の分離及び移行手順の明確化

システム開発において、開発環境と運用環境が同一であると、運用環境で使用しているプログラムやファイルを誤って書き換えてしまうことが発生しやすくなるので、システムの開発環境と運用環境は、できる限り分離し、セキュリティに配慮した設計にすることが必要である。また、情報システム管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認しなければならない。

（注９）情報システムの導入に当たっては、利用する業務の内容や取り扱う情報の重要度に応じて、万一の障害に備えた冗長性や可用性が必要となる場合がある。事前に確認しておく事項としては、例えば次のものがある。

・その箇所が働かないとシステム全体が停止してしまう箇所の有無とその対策内容（冗長化・障害時の円滑な切り替えなど）

・広域災害対策の有無(バックアップ設備を遠隔地に配置しているなど)や対応方針（サービス継続を優先するかセキュリティ対策の確保を優先するかなど）

② テスト

運用環境への移行は、業務に精通している利用部門の協力を得て、擬似環境における操作についてテストを行い、その結果を確認した後に行う必要がある。

（４） システム開発・保守に関連する資料等の整備・保管

① システム開発や機器等の導入において、開発や機器等の導入に関する資料やシステム関連文書等は、保守や機器更新の際に必要となることから、適正に整備し保管することが必要である。

② 情報システム管理者は、所管する情報システムを構成するサーバ装置及び端末に関連する情報として、以下を含む文書を整備することが望ましい。

a) サーバ装置及び端末を管理する職員等及び利用者を特定する情報

b) サーバ装置及び端末の機種並びに利用しているソフトウェアの種類及びバージョン

c) サーバ装置及び端末で利用するソフトウェアを動作させるために用いられる他のソフトウェアであって、以下を含むものの種類及びバージョン

・動的リンクライブラリ等、ソフトウェア実行時に読み込まれて使用されるもの

・フレームワーク等、ソフトウェアを実行するための実行環境となるもの

・プラグイン等、ソフトウェアの機能を拡張するもの

・静的リンクライブラリ等、ソフトウェアを開発する際に当該ソフトウェアに組み込まれるもの

・インストーラー作成ソフトウェア等、ソフトウェアを開発する際に開発を支援するために使用するもの

d) サーバ装置及び端末の仕様書又は設計書

③ 情報システム管理者は、前項 b) 及び c) の情報を収集するため、自動でソフトウェアの種類やバージョン等を管理する機能を有する IT 資産管理ソフトウェアを導入するなどにより、これら情報を効率的に収集する手法を決定することが望ましい。

（5） 情報システムにおける入出力データの正確性の確保

情報システムの処理は、入力処理、内部処理、出力処理で構成されている。これらの処理を行うプログラムの設計が正確に行われないと、データが不正確なものになるおそれがある。

入力処理の際は、不正確なデータの取り込みが行われないよう、入力データの範囲チェックや不正な文字列等の入力を除去する機能を組み込むことが必要になる。

内部処理においても、データの抽出条件の誤りやデータベースの更新処理での計算式のミス等で、データ内容を誤った結果に書き換えてしまうことのないよう、これらを検出するチェック機能を持たせる必要がある。さらには、内部処理が正確に行われていた場合であっても、出力処理で誤った処理がされると、端末画面の表示や印刷物を利用する者に対して、誤ったデータ内容を認識させてしまうおそれがある。このことから、情報システムの処理した結果の正確性が確保されるよう、システム及びプログラムの設計を行う必要がある。

（注１０）ウェブシステムの設計においては、ソースコードの記述内容にセキュリティ機能の必要性を調査せずに設計が行われるとセキュリティホールを残してしまうことがある。そこで、セキュリティ上の機能要件を洗い出し、システム開発の計画時に盛り込む必要があるほか、現在、運用しているウェブシステムについても、これらのソースコードの記述内容にセキュリティホールが潜

んでいる場合があるため、ソースコードを確認する必要がある。

（注１１）ウェブアプリケーションの開発においては、セキュリティを考慮した実装を行わなければ脆弱性を作り込んでしまうおそれがある。適正なセキュリティを考慮したウェブサイトを構築するための注意点や脆弱性の有無の判定基準については、「安全なウェブサイトの作り方 改訂第７版」及びその別冊資料（平成 28 年１月 27 日 情報処理推進機構）を参照されたい。

また、ウェブサイトを構築する場合は、「lg.jp」ドメインを含む属性型・地域型 JP ドメイン名の使用を調達仕様書に含めることが必要である。「lg.jp」ドメインの適用が困難なサービスを利用する場合は、そのドメインが団体のものとは異なることとその理由を団体のウェブサイトに掲示することが望ましい。インターネットに公開するウェブサイトにおいては、転送される情報の盗聴及び改ざんの防止のため、全ての情報に対する暗号化及び電子証明書による認証の対策（常時 TLS~~（SSL）~~化）を講じることが望ましい。

（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、第三者に不正に取得され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。

（注１３）ウェブサイトや電子メール等を利用し、庁外の者が提供するウェブアプリケーション・コンテンツを告知する場合は、以下の対策を講じること。

・告知するアプリケーション・コンテンツを管理する組織名を明記する

・告知するアプリケーション・コンテンツの所在場所の有効性（リンク先の URL のドメイン名の有効期限等）を確認した時期又は有効性を保証する機関について明記する

・電子メールにて告知する場合は、告知内容についての問合せ先を明記する

（６） 情報システムの変更管理

情報システムのプログラムを保守した場合は、必ず変更履歴を作成しておくことが必要になる。変更履歴がないと、プログラム仕様書と実際のソースコードに不整合が生じ、変更時の見落としからシステム障害を招く可能性が高まる。

（７） 開発・保守用のソフトウェアの更新等

数年間のシステム開発等、長期の開発期間を要する場合には、運用環境のシステム保守状況を踏まえて、移行時にシステム障害が生じないように、開発環境のソフトウェアの更新を行っておく必要がある。ソフトウェアのバージョンが違っていたために、運用環境でシステムが緊急停止をすることや、他のシステムに影響を与えることがあり、これを未然に防止することが重要である。

（８） システム更新又は統合時の検証等

システムを更新又は統合する場合は、システムの長時間の停止や誤動作等による業務への影響が生じないように、事前に慎重な検証等を行っておく必要がある。

（注１４）検証等を行う事項としては、例えば次のものがある。

・システム更新又は統合作業時に遭遇する想定外の事象に対応する体制

・システム及びデータ移行手続が失敗した場合や移行直後に障害等が生じた場合における、旧システムへ戻す計画とその手順

・更新又は統合によって影響される業務運営体制

・システム及びデータ移行手続における検証チェックポイントや移行の妥当性基準の明確化

6.4. 不正プログラム対策

【趣旨】

情報システムにコンピュータウイルス等の不正プログラム対策が十分に実施されていない場合は、システムの損傷、情報漏えい等の情報セキュリティインシデントが発生するおそれがある。不正プログラム対策としては、不正プログラム対策ソフトウェアを導入するとともに、パターンファイルの更新、ソフトウェアのパッチの適用等を確実に実施することが基本であり、被害の拡大を防止することになる。

これらを踏まえ、不正プログラムの感染、侵入を予防し、さらには感染時の対応として取るべき手段を規定する。

【例文】

（1） 統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正プログラム対策として、次の事項を措置しなければならない。

①外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止しなければならない。

②外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止しなければならない。

③コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

④所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。

⑤不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

⑥不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

⑦業務で利用するソフトウェアは、パッチやバージョンアップなどの開発元のサポートが終了したソフトウェアを利用してはならない。

（2） 情報システム管理者の措置事項

情報システム管理者は、不正プログラム対策に関し、次の事項を措置しなければならない。

①情報システム管理者は、その所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアをシステムに常駐させなければ

ならない。

②不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。

③不正プログラム対策のソフトウェアは、常に最新の状態に保たなければならない。

④インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、市が管理している媒体以外を職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

⑤不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報システム管理者が許可した職員を除く職員等に当該権限を付与してはならない。

（３） 職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

①パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。

②外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。

③差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

④端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。

⑤添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルを LGWAN 接続系に取り込む場合は無害化しなければならない。

⑥統括情報セキュリティ責任者が提供するウイルス情報を、常に確認しなければならない。

⑦コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末において LAN ケーブルの取り外しや、通信を行わない設定への変更などを実施しなければならない。

（４） 専門家の支援体制

統括情報セキュリティ責任者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておかなければならない。

（解説）

（１） 統括情報セキュリティ責任者の措置事項

インターネットからの不正プログラム感染、侵入を防御するためには、庁内ネットワークとインターネットの境界で不正プログラム対策ソフトウェアを導入する必要がある。

（注１）不正プログラムには、コンピュータシステムの破壊、無差別の電子メールの送信による感染の拡散を行うコンピュータウイルスのほか、暗証番号やパスワード等を盗むことを目的にしているスパイウェアなど、多くの種類が存在している。また、ウィニー等のファイル共有ソフトウェアがコンピュータウイルスに感染したことによる情報漏えい事案が数多く発生している。

（注２）ソフトウェアの更新は、開発元等から提供されるセキュリティホールのパッチ適用やバージョンアップ等で行うが、これらは開発元がサポートしている期間内でのみ行うことができるため、適宜サポートが終了していないソフトウェアへ切り替え等を行う必要がある。なお、ソフトウェアの更新についてはパソコン等の端末だけでなくサーバやモバイル端末についても同様にOSの更新や修正プログラムを適用する必要がある。

（注３）インターネットからの不正プログラム感染、侵入を防御するための方式として、パターンファイルでは未知の不正プログラムの検知が難しいことから、不正プログラムの挙動を検知する方式等によって既知及び未知の不正プログラムの検知並びにその実行を防止する機能を有するソフトウェアを導入することも有益である。

（２） 情報システム管理者の措置事項

ウイルスチェック等のパターンファイルや不正プログラム対策ソフトウェアは常に最新の状態に保って利用することが不可欠である。

なお、インターネットに接続していないシステムは、不正プログラムの感染、侵入の可能性は低いが、原則として職員等が持ち込んだ電磁的記録媒体や古くから保管していた電磁的記録媒体から感染することもあり得るので、電磁的記録媒体の使用は組織内で管理しているものに限るとともに、不正プログラム対策ソフトウェアを開発元等から定期的に取り寄せ、パターンファイルの更新やパッチの適用を確実に実施することが必要である。

（３） 職員等の遵守事項

職員等には、不正プログラムに関する情報及び対策を周知して対策を徹底することが必要であり、特に、不審なメールやファイルの削除、不正プログラム対策ソフトウェアを常に最新の状態に保たせることが重要である。コンピュータウイルスに感染した兆候がある場合には、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応を行わなければならない。初動対応時の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末においてLANケーブルの取り外し（パソコン等の端末の場合）や、通信を行わない設定への変更（モバイル端末の場合）などを実施しなければならない。

（4） 専門家の支援体制

不正プログラム対策ソフトウェアの開発元等の専門家と連絡を密にし、不正プログラム感染時等に、支援を受けられるようにしておく必要がある。

6.5. 不正アクセス対策

【趣旨】

情報システムに不正アクセス対策が十分に実施されていない場合は、システムへの攻撃、情報漏えい、損傷、改ざん等の被害を及ぼすおそれがある。このことから、不正アクセスの防止又は被害を最小限にするため、不正アクセス対策として取るべき措置、攻撃を受けた際の対処及び関係機関との連携等について規定する。

【例文】

（1） 統括情報セキュリティ責任者の措置事項

統括情報セキュリティ責任者は、不正アクセス対策として、以下の事項を措置しなければならない。

①使用されていないポートを閉鎖しなければならない。

②不要なサービスについて、機能を削除又は停止しなければならない。

③不正アクセスによるウェブページの改ざんを防止するために、データの書換えを検出し、統括情報セキュリティ責任者及び情報システム管理者へ通報するよう、設定しなければならない。

④重要なシステムの設定を行ったファイル等について、定期的に当該ファイルの改ざんの有無を検査しなければならない。【推奨事項】

⑤統括情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

（2） 攻撃への対処

CISO 及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。また、総務省、都道府県等と連絡を密にして情報の収集に努めなければならない。

（3） 記録の保存

CISO 及び統括情報セキュリティ責任者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

（4） 内部からの攻撃

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、職員等及び外部委託事

業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（５） 職員等による不正アクセス

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、職員等による不正アクセスを発見した場合は、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、適正な処置を求めなければならない。

（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。

（７） 標的型攻撃

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、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じなければならない。~~情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。~~

（解説）

（１） 統括情報セキュリティ責任者の措置事項

使用されていない TCP/UDP ポートや不要なサービスは、不正アクセスによる侵入や悪用に利用される可能性が高いため、ポート閉鎖やサービス停止処理を行う。

（注１）重要なファイルの改ざんについては、改ざん検知ソフトウェアの利用によって、不正アクセス、不正プログラムの侵入を検知することが可能である。

（注２）DNS の導入時には以下の対策を講じなければならない。

・庁外からの名前解決の要求に応じる必要性があるかについて検討し、必要性がないと判断される場合は庁内からの名前解決の要求のみに応答をするよう措置を講じる。

・DNS キャッシュポイズニング攻撃から保護するための措置を講じる。

・キャッシュサーバにおいて、ルートヒントファイル（DNS ルートサーバの情報が登録されたファイル）の更新の有無を定期的（３か月に一度程度）に確認し、最新の DNS ルートサーバの情報を維持する。

（注３）庁内の CSIRT を活用して CISO への報告、各部部局への指示、ベンダとの情報共有及び報道機関への通知・公表などの対応を行うとともに、地方公共団体情報システム機構（自治体 CEPTOAR）等の関係機関や他の地方公共団体の同様の窓口機能、外部の事業者等と連携して情報共有を行うことが望ましい。

（２） 攻撃への対処

情報システムに対する攻撃予告があり、攻撃を受けることが確実な場合には、システム停止等の措置を講じなければならない。また、総務省、都道府県等との連絡を密にし、情報収集に努めなければならない。

（注４）攻撃を受けた際の対応として、「緊急時対応計画」に基づき、ログの確保、被害を受けた場合の復旧手順の策定、庁内関係者の役割等を再確認しておく必要がある。

（３） 記録の保存

外部から不正アクセスを受けた場合に、その記録としてログ、対応した記録等を保存しておくことは、事実確認、原因追及及び対策検討のため、必要であり、記録の保存について定めておく必要がある。

（注５）不正アクセスについてログ解析を行う場合は、証拠保全用と解析用と分けて保管する必要がある。

（４） 内部からの攻撃

庁内ネットワークに接続したパソコン、モバイル端末及び不正プログラムに感染した庁内サーバを使って、庁内のサーバや外部のサーバ等に攻撃を仕掛けられる場合があり、これらを監視しなければならない。

（注６）庁舎内で住民、観光客に公衆通信回線を提供する場合は、内部の情報システムとネットワークを切り分け、不正アクセスを防止する対策を講じなければならない。

（５） 職員等による不正アクセス

職員等が庁内にあるパソコンやモバイル端末を利用し、不正アクセスを発見した場合には、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。

（６） サービス不能攻撃

サービス不能攻撃は DoS（Denial of Service）攻撃や DDoS（Distributed Denial of Service）攻撃とも呼ばれている。第三者からサービス不能攻撃を受けた場合でも、情報システムの可用性を維持するために次の例のような対策を実施する必要がある。また、これらの対策が適正に実施されているかをモニタリングし、確かめる必要があ

る。

①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

・サーバ装置、端末及び通信回線装置について、サービス不能攻撃に対抗するための機能が実装されている場合は、これらを有効にする。

・通信事業者と協議し、サービス不能攻撃が発生時の対処手順や連絡体制を整備する。

②サービス不能攻撃を想定した情報システムの構築

・サービス不能攻撃を受けた場合を想定し、直ちに情報システムを外部ネットワークから遮断したり、通信回線の通信量を制限したりするなどの手段を有する情報システムを構築する。

・サービスを提供する情報システムを構築するサーバ装置、端末、通信回線装置及び通信回線を冗長化し、許容される時間内に切り替えられるようにする。

・サービス不能攻撃の影響を排除又は低減するための専用の対策装置を導入する。

③通信事業者の提供するサービスの利用

・通信事業者が別途提供する、サービス不能攻撃に係る通信の遮断等のサービスがある場合は、これを利用する。

④情報システムの監視及び監視記録の保存

・庁外からアクセスされるサーバ装置や、そのアクセスに利用される通信回線装置及び通信回線の中から、特に高い可用性が求められるものを優先的に監視する。

・監視の記録については、監視対象の状態の変動を考慮した上で記録を一定期間保管する。

（7） 標的型攻撃

標的型攻撃による外部から庁内への侵入を防ぐため、標的型攻撃メール受信時の人的対策のほか、電磁的記録媒体やネットワークに対する技術的対策についても次の例のような対策を実施する必要がある。また、これらの対策が適正に実施されているかをモニタリングし、確かめる必要がある。なお、対策の検討にあたっては、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」(平成 28 年 10 月 7 日 サイバーセキュリティ対策推進会議) 及び「高度サイバー攻撃対処のためのリスク評価等のガイドライン 付属書」(平成 28 年 10 月 7 日 内閣官房内閣サイバーセキュリティセンター) も参照されたい。

①人的対策例（標的型攻撃メール対策）

・差出人に心当たりがないメールは、たとえ興味のある件名でも開封しない。

・不自然なメールが着信した際は、電話等の別の手段で差出人にメール送信の事実を確認する。

・メールを開いた後で標的型攻撃と気付いた場合、添付ファイルは絶対に開かず、メールの本文に書かれた URL もクリックしない。
・標的型攻撃と気付いた場合、システム管理者に対して着信の事実を通知し、組織内への注意喚起を依頼した後に、メールを速やかに削除する。
・システム管理者は、メールやログを確認し、不正なメールがなかったかチェックする。（事後対策）

②電磁的記録媒体に対する対策例
・出所不明の電磁的記録媒体を内部ネットワーク上の端末に接続させない。
・電磁的記録媒体をパソコン等の端末に接続する際、不正プログラム対策ソフトウェアを用いて検査する。
・パソコン等の端末について、自動再生（オートラン）機能を無効化する。
・パソコン等の端末について、電磁的記録媒体内にあるプログラムを媒体内から直接実行することを拒否する。

③ネットワークに対する対策例
・ネットワーク機器のログ監視を強化することにより、情報を外部に持ち出そうとするなどの正常ではない振る舞いや外部との不正な通信を確認し、アラートムを発したりその通信を遮断する。
・不正な通信がないか、ログをチェックする。（事後対策）

6.6. セキュリティ情報の収集

【趣旨】

ソフトウェアにセキュリティホールが存在する場合、システムへの侵入、改ざん、損傷、漏えい等の被害を及ぼすおそれがある。また、情報セキュリティを取り巻く社会環境や技術環境等は刻々と変化しており、新たな脅威により情報セキュリティインシデントを引き起こすおそれがある。これらのことから、セキュリティホールをはじめとするセキュリティ情報の収集、共有及び対策を講じることについて規定する。

【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、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。

（2） 不正プログラム等のセキュリティ情報の収集・周知

統括情報セキュリティ責任者は、不正プログラム等のセキュリティ情報を収集し、必要に応じ対応方法について、職員等に周知しなければならない。

（3） 情報セキュリティに関する情報の収集及び共有

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、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

（解説）

（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

セキュリティホールは日々発見される性質のものであることから、積極的に情報収集及び対応の検討を行う必要がある。セキュリティホールの対策状況の定期的な確認により、セキュリティホールへの対策が講じられていない状態が確認された場合並びにサーバ装置、端末及び通信回線装置上で利用するソフトウェアに関連するセキュリティホールの情報を入手した場合には、セキュリティパッチの適用又はソフトウェアのバージョンアップ等による情報システムへの影響を考慮した上で、ソフトウェアに関するセキュリティホールへの対策計画を策定し、措置を講ずることが必要である。

（注１）セキュリティホールの情報収集に関しては、情報収集の体制、分析の手順、情報収集先、情報共有先等を決めておくことが望まれる。

（注２）セキュリティホールの緊急度のレベルに応じて、更新の実施の有無を検討する。深刻なセキュリティホールが発見された場合は、直ちに対応しなければならないが公開された脆弱性の情報がない段階においては、サーバ、端末及び通信回線上で取り得る対策を検討する。また、更新計画を定め、他のシステムへの影響、テスト方法、バックアップの実施、パッチの適用後のシステム障害が生じた場合の復旧手順等を盛り込むことが望ましい。

なお、近年の IT の利活用拡大により、システムで使用しているソフトウェア等の種類も増加していることから、IT 資産を手作業で漏れなく正確に把握するには多大な労力が必要となる。そのため、自動でソフトウェアの種類及びバージョンを管理する機能を有する IT 資産管理ソフトウェアを導入することが考えられる。また、脆弱性対策が計画通りに実施されないことは、システムの損傷、情報漏えい等の情報セキュリティインシデントが発生する原因にもなるため、脆弱性対策が計画どおり実施されていることについて、実施予定時期の経過後、遅滞なく確認することが望ましい。

（注３）不正プログラム、セキュリティホールのパッチの適用情報については、必要に応じ、イントラネットを利用して閲覧できるようにし、職員等に対して速やかに周知することが望ましい。

（注４）OS や各種サーバ、ファイアウォール等の通信回線装置等におけるセキュリティホールの対策状況を効率的に確認する方法として、専用ツールを用いて自らが脆弱性診断を行ったり、事業者が提供するサービス等を利用して脆弱性診断を行うことが挙げられる。脆弱性診断には、ソースコード診断、プラットフォーム診断、ウェブアプリケーション診断等の種類があり、ソフトウェアの種類によって利用する脆弱性診断を使い分ける必要がある。

ソースコード診断では、独自に開発したソフトウェアのソースコードを対象に、静的解析ツール等を用いて脆弱性の有無を検証する。したがって、運用開始までにソースコード診断を実施し、運用開始後にソースコードへ修正を加えた場合は、再度診断を実施することが望ましい。

プラットフォーム診断では、OS や各種サーバ、ファイアウォール等を対象に、テスト用の通信パケットを送信するなどの方法によって、最新のセキュリティパッチが適用されているか、設定が適切に行われているか、不要な通信ポートが開いていないかなどを検証する。したがって、運用開始までにプラットフォーム診断を実施し、その後も例えば年に１回診断を実施するなど、定期的に実施することが望ましい。

ウェブアプリケーション診断では、独自に開発したウェブアプリケーションを対象に、実際に不正なデータをウェブアプリケーションに送信するなどの方法によって、SQL インジェクションやクロスサイトスクリプティング等の脆弱性が存在しないかを検証する。したがって、運用開始までにウェブアプリケーション診断を実施し、運用開始後においても、ウェブアプリケーション

へ修正を加えた場合や新たな脅威が確認された場合は、再度診断を実施することが望ましい。

（２） 不正プログラム等のセキュリティ情報の収集・周知

（注５）セキュリティ情報の入手先としては、情報システムの納入業者のほかに、JPCERT/CC（一般社団法人 JPCERT コーディネーションセンター）、IPA（独立行政法人 情報処理推進機構）等がある。

（３） 情報セキュリティに関する情報の収集及び周知

情報セキュリティに関する技術は、新たな技術の開発や普及状況の変化により、期待した情報セキュリティの有効性が失われることや新技術への移行によって既存技術を利用したサービスを受けることができなくなる等、新たなリスクを発生する可能性もあり、情報システム等の情報セキュリティインシデントやセキュリティ侵害の未然の防止のために情報セキュリティに関する技術の動向や技術環境等の変化に関する情報収集と対策を講じる必要がある。

（注６）情報セキュリティに関する技術の変化による新たな脅威として、「重要インフラにおける情報セキュリティ確保に係る「安全対策基準等」策定に当たっての指針(第３版)対策編」（平成 22 年７月 30 日（平成 26 年３月 26 日改定）重要インフラ専門委員会）では、下記の事項が挙げられている。

・電子計算機の性能向上等により暗号の安全性が低下する「暗号の危殆化」

・インターネットの普及による IPv4 アドレス枯渇化に伴う「IPv6 移行」

また、情報収集と対策の検討に当たっては、必要に応じて、外部専門家等の活用も検討する必要がある。

（注７）暗号の危殆化については、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC 暗号リスト）」（平成 25 年３月１日（令和３~~２~~年４~~12~~月 ~~２~~1 日最終更新）総務省・経済産業省）及び同リストを策定した CRYPTREC の今後の報告を参考とすることができる。

（注８）TLS~~（SSL）~~暗号設定については、「TLS 暗号設定ガイドライン Ver3.0.1」(CRYPTREC 令和２年７月)を参照されたい。

（注９）IPv6 への移行については、IPv6 通信を導入する場合における他の情報システムへの影響や、IPv6 通信を想定していないネットワークに接続される全ての情報システム及びネットワークに対する IPv6 通信を抑止するための措置、IPv6 通信を想定していないネットワークを監視し、IPv6 通信が検知された場合には通信している装置を特定し、IPv6 通信を遮断するための措置を講じる必要がある。

（注１０）導入しているソフトウェア（OS を含む。）のサポートが終了した場合、新たな脆弱性が発見されたとしても修正プログラムが製造元から提供されず、情報の流出や第三者を攻撃するための踏み台として利用される等の可能性が高まるため、サポート期間の情報を収集し、適正な対策を講じる必要がある。

~~なお、Java、WindowsXP、Windows Vista、Windows7、Windows Server 2003~~

~~及び Windows Server 2008 等のサポート期限に関しては、総務省が発出した注意喚起文書等を参照されたい。~~

7. 運用

7.1. 情報システムの監視

【趣旨】

情報システムにおいて、不正プログラム、不正アクセス等による情報システムへの攻撃・侵入、部内職員の不正な利用、自らのシステムが他の情報システムに対する攻撃に悪用されることを防ぐためには、ネットワーク監視等により情報システムの稼働状況について常時監視を行うことが必要である。したがって、情報システムの監視に係る対策について規定する。

【例文】

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。

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、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる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、外部と常時接続するシステムを常時監視しなければならない。

④暗号化された通信データを監視のために復号することの要否を判断し、要すると判断した場合は、当該通信データを復号する機能及び必要な場合はこれを再暗号化する機能を導入しなければならない。【推奨事項】

（解説）

監視に必要な要素は、不正アクセスや不正利用の検知と記録（ログ等）である。情報システムの稼働状況について、インターネットからの不正アクセスの状況や部内職員の利用状況も含め、ネットワーク監視等により常時確認を行うことが必要である。また、記録については、証拠としての正確性を確保するために、サーバの時刻設定を正確に行う必要がある。サーバ間で時刻記録に矛盾が生じると、ログ解析等追跡が困難になるとともに、証拠としての正確性が担保できないことになる。

ウェブの常時暗号化（TLS~~(SSL)~~化）や電子メールサーバ間通信の暗号化（TLS~~(SSL)~~化）等といった通信の暗号化が社会的に進められ、その利用割合が上昇する中で、不正なプログラム等の脅威が暗号化された通信の中に含まれていると、当該通信の監視による脅威の検知が困難になる。このため、監視に際しては、監視対象のデータが暗号されているかどうかを把握し、対象とする脅威の監視可否に与える影響を考慮した上で復号の要否を判断し、必要と判断した場合にはその対策を講じなければならない。なお、自治体情報セキュリティクラウド側の機能とした上で、活用することも可能である。

（注１）ネットワーク及び情報システムの稼働中は常時監視し、障害が起きた際にも速やかに対応できる体制である必要がある。このため、リスクに応じて侵入検知シ

ステム（IDS：Intrusion Detection System）等の利用、監視体制の整備等の措置を講じる必要がある。ネットワーク監視で侵入検知に利用する、IDS ~~侵入検知システム（IDS：Intrusion Detection System）~~は、不正プログラム対策ソフトウェアのパターンファイルと同様に、不正アクセスのパターンを検知するためのファイルの更新を行い、検知能力を維持する必要がある。また、侵入検知だけではなく、侵入を防御する、侵入防御システム（IPS：Intrusion Prevention System）も存在する。

（注２）システム管理者などの特別な権限を持つIDの利用者の記録の確認については、本人以外のシステム管理者又はシステム管理者以外の者が確認するようにし、客観的に確認できる仕組みを構築する必要がある。

7.2. 情報セキュリティポリシーの遵守状況の確認

【趣旨】

情報セキュリティポリシーの遵守を確保するため、情報セキュリティポリシーの遵守状況等を確認する体制を整備するとともに、問題があった場合の対応について規定する。

【例文】

（１） 遵守状況の確認及び対処

①情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティポリシーの遵守状況について確認を行い、問題を認めた場合には、速やかに CISO 及び統括情報セキュリティ責任者に報告しなければならない。

②CISO は、発生した問題について、適正かつ速やかに対処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、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

（２） パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

CISO 及び CISO が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等のログ、電子メールの送受信記録等の利用状況を調査することができる。

（３） 職員等の報告義務

①職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに統括情報セキュリティ責任者及び情報セキュリティ管理者に報告を行わなければならない。

②当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ責任者が判断した場合において、職員等は、緊急時対応計画に従って適正に対処しなければならない。

(解説)

（１） 遵守状況の確認及び対処

情報セキュリティポリシーを運用する過程において、遵守状況を確認し、違反の有無、情報セキュリティポリシーの問題点などを明らかにすることが求められる。確認の結果、問題があった場合には、CISO は速やかに対処する必要がある。

（注１）遵守状況の確認方法としては、自己点検等の実施、情報セキュリティインシデントの報告、日常の業務からの情報セキュリティ対策の問題事項の報告、ログ等からの異常時の発見などがある。

（２） パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

職員等はパソコン、モバイル端末及び電磁的記録媒体等を業務のため使用しているのであって、私的な使用はあってはならない。職員等の業務以外の目的での利用を抑止するため、電子メールの送受信記録等を調査できる権限を CISO 及びその指名した者に付与する。

（注２）職員等が使用しているパソコン、モバイル端末及び電磁的記録媒体等や電子メールの送受信記録等の情報を調査することをあらかじめ周知しておくことも重要である。調査が行われるかもしれないということが、不正行為に対する抑止力として効果がある。

（注３）職員等が利用しているパソコン、モバイル端末及び電磁的記録媒体等の状況を調査することは、職員等のプライバシーとの関係が問題になるが、基本的には業務利用のパソコン、モバイル端末及び電磁的記録媒体等には、個人のプライバシー侵害になる記録は存在しないと考えられる。したがって、インターネット閲覧記録、電子メールの送受信記録等の調査権を確保しておくことは重要なことになる。ただし、調査は、CISO 又は CISO が指名した者が行う必要がある。

（３） 職員等の報告義務

職員等は、日々の業務で、情報セキュリティポリシーに違反した行為を発見した場合、その報告が求められる。統括情報セキュリティ責任者は、その報告を受け、情報セキュリティ上重大な影響があると判断した場合に、緊急時対応計画に沿って適正に対処する。

7.3. 侵害時の対応等

【趣旨】

情報セキュリティインシデント、システム上の欠陥及び誤動作並びに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事案が発生した場合に、迅速かつ適正に被害の拡大防止、迅速な復旧等の対応を行うため、緊急時対応計画の策定について規定する。

【例文】

（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。

（2） 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、以下の内容を定めなければならない。

①関係者の連絡先

②発生した事案に係る報告すべき事項

③発生した事案への対応措置

④再発防止措置の策定

（3） 業務継続計画との整合性確保

自然災害、大規模・広範囲にわたる疾病等に備えて別途業務継続計画を策定し、情報セキュリティ委員会は当該計画と情報セキュリティポリシーの整合性を確保しなければならない。

（4） 緊急時対応計画の見直し

CISO 又は情報セキュリティ委員会は、情報セキュリティを取り巻く状況の変化や組織体制の変動等に応じ、必要に応じて緊急時対応計画の規定を見直さなければならない。

（解説）

（1） 緊急時対応計画の策定

情報セキュリティが侵害された場合又は侵害されるおそれがある場合等における具体的な措置について、緊急時対応計画として定める。

緊急時対応計画には、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おける連絡、証拠保全、被害拡大の防止、復旧等の迅速かつ円滑な実施と、再発防止策

の措置を講じるために必要な事項を定める必要がある。

また、自らが所有する情報資産における被害拡大防止のほか、外部への被害拡大のおそれがある場合には、その防止に努めることを定める必要がある。情報が漏えいすることなどにより被害を受けるおそれのある関係者に対し早急に連絡することが重要である。

当該事案が不正アクセス禁止法違反等の犯罪の可能性がある場合には、警察・関係機関と緊密な連携に努めることも重要である。

（注１）緊急時対応計画を策定する場合は、他の危機管理に関する規程等と整合性を確保し策定する必要がある。また、他の危機管理に関する規程の改定と情報セキュリティポリシーの見直しの時期が異なることにより一時的に不整合が生じないよう、配慮する必要がある。

（注２）庁内の CSIRT が担う役割についても緊急時対応計画を策定する場合に考慮することが望ましい。

（２） 緊急時対応計画に盛り込むべき内容

緊急時対応計画に定める事項としては、例えば次のものがある。

①関係者の連絡先

・地方公共団体の長
・CISO
・統括情報セキュリティ責任者
・情報システム管理者
・情報セキュリティに関する統一的な窓口（庁内の CSIRT）
・ネットワーク及び情報システムに係る外部委託事業者
・広報担当課
・都道府県の関係部局
・警察
・関係機関
・被害を受けるおそれのある個人及び法人

②発生した事案に係る報告すべき事項

セキュリティに関する事案を発見した者は、次の項目について速やかに統括情報セキュリティ責任者に報告しなければならない。

・事案の状況
・事案が発生した原因として、想定される行為
・確認した被害・影響範囲（事案の種類、損害規模、復旧に要する額等）
・事案が情報セキュリティインシデントに該当するか否かの判断結果
・記録

また、統括情報セキュリティ責任者は、事案の詳細な調査を行うとともに、CISO 及び情報セキュリティ委員会へ報告しなければならない。

（注３）統括情報セキュリティ責任者が事案の詳細な調査を行うに当たっては、

必要に応じて外部専門家のアドバイスを受ける、JPCERT/CC（一般社団法人 JPCERT コーディネーションセンター）及び地方公共団体情報システム機構（自治体 CEPTOAR）等の関係機関に相談する等、事実確認を見誤らないように努める必要がある。

（注４）庁内の CSIRT に報告を集約し、窓口経由で外部への問合せや相談を行うことが考えられる。

（注５）情報共有や相談については、「地方公共団体における情報セキュリティ対策及び政府の一層の充実・強化について（依頼）」（平成 23 年 10 月 11 日総務省　事務連絡）を参照されたい。

③発生した事案への対応措置

（ア） 統括情報セキュリティ責任者は、次の事案が発生した場合、定められた連絡先へ連絡しなければならない。

・サイバーテロそのほか市民に重大な被害が生じるおそれのあるとき
　→地方公共団体の長、CISO、都道府県の関係部局、警察、影響が考えられる個人及び法人に連絡
・不正アクセスそのほか犯罪と思慮されるとき
　→地方公共団体の長、CISO、都道府県の関係部局、警察に連絡
・踏み台となって他者に被害を与えるおそれがあるとき
　→地方公共団体の長、CISO、都道府県の関係部局、警察に連絡
・情報システムに関する被害
　→情報システム管理者、必要と認められる事業者に連絡
・その他情報資産に係る被害
　→関係部局等に連絡

（イ） 統括情報セキュリティ責任者は、次の事案が発生し、情報資産を保護するためにネットワークを切断することがやむを得ない場合、ネットワークを切断する。

・異常なアクセスが継続しているとき又は不正アクセスが判明したとき
・システムの運用に著しい支障をきたす攻撃が継続しているとき
・コンピュータウイルス等、不正プログラムがネットワーク経由で拡がっているとき
・情報資産に係る重大な被害が想定されるとき

（ウ） 情報システム管理者は、次の事案が発生し、情報資産の防護のために情報システムを停止することがやむを得ない場合、情報システムを停止する。

・コンピュータウイルス等、不正プログラムが情報資産に深刻な被害を及ぼしているとき
・災害等により電源を供給することが危険又は困難なとき
・そのほかの情報資産に係る重大な被害が想定されるとき

（エ） 個々のパソコン等の端末のネットワークからの切断については、セキュリティポリシーにおいて特段の定めがあるものを除き、統括情報セキュリティ責任者の

許可が必要である。

ただし、情報資産の被害の拡大を直ちに停止させる必要がある場合は、事後報告とすることができる。

（オ） 事案に係るシステムのログ及び現状を保存する。

（カ） 事案に対処した経過を記録する。

（キ） 事案に係る証拠保全の実施を完了するとともに、応急措置を講じる。

（ク） 応急措置を講じた後、復旧する。

（ケ） 復旧後、必要と認められる期間、再発の監視を行う。

④再発防止措置の策定

（ア） 統括情報セキュリティ責任者は、当該事案に係る調査を実施し、情報セキュリティポリシー及び実施手順の改善を含め、再発防止計画を策定し、情報セキュリティ委員会へ報告する。

（イ） 情報セキュリティ委員会は、再発防止計画が有効であると認められた場合はこれを承認し、事案の概要とあわせ職員等に周知する。

（３） 業務継続計画との整合性確保

地震及び風水害等の自然災害等や大規模・広範囲にわたる疾病等の事態に備えて、情報セキュリティにとどまらない危機管理規定として業務継続計画（あるいは、ICT部門における業務継続計画）を策定することが重要である。ただし、業務継続計画と情報セキュリティポリシーの間に矛盾があると、職員等は混乱し、適正な対応をとることができなくなるおそれがあるため、各地方公共団体において業務継続計画を策定する際には、情報セキュリティポリシーとの整合性をあらかじめ検討し、必要があれば、情報セキュリティポリシーを改定しなければならない。

（注６）整合性を検討すべき事項は、例えば、施設の耐災害性対策、施設・情報システムの地理的分散、非常用電源の確保、人手による業務処理や郵送・電話の利用を含む情報システム以外の通信手段の利用、事態発生時の対応体制及び要員計画などがある。

（注７）危機管理には、大規模・広範囲にわたる疾病等によるコンピュータ施設の運用にかかる機能不全等への考慮も望まれる。

（注８）大地震を対象事態とした ICT 部門における業務継続計画の策定については、「地方公共団体における ICT 部門の業務継続計画（BCP）策定に関するガイドライン」（平成 20 年 8 月 総務省）及び「地方公共団体における ICT 部門の業務継続計画（ICT-BCP）初動版サンプル」（平成 25 年 5 月 8 日 総務省）を参照されたい。

（４） 緊急時対応計画の見直し

緊急時対応計画の実効性を確保するため、新たな脅威の出現等の情報セキュリティに関する環境の変化や組織体制の変化等を盛り込んだ最新の内容となるよう、定期的に見直すことが必要である。また、緊急時対応計画の発動した場合を仮定した訓練や机上試験を定期的に実施しておくことも、緊急時対応計画の実効性を確保す

る観点から重要である。

7.4. 例外措置

【趣旨】

情報セキュリティポリシーの規定をそのまま適用した場合に、行政事務の適正な遂行を著しく妨げるなどの理由により、これに代わる方法によることやポリシーに定められた事項を実施しないことを認めざるを得ない場合がある。このことから、あらかじめ例外措置について規定する。

【例文】

（1） 例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用する又は遵守事項を実施しないことについて合理的な理由がある場合には、CISO の許可を得て、例外措置を講じることができる。

（2） 緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避のときは、事後速やかに CISO に報告しなければならない。

（3） 例外措置の申請書の管理

CISO は、例外措置の申請書及び審査結果を適正に保管し、定期的に申請状況を確認しなければならない。

（解説）

例外措置は、情報セキュリティポリシーの適用を例外的に排除するものであることから、その承認は、ポリシーの適用が著しく行政事務の遂行を妨げる、緊急を要し通常の手続を取る時間的な猶予がない、技術的に困難であるなどの合理的な理由が必要である。なお、その場合でも、例外措置は単に適用を排除するだけでなく、リスクに応じて代替措置を定めること及び期限を設けて認めることが望ましい。

CISO は、例外措置についての手続を定め、明示することによって、ローカルルールの氾濫や、対策の未実施を防止することができる。

（注１）例外措置の内容から判断し、情報セキュリティポリシーの遵守自体に無理があると判断される場合には、当該ポリシーの見直しについて検討する必要がある。

7.5. 法令遵守

【趣旨】

職員等は、全ての法令を遵守することは当然であるが、職員等が業務を行う際の参考として、情報セキュリティに関する主要な法令を明示し、法令の遵守を確実にする。

【例文】

職員等は、職務の遂行において使用する情報資産を保護するために、次の法令のほか関係法令を遵守し、これに従わなければならない。

①地方公務員法（昭和 25 年法律第 261 号）

②著作権法（昭和 45 年法律第 48 号）

③不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）

④個人情報の保護に関する法律（平成 15 年法律第 57 号）

⑤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（平成 25 年法律第 27 号）

⑥サイバーセキュリティ基本法（平成 2~~68~~年法律第 104~~31~~号）

⑦○○市個人情報保護条例（平成○○年条例第○○号）

（解説）

情報セキュリティ対策において関連のある主要な法令について明示し、法令遵守を確実にする。また、法令への適合を確実なものにするためには、必要に応じて有識者による法的な助言を受けることが望ましい。

また、関連する最新の法令に基づき定期的に情報セキュリティポリシーの見直しを行い、最新に保つことが望ましい。

7.6. 懲戒処分等

【趣旨】

情報セキュリティポリシーの遵守事項に対して、職員等が違反した場合の事項を定めておくことは、情報セキュリティポリシー違反の未然防止に一定の効果が期待される。このことから、情報セキュリティポリシー違反に対する懲戒処分の規定及び懲戒に係る手続について規定する。

【例文】

（1） 懲戒処分

情報セキュリティポリシーに違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

（2） 違反時の対応

職員等の情報セキュリティポリシーに違反する行動を確認した場合には、速やかに次の措置を講じなければならない。

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. 外部委託~~サービスの利用~~

8.1. 業務~~外部~~委託

【趣旨】

外部の者に、情報システムやアプリケーションプログラムの開発・運用・保守等を委託する際に、職員等が当該委託先における情報セキュリティ対策を直接管理することが困難な場合は、委託先において対策基準に適合した情報セキュリティ対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とする必要がある。

業務委託には以下の例のように様々な種類があり、また、契約形態も、請負契約や委任、準委任、約款への同意等様々であるが、いずれの場合においても、前述のように委託先において対策基準に適合した情報セキュリティ対策が確実に実施される必要のある業務委託の契約時には、委託する業務の範囲や委託先の責任範囲等を明確化し、契約者双方で情報セキュリティ対策の詳細について合意形成することが重要である。

なお、委託先で外部サービスを利用する場合は、委託先においても外部サービス特有のリスクがあることから、「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）」で規定する内容についても委託先への要求事項に含める必要がある。

＜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
・ 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）~~情報システムの外部委託を行う際は、外部委託事業者からの情報漏えい等の事案を防止するために、情報セキュリティを確保できる外部委託事業者を選定し、契約で遵守事項を定めるとともに、定期的に対策の実施状況を確認する必要がある。~~

~~このことから、外部委託を行う際に、情報セキュリティ確保上必要な事項について規定する。~~

~~なお、個別団体が単独で外部委託する場合だけでなく、共同アウトソーシングやクラウドサービス利用の形態等により地方公共団体が共同で外部委託する場合にも対策を実施する必要があることに留意する。（クラウドサービスの利用については、「8.4. クラウドサービスの利用」も参照されたい。）~~

【例文】

（１） 外部委託事業者の選定基準

①情報セキュリティ管理者は、外部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、事業者を選定しなければならない。【推奨事項】

（２） 契約項目

情報システムの運用、保守等を業務~~外部~~委託する場合には、外部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
・外部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
・外部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
・外部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受託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、外部委託事業者において十分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。

（解説）

（１） 外部委託事業者の選定基準

外部委託事業者を選定するに当たっては、情報セキュリティ上、重要な情報資産を取り扱う可能性があることから、技術的能力、信頼性等について考慮して、情報セキュリティ対策が確保されることを確認する必要がある。

また、外部委託事業者の選定にあたり、事業者の情報セキュリティ水準を評価する際には、国際規格の認証取得状況等を参考にして決定することが望ましい。

なお、外部委託事業者の選定条件として仕様等に盛り込む内容としては、例えば次のものがある。

・外部委託事業者に提供する情報の委託事業者における目的外使用の禁止
・外部委託事業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
・外部委託事業の実施にあたり、外部委託事業者の組織若しくはその従業員、再委託事業者、又はその他の者による意図せざる変更が加えられないための管理体制
・外部委託事業者の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・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
・情報セキュリティ要件の適正な実装
・情報セキュリティの観点に基づく試験の実施
・情報セキュリティインシデントへの対処方法
・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
・情報セキュリティ対策の実施が不十分な場合の対処方法

（注１）これらの選定方法については、「公共 IT におけるアウトソーシングに関するガイドライン」（平成 15 年 3 月　総務省）を参照されたい。

（注２）現在の最新の規格である ISO/IEC27001 については、一般財団法人日本情報経済社会推進協会のホームページ（ISMS 適合性評価制度）又は一般財団法人日本規格協会のホームページを参照されたい。

（注３）ホスティングサービスの利用等においては、サービス提供者側のミスや機器の故障などの不測の事態によりデータの消失などの事態が発生するおそれがあるため、情報システムや取り扱う情報の重要度に応じたバックアップなどの必要な対策を講じておく必要がある。なお、ホスティング時のデータ消失に関する対策については、「ホスティングサービス等利用時におけるデータ消失事象への対策実施及び契約内容の再確認等について（注意喚起）」（平成 24 年 7 月 6 日　総務省 事務連絡）を参照されたい。

（注４）外部委託事業者の委託判断基準

業務~~外部~~委託にあたっては、外部委託事業者の委託判断基準を作成しておくことが望ましい。規定すべき内容としては、例えば次のものがある。

・業務~~外部~~委託を許可（又は禁止）する業務又は情報システムの範囲
・業務~~外部~~委託を許可（又は禁止）する業務又は情報システムの具体的例示（公開ウェブサーバは外部委託可等）
・格付及び取扱制限その他取り扱う情報の特性に応じた、情報の取扱いを許可（又は禁止）する場所

特に、委託業務において取り扱われる情報が海外のデータセンターに存在する場合等においては、保存している情報に対して現地の法令等が適用されるため、国内であれば不適切と判断されるアクセスが行われる可能性があることに注意が必要である。

（２）　契約項目

外部委託事業者に起因する情報漏えい等の事案を防ぐため、各団体で実施する場合と同様の対策を当該委託事業者に実施させるよう必要な要件を契約等に定める必要がある。以下に示す項目について、委託する業務の内容に応じて明確に要件を規定することが必要である。

①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

外部委託事業者の要員に対して、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について、委託業務に関係する事項を遵守することを定める。外部委託事業者において情報セキュリティインシデントが発生した場合に備えて、対処方法（対処手順、責任分界、対処体制等）について契約前に合意しておかなければならない。

②外部委託事業者の責任者、委託内容、作業者、作業場所の特定

外部委託事業者の責任者や作業者を明確にするとともに、これらの者が変更する場合の手続を定めておき、担当者の変更を常に把握できるようにする。また、作業場所を特定することにより、情報資産の紛失等を防止する。

③提供されるサービスレベルの保証

通信の速度及び安定性、システムの信頼性の確保等の品質を維持するために、必要に応じて、サービスレベルを保証させる。

④委託事業者に許可する情報の種類とアクセス範囲、アクセス方法

委託に関わる情報の種類を定義し、種類ごとのアクセス許可、アクセス時の情報セキュリティ要求事項並びにアクセス方法の監視及び管理を行う。

⑤従業員に対する教育の実施

外部委託事業者において、情報セキュリティに対する意識の向上を図るために、従業員に対し教育を行うように規定しておく。

⑥提供された情報の目的外利用及び受託者以外の者への提供の禁止

外部委託事業者に提供した情報について、不正な利用を防止させるために、業務以外での利用を禁止する。

⑦業務上知り得た情報の守秘義務

業務中及び業務を終了した後も、情報の漏えいを防止するために、業務上知り得た秘密を漏らしてはならない旨を規定する。

⑧再委託に関する制限事項の遵守

一般的に、再委託した場合、再委託事業者のセキュリティレベルは下がることが懸念されるために、再委託は原則禁止する。例外的に再委託を認める場合には、再委託事業者における情報セキュリティ対策が、他の外部委託事業者と同等の水準であることを確認し、外部委託事業者に担保させた上で許可しなければならない。

⑨委託業務終了時の情報資産の返還、廃棄等

委託業務終了時に、不要になった情報資産を返還させるか廃棄させるか等その取扱いについて明確に規定する必要がある。委託終了後の取扱いを明確にすることにより、不要になった情報資産から情報が漏えいする可能性を減らす。なお、マ

イナンバー利用事務系の領域において取り扱われる機器をリースにより調達しようとする場合には、当該機器についてリース契約終了後、物理的破壊を行う旨、入札における仕様に明記するとともに、契約に位置づけることが望ましい。

⑩委託業務の定期報告及び緊急時報告義務

定期報告及び緊急時報告の手順を定め、委託業務の状況を適正かつ速やかに確認できるようにすることが必要である。緊急時の職員への連絡先は、外部委託業者に通知しておく必要がある。連絡網には、職員の個人情報が記載される場合もあるため、取扱いに注意する。

⑪地方公共団体による監査、検査

外部委託事業者が実施する情報システムの運用、保守、サービス提供（クラウドサービス含む）等の状況を確認するため、当該委託事業者に監査、検査を行うことを明確に規定しておくことが必要である。

なお、地方公共団体において、当該委託事業者に監査、検査を行うことが困難な場合は、地方公共団体による監査、検査に代えて、第三者や第三者監査に類似する客観性が認められる外部委託事業者の内部監査部門による監査、検査又は国際的なセキュリティの第三者認証(ISO/IEC27001 等)の取得等によって確認する。

⑫地方公共団体による情報セキュリティインシデントの公表

委託業務に関し、情報セキュリティインシデントが発生した場合、住民に対し適正な説明責任を果たすため、当該情報セキュリティインシデントの公表を必要に応じ行うことについて、外部委託事業者と確認しておく。

⑬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)

外部委託事業者においての情報セキュリティポリシーが遵守されなかったため、被害を受けた場合には、当該委託事業者が損害賠償を行うことを契約書上明記しておく。

（注５）これらの契約項目については、「地方公共団体における業務の外部委託事業者に対する個人情報の管理に関する検討」報告書（平成 21 年 3 月 総務省）を参照し、「個人情報の取扱いに関する特記仕様書（雛型）」を活用されたい。

（注６）外部委託事業者に対して、情報セキュリティポリシーの該当部分について、十分に説明しておくことが必要である。

（注７）指定管理者制度に関する考慮事項

指定管理者制度においては、条例により、地方公共団体と指定管理者との間で協定を締結することになるが、その協定において、委託内容に応じた情報セキュリティ対策が確保されるよう必要な事項を定める必要がある。

（注８）IT サプライチェーンを構成して提供されるサービスを利用する場合は、外部委託事業者との関係におけるリスク（サービスの供給の停止、故意又は過失による不正アクセス、外部委託事業者のセキュリティ管理レベルの低下など）を考慮しそのリスクを防止するための事項について外部委託事業者と合意し、その内容を文書化しておくことが望ましい。

（注９）外部委託事業者に適用される法令としては、法律のほか、各地方公共団体の制定する個人情報保護条例も適用されることを明記しておく必要がある。

（注１０）業務の内容に応じて規定する要件の詳細については、「非機能要求グレード（地方公共団体版）利用ガイド」（平成 26 年 3 月　地方自治情報センター）を参照されたい。

（３）　確認・措置等

情報セキュリティ管理者は、外部委託事業者において十分なセキュリティ対策が実施されているか、定期的に確認し、必要に応じ、改善要求等の措置を講じる必要がある。確認した内容は定期的に統括情報セキュリティ責任者に報告する。個人情報の漏えい等の重大なセキュリティ侵害行為が発見された場合には、速やかに CISO に報告を行う。また、情報セキュリティ管理者は、情報システムの運用・保守を外部委託する場合は、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、速やかに報告させる必要がある。

なお、外部委託事業者に対する監査については、本ガイドラインの「9.1 監査（４）外部委託事業者に対する監査」を参照されたい。

8.2. ~~約款による~~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）

【趣旨】

今後クラウドサービスなどの外部サービスの利用の拡大が見込まれているところ、外部サービスの利用に当たっては、外部サービス基盤部分を含む情報の流通経路全般を俯瞰し、総合的に対策を設計した上で、セキュリティを確保する必要がある。

外部サービス提供者に取扱いを委ねる情報は、当該提供者によって適正に取り扱われなければならないが、外部サービスの利用においては、適正な取扱いが行われていることを直接確認することが一般に容易ではない。また、外部サービスでは、複数利用者が共通の外部サービス基盤を利用する可能性があり、自身を含む他の利用者にも関係する情報の開示を受けることが困難になる場合もある。外部サービスを利用して機密性２以上の情報を取り扱う場合は、外部サービス提供者を適正に選択するために、このような外部サービスの特性を理解し、自組織による外部サービス提供者へのガバナンスの有効性や利用の際のセキュリティ確保のために必要な事項を十分に考慮し、自組織と外部サービス提供者の役割や責任分担を明確にした上で、外部サービスが選定基準及びセキュリティ要件を満たすことを確実にすることが求められる。

さらに、外部サービスを利用する際のセキュリティ対策は、選定や契約時における対策だけでなく、契約後の情報システムの導入・構築、その後の運用・保守、更には契約終了時に至るまで情報システムのライフサイクル全般において行う必要がある。特に外部サービスのサービス内容は非常に早いサイクルで変化しており、利用開始時に行ったセキュリティ対策が途中で無効になることも考えられるため、運用・保守のフェーズにおける対策は定期的に漏れなく実施することが求められる。

＜外部サービスの例＞

- クラウドサービス
- 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

なお、民間事業者等が不特定多数の利用者に対して提供する、画一的な約款や規約等への同意のみで利用可能となる外部サービスでは、セキュリティ対策やデータの取扱いなどについて自組織への特別な扱いを求めることができない場合が多く、機密性２以上の情報を取り扱う上で必要十分なセキュリティ要件を満たすことが一般的に困難であることから、原則として機密性２以上の情報を取り扱うことはできない。~~民間事業者が約款に基づきインターネット上で無料で提供する情報処理サービス等を利用する場合には、リスクを十分踏まえた上で利用を判断し、適正なセキュリティ対策を講じる必要がある。~~

【例文】

（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、外部サービスの提供が行われる施設等の場所、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

(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。

~~（１）約款による外部サービスの利用に係る規定の整備~~

~~情報セキュリティ管理者は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用において、機密性２以上の情報が取り扱われないように規定しなければならない。~~

~~①約款によるサービスを利用して良い範囲~~
~~②業務により利用する約款による外部サービス~~
~~③利用手続及び運用手順~~
~~（２）約款による外部サービスの利用における対策の実施~~
~~職員等は、利用するサービスの約款、その他提供条件から、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約款による外部サービスの利用を申請し、適正な措置を講じた上で利用しなければならない。~~

（解説）

（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

① 外部サービスの利用においても、「8.1.業務委託（１）外部委託事業者の選定基準」で整備を求めている「委託業者の選定基準」と同等の規定が求められる。また、外部サービス利用者が外部サービスを利用する際の接続方法等（テレワーク等により、外部の通信回線から直接外部サービスにアクセスすることの可否等）についても規定することが必要である。

外部サービスの利用に当たっては、情報の管理や処理を外部サービス提供者に委ねるため、その情報の適正な取扱いの確認が容易ではなくなる。そこで、適切な外部サービス提供者を選定することにより以下のようなリスクを低減することが考えられる。

・外部サービスは、そのサービス提供の仕組みの詳細を利用者が知ることがなくても手軽に利用できる半面、外部サービス提供者の運用詳細は公開されないために外部サービス利用者にブラックボックスとなっている部分があり、外部サービス利用者の情報セキュリティ対策の運用において必要な情報の入手が困難である。

・オンプレミスと外部サービスの併用や外部サービスと他の外部サービスの併用等、多様な利用形態があるため、利用者と外部サービス提供者との間の責任分界点やサービスレベルの合意が容易ではない。

・外部サービス提供者が所有する資源の一部を利用者が共有し、その上に個々の利用者が管理する情報システムが構築されるなど、不特定多数の利用者の情報やプログラムを一つの外部サービス基盤で共用することとなるため、情報が漏えいするリスクが存在する。

・外部サービスで提供される情報が国外で分散して保存・処理されている場合、裁判管轄の問題や国外の法制度が適用されることによるカントリーリスクが存在する。

・サーバ装置等機器の整備環境が外部サービス提供者の都合で急変する場合、サプライチェーン・リスクへの対策の確認が容易ではない。

なお、情報セキュリティ確保のために外部サービス利用者自らが行うべきことと、外部サービス提供者に対して求めるべきこと等をまとめたガイドラインについては、以

下の取組を参考にするとよい。

参考：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）」（2021 年９月）
（https://www.soumu.go.jp/main_content/000566969.pdf）

参考：経済産業省「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」（2013 年度版）
（ https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudsec2013fy.pdf）

参考：経済産業省「クラウドセキュリティガイドライン活用ガイドブック」（2013 年度版）
（ https://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudseckatsuyou2013fy.pdf）

参考：公益財団法人 金融情報システムセンター「金融機関におけるクラウド利用に関する有識者検討会報告書」（平成 26 年 11 月）
（https://www.fisc.or.jp/document/fintech/file/1900.pdf）

② 利用申請の許可権限者と外部サービス管理者

例文では、「利用申請の許可権限者」と「外部サービス管理者」を設けることとしているが、小規模の地方公共団体などにおいては、統括情報セキュリティ責任者と利用申請の許可権限者の兼務や情報セキュリティ責任者と外部サービス管理者の兼務など、柔軟に対応することが必要となる。ただし、利用申請を行う職員等が利用申請の許可権限者や外部サービス管理者を兼務することは職務の分離の観点から禁止とする。

（２）外部サービスの選定

① 外部サービスの利用に当たっては、情報の管理や処理を外部サービス提供者に委ねるため、その情報の適正な取扱いの確認が容易ではなくなることを踏まえ、適切な外部サービス提供者を選定することによりリスクを低減することが考えられる。

（注１）外部サービスの利用に当たっては、「地方公共団体における ASP・SaaS 導入活用ガイドライン」（平成 22 年４月　総務省）を参照されたい。

② インターネットを介して提供される外部サービスの利用に当たっては、外部サービス提供者の事業所の場所に関わらず、データセンターの存在地の国の法律の適用を受ける場合があることに留意する必要がある。具体的には、外部サービス提供者のサービスの利用を通じて海外のデータセンター内に蓄積された地方公共団体の情報が、データセンターの設置されている国の法令により、日本の法令では認められていない場合であっても海外の当局による情報の差し押さえや解析が行われる可能性があるため、日本の法令の範囲内で運用できるデータセンターを選択する必要がある。

管轄裁判所に関しては、国外の裁判所で裁判を行うこととならないよう、契約において日本国内の裁判所（必要に応じて地方公共団体の所在地を管轄する裁判所）を合意管轄裁判所として規定する必要がある。また、外国に本社を置く企業が提供するサービスを地方公共団体が利用する場合の紛争を当該企業の本社の所在地を管轄する裁判所が管轄することも考えられる一方、その場合は日本の国内法と同等の個人情報の保護などが確立されないおそれがあることについては利用者である地方公共団体において契約締結の際に十分な留意が必要となる。

③　外部サービスを利用するに当たり、サービスの中断や終了時に際し、円滑に業務を移行するための対策として、以下を例とするセキュリティ対策を実施することを外部サービスの選定条件とし、仕様内容にも含める必要がある。

・取り扱う情報の可用性区分の格付に応じた、サービス中断時の復旧要件

・取り扱う情報の可用性区分の格付に応じた、サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法

④　情報セキュリティ管理者は、外部サービス部分を含む情報の流通経路全般にわたるセキュリティ対策を実施する必要がある。システムの重要度に応じて求められる可用性のレベル等（稼働率、目標復旧時間、バックアップの保管方法など）を十分に検討し、調達の際に、検討した結果を調達仕様書に具体的に盛り込まなければならない。また、必要となる条項（インシデントの報告義務、損害賠償等）を盛り込んだ契約及びサービスレベルを保証させるための SLA を締結する必要がある。特に、バックアップについては、契約において、各業務システムの重要度を勘案した適切なバックアップレベルを設定し、別途のバックアップの取得など、レベルに応じた適切な対策を実施することが重要である。

（注２）外部サービスの大規模障害により、自治体の業務に長時間支障が発生した事案を踏まえたセキュリティ対策については、「「Jip-Base」事案を踏まえたクラウドサービスの利用に係る注意喚起」（令和２年５月 22 日　総行情第 76 号　総務省自治行政局地域情報政策室長通知）を参照されたい。

（注３）契約に必要となる条項については「8.1. 業務委託（３）契約項目」及び「地方公共団体における ASP・SaaS 導入活用ガイドライン」（平成 22 年４月　総務省）を参照されたい。また、セキュリティ要件の検討を行う際は、「非機能要求グレード（地方公共団体版）利用ガイド」（平成 26 年３月　地方自治情報センター）も併せて参照されたい。

⑤　情報セキュリティ管理者は、外部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、外部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。

外部サービス提供者及び当該サービスの信頼性が十分であることを総合的に判断するためには、外部サービスで取り扱う情報の機密性・完全性・可用性が確保されるように、外部サービス提供者のセキュリティ対策を含めた経営が安定してい

ること、サービスを提供する基盤環境やアプリケーションに係るセキュリティ対策が適切に整備され、運用されていること等を評価する必要がある。

このような評価に当たって、外部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/IEC27001 による ISMS 認証、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。外部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。

参考：国際規格

「ISO/IEC 27017（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：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）

⑥　目的外利用の禁止

自組織が取り扱う情報は、外部サービス提供者において外部サービスの提供に必要な範囲で利用を認めるものであって、それ以外の目的で利用をさせてはならない。

目的外利用に当たる場合としては、例えば、外部サービス提供者が自組織の利用する外部サービスの契約情報等を保有し、今後の営業活動で利用するなどが考えられる。

⑦　本市の意図しない変更が加えられないための管理体制

外部サービス提供者が行う外部サービスの開発及び運用において、「本市の意図しない変更が加えられないための管理体制」が確保されることを求めている。

具体的に外部サービス提供者の選定条件に含める内容としては、例えば以下が考えられる。

・外部サービスの開発及び運用において、自組織の意図しない変更が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。また、当該品質保証体制が書類等で確認できること。

・外部サービスに自組織の意図しない変更が行われるなどの不正が見付かったときに、追跡調査や立入検査等、自組織と外部サービス提供者が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。

⑧　情報セキュリティインシデントへの対処方法

外部サービス提供者において発生した情報セキュリティインシデントによる被害を最小限に食い止めるための対処方法（対処手順、責任分界、対処体制等）について、外部サービス提供者の選定条件に含めておくとよい。対処方法についての合意がないと、インシデントが発生しているにもかかわらず外部サービス提供者と連絡がつかない、営業時間外の対応を断られるなどのトラブルになるおそれがあるため、可能な範囲で事前に具体化することが重要である。対処方法には、例えば、復旧を優先する場合は外部サービスの利用を一時的に停止するための手順を規定し、業務継続を優先する場合は、外部サービスの利用を継続した上で情報セキュリティインシデントに対処する手順について、対処の主体とともに規定することが考えられる。また、情報セキュリティインシデントに係る外部サービス提供者と自組織間の情報エスカレーション方法やそのタイミングについて規定することも考えられる。

⑨　情報の取扱手順

格付及び取扱制限の明示等、運搬又は送信、消去等の情報の取扱いに関して、外部サービス提供者においても自組織の対策基準に定める内容と同等の取扱いが行われるよう、あらかじめ外部サービス提供者と合意しておくことが重要である。また、外部サービス提供者に提供する情報は必要最小限にとどめる必要があるが、情報システムの利用等において目的外の不必要なアクセスが行われる可能性も考慮し、外部サービス提供者における情報の取扱状況を適宜把握することも重要である。

なお、外部サービス提供者において、業務委託、他の外部サービス等を用いて外部サービスを提供することが考えられる場合は、「8.1.業務委託」、「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）」の規定を外部サービス提供者においても遵守させるよう仕様書等に規定し、外部サービス提供者とあらかじめ合意しておくことが望ましい。

⑩　外部サービスに係るアクセスログ等の証跡の保存

外部サービス上におけるアクセスログ等の証跡に係る保存期間については、情報システム又は当該システムに保存される情報の特性に基づき、設定される。ただし、標的型攻撃に関し、攻撃の初期段階から経緯を確認する観点からは、過去の事例を踏まえ、ログは１年間以上保存することが望ましい。

なお、記憶媒体に保存する期間については、過去に遡って調査する期間や頻度、どの程度のコストをログの保存にかけられるかを考慮して決定する（「6.1. コンピュータ及びネットワークの管理　(6)ログの取得等」を参照のこと。）。

⑪　外部サービス提供者による情報の管理・保管

情報管理上の問題として、仮に情報が外部サービス上にあったとしても、当該情報の責任は利用者である情報オーナーが負うことになるため、利用者は外部サービス提供者による情報の管理・保管方法について事前に把握する必要がある。

また、外部サービス提供者が情報の管理・保管を他の事業者へ委託する場合、当該情報が外部サービス利用者の意図しない場面で二次利用されることも懸念されるため、当該事業者における情報セキュリティ水準や情報の取扱方法に関して外部サービス提供者に確認の上、合意しておく必要がある。

⑫　情報開示請求に対する開示項目や範囲

外部サービスに関し、外部サービス提供者が一般に公開している内容以上の情報提供について、情報セキュリティ対策や監査の観点から、事前に自組織と外部サービス提供者が協議の上、外部サービス提供者が提供する内容の項目や範囲を契約において明記することが必要である。また、対象情報の機密性が高い場合、両者間で秘密保持契約（NDA：Non-Disclosure Agreement）を締結するなど必要な措置を講じた上で取得することが求められる。

（３）外部サービスの利用に係る調達・契約

①　調達仕様の内容を契約に含める際、外部サービス提供者との情報セキュリティに関する役割及び責任の範囲が明確になっていることを確認すること。

（４）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　構築時におけるアクセス制御に係る規定を策定する場合、以下を含む内容を規定すること。

（ア）外部サービスを利用する際に外部サービス提供者が付与又は外部サービス利用者が登録する識別コードの作成から廃棄に至るまでのライフサイクルにおける管理

（イ）外部サービスを利用する際に使用するネットワークに対するサービスごとのアクセス制御

（ウ）外部サービスを利用する情報システムの管理者特権を保有する外部サービス利用者に対する強固な認証技術の利用

（エ）外部サービス提供者が提供する主体認証情報の管理機能が要求事項を満たすことの確認

（オ）外部サービス上に保存する情報や外部サービスの機能に対してアクセス制御できることの確認

（カ）外部サービス利用者による外部サービスに多大な影響を与える操作の特定と誤操作の抑制

（キ）外部サービス上で構成される仮想マシンに対する適切なセキュリティ対策の実施

（ク）インターネット等の外部の通信回線から庁内通信回線を経由せずに外部サービス上に構築した情報システムにログインすることの要否の判断と認める場合の適切なセキュリティ対策の実施

② 構築時における暗号化に係る規定を策定する場合、以下を含む内容を規定すること。

（ア）外部サービス内及び通信経路全般における暗号化の確認

（イ）利用する情報システムに係る法令や規則に対する暗号化方式の遵守度合い

③ 構築時における開発に係る規定を策定する場合、以下を含む内容を規定すること。

（ア）情報システムの構築において外部サービスを利用する場合の外部サービス提供者へのセキュリティを保つための開発手順等の情報の要求とその活用

（イ）情報システムの構築において、外部サービス上に他ベンダが提供するソフトウェア等を導入する場合のそのソフトウェアの外部サービス上におけるライセンス規定

④ 構築時における設計・設定に係る規定を策定する場合、以下を含む内容を規定すること。

（ア）外部サービス上に情報システムを構築する際の外部サービス提供者への設計、構築における知見等の情報の要求とその活用

（イ）外部サービス上に情報システムを構築する際の設定の誤りを見いだすための対策

（ウ）外部サービス上に構成された情報システムのネットワーク設計におけるセキュリティ要件の異なるネットワーク間の通信の監視

（エ）利用する外部サービス上の情報システムが利用するデータ容量や稼働性能についての監視と将来の予測

（オ）利用する外部サービス上で可用性２の情報を取り扱う場合の可用性を考慮した設計

（カ）外部サービス内における時刻同期の方法の確認

（５）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、運用・保守時における利用方針に係る規定を策定する場合、以下を含む内容を規定すること。

（ア）責任分界点を意識した外部サービスの利用

（イ）利用承認を受けていない外部サービスの利用禁止
（ウ）外部サービス提供者に対する定期的なサービスの提供状態の確認
（エ）利用する外部サービスに係る情報セキュリティインシデント発生時の連絡体制

② 統括情報セキュリティ責任者は、運用・保守時における教育に係る規定を策定する場合、以下を含む内容を規定すること。
（ア）外部サービス利用のための規定及び手順について
（イ）外部サービス利用に係る情報セキュリティリスクとリスク対応について
（ウ）外部サービス利用に関する適用法令や関連する規制等について

③ 統括情報セキュリティ責任者は、運用・保守時における資産管理に係る規定を策定する場合、以下を含む内容を規定すること。
（ア）外部サービス上で利用する IT 資産の適切な管理
（イ）外部サービス上に保存する情報に対する適切な格付・取扱制限の明示
（ウ）外部サービスの機能に対する脆弱性対策について、外部サービス利用者の責任範囲の明確化と対策の実施

④ 統括情報セキュリティ責任者は、運用・保守時におけるアクセス制御に係る規定を策定する場合、以下を含む内容を規定すること。
（ア）管理者権限を外部サービス利用者へ割り当てる場合のアクセス管理と操作の確実な記録
（イ）外部サービス利用者に割り当てたアクセス権限に対する定期的な見直し
（ウ）外部サービスのリソース設定を変更するユーティリティプログラムを使用する場合の機能の確認と利用者の制限
（エ）利用する外部サービスの不正利用の監視

⑤ 統括情報セキュリティ責任者は、運用・保守時における暗号化に係る規定を策定する場合、以下を含む内容を規定すること。
（ア）暗号化に用いる鍵の管理者と鍵の保管場所
（イ）鍵管理機能を外部サービス提供者が提供する場合の鍵管理手順と鍵の種類の情報の要求とリスク評価
（ウ）鍵管理機能を外部サービス提供者が提供する場合の鍵の生成から廃棄に至るまでのライフサイクルにおける情報の要求とリスク評価

⑥ 統括情報セキュリティ責任者は、運用・保守時における通信に係る規定を策定する場合、以下を含む内容を規定すること。
（ア）利用する外部サービスのネットワーク基盤が他のネットワークと分離されていることの確認

⑦ 統括情報セキュリティ責任者は、運用・保守時における設計・設定に係る規定を策定する場合、以下を含む内容を規定すること。
（ア）外部サービスの設定を変更する場合の設定の誤りを防止するための対策
（イ）外部サービス利用者が行う可能性のある重要操作の手順書の作成と監督者

の指導の下での実施

⑧　統括情報セキュリティ責任者は、運用・保守時における事業継続に係る規定を策定する場合、以下を含む内容を規定すること。

（ア）不測の事態に対してサービスの復旧を行うために必要なバックアップの確実な実施。又は、外部サービス提供者が提供する機能を利用する場合は、その実施の確認

（イ）可用性２の情報を外部サービスで取り扱う場合の十分な可用性の担保、復旧に係る手順の策定と定期的な訓練の実施

（ウ）外部サービス提供者からの変更通知の内容確認と復旧手順の確認

（エ）外部サービスで利用しているデータ容量、性能等の監視

⑨　情報キュリティ責任者は、運用・保守時におけるインシデント対応に係る規定を策定する場合、以下を含む内容を規定すること。

（ア）外部サービス上での情報セキュリティインシデント、情報の目的外利用等を認知した場合の外部サービス管理者への報告

（イ）外部サービス管理者がインシデント報告を受けた場合の対応

（６）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、更改・廃棄時における利用終了手順に係る規定を策定する場合、以下を含む内容を規定すること。

（ア）外部サービスの利用を終了する場合の移行計画書若しくは終了計画書の作成

（イ）移行計画書若しくは終了計画書の外部サービス利用者への事前通知

②　統括情報セキュリティ責任者は、更改・廃棄時における情報の廃棄に係る規定を策定する場合、以下を含む内容を規定すること。なお、情報資産の廃棄は「2. 情報資産の分類と管理（２）情報資産の管理 ⑩情報資産の廃棄」、「4.1. サーバ等の管理（７）機器等の廃棄」を参照すること。

（ア）情報の廃棄方法

（イ）基盤となる物理機器の廃棄

③　統括情報セキュリティ責任者は、更改・廃棄時におけるアカウントの廃棄に係る規定を策定する場合、以下を含む内容を規定すること。

（ア）作成された外部サービス利用者アカウントの削除

（イ）利用した外部サービス管理者アカウントの削除・返却と再利用の確認

（ウ）外部サービス利用者アカウント以外の特殊なアカウントの削除と関連情報の廃棄

~~（１）　約款による外部サービスの利用に係る規定の整備~~

~~有料、無料に関わらず、約款への同意及び簡易なアカウントの登録により当該機能を利用可能なサービスは約款による外部サービスとなる。この代表例としては、以下のものがある。~~

・電子メール
・ファイルストレージ
・グループウェア等のクラウドサービス　など

なお、電気通信サービスや郵便、運送サービス等は約款による外部サービスの適用範囲外である。

また、約款による外部サービスを利用する場合は、約款の範囲内でのサービス利用となり、特約等を個別に締結することが困難であることが多い。このため、リスクを十分踏まえた上で利用を判断し、セキュリティ対策を適正に講じる必要がある。具体的には次の事項が考えられる。

①約款による外部サービスの利用手順を定める
・利用申請の許可権限者の決定
・利用申請時の申請内容
－利用する組織名
－利用するサービス
－利用目的（業務内容）
－利用期間
－利用責任者（利用アカウントの責任者）　など

②サービス利用中の安全管理に係る運用手順を定める
・サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認
・情報の滅失、破壊等に備えたバックアップの取得
・利用者への定期的な注意喚起
・情報セキュリティインシデント発生時の連絡体制

（２）約款による外部サービスの利用における対策の実施

約款による外部サービスの利用を検討する際は、当該サービスの約款、利用規約、その他の利用条件を確認し、利用の必要性を判断した上、セキュリティ対策も適正に講じる必要がある。具体的には次の事項が考えられる。

・政府機関の関心事項等の情報が分析され、漏えいすることを防ぐため、利用端末や送信元をインターネット上で匿名化する対策の導入を検討することが望ましい。
・外部サービスの提供事業者において情報セキュリティインシデントが発生した場合に備えて、約款に基づき、対処方法（対処手順、責任分界、対処体制等）について契約前に確認しなければならない。
・サーバ装置の故障や運用手順誤り等により、サーバ装置上の情報が滅失し復元不可能となる場合に備えてバックアップを取得する
・サービスの突然の停止に備え、予め代替サービスを確認しておく
・約款や利用規約が予告なく一方的に変更され、セキュリティ設定が変更される場合や一度記録された情報を確実に消去できない場合に備え、サービスで取り扱うことのできる情報をあらかじめ定めておく　等

~~（注１）グループメールサービスの業務利用においても、その設定によってはメールの内容が外部から閲覧可能な状態となり、必要なセキュリティが確保できない場合があるため利用を禁止する必要がある。やむを得ず利用する場合は、利用の要否を十分に検討の上、必要な対策を講じた上で利用する。なお、グループメールサービス利用時の注意喚起については、「グループメールサービスの利用について（注意喚起）」（平成 25 年 7 月 11 日 総務省　事務連絡）を参照されたい。~~

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）~~ソーシャルメディアサービスの利用~~

【趣旨】

機密性２以上の情報を取り扱わない場合であって、外部サービス提供先における高いレベルの情報管理を要求する必要がない場合においても、種々の情報を送信していることを十分認識し、リスクを十分踏まえた上で利用の可否を判断して利用することが求められる。一方、機密性２以上の情報を取り扱う場合と同等のセキュリティ対策を求めることは外部サービスの利用推進を妨げるものであるため、機密性２以上の情報を取り扱わない前提で外部サービスを利用する場合は、「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）」で定めた遵守事項に従って情報セキュリティ対策を適切に講ずることが求められる。~~住民への情報提供など、ソーシャルメディアサービスを利用する場合は、約款による外部サービスを利用することが多くなるが、なりすましやサービス停止のおそれがあるため、ソーシャルメディアサービスによる情報発信時の対策を講じる必要がある。~~

【例文】

（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。

~~①情報セキュリティ管理者は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。~~

~~（ア）本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理ウェブサイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法で~~

~~なりすまし対策を実施すること。~~

~~（イ）パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（IC カード等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること~~

~~②機密性２以上の情報はソーシャルメディアサービスで発信してはならない。~~

~~③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なければならない。~~

~~④アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければならない。~~

（解説）

（１）外部サービスの利用に係る規定の整備

① 統括情報セキュリティ責任者は、自組織において機密性２以上の情報を取り扱わない前提で外部サービスを業務に利用する場合は、以下を例に利用手続を定めること。

（ア）利用申請の許可権限者

（イ）利用申請時の申請内容

・外部サービスの名称（必要に応じて機能名までを含む）

・外部サービス提供者の名称

・利用目的（業務内容）

・取り扱う情報の格付

・利用期間

・利用申請者（所属・氏名）

・利用者の範囲（自組織の関係者内に限る、部局内に限る など）

・選定時の確認結果

② 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わない場合の外部サービスの利用状況を、以下を例に管理すること。

（ア）利用申請の許可権限者は、申請ごとに外部サービス管理者を指名すること。

（イ）利用承認した外部サービスは、その内容を遅滞なく記録するよう運用ルールを定め、常に最新の外部サービスの利用状況を把握できるようにする。記録する際は、以下を例とする項目を記録し自組織内で共有すること。

・外部サービスの名称（必要に応じて機能名までを含む）

・外部サービス提供者の名称

・利用目的（業務内容）

・取り扱う情報の格付

・利用期間

・利用申請者（所属・氏名）

・利用者の範囲（自組織の関係者内に限る、部局内に限る など）。

・外部サービス管理者（所属・氏名）

③ 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わない前提で外部

サービスを業務に利用する場合は、以下を例に運用手順定めること。

（ア）サービス利用中の安全管理に係る運用手順

・サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認

・情報の滅失、破壊等に備えたバックアップの取得

・利用者への定期的な注意喚起（禁止されている機密性２以上の情報の取扱いの有無の確認等）

（イ）情報セキュリティインシデント発生時の連絡体制

~~インターネット上における、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等のソーシャルメディアサービスは、積極的な広報活動等に利用することができるが、外部サービスを利用せざるを得ず、第三者によるなりすましやアカウントの乗っ取り、予告なしでサービスが停止するといった事態が発生する可能性がある。そのため、利用にあたっては、ソーシャルメディアサービスの運用ポリシーや運用手順を定め、ルールに沿った利用を行うことが求められる。具体的には次の事項が考えられる。~~

~~①なりすまし対策~~

~~・庁内で管理しているウェブサイト内において、利用するソーシャルメディアサービスのサービス名と当該アカウントページへのハイパーリンクを明記するページを設ける。~~

~~・運用しているソーシャルメディアサービスの自由記述欄において、庁内ウェブサイト上のページの URL を記載する。~~

~~・ソーシャルメディアサービスの提供事業者が、「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合は、これを利用する。~~

~~②アカウント乗っ取り対策~~

~~・パスワードを適正に管理する。~~

~~・二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されている場合は、可能な限り利用する。~~

~~・ソーシャルメディアサービスへのログインに利用する端末が不正アクセスや盗難されないよう、最新のセキュリティパッチや不正プログラム対策ソフトウェアの導入、端末管理等のセキュリティ対策を実施する。~~

~~なお、アカウント乗っ取りを確認した場合には、被害を最小限にするため、ログインパスワードの変更やアカウントの停止を速やかに実施し、自己管理ウェブサイト等で周知を行うとともに、自組織の情報セキュリティの統一的な窓口に報告すること。~~

~~③サービスが終了・停止した場合の対応~~

~~・あらかじめ発信した情報のバックアップを庁内に保管しておく等、スムーズに別のサービスへの移行が行えるよう適正な準備をしておく。~~

8.4. クラウドサービスの利用

【趣旨】

クラウドサービスの利用に当たっては、クラウド基盤部分を含む情報の流通経路全般を俯瞰し、総合的に対策を設計（構成）した上で、セキュリティを確保する必要がある。

クラウドサービスを利用する際、クラウドサービスの委託先に取扱いを委ねる情報は、当該委託先において適正に取り扱われなければならないが、クラウドサービスの利用においては、適正な取扱いが行われていることを直接確認することが一般に容易ではない。また、クラウドサービスでは、複数利用者が共通のクラウド基盤を利用することから、自身を含む他の利用者にも関係する情報の開示を受けることが困難である。クラウドサービスの委託先を適正に選択するためには、このようなクラウドサービスの特性を理解し、委託先へのガバナンスの有効性や利用の際のセキュリティ確保のために必要な事項を十分考慮することが求められる。

【例文】

①情報セキュリティ管理者は、クラウドサービス（民間事業者が提供するものに限らず、本市が自ら提供するもの等を含む。以下同じ。）を利用するに当たり、取り扱う情報資産の分類及び分類に応じた取扱制限を踏まえ、情報の取扱いを委ねることの可否を判断しなければならない。

②情報セキュリティ管理者は、クラウドサービスで取り扱われる情報に対して国内法以外の法令が適用されるリスクを評価して委託先を選定し、必要に応じて委託事業の実施場所及び契約に定める準拠法・裁判管轄を指定しなければならない。

③情報セキュリティ管理者は、クラウド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、委託先を選定する際の要件としなければならない。

④情報セキュリティ管理者は、クラウドサービスの特性を考慮した上で、クラウドサービス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セキュリティ要件を定めなければならない。

⑤情報セキュリティ管理者は、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提供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。

（解説）

① クラウドサービスの利用に当たっては、情報の管理や処理をクラウドサービス事業者に委ねるため、その情報の適正な取扱いの確認が容易ではなくなることを踏まえ、適切なクラウドサービス事業者を選定することによりリスクを低減することが考えられる。

（注１）クラウドサービスの利用に当たっては、「地方公共団体における ASP・SaaS 導入活用ガイドライン」（平成 22 年 4 月　総務省）を参照されたい。

② インターネットを介してサービスを提供するクラウドサービスの利用に当たっては、クラウドサービス事業者の事業所の場所に関わらず、データセンターの存在地の国の法律の適用を受ける場合があることに留意する必要がある。具体的には、クラウドサービス事業者のサービスの利用を通じて海外のデータセンター内に蓄積された地方公共団体の情報が、データセンターの設置されている国の法令により、日本の法令では認められていない場合であっても海外の当局による情報の差し押さえや解析が行われる可能性があるため、住民情報等の機密性の高い情報を蓄積する場合は、日本の法令の範囲内で運用できるデータセンターを選択する必要がある。

管轄裁判所に関しては、国外の裁判所で裁判を行うこととならないよう、契約において日本国内の裁判所（必要に応じて地方公共団体の所在地を管轄する裁判所）を合意管轄裁判所として規定する必要がある。また、外国に本社を置く企業が提供するサービスを地方公共団体が利用する場合の紛争を当該企業の本社の所在地を管轄する裁判所が管轄することも考えられる一方、その場合は日本の国内法と同等の個人情報の保護などが確立されないおそれがあることについては利用者である地方公共団体において契約締結の際に十分な留意が必要となる。

オープンデータ、環境計測値等の機密性の低い情報をクラウドサービスに蓄積する場合は、どの国の法令が適用されるのかを確認し、リスク等を考慮した上で選択することが望ましい。

③ クラウドサービスを利用するに当たり、サービスの中断や終了時に際し、円滑に業務を移行するための対策として、以下を例とするセキュリティ対策を実施することをクラウドサービスの選定条件とし、仕様内容にも含める必要がある。

・取り扱う情報の可用性区分の格付に応じた、サービス中断時の復旧要件

・取り扱う情報の可用性区分の格付に応じた、サービス終了又は変更の際の事前告知の方法・期限及びデータ移行方法

④ 情報セキュリティ管理者は、クラウドサービス部分を含む情報の流通経路全般にわたるセキュリティ対策を実施する必要がある。システムの重要度に応じて求められる可用性のレベル等（稼働率、目標復旧時間、バックアップの保管方法など）を十分に検討し、調達の際に、検討した結果を調達仕様書に具体的に盛り込まなければならない。また、必要となる条項（インシデントの報告義務、損害賠償等）を盛り込んだ契約及びサービスレベルを保証させるための SLA を締結する必要がある。特に、バックアップについては、契約において、各業務システムの重要度を勘案した適切なバックアップレベルを設定し、別途のバックアップの取得など、レベルに応じた適切な対策を実施することが重要である。

（注２）クラウドサービスの大規模障害により、自治体の業務に長時間支障が発生した事案を踏まえたセキュリティ対策については、「「Jip-Base」事案を踏

まえたクラウドサービスの利用に係る注意喚起」（令和2年5月22日　総行情第76号　総務省自治行政局地域情報政策室長通知）を参照されたい。

（注3）契約に必要となる条項については「8.1.外部委託（3）契約項目」及び「地方公共団体におけるASP・SaaS導入活用ガイドライン」（平成22年4月　総務省）を参照されたい。また、セキュリティ要件の検討を行う際は、「非機能要求グレード（地方公共団体版）利用ガイド」（平成26年3月　地方自治情報センター）も併せて参照されたい。

⑤　情報セキュリティ管理者は、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。

クラウドサービス事業者及び当該サービスの信頼性が十分であることを総合的に判断するためには、クラウドサービスで取り扱う情報の機密性・完全性・可用性が確保されるように、クラウドサービス事業者のセキュリティ対策を含めた経営が安定していること、クラウドやアプリケーションに係るセキュリティ対策が適切に整備され、運用されていること等を評価する必要がある。

このような評価に当たって、クラウドサービス事業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ことが考えられる。

なお、参考となる認証には、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、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事業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）を活用することも考えられる。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。

参考：国際規格

「ISO/IEC 27017（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：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」

「クラウド情報セキュリティ監査制度規程」

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）」

参考：米国公認会計士協会「Service Organization Control (SOC) Reports」

9. 評価・見直し

9.1. 監査

【趣旨】

情報セキュリティポリシーの実施状況について、客観的に専門的見地から評価を行う監査が実施されない場合は、情報セキュリティ対策が徹底されない状態や情報セキュリティポリシーが業務に沿わない状態が続くおそれがある。このことから、監査の実施及びその方法について規定する。

監査を行う者は、十分な専門的知識を有するものでなければならない。また、適正な監査の実施の観点から、監査の対象となる情報資産に直接関係しない者であることが望ましい。また、地方公共団体内の情報セキュリティ対策の監査・報告について中立性を保証され、監査に必要な情報へのアクセス等の権限が明確に与えられる必要がある。監査作業に伴う情報の漏えいのリスクを最小限とするため、監査人等が取り扱う監査に係る情報について、漏えい、紛失等が発生しないように保管する必要がある。

【例文】

（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て監査を行わせなければならない。

（2） 監査を行う者の要件

①情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

②監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

（3） 監査実施計画の立案及び実施への協力

①情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

②被監査部門は、監査の実施に協力しなければならない。

（4） 外部委託事業者に対する監査

外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

（５） 報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、情報セキュリティ委員会に報告する。

（６） 保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適正に保管しなければならない。

（７） 監査結果への対応

CISO 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、当該事項への対処を指示しなければならない。また、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。なお、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、当該事項への対処を指示しなければならない。

（８） 情報セキュリティポリシー及び関係規程等の見直し等への活用

情報セキュリティ委員会は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（解説）

（１） 実施方法

情報セキュリティ対策状況に対して、定期的な監査だけでなく、様々な状況に対応して監査が行えることを定めておく必要がある。随時監査を行うことを明確にすることにより、情報セキュリティポリシーの違反行為に対する抑止効果も期待できる。

（２） 監査を行う者の要件

内部監査、外部監査、いずれの場合も、監査人は、監査対象範囲から独立性を有し、公平な立場で客観的に評価を行うことが求められる。監査人は、監査及び情報セキュリティについて、十分な専門的知識を有する者でなければならない。

（注１）一部又は全部の監査対象範囲に対して、小規模な組織等の理由によって、独立性を維持することができない場合又は組織内に十分な専門的知識を有する者が確保できない場合は、必要な範囲に対して外部の監査人を利用することを検討することが必要である。また、職員等が自らが所属しないその他の部門に対して監査をする相互監査や近隣の地方公共団体との相互監査も有効である。

（注２）監査人は、監査項目が実施できているか否かだけでなく適正な記録が取得

されているかについても確認する必要がある。また、監査項目が実施できていない又は適正な記録が取得されていない場合は、なぜできていないのかその原因にまで踏み込んで分析・報告できることが望ましい。

（３） 監査実施計画の立案及び実施への協力

情報セキュリティ監査統括責任者は、情報セキュリティ監査を行うに当たって、監査人の権限、監査実施に関する項目及び内容を定め、これに基づいて監査実施計画を立案する。監査人は、この計画に基づき監査を実施する。なお、システムに対する監査の実施によって業務が中断される可能性があるため、計画の立案に当たっては中断のリスクを最小限に抑えるよう配慮することが必要である。また、システム監査を行うツールにより、監査人は特権的にデータ等へアクセスし得ることから、誤用・悪用を防止するための適正な管理が求められる。

（注３）情報セキュリティ監査統括責任者は、監査計画及びそれに付随するリスクを効果的かつ効率的に管理するのに必要な資質、並びに次の領域における知識及び技能を有することが望ましい。ただし、必要な資質、並びに知識及び技能を有することが困難な場合は、外部の専門家をあてて能力を補完することも考えられる。

・監査の原則、手順及び方法に関する知識
・マネジメントシステム規格及び基準文書に関する知識
・被監査部門の業務、製品及びプロセスに関する知識
・被監査部門の業務及び製品に関し、適用される法的及びその他の要求事項に関する知識
・該当する場合には、被監査部門の利害関係者に関する知識

また、情報セキュリティ監査統括責任者は、監査計画を管理するのに必要な知識及び技能を維持するために適正な専門能力の継続的開発・維持活動に積極的にかかわることが望ましい。

（注４）監査項目には、庁内外において発生した情報セキュリティインシデントから学んだ対策等の遵守状況の確認や、電磁的記録媒体の管理、情報の持ち出し管理、ソフトウェアライセンス管理、FAX 誤送信防止策等の具体的な情報セキュリティ対策の運用状況の確認も含まれることが望ましい。

（４） 外部委託事業者に対する監査

情報システムの運用、保守等を外部委託している場合は、情報資産の管理が契約に従い適正に実施されているかを点検、評価する必要がある。また、これによって、セキュリティ侵害行為に対する抑止効果も期待できる。

（５） 報告

情報セキュリティ監査統括責任者は、監査調書をもとに、被監査部門に対する監査人の指摘事項の正確性や指摘に対する改善提案の実現性を確認し監査報告書を作成し、監査報告書を情報セキュリティ委員会に報告する。

CISO は、監査報告を受けて、被監査部門に改善を指示する。被監査部門は、改善

計画を立案し実施する。最後に監査人は、フォローアップ監査により、改善状況や改善計画の完了について確認を行う必要がある。

（６） 保管

監査により作成した監査調書には、脆弱性の情報等機微な情報が含まれていることが多いことから、情報セキュリティ監査統括責任者は、紛失等が生じないように保管する必要がある。

（７） 監査結果への対応

監査結果を適正にセキュリティ改善に結び付けるため、CISO に関係部局への指示を義務付けた規定である。また、監査の指摘事項と同種の課題が他の部署にも存在する場合があることから、当該可能性の高い部署に対しては、課題や問題点の有無を確認させる必要がある。

（８） 情報セキュリティポリシー及び関係規程の見直し等への活用

監査結果は、情報セキュリティポリシー及び関係規程の見直し等の基礎資料として活用しなければならない。

（注５）情報セキュリティ監査の実施方法等については、「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」（令和 X2 ~~2~~ 年 XX ~~12~~ 月　総務省）及び「地方公共団体情報セキュリティ管理基準解説書」（平成 17 年 2 月　総務省）を参考にされたい。

9.2. 自己点検

【趣旨】

情報セキュリティポリシーの履行状況等を自ら点検、評価することは、情報セキュリティポリシーの遵守事項を改めて認識できる有効な手段である。自己点検は、情報システム等を運用する者又は利用する者自らが実施するので、監査のような客観性は担保されないが、監査と同様に、点検結果を踏まえ各部門で改善を図ったり、組織全体のセキュリティ対策の改善を図る上での重要な情報になる情報セキュリティ対策の評価を行い、対策の見直しに資するものである。また、職員等の情報セキュリティに関する意識の向上や知識の習得にも有効である。

このことから、自己点検を定期的に実施する規定を設け、その活用方法とあわせて規定する。

【例文】

（１） 実施方法

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、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

②情報セキュリティ責任者は、情報セキュリティ管理者と連携して、所管する部局における情報セキュリティポリシーに沿った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て自己点検を行わなければならない。

（２） 報告

統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。

（３） 自己点検結果の活用

①職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

②情報セキュリティ委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（解説）

（１） 実施方法

情報セキュリティ対策の実施状況について、定期的な自己点検だけでなく、様々な状況に対応して自己点検を実施する。

（注１）自己点検は自己点検票を用いた、アンケート方式で行う場合が多い。アンケートを行う場合に留意すべき点は、そのセキュリティ対策上担う役割に応じたアンケート項目とすることである。アンケートは、回答者による再認識や新たな発見にもつながり得る。アンケート項目によって、自部門の対策で、何が欠落しているのか鮮明にすることが可能になるために、改善の必要性の認識をさせられる効果もある。

（注２）保有する個人情報の人的な要因による漏えいを踏まえた点検については、「地方公共団体の保有する情報資産の管理状況等の再点検について（周知）」（平成24年10月29日　総行情第71号　総務省自治行政局地域情報政策室長通知）及び「地方公共団体における個人情報の漏洩防止対策について（注意喚起）」（平成25年8月5日　総務省　事務連絡）を参照されたい。

（注３）技術的な脆弱性の悪用に対する点検については、「地方公共団体等が管理するウェブサイトに係る脆弱性の確認及び対策の点検・実施等について（依頼）」（平成24年9月26日　総行情第66号　総務省自治行政局地域情報政策室長通知）を参照されたい。

（２）　報告

情報セキュリティ責任者は、自己点検結果について、自らが担当する組織のまとまり特有の課題の有無を確認するなどの観点から自己点検結果を分析、評価することが望ましい。また、統括情報セキュリティ責任者は、共通の課題の有無を確認するなどの観点から自己点検結果を分析、評価することが望ましい。

（３）　自己点検結果の活用

自己点検結果は、職員等が自らの業務の見直しに活用するとともに、監査結果と同様に、情報セキュリティポリシーの見直し等の情報として活用することができる。

（注４）総務省が平成18年3月に公表した「地方公共団体の情報セキュリティレベルの評価に係る制度の在り方に関する調査研究報告書」の参考資料である「情報セキュリティレベル評価ツール」を自己点検に用いることも可能である。

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

【趣旨】

情報セキュリティ対策は、情報セキュリティに関する脅威や技術等の変化に応じて、必要な対策が変化するものであり、情報セキュリティポリシー及び関係規程等は、定期的に見直すことが求められる。また監査や自己点検の結果等から、同ポリシー及び関係規程等の見直しの必要性が確認される場合もある。

このことから、情報セキュリティポリシー及び関係規程等の見直しについて規定する。

【例文】

情報セキュリティ委員会は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、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、必要があると認めた場合、改善を行うものとする。

（解説）

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、監査や自己点検の結果を受けて、情報セキュリティ分野の専門家による評価や保有する情報システムに関するリスク評価の結果等を活用しつつ、情報セキュリティポリシー及び関係規程等の見直しを行う。

また、情報セキュリティポリシー及び関係規程等は、組織にとっての脅威の変化や組織体制の変更、新たな対策技術の提供等によっても見直すべきものであり、あらかじめ定めた間隔及び重大な変化が発生した場合等、状況に応じて柔軟に運用していくことが必要である。

（注１）見直しに当たっては、情報セキュリティポリシー及び関係規程等と実態との相違を十分考慮することが重要であり、関係部局から意見聴取等を行い、実態把握を行うことが望ましい。また、情報セキュリティポリシー及び関係規程等を見直す際には、必要に応じてリスク分析の見直しを行うことが重要である。日頃から新たな攻撃方法や対策技術の情報収集に努め、情報セキュリティポリシー及び関係規程等の見直しに活用することも必要である。

（注２）情報セキュリティポリシー及び関係規程等の見直しは、地方公共団体の長及びこれに準じる者の決裁により正式に決定される。

（注３）情報セキュリティポリシー及び関係規程等を見直した際には、その内容を職員等や外部委託事業者に十分に周知する必要がある。

（注４）見直しの際は、情報セキュリティポリシー及び関係規程等に次の事項によって生じる要求事項が含まれているか確認すること。

・事業計画

・規制、法令及び契約
・現在及び将来予想される情報セキュリティの脅威環境

10. 用語の定義

本ガイドラインにおいて次の各号に掲げる用語の定義は、当該各号に定めるところによる。

【あ】

●「遠隔消去機能」

「遠隔消去機能」→「リモートワイプ機能」を参照。

●「暗号化消去」

「暗号化消去」とは、情報を電磁的記録媒体に暗号化して記録しておき、情報の抹消が必要になった際に情報の復号に用いる鍵を抹消することで情報の復号を不可能にし、情報を利用不能にする論理的削除方法をいう。暗号化消去に用いられる暗号化機能の例としては、ソフトウェアによる暗号化（Windows の BitLocker 等）、ハードウェアによる暗号化（自己暗号化ドライブ（Self-Encrypting Drive）等）などがある。

● 「Web 会議サービス」

「Web 会議サービス」とは、専用のアプリケーションや Web ブラウザを利用し、映像又は音声を用いて会議参加者が対面せずに会議を行える外部サービスをいう。なお、特定用途機器どうしで通信を行うもの（テレビ会議システム等）は含まれない。

【か】

● 「外部サービス」

「外部サービス」とは、民間事業者等の庁外の組織が情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において自組織の情報が取り扱われる場合に限る。

● 「外部サービス管理者」

「外部サービス管理者」とは、外部サービスの利用における利用申請の許可権限者から利用承認時に指名された当該外部サービスに係る管理を行う者をいう。

● 「外部サービス提供者」

「外部サービス提供者」とは、外部サービスを提供する事業者をいう。外部サービスを利用して自組織に向けて独自のサービスを提供する事業者は含まれない。

● 「外部サービス利用者」

「外部サービス利用者」とは、外部サービスを利用する自組織の職員等又は業務委託した委託先において外部サービスを利用する場合の委託先の従業員をいう

●「供給者」

「供給者」とは、サプライチェーンの一部を構成し、データの処理やサービス等で連携する組織をいう。

●「クラウドサービス」

「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。この構成要素として、SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）が存在する。

~~●「クラウドサービス事業者」~~

~~「クラウドサービス事業者」とは、クラウドサービスを提供する事業者又はクラウドサービスを用いて情報システムを開発・運用する事業者をいう。~~

【さ】

●「サプライチェーン」

「サプライチェーン」とは、部品やサービス等の供給に多種多様な主体が係わった取引の連鎖をいう。

●「シンクライアント」

「シンクライアント」とは、サーバ側に仮想的なクライアント環境を設けた上で、当該クライアント環境にパソコンやモバイル端末が専用のアプリケーションを使用してアクセスし、パソコンやモバイル端末にデータを保存せずに、データの閲覧や編集を行うことを可能とする機能をいう。

●「事業継続計画」

「事業継続計画」→「BCP」を参照。

●「情報セキュリティインシデント」

「情報セキュリティインシデント」とは、望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

●「情報セキュリティ事象」

情報セキュリティ方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象

●「送信ドメイン認証技術」

「送信ドメイン認証技術」とは、メール送信者情報のドメインが正しいものかどうかを検証することができる仕組みをいう。現在のメール送信においては、送信者情報を詐称することが可能で、実際、多くの迷惑メールは他のアドレスになりすまして送られているため、成りすまし対策として用いられる。

●「ソーシャルメディアサービス」

「ソーシャルメディアサービス」とは、インターネット上で展開される情報メディアのあり方で、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアのことをいう。利用者の発信した情報や利用者間のつながりによってコンテンツを作り出す要素を持ったWeb サイトやネットサービスなどを総称する用語で、電子掲示板(BBS)やブログ、動画共有サイト、動画配信サービス、ショッピングサイトの購入者評価欄などを含む。

【た】

●「多要素認証」

「多要素認証」とは、システムが正規の利用者かどうかを判断する際の信頼性を高めるために、複数の認証手段を組み合わせて認証する方式をいう。認証方式は大きく分けて「知識」、「所持」及び「存在」を利用する方式がある。それぞれの認証手段には各々異なった利点と欠点があり、複数の認証方式を組み合わせることが利用者認証の信頼性を高める意味でも有効である。

●「端末」

「端末」とは、情報システムの構成要素である機器のうち、職員が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りが無い限り、地方公共団体が調達又は開発するものをいう。

●庁内ネットワーク

「庁内ネットワーク」とは、地方公共団体の庁舎・出先機関を含めた団体が管理主体となるネットワーク及び同ネットワークを外部委託データセンターに設置している情報システムをいう。

●「電子署名」

「電子署名」とは、情報の正当性を保証するための電子的な署名情報をいう。

●「特権 ID」

「特権 ID」とは、サーバの起動や停止、アプリケーションのインストールやシステム設定の変更、全データへのアクセスなど、通常の ID よりもシステムに対するより高いレベルでの操作が可能な ID をいう。

●「ドメイン名」

「ドメイン名」とは、国、組織、サービス等の単位で割り当てられたネットワーク上の名前であり、英数字及び一部の記号を用いて表したものをいう。

【は】

●「パソコン」

「パソコン」とは、端末のうち、机の上等に備え置いて業務に使用することを前提とし、移動させて使用することを目的とはしていないものをいい、端末の形態は問わない。

●「標的型攻撃」

「標的型攻撃」とは、明確な意思と目的を持った人間が特定のターゲットや情報に対して特定の目的のために行うサイバー攻撃の一種をいう。

【ま】

●「モバイル端末」

「モバイル端末」とは、端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

【や】

●「約款による外部サービス」

「約款による外部サービス」とは、民間事業者等の庁外の組織が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うものをいう。ただし、利用者が必要とする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除く。

【ら】

●「リスク分析」

「リスク分析」とは、リスク特定、リスク分析、リスク評価を網羅するプロセス全体を指す。リスク分析を行った後、リスク対応を行う。リスク対応の手段には、リスク源の除去、起こりやすさの変更、結果の変更、他者とのリスクの共有、リスクの保有などがある。

●「リモートワイプ機能」

「リモートワイプ機能」とは、携帯電話などに記録してあるデータを、当該端末から操作するのではなく離れた場所から、遠隔操作（リモート）で、消去、無効化する機能をいう。携帯電話を紛失したり盗難にあった場合の、情報漏えいを防ぐ目的で利用される。

【A～Z】

●「BCP（Busisness Continuity Plan：事業継続計画）」

「BCP」とは、組織において特定する事業の継続に支障をきたすと想定される自然災害、人的災害・事故、機器の障害等の事態に組織が適正に対応し目標とする事業継続性の確保を図るために当該組織において策定する、事態の予防及び事態発生後の事業の維持並びに復旧に係る計画をいう。

●「CRYPTREC（Cryptgraphy Research and Evaluation Commmittiees）」

「CRYPTREC」とは、電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクトである。

●「CSIRT（Computer Security Incident Response Team）」

「CSIRT」とは、コンピュータやネットワーク（特にインターネット）上で何らかの問題（主にセキュリティ上の問題）が起きていないかどうか監視すると共に、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う組織の総称。

●「URL（Uniform Resource Locator）」

「URL」とは、インターネット上の情報資源の場所とその属性を指定する記述方式。情報資源の種類やアクセス方法、情報を提供するウェブサーバの識別名、ファイルの所在を指定するパス名などで構成される。

●「VPN（Virtual Private Network）」

「VPN」とは、暗号技術等を利用し、インターネット等の公衆回線を仮想的な専用回線として利用するための技術である。