

地方公共団体における
情報セキュリティポリシーに関する
ガイドライン(平成22年11月版)

平成13年 3月30日 策 定
平成15年 3月18日 一部改定
平成18年 9月29日 全部改定
平成22年11月 9日 一部改定

総務省

目次

第1章 総則	2
1.1. 本ガイドラインの目的	2
1.2. 本ガイドラインの経緯	3
1.3. 地方公共団体における情報セキュリティの考え方	5
1.4. 情報セキュリティポリシーの必要性と構成	6
1.5. 情報セキュリティ対策の実施サイクル	7
1.6. 策定及び導入.....	8
1.6.1. 策定及び導入の概要	8
1.6.2. 組織体制の確立	8
1.6.3. 情報セキュリティ基本方針の策定	9
1.6.4. リスク分析の実施.....	9
1.6.5. 情報セキュリティ対策基準の策定	10
1.6.6. 情報セキュリティポリシーの決定	10
1.6.7. 実施手順の策定	10
1.6.8. 情報セキュリティポリシー及び実施手順の周知	11
1.7. 運用	12
1.8. 評価・見直し.....	13
1.8.1. 監査・自己点検	13
1.8.2. 情報セキュリティポリシーの見直し	13
1.9. 本ガイドラインの構成と対策レベルの設定	14
1.9.1. 本ガイドラインの構成	14
1.9.2. 本ガイドラインにおける対策レベルの設定	14
第2章 情報セキュリティ基本方針	16
2.1. 情報セキュリティ基本方針の目的.....	16
2.2. 情報セキュリティ基本方針の形式.....	16
2.3. 基本的事項を規定する形式	17
2.4. 宣言書の形式.....	20
第3章 情報セキュリティ対策基準	22
3.1. 対象範囲	22
3.2. 組織体制	24
3.3. 情報資産の分類と管理方法	30

3.4. 物理的セキュリティ	35
3.4.1. サーバ等の管理	35
3.4.2. 管理区域(情報システム室等)の管理	39
3.4.3. 通信回線及び通信回線装置の管理	42
3.4.4. 職員等のパソコン等の管理	43
3.5. 人的セキュリティ	45
3.5.1. 職員等の遵守事項	45
3.5.2. 研修・訓練	49
3.5.3. 事故、欠陥等の報告	52
3.5.4. ID及びパスワード等の管理	54
3.6. 技術的セキュリティ	56
3.6.1. コンピュータ及びネットワークの管理	56
3.6.2. アクセス制御	64
3.6.3. システム開発、導入、保守等	68
3.6.4. 不正プログラム対策	73
3.6.5. 不正アクセス対策	76
3.6.6. セキュリティ情報の収集	78
3.7. 運用	80
3.7.1. 情報システムの監視	80
3.7.2. 情報セキュリティポリシーの遵守状況の確認	81
3.7.3. 侵害時の対応	83
3.7.4. 外部委託	87
3.7.5. 例外措置	91
3.7.6. 法令遵守	92
3.7.7. 懲戒処分等	93
3.8. 評価・見直し	94
3.8.1. 監査	94
3.8.2. 自己点検	97
3.8.3. 情報セキュリティポリシーの見直し	99

【参考】

情報セキュリティ対策基準の例文
権限・責任等一覧表

総則

第1章 総則

1.1. 本ガイドラインの目的

情報セキュリティポリシーとは、組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた文書をいう。

地方公共団体における情報セキュリティは、各地方公共団体が保有する情報資産に自ら責任を持って確保すべきものであり、情報セキュリティポリシーも各地方公共団体が組織の実態に応じて自主的に策定するものである。

本ガイドラインは、各地方公共団体が情報セキュリティポリシーの策定や見直しを行う際の参考として、情報セキュリティポリシーの考え方及び内容について解説したものである。したがって、本ガイドラインで記述した構成や文例は、参考として示したものであり、各地方公共団体が独自の構成、表現により、情報セキュリティポリシーを定めることを妨げるものではない。

既に、多くの地方公共団体において、情報セキュリティポリシーが策定されているが、今後は情報セキュリティポリシーの定期的な評価・見直しを行い、情報セキュリティ対策の実効性を確保するとともに、対策レベルを高めていくことが重要である。本ガイドラインは、三度の改定を通じて、新たな脅威等に対応した情報セキュリティ対策を追加しているので、情報セキュリティポリシーの評価・見直しを行う際にも、本ガイドラインが活用されることが期待される。

1.2. 本ガイドラインの経緯

総務省では、地方公共団体における情報セキュリティポリシーの策定を推進するため、平成 13 年 3 月 30 日に「地方公共団体における情報セキュリティポリシーに関するガイドライン」を策定した。その後、平成 15 年 3 月 18 日に同ガイドラインを一部改定し、①外部委託に関する管理、②情報セキュリティ監査、③無線 LAN 等の新たな技術動向等を踏まえた記述等の追加を行った。さらに、平成 18 年 9 月 29 日に全部改定し、①地方公共団体のセキュリティ水準の強化、②「重要インフラにおける情報セキュリティ確保に係る『安全基準等』策定にあたっての指針」（以下「重要インフラ指針」という。）への対応、③分かりやすい表現への変更等を行った。

一方、平成 18 年 2 月 2 日、政府の情報セキュリティ政策会議は、「第 1 次情報セキュリティ基本計画」を決定し、この中で、地方公共団体に関して、政府は平成 18 年 9 月を目処に「地方公共団体における情報セキュリティポリシーに関するガイドライン」の見直しを行うこととされ、見直しに当たっては、重要インフラ指針を踏まえることとされた。

また、平成 21 年 2 月 3 日、政府の情報セキュリティ政策会議は、「第 1 次情報セキュリティ基本計画」に基づく各種の取組み進展や社会環境の変化などを踏まえ、引き続き我が国全体として情報セキュリティ問題への取組みを力強く推進するために、平成 21 年度以降を念頭に置いた「第 2 次情報セキュリティ基本計画」を決定し、この中で、地方公共団体に関して、小規模な地方公共団体も含め、全ての地方公共団体において、望ましい情報セキュリティ対策が実施されることを目指し、対策の促進を行うこととされた。

さらに、平成 22 年 5 月 11 日、政府の情報セキュリティ政策会議は、「第 2 次情報セキュリティ基本計画」に基づく官民の各主体による取組を継続しつつ、新たな環境変化に対応した政府の取組を進めるために、「第 2 次情報セキュリティ基本計画」を含有する、「国民を守る情報セキュリティ戦略」を決定し、平成 32 年までに、インターネットや情報システム等の情報通信技術を利用者が活用するに当たっての脆弱性を克服し、全ての国民が情報通信技術を安心して利用できる環境（高品質、高信頼性、安全・安心を兼ね備えた環境）を整備し、世界最先端の「情報セキュリティ先進国」を実現することを目標としている。

なお、重要インフラ指針については、平成 18 年 2 月 2 日に政府の情報セキュリティ政策会議によって決定以降、平成 19 年 6 月 14 日及び平成 22 年 5 月 11 日に改定され、平成 22 年 7 月 30 日には「対策編」が策定されている。

総務省では、これらの新たな対策技術の動向、政府の情報セキュリティ政策の改定等を踏まえ、横断的に俯瞰して必要度が高い項目や先進的な取組みを参考とすることにより、地方公共団体の情報セキュリティ水準の向上及び情報セキュリティ対策の浸透を推進するため、今般、ガイドラインを改定したものである。

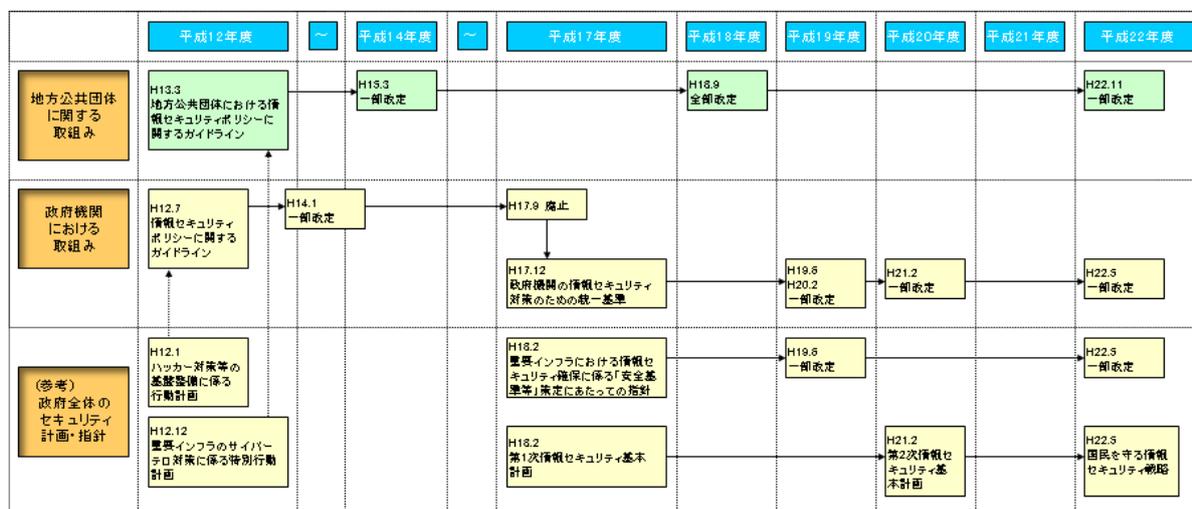
1.2. 本ガイドラインの経緯

【参考】政府機関の情報セキュリティ対策

政府機関については、平成12年7月18日に情報セキュリティ対策推進会議が「情報セキュリティポリシーに関するガイドライン」を決定し、このガイドラインに基づき、各府省庁が情報セキュリティポリシーを策定することにより、情報セキュリティ対策を実施してきた。

しかし、各府省庁の情報セキュリティ対策の整合化・共通化を促進し、政府機関全体としての情報セキュリティ水準の向上を図るため、平成17年12月13日に情報セキュリティ政策会議が、新たに「政府機関の情報セキュリティ対策のための統一基準（2005年12月版（全体版初版）」を策定し、各府省は統一基準を踏まえ、情報セキュリティポリシー等の見直しを行い、対策を実施している。

なお、「政府機関の情報セキュリティ対策のための統一基準」は、技術や環境の変化を踏まえ見直しを行うこととされており、平成19年6月14日、情報セキュリティ政策会議第12回会合、平成20年2月4日、情報セキュリティ政策会議第16回会合、平成21年2月3日、情報セキュリティ政策会議第20回会合、及び平成22年5月11日、情報セキュリティ政策会議第23回会合において、改訂版が決定されている。



図表1 情報セキュリティポリシー等に関する取組の推移

1.3. 地方公共団体における情報セキュリティの考え方

地方公共団体は、法令等に基づき、住民の個人情報や企業の経営情報等の重要情報を多数保有するとともに、他に代替することができない行政サービスを提供している。また、地方公共団体の業務の多くが情報システムやネットワークに依存していることから、住民生活や地域の社会経済活動を保護するため、地方公共団体は、情報セキュリティ対策を講じて、その保有する情報を守り、業務を継続することが必要となっている。

今後、各種手続のオンライン利用の本格化や情報システムの高度化等、電子自治体が進展することにより、情報システムの停止等が発生した場合、広範囲の業務が継続できなくなり、住民生活や地域の経済社会活動に重大な支障が生じる可能性も高まる。また、地方公共団体は LGWAN 等のネットワークにより相互に接続しており、一部の団体で発生した IT 障害がネットワークを介して他の団体に連鎖的に拡大する可能性は否定できない。

これらの事情から、すべての地方公共団体において、情報セキュリティ対策の実効性を高めるとともに対策レベルを一層強化していくことが必要となっている。また、情報セキュリティの確保に絶対安全ということはないことから、情報セキュリティに関する事故の未然防止のみならず、事故が発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じていくことが必要である。

なお、情報セキュリティ対策は、個人情報保護対策と内容的に重なる部分も多い。また、自然災害時や大規模・広範囲にわたる疾病における対応という意味では防災対策とも重なる。情報セキュリティを対策する部署とこれらを担当する部署は、相互に連携をとって、それぞれの対策に取り組むことが求められる。

また、地方公共団体は、自らの情報セキュリティを確保するとともに、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ことが望まれる。例えば、住民等への広報による啓発、IT 講習等による住民等への情報セキュリティに関する研修の実施、業務面で関係する団体に対する情報セキュリティポリシーの策定の働きかけなどの取り組みを行うことが考えられる。

1.4. 情報セキュリティポリシーの必要性と構成

地方公共団体においては、情報セキュリティ対策を徹底するには、対策を組織的に統一して推進することが必要であり、そのためには組織として意思統一し、明文化された文書として、情報セキュリティポリシーを定めなければならない。

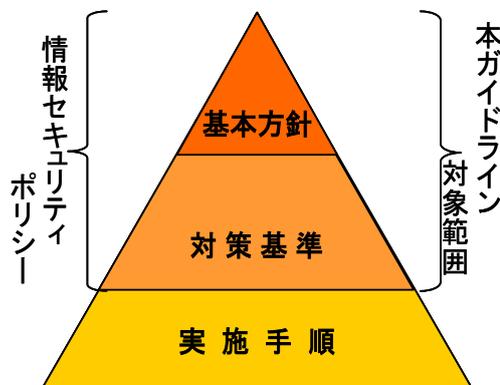
なお、行政手続等における情報通信の技術の利用に関する法律（平成 14 年法律第 151 号）第 9 条第 1 項は、「地方公共団体は、地方公共団体に係る申請、届出その他の手続における情報通信の技術の利用の促進を図るため、この法律の趣旨にのっとり、当該手続に係る情報システムの整備及び条例又は規則に基づく手続について必要な措置を講ずること」に努めなければならないと規定しており、条例等に基づく手続きについては、同法第 8 条第 2 項（安全性及び信頼性の確保）の趣旨にのっとり、地方公共団体は情報セキュリティポリシーの策定や見直しを行うことが求められている。

情報セキュリティポリシーの体系は、図表 2 に示す階層構造となっている。

各地方公共団体の情報セキュリティ対策における基本的な考え方を定めるものが、「基本方針」である。この基本方針に基づき、すべての情報システムに共通の情報セキュリティ対策の基準を定めるのが「対策基準」である。この「基本方針」と「対策基準」を総称して「情報セキュリティポリシー」という。この「対策基準」を、具体的なシステムや手順、手続に展開して個別の実施事項を定めるものが「実施手順」である。

このように、情報セキュリティポリシーは、情報セキュリティ対策の頂点に位置するものであることから、地方公共団体の長をはじめ、すべての職員等及び外部委託事業者は、業務の遂行に当たって情報セキュリティポリシーを遵守する義務を負う。

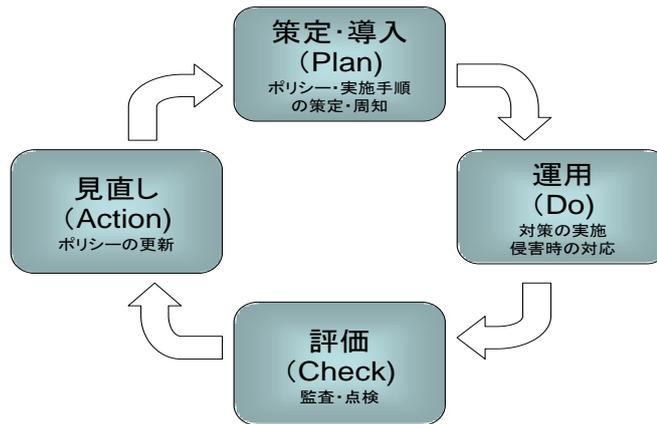
なお、本ガイドラインの対象とする範囲は「情報セキュリティポリシー」を構成する「基本方針」及び「対策基準」であり、「実施手順」は含まれない。



図表 2 情報セキュリティポリシーに関する体系図

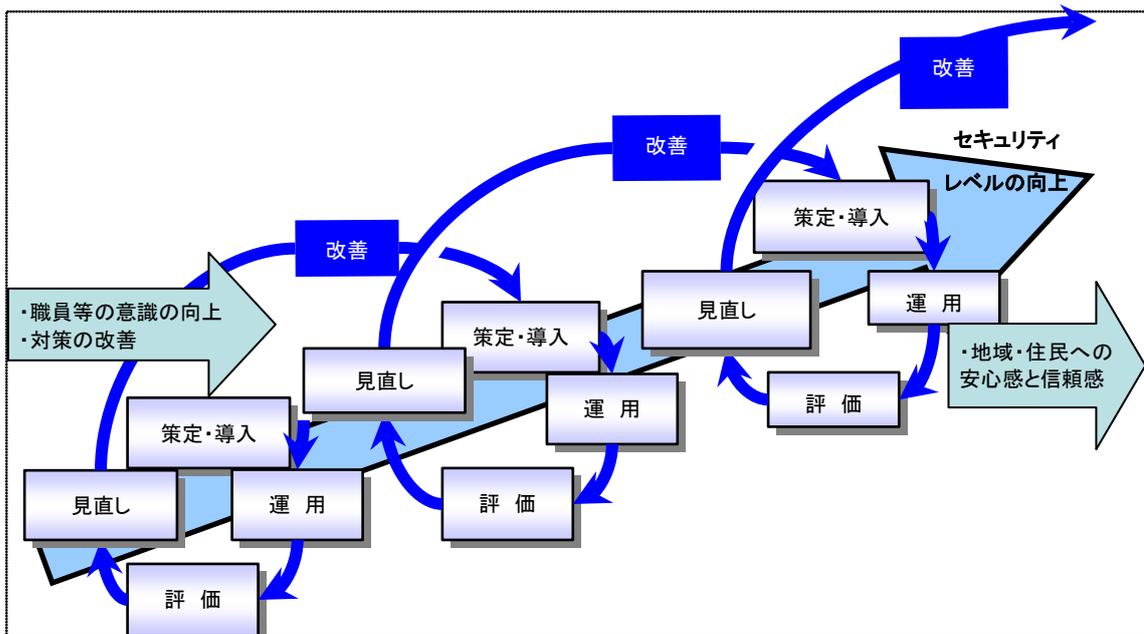
1.5. 情報セキュリティ対策の実施サイクル

情報セキュリティ対策の実施プロセスは、図表 3 のとおり、策定・導入 (Plan)、運用 (Do)、評価 (Check)、見直し (Action) の 4 段階に分けることができ、この実施サイクルを繰り返すことによって情報セキュリティは確保される。この実施サイクルは、それぞれの項目の頭文字をとって、PDCA サイクルとも呼ばれる。



図表 3 情報セキュリティ対策の PDCA サイクル

情報セキュリティを取り巻く脅威や対策は常に変化しており、以上の PDCA サイクルは、一度限りではなく、図表 4 のとおり、これを定期的に繰り返すことで、環境の変化に対応しつつ、情報セキュリティ対策の水準の向上を図らなければならない。



図表 4 PDCA サイクルの繰り返しによる情報セキュリティ対策の水準の向上

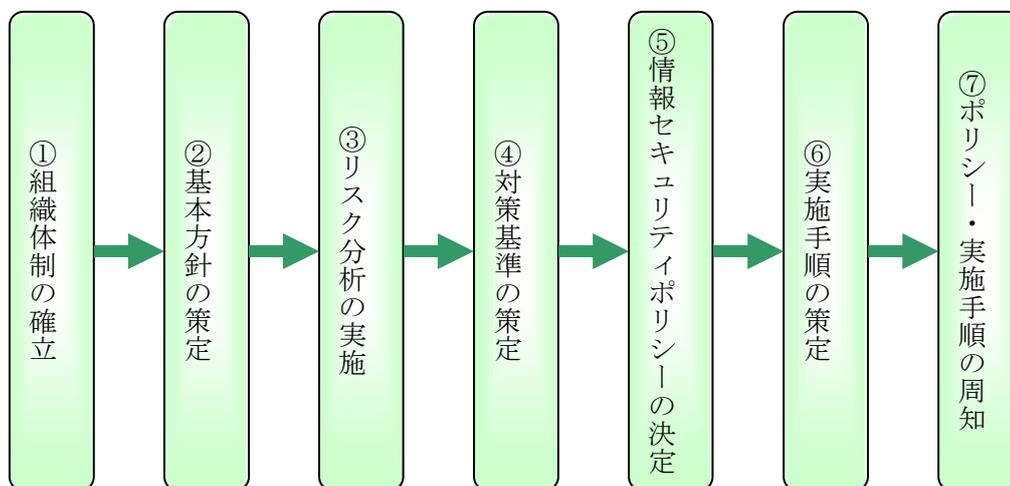
1.6.1. 策定及び導入の概要

～ 1.6.2. 組織体制の確立

1.6. 策定及び導入

1.6.1. 策定及び導入の概要

情報セキュリティポリシーの策定及び導入は、図表 5 のとおり、まず、①策定のための組織体制を確立し、その組織体制の下で、②地方公共団体の基本方針を策定する。次に、③リスク分析を実施し、その結果に基づき、④対策基準の策定を行い、⑤情報セキュリティポリシーを正式に決定する。この後、情報セキュリティポリシーに基づき、⑥実施手順を策定し、⑦ポリシー・実施手順の周知を行うというプロセスになる。



図表 5 情報セキュリティポリシーの策定・導入のプロセス

1.6.2. 組織体制の確立

(1) 組織体制の確立

情報セキュリティポリシーの策定には、幹部職員の関与が不可欠である。また、情報セキュリティポリシーは、組織内の様々な部局の情報資産に係る問題を取り扱うことから、責任の所在を明確にするため、すべての部局の長、情報システムを所管する課室長及び情報セキュリティに関する専門的知識を有する者などで構成する組織又はこれに代わる組織（以下、本章において、「情報セキュリティ委員会等」という。）が行う。

（注1）小規模の団体の場合には、新たに、組織を立ち上げるのではなく、「情報化推進委員会」等の既存の類似する組織が行う場合もありえる。

（注2）組織が有機的に機能するために全組織横断的な指示、連絡可能な役割及び権限を明確にすることが望ましい。

(2) 情報セキュリティポリシー策定チームの編成

情報セキュリティ委員会等は、情報セキュリティポリシーの策定作業の一部を下部の組織（情報セキュリティポリシー策定チーム等）に行わせることができる。策定チームには、すべての部、課等の関係者が関与することが望ましいが、主たる関係部署に絞って構成する場合もある。

部署	選定の理由
情報政策担当課	庁内業務の情報政策の主管
情報システム担当課	庁内の情報システムの主管
総務担当課	個人情報保護条例の主管
文書担当課	文書管理システム、文書管理規程の主管
防災担当課	災害等の危機管理の主管
施設管理担当課	庁内の施設管理の主管
広報担当課	報道機関への対応の主管

図表 6 情報セキュリティポリシー策定チームの編成例

1.6.3. 情報セキュリティ基本方針の策定

情報セキュリティ基本方針においては、情報セキュリティ対策の目的、体系等、各地方公共団体の情報セキュリティに対する基本的な考え方を示す。

1.6.4. リスク分析の実施

リスク分析とは、各地方公共団体が保有する情報資産を明らかにし、それらに対するリスクを評価することである。具体的なリスク分析・評価方法については「地方公共団体における情報資産のリスク分析・評価に関する手引き」（平成 21 年 3 月 総務省）を参照されたい。その他、様々なリスク分析方法があるが、例えば、図表 7 のとおり、次の手順で行う。

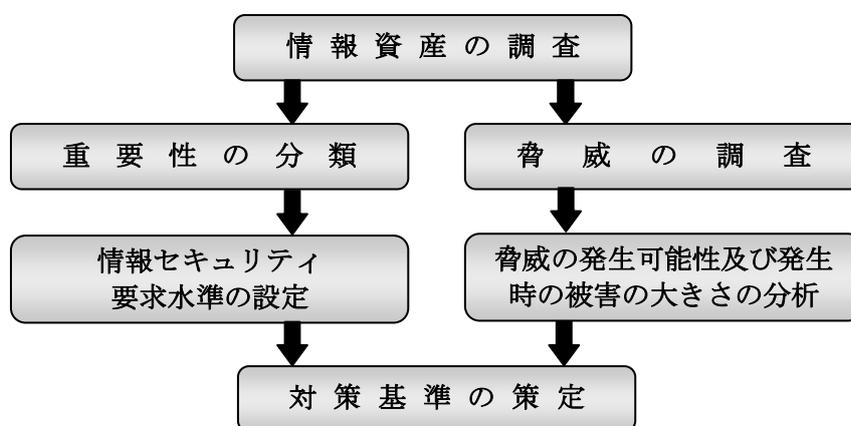
- (1) 各地方公共団体の保有する情報資産を調査の上、重要性の分類を行い、この結果に基づき、要求されるセキュリティの水準を定める。
- (2) 各地方公共団体の情報資産を取り巻く脅威の調査を行い、その発生可能性及び発生した際の被害の大きさからリスクの大きさを求める。
なお、一般的に両者の積をリスクの大きさとしている。
- (3) リスクの大きさがセキュリティ要求水準を下回るよう対策基準を策定し、適切なリスク管理を行う。

1.6.5. 情報セキュリティ対策基準の策定

～ 1.6.7. 実施手順の策定

なお、情報資産や情報資産に対するリスクに大きな変化が生じたときには、関係する情報資産についてリスク分析を再度行い、その結果、情報セキュリティポリシーの見直しが必要と判断される場合にはその見直しを行う。また、定期的な情報セキュリティポリシーの評価・見直しの際にもリスク分析から再検討することが必要である。

リスク分析に関する資料は、情報セキュリティポリシー策定の基礎資料として保管する必要があるが、当該資料には情報資産の脆弱性に関する事項が記載されているため、厳重な管理が必要である。



図表7 リスク分析の事例

1.6.5. 情報セキュリティ対策基準の策定

リスク分析の結果得られる情報セキュリティ要求水準に対して、それを実現するための遵守事項や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。情報セキュリティ対策基準は、想定される情報リスクに十分に対処し、情報セキュリティ要求水準を満たすものでなければならない。

1.6.6. 情報セキュリティポリシーの決定

情報セキュリティ委員会等が策定した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について、地方公共団体の長又はこれに準じる者の決裁により、当該地方公共団体における情報セキュリティポリシーとして正式に決定する。

1.6.7. 実施手順の策定

実施手順は、職員等関係者が、各々の扱うネットワーク及び情報システムや携わる業務において、どのような手順で情報セキュリティポリシーに記述された内容を実行していくかを定めるマニュアルに該当する。このマニュアルには、主要な情報

1.6.8. 情報セキュリティポリシー及び実施手順の周知

資産に対するセキュリティ対策実施手順も含まれる。

実施手順は、個別の目的のために作成し、見直し等を柔軟に行っていくため、業務担当課において情報システムや情報資産を管理する者等が策定することが適当である。

1.6.8. 情報セキュリティポリシー及び実施手順の周知

情報セキュリティ対策を最終的に実施するのは職員等であるため、実効性を確保するため情報セキュリティポリシーの配布や説明会などにより、情報セキュリティポリシーを職員等に十分に周知する。また、実施手順については、各課部局の責任者が当該手順を実行する者に周知する。

1.7. 運用

1.7. 運用

情報セキュリティポリシーを確実に運用していくため、情報システムの監視や情報セキュリティポリシーに従って対策が適切に遵守されているか否かを確認し、情報資産に対する侵害や情報セキュリティポリシー違反に対し、適正に対応しなければならない。このため、緊急時対応計画の策定、同計画に基づく訓練、同計画の評価・見直し等を実施する。

1.8. 評価・見直し

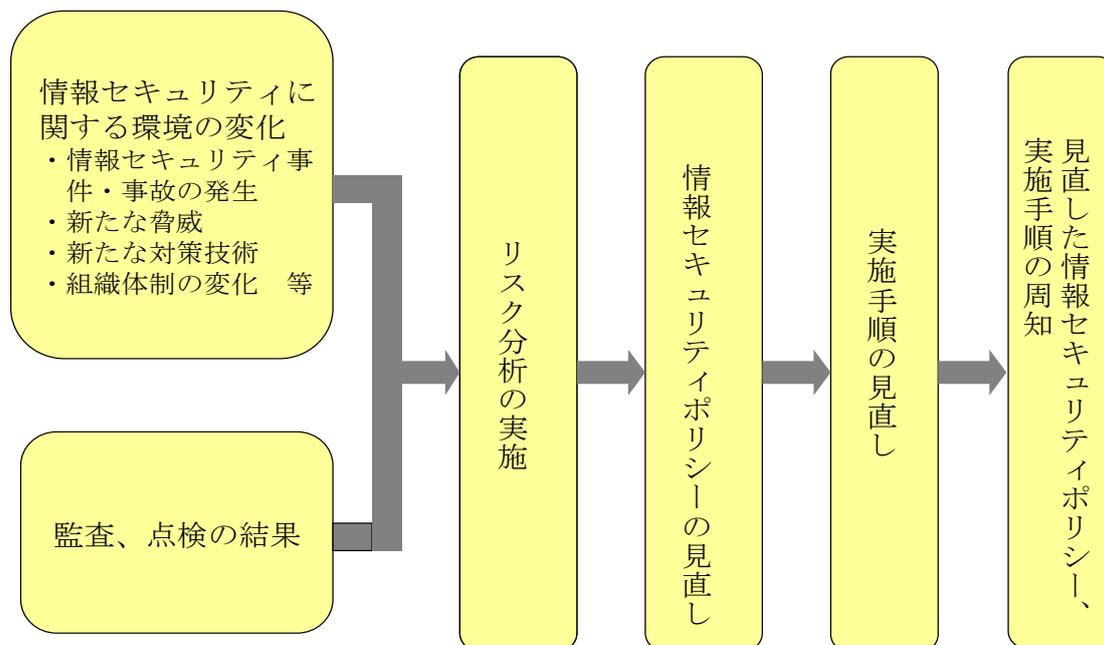
情報セキュリティポリシーの実効性を確保するとともに、情報資産や情報システム等の変化、情報セキュリティに関する脅威や対策等の変化に対応していくためには、情報セキュリティポリシーの評価・見直しを行い、前述のPDCAサイクル（1.5 情報セキュリティ対策の実施サイクル 参照）を繰り返し、情報セキュリティ対策を不断に強化し続けることが不可欠である。

1.8.1. 監査・自己点検

地方公共団体において情報セキュリティ対策の実効性を確保するには、情報セキュリティ対策の実施状況を検証し、情報セキュリティポリシーの見直しに反映させることが必要である。このため、独立かつ専門的知識を有する専門家（部内者であっても監査対象から独立した監査担当者等が行う場合を含む。）による検証である情報セキュリティ監査や情報システム等を運用する者自らによる検証である自己点検を行う。

1.8.2. 情報セキュリティポリシーの見直し

情報セキュリティポリシーの見直し作業は、情報セキュリティ委員会等の下で、情報セキュリティポリシーの策定手順（1.6 策定及び導入 参照）に準じて、図表8のとおり実施する。



図表8 情報セキュリティポリシーの見直しのプロセス

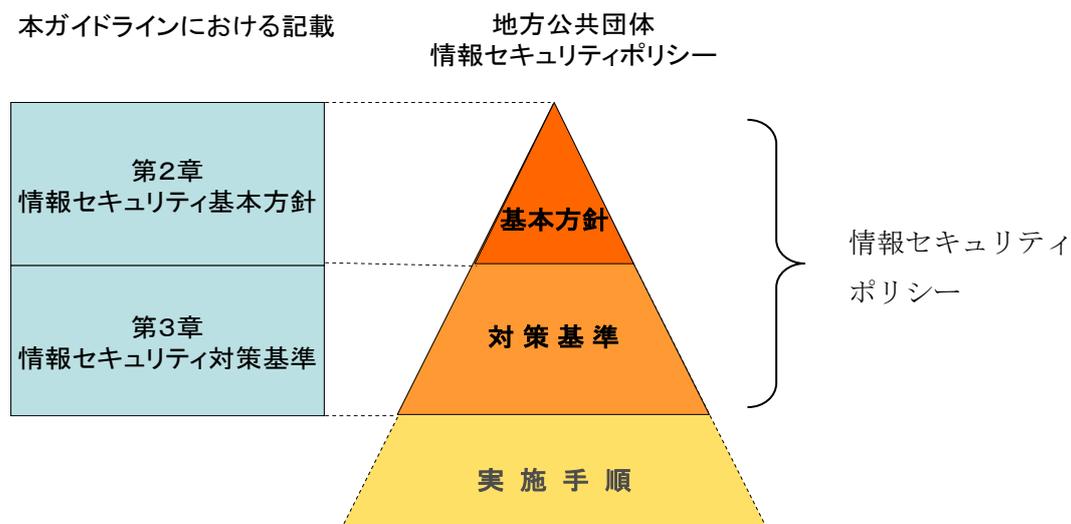
1.9.1. 本ガイドラインの構成

～ 1.9.2. 本ガイドラインにおける対策レベルの設定

1.9. 本ガイドラインの構成と対策レベルの設定

1.9.1. 本ガイドラインの構成

次章より、情報セキュリティポリシーの具体的な解説を扱うが、図表9のとおり、第2章が「情報セキュリティ基本方針」に関するガイドライン、第3章が「情報セキュリティ対策基準」に関するガイドラインとなっている。



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

1.9.2. 本ガイドラインにおける対策レベルの設定

地方公共団体において扱う情報資産の重要性や取り巻く脅威の大きさによって、必要とされる対策は一樣でないことから、本ガイドラインでは、特段の理由がない限り対策することが望まれる事項に加え、各地方公共団体において、その事項の必要性の有無を検討し、必要と認められる時に選択して実施することが望ましいと考えられる対策事項については、推奨事項として示している。

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

基本方針

2.1. 情報セキュリティ基本方針の目的

～ 2.2. 情報セキュリティ基本方針の形式

第2章 情報セキュリティ基本方針

2.1. 情報セキュリティ基本方針の目的

情報セキュリティ基本方針は、各地方公共団体における情報セキュリティ対策の基本となる事項を定めるとともに、地方公共団体が積極的に情報セキュリティ対策に取り組み、情報セキュリティの確保を図ることを住民に示すものである。

2.2. 情報セキュリティ基本方針の形式

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項目立てて規定する形式のものと、民間企業等で情報セキュリティ対策を明らかにする際に多く使われる宣言書形式のものがある。

(1) 基本的事項を規定する形式の構成

基本的事項を記載する形式の情報セキュリティ基本方針では、地方公共団体において情報セキュリティ対策に取り組む基本的事項として、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及び情報セキュリティ実施手順の策定等について規定する。

(2) 宣言書形式の構成

宣言書形式の情報セキュリティ基本方針は、地方公共団体の長又は最高情報統括責任者が、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ところに特色がある。

宣言書形式の情報セキュリティ基本方針では、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、職員等のセキュリティポリシー遵守義務等を規定している。地域全体の情報セキュリティ基盤の強化に積極的に貢献していくことを宣言に含めることも考えられる。

なお、宣言書形式の基本方針とする場合、情報セキュリティ対策基準に用語の定義、対象とする脅威、実施手順書の非公開に関する規定等を設ける必要がある。

2.3. 基本的事項を規定する形式

【例文】

情報セキュリティ基本方針

1 目的

本基本方針は、本市が保有する情報資産の機密性、完全性及び可用性を維持するため、本市が実施する情報セキュリティ対策について基本的な事項を定めることを目的とする。

2 定義

(1) ネットワーク

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

(2) 情報システム

コンピュータ、ネットワーク及び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。

3 対象とする脅威

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

(1) サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービ

2.3. 基本的事項を規定する形式

ス不能攻撃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な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提供サービスの障害からの波及等

4 適用範囲

(1) 行政機関の範囲

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

(2) 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

- ①ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体
- ②ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）
- ③情報システムの仕様書及びネットワーク図等のシステム関連文書

5 職員等の遵守義務

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

6 情報セキュリティ対策

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

(1) 組織体制

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

(2) 情報資産の分類と管理

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

(3) 物理的セキュリティ

サーバ等、情報システム室等、通信回線等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。

(4) 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。

(5) 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。

(6) 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、情報資産への侵害が発生した場合等に迅速かつ適切に対応するため、緊急時対応計画を策定する。

7 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

8 情報セキュリティポリシーの見直し

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

9 情報セキュリティ対策基準の策定

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

10 情報セキュリティ実施手順の策定

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

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

2.4. 宣言書の形式

【例文】

情報セキュリティ基本方針

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切に管理する。
- (4) 情報セキュリティ対策の重要性を認識させ、当該対策を適切に実施するために、職員等に対して必要な教育を実施する。
- (5) 情報セキュリティに関する事故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) すべての職員等は、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。

平成〇〇年〇〇月〇〇日

〇〇市長（又は、最高情報統括責任者）

对策基準

第3章 情報セキュリティ対策基準

3.1. 対象範囲

【趣旨】

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する。

【例文】

(1) 行政機関の範囲

本対策基準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

本対策基準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、情報システム、これらに関する設備、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)

(1) 行政機関の範囲

各地方公共団体の執行機関を基本に、情報セキュリティポリシーを適用させる範囲を決定する。

実際には、各団体の実情に応じ適用させる機関を決定することになるが、執行機関によって情報セキュリティ対策を進めて必要性に変わりはないことから、基本的にすべての執行機関を対象とすることが望ましい。

(2) 情報資産の範囲

例文において、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のとおりであるが、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切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、すべ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
ネットワーク	通信回線、ルータ等の通信機器
情報システム	サーバ、パソコン、汎用機、オペレーティングシステム、ソフトウェア等
これらに関する施設・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
電磁的記録媒体	CD-R、DVD-R、フロッピーディスク、MO、DLT (Digital Linear Tape) 、USB フラッシュメモリ等
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（これらを印刷した文書を含む。）
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

3.2. 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) 最高情報統括責任者

- ①副市長を、最高情報統括責任者とする。最高情報統括責任者は、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。
- ②最高情報統括責任者は、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アドバイザーとして置くものとする。【推奨事項】

(2) 統括情報セキュリティ責任者

- ①情報政策担当部長を、最高情報統括責任者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最高情報統括責任者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侵害が発生した場合又は侵害のおそれがある場合に、最高情報統括責任者の指示に従い、最高情報統括責任者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行う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、最高情報統括責任者、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整備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及び職員等（職員、非常勤職員及び臨時職員をいう。以下同じ。）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、情報資産に対する侵害が発生した場合又は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最高情報統括責任者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

3.2. 組織体制

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行うため、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監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

(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、情報セキュリティ対策に取り組むことを想定している。

(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と便利である。

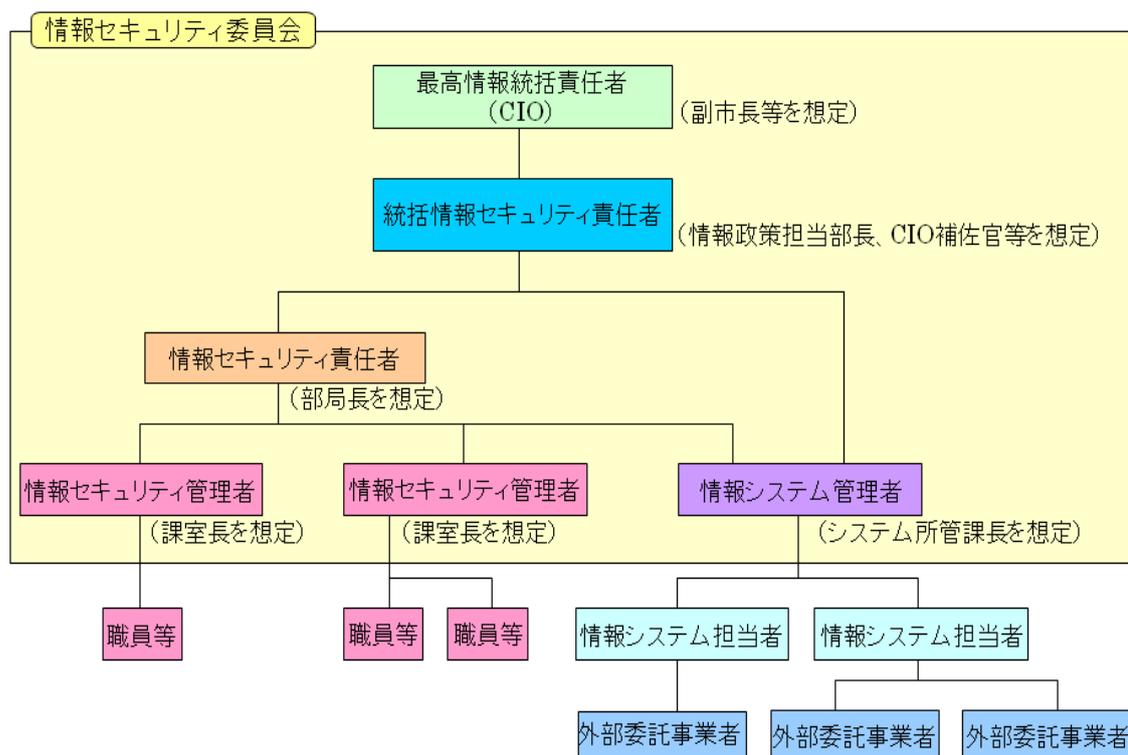
(1) 最高情報統括責任者

最高情報統括責任者は、地方公共団体におけるすべてのネットワーク、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。

(注 3) 最高情報統括責任者 (CIO: Chief Information Officer) 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充てることが望ましい。

(注 4) 例文では、最高情報統括責任者が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しているが、内部統制を徹底するという観点からは、情報セキュリティ対策が進んだ段階では、最高情報統括責任者とは別に最高情報セキュリティ責任者 (CISO: Chief Information Security Officer) を置くことが望ましい。

また、適切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、情報セキュリティに関する専門家をアドバイザーとして設置することが推奨される。



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充て、最高情報統括責任者の直属とすべきである。

(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。

最高情報統括責任者が不在の場合には、統括情報セキュリティ責任者がその権限を最高情報統括責任者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。

(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充てることが想定される。

(4) 情報セキュリティ管理者

3.2. 組織体制

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。

(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充てることが想定される。

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、情報資産に対する侵害又は侵害のおそれがある状況に直面する可能性が高い。このため、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最高情報統括責任者に対する報告義務を定める。

(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に関する権限及び責任を有する。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。

(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充てることが想定される。

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。

(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、見直し等の作業を行う。

(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、最高情報統括責任者、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最高情報統括責任者が構成員を招集し、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づ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に代替する者がいない場合などをいう。

3.3. 情報資産の分類と管理方法

【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	<ul style="list-style-type: none"> ・私物パソコンでの作業禁止（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
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	<ul style="list-style-type: none"> ・保管場所の制限、保管場所への必要以上の外部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 ・外部記録媒体の施錠可能な場所への保管
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	<ul style="list-style-type: none"> ・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 ・外部記録媒体の施錠可能な場所への保管
完全性 1	完全性 2 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	<ul style="list-style-type: none"> ・バックアップ、指定する時間以内の復旧 ・外部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）、格納する記録媒体（CD-R のラベル等）、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切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。

3.3. 情報資産の分類と管理方法

(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、適切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、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、情報資産を適切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外部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、利用頻度が低い外部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外部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の情報を記録した外部記録媒体を保管する場合は、耐火、耐熱、耐水及び耐湿を講じた施設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) 機密性 2 以上の情報資産を廃棄する者は、情報を記録している記録媒体が不要になった場合、記録媒体の初期化等、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、完全性及び可能性に基づき、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うる。

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。

3.3. 情報資産の分類と管理方法

- 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目録を作成することが望ましい。これにより、情報資産の所在、情報資産の分類、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すべ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。

3.4. 物理的セキュリティ

3.4.1. 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切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切に固定する等、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、当該機器が適切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

3.4.1. サーバ等の管理

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切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、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施さなければならない。

(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、記録媒体を内蔵する機器を外部の事業者修理させる場合、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、外部の業者に故障を修理させるに当たり、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他、秘密保持体制の確認などを行わなければならない。

(6) 敷地外への機器の設置

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、庁舎の敷地外にサーバ等の機器を設置する場合、最高情報統括責任者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、すべ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、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切であることを確認しなければならない。

(6) 敷地外への機器の設置

庁舎の敷地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なされているか、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、当該委託先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

3.4.1. サーバ等の管理

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

パソコンが不要になった場合やリース返却等を行う場合には、ハードディスクから情報を消去する必要がある。

(注5) 情報を消去する場合、オペレーティングシステム (OS) の機能による初期化だけでは、再度復元される可能性がある。データ消去ソフトウェア若しくはデータ消去装置の利用又は物理的な破壊若しくは磁気的な破壊などの方法を用いて、すべての情報を復元が困難な状態にし、情報が漏えいする可能性を低減しなければならない。

3.4.2. 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切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、当該機器等の管理並びに運用を行うための部屋（以下「情報システム室」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すべ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、機器等及び記録媒体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又は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

3.4.2. 管理区域（情報システム室等）の管理

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。【推奨事項】

- 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コンピュータ、通信回線装置、外部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。【推奨事項】

(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、湿度等の対策を施す必要がある。

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に、手動で扉を開閉できるように、自動扉開閉制御を解除するスイッチの場所を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、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。

(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、外部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。

3.4.2. 管理区域 (情報システム室等) の管理

(注3) 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4) 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ではなく、職員が行う必要がある。

3.4.3 通信回線及び通信回線装置の管理

3.4.3. 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切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、適切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切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、適切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。

（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。

（注1）図面管理を外部委託事業者に依頼する場合でも、当該委託先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。

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めることから、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、適切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る。

3.4.4. 職員等のパソコン等の管理

【趣旨】

職員等が利用するパソコン等の端末が適切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、職員等のパソコン等の盗難及び情報漏えい防止策、パソコン等の持ち出し・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、執務室等のパソコン等の端末について、盗難防止のため、ワイヤーによる固定等の物理的措置を講じなければならない。
- ②情報システム管理者は、情報システムへのログインパスワード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、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、パスワード以外に指紋認証等の生体認証を併用しなければならない。【推奨事項】
- ⑤情報システム管理者は、パソコン等の端末のディスク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。【推奨事項】

(解説)

執務室等からパソコン等が盗難され、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が盗難等に遭った場合でも、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。

①BIOS パスワード

パソコンを起動したときに、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。

②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。

③ログインパスワード

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。

3.4.4. 職員等のパソコン等の管理

④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。

⑤生体認証の併用

前述したパスワード機能に、生体認証である指紋認証等を併用することによって、よりセキュリティ機能は強化されることになる。

(注1) 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2) 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3) パソコン、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行うことがある。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。

3.5. 人的セキュリティ

3.5.1. 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うる。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、非常勤職員及び臨時職員、外部委託事業者についても、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、職員等の故意又は過失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パソコン等の端末の持ち出し及び外部における情報処理作業の制限

(ア) 最高情報統括責任者は、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、本市のパソコン等の端末、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。

(エ) 職員等は、外部で情報処理作業を行う際、私物パソコンを用いる場合には、情報セキュリティ管理者の許可を得た上で、安全管理措置を遵守しなければならない。また、機密性3の情報資産については、私物パソコンによる情報処理を行っ

3.5.1. 職員等の遵守事項

てはならない。

④パソコン等の端末等の持込

職員等は、私物のパソコン及び記録媒体を庁舎内に持ち込んで서는ならない。ただし、業務上必要な場合は、情報セキュリティ管理者の許可を得て、これらを持ち込むことができる。

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パソコン等の端末におけるセキュリティ設定変更の禁止

職員等は、パソコン等の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、パソコン等の端末や記録媒体、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、離席時の端末のロックや記録媒体、文書等の容易に閲覧されない場所への保管等、適切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にパソコン等の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が発注する場合、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、すべ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パソコン等の端末等の持ち出し

情報の漏えいは、不正なパソコンの持ち出しや移動中にパソコンが盗難に遭うなどしたことが原因で発生するケースが多い。重要な情報資産を使って外部で作業する場合には、庁舎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、パソコン等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切である。

(注1) パソコン等の持ち出しを許可した場合にも、パソコン等は常に携帯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。

また、自宅や庁外等の外部での情報処理作業において私物のパソコンを使うときには、特に情報漏えい等に留意する必要がある。したがって、私物パソコンの使用は許可制とし、機密性の高い情報資産については私物パソコンでの作業を禁止するのが適切である。

(注2) 私物パソコンの使用を許可する場合にも、私物パソコンにコンピュータウイルスチェックやファイル共有ソフトウェアの導入がされていないか確認させるなどの対策を講じる必要がある。共用しているパソコン、記録

3.5.1. 職員等の遵守事項

媒体は管理がずさんになりやすい傾向があることから、特に注意する。

(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をしないようにし、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) テレワークを導入する場合は、更なるセキュリティポリシー遵守の徹底や技術的対策の追加が必要となる。なお、テレワーク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2版）」（平成18年4月 総務省）を参照されたい。

②パソコン等の端末等の持ち込み

私物のパソコン、記録媒体を持ち込むことは原則として禁止し、無許可での行政情報等を記録、持ち出す行為を防止する必要がある。

③持ち出し及び持ち込みの記録

(注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、管理者の確認印等を設ける。

(注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、管理者の確認印等を設ける。

(2) 非常勤及び臨時職員への対応

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、パソコン等の端末の機能は、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切である。

(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、「3.7.4. 外部委託」を参照のこと。

3.5.2. 研修・訓練

【趣旨】

情報セキュリティを適切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すべ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事故の多くが、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、実際に事故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

最高情報統括責任者は、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) 研修計画の立案及び実施

①最高情報統括責任者は、幹部を含めすべ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を定期的に立案し、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行なければならない。

⑤最高情報統括責任者は、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

3.5.2. 研修・訓練

最高情報統括責任者は、緊急時対応を想定した訓練を定期的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

幹部を含めたすべての職員等は、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最高情報統括責任者であり、かつ、研修・訓練は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

最高情報統括責任者は、幹部を含めたすべての職員等が、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、すべ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事故等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、最高情報統括責任者に、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る義務を負わせておく。

また、最高情報統括責任者は、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。

(3) 緊急時対応訓練

実際に情報の漏えい等の事故が発生した場合に、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実施しなければならない。

(4) 研修・訓練への参加

幹部を含めたすべての職員に対し、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3) 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。

3.5.3. 事故、欠陥等の報告

3.5.3. 事故、欠陥等の報告

【趣旨】

情報セキュリティに関する事故や情報システム上の欠陥の発生の予防が重要なことはいうまでもないが、完全な予防は事実上困難であることから、実際に事故や欠陥が発生した場合に、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、情報セキュリティに関する事故、欠陥があっ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、「3.7.3. 侵害時の対応」による。

【例文】

(1) 庁内からの事故等の報告

- ①職員等は、情報セキュリティに関する事故、システム上の欠陥及び誤動作を発見した場合、速やかに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、報告のあった事故等について、必要に応じて最高情報統括責任者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) 住民等外部からの事故等の報告

- 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事故、欠陥について、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、当該事故等について、必要に応じて最高情報統括責任者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。
- ④最高情報統括責任者は、情報システム等の情報資産に関する事故、欠陥について、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) 事故等の分析・記録等

統括情報セキュリティ責任者は、事故等を引き起こした部門の情報セキュリティ管理者及び情報システム管理者と連携し、これらの事故等を分析し、記録を保存しなければならない。

(解説)

(1) 庁内からの事故等の報告

職員等は、情報セキュリティに関する事故やシステム上の欠陥を発見した場合に、自らの判断でその事故又は欠陥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。その事故又は欠陥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) 事故時の報告ルートは、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) 住民等外部からの事故等の報告

住民からの報告が契機となって、重大な事故や欠陥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ことが望ましい。

(注2) 住民からの報告に対しては、適切に処理し、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) 事故等の分析・記録等

事故等の原因を分析し、効果的な再発防止策を検討するために、事故等を引き起こした部門の情報セキュリティ管理者は、事故等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3) 他部門も含めて同様の事故等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、「3.7.3. 侵害時の対応 ④再発防止措置の策定」を参照されたい。

3.5.4. ID及びパスワード等の管理

3.5.4. 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）の管理が適切に行われなかった場合は、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、人的な原因で情報の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ー若しくはパソコン等の端末のスロット等から抜いておかななければならない。
 - (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パスワードは定期的に、又はアクセス回数に基づいて変更し、古いパスワードを再利用してはならない。
- ⑥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。
- ⑦仮のパスワードは、最初のログイン時点で変更しなければならない。
- ⑧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。
- ⑨職員等間でパスワードを共有してはならない。

(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。

(注1) 情報システム仕様書等は、機密性2又は3に指定して管理すべきである。

(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、大文字と小文字を組み合わせる、数字とアルファベットと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2) 複数のシステムを取扱う等により、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していれば、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。

3.6. 技術的セキュリティ

3.6.1. 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、アクセス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切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、適切に管理しなければならない。

(6) アクセス記録の取得等

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、各種アクセス記録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、アクセス記録等が詐取、改ざん、誤消去等されないように必要な措置を講じなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、システムから自動出力したアクセス記録等について、必要に応じ、外部記録媒体にバックアップしなければならない。【推奨事項】

(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、適切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、ネットワークに適切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

3.6.1. コンピュータ及びネットワークの管理

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、最高情報統括責任者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、庁内のすべてのネットワーク、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うえ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) 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づ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。【推奨事項】

(12) 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、委託先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しなければならない。【推奨事項】

(13) 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フリーメール、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。

(14) 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、最高情報統括責任者が定めた電子署名、暗号化又はパスワード設定の方法を使用して、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最高情報統括責任者が定める以外の方法を用いてはならない。また、最高情報統括責任者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。

(15) 無許可ソフトウェアの導入等の禁止

- ①職員等は、パソコン等の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。

3.6.1. コンピュータ及びネットワークの管理

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。

(16) 機器構成の変更の制限

- ①職員等は、パソコン等の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、パソコン等の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。

(17) 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等の端末をネットワークに接続してはならない。

(18) 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切な措置を求めなければならない。

(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他、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。

(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ない。

(注3) これを担保するため、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取ることが望ましい。

(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切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) アクセス記録の取得等

アクセス記録（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、改ざん、紛失等が生じないように保管する。

(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、障害記録を適切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切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、ネットワークに適切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

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、外部の人々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

3.6.1. コンピュータ及びネットワークの管理

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) この他、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。

(1 1) 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。

(注7) 暗号化方式の1つである WEP (Wired Equivalent Privacy) 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を採用しなければならない。

(注8) 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。

(1 2) 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。

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9) 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等もある。

(1 3) 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、フリー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、禁止する必要がある。

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10) HTML 形式の電子メールを使用禁止にする、メールソフトのプレビュー機能を使用しないことによってコンピュータウイルス感染の可能性の低減を

図ることができる。

(1 4) 電子署名・暗号化

暗号方法は、組織として特定の方法を定める。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、復号できなくなる可能性が高く、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ことがあるためである。

(1 5) 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等の端末に導入すると、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。

(注 1 1) 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える。

(1 6) 機器構成の変更の制限

職員等が、メモリー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。

(1 7) 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切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。

(注 1 2) 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無線 LAN カード等を持ち込み、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。

(1 8) 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アクセス記録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。

3.6.2. アクセス制御

3.6.2. 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、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。

【例文】

(1) アクセス制御

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、最高情報統括責任者が認めた者でなければならない。

(ウ) 最高情報統括責任者は、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。

(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パソコン等の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パソコン等の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及びログイン試行回数の制限、アクセスタイムアウトの設定、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。【推奨事項】

3.6.2. アクセス制御

(5) パスワードに関する情報の管理

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、職員等のパスワードに関する情報を厳重に管理しなければならない。パスワード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パスワード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、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。

(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（サーバのすべての機能を利用できる権限）等の特権は、すべ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。

(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、すべ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

(2) 職員等による外部からのアクセス等の制限

外部から社内ネットワーク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の暗号化等の必要な措置を取らなければならない。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。

(注3) 持ち込んだ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取られていないモバイル用のパソコンを庁内ネットワークに接続させないシステムである。モバイル用のパソコンを庁舎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低減することができる。

(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、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) パスワードに関する情報の管理

パスワードの機能は、ソフトウェアにより様々な機能があるために、これらの機能を有効に利用することが求められる。

(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、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。

3.6.3. システム開発、導入、保守等

3.6.3. 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行われない場合は、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。
- 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。【推奨事項】

(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し、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。

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。

(4) システム開発・保守に関連する資料等の保管

- 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文書を適切な方法で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切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

3.6.3. システム開発、導入、保守等

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扱う情報の重要性に応じて、システム運用及び利用面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、又は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) システム調達、開発、導入を行うに当たっては、最高情報統括責任者の許可を得て実施することが望ましい。

(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切な措置をとることが望まれる。

(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。

(注4) 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、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、適切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、できる限り分離することが必要である。

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保管

システム開発において、開発に関する資料等は、保守や機器更新の際に必要なことから、適切に保管することが必要である。

(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う、入力データの範囲チェックや不正な文字列等の入力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、システムの設計及びプログラムの設計を行う必要がある。

3.6.3. システム開発、導入、保守等

(注5) 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。

(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6) 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

3.6.4. 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行われていない場合は、システムの損傷、情報漏えい等の事故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。

(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。

3.6.4. 不正プログラム対策

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、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。

(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パソコン等の端末において、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。

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は、LAN ケーブルの即時取り外しを行わなければならない。

(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。【推奨事項】

(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他、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。

(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ですが、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記録媒体から感染することもありえるので、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、即座に LAN ケーブルを取り外し、被害の拡大を防がなければならない。

(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。

3.6.5. 不正アクセス対策

3.6.5. 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行われていない場合は、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、データの手書きを検出し、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。
- ③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】

(2) 攻撃の予告

最高情報統括責任者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ることが明確になった場合、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、関係機関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

最高情報統括責任者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、適切な処置を求めなければならない。

(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 ポートは、不正アクセスによる侵入が行われる可能性が高いために閉鎖する。

(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。

(2) 攻撃の予告

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とらなければならない。また、関係機関との連絡を密にし、情報収集に努めなければならない。

(注2) 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、その記録としてアクセスログ、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3) 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等の端末や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。

(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等の端末を利用し、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、適切な措置を求めなければならない。

3.6.6. セキュリティ情報の収集

3.6.6. 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事件、事故等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、共有及び対策の実施について規定する。

【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、セキュリティ侵害等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、積極的に情報収集を行う必要がある。
(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。
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を適用して行う。
(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。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。

(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。

(2) 不正プログラム等のセキュリティ情報の収集・周知

(注4) 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他に、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事件・事故や侵害等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行う必要がある。

(注5) 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、重要インフラ指針(第3版)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6) 暗号の危殆化については、「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」(平成 20 年 4 月 22 日 情報セキュリティ政策会議決定)、「電子政府推奨暗号リスト」(総務省及び経済産業省 平成 15 年 2 月 20 日)及び同リストを策定した CRYPTREC (Cryptography Research and Evaluation Committees) の今後の報告を参考とすることができる。

(注7) 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すべ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考慮する必要がある。

(注8) 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、適切な対策を実施する必要がある。

3.7. 運用

3.7.1. 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、重要なアクセス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。

(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（アクセスログ等）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。

(注) 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、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。

3.7.2. 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、速やかに最高情報統括責任者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。
- ②最高情報統括責任者は、発生した問題について、適切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切かつ速やかに対処しなければならない。

(2) 端末及び記録媒体等の利用状況調査

最高情報統括責任者及び最高情報統括責任者が指名した者は、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等の端末、記録媒体のアクセス記録、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場合と統括情報セキュリティ責任者が判断した場合は、緊急時対応計画に従って適切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、最高情報統括責任者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、情報セキュリティ事件・

3.7.2. 情報セキュリティポリシーの遵守状況の確認

事故の報告、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、アクセスログ等からの異常時の発見などがある。

(2) 端末及び記録媒体等の利用状況調査

職員等はパソコン等の端末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最高情報統括責任者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等の端末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、最高情報統括責任者又は最高情報統括責任者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切に対処する。

3.7.3. 侵害時の対応

【趣旨】

情報セキュリティに関する事故、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侵害事案が発生した場合に、迅速かつ適切に被害の拡大防止、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

最高情報統括責任者又は情報セキュリティ委員会は、情報セキュリティに関する事故、情報セキュリティポリシーの違反等により情報資産への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切に実施するために、緊急時対応計画を定めておき、侵害時には当該計画に従って適切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

本市が自然災害、大規模・広範囲にわたる疾病等に備えて業務継続計画を策定する場合、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

最高情報統括責任者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。

3.7.3. 侵害時の対応

緊急時対応計画には、情報資産への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に、配慮する必要がある。

(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
- ・ 最高情報統括責任者
- ・ 統括情報セキュリティ責任者
- ・ 情報システム管理者
- ・ 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）
- ・ 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、最高情報統括責任者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2) 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）等に相談する等、事実確認を見誤らないように努める必要がある。

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。

- ・サイバーテロその他の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、最高情報統括責任者、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
- ・不正アクセスその他犯罪と思慮されるとき
→地方公共団体の長、最高情報統括責任者、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、最高情報統括責任者、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
- ・その他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。

3.7.3. 侵害時の対応

- (オ) 事案に係るシステムのアクセス記録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、暫定措置を検討する。
- (ク) 暫定措置を講じた後、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（BCP: Business Continuity Plan）を策定する場合、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、適切な対応をとることができなくなるおそれがある。このため、各地方公共団体において業務継続計画を策定する場合には、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2）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3）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4）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）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。

3.7.4. 外部委託

【趣旨】

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委託先を選定し、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 ASP・SaaS 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行う必要があることに留意する。

【例文】

(1) 外部委託先の選定基準

- ①情報セキュリティ管理者は、外部委託先の選定に当たり、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、保守等を外部委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

- ・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
- 委託先の責任者、委託内容、作業員、作業場所の特定
- ・提供されるサービスレベルの保証
- ・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
- 市による事故時等の公表
- ・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）

3.7.4. 外部委託

(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必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、(2)の契約に基づき措置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最高情報統括責任者に報告しなければならない。

(解説)

(1) 外部委託先の選定基準

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。

(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。

また、外部委託事業者の選定に当たり、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。

(注2) 現在の最新の規格である ISO/IEC27001 については、財団法人日本情報処理開発協会のホームページ (ISMS 適合性評価制度) を参照されたい。

(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を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

外部委託先要員に対して、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。

②外部委託事業者の責任者、委託内容、作業員、作業場所の特定

外部委託事業者の責任者や作業員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きを定めておき、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。

⑤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。

⑥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。

⑦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、再委託先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、再委託先の業者における情報セキュリティ対策が十分取られており、外部委託事業者と同等の水準であることを確認した上で許可しなければならない。

⑧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下げる。

⑨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切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。

⑩市による監査、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、検査によって確認する。

⑪市による事故時等の公表

委託業務に関し、情報セキュリティに関する事件・事故等が発生した場合、住民に対し適切な説明責任を果たすため、当該事故等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。

⑫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上明記しておく。

(注3) 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

3.7.4. 外部委託

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 4）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 5）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 6）ASP・SaaS サービスの利用に関する考慮事項

インターネットを介してサービスを提供する ASP・SaaS の利用に当たっては、ASP・SaaS 事業者の事業所の場所にかかわらず、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、ASP・SaaS 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ことに留意が必要である。

なお、ASP・SaaS サービスの利用に当たっては、契約の形態が従前の委託や請負と異なることが想定されることから、「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。

（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なされているか、定期的に確認し、必要に応じ、改善要求等の措置を取る必要がある。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侵害行為が発見された場合には、速やかに最高情報統括責任者に報告を行う。

なお、外部委託先事業者に対する監査については、本ガイドラインの「3.8.1 監査

（4）外部委託事業者に対する監査」を参照されたい。

3.7.5. 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し、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、最高情報統括責任者の許可を得て、例外措置を取ることができる。

(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、事後速やかに最高情報統括責任者に報告しなければならない。

(3) 例外措置の申請書の管理

最高情報統括責任者は、例外措置の申請書及び審査結果を適切に保管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き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。

例外措置についての手続きを定め、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) 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。

3.7.6. 法令遵守

3.7.6. 法令遵守

【趣旨】

職員等は、すべ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）
- ⑤〇〇市個人情報保護条例（平成〇〇年条例第〇〇号）

（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。

3.7.7. 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きについて規定する。

【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、適切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、適切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最高情報統括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なければならない。

3.8.1. 監査

3.8. 評価・見直し

3.8.1. 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

情報セキュリティ委員会は、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切に保管しなければならない。

(7) 監査結果への対応

最高情報統括責任者は、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。

(8) 情報セキュリティポリシー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自治体との相互監査も有効である。

(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

3.8.1. 監査

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うることから、誤用・悪用を防止するための適切な管理が求められる。

(注2) 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事件・事故等から学んだ対策等の遵守状況の確認や、外部記録媒体の管理、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切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、情報セキュリティ侵害の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、監査調書を基に、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。

最高情報統括責任者は、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

監査結果を適切にセキュリティ改善に結びつけるため、最高情報統括責任者に関係部局への指示を義務づけた規定である。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可能性があることから、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3) 情報セキュリティ監査の実施方法等については、総務省が平成 15 年 12 月に策定した「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」及び平成 17 年 2 月に策定した「地方公共団体情報セキュリティ管理基準解説書」を参考にされたい。

3.8.2. 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。

3.8.2. 自己点検

(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うる。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。

(2) 報告

自己点検結果を情報セキュリティ委員会に報告し、団体全体における対策の状況を把握することが必要である。

(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2) 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。

3.8.3. 情報セキュリティポリシーの見直し

【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、情報セキュリティポリシーについて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ふまえ、毎年度評価を行い、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、情報セキュリティ事件・事故、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等を活用しつつ、情報セキュリティポリシーの見直しを行う。

また、情報セキュリティポリシーは、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、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を見直した際には、その内容を職員等や外部委託事業者十分に周知する必要がある。

参考

○情報セキュリティ対策基準の例文

○権限・責任等一覧表

情報セキュリティ 対策基準の例文

情報セキュリティ対策基準の例文

3.1. 対象範囲

(1) 行政機関の範囲

本対策基準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

本対策基準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、情報システム、これらに関する設備、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

3.2. 組織体制

(1) 最高情報統括責任者

- ①副市長を、最高情報統括責任者とする。最高情報統括責任者は、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。
- ②最高情報統括責任者は、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アドバイザーとして置くものとする。【推奨事項】

(2) 統括情報セキュリティ責任者

- ①情報政策担当部長を、最高情報統括責任者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最高情報統括責任者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侵害が発生した場合又は侵害のおそれがある場合に、最高情報統括責任者の指示に従い、最高情報統括責任者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行う権限及び責任

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、最高情報統括責任者、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整備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及び職員等（職員、非常勤職員及び臨時職員をいう。以下同じ。）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、情報資産に対する侵害が発生した場合又は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最高情報統括責任者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行うため、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監査を受ける者とその監査を実施する者は、やむを得ない場合を除き、同じ者が兼務してはならない。

3.3. 情報資産の分類と管理方法

(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	<ul style="list-style-type: none"> ・私物パソコンでの作業禁止（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
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	<ul style="list-style-type: none"> ・保管場所の制限、保管場所への必要以上の外部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 ・外部記録媒体の施錠可能な場所への保管
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	<ul style="list-style-type: none"> ・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 ・外部記録媒体の施錠可能な場所への保管
完全性1	完全性2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	<ul style="list-style-type: none"> ・ バックアップ、指定する時間以内の復旧 ・ 外部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）、格納する記録媒体（CD-R のラベル等）、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切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、適切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、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、情報資産を適切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外部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、利用頻度が低い外部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外部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の情報を記録した外部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) 機密性 2 以上の情報資産を廃棄する者は、情報を記録している記録媒体が不要になった場合、記録媒体の初期化等、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。

3.4. 物理的セキュリティ

3.4.1. サーバ等の管理

(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切に固定する等、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

適切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切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、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施さなければならない。

(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、記録媒体を内蔵する機器を外部の事業者修理させる場合、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、外部の業者に故障を修理させるに当たり、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他、秘密保持体制の確認などを行わなければならない。

(6) 敷地外への機器の設置

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、庁舎の敷地外にサーバ等の機器を設置する場合、最高情報統括責任者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、すべ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。

3.4.2. 管理区域（情報システム室等）の管理

（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、当該機器等の管理並びに運用を行うための部屋（以下「情報システム室」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すべ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、機器等及び記録媒体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又は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。【推奨事項】
- 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コンピュータ、通信回線装置、外部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。【推奨事項】

(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、職員を立ち合わせなければならない。

3.4.3. 通信回線及び通信回線装置の管理

- 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、適切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切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、適切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。

3.4.4. 職員等のパソコン等の管理

- ①情報システム管理者は、執務室等のパソコン等の端末について、盗難防止のため、ワイヤーによる固定等の物理的措置を講じなければならない。
- ②情報システム管理者は、情報システムへのログインパスワード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、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、パスワード以外に指紋認証等の生体認証を併用しなければならない。【推奨事項】
- ⑤情報システム管理者は、パソコン等の端末のディスク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。【推奨事項】

3.5. 人的セキュリティ

3.5.1. 職員等の遵守事項

(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パソコン等の端末の持ち出し及び外部における情報処理作業の制限

(ア) 最高情報統括責任者は、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、本市のパソコン等の端末、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。

(エ) 職員等は、外部で情報処理作業を行う際、私物パソコンを用いる場合には、情報セキュリティ管理者の許可を得た上で、安全管理措置を遵守しなければならない。また、機密性3の情報資産については、私物パソコンによる情報処理を行ってはならない。

④パソコン等の端末等の持込

職員等は、私物のパソコン及び記録媒体を庁舎内に持ち込んで서는ならない。ただし、業務上必要な場合は、情報セキュリティ管理者の許可を得て、これらを持ち込むことができる。

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パソコン等の端末におけるセキュリティ設定変更の禁止

職員等は、パソコン等の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、パソコン等の端末や記録媒体、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、離席時の端末のロックや記録媒体、文書等の容易に閲覧されない場所への保管等、適切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にパソコン等の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。

3.5.2. 研修・訓練

(1) 情報セキュリティに関する研修・訓練

最高情報統括責任者は、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) 研修計画の立案及び実施

①最高情報統括責任者は、幹部を含めすべ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を定期的に立案し、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行なければならない。

⑤最高情報統括責任者は、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

最高情報統括責任者は、緊急時対応を想定した訓練を定期的に行なければならない。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

幹部を含めたすべての職員等は、定められた研修・訓練に参加しなければならない。

3.5.3. 事故、欠陥等の報告

(1) 庁内からの事故等の報告

①職員等は、情報セキュリティに関する事故、システム上の欠陥及び誤動作を発見した場合、速やかに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、報告のあった事故等について、必要に応じて最高情報統括責任者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) 住民等外部からの事故等の報告

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事故、欠陥について、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、当該事故等について、必要に応じて最高情報統括責任者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。

④最高情報統括責任者は、情報システム等の情報資産に関する事故、欠陥について、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) 事故等の分析・記録等

統括情報セキュリティ責任者は、事故等を引き起こした部門の情報セキュリティ管理者及び情報システム管理者と連携し、これらの事故等を分析し、記録を保存しなければならない。

3.5.4. ID 及びパスワード等の管理

(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ー若しくはパソコン等の端末のスロット等から抜いておかななければならない。

(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パスワードは定期的に、又はアクセス回数に基づいて変更し、古いパスワードを再利用してはならない。
- ⑥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。
- ⑦仮のパスワードは、最初のログイン時点で変更しなければならない。
- ⑧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。
- ⑨職員等間でパスワードを共有してはならない。

3.6. 技術的セキュリティ

3.6.1. コンピュータ及びネットワークの管理

(1) 文書サーバの設定等

- ①情報システム管理者は、職員等が利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切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、適切に管理しなければならない。

(6) アクセス記録の取得等

- 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、各種アクセス記録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、アクセス記録等が詐取、改ざん、誤消去等されないように必要な措置を講じなければならない。
- ③統括情報セキュリティ責任者及び情報システム管理者は、システムから自動出力したアクセス記録等について、必要に応じ、外部記録媒体にバックアップしなければならない。【推奨事項】

(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、適切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、ネットワークに適切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、最高情報統括責任者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、庁内のすべてのネットワーク、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うえ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) 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づ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。【推奨事項】

(1 2) 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、委託先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しなければならない。【推奨事項】

(1 3) 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フリーメール、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。

(1 4) 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、最高情報統括責任者が定めた電子署名、暗号化又はパスワード設定の方法を使用して、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最高情報統括責任者が定める以外の方法を用いてはならない。また、最高情報統括責任者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。

(15) 無許可ソフトウェアの導入等の禁止

- ①職員等は、パソコン等の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。

(16) 機器構成の変更の制限

- ①職員等は、パソコン等の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、パソコン等の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。

(17) 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等の端末をネットワークに接続してはならない。

(18) 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切な措置を求めなければならない。

3.6.2. アクセス制御

(1) アクセス制御

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、最高情報統括責任者が認めた者でなければならない。

(ウ) 最高情報統括責任者は、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。

(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パソコン等の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パソコン等の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及びログイン試行回数の制限、アクセスタイムアウトの設定、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。【推奨事項】

(5) パスワードに関する情報の管理

- 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、職員等のパスワードに関する情報を厳重に管理しなければならない。パスワード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パスワード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、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。

(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。

3.6.3. システム開発、導入、保守等

(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。

②システム開発における責任者、作業者のIDの管理

①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。

②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。【推奨事項】

(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し、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。

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。

(4) システム開発・保守に関連する資料等の保管

- 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文書を適切な方法で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切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。

3.6.4. 不正プログラム対策

(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。

(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、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。

(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パソコン等の端末において、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の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。
- 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は、LAN ケーブルの即時取り外しを行わなければならない。

(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。【推奨事項】

3.6.5. 不正アクセス対策

(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。
- ③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】

(2) 攻撃の予告

最高情報統括責任者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ることが明確になった場合、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、関係機関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

最高情報統括責任者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、適切な処置を求めなければならない。

3.6.6. セキュリティ情報の収集

(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、セキュリティ侵害等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。

3.7. 運用

3.7.1. 情報システムの監視

- ①統括情報セキュリティ責任者及び情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない。
- 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、重要なアクセス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。

3.7.2. 情報セキュリティポリシーの遵守状況の確認

(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、速やかに最高情報統括責任者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。
- ②最高情報統括責任者は、発生した問題について、適切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切かつ速やかに対処しなければならない。

(2) 端末及び記録媒体等の利用状況調査

最高情報統括責任者及び最高情報統括責任者が指名した者は、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等の端末、記録媒体のアクセス記録、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場合と統括情報セキュリティ責任者が判断した場合は、緊急時対応計画に従って適切に対処しなければならない。

3.7.3 侵害時の対応

(1) 緊急時対応計画の策定

最高情報統括責任者又は情報セキュリティ委員会は、情報セキュリティに関する事故、情報セキュリティポリシーの違反等により情報資産への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切に実施するために、緊急時対応計画を定めておき、侵害時には当該計画に従って適切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

本市が自然災害、大規模・広範囲にわたる疾病等に備えて業務継続計画を策定する場合、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

最高情報統括責任者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しなければならない。

3.7.4. 外部委託

(1) 外部委託先の選定基準

①情報セキュリティ管理者は、外部委託先の選定に当たり、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、保守等を外部委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

- ・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
- ・委託先の責任者、委託内容、作業員、作業場所の特定
- ・提供されるサービスレベルの保証
- ・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
- ・市による事故時等の公表
- ・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必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、(2)の契約に基づき措置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最高情報統括責任者に報告しなければならない。

3.7.5. 例外措置

(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し、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、最高情報統括責任者の許可を得て、例外措置を取ることができる。

(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、事後速やかに最高情報統括責任者に報告しなければならない。

(3) 例外措置の申請書の管理

最高情報統括責任者は、例外措置の申請書及び審査結果を適切に保管しなければならない。

3.7.6. 法令遵守

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(昭和二十五年十二月十三日法律第二百六十一号)
- ②著作権法(昭和四十五年法律第四十八号)
- ③不正アクセス行為の禁止等に関する法律(平成十一年法律第二百二十八号)
- ④個人情報の保護に関する法律(平成十五年五月三十日法律第五十七号)
- ⑤〇〇市個人情報保護条例(平成〇〇年条例第〇〇号)

3.7.7. 懲戒処分等

(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、適切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、適切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最高情報統括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なければならない。

3.8. 評価・見直し

3.8.1. 監査

(1) 実施方法

情報セキュリティ委員会は、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切に保管しなければならない。

(7) 監査結果への対応

最高情報統括責任者は、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。

(8) 情報セキュリティポリシー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。

3.8.2. 自己点検

(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。

3.8.3. 情報セキュリティポリシーの見直し

情報セキュリティ委員会は、情報セキュリティポリシーについて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ふまえ、毎年度評価を行い、必要があると認めた場合、改善を行うものとする。

權限・責任等一覽表

権限・責任等一覧表

※本一覧表は「第3章 情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分 (対策基準の例文の規定箇所)		項目	情報セキュリティ	最高情報統括責任者	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	情報セキュリティ監査責任者	職員等の義務	関係規定 外部委託		
3.1 対象範囲		適用される行政機関等の定義												
3.2 組織体制	(1)	①	最高情報統括責任者の設置		○									
		②	アドバイザーの設置		○									
	(2)	①	統括情報セキュリティ責任者の設置		△	○								
		②	ネットワークにおける開発等の権限及び責任			○								
		③	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			○								
		④	情報セキュリティ責任者等に対する指導及び助言			○	△	△	△	△				
		⑤	情報資産に対する侵害が発生した場合等の権限及び責任		△	○								
		⑥	情報セキュリティ実施手順の維持・管理の権限及び責任			○								
		⑦	最高情報統括責任者等との連絡体制の整備		△	○	△	△	△	△				
	(3)	①	情報セキュリティ責任者の設置				○							
		②	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				○							
		③	部局等の情報システムの開発等の統括的な権限及び責任				○							
		④	部局等の情報システムにおける連絡体制の整備等				○							
	(4)	①	情報セキュリティ管理者の設置					○						
		②	課室等の情報セキュリティ対策に関する権限及び責任					○						
		③	情報資産に対する侵害が発生した場合等の報告等		△	△	△	○						
	(5)	①	情報システム管理者の設置						○					
		②	情報システムにおける開発等の権限及び責任						○					
		③	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						○					
		④	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						○					
	(6)		情報システム担当者の設置						△	○				
	(7)	①	情報セキュリティ委員会の設置	○										
		②	情報セキュリティ対策の改善計画の策定、実施状況の確認	○										
	(8)	①	情報セキュリティ対策の実施における承認等の申請者とその承認者等の兼務の禁止											
		②	監査を受ける者と監査を実施する者の兼務の禁止											
	3.3 情報資産 の分類と 管理方法	(1)		情報資産の分類										
		(2)	①	(ア) 情報資産の管理責任					○					
			(イ) 複製等された情報資産の管理責任						○					
②			情報資産の分類の表示									○		
③		(ア)	業務上必要のない情報の作成の禁止										○	
		(イ)	情報作成時の情報の分類と取扱制限の設定										○	
		(ウ)	作成途上の情報の取扱										○	
④		(ア)	庁内の者が作成した情報資産の取扱い										○	
		(イ)	庁外の者が作成した情報資産の分類と取扱い										○	
		(ウ)	分類が不明な情報資産を入手した際の対応						△				○	
⑤		(ア)	情報資産の業務外目的の利用の禁止										○	
		(イ)	情報資産の分類に応じた適切な取扱い										○	
		(ウ)	情報資産の分類が異なる記録媒体の取扱い										○	

権限・責任等一覧表

※本一覧表は「第3章 情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分 (対策基準の例文の規定箇所)		項目		情報セキュリティ	最高情報統括責任者	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	情報セキュリティ監査責任者	職員等の義務	外部委託	関係規定		
		⑥	(ア) 情報資産の分類に応じた適切な保管					○	○							
			(イ) 長期保管する情報資産を記録した外部記録媒体の保管					○	○							
			(ウ) 利用頻度の低い外部記録媒体等の保管					○	○							
			(エ) 外部記録媒体の施錠可能な場所への保管					○	○							
		⑦	電子メール等での送信時の対策											○		
			⑧	(ア) 車両等での情報資産運搬時の対策											○	
		(イ) 情報資産運搬の許可							許					○		
		⑨	(ア) 情報資産の外部への提供時の対策												○	
			(イ) 情報資産の外部への提供の許可						許						○	
			(ウ) 住民に公開する情報資産の取扱い						○							
		⑩	(ア) 情報資産廃棄時の対策												○	
			(イ) 情報資産廃棄時の処理の記録												○	
			(ウ) 情報資産廃棄の許可							許					○	
		3.4 物理的セキュリティ	3.4.1 サーバ等の管理	(1)	サーバ等取付け時の必要な措置						○					
(2)	① サーバの冗長化								○							
	② システム運用停止時間の最小化									○						
(3)	① 予備電源の設置						△			○						
	② 過電流に対する機器の保護措置						△			○						
(4)	① 通信ケーブル等の損傷防止措置						○			○						
	② 通信ケーブル等の損傷等時の対応						○			○						
	③ ネットワーク接続口の管理						○			○						
	④ 配線の変更・追加の防止措置						○			○	△					
(5)	① 機器の定期保守の実施									○						
	② 修理時における外部事業者からの情報漏えい防止措置									○						△
(6)	敷地外への機器の設置					承	○		○							
(7)	機器の廃棄等の措置								○							
	3.4.2 管理区域(情報システム室等)の管理			(1)	① 管理区域の定義											
		② 管理区域の構造					○		○							
		③ 管理区域への立入制限等					○		○							
		④ 耐震対策等の対策					○		○							
		⑤ 外壁等の床下開口部における措置					○		○							
		⑥ 消化薬剤等の設置方法					○		○							
		(2)	① 入退室管理方法							○				○	○	
			② 入室時の身分証明書等の携帯及び提示											○	○	
			③ 外部からの訪問者に対する入室管理							○				△		
			④ 情報システムに関連しないコンピュータ等の持ち込み禁止							○						
		(3)	① 搬入する機器の既存情報システムへの影響確認							○				△	△	
			② 機器等の搬入時の職員の立ち会い							○				△		

権限・責任等一覧表

※本一覧表は「第3章 情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分 (対策基準の例文の規定箇所)		項目	情報セキュリティ	最高情報統括責任者	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	情報セキュリティ監査責任者	職員等の義務	関係規定 外部委託		
3. 4. 3 通信回線及び通信回線装置の管理	①	庁内の通信回線等の適切な管理等			○									
		外部へのネットワーク接続の限定措置			○									
		行政系ネットワークのLGWANへの集約			○									
		通信回線に利用する回線の選択等			○									
		回線の十分なセキュリティ対策の実施			○									
	3. 4. 4 職員等のパソコン等の管理	①	ノートパソコン等の盗難防止措置						○					
			情報システムへのログインパスワードの設定					○						
			BIOS/パスワード設定等措置					○						
			生体認証等措置の併用措置					○						
			ディスクデータの暗号化等の利用					○						
3. 5 人的セキュリティ	3. 5. 1 職員等の遵守事項	(1) ①	情報セキュリティポリシー等の遵守					△				○		
			情報資産の業務目的以外での使用の禁止										○	
		③	(ア) 情報資産の外部での処理時の安全管理措置		○									
			(イ) 端末等の持ち出しの許可					許						○
			(ウ) 外部での情報処理業務の許可					許						○
			(エ) 外部での私物パソコン使用時の安全管理措置等					許						○
			④ 私物パソコンの庁舎内への持込禁止等					許						○
		⑤ 端末等の持出及び持込の記録等					○							
		⑥ パソコン等のセキュリティ設定変更の禁止					許						○	
		⑦ 机上の端末等の管理					許						○	
		⑧ 退職時等の遵守事項											○	
		(2) ①	非常勤職員等の採用時の対応						○					△
			非常勤職員等の採用時の同意書への署名						○					△
	インターネット接続等の利用の制限							○					△	
	(3)	情報セキュリティポリシー等の掲示					○						△	
	(4)	外部委託事業者に対する説明					○						△	
	3. 5. 2 研修・訓練	(1)	情報セキュリティに関する研修・訓練の実施		○									
			(2) ① 研修計画の立案等		承	○								
		②	情報セキュリティ研修の受講											○
			新規採用の職員等に対する研修の設定			○								△
			理解度等に応じた研修の実施			○	△	△	△	△	△			△
			研修の受講状況の報告		△	○								
			(3)	緊急時対応訓練の実施			○							
		(4)	研修・訓練の参加義務											○
		3. 5. 3 事故、欠陥等の報告	(1) ①	事故等の報告						△				
	情報システムに関連する事故等の報告						△		○	△				
	事故等の必要に応じた報告					△		△	○					
	(2) ①		住民等外部からの報告時の対応						△					
情報システム又はネットワークに関連する事故等の報告						△		○	△					
事故等の必要に応じた報告					△		△	○						
住民等外部に対する窓口の設置等					○									
(3)	事故等の分析・記録等				○			△	△					

権限・責任等一覧表

※本一覧表は「第3章 情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分 (対策基準の例文の規定箇所)		項目		情報セキュリティ	最高情報統括責任者	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	情報セキュリティ監査責任者	職員等の義務	関係規定 外部委託	
3.5.4 ID及びパスワード等の管理	(1) ①	(ア)	認証に用いるICカード等の職員等間共有の禁止									○		
		(イ)	ICカード等のカードリーダーへの常時挿入禁止										○	
		(ウ)	ICカード等紛失時の通報			△			△					○
	(1) ②		ICカード紛失時のアクセス停止措置			○				○				
		(1) ③		ICカード切り替え時の旧カードの廃棄方法			○			○				
				自己のIDの他人による利用の禁止										
	(3) ①		パスワードの管理											○
			パスワードの秘密保持											○
			パスワードの文字の選択											○
			パスワードの流出したおそれのある時の措置						△					○
			パスワードの定期的な更新											○
			パスワードのシステム間の共有禁止											○
			仮パスワードの変更											○
			パスワードの記憶機能の利用禁止											○
			職員等間でのパスワード共有禁止											○
		3.6 技術的セキュリティ	(1) ①		文書サーバの容量の設定等						○			
				文書サーバの課室等单位での設定						○				
				特定の情報のためのディレクトリ設定						○				
(2)			バックアップの実施			○			○					
			他団体との情報システムに関する情報等の交換の許可等				許	許		○				
(4) ①			情報システムの運用に係る作業記録の作成						○					
			システム変更等時の作業内容記録作成等			○			○					
			システム変更の作業方法			○			○	○				○
(5)			ネットワーク構成図等の保管			○			○					
	(6) ①			アクセス記録等の取得等			○			○				
				アクセス記録等の管理			○			○				
			アクセス記録等のバックアップ			○			○					
(7)			システム障害等の記録、保存			○			○					
	(8) ①			通信ソフトウェア等の設定情報の管理			○							
			ネットワークのアクセス制御			○								
(9)			外部の者が利用できるシステムの分離等							○				
	(10) ①			ネットワークの外部接続の許可			許	許		○				
				外部ネットワークの接続による影響確認						○				
				外部ネットワーク管理責任者による損害賠償責任の契約上の担保						○				
				ファイアウォール等の設置			○			○				
			問題発生時の物理的な遮断			△			○					
	(11) ①		無線LAN利用時の暗号化等の使用義務設定			○								
		機密性の高いネットワークへの暗号化等の措置			○									

権限・責任等一覧表

※本一覧表は「第3章 情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分 (対策基準の例文の規定箇所)	項目	情報セキュリティ	最高情報統括責任者	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	ティイ監査責任者	職員等の義務	関係規定 外部委託		
		情報セキュリティ	最高情報統括責任者	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	ティイ監査責任者	職員等の義務	関係規定 外部委託		
	(12)	① 電子メールの中継処理禁止の設定			○								
		② スпамメール等を検知した際のサーバ運用停止			○								
		③ 電子メールの送受信容量の上限設定等			○								
		④ 電子メールボックスの容量の上限設定等			○								
		⑤ 外部委託事業者の電子メールアドレス利用取り決め			○							○	
		⑥ 添付ファイルの監視等			○								
	(13)	① 自動転送機能の禁止										○	
		② 業務上必要のない送信先への送信禁止										○	
		③ 複数人に電子メールを送信する際の方法										○	
		④ 重要メールの誤送信時の報告					△					○	
		⑤ ウェブ上のフリーメール等の使用禁止										○	
	(14)	① 電子署名、暗号化等による送信		○								○	
		② 暗号化の方法及び鍵の管理		○								○	
	(15)	① ソフトウェアの無断導入の禁止										○	
		② ソフトウェアの導入の許可の取得				許		許				○	
		③ 不正コピーしたソフトウェアの利用禁止										○	
	(16)	① 機器の改造及び増設・交換の禁止										○	
		② 機器の改造等の許可				許		許				○	
	(17)	無許可でのネットワーク接続の禁止				許						○	
	(18)	① 業務目的外のウェブ閲覧の禁止										○	
		② 業務目的外のウェブ閲覧発見時の対応				○		△					
	3. 6. 2 アクセス 制御	(1)	① アクセス制御			○			○				
			② (ア) 利用者の情報管理やIDの取扱い等の設定	(イ) 利用者登録抹消の申請			△			△			○
				(ウ) 利用されるIDの点検			○			○			
③ (ア) ID及びパスワードの管理						○			○				
(イ) 統括情報セキュリティ責任者等の特権を代行する者の要件				○	○			○					
(ウ) 特権代行者の通知				○	△	△	△	△					
(エ) 特権付与されたID等の変更の外部事業者への委託禁止					○			○			○		
(オ) 特権付与されたID等のセキュリティ機能強化					○			○					
(2)		① 外部から内部ネットワーク等へのアクセスの許可				許			許			○	
		② 外部からのアクセス可能人数の制限				○							
		③ 外部からのアクセス時の本人確認の機能の確保				○							
		④ 外部からのアクセス時の暗号化等の措置				○							
		⑤ 外部アクセス用端末等付与時のセキュリティの確保				○			○				
		⑥ 外部から持ち込んだ端末等のウイルスの確認等										○	
(3)		自動識別の設定				○			○				
(4)		ログイン時のシステム設定							○				
(5)		① 職員等のパスワード情報の管理等				○			○				
		② パスワード発行等				○			○				
(6)		特権によるネットワーク等への接続時間の制限							○				

権限・責任等一覧表

※本一覧表は「第3章 情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分 (対策基準の例文の規定箇所)		項目		情報セキュリティ	最高情報統括責任者	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	情報セキュリティ監査責任者	職員等の義務	関係規定 外部委託		
3. 6. 3 システム開発、導入、保守等	(1)	①	調達仕様書への技術的なセキュリティ機能の明記			○			○						
		②	調達時のセキュリティ機能の調査等			○			○						
	(2)	①	システム開発の責任者及び作業者の特定							○					
		②	(ア)	システム開発の責任者等のIDの管理等						○					
			(イ)	システム開発の責任者等のアクセス権限の設定						○					
		③	(ア)	システム開発におけるソフトウェア等の特定						○					
			(イ)	認定外のソフトウェアの削除						○					
		(3)	①	(ア)	システム開発等環境とシステム運用環境の分離						○				
	(イ)			システム開発環境からシステム運用環境への移行の手順の明確化						○					
	(ウ)			移行に伴うシステム停止等の影響の最小化						○					
	②		(ア)	新たなシステム導入前の十分な試験の実施						○					
			(イ)	運用テスト時の擬似環境による操作確認の実施						○					
			(ウ)	テストデータとして個人情報等の使用禁止						○					
	(4)	①	システム開発等の資料等の保管						○						
		②	テスト結果の保管						○						
		③	情報システムに係るソースコードの保管						○						
	(5)	①	入力データの正確性を確保できる情報システム設計						○						
		②	情報の改ざん等を検出する情報システム設計						○						
		③	出力データの正確性を確保できる情報システム設計						○						
	(6)		プログラム仕様書等の変更履歴の作成						○						
	(7)		ソフトウェア更新等時の他の情報システムとの整合性確認						○						
	(8)		システム更新又は統合時の検証等の実施						○						
	3. 6. 4 不正プログラム対策	(1)	①	不正プログラムのシステムへの侵入防止措置			○								
			②	不正プログラムの外部への拡散防止措置			○								
			③	不正プログラム情報の収集、職員等への注意喚起			○								
			④	不正プログラム対策ソフトウェアの常駐			○								
			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の更新			○								
			⑥	不正プログラム対策ソフトウェアの更新			○								
(2)		①	不正プログラム対策ソフトウェアの常駐						○						
		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の更新						○						
		③	不正プログラム対策ソフトウェアの更新						○						
		④	インターネットに接続していないシステムにおける記録媒体の制限及び不正プログラム対策ソフトウェアの導入等						○						
(3)		①	不正プログラム対策ソフトウェアの設定変更の禁止										○		
		②	外部からのデータ取込時のウイルスチェックの実施										○		
		③	差出人が不明等のファイルの削除										○		
		④	不正プログラム対策ソフトウェアによる定期的なフルチェックの実施										○		
		⑤	添付ファイル送受信時のウイルスチェックの実施										○		
		⑥	ウイルス情報の確認			△							○		
		⑦	ウイルス感染時の対処方法										○		
(4)			外部の専門家の支援体制の整備			○									

権 限 ・ 責 任 等 一 覧 表

※本一覧表は「第3章 情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区 分 (対策基準の例文の規定箇所)		項 目		情報セキュリティ	最高情報統括責任者	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	情報システム担当者	情報セキュリティ担当者	職員等の義務	外部委託	関係規定	
3. 6. 5 不正アクセス対策	(1)	①	使用されていないポートの閉鎖			○								
		②	ウェブページの改ざんを防止するための設定			○			△					
		③	定期的なファイルの改ざんの有無の検査			○								
	(2)	攻撃の予告時の対応		○	○									
	(3)	攻撃を受けた時の対応		○	○									
	(4)	内部からの攻撃等の監視			○			○						
	(5)	職員等による不正アクセス時の対応			○			△	○					
	3. 6. 6 セキュリティ情報の収集	(1)	セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等				○			○				
		(2)	不正プログラム等のセキュリティ情報の収集・周知				○							
		(3)	情報セキュリティに関する技術情報の収集及び共有				○			○				
3. 7 運用	3. 7. 1 情報システムの監視	①	情報システムの監視			○			○					
		②	サーバの正確な時刻設定等の措置			○			○					
		③	外部と常時接続するシステムの監視			○			○					
	3. 7. 2 情報セキュリティポリシーの遵守状況の確認	(1)	①	情報セキュリティポリシーの遵守状況の確認等		△	△	○	○					
			②	問題発生時の対処		○								
			③	システム設定等における情報セキュリティポリシー遵守状況の確認等			○			○				
		(2)	端末及び記録媒体等の利用状況調査			○								
		(3)	①	違反行為の発見時の報告			△		△					○
	②		緊急時対応計画に従った対応			○								
	3. 7. 3 侵害時の対応	(1)	緊急時対応計画の策定		○	○								
		(2)	緊急時対応計画に盛り込むべき内容		○	○								
		(3)	業務継続計画と情報セキュリティポリシーの整合性の確保		○									
		(4)	緊急時対応計画の見直し		○	○								
	3. 7. 4 外部委託	(1)	①	外部委託先の選定時の確認事項						○				○
			②	国際規格の認証取得状況等を参考にした事業者の選定						○				○
(2)		契約項目											○	
(3)		委託先事業者のセキュリティ確保の確認等			△	△		○					○	
3. 7. 5 例外措置	(1)	例外措置の許可			許			○						
	(2)	緊急時の例外措置			△			○						
	(3)	例外措置の申請書の管理			○									
3. 7. 6	法令遵守											○		
3. 7. 7 懲戒処分等	(1)	懲戒処分				○	○	○	○	○	○	○		
	(2)	①	違反時の対応(統括情報セキュリティ責任者確認時)			○		△						
		②	違反時の対応(情報システム管理者確認時)			△		△	○					
		③	違反を改善しない職員等のシステム使用の権利の停止等		△	○		△						

権限・責任等一覧表

※本一覧表は「第3章 情報セキュリティ対策基準」で示した例文に基づき作成している。

※記号:「○」権限又は責任等を有している者。「△」記載がある者又は報告先等。「許」許可を与える者。「承」承認を与える者。

区分 (対策基準の例文の規定箇所)		項目		情報セキュリティ	最高情報統括責任者	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	情報セキュリティ監査責任者	職員等の義務	関係規定 外部委託	
3.8 評価・見直し	3.8.1 監査	(1)	情報セキュリティ対策状況について監査の実施	○							△			
		(2)	① 被監査部門から独立した者への監査の実施依頼									○		
			② 監査を行う者の要件											
		(3)	① 監査実施計画の立案等	承								○		
			② 監査の実施に対する協力											
		(4)	外部委託事業者に対する監査									○		○
		(5)	監査結果の報告	△								○		
		(6)	監査証拠等の保管									○		
	(7)	監査結果への対応		○			△							
	(8)	監査結果の情報セキュリティポリシー見直し等への活用	○											
	3.8.2 自己点検	(1)	① ネットワーク等の自己点検の実施			○			○					
			② 情報セキュリティ対策状況の自己点検				○	○						
		(2)	点検結果と改善策の報告	△			○							
		(3)	① 自己の権限の範囲内での改善											○
	② 点検結果の情報セキュリティポリシー見直し等への活用		○											
3.8.3 情報セキュリティポリシーの見直し		情報セキュリティポリシーの見直しに関する規定	○											