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30年X月版)

平成13年　3月30日　　策　　定
平成30年　x月xx日　　改　　定

総　務　省

（目次）

はじめに

「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」（以下「本ガイドライン」という。）では、以下の構成としている。

第１編は、総則として、本ガイドラインの目的や構成について、第２編で、情報セキュリティポリシーの例文を示している。そして、第３編で、情報セキュリティポリシーの考え方及び内容について、第２編の例文と対応する形で解説する形式としている。また、関連する参考資料を第４編として付けている。

「情報セキュリティポリシー」は、「情報セキュリティ基本方針」と「情報セキュリティ対策基準」から構成されており、「情報セキュリティ基本方針」は情報セキュリティ対策における基本的な考え方を定めており、「情報セキュリティ対策基準」は、「情報セキュリティ基本方針」に基づき、情報システムに必要となる情報セキュリティ対策の基準を定めている。

本ガイドラインを参考として、各地方公共団体においては、必要に応じて内容を取込み、情報セキュリティ強化により一層ご尽力いただくことを願うものである。

第１編

総則

（目次）

第１章

本ガイドラインの目的等

（目次）

第1章　本ガイドラインの目的等

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を守るにあたって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例文は、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、五次の改定を通じて、新たな情報機器、サービス及び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。

本ガイドライン内で記載している例文は、参考としやすくするため基礎的な地方公共団体の中でも最も数の多い市制施行されている地方公共団体を想定して記述している。

なお、本ガイドラインは、読者として情報セキュリティポリシーの策定を行う者、セキュリティ上の職責を担う者などを想定して記述している。

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」に基づく各種の取り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り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り組みを継続しつつ、新たな環境変化に対応した政府の取り組みを進めるために、「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、平成 22 年 5 月 11 日及び平成 25 年 2 月 22 日に改定され、「対策編」が平成 22 年 7 月 30 日に策定、平成 25 年 3 月 30 日に改定されている。さらに、平成 27 年 5 月 25 日に指針本編と「対策編」の改定と、新たに「手引書」が策定された。さらに現在、平成 29 年 4 月 18 日に決定された第 4 次行動計画のもと、指針本編と「対策編」及び「手引書」の改定が進められている。

その他、地方公共団体に関連する法令として、平成 25 年 5 月 24 日に成立し、平成

25 年 5 月 31 日に公布された社会保障・税の分野における給付と負担の公平化や各種行政事務の効率化のための「行政手続における特定の個人を識別するための番号の利用等に関する法律」や平成 26 年 11 月 6 日に成立し、平成 26 年 11 月 12 日に公布された、サイバーセキュリティに関する施策を総合的かつ効果的に推進することを目的とした「サイバーセキュリティ基本法」がある。

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及び新たに成立した法令等を踏まえ、平成 27 年 3 月 27 日に一部改定を行った。平成 27 年度には、自治体情報セキュリティ対策検討チームを構成し、地方公共団体の情報セキュリティに関わる抜本的な対策の検討が行われた。「新たな自治体情報セキュリティ対策の抜本的強化について」（平成 27 年 12 月 25 日総行情第 77 号　総務大臣通知）」にて、地方公共団体におけるセキュリティ対策の抜本的強化への取り組みが示された。

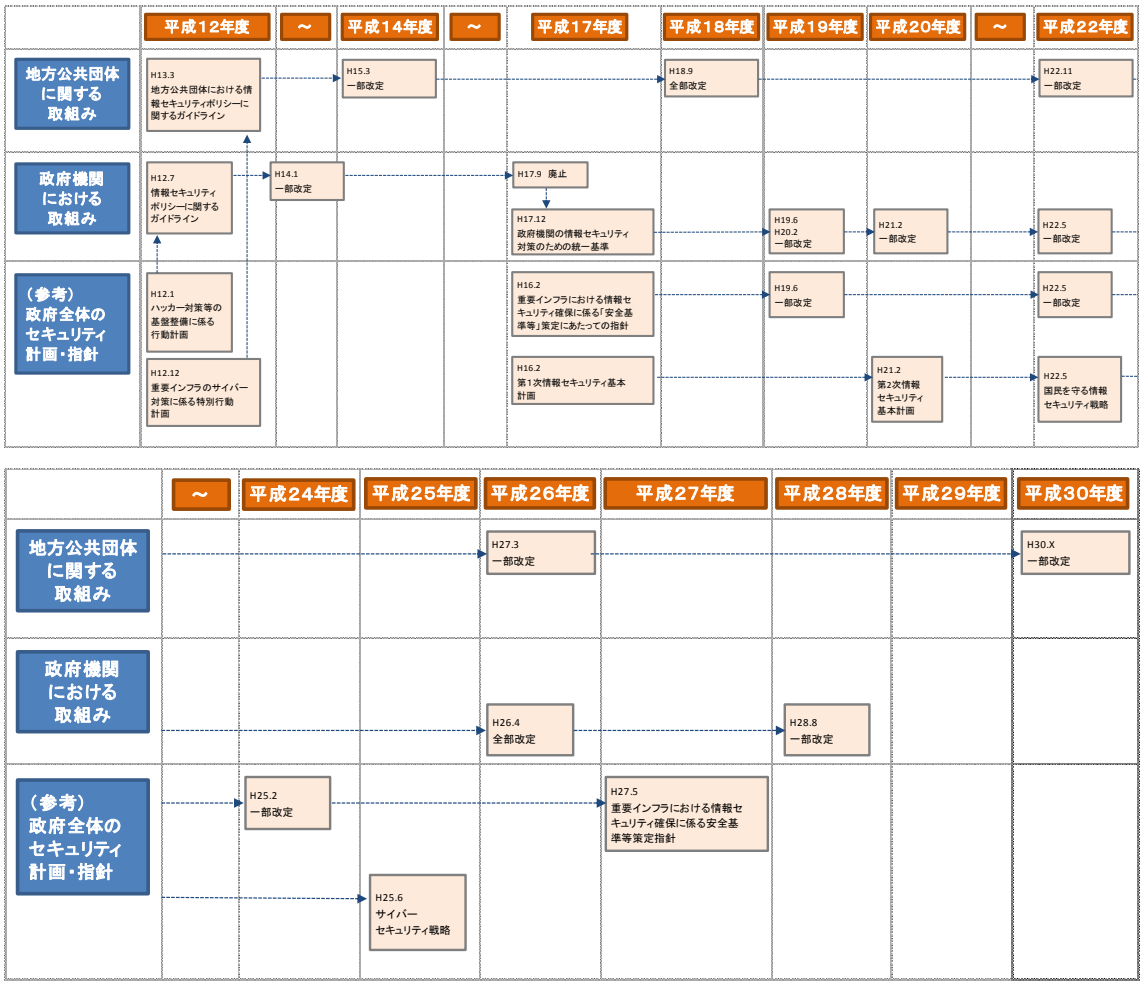
自治体情報セキュリティ対策検討チームの報告、政府機関の情報セキュリティ対策のための統一基準の改定等を踏まえて、今般、ガイドラインを改定したものである。

【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、平成 22 年 5 月 11 日、情報セキュリティ政策会議第 23 回会合及び平成 26 年 5 月 19 日、情報セキュリティ政策会議第 39 回会合、平成 28 年 8 月 31 日、サイバーセキュリティ戦略本部第 9 回会合において、改定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り組みの推移

第２章

地方公共団体における情報セキュリティとその対策

（目次）

第2章　地方公共団体における情報セキュリティとその対策

1.　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、ほか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、全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障害・事故及びシステム上の欠陥（以下「情報セキュリティインシデント」という。）の未然防止のみならず、情報セキュリティインシデント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。

2.　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。

さらに、「サイバーセキュリティ基本法」第 5 条では、地方公共団体においてサイバーセキュリティに関する自主的な施策の策定と実施が責務規定として法定化された。これにより、情報セキュリティポリシーの未策定団体においては策定が必須となり、策定済み団体においても、適時適切な見直しとそれを遵守することが重要となっている。

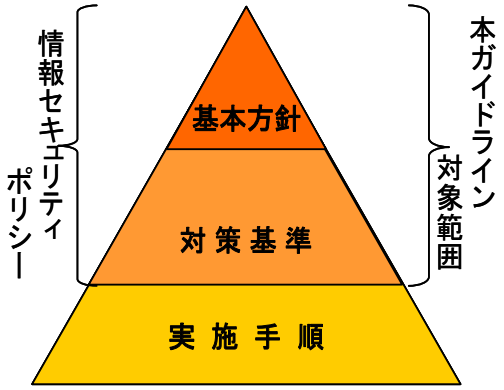
また、番号制度等の最新の制度に係るセキュリティ対策、例えば、情報提供ネットワークシステム等の技術的基準、「特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）」（平成 29 年 5 月 30 日改正　個人情報保護委員会）が示す安全管理措置等についても遵守しなければならない。

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、全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、全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。

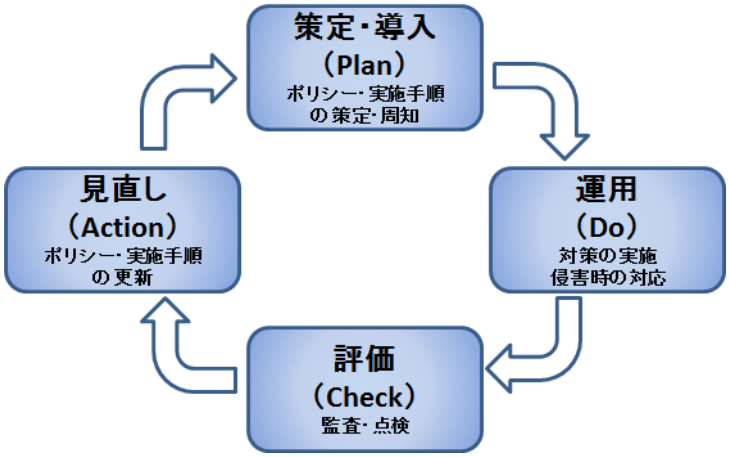
なお、本ガイドラインの対象とする範囲は「情報セキュリティポリシー」を構成する「基本方針」及び「対策基準」であり、「実施手順」は含まれない。



図表２　情報セキュリティポリシーに関する体系図

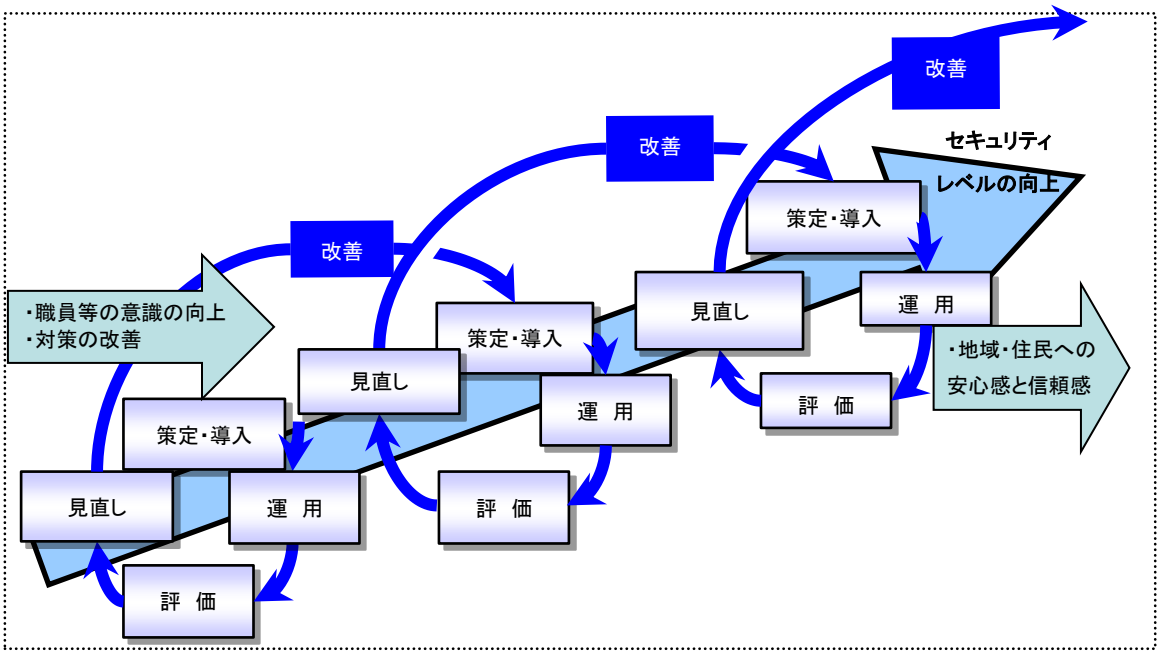
3. 情報セキュリティ対策の実施サイクル

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

第３章

情報セキュリティの管理プロセス

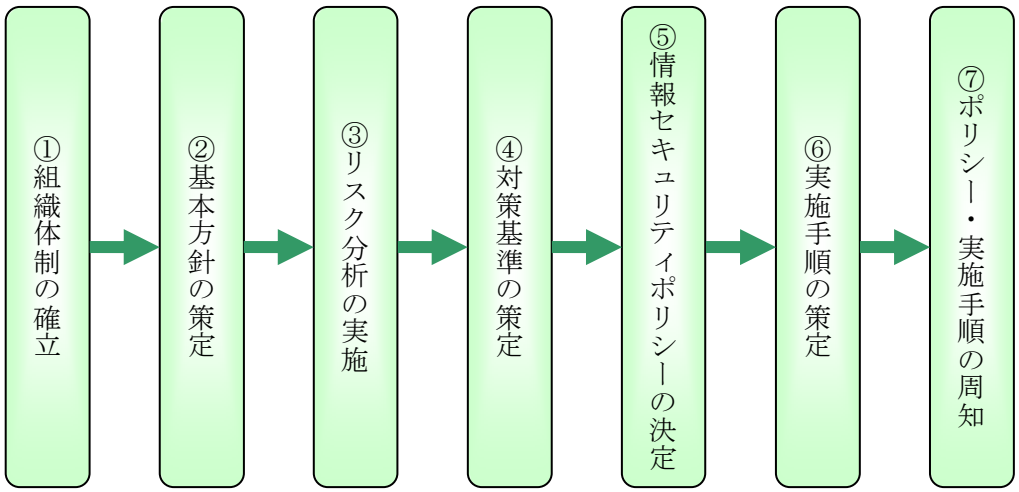
（目次）

第3章　情報セキュリティの管理プロセス

1.　策定及び導入

（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

（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、全ての部局の長、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得る。

（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、全ての部、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。（注：情報セキュリティポリシー監査の見直し等については、本ガイドライン 「第１編 第３章 ３．評価・見直し」を参照されたい。）

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	文書管理規程、文書管理システムの主管
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

（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。

（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）、「高度サイバー攻撃対処のためのリスク評価等のガイドライン」（平成 28 年 10 月 7 日　サイバーセキュリティ対策推進会議）及び「高度サイバー攻撃対処のためのリスク評価等のガイドライン 付属書」（平成 28 年 10 月 7 日　内閣官房内閣サイバーセキュリティセンター）を参照されたい。

進め方として、まずは、利用している情報資産に関わらない組織全体としての情報セキュリティ対策の現状に対するリスク分析・評価を行い、次のステップとして図表７にあるような、情報資産に関わる情報セキュリティ対策の現状に対するリスク分析・評価を行う方法もある。

第１ステップ

庁内の情報セキュリティ規程・規則等の策定状況、組織体制の確立状況について、マネジメント体制の観点（組織的対策、人的対策）からリスク分析・評価を行う。

第２ステップ

保有する情報資産における情報セキュリティリスクを分析・評価する。具体的には以下の作業を行う。

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。

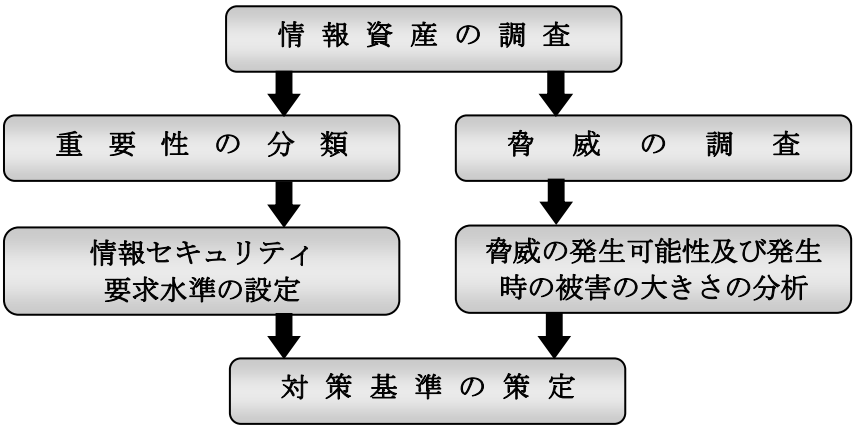
② 各地方公共団体の情報資産を取り巻く脅威及び脆弱性を調査し、リスクを特定する。リスクの発生可能性及び発生した際の被害の大きさからリスクの大きさを求める。

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。

なお、スマートデバイス等の新しいモバイル端末、クラウドサービス等の新しい技術の導入や新たな脅威の発生等の情報セキュリティに関する環境変化により、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

（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。

（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。

（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。

（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。

2. 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、情報資産に対するセキュリティ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。

3. 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（第1編 第2章 3.情報セキュリティ対策の実施サイクル 図表3参照）を繰り返すとともに、PDCA サイクルの有効性の確認のために監査・自己点検を活用し、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。

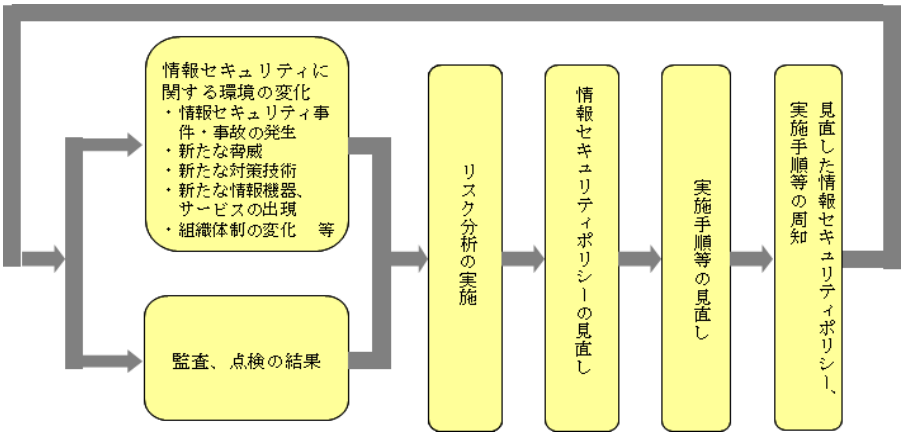
（1） 監査・自己点検

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。なお、総務省では、本ガイドラインで記述されている内容を踏まえ、監査・点検の手順や監査テーマに応じた監査項目の選定のための「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」（平成 30 年 X 月　総務省）を策定しており、同ガイドラインの「第2章 情報セキュリティ監査手順」を参照され

たい。

（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（第１編 第３章 1.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

第４章

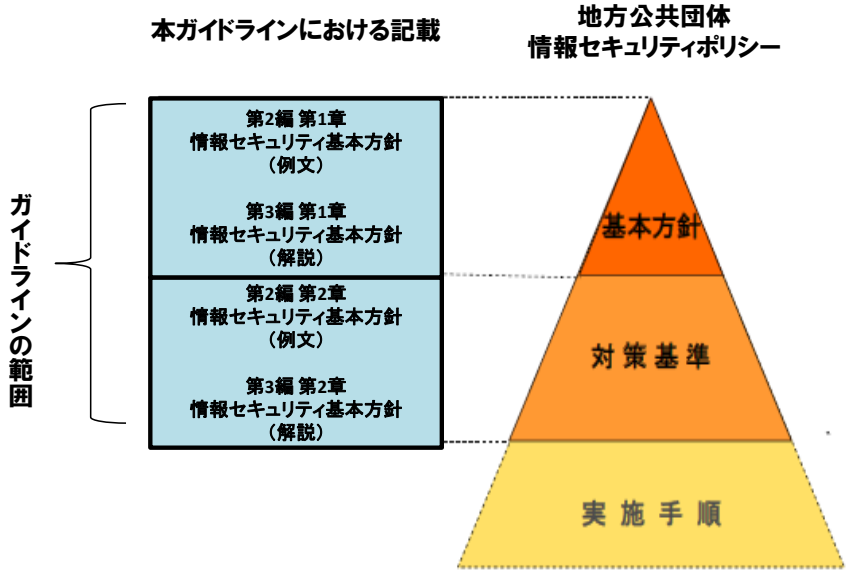
本ガイドラインの構成と対策レベルの設定

（目次）

第4章　本ガイドラインの構成と対策レベルの設定

1.　本ガイドラインの構成

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



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

2.　本ガイドラインにおける対策レベルの設定

地方公共団体において扱う情報資産の重要性や取り巻く脅威の大きさによって、必要とされる対策は一様でないことから、本ガイドラインでは、特段の理由がない限り対策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。

第２編

地方公共団体における
情報セキュリティポリシー
（例文）

（目次）

第１章

情報セキュリティ基本方針
（例文）

（目次）

第1章　情報セキュリティ基本方針（例文）

1.　目的

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

2.　定義

（1）　ネットワーク

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

（2）　情報システム

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

（3）　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（4）　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（5）　機密性

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

（6）　完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（7）　可用性

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

（8）　マイナンバー利用事務系（個人番号利用事務系）

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

（9）　ＬGWAN接続系

人事給与、財務会計及び文書管理等 LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう。

（１０）　インターネット接続系

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

（１１） 通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

（１２） 無害化通信

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

3. 対象とする脅威

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

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

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

（3） 地震、落雷、火災等の災害によるサービス及び業務の停止等

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

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

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） 情報システム全体の強靭性の向上

情報システム全体に対し、次の三段階の対策を講じる。

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

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

③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を行う。高度な情報セキュリティ対策として、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を行う。

（４） 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。

（５） 人的セキュリティ

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

（６） 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（７） 運用

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

（８） 外部サービスの利用

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

約款による外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

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

（９） 評価・見直し

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

7. 情報セキュリティ監査及び自己点検の実施

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

8. 情報セキュリティポリシーの見直し

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

9. 情報セキュリティ対策基準の策定

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

10. 情報セキュリティ実施手順の策定

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

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

（注）情報セキュリティ基本方針は、基本的事項を規定する形式で作成する必要がある。また、宣言書形式での情報セキュリティポリシー基本方針の作成は任意とする。これらの形式の詳細は「第３編　地方公共団体における情報セキュリティポリシー（解説）」の「第１章　情報セキュリティ基本方針（解説）」を参照されたい。

第２章

情報セキュリティ対策基準
（例文）

（目次）

第2章　情報セキュリティ対策基準（例文）

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

1. 組織体制

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

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

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

③CISO は、情報セキュリティインシデントに対処するための体制（CSIRT：Computer Security Incident Response Team、以下「CSIRT」という。）を整備し、役割を明確化する。

（2） 統括情報セキュリティ責任者

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

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

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

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

⑤統括情報セキュリティ責任者は、本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISO の指示に従い、CISO が不在の場合には自らの判断に基づき、必要かつ十分な措置を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、CISO、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

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

（3）情報セキュリティ責任者

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

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

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

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

（4） 情報セキュリティ管理者

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

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

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

（5）情報システム管理者

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

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

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

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

（6）情報システム担当者

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

（7）情報セキュリティ委員会

①本市の情報セキュリティ対策を統一的に行うため、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。

（9）CSIRT の設置・役割

①CISO は、CSIRT を整備し、その役割を明確化すること。

②CISO は、CSIRT に所属する職員を選任し、その中から CSIRT 責任者を置くこと。また、CSIRT 内の業務統括及び外部との連携等を行う職員を定めること。

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

④CISO による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供すること。

⑤情報セキュリティインシデントを認知した場合には、CISO、総務省、都道府県等へ報告すること。

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

⑦情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行うこと。

2. 情報資産の分類と管理

（1）情報資産の分類

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

機密性による情報資産の分類

分類	分類基準	取扱制限
機密性３	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	・支給以外の端末での作業の原則禁止（機密性３の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性２	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
機密性１	機密性２又は機密性３の情報資産以外の情報資産	

完全性による情報資産の分類

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

可用性による情報資産の分類

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

（２）情報資産の管理

①管理責任

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

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

②情報資産の分類の表示

職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適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、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑥情報資産の保管

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

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

（エ）情報セキュリティ管理者又は情報システム管理者は、機密性２以上、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

⑦情報の送信

電子メール等により機密性２以上の情報を送信する者は、必要に応じ、暗号化又はパスワード設定を行わなければならない。

⑧情報資産の運搬

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

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

⑨情報資産の提供・公表

（ア）機密性２以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

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

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

⑩情報資産の廃棄

（ア）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電磁的記録媒体が不要になった場合、電磁的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. 情報システム全体の強靭性の向上

（１）マイナンバー利用事務系

①マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。ただし、マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(MAC アドレス、IP アドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。なお、外部接続先もインターネット等と接

続してはならない。

②情報のアクセス及び持ち出しにおける対策

（ア）情報のアクセス対策

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

（イ）情報の持ち出し不可設定

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

（２）LGWAN 接続系

①LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

（ア）インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送する方式

（イ）インターネット業務端末から、LGWAN 接続系の端末へ画面を転送する方式

（３）インターネット接続系

①インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び LGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を行わなければならない。

②市区町村のインターネット接続口を集約する自治体情報セキュリティクラウドに参加するとともに、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進しなければならない。

4. 物理的セキュリティ

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

（６）庁外への機器の設置

統括情報セキュリティ責任者及び情報システム管理者は、庁外にサーバ等の機器を設置する場合、CISO の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（７）機器の廃棄等

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

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」という。）や電磁的記録媒体の保管庫をいう。

②統括情報セキュリティ責任者及び情報システム管理者は、管理区域を地階又は１階に設けてはならない。また、外部からの侵入が容易にできないように無窓の外壁にしなければならない。【推奨事項】

③統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

④統括情報セキュリティ責任者及び情報システム管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

⑤統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部を全て塞がなければならない。【推奨事項】

⑥統括情報セキュリティ責任者及び情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的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や入退室管理簿の記載による入退室管理を行わなければならない。

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

③情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。

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

（３）機器等の搬出入

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出入について、職員を立ち会わせなければならない。

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。

⑥統括情報セキュリティ責任者は、可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。

また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

4.4. 職員等の利用する端末や電磁的記録媒体等の管理

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

②情報システム管理者は、情報システムへのログイン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、端末の電源起動時のパスワード（BIOS パスワード、ハードディスクパスワード等）を併用しなければならない。【推奨事項】

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

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

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

5. 人的セキュリティ

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モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

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

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

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

④支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

（ア） 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、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利用することができる。

（イ）職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置を遵守しなければならない。

⑤持ち出し及び持ち込みの記録

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

⑥パソコンやモバイル端末におけるセキュリティ設定変更の禁止

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

⑦机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適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やモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

（３）情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

（４）外部委託事業者に対する説明

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

5.2. 研修・訓練

（１）情報セキュリティに関する研修・訓練

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

（２）研修計画の策定及び実施

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

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

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

④研修は、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

⑤CISO は、毎年度１回、情報セキュリティ委員会に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

（３）緊急時対応訓練

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

め、また、効果的に実施できるようにしなければならない。

（4）研修・訓練への参加

幹部を含めた全ての職員等は、定められた研修・訓練に参加しなければならない。

5.3. 情報セキュリティインシデントの報告

（1）庁内での情報セキュリティインシデントの報告

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

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

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

（2）住民等外部からの情報セキュリティインシデントの報告

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

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

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

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

（3）情報セキュリティインシデント原因の究明・記録、再発防止等

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

②CSIRT は、情報セキュリティインシデントであると評価した場合、CISO に速やかに報告しなければならない。

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

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

止策を検討し、CISO に報告しなければならない。

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

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ければならない。

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

②統括情報セキュリティ責任者及び情報システム管理者は、IC カード等の紛失等の通報があり次第、当該 IC カード等を使用したアクセス等を速やかに停止しなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、IC カード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

（2）ID の取扱い

職員等は、自己の管理する ID に関し、次の事項を遵守しなければならない。

①自己が利用している ID は、他人に利用させてはならない。

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

（3）パスワードの取扱い

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

①パスワードは、他者に知られないように管理しなければならない。

②パスワードを秘密にし、パスワードの照会等には一切応じてはならない。

③パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。

④パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。

⑤複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

⑥仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。

⑦パソコン等の端末にパスワードを記憶させてはならない。
⑧職員等間でパスワードを共有してはならない。

6. 技術的セキュリティ

6.1. コンピュータ及びネットワークの管理

（1）文書サーバの設定等

①情報システム管理者は、職員等が使用できる文書サーバの容量を設定し、職員等に周知しなければならない。
②情報システム管理者は、文書サーバを課室等の単位で構成し、職員等が他課室等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。
③情報システム管理者は、住民の個人情報、人事記録等、特定の職員等しか取り扱えないデータについて、別途ディレクトリを作成する等の措置を講じ、同一課室等であっても、担当職員以外の職員等が閲覧及び使用できないようにしなければならない。

（2）バックアップの実施

統括情報セキュリティ責任者及び情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

（3）他団体との情報システムに関する情報等の交換

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

（4）システム管理記録及び作業の確認

①情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。
②統括情報セキュリティ責任者及び情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適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）ログの取得等

①統括情報セキュリティ責任者及び情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

（７）障害記録

統括情報セキュリティ責任者及び情報システム管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適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、CISO 及び統括情報セキュリティ責任者の許可を得なければならない。

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

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

④統括情報セキュリティ責任者及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

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

（１１） 複合機のセキュリティ管理

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

②統括情報セキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

③統括情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

（１２） 特定用途機器のセキュリティ管理

①統括情報セキュリティ責任者は、特定用途機器について、取り扱う情報、利用方法、通信回線への接続形態等により、何らかの脅威が想定される場合は、当該機器の特性に応じた対策を実施しなければならない。

（１３）無線 LAN 及びネットワークの盗聴対策

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

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

（１４）電子メールのセキュリティ管理

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

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

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

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

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

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

（１５）電子メールの利用制限

①職員等は、自動転送機能を用いて、電子メールを転送してはならない。

②職員等は、業務上必要のない送信先に電子メールを送信してはならない。

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

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

⑤職員等は、ウェブで利用できるフリーメール、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。

（１６）電子署名・暗号化

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

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

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

（１７）無許可ソフトウェアの導入等の禁止

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

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

③職員等は、不正にコピーしたソフトウェアを利用してはならない。

（１８）機器構成の変更の制限

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

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

（１９）無許可でのネットワーク接続の禁止

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

（２０）業務以外の目的でのウェブ閲覧の禁止

①職員等は、業務以外の目的でウェブを閲覧してはならない。

②統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適切な措置を求めなければならない。

6.2. **アクセス制御**

（1）アクセス制御等

①アクセス制御

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

②利用者 ID の取扱い

（ア）統括情報セキュリティ責任者及び情報システム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者 ID の取扱い等の方法を定めなければならない。

（イ）職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。

（ウ）統括情報セキュリティ責任者及び情報システム管理者は、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。

③特権を付与された ID の管理等

（ア）統括情報セキュリティ責任者及び情報システム管理者は、管理者権限等の特権を付与された ID を利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。

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

（ウ）CISO は、代行者を認めた場合、速やかに統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。

（エ）統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID 及びパスワードの変更について、外部委託事業者に行わせてはならない。

（オ）統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID 及びパスワードについて、職員等の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

（カ）統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID を初期設定以外のものに変更しなければならない。

（２）職員等による外部からのアクセス等の制限

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

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

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

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

⑤統括情報セキュリティ責任者及び情報システム管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、セキュリティ確保のために必要な措

置を講じなければならない。

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

⑦統括情報セキュリティ責任者は、公衆通信回線（公衆無線 LAN 等）の庁外通信回線を庁内ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者の ID 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）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

（３）自動識別の設定

統括情報セキュリティ責任者及び情報システム管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。【推奨事項】

（４）ログイン時の表示等

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

（５）認証情報の管理

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

②統括情報セキュリティ責任者又は情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

③統括情報セキュリティ責任者又は情報システム管理者は、認証情報の不正利用を防止するための措置を講じなければならない。

（６）特権による接続時間の制限

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

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。また、システム開発のための規則を確立しなければならない。

②システム開発における責任者、作業者のＩＤの管理

（ア）情報システム管理者は、システム開発の責任者及び作業者が使用するＩＤを管理し、開発完了後、開発用ＩＤを削除しなければならない。

（イ）情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

③システム開発に用いるハードウェア及びソフトウェアの管理

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

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

（3）情報システムの導入

①開発環境と運用環境の分離及び移行手順の明確化

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

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

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

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

②テスト

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

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

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

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

（４）システム開発・保守に関連する資料等の整備・保管

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

②情報システム管理者は、テスト結果を一定期間保管しなければならない。

③情報システム管理者は、情報システムに係るソースコードを適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

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。

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。

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

（２）情報システム管理者の措置事項

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

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

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

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

④インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、市が管理している媒体以外を職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著

しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。

（3）職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

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

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

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

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

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

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

⑦コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、以下の対応を行わなければならない。

（ア）パソコン等の端末の場合

LAN ケーブルの即時取り外しを行わなければならない。

（イ）モバイル端末の場合

直ちに利用を中止し、通信を行わない設定への変更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。

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不要なサービスについて、機能を削除又は停止しなければならない。

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

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

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

（2）攻撃への対処

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

（3）記録の保存

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

（4）内部からの攻撃

統括情報セキュリティ責任者及び情報システム管理者は、職員等及び外部委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視しなければならない。

（5）職員等による不正アクセス

統括情報セキュリティ責任者及び情報システム管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

（6）サービス不能攻撃

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

（７）標的型攻撃

統括情報セキュリティ責任者及び情報システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

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。

7. 運用

7.1. 情報システムの監視

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

②統括情報セキュリティ責任者及び情報システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、外部と常時接続するシステムを常時監視しなければならない。

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CISO及び統括情報セキュリティ責任者に報告しなければならない。

②CISOは、発生した問題について、適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）パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

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

（３）職員等の報告義務

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

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

7.3. 侵害時の対応等

（１）緊急時対応計画の策定

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

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

（４）緊急時対応計画の見直し

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

7.4. 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、CISO 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 CISO に報告しなければならない。

（３）例外措置の申請書の管理

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

7.5. 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 25 年法律第 261 号)
② 著作権法（昭和 45 年法律第 48 号）
③ 不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）
④ 個人情報の保護に関する法律（平成 15 年法律第 57 号）

⑤ 行政手続における特定の個人を識別するための番号の利用等に関する法律(平成 25 年法律第 27 号)
⑥ サイバーセキュリティ基本法（平成 28 年法律第 31 号）
⑦ ○○市個人情報保護条例（平成○○年条例第○○号）

7.6. 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 CISO 及び当該職員等が所属する課室等の情報セキュリティ管理者に通知しなければならない。

8. 外部サービスの利用

8.1. 外部委託

（1）外部委託事業者の選定基準

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

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

③情報セキュリティ管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

（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、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

・情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
・外部委託事業者の責任者、委託内容、作業者、作業場所の特定
・提供されるサービスレベルの保証
・外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法
・外部委託事業者の従業員に対する教育の実施
・提供された情報の目的外利用及び受託者以外の者への提供の禁止
・業務上知り得た情報の守秘義務
・再委託に関する制限事項の遵守
・委託業務終了時の情報資産の返還、廃棄等
・委託業務の定期報告及び緊急時報告義務
・市による監査、検査
・市による情報セキュリティインシデント発生時の公表
・情報セキュリティポリシーが遵守されなかった場合の規定(損害賠償等)

（３）確認・措置等

情報セキュリティ管理者は、外部委託事業者において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CISOに報告しなければならない。

8.2. 約款による外部サービスの利用

（１）約款による外部サービスの利用に係る規定の整備

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

①約款によるサービスを利用して良い範囲
②業務により利用する約款による外部サービス
③利用手続及び運用手順

（２）約款による外部サービスの利用における対策の実施

職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

8.3. ソーシャルメディアサービスの利用

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

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

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

②機密性２以上の情報はソーシャルメディアサービスで発信してはならない。

③利用するソーシャルメディアサービスごとの責任者を定めなければならない。

9. 評価・見直し

9.1. 監査

（１）実施方法

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

CISO は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

（8）情報セキュリティポリシー及び関係規程等の見直し等への活用

情報セキュリティ委員会は、監査結果を情報セキュリティポリシー及び関係規定等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

9.2. 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及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

9.3. 情報セキュリティポリシー及び関係規程等の見直し

情報セキュリティ委員会は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等を踏まえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。

第３編

地方公共団体における
情報セキュリティポリシー
（解説）

（目次）

第１章

情報セキュリティ基本方針
（解説）

（目次）

第1章　情報セキュリティ基本方針（解説）

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

1.　目的

【例文】

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

（解説）

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

2.　定義

【例文】

（１）　ネットワーク

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

（２）　情報システム

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

（３）　情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（４）　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準をいう。

（５） 機密性

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

（６） 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

（７） 可用性

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

（８） マイナンバー利用事務系（個人番号利用事務系）

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

（９） LGWAN 接続系

人事給与、財務会計及び文書管理等 LGWAN に接続された情報システム及びその情報システムで取り扱うデータをいう。

（１０） インターネット接続系

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

（１１） 通信経路の分割

LGWAN 接続系とインターネット接続系の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

（１２） 無害化通信

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

(解説)

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

3. 対象とする脅威

【例文】

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

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

取、内部不正等

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

（３） 地震、落雷、火災等の災害によるサービス及び業務の停止等

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

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

(解説)

情報資産の「機密性」、「完全性」、「可用性」を脅かす脅威を明確にしている。

例文には、昨今、想定される脅威の例を挙げている。

4. 適用範囲

【例文】

（１） 行政機関の範囲

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

（２） 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

①ネットワーク、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

(解説)

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

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

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

情報資産の種類	情報資産の例
ネットワーク	通信回線、ルータ等の通信機器等
情報システム	サーバ、パソコン、モバイル端末、汎用機、複合機、オペレーティングシステム、ソフトウェア等
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	サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、USB メモリ、外付けハードディスクドライブ、DVD-R、磁気テープ等の外部電磁的記録媒体
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

5. 職員等の遵守義務

【例文】

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。

（解説）

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

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

なお、「職員等」とは、例示された者を含む全ての職員が該当するものである。

6. 情報セキュリティ対策

【例文】

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

（１） 組織体制

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

（２） 情報資産の分類と管理

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

（３） 情報システム全体の強靭性の向上

情報システム全体に対し、次の三段階の対策を講じる。

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

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

③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を行う。高度な情報セキュリティ対策として、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を行う。

（４） 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。

（５） 人的セキュリティ

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

（６） 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

（７） 運用

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

切に対応するため、緊急時対応計画を策定する。

（8） 外部サービスの利用

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

約款による外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

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

（9） 評価・見直し

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

（解説）

情報セキュリティ対策の基本方針について記載する。例文では、組織体制、情報資産の分類と管理方法、情報システム全体の強靭性の向上、物理的セキュリティ、人的セキュリティ、技術的セキュリティ、運用、外部サービスの利用及び評価・見直しにおける情報セキュリティ基本方針を記載している。

7. 情報セキュリティ監査及び自己点検の実施

【例文】

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

（解説）

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

評価のためには、日常的に職員等へのモニタリングを行い、地方公共団体の情報セキュリティポリシー及び情報セキュリティ実施手順が運用の中で遵守されているかについて、職員等や外部の組織によって定期的又は必要に応じて確認しなければならないことを明確にしている。この際に、情報セキュリティポリシーが現場の状況に適合しているか、最

新の法令や組織の現状を踏まえ、情報セキュリティポリシーに不備や不足はないか、なども考慮する必要がある。

8. 情報セキュリティポリシーの見直し

【例文】

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

(解説)

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

9. 情報セキュリティ対策基準の策定

【例文】

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

(解説)

情報セキュリティ基本方針「６．情報セキュリティ対策」、「７．情報セキュリティ監査及び自己点検」及び「８.情報セキュリティポリシーの見直し」で示した情報セキュリティ対策について、遵守事項及び判断基準を定める必要がある。遵守事項及び判断基準は本ガイドラインの情報セキュリティ対策基準に記載している。

10. 情報セキュリティ実施手順の策定

【例文】

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

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

(解説)

情報セキュリティ対策基準を策定するとともに、その対策基準に対して具体的な手順

を定めた情報セキュリティ実施手順を策定する必要がある。情報セキュリティ実施手順は、公にすると、サイバー攻撃を受けるリスクが高くなってしまうため、非公開にする必要がある。

11. 宣言書の形式

（解説）

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

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

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

【宣言書の形式例】

情報セキュリティ基本方針（宣言書）

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

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

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

（1） 情報セキュリティ対策に取り組むための全庁的な体制を確立する。

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

（3） 本市の保有する情報資産を適切に管理する。

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

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

（7） 全ての職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティ基本方針、情報セキュリティ対策基準及び情報セキュリティ実施手順を遵守する。

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

平成○○年○○月○○日

○○市長（又は、最高情報セキュリティ責任者）

第２章

情報セキュリティ対策基準
（解説）

（目次）

第2章　情報セキュリティ対策基準（解説）

1. 組織体制

【趣旨】

組織として、情報セキュリティ対策を確実に実施するには、情報セキュリティ対策に取り組む十分な組織体制を整備し、一元的に情報セキュリティ対策を実施する必要がある。このことから、情報セキュリティ対策のための組織体制、権限及び責任を規定する。

【例文】

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

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

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

③CISOは、情報セキュリティインシデントに対処するための体制（CSIRT：Computer Security Incident Response Team、以下「CSIRT」という。）を整備し、役割を明確化する。

（2） 統括情報セキュリティ責任者

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

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

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

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

⑤統括情報セキュリティ責任者は、本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISOの指示に従い、CISOが不在の場合には自らの判断に基づき、必要かつ十分な措置を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、CISO、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。

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

（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、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、情報セキュリティ責任者、統括情報セキュリティ責任者及びCISOへ速やかに報告を行い、指示を仰がなければならない。

（5） 情報システム管理者

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

②情報システム管理者は、所管する情報システムにおける開発、設定の変更、運用、

見直し等を行う権限及び責任を有する。

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

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

（6） 情報システム担当者

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

（7） 情報セキュリティ委員会

①本市の情報セキュリティ対策を統一的に行うため、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。

（9） CSIRT の設置・役割

①CISO は、CSIRT を整備し、その役割を明確化すること。

②CISO は、CSIRT に所属する職員を選任し、その中から CSIRT 責任者を置くこと。また、CSIRT 内の業務統括及び外部との連携等を行う職員を定めること。

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

④CISO による情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部局等に提供すること。

⑤情報セキュリティインシデントを認知した場合には、CISO、総務省、都道府県等へ報告すること。

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

⑦情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行うこと。

（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。

・CISO・CSIRT の設置等
・インシデント連絡ルートの多重化
・緊急時対応計画の見直しと緊急時対応訓練の実施
・標的型攻撃への対策

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

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

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

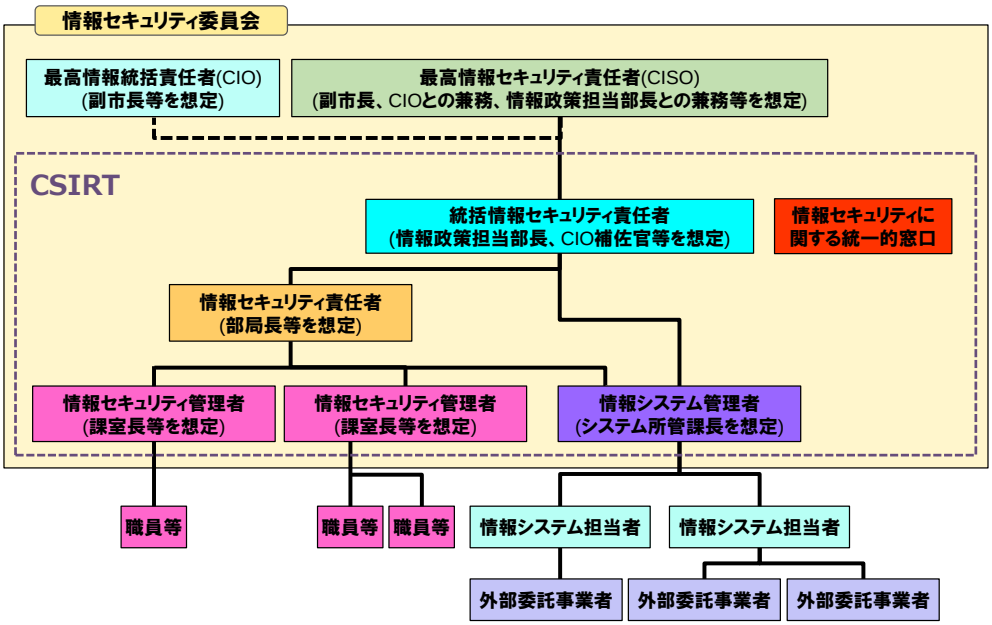
（１） 最高情報セキュリティ責任者（CISO: Chief Information Security Officer、以下「CISO」という。）

CISO は、地方公共団体における全てのネットワーク、情報システム等の情報資産の管理や情報セキュリティに関する権限及び責任を有する。

例文では、CISO が、情報資産の管理や情報セキュリティ対策に関する最終決定権限及び責任を有することとしているが、小規模の地方公共団体などにおいては、情報通信技術の活用による住民の利便性の向上及び行政運営改善等に関するものを統括する最高情報統括責任者（CIO: Chief Information Officer、以下「CIO」という。）との兼務や情報政策担当部長との兼務など、柔軟な対応が必要となる。

また、適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、内部の職員のみならず、情報セキュリティに関する外部の専門家を最高情報セキュリティアドバイザー（CISO の補佐）として置くことが望ましい。また、情報セキュリティインシデントに備える体制として CSIRT を設置する必要がある。

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



図表 11　情報セキュリティ推進の組織体制例

（2）　統括情報セキュリティ責任者

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

CISO が不在の場合には、統括情報セキュリティ責任者がその権限を CISO に代わって行使できるよう、権限の委譲についても規定しておく。また、情報セキュリティインシデント発生時等の緊急時には、統括情報セキュリティ責任者が中心となり被害の拡大防止、事態の回復のための対策実施、再発防止策の検討を行う必要がある。

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

（3）　情報セキュリティ責任者

情報セキュリティ責任者は、各部局等の情報セキュリティ対策に関する権限及び責任を有する。

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

（4）　情報セキュリティ管理者

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

情報セキュリティ管理者は、システムの利用現場の担当者であり、所管する課室等において、情報資産に対するセキュリティ侵害又はセキュリティ侵害のおそれがあ

る状況に直面する可能性が高い。そのため、このような場合を想定し、情報セキュリティ責任者、統括情報セキュリティ責任者及びCISOに対する報告義務を定める。

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

（５） 情報システム管理者

情報システム管理者は、個々の情報システム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。

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

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

（６） 情報システム担当者

情報システム担当者とは、情報システム管理者の指示等に従う職員で、開発、設定の変更、運用、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、CISO、CIO、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者等が想定され、定期的及び必要に応じてCISOが構成員を招集し、開催する。

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

（注１１）情報セキュリティに関する意思決定機関として情報セキュリティ委員会以外に庁議や幹部会議等を位置付けることも可能である。

（８） 兼務の禁止

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

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

（９） CSIRT の設置・役割

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

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

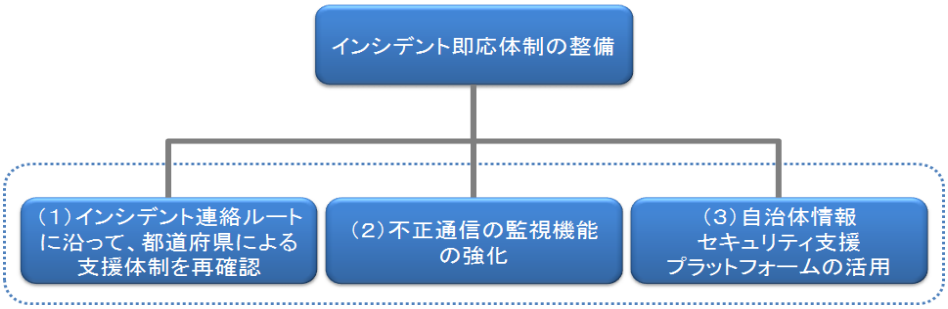
また、地方公共団体情報システム機構（自治体 CEPTOAR）等の関係機関や他の地方公共団体における同様の窓口機能、外部の事業者等と連携して体制を強化することが求められる。

（注１２）一般的に情報システムに対するサイバー攻撃等の情報セキュリティインシデントが発生した際に、発生した情報セキュリティインシデントを正確に把握・分析し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とするための機能を有する体制は CSIRT と呼ばれている。CSIRT の持つ機能や在り方は組織によって様々であるが、まずは、地方公共団体においては情報セキュリティに関する統一的な窓口の機能を有する体制を整えることが重要である。

（注１３）情報セキュリティインシデントに関しては、単独で対応することが困難なケースもあること、また同様の被害拡大防止、発生の予防が重要であることから、インシデント即応体制は図表 12 の３つの視点から整備することが必要である。都道府県は、各都道府県内の市区町村における情報セキュリティインシデント発生時において、国への連絡を行うとともに、当該市区町村の情報セキュリティインシデント対応の支援を実施することが期待される。平常時から、都道府県と管内市区町村との間の連絡を密にして、各都道府県において、都道府県 CSIRT と市区町村 CSIRT の連携体制を構築しておくことが望ましい。

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

しい。



図表 12　情報セキュリティ推進の組織体制例

2. 情報資産の分類と管理

【趣旨】

情報資産を保護するには、まず情報資産を分類し、分類に応じた管理体制を定める必要がある。情報資産の管理体制が不十分な場合、情報の漏えい、紛失等の被害が生じるおそれがある。そこで、機密性・完全性・可用性に基づく情報資産の分類と分類に応じた取扱いを定めた上で、情報資産の管理責任を明確にし、情報資産のライフサイクルに応じて取るべき管理方法を規定する。

【例文】

（1） 情報資産の分類

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

機密性による情報資産の分類

分類	分類基準	取扱制限
機密性３	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性を要する情報資産	・支給以外の端末での作業の原則禁止（機密性３の情報資産に対して） ・必要以上の複製及び配付禁止 ・保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止 ・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納 ・復元不可能な処理を施しての廃棄 ・信頼のできるネットワーク回線の選択 ・外部で情報処理を行う際の安全管理措置の規定 ・電磁的記録媒体の施錠可能な場所への保管
機密性２	行政事務で取り扱う情報資産のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報資産	
機密性１	機密性２又は機密性３の情報資産以外の情報資産	

完全性による情報資産の分類

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

可用性による情報資産の分類

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

（２） 情報資産の管理

①管理責任

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

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

②情報資産の分類の表示

職員等は、情報資産について、ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）、格納する電磁的記録媒体のラベル、文書の隅等に､情報資産の分類を表示し､必要に応じて取扱制限についても明示する等適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、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱わなければならない。

⑥情報資産の保管

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

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

（エ） 情報セキュリティ管理者又は情報システム管理者は、機密性２以上、完全性２又は可用性２の情報を記録した電磁的記録媒体を保管する場合、耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管しなければならない。

⑦情報の送信

電子メール等により機密性２以上の情報を送信する者は、必要に応じ、暗号化又はパスワード設定を行わなければならない。

⑧情報資産の運搬

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

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

⑨情報資産の提供・公表

（ア） 機密性２以上の情報資産を外部に提供する者は、必要に応じ暗号化又はパスワードの設定を行わなければならない。

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

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

⑩情報資産の廃棄

（ア） 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電磁的記録媒体が不要になった場合、電磁的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得る。

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

（２）　情報資産の管理

①管理責任

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

（注２）管理に当たっては、重要な情報資産について台帳を作成することが望ましい。これにより、情報資産の所在、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全ての者に周知する方法もある。

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

③情報の作成～⑩情報資産の廃棄

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

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

3. 情報システム全体の強靭性の向上

【趣旨】

複雑・巧妙化しているサイバー攻撃の脅威により、地方公共団体の行政に重大な影響を与えるリスクが想定されるため、各地方公共団体においては、機密性はもとより、可用性や完全性の確保にも十分配慮された攻撃に強い情報システムが望まれる。

【例文】

（１） マイナンバー利用事務系

①マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。ただし、マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(MAC アドレス、IP アドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。なお、外部接続先もインターネット等と接続してはならない。

②情報のアクセス及び持ち出しにおける対策

（ア）情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。また、業務毎に専用端末を設置することが望ましい。なお、外部接続先もインターネット等と接続してはならない。

（イ）情報の持ち出し不可設定

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

（２） LGWAN 接続系

①LGWAN 接続系とインターネット接続系の分割

LGWAN 接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータを LGWAN 接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

（ア)インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送する方式

（イ）インターネット業務端末から、LGWAN 接続系の端末へ画面を転送する方式

（３） インターネット接続系

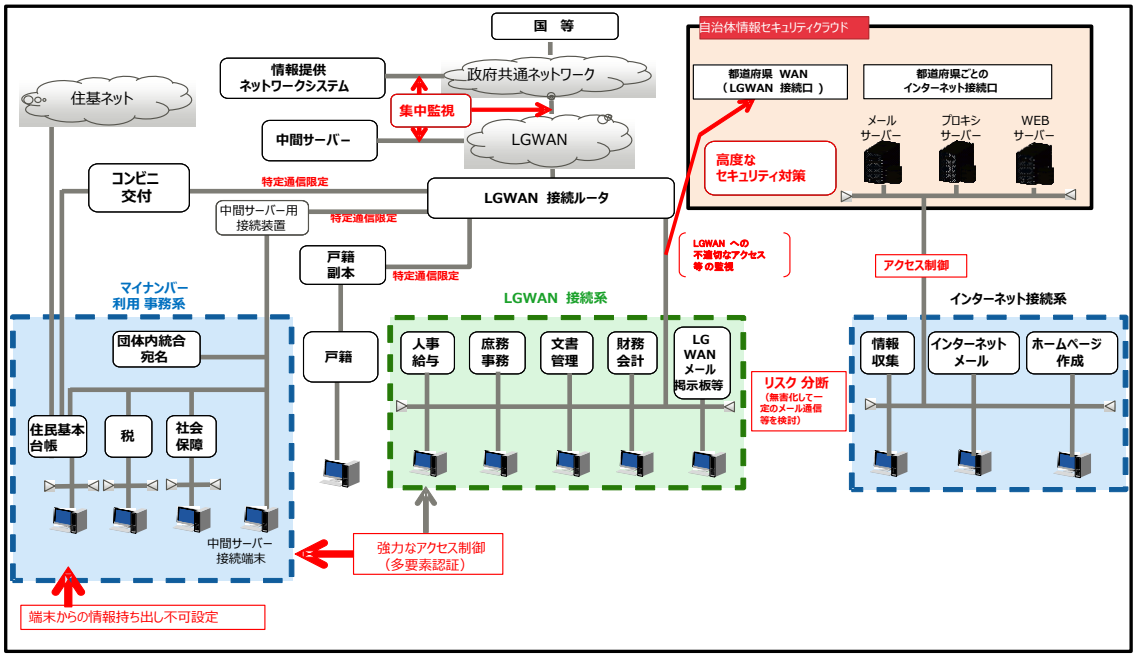
①インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及び LGWAN への不適切なアクセス等の監視等の情報セキュリティ対策を行わなければならない。

②市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を行い、関係省庁や都道府県等と連携しながら、情報セキュリティ対策を推進しなければならない。

（解説）

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

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



図表 13　三層の構えによる自治体情報システム例

（１） マイナンバー利用事務系

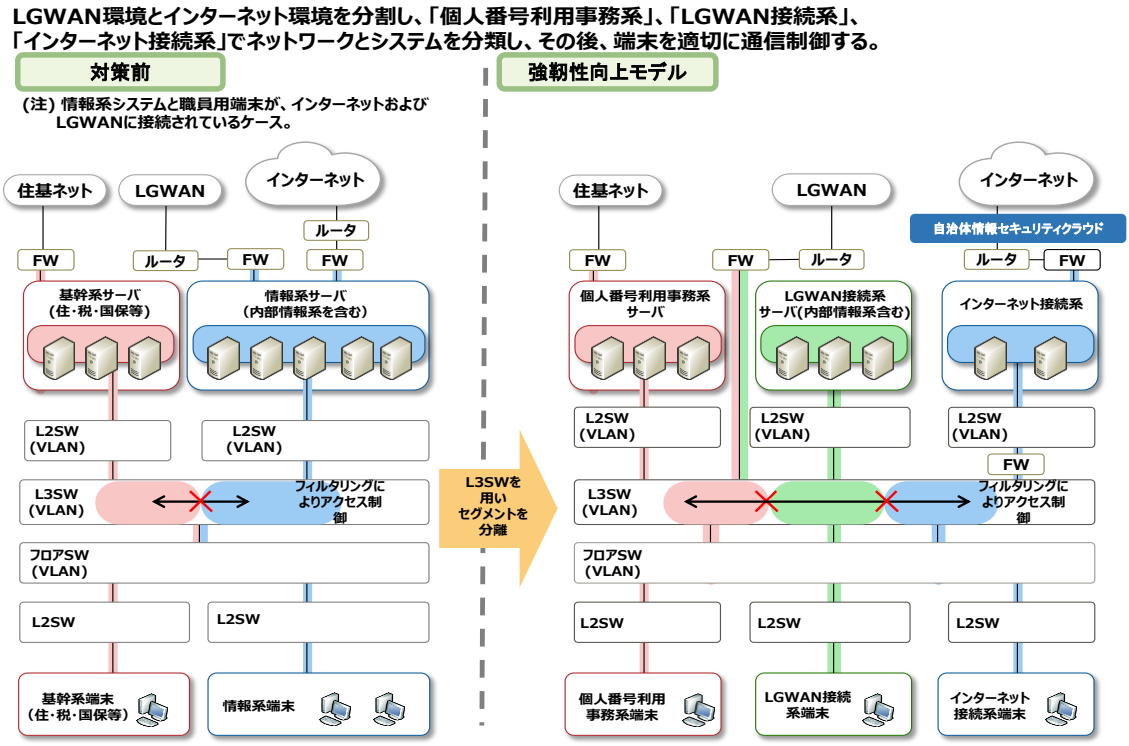
①マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系においては、住民情報の流失を防ぐ必要があることから、他の領域（LGWAN 接続系及びインターネット接続系）との通信をできないようにしなければならない。統合パッケージシステムを利用している場合であっても、

マイナンバー利用事務系と LGWAN 接続系との端末は分けなければならない。

総合窓口を実施している場合等、業務毎に専用端末を設置することが難しい場合には、端末からの情報持ち出し不可設定や端末への多要素認証の導入を図り、利用状況をチェックする運用体制などを整備した上で実施することが望ましい。

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



図表 14　強靭性向上モデルにおけるネットワーク再構成の一つのイメージ

マイナンバー利用事務系と外部との通信の必要がある場合は、通信経路の限定（MAC アドレス、IP アドレス）に加えて、アプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。これらの限定を行った通信を特定通信という。

特定通信を行う際は、以下の点に留意しなければならない。

- L2SW/L3SW による通信経路限定、ファイアウォールによる通信プロトコル限定等を行うことで通信を制限すること。
- その他外部ネットワークとの通信が発生する場合は専用回線サービスを検討すること。

特定通信となる外部接続の例として、住民基本台帳ネットワークシステム、マイナンバー制度における中間サーバ連携や住民票の写し等のコンビニ交付用の

LGWAN 接続、データバックアップセンターや共同利用／クラウドセンター等、十分に情報セキュリティが確保された通信先との限定的な接続がある。

なお、特定通信を行う外部接続先についても、インターネット等と接続されていてはならない。

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

（注２）指定金融機関から税などの口座引落済みデータ（消し込みデータ）等の外部データを受信し、マイナンバー利用事務系へ取り込みを行う場合は、LGWAN-ASP 等を利用して受信しなければならない。マルウェア感染しているファイルをマイナンバー利用事務系に取り込んでしまうことを防止するため、以下の手順で取り込むことが考えられる。

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

（イ）他の用途で使用されることのない専用の電磁的記録媒体に保存

（ウ）システム管理責任者による電磁的記録媒体接続禁止の一時的解除

（エ）マイナンバー利用事務系端末でウイルスチェックを実施後に取り込む

②情報のアクセス及び持ち出しにおける対策

（ア）情報のアクセス対策

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

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

図表 15　認証の種類と手段

認証手段の概要と具体例		利点	欠点
「知識」を利用する手段	● パスワード ● パスフレーズ ● 暗証番号 ● ピクチャーパスワード	●運用コストが安い ●特別な装置が不要で、非常に簡便	● 複雑すぎる「知識」は記憶できない ● 簡単な「知識」えあれば、正規の利用者 でなくても､「知識」を推定して正規の 利用者になりすますことができる ●「知識」忘失の恐れがある
「知識」と「所持」を併用	● IC カードと暗証番号の併用 ● ワンタイムパスワードトークンとパスワード(暗証番号）の併用 ● SIM9 カード（携帯電話／スマートフォンの固有番号）とパスワードの併用	● 「知識」と「所持」を併用することで､「知識」だけ、あるいは「所持」だけに頼るよりも安全性が高い	● カードやトークン等が必要で運用コストが高い ● カードやトークン等の盗難・紛失の恐れがある ● 「知識」忘失の恐れがある

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

図表 16　情報システムが正規の利用者かどうかを判断する認証手段

（注３）接続する端末を特定するために MAC アドレスの管理を行うことが望ましい。

（イ）情報の持ち出し不可設定

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

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

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

（２） LGWAN 接続系

①LGWAN 接続系とインターネット接続系の分割

分割とは、一旦両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにすることをいう。

（ア）インターネット環境で受信したインターネットメールの本文のみを LGWAN 接続系に転送する方式

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

（イ）インターネット業務端末から、LGWAN 接続系の端末へ画面を転送する方式

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

上記の他に、ファイルを一旦分解した上で、ウイルスが潜んでいる可能性のある部分について除去を行った後、ファイルを再構築し分解前と同様のファイル形式に復元する方法（サニタイズ処理）がある。

（注４）インターネットメールの添付ファイルやインターネットからダウンロードしたファイルの閲覧は、インターネット接続系の端末やプリンタで実施すべきであるが、LGWAN 接続系のメールサーバ等にデータを受け渡す際には、インターネット接続系端末でのウイルスチェックに加え、標的型攻撃への対策として次の仕組みを導入する必要がある。

・添付ファイルからテキストのみを抽出
・添付ファイルを画像 PDF に変換
・無害化するサービス等を活用してファイルを無害化

（注５）インターネット接続系から LGWAN 接続系にインターネットからダウンロードしたファイルやインターネットメールの添付ファイルを取り込む場合は、マルウェア感染がないことを前提に、ファイル無害化機器、ソフト

ウェア、サービス等を利用し、無害化されていることを確認しなければならない。

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

（３） インターネット接続系

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

（ア）監視対象の集約化

集約化することにより、監視の効率化を図る。監視対象としてＷｅｂサーバ、メールリレーサーバ、プロキシサーバ、外部ＤＮＳサーバ、LGWAN 接続ファイアウォールのログがある。

（イ）情報セキュリティ機器の導入

通信パケットの監視及び破棄、通信ポートの制御、不正なプログラムの検知、不審なメールの検知及び遮断、不審なＵＲＬへのアクセス遮断、ログ監視、コンテンツの改ざん検知等の機能を持った、高度な情報セキュリティ機器を導入する。

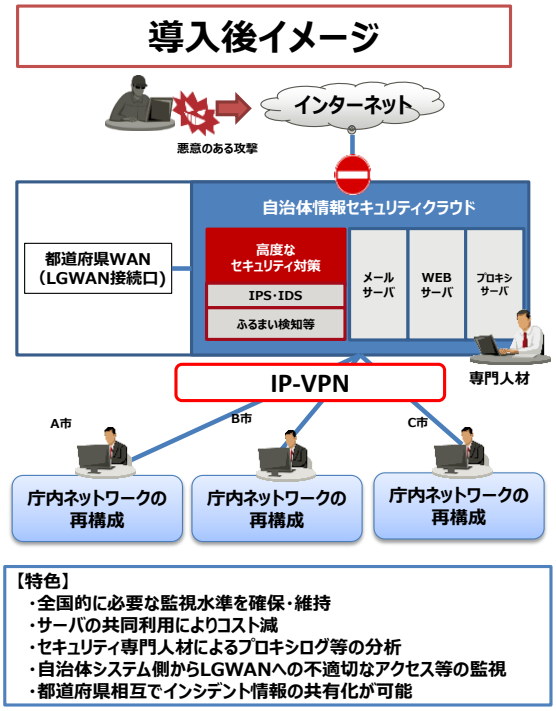
（ウ）情報セキュリティ運用監視

情報セキュリティ運用監視は、情報セキュリティ専門人材による高水準なセキュリティ運用監視である。

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

・各市区町村において必要な情報セキュリティレベルの確保・向上
・情報セキュリティ専門人材によるインシデントの早期発見と対処
・各市区町村システム側からLGWANへの不適切なアクセス等の監視
・機器・運用の共同利用によるコスト削減

（注７）都道府県単位で集約化されたインターネット接続口のため、業務に支障のない稼働が望まれる。情報セキュリティインシデントに対し迅速かつ適切に対応するために、予兆を含め早期検知と常駐する専門人材による早期判断が重要であり、そのため運用委託先には24時間365日有人での集中監視を求めなければならない。



図表 17　自治体情報セキュリティクラウド

（注８）LGWAN への不適切なアクセスの監視を目的に、都道府県が市区町村側の LGWAN 用ファイアウォールの不正パケットログを集中監視する仕組みを整備することが望ましい。監視の観点として、(a)～(d)の対応が考えられる。

(a) マイナンバー利用事務系及び LGWAN 接続系から LGWAN への通信のうち、不正な通信元からのアクセスを自動的に遮断（パケットを破棄）し、遮断したアクセスログから、不正な通信元及び通信先の IP アドレス・MAC アドレスを取得・分析する。

(b) LGWAN の規約上で許可されているプロトコル（DNS、NTP、SMTP、HTTP、HTTPS、LDAP 等）以外のプロトコルを使用したアクセスを自動的に遮断（パケットを破棄）し、遮断したアクセスログから、使用されたプロトコルを取得・分析する。

(c) マイナンバー利用事務系及び LGWAN 接続系から LGWAN への不正なファイル交換ソフト（Winny 等）のアクセスに対するアクセスログから通信元を確認し、不正なファイル共有アプリケーションの削除が求められる。

(d) マイナンバー利用事務系及び LGWAN 接続系からのサービス妨害攻撃を疑われる大量アクセスの通信元を確認し、ネットワークからの遮断及びマルウェア感染有無の確認等を実施する。

（４） その他のセキュリティ対策

①プリンタ・複合機の情報セキュリティ対策

プリンタ・複合機は、必要に応じてマイナンバー利用事務系、LGWAN 接続系、インターネット接続系のネットワーク毎に設置されることが望ましい。共有する場合においてもマイナンバー利用事務系又は LGWAN 接続系について、インターネット接続系と共有することは認められない。共有する場合には、１台のプリンタ・複合機にネットワーク毎に専用の LAN ポートを設け、他の領域と分離された通信を保証することが望ましい。それが困難である場合には、ネットワークの一方を LAN ポートに、もう一方は USB ポートにプリンタサーバを繋ぐなどの方法を検討する必要がある。

②本庁・支所・出先機関間でのネットワーク通信

本庁、支所、出先機関でマイナンバー利用事務系と LGWAN 接続系を構築するネットワークは、相互の通信でインターネット回線を利用している場合、VPN 通信等を用いて、通信元と通信先が特定されており、通信経路が限定されていなければならない。ただし原則はインターネット回線ではなく閉域網を利用すること。

③マイナンバー利用事務系と LGWAN 接続系における無線 LAN の利用

無線 LAN については、電波を遮蔽しきれない等の理由で完全に分離している状態とは言えない。インターネット接続系を除き、無線 LAN の利用は避けることが望ましい。

④修正プログラム及びパターンファイルの更新

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

⑤自動交付機による証明交付

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

⑥VPN 接続による外部との通信

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

⑦インターネット経由での各種業務システムの利用

テレワーク等のインターネット経由で各種業務システムにアクセスする場合は、以下のような情報セキュリティ対策を実施しなければならない。

・仮想デスクトップ接続に限定

・利用可能なネットワークをインターネット接続系に限定
・専用端末化（電子証明書、MAC アドレスによるフィルタリングなど）
・通信の暗号化（WPA2 方式など）
・データのダウンロード制限

上記の他、多要素認証で端末の正規の利用者を確実に認証することが望ましい。

⑧J-ALERT 等の LGWAN 接続系とインターネット接続系の双方への接続が必要な情報システムへの対応

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

⑨インターネットメールによる障害通報

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

⑩アクセス記録を外部に提供する場合、もしくは他団体からアクセス記録を受領する場合

アクセス記録に個人情報が含まれる場合、個人情報保護条例及び情報セキュリティ管理関係の規程に従わなければならない。

4. 物理的セキュリティ

4.1. サーバ等の管理

【趣旨】

サーバ等のハードウェアは、情報システムの安定的な運用のために適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、電磁的記録媒体を内蔵する機器を外部の事業者に修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管理者は、外部の事業者に故障を修理させるにあたり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認などを行わなければならない。

（６） 庁外への機器の設置

統括情報セキュリティ責任者及び情報システム管理者は、庁外にサーバ等の機器を設置する場合、CISO の承認を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。

（７） 機器の廃棄等

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

（解説）

（１） 機器の取付け

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

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

（２） サーバの冗長化

サーバ等の機器が緊急停止した場合にも、業務を継続できるようにするために、

バックアップシステムを設置することが有効である。

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

（３） 機器の電源

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

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

（４） 通信ケーブル等の配線

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

（５） 機器の定期保守及び修理

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

（６） 庁外への機器の設置

庁外にサーバ等の機器を設置する場合には、十分なセキュリティ対策がなされているか、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、当該外部委託事業者の要員の変化等を把握する。地方公共団体職員によるデータセンター内部への立入りがデータセンターのセキュリティポリシーに違反する等、外部委託事業者を訪問できない場合は、訪問調査に代えて第三者による情報セキュリティ監査報告書、外部委託事業者の内部監査部門による情報

セキュリティ監査報告書等によって確認する。

（７） 機器の廃棄等

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、全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。

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、機器等の搬出入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」という。）や電磁的記録媒体の保管庫をいう。

②統括情報セキュリティ責任者及び情報システム管理者は、管理区域を地階又は1階に設けてはならない。また、外部からの侵入が容易にできないように無窓の外壁にしなければならない。【推奨事項】

③統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区域から外部に通ずるドアは必要最小限とし、鍵、監視機能、警報装置等によって許可されていない立入りを防止しなければならない。

④統括情報セキュリティ責任者及び情報システム管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

⑤統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携して、管理区域を囲む外壁等の床下開口部を全て塞がなければならない。【推奨事項】

⑥統括情報セキュリティ責任者及び情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び電磁的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や入退室管理簿の記載による入退室管理を行わなければならない。

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

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

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

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

（３） 機器等の搬入出

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

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

（解説）

（１） 管理区域の構造等

情報システムの安定的な運営等のために、情報システム室や保管庫（磁気テープ等の保管庫）である管理区域の管理方法について定める。管理区域内には精密機器が多いことから、火災、水害、埃、振動、温度、湿度等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、手動で扉を開閉できるように、平時から管理区域を管理している情報システム管理者が、自動扉開閉制御を解除するスイッチの場所を入室権限のある職員等に周知しておくことが必要である。鍵等による立入り防止措置についても同様である。

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

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

（２） 管理区域の入退室管理等

管理区域は情報資産の分類に応じて厳格な管理が行われなければならない。リスク評価を行って許可する範囲を検討し、入室できる者は許可された者のみに制限する。また、外部からの訪問者が管理区域に入室する場合、職員が付き添うとともに、

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

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

（３） 機器等の搬出入

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

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

4.3. 通信回線及び通信回線装置の管理

【趣旨】

ネットワーク利用における通信回線及び通信回線装置が適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。

⑥統括情報セキュリティ責任者は、可用性２の情報を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする回線を選択しなければならない。また、必要に応じ、回線を冗長構成にする等の措置を講じなければならない。

（解説）

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

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

通信回線として利用する回線は、当該システムで取り扱う情報資産の重要性に応じて、適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り、通信回線の性能低下や異常によるサービス停止を防ぐために、通信回線や通信回線装置を冗長構成にした

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

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

4.4. 職員等の利用する端末や電磁的記録媒体等の管理

【趣旨】

職員等が利用するパソコン、モバイル端末及び電磁的記録媒体等が適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、職員等の利用するパソコン、モバイル端末及び電磁的記録媒体等の盗難及び情報漏えい防止策、持ち出し・持ち込み等に関する対策を規定する。

【例文】

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

②情報システム管理者は、情報システムへのログイン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、端末の電源起動時のパスワード（BIOS パスワード、ハードディスクパスワード等）を併用しなければならない。【推奨事項】

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

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

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

（解説）

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

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

①ログインパスワード

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

②多要素認証の利用

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

③電源起動時のパスワード（BIOS パスワード）

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

④電源起動時のパスワード（ハードディスクパスワード）

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

⑤セキュリティチップの暗号化機能

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

⑥モバイル端末のセキュリティ

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

（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、モバイル端末、通信機器、ケーブル等からは、微弱電磁波が流れている。これらから流れる電磁波から、指向性の高いアンテナを利用して、

情報を盗聴することが技術的には可能である。このため、機密性の非常に高い情報を取り扱う企業等では、電磁波により重要情報が外部に漏えいすることを防止する対策を行うことがある。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。

（注４）モバイル端末の遠隔消去（リモートワイプ）機能は、モバイル端末に電源が入っており、かつ通信状態が良好な場合にしか効果が期待できない点に留意する必要がある。このことから、本機能とあわせて、データを暗号化する等、漏えいしても内容が知られることのない仕組みを合わせて導入することが有効である。

5. 人的セキュリティ

5.1. 職員等の遵守事項

【趣旨】

職員等が情報資産を不正に利用したり、適正な取扱いを怠った場合、コンピュータウイルス等の感染、情報漏えい等の被害が発生し得る。このことから、情報セキュリティポリシーの遵守や情報資産の業務以外の目的での使用の禁止等、職員等が情報資産を取り扱う際に遵守すべき事項を明確に規定する。職員だけでなく、非常勤職員及び臨時職員、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、職員等の過失又は故意による規定違反から生じており、職場の実態等を踏まえつつ、職員等の遵守事項を適正に定めるとともに、規程の実効性を高める環境を整備することが重要である。

【例文】

（１） 職員等の遵守事項

①情報セキュリティポリシー等の遵守

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

②業務以外の目的での使用の禁止

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

③モバイル端末や電磁的記録媒体等の持ち出し及び外部における情報処理作業の制限

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

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

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

④支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用

（ア） 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、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利用することができる。

（イ） 職員等は、支給以外のパソコン、モバイル端末及び電磁的記録媒体等を用いる場合には、情報セキュリティ管理者の許可を得た上で、外部で情報処理作業を行う際に安全管理措置を遵守しなければならない。

⑤持ち出し及び持ち込みの記録

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

⑥パソコンやモバイル端末におけるセキュリティ設定変更の禁止

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

⑦机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報セキュリティ管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適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やモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

（3） 情報セキュリティポリシー等の掲示

情報セキュリティ管理者は、職員等が常に情報セキュリティポリシー及び実施手順を閲覧できるように掲示しなければならない。

（４） 外部委託事業者に対する説明

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

（解説）

（１） 職員等の遵守事項

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

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

①モバイル端末の持ち出し及び外部における情報処理作業

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

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

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

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

（注４）テレワークを導入する場合は、本人確認手段の確保、通信途上の盗聴を防御するために、安全な通信回線サービスを利用しなければならない。その際、通信する情報の機密性に応じて、ファイル暗号化、通信経路の暗号化等の必要な措置を取ることが求められる。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 4 版）」（平成 30 年 4 月　総務省）を参照されたい。

②支給以外のパソコンやモバイル端末等の業務利用

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

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

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

さらに、支給以外の端末から庁内ネットワークに接続を行う可能性がある場合は、情報漏えいを防ぐため、以下のような対策を講じる必要がある。

・シンクライアント環境やセキュアブラウザを使用する
・ファイル暗号化機能を持つアプリケーションでの接続のみを許可する

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

③持ち出し及び持ち込みの記録

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

（注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、パソコンやモバイル端末の機能は、非常勤職員等の業務内容に応じて、不必要な機能については制限することが適切である。

（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、「8.1. 外部委託」を参照のこと。

5.2. 研修・訓練

【趣旨】

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

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

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

【例文】

（1） 情報セキュリティに関する研修・訓練

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

（2） 研修計画の策定及び実施

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

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

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

④研修は、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。

⑤CISO は、毎年度１回、情報セキュリティ委員会に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

（３） 緊急時対応訓練

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

（４） 研修・訓練への参加

幹部を含めた全ての職員等は、定められた研修・訓練に参加しなければならない。

(解説)

（１） 情報セキュリティに関する研修・訓練

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

（２） 研修計画の立案及び実施

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

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

（注２）部外の研修等に、職員等を参加させることも有益である。

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

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

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

また、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者及び職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じた研修を実施することが必要である。これは不正アクセスから情報資産を防御することはもとより、不正プログラムの感染、侵入、内部者による情報の漏えい、外部への攻撃等を防ぐ観点からも重要である。

研修受講を確実にするため、CISO に、毎年度 1 回、情報セキュリティ委員会に対して職員等の研修の実施状況を報告させる義務を負わせておく。

また、CISO は、研修計画を通じて将来の情報セキュリティを担う人材の育成や要

員の管理を行うとともに、地方公共団体の長によるメールでの周知等、研修効果を向上させる施策を講じることが望ましい。

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

（３） 緊急時対応訓練

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

（４） 研修・訓練への参加

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

（注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。

5.3. 情報セキュリティインシデントの報告

【趣旨】

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

なお、報告に対する対応については、「7.3. 侵害時の対応等」による。

【例文】

（1） 庁内での情報セキュリティインシデントの報告

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

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

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

（2） 住民等外部からの情報セキュリティインシデントの報告

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

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

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

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

（3） 情報セキュリティインシデント原因の究明・記録、再発防止等

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

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

に報告しなければならない。

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

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

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

(解説)

（１） 庁内からの情報セキュリティインシデントの報告

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

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

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

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

（２） 住民等外部からの情報セキュリティインシデントの報告

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

（注４）住民からの報告に対しては、適切に処理し、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） 情報セキュリティインシデント原因の究明・記録、再発防止等

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

指示または勧告を行う必要がある。

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

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

5.4. ID及びパスワード等の管理

【趣旨】

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

認証情報等は、人的な原因により漏えいしやすい情報である。情報システム管理者からの認証情報等の発行から職員等での管理に至るまで、人的な原因で情報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ければならない。

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

②統括情報セキュリティ責任者及び情報システム管理者は、IC カード等の紛失等の通報があり次第、当該ICカード等を使用したアクセス等を速やかに停止しなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、IC カード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

（２） IDの取扱い

職員等は、自己の管理するIDに関し、次の事項を遵守しなければならない。

①自己が利用しているIDは、他人に利用させてはならない。

②共用IDを利用する場合は、共用IDの利用者以外に利用させてはならない。

（３） パスワードの取扱い

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

①パスワードは、他者に知られないように管理しなければならない。
②パスワードを秘密にし、パスワードの照会等には一切応じてはならない。
③パスワードは十分な長さとし、文字列は想像しにくいものにしなければならない。
④パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。
⑤複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。
⑥仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。
⑦パソコン等の端末にパスワードを記憶させてはならない。
⑧職員等間でパスワードを共有してはならない。

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

パスワードのメモを作成し、机上、キーボード、ディスプレイ周辺等にメモを置くことは禁止する必要はあるが、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。

6. 技術的セキュリティ

6.1. コンピュータ及びネットワークの管理

【趣旨】

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

【例文】

（1） 文書サーバの設定等

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

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

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

（2） バックアップの実施

統括情報セキュリティ責任者及び情報システム管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施しなければならない。

（3） 他団体との情報システムに関する情報等の交換

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

（4） システム管理記録及び作業の確認

①情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適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） ログの取得等

①統括情報セキュリティ責任者及び情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

②統括情報セキュリティ責任者及び情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適切にログを管理しなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

（7） 障害記録

統括情報セキュリティ責任者及び情報システム管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適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、CISO 及び統括情報セキュリティ責任者の許可を得なければならない。

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

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

④統括情報セキュリティ責任者及び情報システム管理者は、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

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

（１１） 複合機のセキュリティ管理

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

②統括情報セキュリティ責任者は、複合機が備える機能について適切な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。

③統括情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

（１２） 特定用途機器のセキュリティ管理

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

（１３） 無線 LAN 及びネットワークの盗聴対策

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

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

（１４） 電子メールのセキュリティ管理

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

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

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

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

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

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

（１５） 電子メールの利用制限

①職員等は、自動転送機能を用いて、電子メールを転送してはならない。

②職員等は、業務上必要のない送信先に電子メールを送信してはならない。

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

④職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告し

なければならない。

⑤職員等は、ウェブで利用できるフリーメール、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。

（１６） 電子署名・暗号化

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

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

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

（１７） 無許可ソフトウェアの導入等の禁止

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

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

③職員等は、不正にコピーしたソフトウェアを利用してはならない。

（１８） 機器構成の変更の制限

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

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

（１９） 無許可でのネットワーク接続の禁止

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

（２０） 業務以外の目的でのウェブ閲覧の禁止

①職員等は、業務以外の目的でウェブを閲覧してはならない。

②統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関

係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適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ほか、物理的セキュリティ対策を実施する必要がある。

（２） バックアップの実施

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

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

（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） ログの取得等

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

（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。

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

（９） 外部の者が利用できるシステムの分離等

電子申請受付システム、庁舎を訪問した住民等に対する庁舎案内システムなど、外部の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

インターネットに接続し、公開しているウェブサーバ等が、外部から攻撃を受けた場合に、庁内ネットワークへの侵入を可能な限り阻止するために、庁内と外部ネット

ワークの境界にファイアウォールを設置する必要がある。

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

（１１） 複合機のセキュリティ管理

（注７）プリンタ、ファクシミリ、イメージスキャナ、コピー機等の機能が一つにまとめられている機器を「複合機」という。複合機は、庁内ネットワークや公衆電話網等の通信回線に接続して利用されることが多く、その場合には、ウェブによる管理画面を始め、ファイル転送、ファイル共有、リモートメンテナンス等多くのサービスが動作するため、様々な脅威が想定されることに注意が必要である。

（１２） 特定用途機器のセキュリティ管理

（注８）テレビ会議システム、IP 電話システム、ネットワークカメラシステム等の特定の用途に使用される情報システム特有の構成要素であって、通信回線に接続されている又は電磁的記録媒体を内蔵しているものを「特定用途機器」という。これらの機器についても当該機器の特性や取り扱う情報、利用方法、通信回線の接続形態等により想定される脅威に注意が必要である。

（１３） 無線 LAN 及びネットワークの盗聴対策

無線 LAN を利用する場合は、解読が困難な暗号化及び認証技術を使用し、アクセスポイントへの不正な接続を防御する必要がある。

（注９）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１０）無線 LAN の不正利用調査を行い、探査ツール等を用い、無許可のアクセスポイントや使用されていないアクセスポイントが設置されていないことを点検することも有益である。

（１４） 電子メールのセキュリティ管理

メールサーバに対するセキュリティ対策等、電子メールのセキュリティ管理について定める。外部からの電子メール受信及び、外部への電子メール送信においてなりすましを防ぐため、メールサーバのセキュリティ対策として電子署名を用いた DKIM（DomainKeys Identified Mail）や SPF（Sender Policy Framework）等の対策を行うとともに、DMARC（Domain-based Message Authentication, Reporting & Conformance）も行わなければならない。また、電子メールの不正な中継を行わないようにメールサーバを設定しなければならない。外部へ情報を持ち出すために電子

メールが用いられることを考慮し、フィルタリングソフトウェア等による監視を行うことが望ましい。

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

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

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

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

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

（１５） 電子メールの利用制限

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

プロバイダーが提供するサービスである、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、適切なセキュリティ対策を講じる必要がある。

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

（注１４）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。

（１６） 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。

その方法について情報システム管理者は、 暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」を

参照した上で、情報システム及び電子署名のアルゴリズム並びにそれを使用した安全なプロトコル及びその運用方法について、定めなければならない。

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

（１７） 無許可ソフトウェアの導入等の禁止

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

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

（１８） 機器構成の変更の制限

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

（１９） 無許可でのネットワーク接続の禁止

セキュリティ上、ネットワークとの接続には適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１６）特に、庁内で無線 LAN を使用している場合に、職員等や外部委託事業者がパソコンやモバイル端末等を持込み、無許可でアクセスポイントへ接続する行為を禁止する必要がある。

（２０） 業務以外の目的でのウェブ閲覧の禁止

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

6.2. アクセス制御

【趣旨】

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

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

【例文】

（1） アクセス制御等

①アクセス制御

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

②利用者 ID の取扱い

（ア） 統括情報セキュリティ責任者及び情報システム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者 ID の取扱い等の方法を定めなければならない。

（イ） 職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、統括情報セキュリティ責任者又は情報システム管理者に通知しなければならない。

（ウ） 統括情報セキュリティ責任者及び情報システム管理者は、利用されていない ID が放置されないよう、人事管理部門と連携し、点検しなければならない。

③特権を付与された ID の管理等

（ア） 統括情報セキュリティ責任者及び情報システム管理者は、管理者権限等の特権を付与された ID を利用する者を必要最小限にし、当該 ID のパスワードの漏えい等が発生しないよう、当該 ID 及びパスワードを厳重に管理しなければならない。

（イ） 統括情報セキュリティ責任者及び情報システム管理者の特権を代行する者は、統括情報セキュリティ責任者及び情報システム管理者が指名し、CISO が認

めた者でなければならない。

（ウ） CISO は、代行者を認めた場合、速やかに統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者及び情報システム管理者に通知しなければならない。

（エ） 統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID 及びパスワードの変更について、外部委託事業者に行わせてはならない。

（オ） 統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID 及びパスワードについて、職員等の端末等のパスワードよりも定期変更、入力回数制限等のセキュリティ機能を強化しなければならない。

（カ） 統括情報セキュリティ責任者及び情報システム管理者は、特権を付与された ID を初期設定以外のものに変更しなければならない。

（２） 職員等による外部からのアクセス等の制限

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

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

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

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

⑤統括情報セキュリティ責任者及び情報システム管理者は、外部からのアクセスに利用するモバイル端末を職員等に貸与する場合、セキュリティ確保のために必要な措置を講じなければならない。

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

⑦統括情報セキュリティ責任者は、公衆通信回線（公衆無線 LAN 等）の庁外通信回線を庁内ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、利用者の ID 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）による認証に加えて通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講じなければならない。

（３） 自動識別の設定

統括情報セキュリティ責任者及び情報システム管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。【推奨事項】

（４） ログイン時の表示等

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

（５） 認証情報の管理

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

②統括情報セキュリティ責任者又は情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させなければならない。

③統括情報セキュリティ責任者又は情報システム管理者は、認証情報の不正利用を防止するための措置を講じなければならない。

（６） 特権による接続時間の制限

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

（解説）

（１） アクセス制御

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

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

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

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

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

（２） 職員等による外部からのアクセス等の制限

外部から庁内ネットワークや情報システムに接続を認める場合は、外部から攻撃を受けるリスクが高くなることから、本人確認手段の確保、通信途上の盗聴を防御するために、原則、安全な通信回線サービスを利用しなければならない。その際、通信する情報の機密性に応じて、ファイル暗号化、通信経路の暗号化、専用回線の利用等の必要な措置を取ることが求められる。また、接続に当たっては許可制とし、許可は必要最小限の者に限定しなければならない。

（注３）持ち込んだモバイル端末を確認するシステムとして、検疫システムがある。検疫システムとは、OS のパッチやコンピュータウイルス対策ソフトウェアのパターンファイルが最新でない、不正プログラムが侵入しているなど、十分なセキュリティ対策が取られていないモバイル端末を庁内ネットワークに接続させないシステムである。モバイル端末を庁内に持ち帰った場合等に、検疫システムによる確認を義務付けることにより、様々な脅威の発生を防止することができる。

（注４）庁外から庁内のネットワークや情報システムにアクセスする際に公衆無線 LAN 等の庁外通信回線を利用することは原則禁止であるが、やむを得ず利用する場合は、統括情報セキュリティ責任者の許可を得た上で、必要最小限の範囲のみのアクセスとする。さらに、ログを取得し、不正なアクセスがないかを定期的に確認することが求められる。

（３） 自動識別の設定

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

（4） ログイン時の表示等

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

（5） 認証情報の管理

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

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

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

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

（6） 特権による接続時間の制限

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

6.3. システム開発、導入、保守等

【趣旨】

システム開発、導入、保守等において、技術的なセキュリティ対策が十分に行われない場合は、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。また、システム開発のための規則を確立しなければならない。

②システム開発における責任者、作業者の ID の管理

（ア） 情報システム管理者は、システム開発の責任者及び作業者が使用する ID を管理し、開発完了後、開発用 ID を削除しなければならない。

（イ） 情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならならない。

③システム開発に用いるハードウェア及びソフトウェアの管理

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

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

（３） 情報システムの導入

①開発環境と運用環境の分離及び移行手順の明確化

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

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

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

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

②テスト

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

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

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

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

（４） システム開発・保守に関連する資料等の整備・保管

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

②情報システム管理者は、テスト結果を一定期間保管しなければならない。

③情報システム管理者は、情報システムに係るソースコードを適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

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

（７） 開発・保守用のソフトウェアの更新等

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

（８） システム更新又は統合時の検証等

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

（解説）

（１） 情報システムの調達

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

（注１）情報機器及びソフトウェア等の情報セキュリティ機能の評価に当たっては、第三者機関による客観的な評価である、ISO/IEC15408 に基づく IT セキュリティ評価及び認証制度による認証の取得の有無を評価項目として活用すること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、CISO 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。

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

・機密性を高める対策例

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

・完全性を高める対策例

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

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

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

（注７）オンラインでの申請及び届出等の手続を提供するシステムについては、「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」（平成 22 年 8 月 31 日　各府省情報化統括責任者（CIO）連絡会議決定）を参照されたい。

（２）　情報システムの開発

①　システム開発における責任者及び作業者の特定

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

（注８）システム開発において、作業進捗が悪い場合等に、要員の投入が逐次行わ

れるケースがあるが、これらのことが、要員の調整等に不備が生じるケースがある。特に、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、できる限り分離し、セキュリティに配慮した設計にすることが必要である。

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

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

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

② テスト

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

（4） システム開発・保守に関連する資料等の整備・保管

システム開発や機器等の導入において、開発や機器等の導入に関する資料やシステム関連文書等は、保守や機器更新の際に必要となることから、適切に整備し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よう、入力データの範囲

チェックや不正な文字列等の入力を除去する機能を組み込むことが必要になる。

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

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

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

また、ウェブサイトを構築する場合は、「lg.jp」ドメインを含む属性型・地域型 JP ドメイン名の使用を調達仕様書に含めることが望ましい。

（注１２）庁外の者が地方公共団体の名前をタイトルに掲げるなどし、地方公共団体のウェブサイトと誤解されかねないウェブサイトを構築することがあり、これを完全に防ぐことは困難である。このため、以下を例とする対策を実施する必要がある。

・正規のウェブサイトが検索サイトで上位に表示されるよう検索エンジン最適化の措置を実施する

・情報システム管理者は、庁外に提供するウェブサイトに関連するキーワードで定期的にウェブサイトを検索し、不審なサイトが検索結果に表示された場合は、検索サイト事業者に報告するなどの対策を実施する

・以前利用していたドメイン（旧ドメイン）を運用停止する場合は、第三者に不正に取得されないようドメインを一定期間保持する。詳細は「ドメイン管理ガイド(2.0 版)」（平成 28 年 12 月１日 内閣官房情報通信技術（IT）総合戦略室）を参照されたい。

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

・告知するアプリケーション・コンテンツを管理する組織名を明記する

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

・電子メールにて告知する場合は、告知内容についての問合せ先を明記する

（６） 情報システムの変更管理

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

（７） 開発・保守用のソフトウェアの更新等

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

（８） システム更新又は統合時の検証等

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

（注１４）検証等を行う事項としては、例えば次のものがある。

・システム更新又は統合作業時に遭遇する想定外の事象に対応する体制

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

・更新又は統合によって影響される業務運営体制

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

6.4. 不正プログラム対策

【趣旨】

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

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

【例文】

（1） 統括情報セキュリティ責任者の措置事項

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

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

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

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

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

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

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

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

（2） 情報システム管理者の措置事項

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

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

ならない。

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

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

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

（３） 職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

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

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

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

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

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

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

⑦コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、以下の対応を行わなければならない。

（ア） パソコン等の端末の場合

LAN ケーブルの即時取り外しを行わなければならない。

（イ） モバイル端末の場合

直ちに利用を中止し、通信を行わない設定への変更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。

（解説）

（１） 統括情報セキュリティ責任者の措置事項

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

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

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

（２） 情報システム管理者の措置事項

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

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

（３） 職員等の遵守事項

職員等には、不正プログラムに関する情報及び対策を周知して対策を徹底することが必要であり、特に、不審なメールやファイルの削除、不正プログラム対策ソフトウェアを常に最新の状態に保たせることが重要である。コンピュータウイルスに感染した兆候がある場合には、即座に LAN ケーブルを取り外す（パソコン等の端末の場

合）又は通信を行わない設定への変更（モバイル端末の場合）を行い、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。

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不要なサービスについて、機能を削除又は停止しなければならない。

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

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

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

（2） 攻撃への対処

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

（3） 記録の保存

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

（4） 内部からの攻撃

統括情報セキュリティ責任者及び情報システム管理者は、職員等及び外部委託事

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

（５） 職員等による不正アクセス

統括情報セキュリティ責任者及び情報システム管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適切な処置を求めなければならない。

（６） サービス不能攻撃

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

（７） 標的型攻撃

統括情報セキュリティ責任者及び情報システム管理者は、情報システムにおいて、標的型攻撃による内部への侵入を防止するために、教育や自動再生無効化等の人的対策や入口対策を講じなければならない。また、内部に侵入した攻撃を早期検知して対処するために、通信をチェックする等の内部対策を講じなければならない。

（解説）

（１） 統括情報セキュリティ責任者の措置事項

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

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

（注２）DNS の導入時には以下の対策を講じなければならない。

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

・DNS キャッシュポイズニング攻撃から保護するための措置を講ずる。

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

（注３）庁内の CSIRT を活用して CISO への報告、各部部局への指示、ベンダとの情報共有及び報道機関への通知・公表などの対応を行うとともに、地方公共

団体情報システム機構（自治体 CEPTOAR）等の関係機関や他の地方公共団体の同様の窓口機能、外部の事業者等と連携して情報共有を行うことが望ましい。

（２） 攻撃への対処

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

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

（３） 記録の保存

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

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

（４） 内部からの攻撃

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

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

（５） 職員等による不正アクセス

職員等が庁内にあるパソコンやモバイル端末を利用し、不正アクセスを発見した場合には、情報セキュリティ管理者に通知し、適切な措置を求めなければならない。

（６） サービス不能攻撃

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

①情報システムを構成する機器の装備している機能による対策の実施

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

・通信事業者と協議し、サービス不能攻撃が発生時の対処手順や連絡体制を整備

する。

②サービス不能攻撃を想定した情報システムの構築

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

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

・サービス不能攻撃の影響を排除又は低減するための専用の対策装置を導入する。

③通信事業者の提供するサービスの利用

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

④情報システムの監視及び監視記録の保存

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

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

（7） 標的型攻撃

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

①人的対策例（標的型攻撃メール対策）

・差出人に心当たりがないメールは、たとえ興味のある件名でも開封しない。

・不自然なメールが着信した際は、差出人にメール送信の事実を確認する。

・メールを開いた後で標的型攻撃と気付いた場合、添付ファイルは絶対に開かず、メールの本文に書かれた URL もクリックしない。

・標的型攻撃と気付いた場合、システム管理者に対して着信の事実を通知し、組織内への注意喚起を依頼した後に、メールを速やかに削除する。

・システム管理者は、メールやログを確認し、不正なメールがなかったかチェックする。（事後対策）

②電磁的記録媒体に対する対策例

・出所不明の電磁的記録媒体を内部ネットワーク上の端末に接続させない。

・電磁的記録媒体をパソコン等の端末に接続する際、不正プログラム対策ソフトウェアを用いて検査する。

・パソコン等の端末について、自動再生（オートラン）機能を無効化する。

・パソコン等の端末について、電磁的記録媒体内にあるプログラムを媒体内から直接実行することを拒否する。

③ネットワークに対する対策例

・ネットワーク機器のログ監視を強化することにより、情報を外部に持ち出そうとするなどの正常ではない振る舞いや外部との不正な通信を確認し、アラームを発したりその通信を遮断する。

・不正な通信がないか、ログをチェックする。（事後対策）

6.6. セキュリティ情報の収集

【趣旨】

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

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

（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ほかに、JPCERT/CC（一般社団法人 JPCERT コーディネーションセンター)、IPA（独立行政法人 情報処理推進機構）等がある。

（３） 情報セキュリティに関する情報の収集及び周知

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

（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 24 年 10 月 26 日改定 情報セキュリティ政策推進会議決定)、「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC（Cryptography Research and Evaluation Committees）暗号リスト)」（平成 28 年 3 月 29 日 総務省・経済産業省）及び同リストを策定した CRYPTREC の今後の報告を参考とすることができる。

（注７）SSL/TLS 暗号設定については、「SSL/TLS 暗号設定ガイドライン Ver2.0」(CRYPTREC 平成 30 年 5 月 8 日)を参照されたい。

（注８）IPv6 への移行については、IPv6 通信を導入する場合における他の情報システムへの影響や、IPv6 通信を想定していないネットワークに接続される全ての情報システム及びネットワークに対する IPv6 通信を抑止するための措置、IPv6 通信を想定していないネットワークを監視し、IPv6 通信が検知された場合には通信している装置を特定し、IPv6 通信を遮断するための措置を考慮する必要がある。

（注９）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。なお、Java、WindowsXP、Windows Vista、Windows7 及び Windows Server 2003、Windows Server 2008 等のサポート期限に関しては、総務省が発出した注意喚起文書等を参照されたい。

7. 運用

7.1. 情報システムの監視

【趣旨】

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

【例文】

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

②統括情報セキュリティ責任者及び情報システム管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じなければならない。

③統括情報セキュリティ責任者及び情報システム管理者は、外部と常時接続するシステムを常時監視しなければならない。

(解説)

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

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

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

7.2. 情報セキュリティポリシーの遵守状況の確認

【趣旨】

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

【例文】

（１） 遵守状況の確認及び対処

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

②CISOは、発生した問題について、適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） パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

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

（３） 職員等の報告義務

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

②違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると統括情報セキュリティ責任者が判断した場合は、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、CISOは速やかに対処する必要がある。

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

（２） パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

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

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

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

（３） 職員等の報告義務

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

7.3. 侵害時の対応等

【趣旨】

情報セキュリティインシデント、システム上の欠陥及び誤動作並びに情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害事案が発生した場合に、迅速かつ適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

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

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

（4） 緊急時対応計画の見直し

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

(解説)

（1） 緊急時対応計画の策定

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

緊急時対応計画には、情報資産に対するセキュリティ侵害が発生した場合等における連絡、証拠保全、被害拡大の防止、復旧等の迅速かつ円滑な実施と、再発防止策

の措置を講じるために必要な事項を定める必要がある。

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

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

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

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

（２） 緊急時対応計画に盛り込むべき内容

緊急時対応計画に定める事項としては、例えば次のものがある。

①関係者の連絡先

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

②発生した事案に係る報告すべき事項

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

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

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

（注３）統括情報セキュリティ責任者が事案の詳細な調査を行うに当たっては、必要に応じて外部専門家のアドバイスを受ける、JPCERT/CC（一般社団法人 JPCERT コーディネーションセンター）及び地方公共団体情報システム機構（自治体 CEPTOAR）等の関係機関に相談する等、事実確認を見誤らないように努める必要がある。

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

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

③発生した事案への対応措置

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

・サイバーテロそのほか市民に重大な被害が生じるおそれのあるとき
→地方公共団体の長、CISO、都道府県の関係部局、警察、影響が考えられる個人及び法人に連絡

・不正アクセスそのほか犯罪と思慮されるとき
→地方公共団体の長、CISO、都道府県の関係部局、警察に連絡

・踏み台となって他者に被害を与えるおそれがあるとき
→地方公共団体の長、CISO、都道府県の関係部局、警察に連絡

・情報システムに関する被害
→情報システム管理者、必要と認められる事業者に連絡

・その他情報資産に係る被害
→関係部局等に連絡

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

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

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

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

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

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

（オ） 事案に係るシステムのログ及び現状を保存する。

（カ） 事案に対処した経過を記録する。

（キ） 事案に係る証拠保全の実施を完了するとともに、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（若しくは、ICT部門における業務継続計画）を策定することが重要である。ただし、業務継続計画と情報セキュリティポリシーの間に矛盾があると、職員等は混乱し、適切な対応をとることができなくなるおそれがあるため、各地方公共団体において業務継続計画を策定する際には、情報セキュリティポリシーとの整合性をあらかじめ検討し、必要があれば、情報セキュリティポリシーを改定しなければならない。

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

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

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

（４） 緊急時対応計画の見直し

緊急時対応計画の実効性を確保するため、新たな脅威の出現等の情報セキュリティに関する環境の変化や組織体制の変化等を盛り込んだ最新の内容となるよう、

定期的に見直すことが必要である。また、緊急時対応計画の発動した場合を仮定した訓練や机上試験を定期的に実施しておくことも、緊急時対応計画の実効性を確保する観点から重要である。

7.4. 例外措置

【趣旨】

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

【例文】

（１） 例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティ関係規定を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用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、CISO 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 CISO に報告しなければならない。

（３） 例外措置の申請書の管理

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

（解説）

例外措置は、情報セキュリティポリシーの適用を例外的に排除するものであることから、その承認は、ポリシーの適用が著しく行政事務の遂行を妨げる、緊急を要し通常の手続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。

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

7.5. 法令遵守

【趣旨】

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

【例文】

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

①地方公務員法（昭和 25 年法律第 261 号）
②著作権法（昭和 45 年法律第 48 号）
③不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）
④個人情報の保護に関する法律（平成 15 年法律第 57 号）
⑤行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）
⑥サイバーセキュリティ基本法（平成 28 年法律第 31 号）
⑦○○市個人情報保護条例（平成○○年条例第○○号）

（解説）

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

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

7.6. 懲戒処分等

【趣旨】

情報セキュリティポリシーの遵守事項に対して、職員等が違反した場合の事項を定めておくことは、情報セキュリティポリシー違反の未然防止に、一定の効果が期待される。このことから、情報セキュリティポリシー違反に対する懲戒処分の規定及び懲戒に係る手続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CISO及び当該職員等が所属する課室等の情報セキュリティ管理者に通知しなければならない。

8. 外部サービスの利用

8.1. 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外部委託事業者を選定し、契約で遵守事項を定めるとともに、定期的に対策の実施状況を確認する必要がある。

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

なお、個別団体が単独で外部委託する場合だけでなく、共同アウトソーシングやクラウドサービス利用の形態等により地方公共団体が共同で外部委託する場合にも対策を行う必要があることに留意する。

【例文】

（1） 外部委託事業者の選定基準

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

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

③情報セキュリティ管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない。

（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、外部委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

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

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

（３） 確認・措置等

情報セキュリティ管理者は、外部委託事業者において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CISOに報告しなければならない。

（解説）

（１） 外部委託事業者の選定基準

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

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

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

・外部委託事業者に提供する情報の委託事業者における目的外使用の禁止
・外部委託事業者における情報セキュリティ対策の実施内容及び管理体制
・外部委託事業の実施にあたり、外部委託事業者の組織又はその従業員、再委託事業者、若しくはその他の者による意図せざる変更が加えられないための管理体制
・外部委託事業者の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供
・情報セキュリティ要件の適切な実装
・情報セキュリティの観点に基づく試験の実施
・情報セキュリティインシデントへの対処方法
・情報セキュリティ対策その他の契約の履行状況の確認方法
・情報セキュリティ対策の履行が不十分な場合の対処方法

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

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

（注３）ホスティングサービスの利用等においては、サービス提供者側のミスや機器の故障などの不測の事態によりデータの消失などの事態が発生するおそれ

があるため、情報システムや取り扱う情報の重要度に応じたバックアップなどの必要な対策を講じておく必要がある。なお、ホスティング時のデータ消失に関する対策については、「ホスティングサービス等利用時におけるデータ消失事象への対策実施及び契約内容の再確認等について（注意喚起）」（平成 24 年 7 月 6 日　総務省 事務連絡）を参照されたい。

（2） 契約項目

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

①情報セキュリティポリシー及び情報セキュリティ実施手順の遵守

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

②外部委託事業者の責任者、委託内容、作業者、作業場所の特定

外部委託事業者の責任者や作業者を明確にするとともに、これらの者が変更する場合の手続きを定めておき、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委託事業者に許可する情報の種類とアクセス範囲、アクセス方法

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

⑤従業員に対する教育の実施

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

⑥提供された情報の目的外利用及び受託者以外の者への提供の禁止

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

⑦業務上知り得た情報の守秘義務

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

⑧再委託に関する制限事項の遵守

一般的に、再委託した場合、再委託事業者のセキュリティレベルは下がることが懸念されるために、再委託は原則禁止する。例外的に再委託を認める場合には、再

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

⑨委託業務終了時の情報資産の返還、廃棄等

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

⑩委託業務の定期報告及び緊急時報告義務

定期報告及び緊急時報告の手順を定め、委託業務の状況を適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。

⑪地方公共団体による監査、検査

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

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

⑫地方公共団体による情報セキュリティインシデントの公表

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

⑬情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

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

（注４）これらの契約項目については、「地方公共団体における業務の外部委託事業者に対する個人情報の管理に関する検討」報告書（平成 21 年 3 月　総務省）を参照し、「個人情報の取扱いに関する特記仕様書（雛型）」を活用されたい。

（注５）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６）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７）クラウド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クラウドサービスの利用に当たっては、クラウドサービス事業者の事業所の場所に関わらず、データセンターの存在地の国の法律の適用を受ける場合があることに留意する必要がある。具体的には、クラウドサービス事業者のサービスの利用を通じて海外のデータセンター内に蓄積された地方公共団体の情報が、データセンターの設置されている国の法令により、日本の法令では認められていない場合であっても海外の当局による情報の差し押さえや解析が行われる可能性があるため、住民情報等の機密性の高い情報を蓄積する場合は、日本の法令の範囲内で運用できるデータセンターを選択する必要がある。

なお、クラウド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。

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

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

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

（３）　確認・措置等

情報セキュリティ管理者は、外部委託事業者において十分なセキュリティ対策がなされているか、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セキュリティ侵害行為が発見された場合には、速やかに CISO に報告を行う。

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

8.2. 約款による外部サービスの利用

【趣旨】

民間事業者が約款に基づきインターネット上で無料で提供する情報処理サービス等を利用する場合には、リスクを十分踏まえた上で利用を判断し、適切なセキュリティ対策を講じる必要がある。

【例文】

（１）約款による外部サービスの利用に係る規定の整備

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

①約款によるサービスを利用して良い範囲

②業務により利用する約款による外部サービス

③利用手続及び運用手順

（２）約款による外部サービスの利用における対策の実施

職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

（解説）

（１） 約款による外部サービスの利用に係る規定の整備

有料、無料に関わらず、約款への同意及び簡易なアカウントの登録により当該機能を利用可能なサービスは約款による外部サービスとなる。この代表例としては、以下のものがある。

・電子メール

・ファイルストレージ

・グループウェア等のクラウドサービス　など

なお、電気通信サービスや郵便、運送サービス等は約款による外部サービスの適用範囲外である。

また、約款による外部サービスを利用する場合は、約款の範囲内でのサービス利用となり、特約等を個別に締結することが困難であることが多い。このため、リスクを十分踏まえた上で利用を判断し、セキュリティ対策を適切に講ずる必要がある。具体的には次の事項が考えられる。

①約款による外部サービスの利用手順を定める

・利用申請の許可権限者の決定

・利用申請時の申請内容

－利用する組織名

－利用するサービス
－利用目的（業務内容）
－利用期間
－利用責任者（利用アカウントの責任者）　など

②サービス利用中の安全管理に係る運用手順を定める

・サービス機能の設定（例えば情報の公開範囲）に関する定期的な内容確認
・情報の滅失、破壊等に備えたバックアップの取得
・利用者への定期的な注意喚起
・情報セキュリティインシデント発生時の連絡体制

（２）約款による外部サービスの利用における対策の実施

約款による外部サービスの利用を検討する際は、当該サービスの約款、利用規約、その他の利用条件を確認し、利用の必要性を判断した上、セキュリティ対策も適切に講ずる必要がある。具体的には次の事項が考えられる。

・政府機関の関心事項等の情報が分析され、漏えいすることを防ぐため、利用端末や送信元をインターネット上で匿名化する対策の導入を検討することが望ましい。
・外部サービスの提供事業者において情報セキュリティインシデントが発生した場合に備えて、約款に基づき、対処方法（対処手順、責任分界、対処体制等）について契約前に確認しなければならない。
・サーバ装置の故障や運用手順誤りに等により、サーバ装置上の情報が滅失し復元不可能となる場合に備えてバックアップを取得する
・サービスの突然の停止に備え、予め代替サービスを確認しておく
・約款や利用規約が予告なく一方的に変更され、セキュリティ設定が変更される場合や一度記録された情報を確実に消去できない場合に備え、サービスで取り扱うことのできる情報をあらかじめ定めておく　等

（注１）グループメールサービスの業務利用においても、その設定によってはメールの内容が外部から閲覧可能な状態となり、必要なセキュリティが確保できない場合があるため利用を禁止する必要がある。やむを得ず利用する場合は、利用の要否を十分に検討の上、必要な対策を講じた上で利用する。なお、グループメールサービス利用時の注意喚起については、「グループメールサービスの利用について（注意喚起）」（平成 25 年 7 月 11 日 総務省　事務連絡）を参照されたい。

8.3. ソーシャルメディアサービスの利用

【趣旨】

住民への情報提供など、ソーシャルメディアサービスを利用する場合は、約款による外部サービスを利用することが多くなるが、なりすましやサービス停止のおそれがあるため、ソーシャルメディアサービスによる情報発信時の対策を講じる必要がある。

【例文】

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

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

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

②機密性２以上の情報はソーシャルメディアサービスで発信してはならない。

③利用するソーシャルメディアサービスごとの責任者を定めなければならない。

（解説）

ソーシャルメディアサービスの利用

インターネット上における、ブログ、ソーシャルネットワーキングサービス、動画共有サイト等のソーシャルメディアサービスは、積極的な広報活動等に利用することができるが、外部サービスを利用せざるを得ず、第三者によるなりすましやアカウントの乗っ取り、予告なしでサービスが停止するといった事態が発生する可能性がある。そのため、利用にあたっては、ソーシャルメディアサービスの運用ポリシーや運用手順を定め、ルールに沿った利用を行うことが求められる。具体的には次の事項が考えられる。

①なりすまし対策

・庁内で管理しているウェブサイト内において、利用するソーシャルメディアサービスのサービス名と当該アカウントページへのハイパーリンクを明記するページを設ける。

・運用しているソーシャルメディアサービスの自由記述欄において、庁内ウェブサイト上のページの URL を記載する。

・ソーシャルメディアサービスの提供事業者が、「認証アカウント（公式アカウント）」と呼ばれるアカウントの発行を行っている場合は、これを利用する。

②アカウント乗っ取り対策

・パスワードを適切に管理する。

・二段階認証やワンタイムパスワード等、アカウント認証の強化策が提供されてい

る場合は、可能な限り利用する。

・ソーシャルメディアサービスへのログインに利用する端末が不正アクセスや盗難されないよう、最新のセキュリティパッチや不正プログラム対策ソフトウェアの導入、端末管理等のセキュリティ対策を行う。

③サービスが終了・停止した場合の対応

・あらかじめ発信した情報のバックアップを庁内に保管しておく等、スムーズに別のサービスへの移行が行えるよう適切な準備をしておく。

9. 評価・見直し

9.1. 監査

【趣旨】

情報セキュリティポリシーの実施状況について、客観的に専門的見地から評価を行う監査が実施されない場合は、情報セキュリティ対策が徹底されない状態や情報セキュリティポリシーが業務に沿わない状態が続くおそれがある。このことから、監査の実施及びその方法について規定する。

監査を行う者は、十分な専門的知識を有するものでなければならない。また、適正な監査の実施の観点から、監査の対象となる情報資産に直接関係しない者であることが望ましい。また、地方公共団体内の情報セキュリティ対策の監査・報告について中立性を保証され、監査に必要な情報へのアクセス等の権限が明確に与えられる必要がある。監査作業に伴う情報の漏えいのリスクを最小限とするため、監査人等が取り扱う監査に係る情報について、漏えい、紛失等が発生しないように保管する必要がある。

【例文】

（1） 実施方法

CISO は、情報セキュリティ監査統括責任者を指名し、ネットワーク及び情報システム等の情報資産における情報セキュリティ対策状況について、毎年度及び必要に応じて監査を行わせなければならない。

（2） 監査を行う者の要件

①情報セキュリティ監査統括責任者は、監査を実施する場合には、被監査部門から独立した者に対して、監査の実施を依頼しなければならない。

②監査を行う者は、監査及び情報セキュリティに関する専門知識を有する者でなければならない。

（3） 監査実施計画の立案及び実施への協力

①情報セキュリティ監査統括責任者は、監査を行うに当たって、監査実施計画を立案し、情報セキュリティ委員会の承認を得なければならない。

②被監査部門は、監査の実施に協力しなければならない。

（4） 外部委託事業者に対する監査

外部委託事業者に委託している場合、情報セキュリティ監査統括責任者は外部委託事業者から下請けとして受託している事業者も含めて、情報セキュリティポリシーの遵守について監査を定期的に又は必要に応じて行わなければならない。

（５） 報告

情報セキュリティ監査統括責任者は、監査結果を取りまとめ、情報セキュリティ委員会に報告する。

（６） 保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適切に保管しなければならない。

（７） 監査結果への対応

CISOは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。

（８） 情報セキュリティポリシー及び関係規程等の見直し等への活用

情報セキュリティ委員会は、監査結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（解説）

（１） 実施方法

情報セキュリティ対策状況に対して、定期的な監査だけでなく、様々な状況に対応して監査が行えることを定めておく必要がある。随時監査を行うことを明確にすることにより、情報セキュリティポリシーの違反行為に対する抑止効果も期待できる。

（２） 監査を行う者の要件

内部監査、外部監査、いずれの場合も、監査人は、監査対象範囲から独立性を有し、公平な立場で客観的に評価を行うことが求められる。監査人は、監査及び情報セキュリティについて、十分な専門的知識を有する者でなければならない。

（注１）一部又は全部の監査対象範囲に対して、小規模な組織等の理由によって、独立性を維持することができない場合又は組織内に十分な専門的知識を有する者が確保できない場合は、必要な範囲に対して外部の監査人を利用することを検討することが必要である。また、職員等が自らが所属しないその他の部門に対して監査をする相互監査や近隣の地方公共団体との相互監査も有効である。

（注２）監査人は、監査項目が実施できているか否かだけでなく適切な記録が取得されているかについても確認する必要がある。また、監査項目が実施できていない又は適切な記録が取得されていない場合は、なぜできていないのかその原因にまで踏み込んで分析・報告できることが望ましい。

（３） 監査実施計画の立案及び実施への協力

情報セキュリティ監査統括責任者は、情報セキュリティ監査を行うに当たって、監査人の権限、監査実施に関する項目及び内容を定め、これに基づいて監査実施計画を立案する。監査人は、この計画に基づき監査を実施する。なお、システムに対する監査の実施によって業務が中断される可能性があるため、計画の立案に当たっては中断のリスクを最小限に抑えるよう配慮することが必要である。また、システム監査を行うツールにより、監査人は特権的にデータ等へアクセスし得ることから、誤用・悪用を防止するための適切な管理が求められる。

（注３）情報セキュリティ監査統括責任者は、監査計画及びそれに付随するリスクを効果的かつ効率的に管理するのに必要な資質、並びに次の領域における知識及び技能を有することが望ましい。ただし、必要な資質、並びに知識及び技能を有することが困難な場合は、外部の専門家をあてて能力を補完することも考えられる。

・監査の原則、手順及び方法に関する知識
・マネジメントシステム規格及び基準文書に関する知識
・被監査部門の業務、製品及びプロセスに関する知識
・被監査部門の業務及び製品に関し、適用される法的及びその他の要求事項に関する知識
・該当する場合には、被監査部門の利害関係者に関する知識

また、情報セキュリティ監査統括責任者は、監査計画を管理するのに必要な知識及び技能を維持するために適切な専門能力の継続的開発・維持活動に積極的にかかわることが望ましい。

（注４）監査項目には、庁内外において発生した情報セキュリティインシデントから学んだ対策等の遵守状況の確認や、電磁的記録媒体の管理、情報の持ち出し管理、ソフトウェアライセンス管理、FAX 誤送信防止策等の具体的な情報セキュリティ対策の運用状況の確認も含まれることが望ましい。

（４） 外部委託事業者に対する監査

情報システムの運用、保守等を外部委託している場合は、情報資産の管理が契約に従い適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、セキュリティ侵害行為に対する抑止効果も期待できる。

（５） 報告

情報セキュリティ監査統括責任者は、監査調書をもとに、被監査部門に対する監査人の指摘事項の正確性や指摘に対する改善提案の実現性を確認し監査報告書を作成し、監査報告書を情報セキュリティ委員会に報告する。

CISO は、監査報告を受けて、被監査部門に改善を指示する。被監査部門は、改善計画を立案し実施する。最後に監査人は、フォローアップ監査により、改善状況や改善計画の完了について確認を行う必要がある。

（６） 保管

監査により作成した監査調書には、脆弱性の情報等機微な情報が含まれていることが多いことから、情報セキュリティ監査統括責任者は、紛失等が生じないように保管する必要がある。

（７） 監査結果への対応

監査結果を適切にセキュリティ改善に結び付けるため、CISO に関係部局への指示を義務付けた規定である。また、監査の指摘事項と同種の課題が他の部署にも存在する場合があることから、当該可能性の高い部署に対しては、課題や問題点の有無を確認させる必要がある。

（８） 情報セキュリティポリシー及び関係規程の見直し等への活用

監査結果は、情報セキュリティポリシー及び関係規程の見直し等の基礎資料として活用しなければならない。

（注５）情報セキュリティ監査の実施方法等については、「地方公共団体における情報セキュリティ監査に関するガイドライン」（平成 30 年 X 月　総務省）及び「地方公共団体情報セキュリティ管理基準解説書」（平成 17 年 2 月　総務省）を参考にされたい。

9.2. 自己点検

【趣旨】

情報セキュリティポリシーの履行状況等を自ら点検、評価することは、情報セキュリティポリシーの遵守事項を改めて認識できる有効な手段である。自己点検は、情報システム等を運用する者又は利用する者自らが実施するので、監査のような客観性は担保されないが、監査と同様に、点検結果を踏まえ各部門で改善を図ったり、組織全体のセキュリティ対策の改善を図る上での重要な情報になる情報セキュリティ対策の評価を行い、対策の見直しに資するものである。また、職員等の情報セキュリティに関する意識の向上や知識の習得にも有効である。

このことから、自己点検を定期的に実施する規定を設け、その活用方法とあわせて規定する。

【例文】

（1） 実施方法

①統括情報セキュリティ責任者及び情報システム管理者は、所管するネットワーク及び情報システムについて、毎年度及び必要に応じて自己点検を実施しなければならない。

②情報セキュリティ責任者は、情報セキュリティ管理者と連携して、所管する部局における情報セキュリティポリシーに沿った情報セキュリティ対策状況について、毎年度及び必要に応じて自己点検を行わなければならない。

（2） 報告

統括情報セキュリティ責任者、情報システム管理者及び情報セキュリティ責任者は、自己点検結果と自己点検結果に基づく改善策を取りまとめ、情報セキュリティ委員会に報告しなければならない。

（3） 自己点検結果の活用

①職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

②情報セキュリティ委員会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用しなければならない。

（解説）

（１） 実施方法

情報セキュリティ対策の実施状況について、定期的な自己点検だけでなく、様々な状況に対応して自己点検を実施する。

（注１）自己点検は自己点検票を用いた、アンケート方式で行う場合が多い。アンケートを行う場合に留意すべき点は、そのセキュリティ対策上担う役割に応じたアンケート項目とすることである。アンケートは、回答者による再認識や新たな発見にもつながり得る。アンケート項目によって、自部門の対策で、何が欠落しているのか鮮明にすることが可能になるために、改善の必要性の認識をさせられる効果もある。

（注２）保有する個人情報の人的な要因による漏えいを踏まえた点検については、「地方公共団体の保有する情報資産の管理状況等の再点検について（周知）」（平成 24 年 10 月 29 日　総務省　総行情第 71 号）及び「地方公共団体における個人情報の漏洩防止対策について（注意喚起）」（平成 25 年 8 月 5 日　総務省　事務連絡）を参照されたい。

（注３）技術的な脆弱性の悪用に対する点検については、「地方公共団体等が管理するウェブサイトに係る脆弱性の確認及び対策の点検・実施等について（依頼）」（平成 24 年 9 月 26 日　総務省　総行情第 66 号）を参照されたい。

（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４）総務省が平成 18 年 3 月に公表した「地方公共団体の情報セキュリティレベルの評価に係る制度の在り方に関する調査研究報告書」の参考資料である「情報セキュリティレベル評価ツール」を自己点検に用いることも可能である。

9.3. 情報セキュリティポリシー及び関係規程等の見直し

【趣旨】

情報セキュリティ対策は、情報セキュリティに関する脅威や技術等の変化に応じて、必要な対策が変化するものであり、情報セキュリティポリシー及び関係規程等は、定期的に見直すことが求められる。また監査や自己点検の結果等から、同ポリシー及び関係規程等の見直しの必要性が確認される場合もある。

このことから、情報セキュリティポリシー及び関係規程等の見直しについて規定する。

【例文】

情報セキュリティ委員会は、情報セキュリティ監査及び自己点検の結果並びに情報セキュリティに関する状況の変化等をふまえ、情報セキュリティポリシー及び関係規程等について毎年度及び重大な変化が発生した場合に評価を行い、必要があると認めた場合、改善を行うものとする。

(解説)

情報セキュリティ委員会は、情報セキュリティインシデント、監査や自己点検の結果を受けて、情報セキュリティ分野の専門家による評価等を活用しつつ、情報セキュリティポリシー及び関係規程等の見直しを行う。

また、情報セキュリティポリシー及び関係規程等は、組織にとっての脅威の変化や組織体制の変更、新たな対策技術の提供等によっても見直すべきものであり、あらかじめ定めた間隔及び重大な変化が発生した場合等、状況に応じて柔軟に運用していくことが必要である。

(注１) 見直しに当たっては、情報セキュリティポリシー及び関係規程等と実態との相違を十分考慮することが重要であり、関係部局から意見聴取等を行い、実態把握を行うことが望ましい。また、情報セキュリティポリシー及び関係規程等を見直す際には、必要に応じてリスク分析の見直しを行うことが重要である。日頃から新たな攻撃方法や対策技術の情報収集に努め、情報セキュリティポリシー及び関係規程等の見直しに活用することも必要である。

(注２) 情報セキュリティポリシー及び関係規程等の見直しは、地方公共団体の長及びこれに準じる者の決裁により正式に決定される。

(注３) 情報セキュリティポリシー及び関係規程等を見直した際には、その内容を職員等や外部委託事業者に十分に周知する必要がある。

(注４) 見直しの際は、情報セキュリティポリシー及び関係規程等に次の事項によって生じる要求事項が含まれているか確認すること。

・事業計画

・規制、法令及び契約

・現在及び将来予想される情報セキュリティの脅威環境

10. 用語の定義

本ガイドラインにおいて次の各号に掲げる用語の定義は、当該各号に定めるところによる。

【あ】

●「遠隔消去機能」

「遠隔消去機能」→「リモートワイプ機能」を参照。

【か】

●「供給者」

「供給者」とは、サプライチェーンの一部を構成し、データの処理やサービス等で連携する組織をいう。

【さ】

●「サプライチェーン」

「サプライチェーン」とは、部品やサービス等の供給に多種多様な主体が係わった取引の連鎖をいう。

●「シンクライアント」

「シンクライアント」とは、サーバ側に仮想的なクライアント環境を設けた上で、当該クライアント環境にパソコンやモバイル端末が専用のアプリケーションを使用してアクセスし、パソコンやモバイル端末にデータを保存せずに、データの閲覧や編集を行うことを可能とする機能をいう。

●「事業継続計画」

「事業継続計画」→「BCP」を参照。

●「情報セキュリティインシデント」

「情報セキュリティインシデント」とは、望まない単独若しくは一連の情報セキュリティ事象、又は予期しない単独若しくは一連の情報セキュリティ事象であって、業務の遂行を危うくする確率及び情報セキュリティを脅かす確率が高いものをいう。

●「情報セキュリティ事象」

情報セキュリティ方針への違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象

●「送信ドメイン認証技術」

「送信ドメイン認証技術」とは、メール送信者情報のドメインが正しいものかどうかを検証することができる仕組みをいう。現在のメール送信においては、送信者情報を詐称することが可能で、実際、多くの迷惑メールは他のアドレスになりすまして送られているため、成りすまし対策として用いられる。

●「ソーシャルメディアサービス」

「ソーシャルメディアサービス」とは、インターネット上で展開される情報メディアのあり方で、組織や個人による情報発信や個人間のコミュニケーション、人の結びつきを利用した情報流通などといった社会的な要素を含んだメディアのことをいう。利用者の発信した情報や利用者間のつながりによってコンテンツを作り出す要素を持ったWeb サイトやネットサービスなどを総称する用語で、電子掲示板(BBS)やブログ、動画共有サイト、動画配信サービス、ショッピングサイトの購入者評価欄などを含む。

【た】

●「端末」

「端末」とは、情報システムの構成要素である機器のうち、職員が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいい、特に断りが無い限り、地方公共団体が調達又は開発するものをいう。

●「電子署名」

「電子署名」とは、情報の正当性を保証するための電子的な署名情報をいう。

●「特権 ID」

「特権 ID」とは、サーバの起動や停止、アプリケーションのインストールやシステム設定の変更、全データへのアクセスなど、通常の ID よりもシステムに対するより高いレベルでの操作が可能な ID をいう。

●「ドメイン名」

「ドメイン名」とは、国、組織、サービス等の単位で割り当てられたネットワーク上の名前であり、英数字及び一部の記号を用いて表したものをいう。

【な】

●「二要素認証」

「二要素認証」とは、二つの認証方式を組み合わせて認証する方式をいう。認証方式は大きく分けて、ID/パスワードなど対象者の知識を利用したもの、USB トークンやスマートカードなど対象者の持ち物を利用したもの、バイオメトリクスなど対象者の身体の特徴を利用したもの、の 3 つに分かれる。通常はこのうちどれか一つを利用して認証を行うが、それぞれに一長一短があり、単一の方法で精度を高めるには限度があるため、このうちの二つの認証方式を組み合わせてセキュリティを高める方式である。

【は】

●「パソコン」

「パソコン」とは、端末のうち、机の上等に備え置いて業務に使用することを前提とし、移動させて使用することを目的とはしていないものをいい、端末の形態は問わない。

●「標的型攻撃」

「標的型攻撃」とは、明確な意思と目的を持った人間が特定のターゲットや情報に対して特定の目的のために行うサイバー攻撃の一種をいう。

【ま】

●「モバイル端末」

「モバイル端末」とは、端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。

【や】

●「約款による外部サービス」

「約款による外部サービス」とは、民間事業者等の庁外の組織が約款に基づきインター

ネット上で提供する情報処理サービスであって、当該サービスを提供するサーバ装置において利用者が情報の作成、保存、送信等を行うものをいう。ただし、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除く。

【ら】

●「リスク分析」

「リスク分析」とは、リスク特定、リスク分析、リスク評価を網羅するプロセス全体を指す。リスク分析を行った後、リスク対応を行う。リスク対応の手段には、リスク源の除去、起こりさすさの変更、結果の変更、他者とのリスクの共有、リスクの保有などがある。

●「リモートワイプ機能」

「リモートワイプ機能」とは、携帯電話などに記録してあるデータを、当該端末から操作するのではなく離れた場所から、遠隔操作（リモート）で、消去、無効化する機能をいう。携帯電話を紛失したり盗難にあった場合の、情報漏えいを防ぐ目的で利用される。

【A～Z】

●「BCP（Bussness Continuity Plan：事業継続計画）」

「BCP」とは、組織において特定する事業の継続に支障をきたすと想定される自然災害、人的災害・事故、機器の障害等の事態に組織が適切に対応し目標とする事業継続性の確保を図るために当該組織において策定する、事態の予防及び事態発生後の事業の維持並びに復旧に係る計画をいう。

●「CRYPTREC（Cryptgraphy Research and Evaluation Commmittiees）」

「CRYPTREC」とは、電子政府推奨暗号の安全性を評価・監視し、暗号モジュール評価基準等の策定を検討するプロジェクトである。

●「CSIRT（Computer Security Incident Response Team）」

「CSIRT」とは、コンピュータやネットワーク（特にインターネット）上で何らかの問題（主にセキュリティ上の問題）が起きていないかどうか監視すると共に、万が一問題が発生した場合にその原因解析や影響範囲の調査を行ったりする組織の総称。

●「URL（Uniform Resource Locator）」

「URL」とは、インターネット上の情報資源の場所とその属性を指定する記述方式。 情

報資源の種類やアクセス方法、情報を提供するウェブサーバの識別名、ファイルの所在を指定するパス名などで構成される。

●「VPN (Virtual Private Network)」

「VPN」とは、暗号技術等を利用し、インターネット等の公衆回線を仮想的な専用回線として利用するための技術である。

第４編

付録

（目次）

権限・責任等一覧表

付録1　　権限・責任等一覧表

（目次）

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	情報セキュリティ委員会	最高情報セキュリティ責任者	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	（統一的窓口）CSIRT	関係規定外部委託
1 組織体制	(1)	①	最高情報セキュリティ責任者の設置		○									
		②	最高情報セキュリティアドバイザーの設置		○									
		③	CSIRTの整備		○									
	(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	情報資産に対するセキュリティ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	最高情報セキュリティ責任者等との連絡体制の整備		△	○	△	△	△	△				
		⑧	緊急時の報告と回復のための対策		△	○								
	(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	情報資産に対するセキュリティ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											
	(9)	①	CSIRTの整備		○									
		②	CSIRTに属する職員の選任		○	△	△	△	△					
		③	情報セキュリティに関する統一的な窓口の設置		○									
		④	セキュリティ戦略の意思決定が行われた際に、内容を関係部局等に提供		△	△	△	△	△				○	
		⑤	情報セキュリティインシデントの関係機関機関への報告										○	
		⑥	情報セキュリティインシデントの報道機関への通知・公表等										○	
		⑦	情報セキュリティに関する他の関係機関や窓口等との情報共有										○	

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	情報セキュリティ委員会	最高情報セキュリティ責任者	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	（統一的窓口）CSIRT	関係規定外部委託
2 情報資産の分類と管理	(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電磁的記録媒体の取扱い									○		
		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電磁的記録媒体の保管					○	○					
			(ウ)	利用頻度の低い電磁的記録媒体等の保管					○	○					
			(エ)	電磁的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 情報システム全体の強靭性の向上	(1)	①		マイナンバー利用事務系と他の領域との分離		○	○								
		②	(ア)	情報のアクセス対策									○		
			(イ)	情報の持ち出し不可設定									○		
	(2)	①		LGWAN接続系とインターネット接続系の分割		○	○								
	(3)	①		高度な情報セキュリティ対策		○	○								
		②		自治体情報セキュリティクラウドの導入		○	○								

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	情報セキュリティ委員会	最高情報セキュリティ責任者	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	CSIRT（統一的窓口）	外部委託関係規定
4 物理的セキュリティ	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)		庁外への機器の設置		承	○			○					
		(7)		機器の廃棄等の措置						○					
	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	消火薬剤等の設置方法			○			○					
		(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						○			△		
	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			○								
			②	外部へのネットワーク接続の限定措置			○								
			③	行政系ネットワークのLGWANへの集約			○								
			④	通信回線に利用する回線の選択等			○								
			⑤	回線の十分なセキュリティ対策の実施			○								
			⑥	機密性の高い情報を扱う通信回線の可用性の確保			○								
	4．4 職員等の利用する端末や電磁的記録媒体等の管理		①	パソコン、モバイル端末等の盗難防止措置						○					
			②	情報システムへのログインパスワードの設定						○					
			③	端末の電源起動時のパスワード設定等措置						○					
			④	多要素認証の設定						○					
			⑤	パソコン、モバイル端末等におけるデータの暗号化等の利用						○					
			⑥	モバイル端末に対する遠隔消去機能の利用						○					

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	情報セキュリティ委員会	最高情報セキュリティ責任者	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	ティ監査責任者情報セキュリ	職員等の義務	（統一的窓口）CSIRT	関係規定外部委託
5 人的セキュリティ	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					△				○		
			②		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)	モバイル端末や電磁的記録媒体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				○		
			④	(ア)	支給以外のパソコン、モバイル端末及び電磁的記録媒体等の業務利用禁止					許				○		
				(イ)	支給以外のパソコン、モバイル端末及び電磁的記録媒体等の安全管理措置					許				○		
			⑤		端末等の持出及び持込の記録等					○						
			⑥		パソコンやモバイル端末におけるセキュリティ設定変更の禁止					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					○				△		
			②		非常勤職員等の採用時の同意書への署名					○				△		
			③		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					○						△
	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		研修計画の策定等	承	○									
			②		情報セキュリティ研修の受講									○		
			③		新規採用の職員等に対する研修の設定		○							△		
			④		理解度等に応じた研修の実施		○	△	△	△	△	△		△		
			⑤		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									○		
	5．3 情報セキュリティインシデントの報告	(1)	①		情報セキュリティインシデントの報告					△				○	△	
			②		情報システムに関連する情報セキュリティインシデントの報告			△		○	△				△	
			③		情報セキュリティインシデント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					△				○		
			②		情報システム又はネットワークに関連する情報セキュリティインシデントの報告			△		○	△					
			③		情報セキュリティインシデントの必要に応じた報告		△		△	○						
			④		住民等外部に対する窓口の設置等		○									
		(3)	①		情報セキュリティインシデントの可能性に対する評価										○	
			②		情報セキュリティインシデントの報告		△								○	
			③		応急措置の実施及び復旧に係る指示			△	△	△	△	△		△	○	
			④		情報セキュリティインシデント原因の究明、再発防止策の報告		△								○	
			⑤		再発防止策に必要な措置の指示		○								△	

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	情報セキュリティ委員会	最高情報セキュリティ責任者	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	CSIRT（統一的窓口）	外部委託関係規定
	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への常時挿入禁止									○		
				(ウ)	ICカード等紛失時の通報			△			△			○		
			②		ICカード紛失時のアクセス停止措置			○			○					
			③		ICカード切り替え時の旧カードの廃棄方法			○			○					
		(2)	①		自己のIDの他人による利用の禁止									○		
			②		共用ID利用者以外による共用ID利用禁止									○		
		(3)	①		パスワードの管理									○		
			②		パスワードの秘密保持									○		
			③		パスワードの文字の選択									○		
			④		パスワードの流出したおそれのある時の措置					△				○		
			⑤		パスワードのシステム間の共有禁止									○		
			⑥		仮パスワードの変更									○		
			⑦		パスワードの記憶機能の利用禁止									○		
			⑧		職員等間でのパスワード共有禁止									○		
6 技術的セキュリティ	6．1 コンピュータ及びネットワークの管理	(1)	①		文書サーバの容量の設定等						○					
			②		文書サーバの課室等単位での設定						○					
			③		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			○			○					
		(3)			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						○					
			②		システム変更等時の作業内容記録作成等			○			○					
			③		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		ログの取得等			○			○					
			②		ログの管理			○			○					
			③		ログの点検・分析			○			○					
		(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			○								
			②		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			○					
			②		外部ネットワークの接続による影響確認						○					
			③		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						○					
			④		ファイアウォール等の設置			○			○					
			⑤		問題発生時の物理的な遮断			△			○					

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	情報セキュリティ委員会	最高情報セキュリティ責任者	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	CSIRT（統一的窓口）	外部委託関係規定
		(11)	①		複合機を調達する場合のセキュリティ要件の策定			○								
			②		複合機に対するセキュリティ設定と情報セキュリティインシデント対策の実施			○								
			③		複合機の運用終了時の対策			○								
		(12)	①		特定用途機器に対する対策の実施			○								
		(13)	①		無線LAN利用時の暗号化等の使用義務設定			○								
			②		機密性の高いネットワークへの暗号化等の措置			○								
		(14)	①		電子メールの中継処理禁止の設定			○								
			②		スパム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			○								
		(15)	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									○		
		(16)	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		○							○		
			③		電子署名の正当性を確認する手段の提供		○									
		(17)	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									○		
		(18)	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			○		
		(19)			無許可でのネットワーク接続の禁止			許						○		
		(20)	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			○		△						
	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			○			○					
				(カ)	特権付与されたIDの初期設定以外のものへの変更			○			○					

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	情報セキュリティ委員会	最高情報セキュリティ責任者	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	CSIRT（統一的窓口）	関係規定外部委託
		(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									○		
			⑦		公衆通信回線等の庁内ネットワークへの接続禁止			○								
		(3)			自動識別の設定			○			○					
		(4)			ログイン時のシステム設定						○					
		(5)	①		職員等の認証情報の管理等			○			○					
			②		パスワード発行等			○			○					
			③		認証情報の不正利用防止			○			○					
		(6)			特権によるネットワーク等への接続時間の制限						○					
	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と規則の確立						○					
			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						○					
				(エ)	導入されるシステムやサービスの可用性の確保確認						○					
			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						○					
				(エ)	受け入れ時の別々の組織でのテストの実施						○					
		(4)	①		システム開発等の資料等の整備・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						○					

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	情報セキュリティ委員会	最高情報セキュリティ責任者	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	CSIRT（統一的窓口）	外部委託関係規定
	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			○								
			⑦		サポート終了ソフトウェアの使用禁止			○								
		(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電磁的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、無害化処理の実施									○		
			⑥		ウイルス情報の確認			△						○		
			⑦	(ア)	パソコン等の端末のウイルス感染時の対処方法									○		
				(イ)	モバイル端末の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			○								
	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		不要なサービス機能の削除、停止			○								
			③		ウェブページの改ざんを防止するための設定			○			△					
			④		定期的なファイルの改ざんの有無の検査			○								
			⑤		監視、通知、外部連絡窓口などの体制及び連絡窓口の構築			○							○	
		(2)			攻撃を受けた場合、または受けた可能性への対応		○	○								
		(3)			攻撃を受けた記録の保存		○	○								
		(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			○		△	○					
		(6)			サービス不能攻撃対策の実施			○			○					
		(7)			標的型攻撃対策の実施			○			○					
	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			○			○					

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	情報セキュリティ委員会	最高情報セキュリティ責任者	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	（統一的窓口）CSIRT	外部委託関係規定
7 運用	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			○			○					
	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)			モバイル端末及び電磁的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			○								
	7.3 侵害時の対応等	(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	○	○									
	7.4 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		○									
	7.5 法令遵守				主要な法令遵守									○		
	7.6 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		△	○		△						
8 外部サービスの利用	8.1 外部委託	(1)	①		外部委託事業者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					○						○
			③		クラウドサービス利用時の機密性に応じたセキュリティレベルの確認					○						
		(2)			契約項目											○
		(3)			外部委託事業者のセキュリティ確保の確認等		△	△		○						○
	8.2 約款による外部サービスの利用	(1)	①	(ア)	約款によるサービスを利用可能な範囲の規定					○						
				(イ)	業務により利用できる約款によるサービスの範囲の規定					○						
				(ウ)	約款によるサービスの利用手続及び運用手順の規定					○						
		(2)	①		約款によるサービスの利用における対策の実施									○		
	8.3 ソーシャルメディアサービスの利用	(1)	①	(ア)	なりすまし対策の実施					○						
				(イ)	不正アクセス対策の実施					○						
		(2)			機密性2以上の情報の発信禁止					○						
		(3)			利用するソーシャルメディアサービスごとの責任者の決定					○						

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	情報セキュリティ委員会	最高情報セキュリティ責任者	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	CSIRT（統一的窓口）	外部委託関係規定
9 評価・見直し	9．1 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及び関係規程等の見直し等への活用	○										
	9．2 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及び関係規程等の見直し等への活用	○										
	9．3 情報セキュリティポリシー及び関係規程等の見直し			情報セキュリティポリシー及び関係規程等の見直しに関する規定	○										

自治体情報セキュリティ
強化対策事業実施要領
（その１）
（自治体情報システム強靭性向上事業）

付録2　　自治体情報セキュリティ強化対策事業実施要領（その１）（自治体情報システム強靭性向上事業）

（目次）

自治体情報セキュリティ強化対策事業実施要領（その１）
（自治体情報システム強靭性向上事業）

自治体情報セキュリティ強化対策事業（補助金名：地方公共団体情報セキュリティ強化対策費補助金）の自治体情報システム強靭性向上事業については、この要領を参照の上、実施するものとする。

なお、自治体情報セキュリティクラウド事業については、「自治体情報セキュリティ強化対策事業実施要領（その２）」を参照されたい。

第1 【手順１】ネットワーク接続ルールの確認

１．現有サーバが保持する情報の性質に応じて外部との接続関係を整理する

（１）主に従来基幹系システムとして整理されてきた情報資産(個人番号利用事務系)

個人番号利用事務、住基と密接に係る戸籍事務等に供する情報システム(ハードウェア、ソフトウェア、ネットワーク等)及びデータ。代表的なシステムには、住基、税務、社会保障、戸籍等がある。主に従来は、基幹系システムとして整理されてきたインターネットと接続する必要がない情報資産。

（２）主に従来情報系システムとして整理されてきた情報資産

主に従来は、情報系システムとして整理されてきた情報資産。ＬGWAN及びインターネットに接続されることが多かったが、今般のマイナンバー制度の施行を受けて、次のとおり分割することが望まれる。

① ＬGWAN接続系情報資産

個人番号関係事務等に供する情報システム(ハードウェア、ソフトウェア、ネットワーク等)及びデータ。代表的なシステムには、人事給与、財務会計、文書管理等がある。LGWAN がマイナンバーによる情報連携に活用されることから、特にインターネットのリスクとの分離が望まれる。

② インターネット接続系情報資産

インターネットメール、Ｗｅｂ閲覧、ＣＭＳ等に利用する情報システム(ハードウェア、ソフトウェア、ネットワーク等)及びデータ。従来は情報系システムの一機能として整理されることが一般的であったが、今回の整理によってLGWAN接続系とは分割して、新たに分類されることが望まれる情報資産である。

２．必要な外部接続条件を整理一覧化する

個人番号利用事務系、ＬGWAN接続系、インターネット接続系それぞれが接続する外部ネットワークを洗い出し、ネットワーク接続情報として整理一覧化する。

（参考１「自治体情報システムに係るサーバ・端末別の接続ネットワーク」）

（1）個人番号利用事務系

外部接続として、住基ネット、マイナンバー制度における中間サーバ連携や住民票の写し等のコンビニ交付用のＬＧＷＡＮ接続、データバックアップセンターや共同利用／クラウドセンター等、十分にセキュリティが確保された特定通信先と限定的に接続することが必要である。

なお、外部接続先も、インターネット等と接続されていてはならないことも留意する。また、ＯＳアップデートやウイルス対策ソフトのパターンファイルの更新等においても、インターネットに接続して利用しないことに留意すべきである。

（2）ＬＧＷＡＮ接続系

ＬＧＷＡＮメール、ＬＧＷＡＮ－ＡＳＰ等の特定通信先と限定的に接続する。直接インターネットと接続しないことに留意すること。インターネットとの接続する場合については、例えばインターネットへのメール発信と、インターネット接続系にてＨＴＭＬメールのテキスト化や添付ファイルの削除が行われた受信メールの取込み等の無害化された通信とすることを図る。

（3）インターネット接続系

外部接続としてインターネットが含まれるため、ＩＰＳ・ＩＤＳ、ふるまい検知等の導入を始めとする自治体情報セキュリティクラウドの利用等、高度なセキュリティ対策を検討する必要がある。

（4）管理系

ユーザーや機器の認証に用いられる認証サーバや、情報システムの運用上必要となる監視やバックアップの管理サーバは、必要に応じて各ネットワークに設置される必要があるが、個人番号利用事務系とＬＧＷＡＮ接続系の認証サーバや管理サーバ同士の同期等については、リスクから隔離された専用ネットワークとして通信することの検討も必要な場合がある。

なお、インターネット接続系のサーバ等の管理が必要な場合は、別途インターネット接続系管理ネットワークを検討すること。

第2 【手順２】サーバ間接続ルールの確認

サーバ間の接続ルールについて次のとおり確認する。

1．接続先サーバを確認する

各サーバについて、その接続先サーバ及びアクセスの内容(通信プロトコル、データ等)を洗い出す。接続先サーバとネットワークを超えて接続されている場合には、各ネットワークの許容できる接続範囲、アクセスの内容を超えていないことを確認する。

２．サーバ間接続ルールを確認する

先に確認した各サーバの接続先情報と、手順１で整理したネットワーク接続情報を照合し、サーバ間接続情報が外部接続条件に抵触していないことを確認する。

３．サーバ間接続情報を整理一覧化する

先に確認した各サーバの接続先ネットワーク及び接続先サーバを一覧化し、サーバ間接続情報として整理一覧化する。

（参考２「サーバ間連携イメージ」）

第3 【手順３】端末接続ルールの確認

１．端末が接続するサーバを確認する

団体内の端末（ＰＣ）を洗い出し、それぞれ個人番号利用事務系、ＬＧＷＡＮ接続系、インターネット接続系のどのサーバに接続すべきかを確認する。

２．端末接続ルールを確認する

（１）個人番号利用事務系

各端末について、その接続先サーバ及びアクセスの内容（通信プロトコル、データ等）が、接続条件に抵触していないことを確認する。

（２）ＬＧＷＡＮ接続系

各端末について、その接続先サーバ及びアクセスの内容(通信プロトコル、データ等)が、接続条件に抵触していないことを確認する。なお、特に秘匿性の高い情報を取り扱う業務を除いては、一台の端末で複数の業務を取り扱うことも想定される。

（３）インターネット接続系

各端末について、その接続先サーバ及びアクセスの内容(通信プロトコル、データ等)が接続条件に抵触していないことを確認する。

３．端末接続情報を整理一覧化する

先に確認した各端末の接続先ネットワーク及び接続先サーバを一覧化し、端末接続情報として整理一覧化する。

（参考３「端末アクセスコントロール」）

第4 【手順４】追加整備が必要なネットワーク機器の洗い出し

１．ネットワーク機器を整理一覧化する

先に確認した、ネットワーク接続情報、サーバ間接続情報、端末接続情報に基づき、実際にネットワークを敷設する際に必要となるネットワーク機器(メインスイッチ、フロアスイッチ、島ハブ、ＦＷ等)を配備先フロア・組織単位に整理して現有するネットワーク機器と照合し、追加整備が必要なネットワーク機器を整理一覧化する。(参考４「組織別　端末ポート数イメージ」)

第5 【手順５】必要な経費の算出

先に整理したネットワーク接続情報、サーバ間接続情報、端末接続情報に基づき、必要な対応策にかかる経費を算出する。

１．追加機器に係る経費を算出する。

２．作業に係る経費を算出する。

＜要件対応算出上の留意点＞

（１）ＬＧＷＡＮとインターネットの分割※

※分割：一旦両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにすること。

①　ハードウェア

・メインスイッチ(Ｌ３ＳＷ)：既存機器を利用(分割に伴うＶＬＡＮ等の設定変更)する。既存機器を利用できない場合は新設する。

・フロアスイッチ(Ｌ２ＳＷ)：各フロアでネットワーク環境分割のために必要な台数を確保する。本庁舎、出先機関等でフロア毎に概ね１台設置を基本とするが、フロアの規模等により適切な設置台数を算出する。既存機器の流用を検討し、不足分について新設する。

・島ハブ：各フロアのＬ２ＳＷ、端末台数により適切な設定台数を算出する。既存機器の流用を検討し、不足分について新設する。

・ＦＷ：環境分割後において、特定の通信に限定する設定を行うために必要台数を確保する。既存機器の流用を検討し、不足分について新設する。

・認証サーバ：個人番号利用事務系、ＬＧＷＡＮ接続系、インターネット接続系にそれぞれ認証サーバを設置する。既存機器を流用できる場合は、不足する側のサーバのみ新設する。(認証サーバ：Active Directory 等※のユーザー認証・管理用ディレクトリ・サービスのサーバを指す)

※サーバＯＳバンドル品等を使用する。

② 作業経費

環境の分割に必要なネットワーク設計、各機器の設定、テスト、ネットワーク工事等の経費を算出する。

（２）無害化メールの通信の一例

メール無害化の方式として、インターネット環境で受信したインターネットメールの添付ファイルの削除、及びＨＴＭＬメールのテキスト化を行い、本文のみをＬＧＷＡＮ接続系に転送する方式を採用した場合の算出の考え方を以下に示す。この場合、メール転送に必要な特定サーバ間以外の通信を遮断するとともに、ＬＧＷＡＮ環境とインターネット環境はＳＭＴＰ以外のＷｅｂ通信を始めとするプロトコルを遮断することを前提とする。

① ハードウェア

・サーバ：ＬＧＷＡＮ接続系、インターネット接続系それぞれにメールサーバを設置する。既存機器を流用できる場合は、不足する側のサーバのみ新設する。

② ソフトウェア

・ソフト本体：インターネット側に、インターネットメールの添付ファイルを削除しＬＧＷＡＮ接続系へメールを出来るサーバーソフトウェアを利用する。既存メールサーバーソフトウェアを利用できる場合は、無害化・転送の設定を追加してこれを活用する。

③ 作業経費

メール無害化、メール転送に必要な設定作業に関わる経費を算出する。

第6 【手順６】個人番号利用事務における対策

１．個人番号利用事務に係る端末への二要素認証の導入の検討

① ハードウェア

・サーバ：端末台数に応じて必要な能力（メモリ、ＣＰＵ、ネットワーク性能等）を確保する。(既存の仮想サーバの空き等を積極的活用すること。)

・認証装置：端末台数分を確保する。

② ソフトウェア

・ソフト本体：端末台数に応じた必要な性能要件を保有したソフトウェアを選定する。

・端末(ユーザー)ライセンス：端末台数分(ユーザー数等、製品に準じる)を確保する。

③　作業経費

二要素認証導入に必要なサーバ構築、端末設定等の最低限必要な経費を算出する。

２．個人番号利用事務に係る端末への外部媒体による情報持ち出し禁止の検討

①　ハードウェア

・サーバ：端末台数に応じて必要な能力（メモリ、ＣＰＵ、ネットワーク性能等）を確保する。(既存の仮想サーバの空き等を積極的活用すること。

②　ソフトウェア

・ソフト本体：端末台数に応じて必要な性能要件を保有したソフトウェアを選定する。

・端末(ユーザー)ライセンス：端末台数分(ユーザー数等、製品に準じる)を確保する。

③　作業経費

持出し禁止設定に必要なサーバ構築、端末設定等の最低限必要な経費を算出する。

第7 【手順７】要件シートのその他各項目の検討

参考５「自治体情報システム強靭性向上モデル要件シートの一例」を参考に、その他の各項目についても、手順５、６に準じて検討する。

参考１．自治体情報システムに係るサーバ・端末別の接続ネットワーク

配置すべきセグメント	業務システム名			サーバ/端末	インターネット分離環境	LGWAN等専用回線	インターネット接続環境		LGWAN・インターネットなど外部のネットワークに接続させている理由	端末のあり方
							連携あり	参照のみ		
	住民記録									
個人番号利用事務系	住民記録 利用	住民基本台帳（既存住基）		サーバ	○					
				端末	○					専用
		印鑑証明		サーバ	○					
				端末	○					専用
		選挙		サーバ	○					
				端末	○					専用
		法務省情報連携（外国人住民）		端末		○			「法務省市町村連携サーバ」と接続するため	（法務省配付専用品PC）
	戸籍	戸籍		サーバ	○					
				端末	○					専用
		戸籍副本		市区町村専用装置		○			法務局の「戸籍副本データ管理システム」に接続するため	（法務省配付専用品サーバ相当PC）
	証明書自動交付	自動交付機		サーバ	○					
				端末	○					専用
		コンビニ交付（LGWANセルフASP）		サーバ		○				
				端末		○			J-LISの「証明書交付センター」と接続するため	専用
		コンビニ交付（LGWAN-ASP）		端末		○				専用
	宛名管理									
個人番号利用事務系	宛名管理	統合宛名		サーバ	○					
				端末	○					専用
		団体内統合宛名		サーバ		○				
				端末		○				専用
	中間サーバー関連	管理端末		端末		○			J-LISの「中間サーバー・プラットフォーム（LGWAN-ASP）」と接続するため	専用
		中間サーバー接続端末		端末		○				専用
	税									
個人番号利用事務系	税 利用	個人住民税		サーバ	○					
				端末	○					専用
		法人住民税		サーバ	○					
				端末	○					専用
		固定資産税		サーバ	○					
				端末	○					専用
		軽自動車税		サーバ	○					
				端末	○					専用
			軽自動車検査情報	端末		○			J-LISの「軽自動車検査情報の提供システム」と接続するため	専用
		収滞納管理		サーバ	○					
				端末	○					専用
			地方税電子申告（eLTAX）	端末		○			認定委託先事業者の「審査サーバ・受信サーバ」（※）および「地方税電子化協議会の「ポータルセンタ」に接続するため （※）都道府県・指定都市はオンプレミスの場合あり インターネット参照がある場合がある	専用
			電子収納［Pay-easy、コンビニ交付］	端末		○			「公金収納システム」に接続するため	専用
			ふるさと納税（LGWAN-ASP）	端末		○				専用
	社会保障									
個人番号利用事務系	生活保護 利用			サーバ	○					
				端末	○					専用
	国民年金 利用			サーバ	○					
				端末	○					専用
	国民健康保険 利用	国民健康保険		サーバ	○					
				端末	○					専用
		国保連合会接続端末		端末		○			保険者用ネットワーク経由で国保連合会の「国保総合システム」に接続するため	専用
	後期高齢者医療 利用	後期高齢者医療		サーバ	○					
				端末	○					専用
		後期高齢者医療制度広域連合電算処理システム（標準システム）		端末		○			各後期高齢者医療連合の「標準システム」に接続するため	専用
	介護保険 利用	介護保険		サーバ	○					
				端末	○					専用
		国保連合会接続端末		端末		○			保険者用ネットワーク経由で国保連合会の「介護保険審査・支払等システム」に接続するため	専用
	ひとり親医療 利用			サーバ	○					
				端末	○					専用
	老人医療 利用			サーバ	○					
				端末	○					専用
	障害者医療 利用			サーバ	○					
				端末	○					専用
	障害者福祉			サーバ	○					
				端末	○					専用
	児童福祉	児童手当 利用		サーバ	○					
				端末	○					専用
		児童扶養手当 利用		サーバ	○					
				端末	○					専用
		特別児童扶養手当 利用		サーバ	○					
				端末	○					専用
		子ども・子育て 利用		サーバ	○					
				端末	○					専用
			子ども・子育て支援全国総合システム	端末		○			内閣府の「子ども・子育て支援全国総合システム」に接続するため	専用
	健康管理 利用			サーバ	○					
				端末	○					専用
	特定健診 利用			サーバ	○					
				端末	○					専用

利用　：個人番号利用事務　　関係　個人番号関係事務

配置すべきセグメント	業務システム名		サーバ/端末	インターネット分離環境	LGWAN等専用回線	インターネット接続環境		LGWAN・インターネットなど外部のネットワークに接続させている理由	端末のあり方
						連携あり	参照のみ		
	地方公営事業								
	上下水道管理	上下水道管理	サーバ	○					
			端末	○					専用
個人番号利用事務系	公営住宅管理 利用	公営住宅管理（オンプレミス）	サーバ	○					
			端末	○					専用
		公営住宅管理（LGWAN-ASP）	サーバ		○				
			端末		○				専用
	内部情報系								
LGWAN接続系	人事給与 関係		サーバ	○					
			端末	○					専用
	財務会計 関係	財務会計	サーバ	○					
			端末	○					専用
		地方財政決算情報管理	サーバ		○			総務省の「地方財政決算管理情報システム」に接続するため	
			端末		○				専用
	庶務事務 関係		サーバ	○				旅費計算等でインターネット上のサービスと連携する接続する場合がある	
			端末	○					共用
	文書管理		サーバ	○					
			端末	○					共用
	ファイルサーバ		サーバ	○					
			端末	○					共用
	グループウェア		サーバ	○					
			端末	○					共用
	防災								
LGWAN接続系	J-ALERT	受信機	専用装置		○			LGWANによる地上回線から受信のため（衛生通信のバックアップ）	
		エリアメール転送用	端末			○		通信キャリアのエリアメール転送用	専用
	Em-Net		端末		○			緊急メール受信のため	共用
	安否情報システム		サーバ		○			LGWANによる都道府県・国への通信のため	
			端末		○				専用
	調達・施設予約								
	電子申請（オンプレミス）		サーバ	○		○		インターネットからの受付のため	
			端末	○		○		外部・内部サーバの両方がある	専用
	電子申請（LGWAN-ASP）		端末		○				専用
	電子調達（オンプレミス）		サーバ	○		○		インターネットからの受付のため	
			端末	○		○		外部・内部サーバの両方がある	専用
	電子調達（LGWAN-ASP）		端末		○				専用
	工事実績情報（CORINS）		端末				○	公共工事の実績を確認するため	共用
	施設予約（オンプレミス）		サーバ	○		○		インターネットからの受付のため	
			端末	○		○		外部・内部サーバの両方がある	専用
	施設予約（LGWAN-ASP）		端末		○				共用
	図書館		サーバ	○		○		インターネットからの受付のため	
			端末	○		○		外部・内部サーバの両方がある	専用
	メール/インターネットアクセス								
LGWAN接続系	LGWAN掲示板		サーバ		○				
			端末		○				共用
	LGWANメール		サーバ		○				
			端末		○				共用
インターネット接続系	インターネットメール		サーバ			○			
			端末			○			共用
	WEBアクセス		サーバ			○			
			端末			○			共用
	ホームページ/作成等		サーバ			○			
			端末			○			共用

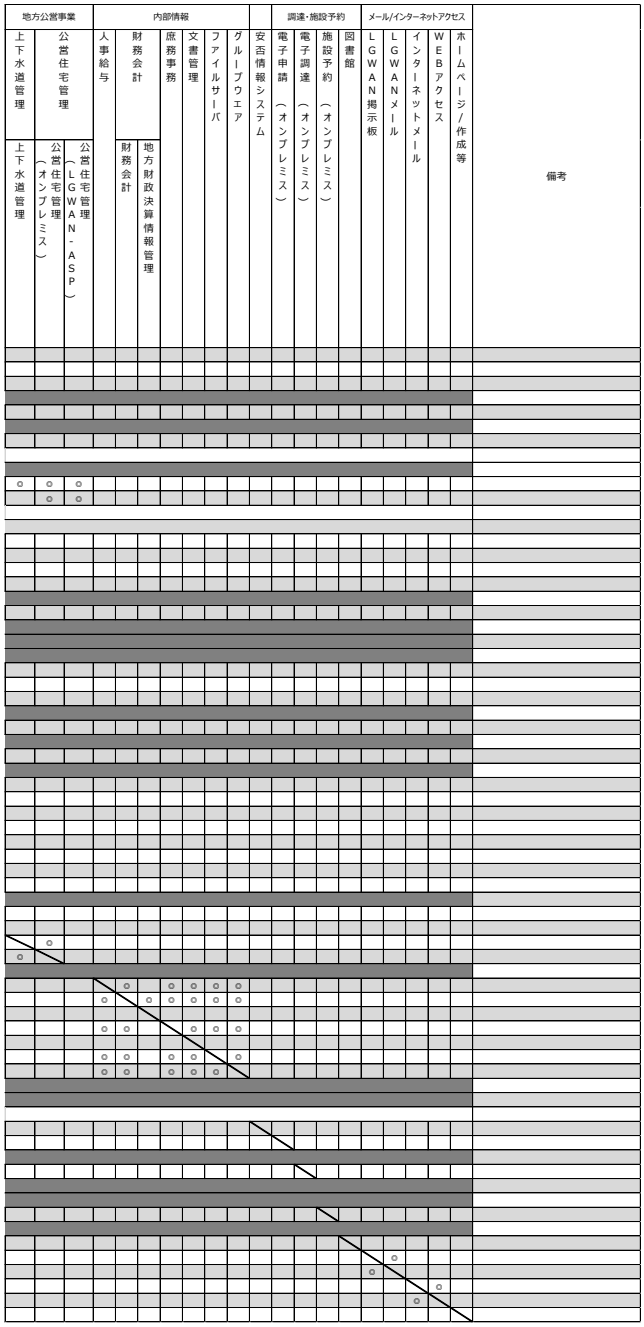
利用　：個人番号利用事務　　関係　個人番号関係事務

参考２. サーバ間連携イメージ

・各行に記載したサーバから、各列のどのサーバと連携を許可するか一例を示したもの。

は端末のみ自庁内に存在し、サーバは庁内でなく外部に存在するものであり、本資料の対象外

連携元のサーバ ＼ 連携先のサーバ			住民記録								宛名管理		税					社会保障																		
			住民記録			戸籍		証明書自動交付			宛名管理		税					生活保護	国民年金	国民健康保険	後期高齢者医療	介護保険	ひとり親医療	老人医療	障害者医療	障害者福祉	児童福祉					健康管理	特定健診
			（既存住基）住民基本台帳	印鑑証明	選挙	戸籍	戸籍副本	自動交付機	コンビニ交付（LGWANセルフASP）	コンビニ交付（LGWAN-ASP）	統合宛名	団体内統合宛名	個人住民税	法人住民税	固定資産税	軽自動車税	収滞納管理			国民健康保険	後期高齢者医療	介護保険					児童手当	児童扶養手当	特別児童扶養手当	子ども子育て		
住民記録	住民記録	住民基本台帳（既存住基）		○	○	○					○	○																					
		印鑑証明						○	○	○																							
		選挙	○																														
		法務省情報連携（外国人住民）	LGWAN上の「法務省市町村連携サーバ」と接続																														
	戸籍	戸籍					○	○	○	○																							
		戸籍副本	LGWAN経由にて法務局の「戸籍副本データ管理システム」に接続																														
	証明書自動交付	自動交付機							○	○																							
		コンビニ交付（LGWANセルフASP）						○		○																							
		コンビニ交付（LGWAN-ASP）	LGWAN経由にて「証明書交付センター」と接続										LGWAN経由にて「証明書交付センター」と接続																				
宛名管理	宛名管理	統合宛名	○					○	○			○	○		○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
		団体内統合宛名									○		○																			○	○
	中間サーバー関連	管理端末	暗号装置を経由しLGWAN上にある中間サーバー・プラットフォームへ接続																														
		中間サーバー接続端末	暗号装置を経由しLGWAN上にある中間サーバー・プラットフォームへ接続																														
税	税	個人住民税						○	○	○	○	○					○																
		法人住民税						○	○	○	○	○					○																
		固定資産税						○	○	○	○	○					○																
		軽自動車税						○	○	○	○	○					○																
		軽自動車検査情報	LGWAN経由にてJ-LISの「軽自動車検査情報の提供システム」と接続																														
		収滞納管理									○	○	○	○	○	○																	
		地方税電子申告（eLTAX）	「審査サーバ・受付サーバ」および地方税電子化協議会のポータルセンターに接続するため。																														
		電子収納［Pay-easy、コンビニ交付］	LGWANとしては専用線にて「公金収納システム」に接続																														
		ふるさと納税（LGWAN-ASP）	LGWANを経由してシステムと連携																														
社会保障	生活保護										○	○																					
	国民年金																																
	国民健康保険	国民健康保険									○	○																					
		国保連合会接続端末	保険者用ネットワークを経由して国保連合会の「国保総合システム」に接続するため																														
	後期高齢者医療	後期高齢者医療																															
		後期高齢者医療制度広域連合電算処理システム（標準システ	専用ネットワークを通じて後期高齢者医療広域連合の標準システムに接続するため																														
	介護保険	介護保険									○	○																					
		国保連合会接続端末	保険者用ネットワークを経由して国保連合会の「介護保険審査・支払等システム」に接続するため																														
	ひとり親医療										○	○																					
	老人医療										○	○																					
	障害者医療										○	○																					
	障害者福祉										○	○																					
	児童福祉	児童手当									○	○																					
		児童扶養手当									○	○																					
		特別児童扶養手当									○	○																					
		子ども子育て									○	○																					
		子ども・子育て支援全国総合システム	内閣府の「子ども・子育て支援全国総合システム」に接続するため																														
	健康管理										○	○																					○
	特定健診										○	○																					○
地方公営事業	上下水道管理	上下水道管理									○						○																
	公営住宅管理	公営住宅管理（オンプレミス）									○						○																
		公営住宅管理（LGWAN-ASP）																															
内部情報系	人事給与																																
	財務会計	財務会計																															
		地方財政決算情報管理																															
	庶務事務																																
	文書管理																																
	ファイルサーバ																																
	グループウェア																																
防災	J-ALERT	受信機	LGWANと衛星回線に接続																														
		エリアメール転送用	内閣府からの緊急メールをLGWAN経由にて受信																														
	Em-Net																																
	安否情報システム																																
調達・施設予約	電子申請（オンプレミス）																																
	電子申請（LGWAN-ASP）																																
	電子調達（オンプレミス）																																
	電子調達（LGWAN-ASP）																																
	工事実績情報（CORINS）	公共工事の実績を確認するためインターネットに接続																															
	施設予約（オンプレミス）																																
	施設予約（LGWAN-ASP）																																
	図書館																																
インターネットメールアクセス	LGWAN掲示板																																
	LGWANメール																																
	インターネットメール																																
	WEBアクセス																																
	ホームページ/作成等																																


地方公営事業
内部情報
調達・施設予約
メール/インターネットアクセス
上下水道管理
公営住宅管理
人事給与
財務会計
庶務事務
文書管理
ファイルサーバ
グループウェア
安否情報システム
電子申請（オンプレミス）
電子調達（オンプレミス）
施設予約（オンプレミス）
図書館
LGWAN掲示板
LGWANメール
インターネットメール
WEBアクセス
ホームページ/作成等
備考
上下水道管理
公営住宅管理（オンプレミス）
公営住宅管理（LGWAN-ASP）
財務会計
地方財政決算情報管理

参考３．端末アクセスコントロールイメージ

・各行に記載した端末から、各列のどのサーバへアクセスできるように設定するか一例を示したもの。

サーバ ＼ 端末				住民記録									宛名管理		税					社会保障																		
				住民記録			戸籍		証明書自動交付				宛名管理		税					生活保護	国民年金	国民健康保険	後期高齢者医療	介護保険	ひとり親医療	老人医療	障害者医療	障害者福祉	児童福祉					健康管理	特定健診
				住民記録（既存住基）	印鑑証明	選挙	戸籍	戸籍副本	自動交付機	コンビニ交付（LGWANセルフASP）	コンビニ交付（LGWAN-ASP）		統合宛名	団体内統合宛名	個人住民税	法人住民税	固定資産税	軽自動車税	収滞納管理			国民健康保険	後期高齢者医療	介護保険					児童手当	児童扶養手当	特別児童扶養手当	子ども子育て			
住民記録	住民記録	住民基本台帳（既存住基）		○	○	○								○																					
		印鑑証明		○	○	○																													
		選挙		○	○	○																													
		法務省情報連携（外国人住民）		LGWAN上の「法務省市町村連携サーバ」と接続																															
	戸籍	戸籍					○																												
		戸籍副本						○	LGWAN経由にて法務局の「戸籍副本データ管理システム」に接続																												
	証明書自動交付	自動交付機							○																										
		コンビニ交付（LGWANセルフASP）								○			LGWAN経由にて「証明書交付センター」と接続																						
		コンビニ交付（LGWAN-ASP）									○		LGWAN経由にて「証明書交付センター」と接続																						
宛名管理	宛名管理	統合宛名											○																						
		団体内統合宛名												○																						
	中間サーバー関連	管理端末		暗号装置を経由しLGWAN上にある中間サーバー・プラットフォームへ接続																															
		中間サーバー接続端末		暗号装置を経由しLGWAN上にある中間サーバー・プラットフォームへ接続																															
税	税	個人住民税												○	○	○	○	○	○																
		法人住民税													○	○	○	○	○																
		固定資産税													○	○	○	○	○																
		軽自動車税													○	○	○	○	○																
			軽自動車検査情報	LGWAN経由にてJ-LISの「軽自動車検査情報の提供システム」と接続																															
		収滞納管理													○	○	○	○	○																
			地方税電子申告（eLTAX）	「審査サーバ・受付サーバ」および地方税電子化協議会のポータルセンターに接続するため。																															
			電子収納［Pay-easy、コンビニ交付］	LGWANもしくは専用線にて「公金収納システム」に接続																															
			ふるさと納税（LGWAN-ASP）	LGWANを経由してシステムと連携																															
社会保障	生活保護													○						○															
	国民年金													○							○														
	国民健康保険	国民健康保険																				○													
		国保連合会接続端末		保険者用ネットワークを経由して国保連合会の「国保総合システム」に接続するため																															
	後期高齢者医療	後期高齢者医療																					○												
		後期高齢者医療制度広域連合電算処理システム（標準システ		専用ネットワークを通じて後期高齢者医療広域連合の標準システムに接続するため																															
	介護保険	介護保険												○										○											
		国保連合会接続端末		保険者用ネットワークを経由して国保連合会の「介護保険審査・支払等システム」に接続するため																															
	ひとり親医療													○											○										
	老人医療																									○									
	障害者医療																										○								
	障害者福祉													○														○							
	児童福祉	児童手当												○															○						
		児童扶養手当												○																○					
		特別児童扶養手当												○																	○				
		子ども子育て	子ども子育て											○																		○			
			子ども・子育て支援全国総合システム	内閣府の「子ども・子育て支援全国総合システム」に接続するため																															
	健康管理													○																			○		
	特定健診													○																					○
地方公営事業	上下水道管理	上下水道管理																																	○
	公営住宅管理	公営住宅管理（オンプレミス）																																	
		公営住宅管理（LGWAN-ASP）																																	
内部情報系	人事給与																																		
	財務会計	財務会計																																	
		地方財政決算情報管理																																	
	庶務事務																																		
	文書管理																																		
	ファイルサーバ																																		
	グループウェア																																		
防災	J-ALERT	受信機		LGWANと衛星回線と接続																															
		エリアメール転送用																																	
	Em-Net			内閣府からの緊急メールをLGWAN経由にて受信																															
	安否情報システム																																		
調達・施設予約	電子申請（オンプレミス）																																		
	電子申請（LGWAN-ASP）			LGWANを経由してシステムと連携																															
	電子調達（オンプレミス）																																		
	電子調達（LGWAN-ASP）			LGWANを経由してシステムと連携																															
	工事実績情報（CORINS）			公共工事の実績を確認するためインターネットに接続																															
	施設予約（オンプレミス）																																		
	施設予約（LGWAN-ASP）			LGWANを経由してシステムと連携																															
	図書館																																		
インターネットメールアクセス	LGWAN掲示板																																		
	LGWANメール																																		
	インターネットメール																																		
	WEBアクセス																																		
	ホームページ/作成等																																		

地方公営事業			内部情報								調達・施設予約				メール/インターネットアクセス					アクセス制御要件			
上下水道管理	公営住宅管理（オンプレミス）	公営住宅管理（LGWAN-ASP）	人事給与	財務会計 財務会計	財務会計 地方財政決算情報管理	庶務事務	文書管理	ファイルサーバ	グループウェア	安否情報システム	電子申請（オンプレミス）	電子調達（オンプレミス）	施設予約（オンプレミス）	図書館	LGWAN掲示板	LGWANメール	インターネットメール	WEBアクセス	ホームページ/作成等	L2SW（原則MACアドレスフィルタリングを実施。欄外※1を参照）	フロアSW（欄外※2を参照）	L3SW（欄外※3を参照）	備考
																				○	○	○	
																				○	○	○	
																				○	○	○	
																				○	○	○	LGWAN通信に関しては静的経路追加が必要。
																				○	○	○	
																				○	○	○	LGWAN通信に関しては静的経路追加が必要。
																				○	○	○	
																				○	○	○	LGWAN通信に関しては静的経路追加が必要。
																				○	○	○	LGWAN通信に関しては静的経路追加が必要。
																				○	○	○	
																				○	○	○	
																				○	○	○	LGWANと暗号装置との通信に関しては静的経路追加が必要。
																				○	○	○	LGWANと暗号装置との通信に関しては静的経路追加が必要。
																				○	○	○	
																				○	○	○	
																				○	○	○	
																				○	○	○	
																				○	○	○	LGWAN通信に関しては静的経路追加が必要。
																				○	○	○	
																				○	○	○	LGWAN通信に関しては静的経路追加が必要。 一部インターネットを参照する場合は、専用ルーターを使って接続すること
																				○	○	○	LGWAN通信に関しては静的経路追加が必要。
																				○	○	○	LGWAN通信に関しては静的経路追加が必要。
																				○	○	○	
																				○	○	○	
																				○	○	○	
																				○	○	○	LGWAN通信に関しては静的経路追加が必要。
																				○	○	○	
																				○	○	○	LGWAN通信に関しては静的経路追加が必要。
																				○	○	○	
																				○	○	○	LGWAN通信に関しては静的経路追加が必要。
																				○	○	○	
																				○	○	○	
																				○	○	○	
																				○	○	○	
																				○	○	○	
																				○	○	○	
																				○	○	○	
																				○	○	○	
																				○	○	○	LGWAN通信に関しては静的経路追加が必要。
																				○	○	○	
◎																				○	○	○	
◎	◎																			○	○	○	
◎	◎																			○	○	○	
		◎																		○	○	○	LGWAN通信に関しては静的経路追加が必要。
			◎			◎	◎	◎	◎											○	○	○	
				◎		◎	◎	◎	◎											○	○	○	
				◎	◎								総務省の「地方財政決算管理情報システム」に接続							○	○	○	LGWAN通信に関しては静的経路追加が必要。
						◎	◎	◎	◎											○	○	○	
						◎	◎	◎	◎											○	○	○	
						◎	◎	◎	◎											○	○	○	
						◎	◎	◎	◎											○	○	○	
																				○	○	○	LGWANからの通信と衛星回線のみIPフィルタにて通信を許可 また、エリアメールへの気象データ送信のみIPフィルタにて通信を許可
																		◎		○	○	○	キャリア専用のHPのみURLフィルタリングにより通信を許可
															◎	◎				○	○	○	
										◎										○	○	○	
											◎									○	○	○	内部用サーバのみIPフィルタリングにより通信を許可。
																				○	○	○	LGWAN通信に関しては静的経路追加が必要。
												◎								○	○	○	内部用サーバのみIPフィルタリングにより通信を許可。
																				○	○	○	LGWAN通信に関しては静的経路追加が必要。
																				○	○	○	URLフィルタリングにより公共工事の実績のHPの参照のみ可能とする
													◎							○	○	○	内部用サーバのみIPフィルタリングにより通信を許可。
																				○	○	○	LGWAN通信に関しては静的経路追加が必要。
														◎						○	○	○	内部用サーバのみIPフィルタリングにより通信を許可。
															◎	◎				○	○	○	
															◎	◎				○	○	○	
																	◎	◎		○	○	○	
																	◎	◎		○	○	○	
																			◎	○	○	○	

※１
L2SW： **課室毎に L2SW による MAC アドレスフィルタリングの設定を検討すること。**
ただし、端末を他業務との間で共用しない場合に、フロア SW による L2SW 単位のフィルタリングでも可能とする。
※２
フロア SW： 「個人番号利用事務」、「個人番号関係事務等」、「その他業務/インターネット接続」の３つのネットワークに分離し、３ネットワークの相互通信を遮断すること。
異なる業務端末を接続する HUB 間の通信遮断を行うこと。
※３
L3SW：原則、IP フィルタリングにより、端末からサーバー間（LGWAN 含む）の通信を特定する設定をすること。
「個人番号利用事務」、「個人番号関係事務等」、「その他業務/インターネット接続」の３つのネットワークに分離し、３ネットワークの相互通信を遮断すること。

参考４．組織別　端末ポート数イメージ

フロア	原課名	個人番号利用事務	個人番号関連事務等	その他業務/インターネット接続	HUB	L2SW ※１	フロアSW	L3SW ※２
		端末台数	端末台数	端末台数				
1F	市民課	13	26	5	11	3	1	1
	社会福祉課	0	13	2				
	障がい者福祉課	1	12	2				
	高齢者介護課	5	2	1				
	保険年金課	2	1	0	14			
		10	20	5				
	こども課	4	23	3				
	地域医療対策課	4	15	2				
	市民税課	5	18	2				
	資産税課	7	20	4	12			
	納税課	10	15	4				
	軽自動車税課	6	12	3				
	会計課	7	13	2				
2F	情報政策課	13	24	3	3	3	1	
	地域政策支援課	2	25	3	3			
	改革推進課	13	30	4	3			
	秘書広報課	1	12	1	6			
	都市整備課	2	15	2				
3F	保健センター事務室	0	2	1	3	3	1	
	保健センター受付	0	2	0				
	生活衛生課	1	13	2	6			
	環境推進課	4	9	2				
	森づくり課	2	7	1	6			
	下水道課	1	8	1				
4F	管財課	2	15	2	3	3	1	
	地域包括支援センター	1	2	1	6			
	財政課	2	8	1				
	契約課	2	8	1	6			
	市民生活課	4	17	2				
5F	危機管理課	0	7	1	5	3	1	
	工事検査課	5	10	2				
	人事課	5	12	2	4			
	市民相談所	0	2	0				
	総務課	0	13	2	5			
	市役所本庁舎等建設推進	13	8	1				
支所A	市民福祉課	10	26	10	3	3	1	
	地域振興課	12	24	10	3	3	1	
支所B	市民福祉課	12	24	10	3	3	1	
	地域振興課	12	24	10	3	3	1	
出先	出先機関×２０カ所	20	20	20	0	60	20	
合計		213	557	130	108	87	29	1

参考５．自治体情報システム強靭性向上モデル　要件シートの一例

【重要要件】：LGWAN 環境とインターネット環境を分割し、重要情報（個人番号等）の取り扱い形態に基づき、「個人番号利用事務系」、「ＬＧＷＡＮ接続系」、「インターネット接続系」でネットワークを分離

分類	No.	カテゴリ	要件(例)	要件の実現手法(例)	備考(例)
個人番号利用事務系	1	庁内ネットワーク	①個人番号利用事務専用のネットワークセグメントとすること。（徹底分離）	①-1：スイッチ等の設定変更もしくは新規機器導入によりネットワークを分離する。 ①-2：異なるセグメント間で通信機器を共有しない。	・戸籍は個人番号利用事務ではないものの、従来から基幹系業務として住基と密接な関係があるため本セグメントに設置する。戸籍専用セグメントを設け設置することも可とする。 ・ネットワーク接続を許可した機器以外は、ネットワークに接続できない設定等にも十分留意すること。
	2	外部との接続	①個人番号利用事務ネットワーク以外との通信は、アクセスしても安全と認められる特定通信限定とする。特定通信に限定する際は、通信経路の限定(MACアドレス、IPアドレス)に加えて、アプリケーションプロトコル(ポート番号)のレベルでの限定も行うこと。	①-1：特定通信する場合は、L2SW／L3SWによる通信経路限定、ファイアウォールによる通信プロトコル限定等を行うことで通信を制限する。 ①-2：その他外部ネットワークとの通信が発生する場合は専用回線サービスを検討する。	・特定通信とは、LGWANを介した（コンビニ交付、中間サーバー等との）接続、およびデータバックアップや共同利用・クラウドセンタ等との特定のドメイン、アドレスに対して、十分にセキュリティが確保された通信先との接続を指す。 ・その他の外部ネットワークとは、国保連合や厚労省等との通信に用いられる専用回線サービスを指す。
			②特定通信先のサーバーや端末もインターネットとの通信ができないこと。		
	3	端末	①個人番号利用事務に関わる各業務の専用端末とし、業務毎に端末を設置すること。	①個人番号利用事務専用として、各業務毎に専用端末を設置することが望ましい。	・ソフトウェアの脆弱性対策や一般的なウィルス対策を実施すること。
			②ID、パスワードの他に認証方法を導入し二要素認証とすること。 　アクセス権を正しく設定すること。	②-1：認証方法としては、パスワード入力の他にICカード、生体認証（指紋、静脈、顔等）がある。 ②-2：認証において人事情報と連携し、ユーザー、組織単位ごとにアクセス制限を設定すること。	・認証サーバーはセグメント毎に設置すること。 （個人番号関係事務等のセグメントに所在する認証サーバーとの同期は可能とする。その際は特定通信として設定する。）
			③アクセスの記録を残して不正な利用を発見できること。 　なお、アクセスの記録とは端末操作の記録及びサーバ等のアクセス先の情報資源に対する操作の記録双方を指す。	③ユーザーの操作ログをサーバ等で履歴を残し、管理者が確認できること。	
	4	媒体	①USBメモリ等の外部記憶媒体による端末からの情報持ち出しができないように設定すること。	①媒体等による情報持ち出しを禁止する機能を導入し設定すること。	（例外取扱）納付書など大量帳票のアウトソーシングや指定金融機関に対する口座振替情報の提供など止むを得ない場合においては、管理者権限を持つ職員によってその都度限定を解除する、または管理者権限を持つ職員のみに許可する設定とすること。
LGWAN接続系	5	庁内ネットワーク	①LGWAN接続系専用のネットワークセグメントとすること。 （LGWAN環境とインターネット環境を分割して、無害化したメール通信のみを許可する）	①：スイッチ等の設定変更もしくは新規機器導入によりネットワークを分割する。	・ネットワーク接続を許可した機器以外は、ネットワークに接続できない設定等にも十分留意すること。
	6	外部との接続	①LGWAN-ASP（LGWANメール含む）など特定通信限定とすること。	①-1：特定通信する場合は、L2SW／L3SWによる通信経路限定、ファイアウォールによる通信プロトコル限定等を行うことで通信を制限する。 ①-2：その他外部ネットワークとの通信が発生する場合は専用回線サービスを検討する。	
			②インターネットにアクセス可能なネットワークとの通信は、直接、間接を問わず禁止すること。 　ただし、添付ファイル削除やテキストデータ化によって無害化を行っているインターネットメールの取込みや仮想デスクトップによって分離された端末環境での利用は要検討。	②-1：インターネットメールの無害化の方法として、インターネット接続環境側でインターネットメールのテキスト本文のみ抽出し、LGWAN接続系に送る仕組みを構築する。 ②-2：インターネット業務端末を仮想化し、仮想環境からLGWAN接続系の端末へ画面を転送する仕組みを構築する。 ②-3：庶務事務の旅費精算等でインターネットのサービス（経路検索・運賃計算等）を利用している場合には、イントラネット版サービスに変更することでインターネット接続を不要とする。	②-1：インターネットメールの無害化の方法（テキスト本文のみの利用） 　インターネットメールの受信メールは、インターネット接続環境側でテキスト本文のみ抽出した無害化メールとし、LGWAN接続系のメールサーバに転送することで、インターネットメール（テキスト本文のみ）をLGWAN接続系の端末（メーラー）で閲覧可能とする。この場合、インターネットメールの添付ファイルの閲覧や印刷は、インターネット接続環境のメーラーやプリンタで行う。 ②-2：インターネットメールの無害化の方法（仮想デスクトップ環境での利用） 　インターネット接続環境のみ仮想デスクトップ化し、LGWAN接続系の端末で添付ファイルも含むメールの閲覧を可能とする。添付ファイルの印刷は、インターネット環境のプリンタより出力する。 ※LGWAN接続系からの添付ファイルも含めたインターネットへのメール送信は可とする考え方もある。
	7	端末	①LGWAN接続系に関わる業務の専用端末とする。LGWAN接続系内の複数の業務についても同一端末上での必要な利用を認める。	①LGWAN接続系に関わる業務の専用端末とする。同一端末から必要な複数のLGWAN接続系の業務サーバにアクセス可能とする。	・ソフトウェアの脆弱性対策や一般的なウィルス対策を実施すること。
			②ID、パスワードの他に認証方法を導入し二要素認証とすることが望ましい。 　アクセス権を正しく設定すること。	②認証において人事情報と連携し、ユーザー、組織単位ごとにアクセス制限を設定すること。	・認証方法としては、パスワード入力の他にICカード、生体認証（指紋、静脈、顔等）がある。
			③アクセスの記録を残して不正な利用を発見できること。 　なお、アクセスの記録とは端末操作の記録及びサーバ等のアクセス先の情報資源に対する操作の記録双方を指す。	③ユーザーの操作ログをサーバ等で履歴を残し、管理者が確認できること。	
	8	媒体	①USBメモリ等の外部記憶媒体等による端末からの情報持ち出しは管理すること。 　併せて、端末等からのマルウエア感染を防ぐ入口対策にも十分留意すること。	①媒体利用を管理・制限する機能等を導入する。 　データがその他業務の端末で利用が必要な場合は備考の処置を実施すること。 　個人番号に関わるデータについては、個人番号利用事務の備考と同等の対応をすること。	・データ受け渡しによる媒体利用の必要がある場合は、以下の条件を満たすこと。 　管理負荷を考慮し、セキュリティソリューション等の導入を推奨する。 　-端末には利用許可された媒体のみ接続可能とすること。 　-データは暗号化しパスワードを設定すること。 　-（推奨）利用媒体は、全て管理し利用履歴を残せること。 　-（推奨）データの受け渡しには、必ず上司の承認と承認記録を残すこと。

（インターネット接続系については、自治体情報セキュリティクラウドの導入と併せて検討すること）

分類	No.	カテゴリ	要件(例)	要件の実現手法(例)	備考(例)
インターネット接続系	9	外部との接続	①インターネットのセキュリティ対策を実施すること。	①ファイアーウォール、侵入防止、ウィルス検知、WEBフィルタリング等の対策を実施すること。 その他業務の情報の重要度を考慮して対策を実施すること。	・セキュリティ対策としては、侵入検知(IDS)、侵入防止(IPS)、ふるまい検知、アプリケーションファイアウォール(WAF)等がある。 ・ログについてはセキュリティ関連機器のログ(FWのログ、IPSのログ、サンドボックス製品のログ、アンチウイルス製品のログ等)およびメールサーバログ、WEBサーバログ、Proxyログ、ADログ、DNSログ等を一定期間保管し、つき合わせが出来ることが望ましい。 ・高度なセキュリティには専門的な運用監視体制が必須となるが、体制が作れない場合はベンダーの運用サービスの導入も検討すること。 ・各団体で実施する方法もあるが、侵入検知(IDS)、侵入防止(IPS)、ふるまい検知については、自治体セキュリティクラウドを利用することが望ましい。
	10	端末	①その他業務、インターネット接続に用いる専用端末とし、個人番号利用事務系への利用やLGWAN接続系への利用を禁止すること。	①他の事務とは共有させない。	・ソフトウェアの脆弱性対策や一般的なウィルス対策を実施すること。 ・専用端末として利用する方法として、仮想化する方法もある。 その場合端末から独立した仮想デスクトップを作成し仮想環境から転送された画面をLGWAN接続系のネットワーク上で操作させる。
			②アクセスの記録を残して不正な利用を発見できること。	②ユーザーの操作ログをサーバ等で履歴を残し、管理者が確認できること。	・認証、アクセス権、ログ等の管理についてはセキュリティ製品を活用することが望ましい。
			③標的型攻撃など未知のウイルスに備えたセキュリティ対策を行うこと。	③ウイルス対策ソフトを導入する。 未知のマルウェア等に即時対応できる仕組みの導入を推奨する。	・セキュリティ対策として以下の仕組みもしくは製品の導入も検討すること。 -標的型対策 -ゲートウェア型セキュリティ製品と情報連携し未知のマルウェア対策パッチを端末に配布する仕組み -感染した端末をネットワークから切り離す仕組み等
			④WEB閲覧、メール文、添付については細心の注意を行うこと。(マルウェア、ランサムウェア※等の対策)	④ データはインターネット環境のみとし、確認が必要な場合はプリントアウトして、データを他の事務に持ち込まないこと。	※ランサムウェア:感染したコンピュータのシステムへのアクセスを制限する。アクセス制限解除等に身代金を要求する場合が多い。
	11	媒体	①USBメモリ等の外部記憶媒体等による端末からの情報持ち出しは管理すること。	①媒体利用を管理・制限する機能等を導入する。	・データ受け渡しによる媒体利用の必要がある場合は、以下の条件を満たすこと。 管理負荷を考慮し、セキュリティソリューション等の導入を推奨する。 -端末には利用許可された媒体のみ接続可能とすること。 -データは暗号化しパスワードを設定すること。 -(推奨)利用媒体は、全て管理し利用履歴を残せること。

自治体情報セキュリティ
強化対策事業実施要領
（その２）
（自治体情報セキュリティクラウド事業）

付録3　　自治体情報セキュリティ強化対策事業実施要領（その２）（自治体情報セキュリティクラウド事業）

（目次）

自治体情報セキュリティ強化対策事業実施要領（その２）
（自治体情報セキュリティクラウド事業）

自治体情報セキュリティ強化対策事業（補助金名：地方公共団体情報セキュリティ対策強化費補助金）の自治体情報セキュリティクラウド事業については、この要領を参照の上、実施するものとする。

なお、自治体情報システム強靭性向上事業については、「自治体情報セキュリティ強化対策事業実施要領（その１）」を参照されたい。

自治体情報セキュリティクラウド（以下「セキュリティクラウド」という。）とは、現在各市区町村が個別に設置しているＷｅｂサーバ等の監視対象を都道府県と市区町村が協力して集約し、監視およびログ分析・解析をはじめ高度なセキュリティ対策を実施するもの。

第1 監視対象

セキュリティクラウドで想定する主な監視対象は、セキュリティクラウド上に集約された機器およびログとする。

①Ｗｅｂサーバ、②メールリレーサーバ（メールサーバを含む場合もある。以下同じ。）、③プロキシサーバ、④外部ＤＮＳサーバ、⑤ＬＧＷＡＮ接続ファイアウォール（機器は集約せず、セキュリティクラウド上のログ分析システムにログを転送するように設定を変更）である。

① Ｗｅｂサーバ（ホームページ公開用）

各市区町村のホームページ等をインターネットに公開するためＷｅｂサーバを集約したもの。

② メールリレーサーバ

インターネットとの間でメールの中継を行っている各市区町村のメールリレーサーバを集約したもの。あわせて、各市区町村のインターネット側のメールボックスを保有しているメールサーバを集約したものを対象とする場合もある。

③ プロキシサーバ（インターネット閲覧用）

各市区町村のインターネット接続の端末等よりインターネット閲覧を行う際に、各端末等の代理でインターネットとのデータ送受信を行うプロキシサーバを集約したもの。

④ 外部ＤＮＳサーバ

各市区町村のドメイン情報（サーバのホスト名(URL)とグローバルＩＰアドレスの変換）をインターネットに公開している外部ＤＮＳサーバを集約したもの。

⑤　ＬＧＷＡＮ接続ファイアウォール（ＬＧＷＡＮ接続セグメント用）

各市区町村の庁内ＬＡＮとＬＧＷＡＮ接続ルータとの間にあるＬＧＷＡＮ接続ファイアウォールから、セキュリティクラウド上のログ分析システムへ転送されたログ。

第2 セキュリティ対策のツール例

セキュリティ対策に関する典型的なツール例を以下に示す。

① ファイアウォール

インターネットとの通信について、ＩＰアドレス又はポート番号に着目し、セキュリティ管理者が作成した以下の「許可/拒絶ルール」に基づき、通信パケットの転送、破棄等を行うもの。

(a) 送信元と送信先のポート番号を制限する

(b) ＩＰアドレスの送信元と送信先を制限する

② ＩＤＳ／ＩＰＳ

インターネットとの通信について、通信内容全体に着目し、セキュリティベンダーが提供するパターンファイルを用いたパターンマッチング等により、不正な通信パターンと合致する通信や、通信プロトコルの仕様と異なる通信、通常の状態をはるかに超える通信等を異常として検知・拒絶するもの。

③ 振る舞い検知機器

インターネットとの通信に含まれるファイルについて、隔離した擬似環境で動作させ、新たなプログラムをダウンロードしようとしたり、一定間隔で通信が発生したり、サーバの内部を勝手にスキャンしたり、レジストリを書き換えようと試みるなど、マルウェアのような異常な動作をするプログラムを検知するもの。

④ スパム対策機器

インターネットとの送受信メールについて、セキュリティベンダーが提供するパターンファイルを用いたパターンマッチングや、セキュリティ管理者が設定したルール等に基づき、迷惑メール・スパムメールの拒絶を行うもの。

⑤ ＵＲＬフィルタ機器

インターネットへのＷｅｂ閲覧通信について、全ての端末のアクセスログを残すとともに、セキュリティベンダーが提供するパターンファイルを用いたパターンマッチングや、セキュリティ管理者が設定したルール等に基づき、不正なＵＲＬへの接続を拒絶するもの。

⑥ ログ分析システム（収集・分析）

各機器のログを収集し、ログを時系列に検証し、成功失敗などの事象から分析を行い、セキュリティベンダーが提供するパターンファイル及びセキュリティ管理者が設定したルールに基づき不正な事象もしくは不正と疑われる事象を検知するもの。

⑦　コンテンツ改竄検知ツール

インターネットに公開するＷｅｂサーバ上のコンテンツについて、事前に保存した内容と、現在公開している内容を比較して、コンテンツの改竄を検知するもの。又は、改竄があった場合に、事前に保存した内容を使用して自動修復を行うもの。

⑧　イベント監視ツール

インターネットに公開するサーバ内で発生するプログラム起動などのイベントについて、サーバ内のログにて監視し、セキュリティベンダーが提供するパターンファイルを用いたパターンマッチングや、セキュリティ管理者が設定したルール等に基づき、許可していないイベントの発生を検知するもの。

⑨　ＷＡＦ（Ｗｅｂ　Ａｐｐｌｉｃａｔｉｏｎ　Ｆｉｒｅｗａｌｌ）

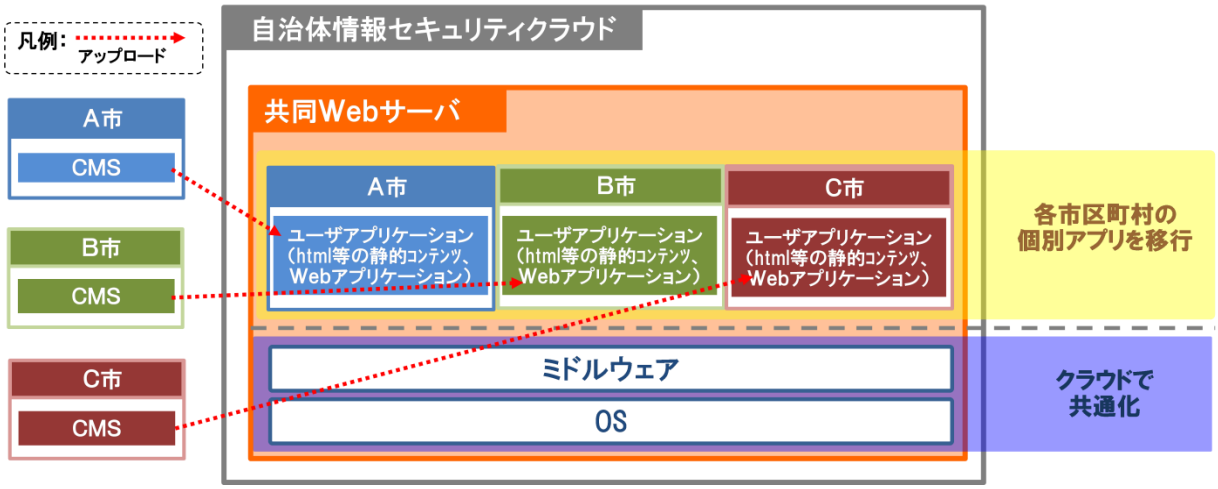
インターネットに公開する Web サーバの通信について、セキュリティベンダーが提供するパターンファイルを用いたパターンマッチングにより、Ｗｅｂアプリケーションに特化したＳＱＬインジェクションやクロスサイトスクリプティング等の脆弱性を狙った不正な通信（リクエストＵＲＬにセキュリティホールを突くような命令を付加するなど）を検知・防御するもの。

第3 移行の際の留意点

セキュリティクラウドへの移行時における留意点を以下に示す。

①　Ｗｅｂサーバ（ホームページ公開用）

(a) 共同 Web サーバを導入するにあたっては、動作環境設定(ユーザアプリケーションで利用できるプログラム言語種類等)も共通となることに留意する。



(b) 各市区町村のコンテンツ管理システム（CMS）設定先を、セキュリティクラウド上の共同Ｗｅｂサーバに変更する。

(c) 各市区町村の主たるホームページの他に、議会中継システムや防災情報提供システム等の公開ページもセキュリティクラウド上で動作するように設定する場合、周辺システム等との接続形態により、段階的な移行もありうる。

② メールリレーサーバ

(a) 共同メールリレーサーバを導入するにあたっては、動作環境設定（送受信可能サイズ等）も共通となることに留意する。なお、メールサーバも併せて集約する場合も同様。

(b) 無害化対策サーバをセキュリティクラウド上に構築することも妨げない。なお、無害化対策としては、添付ファイル削除、及びＨＴＭＬメールのテキスト化や、VDI などの仮想化技術が想定される。

③ プロキシサーバ（インターネット閲覧用）

(a) 共同プロキシサーバを導入するにあたっては、動作環境設定(キャッシュ間隔等）も共通となることに留意する。

④ 外部ＤＮＳサーバ

(a) 共同外部 DNS サーバを導入するにあたっては、動作環境設定(キャッシュ有効期間等）も共通となることに留意する。

⑤ ＬＧＷＡＮ接続ファイアウォール

(a) 各市区町村のＬＧＷＡＮ接続ファイアウォールにおいて、セキュリティクラウド上のログ分析システムへ拒絶パケットのログを転送するように設定すること。なお、ログ分析システムへのログ転送に別途機器が必要な場合もあるので留意する。また、別途セキュリティクラウド向けの回線が必要となることにも留意する。

⑥ セキュリティクラウド接続回線

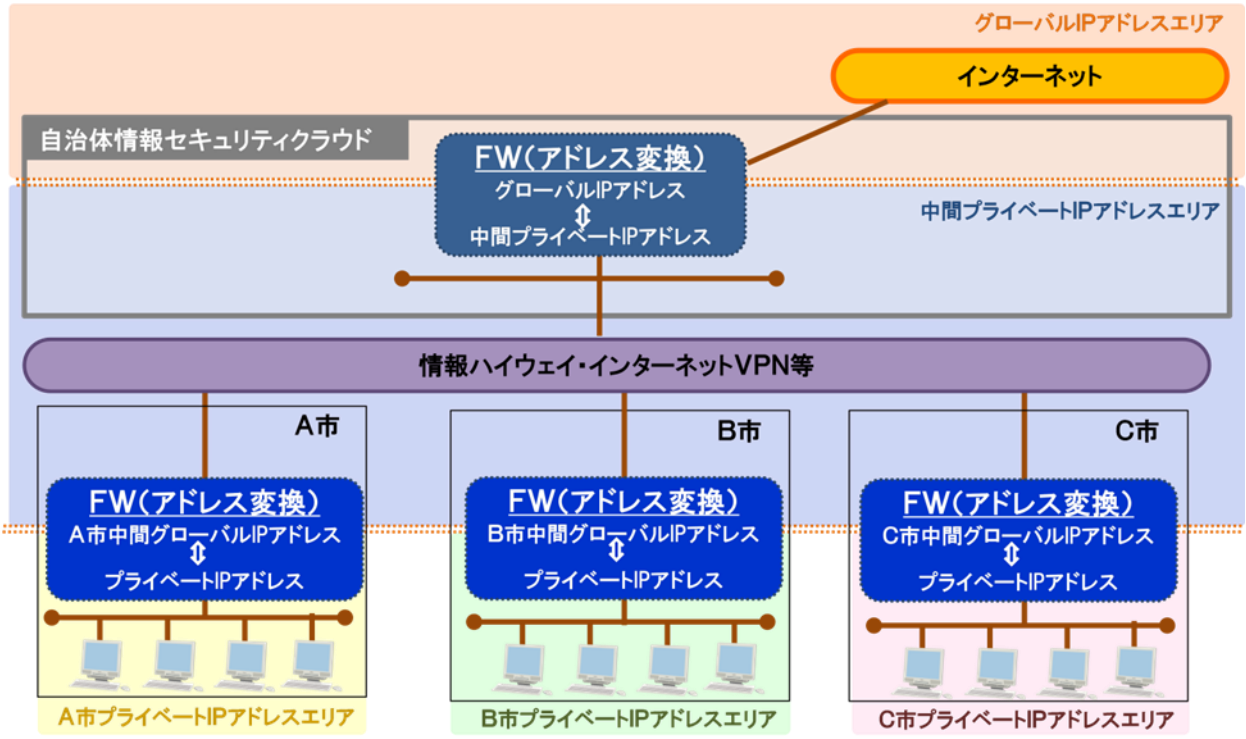
(a) 各市区町村のインターネット接続系とセキュリティクラウドを接続する回線は、各都道府県内の情報ハイウェイを活用することが望ましい。なお、情報ハイウェイが無い場合には、ＩＰ－ＶＰＮ、インターネットＶＰＮ等の利用が想定される。

⑦ 各市区町村のインターネット接続ファイアウォール（既存）

(a) 各自治体情報セキュリティクラウドは、クラウド上のファイアウォールにおいて、それぞれ一意のグローバル IP アドレスを有する。

(b) 各市区町村の既存のグローバルＩＰアドレスは、市区町村ごとに一意の中間プライベートＩＰアドレスとして、各市区町村の既存のインターネット接続ファイアウォールにおいて設定変更する。

(c) 各市区町村の既存のインターネット接続ファイアウォールにおいて、各市区町村内の既存のプライベートＩＰアドレスと新たに設定された中間プライベートＩＰアドレスとが、変換されるように設定変更する。


グローバルIPアドレスエリア
インターネット
自治体情報セキュリティクラウド
FW(アドレス変換)
グローバルIPアドレス
⇕
中間プライベートIPアドレス
中間プライベートIPアドレスエリア
情報ハイウェイ・インターネットVPN等
A市
FW(アドレス変換)
A市中間グローバルIPアドレス
⇕
プライベートIPアドレス
A市プライベートIPアドレスエリア
B市
FW(アドレス変換)
B市中間グローバルIPアドレス
⇕
プライベートIPアドレス
B市プライベートIPアドレスエリア
C市
FW(アドレス変換)
C市中間グローバルIPアドレス
⇕
プライベートIPアドレス
C市プライベートIPアドレスエリア