印西地区消防組合
情報セキュリティポリシー

（平成１８年　９月２２日　制　　定）
（平成２９年１１月　１日　一部改正）
（令和　２年　１月　７日　一部改正）
（令和　５年　４月　１日　一部改正）
（令和　８年　３月３１日　全部改正）

<目次>

序 情報セキュリティポリシーの背景と構成

背　景

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。

印西地区消防組合（以下「消防組合」という。）が所掌する情報資産には、住民の個人情報を始めとし行政運営上重要な情報など、外部に漏洩した場合にはきわめて重大な結果を招く情報が多数含まれている。これらの情報資産を人的脅威や災害、事故等から守ることは、住民の権利、利益を守るために必要不可欠である。

また、行政事務の合理化に取り組むうえで、本消防組合における情報システムの利用範囲と利用形態は拡大と高度化をしつづけており、行政運営面からみて従来以上に重要なものとなっている。そのため他に代替することができない行政サービスを将来にわたって安定的、継続的に運営するために、本消防組合が管理しているすべての情報システムが高いレベルで安全性を有していることが不可欠である。

さらに、多様化した住民活動、社会活動、経済活動を支える上で、消防組合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、本消防組合の保有する情報資産の機密性、完全性及び可用性（注記）を維持するための対策を整備するため、印西地区消防組合情報セキュリティポリシーを定め、情報セキュリティの確保に最大限取り組むこととする。

（注記）

国際標準化機構（ＩＳＯ）で定義された、情報が守られている状態のためのセキュリティ・アーキテクチャーの考え方であり、以下の３要素で構成されている。

機密性(Confidentiality):　情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

完全性(Integrity):　情報及び処理の方法の正確さ及び完全である状態を安全防護すること。

可用性(Availability)：　許可された利用者が必要なときに情報にアクセスできることを確実にすること。

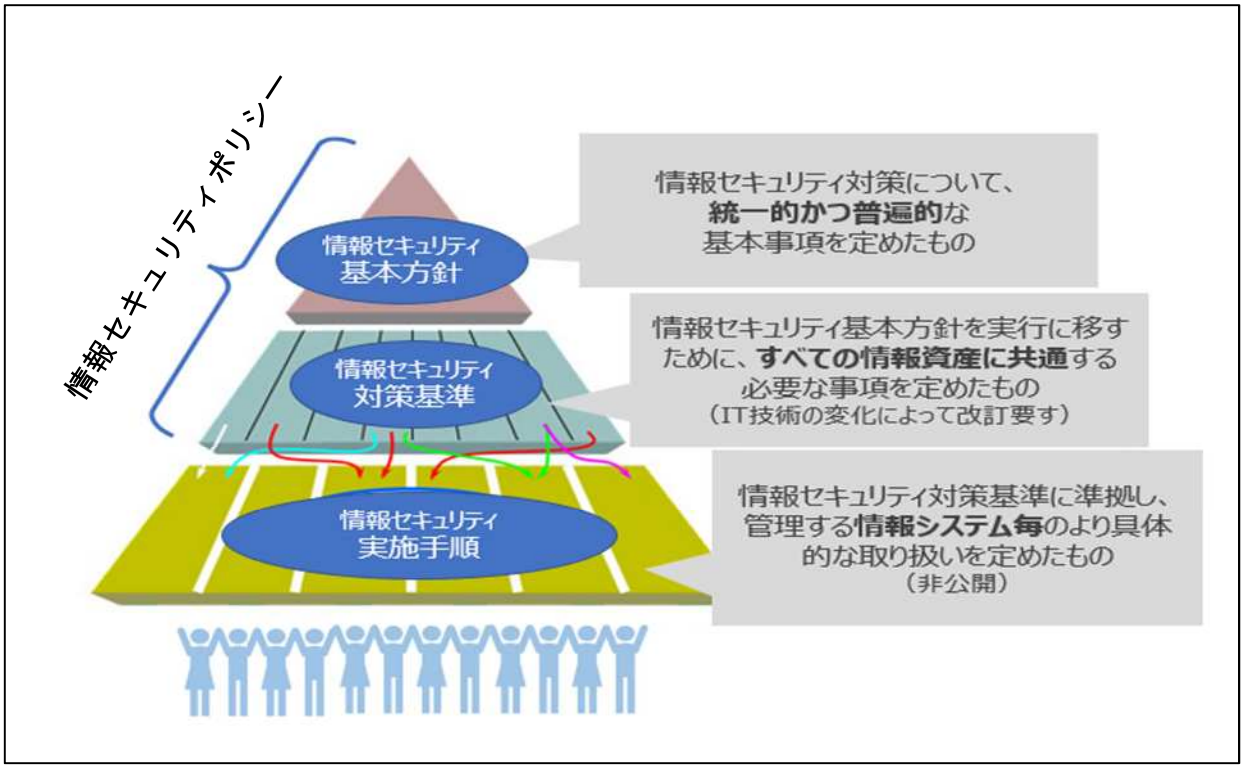
構　成

印西地区消防組合情報セキュリティポリシー（以下、「情報セキュリティポリシー」という。）とは、本消防組合が所掌する情報資産に関するセキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものである。

情報セキュリティポリシーは、情報資産を支えるクラウドコンピューティングや仮想化技術に代表される情報処理技術や通信技術等の進展に伴う急速な状況の変化に、柔軟に対応する必要があるとともに、本消防組合の情報資産を取り扱うすべての職員に浸透、定着しなければならない。

このようなことから、情報セキュリティポリシーは、情報セキュリティ対策に関する普遍性のある方針として、「情報セキュリティ基本方針」、情報資産を取り巻く状況の変化に適切に対応する部分としての「情報セキュリティ対策基準」の２階層に分け策定することとする。また、情報セキュリティポリシーに基づき、情報システム毎に、具体的な情報セキュリティ対策の実施手順として「情報セキュリティ実施手順」を策定することとする。

情報セキュリティポリシーの構成



第１章　情報セキュリティ基本方針

１．目的

本消防組合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、本消防組合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）　実施機関

印西地区消防組合をいう。

（２）　課等

印西地区消防組合消防本部及び消防署の設置等に関する条例（昭和４７年条例第４号）第３条に掲げる消防署、印西地区消防組合消防本部の組織に関する規則（昭和５５年規則第３号）第２条に掲げる課をいう。

（３）　ＣＳＩＲＴ

Computer Security Incident Response Team の略であり、情報セキュリティにかかるインシデント（障害）に対処するために設置される、課等の組織に縛られない組織横断的な体制である。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定を行う役割と、ＣＳＩＲＴ内の業務統括を行う役割の２つで構成される。

（４）　電子計算機

ハードウェア、仮想技術（ハイパーバイザー）及びソフトウェアで構成するコンピュータ及び周辺機器をいう。また、電子計算機のうち職員等が情報処理を行うために直接操作する機器をパソコンまたは端末といい、そのうち必要に応じて携帯して（移動して）使用することを目的として導入したものをモバイル端末またはタブレット端末という。

またビデオ会議システム、映像送出システム、IP 電話システム、ネットワークカメラ、スマートフォン、その他 IoT 機器についても、電子計算機に含めて扱う。

（５）　ネットワーク

電子計算機等を相互に接続するための通信網及びその構成機器（ハードウェア及びソフトウェア、場合により仮想化技術を含む）をいう。

（６）　電磁的記録媒体

電子計算機に使用される磁気ディスク、磁気テープ、光学ディスク、フラッシュメモリ、フラッシュメモリを用いたソリッドステートドライブ（ＳＳＤ）、その他、電磁的記録の如何にかかわらずこれに類する媒体をいう。

（７）　情報システム

電子計算機、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。

（８）　通信経路

ネットワークに接続された情報システムがデータの送受信を行う道筋を意味し、以下のもので構成される。

① インターネット接続系ネットワーク

インターネットにアクセス又はインターネットからのアクセスを許可する情報システムが接続するネットワークをいう。

② 独立系ネットワーク

上記の①の要件に該当しない情報システムが接続する共用ネットワーク及び情報システム専用のネットワークをいう。

（９）　通信経路の分割

業務用システム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うえで、安全が確保された情報だけを許可できるようにすることをいう。

（１０）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、コンピュータウィルス等の不正プログラムの付着がない等、安全が確保された通信をいう。

（１１）行政情報

本消防組合の行政事務の執行に関わる情報で、かつ情報システムで取り扱う電磁的記録媒体等に記録された情報及び紙等に記録された情報をいう。

（１２）情報資産

本消防組合の情報システム及びこれらに関する設備、電磁的記録媒体並びに行政情報をいう。

（１３）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。

（１４）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。

（１５）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。

（１６）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。

（１７）外部サービス

外部サービスとは，外部の事業者が提供するサービスの総称であり，以下のものをいう。

① 委託による外部サービス

本消防組合の業務を外部の事業者に委託することにより調達する外部サービスのことをいう。

② 約款等による外部サービス

無料有料を問わず，以下の形態により調達する外部サービスのことをいう。

ア） 約款への同意のみにより利用可能となる外部サービス

事業者が定める約款への同意によって利用可能となるサービスのことをいう。

イ） 約款に特約等を付して調達する外部サービス

事業者が定める約款に取扱う行政情報の保護に関する特約等を付加し，利用するサービスのことをいう。

３．情報セキュリティポリシーの位置付け

情報セキュリティポリシーは、本消防組合の情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の最高位に位置するものである。

４．情報セキュリティポリシーの対象範囲

（１）行政機関・職員の範囲

情報セキュリティポリシーが対象とする行政機関及び職員は、本消防組合の実施機関における情報資産、情報資産に接する全ての職員及び外部委託事業者（以下、「職員等」という。）とする。

（２）情報資産の範囲

情報セキュリティポリシーが対象とする情報資産は、次のとおりとする。なお外部に行政情報を提供したことによる二次利用されたデータ等、管理責任が本消防組合から離れたものを除く。

① ネットワークおよび情報システム並びにこれらに関する設備及び電磁的記録媒体

② ネットワークおよび情報システムで取り扱う情報（これらを印刷したデータ）

③ 情報システム並びにネットワーク図といったシステム仕様書や関連図書

５．職員等の遵守義務

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つとともに、情報セキュリティポリシーを遵守するものとし、業務の遂行に当たり、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．情報資産への脅威

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、ウィルス攻撃、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、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

７．情報セキュリティ対策

上記６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

本消防組合の情報資産について、情報セキュリティ対策を推進・管理するための全庁的な組織体制を確立する。

（２） 情報資産の分類と管理

情報資産をその内容に応じて分類し、当該分類に基づき情報セキュリティ対策を行うものとする。

（３） 情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の二段階の対策を講じる。

① 業務用システムと、インターネット接続系ネットワークとの通信経路を分割する。なお両システム間で情報をやり取りする場合には、無害化通信を実施する。

② インターネット接続系ネットワークにおいては、不正通信の監視機能の強化等の情報セキュリティ対策を実施する。

（４） 物理的セキュリティ

サーバ、サーバ室、通信回線及び職員が利用するパソコン・端末等の管理について、物理的な対策を講じる。

（５） 人的セキュリティ

情報資産に接する職員の情報セキュリティに関する権限や責任等を定めるとともに、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、併せて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） 業務委託と外部サービスの利用

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

外部サービスを利用する場合には、利用に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サービスごとの責任者を定める。

８．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し、運用改善を行い、情報セキュリティの向上を図る。

９．情報セキュリティポリシーの見直し

情報セキュリティ自己点検の結果、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しするものとする。

１０．情報セキュリティ対策基準の策定

上記７、８及び９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。

１１．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消防組合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。

第２章　情報セキュリティ対策基準

情報セキュリティ対策基準とは、情報セキュリティ基本方針を実行に移すための本消防組合の情報資産に関する情報セキュリティ対策の基準である。

１．組織及び管理体制

本消防組合の情報セキュリティ管理については、以下の組織・体制とする。

（１）最高セキュリティ責任者

本消防組合の情報資産に関する情報セキュリティを統括する最高責任者として、最高セキュリティ責任者（ＣＩＳＯ: Chief Information Security Officer、以下、「ＣＩＳＯ」という。）を置き、消防長をＣＩＳＯに充てる。ＣＩＳＯは、本消防組合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し、以下の権限と責任を有する。

① 情報セキュリティに関して、統括情報セキュリティ責任者、情報セキュリティ責任者及び情報システム管理者に対して、必要な指示及び助言を行う。

② ＣＳＩＲＴを統括情報セキュリティ責任者の下に設置し、その役割を明確にしなければいけない。

（２）ＣＩＯ補佐官

ＣＩＯ補佐官は、情報システム及び情報セキュリティ並びに情報化戦略に関する専門知識を有する者でＣＩＳＯが必要に応じてＣＩＳＯを補佐する者として消防組合の職員又は、外部専門人材から登用し、次に掲げる職務を行うものとする。

① ＤＸ推進方針の策定又は改定に関する支援及び助言

② デジタル技術の導入に関する企画、調達、開発等に係る適正評価及び助言並びに技術的な支援及び助言

③ デジタル技術の活用に関する規程等の作成並びに改定に係る技術的な支援及び助言

④ 情報セキュリティ対策に関する支援及び助言

⑤ 行政のデジタル化に資する人材の育成

（３）統括情報セキュリティ責任者

① 統括情報セキュリティ責任者は本消防組合全体のセキュリティ対策の責任者とし、次長をもってこれに充てる。また、以下の権限、責任を有する。

② ＣＩＳＯの補佐

③ 本消防組合の情報資産に対してセキュリティ侵害が発生した場合（若しくは発生の恐れがある場合）はＣＩＳＯの指示（不在の場合は自らの判断）に従い必要かつ十分な措置を行う。

④ 緊急時のＣＩＳＯへの報告及び回復のための対策に関すること。

⑤ 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こと。

⑥ ＣＳＩＲＴ責任者として、情報資産に対するセキュリティ侵害の発生について課等より報告を受けた場合には、その状況を確認し、セキュリティ障害対応に必要な報告等が行われる体制の整備を行う。

⑦ 本消防組合における情報セキュリティに関する施策等の内容を関係課等に提供する。

⑧ セキュリティ障害の発生を認めた場合には、必要に応じてＣＩＳＯ、県、総務省等関連機関との情報共有を行う。

（４）情報セキュリティ責任者

情報セキュリティ責任者は、所掌する課等の情報セキュリティ対策を統括する責任者としての権限と責任を有し、各課等の長をもってこれに充てる。また、以下の権限、責任を有する。

① 所掌する課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。

② 所掌する課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等に対する教育、訓練、助言及び指示を行う。

（５）情報システム管理者

情報システム管理者は、情報システムの正常な動作を維持するための管理者とし、総務課長をもってこれに充てる。また、以下の権限、責任を有する。

① 情報システムにおける追加、変更に関する承認。

② 情報システムにおける情報セキュリティに関する定期的な状況把握及び助言、指導。

③ 情報セキュリティ実施手順の作成・維持管理に関する情報管理者への助言及び指導。

④ 緊急時の円滑な情報共有を図るための緊急連絡網に関すること。

⑤ 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に関すること。

⑥ 情報セキュリティに関する教育及び訓練に関すること。

⑦ ＣＳＩＲＴ管理者として、情報セキュリティ障害の発生について情報セキュリティ責任者又は情報管理者より報告を受けた場合には、その状況を確認し、ＣＳＩＲＴ責任者に報告する。

⑧ 最新のサイバー攻撃に対応した対策が可能となるよう、サイバー攻撃に関する情報共有活動へ参加し、積極的な情報入手に努め、入手した情報を有効活用するための環境整備を行う。

（６）情報管理者

情報管理者は、課等の情報セキュリティに関する権限及び責任を有し、各課等の長をもってこれに充てる。また、以下の権限、責任を有する。

① 所掌する情報システムの追加・変更に関すること。

② 所掌する情報システムに係る情報セキュリティ実施手順の作成・維持管理に関すること。

③ 所掌する情報システムの機器や記録媒体の適正な管理に関すること。

④ 所掌する課等の職員に対する情報セキュリティポリシーの遵守に関すること。

⑤ ＣＳＩＲＴ担当者として、所掌する情報資産に対するセキュリティ侵害が発生した場合（若しくは侵害の恐れがある場合）の情報セキュリティ責任者、情報システム管理者、統括情報セキュリティ責任者及びＣＩＳＯへの速やかな報告を行う。

（7）ＣＳＩＲＴの設置

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事故が発生した際に備え、または情報セキュリティ事故の発生を可能な限り予防することを目的として、ＣＩＳＲＴを設置し、以下の役割を付する。

① 情報セキュリティ事故を認知した場合には、ＣＩＳＯ、総務省、千葉県等へ報告すること。

② 情報セキュリティ事故を認知した場合には、その重要度や影響範囲を勘案し、関係者をはじめ、報道機関への通知・公表対応を行うこと。

③ 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を有する部署、委託業者等との情報共有を行い、情報セキュリティ事故（インシデント）の発生を可能な限り防止する対策を講じること。

２．情報資産の分類と管理方法

（1）情報資産の分類

情報管理者は、所掌する情報資産を機密性、完全性及び可用性の点から、重要度の高いものから重要性分類Ⅰ、Ⅱ及びⅢとし、次の要件に従って分類する。

① 重要性分類Ⅰ

ア）個人情報の保護に関する法律（平成１５年法律第５７号）第２条第１項に規定する個人情報。

イ）法令又は条例（以下「法令等」という。）の定めにより守秘義務を課されている行政情報。

ウ）法人その他の団体に関する行政情報で漏えいすることにより当該団体の利益を害する恐れのある情報。

エ）漏えいした場合、行政に対する信頼を著しく害するおそれのある行政情報。

オ）滅失し、又はき損した場合、その復元が著しく困難となり、行政の円滑な執行を妨げる恐れのある行政情報。

カ）情報システムに係るパスワード及びシステム設定情報。

② 重要性分類Ⅱ

脅威にさらされた場合に実害を受ける危険性は低いが、行政事務の執行において重要性は高いと評価される行政情報（公開されると行政の円滑な執行に侵害を生ずる恐れのある行政情報）。

③ 重要性分類Ⅲ

上記以外の行政情報

（２）情報資産の管理

① 管理責任

ア）情報管理者は、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、重要性分類Ⅰ・Ⅱの情報資産について、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い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）他の職員等が作成した情報資産を入手した時は、作成者が定めた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）外部の者が作成した情報資産を入手した者は、当該情報の分類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、最重要度の分類に従って、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）情報管理者又は情報システム管理者は、情報資産のバックアップデータ等の重要な情報を記録した電磁的記録媒体を保管する場合は、火災、水害等の影響を受けない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重要性分類Ⅱ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）車両等により情報資産を運搬する者は、情報の分類に応じ情報資産の不正利用を防止するための必要な措置を講じなければならない。

イ）重要性分類Ⅱ以上の情報資産を運搬する者は、情報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）業務上必要な情報資産を外部に提供する場合は、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。また、契約書等により提供先に適切な管理を保証させなければならない。

イ）重要性分類Ⅱ以上の情報資産を外部に提供する者は、情報管理者に許可を得なければならない。

ウ）情報管理者は、住民等に公開する行政情報について、完全性を確保しなければならない。

⑩ 情報資産の廃棄

ア）情報資産を廃棄する者は、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）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、情報セキュリティ事故の早期発見と対処等の情報セキュリティ対策を講じなければならない。

② 業務用システム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、必要な情報だけを許可できるように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

重要な情報を格納しているサーバは冗長化し、障害が発生した場合でもシステムの運用停止時間が最小限となるようにしなければならない。

（３）機器の電源

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。

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

通信ケーブル及び電源ケーブル配線は、傍受又は損傷等を受けることがないよう可能な限り必要な措置を講じなければならない。

（５）機器の定期保守及び修理

① 重要な情報を格納しているサーバ等機器は定期保守を実施しなければならない。

② 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は、修理する事業者との間で、守秘義務契約の締結若しくは秘密保持体制の確認を行わなければならない。

４．２．設置及び保管

（１）設置及び保管場所の管理

① 情報管理者は、重要性分類Ⅱ以上の行政情報の記録されている媒体保管場所及びそれを取り扱う情報システムの設置場所（以下、「管理区域」という。）への入退室の管理について必要な措置を講じなければならない。

② 管理区域への入退室は許可された者のみに制限し、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。

③ 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。

④ 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立ち会うものとし、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。

（２）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、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。

（３）機器の廃棄等

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）情報システムの搬入・搬出

① 機器等を搬入・搬出する場合は、あらかじめ既存情報システム等に対する安全性について、職員等による確認を行わなければならない。

② 機器等の搬入・搬出には、職員が立ち会う等の必要な措置を講じなければならない。

４．３．通信回線

（１）通信回線及び通信回線装置の管理

① 情報システム管理者は、庁内の通信回線及び通信回線装置を適切に管理しなければならない。また、これらに関連する文書を適切に保管しなければならない。

② 情報管理者は、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 情報管理者は、重要性分類Ⅱ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。

④ 情報管理者は、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。

⑤ 情報管理者は、重要性の高い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．記録媒体等の管理

（１）職員等用端末及び電磁的記録媒体等の管理

① 情報管理者は、盗難防止のため執務室等で利用するパソコン等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。

④ 電磁的記録媒体については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。

⑤ 情報管理者は、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。

５．人的セキュリティ

（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、速やかに情報管理事務担当者に相談し、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

職員等は、本消防組合のモバイル端末、電磁的記録媒体等の情報資産を外部に持ち出す場合には、情報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

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、情報管理者の許可を得て利用することができる。

⑤ 持ち出し及び持ち込みの記録

情報管理者は、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文書等について、第三者による使用又は閲覧されることがないように、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）外部委託事業者に対する説明

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等を説明しなければならない。

（３）教育・訓練

① ＣＩＳＯは、職員に対し情報セキュリティポリシーについて啓発に努めるとともに、職員を対象とした情報セキュリティポリシーに関する研修の場を設けなければならない。

② 情報管理者は、情報管理者として必要な知識を維持するための情報通信技術や情報セキュリティに関する研修を受けなければならない。

③ 情報システムを所管する情報管理者は、情報システムの運用に支障を来さない範囲において、緊急時対応を想定した訓練等を職員に行わせなければならない。

④ 職員は、情報セキュリティポリシーに関する研修を受講し、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理解し、情報セキュリティ上の問題が生じないようにしなければならない。

（４）研修・訓練への参加

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。また、情報管理者は職員に研修参加の機会を付与しなければならない。

（５）情報セキュリティ事故の報告

① 庁内からの情報セキュリティ事故の報告

ア）職員等は、情報セキュリティ事故を認知した場合、速やかに情報管理者に報告しなければならない。

イ）報告を受けた情報管理者は、速やかに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。

ウ）情報システム管理者は、報告のあった情報セキュリティ事故について、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。

② 住民等外部からの情報セキュリティ事故等の報告

ア）職員等は、本消防組合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事故について、住民等外部から報告を受けた場合、情報管理者に報告しなければならない。

イ）報告を受けた情報管理者は、速やかに事象を確認したうえで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。

ウ）情報セキュリティ責任者は、当該情報セキュリティ事故について、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。

③ 情報セキュリティ事故原因の究明・記録、再発防止等

ア）統括情報セキュリティ責任者は、ＣＳＩＲＴ責任者として他のＣＳＩＲＴ担当と連携し、報告された情報セキュリティ事故の可能性について状況を確認し、情報セキュリティ事故であるかの評価を行わなければならない。

イ）ＣＳＩＲＴは、情報セキュリティ事故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。

ウ）ＣＳＩＲＴは、情報セキュリティ事故に関係する情報管理者及び情報システム管理者に対し、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。

エ）ＣＳＩＲＴは、情報セキュリティ事故の対応状況について、ＣＩＳＯの他に千葉県、総務省、ＮＩＳＣに報告する。

オ）ＣＳＩＲＴは、これらの情報セキュリティ事故原因を究明し、記録を保存しなければならない。また、情報セキュリティ事故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。

カ）ＣＩＳＯは、情報セキュリティ責任者から、情報セキュリティ事故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。

（６）ＩＤ及びパスワード等の管理

①職員等は、自己の管理するログイン用ＩＤに関し、次の事項を遵守しなければならない。

ア）自己が利用しているＩＤは、他人に利用させてはならない。

イ）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。

②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。

ア）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。

イ）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。

ウ）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（アルファベットの大文字及び小文字の両方を用い、数字や記号を織り交ぜる等）にしなければならない。

エ）パスワードが流出したおそれがある場合には、情報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。

オ）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。

カ）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。

キ）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。

ク）職員等間でパスワードを共有してはならない（ただし、共用 ID に対するパスワードは除く）。

６．技術的セキュリティ

６．１．サーバ等及びネットワークの管理

（１）共有ファイルサーバの設定

① 情報システム管理者は、職員等が使用できるファイルサーバを用意しなければならない。

② 情報システム管理者は、ファイルサーバを課等の単位で構成し、その領域に保存できる容量を指定したうえで職員等が他課等のフォルダ及びファイルを閲覧及び使用できないように、設定しなければならない。

③ 情報システム管理者は、住民の個人情報、人事記録等、特定の職員等しか取扱えないデータについて、別途領域を作成する等の措置を講じ、同一所属であっても、担当以外の職員等が閲覧等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

情報システム管理者は、業務システムのデータベースやファイルサーバ等に記録された情報について、定期的にバックアップを実施しなければならない。

（３）システム管理記録及び作業の確認

① 情報管理者は、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 情報管理者は、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 システムの変更作業を行う場合は、複数名で実施し、互いに作業を確認しなければならない。

（４）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。

（５）ログの取得等

① 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 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。

（６）障害記録

情報管理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。

（７）ネットワークの接続制御、経路制御等

① 情報システム管理者は、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 情報システム管理者は、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。

（８）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 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。

（９）複合機のセキュリティ管理

① 情報システム管理者は、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 情報システム管理者は、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事故への対策を講じなければならない。

③ 情報システム管理者は、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。

（１０）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 情報システム管理者は、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。

（１１）電子メールのセキュリティ管理

① 情報システム管理者は、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 情報システム管理者は、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。

（１２）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、情報管理者に報告しなければならない。

（１３）暗号化

① 職員は、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、パスワード等による暗号化等、セキュリティを考慮して送信しなければならない。

② 暗号化に用いた暗号鍵及び暗号化された行政情報は、別々に適切な管理をしなければならない。

（１４）ソフトウェアの導入

① 職員は、新たにソフトウェアを導入する場合は、情報システム管理者及び情報管理者の許可を得なければならない。

② 職員は、正規のライセンスのないソフトウェアを導入してはならない。

③ 職員は、業務上不必要なソフトウェア及び出所不明なソフトウェア等を導入してはならない。

④ 情報システム管理者及び情報管理者は、ソフトウェアのライセンスを管理しなければならない。

（１５）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・機器交換及びＳＩＭカード等の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、情報システム管理者の許可を得なければならない。

（１６）無許可でのネットワーク接続の禁止

職員等は、情報システム管理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。

（１７）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 情報システム管理者は、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、情報管理者に通知し適切な措置を求めなければならない。

（１８）Ｗｅｂ会議サービスの利用時の対策

① 職員等は、Ｗｅｂ会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。

② 職員等は、Ｗｅｂ会議を主催する場合、会議に無関係の者が参加できないよう対策を講じること。

（１９）ソーシャルメディアサービスの利用

① 本消防組合のアカウントによる情報発信が、実際の本消防組合のものであることを明らかにするために、本消防組合のＷｅｂサイト（ホームページ）に当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。

② 重要性分類Ⅱ以上の情報はソーシャルメディアサービスで発信してはならない。

③ 利用するソーシャルメディアサービスごとの責任者を定めなければならない。

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

６．２．アクセス制御

（１）アクセス制御等

① 情報管理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 情報管理者及び情報システム管理者は、利用者の登録、変更、抹消等に係るＩＤの取扱い方法を定めなければならない。

③ 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、情報管理者又は情報システム管理者に届け出なければならない。

④ 情報管理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、確認しなければならない。

⑤ 情報管理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厳重に管理しなければならない。

（２）自動識別の設定

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。

（３）パスワードに関する情報の管理

① 情報システム管理者及び情報管理者は、職員等のパスワードに関する情報を厳重に管理しなければならない。パスワードファイルを不正利用から保護するため、オペレーティングシステム等でパスワード設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

② 情報システム管理者及び情報管理者は、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。

（４）特権による接続時間の制限

情報システム管理者及び情報管理者は、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 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 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における責任者及び作業者の特定

① 情報システムの開発を行う場合は責任者及び作業者を選任しなければならない。

② 情報システム管理者又は情報管理者はシステム開発に従事する職員等のＩＤ及びアクセス権限を適切に管理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）情報システムを導入する場合、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準備するよう努める。

イ）情報システムの移行にあたっては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。

ウ）情報システム管理者又は情報管理者は、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）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）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。また、個人情報等機密性の高いデータを、テストデータに使用してはならない。

（４）システム開発・保守に関連する資料等の整備・保管

情報システム管理者及び情報管理者は、システム開発・保守に関連する仕様書及び導入作業に係る文書等の資料を適切に整理・保管しなければならない。また、システムを変更した場合は、プログラム仕様書等の変更記録を作成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

情報システムの導入又は改修を行った場合、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、出力されることを確認しなければならない。

６．４．不正プログラム対策

（１）不正プログラム対策

① 情報システム管理者は、コンピュータウィルス等の不正プログラムを検出・駆除する対策プログラム及び外部ネットワーク接続点での対策機器を導入し、不正プログラムによる被害発生を防止しなければならない。

② コンピュータウィ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。

③ 不正プログラム対策ソフトウェア及び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。

④ 業務で利用するソフトウェアは、パッチ提供等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）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 情報システム管理者が提供するウィルス情報を、常に確認しなければならない。

⑥ 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情報システムに取り込む場合は無害化しなければならない。

⑦ ウィルスに感染した疑いがある場合には、ネットワークの接続を外し、感染の拡大を防がなければならない。また、速やかに情報システム管理者に報告しなければならない。

（３）専門家の支援体制

情報システム管理者は、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）不正アクセス対策

① 情報システム管理者は、情報システムのセキュリティに関する情報を常に収集し、メーカー等から修正プログラムの提供があった時は、速やかに対応しなければならない。

② 情報管理者は、情報システムに不正アクセスの疑いがある場合には、情報システム管理者に報告し、適切な措置を講じなければならない。

③ 職員からの不正アクセスがあった場合は、当該情報システムを所掌する情報管理者及び当該職員が属する情報管理者並びに情報システム管理者に報告し、必要な措置を講じなければならない。

④ 統括情報セキュリティ責任者は、監視、報告、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、システムの停止を含む必要な措置を講じなければならない。また、関係機関と連絡を密にして情報の収集に努めなければならない。

（３）記録の保存

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）サービス不能攻撃

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。

（５）標的型攻撃

統括情報セキュリティ責任者、情報セキュリティ責任者、情報システム管理者及び情報管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。

６．６．セキュリティ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

情報管理者は、情報システムの運用にあたっては、常に情報システムを監視するとともに情報セキュリティに対して注意を払わなければならない。

７．２．情報セキュリティポリシーの遵守状況の確認

（１）情報セキュリティポリシーの遵守状況

統括情報セキュリティ責任者及び情報管理者は、情報セキュリティポリシーの遵守状況について、また、運用上支障が生じていないかについて確認を行わなければならない。

（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。

７．３．情報セキュリティ侵害時の対応等

（１）緊急時対応計画の策定

ＣＩＳＯは、情報セキュリティ事故、情報セキュリティポリシーの違反等により情報資産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

① 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。

② 関係者の連絡先

③ 発生した事案に係る報告すべき事項

④ 発生した事案への対応措置

⑤ 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、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

情報システム管理者及び情報管理者は、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

情報システム管理者及び情報管理者は、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．法令等の遵守及び違反時の対応

（1）法令遵守義務

職員は、使用する情報資産について、次の法令を遵守しなければならない。また、マナーと倫理をもって情報システムを利用しなければならない。

なお、情報セキュリティポリシーに違反した者については、その重大性及び発生した事案の状況等に応じ、関係法令に定めるところにより処分の対象とする。

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）

（2）懲戒処分

情報セキュリティポリシーに違反した職員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。

（3）違反時の対応

① 情報システム管理者は情報セキュリティポリシー及び実施手順書に違反した職員に対し、その者が所属する情報管理者を通じて改善を求める。
② 情報システム管理者は、情報管理者の指導による改善が認められない場合は、当該職員による情報システムの利用を停止する。

８．業務委託と外部サービスの利用

８．１．業務委託

（1）外部委託事業者の選定基準

① 情報管理者は、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等を参考にして、事業者を選定しなければならない。

（2）契約項目

重要な情報資産を取扱う業務を委託する場合には、委託事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

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
② 委託事業者の責任者、委託内容、作業者、作業場所の特定
③ 提供されるサービスレベルの保証
④ 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
⑤ 委託事業者の従業員に対する教育の実施
⑥ 提供された情報の目的外利用及び委託事業者以外の者への提供の禁止
⑦ 業務上知り得た情報の守秘義務
⑧ 再委託に関する制限事項の遵守
⑨ 委託業務終了時の情報資産の返還、廃棄等
⑩ 委託業務の定期報告及び緊急時報告義務
⑪ 消防組合による監査、検査
⑫ 消防組合による情報セキュリティ事故発生時の公表
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）

（３）確認・措置等

情報管理者は、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．外部サービスの利用（重要性分類Ⅱ以上の情報を取り扱う場合）

（１）外部サービスの利用に係る規定の整備

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

① 外部サービスを利用可能な業務及び情報システムの範囲並びに情報の取扱いを許可する場所を判断する基準（以下「外部サービス利用判断基準」という。）
② 外部サービス提供者の選定基準
③ 外部サービスの利用申請の許可権限者と利用手続
④ 外部サービス管理者の指名と外部サービスの利用状況の管理

（２）外部サービスの選定

① 情報管理者は、取り扱う情報の格付及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。
② 情報管理者は、外部サービスで取り扱う情報の格付及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。

また、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めること。

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

（イ）外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制

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

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

（オ）情報セキュリティインシデントへの対処方法

（カ）情報セキュリティ対策その他の契約の履行状況の確認方法

（キ）情報セキュリティ対策の履行が不十分な場合の対処方法

③ 情報管理者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含めること。

④ 情報管理者は、外部サービスの利用を通じて本消防組合が取り扱う情報の格付等を勘案し、必要に応じて以下の内容を外部サービス提供者の選定条件に含めること。

（ア）情報セキュリティ監査の受入れ

（イ）サービスレベルの保証

⑤ 情報管理者は、外部サービスの利用を通じて本消防組合が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて本消防組合の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めること。

⑥ 情報管理者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託されることにより生ずる脅威に対して情報セキュリティが十分に確保されるよう、外部サービス提供者の選定条件で求める内容を外部サービス提供者に担保させるとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を本消防組合に提供し、本消防組合の承認を受けるよう、外部サービス提供者の選定条件に含めること。また、外部サービス利用判断基準及び外部サービス提供者の選定基準に従って再委託の承認の可否を判断すること。

⑦ 情報管理者は、外部サービスの特性を考慮した上で、外部サービスが提供する部分を含む情報の流通経路全般にわたるセキュリティが適切に確保されるよう、情報の流通経路全般を見渡した形でセキュリティ設計を行った上で、情報セキュリティに関する役割及び責任の範囲を踏まえて、セキュリティ要件を定めること。

⑧ 統括情報セキュリティ責任者は、情報セキュリティ監査による報告書の内容、各種の認定・認証制度の適用状況等から、外部サービス提供者の信頼性が十分であることを総合的・客観的に評価し判断すること。

（３）外部サービスの利用に係る調達・契約

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

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

（４）外部サービスの利用承認

① 情報管理者は、外部サービスを利用する場合には、利用申請の許可権限者へ外部サービスの利用申請を行うこと。

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

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

（５）外部サービスを利用した情報システムの導入・構築時の対策

① 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方等を踏まえ、以下を含む外部サービスを利用して情報システムを構築する際のセキュリティ対策を規定すること。

（ア）不正なアクセスを防止するためのアクセス制御

（イ）取り扱う情報の機密性保護のための暗号化

（ウ）開発時におけるセキュリティ対策

（エ）設計・設定時の誤りの防止

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

（６）外部サービスを利用した情報システムの運用・保守時の対策

① 統括情報セキュリティ責任者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスを利用して情報システムを運用する際のセキュリティ対策を規定すること。

（ア）外部サービス利用方針の規定

（イ）外部サービス利用に必要な教育

（ウ）取り扱う資産の管理

（エ）不正アクセスを防止するためのアクセス制御

（オ）取り扱う情報の機密性保護のための暗号化

（カ）外部サービス内の通信の制御

（キ）設計・設定時の誤りの防止

（ク）外部サービスを利用した情報システムの事業継続

② 情報管理者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備すること。

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

（７）外部サービスを利用した情報システムの更改・廃棄時の対策

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

（ア）外部サービスの利用終了時における対策

（イ）外部サービスで取り扱った情報の廃棄

（ウ）外部サービスの利用のために作成したアカウントの廃棄

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

８．３．外部サービスの利用（重要性分類Ⅱ以上の情報を取り扱わない場合）

（１）外部サービスの利用に係る規定の整備

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

（ア）外部サービスを利用可能な業務の範囲

（イ）外部サービスの利用申請の許可権限者と利用手続

（ウ）外部サービス管理者の指名と外部サービスの利用状況の管理

（エ）外部サービスの利用の運用手順

（２）外部サービスの利用における対策の実施

① 職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で重要性分類Ⅱ以上の情報を取り扱わない場合の外部サービスの利用を申請すること。また、承認時に指名された外部サービス管理者は、当該外部サービスの利用において適切な措置を講ずること。

② 情報管理者は、職員等による外部サービスの利用申請を審査し、利用の可否を決定すること。また、承認した外部サービスを記録すること。

９．評価・見直し

（１）監査・自己点検

情報管理者は、当該部署の情報セキュリティが確保されていることを確認するため、監査及び自己点検を行い、必要に応じ改善措置を講じなければならない。

（２）評価及び見直しの対象となる事象の発生

ＣＩＳＯは、評価及び見直しが必要となる事象が発生した場合には、必要な見直しを行い、適切な情報セキュリティポリシーの維持及び運用に努めなければならない。