

新城市情報セキュリティポリシー

令和8年2月1日

新 城 市

＜ 目 次 ＞

第1章	総則	1
1.1	情報セキュリティポリシーの目的	1
1.2	本市における情報セキュリティの考え方	1
1.3	情報セキュリティポリシーの構成	1
第2章	情報セキュリティ基本方針	3
2.1	目的	3
2.2	定義	3
2.3	対象とする脅威	4
2.4	適用範囲	4
2.5	職員等及び外部委託事業者の遵守義務	5
2.6	情報セキュリティ対策	5
(1)	組織体制	5
(2)	情報資産の分類と管理	5
(3)	情報システム全体の強靱性の向上	5
(4)	物理的セキュリティ	5
(5)	人的セキュリティ	6
(6)	技術的セキュリティ	6
(7)	運用	6
(8)	外部委託と外部サービスの利用	6
2.7	情報セキュリティ監査及び自己点検の実施	6
2.8	情報セキュリティポリシーの見直し	6
2.9	情報セキュリティ対策基準の策定	6
2.10	情報セキュリティ実施手順の策定	6
第3章	情報セキュリティ対策基準	8
3.1	組織体制	8
(1)	最高情報セキュリティ責任者	8
(2)	統括情報セキュリティ責任者	8
(3)	情報セキュリティ責任者	9
(4)	情報セキュリティ管理者	9
(5)	情報システム管理者	9
(6)	情報システム担当者	9
(7)	情報セキュリティ所管課	9
(8)	情報セキュリティに関する意思決定	9
(9)	兼務の禁止	9
(10)	CSIRT の設置・役割	10
3.2	行政情報の分類と管理	11
(1)	情報資産の分類	11
(2)	情報資産の管理	12
3.3	情報システム全体の強靱性の向上	13
(1)	マイナンバー利用事務系	13
(2)	LGWAN 接続系	14
(3)	インターネット接続系	14
3.4	物理的セキュリティ	14

3.4.1	サーバー等の管理	14
(1)	機器の取付け	14
(2)	サーバーの冗長化	15
(3)	機器の電源	15
(4)	通信ケーブル等の配線	15
(5)	機器の定期保守及び修理	15
(6)	庁外への機器の設置	15
(7)	機器の廃棄等	15
3.4.2	管理区域（サーバ室等）の管理	16
(1)	管理区域の構造等	16
(2)	管理区域の入退室管理等	16
(3)	機器等の搬入出	16
3.4.3	通信回線及び通信回線装置の管理	16
3.4.4	職員等の利用する端末や記録媒体等の管理	17
3.5	人的セキュリティ	17
3.5.1	職員等の遵守事項	17
(1)	職員等の遵守事項	17
(2)	会計年度任用職員への対応	18
(3)	情報セキュリティポリシー等の掲示	18
(4)	外部委託事業者に対する説明	18
3.5.2	研修・訓練	19
(1)	情報セキュリティに関する研修・訓練	19
(2)	研修計画の策定及び実施	19
(3)	緊急時対応訓練	19
(4)	研修・訓練への参加	19
3.5.3	情報セキュリティインシデントの報告	19
(1)	庁内での情報セキュリティインシデントの報告	19
(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	20
(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	20
3.5.4	ID 及びパスワード等の管理	20
(1)	IC カード等の取扱い	20
(2)	ID の取扱い	20
(3)	パスワードの取扱い	21
3.6	技術的セキュリティ	21
3.6.1	コンピューター及びネットワークの管理	21
(1)	文書サーバーの設定等	21
(2)	バックアップの実施	21
(3)	他団体との情報システムに関する情報等の交換	21
(4)	システム管理記録及び作業の確認	22
(5)	情報システム仕様書等の管理	22
(6)	ログの取得等	22
(7)	障害記録	22
(8)	ネットワークの接続制御、経路制御等	22
(9)	外部の者が利用できるシステムの分離等	23
(10)	外部ネットワークとの接続制限等	23

(11)	複合機のセキュリティ管理.....	23
(12)	IoT 機器を含む特定用途機器のセキュリティ管理	23
(13)	無線 LAN のセキュリティ対策及びネットワークの盗聴対策.....	24
(14)	電子メールのセキュリティ管理	24
(15)	電子メールの利用制限	24
(16)	電子署名・暗号化.....	24
(17)	無許可ソフトウェアの導入等の禁止	24
(18)	機器構成の変更の制限	25
(19)	業務外ネットワークへの接続の禁止	25
(20)	業務以外の目的でのウェブ閲覧の禁止	25
(21)	Web 会議サービスの利用時の対策	25
(22)	ソーシャルメディアサービスの利用	25
3.6.2	アクセス制御	26
(1)	アクセス制御等	26
(2)	職員等による外部からのアクセス等の制限	26
(3)	自動識別の設定	27
(4)	認証情報の管理	27
(5)	特権による接続時間の制限	27
3.6.3	システム開発、導入、保守等	27
(1)	情報システムの調達.....	27
(2)	情報システムの開発.....	28
(3)	情報システムの導入.....	28
(4)	情報システムの基盤を管理又は制御するソフトウェア導入時の対策.....	29
(5)	情報システムの基盤を管理又は制御するソフトウェア運用時の対策.....	29
(6)	システム開発・保守に関連する資料等の整備・保管.....	29
(7)	情報システムにおける入出力データの正確性の確保.....	29
(8)	情報システムの変更管理	30
(9)	開発・保守用のソフトウェアの更新等	30
(10)	システム更新又は統合時の検証等.....	30
(11)	情報システムについての対策の見直し	30
3.6.4	不正プログラム対策	30
(1)	統括情報セキュリティ責任者の措置事項	30
(2)	情報システム管理者の措置事項	31
(3)	職員等の遵守事項	31
(4)	専門家の支援体制	31
3.6.5	不正アクセス対策.....	32
(1)	統括情報セキュリティ責任者の措置事項	32
(2)	攻撃への対処.....	32
(3)	記録の保存	32
(4)	内部からの攻撃	32
(5)	職員等による不正アクセス	32
(6)	サービス不能攻撃	32
(7)	標的型攻撃	32
3.6.6	セキュリティ情報の収集.....	33
(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	33

(2) 不正プログラム等のセキュリティ情報の収集・周知.....	33
(3) 情報セキュリティに関する情報の収集及び共有	33
3.7 運用	33
3.7.1 情報システムの監視	33
(1) 情報システムの運用・保守時の対策.....	33
(2) 情報システムの監視機能	33
(3) 情報システムの監視.....	33
3.7.2 情報セキュリティポリシーの遵守状況の確認	34
(4) 遵守状況の確認及び対処	34
(5) パソコン、モバイル端末及び記録媒体等の利用状況調査	34
(6) 職員等の報告義務	34
3.7.3 セキュリティ侵害時の対応	34
(1) 新城市情報セキュリティ事故対応ガイドラインの策定.....	34
(2) 新城市情報セキュリティ事故対応ガイドラインに盛り込むべき内容.....	34
(3) 業務継続計画との整合性確保.....	35
(4) 新城市情報セキュリティ事故対応ガイドラインの見直し	35
3.7.4 例外措置.....	35
(1) 例外措置の許可	35
(2) 緊急時の例外措置	35
(3) 例外措置の申請書の管理	35
3.7.5 法令遵守.....	35
3.7.6 懲戒処分等	35
(1) 懲戒処分	35
(2) 違反時の対応.....	35
3.8 外部サービスの利用	36
3.8.1 外部委託.....	36
(1) 外部委託事業者の選定基準	36
(2) 契約項目	36
(3) 確認・措置等.....	36
3.8.2 約款による外部サービスの利用	37
(1) 約款による外部サービスの利用に係る規定の整備	37
(2) 約款による外部サービスの利用における対策の実施.....	37
3.9 評価・見直し	37
3.9.1 監査	37
(1) 実施方法	37
(2) 監査を行う者の要件.....	37
(3) 監査実施計画の立案及び実施への協力	37
(4) 外部委託事業者に対する監査.....	37
(5) 報告.....	37
(6) 保管.....	38
(7) 監査結果への対応	38
(8) 情報セキュリティポリシーの見直し等への活用	38
3.9.2 自己点検.....	38
(1) 実施方法	38
(2) 報告.....	38

(3) 自己点検結果の活用.....	38
3.9.3 情報セキュリティポリシー及び関係規定等の見直し.....	38

第1章 総則

1.1 情報セキュリティポリシーの目的

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。

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するため、継続的に情報漏えいの防止やセキュリティ水準の向上のためのさまざまな対策を行っていく必要がある。情報セキュリティ対策を行っていく上で、まず、組織として意思統一し、明文化した行動原則としての文書を示すことが重要であり、組織内のセキュリティを維持するために必要な方針、体制、対策等を「新城市情報セキュリティポリシー」として包括的に示す。

1.2 本市における情報セキュリティの考え方

本市は、法令等に基づき、市民の個人情報や企業の経営情報等の重要情報を多数保有するとともに、他に代替することができない行政サービスを提供している。また、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、市民生活や地域の社会経済活動を保護するため、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、市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、本市においても、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、情報セキュリティインシデントの未然防止のみならず、事故が発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じていくことが必要である。

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

1.3 情報セキュリティポリシーの構成

情報セキュリティポリシーは、本市が所掌する情報資産に関する業務に携わる職員等に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、

技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを、一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に依存する部分（対策基準）に分けて策定することとした。

具体的には、情報セキュリティポリシーを、

- ① 情報セキュリティ基本方針
- ② 情報セキュリティ対策基準

の2階層に分け、それぞれを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、情報システム毎の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（下図参照）。

情報セキュリティポリシーの構成

文 書 名		内 容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準。
情報セキュリティ実施手順		ネットワーク及び情報システム毎に定める情報セキュリティ対策基準に基づいた具体的な実施手順

第2章 情報セキュリティ基本方針

2.1 目的

本市が取り扱う情報資産には、市民の個人情報をはじめとし、行政運営上重要な情報など、外部への漏えい等が発生した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、これらの情報資産を様々な脅威から防御し、高度な安全性を保つことは、市民等の財産、プライバシーの保護、行政事務の安定的な運営のためにも必要不可欠である。ひいては、このことが本市に対する市民等からの信頼の維持向上に寄与するものである。

そのため、本市の情報資産の機密性、完全性及び可用性を維持するための対策（情報セキュリティ対策）を整備するために本市情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については、本市の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

2.2 定義

(1) ネットワーク

コンピューター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

コンピューター、ネットワーク、記録媒体及び周辺機器で構成され、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（マイナンバー利用事務系を除く。）。

(10) インターネット接続系

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

(11) 通信経路の分割

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

(12) 無害化通信

インターネットメールのウイルスチェックや端末への画面転送等により、コンピューターウイルス等の不正プログラムの影響を受けない安全が確保された通信をいう。

2.3 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

2.4 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、教育部（小・中学校を除く）、議会事務局、監査委員事務局、選挙管理委員会事務局、公平委員会事務局、固定資産評価審査委員会事務局、農業委員会事務局、上下水道部、市民病院（経営管理部門）及び消防本部とする。

(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、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

情報資産の種類	情報資産の例
ネットワーク	通信回線、ルーター等の通信機器
情報システム	サーバー、パソコン、モバイル端末、汎用機、オペレーティングシステム、ソフトウェア等
これらに関する施設・設備	コンピューター室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル
記録媒体	サーバー装置、端末、通信回線装置等に内蔵される内蔵記録媒体と、USBフラッシュメモリ、外付けハードディスクドライブ、光学的記録媒体、磁気テープ等の外部記録媒体
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

2.5 職員等及び外部委託事業者の遵守義務

職員、会計年度任用職員（以下「職員等」という。）及び外部委託事業者は、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。

2.6 情報セキュリティ対策

上記2.3の脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

(1) 組織体制

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

(2) 情報資産の分類と管理

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

(3) 情報システム全体の強靱性の向上

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

- ① マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で住民情報の流出を防ぐ。
- ② LGWAN接続系においては、LGWANと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。
- ③ インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、愛知県と愛知県内市町村のインターネット接続口を集約した、あいち情報セキュリティクラウドへの接続を実施する。

(4) 物理的セキュリティ

サーバー、サーバ室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

(5) 人的セキュリティ

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

(6) 技術的セキュリティ

コンピューター等の管理、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、新城市情報セキュリティ事故対応ガイドラインを策定する。

(8) 外部委託と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。

2.7 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。

2.8 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、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

2.9 情報セキュリティ対策基準の策定

上記 2.6、2.7 及び 2.8 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。

2.10 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。

第3章 情報セキュリティ対策基準

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。

3.1 組織体制

(1) 最高情報セキュリティ責任者

- ① 副市長を最高情報セキュリティ責任者（CISO：Chief Information Security Officer、以下「CISO」という。）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。
- ② CISO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。
- ③ CISO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。
- ④ CISOは、CISOを助けて本市における情報セキュリティに関する事務を整理し、CISOの命を受けて本市の情報セキュリティに関する事務を統括する最高情報セキュリティ副責任者（以下「副CISO」という。）1人を必要に応じて置く。
- ⑤ CISOは、本対策基準に定められた自らの担務を、副CISOその他の本対策基準に定める責任者に担わせることができる。

(2) 統括情報セキュリティ責任者

- ① 情報政策を所管する部長を CISO 直属の統括情報セキュリティ責任者とする。統括情報セキュリティ責任者は、CISO 及び副 CISO を補佐しなければならない。
- ② 統括情報セキュリティ責任者は、CISO が不在となった場合は、CISO の代理を務める。
- 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。
- ④ 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。
- ⑤ 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。
- ⑥ 統括情報セキュリティ責任者は、本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、CISO の指示に従い、CISO が不在の場合には自らの判断に基づき、必要かつ十分な措置を実施する権限及び責任を有する。
- ⑦ 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。
- ⑧ 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。
- ⑨ 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。
- ⑩ 統括情報セキュリティ責任者は、情報セキュリティ関係規程に係る課題及び問題点を含む運用状況を適時に把握し、必要に応じて CISO にその内容を報告しなければならない。

(3) 情報セキュリティ責任者

- ① 内部部局の長、議会事務局長、監査委員事務局長、上下水道部の長、市民病院（経営管理部門）の長及び消防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、会計年度任用職員（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、議会事務局長の課長、監査委員事務局長の課長、上下水道部の課室長、市民病院（経営管理部門）の課室長及び消防本部の課長を、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 CIS0 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) 情報セキュリティ所管課

情報政策を所管する課を情報セキュリティ所管課とする。

(8) 情報セキュリティに関する意思決定

本市の情報セキュリティ対策を統一的に実施するための、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は、市政経営会議等にて諮ったうえで決定する。

(9) 兼務の禁止

- ① 情報セキュリティ対策の実施において、やむを得ない場合を除き、承認又は許可の申請を

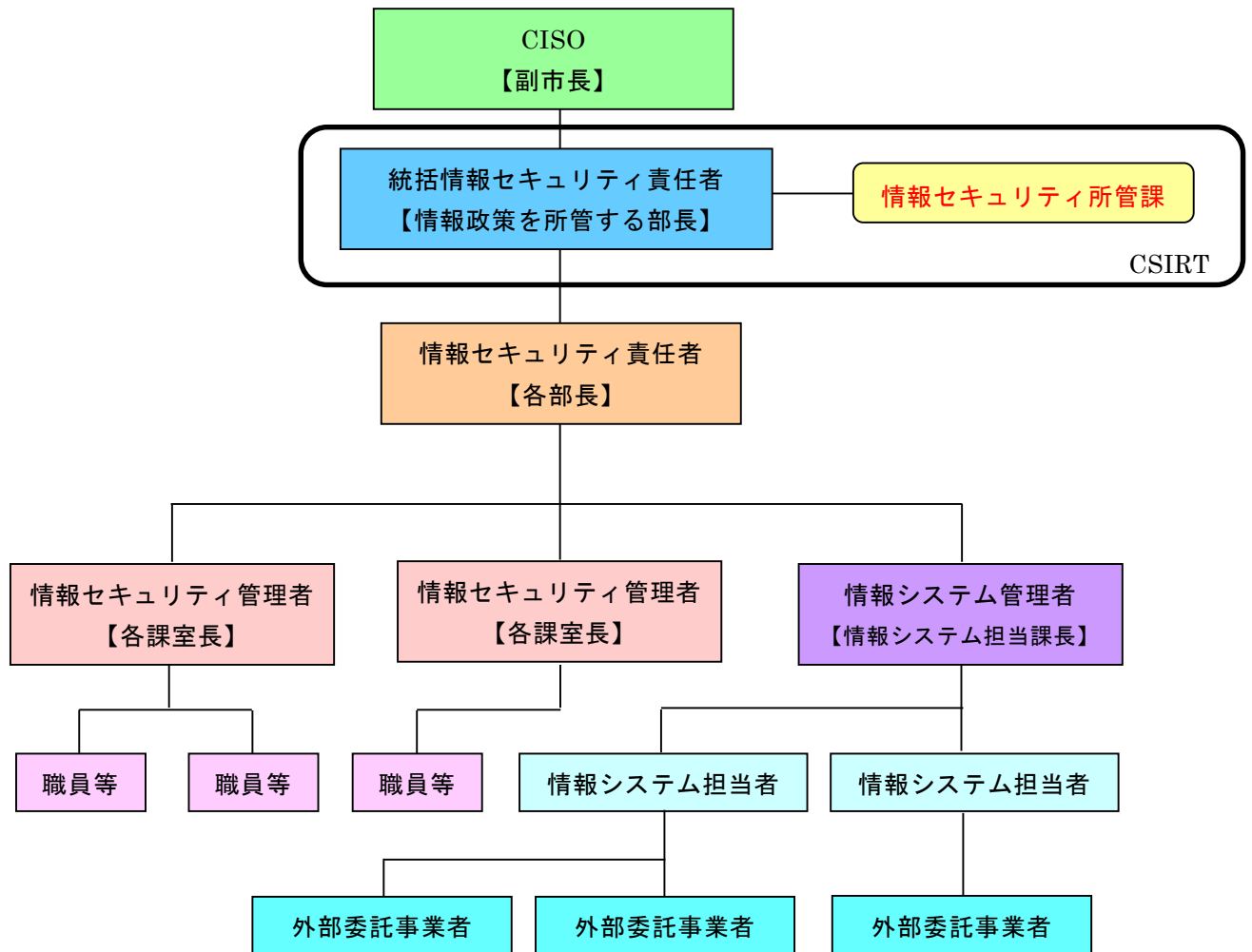
行う者とその承認者又は許可者は、同じ者が兼務してはならない。

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

(10) CSIRT の設置・役割

- ① CISOは、CSIRTを整備し、その役割を明確化しなければならない。
- ② CISOは、CSIRTに所属する職員等を選任し、その中からCSIRT責任者を置かなければならない。また、CSIRT内の業務統括及び外部との連携等を行う職員等を定めなければならない。
- ③ CISOは、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備しなければならない。
- ④ CISO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、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は、その内容を関係部局等に提供しなければならない。
- ⑤ 情報セキュリティインシデントを認知した場合には、CISO、総務省、愛知県へ報告しなければならない。
- ⑥ 情報セキュリティインシデントを認知した場合には、その重要度や影響範囲等を勘案し、報道機関への通知・公表対応を行わなければならない。
- ⑦ 情報セキュリティに関して、関係機関や他の地方公共団体の情報セキュリティに関する統一的な窓口の機能を有する部署、外部の事業者等との情報共有を行わなければならない。

情報セキュリティ推進の組織体制



3.2 行政情報の分類と管理

(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
自治体 機密性 3 A	行政事務で取り扱う情報資産のうち、「行政文書の管理に関するガイドライン」（平成 23 年 4 月 1 日内閣総理大臣決定）に定める秘密文書に相当する機密性を要する文書	<ul style="list-style-type: none"> ・ 支給以外の端末での作業の原則禁止（自治体機密性 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記録媒体等の持ち込み禁止
自治体 機密性 3 B	行政事務で取り扱う情報資産のうち、漏えい等が生じた際に、個人の権利利益の侵害の度合いが大きく、事務又は業務の規模や性質上、取扱いに非常に留意すべき情報資産	<ul style="list-style-type: none"> ・ 運搬・提供時における安全性の確保 ・ 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
自治体	行政事務で取り扱う情報資産のうち、	<ul style="list-style-type: none"> ・ 記録媒体の施錠可能な場所への保管

機密性 3 C	自治体機密性 3B 以上に相当する機密性は要しないが、基本的に公表することを前提としていないもので、業務の規模や性質上、取扱いに留意すべき情報資産	
自治体 機密性 2	行政事務で取り扱う情報資産のうち、自治体機密性 3 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	
自治体 機密性 1	自治体機密性 2 又は自治体機密性 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
自治体 完全性 2	行政事務で取り扱う情報資産のうち、改ざん、誤びゅう又は破損により、住民の権利が侵害される、又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	<ul style="list-style-type: none"> ・ バックアップ、電子署名付与 ・ 外部で情報処理を行う際の安全管理措置の規定 ・ 記録媒体の施錠可能な場所への保管
自治体 完全性 1	自治体完全性 2 の情報資産以外の情報資産	—

可用性による情報資産の分類

分類	分類基準	取扱制限
自治体 可用性 2	行政事務で取り扱う情報資産のうち、滅失、紛失又は当該情報資産が利用不可能であることにより、住民の権利が侵害される、又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報資産	<ul style="list-style-type: none"> ・ バックアップ、指定する時間以内の復旧 ・ 記録媒体の施錠可能な場所への保管
自治体 可用性 1	自治体可用性 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。

③ 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。
- ④ 情報資産の利用
 - (ア) 情報資産を利用する者は、業務以外の目的に情報資産を利用してはならない。
 - (イ) 情報資産を利用する者は、情報資産の分類に応じ、適正な取扱いをしなければならない。
 - (ウ) 情報資産を利用する者は、記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該記録媒体を取り扱わなければならない。
- ⑤ 情報資産の保管
 - (ア) 情報セキュリティ管理者又は情報システム管理者は、情報資産の分類に従って、情報資産を適正に保管しなければならない。
 - (イ) 情報セキュリティ管理者又は情報システム管理者は、情報資産を記録した記録媒体を長期保管する場合は、改変してはならない。
 - (ウ) 情報セキュリティ管理者又は情報システム管理者は、自治体機密性2以上、自治体完全性2又は自治体可用性2の情報を記録した記録媒体を保管する場合、防災対策を講じた施設可能な場所に保管しなければならない。
- ⑥ 情報の送信
 - 電子メール等により自治体機密性2以上の情報を送信する者は、必要に応じパスワード等による情報漏えいへの対策を行わなければならない。
- ⑦ 情報資産の運搬
 - (ア) 車両等により自治体機密性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) 自治体機密性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。
- ⑧ 情報資産の提供・公表
 - (ア) 自治体機密性2以上の情報資産を外部に提供する者は、必要に応じパスワード等による情報漏えいへの対策を行わなければならない。
 - (イ) 自治体機密性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。
- ⑨ 情報資産の廃棄
 - (ア) 自治体機密性2以上の情報資産の廃棄やリース返却等を行う者は、情報を記録している記録媒体が不要になった場合、記録媒体の初期化等、情報を復元できないように処置した上で廃棄やリース返却等を行わなければならない。
 - (イ) 情報資産の廃棄やリース返却等を行う者は、行った処理について、日時、担当者及び処理内容を記録しなければならない。
 - (ウ) 情報資産の廃棄やリース返却等を行う者は、情報セキュリティ管理者の許可を得なければならない。

3.3 情報システム全体の強靱性の向上

(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。また、その外部接続先についてもインターネット等と接続してはならない。ただし、国等の公的機関が構築したシステム等、十分に安全性が確保された外部接続先については、この限りではなく、LGWANを経由して、インターネット等とマイナンバー利用事務系との双方向通信でのデータの移送を可能とする。

② 情報のアクセス及び持ち出しにおける対策

（ア） 情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用することが望ましい。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

① LGWAN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接続系に転送するインターネット環境で受信したインターネットメールは無害化しLGWAN接続系に転送する方式

（イ） インターネット接続系の端末又はシステムから、LGWAN接続系の端末へ画面を転送する方式

（ウ） 危険因子をファイルから除去し、又は危険因子がファイルに含まれていないことを確認し、インターネット接続系から取り込む方式

(3) インターネット接続系

① インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及びLGWANへの不適切なアクセス等の監視等の情報セキュリティ対策を講じることが望ましい。

② 愛知県及び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、関係省庁や愛知県等と連携しながら、情報セキュリティ対策を推進しなければならない。

3.4 物理的セキュリティ

3.4.1 サーバー等の管理

(1) 機器の取付け

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

(2) サーバーの冗長化

- ① 重要情報を格納しているサーバー、セキュリティサーバー、住民サービスに関するサーバー及びその他の基幹サーバーを可能な限り冗長化し、同一データを保持しなければならない。
- ② 情報システム管理者は、メインサーバーに障害が発生した場合に、速やかに復旧作業を行い、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。

(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、サーバー等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適正に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなければならない。
- ② 情報システム管理者は、統括情報セキュリティ責任者及び施設管理部門と連携し、落雷等による過電流に対して、サーバー等の機器を保護するための措置を講じなければならない。

(4) 通信ケーブル等の配線

- ① 統括情報セキュリティ責任者及び情報システム管理者は、施設管理部門と連携し、通信ケーブル及び電源ケーブルの損傷等を防止するために、配線収納管を使用する等必要な措置を講じなければならない。
- ② 統括情報セキュリティ責任者及び情報システム管理者は、主要な箇所の通信ケーブル及び電源ケーブルについて、施設管理部門から損傷等の報告があった場合、連携して対応しなければならない。
- ③ 統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク接続口（ハブのポート等）を他者が容易に接続できない場所に設置する等適正に管理しなければならない。
- ④ 統括情報セキュリティ責任者及び情報システム管理者は、自ら又は情報システム担当者及び契約により操作を認められた外部委託事業者以外の者が配線を変更、追加できないように必要な措置を講じなければならない。

(5) 機器の定期保守及び修理

- ① 情報システム管理者は、自治体可用性2のサーバー等の機器の定期保守を実施しなければならない。
- ② 情報システム管理者は、記録媒体を内蔵する機器を外部の事業者修理させる場合、内容を消去した状態で行わせなければならない。内容を消去できない場合、情報システム管理者は、外部の業者に故障を修理させるにあたり、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、庁外にサーバー等の機器を設置する場合、CIS0の承認を得なければならない。また必要に応じて、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。

3.4.2 管理区域（サーバ室等）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、当該機器等の管理及び運用を行うための部屋（以下「サーバ室」という。）や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、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、サーバ室内の機器等に、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。
- ⑥ 統括情報セキュリティ責任者及び情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器等及び記録媒体に影響を与えないようにしなければならない。
- ⑦ 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、サーバ室内の機器等をサーバー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、サーバーラックの施錠管理をしなければならない。

(2) 管理区域の入退室管理等

- ① 情報システム管理者は、管理区域への入退室を許可された者のみに制限し、ICカード、指紋認証等の生体認証又は入退室管理簿の記載による入退室管理を行わなければならない。
- ② 職員等及び外部委託事業者は、管理区域に入室する場合、身分証明書等を携帯し、求めにより提示しなければならない。
- ③ 情報システム管理者は、外部からの訪問者が管理区域に入る場合には、必要に応じて立ち入り区域を制限した上で、管理区域への入退室を許可された職員等が付き添うものとし、外見上職員等と区別できる措置を講じなければならない。
- ④ 情報システム管理者は、自治体機密性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、又は個人所有であるコンピューター、モバイル端末、通信回線装置、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、サーバ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。

3.4.3 通信回線及び通信回線装置の管理

- ① 統括情報セキュリティ責任者は、庁内の通信回線及び通信回線装置を、施設管理部門と連携し、適正に管理しなければならない。また、通信回線及び通信回線装置に関連する文書を適正に保管しなければならない。
- ② 統括情報セキュリティ責任者は、通信回線装置に対して適切なセキュリティ対策を実施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。
- ④ 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。
- ⑤ 統括情報セキュリティ責任者は、自治体機密性2以上の情報資産を取り扱う情報システムに通信回線を接続する場合、必要なセキュリティ水準を検討の上、適正な回線を選択しなければならない。また、必要に応じ、送受信される情報の暗号化を行わなければならない。
- ⑥ 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。
- ⑦ 統括情報セキュリティ責任者は、通信回線装置が動作するために必要なソフトウェアの状態等を必要性に応じて調査し、認識した脆弱性等について対策を講じなければならない。
- ⑧ 統括情報セキュリティ責任者は、自治体可用性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。

3.4.4 職員等の利用する端末や記録媒体等の管理

- 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、モバイル端末及び記録媒体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。記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去しなければならない。
- ② 情報システム管理者は、情報システムへのログインに際し、パスワード、スマートカード、或いは生体認証等複数の認証情報の入力が必要とするように設定することが望ましい。
- 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）を併用するなどセキュリティ対策に努めなければならない。
- ④ 情報システム管理者は、マイナンバー利用事務系では2回以上の認証を行うよう設定しなければならない。

3.5 人的セキュリティ

3.5.1 職員等の遵守事項

(1) 職員等の遵守事項

- ① 情報セキュリティポリシー等の遵守
職員等は、情報セキュリティポリシー及び実施手順を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者に相談し、指示を仰がなければならない。
- ② 業務以外の目的での使用の禁止
職員等は、業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。
- ③ モバイル端末や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) CIS0 は、自治体機密性2以上、自治体可用性2、自治体完全性2の情報資産を外部で処理する場合は、安全管理措置を定めなければならない。
 - (イ) 職員等は、パソコン等端末・記録媒体・情報資産及びソフトウェアを外部に持ち出す場合には、情報セキュリティ所管課に届出をしなければならない。

(ウ) 職員等は、外部で情報処理業務を行う場合には、情報セキュリティ所管課に届出をしなければならない。

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、モバイル端末及び記録媒体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、情報セキュリティ所管課に届出をしなければならない。

(イ) 職員等は、支給以外のパソコン、モバイル端末及び記録媒体等を用いる場合には、情報システム担当課に届出を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等の端末のソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者の許可なく変更してはならない。

⑦ 机上の端末等の管理

職員等は、パソコン、モバイル端末、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記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じなければならない。

⑧ 退職時等の遵守事項

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

(2) 会計年度任用職員への対応

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、会計年度任用職員に対し、採用時に情報セキュリティポリシー等のうち、会計年度任用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、会計年度任用職員の採用の際、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、会計年度任用職員にパソコン等の端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにしなければならない。

(3) 情報セキュリティポリシー等の掲示

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

(4) 外部委託事業者に対する説明

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

3.5.2 研修・訓練

(1) 情報セキュリティに関する研修・訓練

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

- ① CISO は、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を定期的に立案しなければならない。
- 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。
- ③ 新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。
- ④ 研修は、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者、情報システム担当者及びその他職員等に対して、それぞれの役割、情報セキュリティに関する理解度等に応じたものにしなければならない。
- ⑤ 情報セキュリティ管理者は、所管する課室等の研修の実施状況の把握に努めなければならない。
- ⑥ 統括情報セキュリティ責任者は、CISO に情報セキュリティ対策に関する研修の実施状況について報告しなければならない。

(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

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。

3.5.3 情報セキュリティインシデントの報告

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を発見した場合、又は外部からの事故等の報告があった場合は、「新都市情報セキュリティ事故対応ガイドライン」に従い、以下の対応を実施しなければならない。

(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、システム上の欠陥及び誤動作を発見した場合、速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口へ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。
- ④ 情報セキュリティインシデントにより、個人情報・特定個人情報の漏えい等が発生した場合、必要に応じて個人情報保護委員会へ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。
- ④ CISO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。

(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

- ① CSIRT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。
- ② CSIRT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。
- ③ CSIRT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。また、CSIRTは、同様の情報セキュリティインシデントが別の情報システムにおいても発生している可能性を検討し、必要に応じて当該情報システムを所管する情報システム管理者へ確認を指示しなければならない。
- ④ CSIRT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。
- ⑤ CISO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。

3.5.4 ID及びパスワード等の管理

(1) ICカード等の取扱い

- ① 職員等は、自己の管理するICカード等に関し、次の事項を遵守しなければならない。
 - (ア) 認証に用いるICカード等を、職員等間で共有してはならない。
 - (イ) 業務上必要のないときは、ICカード等をカードリーダー若しくはパソコン等の端末のスロット等から抜いておかななければならない。
 - (ウ) ICカード等を紛失した場合には、速やかに統括情報セキュリティ責任者及び情報システム管理者に通報し、指示に従わなければならない。
- ② 統括情報セキュリティ責任者及び情報システム管理者は、ICカード等の紛失等の通報があり次第、当該ICカード等を使用したアクセス等を速やかに停止しなければならない。
- ③ 統括情報セキュリティ責任者及び情報システム管理者は、ICカード等を切り替える場合、切替え前のカードを回収し、破砕するなど復元不可能な処理を行った上で廃棄しなければならない。

(2) IDの取扱い

職員等は、自己の管理するIDに関し、次の事項を遵守しなければならない。

- ① 自己が利用している ID は、他人に利用させてはならない。
- ② 共用 ID を利用する場合は、共用 ID の利用者以外に利用させてはならない。

(3) パスワードの取扱い

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

- ① パスワードは、他者に知られないように管理しなければならない。
- ② パスワードを秘密にし、パスワードの照会等には一切応じてはならない。
- ③ パスワードは 10 桁以上の長さとし、文字列は大文字小文字のアルファベットと数字・記号の内 3 種類以上を組み合わせ、想像しにくいものにしなければならない。
- ④ パスワードが流出したおそれがある場合には、情報セキュリティ管理者に速やかに報告し、パスワードを速やかに変更しなければならない。
- ⑤ 複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。
- ⑥ 仮のパスワード（初期パスワード含む）は、最初のログイン時点で変更しなければならない。
- ⑦ サーバー、ネットワーク機器及びパソコン等の端末に、パスワードを記憶させることで、パスワードの入力なしに認証を可能とする設定は行ってはならない。
- ⑧ 職員等間でパスワードを共有してはならない。（ただし共有 ID に対するパスワードは除く）

3.6 技術的セキュリティ

3.6.1 コンピューター及びネットワークの管理

(1) 文書サーバーの設定等

- 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ーの容量を設定し、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、文書サーバー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

- 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、ファイルサーバー等に記録された情報について、サーバー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。
- 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、重要な情報を取り扱うサーバー装置については、適切な方法でサーバー装置のバックアップを取得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、重要な情報を取り扱う情報システムを構成する通信回線装置については、運用状態を復元するために必要な設定情報等のバックアップを取得し保管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、情報システム及びソフトウェアに関する情報を交換する場合、その取扱いに関する事項をあらかじめ定め、統括情報セキュリティ責任者及び情報セキュリティ責任者の許可を得なければならない。

(4) システム管理記録及び作業の確認

- ① 情報システム管理者は、所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない。
- ② 統括情報セキュリティ責任者及び情報システム管理者は、所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理し、運用・保守によって機器の構成や設定情報等に変更があった場合は、情報セキュリティ対策が適切であるか確認し、必要に応じて見直さなければならない。
- 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。ただし、日常的に発生する定められた手順については報告を受けることで1名での作業を可能とする。

(5) 情報システム仕様書等の管理

統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク構成図、情報システム仕様書について、記録媒体に関わらず、業務上必要とする者以外の者が閲覧したり、紛失等がないよう、適正に管理しなければならない。

(6) ログの取得等

- ① 統括情報セキュリティ責任者及び情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。
- ② 統括情報セキュリティ責任者及び情報システム管理者は、ログとして取得する項目、保存期間、取扱方法及びログが取得できなくなった場合の対処等について定め、適正にログを管理しなければならない。
- ③ 統括情報セキュリティ責任者及び情報システム管理者は、取得したログを定期的に点検又は分析する体制を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

(7) 障害記録

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

(8) ネットワークの接続制御、経路制御等

- ① 統括情報セキュリティ責任者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルーター等の通信ソフトウェア等を設定しなければならない。
- ② 統括情報セキュリティ責任者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。
- ③ 統括情報セキュリティ責任者は、保守又は診断のために、外部の通信回線から内部の通信回線に接続された機器等に対して行われるリモートメンテナンスに係る情報セキュリティを確保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、必要に応じて見直さなければならない。
- ④ 異なるネットワーク間の接続については、統括情報セキュリティ責任者または情報セキュリティ所管課と協議をしなければならない。

(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、ウェブサーバー等をインターネットに公開する場合、次のセキュリティ対策を実施しなければならない。
 - (ア) 庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置したうえで接続しなければならない。
 - (イ) 脆弱性が存在する可能背が増大することを防止するため、ウェブサーバーが備える機能のうち、必要な機能のみを利用しなければならない。
 - (ウ) ウェブサーバーからの不用意な情報漏洩を防止するための措置を講じなければならない。
 - (エ) 情報システム管理者は、ウェブコンテンツの編集作業を行う主体を限定しなければならない。
 - (オ) インターネットを介して転送される情報の盗聴及び改ざんの防止のため、通信の暗号化及び電子証明書による認証の対策を講じるよう努めなければならない。
- 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、適正なセキュリティ要件を策定しなければならない。
- ② 統括情報セキュリティ責任者は、複合機が備える機能について適正な設定等を行うことにより運用中の複合機に対する情報セキュリティインシデントへの対策を講じなければならない。
- ③ 統括情報セキュリティ責任者は、複合機の運用を終了する場合、複合機の持つ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) IoT 機器を含む特定用途機器のセキュリティ管理

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

(13) 無線 LAN のセキュリティ対策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、電子メールサーバー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、情報セキュリティにおける重大なリスクがあると判断された場合は、メールサーバー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。

(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、電子メールを外部へ転送してはならない。
- ② 職員等は、業務上必要のない送信先に電子メールを送信してはならない。
- ③ 職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない。
- ④ 職員等は、重要な電子メールを誤送信した場合、情報セキュリティ管理者に報告しなければならない。
- ⑤ 職員等は、ウェブで利用できる電子メール、ネットワークストレージサービス等を使用する場合には、情報セキュリティ所管課に届出をしなければならない。

(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、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 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。
- ③ CISO 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、情報セキュリティ所管課に届出をすることでソフトウェアを導入できる。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) 業務外ネットワークへの接続の禁止

- ① 職員等は、支給された端末を、有線・無線を問わず、その端末を接続して利用するよう情報システム管理者によって定められたネットワークと異なるネットワークに接続してはならない。
- ② 情報セキュリティ管理者は、支給した端末について、端末に搭載された OS のポリシー設定等により、端末を異なるネットワークに接続できないよう技術的に制限することが望ましい。

(20) 業務以外の目的でのウェブ閲覧の禁止

- ① 職員等は、業務以外の目的でウェブを閲覧してはならない。
- ② 統括情報セキュリティ責任者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知し適正な措置を求めなければならない。

(21) Web 会議サービスの利用時の対策

- ① 統括情報セキュリティ責任者は、Web 会議を適切に利用するための利用手順を定めなければならない。
- ② 職員等は、本市の定める利用手順に従い、Web 会議の参加者や取り扱う情報に応じた情報セキュリティ対策を実施すること。
- ③ 職員等は、Web 会議を主催する場合、会議に無関係の者が参加できないよう対策を講ずること。
- ④ 職員等は、外部から Web 会議に招待される場合は、本市の定める利用手順に従い、必要に応じて利用申請を行い、承認を得なければならない。

(22) ソーシャルメディアサービスの利用

- ① 情報セキュリティ管理者は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。
 - (ア) 本市のアカウントによる情報発信が、実際の本市のものであることを明らかにするために、本市の自己管理 Web サイトに当該情報を掲載して参照可能とするとともに、当該アカウントの自由記述欄等にアカウントの運用組織を明示する等の方法でなりすまし対策を実施すること。
 - (イ) パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ハードディスク、USB フラッシュメモリ、紙等）等を適正に管理するなどの方法で、不正アクセス対策を実施すること。
- ② 自治体機密性 2 以上の情報はソーシャルメディアサービスで発信してはならない。
- ③ 利用するソーシャルメディアサービスごとの責任者を定めなければならない。
- ④ アカウント乗っ取りを確認した場合には、被害を最小限にするための措置を講じなければなら

らない。

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

3.6.2 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必要最小限の範囲で適切に設定する等、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。
- (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、主体から対象に対する不要なアクセス権限が付与されていないか、必要に応じて確認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は、管理者権限の特権を持つ主体の識別コード及び主体認証情報が、悪意ある第三者等によって窃取された際の被害を最小化するための措置及び、内部からの不正操作や誤操作を防止するための措置を講じるよう努めなければならない。
- (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。
- (エ) 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。
- (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 及びパスワードの変更について、外部委託事業者に行わせてはならない。
- (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 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するよう努めなければならない。
- (キ) 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、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、外部から持ち込んだ端末を、庁内のネットワークに接続してはならない。また、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、コンピューターウイルスに感染していないこと、パッチの適用状況等を確認し、情報セキュリティ管理者の許可を得るか、若しくは情報セキュリティ管理者によって事前に定義されたポリシーに従って接続しなければならない。
- ⑦ 統括情報セキュリティ責任者は、内部のネットワークまたは情報システムに対するインターネットを介した外部からのアクセスを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必要に応じてシステムを設定しなければならない。

(4) 認証情報の管理

- ① 統括情報セキュリティ責任者又は情報システム管理者は、職員等の認証情報を厳重に管理しなければならない。認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。
- ② 統括情報セキュリティ責任者又は情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、初回ログイン後直ちに仮のパスワードを変更させなければならない。ただし、仮のパスワードが発行されない場合はこの限りではない。
- 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。

(5) 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するよう努めなければならない。

3.6.3 システム開発、導入、保守等

(1) 情報システムの調達

- ① 統括情報セキュリティ責任者及び情報システム管理者は、情報システム開発、導入、保守等

の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を必要に応じて明記しなければならない。また、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮した技術的なセキュリティ機能を調達仕様書に記載するよう努めなければならない。

- 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、必要に応じて当該製品のセキュリティ機能を調査し、情報セキュリティ上問題のないことを確認しなければならない。

(2) 情報システムの開発

- ① システム開発における責任者及び作業者の特定
情報システム管理者は、システム開発の責任者及び作業者を特定しなければならない。
- ② システム開発における責任者、作業者の ID の管理
 - (ア) 情報システム管理者は、システム開発の責任者及び作業者が使用する ID を管理し、開発完了後、開発用 ID を削除しなければならない。
 - (イ) 情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。
- ③ システム開発に用いるハードウェア及びソフトウェアの管理
 - (ア) 情報システム管理者は、システム開発の責任者及び作業者が使用するハードウェア及びソフトウェアを特定しなければならない。
 - (イ) 情報システム管理者は、利用を認めたソフトウェア以外のソフトウェアが導入されている場合、当該ソフトウェアをシステムから削除しなければならない。
- ④ アプリケーション・コンテンツの開発時の対策
情報システム管理者は、ウェブアプリケーションの開発において、セキュリティ要件として定めた仕様に加えて、既知の種類のウェブアプリケーションの脆弱性を排除するための対策を講じなければならない。

(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。
 - (イ) 情報システム管理者は、システム開発・保守及びテスト環境からシステム運用環境への移行について、システム開発・保守計画の策定時に手順を明確にしなければならない。
 - (ウ) 情報システム管理者は、移行の際、情報システムに記録されている情報資産の保存を確実にし、移行に伴う情報システムの停止等の影響が最小限になるよう配慮しなければならない。
 - (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。

- (オ) 情報システム管理者は、業務システムに誤ったプログラム処理が組み込まれないよう、不具合を考慮したテスト計画を策定し、確実に検証が実施されるよう、必要かつ適切に外部委託事業者の監督を行うよう努めなければならない。

③ 機器等の納入時または情報システムの受け入れ時

- (ア) 情報システム管理者は、機器等の納入時又は情報システムの受け入れ時の確認・検査において、必要に応じて、情報セキュリティ対策に係る要件が満たされていることを確認しなければならない。
- (イ) 情報システム管理者は、情報システムが構築段階から運用保守段階へ移行する際に、当該情報システムの開発事業者から運用保守事業者へ引き継がれる項目に、情報セキュリティ対策に必要な内容が含まれていることを確認するよう努めなければならない。

(4) 情報システムの基盤を管理又は制御するソフトウェア導入時の対策

- ① 情報システム管理者は、情報セキュリティの観点から情報システムの基盤を管理又は制御するソフトウェアを導入する端末、サーバー装置、通信回線装置等及びソフトウェア自体を保護するための措置を講じるよう努めなければならない。
- ② 利用するソフトウェアの特性を踏まえ、必要に応じて、以下の実施手順を整備しなければならない。
 - (ア) 情報システムの基盤を管理又は制御するソフトウェアの情報セキュリティ水準維持に関する手順
 - (イ) 情報システムの基盤を管理又は制御するソフトウェアで発生した情報セキュリティインシデントを認知した際の対処手順

(5) 情報システムの基盤を管理又は制御するソフトウェア運用時の対策

- ① 情報システム管理者は、情報システムの基盤を管理又は制御するソフトウェアを運用・保守する場合は、必要に応じて、以下のセキュリティ対策を実施しなければならない。
 - (ア) 情報システムの基盤を管理又は制御するソフトウェアのセキュリティを維持するための対策
 - (イ) 脅威や情報セキュリティインシデントを迅速に検知し、対応するための対策
- ② 情報システム管理者は、利用を認めるソフトウェアについて、必要に応じて見直しを行わなければならない。

(6) システム開発・保守に関連する資料等の整備・保管

- ① 情報システム管理者は、システム開発・保守に関連する資料及びシステム関連文書を適正に整備・保管しなければならない。
- ② 情報システム管理者は、テスト結果を一定期間保管しなければならない。
- ③ 情報システム管理者は、必要に応じて納品させた情報システムに係るソースコードについて、適正な方法で保管しなければならない。

(7) 情報システムにおける入出力データの正確性の確保

- ① 情報システム管理者は、情報システムに入力されるデータについて、範囲、妥当性のチェック機能及び不正な文字列等の入力除去する機能を組み込むように情報システムを設計しなければならない。
- ② 情報システム管理者は、ウェブアプリケーションやウェブコンテンツにおいて、次のセキュリティ対策を実施することが望ましい。

- (ア) 利用者の情報セキュリティ水準の低下を招かぬよう、アプリケーションおよびウェブコンテンツの提供方式等を見直ししなければならない。
 - (イ) 運用中のアプリケーション・コンテンツにおいて、定期的に脆弱性対策の状況を確認し、脆弱性が発覚した際は必要な措置を講じなければならない。
 - (ウ) ウェブアプリケーションやウェブコンテンツにおいて、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。

(8) 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、必要に応じて、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。

(9) 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。

(10) 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。

(11) 情報システムについての対策の見直し

情報システム管理者は、情報システムの情報セキュリティ対策を、必要に応じて見直さなければならない。

3.6.4 不正プログラム対策

(1) 統括情報セキュリティ責任者の措置事項

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

- ① 外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピューター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ー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 コンピューター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 所掌するサーバー及びパソコン等の端末に、コンピューター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つように努めなければならない。
- 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つように努めなければならない。
- 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。また、当該製品の利用を予定している期間中に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する予定がないことを確認しなければならない。

(2) 情報システム管理者の措置事項

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

- ① 情報システム管理者は、その所掌するサーバー及びパソコン等の端末に、コンピューター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つように努めなければならない。
- 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つように努めなければならない。
- ④ インターネットに接続していないシステムにおいて、記録媒体を使う場合、コンピューターウイルス等の感染を防止するために、市が管理している媒体以外を職員等に利用させてはならない。また、不正プログラムの感染、侵入が生じる可能性が著しく低い場合を除き、不正プログラム対策ソフトウェアを導入し、定期的に当該ソフトウェア及びパターンファイルの更新を実施しなければならない。
- ⑤ 不正プログラム対策ソフトウェア等の設定変更権限については、一括管理し、情報システム管理者が許可した職員を除く職員等に当該権限を付与してはならない。

(3) 職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

- ① パソコンやモバイル端末において、不正プログラム対策ソフトウェアが導入されている場合は、当該ソフトウェアの設定を変更してはならない。
- ② 外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。
- ③ 差出人が不明又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。
- ④ 端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的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 コンピューターウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、事前に決められたコンピューターウイルス感染時の初動対応の手順に従って対応を行わなければならない。初動対応の手順が定められていない場合は、被害の拡大を防ぐ処置を慎重に検討し、該当の端末において LAN ケーブルの取り外しや、通信を行わない設定への変更などを実施しなければならない。

(4) 専門家の支援体制

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

3.6.5 不正アクセス対策

(1) 統括情報セキュリティ責任者の措置事項

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

- ① 使用されていないポートを閉鎖しなければならない。
- ② 不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 統括情報セキュリティ責任者は、情報セキュリティに関する統一的な窓口と連携し、監視、通知、外部連絡窓口及び適正な対応などを実施できる体制並びに連絡網を構築しなければならない。

(2) 攻撃への対処

CISO 及び統括情報セキュリティ責任者は、サーバー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、愛知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、サーバー等に攻撃を受け、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ー等に対する攻撃や、外部のサイトに対する攻撃を検知した場合、当該端末の通信を遮断しなければならない。

(5) 職員等による不正アクセス

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

(6) サービス不能攻撃

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

(7) 標的型攻撃

統括情報セキュリティ責任者及び情報システム管理者は、標的型攻撃による内部への侵入を防止するために、教育等の人的対策を講じなければならない。また、標的型攻撃による組織内部への侵入を低減する対策（入口対策）や内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、外部との不正通信を検知して対処する対策（内部対策及び出口対策）を講じるよう努めなければならない。

3.6.6 セキュリティ情報の収集

(1) セキュリティホールに関する情報の収集・共有及びソフトウェアの更新等

統括情報セキュリティ責任者及び情報システム管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じて、ソフトウェア更新等の対策を実施しなければならない。

(2) 不正プログラム等のセキュリティ情報の収集・周知

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

(3) 情報セキュリティに関する情報の収集及び共有

統括情報セキュリティ責任者及び情報システム管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有しなければならない。また、情報セキュリティに関する社会環境や技術環境等の変化によって新たな脅威を認識した場合は、セキュリティ侵害を未然に防止するための対策を速やかに講じなければならない。

3.7 運用

3.7.1 情報システムの監視

(1) 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及び情報セキュリティ管理者は、情報システムの運用・保守において、情報システムに実装された監視を含むセキュリティ機能を適切に運用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、情報システムの情報セキュリティ対策について新たな脅威の出現、運用、監視等の状況により見直しを適時検討し、必要な措置を講じなければならない。
- ③ 統括情報セキュリティ責任者及び情報セキュリティ管理者は、重要な情報を取り扱う情報システムについて、危機的事象発生時に適切な対処が行えるよう運用をしなければならない。

(2) 情報システムの監視機能

- ① 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は、必要に応じて、情報システム運用時の監視に係る運用管理機能要件を策定し、監視機能を実装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、情報システムの運用において、情報システムに実装された監視機能を適切に運用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、新たな脅威の出現、運用の状況等を踏まえ、情報システムにおける監視の対象や手法を必要に応じて見直し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、サーバー装置上での情報セキュリティインシデントの発生を監視するため、必要に応じて、当該サーバー装置を監視するための措置を講じなければならない。

(3) 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ーの正確な時刻設定及びサーバー間の時刻同期ができる措置を講じなければならない。
- ③ 統括情報セキュリティ責任者及び情報システム管理者は、外部と常時接続するシステムを常

時監視しなければならない。

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

3.7.2 情報セキュリティポリシーの遵守状況の確認

(4) 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。
- ② CISO は、発生した問題について、適正かつ速やかに対処しなければならない。
- ③ 統括情報セキュリティ責任者及び情報システム管理者は、ネットワーク及びサーバー等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処しなければならない。

(5) パソコン、モバイル端末及び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。

(6) 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場合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、新城市情報セキュリティ事故対応ガイドラインに従って適正に対処しなければならない。

3.7.3 セキュリティ侵害時の対応

(1) 新城市情報セキュリティ事故対応ガイドラインの策定

CISO は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適正に実施するために、新城市情報セキュリティ事故対応ガイドラインを定めておき、セキュリティ侵害時には当該ガイドラインに従って適正に対処しなければならない。

(2) 新城市情報セキュリティ事故対応ガイドラインに盛り込むべき内容

新城市情報セキュリティ事故対応ガイドラインには、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業務継続計画を策定する場合、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) **新城市情報セキュリティ事故対応ガイドラインの見直し**

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、必要に応じて新城市情報セキュリティ事故対応ガイドラインの規定を見直さなければならない。

3.7.4 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する又は遵守事項を実施しないことについて合理的な理由がある場合には、CISO の許可を得て、例外措置を講じることができる。

(2) **緊急時の例外措置**

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

(3) **例外措置の申請書の管理**

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

3.7.5 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 26 年法律第 104 号)

3.7.6 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、適正な措置を求めなければならない。
- ② 情報システム管理者等が違反を確認した場合は、違反を確認した者は速やかに統括情報セキュリティ責任者及び当該職員等が所属する課室等の情報セキュリティ管理者に通知し、適正な措置を求めなければならない。
- ③ 情報セキュリティ管理者の指導によっても改善されない場合、統括情報セキュリティ責任者は、当該職員等のネットワーク又は情報システムを使用する権利を停止あるいは剥奪することができる。その後速やかに、統括情報セキュリティ責任者は、職員等の権利を停止あるいは剥奪した旨を CISO 及び当該職員等が所属する課室等の情報セキュリティ管理者に通知しなければならない。

3.8 外部サービスの利用

3.8.1 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。
- 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、作業者の所属、作業場所の特定
- ・ 提供されるサービスレベルの保証
- ・ 外部委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法
- ・ 外部委託事業者の従業員に対する教育の実施
- ・ 提供された情報の目的外利用及び受託者以外の者への提供の禁止
- ・ 業務上知り得た情報の守秘義務
- ・ 再委託に関する制限事項の遵守
- ・ 委託業務終了時の情報資産の返還、廃棄等
- ・ 委託業務の定期報告及び緊急時報告義務
- ・ 市による監査、検査
- ・ 市による情報セキュリティインシデント発生時の公表
- ・ 情報セキュリティポリシーが遵守されなかった場合の規定（損害賠償等）

(3) 確認・措置等

情報セキュリティ管理者は、外部委託事業者において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、（２）の契約に基づき措置を実施しなければならない。ま

た、その内容を統括情報セキュリティ責任者に報告するとともに、その重要度に応じてCISOに報告しなければならない。

3.8.2 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、必要に応じて、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、自治体機密性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 約款による外部サービスを利用可能な範囲
- 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届を提出し、適正な措置を講じた上で利用しなければならない。

3.9 評価・見直し

3.9.1 監査

(1) 実施方法

CISOは、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、必要に応じて情報セキュリティ監査統括責任者を指名し、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(再委託事業者を含む。)に対して、情報セキュリティポリシーの遵守について監査を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、CISOに報告する。

(6) 保管

情報セキュリティ監査統括責任者は、監査の実施を通して収集した監査証拠、監査報告書の作成のための監査調書を、紛失等が発生しないように適正に保管しなければならない。

(7) 監査結果への対応

CISO は、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者に対し、当該事項への対処を指示しなければならない。また、指摘事項を所管していない情報セキュリティ管理者に対しても、同種の課題及び問題点がある可能性が高い場合には、当該課題及び問題点の有無を確認させなければならない。なお、庁内で横断的に改善が必要な事項については、統括情報セキュリティ責任者に対し、当該事項への対処を指示しなければならない。

(8) 情報セキュリティポリシーの見直し等への活用

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。

3.9.2 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、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、CISO 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 この点検結果を情報セキュリティポリシー及び関連規程等の見直し、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。

3.9.3 情報セキュリティポリシー及び関係規定等の見直し

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。