

# 名古屋市情報セキュリティ対策基準

名古屋市

## 改訂履歴

年月日	改定内容等
令和 5 年 3 月 24 日	初版策定（令和 5 年 4 月 1 日施行）
令和 6 年 3 月 27 日	クラウドサービス利用に係る規定の見直し等（令和 6 年 4 月 1 日施行）
令和 7 年 7 月 1 日	名古屋市情報セキュリティ基本方針策定に伴う規定の整理（令和 7 年 7 月 1 日施行）

# 目次

1	目的.....	1
2	定義.....	1
	(1) ネットワーク.....	1
	(2) 情報システム.....	1
	(3) 情報セキュリティ.....	1
	(4) 情報セキュリティポリシー.....	1
	(5) 機密性.....	2
	(6) 完全性.....	2
	(7) 可用性.....	2
	(8) マイナンバー利用事務系（個人番号利用事務系） .....	2
	(9) LGWAN 接続系 .....	2
	(10) インターネット接続系.....	2
	(11) 無害化通信.....	2
	(12) 外部サービス.....	2
	(13) ガバメントクラウド.....	3
3	対象とする脅威.....	4
4	適用範囲.....	5
	(1) 行政機関の範囲.....	5
	(2) 情報資産の範囲.....	5
5	組織体制.....	6
	(1) 電子情報保護統括管理者.....	6
	(2) 電子情報保護副統括管理者.....	6
	(3) 局区等電子情報保護管理者.....	6
	(4) ネットワーク管理者.....	6
	(5) 情報システム管理者.....	6
	(6) 所管課長.....	7
	(7) 端末等管理者.....	7
	(8) 外部サービス利用管理者.....	7

(9) 電子情報保護部会.....	7
(10) 兼務の禁止.....	8
(11) CSIRT の設置・役割 .....	8
(12) クラウドサービス利用における組織体制 .....	8
<b>6 情報システム全体の強靱性の向上 .....</b>	<b>9</b>
(1) マイナンバー利用事務系.....	9
ア マイナンバー利用事務系と他の領域との分離 .....	9
イ マイナンバー利用事務系における特定通信 .....	9
ウ 情報のアクセス及び持ち込み・持ち出しにおける対策 .....	9
エ マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの取扱.....	9
オ マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱.....	10
(2) LGWAN 接続系 .....	10
ア LGWAN 接続系とインターネット接続系の分割.....	10
イ LGWAN 接続系と接続されるクラウドサービス上での情報システムの取扱.....	10
(3) インターネット接続系.....	11
<b>7 物理的情報保護対策 .....</b>	<b>12</b>
(1) サーバー等の管理.....	12
ア 機器の取付け.....	12
イ 情報システムの冗長化.....	12
ウ 機器の電源.....	12
エ 通信ケーブル等の配線.....	12
オ 機器の定期点検及び修理.....	13
カ 機器の外部施設等への設置.....	13
キ 機器の廃棄等.....	13
(2) 管理区域（情報管理室等）の管理 .....	13
ア 管理区域の構造等.....	13
イ 管理区域の入退室管理等.....	14

ウ	機器等の搬入.....	14
エ	管理区域の運用管理.....	14
(3)	通信回線及び通信機器の管理 .....	14
(4)	職員の利用する端末や記録媒体等の管理 .....	15
<b>8</b>	<b>人的情報保護対策 .....</b>	<b>17</b>
(1)	職員の遵守事項.....	17
ア	情報セキュリティポリシーの遵守 .....	17
イ	業務以外の目的での利用の禁止 .....	17
ウ	端末等の持ち出し及び外部における利用の制限 .....	17
エ	支給以外のパソコン及びモバイル端末の業務利用 .....	17
オ	持ち出しの記録.....	18
カ	端末等における設定変更の禁止 .....	18
キ	机上の端末等の管理.....	18
ク	異動時・退職時等の遵守事項 .....	18
ケ	外部サービス利用時等の遵守事項 .....	18
(2)	研修・訓練.....	18
ア	情報セキュリティに関する研修 .....	18
イ	緊急事態対応訓練.....	18
(3)	緊急事態への対応.....	19
(4)	ID 及びパスワード等の管理 .....	19
ア	ID の取扱 .....	19
イ	パスワードの取扱.....	19
ウ	IC カード等の取扱 .....	20
<b>9</b>	<b>技術的情報保護対策 .....</b>	<b>21</b>
(1)	情報システム及びネットワークの管理 .....	21
ア	バックアップの実施.....	21
イ	情報システムの管理記録及び作業の確認 .....	21
ウ	情報システム仕様書等の管理 .....	21
エ	ログの取得等.....	21
オ	障害記録.....	22

カ	ネットワークの接続制御、経路制御等 .....	22
キ	外部ネットワークとの接続制限等 .....	22
ク	IoT 機器を含む特定用途機器の情報セキュリティ管理 .....	23
ケ	無線 LAN の情報セキュリティ管理 .....	23
コ	電子メールの情報セキュリティ管理 .....	23
サ	電子メール等の利用制限 .....	24
シ	データの暗号化等 .....	24
ス	ソフトウェアの資産管理 .....	25
セ	機器構成の変更の制限 .....	25
ソ	業務外ネットワークへの接続の禁止 .....	25
タ	業務以外の目的でのウェブサイト閲覧の禁止 .....	25
(2)	アクセス制御等 .....	26
ア	アクセス制御等 .....	26
イ	外部からのアクセス等の制限 .....	27
ウ	認証情報の管理 .....	28
(3)	情報システムの開発、導入、保守等 .....	28
ア	情報システムの調達 .....	28
イ	情報システムの開発 .....	28
ウ	情報システムの導入 .....	29
エ	情報システムの開発・保守に関連する資料等の整備・保管 .....	30
オ	情報システムにおける入出力データの正確性の確保 .....	30
カ	情報システムの変更管理 .....	30
キ	情報システムの更新又は統合時の検証等 .....	30
ク	情報システムに係る不具合、障害への対応 .....	31
(4)	不正プログラム対策 .....	31
ア	端末等管理者等の措置事項 .....	31
イ	職員の遵守事項 .....	31
(5)	不正アクセス対策 .....	32
ア	情報システム管理者の措置事項 .....	32
イ	攻撃への対処 .....	33

ウ	記録の保存.....	33
エ	内部からの攻撃.....	33
オ	職員による不正アクセス.....	33
カ	サービス不能攻撃（DoS 攻撃・DDoS 攻撃） .....	33
キ	標的型攻撃.....	33
(6)	情報セキュリティに関する情報の収集等 .....	34
ア	脆弱性情報の収集及びソフトウェアの更新等 .....	34
イ	不正プログラム等の情報の収集等 .....	34
ウ	情報セキュリティ技術等に関する情報の収集等 .....	34
<b>10</b>	<b>運用.....</b>	<b>35</b>
(1)	情報システムの監視.....	35
(2)	情報セキュリティポリシーの遵守状況の確認等 .....	35
ア	遵守状況の確認及び対処.....	35
イ	情報システム等の情報セキュリティ対策に関する点検 .....	36
ウ	パソコン、モバイル端末及び記録媒体等の利用状況調査 .....	36
エ	職員の報告義務等.....	36
(3)	侵害時の対応等.....	36
ア	緊急事態対応計画の策定.....	36
イ	業務継続計画との整合性確保 .....	37
ウ	緊急事態対応計画の見直し.....	37
(4)	例外措置.....	37
(5)	法令等の遵守.....	37
(6)	懲戒処分等.....	38
ア	懲戒処分等.....	38
イ	違反時の対応.....	38
<b>11</b>	<b>外部サービスの利用 .....</b>	<b>39</b>
<b>12</b>	<b>情報セキュリティ監査（評価・見直し） .....</b>	<b>40</b>
(1)	情報システム監査.....	40
ア	情報システム監査の実施.....	40
イ	監査を行う者の要件.....	40

ウ	監査計画の立案及び実施への協力 .....	40
エ	報告.....	40
オ	保管.....	40
カ	統括管理者による措置.....	40
キ	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 ...	40
(2)	セルフチェック.....	41
ア	実施方法.....	41
イ	報告.....	41
ウ	セルフチェックの結果の活用 .....	41
(3)	情報セキュリティポリシー及び関係規程等の見直し .....	41



# 名古屋市情報セキュリティ対策基準

## 1 目的

名古屋市情報セキュリティ対策基準（以下「市対策基準」という。）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、名古屋市情報セキュリティ基本方針に基づき、電子情報の保護対策の基準を定めたものである。

## 2 定義

市対策基準において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

### (1) ネットワーク

電子計算機等を相互に接続し、情報を伝送するための通信回線網その他の仕組みをいう。

### (2) 情報システム

電子計算機により継続的に情報を処理する仕組み（ネットワーク上のものを含む。）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

名古屋市情報あんしん条例、名古屋市情報あんしん条例施行細則、名古屋市情報あんしん条例施行規程、各実施機関で制定している関係規程※、名古屋市情報セキュリティ基本方針及び市対策基準等をいう。

※市会事務局情報あんしん条例施行規程、名古屋市教育委員会情報あんしん条例施行規程、名古屋市選挙管理委員会情報あんしん規程、名古屋市人事委員会情報あんしん条例施行規程、名古屋市監査事務局情報の保護及び管理に関する規程、名古屋市固定資産評価審査委員会情報あんしん条例施行規程、名古屋市上下水道局情報あんしん条例施行規程、名古屋市情報あんしん条例施行規程（平成16年名古屋市交通局管理規程第16号）、消防局情報の保護及び管理に関する規程、公立大学

法人名古屋市長立大学情報あんしん条例施行規程

(5) 機密性

情報が、不必要な若しくは権限なき閲覧、第三者への不当な開示又は盗聴等により漏えいされないことをいう。

(6) 完全性

情報が、意図しない変更、改ざん、又は損壊されないことにより、正確性を保つことをいう。

(7) 可用性

情報の利用を認められた者が、必要な時にその情報を適切に利用できる状態であることをいう。

(8) マイナンバー利用事務系（個人番号利用事務系）

行政手続き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）第2条第10項に規定する個人番号利用事務又は戸籍事務等に関わる情報システム、ネットワーク及びその情報システム等で取り扱うデータをいう。

(9) LGWAN接続系

LGWANに接続された情報システム、ネットワーク及びその情報システム等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

インターネットに接続された情報システム、ネットワーク及びその情報システム等で取り扱うデータをいう。

(11) 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、マルウェア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。

(12) 外部サービス

実施機関以外の者が、官民データ活用推進基本法（平成28年法律第103号）第2条第4項に規定するクラウド・コンピューティング・サービス関連技術を用いて提供するサービスその他の情報システムの一部又は全部の機能を提供するものをいう。

(13) ガバメントクラウド

外部サービスのうち、国が地方公共団体情報システムの標準化に関する法律（令和 3 年法律第 40 号）第 10 条に基づき自治体に提供するクラウドサービスをいう。

### 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、マルウェア攻撃、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、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

## 4 適用範囲

### (1) 行政機関の範囲

市対策基準が適用される実施機関は、市長、議長、教育委員会、選挙管理委員会、人事委員会、監査委員、農業委員会、固定資産評価審査委員会、公営企業管理者、消防長とする。

### (2) 情報資産の範囲

市対策基準が対象とする情報資産は、次のとおりとする。

ア ネットワーク及び情報システム並びにこれらに関する設備及び記録媒体

イ ネットワーク及び情報システムで取り扱う情報

ウ 情報システムの仕様書及びネットワーク図等の情報システム関連文書

※ただし、名古屋市教育情報セキュリティ対策基準 4(2)に規定する情報資産は除く。

## 5 組織体制

### (1) 電子情報保護統括管理者(以下「統括管理者」という。)

ア 総務局長を統括管理者とする。また、統括管理者を最高情報セキュリティ責任者(Chief Information Security Officer)とする。

イ 統括管理者は、本市における電子情報の保護対策について実施状況を継続的に監視し、必要に応じ、局区等の長に対して電子情報の保護対策上必要な措置を要請することができる。

ウ イの規定にかかわらず、統括管理者は、緊急事態対応計画に定める事態が発生したときは、当該計画に基づき、副統括管理者、局区等管理者、ネットワーク管理者、情報システム管理者及び所管課長に対し、必要な措置を指示するものとする。

### (2) 電子情報保護副統括管理者(以下「副統括管理者」という。)

ア 総務局行政DX推進部長を副統括管理者とする。

イ 副統括管理者は、本市における電子情報の保護対策について、統括管理者を補佐するとともに、局区等管理者、ネットワーク管理者、情報システム管理者及び所管課長相互の連絡調整を行うものとする。

### (3) 局区等電子情報保護管理者(以下「局区等管理者」という。)

ア 電子情報保護部会の部会員を局区等管理者とする。

イ 局区等管理者は、当該局区等における電子情報の保護対策について、局区等の長を補佐するとともに、その実施状況を継続的に監視し、当該局区等に所属するネットワーク管理者、情報システム管理者及び所管課長に対し、必要な措置を指示するものとする。

### (4) ネットワーク管理者

ア ネットワークを所管する課等(課、室及び公所等(課を置かないものに限る。))をいう。以下同じ。)の長をネットワーク管理者とする。

イ ネットワーク管理者は、所管するネットワークに係る運用管理に関する規程を定め、適切な電子情報の保護対策を実施するとともに、当該ネットワークを利用するネットワーク管理者、情報システム管理者及び所管課長に対し、必要な措置を指示するものとする。

### (5) 情報システム管理者

ア 情報システムを所管する課等の長を情報システム管理者とする。

イ 情報システム管理者は、所管する情報システムに係る運用管理に関する規程を定め、適切な電子情報の保護対策を実施するとともに、当該情報システムを利用する情報システム管理者及び所管課長に対し、必要な措置を指示するものとする。

(6) 所管課長

ア 情報を所管する課等の長とする。

イ 所管課長は、法令及びこれらに基づき定められる諸規程に従い、職員を適切に指揮監督するとともに、当該課等に設置されている全ての電子計算機、通信機器、通信回線、記録媒体等を適切に管理しなければならない。

(7) 端末等管理者

ア パソコン、モバイル端末及び記録媒体（以下「端末等」という。）の機器の管理を所管する課等の長を端末等管理者とする。

イ 端末等管理者は、所管する端末等に係るハードウェア、ソフトウェア、ライセンスについて、調達から廃棄に至るライフサイクルにわたって、必要な管理を行うものとする。

(8) 外部サービス利用管理者

ア 外部サービスを所管する課等の長をいう。

イ 外部サービス利用管理者は、外部サービスの利用に当たっては、取り扱う情報資産の分類やこれに応じた取扱制限等を踏まえ適切な外部サービスを選定するとともに、所属における外部サービスの運用手順を定めるなど、適切に運用するものとする。

(9) 電子情報保護部会

ア ネットワークに接続された電子計算機等及びネットワークを利用する情報システムにおいて取り扱う電子情報に関して、総合的に保護対策を講ずるため、電子情報保護部会を設置する。

イ 本市の情報セキュリティ対策を統一的に実施するため、電子情報保護部会において、市対策基準等、電子情報に関する情報セキュリティについての重要な事項を決定する。

(10) 兼務の禁止

ア 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、許可等の申請を行う者と許可等する者は、同じ者が兼務してはならない。

イ 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。

(11) CSIRTの設置・役割

ア 統括管理者は、CSIRT (Computer Security Incident Response Team) を整備し、その役割を明確化しなければならない。

イ 統括管理者は、CSIRTに所属する職員を選任し、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。

ウ 統括管理者は、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ネットワーク管理者、情報システム管理者又は所管課長等より報告を受けた場合には、その状況を確認し、事案の程度に応じて、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。

エ 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、受託者等との情報共有を行わなければならない。

(12) クラウドサービス利用における組織体制

外部サービス利用管理者は、クラウドサービスを利用する際には、複数の事業者の存在・責任の所在を確認し、複数の事業者が存在する場合は、必要な連絡体制を構築しなければならない。また、副統括管理者は、クラウドサービス利用における情報セキュリティ対策に取り組む十分な組織体制を確立しなければならない。



## 6 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

#### ア 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は、他の領域と分離し、通信をできないようにしなければならない。

#### イ マイナンバー利用事務系における特定通信

マイナンバー利用事務系において、外部接続先（マイナンバー利用事務系以外の領域）と通信をする必要がある場合は、通信経路の限定（MACアドレス又は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った通信（以下「特定通信」という。）としなければならない。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情報システム等、十分な安全性が確認されていると統括管理者が判断した外部接続先についてはその限りではなく、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。その場合、別に定める方法による通信の限定を行わなければならない。

#### ウ 情報のアクセス及び持ち込み・持ち出しにおける対策

##### (ア) 情報のアクセス対策

①マイナンバー利用事務系での利用者の認証に当たっては、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。

②情報システムにおいて接続できる端末等を制御することが望ましい。

##### (イ) 情報の持ち込み・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に対する情報の持ち込み・持ち出しができないように設定しなければならない。

#### エ マイナンバー利用事務系と接続されるクラウドサービス上での情報システムの取扱

マイナンバー利用事務系の端末・サーバー等と専用回線サービスにより接続されるクラウドサービス（ガバメントクラウドを含む。）上の

情報システムの領域については、マイナンバー利用事務系として扱い、本市の他の領域とはネットワークを分離しなければならない。

オ マイナンバー利用事務系と接続されるクラウドサービス上での情報資産の取扱

マイナンバー利用事務系の情報システムをクラウドサービス（ガバメントクラウドを含む。）上において利用する場合は、その情報資産の機密性を考慮し、暗号化による対策を実施する。その場合、暗号は十分な強度を持たなければならない。また、クラウドサービス事業者が暗号化に関する対策を行う場合又はクラウドサービス事業者が提供する情報資産を保護するための暗号化機能を利用する場合、クラウドサービス事業者が提供するそれらの機能や内容について情報を入手し、その機能について理解に努め、必要な措置を行わなければならない。

(2) LGWAN接続系

ア LGWAN接続系とインターネット接続系の分割

LGWAN接続系は、インターネット接続系と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、電子メールやファイル等を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電子メールの本文のみをLGWAN接続系に転送するメールテキスト化方式
- (イ) インターネット接続系の端末から、LGWAN接続系の端末へ画面を転送する方式
- (ウ) 危険因子をファイル等から除去し、又は危険因子がファイル等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

イ LGWAN接続系と接続されるクラウドサービス上での情報システムの取扱

LGWAN接続系の情報システムをクラウドサービス上へ配置する場合は、その領域をLGWAN接続系として扱い、マイナンバー利用事務系とネットワークを分離し、専用回線サービスを用いて接続しなければならない。

### (3) インターネット接続系

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接続系への不適切なアクセス等の監視等の情報セキュリティ対策を講じなければならない。

## 7 物理的情報保護対策

### (1) サーバー等の管理

#### ア 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する。

また、サーバー等の盗難対策として、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。

#### イ 情報システムの冗長化

情報システム管理者は、必要に応じて、情報システムに代替又は縮退運転を行う機能を設けなければならない。

#### ウ 機器の電源

(ア) 情報システム管理者は、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る等の措置を講じなければならない。

(イ) 情報システム管理者は、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。

#### エ 通信ケーブル等の配線

(ア) ネットワーク管理者又は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。

(イ) ネットワーク管理者又は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。

(ウ) 情報システム管理者又は所管課長は、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。

(エ) 情報システム管理者又は所管課長は、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受託者以外の者が配線を変更、追加で

きないように監視や点検を行わなければならない。

#### オ 機器の定期点検及び修理

(ア) 情報システム管理者は、必要に応じてサーバー等の機器の定期点検を実施しなければならない。

(イ) 情報システム管理者又は所管課長は、機密情報を含む記録媒体又はそれを内蔵する機器を受託者に修理させる場合、内容を復元不可能な方法により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又は所管課長は、受託者に故障を修理させるにあたり、受託者との間で秘密保持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。

#### カ 機器の外部施設等への設置

情報システム管理者は、外部の施設等にサーバー等の機器を設置する場合、受託者等に適切な物理的情報保護対策を講じさせるとともに、その内容を契約書等に明記しなければならない。また、定期的に当該機器への対策の実施状況について確認しなければならない。

#### キ 機器の廃棄等

ネットワーク管理者、情報システム管理者又は所管課長は、機器を廃棄、リース会社へ返却等する場合、機器内部の記録媒体から、全ての情報を消去の上、復元不可能な状態にするなどの必要な措置を講じなければならない。

### (2) 管理区域（情報管理室等）の管理

#### ア 管理区域の構造等

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

(イ) 管理区域は、原則として地階又は1階を避けるよう努めなければならない。

(ウ) ネットワーク管理者又は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。

らない。

(エ) ネットワーク管理者又は情報システム管理者は、情報管理室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置、防じん措置等を講じなければならない。

(オ) ネットワーク管理者又は情報システム管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器及び記録媒体等に影響を与えないようにしなければならない。

#### イ 管理区域の入退室管理等

(ア) ネットワーク管理者又は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。

(イ) 管理区域に入室する者は、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。

(ウ) ネットワーク管理者又は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、管理区域への入退室を許可された職員の立会い等の措置を講じなければならない。

(エ) ネットワーク管理者又は情報システム管理者は、機密情報を取り扱う情報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パソコン、モバイル端末、通信機器、記録媒体等を原則として持ち込ませないようにしなければならない。

#### ウ 機器等の搬入

ネットワーク管理者又は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受託者に確認を行わせなければならない。

#### エ 管理区域の運用管理

管理区域を管理する所管課長は、当該管理区域の運用管理に関する規程を定めなければならない。

#### (3) 通信回線及び通信機器の管理

- ア ネットワーク管理者又は情報システム管理者は、庁内の通信回線及び通信機器を、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、通信回線及び通信機器に関連する文書を所定の棚や保管庫等において適正に保管しなければならない。
- イ ネットワーク管理者又は情報システム管理者は、外部へのネットワーク接続を必要最小限に限定し、できる限り接続ポイント及び通信を減らさなければならない。
- ウ ネットワーク管理者又は情報システム管理者は、原則として、所管するネットワークを名古屋市行政情報ネットワーク（名古屋市行政情報ネットワーク運用管理事務取扱第 2(2)に規定する「名古屋市行政情報ネットワーク」をいう。）に集約することが望ましい。
- エ ネットワーク管理者又は情報システム管理者は、機密情報を取り扱う情報システムに通信回線を接続する場合、必要な情報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適切に行わなければならない。
- オ ネットワーク管理者又は情報システム管理者は、ネットワークに使用する回線について、伝送途上に情報の破壊、盗聴、改ざん、消去等が生じないように十分な情報セキュリティ対策を実施しなければならない。
- カ ネットワーク管理者又は情報システム管理者は、必要に応じて、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。また、機密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は、継続的な運用を可能とする回線を選択するように努めなければならない。
- (4) 職員の利用する端末や記録媒体等の管理
- ア 端末等管理者は、盗難防止のため、執務室等で利用する端末等について適切な措置を講じなければならない。
- イ 記録媒体については、別に定めがあるものはそれに基づき適切に管理を行うとともに、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。
- ウ 情報システム管理者又は端末等管理者は、情報システムへのログイン

に際し、「知識（パスワード等）」、「所持（ICカード等）」、又は「存在（生体認証等）」等の認証情報の入力が必要とするように設定しなければならない。なお、機密情報を取り扱わない端末等への利用者権限のログイン等（管理者権限は除く。）については、この限りでない。

エ 情報システム管理者又は端末等管理者は、マイナンバー利用事務系及びテレワークで利用する端末では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証）を行うよう設定しなければならない。

オ 情報システム管理者又は端末等管理者は、端末において機密情報を保存する場合、ハードディスク等の暗号化機能を有効に利用しなければならない。同様に、機密情報を保存する外部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。

カ 情報システム管理者又は端末等管理者は、モバイル端末においては十分な情報セキュリティを確保できる場合を除き、原則として端末内に機密情報を保存させてはならない。機密情報を保存する場合においても、執務場所以外での業務利用を行う際は、遠隔消去機能を利用する等の適切な措置を講じなければならない。

キ 情報システム管理者又は端末等管理者は、モバイル端末のうちスマートフォン・タブレットについては、定期的にセキュリティ設定等の状態を確認しなければならない。



## 8 人的情報保護対策

### (1) 職員の遵守事項

#### ア 情報セキュリティポリシーの遵守

職員は、情報セキュリティポリシーを遵守し、電子情報が漏えい、滅失又は毀損されることがないように常に注意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、速やかに所管課長に相談し、指示を仰がなければならない。

#### イ 業務以外の目的での利用の禁止

職員は、業務以外の目的で、情報資産の外部への持ち出し、情報システムやサーバー等へのアクセス、支給されたパソコンなどの端末や電子メールアドレス等の利用及び本市のネットワーク又はパソコンなどによるインターネットの利用を行ってはならない。

#### ウ 端末等の持ち出し及び外部における利用の制限

職員は、本市の端末等を外部に持ち出す場合には、所管課長の許可を得なければならない。また、盗難、盗聴又はのぞき見等を防止するために、必要な措置を講じなければならない。

#### エ 支給以外のパソコン及びモバイル端末の業務利用

(ア) 職員は、支給以外の端末等を市のネットワークに接続し、又は業務に利用してはならない。

ただし、支給以外のパソコン及びモバイル端末の業務での利用については、次に掲げる場合に限り、別に定める措置を講じ、所管課長の許可を得て利用することができる。

①職員がスケジュール管理、連絡、メモ等の用途に利用する場合

②職員が専ら外部の情報を閲覧するために利用する場合

③①、②に定めるもののほか、やむを得ない事情があると認める場合

(イ) 職員は、(ア)のただし書の場合においても、支給以外のパソコン及びモバイル端末で市の保有する機密情報を取り扱ってはならない。ただし、職員が前号①又は③の規定により許可を受けて利用する場合において、必要不可欠な機密情報に限り、別に定める措置を講じ、所管課

長の許可を得て取り扱うことができる。

オ 持ち出しの記録

所管課長は、本市の端末等の持ち出しについて、記録を作成し、保管しなければならない。

カ 端末等における設定変更の禁止

職員は、端末等のソフトウェアに関する情報セキュリティ機能の設定を端末等管理者の許可なく変更してはならない。

キ 机上の端末等の管理

職員は、端末等の盗難、盗聴又はのぞき見等を防止するために、離席時のパソコン及びモバイル端末のロックや記録媒体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。

ク 異動時・退職時等の遵守事項

職員は、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するとともに、当該情報資産を職務目的以外で閲覧、利用又は削除してはならない。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。

ケ 外部サービス利用時等の遵守事項

職員等は、クラウドサービスを始めとした外部サービスの利用にあっても、名古屋市外部サービス利用基準などの情報セキュリティポリシーを遵守し、外部サービスの利用に関する自らの役割及び責任を意識しなければならない。

(2) 研修・訓練

ア 情報セキュリティに関する研修

統括管理者は、次の各号に掲げる研修を実施しなければならない。

(ア) 職員を対象とした研修

(イ) 管理職員を対象とした研修

(ウ) ネットワーク又は情報システムの運用に携わる職員を対象とした研修

(エ) (ア)～(ウ)に定めるもののほか、電子情報の保護及び管理に関し、実施機関において周知徹底を図るために必要な研修

イ 緊急事態対応訓練

ネットワーク管理者又は情報システム管理者は、緊急事態の対応を想定した訓練を定期的の実施するように努めなければならない。

(3) 緊急事態への対応

ネットワーク管理者、情報システム管理者又は所管課長は、情報セキュリティインシデントなどの緊急事態が発生した場合、緊急事態対応計画に基づき、適切に対応を行わなければならない。

(4) ID及びパスワード等の管理

ア IDの取扱

職員は、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。

(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。

イ パスワードの取扱

(ア) 職員は、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、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。）。

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複雑性を持たせなければならない。

④パスワードが流出した恐れがある場合には、情報システム管理者又は所管課長に速やかに報告し、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は、同一のパスワードを情報システム間で用いてはならない（シングルサインオン機能を利用する場合は除く。）。

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

⑦パスワードを紛失、漏えい、滅失又は毀損した場合には、速やかに

情報システム管理者又は所管課長に通報し、指示に従わなければならない。

- (イ) 情報システム管理者又は所管課長は、所管するパスワードの紛失等が生じた場合の必要な手続きを定めるとともに、職員から通報を受けた際は、当該パスワード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。

ウ ICカード等の取扱い

- (ア) 職員は、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。

①認証に用いるICカード等を、職員間で共有してはならない（ただし、共有で利用するICカードの場合は除く。）。

②業務上必要のないときは、ICカード等をカードリーダー又はパソコン等の端末のスロット等から外し、適切に保管しなければならない。

③ICカード等を紛失した場合には、速やかに情報システム管理者又は所管課長に通報し、指示に従わなければならない。

- (イ) 情報システム管理者又は所管課長は、ICカード等の紛失等が生じた場合の必要な手続きを定めるとともに、職員から通報を受けた際は、当該ICカード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。

- (ウ) 情報システム管理者又は所管課長は、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。

## 9 技術的情報保護対策

### (1) 情報システム及びネットワークの管理

#### ア バックアップの実施

情報システム管理者は、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。

#### イ 情報システムの管理記録及び作業の確認

(ア) 情報システム管理者は、所管する情報システムの保守及び運用において、作業体制を定めるとともに、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。

(イ) 情報システム管理者は、所管する情報システムにおいて、情報システムの変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適正に管理しなければならない。

(ウ) 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受託者が情報システムの変更等の作業を行う場合は、必要に応じて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。

#### ウ 情報システム仕様書等の管理

情報システム管理者は、情報システム構成図（ネットワーク構成図を含む。）、情報システム仕様書等について、記録媒体に関わらず、業務上必要とする者以外による閲覧、紛失等がないよう、所定の棚や保管庫等において適正に管理しなければならない。

#### エ ログの取得等

(ア) 情報システム管理者は、情報システムで取り扱う機密情報等重要な情報の利用に関するアクセスログを取得し、一定の期間保存しなければならない。また、端末操作ログなどのその他ログ等については、情報セキュリティの確保に必要な場合は、適宜取得し、一定の期間保存しなければならない。

(イ) 情報システム管理者は、ログを取得する目的や取得する機器、取得する項目、保存期間、取扱方法等を定めるとともに、取得したログは、改ざんや消失等が起こらないよう、適正に保存しなければならない。

また、必要に応じて、情報システムから出力したログを記録媒体にバックアップしなければならない。

- (ウ) 情報システム管理者は、悪意ある第三者等からの不正侵入、不正操作等の有無を確認するため、必要に応じて取得したログの点検又は分析を実施しなければならない。

#### オ 障害記録

情報システム管理者は、職員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。

#### カ ネットワークの接続制御、経路制御等

- (ア) ネットワーク管理者は、通信に影響を与える不整合が生じないように、通信機器等を適切に設定しなければならない。
- (イ) ネットワーク管理者は、不正アクセスを防止するため、ネットワークに適正なアクセス制御を施さなければならない。

#### キ 外部ネットワークとの接続制限等

- (ア) ネットワーク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を外部ネットワークに接続する場合は、当該外部ネットワークに係るネットワーク構成、機器構成、情報セキュリティ技術等を詳細に調査し、庁内の情報資産に影響が生じないように対応しなければならない。
- (イ) ネットワーク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を外部ネットワークに接続する場合は、不正アクセスを防御するために、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、通過する通信のプロトコルを必要最小限に限定するなどの通信制御を行わなければならない。
- (ウ) ネットワーク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を外部ネットワークに接続する場合は、当該外部ネットワークからネットワーク等への不正侵入を防止するため、脆弱性などの情報セキュリティに関する情報収集に努めるとともに、必要な技術的な措置を講じること。

- (エ) ネットワーク管理者又は情報システム管理者は、接続する外部ネットワークを利用した情報の閲覧又は情報の伝達の際の利用上の取扱方法を定め、利用者に周知しなければならない。
- (オ) ネットワーク管理者又は情報システム管理者は、職員が外部ネットワーク等を利用した外部情報の閲覧を適切に行っているかを調査することができる。
- (カ) 所管課長は、職員が外部ネットワーク等を利用した外部情報の閲覧を適切に行うよう指揮監督しなければならない。

#### ク IoT機器を含む特定用途機器の情報セキュリティ管理

情報システム管理者は、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。

#### ケ 無線LANの情報セキュリティ管理

- (ア) ネットワーク管理者は、無線LANの利用を認める場合、解読が困難な暗号化、適切な機器設定及び認証方式の採用を行わなければならない。また、構成する機器等の脆弱性情報を継続的に把握する体制を整え、用途上悪影響が予想される脆弱性が発見された場合は、ファームウェアの更新等の対応を適切に実施しなければならない。
- (イ) ネットワーク管理者は、機密情報を無線LANにて取り扱う場合、情報セキュリティを確保するために別途定める要件を満たすことを確認し、副統括管理者による点検を受けなければならない。
- (ウ) マイナンバー利用事務系においては無線LANを使用してはならない。

#### コ 電子メールの情報セキュリティ管理

- (ア) 電子メールシステムを所管する情報システム管理者は、なりすましや電子メールの盗聴及び改ざんを防止等するとともに、発せられた電子メールが外部ネットワーク等に悪影響を及ぼさないように必要な措置を講じなければならない。
- (イ) 電子メールシステムを所管する情報システム管理者は、職員が電子メールシステムを適切に利用しているか調査することができる。
- (ウ) 電子メールシステムを所管する情報システム管理者は、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。

(エ) 電子メールシステムを所管する情報システム管理者は、職員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に周知しなければならない。

(オ) 電子メールシステムを所管する情報システム管理者は、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受託者の作業員による電子メールアドレス利用について、受託者との間で利用方法を取り決めなければならない。

#### サ 電子メール等の利用制限

(ア) 職員は、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。ただし、業務上の必要があり、やむを得ず内部に転送する場合は、所管課長の許可を得た上で実施すること。

(イ) 職員は、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。

(ウ) 職員は、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、BCC等を利用して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。

(エ) 職員は、重要な電子メールを誤送信した場合、速やかに所管課長に報告しなければならない。

(オ) 職員は、インターネット上で利用できる電子メールやファイルストレージ等において、私的な個人アカウント等を使用してはならない。

(カ) 所管課長は、職員が電子メールシステムを適切に利用するように指揮監督しなければならない。

#### シ データの暗号化等

(ア) 職員は、機密情報を外部に送信する場合は、統括管理者がインターネット接続系に用意するファイル転送サーバーを利用するよう努めなければならない。

(イ) 職員は、機密情報を外部に送信する際に、業務の都合等によりファイル転送サーバーを利用することが困難である等、電子媒体で持ち出す場



合又は電子メール等で送信する場合は、権限のない者が閲覧又は利用できないように、データの暗号化を適切に行わなければならない。

#### ス ソフトウェアの資産管理

- (ア) 情報システム管理者又は端末等管理者は、ソフトウェアのライセンスを適切に管理しなければならない。
- (イ) 情報システム管理者又は端末等管理者は、サーバー及び端末等に業務に不要なソフトウェアを許可なく導入又は削除できないよう適切に管理しなければならない。
- (ウ) 職員は、サーバー及び端末等に情報システム管理者又は端末等管理者に許可を受けることなく、無断でソフトウェアを導入又は削除してはならない。
- (エ) 職員は、不正にコピーしたソフトウェアを利用してはならない。

#### セ 機器構成の変更の制限

- (ア) 職員は、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。
- (イ) 職員は、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、端末等管理者の許可を得なければならない。

#### ソ 業務外ネットワークへの接続の禁止

- (ア) 職員は、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。
- (イ) 端末等管理者は、支給する端末について、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。

#### タ 業務以外の目的でのウェブサイト閲覧の禁止

- (ア) 職員は、業務以外の目的で本市のネットワーク又はパソコンなどによりウェブサイトを開覧してはならない。
- (イ) ネットワーク管理者は、職員のウェブサイト利用について、明らかに業務に関係のないウェブサイトを開覧していることを発見した場合

は、所管課長に通知し適正な措置を求めなければならない。

(2) アクセス制御等

ア アクセス制御等

(ア) アクセス制御

情報システム管理者、ネットワーク管理者又は所管課長は、所管するネットワーク、情報システム、ファイルサーバー及びNAS等について、利用者及び管理者の範囲、処理権限、利用者のアクセスできる情報の範囲を最小化するなど、アクセスする権限のない職員がアクセスできないように情報システム等において制限しなければならない。

(イ) IDの管理等

情報システム管理者、ネットワーク管理者又は所管課長は、IDの管理等に当たっては以下の措置を講じなければならない。また、職員は、業務上必要がなくなった場合は、ID登録を抹消するよう、管理者に通知しなければならない。

- ①人事異動や退職等により業務上必要がなくなったIDは速やかに削除・無効化するなどIDの登録、変更、抹消等の情報管理、職員の異動、出向、退職者に伴うIDの取扱い等の方法を定め、運用する。
- ②原則として、利用者IDは個人単位で設定する。
- ③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する等し、適切に点検・管理する。
- ④管理者権限等の特権を付与されたID（管理者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する。
- ⑤機密情報を取り扱う情報システムにおいては、パソコンや記録媒体等へデータを複製する業務を明確にし、複製できる利用者IDを最小化する。
- ⑥特定個人情報を取り扱う情報システムにおいては、管理者IDにおいても、必要性に応じた特定個人情報ファイルへのアクセス制限を実施する。

(ウ) 共有ファイルサーバー及びNASの設定等

情報システム管理者及び所管課長は、共有ファイルサーバー及びNASの設定等に当たっては、(ア)(イ)に加え、以下の措置を講じなければならない。また、NASの利用に当たっては、「NASの導入・運用に関するガイドライン」も踏まえ適切に対応すること。

①原則として、課室等の単位で構成し、業務上の必要がない職員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。

②住民の個人情報、人事記録等、特定の職員しか取り扱えないデータについて、同一課室等であっても、担当職員以外の職員が閲覧及び使用できないようにするなど適切にアクセス制御を行わなければならない。

#### イ 外部からのアクセス等の制限

(ア) 職員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、情報システム管理者又は所管課長の許可を得なければならない。

(イ) 情報システム管理者又は所管課長は、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。

(ウ) 情報システム管理者又は所管課長は、外部からのアクセスを認める場合、情報システム上利用者の認証を行う機能を確保しなければならない。

(エ) 情報システム管理者又は所管課長は、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。

(オ) 情報システム管理者又は所管課長は、外部からのアクセスに利用する端末等を職員に貸与する場合、情報セキュリティの確保のために必要な措置を講じなければならない。

(カ) 職員は、外部から持ち帰った端末等を庁内のネットワークに接続する際は、マルウェアに感染していないこと等を確認しなければならない。

- (キ) マイナンバー利用事務系は、住民情報等の特に重要な情報資産が配置されており、情報漏えいリスクが高いこと等を踏まえ、テレワークなど外部からのアクセスを行ってはならない。

#### ウ 認証情報の管理

- (ア) 情報システム管理者は、職員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、情報システム等で認証情報設定の情報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。
- (イ) 情報システム管理者は、原則として、職員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。
- (ウ) 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。

### (3) 情報システムの開発、導入、保守等

#### ア 情報システムの調達

- (ア) 情報システム管理者は、当該情報システムが取り扱う情報に必要な機密性及び完全性を確保するとともに、当該情報システムに必要な可用性を保持するため、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情報セキュリティ機能等を明記しなければならない。
- (イ) 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、当該製品の情報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。

#### イ 情報システムの開発

##### (ア) 情報システムの開発における作業体制等の確立

情報システム管理者は、事故及び不正行為を防止するために、システム開発の責任者、作業員などの作業体制等を定めなければならない。

##### (イ) 情報システムの開発における責任者、作業員のIDの管理

- ① 情報システム管理者は、システム開発の責任者及び作業員が使用する開発用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

ない。

- ②情報システム管理者は、システム開発の責任者及び作業者のアクセス権限を設定しなければならない。

(ウ) 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

- ①情報システム管理者は、システム開発の責任者及び作業者が使用する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。
- ②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。

ウ 情報システムの導入

(ア) 開発環境と運用環境の分離及び移行手順の明確化

- ①情報システム管理者は、システム開発等における事故等の影響を鑑み、システム運用環境から分離された疑似環境を用意する等し、十分な動作確認をしなければならない。
- ②情報システム管理者は、システム開発・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。
- ③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之、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。
- ④情報システム管理者は、導入する情報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。

(イ) テスト

- ①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調整及び十分な試験を行わなければならない。
- ②情報システム管理者は、運用テストを行う場合、あらかじめ疑似環境等による操作確認を行わなければならない。
- ③情報システム管理者は、原則として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。

(ウ) 運用・保守に関する事項

①情報システム管理者は、情報システムの運用・保守に当たっては、以下の事項を定めること。

- 必要な作業体制等
- データ等のバックアップに関する対応
- 不具合の是正に関する対応

②情報システム管理者は、その他機密情報を取り扱う情報システムの運用に当たって、必要な保護対策を定めること。

エ 情報システムの開発・保守に関連する資料等の整備・保管

(ア) 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情報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。

(イ) 情報システム管理者は、テストに使用した情報及び資料を一定期間保管しなければならない。

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

オ 情報システムにおける入出力データの正確性の確保

(ア) 情報システム管理者は、所管する情報システムにおいて入力データの正確性が求められる場合、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等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。

(イ) 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恐れがある場合に、これを検出及び防止する手段を講じなければならない。

(ウ) 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。

カ 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。

キ 情報システムの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。

ク 情報システムに係る不具合、障害への対応

情報システム管理者は、所管する情報システムにおいて、不具合や障害が発生した場合は、被害を最小限にするために、適切に対応しなければならない。また、再発防止策を講じるとともに、不具合や障害に関する記録を作成し、保存しなければならない。

(4) 不正プログラム対策

ア 端末等管理者等の措置事項

ネットワーク管理者、情報システム管理者又は端末等管理者は、次の事項を措置しなければならない。

- (ア) マルウェアの検知を遅滞なく知り、対応できる体制を整備するとともに、マルウェア等の不正プログラム情報を収集し、必要に応じて職員に対して注意喚起しなければならない。
- (イ) 所管するサーバー及びパソコン等の端末は、外部記録媒体の自動実行機能を無効にするとともに、マルウェア等の不正プログラム対策ソフトウェアを常駐させパターンファイルを適切な状態に保つなど必要な措置を講じなければならない。
- (ウ) 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。
- (エ) 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、許可した職員を除く職員に当該権限を付与してはならない。
- (オ) マイナンバー利用事務系においては、インターネット上のウェブサイトの閲覧及びインターネットを介した電子メールの利用を禁止しなければならない。

イ 職員の遵守事項

職員は、次の事項を遵守しなければならない。

- (ア) 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。
  - (イ) 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。
  - (ウ) 副統括管理者等が提供するコンピューターウイルス等のマルウェア情報を、常に確認しなければならない。
  - (エ) マルウェア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、直ちに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するとともに、CSIRTへ報告しなければならない。
- (5) 不正アクセス対策

ア 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。

- (ア) 通信プロトコルを必要最小限に限定するため、使用されていないポートを閉鎖しなければならない。
- (イ) 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。
- (ウ) 不正アクセスによる情報システムの改ざんを防止するために、必要に応じてデータの書換えを検出し、通報するよう、設定しなければならない。
- (エ) 重要なシステムの設定を行ったファイル等について、必要に応じ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。
- (オ) ウェブサイト、ウェブアプリケーションを開発する際は、以下の措置を講じるすること。
  - ①情報システム管理者は、開発するウェブサイト等にて表示している情報の改ざんの防止に関して、必要な措置を講じること。
  - ②情報システム管理者は、開発するウェブサイト等にて機密情報を収集又は蓄積する場合は、情報の漏えい等の防止に関して、必要な措置を



講じること。

- (カ) 名古屋市行政情報ネットワーク上に構築し、かつ機密情報を取り扱う情報システムにおいては、権限を有しない職員等によるサーバーへの不正アクセスを防止するために適切な措置を講じなければならない。

#### イ 攻撃への対処

情報システム管理者は、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、情報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。

#### ウ 記録の保存

情報システム管理者は、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、関係機関との緊密な連携に努めなければならない。

#### エ 内部からの攻撃

情報システム管理者は、職員及び受託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監視するように努めなければならない。

#### オ 職員による不正アクセス

情報システム管理者又は端末等管理者は、職員による不正アクセスを発見した場合は、直ちに当該職員が所属する課室等の所管課長に通知し、適正な処置を求めるとともに、CSIRTに報告しなければならない。

#### カ サービス不能攻撃（DoS攻撃・DDoS攻撃）

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。

#### キ 標的型攻撃

統括管理者は、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等の措置を講じなければならない。

(6) 情報セキュリティに関する情報の収集等

ア 脆弱性情報の収集及びソフトウェアの更新等

副統括管理者や情報システム管理者等は、脆弱性情報を収集し、必要に応じ、関係者間での共有や職員への周知等を行わなければならない。また、当該脆弱性の緊急度及び影響度に応じて、ソフトウェア更新や影響を受けるサービスを停止する等の対策を実施しなければならない。

イ 不正プログラム等の情報の収集等

副統括管理者や情報システム管理者等は、不正プログラム等の情報を収集し、必要に応じ、関係者間での共有や職員への周知等を行わなければならない。

ウ 情報セキュリティ技術等に関する情報の収集等

副統括管理者や情報システム管理者等は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間での共有や職員への周知等を行わなければならない。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、情報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。

## 10 運用

### (1) 情報システムの監視

ア 情報システム管理者は、取り扱う電子情報等の重要性や情報システムが停止した場合の業務への影響等を勘案し、情報セキュリティに関する事案を検知するため、情報システムを適切に監視しなければならない。

イ 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。

ウ 情報システム管理者は、外部と常時接続する情報システムを適切に監視しなければならない。

### (2) 情報セキュリティポリシーの遵守状況の確認等

#### ア 遵守状況の確認及び対処

(ア) 局区等管理者又は所管課長は、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、重大な問題を認めた場合には、適正かつ速やかに対処するとともに、副統括管理者に報告しなければならない。

(イ) ネットワーク管理者、情報システム管理者又は端末等管理者は、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、重大な問題が発生していた場合には適正かつ速やかに対処するとともに、副統括管理者に報告しなければならない。

(ウ) 副統括管理者は、把握した問題について、適正かつ速やかに対処しなければならない。

(エ) 副統括管理者は、必要に応じて、本市で稼働しているネットワーク、情報システム等の情報セキュリティポリシーの遵守状況について確認等を行うことができる。確認等は当該情報資産を所管するネットワーク管理者、情報システム管理者又は所管課長と協議の上実施するとともに、確認等において重大な問題が発生していた場合には、ネットワーク管理者、情報システム管理者又は所管課長に対して必要な措置を要請する。

#### イ 情報システム等の情報セキュリティ対策に関する点検

- (7) 副統括管理者は、新たに開発・変更等されるネットワーク及び情報システムを対象として、情報セキュリティポリシーの遵守状況等に関する点検（以下「情報セキュリティ対策に関する点検」という。）を実施する。
- (4) ネットワーク管理者又は情報システム管理者は、ネットワーク及び情報システムを新たに開発・変更等する場合は、原則として、テスト稼働までに情報セキュリティ対策に関する点検を受けなければならない。
- (9) 新たに開発・変更等されるネットワーク及び情報システムのうち、当該実施機関内に限り利用される情報システムについては、稼働までに実施機関において点検を行い、その結果を副統括管理者に報告することをもって、情報セキュリティ対策に関する点検に代えることができる（ただし、実施機関内であっても複数の局区室を跨いで利用される場合は除く。）。

#### ウ パソコン、モバイル端末及び記録媒体等の利用状況調査

統括管理者又は統括管理者が指名した者は、不正アクセス、不正プログラム等の調査のために、職員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。

#### エ 職員の報告義務等

- (7) 職員は、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、直ちに所管課長を通じて、副統括管理者に報告を行わなければならない。
  - (4) 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して副統括管理者が判断した場合において、職員は、緊急事態対応計画に従って適正に対処しなければならない。
- (3) 侵害時の対応等

#### ア 緊急事態対応計画の策定

実施機関は、名古屋市電子情報保護緊急事態対応指針を踏まえ、緊急

事態対応計画を策定し、情報セキュリティ侵害時には当該計画に従って適正に対処しなければならない。

イ 業務継続計画との整合性確保

実施機関は業務継続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。

ウ 緊急事態対応計画の見直し

実施機関は、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、必要に応じて緊急事態対応計画の規定を見直さなければならない。

(4) 例外措置

ネットワーク管理者又は情報システム管理者は、ネットワーク及び情報システムを新たに開発・変更等する際に、市対策基準及び市管理基準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、電子情報保護分科会の審査を受け、統括管理者の許可を得て、例外措置を講じることができる。

(5) 法令等の遵守

職員は、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、次の法令等のほか関係する法令等を遵守し、これに従わなければならない。

ア 地方公務員法(昭和25年法律第261号)

イ 著作権法(昭和45年法律第48号)

ウ 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)

エ 個人情報保護に関する法律(平成15年法律第57号)

オ 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

カ サイバーセキュリティ基本法(平成26年法律第104号)

キ 名古屋市情報あんしん条例(平成16年名古屋市条例第41号)

ク 名古屋市個人情報保護条例(令和4年名古屋市条例第56号)

ケ 名古屋市における特定個人情報の適正な取扱いに関する方針

(6) 懲戒処分等

ア 懲戒処分等

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等の対象となる場合がある。

イ 違反時の対応

職員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。

(ア) 副統括管理者は、職員の違反を確認した場合、当該職員が所属する課等の所管課長に通知し、適正な措置を求めなければならない。

(イ) ネットワーク管理者、情報システム管理者又は端末等管理者は、職員の違反を確認した場合、速やかに副統括管理者に報告するとともに、当該職員が所属する課等の所管課長に通知し、適正な措置を求めなければならない。

(ウ) (ア)(イ)における措置（所管課長の指導等）によっても改善されない場合、副統括管理者は、当該職員のネットワーク又は情報システム等を使用する権利を停止又は剥奪するようネットワーク管理者、情報システム管理者又は端末等管理者に要請することができる。なお、職員の権利を停止又ははく奪した場合、ネットワーク管理者、情報システム管理者又は端末等管理者は速やかに、その旨を副統括管理者及び当該職員が所属する課等の所管課長に通知等しなければならない。

## 1 1 外部サービスの利用

職員は、外部サービスの利用に当たっては、名古屋市外部サービス利用基準を遵守しなければならない。また、外部サービス利用管理者は、適切にサービスの選定及び運用管理を行うとともに、原則として機密情報を取り扱う場合は副統括管理者に事前申請を行い、承認を受けなければならない。

## 1 2 情報セキュリティ監査（評価・見直し）

### (1) 情報システム監査

#### ア 情報システム監査の実施

ネットワーク管理者又は情報システム管理者は、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、必要に応じて情報システム監査を実施しなければならない。

#### イ 監査を行う者の要件

(ア) 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。

(イ) 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。

#### ウ 監査計画の立案及び実施への協力

(ア) 電子情報保護部会は、監査を行うに当たっての監査計画を立案する。

(イ) 被監査部門は、監査の実施に協力しなければならない。

#### エ 報告

電子情報保護部会は、監査結果を取りまとめ、副統括管理者に報告する。

#### オ 保管

ネットワーク管理者又は情報システム管理者は、監査の実施を通して収集した監査証拠及び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。

#### カ 統括管理者による措置

統括管理者は、監査で見つかった不適切な事項に対する改善状況等を継続的に監視するとともに、改善計画の内容が情報セキュリティ対策上、不十分な内容であったり、改善が著しく遅延したりするような場合などは、関連部署を所管する局区等の長に対し、必要な措置を要請することができる。

#### キ 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

統括管理者は、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。



ならない。

## (2) セルフチェック

### ア 実施方法

- (ア) 情報システム管理者は、所管する情報システムについて、毎年度及び必要に応じてセルフチェックを実施しなければならない。

### イ 報告

電子情報保護部会は、セルフチェックの結果とセルフチェックの結果に基づく改善策を取りまとめ、副統括管理者に報告しなければならない。

### ウ セルフチェックの結果の活用

- (ア) 職員は、セルフチェックの結果に基づき、自己の権限の範囲内で改善を図らなければならない。
- (イ) 統括管理者は、セルフチェックの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) 情報セキュリティポリシー及び関係規程等の見直し

統括管理者は、情報セキュリティ監査の結果及び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、改善等を行うものとする。