

八王子市

## 指定管理者における情報セキュリティガイドライン

平成27年(2015年)12月 策定

平成28年(2016年)10月 改定

令和元年(2019年)6月 改定

令和3年(2021年)5月 改定

## 目次

1	目的 .....	1
2	用語の定義 .....	1
3	対象とする脅威 .....	2
4	適用範囲 .....	2
5	組織体制 .....	3
6	指示体制 .....	5
7	情報資産及びネットワークの分類と管理.....	6
8	セキュリティ区域 .....	9
9	パソコン等の管理 .....	9
10	指定管理業務従事者の遵守事項 .....	10
11	ガイドライン等の閲覧 .....	10
12	情報セキュリティに関する研修・訓練.....	10
13	情報セキュリティインシデントの報告.....	11
14	指定管理業務に係る ID 及びパスワード等の取扱い.....	11
15	指定管理業務に係るシステムの取扱い.....	12
16	機器等の使用に係る遵守事項 .....	15
17	不正プログラム対策 .....	16
18	緊急時対応計画の策定 .....	17
19	委託 .....	17
20	クラウドサービスの利用 .....	17
21	約款による外部サービスの利用 .....	18
22	ソーシャルメディアサービスの利用.....	18
23	ウェブサイト .....	20
24	自己点検 .....	21
25	監査 .....	21

## 1 目的

八王子市指定管理者における情報セキュリティガイドライン(以下「ガイドライン」という。)は、八王子市情報セキュリティ基本方針(以下「基本方針」という。)で規定した事項を具体的に実現するため、指定管理者が危機意識を持って遵守すべきものであり、指定管理業務に係る情報資産の機密性、完全性及び可用性を確保するための事項を記載し、情報セキュリティを確立することを目的とする。また、行政手続における特定の個人を識別する番号の利用等に関する法律(平成25年法律第27号。以下「番号法」という。)及び「八王子市個人情報保護条例」(平成16年八王子市条例第33号。以下「個人情報保護条例」という。)に定める特定個人情報の取扱いに関しても、必要な措置を定めるものとする。

## 2 用語の定義

### (1) 情報資産

指定管理業務に係る情報及び情報を管理する仕組みの総称

### (2) 情報セキュリティ

保有する情報資産を脅威から守ること。具体的には、情報資産の機密性、完全性及び可用性を維持すること。

### (3) 情報セキュリティポリシー

情報資産を脅威から守るための対策及び情報セキュリティを確保するための組織体制と運用を規定したもの。情報セキュリティ基本方針及び情報セキュリティ対策基準の2階層で構成される。

### (4) 情報セキュリティ実施手順

対策基準に基づき、情報セキュリティを確保するため具体的な手順を定めたもの

### (5) 機密性

権限を有する者だけが権限の範囲内のみで情報資産にアクセスできること。

### (6) 完全性

情報資産の内容が正確で最新であること。

### (7) 可用性

情報資産に対して、権限を有する者が必要な時にいつでもアクセスできること。

### (8) ネットワーク

コンピュータ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。

### (9) 情報システム

コンピュータ、ネットワーク及び記憶媒体で構成され、情報処理を行う仕組みのこと。

### (10) 脅威

情報システムや組織に損害を与える可能性がある原因のこと。

(11) 脆弱性

脅威によって影響を受ける情報資産の弱点のこと。

(12) 情報セキュリティインシデント

情報セキュリティに関する事故、事件又はその兆候及びシステム上の欠陥をいう。

(13) 外部記憶媒体

コンピュータの外部で情報資産を電磁的又は光学的に記憶することのできる媒体。USBメモリ、磁気テープ、磁気ディスク、光ディスク、光磁気ディスク等がある。

(14) クラウドサービス

データやソフトウェア、ハードウェア等をネットワーク経由で、サービスとして利用者に提供されるもの

(15) 個人番号

マイナンバーのこと。番号法第7条第1項又は第2項の規定により、住民票コードを変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう(番号法第2条第6項及び第7項、第8条並びに第48条並びに附則第3条第1項から第3項まで及び第5項における個人番号)。

(16) 特定個人情報

マイナンバーを含む個人情報のこと。個人番号(個人番号に対応し、当該個人番号に代わって用いられる番号、記号その他の符号であって、住民票コード以外のものを含む。番号法第7条第1項及び第2項、第8条並びに第48条並びに附則第3条第1項から第3項まで及び第5項を除く。)をその内容に含む個人情報をいう。

### 3 対象とする脅威

情報資産に対する脅威として、次の脅威を想定し、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、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の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情報システムの運用の機能不全等
- (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

本ガイドラインが対象とする情報資産及び対象者の範囲は次のとおりとする。

(1) 情報資産の範囲

- ア ネットワーク、情報システム及びこれらに関する設備並びに電磁的・光学的的外部記憶媒体等
- イ ネットワーク及び情報システムで取り扱う情報
- ウ 文書(情報システムに関連するデータを入力するための文書、印刷した文書、仕様書、ネットワーク図、各種レセプト類等も含む。)

(2) 対象範囲

- ア 上記(1)「情報資産の範囲」で規定された情報資産を取り扱う職員
- イ 本市の情報資産を取り扱う全ての情報システム

## 5 組織体制

(1) 最高情報責任者(CIO: Chief Information Officer)

デジタル推進室に関する事務を所掌する副市長を最高情報責任者とする。最高情報責任者は、本市における全てのネットワーク及び情報システム等の情報資産の管理責任を有するとともに、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最高情報セキュリティ責任者(CISO)を兼務し、CIOと呼ぶ。

(2) CIO 補佐官

最高情報責任者が、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 CIO 補佐官として置くもの

(3) 情報セキュリティ総括責任者

デジタル推進室長を、情報セキュリティ総括責任者とする。情報セキュリティ総括責任者は、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。また、情報セキュリティ総括責任者は、個人番号(生存する個人のものだけでなく死者のものも含む。)及び特定個人情報の管理に関する事務を総括する任に当たる。

(4) 情報セキュリティ責任者

八王子市の当該指定管理業務を所管する部等の部長又はこれに相当する職にある職員(以下「部長等」という。)を情報セキュリティ責任者とする。

(5) 情報セキュリティ管理者

八王子市の当該指定管理業務を所管する課等の課長又はこれに相当する職にある職員(以下「課長等」という。)を情報セキュリティ管理者とする。

(6) 情報システム管理者

八王子市の各情報システムの担当課長等を、当該情報システムに関する情報システム管理者とする。なお、課長等が不在の部等については、情報セキュリティ責任者が兼務する。

(7) 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市の担当者を情報システム担当者とする。

(8) CSIRT(Computer Security Incident Response Team)

サイバー攻撃などの情報セキュリティインシデントが発生した際に、発生状況の取りまとめや、関係者へ連絡、報告などをするチームであり、コンピュータやネットワークでセキュリティ上の問題が起きていないかどうか監視すると共に、万が一問題が発生した場合に、原因の分析や調査を行う組織。デジタル推進室情報管理担当主幹を CSIRT 管理者とし、情報管理担当職員を CSIRT 職員とする。

(9) 情報セキュリティ対策責任者

ア 指定管理者における情報セキュリティの責任者を情報セキュリティ対策責任者とする。

イ 情報セキュリティ対策責任者は、番号法で定める個人番号及び特定個人情報を取り扱う事務の範囲並びにその事務で取り扱う特定個人情報の範囲を明確にしておかなければならない。

ウ 情報セキュリティ対策責任者は、特定個人情報事務取扱担当者の役割及び取り扱う特定個人情報の範囲を明確化しなければならない。

(10) 情報システム対策担当者

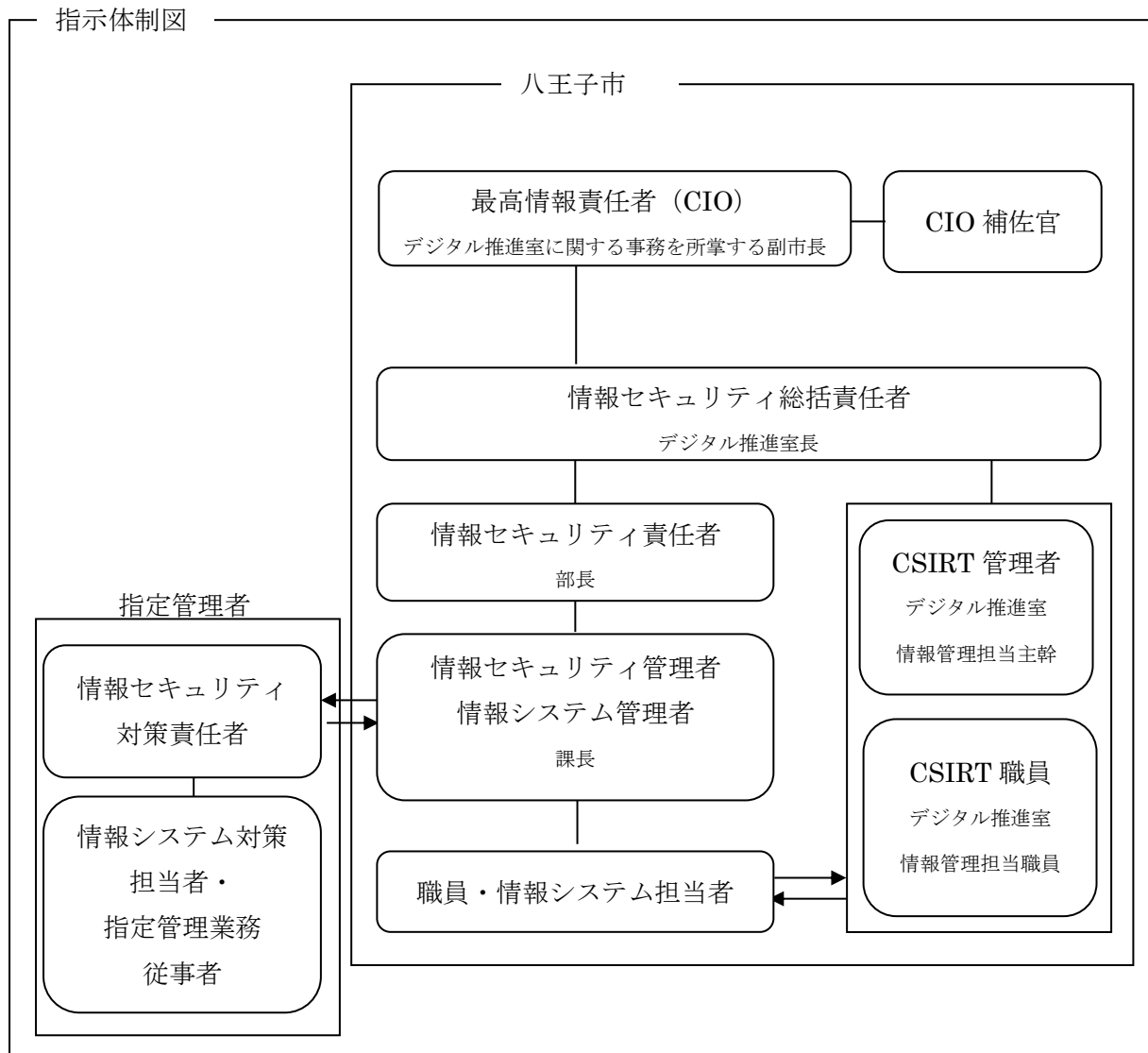
指定管理者における、情報システムの開発、設定の変更、運用、更新等の作業を行う者を情報システム対策担当者とする。

(11) 指定管理業務従事者

指定管理業務を行う者を指定管理業務従事者とする。

## 6 指示体制

(1) 情報セキュリティに関する指示体制は次のとおりとする。



(2) 指定管理者は、指定管理業務の実施前に「情報セキュリティ対策責任者」及び「情報セキュリティ対策責任者が不在の際にその責務を代行できる者」を定め市に報告すること。

## 7 情報資産及びネットワークの分類と管理

(1) 情報資産の分類、管理及び取扱いとは下表のとおりとする。

分類	分類基準	管理及び取扱い
機密性		
機密性 3	<p>1 情報公開条例第8条の次の各号で定める非公開情報</p> <p>(1) 第1号(法令秘密)</p> <p>(2) 第2号(個人情報)</p> <p>2 その他</p> <p>セキュリティ侵害等により、市の情報セキュリティ及び市民の権利に重大な影響を及ぼすもの</p>	<p>【機密性3】</p> <ul style="list-style-type: none"> <li>・電子メール及びファクシミリによる送信の制限</li> <li>・保存時の暗号化又はパスワード設定</li> </ul> <p>【機密性3及び機密性2】</p> <ul style="list-style-type: none"> <li>・私物の端末による作業禁止</li> <li>・自宅への持ち帰りを原則禁止</li> <li>・必要以上の複製及び配布を原則禁止</li> </ul>
機密性 2	<p>1 情報公開条例第8条の次の各号で定める非公開情報</p> <p>(1) 第3号(法人情報)</p> <p>(2) 第4号(安全・秩序維持)</p> <p>(3) 第5号(審議・検討等)</p> <p>(4) 第6号(行政運営)</p> <p>(5) 第7号(任意提供)</p> <p>2 その他</p> <p>セキュリティ侵害等により、市民の権利又は指定管理事務の適確な遂行に影響を及ぼすおそれがあるもの</p>	<ul style="list-style-type: none"> <li>・保管場所の制限、保管場所への必要以上の記憶媒体の持ち込みを原則禁止</li> <li>・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定</li> <li>・鍵付きケースへの格納等の対策</li> <li>・復元不可能な処理を施しての廃棄</li> <li>・信頼のできるネットワーク回線の選択</li> <li>・外部における情報処理作業の制限</li> <li>・記憶媒体の施錠可能な場所への保管</li> </ul>
機密性 1	機密性2又は機密性3の情報資産以外のもの	



完全性		
完全性 2	情報資産のうち、改ざん、誤びゅう又は破損により、市民等の権利が侵害される、又は指定管理事務の適確な遂行に影響(軽微なものを除く。)を及ぼすおそれがあるもの	<ul style="list-style-type: none"> <li>・バックアップ</li> <li>・外部における情報処理作業の制限</li> <li>・記憶媒体の施錠可能な場所への保管</li> </ul>
完全性 1	完全性 2 の情報資産以外のもの	
可用性		
可用性 2	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、市民等の権利が侵害される又は指定管理業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もの	<ul style="list-style-type: none"> <li>・バックアップ、指定する時間以内の復旧</li> <li>・記憶媒体の施錠可能な場所への保管</li> </ul>
可用性 1	可用性 2 の情報資産以外のもの	

## (2) 情報資産台帳の作成

保有する情報資産を台帳等に記録し、適正に管理すること。また作成した情報資産の記録を市の求めに応じて速やかに提出すること。記載すべき内容は以下の内容とする。

- ア 情報資産の種類(表示例:ハードウェア、ソフトウェア、外部記憶媒体、設備、ドキュメント等)
- イ 情報資産の名称・型番(表示例:○○システム用端末、○○システム用ソフトウェア、CD-R、無停電電源装置、○○システム開発資料等)
- ウ 台数・個数
- エ 保管場所
- オ バックアップの有無
- カ 廃棄方法(表示例:○年○月○日、業者により廃棄等)
- キ 情報資産の分類(表示例:機密性3、完全性2、可用性2等)
- ク 管理責任者

## (3) 情報資産の作成

機密性3の情報には、原則として複製禁止とする。やむを得ず複製して媒体や他のシステム又は外部にデータを提供する場合は、情報セキュリティ対策責任者が許可をし、暗号化又はパスワード設定をすること。

(4) 情報資産の入手

組織外から受け取った外部記憶媒体は、当該組織との間で情報を運搬する目的に限って使用するものとし、事前にウイルスチェックするなど、当該記憶媒体から情報を読み込む場合及び、これに情報を書き出す場合の安全を確保すること。

(5) 情報資産の利用

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。

(6) 情報資産の保管

ア 作成又は入手した情報資産は、7 (1) に基づき、当該情報の分類を定めること。また、分類に応じた管理及び取扱いをすること。

イ 機密性2以上、完全性2又は可用性2の文書は施錠保管すること。

ウ 機密性2以上、完全性2又は可用性2の電子データを格納した記憶媒体は施錠保管すること。

エ 情報セキュリティ対策責任者は外部記憶媒体を施錠保管すること。

オ USBメモリは施錠保管し、外付けハードディスクは施錠保管又はセキュリティワイヤーで固定するなど、盗難防止措置を講じること。

カ 機密性3の電子データを保存する場合は、適正なアクセス制限を実施し、暗号化又はパスワード設定をすること。

キ 指定管理業務従事者は必要に応じて、情報のバックアップを実施すること。

ク 特定個人情報等を取り扱う場合は、当該情報の利用及び保管等の取扱状況について記録を行い、取扱記録について7年間保存すること。

(7) 情報資産の持ち出し・運搬

ア 機密性2以上の情報資産を情報セキュリティ区域外に持ち出し又は運搬するときは、暗号化又はパスワード設定をし、鍵付きケースに格納する等の安全措置を講じること。

イ 機密性2以上の情報資産を情報セキュリティ区域外に持ち出し又は運搬する者は、情報セキュリティ対策責任者の許可をとり、記録を残すこと。

(8) 情報資産の提供

ア 機密性2以上の情報資産を外部に提供するときは、暗号化又はパスワード設定をし、鍵付きケースに格納する等の安全措置を講じること。また、情報セキュリティ対策責任者の許可をとり、記録を残すこと。

イ 個人情報を含む情報資産を外部に提供する場合は、個人情報保護条例の規定を確認すること。

ウ 情報セキュリティ対策責任者は、外部に公開する情報資産について、完全性を確保すること。

(9) 情報資産の廃棄

ア 機密性2以上の情報資産を廃棄する者は、記憶媒体の初期化、データ消去ソフトウ

ェアによる消去又は物理的破壊など、情報を復元できないように処置した上で廃棄し、紙媒体についてはシュレッダー、焼却又は溶解等により廃棄すること。ただし、マイナンバーを含む情報を直接保存した記憶装置を廃棄する者は、原則として物理的破壊、磁氣的破壊など、情報を完全に復元できないように処置した上で廃棄すること。

イ 情報資産の廃棄や入れ替えを行うときは、情報資産台帳に日時、担当者及び処理内容を記録すること。

ウ 個人番号又は特定個人情報情報を削除又は廃棄した場合には、その記録を保存すること。

エ 特定個人情報に関する廃棄記録は、7 年間保存すること。

#### (10) 情報の送信

ア 電子メール等により機密性 2 以上の情報を送信する場合は、本文に当該情報を記載せず、添付ファイルを暗号化又はパスワード設定の上、送信すること。

イ 誤送信を避けるため、送信前に必ず宛先を確認すること。

#### (11) ネットワークの分類と管理

ア 特定個人情報を取り扱うネットワークとインターネットに接続するネットワークは分離し、互いに通信できないようにしなくてはならない。

### 8 セキュリティ区域

- (1) セキュリティ区域とは、機密性2以上の情報やそれら进行处理する機器等が保管・設置されている領域をいう。
- (2) 情報セキュリティ対策責任者はセキュリティ区域を定義し、セキュリティ区域図を作成すること。
- (3) 機密性 2 以上の情報やそれら进行处理する機器等は、セキュリティ区域内に保管及び設置し、この区域のセキュリティを確保すること。
- (4) セキュリティ区域に入室できる者を定め、権限のない者が許可なく入室しない旨を記載した、セキュリティ区域の表示を行うこと。
- (5) セキュリティ区域内に入室できる者以外の者の入退室を記録し、管理すること。
- (6) 外部からの訪問者がセキュリティ区域に入る場合には、セキュリティ区域への入退室を許可された指定管理業務従事者が必ず付き添うこと。
- (7) 情報セキュリティ対策責任者は、鍵管理簿等を用いて、必要に応じて鍵の管理簿等の記載による貸出・返却管理を行うこと。

### 9 パソコン等の管理

- (1) 指定管理業務に係るパソコン等の機器は、適正に管理すること。
- (2) 指定管理料においてパソコン等の購入、指定管理料で購入したパソコン等の廃棄を行う

場合は、情報セキュリティ管理者に報告すること。

- (3) 情報セキュリティ対策責任者は、所管する端末で利用されているすべてのソフトウェアを把握した上で定期的に調査を行い、不適正な状態にある端末を検出した場合には改善を図ること。
- (4) 指定管理業務に係るパソコン等のOS及びソフトウェア等は最新のセキュリティ更新プログラムを適用すること。
- (5) 情報セキュリティ対策責任者は、管理するパソコンや外付けのハードディスクに、盗難防止の対策を講じること。

#### 10 指定管理業務従事者の遵守事項

- (1) 本ガイドラインを遵守すること。
- (2) 情報セキュリティ対策責任者は、本ガイドラインについて不明な点、遵守できていない項目が発見された場合は、速やかに情報セキュリティ管理者に相談し、指示を仰ぐこと。
- (3) 情報資産、インターネット及びメールを業務以外の目的で利用しないこと。
- (4) 情報資産の機密性によって、適正に管理及び取り扱いを行うこと。
- (5) 情報資産の持ち出し及び外部における情報処理作業を行う場合は、安全措置を講じること。
- (6) 指定管理業務においてソーシャルメディアサービスの個人アカウントを利用し業務連絡をする場合は、機密性2以上の情報は取り扱わないこと。
- (7) 指定管理業務において、市で調達したもの、指定管理料で調達したもの、指定管理者所有のもの以外のパソコン等の利用は原則として禁止する。ただし、情報セキュリティ管理者の許可を得た場合はこの限りではない。
- (8) 情報資産の持ち出し及び持ち込みを行う場合は記録すること。
- (9) 指定管理業務に係るパソコン等の端末におけるセキュリティ設定を変更しないこと。
- (10) 端末から離れるときにはロックをかけること。
- (11) 机上の文書等は適正に管理すること。(クリアデスクの実施)
- (12) 退職時等は情報資産等を返却し、退職等の後も指定管理業務で知り得た情報を漏らしてはならない。

#### 11 ガイドライン等の閲覧

情報セキュリティ対策責任者は、指定管理業務従事者が本ガイドライン及び緊急時対応計画等を閲覧できるようにすること。

#### 12 情報セキュリティに関する研修・訓練

- (1) 新たに指定管理業務従事者を採用した場合は、配属時に本ガイドラインに関する研修を実施すること。

- (2) 情報セキュリティ対策責任者は、年1回以上指定管理業務従事者に対して情報セキュリティに関する研修を実施すること。
- (3) 情報セキュリティ対策責任者は、特定個人情報の事務取扱担当者に対し、必要な教育研修を行うこと。また、事務取扱担当者のうち特定個人情報ファイルを取り扱う事務に従事する者に対し、番号法第29条の2に定めるサイバーセキュリティの確保に関する事項その他の事項に関する研修を実施すること。
- (4) 緊急時対応を想定した訓練を行うこと。

### 1 3 情報セキュリティインシデントの報告

情報セキュリティ対策責任者は、指定管理業務において事故、欠陥等の情報セキュリティインシデントが発生した場合、次のとおり対応すること。

- (1) 緊急時対応計画を遵守すること。
- (2) 6 指示体制に基づき報告すること。
- (3) 原因を究明し、記録及び再発防止策を情報セキュリティ管理者に報告すること。
- (4) 指定管理業務に係るパソコン等でウイルスを検出又は感染した場合は、直ちに情報セキュリティ管理者又は情報システム管理者に報告すること。

### 1 4 指定管理業務に係る ID 及びパスワード等の取扱い

指定管理者は、指定管理業務に係るID及びパスワード等について、次のとおり取り扱うこと。

- (1) ID及びパスワードは、システム及びOSにおいて、必ず設定すること。
- (2) ユーザID及びパスワードは適正に発行及び管理を行うこと。
- (3) 個人のIDは他者に利用させないこと。
- (4) 共用IDは原則禁止とする。ただし、業務上又はシステム上必要な場合は、必要最小限での運用とし、権限のない者に利用させないこと。
- (5) 特権 ID の利用者登録は厳格に行い、誤設定、悪意を持った設定変更をけん制するために二人以上の者に付与すること。
- (6) 特権IDを付与された者は、管理者としての業務遂行時に限定して当該IDを利用すること。
- (7) 利用を新たに開始する時は、初期パスワードから変更すること。
- (8) パスワードは8桁以上とし、数字、アルファベット、大文字小文字、記号を混ぜ、想像しにくいものにしなければならない。ただし、システム上設定が不可能な場合において、情報システム管理者が認めた場合はこの限りではない。
- (9) パスワードは他者に知られないよう留意し、パスワードの照会等には一切応じてはならない。
- (10) パスワードは定期的に変更し、他者から容易に推測されないように留意すること。  
(推奨:90日)

- (11) サーバ、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てはならない。
- (12) 指定管理業務従事者等から、パスワードの初期化依頼があった場合には、正当な利用者であることを確認した上で初期化すること。
- (13) 異動、退職等で付与されたIDを利用する必要がなくなった場合には、直ちにIDを返却すること。

## 1 5 指定管理業務に係るシステムの取扱い

情報システム対策担当者は、指定管理業務に係るシステムについて、以下の事項を遵守すること。

### (1) 物理的セキュリティ対策

- ア 情報資産を安全に保管できるよう、設備を整備すること。
- イ 情報システムで利用する機器は、湿度、温度に敏感であることから、室内環境を整えること。
- ウ サーバの二重化をするよう努めること。
- エ 無停電電源装置を設置するなど、停電時等の対策を講じること。
- オ 通信ケーブル等は損傷を防ぐよう配線すること。
- カ 情報システムの安定的な運営のため、定期的に保守点検を実施すること。
- キ 指定管理者の施設外にサーバの機器を設置している場合は、定期的に物理的なセキュリティ状況を確認すること。
- ク 機器を廃棄等する場合には、ハードディスクからの確実なデータ消去を実施すること。業者等に廃棄を委託する場合は、廃棄証明書を徴するなどして確認すること。
- ケ 機器の搬入出時は、指定管理業務従事者等が立会うこと。
- コ 通信回線及び通信回線装置の管理を適正に行うこと。
- サ サーバ及びパソコン等の端末を、不正利用、紛失、盗難、情報漏えい等の被害から防止するための対策を講じて管理すること。
- シ 特定個人情報情報を保存するサーバ等の機器を設置する場合は、情報セキュリティ総括責任者の承認を得ること。
- ス 特定個人情報情報を保存するサーバ等の機器を設置する場合は、施錠設備、監視設備、警報装置等を備えるなど、許可されていない者の立入りを防止すること。また、必要に応じて出入口の特定化による入退室の管理の容易化、入室に係る認証機能の設定、パスワード等の管理に関する定めの整備(その定期又は随時の見直しを含む。)及びパスワード等の読取防止等を行うために必要な措置を講じること。

### (2) 情報システムの管理

- ア 指定管理業務従事者に、業務の遂行以外の目的で情報システムを利用させないこと。
- イ 指定管理業務従事者に、情報セキュリティ総括責任者が接続許可を与えた通信回線

及びネットワーク以外に市の情報システムを接続させないこと。

- ウ ネットワーク接続制御及びアクセス制御等を十分活用するためハードウェア・ソフトウェアの設定を適正に行うこと。
- エ ファイルサーバの容量を設定し、指定管理業務従事者に周知すること。
- オ ファイルサーバには権限設定をすること。
- カ 緊急時に備え、バックアップを実施すること。
- キ システムの管理、作業記録を行い、適正に管理すること。
- ク 情報システム仕様書等は適正に管理すること。
- ケ 情報セキュリティの確保に必要なアクセスログや記録を取得し、一定の期間保存するよう努めること。
- コ アクセス記録を取得し、適正に管理すること。
- サ ログの不正な削除、窃取及び改ざん等を防止するため、適正な管理を行うとともに、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定期的に点検又は分析を実施するよう努めること。
- シ 特定個人情報の取り扱いに関する各種ログ及び情報セキュリティの確保に必要な記録を必ず取得し、7年間保存すること。
- ス 障害があった場合には障害記録を作成し、適正に保管すること。
- セ デバイス制御を行い、許可されたUSB接続機器以外は接続できないようにすること。
- ソ 無線LANを設置する場合は、設置前に本市に協議し許可を得ること。また、盗聴対策を適正に行うこと。
- タ 電子メールをシステムで利用する場合、以下の事項を遵守すること。
  - (ア) 大量のスパムメール等の受信又は送信を検知した時はメールサーバの運用を停止する。
  - (イ) 電子メールの送受信容量の上限を設定する。
  - (ウ) 電子メールボックスの容量の上限を設定する。
  - (エ) 委託業者等外部の者にメールを利用させない。
- チ ソフトウェアを情報セキュリティ対策責任者の許可なく導入させないこと。
- ツ 機器構成の変更を制限すること。

### (3) アクセス制御

- ア 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がアクセスできないように、システム上制限すること。
- イ 業務利用のために用意された端末以外のパソコン、モバイル端末及び外部記憶媒体等がシステムにアクセスできないよう制御を行うこと。
- ウ 無許可でネットワークに接続しないこと。新たにインターネットや外部のシステムに接続を要する場合は構成図等を提出し、情報セキュリティ管理者の許可を得ること。
- エ 外部からシステムへの接続を制限すること。

オ 自動接続について適正に設定すること。

(4) 情報システムの調達

ア 情報システムを調達する場合は、セキュリティ要件を明記した仕様書を作成すること。

イ 機器及びソフトウェアを調達する場合は、セキュリティ機能を調査し、問題がないことを確認すること。

ウ 取り扱う情報に応じて適正な回線種別を選択し、必要に応じて、通信内容の秘匿やサーバ装置及び端末のアクセス制御及び経路制御を行う機能を設けること。

エ 情報システムの開発責任者及び作業者を特定すること。

オ 情報システムの開発用IDを適正に管理し、開発終了後に必ず開発用IDを削除させること。

カ 情報システムの開発に用いるハードウェア及びソフトウェアを管理すること。

キ アプリケーションやコンテンツの作成を外部委託する場合は、不正プログラムや脆弱性が含まれることのないよう留意すること。

ク 開発環境と運用環境は分離し、移行手順を明確にすること。

ケ 運用環境への移行は、テストを行いその結果を確認した後に行うこと。機密性3の情報及び生データをテストデータに使用しないこと。ただし、情報セキュリティ責任者に許可を得た場合はこの限りではない。

コ システム開発・保守に関する資料はシステムが存在する期間適正に保管すること。

サ 情報システムにおける入出力データの正確性を確保すること。

シ システムのプログラムを変更した場合は、変更履歴を作成すること。

ス サーバ、端末及び通信回線装置の設置又は運用開始時に、当該機器上で利用するソフトウェアに関連する公開された脆弱性についての対策を実施すること。

セ 開発・保守用のソフトウェアにおいてもソフトウェアの更新、セキュリティパッチの適用を行うこと。

ソ 指定管理業務従事者による業務遂行を目的としたリモートアクセス環境を構築する場合は、VPN回線を整備し通信経路及びアクセス先のセキュリティを確保すること。

(5) 不正アクセス対策

ア 不正アクセスを防止するため使用されていないTCP/IPポートは閉鎖すること。

イ 攻撃の予告があった場合は、システムの停止等を検討し、本市に報告すること。

ウ アクセス記録、対応記録等を保存すること。

エ 内部からの攻撃への対策を講じること。

オ 指定管理業務従事者等による不正アクセスを防止するための対策を講じること。

カ サービス不能攻撃を防止するための対策を講じること。

キ 標的型攻撃を防止するため、教育及び訓練等の人的対策並びに入口対策等のシステムの対策を総合的に講じること。

ク 本市の求めに応じ、地方公共団体情報システム機構によるサイバー攻撃検知通報事



業や脆弱性診断の実施、ウェブ感染型マルウェア検知等の事業に参加・協力すること。

(6) セキュリティ情報の収集

- ア 情報セキュリティ対策責任者は、サーバ、端末及び通信回線上で利用するソフトウェアにおける脆弱性対策の状況を定期的に確認し、脆弱性対策が行われていない場合には、速やかに対策を行うこと。
- イ セキュリティパッチの適用を適宜行うこと。深刻なセキュリティホールが見つかった場合には直ちに対応すること。
- ウ サポート終了OSは原則使用しないこと。システム上やむを得ずサポートの終了したOSを使用しなくてはならない場合は、情報セキュリティ管理者又は情報システム管理者の許可を得ること。
- エ 情報セキュリティ事件・事故や侵害等の未然の防止のために、セキュリティ情報の収集、対策を行うこと。

(7) 侵害時の対応に関する遵守事項

緊急時対応計画を策定し、侵害時の対応を定めておくこと。

## 1 6 機器等の使用に係る遵守事項

- (1) 情報セキュリティ対策責任者は、適正にファイルサーバを設定すること。
- (2) 情報セキュリティ対策責任者は、指定管理業務の電子データについて、バックアップを実施すること。
- (3) 情報セキュリティ対策責任者は、指定管理業務において複合機を使用する場合、適正なセキュリティ設定を行うこと。
- (4) 情報セキュリティ対策責任者は、指定管理業務において特定用途機器を使用する場合、適正なセキュリティ設定を行うこと。
- (5) 情報セキュリティ対策責任者は、指定管理業務においてUSBメモリ、外付けのハードディスクドライブ、外付けのストレージサーバ、モバイル端末(スマートフォン、タブレット)及びカードリーダーを使用する場合、使用を開始する前に、情報セキュリティ管理者に申請し、情報セキュリティ管理者は、情報セキュリティ総括責任者に協議すること。
- (6) 情報セキュリティ対策責任者は、指定管理業務において USB 接続機器(デジタルカメラやスキャナ等)を使用する場合は、使用を開始する前に、情報システム管理者に届出をすること。
- (7) 指定管理業務においてUSBメモリ、外付けのハードディスクドライブ、外付けのストレージサーバ、モバイル端末(スマートフォン、タブレット)及びカードリーダーを使用する場合、以下の事項を遵守すること。
  - ア システムや端末に接続する機器は最小限とすること。
  - イ 接続するUSB機器は、ウイルス対策機能付暗号化USBメモリを使用するよう努めるこ

と。

ウ 定められた機器以外は利用できないよう制御を行うよう努めること。

- (8) 指定管理業務従事者は、指定管理業務において電子メールを利用する場合、以下の事項を遵守すること。

ア 自動転送機能を用いないこと。

イ 機密性2以上の情報を送信する場合は、必要に応じて暗号化又はパスワード設定を行うこと。

ウ 機密性3の情報を電子メールで送信することは原則として禁止する。やむを得ず送信する場合は、情報セキュリティ対策責任者の許可を得た上で、暗号化又はパスワード設定を行い、複数で確認を行ってから送信をすること。

エ 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で送信するなど、他の送信先の電子メールアドレスが分からないようにすること。

オ 重要なメールを誤送信した場合、直ちに情報セキュリティ対策責任者及び情報セキュリティ管理者に報告すること。

カ ウェブで利用できるフリーメール、ネットワークストレージサービス等を使用しないこと。

- (9) 指定管理業務従事者は、指定管理業務においてファクシミリを利用する場合、以下の事項を遵守すること。

ア 機密性3の情報をファクシミリで送信することは原則として禁止する。やむを得ず送信する場合は、情報セキュリティ対策責任者の許可を得ること。

イ 誤送信を避けるため、電話等で送信を予告し、ファクシミリの完了レポート等で送信文書の到達を確認すること。

- (10) 指定管理業務に係るパソコン等の端末において、新たなソフトウェアの導入を行わないこと。ただし、業務上必要があるソフトウェアについては、情報セキュリティ管理者又は情報システム管理者の許可を得て、使用許諾条件を確認した上で導入すること。

- (11) 指定管理業務従事者は、指定管理業務において、業務以外の目的でウェブを閲覧しないこと。

## 17 不正プログラム対策

指定管理業務に係るパソコン等において、以下の事項を実施すること。

- (1) 情報セキュリティ対策責任者は、ウイルス対策ソフトを常駐させること。
- (2) 情報セキュリティ対策責任者は、ウイルス定義ファイルを最新のものに更新すること。
- (3) 指定管理業務従事者は、外部からデータ又はソフトウェアを取り入れる場合はウイルスチェックを行うこと。
- (4) 情報セキュリティ対策責任者は、指定管理業務において不自然なメールを受信した場合は、開封せずに情報セキュリティ管理者に報告すること。

## 18 緊急時対応計画の策定

- (1) 情報セキュリティ対策責任者は、情報セキュリティインシデントの発生に備え、緊急時対応計画を定め、有事の際は当該計画に従って対処すること。
- (2) 緊急時対応計画には、関係者の連絡先、想定される事故や障害、発生した事案への対応措置を記載すること。
- (3) 情報セキュリティ対策責任者は、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更に応じて緊急時対応計画を適宜見直すこと。

## 19 委託

指定管理業務の一部を委託する場合、以下の事項を遵守すること。

- (1) 情報セキュリティ対策責任者は、再委託を行う場合は、委託先が再委託をする事務において取り扱う情報資産に対して、適正なセキュリティ対策が講じられていることを確認した上で、市の承認を得ること。なお、再委託先が更に委託をする場合(再々委託)及びそれ以降の委託についても同様である。
- (2) 個人番号利用事務等の全部又は一部の委託を受けたものが再委託をする場合には、委託をする個人番号利用事務等において取り扱う特定個人情報の適正な安全管理が図れることを確認した上で、市の承認を得ること。

## 20 クラウドサービスの利用

クラウドサービスを利用する場合は、以下の事項を遵守すること。

- (1) クラウドサービスを利用する場合は、ハードウェア、ソフトウェア、取り扱うデータ等の情報資産を情報資産台帳に記載すること。
- (2) 無料クラウドサービスを利用して機密性2以上の情報資産を保存しないこと。
- (3) 機密性2以上の情報資産をクラウドサービスで取り扱う場合は、クラウドサービスの関連設備はすべて日本国内に設置していることを確認すること。
- (4) 機密性2以上の情報資産をクラウドサービスで取り扱う場合は、特定のネットワークや端末からの接続のみ許可する仕組み(グローバルIPアドレス指定・MACアドレス指定等)を導入するよう努めること。
- (5) 機密性3の情報資産をクラウドサービスで取り扱う場合は、回線は安全な通信ができるもの(専用線やVPNなど)を選択するよう検討し、可能であれば回線の二重化等の冗長化を行うよう努めること。
- (6) 機密性3の情報資産をクラウドサービスで取り扱う場合は、HTTPS通信又はこれと同等以上の暗号化通信を使用すること。
- (7) クラウドサービス事業者が以下のような情報セキュリティ対策を継続して適正に行っているかを確認の上、選定すること。  
ア データセンターの物理的な情報セキュリティ対策(災害対策や侵入対策等)を取ってい

ること。

イ データのバックアップを定期的を取得していること。

ウ ハードウェア機器の障害対策を実施していること。

エ 仮想サーバ等のホスト側のOS、ソフトウェア、アプリケーションにおける脆弱性の判定と対策(セキュリティ更新プログラムの適用)を実施していること。

オ 不正アクセスの防止対策を講じていること。

カ アクセスログの管理をしていること。

キ 通信の暗号化を実施していること。

- (8) ID、パスワードを適正に管理すること。ID、パスワードの変更管理については、14 指定管理業務に係るID及びパスワード等の取扱いに準ずること。
- (9) クラウドサービスを利用する端末は、17 不正プログラム対策に準ずること。
- (10) クラウドサービスを利用する時は、外部からの通信の制限や自動接続の設定に関して適正なアクセス制限を行うこと。
- (11) クラウドサービスを利用する時は、クラウド事業者と合意されたバックアップ方針に従って定期的にバックアップを行うこと。
- (12) クラウドサービスで機密性2以上の情報資産を取り扱う場合は、クラウドサービス事業者に対して国内法令が適用されることを仕様書で明確にすること。

## 2 1 約款による外部サービスの利用

情報セキュリティ対策責任者は、以下を含む約款による外部サービスの利用に関する規定を整備しなければならない。また、当該サービスの利用におけるリスクが許容できるかを確認するとともに、原則として機密性2以上の情報が取り扱われないように規定しなければならない。

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

## 2 2 ソーシャルメディアサービスの利用

ツイッターやフェイスブックをはじめとするソーシャルメディアサービスを、指定管理業務において利用する場合、以下の事項を遵守すること。

- (1) 情報セキュリティ対策責任者は、ソーシャルメディアによる情報発信の運用開始前に情報セキュリティ管理者と調整を行うこと。
- (2) なりすまし対策を講じること。また、指定管理者になりすましたソーシャルメディアのアカウントを発見した場合は、指定管理者ホームページを通じ、当該アカウントを指定管理者が運用をしていない旨の周知を行うとともに、当該ソーシャルメディア管理者に対し削除依頼を行うこと。
- (3) パスワードを適正に管理し、利用する端末を限定するなどして、不正アクセス対策を講じる

こと。また、パスワードは15桁以上とすること。

- (4) 複数のソーシャルメディアサービスを利用する場合、同一のパスワードを使いまわさないこと。
- (5) 機密性2以上の情報(公開情報以外)は発信しないこと。
- (6) 利用するソーシャルメディアサービスごとに責任者を定めること。
- (7) 次の事項を定めたアカウント運用ポリシーを設定し、指定管理者ホームページに明記するとともに、利用者が容易にソーシャルメディアにたどりつけるよう、指定管理者ホームページにURLを記載しリンク等を設定すること。

ア 情報発信の目的・内容

イ 利用するソーシャルメディアの種類

ウ アカウント名

エ 管理者

オ 運用期間及び運用時間

カ 投稿等への対応(情報収集、返信の有無)

キ 禁止事項

ク 知的財産権

ケ 免責事項

- (8) 公式に運用することを周知するため、ソーシャルメディアの提供機関が認証アカウントの発行を行っている場合は、原則として認証アカウントを取得すること。
- (9) 利用するソーシャルメディアのアカウント説明欄等において、当該アカウントの運用を行っている旨の表示をしている指定管理者ホームページのURLを記載すること。
- (10) 基本的人権、肖像権、プライバシー権、著作権等に関して十分留意すること。
- (11) 一度インターネット上に公開された情報は完全には削除できないことを十分理解し、発信する情報は正確に記述するとともに、その内容について誤解を招かぬよう留意すること。
- (12) 公平・中立な立場で情報を発信し、第三者に不快感を与えるような表現を用いないこと。
- (13) 全ての市民がソーシャルメディアを利用しているものではないことを踏まえ、また、従来の情報媒体との特性の違いを理解し、相互に補完できるよう効果的な情報発信に努めること。
- (14) 次に掲げる情報は発信してはならない。
  - ア 誹謗、中傷、不敬な言い方を含む情報
  - イ 市のセキュリティを脅かすおそれのある情報
  - ウ 意思形成過程の情報
  - エ 人種、思想、信条等の差別、又は差別を助長させる情報
  - オ 違法行為又は違法行為を煽る情報
  - カ 噂話や噂を助長させる情報
  - キ 業務上必要のない指定管理業務従事者の個人的な状況や意見等の情報

ク 公の秩序又は善良の風俗に反する情報

- (15) 投稿等への対応については、アカウント運用ポリシーに記載している事項を除き、アカウントごとに定めるものとする。
- (16) 事実と反する内容が投稿された場合は次の対応を行うこと。
  - ア 当該ソーシャルメディアから正しい情報を発信し、必要に応じて正しい情報を発信しているホームページへのリンクを掲載する。
  - イ 当該投稿は、アカウント運用ポリシーに基づき削除する。
- (17) 批判や苦情が殺到し、収集がつかなくなった場合は、発信した情報により、誤解を生じさせた場合には、誠実に対応するとともに、正しく理解されるよう努めること。また、発信した情報に対し攻撃的な反応があった場合には、反論や抗弁は控えるなど、冷静に対応し無用な議論となることを避けるようにすること。
- (18) 本来のURLをわかりにくくするURL短縮サービスは、原則として使用しないこと。
- (19) 第三者アカウント情報の引用や、第三者が管理又は運用するページへのリンクを掲載する場合は、指定管理者が当該情報を信頼性があるものとして認めたものと受け取られることを考慮した上で行わなければならない。
- (20) アカウント乗っ取りを確認した場合には、情報セキュリティ管理者に速やかに報告し、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。

## 2.3 ウェブサイト

指定管理業務においてウェブサイトを作成、管理する場合は、以下の事項を遵守すること。

- (1) ウェブサイトの構築、改修又は保守を行う場合、本市の求めにより脆弱性の診断を行える旨仕様書等に明記すること。
- (2) 脆弱性が発覚した場合には、修正すること。なお、重大な脆弱性が発覚した場合には、情報セキュリティ管理者へ報告し、運用を一時的に中止し、直ちに修正すること。運用の再開は、情報セキュリティ管理者の許可を得た後に行うこと。
- (3) ウェブコンテンツの編集作業者を限定すること。
- (4) 公開してはならない又は不要なウェブコンテンツが公開されないよう管理すること。
- (5) ウェブサイトにログインする際のID、パスワードを適正に管理すること。ID、パスワードの変更管理については、14 指定管理業務に係るID及びパスワード等の取扱いに準ずること。
- (6) 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、全ての情報に対する暗号化及び電子証明による認証の対策の導入に努めること。
- (7) ウェブサイトの開発において、既知の脆弱性を排除するための対策を講じること。
- (8) データベースを導入する際は機密性を確保するため、適正なアクセス制御を行うこと。
- (9) データベースに機密性3の情報を格納する場合は、不正な操作を防止する対策を講じ、データベースを必要に応じ暗号化すること。

- (10) ウェブサイト公開期間中にウェブサイトのアドレスを変更したとき及び公開終了後にウェブサイトのアドレスの利用が終わったときに、悪意のある第三者が当該ウェブサイトのアドレスを取得し、なりすましができるリスクを避けるため、旧アドレスの利用をしなくなったときには、一定期間ドメインを解約せずに残しておき、訪れた利用者にサイトが閉鎖したこと及び新しいウェブサイトがある場合は、新しいウェブサイトへの案内文を載せ周知すること。

## 2 4 自己点検

情報セキュリティ対策責任者は、本ガイドラインに沿った情報セキュリティ対策状況について毎年度自己点検すること。

## 2 5 監査

- (1) 指定管理者は、本市の求めに応じて情報セキュリティ監査の実施に協力すること。
- (2) 指定管理者は、監査の指摘事項の改善に努めること。