

「板橋区情報セキュリティ対策基準」

【別冊】クラウドサービス上で標準準拠システム等を整備及び運用する場合における対策基準（第1版）

令和6年4月1日

目次

総則.....	- 1 -
第1部 組織体制	- 2 -
第2部 情報資産の分類と管理.....	- 4 -
第3部 情報システム全体の強靱性の向上.....	- 8 -
第4部 物理的セキュリティ	- 10 -
第1章 サーバ等の管理.....	- 10 -
第2章 管理区域（情報システム室等）の管理.....	- 13 -
第3章 通信回線及び通信回線装置の管理	- 14 -
第4章 職員等の利用する端末や電磁的記録媒体等の管理	- 14 -
第5部 人的セキュリティ.....	- 15 -
第5章 職員等の遵守事項	- 15 -
第6章 研修・訓練.....	- 16 -
第7章 ID 及びパスワード等の管理	- 17 -
第6部 技術的セキュリティ	- 19 -
第8章 コンピュータ及びネットワークの管理.....	- 19 -
第9章 アクセス制御	- 24 -
第10章 システム開発、導入、保守等.....	- 26 -
第11章 不正プログラム対策.....	- 29 -
第12章 不正アクセス対策	- 32 -
第13章 セキュリティ情報の収集.....	- 33 -
第7部 運用	- 34 -
第14章 情報システムの監視.....	- 34 -
第15章 情報セキュリティポリシーの遵守状況の確認.....	- 34 -
第16章 情報セキュリティ事故管理	- 35 -
第17章 法令遵守.....	- 36 -
第8部 業務委託と外部サービスの利用	- 38 -
第18章 業務委託.....	- 38 -
第19章 外部サービスの利用	- 39 -
第9部 評価・見直し	- 42 -
第20章 監査.....	- 42 -
第21章 自己点検.....	- 43 -
第22章 情報セキュリティポリシー及び関係規程等の見直し.....	- 43 -

総 則

地方公共団体情報システムの標準化に関する法律第5条第1項に基づき、地方公共団体情報システムの標準化の推進を図るための基本的な方針として策定された「地方公共団体情報システム標準化基本方針」では、以下が示されたところである。

- ① 地方公共団体が利用する標準準拠システムに適合する基幹業務システム等の整備及び運用に当たっては、サイバーセキュリティ等に関する標準化基準として、標準準拠システムのセキュリティ、可用性、性能・拡張性、運用・保守性、移行性、システム環境・エコロジーに係る機能要件以外の要件（非機能要件）について、指標、選択レベル及び選択時の条件の基準を定めること。
- ② 総務省が作成する「地方公共団体における情報セキュリティポリシーに関するガイドライン」を参考にしながら、セキュリティ対策を行うものとする。
- ③ 地方公共団体は、基本方針及び「地方公共団体の基幹業務システムのガバメントクラウドの利用に関する基準」で示される国と地方の責任分界に基づき、地方公共団体の責任とされる範囲において具体的なセキュリティ対策を行うこと。
- ④ マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド上の領域についてもガイドライン上のマイナンバー利用事務系として扱うこと。

このような状況を踏まえ、ガバメントクラウドの利用を中心として、クラウドサービス上で標準準拠システム・関連システム等の業務システム（以下「標準準拠システム等」という）を整備及び運用する場合の対策基準を「板橋区情報セキュリティ対策基準」の別冊として示す。

なお、本書は標準準拠システム等を整備及び運用する場合の対策事項を「板橋区情報セキュリティ対策基準」の本文に追記した構成となっている。

第 1 部 組織体制

1. DX推進本部

区の情報化施策の総合調整、推進をし、情報セキュリティについて統括する機関を板橋区DX推進本部（以下「本部」という。）とする。

2. 情報セキュリティ部会

区の情報セキュリティ対策を推進する機関を本部に設置する情報セキュリティ部会（以下「部会」という。）とする。

構成員は次のとおりとする。

- (1) 部会長は、政策経営部長とする。
- (2) 副部会長は、IT推進課長とする。
- (3) その他の構成員及び部会の役割は、別途定める。

3. 最高情報セキュリティ責任者（以下「CISO」という。）

- (1) CISOは、副区長とする。
- (2) CISOは、区における全てのネットワーク、情報システム等の情報資産の管理や情報セキュリティに関する権限及び責任を有する。

4. CISO補佐官

- (1) CISO補佐官は、政策経営部長とする。
- (2) CISO補佐官は、CISOを補佐し、その職務を代理することができる。

5. ネットワーク管理者

- (1) ネットワーク管理者は、IT推進課長とする。
- (2) ネットワーク管理者は、区の全ての情報システムにおける管理運用、情報セキュリティ対策等について、CISOを技術的側面で支援する。
- (3) ネットワーク管理者は、区の全ての情報システムにおける管理運用、情報セキュリティ対策等について、必要に応じて、情報化推進管理者から報告を受け、助言勧告する権限を有する。
- (4) ネットワーク管理者は、情報セキュリティ事故が発生した際、各課又は所より報告を受け、その状況を確認する統一的な窓口の機能を有する組織体制（CSIRT）を整備する。

6. 情報化推進管理者

- (1) 情報化推進管理者は、課長又は所長とする。ただし、学校、幼稚園は別途定めるものとする。
- (2) 情報化推進管理者は、実施手順を作成、維持、管理を行い、各課又は所における情報資産の適切な管理及び利用の推進を行う。
- (3) 情報化推進管理者は、情報システムの管理者として、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。

- (4) 情報化推進管理者は、各課又は所及び所管する情報システム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) 情報化推進管理者は、年に1回、各課又は所及び所管する情報システムにおける情報セキュリティ対策の実施状況を部会に報告する。
- (6) 情報化推進管理者は、情報セキュリティについて、各課又は所内の職員への教育、啓発、指導に努める。

7. 情報化推進リーダー

情報化推進管理者は、自らの役割を適切に遂行するため、補助を行う情報化推進リーダーを任命し、ネットワーク管理者に通知する。ただし、学校、幼稚園は別途定める。

8. 兼務の禁止

- (1) 情報セキュリティ監査の実施において、止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。

9. 管理責任

- (1) I T推進課が所管する情報システムについては、I T推進課の情報化推進管理者が管理責任を持つ。
- (2) 各課又は所が導入するシステムについては、各課又は所の情報化推進管理者が管理責任を持つ。
- (3) 各情報システムで取り扱う情報については、各課又は所の情報化推進管理者が管理責任を持つ。

10. クラウドサービス利用における組織体制

- (1) 情報化推進管理者は、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、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。

第2部 情報資産の分類と管理

1. 情報資産の分類及び情報区分における取扱制限

区における情報資産は、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。

(1) 情報区分Ⅰ

区の保有する情報資産のうち、「秘密文書等の取扱いについて（昭和40年4月15日事務次官等会議申合せ）」に定める秘密文書、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に定める特定個人情報及び個人情報の保護に関する法律に定める個人情報¹（要配慮個人情報・個人識別符号含む）・仮名加工情報。

(2) 情報区分Ⅱ

情報区分Ⅰ以外の情報資産のうち、東京都板橋区情報公開条例（以下「情報公開条例」という。）第2条第2号に定める公文書（公文書の作成を目的として記録されたものを含む）であって、情報公開条例第6条第1項各号で定める公開文書以外のもの。

(3) 情報区分Ⅲ

情報区分Ⅰ・Ⅱ以外の情報資産。

(4) 情報区分Ⅰ・Ⅱにおける取扱制限

- ① 必要以上の複製及び配付禁止
- ② 保管場所の制限、保管場所への必要以上の電磁的記録媒体等の持ち込み禁止
- ③ 情報の送信、外部記憶媒体を用いた情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納
- ④ 信頼のできるネットワーク回線の選択
- ⑤ 外部で情報処理を行う際の安全管理措置（ただし、外部サービスを利用する場合は、外部サービス利用ガイドラインによるものとする）
- ⑥ 電磁的記録媒体の施錠可能な場所への保管

2. 情報資産の管理

(1) 管理責任

- ① 情報化推進管理者は、その所管する情報資産について管理責任を有する。
- ② 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すること。
- ③ 情報推進管理者は、クラウドサービスの環境に保存される情報資産についても（1）の分類に基づき管理しなければならない。また、情報資産におけるライフサイクルの取扱いを定める。クラウドサービスを更改する際の情報資産の移行及びこれらの情報資産の全ての複製のクラウドサービス事業者からの削除の記述を含むサービス利用の終了に関する内容について、サービス利用前に文書での提示を求め、又は公開されている内容を確認すること。

¹ 法律に定める個人情報のうち、保有個人情報に限定する。仮名加工情報についても保有個人情報から生成されるものに限定する。

表1 情報資産の種類及び例

情報資産の種類	情報資産の例
文書	紙の文書
電磁的記録媒体	FD、MO、CD、USBフラッシュメモリ、DAT、CGMT等
電子データ	実施機関の職員が職務上作成・取得した情報 ² のうち、サーバ又はパソコンの磁気ディスク装置、電磁的記録媒体等に記憶している電子データ（電子文書、ソフトウェア、組織で運用している情報システムのソースコード等を含む。）
設置型ハードウェア ※床置き、机上、ラック等に設置等して使用する資産	サーバ、デスクトップパソコン、ルータ、スイッチ、プリンタ、ファクシミリ、コピー機、スキャナー等
移動型ハードウェア ※持ち出しができるように製造された資産	ノートパソコン、携帯電話、デジタルカメラ、ICレコーダ等

(2) 情報の作成

- ① 職員等は、業務上必要のない情報を作成してはならない。
- ② 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行うこと。また、情報区分に変更があった場合、変更後の情報区分に従った情報管理を行うこと。
- ③ 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すること。また、情報の作成途上で不要になった場合は、当該情報を消去すること。

(3) 情報資産の利用

- ① 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。
- ② 情報資産を利用する者は、情報資産の分類に応じ、適正に取扱うこと。
- ③ 情報資産を利用する者は、電磁的記録媒体に情報資産の分類が異なる情報が複数記録されている場合、最高度の分類に従って、当該電磁的記録媒体を取り扱うこと。

(4) 情報資産の保管

- ① 情報化推進管理者は、情報資産の分類に従って、情報資産を適正に保管すること。
- ② 情報化推進管理者は、情報資産を記録した電磁的記録媒体を長期保管する場合は、書込禁止の措置を講じること。
- ③ 情報区分Ⅰ・Ⅱの情報は、原則として情報セキュリティ対策が施されたサーバ内に保管すること。やむを得ず外部記憶媒体に記録する場合は、暗号化の上で、施錠可能な場所に保管すること。
- ④ 情報区分Ⅰ・Ⅱの情報は、原則としてインターネットに接続している情報システム機

² 内閣府「統計等データの提供等の判断のためのガイドライン」より引用
<<https://www.gyoukaku.go.jp/ebpm/guideline/index.html>>

器に保管することを禁止する。ただし、やむを得ず保管する場合は、ネットワーク管理者に協議した上で、アクセス制御などの保護措置を施すこと。（ただし、外部サービスを利用する場合は、外部サービス利用ガイドラインによるものとする）

(5) 情報の送信

- ① 個人情報等機密性の高い情報を原則として電子メールで送信してはならない。
- ② 個人情報等機密性の高い情報を送受信する場合は、情報化推進管理者の許可を得たうえで、ファイルストレージシステム等の定められた方法により実施すること。

(6) 情報の持ち出し

- ① 情報を持ち出す際は、利用目的及び権限の確認をすること。
- ② 情報区分Ⅰ・Ⅱの情報は、原則として持ち出しを禁止する。ただし、業務上必要とする場合は、情報化推進管理者の許可を得た上で、台帳を作成し、記録を残すこと。
- ③ 情報区分Ⅰ・Ⅱの情報を持ち出す際は、データの暗号化、施錠可能なケースに収納する等の情報漏洩対策を講じること。

(7) 情報資産の運搬

- ① 車両等により情報区分Ⅰ・Ⅱの情報資産を、外部記憶媒体を用いて運搬する者は、必要に応じ鍵付きのケース等に格納し、パスワード等による暗号化を行う等、情報資産の不正利用を防止するための措置を講じること。
- ② 情報区分Ⅰ・Ⅱの情報資産を、外部記憶媒体を用いて運搬する者は、情報化推進管理者に許可を得ること。また、追跡可能な移送手段を用いること。
- ③ 物理的な破損や衝撃から保護する梱包等、外部記憶媒体を保護するための処置を施すこと。

(8) 情報資産の提供・公表

- ① 情報を提供する外部機関に対し、情報の利用範囲を確認し、適正な管理を保証させること。
- ② 情報区分Ⅰ・Ⅱの情報資産を外部に提供する者は、情報化推進管理者に許可を得ること。
- ③ 情報区分Ⅰ・Ⅱ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暗号化を行うこと。
- ④ 情報化推進管理者は、住民に公開する情報資産について、完全性を確保すること。

(9) 情報の閲覧

情報区分Ⅰの情報を閲覧させる際は、情報化推進管理者の書面による許可を得た上で閲覧台帳を作成し、記録を残すこと。

(10) 情報資産の廃棄等

- ① 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電磁的記録媒体について、その情報の機密性に応じ、情報を復元できないように処置すること。
- ② 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すること。
- ③ 情報資産の廃棄やリース返却等を行う者は、情報化推進管理者の許可を得ること。
- ④ クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了

時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理すること。

第3部 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を通信できないようにすること。ただし、やむを得ず外部との通信をする必要がある場合は、特定通信で行うこと。なお、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、インターネット等からLGWANを経由して双方向での情報の移送を可能とするが、以下の対策を講じること。
 - ① 外部接続先とは、連携サーバを設置して通信を行うこと。
 - ② 外部接続先との通信先を限定すること。
 - ③ 許可されていない端末から外部接続先へ接続しないこと。
 - ④ 外部接続先とは、認証・暗号化・改ざんへの検知等の対策を講じること。また、通信の履歴等を取得すること。
 - ⑤ 外部接続に利用する端末についても持ち出し不可設定等の措置を講じること。
- (2) 端末からの情報の持ち出し不可設定や端末への二要素認証対策を講ずること。
- (3) 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扱い
マイナンバー利用事務系の端末・サーバ等と専用回線により接続されるガバメントクラウド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、区の他の領域とはネットワークを分離すること。
- (4) 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い
マイナンバー利用事務系の情報システムをガバメントクラウド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せること。
また、クラウドサービス事業者が暗号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、必要な措置を行うこと。

2. LGWAN 接続系

- (1) LGWANと接続する情報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し、以下の無害化通信対策を講ずること。
 - ① 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接続系に転送するメールテキスト化方式を実施すること。
 - ② インターネット接続系の端末から、LGWAN接続系の端末に画面転送する方式を実施すること。
 - ③ 危険因子をファイルから除去し、又は危険因子が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を実施すること。
- (2) 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扱い
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、専用回線を用いて接続するこ

と。

3. インターネット接続系

(1) 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講ずるため、自治体情報セキュリティクラウドの利用を実施すること。

(2) 業務の効率性・利便性の向上を目的とし、インターネット接続系に主たる業務端末を配置する場合、必要な情報セキュリティ対策を講じたうえで、事前に外部による確認を実施し、確認の報告書を地方公共団体情報システム機構へ提出すること。また、配置後も定期的に外部監査を実施することとし、監査報告書を地方公共団体情報システム機構へ提出すること。

(3) インターネット接続系に主たる業務端末を配置する場合、以下のセキュリティ対策を実施すること。

① ネットワークは原則、閉域網を利用すること。ただし、やむを得ずインターネット回線を利用する場合、VPN通信等を用い、かつ、通信元と通信先を特定し、通信経路を限定的にすること。

② 重要な情報をLGWAN接続系で取り扱う場合（ β モデル）

（ア）無害化处理

（イ）LGWAN系の画面転送

（ウ）未知の不正プログラム対策

（エ）業務システムログの管理

（オ）脆弱性管理

（カ）組織的なセキュリティ対策基準の順守

③ 重要な情報をインターネット接続系で取り扱う場合（ β' モデル）

（ア）無害化处理

（イ）LGWAN系の画面転送

（ウ）未知の不正プログラム対策

（エ）業務システムログの管理

（オ）情報資産単位でのアクセス制御

（カ）脆弱性管理

（キ）セキュリティの継続的な検知・モニタリング体制の整備

（ク）組織的なセキュリティ対策基準の順守

（ケ）データベースやファイルの暗号化

（コ）区が許可していない外部接続先のサービスへのアクセスを監視、遮断

第4部 物理的セキュリティ

第1章 サーバ等の管理

1. 機器の取付け

情報化推進管理者は、サーバ等の機器の取付けを行う場合、火災、水害、埃、振動、温度、湿度等の影響を可能な限り排除し、入室が制限された場所に設置し、容易に取り外せないよう適正に固定する等、必要な措置を講じること。

2. 機器の電源

(1) 情報化推進管理者は、サーバ等の機器の電源について、停電等による電源供給の停止に備え、当該機器が適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ること。

(2) 情報化推進管理者は、落雷等による過電流に対して、サーバ等の機器を保護するための措置を講じること。

3. 通信ケーブル等の配線

(1) 情報化推進管理者は、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ること。

(2) 情報化推進管理者は、自ら又は情報化推進リーダー及び契約により操作を認められた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ずること。

4. 機器の定期保守及び修理

(1) 情報化推進管理者は、サーバ等の機器の定期保守を実施し、可用性を維持すること。

(2) 情報化推進管理者は、電磁的記録媒体を内蔵する機器を事業者に修理させる場合、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うこと。

5. 庁外への機器の設置

情報化推進管理者は、データセンターの利用等庁外に機器を設置する場合には、情報の機密性に応じたセキュリティレベルが確保されるサービスを利用すること。また、定期的に情報セキュリティ実施状況を確認すること。

6. 機器の廃棄等

(1) 情報化推進管理者は、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こと。

(2) クラウドサービス事業者が利用する資源（装置等）の処分（廃棄）をする者は、セキュリティを確保した対応となっているか、クラウドサービス事業者の方針及び手順について確認しなければならない。

なお、当該確認にあたっては、クラウドサービス事業者が利用者に提供可能な第三者による監査

報告書や認証等を取得している場合には、その監査報告書や認証等を利用できる。

表2 機器の廃棄方法

分類	機器の廃棄方法	廃棄の確認方法
<p>A マイナンバー利用事務系の領域において住民情報を保存する記録媒体</p> <p>※マイナンバー利用事務系：社会保障、地方税、防災、戸籍事務等に関する情報システム及びデータ</p>	<p>当該媒体を分解・粉碎・溶解・焼却・細断などによって物理的に破壊し、確実に復元を不可能とすること</p> <p>リース契約により調達する場合においても、リース契約終了後、当該機器の記録媒体については、物理的に破壊を行う。この場合、予め仕様に明記のうえ、機器の廃棄方法を契約において明記すること</p> <p>データセンターを利用している場合であっても、機器を原則として物理的に破壊すること</p> <p>なお、サービス利用形態等により、物理的な破壊が困難な場合のデータの消去方法については、予めネットワーク管理者と協議すること</p>	<ul style="list-style-type: none"> ・職員による立ち会いによる確認 ・庁内において情報の復元が困難な状態までデータ消去を行った上で、物理的破壊の完了証明書の確認 ・完了証明書は、破壊の証拠写真が貼付及び提出期限が定められていること
<p>B 情報区分Ⅰ又はⅡ以上に該当する情報を保存する記録媒体（上記Aに該当するものは除く）</p>	<ul style="list-style-type: none"> ① 物理的な方法による破壊 ② 磁気的な方法による破壊 ③ OS 等からのアクセスが不可能な領域も含めた領域をデータ消去装置またはデータ消去ソフトウェアによる上書き消去 ④ ブロック消去 ⑤ 暗号化消去 <p>のうち、いずれかの方法を選択</p>	<ul style="list-style-type: none"> ・庁内において情報の復元が困難な状態までデータ消去を行った上で、データ消去の完了証明書を確認（ただし、外部サービスを利用する場合は、外部サービス利用ガイドラインによるものとする）

<p>C 情報区分Ⅲ該当するもの</p>	<p>上記①～⑤の方法のほか、 ⑥ OS 等からアクセス可能な全てのストレージ領域をデータ消去装置またはデータ消去ソフトウェアによる上書き消去のうち、いずれかの方法を選択</p>	<p>・ 庁内において情報の復元が困難な状態までデータ消去を行った上で、データ消去の完了証明書を確認（ただし、外部サービスを利用する場合は、外部サービス利用ガイドラインによるものとする）</p>
----------------------	-----------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------

第2章 管理区域（情報システム室等）の管理

1. 管理区域の構造等

- (1) 管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための部屋（以下「情報システム室」という。）や電磁的記録媒体の保管庫をいう。
- (2) 情報化推進管理者は、管理区域に関する管理体制を明確にすること。
- (3) 情報化推進管理者は、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すること。
- (4) 情報化推進管理者は、情報システム室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じること。
- (5) 情報化推進管理者は、管理区域に配置する消火薬剤や消防用設備等が、機器及び電磁的記録媒体等に影響を与えないようにすること。

2. 管理区域の入退室管理等

- (1) 情報化推進管理者は、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うこと。また、1年ごとに入退室者の妥当性を確認すること。
- (2) 職員等及び委託事業者は、管理区域に入室する場合、身分証明書等を携帯すること。
- (3) 情報化推進管理者は、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ること。
- (4) 情報化推進管理者は、情報区分Ⅰ・Ⅱ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、または個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないこと。

3. 機器等の搬入出

- (1) 情報化推進管理者は、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、あらかじめ確認すること。
- (2) 情報化推進管理者は、情報システム室の機器等の搬入出は、職員が立ち合いのうえ行うこと。

4. その他措置事項

- (1) 情報システム室を管理する情報化推進管理者の許可がない限り、電子機器、写真、ビデオ等による撮影及び録音は禁止すること。
- (2) 一般常識上危険物と認められる物の持ち込みは禁止すること。
- (3) 喫煙及び飲食は禁止すること。
- (4) 複写機及びFAX機器は可能な限り設置しないこと。

第3章 通信回線及び通信回線装置の管理

1. ネットワーク管理者は、庁内の通信回線及び通信回線装置を、適正に管理すること。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すること。
2. ネットワーク管理者は、外部へのネットワーク接続及び接続ポイントを必要最低限に限定すること。
3. ネットワーク管理者は、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ること。
4. ネットワーク管理者は、情報区分Ⅰ・Ⅱ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、適正な回線を選択すること。また、必要に応じ、送受信される情報の暗号化を行うこと。
5. ネットワーク管理者は、ネットワークに使用する回線について、伝送途上に情報が破壊、盗聴、改ざん、消去等が生じないように十分なセキュリティ対策を実施すること。
6. ネットワーク管理者は、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すること。また、必要に応じ、回線を冗長構成にする等の措置を講じること。

第4章 職員等の利用する端末や電磁的記録媒体等の管理

1. 情報化推進管理者は、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、モバイル端末及び電磁的記録媒体の使用時以外の施錠管理等の物理的措置を講じること。電磁的記録媒体については、情報が保存される必要がなくなった時点で速やかに記録した情報を消去すること。
2. 情報化推進管理者は、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。
3. 情報化推進管理者は、マイナンバー利用事務系では「知識」、「所持」、「存在」を利用する認証手段のうち二つ以上を併用する認証（多要素認証）を行うよう設定すること。
4. 情報化推進管理者は、モバイル端末の庁外での業務利用の際は、上記対策に加え、端末のデータ非保持、遠隔消去機能を利用する等の措置を講じること。

第5部 人的セキュリティ

第5章 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すること。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、速やかにネットワーク管理者に相談し、指示を仰ぐこと。

(2) 業務以外の目的での使用の禁止

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

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

職員等は、区のモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合には、情報化推進管理者の許可を得ること。

(4) 職員等は、外部で情報処理業務を行う場合には、情報化推進管理者の許可を得ること。

(5) 支給以外のパソコン、モバイル端末及び電磁的記録媒体等を原則業務に利用してはならない。ただし、業務上やむを得ず利用する場合は、情報化推進管理者の許可を得ること。

(6) 持ち出し及び持ち込みの記録

情報化推進管理者は、端末等の持ち出し及び持ち込みについて、記録を作成し、保管すること。

(7) パソコンやモバイル端末におけるセキュリティ設定変更の禁止

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

(8) 机上の端末等の管理

職員等は、パソコン、モバイル端末、電磁的記録媒体及び情報が印刷された文書等について、第三者に使用されること又は情報化推進管理者の許可なく情報を閲覧されることがないように、離席時のパソコン、モバイル端末のロックや電磁的記録媒体、文書等の容易に閲覧されない場所への保管等、適正な措置を講じること。

(9) 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すること。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。

(10) クラウドサービス利用時等の遵守事項

職員等は、クラウドサービスの利用にあたって情報セキュリティポリシーを遵守し、クラウドサービスの利用に関する自らの役割及び責任を意識すること。

2. 会計年度任用職員及び臨時職員等への対応

(1) 情報セキュリティポリシー等の遵守

情報化推進管理者は、会計年度任用職員及び臨時職員に対し、採用時に情報セキュリティポリシー等のうち、会計年度任用職員及び臨時職員が守るべき内容を理解させ、また実施及び遵守させること。

(2) インターネット接続及び電子メール使用等の制限

情報化推進管理者は、会計年度任用職員及び臨時職員にパソコンやモバイル端末による作業を行わせる場合において、インターネットへの接続及び電子メールの使用等が不要の場合、これを利用できないようにすること。

3. 情報セキュリティポリシー等の掲示

情報化推進管理者は、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すること。

4. 委託事業者に対する説明

情報化推進管理者は、ネットワーク及び情報システムの開発・保守等を事業者が発注する場合、再委託事業者も含めて、情報セキュリティポリシー等のうち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すること。

第6章 研修・訓練

1. 情報セキュリティに関する研修・訓練

(1) 定期的に情報セキュリティに関する研修・訓練を実施すること。

(2) 定期的にクラウドサービスを利用する職員等の情報セキュリティに関する意識向上、教育及び訓練を実施するとともに、委託先を含む関係者については委託先等で教育、訓練が行われていることを確認すること。

2. 研修計画の策定及び実施

(1) 全ての職員等に対する情報セキュリティに関する研修計画の策定とその実施体制の構築を定期的に行い、部会の承認を得ること。

(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すること。

(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すること。

(4) 各課又は所の職員及び長期間に渡って勤務する委託事業者に対し、情報セキュリティ教育研修を実施し、基本方針、対策基準及び実施手順を理解させ、情報セキュリティ上の問題が生じないようにさせること。

(5) 情報セキュリティに関する研修の内容には、特定個人情報等の適切な管理に関する内容を含めること。

(6) 情報化推進管理者は、所管する各課又は所の研修の実施状況を記録し、部会に報告すること。

(7) 情報セキュリティに関する研修実施後は、適宜内容を評価し、研修内容を見直すこと。

3. 緊急時対応訓練

緊急時対応を想定した訓練を定期的実施すること。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すること。

4. 研修・訓練への参加

全ての職員等は、定められた研修・訓練に参加すること。

第7章 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、次の事項を遵守すること。

- ① 認証に用いるIC カード等を、職員等間で共有しないこと。
- 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抜いておくこと。
- ③ IC カード等を紛失した場合には、速やかに情報化推進管理者に通報し、指示に従うこと。

(2) 情報化推進管理者は、IC カード等の紛失等があった場合は、当該IC カード等を使用したアクセス等を速やかに停止すること。

(3) 情報化推進管理者は、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すること。

2. ID の取扱い

職員等は、自己の管理するID に関し、次の事項を遵守すること。

- (1) 自己が利用しているID は、他人に利用させないこと。
- (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ないこと。

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、次の事項を遵守すること。

- (1) パスワードは、他者に知られないように管理すること。
- (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ないこと。
- (3) パスワードは十分な長さとし、文字列は想像しにくいものにすること。
- (4) パスワードが流出したおそれがある場合には、情報化推進管理者に速やかに報告し、パスワードを速やかに変更すること。
- (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ないこと。

- (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を変更すること。
- (7) 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ないこと。
- (8) 職員等間でパスワードを共有しないこと（ただし、共用ID に対するパスワードは除く）。

第6部 技術的セキュリティ

第8章 コンピュータ及びネットワークの管理

1. 情報システム運用手順書の整備

情報化推進管理者は、システムの運用を明確にするため、運用手順書を整備すること。運用手順書は、各システムの機能や特性に応じて、次の項目から必要な観点を踏まえること。

- ① 情報システムの形態・緊急時の連絡経路を含む管理体制
- ② 情報システムにおける機器・ソフトウェア・ネットワークの構成及び運用管理体制
- ③ 情報システムの起動及び停止方法
- ④ 停電、災害等のシステムの復旧方法
- ⑤ アカウントの管理方法
- ⑥ データのバックアップ、リストア方法
- ⑦ 記録媒体の管理方法
- ⑧ ICカードの管理方法
- ⑨ 各種ログの確認方法
- ⑩ 無停電電源装置の確認方法
- ⑪ 外部機関とのデータ交換方法
- ⑫ システムの保守方法
- ⑬ ウイルス対策

2. フォルダ及びファイルの設定等

情報化推進管理者は、ファイルサーバを構築する場合は、次の事項を実施すること。

- (1) 職員等が使用できるフォルダの容量を設定し、職員等に周知すること。
- (2) 共有のフォルダ領域を各課又は所の単位で構成し、職員等が他課又は所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、設定すること。
- (3) 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、同一課又は所であっても、担当職員以外の職員等が閲覧及び使用できないように設定すること。
- (4) 新規に作成されたフォルダやファイル等のアクセス権限の初期設定は、アクセス権限のない者による不正利用ができない設定とすること。

3. バックアップの実施

- (1) 情報化推進管理者は、ファイルサーバ等に記録された情報について、サーバの冗長化対策に関わらず、必要に応じて定期的にバックアップを実施すること。

また、オンプレミスでファイルサーバを構築する場合は、バックアップにあたって以下を実施すること

- ① データのバックアップの手順を明確にすること。
- ② 重要な業務データのバックアップは、定期的に採取すること。
- ③ バックアップの世代管理を行うこと。
- ④ 正常にバックアップが実行されているか定期的に確認すること。
- ⑤ 媒体の劣化を考慮して定期的に媒体を交換すること。

(2) 情報課推進管理者は、クラウドサービス事業者のバックアップ機能を利用する場合、クラウドサービス事業者にバックアップ機能の仕様を要求し、その仕様を確認すること。また、その機能の仕様が区の求める要求事項を満たすことを確認すること。クラウドサービス事業者からバックアップ機能を提供されない場合やバックアップ機能を利用しない場合は、自らバックアップ機能の導入に関する責任を負い、バックアップに関する機能を設け、情報資産のバックアップを行うこと。

4. 他団体との情報システムに関する情報等の交換

情報化推進管理者は、他の団体と情報システムに関する情報及びソフトウェアを交換する場合、その取扱いに関する事項をあらかじめ定め、ネットワーク管理者の許可を得ること。

5. システム管理記録及び作業の確認

- (1) 情報化推進管理者は、情報システムの運用において実施した作業について、作業記録を作成すること。
- (2) 情報化推進管理者は、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すること。
- (3) 情報化推進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すること。

6. 情報システム仕様書等の管理

情報化推進管理者は、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の閲覧や、紛失等がないよう、適正に管理すること。

7. ログの取得等

- (1) 情報化推進管理者は、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、一定の期間保存すること。
- (2) 情報化推進管理者は、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、適正にログを管理すること。
- (3) 情報化推進管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施すること。なお、クラウドサービス事業者が収集し、保存する記録（ログ等）に関する保護（改ざんの防止等）の対応について、ログ管理等に関する対策や機能に関する情報を確認し、記録（ログ等）に関する保護が実施されているのか確認しなければならない。
- (4) 情報化推進管理者は、監査及びデジタルフォレンジック11に必要となるクラウドサービス事業者の環境内で生成されるログ等の情報（デジタル証拠）について、クラウドサービス事業者

から提供されるログ等の監視機能を利用して取得することで十分では無い場合は、クラウドサービス事業者に提出を要求するための手続を明確にすること。

8. 障害記録

情報化推進管理者は、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、適正に保存すること。

9. ネットワークの接続制御、経路制御等

- (1) ネットワーク管理者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定すること。
- (2) ネットワーク管理者は、不正アクセスを防止するため、侵入検知（侵入防止）システムを設置する等、ネットワークに適正なアクセス制御を施すこと。
- (3) ネットワーク管理者は、ネットワーク接続制御の適切な動作のため、定期的に性能の点検をすること。
- (4) ネットワーク管理者は、ネットワークの帯域を制御し、ネットワークの性能を維持すること。
- (5) ネットワーク管理者は、職務上及び運用上の条件を考慮して、ネットワーク接続制御内容を明確にすること。通過させるサービスは、必要最小限のものとすること。
- (6) 機密性が求められるシステムは、完全に切り離れた独立ネットワーク又は、それに相当する構成とすること。やむを得ず接続する場合は、十分な情報セキュリティ対策を講じ、安全性を確保すること。

10. 外部の者が利用できるシステムの分離等

情報化推進管理者は、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ること。

11. ネットワークの接続管理

ネットワーク管理者は、ネットワークに関する管理体制及び管理手順を明確にすること。

管理手順には次の項目を含め、1年ごとに見直すこと。また、変更があった場合は随時更新を行うこと。

- (1) ネットワーク全体の構成図
- (2) ネットワークの運用管理方法
- (3) ネットワーク運用管理体制図
- (4) ネットワーク接続基準
- (5) 情報システム機器を庁内ネットワークに接続する際の申請手順

12. 外部ネットワークとの接続制限等

- (1) 情報化推進管理者は、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、ネットワーク管理者の許可を得ること。

- (2) 情報化推進管理者は、接続方法等について、外部機関と協議の上、接続手順を明確にすること。
- (3) 情報化推進管理者は、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すること。
- (4) ネットワーク管理者は、外部機関から庁内のネットワークへの接続について、利用できる内部の業務システムを制限すること。
- (5) 情報化推進管理者は、外部機関とのネットワーク接続については、利用者認証を行うこと。
- (6) 情報化推進管理者は、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すること。
- (7) 情報化推進管理者は、ウェブサーバ等をインターネットに公開する場合、庁内ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続すること。
- (8) 情報化推進管理者は、ネットワーク接続を提供している通信事業者に対して、契約書等により適切な管理を保証させること。
- (9) 情報化推進管理者は、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、ネットワーク管理者の判断に従い、速やかに当該外部ネットワークを物理的に遮断すること。

13. 複合機のセキュリティ管理

- (1) 情報化推進管理者は、複合機を調達する場合、当該複合機が備える機能及び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対策を実施すること。
- (2) 情報化推進管理者は、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ること。
- (3) 情報化推進管理者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消する又は再利用できないようにする対策を講じること。

14. IoT 機器を含む特定用途機器のセキュリティ管理

ネットワーク管理者は、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ること。

15. 無線LAN 及びネットワークの盗聴対策

- (1) 情報化推進管理者は、無線LANを構築する際には、盗聴対策等の情報セキュリティ対策を講じること。
- (2) 情報化推進管理者は、無線LANの情報セキュリティ対策等の管理手順を明確にすること。
- (3) 情報化推進管理者は、無線LANを利用する機器の導入、使用する場合は、ネットワーク管理者に事前に協議を行うこと。

16. 電子メールのセキュリティ管理

- (1) ネットワーク管理者は、権限のない利用者により、外部から外部への電子メール転送（電子メールの中継処理）が行われることを不可能とするよう、電子メールサーバの設定を行うこと。
- (2) ネットワーク管理者は、スパムメール等が内部から送信されていることを検知した場合は、メールサーバの運用を停止すること。
- (3) ネットワーク管理者は、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すること。
- (4) ネットワーク管理者は、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すること。
- (5) ネットワーク管理者は、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、委託事業者との間で利用方法を取り決めること。

17. 電子メールの利用制限

- (1) 職員等は、自動転送機能を用いて、電子メールを転送してはならない。
- (2) 職員等は、業務上必要のない送信先に電子メールを送信してはならない。
- (3) 職員等は、複数人に電子メールを送信する場合、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにすること。
- (4) 職員等は、重要な電子メールを誤送信した場合、情報化推進管理者に報告すること。

18. 電子署名・暗号化

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、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、送信すること。

19. 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、情報化推進管理者の許可を得て、ソフトウェアを導入することができる。なお、導入する際は、情報化推進管理者は、ソフトウェアのライセンスを管理すること。
- (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。

20. 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、情報化推進管理者の許可を得ること。

21. 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化推進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ないこと。
- (2) 情報化推進管理者は、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。

22. 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ないこと。
- (2) ネットワーク管理者は、職員等のウェブ利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報化推進管理者に通知し適正な措置を求めること。

23. Web 会議サービスの利用時の対策

- (1) ネットワーク管理者は、Web 会議を適切に利用するための利用手順を定めること。
- (2) 職員等は、区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、区の定める利用手順に従い、必要に応じて利用申請を行い、承認を得ること。

24. ソーシャルメディアサービスの利用

情報化推進管理者は、区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、ソーシャルメディアサービス運用手順を定め、次のセキュリティ対策を講じること。

- (1) 区のアカントによる情報発信が、実際の区のものであることを明らかにするために、区の自己管理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。
- (2) 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こと。
- (3) アカ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ること。

第9章 アクセス制御

1. アクセス制御等

(1) アクセス制御

- ① 情報化推進管理者は、所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限すること。
- ② 情報化推進管理者は、利用者登録、パスワード管理等の情報セキュリティ管理に関わる機能やセキュリティ情報を格納したファイルは、その利用を管理権限を持つ者のみに制限すること。

- ③ 情報化推進管理者は、情報システム利用時において、利用者が設定された一定期間に操作しない場合には、処理をロック（中断）又は、終了する機能を実装すること。

(2) 利用者ID の取扱い

- ① 情報化推進管理者は、利用者IDを一意に付与すること。
- ② 情報化推進管理者は、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ること。
- ③ 職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、情報化推進管理者に通知すること。
- ④ 情報化推進管理者は、利用されていないIDが放置されないよう、定期的に点検を行うこと。
- ⑤ 情報化推進管理者は、端末装置にパスワード情報を入力する際は、非表示又は、伏せ字にすること。

(3) 特権を付与されたID の管理等

- ① 情報化推進管理者は、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すること。
- ② 情報化推進管理者は、管理権限の利用者IDは、業務において一般に使用される利用者IDとは別に設けること。
- ③ 情報化推進管理者は、管理権限利用者の利用者IDに割り当てられるアクセス権限は、定期的に点検し、その正当性を確認すること。
- ④ 情報化推進管理者は、特権を付与されたID及びパスワードの変更について、委託事業者に行わせないこと。
- ⑤ 情報化推進管理者は、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こと。
- ⑥ 情報化推進管理者は、特権を付与されたIDを初期設定以外のものに変更すること。
- ⑦ 情報化推進管理者は、管理権限の利用者IDによる情報システム利用についてのアクセスログは、定期的に監査を行うこと。

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、情報化推進管理者の許可を得ること。
- (2) 情報化推進管理者は、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すること。
- (3) 情報化推進管理者は、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すること。
- (4) 情報化推進管理者は、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ること。
- (5) 情報化推進管理者は、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ること。

- (6) 職員等は、持ち込んだ又は外部から持ち帰ったモバイル端末を庁内のネットワークに接続する前に、コンピュータウイルスに感染していないこと、パッチの適用状況等を確認し、情報化推進管理者の許可を得るか、もしくは情報化推進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すること。
- (7) 内部のネットワーク又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する。ただし、止むを得ず接続を許可する場合は、利用者のID、パスワード及び生体認証に係る情報等の認証情報並びに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ること。

3. 自動識別の設定

情報化推進管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定すること。

4. ログイン時の表示等

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

5. 認証情報の管理

- (1) 情報化推進管理者は、職員等の認証情報を厳重に管理すること。認証情報ファイルを不正利用から保護すること。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、これを有効に活用すること。
- (2) 情報化推進管理者は、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ること。
- (3) 情報化推進管理者は、認証情報の不正利用を防止するための措置を講じること。

6. 特権による接続時間の制限

情報化推進管理者は、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こと。

第 10 章 システム開発、導入、保守等

1. 情報システムの調達

- (1) 情報化推進管理者は、情報システム開発、導入、保守等の調達に当たっては、調達仕様書に必要とする技術的なセキュリティ機能を明記すること。
- (2) 情報化推進管理者は、機器及びソフトウェアの調達に当たっては、当該製品のセキュリティ

機能を調査し、情報セキュリティ上問題のないことを確認すること。

- (3) 情報化推進管理者は、情報システム機器に十分な処理能力及び記憶容量が得られるように、将来の要求容量の予測も含めて調達すること。

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

情報化推進管理者は、システム開発の責任者及び作業者を特定すること。またシステム開発の手順等管理体制を明確にすること。

(2) システム開発における責任者、作業者のID の管理

- ① 情報化推進管理者は、システム開発の責任者及び作業者が使用するID を厳重に管理し、開発完了後、開発用ID を削除すること。
- ② 情報化推進管理者は、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すること。

(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

- ① 情報化推進管理者は、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すること。
- ② 情報化推進管理者は、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すること。

(4) 開発品質の維持等

開発品質の維持及び著作権の所有について、契約書又は要求仕様書等に記載すること。

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

- ① 情報化推進管理者は、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すること。
- ② 情報化推進管理者は、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すること。
- ③ 情報化推進管理者は、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すること。

(2) テスト

- ① 情報化推進管理者は、テスト実施時には、次の項目を記述したテスト仕様書を作成すること。
 - (ア) 各機能のテスト内容
 - (イ) 予想結果
 - (ウ) 実際のテスト結果
 - (エ) テスト結果の合否
- ② 情報化推進管理者は、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うこと。

- ③ 情報化推進管理者は、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うこと。
- ④ 情報化推進管理者は、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。やむを得ず使用する場合は管理手順を明確にし、次の保護対策を講じること。
 - (ア) 重要情報が特定できるデータのマスク処理等による消去
 - (イ) 本番環境と同等のアクセス制御
 - (ウ) 複写・複製等のテストデータに関する作業記録の収集
 - (エ) テスト完了後、テストで使用した本番データの削除
- ⑤ 情報化推進管理者は、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うこと。
- ⑥ 情報化推進管理者は、既存の各機能に影響を及ぼさず、セキュリティ機能が仕様通り動作したことを確認すること。

4. 情報システム機器及びソフトウェアの保守

- (1) 情報化推進管理者は、保守作業の手順を明確にすること。保守手順には保守後の情報セキュリティ機能が確保されているか確認するための手順も含めること。
- (2) 保守作業の範囲及び作業者を定めること。
- (3) 保守を定期的に実施すること。
- (4) 保守作業終了後には必ず作業終了報告を行わせること。
- (5) 保守作業記録は一定期間保管すること。
- (6) 定期保守について、その妥当性を必要に応じて見直すこと。
- (7) 保守時には職員が立ち会いを行うこと。
- (8) 情報化推進管理者は、情報システム機器の保守のために装置を外部事業者に出すときには、外部事業者に対して、契約書等により、適切な情報セキュリティ管理を保証させること。
- (9) 情報化推進管理者は、情報セキュリティに重大な影響を及ぼすソフトウェアについては、適切な保守が行われるようにし、その不具合については、速やかに修正等の対応を行うこと。

5. リモート保守の管理体制

- (1) 情報化推進管理者は、リモート保守の管理体制、許可手順、情報セキュリティ対策を明確にすること。
- (2) 情報化推進管理者は、外部事業者のリモート保守の許可を与える際、ネットワーク管理者と事前に協議を行い、他の情報システムへの影響を確認すること。
- (3) 情報化推進管理者は、リモート保守を実施する際は、保守対象情報システム担当者に事前に連絡を行わせること。
- (4) 情報化推進管理者は、リモート保守のアクセスログを取得すること。
- (5) 情報化推進管理者は、外部事業者の契約終了等の理由により、リモート保守の必要が無くなった場合には、速やかに利用者IDを削除すること。

6. システム開発・保守に関連する資料等の整備・保管

- (1) 情報化推進管理者は、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・保管すること。
- (2) 情報化推進管理者は、テスト結果を一定期間保管すること。
- (3) 情報化推進管理者は、情報システムに係るソースコードを適正な方法で保管すること。

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) 情報化推進管理者は、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すること。
- (2) 情報化推進管理者は、故意又は過失により情報が改ざんされる又は漏えいするおそれがある場合に、これを検出するチェック機能を組み込むように情報システムを設計すること。
- (3) 情報化推進管理者は、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すること。

8. 情報システムの変更管理

- (1) 情報化推進管理者は、情報システムの変更手順を明確にすること。
- (2) 情報化推進管理者は、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すること。
- (3) 変更手順には、情報システムの変更によるトラブルに備えた復旧及び対応方法を記述すること。
- (4) 変更手順の内容が有効であるかどうか事前にテストを行い確認すること。
- (5) 情報システムの変更にあたり、作業者の情報システムへのアクセス権限を必要な部分に限定すること。
- (6) 情報化推進管理者は、情報システム変更前のドキュメントや情報システム設定値は、最低限、変更後の安定稼動が確認できるまでの期間、旧バージョンである旨を明記して保管しておくこと。

9. 開発・保守用のソフトウェアの更新等

情報化推進管理者は、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すること。

10. システム更新又は統合時の検証等

情報化推進管理者は、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うこと。

第 11 章 不正プログラム対策

1. 不正プログラム対策における措置事項

- (1) 情報化推進管理者は、外部ネットワークから受信したファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等の不正プログラムのチェックを行い、不正プログラムのシステムへの侵入を防止すること。
- (2) 情報化推進管理者は、外部ネットワークに送信するファイルは、インターネットのゲートウェイにおいてコンピュータウイルス等不正プログラムのチェックを行い、不正プログラムの外部への拡散を防止すること。
- (3) 情報化推進管理者は、所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させること。
- (4) 情報化推進管理者は、不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保つこと。なお、 β モデル又は β 〃 モデルを採用する場合は、不正プログラム対策ソフトウェアは、未知の不正プログラムに対する対応も可能となるよう対策を講じること。
- (5) 情報化推進管理者は、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こと。
- (6) 情報化推進管理者は、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すること。
- (7) 情報化推進管理者は、インターネットに接続していないシステムにおいて、電磁的記録媒体を使う場合、コンピュータウイルス等の感染を防止するために、区が管理している媒体以外を利用しないこと。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すること。
- (8) 仮想マシンを設定する際に不正プログラムへの対策（必要なポート、プロトコル及びサービスだけを有効とすることやマルウェア対策及びログ取得等の実施）を確実に実施すること。SaaS 型を利用する場合は、これらの対応が、クラウドサービス事業者側でされているのか、サービスを利用する前に確認すること。また、サービスを利用している状況下では、これらのセキュリティ対策が適切にされているのか定期的にクラウドサービス事業者へ報告を求めること。
- (9) 情報化推進管理者は、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、情報化推進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。
- (10) 職員等は、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ないこと。
- (11) 職員等は、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うこと。
- (12) 職員等は、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、速やかに削除すること。
- (13) 職員等は、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すること。

- (14) 職員等は、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 接続系に取り込む場合は無害化すること。
- (15) 情報化推進管理者は、コンピュータウイルス等の不正プログラムの関連情報を収集し、職員等に教育研修を実施すること。
- (16) 職員等は、コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、事前に決められたコンピュータウイルス感染時の初動対応の手順に従って対応すること。

2. 不正プログラムの検査

- (1) 職員等は、定期的にコンピュータウイルス等の不正プログラムの検査を行うこと。
- (2) 職員等は、定期的な検査とは別に次の場面においてコンピュータウイルス等の不正プログラムの検査を行うこと。
 - ① 庁外へ情報システム機器や記録媒体を提供する場合
 - ② 新規にソフトウェアを導入する場合
 - ③ ネットワークを利用して、データを送信する場合
 - ④ 新しい情報システム機器や記録媒体を持ち込む場合
 - ⑤ 電子メールで受信した添付ファイルを開封する場合
 - ⑥ ダウンロードしたファイルを利用する場合

3. 不正プログラム発見時の手順の整備

情報化推進管理者は、コンピュータウイルス等の不正プログラム発見時の対応手順を明確にすること。また、手順には次の項目を含めること。

- ① 関係各所への緊急連絡網
- ② 情報システムに異常が生じた場合の速やかな原因究明
- ③ 感染した情報システムのネットワークからの隔離
- ④ 感染した情報システムの使用の禁止
- ⑤ 安全な復旧方法
- ⑥ 再発防止策
- ⑦ 所定機関の届け出に必要な情報
- ⑧ 事故報告の体制

4. 専門家の支援体制

ネットワーク管理者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、外部の専門家の支援を受けられるようにしておくこと。

第 12 章 不正アクセス対策

1. 不正アクセス対策における措置事項

不正アクセス対策として、以下の事項を措置すること。

- (1) ネットワーク管理者は、使用されていないポートを閉鎖すること。
- (2) ネットワーク管理者は、不要なサービスについて、機能を削除又は停止すること。
- (3) ネットワーク管理者は、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、情報化推進管理者へ通報するよう、設定すること。
- (4) 情報化推進管理者は、ネットワーク管理者と連携し、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すること。
- (5) 区が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）におけるアクセス制御に関する事項が、クラウドサービスにおいて実現できるのか又はクラウドサービス事業者の提供機能等により実現できるのか、利用前にクラウドサービス事業者を確認すること。
- (6) クラウドサービスを利用する際に、委託事業者等に管理権限を与える場合、多要素認証を用いて認証させ、クラウドサービスにアクセスさせなければならない。
- (7) パスワードなどの認証情報の割り当てがクラウドサービス側で実施される場合、その管理手順等が、区が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たすことを確認すること。

2. 攻撃への対処

- ① ネットワーク管理者及び情報化推進管理者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じること。また、総務省、都道府県等と連絡を密にして情報の収集に努めること。

3. 記録の保存

- ① ネットワーク管理者及び情報化推進管理者は、サーバ等に攻撃を受け、当該攻撃が不正アクセス禁止法違反等の犯罪の可能性がある場合には、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めること。

4. 内部からの攻撃

- ① ネットワーク管理者及び情報化推進管理者は、職員等及び委託事業者が使用しているパソコン等の端末からの庁内のサーバ等に対する攻撃や外部のサイトに対する攻撃を監視すること。

5. 職員等による不正アクセス

- ① ネットワーク管理者は、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各課又は所の情報化推進管理者に通知し、適正な処置を求めること。

6. サービス不能攻撃

- ① 情報化推進管理者は、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ること。

7. 標的型攻撃

- ① 情報化推進管理者は、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ること。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）を講じること。

第 13 章 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

- (1) 情報化推進管理者は、セキュリティホールに関する情報を収集し、必要に応じ、関係者間で共有すること。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すること。
- (2) 情報セキュリティ管理者は、クラウドサービス事業者に対して、利用するクラウドサービスに影響し得る技術的脆弱性の管理内容について情報を求め、区の業務に対する影響や保有するデータへの影響について特定する。そして、技術的脆弱性に対する脆弱性管理の手順について、クラウドサービス事業者を確認すること。

2. 不正プログラム等のセキュリティ情報の収集・周知

情報化推進管理者は、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、職員等に周知すること。

3. 情報セキュリティに関する情報の収集及び共有

情報化推進管理者は、情報セキュリティに関する情報を収集し、必要に応じ、関係者間で共有すること。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ること。

第7部 運用

第14章 情報システムの監視

1. 情報化推進管理者は、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すること。
2. 情報化推進管理者は、監視作業手順には次の項目を含めること。
 - (1) 必要なイベント事象のログ記録
 - (2) 異常が発見された場合の対処手順
3. 情報化推進管理者は、重要なログ等を取得するサーバの正確な時刻設定及びサーバ間の時刻同期ができる措置を講じること。また、利用するクラウドサービスで使用する時刻の同期についても適切になされているのか確認しなければならない。
4. 情報化推進管理者は、外部と常時接続するシステムを常時監視すること。
5. 情報化推進管理者は、必要となるリソースの容量・能力が確保できるクラウドサービス事業者を選定すること。また、利用するクラウドサービスの使用において必要な監視機能を確認するとともに監視により、業務継続の上で必要となる容量・能力を予測し、業務が維持できるように努めること。
6. 情報化推進管理者は、イベントログ取得に関するポリシーを定め、利用するクラウドサービスがその内容を満たすことを確認し、クラウドサービス事業者からログ取得機能が提供される場合は、そのログ取得機能が適切かどうか、ログ取得機能を追加して実装すべきかどうかを検討すること。
7. 情報化推進管理者は、クラウドサービス利用における重大なインシデントに繋がるおそれのある以下の重要な操作に関して、手順化し、確認しなければならない。
 - (1) サーバ、ネットワーク、ストレージなどの仮想化されたデバイスのインストール、変更及び削除
 - (2) クラウドサービス利用の終了手順
 - (3) バックアップ及び復旧

第15章 情報セキュリティポリシーの遵守状況の確認

1. 遵守状況の確認及び対処
 - (1) 情報化推進管理者は、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、速やかにネットワーク管理者に報告すること。

- (2) ネットワーク管理者は、発生した問題について、適正かつ速やかに対処すること。
- (3) 情報化推進管理者は、ネットワーク及びサーバ等のシステム設定等における情報セキュリティポリシーの遵守状況について、定期的に確認を行い、問題が発生していた場合には適正かつ速やかに対処すること。

2. パソコン、モバイル端末及び電磁的記録媒体等の利用状況調査

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

3. 職員等の報告義務

- (1) 職員等は、情報セキュリティポリシーに対する違反行為を発見した場合、直ちに情報化推進管理者に報告を行うこと。
- (2) 当該違反行為が直ちに情報セキュリティ上重大な影響を及ぼす可能性があると情報化推進管理者が判断した場合において、職員等は、緊急時対応手順に従って適正に対処すること。

第 16 章 情報セキュリティ事故管理

1. 「板橋区CSIRT設置基準」の策定

部会は、情報セキュリティインシデント、情報セキュリティポリシーの違反等により情報資産に対する情報セキュリティ事故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、事故対応手順を定めておき、情報セキュリティ事故発生時には当該手順に従って適正に対処すること。

また、部会は、クラウドサービス事業者と情報セキュリティインシデント管理における責任と役割の分担を明確にし、これらを踏まえてクラウドサービスの障害時を想定した事故対応手順を定めておき、情報セキュリティ事故発生時には当該手順に従って適正に対処すること。

2. 情報セキュリティ事故への準備

部会は、情報セキュリティ事故に係る管理体制及び事故対応手順を明確にすること。また、事故対応手順には次の内容を含めること。

- (1) 関係各所への緊急連絡網
- (2) 関係各所への報告体制
- (3) 情報セキュリティ事故によりサービスが停止した場合の復旧手段及び代替案
- (4) 発生原因の調査
- (5) 情報セキュリティ事故への対策手段の検討
- (6) 情報セキュリティ事故に関する情報の収集及び保管体制

3. 情報セキュリティ事故への対応

- (1) 情報化推進管理者は、情報セキュリティ事故からの復旧後に、情報システムのセキュリティ機能の正常動作を確認すること。
- (2) 情報化推進管理者は、情報セキュリティ事故の発生、調査結果、復旧手段について記録し、保存すること。
- (3) 情報化推進管理者は、再発防止策を検討し、同様の情報セキュリティ事故発生を防止すること。
- (4) 情報化推進管理者は、情報セキュリティ事故の被害レベルに応じ、「板橋区危機管理対応指針」及び「板橋区CSIRT設置基準」に基づき、必要な対応をとること。
- (5) ネットワーク管理者は、情報化推進管理者から情報セキュリティ事故について報告を受けた際は、事故の被害レベルに応じ、関係所管に報告すること。

4. 事故対応手順の見直し

ネットワーク管理者は、事故対応手順に沿って定期的に訓練を実施し、訓練の結果を受けて改善点がある場合には手順を見直すこと。

5. 外部からの情報セキュリティインシデントの報告

情報化推進管理者は、クラウドサービス事業者が検知した情報セキュリティインシデントの報告や情報セキュリティインシデントの状況を追跡する仕組みの構築を契約等で取り決めなければならない。

第17章 法令遵守

1. 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) 東京都板橋区個人情報保護法施行条例（令和4年板橋区条例第54号）
- (6) 東京都板橋区情報公開条例（平成12年東京都板橋区条例第1号）
- (7) 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）
- (8) 東京都板橋区個人番号及び特定個人情報の取扱いに関する条例（平成27年板橋区条例第56号）
- (9) サイバーセキュリティ基本法（平成26年法律第104号）

2. 情報化推進管理者は、クラウドサービスに商用ライセンスのあるソフトウェアをインストールする（IaaS等でアプリケーションを構築）場合は、そのソフトウェアのライセンス条項への違反

を引き起こす可能性があるため、利用するソフトウェアにおけるライセンス規定に従うこと。

第 18 章 業務委託

1. 委託事業者の選定基準

- (1) 情報化推進管理者は、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すること。

2. 契約項目

委託内容に応じて、契約時に次の項目を契約内容に含めること。

- (1) 秘密の保持
- (2) 個人情報保護に関する規定の提出
- (3) 処理施設、処理日程及び作業従事者の通知
- (4) 授受担当従事者の通知
- (5) 目的外利用及び外部提供の禁止
- (6) 例外的に再委託を認める場合には、再委託事業者における情報セキュリティ対策が、他の委託事業者と同等の水準であることを確認し、委託事業者に担保させた上で許可しなければならない。
- (7) 複写及び複製の禁止
- (8) 個人情報の授受
- (9) 個人情報の保管
- (10) 個人情報の返還
- (11) 製品の引き渡し
- (12) 個人情報の搬送
- (13) 個人情報の外部結合による電送等
- (14) 立入検査及び調査
- (15) 事故発生 の 報告
- (16) 不良製品の処分
- (17) 契約の解除及び損害賠償
- (18) 公表措置

3. 確認・措置等

情報化推進管理者は、委託事業者において必要なセキュリティ対策が確保されていることを定期的に確認し、必要に応じ、2の契約に基づき措置を実施すること。

また、委託対象業務の特性上必要がある場合には、外部事業者の不正を防止するため、作業中に職員の立ち会いを義務付けること。

第 19 章 外部サービスの利用

1. 外部サービスの選定

- (1) 情報化推進管理者は、取り扱う情報区分及び取扱制限を踏まえ、外部サービス利用判断基準に従って外部サービスの利用を検討すること。
- (2) 情報化推進管理者は、外部サービスで取り扱う情報区分及び取扱制限を踏まえ、外部サービス提供者の選定基準に従って外部サービス提供者を選定すること。また、以下の内容を含む情報セキュリティ対策を外部サービス提供者の選定条件に含めること。
- (3) 情報化推進管理者は、以下の内容を含む情報セキュリティ対策に関する情報の提供を求め、その内容を確認し、利用する外部サービス（クラウドサービス）が、区が定めたクラウドサービスの利用に関するポリシー（情報セキュリティポリシー）を満たしているか否かを評価すること。
 - ① 外部サービスの利用を通じて区が取り扱う情報の外部サービス提供者における目的外利用の禁止
 - ② 外部サービス提供者における情報セキュリティ対策の実施内容及び管理体制
 - ③ 外部サービスの提供に当たり、外部サービス提供者若しくはその従業員、再委託先又はその他の者によって、区の意図しない変更が加えられないための管理体制
 - ④ 外部サービス提供者の資本関係・役員等の情報、外部サービス提供に従事する者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び調達仕様書による施設の場所や地域の指定
 - ⑤ 情報セキュリティインシデントへの対処方法
 - ⑥ 情報セキュリティ対策その他の契約の履行状況の確認方法
 - ⑦ 情報セキュリティ対策の履行が不十分な場合の対処方法
- (4) 情報化推進管理者は、クラウドサービス事業者と情報セキュリティに関する役割及び責任の分担について確認する。
- (5) 情報化推進管理者は、外部サービスの中断や終了時に円滑に業務を移行するための対策を検討し、外部サービス提供者の選定条件に含めること。
- (6) 情報化推進管理者は、外部サービスの利用を通じて区が取り扱う情報区分等を勘案し、必要に応じて以下の内容を外部サービス提供者の選定条件に含めること。

(注) クラウドサービスの利用前に合意した事項があれば、その内容についてサービス合意書（SLA）に定める。クラウドサービス事業者のサービス利用規約等が変更できない場合は、機密性・完全性・可用性・安全性・個人情報等の扱いに関するクラウドサービス事業者の定める条件を鑑み、その規約内容が区によって受容可能か判断すること。

 - ① 情報セキュリティ監査の受入れ
 - ② サービスレベルの保証
- (7) 情報化推進管理者は、外部サービスの利用を通じて区が取り扱う情報に対して国内法以外の法令及び規制が適用されるリスクを評価して外部サービス提供者を選定し、必要に応じて区の情報が取り扱われる場所及び契約に定める準拠法・裁判管轄を選定条件に含めること。
- (8) 情報化推進管理者は、外部サービス提供者がその役務内容を一部再委託する場合は、再委託

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

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

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

2. 外部サービスの利用に係る調達・契約

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

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

3. 外部サービスを利用した情報システムの導入・構築時の対策

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

- ① 不正なアクセスを防止するためのアクセス制御
- ② 取り扱う情報の機密性保護のための暗号化
- ③ 開発時におけるセキュリティ対策
- ④ 設計・設定時の誤りの防止

(2) 情報化推進管理者は、前項において定める規定に対し、構築時に実施状況を確認・記録すること。

4. 外部サービスを利用した情報システムの運用・保守時の対策

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

- ① 外部サービス利用方針の規定
- ② 外部サービス利用に必要な教育
- ③ 取り扱う資産の管理
- ④ 不正アクセスを防止するためのアクセス制御
- ⑤ 取り扱う情報の機密性保護のための暗号化
- ⑥ 外部サービス内の通信の制御

- ⑦ 設計・設定時の誤りの防止
- ⑧ 外部サービスを利用した情報システムの事業継続
- ⑨ 設計・設定変更時の情報や変更履歴の管理

- (2) 情報化推進管理者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、外部サービスで発生したインシデントを認知した際の対処手順を整備すること。
- (3) 情報化推進管理者は、前各項において定める規定に対し、運用・保守時に実施状況を定期的に確認・記録すること。
- (4) 情報化推進管理者は、情報セキュリティに配慮した運用・保守の手順及び実践がされているか、クラウドサービス事業者に情報を求め、実施状況を定期的に確認及び記録すること。

5. 外部サービスを利用した情報システムの更改・廃棄時の対策

- (1) ネットワーク管理者は、外部サービスの特性や責任分界点に係る考え方を踏まえ、以下を含む外部サービスの利用を終了する際のセキュリティ対策を規定すること。
 - ① 外部サービスの利用終了時における対策
 - ② 外部サービスで取り扱った情報の廃棄
 - ③ 外部サービスの利用のために作成したアカウントの廃棄
- (2) 情報化推進管理者は、前項において定める規定に対し、外部サービスの利用終了時に実施状況を確認・記録すること。
- (3) 情報化推進管理者は、クラウドサービス上で機密性の高い情報（住民情報等）を保存する場合は、機密性を維持するために暗号化するとともに、その情報資産を破棄する際は、データ消去の方法の一つとして暗号化した鍵（暗号鍵）を削除するなどにより、その情報資産を復元困難な状態とすること。

6. 情報区分Ⅰ・Ⅱの情報を取扱わない外部サービスの利用

職員等は、利用するサービスの約款、その他の提供条件等から、利用に当たってのリスクが許容できることを確認した上で、情報化推進管理者の許可を得て利用すること。

第20章 監査

1. 情報セキュリティ監査の準備

- (1) 部会は、情報セキュリティ監査の実施体制を明確にすること。
- (2) 情報セキュリティ監査を定期的に実施すること。
- (3) 必要に応じて、外部監査組織による情報セキュリティ監査を実施すること。
- (4) 情報セキュリティ監査実施にあたって、次の監査計画を作成すること。
 - ① 監査の方針・目的や監査スケジュール・重点テーマ等を記述した全体の監査計画
 - ② 監査対象・監査目的・監査日程・監査実施責任者・被監査部門・監査項目・監査手続等を記述した個別の計画
- (5) 情報セキュリティ監査実施にあたっては、必要に応じて情報システムに精通した要員を確保すること。
- (6) 情報セキュリティ監査の過程で知り得た情報を、監査以外の目的で利用しないこと。

2. 情報セキュリティ監査の実施

- (1) 部会は、情報セキュリティ監査の実施を、区の監査部門等に委任することができる。
- (2) 必要に応じて、情報セキュリティ監査を実施する前に予備調査を実施すること。また、予備調査の結果を受けて監査計画を見直すこと。
- (3) 情報セキュリティ監査は計画に従って行い、監査の証拠となり報告の根拠となるものを収集すること。収集の手段としては次の項目が考えられる。
 - ① 現地環境の調査
 - ② 被監査部門に対するヒアリング
 - ③ 被監査部門の行動の観察
 - ④ 入退記録やアクセスログの証拠の閲覧
 - ⑤ 監査人による情報システム運用作業手順等の実施
 - ⑥ 法制度や手順に関する準拠状況の確認
- (4) 監査結果を裏付けるために証拠を収集し記録すること。
- (5) 監査報告の作成にあたっては、被監査部門と意見交換を行い監査結果の確認を行うこと。

3. 情報セキュリティ監査結果の報告及び改善

- (1) 監査部門は、情報セキュリティ監査の結果について監査報告書を作成すること。
- (2) 監査報告書には、監査計画と対応させ、監査対象、監査目的、監査日程、監査実施者、被監査部門、監査項目、監査手続、報告書作成日程等、実施した監査の概要を記述すること。
- (3) 被監査部門は、監査報告を受けて、監査結果に対する今後の改善策等を明確にするため、改善計画書を監査部門に提出すること。
- (4) 監査部門は、提出を受けた改善計画書を部会に報告するとともに、必要に応じて被監査部門

に改善の勧告を行うこと。

4. 被監査部門の留意点

- (1) 被監査部門は、事前に監査項目を確認すること。
- (2) 監査人の情報システム及びデータへのアクセス権限を、必要最小限の範囲に止めること。
- (3) 監査人が情報システムの操作等を行った場合はそのアクセスログ等を収集し、追跡可能とすること。

5. 委託事業者に対する監査

- (1) 事業者が業務委託を行っている場合、情報化推進管理者は委託事業者（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、定期的に又は必要に応じて監査を行うこと。
- (2) クラウドサービスを利用している場合は、クラウドサービス事業者が自ら定める情報セキュリティポリシーの遵守について、定期的に監査を行うこと。クラウドサービス事業者によるその証拠（文書等）の提示を求める場合は、第三者の監査人が発行する証明書や監査報告書等をこの証拠とすることもできる。

第 21 章 自己点検

1. 実施方法

- (1) 情報化推進管理者は、所管するネットワーク及び情報システムにおける情報セキュリティ実施状況について、毎年度及び必要に応じて自己点検を実施すること。

2. 報告

情報化推進管理者は、所管する情報システムにおける情報セキュリティ実施状況を、部会に報告すること。

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ること。
- (2) 部会は、この点検結果を情報セキュリティポリシー及び関係規程等の見直し、その他情報セキュリティ対策の見直し時に活用すること。

第 22 章 情報セキュリティポリシー及び関係規程等の見直し

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