高松市情報セキュリティ対策基準
（解説入り）

平成29年6月1日

平成31年4月1日改正

改版履歴

版数	改版日	改版項	改版履歴
1.0	2017/6/1	全体	高松市情報セキュリティ対策基準（平成 15 年７月１日施行）の全部を改正する。
1.1	2018/4/1	1.1 2.3. a) 2.4. a)	組織機構の見直しに伴い、一部を改正する。
1.2	2019/4/1	全体	高松市情報セキュリティ対策基準（平成 29 年６月１日施行）の全部を改正する。

目次

1. 対象範囲

1.1. 行政機関の範囲

本対策基準が適用される行政機関は、市長部門、消防局、病院局、教育委員会事務局及び市立小・中学校の事務部門、監査委員、選挙管理委員会、公平委員会、農業委員会及び市議会事務局とする。

1.2. 情報資産の範囲

本対策基準が対象とする情報資産は、高松市が管理する以下の資産とする。

a）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記録媒体

b）全ての行政文書（高松市公文書等の管理に関する条例（平成 25 年高松市条例第２号）第２条第２項で規定する行政文書（※[1]）をいう。）

2. 組織体制

2.1. 最高情報セキュリティ責任者

a）最高情報セキュリティ責任者（以下「ＣＩＳＯ」という。）は、本市の全てのネットワーク、情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有し、市長が任命する。

b）ＣＩＳＯは、自らに属する権限のうち、定例的なもの又は軽微なものについて、統括情報セキュリティ責任者へ事務を委任することができる(※[2])。

c）ＣＩＳＯは、情報セキュリティインシデントに対処するための体制ＣＳＩＲＴを整備し、役割を明確化する。

2.2. 統括情報セキュリティ責任者

a）統括情報セキュリティ責任者は、ＣＩＳＯを補佐し、情報政策部門を担当する局長をもって充てる。

b）統括情報セキュリティ責任者は、本市の全てのネットワークにおける開発、設定の変更、運用、見直し等を行う権限及び責任を有する。

---

[1] 高松市公文書等の管理に関する条例

第２条第２項　この条例において「行政文書」とは、実施機関の職員が職務上作成し、又は取得した文書、図画、写真、マイクロフィルム及び電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られた記録をいう。以下同じ。）であって、当該実施機関の職員が組織的に用いるものとして、当該実施機関が保有しているものをいう。ただし、次に掲げるものを除く。

（1） 官報、白書、新聞、雑誌、書籍その他不特定多数の者に販売することを目的として発行されるもの

（2） 市民の利用に供することを目的として保有しているもの

（3） 特定歴史公文書等

（4） 歴史的若しくは文化的な資料又は学術研究用の資料として特別に管理しているもの（前号に掲げるものを除く。）

[2] 事務を委任できる例は次のとおりとする。

・7.4.(1)例外措置の許可について、期間を延長する許可

・7.5.対策基準に記載のない技術への対応について、既に可否判断した技術と同等の内容の申し出に対する可否判断

c）統括情報セキュリティ責任者は、本市の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。
d）統括情報セキュリティ責任者は、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者に対して、情報セキュリティに関する指導及び助言を行う権限を有する。
e）統括情報セキュリティ責任者は、本市の情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合に、ＣＩＳＯの指示に従い、ＣＩＳＯが不在の場合には自らの判断に基づき、必要かつ十分な措置を行う権限及び責任を有する。
f）統括情報セキュリティ責任者は、本市のネットワーク、情報システム及び情報資産に関する情報セキュリティ実施手順の維持・管理を行う権限及び責任を有する。
g）統括情報セキュリティ責任者は、緊急時等の円滑な情報共有を図るため、ＣＩＳＯ、統括情報セキュリティ責任者、情報セキュリティ責任者、情報セキュリティ管理者、情報システム管理者及び情報システム担当者を網羅する連絡体制を含めた緊急連絡網を整備しなければならない。
h）統括情報セキュリティ責任者は、緊急時にはＣＩＳＯに早急に報告を行うとともに、回復のための対策を講じなければならない。
i）統括情報セキュリティ責任者は、情報資産を取り扱う者（以下「職員等」という。）に対し、定期的に情報セキュリティに関する研修を実施しなければならない。
j）統括情報セキュリティ責任者は、自らに属する権限のうち、定例的なもの又は軽微なものについて、情報政策部門の課長へ事務を委任することができる。

2.3. 情報セキュリティ責任者

a）情報セキュリティ責任者は、市長部局の局長、会計管理者、消防局長、病院局長、教育局長、監査委員事務局長、選挙管理委員会事務局長、農業委員会事務局長、市議会事務局長をもって充てる。
b）情報セキュリティ責任者は、その所管する部局等の情報セキュリティ対策に関する統括的な権限及び責任を有する。
c）情報セキュリティ責任者は、その所管する部局等において所管している情報システムについて、緊急時等における連絡体制の整備、訓練、情報セキュリティ方針の遵守に関する意見の集約及び職員等に対する助言及び指示を行う。

2.4. 情報セキュリティ管理者

a）情報セキュリティ管理者は、市長部門、消防局、病院局、教育委員会

事務局、監査委員事務局、選挙管理委員会事務局、農業委員会事務局及び市議会事務局に属する各課の課長をもって充てる。

b）情報セキュリティ管理者は、その所管する課室等の情報セキュリティ対策に関する権限及び責任を有する。

c）情報セキュリティ管理者は、その所管する課室等において、情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、情報セキュリティ責任者及び統括情報セキュリティ責任者へ速やかに報告を行い、指示を仰がなければならない。

2.5. 情報システム管理者

a）情報システム管理者は、各情報システムを管理する課室等の課長又はこれに準ずる者をもって充てる。

b）情報システム管理者は、その管理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。

c）情報システム管理者は、その管理する情報システムにおける情報セキュリティに関する権限及び責任を有する。

d）情報システム管理者は、その管理する情報システムに係る情報セキュリティ実施手順の維持・管理を行う。

2.6. 情報システム担当者

a）情報システム担当者は、情報システム管理者が指名する者をもって充てる。

b）情報システム担当者は、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・導入、設定の変更、運用、更新等を担当する。

2.7. 高松市ＩＣＴ推進会議

a）本市の情報セキュリティ対策を統一的に行うため、高松市ＩＣＴ推進会議（以下「ＩＣＴ推進会議」という。）において、情報セキュリティ方針等の情報セキュリティに関する重要な事項を検討する。

b）ＩＣＴ推進会議は、監査計画及び監査結果の報告を受け、本市における情報セキュリティ対策の改善計画を検討しなければならない。

2.8. CSIRT の設置・役割

a）ＣＩＳＯは、ＣＳＩＲＴを整備し、その役割を明確化する。

b）ＣＩＳＯは、ＣＳＩＲＴに所属する職員を選任し、その中からＣＳＩＲＴ責任者を置く。また、ＣＳＩＲＴ内の業務統括及び外部との連携等を行う職員を定める。

c）ＣＩＳＯは、情報セキュリティの統一的な窓口を整備し、情報セキュリティインシデントについて部局等より報告を受けた場合には、その状況を確認し、自らへの報告が行われる体制を整備する。

d）ＣＳＩＲＴは、ＣＩＳＯによる情報セキュリティ戦略の意思決定が行われた際には、その内容を関係部署に提供する。
e）ＣＳＩＲＴは、情報セキュリティインシデントを認知した場合には、必要に応じてＣＩＳＯ、総務省、県等へ報告する。
f）ＣＳＩＲＴは、情報セキュリティインシデントを認知した場合は、その重要度や影響範囲等を勘案し、報道機関への通知・公表等の対応を情報セキュリティ管理者又は情報システム管理者等に対し指示する。
g）ＣＳＩＲＴは、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ＣＳＩＲＴの機能を有する部署、外部の事業者等との情報共有を行う。

3. 情報資産の分類と管理方法

3.1. 情報資産の分類

本市における情報資産は、次のとおり分類するものとする。

（１） 重要性分類Ⅰ

a）個人情報に係るセキュリティ侵害があった場合に、市民の生命、健康、財産又はプライバシーに影響を及ぼす可能性のあるもの。
b）市が保有する民間事業者に関する営業情報等に係るセキュリティ侵害があった場合に、事業活動に影響を及ぼす可能性があるもの。
c）公開することを予定していないもの。
d）セキュリティ侵害があった場合に、行政事務の執行等に重大な影響を及ぼす可能性が高いもの。

（２） 重要性分類Ⅱ

セキュリティ侵害があった場合に、行政事務の執行等に影響を及ぼす可能性のあるもの。

（３） 重要性分類Ⅲ

上記（１）及び（２）以外の情報資産

3.2. 情報資産の管理

（１） 管理責任

a）情報セキュリティ管理者は、その所管する情報資産について管理責任を有する。
b）情報セキュリティ管理者は、重要性分類Ⅰの情報資産について、情報資産台帳を作成するものとする(※[3])。【様式第１号】

[3] 情報資産台帳は、簿冊や電磁的記録媒体ごとに、次の項目を記載する。
情報資産名、主な内容、資産の形態（簿冊、USB メモリ、NAS 等）、作成日、重要性分類、保管場所、その他

c）職員等は、情報資産が複製又は伝送された場合には、当該複製又は伝送された情報資産も重要性分類Ⅰ～Ⅲに分類し、管理しなければならない。

（２） 情報資産の分類の表示

職員等は、重要性分類Ⅰ及びⅡに属する情報資産について、情報資産の分類を表示し、必要に応じて取扱制限についても明示する等適切な管理を行わなければならない(※[4])(※[5])(※[6])。

（３） 情報資産の作成

a）職員等は、業務上必要のない情報資産を作成してはならない。

b）情報資産を作成する職員等は、情報資産の作成時に 3.1 の規定により、当該情報資産の分類と取扱制限を定めなければならない。

c）情報資産を作成する職員等は、作成途上の情報資産についても、紛失や流出等を防止するよう努めなければならない。また、情報資産の作成途上で不要となった場合は、当該情報資産を消去しなければならない。

（４） 情報資産の入手

a）他の職員等が作成した情報資産を入手した職員等は、入手元の情報資産の分類に基づいた取扱いをしなければならない。

b）外部の者が作成した情報資産を入手した職員等は､3.1 の規定により、当該情報資産の分類と取扱制限を定めなければならない。

c）情報資産を入手した職員等は、入手した情報資産の分類が不明な場合は、情報セキュリティ管理者に判断を仰がなければならない。

（５） 情報資産の利用

4　重要性分類Ⅰ及びⅡの情報資産については、次のように取り扱う。
・支給している以外のパソコン等での作業の原則禁止
・必要以上の複製及び配付の禁止
・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込み禁止
・情報の送信、情報資産の運搬・提供時における暗号化・パスワード設定や鍵付きケースへの格納
・復元不可能な処理を施しての廃棄
・信頼のできるネットワーク回線の選択
・外部で情報処理を行う際の安全管理措置の規定
・電磁的記録媒体の施錠可能な場所への保管

5 取扱制限を明示する例は、次のとおりとする。
・部外秘
・コピー禁止
・使用後回収
・裏紙使用禁止
・その他、情報セキュリティ管理者が適切と認める表現

6 取扱制限を表示する場所の例は、次のとおりとする。
・ファイル（ファイル名、ファイルの属性（プロパティ）、ヘッダー・フッター等）
・格納する電磁的記録媒体のラベル
・文書の隅

a）情報資産を利用する職員等は、業務以外の目的に情報資産を利用してはならない。

b）情報資産を利用する職員等は、情報資産の分類に応じ、適切な取扱いをしなければならない(※[7])。

c）情報資産を利用する職員等は、電磁的記録媒体に情報資産の分類が異なる情報資産が複数記録されている場合は、Ⅰが含まれている場合はⅠとして、Ⅱ及びⅢのみが含まれている場合はⅡとして、当該電磁的記録媒体を取り扱わなければならない。

（６） 情報資産の保管

a）情報セキュリティ管理者又は情報システム管理者は、情報資産の分類に従って、適切に保管しなければならない(※[8])。

b）情報セキュリティ管理者又は情報システム管理者は、重要性分類Ⅰ及びⅡの情報資産を記録した電磁的記録媒体を長期間保管する場合は、書込禁止の措置を講じなければならない。

c）情報セキュリティ管理者又は情報システム管理者は、市民サービスに重大な影響を及ぼす情報システムについて、バックアップ等により取得した情報資産を記録する電磁的記録媒体を保管する場合は、必要に応じて、自然災害を被る可能性が低い地域に保管しなければならない(※[9])。

d）情報セキュリティ管理者又は情報システム管理者は、重要性分類Ⅰ及びⅡの情報を記録した電磁的記録媒体を保管する場合は、施錠することが可能で、必要に応じて耐火、耐熱、耐水及び耐湿の措置を講じた場所に保管しなければならない。また、必要に応じて暗号化を施して保管しなければならない。

（７） 情報の送信・提供・公表

a）職員等は、電子メール等により重要性分類Ⅰ及びⅡの情報資産を送信又は外部に提供しようとする場合は、情報セキュリティ管理者に許可を得なければならない。【様式第２号】

b）職員等は、電子メール等により重要性分類Ⅰ及びⅡの情報資産を送信又は外部に提供する場合、暗号化又はパスワード設定を行わなければ

---

[7] 適切な取扱いとは 3.2.(2)で制限された取扱いである。

[8] 適切な保管の例は次のとおりであり、重要性分類Ⅰの情報資産を保存する場合は全てを満たす必要がある。
・重要性分類を外部に表示する。
・施錠できる場所に保管する。
・定期的にウィルスチェックを行う。
・情報セキュリティ管理者の許可がある場合を除き、外部に持出さない。
・フラッシュメモリを利用する USB メモリ、SD メモリカード等については、原則として、端末から端末への情報の移動に利用し、長期間の保管は行わない。

[9] 市民サービスに重大な影響を及ぼす情報システムとは、重要性分類Ⅰの情報を取り扱う情報システム（NAS を含む）、高松市業務継続計画の非常時優先業務表（継続業務）で１日未満に業務開始目標時期が設定されている業務で利用する情報システムその他情報システム管理者が必要と認める情報システムをいう。

ならない。

c）情報セキュリティ管理者は、市民に公表する情報資産について、完全性を確保しなければならない(※[10])。

（８） 情報資産の運搬

a）職員等は、重要性分類Ⅰ及びⅡの情報資産を市の施設外へ運搬する場合は、必要に応じて鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置を講じなければならない。

b）職員等は、重要性分類Ⅰ及びⅡの情報資産を市の施設外へ運搬する場合は、あらかじめ情報セキュリティ管理者に許可を得なければならない。【様式第２号】

（９） 情報資産の廃棄

a）職員等は、重要性分類Ⅰ及びⅡの情報資産を記録している電磁的記録媒体を廃棄する場合は、情報資産を復元できないように処置した上で廃棄しなければならない(※[11])。また、廃棄を外部に委託する場合は、委託先が確実に削除又は廃棄をしたことについて、証明書等により確認を行わなければならない。

b）職員等は、重要性分類Ⅰ及びⅡの情報資産の廃棄を行う場合は、行った処理について日時、担当者及び処理内容を記録しなければならない。

c）職員等は、重要性分類Ⅰ及びⅡの情報資産の廃棄を行う場合は、あらかじめ情報セキュリティ管理者の許可を得なければならない。【様式第３号】

4. 情報システム全体の強靭性の向上

4.1. マイナンバー利用事務系

（１） マイナンバー利用事務系と他の領域との分離

マイナンバー利用事務系と他の領域を通信できないようにしなければならない。ただし、マイナンバー利用事務系と外部との通信をする必要がある場合は、通信経路の限定(ＭＡＣアドレス、ＩＰアドレス)及びアプリケーションプロトコル（ポート番号）のレベルでの限定を行わなければならない。なお、外部接続先もインターネット等と接続してはならない。

---

10 完全性の確保とは、審査・決裁等の手段で誤り等を無くすことをいう。

11 情報を復元できないような処置とは次のとおりである。

・物理的破壊・・・ハンマー等で強い衝撃を与えて躯体を変形させる、又は、躯体を穿孔する。

・物理的破壊ができない場合・・・米国 NSA 又は DoD 規格に基づく消去方式をもつ専用ソフトウェアを利用する。

・ファイル削除、論理フォーマット、物理フォーマットでは、データは完全に消去されないので、その状態で廃棄等を行ってはならない。

（２） 情報のアクセス及び持ち出しにおける対策

a）情報のアクセス対策

情報システムが正規の利用者かどうかを判断する認証手段のうち、二つ以上を併用する認証（多要素認証）を利用しなければならない。

b）情報の持ち出し不可設定

原則として、ＵＳＢメモリ等の電磁的記録媒体による端末からの情報持ち出しができないように設定しなければならない。

4.2. ＬＧＷＡＮ接続系

（１） ＬＧＷＡＮ接続系とインターネット接続系の分割

ＬＧＷＡＮ接続系とインターネット接続系は両環境間の通信環境を分離した上で、必要な通信だけを許可できるようにしなければならない。なお、メールやデータをＬＧＷＡＮ接続系に取り込む場合は、次の実現方法等により、無害化通信を図らなければならない。

a）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接続系に転送する方式

b）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

4.3. インターネット接続系

（１） インターネット接続系においては、通信パケットの監視、ふるまい検知等の不正通信の監視機能の強化により、情報セキュリティインシデントの早期発見と対処及びＬＧＷＡＮへの不適切なアクセスの遮断等の情報セキュリティ対策を講じなければならない。

（２） 県内市町のインターネット接続口を集約するかがわ情報セキュリティクラウドに参加するとともに、県等と連携しながら、情報セキュリティ対策を推進しなければならない。

5. 物理的セキュリティ

5.1. サーバ等の管理

（１） 機器の取付け

情報システム管理者は、サーバ等の機器の取付けを行う場合は、当該機器を火災、水害、ほこり、振動、温度、湿度等の影響を可能な限り排除した場所に設置し、容易に取り外せないよう適切に固定する等、必要な措置を講じなければならない(※[12])。

[12] 原則として、サーバ等の機器は、条件を満たす高松市のサーバ室に設置する。それ以外の場所に設置する場合でも、鍵付きのラック内に置き、ラックは床にボルト等で固定する。NAS 等簡易なサーバ等であっても、落下等による損傷のおそれがない場所に設置する。

（２） サーバの冗長化

情報システム管理者は、市民サービスに重大な影響を及ぼす情報システムについて、冗長化等により、システムの運用停止時間を最小限にしなければならない(※[13])。

（３） 機器の電源

a) 情報システム管理者は、施設管理部門と連携し、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なければならない(※[14])。

b) 情報システム管理者は、施設管理部門と連携し、落雷等による過電流に対して、サーバ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(※[15])。

（４） 通信ケーブル等の配線

a) 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、必要に応じて配線収納管を使用する等の措置を講じなければならない(※[16])。

b) 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は、施設管理部門と連携して対応しなければならない。

c) 情報システム管理者は、ネットワーク接続機器を、他者が容易に発見できない場所に設置しなければならない(※[17])。

（５） 機器の定期保守及び修理

a) 情報システム管理者は、サーバ等の機器の定期保守を実施しなければならない。

b) 情報システム管理者は、電磁的記録媒体を内蔵する機器を外部の事業

---

13 機器の冗長化とは、情報システムに障害等が発生した際、直ちに復旧できるよう、サーバ等の機器を複数配置し運用することをいう。概ね次のような方式があり、必要に応じて組み合わせる場合もある。

・コールドスタンバイ：予備機に情報システムを構築しておき、障害時に稼動させて本番機を代替するが、最新のデータは保持しない。機器が複数必要となり、コストを要する。予備機の立上げ時間とデータバックアップからのリカバリが必要で、数分～数時間かかる場合がある。

・ホットスタンバイ：予備機を本番機と同等に稼動して、データも含めて常時バックアップする。機器が複数必要となり、かつ常時同等のデータを保有する仕組みも必要なことから、相当なコストを要する。 瞬時に予備機へ切り替え可能であり、業務への影響は最小限。

14 電源供給の停止に備えるため、次の機器・機能を組合わせること。

・非常用発電装置

・UPS（無停電電源装置、Uninterruptible Power Supply）

・CVCF（定電圧定周波数装置、Constant Voltage Constant）

15 落雷等による異常(雷サージ)電流については、電気系統以外に通信系統から侵入する可能性があるため、屋外ケーブルに接続される電源、通信アース線等の回路に SPD(サージ防護デバイス、Surge Protective Device) を設置すること。

16 配線収納管以外に、OA フロア等も考えられる。

17 容易に発見できない場所とは次のとおりである。

・基幹スイッチ・・・サーバ室等入退室が管理された区域

・フロアスイッチ・・・施錠可能な情報ボックス

・エッジスイッチ・ハブ・・・机の裏面等

者に修理させる場合は、内容を消去した状態で行わせなければならない。内容を消去できない場合は、情報システム管理者は、外部の事業者に故障を修理させるに当たり、修理を委託する事業者との間で、守秘義務契約を締結するほか、秘密保持体制の確認等を行わなければならない。

（６） 市の施設外への機器の設置

情報システム管理者は、重要性分類Ⅰ及びⅡの情報資産を取り扱うサーバ等の機器を市の施設外に設置する場合は、あらかじめＣＩＳＯの許可を得なければならない。また、定期的に当該機器への情報セキュリティ対策状況について確認しなければならない。【様式第 4 号】

（７） 機器の廃棄等

情報システム管理者は、機器を廃棄、リース期間の終了による返却等をする場合は、機器内部の記憶装置から、情報資産を復元できないように処置しなければならない(※[18])。

また、廃棄を外部に委託する場合は、委託先が確実に削除又は廃棄をしたことについて、証明書等により確認を行わなければならない。

5.2. 管理区域（サーバ室等）の管理

（１） 管理区域（サーバ室等）の構造等

a) 管理区域とは、ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための部屋（以下「サーバ室」という。）又は電磁的記録媒体の保管庫をいう。

b) 統括情報セキュリティ責任者は、施設管理部門と連携して、サーバ室から外部に通ずる出入口の設置を必要最小限とし、監視機能等によって許可されていない立入りを防止するよう努めなければならない。

c) 統括情報セキュリティ責任者は、サーバ室内の機器等に、転倒及び落下防止等の耐震対策、防火措置、防水措置等を講じなければならない。

d) 統括情報セキュリティ責任者は、サーバ室に配置する消火薬剤や消防用設備等が、機器等及び電磁的記録媒体に影響を与えないようにしなければならない。

（２） サーバ室の入退室管理等

a) 統括情報セキュリティ責任者は、サーバ室への入退室を許可された者のみに制限し、多要素認証や入退室管理簿の記載等による入退室管理

18 情報を復元できないような処置とは次のとおりである。
・物理的破壊・・・ハンマー等で強い衝撃を与えて躯体を変形させる、又は躯体を穿孔する。
・物理的破壊ができない場合・・・米国 NSA 又は DoD 規格に基づく消去方式をもつ専用ソフトウェアを利用する。
・ファイル削除、論理フォーマット、物理フォーマットでは、データは完全に消去されないので、その状態で廃棄等を行ってはならない。

を行わなければならない。【様式第 5 号】

b）職員等及び外部の事業者は、サーバ室に入室する場合は、身分証明書等を携帯し、求めがあるときは、これを提示しなければならない。

c）統括情報セキュリティ責任者は、重要性分類Ⅰ及びⅡの情報を取り扱うシステムを設置しているサーバ室に、当該情報システムに関連しないコンピュータ（パソコンを含む。）、モバイル端末、通信回線装置、電磁的記録媒体等を許可なく持込ませないようにしなければならない。

（３） 機器等の搬入出

a）統括情報セキュリティ責任者は、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、あらかじめ確認しなければならない。

b）統括情報セキュリティ責任者は、サーバ室の機器等を搬出入するときは、当該職員を立ち会わせなければならない。

5.3. 通信回線及び通信回線装置の管理

a）情報システム管理者は、市の施設内及び市の施設間の通信回線及び通信回線装置を適切に管理しなければならない(※[19])。また、通信回線及び通信回線装置に関連する文書を適切に保管しなければならない(※[20])。

b）情報システム管理者は、外部へのネットワーク接続を行おうとする場合は、できる限り接続ポイントを減らし、事前に統括情報セキュリティ責任者の許可を得なければならない(※[21])。【様式第 6 号】

c）情報システム管理者は、重要性分類Ⅰ及びⅡの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は、必要なセキュリティ水準を検討の上、適切な通信回線を選択しなければならない(※[22])。また、必要に応じて、送受信される情報の暗号化を行わなければならない。

d）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、伝送途上に情報が破壊、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(※[23])。

e）情報システム管理者は、重要性分類Ⅰ及びⅡの情報資産を取り扱う情報システムが接続される通信回線について、継続的な運用を可能とする通信回線を選択しなければならない(※[24])。また、必要に応じて、通信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。

5.4. 職員等のパソコン等の管理

19 通信回線及び通信回線装置の適切な管理とは、回線状態の常時監視や利用状況の定期的な把握である。
20 関連文書の適切な管理とは、定められた場所に規則的に設置し、盗難や毀損を防ぐため施錠等を行うことである。
21 FAX(複合機を含む。)の設置についても、許可を必要とする。
22 適切な回線とは、ダークファイバ、専用線、広域イーサネット、IP-VPN 等の回線サービスである。
23 ネットワークに使用する回線の情報セキュリティ対策とは、VPN 等である。
24 継続的な運用とは、契約等により性能低下や異常によるサービス停止を防ぐことである。

a）職員等は、盗難防止のため、執務室内で使用するパソコンを未使用時には施錠のできる場所へ格納しなければならない。また、電磁的記録媒体は、情報資産を保存す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。

b）情報システム管理者は、執務室等で使用するパソコンが施錠できる場所へ格納できない場合は、ワイヤーによる固定等の物理的措置を講じなければならない。

c）情報システム管理者は、情報システムへのログインに際し、パスワード、IC カード又は生体認証等複数の認証情報の入力を必要とするように設定しなければならない。

d）情報システム管理者は、必要に応じて端末の電源起動時のハードディスクパスワード等を使用しなければならない。

e）情報システム管理者は、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（多要素認証等）を行うよう設定しなければならない。

f）情報システム管理者は、パソコンやモバイル端末等におけるデータの暗号化等の機能を有効に利用しなければならない。端末にセキュリティチップが搭載されている場合、その機能を有効に活用しなければならない。同様に、電磁的記録媒体についても、必要に応じて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。

6. 人的セキュリティ

6.1. 職員等の遵守事項

（１） 職員等の遵守事項

a）情報セキュリティ方針等の遵守

職員等は、高松市情報セキュリティ基本方針及び高松市情報セキュリティ対策基準で構成する高松市情報セキュリティ方針を遵守しなければならない。また、情報セキュリティ対策について不明な点、遵守することが困難な点等がある場合は、速やかに情報セキュリティ管理者の指示を仰がなければならない。

b）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。

c）モバイル端末や電磁的記録媒体等の持出し及び市の施設外における情報処理作業の制限

（ア）情報セキュリティ管理者は、重要性分類Ⅰの情報資産を市の施

設外で処理する場合における安全管理措置を定めなければならない(※[25])。

（イ）職員等は、市の施設外で情報処理業務を行う場合には、情報セキュリティ管理者の許可を得なければならない。【様式第 7 号】

d）職員等は、支給されているもの以外のパソコン、モバイル端末及び電磁的記録媒体等を業務に利用してはならない。ただし、情報セキュリティ管理者が業務上やむを得ないと認め、許可した場合を除く(※[26])。【様式第 8 号】

e）持込みの記録

情報セキュリティ管理者は、支給しているもの以外のパソコン、モバイル端末及び電磁的記録媒体等の持込みについて、記録を作成し、保管しなければならない(※[27])。【様式第 9 号】

f）パソコンにおけるセキュリティ設定変更の禁止

職員等は、パソコンのソフトウェアに関するセキュリティ機能の設定を情報セキュリティ管理者及び情報システム管理者の許可なく変更してはならない(※[28])。【様式第 10 号】

g）机上の端末等の管理

職員等は、パソコン、電磁的記録媒体及び情報資産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を閲覧されることがないように、離席時のパソコンのロック、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切な措置を講じなければならない(※[29])。

h）退職時等の遵守事項

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

（２） 非常勤嘱託職員、臨時的任用職員等への対応

a）情報セキュリティ方針等の遵守

---

25 安全管理措置においては、次のような項目(例)について事前に定めるものとする。
・使用する情報資産
・処理する職員等
・処理を行う場所
・使用する機器等
・機器等の安全管理（画面ロック、パスワード設定、ネットワーク設定、ウイルス対策ソフトの設定等）
・運搬時の安全管理（鍵つきカバンの利用、車内や網棚等への放置禁止等)
・その他、情報セキュリティ管理者が必要と認める項目

26 ネットワークへの接続は、別途 6.1.(15)に基づく申請が必要である。

27 事前に 5.1.(1)d)に基づく許可が必要である。

28 情報政策課が配布するパソコンの場合、情報セキュリティ管理者(自らの課長)と情報システム管理者(情報政策課が管理しているので情報政策課長)両方の許可が必要になる。

29 本文以外、適切な措置の例は、次のとおりである。
・ＩＤ、パスワードのメモを貼り付けない。
・来庁者が無許可で執務室内へ立ち入ることを制限する。
・執務室内が無人になる場合は施錠する。

情報セキュリティ管理者は、非常勤嘱託職員及び臨時的任用職員に対し、採用時に情報セキュリティ方針等のうち、非常勤嘱託職員及び臨時的任用職員が守るべき内容を理解させ、また実施及び遵守させなければならない。

b）契約により業務を行う者への準用

情報セキュリティ管理者は、契約により本市の業務の一部を行わせる者（システム開発において請負契約により協業する者及び事務処理のために派遣契約を基に業務を行う者を含む。）についても、前項に規定する事項と同様とする。

（３） 情報セキュリティ方針等の掲示

情報セキュリティ管理者は、職員等が常に情報セキュリティ方針等を閲覧できるように掲示しなければならない。

（４） 外部の事業者に対する説明

情報セキュリティ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の開発・保守等を外部の事業者に委託する場合は、情報セキュリティ方針等のうち外部の事業者（外部の事業者が再委託をする場合の当該再委託先の事業者を含む。）が守るべき内容の遵守及びその機密事項を説明しなければならない(※[30])。

6.2. 研修・訓練

（１） 研修計画の策定及び実施

a）統括情報セキュリティ責任者は、全ての職員等を対象とした情報セキュリティに関する研修計画の策定を定期的に行わなければならない。

b）統括情報セキュリティ責任者は、新規採用の職員等を対象とする情報セキュリティに関する研修を実施しなければならない。

c）統括情報セキュリティ責任者は、b)に規定する研修を職員等の役割等に応じたものにしなければならない。

d）統括情報セキュリティ責任者は、ＩＣＴ推進会議に対して、職員等の情報セキュリティ研修の実施状況について報告しなければならない。

（２） 緊急時対応訓練

情報セキュリティ責任者は、緊急時における対応を想定した訓練を定期的に実施しなければならない。当該訓練は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の体制、範囲等を定め、また、効果的に実施できるようにしなければならない。

[30] 主に情報システム管理者の遵守事項となるが、情報システムを保有しないでサービスのみ利用する場合、情報セキュリティ管理者も対象となる。

（３） 研修・訓練への参加

職員等は、定められた研修・訓練に参加しなければならない。また、情報セキュリティ管理者は職員等が研修・訓練に参加できるよう配慮しなければならない。

6.3. 情報セキュリティインシデントの報告

（１） 市役所内部からの情報セキュリティインシデントの報告

a) 職員等は、情報セキュリティインシデントを発見した場合は、速やかに情報セキュリティ管理者に報告しなければならない。(※[31])。

b) 報告を受けた情報セキュリティ管理者は、速やかに情報システム管理者及びＣＳＩＲＴに報告しなければならない。

c) 情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、必要に応じて統括情報セキュリティ責任者及び情報セキュリティ責任者に報告しなければならない(※[32])。【様式第 11-1 号】

d) 統括情報セキュリティ責任者は、報告のあった情報セキュリティインシデントについて、特に重要と認める場合は、ＣＩＳＯに報告しなければならない(※[33])。

（２） 市民等外部からの情報セキュリティインシデントの報告

a) 職員等は、市民等外部から本市が管理するネットワーク及び情報システム等の情報資産に係る情報セキュリティインシデントの報告を受けた場合は、情報セキュリティ管理者に報告しなければならない。

b) a)の規定による報告を受けた情報セキュリティ管理者は、速やかにその内容を情報システム管理者及びＣＳＩＲＴに報告しなければならない。

c) a)の規定による報告を受けた情報セキュリティ管理者は、報告のあった情報セキュリティインシデントについて、必要に応じて速やかにその内容を統括情報セキュリティ責任者及び情報セキュリティ責任者に報告しなければならない(※[34])。【様式第 11-1 号】

d) c)の規定による報告を受けた統括情報セキュリティ責任者は、報告のあった情報セキュリティインシデントについて、特に重要と認める場

---

[31] 迅速性が求められるため、第一報は口頭で構わない。概ね次の項目について報告を行う。
・発生した日時、場所、事象、原因、発見者（原因者）
・その時点における被害、影響

[32] 必要に応じてとは、重要性分類Ⅰの情報資産に係る情報セキュリティインシデント及び情報セキュリティ管理者が必要と認める場合である。

[33] ＣＩＳＯへの報告は、次の 2 種類がある。迅速性が求められるため、どちらを優先しても良い。
・5.3.(1)d)及び 5.3.(2)d)に基づく統括情報セキュリティ管理者からの報告は、主に情報セキュリティインシデントの社会的な影響や行政としての対応等である。
・2.8.a)に基づくＣＳＩＲＴからの報告は、主にシステム遮断、通信経路分析等技術的な対応である。

[34] ※33 と同様。

合は、速やかにその内容をＣＩＳＯに報告しなければならない(※[35])。

（３） 情報セキュリティインシデント原因の究明・記録、再発防止等

a) ＣＳＩＲＴは、報告された情報セキュリティインシデントの可能性について状況を確認し、情報セキュリティインシデントであるかの評価を行わなければならない。

b) ＣＳＩＲＴは、情報セキュリティインシデントであると評価した場合、ＣＩＳＯ及び統括情報セキュリティ責任者に速やかに報告しなければならない。

c) ＣＳＩＲＴ又は統括情報セキュリティ責任者は、情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び復旧に係る指示を行わなければならない。

d) ＣＳＩＲＴ及び統括情報セキュリティ責任者は、これらの情報セキュリティインシデント原因を究明し、記録を保存しなければならない。また、情報セキュリティインシデントの原因究明の結果から、再発防止策を検討し、ＣＩＳＯに報告しなければならない。【様式第 11-2 号】

e) ＣＩＳＯは、ＣＳＩＲＴ及び統括情報セキュリティ責任者から、情報セキュリティインシデントについて報告を受けた場合は、その内容を確認し、再発防止策を実施するために必要な措置を指示しなければならない。

6.4. ＩＤ及びパスワード等の管理

（１） ＩＣカードの取扱い

a) 職員等は、自己の管理するＩＣカードに関し、次の事項を遵守しなければならない。

（ア）認証に用いるＩＣカードを、職員等間で共有してはならない。

（イ）業務上必要のない場合は、ＩＣカードを放置してはならない。

（ウ）ＩＣカードを紛失した場合は、速やかに情報システム管理者に報告し、指示に従わなければならない。

b) 情報システム管理者は、ＩＣカードの紛失等の報告があり次第、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。

c) 組織の管理するＩＣカードを利用する場合は、利用が認められた者以外に利用させてはならない。

d) 組織の管理するＩＣカードの取扱いについては、職員等が管理するＩＣカードの規定を準用する。

（２） ＩＤの取扱い

[35] ※34 と同様。

職員等は、自己の管理するＩＤに関し、次の事項を遵守しなければならない。

a）自己が利用しているＩＤは、他人に利用させてはならない。

b）共用ＩＤを利用する場合は、利用が認められた者以外に利用させてはならない。

（３） パスワードの取扱い

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

a）パスワードは、他者に知られないように管理しなければならない。

b）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。

c）パスワードの文字数は十分な数を設定するものとし、文字列は想像しにくいものにしなければならない。

d）パスワードが流出したおそれがある場合は、情報セキュリティ管理者に速やかに報告し、パスワードを変更しなければならない。

e）パスワードは定期的に変更しなければならない。

f）複数の情報システムを扱う職員等は、同一のパスワードをシステム間で用いてはならない。

g）仮のパスワードは、最初のログイン時点で変更しなければならない。

h）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。

i）職員等間でパスワードを共有してはならない。また、共同ＩＤで利用するパスワードを共同ＩＤ利用者以外で共有してはならない。

7. 技術的セキュリティ

7.1. 情報システム及びネットワークの管理

（１） バックアップの実施

情報システム管理者は、情報システムに記録された情報資産について、必要に応じて定期的にバックアップを実施しなければならない。

（２） システム管理記録及び作業の確認

a）情報システム管理者は、その所管する情報システムの運用において実施した作業について、作業記録を作成しなければならない(※[36])。

[36] 受託者が作業する場合は、受託者作成の様式を用いて構わない。
職員等が自ら作業する場合は、概ね次の項目について記録を作成する。
・作業日時
・作業者及び確認者
・作業場所
・作業内容

b）情報システム管理者は、その所管するシステムにおいて、システム変更等の作業を行った場合は、作業内容について記録を作成し、詐取、改ざん等をされないように適切に管理しなければならない(※[37])。

c）重要性分類Ⅰ及びⅡの情報を取り扱う情報システムを担当する情報システム管理者は、契約により操作を認められた外部の事業者がシステム変更等の作業を行う場合に、情報システム担当者を立ち会わせる等、その作業を確認しなければならない。

（３） 情報システム仕様書等の管理

情報システム管理者は、ネットワーク構成図及び情報システム仕様書を、記録媒体にかかわらず、業務上必要とする者以外の者が閲覧したり、紛失等をしたりすることがないよう、適切に管理しなければならない(※[38])。

（４） ログの取得等

a）情報システム管理者は、各種ログ及び情報セキュリティの確保に必要な記録を取得し、一定の期間保存しなければならない。

b）重要性分類Ⅰ及びⅡの情報を取り扱う情報システムにおいて、情報システム管理者は、取得したログを定期的に点検又は分析する機能を設け、必要に応じて悪意ある第三者等からの不正侵入、不正操作等の有無について点検又は分析を実施しなければならない。

（５） 障害記録

情報システム管理者は、職員等からのシステム障害の報告、システム障害に対する処理結果又は問題等を、障害記録として記録し、適切に保存しなければならない(※[39])。

（６） ネットワークの接続制御、経路制御等

a）情報システム管理者は、フィルタリング及びルーティングについて、設定の不整合が発生しないように、ファイアウォール、ルータ等の通信ソフトウェア等を設定しなければならない。

b）情報システム管理者は、不正アクセスを防止するため、ネットワークに適切なアクセス制御を施さなければならない(※[40])。

・その他必要な項目

37 適切な管理の例は次のとおりである。
・バックアップの作成、保存先の書込み禁止
・暗号化、パスワードの設定、保存先のアクセス制御

38 適切な管理の例は次のとおりである。
・保存先のアクセス制御、施錠
・保存媒体のバックアップ作成

39 適切な保存とは、文書管理規程等に基づき、一定期間定められた場所に保存することである。

40 適切なアクセス制御の例は次のとおりである。
・利用目的によるネットワークの分離

（７） 外部の者が利用できるシステムの分離等

情報システム管理者は、市民が利用できるシステムについて、必要に応じて他のネットワーク及び情報システムと物理的に分離する等の措置を講じなければならない。

（８） 外部ネットワークとの接続制限等

a) 情報システム管理者は、その所管するシステムを外部ネットワークと接続等しようとする場合には、統括情報セキュリティ責任者の許可を得なければならない。【様式第 6 号】

b) 情報システム管理者は、接続しようとする外部ネットワークに係るネットワーク構成、機器構成、セキュリティ技術等を詳細に調査し、市が管理する全てのネットワーク、情報システム等の情報資産に影響が生じないことを確認しなければならない。

c) 情報システム管理者は、ウェブサーバ等をインターネットに公開する場合は、内部ネットワークへの侵入を防御するために、ファイアウォール等を外部ネットワークとの境界に設置した上で接続しなければならない。

d) 情報システム管理者は、接続した外部ネットワークのセキュリティに問題が認められ、情報資産に脅威が生じることが想定される場合には、速やかに当該外部ネットワークを物理的に遮断しなければならない。

（９） 複合機のセキュリティ管理

a) 複合機を所管する情報セキュリティ管理者は、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なければならない。

b) 複合機を所管する情報セキュリティ管理者は、複合機の運用を終了する場合、複合機の持つ電磁的記録媒体の全ての情報を抹消又は再利用できないようにする対策を講じなければならない。

（１０） 特定用途機器のセキュリティ管理

特定用途機器を所管する情報セキュリティ管理者は、当該機器について、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。

（１１） 無線ＬＡＮ及びネットワークの盗聴対策

a) 情報システム管理者は、無線ＬＡＮを利用する場合は、解読が困難な暗号化及び認証技術等の対策を講じなければならない。

b) 情報システム管理者は、機密性の高い情報を取り扱うネットワークに

・利用者ごとに各ネットワークへのアクセス権限の付与

ついて、情報の盗聴等を防ぐため、暗号化等の措置を講じなければならない。

（１２）電子メールのセキュリティ管理

a）情報システム管理者は、権限のない利用者により、外部から外部への電子メールの転送（電子メールの中継処理）が行われることがないように、電子メールサーバの設定を行わなければならない。

b）情報システム管理者は、大量のスパムメール等の受信又は送信の検知等情報資産に脅威が生じると想定される場合は、電子メールサーバの運用を停止しなければならない。

c）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。

d）情報システム管理者は、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しなければならない。

e）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外部委託事業者の作業員による電子メールアドレス利用について、外部委託事業者との間で利用方法を取り決めなければならない。

f）情報システム管理者は、職員等が電子メールの送信等により情報資産を無断で外部に持ち出すことが不可能となるように添付ファイルの監視等によりシステム上措置を講じなければならない。

（１３）電子メールの利用制限

a）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。

b）職員等は、複数人に電子メールを送信する場合は、必要がある場合を除き、他の送信先の電子メールアドレスが分からないようにしなければならない(※[41])。

c）職員等は、重要性分類Ⅰ及びⅡの情報資産を含む電子メールを誤送信した場合は、直ちに情報セキュリティ管理者に報告しなければならない(※[42])。

d）職員等は、ウェブで利用することが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てはならない。ただし、業務上やむを得ないと情報セキュリティ管理者が認める場合は、許可を得て利用

[41] 他の送信先の電子メールアドレスがわからない方法とは、bcc 欄へのアドレスの記入である。

[42] 迅速性が求められるため、第一報は口頭で構わない。
概ね次の項目について報告を行う。
・発生した日時、場所、事象、原因、発見者（原因者）
・その時点における被害、影響

することができる。【様式第 10 号】

（１４） 電子署名・暗号化

職員等は、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、暗号化又はパスワード設定等、セキュリティを考慮して送信しなければならない。

（１５） 無許可ソフトウェアの導入等の禁止

a）職員等は、パソコン等に無断でソフトウェアを導入してはならない。

b）職員等は、業務上やむを得ないと情報セキュリティ管理者及び情報システム管理者が認める場合は、許可を得てパソコン等にソフトウェアを導入することができる。なお、導入する際、情報セキュリティ管理者又は情報システム管理者は、ソフトウェアのライセンスを管理しなければならない。【様式第 10 号】

c）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。

（１６） 機器構成の変更の制限

a）職員等は、パソコン等に対し機器の改造、増設又は交換を行ってはならない。

b）職員等は、業務上やむを得ないと情報セキュリティ管理者及び情報システム管理者が認める場合は、許可を得てパソコン等機器の改造、増設又は交換を行うことができる。【様式第 10 号】

（１７） 無許可でのネットワーク接続の禁止

職員等は、情報セキュリティ管理者及び情報システム管理者の許可を得た場合を除き、パソコン、モバイル端末、プリンタ、複合機等ネットワークに接続できる機器をネットワークに接続してはならない。【様式第 10 号】

（１８） 業務以外の目的でのウェブ閲覧の禁止

a）職員等は、業務以外の目的でウェブを閲覧してはならない。

b）情報システム管理者は、職員等のウェブの利用について、明らかに業務に関係のないサイトを閲覧していることを発見した場合は、情報セキュリティ管理者に通知しなければならない。

7.2. アクセス制御

（１） アクセス制御

a）アクセス制御等

情報システム管理者は、その所管するネットワーク又は情報システムごとにアクセスする権限のない職員等がアクセスできないように、システム上制限しなければならない。

b）利用者ＩＤ の取扱い

（ア）情報システム管理者は、利用者の登録、変更、抹消等の情報管理、職員等の異動、出向、退職者に伴う利用者ＩＤの取扱い等の方法を定めなければならない。

（イ）職員等は、業務上必要がなくなった場合は、利用者登録を抹消するよう、情報システム管理者に通知しなければならない。

（ウ）情報システム管理者は、利用されていないＩＤが放置されないよう、人事管理部門等と連携し、点検しなければならない。

c）特権を付与されたＩＤ の管理等

（ア）情報システム管理者は、管理者権限等の特権を付与されたＩＤを利用する者を必要最小限に設定するものとし、当該ＩＤのパスワードの漏えい等が発生しないよう、当該ＩＤ及びパスワードを厳重に管理しなければならない。

（イ）情報システム管理者の特権を代行する者は、当該情報システム管理者が指名する。

（ウ）情報システム管理者は、特権を付与されたＩＤ及びパスワードの変更について、外部の事業者に行わせる場合は、情報システム担当者を立ち会わせなければならない。

（２） 職員等による外部からのアクセス等の制限

a）職員等が外部から内部のネットワーク又は情報システムにアクセスする場合は、当該情報システムを管理する情報システム管理者の許可を得なければならない。【様式第 12 号】

b）情報システム管理者は、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しなければならない。

c）情報システム管理者は、外部からのアクセスを認める場合は、システム上利用者の本人確認を行う機能を確保しなければならない。

d）情報システム管理者は、外部からのアクセスを認める場合は、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。

e）情報システム管理者は、公衆通信回線（公衆無線ＬＡＮ等）の外部通信回線を内部ネットワークに接続することは原則として禁止しなければならない。ただし、やむを得ず接続を許可する場合は、情報セキュリティ確保のために必要な措置を講じなければならない(※[43])。

[43] 必要な措置は、次のとおりである。
・利用者のＩＤ及びパスワード
・生体認証に係る情報等の認証情報及びこれを記録した媒体（ＩＣカード等）による認証
・通信内容の暗号化
・その他情報システム管理者が必要と認める措置

（３） 自動識別の設定

情報システム管理者は、ネットワークで使用される機器について、機器固有情報によって端末とネットワークとの接続の可否が自動的に識別されるようシステムを設定しなければならない。

（４） ログイン時の表示等

重要性分類Ⅰ及びⅡの情報を取り扱う情報システムを担当する情報システム管理者は、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当該情報システムを設定しなければならない(※[44])。

（５） 認証情報の管理

a) 情報システム管理者は、職員等の認証情報を厳重に管理しなければならない(※)。認証情報ファイルを不正利用から保護するため、オペレーティングシステム等で認証情報設定のセキュリティ強化機能がある場合は、これを有効に活用しなければならない。

b) 情報システム管理者は、職員等に対してパスワードを発行する場合は、仮のパスワードを発行し、ログイン後直ちに仮のパスワードを変更させ、又は期限が限定されたパスワードを発行しなければならない。

c) 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。

（６） 特権による接続時間の制限

情報システム管理者は、特権によるネットワーク及び情報システムへの接続時間を必要最小限に制限しなければならない。

7.3. 不正プログラム対策

（１） 情報システム管理者の措置事項

重要性分類Ⅰ及びⅡの情報を取り扱う情報システムの全て及びそれ以外の情報システムで必要と認められるものについて、担当する情報システム管理者は、不正プログラム対策として、次の事項を措置しなければならない。

a) 自らが管理を行うサーバ及びパソコン等の端末について、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、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なければ

[44] 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できるような設定とは、次のとおりである。
・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
・ログイン・ログアウト時刻の表示
・その他情報システム管理者が必要と認める措置

ならない。

b）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たなければならない。

c）不正プログラム対策のソフトウェアは、他のソフトウェアとの整合性を確認した上で、最新の状態に保たなければならない。

d）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等の開発元のサポートが終了したソフトウェアを利用してはならない。

e）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しなければならない。

f）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しなければならない。

g）コンピュータウイルス等の不正プログラム情報を収集し、必要に応じ職員等に対して注意喚起しなければならない。

（２） 職員等の遵守事項

職員等は、不正プログラム対策に関し、次の事項を遵守しなければならない。

a）パソコン等において、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。

b）外部からデータ又は許可を得て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。

c）差出人が不明な場合又は不自然に添付されたファイルを受信した場合は、速やかに削除しなければならない。

d）端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的に実施しなければならない。（※[45]）

e）添付ファイルが付いた電子メールを受信する場合は、不正プログラム対策ソフトウェアでチェックを行わなければならない。（※[45]）インターネット接続系で受信したインターネットメール又はインターネット経由で入手したファイルをＬＧＷＡＮ接続系に取込む場合は無害化しなければならない。

f）情報システム管理者が提供するウイルス情報を、常に確認しなければならない。

g）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、パソコン等の端末に接続されているＬＡＮケーブル

[45] 不正プログラム対策ソフトウェアの設定を変更していなければ、自動的に実施される。

の即時取り外しを行わなければならない。

（３） 専門家の支援体制

重要性分類Ⅰ及びⅡの情報を取り扱う情報システムを担当する情報システム管理者は、実施している不正プログラム対策では不十分な事態が発生した場合に備え、必要に応じて外部の専門家の支援を受けなければならない。

7.4. 不正アクセス対策

（１） 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、次の事項を措置しなければならない。

a) ネットワーク上で利用されていないプロトコルが使用するポート番号を閉鎖しなければならない。

b) 利用されていないネットワーク上のサービスについて、機能を削除又は停止しなければならない。

c) 情報システム管理者は、ＣＳＩＲＴと連携し、監視、通知、外部連絡窓口及び適切な対応等を実施できる体制並びに連絡網を構築しなければならない。

（２） 攻撃への対処

ＣＩＳＯ及び統括情報セキュリティ責任者は、サーバ等に攻撃を受けた場合又は攻撃を受けるリスクがある場合は、システムの停止を含む必要な措置を講じなければならない。また、総務省、県等と連絡を密にして情報の収集に努めなければならない。

（３） 記録の保存

情報システム管理者は、自らが管理するサーバ等に攻撃を受け、当該攻撃が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）違反等の犯罪の可能性がある場合には、ＣＳＩＲＴに報告を行い、攻撃の記録を保存するとともに、警察及び関係機関との緊密な連携に努めなければならない。

（４） 職員等による不正アクセス

情報システム管理者は、職員等による不正アクセスを発見した場合は、当該職員等が所属する課室等の情報セキュリティ管理者に通知しなければならない。

（５） サービス不能攻撃

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。

（６） 標的型攻撃

統括情報セキュリティ責任者及び情報システム管理者は、必要に応じて、標的型攻撃による内部への侵入を防止するための教育、自動再生無効化等の人的対策又は入口対策を講じなければならない。

7.5. 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

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

（２） 不正プログラム等のセキュリティ情報の収集・周知

情報システム管理者は、不正プログラム等のセキュリティ情報を収集し、必要に応じて対応方法について、職員等に周知しなければならない。

（３） 情報セキュリティに関する情報の収集及び共有

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

8. 運用

8.1. 情報システムの監視

a) 重要性分類Ⅰ及びⅡの情報を取り扱う情報システムを担当する情報システム管理者は、セキュリティに関する事案を検知するため、情報システムを常時監視しなければならない(※[46])。

b) 情報システム管理者は、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なければならない。

c) 重要性分類Ⅰ及びⅡの情報を取り扱う情報システムを担当する情報システム管理者は、外部と常時接続するシステムを常時監視しなければならない。

8.2. 情報セキュリティ方針の遵守状況の確認

[46] 本項は、ネットワーク単位で常時監視でも可とする。

（１） 遵守状況の確認及び対処

a) 情報セキュリティ責任者及び情報セキュリティ管理者は、情報セキュリティ方針の遵守状況について確認を行い、問題があると認めた場合には、速やかに統括情報セキュリティ責任者に報告しなければならない。【様式第 11-1 号】

b) 統括情報セキュリティ責任者は、発生した問題について、適切かつ速やかに対処しなければならない。

c) 情報システム管理者は、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方針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切かつ速やかに対処しなければならない。

（２） パソコン及び電磁的記録媒体等の利用状況調査

統括情報セキュリティ責任者及び統括情報セキュリティ責任者が指名した者は、不正アクセス、不正プログラム等の調査のために、職員等が使用しているパソコン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(※[47])。

（３） 職員等の報告義務

a) 職員等は、情報セキュリティ方針に対する違反行為を発見した場合、直ちに情報セキュリティ管理者に報告を行わなければならない。

b) a)の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セキュリティ管理者が判断した場合は、統括情報セキュリティ責任者及び情報セキュリティ責任者への報告等、7.3.(1)に定める緊急時対応計画に従って適切に対処しなければならない。【様式第 11-1 号】

8.3. 侵害時の対応等

（１） 緊急時対応計画の策定

ＣＩＳＯは、情報セキュリティインシデント、情報セキュリティ方針の違反等により情報資産に対するセキュリティ侵害が発生した場合又は発生するおそれがある場合において、連絡、証拠保全、被害拡大の防止、復旧、再発防止等の措置を迅速かつ適切に実施するために、緊急時対応計画を定めておかなければならない。

また、情報システム管理者及び情報セキュリティ管理者は、セキュリティ侵害時に当該計画に従って適切に対処しなければならない。

---

[47] 本項の規定は、次のような流れで処理する。
・情報システム管理者、情報セキュリティ管理者、その他(人事課等)から調査の依頼→情報政策課経由
・情報政策課から統括情報セキュリティ責任者へ報告、調査及び調査者の指名について決裁→調査実施

（２） 緊急時対応計画に盛り込むべき内容

緊急時対応計画には、次の内容を定めなければならない。

a) 関係者の連絡先
b) 発生した事案に係る報告すべき事項
c) 発生した事案への対応措置
d) 再発防止措置の策定

（３） 緊急時対応計画の見直し

統括情報セキュリティ責任者は、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動等に応じ、必要に応じて緊急時対応計画を見直さなければならない。

8.4. 例外措置

（１） 例外措置の許可

情報セキュリティ管理者及び情報システム管理者は、情報セキュリティ方針等を遵守することが困難な状況で、行政事務の適正な遂行を継続するため、遵守事項とは異なる方法を採用し、又は遵守事項を実施しないことについて合理的な理由がある場合には、ＣＩＳＯに協議の上、市長の許可を得て、例外措置を取ることができる。【様式第 13-1 号】

（２） 緊急時の例外措置

情報セキュリティ管理者及び情報システム管理者は、行政事務の遂行に緊急を要する等の場合であって、例外措置を実施することが不可避なときは、（１）によらずに例外措置をとることができる。この場合において、事後速やかにＣＩＳＯ及び統括情報セキュリティ責任者に報告しなければならない。【様式第 13-2 号】

（３） 例外措置の申請書の管理

ＣＩＳＯは、統括情報セキュリティ責任者に例外措置の申請書及び結果を適切に保管させ、定期的に申請状況を確認させなければならない。

8.5. 本対策基準に記載のない技術への対応

a) ＣＩＳＯは、本対策基準に記載のない新たな情報通信技術等に関し、情報システム管理者から利用の申し出があった場合は、必要に応じて情報セキュリティ対策について検討を行い、可否を判断しなければならない。
b) ＣＩＳＯは、a)に基づく検討結果について、情報セキュリティ方針の見直し時に活用しなければならない。

8.6. 法令遵守

職員等は、職務の遂行において使用する情報資産を保護するために、次の法

令のほか関係法令を遵守し、これらに従わなければならない。

a）地方公務員法（昭和 25 年法律第 261 号）
b）著作権法（昭和 45 年法律第 48 号）
c）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）
d）個人情報の保護に関する法律（平成 15 年法律第 57 号）
e）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）
f）サイバーセキュリティ基本法（平成 28 年法律第 31 号）
g）高松市個人情報保護条例（平成 10 年条例第 7 号）

8.7. 懲戒処分等

（１） 懲戒処分

情報セキュリティ方針に違反した職員等及びその監督責任者は、その重大性、発生した事案の状況等に応じて、地方公務員法による懲戒処分の対象とする。

（２） 違反時の対応

職員等の情報セキュリティ方針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。

a）情報セキュリティ管理者は、重大な違反を確認した場合は、統括情報セキュリティ責任者並びに当該職員等が所属する情報セキュリティ責任者及び情報セキュリティ管理者に通知しなければならない。
b）情報システム管理者は、重大な違反を確認した場合は、統括情報セキュリティ責任者並びに当該職員等が所属する情報セキュリティ責任者及び情報セキュリティ管理者に通知しなければならない。
c）統括情報セキュリティ責任者は、重大な違反を確認した場合は、当該職員等が所属する情報セキュリティ責任者及び情報セキュリティ管理者に通知しなければならない。
d）情報セキュリティ管理者の指導によっても改善されない場合は、統括情報セキュリティ責任者は、情報システム管理者に命じて当該職員等のネットワーク又は情報システムを使用する権利を停止し、又は剥奪することができる。この場合において、統括情報セキュリティ責任者は、速やかに職員等の権利を停止し、又は剥奪した旨をＣＩＳＯ並びに当該職員等が所属する情報セキュリティ責任者及び情報セキュリティ管理者に通知しなければならない。

8.8. リスクマネージャーの活用

a）情報セキュリティ対策は、リスクマネジメントの一環でもあることから、リスクマネージャーを情報セキュリティ管理者を補佐する者とし

て位置付け、日頃の情報セキュリティ対策のほか、情報セキュリティ監査実施前の自己点検への対応等に当たらせるものとする。

9. 外部サービスの利用

9.1. 外部委託

（１） 外部の事業者の選定基準

a）情報セキュリティ管理者又は情報システム管理者は、外部の事業者にネットワーク及び情報システムの開発・保守等を委託する場合は、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない(※[48])。

b）情報セキュリティ管理者又は情報システム管理者は、クラウドサービスを利用する場合は、情報の機密性に応じたセキュリティレベルが確保されているサービスを利用しなければならない(※[49])。

（２） 契約項目

情報セキュリティ管理者又は情報システム管理者が、情報システムの運用、保守等を外部委託する場合には、外部の事業者との間で必要に応じて次の情報セキュリティ要件を明記した契約を締結しなければならない。

- 情報セキュリティ方針及び情報セキュリティ実施手順の遵守
- 外部の事業者の責任者、委託内容、作業者、作業場所の特定
- 提供されるサービスレベルの保証
- 外部の事業者にアクセスを許可する情報の種類と範囲､アクセス方法
- 外部の事業者の従業員に対する教育の実施

---

48 外部の事業者の選定に当たっては、情報セキュリティ上、重要な情報資産を取り扱う可能性があることから、技術的能力、信頼性等について考慮して、情報セキュリティ対策が確保されることを確認する必要がある。

また、外部の事業者の選定に当たり、当該事業者の情報セキュリティ水準を評価する際には、国際規格の認証取得状況等を参考にして決定することが望ましい。

なお、外部の事業者の選定条件として仕様等に盛り込む内容としては、例えば次のものがある。

・外部の事業者に提供する情報の委託事業者における目的外使用の禁止
・外部の事業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
・外部委託事業の実施にあたり、外部の事業者の組織又はその従業員、再委託事業者、若しくはその他の者による意図せざる変更が加えられないための管理体制
・外部の事業者の資本関係・役員等の情報、委託事業の実施場所、委託事業従事者の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績及び国籍に関する情報提供
・情報セキュリティ要件の適切な実装
・情報セキュリティの観点に基づく試験の実施
・情報セキュリティインシデントへの対処方法
・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
・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

49 セキュリティレベルが確保されているサービスとは、次のとおりである。

・サービス提供者側のミスや機器の故障等の不測の事態によりデータの消失等の事態が発生しないよう、情報システムや取り扱う情報の重要度に応じたバックアップ等の必要な対策を講じられている。

- 提供された情報の目的外利用及び受託者以外の者への提供の禁止
- 業務上知り得た情報の守秘義務
- 再委託に関する制限事項の遵守
- 委託業務終了時の情報資産の返還、廃棄等
- 委託業務の定期報告及び緊急時報告義務
- 市による監査、検査
- 市による情報セキュリティインシデント発生時の公表
- 情報セキュリティ方針が遵守されなかった場合の規定(損害賠償等)

（３） 確認・措置等

情報セキュリティ管理者又は情報システム管理者は、外部の事業者において必要な情報セキュリティ対策が確保されていることを定期的に確認し、必要に応じ、（２）の契約に基づき措置しなければならない。

9.2. 約款による外部サービスの利用

（１） 約款による外部サービスの利用に係る規定の整備

情報セキュリティ管理者又は情報システム管理者は、必要に応じて次の事項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(※[50])。また、当該サービスの利用において、重要性分類Ⅰ及びⅡの情報資産が取り扱われないように規定しなければならない。

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

（２） 約款による外部サービスの利用における対策の実施

職員等は、利用するサービスの約款、その他提供条件から、利用に当たってのリスクが許容できることを確認した上で約款による外部サービスの利用を申請し、適切な措置を講じた上で利用しなければならない。

9.3. ソーシャルメディアサービスの利用

a）情報セキュリティ管理者は、本市が管理するアカウントでソーシャルメディアサービスを利用する場合、情報セキュリティ対策に関する次の事項を含めたソーシャルメディアサービス運用手順を定めなければならない。

（ア）本市のアカウントによる情報発信が、実際の本市のものである

[50] 約款による外部サービスの利用とは、外部委託等の契約を結ぶことなく、インターネット上のサービス等をサービス提供者が示す約款に基づき利用することであり、次のような例がある。
・Google の各種サービスのうち、特定のＩＤを取得して情報の保管等を行うもの（メール、カレンダー、ドライブ、マップ等)。

ことを明らかにするために、本市の自己管理ウェブ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行うこと。

（イ）パスワードや認証のためのコード等の認証情報及びこれを記録した媒体（ＩＣカード等）等を適切に管理する等の方法で、不正アクセス対策を行うこと。

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

c）利用するソーシャルメディアサービスごとの責任者を定めなければならない。

10. 評価・見直し

10.1. 監査

（１） 実施方法

ＣＩＳＯは、統括情報セキュリティ責任者に、情報セキュリティ方針の遵守状況等について、毎年度及び必要に応じて監査を行わせなければならない。

（２） 監査を行う者の要件

a）統括情報セキュリティ責任者は、監査を実施する場合は、監査人を指名し、監査を実施させなければならない。

b）統括情報セキュリティ責任者は、監査人に、監査及び情報セキュリティに関する専門知識を教育しなければならない。

（３） 監査実施計画の立案及び実施への協力

a）統括情報セキュリティ責任者は、監査を行うに当たって、監査計画を立案し、ＩＣＴ推進会議に報告しなければならない。

b）被監査者は、監査の実施に協力しなければならない。

（４） 外部の事業者に対する監査

統括情報セキュリティ責任者は、外部の事業者に委託している場合、外部の事業者が再委託をする場合の当該再委託先の事業者も含めて、情報セキュリティ方針の遵守について監査を必要に応じて行わなければならない。

（５） 報告

統括情報セキュリティ責任者は、監査結果を取りまとめ、ＣＩＳＯ及びＩＣＴ推進会議に報告するものとする。

（６） 保管

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

（７） 監査結果への対応

ＣＩＳＯは、監査結果を踏まえ、指摘事項を所管する情報セキュリティ管理者及び情報システム管理者に対し、当該事項への対処を指示しなければならない。

（８） 情報セキュリティ方針及び関係規程等の見直し等への活用

ＩＣＴ推進会議は、監査結果を情報セキュリティ方針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。

10.2. 自己点検

（１） 実施方法

a) 情報システム管理者は、その所管するネットワーク及び情報システムについて、自己点検を実施しなければならない。

b) 情報セキュリティ管理者は、職員等に情報セキュリティ方針の遵守状況を、自己点検させなければならない。

（２） 自己点検結果の活用

職員等は、自己点検の結果に基づき、自己の権限の範囲内で改善を図らなければならない。

10.3. 情報セキュリティ方針及び関係規程等の見直し

ＩＣＴ推進会議は、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、情報セキュリティ方針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。

附　則

この対策基準は、平成１５年７月１日から施行する。

附　則

この対策基準は、平成１７年１０月１４日から施行する。

附　則

この対策基準は、平成２４年４月１日から施行する。

附　則

この対策基準は、平成２７年８月３１日から施行する。

附　則

この対策基準は、平成２９年６月１日から施行する。

附　則

この対策基準は、平成３０年４月１日から施行する。

附　則

この対策基準は、平成３１年４月１日から施行する。