藤沢市図書館情報セキュリティポリシー

＜　対策基準　＞

基本編・詳細編

文書の新規発行／改定

版数	改正／施行年月日	文書の新規制定／改定内容	承認者	作成部署	文書整理番号
00	改正:平成　　年　　月　　日 施行：平成　24 年　4 月　1 日	新規制定	永井 生涯学習 部部長	総合市民 図書館	
01	改正：平成　　年　　月　　日 施行：平成　　年　　月　　日				
02	改正：平成　　年　　月　　日 施行：平成　　年　　月　　日				
03	改正：平成　　年　　月　　日 施行：平成　　年　　月　　日				
04	改正：平成　　年　　月　　日 施行：平成　　年　　月　　日				
05	改正：平成　　年　　月　　日 施行：平成　　年　　月　　日				
06	改正：平成　　年　　月　　日 施行：平成　　年　　月　　日				

（注意）

(1) 本文書を一部改定したときは、当該一部改正に係る部分（影響するページ）を加除方式により差し替え、最新化する。

(2) 本文書を全部改定したときは、改正前の本文書を各所管において速やかに撤去し、廃棄するものとする。

(3) 文書の新規制定／改定内容は、制定及び改定の都度、当該制定及び改定の履歴を記載したものと差し替える。

目　次

＜基本編＞

＜基本編＞

1. 目的

藤沢市図書館が保有する情報資産の機密性、完全性及び可用性を維持・向上するための対策（以下「情報セキュリティ対策」という。）を、遵守すべき行為や判断等の基準を統一的なレベルで定め、統合的、体系的かつ具体的に取りまとめるため、『藤沢市図書館情報セキュリティポリシー＜対策基準＞』を策定する。

本対策基準は藤沢市図書館が保有する情報資産に関する業務に携わる職員、非常勤職員及び臨時職員（以下「職員等」という。）並びに図書館業務委託事業者の職員（以下「委託スタッフ」という。）並びに外部委託事業者及びその職員等に対し、情報セキュリティの維持、強化を促すものである。

『藤沢市図書館情報セキュリティポリシー』の体系を以下とする。

・『藤沢市図書館情報セキュリティポリシー＜基本方針＞』
・『藤沢市図書館情報セキュリティポリシー＜対策基準＞基本編・詳細編』
・実施手順書類

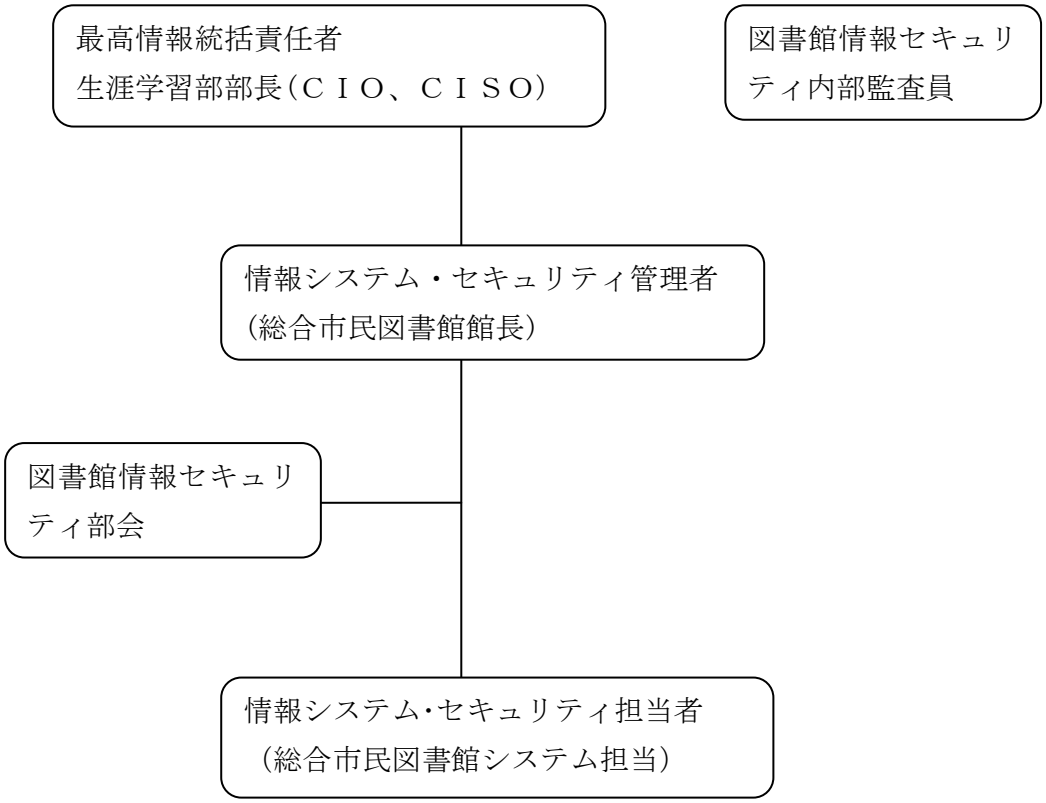
2. 対象範囲

本対策基準は、藤沢市図書館が所有する情報資産のすべてを対象とする。また、藤沢市個人情報の保護に関する条例（平成 15 年藤沢市条例第 7 号）（以下「条例」という。）第４条第１項第２号に規定する個人情報の取扱いについては、総合市民図書館の責務とする。

3. 組織及び体制

藤沢市図書館の情報資産について、情報セキュリティ推進体制を組織し、情報セキュリティ対策を推進する。

3.1. 情報セキュリティ推進体制



3.2. 情報セキュリティ組織員の構成員と役割の概要

組織名称	構成員・担当者	役割の概要
最高情報統括責任者（ＣＩＯ、ＣＩＳＯ）	教育委員会生涯学習部部長	情報セキュリティ運営の最高責任を持つ
図書館情報セキュリティ委員会	委員長：最高情報統括責任者 副委員長：情報統括責任者 委員：生涯学習課の職員から選出	情報セキュリティ推進に関する重要な意思決定をする
情報統括責任者	教育委員会生涯学習部生涯学習課参事	最高情報統括責任者を補佐し、情報セキュリティ対策に関する計画・実行・検証などに責任を持つ
情報システム・セキュリティ管理者	藤沢市総合市民図書館館長	図書館における情報セキュリティに関する責任を持つ
情報システム・セキュリティ担当者	藤沢市総合市民図書館システム担当者	情報システム･セキュリティ管理者を補佐し、館内における情報セキュリティ対策を推進する

4. 定義

(1)情報システム

総合市民図書館及び南市民図書館・辻堂市民図書館・湘南大庭市民図書館に設置されているコンピュータシステム（ネットワーク、ハードウェア及びソフトウェア）及び記録媒体で構成され、処理を行う仕組みをいう。

(2)情報資産

組織が持つ情報と情報システム及びこれらが適切に保護され機能するために必要な要件の総称をいう。

(3)情報セキュリティ

情報資産に関し機密を保持し（機密性)、正確性及び完全性を維持し（完全性)、定められた範囲内において利用可能な状態（可用性）にすることをいう。

(4)記録媒体

記録媒体とは、次に掲げるものをいう。

①磁気式、光学式、半導体メモリ等、電子データとして情報を記録する媒体をいう。

②ハードディスク等コンピュータ内において磁気データとして情報を記録する媒体、ハードディスクが取外し不可能な場合や取外していない場合は、当該コンピュータ自体も記録媒体という。

③情報をバーコード等復元又は解読可能な形式で印字した紙等媒体をいう。

(5)端末

端末とは以下をいう。

①業務系端末

②情報系端末

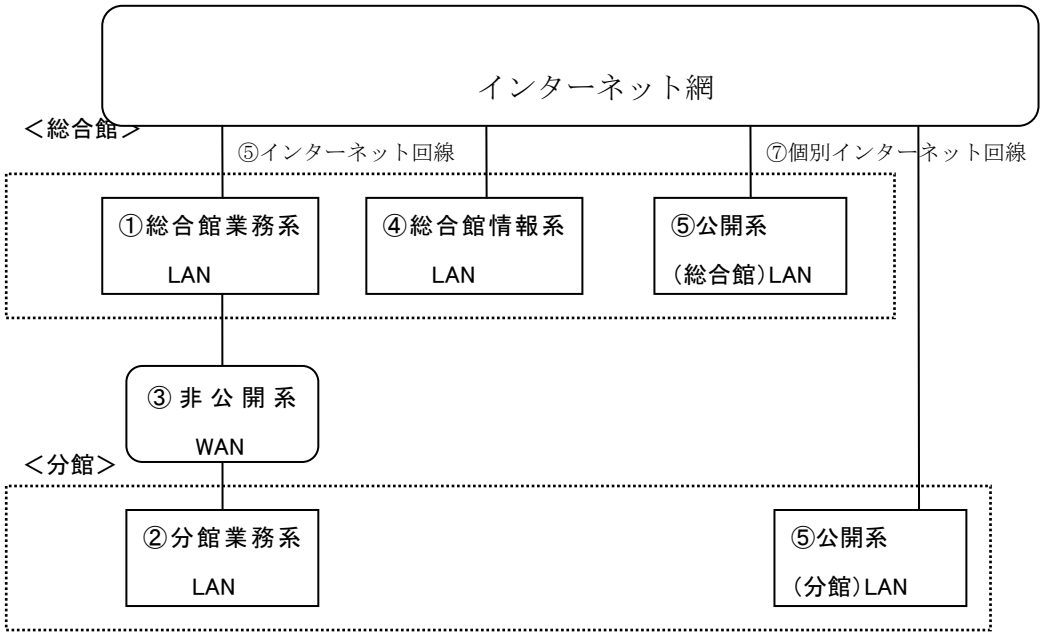
(6)ネットワーク

ネットワークとは、藤沢市図書館が所掌する情報通信網、その構成機器（ハードウェア及びソフトウェア）及び記録媒体で構成され、処理を行う仕組みをいう。

①総合館業務系 LAN：総合市民図書館内に構成され、資料貸出記録等の重要な個人情報等を保存した各種情報システムが稼動するサーバ及びその端末が接続されたLANで、十分なセキュリティ対策を施した上で、インターネットと接続されている。情報系LAN,非公開系WAN、公開系LANとは、物理的又は論理的に独立したネットワークである。

②分館業務系 LAN：南市民図書館・辻堂市民図書館・湘南大庭市民図書館内に構成され、総合館業務系 LAN 上の資料貸出記録等の重要な個人情報等へのアクセス可能な端末が接続されたLANで、非公開系WANを経由して総合館業務系LANと接続されている。また、非公開系WAN及び総合館業務系LANを経由して十分なセキュリティ対策を施した上で、インターネットと接続

されている。総合館情報系 LAN、非公開系 WAN、公開系 LAN とは、物理的又は論理的に独立したネットワークである。
③非公開系 WAN：総合館業務系 LAN と分館系 LAN を経由する WAN で、インターネット、総合館業務系 LAN、公開系 LAN とは、物理的又は論理的に独立したネットワークである。
④総合館情報系 LAN：総合市民図書館内に構成され、図書館からの情報発信に必要な情報等を保存した各種情報システムが稼働するサーバが接続された LAN で、十分なセキュリティ対策を施した上で、インターネットと接続された LAN をいう。
⑤公開系 LAN：各館内に構成され、総合目録検索、大学図書館蔵書検索等のインターネット利用のためのインターネット端末が接続された LAN、又はインターネット利用のための専用 LAN をいう。
⑥インターネット回線：インターネット接続事業者の回線と総合館業務系 LAN および総合館情報系 LAN に設置された当該接続設備で、インターネット接続事業者の回線は総合市民図書館にのみ用意される。
⑦個別系インターネット回線：インターネット接続事業者の回線と各館公開系 LAN に設置された当該接続設備で、インターネット接続事業者の回線は各館にそれぞれ用意され、異なる拠点での共有は行わない。インターネット回線とは、物理的かつ論理的に独立したネットワークである。
⑧相関図



(7)装置

装置とは、次に掲げるものをいう。

①フロッピーディスク等の記録媒体を用いてコンピュータの補助及び拡張機能を実現するためにコンピュータに接続又は内蔵された機械。

②耐震や防塵等の適切なコンピュータ機器の設置､又はネットワークの敷設を行うための設備。

③コンピュータ機器（ネットワークを含む)。

5. 情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うことをいう。

6. 情報資産への脅威

本対策基準を策定する上で、脅威の発生度合や発生した場合の影響を考慮すると、特に認識すべき脅威は、次のとおりである。

(1)部外者による故意の不正アクセス、不正操作によるデータ又はプログラムの持出し、盗聴、改ざん及び消去、機器又は媒体の盗難、サービス妨害等。

(2)職員等並びに委託スタッフ並びに外部委託事業者及びその職員等による意図しない操作､故意の不正アクセス、不正操作によるデータ又はプログラムの持出し、盗聴、改ざん及び消去、機器又は媒体の盗難及び許可されていない端末の接続によるデータの漏えいや情報システムの停止等。

(3)コンピュータウィルス、地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止。

(4)著作権法等の法令に反するソフトウェアの保持、複製、利用等。

(5)インターネット等の公共ネットワークにおける公的秩序に反する発言等による社会的信用の低下等。

7. 情報セキュリティ対策

6.で示した脅威から情報資産を保護するために、次の情報セキュリティ対策を講ずるものとする。

(1)物理的セキュリティ対策

情報システムを有する施設への不正な立ち入り、及び情報資産の損傷、妨害等から保護するために物理的な対策を講ずる。

(2)人的セキュリティ対策

情報セキュリティに関する権限及び責任を定め、職員等並びに委託スタッフに『藤沢市図書館情報セキュリティポリシー』の内容を周知徹底する等、十分な教育及び啓発をするための対策を講じる。

(3)技術及び運用におけるセキュリティ対策

外部からの不正なアクセス等から情報資産を適切に保護するため、情報資産へのアクセスの制御、ネットワーク管理等の技術面対策、また、システム開発等の外部委託、ネットワークの監視、『藤沢市図書館情報セキュリティポリシー』の遵守状況確認等の運用面での対策、及び緊急事態が発生した際の迅速な対応を可能とするため、危機管理対策を講ずる。

8. 情報セキュリティ実施手順の策定

本対策基準を遵守して情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要がある。そのため、情報資産に対する脅威及び情報資産の重要度に対応する本対策基準の基本的な要件に基づき、藤沢市図書館が所掌する情報資産の情報セキュリティ実施手順を策定する。

9. 情報セキュリティ監査の実施

『藤沢市図書館情報セキュリティポリシー』が遵守されていることを検証するため、必要に応じて監査を実施する。

10. 評価及び見直しの実施

図書館情報セキュリティ委員会による監査の結果等により、『藤沢市図書館情報セキュリティポリシー』に定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するため、必要に応じて『藤沢市図書館情報セキュリティポリシー』の見直しを実施する。

11. 『藤沢市図書館情報セキュリティポリシー』に定めのない事項

『藤沢市情報セキュリティポリシー』に定めのない事項について、緊急に対処又は解決すべき事案が発生した場合には、所属長等の指示に従い適切な措置を講じなければならない。当該事案の緊急性によりやむを得ない場合に限り、図書館情報セキュリティ委員会に事後報告とすることができる。

12. 『藤沢市図書館情報セキュリティポリシー』の公開

『藤沢市図書館情報セキュリティポリシー＜基本方針＞』及び『藤沢市図書館情報セキュリティポリシー＜対策基準＞基本編･詳細編』は公開とするが、各情報セキュリティ実施手順は、公にすることにより藤沢市の図書館運営に重大な支障を及ぼす恐れがあるため、非公開とする。

13. その他特記事項

図書館業務委託事業者については、辻堂市民図書館および湘南大庭市民図書館の貸出・返却業務、利用者管理業務、予約業務など図書館利用者の個人情報を含む情報資産を扱う図書館業務の一部を委託している。そのため、本図書館の情報資産を保護するためには、その職員である委託スタッフによる情報資産の機密性、完全性及び可用性の維持･向上が必要不可欠となる。以上から、委託スタッフについては、藤沢市と業務委託をしている事業者の職員ではあるが、『藤沢市図書館情報セキュリティポリシー』のうち遵守すべき内容を職員等と同等に設定する。

目　次

＜**詳細編**＞

＜詳細編＞

1. 目的

本対策基準で職員等並びに委託スタッフが従うべき情報セキュリティ対策を規定する。なお、本対策基準のうち、遵守が困難な場合については、情報システム・セキュリティ管理者の承認を得ることにより、除外又は代替策を適用することを可能とする。ただし、情報システム・セキュリティ管理者は、必要に応じて最高情報統括責任者の承認を得なければならない。

2. 情報の分類と管理

2.1. 情報の管理責任

(1)管理責任

情報は､情報システム･セキュリティ管理者が､情報管理責任者として管理責任を有する。

(2)利用者の責任

情報を利用する者は、情報の分類に従い利用する責任を有する。

(3)重要性の効力

情報が複製され又は伝送された場合には､当該複製され又は伝送された情報も分類に基づき管理しなくてはならない。

2.2. 情報の分類と管理方法

(1)情報の分類

対象となる情報は、各々の情報の機密性、完全性及び可用性を踏まえ、次の重要性分類に従って分類する。

重　要　性　分　類
Ⅰ　個人情報及び情報セキュリティ侵害が住民の生命、財産等へ重大な影響を及ぼす情報。
Ⅱ　公開することを予定していない情報及び情報セキュリティ侵害が行政事務の執行等に重大な影響を及ぼす情報。
Ⅲ　外部に公開する情報のうち、情報セキュリティ侵害が、行政事務の執行等に微妙な影響を及ぼす情報。
Ⅳ　上記以外の情報。

(2)情報の入力管理

①情報システム・セキュリティ管理者は、入力データの正確性を確保し、不正なデータ入力（更新及び削除を含む。）を防止するために、入力データの入力手引書等を定め、職員等並びに委託スタッフは当該入力手引書に従いデータ入力を実施しなくてはならない。

②情報システム・セキュリティ管理者は、データの種類、入力者等を事後に確認することができるように手順を定めなくてはならない。

③情報システム・セキュリティ管理者は、不正な入力等を防止するために、適切な措置を講じなければならない。

④職員等並びに委託スタッフは、不正な入力等を防止するために、端末を離れる場合にはログオフする等適切な措置を講じなければならない。

(3)情報の管理方法

①情報の分類の表示

情報システム・セキュリティ管理者は、情報システムで扱う情報については、部外者が当該情報の重要性の識別を容易に認識することができないよう留意しつつ、ファイル名、記録媒体等に情報の分類が分かるように表示をする等、適切な管理を行わなければならない。

②情報の管理及び取扱い

- 情報システム・セキュリティ管理者は、情報についてそれぞれの分類に従い、アクセス権限を定めなければならない。
- 職員等並びに委託スタッフは、情報を複製した物を保管場所に移動する場合、又は当該保管場所からバックアップのために情報システムの設置箇所に戻す場合、並びに業務上必要な場合においては、情報システム・セキュリティ管理者の許可を得た上での移動、及び外部への持出し又は送付をしなければならない。また、許可を得た上で情報を持ち出す場合は、外部から見えないようにする等、適切な措置を講じなければならない。
- 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。
- 職員等並びに委託スタッフは、業務上必要のない情報を作成してはならない。
- 職員等並びに委託スタッフは、私物パソコンでの作業及び私物記録媒体を利用してはならない。

(4)記録媒体の管理

①情報システム・セキュリティ管理者は、取り外し可能な記録媒体を適切に管理しなければならない。

②職員等並びに委託スタッフは、誤操作による改ざんや消去を防ぐため、必要に応じて記録媒体の書込み禁止措置を行った上で保管しなければならない。

③職員等並びに委託スタッフは、重要かつ復元が困難な情報は別の記録媒体に複製し、必要に応じて自然災害を被る可能性が低い地域に別途保管しなければならない。

④職員等並びに委託スタッフは、重要な情報を記録した記録媒体は、耐火、耐熱、耐水及

び耐湿の対策を講じた施錠可能な場所に保管しなければならない。

⑤情報システム・セキュリティ管理者は、記録媒体を移動しようとする場合は、あらかじめ職員等並びに委託スタッフ又は適切な業者を選定し、複製の禁止及び記録媒体の物理的保護に関する規則に従わなければならない。

(5)記録媒体の処分

①職員等並びに委託スタッフは、記録媒体が不要となった場合においては、当該記録媒体に含まれる重要な情報について、記録媒体の初期化等、情報を復元することができないよう処置を行った上で当該記録媒体を廃棄しなければならない。

②職員等並びに委託スタッフは、重要な情報を記録した記録媒体を廃棄しようとするときは、情報システム・セキュリティ管理者の許可を得なければならない。重要な情報を記録した記録媒体の廃棄に関しては、処理の日時、内容及び担当者を記録しておかなければならない。

3. 情報システム及びネットワークの分類

対象となるネットワーク及び情報システムは、各々の機密性、完全性及び可用性を踏まえ、次の重要性分類に従って分類し、重要度に応じて管理を実施する。

重　要　性　分　類		
A	特に重要なシステム	個人情報及び住民の生命、身体、財産及びプライバシーに直接重大な影響を及ぼす情報を取扱い、それらの処理を実行する情報システム及びネットワークであり、機密性、完全性及び可用性に特に配慮する必要がある情報システム及びネットワーク。
B	重要なシステム	Aに該当しない行政運営執行上重要な情報システムであり、機密性、完全性及び可用性に配慮する必要がある情報システム及びネットワーク。
C	その他のシステム	A及びBに該当しない情報システム及びネットワーク。

4. ハードウェアの分類

対象となるハードウェアは、各々の機密性、完全性及び可用性を踏まえ、次の重要性分類に従って分類し、重要度に応じて管理を実施する。

重　要　性　分　類		
A	重要なハードウェア	総合館、分館に設置されたコンピュータやネットワーク機器等

		で、重要な情報が記録されているもの、又はその障害等に起因して重要な情報システムが停止すること等により、行政運営等に重大な影響を及ぼす恐れがあるもの。
B	その他のハードウェア	Aに該当しないハードウェア。

5. 物理的セキュリティ

5.1. サーバ等

(1)装置の取付け等

①情報システムの取付けを行う場合には、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、容易に取り外すことができないよう、適切な措置を施さなければならない。また、オペレーション及び保守のためのスペースも併せて確保しなければならない。

②情報システム・セキュリティ管理者等の管理者権限を有する者以外の者が容易に接触しないように、原則として施錠可能な室等に設置し、その鍵を厳重に管理しなければならない。

③図書館運営上停止してはならない情報システムが稼動するサーバについては、可能な限り冗長化等の措置を講じなければならない。

④情報システム・セキュリティ管理者、及び契約により操作を認められた外部委託事業者以外の者が容易に操作することができないように、利用者 ID、パスワードの設定等の措置を講じなければならない。

- 付与する ID の権限は、操作のために必要最低限のものとし、最上位の権限の ID は特に厳重に管理し、定期的に変更する等の措置を講ずること。
- 不要となった ID は速やかに削除すること。
- パスワードは可能な限り複雑なものにすること。この場合において、OS 等のソフトウェアが辞書掲載語等の解読が比較的容易な語句によるパスワードの設定を禁止する機能を有する場合は、当該機能を活用すること。
- パスワードの再利用はしないこと。

⑤サーバについては、フロッピーディスク等の入出力装置を施錠により保護可能なものとし、取り外しが可能な入出力装置等は、取り外しておかなければならない。鍵は、情報システム・セキュリティ管理者が厳重に管理しなければならない。

⑥配線等から放射される電磁波により、重要な情報が外部に漏えいすることがないよう、情報システム及びネットワーク単位で、必要に応じて対策措置を講じなければならない。

⑦全てのネットワーク内には原則として無線ＬＡＮのアクセスポイントを収容してはならない。また、情報ネットワーク・セキュリティ管理者の許可において無線ＬＡＮのアクセスポイントを収容する場合には、ＭＡＣアドレス認証、通信の暗号化、アクセスポイントの隠蔽等の情報漏えい防止策を実施しなければならない。

(2)電源

①重要なハードウェアに該当するサーバ機器等の電源については、当該機器を適切に停止するまでの間に十分な電力を供給する容量の予備電源を備え付けなくてはならない。

②落雷等による過電流に対して、サーバ等の重要な機器を保護するための措置を講じなければならない。

(3)配線

①配線は、傍受、損傷等を受けることがないように必要な措置を講じなければならない。庁舎間を接続するために屋外に敷設される配線については、部外者が容易に接触することができないように、敷設経路を空中又は地中にし、強固な配管素材を用いる等、特に配慮しなければならない。

②配線は、敷設後の管理及び運用作業に支障を来たさないように必要な措置を講じなければならない。

③EPS や MDF 等は必ず施錠し、鍵の受払履歴を記録しなければならない。

④主要な箇所の配線については、損傷等に関し定期的に点検を行わなければならない。

⑤ネットワーク接続口（ハブのポート等）は、他の者が容易に発見又は接続することができない場所に設置しなければならない。

⑥情報システム・セキュリティ管理者、及び契約により操作を認められた以外の者が配線を変更し、又は追加ができないように必要な措置を講じなければならない。

(4)点検

情報システム・セキュリティ管理者は、サーバ等の設置環境及び設備を定期的に点検し、その安全性を確認しなければならない。

(5)敷地外への機器の設置

情報システム・セキュリティ管理者は、庁舎の敷地外にサーバ等の機器を設置する場合には、定期的に機器を設置している室内の状況を確認しなければならない。

(6)機器の廃棄

情報システム・セキュリティ管理者は、パソコン等情報が格納されている機器が不要になった場合やリース返却等を行う場合には、ハードディスクから情報を消去し、全ての情報の復元が困難な状態にしてから廃棄しなければならない。

5.2. 管理区域

(1)管理区域

対象となる区域は、各々の機密性、完全性及び可用性を踏まえ、次の重要性分類に従って分類し、重要度に応じて管理を実施する。

重　要　性　分　類		
A	特に重要な区域	重要なシステム、ネットワーク基幹機器が設置されている領域。 重要なシステムの運用・管理を行う領域。
B	重要な区域	重要なシステムの運用・管理を行う業務室。 重要な図書館運営を行う業務室。
C	その他の区域	A、Bに該当しない領域。

管理区域では、以下の対策を講じなければならない。

①管理区域の機器類の配置は、緊急時に職員等並びに委託スタッフが円滑に避難することができるよう配慮しなければならない。

②重要機能室については、その表示を行わない等、所在を明らかにしないようにすること。

(2)管理区域の入退室管理

分類された区域の重要性に応じて、各管理区域に入退室対策を実施する。

重　要　性　分　類		
A	特に重要な区域	鍵等により強固な安全対策を講じる。 許可された職員等及び許可された部外者のみの入室を可能とする。
B	重要な区域	職員等並びに委託スタッフの入室を可能とする。 部外者の立ち入りは、職員等が監視する。
C	その他の区域	部外者の立ち入りは、職員等並びに委託スタッフが監視する。

情報システム・セキュリティ管理者は、管理区域の入退室管理に責任を持ち、職員等並びに委託スタッフ及び部外者は、身分証明書等を携帯し、求めにより提示しなければならない。

(3)機器等の搬入場所

①管理区域に機器等を搬入する場合は、あらかじめ当該機器等の既存情報システムに対する安全性について職員等による確認を行わなければならない。

②機器等の搬入には職員等並びに委託スタッフが同行する等、必要な措置を講じなければならない。

5.3. ネットワーク

(1)ネットワーク構成

①外部へのネットワーク接続は、必要最小限のものに限定し、できる限り接続ポイントを減らさなければならない。

②可用性及び将来的な拡張性に優れたネットワーク構成とすることについて、十分に配慮しなければならない。

③ネットワークの体系は、障害箇所（障害が発生している特定の支線等）を隔離し、障害による影響範囲を極少化するよう配慮しなければならない。

④サブネットワーク分割(論理的ネットワーク分割)等を有効的に利用しなければならない。

⑤WAN 回線は、原則として常時接続専用サービスのみとするが、業務形態の必要に応じてダイアルアップサービスを利用することができる。この場合において、ダイアルアップサービスを利用するときは、特定電話番号間通話固定サービスを付加契約するとともに、必要に応じて暗号化等についても配慮しなければならない。

(2) ネットワーク機器

①多数の回線を収容している等、当該ネットワーク機器の停止等が広い範囲に影響を及ぼすものについては、二重化及び代替機を用意し、代替機能が確実に機能することを試験する等の措置を講じなければならない。

②ネットワーク機器の取付けを行う場合には、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、容易に取り外すことができないよう、適切な措置を講じなければならない。

③ネットワーク機器を特に重要な区域以外に設置する場合には、床清掃（水害）や職員等並びに委託スタッフの不用意な接触等から保護するための対策を講じなければならない。

5.4. 職員等並びに委託スタッフの端末

(1) 端末は、盗難防止のため、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。

(2)配線等から放射される電磁波により、重要な情報が外部に漏えいすることがないように、情報システム及びネットワーク単位で、必要に応じた対策措置を講じなければならない。

(3)職員等並びに委託スタッフは、長時間端末を離れる場合は、端末の電源を切断又はログオフ、若しくはスクリーンセーバーのパスワード保護機能等を利用して、不正利用を防止しなければならない。

(4)職員等並びに委託スタッフは、全ての端末を図書館外に持ち出してはならない。業務上端末を図書館外に持ち出す必要があるときは、情報システム・セキュリティ管理者の承認を

得なければならない。この場合においては、情報システム・セキュリティ管理者は、持出の記録を一定期間保管しなければならない。

(5)職員等並びに委託スタッフは、図書館外において端末を使用する場合は、盗難、盗み見等に十分配慮するとともに、図書館外に持ち出すデータは情報システム・セキュリティ管理者の許可を得た必要最小限のものとする。また、盗難等の事故が発生した場合においても、情報の漏えいが生じないように、必要に応じて暗号化等の対策を講じなければならない。

(6)個人情報を取り扱う端末には、部外者に見られないように、原則として画面にプライバシーフィルター等を装着しなければならない。

5.5. 屋外に設置する機器等

無線通信機器等屋外に設置する装置は、盗難、部外者の接触、落雷等に十分配慮して適切な措置を講じなければならない。

6. 人的セキュリティ

6.1. 役割・責任

(1)最高情報統括責任者（ＣＩＯ、ＣＩＳＯ）

最高情報統括責任者は、『藤沢市図書館情報セキュリティポリシー』の対象範囲における全ての情報資産の情報セキュリティを統括する。

(2)情報システム・セキュリティ管理者（コンピュータ利用管理者）

①最高情報統括責任者を補佐しなければならない。

②ネットワークにかかる開発、設定の変更、運用、更新等を行う。

③ネットワークに係る情報セキュリティの維持及び向上を行う。

④ネットワーク及び情報システムに関し、サーバ等ハードウェア及び配線等の構成情報を把握し、管理しなければならない。当該構成情報に変更等が生じた場合には、速やかに当該変更等に係る箇所を修正するとともに、修正履歴を記録しなければならない。

⑤ネットワーク及び情報システムに関し、ソフトウェアの配布状況、ライセンス等の情報を把握し管理しなければならない。また、当該情報に変更等が生じた場合は、速やかに当該変更等に係る箇所を修正するとともに、修正履歴を記録しなければならない。

⑥情報資産を侵害され又は侵害の恐れがある場合には、最高情報統括責任者の指示に従い、必要かつ十分なすべての措置を行う。最高情報統括責任者が不在の際は自らの判断に基づき措置を行う。

⑦情報資産に関する情報セキュリティ実施手順の維持及び管理を行う。

⑧情報資産に関する連絡体制の構築、『藤沢市図書館情報セキュリティポリシー』の遵守に関する意見の集約並びに職員等対する研修、訓練、助言及び指示を行う

⑨図書館業務委託事業者に対して、『藤沢市図書館情報セキュリティポリシー』の遵守に関する必要な教育研修を定期的、継続的に行うように促し、委託スタッフが職員等と同様の知識や意識を持つよう配慮する。

(3)図書館情報セキュリティ部会

情報セキュリティの維持管理を統一的な視点で行うため、情報セキュリティに関する重要な事項を審議し、決定する。

(4)情報システム・セキュリティ担当者

情報システムに関し、情報システム・セキュリティ管理者の指示等に従い、開発、設定の変更、運用、更新等の作業を行う。

(5)職員

①情報セキュリティ対策の遵守義務

- 『藤沢市図書館情報セキュリティポリシー』に定めた事項を遵守しなければならない。
- 情報セキュリティ対策における実施すべき対策の判別が困難な場合、及び遵守することが困難な場合等には、速やかに情報システム・セキュリティ管理者に相談し、指示等を受けなければならない。

②その他

- 使用する端末及び記録媒体、情報が印刷された文書等については、第三者に使用されること、又は情報システム・セキュリティ管理者の許可なく当該記録媒体に記録された情報を閲覧されることがないように、離席時の端末のロックや記録媒体、文書等が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。
- 情報システム・セキュリティ管理者の許可を得ずに、端末及び記録媒体等を執務室から図書館外へ持ち出してはならない。また、許可を得た上で情報を持ち出す場合には、外部から見えないようにする等、適切な措置を講じなければならない。
- 配布された端末又は記録媒体は、図書館が管理していない機器等に接続してはならない。やむを得ず接続する場合には、図書館のセキュリティレベルと同等であることを確認し、情報システム・セキュリティ管理者の許可を得なければならない。
- 私物のパソコン及び記録媒体を図書館内に持ち込み、業務で使用してはならない。
- 私物のパソコン及び記録媒体に業務情報を入れてはならない。
- 異動、退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を他に漏らしてはならない。

(5)非常勤職員及び臨時職員

①情報セキュリティ対策の遵守義務

- 『藤沢市図書館情報セキュリティポリシー』に定めた事項を遵守しなければならない。
- 情報セキュリティ対策における実施すべき対策の判別が困難な場合、及び遵守することが困難な場合等には、速やかに情報システム・セキュリティ管理者に相談し、指示等を受けなければならない。

②その他

- 使用する端末及び記録媒体、情報が印刷された文書等については、第三者に使用されること、又は情報システム・セキュリティ管理者の許可なく当該記録媒体に記録された情報を閲覧されることがないように、離席時の端末のロックや記録媒体、文書等が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。
- 情報システム・セキュリティ管理者の許可を得ずに、端末及び記録媒体等を執務室から図書館外へ持ち出してはならない。また、許可を得た上で情報を持ち出す場合には、外部から見えないようにする等、適切な措置を講じなければならない。
- 配布された端末又は記録媒体は、図書館が管理していない機器等に接続してはならない。やむを得ず接続する場合には、図書館のセキュリティレベルと同等であることを確認し、情報システム・セキュリティ管理者の許可を得なければならない。
- 私物のパソコン及び記録媒体を図書館内に持ち込み、業務で使用してはならない。
- 私物のパソコン及び記録媒体に業務情報を入れてはならない。
- 退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を他に漏らしてはならない。

(6) 委託スタッフ

①情報セキュリティ対策の遵守義務

- 『藤沢市図書館情報セキュリティポリシー』に定めた事項を遵守しなければならない。
- 情報セキュリティ対策における実施すべき対策の判別が困難な場合、及び遵守することが困難な場合等には、速やかに図書館業務委託事業者が定める責任者に相談しなければならない。
- 図書館業務委託事業者責任者が定める責任者は委託スタッフより情報セキュリティ対策に関する相談を受けた場合は、速やかに情報システム・セキュリティ管理者からの指示等を受け、委託スタッフにその指示等を伝えなければならない。

②その他

- 使用する端末及び記録媒体、情報が印刷された文書等については、第三者に使用されること、又は情報システム・セキュリティ管理者の許可なく当該記録媒体に記録された情報を閲覧されることがないように、離席時の端末のロックや記録媒体、文書等が

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。

- 情報システム・セキュリティ管理者の許可を得ずに、端末及び記録媒体等を執務室から図書館外へ持ち出してはならない。また、許可を得た上で情報を持ち出す場合には、外部から見えないようにする等、適切な措置を講じなければならない。
- 配布された端末又は記録媒体は、図書館が管理していない機器等に接続してはならない。やむを得ず接続する場合には、図書館のセキュリティレベルと同等であることを確認し、情報システム・セキュリティ管理者の許可を得なければならない。
- 私物のパソコン及び記録媒体を図書館内に持ち込み、業務で使用してはならない。
- 私物のパソコン及び記録媒体に業務情報を入れてはならない。
- 退職等により業務を離れる場合には、利用していた情報資産を返却しなければならない。また、その後も業務上知り得た情報を他に漏らしてはならない。

(7)外部委託に関する管理

①外部委託先の選定基準

- 情報システム・セキュリティ管理者は、外部委託先の選定にあたり、委託内容に応じた情報セキュリティ対策が確保されることを確認しなければならない。
- 情報システム・セキュリティ管理者は、情報セキュリティマネジメントシステム（ＩＳＭＳ）の認証取得状況等を参考にして、事業者を選定しなければならない。

②契約項目

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

- 『藤沢市図書館情報セキュリティポリシー』の遵守
- 委託先の責任者、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
- 従業員に対する教育の実施（必要な資格等）
- 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
- 藤沢市による監査、検査
- 事故発生時の藤沢市からの公表
- 『藤沢市図書館情報セキュリティポリシー』が遵守されなかった場合の規定（損害賠

償等）

③その他

・ 外部委託事業者から書面による再委託の承諾願いを受け、再委託を受諾する場合には、外部委託先事業者と同等のセキュリティレベルであることを確認するとともに、再委託先の経営状況を的確に把握し、導入前の検査要求事項等を契約事項として定めなければならない。

・ 情報システム・セキュリティ管理者は、作業中に身分証明書の提示を事業者に求めるとともに、契約で定められた資格を有する者が作業に従事していることの確認を行わなければならない。

6.2. 研修・訓練

(1)最高情報統括責任者（ＣＩＯ、ＣＩＳＯ）

①すべての職員等並びに委託スタッフ及び関係する者に対し、『藤沢市図書館情報セキュリティポリシー』についての啓発をしなければならない。

②情報システム・セキュリティ管理者が立案する情報セキュリティに関する研修計画について報告を受け、その計画について把握しなければならない。

③緊急時対応を想定した訓練の実施状況について報告を受け、その内容等について把握しなければならない。

(2)情報システム・セキュリティ管理者

①最新の技術動向を把握するための研修を受けなければならない。

②最高情報統括責任者を含めたすべての職員等に対する情報セキュリティに関する研修計画を立案し、図書館情報セキュリティ部会の承認を得るとともに、定められた研修・訓練を受講させ、その実施状況の報告を図書館情報セキュリティ部会に行わなければならない。

③緊急時対応を想定した訓練を定期的に実施しなければならない。訓練計画は、ネットワーク及び各情報システムの規模等を考慮し、訓練実施の範囲等を定めるとともに、より効果的に当該訓練を実施することができるような計画を立てるものとする。

④図書館業務委託事業者に対して情報セキュリティに関する研修計画の立案およびその計画の実施を促し、研修計画と研修・訓練の実施状況について報告を受け、その内容について図書館情報セキュリティ部会に了承を得なければならない。

(3)情報システム・セキュリティ担当者

①最新の技術動向を把握するための研修を受けなければならない。

②情報システム・セキュリティ管理者が定めた研修計画および訓練計画の立案、実施に関して、情報システム・セキュリティ管理者の指示等に従い、作業に従事しなければならない。

(4)職員等

すべての職員等は、情報システム・セキュリティ管理者によって定められた研修・訓練に参加しなければならない。

(5)委託スタッフ

委託スタッフは、図書館業務委託事業者によって定められた研修・訓練に参加しなければならない。

6.3. 事故・欠陥に対する報告

(1)職員等は、情報セキュリティに関する事故、又はシステム上の欠陥若しくは誤動作を発見した場合には、速やかに情報システム・セキュリティ管理者に報告し、情報システム・セキュリティ管理者の指示に従い必要な措置を講じなければならない。

(2)委託スタッフは、情報セキュリティに関する事故、又はシステム上の欠陥若しくは誤動作を発見した場合には、速やかに図書館業務委託事業者の責任者に報告しなければならない。

(3)図書館業務委託事業者は、情報セキュリティに関する事故、又はシステム上の欠陥若しくは誤動作の報告を受けた場合は、責任者を通じて速やかに情報システム・セキュリティ管理者に報告し、情報システム・セキュリティ管理者の指示に従い必要な措置を講じなければならない。

(2) 情報システム・セキュリティ管理者は、職員等並びに図書館業務委託事業者から報告があった情報セキュリティに関する事故等について、最高情報統括責任者に報告しなければならない。また、情報システム・セキュリティ管理者は、効果的な再発防止策を検討するために、事故等の発生から対応までの記録を作成しておかなければならない。

(3)情報システム・セキュリティ管理者は、住民等外部からの事故等の報告があった場合も同様な処理を行うとともに、必要に応じて住民等外部から報告を受けるための窓口を設置し、当該窓口への連絡手段を公表しなければならない

6.4. 利用者 ID の管理

(1)職員等並びに委託スタッフは利用者 ID を秘密にし、照会等には一切応じてはならない。

(2)職員等並びに委託スタッフの利用者 ID は、容易に目視可能な場所に放置、貼付等をしてはならない。

(3)職員等並びに委託スタッフ間では原則として利用者 ID を共有してはならない。ただし、情報システム・セキュリティ管理者及び情報システム・セキュリティ担当者が使用する、管理及び運用の管理者 ID はこの限りでない。

(4)職員等は担当業務の変更等で利用者 ID が不要になった場合には、速やかに情報システム・セキュリティ管理者に報告しなければならない。情報システム・セキュリティ管理者は、当該報告があったときは、速やかに当該職員等の利用者 ID を抹消又は無効にしなければならない。

(5)委託スタッフは担当の変更等で利用者 ID が不要になった場合には、速やかに図書館業務委託事業者の責任者に報告しなければならない。この報告があった場合は、図書館業務委託事業者は速やかに情報システム・セキュリティ管理者に報告しなければならない。情報システム・セキュリティ管理者は、当該報告があったときは、速やかに当該職員等の利用者 ID を抹消又は無効にしなければならない。

(6)職員等の利用者 ID 若しくはパスワードを他人が利用していることを発見した場合、若しくはその疑いがある場合には、速やかに情報システム・セキュリティ管理者に報告しなければならない。情報システム・セキュリティ管理者は、当該報告があったときは、速やかに利用者 ID 又はパスワードの変更等の対処を実施しなければならない。

(7)委託スタッフの利用者 ID 若しくはパスワードを他人が利用していることを発見した場合、若しくはその疑いがある場合には、速やかに図書館業務委託事業者の責任者に報告しなければならない。この報告があった場合は、図書館業務委託事業者は速やかに情報システム・セキュリティ管理者に報告しなければならない。情報システム・セキュリティ管理者は、当該報告があったときは、速やかに利用者 ID 又はパスワードの変更等の対処を実施しなければならない

6.5. パスワードの管理

(1)職員等並びに委託スタッフは、パスワードを秘密にして照会等には一切応じてはならない。

(2)職員等並びに委託スタッフは、パスワードを容易に目視可能な場所に放置、貼付等をしてはならない。

(3)職員等並びに委託スタッフは、パスワードの長さを十分な長さとし、文字列は容易に想像できるものであってはならない。

(4)職員等並びに委託スタッフは、パスワードを定期的に変更し、古いパスワードを再利用してはならない。

(5)職員等並びに委託スタッフは、パスワードが流出した恐れがある場合には、速やかに情報システム・セキュリティ管理者に報告するとともに、パスワードを変更しなければならない。

(6)職員等並びに委託スタッフは、仮のパスワードを最初のログイン時点で変更しなければ

ならない。

(7)職員等並びに委託スタッフは、端末にパスワードを記憶させてはならない。必要に応じて暗号化等を行うことによって、他者がパスワードを読むことができないような措置を講じなければならない。

(8)職員等並びに委託スタッフ間でパスワードを共有してはならない。

(9)職員等は、業務上の担当変更等でパスワードが不要になった場合には、速やかに情報システム・セキュリティ管理者に報告しなければならない。情報システム・セキュリティ管理者は、当該報告があった場合には、速やかに当該職員等のパスワードを抹消又は変更しなければならない。

(10)委託スタッフは、業務上の担当変更等でパスワードが不要になった場合には、速やかに図書館業務委託事業者の責任者に報告しなければならない。この報告があった場合は、図書館業務委託事業者は速やかに情報システム・セキュリティ管理者に報告しなければならない。情報システム・セキュリティ管理者は、当該報告があった場合には、速やかに当該委託スタッフのパスワードを抹消又は変更しなければならない。

6.6. インターネットの利用

(1) 職員等並びに委託スタッフは、インターネットの利用に関し、次の事項を順守しなければならない。

①暴力等の社会的モラルに反するウェブページにアクセスしてはならない。ただし、情報ネットワーク・セキュリティ管理者の許可を受けたものはこの限りでない。

②重要な情報、重要な情報と思われる情報、及び社会的モラルに反する情報を掲示板等に記載してはならない。また、一般的に信頼性が認知されていないウェブページに記載してはならない

③ウェブページ上の情報又はプログラムの引用、複製等を行う場合には、当該情報の著作権等に十分注意し、著作権等に違反する行為を行ってはならない。

(2)情報システム・セキュリティ管理者及び情報システム・セキュリティ担当者等を除く職員等並びに委託スタッフは、インターネットの利用に関し、次の事項を順守しなければならない。

①情報ネットワーク・セキュリティ管理者の許可を得た場合を除き、ファイル及びプログラムのダウンロード、又はアップロードをしてはならない。

②情報システム・セキュリティ管理者が定めたソフトウェア及びバージョン以外のブラウザ等、インターネット用ソフトウェアの使用及び設定の変更をしてはならない

6.7. 電子メールの利用

(1)職員等並びに委託スタッフは、電子メールの利用に関し、次の事項を遵守しなければならない。

①業務上必要な場合を除き、重要な情報、重要な情報と思われる情報又は社会的モラルに反する情報を電子メールによって送信してはならない。

②重要な情報を送信する場合は、必要最小限の宛先とするよう注意しなくてはならない。

③自動転送機能を用いて、藤沢市図書館が管理していない端末に電子メールを転送してはならない。ただし、業務上必要な場合において情報システム・セキュリティ管理者が許可した場合はこの限りでない。

④複数人に電子メールを送信する場合には、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。

⑤重要な電子メールを誤送信した場合には、速やかにその旨を情報システム・セキュリティ管理者に報告しなければならない。

(2)情報システム・セキュリティ管理者及び情報システム・セキュリティ担当者等を除く職員等並びに委託スタッフは、電子メールの利用に関し、次の事項を順守しなければならない。

①情報システム・セキュリティ管理者が定めたソフトウェア及びバージョン以外の電子メール用ソフトウェアを使用してはならない。

②電子メールアカウントの設定を変更してはならない。

7. 技術的セキュリティ

7.1. コンピュータ及びネットワークの管理

(1)アクセス記録の取得等

①情報システム・セキュリティ管理者は、各種アクセス記録及び情報セキュリティの確保に必要な記録をすべて取得し、一定の期間保存しなければならない。

②情報システム・セキュリティ管理者は、アクセス記録等が窃取、改ざん、消去等をされないよう、必要な措置を講じなければならない。

③情報システム・セキュリティ管理者は、必要に応じてアクセス記録等を分析し、監視するとともに、外部記録媒体にバックアップを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

①情報システム・セキュリティ管理者は、管理するシステムの運用において実施した作業について、作業記録を作成しなければならない。

②情報システム・セキュリティ管理者は、管理するシステムにおいて実施したシステム変更等の作業内容の記録について、窃取、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。

(3)障害記録

情報システム・セキュリティ管理者は、職員等から報告のあった障害の情報及びシステムの障害に対する処理、問題等の記録を残し、保存しなければならない。

(4)情報システム仕様書等の管理

①情報システム・セキュリティ管理者は、ネットワーク構成図、情報システム仕様書等について、記録媒体に関わらず、業務上必要とする者のみが閲覧することができる場所に保管しなければならない。また、構築に際して事業者に外部委託する場合は、当該事業者と守秘義務について契約を結ばなければならない。

②情報システム・セキュリティ管理者は、ネットワーク構成図、情報システム仕様書等について統一の様式を定め、職員等並びに委託スタッフ及び外部委託事業者に対し、当該様式を遵守するよう周知しなければならない。

③情報システム・セキュリティ管理者は、ネットワーク又は情報システムの構成等に変更及び追加した場合には、速やかに当該変更又は追加があった箇所を修正し、変更履歴を記録しなければならない。

④情報システム・セキュリティ管理者は、情報システム仕様書等を廃棄する場合には、裁断等適切な措置を講じなければならない。

(5)情報及びソフトウェアの交換

①情報システムに関する情報又はソフトウェアを他団体と交換する場合は、その取扱いに関する事項をあらかじめ定め、情報システム・セキュリティ管理者の許可を得なければならない。

②情報システム・セキュリティ管理者は、他団体とソフトウェアを交換する場合は、当該ソフトウェアの使用許諾内容を十分に確認しなければならない。また、当該使用許諾内容に抵触する恐れがある場合には、ソフトウェアの交換を中止させなければならない。

(6) バックアップ

①情報システム・セキュリティ管理者は、ディレクトリサーバ等に記録された情報について、冗長化措置にかかわらずその重要度に応じて期間を設定し、定期的にバックアップをとらなければならない。

②情報システム・セキュリティ管理者は、取得したバックアップ用ファイル及び変更履歴を厳重に管理し、保管しなければならない。

(7)メール

①情報システム・セキュリティ管理者は、外部から外部へのメール転送（メールの中継処理）を不可能とする等、情報システム全般に悪影響を与えないような設定を講じなければならない。

②情報システム・セキュリティ管理者は、外部に送信するメールの容量の上限を別途定め周知するとともに、設定等により当該上限を超えるメールの送信をすることができないようにしなければならない。

③職員等並びに委託スタッフは、メールの自動転送機能を用いて、図書館が管理していない端末に職場のメールを転送してはならない。

(8)ディレクトリサーバ

ディレクトリサーバは、館単位もしくは事前に図書館情報セキュリティ部会で承認された組織単位で構成し、情報システム・セキュリティ管理者及び情報システム・セキュリティ担当者及び管理者が指定する者以外はフォルダ及びファイルを閲覧し、使用することができないような措置を講じなければならない。

(9)外部の者が利用するシステム

外部の者が利用するシステムについては、必要に応じて他の情報システムと物理的又は論理的に分離する等、情報セキュリティ対策について特に強固な対策を講じなければならない。

(10)情報システムの入出力データ

①情報システムに入力されるデータは、適切なチェックを行い、それが正確であることを確実にするための対策を講じなければならない。

②エラー又は故意の行為により情報が改ざんされる恐れがある場合は、これを検出する措置及び、必要に応じて情報の修復を行う措置を講じなければならない。

③情報システムから出力されるデータについては、保存された情報の処理が正しく反映された上で出力されるように、必要な措置を講じなければならない。

(11)電子署名及び暗号化

①外部へ送るデータが完全であることを担保することが必要な場合には、定められた電子署名方法及び暗号化方法を使用して送信しなければならない。

②暗号化の実施及び暗号の鍵の管理については、定められた方法で管理しなければならない。

(12)勤務時間内での業務目的以外のウェブページ閲覧の禁止

①職員等並びに委託スタッフは、勤務時間内に業務目的以外での情報システムへのアクセス、メールの使用及びウェブページを閲覧してはならない。職員等並びに委託スタッフが勤務時間内に業務目的以外でウェブページを閲覧した場合においては、情報ネットワーク・セキュリティ管理者は、当該職員等並びに委託スタッフが所属する課等の情報シ

ステム・セキュリティ管理者に通知し、適切な措置を求めなければならない。改善されない場合においては、情報ネットワーク・セキュリティ管理者は、当該職員等並び委託スタッフのウェブページ閲覧に関する権利を停止することができる。

②情報システム・セキュリティ管理者は、職員等並びに委託スタッフのウェブページ閲覧に関する権利を停止したときは、その旨を図書館情報セキュリティ部会に報告しなければならない。

(13)標準ソフトウェアの削除等、無許可ソフトウェアの導入等の禁止

①職員等並びに委託スタッフが、業務上の必要から次の行為をする場合には、情報システム・セキュリティ管理者の許可を得なければならない。

- 標準実装以外のアプリケーション・ソフトウェアの端末へのインストール
- 標準実装アプリケーション・ソフトウェアの端末からのアンインストール
- 端末の設定の変更

②情報システム・セキュリティ管理者は、職員等並びに委託スタッフが容易にアプリケーション・ソフトウェアの削除、追加等をすることができないようにするため、OS の設定等の対策を講じなければならない。

③アプリケーション・ソフトウェアのインストール及び端末の設定変更は、可能な限りシステムにより監視しなければならない。

④情報システム・セキュリティ管理者は、ソフトウェアのライセンス管理をしなければならない。

(14)機器構成の変更

①職員等並びに委託スタッフは、端末について改造又は機器の増設及び交換を行ってはならない。

②職員等並びに委託スタッフは、端末について業務を遂行するために機器の増設又は交換を行う必要がある場合は、情報システム・セキュリティ管理者の許可を得なければならない。

③職員等並びに委託スタッフは、モデム等の機器を増設して他の環境へのネットワーク接続を行う場合、又は外部からのアクセスを可能とする仕組みを構築する場合は、情報システム・セキュリティ管理者の許可を得なければならない。

④情報システム・セキュリティ管理者は、職員等並びに委託スタッフが容易に機器の増設等を実施することができないようにするため、OS の設定等の対策を講じなければならない。

(15)無線 LAN 及びネットワークの盗聴対策

①情報システム・セキュリティ管理者は、無線 LAN の利用を認める場合、解読が困難な暗

号化及び認証技術の使用を義務づけなければならない。

②情報システム・セキュリティ管理者は、機密性の高い情報を扱うネットワークについて、情報の盗聴等を防ぐために暗号化等の措置を講じなければならない。

(16) その他

職員等並びに委託スタッフが利用することができるプロトコルは、業務上必要最小限のものとする。

7.2. アクセス制御

(1)利用者登録

①情報システム・セキュリティ管理者は、利用者の登録、変更及び抹消、登録情報の管理及び異動、職員等並びに委託スタッフ、退職者における利用者 ID の取扱い等については、定められた方法に従って行わなければならない。

②職員等並びに委託スタッフは、必要な利用者の登録及び変更又は抹消について、速やかに情報システム・セキュリティ管理者に申し出なければならない。

③情報システム・セキュリティ管理者は、利用されていない ID が放置されないよう、情報システム・セキュリティ担当と連携し、点検しなければならない。

(2)管理者権限

①ネットワーク又は情報システムの管理者権限は、必要最小限の者に与え、厳重に管理しなければならない。また、情報システム・セキュリティ管理者の権限を代行する者は、情 報システム・セキュリティ管理者が指名し、図書館情報セキュリティ部会が認めた者でなければならない。

②ネットワーク又は情報システムの管理及び運用を目的として契約により認められた者に付与する権限は、当該作業実行に必要な最小限のレベルに設定しなければならない。

(3)インターネット以外のネットワークにおけるアクセス制御

①アクセス可能なネットワーク及びネットワークサービス等については、ネットワークごとにアクセスすることができる者及びプロトコルを定めなければならない。

②情報システム・セキュリティ管理者は、ネットワークサービスを使用する権限を有しない職員等並びに委託スタッフに、当該サービスの権限を与えてはならない。

③情報システム・セキュリティ管理者は、職員等並びに委託スタッフが持ち込んだ端末等をネットワークに接続することができないようにするため、ネットワーク機器の配置又は機能により対策を講じなければならない。また、職員等並びに委託スタッフが持ち込み又は接続した端末から、情報システムへのアクセス又はネットワーク上の伝送データ

の収集を行うことができないようにするため、ネットワーク機器の配置又は機能により対策を講じなければならない。

(4)強制的な経路制御

情報システム・セキュリティ管理者は、ネットワーク経路制御を講じ、次に示す不正アクセスを防止しなければならない。

①外部ネットワークからの不正アクセス

②重要な情報システムが設置されたネットワークへの不正アクセス

③ダイアルアップサービスにおける登録外の電話番号からの着信及び登録外の電話番号への発信

(5)外部からのアクセス

①外部からのアクセスの許可は、必要最低限にしなければならない。

②アクセス方法及び使用方法等は、利用者の真正性を確保することができるものでなければならない。

③ネットワーク及び情報システムへの端末等による外部からのアクセスは、認可された特定業務の利用を除き禁止する。

(6)インターネットとの接続

①図書館内ネットワークとの接続点にはファイアーウォールを設置するとともに、次の措置を講じなければならない。また、すべての履歴を記録し、必要に応じて可視的な媒体に出力可能としなければならない。

- 情報システム･セキュリティ管理者が許可する以外の全ての通信は通信中継処理（プロキシ）し、インターネットから図書館内のコンピュータに直接接続させないようにすること。
- 図書館内の IP アドレス情報が流出しないように IP アドレス変換を行うこと。
- 許可を得ていない IP アドレス及びサービス（Telnet 等）の検知、通知等を行うこと。
- 情報システム・セキュリティ管理者が業務上不要又は不適切と判断したウェブページのアドレスを記録し、アクセスの検知、切断、通知等を行うこと。
- 不正アクセス、又は不正アクセスに類似するアクセスの検知、通知等を行うこと。

②情報システム・セキュリティ管理者は、職員等並びに委託スタッフが『藤沢市図書館情報セキュリティポリシー』に違反する行為をしないように、ブラウザを適切に設定するとともに、職員等並びに委託スタッフによる設定変更を防止するための対策を講じなければならない。

③インターネットにより情報又はサービスを提供する場合は、情報の保存又はサービスが実行されるコンピュータについて、次の対策を講じなければならない。

・ 専用のコンピュータ上において実施すること。
・ 公開する情報は、原則として原本（マスターデータ）を用いず、複製したものを用いること。
・ たとえ複製したものであっても、重要な情報である場合には、暗号化又はプログラムを実行するコンピュータと情報を保存するコンピュータとを分離して、双方間のアクセス制御を施すこと等の対策を講ずること。
・ プログラムの起動、及び常駐させるプログラム等は、必要最小限とすること。

(7)外部ネットワークとの接続

①外部ネットワークとの接続に際しては、当該外部ネットワークのネットワーク構成、機器構成、セキュリティレベル等を詳細に検討し、ネットワーク及び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た上で、情報システム・セキュリティ管理者及び図書館情報セキュリティ部会の許可を受けて接続しなければならない。

②接続した外部ネットワークの情報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、情報システム・セキュリティ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しなければならない。

(9) 自動識別

情報システム・セキュリティ管理者は、ネットワーク経路制御を講じ、次に示す不正アクセスを防止しなければならない。

(10)ログイン手順

①ログイン手順中におけるメッセージ、ログイン・ログアウト時刻の表示等、正当なアクセス権を持つ職員等並びに委託スタッフがログインしたことを確認することができる手順を定めなければならない。

②ログイン手順中のログを記録し、一定期間保存しなければならない。

(11)パスワードの管理方法

情報システム・セキュリティ管理者は、ネットワーク経路制御を講じ、次に示す不正アクセスを防止しなければならない。

①職員等並びに委託スタッフにパスワードを発行する場合は、職員等並びに委託スタッフのパスワードに関する情報を厳重に管理しなければならない。

②職員等並びに委託スタッフのパスワードについて、複雑性を要求するとともに、できる限りシステム側で制限をし、要求を満たさない職員等並びに委託スタッフについては使用を禁止させる。

③盗み見等の漏えい対策のために、パスワードを非印字又は非表示にする等の対策を講じなければならない。

④本人以外に読まれることのないようにするため、暗号化等パスワードを扱う方法を定めなければならない。

⑤ダイアルアップサービス、インターネット等を経由して図書館内ネットワークと接続する場合においては、必ずパスワードは暗号化しなければならない。

(12)接続の制限

①管理者権限によるネットワーク及び情報システムへの接続については、情報システム・セキュリティ担当者及び特定の職員に制限しなければならない。

②情報システムごとに接続可能な利用者 ID 等を定め、接続を制限しなければならない。

7.3. 情報システムの開発、導入、保守等

(1)情報システムの調達

情報システム・セキュリティ管理者は、情報システムの調達について、次の事項を遵守しなければならない。

①応用ソフトウェアの導入、変更及び運用についての手順等を明らかにしなければならない。

②機器及び基本ソフトウェアの導入、保守及び撤去についての手順等を明らかにしなければならない。

③情報システムの調達に当たっては、一般に公開する調達仕様書が情報セキュリティを確保するように努めなければならない。

④機器及びソフトウェアの購入等をする場合には、当該製品が情報セキュリティに影響を与えないように努めなければならない。

(2)情報システムの変更管理

情報システム・セキュリティ管理者は、情報システムの追加、変更、廃棄等をした場合は、その際の設定、構成等の履歴を記録し、保存しなくてはならない。

(3) 情報システムの開発

①情報システム・セキュリティ管理者は、情報システムの開発及び保守の際の事故及び不正行為を防止するため、次の事項を含むソフトウェア開発手順を定めるよう努めなければならない。

- 責任者及び監督者の選任
- 作業者及び作業範囲の決定
- 実施手順
- 承認手順
- 点検及び検証手順

・ ドキュメント作成手順
・ 情報システム開発、保守の際の事故及び不正行為に係るリスク分析
・ 開発及び保守に用いるシステムと運用システムとの分離
・ 開発及び保守に関するソースコードの提出
・ 開発及び保守の際のセキュリティ上問題となり得る恐れがある OS、ミドルウェア及びアプリケーション・ソフトウェアの使用禁止
・ 開発及び保守の際のアクセス制限
・ 機器の搬出、又は搬入する際の許可及び確認
・ 開発及び保守記録の提出義務
・ マニュアル等の定められた場所への保管
・ 開発及び保守を行った者の利用者 ID、パスワード等の開発及び保守終了後に不要となった時点での速やかな抹消

②情報システム・セキュリティ管理者は、システム開発手順に則したシステム開発を実施しなければならない。

③情報システム･セキュリティ管理者は､開発する情報システムの品質を確保するために、想定した容量及び処理能力を考慮しなければならない。

(4)情報システムの導入

①情報システム・セキュリティ管理者は、新たにシステムを導入する際には、既に稼動しているシステムに接続する前に十分な試験を行わなければならない。

②情報システム・セキュリティ管理者は、原則として、試験に使用したデータ及び試験の結果　を情報統括責任者に報告するとともに、厳重に保管しなければならない。

(5)ソフトウェアの保守及び更新

①ソフトウェア（独自開発ソフトウェア及び汎用ソフトウェア）等を更新し、又は修正プログラムを導入する場合は、不具合及び他の情報システムとの相性の確認を行い、計画的に更新又は導入をしなければならない。

②情報システム・セキュリティ管理者は、情報セキュリティに重大な影響を及ぼす不具合に対する修正プログラムについて、速やかな対応を行い、その他のソフトウェアの更新等については、計画的に実施しなければならない。

③情報システム・セキュリティ管理者は、システム更新又は統合時の検証等をしなければならない。

(6)機器の修理及び廃棄

①記録媒体が含まれる機器を外部の業者に修理させ、又は廃棄させようとするときは、当該記録媒体に記録された情報を消去することを契約事項として定めなければならない。

②外部の業者に故障を修理させ、又は廃棄させようとする場合において、修理又は廃棄を委託する業者に対し秘密を守ることを契約事項として定めなければならない。

7.4. コンピュータウィルス対策

(1)情報システム・セキュリティ管理者が許可した職員等並びに委託スタッフを除いて、外部のネットワークからの HTTP、FTP 等によるプログラムファイル等のダウンロード及びアップロードを禁止する。

(2)メールにより外部のネットワークから受信したファイルは、各サーバ及び端末等でウィルスチェックを行い、内部へのウィルス拡散を防止しなければならない。

(3)メールにより外部のネットワークへ送信するファイルは、各サーバ及び端末等でウィルスチェックを行い、外部へのウィルス拡散を防止しなければならない。

(4)情報システム・セキュリティ管理者は、次の事項を実施しなければならない。

①ウィルス情報について、職員等並びに委託スタッフに対する注意喚起を行う。

②常時ウィルスに関する情報収集に努める。

③図書館内で使用しているソフトウェア、及びソフトウェアの設定等にウィルスへの脆弱性が発覚した場合は、業務に支障がないことを確認した上で速やかに修正プログラムを適用する等の対策を講じなければならない。

④サーバ及び端末にウィルス対策ソフトウェアを導入し、定期的にウィルスチェックを行う。

⑤ウィルスチェック用のパターンファイルは、常に最新のものに保つ。

⑥ウィルスの感染及び駆除の履歴を記録して一定期間保管する。

(5)職員等並びに委託スタッフは、次の事項を順守しなければならない。

①外部からデータ又はソフトウェアを取り入れる場合、及びメール等により外部へデータ又はソフトウェアを持ち出す場合には、必ずウィルスチェックを行う。

②差出人が不明のメール、又は不自然に添付されたファイルは、速やかに削除する。

③ウィルスチェックを実行（端末等で自動実行）する。

④情報ネットワーク・セキュリティ管理者が提供するウィルス情報を常に確認する。

⑤添付ファイルのあるメールを送信又は受信する場合には、ウィルスチェックを実行する。

⑥ウィルス対策ソフトウェアを削除してはならない。

⑦コンピュータウィルス等の不正プログラムに感染した場合は、ＬＡＮケーブルの即時取り外しを行わなければならない。

7.5. 不正アクセス対策

(1)情報システム・セキュリティ管理者は、次の事項を実施しなければならない。

①業務に必要のないポートを開けてはならない。臨時でポートを開ける場合には、長時間空けたままにしてはならない。ただし、直ちに実施することができない場合は、計画的に実施しなければならない。

②サーバを再利用する場合は、フォーマットした上で再インストールしなければならない。

③セキュリティホールの発見に努め、メーカー等からセキュリティパッチの提供又は対処方法の提示があったときは、直ちに稼動中の情報システムに影響のないことを十分確認した上で、速やかにセキュリティパッチの適用又は設定変更を行わなければならない。

④不正アクセスによるウェブページ書換え防止を確実にするために、担当職員等並びに委託スタッフによるものであるかどうかにかかわりなく、データの書換えを検知し、情報システム・セキュリティ管理者に通報する設定を講じなければならない。

⑤重要なシステムの設定に係るファイル等について、定期的に当該ファイルの改ざんの有無を検知しなければならない。

(2)攻撃を受けることが明確な場合には、情報システム・セキュリティ管理者は、システムの停止を含む必要な措置を行うとともに、各機関との連絡を密にして情報の収集に努めなければならない。

(3) 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おいては、記録の保存に努めるとともに、警察その他関係機関との緊密な連携に努めなければならない。

(4) 職員等並びに委託スタッフは、データの漏えい、破壊又は改ざん、システムダウン等により、攻撃の可能性が明確で行政運営に深刻な影響を与えるような恐れがある場合には、情報システム・セキュリティ管理者等への報告を含め、速やかに対応しなければならない。

(5)情報システム・セキュリティ管理者は、職員等並びに委託スタッフによる不正アクセスがあった場合には、故意又は過失にかかわらず、適切な処置を求めなければならない。

(6)職員等並びに委託スタッフは、許可されないアクセスを行ってはならない。

7.6. セキュリティ情報の収集

(1)情報システム・セキュリティ管理者は、以下の情報セキュリティに関する情報を収集しなければならない。

①セキュリティホールに関する情報を収集し、必要に応じて関係者間で共有しなければならない。また、当該セキュリティホールの緊急度に応じてソフトウェアの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を収集し、必要に応じて対応方法について、職員等並びに委託スタッフに周知しなければならない。

(2)情報システム・セキュリティ管理者は、これらの情報を定期的に取りまとめ、『藤沢市図書館情報セキュリティポリシー』の改定につながる情報については、図書館情報セキュリティ委員会に報告しなければならない。

(3)情報システム・セキュリティ管理者は緊急に連絡すべき情報を入手した場合は、速やかに最高情報統括責任者に連絡しなければならない。

8.運用

8.1. 情報システムの監視

(1) 情報システム・セキュリティ管理者は、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。

(2)情報セキュリティに関する事案を検知するため、情報システム・セキュリティ管理者は、常に情報システムの監視を行わなければならない。

(3)外部と常時接続するシステムについては、ネットワーク侵入監視装置を設置し、24 時間監視を行わなければならない。

(4)内部のシステムについてはアクセス権の設定等を行い、異常な運用等の監視を行わなければならない。

(5)監視により得られた結果については、消去や改ざんをされないために必要な措置を講じ、安全な場所に保管するとともに記録の正確性を確保するため、当該時刻を正確に保たなければならない。

8.2. 『藤沢市図書館情報セキュリティポリシー』の遵守状況の確認

(1)情報システム・セキュリティ管理者は、『藤沢市図書館情報セキュリティポリシー』の遵守及び、問題の発生の有無について常に確認を行い、問題が発生している場合には速やかに情報システム・セキュリティ管理者に報告しなければならない。

(2)情報システム・セキュリティ管理者は、遵守状況に対し問題を発見した場合には、速やかに適切な処置をしなければならない。

(3)職員等は、『藤沢市図書館情報セキュリティポリシー』の違反が発生した場合は、直ちに情報システム・セキュリティ管理者に報告を行わなければならない。この場合において、当該違反の発生が直ちに情報セキュリティ上重大な影響を及ぼす恐れがあると情報システム・セキュリティ管理者が判断した場合には、最高情報統括責任者に報告するととも

に速やかに適切な処置を開始しなければならない。

(3)委託スタッフは、『藤沢市図書館情報セキュリティポリシー』の違反が発生した場合は、直ちに図書館委託業務事業者の責任者に報告を行わなければならない。この報告を受けた場合は、図書館委託事業者は速やかに情報システム・セキュリティ管理者に報告を行わなければならない。この場合において、当該違反の発生が直ちに情報セキュリティ上重大な影響を及ぼす恐れがあると情報システム・セキュリティ管理者が判断した場合には、最高情報統括責任者に報告するとともに速やかに適切な処置を開始しなければならない。

(4)情報システム・セキュリティ管理者は、サーバ等のシステム設定が『藤沢市図書館情報セキュリティポリシー』を遵守したものであるかどうか、又は問題が発生していないかどうかについて定期的に確認を行い、問題が発生していると認められたときは、速やかに適切な処置をしなければならない。

8.3. 運用管理における留意点

(1)情報システム・セキュリティ管理者は、アクセス記録、メール等個人のプライバシーに係る情報を閲覧することができる権限を有する職員を定め、情報セキュリティ実施手順に記載しなければならない。ただし、法令で定められた個人情報の保護に関する情報の閲覧は、当該法令に従わなければならない。

(2)情報システム・セキュリティ管理者は、職員等並びに委託スタッフが常に『藤沢市図書館情報セキュリティポリシー』を参照することができるように配慮しなければならない。

8.4. 緊急時の対応

(1) 事故及び侵害時の対処

情報資産への侵害が発生した場合、広範囲におけるシステム障害が発生した場合等には、緊急時における連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講じるために、次のように定める。

①連絡先

- 藤沢市長
- 最高情報統括責任者
- 情報システム・セキュリティ管理者
- 情報システムに係る外部委託先
- 市長室広報担当
- 神奈川県

・ 警察
・ 影響が考えられる個人及び法人

②事案の調査

情報セキュリティ及び障害に関する事案を認めた者は、次の事項について、速やかに情報システム・セキュリティ管理者に報告しなければならない。ただし、委託スタッフについては、図書館委託業務事業者を通じて連絡することとする。

・ 事案の内容
・ 事案が発生した原因として想定される行為
・ 確認した被害及び影響範囲
・ 障害事案の記録

情報システム・セキュリティ管理者は、事案の詳細な調査を行うとともに、最高情報統括責任者との情報の共有､及び図書館情報セキュリティ部会への報告を行わなければならない。

③事案への対処

＜連絡＞

情報システム・セキュリティ管理者は、次の事案が発生した場合は、それぞれ定められた連絡先に連絡しなければならない。

事案	連絡先
サイバーテロ他、市民に重大な被害が生じる恐れがある場合	藤沢市長、最高情報統括責任者、情報統括責任者、警察及び影響が考えられる個人、法人(別表１)
不正アクセスその他の犯罪と思慮される場合	藤沢市長、最高情報統括責任者、情報統括責任者、警察
踏み台となって他者に被害を与える恐れがある場合	藤沢市長、最高情報統括責任者、情報統括責任者、警察
情報システムに関する被害の恐れがある場合	最高情報統括責任者及び必要と認められる外部委託先
その他、情報資産に係る被害の恐れがある場合	最高情報統括責任者

＜ネットワークの切断＞

情報システム・セキュリティ管理者は、次の事案が発生した場合において、情報資産を防護するためにネットワークを切断しなければならない。

・ 異常なアクセスが継続しているとき、又は不正アクセスが判明したとき
・ 情報システムの運用に著しい支障を来す攻撃が継続しているとき

・ コンピュータウィルス等、不正プログラムがネットワーク経由で拡がっているとき
・ その他、情報資産に係る重大な被害が想定されるとき

＜システムの停止＞

情報システム・セキュリティ管理者は、次の事案が発生した場合において、情報資産の防護のために情報システムを停止しなければならない。

・ コンピュータウィルス等、不正プログラムが情報資産に深刻な被害を及ぼしているとき
・ 災害等により電源を供給することが危険又は困難なとき
・ その他、情報資産に係る重大な被害が想定されるとき

＜端末の切断＞

個々の端末のネットワークからの切断については、情報システム・セキュリティ管理者の許可を受けなければならない。ただし、情報資産の被害の拡大を直ちに停止させる必要がある場合には、事後報告とすることができる。

＜対応＞

情報システム・ネットワーク管理者は、事案に対応するために、次の事項を実施しなければならない。

・ 事案に係るシステムのアクセス記録及び現状を保存すること
・ 事案に対処した経過を記録すること
・ 事案に係る証拠保全の実施を完了するとともに、再発防止の暫定措置を検討すること
・ 再発防止の暫定措置を講じた後、復旧すること
・ 復旧後、必要と認められる期間、再発監視を行うこと

④再発防止の措置

・ 情報システム・セキュリティ管理者は、当該事案に係るリスク分析を実施し、『藤沢市図書館情報セキュリティポリシー』の改善に繋がる再発防止計画を策定し、図書館情報セキュリティ部会に報告しなければならない。
・ 図書館情報セキュリティ部会は、『藤沢市図書館情報セキュリティポリシー』の改善に繋がる再発防止計画が有効であると認められる場合は、これを承認する。
・ 情報システム・セキュリティ管理者は、各種情報セキュリティ対策の改善に係る再発防止計画を策定し、最高情報統括責任者に報告しなければならない。
・ 最高情報統括責任者は、これらの再発防止計画が有効であると認められる場合はこれを承認し、その承認を受けて情報システム・セキュリティ管理者は、事案の概要とあわせて職員等並びに委託スタッフに周知しなければならない。

(3)業務継続計画との整合性の確保

藤沢市が自然災害等に備えて業務継続計画を策定する場合、図書館情報セキュリティ部会は当該対応と『藤沢市図書館情報セキュリティポリシー』の整合性を確保しなければならない。

8.5. 外部委託による運用契約

運用を外部委託する場合は、委託に関する責任を有する者を明確にするとともに、外部委託先に対して必要な情報セキュリティ要件及び運用要件を記載した契約書による契約を締結しなければならない。

9. 法令遵守

職員等並びに委託スタッフは、職務遂行の際の情報資産について、次の法令等を遵守しなければならない。

(1)地方公務員法（昭和 25 年法律第 261 号）
(2)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）
(3)著作権法（昭和 45 年法律第 48 号）
(4)電子署名及び認証業務に関する法律（平成 12 年法律第 102 号）
(5)個人情報の保護に関する法律（平成 15 年法律第 57 号）
(6)藤沢市個人情報の保護に関する条例（平成 15 年藤沢市条例第 7 号）
(7)藤沢市行政手続等における情報通信の技術の利用に関する条例（平成 17 年藤沢市条例第 5 号）
(8)藤沢市コンピュータシステム管理運営規程（昭和 55 年藤沢市訓令甲第 5 号）

10. 情報セキュリティに関する違反に対する対応

『藤沢市図書館情報セキュリティポリシー』に違反した者については、図書館情報セキュリティ部会で調査の上、その重大性、発生した事案の状況等に応じて、藤沢市職員綱紀審査委員会規程（昭和 57 年藤沢市訓令甲第 4 号）第３条に規定する藤沢市職員綱紀審査委員会委員長に報告を行う。

11. 評価及び見直し

11.1. 監査

(1)情報システム・セキュリティ管理者は、ネットワーク及び情報システムの情報セキュリティについて、毎年度及び必要に応じて図書館情報セキュリティ内部監査員による監査を受けなければならない。

(2)外部委託をしている場合は、情報システム・セキュリティ管理者は、外部委託先から再委託された事業者も含めて、『藤沢市図書館情報セキュリティポリシー』の遵守についての監査を毎年度及び必要に応じて行わなければならない。

(3) 図書館情報セキュリティ内部監査員は監査結果を取りまとめ、図書館情報セキュリティ部会に報告を行う。図書館情報セキュリティ委員会は、この報告結果を『藤沢市図書館情報セキュリティポリシー』の更新の際に参照する情報として活用しなければならない。

11.2. 点検

(1)情報システム・セキュリティ管理者は、『藤沢市情報セキュリティポリシー』に沿った情報セキュリティが実施されているかどうかについて職員等並びに委託スタッフにアンケート等を行うとともに、毎年及び必要に応じて自己点検を行わなければならない。

(2)情報システム・セキュリティ管理者は、自主点検の結果を取りまとめ、図書館情報セキュリティ部会に報告しなければならない。

(3)図書館情報セキュリティ部会は、この報告結果を『藤沢市図書館情報セキュリティポリシー』の更新の際に参照する情報として活用しなければならない。

11.3. 『藤沢市図書館情報セキュリティポリシー』の更新

図書館情報セキュリティ部会は、新たに対策を講ずる必要が生じた場合、又は監査若しくは点検の結果、その必要があると認めた場合には、『藤沢市図書館情報セキュリティポリシー』の実効性を評価し、必要な部分を見直した上で、内容及び時期についての決定を行う。この決定に基づき、『藤沢市図書館情報セキュリティポリシー』の更新を実施し、更新の内容については、図書館情報セキュリティ委員会が決定しなければならない。