

# 相模原市情報セキュリティポリシー

【相模原市の電子情報資産の安全管理対策に関する基本的方針】

平成15年4月1日

平成19年4月1日（改正）

平成22年4月1日（改正）

相 模 原 市

# 相模原市情報セキュリティポリシー

はじめに	1
情報セキュリティ基本方針 (相模原市職員の電子情報資産の安全管理対策に関する規程)	2
情報セキュリティ対策基準	4
Ⅰ 相模原市情報セキュリティポリシーの体系	4
Ⅱ 情報セキュリティ基本方針の取扱い	4
1 情報セキュリティ基本方針の作成及び承認	
2 情報セキュリティ基本方針の遵守	
3 法規制等の遵守	
Ⅲ 管理体制	5
1 組織	
2 責任及び権限	
(1) 情報セキュリティ対策最高責任者の責任及び権限	
(2) 情報セキュリティ評価委員会の責任及び権限	
(3) 情報セキュリティ監査チームの責任及び権限	
(4) 情報セキュリティ向上委員会の責任及び権限	
(5) システム管理者の責任及び権限	
(6) 各課及び職員の責任及び権限	
Ⅳ 電子情報の管理	7
1 管理責任	
2 管理すべき電子情報	
3 電子情報の分類	
4 電子情報の管理手順	
Ⅴ 人的セキュリティ対策	8
1 職員の責任及び権限	
2 教育及び訓練	
3 セキュリティ事故への対応	
Ⅵ 物理的セキュリティ対策	10
1 装置の物理的セキュリティ対策	
(1) サーバの物理的セキュリティ対策	
(2) クライアントの物理的セキュリティ対策	
(3) プリンタ、コピー機及びFAXの物理的セキュリティ対策	
(4) 装置の廃棄又はリース機器の返却	

<b>VII 技術的セキュリティ対策</b>	<b>12</b>
1 アクセス記録の取得等	
2 アクセス制御	
(1) システムのアクセス制御	
(2) インターネットのアクセス制御	
(3) モデム接続及びモバイルコンピューティングのアクセス制御	
3 パスワード管理	
4 コンピュータウイルス対策	
5 障害対策	
(1) 目的	
(2) 電源バックアップ管理	
(3) データバックアップ管理	
<b>VIII 運用管理</b>	<b>15</b>
1 管理すべき文書	
2 インターネット関連の運用	
(1) 電子メール	
(2) ホームページの閲覧等	
3 新規システムの導入管理	
4 情報システムの外部委託管理	
5 セキュリティ情報の収集	
<b>IX 監視・検証、監査及び評価・見直し</b>	<b>17</b>
1 監視及び検証	
2 情報セキュリティ監査	
3 情報セキュリティポリシーの評価及び見直し	
<b>X 情報セキュリティポリシーに関する文書及び記録管理の遵守事項</b>	<b>18</b>
1 文書の管理	
2 記録の管理	

## はじめに

地方公共団体が扱う情報は、市民の個人情報のみならず、様々な行政執行上の重要な情報を含んでおりますが、近年の情報通信技術の進展に伴い、地方公共団体の諸活動は様々な情報システムを活用して展開されるようになっており、その取扱いについては慎重に行う必要があります。

特に、ネットワークを介した情報の高度利用とインターネットの爆発的な普及は行政事務の在り方にも大きな変革をもたらし、市民や他の地方公共団体との情報交流等の面において利便性が高まった反面、一旦、電子情報の漏えいやシステム障害等が発生した場合には市民生活及び行政執行に多大な影響を及ぼすこととなります。

このため、市の電子情報資産を様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、また、行政の事務執行を円滑にかつ継続的に確保するためにも必要不可欠なものであり、電子情報資産に関するセキュリティ対策について、総合的、体系的かつ具体的に取りまとめた情報セキュリティポリシーを作成する必要が生じて来ました。

本市の情報セキュリティポリシーは、現状の調査及び分析を行った後、一定の普遍性を備えた基本方針（相模原市職員の電子情報資産の安全管理対策に関する規程）と具体的な行動や判断の統一的な基準を定めた対策基準に分けて策定したものであり、職員個々に、この情報セキュリティポリシーの遵守を義務付け、電子情報資産を適正に管理すること及びその利用は業務遂行のみに限定し目的外には利用しないものとするものです。

今後は、継続的に評価及び見直しを行いながらこの情報セキュリティポリシーの適正な運用を行い、本市の電子情報資産の利用並びに管理における市民への安心の提供と行政の円滑な事務執行を図ってまいります。

# 相模原市職員の電子情報資産の安全管理対策に関する規程

(平成15年3月31日訓令第4号)

庁 中 一 般  
行政機関一般  
出先機関一般

## (目的)

第1条 この訓令は、市が所管する電子情報資産の機密性、完全性及び可用性を確保するため、様々な脅威に対する抑止、予防、検知及び回復について、組織的かつ体系的に取り組むための統一的な方針並びに電子情報資産の安全管理対策を実践するにあたっての基本的な考え方及び方策を定めることを目的とする。

## (定義)

第2条 この訓令において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

- (1) ネットワーク コンピュータを相互に接続するための通信回線網及びその構成機器をいう。
- (2) 情報システム ハードウェア、ソフトウェア、ネットワーク及びそれらの組み合わせをいう。
- (3) 電子情報 電子化されたプログラム及びデータ（資料及び帳票を含み、職員個人が資料整理等のために作成した個人利用ファイルは除く。）をいう。
- (4) 電子情報資産 電子情報並びに電子情報を作成し、管理し、及び保護する上で必要とされる情報システムをいう。
- (5) 機密性 アクセスを許可された者だけが、電子情報にアクセスできることをいう。
- (6) 完全性 電子情報及び処理方法が正確かつ完全であることをいう。
- (7) 可用性 許可された利用者が必要ときに電子情報にアクセスできることをいう。
- (8) 情報セキュリティ 守るべき電子情報資産を改ざん、喪失等の脅威から、機密性、完全性及び可用性の観点により保護することをいう。

2 この訓令において、「課」とは、相模原市行政組織及び事務分掌規則(平成19年相模原市規則第66号)第37条第1項及び相模原市区役所組織及び事務分掌規則(平成22年相模原市規則第19号)第6条第1項の課等、相模原市消防局組織等規則(平成19年相模原市規則第67号)第2条第1項に規定する課及び相模原市消防署組織等規程(昭和39年相模原市消防本部告示第5号)第2条第1項に規定する課をいい、「課長」とは、その長をいう。

## (職員の義務)

第3条 職員は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行において、情報セキュリティに関する法令等を遵守しなければならない。

2 職員は、契約により市の事務事業の委託を受けた事業者に対して、事業執行にあたりこの訓令を遵守するよう指導しなければならない。

(管理体制)

第4条 電子情報資産の統一的な情報セキュリティを確保するため、次に掲げる責任者、委員会及びチームを置く。

- (1) 情報セキュリティ対策最高責任者
- (2) 情報セキュリティ評価委員会
- (3) 情報セキュリティ向上委員会
- (4) 情報セキュリティ監査チーム

(電子情報の分類及び管理)

第5条 課長は、課で作成した電子情報及び外部から収受した電子情報について、機密性、完全性及び可用性を踏まえた分類を行い、その重要性に応じ、適切な管理を行うものとする。

(情報セキュリティ対策)

第6条 課長は、課で管理する電子情報資産を、不正アクセス、改ざん、入力誤り、操作誤り、災害その他の脅威から守るため、次に掲げる対策を行うものとする。

- (1) 人的セキュリティ対策として、情報セキュリティに関する権限及び責任並びに遵守すべき事項を明確に定め、職員に対する周知及び徹底を図るとともに、十分な教育及び啓発が行われるよう必要な対策を講ずる。
- (2) 物理的セキュリティ対策として、情報システムの設置場所への不正な立入り並びに電子情報資産への損害及び利用の妨害等から保護するための物理的な対策を講ずる。
- (3) 技術的セキュリティ対策として、電子情報資産を不正アクセス等から保護するため、電子情報資産へのアクセス制御、ネットワーク管理等の技術的な対策を講ずる。
- (4) 電子情報資産の運用における対策として、情報システムの監視、情報セキュリティ対策の遵守状況の確認その他情報セキュリティ運用面の対策を講ずる。
- (5) 緊急時における情報セキュリティ対策として、緊急事態が発生した場合に、迅速かつ適切な対応を行うための危機管理対策を講ずる。

2 情報セキュリティ向上委員会は、情報セキュリティ対策の実行に関して、職員への支援及び指導を行うものとする。

(情報セキュリティ監査の実施)

第7条 情報セキュリティ監査チームは、情報セキュリティ対策が遵守されていることを検証するため、定期に又は臨時に情報セキュリティ監査を実施するものとする。

(評価)

第8条 情報セキュリティ評価委員会は、情報セキュリティ監査の結果及び情報セキュリティを取り巻く状況の変化等を踏まえ、情報セキュリティ対策が有効に機能しているか検証するため随時に評価を実施し、評価結果を情報セキュリティ対策最高責任者へ報告するものとする。

(委任)

第9条 この訓令に定めるもののほか、情報セキュリティ対策の実施に関し必要な事項は、別に定める。

附 則

この訓令は、平成15年4月1日から施行する。

附 則(平成19年3月30日訓令第13号)

この訓令は、平成19年4月1日から施行する。

附 則(平成22年3月31日訓令第14号)

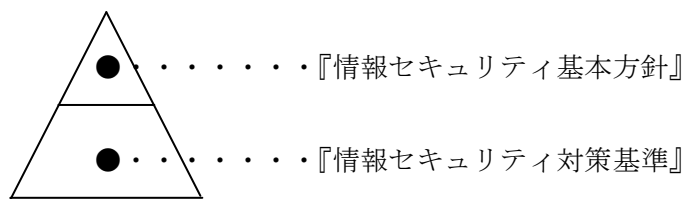
この訓令は、平成22年4月1日から施行する。

# 情報セキュリティ対策基準

この基準は、相模原市職員の電子情報資産の安全管理対策に関する規程（平成15年3月31日訓令第4号、以下「情報セキュリティ基本方針」という。）第9条に基づき、情報セキュリティ対策を実施するにあたっての遵守すべき事項や判断等の統一的な基準として必要な事項を定める。

## I 相模原市情報セキュリティポリシーの体系

相模原市の情報セキュリティポリシーの体系は、次のとおりである。



なお、個々の情報システムについての情報セキュリティ対策を具体的を実施するため、「情報セキュリティ実施手順」を定める。

## II 情報セキュリティ基本方針の取扱い

### 1 情報セキュリティ基本方針の作成及び承認

情報セキュリティ基本方針は、情報セキュリティ対策最高責任者が原案を作成し、市長の承認をもって施行する。

### 2 情報セキュリティ基本方針の遵守

(1) 情報セキュリティ対策最高責任者は、次の手段により情報セキュリティ基本方針の公表を行い、職員及び関連する委託事業者の理解及び自覚を促進する。

- ・ホームページへの掲載
- ・グループウェアの掲示板への掲載

(2) 職員及び関連する委託事業者は、情報セキュリティ基本方針を理解し、確実に実行する。

### 3 法規制等の遵守

#### (1) 法規制の遵守

情報セキュリティポリシーは、法規制等を遵守するものであり、常に関連法規制との整合を維持するものとする。

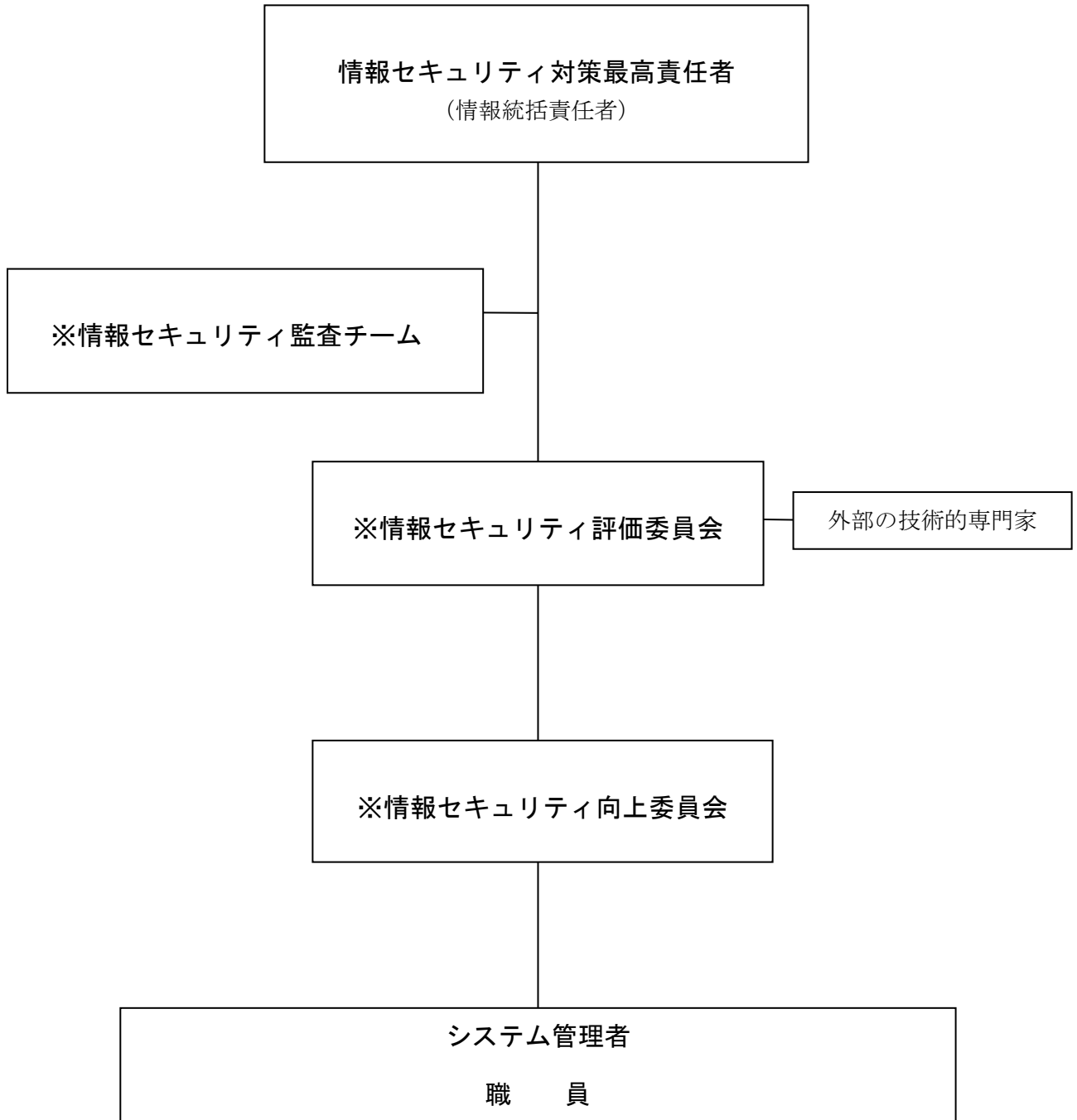
#### (2) 関連する法規制等の管理

情報セキュリティ法規制等登録簿により管理する。

### Ⅲ 管理体制

#### 1 組織

次のとおり組織を整備する。



※詳細については、別途各設置要綱に定める。

## 2 責任及び権限

- (1) 情報セキュリティ対策最高責任者の責任及び権限
  - ①情報セキュリティポリシーに定められた全ての活動に関する最終責任と権限
  - ②情報セキュリティポリシーの遵守の徹底
  - ③情報セキュリティ評価委員会の設置
  - ④情報セキュリティ監査チームの設置
  - ⑤情報セキュリティ基本方針の見直し
- (2) 情報セキュリティ評価委員会の責任及び権限
  - ①効果的な情報セキュリティ対策の仕組みの確立、実行及び維持
  - ②情報セキュリティポリシーの実施状況について情報セキュリティ対策最高責任者への報告
  - ③情報セキュリティポリシーの実行に必要な教育訓練の計画
  - ④情報セキュリティ対策基準の見直し
- (3) 情報セキュリティ監査チームの責任及び権限
  - ①情報セキュリティ監査の計画及び実施
  - ②情報セキュリティ監査の報告
- (4) 情報セキュリティ向上委員会の責任及び権限
  - ①情報セキュリティ評価委員会から指示された情報セキュリティ対策に関する計画及び実施
  - ②情報セキュリティポリシーの実行に関する各職員への支援及び指導
- (5) システム管理者の責任及び権限
  - ①所管する情報システムの全ての活動に関する最終責任と権限
  - ②所管する情報システムのセキュリティに関する最終責任と権限
  - ③所管する情報システムの実施手順の維持及び管理
- (6) 職員の責任
  - ①情報セキュリティ対策の重要性の認識と確実な実行
  - ②情報セキュリティ監査への協力
  - ③情報セキュリティ実施手順の管理
  - ④記録の管理

## IV 電子情報の管理

### 1 管理責任

電子情報は、当該電子情報を作成した各課・機関及び外部から収受した各課・機関の長が管理責任を有するものとする。

### 2 管理すべき電子情報

管理すべき電子情報は、特定の業務を行うシステム（以下「業務システム」という。）で管理する電子情報、パソコンで作成管理するデータ及びこれらに関連する紙媒体とする。

### 3 電子情報の分類

各課は、管理すべき電子情報を、機密性、完全性及び可用性の観点から総合的に評価し、重要性に応じて分類する。

### 4 電子情報の管理手順

各課は、業務システム、パソコンデータ及び紙媒体について、共通実施手順書に従い、電子情報の分類、保管の手順、取扱いの手順及び廃棄の手順を定め、適切な管理を行うものとする。

なお、具体的な管理手順については、共通実施手順書に定める。

## V 人的セキュリティ対策

### 1 職員の責任及び権限

(1) 職員の責任及び権限は次のとおりとする。

区分	システム管理者	職員	情報政策課長
電子情報資産の管理	◎	○	◎
セキュリティに関する教育及び訓練	○		◎
セキュリティ事故への対応	◎	○	◎
物理的セキュリティ対策	◎	○	◎
アクセス制御の管理	◎	○	◎
パスワード管理	◎	◎	
コンピュータウイルス対策	◎	○	◎
障害対策	◎	○	◎
システムの運用	◎	○	
ネットワークの運用管理	◎	○	◎
インターネット関連の運用	◎	○	◎
新規システムの導入管理	◎		
情報システムの外部委託管理	◎		
監視及び測定	○		◎
文書及び記録の管理	◎	○	◎
共通実施手順書の作成			◎
業務システム実施手順書の作成	◎		

◎：総括的な責任及び権限を有する者 ○：責任を有する者

(2) 責任及び権限の詳細は、情報セキュリティ業務分掌職務権限一覧表に定める。

### 2 教育及び訓練

#### (1) 分類

分類	受講対象者	教育及び訓練の概要	実施責任者
新規採用職員教育	新規採用職員	情報セキュリティポリシーを理解し、確実に実行することを目的とした教育	情報政策課長
セキュリティ啓発教育	職員	セキュリティ対策の重要性及び管理対策の意義など、セキュリティ対策の自覚向上を目的とした教育	情報政策課長
システム運用教育	新規システム利用者	新しいシステムに対する、適正な操作を行えることを目的とした教育	システム管理者
セキュリティ内部監査員養成教育	新規セキュリティ内部監査員	内部監査員の資格要件を満たすことを目的とした教育	情報セキュリティ監査チームリーダー
随時教育	職員	職員への随時の教育	各課・機関の長
	非常勤及び臨時職員	非常勤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を目的とした教育	

(2) 教育の計画及び実施

各教育実施責任者は、効果的な教育を実施するために以下の内容により教育の計画を立案し、実施する。

- ・教育の実施予定日
- ・教育実施者
- ・受講対象者
- ・実施内容及び使用するテキスト
- ・教育の効果測定方法
- ・上記以外で教育実施責任者が必要と判断した内容

(3) 教育の効果の確認

教育実施責任者は、実施した教育に関する効果の確認を行う。効果の確認手段とは次のとおりとする。

- ・アンケートの実施
- ・理解度テストの実施
- ・受講者へのインタビューの実施
- ・その他

(4) 報告書の作成

各教育実施責任者は、教育を実施後、実施報告書を作成する。

3 セキュリティ事故への対応

(1) 危機管理手順書の整備

各システム管理者はセキュリティ事故が起こった場合、迅速な復旧及び二次被害発生の防止を確実にするため対応手順が記載された危機管理手順書を整備すること。

また、システムを利用する課においては、システムダウン時の窓口対応マニュアルの整備を行う。

(2) 報告義務

全ての職員は、情報セキュリティ事故が発生した場合は、各システム管理者へ速やかに報告する。また、発生する恐れがある場合も同様とする。

(3) 対応手順

- ①情報セキュリティ事故を発見した職員は、各システム管理者へ報告する。
- ②報告を受けたシステム管理者は内容を確認し、必要な措置を講ずる。
- ③システム管理者は、事故状況を情報政策課長へ報告する。
- ④情報政策課長は、必要に応じて情報セキュリティ対策最高責任者及び情報セキュリティ評価委員会へ報告する。

(4) 事故の対応結果について、情報セキュリティ事故管理台帳に記録する。

## VI 物理的セキュリティ対策

### 1 装置の物理的セキュリティ対策

#### (1) サーバの物理的セキュリティ対策

##### ①目的

- ・許可されないアクセスからの不正なアクセスの防止
- ・許可されたアクセスの誤使用の防止
- ・システム障害につながるホコリからの保護及び空調管理等
- ・地震や火災などの災害からの保護

##### ②サーバ装置はロックで管理し、電子情報の重要性に応じて以下の管理策を講ずる。

###### a 管理策

管理レベル	管理策
高	専用施設での管理
↑	サーバールームでの管理
↓	パーティション設置などの管理
低	上記以外の管理

###### b サーバ別の管理策の詳細は、電子情報資産管理台帳に定める。

#### ③専用施設及びサーバールーム（セキュリティ区画）の管理

##### a 管理策

電子情報の重要性に応じて、以下の管理策を講ずる。

管理対象	管理策
表示など	原則としてセキュリティ区画と判断できる表示は行わない。
不正侵入者の防止	常に施錠を行う。（IDカード、パスワードキー等の利用）
入退室管理	入退室者の管理を行う。
空調管理	空調設備の設置等による適切な温度管理を行う。
納品及び出荷管理	セキュリティ区画での直接の納品及び出荷は原則として禁止する。
防災対策	耐震補強、防火設備等必要な措置を講ずる。

##### b セキュリティ区画への立入許可

外部委託者に、セキュリティ区画への立入を許可する場合は、次の要件を満たすものとする。

- ・契約書に守秘義務を含むセキュリティ要求事項を明確にする。
- ・事前に名簿を提出するとともに、名札、制服等の着用を義務付ける。
- ・管理者若しくは管理者が任命した者が立会い、作業を行わせる。

#### (2) クライアントの物理的セキュリティ対策

##### ①目的

- ・許可されないアクセスからの不正なアクセスの防止
- ・許可されたアクセスの誤使用の防止
- ・盗難又は紛失による情報漏えいの防止
- ・故障又は破損による利用不能状態の防止

②管理策

管理対象名		管理策
モニター画面		<p>離席時は、以下の管理の内、適切な措置を講ずる。</p> <p>a 長時間の場合</p> <ul style="list-style-type: none"> <li>・ パソコン又はモニターの電源を切る</li> <li>・ パスワード付スクリーンセイバーを設定する</li> <li>・ コンピュータのロックを行う</li> </ul> <p>b 短時間の場合</p> <ul style="list-style-type: none"> <li>・ 画面表示を起動初期状態にする</li> </ul>
I Dカードの利用 (該当する端末のみ)		<p>以下の行為を禁止する。</p> <p>a 他人の I Dカードの利用又は他人への貸し出し</p> <p>b 装置付近への I Dカードの放置</p>
ノート型 パソコン	保管	<p>以下の管理の内、適切な措置を講ずる</p> <p>a 鍵付キャビネット等で保管する</p> <p>b 鍵付チェーンなどで保護しデスク上で管理する</p>
	外部への 持ち出し	<p>原則として禁止する。</p> <p>ただし、業務上やむを得ない場合は、所属長の許可を得ること。なお、重要な電子情報がパソコンに保存されている場合は、以下の管理の内、適切な措置を講ずること。</p> <p>a ファイルを削除する</p> <p>b ファイルへのパスワード設定又は暗号化</p> <p>c 装置のロック</p>

(3) プリンタ、コピー機及びFAXの物理的セキュリティ対策

①目的

- ・ 許可されないアクセスからの不正なアクセスの防止
- ・ 許可されたアクセスの誤使用の防止
- ・ 印刷物等の盗難又は紛失による情報漏えいの防止

②管理策

設置にあたっては、印刷物等が第三者による意図しない参照又は盗難を予防できる場所とする等、適切な管理を行う。また、利用後の原紙や印刷物等の長時間の放置や取り忘れを防止する。

(4) 装置の廃棄又はリース機器の返却

①目的

- ・ 廃棄装置からの情報漏えいの防止
- ・ 返却装置からの情報漏えいの防止

②管理策

廃棄又は返却時は、データの完全消去やハードディスク等を物理的に破壊するなど、各システム管理者が責任をもって実施する。

## Ⅶ 技術的セキュリティ対策

### 1 アクセス記録の取得等

重要な電子情報を扱う業務システムについては、システム管理者は各種アクセス記録を取得し、一定期間保存するものとする。

### 2 アクセス制御

#### (1) システムのアクセス制御

##### ①目的

- ・許可されないアクセスからの不正なアクセスの防止
- ・許可されないアクセスのシステムの不正な変更防止

##### ②業務システム及びサーバの管理策

電子情報の重要性の分類に応じ、次のうち適切な管理を行う。

- ・セグメント分離
- ・ルータ等の装置によるアクセス制御
- ・暗号化
- ・パスワード設定
- ・アプリケーション、ドライブの利用制限

##### ③パソコンの管理策

電子情報の重要性の分類に応じ、次のうち適切な管理を行う。

- ・認証キー
- ・ICカード
- ・ファイルの暗号化
- ・パスワード設定

##### ④各管理対象別のアクセス制御管理策の詳細は、電子情報資産管理台帳に定める。

#### (2) インターネットのアクセス制御

##### ①目的

- ・許可されないアクセスからの不正なアクセスの防止
- ・許可されないアクセスのシステムの改ざん防止
- ・サービス停止による市民サービスの低下の防止

##### ②管理策

ファイアウォール	a 不要なポートは制御するなど、適切な設定を行う。 b 不正アクセスの監視等の防御策を施す。 c 設定権限を適正に管理する。 d 定期的にログを監視及び保存する。 e セキュリティパッチは遅滞なく適用する。
ルータ	a 必要のないプロトコルやサービス等を制御する。 b 設定権限を適正に管理する。 c セキュリティパッチは遅滞なく適用する。

##### ③インターネットのアクセス制御管理策の詳細については、インターネットアクセス制御管理台帳に定める。

#### (3) モデム接続及びモバイルコンピューティングのアクセス制御

モデム接続及びモバイルコンピューティングの利用は、原則として禁止する。

### 3 パスワード管理

#### (1) 目的

- ・許可されないアクセスからの不正なアクセスの防止
- ・許可されたアクセスの誤用（意図されない利用・参照）防止

#### (2) サーバのパスワード管理

次の事項を遵守し、適切な管理を行う。

- 設定又は変更する場合は、推測可能なものを使用しないこと。
- 変更する場合は、過去に使用したパスワードを使用しないこと。
- パスワードを口外したり、記録したメモなどを放置したりしないこと。

サーバのパスワードに関する管理策の詳細は、電子情報資産管理台帳に定める。

#### (3) クライアントのパスワード管理

次の事項を遵守し、適切な管理を行う。

- 設定又は変更する場合は、推測可能なものを使用しないこと。
- 変更する場合は、過去に使用したパスワードを使用しないこと。
- パスワードを記録したメモなどを放置しないこと。

### 4 コンピュータウィルス対策

#### (1) 目的

- ・許可されないアクセスからの不正なアクセスの防止
- ・許可されないアクセスからの情報の改ざんの防止
- ・ウィルス感染によるネットワーク、パソコン等のシステム停止の防止

#### (2) 対策

##### ①各システム管理者の遵守事項

システム導入時	<ol style="list-style-type: none"><li>サーバ及びクライアントには必ずウィルス対策ソフトを導入しなければならない。</li><li>必要に応じてゲートウェイサーバ等の対策を行う。</li></ol>
システム導入後	<ol style="list-style-type: none"><li>ウィルス定義ファイルは常に最新版に更新しなければならない。</li><li>内部セキュリティ監査の結果に基づき、必要に応じて情報政策課は、各システムのウィルス対策について指導する。</li></ol>

##### ②利用者の遵守事項

- 送信元不明等、不審な電子メールの添付ファイルに対しては、これに操作を加えてはならない。
- 電子メールやフロッピーディスク等で外部へ提供するファイルは、必ずウィルス検査を行うこと。
- ウィルスの感染やウィルスと思われる症状を発見した場合は、各システム管理者へ速やかに報告を行う。

## 5 障害対策

### (1) 目的

- ・システムの障害による情報利用停止の防止
- ・システムの障害による情報破損・紛失の防止

### (2) 電源バックアップ管理

#### ①遵守事項

- a 電子情報資産管理台帳に登録されたサーバは十分な電源を確保し、必ずUPS（無停電電源装置）の設置を行うこと。
- b UPSでのバックアップ対象は、必要最低限の装置とすること。（プリンタ及びモニタ画面などの出力装置は極力接続しないこと）
- c UPSは、バックアップ対象の電源規定量を確認の上選定を行うこと。
- d 製造元の取扱説明書に基づき、定期的にUPSの電池を交換すること。なお、使用状況等を考慮し、必要に応じて性能確認を行うこと。

### (3) データバックアップ管理

#### ①遵守事項

- a サーバのデータは必ずバックアップを行うこと。
- b バックアップ装置は、バックアップ対象の規定量（ディスクサイズ）を確認の上選定すること。
- c バックアップは計画された手順（手法及び頻度）に基づき、定期的に行うこと。
- d バックアップの手順（手法及び頻度）は定期的に見直すこと。
- e バックアップに使用した媒体は適切に保管すること。
- f 内部システム監査等により、定期的に各システムのバックアップ管理の状況を確認する。

②各管理対象別の電子情報バックアップ管理に関する管理策の詳細は、電子情報資産管理台帳に定める。

## Ⅷ 運用管理

### 1 管理すべき文書

基本方針	情報セキュリティ基本方針
対策基準	情報セキュリティ対策基準
実施手順及び 管理台帳等	共通実施手順書
	業務システム実施手順書
	情報セキュリティ法規制等登録簿
	セキュリティ管理記録一覧表
	情報セキュリティ業務分掌職務権限一覧表
	電子情報資産管理台帳
	セキュリティ区画管理台帳
	インターネットアクセス制御管理台帳
	モデム接続管理台帳
	ウイルス対策管理台帳
	情報システム外部委託管理手順書
内部セキュリティ監査マニュアル	
その他	ネットワークシステム管理運用要綱
	インターネット管理運用要領
	OA機器管理運用要領
	電子メール利用基準

### 2 インターネット関連の運用

インターネットの利用は、情報収集や情報伝達が容易である反面、情報漏えいの事故につながりやすいことやコンピュータウィルスの感染経路になることもある。本市が被害者若しくは加害者にならないため、適切な運用を行う。

#### (1) 電子メール

電子メールの利用については、電子メール利用基準に従うものとする。

#### (2) ホームページの閲覧等

ホームページの閲覧等インターネットの利用については、インターネット管理運用要領に従うものとする。

### 3 新規システムの導入管理

新規情報システムの導入及びシステム開発にあたっては、次の事項を遵守しなければならない。

遵守事項	管理手順
開発環境の分離	①運用システムと開発するシステムは、次の単位で分離すること。 a ネットワークのセグメント b 開発室 c サーバ ただし、物理的に困難な場合又は開発段階における事前テスト時はこの限りではない。
開発データの保護	①開発用のデータに個人情報等重要な情報が含まれる場合はマスキングを行うこと。 ②委託先から外部へ流出しないよう管理すること。 a 原則として、業務の再委託を禁止する b データ保管場所の確認 c データ管理の「覚書」等の徴取 ③開発終了時は確実に開発データを消去すること
システム検証の実施	①仕様段階でのセキュリティ要求事項の検証 ②試験成績書の作成 ③試験成績書に基づく検査の実施 ④導入事前テストの実施

### 4 情報システムの外部委託管理

#### (1) 遵守事項

情報システムを外部委託する場合には、情報セキュリティ基本方針を理解させ、確実に実行させるとともに、許可された者の不正アクセスを防止するため、以下の事項を遵守する。

①委託先に情報セキュリティに関する規定及び個人情報保護に関する規定が存在すること。

②契約書上で機密保持契約がなされること。

③上記に合わせ作業員個人との機密保持契約（誓約書）を提出させること。

(2) 情報システムの外部委託に関する手順の詳細は、情報システム外部委託管理手順書に定める。

### 5 セキュリティ情報の収集

#### (1) 目的

情報セキュリティポリシーの有効性の維持及びセキュリティ事故の防止を図るため、積極的に情報収集を行う。

#### (2) 外部環境情報の活用

情報政策課は、セキュリティ技術、セキュリティ事故情報、法規制の制定、改定など入手した外部環境情報を情報セキュリティポリシーの見直しに活用する。

また、必要に応じて各システム管理者に周知する。

## Ⅸ 監視・検証、監査及び評価・見直し

### 1 監視及び検証

#### (1) 目的

- ・許可されない不正なアクセス（ウイルスも含む）の認識
- ・システムの性能低下の把握
- ・情報セキュリティポリシーの有効性の改善

#### (2) 監視及び検証の対象及び手段

分類	対象及び手段		主管部門
システムの運用監視	対象	内部からのアクセス	各システム管理者
	手段	サーバのシステムログ、イベントログ監視	
外部からの不正アクセスの監視	対象	外部からの不正アクセス	情報政策課
	手段	侵入検知システム等による監視	
ネットワーク脆弱性の検証	対象	サーバ、ルータ、ファイアウォールの脆弱性	情報政策課
	手段	脆弱性検査ツールによる検証	
ウイルスの監視	対象	ウイルス感染	各システム管理者
	手段	ウイルス対策ソフトの機能による監視	
ネットワークの性能監視	対象	ネットワークのトラフィック	情報政策課
	手段	専用モニタリング装置による監視	

#### (3) 監視及び検証の手順

- ①各システム管理者は、計画を立案し、計画どおり監視又は検証の実施を行う。
- ②各システム管理者は、監視及び検証の結果に基づき、適切な措置を講ずる。
- ③各システム管理者は、監視及び検証の結果を適宜情報政策課へ報告を行う。
- ④情報政策課は、各システム管理者からの報告を情報セキュリティポリシーの見直しに活用する。

### 2 情報セキュリティ監査

#### (1) セキュリティ内部監査員

- ①情報セキュリティ監査チームリーダーは、セキュリティ内部監査員の互選によるものとする。
- ②セキュリティ内部監査員は次の研修のいずれかを受講する。
  - ・外部研修機関によるセキュリティ内部監査員研修
  - ・上記の研修受講者による内部研修

#### (2) 監査の種類

定期監査	監査される活動の状況及び重要性に基づいて、情報セキュリティ監査チームが作成した情報セキュリティ監査計画書に従い、実施する監査
臨時監査	定期監査以外に、セキュリティ評価委員会の判断により臨時的に行われる監査

### (3) 監査の手順

- ①情報セキュリティ監査チームリーダーは、被監査部門との独立性を考慮し、セキュリティ内部監査員を選任する。
- ②セキュリティ内部監査員は、次の内容を踏まえ、情報セキュリティ監査実施計画書を作成する。
  - ・ 監査スケジュール
  - ・ 監査対象の抽出
  - ・ 監査チェックリスト
- ③実施計画書に基づき、監査を実施する。必要に応じて、監査の全部又は一部を外部の専門家に委託することができる。
- ④監査結果を記録し、情報セキュリティ評価委員会へ報告する。
- ⑤必要により助言、フォローアップを行う。

### 3 情報セキュリティポリシーの評価及び見直し

情報セキュリティポリシーを効果的に運用するため、次に掲げる要因により情報セキュリティポリシーの実効性を評価し、必要に応じて見直しを行う。

- ・ 社会環境の変化及び市民からの要望
- ・ 関連する法規制の改正
- ・ 本市、国及び他の地方公共団体のセキュリティ事故事例
- ・ 有識者からの助言及び情報セキュリティ対策技術の進展
- ・ 情報セキュリティポリシーの遵守状況（内部セキュリティ監査結果等）
- ・ 内部環境の変化

## X 情報セキュリティポリシーに関する文書及び記録管理の遵守事項

### 1 文書の管理

- a 許可された利用者が容易に利用することができるように管理すること。
- b 情報セキュリティ基本方針と情報セキュリティ対策基準との準拠性を維持するために適宜見直しを行い、必要に応じて改定を行うこと。
- c 更新履歴を管理すること。
- d あらかじめ定められた責任権限によって承認されること。
- e 廃止文書は速やかに除去し、常に最新版を利用できるように管理すること。

### 2 記録の管理

- a 必要と認められる期間、保管すること。
- b 許可された利用者が容易に利用することができるように管理すること。
- c 損傷、劣化及び紛失を防ぐ適切な措置を行うこと。

対策基準 改訂履歴

Ver.	制定／改訂 承認年月日	改訂項目	改訂内容	改訂理由
初版	H15.3.31	—	初版制定	—
第2版	H19.3.30	III管理体制 1 組織 2 責任及び権限 (6)	構成員の変更 項目の変更	組織改変に伴う組織体制及び構 成員を各要綱に委任するもの。 項目について修正するもの。
第3版	H22.3.31	V 人的セキュリティ対策 1 職員の責任及び権限 2 教育及び訓練 3 セキュリティ事故への対応  VII 技術的セキュリティ対策 4 コンピュータウィルス対策  VIII 運用管理 5 セキュリティ情報の収集  IX 監視・検証、監査及び評 価・見直し 1 監視及び検証	組織名の変更	組織改変に伴い、組織名を変更するもの。