

相模原市情報セキュリティポリシー

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）

平成24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

相模原市情報セキュリティポリシーの体系

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)

情報セキュリティ対策基準

I 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
- 2 情報セキュリティ基本方針の遵守

II 情報セキュリティ対策基準の取扱い

- 1 情報セキュリティ対策基準の作成及び承認
- 2 情報セキュリティ対策基準の遵守
- 3 適用範囲

III 管理体制

- 1 組織
- 2 責任及び権限

IV 電子情報の管理

- 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

- 1 職員の遵守事項
- 2 教育の実施
- 3 事故、欠陥等の報告対応
- 4 ID及びパスワードの管理

VI 物理的セキュリティ対策

- 1 サーバ等の管理
- 2 管理区域の管理
- 3 通信回線及び通信回線装置の管理
- 4 パソコン等の管理

VII 技術的セキュリティ対策

- 1 コンピュータ及びネットワークの管理
- 2 アクセス制御
- 3 情報システムの開発・保守等
- 4 不正プログラム対策
- 5 不正アクセス対策
- 6 セキュリティ情報の収集

VIII 運用管理

- 1 情報システムの監視
- 2 情報セキュリティポリシーの遵守状況の確認
- 3 危機管理対策
- 4 委託管理
- 5 例外措置
- 6 法令遵守
- 7 情報セキュリティポリシー違反の対応

IX 監査及び評価・見直し

- 1 監査
- 2 情報セキュリティポリシーの評価及び見直し
- 3 自己点検

X 情報セキュリティポリシーに関する文書及び記録の管理

- 1 文書の管理
- 2 記録の管理

はじめに

行政が取り扱う情報は、市民の個人情報や行政執行上の様々な重要情報を含んでいますが、近年の情報通信技術の進展に伴い、行政においてもインターネットをはじめとする情報通信ネットワークや情報システムを活用した諸活動があらゆる面で展開されるようになったため、情報の取り扱いについて適正かつ慎重に行う必要があります。

万が一、個人情報や機密情報の漏えい、不正アクセス、情報システム障害等の重大なセキュリティ事故が発生した場合には、行政の円滑な事務執行のみならず市民生活にも多大な影響を及ぼす恐れがあります。

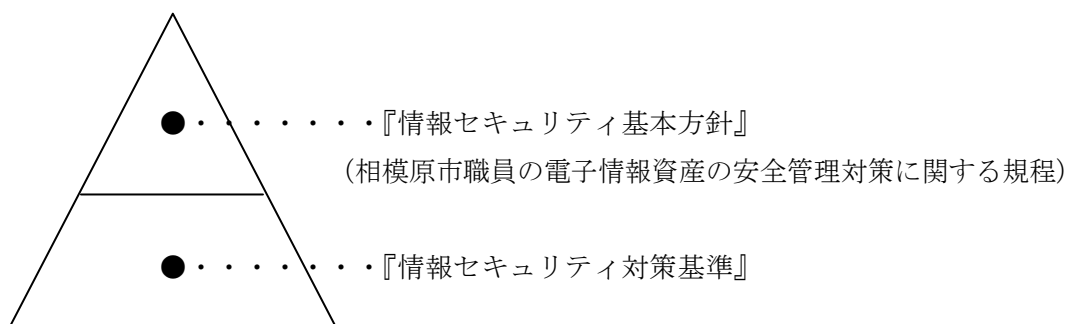
したがって、市民の財産、プライバシー等を守るため、また、行政の円滑な事務執行を安定的かつ継続的に確保するために、適切な情報セキュリティ対策を実施し、様々な脅威から市の電子情報資産を防御することが必要不可欠となります。

このことから、本市では、情報セキュリティ対策における取り組みの基本的な考え方を備えた基本方針（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を取りまとめた情報セキュリティポリシーを策定し、職員個々に、遵守を義務付けています。

今後においても、この情報セキュリティポリシーの適正な運用を行い、継続的に評価及び見直しを行いながら、本市の情報セキュリティ水準を高め、市民の信頼の確保及び行政の円滑な事務執行を図ってまいります。

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、情報セキュリティ対策基準に基づき、情報セキュリティ対策を具体的に実施するための手順等を必要に応じて別に定める。

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当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 コンピュータ、ネットワーク及び記憶媒体で構成され、情報処理を行う仕組みをいう。
- (3) 情報機器 ハードウェア及び記憶媒体(情報システムの構成要素となるものを除く。)をいう。
- (4) 電子情報 電子化されたプログラム及びデータ(これらに関連する資料及び帳票を含む。)をいう。
- (5) 電子情報資産 情報システム、情報機器及び電子情報をいう。
- (6) 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。
- (7) 完全性 電子情報に破壊、改ざん又は誤りがない状態を確保することをいう。
- (8) 可用性 アクセスを許可された者が、必要なときに中断されることなく電子情報にアクセスできる状態を確保することをいう。
- (9) 情報セキュリティ 電子情報資産を機密性、完全性及び可用性の観点から保護することをいう。
- (10) 課 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38条第1項の課等、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項の課等並びに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及び派遣労働者(労働者派遣事業

の適正な運営の確保及び派遣労働者の就業条件の整備等に関する法律(昭和60年法律第88号)第26条第1項に規定する労働者派遣契約に基づき市に派遣され、市の事務事業に従事する者をいう。)に対して、事業執行に当たりこの訓令を遵守するよう周知し、及び徹底しなければならない。

(管理体制等)

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、管理者、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) 統括情報セキュリティ責任者
- (3) 情報セキュリティ管理者
- (4) 情報システム管理者
- (5) 情報セキュリティ評価委員会
- (6) 情報セキュリティ向上委員会
- (7) 情報セキュリティ監査チーム

- 2 情報セキュリティ対策最高責任者は、情報セキュリティに関する全ての活動を総括し、企画市民局長をもって充てる。
- 3 統括情報セキュリティ責任者は、情報セキュリティ対策の実行を統括する責任及び権限を有し、情報政策課長をもって充てる。
- 4 情報セキュリティ管理者は、所管する情報機器及び電子情報のセキュリティ対策の実行に関する責任及び権限を有し、当該情報機器及び電子情報を所管する課の長をもって充てる。
- 5 情報システム管理者は、所管する情報システムのセキュリティ対策の実行に関する責任及び権限を有し、当該情報システムを所管する課の長をもって充てる。
- 6 情報セキュリティ評価委員会は、情報セキュリティ対策の仕組みの確立及び維持に関する責任及び権限を有する。
- 7 情報セキュリティ向上委員会は、情報セキュリティ評価委員会から指示された事項に関する責任を有する。
- 8 情報セキュリティ監査チームは、情報セキュリティ監査の計画及び実施に関する責任及び権限を有する。

(電子情報の分類及び管理)

第5条 情報セキュリティ管理者は、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、完全性及び可用性に基づく分類を行い、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 情報セキュリティ管理者及び情報システム管理者は、課で管理する電子情報資産を、紛失、盗難、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、職員が遵守すべき事項の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 統括情報セキュリティ責任者は、情報セキュリティ対策の実行に関して、情報セキュリティ管理者及び情報システム管理者への指導、助言及び許可を行うものとする。

(情報セキュリティ監査の実施等)

第7条 情報セキュリティ監査チームは、毎年度情報セキュリティ監査計画を作成し、情報セキュリティ評価委員会の承認を得るものとする。

2 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、前項の監査計画又は情報セキュリティ評価委員会の指示に基づき情報セキュリティ監査を実施し、当該監査の結果を情報セキュリティ評価委員会へ報告するものとする。

(評価等)

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。

2 情報セキュリティ向上委員会は、情報セキュリティ評価委員会から指示された事項に関する調査及び分析を行い、当該調査及び分析の結果を情報セキュリティ評価委員会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。

附 則(平成24年3月30日訓令第3号)

この訓令は、平成24年4月1日から施行する。