【B】

羽村市	情報セキュリティ対策基準	概要版 第３版

羽村市
情報セキュリティ対策基準
（概要版）

制定	平成 16 年 6 月	最終改正	平成 28 年 3 月

【B】

羽村市	情報セキュリティ対策基準	概要版 第３版

目　　次

制定	平成 16 年 6 月	最終改正	平成 28 年 3 月

第1章　羽村市情報セキュリティポリシー

１　羽村市情報セキュリティポリシーの構成

羽村市情報セキュリティ基本方針（以下「基本方針」という。）及び羽村市情報セキュリティ対策基準（以下「対策基準」という。）をあわせて、羽村市情報セキュリティポリシー（以下「セキュリティポリシー」という。）という。

２　基本方針

羽村市（以下「市」という。）が保有する情報資産を、様々な脅威から組織的、体系的かつ継続的に保護するための統一的な方針として、基本方針を定めるものとする。

３　対策基準

基本方針に基づき、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及び判断等の統一的な基準として、対策基準を定めるものとする。

４　実施手順

セキュリティポリシーに基づき、情報セキュリティ対策を実施するための具体的な運用基準又は手順として、「羽村市情報セキュリティ実施手順」（以下「実施手順」という。）を定めるものとする。

５　セキュリティポリシーの適用範囲

- 市が保有する情報資産
- 当該情報資産を取り扱う職員及び市の事務事業の委託を受けた者

６　セキュリティポリシーの遵守

職員及び市の事務事業の委託を受けた者（以下「受託者」という。）は、セキュリティポリシーを理解し、遵守しなければならない。

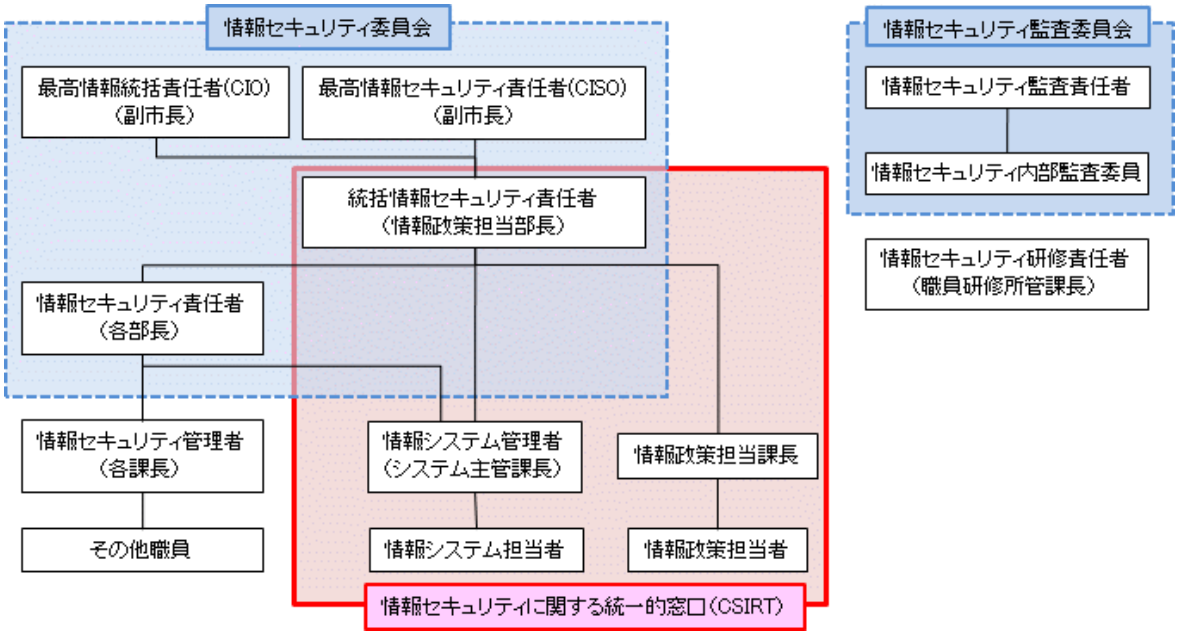
７　法令等の遵守

職員及び受託者は、法令違反及び契約上の義務不履行を避けるため、情報セキュリティに係る関係法令等を遵守しなければならない。

第2章　　組織体制

組織体制

　情報セキュリティ対策を組織的かつ効果的に実施するため、以下のとおり体制を整備する。



第3章　　情報資産の管理

１　情報資産価値の評価基準

情報資産の価値は、機密性、完全性、可用性により、それぞれ評価する。

２　情報資産価値の評価（計算）

情報資産の価値＝機密性による価値＋完全性による価値＋可用性による価値

３　情報資産の分類

情報資産の価値による分類を行う。

- 最重要情報、重要情報、一般情報及び最重要・重要・一般情報以外の情報

４　情報資産の識別情報

資産の識別は、属性ごとに分類・識別する。

- 情報システム、その他の電磁的記録及び紙媒体等

5　情報資産の管理策

情報資産の属性ごとに、保管、取扱い及び廃棄に関する遵守事項を定める。

管理において、複数の分類に該当する情報が混在する場合は、できるだけ分離して管理するよう努める。ただし、混在が避けられない場合は、上位の管理策による。

第4章　人的セキュリティ対策

1　研修

情報セキュリティ対策の実施を確実にするために、研修を行う。

(1)　研修の分類

- 新規採用職員研修
- 情報セキュリティ研修
- 情報システム運用研修
- 情報セキュリティ内部監査委員養成研修

(2)　研修計画

- 情報セキュリティ研修責任者（以下「研修責任者」という。）は、研修計画を策定しなければならない。
- 研修責任者は、研修計画（情報システム運用研修を除く。）について情報セキュリティ委員会（以下「セキュリティ委員会」という。）の承認を得なければならない。

(3) 研修の実施及び効果の確認

研修実施者は、必要に応じて、研修効果を確認しなければならない。

2　セキュリティポリシーに違反した者への対応

セキュリティポリシーの実効性を確保するため、法令等に対する違反及びセキュリティポリシーに対する違反においては、厳正に対応するものとする。

第5章　物理的セキュリティ対策

1　物理的セキュリティ対策の分類

- 施設の物理的セキュリティ対策
- 装置の物理的セキュリティ対策

２　施設の物理的セキュリティ対策

- 施設の入退室管理を行う。
- 施設内における管理のための遵守事項を定める。

３　装置の物理的セキュリティ対策

- サーバ（ホスト）の管理及びサーバ（ホスト）ルーム内における遵守事項を定める。
- クライアント（端末）の管理のための遵守事項を定める。
- プリンタ、ＦＡＸ、コピー機及びコードレス電話の管理のための遵守事項を定める。
- 装置の廃棄又は借用物件の返却における権利のための遵守事項を定める。

第6章　技術的セキュリティ対策

１　アクセス制御

(1)　アクセス制御の分類

- サーバ（ホスト）のアクセス制御
- クライアント（端末）及びパソコンのアクセス制御
- 外部接続のアクセス制御
- モデム等による外部接続のアクセス制御
- 無線 LAN におけるアクセス制御

(2)　サーバ（ホスト）のアクセス制御

サーバ（ホスト）については、情報資産の価値に応じて、適切なアクセス制御を行う。

(3)　クライアント（端末）及びパソコンのアクセス制御

クライアント（端末）及びパソコンについては、情報資産の価値に応じて、適切なアクセス制御を行う。

(4)　外部接続のアクセス制御

外部接続（インターネット接続を含む。）におけるアクセス制御に関する遵守事項を定める。

(5)　モデム等による外部接続のアクセス制御

モデム等を使用する外部接続のアクセス制御に関する遵守事項を定める。

２　アカウント管理

- サーバ(ホスト)、クライアント(端末)、パソコン及び情報システムについては、利用者を識別する符号の管理を行う。
- パスワードに関する遵守事項を定める。

３　コンピュータウイルス対策

- コンピュータのウイルス対策管理者の遵守事項を定める。
- 利用者の遵守事項を定める。

４　装置の冗長化等

- 必要に応じ、適切な装置及び電源の冗長化を講じる。
- 情報のバックアップを行う。

５　不正アクセス対策

教育等の人的対策及び技術的対策（入口・内部・出口対策等）等、必要な不正アクセス対策を講じなければならない。

第7章　情報システムの運用等における対策

１　インターネットの利用

- 電子メールの利用の遵守事項を定める。
- その他のインターネットの利用の遵守事項を定める。

２　プログラム及びハードウェアの管理

- プログラム及びハードウェアを導入する場合は、標準構成を策定するものとする。
- 導入したプログラム及びハードウェアについては、ライセンス（使用許諾権）及びハードウェアの管理をしなければならない。
- プログラム（OS、ファームウェア、その他のプログラム）については、セキュリティ修正プログラムを速やかに適用し、最善の状態を維持しなければならない。
- 情報システム導入等に関する遵守事項を定める。

３　情報収集及びセキュリティ情報の共有

情報セキュリティ対策の有効性の確認及び情報セキュリティ事故を防止するための情報を収集し、活用するものとする。

第8章　外部委託管理

１　委託を受けようとする者の選定

業者を選定する契約担当課は、市が保有する情報資産に関する業務を委託しようとするときは、委託を受けようとする者における情報セキュリティに関する体制について、確認するよう努めなければならない。

２　外部委託の実施

- 個人情報に関する業務を委託する場合は、羽村市個人情報保護条例及び同施行規則に定める事項を内容とする契約によって行う。
- その他の情報資産に関する業務を委託する場合は、次に定める事項を内容とする契約によって行う。

３　委託契約書等への記載事項

- 秘密の保持義務
- 情報の指示目的以外の使用の禁止
- 情報の第三者への提供の禁止
- 情報の複写又は複製の禁止
- 情報の管理方法の指定、管理義務及び返還又は廃棄義務
- 事故発生時の報告義務
- 再委託の禁止又は制限
- 職員による立入調査
- 監査への協力
- 成果（物）に関する所有権又は知的財産権の帰属
- 上記に定める事項に違反した場合の契約解除及び損害賠償

第9章　事業継続管理（情報セキュリティ事故への対応）

情報セキュリティ事故

- すべての職員及び受託者は、事故の大小を問わず、情報セキュリティ事故を報告しなければならない。
- 報告先の対応責任者は、報告者に対し、適切な指示を行わなければならない。
- 情報セキュリティ事故に対応する場合は、最悪の事態を想定しつつ行動する。
- 情報セキュリティ事故に対しては、原因の調査及び再発防止策を講じなければならない。

- 情報セキュリティ事故対応に関する詳細手順は、情報セキュリティ事故対応計画書に定めるものとする。

第10章 監視・検証及びセキュリティポリシーの見直し

１ 監視・検証

- 情報セキュリティ管理者（以下「セキュリティ管理者」という。）は、監視又は検証を実施するものとする。
- セキュリティ管理者は、監視又は検証の実施において、異常等が発生した場合は、「情報セキュリティ事故対応計画書」に基づき報告を行うものとする。
- セキュリティ管理者は、必要に応じて監視又は検証の結果を、セキュリティ委員会に報告するものとする。
- セキュリティ委員会は、セキュリティ管理者に対して監視又は検証の結果報告を求めることができるものとする。
- セキュリティ委員会は、最高情報セキュリティ責任者（以下「CISO」という。」）の指示により、監視又は検証の結果報告を参考にしてセキュリティポリシーの見直しを行うものとする。

２ セキュリティポリシーの評価及び見直し

セキュリティポリシーの評価は、セキュリティ委員会が行う。また、セキュリティポリシーの見直しは、CISO の指示によりセキュリティ委員会が行う。

第11章 監査

１ 情報セキュリティ監査

セキュリティポリシーの遵守状況を検証するため、情報セキュリティ内部監査（以下「監査」という。）を行う。

２ 情報セキュリティ内部監査委員

(1) 情報セキュリティ内部監査委員の選任

- 情報セキュリティ内部監査委員（以下「監査委員」という。）は、CISO が選任する。
- 情報セキュリティ監査責任者（以下「監査責任者」という。）は、監査委員の中から、CISO が選任する。

(2) 監査委員の要件

情報セキュリティ内部監査委員養成研修を修了し、情報セキュリティ内部監査委員登録リストに登録された者とする。

(3) 情報セキュリティ監査委員会の設置

CISO の下に、監査委員による情報セキュリティ監査委員会（以下「監査委員会」）を設置する。

(4) 監査委員の責務

- 監査委員は、監査を適正かつ客観的に行わなければならない。
- 監査委員は、監査によって知り得た情報を、他に漏らしてはならない。

３　監査の種類

監査は、定期監査と臨時監査に分類する。

４　監査の実施

(1) 情報セキュリティ内部監査計画

監査責任者は、定期監査又は臨時監査を実施する場合、あらかじめ情報セキュリティ内部監査計画（以下「監査計画」という。）を策定し、CISO の承認を得なければならない。

(2) 監査の事前準備

- 監査責任者は、監査対象からの独立性を考慮して、監査委員会の中から当該監査作業に従事する監査委員を選び、情報セキュリティ内部監査チーム（以下「監査チーム」という。）を編成する。
- 監査チームは、監査で使用するチェックリストの作成等の事前準備を行う。

(3) 監査の実施

監査チームは、監査計画に基づいて、監査対象におけるセキュリティポリシーの遵守状況を、実地調査、インタビュー、記録の調査等の手段により検証する。

(4) 監査の報告

監査責任者は、監査報告書を作成し、CISO に対して、監査対象におけるセキュリティポリシー遵守状況の検証結果の報告及び改善等の勧告を行う。

(5) フォローアップの実施

監査責任者は、改善勧告等を行った場合、必要に応じて、監査対象における改善実施の有無及び改善結果の有効性等を確認するものとする。

第12章 セキュリティポリシー関連文書及び記録の管理

１　セキュリティポリシー関連文書の管理

⑴　セキュリティポリシー関連文書

セキュリティポリシー関連文書とは、セキュリティポリシー及び実施手順に関する文書をいう。

⑵　セキュリティポリシー関連文書管理の管理策

- セキュリティポリシー関連文書は、承認された者のみが、利用することができるように管理する。（利用管理）
- セキュリティポリシー関連文書は、更新履歴を管理し、その改正があった場合は、速やかに改正部分の差替え、周知する等の措置を行う。（改正履歴管理）
- セキュリティポリシー関連文書は、予め定められた者が承認する。（承認管理）
- セキュリティポリシー関連文書は、常に最新版を利用できるよう管理する。（最新版管理）
- 廃止されたセキュリティポリシー関連文書は、保存期間終了後、速やかに廃棄する。（廃棄管理）

２　記録の管理

⑴　記録

記録とは、セキュリティポリシーの準拠性及び効果的な運用の証拠となる文書をいう。

⑵　記録管理の管理策

- 記録は、セキュリティポリシーの準拠性確認のため、定められた期間、保管する。（保管）
- 記録は、承認された者だけが利用することができるように管理する。（利用管理）
- 記録は、損傷、劣化及び紛失を防ぐ等の適切な措置を講じる。（保管）

３　セキュリティポリシー関連文書の取扱い

セキュリティポリシー関連文書の取扱いは、以下のとおりとする。

- 公開可能文書：基本方針、対策基準（概要）
- 非公開文書（又は一部公開）とする文書：対策基準、実施手順