高崎市情報セキュリティポリシー

（概要版）

ホームページ公開用

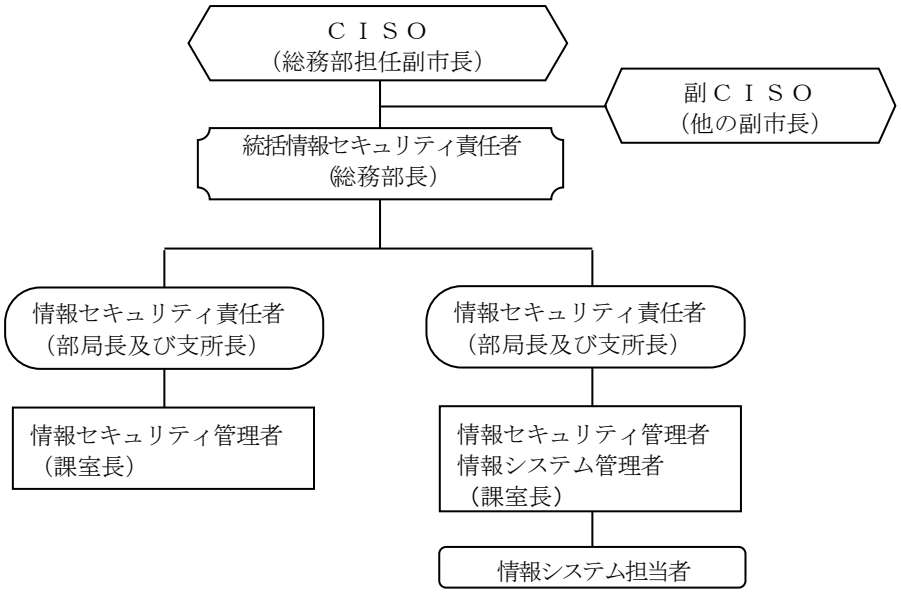
高　崎　市

１　情報資産とは

情報資産とは、業務を実施するのに必要な情報及びそれを扱う情報システムをいう。

２　組織体制

【組織図】



３　情報資産の分類と管理方法

① 情報資産の分類

本市では情報資産のうち、個人情報などのいわゆる非公開情報を「重要性分類Ａ」（以下、Ａ分類）と位置付け、様々な脅威から守るための対策を実施する。

② 管理台帳の作成

漏えいや改ざん、紛失、盗難、破壊などの脅威から守るべき情報資産を職場ごとに洗い出し、台帳に記載する。管理台帳は、情報セキュリティ対策の核となるもので、情報資産の状況を常に反映させる必要があるため、随時更新しなければならない。

③ コピーした情報の扱い

電子情報をコピーした情報も原本と同様、適切に管理しなければならない。

④ 業務目的外の利用

業務以外の目的による情報資産の利用は禁止する。

⑤ 情報資産の保管

情報資産は施錠可能な場所に保管する。

⑥ 情報の送信

個人情報を電子メールやファックスで外部に送信することはできない。

⑦ 情報資産の運搬

情報資産を運搬する場合は、情報セキュリティ管理者の許可を受け、鍵付きのケース等に入れ、暗号化又はパスワードの設定を行う。

⑧ 電磁的記録媒体の廃棄

電磁的記録媒体及び文書等が不要になった場合は、物理的に破壊するなど、情報を復元できないようにしたうえで廃棄しなければならない。

４　人的セキュリティ

① 情報セキュリティポリシーとは

組織の中にある情報資産を、様々な脅威から守るための規約を文書化したものが情報セキュリティポリシーという。

② パソコン、モバイル端末等の持ち出し

パソコン、モバイル端末等を外部へ持ち出すことはできない。

③ 私物パソコン、モバイル端末等の持込み

私物のパソコンやモバイル端末等を業務に利用することはできない。

④ ＵＳＢメモリ等の複数のネットワークでの利用制限

ＵＳＢメモリ等の電磁的記録媒体を、マイナンバー系、ＬＧＷＡＮ系、インターネット系等の複数ネットワークで利用することは禁止する。

⑤ インターネットパソコンへのデータ保存の禁止

インターネットパソコンは、Ａ分類の情報資産を保存することを禁止する。

⑥ 離席時の対応

離席時にはパソコンをシャットダウンまたはロックをしなければならない。

⑦ 事故等の報告

情報セキュリティに関する事故、システム上の欠陥及び誤動作を発見した場合は、速やかに情報セキュリティ管理者に報告する。

⑧ パスワードの管理

パスワードは秘密にし、照会等には一切応じてはいけない。

５　技術的セキュリティ

① 業務目的外の利用

業務以外の電子メール送信を禁止する。

② 複数人に同時送信する場合

電子メールを送信する場合、送信先のメールアドレスを十分に注意しなければならない。

③ 誤送信した場合

電子メールを誤送信した場合は、情報セキュリティ管理者に報告する。

④ フリーメールの利用

フリーメールを許可無く利用することはできない。

⑤ ソフトウェアの導入

パソコンやモバイル端末に対し、情報システム管理者の許可なくソフトウェアの導入（インストール）はできない。

⑥ 不正コピーの禁止

ソフトウェアの不正コピーは違法行為であり、一切認められない。

⑦ パソコン、モバイル端末等の接続制限

パソコン、モバイル端末等を、情報システム管理者の許可なく本市のネットワークに接続してはならない。

⑧ 業務目的外の利用

業務以外の目的で、インターネットへのアクセスや閲覧を行ってはいけない。

⑨ コンピュータウイルス対策

コンピュータウイルスが含まれている可能性がある場合は、添付ファイルを開かずに削除する。明らかに本市を攻撃対象とする標的型攻撃メール等であると判断できた場合は、速やかに情報セキュリティ管理者に報告する。

⑩ コンピュータウイルス対策

コンピュータウイルスの感染が疑われる場合は、ＬＡＮケーブルの即時取り外し又は無線機能の無効化を行う。

６　運用

ポリシーに違反した場合、地方公務員法及び高崎市職員の懲戒処分の基準に関する要綱等に基づき、懲戒処分の対象となる。

７　外部委託

① 外部委託先の選定基準

情報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。

② 契約項目

情報システムの開発・運用等を外部委託する場合には、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。

ア 情報セキュリティポリシーの遵守

イ 委託内容及び作業場所の特定

ウ 提供された情報の目的外利用の禁止及び業務上知り得た情報の守秘義務

エ 再委託に関する制限事項の遵守

オ 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・市による調査権

カ 市による情報セキュリティインシデント発生時の公表

キ 情報漏洩等により、市に損害が発生した場合の規定(損害賠償等)

③ 確認・措置等

情報セキュリティ管理者は、外部委託事業者において必要な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。また、その内容を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に報告するとともに、その重要度に応じてＣＩＳＯに報告しなければならない。

④ 委託事業者の遵守義務

委託事業者は、高崎市長から開示された重要性分類Ａの情報資産を扱う場合、次の事項を遵守しなければならない。

ア 委託事業者は、その中から、開示された情報資産の取扱いに関し、すべての責任と権限を有する情報取扱責任者を任命しなければならない。

イ 委託事業者は、情報取扱責任者をはじめ、情報資産を取扱うすべての従事者の氏名を高崎市長に報告しなければならない。

ウ 情報取扱責任者は、情報資産の機密を保持するため、情報資産を取扱うすべての従事者に対し、遵守すべき事項を研修等により理解させなければならない。

エ 委託事業者は、情報資産への不当なアクセス又は情報資産の漏洩、紛失、破壊、盗難、改ざん等（以下「漏洩等」という。）を防止するための方策を、高崎市長に報告しなければならない。

オ 委託事業者は、漏洩等のリスクを考慮し、最大限の注意をもって情報資産を管理しなければならない。