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

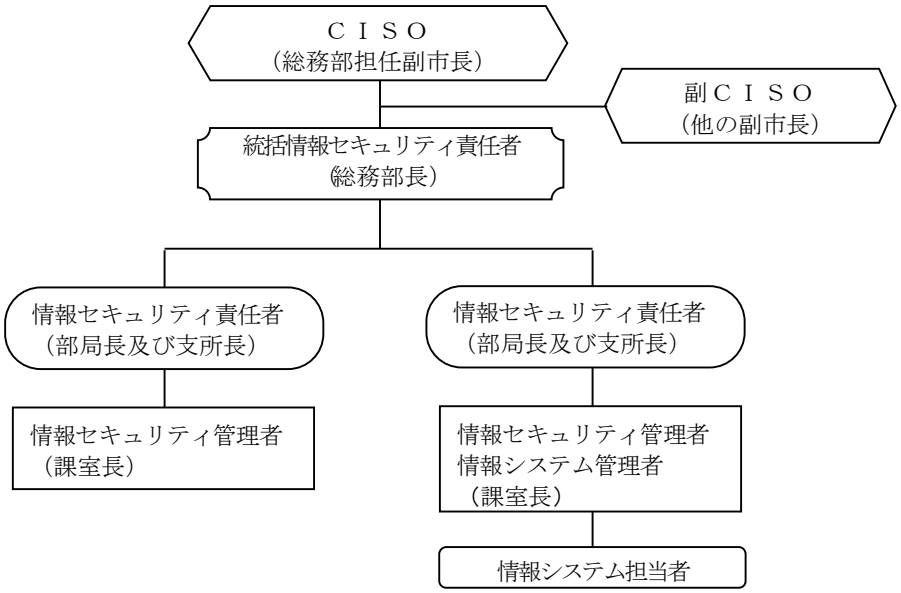
高　崎　市

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

本市では情報資産を機密性、完全性及び可用性により分類し、機密性による分類のうち、個人情報などのいわゆる非公開情報を自治体機密性２以上と位置付け、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 クラウド上の情報の扱い

クラウドサービスの環境に保存される情報も、①の分類に基づき管理しなければならない。

⑤ 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。

⑥ 情報資産の保管

情報資産は施錠可能な場所に保管する。

⑦ 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。

⑧ 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。

⑨ 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、その機密性に応じ、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。

クラウドサービスで利用する全ての情報資産について、クラウドサービスの利用終了時期を確認し、クラウドサービスで扱う情報資産が適切に移行及び削除されるよう管理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を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 支給以外のパソコン、モバイル端末等の持込み

支給以外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、自治体機密性２以上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、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。

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 業務外ネットワークへの接続の禁止

支給された端末を、情報システム管理者によって定められたネットワークと異なる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　業務委託と外部サービス（クラウドサービス）

① 業務委託に係る運用規定の整備

統括情報セキュリティ責任者は、業務委託に係る、委託業務の範囲や委託事業者の選定基準等を含む運用規程を整備しなければならない。

② 業務委託実施前の対策

情報セキュリティ管理者又は情報システム管理者は、業務委託の実施までに、選定条件を含む仕様の策定や、仕様に基づく委託事業者の選定、秘密保持契約の締結などを実施しなければならない。また、重要な情報資産を取扱う業務を委託する場合には、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等に係る要件を明記した契約を締結しなければならない。

- 情報セキュリティポリシー及び情報セキュリティ実施手順の遵守
- 個人情報漏えい防止のための技術的安全管理措置に関する取り決め
- 委託事業者の責任者、委託内容、作業者の所属、作業場所の特定
- 提供されるサービスレベルの保証
- 委託事業者にアクセスを許可する情報の種類と範囲、アクセス方法の明確化など、情報のライフサイクル全般での管理方法
- 委託事業者の従業員に対する教育の実施
- 提供された情報の目的外利用及び委託事業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
- 市による監査、検査
- 市による情報セキュリティインシデント発生時の公表
- 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 業務委託実施期間中の対策

情報セキュリティ管理者又は情報システム管理者は、業務委託の実施期間において、委託判断基準に従った重要情報の提供や、統括情報セキュリティ責任者へ措置内容の報告など含む対策を実施しなければならない。また、情報の適正な取扱いのための情報セキュリティ対策や、その履行状況の定期的な報告などを求めなければならない。

④ 業務委託終了時の対策

情報セキュリティ管理者又は情報システム管理者は、業務委託の終了に際して、セキュリティ対策が適切に実施されたことの確認や、委託事業者において取り扱われた情報が確実に返却、廃棄又は抹消されたことの確認などの対策を実施しなければならない。

⑤ クラウドサービスの選定に係る運用規程の整備

統括情報セキュリティ責任者は、自治体機密性２以上の情報を取り扱う場合、クラウドサービス提供者の選定基準など、外部サービスの選定に関する規定を整備しなくてはならない。

⑥ クラウドサービスの利用に係る運用規程の整備

統括情報セキュリティ責任者は、クラウドサービスの特性や責任分界点に係る考え方等を踏まえ、クラウドサービスを利用して情報システムを構築、運用、更改、廃棄する際のセキュリティ対策の基本方針を運用規程として整備しなければならない。