高崎市等広域消防局
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・安中市消防組合

１　情報セキュリティポリシーとは

組織内の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リュティポリシーという。正規職員・再任用職員・嘱託職員・臨時職員・派遣職員は、このポリシーを遵守しなければならない。

また、当消防局の情報資産を外部委託業者に託す場合には、当該業者にもポリシーの遵守を契約等で義務付け、その内容を理解させなければならない。

２　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。

３　組織体制

（１）情報セキュリティ責任者・・・・・　消防局長
（２）情報セキュリティ副責任者・・・・　消防局次長
（３）情報セキュリティ管理者・・・・・　課長・署長・分署長
（４）情報システム管理者・・・・・・・　警防課長（情報セキュリティ管理者を兼務）
（５）情報システム担当者・・・・・・・　警防課情報管理係

４　情報資産の分類と管理方法

（１）情報資産の分類

当消防局では、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以上と位置づけ、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）コピーした情報及びネットワークストレージ上の情報の扱い

電子情報をコピーした情報及びネットワークストレージ上に保存される情報も、（１）の分類に基づいて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ＦＡＸで外部に送信してはならない。

（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こと。

（８）電磁的記録媒体及び文書等の廃棄

電磁的記録媒体及び文書等が不要になった場合は、その機密性に応じて、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。

５　人的セキュリティ

（１）パソコン及びモバイル端末等の持出し

原則として、指定された端末以外のパソコン及びモバイル端末等を外部へ持出すことはできない。

（２）支給以外のパソコン及びモバイル端末等の持ち込み

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。また、情報システム管理者の許可なく端末を消防局のネットワークに接続してはならない。

（３）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、ＩＷＡＮ回線系、インターネット系等の複数ネットワークで利用してはならない。

（４）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してはならない。

（５）離席時の対応

離席時は、パソコンやモバイル端末をシャットダウン又はサインアウトしなければならない。

（６）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を導入してはならない。また、導入した場合でアカウント等を取得した場合は、情報セキュリティ管理者が取得したライセンスを管理すること。

（７）パスワードの管理

パスワードは秘密にし、照会等に応じてはならない。また、端末機器や机上にパスワードが記載されたラベル等を貼り付け、パスワードを公開するような行為をしてはならない。

６　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してはならない。

（２）複数人に同時にメール送信する場合

電子メールを複数人に送信する場合、必要性がある場合を除き、他の送信先の電子メールアドレスが送信先の端末上に表示されないように送信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速やかに報告しなければならない。

（４）フリーメールの利用

インターネット上のフリーメールを、情報セキュリティ責任者の許可なく利用してはならない。

（５）ストレージサービスの利用

インターネット上で利用できるネットワークストレージサービスを、情報セキュリティ責任者の許可なく利用してはならない。

（６）業務外ネットワークへの接続の禁止

パソコンやモバイル端末等を、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。

（７）コンピュータウィルス対策

メール受信時にコンピュータウィルス等のマルウェア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こと。また、明らかに当消防局を攻撃対象とする標的形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しなければならない

（８）コンピュータウィルスに感染又は感染が疑われる場合

コンピュータウィルスの感染又は感染が疑われる場合は、ＬＡＮケーブルの即時取り外し及び無線機能の無効化を行うこと。

７　約款による外部サービスの利用について

約款による外部サービス（ＬＩＮＥ等の無料通信アプリなど）を業務で利用する場合は、利用する外部サービスに関する規定及び関係省庁からの通知等を踏まえたうえで利用すること。また、当該サービスの利用において、個人情報等の自治体機密性２以上の情報資産を取り扱ってはならない。

８　事故・欠陥等の報告について

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作動を発見した場合は、速やかに情報セキュリティ管理者及び情報セキュリティに関する窓口（情報システム担当）に報告すること。また、情報システム担当は、速やかに当該報告に対応しなければならない。

なお、事故等の対応は、「消防局情報セキュリティ緊急時対応計画」に基づいて実施すること。

９　ポリシー違反に対する罰則について

セキュリティポリシーに違反した場合は、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。