

情報セキュリティ対策基準

- 第 1 情報資産に対するセキュリティ侵害が発生した場合又はセキュリティ侵害のおそれがある場合には、市に速やかに報告を行い、指示を仰ぐこと。
- 第 2 業務上必要のない情報入手、作成、保管及び利用しないこと。
- 第 3 電子メールにより情報を送信する場合、パスワード等による暗号化を適切に行うこと。
- 第 4 原則として電磁的記録媒体等を業務に使用してはならない。ただし、業務上必要な場合は、館長の許可を得て、次に掲げる事項を含めた実施手順を整備すること。
- (1) 電磁的記録媒体の管理方法
 - (2) 電磁的記録媒体の利用管理方法
 - (3) 実施状況の確認
- 第 5 業務以外の目的で情報資産の外部への持ち出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスを行ってはならない。
- 第 6 定期的に情報セキュリティに関する研修及び訓練を実施すること。
- 第 7 情報セキュリティインシデントを認知した場合は、速やかに市に報告すること。
- 第 8 有線によるネットワークの構築が困難であり、かつ、LANの安全が確保されると認めた場合に限り、無線によるネットワークを構築し利用することができる。
- 第 9 無線 LAN の構築を認めるときは、解読が困難な暗号化及び認証技術の使用等により、情報セキュリティの確保のための必要な措置を講じなければならない。

第 10 ウェブの利用に当たって、次に掲げる行為を行ってはならない。

- (1) ウェブへの情報資産の漏えい
- (2) ウェブの情報の改ざん、損傷及び滅失
- (3) ウェブへの虚偽の情報提供
- (4) ウェブへの公序良俗に反する内容、他人を誹謗中傷する内容、若しくは特定個人の名誉を棄損する内容等の情報発信
- (5) 関係法令で認められたものや本人の了承を得られたものの以外の個人情報の発信
- (6) 関係法令の趣旨に反する行為
- (7) その他ウェブ利用に支障を及ぼすおそれのある行為

第 11 ソーシャルメディアサービスを利用する場合は、情報発信のなりすまし対策及び不正アクセス対策を整備すること。また、利用するソーシャルメディアサービスごとの責任者を定めること。

第 12 不正プログラム対策に関し、次の事項を措置しなければならない。

- (1) その所掌するサーバ及びパソコン等の端末に、コンピュータウイルス等の不正プログラム対策ソフトウェアを常駐させなければならない。
- (2) 不正プログラム対策ソフトウェアのパターンファイルは、常に最新の状態に保たなければならない。
- (3) 不正プログラム対策ソフトウェアは、常に最新の状態に保たなければならない。
- (4) インターネットに接続していないシステムにおいては、コンピュータウイルス等の感染を防止するため、原則として電磁的記録媒体を利用してはならない。

- (5) 外部からデータ又はソフトウェアを取り入れる場合には、必ず不正プログラム対策ソフトウェアによるチェックを行わなければならない。
- (6) 差出人が不明な、又は不自然にファイルが添付された電子メールを受信した場合は、速やかに削除しなければならない。
- (7) 端末に対して、不正プログラム対策ソフトウェアによるフルチェックを定期的の実施しなければならない。
- (8) 添付ファイルが付いた電子メールを送受信する場合は、不正プログラム対策ソフトウェアによりチェックを行わなければならない。
- (9) コンピュータウイルス等の不正プログラムに感染した場合又は感染が疑われる場合は、LANケーブルの即時取り外し、通信を行わない設定への変更又は機器の電源遮断を行わなければならない。その場合は、直ちに市へ報告すること。