

桶川市情報セキュリティポリシー基本方針

1 目的

桶川市情報セキュリティ基本方針は、桶川市の情報セキュリティ対策の基本的な方針として情報セキュリティの対象、位置付け等を決め、桶川市の所有する情報資産を様々な脅威から防御し、その機密性、完全性、可用性を維持することを目的として策定されるものである。

2 適用範囲

(1) 行政機関の範囲

本基本方針が適用される行政機関は、次のとおりとする。

- ア 市長部局
- イ 会計機関
- ウ 議会事務局
- エ 各行政委員（会）事務局
- オ 各教育機関（小中学校を除く。）

(2) 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

- ア ネットワーク、情報システム及びこれらに関する設備並びに電磁的記録媒体
- イ ネットワーク及び情報システムで取り扱う情報（これらを印刷した文書を含む。）
- ウ 情報システムの仕様書、ネットワーク図等のシステム関連文書

3 定義

(1) ネットワーク

コンピュータを相互に接続するための通信網及びその附帯設備で構成される仕組みの総称をいう。

(2) 情報システム

コンピュータ、ネットワーク及び記録媒体で構成され、情報処理を行う仕組みをいう。

(3) 情報資産

情報及び情報システムの総称をいう。

(4) 機密性

情報にアクセスすることを認められた者だけが、情報にアクセスできる状態を確保することをいう。

(5) 完全性

情報が破壊、改ざん又は消去されていない状態を確保することをいう。

(6) 可用性

情報にアクセスすることを認められた者が、必要なときに中断されることなく情報にアクセスできる状態を確保することをいう。

(7) 情報セキュリティ

情報資産の機密の保持、正確性及び完全性の維持並びに定められた範囲での利用可能な状態を維持することをいう。

(8) 脅威

情報資産に対して障害や損害を与える原因となるものをいう。

(9) 脆弱性^{ぜい}

情報資産を安全に管理する上でのシステムや管理上の不備をいう。

(10) リスク

脅威が発生して脆弱性と一体となり情報資産に対して損害や障害が発生させる確率をいう。

(11) マイナンバー利用事務系（個人番号利用事務系）

個人番号利用事務（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

(12) LGWAN接続系

人事給与、財務会計及び文書管理等LGWANに接続された情報システム及びその情報システムで取り扱うデータをいう（マイナンバー利用事務系を除く。）。

(13) インターネット接続系

インターネットメール、ホームページ管理システム等に関わるインターネットに接続された情報システム及びその情報システムで取り扱うデータをいう。

(14) 通信経路の分割

LGWAN接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

(15) 無害化通信

インターネットメール本文のテキスト化や端末への画面転送等により、コンピュータウイルス等の不正プログラムの付着がない等、安全が確保された通信をいう。

4 桶川市情報セキュリティポリシーの位置付け

桶川市情報セキュリティポリシーは、桶川市のセキュリティ対策の頂点に位置するものであり、桶川市の情報政策に関する意思決定は、桶川市情報セキュリティポリシーに違反するものであってはならない。また、すべての管理職は、職員に対し、桶川市情報セキュリティポリシーに違反する行為を命じてはならない。

5 適用対象職員の義務

安全対策の実施には、全ての職員が参加しなければならない。また、情報セキュリティの重要性に対しての共通の認識を持つとともに業務の遂行に当たって桶川市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（以下「実施手順」という。）を遵守する義務を負うものとする。

6 情報セキュリティ管理体制

桶川市の情報資産について、市長のトップダウンの下、情報セキュリティ対策

を推進・管理するための全庁的な体制を確立するものとする。

7 情報資産の分類

桶川市の所有する情報資産をその内容に応じて分類し、その重要度に応じた適正な情報セキュリティ対策を行うものとする。

8 情報資産への脅威

桶川市の情報資産に対する脅威については、その発生の度合いや発生した場合の影響を十分に考慮して認識するものとする。

9 情報セキュリティ対策

脅威から情報資産を保護するために、以下の情報セキュリティ対策を講じる。

(1) 組織体制

桶川市の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立する。

(2) 情報資産の分類と管理

桶川市の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類に基づき情報セキュリティ対策を実施する。

(3) 情報システム全体の強靱性の向上

情報システム全体に対し、次の三段階の対策を講じる。

ア マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

イ LGWAN接続系においては、LGWANと接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

ウ インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、インターネット接続口を集約する自治体情報セキュリティクラウドの導入等を実施する。

(4) 物理的セキュリティ

サーバ、情報システム室、通信回線、職員等のパソコン等の管理について、物理的な対策を講じる。

(5) 人的セキュリティ

情報セキュリティに関し、職員等が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の人的な対策を講じる。

(6) 技術的セキュリティ

コンピュータ等の管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的対策を講じる。

(7) 運用

情報システムの監視、情報セキュリティポリシーの遵守状況の確認、外部委託

を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産に対するセキュリティ侵害が発生した場合等に迅速かつ適正に対応するため、緊急時対応計画を策定する。

(8) 業務委託と外部サービス（クラウドサービス）の利用

業務委託を行う場合には、委託事業者を選定し、情報セキュリティ要件を明記した契約を締結し、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確認し、必要に応じて契約に基づき措置を講じる。

外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定し、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。

10 情報セキュリティ対策基準の策定

桶川市の様々な情報資産について、情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した「情報セキュリティ対策基準」（以下、「対策基準」という。）を策定するものとする。なお、対策基準は、行政の運営に関する重要情報であり、情報セキュリティの観点から非公開とする。

11 情報セキュリティ実施手順の策定

対策基準を遵守し、情報セキュリティ対策を実施するために、個々の情報資産の対策手順等をそれぞれ定めていく必要がある。そのため、個々の情報資産に対して、対策基準に沿って具体的な実施手順を明記した実施手順を策定するものとする。なお、実施手順は、行政の運営に関する重要情報であり、情報セキュリティの観点から非公開とする。

12 情報セキュリティ監査の実施

桶川市情報セキュリティポリシーが遵守されていることを検証するため、定期的又は必要に応じて情報セキュリティ監査及び自己点検を実施する。

13 法令の遵守

職員、非常勤職員、臨時職員及び契約により操作を許可された者は、桶川市情報セキュリティポリシーを遵守するとともに、セキュリティに関する他の法令等を遵守する義務を負う。

14 評価及び見直しの実施

情報セキュリティ監査の結果等により、桶川市情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施するとともに、情報セキュリティを取り巻く状況の変化に対応するために、適宜、桶川市情報セキュリティポリシーの見直しを実施する。