古河市情報セキュリティポリシー

平成 17 年 9 月 12 日　策定
平成 20 年 4 月　　全部改正
平成 22 年 8 月　　一部改正
令和元年 12 月　　一部改正
令 和 6 年 3 月　　一部改定
古　　河　　市
古河市情報セキュリティ委員会

情報セキュリティ及び特定個人情報の安全管理に関する基本方針

1. 目的

本基本方針は、本市が保有する情報資産の機密性、完全性及び可用性を維持するため、本市が実施する情報セキュリティ対策について、基本的な事項を定めるとともに、特定個人情報の適正な取扱いを確保するため、市が講ずる安全管理措置の基本的な事項を定めることを目的とする。

2. 定義

本書における用語の意義は、行政手続きにおける特定の個人を識別する番号の利用等に関する法律（平成 25 年法律第 27 号。（以下「番号法」という。）及び古河市個人情報保護条例（平成 17 年条例第 20 号）において使用する用語の例によるほか、巻末の「用語解説／索引」にて定義する。

3. 対象とする脅威

情報資産に対する脅威として、以下の脅威を想定し、情報セキュリティ対策を実施する。

（1）不正アクセス、ウイルス攻撃、サービス不能攻撃（DoS 攻撃及び DDoS 攻撃)、標的型攻撃、ランサムウェア等のサイバー攻撃や部外者の侵入等の意図的な要因による情報資産の漏えい・破壊・改ざん・消去、重要情報の詐取、内部不正等

（2）情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計・開発の不備、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、内部・外部監査機能の不備、委託管理の不備、マネジメントの欠陥、機器故障等の非意図的要因による情報資産の漏えい・破壊・消去等

（3）地震、落雷、火災等の災害によるサービス及び業務の停止等

（4）大規模・広範囲にわたる疾病による要員不足に伴うシステム運用の機能不全等

（5）電力供給の途絶、通信の途絶、水道供給の途絶等のインフラ障害からの波及等

4. 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、内部部局、行政委員会、議会事務局及び地方公営企業とする。

（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。

①ネットワーク、情報システム及びこれらに関する設備・電磁的記録媒体

②ネットワーク、情報システムで取り扱う情報及びこれらを印刷した文書

③情報システムの仕様書及びネットワーク図等のシステム関連文書

④番号法及び古河市行政手続における特定の個人を識別するための番号の利用等に関する法律に基づく個人番号の利用及び特定個人情報の提供に関する条例（平成 27 年条例第 42 号。以下「番号条例」という。）に基づき、市が取り扱う特定個人情報

5.特定個人情報の安全管理措置

市は、特定個人情報の適正な取り扱いを確保するため、上記3の脅威に対する情報セキュリティ対策を実施するほか、特定個人情報に係る次に掲げる事項その他の適切な管理のために必要な措置を講ずるものとする。

①漏えい、滅失及び毀損の防止

②番号法及び番号条例に定められた事務のうち、あらかじめ本人に通知した利用目的の達成に必要な範囲内での適正な収集、保管、利用及び提供並びに不要となった際の速やかな廃棄

③目的外利用の防止

6. 職員等の遵守義務

職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシー及び情報セキュリティポリシー実施手順を遵守しなければならない。

7. 情報セキュリティ対策

上記2.3の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

本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

本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行う。

（３）情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三層の対策を講じる。

①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。

②LGWAN端末系においては、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。

③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、都道府県及び市区町村のインターネットとの通信を集約した上で、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

サーバ等、情報システム室等、通信回線等及び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、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切に対応するため、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する。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ずる。

外部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、発信する情報の担当課室長等を責任者として定める。

（9）評価・見直し

情報セキュリティポリシーの遵守状況を検証するため、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し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

8. 情報セキュリティ監査及び自己点検の実施

情報セキュリティポリシーの遵守状況を検証するため、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。

9. 情報セキュリティポリシーの見直し

情報セキュリティ監査及び自己点検の結果、情報セキュリティポリシーの見直しが必要となった場合及び情報セキュリティ対策並びに特定個人情報の安全管理に関する状況の変化に対応するため新たに対策が必要になった場合には、情報セキュリティポリシーを見直す。

10. 情報セキュリティ対策基準の策定

上記 2.7、2.8 及び 2.9 に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める情報セキュリティ対策並びに特定個人情報の安全管理に関する基準を策定する。

11. 情報セキュリティ実施手順の策定

情報セキュリティ対策及び特定個人情報の安全管理に関する基準に基づき、情報セキュリティ対策を実施するための具体的な手順を定めた情報セキュリティ実施手順を策定するとともに特定個人情報の適正な取り扱いを確保するための実施手順を策定するものとする。なお、情報セキュリティ実施手順は、公にすることにより、本市の行政運営に重大な支障を及ぼすおそれがあることから非公開とする。