安中市情報セキュリティ基本方針

（第2.2版）

令和8年3月13日

安中市

◇策定・改訂履歴

◇策定・改訂履歴版数	策定・改訂年月日	内容
第2.0版	平成28年2月18日	第2.0版
第2.1版	令和4年4月1日	機構の変更による名称等の変更
第2.2版	令和8年3月13日	情報セキュリティに関する庁内外の状況の変化等を踏まえ変更

目次

1. 目的

安中市が取り扱う情報には、市民の個人情報をはじめ行政運営上重要な情報など、外部に漏えいした場合には極めて重大な結果を招く情報が多数含まれている。

これらの本市が所管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の基本的な方針を定めることを目的とする。

ただし、特定個人情報に関する情報セキュリティ対策は別途定める。

2. 用語の定義

（1）情報資産

本基本方針においては、以下の各号を情報資産という。

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）

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

（2）情報セキュリティ

情報資産の機密性、完全性及び可用性を維持することをいう。

（3）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。

（4）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。

（5）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。

（6）ネットワーク

コンピューター等を相互に接続するための通信網、その構成機器（ハードウェア及びソフトウェア）をいう。

（7）情報システム

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

（8）情報セキュリティポリシー

安中市情報セキュリティ基本方針及び安中市情報セキュリティ対策基準をいう。

（9）マイナンバー利用事務系（基幹系）

個人番号利用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。

（10）LGWAN接続系

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。

（11）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。

（12）教育系

地方公共団体が設置する学校の管理運営に係る事務を担う執行機関もしくは学校が掌握するネットワーク、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。

（13）通信経路の分割

LGWAN接続系と他の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。

（14）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無い等、安全が確保された通信をいう。

3. 情報セキュリティポリシーの構成

情報セキュリティポリシーは、本市が所管する情報資産に関する情報セキュリティ対策を総合的かつ体系的に取りまとめたものである。

情報セキュリティポリシーに基づき、具体的な情報セキュリティ対策の実施手順を示す情報セキュリティ実施手順を策定するものとする。

なお、教育委員会は、教育情報セキュリティ対策に関して、独自に教育情報セキュリティ対策基準を定め、当該基準に則って運用を行うものとする。

情報セキュリティポリシーの構成

文署名		内容
情報セキュリティポリシー	安中市情報セキュリティ基本方針	安中市が所管する情報資産に関する情報セキュリティ対策の統一的かつ基本的な方針。
	安中市情報セキュリティ対策基準	安中市情報セキュリティ基本方針に基づき、情報セキュリティ対策を統一的に実施するために本市の職員等が遵守すべき行為及び判断等の基準。
情報セキュリティ実施手順		情報セキュリティポリシーに基づき、本市の職員等が遵守すべき情報セキュリティ対策の実施手順を具体的に規定するもの。全庁的に共通する情報資産の取り扱いを定める実施手順と情報システムごとに取り扱いを定める実施手順を策定する。

（参考：特定個人情報等に関する情報セキュリティ関連規程）

特定個人情報に関する情報セキュリティ対策は下記に定める。

・安中市特定個人情報等の安全管理に関する基本方針

・安中市特定個人情報取扱規程

4. 対象とする脅威

本市は情報資産に対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）サイバー攻撃をはじめとする部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃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、外部委託管理の不備、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提供サービスの障害からの波及等

5. 適用範囲

情報セキュリティポリシーの適用範囲を以下の各号に示す。

(1)機関の範囲

市長、議会、選挙管理委員会、監査委員、公平委員会、農業委員会、固定資産評価審査委員会及び教育委員会とする。

(2)対象者の範囲

上記(1)の機関に所属する本市の職員(非常勤職員、会計年度任用職員等を含む。)及び学校事務に携わる群馬県職員(以下「職員等」という。)とする。

(3)情報資産の範囲

本市が所管する情報資産とする。ただし、公立碓氷病院の所掌する医療・介護業務に供する情報は除く。

(4)適用範囲外の対応

公立碓氷病院は、情報セキュリティポリシーに準じた情報セキュリティ対策を講じることに努める。

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、業務の遂行にあ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4の脅威から本市が所管する情報資産を保護するため、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

本市が所管する情報資産を重要度に応じて区分し、当該区分に応じた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化の向上

情報セキュリティの強化を目的とし、業務の効率化・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を実施する。

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により、住民情報の流出を防ぐ。

②LGWAN接続系においては、LGWANと接続する業務用システムと他の接続系の情報システムとの通信経路を分割する。なお、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、群馬県及び県内市町村のインターネットとの通信を集約した上で、群馬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教育系においては、地方公共団体の他の行政事務とは異なる特徴を有することから、文部科学省にて策定されている「教育情報セキュリティポリシーに関するガイドライン」を基に情報システム全体の強靭性の向上を図る。

（4）物理的セキュリティ対策

情報システムの設置場所、情報資産の保管場所等への不正な立入り、情報資産の損傷及び利用の妨害等から保護するための物理的な対策を講じる。

（5）人的セキュリティ対策

職員等の情報セキュリティに関する権限や責任等を定めるとともに、職員等が遵守すべき事項を周知徹底するため、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対策

コンピューター等の管理、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）運用面におけるセキュリティ対策

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など情報セキュリティポリシーの運用面の対策を講じる。

また、本市が所管する情報資産への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。

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に関する状況の変化に対応するために新たな対策が必要になった場合は、情報セキュリティポリシーの見直しを実施する。

10. 安中市情報セキュリティ対策基準の策定

上記7、8及び9に規定する対策等を実施するため、具体的な遵守事項及び判断基準等を定める安中市情報セキュリティ対策基準を策定する。

安中市情報セキュリティ対策基準は、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。

11. 情報セキュリティ実施手順の策定

情報セキュリティポリシーに基づき、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。

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。

附則
本基本方針は、平成 24 年 2 月 1 日から施行する。
附則
本基本方針は、平成 24 年 11 月 6 日から施行する。
附則
本基本方針は、平成 28 年 2 月 18 日から施行する。
附則
本基本方針は、令和 4 年 4 月 1 日から施行する。
附則
本基本方針は、令和8年 4 月 1 日から施行する。