【井原市情報セキュリティポリシー】

井原市

令和８年３月

はじめに

情報セキュリティポリシーとは、井原市が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的かつ具体的に取りまとめたものを総称する。情報セキュリティポリシーは、本市が所掌する情報資産に関する業務に携わる全職員、会計年度任用職員（以下「職員等」という。）に浸透、普及、定着させるものであり、安定的な規範であることが要請される。しかしながら一方では、技術の進歩等に伴う情報セキュリティを取り巻く急速な状況の変化へ柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた部分（基本方針）と情報資産を取り巻く状況の変化に即した対策を規定する部分（対策基準）に分けて策定することとする。具体的には、情報セキュリティポリシーを、「情報セキュリティ基本方針」及び「情報セキュリティ対策基準」の二階層に分け、それぞれを策定することとする。

■　情報セキュリティ基本方針

【 情報セキュリティ基本方針 】

1　目的

井原市の各情報システムが取り扱う情報には、市民の個人情報のみならず行政運営上機密として保持すべき情報など、外部に漏えい等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。したがって、これらの情報及び情報を取り扱う情報システムを様々な脅威から防御することは、市民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。さらには、このことが本市に対する市民からの信頼の維持向上にも寄与するものである。

また、近年のデジタルトランスフォーメーションの進展により、オンライン手続きや地域のデジタル化による住民サービスの向上が期待されているところである。本市がこれらに積極的に対応するためには、全てのネットワーク及び情報システムが信頼性を保ちつつ、より高度な安全性を確保することが不可欠な前提条件である。

そのため、本市の情報資産の機密性、完全性及び可用性*を維持するための対策(情報セキュリティ対策)を整備するために井原市情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については本市の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

＊（注）：国際標準化機構（ISO）が定めるもの（ISO7498-2：1989）
機密性（confidentiality）　：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。
完全性（integrity）　：情報及び処理の方法の正確さ及び完全である状態を保護すること。
可用性（availability）　：許可された利用者が必要なときに情報にアクセスできることを確実にすること。

2　定義

(1)　ネットワーク

コンピュータを相互に接続し情報を交換するための通信回線網、その構成機器（ハードウェア及びソフトウェア）をいう。

(2)　情報システム

コンピュータ、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。

(3)　情報資産

本市業務で取り扱う情報システム及び情報システムで取り扱うデータ、申請書等の紙媒体を含む全てのデータをいう。

(4)　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。

(5)　情報セキュリティポリシー

本基本方針及び情報セキュリティ対策基準、業務ごとに作成される取扱手順をいう。

(6)　マイナンバー利用事務系

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取り扱う領域をいう。

(7)　総合行政ネットワーク（以下、LGWAN という。）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のデータを取り扱う領域をいう（マイナンバー利用事務系を除く。）。

(8)　インターネット接続系

マイナンバー利用事務系及び LGWAN 接続系以外のデータを取り扱う領域であり、インターネットメール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等をいう（マイナンバー利用事務系を除く。）。

(9)　三層分離

マイナンバー利用事務系、LGWAN 接続系とインターネット接続系の 3 つの領域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。

(10)　無害化通信

インターネット接続系で取得したデータを LGWAN 接続系で利用する際に、データの安全性を確保しながら転送することをいう。例として、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転送方法等が挙げられる。

(11)　クラウドサービス

インターネットなどのコンピュータネットワークを経由して、コンピュータ資源をサービスの形で提供する利用形態をいう。

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の障害からの波及等

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、市長部局、行政委員会、消防組合、議会事務局、地方公営企業及び市長が必要と認めた行政機関とする。ただし、各行政機関において独自に策定している場合はこの限りではない。

(2)　本市が保有する情報資産の範囲

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　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

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及びネットワーク図等のシステム関連文書

5　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を遵守する義務を負うものとする。

6　情報セキュリティ対策

情報資産を脅威から保護するため、以下の情報セキュリティ対策を講じる。

(1)　組織体制

本市の情報資産について、情報セキュリティ対策を推進するため、責任及び権限を明確にした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その内容並びに機密性、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靭性の向上

情報資産を脅威から保護するため、次の３段階の対策を講じ、より強靭にする。

ア　　マイナンバー利用事務系においては、原則として、他の領域との通信が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、無害化通信及び同等の保全策を実施する。

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、都道府県及び市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、情報システム室、執務室、保管庫及び通信回路における設備並びに職員のパソコン等の管理については、情報資産の損傷・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

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、必要かつ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及び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及び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。

(8)　外部サービスの利用

外部委託する場合には、外部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、外部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。

約款による外部サービスを利用する場合には、利用にかか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。

(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。

7　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。

8　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新たに対策が必要になった場合には、保有する情報及び利用する情報システムに係る脅威の発生の可能性及び発生時の損失等を分析し、リスクを検討したうえで、情報セキュリティポリシーを見直す。

9　情報セキュリティ対策基準の策定

上記６、７及び８に規定する対策を実施するために、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基準を策定する。

１０　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。

適用日

この基本方針は、平成 17 年 12 月 9 日から適用する。

改版したこの基本方針は、平成 29 年 4 月 1 日から適用する。

改版したこの基本方針は、令和 4 年 4 月 1 日から適用する。

改版したこの基本方針は、令和 5 年 12 月 1 日から適用する。

改版したこの基本方針は、令和 8 年 4 月 1 日から適用する。