
いすみ市情報セキュリティポリシー

情報セキュリティ基本方針

1. 目的

いすみ市の情報システムが取り扱う情報には、市民の個人情報や行政運営上重要な情報が多数含まれており、情報資産を人的脅威や災害、事故等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、継続的かつ安全・安定的な行政サービスの実施を確保するためにも必要不可欠である。

このため、いすみ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ことを目的としていすみ市情報セキュリティ基本方針を定める。いすみ市の情報資産に関する情報セキュリティ対策の基本的な考え方と方針を規定するものである。

2. 定義

(1) 情報資産

紙の資料、書類に記載されている情報から、コンピュータ等で作成しサーバや記録媒体に保存しているデータまで、記録の形態や保管場所を問わず、すべての情報をいう。

(2) ネットワーク

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

(3) 情報システム

コンピュータ等、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。

(4) データ

コンピューターで処理されるデジタル情報。電子計算機処理に係る入出力帳票、磁気テープ、磁気ディスク、光ディスクその他の記録媒体に記録されている情報又は通信回線により送信される情報をいう。

(5) 情報セキュリティ

情報資産を「機密性」、「完全性」、「可用性」に関する脅威から保護することをいう。

(6) 情報セキュリティポリシー

いすみ市情報セキュリティ基本方針（以下「情報セキュリティ基本方針」という）及びいすみ市情報セキュリティ対策基準（以下「情報セキュリティ対策基準」という）をいう。

(7) 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。

(8) 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。

(9) 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。

(10) 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。

(11) 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（マイナンバー利用事務系を除く）。

(12) 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。

(13) 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。

(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。

(15) クラウドサービス

インターネットや閉域網などネットワーク経由でソフトウェア、ミドルウェア、インフラストラクチャーやデータ等を利用するサービス形態をいう。

3. 情報セキュリティポリシーの位置付け及び構成

情報セキュリティポリシーは、いすみ市が保有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かつ体系的に取りまとめた情報セキュリティ対策の基本となるものであり、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から構成される。

情報セキュリティ対策基準は、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等を実施するために最低限必要な水準として、いすみ市長をはじめとした職員、再任用職員、任期付職員、教員、臨時的任用職員、会計年度任用職員、特別職非常勤職員、労働者派遣契約等によりいすみ市業務に従事する者（以下「職員等」という。）が遵守すべき事項及び判断基準をまとめたものである。いすみ市では、組織等の状況に合わせた情報セキュリティ対策基準を策定する。

4. 対象とする脅威

情報セキュリティ対策を講じるうえでは、情報資産に対する脅威の発生度合いや発生した場合の影響を考慮するものとする。特に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、業務委託等の管理の不備、マネジメントの欠陥、機器故障等の非意図的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

5. 適用範囲

(1) 組織の範囲

いすみ市行政組織条例(平成 25 年 3 月 18 日条例第 1 号)第 2 条に規定する課、いすみ市地域市民局設置条例(平成 17 年 12 月 5 日同第 7 号)第 2 条に規定する地域市民局、いすみ市会計管理者の補助組織設置規則(平成 17 年 12 月 5 日規則第 6 号)第

2条に規定する課、いすみ市教育委員会事務局組織規則(平成17年12月5日教育委員会規則第5号)第13条に規定する課、選挙管理委員会事務局、監査事務局、農業委員会事務局及び市議会事務局、ほか行政委員会とする。

(2) 情報資産の範囲

情報セキュリティ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
- 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
- ④ その他、紙等で保存されている情報

⑤ 情報資産の対象

いすみ市が実施する業務で扱う情報資産を市の情報資産として本基本方針の対象とする。

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つとともに、業務の遂行にあたっては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) 情報セキュリティ管理体制

いすみ市の情報資産について、適切に情報セキュリティ対策を推進・管理するため、全庁的な組織体制を確立するための必要な体制、役割、権限等については情報セキュリティ対策基準にて定める。

(2) 情報資産の分類と管理

いすみ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講じる。

(3) 情報システム全体の強靱性の向上

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、情報資産の分類に応じた情報セキュリティ対策を講じるとともに、次の対策も併せて講じる。

- 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。
- ② 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、無害化通信を行う。
- 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。

(4) 物理的セキュリティ

コンピュータ設置場所への入退室、サーバ等の管理、通信回線及び端末等へ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、十分な研修・訓練及び啓発を実施するなど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、コンピュータウイルス等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、業務委託等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、情報セキュリティインシデント発生時の対応手順書を策定する。

(8) 業務委託等及び外部サービスの利用

業務委託等をする場合には、業務委託事業者等を選定し、情報セキュリティ要件を明記した契約を締結し、業務委託事業者等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、外部サービス利用基準を整備し対策を講じる。

8. 情報セキュリティ監査及び自己点検の実施

情報セキュリティ対策の実施状況を評価するため、定期的及び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7、8及び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基準を策定する。なお、情報セキュリティ対策基準は、公にすることによりいすみ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. 情報セキュリティ個別基準の策定

情報セキュリティ対策基準を参照し補完するために必要な内容に関して、具体的な内容を定める情報セキュリティ個別基準を策定するものとする。なお、情報セキュリティ個別基準は、公にすることによりいすみ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。

12. 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及び情報セキュリティ個別基準に基づき、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、情報セキュリティポリシー及び情報セキュリティ実施手順は、公にすることによりいすみ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。