Ⅲ

いわき市情報セキュリティ基本方針

いわき市長・水道事業管理者・病院事業管理者・いわき市議会

目　　次

いわき市情報セキュリティ基本方針

第１　目的

本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重要な情報など、部外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おり、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。

このため、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を整備するため、いわき市情報セキュリティポリシー（以下「市情報セキュリティポリシー」という。）を定めることとし、このうち、いわき市情報セキュリティ基本方針（以下「基本方針」という。）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、市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）

＜情報セキュリティの３要素＞

機密性：　許可された者だけが情報にアクセスでき、許可を受けていない者は情報にアクセスできない状態を確保すること。

完全性：　情報及び処理の方法が正確であり、破壊、改ざんまたは消去されていない完全な状態を確保すること。

可用性：　許可された者が、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。

第２　用語の定義

１　情報システム

電子計算組織やネットワーク、電磁的記録媒体で構成された、情報処理または通信に用いる仕組みをいう。

２　電子データ

情報システムや電磁的記録媒体により処理または保管されるすべての電子的な情報をいう。

３　ネットワーク

電子計算組織を相互に接続するための通信回線網及びその構成機器をいう。

４　電子計算組織

与えられた一連の処理手順に従い、事務を自動的に処理する電子的機器の組織をいい、一般的にホストコンピュータ、サーバ、パソコン、端末等をいう。

５　記録媒体

ハードディスク、フロッピーディスク、CD-ROM、磁気テープ等電子データを記録するための電磁的記録媒体及び情報システムから出力された紙媒体をいう。

６　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。

７　ソーシャルメディア

インターネット上の Web サービスの一種で、サービス利用者間で双方向のコミュニケーションを可能とするものをいう。

８　アカウント

利用するサービスにログインするための利用者権限をいう。

９　マイナンバー利用事務系

マイナンバー利用事務（社会保障、地方税若しくは防災に関する事務）また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（マイナンバー利用事務系を除く。）。

１１　インターネット接続系

インターネットメール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　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。

１３　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、コンピュータウィルス（以下「ウィルス」という。）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。

１４　クラウドサービス

インターネットを通じて、データの保存やソフトウェア等の機能を利用できるサービスをいう。

第３　市情報セキュリティポリシーの位置付け

市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について、総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティ対策の最上位に位置するものである。

また、基本方針は、地方自治法第 244 条の６第１項で定めるサイバーセキュリティを確保するための方針として位置付けるものとする。

第４　対象とする脅威

情報資産（基本方針第５－３）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、ウィルス攻撃、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

第５　適用範囲

市情報セキュリティポリシーが適用される範囲は次のとおりとする。

１　行政機関の範囲

基本方針が適用される行政機関は、市長部局、選挙管理委員会、監査委員、公平委員会、農業委員会、教育委員会、消防本部、地方公営企業及び議会とする。

２　職員等の範囲

市情報セキュリティポリシーが適用される者は、本市が所管する情報資産の生成、運用、管理及び利用に携わる者（以下「職員等」という。）であり、次のとおりとする。

（１）　地方公務員法（昭和２５年法律第２６１号）第３条に定める本市の地方公務員

（２）　学校教育法（昭和２２年法律第２６号）第２８条及び第４０条に定める本市の小学校及び中学校の校長、教頭、教諭、養護教諭、事務職員等

（３）　学校給食法（昭和２９年法律第１６０号）第５条３に定める本市の小学校及び中学校の学校栄養職員

（４）　契約、協定等により操作等を認められた者

３　情報資産の範囲

市情報セキュリティポリシーが対象とする情報資産は次のとおりとする。

（１）　本市が所管する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記録媒体

（２）　本市が所管するネットワーク及び情報システムで取扱う情報（これらを印刷した紙媒体を含む）

（３）　本市が所管する情報システムの仕様書及びネットワーク図等の情報システム関連文書

第６　職員等の義務

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、業務の遂行において、情報セキュリティに関係する法令等及び市情報セキュリティポリシー、情報セキュリティ実施手順を遵守しなければならない。

第７　情報セキュリティ管理体制

情報資産の統一的な情報セキュリティを確保するため、全庁的な組織体制を整備する。

第８　情報資産の管理及び分類

情報資産については、情報の機密性、完全性及び可用性等を踏まえた情報資産の分類を行い、その重要性に応じ、適切な管理を行うものとする。

第９　情報セキュリティ対策

情報資産を、対象とする脅威から守るとともに、万一災害や情報流出等が発生した場合に被害を最小限に止めるため以下の対策を講じる。

１　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、次の三段階の対策を講じる。

（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。

（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、自治体情報セキュリティクラウドへの参加等を実施する。

２　物理的情報セキュリティ対策

情報資産において、設備的あるいは物理的な対策を講じる。

３　人的情報セキュリティ対策

情報セキュリティに関する権限や責任及び遵守すべき事項を明確に定め、職員等に対する周知及び徹底を図るとともに、十分な教育、啓発が行われるよう必要な対策を講じる。

４　技術的情報セキュリティ対策

情報資産を不正なアクセス等から保護するため、情報資産へのアクセス制御、ネットワーク管理、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。

５　運用における情報セキュリティ対策

情報システムの監視、情報セキュリティ対策の遵守状況の点検、委託を行う際の情報セキュリティの確保等、情報セキュリティの運用面での対策を講じる。

６　緊急時における情報セキュリティ対策

災害や情報流出事故等により情報資産に損害等、緊急事態が発生した場合に、被害を最小限に抑えることを第一に、迅速かつ適切な対応が可能となるような危機管理対

策の整備等の対策を講じる。

７　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。

第１０いわき市情報セキュリティ対策基準の策定

基本方針に基づき、情報セキュリティ対策を実施するに当たっての遵守すべき事項や、判断等の統一的な基準として、いわき市情報セキュリティ対策基準（以下「対策基準」という。）を定めるものとする。

第１１情報セキュリティ実施手順の策定

基本方針及び対策基準に基づき、個々の情報システムについて情報セキュリティ対策を具体的に実施するために、情報セキュリティ実施手順（以下「実施手順」という。）を情報システムごとに定めるものとする。

第１２対策基準及び実施手順の扱い

対策基準及び実施手順について、公にすることにより本市の情報セキュリティ対策に重大な支障を及ぼす恐れのある内容は、非公開とする。

第１３情報セキュリティ監査の実施

情報セキュリティ対策が遵守されていることを確認及び検証するため、定期的に情報セキュリティ監査（以下「監査」という。）を実施する。

第１４評価及び見直しの実施

監査の結果等により、基本方針及び対策基準に定める事項並びに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等を踏まえ、基本方針、対策基準及び実施手順の見直しを実施する。

第１５市情報セキュリティポリシー等違反への対応

基本方針及び対策基準等関係規定に違反した者については、その重大性、発生した事案の状況等に応じて情報資産の使用停止措置あるいは懲戒処分等の対象とする。

附　則

この基本方針は、平成１５年２月１７日から施行する。

附　則

この基本方針は、平成１８年４月１日から施行する。

附　則

この基本方針は、平成１９年１１月１４日から施行する。

附　則

この基本方針は、平成２２年４月１日から施行する。

附　則

この基本方針は、平成２６年７月１日から施行する。

附　則

この基本方針は、令和２年４月１日から施行する。

附　則

この基本方針は、令和４年４月１日から施行する。

附　則

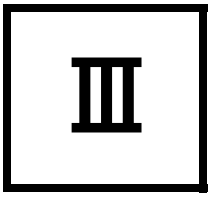
この基本方針は、令和５年４月１日から施行する。

附　則

この基本方針は、令和７年４月１日から施行する。

附　則

この基本方針は、令和８年３月31日から施行する。


III