大田原市情報セキュリティポリシー

（基本方針）

平成２８年３月　策定
令和　６年３月　改定
令和　８年３月　改定

大田原市長
大田原市水道事業管理者
大田原市下水道事業管理者
大田原市議会議長
大田原市代表監査委員
大田原市選挙管理委員会委員長
大田原市公平委員会委員長
大田原市固定資産評価審査委員会委員長
大田原市農業委員会会長
大田原市教育委員会

目次

○　大田原市情報セキュリティポリシーについて

大田原市情報セキュリティポリシー（以下「情報セキュリティポリシー」という。）は、本市が保有する情報資産について、その機密性・完全性・可用性を確保するため、情報セキュリティに関する基本的な考え方、体制および具体的な対策を包括的に定めるものである。

情報通信技術の高度化・業務のデジタル化の進展に伴い、本市が取り扱う情報資産は年々増加・高度化しており、その価値と同時に、漏えい、不正利用、改ざん、サービス停止等のリスクも増大している。ひとたび情報セキュリティ事故が発生した場合、市民の権利利益を侵害するおそれがあるだけでなく、市政に対する信頼の失墜や行政サービスの継続に重大な支障を及ぼす結果となる。

加えて、情報セキュリティ対策は、個人情報保護対策と不可分の関係にあり、個人情報の適正な取扱いを確保するためには、組織的かつ体系的な情報セキュリティ対策の実施が不可欠である。法令等において求められている安全管理措置についても、単なる形式的な対応では不十分であり、組織全体として統一された考え方と基準の下で実施される必要がある。

したがって、情報セキュリティ対策を実効性あるものとするためには、各部署が個別に対応するのではなく、組織として方針を統一し、計画的かつ継続的に推進することが不可欠である。このため、近年の環境変化や新たなリスクを踏まえ、情報セキュリティ対策をより実効性の高いものとするために、本市情報セキュリティポリシーを新たに策定するものである。

情報セキュリティポリシーは、本市における情報セキュリティ対策の最上位に位置づけられるものであり、市長をはじめとする全ての職員等および本市の業務を受託する事業者は、業務の遂行に当たり、これを遵守する義務を負う。

また、情報セキュリティを取り巻く脅威や対策は、技術の進展や社会情勢の変化により常に変化している。このため、情報セキュリティ対策については、策定・導入（Plan）、運用（Do）、評価（Check）、見直し（Action）の四段階からなるPDCAサイクルを継続的に実施し、環境の変化に対応しながら、対策水準の維持および向上を図るものとする。

文書名		内容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策における基本的な考え方
	情報セキュリティ対策基準	「基本方針」に基づき、情報システムに必要となる情報セキュリティ対策の基準
情報セキュリティ実施手順		「対策基準」を、具体的なシステムや手順、手続に展開して個別の実施事項を定めるもの

表１　情報セキュリティポリシーの構成

○　情報セキュリティ基本方針

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ことを目的とする。

２．定義

（１）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、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。

（４）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をいう。

（５）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。

（６）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。

（７）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。

（８）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。

（９）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。）。

（１０）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。

（１１）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。

（１２）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．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、教育委員会（市立小中学校を含む。）、公平委員会、監査委員、農業委員会、固定資産評価審査委員会、水道局、選挙管理委員会及び議会とする。

（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

情報資産の種類	情報資産の例
ア　ネットワーク	通信回線、ルータ等の通信機器等
イ　情報システム	サーバ、パソコン、モバイル端末、汎用機、複合機、オペレーティングシステム、ソフトウェア等
ウ　ア、イに関する施設・設備	サーバ室、コンピュータ室、通信分岐盤、配電盤、電源ケーブル、通信ケーブル等
エ　電磁的記録媒体	サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体、USB メモリ、外付けハードディスクドライブ、DVD―R、磁気テープ等の外部電磁的記録媒体等
オ　ネットワーク及び情報システムで取り扱う情報	ネットワーク、情報システムで取り扱うデータ等（これらを印刷した文書を含む。）
カ　システム関連文書	システム設計書、プログラム仕様書、オペレーションマニュアル、端末管理マニュアル、ネットワーク構成図等

表２　本基本方針が対象とする情報資産の種類と例

５．職員等の遵守義務

行政機関に属するすべての特別職、一般職員及び非常勤職員（以下「職員等」という。）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実施

手順を遵守しなければならない。

６．情報セキュリティ対策

上記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実施する。

（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、サーバ室、通信回線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、業務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正に対応するため、緊急時対応計画を策定する。

（８）業務委託と外部サービス（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。

（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。

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。

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。