昭島市訓令第 3 号

令和　6年　1月２２日

昭島市情報セキュリティ基本方針

（趣旨）

第１条　昭島市（以下「本市」という。）の情報セキュリティ対策について明文化した「昭島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、昭島市情報セキュリティ基本方針（以下「本基本方針」という。）については、情報セキュリティポリシーの対象及び情報セキュリティ対策の基本的な事項を定めるものとする。

（用語の意義）

第２条　本基本方針において、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

（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。

（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　次に掲げるものをいう。

ア　情報システム

イ　情報システムで取り扱う全ての情報（情報システムから紙等の有体物に出力された情報を含む。）

ウ　昭島市文書管理規程（昭和50年昭島市訓令第１号）第２条第１号に規定する文書等

（４）クラウドサービス　事業者によって定義されたインターフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由に管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。

（５）外部サービス　本市以外の者が情報システムの一部又は全部の機能を提供するものをいう。例えば、クラウドサービス、ホスティングサー

ビス、ソーシャルメディアサービス（Social Media Service、以下「ＳＭＳ」という。）等がある。ただし、当該機能を利用して本市の情報が取り扱われる場合に限る。

（６）端末　情報システムの構成要素である機器のうち、職員等が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいう。

（７）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。

（８）セキュリティ侵害　情報漏えい、不正アクセス、ウイルス感染等により本市の事業に著しく支障を与える事象などをいう。

（９）情報セキュリティポリシー　本基本方針及び昭島市情報セキュリティ対策基準をいう。

(10) 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。

(11) 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。

(12) 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。

(13) 職員　本市の特別職及び一般職の全ての職員並びに本市と派遣契約等を締結した上で、本市の業務に従事する者をいう。

(14) 事務取扱担当者　職員のうち、特定個人情報を取り扱う事務を担当する者をいう。

(15) 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）又は戸籍事務等に係る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。

(16) 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。）。

(17) インターネット接続系　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。

(18) 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。

(19) 無害化通信　コンピュータウイルス等の不正プログラムの付着がない等、安全が確保された通信をいう。

（対象とする脅威）

第３条　情報資産に対する脅威として、次に掲げる脅威を想定し、情報セキュリティ対策を講じる。

（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・詐取・盗難・紛失、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・通信・水道供給の途絶等のインフラの障害からの波及等

（適用範囲）

第４条　本基本方針が対象とする情報資産は、本市が所掌する情報資産とする。

２　本基本方針の適用行政組織は、昭島市組織条例（昭和57年昭島市条例第20号）第１条に規定する部、会計課、水道部、昭島市教育委員会事務局処務規則（昭和57年昭島市教育委員会規則第４号）第２条に規定する部、議会事務局、選挙管理委員会事務局、監査事務局、農業委員会事務局とする。

３　本基本方針の適用となる職員は、本市の情報資産を扱う全ての者とする。

（職員の遵守事項）

第５条　職員は、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。

（組織体制）

第６条　本市に最高情報セキュリティ責任者（Chief Information Security Officer、以下「ＣＩＳＯ」という。）を設置する。

２　ＣＩＳＯは、副市長の職にある者をもって充てる。

３　情報セキュリティ対策を組織的かつ効果的に実施する体制について別に

定める。

（情報セキュリティ対策）

第７条　脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講じる。

（１）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講じる。

（２）情報システム全体の強靭性の向上

情報システム全体に対し、次の３段階の対策を講じる。

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、個人情報の流出を防ぐ。

イ　ＬＧＷＡＮ接続系においては、通信経路の分割を行う。なお、ＬＧＷＡＮ接続系とインターネット接続系の間で通信する場合には、無害化通信を実施する。

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講じる。

（３）物理的セキュリティ

マシン室、通信回線及び端末等の管理について、物理的な対策を講じる。

（４）人的セキュリティ

情報セキュリティに関し、職員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。

（５）技術的セキュリティ

情報システムの管理、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な対策を講じる。

（６）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情報セキュリティの確保等、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、情報資産への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、緊急時対応計画を策定する。

（業務委託と外部サービスの利用）

第８条　業務委託を実施する場合は、当該委託事業者において必要な情報セキュリティ対策が確保されていることを確認し、契約等に基づき、情報セ

キュリティポリシーを遵守させるための必要な措置を講じるものとする。

２　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。

３　ＳＭＳを利用する場合には、利用するＳＭＳごとの運用手順を定め、発信できる情報及び責任者を定める。

（情報セキュリティ監査及び自己点検の実施）

第９条　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。

（情報セキュリティポリシーの見直し）

第10条　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は、遅滞なく情報セキュリティポリシーの見直しを行う。

（情報セキュリティ対策基準の策定）

第11条　情報セキュリティ対策を講じるため、具体的に情報セキュリティ対策に取り組む体制、遵守事項及び判断基準等を明確にした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、公開することにより本市の情報セキュリティの維持に重大な支障をきたすおそれがあることから非公開とする。

（情報セキュリティ実施手順の策定）

第12条　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講じ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。なお、情報セキュリティ実施手順は非公開とする。