昭島市の執行機関等におけるサイバーセキュリティ基本方針

（目的）

第１条　この基本方針は、昭島市の執行機関等（第４条第２項に規定する組織をいう。以下同じ。）が実施するサイバーセキュリティ対策に関する基本的な事項を定めることにより、執行機関等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する。

（用語の意義）

第２条　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

ウ　情報システム等に関する設計書、ネットワーク図等のシステムに関連する文書

（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　執行機関等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等がある。ただし、当該機能を利用して執行機関等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）　サイバーセキュリティ　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　脅威により業務の遂行を危うくする確率及びサイバーセキュリティを脅かす確率が高い事象をいう。

（９） 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。

(10) 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。

(11) 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。

(12) 職員等　執行機関等の特別職及び一般職の全ての職員並びに執行機関等と派遣契約等を締結した上で、執行機関等の業務に従事する者をいう。

(13) 管理区域　ネットワークの基幹機器及び重要な情報システムを設置し、当該機器等の管理及び運用を行うための区域をいう。

（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　本方針が対象とする情報資産は、執行機関等が所掌する情報資産とする。

２　本方針の適用組織は、次に掲げる組織とする。

（１） 地方自治法（昭和22年法律第67号）第２編第７章第３節に基づいて設置される委員会及び委員（教育委員会を除く。）

（２） 議会

（職員等の遵守事項）

第５条　職員等は、サイバー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本方針を遵守しなければならない。

（組織体制）

第６条　執行機関等の情報資産について、執行機関等ごとにサイバーセキュリティ対策を推進する組織体制を確立する。

２　執行機関等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。

３　ＣＩＳＯは、執行機関等の長の職にあるもの又は地方自治法第199条の３に規定する代表監査委員をもって充てる。

（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、次に掲げるサイバーセキュリティ対策を講じる。

（１） 情報資産の分類と管理　執行機関等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、当該分類に基づきサイバーセキュリティ対策を講じる。

（２） 物理的セキュリティ　管理区域、通信回線、サーバ及び端末等の管理について、物理的な対策を講じる。

（３） 人的セキュリティ　サイバー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。

（４） 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。

（５） 運用　情報システムの監視、本方針の遵守状況の確認、業務委託を行う際のサイバーセキュリティの確保等、本方針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サイバー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、本方針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、当該利用に係る規定を整備し対策を講じる。

（監査及び自己点検の実施）

第９条　本方針の遵守状況を検証するため、定期的又は必要に応じてサイバーセキュリティに関する監査及び自己点検を実施する。

（サイバーセキュリティ基本方針の見直し）

第10条　サイバーセキュリティに関する監査及び自己点検の結果、本方針の見直しが必要となった場合及びサイバー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、遅滞なく本方針の見直しを行う。