朝日町
情報セキュリティ
基本方針

令和 8 年 3 月 31 日

朝　日　町　役　場

（目的）

第1　本基本方針は、朝日町（以下「町」という。）が保有する情報資産の機密性･完全性･可用性を維持するために町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により、その適正な管理及び効率的な運営を図ることを目的とする。

（定義）

第2　本基本方針において、掲げる用語の意義は次の各号に定めるところによる。

(1)　情報システム　情報処理装置（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。

(2)　ネットワーク　情報処理装置間を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)　電磁的記録媒体　磁気テープ、磁気ディスクその他のデータを記録している媒体をいう。

(4)　情報資産　情報システムの導入から運用に至るまでのすべてのデータ、情報システムに係る入出力帳票及び情報システムに係るドキュメントをいう。

(5)　情報セキュリティ　情報資産の機密性（情報資産に許可された者だけがアクセスできることをいう。）、完全性（情報資産及び処理の方法が正確かつ完全である状態をいう。）及び可用性（許可された利用者が必要なときに情報資産にアクセスできることをいう。）を維持することをいう。

(6)　情報セキュリティポリシー　本基本方針及び別に定める情報セキュリティ対策基準をいう。

(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)　職員　地方公務員法（昭和25年法律第261号）第3条第2項に規定する一般職の職員及び同条第3項第1号に規定する特別職の職員並びに町に勤務する全ての嘱託職員、臨時職員等をいう。

（適用範囲）

第3　本基本方針が適用される行政機関は、内部部局、行政委員会、議会事務局及び地方公営企業とする。

2　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)　情報システム及びこれらに関する設備、電磁的記録媒体

(2)　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、ネットワーク図等のシステム関連文書

（対象とする脅威）

第4　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、業務不能とする攻撃等のサイバー攻撃や部外者の進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、職員による内部不正等

(2)　情報資産の無断持ち出し、無許可の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、内部監査の不備、外部管理委託の不備、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

（職員の遵守事項）

第5　情報セキュリティポリシー等の遵守

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。

（情報セキュリティ対策）

第6　第4の各号の脅威から情報資産を保護するために、次の各号の情報セキュリティ対策を講じる。

(1)　組織体制　町が保有する情報資産について、情報セキュリティ対策を推進する全庁的な組織を確立する。

(2)　情報資産の分類と管理　町が保有する情報資産は、別に定める情報セキュリティ対策基準にある機密性、完全性及び可用性により分類し、その分類に基づき情報セキュリティ対策を行う。

(3)　物理的セキュリティ　サーバ、電算室、通信回線並びにインフラ環境及

び職員のパソコン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　コンピュータの管理、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。

(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、外部委託を行う際の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、緊急時対応計画を定める。

（情報セキュリティ監査及び自己点検の実施）

第7　情報セキュリティポリシーの遵守状況を検証するために、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8　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な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の見直しを行う。

（情報セキュリティ対策基準の策定）

第9　第6から第8に規定する対策を実施するために、具体的な遵守事項及び判断基準等を別に策定する。

（情報セキュリティ実施手順の策定）

第10　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手順書を別に策定する。

　なお、この手順書は、公にすることにより町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。