阿久比町情報セキュリティ基本方針

令和８年４月１日策定

（目的）

第１条　この基本方針は、阿久比町（以下「町」という。）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、町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。

（定義）

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

⑴　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）

⑵　情報システム　コンピュータ、ソフトウェア、ネットワーク及び周辺機器で構成され、情報の処理を行う仕組み

⑶　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。

⑷　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

⑸　機密性　情報にアクセスすることを許可された者だけが、情報にアクセスできる状態を確保すること。

⑹　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。

⑺　可用性　情報にアクセスすることを許可された者が、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。

⑻　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、地方税又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その情報システムで取り扱うデータ

⑼　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（マイナンバー利用事務系を除く。）

⑽　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その他の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

⑾　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

（対象とする脅威）

第３条　情報資産に対して、次の各号に掲げる脅威を想定し、情報セキュリティ対策を実施する。

⑴　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、改ざん又は消去、重要情報の詐取及び内部不正等

⑵　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、設計又は開発の不備、プログラム上の欠陥、操作又は設定ミス、メンテナンス不備、内部又は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、破壊又は消去等

⑶　地震、落雷、火災その他の災害によるサービス及び業務の停止等

⑷　大規模又は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

⑸　電力供給の途絶、通信の途絶又は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　この基本方針が適用される行政機関は、町長(水道事業及び下水道事業の管理者の権限を行う町長を含む。)、教育委員会、選挙管理委員会、監査委員、農業委員会、固定資産評価審査委員会及び議会事務局とする。

２　この基本方針が適用される情報資産は、次の各号に掲げるとおりとする。

⑴　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

⑵　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。）

⑶　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

（遵守義務）

第５条　職員（地方公務員法（昭和２５年法律第２６１号）第３条に規定する地方公

務員をいい、会計年度任用職員及び臨時的任用職員を含む。）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条　第３条に規定する脅威から情報資産を保護するために、次の各号に掲げる項目に応じて、当該各号に定める情報セキュリティ対策を講じる。

⑴　組織体制　町の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体制を確立する。

⑵　情報資産の分類及び管理方法　町の保有する情報資産を機密性、完全性及び可用性を加味して情報セキュリティ対策を実施する。

⑶　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、業務の効率性及び利便性の観点を踏まえ、情報システム全体に対し、次に掲げる対策を講じる。

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を不可とする設定や端末への多要素認証の導入等により、情報の流出を防ぐ。

イ　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、安全が確保された通信だけを許可し、無害化通信を行う。

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行う。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行う。

⑷　物理的セキュリティ対策　サーバ、電算室、通信回線及び職員の端末等の管理について、物理的な対策を講じる。

⑸　人的セキュリティ対策　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。

⑹　技術的セキュリティ対策　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及び不正アクセス対策等の技術的対策を講じる。

⑺　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及び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とともに、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、緊急時対応計画を策定する。

⑻　業務委託　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。

⑼　外部サービスの利用　外部サービスを利用する場合には、利用形態及び取り扱う情報の性質等を踏まえ、必要に応じて利用に係る規定を整備し対策を講じる。

⑽　ソーシャルメディアサービスの利用　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。

⑾　評価及び見直し　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。

（情報セキュリティ監査及び自己点検の実施）

第７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８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、情報セキュリティポリシーの見直しを行う。

（対策基準等）

第９条　前３条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（以下「対策基準」という。）を策定する。

２　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

る情報セキュリティ実施手順（以下「実施手順」という。）を策定する。

3　対策基準及び実施手順は、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ため非公開とする。