皆野町情報セキュリティ基本方針

平成３０年８月

皆野町

目次

1　目的

本基本方針は、本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ため、本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を目的とする。

2　定義

（1）情報

職務の遂行に伴ってコンピュータ及び記録媒体に記録されたデータをいう。

（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）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。

（4）個人番号

住民票コードを変換して得られる番号であって、当該住民票コードが記載された住民票に係る者を識別するために指定されるものをいう。

（5）特定個人情報

個人番号をその内容に含む個人情報をいう。

（6）脅威

技術的脅威（不正アクセス、ウイルス攻撃など）、人的脅威（情報資産の持ち出し、意図的要因による情報漏えい、破壊など）、物理的脅威（自然災害、電力供給の途絶など）をいう。

（7）情報セキュリティ

脅威から皆野町が管理する情報資産を保護し、その機密性、完全性及び可用性を維持することをいう。

（8）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。

（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

皆野町に勤務する職員、非常勤職員、臨時職員、及び町立の小中学校に勤務する教職員のことをいう。

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）技術的脅威

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）人的脅威

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等

（３）物理的脅威

・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
・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
・電力供給の途絶、通信の途絶等のインフラの障害からの波及等

４　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

本町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

本町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行う。

（３）物理的セキュリティ

サーバ等、情報システム室等、通信回線等、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。

（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、緊急時対応計画を策定する。

５　適用範囲

（１）適用対象者

本基本方針の適用対象者は、職員及び関係機関の職員とする。

（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、皆野町が管理する全ての情報資産とする。

①ネットワーク、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

④個人番号利用事務で取り扱う情報（個人番号、特定個人情報など）

６　情報セキュリティ管理体制

本基本方針及び対策基準に規定された情報セキュリティ対策の推進並びに管理にあたり、以下の組織・体制を置くものとする。

(1)　最高情報統括責任者・・・・副町長

(2)　情報統括責任者・・・・・・総務課長

(3)　情報セキュリティ責任者・・各課局次長

(4)　情報システム責任者・・・・総務課防災・情報政策担当職員（情報担当職員）

(5)　情報セキュリティ部会・・・情報セキュリティポリシー、番号制度等、情報政策に関する重要な事項を決定する機関

(6)　情報セキュリティ部会員・・情報セキュリティ責任者が選定した職員

7　職員の遵守義務

全ての職員は、次に掲げる義務を負うものとする。

（1）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。

（2）職員は、情報セキュリティ対策を有効に機能させなければならない。

（3）職員は、職務上知り得た秘密を漏らしてはならない。その職を退いた後も同様とする。

8　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。

9　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、情報セキュリティポリシーを見直す。

１０　情報セキュリティ対策基準の策定

上記４、８及び９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。