吉野町情報セキュリティ基本方針

1. 目的

この基本方針は、本町が保有するネットワーク、情報システム及びこれらに関する設備並びに情報資産（以下、情報資産）について、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により、行政の適正かつ円滑な運営を図り、もって町政に対する町民の信頼を確保することを目的とする。

2. 定義

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。

（１） コンピュータ

パーソナルコンピュータ、サーバ、ストレージ等の機器をいう。

（２） 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。

（３） 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。

（４） 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。

（５） 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。

（６） 機密性

情報資産にアクセスすることを認められた者だけが、情報資産にアクセスできる状態を確保することをいう。

（７） 完全性

情報資産が破壊、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。

（８） 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。

（９） マイナンバー利用事務系（個人番号利用事務系）

個人情報利用事務又は戸籍事務等に関わる情報システム及びデータをいう。

（１０）LGWAN 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。

（１１）インターネット系

インターネットメール等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及びその情報システムで取り扱うデータをいう。

（１２）通信経路の分割

LGWAN 系とインターネット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。

（１３）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ない等、安全が確保された通信をいう。

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） 悪意を持つものによる脅威

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） あらゆる事故による脅威

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、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） 災害による脅威

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

（４） 必要資源の不足、故障等による脅威

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、水道供給の途絶等のインフラの障害からの波及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

4. 適用範囲

（１） 行政機関の範囲

本基本方針が適用される行政機関は、町長部局、教育委員会、選挙管理委員会、監査委員会、農業委員会、固定資産評価審査委員会、議会事務局及び地方公営企業が保有する情報資産、情報資産に関する事務に携わる全ての職員、非常勤職員、臨時職員、労働者派遣事業により本町の事務に携わる者（以下、「職員等」という）及び委託事業者とする。

（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

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職員等が職務上作成又は取得し、保有している文書、図面及び電磁的記録

5. 職員等の遵守義務

上記4に規定する者は、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。

6. 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

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、電算室等、通信回線等及び職員等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。

（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、障害が発生した場合等に迅速かつ適切に対応するため、障害発生時の対策を講じる。

7. 情報セキュリティポリシーの見直し

情報セキュリティの適切な点検の結果、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。

8. 情報セキュリティ対策基準の策定

上記6、7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。 なお、情報セキュリティ対策基準は、公にすることにより本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。

平成 30 年 11 月 1 日策定

平成 31 年 3 月 1 日改訂