梼原町情報セキュリティ基本方針

１．目的

梼原町（以下「町」という。）で取り扱う情報には、町民の個人情報をはじめ行政運営上重要な情報など、外部への情報漏えいやシステムが故障等した場合に、極めて重大な影響を及ぼす情報が多数ある。これらを様々な脅威から確実に保護することは、町民の財産、プライバシー等を守り、また、行政の安定的かつ継続的なサービスや正確な情報の提供を実施していくためにも必要不可欠である。

そのため、町が保有する全ての情報を、様々な脅威から保護し、安全で質の高い行政サービスを実現するために、町が実施する情報セキュリティに関する統一的かつ基本的な事項を定めるものとする。

２．定義

基本方針における用語の意義は次のとおり。

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、その構成機器（ハードウェア及びソフトウェア）をいう。

⑵ 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。

⑶ 情報資産

全ての紙文書、ネットワーク及び情報システムの開発と運用に係る全ての情報並びにネットワーク及び情報システムで取り扱う全ての情報をいう。

⑷ 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。

⑸ 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。

⑹ 機密性

情報資産の利用を許可された者だけが、情報を利用することを確実にすることをいう。

⑺ 完全性

情報及び処理方法が、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。

⑻ 可用性

許可された利用者が、必要な時に情報資産を利用できることを確実にすることをいう。

⑼ 職員等

全ての職員（会計年度任用職員を含む。）をいう。

⑽ 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、地方税若しく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データをいう。

(11) 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をいう（マイナンバー利用事務系を除く。）。

(12) 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等に関わる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をいう。

(13) 通信経路の分割

LGWAN接続系とインターネット接続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。

(14) 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をいう。

３．職員等の遵守義務

本町が所掌する情報資産に関する業務に携わる職員等は、情報セキュリティの重要性について共通の認識を持つとともに、業務の遂行に当たっては情報セキュリティポリシーを遵守しなければならない。

４．情報セキュリティ管理体制

情報資産の統一的な情報セキュリティを確保するため、全庁的な組織体制を整備する。

５．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) 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、重要情報の搾取、機器及び媒体の盗難等

(2) 職員等及び外部委託事業者による情報資産の無断持ち出し・盗聴・改ざん・消去、機器及び媒体の盗難及び承認されていない端末接続によるデータ漏えい等

(3) 情報通信技術を使用しないパスワード等の重要情報の盗み見、なりすまし等

(4) 地震、落雷、火災、水害等の災害並びに事故、故障等によるサービス及び業務の停止

(5) 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

(6) 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

６．適用範囲

⑴ 組織の範囲

内部部局、各行政委員会、地方公営企業、議会

⑵ 人の範囲　対象となる組織の職員等

⑶ 情報資産の範囲

町の対象組織で保有する全ての情報資産

① 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

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

７．情報セキュリティ対策

情報資産を認識すべき脅威から保護するために、以下の情報セキュリティ対策を講ずるものとする。

（１）組織体制

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実施する。

（３）物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産への損傷・妨害等から保護するためにサーバ、情報システム室、通信回線及び職員等のパソコン等の管理について、物理的な対策を講ずる。

（４）人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、職員等に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が行われるように必要な対策を講ずる。

（５）技術及び運用におけるセキュリティ対策

情報資産を外部からの不正アクセス、不正プログラム等から適切に保護するため、情報資産へのアクセス制御、ネットワーク管理等の技術面の対策、またシステム開発等の外部委託のセキュリティ管理、ネットワークの監視、情報セキュリティポリシーの遵守状況を確認する等の運用面の対策を講ずる。

併せて、緊急事態が発生した際に迅速な対応を可能とするため~~の危機管理対策を講ずる~~緊急時対応計画を策定する。

（６）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・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

① 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不可設定や端末への多要素認証の導入等により、

住民情報の流出を防ぐ。
② 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、無害化通信を実施する。
③ 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実施する。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実施する。

８．情報セキュリティ対策基準の策定

基本方針に基づき、遵守すべき行為及び判断等の統一的な基準として、情報セキュリティ対策基準を策定するものとする。

９．情報セキュリティ実施手順の策定

情報セキュリティ対策基準を遵守して、情報セキュリティ対策を実施するために、個々の情報資産に応じた対策手順等をそれぞれ定めていく必要がある。
そのため、情報資産に対する脅威及び情報資産の重要度に対する情報セキュリティ対策基準の基本的な要件に基づき、町が所掌する情報資産の情報セキュリティ実施手順を策定するものとする。

１０．情報セキュリティ対策基準及び情報セキュリティ実施手順の取扱い

情報セキュリティ対策基準及び情報セキュリティ実施手順は、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恐れのある情報であることから非公開とする。
（1）業務委託と外部サービス（クラウドサービス）の利用
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。
外部サービス（クラウドサービス）を利用する場合には、利用に係る規定を整備し対策を講じる。
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。

１１．監査と見直し

情報セキュリティポリシーが遵守されていることを検証するため、定期的または必要に応じて情報セキュリティ監査を実施し、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、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、リスクを検討したうえで、必要があれば見直しを実施する。

１２．情報セキュリティに関する違反に対する対応

この基本方針に違反した職員等は、地方公務員法、町条例による懲戒処分の対象となる。