大台町情報セキュリティ基本方針

（目的）

第１条　この基本方針は、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。

（定義）

第２条　大台町情報セキュリティポリシー（以下「ポリシー」という。）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）　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）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た情報処理を行う仕組みをいう。

（３）　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。

（４）　ポリシー　この基本方針及び情報セキュリティ対策基準を総称したものをいう。

（５）　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。

（６）　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。

（７）　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。

（８）　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基幹系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。

（9） ＬGWAN接続系　ＬGWAN（総合行政ネットワーク）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。）。

（10） インターネット接続系　インターネットメール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。

（11） 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。

（12） 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、コンピューター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。

（13） 情報セキュリティインシデント　組織の情報管理又はシステム運用に関するセキュリティ体制を脅かすセキュリティ上好ましくない事象又は事故のことをいう。

（14） 端末　情報システムの構成要素である機器のうち、情報処理を行うために直接操作するもの（登載されるソフトウェア及び直接接続され一体化として扱われるキーボード、マウス等の周辺機器を含む。）をいう。

（15） パソコン　端末のうち、机の上等に備え置いて業務に使用することを前提とし、移動させて使用することを目的とはしていないものをいい、端末の形態は問わない。

（16） モバイル端末　端末のうち、業務上必要に応じて、移動させて使用することを目的としたものをいい、端末の形態は問わない。

（17） 電磁的記憶媒体　コンピュータによる情報処理に使用する、電子的又は電磁的な記録方式により作成された記録を保持するための媒体。ソリッドステートドライブ（ＳＳＤ）、ハードディスクドライブ（ＨＤＤ）、ＣＤ、ＤＶＤ、ＵＳＢメモリ、ＳＤカード等をいう。

（18） サーバー室　重要な情報システム及びネットワークの基幹機器を設置し、当該機器等の管理及び運用を行うための部屋をいう。

（対象とする脅威）

第３条　情報資産に対する脅威として、次の脅威を想定し、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、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） 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

（３） 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） 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

（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障害からの波及等

（適用範囲）

第４条　ポリシーを適用する範囲は、次のとおりとする。

（１） 行政機関の範囲は、町長部局、行政委員会、監査委員、議会、教育機関及び地方公営企業とする。

（２） 職員の範囲は、適用される情報資産に関わる職員（地方公務員法（昭和25年法律第261号。以下「地方公務員法」という。）第３条に規定する職員をいう。）とし、会計年度任用職員（地方公務員法第22条の２に規定する職員をいう。）及び臨時的任用職員（地

方公務員法第22条の３に規定する職員をいう。）並びに他団体からの研修生等を含む（以下「職員等」という。）。

（３） 情報資産の範囲は、次のとおりとする。

ア　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記録媒体

イ　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。）

ウ　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ち、業務の遂行に当たってポリシー、情報セキュリティ実施手順及び関係規程等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、次の情報セキュリティ対策を講じる。

（１） 組織体制　本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。

（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） 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、次の三段階の対策を講じる。

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の不可設定や端末への多要素認証の導入等により、住民情報等の流出を防止する。

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。ただし、両システム間で通信を行う場合は、無害化通信を実施する。

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実施する。高度な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うえで、自治体セキュリティクラウドの導入等を実施する。

（４）　物理的セキュリティ　サーバ、サーバー室、通信回線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。

（５）　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。

（６）　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。

（７）　運用　情報システムの監視、ポリシーの遵守状況の確認、業務委託を行う際のセキュリティ確保等、ポリシー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正に対応するため、緊急時対応計画を策定する。

（８）　業務委託と外部サービスの利用

ア　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。

イ　外部サービスを利用する場合には、利用にかかる規定を整備し対策を講じる。

ウ　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。

（情報セキュリティ監査及び自己点検の実施）

第７条　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ものとする。

（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、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となった場合には、ポリシーを見直すものとする。

（情報セキュリティ対策基準の策定）

第９条　第６条から前条まで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ものとする。ただし、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。

（情報セキュリティ実施手順の策定）

第10条　ポリシーに基づき、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情報セキュリティ実施手順を策定する。ただし、情報セキュリティ実施手順は、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。