大網白里市
情報セキュリティポリシー基本方針

平成２９年７月　策定
令和　３年３月　改定

大網白里市情報セキュリティ基本方針

（目的）

第１条　大網白里市情報セキュリティ基本方針（以下「基本方針」という。）は、大網白里市（以下「市」という。）が保有する情報資産について、情報セキュリティ対策の基本事項を定めることにより、市民の財産やプライバシー等を守り、市民からの継続的な信頼を得ることを目的とする。

（情報セキュリティポリシーの構成と位置づけ）

第２条　情報セキュリティポリシーは、市が保有する情報資産の情報セキュリティ対策について総合的、体系的かつ具体的に取りまとめたものであり、情報セキュリティに対する取組姿勢を示す基本方針と、この基本方針に定められた情報セキュリティを確保するために遵守すべき行為及び判断等の基準を示す対策基準をもって構成する。

（定義）

第３条　情報セキュリティポリシーにおいて、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

（１）　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。

（２）　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。

（３）　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。

（４）　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。

（５）　職員等

市長、副市長、会計管理者、教育長、大網白里市職員定数条例（昭和 31 年条例第 22 号）第２条に規定する職員、会計年度任用職員、臨時的任用職員、再任用短時間勤務職員及び任期付短時間勤務職員をいう。

（６）　課等

大網白里市課設置条例（昭和 46 年条例第 12 号）第１条に規定する課、白里出張所、会計課、ガス事業課、国保大網病院、下水道課、教育委員会事務部局の課等（管理課、生涯学習課、中央公民館、白里公民館、中部コミュニティセンター及び図書室をいう。）、選挙管理委員会事務部局、農業委員会事務局、監査委員事務局及び議会事務局をいう。

（７）　会計年度任用職員等

会計年度任用職員及び臨時的任用職員をいう。

（８）　外部委託業者

市との契約により、市の情報を取り扱う業務または市のネットワークもしくは情報システムに係る開発、導入、保守等の業務に携わる者をいう。

（９） 行政情報

電磁的に記録された行政事務の執行に係る情報をいう。

(10) 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。

(11) 端末機

ネットワークを通じてサーバに接続されたパソコンをいう。

(12) サーバ等

ネットワーク上で行政情報を処理し、端末機に提供するコンピュータをいう。

(13) 情報システム

行政情報を処理するためのハードウェア及びソフトウェアをいう。

(14) 記録媒体

情報システムでデータ等を記録するための媒体をいう。

(15) モバイル端末

端末機のうち、業務上の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う。

(16) 情報資産

情報システム、ネットワーク及び設備並びにこれらで取り扱われる行政情報（これらを印刷した文書を含む。）をいう。

(17) 無線ＬＡＮ

電波等を利用してデータの送受信を行う構内通信網システムをいう。

(18) ＡＳＰ／クラウド

庁外データセンター等でプログラムやデータベースを管理し、ネットワークを介してこれを利用する仕組みや概念をいう。

(19) データセンター

耐震性に優れた建物にシステムを収容して高速な通信回線を引き込み、空調や入退室管理、カメラによる監視等のセキュリティ対策を施した施設をいう。

(20) 個人情報

個人情報の保護に関する法律（平成 15 年法律第 57 号）に規定する個人情報をいう。

(21) 特定個人情報

行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）に規定する特定個人情報をいう。

(22) 複合機

複写機、プリンター、イメージスキャナ及びファクシミリ等の事務機器の機能を１つの筐体に収めた機器をいう。

(23) ソーシャルメディアサービス

インターネットを利用して双方向のコミュニケーションを促進することを提供するコンテンツ

のことをいう。

(24) 基幹系（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。

(25) 情報系

LGWAN に接続された情報システム及びデータ又はその他の情報システム及びデータをいう。（基幹系を除く。）

(26) 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。

(27) 通信経路の分割

情報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。

(28) 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。

(29) 情報セキュリティインシデント

情報資産を脅かすセキュリティ上好ましくない事象又は事態のことをいう。

（対象とする脅威）

第４条　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・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） 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・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の障害からの波及等

（適用範囲）

第５条　基本方針の適用範囲は次のとおりとする。

（１） 組織的範囲

市の業務を取り扱う全ての部署

（２） 人的範囲

職員等及び外部委託業者

（３） 情報資産の範囲

基本方針が対象とする情報資産は、次のとおりとする。

ア　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

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

（職員等の遵守義務）

第６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、法令、情報セキュリティポリシー及び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７条　第４条に規定する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

市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

市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講じる。

（３）　情報システム全体の強靭性の向上

情報システム全体に対し、次の三段階の対策を講じる。

①　基幹系においては、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制御設定や端末への多要素認証の導入等を行い、情報資産の流出を防ぐ。

②　情報系においては、LGWAN の情報システムと、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、都道府県と市区町村のインターネット接続口を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

（４）　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。

（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、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。また、第４条に規定する脅威で情報セキュリティインシデントが発生した場合等に迅速かつ適正に対応するための危機

管理対策を講じる。

（８） 外部サービスの利用

外部委託する場合には、外部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、外部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。

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８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を実施する。

（情報セキュリティポリシーの見直し）

第９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に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。

（情報セキュリティ対策基準の策定）

第 10 条　第６条、第７条及び第８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を策定する。

２　情報セキュリティ対策基準に基づき、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た情報セキュリティ実施手順を策定するものとする。

なお、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、公にすることで本市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。

（補則）

第 11 条　この基本方針に定めるもののほか、必要な事項は、市長が定める。