北松北部環境組合情報セキュリティ基本方針

（目的）

第１条　本基本方針は、北松北部環境組合（以下「本組合」という。）が保有する情報資産の機密性、完全性及び可用性の維持を確保するため、情報資産の取扱いと情報セキュリティ対策の基本的な考え方及び方策を定め、もって本組合の情報資産の管理を徹底することを目的とする。

（用語の定義）

第２条　情報セキュリティ基本方針における用語の定義は、次のとおりとする。

(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、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　業務に使用するコンピュータ、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)　行政情報　本組合の行政事務の執行に関わる情報で、かつ、情報システムで取り扱うものをいう。

(4)　情報資産　情報システム及び行政情報をいう。

(5)　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。

(6)　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。

(7)　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。

(8)　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。

(9)　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。

(10)　マイナンバー利用事務系（個人番号利用事務系）　個人番号利用事務に関わる情報システム及びデータをいう。

(11)　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。

(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。

(13)　外部サービス　クラウドサービス、WEB会議システム及びソーシャルメディア等の庁外のネットワーク機器又はシステム等を利用するサービスをいう。

（適用範囲）

第３条　本基本方針の適用範囲は、管理者、議会、監査委員とする。

（情報資産の範囲）

第４条　本基本方針において対象となる情報資産は、次のとおりとする。

(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

（職員等の遵守義務）

第５条　職員、臨時・非常勤職員等（以下「職員等」という。）及び外部委託事業者は、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第９条に規定する情報セキュリティ実施手順を遵守しなければならない。

（情報資産への脅威）

第６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・設定のミス、メンテナンス不備、内部・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・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

（情報セキュリティ対策）

第７条　本組合が保有する情報資産を前条の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　本組合の情報資産について、情報セキュリティ対策を推進・管理するための組織体制を確立する。

(2)　物理的セキュリティ対策　サーバ、通信回線及び職員等のパソコン等の管理について、物理的な対策を講じる。

(3)　人的セキュリティ対策　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。

(4)　技術的セキュリティ対策　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。

(5)　運用　本基本方針の遵守状況の確認、データの外部提供（第４条第１項に規定する情報を本組合以外の者に提供することをいう。）に関する手続きその他の情報セキュリティに関する運用面の対策を講じる。また、緊急事態が発生した場合に迅速な対応をするための危機管理対策を講じる。

(6)　業務委託　業務委託を行う場合には、委託業者を選定し、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。

(7)　外部サービス（クラウドサービス）の利用　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。

(8)　ソーシャルメディアサービスの利用　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。

（情報セキュリティ対策基準の策定）

第８条　情報セキュリティ対策を講ずるに当たり、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。

（情報セキュリティ実施手順の策定）

第９条　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。

２　情報セキュリティ実施手順は、公にすることにより本組合の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。

（情報セキュリティ監査及び自己点検の実施）

第10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及び自己点検を実施する。

（情報セキュリティポリシーの見直し）

第11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、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、情報セキュリティポリシーを見直す。