○仙北市サイバーセキュリティ基本方針

第１　目的
この基本方針は、市の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、その総合的かつ体系的な推進を図り、もって市民の財産、プライバシー等の保護と安定的で信頼される行政運営に資することを目的とする。

第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) ネットワーク　通信回線及び通信回線装置で構成され、電子計算機、通信回線、通信回線装置、電磁的記録媒体及び周辺機器（以下「電子計算機等」という。）を相互に接続し情報を交換するための仕組みをいう。
(2) 情報システム　電子計算機、ネットワーク、電磁的記録媒体又は周辺機器で構成され、情報処理を行う仕組みをいう。
(3) 職員　本市職員をいう。会計年度任用職員等も含まれる。
(4) 行政情報　職員が職務上作成し、又は取得した文書、図画及び電磁的記録であって、職員が組織的に用いるものをいう。
(5) 自己管理情報　職員が職務上作成し、又は取得した文書、図画及び電磁的記録であって、行政情報でないものをいう。
(6) 電子情報　情報システムで取り扱う情報をいう。
(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) 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。
(11) 情報セキュリティ対策　情報セキュリティのための対策をいう。
(12) 情報セキュリティポリシー　この基本方針及び情報セキュリティ対策基準をいう。
(13) 強靭性の向上　市の情報システム全体をマイナンバー利用事務系、LGWAN 接続系及びインターネット接続系の 3 つの領域に分割し、各領域間における通信の制御等の情報セキュリティ対策を講じることをいう。なお、技術の進展及び業務効率化の観点から、国が推奨するネットワークモデル（α'モデル等）への移行を検討するものとする。

第３　適用範囲
この基本方針が適用されるのは、市長部局、行政委員会（監査委員を含む）、議会事務局及び地方公営企業とする。
また、この基本方針が対象とする情報資産は、次のとおりとする。
ア　情報システムを構成する機器
イ　情報システムに関する施設・設備

ウ　電子情報
エ　システム関連文書
オ　行政情報
カ　自己管理情報

第４　職員の義務
職員は、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、この基本方針、情報セキュリティ対策基準、情報セキュリティ対策実施手順その他情報セキュリティ対策に関する市の規程及び法令を遵守する義務を負う。

第５　組織及び体制
情報セキュリティ対策を推進するため、次の体制を確立するものとする。
⑴ 統括情報セキュリティ責任者（CISO）を置き、情報セキュリティ対策の総括的な管理を行う。
⑵ 情報セキュリティ責任者及び情報セキュリティ管理者を置き、各部署における対策の実施を管理する。
⑶ 情報セキュリティインシデント発生時の連絡体制及び意思決定体制を整備する。
⑷ 必要に応じて外部専門機関との連携体制を構築する。

第６　情報資産の分類及び管理
市が保有する情報資産について、機密性、完全性及び可用性に応じて次の基準により分類し、当該分類に応じた情報セキュリティ対策を行うものとする。
⑴ 機密性 3A：マイナンバー利用事務で取り扱う特定個人情報等
⑵ 機密性 3B：要配慮個人情報を含む個人情報
⑶ 機密性 3C：機密性 3A 及び 3B 以外の個人情報
⑷ 機密性 2：行政運営上の重要情報
⑸ 機密性 1：公開情報

第７　情報セキュリティへの脅威
情報資産の格付けの後、次の各号に掲げる情報セキュリティに対する脅威について、抽出を行うものとする。
⑴ 不正アクセス、マルウェアによる攻撃、サービス不能攻撃等のサイバー攻撃、部外者の侵入、重要情報の詐取、内部不正等の意図的な要因に伴う情報資産の漏えい、破壊、改ざん、消去等の脅威
⑵ 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、操作・設定ミス、プログラムミス、ネットワークの誤接続、メンテナンスの不備、内部・外部監査機能の不備、業務委託管理の不備、マネジメントの欠陥、機器故障等の非意図的な要因に伴う情報資産の漏えい、破壊、改ざん、消去等の脅威
⑶ 地震、落雷、火災、水害等の災害及び大規模・広範囲にわたる疾病による要員不足に伴うサービス及び業務の停止等の脅威

⑷ 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に伴うサービス及び業務の停止等の脅威

第８　脅威への対策
前項の抽出により明らかになった脅威に対して、以下の情報セキュリティ対策を実施するものとする。
⑴ 物理的な対策
重要な情報資産の保管場所への不正な立入り、窃盗、破壊等を防止する等の物理的な対策
⑵ 人的な対策
情報セキュリティに関する職員の権限及び責任の明確化、職員に対する定期的な教育及び啓発（ランサムウェア等のサイバー攻撃の手口と対策を含む)、研修受講の推奨等の人的な対策
⑶ 技術的な対策
情報システム全体の強靭性の向上、情報資産を不正アクセス等から保護するためのアクセス制御（多要素認証を含む)、マルウェア対策等の技術的な対策
⑷ 運用における対策
情報資産の監視、情報セキュリティ対策の遵守状況の確認、システム障害等の緊急事態が発生した場合の危機管理等の運用における対策
⑸ 業務委託及び外部サービスの利用における対策
業務委託事業者及び外部サービス提供事業者に係る選定基準の整備、情報セキュリティ要件を明記した契約締結等の業務委託及び外部サービスの利用における対策
⑹ クラウドサービス利用における対策
ガバメントクラウド等のクラウドサービスを利用する場合は、次の対策を講じるものとする。
ア 多要素認証及びポリシーベースのアクセス制御の実施
イ サービス提供事業者の信頼性評価及び契約時のセキュリティ要件の明記
ウ データの暗号化及びバックアップ体制の確保
エ サービス利用状況の常時監視及びログの保存
⑺ サイバーレジリエンスの強化
サイバー攻撃による被害からの迅速な復旧を図るため、次の対策を講じるものとする。
ア 業務継続計画（BCP）の策定及び定期的な訓練の実施
イ ランサムウェア攻撃を想定したバックアップ体制の整備
ウ インシデント発生時の初動対応手順の明確化

第９　情報セキュリティ対策の体系
この基本方針に基づき、次の規程を定めるものとする。
⑴ 情報セキュリティ対策基準
情報セキュリティ対策を統一的に実施するために必要な事項を定めるもの
⑵ 情報セキュリティ対策実施手順
情報セキュリティ対策基準に準拠し、情報セキュリティ対策を具体的に実施するために必要な事項を定めるもの

第 10　情報セキュリティ監査及び自己点検の実施

情報セキュリティ対策の遵守状況を検証するため、定期的に及び必要に応じて情報セキュリティ監査及び自己点検を行うものとする。

第 11　情報セキュリティ対策の評価及び見直し

情報セキュリティ監査及び自己点検の結果等に基づき、情報セキュリティ対策の実効性の評価を行い、情報セキュリティ対策の見直しが必要となった場合又は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情報セキュリティ対策が必要となった場合において、保有する情報資産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上で、必要に応じ、情報セキュリティポリシーを見直すものとする。

附則

１　この基本方針は、令和８年３月 23 日から施行する。

２　この基本方針は、地方自治法第 244 条の 6 の規定に基づき、令和８年４月１日までに公表するものとする。