日高市サイバーセキュリティ基本方針

序文

日高市（以下「市」という。）が保有し、又は管理する情報資産には、住民の個人情報をはじめ、行政運営上重要な情報が多数含まれている。これらの情報資産に係る不正アクセス、漏えい、改ざん、業務停止等が発生した場合、住民の権利利益の侵害、行政運営の停滞、さらには市政に対する信用の失墜を招くおそれがある。

近年、情報通信技術の高度化及び行政のデジタル化の進展に伴い、サイバー攻撃の高度化・巧妙化、クラウドサービスの普及、業務委託の拡大等、情報セキュリティを取り巻く環境は大きく変化している。

このような状況を踏まえ、市の機関が相互に連携しつつ、それぞれの権限と責任の下で情報セキュリティを確保するための基本的な方針を定め、統一的かつ継続的な取組を推進する。

（目的）

第１条　日高市サイバーセキュリティ基本方針（以下「市基本方針」という。）は、市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、市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　この市基本方針において、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　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、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) 情報セキュリティポリシー　日高市情報セキュリティポリシー、日高市学校情報セキュリティポリシー又は各実施機関で制定している対策基準をいう。

(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。

（対象とする脅威）

第３条　情報資産に対する脅威として、次に掲げる脅威を想定し、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、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４条　この市基本方針が適用される市の機関は、市長、教育委員会、選挙管理委員会、公平委員会、監査委員、農業委員会、固定資産評価審査委員会及び議会とする。

２　この市基本方針が適用される情報資産は、市の機関が保有する情報資産のうち、次に掲げるものとする。

(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

(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　市の特別職及び一般職の職員、非常勤職員及び臨時職員等（以下「職員等

」という。）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講じる情報セキュリティ対策は、次の各号に掲げる区分に応じ、当該各号に定めるとおりとする。

(1) 組織体制　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　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行う。

(3) 物理的セキュリティ対策　サーバ、パソコン等の情報システム、通信回線、重要機能室等及びその他の情報資産の管理について、物理的な対策を講じる。

(4) 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。

(5) 技術的セキュリティ対策　サーバ、パソコン等の情報システムの管理、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。

(6) 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、業務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。

(7) 業務委託、外部サービス（クラウドサービス）の利用　業務委託、外部サービス（クラウドサービス）を利用する場合には、次の対策を講じる。

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（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。

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。

(8) 評価・見直し　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し、運用改善を

行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

（情報セキュリティ監査及び自己点検の実施）

第７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、定期的に、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８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、情報セキュリティ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　この市基本方針に基づき、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。

附　則

この市基本方針は、令和８年４月１日から施行する。