北海道選挙管理委員会情報セキュリティ基本方針

（目的）

第１条　この方針は、北海道選挙管理委員会の情報システムが取り扱う個人情報及び行政運営上重要な情報の破壊、改ざん又は外部への漏えい等が生じた場合の被害の重大性に鑑み、北海道選挙管理委員会の保有する情報資産を様々な脅威から防御し、北海道選挙管理委員会の情報資産の機密性、完全性及び可用性を維持するための基本的な事項を定め、もって道民の財産及びプライバシーの保全並びに安定的な道行政の実現に資することを目的とする。

（定義）

第２条　この方針において、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子データで構成され、情報処理を行う仕組みをいう。

(3) 電子データ

電子的方式、磁気的方式、光学的方式等の方式により記録された情報をいう。

(4) 情報資産

北海道選挙管理委員会が使用し、所有し、又は管理する次に掲げるものをいう。

①電子データ及びこれを記録するための媒体

②電子データを処理又は伝送するための設備及び機器

③プログラムのライセンス及びその権利を証明するための部材

④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

⑤ネットワーク及び情報システムで取り扱う情報（電子データを入力するための帳票など、印刷した文書を含む。）

⑥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

(5) 情報セキュリティ対策

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

この方針及びこの方針に基づき定められた情報セキュリティ対策基準をいう。

(7) 機密性

情報へのアクセスを認められた者だけが、その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

情報へのアクセスを認められた者が、必要なときに中断することなく、情報及び関連資産にアクセスできる状態を確保することをいう。

(10)その他の関連規程等

道の情報資産の情報セキュリティ対策に関する施策、措置、手順等を定めた規程のほか、通知及び各管理者によるその他の指示事項をいう。

（対象とする脅威）

第３条　情報資産に対する脅威として、次に掲げるものを想定し、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及び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

（適用対象）

第４条　この方針は、地方自治法（昭和 22 年法律第 67 号）第 181 条第２項に規定する北海道選挙管理委員会委員（以下「委員」という。）及び北海道選挙管理委員会規程（昭和 48 年５月 29 日選挙管理委員会告示第 28 号）第 11 条第１項に規定する委員会事務局及び委員会事務局支所（以下「事務局等」という。）に属する職員（以下「職員」という。）に適用する。

（組織体制）

第５条　情報セキュリティ対策の統一的な取組みを確保するため、事務局等において必要な組織体制を整備する。

（委員及び職員の基本的責務）

第６条　委員及び職員は、情報セキュリティ対策の重要性を認識するとともに、業務の遂行に当たっては、情報セキュリティ対策に関係する法令、情報セキュリティポリシー及びその他の関連規程等を遵守しなければならない。

（責務の違反）

第６条の２　前条の責務に違反した委員及び職員は、当該違反の重大性、違反時の状況等に応じて、地方公務員法（昭和 25 年法律第 261 号）第 29 条の規定に基づく懲戒処分等の対象とされる。

（評価及び見直し）

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。また、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。

（情報セキュリティ対策基準の策定）

第 10 条　この方針に基づく対策等を実施するため、必要となる具体的な事項を定めた情報セキュリティ対策基準を策定するものとする。

２　前項の情報セキュリティ対策基準の策定に当たっては、次に掲げる事項について定めるものとする。

(1) 物理的セキュリティに関する事項

(2) 人的セキュリティに関する事項

(3) 技術的セキュリティに関する事項

(4) 運用に関する事項

附則

この方針は、令和８年４月１日から施行する。