富良野広域連合情報セキュリティポリシー

令和８年４月１日

富良野広域連合情報セキュリティ基本方針

本方針は、富良野広域連合を構成する各自治体が共同で策定する情報セキュリティに関する基本方針であり、詳細な技術的・運用的対策については、各構成団体が定める情報セキュリティポリシーに準拠するものとする。

第１章　総則

第１条（目的）

1. 本方針は、富良野広域連合が取り扱う情報資産の機密性、完全性及び可用性を確保することを目的とする。
2. サイバー攻撃、情報漏えい、システム障害等から行政運営及び住民サービスを保護することを目的とする。
3. 各構成団体が異なるネットワーク環境を有していることを前提に、広域連合として共通の基本的な考え方を示すことを目的とする。
4. 構成団体間の連携及び協力により、情報セキュリティ対策の実効性を高めることを目的とする。

第２条（適用範囲）

1. 本方針は、広域連合の事務局、議会及び共同事務に従事する職員等に適用する。
2. 非常勤職員、派遣職員及び業務委託先等の関係者についても、本方針を適用対象とする。
3. 本方針の対象となる情報資産は、広域連合が管理し、又は共同事務のために利用する情報及び情報システムとする。
4. 各構成団体が個別に管理するネットワーク及び情報システムの詳細な取扱いについては、当該構成団体が定める情報セキュリティポリシーに準拠するものとする。

第３条（情報セキュリティの基本要素）

情報セキュリティは、次に掲げる三つの要素を基本とする。

区分	意味	広域連合における基本的な考え方
機密性（Confidentiality）	許可された者のみが情報にアクセスできる状態を保つこと	住民情報や内部情報について、不正な閲覧や漏えいを防止することを基本とする
完全性（Integrity）	情報が正確で改ざんされていない状態を保つこと	共同事務で扱うデータや文書が正確に維持されるよう管理することを基本とする
可用性（Availability）	必要なときに情報やシステムを利用できる状態を保つこと	災害や障害発生時にも行政運営を継続できるよう配慮する

第２章　基本方針

第４条（基本的な考え方）

1. 情報セキュリティ対策は、関係法令並びに国が示す指針及びガイドラインを踏まえて実施するものとする。
2. 情報セキュリティに絶対的な安全は存在しないことを前提とする。
3. 事故の未然防止に加え、発生時の迅速な対応及び再発防止を重視する。
4. 定期的な点検及び見直しにより、継続的な改善を図るものとする。

第５条（組織体制）

1. 広域連合は、情報セキュリティ対策を統括する責任者を定めるものとする。
2. 当該責任者は、方針の推進、構成団体との連絡調整及びインシデント対応方針の整理を担うものとする。
3. 広域連合は、構成団体の情報セキュリティ担当部局と連携し、情報共有及び協力体制の構築に努めるものとする。

第６条（共同利用クラウドの取扱い）

1. 構成団体が共同で利用するクラウドサービスが存在することを前提とする。
2. 共同利用クラウドの利用にあたっては、利用形態及び責任分担を明確にするものとする。
3. 適切なアクセス管理及び情報セキュリティ水準の確保に努めるものとする。
4. 技術的設定及び運用手順の詳細については、各構成団体の情報セキュリティポリシー又は別途定める要領等に基づき実施するものとする。
5. 広域連合は、基本的な考え方の共有及び構成団体間の調整を行うものとする。

第７条（教育・研修）

1. 情報セキュリティに関する教育及び研修は、各構成団体が主体となって実施するものとする。
2. 広域連合は、構成団体と連携し、意識向上及び知識共有を図るものとする。

第８条（インシデント対応）

1. 情報セキュリティインシデントが発生し、又は発生するおそれがある場合には、構成団体と速やかに情報共有を行うものとする。
2. 被害の拡大防止、業務継続及び再発防止に努めるものとする。

第９条（監査・見直し及び合同演習）

1. 本方針の実効性を確保するため、必要に応じて監査又は自己点検を実施するものとする。
2. 点検結果や社会環境等の変化を踏まえ、本方針の見直しを行うものとする。
3. 情報セキュリティに関する合同演習については、実施時期及び内容を別途検討の上、計画的に実施するものとする。

附則

本方針は、令和８年４月１日から施行する。