第１章　情報セキュリティ基本方針

Ⅰ　目的

黒部市の各情報システムが取り扱う情報（以下「情報資産」という。）の中には、市民の個人情報や企業の経営情報等のほか、行政運営上重要な情報など、庁外に漏洩等した場合には極めて重大な信用失墜結果を招く情報が多数含まれている。

一方で、各種手続のオンライン利用の推進や電子自治体の進展が期待されているところであり、黒部市がこの流れに積極的に対応するためには、すべてのネットワーク及び情報システムが高度な安全性を有することが前提条件となり、万が一情報システムの停止等が発生した場合には、広範囲において業務が継続できなくなるなど、住民生活や地域の経済社会活動に重大な支障が生じることとなる。

このため、地方公共団体は LGWAN 等専用のネットワークにより相互に接続しているが、一部の団体で発生した IT 障害がネットワークを介して他の団体に連鎖的に拡大する可能性は否定できない。情報資産の機密性、完全性及び可用性を維持するための対策（以下「情報セキュリティ対策」という。）の実効性を高めるとともに対策レベルを一層強化していくことが求められている。情報資産及び情報システムをさまざまな脅威から防御することは、市民の財産、プライバシー等を守り、事務の安定的な運営と黒部市に対する市民からの信頼の維持向上に寄与するものである。

これらのことから、情報セキュリティ対策を組織的に統一して推進するため、黒部市組織内の情報セキュリティを確保するための方針、体制、対策等を包括的に定めた「黒部市情報セキュリティポリシー」（以下「情報セキュリティポリシー」という。）を定めるものである。

なお、情報セキュリティの確保に絶対安全ということはないことから、情報セキュリティに関する事故の未然防止のみならず、事故が発生した場合の拡大防止・迅速な復旧や再発防止の対策を講じていくことが必要である。

Ⅱ　定義

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

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

本基本方針及び情報セキュリティ対策基準をいう。

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。

8　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（社会保障、地方税若しくは防災に関する事務）又は戸籍事務等に関わる情報システム及びデータをいう。

9　LGWAN 接続系

LGWAN 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（マイナンバー利用事務系を除く。）。

10　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。

11　通信経路の分割

LGWAN 接続系とインターネット接続系の両環境間の通信環境を分離した上で、安全が確保された通信だけを許可できるようにすることをいう。

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。

Ⅲ　対象とする脅威

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

Ⅳ　適用範囲

行政機関及び情報資産の範囲は次のとおりとする。

1 行政機関の範囲

本基本方針が適用される行政機関は、市長部局（水道事業管理者の権限を行う市長部局を含む。）、教育委員会事務局、選挙管理委員会事務局、監査委員事務局、農業委員会事務局及び議会事務局とする。

２ 情報資産の範囲

本基本方針が対象とする情報資産は、次のとおりとする。

ア　ネットワーク、情報システム及びこれらに関する設備、電磁的記録媒体

イ　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。）

ウ　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

Ⅴ　職員等の遵守義務

職員、非常勤職員及び臨時職員（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。

Ⅵ　情報セキュリティ対策

Ⅲで示す脅威から情報資産を保護するため、次の情報セキュリティ対策を講じる。

１　組織体制

本市の情報資産について、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

本市の保有する情報資産を機密性、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　情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の三段階の対策を講じる。

① マイナンバー利用事務系においては、原則として、他の領域との通信をできないようにした上で、端末からの情報持ち出し不可設定や端末への多要素認証の導入等により、住民情報の流出を防ぐ。

② LGWAN 接続系においては、LGWAN と接続する業務用システムと、インターネット接続系の情報システムとの通信経路を分割する。なお、両システム間で通信する場合には、無害化通信を実施する。

③インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。高度な情報セキュリティ対策として、富山県及び県内市町村のインターネットとの通信を集約した上で、自治体情報セキュリティクラウドの導入等を実施する。

４　物理的セキュリティ

サーバ、情報システム室、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。

５　人的セキュリティ

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。

６　技術的セキュリティ

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。

７　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切に対応するため、緊急時対応計画を策定する。

８　業務委託と外部サービスの利用

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。

外部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。

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。

Ⅶ　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。

Ⅷ　情報セキュリティポリシーの見直し

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。

Ⅸ　対策基準の策定

ⅥからⅧまでに規定する対策等を実施するために、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。

Ⅹ　情報セキュリティ実施手順の策定

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。

なお、情報セキュリティ実施手順は、公にすることにより本市の行政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。