第１章　情報セキュリティポリシー

１　目的

高山市の各情報システムが取り扱う情報には、市民の個人情報や行政運営上重要な情報など、外部への漏洩等が発生した場合には極めて重大な結果を招く情報が多数含まれている。

また、近年のいわゆるＤＸ（デジタル・トランスフォーメーション）の進展により、行政のデジタル化が現実のものとなっている。

こうした中、高山市が所掌する情報資産を様々な脅威から防御することは、市民の財産、プライバシー等の保護、事務の安定的な運営、行政のデジタル化のためには必要不可欠である。

また、「サイバーセキュリティ基本法」第 5 条では、地方公共団体においてサイバーセキュリティに関する自主的な施策の策定と実施が責務規定として法定化されている。

このため、高山市が所掌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の対策について総合的、体系的、具体的に取りまとめた高山市情報セキュリティポリシーを定める。

（注）：国際標準化機構（ISO）が定めるもの（ISO7498-2：1989）

機密性（confidentiality）：情報にアクセスすることが認可された者だけがアクセスできることを確実にすること。

完全性（integrity）　：情報及び処理の方法の正確さ及び完全である状態を完全防護すること。

可用性（availability）　：許可された利用者が必要なときに情報にアクセスできることを確実にすること。

２　定義

⑴　ネットワーク

高山市における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）及び記録媒体で構成され、処理を行う仕組みをいう。

⑵　情報

業務の執行に伴ってコンピュータ及び記録媒体に記録されたデータをいう。

⑶　情報システム

業務系のコンピュータ及び記録媒体で構成され、処理を行う仕組みをいう。

⑷　情報資産

ネットワーク及び情報システムの開発と運用に係る全ての情報並びにネットワーク

及び情報システムで取り扱う全ての情報をいう。なお、情報資産には紙等の有体物に出力された情報も含む。

⑸　情報セキュリティ

情報資産の機密性、完全性、可用性を維持することをいう。

⑹　重要機能室

ネットワークの基幹機器及び重要なシステムを設置し、情報システム機器等の管理・運用を行う部屋等の総称をいう。

⑺　管理区域

重要機能室及び情報資産を取り扱う執務室をいう。

⑻　端末等

パソコンやモバイルコンピュータ（持ち運びができる小型軽量なコンピュータのことでタブレット端末やスマートフォンなどのこと）などの情報処理を行う機器の総称をいう。

⑼　情報セキュリティ事故

次に定めることをいう。

- 情報がそれを利用する権限のない者又は職員の操作ミス等により漏洩又は改ざん若しくは破壊されること。
- 情報システムの提供するサービスが妨害され、業務に支障をきたすこと。
- 災害・事故・故障等によりサービス及び業務が停止すること。
- 決定された情報セキュリティ対策が適切に行わないことにより、情報が危険にさらされること。

⑽　情報セキュリティポリシー

高山市が所掌する情報資産に関する情報セキュリティ対策について、総合的、体系的、具体的に取りまとめたものであり、情報セキュリティ対策の最高位に位置するもの。

⑾　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。

⑿　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。）。

⒀　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。

⒁　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するなど、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。

⑮ **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。

⑯ **外部サービス**

Web 会議サービス、SNS（ソーシャルネットワーキングサービス）、検索サービス、翻訳サービス、地図サービス、ホスティングサービスなど、庁外の通信回線やシステムを利用して委託事業者等が提供するサービスをいう。

⑰ **クラウドサービス**

事業者によって定義されたインタフェースを用いた、拡張性、柔軟性を持つ共用可能な物理的又は仮想的なリソースにネットワーク経由でアクセスするモデルを通じて提供され、利用者によって自由にリソースの設定・管理が可能なサービスであって、情報セキュリティに関する十分な条件設定の余地があるものをいう。クラウドサービスの例としては、SaaS（Software as a Service）、PaaS（Platform as a Service）、IaaS（Infrastructure as a Service）等がある。

⑱ **自治体情報セキュリティクラウド**

都道府県と市区町村がインターネット接続回線等を集約し、監視及びログ分析・解析をはじめ高度なセキュリティ対策を実施することをいう。

⑲ **ゼロトラストセキュリティ**

接続元のネットワークを問わず、全てのアクセスを信頼せず検証するセキュリティモデルをいう。

⑳ **安全管理措置**

保有している個人情報の漏洩、滅失又は毀損の防止など、安全に管理するために必要かつ適切な措置を講じることをいう。

㉑ **多要素認証**

システムが正規の利用者かどうかを判断する際の信頼性を高めるために、知識や所有物など複数の認証手段を組み合わせて認証する方式をいう。

㉒ CSIRT（Computer Security Incident Response Team）

コンピュータやネットワーク上で何らかの問題が起きていないかどうか監視すると共に、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う、情報セキュリティに関する統一的な窓口のこと。

3　情報セキュリティポリシーの構成

情報セキュリティポリシーはその性格上、安定的な規範であることが要請されるが、一方では技術の進歩等に伴う情報セキュリティを取り巻く急速な状況への変化に、柔軟に対応することも必要である。

このようなことから、情報セキュリティポリシーを一定の普遍性を備えた情報セキュリティ基本方針と、情報資産を取り巻く状況の変化に依存する情報セキュリティ対策基準に分けて策定する。また、ネットワーク及び情報システム毎の具体的な情報セキュリティ対策については、情報セキュリティ対策基準に基づき情報セキュリティ実施手順を策定する。

項　　目		内　　容
情報セキュリティポリシー	情報セキュリティ基本方針	情報セキュリティ対策に関する統一的かつ基本的な方針
	情報セキュリティ対策基準	情報セキュリティ基本方針を実行に移すための全てのネットワーク及び情報システムに共通の情報セキュリティ対策の基準
情報セキュリティ実施手順		ネットワーク及び情報システム毎に定める情報セキュリティ対策基準に基づいた具体的な実施手順

4　適用範囲

情報セキュリティポリシーの適用範囲を次のように定める。

⑴　適用対象者

職員、 会計年度任用職員（以下、「職員等」という。）及び委託事業者とする。

⑵　適用対象資産

高山市が保有する全ての情報資産とする。

5　職員等及び委託事業者の義務

高山市が所掌する情報資産に関する業務に携わる職員等及び委託事業者は、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、業務の遂行に当たって情報セキュリティポリシー及び実施手順書を遵守する義務を負う。

6　法令遵守

職員等は、職務の遂行において使用する情報資産について、次の法令等を遵守し、これに従わなければならない。

(1)　地方公務員法（昭和２５年法律第２６１号）
(2)　不正アクセス行為の禁止等に関する法律（平成１１年法律第１２８号）
(3)　著作権法（昭和４５年法律第４８号）
(4)　個人情報の保護に関する法律（平成１５年法律第５７号）
(5)　高山市個人情報保護法施行条例（令和４年条例第１２号）
(6)　高山市情報公開条例（平成１２年条例第２４号）
(7)　行政手続における特定の個人を識別するための番号の利用等に関する法律（平成２５年法律第２７号）（以下、「番号法」という。）
(8)　サイバーセキュリティ基本法（平成２６年法律第１０４号）

第２章　情報セキュリティ基本方針

１　目的

情報セキュリティ対策に関する統一的かつ基本的な方針として、情報セキュリティ基本方針を定める。

特に、番号法において定められた事務において、個人番号及び個人番号をその内容に含む個人情報（以下「特定個人情報」という。）を取り扱うため、番号法及び個人情報保護法施行条例に定められる厳格な保護措置もふまえ、管理体制及び対策基準、実施手順等を整備し、職員等に遵守させる等の措置を講じ、適正に特定個人情報を取り扱うことを目的とする。

２　情報セキュリティ管理体制

情報セキュリティ対策を推進、管理するための体制を確立する。

３　情報資産の分類

情報資産をその内容に応じて分類し、その重要性に応じた情報セキュリティ対策を行う。

４　情報セキュリティ対策

情報資産を脅かす脅威の発生度合や発生した場合の影響を考慮し、特に認識すべき脅威を次のとおりとする。

⑴　不正アクセス、ウィルス攻撃、サービス不能攻撃、標的型攻撃等のサイバー攻撃や、部外者による故意の不正アクセス、不正操作による情報資産の破壊・盗難・盗聴・改ざん・消去等

⑵　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洩・破壊・消去等

⑶　職員等や委託事業者による情報資産の持出、誤操作、アクセスのための認証情報、パスワードの不適切管理、故意の不正アクセス、不法行為による破壊・盗聴・改ざん・消去等、搬送中の事故等による情報資産の盗難、規定外の端末接続によるデータ遺漏等

サービス不能攻撃：インターネット経由で大量のデータや不正パケットを送りつけるなどして攻撃対象のシステムがサービスを提供できないようにしたり、システムそのものをダウンさせたりする不正アクセス

標的型攻撃：特定の組織内の情報を狙って行われるサイバー攻撃で、その組織の構成員宛てにコンピュータウィルスが添付された電子メールを送り開封させ感染させる。以降も持続的に潜伏するウィルスも確認されている。

⑷　不正プログラム、地震、落雷、火災等の災害並びに事故、故障等によるサービス及び業務の停止
⑸　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
⑹　電力供給の途絶、通信の断絶、水道供給の途絶等のインフラの障害からの波及等

こうした脅威から情報資産を保護するために、全てのネットワーク及び情報システムに対し次の情報セキュリティ対策を講ずる。

⑴　物理的セキュリティ対策

情報システムを設置する施設への不正な立入り、情報資産に対する脅威・侵害等から保護するための物理的な対策

⑵　人的セキュリティ対策

情報セキュリティに関する権限や責任を定め、全ての職員等及び委託事業者に情報セキュリティポリシーの内容を周知徹底する等、十分な教育及び啓発が講じられるような対策

⑶　技術面及び運用面におけるセキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するための情報資産へのアクセス制御、ネットワーク管理等の技術面の対策、システム開発等の外部委託、ネットワークの監視、情報セキュリティポリシーの遵守状況の確認等の運用面の対策や緊急事態が発生した際に迅速な対応を可能とするための危機管理対策

⑷　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。

ア　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。

イ　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。

ウ　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、都道府県及び市区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を実施する。

⑸　業務委託と外部サービス（クラウドサービス）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（クラウドサービス）を利

用する場合には、利用にかか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。

５　情報セキュリティ対策基準の策定

情報セキュリティ対策を講ずるに当たっては、遵守すべき行為及び判断等の基準を統一的なレベルで定める必要がある。そのため、情報セキュリティ対策を行う上で必要となる基本的な要件を明記した情報セキュリティ対策基準を策定する。

情報セキュリティ対策基準は、公にすることにより高山市の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

６　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を遵守し情報セキュリティ対策を実施するために、個々の情報資産を保護するための対策手順等をそれぞれ定めていく必要がある。そのため、ネットワーク及び情報システムごとに情報セキュリティ実施手順を策定するものとする。

情報セキュリティ実施手順は、公にすることにより高山市の行政運営に重大な支障を及ぼす恐れのある情報であることから非公開とする。

７　緊急時の対策

情報資産への侵害が発生した場合における連絡、証拠保全、被害拡大の防止、復旧等の必要な措置を迅速かつ円滑に実施し、再発防止の措置を講じるために、緊急時の対策を定める。

８　情報セキュリティポリシー遵守状況の確認

情報セキュリティポリシーの遵守を確保するため、情報セキュリティポリシーの遵守状況等を確認する体制を整備するとともに、問題があった場合の対応について定める。

９　情報セキュリティ監査と評価・見直しの実施

情報セキュリティポリシーが遵守されていることを検証するため、定期的に情報セキュリティ監査及び自己点検を実施する。また、監査の結果や、情報セキュリティを取り巻く状況の変化等をふまえ、保有する情報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、リスクを検討したうえで、情報セキュリティポリシーの

評価や見直しを継続的に実施する。