

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IT革命の進展により、電子自治体の構築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、電子自治体構築のためには必要不可欠である。

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性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

(1) 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。

(2) 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。

(3) 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。

(4) 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。

(5) **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。

(6) **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。

(7) **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。

(8) **端末等**

パソコンやモバイルコンピュータなどの情報処理を行う機器の総称をいう。

(9) **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。

(10) **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。

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。

モバイルコンピュータ：持ち運びができる小型軽量の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

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。

(1) 適用対象者

職員、会計年度任用職員（以下、「職員等」という。）及び外部委託事業者とする。

(2) 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 職員等及び外部委託事業者の義務

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外部委託事業者は、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) 行政機関の保有する個人情報の保護に関する法律（平成15年法律第58号）
- (6) 高山市個人情報保護条例（平成12年条例第15号）
- (7) 高山市情報公開条例（平成12年条例第24号）
- (8) 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。）

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。

- (1) ウィルス攻撃、サービス不能攻撃、標的型攻撃等の部外者による故意の不正アクセス又は不正操作による情報資産の破壊・盗難・盗聴・改ざん・消去等
- (2) 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) 職員等又は外部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又はパスワードの不適切管理、故意の不正アクセス又は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。

- (4) 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
- (5) 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
- (6) 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。

(1) 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

(2) 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、全ての職員等及び外部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

(3) 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

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、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。