富山県庁情報セキュリティポリシー

情報政策課

平成２７年７月

目　次

1　目的

「富山県庁情報セキュリティポリシー」（以下「ポリシー」という。）は、情報セキュリティ対策についての基本的事項について定めるものであり、本県が管理する情報資産を様々な脅威から適切に保護し、その機密性、完全性及び可用性を維持することを目的とする。

2　用語の定義

ポリシーに掲げる用語の定義は以下のとおりとする。

（1）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。

機密性：許可された者のみが、その許可された権限の範囲内でのみ情報にアクセスできることが保証されていること。

完全性：情報及びその処理方法が正確であること及び完全であることを保護すること。

可用性：許可された利用者が、必要なときに情報資産に確実にアクセスできることが保証されていること。

（2）情報資産

（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上で管理される情報（これらを印刷した文書を含む。）

（ウ）ネットワーク及び情報システムに関する情報

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）のこと。

情報システム：ネットワーク、コンピュータ他のハードウェア、ソフトウェア及び電磁的記録媒体で構成された業務を処理する仕組みのこと。

（3）脅威

災害、機器障害、故意過失を問わず情報セキュリティを脅かす直接の原因のことであって、以下のものを想定する。

（ア）不正アクセス、ウィルス攻撃、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、重要情報の搾取、内部不正等

（イ）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、プログラム上の欠陥、操作・設定ミス、メンテナンス不備、外部委託管理の不備、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

（ウ）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

（エ）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

（オ）電力供給の途絶、通信の途絶等のインフラの障害からの波及等

（4）脆弱性

情報セキュリティに対する脅威を引き起こす可能性を高める因子のこと。

3　適用範囲

ポリシーは、原則として本県が保有する全ての情報資産及びこれらを利用する者に適用する。

4　適用対象者の責務

職員（非常勤職員及び臨時職員を含む。）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ち、ポリシーの目的を理解し、業務の遂行に当たって遵守しなければならない。

5　情報セキュリティ管理体制

ポリシーの適正な運用による情報セキュリティの確保を図るため、富山県庁情報化推進本部の下に「富山県庁情報セキュリティ対策委員会」（以下「対策委員会」という。）を設置し、これを中心とした全庁的な管理体制を確立する。

6　情報セキュリティマネジメント

情報セキュリティマネジメントは以下により行うものとする。

（1）リスク分析の実施

情報資産ごとに、脅威と情報セキュリティが損なわれた場合の影響及び脆弱性を検証する。

（2）「富山県庁情報セキュリティ対策基準」の策定

情報セキュリティを確保するために行うべき、具体的な遵守事項及び判断基準等を定める「富山県庁情報セキュリティ対策基準」（以下「対策基準」という。）を策定する。対策基準はポリシーに基づき、対策委員会において策定するものとし、対策委員会において、見直しの検討及び情報セキュリティに関する事項の総合 調整を行うものとする。

（3）「富山県庁情報セキュリティ実施手順」の策定

情報セキュリティを確保するため具体的に必要な手段及び手続きについて「富山県庁情報セキュリティ実施手順」（以下「実施手順」という。）を策定する。実施手順は対策基準に基づき、情報システムごとにそれぞれの管理者において策定するものとし、公にすることにより本県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。

（4）情報セキュリティ対策

脅威及び脆弱性を縮小又は除去するために、以下の情報セキュリティ対策を実施する。

ア　人的セキュリティ対策

全てのポリシー適用対象者を情報資産への関わり方により分類し、各々について情報セキュリティに関する権限と責任を定める。また、ポリシーの主旨を周知徹底し、必要な教育及び啓発を行う。

イ　物理的セキュリティ対策

情報資産を有する施設への不正な立入り、損傷、盗難等の事故及び災害から情報資産を保護するための物理的な対策を講ずる。

ウ　技術的セキュリティ対策

コンピュータ等の管理、不正プログラム対策、不正アクセス対策等、情報セキュリティの確保に必要な技術的対策を講ずる。

エ　アクセス制御

情報システムの利用に際して、情報セキュリティの確保に必要なアクセス制御を行う。

オ　運用面の対策

情報システムの監視、ポリシーの遵守状況の確認、外部委託を行う際のセキュリティ確保等、ポリシーの運用面の対策を講じるものとする。また、情報資産への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。

カ　情報システムの開発保守におけるセキュリティ対策

情報システムの開発保守に際して、情報セキュリティ確保に必要な配慮事項を明確に定め、対策を講ずる。

キ　業務継続性の確保対策

情報セキュリティが損なわれた場合においても、その被害を最小限にとどめ、業務を継続し又は速やかに復旧させるために必要な手順をあらかじめ定め、対策を講ずる。

（5）情報セキュリティ監査及び自己点検の実施

ポリシー及びこれに基づく情報セキュリティ対策の遵守状況を確認するため、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行う。

（6）評価及び見直しの実施

ポリシーの実効性を確保するため、環境の変化及び情報セキュリティ監査及び自己点検の結果を踏まえ、定期的にポリシー及び情報セキュリティ対策の評価及び見直しを行う。

7　施行

ポリシーは、平成１５年９月４日から施行する。

ポリシーは、平成１９年５月１４日から施行する。

ポリシーは、平成２３年１２月１４日から施行する。

ポリシーは、平成２７年７月３日から施行する。