岩手県情報セキュリティポリシー

第３.７版

平成 14 年	３月	27 日	策　　定
平成 21 年	１月	27 日	全部改正
平成 22 年	４月	１日	一部改正
平成 26 年	４月	１日	一部改正
平成 27 年	４月	１日	全部改正
平成 31 年	４月	１日	一部改正
令和 ２ 年	４月	１日	一部改正
令和 ３ 年	４月	１日	一部改正
令和 ３ 年	10 月	１日	一部改正
令和 ５ 年	４月	１日	一部改正
令和 ５ 年	10 月	１日	一部改正
令和 ８ 年	３月	31 日	一部改正

ふるさと振興部 科学・情報政策室

目　　　　　次

第１章　情報セキュリティ基本方針

１　目的

県の各情報システムが取り扱う情報には、県民の個人情報のみならず行政運営上重要な情報など、外部に漏えい等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。

したがって、これらの情報及び情報を取り扱う情報システムを様々な脅威から防御することは、県民の財産、プライバシー等を守るためにも、また、事務の安定的な運営のためにも必要不可欠である。ひいては、このことが県に対する県民からの信頼の維持向上に寄与するものである。

また、近年の情報通信技術の普及・高度化と当該技術を活用したサービス等の拡大により、行政運営においてもクラウドサービスをはじめとする外部サービスの利用が増えている。今後もこれらを積極的に活用するためには、情報の漏えい等の防止はもとより、災害等非常時においても常に情報にアクセスできる状態の確保が重要である。

以上のことから、県の情報資産の機密性、完全性及び可用性を維持するための対策（情報セキュリティ対策）を整備するために岩手県情報セキュリティポリシーを定めることとし、このうち、情報セキュリティ基本方針については県の情報セキュリティ対策の基本的な方針として、情報セキュリティポリシーの対象、位置付け等を定めるものとする。

２　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）　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。

（５）　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。

（６）　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。

（７）　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（社会保障又は地方税に関する事務）に関わる情報システム及びデータをいう。

（８）　ＬＧＷＡＮ接続系

財務会計、給与等、総合行政ネットワーク（以下「ＬＧＷＡＮ」という。）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。

（９） インターネット接続系

グループウェア、インターネットメール等、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。

（10） 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。

（11） 無害化処理

インターネットメールの添付ファイル等、インターネット接続系で取得したファイルや外部記憶媒体に保存されたファイルを端末へ取り込む際に、コンピュータウイルス等の不正プログラムの付着が持ち込まれない等、安全な処理を行うことをいう。

（12） 端末

情報システムの構成要素である機器のうち、情報システムの利用者が情報処理を行うために直接操作するもの（搭載されるソフトウェア及び直接接続され一体として扱われるキーボードやマウス等の周辺機器を含む。）をいう。

（13） モバイル端末

端末のうち、業務上の必要に応じて移動させて使用することを目的としたものをいい、端末の形態は問わない。モバイル端末には、職員ひとり一台端末も含まれる。

（14） 電磁的記録媒体

電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、情報システムによる情報処理の用に供されるものが記録される有体物をいう。また、電磁的記録媒体には、サーバ装置、端末、通信回線装置等に内蔵される内蔵電磁的記録媒体と、ＵＳＢメモリ、外付けハードディスクドライブ、ＤＶＤ－Ｒ、磁気テープ等の外部電磁的記録媒体がある。

（15） 外部サービス

事業者等の庁外の組織が情報システムの一部又は全部の機能を提供するものをいう。ただし、当該機能において自組織の情報が取り扱われる場合に限る。

（16） クラウドサービス

事業者によって定義されたインターフェースを用いた、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。

３　情報セキュリティポリシーの位置付けと職員の遵守義務

情報セキュリティポリシーは、県が保有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、体系的かつ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頂点に位置するも

のである。

したがって、知事をはじめとして県が保有する情報資産に関する業務に携わる全ての職員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もつとともに業務の執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する義務を負うものとする。

4　情報セキュリティ管理体制

県の情報資産について、組織として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ものとする。

5　情報資産の分類

情報資産をその内容に応じて分類し、その重要度に応じた情報セキュリティ対策を行うものとする。

6　情報資産への脅威

（1） 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行うものとする。

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、重要情報の搾取、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、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 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等

④ 大規模・広範囲にわたる疾病による要員不足に伴う情報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

（2） その他「地方公共団体における情報セキュリティポリシーに関するガイドライン」をはじめとする国等が策定するガイドライン等を参考に、最新の脅威に対する情報セキュリティ対策を行うものとする。

7　適用範囲

（1） 行政機関の範囲

この情報セキュリティポリシーが対象とする県の組織の範囲は、知事部局、議会事務局、監査委員事務局、各委員会の事務部局及び地方公営企業とし、警察本部及び各教育機関は対象外とする。

ただし、対象外の組織においても、行政情報ネットワークや財務会計システムなど、県の情報システムを利用する範囲内で、この情報セキュリティポリシーを適用するものとする。

なお、教育に関する情報システム及び警察業務に関する情報システムについては、この情報

セキュリティポリシーの対象から除き、対象となる情報システムと物理的に分けなければならない。

また、県以外の組織に県の情報システムが設置されている場合は、この情報セキュリティポリシーを適用する。

（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。

① ネットワーク、情報システム、これらに関する設備及び電磁的記録媒体

② ネットワーク及び情報システムで取り扱う情報（操作記録や設定情報を印刷した文書を含む。）

③ 情報システムの仕様書、設計書及びネットワーク図等の情報システム関連文書

8 情報セキュリティ対策

上記６で示した脅威から情報資産を保護するために、以下の情報セキュリティ対策を講ずるものとする。

（1） 情報システム全体の強靭性の向上

情報セキュリティ強化を目的とし、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ずる。

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、マイナンバーを含む個人情報の流出を防ぐ。

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、無害化処理を実施する。

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、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による通信監視を実施する。

（2） 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、情報資産への損傷・妨害等から保護するために物理的な対策を講ずる。

（3） 人的セキュリティ対策

情報セキュリティに関し、職員が遵守すべき事項を定めるとともに、全ての職員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に必要な対策を講ずる。

（4） 技術的セキュリティ対策

情報資産へのアクセス制御、コンピュータ及びネットワーク管理等の技術的な対策を講ずる。

（5） 運用におけるセキュリティ対策

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等の運用面の対策を講ず

る。

また、情報資産に係る被害が発生した場合又は発生する恐れがある場合に迅速な対応を可能とするための危機管理対策を講ずる。

（６） 外部サービスの利用におけるセキュリティ対策

ネットワーク及び情報システムの開発又は運用保守を外部委託する場合には、外部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、外部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、契約に基づき必要な措置を講ずる。

また、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、対策を講ずる。

（７） 評価・見直し

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し、運用改善を行い、情報セキュリティの向上を図る。情報セキュリティポリシーの見直しが必要な場合は、適宜情報セキュリティポリシーの見直しを行う。

９　情報セキュリティ対策基準の策定

県の様々な情報資産について、上記８の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ものとする。

10　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て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、情報資産に対する脅威及び情報資産の重要度に対応する情報セキュリティ対策基準の基本的な要件に基づき、各室課等の長が保有する重要な情報資産の情報セキュリティ実施手順を策定するものとする。

なお、情報セキュリティポリシーのうち情報セキュリティ対策基準及び情報セキュリティ実施手順は、公にすることにより県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原則非公開とする。

11　情報セキュリティ監査等及び自己点検の実施

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。

12　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となった場合には、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を見直す。