地方独立行政法人岩手県工業技術センター情報セキュリティ基本方針

制定　令和８年３月 31 日

１　目的

本基本方針は、地方独立行政法人岩手県工業技術センター（以下「法人」という。）が保有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、法人が実施する情報セキュリティ対策について基本的な事項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）情報資産

情報資産とは、次のものをいう。

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

（４）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。

（５）情報セキュリティポリシー

本基本方針及び岩手県が策定する「岩手県情報セキュリティポリシー」をいう。

（６）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。

（７）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。

（８）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。

（９）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。

(10) 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。

(11) 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。

(12) 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。

(13) 外部サービス

事業者等の法人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、当該機能において法人の情報が取り扱われる場合に限る。

(14) 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　職員の義務

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

法人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　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）情報システムの強靭性の向上

情報セキュリティ強化を目的とし、不正通信の監視機能の強化等の情報セキュリティ対策を実施する。

（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。

8　情報セキュリティ対策基準

法人の様々な情報資産について、上記７の情報セキュリティ対策を講ずるに当たっては、岩手県が策定する情報セキュリティ対策基準を適用する。

9　情報セキュリティ実施手順

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は、岩手県が策定する情報セキュリティ実施手順を適用する。

なお、情報セキュリティ実施手順は、公にすることにより岩手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されているものである。

10　情報セキュリティ監査等の実施

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。

11　評価の実施

情報セキュリティ監査の結果等により、情報セキュリティポリシーに定める事項及び情報セキュリティ対策の評価を実施する。