公益財団法人岐阜県建設研究センター情報セキュリティ基本方針（平成25年4月1日施行）の一部を改正し、次のとおり定める。

平成29年4月1日

公益財団法人岐阜県建設研究センター　理事長　高木　善幸

公益財団法人岐阜県建設研究センター情報セキュリティ基本方針

（趣旨）

第１条　公益財団法人岐阜県建設研究センター情報セキュリティ基本方針(以下「基本方針」という。)は、公益財団法人岐阜県建設研究センター(以下「研究センター」という。)が公益法人として業務の中立性、公平性、公正性及び透明性を確保し、県、市町村の建設行政を補完支援する機関として、建設ICTの総合支援を目的とした県域統合型GIS等情報システムの活用がその運営に欠かせないものとなっており、研究センターの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、研究センター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ことを目的とする。

（適用範囲）

第２条　基本方針が適用される範囲は、研究センターとする。

２　基本方針が対象とする情報資産は、次の各号のとおりとする。

(１)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

(２)ネットワーク及び情報システムで取り扱う情報

(３)情報システムの仕様書及びネットワーク図等のシステム関連文書

（用語の定義）

第３条　基本方針において、次の各号に掲げる用語の定義は、当該各号に定めるところによる。

(１)機密性

情報にアクセスすることが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。

(２)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。

(３)可用性

情報にアクセスすることが認められた者が、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。

(４)情報セキュリティ

情報の機密性、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。

(6)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。

(7)情報セキュリティポリシー

基本方針及び第９条に規定する情報セキュリティ対策基準をいう。

(8)ドキュメント

情報システムに関する次に掲げる文書及び電磁的記録をいう。

ア　システム設計書　情報処理の手順並びに機器及びプログラムの構成概要を記録したもの

イ　プログラム仕様書　情報処理の手順を記録したもの

ウ　プログラムリスト　情報処理の手順をプログラム言語を用いて記述したもの

エ　操作説明書　機器の操作方法の説明を記録したもの

(役職員の遵守事項)

第４条　研究センターの業務に携わる理事長、常勤の役員及び職員(非常勤職員、臨時職員を含む。以下同じ。)(以下「役職員」という。)並びに外部委託業者は、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は情報セキュリティを遵守しなければならない。

(対象とする脅威)

第５条　研究センターは、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実施する。

（１）部外者の侵入、不正アクセス、ウイルス攻撃、サービス不能攻撃、盗難等の意図的な要因による情報資産の漏えい・破壊・消去、重要情報の詐取、内部不正等

（２）情報資産の無断持ち出し、無許可ソフトウエ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、外部委託管理の不備、マネジメントの欠陥、盗難、紛失、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、火災等の災害や事故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、通信の途絶等のインフラの障害からの波及等

(情報セキュリティ対策)

第６条　研究センターは、前条の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じる。

（１）組織体制

研究センターが保有する情報資産について、情報セキュリティ対策を推進・管理するための組織体制を確立する。

（２）情報資産の分類と管理

研究センターが保有する情報資産を重要度に応じて分類し、当該分類に基づき情報セキュリティ対策を行う。

（３）物理的セキュリティ

情報システム及びその設置場所等の管理について、物理的な対策を講じる。

（４）人的セキュリティ

情報セキュリティに関し、役職員が遵守すべき事項を定めるとともに、十分な教育及び啓発を行う等の必要な人的な対策を講じる。

（５）技術的セキュリティ

コンピュータの管理、アクセス制御、不正プログラム対策、不正アクセス対策等の技術的な対策を講じる。

（６）運用

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、外部委託を行う際のセキュリティ確保等、情報セキュリティポリシーの運用面の対策を講じるものとする。また、情報資産へのセキュリティ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。

（情報セキュリティ監査及び自己点検の実施）

第７条　研究センターは、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する。

（情報セキュリティポリシーの見直し）

第８条　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になった場合には、情報セキュリティポリシーの見直しをする。

（情報セキュリティ対策基準の策定）

第９条　この方針に規定する対策等を実施するために、具体的な遵守事項及び判断基準等を定める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。

（情報セキュリティ対策実施手順の策定）

第 10 条　対策基準に基づき、情報セキュリティ対策を実施するにあたり、具体的な手順を定めた情報セキュリティ対策実施手順(以下「実施手順」という。)を策定するものとする。なお、実施手順は、公にすることにより研究センターの業務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。

附　則

この方針は、平成２５年４月１日から施行する。

附　則

この方針は、平成２９年４月１日から施行する。