福井県丹南広域組合情報セキュリティ対策に関する規則

平成29年2月1日　規則第1号

（目的）

第1条　この規則は、福井県丹南広域組合（以下「組合」という。）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。

（定義）

第2条　この規則において使用する用語は、福井県丹南広域組合行政組織規則（平成3年規則第1号）において使用する用語の例によるほか、次の各号に掲げる用語の意義は、それぞれ当該各号に定めるところによる。

(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並びにその構成機器である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　次に掲げるものをいう。

ア　ネットワーク及び情報システム

イ　アに掲げるものに関する設備

ウ　アに掲げるものに関する電磁的記録媒体

エ　アに掲げるもので取り扱う情報(用紙に出力したものを含む。)

オ　アに掲げるものの設計書、仕様書等関連文書

(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)　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。

(6)　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。

(7)　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、情報にアクセスすることができる状態を確保することをいう。

(8) 情報セキュリティポリシー　この規則及びこの規則に基づき別に定められた福井県丹南広域組合情報セキュリティ対策基準をいう。

(9) 職員等　福井県丹南広域組合職員定数条例（平成２年条例第７号）で規定する一般職の職員、嘱託職員及び臨時職員をいう。

(10) 外部要員　組合との業務委託等の契約に基づき作業する職員等以外の者をいう。

（対象とする脅威）

第３条　管理者は、次の各号に掲げる事項を情報資産に対する脅威として想定し、情報セキュリティ対策を実施する。

(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、改ざん及び消去、重要情報の詐取、内部不正等

(2) 情報資産の無断持ち出し、無許可ソフトウェアの使用等の規定違反、設計及び開発の不備、プログラム上の欠陥、操作及び設定の誤り、メンテナンス不備、内部及び外部の監査機能の不備、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、火災等の災害による業務の停止等

(4) 大規模及び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、通信の途絶による障害からの波及等

（適用範囲）

第４条　この規則の適用範囲は、次に定めるところによる。

(1) 適用対象者　職員等及び本庁で作業する外部要員とする。

(2) 適用資産　組合が管理する全ての情報資産とする。

（職員等の遵守義務）

第５条　職員等は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たって情報セキュリティポリシーを遵守しなければならない。

（出先機関及び附属機関の職員の関与）

第６条　管理者は、出先機関及び附属機関の職員に対し、組合が実施する情報セキュリティ対策に積極的に関与させるよう努めるものとする。

（外部要員の管理）

第７条　管理者は、外部要員を使用する場合、契約等に基づき、第５条と同様の内容を外部要員に対しても義務づけし、管理するものとする。

（情報セキュリティ対策）

第８条　管理者は、第３条に規定する脅威から情報資産を保護するために、次に掲げる情報セキュリティ対策を講ずるものとする。

(1)　情報資産を機密性、完全性及び可用性に応じて分類し、管理すること。

(2)　情報資産の管理について、物理的な対策を講ずること。

(3)　情報セキュリティに関し、職員等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人的な対策を講ずること。

(4)　コンピュータ等の管理、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対策を講ずること。

(5)　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の運用面の対策を講ずること。

（最高情報セキュリティ管理者）

第９条　管理者は、管理者の属する市町の副市町長の職にある者を最高情報セキュリティ管理者とし、情報セキュリティ対策を推進するための全庁的な組織体制を確立させるものとする。

（情報セキュリティ対策基準の策定）

第１０条　管理者は、第８条に掲げる情報セキュリティ対策を実施するための基準（以下「対策基準」という。）を策定するものとする。

（情報セキュリティ実施手順の策定）

第１１条　管理者は、この規則及び対策基準に従い、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を策定するものとする。

（情報セキュリティ監査及び自己点検の実施）

第１２条　管理者は、この規則及び対策基準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ものとする。

（情報セキュリティポリシーの見直し）

第１３条　管理者は、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又は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を見直すものとする。

附　則

この規則は、平成２９年２月１日から施行する。