○相楽東部広域連合情報セキュリティに関する規則

令和３年８月１日

規則第３号

（目的）

第１条　この規則は、相楽東部広域連合（以下「本連合」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、本連合が実施する情報セキュリティ対策に関する基本的な事項を定めることにより、情報システムを活用した行政事務の効率化を図ることを目的とする。

（用語の意義）

第２条　この規則における用語の意義は、次の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、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、電磁的記録媒体及びこれらを接続するネットワークで構成され、情報処理を行う仕組みをいう。

(3)サーバ等

ネットワーク上で情報を処理し、接続されたパソコン等の端末機に情報を提供する、コンピュータ(ホストコンピュータを含む。）をいう。

(4)端末

ネットワークを通じてサーバに接続されたパソコン等の端末機をいう。

(5)電子情報

情報システム並びに情報システムの開発、保守及び運用に係る全ての電子情報(電子的、磁気的、その他人の知覚によって認識することができない方式で作られた記録をいい、プログラム等のソフトウェアを含む。）をいう。

(6)記録媒体

電子情報を保管する記録装置のうち、取りはずして使用することが可能な外部記憶装置(USBメモリ、SDカード等)、光ディスク(CD、DVD等)、光磁気ディスク(MO等)、磁気ディスク(FD等)、磁気テープその他これらに類するものをいう。

(7)アクセス

電子情報を保管する記録装置に対して、データの書き込み、読み出しを行うことをいう。

(8)情報資産

ネットワーク及び情報システムで取り扱う電子情報をいう。

(9)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。

(10)情報セキュリティポリシー

情報セキュリティに関する基本的な考え方を規定した「基本方針(本規則)」と情報セキュリティを確保するために遵守すべき行為等の基準を示した「対策基準(情報セキュリティ対策要綱)」をいう。本連合における情報セキュリティポリシー(以下「ポリシー」という。）は、本規則及びこの規則に基づき別に定められた相楽東部広域連合情報セキュリティ対策要綱（令和３年要綱第１号）をもって構成する。

(11)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。

(12)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。

(13)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。

(14)CISO(シーアイエスオー)

最高情報セキュリティ責任者(Chief Information Security Officer)の略称をいう。
情報セキュリティ体制を強化するため、IT 化推進や情報システム最適化を担う最高情報責任者(CIO：Chief Information Officer)とは別に、情報セキュリティを統括する機関として設置される。

(15)CSIRT(シーサート)

情報セキュリティインシデント対応チーム(Computer Security Incident Response Team)の略称をいう。情報システムに対するサイバー攻撃等による情報セキュリティ上の事故(インシデント)が発生した際に、状況の把握・分析、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能とするための機能を有する体制を指す。

(適用範囲)

第 3 条　この規則が対象とする実施機関の範囲は、総務課、環境課、教育委員会、選挙管理委員会、公平委員会、監査委員会及び議会とする。

2　この規則が対象とする情報資産の範囲は、次の各号に掲げるとおりとする。

(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(これらを印刷した文書を含む。)

(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

(対象とする脅威)

第 4 条　情報資産に対する脅威として、次の各号に掲げる脅威を想定し、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・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・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、水道供給の途絶等のインフラの障害からの波及等

(職員等の遵守義務)

第 5 条　本連合の業務に携わる全ての職員及び会計年度任用職員(以下「職員等」という。)並びに外部委託事業者は、情報セキュリティの重要性について共通の認識を持ち、業務の遂行に当たってポリシーを遵守しなければならない。

(情報セキュリティ対策)

第6条　第4条に規定する脅威から情報資産を保護するために、次の各号に掲げるとおり情報セキュリティ対策を講じる。

(1)組織体制

本連合の情報資産について、情報セキュリティ対策を推進する全庁的な組織体制を確立することをいう。

(2)情報資産の分類と管理

本連合の保有する情報資産を重要性に応じて分類し、当該分類に基づき情報セキュリティ対策を行うことをいう。

(3)物理的セキュリティ

サーバ、通信回線等及び職員等のパソコン等の管理について、物理的な対策を講じることをいう。

(4)人的セキュリティ

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じることをいう。

(5)技術的セキュリティ

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じることをいう。

(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ことをいう。

また、情報資産に対する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。

(外部委託)

第7条　本連合の情報システムの開発、運用、保守等を外部に委託する場合は、情報セキュリティの確保に必要な対策を講じなければならない。

(情報セキュリティに関する事案への対応)

第8条　情報資産に対するセキュリティ侵害等の事案が発生した場合の対応をあらかじめ定めるとともに、情報セキュリティに関する事案(自然災害等を含む。)が発生した際には、定められた対応を迅速かつ円滑に実施し、その影響を最小限にするとともに再発防止のために必要な対策を講じる。

(違反への対応)

第9条　職員等がポリシー、関係法令又は本連合が定める条例等に違反した場合は、地方公務員法(昭和25年法律第261号)等に基づき、懲戒処分等の対象とする。

(情報セキュリティ監査及び自己点検の実施)

第10条　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11条　情報セキュリティ監査及び自己点検の結果、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、ポリシーを見直す。

（公開範囲）

第 12 条　この規則は、本連合の情報資産を利用し、運用、管理及び保守する全ての職員等並びに外部委託事業者に公開するものとする。

（対策要綱及び実施手順の策定）

第 13 条　第 6 条、第 10 条及び第 11 条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要綱を策定する

2　対策要綱に基づき、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実施手順を策定する。実施手順は、公にすることにより本連合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。

（その他）

第 14 条　この規則に定めるもののほか、情報セキュリティに関し必要な事項については、その都度連合長が定める。

附　則

この規則は、令和 3 年 8 月 1 日から施行する。