愛北広域事務組合情報セキュリティポリシー

平成２７年４月１日　策定

令和　８年９月１日　改正

目　次

第1章　情報セキュリティ基本方針

1　目的

この基本方針は、愛北広域事務組合の情報システム等を様々な脅威から守り、情報資産の機密性、完全性及び可用性を維持するための基本的な対策を整備するため「愛北広域事務組合情報セキュリティポリシー」（以下「情報セキュリティポリシー」という。）を定めるものとする。

2　定義

この情報セキュリティポリシーにおいて、次に掲げる用語の意義は、当該各号に定めるところによる。

（１）電子情報システム

電子情報処理装置のハードウェア及びソフトウェア、ネットワーク並びに記録媒体で構成され、電子情報処理を行うシステムをいう。

（２）情報資産

ネットワークを利用しないコンピュータ及び電子情報システムで取り扱う全ての情報(紙等に出力した情報を含む。)をいう。

（３）情報セキュリティ

電子情報システム及び情報資産を様々な脅威から守り、常に適正な管理及び運用が継続できるように安全性を確保することをいう。

（４）機密性

情報にアクセスすることが認可された者だけがアクセスできることを確実にすることをいう。

（５）完全性

情報及び処理の方法の正確さ及び完全である状態を安全防護することをいう。

（６）可用性

許可された利用者が必要なときに情報にアクセスできることを確実にすることをいう。

3　職員等の義務

情報セキュリティポリシーは、情報セキュリティ対策全般の基本方針である。従って、電子情報システム及び情報資産に携わる全ての者（以下「職員等」という。）が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 情報セキュリティ対策

電子情報システム及び情報資産を、不正アクセス等による改ざんや災害、事故等の様々な脅威から防御及び保護するため、次の情報セキュリティ対策を講ずるものとする。

（１）情報セキュリティ管理体制の整備

電子情報システム及び情報資産の適正な管理及び運用のため、情報セキュリティの管理体制を整備する。

（２）セキュリティ対策

電子情報システム及び情報資産を、不正アクセス等による改ざんや災害、事故等の様々な脅威から物理的、技術的、運用において防御及び保護するために必要な措置を整備する。

（３）情報セキュリティ対策等の周知及び教育

職員等に情報セキュリティの重要性を周知徹底するため、教育及び研修を行う。

（４）情報セキュリティ対策の監査及び見直し

情報セキュリティポリシーの遵守状況等を把握するとともに、その時々の ICT 社会に柔軟に対応するため、必要に応じて情報セキュリティに関する監査を実施し、情報セキュリティ対策等の評価及び見直しを行う。

第2章　情報セキュリティ対策基準

1　趣旨

情報セキュリティ対策基準は、不正アクセス等による改ざんや災害、事故等の様々な脅威から電子情報システム及び情報資産を防御及び保護するために必要となる情報セキュリティ対策の基本となる事項を定めることを目的とする。

2　対象範囲

この情報セキュリティポリシーが対象とする範囲は、管理者、監査委員及び議会とする。

3　情報セキュリティ管理体制

情報セキュリティ対策等を適正に管理及び運営するために、管理体制を整備する。

（1）全ての電子情報システム及び情報資産の安全性及び信頼性の確保を図り、情報セキュリティを管理するため、情報システム管理者を置く。

（2）情報システム管理者は、事務局長をもって充てる。

（3）所属において情報セキュリティポリシー及び関連法令等を遵守し、電子情報システム及び情報資産の適正利用を管理及び運営するため、情報処理責任者を置く。

（4）情報処理責任者は、情報処理を所管する課、施設等の長をもって充てる。

（5）情報システム管理者は、情報セキュリティポリシー及び関連法令等の遵守状況の確認及び指導等を行うため、情報処理責任者等を招集して情報セキュリティ会議を開催することができる。

（6）情報処理責任者は、所属職員が情報セキュリティポリシー及び関連法令等を遵守し、適正に電子情報システム及び情報資産を利用するよう指導等を行うことができる。

4　セキュリティ対策

全ての電子情報システム及び情報資産を不正アクセス等による改ざんや災害、事故等の様々な脅威から防御及び保護するため、次に掲げるセキュリティ対策を実施するものとする。

（1）重要な情報資産は、定期的に記憶媒体に情報資産のバックアップ用を複製するものとする。

（2）重要な情報資産を記録している情報機器の電源は、適切に停止するまでの間に十分な電力を供給する容量の予備電源を備えておくものとする。

（3）重要な情報資産を扱う電子情報システムと外部との接続に利用する回線

は、盗聴、改ざん等の脅威を防止できるセキュリティ対策がされたものでなければならないものとする。

（４）重要な情報資産を扱う電子情報システムと外部との接続においては、適切なアクセス制御等の措置を講ずるものとする。

（５）職員等が利用する情報機器については、記憶媒体の利用制限や電子情報システムの管理及び運営に支障を及ぼすような行為ができないようシステム利用上の制限をシステムに設ける等の適切な措置を講ずるものとする。

（６）情報システム管理者は、ネットワークへのアクセス記録や情報セキュリティに必要な記録等電子情報システムの適正な管理及び運営に必要な事項を一定期間保存する措置を講ずるものとする。

（７）情報機器及び情報資産の適正な管理及び運営を図るため、必要な事項を定めるものとする。

（８）電子情報システムの利用を適正に管理及び運営するため、必要な事項を定めるものとする。

（９）情報処理を委託する場合は、情報保護を遵守させるために必要な要件を契約書等に定めるものとする。

（１０）情報システム管理者は、情報処理責任者に対して情報セキュリティに関する事項等について、指導等を行うことができるものとする。

（１１）職員等は、情報セキュリティの重要性を認識し、情報セキュリティポリシー及び関連法令等を遵守しなければならないものとする。

５ 情報セキュリティ対策等の周知及び教育

情報システム管理者及び情報処理責任者は、職員等及び外部委託事業者に対して、情報セキュリティ対策の重要性や情報セキュリティポリシー及び関連法令等を遵守するよう周知徹底に努めるものとする。

６ 情報セキュリティ対策の監査及び見直し

（１）情報セキュリティポリシーの遵守状況等を把握するとともに、その時々のICT 社会に柔軟に対応するため、また、情報セキュリティ対策の点検及び評価を行うため必要に応じて情報セキュリティ監査（以下「セキュリティ監査」という。）を行うものとする。

（２）セキュリティ監査については、外部の機関等に委託することができるものとする。