気仙広域連合・
気仙広域連合議会・
気仙広域連合選挙管理委員会・
気仙広域連合監査委員
情報セキュリティ基本方針

令和８年３月 30 日

気仙広域連合
気仙広域連合議会
気仙広域連合選挙管理委員会
気仙広域連合監査委員

1　目的

気仙広域連合（以下「広域連合」という。）、気仙広域連合議会（以下「議会」という。）、気仙広域連合選挙管理委員会（以下「選挙管理委員会」という。）及び気仙広域連合監査委員（以下「監査委員」という。）の各情報システムが取り扱う情報資産には、個人情報や行政運営上重要な情報など、外部に漏えい等した場合には極めて重大な結果を招く情報が多数含まれている。

したがって、これらの情報及び情報を取り扱う情報システムを人的脅威や災害、事故等から防御することは、気仙広域連合構成市町の住民（以下「住民」という。）の財産、プライバシー等の保護及び事務の安定的な運営に必要不可欠であり、広域連合及び議会並びに選挙管理委員会及び監査委員（以下「広域連合関係機関」という。）に対する住民からの信頼の維持向上にも寄与するものである。

また、住民サービスの向上と業務の効率化を図るため、情報システムは行政運営基盤として欠かせないものとなっており、広域連合関係機関の業務執行を今後も円滑に進めるためには、広域連合関係機関が管理している情報システムが高度な安全性を有することが不可欠である。

このことから、広域連合関係機関の情報資産の機密性、完全性及び可用性（注）を維持するための対策（情報セキュリティ対策）を整備するため、対象、位置付け等を規定する情報セキュリティ基本方針（以下「基本方針」という。）を定めることとし、情報セキュリティの確保に最大限取り組むこととする。

（注）：国際標準化機構(ISO)が定めるもの(ISO7498-2：1989)

機密性 (confidentiality)	情報にアクセスすることが許可された者だけがアクセスできる状態を確保すること。
完全性 (integrity)	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。
可用性 (availability)	情報のアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること。

2　定義

(1) 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。

(2) 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。

(3) 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。

(4) 情報セキュリティインシデント

情報セキュリティに関する障害、事故及びシステム上の欠陥をいう。

(5) 介護認定審査会支援システム接続系

介護認定審査会支援システムに接続された情報システム及びその情報システムで取り扱うデータをいう。

(6) インターネット接続系

インターネットメール、ホームページ管理ソフトウェアなどに関わるインターネットに接続された情報システムで取り扱うデータをいう。

(7) 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。

3 対象とする脅威

情報資産に対する脅威として以下を想定し、情報セキュリティ対策を実施する。

- 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
- 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
- 地震、津波、落雷、火災等の災害によるサービス及び業務の停止等
- 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
- 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

4 適用範囲

(1) 関係職員の範囲

広域連合関係機関の職員及び介護認定審査会支援システム端末を設置している広域連合構成市町の担当課の職員（以下「関係職員」という。）とする。

(2) 情報資産の範囲

基本方針が対象とする情報資産は、次のとおりとし、広域連合のネットワークにより管理している情報資産以外は、基本方針の対象外とする。

ア　ネットワーク及び情報システム並びにこれらに関する設備及び電磁的記録媒体

イ　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。)

ウ　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

5 関係職員の遵守義務

関係職員は、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基本方針を遵守しなければならない。

6 情報セキュリティ対策

上記３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

広域連合関係機関の情報資産について、情報セキュリティ対策を推進する組織体制を確立する。

(2) 情報資産の分類と管理

広域連合関係機関の保有する情報資産を機密性、完全性及び可用性に応じて分類し、当該分類による重要度に応じた情報セキュリティ対策を実施する。

(3) 情報システム全体の強靭性の向上

情報セキュリティの強化を目的とし、業務の効率性・利便性の観点を踏まえ、情報システム全体に対し、次の二段階の対策を講じる。

ア　介護認定審査会支援システム接続系においては、インターネット接続系との通信経路を分割する。

イ　インターネット接続系においては、不正通信の監視機能の強化等の高度な情報セキュリティ対策を実施する。

(4) 物理的セキュリティ

情報システム及び情報機器を設置する施設への不正な立ち入り、情報資産の破損・破壊・窃用・盗難等から保護するために物理的な対策を講じる。

(5) 人的セキュリティ

情報セキュリティに関し、関係職員及び外部委託事業者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。

(6) 技術的セキュリティ

コンピュータ及びネットワークの管理・監視、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。

(7) 運用

情報システムの監視、基本方針の遵守状況の確認、外部委託を行う際のセキュリティ確保等、運用面の対策を講じるものとする。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。

(8) 外部委託とクラウドサービスの利用

外部委託を行う場合には、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、必要に応じて契約に基づき措置を講じる。

クラウドサービスを利用する場合には、利用に係る規程を整備し対策を講じる。

ソーシャルメディアサービスを利用する場合には、ソーシャルメディアサービスの運用手順を定め、ソーシャルメディアサービスで発信できる情報を規定する。

(9) 評価・見直し

基本方針の遵守状況を検証するため、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し、運用改善を行い、情報セキュリティの向上を図る。適宜基本方針の見直しが必要な場合は、その都度見直しを行う。

7　情報セキュリティ監査及び自己点検の実施

基本方針の遵守状況を検証するため、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。

8　基本方針の見直し

情報セキュリティ監査及び自己点検の結果、基本方針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、基本方針を見直す。

9　情報セキュリティ対策基準及び実施手順の策定

(1) 情報セキュリティ対策基準

上記６、７及び８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た情報セキュリティ対策基準を策定するものとする。

(2) 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事項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。