情報セキュリティポリシー

平成 31 年 4 月

広島県国民健康保険団体連合会

情報セキュリティ基本方針

はじめに

近年，我が国の保健医療分野における情報化の進展は著しく，その一方で，情報システムに対するリスク（情報漏えい，コンピュータ犯罪，プライバシー侵害等）が一層拡大している。

また，システムの分散化により，組織内で情報セキュリティの一貫性を保つことが困難になっているため，内部者による意図的な情報の持ち出し，誤操作等の過失による情報流出，外部者によるセキュリティホールを悪用した不正侵入及びウィルス汚染又はネットワークを盗聴することによる情報の漏えい等の危険性を絶えず有し，重要な経営課題となっている。

広島県国民健康保険団体連合会（以下「連合会」という。）は，国民健康保険法に基づき，保険者が共同してその目的を達成するために設立した法人であり，国民健康保険・後期高齢者医療診療（調剤）報酬及び介護給付費等の審査支払業務，保険者共同処理事業，保健事業等の各種事業を行っている。

これらの事業を行うに当たっては，国保総合システムを始めとする多くの情報システムを構築・運用するとともに，レセプト等の個人情報を含む機密性の高い情報を膨大に取り扱っており，連合会が取り扱う情報資産をあらゆる脅威から保護することは，極めて重要な社会的責務である。

このような観点から，連合会が取り扱う情報資産の安全な管理・運営の徹底を図るため，国際規格に準拠した情報セキュリティマネジメントシステム（以下「ＩＳＭＳ」という。）を構築し，情報利用者の情報セキュリティに対する意識の向上はもちろんのこと，組織として統一された情報セキュリティポリシーを策定する。

【広島県国民健康保険団体連合会情報セキュリティポリシー等の構成】（図１）

広島県国民健康保険団体連合会情報セキュリティポリシー（以下「セキュリティポリシー」という。）は，連合会の保有する情報資産等に関する情報セキュリティ対策について，基本方針を総合的にまとめたものである。

なお，情報セキュリティ実施手順（以下「実施手順」という。）は，ＩＳＭＳを有効に実施し，維持するためのＩＳＭＳ実施手順と，情報資産を適正に管理するための情報セキュリティ実施手順により構成する。

また，個々の情報システムについての実施マニュアルについては，必要に応じて各部門において策定することとする。

情報セキュリティポリシー（基本方針）		情報セキュリティ対策に関する統一的・基本的な方針
情報セキュリティ実施手順（対策基準）	ＩＳＭＳ実施手順	日本工業規格（JIS Q27001）に基づき，情報の機密性，完全性，可用性を維持し，かつ，リスクを適切に管理するための実施手順
	情報セキュリティ実施手順	情報資産の分類及び管理基準等を定めた情報セキュリティ対策の実施手順
各システム実施マニュアル		情報システムごとに定める，具体的なセキュリティ対策のための実施マニュアル

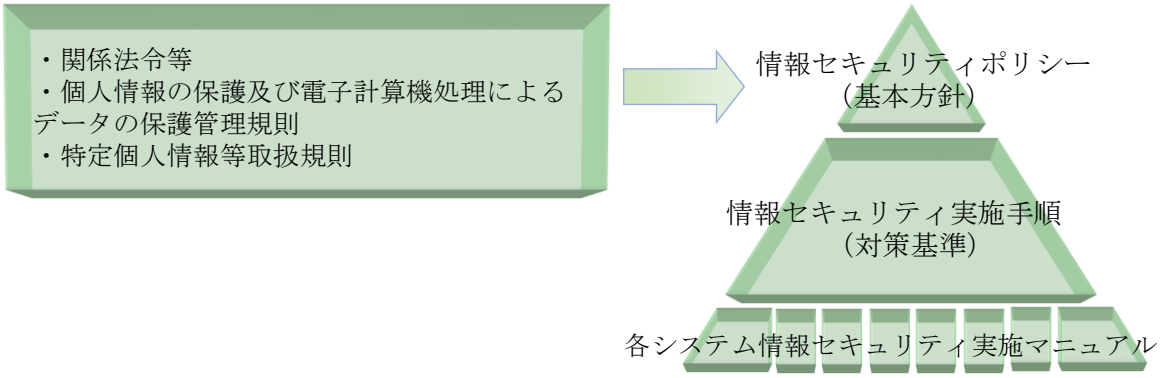


図１　セキュリティポリシー等の構成

情報セキュリティ基本方針

第１　目的

基本方針は，連合会が保有する情報資産の機密性（許可された者のみが情報にアクセスできることを確実にすることをいう。以下同じ。），完全性（情報及び処理方法の精度並びに完全さ（抜け，漏れのないこと）を確保することをいう。以下同じ。）及び可用性（許可された使用者が必要なときに情報及び関連する資産にアクセスできることを確実にすることをいう。以下同じ。）を確保するため，情報資産の取扱い及び情報セキュリティ対策の基本的な考え方及び方策を定め，連合会における情報資産の管理を徹底することを目的とする。

第２　用語の定義

１　情報

情報システムで取扱う電磁的データ及び紙に記載された情報をいう。

２　情報資産

情報及び情報を管理する仕組み（情報システム並びに情報システムの開発，運用及び保守のための資料等を含む。）をいう。

３　情報システム

コンピュータのハードウェア・ソフトウェア，ネットワーク及び記録媒体等で構成されるものであって，これら全体で業務処理を行うための情報処理の体系をいう。

４　ネットワーク

コンピュータ，関連機器等の多目的利用及び各種オンラインシステムのデータ伝送を目的として構築された情報通信基盤をいう。

５　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。

第３　職員等の義務

連合会の保有する情報資産に関する業務に携わるすべての職員及び外部受託者（以下「職員等」という。）は，情報セキュリティの重要性についての共通の認識を持つとともに，業務の遂行に当たってはセキュリティポリシーを遵守する義務を負う。

第４　情報セキュリティ管理体制

連合会の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・管理する体制を次のとおりとする。（図２）

１　最高情報セキュリティ責任者（以下「ＣＩＳＯ」という。）

⑴　事務局長をＣＩＳＯとする。

⑵　連合会における全てのネットワーク，情報システム等の情報資産の管理及び情報セキュリティ対策に関する最終決定権限及び責任を有する。

⑶　情報セキュリティの維持・管理状況や「情報セキュリティポリシー」の改訂状況，及び情報セキュリティに関する事故や問題の発生状況等を常務理事へ報告する。

2　総括情報セキュリティ責任者（以下「ＧＩＳＯ」という。）

⑴　各部長をＧＩＳＯとする。

⑵　ＣＩＳＯを補佐し，連合会の全てのネットワークにおける情報セキュリティ対策に関する権限及び責任を有する。

⑶　総括情報セキュリティ責任者は，ＣＩＳＯの指示を受けた場合，又はＣＩＳＯが不在の場合には自らの判断に基づき，必要かつ十分な措置を行う権限及び責任を有する。

3　総括情報セキュリティ責任者補佐（以下「ＧＩＳＯ補佐」という。）

総括情報セキュリティ責任者は，自らを補佐する総括情報セキュリティ責任者補佐を指名するものとする。

4　情報セキュリティ責任者

⑴　情報セキュリティ責任者は，所管する情報システムの情報セキュリティに関する権限及び責任並びに開発，設定の変更，運用，更新等を行う権限及び責任を有する者で，各情報システムの担当課・室長が当たる。

⑵　情報セキュリティ責任者は，所管する情報システムにおいて，セキュリティポリシーを運用する責任を有する。

5　情報セキュリティ委員会

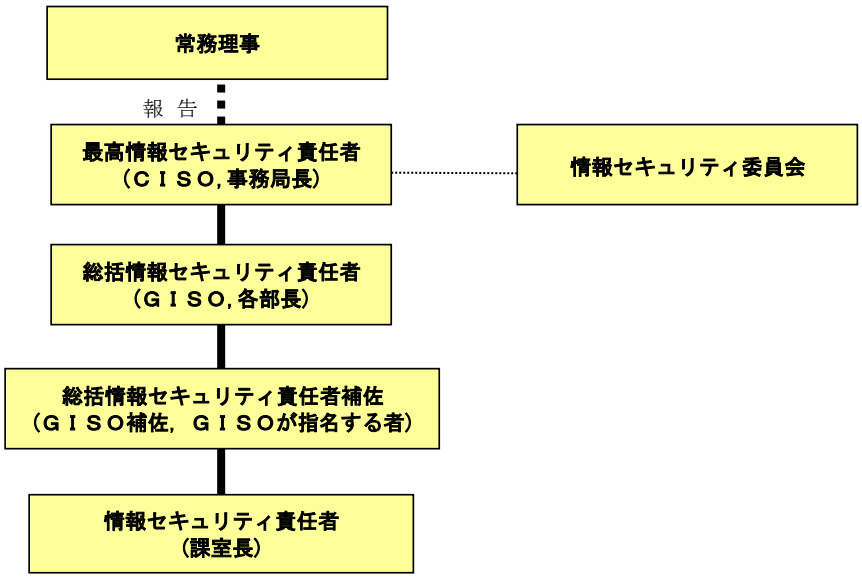
⑴　連合会の情報セキュリティを維持していくために，情報セキュリティ委員会を設け，マネジメント体制を整えるものとする。

⑵　情報セキュリティ委員会は，セキュリティポリシーの見直しについて協議する。

⑶　その他情報セキュリティに関する重要事項について審議する。

⑷　協議結果を基に，ＣＩＳＯは，所要の措置を講じる。

⑸　情報セキュリティ委員会は，委員長をＣＩＳＯとし，委員はＧＩＳＯ，ＧＩＳＯ補佐及びその他事務局長が指名する者をもって構成する。



第５　情報資産の分類

情報資産については，その重要度に応じて分類し，その重要度に応じた情報セキュリティ対策を行うものとする。

第６　情報資産への脅威

情報資産に対する脅威の発生度合いや脅威が発生した場合の影響を考慮し，特に認識すべき脅威は次のとおりである。

１　部外者による故意の不正アクセス又は職員等によるデータやプログラムの持ち出し・盗聴・改ざん・消去，機器及び媒体の盗取等

２　職員等による意図しない誤操作，故意の不正アクセス又は不正操作によるデータやプログラムの持ち出し・盗聴・改ざん・消去，機器及び媒体の盗取並びに規定外の端末接続によるデータ漏えい等

３　地震，落雷，火災等の災害並びに事故，故障等によるサービス及び業務の停止

第７　情報セキュリティ対策

第６で示した脅威から情報資産を保護するために，次のセキュリティ対策を講じるものとする。

１　物理的セキュリティ対策

情報システムを設置する施設への不正な立入りの防止や，情報資産を損傷・妨害等から保護するために物理的な対策を講じる。

２　人的セキュリティ対策

情報セキュリティに関する権限や責任を定め，職員等に基本方針及び情報セキュリティに関する法令等の内容を周知徹底するなど，十分な教育及び啓発が行われるよう必要な対策を講じる。

３　技術的セキュリティ対策

情報資産を外部からの不正なアクセス等から適切に保護するため，アクセス制御，ネットワーク監視等の技術面の対策を講じる。また，緊急事態が発生した場合に迅速な対応を可能とするための危機管理対策を講じる。

第８　実施手順の策定

第７の情報セキュリティ対策を講じるに当たって，遵守すべき行為，判断等の基準を統一的に定めるため，必要となる基本的な要件を明記した実施手順を策定するものとする。ＣＩＳＯ，ＧＩＳＯ，ＧＩＳＯ補佐及び情報セキュリティ責任者は，職員等が常にセキュリティポリシー及び実施手順を参照できるよう配慮するものとする。

なお，セキュリティポリシーを遵守して情報セキュリティ対策を実施するため，個々の情報システムについて具体的な手順を明記した実施マニュアルを必要に応じて策定するものとする。

第９　法令遵守

職員等は，職務の遂行において使用する情報資産について，次の法令等を遵守しなければならない。

１　不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）

２　著作権法（昭和 45 年法律第 48 号）

３　個人情報の保護に関する法律（平成 15 年法律第 57 号）

４　行政手続における特定の個人を識別するための番号の利用等に関する法律（平成 25 年法律第 27 号）
５　広島県国民健康保険団体連合会における個人情報の保護及び電子計算機処理によるデータの保護管理規則（昭和 58 年規則第 10 号）
６　広島県国民健康保険団体連合会国保データベースシステム運用管理業務規則（平成 25 年規則第 19 号）
７　広島県国民健康保険団体連合会特定個人情報等取扱規則（平成 29 年規則第１号）
８　その他全ての情報セキュリティに関連する法令，契約及び規定等

第 10　情報セキュリティに関する違反への対応

情報セキュリティの保持に関して，広島県国民健康保険団体連合会服務規則（昭和 34 年規則第８号）第 59 条に規定する懲戒事由に該当すると認められる行為を行った職員については，その内容，程度に応じて，懲戒処分等の人事管理上必要な措置を講じる。

第 11　情報セキュリティに関する監査の実施

セキュリティポリシーが遵守されるとともに，ＩＳＭＳが有効に実施され，維持されていることを検証するため，監査責任者を設け，これに常任参事を充てることとし，定期的に情報セキュリティに関する内部監査を実施するものとする。

情報セキュリティに関する内部監査の実施に当たっては，監査責任者が各部署から内部監査員を選定し，内部監査員を統括する。

第 12　情報セキュリティ対策の継続的な改善

ＣＩＳＯは，内部監査の結果を踏まえるとともに，情報セキュリティを取り巻く状況の変化に対応するため，定期的に情報セキュリティ対策を見直すなど，継続的に改善を行う。

（平成 19 年 3 月 1 日施行）
平成 20 年 10 月 1 日一部改正
平成 24 年 4 月 1 日一部改正
平成 29 年 10 月 25 日一部改正
平成 30 年 9 月 25 日一部改正
平成 31 年 4 月 1 日一部改正

広島県国民健康保険団体連合会
常務理事　　佐々木　浩　二