セキュリティ規定（素案）

接続機関用

相互接続基盤の事業主体　→　接続機関

平成 30 年 3 月 30 日

目次

第1章　総則

第1条 目的

セキュリティ規定（以下、本規定）は、接続機関が全国保健医療情報ネットワーク（以下、本ネットワーク）を利用する場合に遵守すべきセキュリティ基準と、機関認証主体によるセキュリティ基準の審査方法を定めるものである。本ネットワークを介して交換される情報資産を様々な脅威から防御することは、接続機関自身の権利や利益を守るためだけでなく、他の接続機関の権利や利益を守るためにも、また、業務の安定的、継続的な運営のためにも必要不可欠である。本ネットワークを利用するすべての接続機関は、本規定を十分に理解するとともに、これを誠実に遵守するものとする。

第2条 用語の定義

本規定において、次の用語はそれぞれ次の意味で使用するものとする。

（1） 本ネットワーク

医療等分野の様々なサービスを相互接続して安全かつ効率的に利用でき、個人、患者本位で最適な健康管理、診察、ケアを提供するためのネットワーク。

（2） 相互接続基盤

本ネットワークに接続するネットワークを相互接続するネットワーク基盤。

（3） 相互接続基盤の事業主体

相互接続基盤を運営する主体。

（4） 機関認証主体

本ネットワークに接続する機関について認定を行う認証の主体。

（5） 接続機関

機関認証主体の認定を受けた機関であり、本ネットワークに接続する機関。保険医療機関、保険薬局、介護事業者、地連事業主体、サービス事業者がある。

（6） 保険医療機関

保険指定を受けた病院、診療所であり、健康保険を使った診察、処置を行う。

（7） 保険薬局

保険指定を受けた薬局であり、健康保険を使った処方箋の受付、調剤を行う。

（8） 介護事業者

介護保険法における居宅サービス、地域密着型サービス、居宅介護支援、介護予防サービス等のサービスを提供する事業者。

（9） 地連事業主体

地域医療情報連携ネットワークの事業の主体。

（10）　地域医療情報連携ネットワーク

情報通信技術を活用し、複数の医療機関等で患者の情報共有を行うために構築されたネットワーク。

（11）　サービス事業者

医療情報共有サービスを提供する民間事業者。

（12）　ネットワーク事業者

運営主体の認定を受けた事業者であり、接続機関に本ネットワークへのネットワーク接続サービスを提供

する事業者。

（13） リクエスタ

接続機関の役割のひとつであり、本ネットワークを介して医療等分野の様々な情報を参照する接続機関。主には保険医療機関、保険薬局、介護事業者が対象である。地連事業主体、サービス事業者であっても情報参照のみを行う場合は対象となる。

（14） レスポンダ

接続機関の役割のひとつであり、本ネットワークを介して医療等分野の様々な情報を提供及び参照する接続機関。主には地連事業主体、サービス事業者が対象である。保険医療機関、保険薬局、介護事業者であっても情報提供を行う場合は対象となる。

第3条 適用

本規定の適用対象は接続機関とする。

第2章 セキュリティ基準

第1条 要件

接続機関は、接続機関の役割に応じて、下記の最新のガイドラインに準拠しなければならない。

（1） 医療情報システムの安全管理に関するガイドライン（厚生労働省）

（2） ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン（総務省）

（3） ASP・SaaS における情報セキュリティ対策ガイドライン（総務省）

（4） 医療情報を受託管理する情報処理事業者向けガイドライン（経済産業省）

第2条 リクエスタが準拠すべきガイドライン

リクエスタである接続機関は、下記の最新のガイドラインに準拠しなければならない。

（1） 医療情報システムの安全管理に関するガイドライン（厚生労働省）

第3条 レスポンダが準拠すべきガイドライン

レスポンダである接続機関は、下記の最新のガイドラインに準拠しなければならない。

（1） 医療情報システムの安全管理に関するガイドライン（厚生労働省）

（2） ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン（総務省）

（3） ASP・SaaS における情報セキュリティ対策ガイドライン（総務省）

また、レスポンダである接続機関が、他の接続機関の医療情報を受託管理する場合には、更に下記の最新のガイドラインに準拠しなければならない。

（4） 医療情報を受託管理する情報処理事業者向けガイドライン（経済産業省）

第3章 セキュリティ基準の審査

第1条 準拠性の審査

接続機関は、接続機関の役割に応じて、セキュリティ基準の準拠性を機関認証主体に立証し、機関認証主体の認定を受けなければならない。

第2条 リクエスタの審査

リクエスタである接続機関は、相互接続基盤の事業主体が策定した準拠性チェックシートに準拠性の確認結果を記入し、機関認証主体に提出することで、準拠性を立証するものとする。

第3条 レスポンダの審査

レスポンダである接続機関は、相互接続基盤の事業主体が認める第三者評価機関による適合性評価を受け、適合性評価結果を機関認証主体に提出することで、準拠性を立証するものとする。

第4章　運用

第1条 有効期間

準拠性の認定の有効期間は、相互接続基盤の事業主体が定めるものとする。

第2条 再審査

接続機関は、接続機関の情報システムの構成を大幅に変更した場合や、準拠性の認定の有効期間を超過する前に、再度機関認証主体による準拠性の審査を受けなければならない。

第3条 内部審査

接続機関は、日常業務においてセキュリティ基準の準拠に努めるとともに、接続機関の責任において準拠性の内部審査を定期的に実施しなければならない。

第4条 違反行為に対する措置

接続機関がセキュリティ基準を遵守していないことが判明した場合、機関認証主体は当該接続機関の認定を取り消す等の措置を講じることができるものとする。

第5章　その他

第1条 関係者への通知

本規定は、相互接続基盤の事業主体が、接続機関、ネットワーク事業者及び本ネットワークの運営と構築等に係わる団体、企業、法人等とその関係者に公開するものとする。また、相互接続基盤の事業主体は、ホームページへの掲載その他メーリングリスト等の相互接続基盤の事業主体が適切と判断する方法及び範囲で、必要となる事項を通知するものとする。

第2条 本規定の変更

相互接続基盤の事業主体は、接続機関及びネットワーク事業者の承諾を得ることなく本規定を必要時に変更できるものとする。また、変更等の際は、その変更内容をホームページ上に掲載又は相互接続基盤

の事業主体が適切と判断する方法によって接続機関等の関係者に通知する。その効力は通知された所定の期日から発効するものとする。