

オンライン資格確認等、  
レセプトのオンライン請求及び  
健康保険組合に対する社会保険手続きに  
係る電子申請システムに係る  
セキュリティに関するガイドライン

令和 2 年 1 0 月  
(令和 6 年 1 月一部改正)

厚生労働省

# 目 次

I 総則	1
1 目的	1
2 適用範囲	3
3 位置付け	4
4 構成	5
5 見直し	5
II セキュリティに関するガイドライン	6
1 組織・体制	6
(1) 責任者の任命	6
(2) 責任の所在	6
(3) 連絡体制	6
2 情報の分類と管理	7
(1) 情報の管理責任	7
(2) 情報の分類	7
(3) 情報の分類に応じた管理方法	7
3 物理的セキュリティ	8
(1) 医療機関等の機器の設置等	8
(2) 審査支払機関の機器の設置等	8
(3) 医療保険者等の機器の設置等	8
(4) 実施機関の機器の設置等	8
4 人的セキュリティ	9
(1) すべての人員の基本的な責務	9
(2) 機関の長の責務	9
5 技術的セキュリティ	10
(1) 資格情報等の機密性の確保	10
(2) レセプトデータの機密性の確保	10
(3) 社会保険適用情報の機密性の確保	10
(4) 伝送相手の正当性の確保	10
(5) 伝送事実の正当性の確保	10
(6) システムの機密性の確保	11
(7) 伝送経路の機密性の確保	11
(8) 伝送の完全性等の確保	11
(9) 他システムと接続する場合の要求事項	11
6 オンライン資格確認等システム／オンライン請求システム／健保組合電子申請システムの開発及び管理	12
(1) 開発規程	12
(2) 管理規程	12
(3) 開発及び試験環境と運用環境の分離	12
7 規程遵守	13
(1) セキュリティポリシー	13
(2) オンライン資格確認等業務に係る利用規約等	13
(3) オンライン請求業務に係る利用規約等	13
8 規程に対する違反への対応	14
9 評価・見直し	15
(1) 監査証跡の保管	15
(2) 監査の実施	15
(3) 監査結果に基づく措置	15

# I 総則

## 1 目的

一般に、情報システムを導入することで、事務処理の効率化や利便性の向上等を実現できる。しかしながら、十分なセキュリティ対策を講じないままに情報システムを導入すると、関連データの漏えい、消失及び破壊を招くほか、導入した情報システムが機能停止に陥る等、対象とする事務処理にかえって悪影響を及ぼすことになりかねない。オンライン資格確認システム、診療情報閲覧機能、薬剤情報閲覧機能、特定健診情報閲覧機能、医療費通知情報閲覧機能及びレセプト振替機能に関わるシステム（以下「オンライン資格確認等システム」という。）、診療報酬明細書・調剤報酬明細書・訪問看護療養費明細書（以下「レセプト」という。）等の請求データをオンラインで受け渡す仕組みを整備したシステム（以下「オンライン請求システム」という。）及び健康保険組合に対する社会保険手続に係る電子申請システム（以下「健保組合電子申請システム」という。）についても、決して例外ではない。特に、オンライン資格確認等システム及びオンライン請求システムは、患者の資格情報等及びレセプトを、健保組合電子申請システムでは、加入者の資格情報といった慎重な取扱いを要する個人情報<sup>1</sup>を伝送するシステムであるため、安全性の高いセキュリティ対策を講じる必要がある。

このような観点から、本ガイドラインは、オンライン資格確認等、診療情報閲覧、薬剤情報閲覧、特定健診情報閲覧、医療費通知情報閲覧及びレセプト振替に係る各業務（以下、「オンライン資格確認等業務」と総称する。）、レセプトのオンラインによる提出及び受取（以下「オンライン請求業務」という。）及び健康保険適用処理業務の実施に際し、個人情報等を適切に保護するとともに、円滑な業務遂行に資することを目的として、これらの業務及びこれらのシステムを利用する機関が遵守すべき事項を示すものである。

### ※留意事項

病院、診療所、薬局及び指定訪問看護事業者（以下「医療機関等」という。）は、情報システムの導入に当たっては、「診療録等の保存を行う場所について」（平成14年3月29日付け医政発0329003号・保発第0329001号厚生労働省医政局長・保険局長通知）、「民間事業者等が行う書面の保存等における情報通信の技術の利用に関する法律」（平成16年法律第149号）、「医療・介護関係事業者における個人情報の適切な取扱いのためのガイダンス」（平成29年4月14日付け個情第534号、医政発0414第6号、薬生発0414第1号、老発0414第1号個人情報保護委員会事務局長・厚生労働省医政局長・厚生労働省医薬・生活衛生局長・厚生労働省老健局長通知）、個人情報の保護に関する法律（平成15年法律第57号）、「医療情報システムの安全管理に関するガイドライン」（第6.0版）（厚生労働省大臣官房医薬産業振興・医療情報審議官通知）等の関連法令及び通知を参照して適切に導入する必要がある。「医療情報システムの安全管理に関するガイドライン」は、医療機関等において医療情報を扱う情報システム全般と、それらのシステムの導入、運用、利用、保守及び廃棄に関わる者を対象としている。

オンライン資格確認等システム及びオンライン請求システムは、いずれも医療情報を扱う情

---

<sup>1</sup> **個人情報**：個人に関する情報であつて、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

報システムである。したがって、両システムの導入に際しても、「医療情報システムの安全管理に関するガイドライン」に沿って導入、運用、利用、保守及び廃棄が行われるべきものと考えられる。なお、「医療情報システムの安全管理に関するガイドライン」は、以下の厚生労働省のホームページにおいて掲載しているが、情勢に応じた改定を随時行っており、適宜最新版を参照されたい。

健康保険組合（健保組合電子申請システムにおいて、直接API連携するクラウドサービスを提供する事業者を含む。以下同じ。）は、健保組合電子申請システムの導入に当たり、個人情報の保護に関する法律、「健康保険組合等における個人情報の適切な取扱いのためのガイダンスの一部改正について（通知）」（令和5年3月31日付け個情第633号・保発0331第30号健康保険組合理事長あて個人情報保護委員会事務局長・厚生労働省保険局長通知）、「医療情報システムの安全管理に関するガイドライン」、「行政手続におけるオンラインによる本人確認の手法に関するガイドライン」（平成31年2月25日付け各府省情報化統括責任者（CIO連絡会議決定））等の関連法令及びガイドラインを参照して適切に導入する必要がある。

国民健康保険組合は、情報システムの導入に当たっては、「国民健康保険組合における個人情報の適切な取扱いのためのガイダンスの一部改正について（通知）」（令和5年3月31日付け個情第635号・保発0331第27号個人情報保護委員会事務局長・厚生労働省保険局長通知）、「医療情報システムの安全管理に関するガイドライン」等のシステム関連法令及びガイドラインを参照して適切に導入する必要がある。

国民健康保険団体連合会（以下「国保連合会」という。）及び国民健康保険中央会（以下「国保中央会」という。）は情報システムの導入に当たっては、「国民健康保険団体連合会等における個人情報の適切な取扱いのためのガイダンスの一部改正について（通知）」（令和5年3月31日付け個情第636号・保発0331第24号個人情報保護委員会事務局長・厚生労働省保険局長通知）、「医療情報システムの安全管理に関するガイドライン」等のシステム関連法令及びガイドラインを参照して適切に導入する必要がある。

（参考）厚生労働省のホームページ

「医療情報システムの安全管理に関するガイドライン」（第6.0版）

[https://www.mhlw.go.jp/stf/shingi/0000516275\\_00006.html](https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html)

## 2 適用範囲

本ガイドラインは、オンライン資格確認等システム／オンライン請求システム／健保組合電子申請システムを利用する全ての機関を対象とする。したがって、対象機関には、医療機関等だけでなく、医療保険者等、社会保険診療報酬支払基金（以下「支払基金」という。）・国保連合会により組織される審査支払機関及び本システムを維持・運営する実施機関（以下「実施機関」という。）をも含む。

また、本ガイドラインは、オンライン資格確認等システムにおいて伝送される資格情報等、オンライン請求システムにおいて伝送されるレセプト及び健保組合電子申請システムにおいて伝送される社会保険適用情報をその対象とする。一方で、物理的手法による搬送等の従来からのレセプト請求及びこれらレセプト請求に付随する業務や、健康保険の適用に関する届出及びこれに付随する業務は、対象には含まない。

本ガイドラインの対象範囲を、図1に示す。

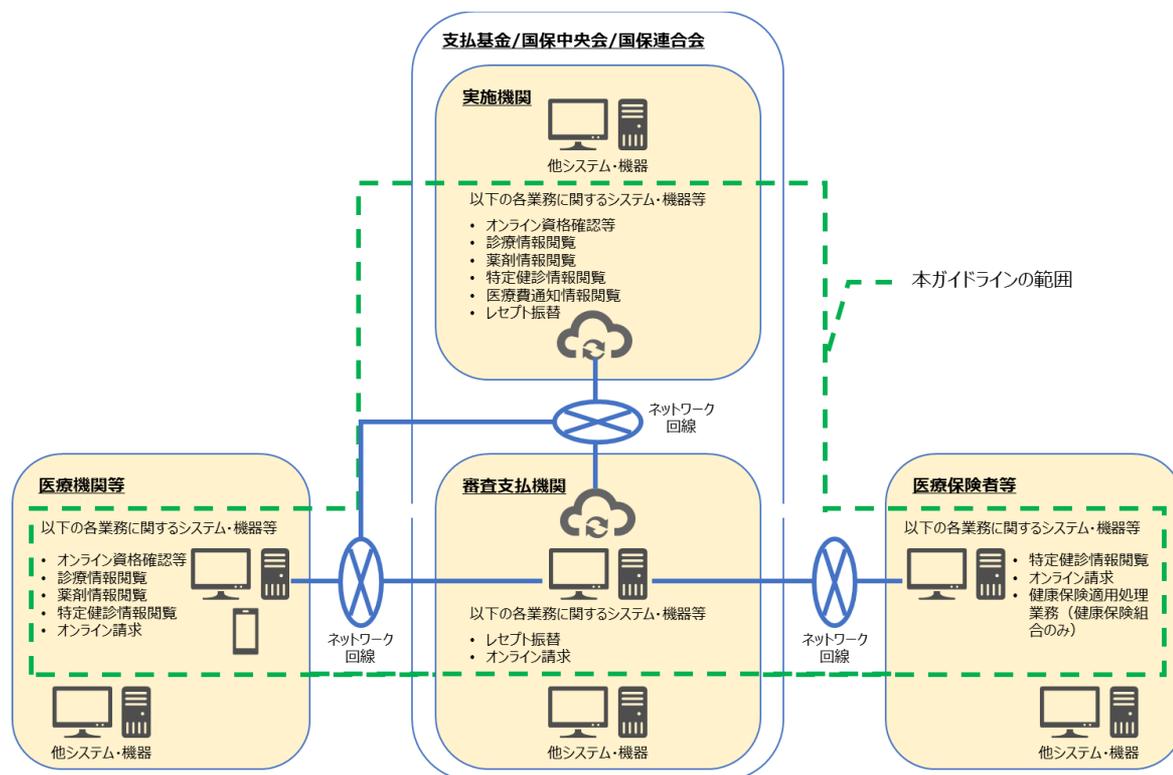


図1：本ガイドラインの対象範囲

### 3 位置付け

本ガイドラインは、前項の適用範囲に基づき、オンライン資格確認等システム、健保組合電子申請システムの利用開始及びレセプトのオンライン化に伴って必要となるセキュリティ対策について、基本的な考え方を示すものであり、オンライン資格確認等業務／オンライン請求業務／健康保険適用処理業務に携わる人、組織及びシステムが最低限満たす必要があると考えられる項目を示している。

したがって、オンライン資格確認等業務／オンライン請求業務／健康保険適用処理業務を実施しようとする機関は、本ガイドラインの内容に基づき、その機関においてどのように目的を達成していくかを示した基本方針等を作成することが求められる。

本ガイドラインの位置付けを、図2に示す。

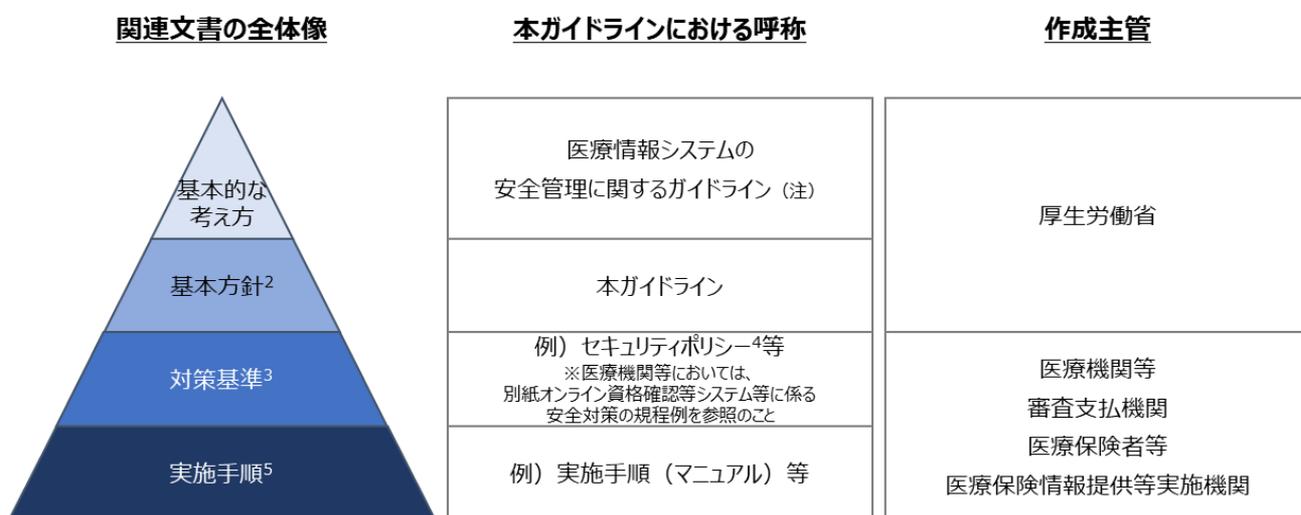


図2：ガイドラインの位置付け

（注）「医療情報システムの安全管理に関するガイドライン」は、主に医療機関等を対象としているが、本ガイドラインでは、支払基金・国保連合会により組織される審査支払機関及び実施機関においてもその考え方を参照する。

- <sup>2</sup> **基本方針**：組織におけるセキュリティ対策に対する根本的な考え方を表わすもので、組織がどのような情報資産をどのような脅威からなぜ保護しなければならないのかを明らかにし、組織の情報セキュリティに対する取組姿勢を示すものをいう。
- <sup>3</sup> **対策基準**：基本方針に定められた情報セキュリティを確保するために遵守すべき行為及び判断等の基準、即ち、基本方針を実現するために何を行なわなければいけないかを示すものをいう。
- <sup>4</sup> **セキュリティポリシー**：組織が所有する情報及び情報システム等の情報資産のセキュリティ対策について、総合的・体系的かつ具体的に取りまとめたものをいう。情報資産への脅威に対する対策について、基本的な考え方及び情報セキュリティを確保するための体制、組織及び運用を含めた規程をいう。基本方針及び対策基準からなる。
- <sup>5</sup> **実施手順**：セキュリティポリシーには含まれないものの、対策基準に定められた内容を具体的な情報システム又は業務において、どのような手順に従って実行していくのかを示すものをいう。

## 4 構成

本ガイドラインの構成を、表 1 に示す。

表 1：ガイドラインの構成

構 成	概 要
組織・体制	オンライン資格確認等業務／オンライン請求業務／健康保険適用処理業務に関わる組織の責任と役割について記述する。
情報の分類 <sup>6</sup> と管理	オンライン資格確認等業務／オンライン請求業務／健康保険適用処理業務に関わる情報等の分類と分類に応じた管理方法について記述する。
物理的セキュリティ	オンライン資格確認等システム／オンライン請求システム／健保組合電子申請システムで使用される機器の設置される環境が備える設備要件について記述する。
人的セキュリティ	オンライン資格確認等業務／オンライン請求業務／健康保険適用処理業務に関わる人員の役割と責任、人員に対する教育について記述する。
技術的セキュリティ	オンライン資格確認等システム／オンライン請求システム／健保組合電子申請システムが備えるセキュリティ機能要件について、ハードウェア、ソフトウェア及びネットワークの観点で記述する。
オンライン資格確認等システム／オンライン請求システム／健保組合電子申請システムの開発及び管理	オンライン資格確認等システム／オンライン請求システム／健保組合電子申請システムの管理運用に関する整備すべき文書及び遵守事項について記述する。
規程遵守	オンライン資格確認等システム／オンライン請求システム／健保組合電子申請システムを導入するに当たり整備すべき文書について記述する。
規程に対する違反への対応	オンライン資格確認等システム／オンライン請求システム／健保組合電子申請システムの運用時における規程違反に対する対応について記述する。
評価見直し	オンライン資格確認等業務／オンライン請求に関わる業務／健保組合電子申請システム、システム及び文書の運用に対する監査について記述する。

## 5 見直し

本ガイドラインは、情報通信に関する環境の変化、オンライン資格確認等業務、オンライン請求及び健康保険の適用に関する届出の状況その他の事情を総合的に勘案し、必要に応じた見直しを行うものとする。

<sup>6</sup> 情報の分類：情報資産に対し、機密性、完全性、可用性の3つの側面から重要性及び開示範囲の分類を行ったものをいう。この分類は、情報資産をどのように扱い、保護するかを決めるための判断基準となり、これに基づき要求されるセキュリティ水準が定められる。

## II セキュリティに関するガイドライン

以下、各規程の冒頭に、当該規程の遵守が求められる対象機関を示している。規程対象の各機関は、図1に示す業務に関して遵守すべきと定められる事項について参照されたい。

### 1 組織・体制

#### (1) 責任者の任命

##### 対象：医療機関等／審査支払機関／医療保険者等／実施機関

機関の長<sup>7</sup>は、必要な情報セキュリティを確保できる体制を確立するため、「医療情報システムの安全管理に関するガイドライン」の責任者の任命に関する規定に準じて、オンライン資格確認等業務／オンライン請求業務／健康保険適用処理業務に携わる人員の情報セキュリティに関する役割と責任を定義するとともに、これについての責任者を任命すること。

#### (2) 責任の所在

##### 対象：医療機関等／審査支払機関／医療保険者等／実施機関

機関の長は、オンライン資格確認等システム／オンライン請求システム／健保組合電子申請システムを適切に運用するため、「医療情報システムの安全管理に関するガイドライン」の責任の所在に関する規定に準じて、責任の所在を明確にしておくこと。

#### (3) 連絡体制

##### 対象：医療機関等／審査支払機関／医療保険者等／実施機関

機関の長は、システム障害等発生時における関係各所（システムを運営する実施機関等）との連絡を円滑に行うため、「医療情報システムの安全管理に関するガイドライン」の連絡体制に関する規定に準じて、連絡体制及び連絡方法を明文化し、これを遵守すること。

---

<sup>7</sup> 機関の長：医療機関等、審査支払機関、医療保険者等及び実施機関において、オンライン資格確認等業務／オンライン請求業務／健康保険適用処理業務に関する全ての責任を有する最高意思決定者をいう。

## 2 情報の分類と管理

### (1) 情報の管理責任

#### **対象：医療機関等／審査支払機関／医療保険者等／実施機関**

機関の長は、オンライン資格確認等システム／オンライン請求システム／健保組合電子申請システムで取り扱う情報について、その管理責任を明確化するため、「医療情報システムの安全管理に関するガイドライン」の情報の管理責任に関する規定に準じて、管理責任者を任命すること。

### (2) 情報の分類

#### **対象：医療機関等／審査支払機関／医療保険者等／実施機関**

機関の長は、オンライン資格確認等システム／オンライン請求システム／健保組合電子申請システムで取り扱う情報について、組織内で重要度の程度を共有するため、「医療情報システムの安全管理に関するガイドライン」の情報の分類に関する規定に準じて、情報の分類を定めること。

### (3) 情報の分類に応じた管理方法

#### **対象：医療機関等／審査支払機関／医療保険者等／実施機関**

機関の長は、オンライン資格確認等システム／オンライン請求システム／健保組合電子申請システムで取り扱う情報について、重要度の程度に応じた適切な取扱いを行うため、「医療情報システムの安全管理に関するガイドライン」の情報の分類に応じた管理方法に関する規定に準じて、2(2)で行った情報の分類に応じた管理方法について定めること。

### 3 物理的セキュリティ

#### (1) 医療機関等の機器の設置等

##### 対象：医療機関等

医療機関等は、その責任において「医療情報システムの安全管理に関するガイドライン」の機器の設置等に関する規定に準じて、機器を設置し、運用すること。

#### (2) 審査支払機関の機器の設置等

##### 対象：審査支払機関

審査支払機関は、その責任において「医療情報システムの安全管理に関するガイドライン」の機器の設置等に関する規定に準じて、機器を設置し、運用すること。

#### (3) 医療保険者等の機器の設置等

##### 対象：医療保険者等

医療保険者等は、その責任において「医療情報システムの安全管理に関するガイドライン」の機器の設置等に関する規定に準じて、機器を設置し、運用すること。

#### (4) 実施機関の機器の設置等

##### 対象：実施機関

実施機関は、その責任において「医療情報システムの安全管理に関するガイドライン」の機器の設置等に関する規定に準じて、機器を設置し、運用すること。

## 4 人的セキュリティ

### (1) すべての人員の基本的な責務

#### **対象：医療機関等／審査支払機関／医療保険者等／実施機関**

オンライン資格確認等業務／オンライン請求業務／健康保険適用処理業務に携わる全ての者は、「医療情報システムの安全管理に関するガイドライン」の人員の基本的な責務に関する規定に準じて、業務における人的セキュリティを確保するように努めること。

### (2) 機関の長の責務

#### **対象：医療機関等／審査支払機関／医療保険者等／実施機関**

機関の長は、「医療情報システムの安全管理に関するガイドライン」の機関の長の責務に関する規定に準じて、その機関におけるオンライン資格確認等業務／オンライン請求業務／健康保険適用処理業務に関する最高責任者として、業務における人的セキュリティを確保するように努めること。

## 5 技術的セキュリティ

### (1) 資格情報等の機密性の確保

**対象：オンライン資格確認等業務を行う医療機関等／審査支払機関／医療保険者等／実施機関**

オンライン資格確認等業務に携わる全ての者は、「医療情報システムの安全管理に関するガイドライン」の機密性の確保に関する規定に準じて、オンライン資格確認等システムで取り扱う資格情報等を、これについて正当な権限を有しない者から適切に保護すること。

### (2) レセプトデータの機密性の確保

**対象：オンライン請求業務を行う医療機関等／審査支払機関／医療保険者等**

オンライン請求業務に携わる全ての者は、「医療情報システムの安全管理に関するガイドライン」の機密性の確保に関する規定に準じて、レセプトデータを、これについて正当な権限を有しない者から適切に保護すること。

### (3) 社会保険適用情報の機密性の確保

**対象：健康保険適用処理業務を行う健康保険組合**

健康保険組合は、「医療情報システムの安全管理に関するガイドライン」の機密性の確保に関する規定に準じて、社会保険適用情報を、これについて正当な権限を有しない者から適切に保護すること。

### (4) 伝送相手の正当性の確保

**対象：医療機関等／審査支払機関／医療保険者等／実施機関**

オンライン資格確認等業務／オンライン請求業務に携わる全ての者は、「医療情報システムの安全管理に関するガイドライン」の機密性の確保に関する規定に準じて、伝送相手が正当な相手であることを相互に認証する機能を有すること。

### (5) 伝送事実の正当性の確保

**対象：医療機関等／審査支払機関／医療保険者等／実施機関**

オンライン資格確認等業務／オンライン請求業務に携わる全ての者は、伝送相手が、資格情報等やレセプトデータの送受信に関する事実を確認できるようにすること。具体的には、デジタル署名付きデータの送付と受領確認データの返送、データの送付に関する受領確認データの相互送信、送信ログ及び受信ログの保管等が挙げられる。

(6) システムの機密性の確保

**対象：医療機関等／審査支払機関／医療保険者等／実施機関**

オンライン資格確認等業務／オンライン請求業務／健康保険適用処理業務に携わる全ての者は、「医療情報システムの安全管理に関するガイドライン」のシステムの機密性の確保に関する規定に準じて、システムの機密性を確保すること。

(7) 伝送経路の機密性の確保

**対象：医療機関等／審査支払機関／医療保険者等／実施機関**

オンライン資格確認等業務／オンライン請求業務／健康保険適用処理業務に携わる全ての者は、ネットワークの接続方式については、実施機関が別途認められたサービス事業者による安全管理がなされた接続方式とするとともに、「医療情報システムの安全管理に関するガイドライン」の伝送経路の機密性の確保に関する規定に準じて、医療機関等、審査支払機関、医療保険者等及び実施機関間を相互に接続するネットワーク回線において、許可されていない者による盗聴及び漏えいに対する機密性を確保する機能を有すること。

(8) 伝送の完全性等の確保

**対象：医療機関等／審査支払機関／医療保険者等／実施機関**

オンライン資格確認等業務／オンライン請求業務／健康保険適用処理業務に携わる全ての者は、「医療情報システムの安全管理に関するガイドライン」の伝送の完全性等の確保に関する規定に準じて、ネットワーク回線の切断、ネットワーク機器の故障等の不測の事態にも対処できる機能を有すること。具体的には、レセプトデータ、資格情報等及び社会保険適用情報の伝送中にネットワーク障害等が起きた場合、送信機器においてネットワークの切断を検知し、伝送を中止するような機器である。

(9) 他システムと接続する場合の要求事項

**対象：医療機関等／審査支払機関／医療保険者等／実施機関**

オンライン資格確認等業務／オンライン請求業務／健康保険適用処理業務に携わる全ての者は、「医療情報システムの安全管理に関するガイドライン」の他システムと接続する場合の要求事項に関する規定に準じて、オンライン資格確認等システム／オンライン請求システム／健保組合電子申請システムと他システムとをネットワーク接続する場合は、他システムからの悪影響を遮断すること。

## 6 オンライン資格確認等システム／オンライン請求システム／健保組合電子申請システムの開発及び管理

### (1) 開発規程

#### 対象：審査支払機関

審査支払機関は、「医療情報システムの安全管理に関するガイドライン」の開発規程に関する規定に準じて、オンライン請求システムの開発におけるセキュリティの方針や対策等について明文化し、これを遵守すること。

#### 対象：実施機関

実施機関は、「医療情報システムの安全管理に関するガイドライン」の開発規程に関する規定に準じて、オンライン資格確認等システムの開発におけるセキュリティの方針や対策等について明文化し、これを遵守すること。

#### 対象：健康保険組合

健康保険組合は、「医療情報システムの安全管理に関するガイドライン」の開発規程に関する規定に準じて、健保組合電子申請システムの開発におけるセキュリティの方針や対策等について明文化し、これを遵守すること。

### (2) 管理規程

#### 対象：審査支払機関

審査支払機関は、「医療情報システムの安全管理に関するガイドライン」の管理規程に関する規定に準じて、オンライン請求システムの管理におけるセキュリティの方針や対策等について明文化し、これを遵守すること。

#### 対象：実施機関

実施機関は、「医療情報システムの安全管理に関するガイドライン」の管理規程に関する規定に準じて、オンライン資格確認等システムの管理におけるセキュリティ対策について明文化し、これを遵守すること。

#### 対象：健康保険組合

健康保険組合は、「医療情報システムの安全管理に関するガイドライン」の管理規程に関する規定に準じて、健保組合電子申請システムの開発におけるセキュリティ対策について明文化し、これを遵守すること。

### (3) 開発及び試験環境と運用環境の分離

#### 対象：審査支払機関／実施機関

オンライン資格確認等システム／オンライン請求システムの開発及び試験環境は、「医療情報システムの安全管理に関するガイドライン」の開発及び試験環境と運用環境の分離に関する規定に準じて、運用環境から分離すること。

## 7 規程遵守

### (1) セキュリティポリシー

#### **対象：医療機関等／審査支払機関／医療保険者等／実施機関**

医療機関等、審査支払機関、医療保険者等及び実施機関は、「医療情報システムの安全管理に関するガイドライン」のセキュリティポリシーに関する規定に準じて、前記1～6において定めた事項を実行するためのオンライン資格確認等システム／オンライン請求システム／健康保険適用処理業務に関わるセキュリティポリシーを策定し、これに基づいて適切にシステムの運用を行うこと。

### (2) オンライン資格確認等業務に係る利用規約等

#### **対象：オンライン資格確認等業務を行う医療機関等／医療保険者等／実施機関**

実施機関は、オンライン資格確認等システムの安全な運用を図るため、医療機関等を相手として一定の契約を締結する目的で、利用規約等を定めることができることとし、医療機関等は、これを遵守すること。同様に、実施機関は、医療保険者等を相手として一定の契約を締結する目的で、利用規約等を定めることができることとし、医療保険者等は、これを遵守すること。

### (3) オンライン請求業務に係る利用規約等

#### **対象：オンライン請求業務を行う医療機関等／医療保険者等／審査支払機関**

審査支払機関は、オンライン請求システムの安全な運用を図るため、医療機関等及び医療保険者等を相手として一定の契約を締結する目的で、利用規約等を定めることができることとし、医療機関等及び医療保険者等は、これを遵守すること。

## 8 規程に対する違反への対応

対象：医療機関等／審査支払機関／医療保険者等／実施機関

機関の長は、自らの機関で定めた内容に対する違反があった場合の対応について、その対応方法及び内容等を明文化するとともに、これに基づき厳正に対応すること。

## 9 評価・見直し

### (1) 監査証跡の保管

#### **対象：審査支払機関**

審査支払機関は、「医療情報システムの安全管理に関するガイドライン」の監査証跡の保管に関する規定に準じて、オンライン請求システムの監査に必要な情報や記録を保管すること。

#### **対象：実施機関**

実施機関は、「医療情報システムの安全管理に関するガイドライン」の監査証跡の保管に関する規定に準じて、オンライン資格確認等システムの監査に必要な情報や記録を保管すること。

### (2) 監査の実施

#### **対象：審査支払機関**

審査支払機関は、「医療情報システムの安全管理に関するガイドライン」の監査の実施に関する規定に準じて、システム及び業務に従事する人員とは独立した監査人を任命して監査に関する規程を策定させ、当該監査人に、オンライン請求に関係するシステム・機器等の運用・保守、関連業務の運用状況及び関連文書の管理が適切に行われているか、定期的に監査を行わせること。

#### **対象：実施機関**

実施機関は、「医療情報システムの安全管理に関するガイドライン」の監査の実施に関する規定に準じて、システム及び業務に従事する人員とは独立した監査人を任命して監査に関する規程を策定させ、当該監査人に、オンライン資格確認等に関係するシステム・機器等の運用・保守、関連業務の運用状況及び関連文書の管理が適切に行われているか、定期的に監査を行わせること。

### (3) 監査結果に基づく措置

#### **対象：審査支払機関**

審査支払機関の長は、「医療情報システムの安全管理に関するガイドライン」の監査結果に基づく措置に関する規定に準じて、監査人より監査結果の報告を受け、指摘事項に対する是正措置を講じること。

#### **対象：実施機関**

実施機関の長は、「医療情報システムの安全管理に関するガイドライン」の監査結果に基づく措置に関する規定に準じて、監査人より監査結果の報告を受け、指摘事項に対する是正措置を講じること。