

レセプトのオンライン請求に係る
セキュリティに関するガイドライン

平成 20 年 2 月

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 物理セキュリティ.....	8
(1) 医療機関及び薬局の送信機器の設置場所.....	8
(2) 審査支払機関の送受信機器の設置場所.....	8
(3) 保険者の受信機器の設置場所	8
4 人的セキュリティ.....	8
(1) すべての人員の基本的な責務	8
(2) 機関の長の責務	9
5 技術的セキュリティ.....	9
(1) レセプトデータの機密性の確保.....	9
(2) 伝送相手の正当性の確保	9
(3) 伝送事実の正当性の確保	9
(4) システムの機密性の確保	9
(5) 伝送経路の機密性の確保	9
(6) 伝送の完全性の確保	10
(7) 他システムと接続する場合の要求事項.....	10
6 運用	10
(1) 開発規程	10
(2) 管理運用規程	10
(3) 開発及び試験環境と運用環境の分離.....	10
7 規程遵守.....	11
(1) セキュリティポリシー	11
8 規程に対する違反への対応.....	11
9 評価・見直し.....	11
(1) 監査証跡の保管	11
(2) 監査の実施	11
(3) 監査結果に基づく措置	11

I 総則

1 目的

情報システムの導入は、事務処理の効率化、利便性の向上等のメリットをもたらすことを目指している。しかし、そのメリットの反面、適切な対策が欠如したまま導入した場合には、データの漏洩、消失及び破壊や、情報システムの停止など、事務処理に多大な影響を与える可能性がある。診療報酬明細書等（以下単に「レセプト」という。）に係る電子情報処理組織の使用による費用の請求に関わるシステム（以下「オンライン請求システム¹」という。）についても決して例外ではなく、特に患者の氏名や傷病名等の慎重な取扱いを要する個人情報²を伝送するシステムであるため、適切な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、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」という。）に際し、レセプトに含まれる個人情報を適切に保護するとともに、オンライン請求業務の円滑な遂行に資することを目的として、オンライン請求業務及びオンライン請求システムに携わる人または組織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（以下「医療機関等」という。）は、情報システムの導入にあたっては、「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ドライン」（平成16年12月24日付け医政発第1224001号、薬食発第1224001号、老発第1224002号厚生労働省医政局長・医薬食品局長・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2版」（平成19年3月31日付け医政発第0330033号厚生労働省医政局長通知。以下「安全管理ガイドライン」という。）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。「安全管理ガイドライン」は、医療に関わる情報を扱うすべての情報システムと、それらのシステムの導入、運用、利用、保守及び廃棄にかかわる人または組織を対象としている。

レセプトを扱うオンライン請求システムは、医療に関わる情報を扱う情報システムであり、したがって、「安全管理ガイドライン」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。一方、オンライン請求に際し、レセプトに含まれる個人情報を適切に保護するとともに、オンライン請求業務の円滑な遂行に資することを目的として、オンライン請求システムに携わる人または組織が特に遵守すべき事項もある。また、オンライン請求業務及びオンライン請求システムに携わる人または組織には、医療機関等

¹ **オンライン請求システム**：レセプトをオンラインを活用した電子的手法により提出及び受取を行うためのシステムをいう。単にシステムと記述されている場合は、送信機器、送受信機器又は受信機器等のハードウェアとデータベース及び専用アプリケーション等のソフトウェアの総称をいう。

² **個人情報**：個人に関する情報であって、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。

だけではなく、医療機関等からレセプトを受取って審査支払を行う審査支払機関及び保険者も含まれる。

このため本ガイドラインは、「安全管理ガイドライン」に沿ってオンライン請求システムの導入、運用、利用、保守及び廃棄が行われることを前提とし、オンライン請求業務及びオンライン請求システムに携わる人または組織に求められる要件を規定するものである。

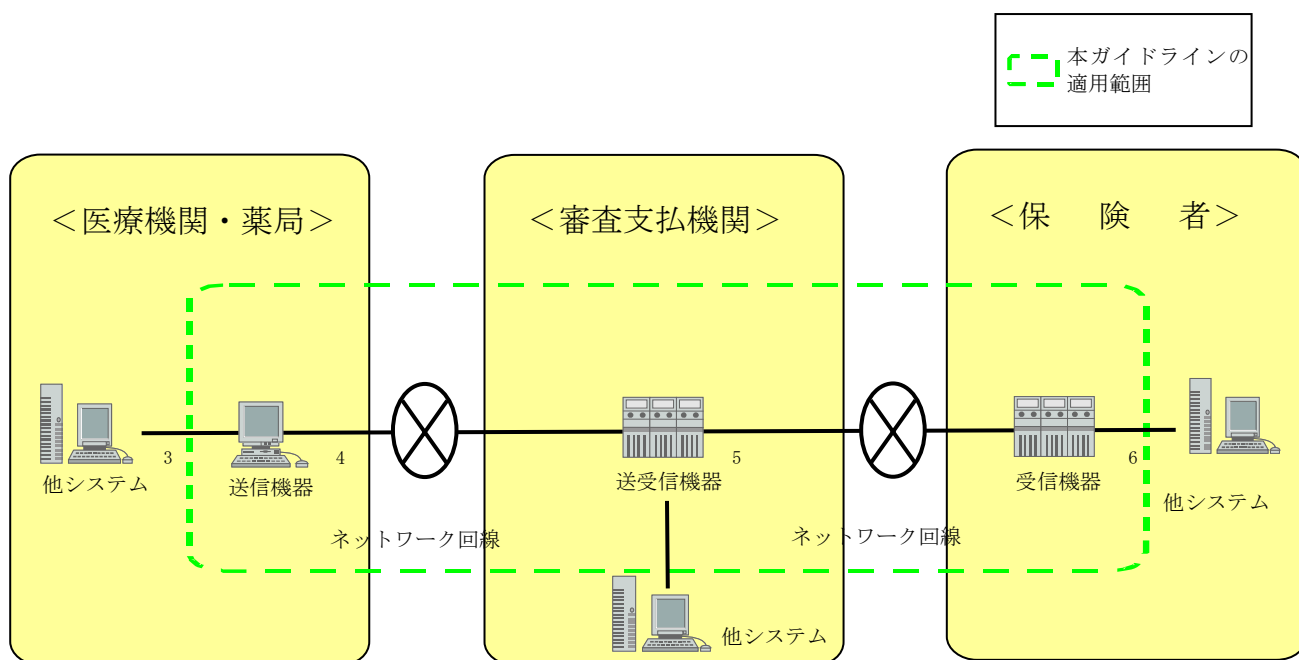
2 適用範囲

本ガイドラインは、オンライン請求システムの導入、運用、利用、保守及び廃棄にかかわる人または組織を対象とし、医療機関等だけではなく、審査支払機関及び保険者も対象になる。

また、本ガイドラインは、オンライン請求システムにおいて伝送されるレセプトをその対象とする。

したがって、物理的手法による搬送などの従来からの請求と、これら請求に付随する業務は、本ガイドラインの対象には含まれない。

本ガイドラインの対象範囲を、図1に示す。



[図 1 : ガイドライン対象範囲]

³ 他システム：オーダーリングシステム及び人事給与システム等、医療機関等で利用しているシステムあるいは、審査支払機関及び保険者が利用している業務システムをいう。

⁴ 送信機器：レセプト等を主に送信する機器の総称をいう。機器とは、例えばパソコン、ネットワーク機器及び外部記憶装置等がある。

⁵ 送受信機器：レセプト等を主に送受信する機器の総称をいう。機器とは、例えばサーバ、パソコン、ネットワーク機器、外部記憶装置、バックアップ装置及び無停電電源装置等がある。

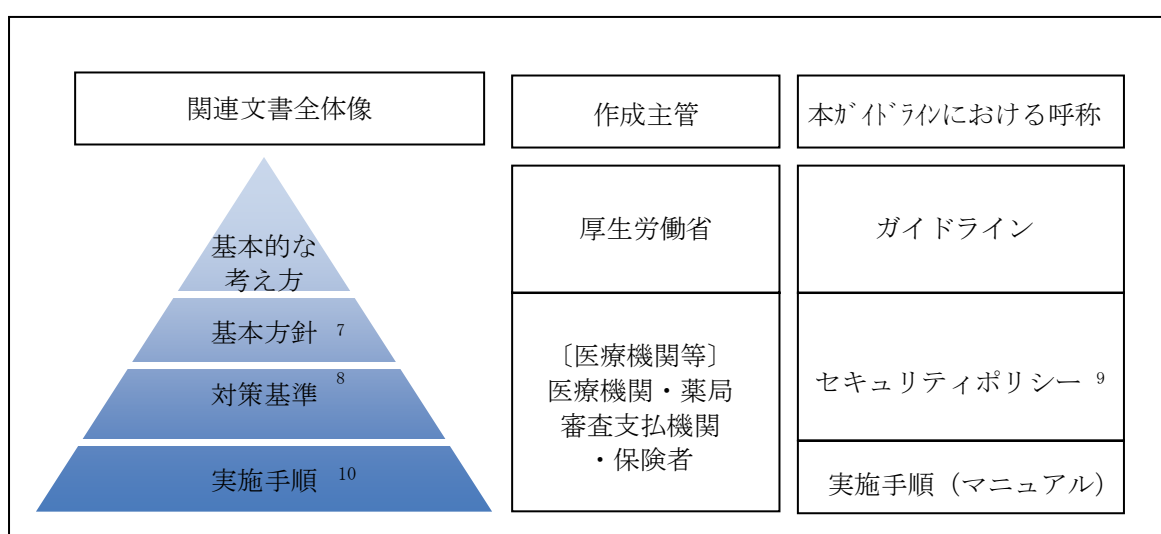
⁶ 受信機器：レセプト等を主に受信する機器の総称をいう。機器とは、例えばパソコン、ネットワーク機器及び外部記憶装置等がある。

3 位置付け

本ガイドラインは、前項の適用範囲に基づき、レセプトのオンライン化に関するセキュリティについて基本的な考え方を示すものであり、オンライン請求業務に携わる人または組織及びオンライン請求システムが最低限満たすことが必要と考えられる項目を示している。

オンライン請求を実施しようとする医療機関、薬局、審査支払機関並びに保険者は、本ガイドラインの内容に基づき、その組織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。また、本ガイドライン以外の対策についても、必要に応じて導入することが望ましい。

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]

⁷ **基本方針**：医療機関等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、医療機関等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、医療機関等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。

⁸ **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、つまり、基本方針を実現するために何をやらなければいけないかを示すものをいう。

⁹ **セキュリティポリシー**：医療機関等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と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、基本的な考え方並びに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定。基本方針及び対策基準からなるもの。

¹⁰ **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	オンライン請求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 ¹¹ と管理	オンライン請求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。
物理セキュリティ	オンライン請求システムで使用される送信機器、送受信機器又は受信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	オンライン請求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	オンライン請求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。
運用	オンライン請求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	オンライン請求システムを導入するにあ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	オンライン請求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	オンライン請求に関わる業務、システム、文書に対する評価及び見直しについて記述する。

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、オンライン請求の状況その他の事情を勘案し、必要に応じ見直しを行うものとする。

¹¹ **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

1 組織・体制

(1) 責任者の任命

機関の長¹²は、情報セキュリティの確保す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 第2版 第10章」に準じて、オンライン請求システムに従事する人員の情報セキュリティに関する役割と責任を定義し、責任者を任命すること。

(2) 責任の所在

機関の長は、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 第2版 第6.3章」、「医療情報システムの安全管理に関するガイドライン 第2版 第6.9章」及び「医療情報システムの安全管理に関するガイドライン 第2版 第6.10章」に準じて、医療機関、薬局、審査支払機関及び保険者のそれぞれの責任の所在を明確にしておくこと。

(3) 連絡体制

機関の長は、システム障害等における組織間の連絡を円滑に行うため、医療機関、薬局、審査支払機関及び保険者との連絡体制を明確にし、遵守すること。

¹² 機関の長：医療機関、薬局、審査支払機関及び保険者において、オンライン請求業務に関するすべ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

機関の長は、オンライン請求システムで取り扱う情報について、「医療情報システムの安全管理に関するガイドライン 第2版 第10章」に準じて、管理責任を明確にするため、管理責任者を定めること。

(2) 情報の分類

機関の長は、オンライン請求システムで取り扱う情報について、組織内で重要度の度合を共有するため、「医療情報システムの安全管理に関するガイドライン第2版 第6.2.2章」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

機関の長は、オンライン請求システムで取り扱う情報について、重要度の度合に応じた適切な取り扱いを行うため、「医療情報システムの安全管理に関するガイドライン 第2版 第6.3章」に準じて、情報の分類に応じた管理方法について定めること。

3 物理セキュリティ

(1) 医療機関及び薬局の送信機器の設置等

医療機関及び薬局は、医療機関及び薬局の責任において「医療情報システムの安全管理に関するガイドライン 第2版 第6.4章」に準じて、送信機器を設置し、運用すること。

(2) 審査支払機関の送受信機器の設置等

審査支払機関は、審査支払機関の責任において「医療情報システムの安全管理に関するガイドライン 第2版 第6.4章」及び「医療情報システムの安全管理に関するガイドライン 第2版 第6.9章」に準じて、送受信機器を設置し、運用すること。

(3) 保険者の受信機器の設置等

保険者は、保険者の責任において「医療情報システムの安全管理に関するガイドライン 第2版 第6.4章」に準じて、送受信機器を設置し、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

オンライン請求業務に携わるすべての者は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.6章」に準じて、オンライン請求業務における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

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 第2版 第6.6章」に準じて、その機関におけるオンライン請求業務に関する最終的な責任を有する者として、オンライン請求業務における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) レセプトデータの機密性の確保

オンライン請求業務に携わるすべての者は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.10章」に準じて、レセプトデータを正当な権限を有さない者から適切に保護すること。

(2) 伝送相手の正当性の確保

オンライン請求業務に携わるすべての者は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.10章」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。

(3) 伝送事実の正当性の確保

オンライン請求業務に携わるすべての者は、伝送相手が、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。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とは、例えば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をお互いに送信、送信ログ及び受信ログの保管などがある。

(4) システムの機密性の確保

オンライン請求業務に携わるすべての者は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.5章」及び「医療情報システムの安全管理に関するガイドライン 第2版 第6.10章」に準じて、システムの機密性を確保すること。

(5) 伝送経路の機密性の確保

オンライン請求業務に携わるすべての者は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.10章」に準じて、医療機関、薬局、審査支払機関及び保険者を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洩に対する機密性を確保する機能を有すること。

(6) 伝送の完全性の確保

オンライン請求業務に携わるすべての者は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.9章」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でも対処できる機能を有すること。伝送時における不測の事態に対処するとは、例えばレセプトデータの伝送中にネットワーク障害等が起きた場合、送信機器でネットワークの切断を検知して伝送を中止するようなことである。

(7) 他システムと接続する場合の要求事項

オンライン請求業務に携わるすべての者は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.10章」に準じて、オンライン請求システムを利用及び運用すること。他システムと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 運用

(1) 開発規程

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 第2版 第10章」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、遵守すること。

(2) 管理運用規程

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 第2版 第10章」に準じて、オンライン請求システムの管理運用におけるセキュリティについて明文化し、遵守すること。

(3) 開発及び試験環境と運用環境の分離

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 第2版 第10章」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

ア 医療機関、薬局、審査支払機関及び保険者は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.2章」に準じて、前記1～6において規定した事項を実行するためのオンライン請求システムに関わるセキュリティポリシーを策定し、運用すること。

イ 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、利用規約を定めることができることとし、医療機関、薬局及び保険者は、その利用規約を遵守すること。

8 規程に対する違反への対応

機関の長は、自らの機関で規定した内容に対する違反があった場合の対処について明確にし、厳正に対応すること。

9 評価・見直し

(1) 監査証跡の保管

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 第2版 第10章」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。

(2) 監査の実施

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 第2版 第10章」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し、オンライン請求についてシステム、文書及び業務が適切であるか定期的に監査を行うこと。

(3) 監査結果に基づく措置

審査支払機関における機関の長は、「医療情報システムの安全管理に関するガイドライン 第2版 第6.2章」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。