別添１

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１０月

厚　生　労　働　省

目　次

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、薬剤情報閲覧機能、特定健診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（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[1]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、薬剤情報閲覧、特定健診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、診療所及び薬局（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」（厚生労働省政策統括官通知）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。「医療情報システムの安全管理に関するガイドライン」は、医療に関わる情報を扱う全ての情報システムと、それらのシステムの導入、運用、利用、保守及び廃棄に関わる人又は組織を対象としている。

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、いずれも医療に関わる情報を扱う情報システムである。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、情勢に応

[1] **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。

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」（平成１５年法律第５７号）、「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」（平成２９年４月１４日付け個情第５３８号保発０４１４第１８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」（厚生労働省政策統括官通知）、「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」（平成２９年４月１４日付け個情第５４０号保発０４１４第１６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」（厚生労働省政策統括官通知）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」（平成２９年４月１４日付け個情第５４１号保発０４１４第１０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」（厚生労働省政策統括官通知）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。

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。

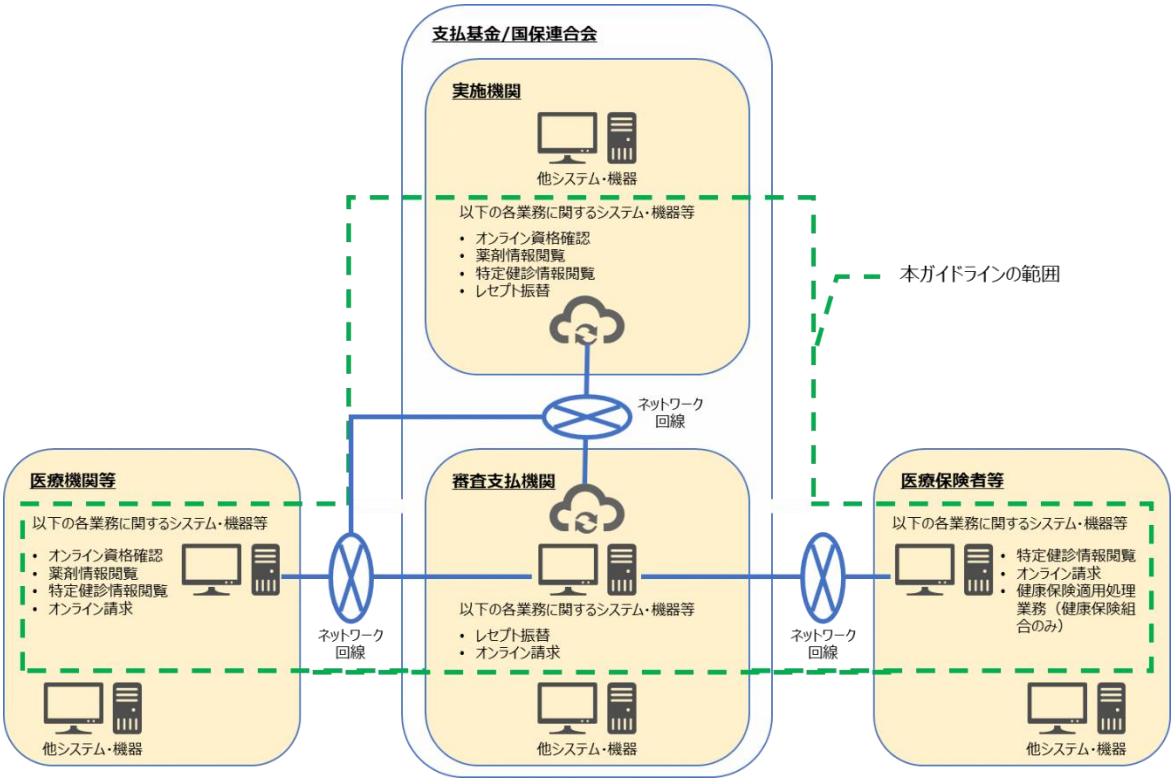

図 1：本ガイドラインの対象範囲

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。

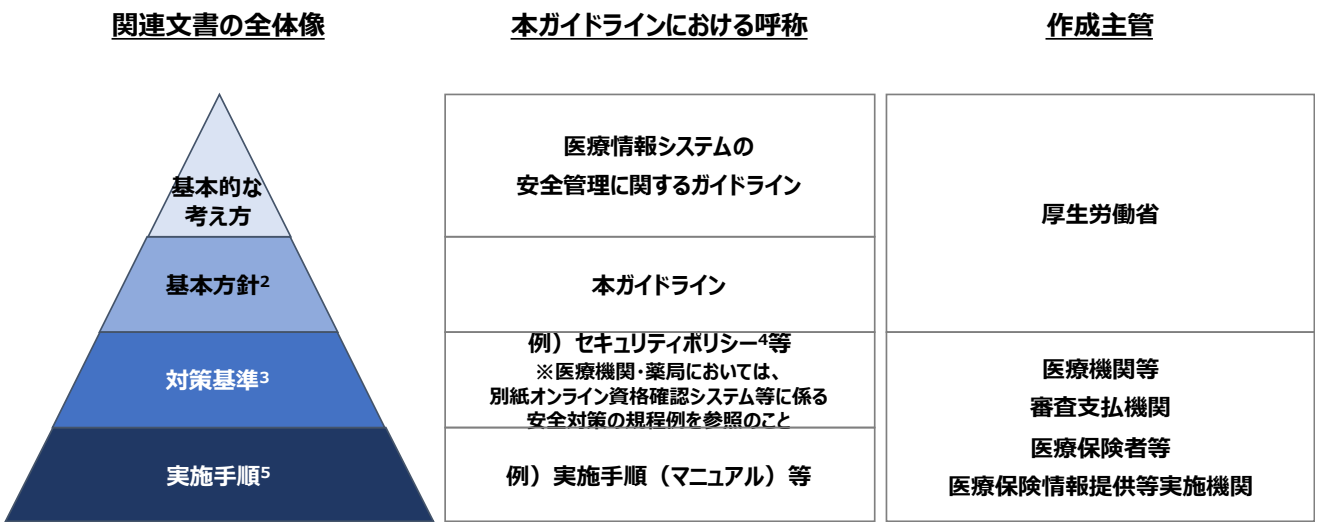

図 2：ガイドラインの位置付け

---

[2] **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。

[3] **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。

[4] **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。

[5] **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[6]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。

[6] **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[7]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　第6.3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10章」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　第４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6.3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6.10章」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　第6.10章」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。

---

[7] **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　第４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6.3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10章」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　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

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　第6.2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10章」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）　医療機関及び薬局の機器の設置等

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　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6.10章」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　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6.10章」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　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6.10章」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　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6.10章」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　第6.6章」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　第6.6章」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　第6.11章」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　第6.11章」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　第6.11章」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　第6.11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。

（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　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6.11章」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たサービス事業者によるクローズドな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　第6.11章」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　第6.10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6.11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　第6.11章」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　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、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　第10章」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　第10章」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　第10章」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　第10章」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　第10章」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　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

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　第6.1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6.2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10章」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　第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。

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　第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10章」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　第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　第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第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。

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　第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。

別添２

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及びレセプトのオンライン請求システムに係る安全対策の規程例（健康保険組合用）

○○健康保険組合

１　目的

この規程（以下「本規程」という。）は、○○健康保険組合（以下「当組合」という。）において、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及びオンライン請求システム（以下「両システム」）で使用される機器、ソフトウェア及び運用に必要な仕組み全般について、その取り扱い並びに管理に関する事項を定め、被保険者（及び被扶養者）の氏名や傷病名等の慎重な取り扱いを要する個人情報を適切に保護し、業務を円滑に遂行できることを目的とする。

２　組織・体制

・　当組合にシステム管理者を置き、理事長をもってこれに充てる。
・　理事長は必要な場合、システム管理者を別に指名することができる。
・　両システムを円滑に運用し、責任の所在を明確にするため、両システムに関する情報管理及び運用について、それぞれのシステム毎に情報管理及び運用のそれぞれを担当する責任者（情報管理責任者及び運用責任者）を置く。
・　情報管理責任者及び運用責任者は、理事長が指名することができる。
・　システム管理者は緊急時及び災害時の連絡、復旧体制並びに回復手順を定め、非常時においても参照できるように保存し、保管する。

３　情報の分類と管理

・　情報管理責任者は、両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いを共有するため、各々の情報の機密性を踏まえ、次の重要性分類に従って分類する。

厳秘：機密性が極めて高い情報の種別（例；レセプトデータ）

秘密：特定の範囲に限り開示することができる機密性が高い情報の種別

（例；実施手順（マニュアル））

公開：広く一般に公開可能である情報の種別

・　両システムで取り扱う情報について、ファイル名又は記録媒体等に情報の分類が分かるように表示をする等適切な管理を行わなければならない。

4　受信機器の設置場所等

・　両システムの受信機器を設置する場所を、パーティション等で仕切るか又は受信機器に覆いをするか等により、関係者以外の者が機器に接しないようにする。

・　両システムの受信機器は、社会保険手続業務及びオンライン請求業務のみに使用する。したがって、業務に必要とするソフトウェア以外のソフトウェアはインストールしない。

5　利用者の責務

・　利用者は、本規程、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の実施手順（マニュアル）及びオンライン請求システムの実施手順（マニュアル）に定められている事項を遵守すること。

・　利用者は、システム管理者の許可を得ず、受信機器及び記録媒体等を部屋外への持ち出しをしないこと。

・　利用者は、両システムを正しく利用するための教育と訓練を受けること。

・　利用者は、職務上知り得た個人情報を漏らさないこと。その職を辞した後も、同様である。

・　利用者は、個人情報の漏えい及び改ざんが生じた場合、並びにそれらが生じる恐れがある場合には、速やかに運用責任者に連絡し、その指示に従うこと。

・　利用者は、情報セキュリティ対策について不明な点、遵守することが困難な点等については、速やかにシステム管理者に相談し、指示を仰ぐこと。

・　利用者は、関係者以外の者が不正に両システムを利用できないようにユーザID及びパスワード等を、適切に管理すること。

6　システム管理者の責務

・　システム管理者は、両システムに関する受信機器の設定変更、更新を行う管理者権限等これらの運用における最終的な責任を負うこと。

・　システム管理者は、受信機器やソフトウェアに変更があった場合においても、利用者が社会保険手続及びオンライン請求業務の遂行を継続的にできるよう環境を整備すること。

・　システム管理者は、両システムを正しく利用させ、個人情報及び重要情報の思わぬ漏えいこれからを防ぐために、運用方法について、教育・訓練計画等を定めた上で、利用者の教育と訓練を行うものとする。

7　ソフトウェアの管理

運用責任者は、受信機器にコンピュータウイルス対策ソフトウェアをインストールするとともに、定期的にコンピュータウイルスのチェックを行い、感染の防止に努める。

8　運用

・　システム管理者は、両システムの取り扱いについて実施手順（マニュアル）を整備し、利用者に周知の上、常に利用可能な状態にしておく。

・　運用責任者は、ネットワークの不正な利用を発見した場合には、直ちにその原因を追求し対策を実施する。

9　規程に対する違反への対応

システム管理者は、本規程で定めた事項及び自らの機関で別に規定した事項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。

10　評価・見直し

システム管理者は、本規程で定めた事項及び自らの機関で別に規定した事項を評価し、定期的に見直す。

11　その他

その他、本規程の実施に関し必要な事項がある場合については、理事長がこれを定める。

12　適用年月日

本規程は令和〇年〇月〇日より適用する。

別添３

レセプトのオンライン請求システムに係る安全対策の規程例
（保険者用（健康保険組合を除く））

（保険者名）

１　目的

この規程（以下「本規程」という。）は、○○○○（以下「○○」という。）において、オンライン請求システムで使用される機器、ソフトウェア及び運用に必要な仕組み全般について、その取り扱い並びに管理に関する事項を定め、被保険者（及び被扶養者）の氏名や傷病名等の慎重な取り扱いを要する個人情報を適切に保護し、業務を円滑に遂行できることを目的とする。

２　組織・体制

・　○○にオンライン請求システム管理者（以下「システム管理者」という。）を置き、理事長をもってこれに充てる。
・　理事長は必要な場合、システム管理者を別に指名することができる。
・　オンライン請求システムを円滑に運用し、責任の所在を明確にするため、オンライン請求システムに関する情報管理及び運用について、それぞれを担当する責任者（情報管理責任者及び運用責任者）を置く。
・　情報管理責任者及び運用責任者は、理事長が指名することができる。
・　システム管理者は緊急時及び災害時の連絡、復旧体制並びに回復手順を定め、非常時においても参照できるように保存し、保管する。

３　情報の分類と管理

・　情報管理責任者は、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いを共有するため、各々の情報の機密性を踏まえ、次の重要性分類に従って分類する。

厳秘：機密性が極めて高い情報の種別（例；レセプトデータ）

秘密：特定の範囲に限り開示することができる機密性が高い情報の種別

（例；実施手順（マニュアル））

公開：広く一般に公開可能である情報の種別

・　オンライン請求システムで取り扱う情報について、ファイル名又は記録媒体等に情報の分

類が分かるように表示をする等適切な管理を行わなければならない。

4　受信機器の設置場所等

・　オンライン請求システムの受信機器を設置する場所を、パーティション等で仕切るか又は受信機器に覆いをするか等により、関係者以外の者が機器に接しないようにする。

・　オンライン請求システムの受信機器は、オンライン請求業務のみに使用する。したがって、業務に必要とするソフトウェア以外のソフトウェアはインストールしない。

5　利用者の責務

・　利用者は、本規程及びオンライン請求システムの実施手順（マニュアル）に定められている事項を遵守すること。

・　利用者は、システム管理者の許可を得ず、受信機器及び記録媒体等を部屋外への持ち出しをしないこと。

・　利用者は、オンライン請求システムを正しく利用するための教育と訓練を受けること。

・　利用者は、職務上知り得た個人情報を漏らさないこと。その職を辞した後も、同様である。

・　利用者は、個人情報の漏えい及び改ざんが生じた場合、並びにそれらが生じる恐れがある場合には、速やかに運用責任者に連絡し、その指示に従うこと。

・　利用者は、情報セキュリティ対策について不明な点、遵守することが困難な点等については、速やかにシステム管理者に相談し、指示を仰ぐこと。

・　利用者は、関係者以外の者が不正にオンライン請求システムを利用できないようにユーザID及びパスワード等を、適切に管理すること。

6　システム管理者の責務

・　システム管理者は、オンライン請求システムに関する受信機器の設定変更、更新を行う管理者権限等これらの運用における最終的な責任を負うこと。

・　システム管理者は、受信機器やソフトウェアに変更があった場合においても、利用者がオンライン請求業務の遂行を継続的にできるよう環境を整備すること。

・　システム管理者は、オンライン請求システムを正しく利用させるため、利用者の教育と訓練を行うこと。

7　ソフトウェアの管理

運用責任者は、受信機器にコンピュータウイルス対策ソフトウェアをインストールするとと

もに、定期的にコンピュータウイルスのチェックを行い、感染の防止に努める。

8　運用

・　システム管理者は、オンライン請求システムの取り扱いについて実施手順（マニュアル）を整備し、利用者に周知の上、常に利用可能な状態にしておく。

・　運用責任者は、ネットワークの不正な利用を発見した場合には、直ちにその原因を追求し対策を実施する。

9　規程に対する違反への対応

システム管理者は、本規程で定めた事項及び自らの機関で別に規定した事項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。

10　評価・見直し

システム管理者は、本規程で定めた事項及び自らの機関で別に規定した事項を評価し、定期的に見直す。

11　その他

その他、本規程の実施に関し必要な事項がある場合については、理事長がこれを定める。

12　適用年月日

本規程は令和〇年〇月〇日より適用する。

別添４

オンライン資格確認等システム及びレセプトのオンライン請求システムに係る安全対策の規程例

○○医院（又は病院、薬局）

１　目的

・　本規程は、○○医院（以下「当医院」という。）がオンライン資格確認システム、薬剤情報閲覧機能、特定健診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。）及び診療報酬明細書・調剤報酬明細書（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。）を適切に運用するために必要となる基本的な事項を定めるものである。

・　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（以下「本システム」という。）の運用に当たって使用される機器、端末、ソフトウェア等の適正な取扱いに関して必要な事項を定めるとともに、本システムで取り扱う患者の資格情報、薬剤情報、特定健診情報等の個人情報の適正な管理に関して必要な事項を定めるものである。

２　組織・体制

・　当医院に、オンライン資格確認等システム管理者（以下「システム管理者」という。）を置き、医院長をもって、これに充てる。

・　医院長は、必要な場合、システム管理者を別に指名することができる。

・　本システムを円滑に運用し、責任の所在を明確にするために、本システムに関する情報管理及び運用について、それぞれを担当する責任者（情報管理責任者及び運用責任者）を置く。

・　情報管理責任者及び運用責任者は、医院長が指名することができる。

・　システム管理者は、緊急時及び災害時の連絡、復旧体制及び回復手順を定めるとともに、非常時においても当該文書等を参照できるよう適切に保管する。

3　システム管理者の責務

・　システム管理者は、本システムに関する送信機器の設定変更、更新を行う管理者権限等これらの運用における最終的な責任を負うものとする。

・　システム管理者は、送信機器やソフトウェアに変更があった場合においても、利用者がオンライン資格確認等業務の遂行を継続的にできるよう環境を整備するものとする。

・　システム管理者は、本システムを正しく利用させ、個人情報及び重要情報の思わぬ漏えいを防ぐために、運用方法について、教育・訓練計画等を定めた上で、利用者の教育と訓練を行うものとする。

4　情報管理責任者の責務

・　情報管理責任者は、本システムで取り扱う患者の個人情報の適正な管理に関する責任を負う。

・　情報管理責任者は、本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いを共有するため、各々の情報の機密性を踏まえ、次の重要性分類を定義する。

厳秘	機密性が極めて高い情報の種別（例：薬剤情報、特定健診情報）
秘密	特定の範囲に限り開示することができる機密性が高い情報の種別 （例:実施手順（マニュアル)）
公開	広く一般に公開可能である情報の種別

・　情報管理責任者は、特に、本システム導入時、適切に管理されていないメディア使用時、又は外部からの情報受領時においては、コンピュータウイルス等の不正なソフトウェアが混入していないか確認する。

5　運用責任者の責務

・　運用責任者は、本システムの運用に当たって使用される機器、端末、ソフトウェア等の適正な取扱いに関する責任を負う。

・　本システムの送受信機器は、以下の業務に使用する。したがって、運用責任者はこれらの業務に必要とするソフトウェア以外のソフトウェアはインストールされていない事を点検する。

- オンライン資格確認等業務
- オンライン資格確認等業務の遂行上必要となる業務
- オンライン請求業務（レセプト作成業務等を含む。）
- オンライン請求業務の遂行上必要となる業務

・　運用責任者は、本システムで使用する送信機器にコンピュータウイルス対策ソフトウェアをインストールするとともに、定期的にコンピュータウイルスのチェックを行い、感染の防止に努める。

・　運用責任者は、ネットワークの不正な利用を発見した場合には、直ちにその原因を追求し対策を実施するものとする。

・　運用責任者は、本システムの取扱いについて実施手順（マニュアル）を整備し、利用者に周知の上、常に利用可能な状態にしておくものとする。

・　運用責任者は、本システムで取り扱う情報、本システムを構成する機器・ソフトウェアをリストアップした上で重要度に応じた分類を行い、必要に応じて情報の分類を表示する。また、常にリストを最新の状態に維持する。
・　本システムに関する送受信機器は、関係者以外の者による覗き見を防止するため、スクリーンフィルタを設置する等の対策を施す。

6　利用者の責務

・　利用者は、本規程及び本システムの実施手順（マニュアル）に定められている事項を遵守するものとする。
・　利用者は、システム管理者の許可を得ず、送信機器等を部屋外への持ち出しをしないものとする。
・　利用者は、本システムを正しく利用するための教育と訓練を受けるものとする。
・　利用者は、職務上知り得た個人情報を漏らさないものとする。その職を辞した後も、同様である。
・　利用者は、個人情報の漏えい及び改ざんが生じた場合及びそれらが生じる恐れがある場合には、速やかに運用責任者に連絡し、その指示に従うものとする。
・　利用者は、情報セキュリティ対策について不明な点、遵守することが困難な点等については、速やかに情報管理責任者に相談するものとする。
・　利用者は、本システムで取り扱う情報については、当医院内において定義した機密性分類に従って、取扱いを行う。
・　利用者は、関係者以外の者が不正に本システムを利用できないようにユーザ ID 及びパスワード等を、本人しか知り得ない状態に保つように適切に管理する。
・　本システムで取り扱うシステムにおいて、２要素認証を採用している場合を除き、利用者は、パスワードを定期的に変更する。（最長でも２か月以内に変更する）
・　利用者は、パスワードについて、類推しやすい文字列、極端に短い文字列、類似の文字列を繰り返し使用しない。

7　規程に対する違反への対応

・　システム管理者は、本規程に定める事項及び本機関で別に定める事項に対する違反があった場合の対処方法について明確にするとともに、それに従って、厳正に対応する。

8　評価・見直し

・　システム管理者は、本規程に定める事項及び本機関で別に定める事項を評価し、必要に応じて、定期的に見直す。

9　その他

・　適切なセキュリティ対策を図るために、当医院は「別表：本システム導入のために特に留意すべきセキュリティ対策」に示す技術的対策等を行う。

・　その他、本規程の実施に関し必要な事項がある場合については、医院長がこれを定める。

10　適用年月日

・　本規程は令和〇年〇月〇日より適用する。

別表：本システム導入のために特に留意すべきセキュリティ対策

1	本システムへのアクセスについては、利用者の識別と認証を行うこと。
2	本システムを導入する際は、オンライン請求ネットワークを利用し、ネットワーク経路でのメッセージ挿入、コンピュータウイルス混入等の改ざんを防止する対策を行うこと。
3	本システムを導入する際は、コンピュータウイルス等の不正なソフトウェアの混入を防ぐ適切な措置をとること。また、その対策の有効性・安全性の確認・維持（例えばパターンファイルの更新の確認・維持）を行うこと。
4	本システムの運用に当たって使用される機器、端末等において、接続できる外部記憶媒体（USB 機器等）の制限を実施すること。
5	本システムを導入する際は、外部ネットワークから本システムへのアクセスを制限する仕組みを導入し、ネットワーク事業者に対して外部ネットワークからのアクセスを制限する仕組みが導入されていることを確認すること。
6	本システムを導入する際は、医療機関等内部ネットワークにおいても、セキュリティ要件の異なるシステム間や安全管理上の重要部分との境界にはファイアウォール等を設置し、ネットワークを物理的又は論理的に分割すること。
7	本システムの導入に当たり無線 LAN を利用する場合は、以下の対策を実施すること。 ・利用者以外に無線 LAN の利用を特定されないようにすること ・関係者以外のアクセスを禁止する対策を施すこと。 ・通信を暗号化し情報を保護すること。
8	本システムを導入する際は、ネットワーク事業者に対して、医療機関間の通信を制限する仕組みを導入していることを確認すること。

別添５

レセプトのオンライン請求システムに係る安全対策の規程例
（保険医療機関及び保険薬局用）

○○医院（又は病院、薬局）

１　目的

この規程（以下「本規程」という。）は、○○医院（以下「当医院」という。）において、オンライン請求システムで使用される機器、ソフトウェア及び運用に必要な仕組み全般について、その取り扱い並びに管理に関する事項を定め、患者の氏名や傷病名等の慎重な取り扱いを要する個人情報を適切に保護し、業務を円滑に遂行できることを目的とする。

２　組織・体制

・　当医院にオンライン請求システム管理者（以下「システム管理者」という。）を置き、医院長をもってこれに充てる。
・　医院長は必要な場合、システム管理者を別に指名することができる。
・　オンライン請求システムを円滑に運用し、責任の所在を明確にするため、オンライン請求システムに関する情報管理及び運用について、それぞれを担当する責任者（情報管理責任者及び運用責任者）を置く。
・　情報管理責任者及び運用責任者は、医院長が指名することができる。
・　システム管理者は緊急時及び災害時の連絡、復旧体制並びに回復手順を定め、非常時においても参照できるように保存し、保管する。

３　情報の分類と管理

・　情報管理責任者は、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いを共有するため、各々の情報の機密性を踏まえ、次の重要性分類に従って分類する。

厳秘：機密性が極めて高い情報の種別（例；レセプトデータ）

秘密：特定の範囲に限り開示することができる機密性が高い情報の種別

（例；実施手順（マニュアル））

公開：広く一般に公開可能である情報の種別

・　オンライン請求システムで取り扱う情報について、ファイル名又は記録媒体等に情報の分

類が分かるように表示をする等適切な管理を行わなければならない。

4　送信機器の設置場所等

・　オンライン請求システムの送信機器を設置する場所を、パーティション等で仕切るか又は送信機器に覆いをするか等により、関係者以外の者が機器に接しないようにする。

・　オンライン請求システムの送信機器は、オンライン請求業務（レセプト作成業務を含む。）のみに使用する。したがって、業務に必要とするソフトウェア以外のソフトウェアはインストールしない。

5　利用者の責務

・　利用者は、本規程及びオンライン請求システムの実施手順（マニュアル）に定められている事項を遵守すること。

・　利用者は、システム管理者の許可を得ず、送信機器及び記録媒体等を部屋外への持ち出しをしないこと。

・　利用者は、オンライン請求システムを正しく利用するための教育と訓練を受けること。

・　利用者は、職務上知り得た個人情報を漏らさないこと。その職を辞した後も、同様である。

・　利用者は、個人情報の漏えい及び改ざんが生じた場合、並びにそれらが生じる恐れがある場合には、速やかに運用責任者に連絡し、その指示に従うこと。

・　利用者は、情報セキュリティ対策について不明な点、遵守することが困難な点等については、速やかにシステム管理者に相談し、指示を仰ぐこと。

・　利用者は、関係者以外の者が不正にオンライン請求システムを利用できないようにユーザID及びパスワード等を、適切に管理すること。

6　システム管理者の責務

・　システム管理者は、オンライン請求システムに関する送信機器の設定変更、更新を行う管理者権限等これらの運用における最終的な責任を負うこと。

・　システム管理者は、送信機器やソフトウェアに変更があった場合においても、利用者がオンライン請求業務の遂行を継続的にできるよう環境を整備すること。

・　システム管理者は、オンライン請求システムを正しく利用させるため、利用者の教育と訓練を行うこと。

7　ソフトウェアの管理

運用責任者は、送信機器にコンピュータウイルス対策ソフトウェアをインストールするとと

もに、定期的にコンピュータウイルスのチェックを行い、感染の防止に努める。

8　運用

・　システム管理者は、オンライン請求システムの取り扱いについて実施手順（マニュアル）を整備し、利用者に周知の上、常に利用可能な状態にしておく。

・　運用責任者は、ネットワークの不正な利用を発見した場合には、直ちにその原因を追求し対策を実施する。

9　規程に対する違反への対応

システム管理者は、本規程で定めた事項及び自らの機関で別に規定した事項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。

10　評価・見直し

システム管理者は、本規程で定めた事項及び自らの機関で別に規定した事項を評価し、定期的に見直す。

11　その他

その他、本規程の実施に関し必要な事項がある場合については、医院長がこれを定める。

12　適用年月日

本規程は令和〇年〇月〇日より適用する。