

## 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

システムは、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機能を有すること。

<細則13（レセプトデータの機密性を確保する機能に関する細則）>

レセプトデータの機密性を確保する機能とは、例えば、以下のとおりである。

- ・ オペレーティング・システム及びデータベース管理システム等によるアクセス制御
- ・ 暗号化によるアクセス制御

### (2) 伝送相手の正当性の確保

システムは、医療機関、薬局、審査支払機関並びに保険者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。

<細則14（伝送相手の正当性を確保する機能に関する細則）>

伝送相手の正当性を確保する機能とは、例えば、以下のとおりである。

- ・ 電子証明書による認証

### (3) 伝送事実の正当性の確保

システムは、医療機関、薬局、審査支払機関並びに保険者が、レセプトデータの送受信に関する事実を確認できる機能を有すること。

<細則15（レセプトデータの送受信に関する事実を確認できる機能に関する細則）>

レセプトデータの送受信に関する事実を確認できる機能とは、例えば、以下のとおりである。

- ・ 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

### (4) システムの機密性の確保

ア システムは、システムの利用及び運用を行う正当な権限者であることを確認する機能を有すること。

<細則16（正当な権限者であることを確認する機能に関する細則）>

正当な権限者であることを確認する機能とは、例えば、以下のとおりである。

- ・ ユーザ ID/パスワードによる認証

イ システムは、システムの稼働に必要なプログラム、システム設定及びログ等を、正当な権限を有さない者から適切に保護する機能を有すること。

<細則17（正当な権限を有さない者から適切に保護する機能に関する細則）>

正当な権限を有さない者から適切に保護する機能とは、例えば、以下のとおりである。

- ・ オペレーティング・システム及びデータベース管理システム等によるアクセス制御

ウ システムは、ネットワークの利用に際して、許可されていない者による不正アクセス<sup>13</sup>を防止する機能を有すること。

<細則18（ネットワークの利用に際する機密性に関する細則）>

以下について遵守すること。

- ・ 審査支払機関のシステムにおいては、ファイアウォール装置及び不正アクセス監視装置を設置するとともに、コンピュータウイルス対策を行うこと。
- ・ 医療機関、薬局並びに保険者のシステムにおいては、ファイアウォール機能及び不正アクセス監視機能を有するとともに、コンピュータウイルス対策を行うことが望ましい。
- ・ 医療機関、薬局、審査支払機関並びに保険者の送信機器、送受信機器又は受信機器にセキュリティホールが発見された場合には、適切にセキュリティパッチの適用を行うこと。

---

<sup>13</sup> 不正アクセス：不正な手段により、正当な利用者以外が行うアクセスあるいは正当な利用者の過失等による権限外のアクセスをいう。

#### (5) 伝送経路の機密性の確保

システムは、医療機関、薬局、審査支払機関並びに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。

<細則19 (伝送経路の機密性に関する細則) >

以下について遵守すること。

- ・ 伝送経路のデータは暗号化して送信し、送受信機器又は受信機器で復号化を行うこと。

#### (6) 伝送の完全性の確保

システムは、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。

<細則20 (伝送時における不測の事態の対処に関する細則) >

以下の機能を備えること。

- ・ 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、送信機器がネットワークの切断を検知し、伝送を中止する。

#### (7) 他システムと接続する場合の要求事項

システムは、オンライン請求業務専用の環境で利用及び運用すること。複合的活用や費用軽減などの事由により、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機能を備えること。

<細則21 (他システムからの悪影響を遮断する機能に関する細則) >

他システムからの悪影響を遮断する機能とは、例えば、以下のとおりである。

- ・ 原則として、医療機関及び薬局の送信機器は、オンライン請求システムで使用する回線とのみ接続
- ・ オンライン請求システムと他システムの間にはルーター等のネットワーク機器を設置することによるアクセス制御

## 6 運用

### (1) 開発規程

審査支払機関は、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。

<細則22（開発におけるセキュリティに関する文書に関する細則）>

セキュリティの方針や対策等に関する文書には、例えば、以下のものがある。

- ・ システムセキュリティ方針
- ・ システムセキュリティ設計書
- ・ システム開発管理マニュアル

### (2) 管理運用規程

審査支払機関は、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。

<細則23（管理運用におけるセキュリティに関する文書に関する細則）>

管理運用におけるセキュリティに関する文書には、例えば、以下のものがある。

- ・ システム利用者マニュアル
- ・ システム管理者マニュアル

### (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、運用環境から分離すること。

<細則24（開発及び試験環境と運用環境の分離に関する細則）>

開発及び試験環境と運用環境の分離に際しては、以下の観点を考慮すること。

- ・ 開発及び試験に使用するハードウェア、ソフトウェア及びネットワークは、運用に使用するこれらのものと異なる機器を使用することが望ましい。
- ・ 開発及び試験に関わる人員と、運用に関わる人員は、職務上分離することが望ましい。
- ・ 開発及び試験を行う場所と、運用を行う場所は、物理的に分離することが望ましい。

## 7 規程遵守

### (1) セキュリティポリシー

ア 医療機関、薬局、審査支払機関並びに保険者は、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。

<細則25（オンライン請求システムに関するセキュリティポリシーに関する細則）>

セキュリティポリシーでは、以下の項目について明らかにすること。

- ・ 組織・体制
- ・ 情報の分類と管理
- ・ 物理セキュリティ
- ・ 人的セキュリティ
- ・ 技術的セキュリティ
- ・ 運用
- ・ 規程遵守
- ・ 規程に対する違反への対応
- ・ 評価・見直し

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、医療機関及び薬局並びに保険者は、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) 監査証拠の保管

審査支払機関は、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、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。

<細則26（オンライン請求システムの監査に関する細則）>

監査においては、少なくとも以下について確認すること。

- ・ システム機能面
  - 正しく機能が実装されているか
  - 正しく設定が行われているか
  - 実装された機能が陳腐化していないか
- ・ システム運用面
  - 整備すべき文書があるか
  - 定められた規程が遵守されているか
  - 不正アクセスの傾向の有無と対処が適切であったか
  - 定められた規程が現実的であるか

### (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、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。

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)

〇〇医院(又は病院、薬局)

1 目的

この規程(以下「本規程」という。)は、〇〇医院(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等を漏らさないこと。その職を辞した後も、同様である。
- ・ 利用者は、個人情報の漏洩及び改竄が生じた場合、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ィ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ィ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

本規程は平成〇年〇月〇日より適用する。

## 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)

〇〇健康保険組合(又は他の保険者名)

### 1 目的

この規程(以下「本規程」という。)は、〇〇健康保険組合(以下「当組合」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

- ・ 当組合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、個人情報の漏洩及び改竄が生じた場合、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

本規程は平成〇年〇月〇日より適用する。