別添１

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１８年４月

厚　生　労　働　省

目　次

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者が遵守すべき事項を示すものである。

---

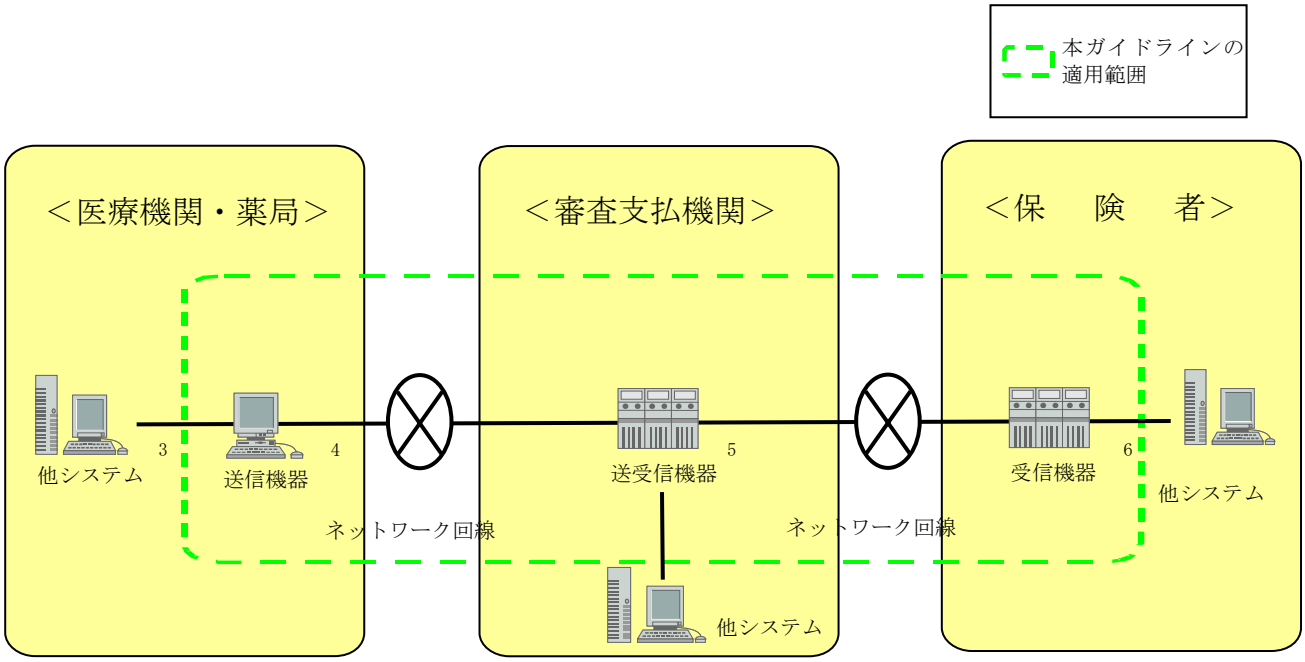
[1] **オンライン請求システム**：レセプトをオンラインを活用した電子的手法により提出及び受取を行うためのシステムをいう。単にシステムと記述されている場合は、送信機器、送受信機器又は受信機器等のハードウェアとデータベース及び専用アプリケーション等のソフトウェアの総称をいう。

[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。

2　適用範囲

本ガイドラインは、オンラインを活用した電子的手法によるレセプトの提出及び受取を対象とし、その業務及びシステムに携わるすべての関係者に適用されるものである。なお、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**：レセコンの医事会計システム、オーダ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。

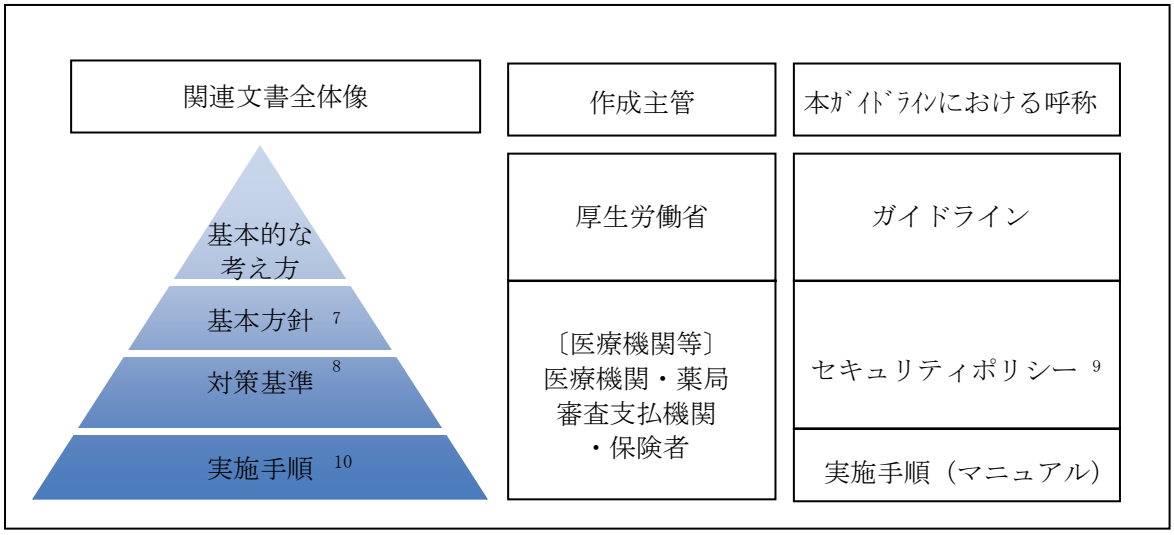
[6] **受信機器**：レセプト等を主に受信する機器の総称をいう。機器とは、例えばパソコン、ネットワーク機器及び外部記憶装置等がある。

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関わる組織及び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、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。

＜細則1（役割と責任に関する細則）＞

責任者には、以下の役割と責任を明確にすること。
- オンライン請求業務全体の責任
- オンライン請求業務及びシステムのセキュリティに対する責任
- オンライン請求業務及びシステムで取り扱う情報の管理に対する責任
- オンライン請求システムの開発及び運用に対する責任
- オンライン請求システムの開発及び管理運用を外部委託する場合の委託会社の管理監督に対する責任

（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、医療機関、薬局、審査支払機関並びに保険者との責任の所在を明確にしておくこと。

＜細則2（責任の所在の明確化に関する細則）＞

例えば、以下の事象について責任を明確にすること。
- サービス品質の低下
- システム障害及びウィルス感染
- 地震及び火災等の災害時

（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、審査支払機関並びに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、審査支払機関並びに保険者において、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、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、情報の分類を定めること。

＜細則3（情報の分類に関する細則）＞

例えば、以下のような分類がある。
- 重要性に応じた分類：「厳秘」「秘密」「公開」
- 開示範囲に応じた分類：「～関係者限り」

（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、情報の分類に応じた管理方法について定めること。

＜細則4（情報の分類に応じた管理方法に関する細則）＞

それぞれの情報の分類について、以下の管理方法を検討すること。
- 情報の分類の明示方法
- 情報に対するアクセス権限
- 情報に対する暗号化の要否
- 情報が格納された媒体の管理
- 情報の保管、変更及び廃棄に関する管理

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場所

ア　医療機関及び薬局の送信機器を設置する部屋は、施錠可能とすること。

イ　医療機関及び薬局の送信機器を設置する部屋は、関係者の入退室を適切に管理すること。

＜細則5（医療機関及び薬局の送信機器を設置する部屋への入退室管理に関する細則）＞

入退室管理とは、例えば、以下のとおりである。
- 関係者の不在時等の施錠管理
- 部屋内での身分証明書の常時着用
- 関係者以外の入室に対する注意

ウ　医療機関及び薬局の送信機器は、オンライン請求業務を専用に行う物理的区画に設置されることが望ましい。

＜細則6（物理的区画に関する細則）＞

セキュリティ向上の観点から、医療機関及び薬局の機器においては、オンライン請求業務を専用に行う部屋に設置されることが望ましい。医療事務等の利便性を考慮して医療機関及び薬局の送信機器が院内受付等に置かれる場合、関係者以外の者が不正に使用できないようにするため、パーティション（空間を仕切る取りはずしが可能な壁。間仕切り。）等で仕切るかあるいは送信機器に覆いをするかなどの対策が講じられることが望ましい。

（2）　審査支払機関の送受信機器の設置場所

ア　審査支払機関の送受信機器は、オンライン請求業務を専用に行う部屋に設置すること。

イ　審査支払機関の送受信機器を設置する部屋は、施錠可能とすること。

ウ　審査支払機関の送受信機器を設置する部屋は、入退室管理が適切に行われること。

＜細則7（審査支払機関の送受信機器を設置する部屋への入退室管理に関する細則）＞
以下について遵守すること。

- 常時施錠管理
- 部屋への入室時の身分証明書（例：社員証、入館許可証等）による身分確認
- 部屋内での身分証明書の常時着用
- 部屋への入退室に関する記録保持

エ　審査支払機関の送受信機器は、災害を防ぐ装置を適切に備えること。

＜細則8（災害を防ぐ装置に関する細則）＞

災害を防ぐ装置とは、例えば、以下のとおりである。
- 消火装置
- 転倒防止装置
- 免震装置

オ　審査支払機関の送受信機器は、施錠可能なラック、棚等の保管設備に収納すること。

（3）　保険者の受信機器の設置場所

ア　保険者の受信機器を設置する部屋は、施錠可能とすること。

イ　保険者の受信機器を設置する部屋は、関係者の入退室を適切に管理すること。

＜細則9（保険者の受信機器を設置する部屋への入退室管理に関する細則）＞

入退室管理とは、例えば、以下のとおりである。
- 関係者の不在時等の施錠管理
- 部屋内での身分証明書の常時着用
- 関係者以外の入室に対する注意

ウ　保険者の受信機器は、オンライン請求業務を専用に行う物理的区画に設置されることが望ましい。

＜細則10（物理的区画に関する細則）＞

セキュリティ向上の観点から、保険者の機器においては、オンライン請求業務を専用に行う部屋に設置されることが望ましい。

４　人的セキュリティ

（１） すべての人員の基本的な責務

ア　オンライン請求業務に携わるすべての者は、レセプトの請求業務の遂行を目的として、オンライン請求システムを開発、運用及び利用すること。

イ　オンライン請求業務に携わるすべての者は、職務上知り得た個人情報を正当な理由なく漏らしてはならない。その職を辞した後も、同様である。

ウ　オンライン請求業務に携わるすべての者は、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、速やかに所属する機関の長に報告すること。

（２） 機関の長の責務

ア　機関の長は、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し、従事する人員が適正に業務を実施するよう監督すること。

イ　機関の長は、システム及び業務に従事する人員に対して、情報セキュリティに関する啓発及び教育を実施すること。

＜細則11（機関の長が行うべき啓発及び教育に関する細則）＞

以下について実施すること。
- 従事するシステム及び業務に応じて必要となる啓発及び教育内容の規定
- 啓発及び教育に関する実施計画の策定
- 啓発及び教育に関する実施記録の保管

ウ　機関の長は、個人情報の漏洩及び改竄が生じたとの報告、並びにそれらが生じる恐れがあるとの報告を受けた場合には、速やかに対処すること。

＜細則12（機関の長が行うべき対処に関する細則）＞

機関の長が行うべき対処は、例えば、以下のとおりである。
なお、以下にあてはまらないものについては、個別に討議し、実施すること。
- 事態の把握、収拾、解明及び再発の防止
- 違反者への懲罰（就業規則に基づく懲戒等）
- 刑事措置（告訴等）

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[13]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、コンピュータウィ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、コンピュータウィ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。

[13] **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）　監査証跡の保管

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。