資料1

# レセプト情報等の利用にあたってのセキュリティ要件について

平成23年８月４日

厚生労働省保険局総務課

# （はじめに）セキュリティ要件の具備について

○　レセプト情報等の利用にあたっては、「レセプト情報・特定健診等情報の提供に関するガイドライン」により、利用者に一定のセキュリティ水準を具備することを求めている。

○　こうしたセキュリティ要件については、６月20日の第６回レセプト情報等の提供に関する有識者会議において、模擬申出に対する実地検査を踏まえた確認・検討事項について議論を行ったところ。

○　本日は、模擬申出に対する実地検査等も踏まえ、改めて、今後、レセプト情報等の利用を予定されている方々に、必要となるセキュリティ要件について御説明を行うことを目的とする。

○　また、特にISMSの実践については、より具体的な説明が必要との御意見もあり、本日改めて説明をするもの。

# データ提供にあたってのセキュリティ要件

## 考え方

〇レセプト情報等については、他の情報との照合による識別性の問題があることから、全て個人情報に準じた措置を講ずる必要（第2回レセプト情報等の提供に関する有識者会議での議論）。

〇したがって、レセプト情報等を利用する者に対して、医療機関等が個人情報を取り扱う場合等に適用される「医療情報システムの安全管理に関するガイドライン」（第4.1版　平成22年2月　厚生労働省）に準じた措置をレセプト情報等にも基本的に講ずることを求める。

〇ただし、有識者会議で集計表情報の提供として認められたものについては、以下のセキュリティ要件を審査基準とはしないこととした。（審査基準とはしないが適切な管理・保管を行う必要がある。）

## セキュリティ要件の概要

①基本的事項（国内のあらかじめ申し出られた場所での利用、外部ネットワークへの接続禁止、第三者への貸与等の禁止など）

②所属機関が一般的に具備すべき条件（必ずしも所属機関全体で対応する必要はなく部、課、研究室等適切な範囲で対応）
ⅰ）個人情報保護に関する方針の策定・公表、ⅱ）情報セキュリティマネジメントシステム（ISMS）の実践
ⅲ）組織的安全対策（体制、運用管理規程）、ⅳ） 人的安全対策（雇用契約における従業員への守秘義務等）
ⅴ）情報の破棄（手順等）、ⅵ）情報システムの改造と保守、ⅶ）災害時等の非常時の対応

③レセプト情報等の利用に際し具備すべき条件（必ずしも所属機関全体で対応する必要はなく部、課、研究室等適切な範囲で対応）
ⅰ）物理的安全対策（保存場所の施錠等）、ⅱ）技術的安全対策（利用者の識別と認証）、
ⅲ）例外的に利用者間での受け渡し等のために持ち出す際の措置

※レセプト情報等の利用に直接的な関連性が低いと考えられるものも所属機関の信頼性を確保する観点から、実施を求めることとし、利用形態を勘案して必要がないと考えられる規定については、個別に利用者から理由を明示させることとした。

# 第６回有識者会議における議論

**＜第６回有識者会議における議論＞**

〇模擬申出により提供したレセプト情報等の利用状況について、厚生労働省保険局において実地検査を実施。６月20日第６回レセプト情報等の提供に関する有識者会議において、その結果について議論し、レセプト情報等の利用にあたっては、今後、以下の点も加味して運用を行う方向とした。

**＜今後の運用について＞**

〇申出の段階で、申出者から具体的な利用形態の概念図を提出させ、それを踏まえてデータ利用の各段階でどのようなリスクがあるかを勘案して審査を行う必要がある。

〇セキュリティ事故防止の観点から、できる限り実地検査はデータ提供前に行うこととして、それが不可能な場合には、利用者の所属する機関の長の名義による内部監査報告等の提出を求めることとしてはどうか。

〇管理責任の明確化の観点からは提供したレセプト情報等の複写は原則１回のみとすることは必要と考えられるが、模擬申出の例のようにレセプト情報等のデータ規模が相当程度大きい場合には、一旦、サーバに格納した上で必要な部分のみを切り出して別の端末で使用する形態も考えられる。
　この場合には、別の端末へデータを運搬する媒体の管理や当該別の端末についてもガイドラインに基づく利用を徹底することにより、例外として認める。

〇情報セキュリティマネジメントシステムの実践等については、ISMS認証を受けること等を必ずしも要求しているものではなく、利用形態等を勘案した合理的な対応を図ることが求められることを周知徹底する必要がある。

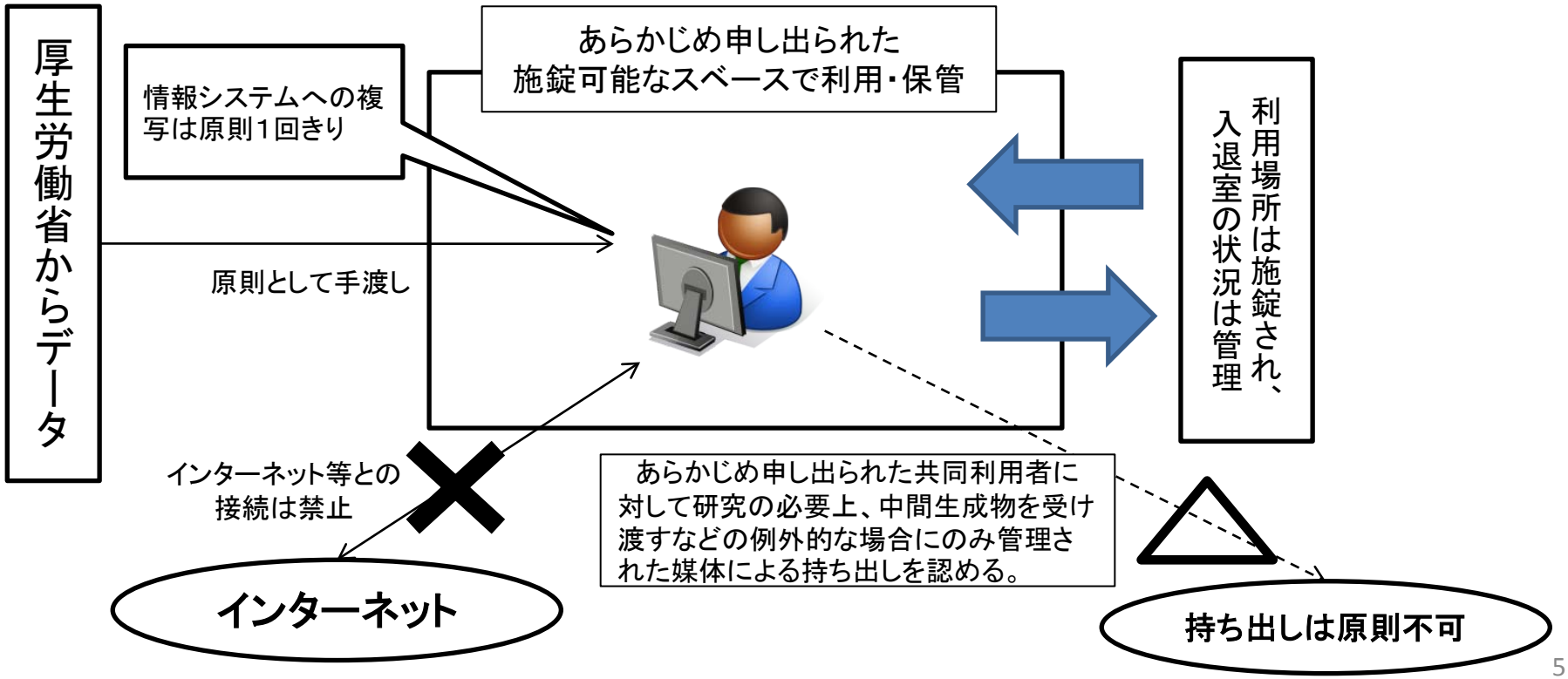
〇現行、ガイドラインに明記されてはいないが、情報の管理が１人の者に集中することをどう考えるか。セキュリティ要件を適切に担保する観点からは、第三者が関与することにより、利用者に対して何らかの牽制効果を発揮できる仕組みを今後検討する必要がある。

# １．基本的な利用形態について

# ガイドラインにおいて想定している利用形態

**＜利用にあたっての基本的な条件（ガイドライン第7　3（5）①など）＞**

- ○提供したレセプト情報等の情報システム等への複写は、前段階でのデータが消去されない限り、原則1回のみ。この原則は、厚生労働省から提供されたレセプト情報等の元データだけでなく当該元データから作成される全ての中間生成物も含め適用される。
- ○利用・保管場所は、あらかじめ申し出られた施錠可能で入退室管理を行っているスペースのみとし、原則として持ち出されないこと。
- ○レセプト情報等を複写した情報システムはインターネット等の外部ネットワークには接続しないこと。
- ○レセプト情報等は事前に申し出られた利用者以外の者が利用してはならないため、これを担保するための情報システムの認証等の措置も必要。
- ○学部、研究室などの合理的な範囲内でガイドライン等のルールを定めた運用管理規程も必要。
- ○運用管理規程の運用状況を確認するための内部監査（自己点検）規程も必要。



# 物理的なセキュリティ要件の具体例

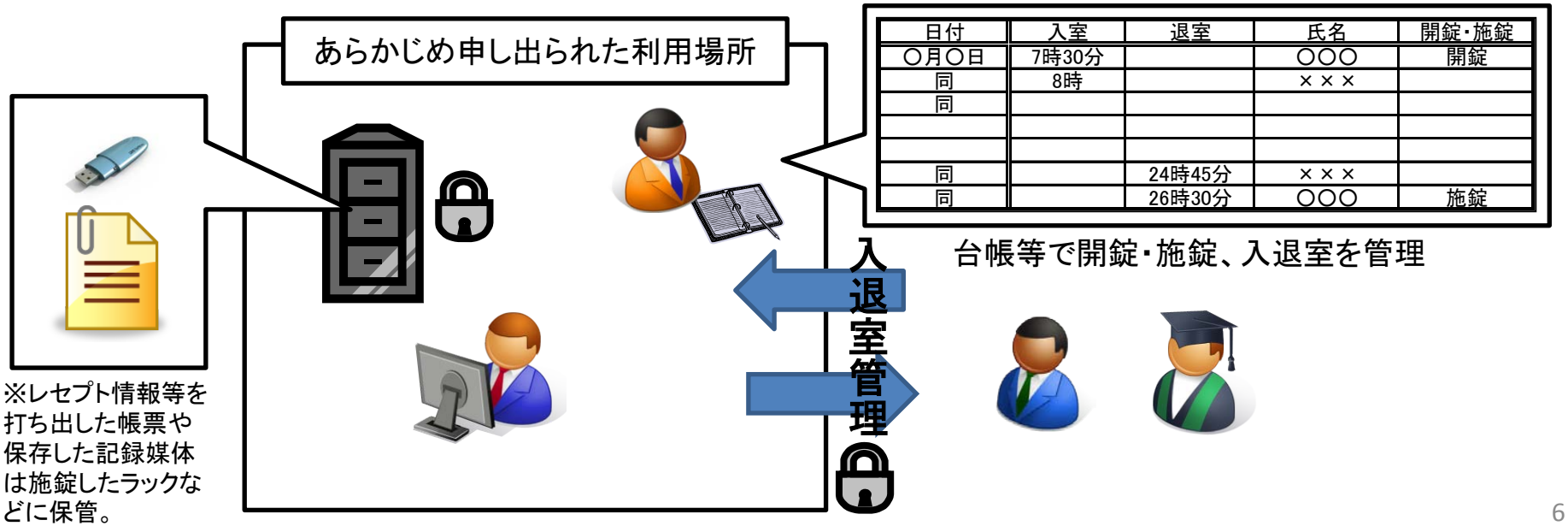
**＜入退室の管理等＞（ガイドライン第7　3（5）③（i）a)c））**

〇レセプト情報等が保存されている機器の設置場所及び記録媒体の保存場所には施錠すること。
〇レセプト情報等の物理的保存を行っている区画への入退管理を行うこと。例えば、以下のことを実施すること。
・入退者には名札等の着用を義務付け、台帳等に記入することによって入退の事実を記録する。
・入退者の記録を定期的にチェックし、妥当性を確認する。

**＜具体例＞**

※管理責任の明確化の観点から利用場所に誰が所在していたかわからない・確認できない状態となるのを防ぐことが主な目的であり、この趣旨に従う限り、必ずしも生体認証といった設備まで必要とするものではない。

〇利用場所の開錠・施錠時刻と開錠・施錠を行った者を台帳に記載する。
〇利用場所の入り口に台帳等を備え付け、担当者が入退室する者の記録を付ける。
〇紙媒体の帳票や、例外的に持ち出しを行う場合に使用するUSBなどの記録媒体があれば、それを保存するラックなどは施錠して管理する。




| 日付 | 入室 | 退室 | 氏名 | 開錠・施錠 |
|---|---|---|---|---|
| 〇月〇日 | 7時30分 | | 〇〇〇 | 開錠 |
| 同 | 8時 | | ×××| |
| 同 | | | | |
| | | | | |
| | | | | |
| 同 | | 24時45分 | ××× | |
| 同 | | 26時30分 | 〇〇〇 | 施錠 |

台帳等で開錠・施錠、入退室を管理

**＜レセプト情報等を使用する情報システムの外部ネットワークへの接続禁止＞（ガイドライン第7　3（5）①iii）など）**
○レセプト情報等を複写した情報システムは、インターネット等の外部ネットワークに接続しないこと。

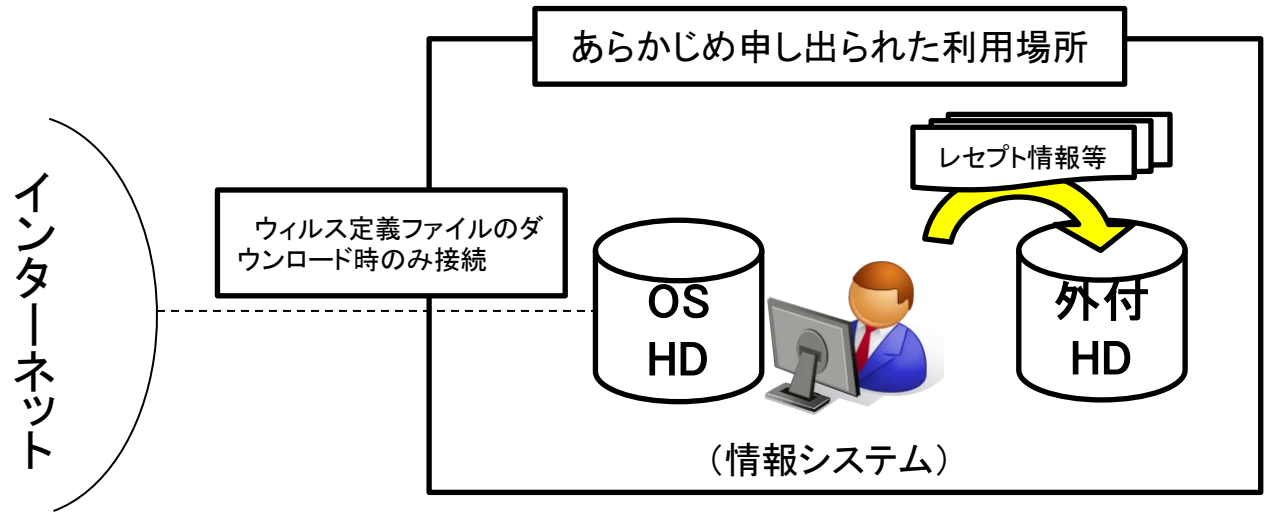
**＜具体例＞**

※外部ネットワークに接続しないため、ネットワークを介したセキュリティ対策ソフトの更新等を適時に行うことができないこととなる。この点については、ネットワークに接続しない場合であっても、例外的に共同研究者間でデータをやりとりする場合などにおいて、USBなどの外部の記録媒体を情報システムに接続する場合があり、それを介して、不正なプログラムが侵入する可能性はないとは言えないと考えられる。

この場合、ネットワークに接続せずに情報システムを使用する以上、たとえ上記のようなケースで不正なプログラムの侵入を許したとしても情報漏えい等のリスクは低いとする考え方もあるが、ゼロではないため、インターネットを通じた適切なセキュリティパッチを施すように努めることも必要と考えられる。この際には、例えば以下のような対応が考えられる。

○本ルールは、レセプト情報等が情報システム内に存在する状態で、外部ネットワークに接続する際の情報流出を避ける趣旨であることから、例えば、インターネットに接続し、セキュリティ対策ソフトの更新等を行う際には、レセプト情報等を情報システム以外の外付けハードディスク等に退避させるなどの措置が考えられる。

○また、例外として、インターネットと接続してセキュリティパッチを行うハードディスクとレセプト情報等を保存するハードディスクをあらかじめ分けておくことも考えられる。




※セキュリティパッチのために外部ネットワークに接続する場合のみ、外付ハードディスクなどにデータを一時退避。

**＜例外的に外部へ持ち出す場合の措置＞（ガイドライン第7　3（5）③iii））**

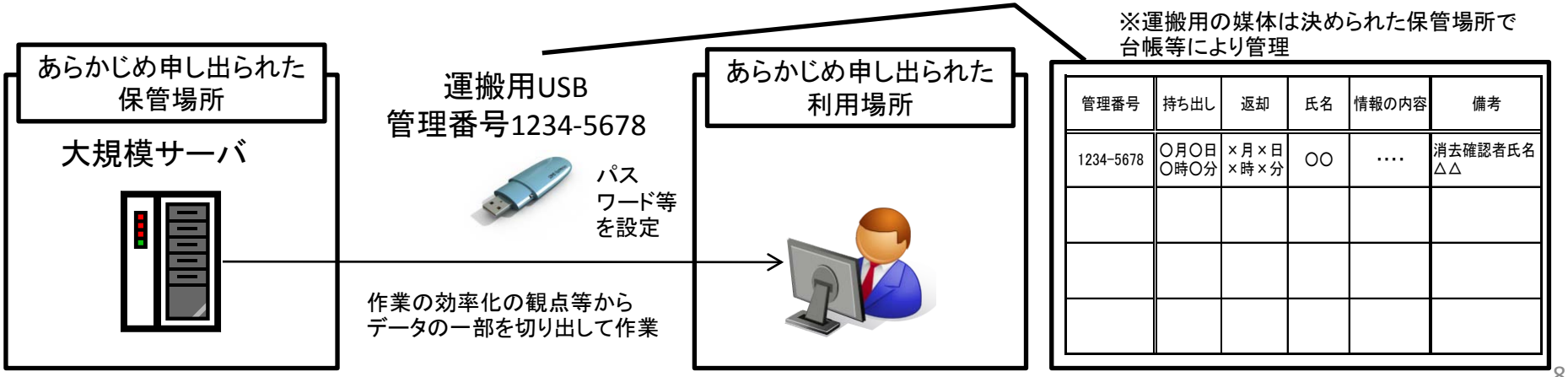
〇レセプト情報等は、事前に申し出られた利用場所から外部へは持ち出されないことを原則とするが、外部委託者や共同研究者間で中間生成物の受け渡しをする必要がある場合などに例外的に以下のような措置を講じることで持ち出しを認める。

・運用管理規程等に持ち出しについての方針やルール、持ち出した情報及び情報機器の管理方法を定める。
・持ち出した媒体が紛失した場合の対応を運用管理規程等に定める。
・レセプト情報等が保存された可搬媒体等の所在を台帳等で管理する。
・持ち出しに利用する媒体にパスワードを設定する。　　など。

**＜具体例＞**

※上記のような研究者相互間での受け渡し以外にも、例えば、本件のように扱うデータ容量が極めて大規模なために、レセプト情報等の元データを大規模なサーバに保存した上で、その一部を別の場所で利用することが考えられる。この場合、例えば以下のような措置全てを講じる等により例外を認めることが考えられる。

〇別の作業場所へレセプト情報等を運搬するUSBメモリ等には、管理番号等を付番し、台帳等で所在場所などを管理する。
〇紛失時の情報漏えい等を防ぐ観点から当該USBメモリ等には、パスワードを設定し、定期的に変更を行うなどの措置を行う。
〇紛失時の対応などをあらかじめ運用管理規程等で定める。



**＜レセプト情報等の廃棄について＞**

〇ガイドラインにおいては、レセプト情報等の利用を終了する際には、利用者は、原則として提供されたレセプト情報等を厚生労働省へ返却するとともに、公表された成果物以外の複写したレセプト情報等と全ての中間生成物を廃棄することとなっている。

〇この廃棄についても、確実にレセプト情報等（中間生成物含む）が復元不可能になっているかを担保するため、廃棄を行った者や廃棄の日時、その手法について記録をとり、厚生労働省に対してデータ措置報告書を提出する。

〇PC等に保存されたレセプト情報等を通常の操作で「削除」（ファイルをごみ箱に入れ「ごみ箱を空にする」を操作）しただけでは、単にデータが保存されている領域のインデックスが消されただけであり、ハードディスク内にデータは存在したままになるため、専用のソフトを使用することによってデータの復元が可能。

したがって市販されているデータ消去の専用ソフトを使用することにより、レセプト情報等の確実な破棄を行うことが必要。

**＜廃棄方法の例＞**

市販されているデータ消去ソフトを使用して、ハードディスクに新たなデータを上書きすることにより、レセプト情報等のデータを復元不可能にすることが必要。ただし、この場合、同一のハードディスクドライブに保存されている他の情報も全て復元不可能になるため、留意が必要。考えられるデータ廃棄の方法は以下の通り。

**①外付けハードディスクを使用**

レセプト情報等を利用するための専用の外付けハードディスクを使用し、データ消去ソフトにより破棄を行う。

**②レセプト情報等を利用するハードディスクドライブを分ける**

パソコンをフォーマットする際などに、レセプト情報等を利用するハードディスクドライブを別に設定し、そのドライブ内で作業を行い、破棄の際は、当該ドライブのみを対象として破棄を行う（より安全性を期すために、アプリケーションとレセプト情報等を利用するドライブを分けることも考えられる。）。

**③物理的にハードディスクを破壊**

確実性を期すため、ハードディスク自体にドリル等により、物理的に破壊・破砕してデータを復元不可能とする。

# ２．セキュリティマネジメントシステムの実践

# セキュリティマネジメントシステムの実践

**＜所属機関の情報セキュリティマネジメントシステムの実践＞（ガイドライン第7 （5）① ii ））**

所属機関の情報セキュリティマネジメントシステム（ISMS）の実践（必ずしもISMS適合性評価制度における認証の取得を求めるものではない。）

**＜考え方＞**

本ガイドラインが準拠している、「医療情報システムの安全管理に関するガイドライン（第4.1版）」においては、「6.2」において、安全管理を適切に行うための標準的なマネジメントシステムとして、ISO（ISO/IEC27001：2005）及びJIS（JIS Q 27001：2006）を例示している。

ISMSの実践については、必ずしも認証を求めることまではしないものの、こうした規格が示す安全管理に関する基本的な考え方としてPDCAサイクルを各機関等で適切に実践していく必要がある。

ISMSプロセスに適用されるPDCAモデルの概要

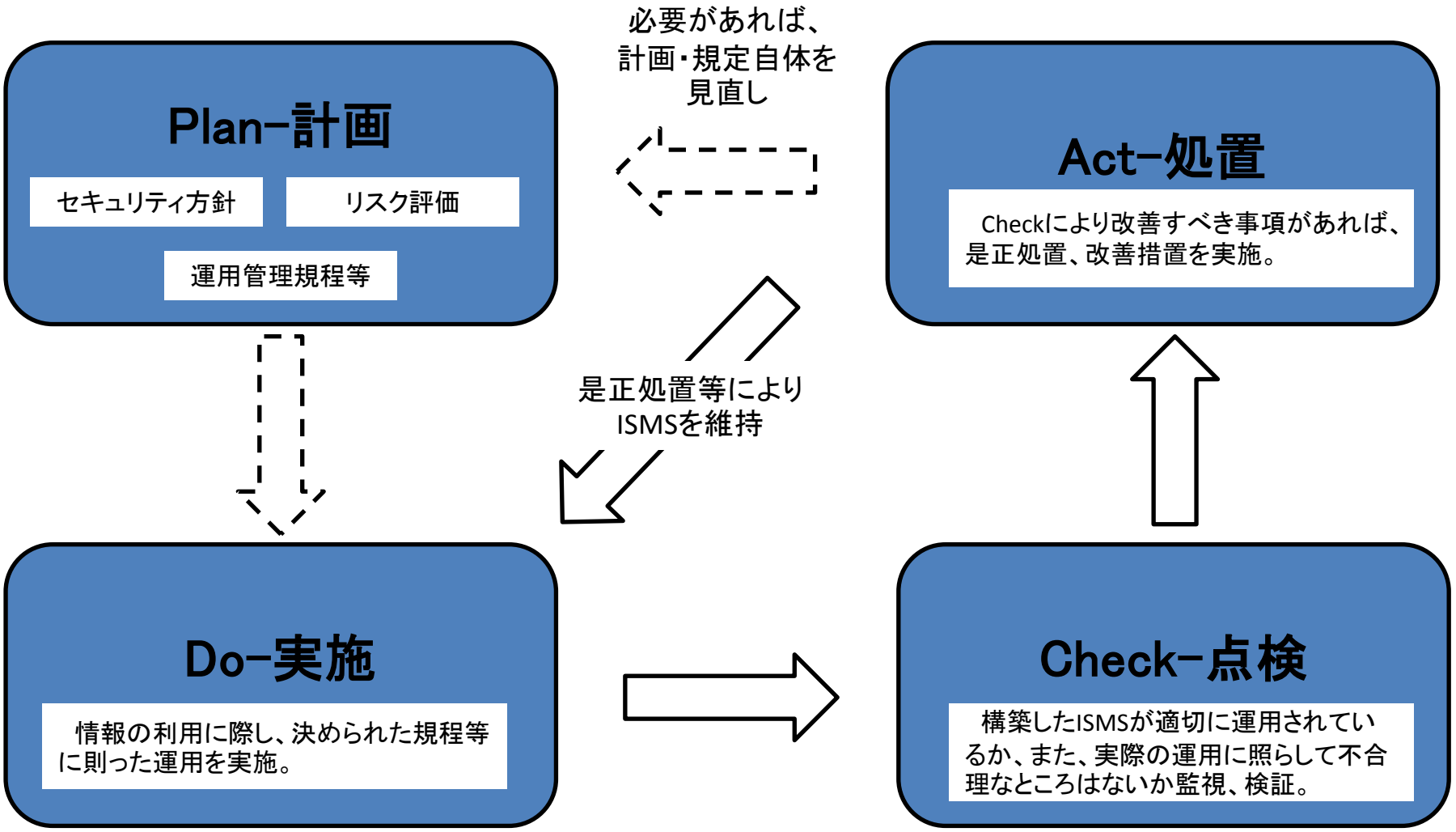
| | |
|---|---|
| Plan-計画<br>（ISMSの確立） | 組織の全般的方針及び目的に従った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連した、ISMS基本方針、目的、プロセス及び手順の確立 |
| Do-実施<br>（ISMSの導入及び適用） | ISMS基本方針、管理策、プロセス及び手順の導入及び運用 |
| Check-点検<br>（ISMSの監視及び見直し） | ISMS基本方針、目的及び実際の経験に照らした、プロセスのパフォーマンスのアセスメント（適用可能ならば測定）、及びその結果のレビューのための経営陣への報告 |
| Act-処置<br>（ISMSの維持及び改善） | ISMSの継続的な改善を達成するための、ISMSの内部監査及びマネジメントレビューの結果又はその他の関連情報に基づいた是正措置及び予防処置の実施 |

PではISMS構築の骨格となる文章（基本方針、運用管理規程等）と文章化されたISMS構築手順を確立する。
DではPで準備した文書や手順を使って実際にISMSを構築する。
Cでは構築したISMSが適切に運用されているか監視と見直しを行う。
Aでは改善すべき点が出た場合に是正処置や予防処置を検討し、ISMSを維持する。

（出典）：「医療情報システムの安全管理に関するガイドライン（第4.1版）」6.2.1

# ISMSの実践のイメージ図

〇レセプト情報等の利用にあたっては、ISMSの認証取得まで要求するものではなく、利用形態を勘案した上で、研究室、学部等の適切な範囲内で以下のようなサイクルの下にデータの適切な利用が図られる必要がある。




所属機関内の研究に直接関わらない部署が関与することが望ましい。

# Plan−計画①～適用範囲の確定～

**＜セキュリティ対策の対象範囲＞**

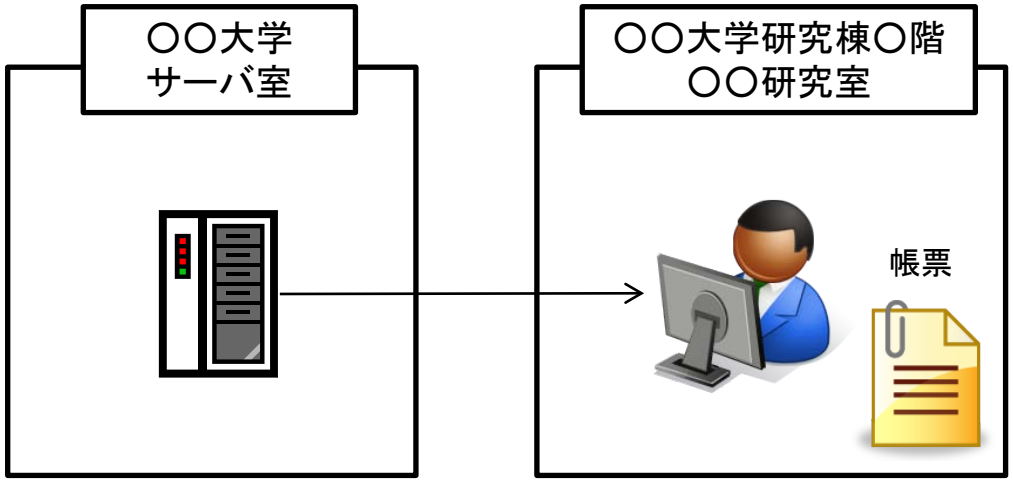
ガイドラインにおいては、第7　3（5）②として、所属機関が一般的に具備すべき条件として、ISMSの実践を挙げているが、これは、「必ずしも所属機関全体で具備する必要はなく、部、課、又は研究室等、申出者の利用形態を勘案して適切な単位で対応すること」としている。

**＜対象範囲の確定＞**

こうしたことを踏まえ、まずレセプト情報等の利用を希望する者は、自らが予定しているレセプト情報等の利用形態を勘案し、ガイドラインが求めるセキュリティ対策を適用する範囲を明確化する必要がある。

その際に、利用場所、データの保存方法を勘案し、セキュリティ対策が適用される場所や資産の範囲を特定。

（利用形態の例）




学内LANで接続

**【適用範囲】**

場所：〇〇大学サーバ室
　　研究棟〇階〇〇研究室

情報技術：
　　大学内LAN、サーバ、研究室の端末

対象となる資産：
- サーバ内のレセプト情報等のデータ
- 端末内のレセプト情報等（中間生成物含む）のデータ
- 出力した帳票

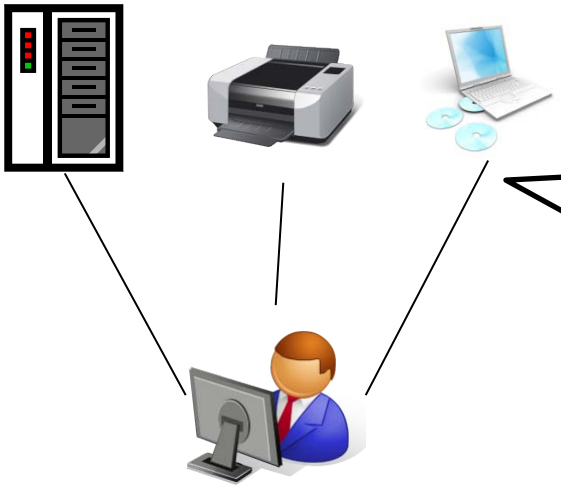
# Plan−計画②～リスク評価・分析～

**＜所属機関の情報セキュリティマネジメントシステムの実践＞（ガイドライン第7 （5）① ii ））**
※確定した適用範囲において、それぞれの情報資産毎にリスク分析を行った上で対応表を作成。
〇研究室の情報システムで扱う情報をすべてリストアップしている。
〇リストアップした情報を安全管理上の重要度に応じて分類を行い、常に最新の状態を維持。
〇リストアップした情報に対してリスク分析を行っている。

**＜具体例＞**
※必ずしもISMSの認証をとることを必要とするものではなく、利用場所における情報システムで扱う情報をそれぞれリストアップし、リスク分析を行った上で、リスクが顕在化した際の対応策をあらかじめ決めておき、所属する構成員間で共有しておくことが必要。

〇研究室で扱っている情報を全てリスト化し、以下のようにリスク値を設定し分類を行った上で対策を決定。

あらかじめ申し出られた利用場所



※利用場所の情報システムで扱うレセプト情報等をその形態毎に全てリストアップしてそれぞれリスク分析と対策をリスト化する。

| No. | 情報資産名 | 所在場所 | 運用状況 | 想定されるリスク | リスク対策 | 残存リスク | 残存リスクへの対応 |
|---|---|---|---|---|---|---|---|
| 1 | 端末内のレセプト情報等のデータ | ○○大学第○研究棟<br>○○研究室 | 当該端末で研究に係る分析<br>を実施。 | ・権限のない者による不正アクセス、漏えい<br>・情報端末の盗難、紛失<br>… | ・○○研究室の入退室管理<br>・情報端末へのアクセス時のID認証<br>・情報端末を施錠したチェーンで固定。<br>… | ・入退室のチェック漏れ<br>・IDの漏えい<br>・チェーンの施錠し忘れ<br>… | ・定期的な第三者によるチェック<br>・1ヶ月毎のID変更<br>・施錠のダブルチェック<br>… |
| 2 | レセプト情報等を出力した帳票 | ○○大学第○研究棟<br>○○研究室 | | | | | |
| 3 | レセプト情報等を保存したUSB | ○○大学第○研究棟<br>○○研究室 | | | | | |
| 4 | | | | | | | |
| 5 | | | | | | | |
| 6 | | | | | | | |

※　ISMSの規格においては、①重要度（情報漏えいの場合の影響など）、②脅威（情報漏えいの可能性の高低など）、③脆弱性（現在のリスクに対する対応状況など）の各レベル値を決め、各情報毎のリスク値を設定することが推奨されているが、レセプト情報等については、**情報の種類・想定される使用形態が限られているため、数値化までは要求しない**。

# Plan−計画③～リスク分析の例～

**＜リスク分析について＞**
医療情報システムの安全管理ガイドラインにおいては、「6.2.3　リスク分析」に、医療機関において想定される脅威の例を挙げている。

① 医療情報システムに格納されている電子データ
(a) 権限のない者による不正アクセス、改ざん、き損、滅失、漏えい
(b) 権限のある者による不当な目的でのアクセス、改ざん、き損、滅失、漏えい
(c) コンピュータウイルス等の不正なソフトウェアによるアクセス、改ざん、き損、滅失、漏えい

② 入力の際に用いたメモ・原稿・検査データ等
(a) メモ・原稿・検査データ等の覗き見
(b) メモ・原稿・検査データ等持ち出し
(c) メモ・原稿・検査データ等のコピー
(d) メモ・原稿・検査データの不適切な廃棄

③ 個人情報等のデータを格納したノートパソコン等の情報端末
(a) 情報端末の持ち出し
(b) ネットワーク接続によるコンピュータウイルス等の不正なソフトウェアによるアクセス、改ざん、き損、滅失、漏えい
(c) ソフトウェア（Winny 等のファイル交換ソフト等）の不適切な取扱いによる情報漏えい
(d) 情報端末の盗難、紛失
(e) 情報端末の不適切な破棄

④ データを格納した可搬媒体等
(a) 可搬媒体の持ち出し
(b) 可搬媒体のコピー
(c) 可搬媒体の不適切な廃棄
(d) 可搬媒体の盗難、紛失

⑤ 参照表示した端末画面等
(a) 端末画面の覗き見

⑥ データを印刷した紙やフィルム等
(a) 紙やフィルム等の覗き見
(b) 紙やフィルム等の持ち出し
(c) 紙やフィルム等のコピー
(d) 紙やフィルム等の不適切な廃棄

⑦ 医療情報システム自身
(a) サイバー攻撃によるIT 障害
・ 不正侵入
・ 改ざん
・ 不正コマンド実行
・ 情報かく乱
・ ウイルス攻撃
・ サービス不能（DoS：Denial of Service）攻撃
・ 情報漏えい 等
(b) 非意図的要因によるIT 障害
・ システムの仕様やプログラム上の欠陥（バグ）
・ 操作ミス
・ 故障
・ 情報漏えい 等
(c) 災害によるIT 障害
・ 地震、水害、落雷、火災等の災害による電力供給の途絶
・ 地震、水害、落雷、火災等の災害による通信の途絶
・ 地震、水害、落雷、火災等の災害によるコンピュータ施設の損壊等
・ 地震、水害、落雷、火災等の災害による重要インフラ事業者等におけるIT の機能不全

これらの脅威に対し、対策を行うことにより、発生可能性を低減し、リスクを実際上問題のないレベルにまで小さくすることが必要になる。

# Plan-計画④～運用管理規程等の作成～

**＜リスク分析を踏まえたセキュリティ対策についての運用管理規程等の作成（ガイドライン第7　3（5）②iii））＞**

　ガイドラインにおいては、これまでの情報資産毎のリスク分析を踏まえたセキュリティ対策を担保するための、ガイドラインの各項目の内容を担保する運用管理規程等を作成し、対象の範囲に含まれる職員間で周知・徹底することにより、レセプト情報等の利用にあたってのセキュリティ対策に万全を期す必要がある。

| 運用管理規程に規定すべき項目 | 規定すべき内容 |
|---|---|
| 理念（基本方針と管理目的の表明） | セキュリティ対策の全体的な基本方針・目的の明確化 |
| 利用者等の体制 | 実際にレセプト情報等を利用する者の体制を記載。 |
| 契約書・マニュアル等の文書の管理 | レセプト情報等の利用に当たり、一部の利用者が外部委託先である場合など、レセプト情報等の利用に当たり交わした契約書・マニュアル等がある場合には、その管理方法について記載。 |
| リスクに対する予防、発生時の対応の方法 | レセプト情報等の形態（データ、帳票、電子媒体など）毎に、想定される情報漏えい等のリスクを分析し、それに対する対応方法について記載。<br>また、こうした対応方法を実施したことについての記録を残すこととし、その手順を規定。 |
| 機器を用いる場合は機器の管理 | レセプト情報等の利用に当たり、使用する情報システム等の機器（PC、サーバーなど）の管理方法（ID認証、持ち出し防止など）を記載。 |
| 個人情報の記録媒体の管理（保管・授受等）の方法 | 仮にレセプト情報等の利用に当たり、USB等の記録媒体を用いる場合には当該記録媒体の管理方法（台帳管理、使用後のデータの削除）を記載。 |
| 監査 | 運用管理規程に定められた内容の実施が担保されているか所属機関内で監査を行う場合の監査の実施主体、方法など。 |
| （苦情・質問の受付窓口） | レセプト情報等の提供先は原則として公開されるため、外部から問い合わせがあった場合に対応する者を想定していることが望ましい。 |

# Do−実施～セキュリティ対策の実践～

**＜セキュリティ対策の実践＞**

決定した運用管理規程等のルールを各レセプト情報等の利用者に周知・徹底し、実際の利用に際して、決められたセキュリティ対策が確実に実践される必要がある。

**＜利用者全員への周知・徹底＞**

レセプト情報等の利用者のうち、その研究活動の責任者にあたる者は、利用者全員に策定した運用管理規程等を周知・徹底し、その実践を求める。

仮に利用者の中に、外部委託先等（当該責任者の所属機関以外の機関に所属する者）がいる場合には、その外部委託先等においても、合理的な範囲内で運用管理規程を策定し、遵守させることとする。

**＜セキュリティ対策の運用の記録＞**

最終的に、運用管理規程等に定めるセキュリティ対策の実施状況について、厚生労働省による監査又は、内部監査等により評価を行うことが重要であることから、定められたセキュリティ対策の実施状況について記録を残しておくことが重要。

【例】

・入退室管理などの実施の記録

・USB等の記録媒体を使用する場合には、台帳管理が行われていたかどうかの記録、

・リスクが発生した場合に想定しておいた対応を図ったかどうかの記録

など。

**＜セキュリティ対策の有効性の評価＞**

レセプト情報等の利用者自らがあらかじめ定められた運用管理規程を実践できているか、又は、規程自体に不合理なところや実態に合わないところがないか、様々な場面で評価を行っていくことも重要。

# Check−点検～監査による見直し～

**＜厚生労働省による監査又は内部の監査の実施（ガイドライン第１３　２）＞**

ガイドライン等においては、厚生労働省は必要に応じて、レセプト情報等の利用場所への立ち入りを求めることができ、利用者はその立ち入りを認めなければならないこととなっている。

また、厚生労働省は立ち入り監査に代えて、提供依頼申出者に対して管理状況報告書の提出を求めることができることとなっており、利用者等は、厚生労働省から求められた場合は、内部監査を実施した上で管理状況報告書の提出をしなければならない。

**＜監査体制の設定・実践＞**

定められたセキュリティ対策の実施状況やその合理性を検証するため、利用者が所属する機関の職員によって内部監査が行われることが必要。監査は、利用者以外の職員であって、所属機関内の異なる部局に所属する職員によって行われることが望ましい（例えば、所属機関のセキュリティを担当している部局）。

**＜内部監査の実施方法の策定＞**

主に以下のような内容の事項をあらかじめ決定し、これに従って内部監査が行われることが重要。

〇内部監査を実施する者・体制・計画
〇内部監査の実施方法（評価方法など）
〇監査結果の報告形式
〇監査に基づく是正対応の内容　など

# ISMSの実践のまとめ

○　これまで述べたことを確実に実践するため、レセプト情報等の提供依頼を申し出る者は、以下の書類を作成し、必要な体制を整備した上でレセプト情報等の利用にあたる必要がある。
（必ずしも書類の形式はこの通りである必要はなく、必要な事項が不足なく記述されていることが重要）

○　また、レセプト情報等の有識者会議の議論も踏まえ、有識者会議の審査終了後、レセプト情報等を実際に提供する前までに厚生労働省が実地監査を行うか、又は利用者において内部監査（自己点検）を行った上で、そのガイドラインの適用宣言書を提出することとする。

| 書類 | 規定内容 |
|---|---|
| ①実施フロー図 | どのようにレセプト情報等の分析を行うか、業務フロー図を作成。（作業を行う場所、保存場所など） |
| ②リスク分析・対応表 | レセプト情報等の形式（データ、帳票、電子媒体）や利用方法に応じたリスク分析とそれへの対応をリストアップしたもの。 |
| ③運用管理規程 | ①で記載されたリスク対応方法を担保するためにレセプト情報等の利用者が遵守すべきルール・運用するための様式（入退室管理簿の様式など）を規程。 |
| ④内部監査（自己点検）規程 | ②の運用管理規程が適切に遵守されているかを内部監査する際の監査実施者、方法などを記載。 |

# （参考）申出書の添付書類の例

# （参考例）

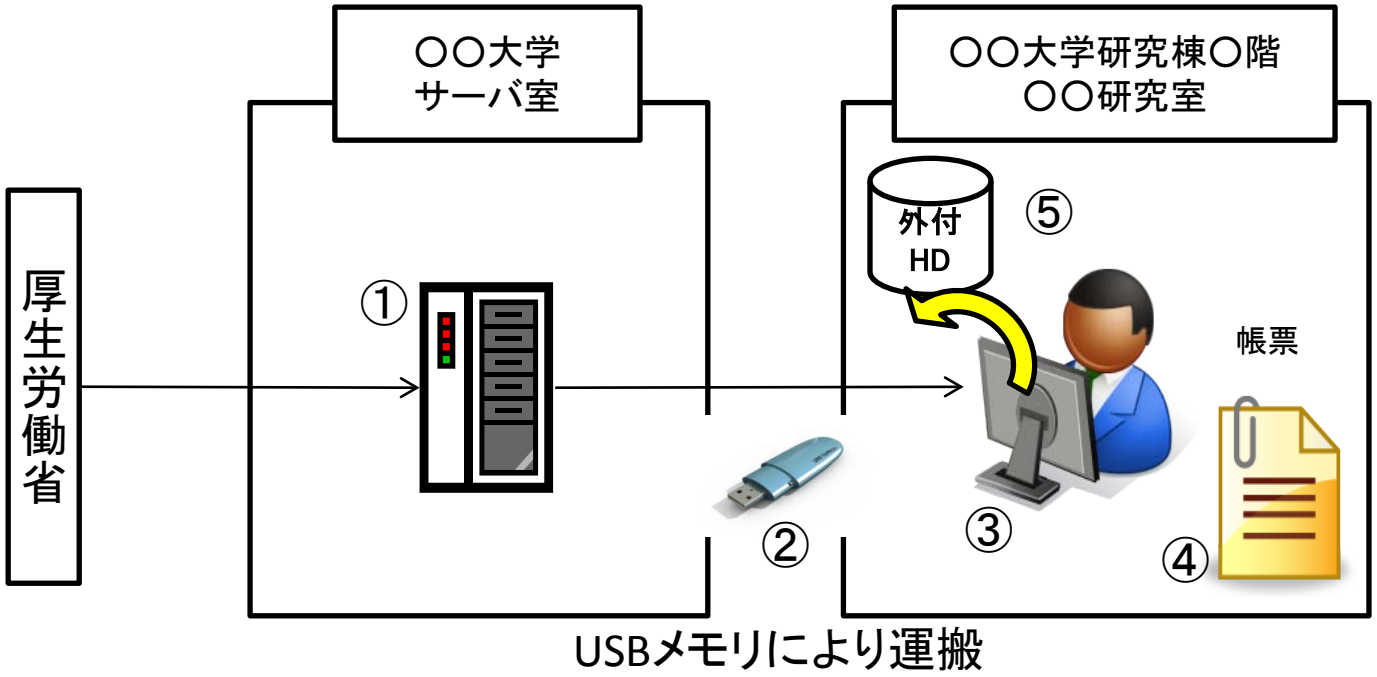
**＜具体的な記載方法＞**

レセプト情報等の提供依頼申出に当たり、添付する必要のあるセキュリティ対策関係の書類の記載方法について、以下のような利用形態を想定した上で、具体例を提示する。

**＜想定する利用形態＞**

〇レセプト情報等の利用者は1名。
〇厚生労働省から提供を受けたレセプト情報等を大学の学内のサーバー室のサーバーに保存。
〇サーバーから一部のデータを切り出してUSBメモリーで研究室の情報端末に複写し、分析を実施。
〇作成した中間生成物は、帳票として一部紙媒体で出力し、分析。
〇データの滅失などの不測の事態に備えるため、外付けハードディスクに定期的に中間生成物を保存。
※提供するデータ容量が極めて大きいことにより、一旦大規模サーバに保存する必要があるなどの事由により、提供したレセプト情報等の複写1回の原則の例外が認められているケースと仮定。

**【実施フロー図の例】**




※本ケースにおけるレセプト情報等の形態は5パターン。

①サーバー内の電磁的データ
②研究室へ運ぶ際のUSBメモリ内のデータ
③研究室の端末内に保存された電磁的データ
④中間生成物を打ち出した帳票
⑤中間生成物のバックアップを保存した外付けハードディスク

# リスク分析・対応表（例）

実施フロー図の中で想定されている5つのパターンのレセプト情報等の形態毎に想定されるリスクとそれへの対策等をリスト化し、利用者間で周知・徹底する。

| | 情報資産名 | 所在場所 | 運用状況 | 想定されるリスク | リスク対策 | 残存リスク | 残存リスクへの対応 |
|---|---|---|---|---|---|---|---|
| ① | サーバー内に電磁的に保存されているレセプト情報等のデータ | ○○大学サーバ室 | データが大規模なため、レセプト情報等を当該サーバに保存。 | ・権限のない者による不正アクセス、漏えい | ・サーバ室の施錠と大学の○○課による入退室管理<br>・サーバを施錠したラックに格納し、サーバ室に入室した他部局の人間によるアクセスも防止。 | ・入退室のチェック漏れ<br>・ラックの施錠忘れ | ・2週間に1度、定期的に入退室管理やサーバーラックの施錠状況等を確認 |
| ② | 研究室に運ぶ際のUSB内のレセプト情報等のデータ | ○○大学○○研究室 | サーバに保存したレセプト情報等から分析のため一部切り出したデータを○○研究室へ運搬。 | ・USBの盗難、紛失による漏えい | ・台帳によるUSBの使用状況の管理<br>・USBにパスワードを設定。<br>・使用後のUSB内データを専用ソフトで初期化<br>・使用した後は○○研究室内の施錠した戸棚にUSBを保管 | ・台帳への記入忘れ<br>・パスワードの設定忘れ<br>・USB使用後のデータ消去忘れ<br>・戸棚の施錠忘れ | ・2週間に1度の管理状況の確認（USB内の情報や戸棚の施錠状況など含む）<br>・定期的なパスワード設定の変更 |
| ③ | ○○研究室の端末内のレセプト情報等のデータ | ○○大学○○研究室 | 厚労省から提供されたレセプト情報等の大規模データから一部を切り出して分析 | ・端末の盗難、紛失による漏えい<br>・端末内への不正アクセスによる漏えい | ・○○研究室について、入退室管理<br>・持ち運びできないよう端末について施錠したチェーンにより固定。<br>・端末にIDとパスワードを設定し、アクセスを制限<br>・インターネット等の外部ネットワークに接続しない。 | ・入退室のチェック漏れ<br>・チェーンの施錠忘れ<br>・ID・パスワードの漏えい・設定忘れ | ・2週間に1度の管理状況の確認<br>・定期的なパスワード設定の変更 |

| | 情報資産名 | 所在場所 | 運用状況 | 想定されるリスク | リスク対策 | 残存リスク | 残存リスクへの対応 |
|---|---|---|---|---|---|---|---|
| ④ | レセプト情報等の中間生成物を打ち出した帳票 | ○○大学<br>○○研究室 | 端末で作成した中間生成物を紙媒体の帳票で出力し分析を実施。 | ・帳票の盗難、紛失 | ・帳票は1枚毎に番号を振り、台帳管理。<br>・使用後は施錠した専用の戸棚に保管。<br>・利用後は速やかにシュレッダーで裁断し廃棄。 | ・台帳への記載漏れ<br>・戸棚の施錠忘れ | ・2週間に1度、定期的な管理状況の確認。 |
| ⑤ | レセプト情報等の中間生成物を保存した外付けハードディスク | ○○大学<br>○○研究所 | 端末で作成した中間生成物についてバックアップを外付けハードディスクに保存。 | ・ハードディスクの盗難、紛失 | ・○○研究室について、入退室管理<br>・持ち出されないように使用後は施錠した専用の戸棚に保管。 | ・入退室のチェック漏れ<br>・戸棚の施錠忘れ | ・2週間に1度の管理状況の確認<br>・1日に1度のハードディスクの所在確認 |

○ここで記載した表は例であり、実際の審査での了承を保証するものではない。

○セキュリティ対策については、別途、「情報セキュリティ自己点検リスト」を配付しており、リスク分析・対応表におけるリスク対策が、この「情報セキュリティ自己点検リスト」の各項目に対応している必要がある。
（利用形態を勘案して、情報セキュリティ自己点検リストに記載されている各項目を満たす必要がないと申出者が判断する場合には、その理由を明記する必要。）

# 運用管理規程（例）

**レセプト情報等の利用に当たっての運用管理規程**

平成23年〇月〇日　〇〇大学〇〇研究室

**1．目的**

厚生労働省から提供を受けたレセプト情報等の利用者が、情報セキュリティと個人情報保護の観点から遵守すべき事項を規定するものである。

**2．適用範囲**

厚生労働省から提供を受けたレセプト情報・特定健診等情報のデータとそれから派生する全ての中間生成物を対象とし（これらを「レセプト情報等」という）、別紙に定める業務、部局、情報技術等に適用するものとする。

**3．運用管理**

（1）利用者

レセプト情報等の利用者は、〇〇のみとし、その他の者は、レセプト情報等にアクセスしてはならない。

（2）利用・保管場所のアクセス制限

・レセプト情報等の利用場所は、〇〇大学〇〇研究室のみとし、サーバ室から〇〇研究室へデータを運搬する場合を除き、この他の場所での利用は行わない。

・レセプト情報等の保管場所は、サーバ室及び〇〇研究室とする。

・サーバ室については、〇〇大学が別途、定めている「〇〇セキュリティ方針（別添）」に則り、〇〇大学〇〇課による入退室管理を行い、権限のない者の入室を認めない。

・〇〇研究室については、原則として〇〇と研究室の構成員××及び△△のみが入室できることとする。研究室は、入退室管理を行い、入室した者の氏名、入退室した時刻、施錠・開錠時刻を記録し、最後に退室する者が必ず研究室に施錠を行うこととする。

（3）利用・保管方法

・〇〇研究室においては、PC（注：管理番号・型番等の端末を特定する情報が必要）内への保存又は打ち出した帳票によるデータの保存以外の方法によるレセプト情報等の保管は行わない。

・PCには個人IDとパスワードを設定し、〇〇以外の者がアクセスできないこととし、パスワードについては、1ヶ月に1度変更を行わなければならない。また、窃視を防止するため、パスワード付のスクリーンセーバーを設定すること。
・PCはインターネット等の外部ネットワークには接続してはならない。また、台帳管理しているUSB等の記録媒体以外の記録媒体を接続してはならない。
・PCは持ち出しを防止するため、施錠したチェーンによって固定すること。
・レセプト情報等を打ち出した帳票は、１枚毎に番号を振り、台帳に記録し管理すること。紛失を防止するため、利用後は必ず、〇〇研究室内の戸棚に保管し、施錠すること。

（4）データの持ち出しについて
・公表される成果物以外のレセプト情報等については、サーバ室から〇〇研究室への運搬を行う場合以外、この2つの場所から持ち出してはならない。
・サーバ室から〇〇研究室への運搬には、USBメモリ（注：特定のため管理番号等を設定する必要）を使用し、使用日時、使用目的、使用後のデータ消去の有無を台帳で管理すること。使用していない時は、〇〇研究室内の戸棚に保管し、施錠すること。

（5）データの返還・廃棄
・レセプト情報等の利用後は、厚生労働省から提供を受けた媒体とそこに保存されたレセプト情報等については、厚生労働省へ返還する。それ以外のサーバー内、PC内に保存されたレセプト情報等及び打ち出された帳票については、確実に廃棄すること。
・サーバー内及びPC内に保存されたレセプト情報等については、市販ソフトにより、物理的フォーマットを行うこと。
・帳票については、シュレッダーにより裁断した上で廃棄すること。

（6）機器の保守
・レセプト情報等の利用期間中に、サーバ及びPCの保守を行う場合には、保守を行う者と保守契約を締結し、機密保持の義務を課すこと。また、保守はオンサイトで行うこととし、サーバ室又は〇〇研究室内で行われなければならない。
・原則として、サーバの保守の場合は〇〇大学の〇〇課の職員が、PCの保守の場合は、〇〇、〇〇研究室の××又は△△が保守作業に立ち会うこと。

（7）運用状況の記録・保存

・本規程に定める運用が適切に行われているか確認できるようにするため、入退室管理等の運用状況について適切に記録する。

・サーバ室及び〇〇研究室の入退室記録並びにUSBメモリの管理台帳の記録に関しては、レセプト情報等の利用期間終了後、１年間保存すること。

・PCへのアクセスログは、レセプト情報等の利用期間終了後、１年間保存すること。

・レセプト情報等を廃棄した場合には、廃棄した日時、廃棄した者、廃棄場所、廃棄方法を記録し、レセプト情報等の利用期間終了後、１年間保存すること。

（8）緊急時の事業継続等

・大規模災害等の不測の事態により、レセプト情報等の紛失、漏えい等があった場合には速やかに厚生労働省へ連絡し、事後の対応を協議すること。

・また、予期せぬデータの滅失による研究事業の遅滞、中断等の事態を避けるため、中間生成物については、定期的にバックアップをとり、外付けハードディスクに保存すること。

**４．内部監査**

本規程に定める運用が適切に行われているか確認することを目的として、「レセプト情報等の利用に当たっての内部監査（自己点検）規程」を作成する。

厚生労働省から、利用状況についてレセプト情報等の利用規約に定める管理状況報告書の提出を求められた場合には、速やかに当該内部監査（自己点検）規程に従った監査を行い、その結果を厚生労働省へ報告する。

**５．外部からの問い合わせ**

レセプト情報等の利用にあたっては、国民の理解を得ることが重要であるため、当該利用について外部から問い合わせがあった場合には、原則として〇〇研究室の××が対応することとする。

〇ここで記載した表は例であり、実際の審査での了承を保証するものではない。

〇この例では、サーバ室は、〇〇研究室ではなく、大学全体のセキュリティを担当している部署が管理責任を有していることを前提としている。

（別紙）運用管理規程の適用範囲

| | 分　類 | 対　象 | 内　容 | 関連文書 |
|---|---|---|---|---|
| 1 | 適用業務 | レセプト情報等を利用した学術研究 | 厚生労働省から提供を受けたレセプト情報等を利用して行う〇〇に関する分析・研究事業 | 提供依頼申出書<br>運用管理規程 |
| 2 | 適用組織 | 〇〇大学〇〇課 | レセプト情報等の大規模データを保存するサーバが所在するサーバ室の管理業務 | 業務フロー図 |
| | | 〇〇大学〇〇研究室 | レセプト情報等を用いた分析業務 | 業務フロー図 |
| 3 | 場所 | 〇〇大学△△棟2階<br>サーバ室 | レセプト情報等の大規模データを保存するサーバ室 | 業務フロー図 |
| | | 〇〇大学××棟6階<br>〇〇研究室 | レセプト情報等を利用した分析を実施 | 業務フロー図<br>入退室管理台帳 |
| 4 | 情報技術 | ネットワーク | インターネット等の外部ネットワークとは接続していない。 | 業務フロー図 |
| 5 | 情報資産 | サーバ室のサーバ | レセプト情報等の大規模データを保存。 | 業務フロー図<br>〇〇課の管理規程 |
| | | 〇〇研究室の端末 | 実際のレセプト情報等の分析に使用。 | 業務フロー図<br>管理台帳 |
| | | 〇〇研究室のUSBメモリ | サーバ室から〇〇研究室へ運搬する際に使用 | 業務フロー図<br>管理台帳 |
| | | 〇〇研究室の帳票 | 中間生成物の一部を紙媒体として打ち出して使用。 | 業務フロー図<br>管理台帳 |
| | | 〇〇研究室の外付けハードディスク | 中間生成物の一部をバックアップとして保存。 | 業務フロー図 |

# 内部監査（自己点検）規程（例）

※　運用管理規程で定められたセキュリティ対策が適切に実施されているか判断するためには、利用者とは別の者（例えば、大学のセキュリティを担当している部署の職員）が行うことが望ましいが、ここでは利用者本人が行う場合の例を記載。

**レセプト情報等の利用についての自己点検規程**

平成23年〇月〇日〇〇大学〇〇研究室

**１．目的**

この規程は、厚生労働省から提供されたレセプト情報等の利用について、運用管理規程に定める運用が適切に実施されているか確認するための方法、確認を行う者をさだめることを目的とする。

**２．自己点検の実施者**

〇〇大学の〇〇（レセプト情報等の利用者）が、本規程の定める点検を行うこととし、〇〇研究室の××がその実施に立ち会うこととする。

**３．点検の方法**

（1）利用場所・保管場所のアクセス制限

〇〇は、〇〇研究室の××及び△△から研究室への入退室状況を聴取し、入退室管理を行っている台帳と照らし合わせることにより、適切に記録がなされているか確認を行う。

サーバ室については、〇〇大学の〇〇課の担当職員から入退室管理の状況を聴取し、確認を行う。

（2）利用・保管方法

・研究室内のPCが施錠されたチェーンで固定されていることを確認する。
・使用していないUSBメモリは、所定の場所に保管され、内部に何もデータが保存されていないことを確認する。
・少なくとも数個の実在するウェブサイトにアクセスを試み、インターネット等の外部ネットワークに接続していないことを確認する。
・PCの端末のアクセスログと入退室の管理記録、USBメモリ及び帳票の管理台帳と照合し、齟齬がないことを確認する。

・帳票の所在場所を確認し、適切に保存がなされていること、又、使用していない帳票がないことを確認する。

（3）機器の保守
・レセプト情報等の利用期間内にサーバ室及びPCの保守が行われるか確認する。
・行われる場合には、保守を行う者との間で運用管理規程に沿った保守作業（オンサイトによる保守、機密保持条項）が行われることが契約上、明記されているか確認する。

（4）利用者以外の者への周知確認
・日常的に〇〇研究室に出入りする××及び△△については、運用管理規程の内容を適切に把握しているか、聴取して確認をする。

**4．点検結果の記録**
〇〇は、本規程の点検を行った日、時間を記録し、レセプト情報等の利用期間終了後、1年間保存すること。

〇ここで記載した表は例であり、実際の審査での了承を保証するものではない。

# 適用宣言書（例）

今まで述べてきた規程等に記載されたルールにより、ガイドラインに記載されたそれぞれの項目が満たされていることを「情報セキュリティ自己点検リスト」でチェックし、利用前に以下のような適用宣言書を厚生労働省へ提出することで実際のレセプト情報等の提供を受けることとなる。

（注）この措置は、申出者が申し出る段階では必ずしもセキュリティ要件を満たした体制を整えておらず、審査で了承されたことを以て、大学等の所属機関と交渉し、所要の体制を整備することも考えられるため、必要な体制の整備の確認はレセプト情報等の提供の直前に行うことが重要であるとの考え方による。

厚生労働大臣　殿

レセプト情報・特定健診等情報の提供に関するガイドラインの適用宣言書

平成23年〇月〇日
〇〇大学〇〇学部〇〇研究室　教授　〇〇

私は別紙の「情報セキュリティ自己点検リスト」に記載したとおり、レセプト情報等の利用にあたり必要となる情報セキュリティ対策を担保するための諸規程と必要となる体制を整備しましたので、その旨を宣言します。