資料1

レセプト情報・特定健診等情報の提供について

平成24年３月21日

厚生労働省保険局総務課

【目次】

1．データベースの概要

レセプト情報・特定健診等情報データベースの構築の経緯

1．平成18年医療制度改革

→高齢者の医療の確保に関する法律・成立 （平成20年4月施行）
→医療費増加の構造的要因に着目し、中長期的な観点から医療費適正化を進める医療費適正化計画の枠組みの導入
→医療費適正化計画の作成、実施及び評価に資するため、厚生労働省が行う調査及び分析等に用いるデータベースの構築へ
※保険者は、厚生労働省に対し、必要な情報を提供

2．「医療サービスの質の向上等のためのレセプト情報等の活用に関する検討会」

○平成１９年７月　　検討開始
→収集するデータの範囲、データの利活用の方法等について検討

○平成２０年２月　　報告のとりまとめ（情報提供の基本的枠組み）

---（**検討会報告を踏まえ、データ収集のための体制の構築**）---

3.「レセプト情報等の提供に関する有識者会議」

○平成22年10月～
→平成20年の検討会報告を踏まえ、「レセプト情報等の提供に関する有識者会議」を立ち上げ。この有識者会議の議論を経て、23年3月末にデータ提供の具体的なルールを定めたガイドラインを制定。23年11月に第1回目の審査で6件の申出を承諾。

（参考）「医療サービスの質の向上等のためのレセプト情報等の活用に関する検討会」（抄）
（平成20年2月７日）

４　国が行う分析の目的に関する考え方

(1)　医療費適正化計画の作成等に資する調査・分析を行うことが、高齢者医療確保法第１６条に基づきレセプトデータ及び特定健診等データを収集する一義的な目的である。

(2)　上記(1)の分析以外であっても、当該データを活用することが、新たに別途データを収集することと比較考量すれば、国民負担の軽減につながり、また迅速な分析、的確・適切な施策の迅速な実施により、行政サービスの向上、行政運営の効率化につながる場合もあると考えられる（例えば、感染症などの疾患の実態把握に基づく施策や、介護給付費と医療費の実態把握に基づく施策など）。
このため、所掌事務の遂行に必要な範囲内であることを前提とした上で、上記(1)の分析のほかにも、当該データの分析・活用が、上記(1)の分析目的と同様に、医療サービスの質の向上等を目指して正確なエビデンスに基づく施策を推進するに当たっての必要かつ有利となる場合についても、国が行う分析の目的に含めて考えることも必要と考えられる。

６　国以外の主体によるレセプトデータ等の活用のあり方

(2)　上記4(2)に示したような考え方を前提とするならば、国以外の主体が、国が収集したレセプトデータ及び特定健診等データを用いて、医療サービスの質の向上等を目指して正確なエビデンスに基づく施策を推進するに当たって有益となる分析・研究、学術研究の発展に資するような研究を行うことを一律に排除することは、国民負担の軽減、的確・適切な施策の迅速な実施という視点に立てば、かえって適切とは言えないと考えられる。
したがって、上記(1)により都道府県が活用する場合のほか、国以外の主体がこうした公益目的で国の収集データの提供を受けて分析・研究し、国において施策を検討する際にその分析・研究の成果を活用できるような仕組みも必要と考えられる。
　ただし、その際には、以下の点について十分留意する必要がある。

①　データの利用目的として公益性の確保が必要であることのほか、研究目的や研究計画、データの分析方法、データの使用・管理方法等について、個別に審査した上で、当該研究に必要な範囲内でデータを提供すること。

②　個別ケースごとの審査に当たって、公平・中立な観点から、データ利用の目的や必要性等について審査し、提供の可否等を決定する仕組みが必要であること。

③　個別ケースごとの審査の基準となる、第三者への提供に係る具体的なルールが別途必要であること。
当該ルールづくりに当たっては、新統計法における調査票情報等の利用及び提供のルール（現在総務省及び内閣府統計委員会において検討中）も踏まえて検討する必要があること。

④　上記③のルールに基づき国から適切にデータの提供を受けた者以外の者が、結果的に当該提供データをそのまま利用することのないよう徹底すること。
また、この点についても上記③のルールの中で必要な措置を講じておくこと。

⑤　レセプトデータ及び特定健診等データには、患者の病名等慎重に取り扱うべきデータが含まれていること等にかんがみ、上記③のルールに基づいて国がデータを提供する際にも、収集データをそのままの形で提供することは適当ではなく、当該データの一部（例えば患者等について原則として同一人物に同一に付される一連の番号、医療機関・薬局コード、一部の病名など）を加工するなどの対応が別途必要であること。
この場合の対応方針についても、上記③のルールの中でできるだけ明確に整理しておく必要があること。

レセプト情報・特定健診等情報データベースの利用

高齢者医療確保法に基づく利用

厚生労働省保険局総務課
医療費適正化対策推進室

都道府県

医療費適正化計画の作成等
のための調査及び分析等

国による分析等

結果の公表

国が公表する結果のほか、都道府県が、国に対し、医療費適正化計画の評価等に必要な情報の提供を要請し、入手

都道府県による分析等

左記目的以外の利用

厚生労働省内の他部局、他課室
関係省庁・自治体

医療サービスの質の向上等を目指した正確なエビデンスに基づく施策の推進

○感染症などの疾患の実態把握に基づく施策
○介護給付費と医療費の実態把握に基づく施策　　等

※所掌事務の遂行に必要な範囲内であることが前提

左記以外の主体
（研究機関等）

○左記のような施策に有益な分析・研究
○学術研究の発展に資する目的で行う分析・研究

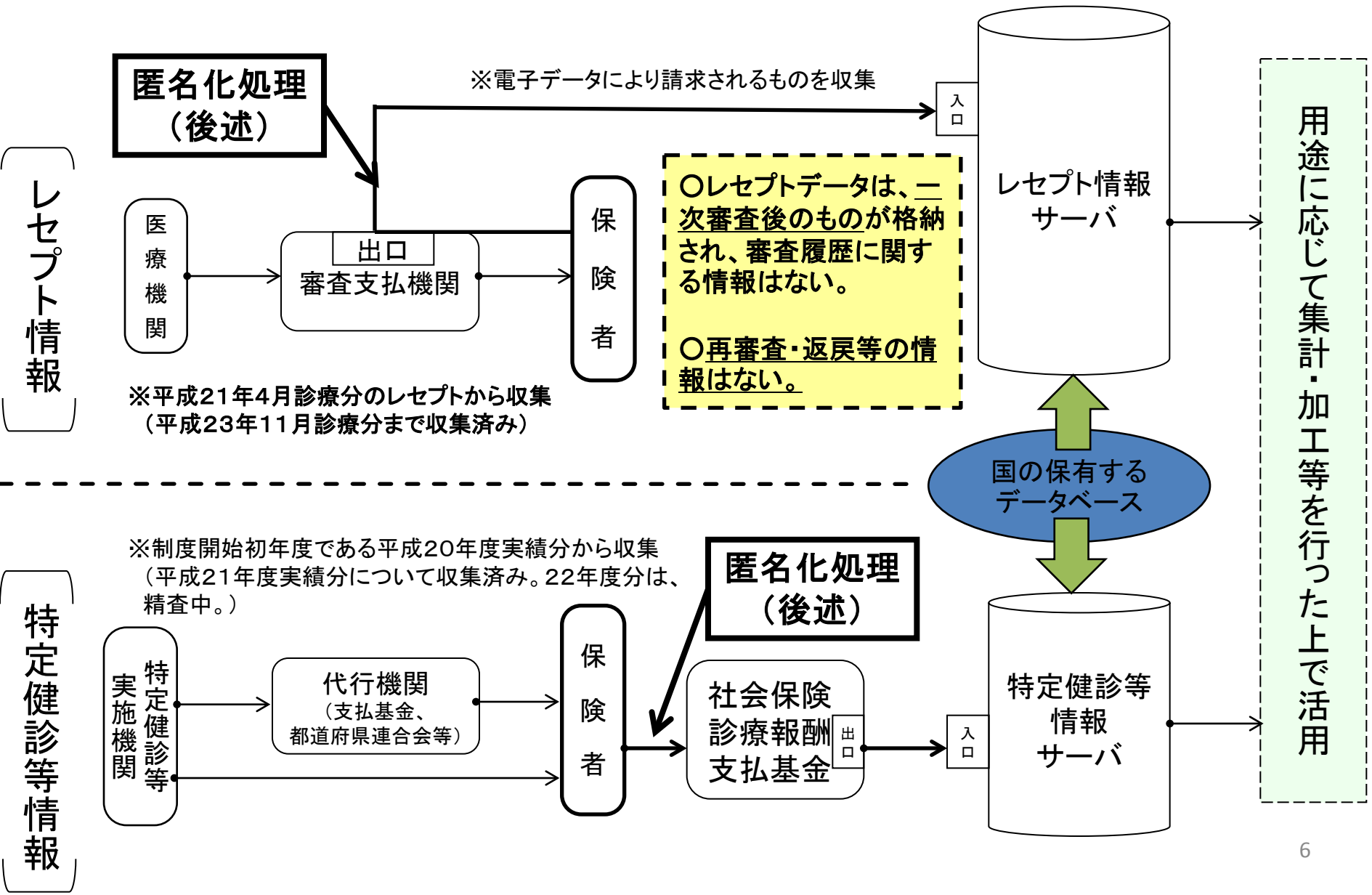
レセプト情報等の提供に関する有識者会議における審査

※データ利用の目的や必要性等について審査
※データ利用の目的として「公益性の確保」が必要

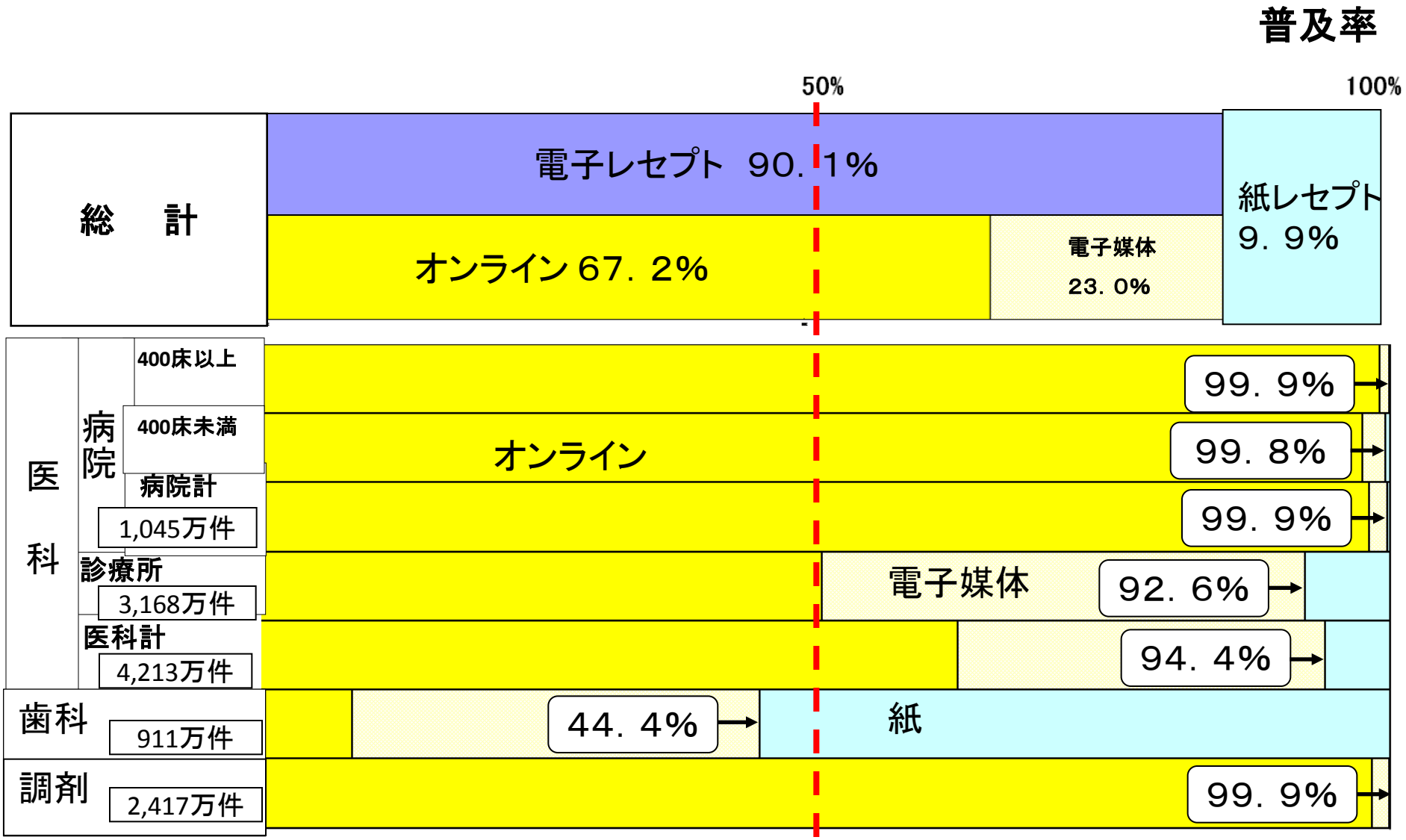
データ提供の可否について大臣に助言

大臣決定

レセプト情報・特定健診等情報の収集経路

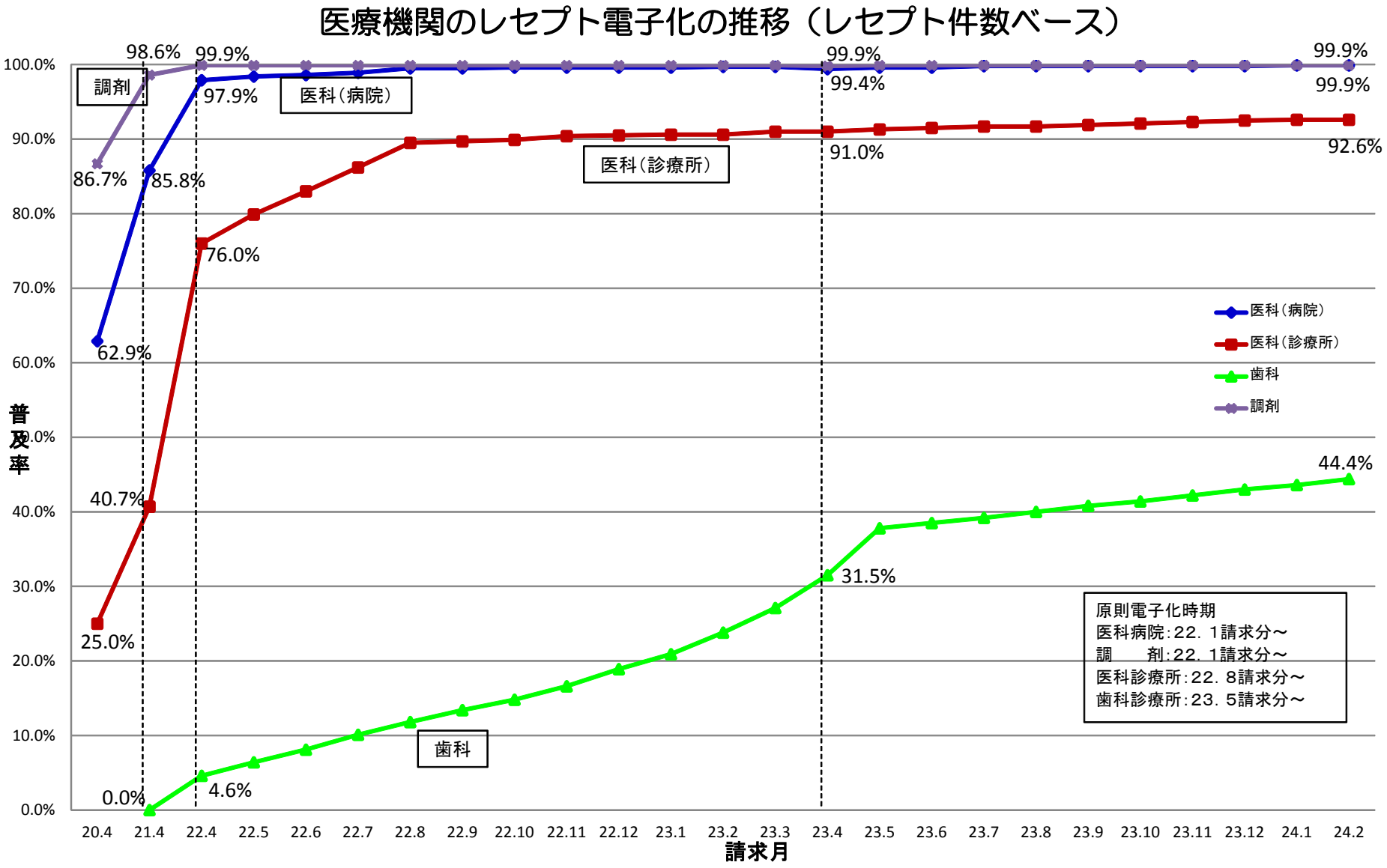


電子レセプト請求普及状況（件数ベース）【平成24年2月請求分】



社会保険診療報酬支払基金調べ

レセプト電子化の推移


医療機関のレセプト電子化の推移（レセプト件数ベース）
普及率
請求月
100.0%
90.0%
80.0%
70.0%
60.0%
40.0%
30.0%
20.0%
10.0%
0.0%
20.4
21.4
22.4
22.5
22.6
22.7
22.8
22.9
22.10
22.11
22.12
23.1
23.2
23.3
23.4
23.5
23.6
23.7
23.8
23.9
23.10
23.11
23.12
24.1
24.2
調剤
医科（病院）
医科（診療所）
歯科
98.6%
99.9%
99.9%
99.4%
99.9%
99.9%
86.7%
85.8%
97.9%
91.0%
92.6%
76.0%
62.9%
40.7%
25.0%
44.4%
31.5%
0.0%
4.6%
医科（病院）
医科（診療所）
歯科
調剤
原則電子化時期
医科病院：22．1請求分～
調　　剤：22．1請求分～
医科診療所：22．8請求分～
歯科診療所：23．5請求分～

レセプトの記載内容

レセプトの主な記載項目

〇傷病名
〇診療開始日、診療実日数
〇医療機関コード
〇初診・再診、時間外等
〇医学管理（医師の指導料等）
〇投薬
〇注射
〇処置
〇手術
〇検査
〇画像診断
〇請求点数（１点につき10円） など

（注1） 診療報酬明細書としての性格から、医療機関の経営状況等の情報は記載されていない。
（注2） 請求点数については、審査支払機関の査定後の点数が保存される。査定の有無はデータとして保存されない。

レセプトデータのうち、以下の項目は、同一人を特定する方策を講じた上で（後述）、匿名化のため削除されてデータベースに収集される。

〇患者の氏名　〇生年月日の「日」　〇保険医療機関の所在地及び名称　〇カルテ番号等　〇国民健康保険一部負担金減額、免除、徴収猶予証明書の証明書番号　〇被保険者証（手帳）等の記号・番号　〇公費受給者番号

特定健診・特定保健指導データについて

特定健診、特定保健指導は、データベース上に別々のファイルで保管。主な記録されている項目は以下のとおり。

〇受診情報（実施日等）
〇保険者番号
〇特定健診機関情報（機関番号のみ）
〇受診者情報の一部（男女区分、郵便番号）
〇健診結果・問診結果
〇保健指導レベル
〇支援形態
〇特定保健指導のポイント数　など

以下の項目は、同一人を特定する方策を講じた上で（後述）、匿名化のため削除されて、データベースに収集される。

〇特定健診・保健指導機関の郵便番号、所在地、名称、電話番号　〇医師の氏名　〇被保険者証の記号及び番号　〇受診者の氏名　〇受診券有効期限

レセプト・特定健診等情報データベースの管理・運用体制

○データベースに蓄積されたデータ件数（平成24年3月現在）

レセプト情報　　約20億71万件
特定健診・保健指導情報　　約2,062万件

※　レセプト情報については、21年４月診療分から、23年10月診療分までのデータ。特定健診・保健指導情報は、平成20年度・21年度実績分。現在のデータベースの容量では５年分程度の蓄積が可能。それ以上の期間のデータを蓄積するには、データベースの容量の拡張が必要。

○データベースの保管・管理方法

1．設置場所

地震・洪水・火災等の災害発生リスクを考慮して、より安全な設置場所を選定。

2．管理・運用体制

「行政機関の保有する個人情報の適切な管理のための措置に関する指針について」（平成16年9月14日総務省通知84号）を踏まえ、下記のような措置を講じつつデータベースの管理・運用を委託。

－緊急事態発生時には、24時間365日連絡・対応がとれるよう体制を整備。
－設置場所において、部外者の進入を防止するための厳格な入退室セキュリティ装置を整備。
－データベースのみでなく媒体についても、保管庫の施錠管理、台帳管理を徹底。
－運用・保守契約において、運用管理業者に対し守秘義務を課すとともに、再委託の原則禁止、厚生労働省による個人情報の管理状況についての立入調査等の個人情報保護の措置を規定。
－厚生労働省においても、データベースのデータを扱う職員を限定し、パスワードの定期的変更等を含む管理を徹底。

２．データの匿名化方法について

ハッシュ関数の採用

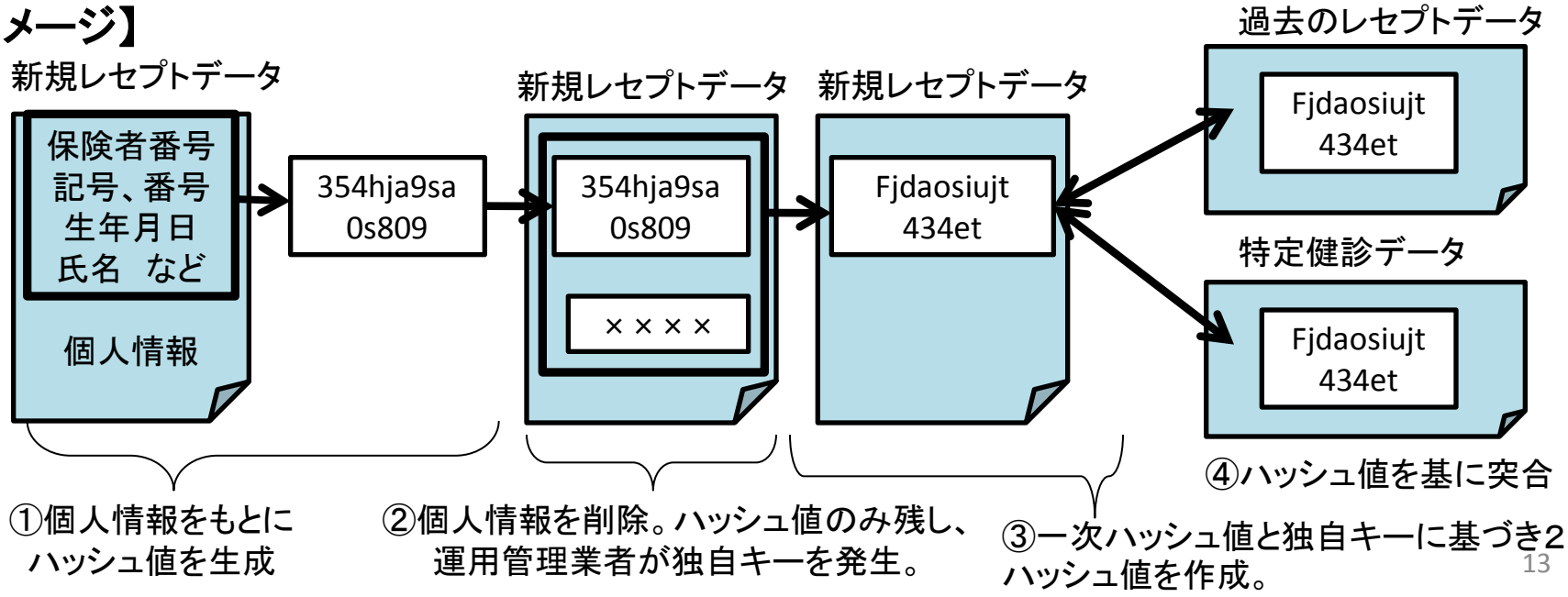
以下の特徴を持つ「ハッシュ関数」を用いることで、個人の直接的な識別情報を削除（「匿名化」）した上で、同一人物の情報であることを識別できるようにし、データベースへ保管している。

【ハッシュ関数の特徴】

①与えられたデータから固定長の疑似乱数（ハッシュ値）を生成する。
②異なるデータから同じハッシュ値を生成することは極めて困難。
③生成された値（ハッシュ値）からは、元データを再現することは出来ない。

※ 個人情報（氏名、生年月日等）を基にしてハッシュ値を生成し、それをIDとして用いることで個人情報を削除したレセプト情報等について、同一人物の情報として特定することが可能。

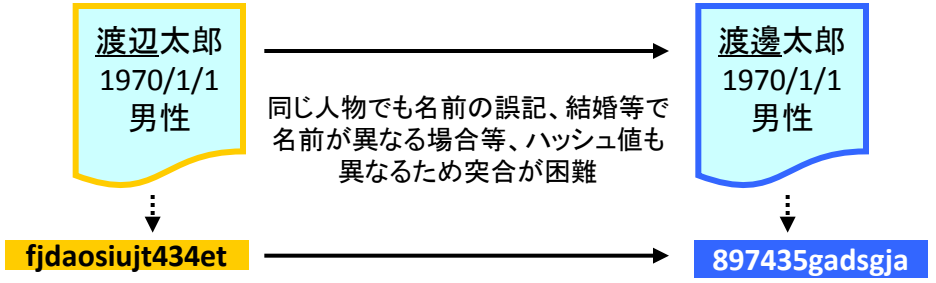
【イメージ】



ハッシュ関数についての留意点

ハッシュ関数自体、及びそのインプットとなる個人情報の管理状況から、同一人物の情報の紐付けを完全には行うことが困難なため、分析目的に応じた考慮（不良データの許容度、修正方針等）が必要。

①個人情報（保険者番号、記号番号、生年月日、性別、氏名）をもとにハッシュ値を生成するため、これらの情報に変化があった場合、突合が困難

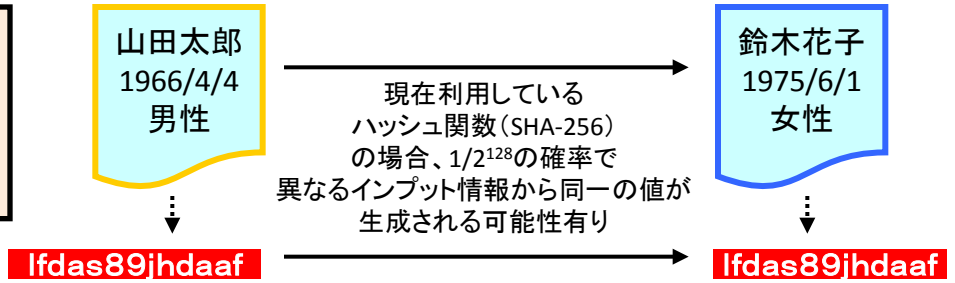


②レセプト情報と健診・保健指導データでは氏名の記載ルールが異なる

■レセプト　：　漢字氏名
■健診・保健指導　：　カナ氏名

インプットが異なるためハッシュ値も異なる

③ハッシュ関数の技術的特性として、極めて小さい確率ではあるが、異なる入力情報から同一のハッシュ値が生成される可能性がある。



留意点への対応

前ページの留意点に対応するため、現在、情報に変化のある「保険者番号、記号・番号」及び「氏名」について、それぞれ別のハッシュ関数を生成させ、データの突合の精度を向上させている。

ハッシュ値を2つ生成させる

① 保険者番号・記号番号・生年月日・性別からハッシュ値①を生成させる。

保険者番号
記号
番号
生年月日
性別
→ fjdaosiujt434et

② 氏名・生年月日・性別からハッシュ値②を生成させる。

氏名
生年月日
性別
→ 897435gadsgja

対応可能なケース

ケース①（記号・番号変更）

転職などで保険者番号、記号・番号が変更になった場合

ハッシュ値②により紐付けが可能

※ ただし、年月日・性別・氏名について同一の人物がいた場合、紐付けが不可能となる。

ケース②（氏名変更）

氏名の記載ミス、結婚などで氏名が変更になった場合

ハッシュ値①により紐付けが可能

※ ただし、生年月日、性別について同じ人物が同一記号・番号内に2名以上、存在した場合、紐付けが不可能となる。（双子など）

ケース③（レセプトと健診・保健指導データの紐付け）

氏名の記載ルールが異なるレセプトと健診・保健指導データを紐付ける場合

ハッシュ値①により紐付けが可能

※ ただし、生年月日、性別について同じ人物が同一記号・番号内に2名以上、存在した場合、紐付けが不可能となる。（双子など）

対応不可能なケース

記号・番号と氏名ともに変更があった場合

・結婚などで保険者が変更、氏名が変更になった場合
・転職などで保険者が変更、氏名の記載ミスがあった場合

３．データ提供にあたっての基本的考え方

行政機関個人情報保護法との関係整理①

個人情報の定義

生存する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。）
（行政機関の保有する個人情報の保護に関する法律第２条第２項）

照合できる「他の情報」には、公知の情報や、図書館等の公共施設で一般に入手可能なものなど一般人が通常入手し得る情報が含まれる。
一方で、特別の調査をすれば入手し得るかもしれないような情報は、通常は含まれない。（「行政機関個人情報保護法の解説（増補版）」総務省行政管理局）

国の保有するレセプト情報・特定健診情報は個人情報か否か

レセプト情報・特定健診等情報データベースについては、
① 患者の方々の個々のデータは、そのデータ単独では特定の患者の方々を識別可能な個人情報とはならないと考えられる。
② 個人立の医療機関・薬局コードについては、経営者個人の情報を識別できるため個人情報に該当。
ただし、特定の情報をデータベースから抽出し、何らかの方法で入手した他の情報と照らし合わせることにより、個人の方が特定される可能性があるとしても、通常それだけではデータベースの情報は、個人情報とはならない。
しかし、例えば以下のように照らし合わせる他の情報が「公知の情報」であれば、個人情報となりうるケースもあると考えられ、個人情報の特定可能性については、データの内容毎に慎重な検討が必要。

【例】
極めて稀な特定の傷病に罹患した患者が、特定の医療機関に入院していることが、報道などによって公知となっているような場合など。

有識者会議における個別の審査を経て判断

行政機関個人情報保護法との関係整理②

保有個人情報の利用・提供の制限

行政機関の長は、法令に基づく場合を除き、利用目的以外の目的のために保有個人情報を自ら利用し、又は提供してはならない。

ただし、本人又は第三者の権利利益を不当に侵害するおそれがない場合で、以下に該当する場合は、保有個人情報を自ら利用し、提供することができる。

①本人の同意があるとき、又は本人に提供するとき。
②行政機関が所掌事務の範囲内で、相当な理由に基づき内部利用するとき。
③他の行政機関、独法、地方公共団体等が相当な理由に基づき法令に基づく業務・事務の遂行に必要な範囲内で利用するとき。
④専ら統計の作成又は学術研究の目的のために提供するとき　など。

（行政機関の保有する個人情報の保護に関する法律第８条）

専ら統計の作成や学術研究のために保有個人情報を利用する場合には、特定個人が識別できない形で用いられるものが通常であり、個人の権利利益を侵害するおそれが少なく、かつ、公共性も高いと考えられることから、利用目的以外の利用・提供の原則禁止の例外としたもの。

（「行政機関個人情報保護法の解説（増補版）」総務省行政管理局）

目的が統計の作成や学術研究であっても特定個人を識別しうる分析・研究方法については審査に当たって抑制的に考える必要がある。

原則として提供されたレセプト情報等とその他の情報との照合を禁止

医療機関・薬局コード及び保険者番号の取扱い

医療機関・薬局コード

各地方厚生局が管内の保健医療機関・保険薬局に付す7桁の番号。

保険者番号

保険者毎に定められた、国民健康保険は6桁、健康保険は8桁の番号。

個別の医療機関コードの情報を提供することが、患者個人の方の特定につながるようなケースは、回避する必要がある。

また、特に市町村国保など、比較的小規模な保険者の場合には、保険者が特定された場合、被保険者個人の識別可能性が高まることが想定される。

○ **医療機関・薬局コード及び保険者番号の提供は原則行わないこととし**、経年データを分析する場合には医療機関等に新たな通し番号等を付番することを基本とする。

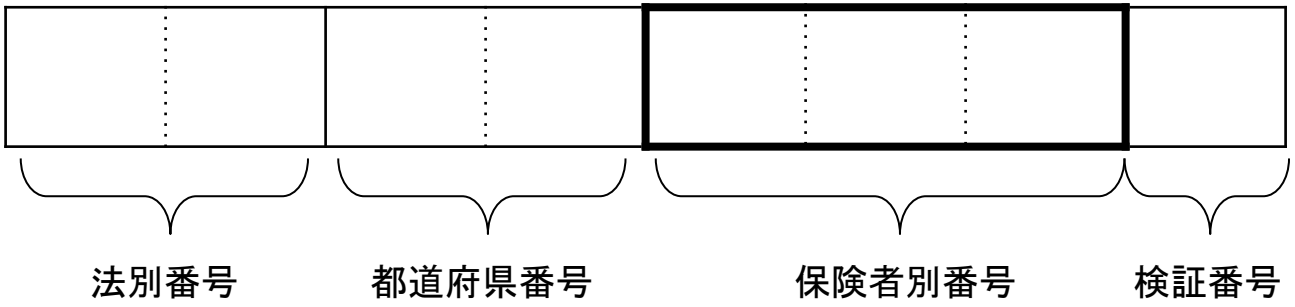
○ ただし、例外的な場合として、地域性の分析・調査にのみ用いる場合に、その目的に照らして最小限の範囲内で有識者会議における審査を経て提供できる場合を認めることとする。

なお、その場合においても、 医療機関等の個別の同意がある場合等、有識者会議が特に認める場合を除いて、公表される成果物の中に特定の医療機関・薬局及び保険者を識別できる資料・データ等は盛り込まないこととし、違反した場合には、他の不適切利用への措置（データ提供禁止）よりも重いペナルティー（氏名・機関の公表）を設けることとする。

（参考）医療機関・薬局コードと保険者番号について

保険者番号

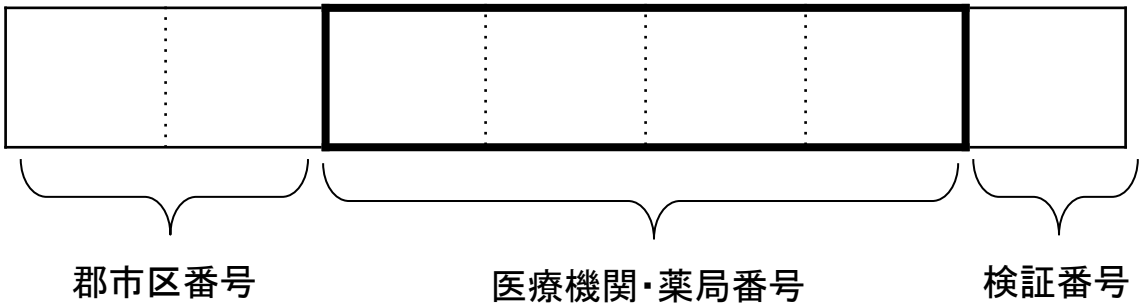
保険者番号は、以下のように法別番号2桁、都道府県番号2桁、保険者(市町村)別番号3桁、検証番号1桁、計8桁の算用数字を組み合わせたもの。ただし、国民健康保険（退職者医療を除く。）の保険者番号については、都道府県番号2桁、保険者(市町村)別番号3桁、検証番号1桁、計6桁の算用数字を組み合わせたもの。



※法別番号は、協会管掌健康保険や船員保険などの制度を表す番号。
※※都道府県番号は都道府県毎に付される番号。

医療機関・薬局コード

医療機関コード及び薬局コードは、以下のように郡市区番号　2桁、医療機関（薬局）番号4桁、検証番号1桁、計7桁の算用数字を組み合わせたもの。



※郡市区番号は、都道府県ごとに、郡、市及び区を単位として、地方厚生（支）局長が定めるもの。
※※医療機関(薬局)番号は、医療機関について、医科にあっては1,000から2,999、歯科にあっては3,000から3,999、薬局にあっては4,000から4,999の一連番号を前記の郡市区ごとに、地方厚生（支）局長がこれを定めるもの。

個別医療機関・保険者の属性情報について

データベース上の個別医療機関・保険者等の属性情報

医療機関	○都道府県コード（01：北海道、02：青森） ○医療機関コード（個別の保険医療機関毎に定められたコード） ○診療科コード（旧総合病院は平成22年３月診療分まで記載） ○病棟区分（01：精神病棟、02：結核病棟、07：療養病棟のいずれかに該当する場合のみ記載。） ○病床数 ○薬局コード（調剤レセプトのみ）
保険者	○保険者番号（各保険者固有の番号）

直接的な識別情報である医療機関コードを削除したとしても、都道府県と病棟区分や病床数との組み合わせで個別の医療機関が推定できる可能性が完全になくなる、とは言い切れないと考えられる。
（例：○○県に結核病棟が極めて少ない場合、病床数が具体的な数（111など）で示される場合など。）

ガイドライン上、そもそも有識者会議が特に認めた場合を除き、**他の情報とのリンケージ（照合）を行わない**、とする取扱いを明記（研究は、基本的に提供を受けたデータセットのみを用いて行うものとする。）。

また、属性情報に応じて一定の処理（数字を丸める、極端なデータは提供しない。）をした上で提供することを有識者会議において検討。

データ提供にあたってのセキュリティ要件

考え方

○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回会議での議論）**。

○これを踏まえ、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。

○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。

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。

不適切利用等に対する措置

〇各要件に応じて、有識者会議の議論を経つつ、所要の措置を科すことを規定（データの消去、返却を求め、以下の②から⑤までについては成果物の公表も禁止する。）。
〇施行期間においては、集計表情報であってもセキュリティ要件に関する規定以外基本的に同様の措置。
〇不適切利用によって不当な利益を得た場合には、当該利益相当額を違約金として支払う。

措置要件	措置内容
①返却期限（利用期間の最終日）までにレセプト情報等の返却を行わない場合	返却を行う日までの間及び返却を行った日から返却を遅延した期間に相当する日数の間、レセプト情報等の提供を禁止する。
②レセプト情報等を依頼書等の記載とは異なるセキュリティ要件の下で利用することなどにより、セキュリティ上の危険に曝した場合（集計表情報の場合を除く）	・行為の態様によって、当該認定をした日から、保険局が定めるまでの間、レセプト情報等の提供を禁止する。
③レセプト情報等を紛失した場合	・行為の態様によって、当該認定をした日から、保険局が定めるまでの間、レセプト情報等の提供を禁止する。 ・レセプト情報等の紛失が利用者の重過失による場合には、利用者の氏名及び所属機関名を公表する。
④レセプト情報等の内容を漏洩した場合	・行為の態様によって、当該認定をした日から、保険局が定めるまでの間、レセプト情報等の提供を禁止する。 ・利用者の氏名及び所属機関名を公表する。
⑤承諾された目的以外への利用を行った場合	・行為の態様によって、当該認定をした日から、保険局が定めるまでの間、レセプト情報等の提供を禁止する。 ・提供されたレセプト情報等に医療機関コード、薬局コード又は保険者番号が含まれていた場合には、利用者の氏名及び機関名を公表する。
⑥その他、利用規約の内容に違反した場合、又は法令違反、国民の信頼を損なう行為を行った場合	行為の態様によって、上記①から⑤の措置に準じた措置を講じる。

利用規約について

〇レセプト情報等の提供は、利用者と厚生労働省との契約に基づくものとして実施。

〇利用者は厚生労働省が定める利用条件（利用規約）に同意するとの誓約書を提出した上で、レセプト情報等の利用を行う。

〇利用規約については、ガイドラインの規定のうち、利用者に具体的な義務を科す項目を記載。

主な利用規約に規定した項目

〇利用者によるレセプト情報等の利用制限（申し出られた利用範囲に限定など）

〇利用期間（最大１年間であらかじめ申し出られた期間（延長可能））

〇厚生労働省保険局が必要に応じ行う立ち入り検査への利用者の応諾義務

〇利用後の処理（レセプト情報等の返却、中間生成物等の消去、公表前の報告義務、利用実績報告など）

〇成果の公表（予定時期までの公表義務、公表する内容によって特定の個人又は医療機関等が第三者に識別されないこと、など。）

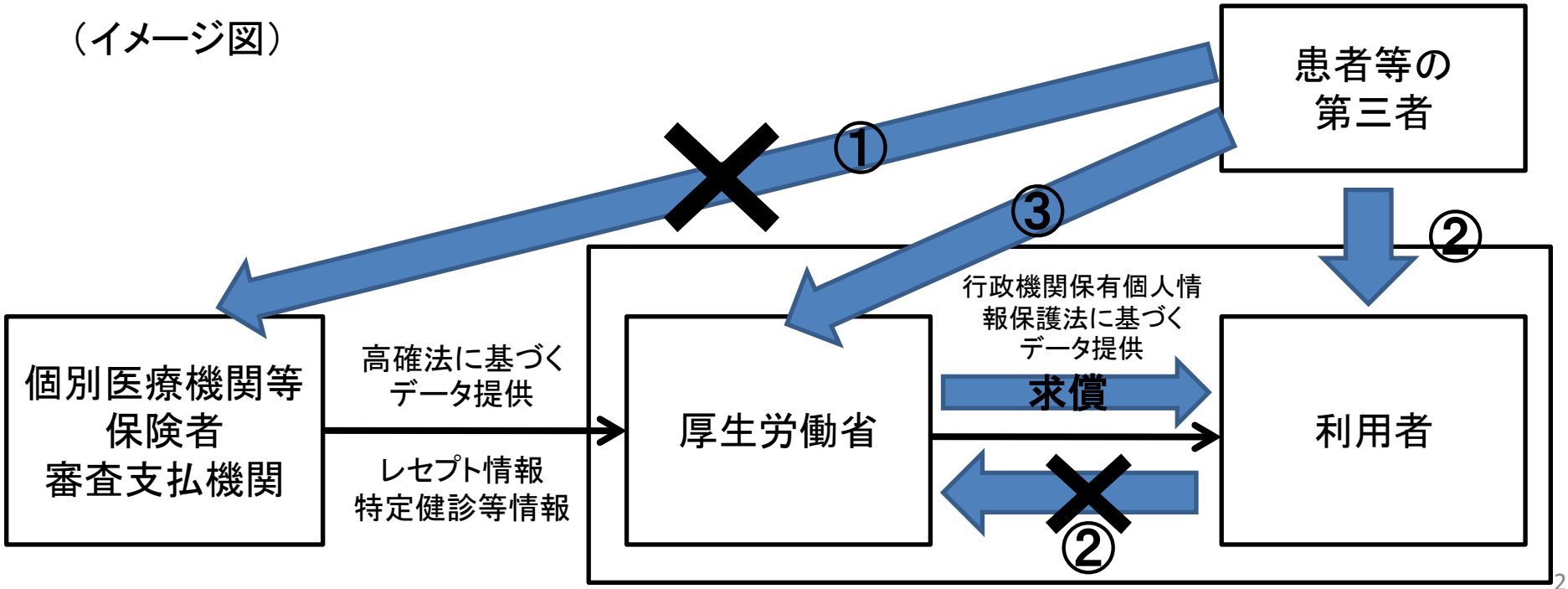
〇ガイドライン及び本規約に違反した場合の措置（レセプト情報等の返却、提供の禁止、公表の禁止、利用者の氏名・所属機関名の公表又は違約金の納付）

データ提供について関係者の責任関係の考え方

○ レセプト情報等の提供は、行政機関保有個人情報保護法第8条第2項第4号の規定に基づき国の責任において行うもの。
　したがって高齢者の医療の確保に関する法律の規定に基づきデータを国へ提供する個別医療機関等は、国が行うレセプト情報等の提供について責任を有さない（①）。

○ また、利用規約において第三者の権利利益の侵害について、利用者は基本的に厚生労働省の責任を問わないことを定めることとし、一義的に利用者が責任を有することとする（②）。
　ただし、国は利用者へのデータ提供の妥当性等について第三者に対し責任を負う場合もありうるが（③）、この場合、国は必要に応じ、利用者へ求償を行うことができる。

（イメージ図）

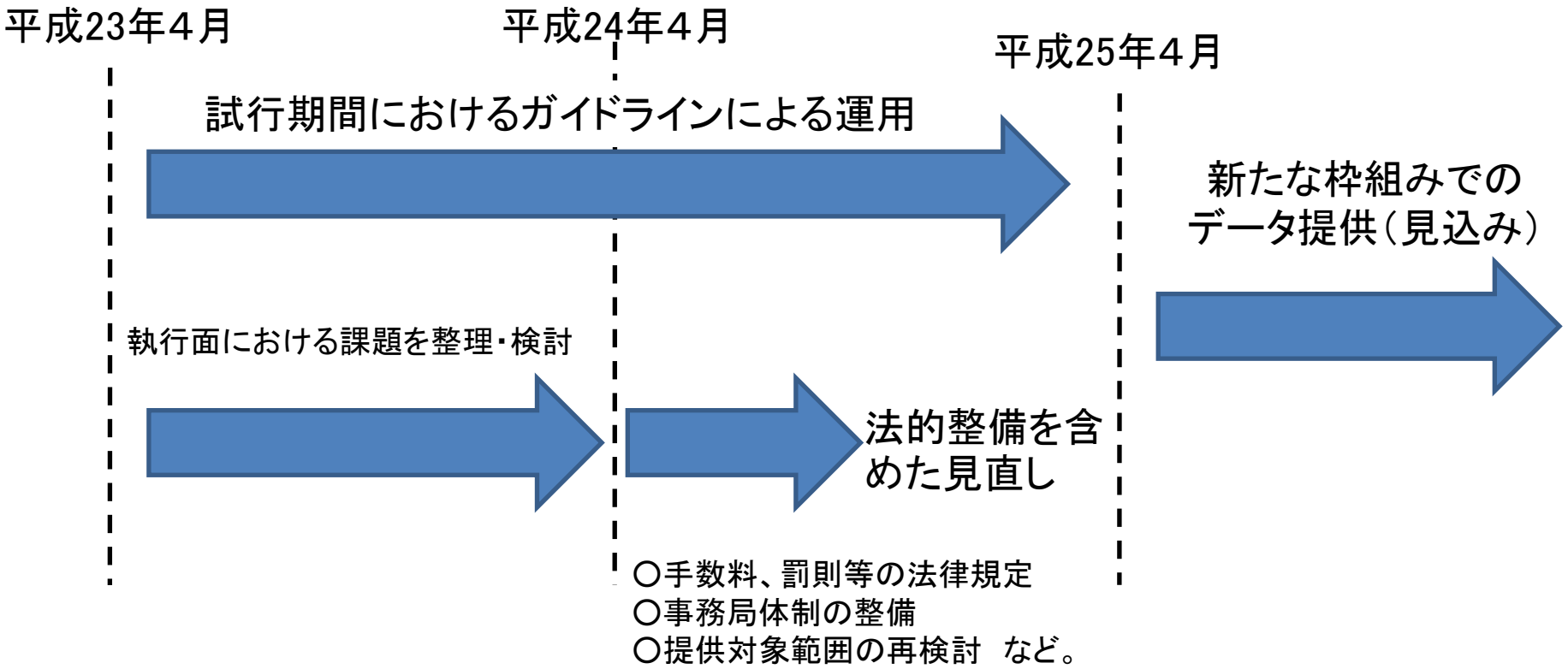


4. スケジュール

試行期間におけるレセプト情報等の提供について

○　統計法の匿名データ提供における試行的提供期間（平成16年～20年）も勘案し、以下のようなスケジュールとして、**23～24年度の実施状況を踏まえ**、有識者会議で議論を行いつつ、将来的に法的整備を含めた制度作りを検討する予定。

○　したがって、現在策定されているガイドラインによるデータ提供については、あくまで試行期間におけるもの、との位置づけであり、今後、実績を勘案し見直しを検討。



次回の提供に向けたスケジュール

○３月２１日
（１）基本データセットに関する事前説明会
（２）次回レセプト情報等提供に関する事前説明会

○４月上旬
・基本データセットの事前相談開始（第１回の申出で不承諾とされた者に限定）
・全数データの事前相談開始
※　今回は事前相談期間における相談を必須とする（詳細は別途公表）。

○４月下旬
・基本データセット、全数データの申出受付（１週間程度）

○４月下旬～
事務局における審査（必要に応じ申出者へも照会）

○５月中
第１０回　有識者会議
・基本データセットの提供申出についての審査

○７月中
第１１回　有識者会議
・全数データの提供申出についての審査

近日中に具体的な日程等について公表を予定

Ⅱ　審査基準について

１．基本的な審査方針

基本的な審査基準について（23年11月10日第1回審査での基本方針）

研究内容・抽出条件等について

①対象が極めて限定される研究について

「個人の識別可能性を下げる」という原則に鑑み、「対象者が極めて限定される可能性がある」申出は、申出者にデータを渡した時点で個人が特定される可能性を否定できないため、事務局審査では提供依頼について不承諾とした。

○「10未満のセルは空欄にする」「申出以外の分析は一切行わない」と明記されている申出であっても、今回は試行期間ということもあり、不承諾と考えた。
○少数セルが多発する可能性は研究を開始してみないとわからない、という意見もあった。
○集計時に少数セルが頻発することが想定される申出のなかには、申出者が配慮すると明記されており、他の審査方針を満たしていたため、総合的にみて承諾と考えたものもある。

②探索的な研究について

「個人の識別可能性を下げる」という原則に鑑み、多数の項目を用いた探索的研究や、SYの「傷病名コード」、SIの「診療行為コード」、IYの「医薬品コード」（DPCの場合にはBU, SB, CD）どれかひとつでも「全て求める」という要望の申出は、事務局審査では提供依頼について不承諾とした。

○多変量解析、propensity score分析、重回帰分析など多くの項目を必要とする申出も探索的研究と考え、今回は不承諾とした。
○何らかの抽出を経たあとのサンプルに対しても、上記のような申し出に対しては同様の判断とし、特定健診等情報を用いた研究の申出にも適用。
○研究手法によってはこうした抽出条件とならざるを得ないものもあり、「サンプリングデータセット」によって対応（第1回に申出を行った者を対象に本日、午前に事前説明会を開催）。
○申出のなかには、傷病名コードを全て求めてはいたものの、「2次医療圏単位の集計」に限定されているなど個々人の特定可能性が極めて低いため、承諾と考えたものもある。

③申出の内容・範囲について

「1申出1審査」という原則に鑑み、「複数の研究」が1申出に盛り込まれている場合も、審査にあたっては他の申出内容も加味したうえで、提供についてはより慎重な評価を行った。

○事務局から内容の照会を行ったことにより再提出において改善がみられたものもあったが、「利用目的」ごとの申出書作成を原則としている（ガイドラインp.9）ことを踏まえた評価を行った。
○細分化された研究が並んでいた申出のなかには、全体が大きな目的で統一されており、その他の審査方針も含めて総合的に鑑みて承諾と考えられるものもあった。

基本的な審査基準について（つづき）

④研究内容の定義について

研究には公益性が求められるため、研究に際して抽出項目の措定や目的と抽出項目との関連において、事務局審査にて「定義が不十分」な箇所があると思われる申出は、相対的にみてより慎重な評価を行った。

〇抽出項目が研究内容からみて最小限とはいえなかったり、関連性が不明、または説明不十分と判断された申出がこれにあてはまる。
〇公表形式の具体例が研究内容に鑑みて非常に限定されていたり、公表形式から想定される必要項目をはるかに超える抽出項目を要求したりする申出のなかには、研究内容の「定義が不十分」と思える申出もみられた。

⑤その他

その他、以下のような事例に対しても、事務局審査において慎重な評価を行った。

〇都道府県単位など、地域に限定したデータ提供の申出については、国が保有する全国レベルのデータベースという位置づけに鑑みて、その公益性について留意した。
〇「集計表情報」の提供を求める申出のなかには、集計表作成が複雑であり学術研究の領域に踏み込んでいると思われるものもあった。集計表情報作成は、簡略な操作にて作成できるもののみを対象とした（単純なクロス集計など）。

セキュリティ要件について

①ISMSの実践

「情報セキュリティマネジメントシステム（ISMS）の、申出者個々の研究環境に応じた合理的な対応」の実践を求めていることに鑑み、独自のセキュリティ規程が一部、もしくは全て欠けている事例は、事務局審査にて提供依頼について不承諾とした。

〇事務局から内容の照会を行ったことにより再提出において改善がみられた申出が複数みられたが、その際にも、「運用フロー図」「リスク分析・対応表」「運用管理規程」「自己点検規程」の整合性について、他の申出と同様に評価を行った。

〇情報資産の安全をチェックする頻度が、上記書類の相互で区々になっている申出など、セキュリティ対策の書類相互において齟齬が著しいものについては、より慎重な評価を行っている。

【不承諾とした例】
情報資産の特定不十分：USBや帳票が、「使われる」ことになっている書類と「使われない」ことになっている書類がある。
チェック体制の不備：自己点検規程には点検頻度が記載されているが、運用管理規程ではそのことについて言及がなされていない。
再提出時にそれらが修正されている場合にはその点も考慮した。一方、改善が不明瞭な場合は不承諾とした（②以下も同様）。

基本的な審査基準について（つづき）

②研究を行う場へのアクセスについて

入退室の管理が不十分であったり、利用者以外のアクセスが可能な場所でレセプト情報等が利用される事例についても、より慎重な評価を行い、なかには不承諾としたものもある。

〇研究室や情報管理室が共有スペースとなっており、他者が容易に解析機器に接触できる事例については、それらに対するセキュリティの強度や透明性の確保をどの程度整備できているのかについて留意した。
〇ISMSの観点からすれば、ハード面でのセキュリティ確保以上に、申出者それぞれの環境に適合した実践可能なセキュリティ対策の整備のほうが、より重要視されている。
〇たとえ「レセプト情報を管理する部屋には研究者のみ入ることができる」と記載されていても、その部屋が新たに準備された部屋と明記されているか、共用スペースと認識されかねない名称であるかで、記載内容の信頼度は変わってくる。研究環境が共用施設である場合には、記載の一貫性が保たれているかどうかについても評価した。

③研究を行う機関について

研究者や所属施設、研究施設が複数（多数）にまたがる事例については、セキュリティ対策実践の難易度が上がると想定されるため、その対応について慎重に評価を行い、不承諾とした申出もある。

〇施設間での業務分担が不明瞭な申出については、不承諾とした。
〇申出のなかには申出者が多数となるものもみられたが、研究環境に即した現実的な対応が提案されていたため、総合的に鑑みたうえで提供依頼について承諾としたものがある。

④技術的なセキュリティ対策について

技術的対策が不十分（ID管理、外部ネットワークとの接続など）な事例については、より慎重な評価を行った。

〇ID管理をする際の本人確認など、透明性の確保の程度に応じて、管理体制の評価を行い、承諾可否の判断根拠の一助とした。

〇やはりISMSの観点により、どれだけ既存の環境のなかで現実的な研究実施体制を構築できているかについて、着目した。
たとえば、外部ネットワークに接続しない機器を用いると記されている場合でも、それが新品であると明記されていたり他の研究への使用を禁じている事例と他の事例とでは、事務局審査において評価に差が生じた。

提供にあたっての優先順位について

○今後、データ提供の申出が増加していくことも考えられるが、申出が非常に多くなり、公益性やセキュリティ要件の面で審査を了する申出が増えた場合、全ての申出についてデータ抽出を行うことは困難となることも考えられる。

（参考）第１回申出における医政局指導課のデータ抽出では、全国の半年間における医科・DPCレセプト4億7,000万件の抽出作業に約200時間を要した（営業日で２週間程度）。

○こうしたことから審査の基準とは別に、各申出にデータ提供の優先順位をつけ、順位の高いものから順番に対応できるものまでデータ提供を行うこととしてはどうか。評価の方法については、有識者会議の委員に協力を仰いで行う部分と事務局において行う部分とを設け、事前に各項目について点数化した上で有識者会議の審査に諮る（イメージは次ページ）。

【評価項目】

以下のうち、①と②については、有識者会議の一部の委員があらかじめ評価を行い、それ以外については事務局において、評価を行った上で有識者会議に諮る。

①学術的な期待度

・申出された研究により、学術的に有意義な結果が得られる期待度が高いかどうか。

②研究内容の簡潔さ・明解さ（複雑・難解なものとなっていないか）

・複雑な研究内容や仮定を置いている研究であるかどうかについて判断することとして、理解が得やすいか否か。

③具体的な政策への反映を想定しているか（単なる基礎資料か否か）

・具体的な政策への反映を想定しているものか否か。

（例）医療計画の策定の基礎資料とするため都道府県への提供を想定　など。

④地域の範囲（全国か、地域限定の研究か）

・全国規模のデータベースという性質を活かす観点から、地域限定をした研究よりは、全国規模の研究を行うものを優先する。

⑤活用するデータ量・規模（大量のデータを使用するものか否か、抽出に要する見込み時間で判断）

・上記を第１回申出における処理時間約200時間を一応の標準的な処理時間として、データ抽出に要する時間についての評価を行う。

（参考）優先順位付けのイメージ

【点数付けの考え方】
〇事務的な作業が膨大であったとしても極めて学術的に有益な研究であれば、データ提供の優先順位上考慮する必要があることから、有識者委員の学術面での評価点数と事務局による実務面での評価点の最高点を同一とする。
〇両者の点数を勘案した総合評価の下にデータの提供の可否を決定。

	項目	評価
通常審査部分	研究内容の公益性	
	セキュリティ要件	
	….	
優先順位評価部分（有識者委員が評価）	①学術的な期待度	□低い（1） □やや低い（2） □普通（3） □ある程度高い（4） □高い（5）
	②研究内容の簡潔さ･明解さ	□難解（1） □ やや難解（2） □普通（3） □ある程度明解（4） □明解（5）
	有識者委員評価点合計	**（2～10）**
	③具体的な政策への反映	□想定していない（0） □想定している（3）
	④研究地域の範囲	□地域限定（0） □全国（2）
	⑤活用するデータ量 ※200時間を一応の標準処理時間とする。概ね300時間超がデータ量が多い。100時間未満が少ない。	□データ量が少ない（～100時間程度）（5） □普通（100～300時間）抽出作業（3） □データ量が多い（300時間～）（0）
	事務局評価部分	**（0～10）**

総合評価	**可･否**

２．審査基準等の詳細について

研究内容の定義

〇レセプト情報等の提供については、公益性の高い学術研究に提供していくことを基本的な方針としており、審査にあたっては研究内容の把握が非常に重要。

〇また、ガイドラインにおいては、研究を実施する上で「必要最小限の範囲」でのデータ提供を行うことを基本的な考え方としており、こうした観点からも研究内容を適切に申出書上明らかとする必要がある。

〇しかし、第１回の申出審査にあたっては、申出書上、研究内容の定義が必ずしも十分でなく、意図している研究内容の全体像が把握しがたいものもあった。

＜基本的な方針＞

〇データ提供にあたっては、研究内容を勘案し、「必要最小限の範囲」で必要な情報を提供することとしていることから、具体的な個々のデータの集計方法、解析方法まで分解した記述が必要。

＜不十分だと考えられる例＞

・特定健診等の情報を用いて、〇〇圏内の住民の糖尿病の有病率等を算出する。

＜十分だと考えられる一例＞

・特定健診の情報の〇〇レコードに〇〇と記載している者を〇〇圏内の住民と仮定。
・特定保健指導の情報の▽▽レコードに××と記載している者を〇〇圏内の住民と仮定。
・当該住民の〇〇と××の検査結果を用いて、算出式（具体的な算出式）によって、算出した率を糖尿病の有病率として仮定。当該有病率を性・年齢階級別（５歳刻み、85歳以上コーディング）で集計を行う。

※　あくまでイメージであり、記述は必ずしも正しくない場合もある。

公表形式について

○レセプト情報等を利用した研究の成果物公表において、
①患者の集計単位が10未満となっていけない、
②病床などの医療機関の属性情報を集計することにより、事実上、医療機関が特定される場合、患者の特定につながるリスクがあるため、医療機関等の集計が3未満となってはいけない、
といった公表形式の一応の基準を設定している。

○一方で地域の医療提供体制の集計を行う場合、地域の中核病院などが限られると集計単位が極めて少量となる可能性が高い（医政局指導課の研究）。

○こうしたことから公益性の高い地域の医療提供体制の研究等を目的としているものについては、できる限り柔軟に対応することが考えられるが一方で、個別の医療機関等に予想外の影響を与えることがないよう慎重な対応も必要となると考えられる。

＜基本的な方針＞
○申出にあたっては、想定している全ての公表形式を（図表、グラフ等の形式）を明示する必要。
○その上で公表前に厚労省へ事前報告を行うことを徹底し、判断が必要と考えられるものについては、有識者会議にも公表形式の適切さについて諮ることとする。こうした個別の実績を積み重ねた上で、可能であれば公表形式についての明確な基準を策定していくこととしている。

※　米国のCMSにおけるメディケア・メディケイドのデータ提供においては、利用者が公表前にCell　Size Suppression　Policyに従っているか確認をとることができる仕組みがある。

（参考）最小集計単位の原則について①

＜基本的な考え方＞

レセプト情報等の提供を受ける者についてはガイドライン等に基づき、利用目的、セキュリティ要件や他の情報との照合の禁止など様々な制約を課すこととしている。

しかし、一旦、研究成果として公表されたものについては、**それを目にした者がその公表された成果物とその他の様々な情報とを照合することについて制限を加えることができない**ため、極力、個人の特定可能性を低める措置を講じる必要がある。

※米国のCMSにおいては、cell size suppression policyとして、研究論文やレポートなどの成果物において、患者等の集計単位が一律10以下になってはならない、とのルールを定めている（第2回レセプト情報等の提供に関する有識者会議資料参照）。

原則として、患者・受診者の集計単位が10未満となる公表形式を認めないこととしてはどうか。

【事例①】地域別に特定の疾病患者数を集計した場合

	A県	B県	C県	D県	E県	F県
疾病①	13人	123人	3人	12人	9人	34人
疾病②	42人	15人	75人	5人	98人	252人

具体的な地域の医療状況を調べることにより、個人を特定できてしまうような事態を防ぐ必要がある。また、このような場合に、個人が特定されると上記の集計結果を前提としたその他の成果物において、その本人に係る他の情報まで識別される可能性がある。（C県の疾病①の患者の状態像の資料があった場合など。）

	A県	B県	C県	D県	E県	F県
疾病①	13人	123人	ー	12人	ー	34人
疾病②	42人	15人	75人	ー	98人	252人

（注）上記のーは、集計結果が10未満となったため、最小集計単位の原則から具体的な計数を記入していない。

（参考）最小集計単位の原則について②

【事例②】属性情報に基づいて個別の医療機関を集計した場合（「属性情報による集計単位」）

※疾病Aの患者数

	A県	B県	C県	D県	E県	F県
800床以上の病院	23人	15人	30人	45人	15人	5人
700～800床の病院	15人	24人	16人	35人	43人	73人

※仮に**A県に800床以上の病院が1つしかなかった場合**、患者の集計単位が10以上だったとしても医療機関が特定されるので公表不可。

※仮にF県の800床以上の病院が複数あったとしても、そもそも集計単位が10未満なので公表不可。

上記のような場合、

○集計単位が10以上だったとしても、属性情報による集計により、特定の集計単位に該当する医療機関が2以下となる場合には、最小集計単位の原則②として公表不可。

○そもそも属性情報による集計により、医療機関が2以下とならない場合でも、集計単位が10未満であれば、原則①により公表不可。

※DPCデータの公表については、個別の医療機関より、公表を前提にデータの授受を受けているため、原則②の運用は行っていないと考えられる。

対応例（1）：該当するセルの計数を表示しない。

or

対応例（2）：集計単位を広くする。

	A県	B県	C県	D県	E県	F県
800床以上の病院	ー	15人	30人	45人	15人	ー
700～800床の病院	15人	24人	16人	35人		

（注）上記のーは、集計結果が10以下となる、又は、属性情報による集計により、該当する医療機関の数が2以下となる、ことにより、最小集計単位の原則から具体的な計数を記入していない。

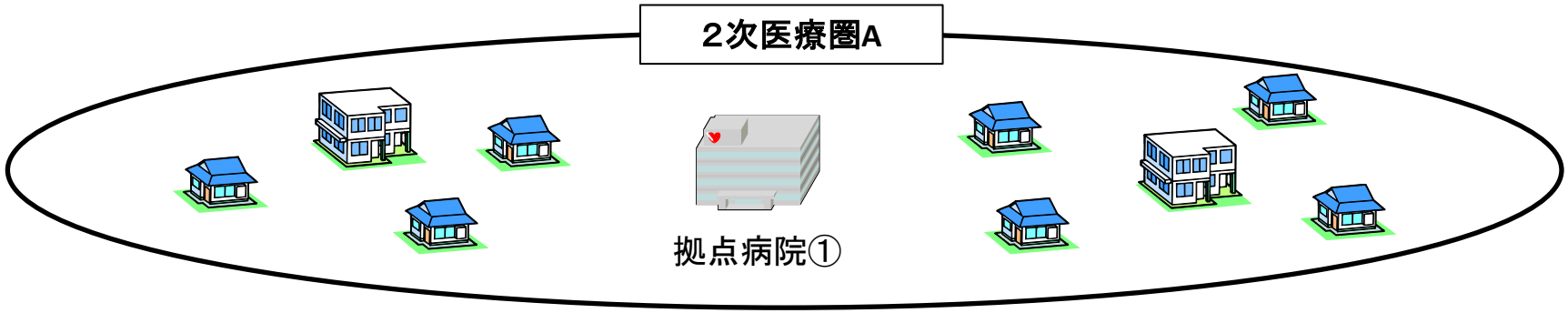
	A県	B県	C県	D県	E県	F県
800床以上の病院	38人	15人	30人	45人	15人	78人
700～800床の病院		24人	16人	35人	43人	

（注）A県及びF県のデータについては一部、集計により対象となる医療機関数が少数になることから、集計単位を広くとった部分がある。

（参考）最小集計単位の原則について③

【事例②`】地域の事情を特に勘案する必要がある場合（例外的な事例）

※　ある地域で特定の診療等（がん治療）を行っている医療機関が1つしかない、又は非常に少ない場合で、それがよく知られている事情である場合など



このような場合に特定の診療行為の情報等を集計・公表できないこととすると、実質的に地域の診療実績を調査することができなくなる可能性があるのではないか。

こうした場合には、
- 当該医療機関の同意がある場合等を除き、原則として公表される成果物に明示的には医療機関名を記載しない、
- 公表形式の集計にあたっては、最小集計単位の原則を遵守する、

ということを前提に、例外的に成果物の公表を認めることとしてはどうか。

集計表情報について

〇統計法のオーダーメード集計においては、集計対象となる項目をあらかじめ限定した上で、集計方法についてもその対象項目を2次元又は3次元までで集計するなどの縛りを設けている。

〇単純なクロス集計であっても、集計単位が複層化していく場合、複雑さが増すと共に個人の特定可能性も高まることが想定されるため、レセプト情報等についても一定の明確な基準が必要。

〇例えば集計対象項目は、レセプト毎の傷病名コード、診療行為コード、医薬品コード、特定器材コード等に限定し、集計方法については、性別、年齢階級別、都道府県別の集計を念頭において、原則、3次元までとすることとしてはどうか。

（参考）医療施設調査のオーダーメード集計の様式

3 集計対象項目

〇病院票
・施設数
・病床数（許可病床数、特殊診療設備、LDR、緩和ケア病棟）
・患者数（特殊診療設備、検査等の実施状況、緩和ケア病棟、緩和ケアチーム）
・設置台数（検査等の実施状況、手術等の実施状況）
・実施件数（在宅医療サービス、手術等の実施状況）
・従事者数（診療録管理専任従事者、分娩取扱従事者）

〇一般診療所票
・施設数
・病床数（許可病床数）
・患者数（検査等の実施状況）
・設置台数（検査等の実施状況、手術等の実施状況）
・実施件数（手術等の実施状況）
・従事者数

〇歯科診療所票
・施設数
・病床数（許可病床数）
・従事者数

5 オーダーメード集計提供項目
利用可能な集計区分は、集計対象項目ごとに分類一覧に示す区分となり、集計区分の組み合わせ（クロス数）は合計が3次元までとなります。ただし、「病床の規模」（病院票）、「病床の有無」（一般診療所票）及び「診療科目（重複計上）」（病院票及び一般診療所票）を含む組み合わせの場合は5次元まで可能となります。

３．セキュリティ要件について

３．セキュリティ要件について
（１）基本的事項について

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）＞

〇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。

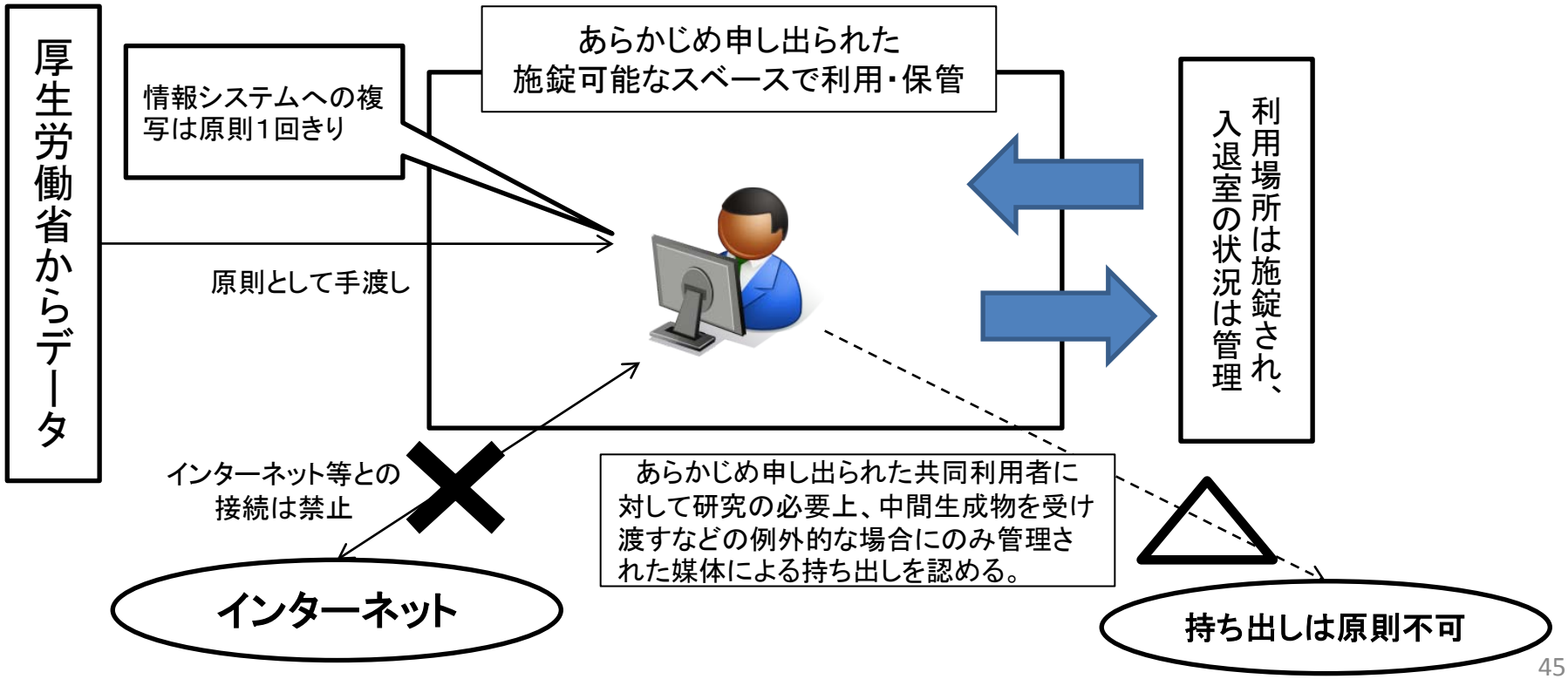
〇利用・保管場所は、あらかじめ申し出られた施錠可能で入退室管理を行っているスペースのみとし、原則として持ち出されないこと。

〇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。

〇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。

〇学部、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。

〇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。

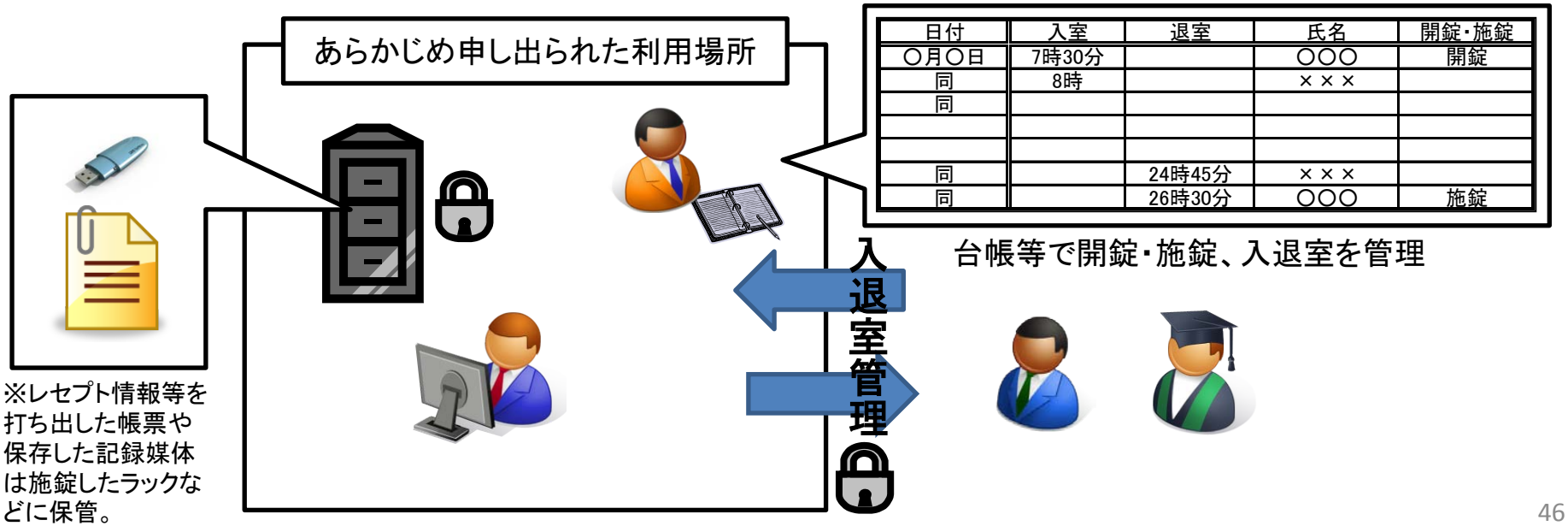


物理的なセキュリティ要件の具体例

＜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。

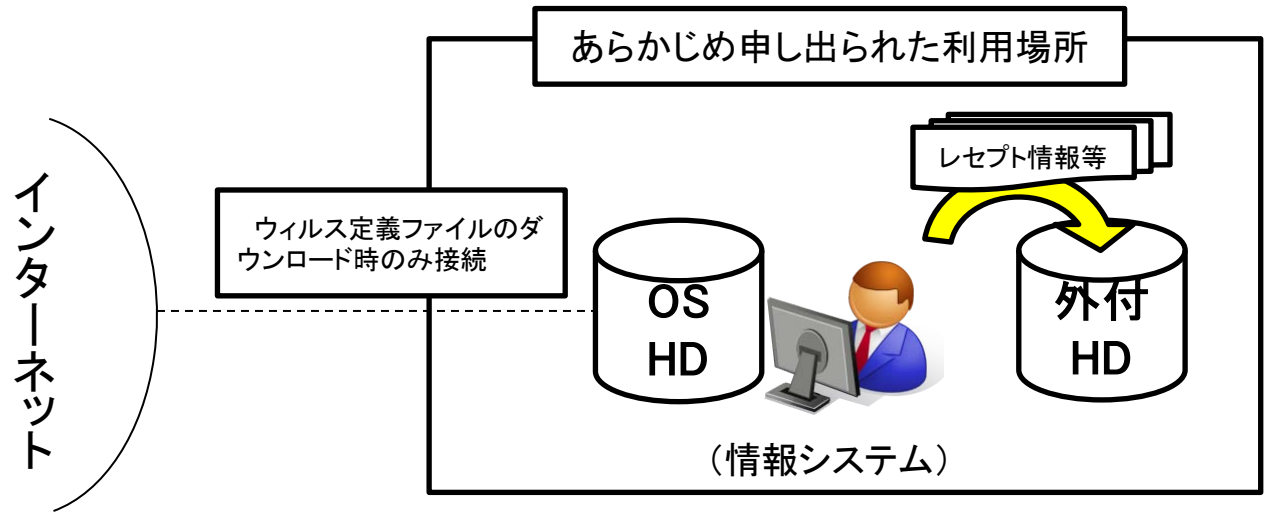
＜具体例＞

※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））

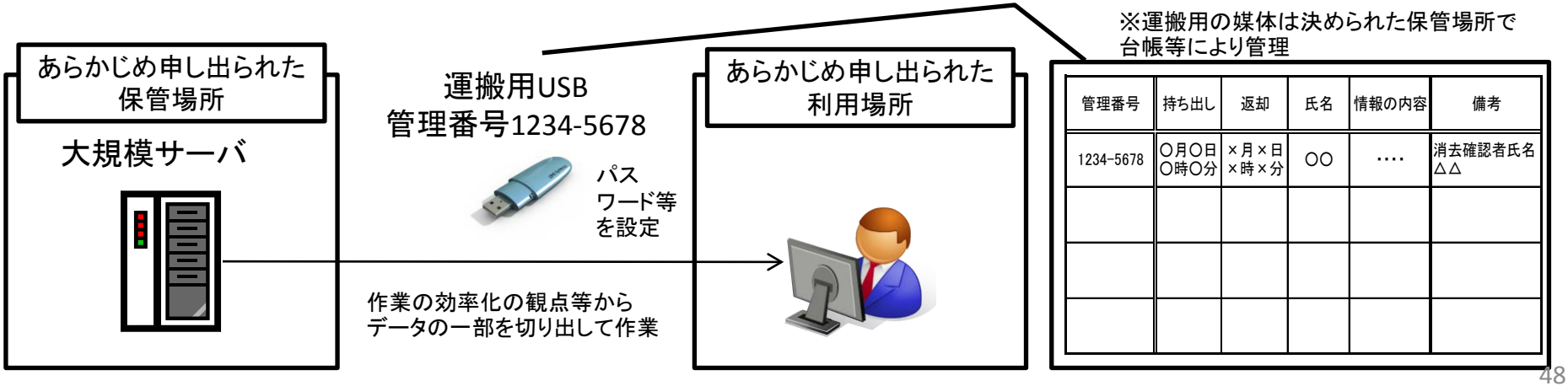
〇レセプト情報等は、事前に申し出られた利用場所から外部へは持ち出されないことを原則とするが、外部委託者や共同研究者間で中間生成物の受け渡しをする必要がある場合などに例外的に以下のような措置を講じることで持ち出しを認める。

・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。

３．セキュリティ要件について
（２）情報セキュリティマネジメントの実践

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

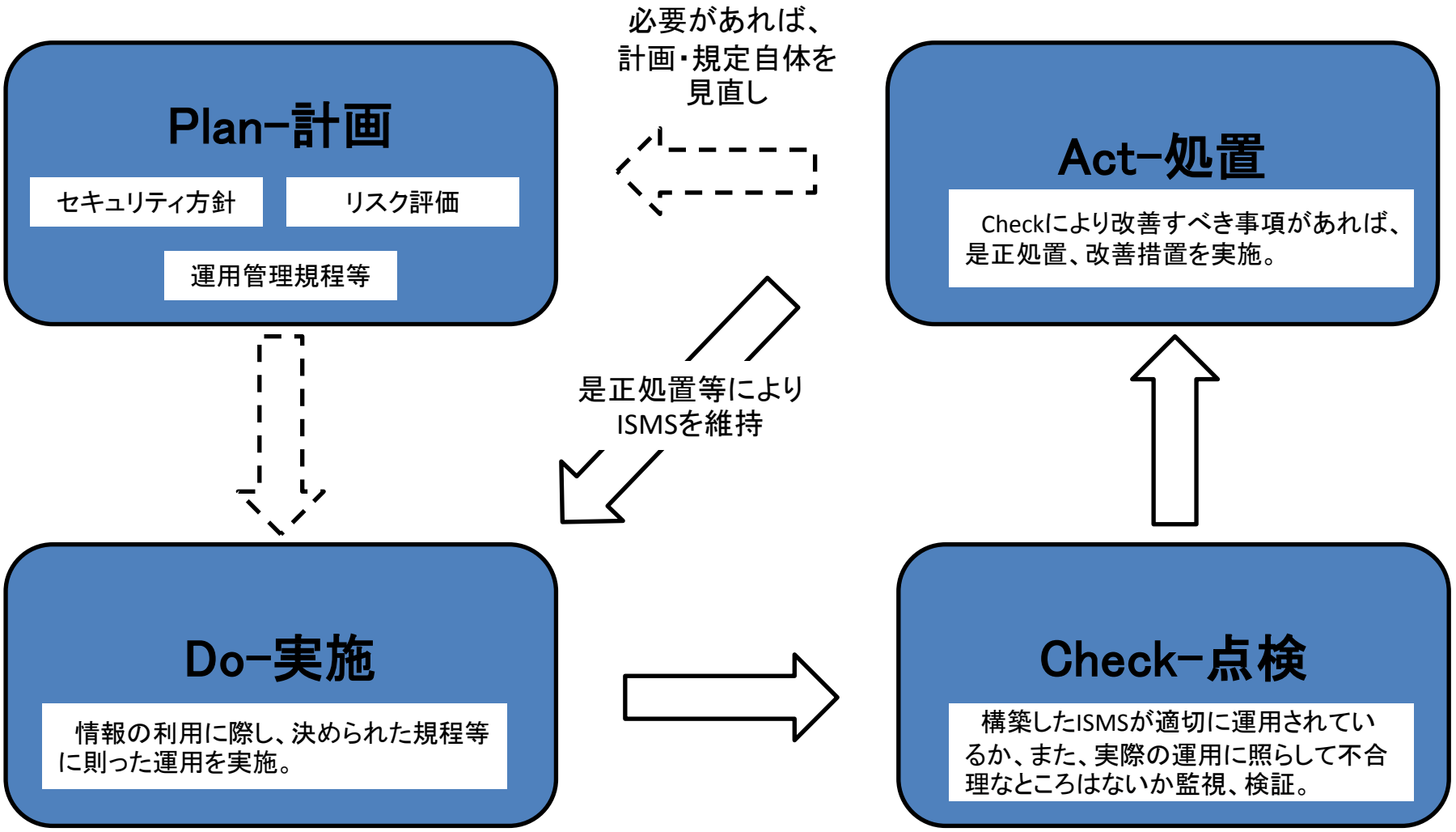
Plan-計画 （ISMSの確立）	組織の全般的方針及び目的に従った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連した、ISMS基本方針、目的、プロセス及び手順の確立
Do-実施 （ISMSの導入及び適用）	ISMS基本方針、管理策、プロセス及び手順の導入及び運用
Check-点検 （ISMSの監視及び見直し）	ISMS基本方針、目的及び実際の経験に照らした、プロセスのパフォーマンスのアセスメント（適用可能ならば測定）、及びその結果のレビューのための経営陣への報告
Act-処置 （ISMSの維持及び改善）	ISMSの継続的な改善を達成するための、ISMSの内部監査及びマネ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

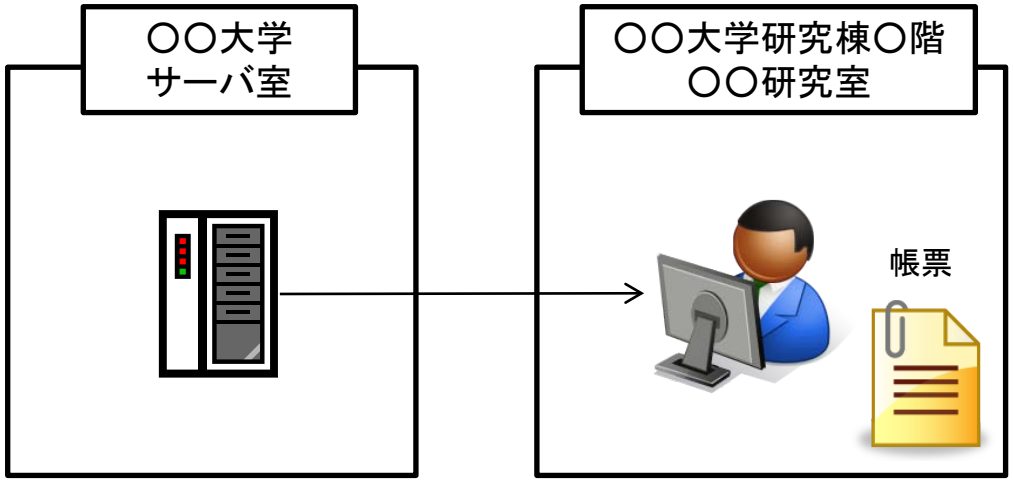
ガイドラインにおいては、第7　3（5）②として、所属機関が一般的に具備すべき条件として、ISMSの実践を挙げているが、これは、「必ずしも所属機関全体で具備する必要はなく、部、課、又は研究室等、申出者の利用形態を勘案して適切な単位で対応すること」としている。

＜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。

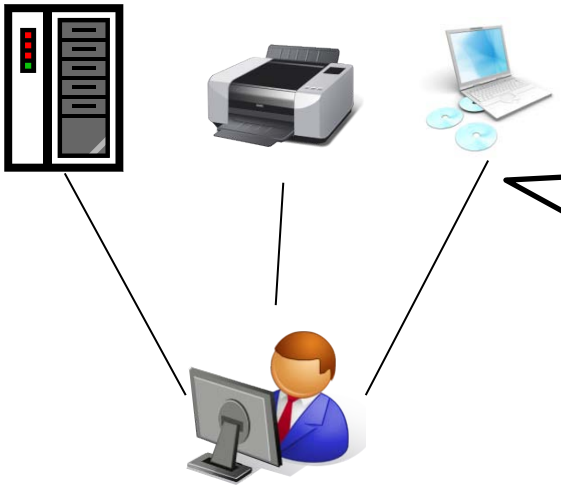
〇リストアップした情報に対してリスク分析を行っている。

＜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 ○○研究室	当該端末で研究に係る分析 を実施。	・権限のない者による不正アクセス、漏えい ・情報端末の盗難、紛失 …	・○○研究室の入退室管理 ・情報端末へのアクセス時のID認証 ・情報端末を施錠したチェーンで固定。 …	・入退室のチェック漏れ ・IDの漏えい ・チェーンの施錠し忘れ …	・定期的な第三者によるチェック ・1ヶ月毎のID変更 ・施錠のダブルチェック …
2	レセプト情報等を出力した帳票	○○大学第○研究棟 ○○研究室					
3	レセプト情報等を保存したUSB	○○大学第○研究棟 ○○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。 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。

３．セキュリティ要件について
（参考）申出書の添付書類の例

（参考例）

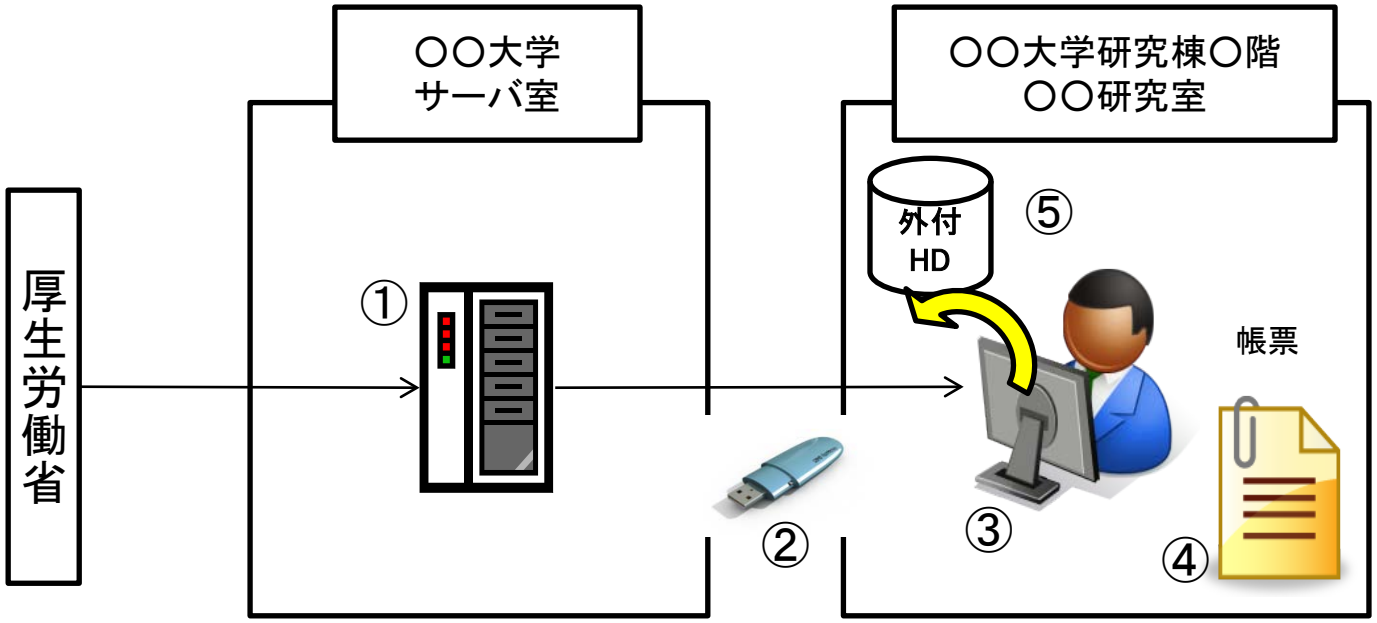
＜具体的な記載方法＞

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 ・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 ・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 ・USBにパスワードを設定。 ・使用後のUSB内データを専用ソフトで初期化 ・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 ・パスワードの設定忘れ ・USB使用後のデータ消去忘れ ・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） ・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 ・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 ・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。 ・端末にIDとパスワードを設定し、アクセスを制限 ・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 ・チェーンの施錠忘れ ・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 ・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 ○○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。 ・使用後は施錠した専用の戸棚に保管。 ・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 ・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 ○○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 ・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 ・戸棚の施錠忘れ	・2週間に1度の管理状況の確認 ・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 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 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 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 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 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 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 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 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。