平成23年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	資料3

実地検査の概要について

平成23年6月20日

厚生労働省保険局総務課

模擬的な検査の実施について

＜模擬的な検査について＞

ガイドラインや利用規約においては、厚生労働省が必要に応じて、レセプト情報等の利用状況や管理状況について、利用場所や保管場所に職員等を派遣して検査を行うことができる、としており、利用者は厚生労働省が検査を行う場合には、それに応じる義務があることを規定。

今回、模擬申出によりレセプト情報等の提供を行った松田委員の御協力を得て、今後のガイドライン等の運用のあり方の参考とするため、実際にレセプト情報等の利用場所・保管場所に職員等を派遣し、模擬的な実地検査を行った。

＜検査の目的＞

こうした模擬的検査の実施により、今後の試行的運用を行う中で、具体的な検査手順を整備することや、レセプト情報等の利用者が特に遵守しなければならない事項を明らかとし、審査における基準を明確化するとともに、必要な情報提供を行うことにより、利用者における適切な体制の整備を促すことを目的とする。

＜検査の概要＞

①日時：平成23年６月９日（木）10時～12時

②場所：産業医科大学　公衆衛生学教室

③検査の実施者：厚生労働省保険局総務課　職員２名　及び財団法人医療情報システム開発センター（MEDIS-DC）職員１名　（※）

※MEDIS-DCは、ガイドラインが準用する医療情報システムの安全管理ガイドラインに基づく医療機関への監査についても実績のある法人であり、今回、模擬的検査にあたり助言を得た。

④検査内容：

〇データの取扱の流れを確認（データの受領から、委託、利用、公表、返却・廃棄の手順など）

〇セキュリティ要件に係る文書の確認

〇実際の現場での運用状況の確認

【参考】本件のレセプト情報等の提供の流れ

23年1月20日　第４回有識者会議　模擬審査→了承

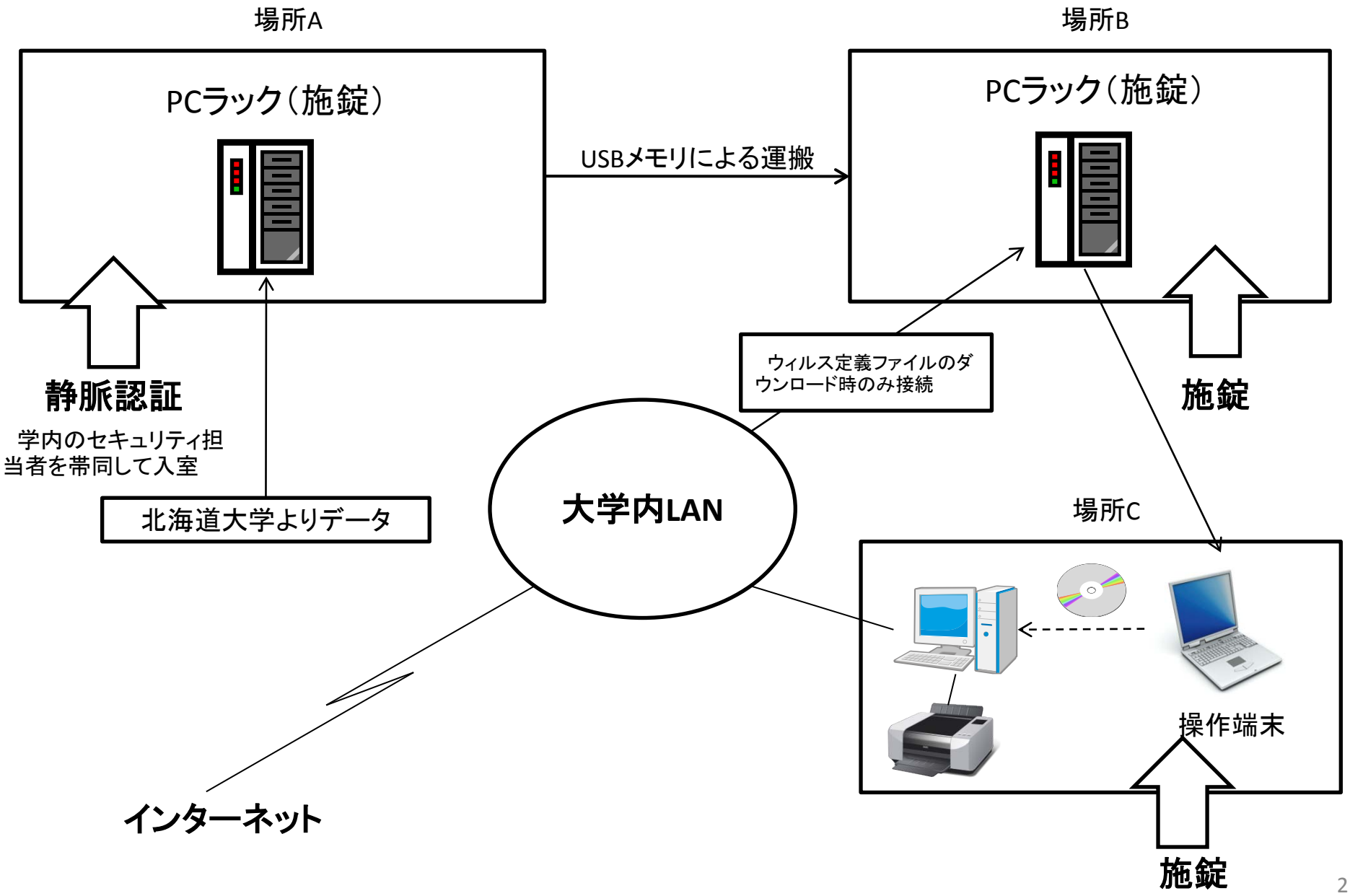
23年4月　　厚生労働省より北海道大学病院地域医療指導医支援センターに元データ提供

23年4月26日　北大より指定の形式に切り出したデータを受領（HD媒体による手渡し）

23年6月9日　　模擬的な実地検査を実施

23年6月20日　第６回有識者会議にて松田委員より途中経過の報告

利用状況の概要


場所A
PCラック（施錠）
USBメモリによる運搬
場所B
PCラック（施錠）
静脈認証
学内のセキュリティ担当者を帯同して入室
北海道大学よりデータ
ウィルス定義ファイルのダウンロード時のみ接続
施錠
大学内LAN
場所C
操作端末
インターネット
施錠

検査結果の概要

＜安全管理がなされていた点＞

〇情報の流れが双方向になることにより手順が複雑となって操作ミス等が発生するリスクを回避する観点から、情報の流れが一方向となるよう工夫がなされていた。

〇北海道大学からの元データは学内で最もセキュリティ水準の高いサーバ室内に保管しており、静脈認証による入退の制限や入退状況の管理がなされていた。また、入室には必ず学内のセキュリティ担当部署の職員が帯同することとなっており、入室する者への牽制効果になっていると考えられる。

〇場所Cにおける操作端末にはプリンタなどの周辺機器は接続しておらず、分析結果のプリンタ出力は、分析結果をCDに出力してCD経由で汎用PCよりプリンタ出力する手順を踏んでおり、汎用PCからの不正ソフトウェアの感染を防止している。

＜ガイドラインの確定を受け、今後、対応が必要と考えられる点＞

当該申出がガイドライン策定前であったことや事務局において必ずしも要件を明確にできていなかったことなどがあったことから、ガイドラインの確定を受け、今後、対応が必要と考えられる点は以下のとおり。

〇申出書において利用場所として記載されていた場所（場所A）以外の2カ所においてもデータの利用・保管を行っており、利用・保管場所の明確化が必要。

〇ガイドラインでは、管理責任の明確化等の観点から、レセプト情報等の情報システム等への複写は、前段階で複写されたものが消去されない限り原則１回のみとしている。今般の運用では、元データについては場所AのPCラックへの複写は1回のみであったが、場所AのPCラックに複写されたデータの一部を場所Bに複写し、そこから場所Cへの複写が行われていた。

〇ガイドラインでは、上記の複写制限の原則の他に、共同研究者等との間でのデータの受け渡しが必要な場合などの例外的な場合には、受け渡しに使用するUSBなどの媒体が適切に管理されることを前提にデータの持ち出しを認めているが、今回の北海道大学からのデータの受け渡しや場所Aから場所Bへのデータの運搬に使用するUSBについては、①本事業のみに使用している、②学外には持ち出さない、③通常はカギのかかる場所C内のデスクに保管されている、④作業終了後は速やかにデータを消去している、といった運用が担保されているとのことであったが、明文化された運用管理規程はなかった。これについては、データがセキュリティエリアから出た時がリスクが発生すると考えられることから、記録媒体内のデータの暗号化やデータを確実に消去するなどの手順の明確化が必要。

〇また、レセプト情報等を利用する情報システム等は、インターネット等の外部ネットワークと接続していないことを求めているが、ウィルスソフトの更新等のために一時的にインターネットに接続している状況があった。

〇場所Aのセキュリティは十分であると考えられるが、場所B及びCにおいては、入退室に関しての記録がなされていないため、少なくとも最初に解錠した時刻・人、最後に施錠した時刻・人を記録することが必要と考えられる。

〇個人情報保護法への対応に関する文書化されたルールはあるが、データの安全管理に関する運用規程はなく、また、情報セキュリティマネジメントシステムの実践や災害等の非常時への対応についても、利用実態に応じた何らかの対応が必要と考えられる。

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＞

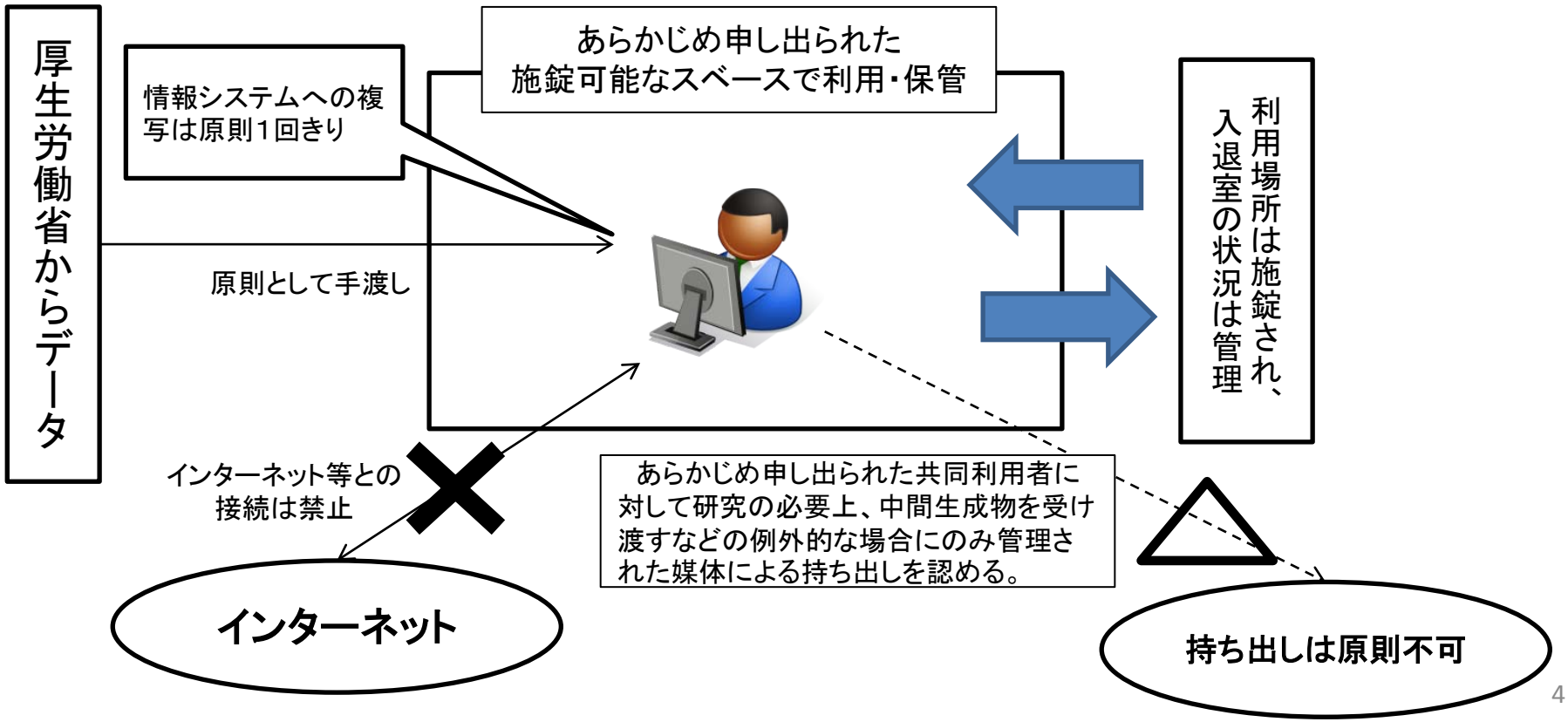
○提供したレセプト情報等の情報システム等への複写は、前段階でのデータが消去されない限り、原則1回のみ。この原則は、厚生労働省から提供されたレセプト情報等の元データだけでなく当該元データから作成される全ての中間生成物も含め適用される。

○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。



模擬的検査を踏まえた対応

＜今後の運用について＞

○申出の段階で、申出者から2ページのような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のではないか。

○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てはどうか。

○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、本件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、例外として認めることとしてはどうか。

○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のではないか。

○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か。

（参考）セキュリティ要件の具体例

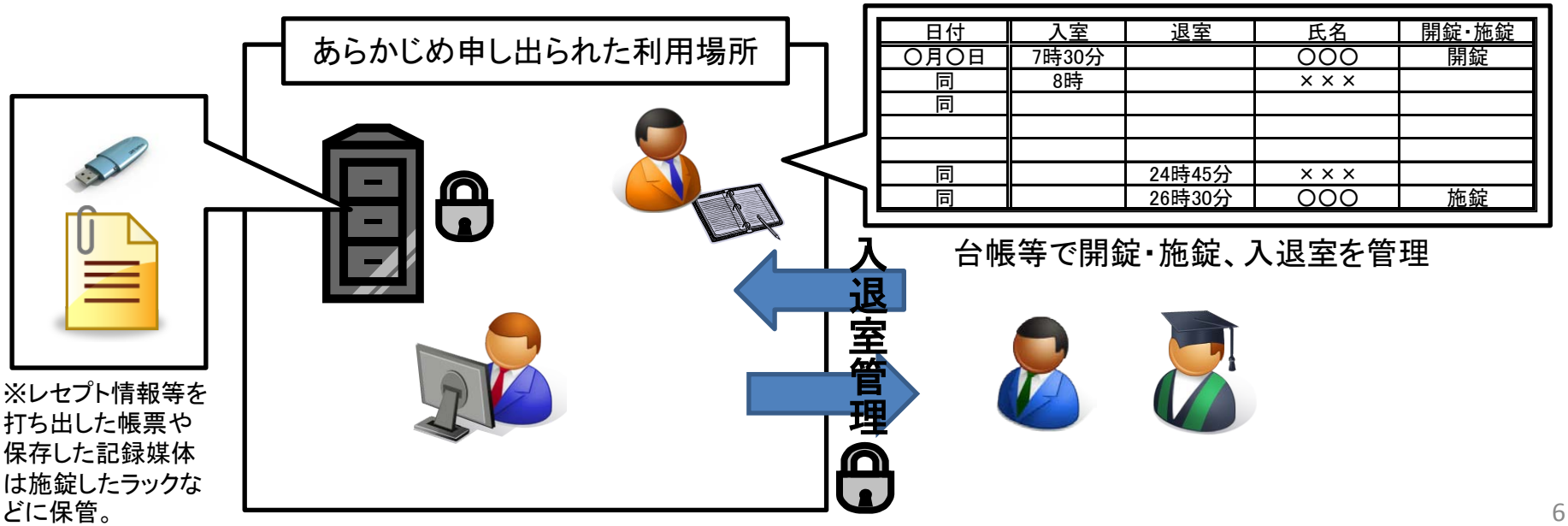
＜入退室の管理等＞（ガイドライン第7　3（5）③（i）a)c））

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

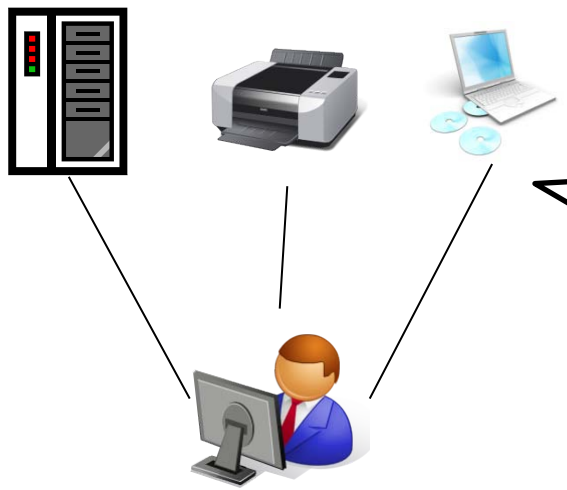
＜所属機関の情報セキュリティマネジメントシステムの実践＞（ガイドライン第7　（5）①ⅱ））
※研究室単位など合理的な範囲内で設定することも可。

○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。
○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。
○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。

○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情報を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.	情報名	運用状況 使用目的	重要度	脅威	脆弱性	リスク値	リスク対策
1	レセプト情報等		3	3	3	27	
2	××		3	1	1	3	
3	○○		3	2	1	6	
4			2	1	1	2	
5			2	1	1	2	
6						0	

＜リスク分析の例＞
情報の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。
各情報に応じて想定されるリスクへの対策をリスト化。

＜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。

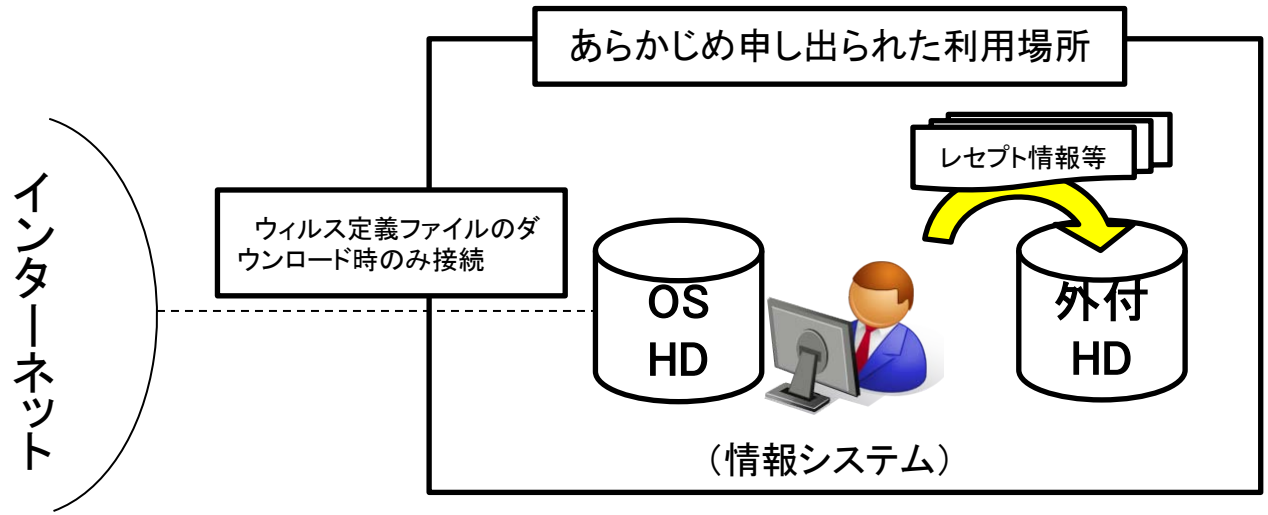
＜具体例＞

※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を講じ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。