

2 サンプリングデータセットにおける 利用環境のあり方について

サンプリングデータセットの適切な利用環境を 検討するにあたっての論点(案): 有識者会議の議論より

考え方

✓ 【利用場所について】

サンプリングデータセットが非常に匿名性の高いデータであることを踏まえ、データ利用場所における厳密な入退室管理までは求めないこととしてよいのではないかと。但し、利用の場所を定めることや、施錠等を行うなどデータの盗難を防止する体制を整えることについては、求めてはどうか。

✓ 【外部ネットワークとの接続について】

利用者が想定しない状況で情報が外部に流出する可能性を否定できないので、外部ネットワークとの接続は、引き続き認めないこととする。

✓ 【アクセス記録について】

サンプリングデータセットは非常に匿名性の高いデータではあるが、データの利用者は限定していることから、利用者のアクセス記録は残すことを求めてはどうか。

✓ 【データの管理について】

サンプリングデータセットが非常に匿名性の高いデータであることから、データについては最低限の盗難防止措置を求めるものの、それらの管理状況を追跡できるようにすることまでは求めないこととしてはどうか。

✓ 【中間生成物の取り扱いについて】

サンプリングデータセットが非常に匿名性の高いデータであること、および公表基準の適用を認めないこととしていることを踏まえ、集計された帳票形式の中間生成物については、規定を設けなくてもよいのではないかと。

データの位置づけや用語の統一について

今後の議論をすすめていくにあたり、これまでは事務局より提供される情報は一律「レセプト情報・特定健診等情報データベース」より提供しているデータとして扱われてきたが、サンプリングデータセット等、さまざまなデータセットが徐々に整備されてきていることから、その位置づけや用語について、以下のように位置づけなおしてみようか。

	用語	位置づけ
既存の整理	レセプト情報・特定健診等情報データベース 略称:レセプト情報等データベース 略称:ナショナルデータベース 略称:NDB	<ul style="list-style-type: none"> 高齢者の医療の確保に関する法律に基づき、国が収集した特定健診・特定保健指導(特定健診等)情報ならびにレセプト情報全般
	レセプト情報・特定健診等情報 略称:レセプト情報等 略称:NDBデータ	<ul style="list-style-type: none"> レセプト情報・特定健診等情報データベースに含まれている、個別の情報
	集計表情報	<ul style="list-style-type: none"> NDBデータを用い、事務局・データセンターにおいて提供依頼申出者の要望に応じて集計処理を施し、集計表形式に加工された状態で提供される情報 <ul style="list-style-type: none"> 第17回有識者会議において、「サンプリングデータセット」と同等のセキュリティ要件のもとで利用するよう定められた。
今回新たに提案	レセプト情報等簡易データ(仮) 略称:簡易データ(仮)	<ul style="list-style-type: none"> NDBデータを用い、研究者等が簡易に利用できるよう加工を施したデータ <ul style="list-style-type: none"> レセプト情報等簡易データとして、現在「サンプリングデータセット」および「基本データセット」がある 特定健診等情報の簡易データは、いまのところ準備されていない 現在、有識者会議で、簡易データ利用時の適切なセキュリティ要件のあり方について議論がなされているところ
	レセプト情報等簡易データ情報(仮) 略称:簡易データ情報(仮)	<ul style="list-style-type: none"> レセプト情報等簡易データに含まれている、個別の情報
	簡易データセット情報等(仮)	<ul style="list-style-type: none"> サンプリングデータセット情報や基本データセット情報といった簡易データ情報、および集計表情報の提供に際して同一のセキュリティ要件を求めることとしていることに則った、これらの情報の総称
	定型表情報	<ul style="list-style-type: none"> 現在、有識者会議で検討課題となっているところ

サンプリングデータセットの適切な利用環境を 検討するにあたっての論点：申出書の項目より①

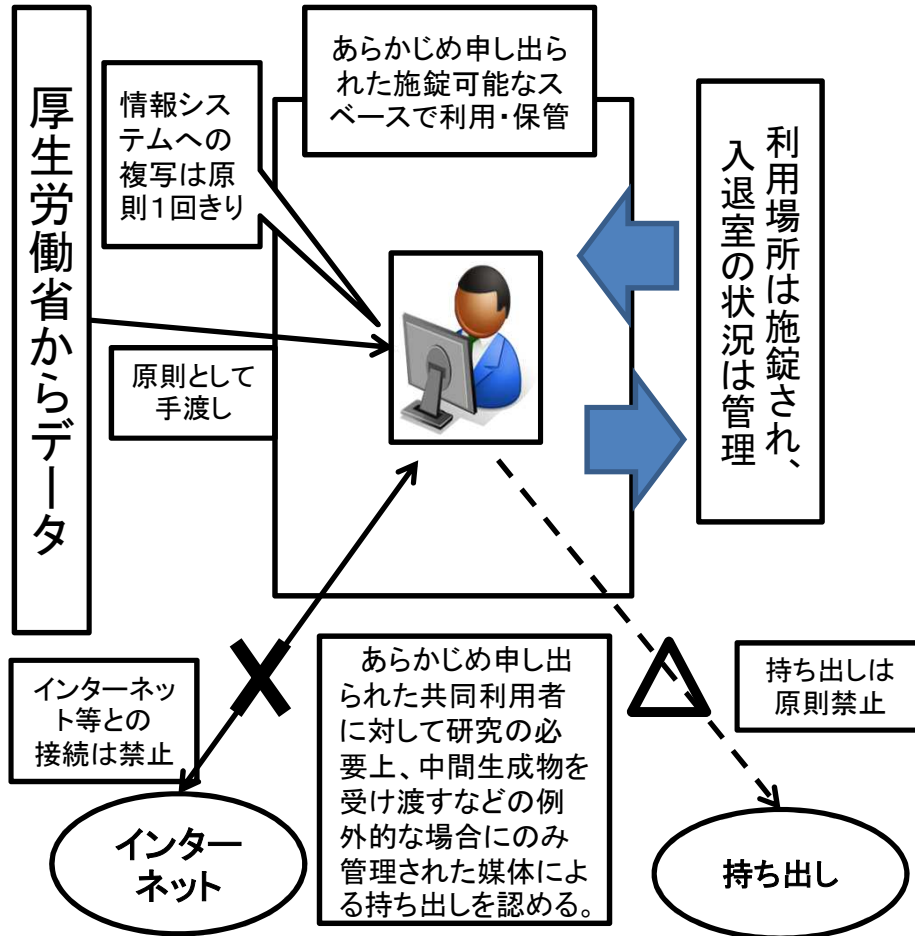
	確認項目	現行のセキュリティ要件（要約）	主な論点
① 基本的な事項	利用場所	国内	データの盗難を防止する対応を求める観点から、現行の要件と同等としてはどうか
	利用場所の範囲	施錠可能なスペースに限定 原則として持ち出されない	
	ネットワークとの接続	外部ネットワークに接続しない	
	利用者	申し出られた利用者のみ	
② 本データの利用に限らず所属機関が一般的に具備すべき条件 (必ずしも所属機関全体で具備する必要はなく、部、課又は 研究室等、申出者の利用形態を勘案して適切な単位で対応)	個人情報保護方針	策定、公開していること 情報システムの安全管理方針も策定していること 提供されるレセプト情報等についてもそれに従うこと	所属機関における個人情報保護方針の有無については、引き続き確認することとしてはどうか 運用管理規程等の整備など、情報セキュリティマネジメントシステムの運用は引き続き求めることとし、現行の要件と同等としてはどうか。ただし、サンプリングデータセットのデータが「実質的個人識別性」のないデータと位置づけられることに鑑み、入退管理の取扱い等、個人情報に準ずる情報の取扱いに関する規程までは求めない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	情報をすべてリストアップしていること リストアップした情報を最新の状態に維持していること このリストをきちんと管理していること リスク分析を実施していること 得られた脅威に対して対策を行っていること	
	組織的安全対策の実施	運用責任者の限定を行うこと 入退管理を定めること アクセス管理規程を定めること 委託時には安全管理の条項を含めること 運用管理規程を定めること	
	人的安全対策の措置	個人情報の安全管理が適切に実施されるよう措置する 事務を外部業者に委託する際には適切な除塵情報保護が行われる措置をとること 外部の保守要員がアクセスする際は、秘密保持の対策を行うこと	
	情報破棄の手順設定	破棄の手順を定めること 破棄する場合は専門知識を有する者が行うこと 外部委託する場合は、安全対策を講ずること	
	運用管理について	申出事項が運用管理規程等に含まれていること	

サンプリングデータセットの適切な利用環境を 検討するにあたっての論点：申出書の項目より②

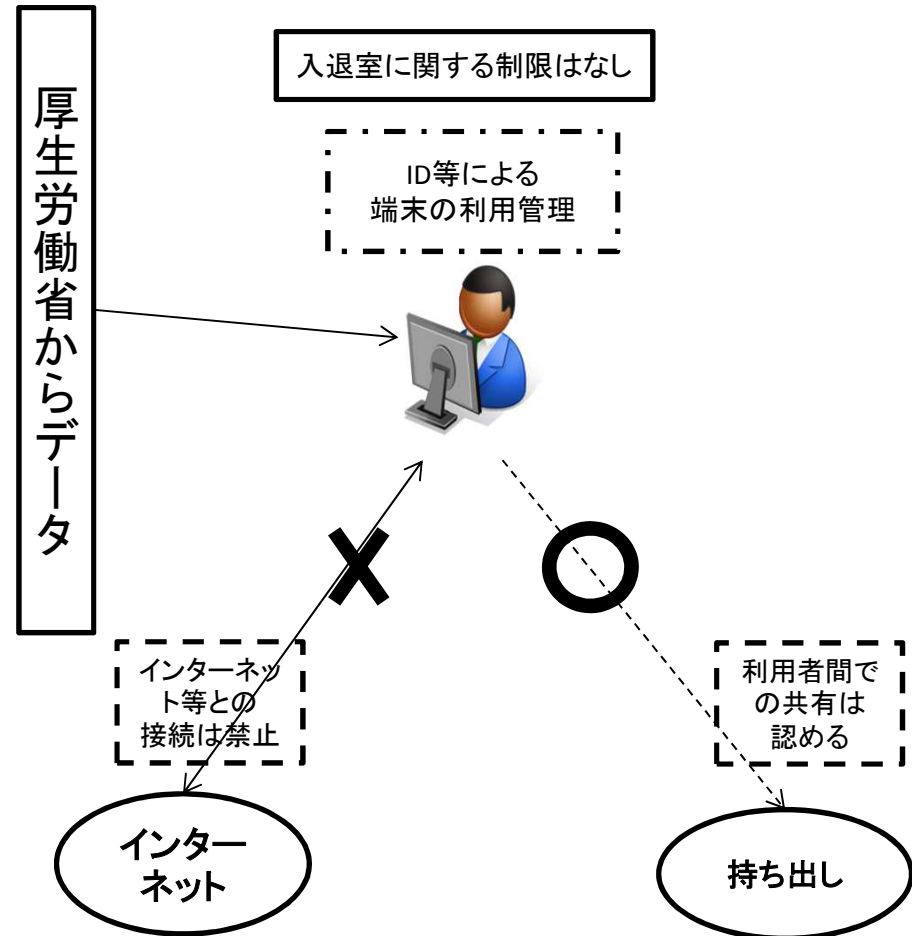
確認項目	現行のセキュリティ要件（要約）	主な論点	
③本データの利用に際し具備すべき条件（必ずしも所属機関全体で具備する必要はなく、部、課又は研究室等、申出者の利用形態を勘案して適切な単位で対応）	物理的安全対策	「厳密な入退室管理を求めない」 「窃視に関する規定を求めない」 「最低限、操作端末へのアクセス記録を残す」 等、サンプリングデータセットのデータが「実質的個人識別性」のないデータと位置づけられうることに鑑み、個人情報に準ずる情報の取扱いに関する規定までは求めないこととしてはどうか	
	技術的安全対策		機器の設置場所、記録媒体保存場所は施錠すること 業務外の時間には立ち入ることができないこと 入退管理を実施すること 盗難防止チェーンを装着すること 窃視防止対策をとること 利用者の識別と認証を行うこと パスワードは、本人しか知りえない状態に保つこと スクリーンセーバーを設置すること 利用者のログイン時刻、アクセス時間等を記録し、利用者が特定できるようにしておくこと アクセス記録機能がない場合は、業務日誌で操作記録を必ず行うこと アクセスログへのアクセス制限を行うこと 適切に管理されていないメディアを接続しないこと パスワードは厳密に管理すること インターネットに接続しないこと 利用後は中間生成物を含め消去すること
	情報及び情報機器の持ち出しについて		あらかじめ申し出られた場所のみで行い、外部での持ち出しを行わないこと 持ち出す場合は、組織としてリスク分析を実施していること、運用管理規程で管理方法を定めること、情報機器の盗難、紛失時の対応を管理規程等に定めること、利用者間に教育を行うこと、台帳等を用いた情報機器所在の把握を行うこと、パスワードを設定すること、等々

サンプリングデータセットの利用形態について(案)

現在の利用形態(抽出データと同じ)



米国FTCの考え方、第17回有識者会議の議論等を踏まえた利用形態の一例



上述の模式図に加えて.....

- ・利用場所は限定し、空間および利用端末の施錠管理は行う
- ・利用端末のアクセスログ記録は残す

サンプリングデータセットの申出手続きについて(案)

別添番号	準備書類題目	現在の申出手続き	米国FTCの考え方、第17回有識者会議の議論等を踏まえた申出手続きの一例
	レセプト情報等の提供に関する申出書(様式1)	必須	必須
別添1	本人確認	必須	必須
	レセプト情報等を利用した研究に関する承認書(様式1-1)	必須	必須
別添2	別添2-1 運用フロー図	必須	情報セキュリティマネジメントシステムの運用は引き続き求めることとしていることから、 <u>これらの書類は、サンプリングデータセットの申出時にも求めることとしてはどうか</u>
	別添2-2 リスク分析・対応表	必須	
	別添2-3 運用管理規程	必須	
	別添2-4 自己点検規程	必須	
別添3	所属組織の個人情報保護に関する規程(プライバシーポリシー、情報セキュリティポリシーなど。複数ある場合は、3-1, 3-2…と付番して提出)	任意	任意
別添4	厚労科研交付通知など、公共性の高い研究であることを示唆する書類	任意	任意
別添5	提供依頼申出者における過去の研究実績を証明するもの(論文の写し等)	任意	任意
別添6	外部委託があれば、守秘義務契約の写し	該当時必須	該当時必須
別添7	倫理委員会承諾書	必須	「実質的個人識別性」のないデータと位置づけられうることから、 <u>申出においては必ずしも提出を求めなくてもよいのではない</u> か。但し、所属機関において円滑に研究を行う上で必要と判断される場合は、適宜倫理委員会に諮ることを妨げるものではない
別添8	詳細な抽出条件	不要	不要
別添9	詳細な公表形式	必須	「実質的個人識別性」のないデータとして位置づけられうることや、探索的研究を認めていることなどから、 <u>詳細な公表形式を申出時に提出することは求めなくてもよいのではない</u> か
	その他適宜必要な書類 (添付の際は「別添10」「別添11」…と番号を振っていただき、どういった書類かを明記して下さい)	必要時添付	必要時添付