

参考：サンプリングデータセットにおける
具体的な利用環境の一例、および
その利用環境に即した各種規程の例について

運用フロー図の例

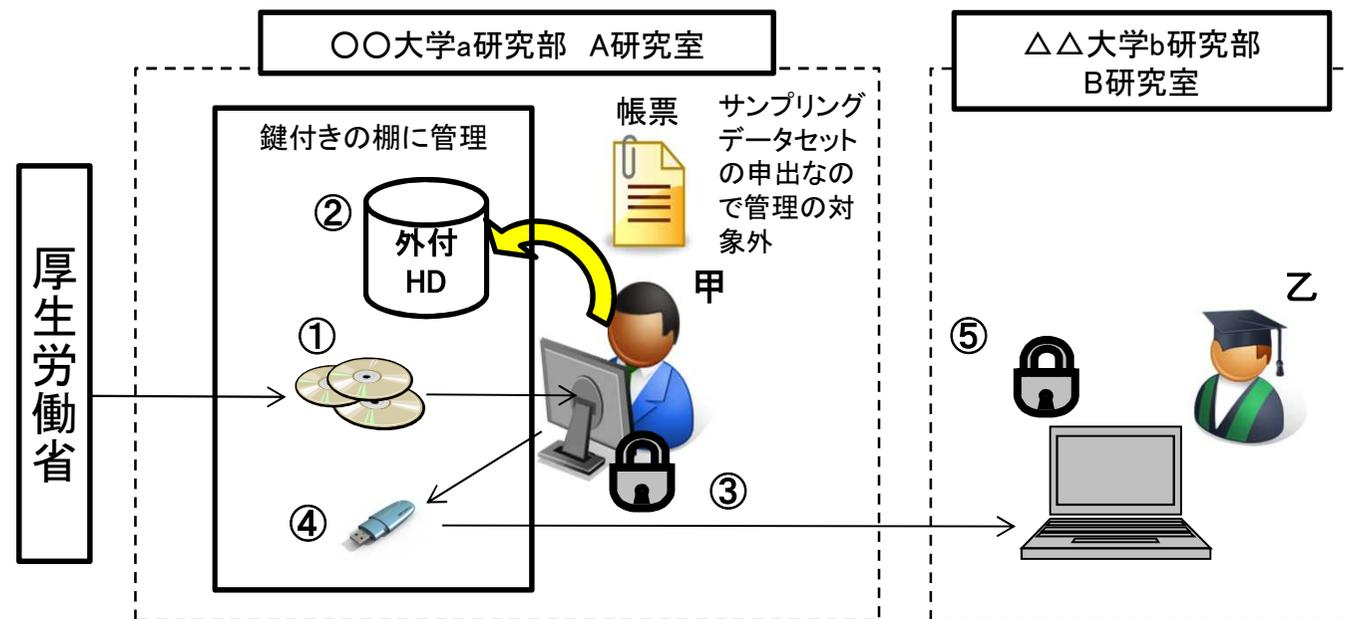
<具体的な記載方法>

サンプリングデータセット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>

- 簡易データ情報等の利用者は、2施設にまたがっており、合計2名（甲および乙）。
※あくまでもひとつの例として述べるものであり、2施設にまたがることを求めるものではない。
- 厚生労働省から提供を受けた簡易データ情報等をA研究室、B研究室にある操作端末に保存。
- 作成した中間生成物のうち、紙媒体で出力した分析用の帳票については特段の管理は行わない。
- 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。
- 両研究機関での情報のやりとりは、パスワードロック機能を備えたUSBを用いて運搬する。

【運用フロー図の例】



※本ケースにおける簡易データ情報の形態は5パターン。

- ① 厚生労働省より受領したサンプリングデータセットの電子媒体
- ② 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
- ③ A研究室の、施錠された操作端末内に保存された電磁的データ
- ④ A研究室とB研究室とで情報のやりとりを行う際のUSB媒体
- ⑤ B研究室の、施錠された操作端末内に保存された電磁的データ

リスク分析・対応表の例

運用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	厚生労働省より受領したサンプリングデータセットの電子媒体	〇〇大学a研究部 A研究室、管理棚	データを操作端末に複製した後、データの原本として保存。	・盗難、紛失による漏えい	・施錠可能な管理棚にて管理 ・盗難時に読み取られるリスクに対し、パスワードを設定して管理	・施錠忘れ	・1～2ヶ月に一度、左記管理の実施が確実になされているかどうか確認
②	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	〇〇大学a研究部 A研究室、管理棚	操作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。	・盗難、紛失による漏えい	・施錠可能な管理棚にて管理 ・盗難時に読み取られるリスクに対し、パスワードを設定して管理	・施錠忘れ	・1～2ヶ月に一度、左記管理の実施が確実になされているかどうか確認
③	A研究室の、施錠された操作端末内に保存された電磁的データ	〇〇大学a研究部 A研究室	厚労省から提供されたサンプリングデータセットから複製したデータを分析	・盗難、紛失による漏えい ・操作端末内への不正アクセスによる漏えい	・持ち運びできないよう操作端末について施錠したチェーンにより固定。 ・操作端末に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	・ID・パスワードの設定不備による、他者の情報アクセス	・1～2ヶ月に一度、左記管理の実施が確実になされているかどうか確認 ・ログ記録の保存
④	A研究室とB研究室とで情報のやりとりを行う際のUSB媒体	〇〇大学a研究部 A研究室、管理棚	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〇〇研究室へ運搬。	・盗難、紛失による漏えい	・施錠可能な管理棚にて管理 ・盗難時に読み取られるリスクに対し、パスワードを設定して管理	・施錠忘れ	・1～2ヶ月に一度、左記管理の実施が確実になされているかどうか確認
⑤	B研究室の、施錠された操作端末内に保存された電磁的データ	△△大学b研究部 B研究室	厚労省から提供されたサンプリングデータセットから複製したデータを分析	・盗難、紛失による漏えい ・操作端末内への不正アクセスによる漏えい	・持ち運びできないよう操作端末について施錠したチェーンにより固定。 ・操作端末に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	・ID・パスワードの設定不備による、他者の情報アクセス	・1～2ヶ月に一度、左記管理の実施が確実になされているかどうか確認 ・ログ記録の保存

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。

運用管理規程の例

簡易データ情報等の利用に当たっての運用管理規程

平成26年〇月〇日 〇〇大学a研究部

平成26年〇月〇日 △△大学b研究部

1. 目的

厚生労働省から提供を受けた簡易データ情報等の利用者が、情報セキュリティおよび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簡易データ情報等のデータとそれから派生する全ての電子情報化された中間生成物を対象とし、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

簡易データ情報等の利用者は、甲、乙のみとし、その他の者は、簡易データ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

- ・簡易データ情報等の利用場所は、〇〇大学a研究部 A研究室および△△大学b研究部 B研究室のみとする。
- ・簡易データ情報等の保管場所は、〇〇大学a研究部 A研究室および△△大学b研究部 B研究室のみとする。

(3) 利用・保管方法

- ・A研究室およびB研究室においては、操作端末内、および中間生成物を保存する外付けハードディスク、A研究室とB研究室の間で簡易データ情報等を運搬するUSB(注:いずれも管理番号・型番等、情報機器を特定する情報が必要)といった記録媒体に対しパスワードロック、及び施錠管理(操作端末の施錠及び記録媒体の戸棚管理)にて保管を行う。
- ・操作端末には個人IDとパスワードを設定し、甲、乙以外の者がアクセスできないこととする。
- ・操作端末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、特定された媒体以外の記録媒体を接続してはならない。

(4) データの持ち出しについて

- ・ A研究室とB研究室間で情報を運搬する場合は、あらかじめ特定されたUSBを用いて行う。

(5) データの返還・廃棄

- ・ 簡易データ情報等の利用後は、厚生労働省から提供を受けた媒体は、厚生労働省へ返還すること。その他、操作端末および記録媒体に残存している簡易データ情報等については、確実に廃棄すること。
- ・ 記録媒体については物理的に破壊し、破壊したことの証明(例:写真画像等)を添えて措置報告を行うこと。
- ・ 操作端末内に保存されたレセプト情報等については、市販ソフトによる物理的フォーマットの上、措置報告を行うこと。

(6) データの返還・廃棄

- ・ 簡易データ情報等の利用期間中に操作端末や情報機器に不具合が発生した場合は、利用者において修復すること。
- ・ 修復ができない場合、操作端末はハードディスクを交換したうえで廃棄証明を添えて、措置報告を行うこと。記録媒体については物理的に破壊し、破壊したことの証明(例:写真画像等)を添えて措置報告を行うこと。

(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、操作端末へのアクセスログは、簡易データ情報等の利用期間終了後、1年間保存すること。
- ・ 簡易データ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、簡易データ情報等の利用期間終了後、1年間保存すること。

4. 自己点検

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、「簡易データ情報等の利用に当たっての自己点検規程」を作成する。

厚生労働省から、利用状況について簡易データ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

簡易データ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、原則として甲が対応することとする。

(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	サンプリングデータセットを利用した学術研究	厚生労働省から提供を受けた簡易データ情報等を利用して行う〇〇に関する分析・研究事業	申出書 運用管理規程
2	適用組織	〇〇大学a研究部	簡易データ情報等を用いた分析業務	運用フロー図
		△△大学b研究部	簡易データ情報等を用いた分析業務	運用フロー図
3	場所	〇〇大学a研究部 A研究室	簡易データ情報等を利用した分析を実施	運用フロー図
		△△大学b研究部 B研究室	簡易データ情報等を利用した分析を実施	運用フロー図
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	運用フロー図 運用管理規程
5	情報資産	A研究室の管理棚に格納されているサンプリングデータセット、外付けハードディスク、USB	簡易データ情報等の保存および運搬	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
		A研究室の操作端末	実際の簡易データ情報等の分析に使用	
		B研究室の操作端末	実際の簡易データ情報等の分析に使用	

自己点検規程の例

簡易データ情報等の利用についての自己点検規程

平成26年〇月〇日 〇〇大学a研究部
平成26年〇月〇日 △△大学b研究部

1. 目的

この規程は、厚生労働省から提供された簡易データ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

- ・A研究室に対して行う際は、乙が本規程の定める点検を行うこととし、甲がその実施に立ち会うこととする。
- ・B研究室に対して行う際は、甲が本規程の定める点検を行うこととし、乙がその実施に立ち会うこととする。

3. 点検の方法

- ・以下の点検を、1～2ヶ月に1度行う。
- ・A研究室、B研究室内の操作端末がチェーン等で施錠されていることを確認する。
- ・A研究室の管理棚が施錠されていることを確認するとともに、外付けハードディスクおよびUSBは、使用されていない時に所定の場所に保管されていることを確認する。
- ・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。
- ・操作端末のアクセスログを確認する。

4. 点検結果の記録

甲及び乙は、本規程の点検を行った日、時間を記録し、簡易データ情報等の利用期間終了後、1年間保存すること。

○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。

自己点検チェックリストの例

自己点検日	実施者	適用組織(いずれかに○をつける)	前回点検日
〇〇年〇月〇日	□□ □□	〇〇大学a研究部、 △△大学b研究部	〇〇年△月△日

自己点検を行う事項	チェックの結果(○か×をつける)
自己点検の間隔は守れているか	
操作端末は施錠で固定されているか	
管理棚は施錠されているか	
外付けハードディスクは管理棚に保管されているか	
USBは管理棚に保管されているか	
操作端末はインターネットに接続されていないか	
操作端末のアクセスログを確認することができるか	
操作端末にはパスワード管理できているか	
操作端末は他者のアクセスがないか確認できたか	
外付けハードディスクはパスワード管理できているか	
USBはパスワード管理できているか	

自己点検結果	各種規程への反映が必要と思われる問題点があれば記載	その他特記事項	次回点検予定日
(問題なし、 問題あり)			〇〇年□月□日頃

○ここで記載したリストはあくまで一例であり、各自の研究環境において情報セキュリティマネジメントシステムが運用となるよう、実行可能かつ適切な自己点検チェックリストを定められたい。

適用宣言書の例

- 上述のセキュリティをデータ提供を受けるまでに実質的に確保できない場合は、これらの書類を作成したうえで、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簡易データ情報等の提供を受けることを可能としている。
- 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簡易データ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。
- 今後、簡易データ情報の提供に関する規定がガイドライン等で整備されるまでは、「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」ならびに本有識者会議での議論に準拠して、セキュリティに対する審査が行われる。

厚生労働大臣 殿

簡易データ情報等の提供に関するガイドラインの適用宣言書

平成26年〇月〇日

〇〇大学a研究部 教授 〇〇 〇〇

私は、簡易データ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。