

背景資料 1 ミクロデータ提供に係る現行の制度（概要）

法的根拠（統計法）		利用目的	利用できる者（統計法施行規則）	手数料	提供方法	公表
第32条 調査票情報の利用	調査実施者が行う統計の作成等	<ul style="list-style-type: none"> ✓ 統計の作成等、調査名簿の作成 ✓ 利用例：府省内での利用 	<ul style="list-style-type: none"> ✓ 調査実施者（行政機関、指定独立行政法人等（※1）） 	無料	DVD等・オンサイト	なし
第33条第1項第1号 調査票情報の提供	公的機関等が行う統計の作成等	<ul style="list-style-type: none"> ✓ 統計の作成等、調査名簿の作成 ✓ 利用例：地方自治体による統計の作成 	<ul style="list-style-type: none"> ✓ 公的機関等（※2）が利用する場合 			
第33条第1項第2号 調査票情報の提供	公的機関等 が行う統計の作成等 と同等の公益性 を有する統計の作成等	<ul style="list-style-type: none"> ✓ 統計の作成等 ✓ 利用例：科研費の補助を受けて行う研究 	<ul style="list-style-type: none"> ✓ 公的機関等が委託又は共同して調査研究を行う者 ✓ 公的機関等が公募の方法により補助する調査研究を行う者 ✓ 行政機関等が政策の企画・立案、実施又は評価に有用であると認める統計の作成等を行う者 		DVD等・オンサイト・リモートアクセス	必要
第33条の2 調査票情報の提供	相当の公益性 を有する統計の作成等	<ul style="list-style-type: none"> ✓ 統計の作成等 ✓ 利用例：大学に所属する教員の行う研究 	<ul style="list-style-type: none"> ✓ 学術研究の発展に資する統計の作成等を行う者 <ul style="list-style-type: none"> ・大学等、公益社団法人又は公益財団法人（公益目的事業に限る）が行う調査研究 ・大学等に所属する教員が行う調査研究 ・大学等、公益社団法人又は公益財団法人が公募の方法により補助する調査研究 ✓ 高等教育の発展に資する統計の作成等を行う者 	有料	オンサイト	必要
第34条 オーダーメイド集計	相当の公益性 を有する統計の作成等	<ul style="list-style-type: none"> ✓ 統計の作成等 	<ul style="list-style-type: none"> ✓ 学術研究の発展に資する統計の作成等を行う者 ✓ 教育の発展に資する統計の作成等を行う者 ✓ デジタル社会形成基本法に規定する特定公共分野に係る統計の作成等を行う者 		DVD等	
第36条 匿名データの提供	相当の公益性 を有する統計の作成等	<ul style="list-style-type: none"> ✓ 統計の作成等 	<ul style="list-style-type: none"> ✓ 上記と同様 ✓ 国際社会における我が国の利益の増進及び国際経済社会の健全な発展に資すると認められる統計の作成等を行う者 		DVD等	

※1：指定独立行政法人等について、現在は日本銀行のみが該当する。

※2：行政機関、地方自治体、独立行政法人等、会計検査院、地方独立行政法人、地方住宅供給公社、地方道路公社、土地開発公社（これらをまとめて「公的機関等」という。）

平成30年の統計法の改正により、提供範囲を拡大（令和元年5月から施行）

背景資料 1 ミクロデータ提供に係る現行の制度（概要）

利用形態	提供される項目	概要	利用者		
			法第33条第1項第1号 (行政機関・自治体等)	法第33条第1項第2号 (科研費の補助を受けた行う 研究等)	法第33条の2第1項 (大学に所属する教員の行う 研究等)
オンサイト利用	全項目 (探索型)	セキュリティが確保されたオンサイト施設から、遠隔にあるセキュリティが確保された環境にある調査票情報が利用可能	可	可	可
リモートアクセス	研究等に必要項目	利用者自身の拠点（研究室や自宅等）から、インターネット回線を経由して遠隔にあるセキュリティが確保された環境にある調査票情報が利用可能。研究室等のセキュリティは利用者自身で確保する必要がある。	不可（※）	可	不可
電磁的記録媒体による提供	研究等に必要項目	研究室等において、研究者自身のPC等で調査票情報を利用することができる。セキュリティの確保は利用者自身の責任。	可	可	不可

※ 「リモートアクセス」は、当面の間は法第33条第1項第2号による申出のみ利用可能。

背景資料 1 調査票情報等の利用実績

区分	調査票情報の提供				オーダーメイド集計		匿名データの提供	
	法第32条	法第33条 第1項第1号	法第33条 第1項第2号	法第33条の 2	利用可能数 (注4)	利用件数	利用可能数 (注4)	利用件数
平成22年度	646	2,975	133	—	20 (87)	12	4 (13)	38
平成23年度	729	2,647	148	—	23 (119)	10	6 (34)	33
平成24年度	625	2,478	169	—	24 (155)	19	6 (36)	32
平成25年度	643	2,504	244	—	26 (203)	13	7 (40)	41
平成26年度	628	2,437	281	—	26 (239)	29	7 (41)	37
平成27年度	596	2,585	267	—	26 (259)	22	7 (43)	39
平成28年度	579	2,586	324	—	26 (278)	17	7 (45)	39
平成29年度	662	2,584	369	—	28 (300)	25	7 (46)	45
平成30年度	613	2,358	382	—	28 (313)	22	7 (50)	49
令和元年度	674	2,000	218	11	30 (335)	35	7 (52)	26
令和2年度	657	2,086	298	10	30 (360)	19	7 (57)	32
令和3年度	674	2,169	278	12	30 (377)	26	7 (66)	21
令和4年度	629	2,206	284	11	30 (394)	21	7 (68)	46
令和5年度	671	2,333	352	9	31 (417)	21	8 (73)	39
令和6年度	688	1,940	302	17	31 (435)	27	8 (76)	36

(注) 1 数値は、統計法施行状況報告に基づく。

2 法第33条第1項第1号は、公的機関が利用する場合、法第33条第1項第2号は、公的機関が公募の方法により補助する調査研究を行う者等が利用する場合。

3 法第33条の2については平成30年の統計法改正により新設されたため、令和元年度から実績を記載している。

4 利用可能数欄の括弧内の数値は、1年次を1調査としてカウントした場合の数。

背景資料 1 ミクロデータ提供実績（R6年度）

各府省	法第32条	法第33条 第1項第1号	法第33条 第1項第2号	法第33条の2	オーダーメイド	匿名データ
内閣府	3	3	3			
こども家庭庁		2	1			
総務省	26	155	69	7	16	28
財務省	7	13	3			
文部科学省	104	174	17	1		
厚生労働省	175	834	118	7	5	8
農林水産省	138	44	6			
経済産業省	101	467	35	1		
国土交通省	133	239	45	1	5	
環境省	1	9	5			
日本銀行					1	
合計	688	1,940	302	17	27	36

背景資料 1 オンサイト施設におけるマイクロデータの利用

イメージ

オンサイト施設



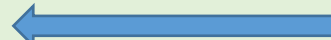
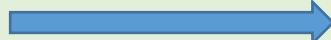
すべての調査項目を利用した探索的、創造的な分析・研究を行うことが可能。

26施設（令和8年5月時点）

オンサイト施設一覧



遠隔操作



仮想PCの画面のみを転送

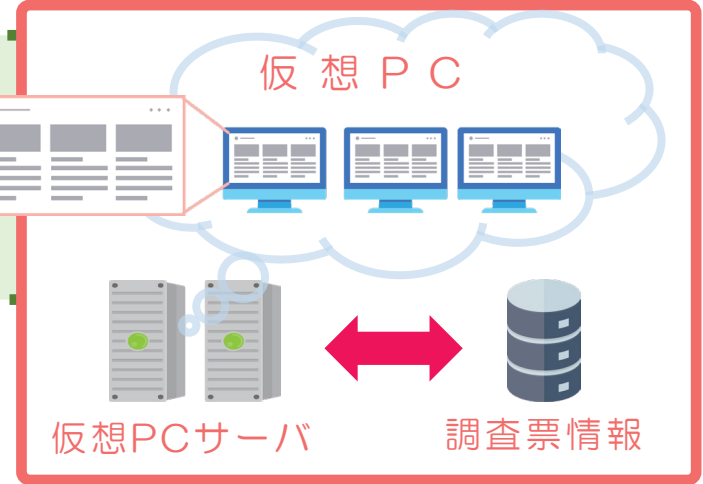
SINET等を活用した専用線による接続

〔インターネットに接続できない〕

- SINET
全国の大学、研究機関等を結ぶ学術情報ネットワーク（国立情報学研究所が構築、運用）

- シンクライアント端末
ユーザーが使用する端末の機能は必要最小限にとどめ、サーバー側で処理を行う仕組み

中央データ管理施設



専用線による接続

統計データ利活用センター(和歌山)

審査



登録



管理



運用管理業務等

背景資料 1 オンラインで利用可能な調査一覧 (93調査884年次、令和7年3月末時点)

(内閣府)

人々のつながりに関する基礎調査
「絆」と社会サービスに関する調査
高齢者の生活と意識に関する国際比較調査
高齢者の経済・生活環境に関する調査
高齢者の健康に関する調査
高齢者の住宅と生活環境に関する調査
高齢者の経済生活に関する調査
高齢者の日常生活・地域社会への参加に関する調査
男女間における暴力に関する調査
企業のワーク・ライフ・バランスに関する調査
消費動向調査

(こども家庭庁)

若者の生活に関する調査
生活状況に関する調査
こども・若者の意識と生活に関する調査

(総務省)

国勢調査
住宅・土地統計調査
労働力調査
就業構造基本調査
社会生活基本調査
個人企業経済調査
科学技術研究調査
サービス産業動向調査
サービス産業動態統計調査
経済センサス-基礎調査
経済センサス-活動調査
経済構造実態調査
家計調査
全国家計構造調査 (全国消費実態調査)
家計消費状況調査
全国単身世帯収支実態調査
小売物価統計調査

(外務省)

海外での滞在や生活等に関する基礎調査

(財務省)

法人企業統計調査
民間給与実態統計調査

(文部科学省)

学校教員統計調査
21世紀出生児縦断調査 (平成13年出生児)

(厚生労働省)

人口動態調査
医療施設調査
患者調査
病院報告
社会福祉施設等調査
21世紀出生児縦断調査 (平成13年出生児)
21世紀成年者縦断調査 (平成14年成年者)
中高年者縦断調査
21世紀出生児縦断調査 (平成22年出生児)
21世紀成年者縦断調査 (平成24年成年者)
国民生活基礎調査
毎月勤労統計調査
労働経済動向調査
雇用動向調査
雇用の構造に関する実態調査
労使関係総合調査 (労働組合活動等に関する実態調査)
賃金構造基本統計調査
労働安全衛生調査 (労働環境調査)
賃金引上げ等の実態に関する調査
就労条件総合調査
労働災害動向調査
労使関係総合調査 (労使コミュニケーション調査)
労働安全衛生調査 (実態調査)
労使関係総合調査 (労使間の交渉等に関する実態調査)

(農林水産省)

漁業センサス
作物統計調査
牛乳乳製品統計調査

(経済産業省)

経済構造実態調査
経済センサス-活動調査
工業統計調査
商業統計調査
商業動態統計調査
特定サービス産業実態調査
特定サービス産業動態統計調査
経済産業省企業活動基本調査
外資系企業動向調査
海外事業活動基本調査
海外現地法人四半期調査
情報通信業基本調査
経済産業省生産動態統計調査
商品流通調査
石油製品需給動態統計調査
経済産業省特定業種石油等消費統計調査
知的財産活動調査
中小企業実態基本調査

(国土交通省)

建築着工統計調査
建設工事受注動態統計調査
建設工事施工統計調査
造船造機統計調査
鉄道車両等生産動態統計調査
内航船舶輸送統計調査
自動車燃料消費量調査
全国輸出入コンテナ貨物流動調査
宿泊旅行統計調査

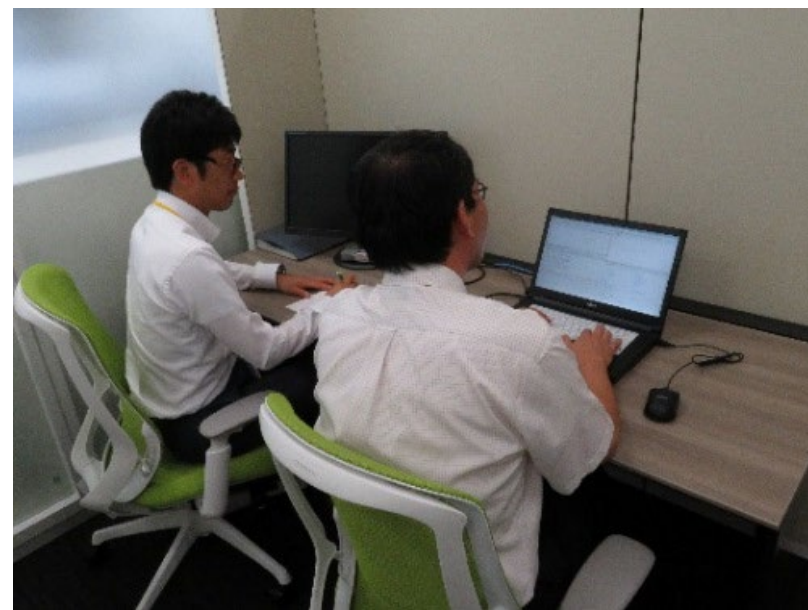
(環境省)

環境経済観測調査
容器包装廃棄物の収集運搬・選別保管費用等に関するアンケート調査

(防衛省)

駐留軍関係離職者帰すう状況調査

背景資料 1 オンサイト施設



(入退室管理や監視カメラを備えた専用室)

背景資料 1 リモートアクセス

- 利用者自身の拠点（研究室や自宅等）から、インターネット回線を経由して調査票情報を格納したサーバにアクセスし、サーバ上の仮想PCを遠隔操作して調査票情報を利用する方法。
- 仮想PCへの接続時は、HTTPSによる暗号化通信や、ID・パスワードに加え認証アプリ（ワンタイムパスワード）を利用した二要素認証による厳格な本人確認により、セキュリティを確保しています。なお、リモートアクセスの利用場所は日本国内に限る。
- 利用者自身が用意したデータ、ソフトウェアやプログラムについても、所定の手続を行った上で仮想PCに持ち込むことができる。分析結果等を仮想PCから持ち出す際は、手続が必要。なお、調査票情報そのものは持ち出せない。



自宅や研究室など

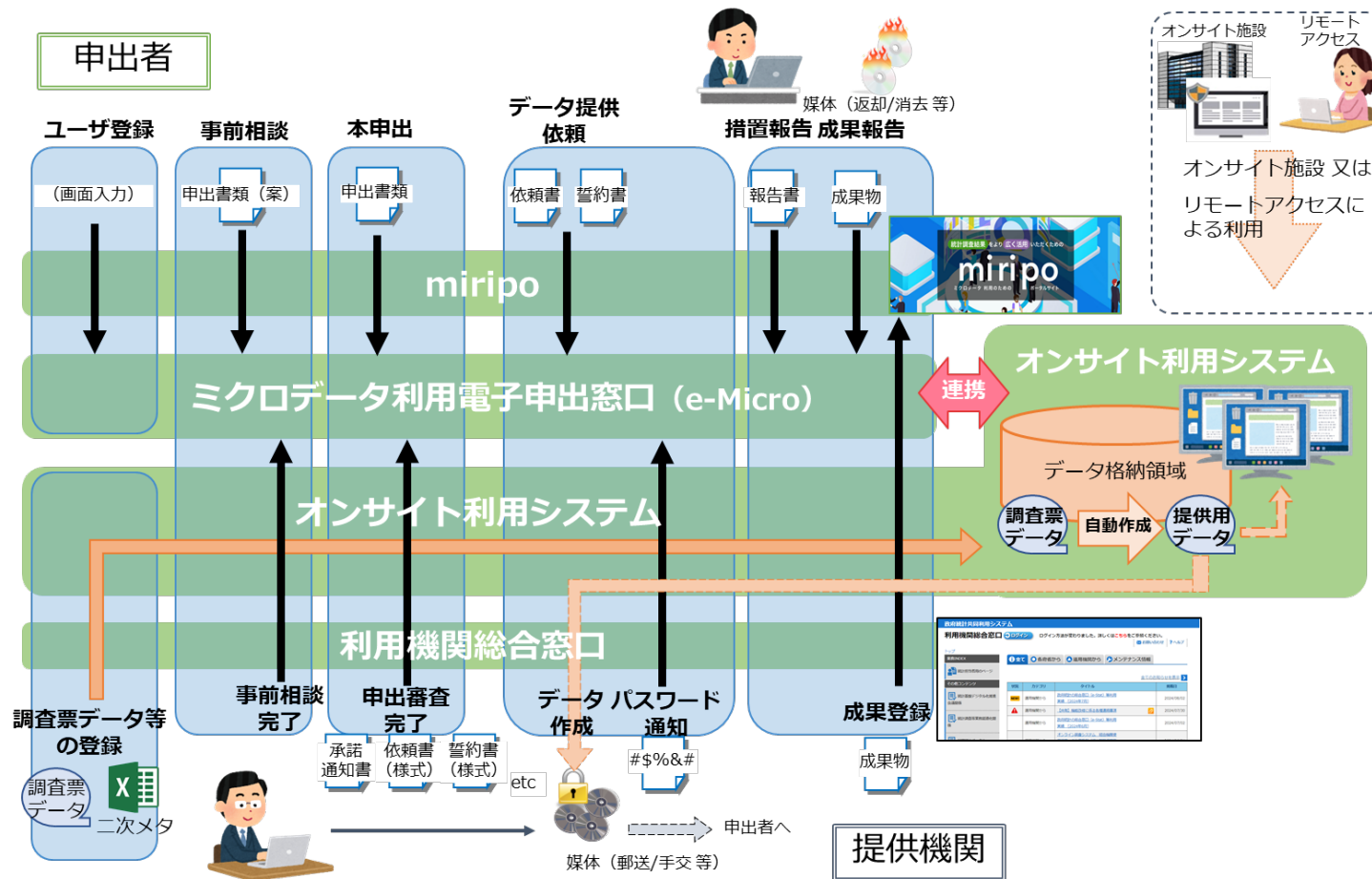


オンサイト利用システム内の仮想PCを利用するため、利用環境の準備が不用。また、利用可能な領域に提供データを格納するため、データの受取も不要。



背景資料 1 調査票情報の利用手続に係るシステム

- 利用申出の受付から利用後の報告までを一元的に実行可能なシステム
- 申出者はインターネット経由で「マイクロデータ利用ポータルサイト」（以下、「miripo」という）上にあるマイクロデータ利用電子申出窓口（e-Micro）から、提供機関はG-Net（政府共通ネットワーク）経由で利用機関総合窓口からアクセス

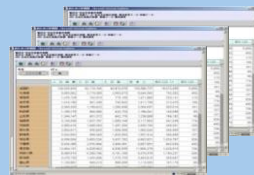


背景資料 1 オーダーメイド集計・匿名データ

平成19年の統計法全面改正において、調査票情報の新たな提供形態として、オーダーメイド集計（委託による統計の作成等）及び匿名データの制度を規定

オーダーメイドによる
統計の作成・提供
(統計法第34条)

国民1人1人が希望する様式での統計表等を入手可能に



匿名データ※の
作成・提供
(統計法第35条及び第36条)

※ 調査票情報の匿名性を高め、特定の個人又は法人その他の団体の識別ができないように加工したもの。作成にあたっては、統計研究研修所の有識者会議において、匿名化処理の妥当性に関する検証を実施した後に統計委員会への諮問（報告）が必要。

より広い範囲の者が、
多変量解析を始め
とする高度な統計
的分析が可能に

学術研究の成果、高等教育の内容等が公表され、社会に還元

研究事例

- ◆ 労働市場の構造変化に伴う就業者属性別の労働移動に関する分析
- ◆ 睡眠および関連症状の時系列変化に関する研究
- ◆ 家計の時間利用とエネルギー消費の関係性に関する分析
など

背景資料 2 Five Safes Framework (イギリス等)

- Five Safesとは、イギリス国家統計局（ONS）が開発した枠組みであり、機密性の高いデータや機微なデータへのアクセスを安全に提供・管理するためのデータセキュリティ・フレームワーク。単一の対策（例：データの匿名化のみ）に頼るのではなく、5つの要素を組み合わせることで多層的に防御することで、「データを最大限に活用しつつ、プライバシーを確実に守る」ことを目的としている。
- データの利活用とプライバシー保護を両立させるための世界的な標準として、イギリス国家統計局、カナダ統計局、オーストラリア統計局及びシンガポール統計局などで採用されている。



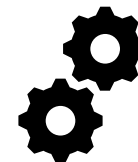
Safe People (安全な利用者)

研究者や利用者が、データを適切かつ責任を持って扱うための訓練を受け、認定されていること。



Safe Projects (安全なプロジェクト)

データの使用目的が適切で、合法的かつ倫理的であり、公的な利益に資するものであること。



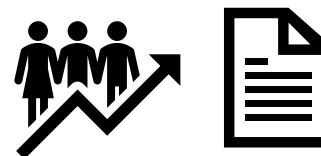
Safe Settings (安全な分析環境)

不正アクセスやデータの持ち出しを防ぐ物理的・技術的なセキュリティが整った環境（信頼できる研究環境など）で作業が行われること。



Safe Data (安全なデータ)

データそのものに匿名化や難読化の処理が施され、個人の特定（プライバシー侵害）のリスクが最小限に抑えられていること。



Safe Outputs (安全な分析結果)

分析結果（統計表やレポートなど）を公開する前に、そこから個人の特定ができないよう厳格にチェックを行う。

背景資料3 カナダ（マイクロデータへのアクセス）

▶ ミクロデータへの安全なアクセス

- カナダ統計局は、研究、エビデンスに基づく意思決定、政策立案、プログラム管理、そして一般の理解を支援するために、複雑な統計分析のための機密マイクロデータへの安全なアクセスを提供。データ利用者は匿名化された調査、管理、統合データに直接アクセスできる。
- 組織は、カナダ統計局との覚書、セクション10合意、または組織アクセス契約を締結することで認定を受けることができる。認定されたデータ利用者は、安全な環境でデータにアクセスするためのプロトコルに従う組織の認可を受けた研究者やアナリスト。
- ミクロデータにアクセスするには、データ利用者はカナダ統計局の従業員とみなされる必要がある。
- すべてのデータ出力は、データ利用者に提供する前にカナダ統計局の職員による機密性の審査を受ける。

▶ 「みなし職員」

- 統計局の職員とみなされるデータ利用者は、社会調査やビジネス調査、管理データ、リンクデータなど多様なデータにアクセスできる。
- 「みなし職員」となるには、セキュリティクリアランスの取得、必須の研修修了、そしてカナダ統計局に対して就任宣誓または秘密保持の宣誓または承認が含まれる。
- 統計法により、カナダ統計局は、一般的な意味での従業員でなくても、個人（自然人、法人契約者、公務員）のサービスを利用して業務を行うことができる。この法律では、これらの個人を「本法の下で雇用されているものとみなす者」と呼んでおり、したがって「みなし職員」という表現が使われる。第5条では、連邦政府の部門からの「みなし職員」の採用、および個人やコンサルタントの採用について規定しており、第10条では州の公務員の採用を認めている。みなし職員とは、特定のサービスを提供する人であり、多くの場合、統計目的での機密情報へのアクセス（RDCで利用可能な非識別データを含む）を伴う。このサービスを行う際、その人物は識別可能な情報を機密として保持する義務について、カナダ統計局の職員と同じ義務を負う。

▶ 学術データ利用者のためのデータアクセス

- リサーチデータセンター(RDC)は、認定された学術研究者が研究目的で匿名化かつ集約されていないマイクロデータにアクセスするための安全な物理的環境。RDCはカナダ各地の大学キャンパスに設置されており、統計局の職員が勤務している。
- バーチャルリサーチデータセンター(vRDC)情報技術プラットフォームは、カナダRDCネットワークとの提携を通じて、学術研究者にカナダ統計局のマイクロデータへの安全なアクセスを提供する最新の仮想インフラ。該当のデータ利用者は、安全なRDC施設内および他の「認可されたワークスペース」(例:自宅やオフィス)からデータにアクセスできる。vRDCは2025年から2026年にかけてローンチ予定。

背景資料3 カナダ（マイクロデータへのアクセス）

➤ 連邦政府利用者のデータアクセス

- 承認された適格アクセス協定を持つ連邦政府職員は、許可されたワークスペース、バーチャルデータラボ(VDL)、またはオタワの旧連邦RDC(FRDC)として知られていたセキュアデータアクセスセンター(SDAC)の現地で機密マイクロデータにアクセスできる。アクセス料はアクセス要件によって異なる。

➤ 州および準州政府ユーザー向けのデータアクセス

- 承認されたプロジェクトを持つ州および準州政府の職員は、VDLを通じて認可されたワークスペースで機密マイクロデータにリモートアクセスできる。アクセス料金はプロジェクトによって異なる。

➤ 非営利団体、非政府組織、民間セクターのデータアクセス

- 非営利団体、非政府組織、民間セクターは、プロジェクトの適格性に応じて、VDLを通じた認可されたワークスペース、オタワのSDAC(旧FRDC)現地、または地元のRDCで機密マイクロデータにアクセスできる。アクセス料金はプロジェクトによって異なる。

➤ カナダ統計局バイオバンク

- 血液、尿、DNA(デオキシリボ核酸)などの生物検体サンプルは、カナダ健康指標調査の同意した参加者から収集され、倫理基準を満たす承認された研究イニシアチブのみが利用可能。その結果得られた解析結果はRDCを通じて提供される。いかなる場合も個人情報や特定可能な情報は公開されない。関心のあるデータセットは、承認された学術および政府のデータ利用者に利用可能。

背景資料 3 カナダ（データアクセスの連続性）

セルフサービス

セキュアアクセス

	自動データ取り込み	データ製品	パブリックユースマイクロデータファイル (PUMF)	セルフサブ集計ツール	機密マイクロデータファイル
アクセス方法	<ul style="list-style-type: none"> ➢ アプリケーションプログラムインターフェース (API) 	<ul style="list-style-type: none"> ➢ ビューまたはダウンロードデータテーブル ➢ 可視化された主要なデータセット ➢ StatCanの記事や出版物を参照 	<ul style="list-style-type: none"> ➢ フリーダウンロード ➢ PUMFプラットフォームのサブスクリプション 	<ul style="list-style-type: none"> ➢ リアルタイムリモートアクセスのサブスクリプション (RTRA) 	<ul style="list-style-type: none"> ➢ バーチャルデータラボ (vDL) ➢ バーチャルリサーチデータセンター (vRDC)
アクセス場所	<ul style="list-style-type: none"> ➢ StatCanウェブデータサービス 	<ul style="list-style-type: none"> ➢ StatCanウェブサイト ➢ StatCanアプリ 	<ul style="list-style-type: none"> ➢ StatCanウェブサイト 	<ul style="list-style-type: none"> ➢ StatCanウェブサイト 	<ul style="list-style-type: none"> ➢ StatCan内のセキュアルーム ➢ 認可されたワークスペース
データ種類	社会・経済データ	社会・経済データ	社会データ	社会データ	社会・経済データ

➢ ミクロデータへのセルフサービスアクセス

カナダ統計局は、公共利用マイクロデータファイル(PUMF)を機関や個人に提供。ファイルには集計されていないデータが含まれており、個人や企業が直接的にも間接的にも特定されないよう慎重に修正・評価されている。有料サブスクリプションでData Liberation Initiative(DLI)またはPUMFコレクションを通じて直接アクセスすることもできる。選ばれた個別のPUMFはカナダ統計局のウェブサイトから無料でダウンロードできる。カナダ統計局はデータ利用者向けにリモートアクセスソリューションも提供。

➢ パブリックユース・マイクロデータファイルコレクション

パブリックユース・マイクロデータファイル(PUMF)コレクションは、匿名化かつ非集約されたすべてのデータに無制限にアクセスできる機関向けのサブスクリプション制サービス。これは電子ファイル転送(EFT)サービスと、使いやすいインターフェースを持つインターネットプロトコル(IP)制限付きオンラインデータベースであるリッチデータサービス(RDS)プラットフォームを通じて利用可能。選ばれたファイルはカナダ統計局のウェブサイトからも無料で入手可能。

➢ リアルタイムリモートアクセス

リアルタイムリモートアクセス(RTRA)は、加入者がSASプログラムをリアルタイムで実行し、テーブルの形で機密マイクロデータから結果を抽出できるオンライン集計ツール。

背景資料3 カナダ（データの共有・提供）

▶ データ共有

- 調査数を削減や時間の節約のために、カナダ統計局は連邦政府や州政府の部門、その他の組織と共有協定を結ぶことがある。カナダ統計局は100以上の組織と有効な協定を結んでいる。
- 統計法第12条に基づき、カナダ統計局は、データ共有契約が適用される際に、回答者が提供した情報にデータ共有契約が適用される場合、またどの組織と共有されるかを通知しなければならない。ほとんどの場合、回答者は統計カナダに他の組織と情報を共有しないよう要請する権利を有する。
- カナダ統計局からデータを受け取る各組織は、データを統計目的のみで使用することに同意し、受領した情報のアクセス、機密性、セキュリティに関する特定の条件および条件を遵守することに同意する。

▶ データ提供

- 統計法には、個人、事業、組織に関するデータを提供することを認める限定的なケースがある(法律で示された例外については下部のページの表を参照)。これら特定の場合に、カナダ統計局長は特定の種類の情報提供を許可することができる。個人、事業、または組織に関する情報は、統計局長が発出した命令によってのみ公開可能。さらに、個人情報には個人の同意、または情報を最初に収集した組織の許可がなければ公開できない。
- 統計法に加え、データ提供はカナダ統計局の特定の政策要件を満たす必要がある。例えば、カナダ統計局は統計目的および公共の利益の必要性が証明された場合にのみ情報を提供する。カナダ統計局はまた、データが提供された場合に個人、組織、企業に害を与えないかを確認するために潜在的な提供を評価する。
- これらの法的および政策的要件に準拠し、カナダ統計局は、政策立案、統計研究、分析に必要な人々がデータを利用可能にできるよう、一般の情報提供プログラムの一環として特定の情報を提供している。
- カナダ統計局はまた、統計および研究目的で情報を必要とする連邦省庁、州省庁、その他の組織に対し、機密性を保護することを書面で約束した機関にも特定の情報を提供している。
- 以降のリストの提供は、統計法第17条第2項に基づき、カナダ最高統計官によって承認される場合がある。カナダ統計局は、統計法の下記の規定に明確に定められている場合を除き、機密情報を提供する権限はない。

統計法第17条第2項の提供規定	説明
(a) 個人、組織、または部門が自らの目的のために収集し、1971年5月1日以前または以降に統計カナダに伝達された情報。ただし、その情報が統計カナダに伝達された際は、収集時と同じ秘密保持要件が適用され、統計カナダが収集官およびチーフ統計局長の合意した方法と範囲でのみ提供できる。	第17条第2項(a)に基づく提供には、情報を最初に収集した個人または組織の同意が必要です。本項で対象となる情報の例としては、所得税記録、重要統計記録、車両登録ファイルなどがあります。
(b) 当該人物または組織が書面で提供に同意した個人または組織に関する情報	第17条第2項(b)に基づく提供には、調査の一環として統計カナダに情報を提供した回答者の書面による同意が必要です。
(c) 事業者によって当面の間、所有者が書面化に同意した事業に関する情報	第17条第2項(c)に基づく提供には、提供時に事業主の書面による同意が必要です。
(d) いかなる法令またはその他の法律の下で一般に公開されている情報	第17条第2項(d)に基づく提供は同意なしに許可される場合があります。この権限は、既存の法律で求められている情報の公開に用いられます。これには情報公開法は含まれていません。

背景資料3 カナダ（データの共有・提供）

統計法第17条第2項の提供規定（続き）	説明（続き）
(e) 病院、精神病院、図書館、教育機関、福祉機関またはその他の類似の非営利機関に関する情報で、個別の患者、受刑者またはその施設の保護下にある者に関連付けられるよう整理された詳細を除くもの	第17条第2項(e)に基づく提供は、 同意なし に許可される場合があります。この権限は特定の非営利組織に関する情報公開に使われますが、学生、患者、クライアント、組織の従業員などの個人の詳細は公開しません。カナダ統計局は、その提供が組織に悪影響を及ぼす可能性がある場合、その情報を公開しません。
(f) 個々の事業所、企業、または事業の索引またはリストの形で、それらに関連する以下のいずれかまたは全部を示す情報： (i) 彼らの氏名と住所、 (ii) 統計に関する連絡先電話番号、 (iii) 統計に関する公用語、 (iv) 彼らが事業の過程で生産、製造、加工、輸送、保管、購入または販売する製品、または提供するサービス、または (v) 従業員数や雇用者数、または従業員構成員の特定の範囲内にあるかどうか	第17条第2項(f)に基づく提供は、 同意なし に許可される場合があります。この権限は、産業の種類や従業員数など、企業や施設の基本情報を公開するために使われます。
(g) 運送業者または公共事業に関する情報	第17条第2項(g)に基づく提供は、 同意なし に許可される場合があります。この権限は、陸上・海上・空路のキャリアや、放送、通信サービス、水処理施設などの公共事業に関する情報公開に使われます。カナダ統計局は、提供が組織に悪影響を及ぼす可能性がある場合、アカシや公共事業のための情報を公開しません。
(e) 病院、精神病院、図書館、教育機関、福祉機関またはその他の類似の非営利機関に関する情報で、個別の患者、受刑者またはその施設の保護下にある者に関連付けられるよう整理された詳細を除くもの	第17条第2項(e)に基づく提供は、 同意なし に許可される場合があります。この権限は特定の非営利組織に関する情報公開に使われますが、学生、患者、クライアント、組織の従業員などの個人の詳細は公開しません。カナダ統計局は、その提供が組織に悪影響を及ぼす可能性がある場合、その情報を公開しません。
(f) 個々の事業所、企業、または事業の索引またはリストの形で、それらに関連する以下のいずれかまたは全部を示す情報： (i) 彼らの氏名と住所、 (ii) 統計に関する連絡先電話番号、 (iii) 統計に関する公用語、 (iv) 彼らが事業の過程で生産、製造、加工、輸送、保管、購入または販売する製品、または提供するサービス、または (v) 従業員数や雇用者数、または従業員構成員の特定の範囲内にあるかどうか	第17条第2項(f)に基づく提供は、 同意なし に許可される場合があります。この権限は、産業の種類や従業員数など、企業や施設の基本情報を公開するために使われます。
(g) 運送業者または公共事業に関する情報。	第17条第2項(g)に基づく提供は、 同意なし に許可される場合があります。この権限は、陸上・海上・空路のキャリアや、放送、通信サービス、水処理施設などの公共事業に関する情報公開に使われます。カナダ統計局は、提供が組織に悪影響を及ぼす可能性がある場合、アカシや公共事業のための情報を公開しません。

背景資料 3 カナダ（二次的利用関連規定）

<統計法>

定義

第2条 この法律において、（略）「識別情報」とは、個人、企業または組織を特定することを可能にする情報をいう。

就任宣誓

第6条

- (1) 主任統計官およびこの法律に基づき雇用されまたは雇用されたとみなされるすべての者は、職務に就く前に、次の宣誓または厳粛な確約を行い、署名しなければならない。私、_____は、統計法の要件ならびにその下のすべての規則および指示に従い、カナダ統計局の職員として誠実かつ正直に職務を遂行すること、および職務上知り得たいかなる事項も正当な権限なくして開示または公表しないことを厳粛に誓います（または確約します）。

証明

- (2) 第1項に定める宣誓または厳粛な確約は、主任統計官が指示する者の前で行われ、主任統計官が指示する方法で返還および記録されるものとする。

法人形態の契約者

- (3) この法律に基づき主任統計官のために特別なサービスを提供するために契約により雇用された者が法人である場合、その最高経営責任者ならびに特別なサービスの提供に使用されるその他の役員、従業員および代理人は、契約に基づく職務を遂行する前に、次の宣誓または厳粛な確約を行い、署名しなければならない。私、_____は、統計法の要件ならびに同法の下すべての規則および指示に従い、（法人名）の職員として（主任統計官との契約を特定する）の遂行に係る雇用に関して誠実かつ正直に職務を遂行すること、および当該雇用上知り得たいかなる事項も正当な権限なくして開示または公表しないことを厳粛に誓います（または確約します）。

証明

- (4) 第3項に定める宣誓または厳粛な確約は、主任統計官が指示する者の前で行われ、主任統計官が指示する方法で返還および記録されるものとする。

情報の共有

第12条

- (1) 大臣は、カナダ統計局または省庁もしくは法人のいずれかが双方を代理して回答者から収集した情報の共有、ならびにその後の当該情報に基づく集計または公表について、省庁または地方自治体その他の法人との間で協定を締結することができる。

協定

- (2) 第1項に基づく協定は、次の事項を定めるものとする。
- (a) 情報がカナダ統計局および当該省庁または法人を代理して収集されていることを通知により回答者に知らせること。
 - (b) 回答者がカナダ統計局による情報の共有に異議を唱える旨を主任統計官に書面で通知した場合、当該省庁または法人が回答者に当該情報の提供を法律により求める権限を有しない限り、当該省庁または法人と情報を共有しないこと。

共有できる情報

- (3) この条に基づき共有される情報は、第2項に従い、回答者がカナダ統計局または当該省庁もしくは法人に提供した最初の調査への回答および補足情報を含むことができる。

背景資料 3 カナダ（二次的利用関連規定）

<統計法>

秘密保持 情報開示の禁止 第17条

- (1) 第11条または第12条に基づき締結された協定の条件に従い情報を伝達する目的のため、およびこの法律に基づく訴追の目的のためを除き、この条に従い、
- (a) この法律に基づき雇用されまたは雇用されたときみなされ、かつ第6条に基づき宣誓した者以外の者は、この法律の目的のために取得された申告書または識別情報を閲覧することを許可されないものとする。
 - (b) 第6条に基づき宣誓した者は、この法律に基づき取得された情報を、その開示により当該情報を特定可能な個人、企業または組織に関連付けることが可能となる方法で、いかなる手段によっても開示し、または故意に開示させてはならない。

禁止の例外

- (2) 主任統計官は、命令により、次の情報の開示を認可することができる。
- (a) 個人、組織または省庁が自らの目的のために収集し、1971年5月1日以前または以後にカナダ統計局に伝達した情報。ただし、当該情報はカナダ統計局に伝達された時点で収集時に適用されていたものと同一の秘密保持要件の対象となり、カナダ統計局はその収集者と主任統計官との間で合意された方法および範囲においてのみ開示することができる。
 - (b) 当該個人または組織の書面による同意を得た個人または組織に関する情報。
 - (c) 当該事業の現在の所有者の書面による同意を得た事業に関する情報。
 - (d) 法律その他の法令により公開されている情報。
 - (e) 病院、精神科施設、図書館、教育機関、福祉施設その他これに類する非営利施設に関する情報。ただし、当該施設に入院中または収容中の個人患者、被収容者その他の者に関連付けることが可能な方法で整理された詳細情報を除く。
 - (f) 個々の事業所、商会または企業の索引または一覧の形式による情報であって、次の事項のいずれか、一部またはすべてを示すもの。
 - (i) 名称および住所
 - (ii) 統計事項に関して連絡可能な電話番号
 - (iii) 統計事項に関して使用を希望する公用語
 - (iv) 事業の過程において生産、製造、加工、輸送、保管、購入もしくは販売する製品、または提供するサービス
 - (v) 雇用する従業員または労働力を構成する者の数が特定の範囲内にあるかどうか
 - (g) 運送業者または公益事業者に関する情報

特権情報——証拠としての不採用

第18条

- (1) この法律に基づく訴追の目的のためを除き、この法律に基づきカナダ統計局に提供された申告書および識別情報、ならびに回答者が所持する申告書の写しは特権情報であり、いかなる手続においても証拠として使用されないものとする。

特権情報——宣誓した者

この条の適用

- (2) 第6条に基づき宣誓した者は、裁判所、審判所その他の機関の命令によっても、いかなる手続においても、この法律の運用の過程で取得した情報に関して口頭証言を行い、または取得した申告書もしくは識別情報を提出することを求められないものとする。
- (3) この条は、この法律によりカナダ統計局が開示を禁じられている情報、または第17条第2項に基づく認可によってのみ開示することができる情報に関して適用される。

背景資料 3 イギリス（匿名性に応じた分類）

データのタイプ	定義	法的取扱い	加工方法	識別リスク
原データ(confidential data)	直接識別子の削除を含む匿名加工がされていない個別データ(調査票情報や未加工の行政記録情報等が該当)	含まれる個別データはGDPR等が原則適用、厳格なデータ保護義務	加工なし	高
非識別データ(De-identified Data)	追加情報なしには特定の個体を特定することが困難であり、かつ研究利用に適したデータ	個別データだが、秘匿措置が施された上でSRS内での利用に限定	直接識別子を仮名化キーに置換した後に、仮名化された直接識別子を削除	中
匿名化マイクロデータ(Anonymized microdata)	統計的開示制限を施したデータで、研究利用も可能	統計登録サービス法における「個人情報」の外に位置づけられるが、入手にあたって、ライセンス(End User Licence)の取得が必要	属性情報に関する区分統合、地理的区分の統合等	中～低
合成データ(Synthetic data)	元データの統計的特性を保持しつつ人工的に生成されたデータ	完全な匿名化がされている場合はデータ保護法の適用外、元データとの照合リスクに応じて評価	統計モデル、機械学習、差分プライバシーの実現方式等に基づく生成等	低～非常に低
完全匿名データ(Public Use File)	個人の識別がもはや不可能なため、一般公開が可能なマイクロデータ	データ保護法の適用外	集約、ノイズ付加等	非常に低

※データ定義の観点から、仮名化されたデータと非識別データの違いはない。違いはアクセスされた環境から生じる。なお、SRSやその他の信頼された研究環境(Trusted Research Environment)を通じたアクセスによって、非識別データの再識別リスクが低減する。

背景資料3 イギリス（承認された研究者制度）

➤ 承認された研究者制度

- Secure Research Service (SRS)は、認定された研究者(accredited researcher)あるいは承認された研究者(approved researcher)に対し、公益のための研究プロジェクトに取り組むために非特定化された未公開データへの安全アクセスを提供。
- SRSは、研究目的のデータ作成および提供に関して、英国統計機構(UK Statistics Authority (UKSA))からデジタル経済法(DEA)2017の処理機関として認定されている。
- 2026年3月現在、6,295人が認定研究者として認定を受け、824のプロジェクトが承認されている。

➤ STEP 1：認定研究者の申請

- SRSのデータにアクセスするには、認定された研究者である必要がある。
- 認定には完全認定（Full accreditation）と暫定的な認定（Provisional accreditation）がある。認定には、数学や統計学の学位や定量的研究経験等を証明する必要がある。完全認定の要件を満たしていない場合には、同じ組織で業務に従事する等の条件を満たした認定研究者を監督者としてつけることで、暫定的な認定を受けることができる。
- 認定の際は、Safe Researcher Trainingを修了し、評価に合格する必要がある。ここでは、データセキュリティや個人の責任、ファイブセーフのフレームワーク、統計的開示管理の原則について研修を受ける。
- 認定研究者は、デジタル経済法により、英国統計機構の公的登録簿への掲載することが義務づけられている。

➤ STEP 2：プロジェクトの申請

- 申請前に「SRSメタデータカタログ」を用いて、利用可能なデータセットや、アクセレベル等を確認する必要がある。一部のデータセットのアクセスはセーフルームに限定されている。プロジェクトの全体的なアクセスレベルは、最も制限の厳しいデータセットによって決まる。各データセットのアクセス条件は、データ所有者によって決定される。
- レベル1では、セーフルームまたはセーフポッドのみ、レベル2では、セーフルーム、セーフポッド、またはAOCオフィスアクセス、レベル3では、セーフルーム、セーフポッド、AOCオフィスアクセス、AOCリモートアクセスとなっている。
- 申請の承認には約10週間程度時間を要する。複雑なプロジェクトやデータ所有者が承認を必要とする場合は時間がかかることがあり、需要が高い時期には処理時間が延長されることもある。

※安全なデータの利用のために、SRSはファイブセーフフレームワークを使用。安全な人々：訓練を受け認定された研究者は、データを適切に活用することを信頼されている。安全なプロジェクト：データは、明確な公的利益をもたらす価値ある倫理的な研究にのみ使用される。安全な環境：データへのアクセスは、SRSの安全な技術システムを使ってのみ可能。安全な出力：すべての研究成果は、データ対象者を特定しないか確認される。安全なデータ：研究者は非特定化されたデータのみを使用。

※セーフルーム(SafeRoom)：国家統計局(ONS)が運営する安全な端末。SRSへのアクセスが安全な部屋のみ限定されている場合、研究者は当施設の安全室のいずれかで端末を予約する必要がある。セーフルームへのアクセスの際は、セキュリティ宣言を行う必要がある。ハンブシャー州ティッチフィールドとサウスウェールズ州グウェントのニューポートにあるオフィス内にある。

※セーフポッド(SafePod)：必要なセキュリティと管理を備えた標準化されたセーフ設定にアクセスする代替手段であり、研究者が英国国内より多くの場所から安全なデータセットにアクセスし利用できる。SafePodsは主に英国各地の大学を拠点とし、承認された研究者が予約・使用できるようになっている。

※AOC（Assured Organisational Connectivity：保証された組織接続性）：AOCは、組織と国家統計局(ONS)との間の合意。認定研究者は、自社のオフィスや承認された場合には自宅からSRSにアクセスできる。AOCアクセスが承認される前に、組織は特定の物理的、ガバナンス、技術的セキュリティ基準を満たす必要があります。

※AOCリモートアクセス：承認されたAOCリモートアクセスを持つ研究者は、自宅から安全なリモートネットワークを利用してSRSを使用できる。

※AOCオフィスアクセス：承認されたAOC契約を持つ研究者は、セーフルームやセーフポッドを予約せずに、その組織の安全なオフィス環境からSRSにアクセスできる。

背景資料3 イギリス（承認された研究者制度）

➤ STEP 2：プロジェクトの申請（続き）

- 申請は、2017年デジタル経済法の基準に基づいて、英国統計機構が設置した研究認定パネル（Research Accreditation Panel）によって審査される。
- 応募書類には、研究目的、方法論、データ要件について明確な情報を提供する必要がある。これによって、データ所有者および英国統計機構は、申請された研究が合法的で倫理的かつ公共の利益にかなっているかが確認される（認定基準の詳細は、研究行動規範及び認定基準のパート2を参照）。
- Secure Research Service(SRS)カタログに含まれていない外部データを取り込んで研究を完了する予定がある場合は、別途申請を行う必要がある。
- プロジェクトや研究者が認定または承認されると、ユーザーアカウントとプロジェクトスペースが作成され、リクエストしたデータセットがプロジェクトにマッピングされ、データにアクセスできるようになる。認定研究者とそのプロジェクトの記録は、研究データへのアクセスの透明性を確保するため、英国統計機構のウェブサイト公開される。

➤ STEP 3：プロジェクト終了後

- プロジェクトが終了後、出力結果を再現するために必要なファイル(コードなど)をクリアしてエクスポートする必要がある。
- デジタル経済法の下で認定されたプロジェクトは、5年以内に完了しなければならない。
- SRSデータの使用が認められた研究者は、研究成果を一般に公開しなければならない。この要件は、2017年デジタル経済法の研究行動規範および認定基準に定められている。
- ピアレビュー後にプロジェクトに戻ってさらなる分析を行う必要がある場合は、簡単に再開可能。再開後、プロジェクトは閉鎖前とまったく同じ外観となり、すべてのファイルや構造は変更されない。
- SRSから結果を持ち出すには、その結果を統計支援チームに提出して認証を受ける必要がある。出力結果には、統計的開示管理が適用される。
- 認証を受け、集計結果の作成や、プロジェクト内での議論のために、公表前にSRSから結果を持ち出すこともできる。これは、プロジェクトチームや研究の委託先、スポンサー内でのみ共有することができる。いかなる場合も公開はできない。プロジェクト完了後は廃棄しなければならない。遵守しない場合には、認定研究資格が取り消される。
- その他、結果の公開に当たっては、SRSでアクセスされるデータに関するグラフィックや言葉を含むすべての情報を統計支援チームに提出し、認証を受ける必要がある。これは承認後は無期限での配布・公開が可能。
- どちらも、すべての基礎となる非加重カウントを表示する必要があり、一般的には閾値10に従う（場合によってはデータに応じてこれより低いまたは高い場合がある）。閾値未満のカウントを持つ出力は、研究上の必要性を示し、出力が依然として安全であることを証明できる特例の場合に考慮されることがある。

背景資料3 イギリス（マッチング・リンケージ）

SRSにおけるマッチング

- 研究者は、Secure Research Service(SRS)プロジェクトで共通の変数を使ってアクセス可能な異なるデータセットを照合することができる。
- 個体識別用のIDが付与されたデータについては、それを仮名化（数字と文字の混合に変換）して、SRS環境外では意味のないイギリス国家统计局(ONS)IDにする。ONS IDは、研究者がSRS環境内のテーブルを照合することを可能にする。仮名化されたIDの例として、「entref」変数があり、これはSRSに蔵されている多くのビジネスデータセットに含まれている。

リンケージ

- デジタル経済法2017の下で認定された研究プロジェクトでは、すべてのデータは投入される前に非識別化されているため、研究者はSRS内部では、直接識別子(名前、住所、生年月日、NHS番号などのIDなど)に基づいてデータセットをリンクすることができない。
- プロジェクトごとに直接識別子を使ってデータセットをリンクするサービスは提供していない。これは専門的なリソースの非効率的な使用になるため。唯一の例外は部門間事業登録簿(IDBR)データ。研究者は、個々のプロジェクトを超えた広範な研究利益を示すことができれば、ONSによるデータセットのリンケージのリクエストを行うことができる。
- リンケージの申請には次の要素を評価される。①ユーザーニーズの強さ、②すべてのデータ所有者からのサポート、③連結の実現可能性と複雑さのレベル、④連結を実行するために必要なONS内のリソース
- リクエストが承認された場合、リンケージのためのデータセットはSRSの外部で作成され、非識別化されたバージョンをSRSに移すことで、すべての認定研究者がプロジェクト申請を行えるようになる。

部門間事業者登録簿を使ったリンケージ方法

- SRSに保有されているデータセット内で特定の事業者サブセットを特定する必要がある場合、またはSRS内のデータをすでに保有している事業者サブセットのデータと照合する必要がある場合、これは二つの方法で行うことができる。
- 会社番号（CRN）を使用する方法：関連するCRNを提供できる場合、SRSチームがこの照合作業を実施することが可能。
- 事業者名および住所を使用する方法：このリンケージの作業はONS内の別のチームによって行われる必要があり、料金が発生。

背景資料3 イギリス（二次的利用関連規定）

<統計登録サービス法>

委員会による情報の使用及び開示

第38条 委員会による情報の使用

- (1) 委員会がいずれかの機能の行使に関して取得した情報は、他の機能の行使に関して使用することができる。
- (2) 第(1)項は、第12条(1)及び第14条(1)に基づく機能の行使に関して委員会が取得した情報には適用されない。
- (3) 第(1)項は、第22条に基づく機能の行使に関して委員会が取得した情報には、情報を提供した者が第(1)項に規定する使用に同意しない限り適用されない。
- (4) 第(1)項は、情報の使用または開示を制限または禁止する法令に従う。

第39条 個人情報の秘密保持

(1) 本条に従い、委員会が機能の行使に関して保有する個人情報は、以下の者が開示してはならない。

- (a) 委員会の委員または職員
- (b) 委員会の委員会のメンバー
- (c) 委員会から直接または間接的に受け取ったその他の者

(2) 本部において「個人情報」とは、特定の者（法人を含む）に関連し、その者を識別する情報を意味するが、委員会の内部管理上の取り決めに関する情報（委員、職員またはその他の者に関するものを問わない）は含まない。

- (3) 第(2)項の目的上、情報が特定の者を識別するのは、その者の身元が以下の場合である。
 - (a) 情報に明記されている場合
 - (b) 情報から推定できる場合
 - (c) 情報と他の公開情報を合わせて推定できる場合
- (4) 第(1)項は以下の開示には適用されない。
 - (a) 法令により要求または許可された開示
 - (b) 同化義務により要求された開示
 - (c) 委員会がその機能を行わせることを可能にし、または支援するために必要な開示
 - (d) すでに合法的に公開されている情報の開示
 - (e) 裁判所命令に基づく開示
 - (f) 刑事捜査または刑事訴訟（英国内外を問わない）の目的のための開示
 - (h) 当該情報に関係する者の同意を得た開示

(i) 承認された研究者への開示

(5) 第(4)(i)項の目的上、「承認された研究者」とは、統計研究の目的のために委員会が保有する個人情報へのアクセスを委員会から許可された個人を意味する。

- (6) 委員会は、第(5)項に規定するアクセスを許可するかどうかを判断する基準を随時公表する。

背景資料3 イギリス（二次的利用関連規定）

<統計登録サービス法>

第39条 個人情報の秘密保持

(7) これらの基準は、委員会が以下を考慮することを要求しなければならない。

- (a) 当該個人が適切かつ適正な者であるかどうか
- (b) アクセスが要請される目的

(8) 委員会は、当該個人が本条の要件を理解していることを宣言する書面（委員会が定める様式による）に署名するまで、第(5)項に規定するアクセスを許可することができない。

(9) 第(1)項に違反した者は犯罪を構成し、以下の刑に処せられる。

- (a) 起訴による有罪判決の場合、2年以下の禁固刑、罰金、またはその両方
- (b) 略式有罪判決の場合、12ヶ月以下の禁固刑、法定最高額以下の罰金、またはその両方

(10) 第(9)項は、開示を行う個人が以下を合理的に信じていた場合には適用されない。

- (a) 第(3)(a)項により個人情報である情報の場合、当該情報に関係する者の身元が情報に明記されていないと信じていた場合
- (b) 第(3)(b)項により個人情報である情報の場合、その者の身元が情報から推定できないと信じていた場合
- (c) 第(3)(c)項により個人情報である情報の場合、その者の身元が情報と他の公開情報を合わせても推定できないと信じていた場合

(11) （略）

第40条 情報公開

(1) 2000年情報公開法第44条（開示の禁止）は、上記第39条により、以下の個人情報には適用されない。

- (a) 委員会から直接または間接的に受け取った公共機関が保有する個人情報
- (b) 当該機関が委員会の代理として保有していない個人情報

(2) 第(1)項において「公共機関」は2000年情報公開法と同じ意味を有する。

(3) 2002年スコットランド情報公開法第26条（開示の禁止）は、上記第39条により、以下の個人情報には適用されない。

- (a) 委員会から直接または間接的に受け取ったスコットランド公共機関が保有する個人情報
- (b) 当該機関が委員会の代理として保有していない個人情報

(4) 第(3)項において「スコットランド公共機関」は2002年スコットランド情報公開法と同じ意味を有する。

第41条 サービス提供者への情報開示

委員会は、委員会に対してサービスを提供する者に対して、当該サービスの提供のために必要または適切と認める場合、機能の行使に関連して取得した情報を開示することができる。

背景資料3 フランス（統計の機密性）

▶ 公的統計の法的枠組み

- 公式統計の法的枠組みは、基本的に二つの文書によって構成されている。公的統計サービスの任務に委ねられた特別な法律である1951年法（1951年6月7日付 法律第51-711号 統計の義務、調整および秘密に関する法律）と、データ保護法（1978年1月6日付けの情報技術、ファイル、自由に関する法律第78-17号）があり、統計処理も自然人に関するすべてのデータ処理と同様にこれに従う。
- 1951年法は、公的統計サービスを定義しており、INSEEと各省の統計サービスで構成され、一般の情報提供の任務や職業上の独立性の原則に関連している。この法律は統計機密性も定義しており、公式統計サービスが統計目的で取得した機密データを、法律で定められた条件のもとで統計、科学研究、歴史研究の目的に利用する場合を除き、開示することを禁止している。また、統計機密性は、直接的または間接的にこのような機密情報を明らかにする可能性のある統計成果物にも適用される。
- この法律はまた、公式統計調査の条件も定めており、特にその調査への参加が義務付けられている場合に適用される。公式統計サービスがその任務を遂行できるように、この法律ではさらに、公式統計の作成に必要な場合には、公的機関が保有する情報へのアクセス権を認めている。その際、その情報が法的な守秘義務によって保護されている場合も含まれる。また、この法律は特定の条件の下で、強制的な統計調査の実施に必要な場合には、民間の組織が保有するデータへのアクセスも認めている。
- 欧州統計への加盟国に適用される一般的な規定は、専用の規則である欧州議会・理事会の欧州統計に関する改正規則（EU）No 223/2009（2009年3月11日制定）に示されている。この規則は、INSEEや各省の統計部門が含まれる欧州統計システムや、このシステムの運営を定めている。
- これは、1951年の法律と同じ主要な原則に基づいている（職業上の独立性、機密保持、データへの容易なアクセス）。ASPの設立は、公式統計官の職業上の独立性を保証する手続きに関してそれが伴う義務から直接生じている。その原則に関しては、公式統計システムのすべての担当者にとっての参照倫理枠組みであるヨーロッパ統計実務規範（European Statistics Code of Practice）にもより広く言及している。2024年の規則改正では、欧州統計の作成に必要な場合に、国の統計機関やEurostatが民間の保有する特定のデータにアクセスすることに関する新しい規定が導入された。
- データ保護法は、すべての個人が自分の個人データの利用をコントロールできるようにすることを目的としており、その過程で個人データの処理の発展と基本的な権利の尊重を両立させることを目的としている。2018年以降、この法律は欧州一般データ保護規則（GDPR）によって定義された統一されたヨーロッパの法的枠組みの一部となっている。
- 法律はすべてのデータ管理者に義務を課しており、その基本は主に2つの原則に基づいている。一つは透明性の原則で、データ主体への情報提供やリクエストへの対応、処理の文書化が含まれる。もう一つは、データ主体のプライバシーに対する処理の影響リスクを管理・制限する原則である。公式統計サービスによる統計的な処理もGDPRやフランスのデータ保護法の対象となる。統計の機密性はデータ保護の重要な保護手段となっており、統計、科学研究、歴史研究の目的で行われる処理に関してEUや国内法が定める特定の法的枠組みの適用にも貢献している。

背景資料3 フランス（データの提供）

➤ 統計の機密性

- 公的統計機関であるINSEEや省庁の統計サービスの職員は、すべての公務員と同様に職業上の秘密を守る義務がある（一般公務員法典L121-6条）。これは、彼らの職務・職責に基づいて知り得た機密情報を第三者に伝えることを禁じており、刑法226-13条に定められた制裁（最長1年の懲役および1万5,000ユーロの罰金）の対象となる。
- 統計上の機密性は、統計目的で取得または作成された機密データに適用される特別な法的枠組み。これは専門的な秘密保持の義務を補完し、こうしたデータの開示を厳しく禁止する。通常の専門秘密とは異なり、統計上の機密性は行政や司法当局からの要求に対しても主張することができる。それでも、統計上の機密性で保護されたデータは、通常は統計機密委員会に相談した上で、統計目的や公的利益に関わる科学的・歴史的研究のための要求に応じて提供される。
- 統計の機密性は、国内法である統計に関する義務、調整及び秘密に関する法律（1951年6月7日付法律第51-711号）上の義務から、他方では一般データ保護規則（GDPR）や欧州統計規則223号によって定められた欧州法上の義務から生じる。
- 統計上の機密性とは、統計目的で収集されたデータが、対象となる個人や法人に関する意思決定の目的で使用されたり再利用されたりしないことを意味する。特に、税務調査や経済的抑圧の目的での使用や再利用は厳格に禁止される。統計上の機密性は主に個別データに適用されるが、集計された統計結果にも適用される場合がある。収集された情報が法律で定められた目的以外に使用されないことを保証することで、統計上の機密性は関係者間の信頼を確保する。
- 統計目的で収集または処理されたデータにアクセスする人（面接官、調査員、統計家、承認された申請者）は、統計上の機密保持の対象となる。

➤ 統計情報の普及への応用

- 統計の機密性では、対象となる個人や法人が特定されるような統計結果の公開は除外される。この義務によって、公開できる情報の詳細が制限される。特に、個人に関するデータの公開に関して適用されている（行政と市民の関係に関するコード第L312-1-2条）。また情報源の種類、データの性質、関係する個人や企業によって変わることがある。
- 個人に関しては、ルールは特に人口センサスのために設定されている。
- 企業に関しては、一般的には、3社未満が対象の場合や、単一の企業がその価値の85%以上を占める場合には結果は公開されない。しかし、企業または事業所の登録簿から抽出されたリストの公表には、経済活動、従業員の階級、売上高の範囲が記載されることは認められている。

➤ ミクロデータファイル

- いくつかの種類の子マイクロデータファイルは、データの詳細レベルや要求者の性質に応じた手続きや配布ルートを通じてアクセスできる。

➤ 一般向け

- 詳細ファイル：ウェブサイト（insee.fr）で提供されている詳細ファイルは、Insee が実施した調査や統計作業に関連する匿名化された個人レコードを含む電子データベースです。これらのファイルは無料でダウンロードでき、サイトの法的通知の範囲内で、商用利用を含めてライセンス料や使用料を支払うことなく再利用することができる。

➤ ヨーロッパ及びフランスの研究促進政策

- Réseau Quetelet: フランスの人文・社会科学データアクセスポータルは、フランス人および外国の研究者が研究に必要なデータベース、特に主要な調査、国勢調査、およびフランスの公的統計システムのその他のデータベースを手に入れるようにしています。配布は無料で行われるが、専用の研究目的などいくつかの条件がある。利用可能なデータの詳細、アクセス手順、注文方法については、クエトレネットワークのウェブサイトに記載されている。いずれの場合も、研究者は個別の契約に署名する必要がある。
- Secure remote data access center: もし上記の解決策だけでは研究者のニーズを満たせない場合、研究と公式統計のためのサービスを提供する事業者であるデータ安全アクセスセンター（CASD）（INSEE、GENES、CNRS、HECパリ、エコール・ポリテクニクで構成される公共団体）が、より詳細なレベルで機密性が求められる公式統計の個別データを、高度に安全な条件で扱えるように設計された設備を提供している。そのため、CASDへのアクセスを申請する必要がある。アクセスは法で定められた認可手続きによって与えられ、統計機密委員会による一連の手続きを踏む必要がある。

出所：<https://www.insee.fr/en/information/2388575>

ガイド：https://www.insee.fr/en/statistiques/fichier/2388575/guide-secret%2028%2007%202018_EN%20relu_PR%20_2509.pdf

背景資料3 フランス（マイクロデータの提供）

➤ 個人データと機密保護

- INSEEおよび省庁統計部門は公的統計目的のために、行政機関は職務遂行の過程で、企業は経営管理目的のために、大学は健康など様々な分野の研究目的のために、個人および企業に関する大量の個人データを収集している。さらに、クレジットカード決済などの電子的手段の利用に伴う個人データが自動的に収集され、その量は増加し続けている。これらの情報は、研究上特に重要な幅広い分野をカバーしている。具体的には、所得、資産、健康、企業の会計データ、地理的位置情報、就学状況、職業上のキャリアなどが含まれる。
- これらのデータのすべてが直接識別データ（氏名や社会保障番号、住所などの識別子）というわけではないが、その精度の高さから、多くが間接的識別データとなっている。一部のデータは法律上センシティブなデータとされており、対象となる個人や企業が特定された場合のリスクはさらに大きくなる。企業については、最小限の情報があれば通常は特定が可能。

➤ 研究者の特有のニーズ

- データは、分野に応じた規制や法律によって様々な形態の機密保護の対象となっている。具体的には、税務上の機密、医療上の機密、刑事上の機密、業務上の機密、そして一般的な職業上の機密がある。公的統計の場合、統計職員の機密保護義務は法律に明記されている。この機密保護義務は「統計的機密」と呼ばれ、職業上の機密の特殊な形態となっている。一般的に、これらの様々な規定は当初、研究目的を考慮していなかった。しかし、研究者がこの非常に豊富なデータソースを定量的分析に活用できるよう、規定は段階的に改正されてきた。
- ケトレネットワーク（Quetelet network）を通じた匿名化された公的統計データへの研究者アクセスに関する初期の進展は、研究者に直接送付されるこれらの詳細度の低いファイルが大きな前進を意味するものの、多くの研究プロジェクトの要件を満たすものではなかった。個人データに関するCNIL（情報処理・自由委員会）の懸念の高まりにより、これらのデータの詳細度はさらに低下し、例えば特定の人口統計学的研究や都市社会学的研究が実施不可能になる場合もあった。並行して、より効果的な計算手段と組み合わせた新たな統計手法が非常に詳細な情報を必要とするようになり、特に経済学者の間では、公共政策の評価に関連する行政データを分析目的でますます活用することが可能になってきた。
- これらの要件を満たすため、「1951年法」として知られる統計的機密に関する法律は、すでに数回の改正を経ていたが（特に研究者が企業データを利用できるようにするための改正）、2008年には研究目的での個人・世帯に関するデータの利用を対象とするよう拡大された。すべての個人データに関するこの趣旨の改正は、2004年の情報処理・自由に関する法律においてなされた。その後、特に税務データの分野においても、他の規定の改正が続いた。
- 法的な発展だけでは、データの機密性を保護するには不十分であった。データへの実際のアクセス時には、追加的な技術的保護措置を提供する適切なセキュリティ対策を適用する必要がある。これらの措置は非常に高い水準を要求するものであり、その機能上、公的統計部門の外部よりも内部において適用が容易であることは明らかであった。このことが、大学や研究センターなどの機関にデータを送付する前に、そのような措置を適用できるようにするために対処しなければならなかった困難さであった。公的統計部門を超えてセキュリティの仕組みを拡張し、データへのアクセスに関する研究者のニーズに応えるという目的のもと、INSEEとGENESはセキュアデータアクセスセンター（CASD）を設立しました。当初は公的統計から得られるデータへのアクセスに焦点を当てていた。

➤ セキュアデータアクセスセンター（CASD）

- CASDは、2018年12月29日の省庁間令により設立された、INSEE、GENES、CNRS、École Polytechnique、HEC Parisを結集した公共利益グループ（コンソーシアム）
- コンソーシアムの主な目的は、非営利の研究、研究、評価、イノベーションのための機密データの安全なアクセスサービスを組織し、実施すること。これらの活動は主に公共の「研究サービス」と呼ばれる。また、機密データ（公的および非公開）へのアクセスを確保するために開発された技術の普及も使命としている。SD-Boxはセキュアアクセスコンピュータボックスで、機密データが保護されている安全なインフラへのリモートアクセスを可能にし、このデータ保存と処理の場所は「セキュアバブル」と呼ばれている。
- 現在、CASDはINSEE、司法省、国民教育省、農業省、食品省、経済省、財務省の税務データを公開。後者の場合、実装命令でアクセスはCASDを通じて提供されなければならない。医療分野では、フランスのすべての公立および民間病院の滞在データ（ATIH PMSIデータ）や特定の健康コホートのデータへのアクセスがCASDを通じて可能。
- 民間セクターでは、多くの企業がすでにCASDのパートナーとなっており、研究者、スタートアップ、コンサルタントとの協力を通じて外部アクセスを通じてデータのセキュリティを強化。
- 2026年6月現在、CASDは575のデータソースが安全に提供されている。また、開始以来、2050のプロジェクト、1233の機関、8199人のデータ利用者に利用されている。
- 400を超える出版物や発表（記事、書籍章、書籍、論文、論文、報告書、会議論文など）が、CASDが提供するデータを利用してユーザーによって作成・引用されている。

背景資料3 フランス（二次的利用関連規定）

＜統計に関する義務、調整及び秘密に関する法律（1951年6月7日付法律第51-711号）＞

第6条においては以下を規定。

- 刑事訴訟法典第40条、第56条、第76条、第97条及び第99条の規定、並びに文化遺産法典第L.213-3条の規定を留保し、本法第2条に定める査証を付された調査票に記載された個人情報であって、個人的・家族的生活、及び一般的に私的性質の事実・行動に関するものは、公的統計又は科学的・歴史的研究を目的とした申請に関して統計秘密委員会の意見を聴取した上で行われる公文書館行政の決定がある場合を除き、調査実施日から75年、又は本人の死亡日から25年（後者の期間の方が短い場合）が経過するまで、受託機関から一切開示されてはならない。
- 刑事訴訟法典第40条、第56条、第76条、第97条及び第99条の規定、並びに文化遺産法典第L.213-3条の規定を留保し、本法第2条に定める査証を付された調査票に記載された経済的又は財政的性質の個人情報は、統計秘密委員会の意見を聴取した上で行われる公文書館行政の決定がある場合を除き、国勢調査又は調査の実施日から25年が経過するまで、受託機関から一切開示されてはならない。
- これらの情報は、いかなる場合も税務調査又は経済的制裁を目的として使用されてはならない。租税手続法典第L.84条及び関税法典第64条A条の規定の適用により、この種の情報を保有する行政機関は情報提供義務を負わない。
- 第4条に定める条件のもとで調査の仲介機関として機能する公共機関及び団体の職員は、刑法典第226-13条及び第226-14条に定める制裁のもとで職業上の秘密保持義務を負う。
- 本法の規定に従って実施された国勢調査及び統計調査は、公文書の性格を有する。

第6条の2においては、以下を規定。

- 統計秘密委員会を設置する。同委員会は、統計に関する秘密に関するあらゆる問題について意見を述べる権限を有する。同委員会は、本法の適用により収集された個人データの開示申請について意見を述べる。
- 委員会は、国務院副大臣に指名された行政裁判所の裁判官が委員長を務める。特に委員会には国民議会及び上院の代表者が含まれる。
- 委員会の構成及び運営方法は、国務会議の政令により定める。
- 統計秘密委員会の意見を踏まえた大臣決定に基づくデータ開示の受益者は、当該データをいかなる者にも開示しないことを誓約する。本項の規定に対するいかなる違反も、刑法典第226-13条に定める刑罰に処せられる。

背景資料3 フランス（二次的利用関連規定）

<統計に関する義務、調整及び秘密に関する法律（1951年6月7日付法律第51-711号）>

第7条の2においては、以下を規定している。

- 経済担当大臣の要請に基づき、国家統計情報評議会の意見を聴取した上で、かつ法律の別段の定めがある場合を除き、行政機関、公法上の法人、又は公共サービスを管理する私法上の法人がその使命の遂行において収集した自然人に関する情報（性的生活に関するデータを除く）及び法人に関する情報は、統計作成のみを目的として、国立統計経済研究所又は各省統計部局に提供される。
- 前項の条件のもとで収集された健康に関する個人データは、保健担当大臣の要請に基づき、公衆衛生政策の策定、実施及び評価に参加する省の統計部局に対し、人口の健康状態、公衆衛生政策又は人口の罹患率に関連する医療・社会保障制度による対応に関する統計の作成の枠内においてのみ、国立統計経済研究所又は当該省の統計部局に提供することができる。第2条に定める事前査証を付された補完的調査を、これらの人口のサンプルに対して実施することができる。
- 前項の条件のもとで収集された健康に関する個人データの提供方法は、個人の識別を可能にするものであってはならない。
- ただし、第2項に定める統計の作成条件上、特に人口サンプルの設定及び複数の情報源からのデータの照合を目的として、個人の直接的又は間接的な識別要素を必要とする場合は、1978年1月6日付法律第78-17号（情報処理、ファイル及び自由に関する法律）の規定を遵守した上で、この最後の義務の例外が認められる。
- 国立統計経済研究所又は公衆衛生政策の策定、実施及び評価に参加する省の統計部局に送信された健康に関する個人データを受領できるのは、処理を実施する権限を与えられた法人が当該目的のために指定した作業責任者のみとする。これらのデータを使用した後、個人の識別要素は廃棄されなければならない。
- 刑事訴訟法典第777-3条を留保し、前各項の規定は職業上の秘密保持に関するすべての反対規定にかかわらず適用される。
- 1978年1月6日付法律第78-17号第2条に定義される個人データに関する提供は、同法の規定に従う。規則行為及び、提供が2つの異なる法人間で行われる場合には、提供者と受領者の間の契約において、送信の方法、予定される処理の目的及び統計処理目的での使用後の情報の取扱いを定める。
- **法人に関する情報の提供は、経済担当大臣及び関係大臣の共同決定により承認される。**
- **刑事訴訟法典第40条、第56条、第76条、第97条及び第99条の規定を留保し、本条の規定に基づき送信された情報であって、適用対象となる自然人又は法人の識別を可能にするものは、受益機関から一切提供されてはならない。**
- 国立統計経済研究所の職員及び各省統計部局の職員は、本条の規定に基づき知ることとなったデータについて、刑法典第226-13条に定める制裁のもとで職業上の秘密保持義務を負う。

第7条の3においては、以下を規定している。

- **統計秘密委員会の全体会議は、関係データを収集した行政機関又は法人の任意の意見を聴取した上で、本法第7条の2の規定に基づき国立統計経済研究所及び各省統計部局に送信された個人データへの科学的研究目的又は経済的研究目的でのアクセスに関する勧告を発する権限を有する。**

背景資料3 フランス（二次的利用関連規定）

<情報処理、ファイル及び自由に関する法律（1978年1月6日付法律第78-17号）>

第4条では以下を規定している。

個人データは以下のとおりでなければならない。

- 1° 適法、公正に処理され、第II編の適用を受ける処理については、データ主体に対して透明な方法で処理されること。
- 2° 特定の、明示的な、かつ正当な目的のために収集され、それらの目的と両立しない方法でその後処理されないこと。ただし、公益上のアーカイブ目的、科学的・歴史的研究目的又は統計目的のためのその後の処理は、2016年4月27日付規則（EU）2016/679及び本法律の当該処理に適用される規定に従って行われ、かつデータ主体に対する決定のために使用されない場合には、当初の収集目的と両立するものとみなされること。
- 3° 処理目的との関係で適切、関連性があり、かつ必要な範囲に限定されること。第III編及び第IV編の適用を受ける処理については、過剰でないこと。
- 4° 正確であり、必要に応じて最新の状態に保たれること。処理目的との関係で不正確な個人データは、遅滞なく消去又は訂正するためのあらゆる合理的な措置が講じられなければならないこと。
- 5° データ主体を識別できる形式で、処理目的のために必要な期間を超えて保存されないこと。ただし、個人データは、公益上のアーカイブ目的、科学的・歴史的研究目的又は統計目的のためにのみ処理される場合には、当該期間を超えて保存することができること。公益上のアーカイブ目的で保存されるデータの選択は、文化遺産法典第L.212-3条に定める条件に従って行われること。
- 6° 適切なセキュリティを確保する方法で処理されること。これには、不正若しくは違法な処理、並びに偶発的な損失、破壊若しくは損傷、又は権限のない者によるアクセスに対する保護が含まれ、適切な技術的・組織的措置を用いること。

背景資料3 ドイツ（データの匿名性）

データの匿名性

- ▶ 公的統計のマイクロデータは厳格な機密保持の対象となっているのが原則。しかし、連邦統計法(BStatG)の特別規定により、特定の要件が満たされれば統計分析目的でマイクロデータが渡されることが認められている。
- ▶ マイクロデータが回答者または関係者に割り当てられない場合、すなわち、データから情報提供者となる単位や個人を特定できない場合（絶対的な匿名性）、これらのマイクロデータは公的統計の安全な施設の外でも使用することができる(連邦統計法第16条第1項第4項)。その場合、データは絶対的な匿名性の基準を満たす。
- ▶ 科学的研究の目的のために、連邦統計法は、回答者または統計単位に割り当てることが「時間、費用、人員の面で不合理な労力を必要とする場合」にマイクロデータを提供することを許可している。これは、データが事実上匿名であることを前提としている。「連邦統計局及び州の統計局に特別に保護された区域内」では、形式的に匿名化されたデータへのアクセスが特定の条件下で認められる場合がある。いずれの場合も、データは「高等教育機関または独立した科学研究を任務とするその他の機関」にのみ提供することが可能。さらに、データを受け取る者は、公務員であるか、または特別に宣誓した者でなければならない(連邦統計法第16条第6項)。
- ▶ 連邦および連邦州統計局の研究データセンターは、これらの規定に基づき匿名化されたデータを提供している。データの匿名性のさまざまな程度については以下で説明。

<データの匿名性の程度>

形式的な匿名性(Formal anonymity)

特に機能的または地域的に深く構造化された分析のために、公式統計の研究データセンターは、データ利用者が遠隔実行の枠組み内または安全なセンターで形式的に匿名化されたマイクロデータを分析する機会を提供しています。形式的な匿名化を実施するために、直接識別子および補助的特徴はデータセットから削除されますが、その他すべての特徴および機能的・地域的構造は変更されずに保持される。

事実上の匿名性(Factual anonymity)

- ▶ マイクロデータは、完全に再識別（個体の特定化）ができない場合でも、個人を再識別するために、過度の時間、費用、および人的資源を費やさなければならない場合（連邦統計法第16条(6)）、事実上の匿名化と呼ばれる。連邦統計法においては、事実上の匿名化データは科学的プロジェクトの目的のみに限り、科学機関に提供することが可能。
- ▶ 事実上の匿名化の主な目的は、統計的に関連する情報価値を維持しながら、変数の値をそれぞれの統計単位に正しく割り当ててをほぼ不可能にすることである。これを達成するため、様々な匿名化手順を適用。一般的には、情報の削減(例:集約、分類)や情報の改変(例:スワッピング)などの手法が用いられる。事実上の匿名化を判断するには、再識別（個体の特定化）の費用と利益を評価する必要がある。
- ▶ しかし、研究データセンターにおける事実上の匿名化は、データの残存情報価値だけでなく、データの使用パラメータとそれに伴う再特定の可能性に関わる問題でもある。マイクロデータセットが事実上匿名化されているとみなせるかどうかは、アクセス条件にも依存する。統計単位について、どの程度の追加知識が利用可能であるか、またデータがどこで使用されるかが決定的に重要。マイクロデータが外部で使用されるか統計局で使用されるかによって、事実上の匿名性は、情報の損失がより大きい場合(科学的利用ファイル)や小さい場合(安全なセンター)に達成され得る。
- ▶ 事実上の匿名マイクロデータは、外国の科学者が統計局の安全な施設、すなわち安全なセンターでのみ使用可能です。科学的利用ファイルは法的な理由から外国へ送付できません。
- ▶ 事実上匿名化されたマイクロデータは、外国の科学者によって統計局の安全な施設、すなわちセーフセンター内でのみ使用することができる。科学利用ファイルは、法的な理由により外国に送ることはできない。

絶対的な匿名性 (Absolute anonymity)

- ▶ 完全に匿名化されたデータは、粗くなったり個々の変数を除去したりして、回答者の特定が不可能になるほど修正される。公的統計は、パブリックユースファイル(PUF)という形で完全に匿名化されたマイクロデータを提供しています。これらはすべての関心のある個人や機関に提供可能です。さらに、方法論的教育のための完全匿名のキャンパスファイルも存在します。

背景資料 3 ドイツ（匿名性に応じた提供）

▶ ドイツ連邦統計局研究データセンター(RDC)

- ・公的統計の研究データセンターは、ドイツ連邦統計局の研究データセンターと連邦州統計局の研究データセンターの組織的に分離された2つのRDCで構成されている。
- ・研究データセンターは、公式マイクロデータへのアクセスにさまざまな機会を提供する。現地と非現地でアクセス方法が異なる。
- ・以下に示すアクセス方法は、利用可能なデータの匿名性とデータの提供方法の点で異なる。データアクセスは特定の条件に結びついている。

▶ データアクセスの方法

匿名化の程度						大
	オンサイト利用		リモートアクセス	オフサイト利用		
アクセス種別	セーフセンター	リモートエグゼキューション	リモート科学利用ファイル (Remote-SUF)	科学利用ファイル (SUF)	パブリックユースファイル(PUF) / キャンパスファイル	
データ匿名化の程度	形式的な匿名性	形式的な匿名性	事実上の匿名性	事実上の匿名性	絶対的な匿名性	
利用資格	研究機関※ 1	研究機関※ 1	研究機関※ 1	研究機関※ 1	制限なし	
データ保存場所	統計局	統計局	統計局	研究機関※ 3	制限なし	
利用場所	RDCの所在地	制限なし	研究機関※ 2	研究機関	制限なし	

大 分析可能性

※ 1 高等教育機関または独立した科学研究の任務を委ねられたその他の機関（連邦統計法第16条第6項）

※ 2 データの使用には、要求する機関がドイツに所在し、特定の技術的および組織的要件を実施する必要があります。リモートアクセスシステムへのアクセスは、ドイツ国内の要求している科学機関の施設内でのみ許可されます。

※ 3 ミクロデータの事実上の匿名化により、公的統計の保護された施設の外でも使用できる。その前提条件として、申請機関が欧州連合に所在していること、提供されたデータがEU内の申請科学機関の施設内でのみ使用されることが必要。

背景資料3 ドイツ（匿名性に応じた提供）

<現地での利用>

➤ セーフセンター

- 研究データセンター(セーフセンター)のすべての場所で、ゲスト研究者向けのPC作業スペースがある。これらは研究者が統計局の安全な施設内でマイクロデータを分析するために使用できる。データはすでにデータアクセス規制やPC作業スペースの設備によって保護されているため、セーフセンターのマイクロデータはデータの機密性に依拠して、事実上または形式的に匿名化された形で提供することができる。連邦統計法(BStatG)第16条第7項に従った統計上の機密保持義務を負うことが、セーフセンターを利用するための前提条件となっている。
- マイクロデータを分析できるPC作業スペースには、一般的な統計ソフトウェア(SPSS、SAS、Stata、部分的にR)が備えられている。電子メールの送受信やインターネット検索のためのインターネット接続付きの別のPCワークスペースも利用可能。1つのプロジェクトの範囲内で、セーフセンターへの複数回訪問が可能。予約は監督RDCと行う必要がある。

➤ リモートエグゼキューション

- リモートエグゼキューションを使用する場合、データ利用者はデータに直接アクセスすることはできない。利用者は、構造や変数の値に関して元の資料に似たデータ構造ファイルを受け取る。これらのファイルを使用して、SPSS、SAS、Stata または一部 R などの統計プログラムを用いてプログラムコードを作成できる。これらのプログラムコードは、統計事務所の職員によって元のデータを分析するために適用される。データ利用者は、関連する機密保持の確認後、これらの分析結果を受け取る。リモートエグゼキューションを通じて、形式的に匿名化されたマイクロデータを分析できる。1つのプロジェクトの範囲内で複数のプログラムコードを提出することが可能。

<リモートアクセス>

➤ リモート科学利用ファイル (Remote-SUF) ※2025年1月から提供開始

- リモート科学利用ファイル (Remote-SUF) は、公的統計から取得される事実上匿名化されたデータセットであり、RDCのリモートアクセスシステムを通じてアクセスできる。データの利用には、申請機関がドイツに所在し、特定の技術的および組織的要件を実施することが必要。リモートアクセスシステムへのアクセスも、ドイツ国内の申請科学機関の敷地内でのみ許可される。すべてのデータ利用者は、連邦統計法 (BStatG) 第16条第7項に従い、統計上の秘密保持義務を負う必要がある。
- リモートアクセスシステムを介した分析は、StataまたはRのいずれかを使用して行うことが可能。選択した分析ソフトウェアによっては、データの使用者数に制限が課される場合がある。

<オフサイト利用>

➤ 科学利用ファイル (SUF)

- 科学利用ファイル (SUF) は、研究データセンターによって作成された標準化データセットで、共通統計データ。現地でのアクセス方法と比べて、SUFは分析の可能性がやや制限されるが、多くの科学研究プロジェクトに適するように設計されている。マイクロデータの事実上の匿名化により、公的統計の保護された施設の外でも使用できる。その前提条件として、申請機関が欧州連合に所在していること、提供されたデータがEU内の申請科学機関の施設内でのみ使用されることが必要。さらに、すべてのデータ利用者は、連邦統計法第16条第7項に従って統計上の秘密保持義務を負う必要がある。
- SUFは、分析プログラムSAS、SPSS、Stata用に提供されるか、または対応する入力ルーチンとともに提供されます。それらは、データを要求した科学機関内でのみ使用することができる。

➤ パブリックユースファイル (PUF)

- 一般利用ファイル (PUF) は、完全に匿名化されたマイクロデータ。強力な匿名化のため、利用可能な変数は限られている。回答者に関する詳細度の高い変数は集約されている。詳細な地域別の内訳は、通常、PUFに基づいて作成することはできない。PUFは、登録が完了すれば無料でダウンロードできる。
- PUFは、分析プログラムSAS、SPSS、Stataで利用可能であるか、またはそれに対応する入力ルーチンとともに提供される。それらの使用は特定の使用場所に限定されない。

➤ キャンパスファイル

- 連邦および連邦州の統計局の研究データセンターは、学校や大学の授業で公的統計のマイクロデータの利用を促進している。そのため、教育用に特別に設計されたキャンパスファイルを提供している。これらには完全に匿名化されたマイクロデータが含まれており、生徒や学生、その他関心のある人々が公的統計のマイクロデータを分析する方法に関する知識を習得し、初めての経験を積むことができる。
- キャンパスファイルは、分析プログラムであるSAS、SPSS、Stata用に提供されている。登録が完了すると無料でダウンロードすることができる。

※ 記載されたアクセス方法も自由に組み合わせることができる。例えば、安全なセンターでの作業とリモートでの実行を組み合わせることがしばしば有用。特に長期の研究プロジェクトでは、このような組み合わせは合理的であることが多い。複合アクセス手段を使うと、通常は追加コストが発生する。

背景資料3 ドイツ（二次的利用関連規定）

<連邦目的の統計に関する法律（連邦統計法・BStatG）>

第16条 守秘義務

- (1) 連邦統計のために提供された個人的及び事実的状况に関する個別データは、連邦統計の実施を委託された公務員及び公務に特別に義務付けられた者によって秘密に保持されるものとする。ただし、特別な法規に別段の定めがある場合を除く。守秘義務は活動終了後も存続する。守秘義務は以下の場合には適用されない。
 1. 関係者が書面により送付又は公表に同意した個別データ。ただし、特別な事情により他の形式の同意が適切な場合を除く。
 2. 第15条第1項に掲げる公的機関に関する一般に公開されている情報源からの個別データ。連邦統計を命じる法規に基づく回答義務が存在する場合も同様とする。
 3. 連邦統計局又は州統計局が他の回答者の個別データと統合し、統計結果として表示した個別データ。
 4. 調査対象者又は関係者に帰属させることができない個別データ。
- (2) 連邦統計の実施を委託された者及び機関間における個別データの送付は、連邦統計の作成のために必要な範囲において許容される。さらに、第3a条に基づく協力に参加する統計局間における個別データの送付、及び1つ又は複数の統計局における当該個別データの集中的処理・利用も許容される。
- (3) 連邦統計局は、州統計局に対し、それぞれの調査範囲に関する個別データを地域レベルでの特別処理のために送付することができる。連邦及び州の国民経済計算及びその他の総合システムの作成のために、連邦統計局及び州統計局は相互に連邦統計からの個別データを送付することができる。
- (4) 立法機関への提出及び計画目的（ただし個別事案の処理を除く）のために、連邦統計局及び州統計局から連邦・州最高官庁に対し、表のフィールドが1件のみを示す場合であっても、統計結果を含む表を送付することができる。第1文に基づく送付は、連邦統計を命じる法規において連邦・州最高官庁への個別データの送付が許容されている場合に限り許容される。
- (5) **専ら統計目的のために、連邦統計局及び州統計局から市町村及び市町村連合の統計業務を担う機関に個別データを送付することができる。これは、連邦統計を命じる法律において送付が規定され、かつ送付すべき個別データの種類及び範囲が定められている場合に限る。送付は、州法により当該機関が他の市町村行政機関から分離されることが確保され、かつ組織及び手続により統計秘密が保証されている場合に限り許容される。**
- (6) **科学的项目の実施のために、連邦統計局及び州統計局は、独立した科学的研究を任務とする大学又はその他の機関に対して、以下のことができる。**
 1. **不均衡に多大な時間・費用・労力をかけなければ帰属させることができない個別データ（事実上匿名化された個別データ）を送付すること。**
 2. **連邦統計局及び州統計局の特別に保護された区域内において、守秘義務の遵守のための有効な措置が講じられている場合に、形式的に匿名化された個別データへのアクセスを認めること。**
 3. **受益者は、公務員、公務に特別に義務付けられた者、又は第7項に基づき義務付けられた者に限られる。**
- (7) 第6項に基づいて個別データを受領すべき者は、公務員又は公務に特別に義務付けられた者でない場合、送付前に守秘義務を課されるものとする。
- (8) 特別な法規又は第4項、第5項若しくは第6項に基づいて送付された個別データは、送付された目的にのみ使用することができる。第6項第1文第1号の場合、科学的项目が完了した後、速やかに削除するものとする。個別データが送付される機関においては、組織的及び技術的措置により、公務員、公務に特別に義務付けられた者、又は第7項第1文に基づき義務付けられた者のみが個別データを受領者となることを確保するものとする。
- (9) 特別な法規又は第4項、第5項若しくは第6項に基づく送付は、内容・送付先機関・日付・送付目的について統計局が記録するものとする。記録は少なくとも5年間保存するものとする。
- (10) 第1項に基づく守秘義務は、特別な法規、第5項、第6項又は第4項に基づく表の受領者にも適用される。第4項に基づく送付における公知の事実については、この限りでない。

第21条 再識別の禁止

本法律又は連邦統計を命じる法規の業務範囲外において、個人・企業・事業所・作業場への帰属を確立する目的で、連邦統計からの個別データ又はかかる個別データを他のデータと統合することは禁止される。

第22条 刑事罰規定

第21条に違反して連邦統計からの個別データ又はかかる個別データを他のデータと統合した者は、1年以下の自由刑又は罰金刑に処する。

背景資料3 シンガポール（マイクロデータの提供状況）

匿名化マイクロデータアクセスプログラム（AMAP）

- 学術研究者とのデータ共有をより促進するため、2021年4月に統計法を改正し、シンガポールの自治大学（Autonomous Universities：AUs）の常勤研究者への匿名化マイクロデータへのアクセスが拡大されました。資格を満たす研究者は、DOSの匿名化マイクロデータ・アクセス・プログラム（AMAP）に参加できるようになり、統計法に基づいて収集された匿名化マイクロデータへのアクセスや、DOS Innovation Data Labにおける研究課題に対応した複雑な分析の実施が可能となっている。

匿名化マイクロデータの重要性

- マイクロデータとは、個人・世帯・事業所に関する個別レベルのデータを指し、統計的集計（例：レコードの分類）に使用され、統計分析やモデリング（例：変数の変換、回帰分析、機械学習）において最大限の柔軟性を提供する。しかし、研究者がマイクロデータから個人・世帯・事業所を特定できる場合、個人情報への暴露の問題が生じる可能性がある。そのため、統計情報の損失を最小限に抑えながら再識別リスクを低減するために、マイクロデータの匿名化が必要。グローバル再コーディングやマイクロ集計などの匿名化技術を適用することで、個人・世帯・事業所の身元が容易に判明・特定されない安全なデータセットが作成される。

DOSにおけるFive Safes Framework

- カナダ統計局、オーストラリア統計局、英国国家統計局などの海外NSOと同様に、DOSのAMAPは学術研究者に研究目的での匿名化マイクロデータへのアクセスを提供している。データの機密性を確保するため、DOSはFive Safesフレームワークを採用。



Safe Project（安全なプロジェクト）

すべてのAMAPプロジェクトは、DOSの統計長官（CS）が議長を務める省庁横断パネルによって審査・承認される。



Safe People（安全な利用者）

承認された研究者のみがAMAPプロジェクトに参加。



Safe Data（安全なデータ）

個人・世帯・事業所の再識別を防ぐため、マイクロデータは匿名化される。



Safe Setting（安全な分析環境）

データへのアクセスはDOS Innovation Data Lab内のみで許可される。



Safe Output（安全な分析結果）

Data Labから持ち出せるのは、漏洩リスクのない統計結果のみ。

背景資料3 シンガポール（マイクロデータの提供状況）

➤ AMAPを通じてアクセス可能な企業・個人に関する包括的で豊富なマイクロデータセット

- AMAPを通じてアクセス可能な匿名化マイクロデータセットには以下が含まれる：
 - 製造業活動センサス（2002年～2022年）
 - 年次産業調査（2009年～2022年）
 - 一般世帯調査（2005年、2015年）
 - 世帯支出調査（2002/03年、2007/08年、2012/13年、2017/18年）
 - 人口センサス（2000年、2010年、2020年）

➤ AMAP参加資格

- AMAPへの参加資格を得るには、研究者は国内AUに常勤職を持ち、適切なセキュリティクリアランスを取得し、データアクセス前に法的誓約書に署名する必要がある。

➤ AMAPの申請プロセス

- AMAPの申請は2段階のプロセスで、各段階の手順は以下のとおり。

第1段階：申請

申請者は、申請者および担当責任者が署名した申請書と法的誓約書をDOSに提出し、DOSは関連するデータソース機関および政策機関とともに申請を審査。DOSは申請者に概算費用への同意を求める。

第2段階：承認

DOSは匿名化マイクロデータ審査パネル（AMRP）に承認のための推薦を提出。承認された場合、DOSは申請者に結果を通知。研究者はDOS Innovation Data Labで匿名化マイクロデータにアクセスすることができる。

※担当責任者は、研究プロジェクトを監督する申請者の自治大学の部門長/副学長またはそれに相当する職位の職員でなければならない。

※AMRPは主要なデータ機関および政策機関のメンバーで構成され、各AMAP申請の審査・承認を担当します。

背景資料3 オーストラリア

➤ ABSマイクロデータプロダクト

- ABSは統計および研究目的でアクセス可能なマイクロデータ製品をリリースしている。
 - ✓ユーザー自身のコンピューティング環境にダウンロード可能な基本的なマイクロデータ
 - ✓詳細なマイクロデータファイルはABS DataLabで入手可能
- ABSはまた、基盤となるマイクロデータを活用して研究者が自動的に機密化された表、グラフ、地図(集計出力)を作成できるTableBuilderもリリース

マイクロデータプロダクト	基本的なマイクロデータ	詳細なマイクロデータ	テーブルビルダー
アクセス方法	<ul style="list-style-type: none"> • マイクロデータダウンロード • 研究者環境への他への安全な転送 	<ul style="list-style-type: none"> • DataLab 	<ul style="list-style-type: none"> • テーブルビルダー
有用性と適合性	基本的な有用性: <ul style="list-style-type: none"> • 調査 • 国勢調査サンプル 	非常に高い有用性: <ul style="list-style-type: none"> • 調査 • センサスデータ • 行政データ • 複合的な統合されたデータ 	高い有用性 <ul style="list-style-type: none"> • 調査 • センサスデータ • 行政データ • 複雑積分データ
目的	<ul style="list-style-type: none"> • 単純なモデリング • 多変量解析 • 探索的解析 	<ul style="list-style-type: none"> • 複雑モデリング • 詳細な分析 	<ul style="list-style-type: none"> • 小規模な集計表から大規模な集計表までを作成 • グラフとマップ
機密保持管理の適用			
データ処理	<ul style="list-style-type: none"> • 直接識別子の削除 • 大まかなレベル(例:州)でのみ利用可能なデータ • 変数の集計(例:5歳または10歳の年齢グループ) • リスクのある属性情報は削除されている。 	<ul style="list-style-type: none"> • 直接識別子の削除 • リスクのある属性情報は削除されている。 	<ul style="list-style-type: none"> • 直接識別子の削除 • リスクのある数値結果は削除されている。
コンテキストコントロール	<ul style="list-style-type: none"> • ユーザー登録 • 法的事業 • ユーザー環境内でのマイクロデータの安全な保存 	<ul style="list-style-type: none"> • 人々の承認 • プロジェクトの承認 • 安全なIT/物理アクセス環境 • システムから削除される出力に適用されるクリアランスプロセス 	<ul style="list-style-type: none"> • 人々の承認 • プロジェクトの承認 • 安全なIT/物理アクセス環境 • システムから削除される出力に適用されるクリアランスプロセス

背景資料3 オーストラリア

➤ ABSマイクロデータプロダクト

- ABSは統計および研究目的でアクセス可能なマイクロデータ製品をリリースしている。
 - ✓ユーザー自身のコンピューティング環境にダウンロード可能な基本的なマイクロデータ
 - ✓詳細なマイクロデータファイルはABS DataLabで入手可能
- ABSはまた、基盤となるマイクロデータを活用して研究者が自動的に機密化された表、グラフ、地図(集計出力)を作成できるTableBuilderもリリース

マイクロデータプロダクト	基本的なマイクロデータ	詳細なマイクロデータ	テーブルビルダー
アクセス方法	<ul style="list-style-type: none"> • マイクロデータダウンロード • 研究者環境への他への安全な転送 	<ul style="list-style-type: none"> • DataLab 	<ul style="list-style-type: none"> • テーブルビルダー
有用性と適合性	基本的な有用性: <ul style="list-style-type: none"> • 調査 • 国勢調査サンプル 	非常に高い有用性: <ul style="list-style-type: none"> • 調査 • センサスデータ • 行政データ • 複合的な統合されたデータ 	高い有用性 <ul style="list-style-type: none"> • 調査 • センサスデータ • 行政データ • 複雑積分データ
目的	<ul style="list-style-type: none"> • 単純なモデリング • 多変量解析 • 探索的解析 	<ul style="list-style-type: none"> • 複雑モデリング • 詳細な分析 	<ul style="list-style-type: none"> • 小規模な集計表から大規模な集計表までを作成 • グラフとマップ
機密保持管理の適用			
データ処理	<ul style="list-style-type: none"> • 直接識別子の削除 • 大まかなレベル(例:州)でのみ利用可能なデータ • 変数の集計(例:5歳または10歳の年齢グループ) • リスクのある属性情報は削除されている。 	<ul style="list-style-type: none"> • 直接識別子の削除 • リスクのある属性情報は削除されている。 	<ul style="list-style-type: none"> • 直接識別子の削除 • リスクのある結果数値は削除されている。
コンテキストコントロール	<ul style="list-style-type: none"> • ユーザー登録 • 法的事業 • ユーザー環境内でのマイクロデータの安全な保存 	<ul style="list-style-type: none"> • 人々の承認 • プロジェクトの承認 • 安全なIT/物理アクセス環境 • システムから削除される出力に適用されるクリアランスプロセス 	<ul style="list-style-type: none"> • 人々の承認 • プロジェクトの承認 • 安全なIT/物理アクセス環境 • システムから削除される出力に適用されるクリアランスプロセス

背景資料3 オーストラリア (Five Safes Framework)

- 以下は、ABSがFive Safes Frameworkをオープンデータ、基本・詳細マイクロデータファイルという3つの異なるデータアクセスチャネルに適用する方法を示す。
- 下の3つのケースすべてにおいて、どちらか一方の対策を単独で適用しても効果的な機密保持の解決策が得られる可能性は低い。しかし、5つの対策をすべてを組み合わせると、全体の開示リスクは非常に低くなる。表形式データは安全なデータと安全な出力によって最も効果的に保護される。ユーザーが自分の環境にデータを読み込むと、一部の対策は他よりも効果的に制御されることがある。データ管理者はデータの利用状況を直接監視することはできない。しかし、データ管理者はデータを直接保護することで開示リスクを軽減する。この方法の欠点は、データの有用性が一部失われること。これらのタイプのデータセットの例には以下のようなものがあります：
 - ✓基本マイクロデータファイル(ABSによって生成)
 - ✓パブリックユースファイル(PUF)
- ABS DataLabのマイクロデータファイルの扱いは、実質的に5つのすべてを対策活用しています。安全な人、安全なプロジェクト、安全な環境、安全なデータ、安全な出力はすべて管理され、情報漏洩のリスクを軽減します。これにより、適切に承認された研究者が非常に詳細なマイクロデータを安全に扱うことが可能になる。

<Five SafesフレームワークのABS適用例3例>

	ウェブサイトまたは集計表 (オープンデータ)	基本マイクロデータファイル (直接ダウンロード経由)	詳細なマイクロデータファイル (ABS DataLab経由)
安全な利用者	管理不要 誰でもオンラインでデータを閲覧可能	一部の管理 ユーザーは使用登録及び使用宣言への署名が必要で、違反は制裁や法的手続の対象となることがある。	高度な管理 ユーザーは、研修を受け、承認手続を完了し、法的拘束力のある守秘義務書及び順守宣言に署名しなければならない
安全なプロジェクト	管理不要 誰でも自分の目的で利用可能	一部の管理 ユーザーはデータを使用する目的について署名する。	高度な管理 ユーザーはデータを使用する目的を詳細に記載する必要がある。目的は実際に生成されるものと比較できる（安全な出力）
安全な分析	制御不要	一部の管理 ユーザーはデータを安全に保存し、自分の物理的及びIT環境でデータを扱う必要がある。	高度な管理 DataLabは安全で閉鎖的な環境で、仮想または現地でアクセス可能。安全なログイン、監査、監視機能、ABSスタッフによる事前確認なしにデータを削除することはできない。
安全なデータ	非常に高度な制御 データは高度に集約されている	高度な管理 データはABSによって処理され、個人が特定される可能性がないことを保証する。	適切な管理 直接識別子は削除され、必要に応じてデータがさらに処理される。データの適切な管理は、統計及び研究目的での有用性を最適化する。
安全な分析結果	非常に高度な制御 全てのテーブルはリリース前に開示の有無を確認（オープンデータの文脈では、データが安全な出力となる）	一部の制御 出力は技術的にはユーザーによって制御されるが、ABSは公開や共有の内容に関するガイドラインやルールを提供する。	高度な管理 すべての統計出力は、ユーザーに公開される前に、ABSによって情報開示の観点から評価される。出力は元のプロジェクト提案との整合性についても比較される場合がある。

背景資料3 韓国（マイクロデータの提供状況）

▶ ミクロデータ統合サービス（MDIS）

韓国統計省は、自ら作成した統計のマイクロデータを収集するだけでなく、政府部門、地方自治体、研究所など他の統計機関のマイクロデータも一元的に収集することで、人々がMDISを通じてさまざまな統計データを便利に利用できるようにしている。

サービスの拡大		2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
サービスにおける統計の数	KOSTAT	36	39	42	44	45	48	49	50	50	50
	その他	20	51	107	131	175	242	281	299	319	335

沿革	主な出来事
2024	手数料の改定、SDCとRDCの完全統合（12月末）
2023	SDCとRDCの段階的統合を開始（DBの移行）、提供データの範囲および時系列カバレッジを拡大
2022	死因情報のデータ連結システムを開発、統計データ分析サービスを開始、統計作成機関向け統計標準項目サービスを提供
2021	メタデータサービスを強化、項目名標準化サービス及びDOIサービスを導入、研究データセンター（RDC）14拠点を運営
2020	チャットボットおよびインテリジェント検索サービスを導入、研究データセンター（RDC）12拠点を運営
2019	オンライン分析サービスを提供開始、研究データセンター（RDC）10拠点を運営
2015	マイクロデータ統合サービス（MDIS）を開始、公開用マイクロデータを無償提供
2014	マイクロデータ統合サービス（MDIS）第1フェーズを実施

背景資料 3 韓国（マイクロデータの提供状況）

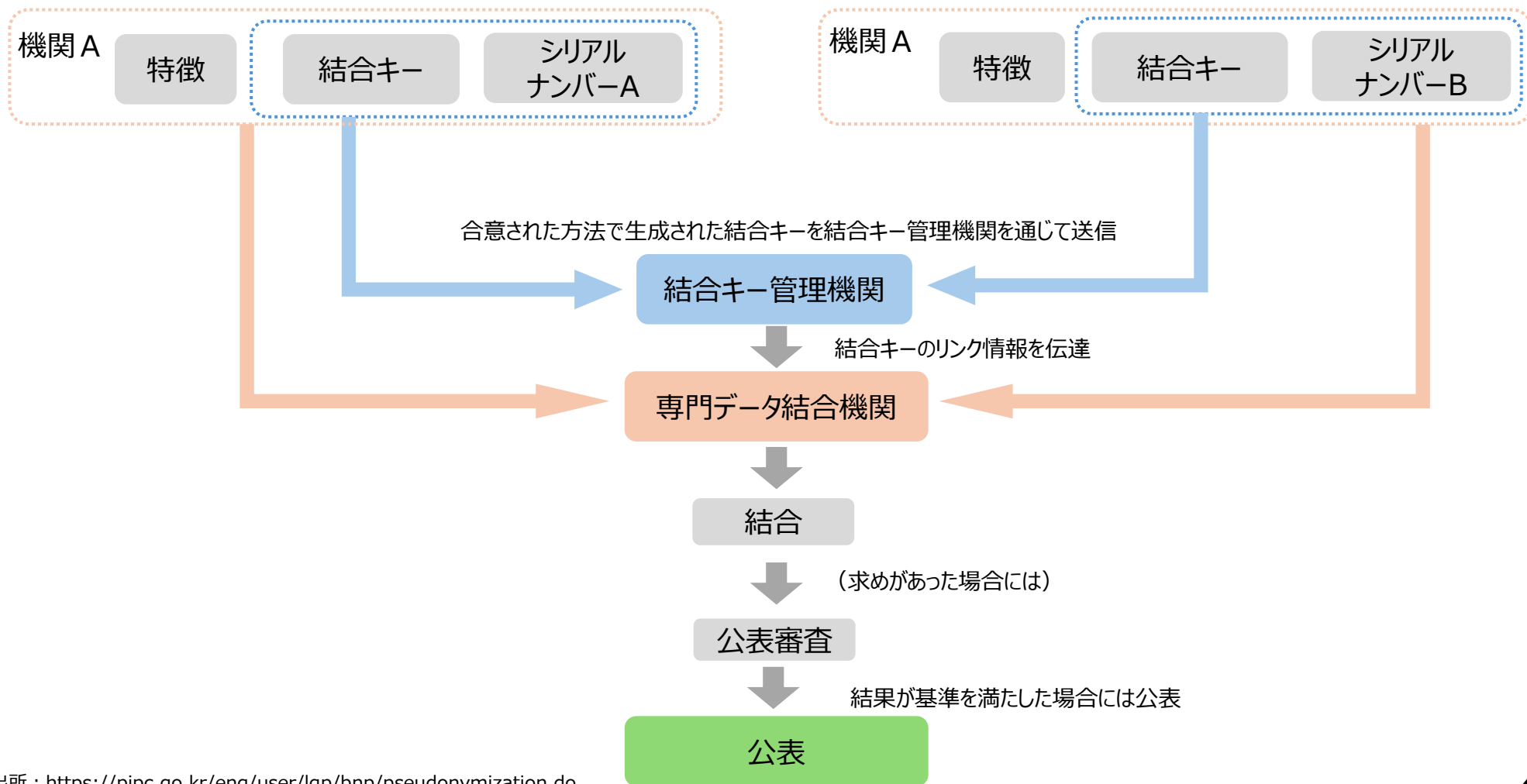
▶ マイクロデータの提供サービス

MDISでは「一般利用」と「承認利用」に分類されたマイクロデータを提供する。一般利用は、ログインのみでアクセス可能、承認利用は、オンライン申請が必要であり、承認期間は14日間程度。

サービスタイプ			データレベル	サービス料金	備考
公開サービス	ダウンロードサービス	ユーザーが選んだデータをPCにダウンロードすることを許可。	【公開データ】 個人識別情報・機微変数等を除く公開データ	無料	
	オンライン分析サービス	データの抽出・編集・分析が可能なオンライン統計分析システムへのアクセスをユーザーに提供。			
承認利用サービス	RAS：リモートアクセスサービス	自宅・職場から事前承認されたデータをリモートアクセスシステムを通じて分析することを許可。承認後に分析結果を出力することができる。	【ライセンスデータ】 RAS-公開データより項目数が多く、詳細な項目レベルのデータのみ	有料	ソウル中区センター、ソウル江南センター、ソウル上岩センター、ソウル国会センター、ソウル大学センター、ソガン大学センター、大田センター、世宗NRC、世宗KDI、光州センター、全北センター、済州センター、釜山センター、大邱センター
	SDC：統計データセンター	ユーザーがSDCで事前承認されたデータを分析することを許可。SDCは安全な物理的環境を備えており、現地訪問が必要。分析結果は承認後に出力することができる。	【ライセンスデータ】 最も多い項目数で、かつ最も詳細な項目レベルのデータを提供し、一部は、連結識別情報含む。	有料	
オンデマンドサービス	統計リスト	世帯・事業所等の統計単位リストを統計目的のためにユーザーに提供	事業所基本情報、世帯リスト	有料	
	死因統計	死因に関する統計データと、利用者が保有するデータを含む他のデータセットとのデータ連結サービスを提供	死因情報		
	統計データ分析サービス	MDISで利用可能なデータの集計・クロス集計を行い、統計表として提供	公開利用データ、承認利用データ		

背景資料 3 韓国（データリンケージ）

- 統計目的、科学研究、公益のための記録保存のために異なる個人情報管理者が処理する偽名情報の組み合わせは、保護委員会が指定した専門機関または関連する中央行政機関の長が行わなければならない（個人情報保護法第28条第3項）。
- 韓国では個人情報保護法に基づき指定された専門的なデータ結合機関（MODS、韓国信用情報院、社会保障情報院等）が運営する、物理的に隔離された環境において、複数機関の仮名化情報を安全に結合するための仕組みが採られている。データ提供機関から仮名化されたデータを受領した後、結合キー（住民登録番号の一方暗号化値等）をもとにデータを結合し、結合キーを削除したうえで申請機関に提供する。



背景資料3 韓国（データリンク等）

- 住民登録番号：韓国には全国民を対象とした固有の識別番号制度として住民登録番号（13桁）があり、行政データ連携の中核インフラとして機能。統計作成における活用方法は以下のとおり。
 - ① 直接利用：統計庁内における統計登録簿（世帯・事業体）の管理において、住民登録番号又は事業者登録番号をそのまま使用。
 - ② 非識別化による間接利用：韓国データ統計省は統計登録簿（世帯・事業体）の構築・管理にあたり、暗号化した住民登録番号を使用。外部機関のデータを結合する際には、SHA-256等の一方向暗号化アルゴリズムにより変換した「結合キー」を使用。住民登録番号の原本は開示されないが、同一人物の異なるデータセットを連携させることが可能。
 - ③ 完全削除：研究者等に提供するマイクロデータにおいては、住民登録番号を完全に削除し、統計分析に必要な属性情報（年齢・性別・地域等）のみを保持する。
- 事業者登録番号：法人統計においては、事業者登録番号（10桁）が同様の役割を担っている。韓国データ統計省の「経済センサス」等では、この番号をもとに行政データ（国税庁の税務データ、雇用労働部の雇用保険データ等）を結合し、全数調査を補完。
- 個人情報、仮名情報、匿名情報の提供状況は以下のとおり。

	提供可否
個人情報	提供不可
仮名情報	認定機関におけるデータ結合のみ許可。 ※MODS(韓国データ統計省)は必要な認定を取得しており、MODSの統計データセンターがこのサービスを提供している。
匿名情報	MDIS（マイクロデータ統合サービス）を通じて一部提供可能。非識別化ガイドラインへの準拠が必要。

背景資料 3 韓国（二次的利用関連規定）

<統計法>

第30条（統計データの提供）

- (1) 統計の作成に必要な場合、統計作成機関の長は他の統計作成機関に統計データの提供を要請することができる。この場合、要請を受けた統計作成機関の長は、やむを得ない理由がない限りこれに従わなければならない。
- (2) 統計作成機関の長は、第1項に基づき他の統計作成機関に統計データを提供するときは、特定の個人・法人・団体等が識別できない形に編集して提供しなければならない。ただし、他の統計作成機関の長が次のいずれかの調査の標本として使用するために第1項の要請を行った場合は、特定の個人・法人・団体等が識別できる形で提供することができる。
 1. 第18条第1項または第20条第1項に基づき承認または協議を経て統計データを作成するための調査
 2. 第18条第1項の承認申請または第20条第1項の協議要請がなされた統計データを作成するための予備調査
- (3) 第2項に基づき統計作成機関が提供した統計データは、提供目的以外の目的に使用し、または他者に提供してはならない。
- (4) 統計データの提供方法等に必要な事項は大統領令で定める。

第31条（統計データの利用）

- (1) 統計データを利用しようとする者は、大統領令で定めるところにより、統計作成機関の長に統計データの提供を申請することができる。
- (2) 統計作成機関の長は、第1項の申請を受けたときは、統計データの利用目的・内容・範囲の適正性を審査し、営業秘密の侵害のおそれがないと判断したときは統計データを提供する。この場合、次の場合を除き、特定の個人・法人・団体等が識別できない形に編集して提供しなければならない。
 1. 統計応答者が自己の回答に係るデータを申請した場合
 2. 第18条に基づき統計庁長官の承認を得て作成された統計のうち、センサスまたは事業体全数調査から得られた事業体名・業種・所在地等、大統領令で定める情報を提供する場合
- (3) 第2項にかかわらず、当該統計データを他のデータと比較・連結することにより次のいずれかに該当するときは、統計作成機関の長は統計データを提供しないことができる。
 1. 特定の個人・法人・団体等が識別できるとき
 2. 事業体の営業秘密が侵害される時
- (4) 第2項に基づき統計作成機関が提供した統計データは、提供目的以外の目的に使用し、または他者に提供してはならない。
- (5) 統計データの提供方法等に必要な事項は大統領令で定める。

（関連法令）：https://mdis.mods.go.kr/bbs/boardList.do?boardId=BBSMSTR_000000009004&curMenuNo=UI_POR_P9027

背景資料3 韓国（二次的利用関連規定）

➤ 韓国では、データ3法の改正により「仮名情報」の概念を導入した。これにより、仮名情報は統計作成や科学的研究、公益的記録保存目的で情報主体の同意なしに処理が可能となった。またGDPR（EU一般データ保護規則）を参考とした法整備が行われ、個人情報の定義や判断基準の明確化、個人情報保護委員会の権限強化などが実現した。

<個人情報保護法>

第2条（定義）

この法律において使用する用語の意味は次のとおりとする。

1. 「個人情報」とは、生存する個人に関する情報であつて、次の各号のいずれかに該当するものをいう。
 - (a) 氏名、住民登録番号及び映像等を通じて個人を識別することができる情報
 - (b) 当該情報のみでは特定の個人を識別することができない場合であっても、他の情報と容易に結合して識別することができる情報。この場合、容易に結合できるか否かは、他の情報の入手可能性等、個人を識別するために要する時間・費用・技術等を合理的に考慮しなければならない。
 - (c) (a) 又は (b) を第1号の2に従つて仮名処理することにより、原状に復元するための追加情報の使用・結合なしには特定の個人を識別することができない情報（以下「仮名情報」という。）**
- 1の2. 「仮名処理」とは、個人情報の一部を削除し、又は一部若しくは全部を代替する等の方法により、追加情報なしには特定の個人を識別することができないように処理することをいう。
2. 「処理」とは、個人情報の収集、生成、連携、運動、記録、保存、保有、加工、編集、検索、出力、訂正、復旧、利用、提供、公開、廃棄その他これに類する行為をいう。
3. 「情報主体」とは、処理される情報によって識別することができる者であつて、その情報の主体となる者をいう。
4. 「個人情報ファイル」とは、個人情報を容易に検索できるよう一定の規則に従つて体系的に配列し、又は構成した個人情報の集合物をいう。
5. 「個人情報処理者」とは、業務を目的として個人情報ファイルを運用するために、自ら又は他の者を通じて個人情報を処理する公共機関、法人、団体及び個人等をいう。
6. ～7の2. （略）
8. 「科学的研究」とは、技術の開発と実証、基礎研究、応用研究及び民間投資研究等、科学的方法を適用する研究をいう。

第3節 仮名情報の処理に関する特例

第28条の2（仮名情報の処理等）

1. **個人情報処理者は、統計作成、科学的研究、公益的記録保存等のために情報主体の同意なく仮名情報を処理することができる。**
2. 個人情報処理者は、第1項に基づき仮名情報を第三者に提供する場合には、特定の個人を識別するために使用されうる情報を含めてはならない。

第28条の3（仮名情報の結合制限）

1. **第28条の2にかかわらず、統計作成、科学的研究、公益的記録保存等のための異なる個人情報処理者間の仮名情報の結合は、保護委員会又は関係中央行政機関の長が指定する専門機関が行う。**
2. 結合を行った機関の外部に結合された情報を搬出しようとする個人情報処理者は、仮名情報又は第58条の2に該当する情報として処理した後、専門機関の長の承認を得なければならない。
3. 第1項に基づく結合の手法と方法、専門機関の指定と指定取消しの基準・手続、管理・監督、第2項に基づく搬出及び承認の基準・手続等必要な事項は大統領令で定める。

第28条の4（仮名情報に対する安全措置義務等）

1. 個人情報処理者は、第28条の2又は第28条の3に基づき仮名情報を処理する場合には、原状に復元するための追加情報を別途分離して保管・管理する等、当該情報が紛失・盗難・漏洩・偽造・変造又は毀損されないよう大統領令で定めるところにより安全性確保に必要な技術的・管理的及び物理的措置をとらなければならない。
2. 個人情報処理者は、第28条の2又は第28条の3に基づき仮名情報を処理する場合、処理目的等を考慮して仮名情報の処理期間を別途定めることができる。
3. 個人情報処理者は、第28条の2又は第28条の3に基づき仮名情報を処理しようとする場合には、仮名情報の処理目的、第三者提供時の提供先、仮名情報の処理期間（第2項に基づき処理期間を別途定めた場合に限る）等仮名情報の処理内容を管理するために大統領令で定める事項に関する関連記録を作成して保管しなければならない。仮名情報を廃棄した場合には廃棄した日から3年以上保管しなければならない。

第28条の5（仮名情報処理時の禁止義務等）

1. **第28条の2又は第28条の3に基づき仮名情報を処理する者は、特定の個人を識別するための目的で仮名情報を処理してはならない。**
2. 個人情報処理者は、第28条の2又は第28条の3に基づき仮名情報を処理する過程で特定の個人を識別することができる情報が生成された場合には、直ちに当該情報の処理を中止し、遅滞なく回収・廃棄しなければならない。