

2025年3月16日 日本安全保障貿易学会第39回研究大会（配布用）

経済安全保障におけるデータセキュリティ 基本的論点の整理

布施 哲

IISE国際社会経済研究所 特別研究主幹

信州大学特任教授

海上自衛隊幹部学校客員研究員

報告の骨子

- (1) なぜデータセキュリティか
- (2) マイクロターゲティングによって武器化されるデータ
- (3) 懸念国との機微データにかかわる取引を禁止、規制する
米政府による最終規則
- (4) 日本の経済安保上の論点

なぜデータセキュリティか

○データは戦略物資に

- ・安全保障的な経済安保の観点
マイクロ・ターゲティングによる「データの武器化」
- ・産業政策的な経済安保の観点
AIによるデータ解析で有意な価値を創出可能に
AIにはデータが必要。AI時代においてデータは貨幣、弾薬

○経済安保推進法でデータは規定されず

国家安全保障、産業政策の両面から保護すべきデータの定義＝
データセキュリティを規定する重要性

⇒米国は国家安全保障の観点から機微データの取引を規制へ

マイクロ・ターゲティングで集団から個人へ

【マイクロ・ターゲティング】

複数のデータを掛け合わせて分析し、個人単位の興味や嗜好を特定
それに応じたインターネット広告をカスタマイズして提示して
対象個人の行動や認識の変容を促す手法

複数のデータで個人をプロファイリング

- ・ 性別、年齢、メールアドレス
- ・ 位置情報
- ・ **スマホの端末識別情報**
- ・ 購買履歴、閲覧履歴、検索履歴
- ・ SNSへの投稿内容
- ・ SNS上の友人関係

「武器化されるデータ」への懸念

○米連邦人事局OPMハッキング事件（2015年）

110万人分の情報機関員、請負業者の身上調査書SF-86

⇒潜在的リクルート対象の特定（異性関係、飲酒歴、通院歴）

○米政府のLGBT交際アプリGrindrの買収阻止（2019年）

- ・ユーザーの位置情報、HIV感染ステータス
- ・中国のゲーム会社が買収も、翌年に米政府が白紙化の命令

⇒情報機関や軍関係者などへの工作への懸念が背景か

出典：National Security Strategy of the United States of America (Dec. 2017),

US Congressional Report “Cyber Intrusion into US Office of Personnel Management: In Brief”および米国の各種報道

米海軍幹部が描く台湾有事における 中国によるマイクロ・ターゲティング

Jared Wilhelm米海軍中佐の論文

(2019年5月、米陸軍大学現代戦争研究所)

AI解析で米軍の作戦運用を支えるキーパーソン500人を抽出

- ・ ミズーリ州のステルス爆撃機基地やグアム、沖縄の基地の指揮官、パイロット、整備士の自宅が所在する区画をピンポイントで停電
- ・ 同上の家族の携帯に脅迫テキストメッセージを送信

出典：<https://mwi.westpoint.edu/autopsy-future-war/>



米司法省 最終規則 (Final Rule)

FACT SHEET: Justice Department Issues Final Rule to Address Urgent National Security Risks Posed by Access to U.S. Sensitive Personal and Government-Related Data from Countries of Concern and Covered Persons

【目的】 国家安全保障上の理由から

- ①大量の機微な個人情報(Bulk of Sensitive Personal Data)
- ②政府関連データ(Government-Related Data)

に関する懸念国との取引を禁止もしくは規制

【懸念国の定義】

中国（香港、マカオ含む）、キューバ、イラン、北朝鮮、ロシア、
ベネエズエラ

Bulk of Sensitive Personal Dataの定義

- (1) 個人特定情報（氏名＋デバイス識別情報、運転免許証、社会保障番号などID番号）※10万人以上
- (2) 情報端末の位置情報 ※1000個以上
- (3) 生体情報（顔画像、声紋、虹彩）※1000人以上
- (4) ゲノム（エピゲノム）情報 ※100人以上
- (5) 健康情報（身長、体重、バイタルサイン、既往症歴、検査結果、診断書、歯科診断、心理診断）
※10000人以上
- (6) 資産・経済情報（クレジット信用情報、銀行口座、返済履歴ふくむ信用スコア）※10000人以上

「政府関連データ」の定義

- ①機微性の高い政府施設（軍施設、情報機関ふくむ）地理的位置情報
- ②軍、連邦職員、請負業者の現職、元職に関する個人情報



FACT SHEET: Justice Department Issues Final Rule to Address Urgent National Security Risks Posed by Access to U.S. Sensitive Personal and Government-Related Data from Countries of Concern and Covered Persons

■ 禁止される取引

- ・ データの仲介（売買）を伴う取引（Data Brokerage）
⇒ 機微個人データと政府関連データの売買を禁止
- ・ 分子レベル、RNA転写物のゲノム関連データへのアクセス
⇒ 生体情報は禁止されず

■ 規制される取引（CISA指定の安全管理措置*が課される取引）

※Appendixを参照

- ・ ベンダー契約、サービス請負取引 (Vendor Agreement)
- ・ 雇用契約
- ・ 長期投資（株式取得）

禁止取引例 データ仲介（売買）= Data Brokerage

- ①位置情報を収集する自動運転技術を持つ企業が懸念国企業に
Bulk Dataを売却
- ②懸念国の大学などから助成を受けながら、学術論文の共著者である
懸念国の研究者に生体情報を提供
- ③ターゲット広告のためにBulk Dataや政府関連データを
懸念国の企業に提供
- ④第3国企業が米モバゲーSNS企業からアプリ開発を受託。
発注元の米企業の要望でアプリにはBulk Dataが協業相手である
懸念国企業に転送される機能を付与した場合、
第3国企業は違反に。米企業も Knowinglyであれば違反に

出典：米司法省最終規則セクション202-214 Data Brokerage
<https://www.justice.gov/nsd/media/1382521/dl?inline>

規制される取引例（安全管理措置が課される取引例）

【ベンダー契約 Vendor Agreement】

- ・ 米SNS企業が懸念国の企業と位置情報を提供するサービス
- ・ 米医療機関が懸念国企業のAIサービスを導入
- ・ 懸念国のクラウド企業の米国法人が米国内にDCを建設し、
米企業向けにBulk Dataを取り扱うクラウドサービスを提供
- ・ 米ゲーム会社が懸念国エンジニアをゲーム開発のために雇用

【投資】

- ・ 米企業が米国内でBulk Dataを保存するDCを建設。懸念国のファンドが出資して過半数を取得
- ・ 米SNSモバゲー企業に懸念国企業がマイナー出資
⇒経営権がない出資でも実質的に経営判断やマネージメントに影響を及ぼしたり、
データへのアクセスが得られる場合

【雇用】

- ・ 生体情報を取り扱う米医療企業が自社IT部門に懸念国の国籍のスタッフを雇用
- ・ 米モバゲー企業が懸念国の国籍のCEOを招聘
- ・ 顔認証情報を持つ米企業がデータベース管理者に懸念国の国籍を任命
- ・ 米金融機関の顧客対応AIの開発チームにい懸念国のエンジニアを採用



最終規則が想定しているデータ悪用の脅威

「データを使って米国人のライフスタイル、購買行動、
金融資産上の問題、嗜好、通院などの個人の行動履歴の分析している」
「データがAIを改良し、改良AIによりデータ悪用がさらに洗練化」

- ・サイバー攻撃
- ・諜報活動（リクルート含む）
- ・脅迫（活動家、研究者、ジャーナリスト）
- ・軍事能力の強化

出典：最終規則ファクトシート
<https://www.justice.gov/archives/opa/media/1382526/dl>

米司法省 最終規則にみえる問題意識

- ・ AI時代におけるデータが持つ国家安全保障上のリスクに危機感
⇒ 個人情報情報の切り口で安保上、保護すべきデータを規定
- ・ 「CFIUSではデータブローカーからのデータ購入、
ベンダー契約や雇用契約を通じたデータ取得を防止できず」
⇒ 合法的な経済行為で取得されるリスクに対応＋CFIUSを補完
- ・ 「中国はAIゴールの達成のために米国人のデータを収集している」

⇒ 軍民融合を念頭に安保に加えて産業競争力からの切り口を示唆も
個人情報に該当しない産業データのセキュリティには踏み込まず

米最終規則のデータセキュリティをめぐる論点

- ・ 基準値未満なら国家安全保障、産業競争力（経済安保）の懸念材料にはならないのか？
Ex)ゲノム、自動運転、AIエージェント
- ・ 個人情報以外の産業データが懸念国主体に合法的な経済行為を通じて取得されることの経済安保上の意味は？
⇒ 技術データ、製造、運用ノウハウ、インフラ、BCPのデータ

日本の経済安保上の論点②

- ・ 米の最終規則におけるデータセキュリティを
日本の経済安保にどう規定するか？
 - 対内直接投資審査制度
 - 基幹インフラ審査制度
 - クラウド事業者のルール
 - データ・ローカライゼーションも視野？
 - 個人情報以外の産業データのセキュリティは？

Appendix CISA安全管理措置



JANUARY 2025

SECURITY REQUIREMENTS FOR RESTRICTED TRANSACTIONS

Pursuant To Exec. Order 14117, *Preventing Access To Americans' Bulk Sensitive Personal Data And United States Government-Related Data By Countries Of Concern*

On February 28, 2024, President Biden signed Executive Order (E.O.) 14117, *Preventing Access to Americans' Bulk Sensitive Personal Data and U.S. Government-Related Data by Countries of Concern*, to address national-security and foreign-policy threats that arise when countries of concern and covered persons can access bulk U.S. sensitive personal data or government-related data that may be implicated by the categories of restricted transactions.

As directed by E.O. 14117, CISA has developed the following security requirements to apply to classes of restricted transactions identified in regulations issued by the Department of Justice (DOJ). See *generally* 28 C.F.R. part 202 (identifying classes of restricted transactions at 28 C.F.R. § 202.401).

出典：https://www.cisa.gov/sites/default/files/202501/Security_Requirements_for_Restricted_Transaction-EO_14117_Implementation508.pdf