資料９

データセキュリティ制度の検討について

経済安全保障法制に関する有識者会議
推進法改正に関する検討会合
第２回資料

2025年12月４日

背景と考え方

● **背景**

✓ **国家安全保障戦略**（2022年12月16日閣議決定）や、**経済財政運営と改革の基本方針2025**（2025年6月13日閣議決定）において、「データ・情報保護について、機微なデータのより適切な管理や情報通信技術サービスの安全性・信頼性確保に向けた更なる対策を講ずる」こと等が指摘。

✓ **諸外国**においても、**機微な個人データや重要インフラを防護するための制度**の検討が進められている。

（諸外国の例）米国：米国人の機微個人データ及び政府関連データへの特定国アクセスの防止に関する大統領令 実施規則
情報通信技術・サービス（ICTS）サプライチェーン保護規則
欧州：改正ネットワーク及び情報システムに関する指令（NIS2指令）
豪州：重要インフラ安全保障法（SOCI法）

＜考え方＞

✓ データが外部に流出すること等により、「**国家及び国民の安全**」が害されることを防ぐ観点から、**データセキュリティに関する措置**が必要。

✓ 具体的には、以下２つの観点が考えられるのではないか。
① 安全保障上重要なデータを取り扱う者に関する措置
② 大量のデータの保存・処理を行うデータセンター・クラウドサービスを提供する者に関する措置

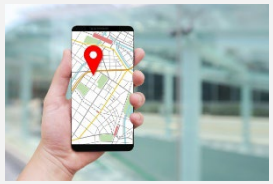
✓ その際、**民間企業**等による**自由なデータ流通や経済活動を必要以上に制限しないよう**、個人情報保護法等の既存制度を踏まえつつ検討を行う。

安全保障上重要なデータの防護について

- 「**国家及び国民の安全**」を確保する観点から、例えば**個人に関する機微なデータ**や**基幹インフラ役務の安定的な提供に必要なデータ**は、下記の観点から**安全保障上重要なデータ**として挙げられるのではないか。

（１）個人に関する機微なデータ

- ✓ 個人に関する機微なデータ（例えば一定量以上の**ゲノムデータ**、**位置情報**、**生体認証情報**、**金融情報**、**医療情報**等）が外部に漏えいした場合、**特定の個人に対する影響力行使等に利用されるリスク**があるのではないか。
- ✓ 外部への情報漏えい等を生じさせる行為として、例えば、**データ提供**、**データの保存・処理を行う情報システムの契約**、**ゲノムデータの解析依頼**等が考えられるのではないか。
- ✓ ゲノムデータ、位置情報、生体認証情報、金融情報、医療情報を取り扱う事業者は、スタートアップ企業を含め、様々な事業者が想定されるところ、民間企業等による自由なデータ流通や経済活動への影響を踏まえ、**事業者の負担が少なく、実効性のある措置を検討**すべきでないか。


（２）基幹インフラ役務の安定的な提供に必要なデータ

- ✓ **基幹インフラ役務の安定的な提供に必要なデータ**（例：特定重要設備を稼働させるために必要なデータ）が外部から**改ざん・滅失**等の行為を受けた場合、**基幹インフラ役務の安定的な提供に支障**が生じ、**国家・国民の安全を損なう事態**が生じるおそれがある。
- ✓ 当該データについては、**既存の基幹インフラ制度を通じて防護**できるよう、その**運用改善**を検討すべきでないか。

（参考）米国人の機微個人データへの特定国アクセスの脅威に対処する大統領令14117実施規則

- ✓ 米司法省は、大統領令14117（2024年2月発行）に基づき、**米国人**（法人含む）**が、特定国**（中国（香港・マカオ含む）、キューバ、イラン、北朝鮮、ロシア、ベネズエラ）**や特定国の影響下にある者と、政府関連データや閾値を超える大量の機微個人データへのアクセスを伴う特定の取引を行うことを禁止又は制限**等を行う最終規則を2025年1月に公表。本年4月8日の一部発効を経て、同10月発効。
- ✓ 同規則は、国家安全保障の観点から、機微個人データ及び政府関連データを対象に、特定国等との取引を禁止又は制限するもの。

		対象データの例	閾値
機微個人データ	①ヒトゲノムデータ等	ヒトゲノムデータ及びその他の生物学的データ（Human `omic data）	百人超の米国人※
	②生体識別情報	顔画像、音声パターン、網膜スキャン等（特徴情報を含む）	千人 〃
	③位置情報データ	1,000メートル以内の精度の個人及びデバイスの位置情報	千人 〃
	④個人健康データ	身長、体重、診断履歴、治療履歴、検査結果、診断、処方箋データ等	一万人 〃
	⑤個人金融データ	クレジットカード、銀行口座、負債、個人の信用に関わる情報等	一万人 〃
	⑥個人識別データ	社会保障番号、運転免許証番号、パスポート番号、MACアドレス等であって他の同種情報と紐づけられるもの	十万人 〃
政府関連データ		①政府関連拠点リストに列挙された地域内の正確な地理情報データ ②軍及び情報機関を含む米国政府職員、元職員、請負業者等にリンク可能な機微個人データ	－

※その他の生物学的データは、千人超

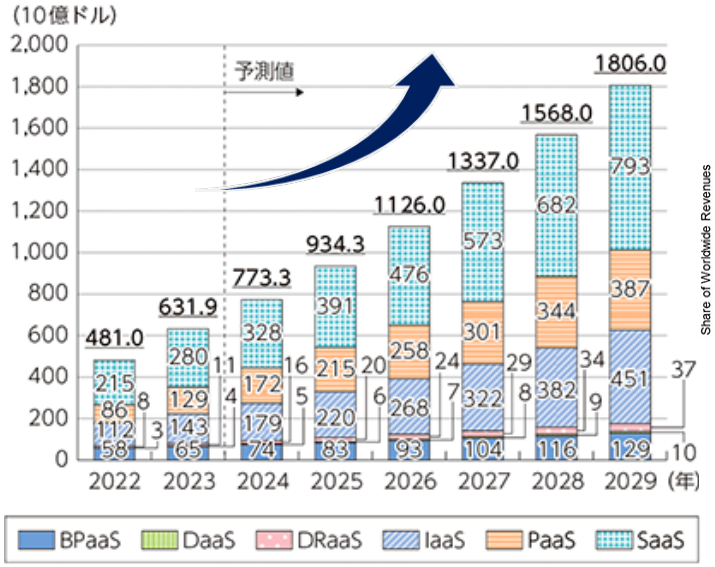
対象取引		定義
米国人は、**特定国**又は特定国の**影響下にある者**と、政府関連データ又は大量の機微個人**データへのアクセス**を伴う**以下の取引に従事してはならない**。		
禁止取引	データ**ブローカー**取引	**データの販売**、**データへのアクセスの供与**又は**類似の商取引**（ベンダー契約、雇用契約、投資契約を除く）
	その他のデータ**ブローカー**取引	特定国や特定国の影響下にある者への**データ転送を伴う**ような、（特定国人以外を含む）外国人との間で行うデータブローカー取引（契約により、特定国等の間でデータ取引を行わないこと等を担保している場合を除く）
	ヒトゲノムデータ等へのアクセスを伴うデータ取引	**ヒトゲノムデータ**等を含む大量の機微個人データ又は大量のヒトゲノムデータ等を抽出可能な試料へのアクセスを伴うデータ取引（**ベンダー契約**、**雇用契約**、**投資契約**を含む）
制限取引（※）	**ベンダー**契約	雇用契約以外の契約又は取決めのうち、支払又はその他の対価と引換えに、クラウドサービスを含む**物品又はサービスを相手方に提供するもの**
	雇用契約	**個人**が、支払又はその他の対価と引換えに、**業務を直接に遂行**するあらゆる合意または取決め
	投資契約	支払又はその他の対価と引換えに、直接又は間接的に、(1) **米国内の不動産**、又は(2) **米国法人**に関する**所有権又は権利を取得する契約又は取決め**

（※）制限取引には、サイバーセキュリティ・社会基盤安全保障庁（CISA）が定める組織・システムレベル要件及びデータレベル要件を遵守すれば従事してよい

データセンター・クラウド上のデータ防護について

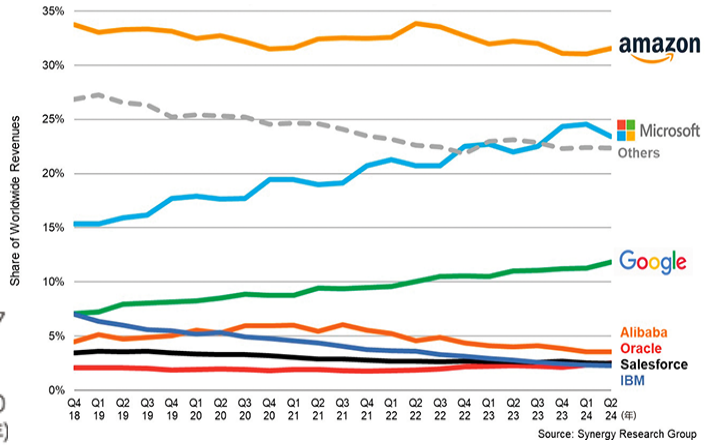
- ✓ データセンターやクラウドサービスは、**デジタル時代の社会・経済活動を支えるインフラ**であり、安全保障上重要なデータを始めとする**大量のデータの処理・保存先**となっている。
- ✓ 経済安全保障の観点から、**我が国の外部から行われる行為からデータセンターやクラウドサービスを防護するための措置**を設けることが必要ではないか。
- ✓ 具体的には、データセンターやクラウドサービス上で取り扱われる**情報の漏えいや滅失を防ぐための措置**や、データセンター・クラウド事業者を通じて、**日本国内のデータセンターの設置状況等を把握するための措置**が必要ではないか。

クラウドサービス市場規模の推移及び予測



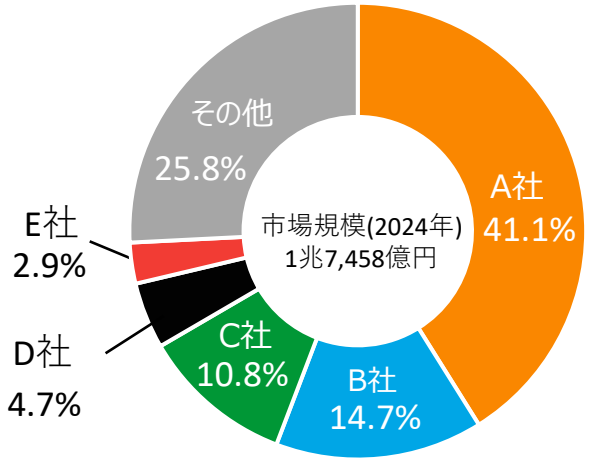
（出典）総務省「令和７年版 情報通信白書 Statista Market Insights（2025年3月14日取得データ）」を基に作成

世界のクラウドサービス市場のシェアの推移



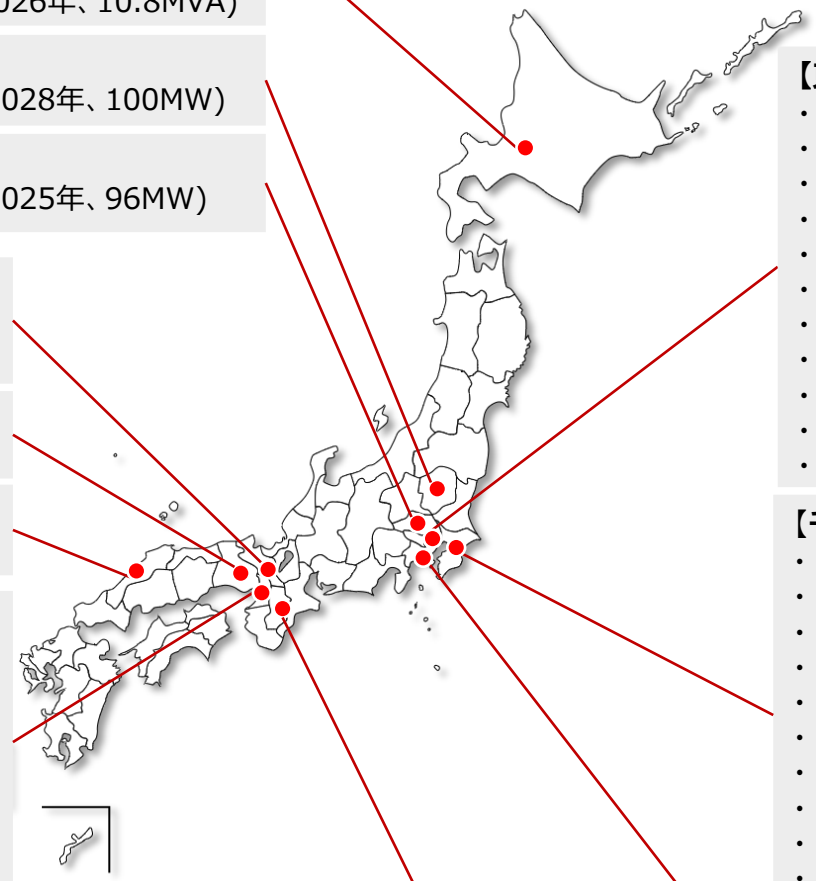
（出典）総務省「令和７年版 情報通信白書」、Synergy「Cloud Market Growth Stays Strong in Q2 While Amazon, Google and Oracle Nudge Higher」

日本のクラウドサービス市場のシェア



（出典）「2025 クラウドコンピューティングの現状と将来展望《市場編》（（株）富士キメラ総研）」における2024年の市場占有率実績を基に作成

2025年以降のデータセンターの新設計画



【北海道】
- さくらインターネット (2025年、 3.0MVA)
- さくらインターネット (2026年、 4.0MVA)
- ソフトバンク (2026年、33.0MVA)
- Flower Communications (2026年、10.8MVA)

【栃木県】
- NTTグローバルデータセンター (2028年、100MW)

【埼玉県】
- プリンストン・デジタル・グループ (2025年、96MW)

【京都府】
- ESR (2026年、72.0MVA)
- NTTグローバルデータセンター (2026年、30.0MVA)

【兵庫県】
- AirTrunk Japan (2026年、20.0MVA)

【島根県】
- インターネットイニシアティブ (2025年、1.2MVA)

【大阪府】
- NTTコミュニケーションズ (2025年、 6.0MVA)
- KDDI (2025年、 非公開)
- ESR (2026年、19.2MVA)
- オプテージ (2026年、 7.2MVA)
- ソフトバンク (2026年、100MVA)
- Vantage (2026年、28.0MVA)
- NTTグローバルデータセンター (2027年、18.0 MW)

【東京都】
- AirTrunk Japan (2025年、48.0MVA)
- Amazon (2026年、31.4MVA)
- SKYY Development (2025年、14.0MVA)
- セコムトラストシステムズ (2025年、 6.0MVA)
- デジタルエッジ・ジャパン (2025年、 4.8MVA)
- デジタルエッジ・ジャパン (2026年、 8.0MVA)
- 日本GLP (2025年、10.0MVA)
- 日本GLP (2026年、10.0MVA)
- 日本GLP (2026年、36.8MVA)
- GAW Capital (2026年、20.0MVA)
- MiTASUN (2028年、 6.0MW)

【千葉県】
- Amazon (2025年、30.0MVA)
- AirTrunk Japan (2025年、48.0MVA)
- AirTrunk Japan (2026年、48.0MVA)
- AirTrunk Japan (2026年、48.0MVA)
- MC デジタル・リアリティ (2025年、31.0MVA)
- Coltデータセンターサービス (2025年、19.8MVA)
- 日本GLP (2026年、17.7MVA)
- NTTグローバルデータセンター (2026年、50.0 MW)
- インターネットイニシアティブ (2026年、10.0 MW)
- STT GDC (2025年、32.0 MW)
- STT GDC (2027年、38.0 MW)

【奈良県】
- ソフトバンク (2025年、20.0MVA)
- 日本GLP (2026年、16.0MVA)

【神奈川県】
- SKYY Development (2025年、16.9MVA)
- 東京電力パワーグリッド (2026年、60.0MVA)

凡例
【都道府県】
・事業者名（開設年、提供可能電力(MVA)or受電容量(MW)）
※下線は外資系企業

（出典）「データセンタービジネス市場調査総覧2025年版《市場編》（富士キメラ総研）」及び公表資料を基に作成

（参考）諸外国におけるデータセンター・クラウドに関する規律

措置	目的・概要	規制対象	主な規律内容
米国ICTS規則 	**情報通信技術・サービス(ICTS)に係る国家安全保障上の脅威への対応を目的**に、商務長官が、特定の取引事案への取引の禁止・中止等を指示できる商務省規則（2024年12月 最終規則公表、2025年２月発効） ⇒ ※ **クラウドコンピューティング及びデータセンター関連設備に関する新たな規則案**を検討中。	・「情報通信、**機微個人データを処理・保管**するサービス（**クラウド・データストレージサービスを含む**。）、重要インフラといった**対象分野で必要なICTS製品・サービス**」に関する取引当事者等	特定国の影響下にある者等により供給された製品等に安保上のリスクがある場合、**商務長官は特定の取引事案ごとに審査の上、取引の禁止・中止等を指示**。 ※ 禁止・中止の効果は、対象分野以外も含め、当該製品・サービスを利用する**全ての米国内取引に及び得る。**
欧州NIS2指令 	**重要インフラのサイバーセキュリティ向上を目的**として、重要インフラ事業者への規律・監督を定めた欧州委員会指令（2022年制定・加盟国に2024年10月までの法制化を要求） ⇒ ※「レジリエンス及びサイバーセキュリティ法案（仏）」や「国内実施法案（独）」など、各国で**NIS2指令の国内法化**を実施中。 ※**セキュリティ評価手法（ICTサプライチェーンツールボックス）**（規律内容②）を検討中。	・EU域内で対象となる**重要インフラ役務を提供する事業者**（エネルギー、金融等18分野のインフラ事業者。**データセンター・クラウド事業者を含む**）	① 事業者登録 ② リスク管理措置の実施（サプライチェーンのセキュリティ確保を求め、その中で**ICTサービス・機器のセキュリティ評価（第三国の不当な影響等のリスク要因含む）の実施結果を考慮することを要求**） ③ インシデント報告
英国NIS規則 	**ネットワーク及び情報システムの安全（＝欧州NIS指令の国内法化）を目的**に、基幹サービス提供者及び関連デジタルサービス提供者への規律・監督を定めた規則（2018年制定） ⇒ ※ 一定規模以上の**データセンターを「基幹サービス提供者」に追加等を行う**改正案を審議中。	・基幹サービス提供者（エネルギー等） ・関連デジタルサービス提供者（オンラインマーケット、オンライン検索エンジン、**クラウドコンピューティングサービス**）	① 事業者登録 ② ネットワーク及び情報システムリスクへの技術的・組織的措置 ③ インシデント報告
豪州SOCI法 	**重要インフラのサイバーセキュリティ向上を目的**として、重要インフラ事業者への規律・監督を定めた法律（2018年制定・2024年最終改正）	・**重要インフラ役務提供**のために必要な豪州域内の設備（重要インフラ資産）の運用者/所有者（エネルギー、金融等11分野のインフラ事業者。重要なデータの保管・処理を行う**データセンター・クラウドサービスを含む。**）	① 重要インフラ資産の運用者/所有者登録 ② サプライチェーン対策を含むリスク管理プログラム（CIRMP）を策定し、実施状況を毎年報告（**サプライヤーが外部主体から悪影響を受けるリスクも考慮**） ③ インシデント報告
韓国情報通信網法 	**情報通信網の利用促進、利用者保護、健全かつ安全な利用環境の整備を目的**として、データセンター事業者を含む情報通信サービス提供者への規律・監督を定めた法律（1986年制定・2025年最終改正）	・情報通信サービス提供者（**データセンター・クラウド事業者を含む**） ・集積情報通信施設事業者（情報通信サービス提供者のうち、他人の情報通信サービスの提供のために集積された情報通信施設を運営・管理する者（**データセンター事業者を含む**））	① 技術的・物理的保護措置等 ② 情報保護管理体系認証取得義務（サプライチェーン対策を含む。データセンター事業者は対象だが、クラウド事業者は対象外） ③ インシデント報告 ※ 電気通信事業法における事業者登録/届出有。

制度の全体イメージ

○ データセキュリティについて以下の２つの観点で検討を進めてはどうか。
① **安全保障上重要な個人データ（ゲノムデータ、金融情報等）を取り扱う者**に関する措置
② 大量のデータの保存・処理を行う**データセンター・クラウドサービスを提供する者**に関する措置

データ取扱事業者

① 安全保障上重要な個人データの防護

安全保障上重要な個人データの取扱事業者

提供（売買等）→ 第三者
解析依頼 → ゲノム解析事業者
情報システムの導入 → 情報システムベンダー（オンプレ/クラウド）


ゲノムデータ・医療情報


金融情報


位置情報


生体認証情報

データの保存・処理

② データセンター・クラウドサービス上のデータの防護

ベンダー等
- サーバ導入等 → **クラウド事業者**
- 電源導入等 → **データセンター事業者**

※ 上記①②とは別途、基幹インフラ役務の安定的な提供に必要なデータの防護については、既存の基幹インフラ制度の運用改善等を検討。