デジタル主権の二重構造

欧州の脱パランティアとアメリカン・ビッグテックの鎖

金景珍（キム・ギョンジン）· 弁護士

目次

1.1 フランス国内治安総局（DGSI）の決断：チャップスビジョン（ChapsVision）アルゴンOSへの移行

フランス国内治安総局は、2014年に国内情報業務を担当していた既存の組織を再編して設立された機関です。テロの脅威を監視し、外国の諜報活動やサイバー攻撃に対応することが同機関の任務です。国内治安総局は2016年から、アメリカ企業パランティアのデータ分析プログラム「ゴッサム」を使用してきました。導入のきっかけは2015年11月にパリで発生したテロ事件でした。国内治安総局はテロ組織の通信記録や移動経路、資金の流れを一つの画面で確認できるツールを急ぎ必要としており、パランティアのプログラムがその穴を埋めることになりました。

フランス政府がこの依存を当初から放置していたわけではありません。内務省は2021年、形式の異なる膨大なデータを単一の国家システムで処理するフランス企業の技術を求める入札事業「OTDH」を実施しました。この入札にはチャップスビジョンをはじめ、防衛大手タレスとIT企業エビデンが共同設立した合弁会社アテア（Athea）、ソフトウェア企業ブルーウェイが参入しました。しかし、どの候補も国内治安総局の日常業務を丸ごと引き継げるほど迅速に定着するには至りませんでした。

国内治安総局が2025年12月にパランティアと再び手を組んだ背景には、このように代替技術がまだ現場に完全に根付いていなかったという現実がありました。

2025年12月15日、パランティアは国内治安総局と多年契約を更新したと発表しました。3年期限の契約でした。契約を新しく結んでから6ヶ月も経たない2026年6月、フランス政府はこの契約と真っ向から対立する決定を下します。

発端は米政府の措置でした。米国の人工知能企業アンソロピックは2026年6月9日、自社で最も優れたモデルである「フェーブル5」と「ミトス5」を公開しました。しかし3日後の6月12日午後5時12分（米国東部時間）、米政府は国家安全保障を理由に、外国籍の者によるフェーブル5およびミトス5へのアクセスを直ちに中断するよう命じる輸出規制指示を出しました。ユーザーの国籍を迅速に識別する方法がなかったため、アンソロピックは欧州を含む海外ユーザー全体のアクセスをひとまず遮断する道を選びました。

登場したばかりの最新モデルを使おうとしていた欧州の研究者や行政機関は、わずか3日でその道が閉ざされる事態に直面しました。このアクセス中断は7月1日前後に輸出規制が解除されたことで復旧しましたが、欧州側は同盟国が法律一つで中核技術へのアクセスを遮断できるという事実を目の当たりにしました。

この事件が発生する数ヶ月前、欧州議会はすでに技術依存を減らす方向へと舵を切っていました。欧州議会は2026年1月22日、欧州の技術主権とデジタルインフラに関する決議案を賛成471票、反対68票、棄権71票で採択しました。この決議案は、クラウドインフラや半導体、人工知能、サイバーセキュリティ分野において少数の外国事業者に過度に依存している状況を懸念し、公共調達におけるオープンソースソフトウェア優先の原則と、100億ユーロ規模の主権技術基金を提案しました。

フランスの決定は、この決議案が採択されてから5ヶ月後に出された、個別国家レベルでの実行事例でした。

フランス政府はこの事態を4日間見守った後に動きました。セバスティアン・ルコルニュ首相は2026年6月16日、国内治安総局が使用していたパランティアのツールを、フランス企業チャップスビジョンの「アルゴンOS」に変更すると発表しました。発表のタイミングは、パリで開催される欧州最大のテクノロジー展示会「ビバテック」の開幕前日でした。その前日である6月15日には、チャップスビジョンがフランスの革新企業指数「ネクスト40」に名を連ねました。

ネクスト40はフランス政府が2019年から運用してきた支援リストで、企業価値が10億ユーロを超えるユニコーン企業か、3年以内に1億ユーロ以上の投資を誘致した企業のみが選ばれます。2つのニュースが2日間のうちに重なったことで、この決定は政府が以前から準備してきた構想であるかのような印象を与えました。ルコルニュ首相は、情報技術分野における新たな戦略的依存を受け入れることはできないと述べ、同盟国の好意に頼る時代は終わったと明らかにしました。

ここで確認しておくべき事実があります。発表と契約終了は同じ出来事ではありません。発表翌日の6月17日、ル・モンド紙は、パランティア側が2025年12月に更新した契約は法的になお有効であると主張していると報じました。フランス政府が新しい供給者を公に宣言したことと、既存の契約が実際に終了することは、それぞれ異なる手続きを経なければなりません。フランス内務省もパランティアと結んだ延長契約の残余期間を認めつつ、契約を整理するには別途の行政手続きが必要であると明らかにしました。

実際の入れ替えにはさらに時間がかかります。フランス内務省は、新プログラムを情報現場に配備し、既存データを移行する作業に18ヶ月から24ヶ月かかると見込んでいます。他の報道では、契約構造全体を考慮すると、完全な転換は2027年から2029年にかけて行われるとの見方もあります。ローラン・ニュニエス内務大臣はこの空白を埋めるため、2027年まで2つのシステムを併用して運用する過渡期を設けると約束しました。移行に時間がかかる理由は、単に一つのプログラムを差し替えるだけの問題ではないからです。

国内治安総局は、これまで使用してきた操作方式を新しい画面に合わせて移植し、要員を再教育し、データが行き交う経路を新たに整備し、進行中の捜査が中断しないよう維持し、実

際の業務量に耐えられるかを検証するという5つの段階を順を追って踏まなければなりません。国内治安総局の要員らはすでにパランティアの画面構成や操作方式に慣れ親しんでおり、情報を保存する方式自体が米国システムの規格に合わせて設計されています。連携を急いで絶つと情報活動に空白が生じるリスクがあるため、フランス政府は段階的な移行を選択しました。

チャップスビジョンが開発中の新しいプラットフォームには、AIエージェントが検索や分析の一部を代行する機能も盛り込まれる予定ですが、この機能が実際の捜査現場でパランティアのツールと同等に安定して作動するかを確認する手続きもまた、移行期間を長期化させる要因となっています。

この決定を後押ししたのは「フランス2030」投資計画でした。政府は人工知能分野の自立のため、6億5,500万ユーロを追加で割り当てました。このうち一部は、公務員向けの対話型人工知能ツールの開発に充てられました。2026年6月16日、公務員担当相のダヴィド・アミエルは、これまで1万人規模で試行運用していたチャットボット「ラシスタント（L'Assistant）」を、100万人に上る公務員全体へと拡大すると発表しました。拡大の第1段階の費用は70万ユーロから75万ユーロの間と計上され、開発はフランスの人工知能企業ミストラルAIが担当しました。

ミストラルAIのアーサー・メンシュCEOは、欧州が米国のクラウドインフラを借り受けて使う構造から脱却し、自前でインフラを保有すべきだと主張してきました。この発言は、国内治安総局の決定に対する論理的な裏付けとなりました。

フランスの新たなプロバイダーとなったチャップスビジョンは、2019年にオリヴィエ・デレンバッハ代表が設立した会社です。デレンバッハ代表は以前、金融分析ソフトウェア会社のeFrontを2019年にブラックロックへ13億ドルで売却した経歴があります。チャップスビジョンは自社開発よりも買収を通じて規模を拡大する戦略を選びました。顧客関係管理ソフトウェア企業のコエリス、リテールデータ企業のオクティファス、電子商取引企業のスパコ、マーケティング自動化企業のNP6を相次いで買い取ったのち、サイバーセキュリティと諜報、音声認識技術を保有するベルタンITとヴェクシスまで買収しました。

ベルタンITとヴェクシスを買収したことで、売上高は3000万ユーロから4000万ユーロへ、従業員数は260人から380人へと増加しました。こうした買収を25件以上繰り返した末、同社はフランスの政府系投資銀行ビピフランスとティケオー・キャピタルの資金を受け取り、2022年には1億ユーロを追加で調達し、2025年通年の売上高は2億ユーロに達しました。

チャップスビジョンが開発したアルゴンOSは、形式の異なる情報を一堂に集めて分析するプログラムです。文書だけでなく映像、音声、公開されたインターネット情報を意味するオープンソース・インテリジェンスまで、一箇所で取り扱います。このプログラムは、外部通信網と遮断されたエアギャップ環境や、国家が直接管理する主権クラウド上で動作します。同社の株

式は全額ヨーロッパの株主が保有しています。この所有構造が重要である理由は、米国のクラウド法（CLOUD Act）のためです。この法律は、米国法人が運営するサービスであれば、サーバーがどの国にあろうと米国の捜査機関の要請に応じて情報を提出しなければならないと規定しています。

アルゴンOSは米国法人ではないため、この法律の適用範囲外に置かれます。

国内治安総局がチャップスビジョンを選定したプロセスについても確認しておく必要があります。同社はフランス内務省が2021年に開始した情報統合事業「OTDH」の入札を経ています。OTDHは形式の異なる膨大なデータを単一の国家システムで処理しようとする事業で、全体予算は約4,000万ユーロと策定されました。チャップスビジョンは3年以上の審査の末、2024年末に元データを整理する第1領域（ロット1）の事業権を獲得しました。第2領域（ロット2）を巡る競争はさらに熾烈でした。

この領域の最終段階には、タレスとエビデンの合弁会社アテア、ソフトウェア企業のブルーウェイ、そしてチャップスビジョンの3社が残り、チャップスビジョンは2026年6月にこの競争にも勝利して、情報を可視化しモデル化する第2領域の事業権まで獲得し、最終落札者となりました。この落札により、アルゴンOSは対内安全総局にとどまらず、多くの司法機関のデータ処理を担う基盤システムとして定着しました。

フランスのこの決定は、隣国にも影響を与えました。ドイツ連邦憲法保全局は2026年5月、フランスに先立ち、同じアルゴンOSを導入することを確定しました。この決定の背景と経緯については、次の節で取り上げます。

フランスの国家機関内からアメリカの技術を完全に排除する作業は、数か月で終わるような事案ではありません。捜査官らの手に馴染んだ操作方法やデータ標準、既存契約の残存期間のすべてが障害として残っています。それでも、フランス政府が公に方針を転換した事実そのものが覆ることはありません。パランティアとの契約がいつ完全に終了するのか、アルゴンOSへの実際の移行がどれほどスムーズに行われるのかは、今後確認すべき事実として残されています。

根拠および参考文献

1. Jon Henley, 'France to ditch Palantir's AI data tools in favour of domestic provider', The Guardian, 2026-06-16, https://www.theguardian.com/world/2026/jun/16/france-ai-data-tools-palantir-chapsvision

2. Palantir Technologies, 'Palantir Announces Renewal of Multi-Year Contract with the DGSI', Business Wire, 2025-12-15, https://www.businesswire.com/news/home/20251215083215/en

3. Anthropic, 'Statement on the US government directive to suspend access to Fable 5 and Mythos 5', Anthropic, 2026-06-12, https://www.anthropic.com/news/fable-mythos-access

4. Anthropic, 'Redeploying Claude Fable 5', Anthropic, 2026, https://www.anthropic.com/news/redeploying-fable-5

5. Le Monde, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, 2026-06-17, https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice_6754592_7.html

6. ChapsVision, 'ChapsVision chosen by France to deploy Argonos for OTDH project', ChapsVision, 2026-06-16, https://www.chapsvision.com/press-release/chapsvision-chosen-by-france-to-deploy-argonos-for-otdh-project/

7. 著者不詳, 'L'Etat français déploie Mistral AI auprès d'un million de fonctionnaires', ChannelNews, 2026-06-16, https://www.channelnews.fr/letat-francais-deploie-mistral-ai-aupres-dun-million-de-fonctionnaires-et-inclut-la-souverainete-numerique-dans-les-objectifs-2026-2029-de-lugap-157317

8. BlackRock, 'BlackRock to Acquire eFront -- Industry Leading Alternatives Investment Software Provider', Business Wire, 2019-03-22, https://www.businesswire.com/news/home/20190322005228/en/BlackRock-to-Acquire-eFront----Industry-Leading-Alternatives-Investment-Software-Provider

9. 著者不詳, 'DGSI : Palantir éjecté, ChapsVision prend le relais en 2029', info.fr, 2026, https://info.fr/palantir-ejecte-dgsi-france-rompt-dependance-americaine-chapsvision/

10. 著者不詳, 'French Security Service to Replace Palantir With Local Software', Bloomberg, 2026-06-16, https://www.bloomberg.com/news/articles/2026-06-16/french-security-service-to-replace-palantir-with-local-software

11. 著者不詳, 'ChapsVision to replace Palantir in major contract with French intelligence agency', Sifted, 2026, https://sifted.eu/articles/chapsvision-to-replace-palantir-in-major-contract-with-french-intelligence-agency

12. 著者不詳, 'Quatre choses à savoir sur Palantir, ce géant technologique américain controversé qui travaille avec la DGSI', franceinfo, 2026, https://www.franceinfo.fr/societe/armee-securite-defense/quatre-choses-a-savoir-sur-palantir-ce-geant-technologique-americain-controverse-qui-travaille-avec-la-dgsi_7682872.html

13. ChapsVision, 'ChapsVision acquiert Bertin IT et Vecsys', ChapsVision, 2021, https://www.chapsvision.fr/acquisition-bertin-it-et-vecsys-par-chapsvision/

14. La mission French Tech, 'French Tech Next40/120', La mission French Tech, 2026, https://lafrenchtech.gouv.fr/en/programme/french-tech-next40-120/

15. 著者不詳, 'Anthropic releases Claude Fable, a version of Mythos, days after warning AI is becoming too dangerous', TechCrunch, 2026-06-09, https://techcrunch.com/2026/06/09/anthropics-claude-fable-5-is-a-version-of-mythos-the-public-can-access-today/

16. European Parliament, 'Texts adopted - European technological sovereignty and digital infrastructure', European Parliament, 2026-01-22, https://www.europarl.europa.eu/doceo/document/TA-10-2026-0022_EN.html

17. GIFAS, 'Athea, ChapsVision et Blueway retenus par la DGSI pour la seconde phase du programme OTDH', GIFAS, 2026, https://gifas.fr/press-summary/athea-chapsvision-et-blueway-retenus-par-la-dgsi-pour-la-seconde-phase-du-programme-otdh

18. 著者不詳, 'La France tourne la page Palantir : ChapsVision remporte le marché de la DGSI pour sa plateforme de traitement et d'exploitation de données', Usine Digitale, 2026, https://www.usine-digitale.fr/souverainete/la-france-tourne-la-page-palantir-chapsvision-remporte-le-marche-de-la-dgsi-pour-sa-plateforme-de-traitement-et-dexploitation-de-donnees.I3EESPQQIBEX3AQXHIF6ABGI3M.html

1.2 ドイツ連邦憲法保全庁（BfV）の離脱と連邦国防クラウドからの排除

ドイツでは、国内情報機関と軍がそれぞれ異なる時期に、しかし同じ方向を向いてパランティアと距離を置きました。二つの決定は一つの出来事ではなく、別々の手続きを経た二つの事実です。

ドイツ連邦憲法保全庁（BfV）は、国内情報を扱う最上位機関です。過激派勢力の動きを監視し、外国の諜報活動を防ぐ役割を担っており、フランスの国内安全保障総局と似た立場にあります。シナン・セレン長官は2025年12月、ドイツ国内の会議で、安全保障機関が欧州の視点をより明確に確立し、長期的な依存から脱却しなければならないと述べました。この発言から5か月後の2026年5月、連邦憲法保全庁はパランティアのプログラムではなく、フランス企業ハブスビジョンのアルゴンOSを調達することを確定しました。ドイツの連邦機関がパランティアを公式に拒否した初の事例として記録されました。

連邦憲法保全庁が選んだアルゴンOSは、前節で説明したものと同じプログラムです。形式の異なる情報を統合して分析し、公開されたインターネット情報を追跡するオープンソース・インテリジェンス機能も備えています。ドイツ側で注目すべき点は、このプログラムを実際に導入する過程で結ばれた提携です。ハブスビジョンは、ドイツの警察データベース「PIAV」を長年管理してきたIT企業ローラ・セキュリティ・ソリューションズと手を組みました。すでにドイツの治安網に定着している企業と協力することで、新しいプログラムが既存の体系の上に無理なく導入されるようにしたのです。

この調達がすぐに現場に配備されるわけではありません。ドイツ連邦政府は、連邦情報局（BND）と連邦憲法保全庁の権限を新たに定める700ページを超える法改正案を準備しています。この改正案は、両機関に脅威となる状況へ直接介入する権限や、人工知能および生体情報を扱う新たな手段を付与し、連邦憲法保全庁、州の情報機関、そして軍の防諜組織である軍事防諜局（MAD）の間の情報共有を義務付ける内容を盛り込んでいます。ドイツ連邦憲法裁判所がこの法改正の期限を2026年末と定めているため、連邦議会は夏の休会が終わった後、直ちにこの法案を審議することになります。

アルゴンOSをはじめとする新たな分析ツールは、この法的枠組みが整って初めて本格的に稼働できます。法がまだ整備されていない状態では、既存の体系を維持しながら過渡期を過ごさなければなりません。調達を確定したという事実と、その調達が実際に稼働する時期は、このように異なる手続きに縛られています。

連邦憲法保全庁の決定とは別に、ドイツ連邦軍は軍事領域においてパランティアを排除する措置を独自に進めました。ドイツ連邦軍は2017年、サイバー・情報空間司令部という独立した

軍種を創設し、サイバー防衛と情報体系の運用を専門に担当させました。同司令部のトーマス・ダウム海軍中将は2026年4月28日、ドイツの経済紙『ハンデルスブラット』とのインタビューで、パランティアを軍事クラウド事業に利用する計画は現時点では全くないと明らかにしました。同氏は、外国の民間会社の従業員にドイツの国家データへのアクセス権を与えることなど考えられないと述べました。

この発言により、パランティアは連邦軍が推進する次世代国防クラウド事業「pCloudBw」の候補から外れました。pCloudBwは、部隊の各所に分散した作戦データと人工知能処理能力を一つの機密クラウド上に統合しようとする事業であり、パランティアが外れるまでは検討対象候補の一つでした。

この排除の背景には、北大西洋条約機構（NATO）に関する懸念があります。NATOは2025年3月にパランティアと短期契約を結び、「メイヴン・スマート・システム」を指揮体系に導入しました。メイヴンは衛星画像情報を処理し、攻撃目標の優先順位を推奨するプログラムです。しかし、このプログラムの日常的な運用と管理は軍人ではなく、パランティア所属の民間技術者が担っています。ドイツ国防当局は、戦術情報の管理権限を同盟国の民間企業に委ねる構造が国家の防衛自主権を損なうおそれがあると判断しました。これに加え、米国クラウド法（CLOUD Act）も障害となりました。

この法律は、米国の法人が扱う情報であれば、サーバーの位置に関わらず米国の捜査当局がアクセスする道をひらいています。ドイツ連邦軍の作戦計画がこの法律の射程内に入ってしまう状況を、国防省は受け入れがたいと判断しました。

排除の後、連邦軍は代替となる候補を欧州域内で探しました。ダウム中将の発言が報じられた2026年4月29日頃、連邦軍はすでにドイツ企業ヘルシングのクラウド・人工知能体系「アルトラ」、ドイツ企業SAPの主権クラウド体系「S3NS」、フランス企業アトスの「ブルセクアナXH3000」に至るまで幅広く検討していました。アルトラはすでに一部の連邦軍部隊に配備されており、S3NSは防衛企業タレスが財務や調達業務の移行に利用していた体系でした。このように幅広く検討した結果、pCloudBw事業の最終候補は3社に絞られました。

シュトゥットガルトに拠点を置くアルマト（Almato）は、ドイツ企業データグループの子会社であり、ドイツ連邦情報セキュリティ庁（BSI）が要求する機密等級「VS-NfD」のデータ処理認証を取得しています。ベルリンのスタートアップ企業オークリスト・テクノロジーズ（Orcrist Technologies）は、形式の異なる大規模情報を一つの状況認識画面に統合する技術を披露しました。パリのハプスビジョンもアルゴンOS（ArgonOS）を前面に押し出してこの競争に参加しました。これら3社は2026年の夏の間、実戦データを連動させる試験を行い、最終落札者は2026年末に発表される予定です。

パランティアを排除したことと、新たに誰を選定するかは、このようにまだ別個の問題として残されています。

パランティアのアレックス・カープCEOはこの決定に即座に反応しました。同氏はドイツメディア『ビルト』とのインタビューでこのニュースに驚いたと語り、ドイツでの議論を魔法にまつわる話に例えました。カープCEOは、パランティアの技術がウクライナの戦場ですでに検証されていると主張し、自身と共同創業者ピーター・ティールがドイツと結んできた縁に言及することもありました。これに対し、ドイツのデジタル相カルステン・ヴィルトベルガーは、外国企業の一方的な統制下に置かれない自立こそが国家安全保障において最優先で守るべき条件であると反論しました。

ドイツがパランティアに対して慎重になった背景には、司法の判断も一役買いました。ヘッセン州は2017年にパランティアの「ゴッサム（Gotham）」を購入し、「ヘッセンデータ（hessenDATA）」という名称で運用してきました。ドイツ連邦憲法裁判所は2023年2月16日、ヘッセン州とハンブルク州が予測警察のためにこの体系を根拠として利用していた法律条項に対し、違憲判決を下しました。裁判所は、市民の通信記録や個人情報を法的根拠なく広範囲に分析する手法が情報自己決定権を侵害すると判断しました。この判決は、その後ドイツの各州がパランティアベースの体系を再検討するきっかけとなりました。

しかし、すべての州が同じ方向に動いたわけではありません。バーデン=ヴュルテンベルク州内務省は2025年3月20日、緑の党との事前協議なしにパランティアのゴーサムプログラム導入契約を結びました。この契約には途中で終了可能な条項が含まれておらず、5年間にわたり総額2,500万ユーロ、年間では約925万ユーロを支払う条件でした。州の連立政府に参加した緑の党内部では、この契約を即座に中止すべきだという意見に92パーセントが賛成票を投じました。しかし、出口条項のない契約は政治的反対だけでは覆らず、州政府は契約をそのまま続けました。

この事例は、調達契約に解約条件をあらかじめ盛り込んでおかなければ、国家が自ら交渉力を失うという事実を示しています。

ここで押さえておくべき点があります。欧州連合（EU）の人工知能法（AI Act）は、軍事、国防、国家安全保障の目的で使用される人工知能システムを規定の適用範囲から除外しています。この法律の第2条と前文第24項は、その根拠を加盟国がそれぞれ負う国家安全保障上の責任と軍事活動の性質に求めています。つまり、連邦憲法養護庁と連邦軍がパランティアを排除した決定は、EUレベルの人工知能規制に従った結果ではなく、ドイツという個別国家が調達と政治の領域で自ら下した選択なのです。

連邦機関と州政府のこのような交錯する動きは、同じ国の内部であっても主権を守る速度や方式が異なるという事実を浮き彫りにしています。連邦憲法保全庁と連邦軍は契約を結ぶ前の段階でパランティアを排除しましたが、バーデン＝ヴュルテンベルク州はすでに署名した契約に縛られています。

根拠および参考文献

1. 著者不明, 'Digital Sovereignty: BfV Buys European Palantir Alternative', heise online, 2026, https://www.heise.de/en/news/Digital-Sovereignty-BfV-Buys-European-Palantir-Alternative-11293717.html

2. Markus Seyfferth, 'Wählt der BfV ArgonOS statt Palantir? Erstmals ja.', Dr. Web, 2026-05-01, https://www.drweb.de/waehlt-der-bfv-argonos-statt-palantir-erstmals-ja/

3. 著者不明, 'Software: Palantir für die Bundeswehr? "Sehe ich momentan überhaupt nicht"', Handelsblatt, 2026-04-28, https://www.handelsblatt.com/technik/it-internet/software-palantir-fuer-die-bundeswehr-sehe-ich-momentan-ueberhaupt-nicht/100217143.html

4. Jonas Brandstetter, 'Bundeswehr verzichtet auf Palantir', Behörden Spiegel, 2026-05-12, https://www.behoerden-spiegel.de/2026/05/12/bundeswehr-verzichtet-auf-palantir/

5. 著者不明, 'Palantir CEO Alex Karp Critiques German Military's Rejection of Advanced Defense Technologies', SSBCrack News, 2026, https://news.ssbcrack.com/palantir-ceo-alex-karp-critiques-german-militarys-rejection-of-advanced-defense-technologies/

6. Bundesverfassungsgericht, 'Urteil vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20', Bundesverfassungsgericht, 2023-02-16, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html

7. 著者不明, 'Baden-Württemberg zahlt Millionen für ein Produkt, das vielleicht nie genutzt wird', Schwäbische, 2026, https://www.schwaebische.de/regional/baden-wuerttemberg/millionen-fuer-eine-software-auf-abruf-4753518

8. 著者不明, 'Neue Regeln für BND und Verfassungsschutz: Regierung will Geheimdienst-Befugnisse massiv ausweiten', Tagesspiegel, 2026, https://www.tagesspiegel.de/politik/neue-regeln-fur-bnd-und-verfassungsschutz-regierung-will-geheimdienst-befugnisse-massiv-ausweiten-15786692.html

9. 著者不明, 'Geheimdienstreform: Zeitenwende für Spione', netzpolitik.org, 2026, https://netzpolitik.org/2026/geheimdienstreform-zeitenwende-fuer-spione/

10. 著者不明, 'Bundeswehr Will Not Use Palantir for Military Cloud and AI Project; European Alternatives Examined', Grosswald, 2026-04-29, https://www.grosswald.org/bundeswehr-rejects-palantir-military-cloud-ai-project-european-alternatives/

11. European Union, 'Regulation (EU) 2024/1689 (Artificial Intelligence Act), Article 2 and Recital 24', EUR-Lex, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

1.3 オランダ国防省の2年以内の全面代替戦略とスイスの徹底した拒否戦線

オランダとスイスは、フランスやドイツとは異なる形でパランティアと距離を置きました。オランダはすでに運用しているプログラムを計画的に取り除こうとしており、スイスは最初からパランティアを導入しない選択を何年にもわたって繰り返してきました。

オランダ国防省をめぐる議論は、調査報道メディア「フォロー・ザ・マネー（Follow the Money）」が、国防省特殊作戦司令部（SOCOM）もパランティアを使用しており、軍事作戦の進行中にパランティア側が機微な情報にアクセスできるという事実を報じたことで火がつきました。フォロー・ザ・マネーは以前の取材でも、オランダの軍と警察が数年にわたりパランティアと密かに取引を行ってきた事実を明らかにしていました。国防省側は、パランティア社員のアクセスは例外的な場合に限定されており、監督の下で単独作業を行うことはなく、実際の機密情報ではなく仮想のデータや古い資料のみを扱っていると釈明しました。

しかし、外国企業の社員がどのような形であれ秘密情報にアクセスするという事実そのものが、国家安全保障に対する直接的な危険であるという指摘は収まりませんでした。国防次官のデルク・ボスワイク氏は、この報道が出る1か月前の2026年5月、パランティアの使用を減らすよう、すでに省内に指示を出していた状態であったと明らかにしました。同氏はパランティアへの依存が懸念される点であることを認めつつ、ヨーロッパ産の代替案を探すよう指示したと述べました。この件が物議を醸したもう一つの理由は、パランティアが人工知能によって攻撃目標を選定する機能まで提供している点でした。

ボスベイク次官は2026年6月2日、下院（Tweede Kamer）で、パランティアを可能な限り速やかに欧州産の代替手段へと変更すると正式に表明しました。同氏は、完全に同等の水準を備えた代替手段を見つけるまでに2年を目標に掲げていると述べる一方で、軍事用人工知能の分野においては現在と同水準の欧州産代替手段が存在しないことも認めました。また、今すぐ関係を断てば、作戦戦闘システムや国防ロジスティクス、情報処理において限定的であっても安全保障上の空白が生じる可能性があるとし、即座の契約打ち切りには慎重な姿勢を示しました。

発表後の実際の進行状況を見ると、テンポは鈍いという評価が出ています。政府が下院に提出した追答には、具体的な終了期限の代わりに「代替案の検討」や「依存度の縮小」という表現にとどまりました。進展が遅れているのにはいくつかの理由があります。国防省内でパランティアと締結した契約が部署ごとに個別に行われており、政府レベルでの統一された契約一覧すら存在しません。進行中、予定、あるいはすでに終了した契約を一目で取りまとめて把握する方法がないということです。これに加え、軍部隊がNATO加盟国と情報をやり取りするた

めには同一のシステムを使用しなければならないという、相互運用性の要件も障害となっています。

国境警備を担う王立マレショセ（Marechaussee）も国境監視システムにパランティアのツールを使用しているため、国防省一所の決定だけでは解決しない問題でもあります。政治的には方向性を定めましたが、それを実行に移す具体的な推進力はまだ弱いというのが、この件を取材してきたメディアの共通した評価です。

スイスはこれとは趣の異なる事例です。フランスやドイツのようにすでに導入したプログラムを撤去するのではなく、複数の政府機関が何年にもわたりパランティアを採用しない決定を繰り返してきたケースに当たります。

スイス連邦保健庁は2020年4月から5月にかけて、新型コロナウイルスワクチンの物流管理に関する入札に参加したパランティアを除外しました。具体的な理由は公表されていませんが、担当部署がパランティアの参加自体を問題視したと伝えられています。同年、スイス連邦統計局はパランティア側からの面談要請に応じませんでした。スイス連邦情報技術庁は2020年から2021年にかけてパランティアと3回の協議を行った後、導入の必要はないとの結論を下しました。スイス国防調達庁アルマスイス（Armasuisse）は2020年、軍情報部の情報技術システム向け入札に参加したパランティアを落選させました。

落選の理由は必須要件を満たせなかったためとされ、その要件が何であったかは明らかにされていません。

2022年10月には、スイスマネーロンダリング通報局（MROS）がパランティアのソフトウェアのデモンストレーションを受けましたが、導入のための法的根拠がなく違法の恐れがあると判断し、導入を見送りました。この流れは2024年まで続きました。パランティアの欧州事業責任者であるルイス・モズレー氏は2024年6月、シンガポールで開催された安全保障会議「シャングリラ・ダイアログ」で、スイス軍参謀総長のトーマス・ジュスリ氏と直接面会し自社製品を売り込みました。

モズレー氏は、データに人工知能やアルゴリズムを適用することにスイス軍が関心を持っている点に着目し、軍部隊の稼働態勢を測定するアプリケーションを含めた実演デモを提案しました。スイス軍参謀部は提案を受けた後、内部検討報告書を作成し、2024年12月初旬にジュスリ参謀総長へ直接報告しました。報告書には、パランティアのツールを導入した場合、スイス軍の機密情報が米中央情報局（CIA）や国家安全保障局（NSA）に流出する恐れがあるとの懸念が盛り込まれており、スイス軍はこの報告を根拠に導入計画を最終的に撤回しました。

5つの機関、4年間にわたる拒絶が積み重なったことで、スイスではパランティアを受け入れない姿勢が一種の組織文化として定着しました。パランティアはこの期間中、スイスの官公庁の門を積極的に叩き続けましたが、結局ただ1件の契約も勝ち取ることができませんでした。

セキュリティ専門メディア「ゼンデータ（Zendata）」が2026年2月14日に報じたところによると、スイスがパランティアを退けた理由は性能不足のためではありませんでした。独占的で不透明な内部構造、外国の司法管轄権、リモートで行われるアップデート方式が、コントロール不能な主権上のリスクと評価されたのです。

データをスイス国内にとどめ、契約書に保護条項を盛り込む程度では、このリスクを十分に防ぎきれないというのがスイス側の判断でした。

パランティアは、こうした拒絶の動きを扱う報道に対しても強く反発しました。スイスの調査報道メディア「レプブリック（Republik）」は2024年12月、パランティアとスイスの関係に危険が伴う可能性を指摘する2本の記事を掲載しました。パランティアはこの報道に対し、23件の反論文を掲載するよう求めてレプブリックを相手に訴訟を起こしました。チューリッヒ商業裁判所は23件のうちわずか1件の掲載のみを認め、パランティアへ支払うよう定められた損害賠償額も9,000スイスフラン程度にとどまりました。この判決は、スイスにおけるパランティアの信頼性にさらなる傷を残す結果となりました。

似たような時期にスペインでも新しい措置が出されました。スペイン首相府は国営企業持株会社（SEPI）傘下の公企業に対し、パランティアと新しく契約しないよう通達を出し、このニュースは2026年7月1日にスペインのメディアを通じて知られることになりました。この措置は、通信企業テレフォニカ、防衛企業インドラ、造船企業ナバンティアのように、高度な通信網や軍事情報を扱う国営企業を対象としたものでした。ただし、すでに締結した契約まで無効にすることはありませんでした。スペイン軍情報センター（CIFAS）がパランティアと結んだ約1,650万ユーロ規模の契約は、2026年11月までそのまま継続されます。

新規契約を阻むことと既存の契約を打ち切ることは別問題であるという事実が、スペインの事例からも同様に確認できます。

オランダとスイス、スペインを並べて見ると、ヨーロッパがパランティアと距離を置く方法が一つではないという事実が明らかになります。オランダは、すでに国防体系のあちこちに浸透したプログラムを、政治的な意志だけでは簡単に取り除けずにいます。スイスは、最初から敷居を跨がせないよう阻んできた複数の機関の判断が積み重なり、現在では新たに説得する必要すら大きくない状態に至っています。スペインは、今後締結する契約の門戸を閉ざしながらも、すでに署名した契約の満期まではそのまま待つ道を選びました。

どちらにせよ、アメリカの技術に依存せず安全保障体制を運用するには、契約書の条項一つ、機関間の協議一つに至るまであらかじめ備えておかなければならないという点は同じです。

根拠および参考文献

1. Egle Kristopaityte, 'The Dutch defense ministry is looking for Palantir alternatives', Cybernews, 2026-06-03, https://cybernews.com/tech/dutch-defense-palantir/

2. 著者不明, 'Defensie zoekt alternatief voor Palantir-software', Computable, 2026-06-03, https://www.computable.nl/2026/06/03/defensie-zoekt-alternatief-voor-palantir-software/

3. 著者不明, 'Defensie wil software Palantir "binnen twee jaar" vervangen door Europees alternatief', Nederlands Dagblad, 2026, https://www.nd.nl/nieuws/politiek/1319116/defensie-wil-software-palantir-binnen-twee-jaar-vervangen-doo

4. 著者不明, 'Over twee jaar exit Palantir? Voorlopig blijft het bij intenties en verkenningen', iBestuur, 2026, https://ibestuur.nl/markt-en-overheid/inkoop-en-aanbesteding/exit-palantir-blijft-het-bij-intenties-en-verkenningen

5. Follow the Money, 'Omstreden techbedrijf Palantir kan bij geheime data van Defensie', Follow the Money, 2026, https://www.ftm.nl/artikelen/omstreden-techbedrijf-palantir-kan-bij-geheime-data-van-defensie

6. Follow the Money, 'Het Nederlandse leger doet al jaren in het geheim zaken met de omstreden techreus Palantir, net als de politie', Follow the Money, 2026, https://www.ftm.nl/artikelen/het-nederlandse-leger-doet-al-jaren-in-het-geheim-zaken-met-de-omstreden-techreus-palantir-net-als-de-politie

7. 著者不明, 'Switzerland Ends Palantir Contract Over Data Sovereignty Risks', ZENDATA Cybersecurity, 2026-02-14, https://zendata.security/2026/02/14/switzerland-ends-palantir-contract-over-data-sovereignty-risks/

8. Republik, 'How tenaciously Palantir courted Switzerland', Republik, 2026-02-18, https://www.republik.ch/2026/02/18/how-tenaciously-palantir-courted-switzerland

9. Republik, 'Überwachungstechnologie: Wie hartnäckig Palantir die Schweiz umwarb', Republik, 2025-12-08, https://www.republik.ch/2025/12/08/wie-hartnaeckig-palantir-die-schweiz-umwarb

10. 著者不明, 'Switzerland rejects Palantir over fears of US access to military data', 20 Minuten, 2026, https://www.20min.ch/story/kontroverser-it-konzern-palantir-umwarb-den-bund-jahrelang-und-blitzte-immer-wieder-ab-103466880

11. 著者不明, 'Palantir Took a Swiss Courtroom Loss and a European Credibility Hit', Yahoo Finance, 2026, https://finance.yahoo.com/markets/stocks/articles/palantir-took-swiss-courtroom-loss-111400896.html

12. The Cradle, 'Spain blacklists Palantir over domestic security concerns', The Cradle, 2026-07-01, https://thecradle.co/articles/spain-blacklists-palantir-over-domestic-security-concerns

2.1 アンソロピック「フェイブル5（Fable 5）」遮断事件と同盟の警告

米国国防総省と人工知能企業アンソロピックの間の摩擦は、2026年以前から静かに積み重なっていました。アンソロピックは政府機関に自社の人工知能モデルを提供する際、二つの線を自ら引いていました。一つは、自社のモデルが人を直接標的にして殺傷する兵器システムに搭載されてはならないということでした。もう一つは、自国民を対象とした無差別な秘密監視業務にモデルが使われてはならないということでした。この二つの条件は、同社が政府と契約を結ぶ前から明らかにしていた利用規約の延長線上にありました。国防総省の首脳部は、この条件を受け入れませんでした。

彼らは何の制約もない完全なアクセス権限を要求しました。人工知能モデルを兵器の標的選定システムにそのまま接続したり、自国民の通信や位置情報をフィルタリングする監視システムに制限なく組み込めるようにしたりすることが、国防総省側の要求の実質的な内容でした。アンソロピックは、こうした要求を受け入れれば自社の人工知能が人の生死を分かつ決定や自国民に対する全面的な監視に直接関与することになると考えました。同社は政府という顧客を失うリスクを冒してでも、この二つの線だけは守るという立場を固持しました。交渉の溝は埋まりませんでした。[1]

国防総省はアンソロピックが譲歩しないと、同社を自国のソフトウェアサプライチェーンの脅威要素として指名しました。国防総省の官僚らはアンソロピックを国家安全保障にとって致命的なサプライチェーン・リスク企業として正式に規定しました。この指定は、それまでアメリカに敵対的な国家の法人にのみ下されていた強力な行政措置でした。民間人工知能企業がこのような指定を受けた例は、それまで稀でした。

トランプ政権は2026年2月28日、連邦政府機関がアンソロピックの人工知能プログラムを使用できないよう命令しました。[1] この命令は表向きには調達規定を扱う行政措置のように見えましたが、実際には国防総省が望むアクセス条件をアンソロピックに受け入れさせるための圧迫手段でした。サプライチェーン・リスク企業という指定は、名前だけの重い表現にとどまりませんでした。この指定を受けた法人は国防総省の調達体系の中で信頼できないサプライヤーとして管理され、新規契約を結ぶことが困難になり、既存の契約も再検討の対象に上るのが一般的でした。

それまでこの措置は、アメリカに敵対的な国家とつながりのある法人を排除する用途に使われていました。シリコンバレーで世界的に名の知られた人工知能開発企業がこのリストに名を連ねたことは、それまでありませんでした。アンソロピックがこの指定を受けたという事実その

ものが、国防総省がこの対立を契約条件を巡る交渉ではなく安全保障上の脅威の問題として扱っていることを示していました。

この圧力に対してアンソロピックは譲らず、事態は法廷へと持ち込まれました。連邦裁判所の裁判官は2026年3月27日、国防総省の主張を認めませんでした。裁判官は、国防総省がアンソロピックに加えた圧力が憲法修正第1条の保障する表現の自由を侵害した政治的報復であると判断しました。[1] 民間企業が自ら定めた利用条件を守ろうとして公共権力と正面から衝突し、その衝突が裁判所の判断へとつながった事件でした。この判決は、アメリカ国内においては牽制機構が作動したという事実を示していました。

行政が民間企業に加えた圧力が不当だと判断されれば、司法がそれを阻むことができました。しかし、この司法による牽制はアメリカという国の中でのみ有効でした。この時点まではアメリカ国内で繰り広げられた行政と民間企業との間の争いであり、欧州の政府や機関はこの争いの結果を見守る術も、その結果に介入する術も持っていませんでした。

この内部対立は国内訴訟にとどまりませんでした。米国商務省は2026年6月12日、人工知能技術の輸出を制限する命令を出しました。商務省はこの措置の根拠として、最上位レベルの国家安全保障の維持を挙げました。[2][3] この命令が明示的に狙いとした対象は、外国籍を持つユーザーのアクセスでした。[2] しかしアンソロピックは、アクセス者の国籍をリアルタイムで判別するフィルターシステムを備えていませんでした。インターネットを通じてサービスを提供する企業が、アカウントを登録した国や決済に使われたカードの発行国を知ることはできても、アクセスしてくる一人ひとりの国籍を即座に確認することは容易ではありません。

そのためアンソロピックは、自社が保有する最も性能の優れたモデルであるクロード・フェイブル5とクロード・ミトス5の海外からのインターネットアクセスを丸ごと停止する方法を選びました。命令書が伝達されてからわずか数時間で、欧州を含むすべての国外のコンピュータからのアクセスが遮断されました。[1][5] 政府の指示は外国籍者を対象としていましたが、実際に遮断されたのは国籍とは無関係な海外からのすべてのアクセスでした。今回の措置は、アメリカが特定の企業や個人を永久に取引禁止リストに載せる制裁とは性質が異なっていました。

商務省が用いた手段は、特定技術の輸出を国家安全保障上の理由から一時的に制限する命令であり、こうした命令は法的に最初から期間が定められないまま発動されたとしても、政策的判断に応じていつでも撤回できる性質を帯びていました。しかし、欧州の利用機関の立場からすれば、その性質の違いを知っていたからといってアクセスが遮断された瞬間の衝撃が和らぐわけではありませんでした。

欧州の複数の行政機関や研究所は、事前の警告を受けないまま、日常的に使っていた人工知能ソフトウェアを失いました。[1][5] 接続が切れた理由を知らせる告知も、異議を申し立てる窓口も用意されていませんでした。 契約書に署名し利用料を支払ってきた機関であっても、

事情は変わりませんでした。 サービスを受け続ける権利は、利用契約ではなく供給本国政府の輸出規制判断の前では何の力も持ちませんでした。 クラウドサービスの利用規約やサービスレベル合意は、このような種類の国家行政措置を防いでくれる装置ではありませんでした。

欧州のセキュリティ専門メディアはこの事態を指して「フェイブル・バン（Fable-Ban）」と名付けて報じました。友邦国の行政命令一つが何らの事前協議もなく同盟国の業務ネットワークを停止させ得るという事実が、取材の焦点でした。[5]

アクセスを失ったのは政府省庁だけではありませんでした。欧州各国の行政機関をはじめ、大学や国策研究所も日常業務にフェイブル5とミトス5を使用しており、これらの機関もまったく同じ瞬間に同じ形でツールを失いました。[8] 公共部門と学術研究部門が共に経験したこの断絶は、今回の事態が特定の省庁や特定の契約関係に限られた問題ではなく、アメリカの技術に依存する欧州のあらゆるユーザー層にまたがる問題であるという認識を広げる契機となりました。[8] ドイツのセキュリティ専門メディア「セキュアクラウド・ブログ」は、「アメリカのソフトウェアが兵器として使われ得る」と題した記事で、パランティアを巡る議論とフェイブル5の遮断を共に取り上げ、欧州に必要なのは個別企業に対する不信感ではなくデジタル主権であるという結論を提示しました。[5] 契約をどの企業と結ぼうとも、その本社の所在地がアメリカにある限り、同様のリスクから完全に逃れることは難しいという指摘でした。[5]

この遮断は18日間続きました。米国政府は2026年7月1日になってようやく輸出制限措置を撤回しました。[3] アンスロピックは規制が解除された後、アクセスを復元する手続きに入ったと発表しました。[4] 同社の説明によると、6月12日の措置により遮断されたアクセスは、規制解除とともに直ちに完全に復旧したのではなく、段階的に復旧が進む形となりました。[4] 政策が覆されたからといって、サービスがその瞬間に再び再開されるわけではありませんでした。切断された接続を再確立するのにも時間がかかりました。遮断は命令書が伝達されてからわずか数時間で行われましたが、復旧はそれほど迅速ではありませんでした。

完全に以前と同じ状態に戻るまでには、さらに日数が必要でした。それでも事件の結末は明確でした。接続は遮断され、そして再び開かれました。

ここで確認すべき事実は2つあります。第一に、フェーブル5とミトス5の海外アクセスは実際に遮断されました。欧州の多くの政府機関や研究所が18日間、このツールなしで業務を行わなければなりませんでした。第二に、その遮断は永久に続いたわけではありませんでした。米国政府は政策を変更し、アクセスは再開されました。この事件を、米国の人工知能技術が欧州に二度と供給されない証拠と解釈するのは事実と異なります。アンスロピックは事件後も欧州で事業を継続し、欧州の機関も再び契約を結んだり既存の契約を継続したりしました。

逆に、この事件を何事もなかったかのように見過ごすことも事実とは異なります。18日間にわたって実際に発生した遮断は不可逆的な損失を残しはしなかったものの、その18日間にアク

セスを必要としていた機関は、代替案を探すか業務を先送りするしかありませんでした。フェーブル5事件が実際に示したのは、供給がいつでも停止する可能性があり、その停止と再開を決定する権限が利用国ではなく供給企業の母国政府にあるという構造でした。この事件を引き起こした対立は、最初から欧州を標的にして始まったものではありませんでした。

国防総省とアンスロピックの争いは米国内で繰り広げられた調達交渉の延長であり、欧州はその交渉とは全く無関係でした。それにもかかわらず、欧州の政府や研究所は交渉 Results（結果）を共に背負わされることになりました。自分たちと無関係な紛争の余波で業務ツールが遮断され得るという事実は、当事国であった場合よりもむしろ大きな不安を残しました。次に同じような形で接続が遮断されるきっかけが何であるか、欧州の政府や機関には予測する方法がありませんでした。

この構造は、それまで欧州の政策決定者たちにとって実感の湧かない概念でした。「デジタル主権」という言葉は、学術セミナーの発表文や政策報告書の序文にしか登場しない表現でした。[1] 友好国政府が自国の国内政治の争いを解決する過程で下した輸出規制命令一つが、わずか数時間で同盟国の政府機関の業務ツールを停止させ得るという事実は、理論ではなく実際に起きた出来事となりました。[1][5] 商務省の命令が狙った標的は外国籍者でしたが、その結果として共に遮断されたのは同盟国の政府や研究所のアクセスでした。

この標的と結果の間のズレこそが、欧州側がこの事件を特別な警告として受け止めた理由でした。米国が欧州を狙って措置を下したわけではないにもかかわらず、欧州がその措置の射程内に一緒に入っていたという事実自体が問題でした。米国の輸出規制は通常、敵対国への技術流出を防ぐ目的で用いられる手段であり、北大西洋条約機構（NATO）加盟国をはじめとする友好国はその対象から慣例的に除外・区別されてきました。しかし、フェーブル5事件ではこのような区別が実際には守られませんでした。

友好国と非友好国を分ける境界は政策の意図の中にのみ存在しただけで、国籍を振り分ける技術的な装置によって裏付けられてはいませんでした。欧州の政府がこの事件から読み取ったのはまさにこのギャップでした。意図上の区別と実際の執行の間に生じた隙間が、同盟国という地位だけでは埋められないという事実でした。

最も素早く動いた国はフランスでした。 フランスのセバスティアン・ルコルニュ内務大臣は、商務省の輸出規制命令が出されてから4日後の2026年6月16日、国内治安総局の情報分析システムを米パランティアのプログラムからフランス企業ハプスビジョンが開発したアルゴンOSへと変更すると発表しました。[6] この発表を、パランティアとの契約がその場で終了したという意味に受け取ってはなりません。 パランティアとフランス政府との契約はその時点でも数年残っており、契約を終了させるには違約金や別途の交渉が必要でした。

実際のシステム切り替えもまた、発表後に進められる別途のプロセスでした。[7] それにもかかわらず、フランス政府が商務省の命令からわずか4日後にこのような方向性の発表を行った

という事実は、フェーブル5の遮断が欧州の政府内でいかに迅速に政策議論へと移行したかを示しています。フランスはこの流れの中で最も早く発表を行った国であったというだけで、唯一の国ではありませんでした。

フェーブル5の遮断から数ヶ月の間に、欧州の他の government（政府）においても米国技術への依存度を再点検する手続きが相次いで開始されました。[8] 各国が具体的にどのような経路をたどったかは国によって異なりましたが、その出発点に今回の事件があったという事実は共通していました。

アンスロピックの事例が欧州に残した教訓は、特定の一社を信用できないということではありませんでした。アンスロピックは国防総省の要求に立ち向かい、自社が定めた利用条件を守り、裁判所も同社の主張を認めました。同社が殺傷兵器と無差別監視という2つの線を守ろうとしたことで受けた圧力は、むしろ同社が自らの定めた原則に忠実であったという事実を示していました。問題視されたのはアンスロピックの態度ではなく、米国政府がその気になれば、どの米国企業の海外サービスであっても同様の方法で停止させられるという構造そのものでした。

今回は国防総省とアンスロピックの間の対立でしたが、次回は別の企業と別の対立が同じ結果をもたらす可能性がありました。その対立が貿易摩擦に起因するものであれ、安全保障政策に起因するものであれ、あるいは今回のように政府と企業間の内部交渉に起因するものであれ、同様でした。欧州の政府や研究所はその対立の当事者ではないにもかかわらず、結果をそのまま背負わされる立場に置かれていました。

18日間という時間は、実際の業務が停止するには決して短くない期間でした。同時に、この期間がいつかは終わるという事実も今回の事件で確認されました。米国政府の判断が変われば、アクセスは再び開かれました。欧州の多くの政府がこの事件の後、自国の技術調達政策を再検討し始めた理由はまさにこの点にありました。契約書にどれほど詳細な条項を盛り込んでも、供給国の母国政府の決定の前ではその条項が力を持ち得ないという事実が、この事件によって明確になりました。接続が遮断されたという事実よりも、接続の開始と終了を決定する権限が自分たちの手の外にあるという事実こそが、より長く尾を引く問題だったのです。

フェイブル5事件は、封鎖が永遠に続いたという話ではなく、封鎖がいつでも再び起こり得ること、そしてその決定権が他国の政府にあるという話として、ヨーロッパの政策文書に残りました。接続が復旧した後も、この事件が引用され続けている理由がここにあります。危機が過ぎ去った後に残る問いは、何が遮断されたかではなく、次回も同じ決定を他国の政府が下し得るかということでした。この問いに対する答えをヨーロッパが自らコントロールできない限り、18日間の遮断は一度限りの事故ではなく、繰り返される可能性として残ります。

根拠および参考文献

1. Centre for Future Generations, 'Enforcement spotlight, Spring 2026', Centre for Future Generations, 2026年春号.

2. Anthropic, 'Statement on the US government directive to suspend access to Fable 5 and Mythos 5', Anthropic, 2026年6月12日, https://www.anthropic.com/news/fable-mythos-access

3. Gyana Swain, 'US reverses export restrictions on Anthropic's Fable 5, Mythos 5 AI models', Computerworld, 2026年7月1日, https://www.computerworld.com/profile/gyana-swain-2/

4. Anthropic, 'Redeploying Claude Fable 5', Anthropic, 2026年, https://www.anthropic.com/news/redeploying-fable-5

5. Sebastian Deck, 'US Software as a Weapon: Palantir's Manifesto Dramatically Highlights the Need for Digital Sovereignty', SecureCloud Blog, 2026年6月8日, https://blog.securecloud.de/en/us-software-als-waffe-palantirs-manifest-zeigt-drastisch-notwendigkeit-digitaler-souveraenitaet

6. Jon Henley, 'France to ditch Palantir's AI data tools in favour of domestic provider', The Guardian, 2026年6月16日, https://www.theguardian.com/world/2026/jun/16/france-ai-data-tools-palantir-chapsvision

7. Le Monde, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, 2026年6月17日, https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice_6754592_7.html

8. 「欧州連合（EU）主要国の脱パランティア動向とデジタル主権化に関する分析報告書」, 2026年, 1-2頁.

2.2 域外立法の罠：米国CLOUD法とFISA 702条 司法射程圏の実体

欧州連合（EU）の加盟国は長年にわたり、データサーバーを自国の領土内に置けば情報が安全に保たれると信じてきました。アマゾンやマイクロソフト、グーグルのような米国系企業も、フランクフルトやパリ、ダブリンにデータセンターを建設し、この信頼を広告のキャッチコピーとして掲げてきました。しかし、サーバーが欧州の土地にあるということと、そのサーバー内の情報が米国法の手に届かない場所にあるということは別の話です。米国議会が制定した二つの法律、CLOUD法と外国情報監視法（FISA）第702条は、国境ではなく企業の所属を基準として作動するからです。

この二つの法律がなぜ今、欧州の調達担当者たちを緊張させているのかを理解するには、まずCLOUD法が誕生した背景を見る必要があります。2013年12月、米国の連邦捜査機関は薬物取引の捜査に関連して、マイクロソフトにある利用者の電子メールアカウント情報を提出するよう求める令状を送付しました。問題は、そのアカウントのデータがアイルランドのダブリンにあるサーバーに保存されていた点です。マイクロソフトは、米国の令状が米国領土外のデータにまで及ぶことはないと主張して訴訟を提起し、2016年にニューヨークの連邦控訴裁判所はマイクロソフト側の主張を認めました。

米国司法省がこの判決を不服として連邦最高裁判所まで上訴する間に、米国議会は2018年3月23日にCLOUD法を可決成立させてしまいました。新法がこの争いの根拠自体を塗り替えてしまったため、最高裁判所は事案をこれ以上審理する必要はないと判断し、訴訟を終了させました。CLOUD法は、このように米国政府が裁判で敗訴しかけていた争いを、立法によって整理する形で誕生した法律です。

この法律の核心は極めてシンプルです。データがどの国に保存されているかは問いません。そのデータを管理する企業が米国の司法管轄内にあるか否かを問うのです。法律用語ではこれを「占有」「保管」「統制」という三つの基準で表現します。米国に本社を置く企業であったり、米国企業が株式や経営権を握っている海外子会社であったりすれば、その企業が占有・保管・統制する情報は、保存されている物理的な場所にかかわらず、米国裁判所の令状や命令書に従って提出しなければなりません。

この点で、CLOUD法が実際に可能にすることと、人々がしばしば誤解していることを区別して見る必要があります。CLOUD法が可能にすることは明確です。米国の司法管轄下にある通信サービスプロバイダーやリモートコンピューティングサービスプロバイダーは、自らが占有・保管・統制する情報であれば、それが世界中のどの国のサーバーにあろうとも、米国政府の適法な要求に応じて提出する法的義務を負います。その一方で、CLOUD法が自動的に意

味するわけではないこともいくつかあります。第一に、この法律は米国政府がすでにすべてのデータを手にしているという意味ではありません。

政府は依然として個別の事案ごとに、裁判所の令状や検察の召喚状といった正式な法的手続きを経なければなりません。第二に、すべての要求が自動的に貫徹されるという意味でもありません。CLOUD法は、米国政府と正式に相互執行協定を結んだ外国政府の国民に限って、企業が裁判所に異議を申し立てることができる狭いルートを開いています。2022年以降、このような協定を結んだ国は英国とオーストラリアの二カ国のみであり、欧州連合はまだこのような協定を米国と結んでいません。したがって、欧州市民の情報に関しては、この例外的な異議申し立て手続きすら適用されません。

協定を結んでいる英国の場合でも、このルートは広くありません。請求の対象が米国籍者でなく、米国に居住してもおらず、かつ情報を引き渡す行為が英国法と実際に衝突するという点を企業側が立証して初めて、裁判所は異議を受け入れます。欧州連合のように協定自体が存在しない場合には、このような制限的なルートすら存在しません。第三に、この法律が及ぶ範囲は企業の国籍と支配構造に依存するのであり、サーバーの物理的な位置に依存するわけではありません。米国と一切の資本関係も経営関係もない純粋な欧州企業であれば、CLOUD法の対象にはなりません。

この構造をひとつの具体的な流れに沿って辿ってみると理解しやすくなります。フランスのある行政省庁がアメリカ企業の欧州子会社と契約を結び、データを必ずフランス領土内に置くという条項を入れたと仮定します。この契約はフランス政府と欧州子会社との間の約束です。しかし、アメリカの検察がそのデータを求めた場合、検察はフランスにある子会社ではなく、アメリカにある親会社に令状を送ります。親会社は子会社の株式と経営権を握る主体であるため、法律上そのデータを占有、保管、統制する立場にあるとみなされます。

親会社が子会社にデータ提出を指示すれば、子会社はフランス政府と交わした契約とは無関係に、その指示に従わざるを得ません。フランス政府は契約の相手方にすぎず、この内部指示の過程に介入する権限を持たないのです。データがフランスの領土を一歩も出なくても、この手続きはそのまま進行します。データが欧州にとどまっているという条件だけで法的リスクが消え去るわけではない理由が、ここにあります。リスクを決定づけるのは、サーバーが置かれている場所ではなく、そのサーバーを管理する企業の国籍と支配構造です。

ここに、さらにもう一つのレイヤーが重なります。欧州連合の一般データ保護規則（GDPR）第48条は、外国の裁判所や行政当局が個人データの移転を要求したとしても、その要求が欧州連合や加盟国と結んだ国際協定に基づかない限り、欧州内でそのまま承認されたり執行されたりすることはできないと定めています。しかし、先ほど見たように、米国と欧州連合の間にはCLOUD法に基づく相互執行協定が存在しません。結局のところ、米国から令状を受けた企業は、二つの異なる法律の間に立たされることになります。

米国の令状に従えば、欧州連合の法律が求める国際協定上の根拠がないまま情報を引き渡すことになり、令状を拒否すれば米国の裁判所で法廷侮辱の責任を問われる可能性があります。この衝突は机上の議論ではなく、実際に米国系クラウド企業が欧州の顧客と契約を結ぶたびに直面する構造的なジレンマです。

イタリアの事例は、このジレンマがいかに根深いかを示しています。イタリア政府は公共行政のための自国戦略クラウドである「ポロ・ストラテジコ・ナツィオナーレ（Polo Strategico Nazionale）」を構築するにあたり、データをイタリア領土内にのみ置き、暗号鍵も自国の機関が直接管理するよう設計しました。しかし、この戦略クラウドを実際に稼働させる基盤技術は、マイクロソフト・アジュールやグーグル・クラウドといった米国系のハイパースケーラーでした。イタリア当局は鍵を手に握っていても、その鍵で施錠する錠前装置自体を米国企業が設計し供給しているという根本的な限界を完全に消し去ることはできませんでした。

データの位置と暗号鍵という二重の防壁を築いても、ソフトウェアの源泉技術の国籍という第三のレイヤーは依然として米国に残されていたのです。

この実体は抽象的な法条文ではなく、実際の証言によって確認されました。マイクロソフトの法務担当役員は2025年7月17日、フランス上院の公聴会に出席し、宣誓の上で証言しました。同氏は、パリに物理的に保存されているユーザーデータであっても、米国の連邦捜査機関がCLOUD法に基づいて情報提出を要求した場合、フランス政府の承認がなくても会社はその情報を引き渡さざるを得ないと認めました。

2025年7月22日に米経済誌フォーブスがこの証言を報じたことで、欧州全域の調達担当公務員は、自国領土内にサーバーを置く政策だけでは米国法の射程圏を逃れることはできないという事実を文書で確認することになりました。

CLOUD法とペアをなすもう一つの脅威は、外国情報監視法第702条です。この条項は2008年に制定された外国情報監視法改正案に含まれており、米国家安全保障局のような情報機関が、米国領土外にいる外国人の通信記録やインターネットデータを、対象者ごとに裁判所の令状審査を受けることなく収集することを認めています。CLOUD法が捜査機関の個別要求に応じた法執行ツールであるならば、第702条は情報機関が海外情報収集という名目で幅広く運用する監視権限です。この条項は期限が定められた時限法であるため、米議会が数年ごとに再び手を入れる必要があります。

2024年4月、米議会は情報改革および米国安全保障法を通じて第702条を再び延長し、2026年4月まで効力を維持させました。その後、議会は期限を6月12日までもう一度先送りしましたが、結局新たな延長法案がその時点までに可決されなかったため、法律の条文自体は2026年6月12日午前0時に効力を失いました。ただし、米外国情報監視裁判所が2026年3月にすでに承認していた1年間の監視認証は、法律の失効後もそのまま維持されるよう設計されているため、実際の監視権限は2027年3月まで継続して作動する状態です。

法律の条文の存廃と実際の監視の継続性がこのように食い違っているという事実自体が、この権限を一つの法律で統制することがいかに困難であるかを示しています。この監視網には一般の市民だけでなく、同盟国の将官や高官外交官の電子メール送信経路も含まれているという事実が、数々の報道を通じて指摘されてきました。第702条が実際にどのように作動するかは、2013年の元米情報機関職員エドワード・スノーデンの告発によって具体的に明らかになりました。

当時公開された文書によると、米国家安全保障局はこの条項を根拠に、グーグルやマイクロソフト、ヤフーといった米国企業のサーバーから外国人ユーザーのデータを直接提供させる「PRISM（プリズム）」という収集システムを運用していました。この告発は、欧州各国の間で第702条を書面上の条文ではなく、実際に稼働している監視インフラとして捉えるようになったきっかけでした。

この監視構造が欧州の法廷で初めて正面衝突した事件がシュレムス判決です。欧州連合司法裁判所は2020年7月16日、オーストリア市民のマクシミリアン・シュレムスが提起した訴訟において、米国の監視システムが欧州市民の個人情報自己決定権を深刻に侵害していると判断し、米国と欧州連合間の個人データ移転協定であるプライバシーシールドを無効と宣言しました。裁判所が問題視したのは、他でもない第702条のような米国の無令状監視権限でした。

欧州企業がどれほど契約書に個人情報保護の条項を詳細に盛り込んだとしても、その情報がアメリカ企業の通信網を経由する限り、アメリカ情報機関の監視権限そのものを契約によって阻むことはできないという点が判決の核心でした。欧州連合執行委員会も2026年6月3日に発議されたクラウド・人工知能開発法の影響評価書で、クラウド法と第702条の二つを欧州のデジタル領土が抱える構造的な安全保障上の欠陥として明確に指摘しました。

この問題は法律条文の解釈にとどまらず、実際の調達政策を変える力として作用しました。ドイツのバーデン＝ヴュルテンベルク州内務省は、マイクロソフトのソフトウェアを基盤とした公共クラウド事業であるデロス・クラウドの実際の稼働条件を精密に分析しました。分析結果は明確でした。データセンター自体はドイツ連邦情報セキュリティ庁の認証を受け、ドイツ領土内で運用されているものの、その上で稼働するアプリケーションソフトウェアの設計と統制権限は、相変わらず米マイクロソフトが握っていたのです。

州内務省は、アプリケーション層の統制権が米国企業に残っている限り、米国の安全保障当局がソフトウェアプロバイダーに対し、ユーザーに知らせずデータ流出経路を仕込むよう指示する可能性そのものを排除できないと結論付けました。データが物理的にドイツにあるという事実だけでは、このリスクを解消することはできませんでした。

同様の懸念はオランダ政府の公式決定につながりました。米国系総合情報技術企業のキンドリルは、2025年11月にオランダのソルビニティを買収すると発表しました。ソルビニティは、オランダ国民約1,650万人が利用する電子身分証システムであるディジドの基盤インフラを運

営する企業でした。オランダ下院では、この買収が米国司法管轄権を通じて自国民の機密性の高い身分情報へのアクセス経路を開く可能性があるとの懸念が続き、政府は買収を阻止する手続きに入りました。

オランダ経済省のアーツ国務次官は2026年5月26日、公共の利益を守る必要があるとして、キンドリルによるソルビニティの買収を正式に阻止すると発表しました。政府が明らかにした根拠は明確でした。米国法は、米国企業が所有する海外子会社のサーバーに保存された情報であっても、米国当局が確保できるように理論上認めているという点でした。2020年に設立されたオランダ投資審査局が、米国企業の買収を阻んだのは今回が初めてのことでした。米国のシンクタンクである戦略国際問題研究所は、この決定を欧州各国の投資審査基準が今後どのように変化するかを測る試金石であると評価しました。

英国では、物理的な位置とは無関係に、契約そのものが国家機密を米国企業へと渡す形で問題が浮き彫りになりました。米国のデータ分析企業パランティアは、英国の核兵器研究機関である原子力兵器施設と1500万ポンド規模のクラウド支援契約を締結しました。2026年1月、この契約を報じた調査報道メディア「ザ・ナーブ」によると、この契約は政府の公式調達公開サイトに登録されておらず、国防省は契約の存在自体を認めることも否定することもしませんでした。

同報道は、パランティアが英国政府と締結した契約の総額が6億7000万ポンドに上ると集計しましたが、原子力兵器施設との契約はそのうち公開リストから除外された状態で把握された規模でした。英国下院科学技術委員会は、国の捜査網や保健データを米国企業に依存している現在の構造が、調達体系の深刻な脆弱点であると指摘しました。核兵器関連情報を扱う契約が公開調達リストから除外されていたという事実は、物理的な国境内で契約を結んだからといって、情報統制権まで自国に残るわけではないという点を改めて確認させました。

ドイツではパランティアに関連するもう一つの法的衝突がありましたが、この事件はCLOUD法や第702条ではなく、ドイツ憲法上の問題であったという点を区別する必要があります。ドイツ連邦憲法裁判所は2023年2月16日、犯罪の容疑がない市民を予測分析する警察プログラムの運用が違憲であると判決を下しました。違憲判定を受けたヘッセンデータ・システムは、パランティアのゴッサム・プラットフォームを基盤に構築された治安プログラムでした。この判決が問題視したのは、米国法の域外適用ではなく、ドイツ基本法が保障する市民の自己決定権でした。

二つの問題は発生原因こそ異なるものの、結果的に同じ結論を指し示していました。アメリカ企業のソフトウェアに国家治安情報を委ねる構造は、アメリカの法律のためであれ自国の憲法のためであれ、複数の方向から同時に揺らぎ得るという事実です。

アメリカの域外司法権が情報提出要求の範囲を超え、制裁の手段としても使われ得るという事実が確認されました。米国財務省外国資産管理室（OFAC）は2025年8月20日、イスラエル

のネタニヤフ首相に対する逮捕状発給に関与した国際刑事裁判所の裁判官らに制裁を科しました。フランス国籍のニコラ・ギユー裁判官も制裁対象に含まれました。その後、彼は銀行カード決済やAmazonサービスへのアクセスが遮断されたとメディアに明らかにしました。同じ制裁対象に挙げられた他の国際刑事裁判所関係者の電子メールアカウントがマイクロソフトによって停止されたという報道が出され、マイクロソフト側はこれを否定しました。

この事件はクラウド法や第702条とは異なる制裁法規に基づくものですが、根を同じくする危険性を示しています。アメリカ企業が提供する決済や通信、クラウドサービスに依存する個人や機関は、アメリカ行政の決定一つで日常的なサービスへのアクセス権を一挙に失う可能性があります。

フランスはこの問題を、認証基準の条文そのものに明確に規定しました。フランス国家情報システムセキュリティ庁は、信頼できるクラウド事業者へ付与するセキュナムクラウド認証基準を改定する際、データを欧州域内に置くという条件だけでは不十分であると明示しました。2025年に改定されたセキュナムクラウド3.2バージョンは、認証を受けようとする事業者に対し、本社所在地とデータセンターが欧州連合域内に存在しなければならないという要件に加え、企業の資本および議決権構造がクラウド法のような域外効力を有する第三国の法律から完全に独立していなければならないという要件を新たに盛り込みました。

国際司法共助の手続きを経ずに第三国がデータの開示を命じたとしても、その命令が通用しない構造を備えて初めて認証を受けられるという意味です。フランス当局が認証基準の条文においてクラウド法を事実上指名して盛り込んだという me º事実, 欧州の政策担当者がこの問題を契約書上の信頼条項ではなく、会社の所有構造によって解決すべき問題と規定したことを示しています。

これらの多様な事例を並べて見ると、一つの結論が浮かび上がります。データを欧州の領域内に置く政策は必要な措置ですが、それだけでは十分ではありません。リスクを実際に軽減するためには、情報を扱う企業自体がアメリカの所有や支配、ソフトウェアの設計権限から脱していなければなりません。サーバーの位置は地図上の座標に過ぎず、その座標内の情報を実際に開閉する権限は、企業の本社がどの国の法律の下にあるかによって決定されるためです。欧州の多くの政府が物理的なデータ主権から企業の統治構造やソフトウェアの源泉技術にまで審査範囲を広げている理由は、まさにここにあります。

欧州委員会はクラウド・人工知能開発法の影響評価書において、この区分を政策の言葉へと置き換えました。評価書は、データの物理的な保存場所、暗号鍵の管理主体、ソフトウェアを設計・支援する企業の所有構造を、それぞれ異なる3つの層に分けて検討しました。フランスのセキュナムクラウド認証が企業の資本構造にまで踏み込んだことも、イタリアの戦略クラウドが暗号鍵まで掌握しながら完全な独立を宣言できなかったことも、これら3つの層が個

別にではなく共に整えられて初めて実質的な保護が成立するという事実を、それぞれのやり方で証明した事例です。

根拠および参考文献

1. U.S. Congress, 'Clarifying Lawful Overseas Use of Data Act', H.R. 4943 (Public Law 115-141), 2018年3月23日. https://www.congress.gov/bill/115th-congress/house-bill/4943/text

2. U.S. Congress, Foreign Intelligence Surveillance Act Amendments Act of 2008, Section 702 (Public Law 110-261), 2008年.

3. U.S. Congress, Reforming Intelligence and Securing America Act (RISAA), 2024年4月20日. https://www.congress.gov/crs-product/R48592

4. Electronic Frontier Foundation, 'Victory! 702 has Expired!', EFF Deeplinks, 2026年6月. https://www.eff.org/deeplinks/2026/06/victory-702-has-expired

5. Court of Justice of the European Union, 'Maximillian Schrems v. Facebook Ireland Limited', Case C-311/18, 2020年7月16日判決.

6. Regulation (EU) 2016/679 (General Data Protection Regulation), Article 48.

7. Polo Strategico Nazionale, 'Secure Public Cloud: the encrypted cloud', polostrategiconazionale.it. https://www.polostrategiconazionale.it/en/solutions/cloud-services-with-csp/secure-public-cloud/

8. United States v. Microsoft Corp., 584 U.S. ___ (2018), 米国連邦最高裁判所. https://supreme.justia.com/cases/federal/us/584/17-2/

9. Emma Woollacott, 'Microsoft can't keep EU data safe from US authorities, representative admits', Forbes, 2025年7月22日. https://www.forbes.com/sites/emmawoollacott/2025/07/22/microsoft-cant-keep-eu-data-safe-from-us-authorities/

10. European Commission, Impact Assessment accompanying the proposal for the Cloud and AI Development Act, SWD(2026) 502 final, 2026年6月3日. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52026SC0502

11. Center for Strategic and International Studies, 'Untapping the Full Potential of CLOUD Act Agreements', CSIS Analysis. https://www.csis.org/analysis/untapping-full-potential-cloud-act-agreements

12. netzpolitik.org, 'Delos-Cloud: Mit Microsoft in die digitale Abhängigkeit', netzpolitik.org, 2024年. https://netzpolitik.org/2024/delos-cloud-mit-microsoft-in-die-digitale-abhaengigkeit/

13. NL Times, 'Netherlands blocks U.S. takeover of DigiD operator Solvinity over security concerns', NL Times, 2026年5月26日. https://nltimes.nl/2026/05/26/netherlands-blocks-us-takeover-digid-operator-solvinity-security-concerns

14. Cleary Antitrust Watch, 'Dutch Government Blocks Kyndryl's Acquisition of Solvinity in First-Ever Telecom FDI Prohibition', Cleary Antitrust Watch, 2026年6月. https://www.clearyantitrustwatch.com/2026/06/dutch-government-blocks-kyndryls-acquisition-of-solvinity-in-first-ever-telecom-fdi-prohibition/

15. The Nerve, 'Revealed: Palantir deals with UK government amount to at least £670m – including £15m contract with nuclear weapons agency', The Nerve, 2026年1月. https://www.thenerve.news/p/palantir-technologies-uk-government-contracts-size-nuclear-deterrent-atomic-peter-thiel-louis-mosley

16. Bundesverfassungsgericht, ヘッセンデータ予測治安プログラムに関する判決, 2023年2月16日.

17. Irish Times, "It's surreal': US sanctions lock International Criminal Court judge out of daily life', Irish Times, 2025年12月12日. https://www.irishtimes.com/world/us/2025/12/12/its-surreal-us-sanctions-lock-international-criminal-court-judge-out-of-daily-life/

18. Computer Weekly, 'Microsoft's ICC email block reignites European data sovereignty concerns', Computer Weekly, 2026年. https://www.computerweekly.com/opinion/Microsofts-ICC-email-block-reignites-European-data-sovereignty-concerns

19. cio-online.com, 'SecNumCloud, une protection contre le droit extraterritorial, pas une garantie absolue', CIO Online, 2025年. https://www.cio-online.com/actualites/lire-secnumcloud-une-protection-contre-le-droit-extraterritorial-pas-une-garantie-absolue-16759.html

20. LSTI, 'SecNumCloud Qualification (ANSSI): Audit & Evaluation', LSTI Certification. https://www.lsti-certification.fr/en/Company-offers/Cybersecurity/SecNumCloud

21. Barton Gellman and Laura Poitras, 'U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program', The Washington Post, 2013年6月6日.

22. Center for Strategic and International Studies, 'The Kyndryl-Solvinity Case: A Barometer for Investment Security Reviews?', CSIS Analysis, 2026年. https://www.csis.org/analysis/kyndryl-solvinity-case-barometer-investment-security-reviews

2.3 「エアギャップ（Air-Gap）」と独自アーキテクチャ：契約条項を超えた技術的隔離

マイクロソフトの法務責任者は2025年7月、フランス上院の公聴会で宣誓の上、証言しました。パリに保存されたユーザーデータであっても、アメリカの連邦捜査機関がクラウド法に基づき情報提出を要求すれば、自社はフランス政府の承認なしに資料を提出せざるを得ないと明らかにしました。この証言は、ヨーロッパの行政担当者たちに一つの事実を明確に示しました。データを自国領土内に置く措置や、契約書にセキュリティ条項を盛り込む措置だけでは、アメリカの司法管轄権の手が届く範囲を脱することはできないという事実です。

契約書とは本来、取引当事者が遵守することで合意した約束を文書として残したものです。ヨーロッパの多くの政府も、アメリカのクラウド企業と契約を結ぶ際、データを域外へ移転しないという条項や、ヨーロッパの裁判所の命令なしには情報を引き渡さないという条項を契約書に盛り込んできました。しかし、こうした条項は、契約相手である企業が自由にその約束を守れる状況においてのみ力を発揮します。その企業がアメリカ法の適用を受ける限り、アメリカ政府が自国法を根拠に情報提出を命令すれば、企業は契約書の約束と自国の法律との間で選択を迫られ、ほとんどの場合、自国の法律に従わざるを得ないのです。

相手企業が自国政府の命令と契約上の約束のどちらかを選ぶよう迫られる瞬間、契約書の文言はもはや保護膜とはなりません。

この事実は、欧州の多くの国が長年にわたり頼りにしてきた安全装置の一つを崩壊させました。欧州連合の個人情報保護規則は早くからデータを域内に保存するよう求めてきましたし、多くの公共機関はサーバーが自国の国境内にあれば情報は安全だと考えてきました。こうした要求はデータローカライゼーションと呼ばれます。しかし、データローカライゼーションは情報が物理的にどの国にあるかを規定するに過ぎず、その情報を処理するソフトウェアを誰が設計し、誰が遠隔接続の権限を握っているかまでは規定しません。サーバーの位置とシステムの統制権は、互いに異なる問題なのです。

ドイツのバーデン＝ヴュルテンベルク州内務省による分析は、この違いを具体的に浮き彫りにしました。州政府が検討したデロス・クラウド事業は、データをドイツ領土内のサーバーに物理的に保管する方式で設計されていました。しかし、このクラウドを実際に動かすアプリケーションの設計および更新権限は、依然としてアメリカのマイクロソフト本社が握っていました。州内務省はこの事実を根拠に、データがドイツの土地に置かれていても、システムの統制権がアメリカ企業の手に残っている限り、クラウド法の捜査射程圏から一歩も逃れられないと結論付けました。

データがどこに保存されているかが問題なのではなく、そのデータを扱うソフトウェアを誰が設計し、誰が更新命令を出すかが問題だったのです。

フランスが国内安全総局（DGSI）の情報システムとして採用したアルゴンOS（Argon OS）は、これら二つの事例が浮き彫りにした問題に対し、異なる形で応えています。アルゴンOSを開発したハプスビジョン（Hapsvision）は、資本株式のすべてをヨーロッパの株主が所有する企業です。このシステムは、外部の有線ネットワークから完全に切断されたエアギャップ環境や、外部接続が遮断されたソブリン・クラウド（主権クラウド）サーバー上でのみ稼働します。システムを所有する会社にアメリカ法人がなく、システムが置かれたネットワークに外部へ伸びる経路が存在しなければ、アメリカの司法機関が差押状を発付したとしても、その差押状を執行する経路自体が存在しないことになります。

契約書に記された約束ではなく、ネットワーク構成と所有構造が隔離を生み出す仕組みです。

この隔離には、データ自体を守る措置を超えた部分がもう一つあります。アルゴンOSは、数万件に及ぶ異種混在の構造化・非構造化データを処理しながら、そのデータをロックする暗号鍵のライフサイクルを自前で管理するよう設計されています。データが暗号化されていても、その鍵を外部企業が管理しているならば、鍵を握る側はいつでも解錠できます。暗号鍵の管理を外部からのアクセスから完全に分離しておくということは、データの内容だけでなく、そのデータを読み取る権限自体を自国内にとどめておくことを意味します。

サーバーの位置と暗号解除権限をともに確保して初めて、隔離が実際に機能するのです。

「エアギャップ」という言葉は、文字通りコンピュータネットワークと外部インターネットとの間に物理的な空白を置く方式を指します。ケーブルが接続されていないため、遠隔から接続遮断の命令を出したり、システムを強制停止させたりする方法はありません。2026年6月に起きたフェーブル5（Fable 5）接続遮断事件は、まさにこの点を突いた事例でした。アンスロピック（Anthropic）のモデルはインターネット経由で提供されており、アメリカ商務省の命令一枚で、海外からの接続がわずか数時間で全面停止されました。外部ネットワークに依存するサービスであれば、契約がいかに強固であっても、供給元の本社が位置する国の行政命令の前には無力なのです。

逆に、外部と接続された経路自体が存在しないシステムであれば、そうした命令を伝達する物理的な経路はありません。

ただし、エアギャップ・アーキテクチャを備えたからといって、すぐに安全が完成するわけではありません。フランス内務省は、国内安全総局（DGSI）がアルゴンOSへと実戦情報活動全体を移行するのに18ヶ月から24ヶ月かかる見込みだと明らかにしました。数十年間にわたりパランティア（Palantir）の画面操作方式に慣れ親しんだ要員たちは、新しいシステムに再適応しなければならず、既存に蓄積されたデータの保存標準自体がアメリカのシステムに合わせ

て設計されているため、移行の過程で情報が欠落したり形式が食い違ったりするリスクが残ります。フランス国家行政機関はこの空白を埋めるため、2027年まで旧システムと新システムを並行運用する過渡期を設けると約束しました。

隔離されたアーキテクチャへと移行する決定と、そのアーキテクチャが実際に完全稼働する時点との間には数年の隔たりがあり、その数年間、二つの異なる体系を同時に維持する負担はそのまま情報機関が負うことになります。

この隔たりの間に支払うコストは、移行期間だけに留まりません。外部ネットワークと切断されたシステムは、大手クラウド企業が提供するリアルタイムアップデートや脅威情報共有サービスからも同時に切り離されます。アルゴンOSのような独自システムを運用する機関は、セキュリティパッチの適用や機能改善を自前の人員で負担しなければならず、これはアメリカの大手クラウド企業の全世界に及ぶデータセンターネットワークが自動的に提供していた「規模の経済」を放棄する選択でもあるのです。

外部と接続された経路自体が存在しない環境では、ソフトウェアの更新すらインターネットを通じた自動配信で処理することができず、検証を終えた記憶媒体に収めて物理的に持ち込む手順を踏まなければならない場合が多くなります。このような手順はインターネットによる更新よりも遅く、更新内容を毎回確認する独自の検証要員を必要とします。ヨーロッパの政策決定者たちが隔離を選択しながらも、それを万能の解決策として掲げない理由がここにあります。隔離は外国政府の一方的な命令によってシステムが停止させられる脅威を防いでくれますが、その代償として常時発生する保守・運用の負担を自国が背負わなければならないのです。

エアギャップが解決できる問題と解決できない問題を分ける基準は、そのシステムがどれほどの計算リソースを必要とするかにもあります。アルゴンOSのように単一機関の情報分析を担うシステムは、比較的限られた規模のサーバーでも完全に隔離された環境で稼働させることができます。しかし、フェーブル5のように膨大な計算を常時要求する大規模な人工知能モデルは事情が異なります。このようなモデルを自国領土内で外部と遮断したまま学習させ運用するには、個別の機関一つでは手に負えない規模のデータセンターと電力、半導体が必要となります。

フェーブル5の遮断事件が欧州に残した課題が、個別システムのエアギャップを超えて大陸規模の計算インフラを構築する問題へと発展した理由がここにあります。

スイスとオランダの対応は、隔離に至る経路が一つではないことを示しています。スイスの連邦機関は2018年から2025年までにパランティアの入札提案を少なくとも9回拒否し、最初から同社のシステムを導入しませんでした。すでに導入したシステムを撤去して新しいアーキテクチャに移行するフランスやドイツとは異なり、スイスは移植という高コストな過程そのものを経験しませんでした。オランダ国防省は2026年6月に、2年以内にパランティアを代替すると

いうロードマップを議会に提出しましたが、ロードマップはまだ計画に過ぎず、実際に旧システムが停止し新システムが全面的に稼働する時期はそれ以降のことです。

最初から依存関係を作らない選択と、すでに生じた依存関係を解消する選択は、同じ目的地を目指すとしても支払うコストが異なります。

隔離を完成させた状態も、永久に固定されるわけではありません。オランダの行政ネットワークの中核ソフトウェアを供給していた地元企業ソルビニティを米系企業キンドリルが買収すると発表すると、オランダ下院は自国民1,650万人の情報を扱っていたインフラの所有権が、一夜にして米国企業へ渡る可能性があるという現実に強い懸念を示しました。今日欧州企業が所有しているシステムであっても、その企業が明日外国資本に買収されれば、所有構造を条件としていた隔離はそのまま崩壊します。

隔離を証明する手続きが導入時点の一回限りの審査にとどまってはならず、所有権や支配構造の変動を継続的に確認する手続きへとつながらなければならない理由がここにあります。

隔離アーキテクチャがもたらす摩擦は、国境を超える軍事協力においても表れています。北大西洋条約機構（NATO）の保安認証委員会が2026年6月22日、パランティアの「メイヴン・スマート・システム」を完全な武器作戦用として認可した状況において、NATO最高司令官たちは、個別の加盟国が治安および行政領域で実施する脱パランティア措置を、軍事的戦場効率を低下させる決定だと批判しました。国内の治安情報ネットワークを外部から遮断されたアルゴンOSへ移行する選択と、同盟軍が共有する目標情報ネットワークが依然としてパランティアのソフトウェア上で稼働している現実は、同じ国の中で対立しています。

一国の情報機関が自国の領域内で隔離を完成させたとしても、その国が所属する同盟全体の情報ネットワークまで隔離することはできません。隔離の境界をどこまで設定するかは技術的な問題であると同時に、同盟関係をどのように維持するかを決める政治的な選択でもあります。

政治的宣言とアーキテクチャの完成との間にも隙間が残ります。ルコルニュ大臣がアルゴンOSへの転換を発表した後も、パランティア社は自社が国内セキュリティ総局（DGSI）と結んだ既存の契約が依然として法的に有効であると明らかにしました。政府の発表、調達プロセスの転換、契約の実際の終了、システムの完全な入れ替えは、同じ日に一度に起きる出来事ではありません。政治的宣言が出された時点と旧システムが実際に停止する時点の間には交渉と履行という別のプロセスが残されており、その期間中、旧契約は文書上で依然として存続し得るのです。

契約を打ち切るという発表自体が隔離を完成させるわけではなく、完成の証拠は発表文書ではなく、実際に稼働を停止した旧システムと実際に稼働を開始した新システムに存在します。

フランスとドイツのこうした決定は、欧州連合（EU）レベルの法律が整備されるのを待たずに各国政府が先手を打って下した決定であった点でも注目に値します。国内保安総局のアルゴンOSへの移行と、連邦憲法擁護庁による同様の選択は、いずれも個別国家の調達手続きを通じて行われました。これは、契約と調達という慣れ親しんだ手続きの中でも、供給企業の所有構造やネットワーク構成を条件として要求すれば、実質的な隔離を生み出せることを示しています。法整備が追いつく前に個別国家が先にアーキテクチャ自体を変化させ、欧州連合の次の課題はこうした個別の事例を共通の調達基準へと落とし込むことでした。

欧州委員会はこの隔離の原則を個別企業の選択に委ねず、調達規定へと移行させようとしています。委員会が2026年6月に提示した「クラウド・AI開発法」案は、まだ欧州議会と理事会の審議を経なければならない法案の草案であり、成立した法律ではありません。それにもかかわらず、この提案は供給企業の所有構造や取締役会の国籍、ソースコードへの外部アクセス権の有無まで審査する等級体系を設け、契約書の約束ではなくシステム自体の設計によって隔離を証明するよう求める方向性を打ち出しています。

最も高い等級では、システムの設計およびソースコードの保守・運用プロセスの全般において、外国資本の干渉を一切許容しないレベルの隔離を求める案が議論されています。

このような審査体系が意味を持つためには、隔離を証明する手続き自体が供給企業の自己申告にとどまってはなりません。フランスがすでに運用している独自の認証規範であるSecNumCloud（セクナムクラウド）は、政府が指定した審査機関がソフトウェアの設計図やソースコードを定期的に監査する手法をとっています。エアギャップや「主権クラウド」というラベルを貼ったということだけで隔離が完成したと見なすことはできません。ネットワーク構成図や所有株式の登記簿、ソースコードリポジトリを外部監査人が直接確認できて初めて、そのラベルは実体を持つのです。

クラウド・AI開発法案には、欧州連合サイバーセキュリティ庁（ENISA）が運用する認証体系において最高等級の資格を要求する案も盛り込まれており、国家レベルの認証と連合レベルの認証がともに隔離を確認する二重構造として設計されています。

契約とアーキテクチャは互いに代替する関係ではなく、共に機能すべき関係です。契約は調達価格やサービスの品質、責任の所在を定める文書として今も必要です。ただし、国家安全保障のように外国政府の介入の可能性そのものを遮断しなければならない領域では、契約が約束する保護をシステムの物理的構成と所有構造が裏付けない限り、その約束は危機の瞬間に守られることはありません。

契約条項は、相手方に約束を守る意思がある場合にのみ機能します。米国のCLOUD法や海外情報監視法（FISA）第702条は、米国企業に対して国家がその意思を撤回させる権限をすでに握っていることを示しており、フェーブル5のアクセス遮断事件は、その権限が同盟国に対しても実際に行使され得ることを証明しました。欧州の情報機関や行政省庁がエアギャップ

と所有構造の隔離へと舵を切った理由は、契約書が約束する保護とネットワーク設計が実際に生み出す保護の間に隔たりがあるという事実を身をもって経験したからです。

その隔たりを埋める作業は法条文一つで終わるものではなく、数年にわたる移植と独自の保守運用、そして独立した監査という三つの条件が揃って初めて完成します。

根拠および参考文献

1. Le Monde, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, 2026年6月17日, https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice_6754592_7.html

2. Todd Spangler, 'Microsoft can't keep EU data safe from US authorities, representative admits', Forbes, 2025年7月22日, https://www.forbes.com/sites/emmawoollacott/2025/07/22/microsoft-cant-keep-eu-data-safe-from-us-authorities/

3. 著者不明, '欧州のPalantir離脱の流れを一次ソースまで確認してまとめました', 2026年.

4. ChapsVision, 'ChapsVision chosen by France to deploy Argonos for OTDH project', ChapsVision, 2026年6月16日.

5. Loïc Duval, 'La DGSI remplace Palantir par ChapsVision', InformatiqueNews, 2026年6月18日.

6. 著者不明, 'La DGSI prépare la sortie progressive de Palantir au profit de ChapsVision', Solutions Numériques, 2026年6月17日.

7. European Commission, 'Proposal for the Cloud and AI Development Act (CADA)', COM(2026) 502, 2026年, https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada

8. Martyna Chmura, 'EU Cloud and AI Development Act: Sovereignty, AI and US Tech Dependence', Bloomsbury Intelligence and Security Institute (BISI), 2026年7月7日.

9. 出典なし（一般知識の補足）。（→データのローカリゼーションと技術的隔離の概念的な違い、エアギャップシステムが外部クラウドのリアルタイム更新や規模の経済から遮断され、自ら保守運用の負担を負うという一般的な技術原理を補足します。）

3.1 国内情報領域と軍事同盟領域の違い

2026年6月16日、フランスのセバスティアン・ルコルニュ首相は、国内セキュリティ総局（DGSI）が使用してきた米パランティアのプログラムを、フランス企業チャップスビジョン（ChapsVision）が開発したアルゴンOSに移行すると発表しました。同日、ル・モンド紙はパランティア側が政府と結んだ契約は依然として有効であると主張しているとあわせて報じました。発表と契約終了、実際のシステム移行はそれぞれ異なる時点で行われる別個の手続きです。6月16日のニュースは移行を開始するという宣言であり、アルゴンOSへの移植が完了したという確認ではありません。

ドイツ連邦憲法擁護庁（BfV）も同様の道を歩みました。2026年5月、BfVはアメリカの監視ソフトウェアに代わり、ハプスビジョンのアルゴンOSを新たに導入することを決定したと複数のドイツメディアが報じました。オランダ国防省は2026年6月、今後2年以内にパランティアのソフトウェアを完全に排除するという計画を発表しました。スイスの連邦機関は2018年から2025年の間に、パランティアが提出した情報関連の入札を少なくとも9回拒否したと伝えられています。スイスによるこの拒否は、ある一つの政府が急に下した決定ではなく、長年にわたり繰り返された調達上の判断でした。

スペインでも同様の動きが見られました。フェルナンド・グランデ＝マルラスカ内務相は、国家警備隊（グアルディア・シビル）とパランティアが共同で進めていたデータ分析事業を中断させました。スペイン軍事情報センターが2023年に結んだ1,650万ユーロ規模の契約は、満了後に延長されませんでした。軍首脳部は契約の維持を要請しましたが、受け入れられませんでした。スペイン政府は代わりに、自国の技術転換公社を通じて7億2,000万ユーロを投じ、独自の人工知能データセンターを建設することにしました。ベルギー政府は2029年までに10億ユーロを投入し、軍用データストレージ施設を自前で建設すると発表しました。

イギリスでは対立がより大きく表面化しました。イギリス下院の科学・イノベーション・技術委員会は、公共データ分析ネットワークをアメリカの民間企業に委ねた構造を安全保障上の脆弱点であると指摘する報告書を公表しました。イギリスの国民保健サービス（NHS）とパランティアが締結した3億3000万ポンド規模の契約をめぐり、下院議員たちは契約を打ち切るべきだと要求しました。議員らはそれほどの費用を払いながらも、データ構造を設計するオントロジーの権限を引き継げなかった点を問題として指摘しました。契約が終了してもイギリス政府の手元に残る技術資産がないという意味です。

下院は2027年2月から発動する主権上の理由による解約権条項を根拠に、パランティアとの関係を清算するよう政府に勧告しました。デンマーク議会でも2025年5月、野党がアメリカ製ソフトウェアへの依存を断ち切ろうという提案を行いました。

これらの決定はいずれも一国の内部で下されたものです。国内の情報機関や国防省は、自国の警察記録や諜報資料を自ら管理する権限を持っています。契約を終了し、他社の製品へ移行する手続きも、その権限の範囲内で比較的迅速に進めることができます。これには法律上の理由があります。アメリカ議会が2018年3月に制定したクラウド法（CLOUD Act）は、アメリカ法人が経営を統制するサービスであれば、データが保存されているサーバーがどの国にあろうと、アメリカの捜査機関からの正式な要請に応じてデータを提出しなければならないと定めています。

この条項が実際にどのような事件に適用されたのか、その要請が毎回合法的に処理されたのかは、事件ごとに判断すべき問題です。ただ、この法律が存在するという事実だけでも、ヨーロッパの情報機関は自国の捜査資料がアメリカ企業のサーバー構造内にある状態を負担として受け止めました。

同じ時期、多国間軍事同盟の決定は逆の方向へと動きました。北大西洋条約機構（NATO）傘下の通信情報局（NCIA）は2025年、パランティアのメイヴン・スマート・システムを連合作戦司令部で運用するための契約を結びました。この契約は、要求事項を策定する段階から署名まで約6か月で完了しました。NATOセキュリティ認証委員会は、それから1年以上が経過した2026年6月、このシステムの完全な技術的・作戦的能力を確認しました。調達契約を結んだ時点と完全運用能力を認証された時点は同一の出来事ではなく、その間には検証と試験を行う長い期間がありました。

この違いが生じる理由は、両領域が扱う業務の構造そのものが異なるためです。一つの国内情報機関が使用するシステムには、その国の国境内で、その国の法律に従う要員のみがアクセスします。フランス国内セキュリティ総局の捜査官が作成した事件記録は、アルゴンOS内でフランス語で保存され、フランスの検察や裁判所の手続きを経て初めて外部へ出ます。一方、メイヴン・スマート・システムは、最初から30か国を超える国の軍人が同じ画面を見つめ、同じ標的リストを共有するように設計されています。

米軍のアーネル・デイヴィッド大佐はこのシステム内で開発した戦術アプリケーションが50個を超えると明らかにし、これらのプログラムはNATO連合軍の通信標準であるSTANAG 4774および4778に従うよう作られました。標準に従うということは、ポーランドの兵士が入力した座標をノルウェーの兵士がすぐさま読み取り、米軍のパイロットがその座標に基づいて航路を設定できるという意味です。国内の捜査記録は国境を越えない方が安全であり、連合作戦の標的情報は国境を越えてこそ役に立ちます。二つの業務は安全の基準自体が反対の方向を指し示しています。

NATOの最高幹部らは、この違いを政治的選択ではなく軍事上の必要性として説明します。NATOの最高変革作戦司令官であるピエール・ヴァンディエ・フランス海軍大将は、ヨーロッパの軍隊が衛星画像を自動で分析し、弾薬補給を調整するのに使える自前のソフトウェアをま

だ保持していないと認めました。彼は、代替技術が熟する前に同盟の作戦遂行能力を低下させるわけにはいかないと述べました。カイ・ローアシュナイダー司令官をはじめとする他の指揮官たちも、加盟国がそれぞれ異なるシステムを使えば、暗号化された通信網間の接続が断たれるおそれがあると警告しました。

彼らの論理は、一国が情報主権を守ろうとして同盟全体の通信体系を弱体化させるならば、その損害の方がより大きいというものです。

この論理には反論も伴います。加盟国が自国の安全保障領域からパランティアを排除した理由は、アメリカの国内法がアメリカ企業のサーバーにアクセスする権限をアメリカの捜査機関に与えているという点にあります。この懸念を国内情報網では深刻に受け止めながら、NATOの指揮体系内では受け入れないとすれば、その基準はデータの性格ではなく、契約相手が国内機関か多国間同盟かによって分かれることになります。

この矛盾は資本の流れにも現れています。ドイツのインターネットメディア「ネッツポリティク（netzpolitik.org）」の報道によると、ヨーロッパ各国の銀行や資産運用会社は、自国政府がパランティアと距離を置いている間にも、パランティア株式の買い入れ規模をむしろ拡大させました。パランティアは2026年第2四半期の業績発表で、売上高が1年前より93パーセント増加したと発表しました。公共部門がパランティアから離れていった一方で、民間資本は同じ時期にパランティアへとさらに近づいていったのです。

これに先立ち、ドイツ連邦憲法裁判所は2023年2月16日、ヘッセン州警察がパランティアのゴッサム・エンジンをもとに構築した自動データ分析システム「ヘッセンデータ」に対し、違憲の決定を下しました。同裁判所は、個人のデータを自動的に結合して危険人物を特定するこのシステムには、十分な法的根拠がないと判断しました。この判決は欧州連合（EU）人工知能法が制定される前に出されたもので、国内の憲法秩序が国家安全保障上の例外とは別に、国内治安用の人工知能システムを統制できるという事実を先んじて示した事例です。

一つの国の憲法裁判所は、自国の警察システムにブレーキをかける力を持っています。しかし、32カ国がともに使う同盟指揮体系には、そのようなブレーキ装置を持つ単一の機関がありません。国内情報領域の離脱と軍事同盟領域の拡大は、統制できる主体がある領域とない領域の違いによって分かれます。

根拠および参考文献

1. フランス上院調査委員会, '欧州連合（EU）主要国の脱パランティアの動きとデジタル主権化に関する分析報告書', フランス政府公式ポータル, 2026.

2. ジョン・ヘンリー, 'France to ditch Palantir's AI data tools in favour of domestic provider', The Guardian, 2026年6月16日.

3. 記者不詳, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, 2026年6月17日.

4. 著者不詳, 'Absage für Palantir: Verfassungsschutz wählt Partner in Frankreich', Cybernews, 2026年5月26日.

5. IT-Daily編集局, 'Palantir: Bundesamt für Verfassungsschutz wählt ChapsVision', IT-Daily, 2026年5月.

6. コリン・バーク, 'Defensie wil binnen twee jaar af van Palantir-software', ICTMagazine, 2026年6月3日.

7. Egle˙Kristopaityte˙, 'Spain blacklists Palantir while NATO embraces its Maven Smart System', Cybernews, 2026年7月2日.

8. Le Soir編集局, 'Palantir s'implante en Belgique: 28 questions à (se) poser', Le Soir, 2026年3月19日.

9. Novara Media編集局, 'MPs Tell Government to End £330m NHS Contract With Palantir', Novara Media, 2026.

10. イギリス下院科学技術委員会, 'MPs warn that Palantir's increasing presence in the UK public sector is an "unacceptable point of weakness"', UK Parliament, 2026.

11. ヤン・エバーリ, 'Banken und Vermögensverwalter: Milliardeninvestitionen aus Europa fließen in Palantir', netzpolitik.org, 2026.

12. Palantir Investor Relations, 'Palantir Reports Q2 2026 U.S. Comm Revenue Growth of 149% Y/Y and Revenue Growth of 93% Y/Y', Palantir Technologies, 2026.

13. ドイツ連邦憲法裁判所, 'Decisions search - Judgment of 16 February 2023', ドイツ連邦憲法裁判所, 2023年2月16日.

14. 著者不詳, '欧州のパランティア離れの動きを一次ソースまで確認してまとめた資料', 2026. (スイスの9回にわたる入札拒否およびデンマーク野党提案の根拠)

15. SHAPE Public Affairs, 'NATO Maven Smart System Achieves Full Technical Operational Capability', SHAPE公式プレスリリース, 2026年6月30日.

16. NATO Communications and Information Agency, 'NATO acquires AI-enabled warfighting system', 2025.

17. U.S. Congress, Clarifying Lawful Overseas Use of Data Act, H.R. 4943, 2018.

3.2 NATO「メイヴン・スマート・システム（MSS）」の完全運用能力獲得と相互運用性の罠

米国国防総省は2017年、人工知能でドローンや衛星画像を分析し、軍事標的を割り出すプロジェクト・メイヴンを開始しました。パランティアはこの計画を足がかりに商用版を開発し、この商用版がNATOの導入したメイヴン・スマート・システムのルーツです。

NATO通信情報局（NCIA）は2025年、このシステムを連合作戦司令部で運用するための契約をパランティアと締結しました。調達要求事項を策定する段階から契約書に署名する瞬間までに要した期間は約6カ月でした。この時点でNATOが確保したのはシステムを使用する権利と契約であって、すべての軍事活動においていつでも運用できるという認証ではありませんでした。

完全な技術的作戦能力、すなわちFOC（Full Operational Capability）認証が得られたのは、それから1年以上が経過した後のことです。NATOセキュリティ認証委員会は2026年6月22日、メイヴン・スマート・システムが機密ネットワークで運用できる水準に達したと確認しました。NCIAのバルト・ファン・ミールト代理最高執行責任者は6月26日、この認証結果を同盟国の司令部に報告しました。NATO最高司令部（SHAPE）は6月30日、同システムが訓練や実戦を含むすべての軍事活動領域で制限なく運用できると公式発表しました。

NCIAのディラン・ブラウン総支配人は、連合軍の戦闘員にこの能力を手渡した協力を誇りに思うと明らかにしました。

契約を結んだ2025年と完全運用を認証した2026年の間には検証の期間がありました。このシステムは2026年5月13日にノルウェーで終了した多国籍演習「ステッドファスト・ディターランス」で、実戦に近い状況を経ました。ドイツ連邦軍のループレヒト・フォン・ブトラー少将は、この演習で人工知能が仮想敵軍の行動シナリオを自動的に作成する性能を確認したと語りました。

メイヴン・スマート・システムは軍事衛星やドローン、レーダーが送信するデータをリアルタイムで収集・分析します。兵士たちはこの画面を見ることで、打撃標的を絞り込む時間を大幅に短縮できます。米軍のアネル・デイヴィッド大佐は、このシステム内で開発された戦術アプリケーションが50個を超えると明らかにし、これらのプログラムは連合軍の通信標準規格であるSTANAG 4774および4778に準拠するよう作られています。この標準を守るということは、加盟国の軍隊が他国の軍隊と標的情報を安全にやり取りできることを意味します。

パランティア側はデータ所有権の問題について明確な立場を示しました。パランティアから派遣されたフィオナ・ブラッドリーは、メイヴン・スマート・システム内のすべてのソフトウェ

アおよびデータ所有権はNATO同盟にあると述べ、自社は顧客のデータを勝手に加工して転売する会社ではないと明らかにしました。この説明はデータが誰のものかという質問には答えていますが、そのデータを扱うプログラムの構造を誰が設計するのかという別の質問には答えになっていません。

システムの核心コードとデータ分類体系、すなわちオントロジーを修正する権限は、依然としてパランティアの民間技術陣にあります。NATO加盟国の軍人が入力した標的座標は、契約上は同盟の資産ですが、その座標を整理し分類する方式は、パランティアが定めた枠組みの中でしか動きません。図書館に例えれば、本の所有権は図書館にあっても、本をどのような順序で分類して棚に並べるかを決める司書の席には、依然としてパランティアの社員が座っている構造に近いです。データの所有権とシステムの設計権は同じ種類の主権ではなく、NATOが確保したのは前者であり、後者は依然としてパランティアの中に残されています。

このシステムの性能は実際の作戦で試練の場に立たされました。米軍は2026年2月、イランと連携する武装勢力を標的とした空爆を準備しました。軍は空爆を開始してから最初の24時間でメイヴン・スマート・システムを運用し、1000カ所を超える打撃候補地点を絞り込みました。この結果を見守った連合軍の指揮官たちは、アメリカ製ソフトウェアの処理速度に信頼を示しました。

同じ時期、フランスとドイツ、オランダは国内領域で正反対の決定を下していました。フランスは6月16日、国内セキュリティ総局のソフトウェアをArgonOS（アルゴンOS）へと移行すると宣言し、ドイツ連邦憲法保全庁も5月に同じ決定を下しました。ドイツ連邦軍のトーマス・ダウム副提督は4月、国防クラウド事業の最終調達規格からパランティアを除外しました。NATO指揮部の上層がパランティアのシステムへより深く入り込んでいく一方で、同じ国々の国内情報機関や国防調達網は同社からさらに遠ざかろうとしていたのです。

この二つの方向性の動きはNATO内部で摩擦を引き起こしました。ヴァンディエ司令官は、欧州の軍隊が衛星画像分析や弾薬補給の調整において、パランティアに対抗できる自国製ソフトウェアを未だ保持していないことを認めました。同氏は、代替技術が成熟する前に同盟の作戦能力を損なうわけにはいかないと述べました。ドイツのカイ・ローアシュナイダー司令官は、加盟国がそれぞれ自国で開発したシステムを個別に運用すれば、暗号化通信網間の接続が絶たれる危険性があると警告しました。

これに対抗して、フランスは独自の代替案を実験し始めました。フランス国防省は2026年6月、ポーランドで開催された調達演習でアルカディア・プラットフォームを試験しました。アルカディアは、フランスの防衛企業タレスとサフラン、そしてミストラルAIが共同開発した戦場認知ソフトウェアです。フランス陸軍副参謀長のパトリック・ジュステル将軍は、NATOが外国のシステムを何の疑いもなく受け入れる慣行が、自国の情報安全を脅かしていると指摘し

ました。フランスとドイツの首脳は2026年7月17日、欧州独自の主権的デジタルバックボーンを構築するという共同宣言に署名しました。

アルカディアがメイヴン・スマート・システムを代替できるほど定着するには時間がかかります。その間、NATO指揮体系の相互運用性の要求は、加盟国が標的情報を共有し通信標準を合わせるよう圧力をかけ続けることになり、その圧力はすでに検証を受け標準を満たしているパランティアのシステムへと調達を引き寄せます。国内情報機関は国境の内側で決定を下し契約を終了させることができますが、32カ国が共同で使用する指揮体系は一国が勝手に変更することはできません。この差異こそが、NATOにおいて相互運用性が国内統制権を圧倒し続ける理由なのです。

根拠および参考文献

1. NATO Communications and Information Agency, 'NATO acquires AI-enabled warfighting system', 2025.

2. SHAPE Public Affairs, 'NATO Maven Smart System Achieves Full Technical Operational Capability', SHAPE公式プレスリリース, 2026年6月30日.

3. Tamara Rozouvan, 'Maven Smart System achieves full operating capability with NATO', Janes, 2026年7月1日.

4. ヌライ・テイラー, 'NATO's 'Digital Lethality Branch' Breaks Records in Drive for Alliance-Wide Interoperability', AFCEA International, 2026年7月31日.

5. フェルナンド・カストロ・デ・ベイロ, 'Foreign software, Europe's War: How Maven and Palantir are already making decisions for Europe', DigitalShield, 2026年7月15日.

6. ウィキペディア(Wikipedia), 'Palantir', 2026年8月9日最終改訂.

7. 記者不詳, 'Spain blacklists Palantir over domestic security concerns', The Cradle, 2026年8月3日.

8. Egle Kristopaityte, 'Spain blacklists Palantir while NATO embraces its Maven Smart System', Cybernews, 2026年7月2日.

9. T.Wiegold, 'Cyber-Kommandeur der Bundeswehr lehnt Software von Palantir ab', Augen geradeaus!, 2026年4月28日.

10. Cybernews編集部, 'France and Germany to build an alternative to Palantir', Cybernews, 2026年7月20日.

11. ジョン・ヘンリー, 'France to ditch Palantir's AI data tools in favour of domestic provider', The Guardian, 2026年6月16日.

12. 著者不詳, 'Absage für Palantir: Verfassungsschutz wählt Partner in Frankreich', Cybernews, 2026年5月26日.

3.3 欧州連合人工知能法（AI Act）安全保障例外条項と統制の死角

人工知能法（AI Act）は、人工知能システムが人に及ぼし得るリスクの大きさに応じて規制の強度を変える法律です。リスクが大きいシステムほど、透明性やリスク評価、人間の監督義務を重く課します。同規則第2条は、軍事、国防、国家安全保障目的でのみ市場に投入されるか使用される人工知能システムには、本法が適用されないと定めています。この例外は、システムを開発または運用する主体が政府機関であるか民間企業であるかを問いません。前文（リサイタル）第24項はその根拠を明らかにしています。

国家安全保障は欧州連合の条約体系において加盟国が単独で責任を負う領域であり、軍事および国防活動はその性質上、欧州連合の共通外交安全保障政策のもとで別途の規律を受けるということです。

この例外条項は、交渉の過程で偶然残された隙間ではなく、加盟国がactivelyに要求して勝ち取った結果です。Centre for Future Generationsの2026年春号の報告書によると、フランスはイタリア、スウェーデンとともに、国家安全保障を理由に例外範囲を広げるロビー活動を主導しました。 these 政府は、治安当局が公共の場所で顔認識カメラや生体認証監視ツールを使用する際、ブリュッセルのリスク評価手続きを経なくても済むことを望んでいました。その結果、国内治安機関の情報網と軍事同盟の標的識別システムは、並んで人工知能法の適用範囲外となりました。

この死角の中に置かれた代表的なシステムが、国内治安用のゴーサム系列プログラムとNATOのメイヴンスマートシステムです。人工知能法が他の高リスクシステムに要求する文書化の義務、誤作動や偏向を追跡する手続き、人間が最終決定を検証する仕組みは、これら二つのシステムには法的に強制されません。NATOセキュリティ認証委員会が2026年6月、メイヴンスマートシステムに完全運用認証を与えた手続きは、本法の審査を経ていません。

しかし、この免除は無規制と同義ではありません。第2条の例外は、軍事、国防、国家安全保障目的でのみ使用される場合に限定されます。同じ企業が開発した同じ種類のソフトウェアであっても、公共行政や民間治安業務のように軍事目的以外の場所で使用されれば人工知能法の適用を受けます。例外は特定企業や特定顧客に付されるラベルではなく、その人工知能が実際に使用される用途に付される条件なのです。

人工知能法が適用されない場所に、他の法的枠組みが全く存在しないわけではありません。ドイツ連邦憲法裁判所は2023年2月16日、人工知能法が制定される前に、ヘッセン州警察の自動データ分析システム「ヘッセンデータ」に対して違憲決定を下しました。この判決は、国家安全保障や治安を名目とする人工知能システムであっても、各国の憲法秩序においては別途の

法的根拠を備えなければならないという原則を打ち立てました。人工知能法の国家安全保障例外は、この規則一つが適用されないということを意味するだけであり、加盟国の憲法や個人情報保護法令、議会の監督権限までもがすべて消失することを意味するわけではありません。

NATOの観点からも、完全な無法地帯というわけではありません。メイヴンスマートシステムがNATOセキュリティ認証委員会の承認を経なければならなかったという事実自体が、人工知能法が適用されない場所にNATO独自の認証手続きが代わりに入り込んでいることを意味します。ただ、この認証手続きはシステムが安全に作動するかを軍事的基準から確認する手続きであり、人工知能法が要求する偏向チェックや市民に対する透明性義務のような基準で設計されてはいません。監督の主体と基準が変わっただけであり、監督そのものが消滅したわけではないのです。

ただ、その監督が国防機密のもとに置かれたことで、市民がその結果を検証する手段は、国内情報領域に比べて遥かに狭くなりました。

欧州議会は2026年1月、アメリカの一部のIT企業への依存を減らそうという技術主権決議案を採決に付して可決しました。議員たちは、マイクロソフトやアマゾンのようなアメリカ企業にデータが過度に集中すれば、アメリカ政府の一つの決定によって欧州のサービスが停止しかねないというリスクを理由に挙げました。米政権はこうした欧州の規制の動きに反発し、貿易報復の可能性を示唆しました。

フランスとドイツの首脳は2026年7月17日、欧州独自の主権的デジタルバックボーンを構築しようという共同宣言に署名しました。この宣言が指し示す方向は、アルカディアのような独自のソフトウェアを実際に完成させることです。人工知能法の国家安全保障例外は、欧州がアメリカの技術に依存している状態を規制によって阻むことはできないという事実を認めた条項であり、その依存を解決する条項ではありません。規制の手が届かない場所を埋める仕事は、欧州が自ら開発した代替技術の役割として残されました。

根拠および参考文献

1. Regulation (EU) 2024/1689, Artificial Intelligence Act, Article 2 and Recital 24, 2024年12月13日.

2. Centre for Future Generations, 「Enforcement spotlight - Spring 2026」, Centre for Future Generations, 2026年春号, 2-3頁.

3. ドイツ連邦憲法裁判所, 'Decisions search - Judgment of 16 February 2023', ドイツ連邦憲法裁判所, 2023年2月16日.

4. フランス上院調査委員会, '欧州連合(EU)主要国の脱パランティアの動きとデジタル主権化に関する分析報告書 (Yuropyeonhap (EU) Juyoguk-ui Tal-Palantier Haengbo-wa Dijiteol Jugwonhwa-e Gwanhan Bunseok Bogoseo)', フランス政府公式ポータル, 2026.

5. SHAPE Public Affairs, 'NATO Maven Smart System Achieves Full Technical Operational Capability', SHAPE公式プレスリリース, 2026年6月30日.

6. オランダ国防省および欧州技術委員会, '欧州のパランティア離脱の傾向を一次ソースまで確認して整理した資料', 2026.

4.1 クラウド・AI開発法（CADA）とデータセンター加速化区域の規制革新

欧州連合執行委員会は2026年6月3日、クラウド・AI開発法の提案を正式に提示しました。英語名は Cloud and AI Development Act、略してCADAと呼ばれます。文書番号はCOM(2026) 502です。まずこの事実を明確にしておかなければなりません。CADAはまだ法律ではありません。欧州連合執行委員会が欧州議会と理事会に審議を求めた規則提案であり、本書が扱う2026年8月11日の時点では正式に採択されていません。

欧州連合において規則（Regulation）は、指令（Directive）とは異なり、加盟国内の議会による別途の立法を必要とせず、直ちに効力を有する強い法的形式です。それだけに、規則として確定するまでの審議手続きも厳格です。通常の立法手続きでは、欧州議会と理事会がそれぞれ修正案を提出し、採決を経て初めて条文が確定します。その過程で、現在の提案書に盛り込まれた条文や数値は変わる可能性があります。本章で説明する4段階の主権保証レベルや加速化区域、解約権条項は、いずれも提案段階の設計図にすぎません。すでに加盟国政府や企業を拘束する規範ではないのです。

この区別は、欧州連合人工知能法（AI Act、Regulation (EU) 2024/1689）とCADAを混同しないためにも必要です。人工知能法は2024年にすでに制定され効力を持っている規則であり、人工知能システムをリスクレベルに応じて分類し、それに応じた義務を課す法律です。一方、CADAはその人工知能が稼働するインフラと調達手続きを扱う別途の提案であり、2026年8月現在、まだ制定されていません。二つの法律の名称にともに「人工知能」という言葉が入っているからといって、両者の法的地位を同等に扱うべきではありません。

一方はすでに施行されている規範であり、他方はまだ審議を待つ提案なのです。

CADAは、執行委員会が推進してきた「人工知能大陸行動計画」の一環として登場しました。この計画の目標は二つに要約されます。欧州域内にあるデータセンターの演算能力を増強することと、その演算能力を欧州国外の司法管轄から守ることです。この二つの目標が一つの法案の中にまとめられた背景には、欧州のクラウド市場の構造が存在します。アマゾン、マイクロソフト、グーグルの3社が欧州のクラウドインフラサービス市場で圧倒的なシェアを占めており、欧州に本社を置く企業のシェアはそれに遠く及ばないと、複数の業界報告書が伝えています。

技術政策メディアのテック・ポリシー・プレス（Tech Policy Press）は2026年6月15日の記事で、このような偏りが公共システムの運命を外国の司法権の下に置く安全保障上の脆弱性につながると指摘しました。

CADAの前にも、欧州は同様の試みを行ったことがあります。2019年にフランスとドイツが主導して発足したガイアX（Gaia-X）は、欧州企業が共同で利用できるデータインフラ規格を構築しようとした民間主導のプロジェクトでした。しかし、ガイアXは法的拘束力のない自主的な協議体であり、参加企業間の利害関係が対立したことから、当初目標としていたほどの成果を上げられなかったと評価されています。CADAがガイアXと異なる点は、自主的な標準ではなく、法的拘束力を持つ規則によって調達市場 payments/調達市場そのものを動かそうとしているところにあります。

ただし、その規則が実際に効力を持つためには欧州議会と理事会の審議を通過しなければならないという点で、CADAもまた、まだ意志の表明段階にとどまっています。

一般の読者には馴染みの薄い話かもしれません。政府や病院、警察が使用するコンピュータシステムだからといって、必ずしもその国の国境内にある建物で稼働しているわけではありません。アマゾンやマイクロソフト、グーグルのような企業のクラウドサービスを借りて利用する場合、実際の演算はその企業が世界各地に建設した大型サーバー群で行われます。このような超大型サーバー群を業界ではハイパースケーラーと呼びます。サーバーの建物が物理的に欧州の土地の上にあっても、その建物を所有・運営する企業が米国法人であれば、米国政府の法的要求がその上のデータに及ぶ可能性があるのです。

物理的な位置と法的統制権が異なる可能性があるというこのギャップこそが、本章全体を貫く核心的な論点です。

これに加えて、クラウド産業には「データ重力」と呼ばれる現象があります。一度、大量のデータを特定の企業のクラウドに移してしまうと、そのデータを処理する他のプログラムやサービスも、同じクラウド内に置く方が速く、安くなります。時間が経つにつれ、データとそれを扱うアプリケーションが、一社のエコシステムの内部にますます深く絡み込まれていくのです。公共機関が当初、ストレージ容量を借りるといった程度の契約から始めたものの、数年もしないうちに、その企業のクラウドなしには行政業務全体が機能しなくなる状態に至ることは珍しくありません。

欧州の政策立案者たちが、市場シェアの数値以上にこの「絡み合いの深さ」を懸念している理由はここにあります。

マリオ・ドラギ元欧州中央銀行（ECB）総裁が2024年9月に欧州連合へ提出した競争力報告書は、この問題をあらかじめ警告した文書として頻繁に引用されます。ドラギ報告書は、欧州が独自に人工知能を開発しサービスを運営するためには、主権が保証された演算処理能力を備えなければならないと勧告しました。この勧告はその後、欧州連合執行委員会の政策文書の随所に繰り返し登場します。欧州域内にサーバーを置いているという事実だけでは不十分であり、そのサーバーを統制する企業の国籍や支配構造まで考慮すべきだという認識が、CADA提案の出発点なのです。

執行委員会は、このデータセンター拡充目標を「AIギガファクトリー」という名称の別途事業と組み合わせて推進しています。AIギガファクトリーは、大規模なグラフィックス処理装置（GPU）クラスタを備えた超大型演算施設を指す名称であり、「人工知能大陸行動計画」で提示された概念です。単にサーバーの台数を増やすことにとどまらず、欧州域内で大型人工知能モデルを最初から最後まで学習させられる演算能力を確保するという目標が、この事業の背景にあります。これまで欧州の研究者や企業は、大型モデルを学習させるために米国クラウド企業が提供する演算資源を借りて利用せざるを得ませんでした。

CADAとAIギガファクトリーは、この賃貸構造そのものを変えようとする試みなのです。

この目標を裏付けるインフラが、すでに一部稼働している点も注目に値します。欧州連合は2018年から「欧州高性能計算共同事業（EuroHPC Joint Undertaking）」を通じて、加盟国とともにスーパーコンピュータを運用してきました。フィンランドのLUMI（ルミ）やスペインのMareNostrum（マレノストルム）といった既存のスーパーコンピュータを人工知能学習用の演算資源へと転換する事業が、CADAの発議に先立ちすでに始まっていました。

CADAとAIギガファクトリー構想は、この既存資産を完全に代替するものではなく、その上に民間資本と加盟国の予算をさらに呼び込んで規模を拡大する方向で設計されています。

欧州委員会が明らかにしたCADAの数値目標は明確です。欧州連合のデータセンター容量を、今後5年から7年の間に3倍以上に拡大するというものです。そのように拡大された容量によって、2035年までに企業と公共行政の需要を満たすことを目標としています。この目標は、欧州委員会が発行した提案文書自体に盛り込まれています。目標がこれほど大きく設定された理由は、需要と供給のギャップがすでに広がりつつあるためです。

欧州議会が2026年1月22日に採択した『欧州の技術主権とデジタルインフラ』文書は、世界の電力消費の相当部分がデータセンターと通信設備から発生しており、欧州のデータセンターの電力消費比率が今後数年の間に目立って増加すると見込んでいます。人工知能の演算が本格的に増えれば、この比率は一層急激に上昇します。データセンターを建設する速度がその需要に追いつかなければ、欧州は人工知能開発において米国や中国のクラウドを借りて使う立場を抜け出すことが難しくなります。

問題は、データセンターの建設自体が遅いという点にあります。加盟国内で公共行政用のデータ保存施設を新設しようとするたびに、複雑な許認可手続きや土地規制、環境影響評価が事業の足かせとなる事例が相次いで報告されました。ドイツ連邦情報セキュリティ庁と国際法律事務所バード＆バードが2026年4月27日に共同で発表した報告書は、ドイツ連邦政府と州政府の間の行政手続きの不一致が、調達仕様書の段階から遅延を生んでいると指摘しました。このような遅延はドイツだけの問題ではありません。

大規模なクラウドサーバー構築計画が地域住民の反発や環境審査の遅延によって縮小されたり白紙化されたりする出来事は、欧州の多くの国で繰り返されてきました。ある地域でデータセンターの敷地を選定し、電力を引き込み、許認可を取得するだけでも数年がかかる間に、演算需要はそのはるかに速いスピードで増加していきます。

CADA提案は、この遅延を減らすための手続き革新を中核の柱としています。政治メディアのポリティコ欧州版は2026年6月4日の報道で、CADAが加盟国政府に対し、地理や電力網の条件が良い敷地をデータセンター加速化区域として指定するよう勧告していると伝えました。法律事務所バード＆バードがまとめた技術主権パッケージ概要報告書もまた、この加速化区域内では許認可手続きが単一窓口に統合され、処理期限に上限が設定されるという提案の趣旨を確認しました。事業者が複数の行政機関を個別に訪問する代わりに、一箇所で事業のライフサイクル全体の調整を受ける仕組みです。この単一窓口が統合しようとする手続きは多岐にわたります。

電力網への接続承認、上水道と冷却水の供給許可、建築安全審査、通信回線の引き込み許可のように、異なる行政機関が個別に管理していた手続きを一つの窓口で調整するというものです。これまでは事業者がこれらの手続きを一つずつ順番に踏まなければならず、一つの段階で遅延が生じると、それに続く手続き全体が遅れる構造でした。報道によれば、この加速化区域内では機密データを扱う施設の許認可処理期限が最大18ヶ月に制限されます。

大型施設を一つ建設するのに必要な許認可手続きに何年もかかる事例が珍しくなかった点を考えると、この上限線は手続き自体を根本から組み直すというシグナルとして読み取ることができます。

環境影響評価の手続きについても、加速化区域内の事業に限Parent simplifying（簡素化）される方向で設計されていると同報告書は伝えています。この簡素化が実際に環境審査自体を免除するレベルなのか、審査期間を短縮するにとどまるレベルなのかは、提案書が欧州議会と理事会の審議を経て具体化される事項です。現段階で確定した条文として断定することは時期尚早です。ただし、その方向性だけは明確です。国家安全保障に直結するインフラ事業であれば、通常の地方自治体による許認可手続きよりも優先順位を高く置くということです。

敷地を加速化区域として指定する権限は、一次的には加盟国政府にあるとされています。地方政府や中央政府が、電力網の余剰容量や通信回線へのアクセス性、物理的セキュリティが確保される敷地を絞り込んで欧州委員会に提案し、欧州委員会がこれを検討して最終リストに反映させる方式です。この手続きは、半導体法がすでに施行しているファウンドリ敷地指定方式と類似した枠組みを取り入れたものと評価されています。

この拡充目標は、欧州連合の気候目標とも連動しています。欧州連合は2050年までにカーボンニュートラルを達成するという目標を、欧州グリーンディールを通じて明確に定めています。データセンターの電力消費が増加し続ける状況でこの目標を守るためには、新設する施設

の相当数を再生可能エネルギーで稼働させなければならないという圧力が生じます。CADAが加速化区域の優遇措置を持続可能性基準と結び付けたことは、スピードのために気候目標を犠牲にはしないというシグナルとして読み取ることができます。

加速化区域の構想にはリスクも伴います。手続きを迅速化する優遇措置は、その特典を受ける事業が実際に公益に適合しているかを検証する仕組みがなければ、税金の無駄遣いにつながりかねません。スウェーデンでは2022年、政府が自国の技術インフラを拡充する目的でデータセンター企業に税制優遇を提供しましたが、それらの企業が再生可能エネルギーの使用計画を実際に守ったかどうかを検証する手続きが不十分だったとの指摘がなされました。スウェーデンのメディアであるSecurityUser.comは2026年3月にこの問題を振り返り、北欧各国がデジタル主権インフラ政策の再設計を進めていると伝えました。

CADAの提案は、このような失敗を繰り返さないために、加速化の優遇措置を受ける事業者に対して持続可能性基準の遵守を証明するよう求める安全装置を含んでいると、バード＆バードの報告書は説明しています。スピードを優先して手続きを削減する一方で、その引き換えに結果を検証する義務を新たに負わせた形です。

財政規模を見ると、CADAが単独で動く法案ではないという事実が明らかになります。欧州委員会が2026年6月3日に併せて公開した付属文書（COM(2026) 555 final/2）は、クラウド・AI開発法と次世代安全保障パッケージを完全に実行するために、2036年までに総額3,000億ユーロに上る投資が必要であると試算しました。このうち、データセンターインフラの拡充に2,000億ユーロが割り当てられます。半導体ファウンドリおよび人工知能ギガファクトリーの構築には、さらに1,000億ユーロが追加で配分されると同文書は見込んでいます。

この投資計画は、クラウド・AI開発法単独のためのものではありません。2023年に発効した欧州連合半導体法が半導体生産能力の拡充を扱ったとすれば、CADAの財政計画 me（その）半導体上で稼働するデータセンターや人工知能インフラを扱う後続事業に近いといえます。業界分析報告書のinnobuは、これら二つの法律が一体となって欧州の技術主権パッケージを構成していると説明しました。なお、この数値はあくまで欧州委員会の試算であり、実際の執行予算は加盟国と欧州議会の予算交渉を経て確定します。

欧州連合の首脳らが2025年11月18日にベルリンに集まり、安全保障会談の共同宣言を発表した出来事が、この財政計画の政治的背景として挙げられています。

このインフラ拡充が扱う脅威の性質は、第2章で確認したモデルへのアクセス遮断とは毛色が異なります。アンスロピックがフェーブル5への外国人アクセスを一時停止した事件は、ソフトウェア層で起きた出来事でした。米国政府の輸出規制指示ひとつで、特定モデルへのアクセス権限そのものが遮断されました。一方、データセンターを所有していない状態で発生する脅威は、より根本的です。演算能力 capabilities そのものを他国の企業から借りている立場であれば、モデルではなく、そのモデルが稼働するハードウェアへのアクセスが遮断されかね

ないということを意味します。CADAが狙いを定めているのは、このハードウェア層の脆弱性です。

バード＆バードとITメディアのイットベルトの報道を総合すると、CADA提案は2030年までに欧州域内の民間企業の相当数が主権クラウドサービスへ移行するよう誘導する目標値もあわせて提示したとのことです。あわせて、低遅延のエッジコンピューティング拠点を大陸全域に細かく配置し、米国系大手プラットフォームへの依存を消費者サービス領域でも引き下げるという構想が共に取り沙汰されています。これらの目標が最終規定で強制義務として残るか、勧告レベルに緩和されるかは、審議過程を見守る必要があります。

この優先順位指定には、地域社会の発言権が狭まるという代償が伴います。データセンターが国家的に重要な戦略事業に指定されれば、その敷地の住民が通常の都市計画手続きで行使できた異議申立てや公聴会への参加の幅が狭まる可能性があります。スピードのために手続きを削減するということは、その手続きの中にあった地域住民の声を取りこぼすということでもあります。このバランスをCADAが最終的にどのように調整するかは、まだ確定していません。

電力確保のあり方を巡り、加盟国間のアプローチも分かれています。原子力発電の比率が高いフランスは、原子力発電所の近くにデータセンターを建設する案を政策的に推進しています。安定した低炭素電力をデータセンターに直接供給できる点が、このアプローチの長所として挙げられます。一方、再生可能エネルギーを中心に電力網を再編してきた国々は、太陽光や風力の間欠性をデータセンターの24時間稼働需要とどう合わせるかという課題を別途解決しなければなりません。CADAの加速化区域の指定基準に電力網の条件が含まれているのも、こうした国ごとの事情の違いを考慮した設計とみられます。

加速化区域の指定が特定の加盟国に集中する可能性も議論されています。電力網や通信インフラがすでに整っている西欧や北欧の一部地域が先に指定要件を満たす公算が大きく、インフラ投資が相対的に遅れている東欧や南欧の一部地域は取り残されるリスクがあります。欧州連合の地域均衡発展の原則と、データセンター加速化というスピードの論理がどのように調和をなすのかも、CADAが最終条文を整える過程で扱うべき課題として残されています。

CADAが描く絵は、結局のところ一つの問いに絞られます。欧州が自らのデータを保存する物理的空間を自前で構築できなければ、その上で稼働するソフトウェアの主権を議論することも空虚になるということです。物理的なデータセンターという土台の上には、もう一つの層が存在します。誰がそのデータセンターを統制するのかを分ける基準です。

根拠および参考文献

1. European Commission, 'Proposal for the Cloud and AI Development Act (CADA)', COM(2026) 502, 2026, https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada

2. European Commission, 'Cloud computing', 2026, https://digital-strategy.ec.europa.eu/en/policies/cloud-computing

3. Cecilia Rikap, 'Does Europe Really Have a Plan for Tech Sovereignty?', TechPolicy.Press, 2026年6月15日, https://www.techpolicy.press/does-europe-really-have-a-plan-for-tech-sovereignty-cada/

4. Mario Draghi, 「The Future of European Competitiveness」, European Commission, 2024年9月.

5. European Parliament, 'Texts adopted - European technological sovereignty and digital infrastructure', 欧州議会官報, 2026年1月22日.

6. ドイツ連邦情報技術保安庁, 「Digitale Souveränität bei IT-Vergaben: Zwischen politischem Anspruch und vergaberechtlicher Wirklichkeit」, Bird & Bird Insights, 2026年4月27日.

7. Tyler Weygold, 'Achieving digital sovereignty: A golden opportunity for the EU?', POLITICO Europe, 2026年6月4日, https://www.politico.eu/video/achieving-digital-sovereignty-a-golden-opportunity-for-the-eu-politico/

8. Kiteworks, 'Tech Sovereignty Package: an overview', Bird & Bird, 2026年6月23日.

9. SecurityUser.com, 'Ny molnpolicy ska ge ökad digital suveränitet i offentlig förvaltning', SecurityUser.com, 2026年3月.

10. European Commission, COM(2026) 555 final/2, 欧州連合官報, 2026年6月3日.

11. innobu, 'EU Tech Sovereignty 2026: Chips Act 2.0 and CAIDA', innobu Insights, 2026年6月.

12. Itwelt 編集局, 'Best European cloud alternatives: Top 10 of 2026', Itwelt, 2026年2月.

4.2 CADAの4段階主権保証レベル（Sovereignty Assurance Levels）設計

CADA提案が掲げた2番目の軸は、データセンターという物理的な外枠ではなく、その内部で稼働するソフトウェアと、それを運用する企業の国籍を見極める基準です。欧州委員会はこの基準を4つの段階に分けて提示しました。英語ではソブリンティ・アシュアランス・レベル（Sovereignty Assurance Level）、略してSEALと呼ばれます。ロンドンの安全保障政策研究機関であるブルームズベリー情報安全保障研究所（BISI）が2026年7月7日に発表した報告書は、この4段階構造をCADAの3つの軸の1つとして整理し、その設計目的は米国のクラウド法（CLOUD Act）や外国情報監視法第702条が欧州の公共データに及ぼす影響力を遮断することにあると説明しました。

米国議会が2018年に可決したクラウド法は、米国法人が経営を支配する情報通信サービス事業者に対し、データがどの国に保存されているかに関わらず、捜査機関に資料を保存し提出する義務を課しています。法案本文や議会の要約で確認できるこの条項は、欧州内に設立された米国企業の子会社にも適用される可能性があります。欧州企業と契約を結び、欧州の領域内にサーバーを置き、欧州の個人情報保護法を遵守していたとしても、そのサーバーを運用する会社の親会社が米国法人であれば、米国の捜査機関による要請が契約書より優先し得るという意味です。

欧州委員会がCADA提案とともに公表した付属実務文書（SWD(2026) 502 final）は、この域外管轄権の問題を詳細に分析しているとされています。

SEAL体制を個人情報保護法と混同してはなりません。欧州連合の一般データ保護規則（GDPR）は、個人情報をどのように収集し処理すべきかを規律する法律であり、すでに2018年から施行されています。GDPRを遵守しているからといって、その情報を扱う企業の国籍問題まで解決されるわけではありません。情報をいくら安全に暗号化し、必要な分だけ収集したとしても、その情報を保管している企業が米国法人であれば、米国政府の法的要請の前ではGDPRによる保護も限界を露呈します。GDPRが規律するのは情報の扱い方であり、SEALが規律しようとしているのはその情報を扱う企業の国籍と支配構造です。

二つの法律は、異なる階層から同じデータを見つめています。

欧州の裁判所は、すでに一度この問題と正面から衝突したことがあります。欧州司法裁判所は2020年7月、いわゆる「シュレムスII（Schrems II）」判決において、米国の情報機関が通信データにアクセスできる米国の監視法制を理由に、欧州連合と米国間の個人データ移転協定である「プライバシーシールド」を無効と判断しました。契約書にいかに緻密な個人情報保護条項を盛り込んだとしても、その契約の相手方が米国法の適用を受ける限り、米国の情報

機関によるアクセス可能性そのものを契約によって阻むことはできないというのが、この判決の骨子でした。

CADAが国籍と支配構造という、契約条項よりもはるかに根本的な基準で主権レベルを区分することにした背景には、こうした司法上の経験の蓄積があります。欧州が得た安全保障上の教訓は, 結局のところ契約書の文言ではなく、会社の支配構造と国籍こそが実質的な保護膜となるという事実でした。

この教訓は市場の反応にもつながりました。アマゾン、マイクロソフト、グーグルはここ数年、欧州の顧客に向けて、それぞれ独自の名称を冠したソブリン型クラウド製品を投入しました。データを欧州内でのみ保存・処理し、欧州人以外の従業員によるアクセスを制限するという約束が、こうした製品に共通する宣伝文句です。しかし、これらの製品がSEALの上位段階である第3段階や第4段階で要求される支配株式や取締役会の議決権まで欧州側に譲渡するケースは極めてまれです。サーバーの位置と運用規定を欧州化することと、会社の所有権そのものを欧州化することは、全く異なる次元の約束です。

SEAL体制が目指しているのは、まさにこの二つの次元を明確に区別し、調達基準に明記することです。

具体的な事例として、アマゾン・ウェブ・サービスは2023年、欧州専用の法人を別途設立し、欧州市民で構成された取締役会と経営陣を置く「欧州ソブリン・クラウド」事業を発表しました。データの保存と運用人員を欧州内に置くという約束でした。しかし、この欧州法人の最終的な株式は依然として米国の親会社であるアマゾン・ドット・コムが握っています。SEALの第3段階と第4段階が要求しているのは、まさにこの最終的な所有構造まで欧州の所有に変わることであるため、このような形態のソブリン型クラウド商品は、下位段階の資格は得られても、上位段階のハードルを越えることは困難です。

SEALの第1段階は、最も基本的な要件を求めています。データの保存と処理が欧州連合の領域内の施設で行われなければならないというものです。この段階は国家機密性の低い一般行政業務に適用され、米国系を含む域外企業の欧州支社であっても、欧州内にデータセンターを備えていれば、この基準を満たして入札に参加することができます。サプライヤーが自ら要件の充足を宣言する自主証明方式で承認が行われ、別途の第三者監査は求められません。

第2段階は、データが物理的にどこにあるかを超えて、そのデータを扱うソフトウェアのサプライチェーンにまで目を向けます。サプライヤーは、ソフトウェアの構成要素を詳細に記録したソフトウェア部品表（SBOM）を提出し、ソースコードのセキュリティ上の脆弱性を検証されなければなりません。ソフトウェア部品表とは、一つのプログラムがどのような部品、すなわちどのような外部ライブラリやオープンソースの構成要素で成り立っているかを緻密に記したリストです。食品の原材料表示に似た概念と考えると理解しやすいでしょう。

ある一つの構成要素でセキュリティ上の欠陥が発見された際、その欠陥が自らの運用するシステムにも含まれているかをリストを見るだけで迅速に確認できるようにするという趣旨です。BISIの報告書によると、この段階は医療情報や金融インフラのように重要度が中程度である公共サービスに適用されるよう設計されています。域外企業であっても、欧州企業と合弁を組んで支配構造を分担し、技術的な隔離措置を証明すれば、この段階の資格を取得できる道が開かれています。

第3段階からは、要件が格段に厳格になります。データを処理するサプライヤー企業およびその下請け企業の本社が欧州連合の領域内に実在しなければならず、支配株式と取締役会の議決権が欧州連合の国籍を有する者の手になければなりません。システムを保守・運用する中核人員もまた、欧州連合の国籍を持つ居住者でなければならず、身元調査を通過する必要があります。ただし欧州委員会は、欧州連合と情報共有条約を結び、司法上の摩擦がない同盟国に対しては、この要件を部分的に緩和する例外措置の枠組みを提案書に残しているとBISI報告書は伝えています。この段階は、国家の治安捜査網やテロ脅威分析のように、安全保障に直結する業務に適用されます。

友邦国に対する例外措置が実際にどの国に適用されるかは、まだ確定していません。情報共有条約と司法協力体制をすでに欧州連合と整えている国が候補として取り沙汰されていますが、具体的な国名リストは提案段階では公表されていません。このあいまいさは、CADAの審議過程において最も激しい交渉の対象となる懸案の一つに挙げられています。例外の範囲を広く設定すれば第3段階の効力が薄れ、狭く設定すれば友邦国との外交的摩擦を甘受しなければなりません。

4つの段階を一度にイメージするのが難しい場合は、建物の入退室管理を思い浮かべてみるとわかりやすいでしょう。ロビーは訪問証さえあれば誰でも入ることができ、オフィス階は社員証が必要で、サーバー室は別途承認を受けた一部の人しか入れず、最も奥にある金庫室は身元調査を終えたごくわずかな人しか入れません。SEALの4つの段階もこれと似ており、扱う情報の重要度が増すにつれて、アクセスが許可される主体の範囲が次第に狭まっていく構造になっています。

第4段階は例外の存在しない段階です。国防や軍事機密、最上位の治安分析など、国家の存立に直結する領域に適用され、第3段階の取締役会の国籍要件や人員条件をそのまま遵守しつつ、同盟国に対してもいかなる例外も認めません。システムの設計段階からソースコードの保守に至るまで、外国の商業資本が関与する余地を根本から遮断します。サプライヤーは欧州連合サイバーセキュリティ庁（ENISA）が発行する欧州サイバーセキュリティ認証制度（EUCS）で最高等級である「ハイ（High）」を取得して初めて入札に参加できます。なお、このEUCS認証制度はCADAが新設したものではありません。

ENISAは既に数年前からこの認証制度を準備してきましたが、最高レベルに非欧州企業の所有持分を制限する条項を盛り込むかどうかを巡り、加盟国間で意見の相違が続いてきたことが知られています。フランスをはじめとする一部の加盟国は所有持分の制限を強く要求し、他の加盟国はそうした制限が市場競争を阻害すると反対してきました。CADAが第4段階の要件にEUCSの「ハイ」レベルを明示的に組み込んだことは、これまで認証制度の中で結論を出せずにいた所有権論争に法的な重みを加えようとする試みと受け止められます。

BISIの報告書は、この4つの段階が実際の公共調達においてどのような割合で適用されるかについての試算も提示しました。公共技術導入事業全体のうち、約70パーセントに達する重要度の低い一般行政業務が第1段階に分類されます。20パーセントに達する中程度の重要度の業務は第2段階に分類されます。残りの10パーセントは第3段階と第4段階に分かれ、9パーセントが第3段階に、1パーセントが第4段階に割り当てられると同報告書は予測しています。この試算はまだ確定した統計ではなく、報告書の分析に基づく予測である点を明記しておく必要があります。ただし、この割合が示唆するところは明確です。

公共調達の大多数は依然として第1段階と第2段階にとどまり、完全な欧州所有を求める第3段階と第4段階は、全体事業の極めて一部にしか適用されないということです。

この段階的な設計は、まったく新しい発明ではありません。フランスはすでに独自の認証制度であるSecNumCloud（セクナムクラウド）を運用しており、国家最高レベルのセキュリティユースケースに対し、米国クラウド法の影響力を根本から遮断する最上位の認証を求めてきました。この認証はフランス国家情報システムセキュリティ庁（ANSSI）が管理しており、最上位等級の取得を目指すクラウド事業者はフランスまたは欧州連合の資本が支配的持分を保有することを求められます。BISI報告書は、CADAの4段階構造について、このフランス式認証制度の論理を欧州連合全体のレベルに拡張した設計であると評価しています。

フランスですでに導入されている制度が存在していたからこそ、CADAはまったく新しい実験ではなく、検証済みのモデルを拡張する提案であるという説明が成り立ちます。

フランスのSecNumCloudだけでなく、いくつかの加盟国はそれぞれの方法で独自の認証制度を発展させてきました。国ごとに基準が異なると、ある国で認証を取得したサプライヤーが、別の国の調達では最初から審査を受け直さなければならないという非効率が生じます。CADAが単一のSEAL体系によってこれらの基準を統一しようとする理由はここにあります。27の加盟国がそれぞれ異なる認証基準にこだわり続ければ、欧州全体をカバーする主権クラウド市場はそもそも成り立ち得ません。

承認手続きにおいても、段階ごとに厳格さが異なります。第1段階はサプライヤーによる自己証明のみで通過でき、中小企業向けには二重の書類審査を免除する簡易ルートが設けられます。一方、第2段階から第4段階までは、欧州連合が指定した独立した第三者監査機関がシステムの元となる設計図まで精密に検証したうえで、加盟国の専門捜査機関が最終承認を下す必

要があります。ある加盟国が行った承認決定は欧州連合の共通登録簿に掲載され、60日間にわたる他の加盟国からの異議申し立てが可能な相互検証期間を経ます。この期間内に異議が解消されない場合、欧州委員会が最終調整案を出して紛争を裁定する手続きが提案されています。

1つの国が下した判断を27の加盟国全体が改めて確認できるようにしたことは、どこか1つの国の甘い審査が連合全体のセキュリティ基準を低下させる抜け穴にならないよう防ぐための設計と考えられます。

認証は一度受ければ終わりではありません。サプライヤーの出資構造や取締役会の構成が変われば、当初通過したSEAL等級の前提自体が崩れる可能性があります。欧州企業として認証を受けた会社が後日、非欧州資本に買収された場合、その会社が遂行していた公共契約の地位はどうなるのかという疑問が残ります。BISI報告書は、CADAがこうした事後変更を監視し再審査する手続きまで含んでいると伝えていますが、その再審査がどのくらいの頻度で、どれほど迅速に行われるかはまだ具体化されていません。

この等級は誰が決めるのかという疑問も残ります。公共機関が新しい事業を調達に付す前に、まずその事業が扱うデータの機密性を自ら診断し、どのSEAL段階に該当するかを判定しなければなりません。一般行政文書を扱う事業であれば第1段階に分類されますが、同じ機関であっても治安や国防情報を扱う事業であれば第3段階や第4段階に分類されることがあります。この判定を誤ると、後になって問題が露呈します。低い段階に分類して契約を結んだものの、後から venture そのデータが国家安全保障に直結することが確認されれば、すでに結んだ契約を再び見直さざるを得ない状況に追い込まれます。

CADA案が判定手続きと監査体系を併せて規定しようとしている理由も、この誤分類のリスクを減らすためだと理解できます。

認証負担が必ずしも大企業にとってのみ軽いわけではありません。第2段階から求められるソフトウェア部品表（SBOM）の作成やソースコードの検証には、専任の人員と費用が必要です。資本力が大きくない欧州のスタートアップ・クラウド企業にとっては、この負担が市場参入そのものを阻む壁となり得ます。CADAが中小企業に第1段階の簡易ルートを開いたこととは別に、成長段階にある欧州企業が上位段階へステップアップできるよう助ける支援策が併せて用意されなければ、上位段階の市場は結局、すでに資本を備えた少数の大企業だけに開かれるという逆説が生じる可能性があります。

この4段階構造が実際に機能するためには、乗り越えるべき課題があります。欧州市場にはまだ第3段階と第4段階の要件を満たせるほどの域内企業の供給能力が十分ではないという点が、複数の業界報告書で共通して指摘されている問題です。欧州企業がこの上位段階の要件を満たすのに時間がかかる理由は、政治的意思の問題だけではありません。大規模なクラウドサービスを運用するには、サーバーハードウェアやネットワーク、冷却設備に巨額の初期投資

が必要であり、その投資を回収するには長期間にわたり安定した顧客層を確保しなければならないからです。

アメリカの大手クラウド企業は、すでに数十年にわたってこの投資と回収の循環構造を作り上げてきました。欧州企業がこの循環構造に短期間で追いつくためには、CADAが定めた等級基準だけでは不十分であり、その等級を満たす企業に対する別途の資本支援が並行して行われなければならないという指摘が出ています。要件をいくら精巧に設計しても、その要件をクリアできる企業が不足すれば、公共機関は結局、低い段階の調達へと後退するか、例外条項に依存することになります。CADAが定めた等級そのものよりも、その等級を満たす欧州企業の能力がどれほど早く成長するかが、この制度の実質的な成否を分ける変数として残っています。

根拠および参考文献

1. Martyna Chmura, 'EU Cloud and AI Development Act: Sovereignty, AI and US Tech Dependence', Bloomsbury Intelligence and Security Institute (BISI), 2026年7月7日.

2. U.S. Congress, Clarifying Lawful Overseas Use of Data Act, H.R. 4943, 2018, https://www.congress.gov/bill/115th-congress/house-bill/4943/text

3. European Commission, SWD(2026) 502 final, 欧州連合官報, 2026年6月3日, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52026SC0502

4. European Commission, 'Cloud and AI Development Act', Shaping Europe's digital future, 欧州連合官報, 2026年6月3日.

5. Kiteworks, 'Tech Sovereignty Package: an overview', Bird & Bird, 2026年6月23日.

6. Court of Justice of the European Union, Judgment in Case C-311/18 (Data Protection Commissioner v Facebook Ireland and Maximillian Schrems), 2020年7月16日.

4.3 「主権理由解約権（Sovereignty Termination Clause）」とポータビリティ義務の制度化

CADAがいかに精緻な等級を設計したとしても、すでに締結された契約をどのように終了させるかという問いに答えられなければ、その等級は新しく始まる事業にのみ適用される中途半端な制度にとどまってしまいます。イギリスの事例は、この問題を最も鮮明に示しています。

イギリスの国民保健サービス（NHS）は2023年、パランティア社と3億3,000万ポンド規模の契約を結び、統合データプラットフォーム（Federated Data Platform）を構築しました。このプラットフォームは、イギリス全土の病院における患者情報や病床状況、待機リストを一つの体系にまとめて分析するシステムです。イギリス下院科学技術委員会は、この契約が国家安全保障上受け入れがたい脆弱性であると警告する報告書を出しました。左派系メディアのノヴァラ・メディアは、複数の下院議員が政府に対しこの契約を終了するよう要求したと報じました。問題は、契約を終了させたくても簡単に終了させられないという点にありました。

下院科学技術委員会の報告書によると、NHSは契約期間中ずっと利用料を支払っていたにもかかわらず、システムの核心資産であるデータ標準モデル（Canonical Data Model）やオントロジーの知的財産権を譲り受けることができませんでした。契約が終了した瞬間にNHSの手元に残るのはデータではなく、パランティアのソフトウェアの上でしか作動しないように構築されたデータの残骸でした。この契約に盛り込まれた理由解約権条項が2027年2月になってようやく発効するという事実も、下院報告書を通じて確認されました。契約を本当に終了させたい瞬間と、実際に終了させることができる法的瞬間の間に数年の隔たりが存在していたことになります。

公共調達契約には、元々解約条項が存在します。契約違反があった際に解約する条項や、特別な理由なく違約金を支払って解約する任意解約条項が一般的に用いられています。CADAが新たに導入しようとしているのは、これら2つとは区別される第3のカテゴリーです。供給企業が契約を誠十分に履行していても、その供給企業の国籍や支配構造が国家安全保障上の脅威になると判断されれば、違約金なしで契約を終了できる根拠を別途設けるというものです。このような理由が法律上で明確に定義されなければ、逆に供給企業から「恣意的な解約だ」として訴訟を提起される余地も残ることになります。

この事例が浮き彫りにする問題は、パランティアという特定の企業に限られたものではありません。公共機関が特定のソフトウェアにデータを預け始めると、そのデータは次第にそのソフトウェア固有の構造内でのみ意味を持つように固定化されていきます。データを他のシステムへ移行する作業は、ファイルをコピーするだけで終わるものではありません。データが格納された分類体系や関係構造、すなわちオントロジー自体を再設計しなければならない場合

が多いのです。オントロジーとは、どのような情報同士がどのような関係を結んでいるかを定義した設計図のようなものと言えます。例えば、患者と病床、診療記録がどのように連結されているかを定めたルール体系がこれに該当します。

このルール体系を他社のシステムに合わせて再構築する作業には、新しい契約や開発人材、多大な予算が必要となります。契約初期には安価に見えた調達が、移行時点では最初の契約以上の大きな費用を要求されるという逆説がここで生じます。このような構造的な拘束効果を、業界では一般にベンダーロックイン（vendor lock-in）と呼びます。

NHS事例が示したロックイン効果は、従来的なデータベースに限定されるものではありません。AI時代の調達では、データだけでなく、そのデータで学習させたモデル、モデルを調整した設定値、検索に使用される埋め込みまでが移行の対象に含まれます。ベンダーがこのような要素を独占的形式で保存すれば、契約終了後に公共機関に残されるのは空っぽのインフラだけであり、その上に築き上げられた知能はそっくりベンダーの手に留まります。CADAのポータビリティー義務が実質的効果を発揮するには、このようなAI特有の資産までを移行の対象に含める詳細規定が必要であるという指摘があります。

ポータビリティを技術的に保証する最も一般的な方法は、オープン標準の採用を義務付けることです。データを特定企業しか読み取れない独占形式ではなく、複数のシステムが共通して読み書きできるオープン形式で保存するよう契約書に明記しておけば、契約終了後もデータを他のシステムへ移行する作業が比較的容易になります。ただし、オープン標準を採用したからといって、オントロジーのようにそのシステムに特化した設計まで自動的に移行されるわけではありません。データの容器をオープン形式に変えることと、その容器の中に収められた知識構造を移行することは、それぞれ別の課題として残ります。

ポータビリティという概念が欧州連合（EU）の法律内にまったく存在しなかったわけではありません。2023年に採択された欧州連合データ法（Data Act、Regulation (EU) 2023/2854）は、クラウドとエッジコンピューティングサービス間の移行を扱う条項をすでに備えています。この法律は、クラウド利用者が一つのサービス供給事業者から別の事業者へ移行する際に課されるスイッチング手数料を段階的に引き下げ、定められた期限以降はこうした手数料自体を撤廃するよう定めています。CADAとは異なり、データ法はすでに発効した法律であるという点に違いがあります。

CADAがこのデータ法のポータビリティー原則を公共調達というはるかに敏感な領域、そして主権というはるかに重い基準に拡張しようとする試みであると理解すれば、両法の関係が明確になります。データ法が一般的な商用クラウド利用者をベンダーロックインから守ろうとしたのに対して、CADAはその保護膜を国家機関と公共サービスにまで広げようとしているのです。

CADAの提案が扱おうとしている部分が、まさにこの点です。欧州委員会が明らかにした政策目標の一つは、公共機関が主権上の理由で契約を解約する権利を持ち、供給事業者は契約終了時にデータや設定値をオープンで相互運用可能な形式で移行する義務を負うというものです。BISI報告書は、CADAの三つの柱の一つがこのポータビリティ義務の制度化であり、その趣旨は公共機関が特定の供給事業者に縛られて交渉力を失う状況を防ぐ点にあるとまとめています。この条項が実際にどのような名称と条文番号で最終規定に盛り込まれるかは、欧州議会と理事会の審議を経て確定することになります。

現時点で確認できるのは、欧州委員会がこのような方向性の条項を提案書に盛り込んだという事実であり、すでに施行されている規範が存在するという事実ではありません。

提案が言及する移行支援期間が具体的にどのような形になるかはまだ定まっていませんが、類似の制度をすでに施行している他の産業の事例から推測することができます。通信サービスの利用者が番号を維持したまま通信事業者を変更するナンバーポータビリティ制度や、銀行口座を変更する際に口座振替の設定までまとめて移行する口座振替移行制度などがその例です。公共機関のデータポータビリティにもこうした発想を適用するなら、旧供給事業者と新供給事業者が一定期間システムを並行運用しながら、データと業務を段階的に引き継ぐ手順が求められることになると見られます。

この制度が成立するには、二つのことが揃っていなければなりません。一つは法律上、解約権を明示することであり、もう一つはその解約権を実際に行使できるよう技術的なポータビリティーを確保することです。法律条項があるだけで、データ形式が依然として閉鎖的であれば、公共機関は契約を終了する権利は持ちながらも、その権利を行使する方法がありません。逆に、技術的にはデータを移動できても、契約書に違約金条項が付いていれば、公共機関は目前の費用のために古いシステムに留まり続けることになります。NHS事例は、この二つの条件のいずれも満たされなかった場合に何が起きるかを示す失敗の記録です。

CADAが実際に施行されたとしても、既に締結されている契約に遡及適用されるかどうかは別の問題として残ります。一般的に、EUの新規制は施行日以降に新たに締結される契約に優先適用され、既存の契約には猶予期間または別途の経過規定が付随することが多いです。CADA提案が最終的に確定する過程で、既存の契約に対する経過規定をどのようにするかが、加盟国間の交渉争点となる可能性が大きいです。既に数年にわたって特定のベンダーにデータを預けてきた公共機関の立場からすれば、新規制が遡及適用されないのであれば、ポータビリティー義務の効果を実感するまでに長い時間がかかるかもしれません。

契約を最初に結ぶ時点では、このような費用は目立ちません。調達担当者は通常、初期導入費用と年間使用料を基準にベンダーを比較し、契約終了後にデータを抽出するのにかかる費用まで事前に計算に入れることはそう多くありません。この非対称性はベンダーにもある種のインセンティブを生み出します。初期価格を低く提示して契約を獲得した後、切り替え費用

を引き上げて顧客を囲い込む戦略がクラウド業界では珍しくなく観察されているという問題は、複数の市場分析で指摘されてきたものです。CADAのポータビリティー義務は、このインセンティブ構造そのものを契約前段階から変えようとする試みと見ることができます。

この問題は、大国よりも小国において、より深刻に現れます。人口が多く財政的に余裕のある加盟国は、契約を検討する専任の法務チームと技術チームを別途組織する余力があります。いっぽう、規模の小さい加盟国の地方政府や小規模な公共機関では、契約書を検討する専門人材すら十分でないケースがめずらしくありません。プロバイダーが提示する標準契約書をそのまま受け入れるほうが、交渉に追われるよりも当面は楽だからです。この非対称性が積み重なると、主権理由解約権が法典に存在しても、その権利を実際に行使する能力を持つ機関とそうでない機関との間に格差が生じます。

CADA提案が中小企業のベンダーに簡易承認経路を開いたのと同じような論理で、契約を締結する公共機関の側にも標準化されたポータビリティー要件と契約書の雛形を事前に用意することが、交渉力の格差を縮める方法であるという指摘があります。

切り替え費用の問題は契約終了後も続きます。データを移動する作業とは別に、そのデータを扱っていた担当者が新しいシステムを習得するのにも時間と予算がかかります。公共機関の予算サイクルは通常一年単位で設定されているため、数年にわたって分散して発生する切り替え費用を一度に確保することが難しい場合が多いです。このため、たとえ解約権が法的に存在していても、予算部署が切り替え費用を負担できず、実質的に契約を延長している事例が複数の国から報告されてきました。CADA提案がポータビリティー義務とともに転換支援期間を規定しようとしているのも、このような現実的な障壁を念頭に置いた設計と見えます。

解約権とポータビリティー義務を法で明示することにはもう一つの法的緊張が伴います。EUの公共調達指令(Directive 2014/24/EU)とEUが加盟している世界貿易機関政府調達協定は、原則として適格を備えた外国の供給者を調達プロセスにおいて不当に差別してはならないと規定しています。国家安全保障と防衛を理由とした例外はEU機能条約第346条に根拠がありますが、この例外は原則として例外として設計されており、原則そのものとしては設計されていません。

CADAがSEALの上位段階において事実上非欧州企業を調達から排除する効果を生むとすれば、その排除が安全保障上の例外の正当な範囲内にあるかをめぐる法的争いが続く可能性があります。この緊張は、CADAが欧州議会と理事会の審議を経る間、条文の表現一つひとつをめぐって引き続き議論される懸案として残っています。

この問題の重みを推し量らせる、もう一つの数字があります。パランティア（Palantir）は2026年第2四半期の業績発表において、前年同期比93%という売上高成長率を記録したと明らかにしました。欧州各国が自国の治安および国防分野からパランティアと距離を置くと宣言する間にも、欧州の投資銀行や資産運用会社はパランティア株式の買い入れに数十億ユーロを投

入してきたと、ドイツのメディア「ネッツポリテイク（netzpolitik.org）」は報じました。公共調達の門からは押し出しながら、金融市場の窓からは資本を招き入れるというこの矛盾は、法律の条項ひとつで解決されるものではありません。

ポータビリティー義務が方向性を持たないツールであることも忘れてはなりません。データを簡単に移動できるようにする規制は、ヨーロッパの企業への移行経路を開くだけでなく、別のアメリカ企業への移行経路も同時に開きます。解約権とポータビリティー義務自体は、特定の国籍の企業を優遇する仕組みではなく、公共機関の交渉力を全般的に高める仕組みに近いです。その交渉力が実際にヨーロッパ企業を選択する結果につながるには、結局のところSEAL体系が規定する国籍と支配構造の要件が共に機能する必要があります。

主権を守るという宣言と、その宣言を支える欧州産代替ソフトウェアの実際の供給能力の間には、なお隔たりが残っています。CADAの解約権とポータビリティー義務は、この隔たりを埋めるための制度的第一歩です。その第一歩が実際の調達現場で機能するかどうかは、欧州議会の審議結果とその後の施行過程で明らかになるでしょう。

根拠および参考文献

1. 英国下院科学技術委員会, 'MPs warn that Palantir's increasing presence in the UK public sector is an "unacceptable point of weakness"', House of Commons, 2026年.

2. Novara Media, 'MPs Tell Government to End £330m NHS Contract With Palantir', Novara Media, 2026年.

3. Martyna Chmura, 'EU Cloud and AI Development Act: Sovereignty, AI and US Tech Dependence', Bloomsbury Intelligence and Security Institute (BISI), 2026年7月7日.

4. Palantir Investor Relations, 'Palantir Reports Q2 2026 U.S. Comm Revenue Growth of 149% Y/Y and Revenue Growth of 93% Y/Y', Palantir Technologies, 2026年.

5. Jan Ebert, 'Banken und Vermögensverwalter: Milliardeninvestitionen aus Europa fließen in Palantir', netzpolitik.org, 2026年.

6. European Union, Regulation (EU) 2023/2854 (Data Act), Official Journal of the European Union, 2023年.

5.1 フランチェスカ・ブリアの「ユーロスタック（EuroStack）」構想と3,000億ユーロの投資の壁

フランチェスカ・ブリア氏はイタリア出身の経済学者で、欧州委員会のアドバイザーとして活動してきました。彼女はバルセロナ市役所でデジタルイノベーション委員を務め、市民が作成したデータを民間企業ではなく市自らが管理させる政策を主導した経歴を持っています。この経歴は、彼女が後に欧州規模のデジタル政策を設計する際、繰り返し引用する準拠点となります。ブリア氏は数々の発言や執筆において、公共インフラをアメリカの民間技術企業に委ねる潮流が民主主義の基盤を揺るがしかねないという懸念を表明してきました。

本書の前の各章で扱った出来事、すなわちフランスDGSIのパランティア離脱やアンソロピックのアクセス遮断事件は、この懸念が抽象的な心配にとどまらないことを示す具体的な事例と見なすことができます。ブリア氏がユーロスタックを設計する中で繰り返し強調する点も、契約書の条項ではなくインフラ自体を所有し統制する主体が誰なのかという問いです。

調査報道メディア「フォロー・ザ・マネー（Follow the Money）」が報じたところによると、ブリア氏は「権威主義スタック（The Authoritarian Stack）」という別の研究を通じて、欧州の投資銀行や資産運用会社がパランティアのようなアメリカ企業に大規模な資本を提供する潮流を指摘しました。欧州の年金基金や銀行が自国の公共インフラを侵食する企業にむしろ資金を提供する矛盾を指摘したのです。この指摘は、本節の後半で扱う欧州内部の投資資本の潮流問題とつながっています。

この懸念を具体的な設計図に移した成果物がユーロスタック報告書です。正式タイトルは『EuroStack – A European Alternative for Digital Sovereignty』で、ブリア氏、パウル・ティマース氏、ファウスト・ゲルノーネ氏が共同執筆しました。ドイツの民間財団ベルテルスマン財団（Bertelsmann Stiftung）が2025年2月13日にこの報告書を公表しました。ベルテルスマン財団は、ドイツの大手メディアグループであるベルテルスマンが設立した非営利財団で、長年にわたり欧州の社会・経済政策の研究を支援してきました。

この財団がユーロスタック報告書を刊行したということは、同報告書が欧州連合の公式文書ではなく、政策研究財団が支援した独立した提案書であることを意味します。まずこの事実を押さえておく必要があります。ユーロスタックは欧州連合が採択した法律や政策ではありません。民間財団が発行した政策提案書であり、著者たちが欧州連合や加盟国政府に対し、このような方向に進むよう促す文書です。本章で扱う数値や設計はすべてこの提案書に盛り込まれた内容であり、実際に執行されている予算や既に制定された規範とは区別して読む必要があります。

第4章で扱ったクラウド・AI開発法（CADA）とこの報告書は、互いに異なる次元にあります。CADAは欧州委員会が欧州議会および理事会に提出した規則案であり、正式な立法手続きを踏んでいます。ユーロスタックはその手続きの外にある民間財団の政策報告書です。CADAがデータセンターを欧州内に建設する問題やその運営企業の国籍を選別する問題を扱うのに対し、ユーロスタックはそれよりもはるかに広い範囲である半導体から人工知能までの7つの階層全体を自立化させようという構想です。

両文書は欧州の技術的自立という同じ目標を共有していますが、一方は立法手続きを踏む規則案であり、他方はその手続きの外で方向性を提示する政策提案書であるという点で、法的重みが異なります。

ブリア氏はユーロスタック構想を説明する際、欧州の単一通貨であるユーロの導入になぞらえる表現を使ってきました。加盟国ごとに異なる通貨を使っていた時代、欧州が通貨の壁を取り払い共通の金融秩序を打ち立てたように、デジタルインフラ領域においても加盟国別に分散した能力を一つに集めなければならないというのが、この比喩の趣旨です。ユーロが導入されるまでに長年にわたる交渉と条約改定が必要であったことを思い起こせば、この比喩はユーロスタックが目標とする統合の規模の大きさを強調する意図として読み取ることができます。

報告書はヨーロッパのデジタル基盤を7つの層に分けています。最下層には、半導体とバッテリーを製造するために必要な原材料、およびデータセンターを運行するために必要なエネルギーと水が置かれています。その上には、半導体チップを製造する層、広帯域通信網を敷設する層、センサーおよびIoTデバイスを製造する層、クラウドインフラストラクチャを運用する層が順次積み重ねられています。最上層には、ソフトウェア層とデータ・人工知能層が位置しています。報告書は、これら7つの層のいずれか1つであっても、ヨーロッパ以外の企業に保有されていれば、その上に積み重ねられた残りの層の自立は完全にはあり得ないと主張しています。

半導体を自国で製造したとしても、その半導体が組み込まれたサーバーをアメリカ企業が所有するデータセンターでのみ稼働させているのであれば、自立は半分にとどまるという論理です。

この7層構造は、家を建てる手順になぞらえると理解しやすくなります。いくら頑丈な資材で壁を立てたとしても、その上に載せる屋根を他人の設計図通りに購入しなければならないのであれば、家全体の安全は屋根を売る者の手に委ねられることになります。ユーロスタック報告書が説く自立も同様です。半導体や通信網、クラウドまでは欧州企業が作っていたとしても、その上で動作する人工知能モデルやデータ管理ソフトウェアをアメリカ企業の製品に依存しているのであれば、下の6つの階層で成し遂げた成果も最上階のたった一つのせいで揺らぎかねない、というのが報告書の論旨です。

報告書は、これら7つの層を組み合わせて市民に直接提供する5つの共同サービスもあわせて提案しています。欧州域内で演算を処理する主権クラウドサービス、市民の身元を確認するデジタル身分証ウォレット、銀行手数料なしで決済できるデジタルユーロ決済システム、加盟国間でデータを安全にやり取りする連合データスペース、そして欧州が直接設計・運営する人工知能エンジンです。5つはいずれも、現在は米国やその他の域外企業のサービスに依存している領域であり、報告書は、この依存を払拭することがユーロスタック構想の実質的な目標であると説明しています。

5つのサービスのうち、市民の日常に最も近いものはデジタルユーロ決済システムです。現在、欧州でカード決済を行うと、その取引情報は概ねアメリカ系のカード会社の決済ネットワークを経由します。店舗がカード決済を受け入れるたびに支払う手数料のうち相当部分が、この決済ネットワークを所有する会社へ流れ込んでいます。報告書が提案するデジタルユーロシステムは、この決済ネットワーク自体を欧州中央銀行の体系内に置き、取引情報が域外へ流出しないようにし、手数料構造も変えようとする構想です。デジタル身分証ウォレットも同様の問題意識から生まれました。

市民がオンラインで身元を証明する際、特定のビッグテックのログインシステムを経由する現在の慣行に代わり、国家が直接管理する身元確認手段を備えようというものです。これら5つのサービスのうち、デジタル身分証ウォレットだけはユーロスタック報告書が初めて提案した概念ではないという点も付言しておく価値があります。欧州連合は既に2024年、欧州デジタル身元規則、いわゆるeIDAS 2.0を採択し、加盟国が市民にEUデジタル身元ウォレットを提供するよう義務付けました。この規則はユーロスタック報告書とは別個に、既に制定されて施行されている法律です。

ユーロスタック報告書は、この既存の制度を廃止して新しく作ろうというものではなく、既に進行中のこの流れを7つの層構造の中に含め、他の層と有機的に連結しようと提案する側に近いです。残り3つのサービスは、政府や企業が向き合う階層に近いです。主権クラウドサービスは、第4章で扱ったCADAの主権保証レベル体系と目指す方向性が重なります。

アマゾン・ウェブ・サービスやマイクロソフトが欧州の顧客をターゲットに出したいわゆる主権型クラウド製品が、第4章で確認したように支配株まで欧州に譲渡するわけではないという限界を抱えていたのとは異なり、ユーロスタックが言う主権クラウドサービスは、所有権そのものが欧州にあるクラウドを指します。連合データスペースは、加盟国の政府や企業がデータをやり取りする際に米国のクラウドを経由しないようにする経路です。この構想は、第4章で扱ったCADAに先立ち、2019年にフランスとドイツが開始したガイアX（Gaia-X）プロジェクトとも脈を通じさせています。

ガイアXが法的拘束力のない自主的な標準化の試みにとどまったという評価を受けたのとは異なり、ユーロスタック報告書はこのデータ共有体系を国家予算が裏付ける共同インフラへと

格上げしようと提案しています。ソブリン人工知能エンジンは、現在欧州の公共機関や企業が米国やその他の域外企業が開発した大規模言語モデルに依存している状況を変えようとする目標を盛り込んでいます。

報告書が提示する投資規模は小さくありません。著者らはこの7つの層のインフラを新設するのに概ね10年がかかると試算し、2035年までに計3,000億ユーロに達する資金が必要だと明らかにしました。これに加え、初期の呼び水となる100億ユーロ規模の別途の技術基金を新設しようという提案も盛り込みました。3,000億ユーロを10年で割ると、年間平均300億ユーロ規模の投資が継続的に行われなければならないという意味です。この数値は報告書の著者らによる計算であり、欧州連合が公式に採択したり配分したりした予算ではありません。

この金額を欧州連合が実際に運用している予算と並べてみると、その隔たりが浮き彫りになります。政策研究機関CERREが2025年9月に発表した報告書は、欧州連合が推進する競争力基金の中でデジタル主権関連項目に割り当てられた予算が550億ユーロ規模にとどまると明らかにしました。ユーロスタック報告書が要求する3,000億ユーロと比較すると、5分の1にも満たない規模です。競争力基金は、欧州連合が2028年から始まる次期多年度予算枠組みの中でデジタルと産業の競争力強化のために編成しようとしている予算項目であり、まだ加盟国と欧州議会の最終承認を残しています。

この予算自体も確定した金額ではないという意味であり、その中でもデジタル主権に割り当てられた分はユーロスタックが要求する金額を大幅に下回っています。この比較が意味するところは明白です。ユーロスタックは方向性を提示する設計図であり、その設計図を完成させる予算がすでに確保されたという意味ではありません。

ブリア氏をはじめとする欧州の政策論議の参加者たちは、この資金ギャップを埋める源泉として政府予算ではなく民間の貯蓄を挙げます。メディア「EUパースペクティブス（EU Perspectives）」が2026年1月に報じたところによると、欧州連合の家計が銀行口座に預けている預金総額は2026年時点で30兆ユーロを上回ります。世界経済フォーラムが2026年1月の年次総会で行った討論で言及された数値では、この金額が欧州連合全体の国内総生産の2倍を超えます。問題は、この資金が動かない点にあります。

「ポリティコ（Politico）」欧州版が2026年6月4日に取り上げた討論で言及された内容によると、スウェーデンのように市民の半数以上が株式やファンドに資金を投じている国がある一方で、欧州の多くの大型加盟国ではその割合が2パーセント前後に留まっています。銀行に眠る資金はスタートアップへと流入せず、実際に投資に向かう資金の相当部分は米国の大手ハイテク株に向かうと、この討論は指摘しました。

年金基金も同様の問題を抱えています。フランス24が2026年6月に放送した討論で指摘された内容によると、欧州の年金基金は安定性を優先する監督規制に縛られており、成長初期段階の技術企業に資金を供給することが困難です。欧州連合の保険・年金監督体系であるソルベン

シーII（Solvency II）のような規制は、年金基金が予期せぬ損失を被らないよう安全資産の比率を一定水準以上に維持させます。

この規制の趣旨は退職者の老後資金を守ることにありますが、結果として成長初期段階の技術企業のようにリスクが大きく収益も不確実な資産へ年金資金が流入する道を狭める効果ももたらしています。この資金の目詰まりは人材流出にもつながります。資金を調達できなかった欧州の技術人材が米国シリコンバレーへ移動する流れが同討論で言及されました。欧州委員会がCADA提案とともに発表した付属実務文書SWD(2026) 502 finalは、この資金ギャップを数値としても示しています。

世界のベンチャーキャピタル投資額のうち欧州が占める割合は5パーセントにとどまる一方、米国は52パーセントを占めています。ブリア氏は2024年のCEPSでの講演で、欧州で誕生した成功したスタートアップのうち相当数が事業を拡大する段階に至って外国資本に買収され、欧州域外へ流出していると指摘しました。

このような診断に基づき、ブリア氏は銀行預金や年金資産が欧州の技術企業へと流れるよう誘導する税制改革を求めてきました。預金を長期間寝かせておく代わりに域内の技術企業に投資する市民に対して減税を行ったり、年金基金がリスク資産に投資できる上限を拡大したりする方法が取り沙汰されています。こうした提案が実際に立法へとつながったかどうかは、本書が確認した資料の範囲内ではまだ確定していません。ユーロスタック報告書が要求する3,000億ユーロのうち相当部分を政府予算ではなく民間資本で賄おうとするならば、このような税制改革が先行されなければならないというのが報告書の論理です。

資金が全く動いていないわけではありません。フランス語圏の経済メディア「エコー・クイック（ÉcoQuick）」が2026年6月4日に報じたところによると、欧州連合は人工知能ギガファクトリーの建設に200億ユーロ規模の公的資金を投入する計画を確定しました。スペイン首相府は2026年7月1日の発表で、自国の人工知能ギガファクトリー建設に7億2,000万ユーロの公的予算を投入する協定を承認したと明らかにしました。スウェーデン系の資産運用会社EQTが運用を担う50億ユーロ規模のスケールアップ・ヨーロッパ・ファンドも2026年秋から資金執行を開始する予定であると、メディア「スタートアップ・オンライン」が2026年5月21日に伝えました。

このファンドは、ドイツ復興金融公庫（KfW）が組成した10億ユーロ規模のディープテックファンドとともに動きます。

これらの実際の執行金額をすべて合わせても、200億に7億2,000万、50億を足して300億ユーロに届きません。ユーロスタック報告書が要求した3,000億ユーロの10分の1にとどまる水準です。欧州連合と一部の加盟国が実際に財布を開いたのは事実ですが、その規模はブリア氏が提示した設計図を埋めるにはまだ程遠い状況です。

これらの数字を並べてみると、問題の性質がより明確になります。欧州連合（EU）の家計が銀行に預けている預金は30兆ユーロを上回り、ユーロスタック報告書が求める投資額は3,000億ユーロです。算術的にのみ見れば、この預金の1パーセントだけでも技術投資に回れば、報告書が求める金額全体を満たせるという意味です。問題は、この1パーセントを動かすインセンティブと制度がまだ整っていない点にあります。資金がないからではなく、その資金を貯蓄から投資へと移動させる税制や金融商品、信頼が不足していることこそが、この格差の本質に近いと言えます。

この格差が縮まらなければ、ユーロスタックが描く7つの層のうち相当数は、設計図の段階にとどまるしかありません。半導体やデータセンターのように莫大な初期投資を必要とする層ほど、この資金不足の影響を真っ先に受けます。加盟国ごとに予算を分けて編成する現在の方式では、3,000億ユーロ規模の事業を負担しきれないという指摘が出る理由であり、ブリア氏が民間貯蓄や年金資産まで引き入れようとしているのもこのためです。

欧州連合が2028年から始まる次期予算交渉でデジタル主権予算をどれほど増やせるかが、ユーロスタック構想が設計図から実際の事業へと移行できるかを占う次の試金石になるとみられます。その交渉の結果が出るまで、ユーロスタックは欧州が進もうとする方向を指し示す地図であり、すでに完成した建物ではありません。

根拠および参考文献

1. Francesca Bria, Paul Timmers, Fausto Gernone, 'EuroStack – A European Alternative for Digital Sovereignty', Bertelsmann Stiftung, 2025年2月13日, https://www.bertelsmann-stiftung.de/en/publications/publication/did/eurostack-a-european-alternative-for-digital-sovereignty

2. Johanna Bröer他, 'Can the EU Reconcile Digital Sovereignty and Economic Competitiveness?', CERRE Issue Paper, 2025年9月, 17頁.

3. Joana Soares, 'Your cloud data lives on American servers. Brussels is moving to act', EU Perspectives, 2026年1月.

4. World Economic Forum, 'Is Europe's Tech Sovereignty Feasible?', WEF Annual Meeting 2026, 2026年1月.

5. POLITICO Europe, 'Achieving digital sovereignty: A golden opportunity for the EU?', POLITICO Europe, 2026年6月4日, https://www.politico.eu/video/achieving-digital-sovereignty-a-golden-opportunity-for-the-eu-politico/

6. FRANCE 24 English, 'Can Europe own its digital destiny? EU unveils tech sovereignty roadmap', FRANCE 24, 2026年6月.

7. European Commission, SWD(2026) 502 final, 欧州連合官報, 2026年6月3日, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52026SC0502

8. Francesca Bria, 'EuroStack: a concrete pathway to European digital sovereignty and strategic autonomy', CEPS Think Tank, 2024年.

9. ロイック・クラフト, 'Souveraineté numérique : Bruxelles renâcle à imposer des contraintes trop fortes', エコー・クイック, 2026年6月4日.

10. スペイン首相府, 'The President calls for public-private partnership to drive forward Spain's artificial intelligence gigafactory', La Moncloa, 2026年7月1日.

11. Startup Online 編集部, '欧州デジタル主権のための演算力・クラウド・オープンソース・資本に関する研究報道', Startup Online, 2026年5月21日.

5.2 代替ソフトウェア同盟：アルカディア（Arcadia）とオープンソース・デジタル公共財

指揮統制システム、一般にC2と略されるソフトウェアは、戦場で起きている出来事を画面に集約して表示し、指揮官の命令を部隊に伝達するためのツールです。どの部隊がどこにいるのか、どのような目標が発見されたのか、どの部隊にどんな命令が下されたのかをリアルタイムで整理して示します。第3章で取り上げたメイブン・スマート・システムがNATO同盟レベルでこの役割を担っているとすれば、アルカディアはフランスが同じ役割を自国製ソフトウェアで代替しようとする試みです。

フランスは、パランティアのメイブン・スマート・システムに代わる自国主導の軍事用人工知能指揮統制体系を開発しています。名称はアルカディアです。防衛メディア「アルメ・ドットコム」と「エコノミー・マタン」が2026年7月9日に共同で報じたところによれば、アルカディアはタレス、エアバス、サフラン、そしてフランスの大規模言語モデル開発会社ミストラルAIがコンソーシアムを結成して開発している戦場指揮ソフトウェアです。ここにはコマンドAIやインパクトといった戦術ソフトウェアのスタートアップ企業も参画しています。

ミストラルAIは2023年にパリで設立された大規模言語モデルの開発会社で、欧州発の人工知能企業の中で最も先頭に立っているとの評価を受けています。同社が軍事用コンソーシアムに参加したという事実は、欧州の民間人工知能産業が国防領域とも結合していることを示しています。

アルカディアは何も無いゼロから出発した事業ではありません。同報道によれば、フランスは以前にもタレスとソプラ・ステリアが共同で進めた戦闘指揮所システム「SIA C2」を長年にわたり推進したものの、技術的不適合の問題で事業が中止された経験があります。アルカディア・コンソーシアムはこの失敗を教訓とし、システムを最初からモジュール式で設計しました。オープン型インターフェース（API）を適用して複数企業が制作したソフトウェアコンポーネントが相互に結合できるようにし、同盟軍間の無線通信を支援するNATOの連合ミッションネットワーク（FMN）標準も満たしました。

FMNはNATO加盟国の異なる指揮統制システムが連合作戦において情報をやり取りできるよう定められた共通規格です。ある国の部隊が自国のシステムで確認した目標情報を、FMN標準に従う他国のシステムでも同じ形式で読み取れるようにすることが本標準の目的です。アルカディアがこの標準を満たしたということは、フランスが独自のソフトウェアを使用しながらも同盟軍との情報共有能力を放棄しなかったことを意味します。国家の独自設計権と同盟軍との相互運用性を同時に満足させようとする設計です。

モジュール式設計とは、大きな完成品をまるごと購入する代わりに、標準化されたパーツを複数の会社から購入して組み立てる方式です。いずれか一つのパーツを製造した企業が廃業したり契約を打ち切ったりしても、同じ規格に適合する他社のパーツに交換すれば、システム全体は稼働し続けます。以前のSIA C2事業が特定ベンダーの閉鎖的な設計に足を引っ張られたのとは対照的に、アルカディアはこのモジュール構造によって、特定企業1社の都合にシステム全体が左右されるリスクを減らそうとしています。

CWIXは連合軍相互運用性演習を意味するNATOの定例行事で、加盟国が開発した兵器体系や通信機器が実際に相互連動するかを毎年点検する場です。新たに開発された指揮統制ソフトウェアが同盟軍の他の装備と実際に通信できるかをこの演習で試験することが慣例となっています。アルカディアは2026年6月にポーランドのビドゴシチで開催された同演習において、初めて試験運用されました。防衛専門メディア「ディフェンスニュース」が2026年6月5日に報じたところによれば、この演習はアルカディアが実戦環境でデータを処理する能力を検証する場でした。

完成したシステムを実戦に全面配備したのではなく、開発中のシステムをNATO標準のもとで試験した段階であるという意味です。同報道によると、フランス陸軍副参謀総長のパトリック・ジュステル将軍はこの演習において、検証なしに外国のソフトウェアを受け入れる姿勢は国家主権を自ら明け渡す行為であると述べ、アルカディアがアメリカの軍事技術の優位に対するフランスの応答であると説明しました。

アルカディアとメイヴンの開発方式には、明確な違いがあります。パランティアは「メイヴン・スマート・システム」を自社が所有するソフトウェアとして開発し、NATOに供給する単一サプライヤー方式を採用しました。アルカディアは逆に、タレス、エアバス、サフラン、ミストラルAI、そして複数のスタートアップがそれぞれの専門領域をモジュール形式で作り結合するコンソーシアム方式を採用しました。特定の1社がシステム全体を左右できないようにするための設計です。この方式は開発スピードを遅らせる可能性があるというデメリットもありますが、特定の1社に安全保障インフラ全体を依存するリスクを減らせるというメリットもあります。

この流れはフランスにとどまりません。メディア「The Next Web」が2026年7月18日に報じたところによると、フランスとドイツの政府は、パランティアの軍事用人工知能ソフトウェアに対抗する欧州レベルの競合体制を共同で構築することを誓約しました。この誓約が具体的な共同開発計画につながったのか、それとも各国がアルカディアのように独自の事業を推進し続けるにとどまったのかは、本書が確認した資料からは明らかではありません。コンサルティング会社のパスファウンダーズ・グループが2026年4月にまとめたリストによると、欧州内でパランティアの代替案として挙げられている企業は、アルカディア・コンソーシアムの参加企業以外にも複数存在します。

単一の勝者が決まるのではなく、複数の企業がそれぞれの領域で競争する構図が形成されつつあることを意味しています。

アルカディアはこれまでのところフランスが主導する事業であり、コンソーシアムに参加している企業も大半がフランス企業です。CWIX演習はNATO加盟国が共に参加する多国間イベントでしたが、アルカディア自体がNATO全体の公式標準として採択されたわけではありません。フランス以外の加盟国がこのシステムを実際に導入するか、あるいは各国がそれぞれ自国で開発した別個のシステムを使用するかは、本書が確認した資料の範囲内ではまだ決まっていません。仮に欧州各国が異なる指揮統制システムを個別に開発した場合、今度は欧州諸国間における相互運用性が新たな課題として浮上する可能性があります。

このコンソーシアムにおいてサフランが担う役割は、別途注目に値します。フランスの経済メディア「レサンシエル・ドゥ・レコー」が2026年6月8日に報じたところによると、航空機エンジンメーカーとして出発したサフランは、2022年から情報分析関連企業を相次いで買収しました。2022年7月にはジャミング（電波妨害）環境下でも正確な位置信号を提供するオロリアを1億100万ドルで買収し、2024年には衛星画像分析企業のプレリジョンを2億2,000万ユーロで吸収して「サフラン.AI」部門を新設しました。2026年2月には地下空間向け抗ジャミング技術を持つシントニーを、2026年5月にはレーダー画像分析企業ケイロスの国防部門を追加で買収しました。

同報道によれば、サフラン.AI部門は300人のエンジニアを擁しており、2025年の売上高は前年比で65パーセント増加し、2026年には90パーセントの成長を見込んでいるとのことです。同部門が開発した標的認識エンジン「ACE」は、シンガポール、カナダ、インドのパートナーと共同開発協定を結ぶ際にも活用されていると、同メディアは伝えました。この協力国の顔ぶれが意味する点も注目に値します。シンガポールとインドは、米国が主導する情報共有同盟「ファイブ・アイズ」には加盟していませんが、西側諸国と安全保障協力を結んできた国々です。

サフランがこうした国々とも手を組むのは、米国中心の情報同盟の外側で独自の情報協力網を広げようとする試みと読み取ることができます。航空機エンジンを製造していた企業がここ数年の間に情報分析企業を相次いで買い取り、人工知能企業へと変貌を遂げたこの事例は、欧州の防衛大手企業がソフトウェアやデータの能力を自社開発する代わりに買収を通じて迅速に確保する流れを示す事例でもあります。

軍事領域の外では、オープンソース・ソフトウェアを中心とした動きが進んでいます。欧州委員会が2026年6月3日に発行した官報文書「COM(2026) 503 final」は、EU加盟国が米国系ソフトウェアのサブスクリプション料金として支払っている費用が年間2,640億ユーロに達すると試算しました。同文書は、この費用を削減するために公共予算で作られたソフトウェアのソ

ースコードを市民に無償で公開しようという原則、いわゆる「公共予算・公共コード」原則を盛り込んだオープンソース戦略を提示しました。

この費用が繰り返し発生する理由は、ソフトウェア産業特有のロックイン効果にあります。ある行政機関が特定企業のオフィス用ソフトウェアで文書を作成・保存し始めると、数年後に他社の製品へ移行しようとしても、文書形式や業務手順がすでにその企業の方式に合わされているため、移行コストが雪だるま式に膨れ上がります。毎年支払うサブスクリプション料金よりもこの移行コストの負担の方が大きいため、行政機関は契約を更新する道を選ぶことになります。オープンソース戦略が狙いを定めているのは、このロックイン構造そのものです。

ソースコードを公開し、複数の企業が同じコード基盤の上で競争するようにすれば、特定のベンダーに縛られる状況を防ぐことができるという論理です。

この原則に従い、フランス、ドイツ、イタリア、オランダ政府は2025年10月、「デジタル・コモンズEDIC」という名称の欧州デジタル・インフラストラクチャー・コンソーシアムを結成しました。EDICは欧州デジタル・インフラストラクチャー・コンソーシアムの略称で、複数の加盟国が共同事業を展開する際に用いる法的組織形態です。各政府が個別に契約を結ぶ代わりに、この単一の組織が参加国を代表して予算を集め、事業を管理します。このコンソーシアムの中心には、ドイツ連邦内務省がMicrosoft 365の代替として開発を承認したオフィス協調作業ソフトウェア「openDesk（オープンデスク）」があります。

openDeskは、ファイル保存ツールのNextcloud、メールサーバーのOpen-Xchange、コンテンツ管理ツールのDrupal、分散型メッセンジャーのMatrixを一つにまとめたソフトウェアパッケージです。各地方政府がソースコードを個別に修正して使う代わりに、「openCoDE」という共有リポジトリを通じてソースコードを共同で管理しています。このオープンソース戦略は、「ワンス・オンリー」と呼ばれる行政原則とも併せて推進されていると、ドイツの調達専門メディア「Cosinex」のブログが伝えています。ワンス・オンリーとは、市民や企業が一度提出した書類や情報を複数の行政機関に重複して再提出しなくても済むように、行政機関同士がすでに提出された情報を共有し合うという原則です。

ソースコードを共有するopenCodeと、行政情報を共有するワンス・オンリーは、扱う対象こそ異なりますが、重複を減らしてリソースを共有するという同じ発想から生まれたものです。フランスの協調作業ソフトウェア「ラ・スイート（La Suite）」、ドイツの「openDesk」、オランダの「マインビューロー（MijnBureau）」は、互いに異なる3か国のソフトウェアが海外クラウドを経由することなく文書を送受信できることを実際に実演してみせたと、関連報道は伝えています。この実演が意味するところは小さくありません。これまでは異なる国の公務員が文書を取り交わす際、結局は同じ米国系クラウドのアカウントに集まるケースが多かったからです。

3か国がそれぞれ異なるソフトウェアを使いながらも相互に連動できることを示したという点は、欧州諸国が単一のソフトウェアに統一しなくても相互運用性を確保する道があることを意味しています。

このオープンソース戦略は、第4章で扱ったCADAの主権保証レベル体系とも連動するものとみられます。openDeskやラ・スイートのような一般行政用ソフトウェアは、SEAL体系において相対的に機密性の低い下位段階に該当する可能性が高く、アルカディアのように国防に直結するソフトウェアは上位段階の厳格な要件が適用される可能性が高いでしょう。ただし、オープンソース・ソフトウェアとSEAL等級体系が実際にどのように連動するかは、CADAが最終条文を確定する過程で具体化される事項です。

地方政府単位の事例もあります。欧州委員会のInteroperable Europeポータルがまとめた資料によると、ドイツ北部のシュレースヴィヒ＝ホルシュタイン州は、2020年から公務員のコンピュータ2万5,000台からマイクロソフトのOSとOutlookを排除し、LibreOfficeへ移行する作業を進めました。州政府が2025年12月4日に発表したプレスリリースによると、この移行によって州政府は年間1,500万ユーロのソフトウェアライセンス費用を削減しました。

スイスは法制定によってさらに先へと進みました。スイスのメディア「ワトソン（Watson）」が2024年12月4日に報じたところによると、スイスは2024年に「電子政府電子手段法（EMBAG）」を可決させ、公共予算で開発されたすべてのソフトウェアのソースコードを原則としてオープンソースで公開することを義務付けました。同法に基づき、スイス連邦軍参謀本部サイバー司令部は自社開発したセキュリティ分析ソフトウェア「Loom（ルーム）」を民間へ無償公開しました。軍が自前で開発したソフトウェアをオープンソースとして公開する事例は極めて珍しいという点で、この決定はスイスが自国の技術自立をどこまで押し進めようとしているかを示しています。

この流れは、第1章で取り上げたフランス国内セキュリティ総局（DGSI）のアルゴンOS（ArgonOS）への移行や、ドイツ連邦憲法養護庁の離脱と同じ脈絡の上にあります。第1章が扱ったのは、従来パランティア社が担っていた業務を別のベンダーの製品へと移す国内情報機関の決定であったのに対し、本節で扱うアルカディアやopenDeskは、その代替品を欧州自らの手で作り出そうとする開発事業であるという違いがあります。調達先を変更する決定と、変更し得る製品そのものを作り出す作業は、それぞれ異なる段階の課題です。

アルカディア、openDesk、EMBAGは、それぞれ異なる階層で動いている事業です。アルカディアは軍事指揮統制ソフトウェアを、openDeskは公共行政のオフィス用ソフトウェアを、EMBAGはソースコード公開義務の法制化をそれぞれ扱っています。この3者が共有している点はひとつです。外国企業の商用製品を借りて使う代わりに、欧州内部でソースコードを所有し、修正できるソフトウェアを作り出すという決断です。

この判断がどれほど広く普及するかは、まだ見守る必要があります。シュレースヴィヒ＝ホルシュタイン州やスイス連邦軍のように目覚ましい成果を上げた事例がある一方で、EU全加盟国が同じスピードでオープンソースへの移行に乗り出しているわけではありません。マイクロソフトやグーグルのソフトウェアにすでに深く依存している行政機関ほど、移行にかかる初期費用や職員の再教育の負担が大きく、この負担を受け入れる政治的意思がすべての加盟国で同程度に形成されているわけではありません。アルカディアやopenDeskが示したのは可能性であり、欧州全域にわたる完結した移行ではありません。

根拠および参考文献

1. Jean-Baptiste Le Roux, 'Cloud de combat : face à Palantir, la France veut faire émerger un champion national des logiciels militaires', Economie Matin, 2026年7月9日.

2. Jean-Baptiste Leroux, 'IA de combat : face au Palantir, la France veut son Maven hexagonal', Armees.com, 2026年7月9日.

3. Rudy Ruitenberg, 'France to test its own AI-powered battlefield command in June NATO exercise', Defense News, 2026年6月5日.

4. L'Essentiel de l'Éco 編集部, 'Comment Safran devient un géant du renseignement par IA', L'Essentiel de l'Éco, 2026年6月8日.

5. European Commission, COM(2026) 503 final, 欧州連合官報, 2026年6月3日, https://ec.europa.eu/newsroom/dae/redirection/document/129100

6. Digital Independence Editorial, 'Digital Sovereignty in Europe', Digital Independence, 2026年2月16日.

7. European Commission, 'Open source progress in Schleswig-Holstein', Interoperable Europe Portal, 2026年.

8. シュレスヴィヒ＝ホルシュタイン州政府, プレスリリース, 2025年12月4日.

9. Watson 編集部, 'Schweizer Armee setzt auf europäische Software statt Microsoft', Watson, 2024年12月4日.

10. TNW 編集部, 'France and Germany pledge to build a European rival to Palantir's military AI software', The Next Web, 2026年7月18日.

11. Pathfounders Group, 'Here are the top five companies vying to take on Palantir in Europe', Pathfounders Group, 2026年4月.

12. Wolf Witte, 'Vergabebeschleunigungsgesetz und digitale Souveränität 2026', cosinex Blog, 2026年5月21日.

5.3 租税回避を行う多国籍企業に対抗する経済主権：CICTAR報告書と公共財政の保護

欧州各国の政府は、パランティアのような米国企業に対し、毎年多額の調達予算を支払っています。この支出が税金として欧州社会にどれほど戻っているかを検証した報告書が、2026年8月5日に公表されました。国際企業課税責任研究所（CICTAR）は、多国籍企業の租税回避構造を追跡してきた研究組織であり、パランティア以前にも数多くの多国籍企業の租税慣行を分析した報告書を発表しています。今回はその対象をパランティアに絞り込みました。

欧州公共サービス労働組合連盟（EPSU）の支援を受けて作成されたこの報告書は、パランティアの租税構造を分析し、同社が公共契約によって得た利益に対して極めて少ない税金しか納めていないと主張しています。この内容は、調査報道メディアの「Follow the Money（フォロワー・ザ・マネー）」が2026年8月5日の記事でまとめて報じました。EPSUは公共部門の労働者を代表する欧州規模の労働組合連盟です。パランティアをはじめとする民間企業が公共調達を拡大させる流れは、公共部門の雇用や予算に直接影響を及ぼす問題であるため、EPSUがこの調査に資金を提供したことは利害関係のある主体による支援であるという点を明らかにしておく必要があります。

この事実によって報告書の分析内容が自動的に無効化されるわけではありませんが、読者がこの報告書を読む際に参考にすべき背景と言えます。

この報告書がドイツの事例を取り上げた背景には、実際の警察調達契約があります。ドイツメディアの「Labnet Germany（ラボネット・ジャーマニー）」の報道によれば、ヘッセン州をはじめとする複数のドイツの州警察は、パランティアのソフトウェアを活用して、潜在的な脅威人物（ドイツ語で「ゲフェーアダー（Gefährder）」と呼ばれる対象）を追跡・分析する業務を行ってきました。このような契約が複数の州で積み重なったことが、CICTARの試算したドイツ国内における課税ベース損失規模の背景になっていると、同メディアは説明しています。

実効税率とは、企業が実際に納めた税額を税引前利益で割った値のことです。法律で定められた法定税率がいかに高くても、各種控除や会計手法を経て実際に納める税金が減れば、実効税率はその分低くなります。CICTARの報告書が問題視しているのは、パランティアが違法行為を犯したということではなく、合法的会計手法を幾重にも駆使してこの実効税率を低く抑えたという点です。税法に違反する「脱税」と、税法が認める手続きの範囲内で税負担を軽減する「租税回避」は、法律上異なる範疇に属します。本報告書が告発しているのは後者です。このような区分は、この問題に対処するアプローチにも影響を与えます。

脱税は捜査や処罰の対象となりますが、租税回避は個別の企業を処罰することで防げる問題ではありません。税法そのものを改正したり、国家間の租税条約を再構築したり、調達契約の条件を変更するといった制度的対応が必要であることを意味します。本章の後半で取り上げるBEFIT（欧州事業課税フレームワーク）案や調達仕様書の改定要求こそが、まさにこうした制度的対応に該当します。

CICTARの報告書は、パランティアの2025年におけるグローバル法人税の実効税率がわずか1.4%にとどまったと主張しています。同報告書によると、パランティアは2025年の1年間で税引前利益として約16億6,000万ドルを稼ぎ出しましたが、世界全体で納付した法人税は2,270万ドルにすぎませんでした。この数値はCICTARおよび「Follow the Money」の分析によるものであり、本書はパランティアの一次財務諸表を別途検証したわけではありません。しかし、この主張が提起している問題そのものは検討する価値があります。

経済協力開発機構（OECD）が主導し、140か国・地域以上が参加したこの合意は「ピラー2（Pillar Two）」と呼ばれ、2021年に大枠で合意された後、参加国ごとに順次国内法へと反映されています。多国籍企業がいずれの国で事業を展開しようとも、最低15%の法人税を課すことがこの合意の目的です。CICTAR報告書が提示した1.4%という数値が事実であれば、これはこの国際合意の趣旨から大きく逸脱した結果と言えます。

米国の税制政策研究機関である「ITEP（租税経済政策研究所）」が2026年3月22日に発表した別の報告書では、パランティアがトランプ政権時代に制定された税制優遇法に基づく研究開発費の即時控除を活用し、米国内の連邦法人税を事実上納めていないと分析しています。

CICTAR報告書は、パランティアが用いる会計手法も紹介しています。多国籍企業の本社と海外支社の間では、しばしば移転価格と呼ばれるものがやり取りされます。支社が本社へ技術使用料やサービス手数料の名目で資金を送る取引です。この金額をいくらに設定するかによって、支社の帳簿上の利益は大きく変わります。支社が本社に多くの資金を送れば支社の利益は減り、その分、支社が所在する国に納める法人税も減ります。報告書によると、欧州各国のパランティア子会社は契約から生じた収益を米国本社へ送金し、その対価として米国本社から少額のサービス手数料だけを受け取る構造で会計帳簿を作成しています。

この構造の下では、欧州子会社の帳簿上の利益が実際の営業規模よりも低く計上されます。一方、スペインでは異なる手法が用いられたと報告書は伝えています。スペイン子会社が公共調達で得た利益の70%を技術ライセンス料名目で米国本社に送金し、課税対象となるスペイン支社の利益を大幅に圧縮したというものです。これに加え、従業員に対して現金ではなく自社株を支給する「株式報酬制度」も、税法上の費用（損金）として処理され、課税所得を圧縮するために利用されていると報告書は指摘しています。企業が従業員に株式を割り当てると、その株式の価値に相当する額を人件費として会計帳簿に計上できるためです。

人件費は税法上の費用として認められるため、この費用が大きくなるほど課税対象となる利益は減少します。現金で給与を支払う代わりに株式で支給する慣行が広く定着しているテクノロジー業界において、この手法は合法的節税手段として頻繁に用いられています。

報告書が提示した国別の数値もあります。CICTARはこのような会計構造により、ドイツで発生した2024年の税源損失が160万ユーロに達すると試算しており、同年パランティアのドイツ子会社が実際に納めた法人税は64万ユーロにとどまったと明らかにしました。スペインでは、パランティアが国家治安関連機関と1,650万ユーロ規模の契約を結びましたが、実際に納めた法人税は14万7,000ユーロに過ぎなかったと報告書は伝えています。これらの数値はいずれもCICTARが分析して提示したものであり、各国政府の公式発表資料ではありません。

英国ではまた別の事例が確認されています。メディアの「Novara Media（ノヴァラ・メディア）」が2026年6月4日に報じたところによると、英国国民保健サービス（NHS）はパランティアと3億3,000万ポンド規模の統合データプラットフォーム契約を締結しました。この契約は「連邦データプラットフォーム（Federated Data Platform）」という名称で呼ばれ、イングランド全域の病院と診療記録を単一のシステムに統合しようとする事業です。パランティアが本事業の優先交渉権者に選定されたのは2023年であり、患者の機微な医療情報を扱う契約であるという点から、選定当時より英国の医療界や政界で物議を醸しました。

同報道によると、パランティアの英国子会社が2024年に英国税務当局に納付した法人税は200万ポンドにとどまりました。契約規模の3億3,000万ポンドと比較すると、納付した法人税はその165分の1にも満たない金額です。もちろん、契約総額と単年度の法人税納付額を直接比較することは正確な計算方法ではありません。契約金の全額がその年の利益として計上されるわけではなく、法人税は売上ではなく利益に課されるためです。ただし、その格差が著しく大きいという事実だけは、これらの数値が示しています。

英国下院科学技術委員会は別の報告書で、公共部門においてパランティアの存在感が高まっている状況を受け入れがたい脆弱性であると評価しました。

ドイツ、スペイン、イギリスの事例を並べてみると、共通のパターンが浮かび上がります。3カ国ともパランティアと相当な規模の公共契約を結びましたが、実際に徴収した法人税は契約規模に比べて大幅に少ないものでした。3カ国の税務当局がそれぞれ異なる方式で会計を調べたにもかかわらず結果が似通っていたことは、この会計構造が特定国の緩い監督のためではなく、パランティアが複数の国に共通して適用する会計方針のためである可能性を示唆していると、CICTAR報告書は分析しています。

CICTAR報告書が例外として挙げた国はフランスです。報告書によると、フランス国税庁はパランティアがフランス国内で上げた利益をフランス支社の帳簿に完全に記録するよう要求し、その結果、パランティアのフランス支社は2024年に160万ユーロの法人税を33％の実効税率で納付しました。他国の数値と比べると遥かに高い割合です。この違いはフランス国税庁の積極

的な税務執行に起因しているというのが報告書の解釈です。フランスは2019年から自国内で売上を上げる巨大デジタル企業に対して別途のデジタルサービス税を課してきた国でもあります。

米国の巨大IT企業を標的としたこの税制は、これまで米国政府と何度も通商摩擦を引き起こしました。パランティアに対するフランス国税庁の執行方式も、こうした租税政策の延長線上にあるものと見ることができます。

欧州委員会は加盟国個別の税務執行だけに頼らず、多国籍企業の課税標準自体を統一する案も別途推進しています。BEFITと呼ばれるこの提案は、欧州連合内で事業を展開する多国籍企業が加盟国ごとに異なる方法で税金を計算する代わりに、ひとつの共通基準で課税所得を算定しようという内容を盛り込んでいます。この提案もまた、まだ欧州議会と理事会の審議を経る段階にあり、CICTAR報告書が指摘した移転価格を利用した所得移転問題を根本的に減らそうとする試みのひとつとして挙げられています。

この報告書が公表された後、労働界からの反応が相次ぎました。ドイツメディアのラブネット・ジャーマニーが2026年8月5日に報じたところによると、国際公務労連（PSI）事務局長のヤン・ウィレム・グードリアンは、公共保健やセーフティネット予算を守らない海外サプライヤーに国の核心的な調達を委ねる慣行をやめるべきだと述べました。同報道はオランダ最大の労働組合FNV関係者の発言も伝えており、公共インフラの恩恵を享受しながらもそれに見合う税金を納めない企業の慣行をこれ以上放置することはできないという内容でした。こうした反応を示した団体は、公共調達の入札仕様書に税金納付実績を反映させようと提案しています。

これまで公共調達は価格と技術性能を主な評価基準としてきましたが、そこにその企業が実際にどれだけの税金を納めたかを追加しようというものです。この提案が実際の調達規定に反映されたかどうかは、本書が確認した資料の範囲内では確認できません。

この租税問題は、5.1で取り上げた投資格差ともつながっています。ユーロスタック報告書は欧州が2035年までに3,000億ユーロを調達しなければならないと試算しましたが、欧州連合が実際に割り当てた予算はそれに大きく及びませんでした。CICTAR報告書が主張するように、パランティアをはじめとする域外企業が欧州で得た利益に見合う税金を納めていたならば、その税収がユーロスタックの求める投資財源の一部になり得たはずだ、というのが租税改革を求める側の主張です。もちろん、この因果関係はCICTAR報告書を支持する側の政治的な主張であり、本書が別途検証した事実ではありません。

この租税問題は、前章で扱った安全保障問題と異なる次元において同じ結論へとつながります。第1章と第4章が扱ったのは、パランティアのような企業に国家のデータとシステム運用を委ねる際に生じる統制権の問題でした。CICTAR報告書が提起しているのは、その契約から実際にどれほどの資金が国家財政に還元されるのかという問題です。イタリア国家サイバーセキ

ュリティ庁はこれら二つの問題を併せて考慮し、国家の中核的な調達から米国系プラットフォームを排除する方向で方針を決定したと明らかにしました。

租税と安全保障という互いに異なるふたつの根拠が同じ結論を指し示しているという事実が、欧州の政策立案者たちがこの問題を先送りできない理由として挙げられています。

ユーロスタックが求める3,000億ユーロも、アルカディアやオッペンデスクを開発する費用も、CICTARが指摘した税源も、結局はひとつの問いに収束します。欧州が米国企業に依存しない技術基盤を構築しようとするとき、その基盤を築く資金はどこから来るのか、という問いです。銀行に眠る預金を掘り起こすにせよ、すでに取り確保された予算でソフトウェアを開発するにせよ、漏れ出る税金を食い止めるにせよ、3つの道はすべて同じ目的地に向かっています。

市民の立場から見れば、この問題は抽象的な会計論争ではありません。警察署や病院、国防省が支出する調達予算は市民の税金から賄われています。その予算の相当部分が、契約を結んだ企業の税金として再び国庫に戻ってこないのであれば、公共サービスに充てられる財源はその分減ってしまいます。CICTARとフォロー・ザ・マネーが提起した問題の中核は、この循環構造が現在断ち切られている点にあります。税金を納め、その税金で公共サービスを運営し、その公共サービスが再び企業の活動を支えるという循環が正常に機能するためには、調達契約を結んだ企業がその国で正当な負担分の税金を納めなければならないという前提が成り立たなければなりません。

根拠および参考文献

1. Sebastiaan Brommersma, 'Tech giant Palantir accused of aggressive tax avoidance at Europe's expense', Follow the Money, 2026年8月5日, https://www.ftm.eu/articles/us-tech-giant-palantir-tax-avoidance-europe

2. Rika Baack, 'Dubiose Praktiken: Palantir drückt sich vor Steuern', netzpolitik.org, 2026年8月5日, https://netzpolitik.org/2026/dubiose-praktiken-palantir-drueckt-sich-vor-steuern/

3. Rika Baack, 'Big Data bei der Polizei', LabourNet Germany, 2026年8月5日.

4. ITEP, 'Palantir Pays Zero Federal Income Tax Despite Explosive Growth, Largely Due to Trump Tax Law', ITEP Reports, 2026年3月22日.

5. Joshua Carroll, 'MPs Tell Government to End £330m NHS Contract With Palantir', Novara Media, 2026年6月4日.

6. 英国下院科学技術委員会, 報告書, House of Commons, 2026年.

7. イタリア国家サイバーセキュリティ庁, 'Sovranità digitale e IA: l'Italia tra autonomia e dipendenza', イタリア政府, 2026年.

結論1 代替手段が成熟する前の宣言、今後2〜3年のリスク期間の克服

2025年12月15日、パランティアはフランス国内安全総局と3年間の複数年契約を新たに締結したと発表しました。この契約から半年も経たない2026年6月16日、フランスのセバスティアン・ルコルニュ首相は、この契約の相手方をフランス企業のハプスビジョンに変更すると宣言しました。翌日、ル・モンド紙は、パランティア側が更新された契約は法的に依然として有効であると主張していると報じました。発表と契約の終了は同じ出来事ではありません。本書の第1章で取り上げたこの事例は、欧州の政府が今後2年から3年の間に管理すべき移行リスクがどのような姿をしているかを凝縮して示しています。

調達の問題から確認する必要があります。フランス内務省は新たなプログラムを導入し既存データを移行するのに18か月から24か月かかると見込んでおり、その他の報道では契約構造全体の完全な移行に2027年から2029年までかかると見られています。ローラン・ニュネズ内務相は、この空白を埋めるために2027年までパランティアとハプスビジョンを併用する過渡期を設けると明らかにしました。ドイツでも同じ問題が繰り返されています。

ドイツ連邦憲法擁護庁は2026年5月、パランティアの代わりにアルゴンOSを調達することを決定しましたが、この調達が実際に運用されるためには、連邦情報局と連邦憲法擁護庁の権限をあらためて定める700ページを超える法律改正案が先に可決されなければなりません。ドイツ連邦憲法裁判所は、この法改正の期限を2026年末に設定しています。調達を決定したという事実と、その調達が実際に運用される時点は、互いに異なる手続きに縛られています。

契約の条件自体が移行の速度を左右することもあります。バーデン＝ヴュルテンベルク州内務省は2025年3月、中途解約条項なしで5年間に2500万ユーロを支払う条件で、パランティアのゴッサムプログラム導入契約を締結しました。州連立政権に参加する緑の党の内部では、この契約を直ちに中止すべきだという意見に92パーセントが賛成しましたが、中途解約条項のない契約は政治的な反対だけでは覆りませんでした。調達契約に解約条件をあらかじめ盛り込んでおかなければ、国家が自ら交渉力を失うという事実を、この契約は数字で示しています。

人材とデータの移行の問題は、契約書の外で生じます。フランス国内治安総局の職員たちはパランティアの画面構成や操作方法にすでに慣れており、情報を保存する方式そのものがアメリカのシステムの規格に合わせて構築されています。新しいプログラムに移行するには、従来の操作方法を新しい画面に合わせて移植し、職員を再教育し、データが行き交う経路を新たに整え、進行中の捜査が中断されないよう維持し、実際の業務量に耐えられるかを検証する段階を順を追って踏まなければなりません。ドイツ連邦軍も同様の手続きを踏んでいます。

サイバー・情報空間司令部のトーマス・ダウム海軍中将は2026年4月、パランティアを軍事クラウド事業「pCloudBw」の候補から除外したと明らかにし、その後、ドイツ企業のアルマート、ベルリンのスタートアップ企業オークリスト・テクノロジーズ、フランス企業のハプスビジョンの3社が、2026年の夏にかけて実戦データを連携させる試験を行いました。最終落札者は2026年末に発表される予定です。パランティアを除外したことと、新たに誰を選定するかは、まだ別の問題として残されています。

オランダは調達の断片化という、もう一つの形のリスクを抱えています。デルク・ボスワイク国防次官は2026年6月2日、下院においてパランティアを可能な限り速やかに欧州製の代替案に置き換えると明らかにし、完全に同等の水準の代替案を見つけるのに2年を目標としていると述べました。しかし、政府がその後下院に提出した答弁書には、具体的な終了時期の代わりに代替案の検討と依存度の縮小という表現にとどまりました。国防省内部でパランティアと締結した契約が部署ごとに個別に結ばれており、政府レベルでの統一された契約リストすら存在しないという事実が、この答弁の背景にあります。

ボスベイク次官自身も、今すぐ関係を断ち切れば作戦戦闘システムや国防兵站、情報処理に安全保障上の空白が生じる可能性があると認めました。宣言の速度と実行の速度が異なるという事実を、オランダ政府は自ら証言したことになります。

連合作戦の領域では、移行の方向性がむしろ逆に動いています。北大西洋条約機構は2025年、パランティアの「メイブン・スマート・システム」を連合作戦司令部で運用するために導入を確保したと発表しました。この導入発表と、2026年現在このシステムが実際にどの範囲まで運用されているかは、区別して考えるべき問題として残されています。ただ、本書の第3章で指摘した通り、国内の治安情報領域からパランティアを排除する動きと、軍事同盟の領域でパランティアの立場が維持される流れが、同じ時期に並行して起きているというfreezer/fact -> という事実 は明確です。

EU人工知能法の第2条および前文第24項は、軍事、国防、国家安全保障を目的とする人工知能システムを規制の適用範囲から除外しています。国内情報機関の離脱が、国防やNATOレベルでの調達にまで自動的に波及するわけではないことを意味します。オランダ国防省が、NATO同盟国と情報をやり取りするためには同一のシステムを使用しなければならないという相互運用性の要件を、移行の障害として挙げた理由もここにあります。さらに、米国クラウド法は、米国法人が扱う情報であればサーバーの位置に関係なく米国の捜査機関がアクセスできる道を開いています。移行が完了していない期間においては、この法律の射程範囲も依然として残ることになります。

代替供給者の成熟度もまた、この移行期の期間の長さを左右します。ハプスビジョンは2019年の設立以降、25件を超える買収を経て2025年に売上高2億ユーロを記録しましたが、歴史の長いパランティアに比べれば依然として成長途上の企業です。ドイツの最終候補であるアルマ

ートとオークリスト・テクノロジーズも、2026年末になってようやく実戦配備の可否が決まります。欧州委員会はクラウド・AI開発法を通じ、欧州のデータセンター能力を5年から7年の間に3倍以上に増やし、2035年までに企業や行政の需要を満たすという目標を提示しました。

この法律は2026年8月現在、欧州委員会が提出した規則提案の段階であり、まだ制定されていません。供給能力を拡大する計画の完成時期そのものが、すでに2030年代半ばを見据えています。

アンスロピックの2026年6月の事件は、これらすべての移行の背景を成しています。米国政府は6月12日、外国籍者による「フェーブル5」および「ミトス5」へのアクセスを遮断するよう、輸出管理指示をアンスロピックに出しました。アクセスはその後、輸出管理が解除されたことで復旧しました。この事件は、永久的な遮断ではなく、供給がいつでも絶たれる可能性があるというリスクを現実のものとして示した出来事でした。フランス、ドイツ、オランダがそれぞれ異なるスピードで代替手段を模索する中、この可能性は消えることなく残り続けています。

本書が扱う事例に共通して見られるのは、宣言の日付と実際の移行が完了する日付の間に、例外なく数年の隔たりが存在するという事実です。その隔たりを埋める間、各国はアメリカの技術とヨーロッパの代替手段を並行して運用する「二重運用」を避けられません。

根拠および参考文献

1. Palantir Technologies, 'Palantir Announces Renewal of Multi-Year Contract with the DGSI', Business Wire, 2025-12-15, https://www.businesswire.com/news/home/20251215083215/en

2. Le Monde, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, 2026-06-17, https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice_6754592_7.html

3. Markus Seyfferth, 'Wählt der BfV ArgonOS statt Palantir? Erstmals ja.', Dr. Web, 2026-05-01, https://www.drweb.de/waehlt-der-bfv-argonos-statt-palantir-erstmals-ja/

4. 著者不詳, 'Baden-Württemberg zahlt Millionen für ein Produkt, das vielleicht nie genutzt wird', Schwäbische, 2026, https://www.schwaebische.de/regional/baden-wuerttemberg/millionen-fuer-eine-software-auf-abruf-4753518

5. 著者不詳, 'Software: Palantir für die Bundeswehr? "Sehe ich momentan überhaupt nicht"', Handelsblatt, 2026-04-28, https://www.handelsblatt.com/technik/it-internet/software-palantir-fuer-die-bundeswehr-sehe-ich-momentan-ueberhaupt-nicht/100217143.html

6. 著者不詳, 'Bundeswehr Will Not Use Palantir for Military Cloud and AI Project; European Alternatives Examined', Grosswald, 2026-04-29, https://www.grosswald.org/bundeswehr-rejects-palantir-military-cloud-ai-project-european-alternatives/

7. Egle Kristopaityte, 'The Dutch defense ministry is looking for Palantir alternatives', Cybernews, 2026-06-03, https://cybernews.com/tech/dutch-defense-palantir/

8. 著者不詳, 'Over twee jaar exit Palantir? Voorlopig blijft het bij intenties en verkenningen', iBestuur, 2026, https://ibestuur.nl/markt-en-overheid/inkoop-en-aanbesteding/exit-palantir-blijft-het-bij-intenties-en-

verkenningen

9. NATO Communications and Information Agency, 'NATO acquires AI-enabled warfighting system', NCIA, 2025, https://www.ncia.nato.int/newsroom/news/nato-acquires-aienabled-warfighting-system

10. European Union, 'Regulation (EU) 2024/1689 (Artificial Intelligence Act), Article 2 and Recital 24', EUR-Lex, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

11. U.S. Congress, 'Clarifying Lawful Overseas Use of Data Act', H.R. 4943, 2018, https://www.congress.gov/bill/115th-congress/house-bill/4943/text

12. European Commission, 'Proposal for the Cloud and AI Development Act (CADA)', COM(2026) 502, 2026, https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada

13. Anthropic, 'Statement on the US government directive to suspend access to Fable 5 and Mythos 5', Anthropic, 2026-06-12, https://www.anthropic.com/news/fable-mythos-access

14. Anthropic, 'Redeploying Claude Fable 5', Anthropic, 2026, https://www.anthropic.com/news/redeploying-fable-5

結論2 開放性を維持する回復力ある自立（Resilient Openness）の道

スイス連邦保健庁、連邦統計庁、連邦情報技術庁、防衛調達庁アルマスイス、資金洗浄報告局は、2020年から2024年にかけて5つの機関が4年にわたり、パランティアを受け入れない決定を繰り返し下しました。スイスはフランスやドイツのように、すでに導入したプログラムを撤去する国ではありません。最初から敷居を跨がせないよう阻んできた機関が積み重なり、現在では新たに説得する必要すらない状態に至っている国です。

セキュリティ専門メディアのゼンデータは2026年2月、スイスがパランティアを退けた理由は性能不足からではなく、独占的で不透明な内部構造や外国の司法管轄権、リモートで行われるアップデート方式が、制御不能な主権リスクと評価されたためだと報道しました。データをスイス国内に留め、契約書に保護条項を盛り込む程度では、このリスクを十分に防ぐことはできないというのがスイス側の判断でした。だからといって、スイスが外国の技術全体を締め出したわけではありません。

スイスが実際に排除したのはパランティアという特定のサプライヤーであり、その判断基準は国籍ではなく、データの所在地と管轄権、アップデートの統制権でした。

スペインの措置も、同様の方向性の選択を示しています。スペイン首相府は2026年7月1日、通信企業テレフォニカや防衛企業インドラ、造船企業ナバンティアなど、国営企業持ち株会社傘下の公企業に対し、パランティアと新規に契約を結ばないよう指示を出しました。既に結んだ契約まで無効にはしませんでした。スペイン軍情報センターがパランティアと結んだ約1,650万ユーロ規模の契約は、2026年11月までそのまま継続されます。新規契約を防ぐことと既存の契約を解除することは別の問題であるという事実を、スペイン政府は政策の設計段階から前提として認めていたと言えます。反対側にはバーデン＝ヴュルテンベルク州の事例があります。

出口条項がないまま5年、2,500万ユーロで縛られたこの契約は、州連立政権内部の反対票92パーセントをもってしても覆すことができませんでした。ドイツ連邦憲法裁判所も2023年2月、ヘッセン州とハンブルク州が予測警察にパランティアベースのシステムを使用していた根拠法律に違憲判決を下し、市民の通信記録や個人情報を法的根拠なく広範囲に分析する方式が情報自己決定権を侵害すると判断しました。契約に出口がなければ、政治的意志も司法の判断も実行へとつながるまでに時間がかかります。

these cases: これらの事例を並べると、完全な閉鎖と無条件の依存という二つの極端が、それぞれ異なる形で立ち行かなくなるという事実が浮き彫りになります。閉鎖側の限界は、オランダの国防次官デルク・ボスワイク氏が自ら認めた点からも確認できます。同氏は、パランテ

ィアと今すぐ関係を断てば作戦戦闘システムや国防兵站、情報処理に安全保障上の空白が生じる可能性があると明かす一方で、軍事用人工知能分野では現在と同水準の欧州による代替案が存在しないという事実も認めました。能力の裏付けがない閉鎖は宣言にとどまります。

逆に依存側の限界は、2026年6月のアンスロピック輸出規制事件や、サーバーの所在地に関わらず米国の捜査機関によるアクセスを認める米国クラウド法が物語っています。条約や契約書の文言だけでは、この露出を防ぐことはできません。欧州連合の人工知能法が軍事、国防、国家安全保障目的の人工知能システムを適用範囲から外しているのも、すべての領域に同じルールを適用するのではなく、領域ごとに異なる基準を設ける道を欧州連合がすでに選択したことの証拠です。

欧州委員会が提示したクラウド・AI開発法案の提案は、これら二つの極端の間で欧州が実際に選んだ道を示しています。この法律は2026年8月現在、制定された法律ではなく欧州委員会の規則提案であり、データセンターの容量を5年から7年の間に3倍以上に増やし、2035年までに企業と公共行政の需要を満たすという目標を「AI大陸実行計画」の一環として盛り込んでいます。本書の第4章で確認した4段階の主権保証レベル設計と、主権上の理由による契約解除権条項は、最も機微な領域だけを選んで隔離し、残りの領域では外国技術を継続調達しつつも、契約から離脱する権利をあらかじめ確保しておく方式です。

バーデン＝ヴュルテンベルク州が直面した出口のない契約の問題を、制度によってあらかじめ防ごうとする試みと捉えることができます。本書の第5章で扱ったフランチェスカ・ブリア氏らの「ユーロスタック」構想も、同様の問題意識から出発しています。欧州全域のデジタルインフラを再構築するためには、かなりの規模で複数年にわたる投資が必要であると、この報告書は指摘しています。正確な総額については、元の報告書の詳細項目を基に改めて確認すべき部分として残されています。

開放性と自立を同時に達成しようとするこのアプローチは、まだ完結した結果ではなく進行中の試みです。その試みが実際にどれほど有効であるかは、今後確認されるいくつかの具体的な時点にかかっています。ドイツ連邦軍はpCloudBw事業の最終サプライヤーを2026年末に決定します。ドイツ連邦議会は連邦憲法裁判所が定めた期限に合わせて2026年末までに情報機関の権限を新たに定める法律を処理しなければなりません。フランス内務省は2027年までパランティアとハプスビジョンを共に運用すると約束しました。スペイン軍情報センターのパランティアとの契約は2026年11月に終了します。

これらの時点が実際に守られるかどうか、そしてその場を埋める欧州の代替案がパランティアの備える水準の安定性を実戦で証明できるかが、閉鎖でも無条件の依存でもないこの折衷案が成立するかどうかを推し量る次の基準です。

根拠および参考文献

1. 著者不明, 'Switzerland Ends Palantir Contract Over Data Sovereignty Risks', ZENDATA Cybersecurity, 2026-02-14, https://zendata.security/2026/02/14/switzerland-ends-palantir-contract-over-data-sovereignty-risks/

2. The Cradle, 'Spain blacklists Palantir over domestic security concerns', The Cradle, 2026-07-01, https://thecradle.co/articles/spain-blacklists-palantir-over-domestic-security-concerns

3. 著者不明, 'Baden-Württemberg zahlt Millionen für ein Produkt, das vielleicht nie genutzt wird', Schwäbische, 2026, https://www.schwaebische.de/regional/baden-wuerttemberg/millionen-fuer-eine-software-auf-abruf-4753518

4. Bundesverfassungsgericht, 'Urteil vom 16. Februar 2023 - 1 BvR 1547/19, 1 BvR 2634/20', Bundesverfassungsgericht, 2023-02-16, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2023/02/rs20230216_1bvr154719.html

5. Egle Kristopaityte, 'The Dutch defense ministry is looking for Palantir alternatives', Cybernews, 2026-06-03, https://cybernews.com/tech/dutch-defense-palantir/

6. Anthropic, 'Statement on the US government directive to suspend access to Fable 5 and Mythos 5', Anthropic, 2026-06-12, https://www.anthropic.com/news/fable-mythos-access

7. U.S. Congress, 'Clarifying Lawful Overseas Use of Data Act', H.R. 4943, 2018, https://www.congress.gov/bill/115th-congress/house-bill/4943/text

8. European Union, 'Regulation (EU) 2024/1689 (Artificial Intelligence Act), Article 2 and Recital 24', EUR-Lex, 2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

9. European Commission, 'Proposal for the Cloud and AI Development Act (CADA)', COM(2026) 502, 2026, https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada

10. European Commission, 'Cloud computing', Digital Strategy, 2026, https://digital-strategy.ec.europa.eu/en/policies/cloud-computing

11. Francesca Bria et al., 'EuroStack: A European Alternative for Digital Sovereignty', 2025, https://www.euro-stackreport.info/docs/EuroStack_2025.pdf

12. 著者不明, 'Software: Palantir für die Bundeswehr? "Sehe ich momentan überhaupt nicht"', Handelsblatt, 2026-04-28, https://www.handelsblatt.com/technik/it-internet/software-palantir-fuer-die-bundeswehr-sehe-ich-momentan-ueberhaupt-nicht/100217143.html

13. Le Monde, 'French security replaces Palantir with domestic firm ChapsVision, a complicated choice', Le Monde, 2026-06-17, https://www.lemonde.fr/en/france/article/2026/06/17/french-security-replaces-palantir-with-domestic-firm-chapsvision-a-complicated-choice_6754592_7.html

14. The Cradle, 'Spain blacklists Palantir over domestic security concerns', The Cradle, 2026-07-01, https://thecradle.co/articles/spain-blacklists-palantir-over-domestic-security-concerns

金景珍（キム・ギョンジン）
kimkj.com