

データセンター・クラウド安全認証（中国系の事実上排除）

報道の検証と知財業務への影響

日本経済新聞（2026 年 10 月 19 日）「データセンター・クラウド、国が安全認証へ 中国系を事実上排除」をめぐって

2026 年 10 月 20 日

Claude Opus 5.5

本書の読み方

- ・本文中の上付き番号 [n] は、文末「参考文献」の番号に対応する。
- ・第 1～5 章は確認できた事実を中心に記載し、推測を含む箇所には「（分析）」と付記した。第 6～7 章は分析・推測であり、確定した法的義務ではない。
- ・本文を直接確認できなかった出典、URL を特定できなかった出典は、参考文献欄に※で注記した。情報は 2026 年 10 月 20 日時点。

要旨

- **事実関係**：日本経済新聞は 2026 年 10 月 19 日 11:30（会員限定）に、総務省・経済産業省が 2027 年度以降、国内に立地する DC 事業者と国内にサーバーを保有するクラウド事業者を対象に安全認証制度を導入し、金融・医療など重要な個人情報を扱う企業に認証サービスの利用を促すと報じた^[1]。審査項目は企業情報、情報流出を防ぐリスク管理体制、設備の調達先などとされる^[2,3]。政府の正式発表・法案・基準案は未公表であり、制度の詳細は未確定。
- **制度的位置づけ**：内閣官房の有識者会議は 2025 年 12 月～2026 年 1 月に、DC・クラウド上の大量データの防護を提言した^[4-6]。しかし 2026 年 3 月 19 日閣議決定の経済安全保障推進法改正案ではデータセキュリティ部分が見送られ、次の課題とされた^[7]。今回の報道は、この積み残しを 2027 年通常国会で法制化し、その上に認証制度を載せる動きと読むのが妥当である（分析）。
- **知財への影響（分析）**：直接の対象は「重要な個人情報」と DC・クラウド事業者で、技術情報・営業秘密は主対象ではない。それでも、①知財系クラウド・生成 AI の選定基準に「支配関係・準拠法・再委託先」が加わる、②中国系クラウド・AI・特許分析ツールの利用は説明責任を問われる対象になる、③特許出願非公開制度の保全対象発明を扱う電子環境で

は、認証クラウドが事実上の標準になる、という形で波及すると予測する。短期的には、ベンダー台帳の作成と情報区分ごとの利用可否ルールの整備が最優先である。

1. 記事の確認状況と要旨

1-1 記事本文へのアクセス

依頼時の印刷用 URL と日経アジア英語版は、いずれも自動取得が拒否され、本文全文は閲覧できなかった。そこで、日経記事ページの公開部分（見出し・リード）^[1]と、同記事を要約・引用した国内外の報道^[2,3,8-10]を突き合わせて要旨を再構成した。

1-2 配信日

日経電子版の配信は **2026 年 10 月 19 日 11:30**（会員限定）である^[1]。翌 20 日朝の文化放送の番組で、同日付朝刊 1 面の記事として言及されており^[2]、20 日付朝刊にも掲載された可能性がある（紙面は未確認）。韓国メディアが「10 月 20 日報道」としているのは、この紙面掲載を指すとみられる^[8,9]。

1-3 報道内容の整理

項目	報道内容	出典・裏付けの程度
所管	総務省・経済産業省	日経リード ^[1] 。各報道で一致
時期	2027 年度以降に導入	同上
対象	国内に立地する DC 事業者、国内にサーバーを保有するクラウド事業者	同上
審査項目	事業者の企業情報、情報流出を防ぐリスク管理体制、設備の調達先など	複数報道で一致 ^[2,3]
利用者側	金融・医療など重要な個人情報を扱う企業（報道により研究機関も）に、認証サービスの利用を促す（義務ではない）	日経リード・要約報道 ^[1,3]
法的基盤	重要な個人情報を保存・提供する企業に事前届出を課す推進法改正案を、2027 年 1 月召集の通常国会に提出。リスクがあれば国が中止命令・勧告	日経記事の要約報道 ^[3,10] （二次情報）
参照基準	IPA の JC-STAR（IoT 製品のセキュリティラベル制度）を参考にする	同上（二次情報）

項目	報道内容	出典・裏付けの程度
排除の論理	中国の国家情報法・国防動員法などが及ぶ事業者は、サーバーが日本国内にあっても安全を担保しにくい	同上（二次情報）

1-4 「事実上排除」の仕組み

国籍で排除する規定は報じられていない。審査項目の「企業情報（資本・支配関係）」と「設備の調達先」を通じて外国法の影響の有無を問う設計とみられ、その結果として、中国・ロシアの影響下にある事業者や懸念国製の機器に依存する事業者が認証を得にくくなる構造である（分析）。日経は、JC-STAR で中国製品の取得実績がないことを前例として挙げている^[3,10]。資本比率の閾値、再委託先・保守要員の要件、中国製サーバー・ネットワーク機器の扱いは、いずれも報じられておらず未確認である。

2. 一次ソースとの照合

2-1 確認できた政府資料

- **有識者会議 資料9「データセキュリティ制度の検討について」（2025年12月4日）**：「安全保障上重要な個人データ（ゲノム、金融情報等）を取り扱う者」と「大量データの保存・処理を行うDC・クラウドの提供者」の2本柱で検討する方針を示した。DC・クラウドについては、情報の漏えい・滅失を防ぐ措置と、国内DCの設置状況等を把握する措置の必要性を明記している。国内クラウド市場（2024年、1兆7,458億円）や、米国ICTS規則、EUNIS2、英国NIS規則、豪州SOCI法、韓国情報通信網法との比較も掲載^[4]。
- **同「提言骨子（データセキュリティ）」（2026年1月16日）・「提言」（1月30日）**：DC・クラウドについて、サプライチェーンリスク対策を含む漏えい・滅失防止措置と、事業実態を把握する措置を提言した。同時に、DFFT（信頼性のある自由なデータ流通）の提唱国としてデータ利活用を必要以上に制限しないこと、国際約束との整合に留意することを求めている^[5,6]。
- **推進法改正案（2026年3月19日閣議決定）**：データセキュリティは法案に盛り込まれず、次の課題とされた^[7]。

2-2 照合結果

有識者会議の枠組み（2 本柱、サプライチェーン審査、国内 DC の把握）と日経報道は整合する。一方で、「認証制度」という名称、所管 2 省の役割分担、JC-STAR の参照、2027 年度の導入時期を記した政府公表資料は確認できなかった。この部分は現時点で日経の独自取材情報にとどまる。パブリックコメント・法案要綱も未公表である。

2-3 他メディアによる裏付け

確認できた報道はいずれも日経記事の転載・要約であり^[2,3,8-10]、独自取材による裏付け報道は見当たらなかった。

3. 制度的背景と関連制度

- **経済安全保障推進法**：クラウドプログラムは特定重要物資の一つ（2022 年 12 月指定）。基幹インフラ制度は 2026 年改正案で医療分野が追加された^[7]。提言骨子は、基幹インフラ事業者の設備のクラウド化を踏まえ、クラウド内データの保護にも留意するよう求めている^[5]。新認証は、基幹インフラ制度と個人データ規律の隙間（DC・クラウド事業者そのもの）を埋める位置づけになるとみられる（分析）。
- **ISMAP**：政府調達向けのクラウド評価制度で、外資を含め約 96 サービスが登録されている^[11]。管理策の実施状況を評価する制度であり、資本・支配関係による選別は中心ではない。新認証は、民間の重要データ向けに「誰が支配しているか」を問う点で補完的な制度になると考えられる（分析）。両制度の関係（相互承認・統合）は未確定。
- **JC-STAR**：IPA が運営する IoT 製品のセキュリティラベル制度（★1～★4）である^[12]。2026 年 1 月の長期脱炭素電源オークション第 3 回入札では、系統用蓄電池の制御系（BMS・PCS・EMS 等）に★1 取得が要件とされ、2027 年 4 月（低圧は同年 10 月）以降に新規に系統接続する太陽光発電・蓄電池にも、★1 を取得した制御システムの使用が要件化される^[13]。中国製蓄電池は取得実績がないと報じられ、中国側は「事実上の排除」と反発している^[14,15]。法律事務所の解説は、評価項目のうち外国の法的環境による影響を問うサプライチェーン・リスクの項目が、中国企業にとって実務上のハードルになり得ると指摘しているとされる^[16]（未検証）。
- **データ保護の役割分担**：有識者会議の検討では、政府保有の重要データは特定秘密保護法・重要経済安保情報保護活用法で、民間の営業秘密は不正競争防止法で手当てされていると整理され、新規の主対象は個人の機微データと基幹インフラ関連データに絞られている^[4,6]。

- **AI・DC 政策**：経産省提出資料は、クラウド・DC を国内で足元 4 兆円規模・年 20%超で拡大する市場と位置づけ、データセキュリティや低遅延が重視される用途では国内の計算資源が必要としている^[17]。認証は国内 DC 投資を促しつつ、「信頼できる国内 DC」を選別する装置としても機能し得る（分析）。
- **生成 AI の前例**：個人情報保護委員会は 2025 年 2 月 3 日、DeepSeek が取得したデータは中国に所在するサーバーに保存され、同国の個人情報保護法、サイバーセキュリティ法、データセキュリティ法、国家情報法等が適用されると情報提供した^[18]。同月 6 日には政府機関向けの業務利用に関する注意喚起も出され、2026 年 6 月の政府の生成 AI 調達・利活用ガイドラインもこれを踏まえた判断を求めている^[19]。今回の認証は、この「準拠法リスク」の考え方をインフラ層に広げるものといえる（分析）。
- **改正個人情報保護法**：2026 年 7 月 10 日成立・17 日公布（施行は公布後 2 年以内）。委託先が委託業務の範囲を超えて個人データを取り扱うことの禁止が明文化され、クラウド・ホスティング事業者等に対し、個人情報保護委員会が取扱い停止等を要請できる規定も設けられた^[20]。新認証との調整は未確定。

4. 海外制度との比較

国・地域	制度の概要	日本の新認証との対比
米国	司法省・大統領令 14117 実施規則：懸念国やその影響下の者との、機微個人データを伴う取引を禁止・制限（2025 年に段階施行）	日本の「重要な個人情報の事前届出」と問題意識が近い（※）
米国	商務省 ICTS 規則：懸念国関連の ICT 取引を個別審査で禁止し得る ^[4]	日本は事前認証型、米国は事後の個別審査型
米国	FCC：2026 年 4 月、中国移动・中国电信・中国联通の米国内 DC・PoP 運営を禁じる規則案を全会一致で前進させた。AI DC 向け中国製光トランシーバーの禁止も起草中 ^[21,22]	米国は事業者・機器単位の直接排除、日本は認証を通じた間接排除
米国	商務省：IaaS 事業者に外国顧客の本人確認（KYC）を求める規則案（2024 年） ^[23]	日本の報道に利用者 KYC の要素はない
EU	EUCS（クラウド認証）：高位レベルの主権要件は草案から削除され未採択 ^[24] 。2026 年 6 月、欧州委員会がクラウド・AI 開発法（CADA）案で 4 段階の主権保証レベルを提案 ^[25,26]	EU は主権要件を段階化し公共調達で適用する方向（提案段階）。日本は民間向け任意認証で、主権要件の扱いは未公表

国・地域	制度の概要	日本の新認証との対比
EU	NIS2：DC・クラウドを含む重要事業者にサプライチェーンのリスク評価を要求 ^[4]	日本の「設備の調達先」審査に近い
豪州	SOCI 法：重要データを扱う DC・クラウドに登録とリスク管理プログラムを義務付け ^[4]	日本は義務ではなく認証
韓国	情報通信網法：DC 事業者情報保護管理体系（ISMS）認証の取得を義務付け ^[4]	日本の制度に最も近い先例

※米国司法省規則の行は、本調査で出典 URL を再確認できていないため番号を付していない。

評価（分析）：日本案は「利用は任意、ただし重要データの保有者は国が監督」という間接型である。米国（直接禁止）や EU（公共調達で主権要件を段階化）と比べて通商上の摩擦は小さい設計だが、実効性は運用次第である。

5. 評価・反響

- **中国政府：**10 月 19 日の中国外交部定例会見では本件への質疑はなかった^[27]。20 日時点で外交部・商務部等の公式反応は確認できていない。先例として、JC-STAR をめぐり中国の蓄電池メーカーは「事実上の排除」と反発している^[15]。また 2026 年 1 月 6 日には中国商務部が日本向けデュアルユース品目の輸出管理強化を発表し、外務省が抗議した^[28]。報復措置の可能性は排除できない（分析）。
- **中国系事業者：**アリババクラウドは 2016 年に東京リージョンを開設し、2026 年 3 月の 4 拠点目に続き、同年 6 月に国内 5 拠点目の DC を開設して、AI 開発基盤「Model Studio」の国内提供も始めた^[29-31]。同社日本法人は、クラウドや AI を日本国内で完結して利用できる点を訴求していた^[31]。データの国内保管を訴求する戦略は、「所在地ではなく支配関係」を問う新認証とは正面から食い違う（分析）。同社・テンセント・ファーウェイ・国内業界団体の本件へのコメントは確認できていない。
- **国内の論評：**田中秀臣・上武大学教授は、安全保障上必要な措置と評価しつつ、所管省庁の管理能力を懸念した^[2]。大田原正幸氏（Cursorvers）は、認証基準・対象範囲は未確定であり、国産か海外製かで安全性を二分する単純な話ではないとして、運営企業の支配構造、契約、アクセス権限、障害時の復旧まで含めて評価すべきだと指摘した^[32]。
- **想定される論点（分析）**

- ・ コスト増：認証取得・監査のコストはクラウド利用料に転嫁され、国内の中小 DC 事業者の負担にもなる。
- ・ 選択肢の縮小：重要データの領域では米系ハイパースケーラーと国内大手への集中が進む。米系企業への米 CLOUD 法の適用も、制度の公平性をめぐる論点になり得る。
- ・ 通商：有識者会議自身が国際約束との整合性に言及している^[5,6]。国籍を明示しない基準は、WTO（GATS）上の内国民待遇・最恵国待遇との抵触を避けるためとみられる。
- ・ 実効性：再委託先・保守要員・中国製機器の扱い、日本法人を通じた迂回、認証取得後の支配関係の変化が抜け穴になり得る。米国でも、FCC が中国系通信事業者の免許を拒否・取り消した後も、設備や DC スペース、相互接続が米国内に残っていたことが 2026 年 8 月の下院特別委員会の調査で指摘されており^[21]、排除後の残存リスクの管理は各国共通の課題である。

6. 知財業務への影響（分析・推測）

以下は、第 1～5 章で確認した制度動向を前提とした分析・推測である。

6-1 知財系クラウドの選定基準・ベンダー監査

- 直接規制されるのは「重要な個人情報」を扱う企業と DC・クラウド事業者であり、特許情報や営業秘密は対象外である。しかし、金融・医療・研究機関が認証の有無を調達基準に組み込めば、取引先や SaaS ベンダーにも「認証 DC 上で稼働しているか」の確認が連鎖的に広がる。
- 知財管理システム、期限管理 SaaS、文書管理、電子メールのベンダー調査票には、ISMAP・ISO/IEC 27001 に加えて、次の項目が入ると予測する：①基盤 IaaS と稼働 DC の運営主体、②最終親会社と支配関係、③準拠法・管轄、④再委託先と保守拠点の所在国、⑤新認証の取得状況。
- 知財 SaaS は他社の IaaS 上で稼働するものが多く、基盤層まで遡って確認しなければ評価として不十分になる。

6-2 営業秘密管理・技術流出防止

- 不正競争防止法上の秘密管理性は、アクセス制限と秘密であることの認識可能性で判断される。外国当局によるガバメントアクセスのリスクが公に指摘されたクラウドに重要技術を置

き続けても、直ちに秘密管理性を失うわけではない。ただし、漏えい時には管理の相当性や経営判断の妥当性を問われる材料になる。

- 経産省の技術情報管理認証制度（TICS）や越境データ管理に関する検討^[33]と組み合わせ、データの所在地だけでなく「どの国の法律が及ぶか」を管理台帳に記録すべきである。

6-3 生成 AI・AI エージェントの利用

- 明細書作成、先行技術調査、IP ランドスケープに使う LLM は、未公開の発明情報を入力する最も機微な経路である。個人情報保護委員会の情報提供^[18]と政府機関向けの注意喚起^[19]に続き、今回の認証方針によって、「中国法が及ぶ AI・クラウドに未公開発明を入力しない」ことは事実上の業界標準になるとみられる。
- 利用経路は区別して扱う。中国事業者のアプリ・API を使う場合は入力データが同社のサーバーに送られる。一方、公開されたモデルの重みを他社クラウドや自社環境で動かす場合はデータは同社に渡らないが、モデル自体の脆弱性や出力の偏りは残る^[19]。前者はデータ移転、後者はモデルの検証が論点であり、社内ルールでは両者を分けて定めるべきである。
- アリババクラウドの「Model Studio」のように国内 DC で提供される中国系 AI サービス^[30]は、「国内保管＝安全」とはみなされない方向になる。

6-4 中国系特許 DB・分析ツール、中国子会社・代理人とのデータ共有

- 中国系の特許 DB・分析ツールで公開特許情報を検索すること自体の機密性は低い。ただし、検索式、ウォッチ対象、社内の技術分類、自社ポートフォリオのアップロードは研究開発の方向性を推知させる情報である。これらは未公開情報と同等に扱い、中国法が及ぶ事業者のツールでは避けるか、匿名化して使うのが妥当である。
- 中国子会社・中国代理人とのデータ共有は、新認証よりも、中国側のデータ規制と日本の外為法（技術提供規制）が主な論点である。中国は 2024 年以降、データの越境移転規制を緩和する一方、国内のサイバーセキュリティ統制は強化しており^[34]、規制の向きが分野で異なる点に注意を要する。共有する情報を出願に必要な最小限に絞り、共有経路（使用するクラウド）を指定するルールを整備すべきである。

6-5 特許出願非公開制度・セキュリティ・クリアランスとの接点

- 特許出願非公開制度は 2024 年 5 月 1 日に施行された^[35]。適正管理措置ガイドライン（案）は、保全対象発明を特許出願後も営業秘密として取り扱うこと、情報取扱者を必要最小限に限ること（知財部門の担当者も情報取扱者になり得る）を示している^[36]。
- 同ガイドライン（案）は外部クラウドの利用も想定しており、クラウド事業者のセキュリティ対策の実施状況、サーバーの管理状況や設置場所の相当性を吟味して事業者を選定し、必要な条件を明示した契約を結ぶこと、保管先サーバーの設置場所を「特定区域」とすることを求めている^[36]。新認証が始まれば、この「相当性」の判断において認証の有無が有力な物差しになると予測する。
- 重要経済安保情報を扱う適合事業者や、日米で議論されている政府向け主権クラウド^[11]との関係では、新認証が上位要件の前提になる可能性がある（未確定）。

6-6 DC・クラウド事業者側の知財戦略と IP ランドスケープの着眼点

- 認証取得を目指す事業者にとっては、次の技術群が差別化要因となり、特許出願と標準化の対象になる：サプライチェーンの真正性検証（ハードウェアの来歴管理、SBOM/HBOM、ファームウェア検証）、機密計算（Confidential Computing）、顧客による鍵管理（BYOK/HYOK）、運用者アクセスの技術的遮断と監査ログ、主権クラウドの分離アーキテクチャ。AI DC の需要拡大に伴い、液冷、高効率電源、ワット・ビット連携（電力と通信の一体整備）関連も重要になる。
- IP ランドスケープでは、①国内 DC 事業者・通信キャリア・国内 SIer の上記分野の出願動向、②中国系事業者（アリババ、ファーウェイ等）の日本出願の推移（市場縮小・撤退のシグナル）、③JC-STAR、NIS2、CADA 等の基準と自社技術の対応関係（標準必須化の余地）を見るのが有効である。

7. 推奨アクション（知財部門）

短期（～6 か月）

1. 知財部門が使うクラウド、SaaS、生成 AI、特許 DB の台帳を作り、運営主体・最終親会社・基盤 IaaS・データ所在国・準拠法・再委託先を記録する。
2. 情報区分（未公開発明、営業秘密、出願済み技術、公開情報）ごとに、中国法が及ぶサービスの利用可否を明文化する。特に未公開発明は、中国系 AI・API への入力を原則禁止とする。

3. ベンダー調査票に支配関係と準拠法の設問を追加し、契約に支配権変更時の通知義務と解約権を盛り込む。
4. 中国子会社・中国代理人との共有経路を棚卸しし、外為法の技術提供規制との整合を確認する。

中期（2027 年通常国会～制度運用開始）

1. 推進法改正案、認証基準案、パブリックコメントを追跡する。あわせて、自社が「重要な個人情報」の事前届出の対象になるか（例：医療・ゲノム研究データを扱う研究開発部門）を法務部門と確認する。
2. 保全指定の可能性がある技術分野（防衛・宇宙・量子・先端材料など）について、認証クラウドを前提とした管理環境を準備する。
3. 自社が DC・クラウド・セキュリティ関連事業を持つ場合は、認証要件に対応する技術の出願・標準化戦略を立て、競合の動きを IP ランドスケープで監視する。
4. 中国による対抗措置（日本企業に対する中国国内での認証・データ規制の強化など）に備え、中国での出願・ライセンス情報の管理も見直す。

8. 留意点

- 日経記事の全文は閲覧できていない。要旨は日経の公開部分と、それを要約した国内外の報道から再構成したもので、細部（特に JC-STAR の参照、2027 年 1 月の法案提出）は二次情報である。
- 認証制度の名称・基準・対象範囲・既存制度（ISMAP 等）との関係を示す政府の正式資料は、2026 年 10 月 20 日時点で確認できていない。法案は未提出であり、国会審議で内容が変わる可能性がある。
- 中国政府・中国系事業者・業界団体の公式反応は、報道から日が浅いこともあり確認できていない。
- 改正個人情報保護法の政令・規則との調整など、関連法制の相互関係も未確定である。
- 第 6～7 章は分析・推測であり、確定した法的義務を示すものではない。

参考文献

URL は 2026 年 10 月 20 日時点。※印は本文を直接確認できていない、または URL を特定できなかった出典を示す。

- [1] 日本経済新聞「データセンター・クラウド、国が安全認証へ 中国系を事実上排除」2026 年 10 月 19 日 11:30 配信（電子版・会員限定）
<https://www.nikkei.com/article/DGXZQOUA171BY0X11C26A0000000/> ※本文は会員限定のため未閲覧。見出し・リード部分のみ確認。依頼時の印刷用 URL (https://www.nikkei.com/news/print-article/?R_FLG=0&bf=0&ng=DXGXZQOUA171BY0X11C26A0000000) は自動取得不可。
- [2] 文化放送 radiko news 記事（2026 年 10 月 20 日、田中秀臣・上武大学教授のコメントを含む）
<https://news.radiko.jp/article/station/QRR/140388/>
- [3] 파이낸셜뉴스（韓国ファイナンシャルニュース）2026 年 10 月 19 日記事（日経報道の要約）。英語版を併記 <https://fnnews.com/news/202610191455273534>
<https://en.fnnews.com/news/202610191455273534>
- [4] 内閣官房「データセキュリティ制度の検討について」経済安全保障法制に関する有識者会議 資料 9（2025 年 12 月 4 日） https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r7_dai13/shiryo9.pdf
- [5] 内閣官房 経済安全保障法制に関する有識者会議「提言骨子（データセキュリティ）」（2026 年 1 月 16 日） https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r8_dai14/teigenkosshi_6.pdf
- [6] 内閣官房 経済安全保障法制に関する有識者会議「提言」（2026 年 1 月 30 日）
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r8_dai15/teigen.pdf
- [7] 参議院『立法と調査』No.483（2026 年 4 月 30 日）所収、経済安全保障推進法改正案に関する論考
https://www.sangiin.go.jp/japanese/annai/chousa/rippou_chousa/backnumber/2026pdf/20260430003.pdf
- [8] SBS News（韓国）英語版記事（2026 年 10 月 20 日、日経報道の要約）
https://news.sbs.co.kr/english/article.do?news_id=N1008806185
- [9] アジア経済（韓国）英語版記事（2026 年 10 月 20 日、日経報道の要約）
<https://www.asiae.co.kr/en/article/2026102009245752419>
- [10] TechNews（台湾）2026 年 10 月 19 日記事（日経報道の要約） <https://technews.tw/2026/10/19/japan-security-certification-cloud-services-exclude-china-russia-influenced-firms/>
- [11] Crowell & Moring, "Japan's Sovereign Cloud Commitment at the U.S.-Japan Summit: Defense Interoperability, Not Just Digital Policy"（クライアントアラート）
<https://www.crowell.com/en/insights/client-alerts/japans-sovereign-cloud-commitment-at-the-us-japan-summit-defense-interoperability-not-just-digital-policy>
- [12] 独立行政法人情報処理推進機構（IPA）"Japan Cyber STAR (JC-STAR)" 制度概要ページ（英語）
<https://www.ipa.go.jp/en/security/jc-star/index.html>
- [13] ITmedia スマートジャパン「蓄電池などの分散型エネルギーリソース、2040 年度の導入見通しと課題対応の方向性：第 2 回『分散型エネルギー推進戦略 WG』」（2026 年 3 月 13 日）
https://www.itmedia.co.jp/smartjapan/spv/2603/13/news042_3.html

- [14] 日本経済新聞「中国蓄電池、日本のサイバー認証いまだゼロ」（2026年3月）
<https://www.nikkei.com/article/DGXZQOUC19AMF0Z10C26A3000000/> ※会員限定のため本文は未閲覧。題名・時期は調査過程の二次情報による。
- [15] 濱本隆太 "JC-STAR and Chinese Storage Batteries: Japan's IoT Cyber Label, Economic Security, and the 'De Facto Exclusion' Dispute [2026 Edition]" TIMEWELL（2026年7月6日）
<https://timewell.jp/en/columns/jc-star-china-battery-economic-security-2026>
- [16] 長島・大野・常松法律事務所による JC-STAR と中国製品・サービスに関する解説（2026年6月30日）
※調査過程で参照されたが、URL を再特定できず本文を直接確認できていない（未検証）。
- [17] 経済産業省提出資料（内閣府 規制改革推進会議 ワーキング・グループ、2026年5月15日）
https://www8.cao.go.jp/kisei-kaikaku/kisei/meeting/wg/2501_06ai/260515/ai10_0104.pdf
- [18] 個人情報保護委員会事務局「DeepSeek に関する情報提供」（2025年2月3日、同年3月5日更新）
https://www.ppc.go.jp/news/careful_information/250203_alert_deepseek/
- [19] 石塚悠悟「DeepSeek の危険性とは？中国の法令・情報漏洩と業務利用の判断基準」GiftX AI 活用ブログ
（2026年10月8日） <https://ai.giftx.co.jp/blog/deepseek-risks-security/>
- [20] 太田祐一（監修）「【2026年最新】個人情報保護法の改正はいつ？どうなる？見直しのポイントをわかりやすく解説」webtru（2026年7月10日公開、同年9月3日更新） <https://webtru.io/blog/personal-information-protection-law-amendment/>
- [21] BlueVoyant Risk Operations Center, "Revoked Isn't Removed: The Supplier Exposure a Federal Ban Leaves Behind"（2026年10月5日） <https://www.bluevoyant.com/blog/chinese-telecom-bans-supplier-exposure>
- [22] mlq.ai「FCC、AI データセンター向け中国製光トランシーバーの新規禁止を検討」趣旨の記事
<https://mlq.ai/news/fcc-weighs-ban-on-new-chinese-optical-transceivers-used-in-ai-data-centers/> ※題名は URL 表記による。
- [23] Davis Wright Tremaine, Artificial Intelligence Law Advisor（2024年2月、米商務省の IaaS 事業者向け KYC・AI 規則案に関する解説） <https://www.dwt.com/blogs/artificial-intelligence-law-advisor/2024/02/commerce-department-proposes-kyc-ai-rules-for-iaas>
- [24] ITBroker 用語集 "European Cybersecurity Certification Scheme for Cloud Services (EUCS)"
<https://www.itbroker.com/resources/glossary/european-cybersecurity-certification-scheme-for-cloud-services-eucs>
- [25] Jones Day, "European Commission's Proposed Cloud Sovereignty Framework Creates New Compliance Tiers for Software Providers"（2026年6月）
<https://www.jonesday.com/en/insights/2026/06/european-commissions-proposed-cloud-sovereignty-framework-creates-new-compliance-tiers-for-software-providers>
- [26] HLC, "The EU's Cloud and AI Development Act (CADA): Towards a Sovereignty-Focused Framework for Cloud" <https://www.hlc.com/en/publications/the-eus-cloud-and-ai-development-act-cada-towards-a-sovereignty-focused-framework-for-cloud>
- [27] 中華人民共和国外交部「2026年10月19日外交部發言人毛寧主持例行記者會」
https://www.mfa.gov.cn/fyrbt_673021/202610/t20261019_12042878.shtml

- [28] 外務省 報道発表「金井外務省アジア大洋州局長から施駐日中国大使館次席公使への申入れ」（令和 8 年 1 月 6 日） https://www.mofa.go.jp/mofaj/press/release/pressit_000001_03185.html
- [29] DatacenterDynamics, "Alibaba Cloud launches fifth data center in Japan" (2026 年 6 月)
<https://www.datacenterdynamics.com/en/news/alibaba-cloud-launches-fifth-data-center-in-japan/>
- [30] Nikkei Asia, "Alibaba's cloud arm opens 5th Japan data center, adding new AI services" (2026 年 6 月)
<https://asia.nikkei.com/business/technology/artificial-intelligence/alibaba-s-cloud-arm-opens-5th-japan-data-center-adding-new-ai-services>
- [31] 日経クロステック ニュース記事（アリババクラウド日本法人の事業展開に関するもの、2026 年 3 月）
<https://xtech.nikkei.com/atcl/nxt/news/24/03131/> ※自動取得不可のため題名・本文を直接確認できない（内容は調査過程の二次情報による）。
- [32] 大田原正幸（Cursorvers）X 投稿（2026 年 10 月 19 日）
<https://x.com/cursorvers/status/2112076287015567498>
- [33] 経済産業省 産業データサブワーキンググループ 配布資料（2025 年 1 月 28 日、越境データ管理関係）
https://www.meti.go.jp/shingikai/mono_info_service/industrial_data_subwg/pdf/20250128_1.pdf ※本文の直接確認は未了。
- [34] エレドン ビリゲ「中国のデータとサイバーセキュリティ規制動向」PwC Japan グループ（日経 Digital Governance フォーラム 2026 セッションレポート、2026 年 6 月 2 日）
<https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/nikkei-digital-governance-forum2026/nikkei-digital-governance-forum08.html>
- [35] 内閣府「特許出願の非公開制度」ウェブページ
https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/patent/patent.html
- [36] 内閣官房 経済安全保障法制に関する有識者会議 特許出願非公開に関する検討会合 第 2 回 資料 8「適正管理措置ガイドライン（案）の概要、損失の補償に関する Q&A（案）の概要」（2023 年 12 月 4 日）
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r5_dai9/siryou8.pdf