

データセンター・クラウド「安全認証」構想と知的財産実務への影響

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」と政府一次資料の分析

調査基準日：2026年10月20日（日本時間）

エグゼクティブサマリー

2026年10月19日、日本経済新聞は、日本政府が国内のデータセンター（DC）と国内にサーバーを置くクラウドサービスを対象に新たな「安全認証」制度を設け、金融・医療など安全保障上重要な個人情報を扱う事業者には認証済みサービスの利用を促す方針だと報じた。報道上、審査項目には事業者情報、リスク管理体制、設備の供給者、さらに「懸念国の影響の有無」が含まれ、中国・ロシア等の影響下にある事業者は事実上選択されにくくなる設計が想定されている。総務省・経済産業省が2027年度以降の導入を目指すとする。

1

ただし、2026年10月20日現在、この「安全認証」の最終的な制度要綱、認証基準、法令案、審査機関、対象事業者の閾値、認証期間、認証取消事由、既存契約の経過措置等は政府から公表されていない。政府の最新の公式な表現は、2026年7月21日閣議決定の「経済財政運営と改革の基本方針2026」が「安全保障上重要な個人機微データ」の防護法案の早期提出と、DC・クラウドの安全性確保のための必要な措置を掲げ、10月16日の第18回有識者会議がなお「データセキュリティ」について検討を続けている、という段階である。したがって、日経記事にある具体的な認証制度像は、**政府方針と整合する有力な先行報道ではあるが、確定法令ではない**という区別が重要である。

2

知財実務上の最大のポイントは、この政策を単なる「中国系クラウド排除」問題として扱わないことである。政府が問題視している方向性は、サーバーの物理所在地だけではなく、**事業者の支配関係、適用法域、外国政府からの影響、管理者アクセス、機器・ソフトウェアのサプライチェーン、バックアップ・ログ・鍵管理を含む“実質的なデータ支配”**である。既存のガバメントクラウド仕様も、国内保存、アクセスログ、暗号化・鍵管理、第三者製品の監査、サプライチェーンリスク、データ消去、移行可能性等を詳細に要求している。新認証がこれと同一になるわけではないが、今後の技術要件を予測するうえで重要なベンチマークとなる。

3

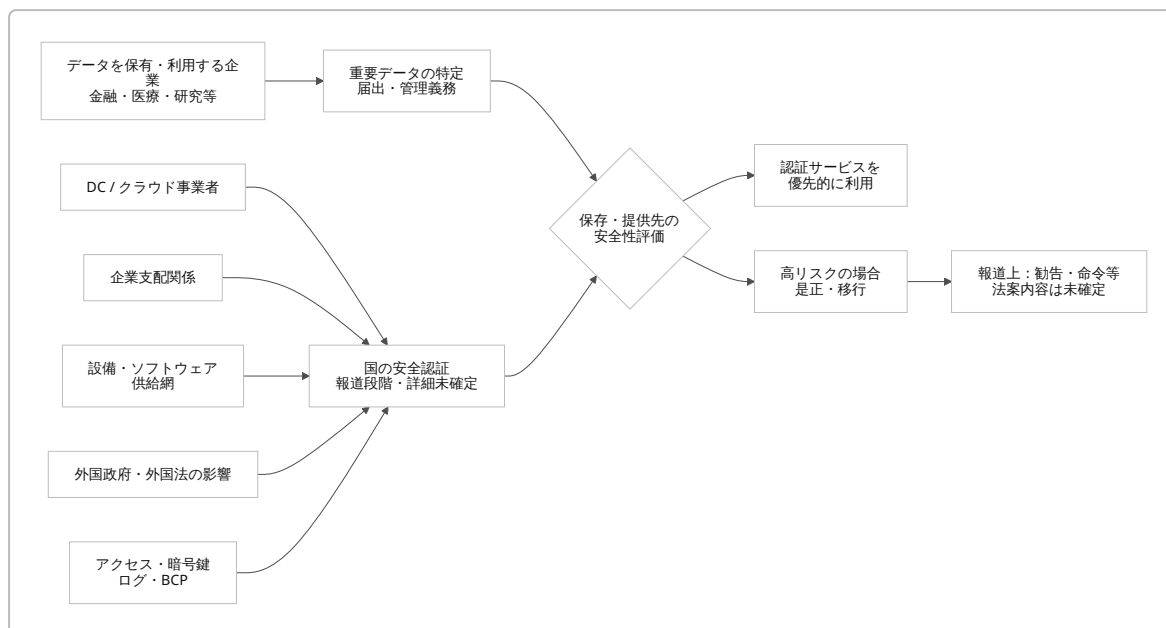
知財部門にとって優先度が最も高いのは、特許出願書類そのものよりも、その前段階にある**未公開発明、実験データ、設計図、ソースコード、製造条件、共同研究データ、ライセンス交渉資料、発明者情報、営業秘密、訴訟証拠**である。これらは「安全保障上重要な個人機微データ」の直接対象外であっても、営業秘密、輸出管理、特許出願非公開制度、研究セキュリティ、契約上の秘密保持義務の対象となり得る。経済産業省は営業秘密について秘密管理性を含む法的保護要件を整理し、技術流出対策ガイダンスでは共同研究・アクセス管理・安全保障貿易管理を組み合わせた管理を求めている。

4

したがって日本企業は、法案成立を待って一斉移行するのではなく、「**データ分類 → クラウド/DC支配関係の把握 → 契約上の退出権確保 → 高機微ワークロードの隔離・暗号鍵主権 → 移行試験**」を2026年度中に開始することが合理的である。特に、中国系クラウドを利用していること自体が現時点で違法になるわけではないが、金融・医療・安全保障関連R&D、デュアルユース技術、ゲノム等の機微情報、重要インフラ関連情報

では、2027年度以降に「技術的には使えるが、規制・監督・取引先要求のため実務上使いにくい」状態になるリスクが高いと評価する。

政策を概念的に整理すると、次の三層構造になる可能性が高い。



この三層構造のうち、DC・クラウド安全性確保という政策目標自体は政府文書で確認できる一方、認証・届出・勧告命令の具体的結合関係は、現段階では日経報道を中心に把握すべき事項である。 5

政策の背景、制度化までの経緯と現在地

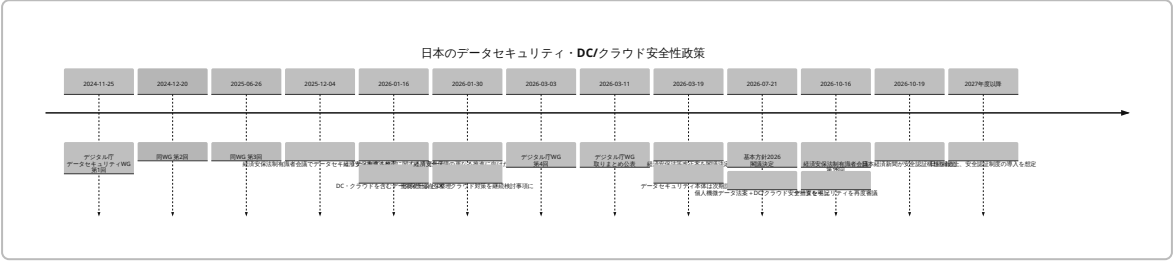
データセキュリティ政策は突然出てきたものではない

政府の検討は、少なくとも2024年から続く「データセキュリティ」の政策線上にある。デジタル庁のデータセキュリティワーキンググループは、国境を越えたデータ共有・利活用を前提としつつ、機微データの保護を制度・技術・運用の組合せで確保することを検討してきた。同WGは2024年11月25日に第1回、同年12月20日に第2回、2025年6月26日に第3回、2026年3月3日に第4回を開催し、2026年3月11日に取りまとめを公表した。これは「国内に全部閉じ込める」単純なデータローカライゼーションではなく、DFFT（Data Free Flow with Trust）との両立を目指す政策文脈である。 6

並行して、経済安全保障法制に関する有識者会議は、2025年末から、①民間が保有する安全保障上重要なデータ、②大量データを処理・保存するDC・クラウドそのもの、という二つの側面から制度を検討した。2026年1月30日の「経済安全保障の更なる推進に向けた提言」は、DC・クラウドを重要インフラとして捉え、情報の漏えい・滅失やサプライチェーンリスク等への対策を検討課題として位置付けた。 7

一方、2026年春に国会提出された経済安全保障推進法等の改正では、このデータセキュリティ論点は盛り込まれず、今後の検討課題として残された。その後、7月21日の「基本方針2026」が改めて「安全保障上重要な個人機微データ」の法案提出とDC・クラウド安全性確保を政府方針として明記し、10月16日の有識者会議で制度検討が再開・深化した、という流れである。 8

タイムライン



日付はデジタル庁、有識者会議、基本方針2026、参議院資料および日経報道を突合した。 9

日経報道と政府が公式に確認していることを分ける

項目	2026年10月20日時点の評価	根拠
DC・クラウドの安全性を政策対象にする	公式確認済み	基本方針2026が「必要な措置」を明記。 10
安全保障上重要な個人機微データについて新法制を検討	公式確認済み	10月16日の有識者会議でも継続検討。 11
国による「安全認証」制度	日経報道段階	日経記事および同記事を引用する報道。 1
総務省・経産省が所管	日経報道段階	報道では2027年度以降に両省が導入するとされる。 12
国内DC、国内サーバーを有するクラウドが対象	日経報道段階	報道上の対象範囲。閾値等は未公表。 12
企業情報、リスク管理、設備供給者、懸念国の影響を審査	日経報道段階	最終認証基準は未公表。 12
中国・ロシア系が自動的に法定排除	確認できず	現時点で国籍を名指しした法文・基準は公表されていない。「事実上排除」は報道上の評価。 13
重要データ保有者への事前届出、政府の勧告・命令	日経報道上の制度案	法案条文は未公表。 12
2027年度開始	報道上の目標	正式施行日・経過期間は未確定。 12

ここは実務上きわめて重要である。「中国企業との契約を直ちに解約する法的義務が発生した」という理解は、2026年10月20日現在では誤りである。一方で、規制業種・重要R&Dの調達基準、監督当局の期待、取引先のセキュリティ質問票が正式法令より先に厳格化する可能性は十分にあり、実務的な対応開始を法施行まで遅らせることも適切ではない。

安全認証の対象・技術要件と法規制上の位置付け

認証制度の想定スコープ

日経報道に基づけば、直接の認証対象は概ね、①日本国内に立地するDCの運営者、②日本国内のサーバーを用いてクラウドサービスを提供する事業者、の二類型と考えられる。金融・医療・研究等の重要データ保有者は認証「申請者」というより、認証サービスを利用するよう促される側になるとみられる。¹²

しかし、次の境界は**すべて未確定**である。

SaaS事業者まで直接認証されるのか、SaaSの基盤IaaSだけで足りるのか。コロケーション、ハウジング、CDN、エッジ、バックアップサービス、生成AI API、マネージドデータベース、海外本社から遠隔運用される日本リージョンがどう扱われるか。DCの電力・通信・設備会社までサプライチェーン審査を受けるか。さらに、売上、設備容量、データ量等による適用閾値もまだ分からない。これらを現段階で「決まった要件」と扱うべきではない。

公表済み情報から見える審査軸

日経報道の四項目と、現在の政府クラウド調達・ISMAPを並べると、今後の審査構造は概ね次のように考えるのが合理的である。

評価軸	新認証について確認できる内容	既存制度から見える技術的論点	状態
企業・支配関係	事業者情報、懸念国の影響を審査すると報道	親会社、株主、取締役、変更支配、外国法の適用、政府アクセス	詳細未確定。 ¹²
リスク管理	リスク管理体制を審査すると報道	ISMS、責任体制、脆弱性管理、インシデント対応	方向性は高確度、具体基準未確定。 ¹⁴
サプライチェーン	設備供給者情報を審査すると報道	現行ガバメントクラウドは第三者製品の監査、製品・製造企業一覧、NIST SP800-53相当の監査枠組みを要求	新認証への転用は未確定。 ¹⁵
データ所在地	新認証の明文基準は未公表	ガバメントクラウドは原則として情報資産を国内保管	新認証が国内保存を義務化するか不明。 ¹⁵
管理者アクセス	未公表	アクセス制御、認証、ログ管理等は既存クラウド調達の中核	外国からの管理アクセス制限が焦点になる可能性が高いが推定。 ¹⁵
暗号・鍵	未公表	現行政府調達は暗号化と暗号鍵の保護・管理を要求	BYOK/HYOKまで要求するか不明。 ¹⁵
ログ・証跡	未公表	政府調達はアクセスログ等の保存・提出を要求し、1年以上の保存を望ましいとしている	認証基準になるか不明。 ¹⁶
データ消去・移行	未公表	政府調達は汎用形式での返還、復元不能な消去、書面報告、原則1年以上のサービス終了事前通知を要求	知財・証拠保全上も重要なベンチマーク。 ¹⁷

評価軸	新認証について 確認できる内容	既存制度から見える技術的論点	状態
可用性・ 災害対策	未公表	国内複数地域、冗長性、RPO等を要求	安全保障上の「可用性」 評価に入る可能性。 ¹⁵
外部認証	未公表	ISMAP、ISO/IEC 27001、27017、 27018、SOC等を現行制度が利用	相互承認・重複審査の扱 いは未確定。 ¹⁸

ISMAPとの違いを明確にしておく必要がある。ISMAPは、政府情報システムで利用するクラウドサービスについて、政府のセキュリティ要求を事前に評価・登録する制度であり、NCO、デジタル庁、総務省、経産省が運営している。監査機関による監査を経た上で登録審査が行われ、政府調達では登録サービスから調達するのが原則である。¹⁹

これに対して今回報道された新制度は、**民間の重要データまで視野に入れ、従来のサイバーセキュリティ統制だけでなく、事業者の支配関係・外国政府の影響・設備サプライチェーンといった経済安全保障上の「主体リスク」を評価するもの**と理解するのが妥当である。ただし、ISMAP登録を新認証の一部として認めるのか、完全に別監査にするのかはまだ分からない。¹⁴

法的根拠は「一本の法律」ではなく多層になる

現時点で新認証そのものの根拠法は確定していない。重要個人データ保有者側の届出・監督については、経済安全保障法制の新法・改正法に位置付けられる可能性が報じられているが、法案条文はまだ公開されていない。DC・クラウド認証については、法律上の登録・認証制度にするのか、政府・業界の調達／推奨制度として構築するのも最終確認できない。²⁰

一方、企業が今すでに遵守すべき既存制度は別途存在する。

個人情報保護法では、外国にある第三者への個人データ提供について、提供先の措置だけでなく、その外国の制度が相当措置に影響し得るかを定期的に確認することが求められる。個人情報保護委員会のガイドラインは、政府による広範な情報収集を可能にする外国制度を明示的な確認対象の例として挙げている。これは「サーバーが東京にあるから外国法リスクはない」という分析が不十分であることを示している。²¹

営業秘密については、不正競争防止法上の保護を受けるための「秘密管理性・有用性・非公知性」が中心となる。METIは2025年3月に営業秘密管理指針を改訂しており、クラウドへの保存そのものが営業秘密性を失わせるわけではないものの、誰に秘密として管理されていると認識させていたか、アクセス権・表示・管理措置がどう実施されていたかが重要になる。²²

特許出願非公開制度では、安全保障上機微な一定の発明について保全審査・保全指定が行われ、外国出願の制限も生じ得る。JPOは外国出願禁止の事前確認制度も設けている。したがって対象になり得る未出願技術については、クラウド上の国外アクセスや共同研究者への共有を通常の発明情報と同じレベルで扱うべきではない。²³

さらに**外為法上の安全保障貿易管理**では、物理的な輸出だけでなく技術の提供が規制され、一定の場合には国内での提供も「みなし輸出」管理の対象になる。共同研究環境やクラウドのアクセス権付与は、情報の種類・相手・アクセス実態を踏まえて別途輸出管理評価が必要である。²⁴

金融分野では、金融庁がクラウドを含むサードパーティ・サイバーリスク管理を継続的に高度化しており、2026年にはITレジリエンスやサードパーティ管理に関する調査・分析を公表している。医療分野でも、厚労省は2026年6月に「医療情報システムの安全管理に関するガイドライン第7.0版」を公表し、遵守を求めている。

る。このため、仮に新制度上「認証サービス利用」が形式上は推奨にとどまっても、金融・医療では既存監督・ガイドラインと結合して事実上の調達条件になりやすい。 25

事業者・市場への影響と中国系サービスの位置付け

日本市場の規模とシェアは「定義」に注意が必要

政府の2026年成長戦略は、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付け、2035年までに国内クラウド市場30兆円を目標としている。この4兆円はクラウドとDC等を含む政策上の広い市場概念であり、IaaS/PaaSの売上シェアとは一致しない。 26

一方、政府検討資料で参照された民間調査データについて公開情報を突合すると、2024年の日本クラウド市場を約1兆7,458億円とし、事業者名を匿名化した構成比として首位41.1%、2位14.7%、3位10.8%、4位4.7%、5位2.9%、その他25.8%という数字が確認できる。公開された富士キメラ総研の市場説明でもAWS、Microsoft Azure、Google Cloudによる寡占構造が指摘されている。ただし、匿名化された割合と個別社名との対応付けは公式発表ではないため、以下の数字は市場構造からの推定である。 27

主な対象候補

事業者	系統	日本での位置付け	日本クラウド市場シェアの目安	新制度上の主な論点
Amazon Web Services	米国	ガバメントクラウド採用事業者	約41.1%と推定。匿名統計の首位との対応付けであり公式個社数字ではない	米国法、親会社支配、国外管理アクセスをどう評価するか。ただし既存政府調達への適合実績は大きい。 28
Microsoft Azure	米国	ガバメントクラウド採用	約14.7%と推定	AWS同様、外国企業でも「中国系と同じ扱い」ではなく、法域・統制・主権性をどう評価するかが鍵。 28
Google Cloud	米国	ガバメントクラウド採用	約10.8%と推定	管理アクセス、サブプロセッサ、AIサービスへのデータ流入を含む統制。 28
Oracle Cloud Infrastructure	米国	ガバメントクラウド採用	2.9～4.7%付近又は「その他」の可能性。公開統計から確定不能	同上。既存政府利用実績はプラス要因。 28
さくらのクラウド	日本	2023年度条件付き採択後、ガバメントクラウド対応を進展	個社比率非公表／公開資料で確定不能	国内資本・国内基盤は主権性面で有利になり得るが、サプライチェーンまで審査されれば外国製機器等の説明が必要。 29

事業者	系統	日本での位置付け	日本クラウド市場シェアの目安	新制度上の主な論点
NTT系クラウド・DC	日本	国内大手DC・IT基盤	クラウド個社比率・DC全国シェアとも統一的公開値なし	国内運用、設備調達、子会社・海外運用体制の説明が中心
KDDI / Telehouse	日本	国内外DC運営	同上	グローバルDC網と日本ワークロードの分離、運用アクセス
IJJ	日本	国内クラウド・ネットワーク・DC	同上	国内管理体制、設備・ソフトウェア供給網
Equinix	米国	日本でコロケーション/DCを展開	DC市場は容量・ラック・売上等の指標が混在し信頼できる統一シェアを算出困難	入居クラウドとは別に、DC運営主体として対象になるか
Digital Realty系	米国系	日本で大規模DCを展開	同上	外国支配、運用権、設備サプライチェーン
Alibaba Cloud	中国系	2026年6月に日本で5番目のDCを開設。東京でAI・クラウド基盤を拡張	公開統計で個社値なし。匿名統計の「その他」等に含まれるとみられ、低シングルディジット以下と推定するのが妥当だが確度は低い	「懸念国の影響」審査が報道通り導入されれば最も直接的な影響候補。日本国内保存だけでは十分でない可能性。 ³⁰
Tencent Cloud	中国系	東京リージョンを運営し、2025年には大阪を新たなクラウドリージョン、国内3番目のDCとして拡張すると公表	個社値非公表。低シングルディジット以下と推定、確度低	Alibabaと同様、所有・支配と外国法上の影響が主要論点。 ³¹
Huawei Cloud 等	中国系候補	サービス別に国内リージョン・再販・設備利用形態が異なるため個別確認が必要	信頼できる日本個社シェアを確認できず	日本国内に対象インフラを有するか、誰が運用・支配するかを個別判定すべき

ここで重要なのは、「中国資本であればサーバー所在地にかかわらず即不合格」「米国資本なら自動合格」という単純な制度になるとはまだ確認できない点である。日経報道上のキーワードは国籍そのものより「懸念国の影響」であり、政策目的から考えれば、**最終的な親会社、議決権、取締役、政府からの法的要求への拘束、特権管理者、暗号鍵、サブプロセッサ、機器サプライヤー**を合わせて評価する制度になる可能性がある。³²

Alibaba Cloudは、むしろ制度導入直前の2026年に日本投資を拡大しており、3月に4番目、6月に5番目の日本DCを開設している。このため政策が厳格に運用された場合、「日本国内に設備があること」と「日本側が安全保障上信頼できると認めること」が切り分けられる象徴的なケースになる。³³

なお、DC事業者の日本市場シェアについては、クラウド売上のような比較可能な公開統計を本調査では確認できなかった。DC市場では売上高、総受電容量、ITロードMW、ラック数、延床面積等の尺度が異なるため、これらを混せて「市場シェア〇%」とするのはかえって誤解を招く。このため上表では推測値を置かなかった。

知的財産業務への具体的影響

新制度で直接規制される可能性が最も高いのは安全保障上重要な「データ」であり、特許・商標・著作権等の権利そのものではない。しかし企業の知財活動は、権利化前の秘密情報を大量に生成・共有・保存するため、**実務上は典型的な高機微クラウドワークロード**である。

特に重要なのは、知財データを「知財部の文書」だけに限定しないことである。研究ノート、ELN、CAD、EDAデータ、ソースコード、AIモデル・学習データ、化合物情報、ゲノム、試験失敗データ、製造パラメータ、発明届、先行技術調査、FTO意見、ライセンス価格、M&Aの技術DD、訴訟ホールドデータまで含めてマッピングする必要がある。

知財ワークフロー	リスク	新政策との接点	主な実務リスク	推奨対策
特許出願・発明届	高	未公開発明が重要技術であれば経済安保・輸出管理と重なる	外国管理者アクセス、出願前漏えい、保全審査対象技術の不適切な国外共有	高機微発明を独立テナント化、国内保管、顧客管理鍵、外国管理者アクセス遮断、国外共同出願前の非公開制度・外為法チェック。JPOの特許出願非公開制度も別途確認する。 ³⁴
営業秘密管理	高	認証の有無が合理的管理措置の説明材料になり得る	過剰な共有、管理者権限、ログ不足が「秘密として管理した」証拠を弱める	秘密区分、need-to-know IAM、MFA、DLP、アクセスログ、ダウンロード制限、退職者即時剥奪、クラウド事業者にも秘密保持義務。METI指針に沿って運用証拠を残す。 ²²
データローカライゼーション	中～高	国内保存要件が将来導入される可能性。ただし新認証では未確定	「東京リージョン」でもバックアップ、サポート、テレメトリ、鍵、AI処理が海外へ出る可能性	保存先だけでなく、複製、DR、ログ、サポート、鍵、AI推論を含む「データ経路表」を作成。国内所在地だけを安全性の代理指標にしない。ガバメントクラウドの国内保管要件は参考になる。 ³⁵
IPライセンス	中～高	クラウド変更で第三者開示・地域制限条項に抵触し得る	ライセンサー秘密情報を未承認サブプロセッサに保存、AI学習への二次利用	「承認クラウド」「Permitted Recipient」「no training/no secondary use」「地域」「サブプロセッサ」の明文化、変更時の同意・通知。
共同R&D	高	研究セキュリティ・みなし輸出・重要技術管理と直接交差	相手方研究者、海外子会社、外国クラウド管理者への意図しない技術提供	パートナーDD、技術分類、プロジェクト専用環境、国・組織・個人別アクセス制御、定期アクセスレビュー。政府の研究セキュリティ手順書も相手方DDとリスクベース対策を求める。 ³⁶

知財ワークフロー	リスク	新政策との接点	主な実務リスク	推奨対策
NDA管理	中～高	認証外クラウドへの保存を「許可された第三者開示」と解釈できるかが問題化	NDAがクラウド・サブプロセッサを想定せず、形式的違反となる	CSPをPermitted Service Providerとして定義し、同等以上の秘密保持、目的外利用禁止、政府要求通知、削除・返還をフローダウン。
証拠保全	高	認証変更に伴うクラウド移行・終了が大量に発生すれば証拠毀損リスク	ログ消失、タイムスタンプ変化、メタデータ喪失、旧環境の自動削除	legal hold優先、移行前スナップショット、ハッシュ、WORM/immutable storage、チェーン・オブ・カस्टディ、旧ログの独立保管。政府クラウドでもログ保存・データ返還が要求されている。 ¹⁶
e-discovery / 国際訴訟	高	ローカライゼーションと外国訴訟上の開示要求が衝突し得る	米国訴訟等への提出時の越境移転、個人情報、営業秘密、アクセス不能	データ所在インデックス、収集API・エクスポート形式の契約保証、法的ホールド、PPC越境ルール確認、protective order等の訴訟戦略と連動。 ³⁷
知財紛争・侵害調査	高	ログの完全性・長期保持が立証能力を左右す	誰がいつ設計図・ソースを取得したか立証できない	IAM・監査ログを証拠資産として扱い、NTP時刻同期、改ざん防止、ユーザーIDの一意性、退職後も証跡保持。
生成AIを使う知財業務	高	AI APIの処理地域や学習利用がDC認証だけでは解決しない	未公開発明、クレーム案、FTO資料がモデル提供者へ送信される	enterprise/no-training設定、推論地域の指定、入力禁止カテゴリ、DLPゲートウェイ、承認モデルのみ利用。政府クラウドでも国外AI推論環境を国内本体から管理分離する設計が採られている。 ¹⁵

特許出願非公開制度との交差

特許出願非公開制度では、国家・国民の安全を損なうおそれのある一定の技術について、特許庁による第一次審査後、内閣府側の保全審査・保全指定につながる仕組みがある。また外国出願禁止の事前確認制度が存在する。³⁸

そのため、特に防衛、量子、半導体、先端材料、宇宙、サイバー、AI基盤等の案件では、発明届を受け取ってから出願するまでだけでなく、**研究データが発生した段階から「国外からアクセス可能か」を確認すべき**である。クラウド上に置いたことが直ちに「外国出願」になるわけではないが、外国人・外国法人への技術提供や国外アクセスについては外為法等の独立した評価が必要である。³⁹

営業秘密では「認証」より運用証拠が重要

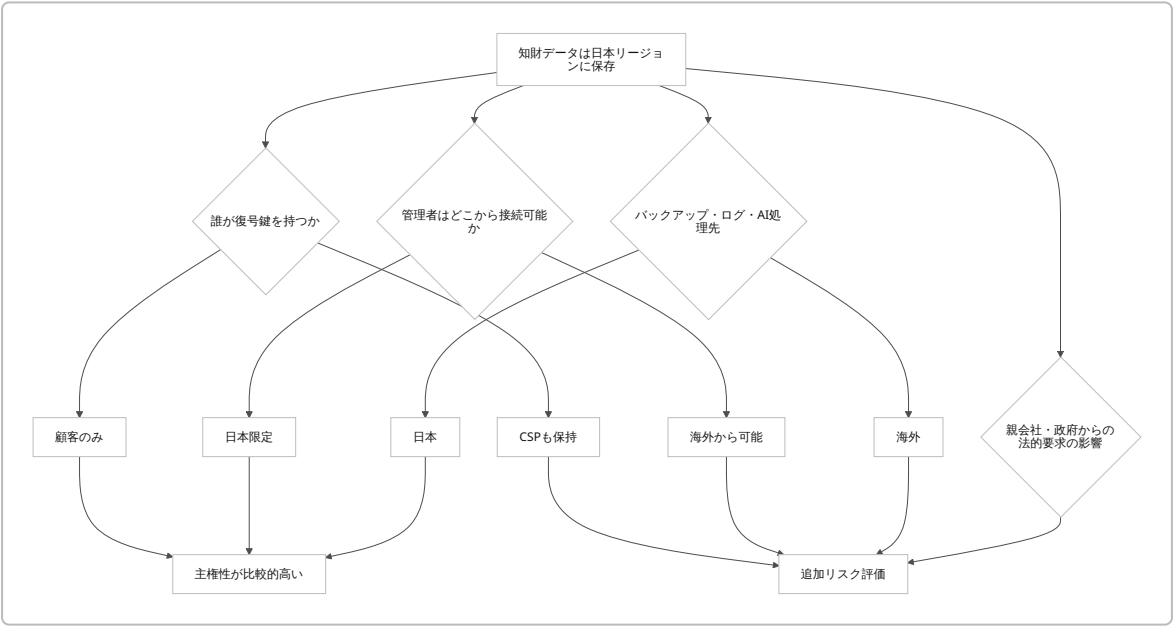
認証サービスを使えば営業秘密性が自動的に認められるわけでも、認証外サービスを使えば秘密管理性が自動的に失われるわけでもない。METIの営業秘密管理指針は法的保護を受けるための管理水準を示しており、重要なのは、対象情報を秘密として認識可能な形で合理的に管理した事実である。²²

ただし将来的には、「極めて重要な設計情報を、政府が高リスクと位置付けるクラウドに漫然と保管していた」という事実が、訴訟における管理合理性、取締役のリスク管理、契約違反等を評価する際の不利な事情として主張される可能性はある。この点は現時点の判例・法令上確立したルールではなく、**新しい政府安全基準が企業の“reasonable security”の事実上のベンチマーク化する可能性に関する分析**である。

「国内保存」だけでは知財保護にならない

個人情報保護委員会の越境移転ガイドラインが示唆するように、データ所在地と、そのデータに外国政府・外国事業者がアクセスできるかは別問題である。同ガイドラインは、外国政府による広範な情報収集を可能にする制度そのものを確認対象としている。 37

知財でも同様であり、



という評価が必要になる。「Japan Region」の表示だけでリスク評価を終えないことが新政策への最も重要な準備の一つである。

コンプライアンス、契約、コストと実務実装

ベンダー側に必要になると考えられる対応

正式な申請要領は未公表だが、報道内容とISMAP・ガバメントクラウドの現行要求から、ベンダーは少なくとも次の情報を迅速に提出できる状態にしておくべきである。これは「新認証の確定要件」ではなく、**認証準備用の推奨データルーム**である。 40

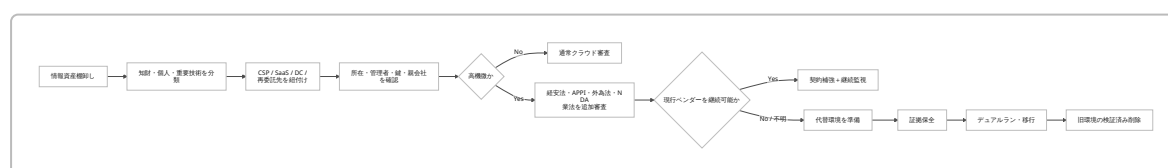
分野	準備すべき情報
法人・支配	最終親会社、議決権、主要株主、取締役、政府保有・政府影響、変更支配履歴
法域	親会社・運営会社に適用される法令、政府アクセス要求への対応方針
人員	特権管理者所在地、国・地域別サポート体制、アクセス承認プロセス
インフラ	国内DC一覧、リージョン・AZ、DR/バックアップ所在地

分野	準備すべき情報
ハードウェア	サーバー、ネットワーク、BMC、ストレージ等の主要供給元
ソフトウェア	ハイパーバイザー、管理プレーン、セキュリティ製品、重要サードパーティ
暗号	at-rest/in-transit、鍵保管、BYOK/HYOK、HSM、鍵アクセス者
ログ	管理者アクセス、API、データアクセス、変更履歴、保持期間、改ざん防止
委託	サブプロセッサ、再委託、海外NOC/SOC、保守委託
事業継続	RTO/RPO、災害時切替、サービス終了・顧客移行支援
保証	ISMAP、ISO 27001/27017/27018、SOC等の取得範囲

既存ガバメントクラウド調達では、サードパーティ製品について製品・製造企業の一覧、第三者監査、提供事業者自身の責任が求められており、また暗号・鍵管理、ログ、脆弱性対策、国内複数地域での災害対策、データ消去等も要件化されている。したがって、ここで挙げた項目の多くは純粋な推測ではなく、政府が既にクラウド調達で重視している統制である。 41

顧客側のコンプライアンス手順

企業側では、クラウド事業者の「認証取得予定」という営業説明だけに依存せず、次のプロセスを内部統制として固定化するのが望ましい。



知財部・法務部・外部弁護士向けチェックリスト

チェック	社内知財・法務	外部弁護士・弁理士
☐ 未公開発明、営業秘密、訴訟資料の保存先を特定	DMS、ELN、Git、Teams/Slack、SaaSまで含める	ヒアリング項目・データマップをレビュー
☐ Alibaba/Tencent等を含む全CSPを棚卸し	直接契約だけでなくSaaSの下層クラウドも確認	契約・DPA・subprocessor listを確認
☐ 親会社・支配・リージョン・管理者所在地を確認	ベンダー質問票を統一	外国法・政府アクセス論点を整理
☐ 高機微発明に「国外管理者アクセス禁止」を適用	IT/CISOとポリシー化	特許出願非公開・外為法との関係を案件別助言
☐ 共同研究環境をプロジェクト単位で隔離	PI・研究部門と共同実施	研究契約、成果帰属、アクセス権を修正
☐ NDAテンプレートを更新	CSP、再委託、AI利用を明記	Permitted Recipient等の定義を整備
☐ 証拠保全ルールを移行手順より優先	litigation holdをIT変更管理に連携	訴訟案件ごとの保全範囲を指定

チェック	社内知財・法務	外部弁護士・弁理士
☐ ベンダー退出テストを実施	データexportと復元を実際に試験	契約上のtransition assistanceを確認
☐ AI利用を別レイヤーで審査	no-training、入力禁止情報を設定	AI利用規約・権利帰属・秘密保持を確認
☐ 認証制度公表時にギャップ分析	30日以内の再評価体制	新法令・省令・ガイドラインの法的評価

契約条項は「セキュリティ条項」だけでは足りない

今後のクラウド・DC契約では、最低でも以下の条項を改訂すべきである。

条項	追加・変更すべき内容	知財上の意味
Certification	新安全認証、ISMAP等について取得・維持、取消・条件変更の即時通知	認証喪失を契約上のトリガーにする
Change of Control	最終支配者・主要株主・親会社変更を事前通知し、高リスク化時に解除可能	「契約時は安全だった」問題を防ぐ
Data Location	primary、backup、DR、logs、support copy、AI processingの場所を列挙	「本体だけ日本」を防止
Privileged Access	特権アクセス可能国・人員を限定。高機微領域は日本限定を選択可能に	営業秘密・重要技術への外国アクセスを制御
Encryption / Keys	顧客管理鍵、BYOK/HYOK、鍵へのCSPアクセス条件	データ所在より強い技術的主権
Government Requests	法令上許される最大限の事前通知、要求範囲の限定・争い、透明性報告	秘密情報が秘密裏に取得されるリスクを低減
Subprocessors	一覧開示、重要変更の事前通知・異議権、同等義務のflow-down	再委託先による抜け穴を防ぐ
No Secondary Use / AI Training	顧客データを広告、モデル学習、サービス改善に使用しない	未公開発明・著作物の目的外利用を防止
Audit / Evidence	SOC等に加え、重大事案時の追加証拠・ログ提供権	営業秘密訴訟・インシデント調査
Log Preservation	通常保持期間＋legal hold発生時の保存停止禁止	e-discovery・侵害立証
Portability	標準形式、API、メタデータ、ACL、ログを含めてexport	ベンダーロックインを軽減
Deletion	本番、複製、backup、cacheまで削除し証明書交付	NDA終了・ライセンス終了への対応
Regulatory Exit	認証喪失、新法令、当局指示時に違約金なしで移行	今回の制度変更に直接対応

条項	追加・変更すべき内容	知財上の意味
Transition Assistance	6～18か月等、案件に応じた移行支援、並行運用	認証変更時の事業継続
Egress Fees	規制変更による退出時のデータ搬出費を減免・上限設定	突発的移行コストを抑える
Indemnity / Liability	秘密保持・セキュリティ違反を通常の低い責任上限から除外又は別上限	知財損害と通常SLA損害を区別

高機微案件では、例えば次の趣旨を契約に入れることが考えられる。

規制変更・認証喪失条項の例（概念案）

本サービスが、日本国の法令、行政上の認証制度若しくは監督上の要請により、顧客が指定する重要情報の保存又は処理に適さないものとなった場合、又は当該サービスに係る必要な認証が停止・取消し・失効した場合、顧客は違約金なく当該ワークロードを終了し、提供者に対して合理的な移行支援、データ・メタデータ・監査ログの移転及び移転完了後の検証可能な消去を求めることができる。

実際の文言は契約準拠法、規制業種、標準約款との優先順位等に応じて調整が必要だが、「**認証取得を保証させる**」だけでなく、「**取得できなかった／失ったときどう逃げるか**」まで契約で設計することが本質である。

コストへの影響

制度要綱も認証料金も未公表であるため、現段階で認証コストを金額推計するのは適切でない。しかし費用項目はかなり予測できる。

ベンダー側では、第三者監査、企業・サプライチェーン情報管理、国内運用要員、特権アクセス分離、ログ・監視、国内DR、鍵管理、セキュリティ認証、外国本社との運用分離が主な増分費用となる。既存のガバメントクラウド仕様が305項目の技術要件等を設定し、サードパーティ監査や複数の外部保証を要求していることから、高保証クラウドへの適合は単純な書類審査にとどまらない。¹⁵

顧客側でより大きいのは、認証料金ではなく**移行コスト**である。データ搬出、ネットワーク再設計、IAM再構築、鍵再生成、アプリケーション改修、検証、二重利用期間、e-discovery証拠保全、ベンダー退出費、教育、契約再交渉が重なる。政府のガバメントクラウド調達サービス終了時の長い事前通知、移行可能性、データ返還・消去を明示しているのは、このスイッチングコストが実務上重大だからである。¹⁷

市場全体では、認証対象サービスが少数に絞られれば競争低下による価格上昇圧力が生じ得る一方、国内クラウド、ソブリンクラウド、暗号鍵管理、セキュリティ監査、国内DCには需要増が見込まれる。これは政策文書が国内クラウド/DCを成長・経済安全保障の双方から強化しようとしている方向とも一致する。⁴²

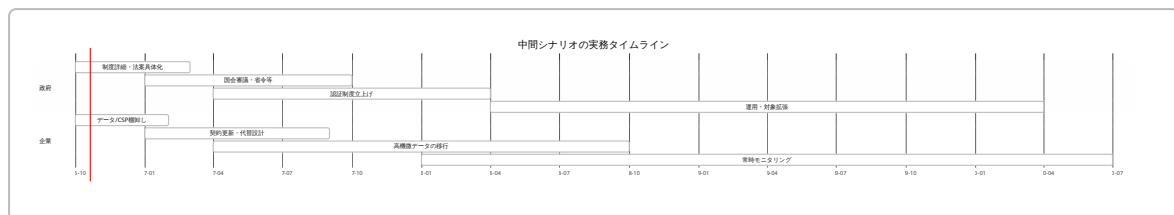
シナリオ分析と優先提言

以下は政府予測ではなく、2026年10月20日時点の公表情報を前提にした実務シナリオである。

中間シナリオ

最も実務計画に使いやすい基準ケースである。

2027年通常国会で安全保障上重要な個人機微データに関する制度が法制化され、2027年度以降に総務省・経産省がDC・クラウド認証を開始する。最初から全企業を義務付けるのではなく、金融・医療等の高機微分野で認証利用を強く推奨し、監督官庁・取引先の調達要件を通じて実効性を持たせる。これは日経報道と、政府が現在「必要な措置」を検討している状態を組み合わせたシナリオである。 43



この場合、中国系サービスは一般的なゲーム、EC、配信等ですぐ全面禁止されるのではなく、まず高機微ワークロードから採用しにくくなる可能性が高い。他方、AWS/Azure/Google等の米系大手も、外国法・管理アクセスに関する追加説明や「日本向け主権型」統制を求められる可能性がある。

最良シナリオ

政府がISMAP、ISO等との相互利用を広く認め、重複監査を避け、認証基準を国籍ベースではなく透明なリスクベースとし、十分な経過措置を設定する。既存契約には12～24か月程度の実務的な移行期間が認められ、顧客管理鍵、国内管理者、国内バックアップ等のリスク軽減策によって外国系事業者も認証可能になる。

この場合、企業への追加負担は比較的限定され、2027～2029年に通常のクラウド刷新サイクルと合わせて対応できる。DFFTを維持しながら高機微ワークロードだけを強化するため、国際共同R&DやグローバルIP管理への悪影響も抑えられる。デジタル庁がデータセキュリティを「制度・技術・運用」の組合せで検討してきたことや、政府研究セキュリティ手順書がゼロリスクを求めず合理的なリスク管理を志向していることから、政策的には十分あり得る設計である。 44

最悪シナリオ

認証で「懸念国の影響」を非常に広く解釈し、親会社法域、設備原産国、海外管理者アクセスまで厳格に制限する一方、経過期間が短く、金融・医療だけでなく重要インフラ・先端R&D・政府補助研究にも急速に利用条件が拡張されるケースである。

この場合、2027～2028年に大規模なクラウド移行が集中し、国内認証済み容量の逼迫、価格上昇、アプリケーション再設計、契約解除紛争、データ搬出費、ログ喪失等が同時発生し得る。中国系事業者だけでなく、米欧系サービスでも管理プレーンや外国サポートを分離できないサービスが一部使いにくくなる可能性がある。知財部門にとって最悪なのは、期限を優先した移行によって営業秘密のアクセス権、Git履歴、メールメタデータ、監査ログ、訴訟ホールド資料を破壊することである。

日本企業・知財実務家への優先提言

最優先は「中国系を使っているか」という質問ではなく、「高機微知財データを、誰が実質的に支配できるクラウドに置いているか」を把握することである。2026年以内に、未公開発明、営業秘密、重要技術、個人機微情報、共同R&D、訴訟資料について、CSP、リージョン、バックアップ、特権管理者、鍵、サブプロセッサ、最終親会社を1枚のデータマップに落とすべきである。政府の政策方向は既に十分明確であり、正式な認証項目を待つ必要はない。 45

次に、2027年以降まで続くクラウド契約には必ず「規制変更時の退出可能性」を確保するべきである。新認証の要件を満たせなかったとき、違約金、最低利用額、巨額のegress fee、独自形式によって移行不能になる

契約は避ける。政府自身のクラウド調達が移行支援、データ返還、消去、サービス終了通知を要求している点は、民間契約でも有力なベンチマークである。 17

特許・営業秘密案件は、通常の個人情報分類とは別に「IP-critical」分類を設けるべきである。 個人情報を含まない半導体設計データや製造レシピはAPPI上の個人データではなくても企業価値・経済安全保障上は極めて重要である。営業秘密管理指針、技術流出対策ガイダンス、研究セキュリティ、外為法を統合した分類が必要である。 46

中国系クラウド上の高機微ワークロードについては、「即時全面撤退」ではなく「新規投入停止+出口準備」が合理的な暫定策である。 現時点では法的禁止は成立していないが、Alibaba CloudやTencent Cloudのように日本国内インフラを拡大している中国系サービスは、日経報道通りの「懸念国影響」基準が採用されれば認証上の不確実性が特に高い。新規の5～10年契約や移行困難な知財基盤を積み増す際は、少なくとも認証結果が判明するまでexit rightを必須条件とするべきである。 47

外部弁護士・弁理士も自らのIT環境を点検すべきである。 顧客側だけを審査しても、法律事務所・特許事務所のDMS、メール、e-discovery、翻訳、AI要約、データルームが別の高リスククラウド上にあれば意味がない。今後は、顧客のベンダーセキュリティ質問票に、事務所が利用するCSP、AI、データ所在地、サブプロセッサ、ログ保持まで問われることを前提にした方がよい。

証拠保全はクラウド移行より先に行う。 規制対応の移行プロジェクトが始まった時点で、係争・ライセンス監査・従業員退職・営業秘密流出調査中のデータにlegal holdをかけ、ログ、メタデータ、ACL、ハッシュを含めて保存する。移行後にファイル本体だけ残っても、アクセス履歴が失われれば営業秘密侵害の立証力が大きく落ちる。

最後に、「認証取得済み＝知財安全」としない。 認証は基盤事業者の一定水準を確認するものにすぎず、ユーザー企業自身のIAM設定、共有リンク、API鍵、Git権限、AIへの入力、研究者アカウント管理、NDA運用まで保証しない。ISMAPを含む既存制度でもクラウドには利用者と提供者の責任分界が存在するため、知財保護は認証、契約、技術統制、人的運用を組み合わせる必要がある。 48

主要一次資料・参考URL

日本経済新聞（対象記事）

「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
<https://www.nikkei.com/article/DGXZQOUA171BY0X11C26A0000000/>
記事の主要内容は日経公式SNSおよび関連報道でも確認できる。 49

内閣府「経済安全保障法制に関する有識者会議（第18回）」2026年10月16日

https://www.cao.go.jp/minister/2609_k_onoda/photo/2026_005.html
データセキュリティについて引き続き政府一体で検討することを明示。 11

内閣官房「経済安全保障の更なる推進に向けた提言」2026年1月30日

https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r8_dai15/teigen.pdf
DC・クラウドを含むデータセキュリティ検討の中核資料。 50

内閣官房「データセキュリティ制度の検討について」2025年12月4日

https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r7_dai13/shiryo9.pdf
重要データとDC・クラウド保護の問題設定を示した資料。 51

内閣官房「経済安全保障推進法改正に関する提言骨子（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

外国制度、事業実態、国際基準等を考慮する方向を示す。 52

内閣府「経済財政運営と改革の基本方針2026」2026年7月21日閣議決定

https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2026/2026_basicpolicies_ja.pdf

個人機微データ法制とDC・クラウド安全性確保を政府方針として明記。 53

デジタル庁「データセキュリティワーキンググループ」

<https://www.digital.go.jp/councils/data-security-wg>

2024～2026年の検討経緯と2026年3月の取りまとめ。 54

デジタル庁「ガバメントクラウド」

https://www.digital.go.jp/policies/gov_cloud

既存の高保証クラウド政策との比較に重要。 55

デジタル庁「令和8年度ガバメントクラウド調達仕様書」

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5107093b-7c29-4ffe-808b-6e39b5e0e5be/984ffd04/20251226_procurement_public_notice_specification_02-1.pdf

国内保存、ISMAP、ログ、暗号、サプライチェーン、データ返還・消去、移行等の具体的な政府要求。 41

ISMAP「制度案内」

https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010005

政府クラウドセキュリティ評価制度の目的、監査・登録構造。 56

個人情報保護委員会「外国にある第三者への提供編」

https://www.ppc.go.jp/personalinfo/legal/guidelines_offshore/

外国政府による情報収集制度を含む外国法制の確認義務等を整理。 37

経済産業省「営業秘密～営業秘密を守り活用する」

<https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html>

2025年改訂営業秘密管理指針等。 57

経済産業省「営業秘密管理指針」

<https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/r7ts.pdf>

秘密管理性等の法的保護要件の実務基準。 58

特許庁「特許出願非公開制度についてのQ&A」

<https://www.jpo.go.jp/system/patent/shutugan/hikokai/qa.html>

保全審査、外国出願禁止、事前確認等。 59

経済産業省「技術流出対策ガイドンス 第2版」

<https://www.meti.go.jp/files/900018891.pdf>

研究開発・共同研究・アクセス管理・技術流出対策を統合的に扱う。 60

内閣府「研究セキュリティの確保に関する取組のための手順書」

https://www8.cao.go.jp/cstp/kokusaiteki/integrity/yushikisha/guidelines_v1.pdf

国際共同研究におけるパートナーDD、重要技術流出防止、リスクベース管理。 61

金融庁「金融分野におけるサイバーセキュリティ対策」

<https://www.fsa.go.jp/policy/cybersecurity/index.html>

2026年のITレジリエンス、クラウド、サードパーティリスク管理を含む政策資料への入口。 62

厚生労働省「医療情報システムの安全管理に関するガイドライン 第7.0版」2026年6月

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

医療機関における最新の情報セキュリティ基準。 63

Alibaba Cloud「日本で5番目のデータセンター開設」2026年6月18日

<https://www.alibabacloud.com/en/press-room/alibaba-cloud-expands-ai-infrastructure-in-japan>

日本国内での中国系クラウド投資状況を確認できる一次資料。 64

Tencent Cloud「大阪クラウドリージョン／日本3番目のDC」2025年4月

<https://www.tencentcloud.com/dynamic/news-details/100667>

Tencent Cloudの日本インフラ展開を確認できる一次資料。 65

総合すると、今回の政策転換は「中国製サービス禁止」という一点よりも、日本企業が知財・個人情報・重要技術を置くデジタル基盤について、物理所在地だけではなく、所有・支配、外国法、管理者アクセス、暗号鍵、設備供給網まで含めた“データ主権の証明”を要求する方向への転換と評価するのが最も適切である。政府が最終基準をまだ公表していない以上、企業が今取るべき対応は特定ベンダーの機械的な排除ではなく、高機微知財データの可視化、出口可能性、暗号鍵主権、証拠保全、契約変更、共同研究アクセス統制を先行実装して、どの最終制度にも対応できる可逆的なアーキテクチャを作ることである。 66

1 12 13 14 27 32 40 43 51 国がデータセンターとクラウドに「安全認証」へ中国系締め出し ...
<https://note.com/hirokimiyano/n/nf106195bc922>

2 5 10 45 53 66 www5.cao.go.jp
https://www5.cao.go.jp/keizai-shimon/kaigi/cabinet/honebuto/2026/2026_basicpolicies_ja.pdf

3 15 16 17 28 35 41 調達仕様書
https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/5107093b-7c29-4ffe-808b-6e39b5e0e5be/984ffd04/20251226_procurement_public_notice_specification_02-1.pdf

4 22 46 57 営業秘密～営業秘密を守り活用する
<https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html>

6 9 44 54 データセキュリティワーキンググループ | デジタル庁
<https://www.digital.go.jp/councils/data-security-wg>

7 50 経済安全保障の更なる推進に向けた 提言
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r8_dai15/teigen.pdf

8 経済安全保障推進法及びJBIC法の一部改正案
https://www.sangiin.go.jp/jpn/shiryo/chousa/rippou_chousa/backnumber/2026pdf/20260430003.pdf

11 20 経済安全保障法制に関する有識者会議（第18回） - 内閣府
https://www.cao.go.jp/minister/2609_k_onoda/photo/2026_005.html

18 19 48 56 制度案内 - ISMAP概要
https://www.ismap.go.jp/csm?id=kb_article_view&sysparm_article=KB0010005

21 37 個人情報の保護に関する法律についてのガイドライン（外国に ...
https://www.ppc.go.jp/personalinfo/legal/guidelines_offshore/

23 34 38 59 特許出願非公開制度についてのQ&A

<https://www.jpo.go.jp/system/patent/shutugan/hikokai/qa.html>

24 39 安全保障貿易管理 ガイダンス [入門編]

<https://www.meti.go.jp/policy/anpo/guidance/guidance.pdf>

25 62 金融分野におけるサイバーセキュリティ対策について

<https://www.fsa.go.jp/policy/cybersecurity/index.html>

26 42 日本成長戦略（案）

https://www5.cao.go.jp/keizai-shimon/kaigi/minutes/2026/0721_shiryo01.pdf

29 55 ガバメントクラウド | デジタル庁

https://www.digital.go.jp/policies/gov_cloud

30 47 64 Alibaba Cloud Expands AI Infrastructure in Japan with ...

https://www.alibabacloud.com/en/press-room/alibaba-cloud-expands-ai-infrastructure-in-japan?_p_lc=1

31 65 Tencent Cloud Japan to Expand Support for Japan's Digital ...

<https://www.tencentcloud.com/dynamic/news-details/100667>

33 Alibaba Cloud Unveils New Datacenter and AI services in ...

https://www.alibabacloud.com/en/press-room/unveils-new-datacenter-and-ai-services-in-japan?_p_lc=1

36 61 www8.cao.go.jp

https://www8.cao.go.jp/cstp/kokusaiteki/integrity/yushikisha/guidelines_v1.pdf

49 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

<https://www.facebook.com/nikkei/posts/%E3%83%87%E3%83%BC%E3%82%BF%E3%82%BB%E3%83%B3%E3%82%BF%E3%83%BC%E3%82%AF%E9%87%91%E8%9E%8D%E3%82%84%E5%8C%BB%E7%99%82%E3%81%AA%E3%81%A9%E9%87%8D%E8%A6%81%E3%81%AA%E5%80%8B%1649418429862886/>

52 経済安全保障推進法改正に関する 提言骨子（データセキュリティ）

https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r8_dai14/teigenkosshi_6.pdf

58 営業秘密管理指針

<https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/r7ts.pdf>

60 技術流出対策ガイダンス 第2版

<https://www.meti.go.jp/files/900018891.pdf>

63 医療情報システムの安全管理に関するガイドライン 第7.0版（令 ...

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html