

データ主権の設計図

クラウド「安全認証」構想と知的財産防衛の最前線

調査基準日：2026年10月20日



1. Not Just “China Exclusion” (単なる中国排除ではない)

日経報道にある「安全認証」の真の狙いは国籍ではなく「データ主権」の回復である。サーバーが日本にあっても、外国法やサプライチェーンの支配下であればリスクと見なされる。



2. IP is the Ultimate Target (知財こそが最大の対象)

新制度が直接照準を合わせるのは「安全保障上機微なデータ」。特許出願書類だけでなく、R&Dデータ、ソースコード、ELNなどの「未公開の知財情報」が最も深刻な影響を受ける。



3. “Exit Rights” Before Migration (移行権の確保が急務)

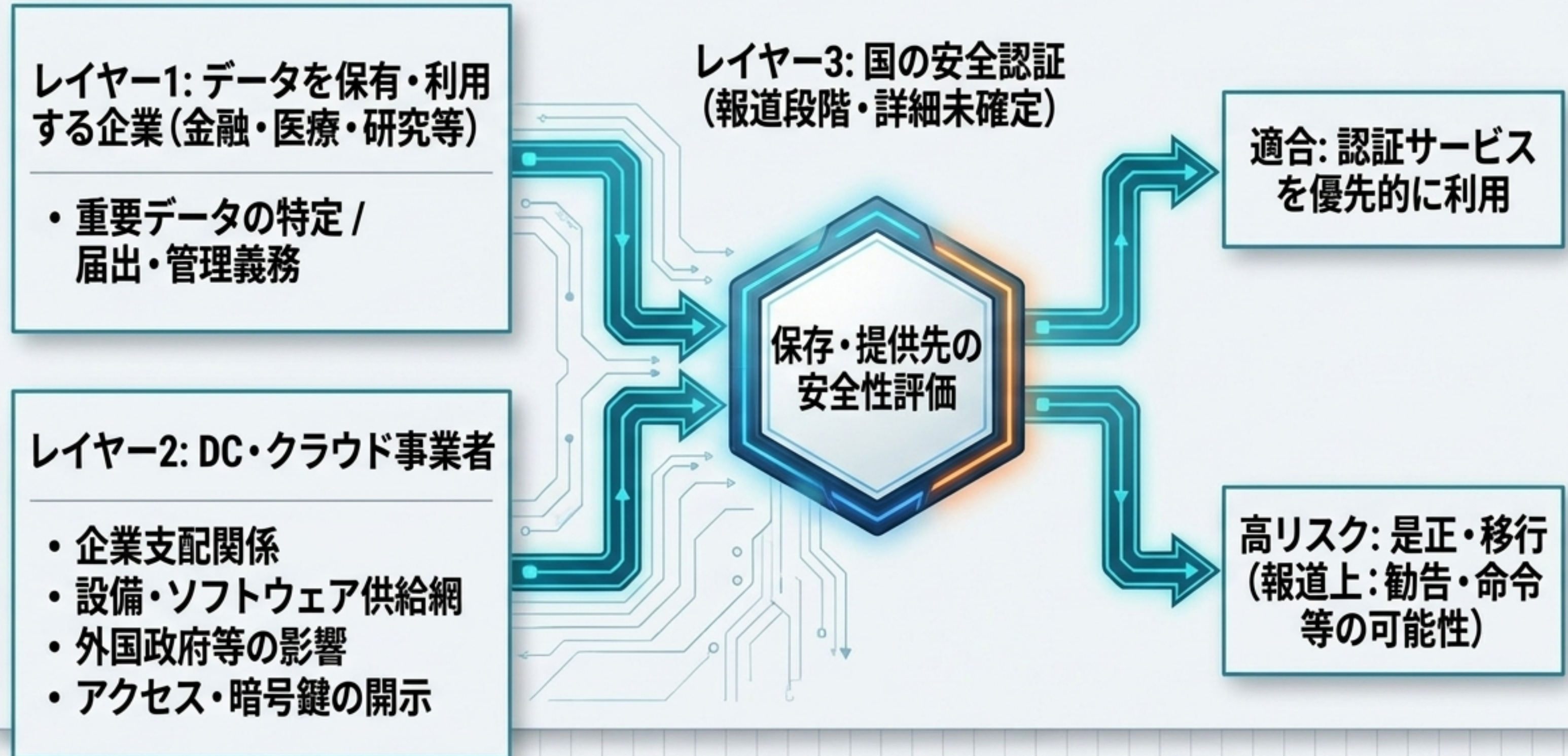
法案成立を待つて動くのでは遅い。今すぐ行うべきは、クラウド契約における「退出権 (Exit Right)」の確保と、既存ベンダーにおける暗号鍵・管理者アクセスの実態把握である。

Fact vs. Rumor: 報道と政府公式方針の境界線

項目	2026年10月20日時点 のステータス	根拠・実態
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」に安全性確保の必要な措置として明記。
国による「安全認証」 制度の創設	日経報道段階	10月19日の日経報道。政府の最終的な制度要綱や法令案は未公表。
企業情報、設備供給者、 懸念国の影響を審査	日経報道段階	報道上の審査項目。既存のISMAPやガバメントクラウドの要件から推測される方向性とは一致。
中国・ロシア系企業を 自動的に法定排除する	確認できず	国籍を名指しした法定基準は存在しない。「懸念国の影響」による事実上の排除は報道上の評価。
中国企業との契約を直ちに 解約する法的義務	誤解（現時点）	2026年10月現在で法的義務はない。ただし、取引先要件の先行厳格化リスクは極めて高い。

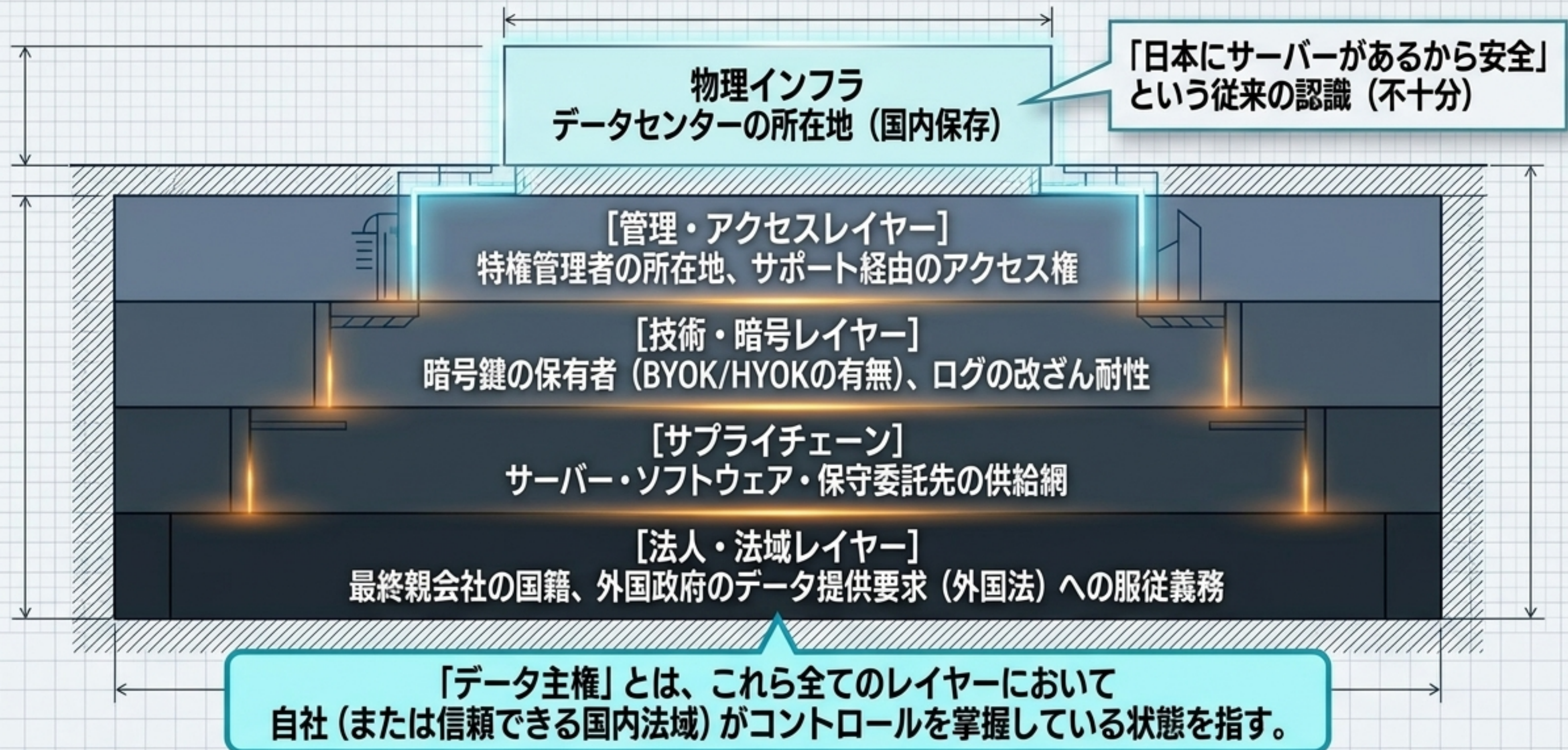
実務上の結論：即時違法化はされないが、規制・監督・取引先要求の連鎖により、高機微データにおいて「実務上使いにくい」状態に追い込まれるリスクが進行中。

Policy Architecture: 制度化に向けた三層構造



The Core Issue: 物理的所在地から「実質的データ支配」へ

政府が問題視しているのは、サーバーの住所ではなく「誰がデータに干渉できるか」である。



Timeline & Scenarios: 2027年施行に向けたシナリオ分析

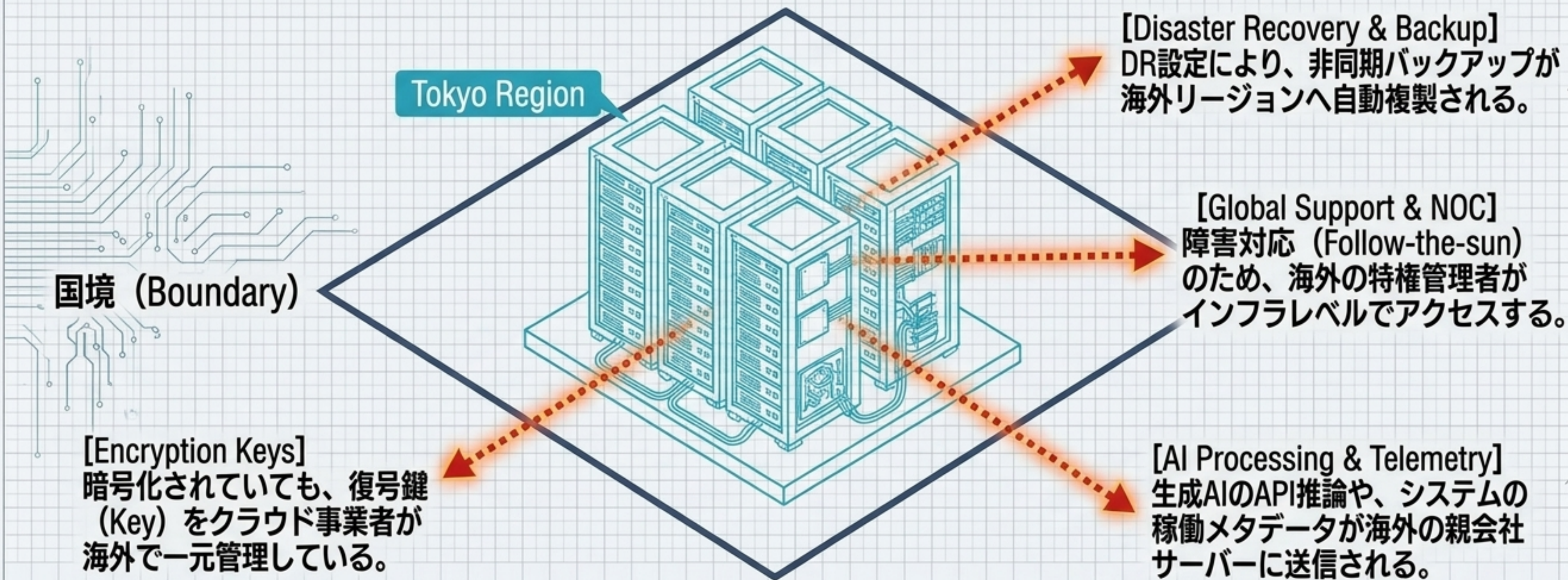


Vendor Landscape: 主要クラウド事業者の立ち位置と審査論点

事業者系統	市場シェア推定	新制度上の審査論点
米国系 (AWS / Microsoft Azure / Google Cloud)	寡占 (計 約66%以上と推定)	既存のガバメントクラウド実績は強み。焦点は「外国法 (米国法) の適用」「AI処理・サブプロセッサ経由のデータ流出」「国外からの管理アクセス」をどう遮断・評価するか。
日本系 (さくら / NTT系 / IJ)	国内資本としての優位性	法人支配やデータ主権の面では最も有利。ただし、インフラの「設備サプライチェーン (外国製機器)」まで審査が及んだ場合の説明責任が焦点。
中国系 (Alibaba Cloud / Tencent Cloud)	低シングルディジット以下 (推定)	最も直接的な影響候補。Alibabaは2026年に日本で5番目のDCを開設するなど投資を拡大中。「設備が日本にあること」と「政府が安全と認めること」が分離される象徴的ケースに。

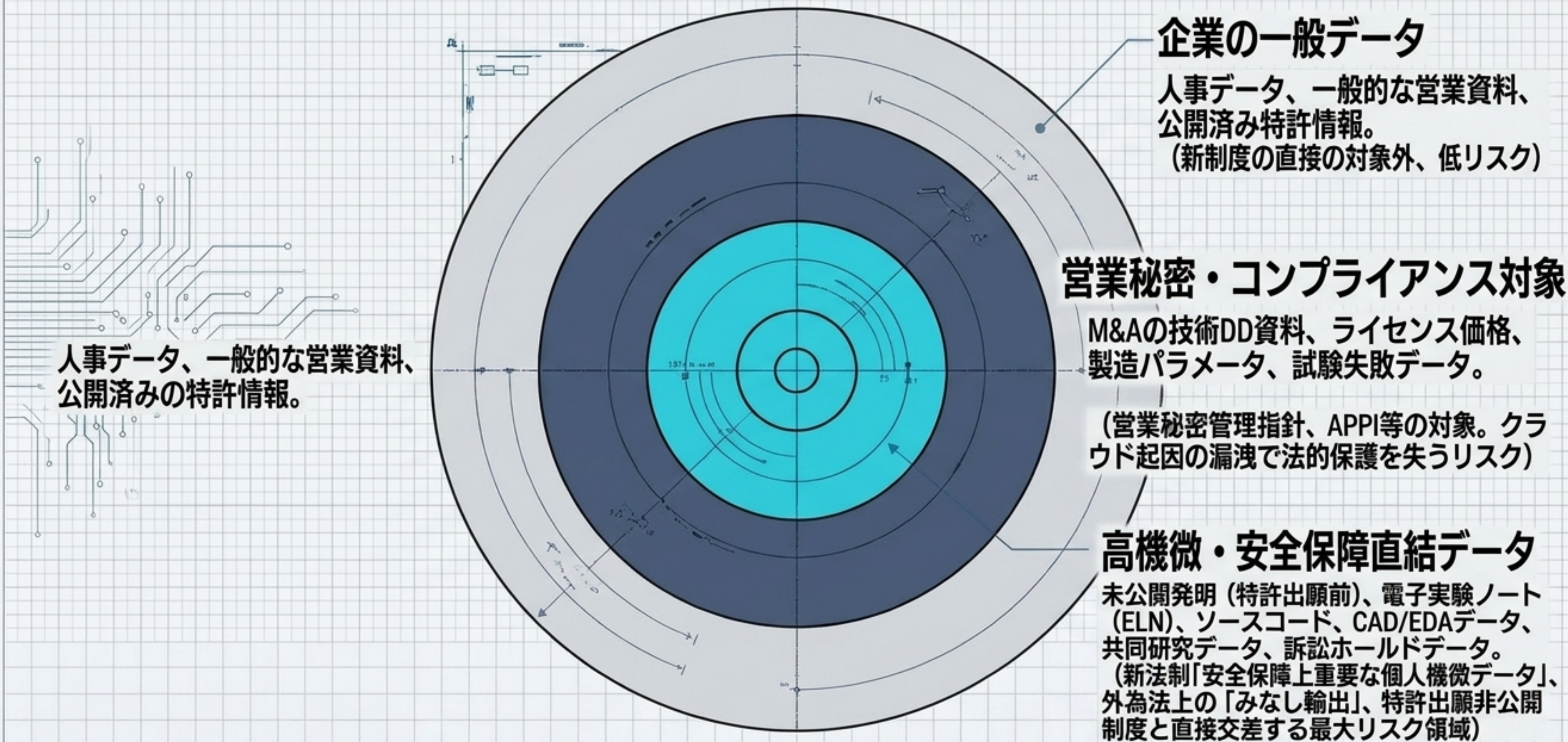
The “Japan Region” Fallacy: 国内保存だけでは知財を守れない理由

「データ保管場所＝日本」の設定のみでリスク評価を終えることは、新政策下では致命的な盲点となる。



契約書の「データ所在 (Data Location)」条項だけでなく、上記経路を塞ぐアーキテクチャ設計が必要。

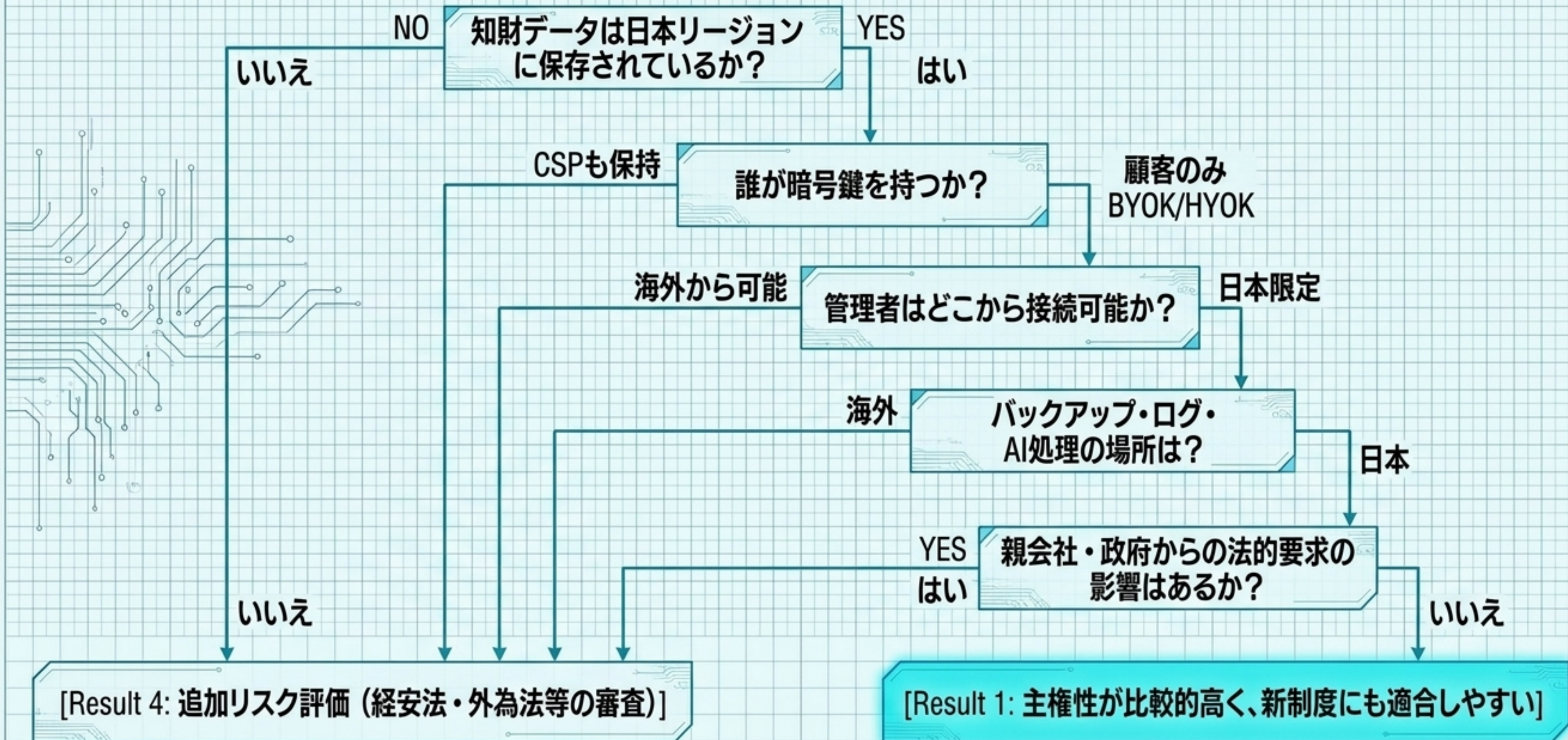
Why IP is the Ultimate Target: 「知財情報」は機微データの集積地



IP Workflow Risk Heatmap: 知財業務に潜むクラウド脅威

知財業務	リスク	実務リスクと対策
特許出願・発明届	高	リスク：出願前漏えい、保全審査対象技術（防衛・量子等）の不適切な国外共有。 対策：高機微発明の独立テナント化、国内管理者限定、特許出願非公開制度との照合。
共同R&D	高	リスク：相手方研究者や海外子会社を通じた「みなし輸出」・重要技術流出。 対策：プロジェクト専用環境での隔離、国籍別アクセス制御、研究セキュリティガイドラインへの準拠。
証拠保全 (e-Discovery)	高	リスク：認証変更に伴うクラウド強制移行時における、監査ログの消失やメタデータの毀損。 対策：リーガルホールドの優先適用、移行前のスナップショット・ハッシュ取得、WORMストレージ利用。
生成AI利用	高	リスク：AI API経由で未公開発明やクレーム案がモデル提供者（海外）へ送信・学習利用される。 対策：Enterprise/no-training設定の徹底、DLPゲートウェイの導入。
NDA管理・ライセンス	中/高	リスク：未認証クラウドへの保存が「許可された第三者開示」に違反するリスク。 対策：CSPをPermitted Service Providerとして定義し、政府要求時の通知義務をフローダウン。

Diagnostic Flowchart: 知財データの主権診断ツリー



The "Exit Right" Imperative: クラウド契約の再設計

単に「ベンダーに認証取得を保証させる」だけでなく、
「認証を失効した際にどう安全に逃げるか」の設計が本質である。

従来の契約 (Before)

- データ所在：「原則として」日本に保存
- 暗号化：業界標準のアルゴリズムで暗号化
(鍵はCSP管理)
- 解除条項：重大なセキュリティ違反時の解除
- 責任上限：通常のSLAに基づく低い責任上限

今後必須となる特約条項 (After)

- [Regulatory Exit] 規制変更や認証喪失時に、
違約金なしでクラウドを移行できる権利。
- [Egress Fees & Transition] 退出時のデータ搬
出費 (Egress Fee) の減免・上限設定、および
6～18ヶ月の並行運用・移行支援 (Transition
Assistance)。
- [Privileged Access] 高機微領域へのアクセスを
日本国内・特定要員に限定する条項。
- [Audit & Evidence] 重大事案時の追加証拠・ロ
グ提供権、移行前のデータ完全消去 (Deletion)
の証明書交付。

Immediate Action Plan: ベンダーDDと内部統制のチェックリスト

Track 1: Vendor Due Diligence (推奨データルーム要求)

クラウドベンダーの「営業トーク」に依存せず、以下を書面・実態として要求する。

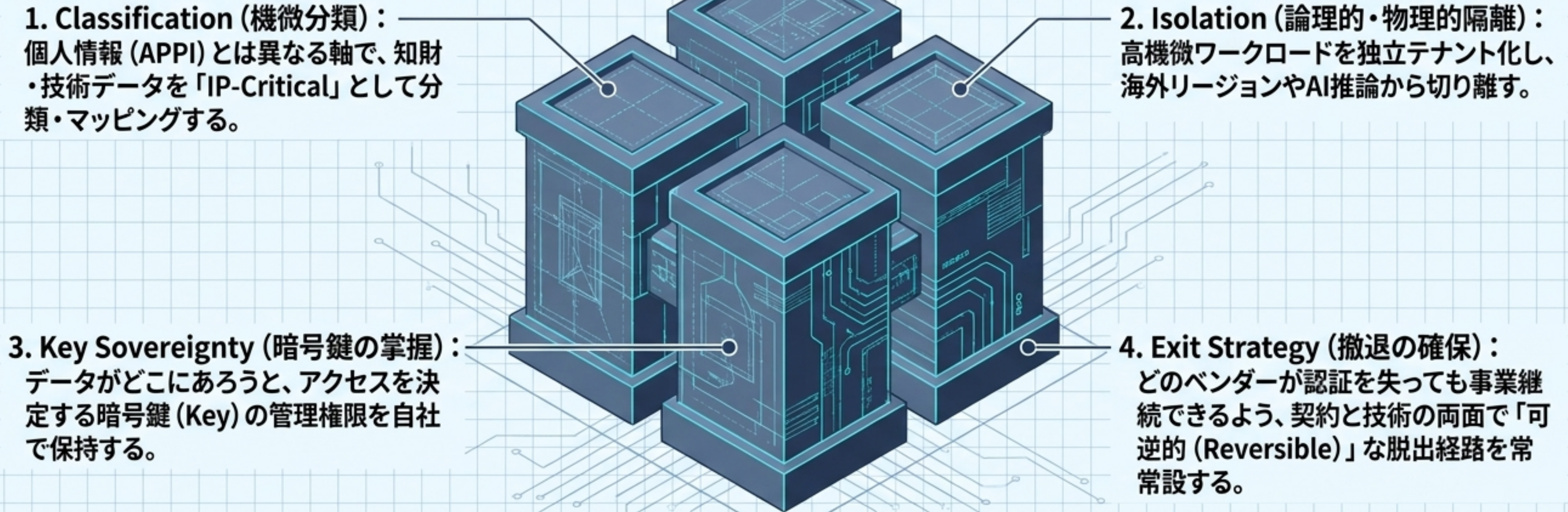
- [法人・支配] 最終親会社、議決権、外国法適用方針、政府アクセス要求への対応履歴
- [インフラ] サブプロセッサ一覧、海外NOC/SOCの有無、バックアップの物理所在地
- [暗号・ログ] BYOK/HYOKのサポート状況、ログの保持期間・改ざん防止機能

Track 2: Internal Compliance (知財・法務・外部弁護士)

- [情報資産の棚卸し] DMS、ELN、ソースコード管理ツール、SaaSを下層クラウドまで紐付けマップ化。
- [証拠保全の先行] 移行プロジェクト始動前に、係争・調査中データのリーガルホールド（メタデータ・ログ確保）を実行。
- [外部専門家の点検] 依頼する法律事務所・特許事務所が使用するクラウドやAI要約ツールの安全性を確認。

Synthesis: 真のデータ主権を確立する4つの原則

「認証取得済み＝知財安全」ではない。認証はインフラのベースラインに過ぎず、最終的な防衛線は企業自身のアーキテクチャ設計に依存する。



安全認証制度の最終確定を待つ必要はない。この4原則の先行実装こそが、あらゆる規制シナリオに耐えうる唯一の防衛策である。