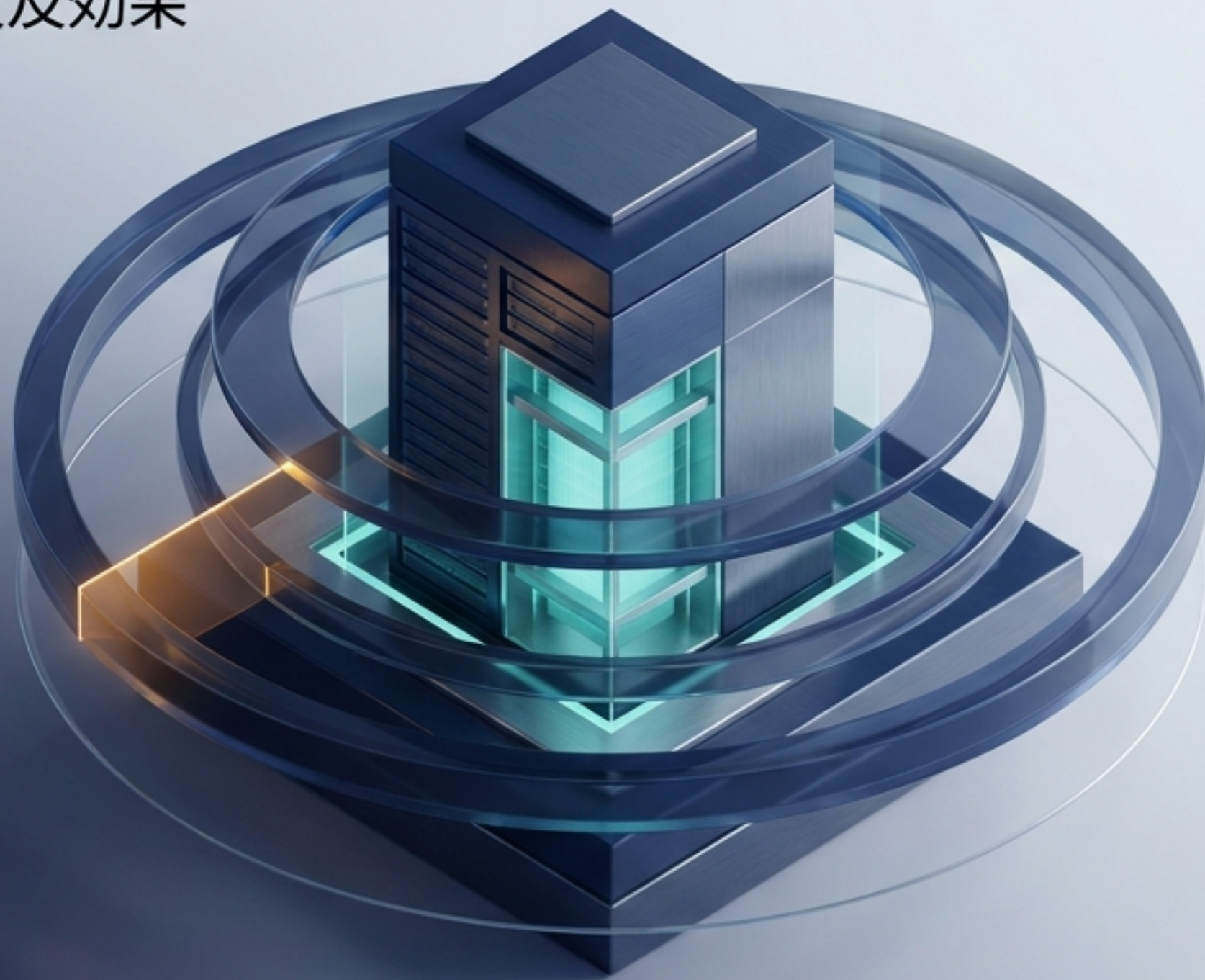


経済安全保障と知財インフラの再構築

データセンター・クラウド安全認証がもたらす「間接的排除」のメカニズムと
知財・R&D部門への波及効果



対象読者：知財部門長、法務・コンプライアンス責任者、R&D戦略担当者



震源地：2027年導入に向けた新認証。金融・医療等の「重要な個人情報」を扱うクラウド・DC事業者が対象。



排除のメカニズム：「国籍」ではなく「支配関係・設備調達先・準拠法」の審査により、中国国家情報法法等の影響下にある事業者を事実上排除。



知財への波及：知財情報は直接の対象外だが、SaaSベンダーの基盤移行を通じて、知財インフラの事実上の標準（デファクト・スタンダード）へと連鎖する。



最優先課題：知財SaaSの基盤IaaS・再委託先を含む「ベンダー台帳」の構築と、**生成AIの入力情報の区分ルール**の策定（0～6ヶ月以内）。

報道のシグナルとノイズを分離する

政府公表資料等による事実

内閣官房有識者会議（2025年12月～26年1月）による「大量データの防護」と「サプライチェーン審査」の提言。

2026年3月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、「積み残し課題」となっている。

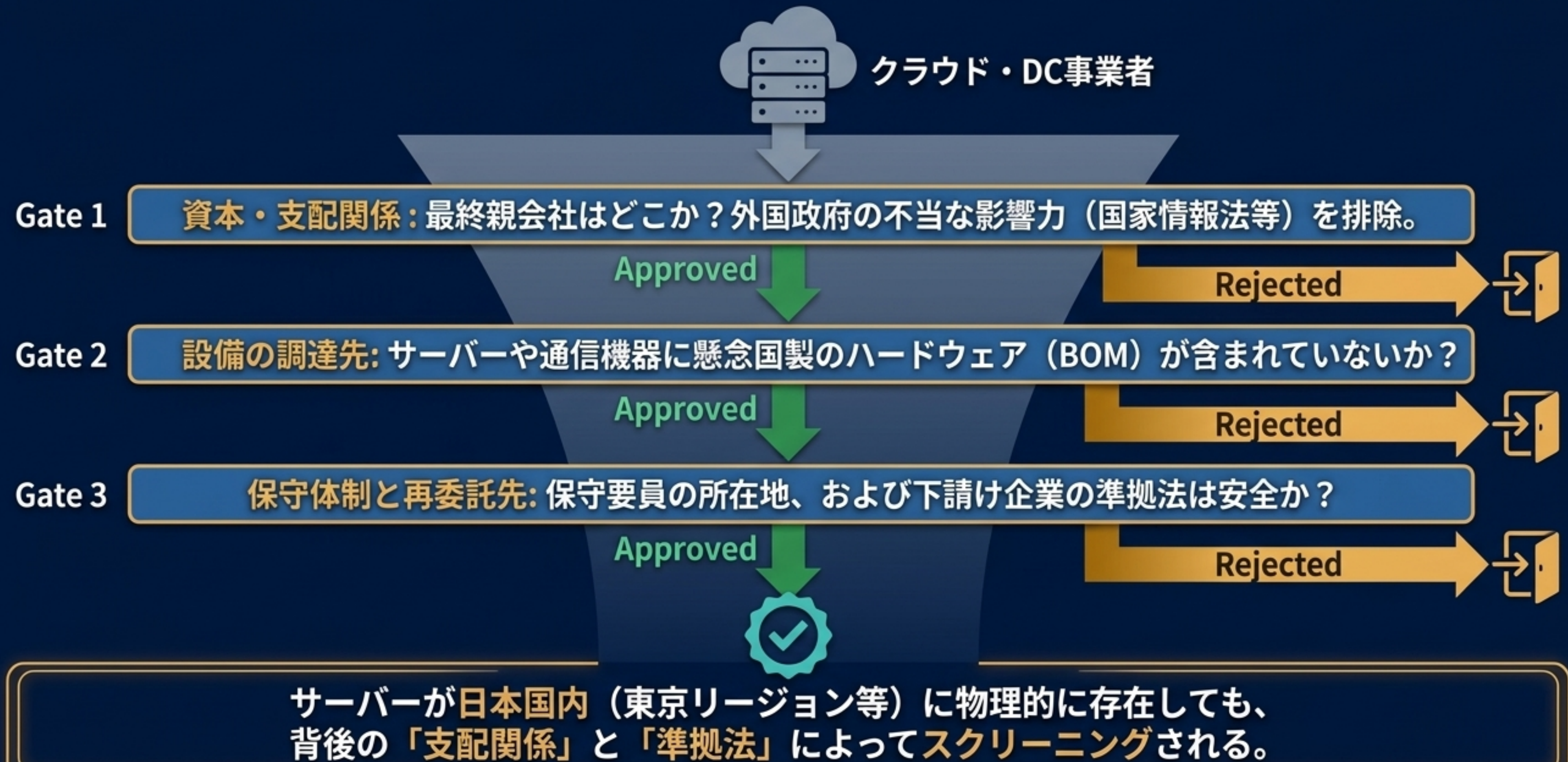
日経報道等による未確定情報・推測

「2027年度以降」という具体的な導入時期。

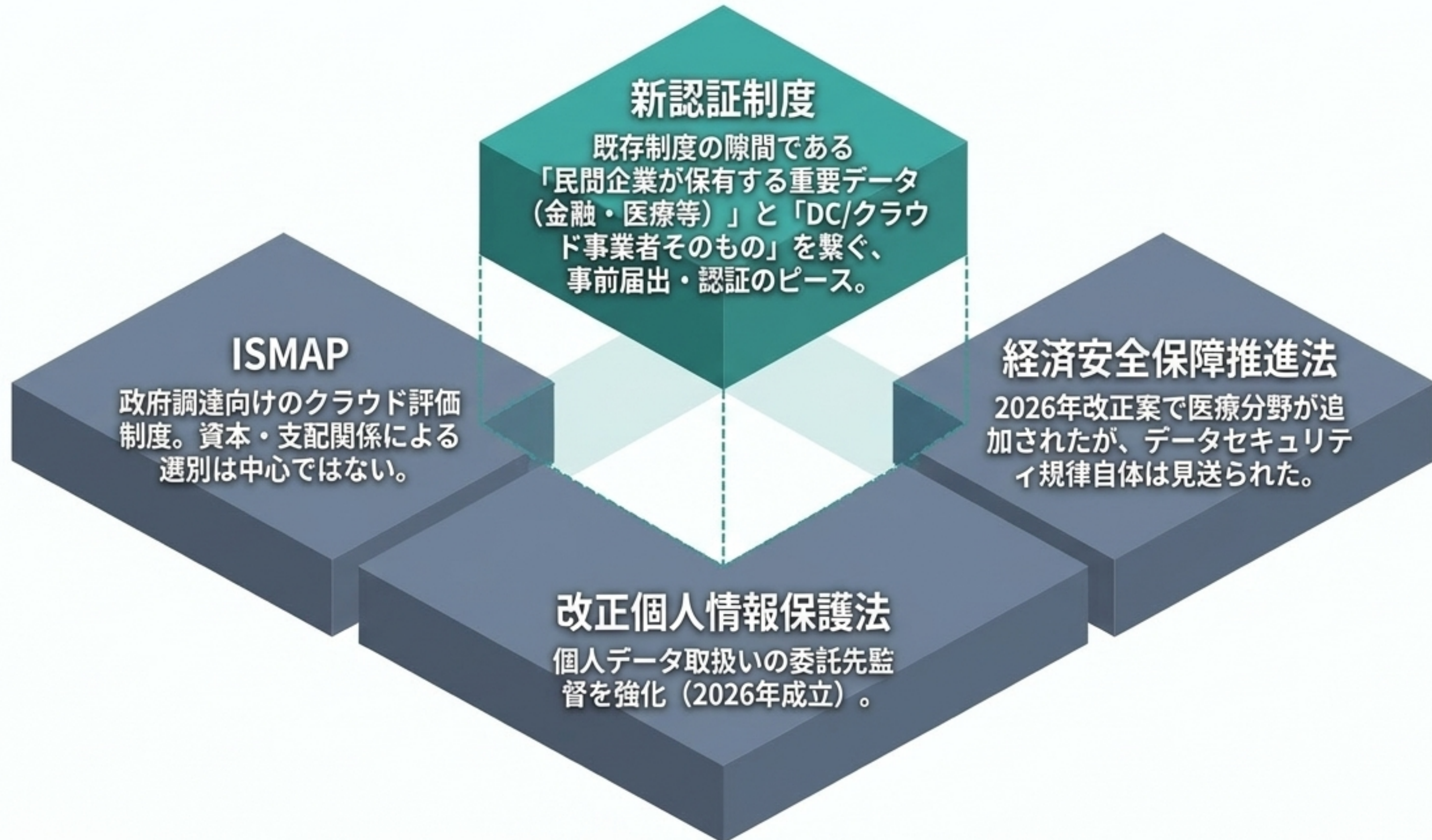
IPAの「JC-STAR（IoT製品セキュリティラベル）」を参考にするという運用方針。

中国系事業者の「事実上排除」という明確な意図（政府は国籍による明示的排除を否定）。

WTO違反を回避する「間接的排除」のメカニズム



日本のデータ・セキュリティ法制における「空白地帯」を埋める



主要国のクラウド・セキュリティ規制アプローチの比較

米国	【アプローチ】 事後的・個別審査型 / 直接的排除（FCC等）。	【対象】 事業者・機器単位での明確な取引禁止・制限。
EU	【アプローチ】 段階的・公共調達重視。	【対象】クラウド・AI開発法（CADA）案等による、主権保証レベルに応じた選別。
日本 - 新認証	【アプローチ】 事前認証型 / 間接的排除。	【対象】 民間向けの任意認証（金融・医療等の重要データ保有者への利用促進）。

日本のアプローチは通商摩擦（WTO違反等）を最小化する設計だが、その分、民間企業の「自己責任によるデューデリジェンス」の負担が極めて重くなる。

知財部門への波及：なぜ技術情報が規制の影響を受けるのか？



震源地:

政府が「重要な個人情報（金融・医療）」を対象にクラウド認証を要求。技術情報・営業秘密は法的的な直接対象外。

IT基盤の移行:

大手SaaSベンダーは、金融・医療等の優良顧客を維持するため、自社の基盤IaaSを「認証済みクラウド」へ強制的に移行・適合させる。

知財インフラへの連鎖:

知財部門が利用する特許管理SaaS、文書管理ツール、AIツールも同じ基盤に乗っているため、結果として新認証が知財インフラの「事実上の標準（デファクト）」となる。

影響ゾーン1：知財SaaSとクラウド調達の隠れたリスク



知財管理SaaS・期限管理ツール（表層的なISMAP・ISO取得の確認のみ）。

基盤IaaS層。SaaSベンダーが背後で利用しているクラウド基盤（例：アリババクラウド等の外国資本クラウドの混入リスク）。

再委託先・保守拠点・準拠法。データが日本国内にあっても、海外の保守要員がアクセス可能な場合、外国法（国家情報法等）の影響下に置かれる。

SaaSベンダーの監査において「基盤層まで遡った検証（ピアシング）」が必須となる。

影響ゾーン2：生成AI（LLM）利用における準拠法リスク

個人情報保護委員会によるDeepSeekへの注意喚起（2025年2月）に基づくリスク分離。



「中国の法令が及ぶクラウド・AIに未公開発明を入力しない」ことが業界標準となる。

影響ゾーン3：対中オペレーションと特許DBのリスク衝突

外為法（FEFTA）による技術提供規制。
未公開技術の不用意な越境移転の制限。

データ越境移転規制と
サイバーセキュリティ統制。


Japanese
Headquarters


Chinese
Subsidiaries/
Agents

中国系特許DBや分析ツールでの検索。
検索式、ウォッチ対象、自社技術分
類の入力は「R&Dの方向性」を推知
させる未公開情報と同等。

共有情報を出願に必要な最小限に絞り、中国法が及ぶ事業者のツールでの
自社ポートフォリオのアップロードを回避する。

影響ゾーン4：特許出願非公開制度（秘密特許）への適合

背景：
2024年5月施行の特許出願非公開制度。適正管理措置ガイドライン(案)は、保管先サーバーを「特定区域」とすることを要求。



これまでの課題：
「外部クラウド利用時の相当性(セキュリティ対策、設置場所)」の明確な基準が存在しなかった。

新たな「データセンター・クラウド安全認証」が、保全対象発明を扱う電子環境における【適正管理措置のデファクト・スタンダード】として機能する。

IPランドスケープの転換：技術覇権の新たな主戦場

認証取得を目指す事業者にとって、以下の技術群が最大の差別化要因（知財・標準化の対象）となる。

機密計算
(Confidential Computing)

顧客による鍵管理
(BYOK / HYOK)

AI DC向け液冷技術・
ワット/ビット連携

サプライチェーンの真正性検証
(ハードウェアBOM / ファームウェア検証)

国内DC事業者や中国系通信機器メーカーの日本出願推移をIPランドスケープで監視し、自社技術の標準必須化の余地を探る。

即応プレイブック：短期アクションプラン（0～6ヶ月）

1



【可視化】

- ☑ 知財クラウド・AIベンダー台帳の構築。
- ☑ SaaSの運営主体だけでなく、最終親会社、基盤IaaS、データ所在国、準拠法、再委託先をピアシングして記録する。

2



【分離】

- ☑ 生成AI入力ルールの特文化。
- ☑ 情報区分（未公開発明、営業秘密 vs 公開情報）ごとに、中国法が及ぶAPI/クラウドへのデータ入力を原則禁止とする。

3



【契約更新】

- ☑ 調達要件の改定。
- ☑ ベンダー調査票に「支配関係」と「準拠法」の設定を追加し、契約条項に支配権変更時の通知義務と解約権を組み込む。

戦略的ホライズン：中期アクションプラン（2027年～）

2027年通常国会

Present



法制化の追跡：推進法改正案、認証基準案、パブリックコメントの監視。自社R&D（ゲノム・医療データ等）が「重要な個人情報の事前届出」の直接対象になるか法務と連携。

セキュア環境の構築：防衛・宇宙・量子等の保全指定可能性のある技術向けに、新認証クラウドを前提とした「特定区域」管理環境を事前準備。

地政学的対抗措置の想定：2026年1月の中国商務部によるデュアルユース輸出管理強化の先例を踏まえ、日本企業に対する中国国内での報復的なデータ規制強化・特許ライセンス制約に備える。

結論：次世代・知財インフラ防衛の3原則

隔離性 (Segregation)

データの機微度（未公開/公開）に応じた厳格なAI・クラウドの経路分離を徹底する。

透過性 (Visibility)

インフラの深層（基盤IaaS・準拠法・資本）までサプライチェーンを透視する。

予見性 (Anticipation)

2027年水準の安全認証を先取りし、秘密特許時代に耐える適正管理インフラを構築する。



経済安全保障は、規制への「対応」から、次世代R&D環境の「競争力」へとフェーズを移行した。