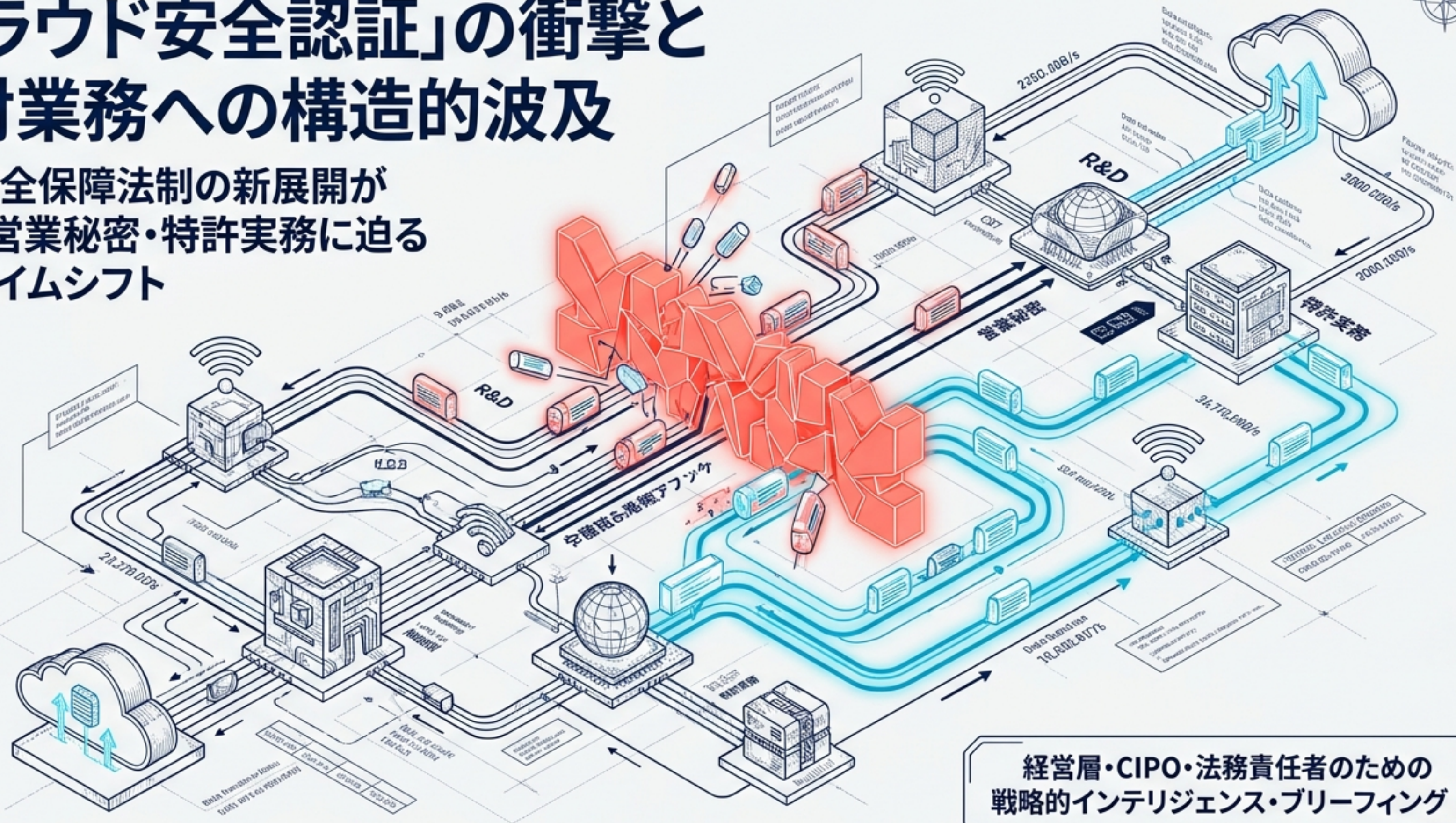


「クラウド安全認証」の衝撃と 知財業務への構造的波及

経済安全保障法制の新展開が
R&D・営業秘密・特許実務に迫る
パラダイムシフト



経営層・CIPD・法務責任者のための
戦略的インテリジェンス・ブリーフィング



データ主権への舵切り

単なるインフラセキュリティ基準の引き上げではない。国家が「個人機微データ」と「情報処理基盤」の主権的統制に乗り出した。



知財・R&Dの死活問題

未認証インフラへの依存は、発明の頓挫（第一国出願義務のコンフリクト）と営業秘密の喪失（秘密管理性の否定）に直結する。



サプライチェーンの再構築

「契約・技術・ガバナンス」の三位一体で、知財・法務部門主導の防壁構築（2026年即時着手）が必須となる。



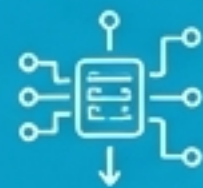
保護法益のパラダイムシフト

【既存の法体系】
個人情報保護法

個人の権利利益保護
(プライバシー)

【新制度の狙い】
データセキュリティ
法制

インフルエンス・
オペレーション
(影響力行使) およ
び諜報活動の阻止
(国家・国民の安全)



データ流出: 医療 (病歴)・金融 (債
務) 等の機微データが外国機関へ



弱みの抽出: AI等で特定標的 (研究
者・技術者) の弱みを特定



工作活動: ブラックメールや金銭的懐
柔によるヒューミント (人的諜報)



最終被害:
国家機密・最重要営業秘密の奪取



※実例: 住宅ローンや病気の子供を抱える対象者を狙った工
作や、通信会社・工作機械関連会社でのロシア通商代表部
員との共謀による営業秘密流出事案が発生。

三層構造の規律設計による特定国インフラの事実上排除メカニズム

第1層: データ保有・利用側

ゲノム・医療・金融の機微データ大量取扱
事業者に対する「事前届出」

第2層: データ保管・処理基盤側 (総務省・経産省)

国内立地DC・国内サーバーに対する4項目の安全
認証 (事業者情報、リスク管理体制、設備供給網、
懸念国[FOCI]影響有無)

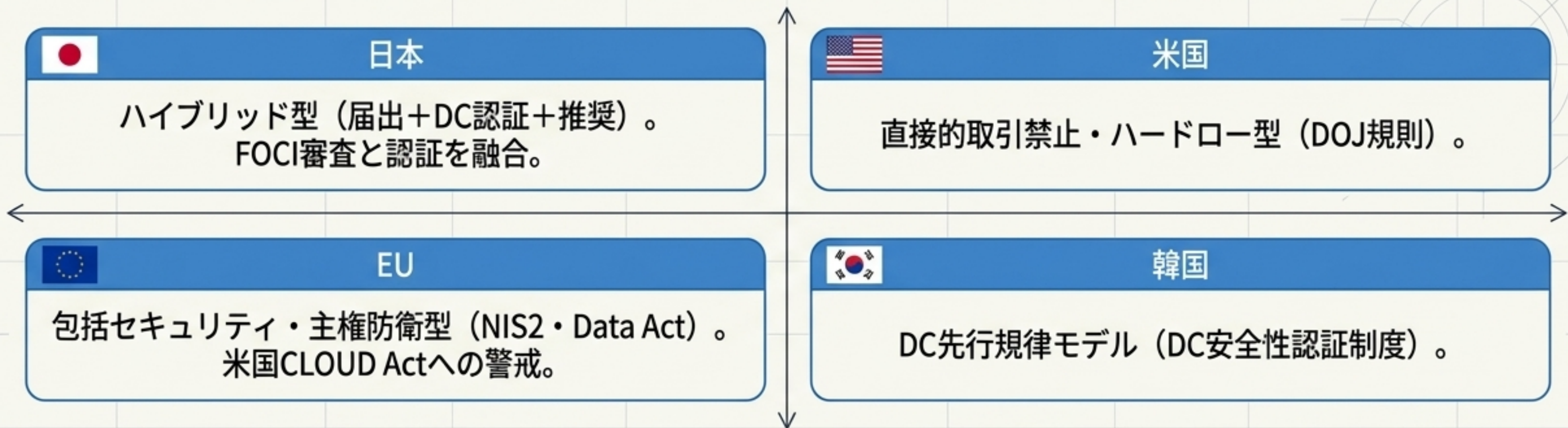
第3層: 国による審査・監督

リスク判定による「中止命令・是正勧告」

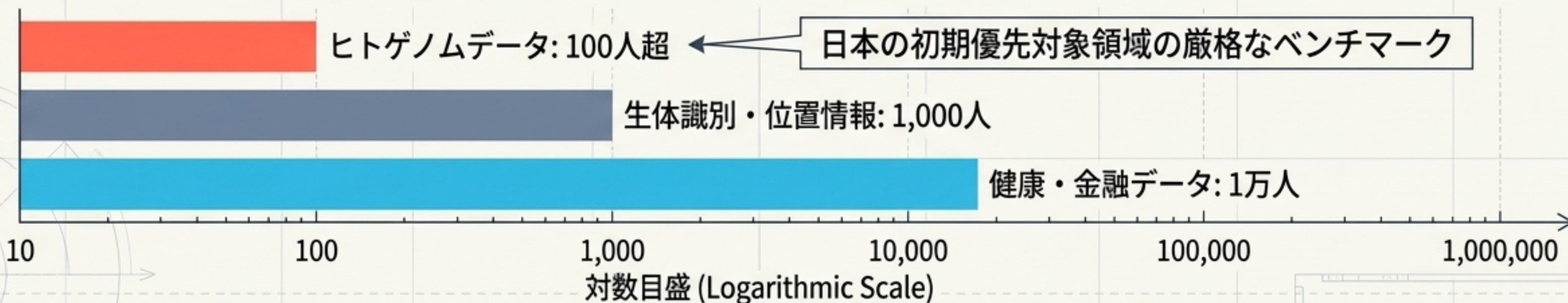
推奨
(インセンティブ)

巧妙なステルス排除のダイナミクス:
WTO違反(特定国名指し)を回避しつつ、基準不適合リスクに
より懸念国インフラを事実上排除する構造。

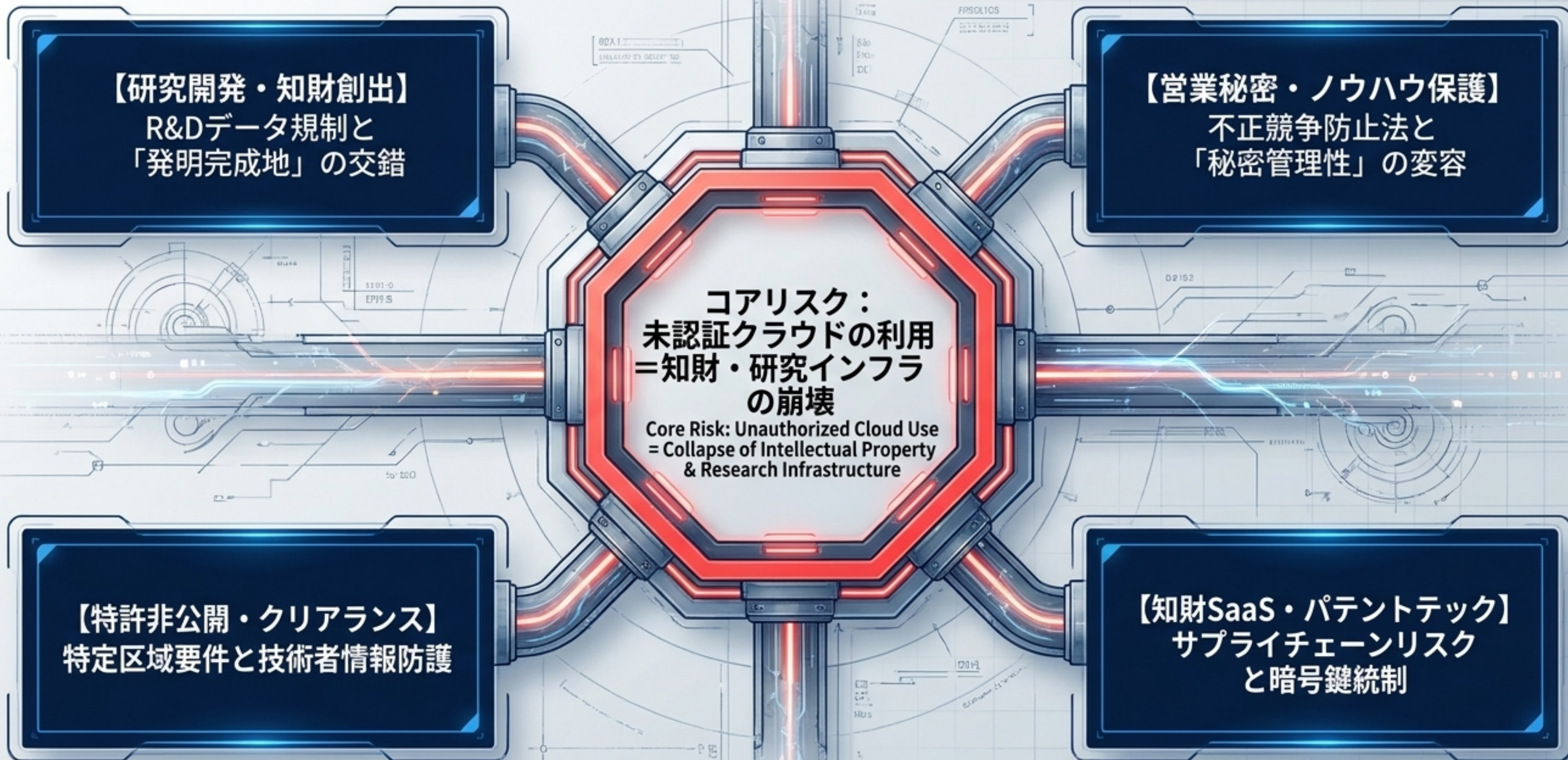
主要国のデータ安保規律比較と大量機微データ規制の数量閾値ベンチマーク



米国DOJ規則（2025年発効）における機微データ規制数量閾値



新データ安保制度が知財業務に及ぼす構造的リスクと対応の全体像 (The Structural Risks and Responses of New Data Security Regulations on Intellectual Property Operations - Overview)



日中両国の法規制の狭間におけるR&D活動の構造的危機

【日本政府からの圧力】

事前届出違反・中止命令
経済安全保障推進法（第78条）
第一国出願義務

日本企業 (R&D部門)

日本で採取した
ゲノム・医療データの
AI解析

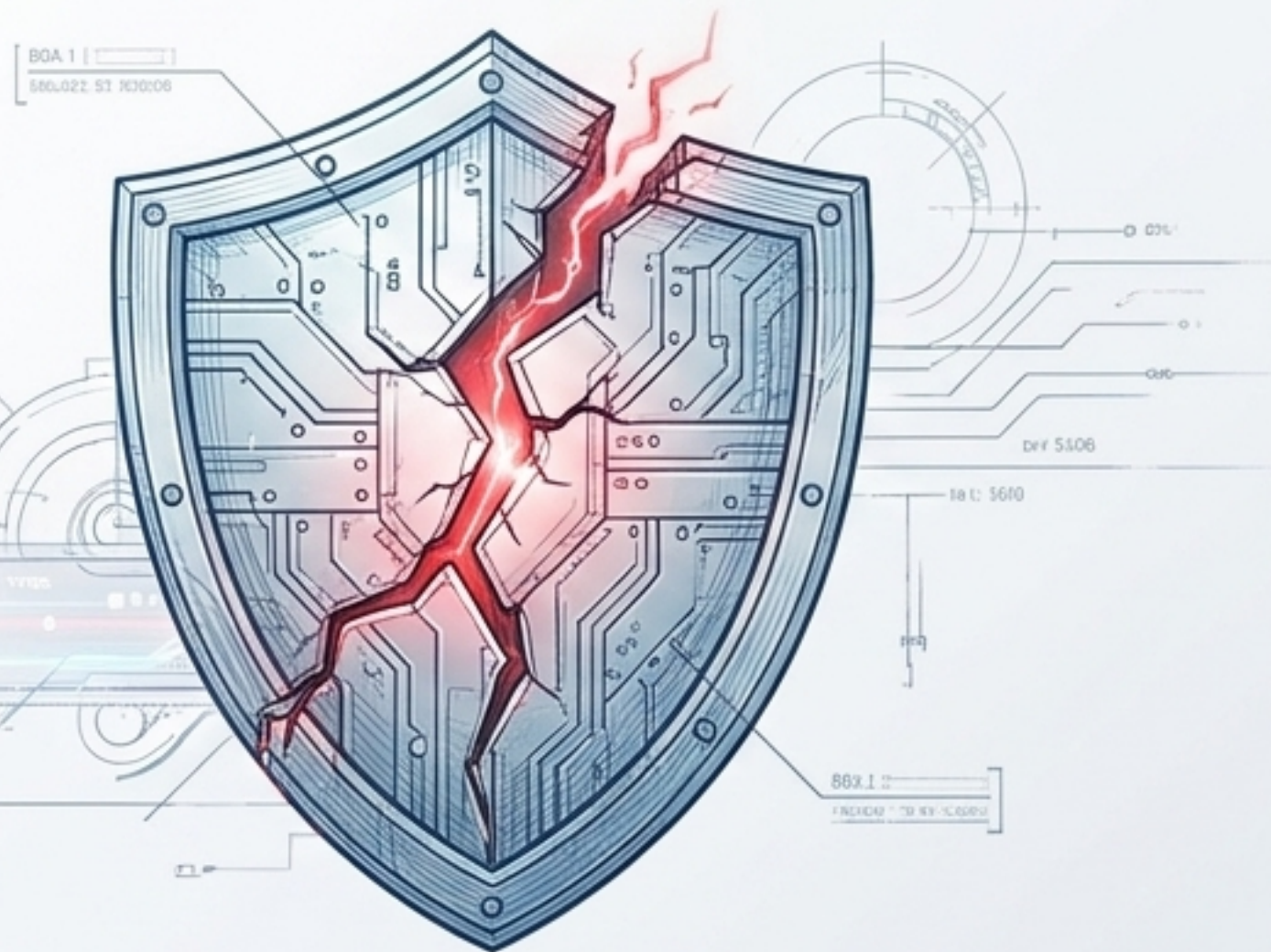
【中国当局からの圧力】

中国専利法第19条（秘密審査義務）
データ三法による越境移転制限

インサイト：データ処理を未認証の海外クラウド（CRO等）に委託した場合、「発明完成地」が国外とみなされ、日中両国の法規制の狭間で権利化そのものが頓挫する。

データセキュリティの新旧パラダイム転換とアクション (The Paradigm Shift and Action in Data Security)

過去のパラダイム



- 防御手段: NDA締結 + ID/パスワードによるアクセス制御
- 盲点: 国家情報法等による『外国法制の強制アクセス』や正規保守ルートからの抜取には無力化

新たなパラダイム



- 新常識: 国の安全認証(FOCI排除)を取得したクラウドへの保管
- リスク: 未認証クラウドの利用は『善管注意義務違反』に直結

【Action】今後の共同研究開発契約(Joint R&D)やNDAにおいて、「認証済みクラウドの指定」がデファクト・スタンダードとなる。人事・健康データの保護は防諜の第一線である。

人的統制

セキュリティ・クリアランス
制度（重要経済安保情
報保護活用法）による
人物の適性評価

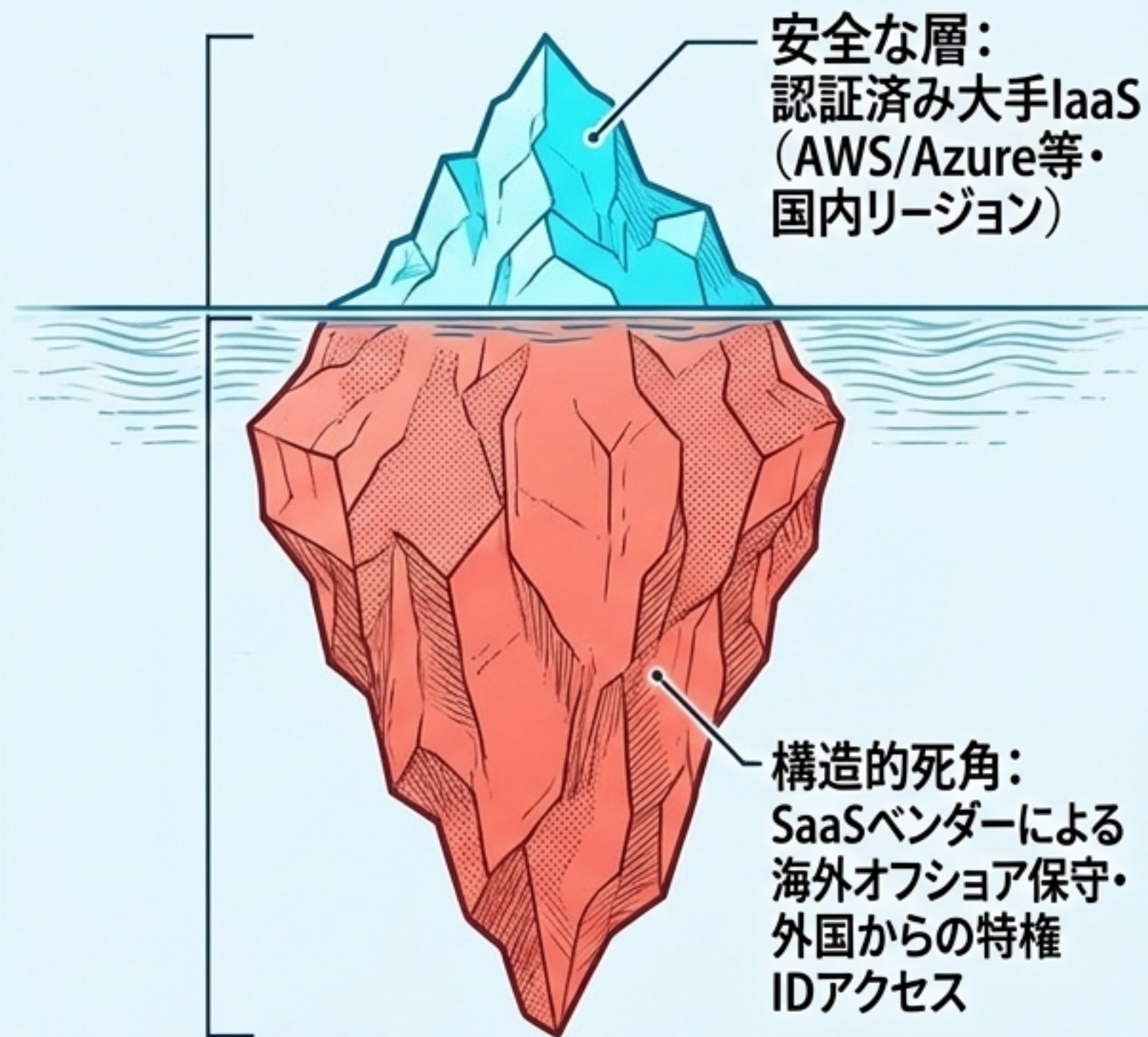
技術的統制

特許出願非公開制度に
おける「特定区域」。
民間企業におけるセーフ
ハーバー要件としての「認証
済み国内クラウド」の利用

推進法第80条「損失補償（類型4）」への連動

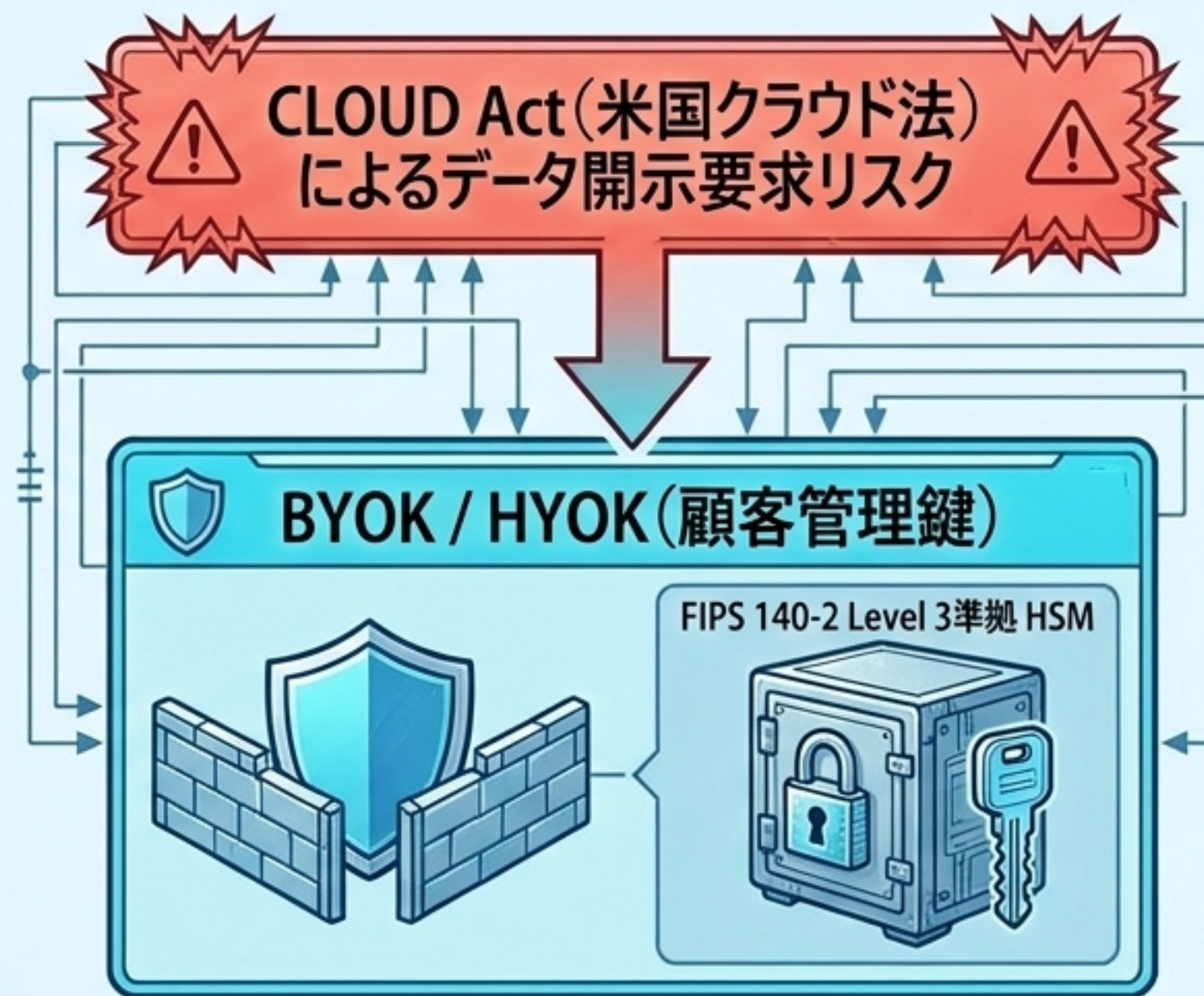
保全指定に伴い、特定区域要件を満たすために認証クラウドへの移行や
専用暗号化環境が必要となった場合、その「追加的に要した費用」は補償対象となる。

Key Takeaway: 平時から契約と費用明細を区分管理し、補償請求のエビデンスを準備せよ。



土台 (IaaS) が安全でも、知財SaaSのレイヤーがザルであれば未公開発明は流出する (非継承問題)。

対米リスクと究極の盾



クラウド事業者に鍵を渡さず、
自社で暗号統制を完結させる。

知財サプライチェーンの再構築

知財 サプライチェーン の再構築

技術的統制 (Technical Control)

- ・国内リージョンへのデータ固定
- ・BYOK/HYOKによる暗号鍵の自社統制
- ・海外からの特権アクセス遮断

契約的統制 (Contractual Control)

- ・NDA・共同研究契約ひな形改定
(認証クラウド利用義務化)
- ・知財SaaS・特許事務所への
FOCIデューデリジェンス

ガバナンス統制 (Governance Control)

- ・ゲノム・機微データの
事前届出プロセス確立
- ・発明者・重要技術者の
個人機微データ防護

知財・法務部門の実務ロードマップ(前半)

Time (期間)

Phase (フェーズ)

Actions (実務アクション)

2026年10月～12月



フェーズ1:
即時着手期

【知財・R&Dデータの棚卸しとマッピング】

- ・ゲノム・医療・金融等の機微データ保管先を特定。
- ・海外CROへの解析委託を総点検し、「発明完成地リスク」を排除。
- ・特許非公開対象 (25分野) データの隔離。



2027年1月～春



フェーズ2:
法案提出期

【知財SaaS・外部委託先のデューデリジェンス】

- ・利用中の知財SaaS・特許事務所に対し、IaaS所在地・資本関係 (FOCI) ・海外保守アクセスの監査を実施。
- ・BYOK暗号化要件のベンダー交渉開始。



知財・法務部門の実務ロードマップ(後半)

Time (期間)

Phase (フェーズ)

Actions (実務アクション)

2027年夏～後半



フェーズ3:
施行準備期

【契約ひな形改定と社内規程のアップデート】

- ・NDA・共同研究契約に「認証クラウド指定条項」を導入。
- ・2025年改訂「営業秘密管理指針」に準拠した社内規程の改定。
- ・人事部門と連携した発明者データ防護体制の構築。



2027年度後半以降

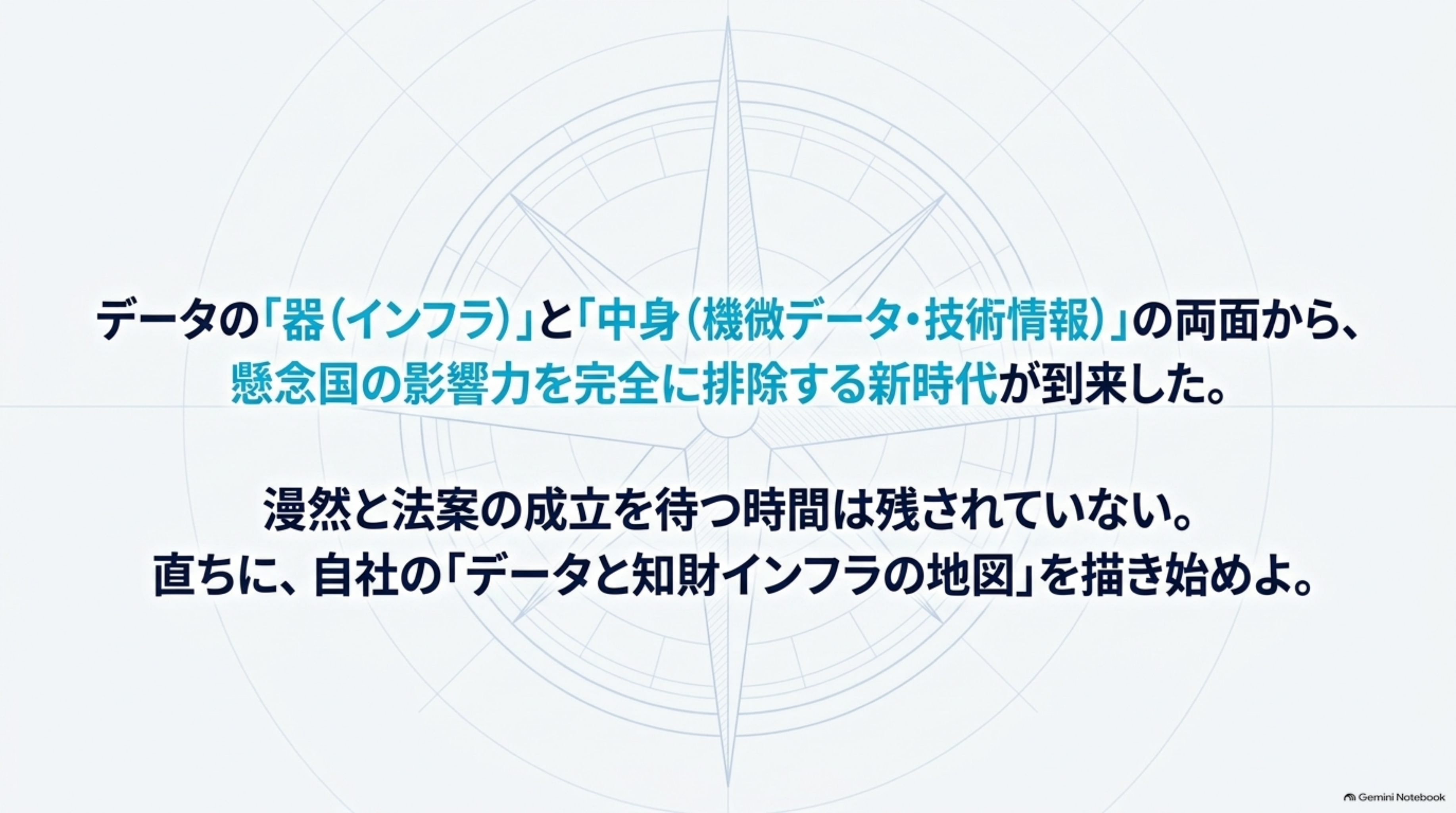


フェーズ4:
制度本格稼働期

【事前届出対応・クラウド移行・補償請求体制の確立】

- ・大量機微データR&Dの「事前届出手続」定型化。
- ・未認証基盤からの計画的データ移行完遂。
- ・保全指定時の特定区域指定と損失補償(追加クラウド費用)の算定エビデンス整備。





**データの「器（インフラ）」と「中身（機微データ・技術情報）」の両面から、
懸念国の影響力を完全に排除する新時代が到来した。**

**漫然と法案の成立を待つ時間は残されていない。
直ちに、自社の「データと知財インフラの地図」を描き始めよ。**