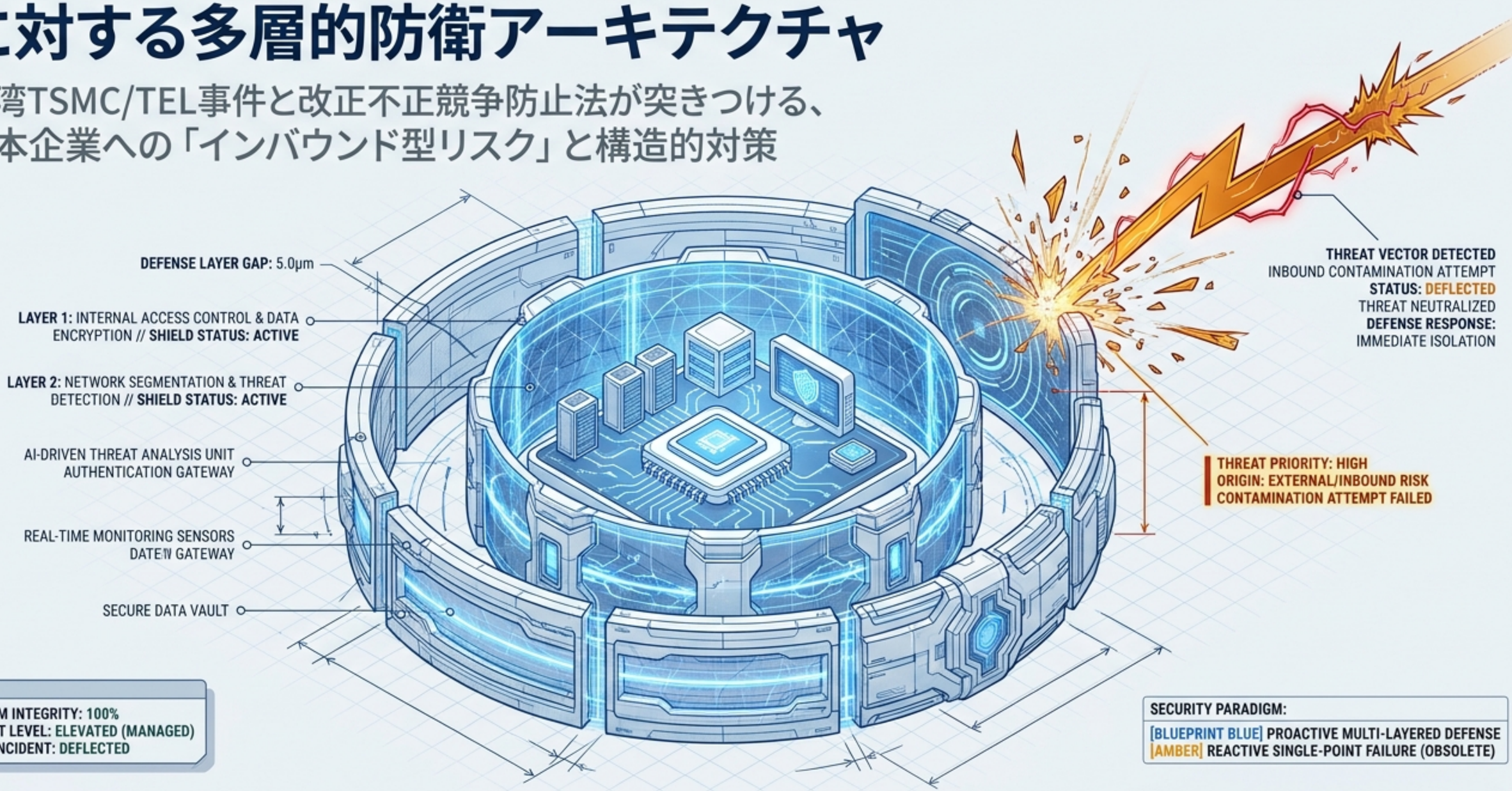
知的財産の防衛パラダイムシフト：技術コンタミネーションに対する多層的防衛アーキテクチャ

台湾TSMC/TEL事件と改正不正競争防止法が突きつける、
日本企業への「インバウンド型リスク」と構造的対策



脅威モデルの逆転：情報漏洩から「技術混入（コンタミネーション）」へ

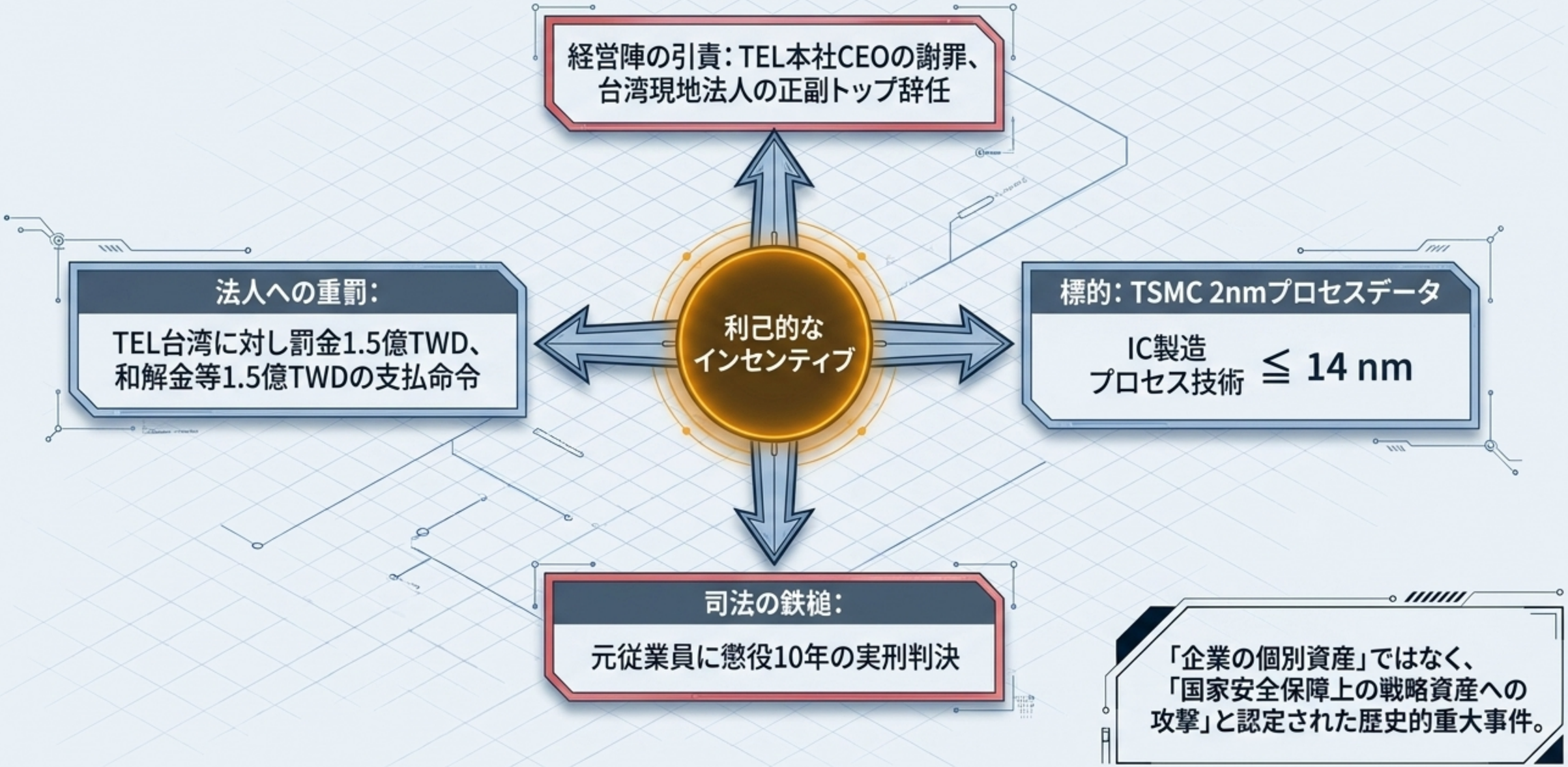
The Threat Inversion Matrix

The Outdated Focus アウトバウンド（漏洩）	The New Existential Threat インバウンド（混入）
ベクトル: 自社技術が外部へ流出	ベクトル: 他社技術が自社開発環境へ侵入
アクター: 退職者、産業スパイ	アクター: 優秀な中途採用エンジニア、 共同開発パートナー
法的リスク: 自社の競争力低下、逸失利益	法的リスク: 巨額の損害賠償、製品販売差止、 企業ブランドの壊滅
企業の立場: 被害者（原告） VICTIM / PLAINTIFF	企業の立場: 加害者（被告） PERPETRATOR / DEFENDANT

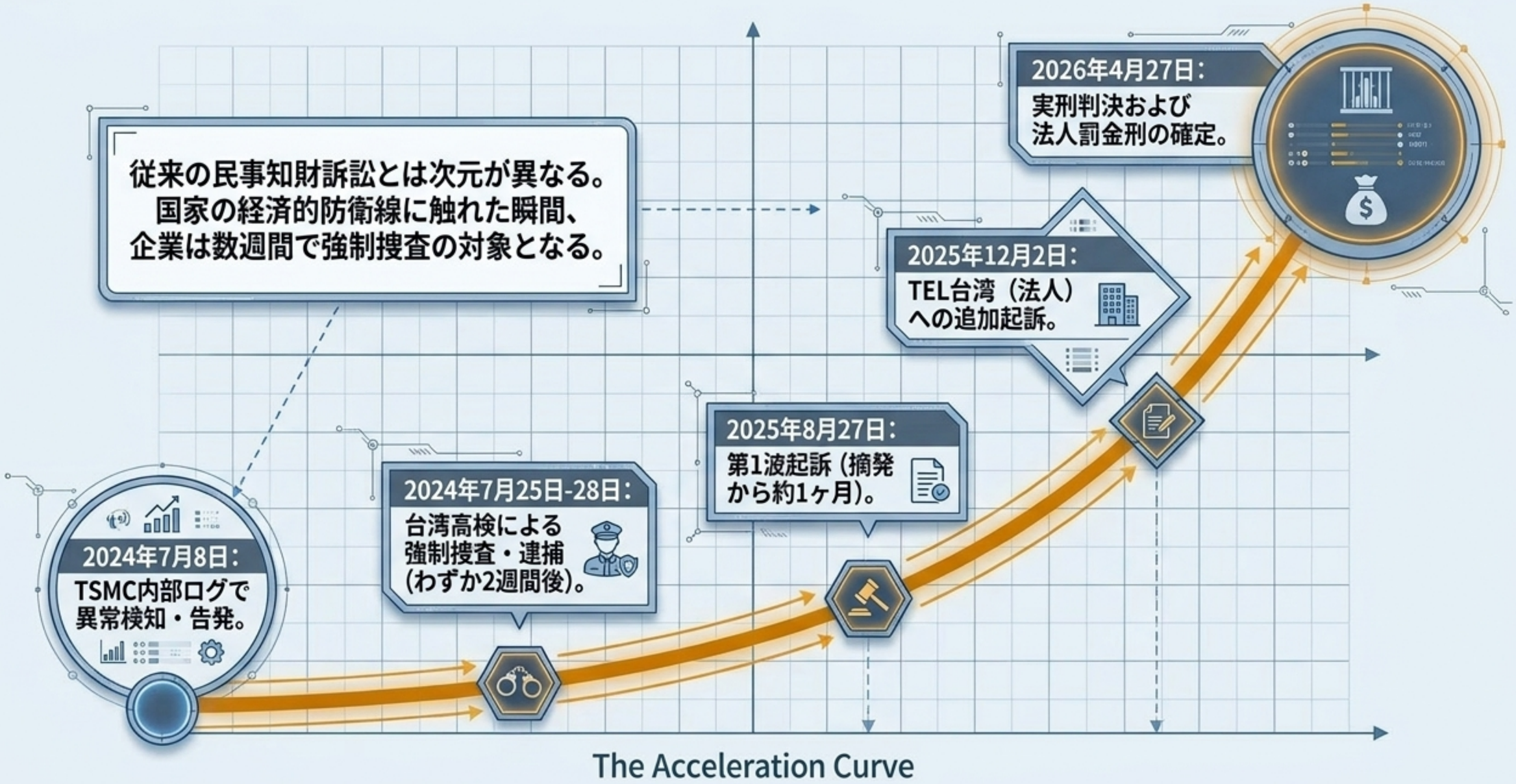
THREAT SHIFT

中途採用による他社技術の「安易なショートカット」は、企業を深刻な加害者へと転落させる致命的なリスクである。

カタリスト・イベント：台湾TSMC 2nm技術不正取得事件



国家安全保障が牽引する「異例のスピード司法」



両罰規定の罠：「受動的なコンプライアンス」は「能動的な過失」と見なされる

台湾営業秘密法第13条の4（法人両罰規定）。TEL台湾側は
「社内規程や警告はあった」と主張したが、裁判所は
「抽象的で形骸化した宣言に過ぎない」として退けた。

「従業員の不正行為」＋「実効的な防御システム（能動的フィルタリング）の不在」＝「法人の刑事責任（使用者責任）」

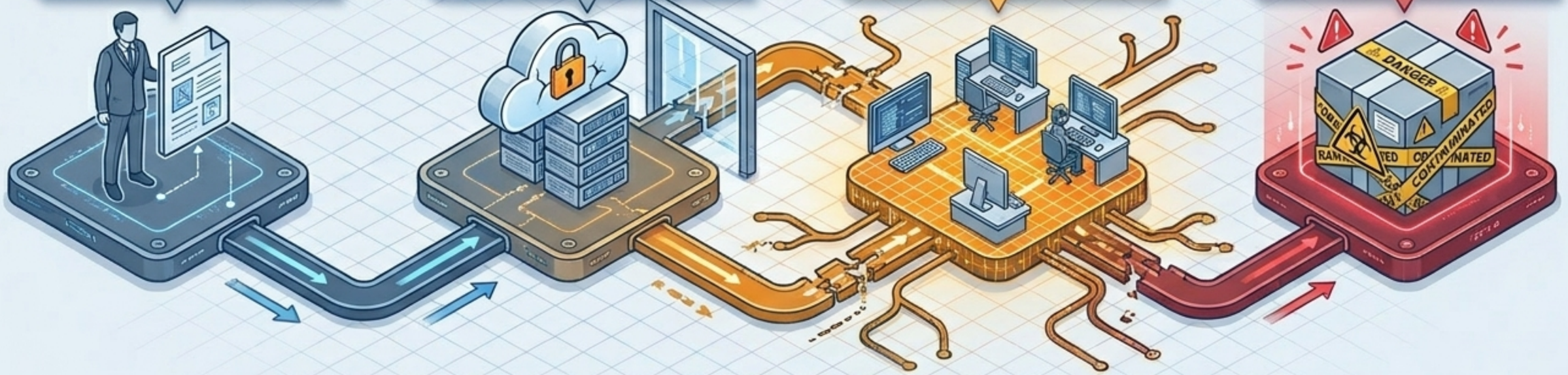
コンタミネーション・ベクトル：一つのファイルがR&D全体を汚染する経路

1. External
中途採用エンジニアが入社。前職の「参考データ」を悪気なく所持。

2. Gateway
システム的な遮断がなく、会社の共有クラウドストレージ(OneDrive等)にファイルをアップロード。

3. Proliferation
R&Dチーム全体がアクセス可能な共有環境でデータが拡散。製品パラメータに組み込まれる。

4. Terminal
新製品全体が「他社の営業秘密を使用した」として法的に汚染される。



The **Trojan Horse** Vector Diagram

悪意のある産業スパイよりも、「前職の知識を活かそうとする優秀なエンジニア」の無自覚な行為が最大の脅威となる。

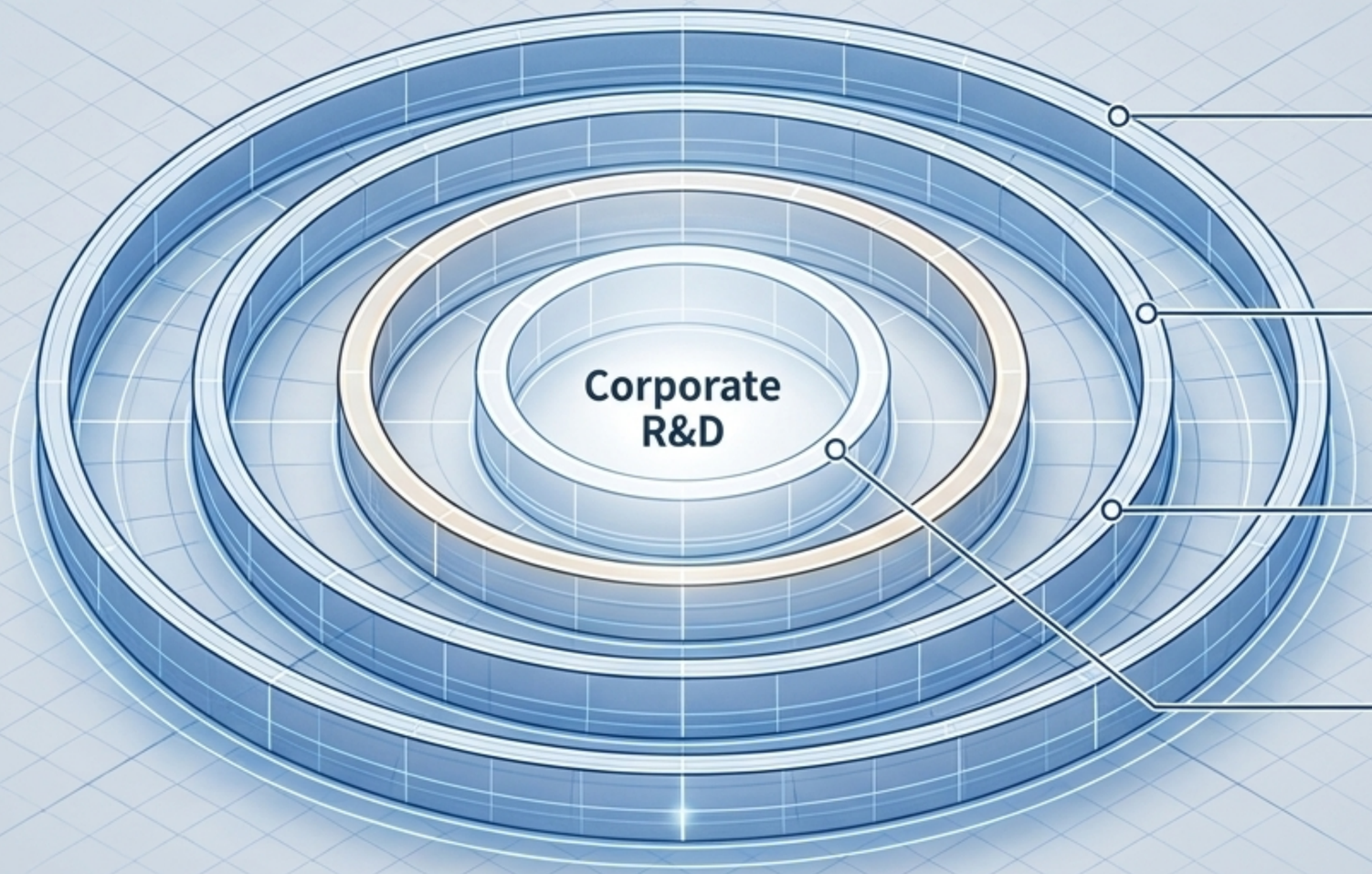
日本法における法的落とし穴：改正不正競争防止法（2024年4月施行）

営業秘密の「使用等の推定規定」の拡張	
改正前	悪質な産業スパイ等に限定。
改正後	アクセス権限を有していた元従業員（一般的な中途採用者）や元業務委託先にも適用。 ⚠

転職者のアクセス権限（前職） ＋ **被告企業の同種製品・役務提供** ⇒ **使用の推定**

転職者が共有ドライブにファイルをコピーしただけで、企業側は「独自開発であること」を客観的証拠で反証しない限り、法的に「使用した」と見なされる。挙証責任が企業側に転換された。

混入防止（インバウンド・コンタミネーション）の4層防衛アーキテクチャ



第1層: 人事・採用フェーズ
（ゲートキーピングの高度化）

第2層: IT・技術的隔離フェーズ
（情報インフラのゾーニング）

第3層: 開発・R&Dフェーズ
（クリーンルーム開発と独自開発立証）

第4層: 組織監査・ガバナンスフェーズ
（事後対策とヘルプライン）

「漏洩防止（アウトバウンド）」と同水準、あるいはそれ以上の厳格さで
「混入防止（インバウンド）」を全社的に構築しなければならない。

第1層：人事・採用フェーズにおけるゲートキーピングの高度化

アクション 1: 秘密開示不要求の明文化

面接時に「前職の技術資料等を一切求めていない」ことをヒアリングシートに記録し、双方署名でアーカイブ。

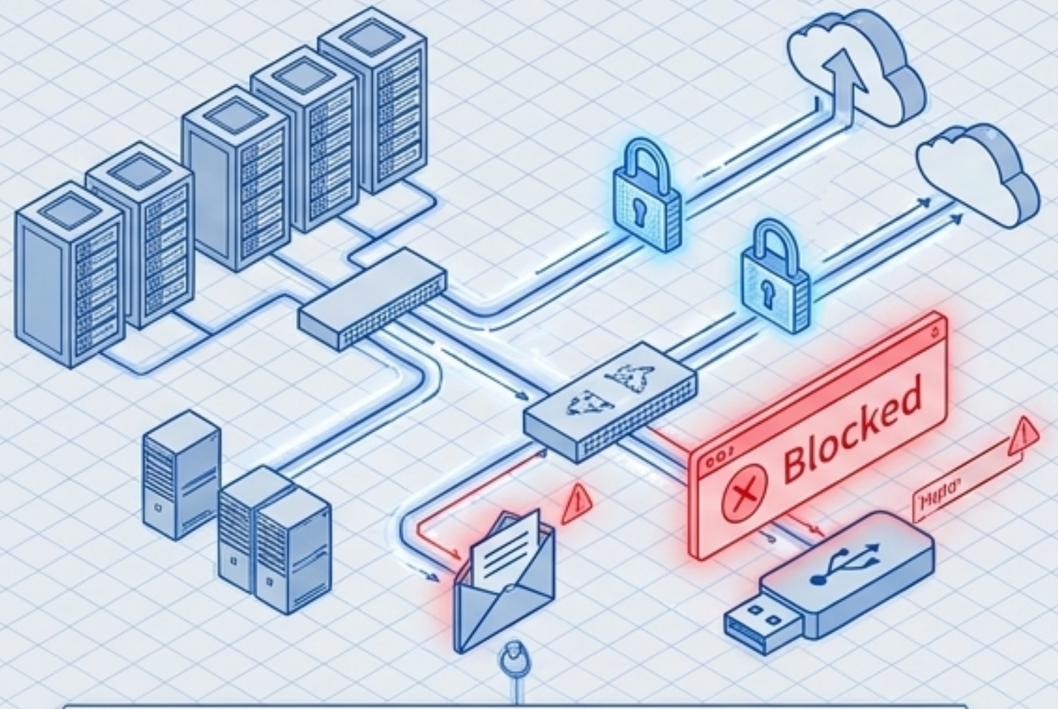
アクション 2: 具体的な表明保証の締結

入社時のNDAを高度化。抽象的な「守秘義務」ではなく、「前職の開発パラメータ、実験ノート等を私用PCから完全消去した」という具体的な表明保証をとる。

法的防護力: 万が一混入が発生した際、法人の無過失（監督義務の履行）を証明し、両罰規定から免責されるための強力な防護証拠となる。

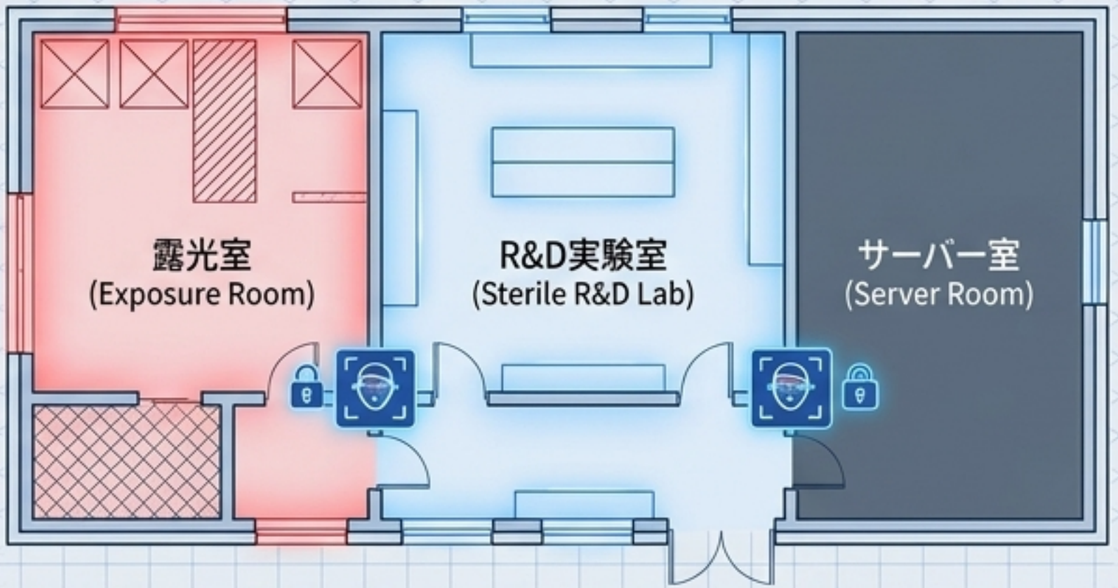
第2層：ITおよび物理的インフラの厳格なゾーニング

デジタル・ゾーニング (Digital Zoning)



共有クラウド（OneDrive等）での最小特権原則。
私用USBや個人メールのシステム的な自動遮断。

物理的ゾーニング (Physical Zoning)



顔認証等による生体アクセスゲート。
露光室、R&D実験室、サーバー室の厳格な物理的分離。

規程による「禁止」ではなく、システムと物理アーキテクチャによる「遮断と追跡（トレーサビリティ）」を実装する。

第3層：法的汚染を遮断する「クリーンルーム開発」モデル

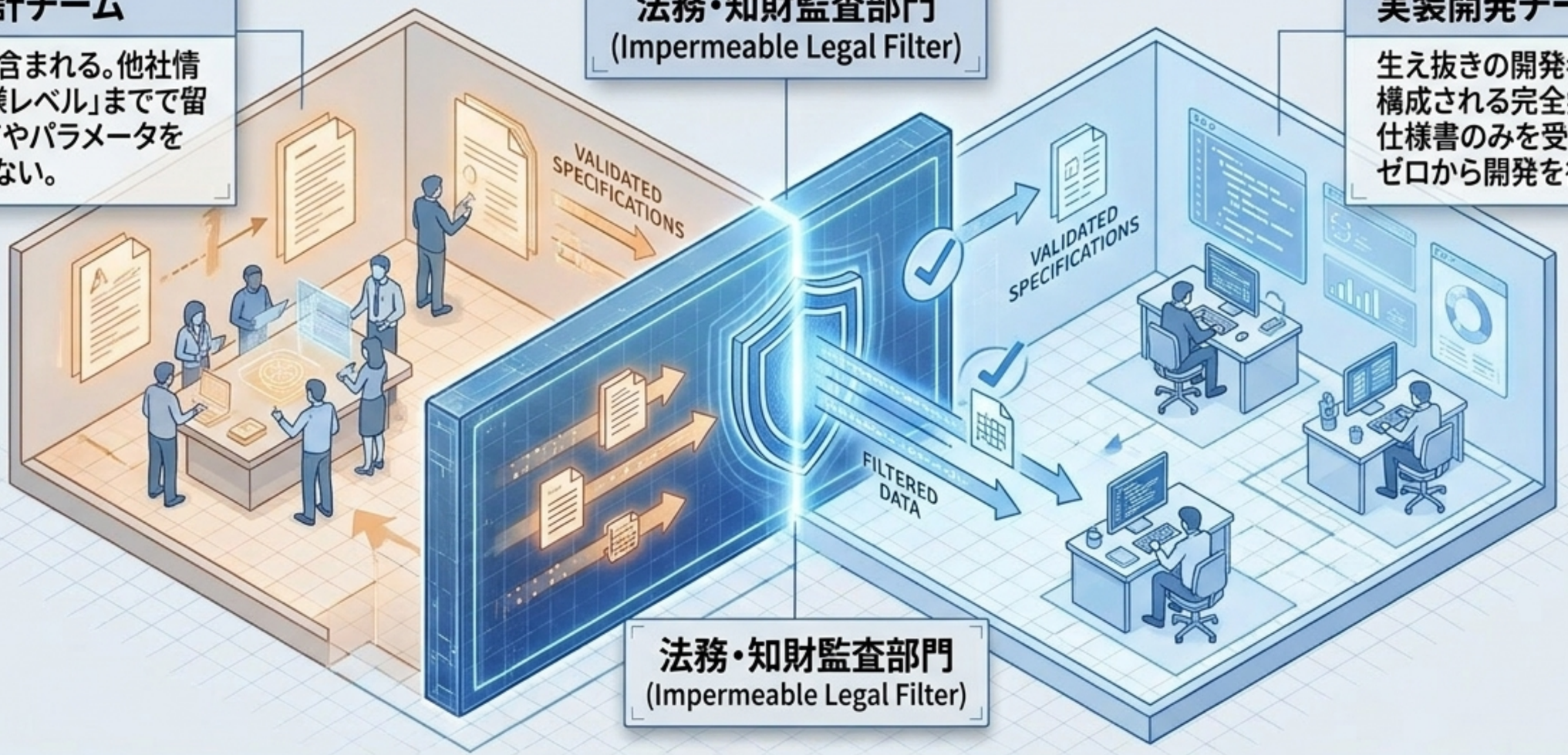
仕様設計チーム

転職者が含まれる。他社情報を「仕様レベル」までで留め、コードやパラメータを持ち込まない。

法務・知財監査部門
(Impermeable Legal Filter)

実装開発チーム

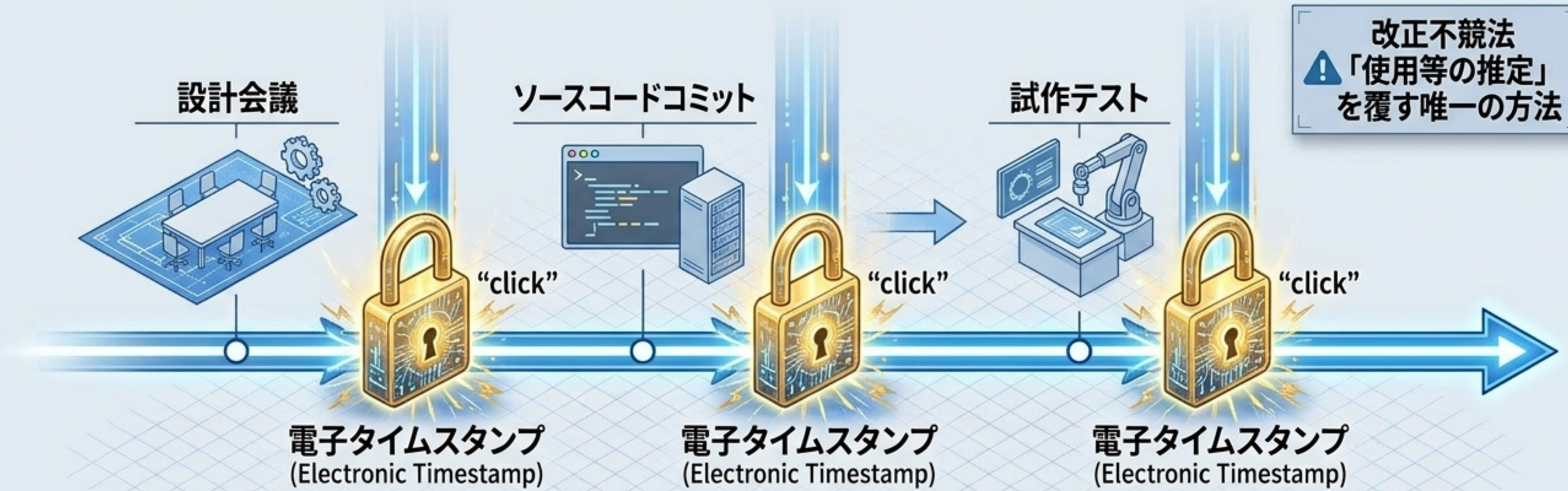
生え抜きの開発者のみで構成される完全無菌層。仕様書のみを受け取り、ゼロから開発を行う。



物理的・組織的な分離により、技術の混入可能性を構造的にゼロに近づけ、独自開発の正当性を担保する。

第3層：反証の切り札となる「電子タイムスタンプ」の系譜

改正不競法
⚠「使用等の推定」
を覆す唯一の方法



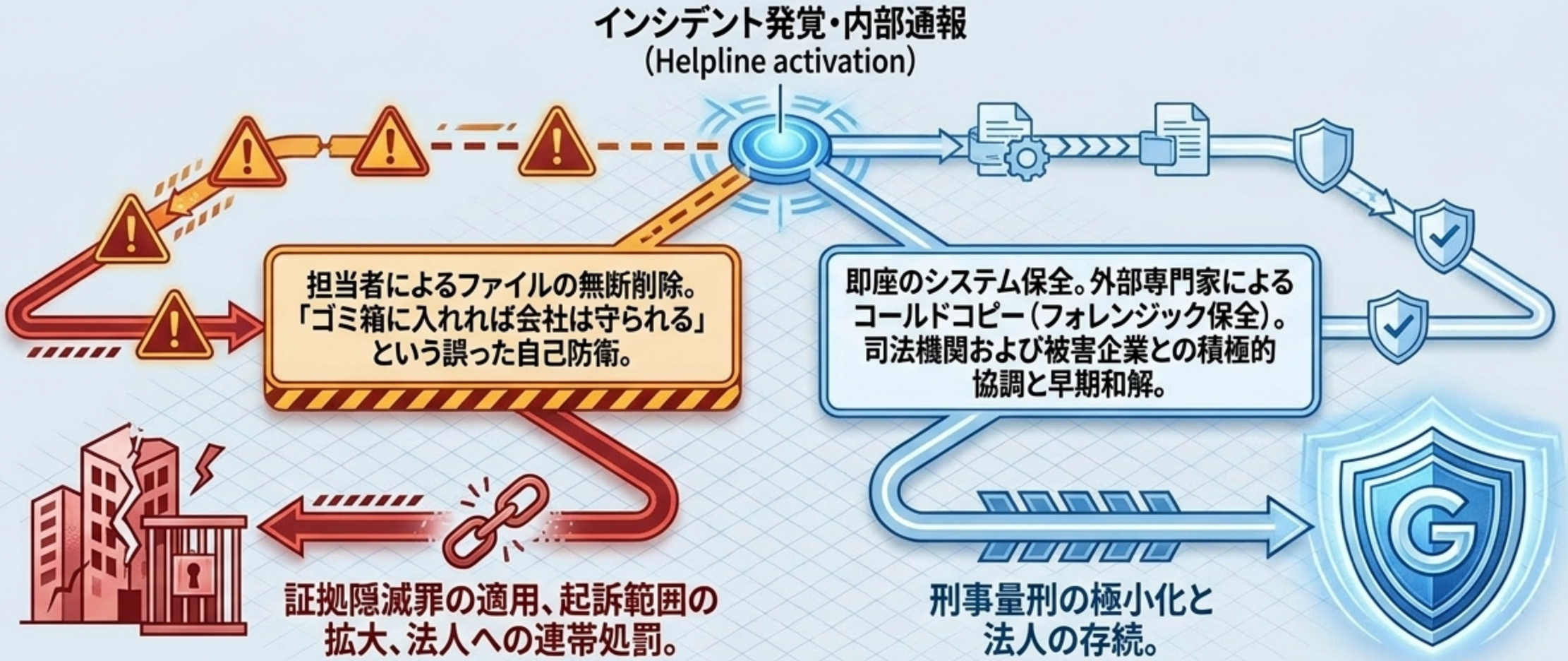
メカニズム

開発ログに改ざん不可能なタイムスタンプを即座に自動付与し、一元管理する。

法的効力

「相手方の技術に接触する以前から、完全に独自で開発していたこと」を客観的に裏付ける鉄壁の防御証拠。

第4層：有事対応ガバナンスと証拠隠滅の阻止



事後の隠蔽は個人の刑事罰を著しく重くし、法人への致命的なダメージを引き起こす。
役員会主導の「有事対応ガイドライン」が必須。

防衛アーキテクチャと法制度のアライメント・マトリクス

防衛の柱	得られる法的防御力	関連法規
人事・採用の高度化	法人の「必要な監督義務」 免責証明資料	台湾営業秘密法第13-4条 経産省ハンドブック
IT・物理ガバナンス	混入ルートのシャットアウトと ログの追跡可能性	不正競争防止法第2条 （秘密管理性要件）
独自開発の確保 （クリーンルーム/タイムスタンプ）	「使用等の推定規定」に対する 科学・改ざん不可能な反証	改正不競法第5条の2
ガバナンスと有事対応	証拠隠滅による企業犯罪への 延焼防止、量刑極小化	各国刑法、法人両罰規定

コンプライアンスから「生存のための戦略防衛投資」へ

知的財産の国家安全保障化

知的財産の取り扱いは、もはや倫理問題ではなく、
国家安全保障と直結する死活問題である。

サプライチェーン排除のリスク

他社技術への安易な「ショートカット」は、
企業を最先端サプライチェーンから永久に排除する。

新たな「標準防衛装備」

多層的防衛管理プログラム（人事・IT・R&D・ガバナンス） は、不必要なコストではない。グローバルに信頼されるトップランナーとして日本企業が競争を勝ち抜くための、新たな「標準防衛装備」である。

**経営幹部主導による、現行インフラの即時監査と
防衛アーキテクチャの構築を推奨する。**