企業リスクの解剖と防衛設計図：台湾半導体営業秘密事件の教訓

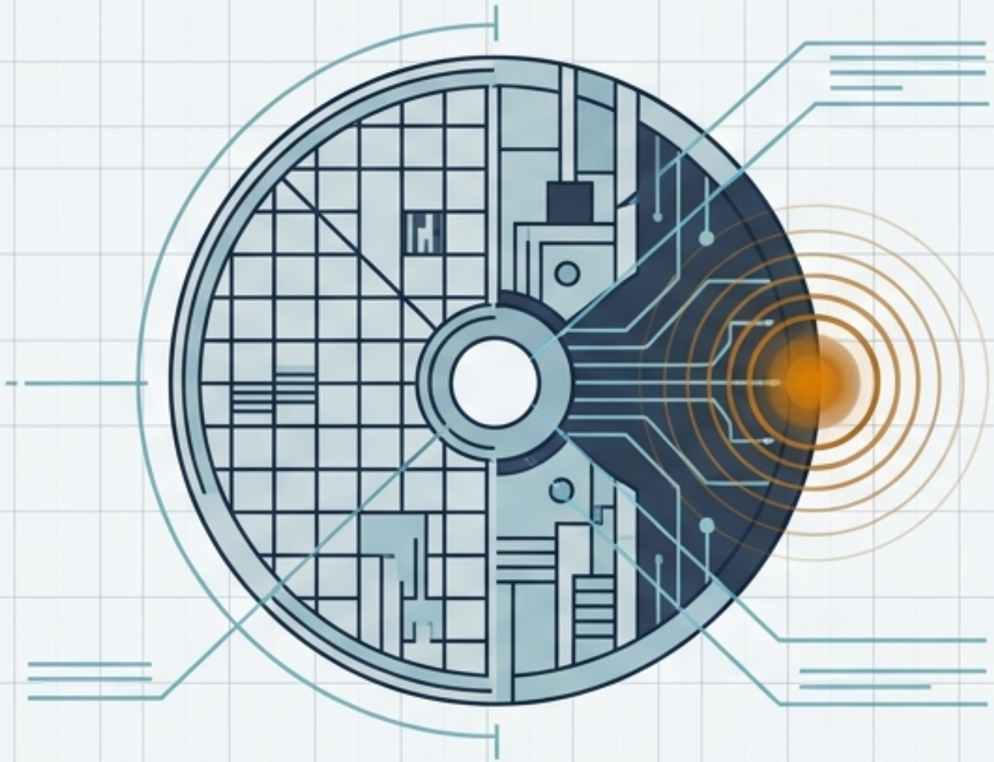
顧客接点からの情報流出メカニズムと「尽力防止」の境界線

罰金額:
1.5億台湾元
(刑事罰)

核心論点:
法人両罰規定と経営の監督責任

対象読者:
経営層・CISO・法務・事業部門長

事件の核心



元TSMC社員が東京威力科創（東京エレクトロン台湾子会社）入社後、TSMC在職者から先端プロセス（14nm/2nm）向けエッチング装置の営業秘密を不正取得。目的は自社装置の採用拡大。

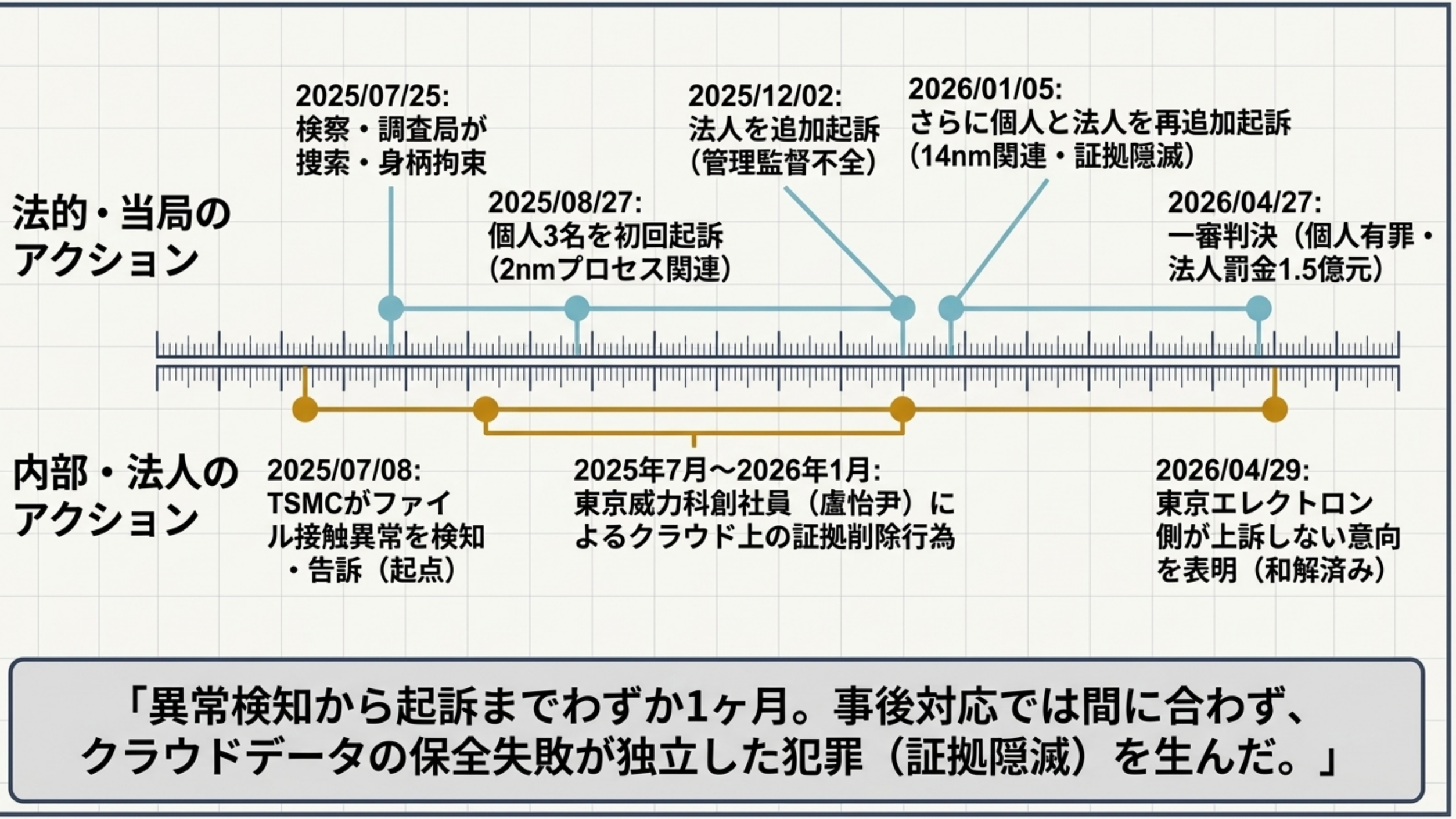
法的帰結

1.5億元

台湾「国家安全法」違反。公開情報上、民事賠償ではなく法人に対する刑事罰（罰金）。東京エレクトロン側は上訴せず和解済み。

企業への警鐘

情報漏えいはR&D部門からだけでなく、「顧客接点部門（営業・FAE）」から発生する。形式的な規程だけでは法人の「尽力防止」抗弁は認められない。



「異常検知から起訴までわずか1ヶ月。事後対応では間に合わず、
クラウドデータの保全失敗が独立した犯罪（証拠隠滅）を生んだ。」

TSMC側 - 情報の源泉

吳秉駿・戈一平
（在職エンジニア）：
秘密情報を提供

陳韋傑（在職者）：
同僚アカウントを悪用し
データベースへ侵入

写真撮影 /
アカウント借用 /
メール添付

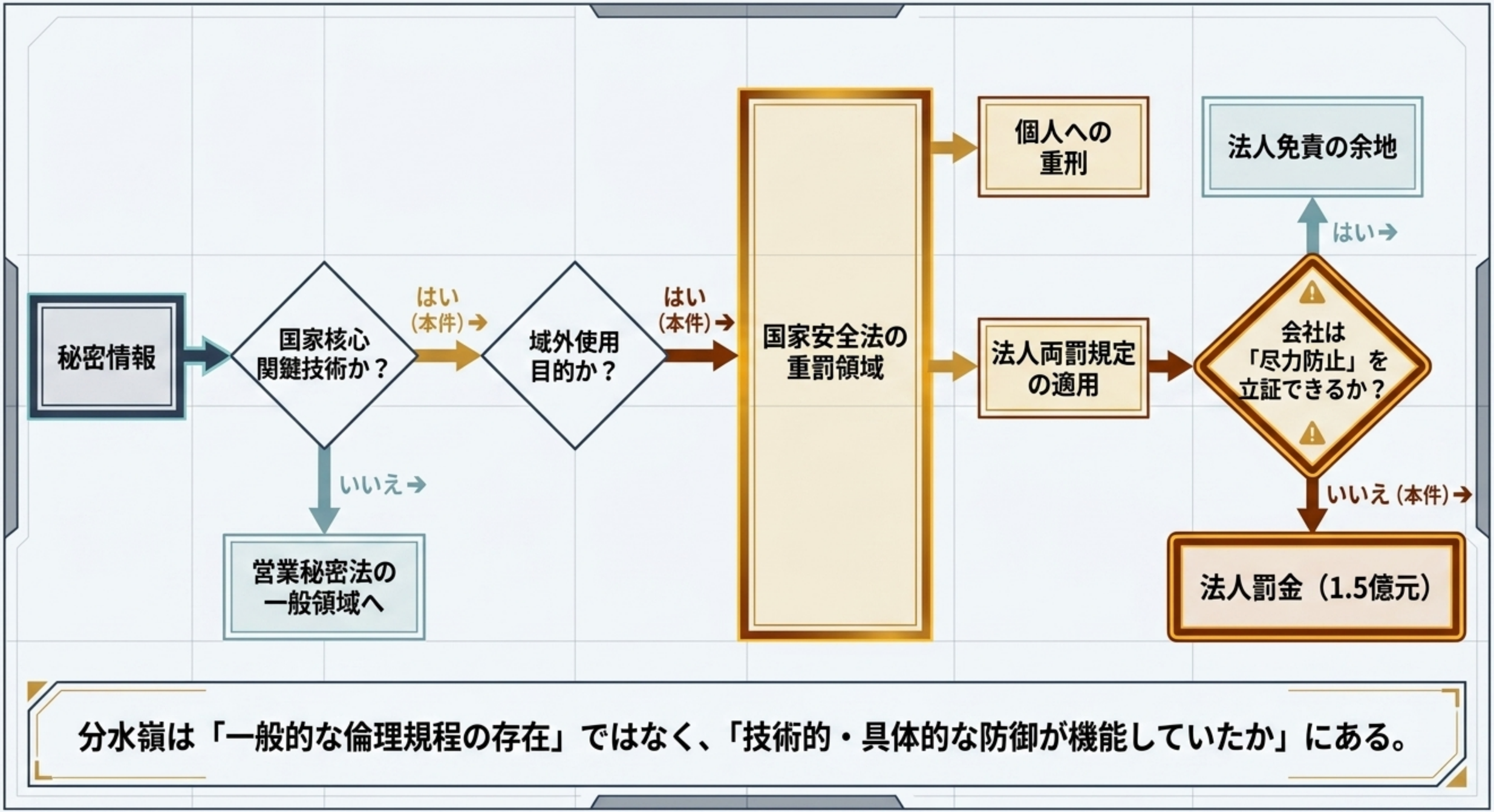
東京威力科創側 - 取得と隠滅

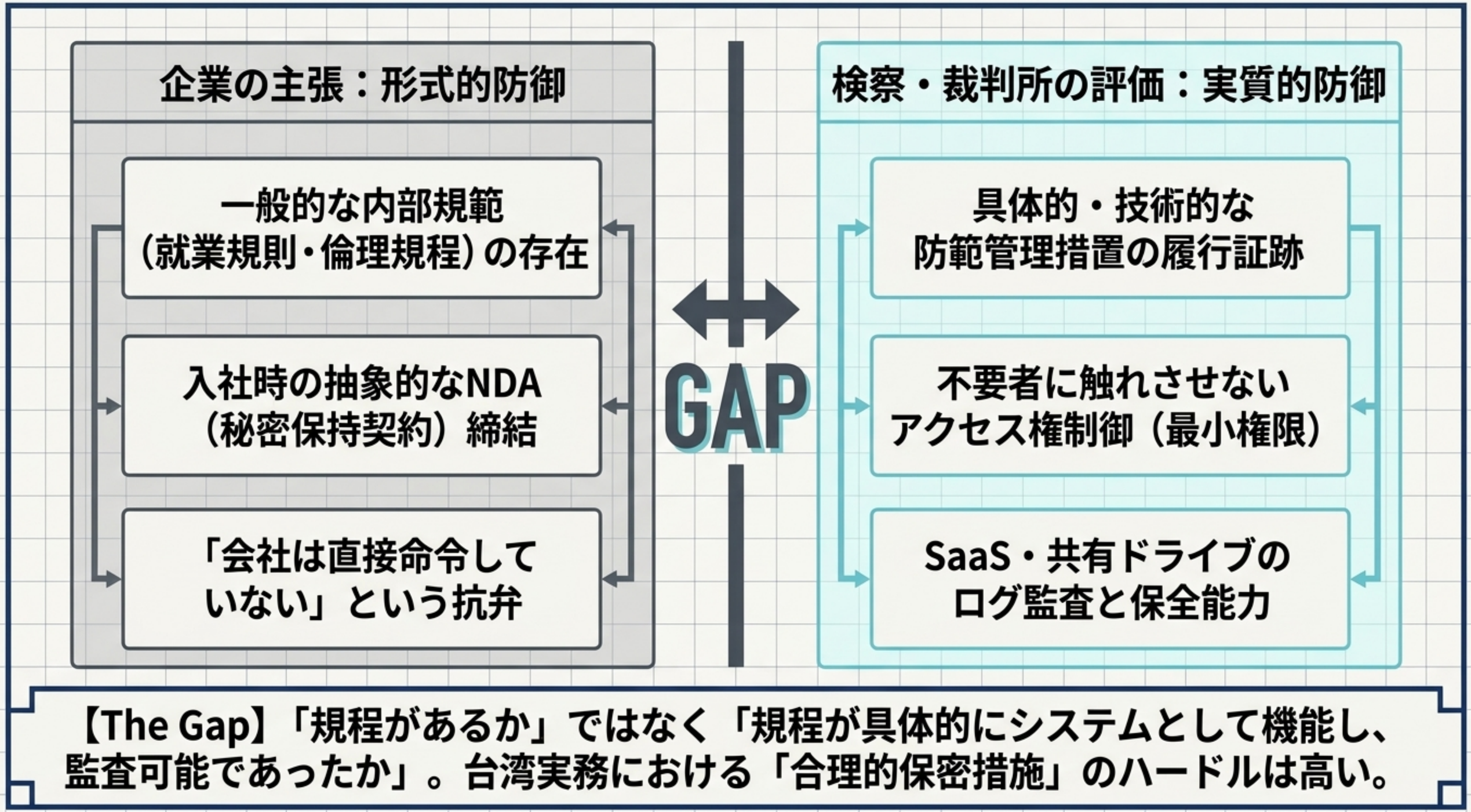
陳力銘（元TSMC・営業部門）：
旧知の仲を利用し情報取得を主導。自社装置の改善・採用拡大（業務執行）に利用。

会社雲端系統（クラウド）：
14ナノ以下関連資料を保存。

盧怡尹（社員）：
発覚後にクラウド上の図檔を削除（証拠隠滅）。

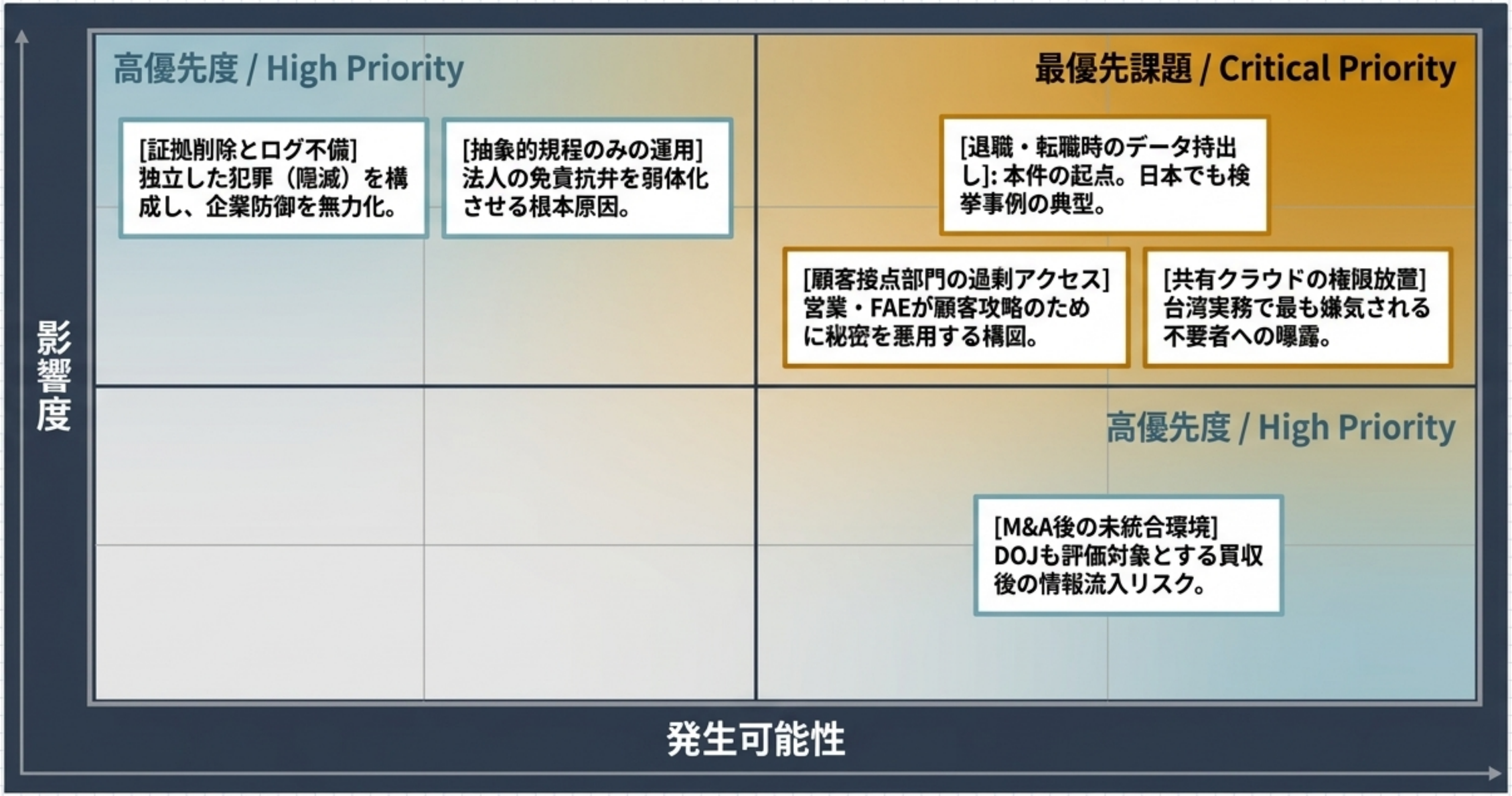
「取得 ➡ 共有 ➡ 隠滅」が法人システム上で連続。単なる個人の逸脱ではなく、会社の「業務目的（業績向上）」と紐づいた構造的インシデント。


秘密情報
国家核心
関鍵技術か？
はい
(本件)
域外使用
目的か？
はい
(本件)
国家安全法の
重罰領域
個人への
重刑
法人両罰規定
の適用
会社は
「尽力防止」を
立証できるか？
はい
法人免責の余地
いいえ
営業秘密法の
一般領域へ
いいえ (本件)
法人罰金（1.5億元）
分水嶺は「一般的な倫理規程の存在」ではなく、「技術的・具体的な防御が機能していたか」にある。

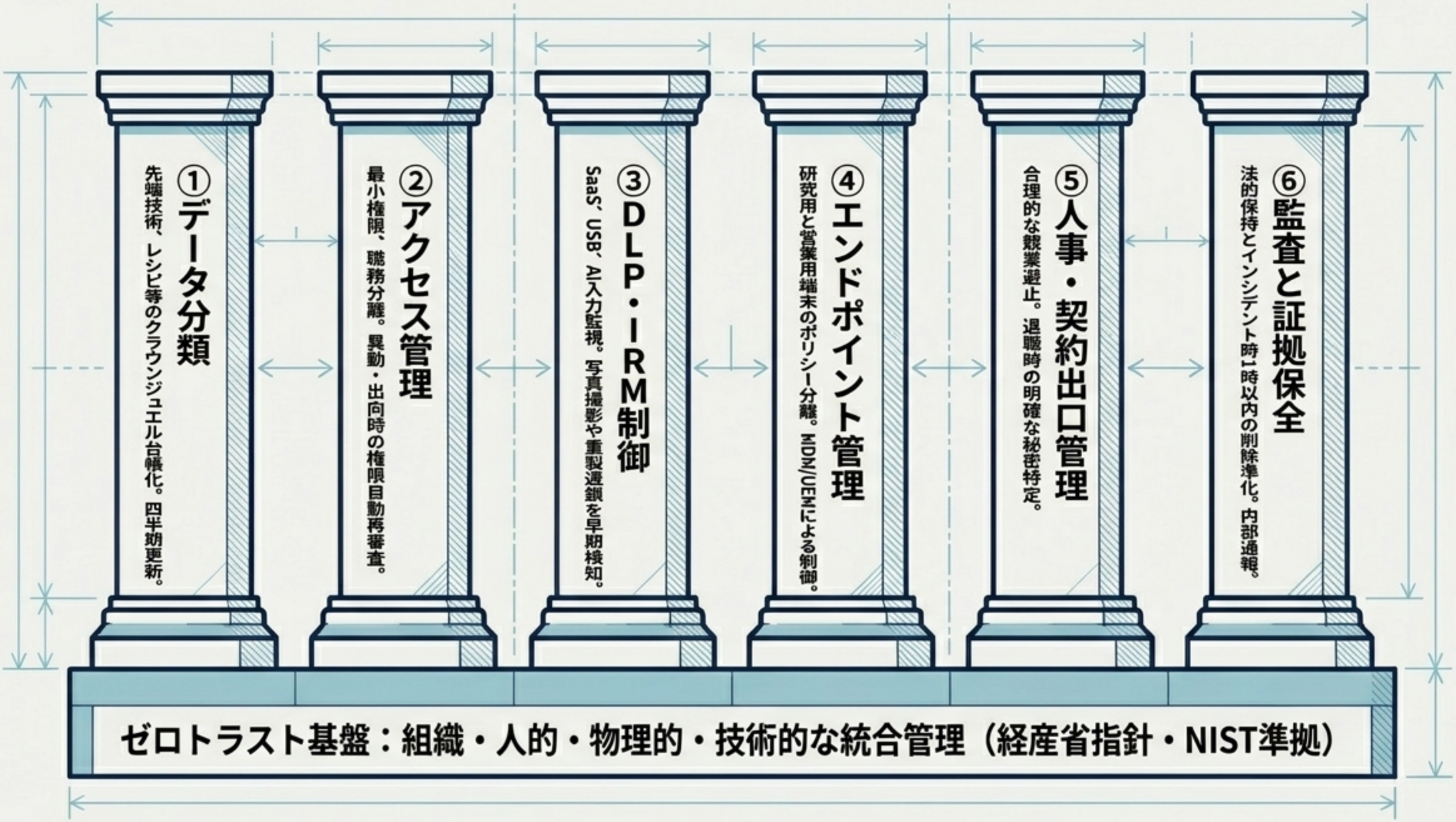

企業の主張：形式的防御
一般的な内部規範
（就業規則・倫理規程）の存在
入社時の抽象的なNDA
（秘密保持契約）締結
「会社は直接命令して
いない」という抗弁
GAP
検察・裁判所の評価：実質的防御
具体的・技術的な
防範管理措置の履行証跡
不要者に触れさせない
アクセス権制御（最小権限）
SaaS・共有ドライブの
ログ監査と保全能力
【The Gap】「規程があるか」ではなく「規程が具体的にシステムとして機能し、
監査可能であったか」。台湾実務における「合理的保密措施」のハードルは高い。

事件	構図・法的基盤	結末
本件：TSMC vs 東京威力科創	元従業員経由の先端プロセス漏えい **台湾国家安全法（経済安保）＋法人両罰**	個人実刑、法人に刑事罰金**1.5億元**。 企業側の防止努力が正面から問われた。
美光(Micron) vs 聯電(UMC)・晋華	元社員らによるDRAM秘密の移転 **台湾営業秘密法＋米国連邦法（経済安保）**	米国で有罪答弁、**6千万ドル**罰金。 国境横断リスクの典型。
東芝 vs SKハイニックス	NANDフラッシュ機密の不正取得 日本不競法ベースの民事紛争	**2.78億ドル**和解、その後協業拡大。 紛争と取引継続の両立。
ASML vs XTAL	元従業員関与のソフトウェア窃取 米国Trade Secrets実務	民事最終判決で約**8.45億ドル**相当。

経済安保（国家核心関鍵技術）が絡むと、純粋な民事紛争を超え、巨額の罰金と厳格な法人処罰の対象となる。もはや法務単独の課題ではない。



リスクの震源地は「高度なサイバー攻撃」ではなく、「退職」「クラウド共有」「営業活動」という日常業務の中に埋め込まれている。


①データ分類
先端技術、レシピ等のクラウンジュエル台帳化。四半期更新。
②アクセス管理
最小権限、職務分離。異動・出向時の権限自動再審査。
③DLP・IRM制御
SaaS、USB、AI入力監視。写真撮影や重製遮断を早期検知。
④エンドポイント管理
研究用と営業用端末のポリシー分離。MDM/UEMによる制御。
⑤人事・契約出口管理
合理的な競業避止。退職時の明確な秘密特定。
⑥監査と証拠保全
法的保持とインシデント時1時以内の削除準化。内部通報。
ゼロトラスト基盤：組織・人的・物理的・技術的な統合管理（経産省指針・NIST準拠）

短期 (Short-term) - 最優先

施策: 秘密情報棚卸し、退職時権限剥奪の徹底、法的保持手順の策定。

成果物: クラウンジュエル台帳、保全手順書。

中期 (Mid-term) - 高優先

施策: 高リスク部門（営業・FAE）へのDLP・UEM先行導入、監査ログ統合。

成果物: 監視ルール、証跡ダッシュボード。

長期 (Long-term) - ガバナンス定着

施策: 全社ゼロトラスト化、M&A時の買収後100日クリーンアップ計画。

成果物: 取締役会向けKPI、第三者統制標準。

TCO（総所有コスト）目安

- Microsoft 365 E3 ➡ E5への移行を想定。
- 1ユーザー差額: 月額約$21。
- 1,000ユーザー規模の高リスク職種へ先行導入した場合、年間約25.2万ドルの追加投資。
- 訴訟・罰金（1.5億元）と比較し、極めて合理的な防衛コスト。

“本件は単なる従業員の不祥事ではない。
営業秘密管理を経営・営業・人事・法務・ITの
共同責任として再設計しなかった企業体制
企業体制への判決である。”

1. 規程の錯覚

規程は「存在する」だけでは無力。技術的な運用証跡（ログ・DLP）が法人の盾となる。

2. 最前線の脆弱性

リスクの最前線はR&Dの奥深くではなく、顧客と直接接する営業・FAE・クラウド共有にシフトしている。

3. 企業価値の防衛

「法廷での勝敗」よりも「顧客信頼と事業継続」が重要。実効的な再発防止策の実装こそが企業価値を守る最適解。