Executive Risk Advisory & Strategic Briefing

旭化成・営業秘密漏えい事件と経済安全保障の未来

人的資本リスクの再定義と「ゼロトラスト」型ガバナンスへの移行

Gemini Notebook

事件の全容：単なる不正持ち出しを超えた「時限爆弾型」内部脅威

The Actors（関与者）



旭化成（被害企業）

古川祥一被告・66歳（元社員）

山東聖泉新材料股份有限公司（流出先の中国企業・半導体材料の商業化能力を保有）

The Asset（対象情報）



半導体・電子材料用途にも関係する「潜在性硬化剤」の機密データ。

The Core Takeaway（核心的教訓）

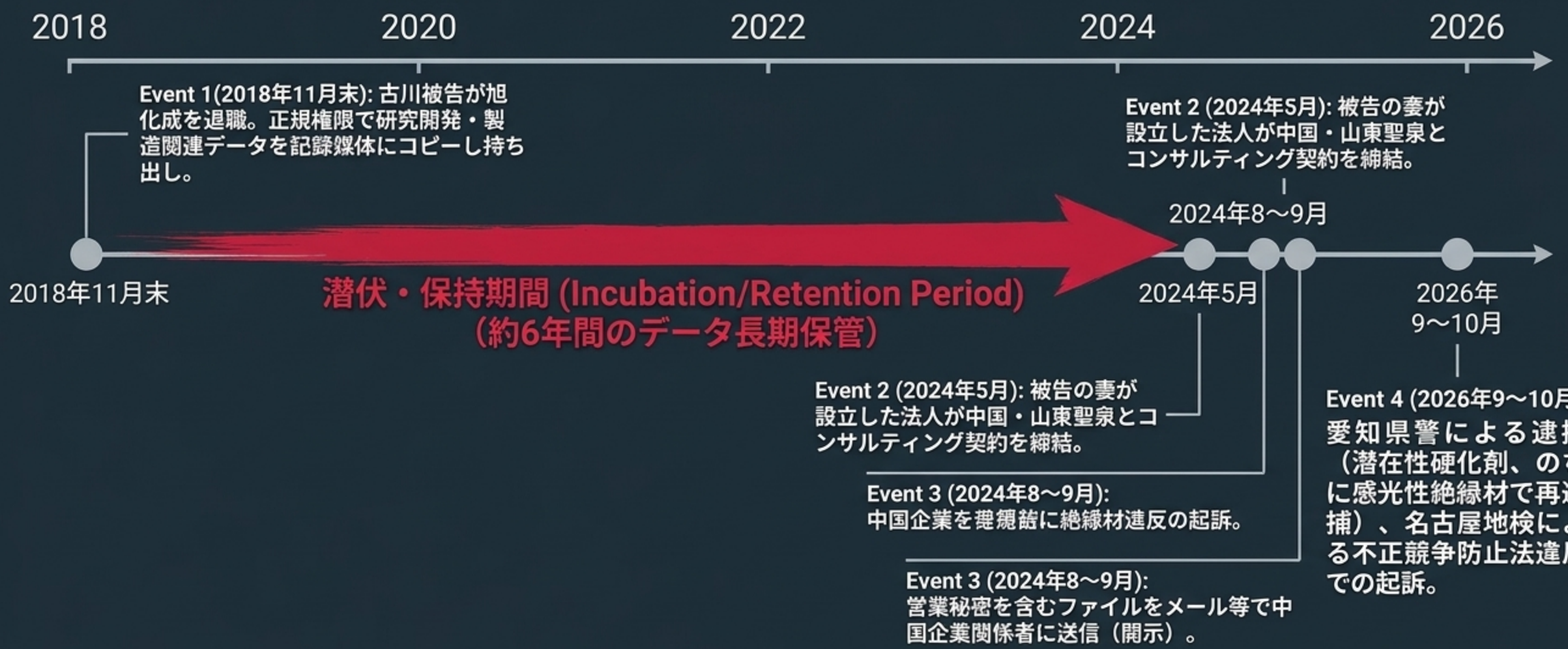


2018年の退職時の持ち出しから2024年の漏えいまで6年間の「潜伏期間」が存在。退職日のアカウント停止だけでは防げない、日本企業の退職者管理の構造的脆弱性が露呈した。

Gemini Notebook

Executive Intelligence Briefing

脅威のタイムライン：退職から漏えいまで「6年間の空白」



Gemini Notebook

脅威アクターのプロファイル：複合的動機と「正規権限」の悪用



Motive 1 (経済的利益)：
中国側からの高額報酬、送迎、専属アシスタントなどの厚遇。「待遇が良く、専門家としての地位を保ちたかった」

Motive 2 (承認欲求・自己誇示)：
退職後の自身の市場価値証明。
「知識や経験が豊富であることを示したかった」「何かに役立つと思った」



Gemini Notebook

証拠構造と法的評価：立証された事実と最大の不確定要素

強い客観証拠（Strong Objective Evidence）

- 押収されたPC・HDD（持ち出しの客観化）
- 電子メール送信記録（第三者への直接的開示）
- 旭化成の内部調査による特定秘密の流出確認
- 漏えい先とのコンサルティング契約の存在

未立証・不確定要素（Unproven Variables）

- 中国企業（山東聖泉）における**実際の製品開発・製造への「利用」の有無**
- 旭化成にもたらされた具体的な**経済損害の規模**



刑事責任は判決確定まで未確定。量刑や民事訴訟の規模は、この「実利用」の有無に大きく左右される。

Gemini Notebook

ガバナンス・ギャップ分析：旭化成の体制と経産省・IPA基準の比較

	旭化成（事件前）	本件後の旭化成（改善策）	経産省・IPAが示す水準
情報分類	○	◑	●
アクセス制御	◑	◑	●
退職者管理	○ 退職者管理と証拠保存が実効性不足	● 誓約書・貸与PC管理強化	● 退職前アクセス制限、数か月遡ったログ監査
DLP・持出監視	◑ 「システム監視」のみで不十分	● 新ITツール導入	● コピー外部送信検知
教育	◑	●	●
退職後の秘密保持	○	◑	● 合理的な退職後誓約
証拠保存	○	◑	●

Insight: IPA調査では中途退職者による漏えい経験企業は17.8%。人を介した漏えいは依然最大の内部リスクである。

Gemini Notebook

過去の重大判例との比較：東芝・SKハイニックス事件が示すリスク水準

旭化成事件（現在）

- 対象：半導体・電子材料（潜在性硬化剤等）
- 主体：元社員
- 動機：専門家としての地位維持・高額報酬
- 損害規模：未確定

東芝・SKハイニックス事件（2014年）

- 対象：NAND型フラッシュメモリ技術
- 主体：元技術者
- 動機：転職先での地位維持
- 結果：懲役5年の実刑・罰金300万円。民事和解金 約331億円。

Key Insight: **「専門家としての地位維持」という動機構造は完全に一致。**中国側で技術の商業利用が立証された場合、**実刑判決および数百億円規模の巨額民事損害賠償に発展するリスクを孕む。**

Gemini Notebook

法的責任の構造：刑事罰の枠組みと民事訴訟における立証の壁

刑事責任（Criminal Liability）– 不正競争防止法違反

自然人に対して原則10年以下の拘禁刑または2,000万円以下の罰金。海外使用等の加重類類型が適用されれば罰金上限3,000万円。量刑は「実利用の有無」と「被害額」に依存。

民事責任（Civil Liability）

差止請求権および損害賠償請求。旭化成はすでに利用停止・廃棄を求める方針を公表。2024年4月法改正により国外侵害への日本法適用が明確化。

The Hurdle: 最大の立証課題:「受領した秘密情報と山東聖泉側の研究成果・製品との因果関係」。相手が独自技術を主張した場合、不正使用の技術的立証は極めて困難。

Gemini Notebook

企業価値・事業への影響予測タイムライン



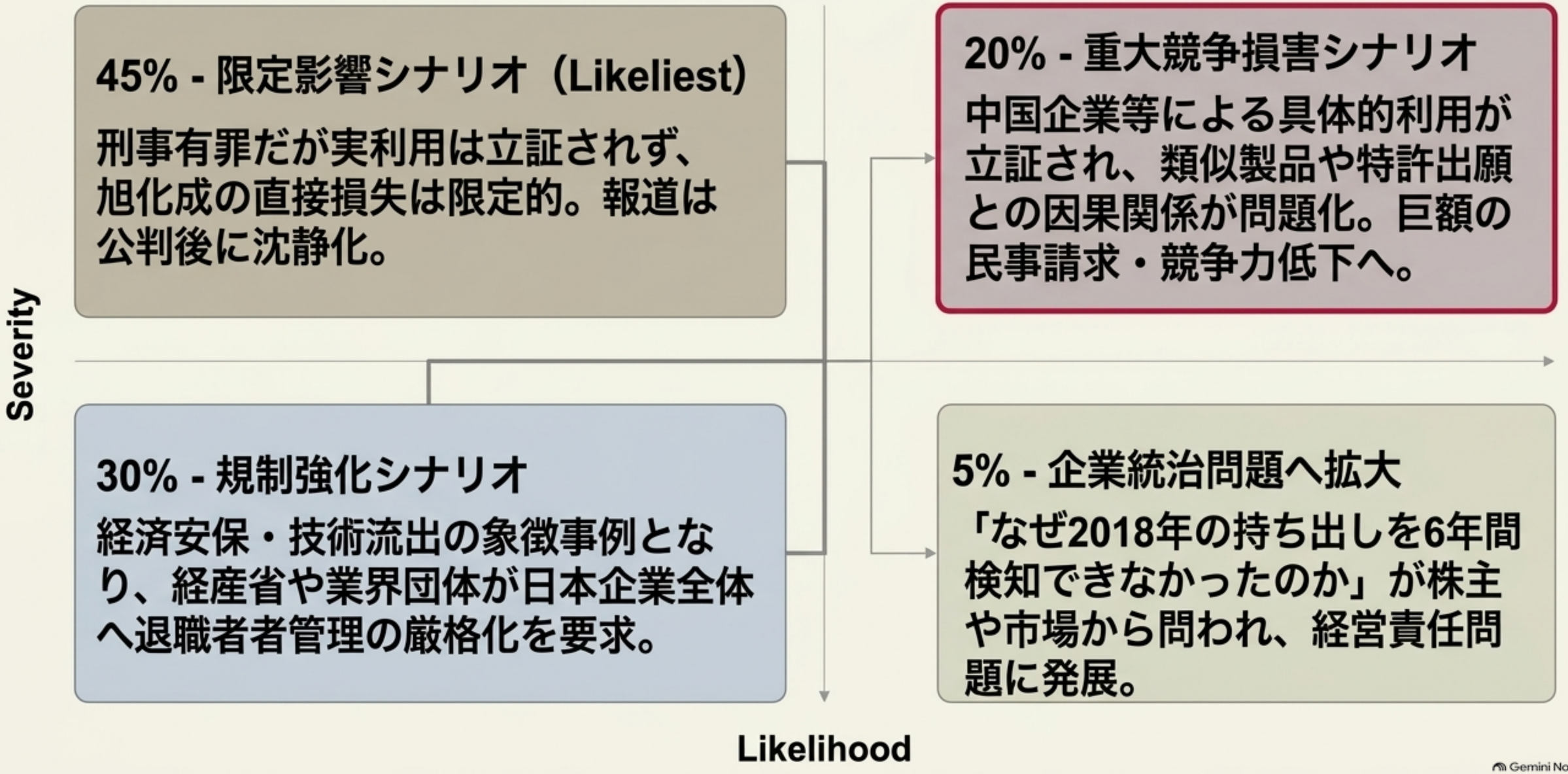
短期（2026年9月-11月 / 2027年）
逮捕・起訴、刑事公判・民事訴訟開始。
株価への直接的影響は低。
主な影響はレピュテーション（中）、
法務・調査コスト（中）、
情報管理投資（中〜高）、顧客監査の
増加（中）。

中期（2027-2028年）
「中国側での利用有無」が最大の焦点。
利用なしなら影響縮小。
利用ありなら競争影響（高）。

長期（2028年以降）
技術差別化への影響判明。
R&D再構築・特許戦略見直し。
業界全体での経済安保規制強化の可能性。

Gemini Notebook

今後の展開シナリオ：4つの確率的予測とトリガー



Gemini Notebook

パラダイムシフト：性善説の終焉と「ゼロトラスト」型R&Dへの移行



経済安全保障の要請
(Economic Security Demands)



Left (旧モデル：性善説と境界防御)

- 従業員の忠誠心を前提。
- 退職時のPC返却と一律の誓約書でよしとする。
- ノウハウを「秘匿」するのみの属人的管理。

Right (新モデル：ゼロトラストと区画化管理)

- フライトリスク (離職・情報持ち出しリスク) を常時想定。
- 重要技術を分割管理（Need-to-Know）し、アクセス履歴を常時監査。
- 退職前から遡及的な監視を実施。

Core Insight: 本件の真のインパクトは、日本の製造業における「退職者・専門家」という人的経路を、独立した経済安全保障リスクとして管理する契機となったことにある。

Gemini Notebook

次世代・経済安全保障防衛フレームワーク（6つの柱）

Pillar 1: 技術的措置
（アクセス制御、DLP、ログ統合）

Pillar 2: 組織的措置
（クロスファンクショナルな退職者レビュー）



Pillar 3: 契約的措置
（解像度の高い秘密保持義務の特定）

Pillar 4: フォレンジック措置
（退職前ログの自動スコアリング）

Pillar 5: 第三者管理
（前職秘密の持ち込み禁止の徹底）

Pillar 6: 取締役会レベルの管理
（独立したKRIとしての監視）

Gemini Notebook

防衛策深掘り(1)：退職前「90〜180日」の遡及的フォレンジック

The Flaw: 「退職申告日」からのアクセス遮断では、計画的な持ち出し (2018年事案) は防げない。

T-180 to T-90: 定常的なDLP監視。異常大量ダウンロード検知、USB/外部HDDへのコピー制御。

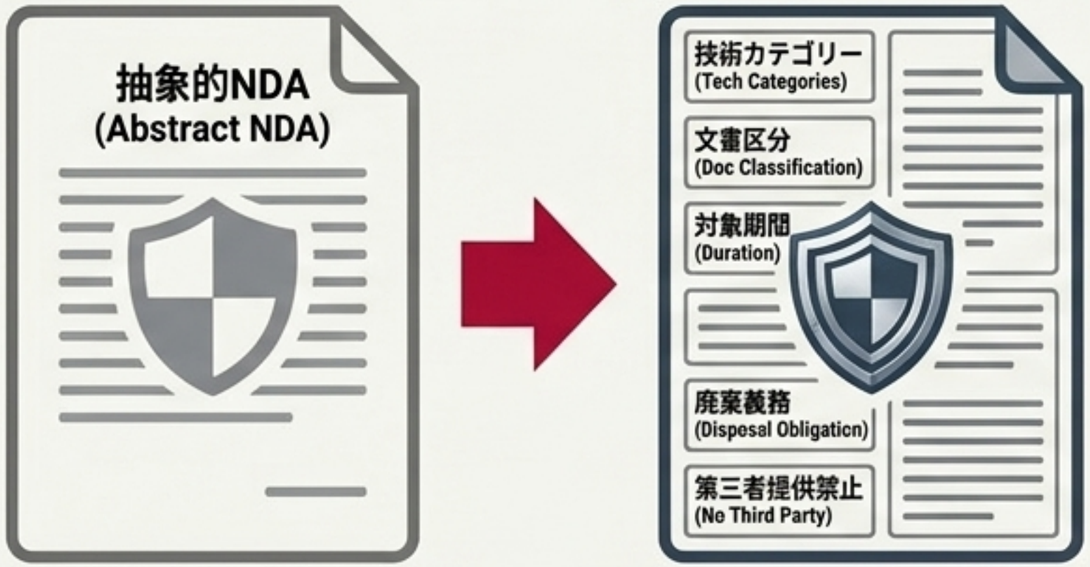
T-90 (Resignation Indication): 退職フラグ起動。過去3〜6ヶ月のログ（個人メール送信、クラウド同期、プリント履歴、ソースコードへの異常アクセス）を自動スコアリング。

T-0 (Departure): 証拠保全。端末依存アクセスの確実な無効化とログの長期保存（経産省・IPA推奨）。

Gemini Notebook

防衛策深掘り(2)：契約の解像度向上と組織的サイロの打破

契約的措置（脱・抽象化）



「一切の情報」とする広範すぎるNDAは実効性を欠く。技術カテゴリー、文書区分、対象期間、廃棄義務、第三者提供禁止を具体的に特定した誓約書へ移行する。（経産省ガイドライン準拠）

組織的措置（退職者リスクレビュー）



退職手続きを人事（HR）単独の事務処理にしない。法務・知財・IT・事業部門が連携する「退職者リスクレビュー」チームを組成。技術責任者や長期在籍研究者など高リスク職種には、通常職より厳格なオフボーディングを義務化する。

Gemini Notebook

取締役会アクションプラン：経営トップが主導すべき3つの命題



Action 1: 技術流出を「独立したKRI」へ格上げ

情報漏えいを一般的なサイバーセキュリティの下位概念として扱わず、知財・経済安全保障・人的資本を横断する独立した重要リスク指標（KRI）として取締役会で監視する。



Action 2: 人的資本リスクと経済安全保障の統合

「退職者・専門家・技術コンサル」という人的経路が最大の脆弱性であることを認識し、人材流動化時代に即したゼロトラスト環境への投資を承認する。



Action 3: サプライチェーン監査とTICSへの備え

経産省が推進するTICS（技術情報管理認証制度）等を見据え、顧客からの技術管理監査（NDA、アクセス管理、データ隔離）に耐えうる体制を構築・維持する。

Gemini Notebook