ChatGPT

台湾半導体営業秘密事件判決と東京エレクトロン子会社の責任分析

Executive Summary

本件は、台湾の智慧財産及商業法院が、東京エレクトロンの台湾子会社である東京威力科創股份有限公司に対し、ＴＳＭＣの国家核心関鍵技術に関わる営業秘密の不正取得・域外使用目的事案について、新台幣一億五千万元の罰金を科した判決です。重要なのは、これは公開一次資料上、**ＴＳＭＣへの民事損害賠償命令ではなく、法人に対する刑事罰としての罰金**である点です。これとは別に、東京エレクトロン側は顧客と和解済みであり、上訴しない方針と、業績への重要な影響は見込んでいない旨を表明しています。 1

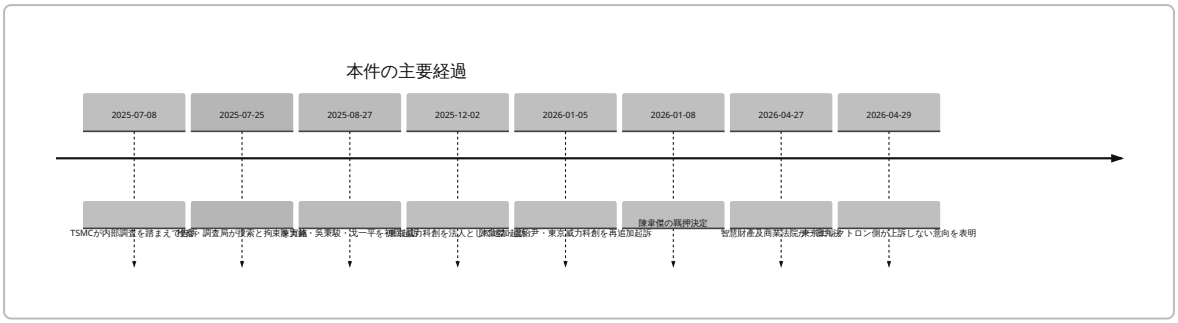
事件の骨格は、元ＴＳＭＣ社員の陳力銘が東京威力科創入社後、ＴＳＭＣ在職者との人的関係を利用して、先端プロセス向けエッチング装置の性能改善・採用拡大を狙い、ＴＳＭＣの営業秘密を写真撮影・複製させたと認定されたことにあります。ＴＳＭＣは社内で異常なファイル接触を検知して内部調査を行い、二〇二五年七月に告訴し、同年八月に初回起訴、同年十二月に法人追加起訴、二〇二六年一月に十四ナノ以下製程情報と証拠隠滅行為に関する追加起訴が行われ、二〇二六年四月に一審判決が出ました。 2

法的には、台湾国家安全法の「国家核心関鍵技術営業秘密」の域外使用目的犯と、営業秘密法の一般的な営業秘密侵害罪、さらに法人両罰規定が中核です。法人責任のポイントは、**従業員らの行為が「執行業務」に当たること**と、会社側が「犯罪の発生について尽力して防止した」ことを立証できなければ、法人にも罰金刑が及ぶという構造です。台湾の判例・行政ガイドを踏まえると、形式的な倫理規程や抽象的なＮＤＡだけでは足りず、誰が何にアクセスできるか、どう監査し、どう退職・異動・顧客常駐・ベンダー連携を統制するかという**具体的・技術的・継続的な管理**が要件充足に直結します。 3

実務上の示唆は明快です。第一に、営業・フィールドアプリケーション・顧客常駐人材を含む「顧客接点部門」を、研究開発部門と同等以上の漏えい高リスク部門として扱うこと。第二に、持ち出し防止はＤＬＰ単体ではなく、データ分類、最小権限、ゼロトラスト、エンドポイント管理、証拠保全、内部通報、雇用契約、第三者・Ｍ＆Ａデューデリジェンスを束ねた統合プログラムとして再設計すること。第三に、過度に広い競業避止条項へ依存せず、台湾労基法上有効な範囲に収めつつ、**秘密管理と監査可能性**を前面に出した運用へ転換することです。 4

事件の全体像と時系列

公開一次資料で確認できる範囲では、本件はＴＳＭＣの社内検知から始まり、台湾高等検察署智慧財産檢察分署による複数段階の起訴を経て、智慧財産及商業法院が個人と法人の双方に有罪判断を示した事件です。なお、和解条件の内容、社内処分の詳細、取締役会での具体的審議内容、判決全文における全量の論理構成は、少なくとも本報告作成時点で一般公開資料からは確認できず、未指定として扱います。 5



上の時系列は、検察・裁判所・報道の公開資料を統合したものです。ＴＳＭＣは在職員のファイル接触異常を検知し、内部調査後に告訴しました。検察は七月下旬に被告らの住居等を捜索して三人の羈押禁見を請求し、その後、二奈米製程用エッチング設備の站點獲得を狙った営業秘密取得として初回起訴を行いました。さらに、東京威力科創の法人責任を同年十二月に、十四ナノ以下製程情報と証拠削除行為を二〇二六年一月に追加起訴し、四月の判決へ至っています。 2

時点	関係者	行為・出来事	法的・実務的意味	主な根拠
二〇二五年七月	ＴＳＭＣ、智慧財產檢察分署	ＴＳＭＣが在職員の異常なファイル接触を検知し、内部調査後に告訴	企業側の**内部監視とログ分析**が刑事立件の起点になった	6
二〇二五年七月下旬	検察、調査局、陳力銘ら	住居所等の捜索、伝喚・拘提、三人の羈押禁見請求	初動で証拠保全と身柄確保を優先した典型的な営業秘密捜査	6
二〇二五年八月	陳力銘、吳秉駿、戈一平	二奈米製程エッチング站點の量産機台資格獲得を目的に、ＴＳＭＣの営業秘密を提供・重製したとして起訴	改正国家安全法下の**国家核心関鍵技術営業秘密**事件としての最初期事例	7
二〇二五年十二月	東京威力科創	法人として四罪で追加起訴、検察は合計一億二千万元の罰金を求刑	法人両罰規定の適用。会社の一般規程だけでは「尽力防止」の抗弁に足りないとの当局判断	8
二〇二六年一月	陳韋傑、盧怡尹、東京威力科創	十四ナノ以下製程の情報、雲端硬碟内資料、証拠削除行為について再追加起訴	事件が**二奈米関連に限らず、十四ナノ以下設備・材料技術**にも拡張したことを示す	9
二〇二六年四月	智慧財產及商業法院	陳力銘に十年、吳秉駿に三年、戈一平に二年、陳韋傑に六年、盧怡尹に十月・緩刑三年、東京威力科創に一億五千万元罰金・緩刑三年	個人刑責と法人刑責を同時に明示。公開資料上、**罰金は公法上制裁であり、ＴＳＭＣへの民事賠償命令ではない**	10
判決後	東京エレクトロン側	上訴しない、顧客と和解済み、事業・業績への重要影響は見込まないと説明	刑事判決と商業和解が並行し得ることを示す	11

本件の証拠構造は、秘密情報窃取事件で典型的に重視される五類型から成ります。すなわち、①ＴＳＭＣの社員アカウント・監視システムログ、②簡訊や電子メール添付、③東京威力科創のクラウド保存ファイル、④翻拍・撮影された機密資料、⑤保密協定と関係者供述です。追加起訴部分では、クラウド上に残った十四ナノ以下製程関連資料と、それを削除した行為自体が新たな犯罪事実とされました。 12

関係者	役割	認定された主な行為	公開資料で確認できる主要証拠	根拠
陳力銘	元ＴＳＭＣ社員、後に東京威力科創営業部門	ＴＳＭＣ在職者に技術・営業秘密提供を求め、撮影・重製して装置改善に利用	簡訊、電子メール、翻拍資料、証人供述、クラウド資料	13
吳秉駿・戈一平	ＴＳＭＣ在職エンジニア	先端製程関連秘密の提供	保密協定、対話記録、業務接触情報	14
陳韋傑	ＴＳＭＣ在職者	同僚アカウントで資料庫へログインし、国家核心関鍵技術情報を重製・送信	資料庫ログ、監控系統紀錄、メール添付、東京威力クラウド資料	15
盧怡尹	東京威力科創社員	陳力銘のアップロード資料を削除し、証拠隠滅	クラウド削除状況、事件認識後の行動経過	16
東京威力科創	法人	従業員監督・防止措置が不十分と認定	内部規範、答弁資料、クラウド管理実態	17

法的根拠と判決の読み解き

本件の法的基盤は、台湾国家安全法、営業秘密法、中華民國刑法、そして国家核心関鍵技術認定制度です。国家安全法第三条は、外国・中国大陸・香港・澳門等での使用目的をもって、国家核心関鍵技術の営業秘密を不正取得・使用・漏示する行為を禁じ、同法第八条は個人刑と法人両罰、さらに「已盡力為防止行為者」の免責抗弁を定めています。営業秘密法は第二条で営業秘密の三要件を示し、第十三条之一・之二で一般の営業秘密侵害と域外使用目的犯を処罰し、第十三条之四で法人併罰を定めます。証拠削除には刑法第百六十五条・第百六十六条が対応します。 18

法源	本件での機能	実務上の意味	主な根拠
国家安全法第三条・第八条・第十八条	国家核心関鍵技術営業秘密の不正取得・域外使用目的犯、法人両罰、知財商業法院の専属管轄	通常の営業秘密事件より重い刑と、法人責任の追及を可能にする	19
営業秘密法第二条	秘密性、経済価値、合理的保密措置の三要件	「何が営業秘密か」の入口判断	20
営業秘密法第十三条之一・之二	一般の営業秘密侵害と域外使用目的犯	国家安全法該当前でも、一般営業秘密罪と並存し得る	21
営業秘密法第十三条之四	法人・自然人への併罰	管理監督不全が法人の独立リスクになる	22

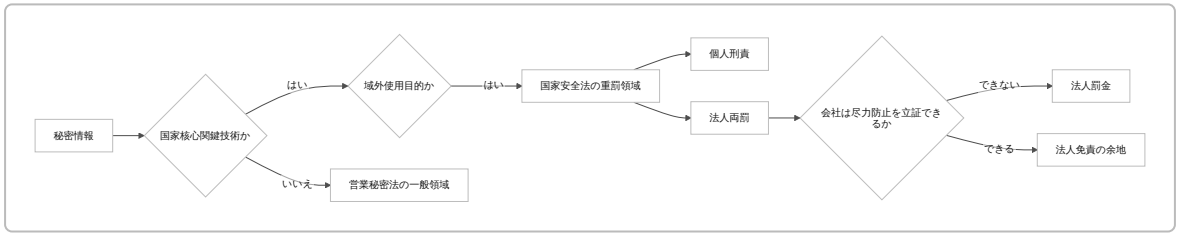
法源	本件での機能	実務上の意味	主な根拠
中華民國刑法第百六十五条・第百六十六条	他人の刑事事件証拠の隠滅と自白による減免	証拠削除が独立の犯罪になる	23
国家核心関鍵技術認定辦法	認定手続、主管機関、定期見直し	刑罰適用の前提となる「国家核心関鍵技術」認定の制度面	24

本件を通常の転職漏えいより重くしたのは、単なる営業秘密法違反ではなく、**国家安全法上の「国家核心関鍵技術」**をめぐる域外使用目的犯として処理された点です。検察は、二奈米製程向けエッチング設備の站點獲得を狙って営業秘密が取得されたと位置づけ、追加起訴では雲端硬碟内に「十四ナノ以下製程のＩＣ製造技術及其關鍵氣體、化學品及設備技術」に関する資料が残っていたと具体的に摘示しました。 25

法人責任については、「会社が直接命令した」ことまで公開資料上は要件化されていません。国家安全法第八条第七項と営業秘密法第十三条之四は、代表者・代理人・受雇人等が**執行業務により**犯罪をしたとき、行為者本人とは別に法人にも罰金刑を科す構造であり、会社側が「尽力して防止した」と示せなければ逃れにくい設計です。検察は、東京威力科創が一般的・警告的な内部規範を備えていたこと自体は認めつつも、具体的な防範管理措置の履行事実が不足すると評価しました。 26

台湾実務の「合理的保密措施」論は、本件の予防策を考えるうえでも重要です。智慧財産及商業法院や関連裁判要旨では、合理的保密措置とは、所有者が主観的に秘密保護意思を持ち、客観的に積極的な保密行為をとって、不要な者に触れさせず、必要な者にも必要範囲でのみ触れさせることだと整理されています。逆に、共有槽・共用フォルダで広く閲覧可能であったり、一般的な管理規程しかなく技術的統制がない場合には、営業秘密性や防止努力を弱めます。 27

雇用契約・競業避止については、台湾労動基準法第九条の一が、保護すべき正当利益、秘密接触職務、合理的な期間・地域・範囲・就業対象、合理的補償の四要件を課し、最長二年としています。さらに、最高法院一〇九年度台上字第一六一六号判決の要旨では、**全球・無補償の競業避止**は顕失公平無効となり得ると示されました。したがって、実務の重点は「広く縛ること」ではなく、「誰が秘密に触れるかを明確にし、退職前後にどう制御するか」に移ります。 28



上の法的フローは、本件の公開資料から読み取れる論理を抽象化したものです。つまり、対象情報の性質、域外使用目的、従業員の業務執行性、会社の防止努力の四点が、刑の重さと法人責任の分水嶺になっています。 29

東京エレクトロン側の主張と対応、元従業員の役割、監督責任

公開資料で確認できる東京エレクトロン側の明示的な対外メッセージは限定的です。もっとも確度が高いのは、判決後に同社が**上訴しない方針**を示し、**顧客と和解済み**であり、**今後の事業・財務見通しに重大な悪影**

響は見込まないと説明した点です。逆に、和解条件、内部処分、取締役会の是正計画、保険填補の有無などは公開確認できず、未指定です。 [11]

検察資料から確認できる「会社側の主張」は、主として、内部規範や答弁資料を通じて防止努力を示そうとした点です。しかし検察は、東京威力科創には陳力銘に対する監督責任があり、提出された資料を検討しても、内部規範は一般的・警告的なものにとどまり、**具体的な防範管理措置を履行した事実が不足する**として、国家安全法第八条第七項等の法人刑責で追加起訴しました。つまり、会社のロジックと当局の評価が食い違った争点は、「規程があるか」ではなく「規程が具体的に機能していたか」にあります。 [8]

元従業員の役割は、本件の企業責任を理解するうえで決定的です。陳力銘は、もともとＴＳＭＣ十二廠の良率部門エンジニアで、離職後に東京威力科創の行銷部門へ移りました。検察は、陳力銘がＴＳＭＣ時代に身につけた内部統制・機密保護の運用を熟知していたにもかかわらず、旧知のＴＳＭＣ在職者に技術・営業秘密の提供を求め、それを撮影・重製し、東京威力科創のエッチング機台の改善とＴＳＭＣ二奈米製程の供給站點獲得に役立てようとしたと述べています。これは、個人の私的逸脱ではなく、**業績・営業上の利益追求と結びつく業務行為**として位置づけられやすい構図です。 [30]

追加起訴された陳韋傑と盧怡尹の存在も、監督責任論を強めました。陳韋傑について裁判所は、同僚のアカウント・パスワードを借りてＴＳＭＣ資料庫にアクセスし、「f」とされた国家核心関鍵技術情報を重製して陳力銘へ送ったとする嫌疑を重大と見て羈押しました。盧怡尹については、陳力銘の行為がＴＳＭＣに発覚したことを知った後、東京威力科創のクラウド上の関連図檔を削除し、証拠隠滅罪で有罪とされています。*秘密取得・共有・隠滅が同じ企業システム上で連続していた**ことは、組織統制の失敗を印象づける事情でした。 [31]

この点を日本企業のガバナンス言語に引き直すと、本件の監督責任法理は「取締役が違法行為を指示したか」よりも、「高リスク職種に対し、必要最小権限、利用目的限定、持出し制御、ログ監査、退職・異動統制、証拠保全措置を運用していたか」を問う**デューデリジェンス防御**です。経済産業省の営業秘密管理指針も、営業秘密の管理を単なる契約論ではなく、組織・人的・物理的・技術的な統合管理として捉えています。 [32]

論点	当局・裁判所が重視した点	日本企業への含意	根拠
元社員の業務執行性	元ＴＳＭＣ社員が東京威力科創の営業目的で情報取得を主導した	営業・ＦＡＥ・顧客常駐人材も「高機密アクセス職」として扱う必要	14
監督責任の抗弁	一般規程のみで具体的な防止措置が見えない	規程より運用証跡。アクセス権台帳、例外承認記録、監査結果が必要	33
クラウド管理	会社雲端系統にＴＳＭＣ資料が残存	ＳａａＳ・共有ドライブの保全と監査証跡が最重要	16
証拠削除	社員が関連図檔を削除し有罪	法的保持とインシデント時の削除停止を即時発動すべき	34
対外対応	上訴せず、顧客と和解済みと説明	刑事・顧客関係・開示対応を分けて同時並行で処理する体制が要る	11

類似事件との比較

本件を位置づけるには、台湾・日本・米国の半導体関連営業秘密事件との比較が有益です。比較すると、**元従業員の移籍、顧客・競争関係、国外使用目的、法人責任、巨額の民事和解または制裁**という共通パターン

が見えますが、本件はその中でも「国家核心関鍵技術」と「台湾国家安全法」の組み合わせが際立っています。[35]

事件	概要	主な法的構図	帰結	本件との比較ポイント	根拠
ＴＳＭＣ対東京威力科創	元ＴＳＭＣ社員・在職者を通じ、先端製程関連秘密が東京威力科創側へ流れたと認定	台湾国家安全法＋営業秘密法＋法人両罰	個人有罪、法人に新台幣一億五千万元罰金	国家安全保障色が強く、会社の防止努力不足が正面から問われた	[36]
美光対聯電・晋華	元 Micron Taiwan 社員らがＤＲＡＭ関連秘密を聯電・晋華へ流したとされる事件	台湾営業秘密法、米国連邦営業秘密法、経済安全保障	台湾で有罪判断の要旨、聯電は米国で有罪答弁し六千万ドル罰金	**元従業員経由の移転**と**国境横断利用**の構図が本件と近い	[37]
東芝対ＳＫハイニックス	ＮＡＮＤフラッシュの機密情報不正取得をめぐる民事紛争	日本の営業秘密・不競法を基盤とする民事・和解実務	二億七千八百万ドルで和解、協業拡大も発表	紛争と取引継続が両立し得る点が、本件の「和解済み」説明と通じる	[38]
ＡＳＭＬ対ＸＴＡＬ	元従業員が関与したソフトウェア・知財窃取をめぐる米国民事訴訟	米国 trade secrets・injunction 実務	最終判決で八億四千五百万ドル相当	民事賠償・差止めの露出は刑事罰金を大きく上回り得る	[39]

比較から得られる示唆は三つあります。第一に、半導体装置・製造プロセス・設計ルールのいずれであっても、**人の移動を介して漏えいが起きる**こと。第二に、国家安全保障や対中・域外利用が絡むと、純粋な企業間紛争を超えて、刑事・通商・輸出管理・投資審査へ波及しやすいこと。第三に、和解によって顧客関係の一部が修復されても、刑事責任や再発防止義務は消えないことです。[40]

再発防止策と実行ロードマップ

再発防止策は、台湾の「合理的保密措施」実務、日本の経産省営業秘密管理指針、米国ＮＩＳＴ・ＣＩＳＡ・ＤＯＪのガイダンスを横断すると、①秘密情報の明確化、②最小権限とゼロトラスト、③持出し検知と証拠保全、④人事・法務の出口管理、⑤内部通報、⑥第三者・Ｍ＆Ａ管理の六本柱に収れんします。ＤＬＰは重要ですが、それ単体ではなく、「data at rest / in motion / in use」を扱う統合制御として位置づける必要があります。[41]

領域	具体策	本件との結び付き	実装の勘所	主な根拠
データ分類	先端製程、装置レシピ、顧客要求、評価結果、設計ルールを「クラウンジュエル」として台帳化	何が国家核心関鍵技術・営業秘密かを可視化しないと防御不能	法務・技術・営業の共同棚卸しを四半期更新	[42]

領域	具体策	本件との結び付き	実装の勘所	主な根拠
アクセス管理	最小権限、職務分離、ＪＩＴ付与、強い認証、ゼロトラスト	不要者への共有を防ぎ、「尽力防止」の立証材料になる	異動・兼務・出向時に自動再審査	43
ＤＬＰ・ＩＲＭ	メール、クラウド、ＵＳＢ、印刷、スクリーンショット、生成ＡＩ入出力を監視	写真撮影・重製・送信・削除の連鎖を早期に検知	高リスク部門から先行導入し、誤検知を調整	44
エンドポイント管理	ＭＤＭ／ＵＥＭ、管理外端末遮断、特権昇格制御、外部媒体制限	証拠削除や持出しの痕跡を残しやすくする	研究端末と営業端末を別ポリシーに分離	45
雇用契約・競業避止	秘密情報定義の具体化、退職時確認書、合理的範囲の競業避止、補償設計	広すぎる競業避止は無効化され得る一方、具体的守秘は有効性が高い	台湾法の四要件と二年上限を前提に設計	28
監査・証拠保全	法的保持、削除停止、クラウド保全、監査ログ集中管理	盧怡尹の証拠削除類型を防ぐ	インシデント発報から一時間以内の保全手順を標準化	46
内部通報	部門横断窓口、独立性、外部委託窓口、予算・人員の確保	現場が早期に異常を上げられる経路を作る	人事窓口と兼ねてもよいが独立性が要る	47
第三者・Ｍ＆Ａ	ベンダー・顧客受領情報の出所確認、クリーンルーム、買収前後ＤＤ	「持ち込まれた秘密情報」を会社が受け取るリスクを下げる	買収後百日以内の秘密情報クリーンアップを標準化	48

コスト感は、企業規模が未指定であるため、**一千ユーザー規模の目安**で示すのが実務的です。公表価格ベースでは、Microsoft 365 E3 が一ユーザー月額三十六ドル、E5 が五十七ドルで、差額は二十一ドルです。単純計算では、一千ユーザーを E3 から E5 へ上げると年間約二十五万二千ドルの追加ライセンス負担になります。さらに、Purview の一部機能は資産課金や DSPU ベースの従量課金であり、Intune Suite は Intune Plan 1 前提です。したがって、**全社一括導入より、高リスク職種・高秘密区分からの段階導入**が合理的です。 49

期間	優先施策	主要成果物	コスト感	優先度
短期	秘密情報棚卸し、退職・異動時権限剥奪、外部送信・ＵＳＢ制御の緊急強化、法的保持手順、内部通報窓口の再設計	クラウンジュエル台帳、ＪＭＬ統制表、保全手順書、通報運用規程	低〜中。既存基盤活用なら追加ライセンスは限定的	最優先 50
中期	ＤＬＰ・ＩＲＭ・ＵＥＭの高リスク部門先行導入、営業・ＦＡＥ・常駐人材の権限再設計、監査ログ統合	高リスク部門の監視ルール、例外承認記録、証跡ダッシュボード	中〜高。ライセンス uplift と運用設計が発生	高 51
長期	ゼロトラスト化、秘密情報クリーンルーム、買収先ＤＤ標準、インサイダーリスク委員会、定期レッドチーム	取締役会向けＫＰＩ、買収後百日計画、第三者統制標準	高。ツール費よりもプロセス・人員整備が支配的	高 52

このロードマップで重要なのは、短期に「違法持出しを難しくし、起きても消せない」状態をつくり、中期に「高リスク人材とデータフローを見える化」し、長期に「会社全体の商流・人流・買収流入まで統合管理」することです。経産省指針、ＣＩＳＡのインサイダー脅威ガイド、ＤＯＪのＭ＆Ａガイダンスを突き合わせても、成功パターンはこの順序にほぼ一致します。 53

リスク評価と優先順位

日本企業が本件から引き出すべきリスクは、抽象的な「技術流出」ではありません。より具体的には、**転職・出向・顧客常駐・ベンダー連携・買収統合**という企業活動の通常プロセスの中に、営業秘密侵害と法人責任のトリガーが埋め込まれている点です。警察庁も、日本では営業秘密侵害事犯の検挙が二〇二四年に二十二事件あり、転職・独立時の持出しが多いと明示しています。これは本件の構造が台湾特有ではなく、日本企業にも高い再現性を持つことを示します。 54

リスク項目	影響度	発生可能性	優先順位	理由	主な根拠
退職・転職局面での持出し	極めて高い	高い	最優先	本件の起点であり、日本でも典型パターン	55
営業・ＦＡＥ・顧客常駐人材の過剰アクセス	極めて高い	高い	最優先	元ＴＳＭＣ社員が営業部門で顧客攻略に秘密を使った構図	56
共有クラウド・共用フォルダの権限放置	高い	高い	最優先	台湾実務は「不要者に触れさせない」を重視し、本件でもクラウド残存が争点	57
証拠削除・ログ不備	高い	中〜高	最優先	証拠隠滅は独立犯罪で、企業防御も困難化する	34
抽象的規程だけで具体運用がない状態	高い	高い	最優先	法人の「尽力防止」抗弁が弱くなる	58
無効な競業避止条項への依存	中〜高	中	高	全球・無補償型は無効リスクが高く、本質的防御にならない	59
ベンダー・顧客からの受領情報の出所不明	高い	中	高	「持ち込まれた秘密」を使う側にも重大責任が及ぶ	60
Ｍ＆Ａ後の秘密情報持込・未統合環境	高い	中	高	ＤＯＪは買収前後ＤＤと統合を明示的に評価対象化	48
内部通報不全	中	中〜高	中	異常兆候が制度外に流れると初動が遅れる	61

結論として、本件は「元従業員の不祥事」ではなく、**営業秘密管理を経営・営業・人事・法務・情報システムの共同責任として再設計しなかった企業のリスク**を可視化した判決です。法人に求められているのは、規程の整備そのものではなく、秘密情報の分類、最小権限、持出し制御、証跡、通報、買収・第三者管理まで含めた**実効的な管理の運用証明**です。東京エレクトロン側が和解し上訴を見送ったことも、この種の事案では「法廷勝敗」よりも「顧客信頼、規制対応、再発防止の実装」の方が企業価値に与える影響が大きいことを示しています。 62

1 10 36 https://ipc.judicial.gov.tw/tw/cp-663-2849455-f5180-091.html
https://ipc.judicial.gov.tw/tw/cp-663-2849455-f5180-091.html

2 5 6 https://www.thip.moj.gov.tw/12606/914012/12690/1313833/post
https://www.thip.moj.gov.tw/12606/914012/12690/1313833/post

3 18 19 26 29 https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030028
https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=A0030028

4 https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide
https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide

7 13 14 25 30 55 56 https://www.thip.moj.gov.tw/12606/914012/12690/1320976/post
https://www.thip.moj.gov.tw/12606/914012/12690/1320976/post

8 17 33 58 62 https://www.thip.moj.gov.tw/12606/914012/12690/1349105/post
https://www.thip.moj.gov.tw/12606/914012/12690/1349105/post

9 12 16 34 46 57 https://www.thip.moj.gov.tw/12606/914012/12690/1359708/post
https://www.thip.moj.gov.tw/12606/914012/12690/1359708/post

11 https://jp.reuters.com/world/security/5XCV5G3AI5PUTPKIWDAVVQTGLE-2026-04-27/
https://jp.reuters.com/world/security/5XCV5G3AI5PUTPKIWDAVVQTGLE-2026-04-27/

15 31 https://www.judicial.gov.tw/tw/cp-1888-1475163-3c2d6-1.html
https://www.judicial.gov.tw/tw/cp-1888-1475163-3c2d6-1.html

20 42 https://law.moj.gov.tw/LawClass/LawSingle.aspx?flno=2&pcode=J0080028
https://law.moj.gov.tw/LawClass/LawSingle.aspx?flno=2&pcode=J0080028

21 60 https://law.moj.gov.tw/LawClass/LawSingle.aspx?flno=13-1&pcode=J0080028
https://law.moj.gov.tw/LawClass/LawSingle.aspx?flno=13-1&pcode=J0080028

22 https://law.moj.gov.tw/LawClass/LawSingle.aspx?flno=13-4&pcode=J0080028
https://law.moj.gov.tw/LawClass/LawSingle.aspx?flno=13-4&pcode=J0080028

23 https://law.moj.gov.tw/LawClass/LawSingle.aspx?flno=165&pcode=C0000001
https://law.moj.gov.tw/LawClass/LawSingle.aspx?flno=165&pcode=C0000001

24 https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=H0160089
https://law.moj.gov.tw/LawClass/LawAll.aspx?pcode=H0160089

27 https://www.tipo.gov.tw/wSite/public/Attachment/0/f1744269405311.pdf
https://www.tipo.gov.tw/wSite/public/Attachment/0/f1744269405311.pdf

28 59 https://law.moj.gov.tw/LawClass/LawSingle.aspx?flno=9-1&pcode=N0030001
https://law.moj.gov.tw/LawClass/LawSingle.aspx?flno=9-1&pcode=N0030001

32 41 50 53 https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/r7ts.pdf
https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/r7ts.pdf

35 40 https://www.justice.gov/archives/opa/pr/taiwan-company-pleads-guilty-trade-secret-theft-criminal-case-involving-prc-state-owned
https://www.justice.gov/archives/opa/pr/taiwan-company-pleads-guilty-trade-secret-theft-criminal-case-involving-prc-state-owned

37 https://www.judicial.gov.tw/tw/cp-1888-230692-b054f-1.html
https://www.judicial.gov.tw/tw/cp-1888-230692-b054f-1.html

38 https://jp.reuters.com/article/world/japan/-idUSKBN0JX0RK/
https://jp.reuters.com/article/world/japan/-idUSKBN0JX0RK/

39 https://www.asml.com/news/press-releases/2019/us-court-issues-final-judgment-in-favor-of-asml-against-xtal
https://www.asml.com/news/press-releases/2019/us-court-issues-final-judgment-in-favor-of-asml-against-xtal

43 https://csrc.nist.gov/glossary/term/least_privilege
https://csrc.nist.gov/glossary/term/least_privilege

44 https://www.nist.gov/publications/data-loss-prevention
https://www.nist.gov/publications/data-loss-prevention

45 https://www.microsoft.com/ja-jp/security/business/microsoft-intune
https://www.microsoft.com/ja-jp/security/business/microsoft-intune

47 https://www.caa.go.jp/policies/policy/consumer_partnerships/whisleblower_protection_system/overview
https://www.caa.go.jp/policies/policy/consumer_partnerships/whisleblower_protection_system/overview

48 https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl?inline=
https://www.justice.gov/criminal/criminal-fraud/page/file/937501/dl?inline=

49 https://www.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-plans-and-pricing
https://www.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-plans-and-pricing

51 https://azure.microsoft.com/en-us/pricing/details/purview/
https://azure.microsoft.com/en-us/pricing/details/purview/

52 https://csrc.nist.gov/pubs/sp/800/207/final
https://csrc.nist.gov/pubs/sp/800/207/final

54 https://www.npa.go.jp/publications/statistics/safetylife/R06_nennpou_teisei.pdf
https://www.npa.go.jp/publications/statistics/safetylife/R06_nennpou_teisei.pdf

61 https://www.caa.go.jp/policies/policy/consumer_partnerships/whisleblower_protection_system/overview/assets/overview_211013_0001.pdf
https://www.caa.go.jp/policies/policy/consumer_partnerships/whisleblower_protection_system/overview/assets/overview_211013_0001.pdf