台湾TSMC最先端技術流出事件の深層と日本企業における技術混入防止の要諦

Gemini 3.5 Flash

緒言と事件の本質

2026年4月27日、台湾の知的財産商業裁判所において、台湾積体電路製造（TSMC）の最先端プロセス技術である2 nm世代の営業秘密を組織的・継続的に不正取得したとして、東京エレクトロン（TEL）の台湾子会社（以下、TEL台湾）および関係者らに対し、有罪判決が言い渡された[1]。この判決は、2022年に改正された台湾国家安全法が定める「国家核心關鍵技術（国家核心技術）」の営業秘密保護条項が、法人および個人に対して初めて適用された記念碑的な事例となった[1]。

半導体微細化の物理的限界が迫る中、次世代の主導権を握るための開発競争は、かつてないほど激化している[5]。本事件の本質は、単に従業員が自社の営業秘密を競合他社へ流出させたという従来型のアウトバウンド型情報漏洩にとどまらない[3]。真の脅威は、中途採用した他社のエンジニアや既存顧客のネットワークを悪用し、他社の営業秘密を自社の製品開発や性能改善のプロセスへ不正に引き入れる「インバウンド型技術混入（コンタミネーション）」にある[3]。

装置サプライヤーであるTEL台湾のマーケティング部門に所属する元TSMCエンジニアが、自社製エッチング装置の性能向上を図り、TSMCの2 nmプロセス量産ラインにおける装置サプライヤーとしての選定（納入権の獲得）を優位に進めるという利己的なインセンティブが、この巨大なコンプライアンス違反を引き起こした[3]。この問題は、単に現地法人の一部門における偶発的な不祥事として片付けることはできない。グローバルな技術競争に身を置く全ての日本企業に対し、他社技術の「不正流出」のみならず、自社内への「不正流入」を防ぐための多層的な防御機構の構築を義務付けるものである[3]。

事件の事実関係と時系列の精査

本事件は、2023年下半期から2024年上半期にかけての陳力銘（元TSMCエンジニア、後にTEL台湾マーケティング部門に勤務）の執拗な情報収集行為を端緒とする[3]。陳は、TSMCの現職エンジニアらに対して、TSMCの最先端2 nm技術に関する製造工程の写真や内部ファイルなどの営業秘密を繰り返し要求した[3]。現職のエンジニアらは、これらの要求に応じて機密ファイルを複写・撮影し、陳へ共有した[3]。共有されたデータの中には、プロセスの詳細を示す約400枚に及ぶ写真などが含まれていた[5]。

TSMCの内部監査チームは2024年7月8日、システムアクセスログの異常検知から情報の不正取得の疑いを察知し、台湾検察当局へ告発した[3]。これを受け、台湾高等検察署は同年7月25日から28日にかけて強制捜査を断行し、関係者の逮捕および身柄の拘束、家宅捜索を行った[3]。捜査当局とTSMCは、この事件を台湾の経済的ライフラインを脅かす国家安全保障上の歴史的重大事件と捉え、異例の「超スピード捜査」を展開した[3]。結果として、摘発からわずか1ヶ月後の2025年8月27日には第1波の起訴が行われた[3]。

事件の波紋は、東京エレクトロンのグループ経営体制を大きく揺るがした[3]。2025年9月には、東京エレクトロン本社の河合利樹代表取締役社長CEOが急遽訪台してTSMCへ謝罪し、事態の収拾を図った[10]。これと時を同じくして、TEL台湾の伊東晃董事長および張天豪総裁が事実上の引責辞任

に追い込まれ、経営幹部の刷新を余儀なくされた[10]。
その後、検察当局のデジタルフォレンジック調査の過程で、TEL台湾が共有するクラウドストレージ内から、TSMCが厳格に管理する国家核心關鍵技術に該当する営業秘密（14 nm以下のIC製造技術に関する12ページにおよぶ極秘ファイル）が検出された[3]。これにより、法人が従業員に対する監督義務を怠っていたという組織的過失が客観的に証明され、2025年12月2日にTEL台湾（法人）が国家安全法違反の罪で追加起訴されるに至った[3]。2026年1月には、更なる証拠隠滅を意図したファイル削除の疑いでTEL台湾の元主管である盧怡尹らが追加起訴され、2026年4月27日に一審判決が言い渡された[3]。
TEL台湾は、判決で指摘された監督責任の不備を厳粛に受け止め、さらなる情報管理体制の強化を約束するとともに、2026年5月21日に本判決に対する控訴を断念する（一審判決を受け入れる）旨の書面回答を表明し、本訴訟は司法的に確定した[3]。

年月日	主な出来事と司法手続きの展開
2023年下半期～**2024**年上半期	元TSMCエンジニアの陳力銘が、TSMC現職エンジニアに対し営業秘密の提供を要求[3]。現職らが工程写真等（約400枚）を流出[3]。
2024年**7**月**8**日	TSMCが内部システムログの異常から技術流出の疑いを検知し、台湾検察当局へ刑事告発[3]。
2024年**7**月**25**日～**28**日	台湾高等検察署が強制捜査を実施し、陳力銘ら主要容疑者の逮捕・勾留および家宅捜索を敢行[3]。
2025年**8**月**27**日	検察当局が、陳力銘およびTSMC現職エンジニア2名を国家安全法および営業秘密法違反で起訴（第1波起訴）[3]。
2025年**9**月	東京エレクトロンの河合利樹社長CEOが訪台してTSMCへ謝罪。TEL台湾の伊東晃董事長および張天豪総裁が辞任[10]。
2025年**12**月**2**日	検察が、TEL台湾（法人）を従業員に対する監督義務懈怠により国家安全法違反で起訴（法人初起訴）[3]。
2026年**1**月**5**日	クラウドストレージから国家核心關鍵技術の混入を確認し、検察がTEL台湾を追起訴。陳韋傑および証拠隠滅の疑いで盧怡尹を起訴[3]

	。
2026年4月27日	知的財産商業裁判所が一審判決を言い渡し、被告5名の実刑判決およびTEL台湾への罰金刑を確定 [1]。
2026年5月21日	TEL台湾が司法プロセスへの敬意を表明し、一審判決を受け入れ控訴を断念する決定を発表 [4]。

司法判断と各被告に対する量刑分析

台湾の知的財産商業裁判所が下した一審判決は、国家安全保障に関わる高度な営業秘密の不法取得に対して、極めて厳格な姿勢を示すものとなった [1]。

主犯格の陳力銘に対しては、検察側が求刑していた懲役14年（追加求刑分を含む）に準じ、有期徒刑10年という営業秘密不正取得事案としては極めて異例の長期実刑判決が下された [2]。情報を複写して陳に横流ししたTSMCのエンジニアである呉秉駿と戈一平に対しても、それぞれ有期徒刑3年、有期徒刑2年という猶予なしの実刑判決が言い渡された [3]。さらに、2026年1月に追加起訴された陳韋傑に対しては、有期徒刑6年が科された [3]。

本事件における司法の厳格さは、事後的な隠蔽工作に対する処分にも表れている [9]。TEL台湾の元主管である盧怡尹は、事件発覚後に関連ファイルやアップロードされたTSMCの機密データを削除し、捜査当局のデジタルフォレンジック解析を妨害した証拠隠滅の罪に問われた [3]。裁判所は盧に対し、有期徒刑10ヶ月、執行猶予3年を宣告すると同時に、公庫へ100万台湾ドル（TWD）の支払いを命じた [3]。

一方、法人としての刑事責任を問われたTEL台湾に対しては、罰金1億5000万TWD（約7億6000万円）の支払いが命じられた [1]。この判決には3年の執行猶予が付されているが、その条件として、損害を与えた相手方であるTSMCに対して1億TWD、台湾の国庫（公庫）に対して5000万TWDを支払う義務が課された [3]。TSMC側が最終的に和解に応じ、寛大な処分を司法に委ねる姿勢を示したことが、法人に対する執行猶予付きの判決へと繋がったが、企業ブランドが受けた社会的毀損および高額な和解金・制裁金の負担は、グローバルサプライチェーンに属する企業にとって破壊的なインパクトとなった [3]。

被告名（役職・背景）	起訴事実と訴訟における役割	検察官の求刑	第一審判決（**2026年4月27日**）
陳 力銘 （元TSMCエンジニア、TEL台湾社員）	主犯。TELのエッチング装置改善のため、元同僚へ2nm等に関する国家核心技術の提供を執拗に要求・不正	懲役14年（追加起訴分でさらに懲役7年） [3]	有期徒刑**10年**（実刑・上訴可） [3]

	取得[3]。		
陳 韋傑 （元TSMCエンジニア）	国家核心技術を複写・重製し、陳力銘へ提供した不正取得の実行者[3]。	懲役8年8ヶ月[3]	有期徒刑**6**年（実刑）[3]
吳 秉駿 （元TSMCエンジニア）	在職中、陳力銘の要求に応じてTSMCの営業秘密を撮影・提供[3]。	懲役9年[3]	有期徒刑**3**年（実刑）[3]
戈 一平 （元TSMCエンジニア）	在職中、陳力銘の要求に応じてTSMCの営業秘密を撮影・提供[3]。	懲役7年[3]	有期徒刑**2**年（実刑）[3]
盧 怡尹 （TEL台湾元主管）	事件発覚後、陳力銘がアップロードしたファイルを削除し証拠を隠滅[3]。	懲役1年[3]	有期徒刑**10**ヶ月（執行猶予3年、公庫へ100万TWDの支払義務）[3]
東京エレクトロン台湾 （法人）	行為者である陳力銘に対する監督・防止義務の懈怠[3]。	罰金1.2億TWD（追加起訴分でさらに2500万TWD）[3]	罰金**1**億**5000**万**TWD**（執行猶予3年、TSMCへ1億TWD、公庫へ5000万TWDの支払義務）[3]

台湾国家安全法の地政学的文脈と両罰規定の論理

国家核心關鍵技術と地政学的防衛

台湾政府が本事件に対して超スピード起訴と異例の厳罰をもって臨んだ背景には、技術覇権を巡るグローバルな地政学的対立が存在する[4]。台湾は2022年、自国の基幹産業であり経済的防衛線でもある最先端技術を外国の競合や敵対勢力への流出から保護するため、国家安全法を抜本的に改正した[8]。この改正により「国家核心關鍵技術」という新たな枠組みが制定された[8]。
この法的定義における半導体分野の保護基準は、以下の不等式に集約される。

$$\text{IC製造プロセス技術} \leq 14\,\text{nm}$$

この定義に基づき、経済部や行政院などの関係省庁によって「14 nmプロセス以下のIC製造技術、およびそれに用いる重要なガス、化学品、装置技術」が国家核心關鍵技術リストに明示的

に登録された[15]。
本事件において不当に取得された技術データは、世界的にも最も微細化が進んだ最先端の$2\text{ nm}世代に属しており、この基準値である14\text{ nm}$の閾値を遥かに下回るものであった[8]。台湾当局からすれば、本技術は台湾が世界に誇る「国宝級」の重要資産であり、安全保障戦略上の生命線である[8]。したがって、単なる「企業の個別資産としての営業秘密」としてではなく、「台湾の安全保障を直接的に脅かす戦略資産への攻撃」と認定され、国家安全法の最高罰則規定が適用されるに至ったのである[3]。

営業秘密法第13条の4（両罰規定）が求める実効的な監督義務

東京エレクトロンは本社の見解として、組織的な関与を終始否定し、従業員個人による単独犯行であると主張した[3]。しかし、台湾営業秘密法第13条の4に規定される「法人両罰規定」は、法人が「従業員の不法行為を防ぐために、客観的かつ実効的な防止措置と監督を尽くしていたこと」を自ら証明できない限り、法人の過失責任（使用者責任）を免除しない[3]。
判決の中で台湾の知的財産商業裁判所は、TEL台湾が社内に一般的なコンプライアンス規程や一般的な情報セキュリティ警告を表示していたという弁護側の主張を退けた[3]。裁判所は、それらの規程が単なる「抽象的で形骸化した宣言」に過ぎず、中途採用者が前職から特定のデータを違法に持ち込んで自社の共有環境へ格納することを能動的にフィルタリング・監査する仕組みを備えていなかったと判断した[3]。
この判断は、企業が形式的にコンプライアンスポリシーを制定するだけでは足りず、技術や開発の現場レベルにおいて「他社秘密の混入を能動的に防ぐ実行システム」を稼働させていなければ、刑事両罰責任から免責されないという厳しい教訓を突きつけている[3]。

日本法における他社技術「混入」リスクの激化：改正不正競争防止法の影響

台湾における法制強化の流れは、日本国内における法的リスクの高まりとも完全に連動している[7]。日本においても、2024年4月に施行された改正不正競争防止法（知財一括法）により、他社の営業秘密が社内に混入した場合の訴訟リスクが飛躍的に増大している[18]。
最も警戒すべきは、営業秘密の「使用等の推定規定」（同法第5条の2）の対象範囲が大幅に拡張された点である[20]。この法改正により、転職者が前職から営業秘密（技術上の秘密など）を持ち出して新雇用主に開示・混入させた場合、以下の条件が揃うだけで、新雇用主（企業）がその営業秘密を「実際に製品開発に使用した」と法律上推定されることとなった[21]。

$$\text{転職者のアクセス権限（前職）} + \text{被告企業の同種製品・役務提供} \implies \text{使用の推定}$$

[redacted]

[redacted]
[redacted]

[redacted]
[redacted]
[redacted]
[redacted]

この法改正により、転職者が「前職で自分が手がけたプログラムやパラメータだから参考にする程度なら問題ない」と誤認して共有ドライブにファイルをコピーしただけで、受入企業は製品開発プロセスの全体において「他社技術を不当に使用した」という強力な法律上の推定を受けることとなる[21]。
一度この使用推定が働くと、企業側は「自社の技術は転職者の持ち込み情報とは無関係に、完全に独自に開発されたものであること」を、客観的な証拠をもって自ら反証しなければならない[21]。十分な開発ログやタイムスタンプ等の証拠を日頃からアーカイブしていなければ、反証は事実上不可能であり、巨額の損害賠償請求（改正法により、原告企業の生産能力を超える部分もライセンス相当額として算定可能となった）や、製品の販売差し止め、製造設備の廃棄、さらには社会的信頼の喪失といった壊滅的な事態を招くことになる[21]。

日本企業が実践すべき多層的「混入防止（コンタミネーション・コントロール）」戦略

TSMC最先端技術流出事件、および日本国内の法改正に対応するため、日本企業は自社の営業秘密の流出を防ぐ「漏洩防止（アウトバウンド）」対策と同水準、あるいはそれ以上の厳格さをもって、他社の営業秘密を自社に入り込ませない「混入防止（インバウンド）」対策を全社的に構築しなければならない[7]。この多層的防御プログラムは、以下の4つのフェーズにわたって実践されるべきである。

人事・採用フェーズ：ゲートキーピングの高度化

中途採用時において、前職の営業秘密を持ち込ませないための事前契約管理および心理的抑止力の付与を徹底する[25]。
面接および採用内定時のチェックシートを導入し、候補者が前職で負っている秘密保持誓約や競業避止義務の存続期間、適用対象範囲を詳細にヒアリングして記録に残す[21]。このヒアリングの過程で、前職における具体的な技術資料やプログラムコードの開示を新雇用主側が一切求めていないことを明文化し、面接官および候補者の双方が署名して保管する[23]。
さらに、入社時に取り交わす秘密保持誓約書（NDA）を高度化する[25]。単に「前職の秘密を守る」という抽象的な文言にとどめず、前職での開発パラメータ、シミュレーション用データベース、社内顧客リスト、実験ノート等の具体的な複製媒体について「これらを一切保有しておらず、私用PCや外部ストレージからも完全に消去した」ことを誓約（表明保証）させる[25]。これにより、万が一混入が発生した際にも、企業側が「労働者に対して可能な限りのスクリーニングと監督、注意喚起を行っていた」という無過失（監督義務の履行）を裁判所へ証明するための強力な防護証拠となる[3]。

IT・技術的隔離フェーズ：情報インフラのゾーニング

システムおよび物理的な観点から、他社のデータが自社の社内環境に侵入・定着する経路を遮断する[3]。
企業用共有クラウドストレージ（OneDrive、Google Drive、Box等）のアクセス権限（パーミッション）を厳格に階層化し、部外者がアクセスできる範囲を必要最小限に抑える（最小特権原則）[28]。同時に、外部からのデータ持ち込みやアップロードをシステムログ上で常時追跡し、不審なファイル名の検出や一括インポート履歴を監視する自動スクリーニングを導入する。特に、私用のUSBメモリや外部ストレージの接続をシステム側で物理的・技術的に完全封鎖し、私用メールへのデータ送信やパーソナルクラウドへのサインインをプロキシ設定によって遮断する[21]。
また、半導体工場や研究開発エリアへのアクセス制御として、顔認証等の生体認証を用いた高度な物理的ゾーニング（露光室、R&D実験室、サーバー室等）を実施し、物理的ななりすまし入室や不審な行動、権限外領域での記録行為を根絶する[28]。

開発・R&Dフェーズ：クリーンルーム開発と独自開発立証

他社の営業秘密が存在する、あるいは持ち込みが疑われる状況であっても、自社の知的財産権と独自開発プロセスを守るための技術的アプローチを採用する[23]。
自社の新製品開発を、他社の秘密情報や外部からの中途エンジニアの影響から物理的・組織的に完全に遮断した部屋で行う「クリーンルーム開発（物理的・論理的クリーンルーム）」を導入する[29]。この手法では、開発に関わる人員を「仕様設計チーム（転職者が含まれていてもよい、他社情報を仕様レベルまでフィルタリングする役割）」と「実装開発チーム（他社情報を一切持たない、生え抜きの開発者等で構成される完全無菌層）」に厳格に分離する[29]。両チーム間の情報移転は、法務や知財監査部門による徹底的なフィルタリングを経て行われるため、開発されたプログラムや装置パラメータに他社の技術が混入（コンタミネーション）する可能性を構造的にゼロに近づけることができる[23]。
加えて、開発プロセスにおける全ての設計会議、ソースコードのコミット履歴、試作テスト結果等の開発記録（開発ログ）に対して、信頼できる第三者機関が保証する電子タイムスタンプを即座に付与し、改ざん不可能な状態で一元管理する[23]。他社から営業秘密の不当使用を訴えられた際、このタイムスタンプ付き開発ドキュメントが「相手方の技術に接触する以前から、自社がこの技術を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となる[23]。

組織監査・ガバナンスフェーズ：事後対策とヘルプライン

万が一の不正取得や混入インシデントに備え、被害を最小限に食い止め、自社が証拠隠滅等の組織犯罪の加担者とならないための統治機構を構築する[3]。
中途採用者やその上司、あるいは共同開発の現場において、他社の秘密保持契約に著しく反する情報の共有指示や「手土産」の強要などの不審な動きが見られた場合、法務やコンプライアンス部門へ直接（また匿名で）告発・相談できる内部通報・ヘルプライン制度を整備し、その実効性を全社に周知する[30]。
さらに、万が一他社データの混入インシデントが発覚、またはその疑いが生じた場合、当事者や現場責任者が「ファイルをゴミ箱に入れて消去すれば会社は守られる」という誤った自己防衛（証拠隠滅行為）に走ることを、徹底的な教育によって未然に防ぐ[3]。今回、TEL台湾の主管がファイルを削除したことで証拠隠滅罪が適用され、起訴範囲が拡大したように、事後の隠蔽は個人の刑事罰を著し

く重くし、法人への連帯処罰の重要な根拠とされる[3]。インシデント発生時には、直ちにシステムアクセスログおよびデータをコールドコピー（フォレンジック保全）して保全した上で、速やかに第三者の法律事務所を介入させ、被害企業（TSMC等）および司法当局と積極的に協調し、誠実に事後調査と補償、和解へと進むための「有事対応ガイドライン」を役員会主導で策定しておく必要がある[3]。

技術混入防止に向けた多層的防衛管理プログラムの全体像

以下のマトリクス表は、他社技術の混入から自社を防御するために必要不可欠なコンプライアンス管理措置、得られる法的・実務的効用、および主な関連法規の対応関係をまとめたものである[17]。

防御の柱	実施すべき具体的アクション（管理措置）	得られる実効的効用・法的な防御力	関連する法制度・指針
人事・採用の高度化	・前職の守秘・競業避止契約の事前適合性審査[25] ・「前職データの無混入・消去」に関する具体的誓約（表明保証）の締結[25] ・中途採用プロセスの面接ログ（秘密開示不要求）の確実なアーカイブ[23]	・台湾営業秘密法第13-4条等における「必要な監督義務を尽くした」とする法人免責の証明資料化[3] ・労働者に対する強い心理的・法的抑止効果の付与[25]	台湾営業秘密法第13-4条[17] 経産省「秘密情報の保護ハンドブック」[31]
IT・物理ガバナンス	・共有クラウドでの厳格なアクセス権限（最小特権）設計[28] ・私用USB/外部ストレージ/個人用メールのシステム的遮断[21] ・生体認証を伴う開発区域の細分化・ゾーニング[28]	・他社からの不審ファイルの混入ルートの物理的・論理的シャットアウト[3] ・アクセスログの追跡可能性（トレーサビリティ）の確保[3]	不正競争防止法第2条第6項（秘密管理性要件）[23]
開発手法の独自性確保	・「仕様設計」と「実装開発」を分離するクリーンルーム手法の	・不競法改正による「使用等の推定規定」に対する科学的・	不正競争防止法第5条の2（使用等の推定規定）[20]

	適用[29] ・独自開発のすべてのプロセス（ソースコード履歴、試作等）への電子タイムスタンプの自動付与[23]	改ざん不可能な反証資料の確保[20] ・他社秘密に接触しない「無菌開発」の担保[29]	
ガバナンスと有事対応	・他社秘密混入に関する匿名相談・内部通報ホットラインの構築[30] ・インシデント発覚時の無断ファイル削除（証拠隠滅）の厳禁教育[3] ・外部フォレンジック専門家による迅速な一次保全と自主開示体制[3]	・事後の隠蔽による企業犯罪への延焼（証拠隠滅罪適用・起訴拡大）の防止[3] ・司法機関や被害企業との早期和解を通じた刑事量刑の極小化[3]	各国刑法（証拠隠滅罪等）[9] 台湾国家安全法（法人両罰規定）[3]

結論

東京エレクトロン台湾子会社によるTSMC最先端技術の不当取得事件は、かつて企業の自主的なガバナンスや一部の従業員の倫理問題として片付けられていた「知的財産の取り扱い」が、現代の地政学的対立下においては、国家安全保障を直接的に左右する死活的な論点へ昇華したことを示している[4]。

高度な独自技術を保有する日本企業は、競合他社からの自社技術流出（アウトバウンド）を恐れると同時に、自社内への他社営業秘密の混入（インバウンド・コンタミネーション）が引き起こす破壊的なリスクに眼を向けなければならない[7]。転職者が、あるいは共同開発の現場が、他社技術への安易な「ショートカット」を選択した瞬間、企業は莫大な損害賠償、経営幹部の失脚、さらには最先端サプライチェーンからの永久的な排除という深刻な危機に直面することになる[4]。

本提言に示した「人事スクリーニング、ITゾーニング、クリーンルーム開発、有事における適正なデジタルガバナンス」の構築は、不必要なコストや規制ではなく、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」に他ならない[7]。経営者は、コンプライアンスを単なる「事後の予防」から「生存のための戦略防衛投資」として位置づけ、多層的防御プログラムを即座に導入・機能させることが強く求められている[3]。

引用文献

1. TSMC元エンジニア4名に最長10年の実刑-2nm 先端技術の営業秘密 ..., 5月 24, 2026にアクセス、https://rocket-boys.co.jp/security-measures-lab/tsmc-2nm-trade-secret-leak-engineers-sentenced/
2. Taiwan court hands down jail terms in TSMC trade secrets case - Al Jazeera, 5月 24, 2026にアクセス、https://www.aljazeera.com/economy/2026/4/27/taiwan-court-hands-down-jail-terms-in-tsmc-trade-secrets-case
3. TSMC機密不正取得 元社員に最大懲役10年 東京エレク台湾子会社に ..., 5月 24, 2026にアクセス、https://japan.focustaiwan.tw/society/202604270005
4. Tokyo Electron Taiwan won't appeal TSMC trade secrets ruling, 5月 24, 2026にアクセス、https://www.techinasia.com/news/tokyo-electron-taiwan-appeal-tsmc-trade-secrets-ruling
5. TSMC営業秘密流出疑惑と東京エレクトロン：各国メディア報道を読み解く｜TechBits - note, 5月 24, 2026にアクセス、https://note.com/techbits/n/n07687bd074aa
6. Taiwan court sentences ex-Tokyo Electron staff to 10 years in TSMC trade secrets case, 5月 24, 2026にアクセス、https://www.wsls.com/tech/2026/04/27/taiwan-court-sentences-ex-tokyo-electron-staff-to-10-years-in-tsmc-trade-secrets-case/
7. 転職者が持ち込んだ他社営業秘密を 使用することによる侵害リスク, 5月 24, 2026にアクセス、https://jpaa-patent.info/patent/viewPdf/4722
8. 台湾TSMCの「国宝級」2ナノ技術流出で3人をスピード起訴――東京 ..., 5月 24, 2026にアクセス、https://toyokeizai.net/articles/-/901511?display=b
9. TSMC 2nmプロセス 機密情報漏洩事件で東京エレクトロン 元主管が出廷 証拠隠滅の疑いで懲役1年求刑 - 合同会社ロケットボーイズ, 5月 24, 2026にアクセス、https://rocket-boys.co.jp/security-measures-lab/tsmc-2nm-leak-case-tokyo-electron-ex-manager-faces-1-year-sentence/
10. 東京エレク子会社を起訴、TSMC機密事件で罰金1.2億元求刑【図表】(トップニュース), 5月 24, 2026にアクセス、https://www.ys-consulting.com.tw/news/125676.html
11. Tokyo Electron's Taiwan unit says it will not appeal ruling in TSMC trade secrets case, 5月 24, 2026にアクセス、https://www.thestar.com.my/tech/tech-news/2026/05/21/tokyo-electron039s-taiwan-unit-says-it-will-not-appeal-ruling-in-tsmc-trade-secrets-case
12. TSMCから半導体技術を不正取得、元従業員に懲役10年...転職先の東京エレクトロン子会社に罰金7・6億円 - 読売新聞, 5月 24, 2026にアクセス、https://www.yomiuri.co.jp/world/20260428-GYT1T00026/
13. 東京エレ子会社に罰金7億円, 5月 24, 2026にアクセス、https://www.oanda.jp/lab-education/market_news/kn_20260427010000983/
14. Tokyo Electron's Decision on Trade Secrets Case and Its Impact on Semiconductor Industry, 5月 24, 2026にアクセス、https://www.valuethemarkets.com/cryptocurrency/news/tokyo-electrons-decision-on-trade-secrets-case-and-its-impact-on-semiconductor-industry
15. 台湾：国家安全法の改正 - 国立国会図書館デジタルコレクション, 5月 24, 2026にアクセス、https://dl.ndl.go.jp/view/prepareDownload?itemId=info:ndljp/pid/12888736

16. 行政院、改定「国家核心重要技術リスト」を公表 - 理律法律事務所, 5月 24, 2026にアクセス、https://www.leeandli.com/JP/Newsletters/7454.htm
17. 従業員が業務執行中に他人の営業秘密を使用して社内プレゼンを行うことについて、会社が違法行為防止のために必要な措置を講じなかったのは、「防止・回避に尽力していない」ものである。- 台灣國際專利法律事務所, 5月 24, 2026にアクセス、https://tiplo.com.tw/jp/news/1328/2588
18. 法改正で営業秘密侵害の訴訟リスク増す懸念 特に転職者の情報持ち込みへの対策に注意, 5月 24, 2026にアクセス、https://mscompass.ms-ins.com/business-news/trade-secret-violation/
19. 日本 2024年 4月に改正された不正競争防止法とは, 5月 24, 2026にアクセス、https://www.asamura.jp/blog/2024/04/04/unfair-competition-prevention-law-revised-in-april-2024/
20. 【2024 年 4 月施行】改正不正競争防止 法による営業秘密保護の強化, 5月 24, 2026にアクセス、https://jmatsuda-law.com/wp-content/uploads/2024/02/note_2024_6.pdf
21. 法改正で営業秘密侵害の訴訟リスク増す懸念 特に転職者の情報持ち込みへの対策に注意, 5月 24, 2026にアクセス、https://rm-navi.com/search/item/1862
22. 不正競争防止法の営業秘密とは？営業秘密の要件や侵害行為の内容を具体例で分かりやすく解説！ - 契約ウォッチ, 5月 24, 2026にアクセス、https://keiyaku-watch.jp/media/hourei/huseikyousouboushi-eigyou/
23. 秘密情報の保護ハンドブック ～企業価値向上に向けて～ - 経済産業省, 5月 24, 2026にアクセス、https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/1706blueppt.pdf
24. 営業秘密のツボ 2024年05月15日 第95号 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構, 5月 24, 2026にアクセス、https://www.ipa.go.jp/security/economics/mailmag/20240515.html
25. 中途採用者/退職予定者が保有する情報の取扱いで注意したい事項 ..., 5月 24, 2026にアクセス、https://media.ys-law.jp/risk/post-765/
26. 【営業秘密管理・侵害における企業法務実務ガイド】2025年改訂指針と最新判例対応, 5月 24, 2026にアクセス、https://nao-lawoffice.jp/venture-startup/intellectual-property-right/eigyo-himitsu-kanri-shingai-jitsumu.php
27. 知っておきたい営業秘密 - 経済産業省, 5月 24, 2026にアクセス、https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/shitteokitai_eigyohimitsu.pdf
28. 半導体工場のクリーンルーム管理と情報漏洩防止を実現する入退室管理システムを解説！ - オープンセサミ北海道, 5月 24, 2026にアクセス、https://open888sesame.com/%E5%8D%8A%E5%B0%8E%E4%BD%93%E5%B7%A5%E5%A0%B4/semiconductor-factory_access-control.html
29. 米国企業等との取引における情報コンタミネーションリスクへの対策 - 弁護士知財ネット, 5月 24, 2026にアクセス、https://iplaw-net.com/doc/2022/tradesecret-mailmagazine-column_65.pdf
30. 【営業秘密】転職者を通じたライバル会社のデータ流入の違法性（不正競争防止法・判例解説）, 5月 24, 2026にアクセス、https://ksltp.com/expert-blog/cat-legal_tax_advisor/4500/

31. 平成28年2月（最終改訂：令和6年2月）経済産業省, 5月 24, 2026にアクセス、https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf
32. 営業秘密～営業秘密を守り活用する - 経済産業省, 5月 24, 2026にアクセス、https://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html