APPTraS 第21回オープンセミナー

重要技術情報漏えいの脅威類型と持つべきリスク認識

2025. 11. 14

橘　了道
PwCコンサルティング合同会社

Agenda

1. 重要技術保護と経済安保の関係性
2. 企業における営業秘密管理の実態
3. 脅威類型の概観
4. 各脅威類型について
5. さいごに

自己紹介

橘　了道
Ryo Tachibana
Manager
Consulting, Japan

所属
PwCコンサルティング合同会社
トラストコンサルティング　サイバー＆リスクコンサルティング

経歴／専門領域

大手外資系メーカー出身。品質保証部にてグローバル品質保証体制の見直しや品質KPIの可視化を推進。戦略調達部門では、品質監査やデューデリジェンスを通じてサプライチェーン改革をリード。知的資産保護部門では、日本地区の統括として各拠点の情報セキュリティ体制を強化し、クロスファンクショナルな協力体制を構築。グローバルワイドで重要サプライヤーに対する情報セキュリティトレーニング・監査を実施し、グローバル全体のセキュリティレベルの向上を実現。

コンサルティング分野においては、バリューチェーン全体にわたる経験を活かし、IPプロテクション・営業秘密保護の専門家として活躍。宇宙産業・基幹インフラ産業・自動車産業への支援を中心に展開。ERM分野においては、広告業や飲食業への支援も実施。

資格

・CISSP
・ISO27001審査員補　etc.

執筆

PwCインサイト「営業秘密」の保護と利活用シリーズ
https://www.pwc.com/jp/ja/knowledge/column/awareness-cyber-security/protection-and-utilization-of-trade-secrets.html

1

重要技術保護と経済安保の関係性

【警察庁】(リスク＆ケーススタディ編)技術流出の防止に向けて

■ ここで警察庁の啓蒙動画をご覧ください。
（時間の関係上、2倍速にて再生いたします）

国を挙げた「重要技術情報保護」体制の全貌

■ 日本政府は、技術情報の流出防止を国家・経済の最重要課題と位置づけています。経産省、内閣府、警察庁、公安調査庁がそれぞれ施策を展開し、官民一体の「多層防衛体制」が本格的に動き始めています。

行政機関	部局・組織	主な施策・制度	目的・観点	最新公表・改定時期
内閣官房／防衛省	内閣サイバーセキュリティセンター（NISC）／防衛省	**能動的サイバー防御（Active Cyber Defense）**	政府が攻撃経路を特定・遮断し、国家レベルのサイバー防衛を実施	**2025年5月23日 公布**
経済産業省	産業技術環境局 産業技術政策課	**技術流出対策ガイダンス（第1版）**	海外拠点・委託・人材流出を防ぐ実践的対応指針	**2025年5月23日 公表**
	貿易経済安全保障局技術調査・流出対策室	**技術情報管理認証制度（TICS）**	技術情報の「特定・体制・制御・教育・監査」を評価・認証	**2025年5月20日 自己診断シート改訂**
	経済産業政策局 経済安全保障室	**民間ベストプラクティス集（第2.0版）**	実在企業の好事例を共有し、実務文化を普及	**2025年5月23日時点版**
	商務情報政策局 サイバーセキュリティ課	**サプライチェーンセキュリティ対策評価制度（中間報告）**	サプライヤーのセキュリティ成熟度を可視化・格付け	**2025年4月14日 公表（導入目標：2026年度）**
内閣府	科学技術・イノベーション推進事務局（CSTI）	**研究セキュリティ手順書（原案）**	研究・学術機関における国外流出防止の標準手順を策定	**2025年10月23日 原案（第6回有識者会議）**
	国家安全保障局 経済安全保障推進室	**セキュリティクリアランス制度（重要経済安保情報保護活用法）**	機微情報を扱う人材の適格性審査制度	**2024年5月17日 公布**
警察庁	生活安全局 情報技術犯罪対策課	**技術流出防止特設サイト（3S原則）**	自社・研究機関向けの啓発と防止策	**2025年1月 開設**
公安調査庁	経済安全保障情報対策室	**経済安全保障特集ページ／啓発パンフレット『技術・データ・製品の流出防止』**	技術流出リスクの分析、啓発資料の提供、相談・通報窓口の運用	**2025年3月 啓蒙パンフレット発行**

重要技術情報をめぐる構造変化

■ 技術情報を取り巻く環境は、企業の枠を越えて大きく変化しています。経済安全保障の潮流の中で、情報を「守る」ことは国家戦略の一部になりました。企業・産業・研究・治安などの**官民連携による統合管理**という時代に入っています。

これまで

技術情報の位置づけ
- 知財・企業競争力の一部（社内資産）
- 漏えい＝企業の不祥事・信用問題

想定されていたリスク
- 内部不正・退職者の持ち出し
- 委託先・取引先の管理ミス
- 一過性の事故

背景・社会環境
- グローバル化・アウトソーシング進展
- サイバー攻撃は限定的

対応のあり方
- 企業ごとの自主対策（任意）
- 守秘義務や不正競争防止法で個別対応
- 教育・内部統制中心

今求められること

技術情報の位置づけ
- 国家競争力・安全保障の根幹
- 漏えい＝国家リスク・外交問題・経済損失

現在のリスク構造
- 国家関与のサイバー攻撃
- サプライチェーンを経由した攻撃
- 計画的・継続的な情報収集活動

背景・社会環境
- 経済安全保障/技術覇権競争
- AI/半導体/量子など戦略技術
- 外国勢力によるリクルートや投資

対応のあり方
- 国家・産業・研究・治安が連携
- 事前予防とリスク共有を重視する構造
- 経営レベルで統合管理

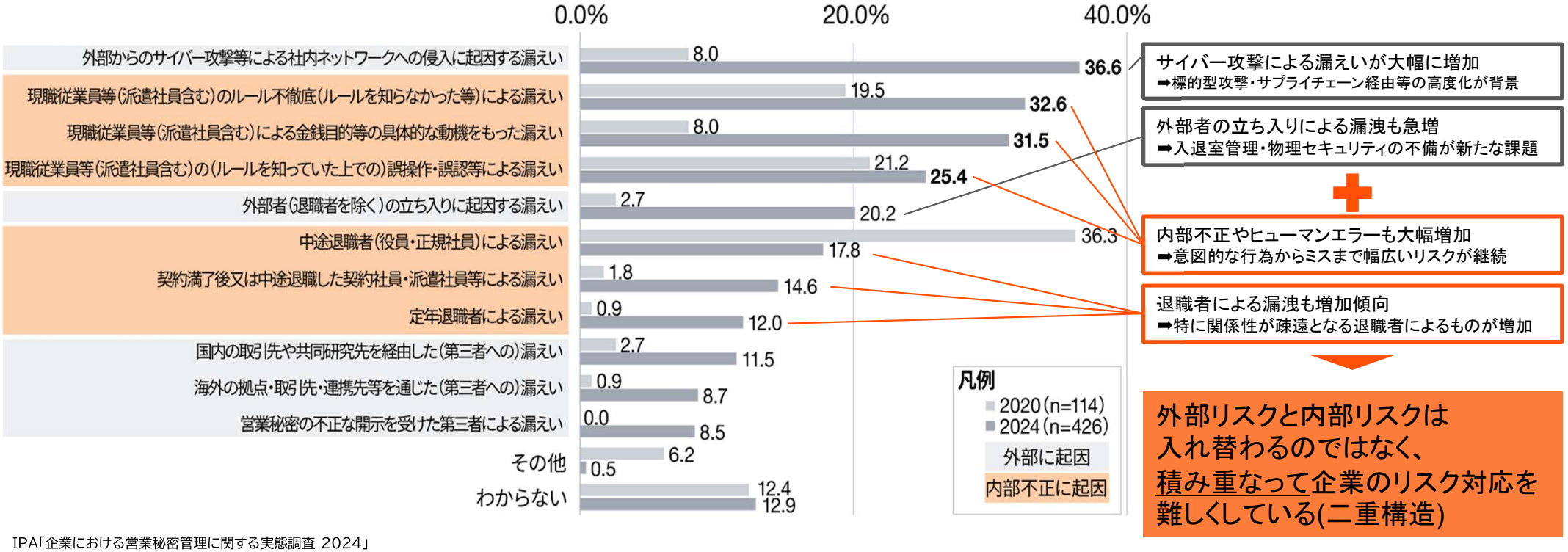
アメリカ・EU・中国等も同様に経済安全保障を
軸とした技術流出防止の施策を発表している

2 企業における営業秘密管理の実態

技術情報流出の実態 – 外部と内部の二重構造

■ IPAが今年公表した実態調査では、技術情報流出の経路が**外部起因型と内部起因型の二重構造**を呈していることが確認されました。サイバー攻撃を起点とした外部侵入が増加する一方、内部不正や委託先・共同研究先からの漏えいも依然として深刻です。

【営業秘密の漏えいルートの推移】



IPA「企業における営業秘密管理に関する実態調査 2024」
https://www.ipa.go.jp/security/reports/economics/ts-kanri/j5u9nn0000004yjn-att/TradeSecret_report_2024_r1.pdfより引用

技術情報流出の実態 – 経営層の認識不足

■ IPAの同調査では、**経営層と現場の脅威認識に大きなギャップ**があることが明らかになりました。
多くの企業の実務レベルでは課題を感じている一方、経営層の45.1%は、内部不正の要因について「当てはまる物はない」と回答しています。この乖離は、**経営層が潜在的な内部不正リスクを十分に認識していない傾向を示している**と言えます。

【「内部不正を誘発する環境や状況」の回答結果】

部門別(%)		同じ業務を同じ人が長期継続	少ない人数で業務を回している	人間関係等への恨みが大きい	借金のある人が営業秘密を扱う	弱みを握られて脅迫されている	当てはまる物はない	回答したくない
全体 n=1200		36.8	39.5	21.2	10.3	6.8	26.1	6.2
部門別	企業における情報システム関連部門	46.2	38.9	21.0	11.9	7.6	22.2	7.9
部門別	**企業のリスクマネジメント計画・実践に関わる部門**	32.3	43.0	**37.3**	**18.4**	**10.1**	12.7	3.2
部門別	**企業のサイバーセキュリティに関わる部門**	40.5	48.1	**43.0**	**30.4**	**16.5**	7.6	2.5
部門別	経営企画部門	31.9	33.3	22.5	6.6	6.6	26.3	8.9
部門別	**経営層**	**32.0**	**38.7**	5.4	1.7	1.0	**45.1**	4.7
部門別	その他セキュリティやリスクマネジメントに関する業務を実施している部門	34.7	43.5	22.6	10.5	8.9	19.4	6.5

IPA「企業における営業秘密管理に関する実態調査 2024」
https://www.ipa.go.jp/security/reports/economics/ts-kanri/j5u9nn0000004yjn-att/TradeSecret_report_2024_r1.pdfより引用

技術情報流出の脅威は全ての企業に...

■ 技術情報を狙う攻撃は、大企業や最先端技術だけの問題ではありません。攻撃者は“防御の甘い取引先や中小企業”を標的とし、民生用途の技術や部品を通じて軍事転用・産業スパイ活動を進めています。「うちには関係ない」という思い込みこそ、最大のリスクとなり得ます。

技術・製品分野	一般的な用途	なぜ狙われたか／実際の転用先
磁気センサー用素材	スマートフォン・家電の角度検知	軍用航空機・ミサイルの姿勢制御に転用可能
炭素繊維（CFRP）	スポーツ用品・釣竿・ゴルフクラブ	軽量・高強度素材として戦闘機やミサイル外装に利用
真空ポンプ・制御弁	半導体製造装置、医療機器	核関連施設やミサイル燃料製造ラインに転用
高性能カメラレンズ／赤外線センサー	監視カメラ・自動車安全装置	軍用ドローンや照準装置に転用可能
高精度ベアリング（軸受）	自動車・工作機械	ミサイル発射装置や潜水艦の回転系に利用
無人搬送車（AGV）制御ソフト	工場内物流の自動化	軍需施設や弾薬工場の自動搬送に応用
ドローン用通信モジュール	農業・測量用ドローン	偵察・標的誘導ドローンに転用
3Dプリンタ用粉末金属技術	医療機器・部品成形	航空機エンジンや兵器部品の現地製造に応用
AI画像解析アルゴリズム	製造検査・広告分析	軍用監視・標的認識・自動操縦技術の基礎
工作機械制御NCプログラム	民生工作機械	ウラン濃縮やロケットエンジン製造ラインに転用
電子顕微鏡部品	医療・材料研究	原子レベル観測による半導体・核材料研究に転用
樹脂添加剤／接着剤技術	自動車・包装材料	ロケット燃料・軍需塗装材に応用
水処理膜技術	工業用水・環境設備	化学兵器原料精製・軍需施設排水処理に転用
数値制御用ソフトウェア（CAD/CAM）	製造業一般	兵器部品の製造に直接利用可能
リチウムイオン電池制御基板	電動工具・自転車	無人兵器・潜水機器の動力制御

3

脅威類型の概観

脅威の性質と特徴

- 技術情報を脅かす脅威は、**攻撃の起点（内部か外部か）**と**手段（サイバーか物理か）**によって、その性質と影響が大きく異なります。外部からの攻撃は防御の突破を狙い、内部からの不正は信頼の仕組みを悪用する。サイバー攻撃は電子的手段により大量の情報を奪取し、物理的行為は人や現場を介して静かに情報を持ち出す。
- これら4つの特性を理解することは、技術情報保護体制を構築するうえでの前提となります。

外部

起点：組織外部の攻撃者

国家・犯罪組織・産業スパイなどが秘密裏に侵入。

防御の突破を狙う。大量の情報を奪い、他国・他社で再利用。
なりすまし等で発覚が難しい場合が多い。

内部

起点：信頼の内側

社員・退職者・委託先が動機を持って正規権限悪用。

どこに何があるかを知り、必要な情報だけを抜く。
静かに進行し、発覚は漏えい後であることが一般的。

サイバー

手段：電子的侵入と奪取

クラウド・VPN・メールなどネットワーク経由で攻撃。

自動化・同時多発が容易で、一度に大量の情報を取得可能。
技術的対策が要。

物理

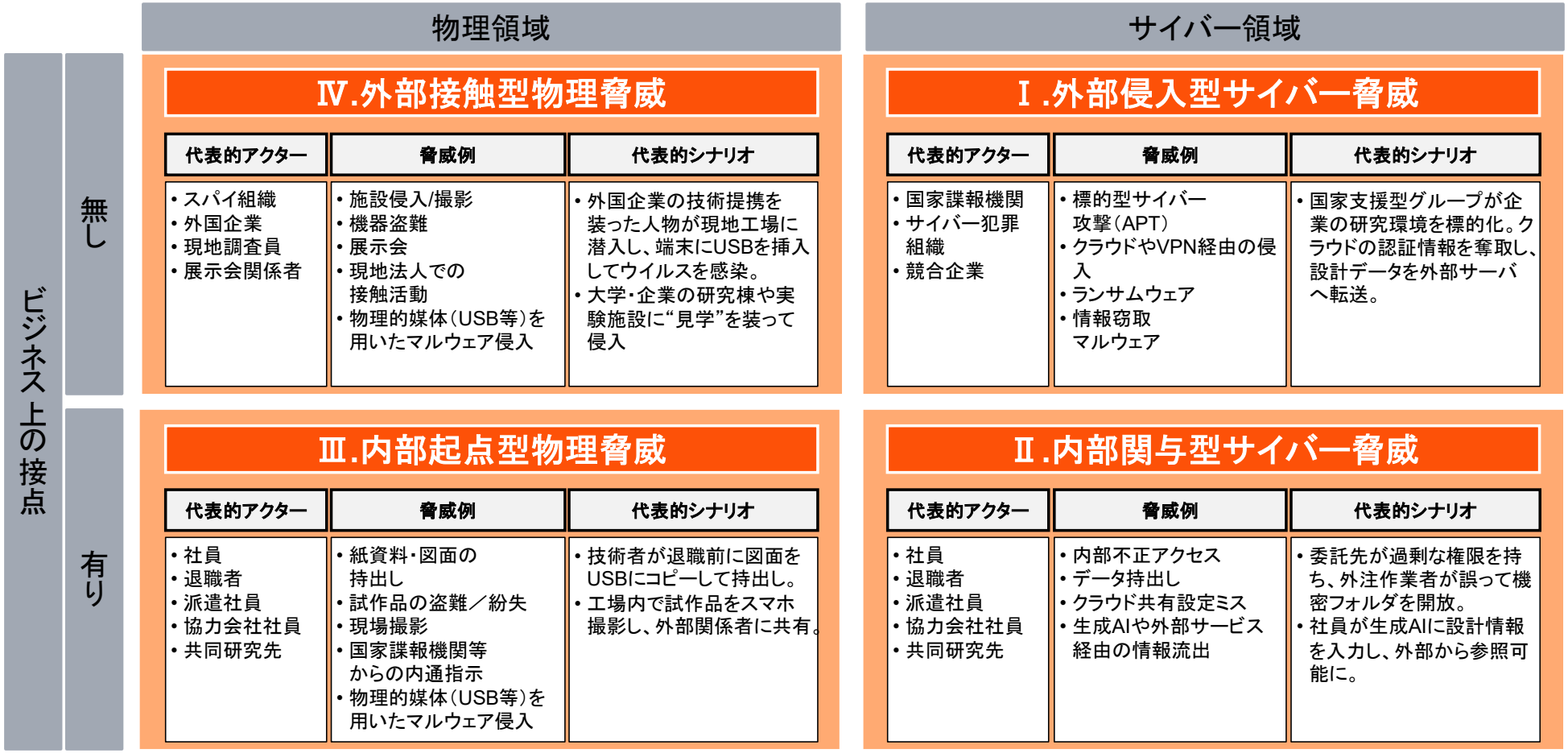
手段：現場への人の侵入

観察・撮影・試作品持出しなど“目に見えない奪取”。

USB等を使ったマルウェア感染の起点にもなる。
防御は入退室管理・教育・文化が鍵。

脅威の4類型 – サイバー領域と物理領域の双方から迫るリスク

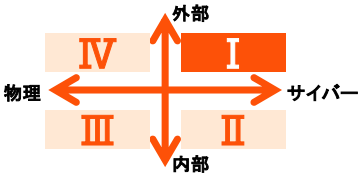
■ サイバー領域と物理領域という2つの視点から脅威を体系化し、「脅威の4類型」としてその全体像を整理します。



4

各脅威類型について

Ⅰ:外部侵入型サイバー脅威｜攻撃ライフサイクル

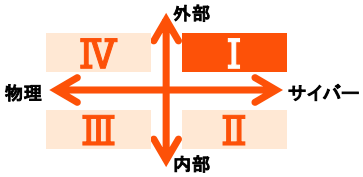


■ 攻撃は単発のイベントではなく、初期侵入、踏み台化、定着、潜伏、漏えい、破壊と続くプロセスです。

フェーズ	攻撃の目的	主な攻撃名称（代表例）
1. 入口	初期侵入の確立	• 標的型メール攻撃／フィッシング • VPN脆弱性攻撃 • ゼロデイ攻撃
2. 踏み台化	関連組織経由の侵入拡大	• 業務上のサプライチェーン攻撃 • ソフトウェア上のサプライチェーン攻撃
3. 内部定着	権限奪取・内部展開	• 認証情報窃取 • 権限昇格・横展開
4. 長期潜伏	情報収集・窃取	• 通信の秘匿化 • 通信痕跡の隠蔽 • データ断続送信
5. 最終段階	金銭化・恐喝・破壊・漏えい	• ランサムウェア攻撃 • ワイパー攻撃

特に自社では対応が難しいサプライチェーン攻撃について説明します。

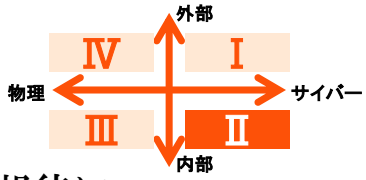
Ⅰ:外部侵入型サイバー脅威｜サプライチェーン攻撃



■ サプライチェーン網は企業活動を支える一方で、攻撃者にとっては“**侵入の連鎖経路**”でもあります。
攻撃者は、直接攻撃が難しい大企業を狙う際、**より脆弱な取引先・委託先を踏み台に侵入**し、そこから機密情報を奪います。

区分	概要	攻撃経路・特徴	想定される攻撃者	主な被害・影響
業務上のサプライチェーン攻撃	企業間取引や業務委託など、**ビジネス上の繋がり**を悪用 標的会社ではなく取引先・委託先・子会社など、より防御の甘い関係先を踏み台にする。	弱い取引先・委託先への侵入 ➡正規VPN／共有システム経由 ➡標的企業ネットワーク ➡情報窃取・侵入拡大	•組織的犯罪グループ •国家支援型攻撃者 •高度サイバー犯罪組織	•機密情報の漏えい •ランサムウェア感染連鎖 •取引停止 •信用失墜 •損害賠償
ソフトウェアのサプライチェーン攻撃	ソフトウェアやサービスの開発・配布プロセスを悪用 開発元・MSP・OSSなど**技術的な繋がり**を汚染し、利用企業に拡散。	開発者・MSP侵入 ➡更新プログラム改ざん／コード汚染 ➡ユーザー企業環境へ感染拡大 ➡情報窃取・制御奪取	•国家支援型攻撃者 •サイバー犯罪組織 •開発元内部協力者	•マルウェア拡散／大量感染 •認証情報漏えい •ソースコード漏えい •業界・国際的サプライチェーン全体への波及

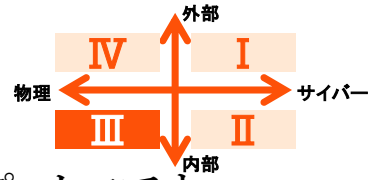
Ⅱ:内部関与型サイバー脅威｜攻撃ライフサイクル



■ 内部関与型サイバー脅威は、**内通者の動機形成が最初のプロセス**となり、外部勢力の指示或いは期待に呼応する形で、**内通者が情報を流出させていく**流れです。

フェーズ	攻撃の目的・状態	主な行為・特徴	想定される関与者	主な被害・影響
0. 動機形成（内通・意識の変化）	不正行為への心理的・社会的動機が生じる	・不満／報復／金銭的欲求 ・外部勢力からの勧誘/命令	社員／契約社員／退職予定者／研究協力者	N/A
1. 内部関与の発生	**不正アクセス権・接点を得る**	攻撃の内通者化 ・権限濫用 ・委託先アカウント悪用 ・USB等媒体を介したマルウェア感染	同上	内部不正の足場の構築
2. 情報持出し	**正規権限で機密情報を探索・取得・送信**	USBコピー／クラウド不正操作/生成AI入力／共有設定変更	同上	機密・研究データ等の漏えい
3. 痕跡隠蔽	発覚を防ぐ	ログ削除／ファイル名偽装／他人アカウント使用	同上	発見遅延・検出困難化
4. 情報活用・拡散	流出情報を第三者が利用・公開	受領ファイル／SNS／生成AI等を通じた解読・展開	競合企業／外部勢力	営業秘密の喪失・国家間技術移転リスク

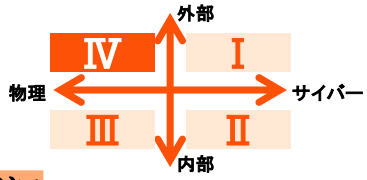
Ⅲ:内部起点型物理脅威｜攻撃ライフサイクル



■ 内部起点型・物理脅威は、**「人の行動」や「物理的接触」**によって技術情報が外部へ持ち出されるプロセスです。
サイバーよりも検知が遅れやすく、**発覚時にはすでに実質的な被害が確定していることが多い**のが特徴です。

フェーズ	攻撃の目的・状態	主な行為・特徴	想定される関与者	主な被害・影響
0. 動機形成（内通・意識の変化）	不正行為への心理的・社会的動機が生じる	・不満/報復/金銭的欲求 ・外部勢力からの勧誘/命令	社員／契約社員／退職予定者／研究協力者	N/A
1. 内部アクセス権・立入権の悪用	**物理的に機密区域・資産へ接近**	・IDカード・鍵・清掃等委託作業を利用 ・夜間・休日・無人時間の出入り	同上	機密エリアへの不正立入
2.情報取得・持出し	**有形・無形情報を直接取得**	・紙資料・部品・試作物持出し ・撮影・録音 ・USBコピー	同上	図面・試作品・ノウハウの流出
3. 痕跡隠蔽	発覚を防ぐ	・監視カメラ映像削除 ・入退室ログ改ざん ・廃棄物への混入 ・正当性を主張する口実	同上	発見遅延・検出困難化
4. 情報活用・拡散	流出情報を第三者が利用・公開	・転職・副業先で利用 ・展示会／SNS／論文で公開 ・冒認特許出願	競合企業/外部勢力	営業秘密の喪失・国家間技術移転リスク

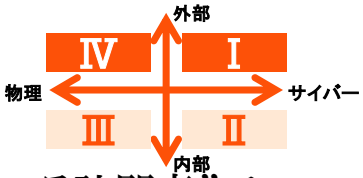
Ⅳ:外部接触型物理脅威｜攻撃ライフサイクル



■ 外部接触型物理脅威は、訪問・作業・委託・共同研究・見学など、**業務上の接点を装って内部環境にアクセスする外部者が起点**となり、観察・撮影・窃取・改ざん等を通じて情報を持ち出すプロセスです。

フェーズ	攻撃の目的・状態	主な行為・特徴	想定される関与者	主な被害・影響
1. 接触機会の獲得	組織内部への立入・接点を得る	・共同研究・商談・取材・設備保守・清掃作業などを装う ・外注契約・訪問申請を通じて物理的アクセス権を得る	外部企業担当者、外国人研究者、業務委託先、報道関係者	N/A
2. 現場観察・情報探索	**現場内で情報を視認・撮影・記録**	・設備・試験装置・掲示物撮影 ・作業員の操作を観察・記録 ・機材持込みによる隠し撮り	同上	設計段階・構想・工程・研究内容・レイアウト・ノウハウが外部に把握される
3. 資料・サンプルの入手	**有形資産を直接取得**	・配布資料・試作品・破棄予定部品の持ち帰り ・実験ノート・USB・紙図面の窃取	同上	図面・試作品・ノウハウの直接的な流出
4.関係維持／離脱	発覚を避けつつ目的を完遂	・なりすましを継続し追加情報を取得 ・プロジェクト終了／契約満了を装って離脱 ・音信不通・関係断絶	同上	追跡困難・事後確認不能
5. 情報活用・拡散	得た情報を外部で利用・分析	・他組織・母国企業・政府機関へ報告・提供 ・公開研究・展示会で応用	外国研究機関、競合企業、国家機関	営業秘密の喪失・国家間技術移転リスク

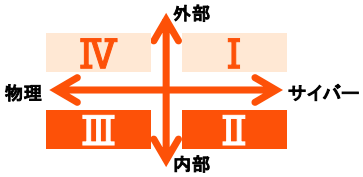
第Ⅰ類型 vs 第Ⅳ類型（外部の視点）



- 第Ⅰ類型は“インターネット越しの見えない侵入者”で、検知と可視化で守り、第Ⅳ類型は“目の前にいる訪問者”で、見せない・触れさせない管理で守ります。
- 経路は違っても、**どちらも境界線の“ゆるみ”を突いてくるという点は同じ**です。

観点	第Ⅰ類型：外部侵入型サイバー脅威	第Ⅳ類型：外部接触型物理脅威
攻撃者の姿	目では見えない相手（インターネット越しの侵入者）	目で見える相手（訪問者・業務委託・研究協力者）
侵入の方法	ネットワーク経由 （脆弱性・マルウェア・認証情報の窃取）	契約・業務・取材・見学を装った物理的接触
狙われる対象	サーバ・システム・データベース	設備・工程・研究内容・試作品・紙媒体の図面等
検知難度	デジタルログの解析で特定可能だが、巧妙化が進んでいる	行動の痕跡が残りにくく、発覚は事後の場合が多い
防御手段	セキュリティ監視・検知・ログ分析・アクセス制御	入退室管理・撮影制限・情報非開示・エスコート徹底
考え方	**見えない相手➡監視・検知（“見える化”）で防ぐ**	**見える相手➡情報を秘匿・制限（“見せない”）で防ぐ**

第Ⅱ類型 vs 第Ⅲ類型（内部の視点）



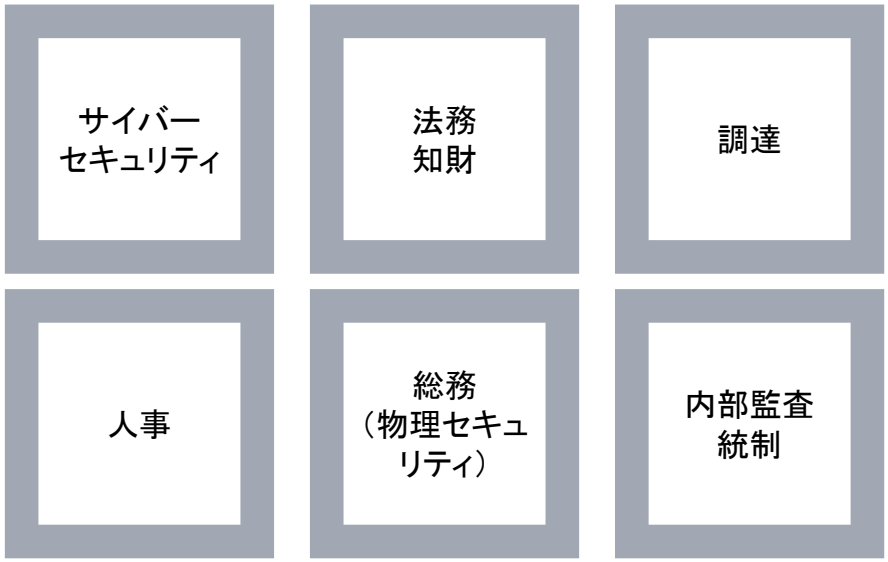
- 第Ⅱ類型と第Ⅲ類型は、どちらも“内部から始まる脅威”です。
- 第Ⅱ類型はITシステム上のログで追跡ができますが、第Ⅲ類型は人の行動を見ないと防げません。
  つまり、**情報セキュリティ部門だけでは完結しない領域である**と言えます。

観点	第Ⅱ類型：内部関与型サイバー脅威	第Ⅲ類型：内部起点型物理脅威
経路	デジタル（システム・クラウド）	物理（現場・紙・試作品・設備）
検知手段	ログ・アラート・システム監視	監視カメラ・通報・在庫管理
発生形態	サイバーインシデント・設定ミス	現場・研究所・製造ラインへの侵入
検知難度	中（デジタル記録あり）	高（行動監視に依存）
対応主体	IT・情報セキュリティ部門	**総務・人事・製造・研究管理部門**
再発防止策	権限管理・システム監査	入退室管理・持込持出制限・教育

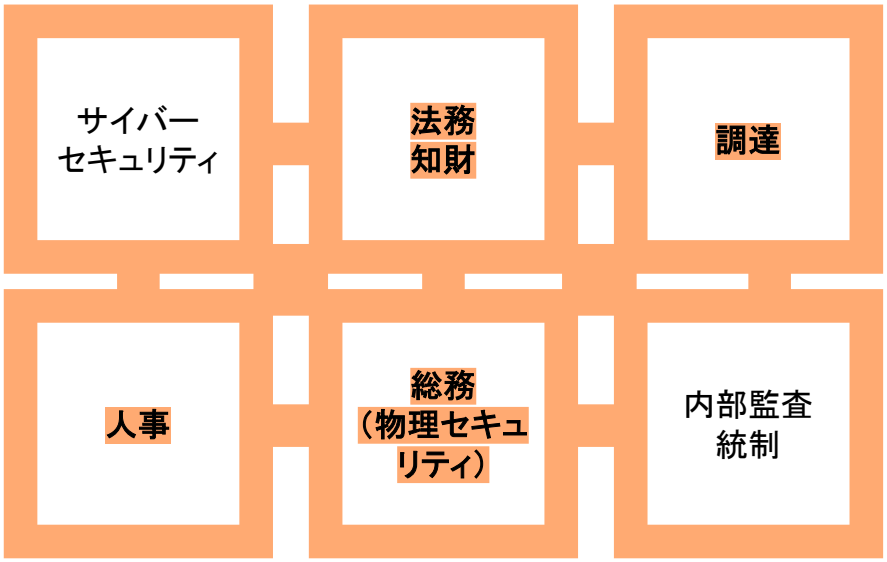
企業を取り巻く情報保護の要請と体制整備の方向性

- 情報をめぐる環境は、サイバー攻撃といった技術的リスクだけでなく、法令遵守、知的財産、取引関係、プライバシー保護など、多面的な要素が絡み合う時代にあります。情報は企業活動の基盤であり、信頼と競争力を支える資産であると同時に、内容によっては国家的な競争力や安全保障にも関わる重要なリスク要因となり得ます。
- こうした背景から、企業には**情報保護の統合的リスク管理**（技術的・法的・人/組織的・制度的観点を横断的に連携させた全社的な管理フレーム）を実現する体制の整備が求められています。

サイロ化した情報管理



情報保護の統合的リスク管理



経済安保上の情報保護の潮流では、
特に人／組織的なリスクが強調されている

5

さいごに

まとめ

■ **第1章では、国を挙げた技術情報保護の体制整備について述べました。**

- 各省庁が連携し、国家・産業・研究・治安の四層で支える多層的な防衛線が構築されつつあることから、**技術情報の保護はもはや企業単独の管理課題ではなく、国家戦略の一部である**ということが確認できました。

■ **第2章では、企業における営業秘密管理の実態について述べました。**

- 営業秘密の漏えいは**外部からのサイバー攻撃と内部要因の双方が複合的に発生する「2重構造化」**が進んでおり、企業規模を問わず被害が拡大していることが明らかになりました。
- 情報漏えいは一部の先端企業だけの問題ではなく、**すべての企業が当事者として備えるべき現実的なリスク**であることが確認されました。

■ **第3章および第4章では、技術情報漏えいの脅威構造と具体的な事例について述べました。**

- 脅威は「物理・サイバー × 内部・外部」の4象限で整理でき、あらゆる方向から侵入・流出が発生し得ることが確認されました。
- それぞれの脅威は、動機の形成から侵入・取得・拡散に至る**攻撃のライフサイクルを持ち、これを理解することがリスク対応を設計する前提**となります。
- 技術情報の保護には「どこから守るか」よりも、**「どの段階で食い止めるか」を意識した継続的な管理と対応設計が必要**であることが確認されました。

- 技術情報流出の脅威は、“日常の業務の中”から始まります。
- 本日お話しした4つの類型は、すべての企業に共通する構造です。
- “うちは関係ない”ではなく、“自社のどこにリスクが潜むのか”を考えることが重要です。
- そして――技術を守ることは、日本の未来を守ること。
- 一人ひとりの意識と行動が、これからの日本の技術基盤を支える防衛線になります。

Thank you

ご清聴ありがとうございました

© 2025 PwC Japan LLC. All rights reserved. PwC refers to the PwC network member firms and/or their specified subsidiaries in Japan, and may sometimes refer to the PwC network. Each of such firms and subsidiaries is a separate legal entity. Please see www.pwc.com/structure for further details.
This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

pwc.com