経済安保 企業の責務

強い供給網と情報保全両立

経済安全保障における企業の責務は、サプライチェーン（供給網）の強靭（きょうじん）化と情報保全に尽きる。国際情勢の不安定化や各国法規制の影響から生じる供給途絶、内部・外部からの情報漏えいのリスクに直面する今、企業は重要部材・高依存国に重点を置いたサプライチェーン管理体制と、サイバー・人的・取引面での情報保全を網羅する統合的ガバナンスを確立しなければならない。

電通総研 経済安全保障研究センター
副センター長
伊藤 隆

いとう・たかし 86年（昭61）慶大法卒、同年三菱電機に入社。半導体業界の通商摩擦対応、国際カルテル訴訟解決、業界再編などを主導。20年経済安全保障統括室長、23年過任後、同年から現職。TMI総合法律事務所顧問、政府アドバイザーなどを兼任。東京都出身、61歳。

海外法規制に翻弄

10月29日付本欄において、企業の経済安全保障リスクマネジメントは、「戦略的自律性」に対応するサプライチェーン強靭化と、「戦略的不可欠性」に対応する情報保全に集約されると述べた。本稿では、この二つの課題を具体的に整理したい。

米国商務省は9月、輸出管理規則（EAR）の適用範囲を拡大し、エンティティ・リスト（EL）に掲載された企業や個人が50％以上出資する企業・団体も同様に規制対象とした。これにより、世界中で約2000件に及ぶEL掲載主体に対する規制が、その関連企業へと波及することになる。

10月には中国がレアアース（希土類）と関連技術の輸出規制強化を発表した。両者の発表に直接の関連はないが、米中の戦略的対抗の一環とみるのが自然である。10月の米中協議により、これらの実施は1年先送りが決定されたとはいえ、日本企業が海外の法規制のもとで翻弄（ほんろう）される状況が続いている。

企業がまず着手すべきは「誰から何を買い、誰に何を売っているのか」を把握することだ。単純に見えるが、実務上は容易でない。取引先データの表記揺れや、正式名称と略称の不一致、さらに多言語対応が妨げとなる。例えば、「電通総研」「（株）電通総研」「株式会社電通総研」は、人が見れば同じ企業だが、データ上は3社にカウントされてしまう。これらを名寄せし、ELなどの制裁リストと照合するには、和名のみならず、英名・簡体字・繁体字などを連携させることも不可欠となる。さらに、制裁リストは全世界に存在するが、その代表格とも言える米国のEL・SDNリストだけでも掲載件数は述べ2万件に及ぶ。

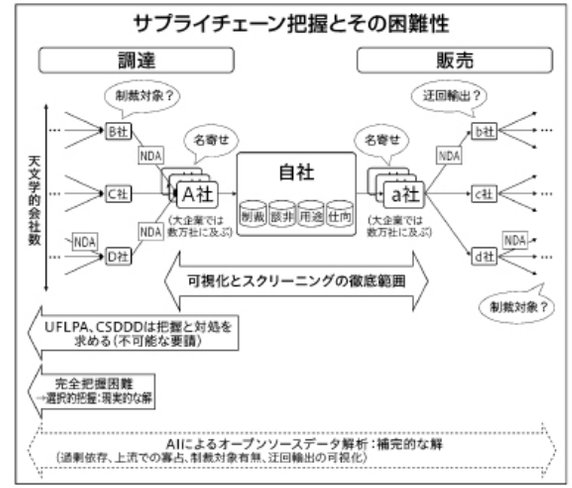
しかも年100回以上の更新があり、人手による管理は事実上不可能だ。まずは専門データベースを導入しなければならないだろう。

しかし、取引先を洗い出しただけでは不十分だ。米国のウイグル強制労働防止法（UFLPA）や欧州連合（EU）の企業持続可能性デューデリジェンス指令（CSDDD）は、サプライチェーンから問題企業の排除を求める。日本の経済安全保障推進法における基幹インフラ保護制度も、機器やソフトウエアの供給網の透明化を求めている。

だが、実際の企業間取引では秘密保持契約（NDA）があり、顧客や仕入れ先を完全に把握することはできない。こうした背景から、すべてのサプライチェーンの網羅的な把握を目指すのは現実的ではない。

問題は制裁対象企業の特定にとどまらない。国際情勢の不安定化に伴う供給途絶リスクに対処するには、自社の供給網のチョークポイントを把握し対策することが最も重要となる。対策は「備蓄」「代替調達ルート」「省資源・リサイクル」「代替品採用・開発」の4種だが、いかに早く着手できるかは、サプライチェーンの可視化の度合いで差が生じる。

限られたリソースを「重要部材」「高依存国」などリスクの高い領域に集中し把握・管理を徹底することが現実解だろう。その上で、サプライチェーン上の脆弱（ぜいじゃく）性特定にオープンソース情報のAI解析などを導入することも有効な施策。しかし、サプライチェーン把握はそれ自身が目的ではなく、対策を講じるための手段である。リスク認識時に代替調達や政府との協議が可能な体制を整えることが肝要だ。



高リスク把握・管理に資源集中

サイバー・人・取引に対策

情報保全も企業存続の要である。企業機密の漏えいに敏感な経営者は多いが、不正競争防止法が定める営業秘密の3要件（秘密管理性・有用性・非公知性）を理解し、運用できている企業ばかりではない。現場の負荷軽減を優先し、ルール通りの管理ができていないケースは少なくない。対処を現場任せにせず、経営が率先して現場をサポートしなければならない。

筆者は情報漏えいの出口は三つ（サイバー、人、取引）と整理している。サイバー分野では、近年ランサムウエアによる被害が急増している。CSIRT（インシデント対応チーム）の設置は常識だが、それだけでは十分ではない。CSIRTの分析手法向上に加え、常時監視・検知・初動対応を担うSOC（Security Operations Center）を設置する企業も増えている。SOCの存在は、予兆検知型の防御体制を意味する。

今後は、国家支援型攻撃（APT攻撃）を想定した監視も必要だ。そこには政府からの情報も欠かせない。日本企業が連続して受けている被害を他山の石として、いま一度、自社のサイバー対策を点検する好機と捉えるべきだ。

人による情報漏えいはさらに複雑だ。米国の防課分野では、金銭、思想・信条、脅迫、虚栄が情報漏えいの動機になるとしてMICE（Money、Ideology、Coercion、Ego）と呼ばれる心理モデルを用いている。こうした動機は経済的・心理的圧力が複雑に絡み合う点に特徴がある。転職時の情報持ち出しや、正義感による内部告発的行為などが典型例だ。外国の影響下にある人物からの働きかけによる情報持ち出しも報告されている。従って、情報が格納されたサーバーへのアクセス権設計も精緻に行う必要がある。

退職者管理も重要だ。退職予定者と秘密保持の覚書を結ぶのは当然だが、むしろ退職意思の表明時点から秘密情報にアクセスさせないといった実効性の高い対処が必要になる。重要な情報に触れられる人物であれば、退職後の無用のトラブルを避けるのが得策だ。加えて、いわゆるセキュリティー・クリアランス保持者の退職といった状況を想定すれば、当該人物の退職後の消息を企業が把握しておくべきことは言うまでもない。

取引に伴う漏えいも見逃せない。設計情報や仕様書をサプライヤーと共有するのは日常的だが、日常的であるが故に情報の扱いが軽視されがちである。加えて、取引先の支配権が変化すれば、情報の流出経路にもなり得る。契約書に定めた支配権変更条項（CoC Change of Control）の順守や、取引先の所有構造の定期的な確認が欠かせない。

では、企業が真に守るべき秘密とは何か。実はこの特定が難しい。自社にとって重要ではない秘密でも、国内の上位競合企業にとって重要な情報かもしれない。筆者の経験では、技術者に「あなたの技術は重要か」と聞けば、全員が「自分の技術は重要だ」と答える。管理する側にとっては実に悩ましい。

筆者は情報の特定より情報の出口を止めることが重要と考えている。企業から情報を出す三つの方法（電子メール・チャット、印刷、USBメモリーなどへの格納）を封じるのが重要であり、それぞれに対策を提案してきた。

結局のところ、情報保全はIT部門だけの課題ではない。人事や調達、経営企画など、組織全体の責任である。例えば人事部門においては、従来は「人の情報を聞かない・持たない」ことがコンプライアンスとされてきたが、今日では「人の情報を適正に把握・管理する」ことこそリスク回避の前提である。経営層はサプライチェーンと情報保全の両輪を統合的に監督し、経済安全保障の観点から企業統治を再設計する責務を負っている。

組織全体で出口止める

情報漏えい 3つの出口

漏えいルート	行為	
サイバー攻撃	・フィッシング ・ランサムウエア ・APT攻撃	・マルウエア ・DDoS攻撃
人を介した漏えい	・経済諜報 ・ルール不徹底・誤認・不注意	・転・退職時の持ち出し ・みなし輸出管理不徹底
取引を介した漏えい	・サプライチェーン ・M&A、アライアンス	・生産拠点の海外展開

企業にとって守るべき情報とは何か？

- 他者情報
  - 国家機密（特定秘密保護法・重要経済安保情報保護活用法など）
  - 他者（顧客など）から預かった情報・個人情報
- 自己情報
  - インサイダー情報・弁護士秘匿特権付き情報など
  - 安全保障上管理が必要な情報
  - 競争力の源泉となる情報（競争環境への十分な配慮も必要）

守るべき「情報の特定」と、その「管理レベル」確定のみならず、「秘匿性を失った情報」の秘密解除も重要

日刊工業新聞　2025年11月26日掲載　無断転載・複製禁止