JPMA NEWS LETTER
2023年11月号 No.218

Topics｜トピックス

経済安全保障セミナー「経済安全保障とサイバーセキュリティ」を開催

2023年9月26日に、製薬協産業政策委員会経済安全保障タスクフォース（経済安保TF）主催による経済安全保障セミナー「経済安全保障とサイバーセキュリティ」が、会員会社を対象にウェブ形式にて開催されました。当日は103名が参加し、東京海上ディーアール主席研究員の川口貴久氏の講演、経済安保TFのサイバーセキュリティサブチームによる報告および質疑が行われました。東京海上ディーアールは2021年11月より、経済安保TFの活動を支援しています。

1. セミナー開催の背景

製薬協産業政策委員会経済安保TFは、米中のデカップリングの動きに端を発する我が国の経済安全保障法制化やそれと呼応する経済団体の動きを踏まえ、製薬協においても経済安全保障に対応する組織が必要との考えに至り、2021年10月に産業政策委員会に設置されました。経済安保TFでは、多岐にわたる経済安全保障の対象を踏まえ、サプライチェーン、研究・開発、サイバーセキュリティの3つのサブチームを設置し、関係省庁との意見交換、法令等へのパブリックコメント対応やセミナー開催による会員会社への情報提供等に取り組んできました。

今回のセミナーは、経済安保TFおよびサイバーセキュリティサブチームの検討結果の一端を紹介するものです。

第1部では、経済安全保障に関する幅広い課題・テーマと業界への影響を確認するとともに、特にサイバーセキュリティ関連のテーマを掘り下げて紹介しました。第2部では、サイバーセキュリティサブチームから、業界の特徴・リスクを踏まえたケーススタディおよび対策時の留意点を紹介しました。

2. 川口貴久氏講演「経済安全保障から見たサイバーセキュリティ問題」

全体像：経済安全保障とサイバーセキュリティ

2022～2023年、日本では経済安全保障政策が大きく進展しました。2022年5月に成立した経済安全保障推進法（推進法）の施行や制度の具体化が進み、2022年12月の「国家安全保障戦略」でも経済安全保障が強調されました。また国外に目を向ければ、G7広島サミット2023、欧州の「経済安全保障戦略」、米中対立の激化等、目まぐるしい動きがあります。

こうした動向を踏まえると、企業が対処すべき経済安全保障上のリスクは推進法の4テーマに限定されません。分類や整理の方法にもよりますが、少なくとも18の経済安全保障上のテーマがあります。これらのうち、いくつかは製薬業界に大きな影響をもたらすものです。

そして、本日のセミナーの焦点である「サイバーセキュリティ」との関連性では、基幹インフラのサイバーセキュリティ強化（下記**表1**中No. 2）、セキュリティ・クリアランス（No. 5）、産業スパイ・サイバーセキュリティ対策（No. 6）、データをめぐる安全保障（No. 7）が注目に値します。

表1　経済安全保障関連の政策課題・テーマ（2023年8月時点）

分類	No.	経済安全保障上のテーマ	業界影響	提言・成果文書等での言及（年/月） G7 23/5	政府 22/12	国会 22/5	与党 23/5	財界 22/9
推進法関連	1	サプライチェーン強靭化	大	●	●	●	●	●
	2	基幹インフラのサイバーセキュリティ強化	小？	●	●	●	●	●
	3	特定重要技術の開発支援	中		●	●	●	●
	4	特許出願の非公開	小		●	●	●	●
	5	セキュリティ・クリアランス	小		●	●	●	●
推進法以外	6	産業スパイ・サイバーセキュリティ対策	中		●		●	
	7	データをめぐる安全保障	大	●			●	
	8	偽情報・ディスインフォメーション対策	中？				●	
	9	研究インテグリティの見直し	中	△	●			
	10	安全保障貿易管理の強化	小	△	●		●	
	11	重要・新興技術管理	大	●	●		●	
	12	国際標準化	中？	●				
	13	非市場的政策、慣行への対応	大？	●				
	14	経済的威圧への対処	小？	●	●			
	15	サプライチェーン上の人権リスク対応	中			●		●
	16	投資審査の取組・体制強化	中	△	●		●	
	17	業界ごとの「リスク点検」	大		●			
	18	経済インテリジェンスの強化	小			●	●	●

大	経営戦略や事業計画の見直しが生じる影響（プラス、マイナスのいずれもあり）がありえる。
中	影響はありえるが、「大」ほどではない。
小	影響はほとんどない。または無視できる。

出典：各種資料を基に筆者作成。
※1「経済安全保障上のテーマ」は相互に排他的・包括的な分類・整理ではない。ここでは、企業が対応すべき経済安全保障上の課題を洗い出すという点で、重複は許容している。また、上記のテーマは既に日本で法整備等が行われたもの、政策形成が進んでいるもの、国会・政府・財界から提言がなされているものをとりあげた（ただし、企業との関係が薄い「重要な土地取引の規制」等は除く）。
※2　セキュリティ・クリアランスについては2024年通常国会に改正経済安全保障推進法を提出し、制度を構築予定であるため、上記の通り表記している。
※3「提言・成果文書等」の詳細は以下の通り。
- G7：「経済的強靭性及び経済安全保障に関するG7首脳声明（仮訳）」（2023年5月20日）
  ●は首脳声明の大項目・中項目のテーマ、△はそれ以外やその他関連文書で言及されたもの（ワンフレーズ程度の言及は除く）。
- 政府：『国家安全保障戦略』（2022年12月16日閣議決定）
- 国会：参議院内閣委員会 附帯決議（2022年5月10日）　※衆議院内閣委員会でも附帯決議を採択しているが、参議院の方が内容・項目数が多いため、こちらを採用。
- 与党：自由民主党政務調査会および経済安全保障推進本部「『経済財政運営と改革の基本方針 2023』に向けた提言」（2023年5月23日）
- 財界：一般社団法人日本経済団体連合会「経済安全保障法制に関する意見：有識者会議提言を踏まえて」（2022年2月9日）

※初出および各テーマの詳細は、川口貴久、渡邉彩恵香「変化する経済安全保障環境と企業のリスク管理」『リスクマネジメント最前線』（2023年9月20日）を参照。

背景：米中対立としてのサイバーセキュリティ問題

経済安全保障全般をめぐる政策議論の背景には米中対立があり、同様にサイバーセキュリティ問題の背景にも米中対立があります（日本固有の事情があるセキュリティ・クリアランスは除く）。

2010年代以降、米中間では2つのサイバーセキュリティ問題が顕在化しました。米国側の主張によれば、（1）中国が先端技術の強制移転を目的として米国等の民間企業に対してサイバー攻撃を行っていること、（2）中国がその支配・影響下にある中国企業を通じてサイバー攻撃を行う恐れがあること、の2点です。前者については、2015年9月、バラク・オバマ大統領と習近平国家主席によって、サイバー産業スパイ行為を禁止する合意に至りましたが、現在、この合意は破綻したというのが一般的な見方です。後者については、中国企業を含むあらゆる組織に中国政府の情報活動への「支持、援助及び協力」を義務付けた国家情報法（2017年6月施行）を懸念し、米国やいくつかの国は中国系の通信機器メーカー等が政府調達や重要インフラ調達に参画することを規制しています。

各論：経済安全保障とサイバーセキュリティの重複領域

こうしたサイバー分野での米中対立を背景に、日本でも経済安全保障の観点でサイバーセキュリティ問題が注目されています。経済安全保障とサイバーセキュリティの交錯分野のうち、いくつかのテーマは業界への影響が小さくありません。

推進法中の「基幹インフラのサイバーセキュリティ強化」は14の基幹インフラ事業のうち、一定規模等の条件を満たす事業者の重要な設備、ソフトウェア、サービス、委託先を政府が事前審査する制度です。目的は一般的なサイバーセキュリティ対策ではなく、外国政府の支配・影響下にある企業を調達から排除すること等（推進法中の用語でいう「特定妨害行為」の防止）です。現在、製薬業界は対象業種ではありません。しかし、指定業種でなかった「港湾」「医療」は近年の大規模サイバー攻撃被害を踏まえて、追加指定が検討されています。製薬業界で大規模な被害をもたらすサイバー攻撃が発生すれば、追加指定の可能性も否定できません。

「産業スパイ・サイバーセキュリティ対策」は、外国政府・軍・情報機関やこれらの「委託先」によるサイバー攻撃を通じた産業スパイ・強制技術移転への対処です。たとえば、米国保健福祉省は2022年9月、バイオテクノロジー企業、がん研究施設、製薬会社等ヘルスケア業界を継続的に狙う「APT41」というハッキンググループに注意喚起を行っています。

「データをめぐる安全保障」とは、外国政府による不当なガバメントアクセス（民間企業が保有するデータへの政府の強制的なアクセス）や個人データ・産業データの越境移転規制等を含むテーマです。G7広島サミット2023等では懸念が表明されました。ビジネスプロセスで生成・収集されたデータを蓄積、移転・共有、分析することはビジネスの効率化や革新に不可欠ですが、各国政府は安全保障を名目にデータに関する規制強化を進めています。

「セキュリティ・クリアランス」とは、機密指定された情報へのアクセスのための適格性審査のことで、2024年の通常国会で関連法案（改正経済安全保障推進法）が提出される予定です。今後、経済制裁にかかわる情報、サイバー脅威情報等が経済安全保障上、重要な情報に指定される見込みです。

対応：企業に求められる経済安全保障対応とサイバーセキュリティ対応

最後に、経済安全保障全般への対応体制、その中でもサイバーセキュリティ対策について紹介します。いずれも、リスク管理体制の「3線防御（3 lines of defense）」でいう第1線、第2線、第2.5線、第3線の役割分担や連携が重要です。

冒頭で示した通り、企業が直面する経済安全保障関連テーマは非常に幅広く、変化する外部環境に左右されます。したがって、さまざまな経済安全保障上のリスクに「抜け・漏れ」なく、かつ個別の経済安全保障リスクに対応することが期待されます。経済安全保障上の課題やリスクに効果的に対応できている企業・組織の特徴として、（1）サイバーセキュリティ対策、安全保障貿易管理、研究インテグリティ等の個別の経済安全保障テーマ・リスクは第1線（事業部門）や第2線で対応し、（2）経済安全保障に関するテーマ・リスク全般や政策動向全般は、第2.5線のような機能が担うことが指摘できます。「第2.5線のような機能」とは、常設組織であれば、リスク統括部門、経営企画部門、経済安全保障専任部門、政策渉外部門等で、業種・企業によりさまざまです。

経済安全保障を考慮したサイバーセキュリティ対策でも、組織内での役割分担や連携が期待されます。第1線（事業部門等）と第2線（IT・セキュリティ部門）が基本的なサイバーセキュリティ対策・投資を行ったうえで、第2.5線（リスク統括部門や政策渉外部門）が、第2線と連携し、政策・規制情報の収集・展開等の経済安全保障を考慮した対策を追加実施することが重要です。

3. サイバーセキュリティサブチーム報告

製薬業界の特徴

製薬協 産業政策委員会 経済安全保障タスクフォース サイバーセキュリティサブチーム　**鶴岡 信子** リーダー

製薬事業者は、その事業の性質上、研究開発情報、患者さんや治験参加者の方の医療情報を含む機微情報を大量に取り扱います。また、社会における重大なミッションとして、製剤を安定的に患者さんに届ける必要があります。

ケーススタディで具体的に触れる通り、業界構造の変化、社会環境・技術革新から、近年、サイバー攻撃による事業への影響が拡大しています。また、翻って外部環境を見ると、日米ともにサイバー攻撃の件数は増加基調にあり、特にランサムウェア被害は、製薬事業者を含む業界カテゴリが両国でトップにランクインしており、発生可能性も高まっています。

このような状況の中、具体的な対応は各社の経営判断によりますが、平時の予防・有事の対応の両面で対応が必要です。そこで、製薬協会員会社において想定される場面を具体的なケースを通じて検討したうえ、実際にインシデントが発生した場合に備えた対応体制構築時における留意点について報告しました。

■ ケーススタディ

内部からの情報漏洩

製薬協 産業政策委員会 経済安全保障タスクフォース サイバーセキュリティサブチーム　**赤尾 雄一郎** 委員

製薬企業にとって情報漏洩がもたらす影響は、レピュテーションの低下、研究開発における国際的な優位性の喪失、治験参加者の減少、といったことが考えられインパクトは大きいものとなります。また、創薬過程が垂直統合型から水平分業型になったことから、大学・ベンチャー、ベンチャーキャピタル、医薬品開発製造受託機関（CDMO）・医薬品製造受託機関（CMO）・医薬品開発業務受託機関（CRO）といった社外関係機関の増加に伴い転職者が増加し、情報漏洩リスクも上がっています。情報漏洩のルートとして、現職従業員と中途退職者からの漏洩が多いことが明らかとなっています。そこで、大手化学メーカーで発生した事例をもとに要因と対策について紹介します。

(1) ケーススタディ

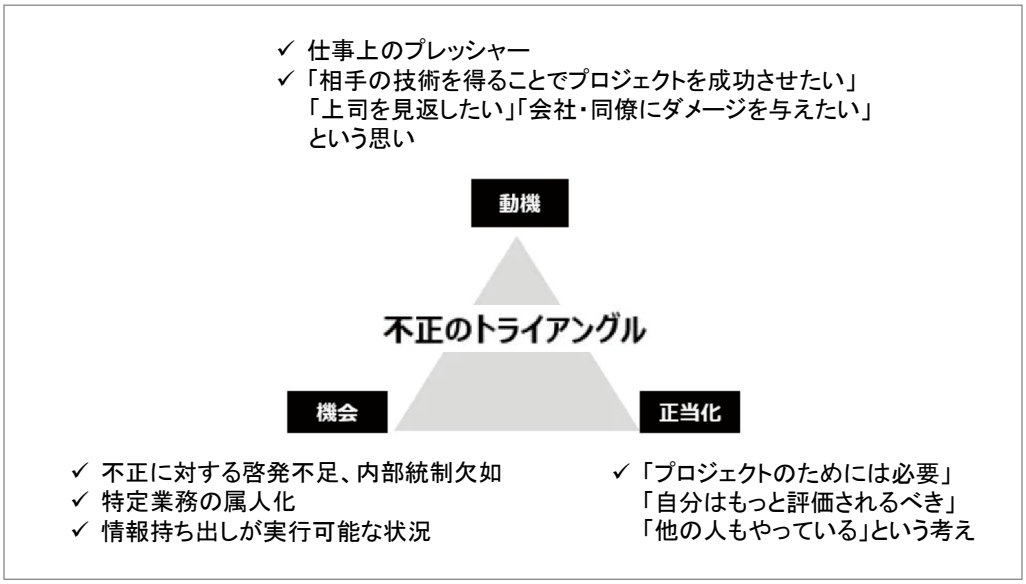
大手化学メーカー（A社）の従業員Bから中国へ情報漏洩が発生しました。

a. ビジネス版SNSを介して、中国企業がA社の従業員Bに接触。技術指導を依頼し顧問のポジションを打診。
b. A社は日ごろから機密情報へのアクセス制限等、管理を行っていたが、従業員Bは製造工程に関する技術情報を外部メモリーにコピーしメールで中国企業に送信。
c. A社の内部調査により不正が発覚し、従業員Bを懲戒解雇し、刑事告訴。
d. 大阪府警が不正競争防止法違反の容疑で元従業員Bを書類送検。
e. 大阪地裁は元従業員Bへ懲役2年、罰金100万円、執行猶予4年の有罪判決を下す。

(2) 情報漏洩の原因分析と対策

不正のトライアングルという理論があり、「動機」「機会」「正当化」の3つの要素が揃うと内部不正が起きやすいとされています。情報漏洩においてそれぞれの要素について、原因を**図1**に挙げました。

図1　不正のトライアングルと情報漏洩の原因



対策としては、経済安全保障の理解、退職意思表明者への対応、セキュリティ対策の強化、従業員との適切な関係性構築、コンプライアンス教育の徹底、といったことが考えられます。外部環境の理解を進めつつ、自社に必要な対策を講じることが重要です。

■ ケーススタディ

サプライチェーンへのサイバー攻撃

製薬協 産業政策委員会 経済安全保障タスクフォース サイバーセキュリティサブチーム　岩井 克仁 委員

医薬品の安定供給は製薬企業としての重要な使命です。そこで、その脅威となり得るサプライチェーンへのサイバー攻撃の特徴や対策について、事例とともに紹介します。

(1) 経済安全保障とサイバー攻撃の関係

ロシア政府によるウクライナへのサイバー攻撃は2015年ごろから始まりました。ウクライナ侵攻後は、同国への支援を表明する諸外国への報復としての攻撃が見られます。ロシア政府との関係性は不明ですが、我が国による対露経済制裁の表明後に国内大手自動車メーカーの委託先にサイバー攻撃がありました。一般的にサプライチェーンへのサイバー攻撃が顕在化すると、被害が長期化する、広範囲に及ぶという特徴があり、本件も甚大な被害につながりました。

(2) サプライチェーンの弱点を悪用した攻撃

スマートファクトリーやIoTが進み、工場システムが域外のものと通信する機会が増える傾向にある中、独立行政法人情報処理推進機構（IPA）による「情報セキュリティ10大脅威」においても「サプライチェーンの弱点を悪用した攻撃」が順位を上げています（**表2**）。

そこで、経済産業省は2022年11月に「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」（https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html）（以下、工場セキュリティガイドライン）を策定しています。

表2　情報セキュリティ10大脅威2023

順位	内容	対前年	順位	内容	対前年
1位	ランサムウェアによる被害	→	6位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	↑
2位	**※サプライチェーンの弱点を悪用した攻撃**	↑	7位	ビジネスメール詐欺による金銭被害	↑
3位	標的型攻撃による機密情報の窃取	↓	8位	脆弱性対策の公開に伴う悪用増加	↓
4位	内部不正による情報漏えい	↑	9位	不注意による情報漏えい等の被害	↑
5位	テレワーク等のニューノーマルな働き方を狙った攻撃	↓	10位	犯罪のビジネス化（アンダーグラウンドサービス）	↑

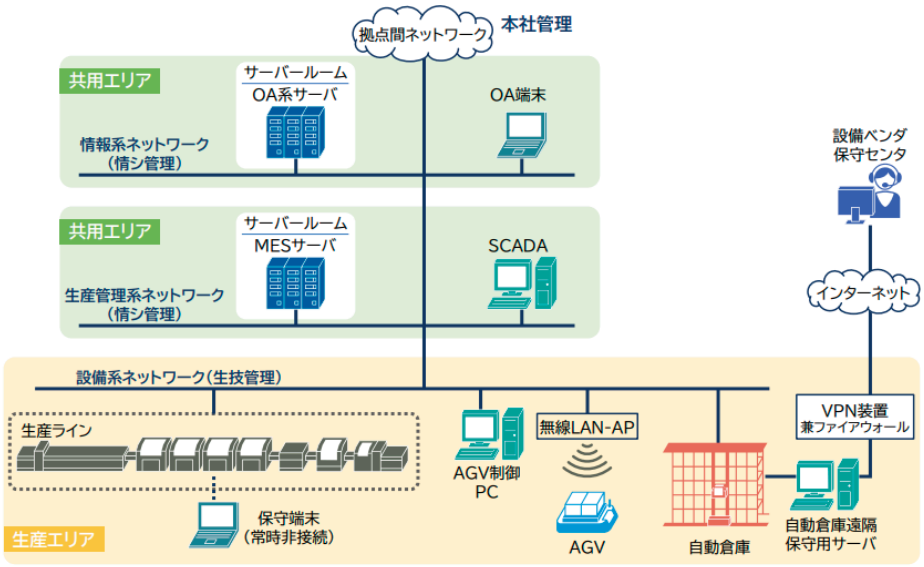
※IPAウェブサイト（https://www.ipa.go.jp/security/10threats/10threats2023.html）より

(3) サプライチェーンへのサイバー攻撃に対する対策

生産エリア内の工場システムのライフサイクルは機械設備と合わせることが多く、10年から20年以上といわれています。結果、どこになにがあるのか、どうつながっているのかがわかりづらくなっているケースが多いです。

そこで、これら工場システムを台帳管理し可視化する、また生産エリア内で通常とは種類の異なる通信があった場合には、速やかに検知できる仕組みを整えることが大切です（**図2**）。

図2　サプライチェーンへのサイバー攻撃に対する対策



工場システムの例（出典：工場セキュリティガイドライン）

(4) 製造委託先への対策

自社医薬品の安定供給のためには、製造委託先を含めてサイバー攻撃への防衛力を強化する必要があります。すでに公表されているセルフチェックシートや外部評価サービス等をうまく活用すれば、製造委託先および自社製造所の防衛力の可視化・改善につながります。

情報セキュリティインシデント対応体制構築時における対応事項

製薬協 産業政策委員会 経済安全保障タスクフォース サイバーセキュリティサブチーム　**鶴岡 信子** リーダー

情報セキュリティインシデントは、発生しないことが理想的ですが、現代の環境において完全に防ぐことは不可能です。実効性を高めるためには、原則として具体的な場面を想定しながら対応検討を進めることが重要です。

(1) インシデント対応の役割分担

インシデント発生時に全体をリードする責任組織と、個別の役割を担う関連部門が連携する際、組織間の役割分担・情報共有範囲の整理を行うことで、不必要な混乱を避けた迅速な対応が可能になります。

(2) 社内対応体制

インシデント発生時に、速やかに情報を把握できる体制構築が求められます。個人情報保護規制では、発生の把握から当局報告まで期限がある場合もあり、法令順守の観点からも特に重要です。

(3) 社外連携体制

インシデントが起きた際には、社外対応も必要となります。連携先、関係者への連絡窓口（社内の役割分担）、連携が必要な場面の事前確認により抜け漏れを防ぎ、適切な優先順位での対応が期待できます。

(4) 社外公表

時々の流行に合わせた仮説を具体的に想定することにより、報告の必要のある程度に事業に重大な影響を与えるインシデ

ントの判断基準を構築し、迅速かつ的確な開示を可能とすることが期待できます。

4. 当日の質疑の様子

それぞれの講演・報告の終了後に質疑の時間が設けられました。経済安全保障リスク管理体制構築における業界ごとの特徴、中国に出張する際の留意点、インシデント対応体制構築時の想定場面の具体例、全社的な危機管理対応部署と情報セキュリティインシデント対応部署との役割分担について質問が出されました。

（産業政策委員会 経済安全保障タスクフォース サイバーセキュリティサブチーム リーダー　鶴岡 信子）