「第 4 回 経済安全保障セミナー」を開催

2024 年 11 月 25 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「第 4 回 経済安全保障セミナー」が、製薬協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 82 名が参加し、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC） 政策担当部長 兼 早期警戒グループマネージャーの佐々木 勇人氏に「サイバー脅威の最新動向と製薬業界」をテーマにご講演いただきました。

開催の背景

経済安保 TF は 2021 年 10 月に設置され、多岐にわたる経済安全保障の業界への影響等の考察を中心に活動を進めてきました。同 TF 内には、サプライチェーン、研究・開発、サイバーセキュリティの 3 つのサブチームが設置されており、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。
なかでもサイバーセキュリティに係るリスクは昨今、経済安全保障面で企業経営における大きなリスクとなっていることから、サイバーセキュリティーチームが中心となり、製薬協会員会社向けのセミナーを開催することに至りました。

開会挨拶

「第 4 回経済安全保障セミナー開催にあたって」
産業政策委員会 谷藤 道久 委員長

私たちは 2020 年から 3 年余りにわたりグローバルパンデミックを経験しました。ワクチンや治療薬といった医薬品の速やかな研究・開発、それらを確実に世界中の皆さんへ届けるためのサプライチェーンの重要性を実感しました。さらに外出が制限される中、デジタル技術とインターネットの恩恵を享受する一方で、サイバー空間の濫用や悪用による新たな脅威が発生しました。今やサイバーセキュリティは経営レベルのリスクです。今回のご講演が皆さんにとって示唆に富んだものになるものと確信しています。

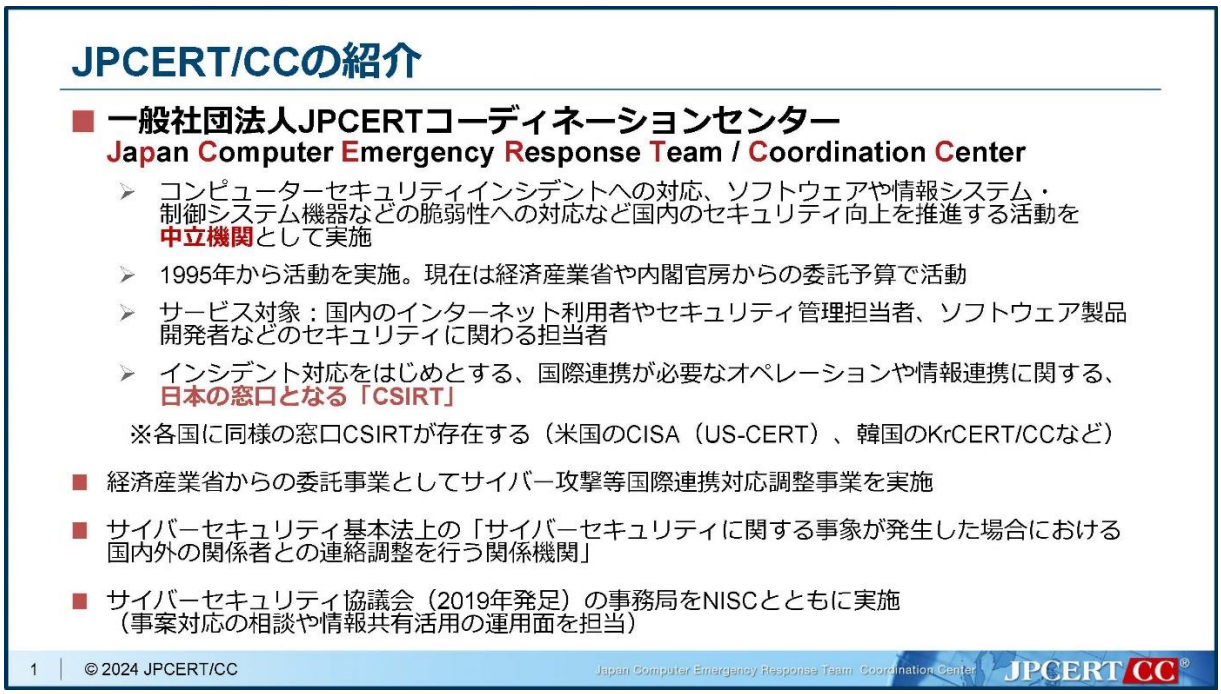
講演

「サイバー脅威の最新動向と製薬業界」

一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）政策担当部長 兼 早期警戒グループマネージャー、脅威アナリスト、
防衛研究所 政策研究部サイバー安全保障室 特任研究員　佐々木 勇人 氏

本日は、皆さんが不幸にもサイバー攻撃を受けてしまった際の被害を最小限に抑える対処法を中心にお伝えします。
はじめに JPCERT/CC を紹介します。世界各国では自国の情報セキュリティ向上を推進するための中立機関が自然発生的に存在しており、その日本版が JPCERT/CC です。情報セキュリティに係るインシデント発生時の初期的な救急対応や国際連携が必要なオペレーション・窓口を担っています（図１）。

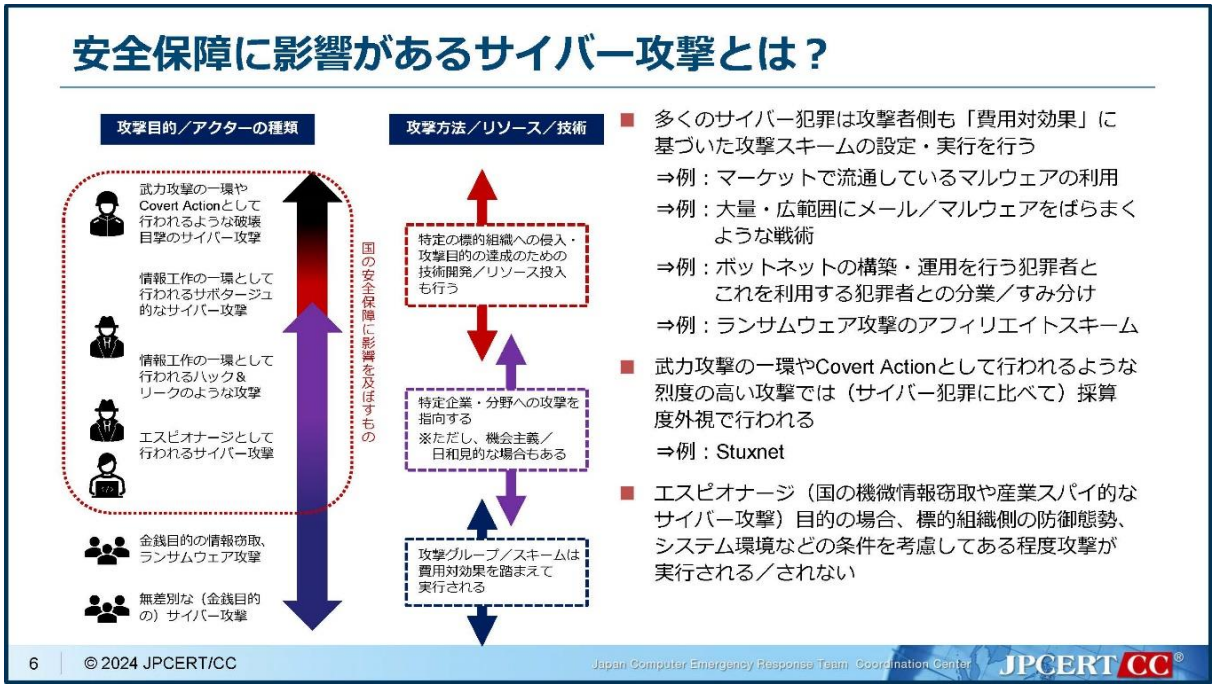
図１．JPCERT/CC の紹介



経済安全保障と製薬企業の関係においては、サプライチェーンの強靭化の中で複数の抗菌剤が特定重要物資に指定され、厚生労働省から「抗菌性物質製剤に係る安定供給確保を図るための取組方針」が公表されています。その中でもサイバーセキュリティの確保に関する記述がありますが、ここに対応するだけでは皆さんの目の前に迫っている脅威への対応としては十分では無いと見ています。そこで、もう少し違う視点からの対策が必要と考えていますので、そちらを紹介します。

はじめに、安全保障に影響があるサイバー攻撃について解説します。
図 2 の左の「攻撃目的／アクターの種類」の上部は国家レベルの武力攻撃や機微情報の搾取に関するものであり、こうした攻撃グループは金銭目的の犯罪グループと比較すると、採算度外視で計画し実行することがあります。
一方で、下部にある金銭目的の情報搾取やランサムウェア攻撃などは特定の集団が費用対効果を見て判断する攻撃です。

図２．安全保障に影響があるサイバー攻撃とは？

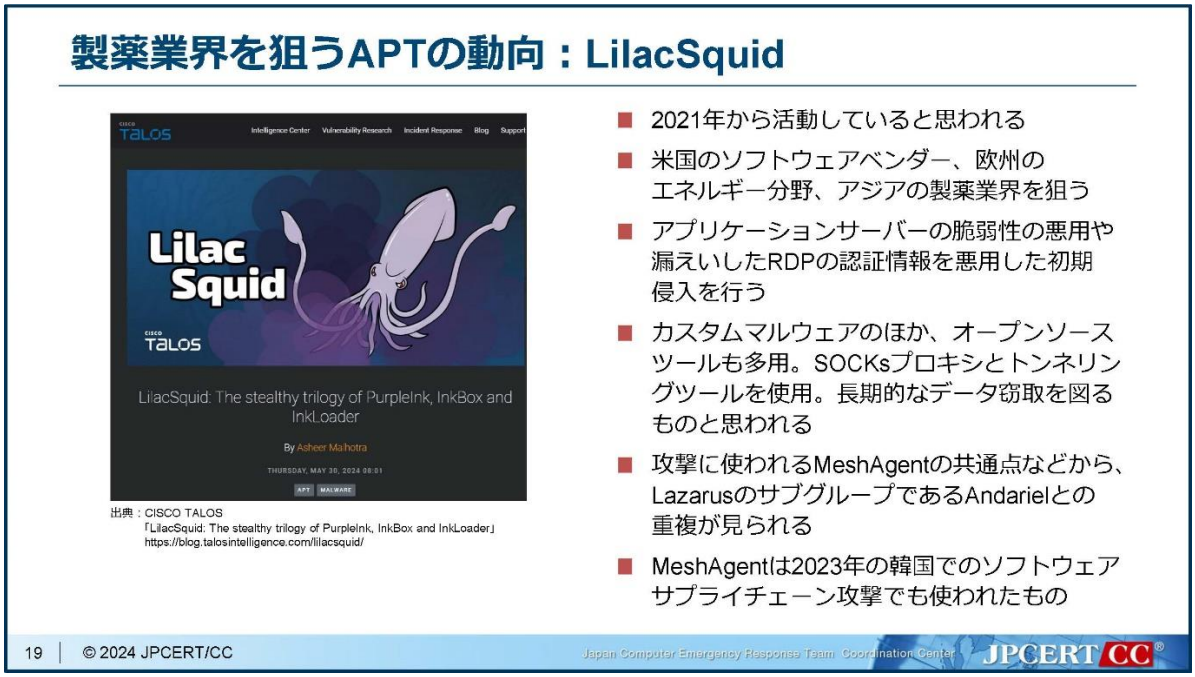


米国では 3 年前に米国東海岸の燃料供給の約半分を担うコロニアル・パイプライン社へのランサムウェア攻撃が発生し、米国最大規模のパイプラインがストップしました。おそらく金銭等を目的にした犯行だと思われます。それが端緒となり、米国においてサプライチェーンとサイバーセキュリティとの関係性が経済安全保障の面からも問題視されるようになりました。このように、国家レベルではない犯罪集団によるサイバー攻撃であっても、国の安全保障に影響を与えうるということです。一般的にこのような犯罪集団は、費用対効果を鑑みて何度も攻撃を仕掛けます。そのような攻撃に対して、我々は無意識に自分たちが「攻撃される確率」をイメージしてしまう傾向がありますが、ここには攻撃の「遭遇率」に対する認識のギャップがあります。たとえば、あるネットワーク機器に脆弱性が発見された場合に「XX%の機器に攻撃がありました」といったことが公表されるケースがあります。しかし、攻撃は公表以降も続きます。その機器を利用する企業として速やかにその脆弱性への対処を済ましておかないと、やがて被害に遭う可能性が高まります。つまり、「遭遇率」が低いからといって被害を受けるリスクも低いという訳ではなく、侵入され被害を受けるのは「時間の問題」なのです。昨今、個人情報などの機密情報を保有する組織だけではなく、より広い範囲で被害が発生する傾向があります。その原因はネットワーク機器の脆弱性を突く攻撃が増えているからです。インターネットに接続されたすべてのネットワーク機器を把握し、適切に管理・対処するこが重要です。
また、その脆弱性を悪用する事案にも変化が見られます。従来はメーカーまたは専門機関による注意喚起が発信されてから、各企業は数日内にその修正対応をするということが一般的でした。しかしなが

ら、脆弱性を悪用した攻撃が実行されるタイミングが早まっています。このような状況下においては、脆弱性への対応をするタイミングでは、すでに侵害されている可能性もあるため、並行して侵害有無を調査しておくことも大切です。

ここからは攻撃・犯罪グループの動向を紹介します。
図 3 は 24 年 5 月に CISCO 社から発出されたレポートの抜粋です。
「Lilac Squid」と名付けられたグループで 21 年ごろから活動しています。米国ソフトウェアベンダーや欧州エネルギー分野、アジアの製薬企業を狙う攻撃が多数確認されています。

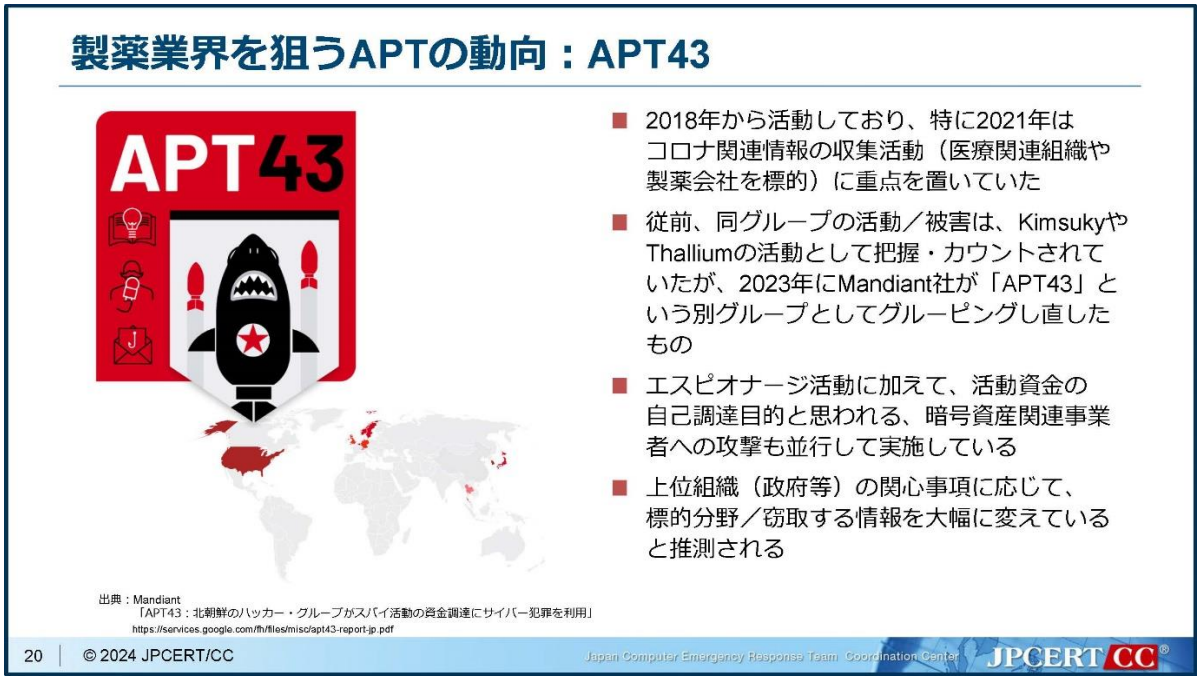
図 3．製薬業界を狙う APT の動向：LilacSquid



出典：CISCO TALOS
「LilacSquid: The stealthy trilogy of PurpleInk, InkBox and InkLoader」
https://blog.talosintelligence.com/lilacsquid/

さらに、図 4 の Mandiant 社レポートから APT43 という北朝鮮で編成された犯罪グループを紹介します。21 年ごろは医療関連組織や製薬会社を標的としていたことから、コロナ関連情報の収集活動をしていたと見られています。上位組織（政府等）の関心事項に応じて標的を集中させているのではないかと仮説を立てています。

図４．製薬業界を狙う APT の動向：APT43

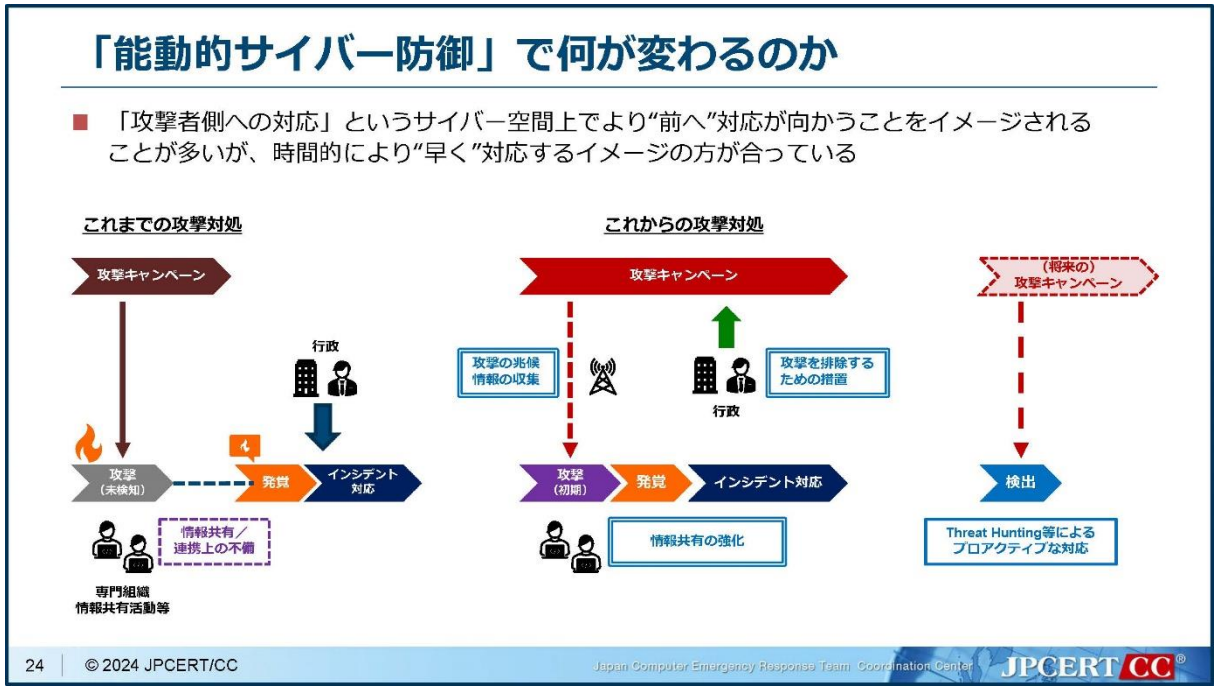


このような情報搾取目的の犯罪グループの最近の動向として、活動資金の自己調達目的などのためにランサムウェア攻撃にも関与するケースがあります。あるいは、搾取した後に、その痕跡を消す、または、攻撃を受けた組織を混乱させることを目的に、ランサムウェア攻撃を仕掛ける可能性も想定されるなど、「ランサムウェア感染が発生したが、実は APT アクターによる機微情報窃取が行われていた」といったケースがあるなど、事象が複雑化しています。

このような背景から、企業がランサムウェア攻撃を受けた場合には、ランサムウェアやアクターを可能な限り特定し、その復旧を図る前に、情報搾取の有無などを調査しておく必要があります。

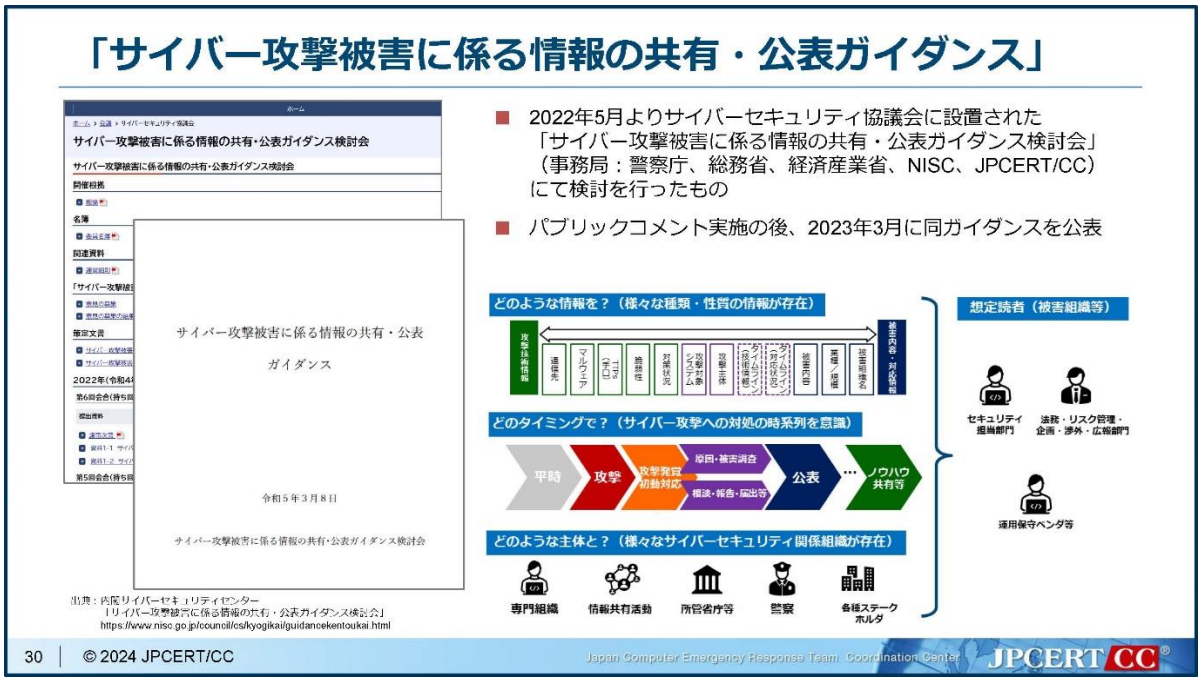
続いて国が進める「能動的サイバー防御（ACD）」という観点からお話しいたします（図５）。

図５．「能動的サイバー防御」で何が変わるのか



2022 年の国家安全保障戦略では、「通信事業者が持つ通信データを活用し、より早くサイバー攻撃の兆候を掴むこと」、「官民の情報連携体制を強化し、より早く国に情報が入るようにすること」さらに、「攻撃の兆候を早くに察知した場合には、その攻撃を止める/無害化する」と示されています。サイバー攻撃を完全に防ぐのではなく、早期に検知し対応することで、被害を最小限に抑え込むといったプロアクティブな考え方です。すでに北米を中心に通信事業者やネットワーク機器事業者が保有する情報から早期に攻撃を検知し、被害の拡大を防いだといった事例が発表されています。
しかしながら、早期に攻撃を検知し対処することで、企業・現場側に攻撃の痕跡が十分に残らないケースが増えます。結果、当局などへの被害報告において、全容を示しづらいという課題が生じます。具体的には、攻撃による被害を最小限に抑え込んだというサイバー専門組織の立場、攻撃そのものはあったという当局の立場、その間に立つ企業の立場というように、立場の違いからミスコミュニケーションが生じる可能性が高まります。当局における攻撃・被害に対する考え方を見直してもらう必要もあるのだと思います。
ミスコミュニケーションといったトラブルを防ぐという目的もあり、23 年 3 月に「サイバー攻撃被害に係る情報の共有・公表ガイダンス」が公開されています（図 6）。どのような情報を、どのタイミングで誰に共有・公表するのかをガイダンスしています。ぜひご覧になってください。

図 6.「サイバー攻撃被害に係る情報の共有・公表ガイダンス」



さらに 2023 年 3 月には経済産業省と我々（JPCERT/CC）が共同で「攻撃技術情報の取扱い・活用手引き」を作成し公開しています。前者のガイダンスは被害組織の観点から記載しています。一方で後者は被害組織を支援するセキュリティベンダー・システム保守ベンダーの観点からのものになっています。被害組織に代わって、それを支援するベンダーがセキュリティ専門組織や他のベンダーへ情報共有することで、より早く攻撃に対処することを目的にしています。
JPCERT/CC では、このようなガイダンス・手引きを用意するとともに、初動対応支援にあたる IT ベンダーといった「ファーストレスポンダー」向けの相談窓口も開設しています。我々をセカンドオピニオンとしてサイバーリスクに係る情報収集、サイバー攻撃の早期解決などにおいて活用いただきたくお願いします。

質疑応答

ご講演後には、参加企業の皆さんから佐々木氏への活発な質問があり、以下の通り貴重なご意見をいただきました。

・サイバー攻撃の初動対応から被害公表までのプロセスにおいては、IT 部門に加えてリスク管理や法務部門などが JPCERT/CC と接触を持つケースが多いこと
・サイバー攻撃を確認した際に、JPCERT/CC などのセキュリティ専門機関へ「共有」し、リスクや技術情報を入手することで、問題の早期解決につながること
・特定の業界をターゲットにする犯罪グループが多いことから、業界内でリスク情報を共有することが有効であること
・サイバー攻撃に係る報告を所管官庁へミスコミュニケーションなく伝えることができるよう、日ごろから当局とコミュニケーションを取っておくことが大切であること

（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）