# サイバー攻撃による被害に関する情報共有の促進に向けた検討会（第2回）
# 議事要旨

## 1. 日時・場所

日時：令和5年5月29日（月） 9時00分～11時00分

場所：ハイブリッド開催

## 2. 出席者

委員　　：星委員（座長）、阿部委員、石川委員、神林委員、庄子委員、武井委員、武智委員、辻委員、蔦委員、名和委員、北條委員、和田委員

オブザーバ：内閣官房内閣サイバーセキュリティセンター、内閣官房サイバー安全保障体制整備準備室、警察庁、個人情報保護委員会、総務省、法務省、最高検察庁、一般社団法人 日本経済団体連合会

事務局　　：経済産業省商務情報政策局 奥田サイバーセキュリティ課長

一般社団法人JPCERTコーディネーションセンター 早期警戒グループマネージャー 佐々木 勇人氏

## 3. 配付資料

資料1 事務局説明資料

資料2 関係者からの説明資料（非公表）

## 4. 議事内容

事務局より資料 1 の説明を行った。

その後、資料 2 について関係者からの説明に続いて、自由討議を行った。

（1） 脅威情報について

- （事業者の実務を考えると、）取り扱う情報の明確化も必要となる。匿名性やデータの利用方法や開示範囲等を明確化されないと、（安心して）情報提供する判断が出来ない。また、提供を受けた側からの守秘義務を担保しなければ、データの提供は難しい。
- 被害企業から見つかったデータは秘密情報として取り扱い、既に公開されている情報はその限りでないとしている。公開情報とは、インターネットに公開されたサーバから入手可能な情報として扱っている。情報共有が困難なケースは、被害組織を推測可能な情報がマルウェアに含まれるケースである。そのようなケースでは、たとえ、公開情報となっていたとしても、意図して情報を共有することは難しい。例えば、攻撃インフラの調査から被害組織が推測されるケースや、あるいは公開サービスにアップロードされており、被害組織が特定可能なケースが該当する。
- 統計データや抽象化したデータは公開可能としている。複数確認された事案についても抽象化した上で、公開している。一方で、共有の価値が高い事例であったとしても、一社を対象とした APT については公開が難しく、共有の壁が高いと考えている。
- 匿名情報を秘密情報から除外するという整理ができないか。情報提供を法令に基づいて行うことに加え、秘密保持を締結している人や組織に共有する場合は、秘密保持違反の例外として扱えないか。また、情報提供をセキュリティサービスの契約における履行の一環と捉え、NDA と競合する場合であっても、当該契約が優先され、情報提供によるフィードバックが得られることで、セキュリティサービスを履行するという形にできないか。
- 共有にも制限が存在する。被害者情報等インシデントの詳細情報は公開しない。共有と公開は同じ扱いにはしていない。共有については「サイバー攻撃被害に係る情報の共有・公表ガイダンス」と同じ考え方に則っており、原則公開しても問題ない情報を共有している。その他、公知情報や合意を得た情報等は公開を行っている。なお、被害組織への通知が必要と考えられるものについては個別に検討する。基本的には政府機関やサイバーセキュリティ協議会が共有先となる。

- 情報を共有する場合、書面または口頭で顧客とやり取りを行い、合意を得るプロセスを踏む。一社を対象とした APT の事例では顧客から合意を得ることが難しいのが現状である。
- APT は発見されにくい面がある。さらに自己申告がない場合、事案自体が明らかにならない。また、日本国内のみで起きている事案があり、他地域での情報収集が役に立たない場合がある。被害がどこにも共有されない場合には、被害が継続して広がるおそれがある。
- 大規模に広がるインシデントの中で、製品の脆弱性が絡むケースがある。IR 対応ベンダーは、実際に被害を受けているサービス事業者やその親会社、また被害を受けているサービスのエンドユーザー全てに関係する場合があり、このような場合のコーディネーションが非常に難しい。どこにも相談できないというのが現状であり、課題として感じている。
- APT において製品の脆弱性が悪用されている場合はその情報を広めるべきであるが、顧客が製品メーカーに対して詳しい情報共有を行わないケースが散見される。その結果、うまく情報共有がなされず、製品対応が終わる状況が見られることから、まずは、国内の APT の被害状況把握を行っていく必要があると認識している。インシデント対応を速やかに実施する必要があることに加え、その後の対応にも影響を与えるためでもあり、今後方針が明確になればよいと考えている。

（2） 情報共有について

- アナリスト間で情報共有を行うことで、調査が迅速に進んだケースがあった。また、新たな攻撃手口や不審通信、SNS 上で確認した情報を共有することによって、危険を未然に防げた事例や早期に必要な情報が得られたケースもあった。
- 他組織のアナリストから受けたフィードバックと、関連する攻撃キャンペーンとのデータが紐付き、その後の被害防止拡大に役立てることができたケースがあった。また、マルウェアの攻撃情報を共有した際、閲覧したユーザーが確認を行うケースやフィードバックを得られたケースもあった。
- 被害組織やベンダー、公的機関との関係性は重要な観点。NDA や各種規約の整備は必要であるが、顧客からは情報共有は漏えいに近い状況になると考えられ、断られるケースが多い。ユニークなインシデントについては抽象化された情報であっても、同意なしに情報共有がなされた場合にはクレームが寄せられる場合があるため、情報共有をためらう状況が発生してしまう。加えて、公的機関などへの情報共有の相談についても、相談自体をしにくい状況が発生してしまうことから、長期的な課題になると認識しており、プロセスや NDA の改変だけでは対応しきれない部分があると認識している。
- 契約でいくら処置しても、顧客間の信頼関係がないと情報共有は困難という点は重要であり、ユーザーベンダー間の信頼醸成のための仕組みづくりが重要である。
- （事業者における）情報共有の取組は（事業者の）経営層を巻き込まなければ難しい。
- 全体のとりまとめの機関がなければ情報を消化できない可能性がある。法的観点の整理も必要と考えている。
- セキュリティベンダーだけではなく、監督省庁や公正取引委員会との調整は必要である。なお、公正取引委員会については、情報連携を目的としていたとしても SOC 事業者が集まり議論をすることになり、独禁法などに抵触する行為が疑われるおそれがあるためである。また、取りまとめ機関を作るのであれば、法的な要請（裏付け）が必要である。
- ナショナルサートの検討等、国際間の情報連携における官の比重が高まっており、既存の政府機関の（非サイバーの）情報の取り扱いルールを脅威情報の取り扱いに適応してしまい失敗しているケースがある。新たなルールが必要になっていると理解している。
- ISAC 間連携について、サイバーセキュリティ協議会のような既存の仕組みが素地として機能すると思われる。
- データの共有をする際には、手作業だと手間がかかるため、データ項目やフォームの統一化やシステム化は必要と考える。したがって、情報共有するためのシステム開発も必要である。SOC ベンダーが運用可能な基準の設定も必要である。

（3） 各組織における情報の扱いについて

- SOC とインシデントレスポンス(IR)のサービスは異なっており、情報共有のハードルが異なる。SOC は同時に複数の顧客に対してサービスを提供するため、ある顧客で収集した情報を他の顧客へ共有することを前提としている。一方で IR は顧客に対して 1 対 1 でサービスを提供するため、情報共有が前提となっていない。
- SOC のみ、IR のみ、両方の契約といった契約内容によって、情報共有の在り方に影響がある。

（4） 海外の取組について

- （他の主要国においては） 訴訟リスクがあるため、国家機関への(任意の)情報共有は一切ない。ただし、一部の国では、かかる情報共有に関連するリスクに対する救済措置を講じ、国家から情報提供を求められる場合に、法的な不利益を被らないような措置を採っているところもある。加えて、新たに関係する組織から被害組織が訴訟を受ける可能性についてもシミュレーションを行っている。
- 国際間では、事案対処能力を有するアナリストや組織間で情報交換がなされる場合がある。例えば、被害組織への通知に係る能力の有無から仲介組織が選定され、選ばれた日本の組織が海外から連絡を受ける。情報交換というよりは何かしらの依頼事項があり、それに伴う情報として攻撃等に関する情報が提供されることがある。
- アメリカでは、MS(Multi-State)-ISAC と研究機関が成功事例集を公表している。特に注目しているのは、ISAC 間を跨ぐ情報連携がなされている点である。例えば、ある APT キャンペーンについて、関係のない ISAC がその兆候を発見し、外部専門機関や標的となった ISAC と連携することで、被害組織側で攻撃を認知できた事例が紹介されている。
- 一方で海外でも全てがうまくいっているわけではない。進んでいる取組として米国 CISA 法がとりあげられることがあるが、この法律が成立したからといって、海外のセキュリティベンダーが被害組織の技術情報をスムーズに渡すようにはなっていないと認識している。政策の専門家は、CISA 法の免責事項が不十分という旨の指摘をしている。
- SolarWinds の事案において、侵害を受けた司法省が CISA とうまく連携できていなかった点が指摘されている。事案が明らかになる一年前から複数のセキュリティベンダーは当該事象を発見していたため、専門組織間、又は官民での情報連携が如何に不足していた点が問題の本質ではないかとされている。

（5）情報共有枠組み（コミュニティ）における取組について

- (J-CSIP では、各組織が IPA との間で情報共有に対する NDA を締結しているところ)NDA があることによって情報提供のハードルが低くなっていると感じている。NDA 締結の際に発生する調整コストが大きいが、NDA がなければ情報共有の構築は難しかった可能性がある。
- 本検討会では、NDA が被害組織・インシデント対応組織外への情報共有を阻害していることが指摘されている。一方、情報共有枠組みにおいては、(J-CSIP における)NDA によってコミュニティ内の情報共有がスムーズになっている面はあると認識しており、例えば、NDA を締結していることによって、情報共有に係る組織内での稟議を省略できる。
- 先日公表された「サイバー攻撃被害に係る情報の共有・公表ガイダンス」が普及することで NDA がなくとも情報共有がスムーズに進むことを望む。どこまで実現するか、難しいところはあると思うが。
- 情報共有枠組みへの参加組織には自ら情報共有する内容や共有するタイミングをコントロールしたいという意向があるように感じている。今までの検討会での議論では、セキュリティベンダーが情報共有できるとよいとの指摘もあったが、各組織に意向があるならば、情報提供元自身がコントロールすることも重要と考えている。
- 情報共有の対象は、必ずしもインジケーター情報や有効なものである必要はないとしている。コミュニティの性質にもよるところ。
- 情報共有を行う際、あえて情報の正確性や網羅性を求めないこともある。コミュニティの方針や考え方によるが、正確性や網羅性が担保されないことを許容するルールや空気感により、共有可能な情報というものもある。

・ 情報共有と公表を同時に行った際、被害組織が特定されてしまうおそれがあるという点も、活動の中で実際の問題として認識している。「サイバー攻撃被害に係る情報の共有・公表ガイダンス」に記載された内容と日々感じている問題は非常に整合している。

お問合せ先
商務情報政策局 サイバーセキュリティ課
電話:03-3501-1253

以上