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3回）
議事要旨

1. 日時・場所

日時：令和5年6月26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、最高検察庁、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　佐々木政策担当部長

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）情報共有の対象となり得る情報

・情報を受け取る側が、どういった情報を集めたいのかという観点もある。

・共有する受け手側の組織で必要な情報というのをある程度すり合わせが必要。

・他方、そのような属性にあたらない情報も収集していかなければならない。難しいところではあるが、各レイヤー(ベンダー/政府レベル)で攻撃の属性を判断した上で、情報共有が必要となる。ユーザにとって判断は難しいが、メリットもある。一般的な攻撃に対する対処とAPTへの対処は異なるので、ユーザ自身が判断できると優先順位付けが可能となる。また、ベンダーへエスカレーションする際に、検体のみが共有されると時間を要する可能性があるが、属性判断ができるとこれを防げる。APT については政府による支援が重要。

・サイバー攻撃の被害に関する情報を抽象化すれば秘密にならない場合もあると考えられる。秘密性については加工前の情報をもとに考えるのではなく、加工後の情報それ自体から判断するのが通常と思われる。

・不正競争防止法上の非公知性の解釈としては、全体の情報を構成する一部に公開情報があっても非公知性は失われないとされている。サイバー攻撃に関する情報も様々なものが組み合わさっていると思うが、一部に公開情報があっても全体としての非公知性は失われないだろう。ただし一部のみを抜粋したものであれば、その部分のみで判断することはあり得るのではないか。

・守秘義務を負う者に対する秘密の開示と「漏えい」の関係については、例えば法令上の守秘義務を負う情報処理安全確保士間での情報共有も、秘密を知るものが秘密を知らない者に伝達した場合は、受領者に法令上の守秘義務が課されているとしても「漏えい」にあたるとも考えられる。ただ、守秘義務については様々な法令で定めがあるが、法令毎に考え方が異なり、上記の例では漏えいに当たらないと考えている法令もあるように思われ、必ずしも確立された見解はない。

・守秘義務と他の義務に基づく開示要請との関係性については、基本的には義務と義務の衝突（守秘義務と開示の

義務）であることが前提で、義務でないものはある程度劣後して考えざるを得ないのではないか。既存の判例では情報共有によるメリットとデメリットを比較衡量して判断することとなっている。

- セキュリティベンダによる契約の履行義務の中に対外的な情報共有も含まれるかというと、現状必ずしもそのように読み取れないことが多いのではないか。
- 米国の取組みとしては CISA 法 2015 があり、DHS(Department of Homeland Security、国土安全保障省)によりインジケータの自動共有を行う AIS(Automated Indicator Sharing)が開発及び整備されている。これとは別に、ICSCC(Intelligence Community Security Coordination Center)が IoC(Indicators of Compromise、侵害の痕跡)やマルウェアに関する情報等を含む脅威情報の共有を強化するツールである ICOAST(Intelligence Community Analysis and Signature Tool)も整備され、Unclassified(非機密)情報の共有ツール ICOAST-U も運用されているが、AIS との関係がやや不明確である。
- ICOAST はメンバー間のコミュニケーションツールを使ってメンバー間での情報共有を実施しており、IPA ICS-CoE でも機密度に応じた情報共有が出来る形の SNS が使われている。AIS は情報を自動的に共有する形をとっており、個人情報取扱の懸念もあり、効果的に活用できていない。
- CISA 法において脅威情報である CTI（Cyber Threat Indicators）が定義されている。セキュリティ制御を破ることや脆弱性を攻撃する方法、C2 サーバに関する情報、サイバーセキュリティ脅威のその他の属性(アトリビューション情報等)が例示されている。
- NDA では秘密情報の定義と秘密保持義務が示される。秘密保持義務違反にならないためには NDA 自体を変更して締結することが望ましいが、それが難しい場合には、右記の 2 点を検討する必要がある。1）秘密情報に該当しないか、2）秘密保持義務の例外又は秘密保持義務違反であっても違法性阻却事由に該当するか。
- 秘密情報について、被害組織に関する情報が全く含まれていない攻撃情報(脅威指標)と被害情報を明確に分け、攻撃情報は秘密情報に該当しないと解釈できないか。また、被害情報から被害組織に関する情報を匿名化すれば秘密情報に該当しないと解釈できないか。さらに、匿名化するガイドラインを経産省から示せないか。
- サイバー攻撃を受けた場合等、個人情報保護法における合理的努力は外部機関による調査を含むと解釈されるのが一般的であるところ、外部機関による調査報告書を受領した個人情報保護委員会が、攻撃情報や被害情報を匿名化してサイバーセキュリティ協議会等に共有することはできないか。
- 個別契約と NDA が別々に締結されている場合、個別契約が優先される条項があれば NDA 違反にあたらないと解釈され得る余地があるのではないか。また、特定条件下では秘密保持義務違反の違法性が阻却されることとできないか。
- 十分な匿名化が行われていれば被害組織の不利益にならないと考えられ、免責されるとできないか。

（2）情報共有の目指すべき在り方

- 早期警戒ということであればベンダーや ISAC の方が情報は早いと思う。
- 被害組織が被害情報を全て共有しているとも言えない実態がある。対象が自社の技術情報等であれば社内のみで対応するということもあるし、中小企業では機器のリセットのみとする場合もあると思う。ここにも課題があると思われる。
- 一般企業が参加するセキュリティコミュニティでも被害情報共有の取決めを作成し、軽微なものでも情報発信することで、有益なレスポンスがもらえる状況がつくれるかもしれない。
- どうしたら相談元に対して有益な情報を共有できるかという視点で IR ベンダーは検討を進めることが必要である。同種事案について解決済み(もしくは対応中)の他の IR ベンダーに対して情報共有ができるとよい。
- 情報共有の仕組みがしっかりした形で行なわれることが担保されるのであれば、その枠組に参加しているセキュリティベンダへセキュリティ業務を依頼するほうがよいと考えているユーザ側企業の意見もある。情報共有がしっかり守られた形で行われ、ユーザ側の意識が変わってくると、情報共有の枠組に入っていないベンダーは選ばれなくなる。

（3）情報共有メリット

・共有が任意の場合には、メリットがあるべき。
・報告・届出機関への報告のメリットは現状不明確であり、その点を明確にすることで報告等がさらに促進されるだろう。
・被害を公表するメリットとあえて出さないメリットについて、現状では情報を出さないメリットが大きいのではないか。被害に遭うことが悪いことであるという世間的な見られ方があるように思う。本来は被害側にいわれはないのだが、世間的にはいじめられる側に原因があると捉えられがちである。自社のメリットにならないと共有があまり進まないかもしれない。しっかりと皆で取組みを進めていくことが是であり、それでみんながメリットを享受できるという公益的な面で整理をして、現状と比較していく必要があるのではないか。
・公表の大切さを伝えていくことに加え、国として共有によるメリットの文化を醸成していく必要がある。
・ここまでやっていたがやられた、もしくはやられた後にこういう対応をしたなどを企業側がわかりやすく示し、政府がそれを認めてあげることが重要。そのためには基準があるとよい。
・情報を共有することで利益と不利益のどちらが重いか、データを提供することで"何かしらの"フィードバックが得られる（得られる可能性がある）、というようなことを示すことで、情報共有のフレームワークがうまく回るのではないか。
・情報共有によって、初動対応の参考となる情報(例：類似の攻撃情報を得ることによる被害拡大防止、他組織の顧客対応の仕方)を入手できるのではないか。専門組織間での情報共有によるマルウェアのパターンファイル作成までの迅速化等にもつながるのではないかと期待。
・他方、共有された情報が SNS で拡散されたり、報道されたりすることも考えられる。その結果、被害組織自身による公表前に被害組織が特定されると、隠蔽を疑われることも考えられる。また、攻撃者が窃取し、ダークウェブに掲載した情報が、情報共有により拡散するなどにより被害が拡大し得る点も懸念される。

○今後の論点

（4）官民連携

・努力をさせる相手が民間だけになっていて、政府による努力が示されていないのではないか。是非とも政府間で行われるべき責任についても議論すべき。
・情報の質の変化が起きており、一企業では判断しようがないものが出てきている。（ディープフェイク映像、SNS 上での顧客個人情報取扱による漏えいの可能性、国際関係等）
・官民で定期的な情報交換を行い、信頼関係を醸成していけないか。例えば、産業横断サイバーセキュリティ検討会においては、経営者だけでセキュリティの討議を行っているが、官民で行ってはどうか。
・官民の役割分担として、企業は企業ネットワーク・セキュリティ対策の可視化が求められる。予防のためのインテリジェンスにおいて、一企業だけでは判断し得ないものの共有・問い合わせができるとありがたい。情報は、①経営者②実務責任者③実務担当者にレベル分けされているとよい。最低限②に情報が集まるようにする。（セキュリティ統括室の設置）
・政府に集まった情報は匿名化して開示願いたい。
・MI6 や NSA と同様の機能、実質的な活動が必要ではないか。（日本のインターネットの出入り口の監視など）
・日本版情報分析組織の育成が必要である。
・情報の収集や共有において最終的に何を目的として、そのためのどのような方法で情報を使うかをはっきりさせる必要があり、議論が必要。匿名化の適切性を誰が判断するか、そのコストを誰が払うかという議論が整理されないと、仕組みとして実効的に機能しないおそれがある。
・法人等の企業に対する攻撃情報の匿名化は、自然人よりも母数が少ないといった事情から、抽象化しても一意に特定されやすい側面があり、個人情報の匿名化よりも判断が難しい。
・被害組織に関するものが含まれた情報の匿名化は、民間セキュリティベンダが責任を負いつつ処理を行うとするのではなく、NISC や JPCERT/CC が匿名化を行い、責任も負うとするのがよいのではないか。

・必要なところに対して同時に情報が届く仕組みが重要であり、その場合は情報のフォーマットも必要になる。時間経過で埋まっていく情報もあるので、事前に順序等について検討するのもよいだろう。フォーマットに関しては、経営ガイドラインの付録Cを活用いただきたい。
・アウトプットに関してもバラバラに出すのではなく一本化が必要なのではないか。見る側からするとバラバラに出されるのは情報収集負荷が高い。また、その情報を広めるためにもメディアリレーションも必要。
・被害組織がどこに情報を共有すべきか方針を緊急時の対応マニュアルに明記し、訓練しておくことは有益。
・諸外国において実施されている、右記の3つの点を日本においても確保していくことが重要。1)政府側の責任の所在の明記、2)企業に対する明確なメッセージの発出、3)デジタルフォレンジック等のセキュリティ専門業者に対しての政府による定期的なレビュー。デジタルフォレンジックを行う業者を登録・維持する仕組みが必要となると考えられるため、既存の経産省の仕組み（情報セキュリティサービス審査登録制度）を利活用いただきたい。

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