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4回）
議事要旨

1. 日時・場所

日時：令和5年7月21日（金） 15時00分～17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　武尾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

4. 議事内容

事務局より資料１の説明を行った。続いて、以下のとおり自由討議を行った。

（1）情報共有の対象となり得る情報

- 事務局資料 P.12-14 について、被害を受けた企業の立場からすると、被害組織に固有の情報が含まれないことを担保することが重要である。誰がそれを判断するか、匿名化をどこまでするかなど、難しいところがある。仮に固有の情報が含まれていたとしても、不利益を被りにくい状況をどのように作るかが重要ではないか。

（2）情報共有の目指すべき在り方

- 本会では比較的詳細な議論がなされており、被害を受ける立場とセキュリティ事業者、情報を受ける行政機関などが関係するが、そこの整理が本会のミッションのひとつと理解。
- 専門組織と被害組織の情報連携については、両者間で対話・合意しながら進めていくことが必要と認識している。
- 情報を受けとる側が一定程度決まっていないと情報を共有しづらいという印象を受けた。
- 共有する組織のレベル感、共有された情報をどう活用するのかを合わせて示す必要があるのではないか。
- 情報共有したい/しなければならない/共有されたいのは誰かという整理が必要となる。情報共有を行う責務が誰にあるのかがわからなくなっている。そこが曖昧では情報を共有しにくいのではないか。負担を減らすという話と情報を出しやすくしてもらうという話は論点としては別で議論する必要がある。
- 大枠として共有できるという方向へ意識を変えなければ情報は流れない。複数機関の連携が必要となる児童虐待の防止の例では、被害情報は機微な個人情報となるため、情報共有がなされず、悲劇が防げなかった。そのため、児童虐待防止法ではポジティブリストを出していて、ただし書を示している。一方でサイバーセキュリティにはそのような仕組みがない。被害組織とセキュリティ企業の関係について提言を出していくことも目的の一つではないか。
- 要求されたデータを提出する際に法令に基づく根拠が必要となる。委託業者がデータを提出した際に刑事・民事訴訟の違法性の阻却をどう担保するかが非常に重要となる。
- 匿名化等を適切に行った上で、知りたい人の多くが情報を知ることができる仕組みの構築についても視野に入れていただきたい。

（3）情報共有メリット

- 情報を公開したほうが、メディアに対してリリースを参照するように伝えられるため、対応コストの軽減につながるという考え方について周知していくべきではないか。
- ユーザ企業は、他社でセキュリティ事案が起こった際に、仮にその攻撃が自社で発生した場合の業務影響を必要な都度、報告している。経営者は自社への影響を気にすることが多いため、どのようなシステムが攻撃されたのか、どのように対処したのか、などの情報を共有する枠組みがあれば、我々も積極的に参加したい。

（4）今後の論点

- 脅威が激しくなっている点は共通認識だと思うので、それを踏まえたミッションステートメントを示すべきではないか。
- 金融庁が所管する開示制度(非財務情報のサステナビリティ情報の開示制度)の改正でサイバーセキュリティがこのサステナビリティ情報に含まれるとされている。また、米国証券取引委員会(SEC)においても、サイバーセキュリティ事案が生じた際の速やかな情報開示が議論されており、開示に関する検討は金融庁を巻き込み行うべきである。総務省の「サイバーセキュリティタスクフォース」の「情報開示分科会」でも類似の検討があり、連携が必要ではないか。
- 今後の論点部分の官民連携について、警察庁の検討会も開催されており、ひな形を作る動きもある。サイバーに関する機関も取り組むことが重要。
- 被害に係る情報を被害組織が公表せずとも公になる場合があるが、公にならない可能性を期待して被害情報を公表しない被害組織は存在する。十分なセキュリティ体制であるといえなければ、公表するメリットはほとんどないため、開示義務の設定等をしなければ難しいのではないか。
- 自社への事業被害が大きいインシデントについて経営者は認識すると考えられるが、APT 事案は事業への即座の影響がなく事業被害も小さいため、経営者が認識しないケースがある。
- 被害組織にはインシデントを報告するインセンティブが少ない。被害が軽微なものであれば、当事者レベルで判断してしまい、インシデントを報告しないケースも見受けられる。また、経営層へエスカレーションされても、公的機関などへの共有は必要ないという判断となることもある。このような事象に対してどのように対応するかは検討が必要となる。既知のインシデントと似たものであれば、一つのものをきっかけにして対応するということもあるが、APT事案についてはそれが難しい側面もある。
- 自分が被害に遭うという観点だけでなく、周りが被害を受けないという社会的な観点を醸成することについて、別の会議体での議論等にも期待したい。情報が広く共有されるようになってから、それを効率的に実施する方法等について本会等で検討していくのかなと思う。
- RFP にて、ある情報共有の枠組に入ってないセキュリティベンダとは契約しないと書いてもらうことが目指す先ではないか。

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