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1回)
議事要旨

1. 日時・場所

日時:令和5年5月15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、北条委員、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、
一般社団法人 日本経済団体連合会

経済産業省:大臣官房 上村サイバーセキュリティ・情報化審議官、
商務情報政策局 奥田サイバーセキュリティ課長

3. 配布資料

資料1-1 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について

資料1-2 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 運営要領(案)

資料2-1 事務局説明資料

資料2-2 JPCERT／CC 説明資料

4. 議事内容

開会にあたり、上村サイバーセキュリティ・情報化審議官より挨拶があった。

続いて、本検討会の星座長より挨拶があった。

次に、本日の議題に入り、事務局より資料2-1及び資料2-2の説明に続いて、自由討議を行った。

(1) 脅威情報について

- 「公知」の解釈をどう考えるのか。脅威情報は公知として扱えるという観点がある一方、それが自社と結びついた時には公表しにくいという観点もある。公知かどうかの判断はつきにくいので、どこかが判断する必要がある。今後は解像度を上げて議論する必要があると思う。
- NDA では自分が保有していないデータを他社から受領した場合に秘密として扱うが、既に保有しているならば秘密にはならないという観点もある。なお、相手から受領したものは全て秘密情報になるケースもある一方、相手から「これは秘密です」と言われたもののみが秘密情報として取り扱われるケースもあるなど、秘密情報に該当するか否かがまちまちであり、その点も契約の文言によって変わり得る。
- 情報のオーナーが誰なのか、という点についても議論が必要。被害を受けた会社もオーナーとなり得るが、SOC 側で分析し、匿名化した場合は SOC 事業者がオーナーとなる場合もあり、さらに公的

機関がオーナーになる場合もあると思われる。資料を拝見したところ、そのあたりの整理が十分になされていないように思う。

- データオーナーが誰かという指摘は重要だが、定まった法則があるわけではない。結局は契約によるところが主であり、経産省の「AI・データの利用に関する 契約ガイドライン」の中にもデータオーナーの記載があるので、そこが出発点になる。ただし、契約内容によってオーナーは変わり得るので、個別の検討が必要となる。
- 今回取扱う「サイバー脅威情報」はレベルに応じて区別があると思うので、先ずは整理が必要ではないか。SOC は顧客から許可を得て監視しているが、そこから得る情報としては、1. 攻撃に係る痕跡(脅威データ)、2. 脅威データを整理・解析し、攻撃に使われた IP アドレスやハッシュタグ等を仕分けしたもの(脅威情報(脅威インフォメーション))、3. これらを更に文脈に応じて評価分析して活用できるようにしたもの(脅威インテリジェンス)等の 3 段階に分かれると理解している。
- 先ず、各々の組織で共有したい情報に差異があるのではないか。最低限のものについて共通認識を検討し、整理するのが良いと思う。窓口やフォーマットを一本化したとしても、結局事業者にとっては得たい情報を得られることが重要と考える。

(2) 情報共有について

- 予防という観点からの情報収集が重要ではないかと感じている。現状は有志、ISAC と連携しながら実施しているが、攻撃トレンドの変化がもたらし得る影響に係る情報について、官民連携を通じ、分析ができないか。
- 一般企業が欲しい情報である、自社の脆弱性や事業継続のために必要な情報が重要であると認識しており、その仕組みを国でどう整備するか。今は有志で推進しているが、もう少し戦略的なレベルで取り組む必要があるのではないか。
- 経営判断に資する情報の分析、広い意味でのインテリジェンス、例えばどのような背景があり、いかなるキャンペーンがあるかなどは特定のベンダーだけでなく、政府と協力して取り組む必要がある。
- 既に情報共有されているものでもうまくいっているところとそうでないものがある。現在の枠組で共有されていないものと区別して議論することが必要。
- 被害組織側のコストは、報告を求められるから生じる。
- 被害組織等が情報を共有することにデメリットがない旨の説明が必要。また、セキュリティ上の理由で回答できないという状況を変えていく必要がある。
- 政府に情報提供することにやや抵抗がある。組織の経営層が状況を理解し、政府に対して報告するメリットを明確化することが必要である。
- 事務局資料2ページ目に記載の目的①～④は被害組織にとってもメリットになるが、⑤～⑥は公的機関のメリットが中心。問題①のような点はこれらを認識すれば解消されるのではないかと思う。情報共有のメリット・デメリットの掘り下げなどがもう少し必要。
- 中小企業で監視もしていないところでは、経営者が被害を認めたくないという場合がある。そこでは情報共有が進まないことも想定されることから、情報が活かされるということ、及びメリットを広報しなければ仕組みが回らないと思う。

- 警察組織に相談しているという理由で共有しないという事態に対しては、被害組織にメリットの大きい方法を探っていく必要がある。
- SOC 事業者の競争力につながるものは外部へは提供できないので、そのあたりは分けて議論できればと思う。
- 被害組織側だけでなく、セキュリティベンダー側の意識改革も必要。被害組織の情報を自社にため込み、外部に出さないという組織も出てくると思う。国内ベンダーA と海外ベンダーB との間で NDA の内容が異なる場合に、外部への情報共有を行わない海外ベンダーB に顧客が流れる懸念もある。
- 被害組織の取組について、個人情報保護委員会のガイドライン及び報告様式では合理的努力として外部への調査委託が必要と読めることもあり、セキュリティベンダーに情報が集まっていると思われる。セキュリティベンダーがどう情報を提供するかについて、規制又は自助努力にするのかは検討の余地がある。
- セキュリティベンダーが他社と情報共有したいというのは語弊があるが、APT の被害はセキュリティベンダー以外誰も把握していない状況が良いのかという思いはある。1 被害組織の問題ではなく、政府や国の問題となる。これをどのように活かしていくのかを議論するのが重要。

（3）各組織における情報の扱い

- 組織によっては、契約に明文化して、被害組織の情報を公共の利益、研究等、その後の施策に広く利用している場合があり、OSINT で得られたものは公開情報として扱う一方、機微な情報を含む被害情報は秘密情報として扱っているところもある。今後このような点についても考慮していく必要がある。
- セキュリティベンダーでは、フォレンジックに係るところは情報をほとんど出さない。一方で、SOC サービスをしているところは共有も行う。社内でもフォレンジックから SOC などに情報共有はされないという認識。顧客にもそのあたりをはっきりさせないと、誤解を招く恐れがある。
- サイバー脅威情報を扱うに当たってのプロセスが記載されていない。これらは具体的な意思決定やアクションに繋がるものであり、また情報の収集、分析、アクションの検討、オペレーション体制の整備等を含む攻撃情報取扱いのプロセスについても、それぞれのフェーズで異なる課題があることから、整理が必要。

（4）その他

- 資料中に海外のベストプラクティスなどの記載がない点が特に気になるところであり、ハブとなって情報共有する組織や責任の所在も明示されていない。インシデントレスポンスの情報を扱う際、一部の主要国では、国家の責任が問われる。
- 海外で実施されるカンファレンスでは、発言を録音せず、厳しい秘密保持契約を結ぶなどの措置を講じたうえで、信頼をベースに情報共有がなされるという点についても考慮するべき。

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