サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会（第 2 回）

議事概要

■ 日時

令和 4 年 6 月 20 日（月）16：30～18：30

■ 場所

オンライン開催

■ 出席者（敬称略）

（委員）　新井　悠　　株式会社 NTT データ エグゼクティブ・セキュリティ・アナリスト

板橋　功　　一般財団法人日本サイバー犯罪対策センター（JC3）
シニアセキュリティフェロー

勝村　幸博　株式会社日経 BP　日経 NETWORK 編集長

武智　洋　　サプライチェーンサイバーセキュリティコンソーシアム（SC3）
運営委員

辻　伸弘　　SB テクノロジー株式会社 プリンシパルセキュリティリサーチャー

蔦　大輔　　森・濱田松本法律事務所 弁護士

花岡　圭心　三菱電機株式会社 情報セキュリティ統括室 セキュリティ技術部長

北條　孝佳　西村あさひ法律事務所 弁護士

星　周一郎　東京都立大学法学部 教授

松坂　志　　独立行政法人情報処理推進機構（IPA）
セキュリティセンター セキュリティ対策推進部
標的型攻撃対策グループ グループリーダー

山岡　裕明　八雲法律事務所 弁護士

吉岡　克成　横浜国立大学大学院環境情報研究院／先端科学高等研究院 准教授

若江　雅子　株式会社読売新聞東京本社 編集委員

（事務局）警察庁、総務省、経済産業省、サイバーセキュリティ協議会事務局（内閣官房内閣サイバーセキュリティセンター、政令指定法人 JPCERT コーディネーションセンター）

（オブザーバー）国家安全保障局

■ 配付資料

資料 1-1 サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会委員名簿

資料 1-2 第 1 回検討会での主なご意見

資料 2-1 サイバーセキュリティインシデント発生時の報告制度等

資料 2-2 警察活動から見た通報・相談の重要性について

資料 2-3 行政機関から見た情報共有への期待

資料 2-4 第 1 回検討会での議論に関連する論点の振り返り

■ 議事概要：

（1）事務局より配付資料確認、事務的事項の説明の後、星座長より議事進行について説明があった。

（2）第 1 回会合の主な議論の紹介

事務局より、第 1 回会合での主な議論の確認があった。

（3）サイバー攻撃被害に係る情報の共有・公表ガイダンスの論点整理

蔦委員より、資料 2-1「サイバーセキュリティインシデント発生時の報告制度等」、大橋警察庁サイバー警察局サイバー企画課長より、資料 2-2「警察活動から見た通報・相談の重要性について」、扇 NISC 基本戦略第 2 グループ企画官より、資料 2-3「行政機関から見た情報共有への期待」の説明。最後に事務局より、資料 2-4 に基づき第 1 回検討会における議論の論点を振り返っての説明があった。

（4）議論

（武智委員）

- 共有・公表というものは、何らの指標もないと、非常に量が多くなってしまうので、現場での考慮要素のようなものが示されれば助かると思っている。

（勝村委員）

- 警察への通報・被害提出は、強固な「アリバイ」になると思う。ガイダンスには、どこに、どのような形で、どう報告するのかを明記し、それが間違いなく捜査や相談につながるものになればよいと思う。
- 行政機関から注意喚起が出ると、記事にしやすい（読者に呼びかけやすい）ので、重要な対策については、積極的に発信してほしい。

（辻委員）

- 法執行機関と、被害組織（事故対応を行う組織）とで、優先順位は全く異なる。被害組織には、警察に協力するメリットや、アトリビューションは何のためにするのかがあまり伝わっていない。どういう活動をしているか、啓発する動きも必要と思う。
- また「窓口多過ぎ問題」があり、被害情報をどこに共有すればいいのか迷う。受ける側の仕組みも大事であり、情報が縦割りの弊害にさらされることがないよう、窓口の一本化が望ましい。もっとも、簡単な話ではないし、そもそもガイダンスのスコープの話ではないかもしれない。

（板橋委員）

- 通報は、サイバー犯罪においては基本であり重要なので、相談者の安全・安心のためにもガイダンスには盛り込むべきである。ただ、その対応の体制は十分ではなく、通報・相談をした場合のメリット・デメリット等も不明確に感じられる。その辺を明確にし、どのレベルでも同じ対応ができるようにすることがのぞましい。
- サイバー警察局、サイバー特別捜査隊が発足したが、この体制の強化と、何ができるかの丁寧な説明が必要と思う。

（北條委員）

- 警察に被害を届け出ると、被害情報の取扱いに制約が課されたり、勝手に公表されたりするのではないかとの懸念をもつ企業の人はいると思う。ガイダンスには、警察の対応と、併せて、被害組織の承諾なく警察が公表することはないことが記載されれば良いと思う。
- 自身の経験を言えば、これまで十社以上、警察に相談に行ったが、警察が勝手に公表したり、企業が公表することを警察に止められたりした例はない。

（警察庁大橋サイバー企画課長）

- サイバー事案に関する通報・相談への警察の対応について、過去の対応等からご指摘をいただくことがあるが、体制面を含めた対処能力が決して十分とは言えない面もあったと認識している。通報・相談を適切に扱える体制を整えることは大変重要な課題であり、現在、サイバー部門のみならず、部門を問わず警察官全体の対処能力強化に取り組むなど、必要な取組

を推進しているところである。トラブルに巻き込まれて不安に感じている被害者が警察に安心して相談・通報できる環境を整えていきたい。

- 警察に被害を届け出ると、被害情報の取扱いに制約が課されたり、勝手に公表されたりするのではないかとの懸念を持たれているとの指摘については、個別の事例を把握しているわけではないが、一般論で申し上げると、個別事案の性質等を踏まえると適切な情報の取扱いが求められるようなものもあり得ると認識している。本ガイダンスにおいて警察としての基本的な考え方等を示し、御理解をいただくことで被害組織と被害情報の取扱いに関して話し合いができる素地を作っていきたいと考える。
- パブリック・アトリビューションの目的等が十分に伝わっていないとのご指摘があったが、様々な事情で犯人の検挙が困難である場合には、抑止効果を狙ったパブリック・アトリビューション等につなげていくことが有効に働くケースがあると認識している。パブリック・アトリビューションありきで捜査をするものではない。

（山岡委員）

- 実際の現場では、公表に際して、独自の体裁で記載して必要以上に目立つことを避けるべく、他社の同種事案に表現の内容や方法をなるべく合わせるなどをしている。その観点から、共有・公表の粒度がガイダンスから分かれば有益である。また、警察に報告するときには、攻撃に使われた国内 IP アドレスの情報を提供すれば、攻撃者の特定には至らないものの、少なくとも攻撃ルートをつぶすことにはつながる。

（花岡委員）

- 自社で経験した「共有」と「公表」の主な課題を述べる。まず共有に関しては、ギブ&テイクの考え方から IoC･TTP 関係情報は複数機関に共有しているが、これで困ったことがあった。1 つ目は、ソフトウェアメーカー、ベンダ、サービス事業者の意思に委ねざるを得ず、弊社が勝手に共有するわけにいかないことである。2 つ目は、共有した情報がメディアに流出してしまうことである。3 つ目は、仕入先でインシデントが発生し、弊社にとってもかなり重要であるにも拘わらず共有できないと言われることである。協議の末、最終的には教えてもらえたが、苦労する。
- 公表に関しては、経産省告示の内容に従って行うが、基本的には特定の客先への報告で済むものは公表しない。昨年、事業部が先に客に報告に行ってしまうという例外が起き、経産省

と相談しつつ、結局は公表に踏み切った。法律や、不特定多数の人へのインパクトにより公表することもある。公表は、基本的に影響と再発防止がポイントになる。公表の際の数値カウント方法やケース分けも苦労する。

（蔦委員）

- 窓口一本化の件については、かつて私が NISC でサイバーセキュリティ協議会をつくるための法改正を担当した際も同じ課題が出ていた。情報共有体制を統合する、または窓口の一本化ができないか検討したが、それぞれの体制で求める情報、タイミングが異なっており、一緒にするのは難しかった。前回（2018 年）のサイバーセキュリティ戦略の策定過程においてもその種の議論はしたし、一本化するという方向性については異論はないし目指すべきと思うが、完全なる一本化は難しいと思う。
- 運用保守ベンダは、情報共有が守秘義務違反になるのではないかという懸念も抱いているので、このガイダンスの検討は有効な解決策になりうるのではないかと思っている。

（新井委員）

- 過去勤務していた経験から申し上げると、セキュリティベンダがインシデントレスポンスの情報を商売にすることは、昔はあったかもしれない。しかし、今は、IoC の周知、ブログ等での啓発活動が、セキュリティベンダの社会的な貢献を示す手段となっており、情報共有にポジティブなのではないかと思う。セキュリティベンダのマインドとして、商売のタネだから情報共有にネガティブということは無いと思う。
- 何を共有すればよいか迷うこともあろうと思うので、ガイダンスには、共有・報告する情報、IoC としてマルウェアのファイルのハッシュ値や IP アドレスを例として提示すると良いと思う。

（松坂委員）

- 実態は明確ではないが、C&C サーバの IP アドレスや URL を持って警察に相談すると、別の企業との情報共有を止められたと相談を受けたことがある。犯人しか知り得ない情報なのでそのままにしておくということらしいが、そういう恐れがあると、しり込みする可能性はある。警察に相談する時点で、「既に IPA に情報を渡している」という順序であれば角は立たないので、順序を工夫しているという組織もあった。

・ インシデントは、どのレベルのものを監督官庁や NISC に報告すべきか。非常に細かい事象でも大事な情報の場合もあるので、受ける側のキャパシティの問題だと思う。この機会に、その相場感、温度感がどの程度のものかが分かると良い。

（吉岡委員）

・ 情報共有の話は全体像がつかみにくい。共有する先もさまざまあり、ほしがるものも異なるのだろう。また共有活動に参加していない組織を入れ込むには、モデルケースが示され、まず自組織がどういう属性を持ち、どういう共有があるのかといった全体像がわかることが必要だ。情報を使う側はあれもこれも共有したいということだろうが、提供する側はそれがどこまでどう派生するかがわからないとやりにくい。それらがわかりやすくまとまったガイダンスがあるといいと思う。

（若江委員）

・ 今回の情報共有の枠組みは任意であり、被害企業にとって共有がメリットと感じられるものでなければ進まない。ガイダンスには共有すればどんなメリットがあるのか、はっきり書くことが必要。そのためにも、例えば、辻委員の言われた、1 つの窓口に言えば一度で、共有が必要なほかの組織にも共有される、、あるいは情報提供側で共有先をコントロールできるなど、提供を受ける側の体制整備が欠かせないと感じる。

（星座長）

・ 連絡窓口の明確化、公表はどういう形でするのか、共有・公表のメリットは何か、受ける側はどの程度のインシデントなら報告を求めるか。また、被害組織が持つ情報の重要度を的確にわかっていない問題もある。
・ 第 3 回はガイダンスの骨子案に着手し、それに基づく議論を予定していたが、もう少し踏み込んだ議論をしてからのほうがいいのか、検討したい。この件は、事務局に意見を寄せてほしい。