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3回会合

議事概要

■ 日時

令和4年8月1日（月）17：00～19：00

■ 場所

Web会議形式での開催

■ 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
兼　公共セキュリティ部　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）内閣府（サイバーセキュリティ・情報化推進室）、国家安全保障局、総務省（大臣官房）

■ 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　共有・公表ガイダンス検討に向けた各ポイントについて

■　議事概要

（１）事務局より配布資料確認、事務的事項の説明の後、星座長より前回会合の振り返りと今回会合の議論の進め方についての説明があった。

（２）共有・公表ガイダンス検討に向けた各ポイントについて

事務局より、資料 1-2 に基づき、共有・公表ガイダンス検討に向けた各ポイントについて資料に沿っての説明と、事前に委員から寄せられた意見についての簡単な紹介がされた。

（３）議論

（辻委員）

- 自ら公表できなくとも、何故やられたのか等、初期侵入の方法が共有されるのは非常に有益。脆弱性、細かい技術情報については中々言いづらいが、実態を世に知らしめるためには、それも非常に大事なポイントと思う。プレスリリース文に、専門組織に共有済みです、と書ければ、被害組織にとってもメリットになる。
- 注意喚起、早期警戒の意味での共有・公表は、その都度とは言わないまでも頻度多く行われるとよい。
- 被害組織に、共有した方が世の中のためになるということを浸透させないといけないと思う。SNS でインシデントに言及するのは、憶測を否定する目的もある。早めに言っておくのは、そういう意味でも意義がある。

（新井委員）

- どんな情報を共有すればいいか、特に技術的な点の明記は、共有元にとっての目安になる。

（松坂委員）

- 共有に実名／匿名があり、公表にも実名／匿名（代理的）があるのではないか。用語の整理が必要であると思う。
- 他企業がこの IoC 情報で助かるかもしれないという状況で、秘密保持を破ることができるか。それを当事者となった情確士が判断するのは難しい。

（吉岡委員）

- アカデミアの世界でも、発見したセキュリティ問題を論文で発表する場合にどうするべきかについて「サイバーセキュリティ研究倫理」として長く議論されている。当該議論において、「どのようなケースで公表をすべきである／すべきでない」ということを個別にガイドラインで示すのは難しいという点は、世界の多くの研究者のコンセンサスが得られている。

（勝村委員）

- 情報共有活動の類型は、既存のフレームワークを使えるハブ・スポーク型が望ましい。信頼できる組織がハブになれば、情報を変に扱われることがないという安心感を担保できる。
- 概念として、被害組織以外による公表は、公表と呼ぶのだろうか。別の組織が起きていることを匿名で伝えるのが公表なのかどうかは疑問に思う。
- リークには、情報リテラシーが甘くてリークしてしまうケースもあれば、これをなぜ公表しないのかといった義憤からのリークもある。ガイドラインに従って情報共有をしているが、利害関係者との調整に手間取っているだけだ、と示すことで、リークを防ぐこともできるのではないか。

（武智委員）

- 共有、報告、公表などの用語の定義・属性を明確にしないと行けないと思う。
- SOC 等のセキュリティベンダとユーザーとの NDA により、出せる情報・出せない情報があろうかと思う。また、中小企業等では、セキュリティベンダではなく情確士が直接ユーザー企業で作業をすることがある。情確士には秘密保持義務もあるので、悩ましいかもしれない。

（北條委員）

・ NDA については、実際にどういう役割を果たし、いかなる障壁になっているのか、現場の実態が判明しているとはいえない。自分の感覚では、NDA が情報共有の障壁になっているようには感じていない。

（若江委員）

・ サイバーインシデントの報道ぶりを批判する内容となっているが、最近ではリークサイト等の名を出さず、URL もなるべく分からないようにするなど配慮する報道もあることに留意が必要だ。情報が社会で共有されることの意義を否定することがないよう、ガイダンスの書きぶりには配慮が必要だと思う。また、ガイダンスにおいて、被害公表の際に情報を具体的に書きすぎると危険な場合がある（例：脆弱性情報、ゼロデイ攻撃）等の留意点の提示は出来ると思うが、公表の必要性はケース・バイ・ケースで生じうるので、「必要がない場合」を限定列挙で書くことは難しいのではないか。

（板橋委員）

・ 特に企業情報の場合は、共有した情報が漏えいするとイメージダウンにつながる可能性がある。共有情報と公開情報は明らかに異なる。

（蔦委員）

・ 秘密保持契約は、契約書の定め方により秘密の範囲や例外が異なる。守秘義務的な条項の条文は、相手方の承諾があるなら出してもいいというのが大半だと思う。
・ 公表に関しては、ガイダンスでタイミングを選ぶメリットを含め、公表を行うことの意義や留意点を示したうえで各組織の判断に委ねることになるのではないか。公表が必要である、公表しなくていい、という促すようなニュアンスを避けるということだと思う。ただ例外的にリークサイトの情報掲載・転載は、犯罪者への加担、リークサイトの宣伝になり得るので控えたほうがいい。問題状況は当然異なるが、情報の拡散によって被害が拡大するという意味では、いわゆる漫画村問題に似ている要素もある。

（花岡委員）

・ 想定読者はガイドラインを参照しつつ対応を考えるので、その被害組織の誰がどういう立場で担当するのかを明確にしたほうがいい。サービス事業者の管轄で被害組織がどうにもでき

ないケースもあるし、ソフトウェアメーカーは知っていても、こちらから先には言えないという場合もある。

- 企業にとって被害公表は大ごとなので、ケースに応じての要否をガイドできればベターである。組織の責任者の判断に役立つ記載があると、現場からの説明が速くなる。

（山岡委員）

- 例えば、自社がマルウェアの Emotet に感染したため、自社になりすましたメールが契機となって、取引先にも被害が出るという事案においては、早期に公表して注意喚起することにより取引先の二次被害を防止することができる。また、仮に取引先に二次被害が発生し、その対応に要した費用について賠償責任を追及された場合、自社の被害を早期に公表していれば、取引先に対して「注意喚起を見て何らかの予防措置はとれたはずだ」ということで過失相殺を主張し、自社の責任軽減に繋げることも可能である。実際、このように主張することで取引先からの責任追及の度合いが弱まったことがある。このように、早期の公表は、二次被害防止に加え法的責任の軽減の観点からも効果があると思っている。

（星座長）

- 公表は、実名だからこそインパクトがあり注意喚起にもなるが、デメリットもある。盾の両面のようなところがあり、だから公表しなくていいとはならないが、難しい問題である。

（事務局コメント）

- インシデント対応を初めて行う、あるいは今後の事案に備えたいという想定読者には、ハブ・スポーク型以外の形態はかなりハードルが高いのではないか。専門組織等に情報伝達を頼み、フィードバックをもらうという場合もある。そういう案内をしたい。
- 被害者が匿名化され、ハブとなる組織が技術的情報だけを共有することは日々行われているので、それについては紹介の必要があると思う。
- 専門組織が、公開のレポートを通じ、注意喚起的な意味で技術的な分析結果を出すことは度々行われているが、被害組織が実名で行う公表とは性質が異なるとの指摘は、そのとおりかもしれない。
- 共有・公表の語をはじめ、用語に関しては、少なくともこのガイダンスにおいてはどういう意味で使っているか、示していきたい。

- NDA に関しては、条項自体がハードルになっているケース、またそれを言い訳に情報を外部の活動等に出さないケースがありうる。NDA のあり方まで記載するのはガイダンスのスコープを超えるが、情報の取り扱いを、ガイダンスを通じて説明する必要はある。
- 対象の情報において何が秘密なのかは重要なポイントだが、そのすべてをガイダンスで書くのは難しい。どのような情報であれば NDA 上の秘密情報にあたらないか、という感じで、例示はできるのではないか。
- 公表は、脆弱性の悪用情報、MSP 等のベンダのサービスが踏み台になっている事案では、匿名か、非匿名かのコントロールも難しい。
- 公表の判断においては、それに資するケース事例、条件を列記できればと考えている。被害組織にはさまざまな判断基準があるが、起きている事象がテクニカルにどういうことか、その公表で第三者に不利益が生じないかについては、専門知見を持つ官民の窓口に相談するのもトラブル回避の方法になる。
- 被害組織から、未公開情報はどのくらいの時間で、あるいはいかなる事由により公になるかという相談を受けることがある。情報が出てしまう蓋然性が高いなら、隠さずに早く公表するという広報戦略もある。また、意図せずに情報が出てしまうのは被害組織にとり重要なので、そうした点をガイドラインには書いていきたい。