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 4 回会合

議事概要

■ 日時

令和 4 年 9 月 22 日（木）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）、内閣官房内閣総務官室、総務省（大臣官房）、防衛省

■ 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　サイバー攻撃被害に係る情報の共有・公表ガイダンス（素案）【非公開】

■ 議事概要

（１）事務局より配布資料確認、出席者関連、事務的事項の連絡の後、星座長より本会合の進め方、チャット機能の活用等に関しての説明とともに、資料 1-2 の「サイバー攻撃被害に係る情報の共有・公表ガイダンス（素案）」を非公開とする旨の決定があった。

（２）サイバー攻撃被害に係る情報の共有・公表ガイダンス（素案）について

事務局より資料 1-2「サイバー攻撃被害にかかる情報の共有・公表ガイダンス（素案）」についての説明があった。

（３）議論

（新井委員）

・ Q29「専門組織から『分析結果をレポートとして公表したい』と聞かれたらどう判断すればいいですか？」に関してだが、被害組織のデメリットが強調され過ぎているため、被害組織は断るのではないか。出すことを積極的に奨励する形の方がベターである。

（板橋委員）

・ Q13「『共有』『公表』はどういう違いがありますか？」に関してだが、「情報共有目的の公表」というのは、書きぶりとして矛盾しているように見える。また、③「その他の目的による公表」は、具体的にどういうものが想定されているのか書いてほしい。

（勝村委員）

・ メディアの過度の批判により被害組織から情報が出ない状況がつくられ、公表による情報共有が望めなくなった。攻撃者から守るための情報共有が今回のねらいであり、このガイダンスの意味だと思う。公表は、技術的な情報共有とはレイヤーが異なるので、公表しなければならない、と読めるような書きぶりは避けた方がいい。

（武智委員）

・ 本ガイダンスをどう使えばいいのか、「はじめに」の部分で明確にしてほしい。共有に重きを置くなら、その趣旨を明確にすればガイダンスは使いやすくなる。共有は基本的に非公開で行われ、ある程度相手が分かっているものの、公表は企業ごとに考えることが違うので、それを網羅してガイダンスに載せるのはかなり難しい。影響が他社に及ぶ場合は公表すべきと書いた上で、その際の留意点を挙げ、各々が考えるというトーンでよいのではないか。
・ このガイダンスの中での言葉の定義、使い方については明記してほしい。それが明確であれば、このガイダンスは非常に読みやすいものになると思う。

（辻委員）

・ 公表のタイミングに関しては、決して早ければいいというものではない。早く出したために問い合わせが殺到し、同じ温度感での回答ができないことは避けなければいけない。学校にサービスを提供する事業者が被害に遭った際は、システム運営の大もとではなく学校に問い合わせがくるので、各学校の説明が必要な場合がある。そこを利害関係者に共有するが、その場合のテンプレートを作成し成功している会社もある。何らかの異常が起きた場合、その詳細までは言えないとしても、異常発生の事実を早く言うのが大事なポイントである。

（蔦委員）

・ 「望ましい」「推奨される」等の語尾は、ガイダンスの中で極力統一すべきであり、そうでないとレベル感が分からない。また、＜被害の公表や法令等に基づく報告・届出について＞のパートは、語尾の使い方に特に留意した方が良い。例えば、Q16「警察への通報・相談は、行った方が良いでしょうか？」の箇所で、「適切です」というのは、ニュアンスが強いので、慎重に考えるべきではないか。
・ 共有、報告／届出、連絡、公表の意義を図で示しているのは分かりやすいが、文字での定義も加筆してほしい。

・ 本ガイダンスのメインではないが、「はじめに」の中の、「行政機関への報告・届出、警察への通報等について」において、図表で NISC の位置付けが不明である。民間企業としては、行政機関間でどのように流通するのかを気にすることもあるという認識なので、読者のためにも NISC の役割は明記してほしい。

（山岡委員）

・ 共有パートには共有についての留意点の Q があるのに、公表パートにはそれが無い。公表パートにもあった方がいいのではないか。

（花岡委員）

・ 当社では共有と公表は概念が真っ二つに分かれている。共有については、セキュリティ技術部門の私の決裁でいいので、ガイダンスに書かれているとおりの方針、考え方でやっているが、公表は、社会に対してのインパクトがベースとなる。
・ 公表となった場合、共有している技術情報をそのまま載せる発想は全くなく、むしろ載せない方向である。管理下の環境だけで片付くケースが少ないためである。技術情報は関係者には伝えるが、基本的に共有することにとどめている。
・ 自分の経験上、個別のインシデントにおいて、ベンダーがブログなどに書いた技術情報が参考になるケースはあるが、具体的な社名等は必要がないのではないか、と思うこともある。その辺りの書き方は難しいと思う。

（北條委員）

・ 基本的には、共有すること／しないことで、責任が発生することは無いとは思うが、企業としては、その有無は気になるポイントである。

（松坂委員）

・ 「用語集補足」については、メッセージ性を弱めないためにも、共有・公表を最初に持ってきてほしい。そして公表についても、社会的責任を果たすための公表、ノウハウを共有するための公表等、はっきりと言い切るべき。何のために、どういうことをしなければいけないかをぜひ書いてほしい。

・ 届出の話は、新たな章でかなり分かりやすく、意義については描き切れていると思う。なぜ国、政府、法執行機関が情報を集めて活動するのか、説明がなされている。

（吉岡委員）

・ ガイダンスのタイトルでは共有と公表が並び立つ形に使われているにもかかわらず、中身では、共有がクローズアップされている。意図的にそうしているのであればよいが、そうであるなら、本文に、情報共有とは何かの説明が、はっきりとあった方がいい。それをしっかり説明した上で、情報共有の意義について書くほうが分かりやすい。

（若江委員）

・ 非常に意欲的なガイダンスと思うが、公表に関する記述が粗く、まだ整理、検討が必要な部分がある。具体的な攻撃や被害の情報が広く一般に共有されるからこそ、様々な対策を講じていく必要性が社会全体で認識され、合意が形成されていくはずで、公表の社会的意義は大きい。現在の書きぶりでは、「この程度なら公表せずともよい」といった誤ったメッセージを与えかねないので、練り直してほしい。
・ 報道への評価も整理が必要だ。報道が、企業のサイバーセキュリティ対策について検証し、問題点があれば批判するのは、当然のことである。報道批判がだめだと言っているのではなく、報道の側に事案への無理解や過剰なバッシングがあれば問題だと思う。だが、今の書きぶりでは、報道すること自体が情報共有活動の阻害要因になっているという表現になっている。これは、サイバーセキュリティ協議会という、官民が関与する組織体に設置された検討会ではあるが、国が関与するガイダンスである以上、報道をコントロールしたいようなニュアンスが出るのは、注意すべきと思う。

（事務局コメント）

・ 全体構成で共有と公表が横並びであるにもかかわらず、共有がクローズアップされている点は、意図的なものである。基本的に共有の部分を重点的にゴールとしたい。Q14「なぜ公表をしなければならないケースがあるのですか？」の後半に、公表の社会的意義を書いているが、この場所で良いかは、あらためて事務局で検討する。
・ NISC の役割は、被害組織から上がってきた情報を、所管省庁を通じて集約することであるので、それが伝わるようにしたい。

- 報道について否定的ニュアンスが見えるという指摘については、そういう意図はないが、そう見えないように工夫したい。
- 冒頭の「共有とは」の後に「公表とは」をどう入れるかについてだが、公表はサイバーセキュリティ以外の要素が多分にあるため、書き切るのは難しいが、意見の相違も踏まえ何とか書きたい。
- ガイダンスは、実務担当者が Q の関連部分を見て使うと想定している。Q ベースで書き、背景の考え方を冒頭で書くのがいいと考えている。
- 共有すること／しないことの責任という形では、現状、書いていない。書くことによる萎縮効果もありうるためである。今後、意見があれば検討したい。
- インシデント対応での公表のタイミングは、早さだけで考えられないのはご指摘のとおりであるので、その点、追加したい。
- Q29「専門組織から『分析結果をレポートとして公表したい』と聞かれたらどう判断すればいいですか？」に関しては、出したほうが社会全体のメリットが大きいと思うので、ポジティブな方向に書きたい。