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 1 回）
議事要旨

■　日時：令和 4 年 5 月 30 日（月）17:40～19:40

■　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
　　若江　雅子　株式会社読売新聞東京本社 編集委員
　　（吉岡委員は都合により欠席）
（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）　国家安全保障局、総務省（大臣官房）

■　配布資料：

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の開催について（令和 4 年 4 月 20 日　サイバーセキュリティ協議会運営委員会決定）
資料１－２ サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会委員名簿
資料１－３ 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運営細則（案）
資料２－１ 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のスコープ及びスケジュール
資料２－２ JPCERT/CC からの論点提示

■　議事概要：

（１）　開会

事務局を代表して総務省 巻口サイバーセキュリティ統括官から挨拶があった。

（２）　議題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について

事務局から、資料１－１、資料１－２及び１－３に基づき、検討会の設置経緯や構成員、運営細則について説明があったあと、委員の互選により、東京都立大学法学部 星教授が検討会の座長に選任された。また、座長により、運営細則が決定された。

（３）　議題２　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

事務局からの説明に先立ち、星座長から、本検討会では、事務局の素案に基づく形式的な議論ではなく、幅広いバックグラウンドを持つ委員の自由討議を重視した議論とし、会の進め方は座長一任としたいとの発言があった。その後、事務局から、資料２－１及び資料２－２について説明があった。各委員からは、以下のような問題意識や意見が出された。

（新井委員）

- IoC の情報、攻撃者とその手口に関する情報等は、得られたときには既に古く、これからの対策ではなく事後的な指標になっている。このことに問題意識を持ち共通認識としたい。

（板橋委員）

- 情報共有においては信頼性が非常に重要で、セキュリティクリアランス制度が不可欠になる。民間にはそういった制度はないが、いろいろな分野で求められることが多いので、今後はぜひ考えねばならない。
- 情報の公表については、その主体の検討と目的の明確化が重要。ステークホルダーが多いと難しいので、なおさら重要になると思う。

（勝村委員）

- これまでさまざまな現場を見た経験から、情報をきちんと共有していれば被害は防げたであろうことや、公開の遅さが腹立たしいことが多々ある。公表は難しい問題も抱えており、すべての問題を解決するようなガイドラインを作るのは不可能だが、企業の現場が何らかのヒントを得られるようなものを検討したい。
- 被害組織は、誰と情報を共有するのかをまず考えねばならない。JPCERT/CC や IPA がハブになればやりやすいし現実的と思うが、これは今後の検討課題である。
- 公表の際に、ガイドラインに則って共有していることをきちんと述べ、それが意義あるものになればインセンティブの１つとなると思う。

（武智委員）

- 企業では、この問題での課題は多岐にわたる。役に立つガイドラインにするには、どういう目的で何を検討するかの議論を深化させ、明確にすることが必要。実効性ある施策につながればありがたい。
- 公開と共有は単純に 2 つの大枠ではない。誰が、誰に対して、何を、何の目的で等々、細かく分析した記述にし、さらに企業、そのサプライチェーン、ステークホルダーもそれぞれ違うので、その点を考慮したガイドラインとしてほしい。

（辻委員）
- 情報に関しては、そもそも何を出していいのか、出すことにより何が返ってくるかがわからないことが、公表されにくい理由の 1 つだと思う。出さなければセキュリティ上、何も起きないと、結局、何も言わない選択をする。その辺、提供する側との相互理解を深めることを主眼において、進める中で協力できればと思う。
- 共有と公開はバランスが非常に難しい。このガイドラインにはその点を示しておいたほうがいいのではないか。
- 脆弱性情報等については、それを届け出る先を周知徹底しておくことが必要。共有によるリスクがないこと、意義、メリット等も考えておいたほうがいい。

（蔦委員）
- 弁護士ならではのできることを考えていたが、例えば、ベンダによる情報共有に NDA 等の障害があるということであれば、成果物で契約のひな形を示して、情報を出せる条件や範囲を設けるというのはどうか。成果物の中で、このような条項を設ける必要性やメリット等もあわせて示すことができればよりよいと思う。
- 情報共有において重要なのは、メリット・インセンティブをどう設計するかと、デメリットの削除・負担の軽減という 2 つだと思う。
- 未公表被害を第三者が勝手に公表してしまうリスクは常にある。会社の隠蔽を疑われかねないので、そうしたレピュテーションリスクを低減するために先行してインシデント関係の情報を公表することはあり得る。

（花岡委員）
- JPCERT/CC のまとめたケーススタディはひととおり経験しているが、3 年前のインシデントでは、当時の情報共有・公表のやり方が反省につながった。公表のポイントに関しては、タイミングを遅らせた結果、先にメディアに出てしまったケースも経験した。そうしたさまざまな反省点を提供していきたい。

（北條委員）
- 難しい問題だが、ランサムウェア、標的型などのサイバー攻撃ごとに情報共有の価値は異なるので、何を出すのか、何を共有するのかを、技術情報の場合は粒度も考慮してク

リアにすることが重要なポイントと感じる。被害組織の大変さを理解し、その視点を入れた書き方をしたほうがいい。

- サイバー警察局が設置された。警察への相談、通報を促進し、同局において対処していただくことも、サイバー攻撃を抑止するための 1 つの方法であろう。この点をガイダンスに盛り込んでいただきたい。
- 情報を共有することにふさわしくない組織を制限できる仕組みづくりも大切。社会的活動として対応できる事業者間で行うことが本来の姿なので、今回の方針と合うか、合わないかも含めて判断の基準になると思う。

（星座長）

- サイバー空間がほとんど世間そのものという現状において、情報をどう共有し公表するかに 1 つの正解はないと思う。国境をたやすくまたいでしまう等、この問題の固有の事情を考え、法執行の観点、国際的共助の観点も含めることが大事だ。
- ガイダンスの着地点はまだよくわからないが、今後の礎となる議論をしたいと考えている。

（松坂委員）

- 10 年以上、日々セキュリティ関連の業務を行っているが、情報共有活動において何が最適なのか、いまだにわからない。今回検討する、目に見える指針となり得るガイドラインがあれば、そうした活動もスムーズに継続できると思う。
- 情報セキュリティインシデントの届出制度があり、そのアウトプットを公開しているが、なかなか活用し切れていない。この検討会では、その辺も含めて議論したい。

（山岡委員）

- 大企業にとって、共有・公表をすべきかどうかはハードルではなく、いつ公表すればいいか、どういった内容を公表すればいいのかが主な問題となるが、中小企業では公表・共有をすべきかどうか自体がハードルで、大きな論点になる。報告することで責任を追及され大事に至りかねないというマインドが原因と推察されるため、ここで重要なのは、ハードルの除去とインセンティブの付与だと思う。公表文を出すことで、担当者のオペレーションの負担を実はかなり減らせることにもなるといったインセンティブを実務上アドバイスすることがある。この会では、このあたりの実務上の視点をお話ししたい。

（若江委員）

- 公表による二次被害、風評被害の懸念や批判も実際に感じているが、一方で、公表によって具体的な情報を社会全体で共有することには、個社の利害を超えた社会的意義もある。専門機関の間で対応・対策のための情報を共有することとも、また違った意義が

あると思われ、まず公表の社会的意義を確認したいと思う。その上で方法を考えたいが、影響範囲の広さや深さなど個別の事情が異なり、一律に公表すべき時期、中身、レベル等を具体的に示すのはなかなか難しい。事例ごとにベストプラクティスを紹介していくやり方もいいのではないか。

（事務局コメント）

- 共有・公表については、誰が誰に対してのものかをもっと精緻化すべき。企業もさまざまな立場の人がいて、ステークホルダーもそれぞれ違うのでひと言では言えないというご発言に関しては、今日の説明ではかなり省略した。参考資料を見ていただきたい。
- 共有と公表については異なる性質のさまざまなプレーヤーがいることが、今までどこからもあまり示されてこなかった。この問題は今後の議論で整理をしたいが、まずは文章にし、何らかのコンテンツとして作るだけでも効果はあるのではないかと考えている。
- 公表の際、ガイドラインに沿って共有していることをアリバイ的に使うのは、まさに事務局も考えているところだ。それにより公表内容の受け止め方が違うのではないか。
- 共有と公表のバランスの件に関しては、実際に不都合が起きていると思う。今後の論点としたい。

以上