事務所ニュース News
2023.2
K-042
発行：税理士法人　行本事務所

経営バイタルの強化書 KEIEI VITAL

サイバー攻撃被害で受ける影響を最小限におさえるためには？

「サイバー攻撃被害に係る情報の共有・公表ガイダンス（案）」

インターネットをはじめ、ネットワークの利用が業務において不可欠となっている昨今、サイバー攻撃を受けてしまうリスクは高まっています。サイバー攻撃を受け被害にあった場合、情報の共有や公表が必要となりますが、どのように情報を共有し、攻撃の状況や被害内容を公表すればよいのかわからないことが多いことと思います。適正な情報共有・公表を行うことで、万一サイバー攻撃被害にあってしまった場合の影響を最小限にすることができます。ガイダンスの内容を理解してサイバー攻撃対策を行いましょう。

ガイダンスの内容を理解してサイバー攻撃に備えましょう！

1 「サイバー攻撃被害に係る情報の共有・公表ガイダンス（案）」意見公募

令和4年12月26日に経済産業省、内閣官房内閣サイバーセキュリティセンター（NISC）、警察庁、総務省は、「サイバー攻撃被害に係る情報の共有・公表ガイダンス（案）」（以下ガイダンス）意見公募を開始しました※1。

医療機関へのサイバー攻撃、自治体へのサイバー攻撃等最近のサイバー攻撃の脅威が高まる中、攻撃を受けた被害組織がサイバーセキュリティ関係組織と被害に係る情報を共有することは、攻撃の全容解明や対策強化を図る上で、被害組織・社会全体の双方にとって有益ですが、実際には、自組織のレピュテーション（風評）に影響しかねない情報共有には慎重であるケースも多く見られます。

そこで、官民の多様な主体が連携する協議体である「サイバーセキュリティ協議会」の運営委員会の下で、「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」が開催され、被害組織の担当部門（システム運用部門、セキュリティ担当、法務・リスク管理部門等）が被害情報を共有する際の実務上の参考となるガイダンスの策定に向けて討議が行われ、この検討会において、「サイバー攻撃被害に係る情報の共有・公表ガイダンス（案）」が作成され、今般意見公募が行われました。

インターネットをはじめ、ネットワークの利用が業務において不可欠となっている昨今、サイバー攻撃を受けてしまうリスクは高まっています。

サイバー攻撃を受け被害にあった場合、情報の共有や公表が必要となりますが、どのように情報を共有し、攻撃の状況や被害内容をどのような形およびタイミングで公表すればよいのか、また相談先、報告先についてもわからないことが多いことと思います。

サイバー攻撃を受け、情報が漏洩してしまった場合、顧客等情報漏洩元への対策や法的な報告を適切に行うことができなければ、信用情報をはじめ経営に大きな影響を及ぼします。

サイバー攻撃を受けてしまった場合に、どのような情報を共有し、公表を行えばよいのか、ガイダンスの内容に沿って解説を行います。

2 「サイバー攻撃被害に係る情報の共有・公表ガイダンス（案）」の内容

ガイダンスの内容は、**1. はじめに**、**2. 情報共有・被害公表の流れ**、**3. FAQ**（情報共有の方法等、被害の公表や法令等に基づく報告・届出、被害組織の保護、攻撃技術情報の取扱い）、**4. ケーススタディ**（標的型サイバー攻撃、脆弱性を突いたWebサーバ等への不正アクセス、侵入型ランサムウェア攻撃）、**5. チェックリスト／フローシート**となっており、情報共有・公表とは

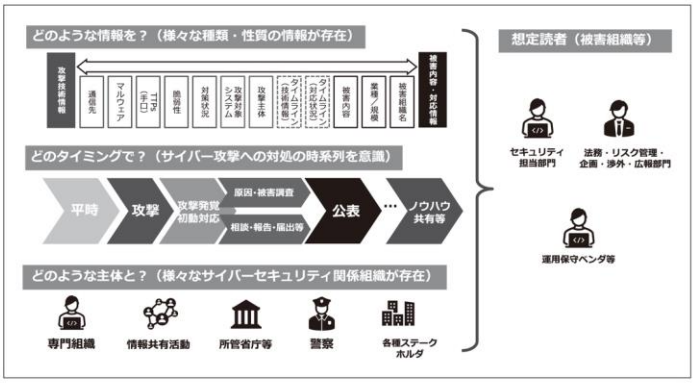
裏面へ続く→

どのようなことをするのか、情報共有・公表することで不利益はないのか等について、被害組織が保護されつつ、円滑かつ効果的に情報共有・公表が行われるためのポイントが示されています。

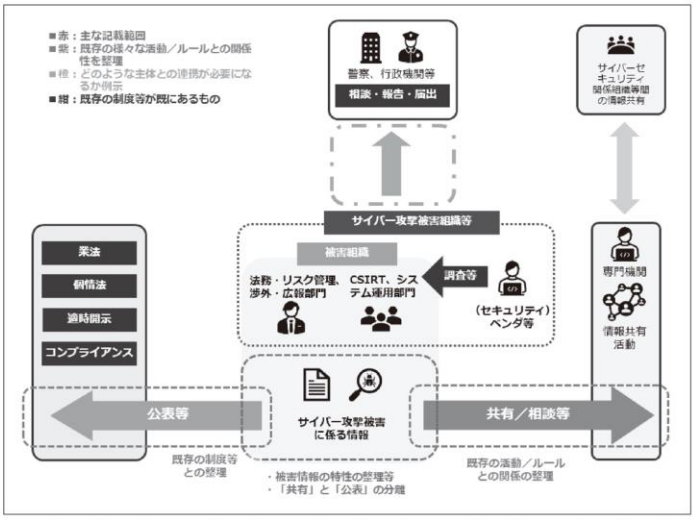
ガイダンスでは、被害組織で見つかった情報を**「何のために」「どのような情報を」「どのタイミングで」「どのような主体に対して」**共有・公表するのかのポイントがFAQの形式で整理されており、また、ケーススタディを通じて標的型サイバー攻撃、脆弱性を突いたWebサーバ等への不正アクセス、侵入型ランサムウェア攻撃等のサイバー攻撃を受けてしまった場合に、どのような対応をどのタイミングで行い、必要な情報を収集し、関係機関へ報告し公表するかについて具体的に説明が行われています。また、攻撃に対して行った対応についてポイントの解説が行われており、同様の被害にあってしまった場合の対策について参考とすることができるようになっています【図1】。

サイバー攻撃被害に係る情報とはどのような情報で構成され、どのような性質を有しており、取り扱いに際してどのような留意点があるのか、また、どのようなタイミングにおいて、各情報をどのように扱えば情報共有の効果が得られるのか、あるいは公表の目的を達成できるのか、ポイントやケーススタディ等が示されています。

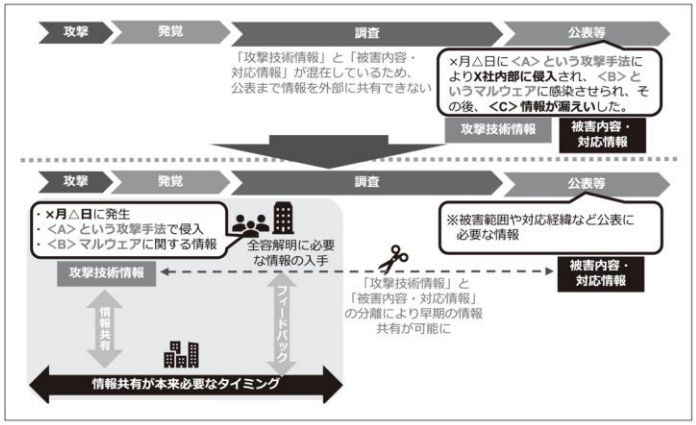
【図1】ガイダンスの内容と想定読者※2



【図2】サイバー攻撃への対応と情報共有・公表の範囲※3



【図3】被害情報の切り分けと情報の共有・公表※2



サイバー攻撃の被害に関する情報には、被害組織名や被害内容など、**「被害そのものや被害組織の対処内容を示す情報」**と、攻撃手法や発見されたマルウェア、不正通信先情報などの**「攻撃手法／攻撃者の活動を示す情報」**の2つの種類の情報が存在します。

「被害そのものを示す情報」（被害内容・対応情報）には、被害組織名を始めとして、公開等で外部に知られることでレピュテーション（風評）リスクとなるものや、自己の過失に関する情報（自己の責任に結びつく可能性のある情報）、あるいは第三者の不利益となるような情報を含む場合があるため、基本的に公表前に外部に伝わることを避ける傾向が強い性質を有します。

他方で、**「攻撃手法／攻撃者の活動を示す情報」**（攻撃技術情報）は、被害組織に紐づくものはほとんどないため外部に伝えてもレピュテーション（風評）リスクは高くなく、かつ未公表の早いタイミングにおいて関係者間で共有されることでその効果を得ることができます。

このように「サイバー攻撃被害に係る情報」と一口に言っても、性質の異なる2つの種類の情報が含まれており、攻撃技術情報が早期に外部に提供されず、その結果、情報共有活動がうまく行えなかったり、情報の共有が行われていても、その効果を十分に発揮できなかったりすることがあります【図2】。

ガイダンスでは、この性質の異なる2つの情報を切り離し、情報の「共有」と「公表」を分離して（【図3】）被害内容・対応情報を適切に扱うことで被害組織保護の強化と攻撃技術情報の速やかな共有を図るための具体的な方法、必要なポイントをFAQとして記載しています。

FAQの内容は、情報共有の方法等、被害の公表や法令等に基づく報告・届出、被害組織の保護、攻撃技術情報の取扱いについての33問題への回答、解説となっており、情報共有・公表の内容がわからない場合には、**「情報共有」**については「Q5.どうやって「情報共有」をすればいいのですか?」「Q6.どのような情報を共有すればいいのですか?」「Q10.情報共有を行う上での留意点はありますか?」、**「情報の公表」**については「Q15.公表のタイミングはどのようなものがありますか?」「Q16.公表の内容としてはどのようなものがありますか?」「Q17.公表する際の留意点はありますか?」「Q18.警察への通報・相談は、行った方が良いでしょうか?」「Q19.警察に通報・相談することによる業務への影響はあるのでしょうか?」「Q20.所管省庁への任意の報告は、行った方が良いでしょうか?」「Q25.共有・公表したことで二次被害が出てしまうような情報はありますか?」を参考にするとよいでしょう。

※1「サイバー攻撃被害に係る情報の共有・公表ガイダンス（案）」に関する意見募集について（URL:https://www.nisc.go.jp/policy/group/kihon-2/pubcom-guidance2022.html）
※2 サイバー攻撃被害に係る情報の共有・公表ガイダンス（案）の概要（PDF）（URL:https://www.nisc.go.jp/pdf/policy/kihon-2/guidance(draft)_gaiyou.pdf）
※3 サイバー攻撃被害に係る情報の共有・公表ガイダンス（案）本文（PDF）（URL:https://www.nisc.go.jp/pdf/policy/kihon-2/guidance(draft)_honbun.pdf）