参考資料 1

JPCERT CC®

令和２年度 総務省「サイバー攻撃の被害に関する情報の望ましい外部への提供のあり方に係る調査・検討の請負」事業報告書

サイバー攻撃被害情報の共有と公表のあり方について

（公開版）

一般社団法人 JPCERT コーディネーションセンター

2021 年 3 月

JPCERT CC®

目次

1．調査の主旨とスコープ

1．1　本調査の主旨について

2020 年 1 月から 2 月にかけ複数の大手電機メーカーなどが半年～数年前のサイバー攻撃被害について公表を行った。一連の公表／報道を踏まえて、総務大臣や経済産業大臣からは、サイバー攻撃による個人情報等の情報流出が疑われた段階で速やかに報告と公表が必要であるとのコメントがあった[1]。また、サイバー攻撃被害の発覚から報告／公表までに相当の期間を要したことについて「サイバー攻撃被害の公表の遅れ」であるとして各メディアに報じられた。

そして、被害を公表した企業のトップからは「広い意味で、情報の共有というところでは遅れたという観点で大変、申し訳なく思う」とコメントがなされた。

なぜ、サイバー攻撃という犯罪被害を受けた企業がその事実を公表すること、特に「公表までの期間」について指摘がなされるのであろうか。

サイバー攻撃被害の発生が公表されることの社会的意義の一つに、サイバーセキュリティ対策を推進するための社会的な合意形成の機能を挙げることができる。すなわち、攻撃被害が公表されることにより、社会の様々な構成員が、我が国がおかれた厳しい現状を把握することができ、政府部門や民間部門において対策を強化していくことについての合意が形成される、という効果である。こうした観点から、サイバー攻撃被害の状況が、可能な範囲で、できる限り早く公知となることの意義は大きい。

他方、この後の章で言及するが、法制度としては、例えばサイバー攻撃被害によって企業が保有する顧客の個人情報が漏えいした場合、「二次被害の防止、類似事案の発生防止等の観点から、事実関係等について、速やかに本人へ連絡」することとされている（平成 29 年個人情報保護委員会告示第 1 号「個人データの漏えい等の事案が発生した場合等の対応について」）。さらに、「漏えい等事案の内容等に応じて、

---

[1] 梶山経済産業大臣の閣議後記者会見（2020 年 1 月 21 日）では、三菱電機の被害報道について記者から問われ、「一般論として、個人情報などの流失が疑われる時点で、影響を受ける方々との関係なども踏まえつつ、速やかに公表することも検討すべきであったと思っております。内容については、精査をしなくちゃならないと思っておりますけれども、そういう不正アクセスがあったということは、やはり社会全体、また企業、他の企業も含めて敏感であると思いますので、こういうことがあったということは、やはり早急に報告すべきであったと思っております。」と回答している。

後日の閣議後記者会見（2020 年 1 月 31 日）では、NEC の被害報道に関して、記者から「公表のタイミング」について問われ、「これはいろいろなケースがあると思うんですね。どういった情報が漏洩したか、漏出したかということの調査も急がなくてはならない部分もある。ただ、不正アクセスを受けたということに関しては、経済産業省の考えとしては、まず第一報を頂きたいと、そしてほかの企業にも注意喚起をしていくということだと思っておりますけれども、機密情報の関連先とのやりとりとか、いろいろなこともあると思いますけれども、そういった中でできる限り速やかにこういったものを報告していただきたいと考えております。」と情報共有／注意喚起、関係者への配慮等の観点が示され、報告について速やかに行われることを希望する旨が示されている。

また、高市総務大臣（当時）は閣議後記者会見（2021 年 1 月 21 日）にて、「一般論といたしまして、普段からサイバーセキュリティ対策をしっかりと強化しておくことはもとより、攻撃を受けてしまった後には、速やかな報告と外部への公表が重要だと考えています。 これはなぜかと言いますと、被害の拡大を防ぐ日本国内の他の事業者であったり、取引先などに被害が拡大する可能性を防ぐという点からも重要だと考えております。サイバー攻撃による被害の特定には時間を要することが少なくございませんが、個人情報流出が疑われる時点で、影響を受ける方々との関係も踏まえて、速やかに公表することを検討すべきであったと思います。」とコメントしている。

二次被害の防止、類似事案の発生防止等の観点から、事実関係及び再発防止策等について、速やかに公表する」こととされているが、一方で、個人情報以外の情報が漏えいした場合については、その事実の公表を求める法制度は現時点で見当たらない。

例えば、ある組織がサイバー攻撃を受け、取引先に関する情報が漏えいした場合、当該取引先にその連絡がなされ、二次被害防止が行われることが望ましいといえるであろう。他方で、この事実を、当該取引先以外に公表しなければならない理由、さらには「速やかに」公表しなければならない理由はなんであろうか。

実際に個人情報や取引先との間の機微な情報が漏えいしていないにもかかわらず、サイバー攻撃被害を受けたことを被害組織が公表するケースは存在する。JPCERT/CC がインシデント対応支援を行う中でも、情報漏えいは確認されず、また、制度上公表が求められるものではないが、被害組織が自主的に公表を行うケースに遭遇することがある。それらについて、公表の有する社会的意義の大きさに留意しつつも、被害組織による個々の判断理由としては、将来何らかの経緯で当該攻撃事象が報道されたり、SNS 上で情報が拡散するなどした場合のレピュテーションリスクを鑑み、“予防的に”被害リリースを出す、といった判断によるところが多いものと推察される。

この場合のレピュテーションリスクは、「(被害企業の) セキュリティ対策または対処能力が低い」という評判への懸念よりも、事案の認知から公表までの期間が長くかかる場合、「対外的に何らかの責任を有する情報の漏えいを隠していたのではないか」という種類の負の評判が発生することを懸念してのものではないかと考えられる。

一般に、サイバー攻撃により情報が攻撃者に窃取された場合、多くのケースでは当該被害組織自身の被害がどうであったかよりも、被害組織の顧客等の「個人情報が漏えいしたか／否か」という点で注視される傾向がある。実際に、サイバー攻撃被害を受けた企業のプレスリリースでは個人情報漏えいの有無に言及するものが多く、必ずしも個人情報を格納しているシステムが侵害されたわけではなくても、漏えいがなかったことをわざわざ記すケースが散見される。

また、個人情報漏えいの場合、企業自身のサイバー攻撃被害よりも、企業が個人情報を漏えい“させた”ことに対してその評価が集中するのではないかと考える。特に、企業の安全管理措置に不備があったことが漏えいに繋がったのではないかという、企業側の落ち度として評価されてしまっているのではないだろうか。

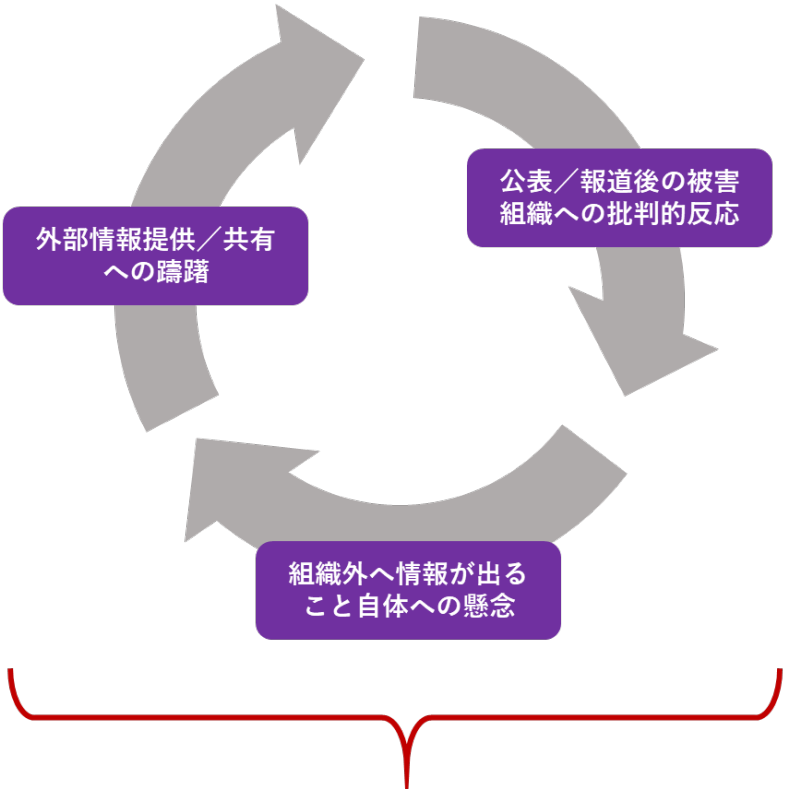
サイバーセキュリティ対策としての情報共有の重要性や必要性についてはこれまでも広く謳われてきた。すなわち、日々高度化／複雑化する最新のサイバー攻撃手法に対抗するためである。これは、裏返すと、他組織との適切な情報共有を行わない組織単体の活動では、もはや最新のサイバー攻撃被害を完全に回避することには技術的限界があることを示しているといえる。

そうした中、被害組織が公表した情報をもって、その対策上の“落ち度”を批判することは情報共有活動の本質的な理解と逆行する結果をもたらす可能性もある。法令上求められる義務を履行していたかどうかは業法等を通じて行政上の判断がなされるとして、本来、被害組織による被害公表とは、その前段階における、サイバー攻撃に対処するための効果的な情報共有という観点や悪意ある攻撃者によって被害にあった組織の保護や追加的な被害を防止するための観点から整理されるべきなのではないだろうか。

サイバー攻撃被害低減のため、日々インシデント対応支援や情報共有活動を行っている JPCERT/CC では、いかに攻撃活動初期の段階で攻撃を封じ込めることができるか考え、そのベースとなる情報共有活動の重要性をこれまでも主張してきた次第である。一方で、情報共有活動がうまく進まないことが一因となり、新たなサイバー攻撃に対して社会全体の対応が後手に回ることも多く、他の専門機関やセキュリティ専門企業などとともに非常に歯がゆい経験も重ねてきた。社会全体におけるサイバー攻撃対処のベースとなる情報共有活動が円滑に行われるためには、「情報共有」単体の概念／方法だけではなく、これと互いに影響しあう、「被害情報の公表」との関係性において、その在り方が検討されるべきであると考える。

また、ここまでにも触れたような、被害情報の公表をめぐる事情が、被害組織に対して「組織の外部に（サイバー攻撃被害に関する）情報が“出ていく”」ことに消極的にさせているのではないかとも考えている。これにより、下記図 1 のように、外部への情報提供・共有は阻害され、社会全体としてサイバー攻撃からの被害が低減できなくなっていくという悪循環が発生しているのではないかとも危惧される。

本報告書は、以上のような JPCERT/CC におけるこれまでのインシデント対応支援の経験を踏まえた問題意識をもとに、サイバー攻撃被害情報の共有と公表のあり方について検討し、情報共有と公表がうまくなされない悪循環を断ち切るための提言についてとりまとめを行うものである。

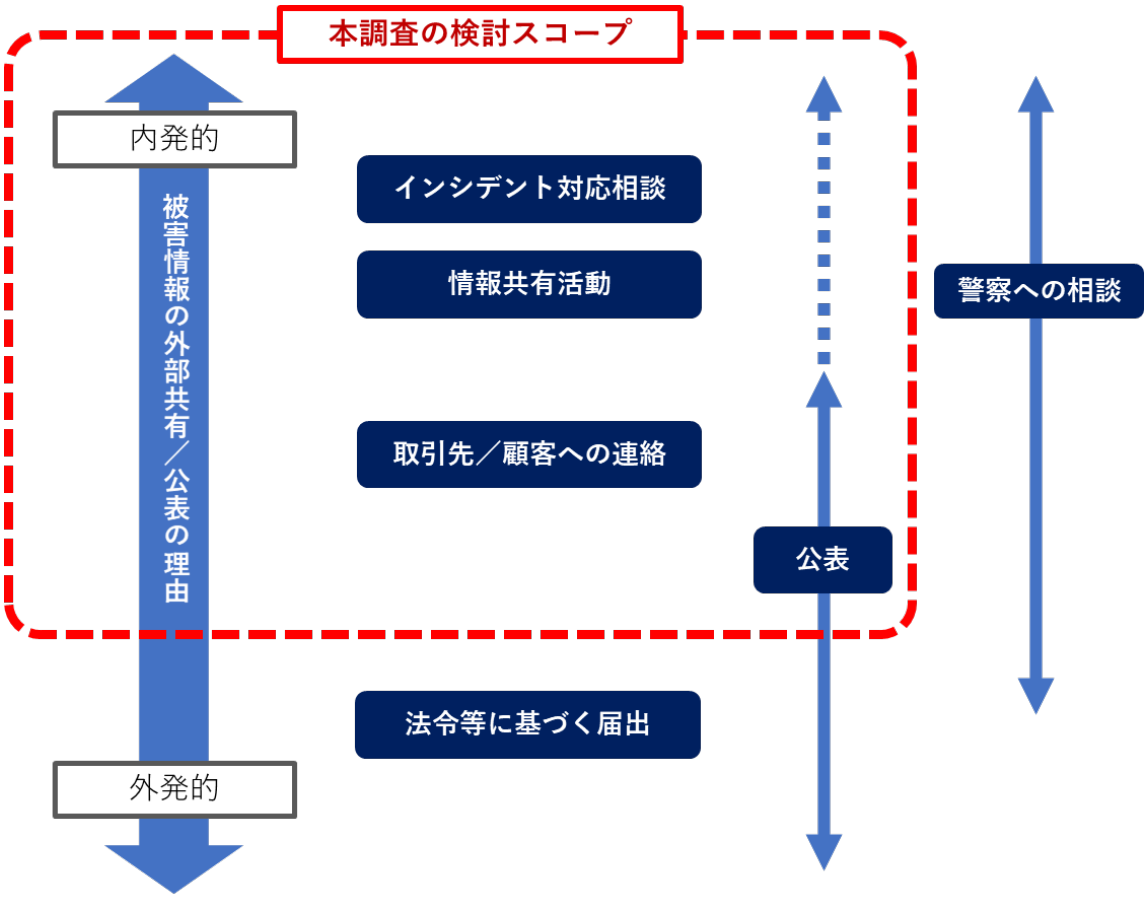


［図 1：外部への情報共有と公表における悪循環］

1．2　本調査のスコープについて

本調査は、サイバー攻撃被害に対するインシデント対応のフェーズを中心に検討を行い、企業のリスク情報開示[2]、犯罪捜査[3]、および法令に基づく届出制度はスコープ外とした。

被害組織から得られるサイバー攻撃被害情報は、サイバー攻撃への対抗や攻撃者の特定に有用な情報である。こうした情報は犯罪捜査や政府の対抗施策を通じて経済社会の防衛力を高めるために必要であり、さまざまな制度運用と相互に関係している。そのため、本調査のとりまとめにあたっては、総務省をはじめとする関係省庁にも検討会などを通じて意見を求めた[4]。



［図 2：本調査の検討スコープ］

---

[2] 総務省「サイバーセキュリティ対策情報開示の手引き」（2019 年 6 月公表）
https://www.soumu.go.jp/main_content/000630516.pdf

[3] 警察庁「令和 2 年度サイバーセキュリティ政策会議報告書　生活様式の変化等に伴うサイバー空間の新たな脅威に対処するための官民連携の更なる推進」（2021 年 3 月公表）
https://www.npa.go.jp/cybersecurity/pdf/20210308_2.pdf

[4] 本報告書は、調査研究の結果をとりまとめたものであり、総務省や関係省庁としての見解を示すものではない。

2．本調査のアプローチ

1．1 で取り上げた一連のケースでは、被害組織は、一体どのようなタイミングで公表していれば、適切な対応であったと評価されたのであろうか。また、サイバー攻撃の被害事実の公表とサイバー攻撃に関する情報共有との違い、被害組織から公表・共有される情報の性質や内容の特性、タイミング等については、これまで具体的に整理されてこなかった。

本調査では、これらの点についてインシデント対応の経験や関係者とのディスカッション・ヒアリングを踏まえて整理を行い、サイバー攻撃被害に関する公表や情報共有について検討を行った。

2．1　情報の「共有」と「公表」の分離について

2020 年 1 月 27 日の総務省サイバーセキュリティタスクフォース（第 20 回）で公表された「我が国のサイバーセキュリティ強化に向けた緊急提言（案）」[5]では、（被害企業において）「サイバー攻撃については、原因究明に一定の期間を要する場合もあるが、個人情報などの流出が疑われる時点で、影響を受ける主体との関係なども踏まえつつ、速やかに情報の公表を検討することが望ましい。また、類似の被害の拡大を防ぐ観点から、インシデントに関する情報の共有を速やかに行うことが求められる」と言及されており、「情報の共有」と「公表」の 2 つの観点が示されている。

また、2020 年 6 月 12 日に経済産業省から公表された「昨今の産業を巡るサイバーセキュリティに係る状況の認識と今後の取組の方向性について」[6]と題された産業界向けへの文書においては情報の「共有」「報告」「公表」の 3 点が整理されている。この整理の中で、被害の公表については、「サイバー攻撃の実態及びその被害を公表することの社会的意義は確実に増大しており、その期待も強くなっていることから、企業が守らなければならない価値とサイバー事案を公表することによる社会的な意義の間のバランスを如何に確保して、抵抗感なく公表を行える環境を実現するかが重要な課題」であると指摘し、公表のタイミングについては「サイバー攻撃による被害が甚大で影響する範囲の特定が難しく、広く関係者を巻き込んでしまう可能性があり、上記①[7]で触れたような小グループでの情報共有では被害拡大の抑制を図ることが難しいと考えられる場合には、速やかにサイバー事案について公表をすることが好ましい」としている。

---

[5] https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00093.html

[6] https://www.meti.go.jp/press/2020/06/20200612004/20200612004.html

[7] 2020 年 6 月 12 日に経済産業省から公表された「昨今の産業を巡るサイバーセキュリティに係る状況の認識と今後の取組の方向性について」において示された「サプライチェーンを共有する企業間におけるサイバー事案に関する高密度な情報共有」のことを指す

［表 1：総務省、経済産業省の文書における情報の共有・報告・公表の整理］

	共有	報告	公表
総務省 「我が国のサイバーセキュリティ強化に向けた緊急提言（案）」	目的：被害の拡大を防ぐ タイミング：速やかに行う	電気通信分野・放送分野における事故報告について言及	「個人情報などの流出が疑われる時点で、影響を受ける主体との関係なども踏まえつつ、速やかに情報の公表を検討することが望ましい」
経済産業省 「昨今の産業を巡るサイバーセキュリティに係る状況の認識と今後の取組の方向性について」	目的：被害の拡大を防ぐ タイミング：速やかに行う 範囲：重要なサプライチェーンを共有する企業間	軍事転用可能な技術に関する情報が流出した可能性がある場合の報告について言及	「サイバー攻撃による被害が甚大で影響する範囲の特定が難しく、広く関係者を巻き込んでしまう可能性があり、（中略）小グループでの情報共有では被害拡大の抑制を図ることが難しいと考えられる場合には、速やかにサイバー事案について公表をすることが好ましい」

両省の文書を整理すると、以下のような整理になると考えられる。

情報の共有：

・　（同じ攻撃による他組織への）被害拡大防止のため、速やかに情報共有が行われるべき

※ただし、一程度の信頼関係のある関係者間で行う（経済産業省文書）

被害の所管省庁への報告：

・　各業法等による制度上の報告（総務省文書）や所管省庁からの求め（経済産業省文書）に基づく。

※１．２に示したとおり、この所管省庁への報告は本調査研究では検討していない。

被害の公表：

・　影響を受ける主体との関係も踏まえつつ、個人情報等の流出が疑われる時点で速やかに検討する（総務省文書）

・　影響範囲が広く限られた関係者間での情報共有では被害拡大防止にならない場合、速やかに公表する（経済産業省文書）

つまり、全体の構造として

- （非公開の）情報共有
- 所管省庁への報告
- 被害の公表

という大きく３つのフェーズに分かれているといえる。

そして、両省とも、「情報共有」とは、被害拡大防止のために速やかに行われるべき活動であると解釈している。他方で、ここに取り上げた両省の文書によれば、「公表」については、①公表することによる関係主体への影響の配慮、②個人情報等の漏えい有無、③情報共有活動の限界を補うための観点、の３つの観点から実施やタイミングが検討されるべきと示されたと解釈できる。したがって、攻撃被害の発覚後、前提条件なく速やかに公表を行わなくてはならないものではなく、上記のような観点（条件）を踏まえて、公表やタイミングが判断されるべきとの考え方を導くことができよう。なお、こうした考え方は、第４章において触れる個人情報保護法の考え方とも整合的である（第４章４．２① 参照）。

２．２　「技術情報」と「コンテクスト情報」の分離について

次に、対外的に発信・提供される情報の違い性質・内容について検討する。サイバー攻撃被害を示す情報を要素分解すると、被害組織の特定につながりやすい「コンテクスト情報」と、被害組織の特定にはつながりにくい「技術情報」におおまかに区分できる。

①　コンテクスト情報

本稿では、個別組織名や対応経緯、被害内容など、被害組織に固有の情報を「コンテクスト情報」と呼ぶ。コンテクスト情報は、コントロールされずに拡散すると、被害組織が特定されたり、被害組織や被害組織の関係組織における二次被害にも繋がる恐れがある情報である。

例えば、サイバー攻撃を受け漏えいした情報の件数や内容などの被害情報や、どのような対応を行ったのか、といった情報がコンテクスト情報にあたる。これらは、個別の被害組織に固有の情報であり、次に掲げる技術情報とは異なり、まったく同じ情報が被害組織以外に存在することはない。

②　技術情報

本稿では、攻撃に使用されたマルウェアや不正通信先情報などを「技術情報」と呼ぶ。技術情報は、他の被害組織でも同一の情報が見つかったり、すでに公開情報である場合が存在するなど、必ずしも被害個社に固有の情報ではない。

攻撃者はマルウェアや通信先を“使いまわす”ため、同じハッシュ値の検体が複数箇所から見つかったり、一つの通信先を使って複数の標的を攻撃することがある。そのため、自分の組織のネットワーク内、端末から見つかったからといって、その被害組織以外誰も知らない情報というわけではない。

さらに、他の被害組織で見つかった検体が、オンラインの解析サービスにアップロードされたり、調査を行ったセキュリティベンダーなどがレポートで公表することがあるため、当該情報が秘匿性のある情報と解釈することは難しい。[8]

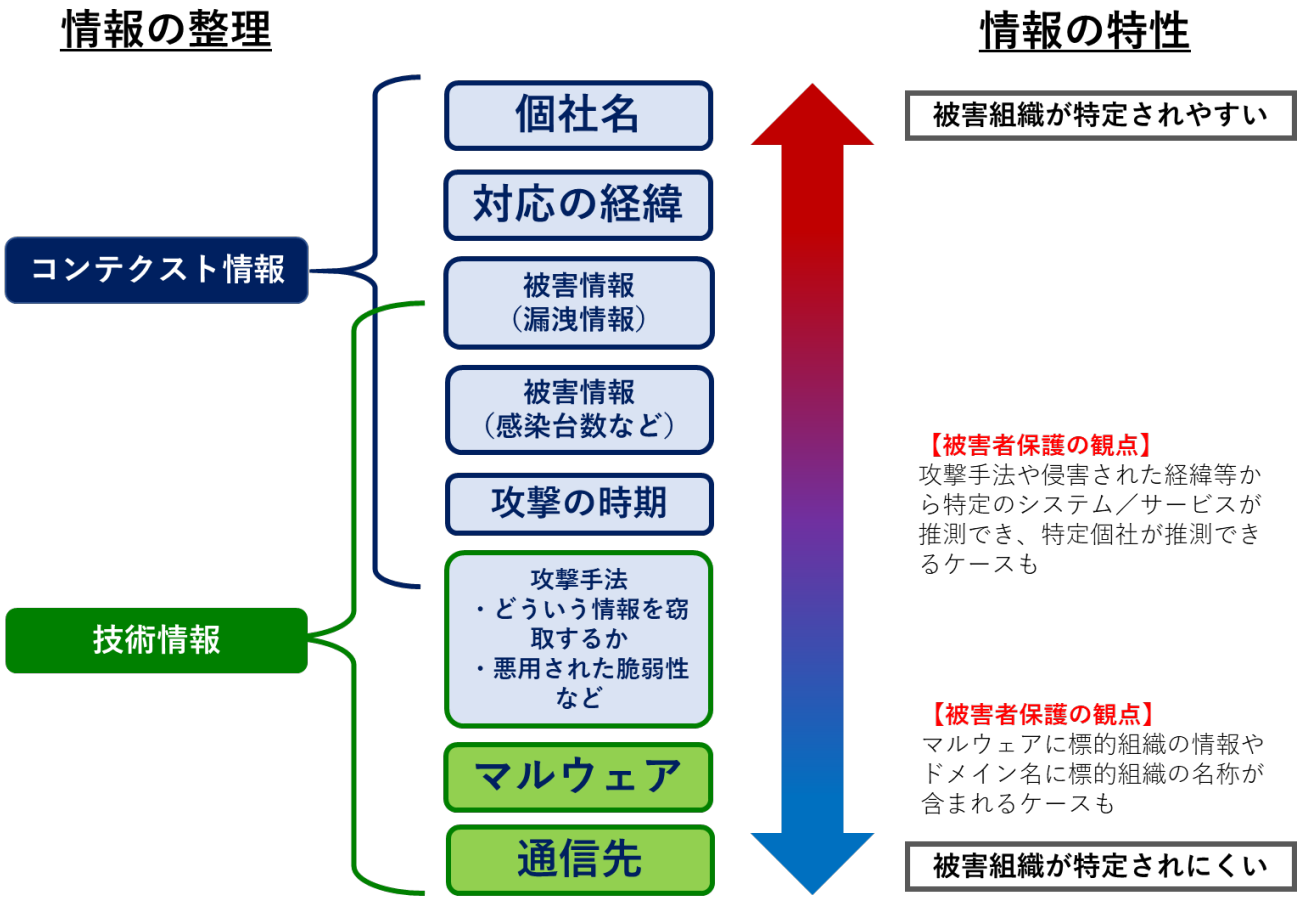
ただし、攻撃の種類によってはマルウェア内に標的組織（被害組織）固有の情報を含んでいる場合があるため、例外は存在する（第３章３．２① 参照）。

③　技術情報とコンテクスト情報の中間の情報

被害の様態として、被害組織が利用していた特定製品の脆弱性が悪用されたり、被害組織以外の第三者の Web サイトや提供するサービスが攻撃の踏み台となる場合がある。この場合、攻撃手法を示す情報として、被害組織を特定する情報ではないが、製品の製造元やサービス提供元といった、第三者の組織名、製品名、サービス名が含まれることになる。

---

[8] 被害が発覚した時点では他の被害組織で見つかった検体情報がオンラインの解析サービスにアップロードされていなくても、時間の経過とともにアップロードされ、公開情報として流通し始める場合がある。



［図 3：技術情報とコンテクスト情報の区分］

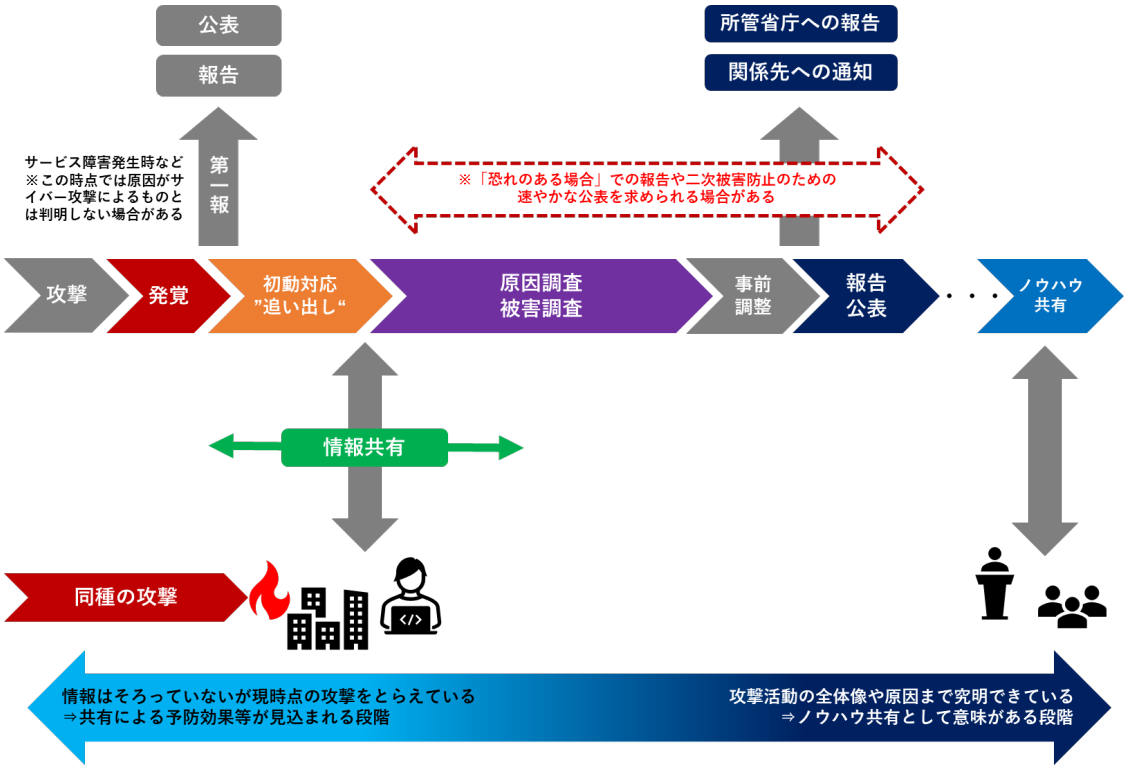
2．3　情報の共有から公表までのタイミングについて

必要な情報が適切なタイミングで共有・提供されるよう、実務に即したタイミングの認識が重要である。この適切なタイミングが、被害組織だけではなく、所管省庁や取引先、メディアなど広く共通認識として理解されることで、被害組織の保護や二次被害の防止、そして攻撃への根本的対処に繋がると考える。

サイバー攻撃への対処の観点からまず重要なのは、「公表前の早期の段階における情報共有」である。時間が経てばたつほど、被害組織自身が情報共有活動から得られるメリットも減衰する。不確かな情報であっても、複数の被害組織が共有しあったり、専門機関の分析が仲介することで攻撃の全容が解明され、各被害組織での原因調査に資するだけでなく、根本的原因への対処（攻撃インフラのテイクダウンや脆弱性調整）にも繋がるものである。次に公表については、2．1に示したように、制度上、速やかな第一報やその後の公表が求められているもの以外については、①二次被害防止、②被害者保護の 2 つの観点を踏まえて、実施やタイミングが判断されるべきである。

発生した攻撃への対処や利害関係者とのさまざまな調整を終え、被害事実を公表する準備が整ったタイミングになって、はじめて技術情報を専門機関等に共有しても、その情報共有に高い効果を期待することはできない。

さらに、二次被害の防止や制度上求められて公表を行う場合、第三者への注意喚起の目的が優先される傾向があることから、「ノウハウ共有」目的の公表としては意味合いが薄く、また、ノウハウ共有に資するような情報は事案対応（インシデント対応⇒公表までの一連の流れ）がひと段落ついたのち、再発防止策や対策強化の運用がある程度軌道にのった時点でないとそろわないことから、公表タイミングよりは後の時間軸上で行われることが望ましい。



［図 4：情報共有および公表のタイミング］

２．４　情報共有の範囲について

既存のさまざまな情報共有活動が存在しているが、大きく分けると

（A）専門機関がハブ機関として存在する情報共有活動

（B）業界固有の情報共有活動

に分けることができる。

（B）の形態は、個社名やコンテクスト情報を含めた「顔の見える関係」での共有を望む活動が多く、個別業界内に閉じることでより質的に豊富な情報を共有することを試みており、必ずしも注意喚起や全容解明目的の情報共有ではなく、ノウハウ共有目的で活動している場合がある。（A）の形態は、分野横断的に行われたり、参加組織の規模や能力に差がある場合において実施されており、匿名提供や断片的な情報提供であっても専門機関の知見や広範囲な参加者からの情報提供によって補われている。

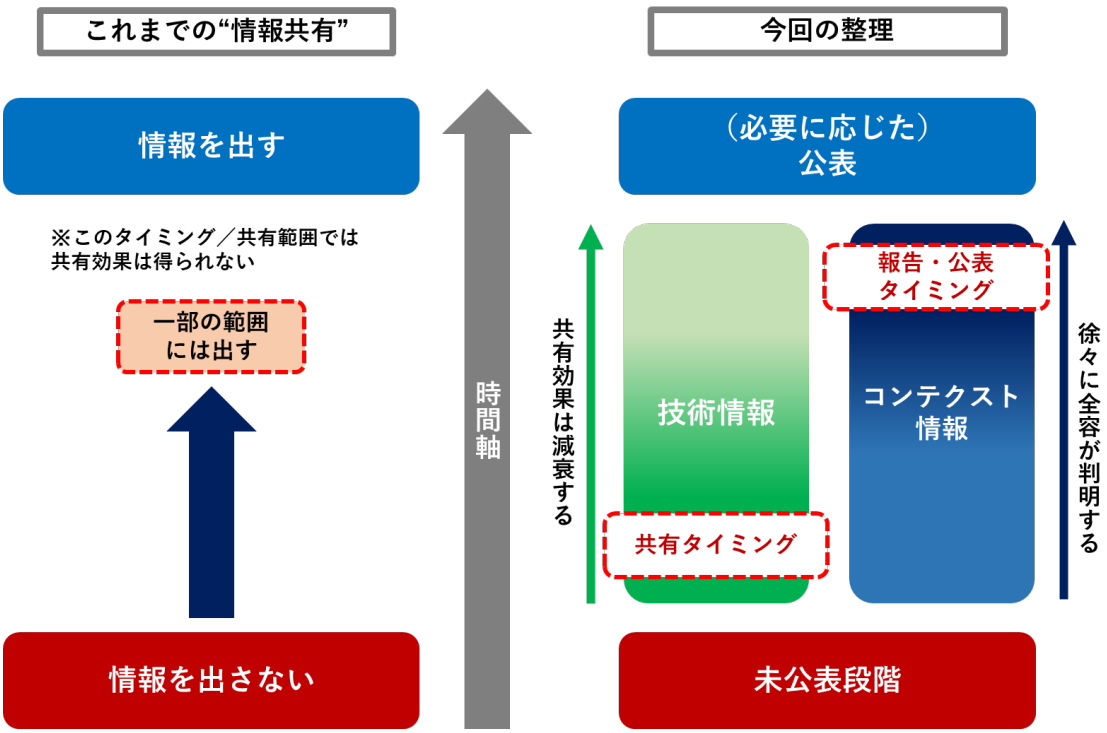
また、（B）は「顔の見える関係」という、参加者の限定と一定度の相互信頼関係のもとで情報の取り扱いを担保しており、（A）は専門機関を通じた匿名化処理によって同じく情報の取り扱いを担保するとともに、被害組織保護を行っている。

いずれの活動に参加するか（または両方に参加）は各組織の要望や業界固有の事情等によるものであり、一概に推奨することはできないが、いずれの活動であっても本報告書で述べる「技術情報とコンテクスト情報」整理に基づく「公表前の速やかな情報共有」と言う観点は有効であろうと考える。

これまでは被害情報を「出す」「出さない」という判断がなされることが多かったが、ここまでの整理のとおり、「どのタイミングで」「どの情報を出すか」という判断が行われるべきであると考える。これまでも、公表前の早い段階で外部に提供しても特定個社名が推測されづらい技術情報がインシデント対応現場で確認されていたが、これにコンテクスト情報が混在していたため、コンテクスト情報を外部提供できる公表段階まで、技術情報の外部提供がいわば「引きずられる」形で保留されていたと想定される。

また、この２つの性質の異なる情報の混在は、「共有先／提供先」の選択にも影響していたと考えられる。これまでは下記図左欄のように限られたコミュニティーや所管省庁等「ごく限られた関係者には情報を出す」ことが行われていたが、技術情報とコンテクスト情報が分離されておらず、また、共有効果のあるタイミングをすでに経過していることから、被害拡大防止や攻撃への根本的対処に資することが少ないものであった。

実際に必要なのは、共有効果が減衰しない早期のタイミングで、技術情報を必要とする適切な関係者へ共有されることであり、これは攻撃の種類や攻撃動向に応じて、特定の業界分野から広範囲な対象まで適宜変化する可能性がある。



［図 5：情報共有の時間軸と共有範囲］

3．情報共有のための視点

3．1　情報共有を巡る論点

情報共有については、2 に示した各観点を踏まえ、次のような論点が存在する。

① 情報の「非対称性」問題があるということ

サイバー攻撃は単一の被害現場を調査することでその手口が必ずしも全容解明できるものではない。攻撃者は検知回避や痕跡消去を行うことがあるため、各現場に残る情報にはばらつきが出る。そのため、被害組織ごとに残っているログの種類や量、検知有無や検体の回収可否が異なるからである。したがって、サイバー攻撃の手口の全容を解明し、情報共有活動の効果を最大限に発揮するには、複数の被害組織で見つかった情報が照合・分析されることが望ましい。

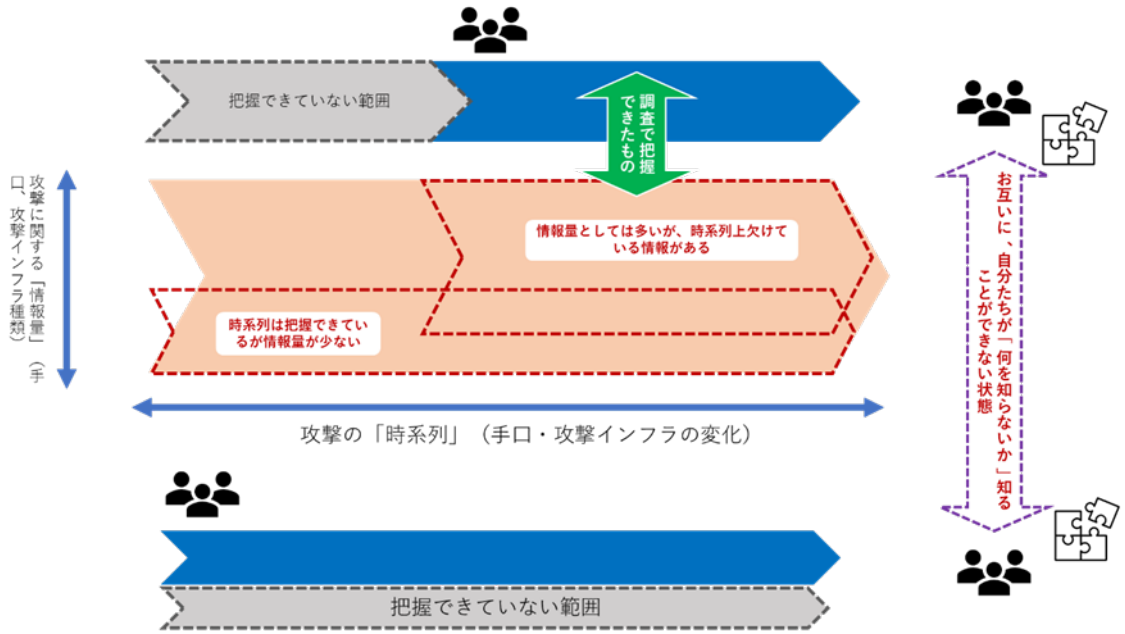
サイバー攻撃情報の共有活動は、類似被害の拡大防止や、早期発見など「社会全体に有益」である面が強調されやすいが、その場合、被害組織自身が得られるメリットを考察する必要がある。

下記に情報共有の「仲介者」がいない場合の情報共有を概念的に示す。

ここで、情報共有を行おうとする参加者は、攻撃に関する情報のすべてを把握できておらず、それぞれの持つ情報には欠損した箇所がある。しかし、お互いに自ら調べた範囲のことしか認知しえないため、「自分は十分に全容を知っている」と考えてしまうことから、情報共有の必要性は自発的に発生しない（これは、「情報の非対称性」による非効率に類する事象と解釈できる）。この場合、攻撃に関する情報の不足によって各被害者において最適な対処を行うことができなくなってしまう。

被害組織間の情報共有のメリットとは、単に「他者の被害軽減／予防のため」だけではない。こうした情報の非対称性が自らにもたらしうる不利益を避けることにある。すなわち、「自らがまだ知らない情報」を得ることであり、そうした不足する情報が補強されて、初めて被害組織自らも原因究明や再発防止策を確実に実施することが可能となるのである。

そして、こうしたパズルのピースが集まって初めて、標的となった／今後なる可能性のあるすべての組織に対して広く有効な対策情報が流通するのである。



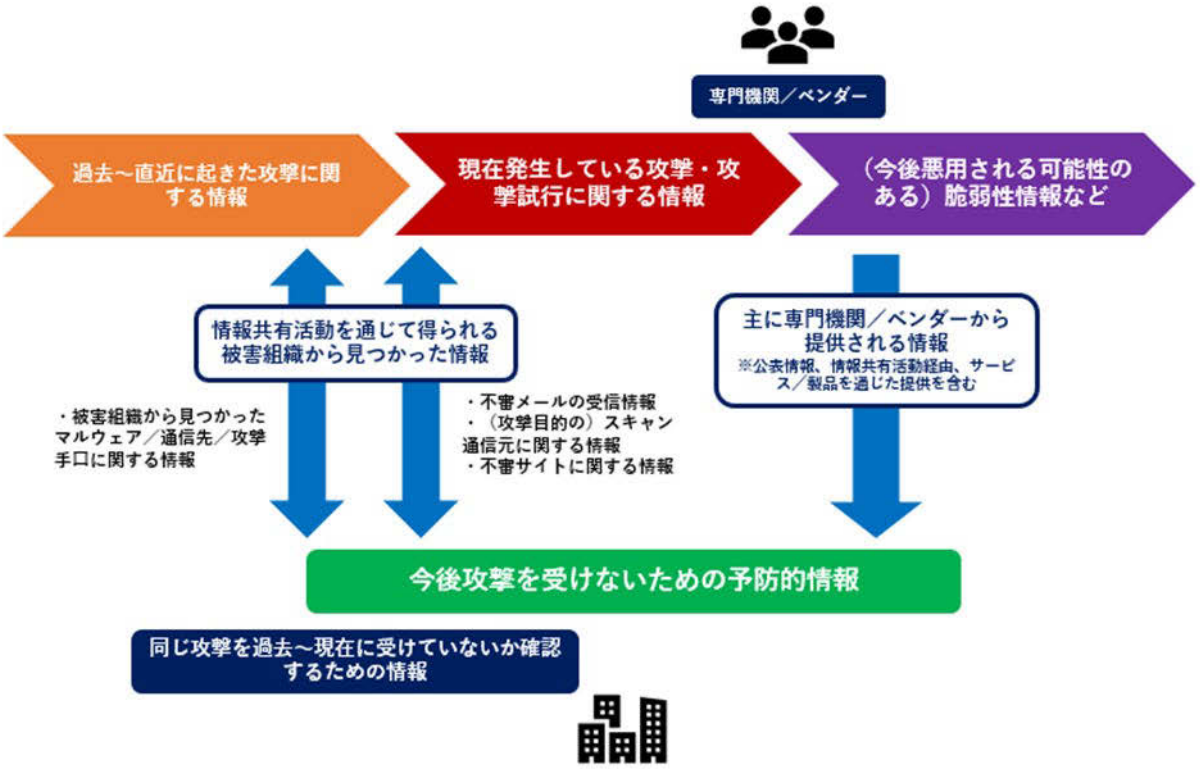
［図 6：情報共有における情報の非対称性］

② 共有のタイミングにより「予防のための情報」と「（過去）被害有無確認のための情報」に分かれてしまうこと

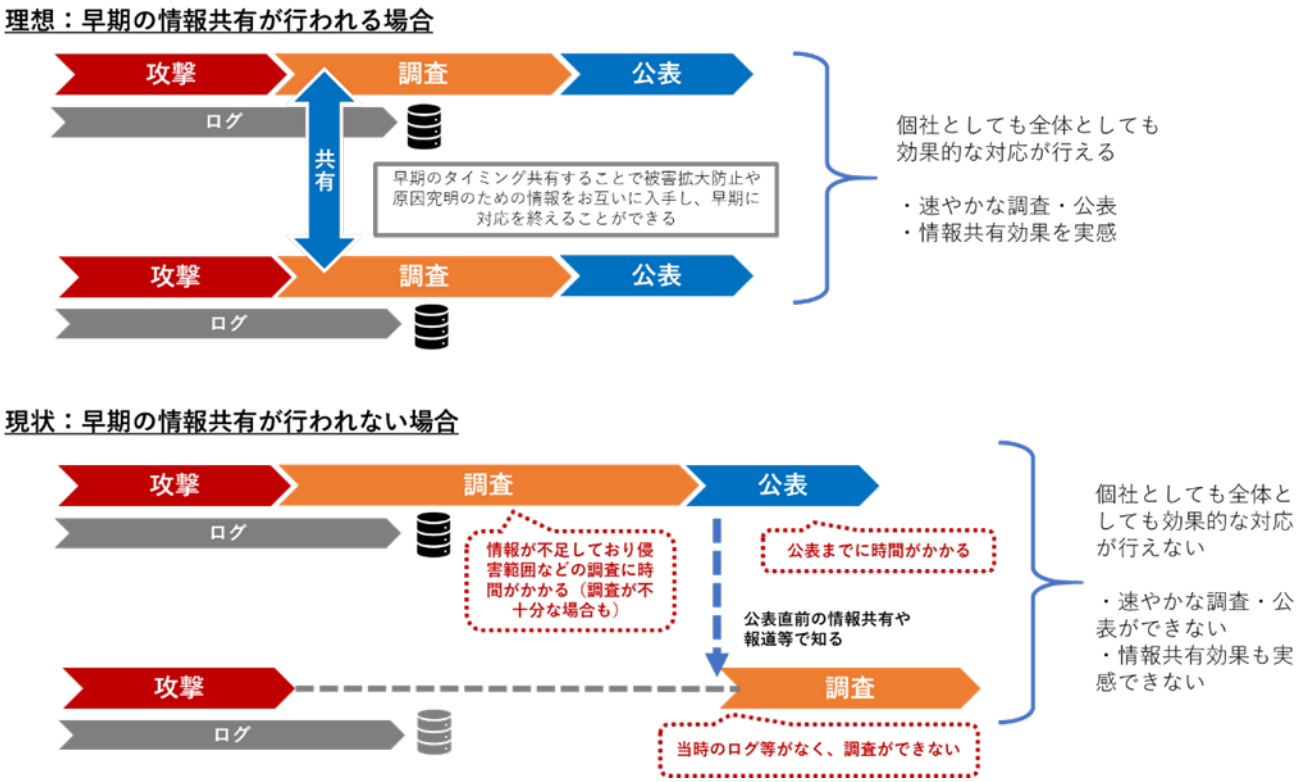
情報共有活動において情報が「どのタイミングで発信されたものなのか」が重要である。

２．３で述べたとおり、実際に被害現場で確認された攻撃情報であっても、時間の経過により情報共有による「（今起きている）攻撃の予防」効果は減衰する。さらに言えば、時間が大幅に経過した情報の場合、新たな被害の発生を予防する効果はまったくなくなってしまい、過去に発生した攻撃被害を“掘り起こす”ための情報となってしまうのである。一部の専門機関を除けば、当該時点で認知していない過去の攻撃被害を“掘り起こす”ための情報への需要は大きいとは考えにくい。

こうして、情報共有までに時間が経過すればするほど、共有される情報が第三者における攻撃被害を予防する効果が減衰するだけでなく、活動へ参加する組織のモチベーションも下げることとなってしまうのである。



［図 7：情報共有までの時間経過と攻撃被害の予防効果］



［図 8：情報共有のタイミングにおける理想と現状］

③ 全容を解明しなければならないということ

前述①のとおり、情報共有活動の参加者間には情報の非対称性があるため、情報共有活動を通じてこれを補完することが望ましい。また、適切な仲介者を介した情報の交換によって攻撃の全容が解明されることで、より効果のある対策情報が流通することになる点は述べたとおりである。

さらにサイバー攻撃の全容解明の必要性を考えると、情報共有活動が攻撃活動自体の収束のためにも必要となる面が見えてくる。

例えば、マルウェアのダウンロード元や不正通信先が特定組織の正規サイトを改ざんしたものであったり、特定のホスティング事業者のサーバーである場合がある。こうした場合、情報共有活動を通じて攻撃の全容を解明し、攻撃元／通信先をテイクダウンすることで攻撃活動自体を収束させることが可能である。

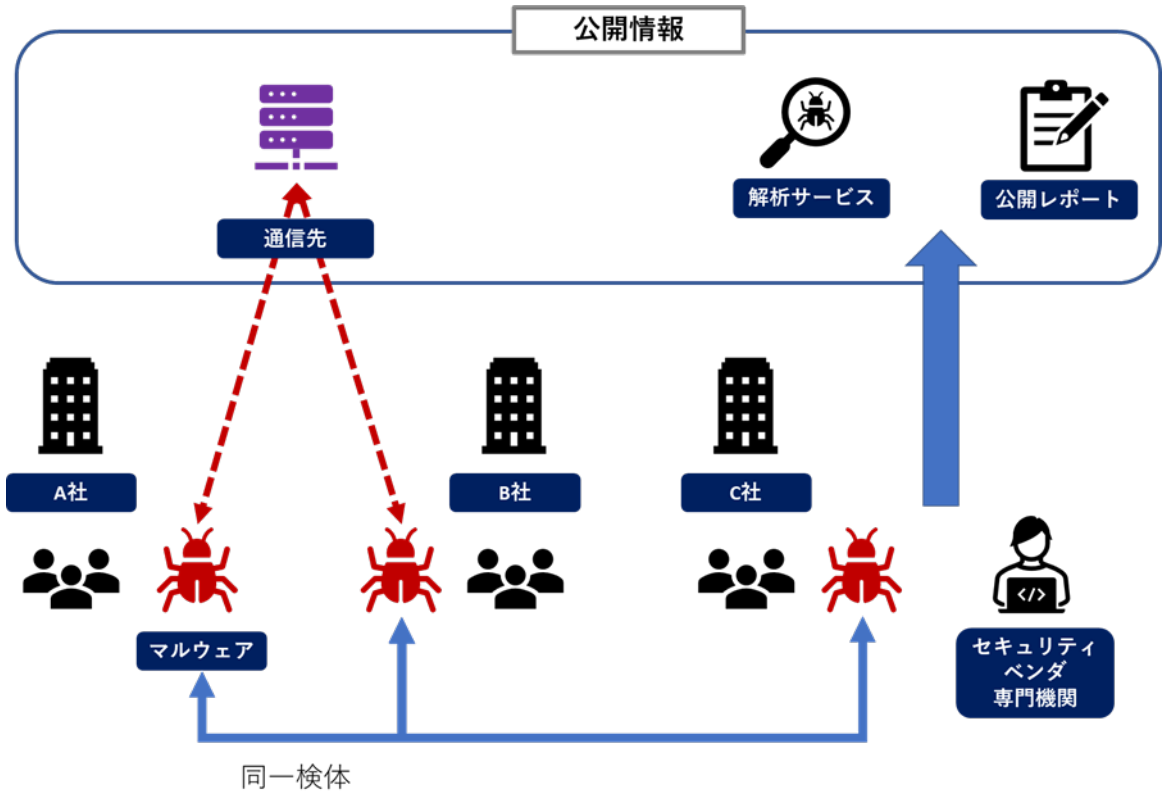
また、攻撃には特定の製品の脆弱性が悪用されていた場合、情報共有活動を通じて攻撃手法を解明することで、悪用されている製品の脆弱性を見つけ出し、当該製品の修正を行うことで攻撃手法を無効化することが可能である。逆に、個別の被害は発覚しており公表などで社会的に認知されているが、情報共有が不十分であるがために攻撃元や侵害原因が解明・解消されず、攻撃活動が延々と継続してしまうケースがある。

以上３点から、情報共有活動には共有活動効果のためだけでなく、攻撃手法の全容解明という根本的な攻撃対処の観点からの意義が大きく、そのためにもタイムリーな情報提供・共有が重要であると言える。

３．２　情報共有における技術情報とコンテクスト情報～被害者保護の観点から～

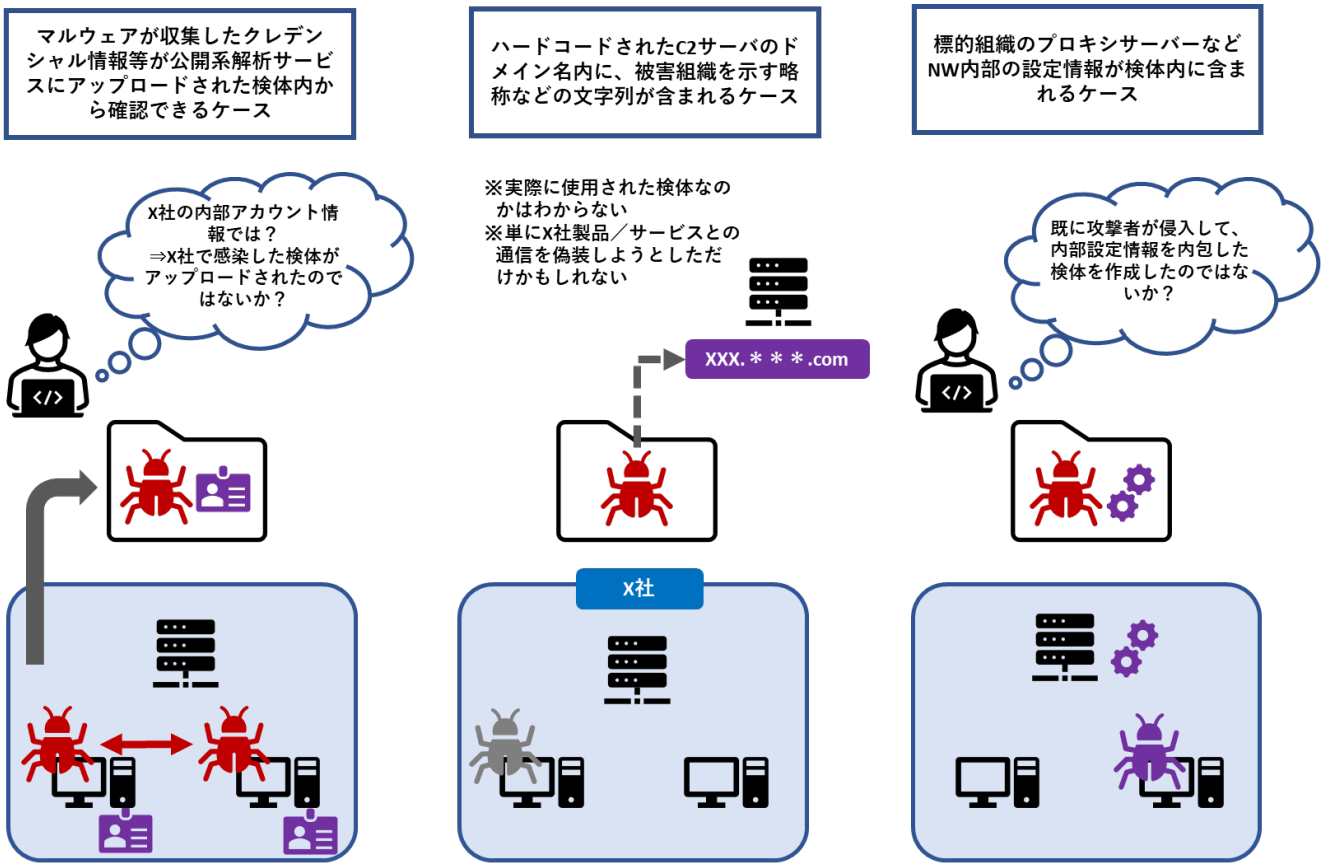
①　技術情報

技術情報は情報共有にとって、被害拡大防止のためにも、また全容解明のためも必要な情報であるため、積極的に共有されることが望ましい。また、マルウェアや通信先情報が外部に伝わったとしても、当該被害組織にただちに結び付く情報ではないから、公表前の段階において、調査に当たっているセキュリティベンダーや専門機関を通じて情報共有活動に匿名で提供することができる。



［図９：技術情報の共有］

ただし、以下に示すケースのように、検体解析等から被害組織が「推測」される場合もあるため、注意が必要である。こうしたリスクがあるため、外部に情報提供する際には専門機関やセキュリティベンダーを通じて行い、以下のようなケースに該当しないかどうか確認が行われた方がよいと考える。



［図 10：技術情報のうち、被害組織が推測されるケース］

② **コンテクスト情報**

コンテクスト情報が意図せず外部に知られた場合、情報の内容には当該組織固有の事情を多分に含むことから、非公開であるはずの被害組織名が推測されてしまう恐れがある。

また、コンテクスト情報とはサイバー攻撃の「結果」を示すものであり、攻撃の方法そのものを示すものではないことから、攻撃の「影響」を伝えることはできても、攻撃を防ぐための「どのような攻撃か」を示すことができない。したがって、基本的には被害拡大防止のための情報共有活動に資する情報ではないと言える。

ただし、どのような規模の影響があるのか示すことは、特に二次被害防止のための注意喚起や、原因となる箇所の対処を直ちに求める注意喚起をすることにおいては有効である。しかしながら、その場合も、特定企業の被害を示すことではなく、「どのようなシステムからどのような種類の情報が漏えいするのか」など、被害個社が特定されない、技術的な情報として伝えられるべきであることと、２．３で整理のとおり、公表までの早期の段階で示されることが望ましいことから、専門機関やセキュリティベンダー等を通じて、匿名化された上で取り扱われるべきである。

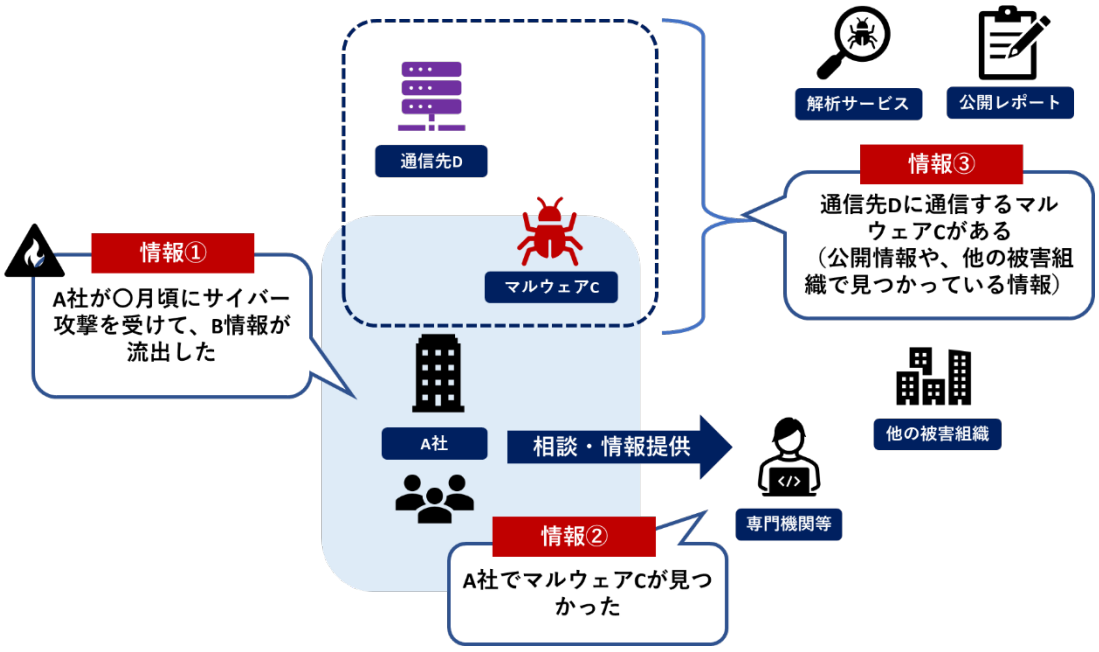
③ **秘匿することの利益と共有することの利益**

コンテクスト情報と技術情報のそれぞれの扱い方については、「秘匿することの利益と共有することの

利益との比較衡量」[9]で整理が可能である。

下記図 11 の情報①はコンテクスト情報であるが、少なくとも公表前のタイミングにおいて、世間一般に対して非公開にしておきたい情報であり、２．２で整理したとおり、公表前に意図しない形で情報が知られてしまうことで、被害組織が不利益を被るような情報である。したがって、少なくとも公表までの段階においては、秘匿することの利益が優先されるだろう。また、情報②も①に似ているが、これは A 社と専門機関との関係性において非公開が求められている情報である。

情報③は、情報②と分離ができるのであれば、例え当該時点で公表となっていないものであっても、共有することの利益が優先する情報である。むしろ、公表するタイミングに至っては、２．３で述べたとおり、被害拡大防止に資する可能性が低くなる。こうした情報は公表前の早期において、その利益が最大化される。



［図 11：秘匿することの利益が優先される情報と、共有することの利益が優先される情報の例］

前述のとおり、情報共有は可能な限り速やかに行うことが望ましい。しかし、被害の公表前のタイミングにおいては、当該共有される情報から特定の組織名等が推測されないことが望まれるため、共有される対象としては技術情報が中心となる。一方で、情報の公表のタイミングにおいては影響範囲や、これまでにどのような対応が行われ、二次被害防止策が行われているのか説明されることが多いことから、コンテクスト情報が中心なる。

---

[9] 高畠健一「秘密保全制度に関する概念的考察―「秘匿の利益」と「共有の利益」のバランス―」（『情報史研究』第 8 号, 2016 年 9 月）

そのほか、情報の秘匿性については、「対世的秘匿性」を示す secret と情報の授受当事者間の関係性の中で価値が判断される、confidential との区分も参考となる。（林紘一郎「情報法のリーガルマインド」（勁草書房　2017 年 2 月）96 頁）

次項では、情報共有が効果的に行われない実態について、それぞれの背景や課題ついて検討するとともに、望ましいと考えられる対応を記載する。

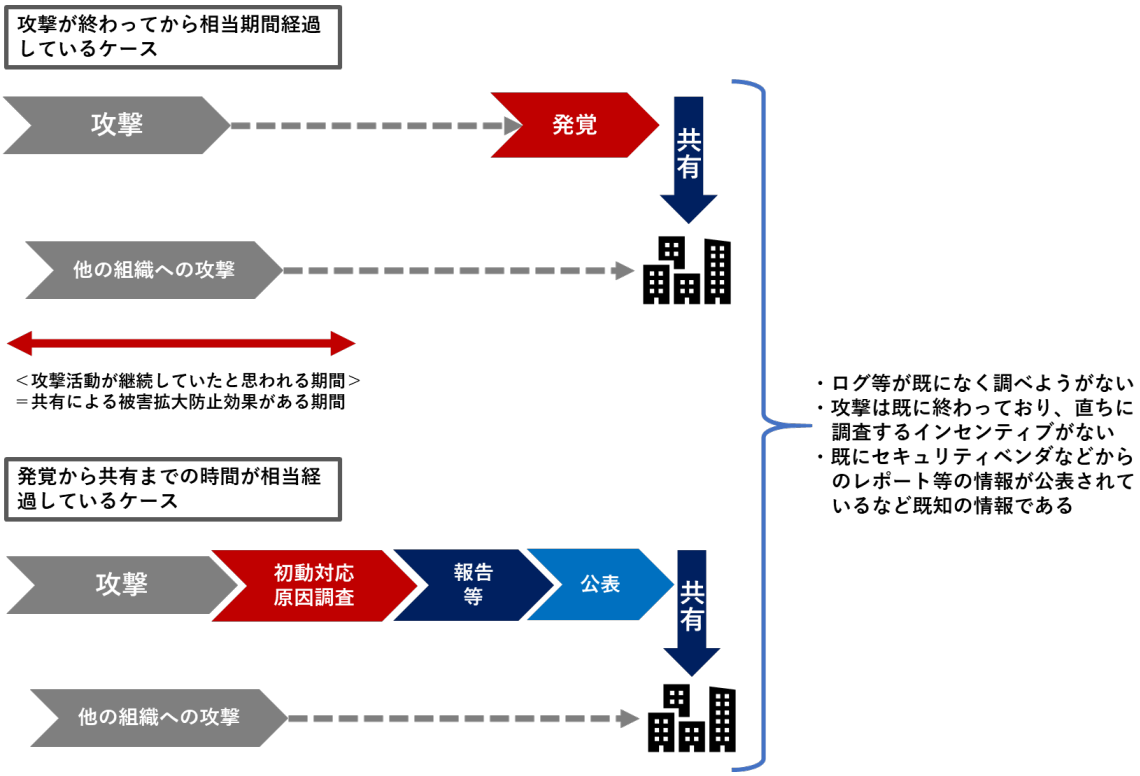
３．３　情報共有が効果的に行われない背景等

実態①　すでに攻撃から長期間経過し「共有効果」が乏しい情報が共有されている

情報共有の効果は３．１で説明したとおりだが、被害拡大防止を目的とした情報共有が効果的に行われるためには、まだ（被害発覚組織以外の）他組織向けの攻撃が行われている／攻撃活動自体が継続する可能性が高いと想定されるタイミングが重要である。

一方で、実際に行われている情報共有の中には、下記図のように、「攻撃が終わって相当期間経過」してしまっているケースや、発覚から共有までに相当の期間が経過してしまい、すでに共有効果が見込めないものが多く存在してしまっている。特に被害の公表前後で外部への情報提供／共有が行われるものについては、より早期のタイミングである発覚直後に情報共有できていた場合、その情報共有効果が見込めた可能性がある。

したがって、被害組織から専門機関や情報共有活動への情報共有は、被害事実の公表と同じタイミングで行われるのではなく、攻撃被害発覚後のより早期のタイミングで行うことが望ましいと考えられる。



［図 12：時間経過により共有効果が乏しい情報］

実態②　公表が「他組織への注意喚起／情報共有」に繋がるとは限らない

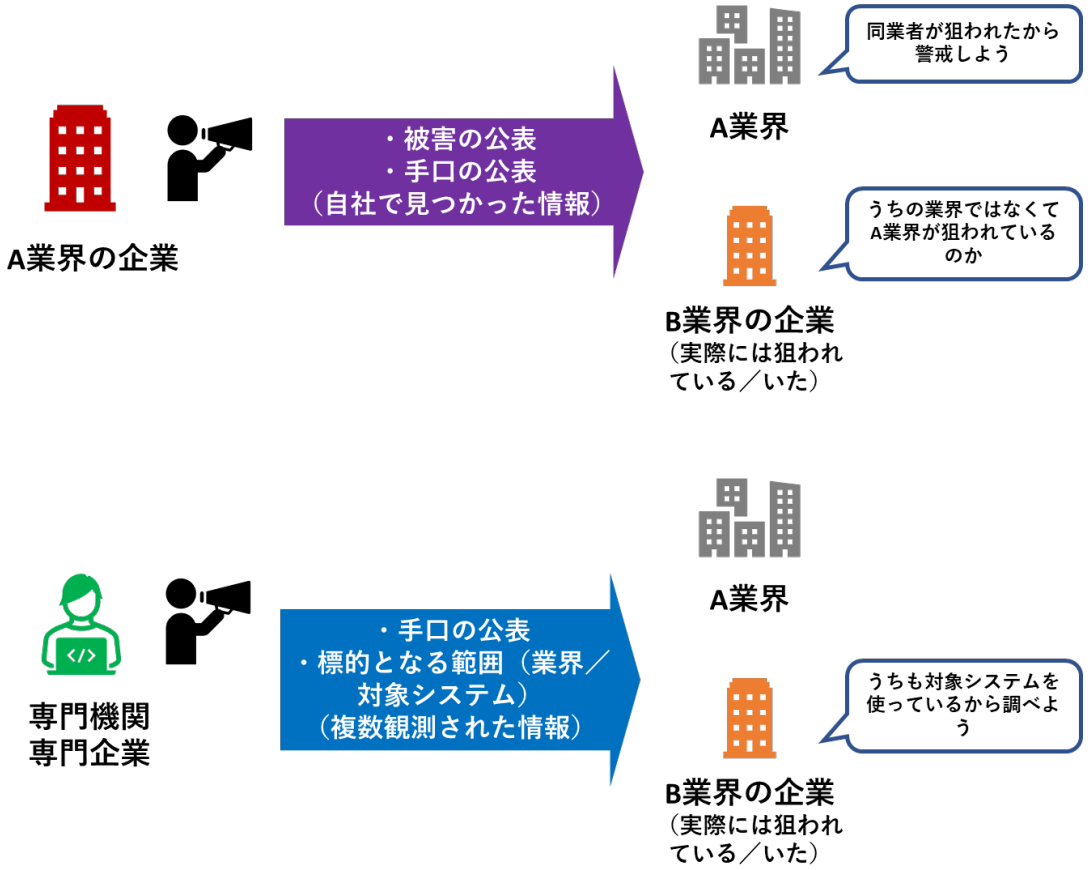
サイバー攻撃被害を速やかに公表することの意義について、公表することにより直接的に第三者への注意喚起／情報共有に繋がるとの議論もある。しかし、実態①で解説のとおり、公表被害組織が被害事実を公表するまでには、どうしても一定度の時間がかかる以上、「公表による情報共有」方式は情報共有に

適切なタイミングを逃しやすい傾向があると言える。

また、3．1で解説のとおり、単一の被害組織から公表される情報は基本的には当該単一の被害組織で見つかった情報で構成されるため、必ずしも攻撃手口の全容を掴んでいない可能性がある。

さらに、下記図のとおり、特定の企業から発信された情報は受け手に対して「その企業または特定業界が狙われた」というバイアスを与えてしまう可能性があるため、共有効果、注意喚起効果が正しく発揮されない恐れがある。

こうしたことを踏まえれば、被害組織が行うサイバー攻撃被害に関する第三者への注意喚起については、2．1の整理を踏まえつつ、公表ではなく、情報共有を通じて行う方が効果的であると考えられる。



［図 13：単一の被害組織から公表される情報と専門機関から提供される情報］

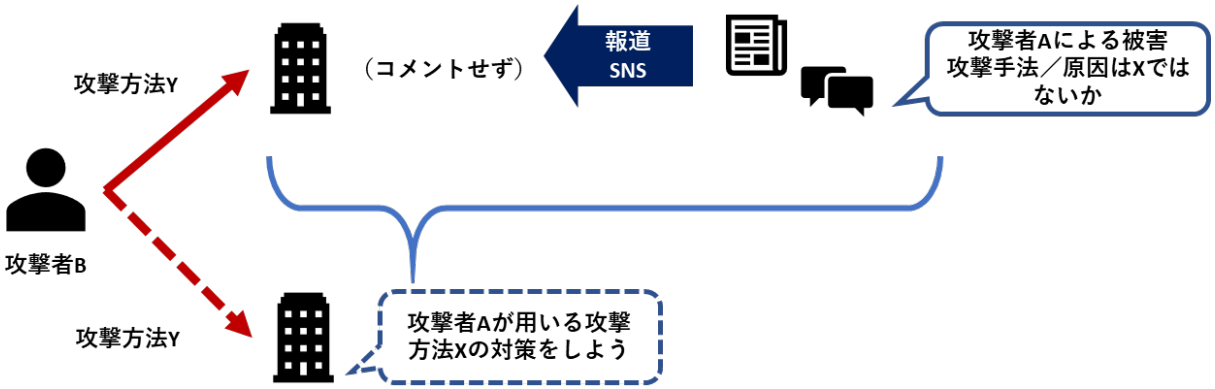
実態③　脅威に対する誤った情報が拡散する

攻撃被害の公表／報道後、被害組織が公表していない情報、例えば攻撃グループ名であるとか攻撃手法、侵入原因に関する憶測が報道や SNS 上で飛び交うケースがある。特に、被害組織が公表前に外部組織に対して適切な情報共有等を行っていない場合、専門機関等から正しい情報が発信されることがなく、公表後に意図せず流れてしまう誤った情報を他の組織が対策の参考としてしまい、適切な対策を取れなくなったり、攻撃被害を見逃す恐れがある。

一度誤った情報が不特定多数に拡散してしまうと、その訂正には多大なコストがかかるとともに、訂正することはかなり困難である。

したがって、攻撃被害を公表する場合には、事前に可能な限り専門機関に技術情報等の共有を行うこと

が望ましいと考えられる。



［図 14：情報共有をしないことにより、誤った情報が拡散されるケース］

４．公表のための視点

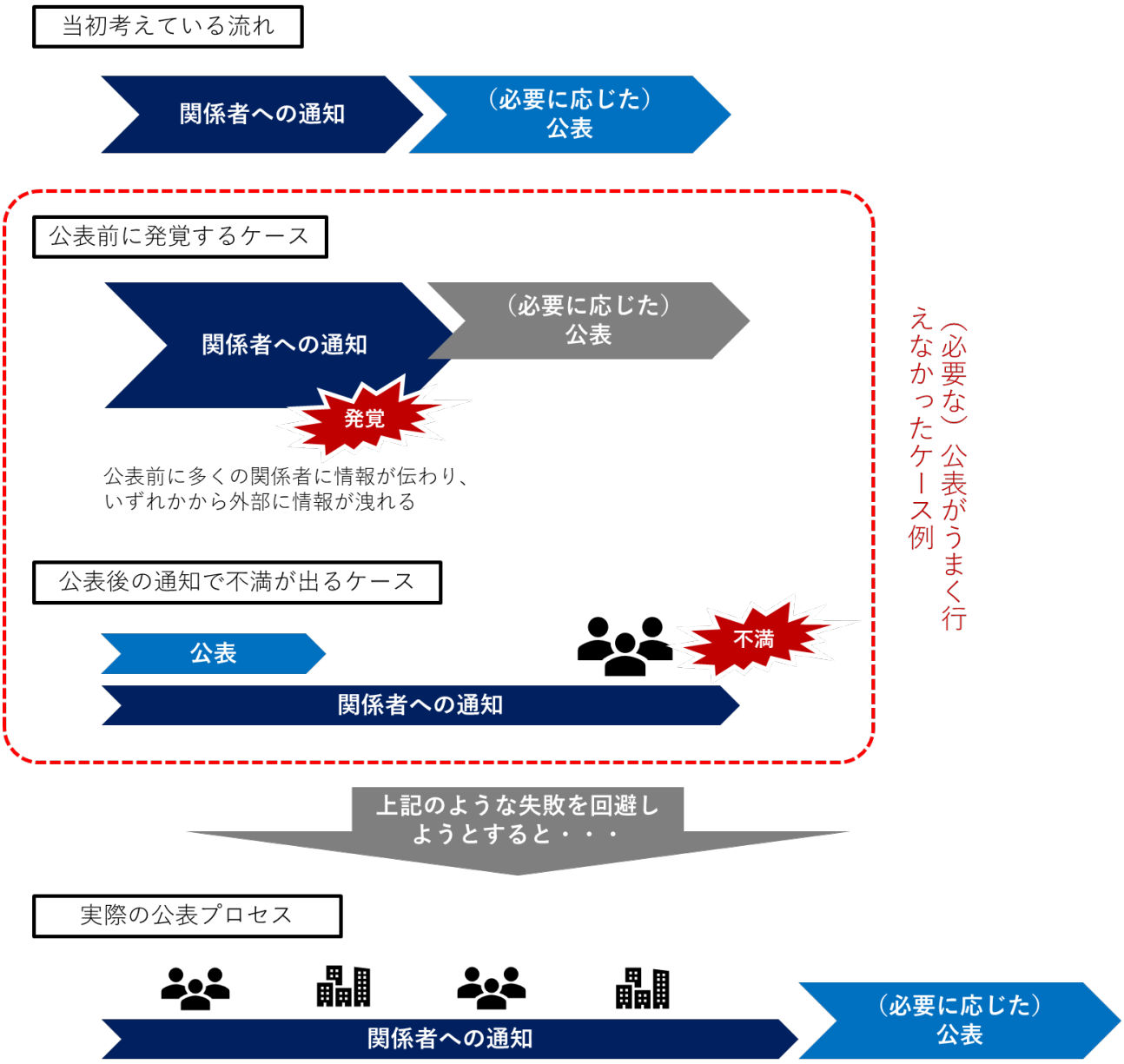
４．１　公表が遅くなる合理的事情

被害組織からの被害事実の公表が遅い、として、メディア等でネガティブに取り上げられることがあるが、公表のタイミングが遅くなる背景には、以下のような合理的事情があると考えられる。ここまで述べたように、攻撃者の動向を踏まえた初動対応や原因究明、被害範囲確定までに相当の時間を要することから、事案発覚から公表までの「なぜそれほどの時間がかかったのか」対外説明をすることで、実態にそぐわない評価を受けるなど、レピュテーションリスク対策にも繋がると思われる。

実態①　利害関係者への通知が済むまで公表ができない

被害組織では、被害事実を公表する必要があると判断した場合でも、一般への公表前に利害関係者に事実関係を通知し、事情を説明することを目指すと考えられる。しかしながら、通知／説明した先の利害関係者から被害情報等が漏えいする恐れから、この説明・通知は、可能な限り、公表の直前に行うことが目指される。

しかしながら、実際には、利害関係者に被害事実の通知・説明を行うためには、平時の利害関係者の担当だけでなく、被害組織のセキュリティ部門／情報システム部門のリソースが必要になる場合も相当程度想定される。こうした場合、説明リソースの限界などから、公表前の利害関係者への通知・説明に時間がかかってしまい、結果的に公表が遅れることになる。



［図 15：関係者への通知と公表タイミングの遅れ］

実態②　実際は必要な対応（専門機関への相談・情報提供等）は行っているが、利害関係者への通知や一般への公表は情報の精査の都合上、遅れがちになる

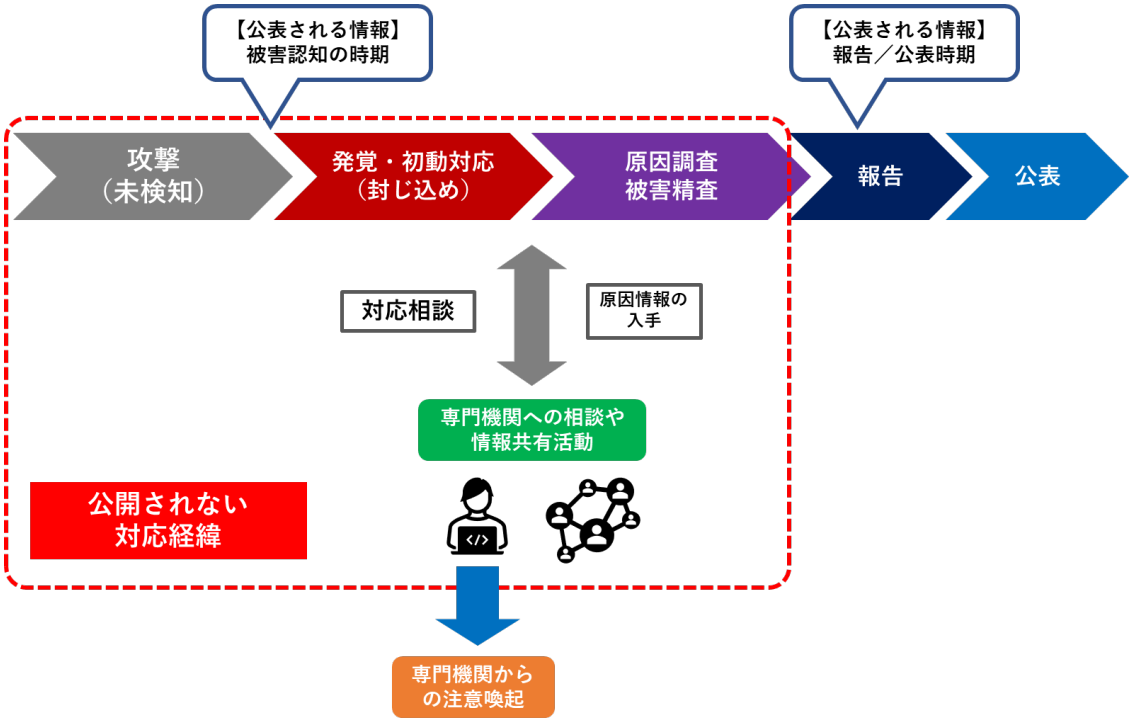
多くのケースでは、被害範囲が確定し、漏えい情報の詳細が判明してから利害関係者への連絡や一般への公表が行われる。

攻撃発覚後の初動段階では、まだ攻撃者が組織内部に侵入している前提であるため、攻撃の「封じ込め」が行われなくてはならず、そのためには「どのように侵入されたのか」原因特定が必要となる。しかし、この原因特定には一程度の時間がかかることが多い。

また、封じ込めや原因の特定と応急処置対応ができたとしても、その後「どこまで侵入され、どのような情報を閲覧／窃取されたのか」という影響範囲を調査することも技術的に困難なケースが多く、したがって、攻撃の「封じ込め」と影響範囲調査を経た後の利害関係者への通知／説明や一般への公表までに

は、相当の期間を要することになるのである。

原因調査や侵害範囲の調査が難航する・時間がかかる背景としては、主に標的型サイバー攻撃では攻撃者が検知回避のために戦術や使用するマルウェア、攻撃ツールを日々進化させていることが挙げられる。



［図 16：公表される情報と公開されない情報］

実態③　そもそも公表が必ずしも求められていない事案を公表している

サイバー攻撃被害に係る公表については、２．１で挙げたとおり、個人情報の漏えいや影響範囲を踏まえてその必要性が判断されるものである。他方で、２．１の観点からは、必ずしも公表が求められていない様態であっても、被害事実を通知・説明した関係者から被害事実がコントロール不能な形で第三者にリークされる懸念もある。被害組織は、こうしたコントロール不能な形でのリークを防ぐために、予防的措置として積極的に公表を行っている場合も多い。

この場合も、【実態②】で説明のとおり、一般への公表は、原因調査や影響範囲調査、情報漏えい有無の調査が完了してから行われるため、攻撃発覚から相当の期間を経て公表されることとなる。

［表 2：被害の程度に応じた所管省庁への報告・公表の根拠となる法令等］

<table>
<tr><th></th><th colspan="2">情報漏えいあり</th><th>情報漏えいなし／サービス停止あり</th><th>左記のいずれもなし</th></tr>
<tr><td rowspan="5">所管省庁等への報告</td><td colspan="2">個人情報漏えい（個人情報保護法）
※2021 年 6 月以降義務化</td><td>各業法による事故報告</td><td rowspan="5"></td></tr>
<tr><td colspan="3">【総務省】電気通信事故報告制度（電気通信事業法第 28 条、電機通信事業法施行規則第 58 条）※「送信型対電気通信設備サイバー攻撃」に限定される
【経済産業省】一定の電力供給障害があった場合の報告（電気事業法 106 条、電気関係報告規則 3 条）
【団体】クレジットカード番号漏えい時の報告（クレジットカード番号等の適切な管理に関する自主規制規則 20 条）
【金融庁】主要行等向けの総合的な監督指針</td></tr>
<tr><td></td><td colspan="2">【防衛省】
装備品等及び役務の調達における情報セキュリティの確保に関する特約条項
（情報の漏えい、紛失、破壊等の事故時）</td></tr>
<tr><td></td><td colspan="2">【経済産業省】
「基本行動指針（共有・報告・公表）」
機微技術情報の流出懸念がある場合の経済産業省への報告</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>FD ルールに基づく情報開示</td><td colspan="4">上場企業における、重要情報（「公表されれば有価証券の価額に重要な影響を及ぼす蓋然性のある情報」）として、FD ルール上の公表義務が発生するケース</td></tr>
<tr><td rowspan="2">公表</td><td colspan="2">個人情報の保護に関するガイドライン（令和 2 年度法改正に基づく新ガイドライン）
「漏えい等事案の内容等に応じて、二次被害の防止、類似事案の発生防止等の観点から、事実関係及び再発防止策等について、速やかに公表することが望ましい。」</td><td>（※各業法においてサービス停止やその原因を広く利用者に伝える必要がある場合）</td><td rowspan="2">※ガバナンスの一環として公表を判断する場合

※自社 HP の改ざん、自社メールサーバーからスパムメールが配信されるなど顧客や第三者に被害が出る恐れがある場合</td></tr>
<tr><td></td><td colspan="2">【経済産業省】
「基本行動指針（共有・報告・公表）」
（昨今の産業を巡るサイバーセキュリティに係る状況の認識と、今後の取組の方向性についての報告書）
【総務省】
「我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項[緊急提言]」</td></tr>
</table>

４．２　被害組織が被害事実を公表する際の判断

被害組織が被害事実の公表を検討する際は、以下のような各視点を踏まえることが有用と考えられる。

①　個人情報漏えい時における二次被害／類似事案防止のための注意喚起／情報共有目的の公表

「個人情報の保護に関する法律についてのガイドライン（通則編）」[10]においては、「3-5-2 漏えい等事案が発覚した場合に講ずべき措置」として、個人情報漏えい時においては「個人情報保護委員会への報告（法第 22 条の 2 第 1 項関係）」と「本人への通知（法第 22 条の 2 第 2 項関係）」が必要となるが、さらに、「漏えい等事案の内容等に応じて、二次被害の防止、類似事案の発生防止等の観点から、事実関係及び再発防止策等について、速やかに公表することが望ましい」と示されている。

すなわち、公表が法的義務とされないケースでも、本人への個別通知では時間的に二次被害防止に間に合わない恐れがある場合や、個別通知では大半の利用者に情報が伝わらない状況が想定される場合は公表をもって広く注意喚起することが選択肢として挙げられていると解釈できる。これは、２．１で分析した総務省や経済産業省の公表文書等から導かれる考え方とも整合的である。

また、「類似事案の発生防止等の観点から」とある点については、前述の短期的な被害防止だけでなく、中長期的な被害防止も考慮されていると考えられる。例えば類似の原因によって他組織でも漏えい事象が発生しないよう、一般利用者を含めた社会全体の知見として、原因や防止策を広く知らしめるためであると考えられる。

②　被害情報の公表と対策知見共有目的の公表の切り分け

制度上の理由や顧客／取引先などへの二次被害防止目的のほかに、情報共有目的や対策知見（ノウハウ）共有目的の情報公表が必要との意見が散見される。ただし、これは目的と手段が混同しているのではないかと考えられる。

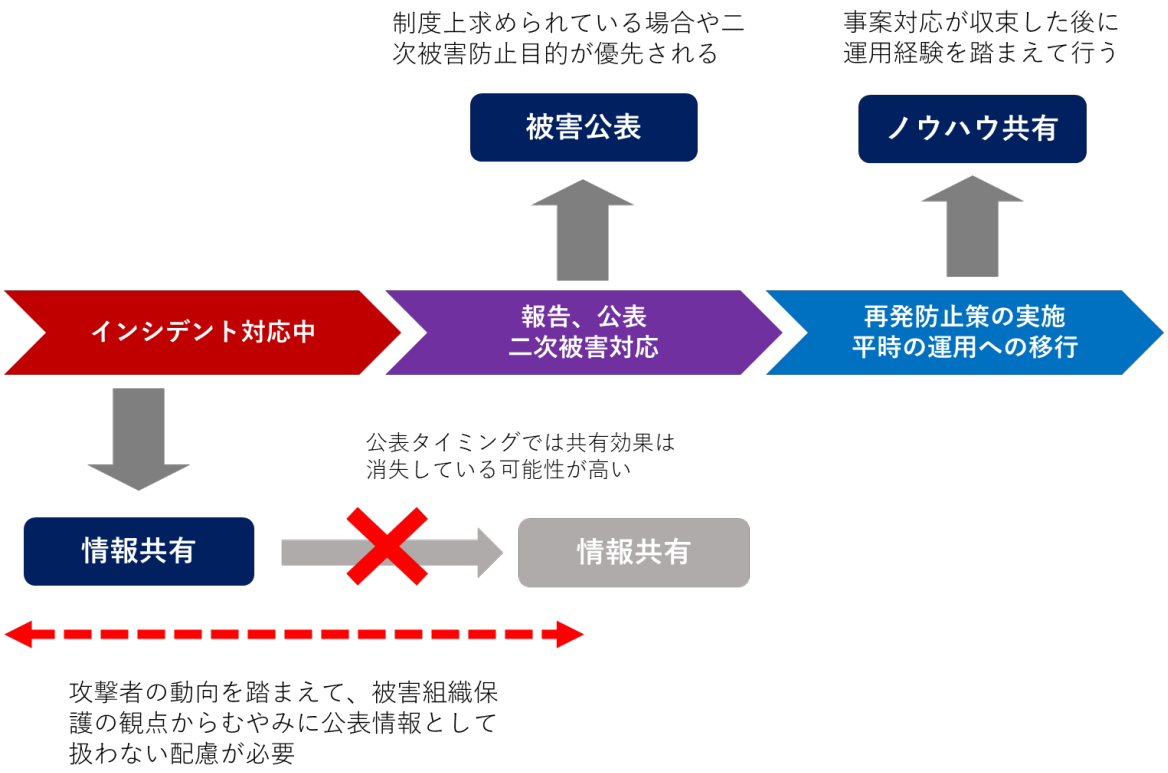
まず情報共有については前章で述べたとおり、「(可能な限り早い) 適切なタイミング」での実施が必要条件であり、原因調査や被害範囲確認を待たなければならない被害公表まで時間が経過すると共有効果が著しく減衰する。

そして、インシデント対応のノウハウや再発防止策については、インシデント対応が収束し、実際に再発防止策などに着手されなければ伝えることができないものであるから、これは公表後に行われる方が適切である。

また、「ノウハウ共有」的な情報共有はインシデント対応を行った担当者や対応全体を指揮した経営層が講演、セミナー等で発表することも想定され、こうした活動は同業他社へのノウハウ共有という実務的効果だけでなく、社会に対して再発防止策に取り組む姿を伝える側面も有していると思われる。したがって、ある程度顧客や取引先対応などの事案対応全体が収束し、また、事案を受けて導入／強化された再発防止策の運用がある程度軌道に乗ったタイミングでなされるのが自然であろう。

---

[10] 参照：令和 2 年度個人情報保護法改正に伴う、個人情報保護法ガイドライン（通則編）の一部を改正する告示（案）（2021 年 5 月 19 日パブリックコメント「個人情報の保護に関する法律についてのガイドライン（通則編、外国にある第三者への提供編、第三者提供時の確認・記録義務編及び匿名加工情報編）の一部を改正する告示」等に関する意見募集について」）



［図 17：被害情報の公表と対策知見共有目的の公表の切り分け］

③　脆弱性悪用事案の注意喚起目的

特定製品の脆弱性が悪用された可能性がある場合、製品開発者から修正プログラムの提供がなされずに悪用事実が公表されてしまうと、さらなる悪用を誘発するリスクが高いため、一般的には、日本国内においては経済産業省告示「ソフトウエア等脆弱性関連情報取扱基準」[11]に基づき運用される早期警戒パートナーシップ[12]に基づいた対応が行われる。

サイバー攻撃被害情報との関係においては、インシデント対応を行ったセキュリティ専門企業から悪用された脆弱性に関する届け出が行われたり、同制度の調整機関でもある JPCERT/CC がインシデント対応のコーディネーションを行う中で認知に至るケースが想定される。

調整が行われ、製品開発者からの公表と修正プログラムの提供が行われ、はじめて専門機関からの注意喚起や被害組織からの注意喚起目的での同脆弱性悪用の言及がなされるべきである。ただし、同脆弱性の調整が被害組織の（同脆弱性以外の情報を含む）被害公表をなんら妨げるものではない。

4．3　被害組織保護の観点の必要性

サイバー攻撃被害に関する情報を公表するのは必ずしも被害組織だけとは限らない。調査を行っている専門機関や所管省庁などの行政機関、報道、リサーチャーや研究者などもその範疇に含まれる。

---

[11] https://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf

[12] https://www.ipa.go.jp/security/ciadr/partnership_guide.html

３．２①で示したように、被害組織からの公表前であっても、公開情報の分析から特定のサイバー攻撃被害の存在を推定する情報を得ることが可能である。また、組織内部からの情報漏えいやステークホルダー等からの情報漏えいにより、被害組織の意志に沿わないタイミング・形態で被害情報が公表前に公になるケースが後を絶たない。

注意喚起目的や二次被害防止のための情報共有や公表については、第 3 章や４．２で示した通りであるが、これ以外の何らかの目的で被害組織以外の第三者が特定のサイバー攻撃被害に関する情報を扱う場合、以下の観点への配慮が必要である。

① 攻撃者動向を踏まえた公表

何らかの経緯で攻撃被害の認知に至った時点ではまだ攻撃者が被害組織の内部ネットワーク内に侵害中であるケースがある。その場合、攻撃者は自らが捕捉されたことに気付き、調査妨害を狙って攪乱行動や証拠隠滅、さらには報復的な攻撃を行う可能性が想定される。

攻撃者が自ら捕捉されたことに気付くケースとしては、潜伏させているマルウェアが削除されたり、テレメトリー的通信が消失するなどの技術的な場合が想定されるが、そのほかにメディア等で得た情報で気付くケースが想定される。

例えば、2020 年 10 月に米司法当局がロシア GRU 要員 6 名の刑事訴追を公表した事例では、2018 年のマルウェア「OlympicDestroyer」による攻撃直後、攻撃者たちが標的とした企業に関するニュースを探していたことが公訴事実として記載されている [13]。このケースでは、攻撃者は自らが被害組織に捕捉されたことを調べるというよりも、攻撃が成功したかどうか確認するためであったとも推測される。このように、攻撃者は被害組織からの発表や報道などの公開情報を用いて、自らの行動の結果の確認をしていることがわかる。

したがって、被害組織が被害を公表する場合、特に原因調査や被害確定前の第一報として公表する場合、最低限、攻撃者の“追い出し”や“封じ込め”ができていることが望ましく、また、被害組織以外の関係者は上記のような事情があり公表まで時間がかかることや、被害組織が意図しない被害情報の拡散が攻撃者の動向に与える影響を考慮すべきである。

なお、攻撃者、あるいは攻撃者に指示をしている主体がどの程度の期間において、公表情報をベースとした状況把握をしているのかは不明である。短期～中期的な活動において前述のような状況把握をしている可能性もあれば、より長期的な情報収集を行い、標的とする国・地域の対処能力を評価している可能性も否めない。標的型サイバー攻撃のような中長期間行われる攻撃活動にはまだ未解明な点が多い現時点においては、長期的にも被害組織に関する情報が保護されるべきと考えられる。したがって、攻撃動向次第では公表そのものを行わないというケースがあることの共通理解が関係者間に必要である。

② 「フェア・コメント（公正な論評）」の観点から

---

[13] https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

フェア・コメントの概念は報道の自由とプライバシー侵害の議論で用いられる概念であるが、事件や不祥事など公共の利害に関する事項が報道等を通じて広く世間一般の関心事として議論される場合の論点を示した法理[14]である。

被害組織が法令上求められた対策を行っていなかったことでサイバー攻撃被害にあい、大規模な個人情報漏えいや対外的なサービス障害など社会一般に二次被害を及ぼすような事象を起こしてしまった場合、これは個人情報保護法や各種業法に基づいた報告と何らかの行政指導／処分を受けることとなる。

ただ、そうした法令・制度上の処分範囲として明確にとらえきれない原因で社会に広く影響が及ぶサイバー攻撃が起きるかもしれない。その場合、そうした行政上の射程圏内にないからといって、なんら原因や再発防止が試みられないのではなく、広く社会的論議の元で再発防止に向けた対策が示される選択肢もあり得るだろう。

特に技術の進展が早い分野であることから、制度上の安全管理基準が必ずしも現状に追いつけているとは限らず、新たな攻撃手法が次々と出現する現状においては、広く被害事案が知られ、社会制度の改善に対する国民の合意を形成し、さらに対策について専門家からＩＴシステム／サービスの一般利用者まで広く知見／意見が集まることが望ましいと言える。

ただし、これはあくまで攻撃の全容が判明し、被害範囲が確定して顧客等の二次被害防止の措置が採られるとともに、同時に原因が特定され、被害組織自身の安全が確保された後という条件が必須である。

また、被害組織の運営体制的な問題やモラル的な問題が原因であった場合を除き、技術的な問題であった場合は、被害組織の個別情報は別として、純粋に技術的問題として分析され、注意喚起が発出されたり対策について議論されるべきものであるため、前述のような専門機関での分析や匿名化された上での知見共有がなされることが妥当であろう。

③　標的型ランサムウェア攻撃への対応

被害組織からの公表だけでなく、メディアなど周囲の関係者が被害情報の取り扱いに配慮が必要なケースとして、被害組織への脅迫タイプの攻撃を挙げることができる。

前述のように、被害情報の公表が攻撃者の行動変化に影響を及ぼす可能性に類似するが、標的型ランサムウェア攻撃のように、被害組織を脅迫する攻撃の場合、被害認知（データの暗号化や脅迫メッセージの受信）時点でなお攻撃者は被害組織にフォーカスしており、被害組織の挙動に注視している状況にある。

標的型ランサムウェア攻撃は報道をはじめ、被害組織以外の関係者がどのくらい注目するか、という点を重視する攻撃である。特に「二重の脅迫」型と呼ばれる、データの暗号化に加えて、窃取した情報をリークサイトに掲載し、より脅迫効果を増強するタイプの攻撃では、リークサイトに世間の注目が集まる事象自体を悪用していると言える。また、攻撃者の中には当該被害組織を脅迫していることや、リークサ

14　「公共の利害に関する事項または一般公衆の関心事であるような事柄について、なにびとといえども論評の自由を有し、それが公的活動とは無関係な私生活暴露や人身攻撃にわたらず、かつ論評が公正であるかぎりは、いかにその用語や表現が激越・辛辣であろうとも、またその結果として、非論評者が社会から受ける評価が低下することがあっても、論評者は名誉棄損の責任を問われることはないとする法理である」山川洋一郎「報道の自由」（信山社　2010 年）116 頁

イトの存在、データ窃取の事実をメディアに自ら伝えて報じさせることで情報拡散≒脅迫効果の増幅を狙う者まで現れている[15]。

以上で述べたとおり、被害情報の公表にあたっては、被害組織自身だけでなく、被害情報の流通／拡散に関わる多くの関係者が、そうした情報発信／拡散すること自体において、二次被害防止の観点と被害者保護の観点から、一程度の配慮がなされるべきである。

[15] 2021 年 5 月に発生した NZ の医療機関を狙った攻撃では、攻撃者が窃取したデータをメディア各局に送り付けたところ、各メディアはこれを報じない判断を行った。また、当局も当該事案が身代金目的かどうかも明らかにしていない。
https://jp.reuters.com/article/newzealand-cyber-idJPKCN2D707Z

５．事例分析

本調査にあたって、国内外の複数のインシデント公表事例について分析を行っているが、その中から公表より前の時点における被害組織の活動について、プレスリリースほか公開情報から判明している以下2事例を抜粋し、ここまで示した観点での整理を行う。以下の2事例を取り上げるのは国内・海外被害組織や関係省庁等の対応の良しあしを比較するものではなく、被害公表以前の情報共有などの対応がどのように行われたのか、制度の異なる国内外の事例を取り上げたものである。

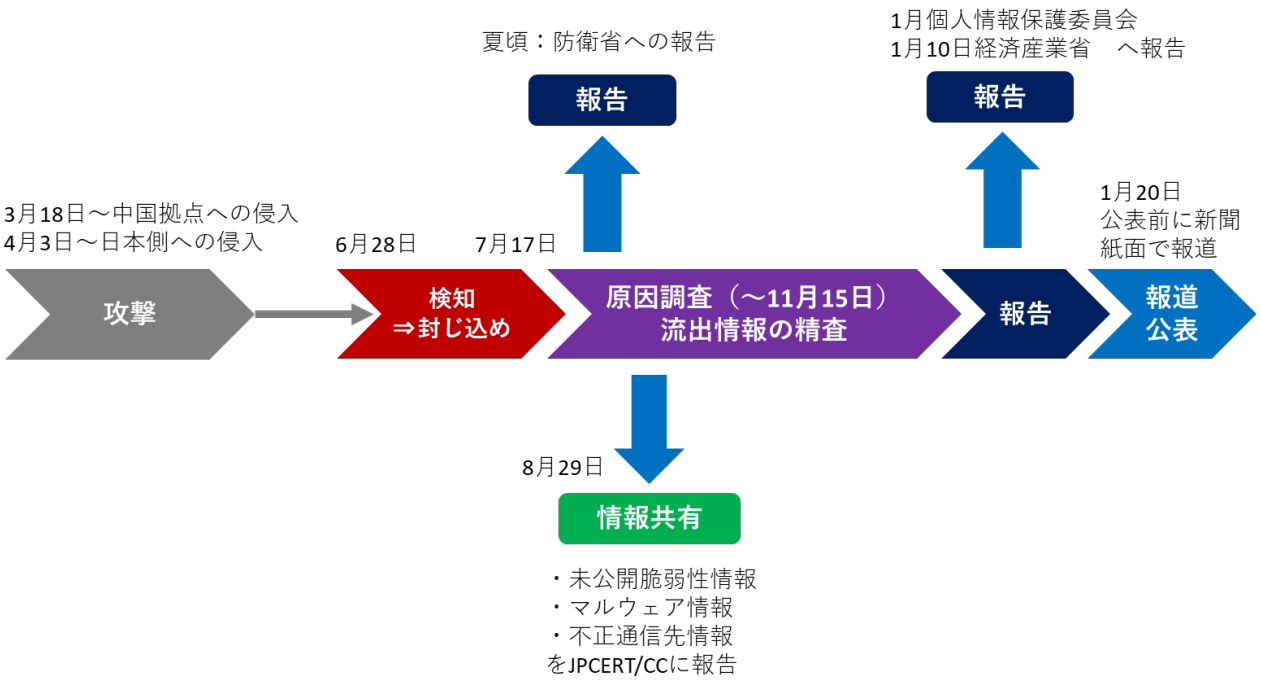
事例分析（国内事例）：三菱電機への標的型サイバー攻撃事案（2020年1月公表）

本件は被害組織からの公表前に報道がなされた事案であるが、公表に至る経緯が当該被害組織自身から公表されているため参考事例として以下のとおり整理する。

【公表前の情報共有】
原因調査が開始されたあとJPCERT/CCにマルウェア情報、不正通信先情報、悪用された可能性のある未公表の脆弱性情報の報告を行っている。
⇒「技術情報」の共有と「脆弱性情報」の公表前の情報提供がなされている

【公表までに行った作業の説明】
発覚から原因調査までの経緯を時系列で説明。また、漏えい情報の確定に至る経緯と判断理由を掲載（2020年2月12日　第3報）。
⇒「コンテクスト」情報が公表時に示されている

【その他】
当初の報道で「防衛、電力、鉄道」に関する情報が漏えいしたと報じられた点について、電力・鉄道などの社会インフラに関する機微な情報は漏えいしてないとした一方、防衛関連情報については当初漏えいを否定したものの（2020年1月20日　報道後の第一報）、公表後の調査で防衛省が定める「注意情報」が流出した可能性のある情報に含まれていたとして訂正した（2020年2月10日　第2報）



［図 18：三菱電機事案の対応時系列（公表情報および報道情報を元に作成）］

事例分析（海外事例）：Solarswinds 事案（2020 年 12 月発覚・公表）

本件は後述のとおり、特定製品の配信経路が悪用された、いわゆるサプライチェーン攻撃であり、広範囲に影響が及ぶ可能性があったところ、当該事実（配信経路経由での感染）と攻撃を分析した情報（技術情報）が広範囲への共有として注意喚起目的で公表された案件であった。

各被害組織における原因調査や被害範囲特定を待たず、潜在的な被害組織が認知できるよう、また原因調査が行えるよう、速やかに情報共有が行われたものである。

【公表前の情報共有】

本件は正確な発覚日は不明なものの、①Solarwins Orion Platform のアップデート配信経路の悪用、②広範囲に及ぶ被害範囲、が想定されたため、ただちに①の回避策や修正対応が準備され、公開と同時に未確定ではあったものの②の点を鑑み、現時点で判明しているマルウェア情報、不正通信先情報が注意喚起目的の公開として、急ぎ共有されたと解釈できる。

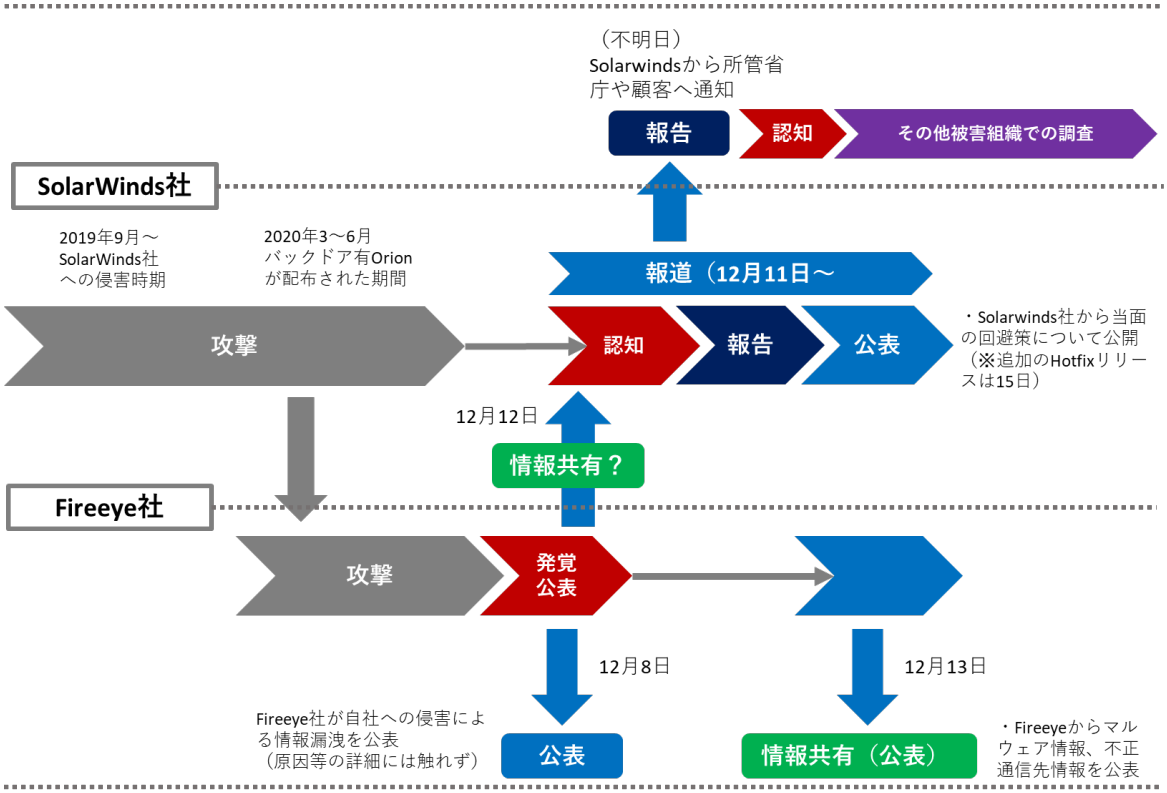
【公表までに行った作業の説明】

Solarwinds 社自身は同社製品のアップデート配信経路が悪用され配布されたマルウェア「SUNBURST」について「12 月 12 日（※どの標準時か不明）に知らされた」と公式ブログで表明している。

また、13 日に Fireeye 社が攻撃について分析レポートを公開した時点では、Solarwinds 社からは同事案に対応した修正版はまだ用意されておらず、暫定的に汚染されていないバージョンへのアップデートが案内され、また、事案に対応した Hotfix は 15 日公開予定である旨が示されていた。

【その他】

Orion は基本的には法人が使用するソフトウェアであるため、理屈上は Solarwinds 社（メーカー）が各ユーザー個別に連絡すればよいのであるが、広範囲の組織が攻撃の標的である可能性や、攻撃の脅威度合いを鑑み、個別通知だけでなく、広く注意喚起目的の公表がなされた。また、本件については、米国の株式公開企業に義務付けられている、重要事項に関する報告（Form 8-K）が被害公表と同日付で米国証券取引委員会（SEC）のホームページから公開された。



［図 19：Solarwinds 事案の対応時系列（公表情報を元に作成）］

［表 3：国内／国外事例の比較］

	情報の共有	製品の脆弱性情報	自社サービスの悪用に関する情報	公表
【国内】 三菱電機へのサイバー攻撃事案	初動対応後、事案の公表までに実施	非公表で専門機関に調整依頼	—	公表前に報道がなされた
【海外】 Solarwinds 事案	公表とともに実施	—	影響のあった法人ユーザーへの通知とともに、公表による注意喚起	公表前に報道がなされた

6．考察

以上、「(被害) 情報の公表の遅れ」批判という事象を端緒に、被害情報の共有と公表のあり方について整理を進めてきた。本稿では、サイバー攻撃にかかる情報の対外発信について、「共有」と「公表」という概念を分け、それぞれを整理した。そして、サイバー攻撃にかかる情報を「技術情報」と「コンテクスト情報」に分類した。また、被害企業が外部に被害関連情報を提供する行為には、インシデント対応の時系列に沿って目的の変化（共有⇒公表）と、扱うべき内容の変化（技術情報⇒コンテキスト情報）があることが整理できた。

したがって、本稿としては、時系列に沿って、「情報の整理」(「技術情報」「コンテクスト情報」) と「タイミング」(「情報共有」と「公表」) がそれぞれ区別され、取り扱われるべきであると考える。この観点からここまで検討した点をまとめると以下のとおりである。

【目的に応じた情報の整理】

- 被害情報はマルウェアや不正通信先など被害組織固有のものでない「技術情報」と、被害組織固有の対応経緯や被害内容といった「コンテクスト情報」に整理することができる
- 「技術情報」と「コンテクスト情報」が混在したままでは速やかな共有は行えないため、被害組織が特定されにくい「技術情報」がまず速やかに情報共有されるべきである
- 法令で定められたものやその他二次被害防止等の理由がない場合、攻撃者の動向を踏まえた被害組織保護等の観点から、公表や第三者による情報の拡散を行うべきでないケースも存在する

【タイミングの観点】

- 公表前の「情報共有」と取引先や所管省庁への「報告」、そして「公表」の 3 つに分かれており、それぞれ適切な順番とタイミングがある
- 「情報共有」は可能な限り速やかに行われなければその共有効果が時間の経過とともに減衰してしまう
- 「報告」「公表」は原因調査や影響範囲調査に時間がかかることから、被害認知後相当の期間を経過しなければ行えない
- 「情報共有」目的の「公表」は共有までの時間がかかりすぎるため、共有効果に乏しい

【上記の例外】

- 広範囲に影響を及ぼす可能性がある場合や、速やかに知らしめなくては二次被害を防ぐことができない場合、共有目的での公表が注意喚起的に行われる
- 未修正の脆弱性情報は製品開発者との調整前に第三者に情報共有されたり、公表されるべきではない

本稿による整理の結果を表にまとめると次のとおりである。

［表 4：情報の整理］

	情報の種類	情報共有のタイミングで望ましい情報	セキュリティ専門企業や専門機関からの注意喚起	公表のタイミングで望ましい情報
コンテクスト情報	対応の経緯	△ 特段の事情がない限り不要 ただし、早期の検知のために必要な情報であれば有効	×	◎ （公表前の）情報共有活動や専門機関等への相談など、公表までの期間で適切な対応を行っていたことを説明
	被害内容	×	△ 匿名化した上で、攻撃のインパクトを伝える場合有効	○ ※詳細については取引先等関係者への報告において優先 ※その他法令等で定められている場合は必須
	攻撃時期	◎	◎	○
	攻撃手法（TTP）	◎	◎	○ 対策とのセットで示されればノウハウ共有としての効果はある
	攻撃手法（悪用された脆弱性や踏み台となったサービスなど）	◎ ※未修正の脆弱性の場合は脆弱性告示制度での対応が優先	◎	△ すでに攻撃活動が終了して一定期間経過している場合、公表による効果は特にない
技術情報	マルウェア 通信先 （IoC）	◎ ※被害組織を示す情報の有無の確認が必要	◎	△ （同上）

サイバー攻撃被害については、ただやみくもな「情報の公表」だけでなく「情報共有」や「注意喚起」

の重要性も社会的に広く認知されている。一方で、そのタイミングや情報の具体的な中身についてはこれまでガイドライン等で明示的に示されてきたものではなく、被害組織ごとに都度判断されてきたため、社会全体で最大限の効果を発揮することができなかったのではないだろうか。さらには、ここまでに整理したような観点について、被害組織だけではなく、被害情報に触れる関係者間において共通理解として明示的に存在していなかったため、冒頭に触れた「公表の遅れ」といった、被害組織の不作為責任的な点での批判が行われてきたのではないだろうか。

したがって、今後の本テーマの検討にあたっては、サイバー攻撃被害情報の共有と公表に係る目安となるガイドラインとなる文書が必要であると考える。

その場合、被害組織だけではなく、サイバー攻撃被害情報に触れる可能性のある関係者が「被害者保護」と「攻撃対処」の観点から必要な対応と配慮ができるようなポイントが盛り込まれるべきである。