サイバー攻撃被害に係る情報の共有・公表ガイダンス

令和５年３月８日

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

目次

用語集.....3

用語集補足.....6

１．はじめに.....9

—情報共有とは何か／公表とは何か.....9
—なぜ「情報共有をするべき」なのか／公表の社会的意義.....13
—本ガイダンスのコンセプト.....17
—本ガイダンスの検討経緯.....20
—本ガイダンスのスコープ.....21
—本ガイダンスを読むにあたって.....27

２．情報共有・被害公表の流れ.....31

３．FAQ.....33

＜情報共有の方法等について＞

Q1.なぜ情報共有が必要なのですか？.....33
Q2.どのタイミングでどのような情報が共有／公表されますか？.....36
Q3.「被害組織」とは何ですか？.....37
Q4.サイバー攻撃被害に係る情報にはどのようなものがありますか？.....38
Q5.どうやって「情報共有」をすればいいのですか？.....44
Q6.どのような情報を共有すればいいのですか？.....47
Q7.「インディケータ情報」とは何ですか？.....51
Q8.いつ情報を共有すればいいのですか？.....57
Q9.情報共有活動に参加していない場合、どこに共有すればいいのですか？.....59
Q10.情報共有を行う上での留意点はありますか？.....62
Q11.攻撃技術情報の共有とノウハウの共有とは何が違いますか？.....64
Q12.専門組織同士はどういう情報を共有していますか？.....65
Q13.なぜ非公開で参加者が限定された情報共有が行われるのですか？.....67

＜被害の公表や法令等に基づく報告・届出について＞

Q14.公表の目的は何ですか？ 70
Q15.公表のタイミングはどのようなものがありますか？ 71
Q16 公表の内容としてはどのようなものがありますか？ 72
Q17.公表する際の留意点はありますか？ 76
Q18.警察への通報・相談は、行った方が良いでしょうか？ 83
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？ 85
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？ 86

＜被害組織の保護の観点について＞

Q21.公表していないのに自組織の被害が知られて公開されてしまうのはなぜですか？ ... 89
Q22.他組織の被害に関する情報を発見した場合、どうしたらよいですか？ 92
Q23.製品の脆弱性が悪用されていた場合、当該情報はどのように扱えばいいですか？ ... 94
Q24.他の被害組織を踏み台として攻撃された場合、当該情報はどのように扱えばいいですか？ 96
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？ 99

＜攻撃技術情報の取扱いについて＞

Q26.マルウェアに関する情報とはどういうものですか？ 102
Q27.不正通信先に関する情報とはどういうものですか？ 104
Q28.攻撃の手口に関する情報とはどういうものですか？ 106
Q29.専門組織から「見つかった情報を共有活動に展開してよいか？」と尋ねられたらどう判断すればいいですか？ 108
Q30.情報共有先をどのように指定／制限すればいいですか？ 109
Q31.専門組織から「分析結果をレポートとして発信してもよいか」と尋ねられたらどう判断すればいいですか？ 111
Q32.どのような攻撃技術情報であれば速やかに共有することができますか？（公開情報と非公開情報の違いについて）（※調査ベンダ向け解説） 113
Q33. どのような攻撃技術情報であれば守秘義務契約上の「秘密情報」にあたりませんか？（※調査ベンダ向け解説） 119

4．ケーススタディ 122

ケース 1：標的型サイバー攻撃 122
ケース 2：脆弱性を突いた Web サーバ等への不正アクセス 130
ケース 3：侵入型ランサムウェア攻撃 141

5．チェックリスト／フローシート 150

用語集

※下記は本ガイダンスにおいて各用語を用いる際の意味を示したものであり、各種標準文書やガイドライン等で用いられている定義と多少異なる場合がありますので、ご了承ください。

用語	用語解説
攻撃試行	攻撃を試みるために行われたアクセス等
攻撃キャンペーン	一定期間内において特定の組織／分野に対して特定の攻撃手法／攻撃インフラを用いて行われる攻撃活動
マルウェア情報	マルウェアを解析した情報（※表層解析程度のものも含む）
マルウェア検体	解析対象たるマルウェアそのもの又はマルウェアが含まれているファイル等
攻撃インフラ	主にＣ＆Ｃ（Command and Control）サーバ（※「C2 サーバ」とも略称）等の通信先や踏み台としたサーバ
TTP 情報	攻撃者が用いた攻撃手法に関する情報 「Tactics（戦術）、Techniques（技術）、Procedures（手順）」の略
攻撃グループ	攻撃を行った者を便宜上グルーピングし、またそれを呼称するもの
サイバー攻撃被害に係る情報	サイバー攻撃の発生により被害組織にて確認される、攻撃技術情報と被害内容・対応情報を含む情報（Q3（37 頁）参照のこと）
攻撃技術情報	マルウェア情報や攻撃インフラ、TTP 情報など攻撃者による攻撃活動やまたはその痕跡を示すもの
被害内容・対応情報	攻撃活動によって発生した被害や攻撃被害発生に対して取った被害組織の対処内容を示す情報
全容解明／把握	攻撃に用いられた手法や攻撃インフラを明らかにすることや、攻撃キャンペーン全体を明らかにすること
フィードバック（情報）	情報共有（提供）に対して、何らかの返答をすること（とその返答時の情報）
インディケータ情報／IoC(Indicator of Compromise：侵害指標)	攻撃者による侵害の痕跡を探すための指標となる情報、不正な通信先を示す「ＩＰアドレス」や「ドメイン名」、マルウェアの「ハッシュ値」、不正な通信の「通信プロトコル／ポート番号」や「通信の発生日時」などの情報
脅威情報	組織やシステムに対して損害を生じるインシデントの発生原因（サイバー攻撃のほか、自然災害など）に関する情報。特に、攻撃者の意図（目的・動機）、機会（攻撃可能な条件）、能力（攻撃手法や攻撃者のリソース、スキル）に関する情報
公開情報	不特定多数の者が何らかの制限なく、様々な媒体を通じて知ることができる情報

非公開情報	特定の者のみが知ることができるように、何らかの制限がかけられた情報
情報共有	サイバー攻撃に関する情報共有のことであり、被害組織で見つかった攻撃技術情報を中心に、非公開の方法で情報共有活動参加組織との間で共有し、そのフィードバックを得ること。 不特定多数の者がまだ認知していなかったり、被害が未公表であったりする個別の攻撃（被害）を特定・調査するために必要なインディケータ情報や、被害予防に必要な侵入経路などの TTP 情報を共有する
（サイバー攻撃被害に係る情報の）公表	サイバー攻撃被害があったことやどのようなインシデント対応を行ったのかについて公開情報として被害組織が情報発信すること
（被害組織以外による攻撃に関する）情報発信	専門機関からの注意喚起やセキュリティベンダなどからの技術的な分析レポート公開といった情報発信
報告	法令に基づき、または任意により、被害事実や対応状況について行政機関に伝えること
届出	ある行為を行うことや認証を受けるために法律等で定められた機関に連絡をすること
情報提供	分析依頼や自らが参加していない情報共有活動への情報の提供や、不正サイトのテイクダウン（無害化）依頼等の特定の目的のために、主に専門組織に対してサイバー攻撃に関する攻撃技術情報を伝えること
相談	インシデント対応に関する技術的支援を要請すること
連絡	取引先や顧客等、なんらかの利害関係者に対して攻撃被害が発生したことや、調査結果等を伝えること
サイバー攻撃被害組織等	サイバー攻撃被害を受けた民間主体やその被害対応にあたる IT ベンダやセキュリティベンダ等の受託者等
専門組織	専門機関やセキュリティベンダ
専門機関	国の法令／制度等に基づき、非営利でインシデント対応相談や分析、情報共有活動を行う組織。例） 一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）、独立行政法人情報処理推進機構（IPA）、一般財団法人日本サイバー犯罪対策センター（JC3）、国立研究開発法人情報通信研究機構（NICT）
情報共有活動	サイバーセキュリティ協議会、分野毎の ISAC（Information Sharing And Analysis Center）、J-CSIP、CISTA（JPCERT/CC）等の情報共有を目的とした活動

（情報共有活動の）ハブ組織	情報共有活動で参加者間の情報伝達の仲介や、一部の分析、他の共有活動や専門組織との窓口を担う組織
（情報共有活動の）窓口組織	前記情報共有活動はあらかじめ登録された参加者間で実施されるところ、非参加者であっても情報提供や共有が行える場合の窓口組織 例）サイバーセキュリティ協議会における（政令指定法人）JPCERT/CC、フィッシング対策協議会（事務局）
届出窓口	法令／制度に基づいて各種セキュリティインシデント等の届出先となっている窓口（組織）。
セキュリティベンダ	セキュリティ製品・サービスを提供することを主たる事業としている企業
ベンダ	いわゆる SIer や運用保守ベンダ
（製造）メーカー	ソフトウェア等の製造元
テイクダウン	不正サイトや C&C サーバなどの攻撃インフラの無害化のこと
レピュテーション	風評、（世間の）評判、評価、信用のこと

用語集補足：

「共有」「報告／届出」「連絡」「公表」の違いについて、様々な法令やガイドライン等の間で用語の定義や使い方に差異があるため、本ガイダンスにおけるそれぞれの用語の考え方／使い方の整理を以下に示します。各法令に基づく行動が求められる場合、各用語の厳密な定義は該当する法令内で示されるものに従ってください。

情報共有

サイバー攻撃に関する情報共有には、①自ら情報共有活動参加者に対して行うものや、②情報共有活動のハブ組織である専門組織や情報共有活動に参加している専門組織を介して情報共有活動に情報を共有し、仲介した専門組織の知見を含むフィードバックを得る方法があります。前者の場合は自組織名を明かして行い、後者の場合は匿名で行われることが多いです（※後者の場合であっても、自組織名（情報提供者名）を明かすことを希望して、情報共有活動のハブ組織等経由での情報共有ができる活動もあります）。

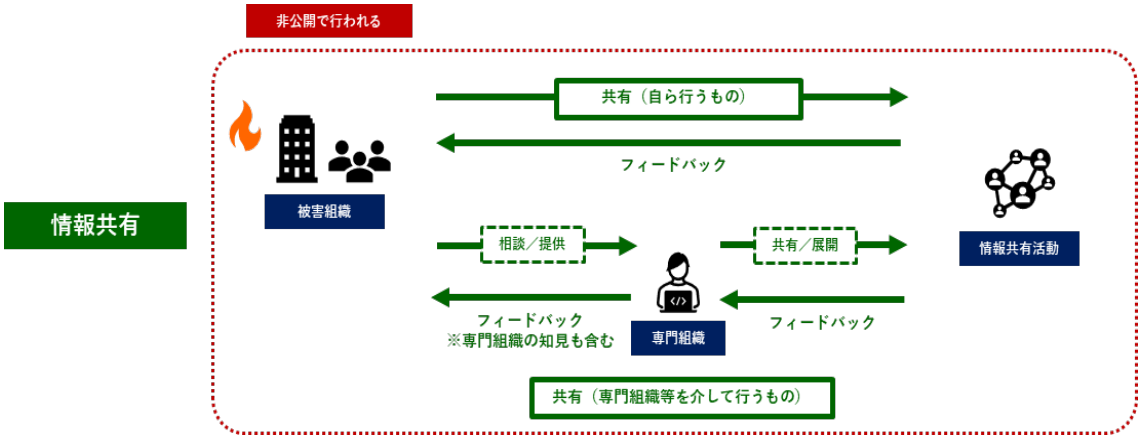


図 1

被害組織による被害の公表

サイバー攻撃被害の公表については、法令／ガイドラインに基づく公表のほか、法令等の定めはないものの被害組織自身の判断で行われる公表があります。後者の判断に至る事情は様々で、例えば、二次被害拡大防止のため注意喚起として行われる公表や、サービス停止時など対外的な説明を行う場合の速報的な公表、広報／リーガルリスク対応としての公表などがあります。

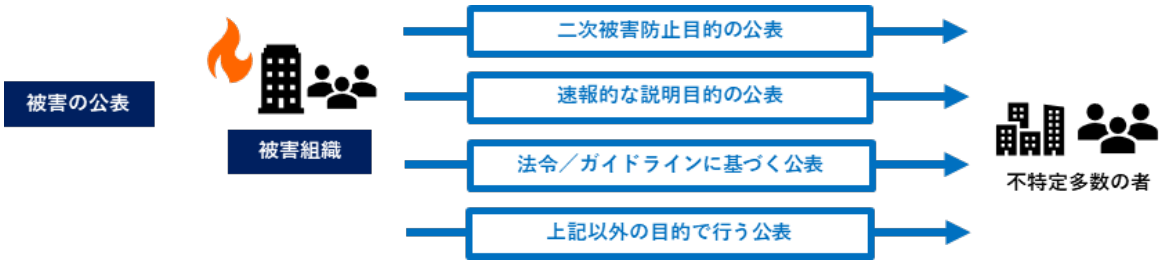


図 2

専門組織による注意喚起やレポートによる情報発信

被害組織からの相談／情報提供を元に、専門組織が攻撃に関する技術的な情報を注意喚起や分析レポートとして情報発信することがあります。この場合、基本的には情報提供元である被害組織が単独であっても複数であっても、個別組織名や個別被害の詳細な情報は明かさない形で情報発信されます。

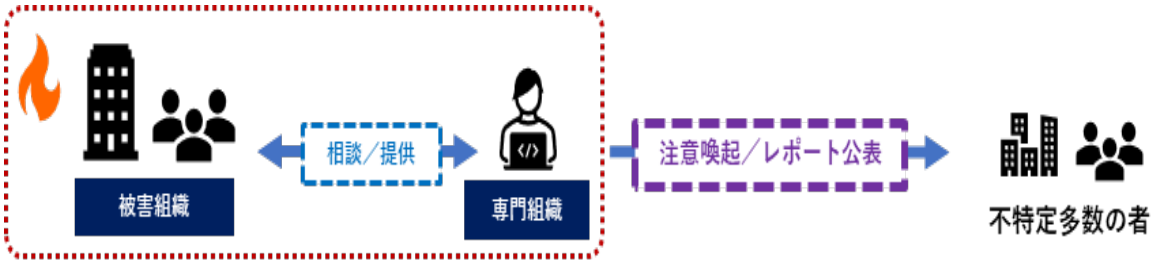


図 3

行政機関への報告／届出、警察への通報等

法令等に基づいて行われる報告のほか、任意のものとして被害組織から行われる報告もあります。

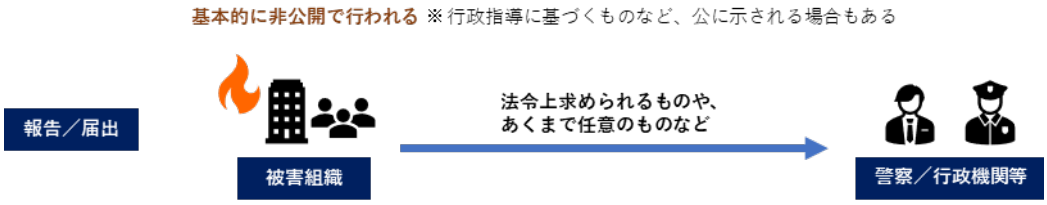


図 4

取引先や顧客への連絡

個人情報漏えいなどで顧客や取引先に二次被害が発生するおそれがある場合などに行われるもの（個人情報の保護に関する法律（以下、「個人情報保護法」という。）26 条に基づ

く本人への「通知」）[1]や、インシデント対応による調査がある程度終わり被害内容や取引先へ影響有無などを伝えるために行われます。

図 5

[1] 法律上、厳密にいえば、漏えいに関して本人通知等の義務があるのは「個人データ」ですが、読みやすさを重視して、本ガイダンスでは、正確な使い分けが必要な箇所以外では、「個人情報」と「個人データ」を厳密に使い分けていないことに御留意下さい。

１．はじめに

―情報共有とは何か／公表とは何か

サイバー攻撃に関する情報共有の意義については、これまでの様々な文書等で示されてきていますが、本ガイダンスはサイバー攻撃の被害に係る情報のうち、どのような情報を、どのタイミングで、どのような主体と共有すれば、被害組織自身がサイバー攻撃の全容を解明し、被害組織自身の対策強化や他組織への攻撃被害の未然防止、被害拡大防止に効果を発揮することができるのか、実務上の参考とすべきものを具体的に示すことを目的として検討を行ったものです。

インシデント対応の一連の流れにおいて、情報共有と切り離せないものとして、被害の公表があります。この２つは異なる目的を有する行為ですが、ともに「被害組織の外部に情報を出す行為」という点で共通する２つの行為の整理はこれまで示されてきませんでした。情報共有が専ら非公開の情報共有活動上で行われるのに対して、被害の公表はプレスリリースや SNS 等を通じて、公開情報として被害組織から発信されます。サイバー攻撃の実態について公開情報として発信されるものとしては、他には専門組織からのレポートや注意喚起などもありますが、こうした「公開情報として広く社会に共有される」ことと、「非公開の活動で情報が共有されること」の関係性も示されてきませんでした。

本ガイダンスの検討にあたっては、「情報共有」のための具体的な方法や留意点に加え、「情報共有」と「（被害）公表」の関係性を整理しています。「（被害）公表」のあり方や具体的方法については、サイバー攻撃被害時におけるインシデント対応の観点だけでなく、企業の危機管理体制やコンプライアンスとの関係などが想定されるため、本ガイダンスでは主たる検討対象とはしていませんが、前述のとおり、情報共有と容易に切り離せないものとして、その関係性を示しています。

情報共有とは何か

「情報共有」は２つの意味で解釈されることがあると考えられます。１つは「“狭義の”情報共有」であり、非公開にて情報共有活動の場や専門組織との間で行われる、主にサイバー攻撃の手法等に関する技術的情報のやりとりのことを指し、本ガイダンスの主たる対象としているものです。

もう１つは「“広義の”情報共有」であり、これには、前述の”狭義”の情報共有に加え、後述する、被害組織による公表（自組織が受けたサイバー攻撃被害の状況や対応内容について広く外部に示すこと）が包含されます。

本ガイダンスでは、“狭義の”情報共有を主に取り上げており、特に説明がない限り、「情報共有」を、“狭義の”情報共有の意味で使います。

（”狭義の”）情報共有の目的としては

①インシデント対応に必要な情報を得るため

②被害の未然防止のための情報を得るため

の２つを挙げることができます。前者は被害者個別の目的であり、高度な攻撃手法に対して不足する情報を補うことを目的としています。後者は情報共有活動全体としての目的であり、①の目的で提供された情報が別の参加組織の②のための情報となることで、情報共有活動を通じた相互の利益につながっていると言えます。

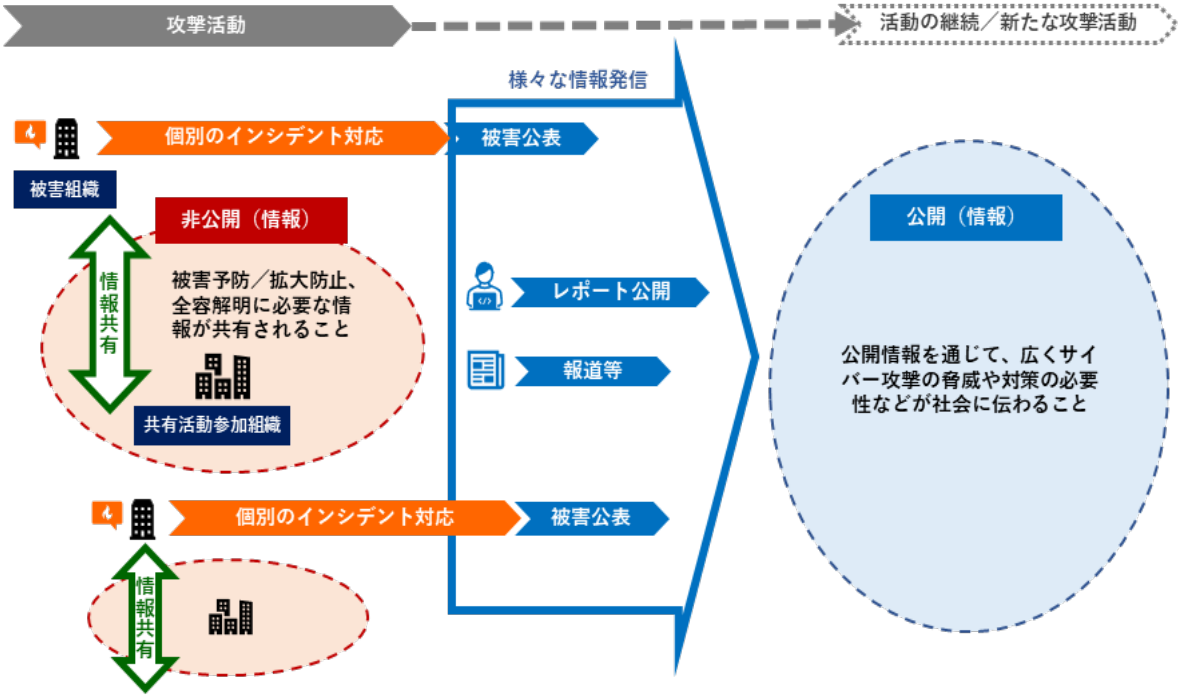


図 6

公表とは何か

被害組織が、自組織が受けたサイバー攻撃被害の状況や対応内容について広く外部に示す公表は、大きく分類すると、法令／ガイドラインで求められている公表と、法令等の定めはないものの被害組織自身の判断で公表するものに分けられます。後者の中には、例えば、二次被害拡大防止のため注意喚起として行われる公表、サービス停止時など発生している事象について対外的説明が必要な場合における速報的な公表、広報／リーガルリスク対応としての公表などがあるでしょう（※詳細は後述の Q14（70 頁）をご覧ください）。公表により、（新たな）サイバー攻撃の脅威や対策の必要性が広く社会に伝わることにもなります。

第三者による情報発信

一方、公表とは厳密には異なりますが、被害組織が提供した情報をもとに専門機関やセキュリティベンダが注意喚起やレポート発信などを、被害組織名を伏せた上で、攻撃実態やマクロな被害状況を知らしめるために行うこともあります。また、報道機関等が被害組織やその他の関係組織の発表や、独自の取材をもとに、攻撃や被害について報道することがあります。

本ガイダンスでは、主に被害組織自身による公表を中心に解説しながら、専門組織が被害組織から提供された情報をもとに行う情報発信との関係についても、被害組織保護に配慮しつつ解説します。

<table>
<tr><td colspan="2" rowspan="2"></td><td colspan="3">発信主体</td></tr>
<tr><td>被害組織自身</td><td>専門組織</td><td>報道機関</td></tr>
<tr><td rowspan="2">被害組織名の明示</td><td>実名</td><td>・プレスリリース
・上場企業における適時開示

本ガイダンスで主に触れる
（「公表」）</td><td>—
※基本的に被害組織名が示されるケースはほとんどない</td><td rowspan="2">各種報道</td></tr>
<tr><td>匿名</td><td>—</td><td>・攻撃に関するレポート
・注意喚起

本ガイダンスで補足的に触れる
（厳密には「公表」ではない）</td></tr>
</table>

表 1

行政機関への報告、警察への通報等との関係

情報共有と公表のほかに、行政機関への報告や警察への通報等があります。法令で義務付けられたもの以外に、任意で行うものについて、これまで情報共有や被害公表との関係性が整理されてきませんでした。

本ガイダンスでは、こうした任意の報告等について、行政機関が有する、①情報共有活動で把握しきれない被害状況の把握機能、②広く国民に情報発信する機能、③警察による犯罪捜査を通じた抑止力の向上、④サイバー攻撃対処の全体像から見た被害に係る情報の必要性の 4 点から整理をしています。

望ましい情報共有と被害の公表が行われることの目的は何か

前述のとおり、情報共有と公表は目的も方法も異なる行為ですが、同じ「被害組織の外部に情報を出す行為」であり、外部の組織に被害事実が知られることによるレピュテーション（風評）リスクのほか、外部に出す情報として、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）を含んだり、第三者の不利益となるような情報を含んだりする場合があるため、情報を出すことに躊躇するケースが多く見受けられます。

本ガイダンスでは、サイバー攻撃被害現場で発生する情報について、「攻撃方法を示す情報」である攻撃技術情報と、「被害内容を示す情報」である被害内容・対応情報の 2 つの情報に切り分け、主に、前者については早期の情報共有活動への提供を目指すことで被害組織自身の早期の全容解明や他の組織の被害予防／被害の早期認知／攻撃被害拡大防止に役立てることを意図しています。後者については、被害組織の保護に配慮しながら、二次被害防止や制度上の報告との関係、被害公表の社会的意義の関係性について整理を示した上で、被害企業への過度な批判ではなく、攻撃の脅威や対策の必要性に対する社会的な問題意識の共有が進むことを目指します。

―なぜ「情報共有を行うべき」なのか／公表の社会的意義

なぜ「情報共有を行うべき」なのか

サイバー攻撃被害に係る情報の共有活動は、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ですが、まず、活動に参加する組織自体の利益を考える必要があります。

個別の人・組織が得ることができる情報には限界があるため、複数の人・組織で情報を共有すればより多くの有益な情報が得られる、ということは一般的には十分理解されているかと思います。サイバー攻撃対応においても同様で、攻撃者は検知回避や痕跡の消去を行うため、個別の製品・サービスやインシデント対応によって発見できる情報にはばらつきが出ます。1 つの組織の調査では攻撃手口の全体を把握しきれなかったとしても、複数の組織の調査結果を組み合わせることで全容が解明できることがあり得ます。

しかしながら、実際には上記のような理屈上の情報共有は行われないケースの方が多いことが実情です。これは、複数の組織間で情報の非対称性があるからではないかと考えることができます。

図 7 の上図は、お互いに「自組織が知らない情報の存在」を知っていることから、情報共有の必要性を認識することができる合理的なケースです。ですが、実際には図 7 下図のように、そもそも「自組織が全体（情報 X）のうち、どの部分（情報 Y）まで知っているのか知ることができない」ため、「自組織が何（通信先 C）を知っていないのか知らない」状態であり、そもそも情報共有の必要性を認識することができないケースにあるのです。

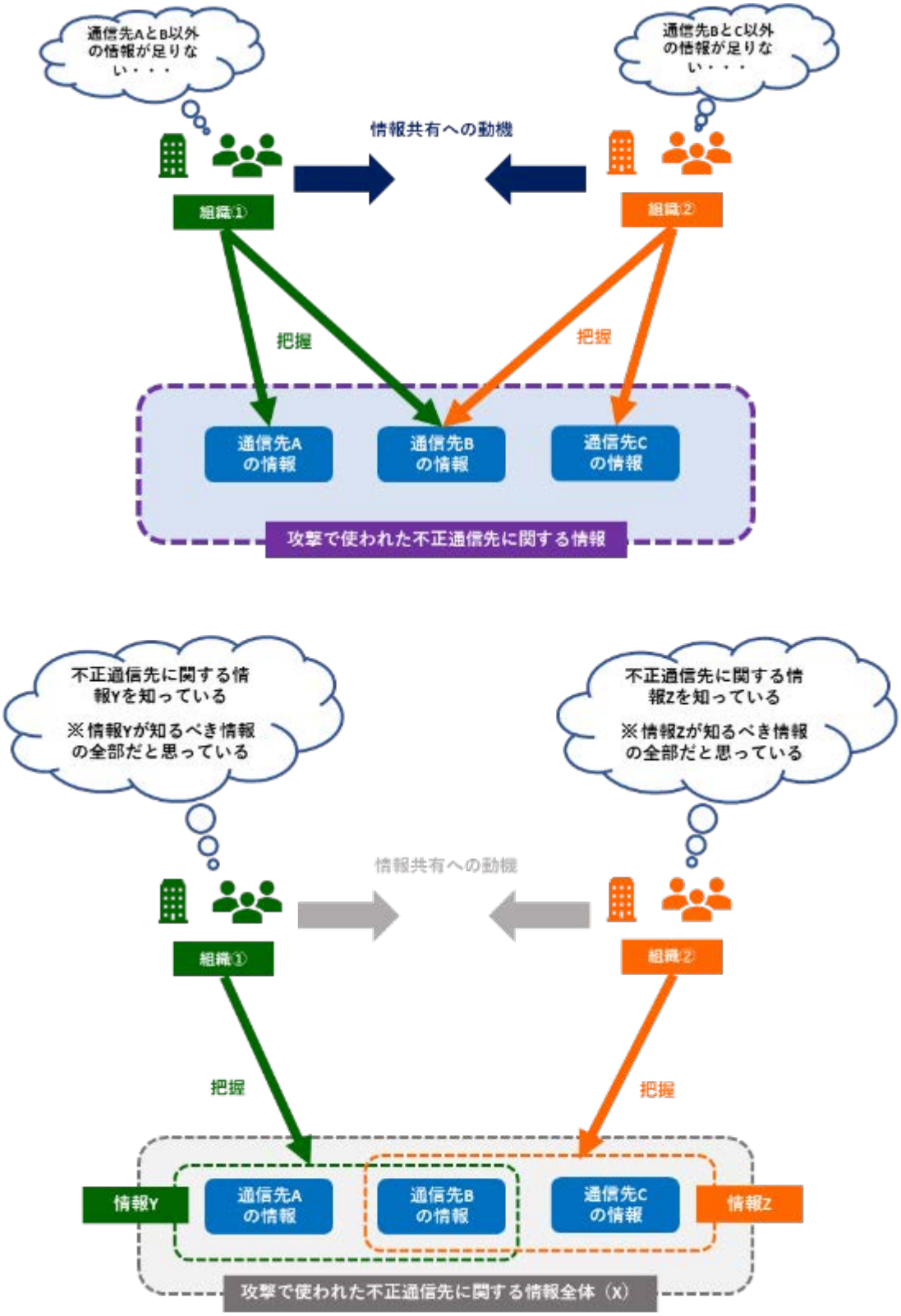

通信先AとB以外の情報が足りない・・・
通信先BとC以外の情報が足りない・・・
情報共有への動機
組織①
組織②
把握
把握
通信先A の情報
通信先B の情報
通信先C の情報
攻撃で使われた不正通信先に関する情報
不正通信先に関する情報Yを知っている
※情報Yが知るべき情報の全部だと思っている
不正通信先に関する情報Zを知っている
※情報Zが知るべき情報の全部だと思っている
情報共有への動機
組織①
組織②
把握
把握
情報Y
通信先A の情報
通信先B の情報
通信先C の情報
情報Z
攻撃で使われた不正通信先に関する情報全体（X）

図 7

サイバー攻撃被害を未然に防止、あるいは侵害を早期に検知し被害を最小限に抑えるためには、攻撃に関する情報、特に「脅威情報」の入手が必要です。不正通信元（先）の情報、侵入手口に関する情報、使用されるマルウェアの情報などがありますが、先述のとおり、単独の組織で得られる情報には限界があります。

下記図８のうち「被害組織Ａが調査によって得た情報」は、侵入後に使用されるマルウェアや不正通信先についてはその大半を把握することができましたが、侵入経路など攻撃の初期段階に関する情報は得られませんでした。「被害組織Ｂが調査によって得た情報」は、攻撃の流れはほぼ全体を把握できましたが、マルウェアや通信先の大半は把握できていません。

被害組織Ａにおいては、侵入経路が不明なため、効果的な再発防止策を確定することができず、被害組織Ｂにおいては、自組織内から完全にマルウェアを除去できたのか不明な状況です。

よって、いずれの被害組織も調査／再発防止策が不徹底に終わってしまいます。

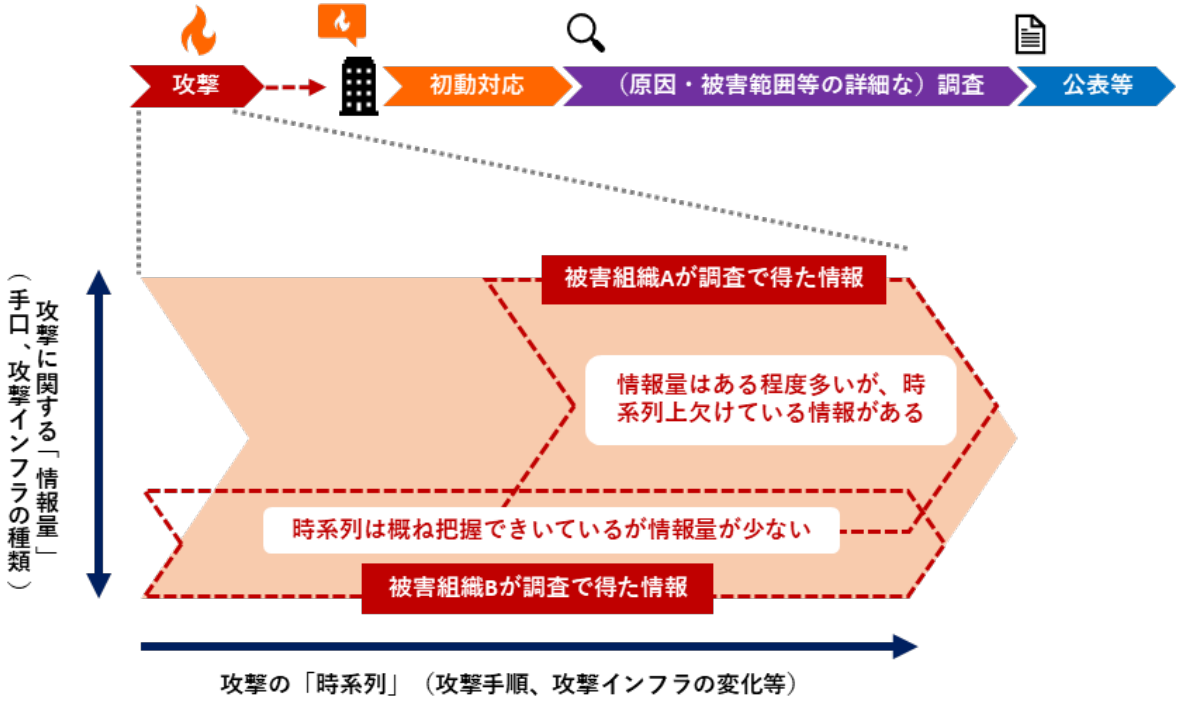


図８

この問題はインシデント対応だけでなく、攻撃被害の未然予防においても同じことが言えます。特に、未知の攻撃手法／攻撃インフラを用いるような新しい攻撃に対しては、初期の段階ではセキュリティ製品・サービスや専門組織毎に把握できている情報にばらつきがあります。こうした情報のばらつきは観測やインシデント対応経験の蓄積などにより、

時間の経過とともに解消されていきますが、その時間差において、各個別の被害が発生してしまうのです。

情報の共有の根底にあるのは、「自組織が何を知らないのか知ることができない」という単独組織での認識の限界です。また、理屈上、協力すべき複数組織間においては「お互いに何を知らないのか知ることができない」状況にあります。「鶏が先か、卵が先か」になってしまいますが、情報共有活動を行っていなければ「自組織が知らなかったこと」「自組織が知らなかったことを他の組織が知っていたこと」を知ることができないため、情報共有の必要性を感じることがそもそもできないのです。

公表の社会的意義について

サイバー攻撃被害を公表した結果、その組織のセキュリティ体制や対応の問題点が批判され、企業イメージを損なうことがあります。そのため、被害祖機の中には、被害をなるべく公表したくないと考える傾向もあるかもしれません。しかし、被害組織の公表は、サイバー攻撃被害の実態を目に見える形で社会に示すことによって、脅威の度合いを測るものさしとなり、日本が置かれているサイバー攻撃被害の現状を社会が正しく理解する助けになります。

前項にて、被害組織間の情報の非対称性を克服するための情報共有の意義について解説しました。情報の非対称性は被害組織やインシデント対応にあたる専門組織と社会全体との間にも存在しています。個別具体的な被害に関する情報が社会に伝わらないことで、攻撃活動や社会に与える深刻な影響が社会に理解されず、制度の整備などを通じて社会全体でサイバー対策を講じることへの社会的な合意が得られないかもしれません。

また、情報の非対称性が解消されることで、被害企業が公表した際の社会からの無理解や誤解に基づく批判なども徐々に減っていく可能性があります。どのような脅威度合いの攻撃を受け、どのような被害が発生し、どのように対処したのか、被害組織が公表したインシデント対応の内容が正しく評価されるためには、日頃から社会全体においてサイバー攻撃やインシデント対応に関する理解がなければなりません。
これも「鶏が先か、卵が先か」というジレンマですが、サイバー攻撃被害に係る情報の公表により社会全体に対して情報が提供されることで、積極的に被害公表を行った組織に対して、より適切な評価がなされるようになると考えます。

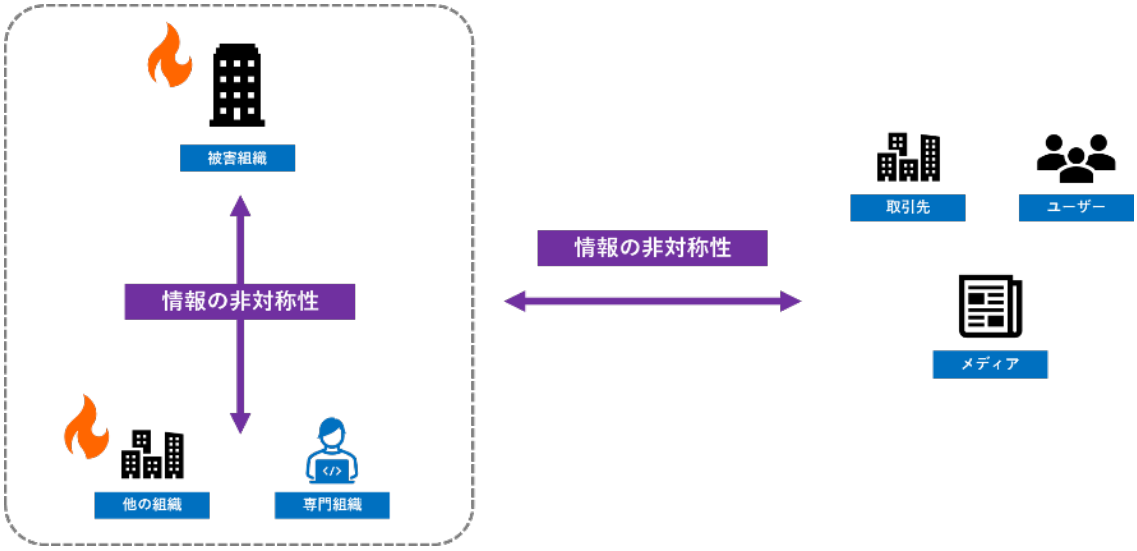


図 9

一本ガイダンスのコンセプト

冒頭で示したとおり、被害組織とサイバーセキュリティ専門組織等との情報共有は被害組織にとっても、社会全体にとっても非常に有益です。

しかしながら、現状としてサイバー攻撃被害を受けた組織にとっては、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、他方で、被害に係る情報のうち、どのような情報を、どのタイミングで、どのような主体と共有することが適当なのか等を検討するための参考資料等に乏しく、この点が、円滑かつ効果的に情報共有が進まない一因となっていると考えられます。

このガイダンスは、被害組織が保護されつつ、円滑かつ効果的に情報共有が行われるためのポイントを示すことを目的としています。そのためのコンセプトとして、以下の情報の整理を示します。

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」**（※後述のとおり、本ガイダンスでは「被害内容・対応情報」と整理しています）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」**（同じく、本ガイダンスでは「攻撃技術情報」と整理しています）の 2 つの種類の情報が存在します。次に示すものは、サイバー攻撃被害に関する報道事例のイメージですが、2 つの種類の情報が存在していることがわかると思います。

○○株式会社が昨年×月にサイバー攻撃被害を受け、同社が保有する××情報が外部に漏えいしたおそれがあることが判明した。

攻撃は同社が使っていたソフトウェアＡの脆弱性を突いた侵入により行われ、社内の××情報を保存したサーバなど、ｎ台のサーバや端末がマルウェアＸに感染し、××業務に影響が出ているという。

今年□月にマルウェアＸに関するレポートを発表したセキュリティベンダーBによると、マルウェアＸは攻撃グループＹが用いており、×××分野などを狙う攻撃キャンペーンが確認されていたという。

被害組織や被害内容に関する情報

被害を受けたシステムや被害範囲に関する情報

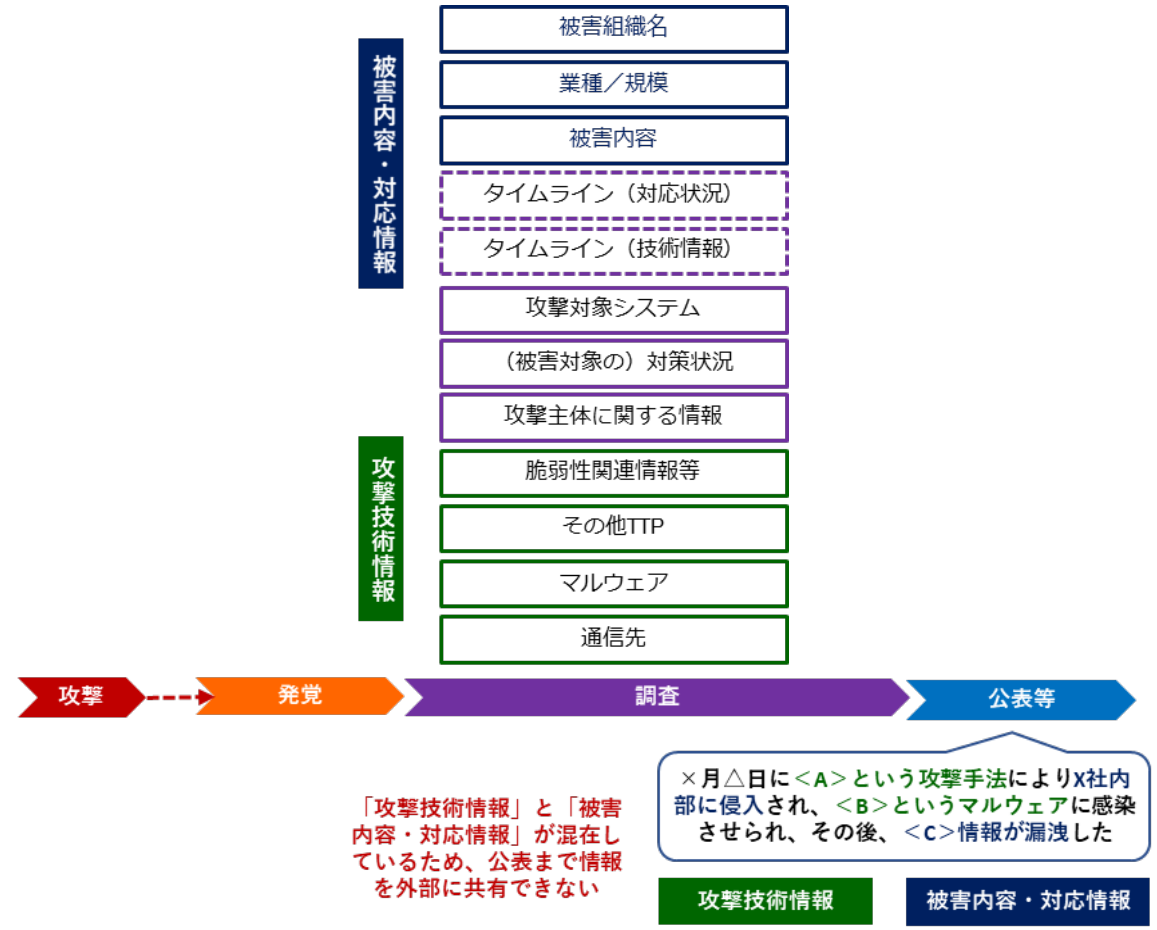
見つかったマルウェアや攻撃者に関する情報

「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／攻撃者の活動を示す情報」（攻撃技術情報）は前述のとおり、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。

本ガイダンスでは、この性質の異なる２つの情報を切り離して、被害内容・対応情報を適切に扱うことで被害組織保護が強化されること、マルウェアや不正な通信先といった攻撃技術情報が速やかに共有されることで情報共有活動が活性化されることを目指しています。この「切り離し」に必要なポイントについて、後述のＦＡＱで解説していきます。


被害内容・対応情報
被害組織名
業種／規模
被害内容
タイムライン（対応状況）
タイムライン（技術情報）
攻撃技術情報
攻撃対象システム
（被害対象の）対策状況
攻撃主体に関する情報
脆弱性関連情報等
その他TTP
マルウェア
通信先
攻撃
発覚
調査
公表等
「攻撃技術情報」と「被害内容・対応情報」が混在しているため、公表まで情報を外部に共有できない
×月△日に＜A＞という攻撃手法によりX社内部に侵入され、＜B＞というマルウェアに感染させられ、その後、＜C＞情報が漏洩した
攻撃技術情報
被害内容・対応情報

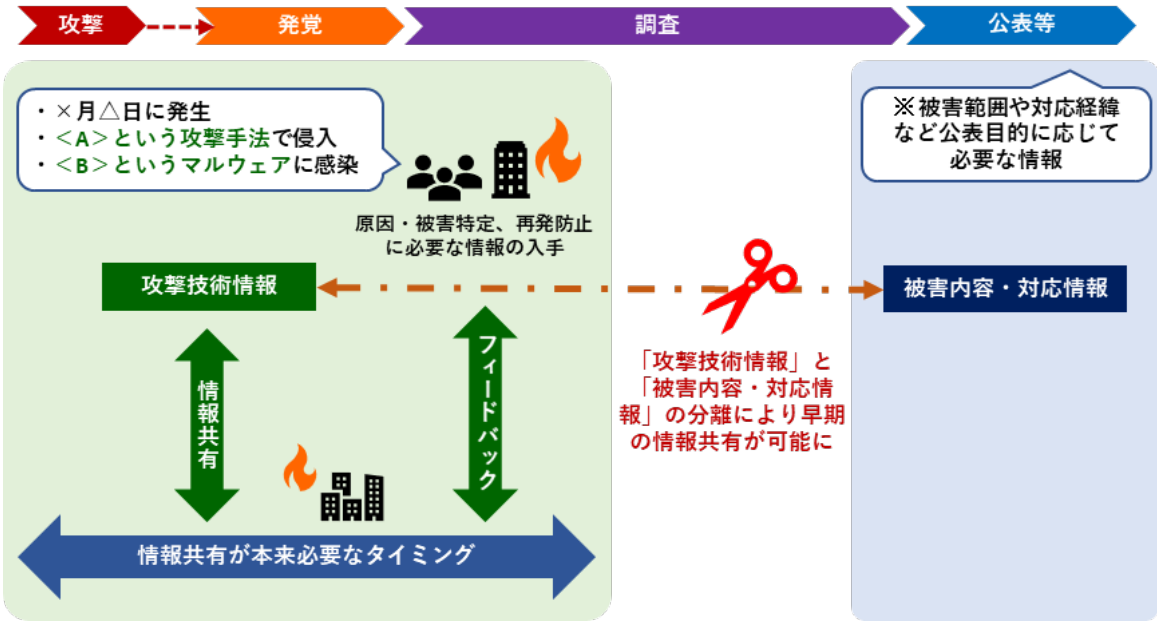

攻撃
発覚
調査
公表等
・×月△日に発生
・＜A＞という攻撃手法で侵入
・＜B＞というマルウェアに感染
原因・被害特定、再発防止に必要な情報の入手
攻撃技術情報
情報共有
フィードバック
情報共有が本来必要なタイミング
「攻撃技術情報」と「被害内容・対応情報」の分離により早期の情報共有が可能に
※被害範囲や対応経緯など公表目的に応じて必要な情報
被害内容・対応情報

図 10

－本ガイダンスの検討経緯

令和 2 年度総務省事業として、「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」事業が実施され、一般社団法人 JPCERT/CC が報告書をまとめました[2]（2021 年 3 月とりまとめ。2021 年 7 月公表）。この調査は、2020 年 1 月から 2 月にかけて、複数の大手電機メーカーなどが過去のサイバー攻撃被害を公表した際に、メディアや所管省庁から「公表の遅れ」等が指摘されたことを踏まえ、サイバー攻撃被害情報の共有と公表のあり方に関する検討を行ったものです。この報告書では結論として、「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」とされ、「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」[3]と示されました。

本ガイダンスの検討に当たっては、2022 年 4 月にサイバーセキュリティ協議会運営委員会において、「サイバー攻撃被害に係る情報を取り扱う様々な担当者の判断に資することを目的として、サイバー攻撃被害組織等の立場にも配慮しつつ、技術情報等組織特定に至らない情報の整理を含めた、サイバー攻撃被害に係る情報の共有・公表ガイダンス（以下「ガイダンス」といいます。）を策定すべく」[4]、同運営委員会の下に「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」を開催することが決定されました。

同検討会は 2022 年 5 月から 12 月にかけて、計 5 回開催され、セキュリティベンダ、専門機関、IT/セキュリティ業界団体、弁護士、研究者、メディアなど様々な分野からの委員が出席し、事務局（警察庁、総務省、経済産業省、内閣サイバーセキュリティセンター及び政令指定法人 JPCERT/CC）と議論を行い、本ガイダンス案のとりまとめを行いました。

---

[2] 「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）」
https://www.soumu.go.jp/main_content/000762951.pdf

[3] 同報告書 39 頁

[4] 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
https://www.nisc.go.jp/pdf/press/kyogikai_guidancekentoukai.pdf

―本ガイダンスのスコープ

本ガイダンスのスコープについて

下記図 11 は本ガイダンスのスコープを概念的に示したものです。

サイバー攻撃被害（情報）を巡る組織間のやりとりについては、既存の情報共有活動や、報告・届出の制度、公表に関する判断基準を示したガイドライン等、既に多く存在しています。本ガイダンスはこれらの既存の制度やルールに対してなんら統一的な基準を示したり、変更を求めたりするものでありません。

本ガイダンスは、どのような共有活動、制度においても共通して触れることになる、サイバー攻撃被害に係る情報の特性の整理や取り扱い上の留意点に関する解説に主眼を置いています（下記図 11 の①赤枠の範囲）。そのうえで、既存の活動・制度等との関係性についてのみ横断的に整理をして示しています（下記図 11 の②紫・③橙枠の範囲）。

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を示しています。

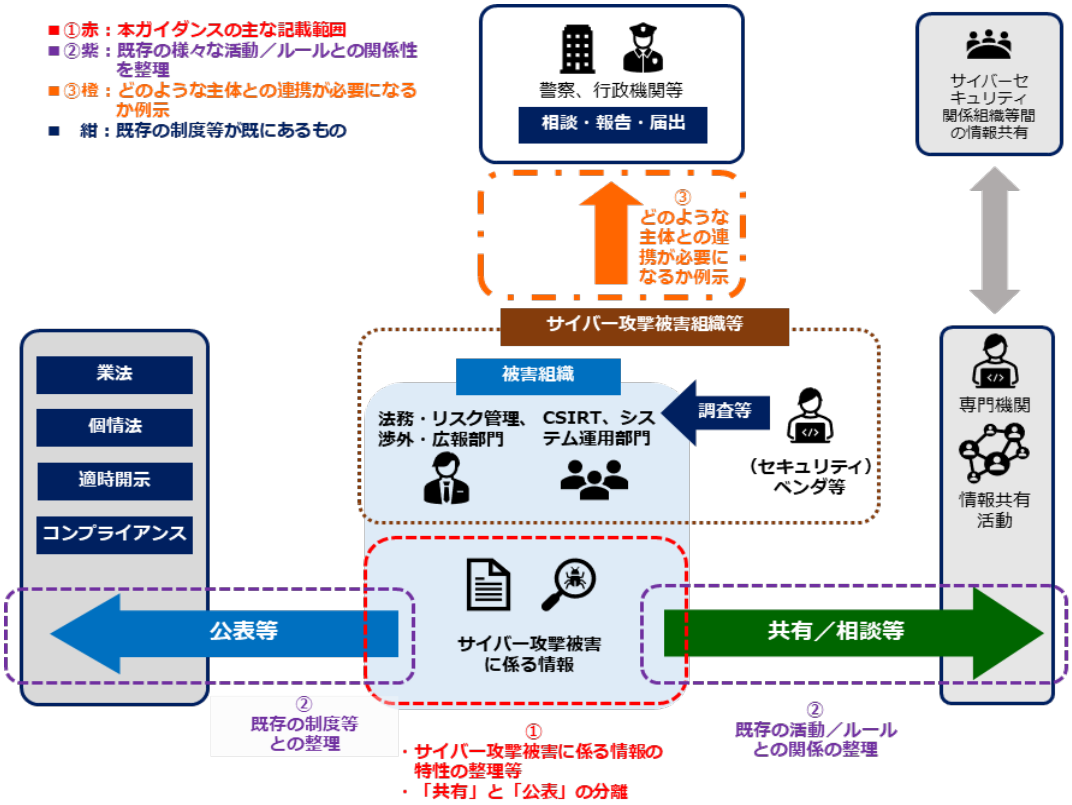


図 11

行政機関への報告・届出、警察への通報等について

本ガイダンスのスコープ図（図 11）に示しているとおり、このガイダンスでは、民間における情報共有だけでなく、行政機関への報告・届出、警察への通報等についても触れています。

特に、重要インフラ（重要インフラのサイバーセキュリティに係る行動計画（サイバーセキュリティ戦略本部）に基づく重要インフラ 14 分野）は、国民生活や経済活動の基盤であって、その機能が停止した場合に多大な影響を及ぼすおそれがあるため、被害の状況や事業継続の見通しについて、法令等に基づく報告が求められています。これらは、ユーザーである一般国民への影響／被害に対する行政機関としての対応であるとともに、同様の攻撃で同業他社においても影響が出ることがないよう、安全基準の改定や行政指導等が必要になるため、将来的な対処に必要な情報を得るための行動でもあります。

これに加えて、セキュリティインシデントにおける業法等の法令に基づかない報告等はなぜ必要なのでしょうか。

なぜ国が情報を集める必要があるのか

サイバーセキュリティにおける「脅威（Threat）」の定義は様々ですが、米 SANS の定義では「脅威＝意図×機会×能力」と示されています[5]。本ガイダンスで主に触れているのは、攻撃が成功してしまうような「機会」を減らすための、未然の被害防止としての情報共有活動です。また、Q12（64 頁）などで一部触れていますが、専門組織が行う情報発信活動等は「能力」への対処の一環と言えます。

攻撃者の「意図」に対して、一般的には犯罪者の検挙などによりその抑止が図られるとされていますが、特に国家主体を背景とするような攻撃活動などに対しては、国としての対処が必要になることがあります。また、「意図」に対しては、攻撃者が何（組織／資産）を狙っているのか把握すること自体も重要です。サイバー攻撃は連鎖的に起きる可能性があることや、被害を受けた事業者がサプライチェーン上重要な事業者である場合など、個別の被害組織である一事業者の事業継続の見通しが、国全体の経済・社会にも影響することがあることから、国としても状況の把握に努めることが必要になります。

こうした対処を行うためには、攻撃側の意図を特定する必要がありますが、サイバー攻撃の実行者を物理的に捕らえることが困難である以上、サイバー攻撃被害に係る情報のうち、被害内容・対応情報をベースとして攻撃者／活動の「意図」を推測するしかありません。したがって、攻撃技術情報を基本とした情報共有活動とは別に、被害内容・対応情報を知るために行政機関が被害組織に対して情報の提供を求めることになります。

---

[5] Mike Cloppert “Security Intelligence: Introduction (pt 2)” SANS Institute , 2009
https://www.sans.org/blog/security-intelligence-introduction-pt-2-/

以下、どのような目的／ケースにおいて、業法等の法令に基づかない報告・届出等が求められているのか解説します。

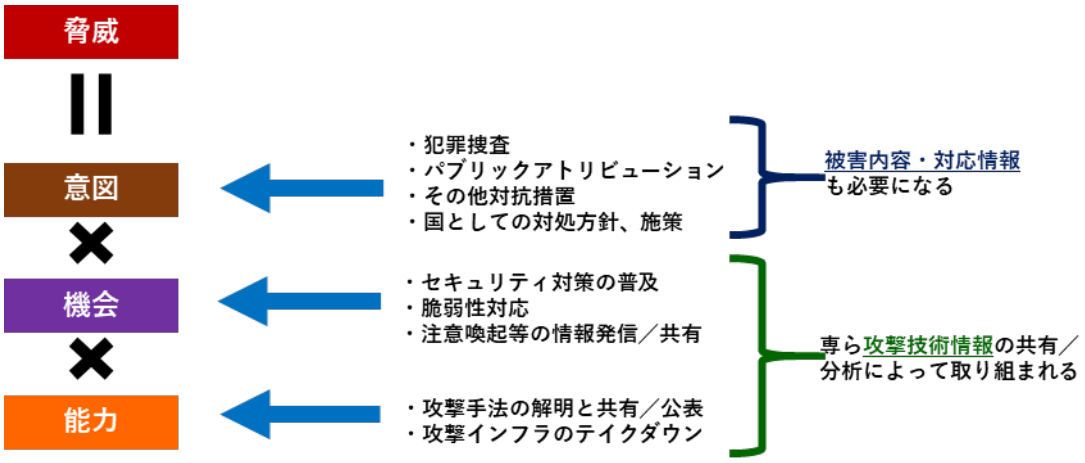


図 12

①情報共有活動外での事象の認知

サイバー攻撃は、同時多発的な攻撃が可能であり、攻撃が連鎖することで、その影響範囲が大きくなることがあります。“守る側”は、業種別や地域別の連携に加えて、サイバーセキュリティ協議会や J-CSIP、CISTA など分野横断での情報共有活動もありますが、あらゆる対象を包括的に一つの活動でカバーすることは困難です。

Emotet[6]を用いた攻撃のように、無差別・大規模に行われるものであれば、分野横断での情報共有活動を運営している専門機関が攻撃（被害の）拡大を早期に捉えられるため、注意喚起の発出等により、広く事象が認知されます（図 13 の左図）。しかしながら、図 13 の右図のような、大規模ではないが分野横断して攻撃が行われるケースでは、分野横断活動の限界（Q13（67 頁）参照）から、専門機関や分野横断による情報共有活動だけでは攻撃動向を早期に認知することができない一方、各所管省庁に報告があがっていた場合、総合調整機能を担う内閣サイバーセキュリティセンター（NISC）をハブとした連携を通じて、広範囲な攻撃の存在を認知することができます 。

特に、攻撃が特定の製品の脆弱性（ぜいじゃくせい）等の悪用や、特定の IT インフラ／サービスを踏み台とした攻撃であった場合、攻撃原因への対処を行わない限り、攻撃が継続するおそれがあるため、早期に共通の攻撃原因を特定するためにも、情報共有活動の枠組みを超えた情報の連携が必要となります。

---

[6] 2019 年以降、世界的な被害をもたらしているマルウェアで、情報の窃取に加え、感染した組織の情報を悪用したなりすましメールにより、他の組織への感染被害を拡大します。ボットネットと呼ばれる感染端末の大規模なネットワークを構築し、感染組織に対して更に別の攻撃者（ランサムウェア攻撃グループなど）を誘導する役割を担っています。

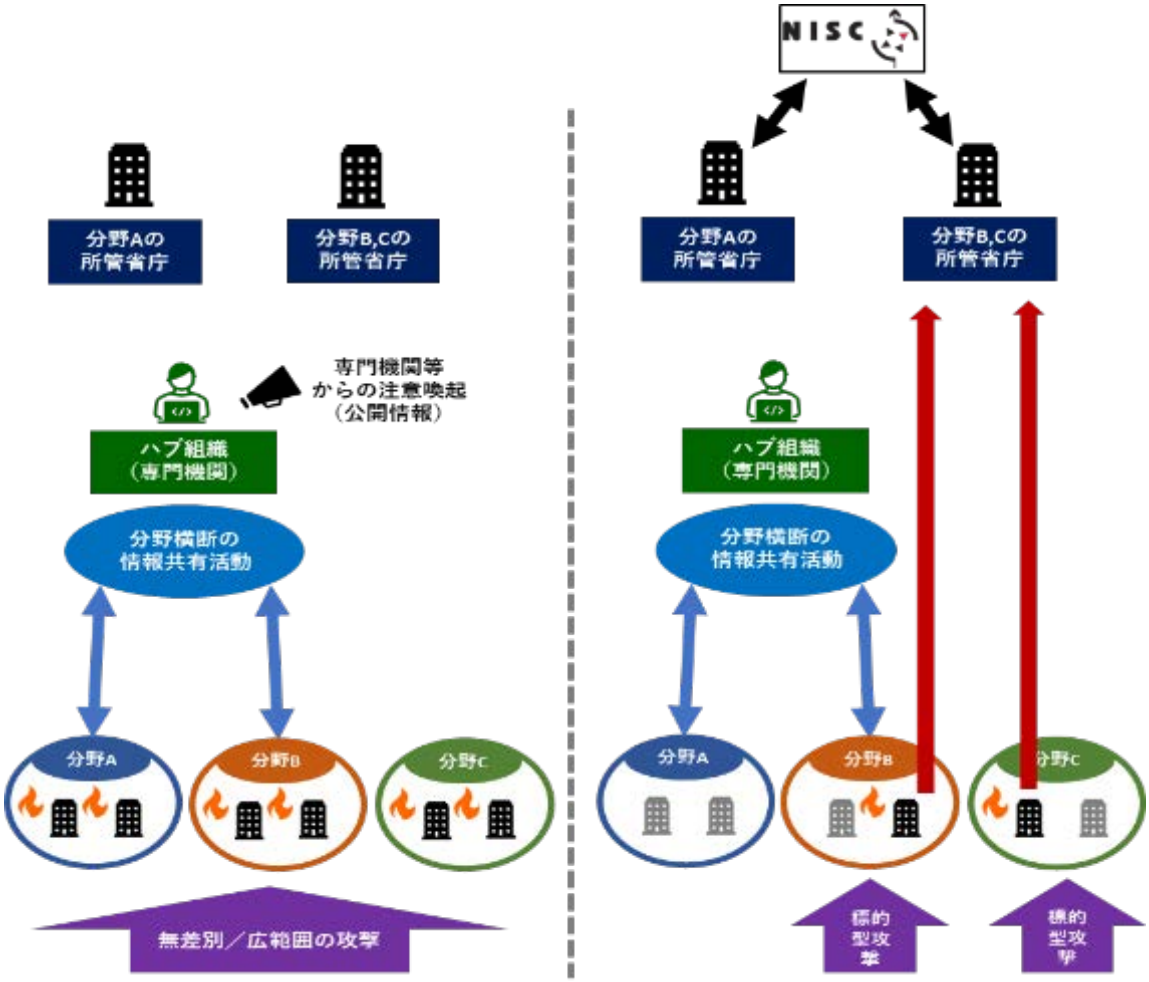


図 13

②広くユーザーに影響を及ぼすような規模の攻撃への対処

また、IT サービス利活用の拡大により、クラウド型のサービスなど、既存の重要インフラのように法令等に基づく報告制度の対象となっていないものの、広く利用されるサービスが普及してきました。

こうしたシステムがサイバー攻撃による影響を受けた場合、影響を受けるユーザーへの通知・二次被害防止の対応は一義的には当該事業者が行うべきものですが、非常に広範囲であり社会的な混乱を生むおそれがある場合や、同業他社でも同様の攻撃被害が発生している場合、あるいはその蓋然性が高い場合などは、所管省庁等からの報道発表等を通じて広く二次被害防止に必要な情報が伝えられる必要があります。また、被害の全体像を把握し、必要な対応につなげていく観点から、所管省庁への報告・届出に関する法令に基づく義務がない場合であっても、被害に関する公表や報道を受けて、当該被害組織に所管省庁から情報提供の依頼がなされる場合があります。

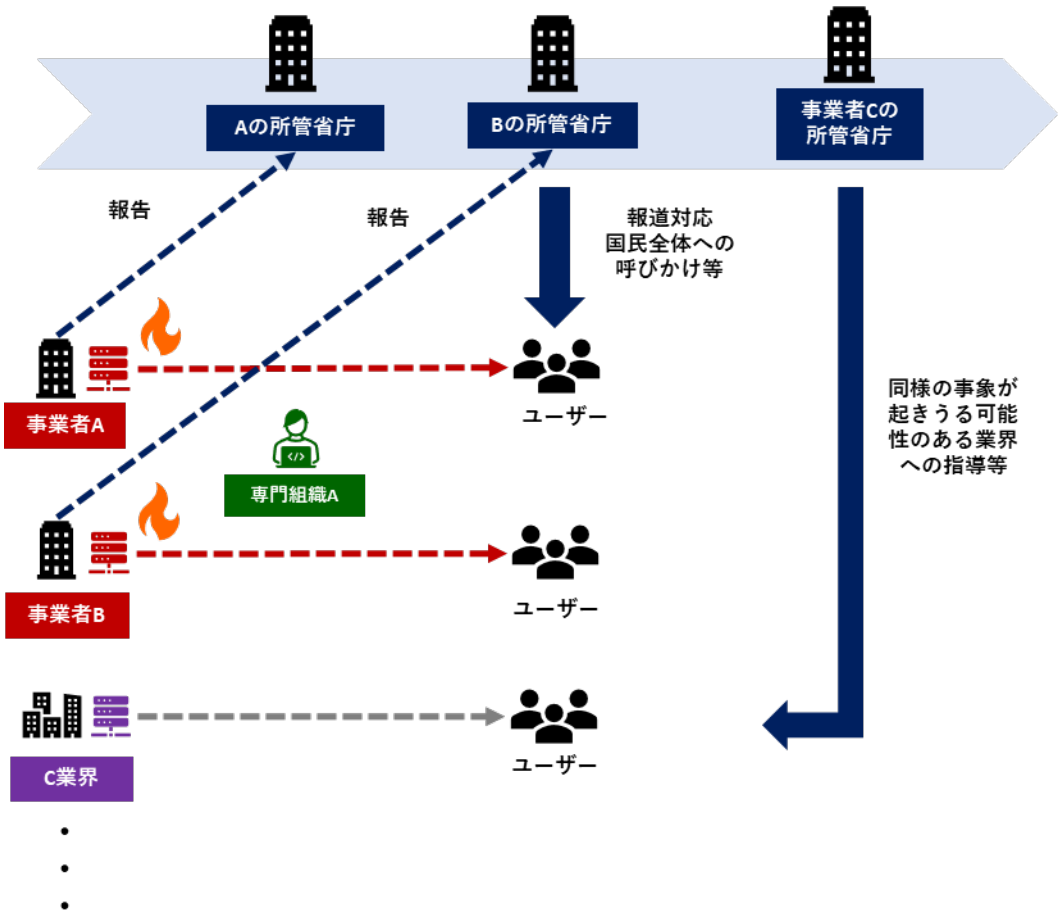


図 14

上述のとおり、影響範囲が大きいものをはじめとして、官民で協力してサイバー攻撃被害を低減するためには、法令に基づく報告等が求められていない業種等であっても、被害からの復旧が最優先ではありますが、できるだけ早期に所管省庁等へ報告・届出を行うことが必要です。

③警察による犯罪捜査を通じた抑止力の向上

サイバー攻撃の攻撃者の「意図」に対するものとして、警察による被疑者の検挙は、犯罪者に対して責任を負わせるとともに、犯罪を企てる他の者等に対して「検挙されるかもしれない」という警告を与えることで、将来的な犯罪の抑止にもつながるものであり、警察による犯罪の捜査は、社会の秩序維持という公益を図る上で大変重要な役割を果たします。また、国家の関与が疑われるサイバー事案の脅威が高まる中、被疑者の検挙まで至ることが困難な状況であっても、捜査を通じて把握された情報等からこうした脅威を分析し、パブリック・アトリビューション（サイバー攻撃の実行者やその行為の最終的な責任を有する国等に関する情報を、非難声明や刑事訴追の公表、分析レポートの発信等を通じて公表するもの。）

等の対応を講じることも、抑止力を向上させる上で重要です。

また、サイバー事案の被害防止のためには、被疑者の検挙等のほか、捜査で判明した手口等を踏まえた対策を講じるなど、警察と関係機関等が連携して、同種の犯罪が起きにくい環境を構築することも必要となります。

これら取組の推進に当たっては、被害を潜在化させないことが何より重要であり、被害組織からの警察への通報・相談及び捜査協力は社会的に極めて重要な意義を持つものであるといえます。

なお、仮に被害組織の内規等において、被害に係る情報の取扱いが厳格に定められていたとしても、警察への通報・相談及び捜査協力については、その社会的意義に鑑み、積極的に行われることが望ましく、これにより、更なる被害の防止を期待できます。

④サイバー攻撃対処の全体像から見た被害に係る情報の必要性

図 15 は中長期的に見たサイバー攻撃対処の全体像を示したものです。本ガイダンスでは主に左側の情報共有を取り上げていますが、政府においては NISC をハブとした各省庁間の連携強化に取り組んでいるところであり、上記のとおり、サイバー攻撃被害に係る情報のうち、攻撃技術情報や被害内容・対応情報がそれぞれ必要な先に伝わることで、サイバー攻撃対処が包括的に取り組まれることになります。技術情報は必ずしも被害現場からのみ見つかるものではありませんが、その質・量ともに限られています。基本的には被害組織から共有／提供される情報がサイバー攻撃対処の根幹をなしています。

他方で、インシデント対応現場では、いかに被害を把握し業務を正常な状態に戻すかということが最優先であり、限られたリソースの中で、同時並行／複数の外部とのやりとりを行うことは大きな負担となります。

いかに被害組織を保護し、過度な負担を避けながらも、こうしたサイバー攻撃対処に必要な情報の共有／提供を目指すのか。本ガイダンスはそのための視点を解説します。

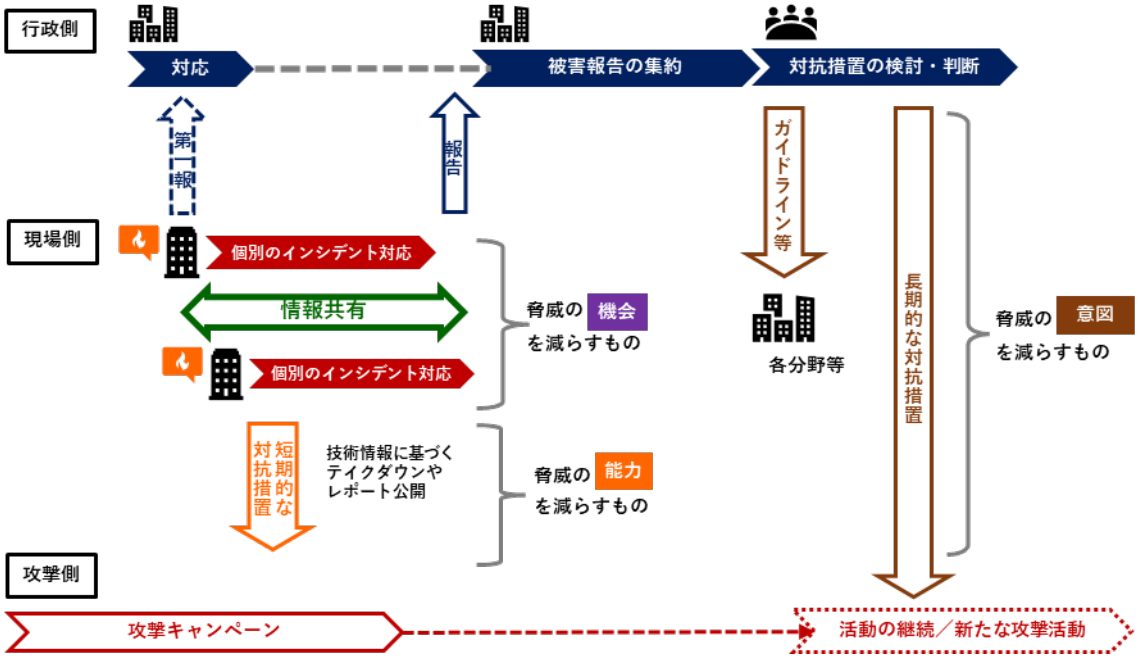


図 15

ー本ガイダンスを読むにあたって

本ガイダンスの想定読者と想定ケース

本ガイダンスは、主にサイバー攻撃を受けた被害組織を想定読者としています。サイバー攻撃を受けた場合、どのような情報をどのタイミングで、どのような主体と情報共有することが適当なのか検討するために実務上参考となるポイントを解説しています。

被害を認知した後に参考としていただくだけではなく、平時からのインシデント対応体制の整備や訓練にあたって参考としてお使いいただくことも想定しています。

本ガイダンスは、サイバーセキュリティ協議会の運営委員会の下に設置された、「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」でとりまとめられましたが、本ガイダンスの想定読者としては、サイバーセキュリティ協議会に参加する構成員のみならず、各構成員が参加する他の情報共有活動や、構成員でない組織においても活用いただくことを想定しています。

既に情報共有ルールを有する情報共有活動においては、本ガイダンス記載内容と異なる運営をされているケースもあるかと思われますが、本ガイダンスはなんら統一的な基準として示されるものではなく、情報共有の活性化に向けた参考として示すものです。

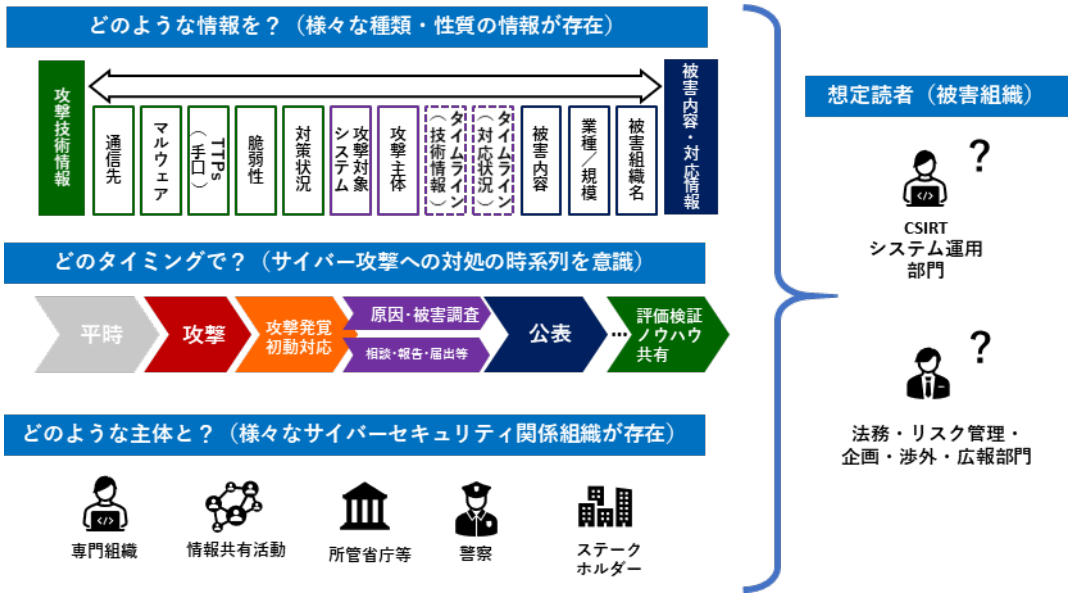


図 16

また、本ガイダンスにおいては、「被害組織保護」の観点で複数の Q&A 項目を記載しています。これは、サイバー攻撃被害に係る情報に触れる可能性のある、被害組織以外の関係者においても重要なポイントです。

被害組織との間で攻撃技術情報をやりとりする専門組織や情報共有活動の相手先だけではなく、公開情報／非公開情報としてサイバー攻撃被害に係る情報に接する関係者においても本ガイダンスをご参考いただくことを推奨します。

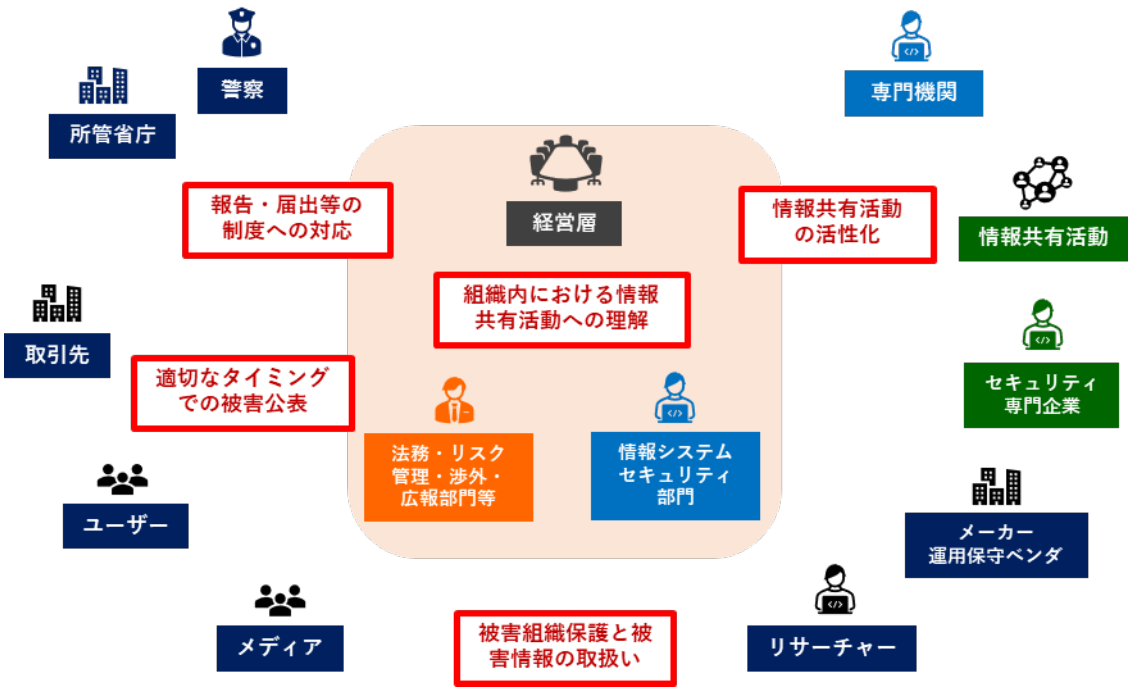


図 17

本ガイダンスの使い方

① 情報共有や公表のやり方がわからない場合の目安として

インシデント対応はどのような組織でも「初めて経験する」ことが大半です。特に法令や所管省庁等が定めるガイドラインで示されていない攻撃被害が発生した場合、従来、参考になるものがないケースが多かったと思われます。本ガイダンスはインシデント対応時の情報共有、被害公表の参考となる Q&A 集です。

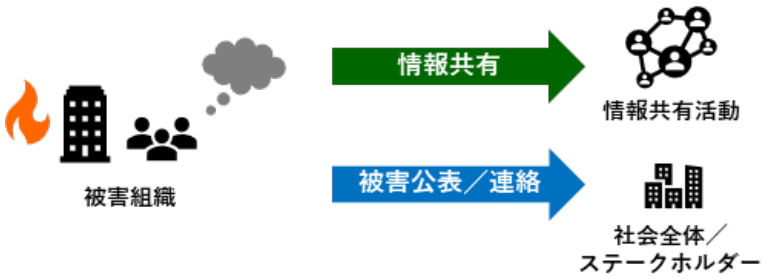


図 18

② 社内理解のための参照情報として

被害組織のシステム担当部門／セキュリティ担当部門においては外部への情報共有を行いたいと考えていても、事前に社内ルール整備等ができておらず、「未公表の段階で外部に情報を出すこと」自体をリスクととらえ、なかなか社内合意に至らないケースがあります。そうした場合に、どのような情報をどのように扱えば、自組織を保護しながらインシデント対応に必要な情報を集めることができるのか、本ガイダンスを参照しながら、説明を行うことができます。また、これから、インシデント発生時の体制整備／ルール整備を行うことを想定している組織においても社内理解促進のため、ケーススタディなどを活用することができます。

図 19

③ 調整の相手方への説明資料として

＜セキュリティ専門組織による被害組織への説明のために＞

セキュリティ専門組織において調査に必要な情報が不足するなどして、外部の情報共有活動に被害現場で見つかった攻撃技術情報を提供し、不足している情報を得たいと考える場合があります。この場合に、攻撃技術情報を外部の専門組織や情報共有活動に提供してよいか被害組織との間で調整する際に、共有の目的／効果、留意点等を説明するための資料として使うことができます。

図 20

＜複数の被害組織間の認識共有のために＞

連鎖的な被害が出ている場合など、被害組織同士で情報共有や被害公表に関する情報の取扱いについて調整しなければならない場合があります。前述のように、情報共有のための調整のほか、被害公表を行うにあたって、複数の被害組織間における認識の共有のために本ガイダンスを活用することができます。

図 21

２．情報共有・被害公表の流れ

FAQ に入る前に、情報共有・被害公表における情報の種類をまとめるともに、情報共有・被害公表の判断をどのように行うのか、簡易なフローを示しておきます。

詳しいチェックリスト、フローシートについては、５．（150 頁）を参照してください。

情報共有と被害公表における情報の種類のチェックリスト（簡易版）

	情報共有	被害公表
タイミング	可能な限り早期のタイミング	ケースバイケース ※二次被害発生のおそれなど注意喚起を目的とする速報が必要な場合はただちに公表
被害内容・対応情報 ・被害組織名 ・被害業種／規模 ・被害内容 ・対応のタイムライン	―	○
中間の情報 ・攻撃のタイムライン ・攻撃対象システムについて ・脆弱性悪用の情報等	△ ※共有に必要なものは専門機関への相談等を踏まえて共有することが望ましい	○
攻撃技術情報 ・マルウェア ・不正通信先 ・その他攻撃手法に関する情報	○	△

○：主な内容となる情報　　△：内容／状況による　　―：基本的に対象外

表 2

情報共有判断のためのフロー（簡易版）

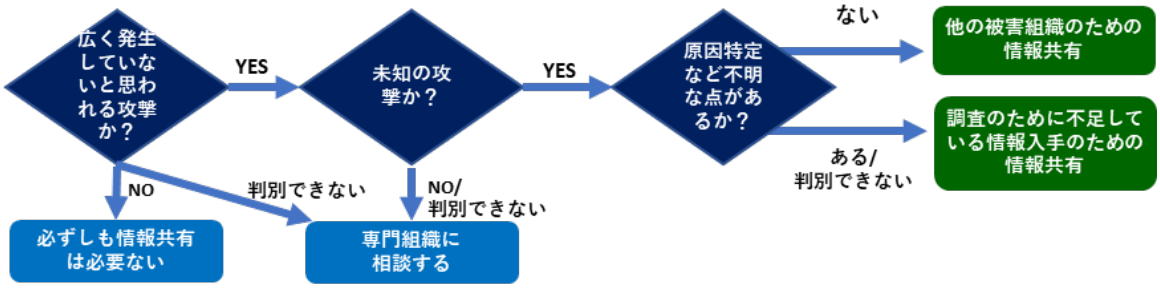


図 22

被害公表判断のためのフロー（簡易版）

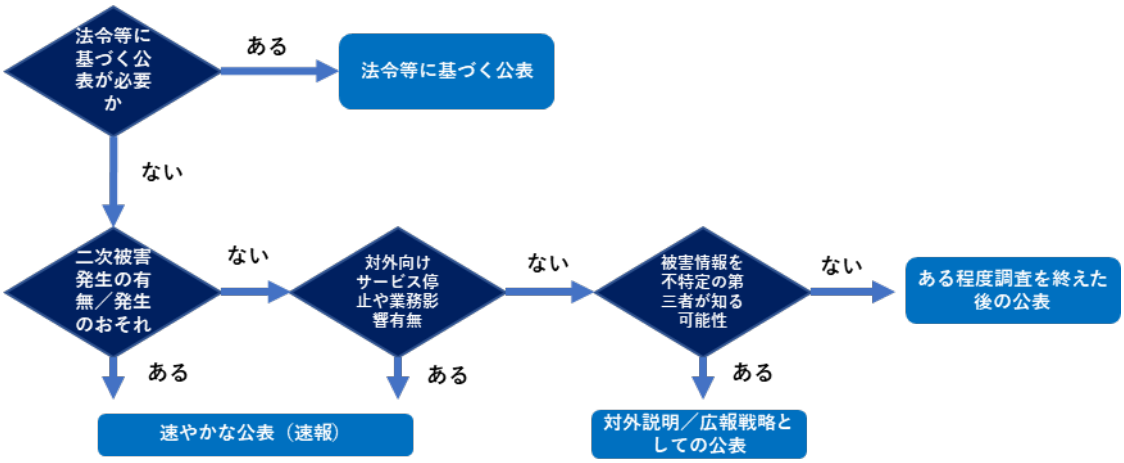


図 23

3．FAQ

＜情報共有の方法等について＞

Q1. なぜ情報共有が必要なのですか？

情報共有活動は

① インシデント対応に必要な情報を得るため

② 被害防止のための情報を得るため

の大きく２つの目的のために必要な活動です。

前者は被害組織個別の目的として、後者は攻撃者に標的とされている業界全体や参加する情報共有活動全体での目的として挙げられますが、後述のとおり、どちらか片方の目的のためだけに行われるものではなく、長期的な情報共有活動における相互のサイクルにより、参加する組織それぞれの利益となります。

攻撃者はセキュリティ対策を回避するため、複雑で高度な攻撃手法を編み出します。そのため、被害組織単独による調査だけでは攻撃原因や被害範囲の特定が困難なケースがあります。そこで、情報共有活動により「自組織だけでは見つけられなかった情報」を得ることを通じて、原因特定や被害範囲の特定を行い、被害拡大防止や適切な再発防止策を行う必要があります。

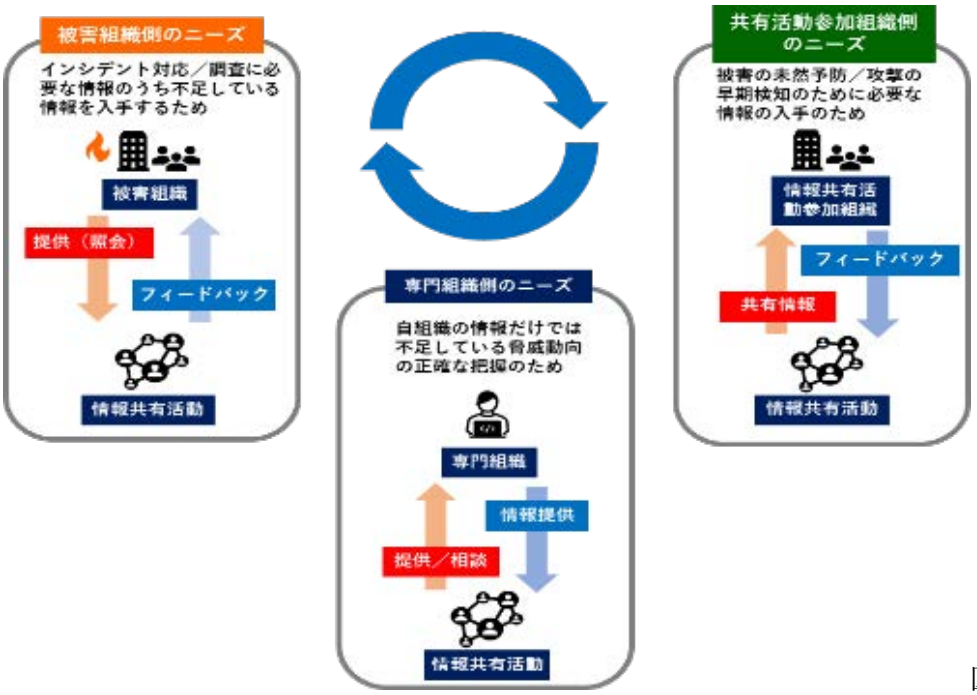


図 24

情報共有しないと何が起きるのか？

各組織においては様々なセキュリティ対策製品／サービスを通じて、不正通信先や新たに登場したマルウェアの検知への取組みが日々行われていますが、製品／サービスの検知をすり抜けようとする新たな攻撃手法や特定の業種／分野だけを限定的に狙う攻撃が登場すると、製品／サービスによっては、対応が間に合わない可能性があるため、このタイムラグを埋めるために、情報共有活動による情報入手が必要になります。

攻撃者は一定期間において、攻撃手法や攻撃インフラ（用語集を参照）を使いまわす傾向があります。図 25 は、そうした攻撃活動と被害組織の関係を図示したものですが、情報共有活動により、「使いまわされる攻撃手法／攻撃インフラ」に関する情報が共有されていない場合、どのような状況が起きるでしょうか。事案 B では侵害された端末をすべて調査することができていますが、事案 A ではまだ検知できていない被害端末が存在しています。事案Cに至っては、また侵害自体を認知できていません。

この 3 つの事案における被害組織の間で情報共有を行うことができれば、

事案 A の被害組織：未検知のマルウェア Y、通信先 Y への不正通信を見つけることができる

事案 B の被害組織：調査漏れがないか確認できる

事案 C の被害組織：侵害に気づくことができる

を行うことができます。

事案 A の被害組織は、「自組織だけでは見つけられなかった情報（マルウェア Y)」を得るために、「(事案 A の被害組織にとって）自組織で見つけた情報（マルウェア X)」を共有することになりますが、この情報は事案 C の被害組織にとっては「見つけられなかった侵害自体の情報」となります。こうした 3 者間の情報の交換が情報共有活動の意義となっています。

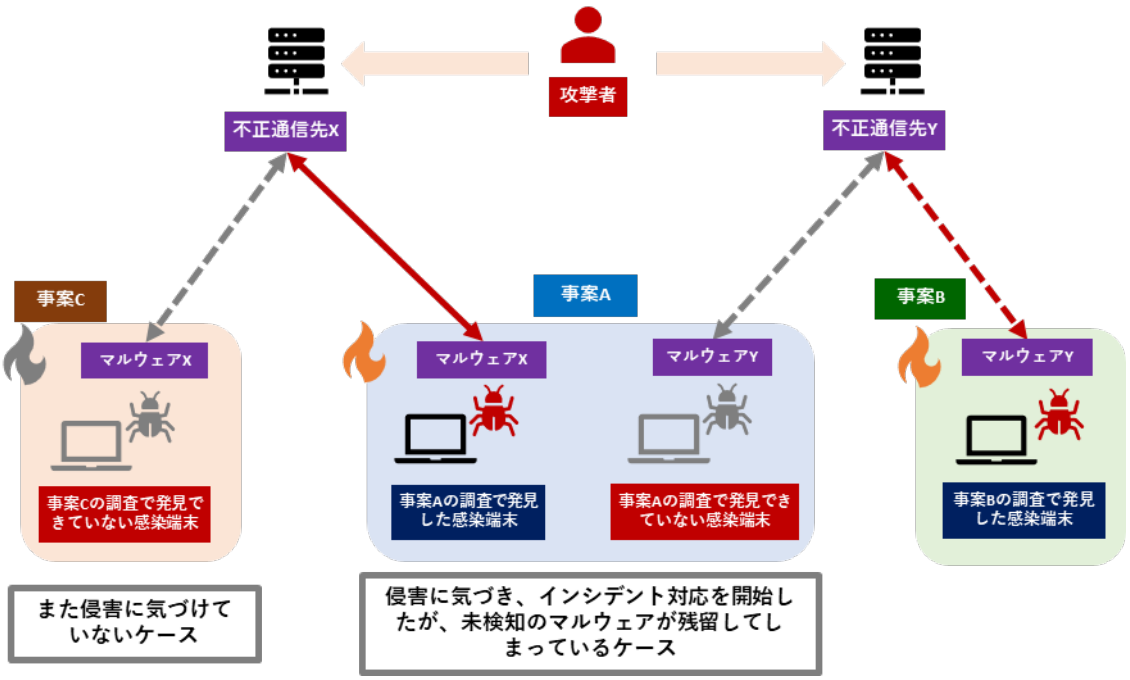

攻撃者
不正通信先X
不正通信先Y
事案C
事案A
事案B
マルウェアX
マルウェアX
マルウェアY
マルウェアY
事案Cの調査で発見できていない感染端末
事案Aの調査で発見した感染端末
事案Aの調査で発見できていない感染端末
事案Bの調査で発見した感染端末
また侵害に気づけていないケース
侵害に気づき、インシデント対応を開始したが、未検知のマルウェアが残留してしまっているケース

図 25

Q2. どのタイミングでどのような情報が共有／公表されますか？

情報共有活動のフェーズは主に、短期・中期・長期に分けることができます。短期的には、本ガイダンスの Q3（37 頁）～Q8（57 頁）で解説するようなインディケータ情報の交換を通じた早期検知／被害拡大予防のための活動であり、基本的に非公開で行われます。中長期的なものは、被害公表や、専門組織によるレポート発信により公開情報となった情報を中心とした社会全体における情報の共有、専門組織同士で行われる攻撃活動の追跡や分析、情報交換を挙げることができます（※）。

※　なお、被害公表に関しては、その具体的なタイミングはケースバイケースですので、Q15（71 頁）を合わせて参照してください

Q8（57 頁）で解説するように、情報共有効果を得るためには早期の共有が必要であり、比較的調査初期の段階で見つかるマルウェアや不正通信先情報を中心としたインディケータ情報（Q7（51 頁）参照）をまず共有します。

その後調査が進むことで判明する TTP 情報（Q7（51 頁）、Q28（106 頁）参照）などの攻撃の詳細は専ら専門組織からのレポート発信などを通じて広く共有され、被害の詳細や対応経緯、再発防止策などの情報は被害組織からの被害公表を通じて社会に共有されます（Q16（72 頁）参照）。

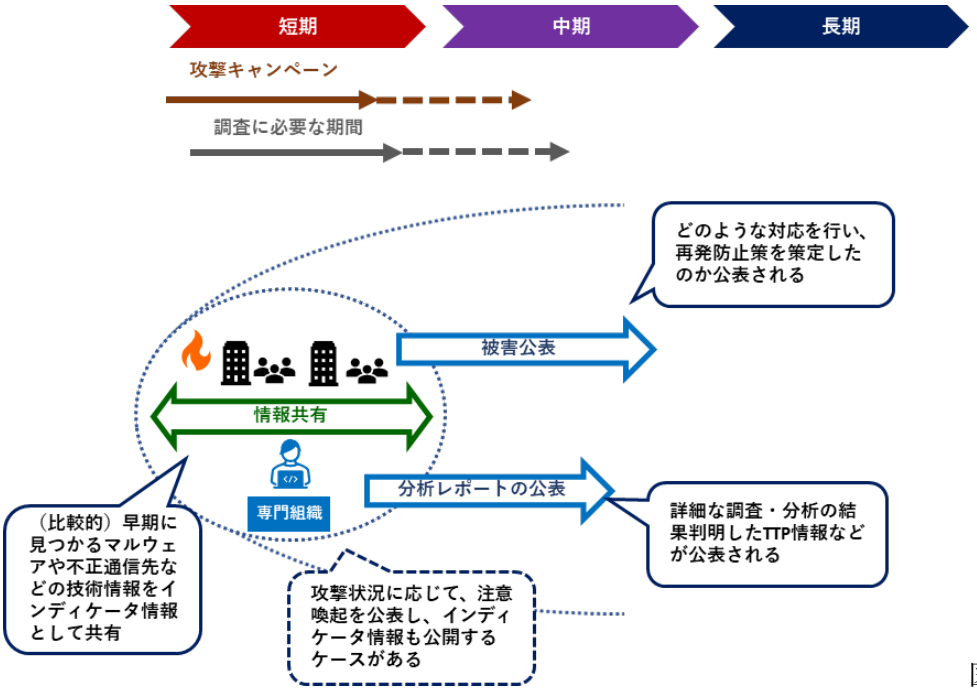


図 26

Q3.「被害組織」とは何ですか？

あくまで本ガイダンスの検討スコープにおける整理ですが、攻撃を受けた対象（システム）の管理者／利用者という観点から大きくは以下のパターンの整理ができます。

① 自組織で管理・運用するシステムやネットワークが侵害された組織
② 運用保守ベンダ経由で侵害された場合のユーザー組織と当該ベンダ
③ クラウドサービスやベンダ管理のシステム上で稼働しているシステムのユーザー組織と当該ベンダ（※サービスやシステムを提供している事業者側が管理する領域が侵害ルートとなった場合）

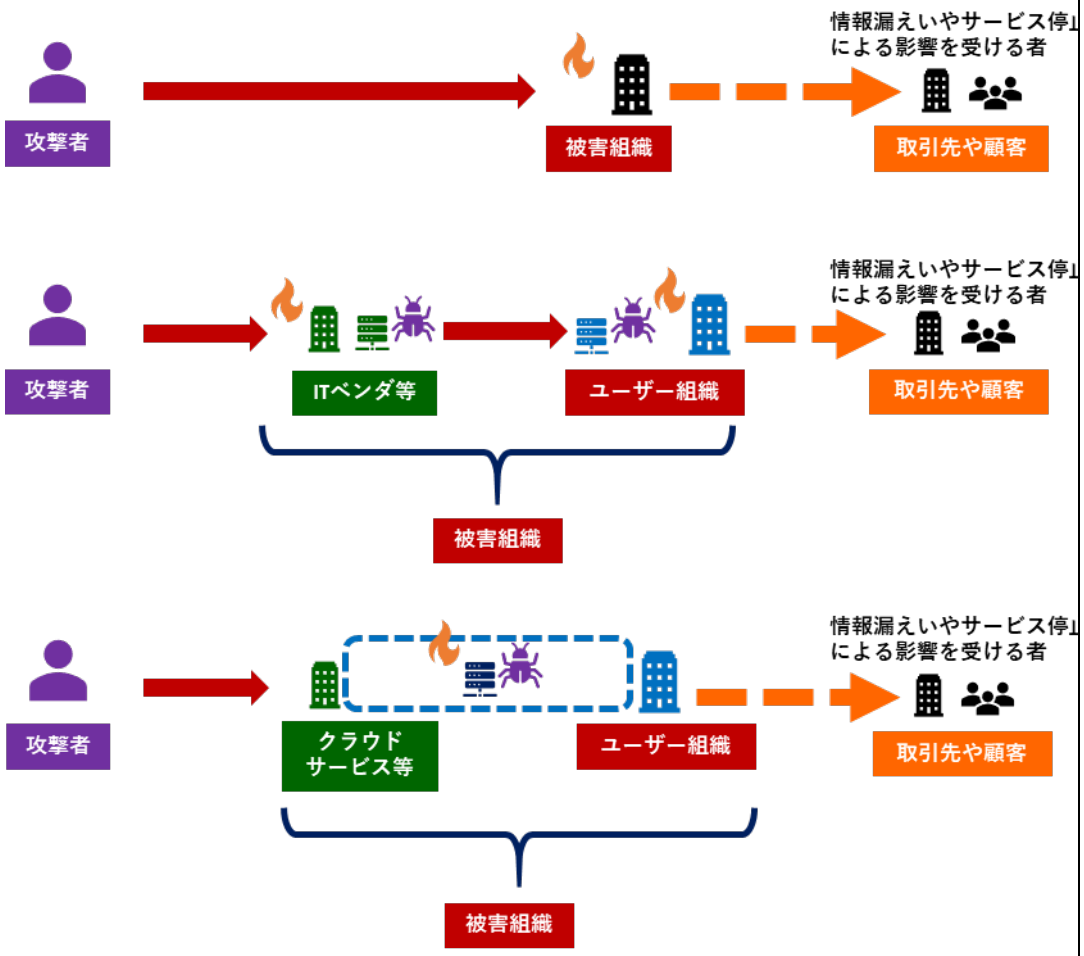


図 27

Q4.サイバー攻撃被害に係る情報にはどのようなものがありますか？

サイバー攻撃被害が発生した場合、①被害内容や被害組織の対処内容を示す情報と、②攻撃者の活動や攻撃方法を示す情報の大きく２つの情報が発生・発覚します。本ガイダンスでは前者を「**被害内容・対応情報**」、後者を「**攻撃技術情報**」と呼称します。

被害内容を示す情報（被害内容・対応情報）は、「どの組織で被害が発生したのか」「どのような情報が漏えいしたのか」といった、被害組織固有の内容や、取引先や顧客等他の被害者に関する機微な情報を含みます。したがって、適切な取り扱いや公表等のタイミングの調整が不十分な場合、二次被害発生のおそれがあります。

他方で攻撃方法を示す情報（攻撃技術情報）は、「不正アクセスの通信元」「見つかったマルウェアやその通信先」などの情報であり、同じ攻撃が行われた複数の被害組織間で同じ情報が見つかります。こちらの情報は、被害内容を示す情報（被害内容・対応情報）とは逆に、被害組織以外の組織と共有されないことで、同一攻撃による被害を防止することができず、被害が拡大するおそれがあります。

被害内容・対応情報（被害内容を示す情報）	被害組織名	―
	業種／規模	―
	被害内容	・感染台数、侵害範囲について ・漏えいした情報の種類や件数、内容について ・システム停止やデータ損失によるサービス停止など
被害内容・対応情報と攻撃技術情報が混在	タイムライン（対応状況）	被害組織がどのような対応を行ったのかという時系列
	タイムライン（技術情報）	攻撃者がどのように侵害したのかという時系列
	攻撃対象システム	攻撃対象となったシステムに関する情報
	（被害対象の）対策状況	攻撃対象となったシステムにおいて事前に取られていたセキュリティ対策／設定に関する情報
	攻撃主体に関する情報	攻撃グループ名や攻撃者が他にどのような攻撃活動を行っているのかという情報
攻撃技術情報（攻撃方法を示す情報）	脆弱性関連情報等	悪用された脆弱性の有無やその詳細について
	マルウェア	現場で見つかったマルウェアに関する情報（※マルウェア検体そのものは含まない場合もある）
	通信先	不正アクセスの通信元やマルウェアの通信先など
	その他 TTP 情報(攻撃の手口)	上記以外の攻撃者が用いた攻撃手法に関する情報

表 3

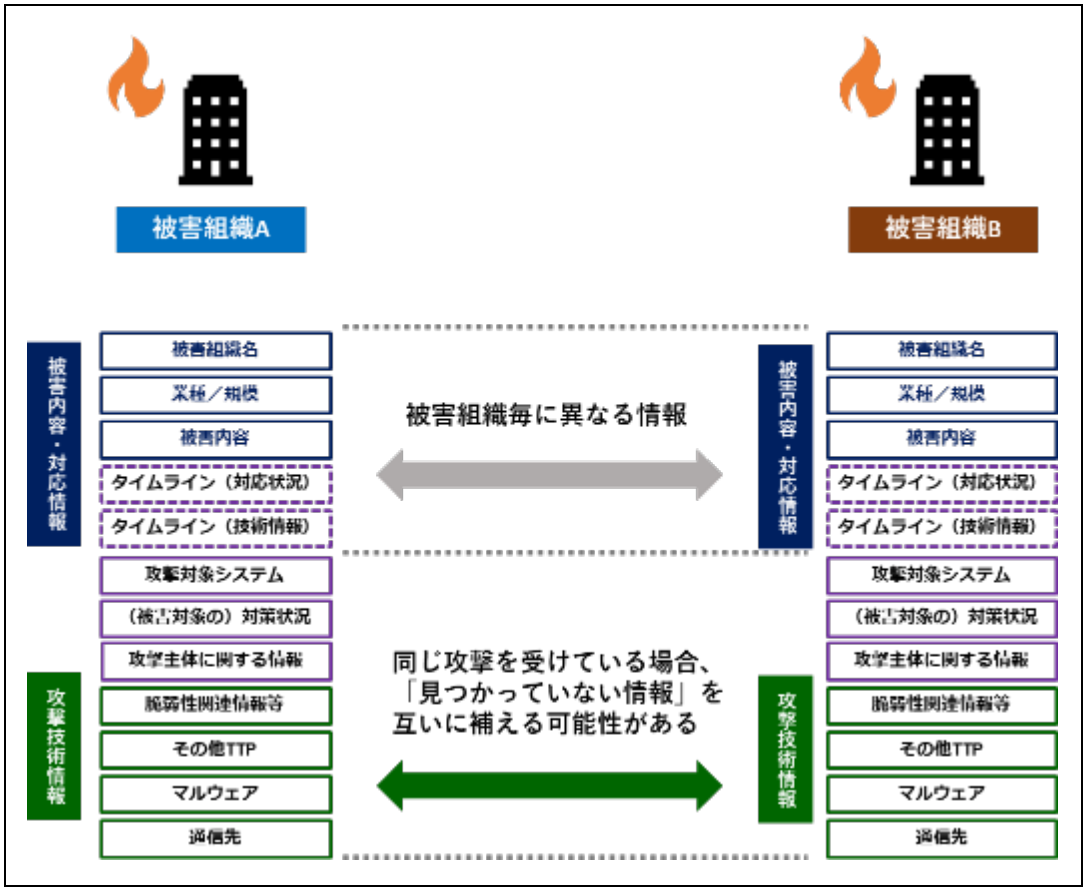

被害組織A
被害組織B
被害内容・対応情報
被害組織名
業種／規模
被害内容
タイムライン（対応状況）
タイムライン（技術情報）
攻撃技術情報
攻撃対象システム
（被害対象の）対策状況
攻撃主体に関する情報
脆弱性関連情報等
その他TTP
マルウェア
過信先
被害組織毎に異なる情報
同じ攻撃を受けている場合、
「見つかっていない情報」を
互いに補える可能性がある

図 28

サイバー攻撃被害に係る情報について

以下は、過去の複数の事案に関する情報を元に架空のインシデントに関する被害組織からのプレスリリースと、専門機関に相談・情報共有依頼をしたときの文面をイメージとして示したものです。被害内容・対応情報や攻撃技術情報のそれぞれの項目がどういった情報のことを指しているのか簡単に解説します。なお、あくまでイメージですので、下記の書きぶり等が本ガイダンスとしてなんら推奨する文面でない点にご注意ください。

弊社システムに対する不正アクセスについて

×月１日

＊＊＊＊＊株式会社

被害組織名

弊社の○○システムが外部からの不正アクセスを受けたことが判明しました。

専門組織とともに調査を行い、原因特定や被害情報の確認を行うとともに、影響のあった関係各所への報告を行っております。

引き続き、再発防止に向けた対策・体制強化に取り組んでまいります。

１．　経緯と対応の流れ

○月１日	攻撃者が○○システムで稼働するソフトウェアの脆弱性を突いて侵入し、マルウェアを設置
○月２日	○○システムから社内の複数のサーバへ侵害拡大
○月５日	一部のサーバでシステム障害が発生したため調査を行ったところ、不審なアクセスを確認したため、不正アクセスの疑義がある事案として調査を開始
○月６日	不正アクセスにより社内Ｎに侵入されたと判断し、社内のインシデント対応チームを中心にインシデント対応を開始
○月７日	セキュリティベンダＡに調査依頼をするとともに、専門機関Ｂにインシデント対応相談。Ｃ県警察に連絡。
○月 15 日	調査の結果、侵入経路が○○システムで稼働するソフトウェアの脆弱性を突いたことであると特定し、ソフトウェアのバージョンアップ等の対処を実施
○月 20 日	見つかったマルウェアの解析結果などを元に、現時点で攻撃者の侵入やマルウェアの残留はないと判断
○月 27 日	侵害された○○システムや複数のサーバの調査から、被害内容を精査し、影響のあった関係先への報告を開始
○月 30 日	暫定的な再発防止策の実施を完了

タイムライン（技術情報）

タイムライン（対応状況）

２．　被害内容

・〇〇システム内には技術情報、取引先に関する情報、個人情報等の機微な情報は保存しておらず、侵入した攻撃者によって認証情報が窃取されたと判断しています。

・さらに侵害を受けた複数のサーバのうち、一部のファイルサーバ内に、取引先企業との個別プロジェクトで使用していた情報が含まれており、漏えいした可能性が否定できなかったため、取引先へその旨の連絡を行いました。取引先との確認の結果、取引先に二次被害等が発生する可能性は低いと判断しています。

・その他、社内ネットワークの認証情報やサーバ等の設置情報が攻撃者により窃取されたと判断しています。

被害内容

３．　原因と再発防止策

今回の侵入はインターネットに接続されている〇〇システム上で稼働するソフトウェアの脆弱性が悪用されたものであったと判明しています。当該脆弱性は侵入の１週間前に修正プログラムが公開されていましたが、定期的なメンテナンス時にアップデート作業をする予定であったため、侵入時点でバージョンアップがなされていませんでした。

今後、専門機関等が出される脆弱性に関する情報を精査し、速やかに対応が必要なものについて優先度を設けて対処するよう、社内ルールや体制整備を進めてまいります。

また、攻撃者に侵入された後の侵害拡大については、ネットワーク設定やサーバの設定で防ぐことが可能だった点が認められたため、これら設定の変更による対策強化をすすめてまいります。

攻撃対象システムや対策状況

図 29

被害組織から外部の専門機関へ相談・情報共有依頼をしたときの文面（イメージ）

※やりとりはこの１回だけではなく、実際には複数回のやりとりにおいて、専門機関による解析結果や情報共有活動に照会した結果（フィードバック情報）の返信、被害現場から見つかった追加情報の送付等が行われます。フィードバック具体例については、後述の「４．ケーススタディ」（122 頁）をご参照ください。

Ｂ組織 ご担当者様

先日ご相談した弊社ネットワークへの不正アクセス事案ですが、セキュリティ企業Ａと調査を進めていたところ、以下のような情報が見つかっております。攻撃手法や対策について情報の共有をお願いいたします。

・先日ご相談の際にご指摘を受けた○○システムで稼働するソフトウェアについてバージョンを確認したところ、古いバージョン（ver.2.1.1）であったことが判明。脆弱なまま稼働していた原因については現在調査中

・○○システムと△△サーバ上で不審なファイルが見つかり、セキュリティ企業Ａの解析ではマルウェアＸではないかとのことで、現在詳細を調査中

見つかった不審ファイル
ファイル名：＊＊＊＊＊＊＊＊
ハッシュ値：(SHA-256)
設置日時：○月１日 0:15 JST
通信先：(IP アドレス)

攻撃対象システムや対策状況

マルウェア

通信先

図 30

被害現場ではどのような情報が見つかるのか／見つからないのか

特に情報共有の対象となり得るような高度なサイバー攻撃では、下の図 31 のような流れで侵入からマルウェアの実行、目的の実行（情報の窃取等）が行われます。調査により、それぞれの攻撃者が活動したポイント毎に技術的な痕跡が見つかり、また、どのような対象のシステムがどのような被害にあったのか見つかっていきます。

ただし、実際のインシデント対応現場では、例えば通信ログの保存期間が不足しており、いつどのような通信が（侵害当時）行われたのか見つけることができなかったり、攻撃者が被害組織のネットワーク内／サーバ内を動いた痕跡を消去したことで、どのくらいの範囲まで侵害されたのか、あるいはどのような情報が閲覧／窃取されたのか追跡できなかったりするケースが多く見られます。

そのため、高度なサイバー攻撃に対しては、先述のとおり、情報共有により調査に必要な攻撃技術情報を外部から得ることがインシデント対応を行う上での重要なポイントとなるのです。

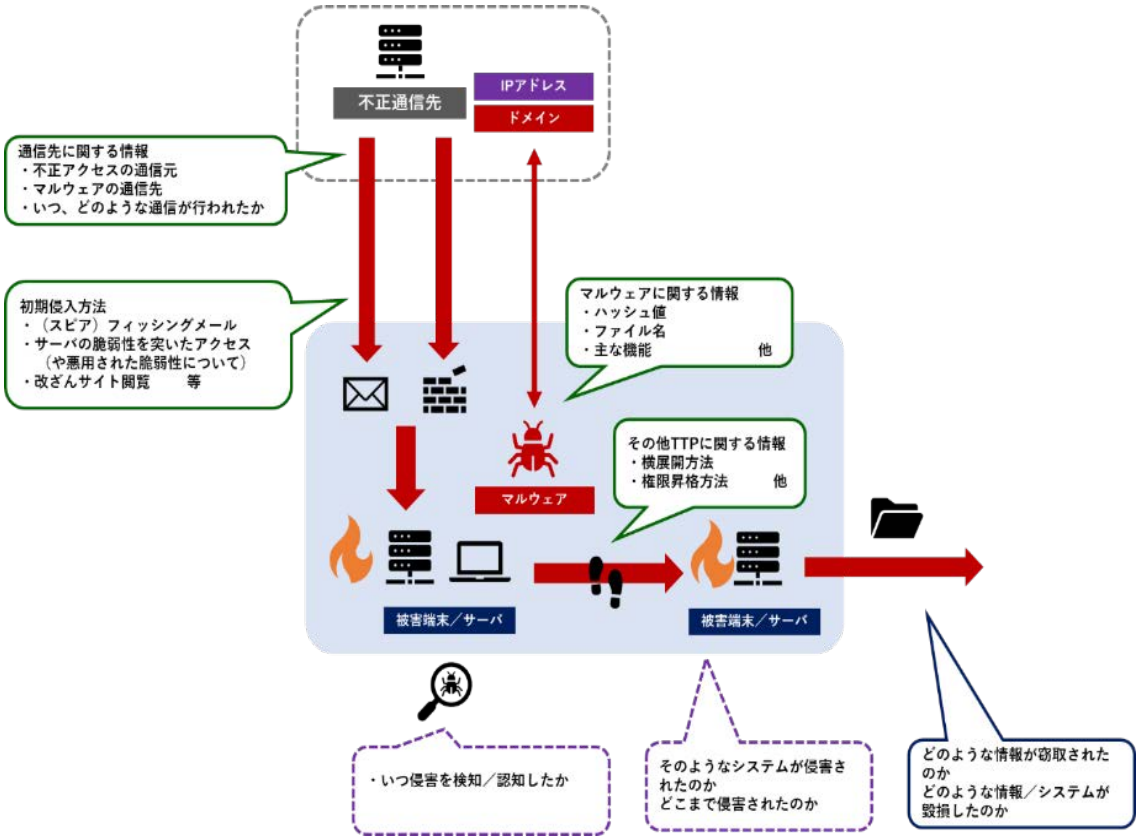


図 31

Q5.どうやって「情報共有」をすればいいのですか？

攻撃技術情報の共有については

・参加している情報共有活動のハブ組織に情報提供し、共有してもらう（ハブ・スポーク型）

・参加している情報共有活動の参加者に対して、自ら情報提供する（ｎ対ｎ型）

・情報共有活動とかかわりのある専門組織に情報提供し、共有してもらう（間接／代理型）

の大きく３つの方法があります。実際に情報を伝達する手段としては、メールやポータルサイト経由など、情報共有活動により様々ですが、情報を非公開のまま安全に渡すことができる方法が選択されます。

匿名での情報共有活動参加を選びたい場合はハブ・スポーク型、仲介役を挟まず直接情報の交換を行いたい場合はｎ対ｎ型、そして、普段は情報共有活動に参加していないが、インシデント対応等で情報共有の必要性が発生した場合などは間接／代理型として、共有活動の窓口組織や、共有活動にコンタクト可能な専門組織に依頼することができます。

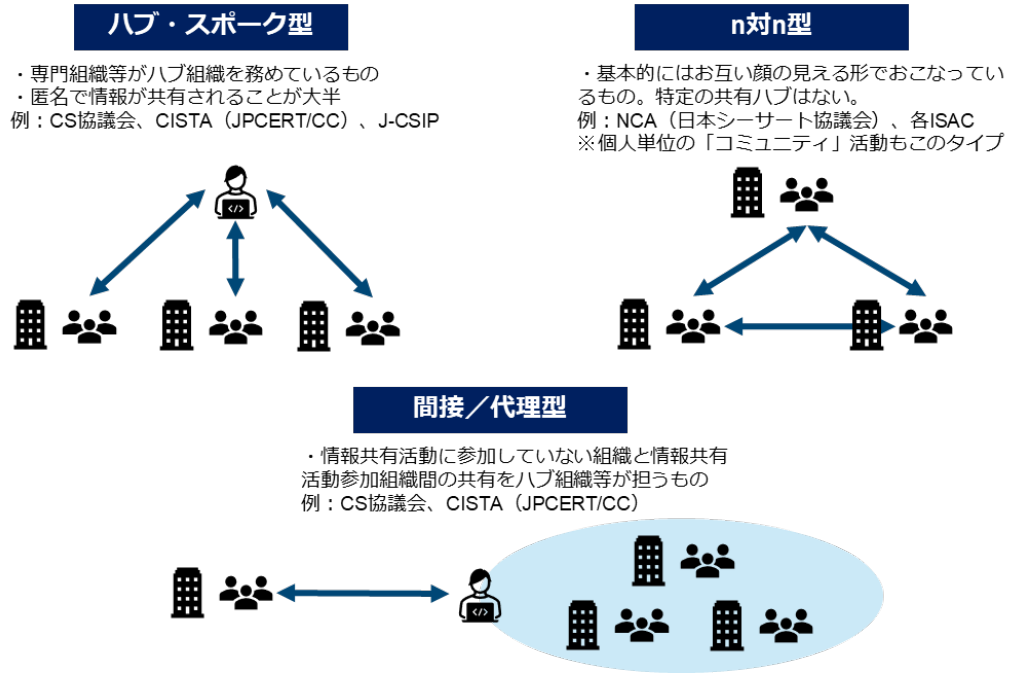


図 32

なぜ、共有は「関係者限り」で行われるのか？

情報共有活動は基本的に非公開で、あらかじめ決められた参加者内限りで行われます。「そんなに有益な情報であれば広くあらゆる組織に展開すべきじゃないか」という指摘があるかと思われますが、以下のとおり、「非公開で行う共有」と「公開で行う注意喚起」の使い分けが行われています。
Q6（47 頁）で解説したとおり、主に情報共有効果が見込まれるのは、

条件（A）：共有対象とする攻撃類型
　特定の範囲／対象に行われていて、まだ広く認知されていない攻撃に対して
条件（B）：共有対象者の範囲
　ある程度同じ攻撃を受ける可能性のある範囲／分野内において
条件（C）：共有タイミング
　可能な限り速やかに共有を行う

ことができた場合です。特に（A）の条件があるため、情報の取扱い次第では、当該時点では被害未公表である情報提供者＝被害組織が特定されてしまったり、Q22（92 頁）で解説するような攻撃の踏み台となった第三者に関する情報が保護されなかったりするおそれがあるため、情報が適切に扱われ、情報提供者やその他第三者の不利益にならないよう配慮が必要であることから、情報展開／共有先のコントロール（Q6（47 頁）、Q30（109 頁）参照）が必要になります。これが必然的に、条件（B）と同じこととなり、ある程度の限定された範囲内で情報共有活動が行われることになります。
　また、「情報を展開しても情報提供者や第三者の不利益にならない」ことをチェックしようとするためには時間がかかるところ、条件（C）を満たすためには、このチェックにあまり時間をかけることはできないことから、万が一展開した情報が情報提供者や第三者の不利益になるような情報を含んでいたとしても影響を最小限にし、また、展開された情報の追跡が可能なように、やはり、関係者を限定することになります。

　他方で、条件（A）ではない状態、つまり広範囲に攻撃が発生している、もしくは発生する蓋然性が高いと思われる場合には、情報共有ではなく、公開による注意喚起を行い、広く注意を呼びかけ、対策情報を伝える必要があります。

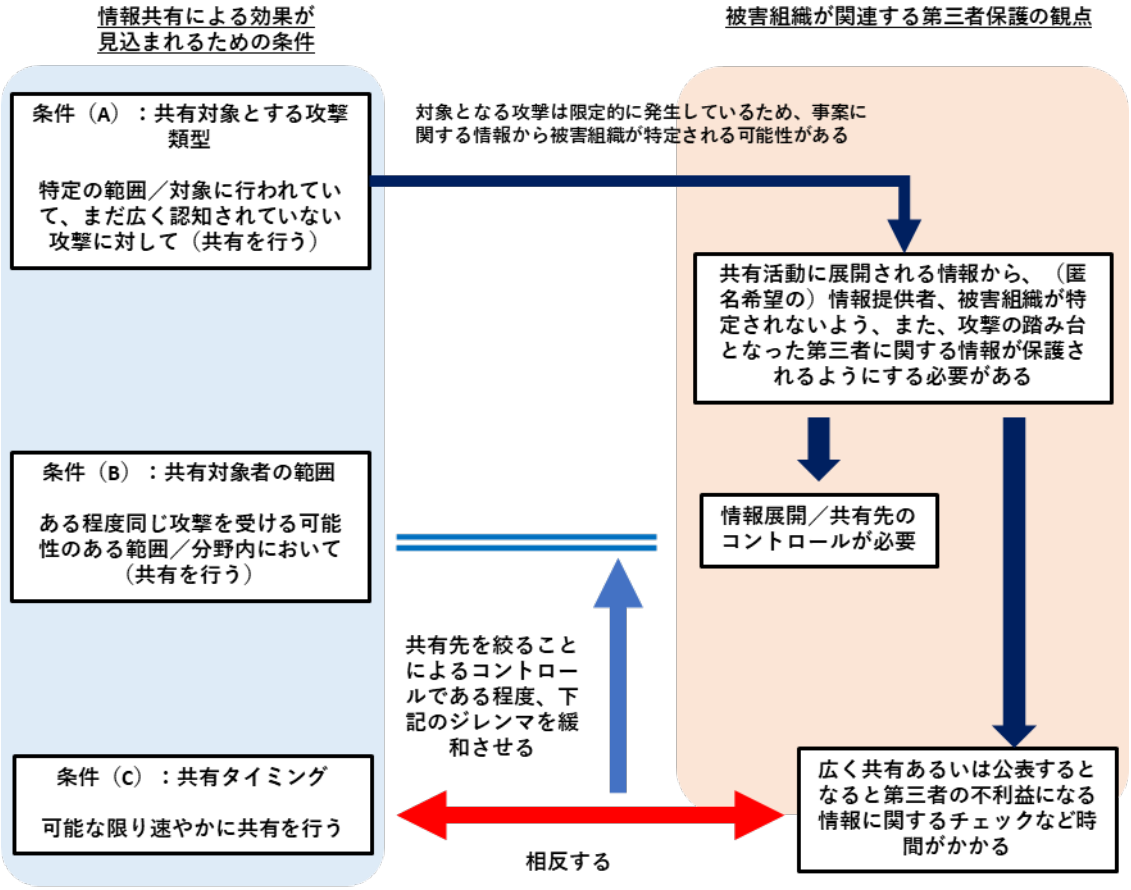

情報共有による効果が
見込まれるための条件
被害組織が関連する第三者保護の観点
条件（A）：共有対象とする攻撃類型
特定の範囲／対象に行われていて、まだ広く認知されていない攻撃に対して（共有を行う）
対象となる攻撃は限定的に発生しているため、事案に関する情報から被害組織が特定される可能性がある
共有活動に展開される情報から、（匿名希望の）情報提供者、被害組織が特定されないよう、また、攻撃の踏み台となった第三者に関する情報が保護されるようにする必要がある
情報展開／共有先のコントロールが必要
条件（B）：共有対象者の範囲
ある程度同じ攻撃を受ける可能性のある範囲／分野内において（共有を行う）
共有先を絞ることによるコントロールである程度、下記のジレンマを緩和させる
条件（C）：共有タイミング
可能な限り速やかに共有を行う
相反する
広く共有あるいは公表するとなると第三者の不利益になる情報に関するチェックなど時間がかかる

図 33

Q6.どのような情報を共有すればいいのですか？

基本的には、サイバー攻撃の被害に関する情報のうち、**攻撃技術情報**を共有することが有効です。特に、「インディケータ情報」と呼ばれる技術情報の共有が被害防止に効果的です。「インディケータ情報」の具体的な説明は次の Q7（51 頁）をご覧ください。

共有効果のある攻撃技術情報についてもう少し詳しく説明すると、

① 他の標的組織に向けても使われている可能性のある攻撃手法／痕跡などの**攻撃技術情報のうち**公表されていないもの

または

② 攻撃手法／痕跡などの**攻撃技術情報**について公表情報があるが、国内に向けた攻撃活動についてはいまだ公表されていないもの

に関する情報を共有することで、情報共有による効果を得ることができます。ただし、自組織の調査によって見つかった攻撃技術情報が既に公表されているものなのか、そうでないのか調べることが難しい場合もあるため、まずは調査支援をしているセキュリティベンダや専門機関に照会をかけることが有効です。

また、共有前の段階では、攻撃に関する情報が断片的であっても、Q1（33 頁）のとおり、情報共有活動を通じて「フィードバック」を得られる可能性があるため、情報提供する価値があります。

具体的な情報の種類については、後述の
Q.マルウェアに関する情報とはどういうものですか？
Q.不正通信先に関する情報とはどういうものですか？
Q.攻撃の手口に関する情報とはどういうものですか？
をご覧ください

どのような情報を共有すれば効果があるのか？

例えば、日々送られてくるスパムメールや Web サーバなどに大量に行われるスキャン通信などは、共有の効果がまったくないわけではありませんが、情報の受渡しに係る作業コストに比べて、得られる効果は低いと考えられます。また、情報共有活動に参加する組織以外にも多くの関係者が同じ攻撃を観測していることから、既に様々な製品／サービスで対処が可能なようになっていたり、専門機関等が公開情報として注意喚起をしていたりするケースが大半です。

一方で、**ある程度特定の分野／組織を絞り込んだ攻撃**や、広範囲に向けた攻撃ではあるものの、まだ**公開情報を通じて広く知られていない攻撃**に関する情報は、対応／調査にあたるベンダや製品／サービスでの対応が追い付いていない可能性があるため、情報共有を行うことによって、他の被害を未然防止するだけでなく、自組織の被害の詳細調査に資する情報が**情報共有活動のフィードバック**（Q1（33 頁）参照）から得られる可能性があります。

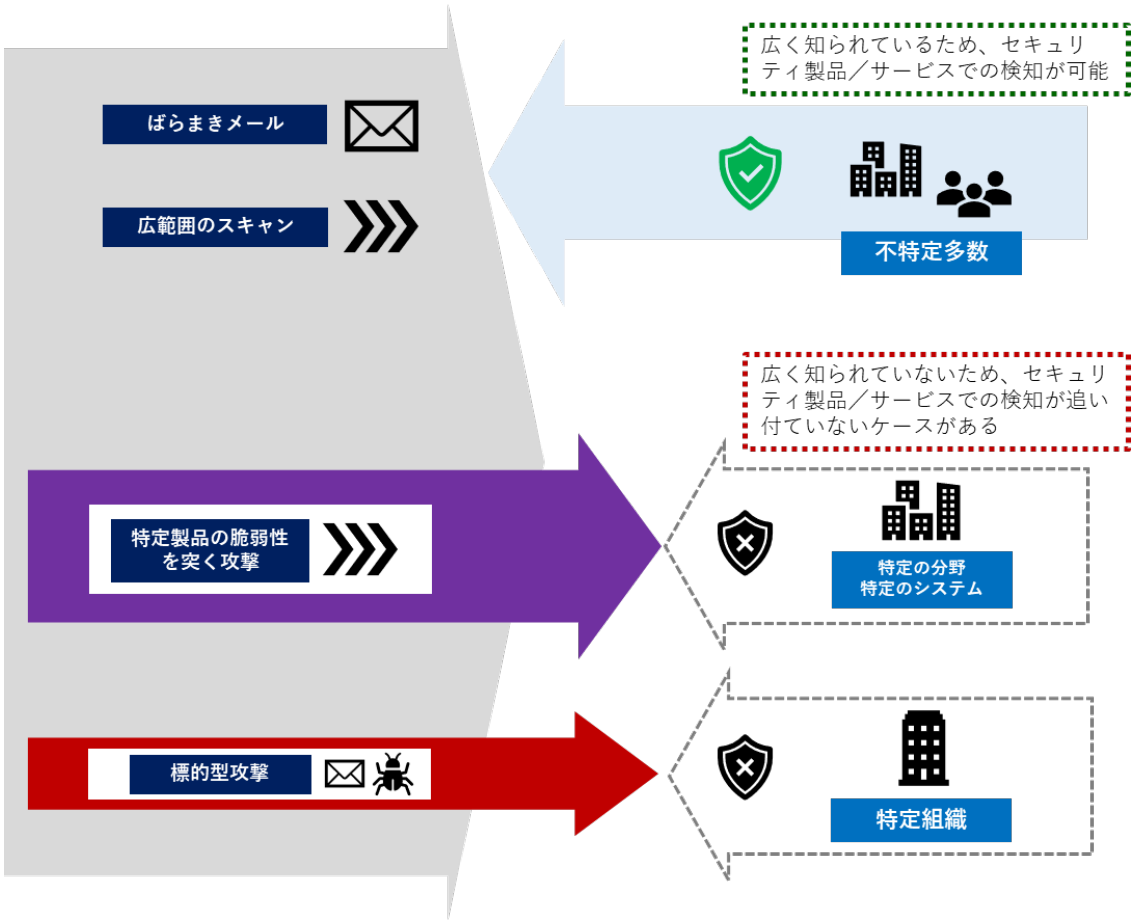


図 34

攻撃技術情報を共有するときの留意点

情報共有をしたとしても、共有先の組織が活動しづらかったり、フィードバックを得にくかったりする場合があります。攻撃発生時期が相当古いものや、共有情報があまりに断片的な場合などが想定されます。

例えば、攻撃が 1 年以上前など、過去に発生していた場合、マルウェアの通信先情報を共有しても、共有先組織における 1 年以上前の通信ログがないため、活用されない可能性があります（Q8（57 頁）の「情報共有タイミング」（58 頁）参照）。あるいは、マルウェアのハッシュ値だけ共有しても、別の攻撃先にはハッシュ値は異なるが性質は同じマルウェア[7]が使用されていた場合、照合することはできず、フィードバックを得ることは困難です。

Q8（57 頁）で解説したとおり、攻撃技術情報の共有においては、調査を経てすべての情報が把握できるまで待たず、速やかな情報共有が望ましいところ、現時点で見つかっている情報が断片的な場合であっても、必ずしも共有効果がないわけではなく、複数要素（マルウェア情報、不正な通信先情報、その他）を組み合わせることや、下記のような注意点に配慮することで共有効果を得ることが可能です。

単独の情報では共有効果があまり得られない情報の種類と回避策

情報の種類	単独で共有した場合の問題点	回避策
通信先の IP アドレス	・FW のログ上では IP アドレスとして見えていても、実際には紐づいていたドメイン宛の通信である場合がある ・タイミングによっては、別の正規サービスに紐づいてしまっている場合がある	・紐づいていたドメインの有無や、確認できていない旨を付記する ・不正な通信が発信していた日時を付記する
通信先のドメイン名	攻撃者が共有ドメインや DDNS サービスを使っている場合、サブドメインまで含めた FQDN で示さないと正規のサービスも巻き込んでしまう場合がある	FQDN での記載をする
マルウェアのハッシュ値	攻撃者が標的毎に設定値等が異なった同一マルウェアを使用している場合、ハッシュ値が異なってしまい照合できない	（判明している範囲において）マルウェア名（検知名や解析した専門組織の見解など）やファイル名、ファイルサイズなどのマルウェアの解析結果を付記する

[7] 同一の種類のマルウェアであっても、攻撃者が攻撃先（被害組織）に応じて機能の追加や変更を行って攻撃に使用した場合、異なるハッシュ値になってしまいます。

悪用された脆弱性情報	脆弱性情報（名称／CVE 番号）だけ共有しても、各組織において侵害痕跡を探し出せない場合がある	・当該脆弱性が悪用されたことを示すログの痕跡や書き換えられた設定情報、設置された不審ファイルなどの「悪用痕跡」に関する情報とセットで共有する
その他攻撃手法に関する情報	特に侵害後の横展開手法などについては、被害組織の環境に依存するなどの理由で、被害組織毎に攻撃の手法やツールが異なる場合がある	基本的には ・初期侵害経路や侵害時に残るログ上の痕跡 ・IP アドレスやマルウェア等のハッシュ値 などのインディケータ情報と組み合わせて共有する

表 4

Q7.「インディケータ情報」とは何ですか？

情報共有活動でやりとりされる攻撃技術情報については「インディケータ情報」あるいは「IoC(Indicator of Compromise：侵害指標)」と呼ばれる情報があります。「Indicator」とは「指標」「尺度」といった意味の単語ですが、まさに攻撃者による侵害の痕跡を探すための指標となる情報、不正な通信先を示す「ＩＰアドレス」や「ドメイン名」、マルウェアの「ハッシュ値」、「通信の発生日時」などの情報が挙げられます。

「インディケータ情報」を共有活動を通じて入手した組織は、自組織の通信ログなどを調査し、同じ通信先へのアクセスが発生していないか、同じような不審なプログラムが存在していないかの調査を行います。

被害組織から専門組織に情報提供がなされる段階ではマルウェア検体や通信ログなどの一次情報が提供されますが、これを専門組織が解析し匿名化することで、インディケータ情報が作成されます。

こうした共有のための情報の加工を被害組織自身で行える組織もあれば、専門組織に依頼する組織もあります。

特に、後述の Q10（62 頁）や Q22（92 頁）のとおり、匿名で共有（展開）した攻撃技術情報と他の情報との突合から提供元（被害組織）が判明しないか、あるいは、共有（展開）しようとしている情報に第三者に関する情報が含まれているのではないかといった疑義がある場合、専門組織のチェックを受けることが効果的です。

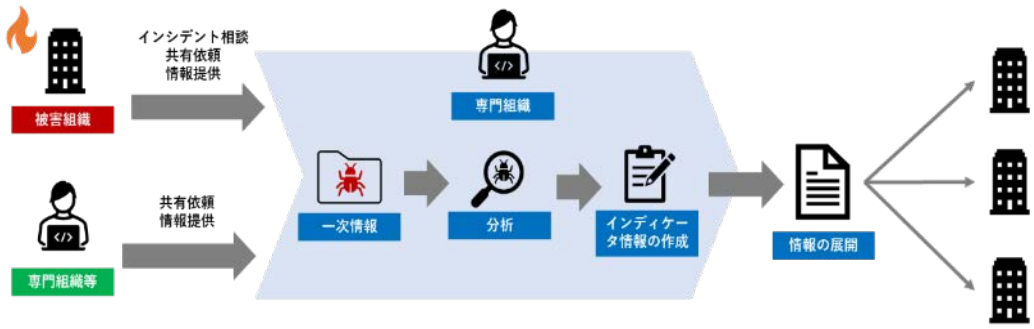


図 35

インディケータ情報の具体例

以下は、JPCERT/CC が被害組織などから得た情報を元に分析・作成し、情報共有活動参加組織に展開しているインディケータ情報の例です。情報共有活動毎にインディケータ情報のフォーマットや記載事項は異なりますが、一般的な形式として参考にしてください。

インディケータ情報の情報共有活動への展開までの流れ（例）

****

情報の共有範囲

本情報は、取扱注意情報（AMBER）です。本情報は、機密性の高い非公開情報を含むため情報の共有範囲が制限されます。共有範囲は自組織および関連組織内の必要最小限としてください。（Web サイトや公開のメーリングリストなどを使用して一般へ公開することを禁止します。）

****

JPCERT/CC で国内の組織に対して行われた標的型攻撃に関する情報を入手いたしましたので、参考までに情報をお伝えします。

以下の標的型攻撃に関する情報を参考のうえ、自システムなどの確認をお勧めします。

1）攻撃が行われた期間

202x 年 x 月以降

2）攻撃の特徴

標的型攻撃メールの本文に URL が記載されており、JPCERT/CC が確認時点で URL へ接続すると ZIP ファイルがダウンロードされました。ZIP ファイル内には、ショートカットファイル（.lnk）が格納されており、実行するとマルウェアに感染し、外部サイトへの接続に繋がります。

[メールの件名]

（※メールの件名を記載）

3）攻撃に使用された検体

JPCERT/CC が確認しているファイルや検体のハッシュ値は次のとおりです。

ファイル名：（※実際のファイル名）.zip

File Type ：

非公開で扱われる共有情報の取扱いに関する注意事項が示されています（参照：Q30（109 頁））

インディケータ情報を受信した組織が「いつの期間の通信ログ等を調べればいいのか」判断できるように攻撃が行われた期間を示しています（参照：Q 4（38 頁））

攻撃手法に関する簡単な説明があり、同じ攻撃を見つける／予防するために、どの箇所（システム、情報）を調査すればよいのか参考となる情報を示しています。

ここでは「メールの件名」が記載されていますが、件名には被害組織や第三者を特定するような文字列が含まれていないことを確認の上、記載しています。（参照：Q21（89 頁））

MD5　　：

SHA-1　　：

SHA-256　：

ファイル名：（※実際のファイル名）.lnk

File Type　：

MD5　　：

SHA-1　　：

SHA-256　：

4）攻撃に使用された通信先

[メールの文中に掲載される URL のドメイン]

[.]******[.]info　　443/TCP(HTTPS)

[lnk ファイルの通信先]

********[.]*******[.]org　　443/TCP(HTTPS)

※安全のため通信先の一部を、[.] に置き換えています。

この攻撃は、以下の JPCERT/CC Eyes ブログなどで紹介した攻撃活動と関連する攻撃として確認していますので、攻撃の詳細は以下の情報もご参考ください。

・JPCERT/CC Eyes

○○○に感染させるショートカットファイルを用いた攻撃

https://blogs.jpcert.or.jp/ja/202x/01/*******.html

（以下略）

攻撃に使われたマルウェア等のファイルのファイル名やハッシュ値を記載しています。
共有活動の参加組織が自組織で見つけた不審なファイルと攻撃に使用されるマルウェアが同じものかどうかを確認するための情報になります。
（参照：Q26（102 頁））

不正な通信先を調査するために必要な通信先（ドメインや IP アドレス）、使用するポート（プロトコル）を示しており、主にプロキシサーバや FW のログを調査するための情報となります。
（参照：Q6（47 頁））

この攻撃キャンペーンの全体像や攻撃手法の技術的詳細、攻撃活動の傾向などの情報を示した公開情報が既にある場合は参考情報として掲載されます。
また、どの攻撃グループの活動なのか、過去の攻撃との関連性の有無などを示す場合もあります。

この攻撃を見つける調査方法や、攻撃への対策方法、不審な通信等を見つけた場合のインシデント対応の相談先などについて記載が続きます。

図 36

インディケータ情報として必要な情報とは

以下の 2 つの情報を見比べてみてください。

情報A

1 月に○国の IP アドレスから不正アクセスを受けていたことが発覚し、調査したところ、×××マルウェアの感染が見つかっている。

情報B

1 月×日に IP アドレス：203.0.113[.]***から不正アクセスを受けたことが発覚し、調査したところ、以下の×××マルウェアが見つかっている。 ファイル名：**** .exe ハッシュ値（MD5）：～

情報Aは、確かに攻撃の概要を示してはいますが、この情報から「同じ攻撃が自組織にも行われたのか確認」することはできません。情報Bには、「日時」、「ＩＰアドレス」、「ファイル名」、「マルウェアのハッシュ値」が記載されていますので、通信ログ上で同様のアクセスがないか調べることができ、また、不審ファイルが見つかった場合に、ファイル名やハッシュ値で同様のものか照合することができます。活用可能なインディケータ情報としては、「各組織のシステム上で照合するために必要な情報」が求められると言えます。

一方で、各組織でどのような機材、データを使って照合できるかには差があります。例えばプロキシサーバを運用している組織では「どのドメイン向けのアクセスが発生したか」を調べられますが、ファイアウォールのみ運用している組織では IP アドレスのみが記録され、ドメイン（FQDN）まで記録されません。

図 37 のケースのように、同じ IP アドレスでも時期によって正規サイトに紐づいていることもあれば、ある期間のみ不正ドメインに紐づいているケースがあります。この場合、不正なドメイン名（FQDN）情報だけでは照合できない組織が出てくる可能性があります。また、IP アドレス情報がセットになっていたとしても、「日時」に関する情報がなければ、正規のアクセスだったのか、不正なアクセスだったのかを判別することができません。

したがって、インディケータ情報としては、「不正なアクセス、ファイルを一意に特定できる情報」も必要であると言えます。

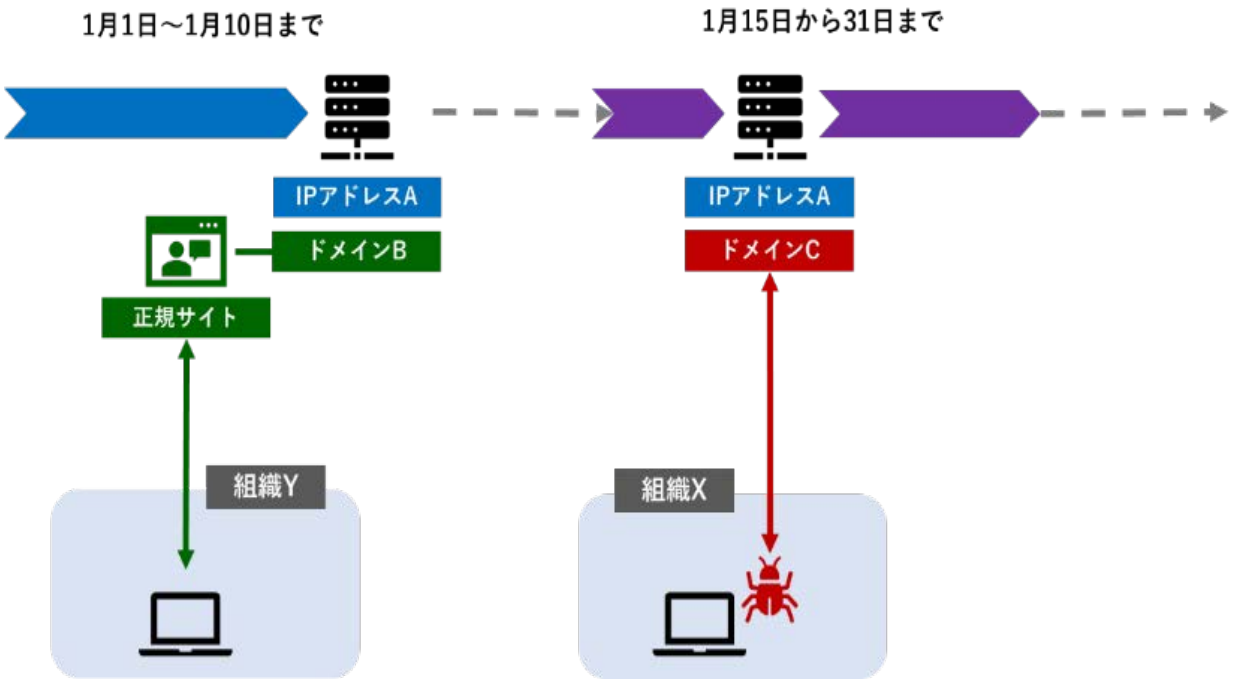


図 37

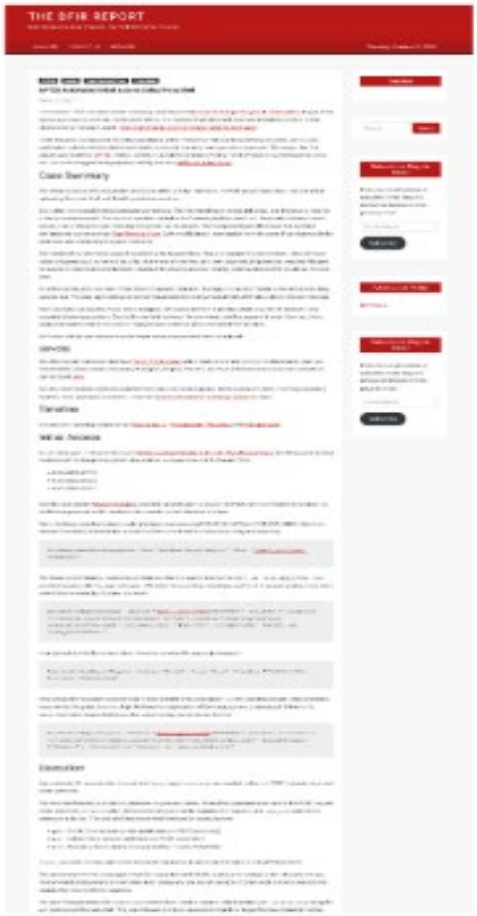
TTP について

「インディケータ情報」、「IoC」と似た用語として「TTP（Tactics, Techniques, and Procedures：戦術、技術、手順)」という用語があります。これは、攻撃者がどのような方法で侵入し、どのような方法でマルウェアを実行し、どのようにして不正に権限を得て、何を行ったのか、攻撃者の「行動」や用いた「攻撃テクニック」を示すものです。

インディケータ情報があくまで侵害されている事実を探すための情報だとすると、TTP はその攻撃の全体像を明かした情報と言えます。相当の調査期間を経なければ、TTP 情報を得ることができないため、情報共有効果が望まれる早期の時点で共有することは難しい一方で、標的型サイバー攻撃や、侵入型ランサムウェア攻撃など、特定の攻撃グループが一定期間内においては同じような戦術を取る場合、TTP 情報を「次の攻撃に備えて」広く共有することは相当程度の予防効果があります。

以下は標的型攻撃キャンペーン被害を調査した結果判明した TTP 情報を示す 2 つのレポートの一部を抜粋したものです。左は文章で攻撃の流れや使われた攻撃テクニックを解説していますが、実際はこの数倍の分量になっており、右は TTP を標準的に表記するためのフレームワーク、MITRE ATT&CK に基づいて記載したものであり、各攻撃フェーズで使用された攻撃テクニックが整理されていますが、実際にどのように被害組織でそれらの攻撃テクニックが用いられたのか詳細はわかりません。包括的な TTP 情報を情報共有活動で伝えることは難しいため、TTP 情報は専門組織が公表する分析レポートを通じて情報発信されることがほとんどです。

TTP を示した情報の例



DreamJob

Reconnaissance	Resource Development	Initial Access	Execution	Persistance	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration
Search Open Websites/Domains (T1593)	Compromise Infrastructure (T1584)	Phishing (T1566)	Command and Scripting Interpreter (T1059)	Create or Modify System Process (T1543)		Obfuscated Files or Information (T1027)	OS Credential Dumping (T1003)	System Network Configuration Discovery (T1016)	Remote Services (T1021)	Archive Collected Data (T1560)	Application Layer Protocol (T1071)	Exfiltration Over C2 Channel (T1041)
	Compromise Accounts (T1586)		User Execution (T1204)	Boot or Logon Autostart Execution (T1547)		Masquerading (T1036)	Network Sniffing (T1040)	Remote System Discovery (T1018)	Lateral Tool Transfer (T1570)		Proxy (T1090)	
	Develop Capabilities (T1587)		System Services (T1569)			Template Injection (T1221)	Unsecured Credentials (T1552)	Network Sniffing (T1040)			Data Encoding (T1132)	
							Credentials from Password Stores (T1555)	Account Discovery (T1087)			Remote Access Software (T1219)	
								Network Share Discovery (T1135)			Encrypted Channel (T1573)	

図 38

右：THE DFIR REPORT: APT35 Automates Initial Access Using ProxyShell,

https://thedfirreport.com/2022/03/21/apt35-automates-initial-access-using-proxyshell/

左：JPCERT/CC, MITRE ATT&CK® Mapping for Lazarus Group,

https://github.com/JPCERTCC/Lazarus-research/blob/main/TTP/MITRE_ATT%26CK_Mapping.md#commonly-used-ttp

Q8.いつ情報を共有すればいいのですか？

専門組織との情報共有の目的は Q1（33 頁）で示したとおり、インシデント対応に必要な情報を得ることと、被害の未然防止のための 2 つの目的がありますが、いずれの目的であっても、下記図 39 のとおり、攻撃活動が行われているうちに速やかに行う必要があります。

攻撃活動が終わってから共有を行っても被害の未然防止は行えないことは当然ですが、インシデント対応のための情報共有であっても、攻撃の詳細が判明しないままでは原因調査や被害調査に不必要に時間がかかったり、あるいは原因等が特定できないままになったりするおそれがあります。

マルウェアや不正通信先、悪用されている脆弱性に関する情報などの攻撃技術情報が見つかり次第、可能な限り速やかに共有することが望ましいですが、Q10（62 頁）のとおり、調査があまり進んでおらず、あまりに情報が断片的な場合は、不正確な情報を流してしまうおそれや、情報を共有しても期待したフィードバックを得ることができない場合があります。

専門組織のサポートも受けながら、各組織のシステム上で照合するために必要な情報等、基本的には、インディケータ情報として使えるだけの情報（Q6（47 頁）を参照）が集まった段階で共有することが望ましいと言えます。

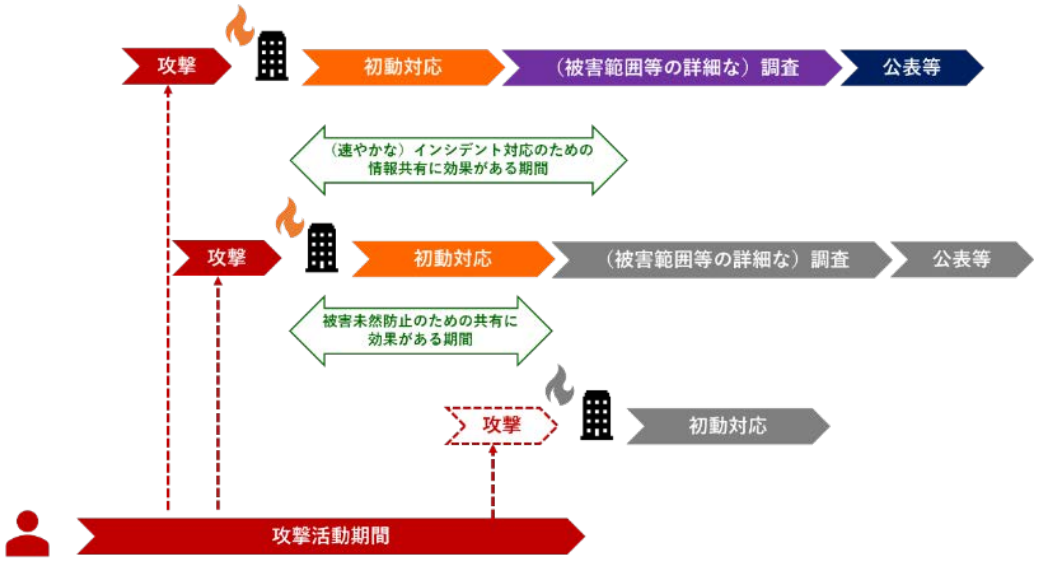


図 39

情報共有タイミングを逃すとどうなるのか？

共有情報にも“鮮度”があり、前述のとおり、攻撃活動期間中のなるべく早い時期に共有がなされることで、情報共有によるメリットを参加者が享受することができます。ただ、これは理想的なタイミングですので、実際には既に攻撃活動が終わってしまったあとに発覚するケースが散見されます。ただ、既に攻撃活動が終わっていたとしても、攻撃に気づいていない組織が早期に被害認知するための共有は必要ですし、攻撃の詳細を全容解明し、適切な原因調査、再発防止策を検討するためには、不足している情報を情報共有によって入手することが必要です（参照：Q1（33 頁））。

しかしながら、余りにも遅いタイミングでの情報共有は逆に参加組織に不必要な手間を発生させる可能性があります。下記の図 40 は異なるタイミングにおける情報共有を図示したものですが、下段の「遅すぎる共有」では、情報を受け取った組織ではもはや当時のログ等が保存されておらず、当該攻撃の有無を調査することすらできません。あるいは、過去に既に対応を終えている組織にとっては、既に対応済みの案件を“掘り返す”ことになるわけで、不必要な対応コストが発生することになります。

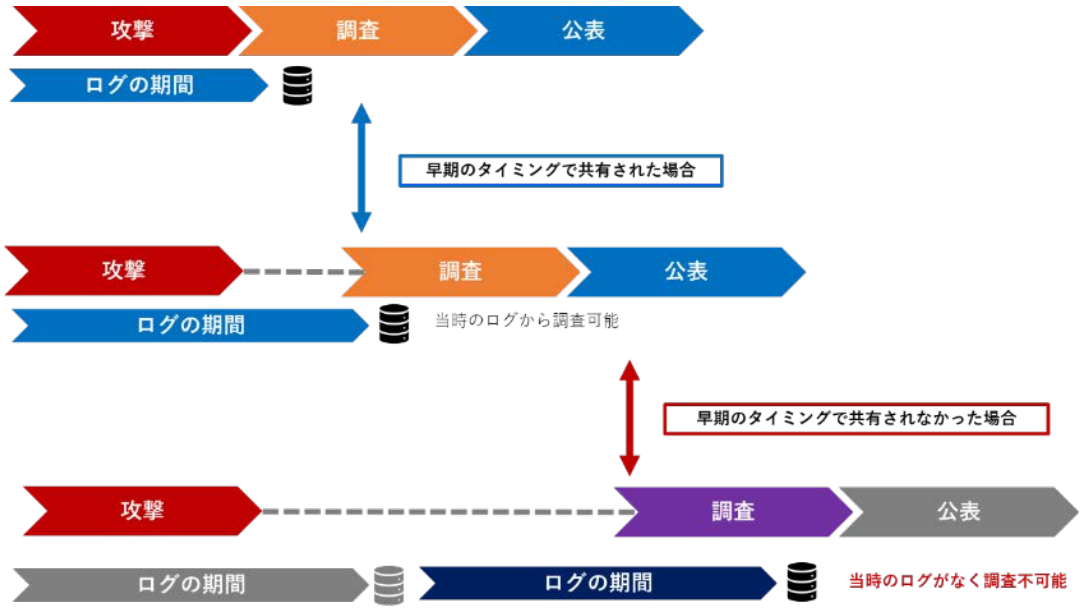


図 40

とはいえ、過去に対応した事案について、ノウハウ共有の目的で他組織と共有したり、公表したりすること自体にも意義はありますので、情報共有目的の活動なのか、ノウハウ共有目的の活動なのか、整理することも重要です（参照：Q2（36 頁））。

Q9.情報共有活動に参加していない場合、どこに共有すればいいのですか？

Q3（37 頁）で情報共有活動の類型を簡単に紹介しましたが、情報共有活動に参加していない場合、どこに共有すればよいのかわからない、という問題があります。

基本的には、

① 情報共有の窓口組織に共有する

② 専門組織に依頼して情報共有活動に提供してもらう

の 2 つのパターンが想定されます。

前者は例えばサイバーセキュリティ協議会であれば、協議会に参加していない組織であってもインシデント対応相談や情報共有活動への情報提供（とフィードバック情報の受領）ができる窓口が公開されています。

後者は、インシデント対応を依頼しているセキュリティベンダや運用保守ベンダ、専門機関に依頼して、それらの専門組織が参加／運営している情報共有活動に代理で情報提供し、フィードバック情報を受け取るものです。

いずれも、基本的には情報共有活動に対して「匿名」で情報提供し、フィードバック情報を受け取ることになりますが、自組織名を示したうえでの情報共有も可能です。

どの相談窓口に相談すればいいのか

日頃から情報共有活動に参加していなかったり、インシデント対応経験がなかったりする組織においては、いざインシデントが発生したときに、「一体どこに相談すればいいのか」「どこに情報を共有すればいいのか」わからないという問題があります。

まず、インシデント対応の観点として、「専門機関の相談窓口等への相談により、おおむね解決できる」ケースと、「セキュリティベンダ等に調査を依頼・契約しなければ解決できないケース」にわかれます。専門機関の窓口に相談した場合、情報共有の必要性があるかどうかも含めて、情報共有に関する相談が可能です。後者のケースであっても、専門企業から専門機関への相談・情報共有活動から追加の情報の入手をアドバイスされる場合があります。あるいは被害組織の判断として、セカンドオピニオン的に専門機関への相談を並行して行う場合もあります。

では、実際に相談・共有のための情報提供を行うと判断した後、どの専門機関の窓口に相談あるいは共有を行えばいいのでしょうか。基本的な考え方としては、“距離”が近い組織を選ぶ、という観点になります。例えば、サイバーセキュリティ協議会の構成員であれば、協議会の相談窓口が想定されます[8]。

各専門企業や専門機関では、それぞれ得意な分野や、行うことができる業務に違いがあります。例えば、不正サイトのテイクダウン（無害化）などで海外の事業者に対する依頼・調整が必要となった場合、基本的には JPCERT/CC へ依頼がなされます。あるいは、特定の攻撃手法について集中的に追跡や対応を行っているかどうかも差異があります。

まずは、自組織が受けたと思われる攻撃手法に関する注意喚起やレポート／ブログ記事を掲載している専門機関に相談することが望ましいです。あるいは、普段から業界団体、地域のコミュニティ活動、都道府県警察などからの案内などに専門機関による特設サイト、レポートの紹介や、相談窓口の案内が掲載されている場合がありますので、そうした「目にしたことがある」相談先にコンタクトすることもわかりやすい方法です。

基本的に、相談先の専門組織が専門組織間の共有活動を行っているのであれば（Q12（65頁）参照）、複数の専門組織に重複して情報提供することは、インシデント対応の初動フェーズにおけるリソースにも影響しますので、必須ではありません。ただし、すべての専門組織が専門組織間の情報共有活動に参加しているわけではないので、情報共有活動を通じた情報の入手が可能かどうかも含めて、相談することが必要になります。先に触れたように、調査を依頼した組織から、セカンドオピニオン的な専門機関への相談や情報共有活動から

[8] 事案発生の疑いが生じた場合等の、サイバーセキュリティ協議会の連絡先については、下記協議会ページをご参照下さい。
https://www.nisc.go.jp/council/cs/kyogikai/index.html

の情報の入手をアドバイスされることもあります。

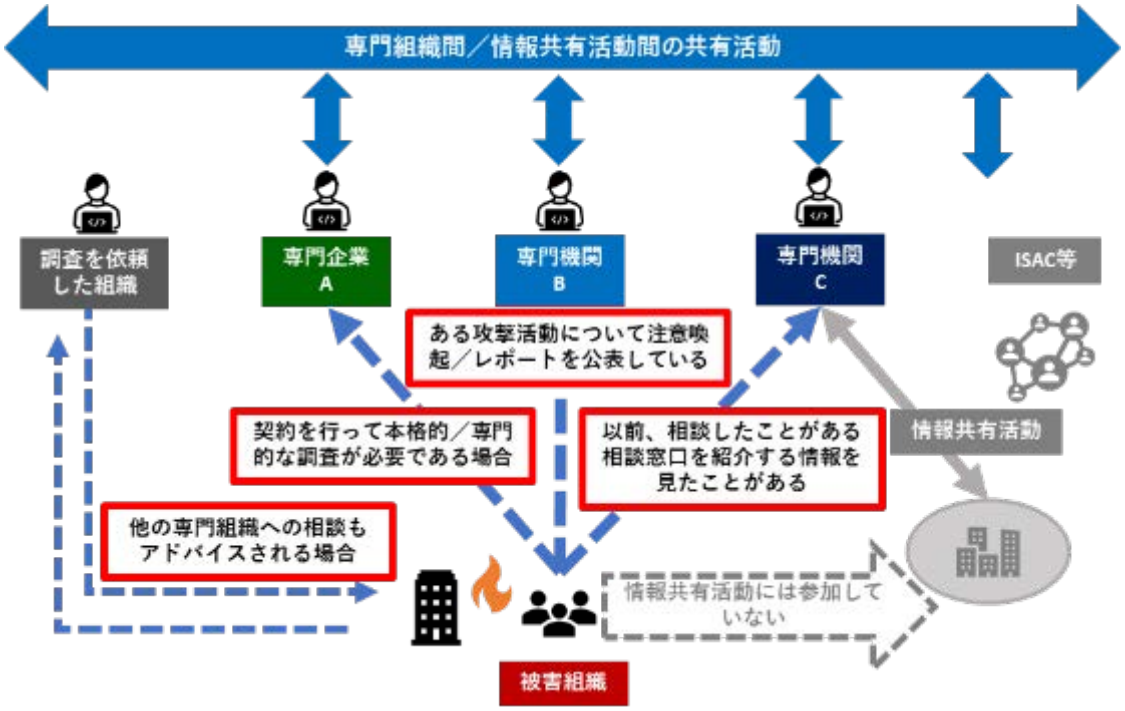


図 41

Q10.情報共有を行う上での留意点はありますか？

以下の点を留意する必要があります。

① 情報共有を行うための対応コストが発生すること
② フィードバックが得られない場合があること
③ 事後に公表した場合、共有活動の参加組織が情報を突合できてしまう可能性があること

まず、インシデント対応とは別に、特に調査を依頼している組織とは別の組織／共有活動の窓口を通じて情報共有を行う場合、情報の提供や提供のための情報の加工等の作業が発生します。また、専門組織／共有活動の窓口組織とのやりとりも発生しますので、こうした対応コストが発生します。

また、情報共有を行ったとして、これ以上の情報を専門組織や情報共有活動に参加する他の組織が有していないケースもあり、その場合、情報の提供をしたのに、何の情報もフィードバックとして得られない、ということになります。「フィードバックがない」こと自体もフィードバックであると解釈することもできますが、あらかじめそういうケースがあることを理解しておく必要があります。

そして、稀なケースではありますが、匿名での情報提供であっても、事後に被害公表をした場合に、公表内容に示された攻撃技術情報の特徴などから、情報共有活動の参加組織が「この公表事例はあの時共有活動に流れた情報のことだったのか」と突合できてしまう場合があります。攻撃が当該被害組織のみでしか確認されていなかったり、攻撃技術情報として提供した情報、例えば被害を受けたシステムに関する情報が、当該被害組織固有のものであったりすると、そうした突合が容易になってしまうおそれがあります。

「フィードバックがない」ことについて

情報共有活動に情報を提供したとしても、必ずフィードバックとして新たな情報が得られるとは限りません。例えば、当該攻撃を受けた／観測した組織が自組織のみだった場合や、他にも攻撃を受けた組織がいるが当該情報共有活動の参加組織ではない場合などです。また、共有するタイミングにとって、フィードバックが得られないこともありますので、「いつ共有すればよいのか」という点については、Q8（57 頁）をご参照ください。

「フィードバック」を得やすい情報共有について

Q6（47 頁）で示しているとおり、そもそも共有することによる効果（被害未然防止／被害拡大防止／被害の早期認知）が得られやすい攻撃に関する情報を共有する、という前提条件がありますが、そのほかにも、同じく、Q6（47 頁）後段で示したように、情報の受け取り手側組織が「調査しやすい」情報を揃えることも必要です。また、Q8（57 頁）などで繰り返し触れているとおり、なるべく攻撃キャンペーン中の早期の段階で共有を行うことで、同じく Q8（57 頁）後段で示すような「過去の事案の“掘り返し”」のような、受け取り手側組織のモチベーションが期待できないような情報共有を避けることができます。

こうした「共有効果を得る」ための条件というのは、情報の受け取り手側の「対応コスト」に配慮することの重要性も示していると言えます。この「対応コスト」を減らす観点では、受け取り手側の「優先度」判断に資する情報を追加することも効果的であり、共有活動参加組織のモチベーション維持に必要です。

組織によっては、目的や共有情報の種類／情報の展開頻度の異なる複数の情報共有活動に参加している場合があり、リソースの都合上、どうしても手間のかかるログ調査等を後回しにせざるを得ない場合が想定され、対応の「優先度」を判断しなければなりません。

例えば情報の展開側は攻撃の深刻度や当該時点で把握している被害範囲、または直近の被害拡大の蓋然性などを示すことが考えられます。「すでに国内で複数の被害を観測している」「被害を受けた場合、サービス停止に至る」といった具体的な記述をすることで、受け取り手側の組織内における作業の優先度を判断しやすくする効果が見込めます。

Q11.攻撃技術情報の共有とノウハウの共有とは何が違いますか？

基本的に本ガイダンスが主眼とする「攻撃技術情報を早期に共有することで、情報共有の効果を得ること」と、「被害組織がインシデント対応から得た対応ノウハウを他の組織を共有すること」は異なるものです。

下記の図 42 はインシデント対応の時系列に沿って、①被害組織が調査によって得る情報の量、と②攻撃に関する情報の“鮮度”、の 2 つの変化を示したものです。インシデント対応初期の段階では、調査が限定的であるため、攻撃の全容に関して得ることができた情報量は少ない状態です。他方で、Q8（57 頁）で示したとおり、攻撃技術情報は可能な限り早期に共有しなければ、共有効果を得ることができません。

他方で、ノウハウを共有するためには、攻撃や被害の全容が判明し、再発防止策などの検討が行われていなければなりません。攻撃技術情報における「早さ」に対して、ノウハウの共有においては「調査のための時間の経過」が必要になります。

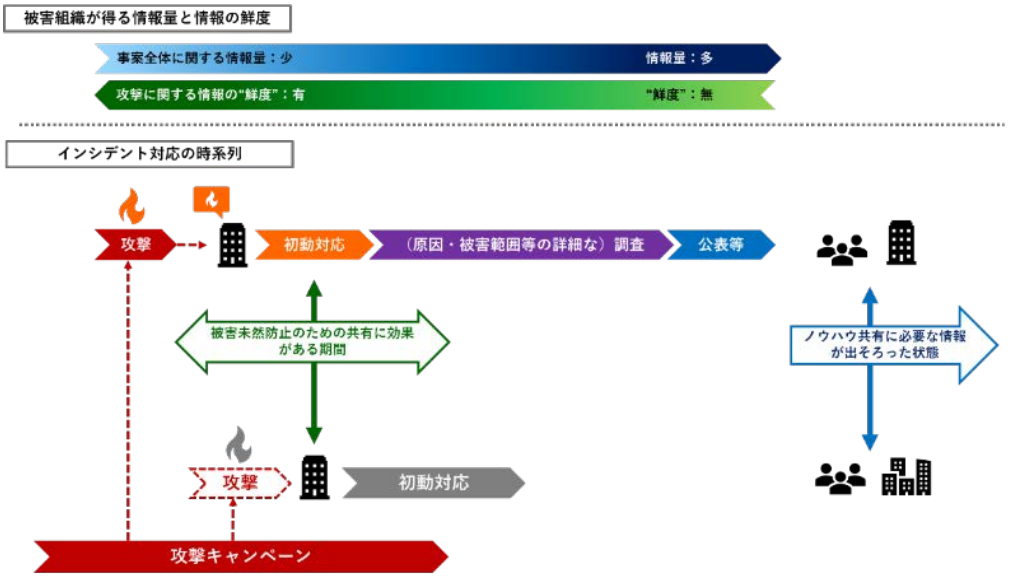


図 42

Q12.専門組織同士はどういう情報を共有していますか？

Q1（33 頁）で述べたとおり、攻撃の高度化により、単独組織だけで攻撃の全容を把握し、最適な対策を行うことは難しくなっています。これは専門組織でも同じで、専門組織コミュニティ内での情報共有が行われています。

例えば、サイバーセキュリティ協議会の第一類構成員は現在、主に専門組織で構成されていますが、自組織単独ではまだ確証を得るに至っていない分析内容を持ち寄り、共同での分析や情報展開等の必要な対応を検討しています。この時に共有される情報は主に攻撃技術情報であり、攻撃の深刻度や、協議会内外での情報展開の判断、展開先の選定を検討するために、攻撃主体や攻撃対象システムに関する情報、攻撃のタイムラインに関する情報などを被害組織が特定されないように共有しています。

例えば、ある攻撃で標的となっているシステムが広く使われており、攻撃手法やタイムライン、攻撃主体のこれまでの傾向等から、今後攻撃が広範囲に行われる蓋然性が高いと分析された場合、協議会内での限定的な情報共有ではなく、専門機関からの注意喚起やセキュリティベンダからのレポート発信などが選択されます。

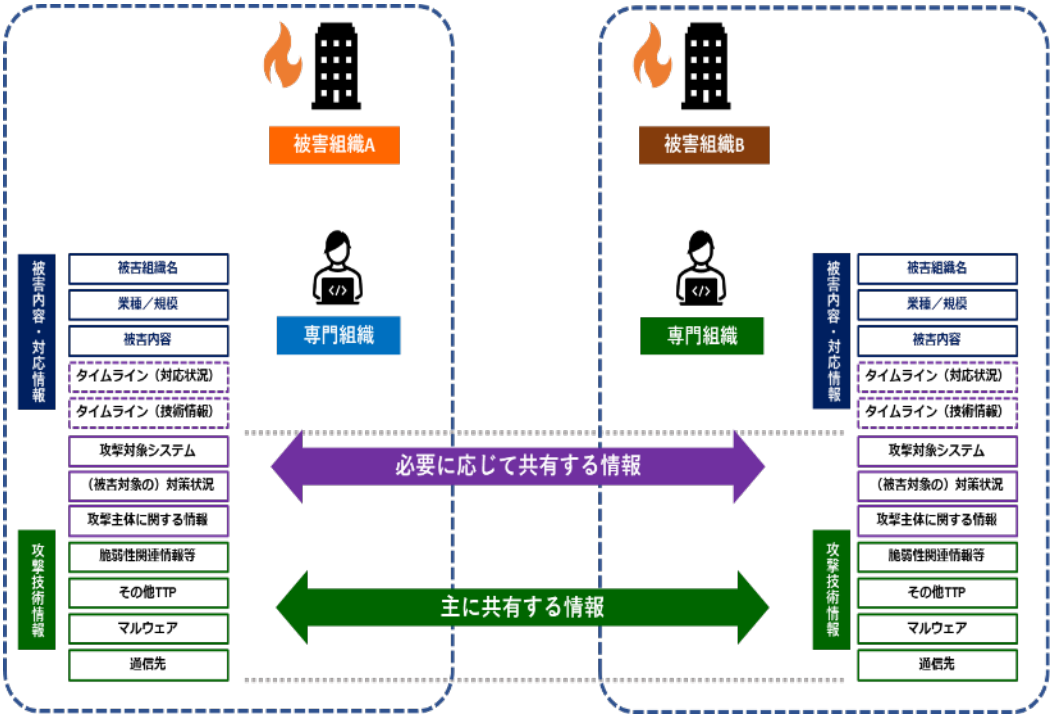


図 43

なぜ専門組織同士の連携が必要なのか

本ガイダンスで度々触れているとおり、攻撃手法が日々変化する中で、単独組織だけで攻撃に対処することは困難です。例えば、改ざんした Web サイト経由でマルウェアに感染させるような、未知の脆弱性を使ったゼロデイ攻撃が発生した場合、被害を認知した個別の組織への対応だけでなく、改ざんサイトの管理組織への対応、まだ感染に気づいていない被害組織への個別通知・支援、脆弱性の修正・公表に向けた製品開発者との調整や注意喚起、その他攻撃インフラのテイクダウン（無害化）、と多数の利害関係者間の調整・通知・対応を同時並行で行わなければなりません。また、すべての被害現場を単独の専門組織でカバーしているわけではありませんので、こうした複雑な攻撃においては、複数の専門組織間での連携オペレーションが必要になります。

さらに複数の組織が同じことを重複して実施しても効果はありませんし、逆に異なる対応をバラバラに行っても効果はありません。1 つの調整先に複数の組織がバラバラに連絡をしたり、逆に、異なる内容の情報発信をタイミングもバラバラに公開したりすれば、被害組織や被害をまだ認知できていない組織に混乱を与えてしまいます。

他方で、専門組織の大半は製品／サービスを提供している専門企業であり、また、各組織がミッションとして担っていることも様々です。お互いに足りない点を補い合いながら、各組織が得意とすることを分担し、それらが組み合わさることで、社会全体でのサイバー攻撃対処が行われています。

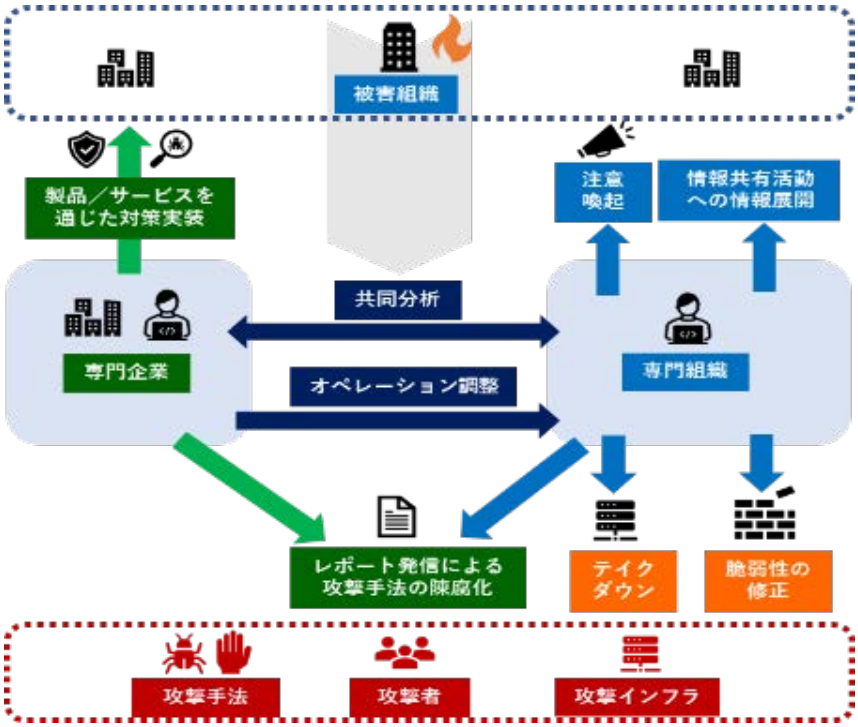


図 44

Q13.なぜ非公開で参加者が限定された情報共有が行われるのですか？

攻撃に関する情報を共有するにあたって、留意点として、以下が挙げられます。

・（可能な限り）攻撃者に知られずに情報を共有しなければならないこと

・情報提供元組織や標的となっている蓋然性が高いと思われる組織が保護されなければならないこと（Q21（89 頁）、Q22（92 頁）参照）

・（上記 2 つの目的のため）意図しない情報漏えいがないよう、ある程度情報が保護された状態でやりとりされなければならないこと

そのため、共有活動は、基本的に非公開で限定された組織間において行われます。

また、Q6（47 頁）で紹介したとおり、ある程度同じ攻撃を受けるおそれのある組織間で情報共有の効果が見込まれるため、分野毎／目的毎に共有活動が編成されます。

図 45

他方で、分野をまたぐ攻撃も発生するため、サイバーセキュリティ協議会のように分野横断的な情報共有活動や参加組織の拡大が想定されますが、無差別／複数の分野に対して行われるような広範囲な攻撃であれば、余りに広範囲に拡大した情報共有活動では被害防止のための情報伝達がタイミング的に間に合わない／範囲としてカバーしきれないことが想定されるため、一般的には専門機関等からの公開での注意喚起が行われます。

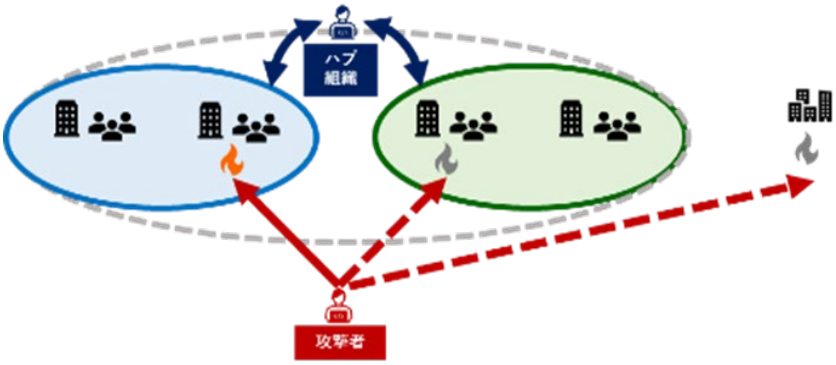


図 46

情報の共有と展開先制限のジレンマ

攻撃者は特定の目的を持った攻撃を行うため、一定期間の攻撃活動内においては、特定の情報を有する分野／システムが標的となります。したがって、理屈上はこうした特定の対象となりうる組織が集まって情報共有を行えば、情報共有による利益を最大限受けることができます。

しかし、実際には下記の図 47 右側のとおり、同じシステムを持つ異なる分野の組織に対して攻撃が行われることもありますので、分野横断的な情報共有も必要になるわけです。

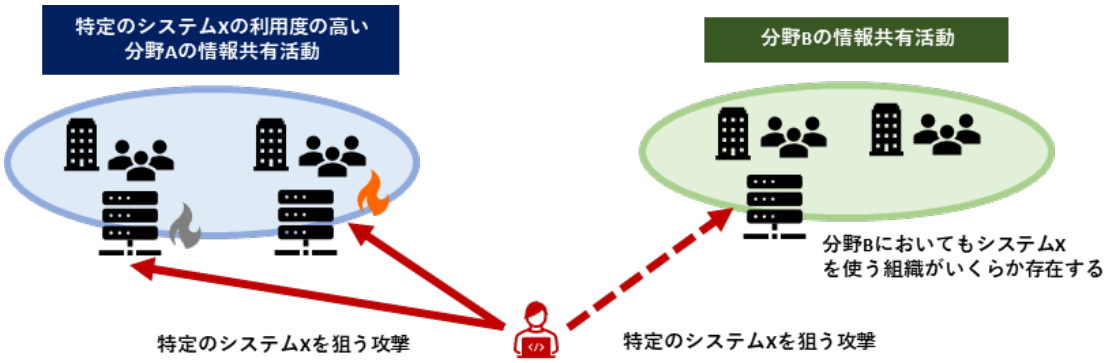


図 47

しかし、この理屈を突き詰めていくと、分野横断の仕組みは果てしなく拡大していくことになるわけですが、一方で、現存の情報共有活動は特定分野単独に行われていたり、分野横断活動の中で分野毎のグループに細分化されていたりするケースがほとんどです。これには情報共有活動が抱える 2 つの課題が背景にあります。

①情報を安全に扱えるかどうか

Q21（89 頁）や Q 22（92 頁）で紹介するように、攻撃に関する情報には、例え攻撃技術情報のみであったとしても、広く公開されることで悪用等の二次被害を生む可能性のある情報があります。したがって、情報共有活動は基本的に非公開の活動として行われており、また、共有範囲指定（Q 30（109 頁）参照）などの情報（や情報提供元）を保護する措置が取られています。

こうした活動における取り決めなどは任意のルールに基づくものが大半ですので、仮に共有ルールに違反したとしても罰則等があるわけではありません。あるいは、意図せず、情報の取扱いの不注意により制限範囲外に情報が漏えいしてしまうこともあるかもしれません。

したがって、情報共有活動は、一定程度の信頼関係のある組織が集まったり、情報が保護されやすい伝達手段を用いたり、そもそも共有範囲（参加組織数）を制限する、という方法で情報漏えいのリスクを可能な限り低減しています。

③ 共有活動の“満足度”をどう維持するか

情報共有活動には対応するコストが発生します。①で述べたとおり、情報の保護のため専用のポータルサイトや厳密な伝達手段の指定などがあるため、情報の受領自体にも作業コストが発生します。そして、インディケータ情報のように、通信ログ等との照合作業といった作業コストも発生します。情報共有活動に参加することは無償であることが多くても、実際には対応コストを負担しているわけです。

そうした場合、対応コストに見合った受益があるのか、という点が情報共有活動に参加するモチベーション、“満足度”として活動に影響するようになります。例えば、特定の分野を狙う攻撃に関する情報を当該特定分野に限定した情報共有活動で受領していれば、受領したインディケータ情報との照合により「実際に攻撃試行が見つかる」ことが多く発生します。他方で、下記の図 48 のとおり、様々な分野の組織が混在した情報共有活動の場合、どのような類型の攻撃の被害に係る情報が共有されるかによりますが、全体としては「全然攻撃試行が見つからない」インディケータ情報の割合が相対的に増えてしまいます。

もちろん、攻撃（試行）がないことが一番ですが、先に触れたとおり、情報共有活動においては、攻撃がなくても、インディケータ情報が流れる分だけ「対応コスト」が発生しますので、「実際にインディケータ情報により攻撃を未然に防げた／早期に発見できた」という情報共有のメリットを感じることなく、対応コストだけが加算されることになってしまいます。

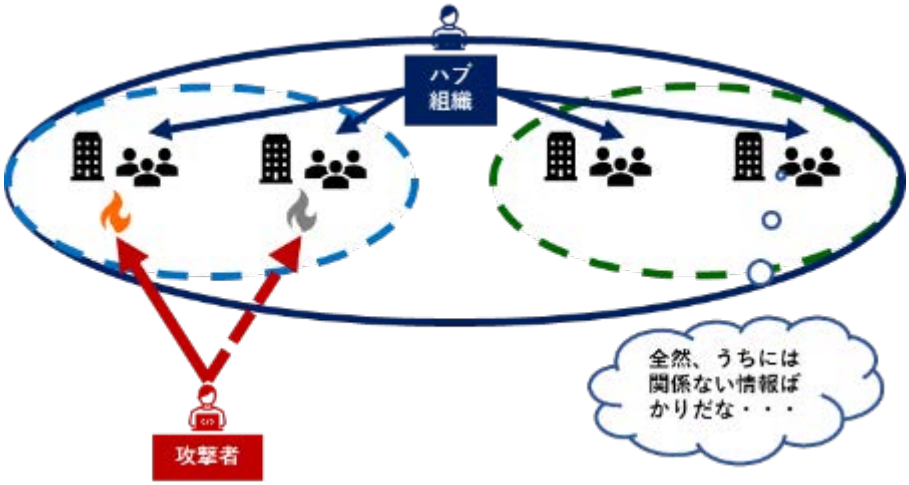


図 48

情報は共有すればするほど価値を高めることができますが、同時に情報の保護のため共有範囲に制限をかけなければならないというジレンマがあります。また、情報共有活動参加組織の“満足度”という課題もあるので、少なくとも活動参加組織のニーズを拾いやすい分野に閉じた情報共有活動間や、ハブ組織間の連携が解決策として想定されます。

＜被害の公表や法令等に基づく報告・届出について＞

Q14.公表の目的は何ですか？

被害公表の種類は、以下のものがあります。

① 法令上の義務や適時開示、ガイドライン等で推奨される対象の事案であるために公表するもの

② 法令等で求められていないが、自主的に公表するもの

後者の、自主的な公表の目的は、例えば以下のように分類できますが、相互排他的なものではなく、実際のケースでは、被害組織において、複数の要素を総合的に判断することになります。

i）二次被害防止など攻撃についての注意喚起

ii）サービスの停止や報道などで被害が既知のものとなった際の、対外的説明

iii）広報／リーガルリスク対応

iv）その他

i）については、後述の理由で、専門組織による注意喚起やレポート発信により攻撃技術情報が広まる方が望ましいケースもあると考えられますので、Q31（111 頁）もご参照ください。

ii）については、SNS 上で被害について事実とは異なる情報が拡散している場合において、正確な情報を発信するために被害公表を行うケースも想定されます。なお、被害が既知のものとなっていない場合でも、説明責任を果たす観点から、積極的に情報を開示することにより、インシデント対応における評価を得る効果があるほか、広く脅威に関する情報を社会全体と共有する意義や社会的効果が見いだされます。

iii）は、そのまま公表しないという判断も可能な場合において、どのような経緯で当該被害が不特定多数に伝わるか不透明であることを踏まえて、先んじて公表を行うケースです。被害に関するプレスリリースを出して問い合わせ先を 1 つの窓口に誘導することで対外応答を整理することができますし、本来、被害について伝えるべきだった者への伝達が漏れていた場合、公表していないことで発生し得るリーガルリスク回避のためにも有効です。

本ガイダンスの「はじめに」で述べたとおり、被害組織から自主的に公表される情報が広く伝わることで、サイバー攻撃の脅威に対する社会的な認知が向上し、社会全体での対策が進む可能性や同様の被害公表を行う被害組織のインシデント対応への理解が向上する可能性につながります。

Q15.公表のタイミングはどのようなものがありますか？

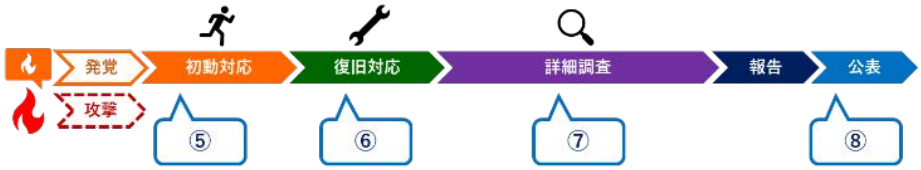
公表のタイミングとしては、主に以下のパターンが想定されます

一般的な不正アクセス事案の場合

①・②事案の発覚時点または初動対応時点で深刻な被害が判明した時点
③詳細な被害調査を進める中で深刻な被害が発覚した時点
④調査を終えた時点

図 49

リアルタイムインシデントの場合



⑤攻撃発生とほぼ同時に攻撃被害が広く知られてしまう／その可能性のある時点
例：犯行声明を伴う DDoS 攻撃による対外サービス停止、侵入型ランサムウェア攻撃におけるリークサイト掲載（いわゆる“二重の脅迫”型の場合）
⑥侵害を受けた／障害が発生していたシステムの復旧タイミング
⑦詳細な被害調査を進める中で深刻な被害が新たに発覚した時点
⑧調査を終えた時点

図 50

上記は代表的なケース想定であり、これ以外にも自主的な判断で公表を行うタイミングがあります。詳しくは Q 14（70 頁）、Q16（72 頁）、Q17（76 頁）をご参照ください。

Q16.公表の内容としてはどのようなものがありますか？

被害公表時に対外的に示す内容としては主に以下の項目を挙げることができます。

・サイバー攻撃の種類／概要
・侵害されたシステム、範囲（現時点で判明しているもの）
・侵害原因（判明している場合）
・サイバー攻撃の発生日時や侵害期間（判明している場合）
・影響内容（業務影響、情報漏えい、サービス停止、その他）、影響範囲（現時点で判明しているもの）
・（即応的な第一報の場合）初動対応内容
・専門組織への相談有無（※公的機関の場合は当該組織名）、（該当する場合）所管省庁等への報告状況
・影響を受ける者・組織や二次被害に関する相談先
----------<以下は調査終了後の公表段階＞----------
・侵害原因、攻撃の経緯
・影響範囲
・対応の経緯
・再発防止策
・公表内容に関する問い合わせ先

上段のものはある程度初動段階で判明する内容もあるため、即応的に第一報を公表する場合（Q15（71 頁）参照）の目安となります。
加えて、調査が進み最終的な公表段階において、下段の内容が加わります。

※「５．チェックリスト／フローシート」の「情報共有と被害公表における情報の種類のチェックリスト」も参照して下さい。

情報の速報性と正確性

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」事業報告書冒頭で示されているとおり、被害公表のスピードが社会的に求められる傾向にあるところ、他方で、サイバー攻撃被害の調査には相当の時間が必要であることから、情報の速報性と正確性との間でジレンマが発生します。

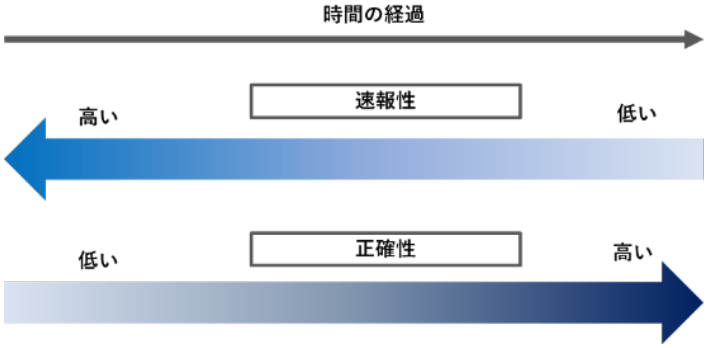


図 51

Q8（57 頁）の解説のとおり、攻撃技術情報については共有に適した“鮮度のある”期間があるため、十分に情報が集まっていない段階でも可能な限り速やかな外部への提供が求められ、多少情報が断片的であっても、専門組織が持っている情報や情報共有活動を通じて情報が補強される可能性が見込めます。

一方で、被害の公表で専ら扱うことになる被害内容・対応情報は攻撃技術情報のように情報共有活動を通じて補うこともできず、自ら調べるしかありません。また、下記のとおり、断片的では情報として意味をなさない場合もあることから、一定程度の調査期間を経た上での情報の正確性が求められることになります。

こうしたジレンマへの対応としては、Q15（71 頁）等のとおり、初報、第２報・・・のように、適切なタイミングに分けて、段階的に情報を開示していくという方法も有効です。

	調査が未完了の場合	調査を終えた場合
攻撃技術情報 例：不正通信先	不審通信先は 198.51.100.*** ←情報として有効	不審通信先は 198.51.100.*** 203.0.113.*** ←情報として有効
被害内容・対応情報 例：被害範囲（侵害された範囲）	端末 1 台がマルウェアに感染していたことが判明	端末５台がマルウェアに感染した後、○○情報を管理するサーバなど３台へ侵入し、情報を持ち出していたことが判明 ←取引先等への影響や二次被害有無など攻撃によるインパクトが大きく変わる

表 5

公表内容にどこまで攻撃技術情報や対応経緯などの詳細を書くべきか

被害公表にあたっては、攻撃類型や被害状況によってケースバイケースでありますが、本 Q16（72 頁）で既述のとおり、基本的に被害内容・対応情報が主たる記載内容になります。しかしながら、一定程度は攻撃技術情報を記すことが求められ、また、対応経緯などの詳細を知ることは、中長期的な視点で見た場合、下記のとおり有益な取り組みになります。

Q12（65 頁）のとおり、情報共有活動にはカバー範囲の限界があるところ、新たな攻撃の動向や対応に必要な情報を得る方法として、「他の被害組織が公表した情報」の入手を挙げることができます。図 52 のとおり、そもそも自組織で発生した事象／被害はどのような攻撃によるものなのか、また、対応の温度感やスピード感を知るために、他の被害組織が公表した情報を参考にすることができます。

この場合、「他の被害組織が公表した情報」の中に、

・特定の攻撃手法／攻撃活動を示すに十分な攻撃技術情報が記されていること

例：　×「マルウェア感染により情報が漏えいした。なりすましメールも送信されている」

　　○「Emotet 感染により認証情報や個人情報が漏えいし、なりすましメールが取引先等に送信された」

※公表前の時点において、匿名での情報共有活動を行っていた場合、公表時の記載内容から、情報共有活動の他の参加組織が、情報を突合することが可能になる場合があります。詳細は Q10（62 頁）をご参照ください。

・対応経緯やどこに相談／報告したのか記されていること

※具体的な例は「ケーススタディ」の「ケース 3 」（140 頁）をご参照ください

が有効であり、こうした取り組みが中長期的に各被害組織で繰り返されることで、お互いにメリットを享受することができます。

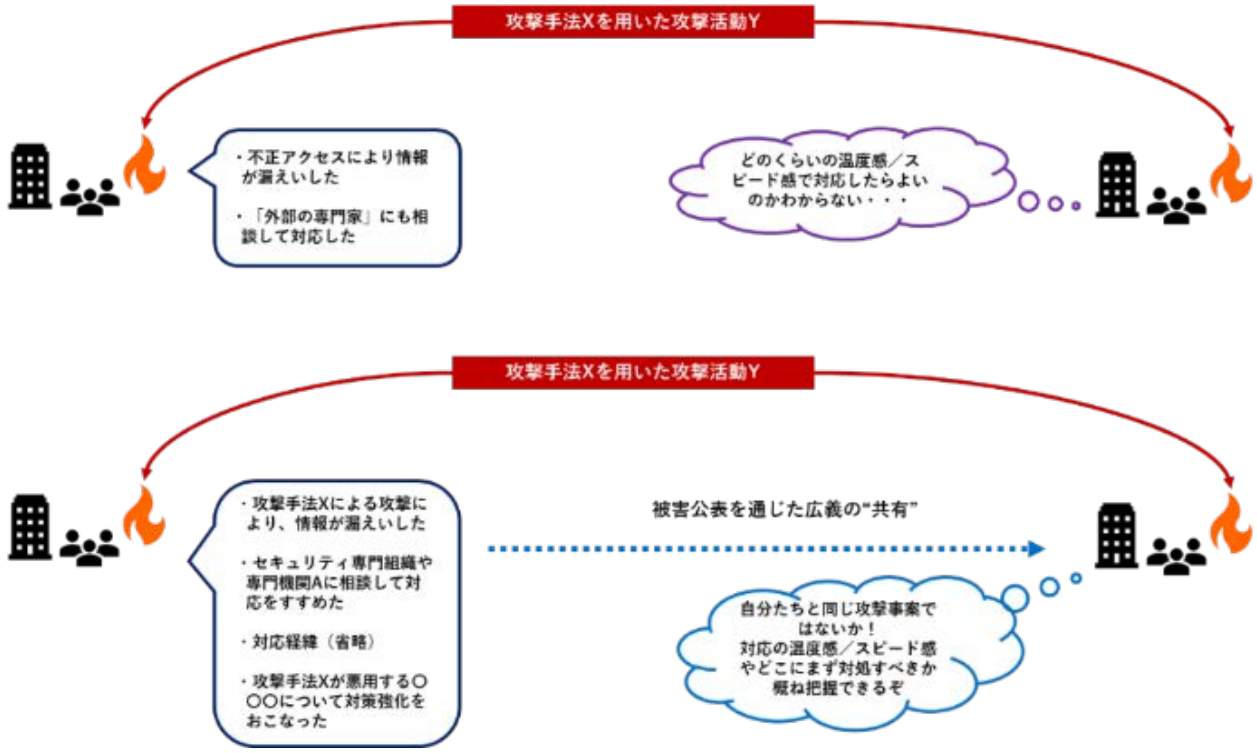

攻撃手法Xを用いた攻撃活動Y
・不正アクセスにより情報が漏えいした
・「外部の専門家」にも相談して対応した
どのくらいの温度感／スピード感で対応したらよいのかわからない・・・
攻撃手法Xを用いた攻撃活動Y
・攻撃手法Xによる攻撃により、情報が漏えいした
・セキュリティ専門組織や専門機関Aに相談して対応をすすめた
・対応経緯（省略）
・攻撃手法Xが悪用する○○○について対策強化をおこなった
被害公表を通じた広義の"共有"
自分たちと同じ攻撃事案ではないか！
対応の温度感／スピード感やどこにまず対処すべきか概ね把握できるぞ

図 52

Q17.公表する際の留意点はありますか？

被害公表を行う際の留意点として、

①必ずしも公表／非公表の判断を自組織だけで行えない（行うべきでない）ケースがあること
②第一報や調査が途中の段階で公表する場合に、不確実な情報を確定情報のように伝えてしまうと誤解を与えるケースがあること
③情報を詳細に示し過ぎることでセキュリティ上のリスクを高めてしまうおそれがあるなどのデメリットがあること

を挙げることができます。

①については、例えば自組織が多数の組織にサービスを提供するシステムが侵害され、システム上にあった多数の組織の情報が漏えい被害に遭った場合、自組織における「システムへの侵害」事案としてだけでなく、これら多数の組織がそれぞれ「情報漏えい」事案として被害公表判断／対応を行うことになります。その場合、個別の被害組織による公表タイミングや内容の判断が存在するため、自組織のみで公表タイミング／公表内容を決定することができなくなるのです。

②については、早い段階からこまめに複数回公表を行ったとしても、一向に原因調査が進んでいなかったり、被害範囲／内容が逐次変動したり、そもそもインシデント対応自体がうまく行えていないのではないか、外部知見を投入できていないのではないか、といった不安や疑問を抱かせるような情報発信の場合、いくら公表を重ねても利害関係者の納得が得られなくなります。

攻撃技術情報について、情報共有での活用（Q8（57 頁））や、専門組織から注意喚起やレポートとして情報発信（Q2（36 頁））されるほか、「どのような攻撃を受けたのか」説明するために被害組織からの公表において示される場合があります。

③については、例えば、マルウェア情報や不正な通信先に関する情報、その他攻撃手法などの技術的情報について専門的知見の不足により不正確なまま示してしまったり、あるいは、被害内容・対応情報のうち、被害にあったシステムの構成などを詳細に書いてしまい、セキュリティ上のリスクを高めてしまったりする場合などが想定されます。技術的に妥当な記載か、また、新たなリスク要因となってしまわないかなど、公表内容についても専門組織に相談することが望まれます。

影響範囲と情報が拡散する範囲

Q21（89 頁）で解説するように、サイバー攻撃に係る様々な情報の特性から、当該時点で非公表の事案について様々な経路／きっかけにより不特定多数の者に知られる場合があります。また、被害の影響範囲に応じて、非公表の事案を知る関係者が変化する点も重要です。

下記の図 53 のとおり、影響範囲が広ければ、それだけ当該事象を知る関係者も増えることになります。さらに、当該事象を知った関係者がさらに別の個人／組織に情報を拡散することも想定されるため、実際の情報の拡散範囲は影響範囲＋α の範囲となります。
したがって、影響の大きい事案ほど、事象を知る関係者を限定し非公開の状態を維持し続けることは困難であると想定されます。

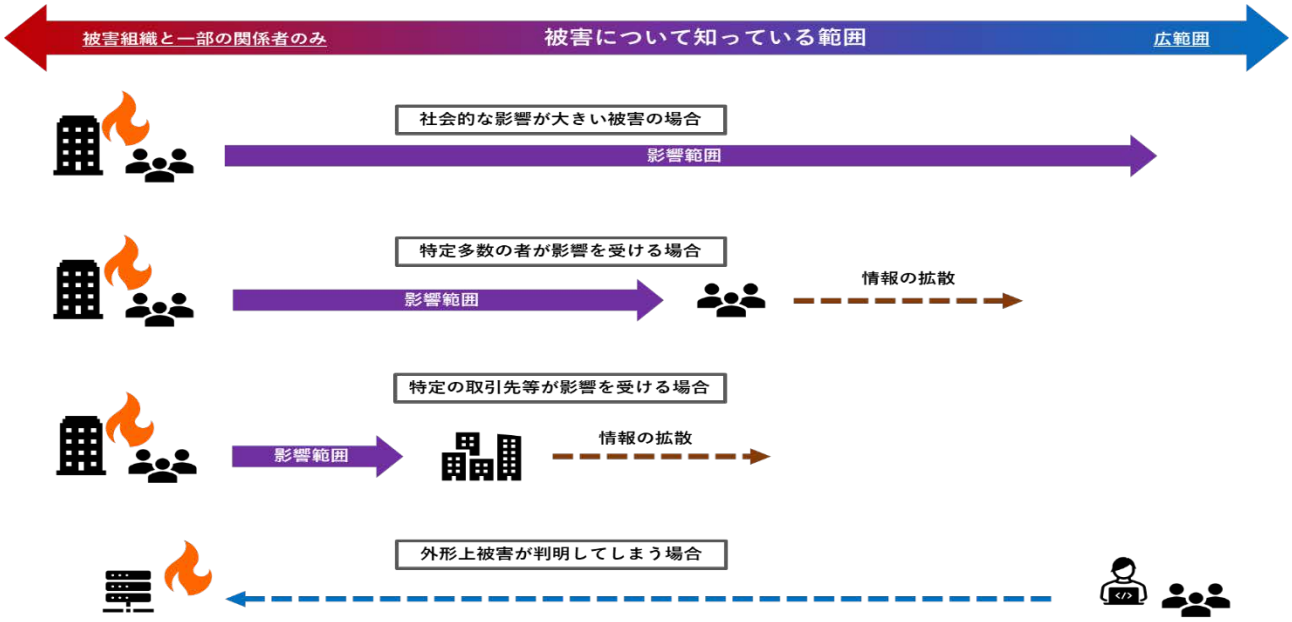


図 53

ケース：過去のサイバー攻撃が発覚し、調査を進めていく場合

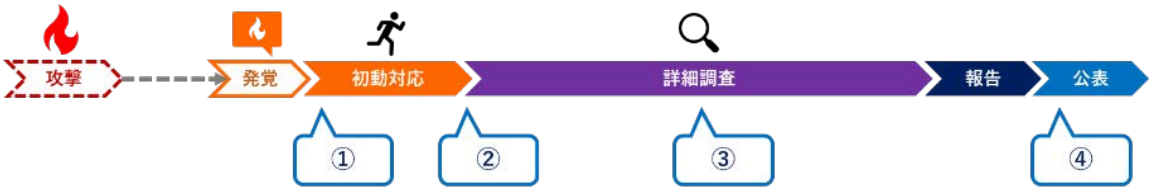


図 54

攻撃が既に終了し、しばらく経過してから発覚した場合、主なインシデント対応としては、過去の通信ログ等を遡って調査し、侵害原因や被害範囲／漏えい情報有無など時間をかけて調査していくことになります。

この場合、被害公表を判断するタイミングとしては、Q15（71 頁）のとおり、

①・②事案発覚時点または初動対応時点で深刻な被害が既に判明した時点
③詳細な被害調査を進める中で深刻な被害が発覚した時点
④調査を終えた時点

を挙げることができます。

このケースにおいて、上記①～③の判断を行うにあたってポイントとなるのは

（A）【影響範囲】判明した被害が、不特定多数の人・組織やその他社会的に大きな影響を及ぼすものかどうか
（B）【情報の拡散範囲】当該時点で公表しなくても、被害組織以外の第三者（攻撃者を含む）によって当該被害が公開情報として発信される可能性があるかどうか
（C）【アカウンタビリティ】（A）のような被害が判明してから、④のタイミングまでの未公表期間が、外部から批判を受けうるほどの長期間がどうか

となります。

（B）について、どのような情報／事象を通じて未公表事案が公開情報となってしまうのか、Q21（89 頁）をご参照ください。

（A）または（C）については、「最終的な調査内容の確定まで相当の時間がかかりそうなので、早めに第一報を公表しておけばよい」という単純な話ではありません。標的型サイバー攻撃のように、ネットワーク内において広範囲、あるいは複数拠点にわたって侵害しているようなケースでは被害範囲や侵害された情報の精査にかなりの期間を要します。「機微な情報／システムを侵害されたかもしれない」という段階で第一報を出したところ、その後の調

査によってそこまで侵害されていなかったことが判明するケースもあり得ますし、逆に第一報段階で「機微な情報漏えいの被害はない」と公表していたが、その後の調査の結果、漏えいしていたことが判明してしまったケースもあります。

したがって、例えば、社会的に大きな影響や取引先／ユーザーに二次被害が及ぶ可能性などが判明した段階や、攻撃被害あるいは調査のためのシステム停止等により対外的なサービス停止が当面続きそうな場合、まずは第 1 報を公表し、相当の調査期間を経なければ正確に把握できない被害内容等は追って続報／最終報で公表する、という多段階での公表の仕方があります。

弊社システムに対する不正アクセスについて（第 1 報）

○月×日

＊＊＊＊＊株式会社

○月 6 日に○○システムが不正アクセスを受けたことが判明し、セキュリティベンダや、専門機関 B に相談の上、現在調査をすすめています。また、本事象については C 県警察にも連絡をしております。

被害の詳細については引き続き調査中ですが、影響を受ける可能性のある取引先様等には、影響が判明次第、順次ご連絡してまいります。

現在、侵入のあった○○システムは調査等のため停止をしておりますが、弊社の△△サービスには影響はございません。

攻撃被害や調査のため対外向けサービスが影響を受ける場合は速報の主たるメッセージとなる

図 55

弊社システムに対する不正アクセスについて（最終報）

×月１日

＊＊＊＊＊株式会社

○月△日に弊社の○○システムが外部からの不正アクセスを受け調査中である旨の公表を行った次第ですが、その後、専門組織とともに調査を行い、原因特定や被害情報の確認を行うとともに、影響のあった関係各所への報告を行っております。

引き続き、再発防止に向けた対策・体制強化に取り組んでまいります。

４．　経緯と対応の流れ

○月１日	攻撃者が○○システムで稼働するソフトウェアの脆弱性を突いて侵入し、マルウェア（「マルウェアＸ」（※マルウェア名））を設置
○月２日	○○システムから社内の複数のサーバへ侵害拡大
○月５日	一部のサーバでシステム障害が発生したため調査を行ったところ、不審なアクセスを確認したため、不正アクセスの疑義がある事案として調査を開始
○月６日	不正アクセスにより社内ネットワークに侵入されたと判断し、社内のインシデント対応チームを中心にインシデント対応を開始
○月７日	セキュリティベンダＡに調査依頼をするとともに、専門機関Ｂにインシデント対応相談。Ｃ県警察に連絡。
○月 15 日	調査の結果、侵入経路が○○システムで稼働するソフトウェアの脆弱性を突いたことであると特定し、ソフトウェアのバージョンアップ等の対処を実施 見つかったマルウェアや不正な通信先に関する情報などを専門機関Ｂを通じた情報共有活動への提供を実施
○月 20 日	見つかったマルウェアの解析結果などを元に、現時点で攻撃者の侵入やマルウェアの残留はないと判断
○月△日	第一報を公表
×月　日	侵害された○○システムや複数のサーバの調査から、被害内容を精査し、影響のあった関係先への報告を開始
×月　日	暫定的な再発防止策の実施を完了

５．　被害内容

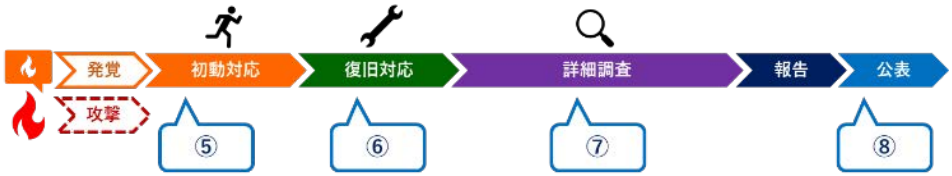
・○○システム内には技術情報、取引先に関する情報、個人情報等の機微な情報は保存しておらず、侵入した攻撃者によって認証情報が窃取されたと判断しています。

・さらに侵害を受けた複数のサーバのうち、一部のファイルサーバ内に、取引先企業との個別プロジェクトで使用していた情報が含まれており、漏えいした可能性が否定できなかったため、取引先へその旨の連絡を行いました。取引先との確認の結果、取引先に二次被害等が発生する可能性は低いと判断しています。
・その他、社内ネットワークの認証情報やサーバ等の設置情報が攻撃者により窃取されたと判断しています。

６．　原因と再発防止策
今回の侵入はインターネットに接続されている〇〇システム上で稼働するソフトウェアの脆弱性（CVE-2022-*****）が悪用されたものであったと判明しています。当該脆弱性は侵入の１週間前に修正プログラムが公開されていましたが、定期的なメンテナンス時にアップデート作業をする予定であったため、侵入時点でバージョンアップがなされていませんでした。
今後、専門機関等が出される脆弱性に関する情報を精査し、速やかに対応が必要なものについて優先度を設けて対処するよう、社内ルールや体制整備を進めてまいります。
また、攻撃者に侵入された後の侵害拡大については、ネットワーク設定やサーバの設定で防ぐことが可能だった点が認められたため、これら設定の変更による対策強化をすすめてまいります。

図 56

ケース：進行中のインシデント対応



弊社に対する侵入型ランサムウェア攻撃について（第一報）

×月１日

＊＊＊＊＊株式会社

弊社ネットワーク内への不正アクセスがおこなわれ、ランサムウェア感染被害が発生しており、現在、一部システム停止による業務影響が出ております。

専門組織とともに調査を行い、原因特定や被害情報の確認を行うとともに、影響のあった関係各所への報告を行っております。

１．経緯

○月×日△時頃、社内サーバ○台に障害が発生していることが確認されたため、調査を行ったところ、あるランサムウェアに感染していることが判明。ランサムウェアによる暗号化がなされてしまったサーバ○台の使用を停止し、調査等の初動対応を開始。

○月△日にセキュリティベンダＡや専門機関Ｂにインシデント対応の相談を行うとともに、Ｃ県警に連絡。リークサイトに弊社名が掲載されていることを確認。

リークサイトに取引先の情報や個人情報が掲載されてしまった場合、続報が必要になるケースも

２．現在の状況と今後の見込み

現在、バックアップからのデータの復旧とともに侵入原因の調査と暫定的な再発防止策の対応を進めています。一部、○○業務についてはサービス停止中ですが、△△業務は通常どおり対応しております。

現時点で○○業務の再開めどは立っておりませんが、代替サービスの提供をしております。

なお、リークサイトに弊社名が掲載されており、現時点で弊社から漏えいした機微なデータ等の掲載は確認されているところですが、弊社内から機微な情報が漏えいした可能性について現在調査をすすめております。

～以下省略～

図 57

Q18.警察への通報・相談は、行った方が良いでしょうか？

警察では、被疑者の検挙に加えて、捜査で判明した犯罪の手口等を関係機関に情報提供してさらなる被害を防止するなどの取組を行っているので、サイバー事案が生じた際には警察への通報・相談を積極的に行うことが望ましいといえます。

サイバー事案は、匿名性が高く物理的痕跡が残らないなどの特徴がありますが、警察にとっては被害を受けたサーバや機器に残された痕跡が重要な捜査の手がかりになります。また、被疑者を追跡するため、関係事業者に対して通信記録等を照会する必要がありますが、こうした記録は一定の期間で消失するおそれがあることから、警察による捜査活動を迅速に開始するためには、被害組織から警察に対する早期の通報・相談が重要となります。

サイバー事案が生じた際に警察に対して早期に提供する情報については、事案に応じて様々なものが考えられますが、例えば、被疑者の追跡・特定に必要不可欠な攻撃元のＩＰアドレス、マルウェアのハッシュ値等の被害サーバ等に記録されたIoC 情報等が挙げられます。しかし、上に述べたとおり、これら全ての情報が収集できるまで警察への通報・相談を控えるのではなく、早期に警察に連絡することが重要です。

被害組織から警察に対する早期の通報・相談は、事案の把握の端緒として必要不可欠なものですが、警察による捜査には、被害組織からの聴取結果、攻撃を受けたサーバや機器に残された記録等も必要とされることから、通報・相談による被害事実の伝達等のみならず、警察の捜査にも可能な限り協力することが望ましく、これにより、更なる被害の防止を期待できます。警察では、被害組織に対して捜査の過程で必要な情報提供を依頼することがありますが、いずれの場合も被害組織における早期復旧等に配慮した初動捜査を推進することとされています。

警察へのサイバー事案の通報・相談は、最寄りの警察署又は都道府県警察本部のサイバー犯罪相談窓口へ行うこととされており、急を要する場合には、最寄りの警察署へ通報・相談することが推奨されます。

【都道府県警察本部のサイバー犯罪相談窓口一覧】

https://www.npa.go.jp/cyber/soudan.html

警察による被害防止対策にはどのようなものがあるか

警察は、被害を受けたサーバ等や攻撃に用いられた不正プログラムを解析した結果、捜査で把握した情報等を総合的に分析し、被害実態の解明に取り組んでおり、その中で明らかになった犯行手口や必要なセキュリティ対策を、広く国民に対して広報啓発するとともに、各地域で活動する多様な主体との間で情報共有、意見交換等を行うなどの取組を推進しており、具体的には以下のような対策を実施しております。

○警視庁において、不正送金被害を受けた金融機関と連携して、速やかに犯行手口を分析の上、モニタリングやインターネットバンキングへのログイン時における認証の強化等の被害防止対策を要請し、当該金融機関において、これらの対策を実施した結果、当該金融機関に開設された口座を送金元とする不正送金被害は確認されなくなりました。

○福岡県警察において、警察への相談により把握したＩｏＴ機器の脆弱性について、当該ＩｏＴ機器の脆弱性対策を講じるよう販売元に働きかけるとともに、注意喚起を実施しました。

○警察において、サイバー事案による被害の防止に向けて、各都道府県警察及び管内の事業者等により構成されるサイバー事案対策に関する協議会を設置するなどした上で、同協議会の会員企業等に対して、サイバー事案の手口やその対策に関する情報提供やサイバー事案認知時における警察への通報体制の確立に向けた取組を推進しています。

○警察では、各都道府県警察及びサイバー事案の標的となるおそれのある重要インフラ事業者等で構築される、サイバーテロ対策協議会を全ての都道府県に設置し、サイバー事案の脅威や情報セキュリティに関する情報提供、民間の有識者による講演及び参加事業者間の意見交換・情報共有を行っているほか、サイバー事案の発生を想定した共同対処訓練等を行っています。

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？

被害組織において、インシデント対応に追われる中で捜査協力として様々な負担を強いられるのではないか、警察において適切に情報が取り扱われるのか、といった懸念から、警察に対する通報・相談がためらわれているとの指摘があります。

被害組織の負担に関する指摘について、警察では、被害組織が被害状況の把握やシステムの復旧、顧客への連絡等、緊急対応の最中であることに留意し、業務への影響が最小限となるよう被害組織による早期復旧等に配慮した初動捜査を推進することとしています。

また、警察における情報の取扱いに関する指摘については、警察が捜査中であることを理由に被害組織が行う情報の共有活動等を妨げられるのではないか、警察が被害の事実を勝手に公表するのではないかといった点が懸念事項として考えられます。この点、警察では、被害組織の意向を確認し、これに配慮しつつ、対応をすることになります。

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？

法令等に基づく報告（※）以外であっても、広く国内において被害が発生している、または発生しているおそれのある事案について、所管省庁がサイバー攻撃被害に係る情報の収集を行う場合があります。個々の被害組織では「自組織で把握した攻撃が他にどのくらい広がりを見せているのか」を知ることは難しいケースがあるため、専門組織に相談した上で、該当するような事案であれば所管省庁への任意の報告が望ましいです（なお、被害に関する公表や報道を受けて、被害組織に所管省庁から情報提供の依頼がなされる場合があります)。

所管省庁への報告の場合には、被害の全体像の把握や、攻撃側の意図の特定のために、攻撃技術情報とともに被害内容・対応情報についても、報告が必要となりますが、その範囲は事件ごとに異なることから、まずは、被害状況や専門組織への相談状況を早期に一報することが望ましいです。

こうした情報は、各所管省庁に報告された後、被害組織の同意を得た上で、省庁間の総合調整機能を担う内閣サイバーセキュリティセンター（NISC）をハブとした連携を通じて、広くユーザーに影響を及ぼすような規模の攻撃への対処、サイバー攻撃対処の全体像からみた長期的な対抗措置（国としての対処）やサイバーセキュリティ対策に関するガイドラインの策定等のために活用されます。

※　例えば、重要インフラ事業者は、重要インフラサービス障害を含むシステムの不具合等に関して、法令等に基づき、被害の状況や事業継続の見通しについて、所管省庁への報告が必要となります。報告すべき内容及びタイミングについては、各法令またはガイドライン等に示されています。

各重要インフラ事業者に関係する法令またはガイドラインについては、「重要インフラのサイバーセキュリティに係る行動計画」の「別紙２　重要インフラサービスとサービス維持レベル」の一覧表中の「左記障害の報告に係る法令、ガイドライン等」の欄を参考にしてください。

【重要インフラのサイバーセキュリティに係る行動計画】

（48 頁以下に、「別紙２　重要インフラサービスとサービス維持レベル」の一覧表あり）

https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf

セキュリティインシデントの報告制度について

所管省庁への報告が義務付けられている法令のほか、その他報告が求められている制度等について以下に紹介します。

＜法的拘束力のある義務＞

（1）法令に基づく義務

個人データの漏えい・滅失・毀損（漏えい等）に対する報告義務	個人情報保護法ほか	一定の要件に該当する個人データの漏えい等又はそのおそれのある事態（報告対象事態）について個人情報保護委員会等への報告義務（個人情報保護法 26 条） ※原則本人への通知が必要、漏えい等事案の内容等に応じて公表が望ましい
特定個人情報の漏えい等に対する報告義務	マイナンバー法	一定の要件に該当する特定個人情報（マイナンバーを含む個人情報）の漏えい等又はそのおそれのある事態等について個人情報保護委員会への報告義務（マイナンバー法 29 条の 4） ※原則本人への通知が必要、漏えい等事案の内容等に応じて公表が望ましい
業法に基づく事故報告義務	各業法	各業法に基づく事故（サイバーセキュリティインシデントを含む）発生時の所管省庁等への報告義務 例）電気通信事業法 28 条（通信の秘密の漏えい・重大事故）
報告等の求めへの対応義務	サイバーセキュリティ基本法ほか各業法等	○当局から法令に基づく報告等の求めがあった場合、原則として対応する義務あり（情報提供・資料提出の求め等） 例）サイバーセキュリティ基本法 17 条 3 項 ○報告徴収をベースとした事故報告義務 例）電気通信事業報告規則 7 条の 3（事故の四半期報告）

表 6

（2）契約・約款上の義務

上場会社の適時開示	上場会社（またはその子会社等）においてサイバーセキュリティインシデントが発生し、それが投資判断に著しい影響を及ぼす場合、適時開示が必要（有価証券上場規程（東京証券取引所）402 条 2 項 x、403 条 2 項 l）
認定個人情報保護団体対象事業者	認定個人情報保護団体の対象事業者は、同団体が定める個人情報保護指針（個人情報保護法 54 条）に基づき、同団体に事故報告が求められる場合がある 例）JIPDEC 個人情報保護指針
プライバシーマーク付与事業者	プライバシーマーク付与事業者は、個人情報に関する事故等の発生時に関係審査機関に報告しなければならない（プライバシーマーク付与に関する規約 12 条） ※負担軽減の措置あり ※「事故等」の範囲は個人データの漏えい等以外も含む

その他契約に基づく義務	○秘密保持契約（NDA）、委託契約、データ取引契約等において、事故発生時等に契約の相手方に報告する義務があるケース ○情報共有体制等の約款において、一定の条件の下での情報提供が求められるケース ※一般論であり、ケースとしては少ないと考えられる

表 7

＜法的拘束力はないが推奨される事項＞

（1）ガイドライン等に基づく推奨事項

分野別のガイドライン等	個人情報保護関係やセキュリティ関係のガイドラインにおいて、所管省庁等への報告や公表が求められる場合がある 「金融分野における個人情報保護に関するガイドライン
重要インフラ事業者による情報連絡	重要インフラ事業者は、重要インフラサービス障害を含むシステムの不具合等に関する情報について、所管省庁を通じて NISC に連絡することとされている（重要インフラのサイバーセキュリティに係る行動計画（サイバーセキュリティ戦略本部））
不正アクセス等に関する届出	コンピュータウイルス・不正アクセス検知時には、IPA へ届け出ることが望ましい 「コンピュータウイルス対策基準」（平成 7 年通商産業省告示第 429 号） 「コンピュータ不正アクセス対策基準」（平成 8 年通商産業省告示第 362 号）
脆弱性発見時の届出	ソフトウェア製品の脆弱性およびウェブサイトの脆弱性を発見した者は、IPA へその旨を届け出ることが望ましい 「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」（平成 29 年経済産業省告示第 19 号）
警察への通報・相談	サイバー事案に係る犯罪の被害に遭った場合には、警察へ通報・相談する対応が望ましい（Q18（83 頁）、Q19（85 頁）参照） 「サイバーセキュリティ戦略」（令和 3 年 9 月閣議決定）等

表 8

（2）その他推奨事項

公的機関の注意喚起	様々な機会において、関係省庁がサイバーセキュリティ対策の強化を呼びかけるケースがあり、その中で、不審な動きを検知した場合等の所管官庁への情報提供・相談を推奨 例）経済産業省・金融庁・総務省・厚生労働省・国土交通省・警察庁・NISC 「サイバーセキュリティ対策の強化について（注意喚起）」（2022 年 3 月 1 日） 例）経済産業省産業サイバーセキュリティ研究会「サイバーセキュリティ対策についての産業界へのメッセージ」（2022 年 4 月 1 日）

表 9

＜被害組織の保護の観点について＞

Q21. 公表していないのに自組織の被害が知られて公開されてしまうのはなぜですか？

サイバー攻撃の被害を示す情報や、攻撃があったことを推測できる情報を以下のような経緯で第三者が入手したり、公開情報として拡散したりすることがあります。

① 外形上攻撃被害が確認できる場合
Web サイトの改ざんなど、そもそも標的となったシステムに不特定多数の者がアクセス可能な状態であった場合など

② 漏えい情報の公開や犯行声明
攻撃者が窃取した内部データをリークサイトに晒したり、名指しで犯行声明を公表したりするような場合

③ （内部）関係者による情報発信
インシデント対応が行われていることなどを組織の関係者が SNS 等で外部に情報発信してしまう場合

④ 解析結果からの被害の推測
公開解析サービスにアップロードした検体の内部に含まれていた情報から、被害組織のシステムを特定する情報が判明してしまう場合

⑤ OSINT（公開情報を元にした調査・分析手法）によるインフラ調査
攻撃を受ける可能性のある脆弱なシステムなどが公開検索サービスで調査可能な場合（※あくまで「攻撃を受ける／受けた可能性があるのではないか」という推測が行われるもの）

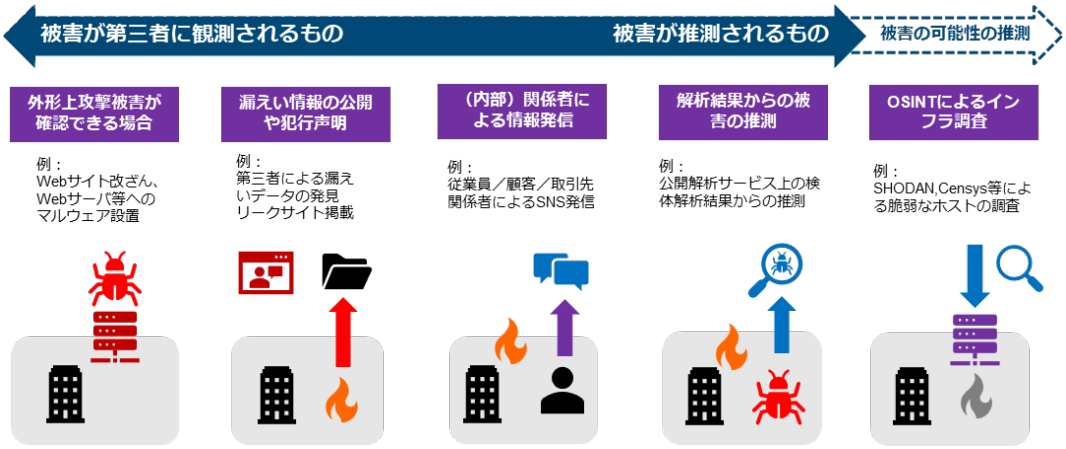


図 58

被害認知の観点から見た侵入型ランサムウェア攻撃対応の難しさ

一般的な不正アクセス事案の場合、基本的には被害組織自身からの公表まで、外部に被害事実が知られることはありません。公表前に上記のような経緯で被害事実の一部が外部に知られるとしても、外部からの問い合わせ等は、ある程度の調査が進んでいる段階で来ることが想定されるため、何らかの回答が可能です。

一方で、ランサムウェア攻撃の場合、特にリークサイトを用いる「二重の脅迫」タイプの攻撃の場合、攻撃（暗号化）の実行直後にリークサイト上に被害組織名や窃取したデータのサンプルデータなどを掲載するため、被害発生とほぼ同タイミングか数日内に不特定多数の者が被害を知ることになってしまいます。そういった、「不特定多数の者が未公表の被害事実を知ることになる」ことも脅迫効果に悪用する攻撃であるため、不特定多数の者に被害を知られることを避けられない攻撃類型と言えますが、他方で、暗号化被害によって主要なシステムが使用不能になったり、予防措置的にサーバやネットワークを停止させることによる業務停止、対外サービス停止が発生したりすることによって、「攻撃によるシステム停止ではないか？」と憶測が出やすい状況になるという側面もあります。

そうしたタイミングで問い合わせ等が来ても、場合によっては初動対応が間に合っておらず、実際に攻撃された拠点が海外拠点やグループ企業であった場合などは被害事実の把握すらままならない状況であったり、そもそもランサムウェアによる攻撃かどうか不明な状況であったりするケースもあります。

先述のとおり、「被害を知った不特定多数の者」の反応すらも身代金要求のプレッシャーに利用しようとするランサム攻撃において、一刻も早く、被害組織が攻撃（原因）を特定し、早期にシステム復旧や業務再開を行い被害を最小限に食い止めるためには、「被害を知ることになった」関係者においても、ランサム攻撃という犯罪の特殊な事情を理解することが求められています。

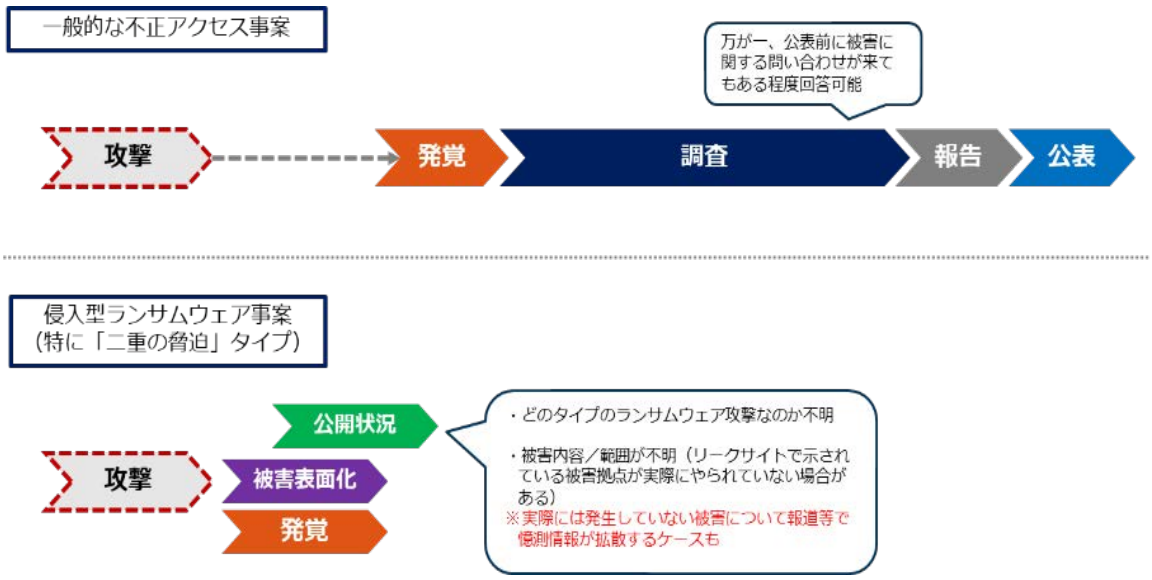

一般的な不正アクセス事案
万が一、公表前に被害に関する問い合わせが来てもある程度回答可能
攻撃
発覚
調査
報告
公表
侵入型ランサムウェア事案
(特に「二重の脅迫」タイプ)
公開状況
攻撃
被害表面化
発覚
・どのタイプのランサムウェア攻撃なのか不明
・被害内容／範囲が不明（リークサイトで示されている被害拠点が実際にやられていない場合がある）
※実際には発生していない被害について報道等で憶測情報が拡散するケースも

図 59

Q22. 他組織の被害に関する情報を発見した場合、どうしたらよいですか？

以下のようなケースにおいて、自組織以外の、他の組織の攻撃被害を示す情報を発見する場合があります。

① 被害組織から漏えいした情報を発見した場合

② 他組織のシステムが踏み台となり、自組織への攻撃に悪用されていた場合（被害組織が他の組織の被害を知るケース）

前者は Q17（76 頁）で紹介したようなランサムウェア攻撃におけるリークサイト掲載情報のほか、インターネット上やダークウェブ上のフォーラムなどで窃取データがやりとりされているケースなどが想定されます。この時、こうした情報を見つけるのは、リサーチャーや研究者、メディアのほか、自組織からの漏えい情報を調査していた被害組織またはその委託を受けた専門企業が他組織からの漏えい情報も偶然発見する場合があります。

いずれのケースであっても、発見した者が他の被害組織に直接伝えることも可能ではありますが、本項の後半や Q23（94 頁）～Q25（99 頁）において後述のように当該データの取扱いに係る法的な注意が必要であったり、当該データの不確かさによるコミュニケーションミスによる不要なトラブルを避けたりするため、専門機関を仲介して伝えることを推奨します。

いずれのケースでも、他の被害組織自身のインシデント対応支援が必要な状況が想定されますので、専門組織へ相談することが望ましいです。

また、特に①のケースでは、「漏えい情報」自体の信ぴょう性が不明であったり、中にはデータを売買しようとする者が虚偽の説明をしていたりする場合もあるため、当該情報をもってして、被害が事実であると判断することは拙速です。

さらには、こうした漏えい情報が存在することが不特定多数の者に伝わることで、漏えい情報を悪用した二次被害が発生するおそれがあるため、発見者は当該情報を被害組織や専門組織以外に伝えることについて留意が必要です。

“漏えい情報”は本当に現在の危険を示しているのか

過去の攻撃によって窃取された情報がアンダーグラウンドマーケットで流通したり、インターネット上で発見されたりする場合があります。こうした場合、「対象の組織に注意を呼びかける」ためとして、当該情報を第三者が公開するなどして拡散することがあります。

例えば、2020 年 11 月に特定の SSL-VPN 製品利用組織の認証情報が大規模に流出した事例がありました。これは、過去にイニシャルアクセスブローカーが脆弱性を突いて窃取したと思われる認証情報が販売されていたところ、何らかの経緯でインターネット上に拡散したものと考えられています。対象ホストの IP アドレス情報から、機器の利用組織が一部特定され、報道等で広く公開されることとなりましたが、この漏洩した認証情報の脅威を正しく理解するには注意が必要です。

下記図 60 の①のとおり、当該認証情報のセットリストは過去に脆弱性を突いた攻撃が発生していた可能性を強く示しています。しかし、JPCERT/CC からの注意喚起や脆弱なまま稼働する機器の利用組織等に対する個別通知が行われていたため、最初の不正アクセスを回避できなかった／検知できていなかったとしても、下記図 60 の④のとおり、脆弱性の修正対応と漏えいの可能性を踏まえた認証情報のリセットの措置がなされていた組織が一定数含まれているため、「現在差し迫った危険が迫っている」とは言えない場合もあります。確かに一定数は③のように侵入型ランサムウェア攻撃の初期侵入に悪用されてしまっていたり、あるいは②のように今後、侵害されたりする可能性が否定できない組織も存在しているとは言えます。

単純に「漏えい情報」と一言で示しても、脅威の度合いは組織によってさまざまであるため、すべてまとめて「注意喚起のため」として公開することが必ずしも妥当であるとは言えず、非公開による対象組織への個別通知など、ケースバイケースの対応が必要になります。

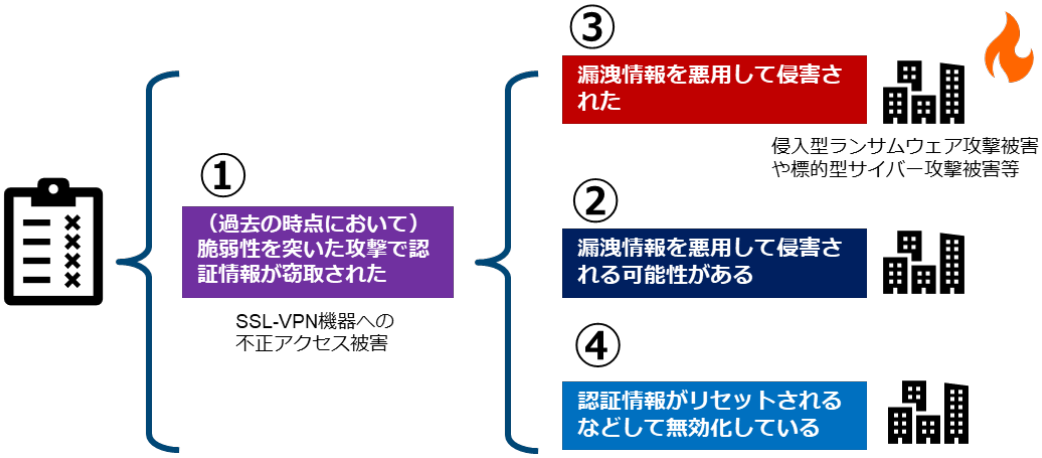


図 60

Q23. 製品の脆弱性が悪用されていた場合、当該情報はどのように扱えばいいですか？

インシデント対応を進めていく中で、特定のソフトウェア製品の脆弱性を悪用した攻撃が見つかる場合があります。この時、

① 既知の脆弱性を悪用した攻撃
② 未知の脆弱性を悪用した攻撃
③ 上記①、②のいずれか不明な攻撃

の３つのケースが想定されます。

①については、被害公表時などに当該脆弱性を悪用した攻撃があった旨などを示すことに何ら問題はありませんが、②または③のケースでは対応に注意が必要です。

脆弱性に対する修正プログラムの提供がなされていない状態で当該情報が公表されてしまうと、新たな攻撃に悪用されるおそれがあります。まずは国内における脆弱性関連情報の取扱いについて定めた、情報セキュリティ早期警戒パートナーシップガイドラインに基づく対応が必要になります。受付機関（IPA）への届出のほか、インシデント対応相談を含めて調整機関（JPCERT/CC）への相談による対応も可能です。制度に基づく対応により、製品開発者から脆弱性の公表や修正プログラムのユーザーへの提供、悪用に関する注意喚起が行われます。
セキュリティベンダによる調査が入っていても、③のように未知の脆弱性悪用かどうか不明な場合も想定されますが、この場合も制度の各窓口への相談が推奨されます。

なお、法人向け製品などで、被害組織（ユーザー組織）が直接または運用保守ベンダ等を経由して、製品開発者に連絡可能なケースがあります。上記の制度はこうした直接の連絡による脆弱性修正対応を否定するものではありません。
ただし、インシデント対応と並行して、脆弱性修正のためのやりとりを行うことが負担になったり、公表に向けた調整に難航したりするケースもありますので、制度に基づいた第三者機関による調整を依頼することが推奨されます。

「未知の脆弱性が悪用された」ことをどこまで公表で示すか

Q17（76 頁）で紹介したような、被害発生とともに直ちに速報的な公表を行わなければならないケースや、中間報告として攻撃原因について触れざるを得ないケースが想定される場合、どこまで対外的に示すべきかの論点があります。

1 つの方法としては、悪用等の二次被害が発生しないように、当該製品名は伏せた上で、制度に基づく届出・調整等の対応を進めている旨を記載することです。

制度に関する規程である、経済産業省告示「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」では、（脆弱性の）発見者が正当な理由なく第三者に開示してはならない「脆弱性関連情報」として、「脆弱性情報」「脆弱性が存在することを検証する方法」「脆弱性を悪用するプログラム、指令又はデータ及びそれらの使用方法」の 3 つを挙げており、製品名を示さず「悪用された可能性のある脆弱性について、制度に基づいた対応を実施している」の旨を対外的に示すことは問題ありません。

製品開発者が脆弱性を公表したものの、攻撃による悪用の有無を明かしていない場合、攻撃発生時点において未知の脆弱性が悪用された事実を被害組織自身が公表することについての論点があります。

被害組織側の立場としては、「いかに予防・回避が難しかったか」を示す重要な情報であることや、同じ製品を使用する他の組織への注意喚起にもなる反面、製品開発者にとっては自社製品のレピュテーション（風評）リスクとなるネガティブな情報です。

また、当該悪用時点で未知の脆弱性が存在していたことだけが、ただちに侵害原因の主たる要因であったかはケースバイケースであり、仮に未知の脆弱性が存在していても、その他の当該ソフトウェア、あるいはシステム全体で別途推奨されている設定等を適切に用いていれば最終的に攻撃が成功しなかったケースなども想定されます。

未知の脆弱性の悪用の有無について、製品名を含めて公表する際には、公表による社会的影響／注意喚起効果といった要素も踏まえて多角的な判断が必要になるため、脆弱性の調整にあたった専門機関を交えて、どのような対応を採るか検討することが望まれます。

Q24. 他の被害組織を踏み台として攻撃された場合や利用するクラウドサービス、運用保守ベンダが管理／提供するシステムが攻撃された場合、当該情報はどのように扱えばいいですか？

基本的には Q22（92 頁） をご参照ください。ここでは以下のケースについて解説します。

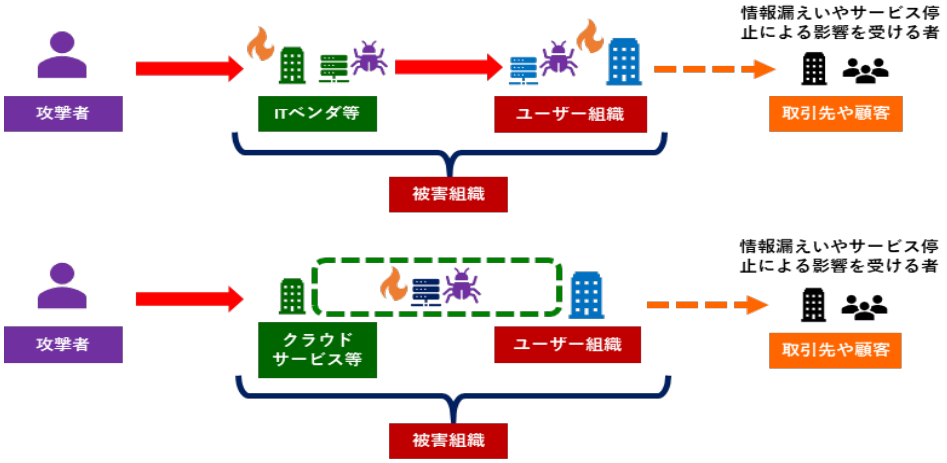


図 61

改ざんサイトの閲覧によるマルウェア感染をトリガーとするケースも類似のケースですが、ここで取り上げるのは、両組織間に契約が存在するケースとなります。

一義的にはサービス提供をしていたベンダ、サービス提供者側は二次被害防止のため、他のユーザー組織向けに通知が求められます。

そのうえで、ユーザー組織側の被害組織が公表を行うにあたって、主原因たる当該サービス経由での侵害について発表するとした場合、サービスを悪用されたベンダ、サービス提供者側がこれにどう応えるかが問題となります。ユーザー側は取引先や個人情報漏えい等の影響を受ける顧客への通知や注意喚起が法令上義務付けられている場合がありますので、これに必要な情報として当該サービスが侵害された旨を示すことを引き留めることは困難です。

一方で、ユーザー組織側で留意すべき点としては、当該原因となったサービスへの侵害について適切な対応が取られていない状態でこれを公表することは二次被害防止の観点から避けるべきですので、ベンダ、サービス提供者側の必要な初動対応が済んだことを確認した上での情報の取扱いが必要です。

この問題についても、両者の利害が衝突する可能性や、未知の脆弱性悪用の可能性などもあるため、第三者としての専門機関への相談が推奨されます。

ユーザーへの個別通知か、情報共有か、注意喚起か

MSP（Managed Service Provider）と呼ばれるような、遠隔での運用保守を行うベンダ経由での攻撃など、運用保守ベンダが主に管理／提供するシステム経由で行われる攻撃の場合、Q3（37 頁）で示したとおり、ベンダ、ユーザー双方が被害組織となります。こうした場合、どちらか片一方の判断では情報共有活動への情報提供や被害公表が行えなくなるケースがあります。

特に、ベンダにおいて問題となるのは、当該システム／サービス経由で侵害が発生していることを多数のユーザー組織にどのように伝え、調査支援していくのかという点です。
こうしたケースの多くは法人向け製品、サービスで発生するため、基本的には個別に非公開で通知・調整していくことが想定されます。

しかしながら、被害組織でもあるベンダ側はインシデント対応でリソースがひっ迫していることもあり、速やかに多数のユーザー組織に同時並行で通知・調査支援することが困難なケースがあります。

したがって、早期に注意を呼びかけ、場合によっては被害拡大を防止するため、①公表による注意喚起を行うか、②情報共有活動を通じた情報展開、が選択肢として挙がります。
ベンダの立場に立てば、自社が提供するシステム／サービスが侵害されているというレピュテーション（風評）上のネガティブ情報を開示することに消極的にならざるをえませんし、いずれ公表するとしても社内外の各種調整に時間がかかります。情報共有活動に展開する場合、情報共有活動内には通知対象となるユーザー組織もいれば、まったく関係のない組織もいることが想定されるため、被害公表までに特定多数の関係者に知られることにはなってしまいますが、公開で注意喚起等を行うよりは展開先がコントロールされます。一方で、①にせよ②にせよ、そのための調整を行っている間に、影響を受けるユーザー組織への通知が遅れたり、非公開で行っていた通知内容が意図せず外部に漏えいしたり、あるいは、悪用被害が発生してしまった場合、公表による注意喚起を行わなかったことが社会的に批判を受ける可能性があります。攻撃の発生状況、被害の把握状況、通知に係る時間・リソース、そうした総合的な観点から通知方法の適切な選択が求められます。

また、こうした攻撃方法は広範囲あるいは深刻な被害を生むところ、同じような攻撃経路を悪用した攻撃が再び起きないように社会全体で対策が行われる必要があります。同業他社を含めて類似のインシデント対応知見が向上し、同じような深刻な攻撃被害が再び発生しないよう、ベンダ自身のインシデント対応や影響のあった各ユーザーにおけるインシデント対応がひと段落した時点において、被害公表やノウハウ共有目的の情報共有が行われることが必要です。

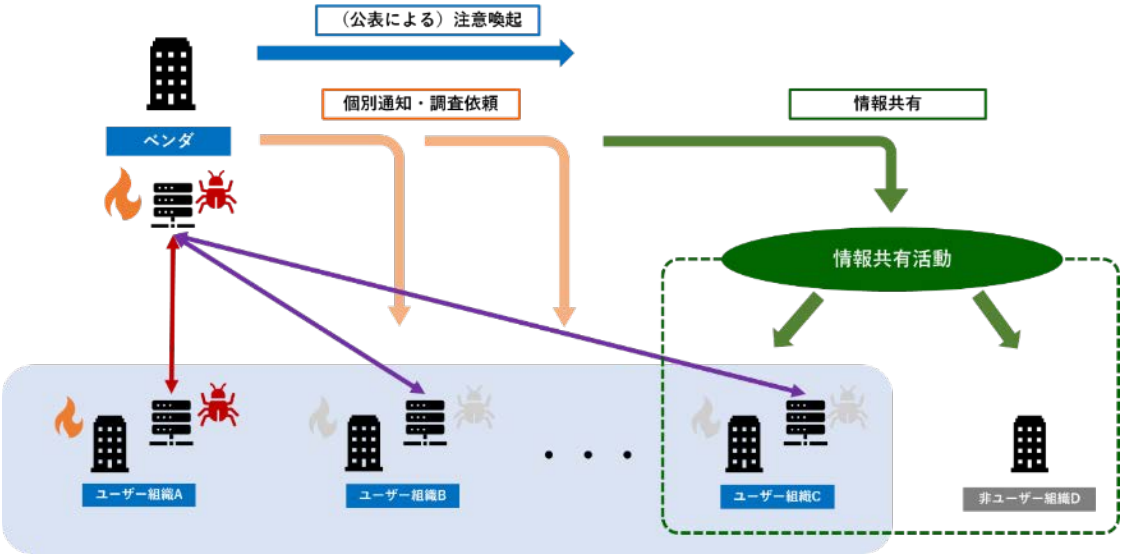

（公表による）注意喚起
個別通知・調査依頼
情報共有
ベンダ
情報共有活動
ユーザー組織A
ユーザー組織B
ユーザー組織C
非ユーザー組織D

図 62

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？

本ガイダンスでは、基本的に攻撃技術情報は速やかに共有され、被害組織が特定されないなどの被害組織保護への配慮がなされている情報については、専門組織からの注意喚起やレポート等を通じて発信されることが望ましい理由などを解説しています。同時に、被害組織自身が公表する場合でも、ある程度の攻撃技術情報を示される場合があることも解説のとおりです（Q16（72 頁））。他方で、非公開での共有にせよ、公開情報にせよ、攻撃事象に関する情報が（不）特定多数に伝わることが好ましくないケースが例外的に存在します。

例えば、個別製品の脆弱性ではなく、広くソフトウェア製品一般にあり得る、管理者側の設定不備に関する情報については、“模倣犯”的な他の攻撃者やその他正当な理由が認められないアクセスなどを惹起してしまうおそれがあります。ただし、製品開発者／サービス提供者側においては、影響対象のユーザーへの個別通知が難しいケースや被害発生前の個別通知が間に合わない場合において、公開での注意喚起を行うことも想定されます。

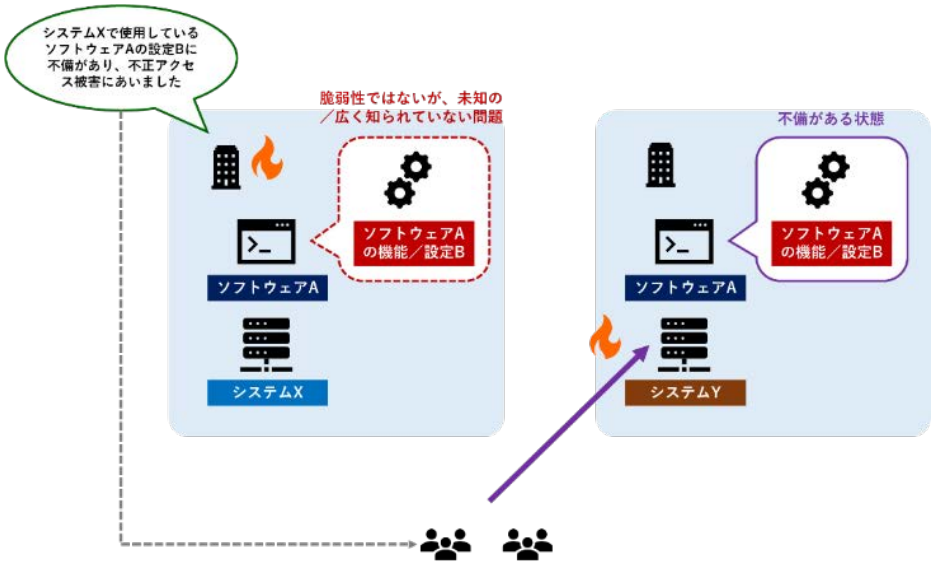


図 63

一般的に正規サイトを模倣したフィッシングサイトなどの不正な Web サイトについては、不特定多数のユーザーに広く知らせるべく、詐称元組織や専門機関等から公開での注意喚起がなされます。

一方で、フィッシングサイトやマルウェアサイトではない偽サイト、「多くのユーザーがアクセスすること自体を不法行為の目的」としているような偽サイトの場

合、こうした事象自体への注目が集まることで検索回数が増えてしまい、より多数の者にアクセスされやすくなってしまうケースがあります。

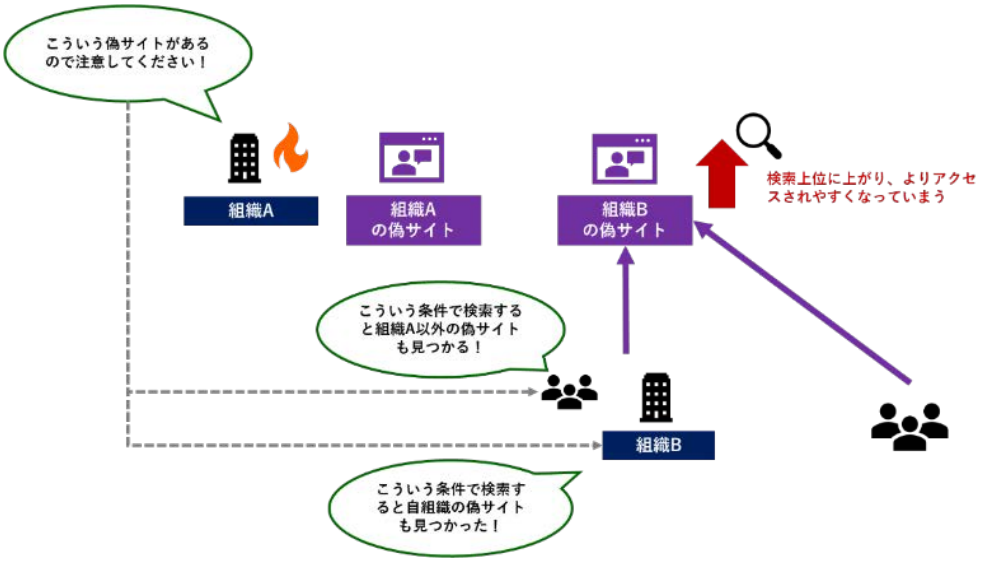


図 64

Need to know の原則について

脅威情報はなるべく多くの組織に共有できれば、それだけ多くの被害を未然に防ぐことが可能です。ただ、問題は Q10（62 頁）で紹介したとおり、参加組織が増えることで（主に意図しない）漏えいリスクが増えることや、活動参加組織の“満足度”が減少する課題があるため、ある程度限定された範囲内において非公開で活動が行われることになります。

「どの範囲／どの組織／誰にまで情報を共有すべきか」という問いに対して、インテリジェンスの世界では「Need to know」の原則が一般的です。サイバーセキュリティの業界においてもこの言葉はよく使われています。

ただ、サイバーセキュリティにおける脅威情報を対象として情報共有活動において異なる点があるとするならば、「誰がこの情報を知るべき（伝えるべき）なのかお互いに知る術がない」状況がある、ということです。

Q6（47 頁）、Q13（67 頁）で述べたとおり、非公開で行われる情報共有活動の大半は、特定分野毎や特定の目的別に運用されていますが、攻撃者は分野横断的に攻撃を行う場合があります。こうした場合、特定分野・目的に閉じた共有活動だけでは被害を受ける可能性のある標的組織をカバーできません。ある程度専門組織が攻撃動向や攻撃者について事前のプロファイリング的な知見を有していたとしても「どこの組織がやられている可能性があるか」絞り込むことは困難なケースが大半です。

したがって、情報共有活動においては、「ある程度攻撃を受ける可能性があると見込まれる対象組織／範囲に情報を展開してみる」というシグナリング的な情報展開（Q21（89頁）参照）が用いられる場合があります。

また、サイバーセキュリティにおける情報伝達においては、“温度感”の問題があります。例えば、同じ脆弱性情報に関する注意喚起でも「既に国内で悪用されている」という情報が付いているかいないかで各組織での対応は大きく変わります（参照：Q23（94頁））。インディケータ情報でも「○○分野の組織で被害が確認されている／○○分野を狙っている××という攻撃グループの攻撃キャンペーンに関するものである」という情報が付加されれば、受信組織の警戒度はかなり変わるはずです。

情報共有活動では「誰に情報を渡すべきなのか知ることができない場合がある」という条件を抱えながら、「本当に知るべき対象にその意図／背景も含めて伝える事が望ましい」という問題にも向き合わなければならないのです。

＜攻撃技術情報の取扱いについて＞

Q26. マルウェアに関する情報とはどういうものですか？

情報共有活動で共有されるマルウェアに関する情報は基本的に

・ハッシュ値
・マルウェアの種類（名称など）
・通信先（またはその有無）
・（被害現場で見つかっている）ファイル名・ファイルパス
・（判明していれば）マルウェアの主な機能
・見つかった経緯

となります。マルウェア検体そのものを交換することはリスクを伴うため、基本的には調査にあたった専門組織が行った解析結果のうち、上記の種類の情報が共有活動に提供されています。あるいは、検体そのものの解析を行えていなくても、使用しているアンチウィルス製品や監視サービスの検知結果として示されるファイル名、検知名（マルウェアの種類）、ハッシュ値などの情報が、情報共有を行うための外部への提供情報として使われます。

専門組織同士が共同で分析を行うケースなどは、検体そのものを交換する場合がありますが、検体を見つけた組織が解析を確実に行えているようであれば、当該専門組織の解析結果を信頼した上で、共同での分析が行われます。

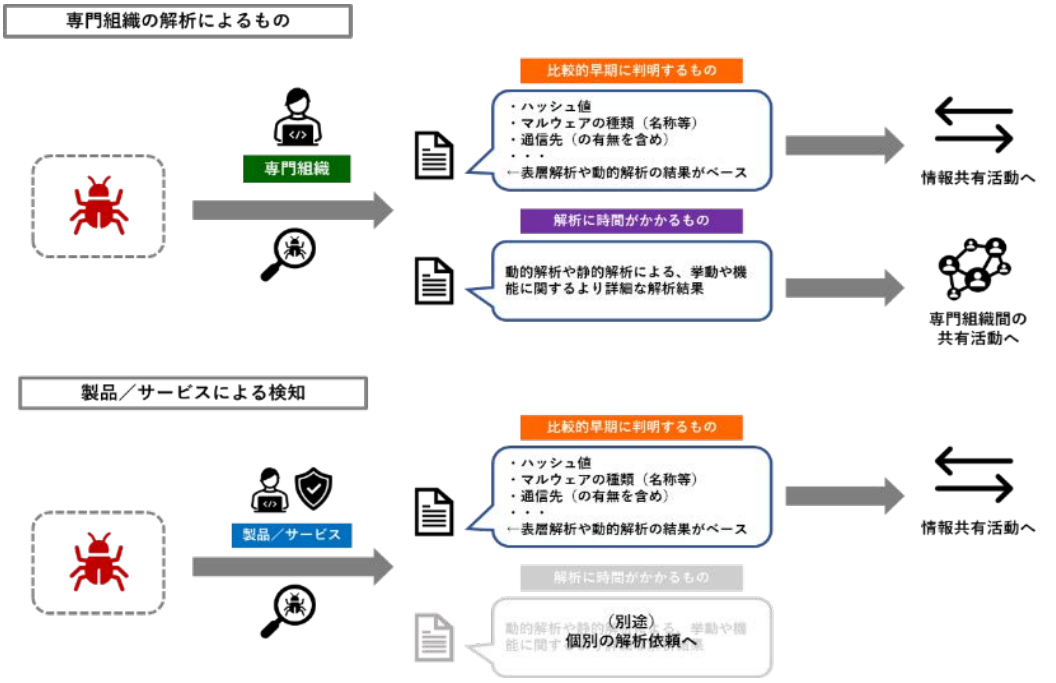


図 65

情報共有活動で流れる解析結果と専門組織が公表する解析結果は違うのか

下記の図 66 の左の図は、JPCERT/CC が 2021 年 9 月にブログで公開した、あるマルウェアに関する解析結果の一部で、攻撃者が当該マルウェアに指令するための各種コマンドを解説した箇所です。この情報を情報共有活動に参加する組織が入手したとしても、自組織における当該マルウェアの感染有無を調べることはできません。

感染有無を調べるためには、主に、マルウェアの通信先への通信が発生していないか、あるいは見つかった不審ファイルが当該マルウェアと一致するかなどの調査を行う必要があります。このブログの一番下には、「Appendix C：通信先情報」と示された箇所があり（下記の図 66 の右の図)、不正通信先のドメイン、IP アドレス、マルウェアのハッシュ値が記載されています。

これはあくまで、攻撃手法を分析したレポートの発信ですので、主に専門家コミュニティにおける情報共有目的で情報の開示が行われます。

より早期に行われる情報共有活動においては、記載される情報は少し異なります。実際に情報共有活動で共有される際には、Q12（65 頁）のとおり、通信先ドメイン、IP アドレスのほか、調査に必要な情報として、攻撃時期（≒ログを調査すべき期間）や通信プロトコルなどの情報が追加されます。

（左）詳細な解析結果

命令によって実行されるコマンド

Gh0stTimesは、大きく5つのコマンド群が実装されています。次が実装されているコマンドグループ名です。

- FileManager（コマンド番号0x1）：ファイル操作関連のコマンド
- ShellManager（コマンド番号0x28）：リモートシェル実行
- PortmapManager（コマンド番号0x32）：C2サーバーリダイレクト機能
- UltraPortmapManager（コマンド番号0x3F）：プロキシ機能実行
- 名前なし（コマンド番号0）：通信終了

```
__int64 __fastcall CKernelManager::OnDecrypt(CKernelManager *a1, unsigned __int8 *a2)
{
  __int64 result; // rax

  result = *a2;
  switch ( *a2 )
  {
    case 0u:
      _InterlockedExchange(&a1->IsActived, 1);
      return result;
    case 1u:
      result = MyCreateThread(0164, 0164, Loop_FileManager, a1->lp_this->c2_socket, 0, 0164, 0);
      goto LABEL_4;
    case 0x28u:
      result = MyCreateThread(0164, 0164, Loop_ShellManager, a1->lp_this->c2_socket, 0, 0164, 1);
      goto LABEL_4;
    case 0x2Au:
      return CreateEventA(0164, 1, 0, &a1->EventName);
    case 0x32u:
      result = MyCreateThread(0164, 0164, Loop_PortmapManager, a1->lp_this->c2_socket, 0, 0164, 1);
      goto LABEL_4;
    case 0x3Fu:
      result = MyCreateThread(0164, 0164, Loop_UltraPortmapManager, a1->lp_this->c2_socket, 0, 0164, 1);
LABEL_4:
      a1->thread_list[a1->num_threads++] = result;
      break;
    default:
      return result;
  }
  return result;
}
```

図9：コマンド一覧

（右）通信先やマルウェアのハッシュ値

Appendix C：通信先

- tftpupdate.ftpserver.biz
- 108.61.163.36
- update.centosupdates.com
- 107.191.61.40
- osscach2023.hicloud.tw
- 103.85.24.122
- 106.186.121.154

Appendix D：マルウェアのハッシュ値

- 01581f0b1818db4f2cdd9542fd8d663896dc043efb6a80a92aadfac59ddb7684
- 18a696b09d0b7e41ad8ab6a05b84a3022f427382290ce58f079dec7b07e86165
- 15b8dddbfa37317ccdfbc340764cd0f43b1fb8915b1817b5666c4816ccb98e7c
- 849ec6055f0c18eff76170912d8500d3da7be1435a9117d67f2134138c7e70c3
- f19ab3fcbc555a059d953196b6d1b04818a59e2dc5075cf1357cee84c9d6260b
- 836b873ab9807fbdd8855d960250084c89af0c4a6ecb75991542a7deb60bd119
- a69a2b2a6f5a68c466880f4c634bad137cb9ae39c2c3e30c0bc44c2f07a01e8a
- bd02ca03355e0ee423ba0e31384d21b4afbd8973dc888480bd4376310fe6af71

図 66

Q27.不正通信先に関する情報とはどういうものですか？

情報共有活動で共有される不正通信先に関する情報は基本的に

・IP アドレス
・ドメイン名
・通信の発生時期／期間
・通信のプロトコル等（例：HTTP, 80/TCP）

となります。

攻撃者が使う不正な通信元は以下の図 67 のようなケースが多く、特に、レンタルサーバやプロキシサービスを使う場合、正規の利用者と同じ通信元 IP アドレス／ドメインから接続してきたように見えるため、不正な通信を特定するための他の要素、通信の発生時期、プロトコルなどの情報がセットで必要になります。

また、正規サイトを改ざんして踏み台として使う場合でも、改ざんされている期間を示す情報とセットで共有されることで、攻撃による通信なのか、正規のサイト閲覧なのか区別することができます。

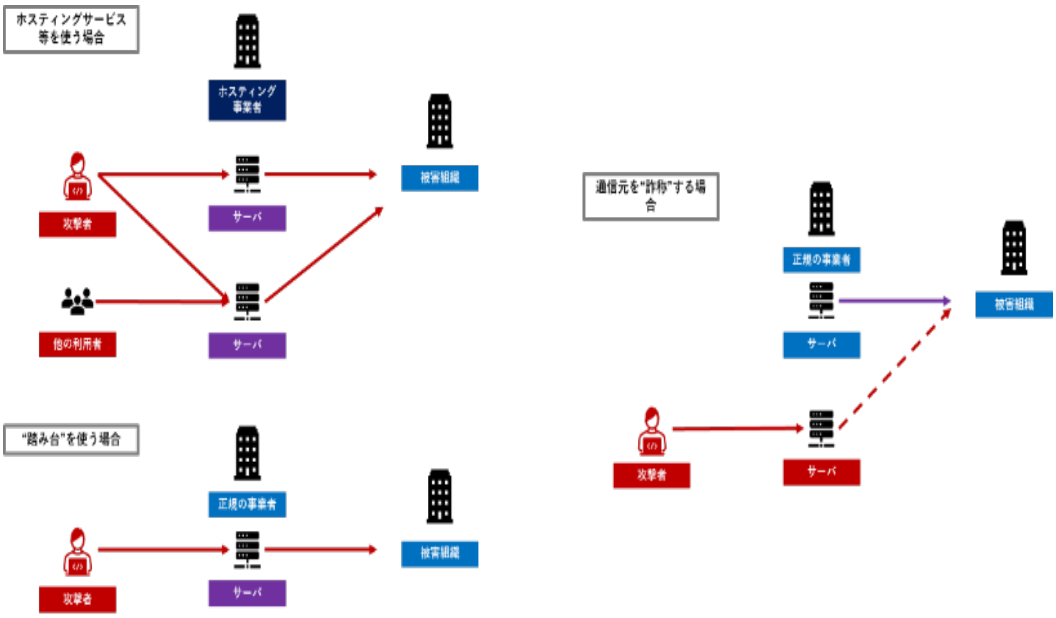


図 67

どのような攻撃類型の通信先情報を共有するべきか

Q10（62 頁）で述べたとおり、あらゆる攻撃類型に関する攻撃技術情報を情報共有活動に展開すれば効果があるわけではありません。当然ながら、セキュリティベンダ等が提供する製品／サービスを通じて攻撃を防ぐことができれば、あらゆる情報を共有活動上で流通させる必要はありません。

また、共有のための「対応コスト」の負担が大きいものや、「共有活動参加組織内では該当しない」見込みが高い攻撃については、共有活動全体で共有効果を得られない／参加者が実感できない、という点からも配慮が必要です。

例えば、下記図 68 の上段のような、プロキシサービス経由でのアクセスを行う攻撃は、通信元を特定／遮断されないように、アクセス毎／標的毎で出口の IP アドレスを変える場合があるため、同じ通信元からアクセスを受けた組織が特定の情報共有活動内に存在する可能性が低くなります。

さらに、同図の中段のような、ボットネットなどの大規模なインフラからアクセスを行う場合は、大量の「不正アクセス元情報」が出現し、また、時間の経過とともに増減するため、大量の情報を何度も流通させる必要が出てきます。

これらの類型における情報共有活動がまったく効果がない、とは言えませんが、製品／サービス上で対策方法が提供される可能性を加味して、取り扱い可否を判断する必要があると言えます。

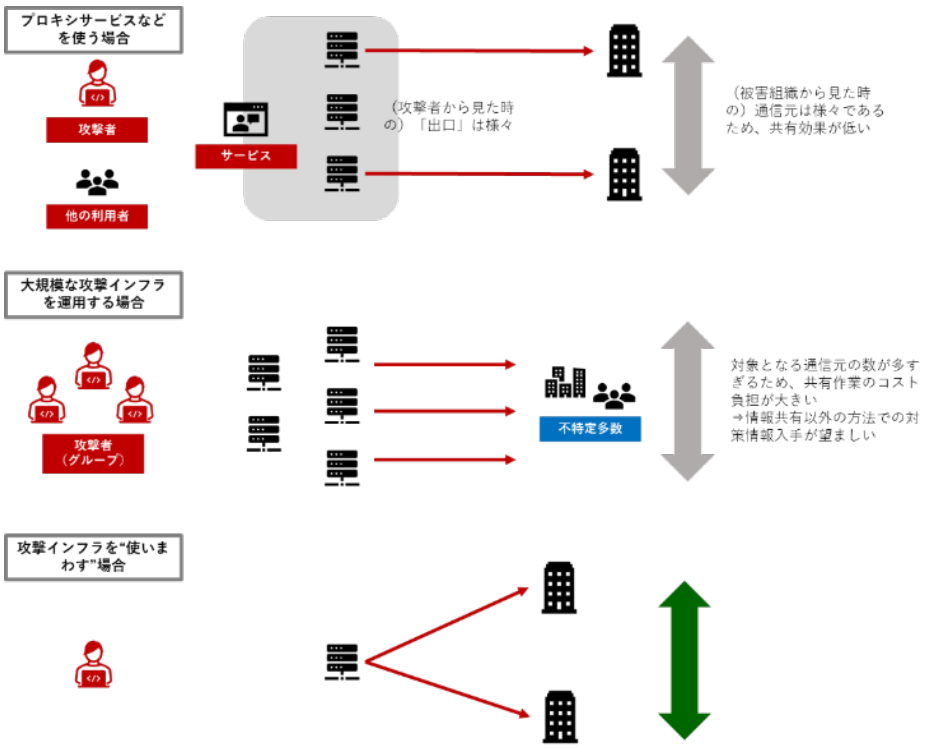


図 68

Q28. 攻撃の手口に関する情報（TTP 情報）とはどういうものですか？

情報共有活動で共有される攻撃の手口に関する情報（TTP 情報）は基本的に

・初期侵入／感染経路
・悪用される脆弱性
・侵入／感染後の動き
・攻撃目的／想定される被害

となります。

以下は、JPCERT/CC が過去に情報共有活動に展開した情報のイメージです。

（省略）

１）攻撃の概要

JPCERT/CC では○○○社の SSL-VPN 製品の脆弱性を悪用し、SSL-VPN のユーザーアカウント情報を窃取した後、ネットワーク内部に侵入する攻撃を国内で複数確認しています。

初期侵入経路／方法

２）攻撃が行われた期間

202x 年 x 月以降

３）攻撃の特徴

次のようなログが出力されるケースを確認しています

（省略）

４）攻撃に使用された通信元

現時点までに確認された IP アドレスと確認された時期を記載します。

123.***.***.***198.51.100[.]***　x 月 x 日

213.***.***.***203.0.113[.]***　x 月 y 日

通信元／時期
※Q6（47 頁）参照

５）悪用された可能性がある脆弱性

CVE-202x-******

○対象製品：＊＊＊シリーズの Ver.1.1.1 以前

○ベンダからのリリース：(省略)

悪用される脆弱性

図 69

TTP 情報はどこまで共有すべきか

以下は、インシデント調査により判明した攻撃の流れのイメージを示したものです。この場合、インディケータ情報としては、不正接続先①～③に関する情報やマルウェアX、Y に関する情報が情報共有活動で流れることがまず想定されます。

例えば、マルウェアは見つからなかったが、不正通信先②の「IP アドレス」への通信だけ発見した場合を想定します。この組織ではプロキシサーバがなくファイアウォールのみ運用しているため、通信ログ上には IP アドレスしか記録されません。不正通信先②はレンタルサーバであるため、IP アドレスは他の正規ドメインと共有になっています。

攻撃有無の判定をするためには、「まず不正通信先①への通信とファイル B のダウンロードがなければ、不正通信先②へのアクセスは発生しない」という情報が必要になります。不正通信先①へのアクセスは確認されておらず、また、ファイルBが保存される場所にも不審ファイルが見つからなければ、攻撃は行われていないと判断できます。このように、通信先やマルウェア情報以外の細かな攻撃技術情報のうち、調査や被害判定に必要な情報は共有が望まれます。

他方で、マルウェアXの構造やコマンドの詳細、不正通信先③にアクセスする際の詳細な暗号化方法といった、静的解析等で判明する情報は、基本的には情報共有活動を通じた侵害有無の調査にはあまり必要とはされません。こうした詳細情報が判明するには相当の時間を要しますので、こうした調査結果を待たずとも判明する TTP 情報の一部はインディケータ情報とともに早期に共有されることが望まれます。

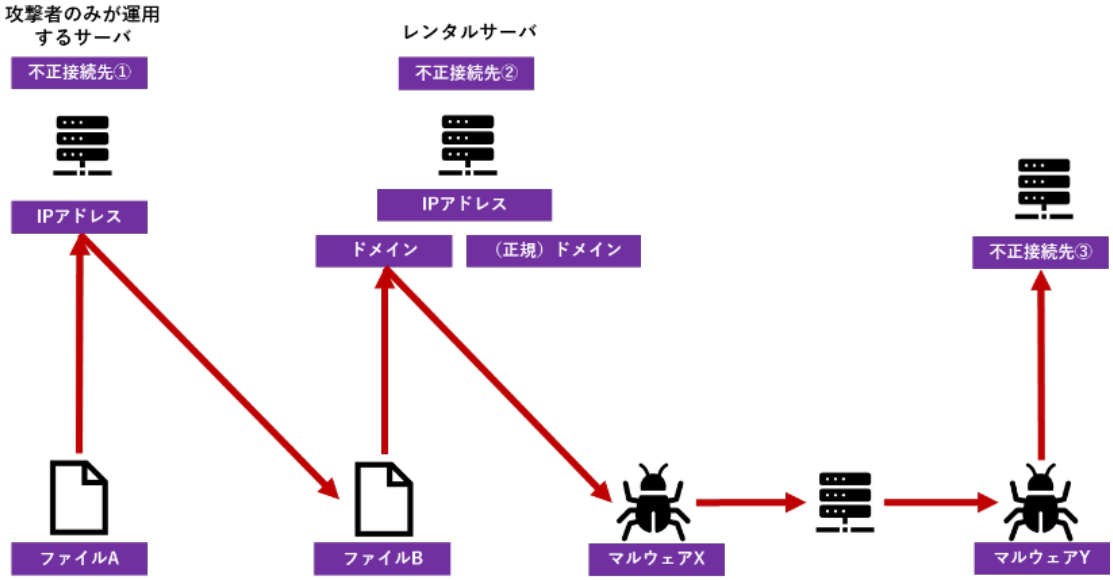


図 70

Q29.専門組織から「見つかった情報を共有活動に展開してよいか？」と尋ねられたらどう判断すればいいですか？

Q1（33 頁）のとおり、情報共有は「他組織の被害予防／早期発見のため」といった他者の利益のためという側面だけでなく、「まだ見つけられていない攻撃に関する情報を入手するため」という、自組織の原因究明・再発防止のために必要な行動という側面もあります。

特に、専門組織からこうした相談がある場合、特に後者の目的として提案されることが多いと考えられますので、情報共有に向けた積極的な対応が望ましいです。

なお、判断にあたって検討が必要なポイントとしては、

① 匿名での提供とするか、自組織名を加えて提供するか
② どのような情報を提供するか
③ 提供範囲（情報共有先）をどこまでに定めるか

といった点が挙げられます。②については、情報の種類によって共有効果が異なりますので、Q26（102 頁）、Q27（104 頁）、Q28（106 頁）をご参照ください。③については後述の Q30（109 頁）をご参考ください。

①についてですが、情報共有活動のうち、専門組織を介した情報共有は匿名にて情報が取り扱われることが多いですが、「自組織が情報共有をした、という事実を特定多数の関係者に知らせる必要性がある／知らせたいという目的がある」場合や、「いずれ公表される情報から、当該情報提供が自組織であることが容易に判明すると想定される」といった特殊なケースでは、あらかじめ自組織名を明記して情報提供／共有する選択肢も存在します。いずれにせよ、特殊なケースになりますので、仲介する専門組織への相談を行ってください。

Q30. 情報共有先をどのように指定／制限すればいいですか？

情報共有活動により様々ですが、一般的には TLP：TRAFFIC LIGHT PROTOCOL が用いられます。それぞれ提供／共有したい情報の必要な箇所（全体や一部指定など）に対して、下記のいずれかの指定を表示して、取り扱い可能範囲を示します。実際に情報共有活動内で展開されている情報にどのように付記されているかは Q7（51 頁）の例示をご参考ください。

TRAFFIC LIGHT PROTOCOL (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0 日本語版 から引用

a. **TLP:RED** = 受信者個人の目と耳に向けた共有に限られ、その先の公開はない。対象となる情報は関係組織のプライバシー、評判、または業務に重大なリスクを生み、第三者の手に渡ることで効果的に作用しない場合には、情報の発信者は TLP:RED を使用してよい。そのため、情報の受信者は、TLP:RED 情報を他の誰にも共有してはならない。例えば会議を想定すると、TLP:RED 情報は、その会議に出席した者に限られる。

b. **TLP:AMBER** = 限定公開、情報の受信者は Need to know の原則に基づき、組織内やそのクライアントにのみ共有できる。**TLP:AMBER+STRICT** は、ある組織のみに共有を限定する。対象となる情報は第三者の手に渡り効果的に作用することが求められるが、同時に関係組織外に共有されるとプライバシー、評判、または業務に対するリスクが生じる場合には、情報の発信者は TLP:AMBER を使用してよい。情報の受信者は、自組織とその組織のクライアントを保護し、更なる被害を防ぐためなら、Need to know の原則に基づき、自組織の構成員とその組織のクライアントに TLP:AMBER 情報を共有してもよい。備考：情報の発信者が共有範囲を一組織**のみ**に限定したいのであれば、TLP:AMBER+STRICT を指定しなければならない。

c. **TLP:GREEN** = 限定公開、情報の受信者はコミュニティ内に情報を共有できる。対象となる情報が、より広いコミュニティで認知度が上がることが有用な場合には、情報の発信者は TLP:GREEN を使用してよい。情報の受信者は、コミュニティ内の仲間とパートナー組織に TLP:GREEN 情報を共有してもよいが、公にアクセス可能な手段を介してはならない。TLP:GREEN 情報は、コミュニティ外には共有してはならない。備考：「コミュニティ」が定義されていない場合は、サイバーセキュリティや防衛のコミュニティを指すと想定すること。

d. **TLP:CLEAR** = 情報の受信者は、全世界に向けて情報を共有できる。公開に制限はない。情報の発信者は、対象となる情報が誤用されるリスクが最小限または想定されない場合に、一般公開に適用される規定と手順に従って TLP:CLEAR を使用してよい。標準的な著作権保護の規定に則り、TLP:CLEAR 情報は制限なく共有してよい。

図 71

また、情報共有活動によっては、活動独自の取扱い指定ルールを設けていたり、上記の TLP に別の指定方法を追加して運用していたりするものもあります。例えば、サイバーセキュリティ協議会では、TLP に加えて、「秘密指定」を設けており、共有範囲指定だけでなく、秘密指定された情報を取扱うことができる者（取扱従事者）の指定も追加することが可能としています。

共有できる相手先が指定された情報の取扱いについて

例えば、Q7（51 頁）で示した、JPCERT/CC が早期警戒情報として共有しているインディケータ情報（サンプル）では、TLP:AMBER と表記してあります。この場合、情報を受信したユーザー組織は、ログの確認等の作業を外注している場合、運用保守先のベンダ等に当該情報を渡して調査作業をしたり、グループ企業の場合はグループ内の各企業に渡して調査したりすることが可能です。ただし、これらの行為はすべて、「自組織を保護するため」に用いることが前提であり、受信した情報を自社やグループ会社が営利目的等で第三者に提供しているサービスに使うことは基本的にできません。

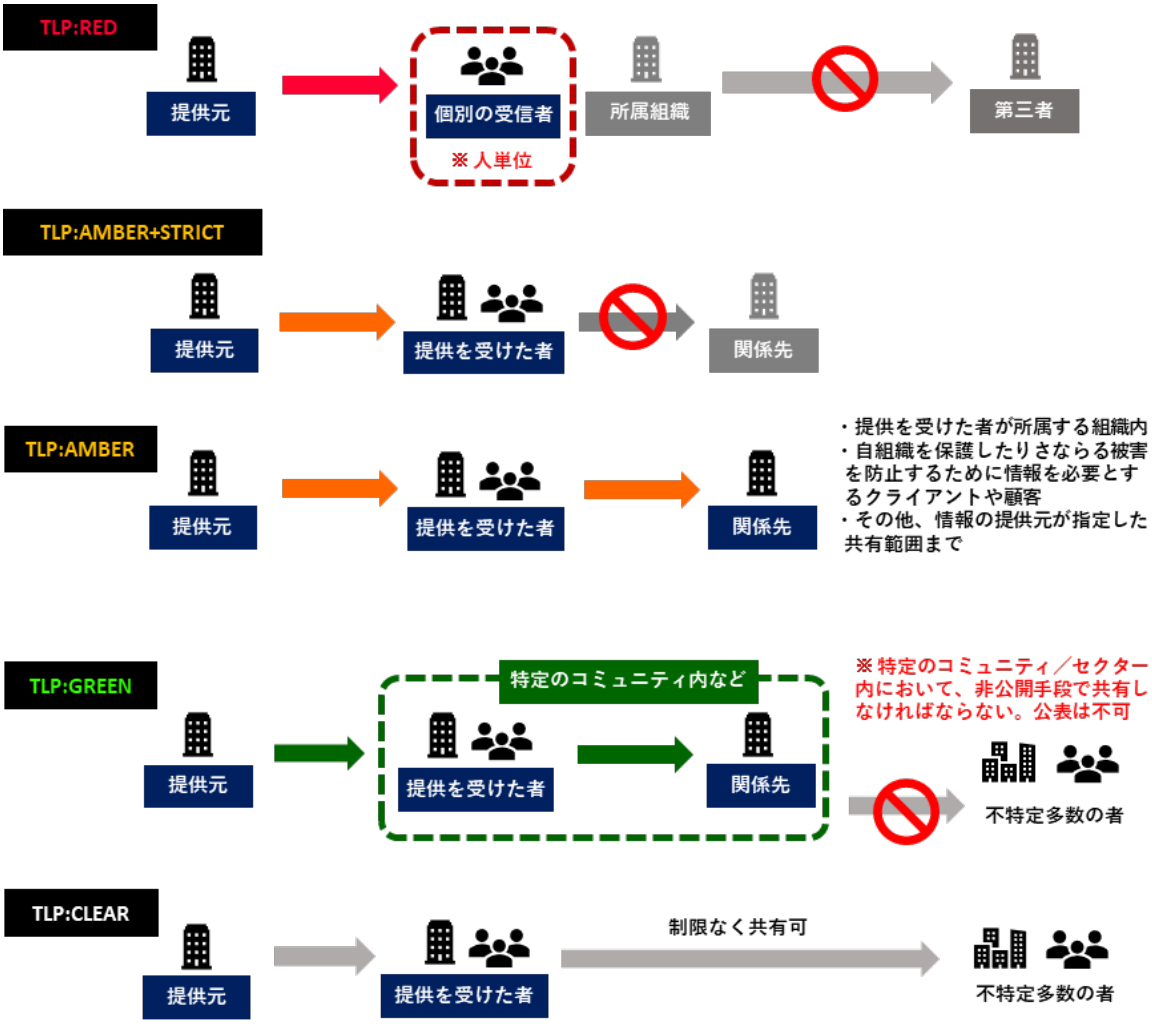


図 72

Q31. 専門組織から「分析結果をレポートとして発信してもよいか」と尋ねられたらどう判断すればいいですか？

Q2（36 頁）、Q12（65 頁）で述べたとおり、専門組織が対応した攻撃の分析結果をレポートとして発信することは

・（攻撃範囲が広く、また、攻撃キャンペーン中～直後であれば）被害拡大防止や、被害の早期発見のための注意喚起としての効果
・（上記のように広範囲／攻撃活動中でなくても）新たな攻撃手法の手の内を“晒す”ことにより、脅威として“陳腐化”させる効果
・中長期的に広く脅威に関する情報を周知する効果

を有しており、積極的な協力が望まれます。

専門組織がレポートとして発信する場合、個別の被害組織名などが容易に特定されてしまうような情報は記載せず、匿名化して事案の詳細などが記載されます。

当該専門組織が、同じ攻撃キャンペーンによる複数の被害を把握していた場合、特定の業種／分野、被害組織の規模感などを示すことがあります。こうした情報があることで、同業他社への注意喚起としての効果が見込まれたり、今後の攻撃傾向について推測／警戒することにも活用したりすることができます。個別の被害組織名が特定されない範囲で、こうした業種などの情報もレポートへの記載を許可することが望まれます。

後半の解説のとおり、専門組織からレポートとして個別事案に関する攻撃技術情報が広く公表されることによって、専門組織間の知見のばらつきを調整する効果があるだけでなく、様々なセキュリティ対策製品／サービスの向上にもつながり、こうしたサイクルが中長期的に継続することは、ひいては、自組織で使用するセキュリティ対策の強化につながるものとなります。

レポート発信の重要性

前述のような分析レポートは専門組織、主に民間のセキュリティベンダから多く公表されています。企業あるいはアナリストとしての分析能力や製品・サービスの優れた点をアピールする目的は当然ながら、分析知見を広く知らせる効果を有しています。レポート発信以外にも、国内外で開催されている各種カンファレンスにおけるアナリストによる発表も、もちろんアナリスト個人の能力を示すためのものであり、かつ知見を広く知らせる効果を有しています。

複数の攻撃者によって広く行われる攻撃方法は、多くの組織、製品、サービスで観測されるため、検知や予防のための情報も速やかに広範囲に知られることになります。他方で、標的型サイバー攻撃のような、限定的な被害組織・分野でしか観測されない攻撃については、当該被害組織のインシデント対応にあたった専門組織など、限定的な組織でしか知見が蓄積されません。

レポート発信やカンファレンスでの発表を通じてこうした知見が広く知られることで、市場全体における知見の偏りによる、社会全体での対策能力の著しい不均一が調整されるようになっているとも言えます。

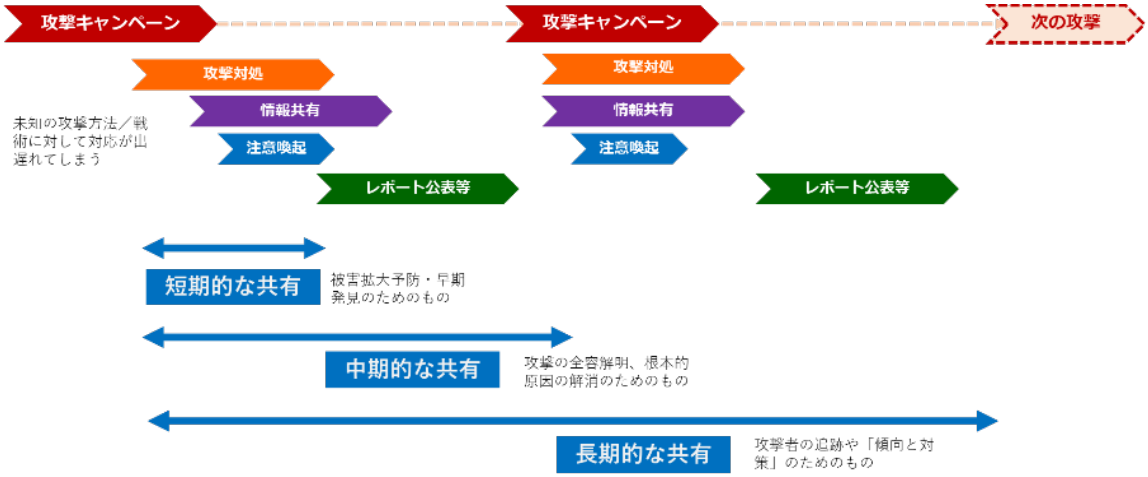


図 73

Q32. どのような攻撃技術情報であれば速やかに共有することができますか？（公開情報と非公開情報の違いについて）（※調査ベンダ向け解説）

後述の Q33（119 頁）のとおり、攻撃技術情報の大半は公知の情報として存在しているか、同じ情報を既に別の専門組織が入手している場合が想定されます。

しかしながら、Q1（33 頁）の解説のとおり、自らの調査により攻撃の全容を解明していて、インシデント対応に十分な攻撃技術情報を把握できているかお互いに知ることができないため、積極的な情報共有による情報の入手が望まれます。Q33（119 頁）のとおり、NDA の秘密情報の対象外である、既に公知の情報となっている攻撃技術情報は、積極的に共有を行い、また、公知の情報ではないが、既に他の専門組織が把握している情報を得るために情報共有活動への働きかけが求められます。

＜マルウェアについて＞

インシデント対応を行うにあたり被害組織との間に NDA 契約を結ぶ場合、被害組織で発見したマルウェアに関する情報も秘密情報に含まれてしまう可能性があるため、情報共有活動に提供する場合、被害組織に個別に了承を取るプロセスを経たり、あるいはそもそも NDA との関係で外部提供自体を行わないと判断されたりするケースがあります（守秘義務契約と攻撃技術情報との関係については、Q33（119 頁）参照）

他方で、情報共有効果が見込まれる攻撃（Q6（47 頁）参照）において、マルウェアや攻撃インフラは複数の標的に対して“使いまわし”されているため、対応している被害現場で見つかった検体と同じ検体や類似検体、同じ通信先に関する情報が、国内外の他の（セキュリティ）ベンダや専門機関からの情報として公開される場合があります。

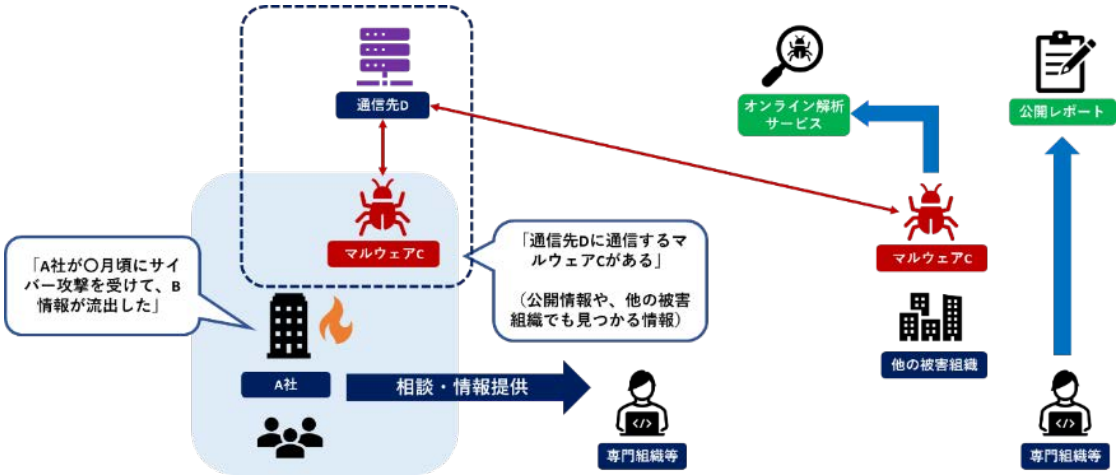


図 74

近年ではアンチウィルス製品による検知を回避するため、ファイルを被害端末に保存しないファイルレス化や正規の機能（Windows API など）を呼び出すことを多用し、また、モジュール化と呼ばれるような、機能毎のプログラムを追加するなどの傾向が見られます。そのため、各マルウェアの機能毎のプログラムはある程度同じハッシュ値のものが複数の被害現場で見つかるため、各被害組織に固有のマルウェアが見つかるものはなくなってきています。また、各マルウェアやモジュールは C2 サーバ上に蔵置されていることが多く、既に公開情報として不特定多数の者が観測可能な状態にあります。

したがって、基本的には、「被害現場で見つかるマルウェアは必ずしも被害組織や調査したベンダのみが知る情報ではない」という前提で対応を進める必要があるといえます。

観点：「他の標的組織に向けても使われている可能性」

被害現場では、ドロッパーやダウンローダー、ペイロードなど様々なフェーズで用いられるマルウェアが見つかります。このうちのいくつかは、他の攻撃でも同一ハッシュ値のものが使用される場合があるため、断片的に発見されているマルウェアであっても、攻撃を検出するために共有することが有効です（Q7（51 頁）を参照）。理屈上、分析の過程において、個別被害組織に対してのみ投入されるマルウェアではないかどうかを確認し、他の標的組織における攻撃にも汎用的に使われている可能性があれば、積極的に情報共有することが望まれるわけですが、「１．はじめに なぜ「情報共有を行うべき」なのか」（13 頁）で解説のとおり、他の標的組織でどのような情報が見つかっているのか事前に把握することは困難です。「鶏が先か、卵が先か」論になりますが、被害現場で見つけた情報が情報共有に有効な情報が知るためにも、早期に情報共有を行わなければならない、ということになります。

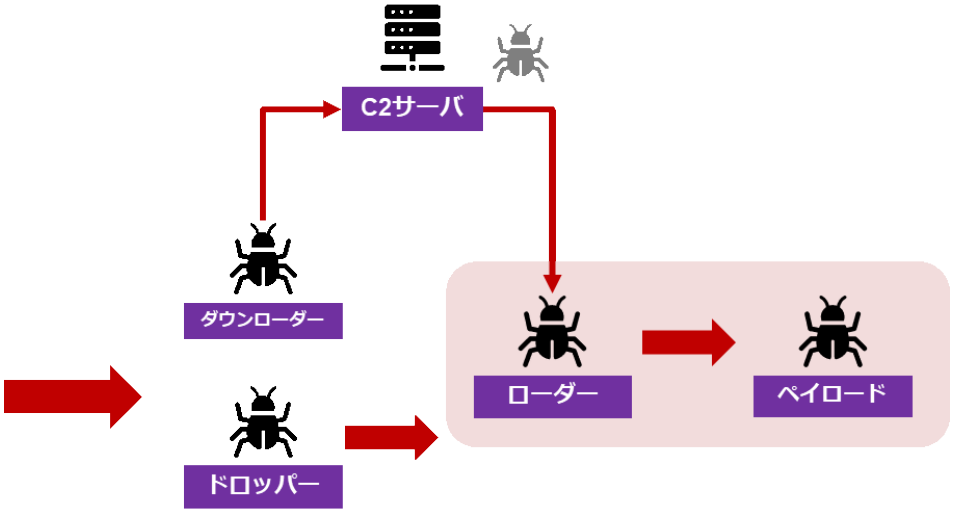


図 75

観点：「公開されていないもの」

現場で見つけた検体あるいは類似検体が公開情報として確認可能かどうかのチェックも必要です。Virustotal 等の公開系解析サービス上に同一検体や類似検体がある場合、その旨を共有するだけで、表層解析結果を伝えることが可能です。既に同一検体が公開情報として存在しているにも関わらず、TLP:RED などの指定をしてしまった場合、当該情報の活用可能範囲を無駄に制限してしまうおそれがあるため、公開情報の有無を確認することは必須です。

また、ペイロードが公開サーバ上に存在している場合、被害組織の特定に結び付かないのであれば（Q22（92 頁）参照)、公開情報として共有することが可能です。

観点：公開情報があるが、国内に向けた攻撃活動についてはいまだ公表されていないもの

海外のセキュリティベンダ／専門機関のレポート等で取り上げられた海外での被害現場において、自組織が国内被害組織で見つけた同一検体や類似検体が見つかっていた場合、「(海外で先に観測された当該攻撃活動が）国内に向き始めた」ことを示している可能性があります。こうした攻撃活動に関する IoC 情報などが公開情報として既に流通していても、未だ国内ベンダや国内の様々なセキュリティサービス／製品では当該攻撃に対応できていない可能性があるため、被害防止のためにも早期の情報共有が望ましいと考えられます。

＜通信先情報について＞

Q27（104 頁）のとおり、通信先情報は基本的に公開状態で存在する情報であるため、調査を行った者の判断で積極的に共有することが可能です。

他方で、通信先を第三者が調査することで匿名を希望している被害組織や被害を未公表の被害組織が特定されることは避ける必要があります。あまり事例としてはありませんが、例えば、不正通信先のサーバがオープンディレクトリになっており、被害組織から窃取した情報や、被害組織と通信した痕跡がわかるデータが見える場合が考えられます。

また、同様に、通信先が調査されることで、被害組織以外の第三者の未公表の被害が発覚する可能性がある場合も同様の配慮が必要です。

観点：「他の標的組織に向けても使われている可能性」

情報共有効果が見込まれる大半の攻撃では、攻撃インフラを使いまわしているため、不正な通信先情報を共有することで被害の未然防止効果などが見込めます。また、Q1（33 頁）で紹介のとおり、複数の通信先を用いる攻撃の場合、単独の被害調査によってその全容を把握することが困難であるため、情報共有により「まだ把握していない不正通信先情報」を入手することが望まれます。

他方、主に標的型サイバー攻撃で標的組織毎に異なった C2 サーバを使用する場合などは通信先情報を共有しても共有効果を得られないケースがあります。しかしながら、当該通信先がごく限定された標的組織のみに使用されているかどうかは単独の被害現場からの情報だけではわからないため、情報共有活動において、まずは、セキュリティベンダや専門機関に相談を行い、どの程度通信先が使いまわされているのか（共有効果の見込みがある情報なのか）照合することが望まれます。

観点：「公開されていないもの」

通信先情報もマルウェア情報と同じく、公開情報の存在有無の確認が必要になります。特に、Web サーバ等の脆弱性をインターネット越しに悪用するような攻撃の場合、通信先情報は膨大になる可能性があり、例えば調査目的のスキャン元の IP アドレスなどが混在するおそれがあります。こうした情報の大半は公開情報として既に周知されている場合があるため、共有活動への提供までに公開情報を“落とす”ことが必要になります。

通信先情報は調査の比較的初期の段階で見つかるものですが、被害組織先のインフラや発見の過程により、その精度がばらつくことがあります。実際には FQDN が割り当てられた通信先であるにも拘らず、被害組織においてプロキシサーバを運用していなかったり、マルウェアに内包された通信先を見つけたりするわけではなく、通信ログ分析から不審な通信先を見つけた場合などにおいては、FQDN ではなく、IP アドレスのみが判明するケース

が想定されます。その場合、情報共有活動に展開したとしても、他の被害を見つけるなどの情報共有効果（Q6（47 頁）参照）を十分に得られない可能性があります。このような場合には、IP アドレスのほかに、ポート番号や通信の特徴を示す情報（HTTP ヘッダの特徴的な文字列など）、通信日時／頻度などの情報とセットで提供することが望まれます。

また、仮に FQDN まで特定した通信先情報を展開できたとしても、情報共有活動を通じて当該情報を受信する組織においてプロキシサーバ等が運用されておらず、ファイアウォール上のログ（IP アドレスベース）のみでの調査が必要な場合をあらかじめ想定し、前述のような複数情報をセットにした展開の配慮が必要です。

観点：公開情報があるが、国内に向けた攻撃活動についてはいまだ公表されていないもの

前項と同様です。

＜その他 TTP に関する情報＞

情報共有活動で共有される攻撃技術情報の大半はインディケータ情報であるため、また、判明するまでに時間を要する TTP 情報の大半は情報共有活動で流れることがあまりなく、多くの場合、専門組織による分析レポートで発信されます（Q7（51 頁）参照）。

しかしながら、特定製品の脆弱性悪用が初期侵害経路であるケースや、その他攻撃被害の未然防止や早期発見に資する、特徴的な攻撃手法に関する情報を共有することが望まれるケースが多くあります。

観点：「他の標的組織に向けても使われている可能性」

例えば、標的型攻撃の一部やランサムウェア攻撃の一部では、商用 RAT（リモートアクセスツール）や正規ツールが侵害後の横展開等で多用されるケースがあり、アトリビューション妨害のために意図的に独自マルウェア／ツールの使用を避ける場合もあります。そのため、情報共有において、複数の事案が同一の攻撃活動によるものなのか識別するためには、マルウェアや攻撃インフラの共通性だけでなく、TTP 情報の比較も重要になります。

ただし、TTP 情報をトリガーとして侵害の有無を調べることは、一般的なユーザー組織では難しく、基本的には専門組織同士が対応している被害事案の比較に使うことが想定されます。

観点：「公開されていないもの」

TTP 情報の要素の一つ一つは既に公開されているものであったとしても、組み合わせる

ことで、特定の攻撃活動や攻撃グループを限定できる場合があります。特定の攻撃活動／グループの TTP 情報が共有されることで、断片的にマルウェアやその通信先が発見されていたり、TTP 情報の一部しか判明していなかったりする被害現場において、未判明の侵害経路や侵害範囲を特定するヒントになる可能性があります。

観点：公開情報があるが、国内に向けた攻撃活動についてはいまだ公表されていないもの

前項と同様です。

Q33. どのような攻撃技術情報であれば守秘義務契約上の「秘密情報」にあたりませんか？（※調査ベンダ向け解説）

インシデント対応にあたる（セキュリティ）ベンダが現場で見つけた情報について、基本的には被害組織との間の秘密保持契約（NDA）における「秘密情報」として、その取扱いの制限を受けることが大半です。秘密情報の例外となる情報としては、

①受領当事者（セキュリティベンダ）が既に知っていた情報
②既に公知の情報
③受領当事者の責めに帰すべき事由によらずに公知となった情報
④第三者から受領当事者が秘密保持義務を負うことなく得た情報

が契約上示されることが多くあります。ただし、発見した攻撃技術情報が、②既に公知の情報なのか直ちに知ることができないケースがあります。同じ攻撃技術情報を特定多数の国内外の専門組織が発見しているのですが、④のような情報交換が行われていなかったり、公開レポートを通じて広く発信されていなかったりするケースです。したがって、②既に公知の情報かどうか、確認するためには、最低限、国内の専門機関や専門組織が集まる情報共有活動に照会をかける必要があります。いきなり、広く、多数の組織が受領する情報共有活動に展開するのではなく、まずは「公知の情報かどうか」知るための限定的な情報共有が行われる必要があることについては、被害組織とセキュリティ専門組織間で認識の共有があらかじめ行われていることが望ましく、例えば、NDA 契約に事前にそうした条項をいれておくことなどが考えられます。

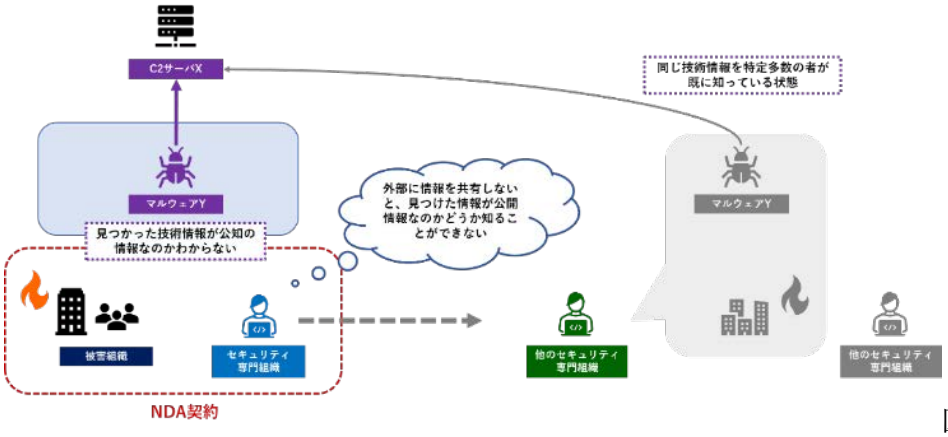


図 76

技術情報は公知の情報か

マルウェアやその通信先（ドメイン名や URL、IP アドレス）といった攻撃技術情報は、サイバー攻撃の特性（同じ攻撃手法を同時多発的に複数個所で使用できる）から、「ただ 1 か所の被害組織でしか見つからない」というケースは稀です。

前頁のとおり、インシデント対応初期の時点においては、「同じ攻撃技術情報は他所にはないのではないか？」と考える場合がありますが、解説のとおり、「『他所に同じ攻撃技術情報がある』ことを知ることができていないだけ」であるケースが大半です。また公開レポートが発信されていない段階においても、オンライン解析サービス上には同一の攻撃技術情報が既にアップロード／公開されているケースもあります。

通信先情報に限れば、そもそも攻撃者が使用するサーバはインターネット上で稼働していますので、誰もが知ることができる情報ですし、パッシブ DNS サービス上の情報を用いれば、過去にどのようなドメインがどの IP アドレスにどの期間紐づいていたのか知ることも可能です。したがって、攻撃技術情報は、当該時点では把握できていなくても、「基本的に公知の情報である可能性が極めて高い情報である」と解釈すること可能です。

ただし、「基本的に公知の情報である可能性が極めて高い情報である」ことをもってして、直ちにＮＤＡ上の秘密情報の適用外であると解釈することと、「秘密情報の適用外」であると解釈して契約の相手方（被害組織）に無断で情報を外部提供したり公表したりすることは別の問題です。前者は法的な問題としてクリアできたとしても、後者は、契約は別として互いの信頼関係の問題であり、Q22（92 頁）のように、稀に攻撃技術情報から被害組織が特定されてしまうケースが発生した場合、致命的な問題にもなりかねません。

前ページに記載のとおり、既に公知の情報であるか判然としない場合は、「公知の情報であるか確認するため」の限定的な情報共有／外部専門機関への照会等を行うよう、事前に被害組織との間で合意しておくなどの配慮が必要です。

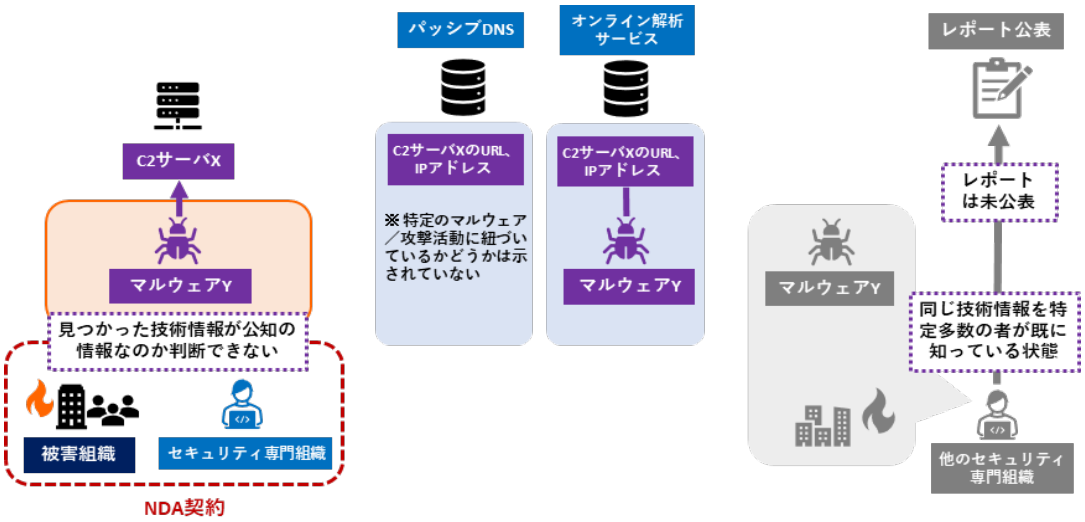


図 77

脆弱性の悪用に関する情報について

例えば、下記の図 78 のとおり、特定のソフトウェア製品Aの脆弱性が悪用されたサイバー攻撃被害現場において、「製品 A の脆弱性が悪用された」という情報を（セキュリティ）ベンダがどのように扱えるのが考えてみたいと思います。

既知の脆弱性悪用であった場合、「製品 A の脆弱性が悪用された」という情報は基本的に情報共有活動に提供することが可能です。ただし、その場合、

①技術的に誤りがないこと（製品 A の（既知の）脆弱性悪用ではないのに、調査不足や憶測でそのような情報を流すことを避けるべき）

②製品 A のメーカーに当該悪用事実が伝わること

への配慮が必要になります。製品 A の脆弱性情報は既に公表されていたとしても、これが実際に攻撃被害につながる悪用があったという事実は製品Aのメーカーにとってはネガティブな情報であり、また、追加の対応（修正プログラムの見直しやユーザーへの再通知など）が必要になる可能性があります。

他方で、未知の脆弱性が悪用されたで場合は、当該調査を行った（セキュリティ）ベンダは脆弱性の発見者として、脆弱性告示制度に基づく届出を行うことができます。この場合、発見者は、「正当な理由がない限り、第三者に脆弱性関連情報を開示しないこと」とされていますが、「正当な理由により開示するときは、あらかじめ受付機関に問い合わせること」とありますので、脆弱性情報の受付機関に問い合わせた上で、正当な理由が認められる範囲で情報共有活動に提供することは可能です。

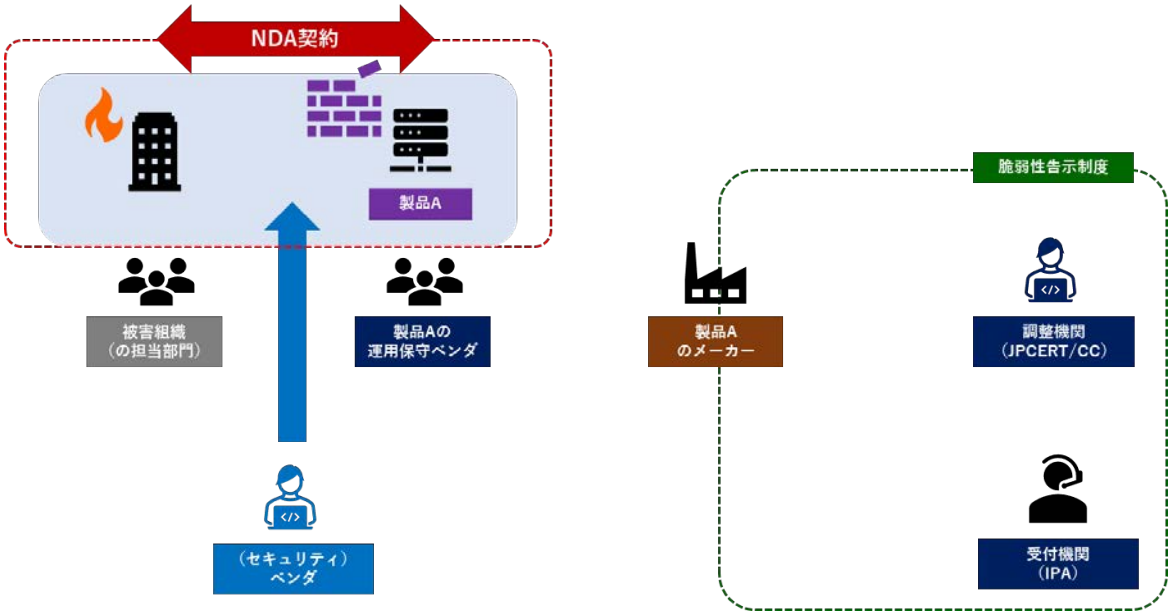


図 78

４．ケーススタディ

ケース１：標的型サイバー攻撃

【共有・公表のポイント】

・長期間潜伏し機微な情報の窃取を試みる標的型サイバー攻撃においては、不正な通信やマルウェアが検知されないように、攻撃者はセキュリティ製品／サービスへの回避策を講じます。同時期に他に標的となった組織や専門組織が何らかのきっかけで発見できた攻撃に関する情報を速やかに共有し、潜伏している攻撃者を見つけだすことが必要です。

・組織のネットワークが広範囲に侵害されていたり、また、攻撃者が痕跡を消去したりする場合もあるため、原因調査や被害範囲調査に相当の期間を要します。断片的であっても、また、情報のやりとりが複数回にわたりますが、判明した技術情報から順番に情報共有活動に提供し、こまめにフィードバックを受ける必要があります。

・長期間侵入されているケースが多い標的型サイバー攻撃においては、発覚時点で既に相当の期間が経過している場合があるので、速やかに情報共有しなければ、情報共有の相手方組織における過去の通信ログ等が保存期間を過ぎ、フィードバックを得られなくなります。前述のとおり、断片的あるいは未確定の情報であっても専門組織の精査を受けるなどして、早期に情報共有を行う必要があります。

・標的型サイバー攻撃においては、前述のとおり、調査に相当の期間を要することや、発覚時点で攻撃から既に相当の期間が経過しているケースが多いため、調査をすべて終えてから公表する場合、攻撃発生から公表まで長期間未公表だったことが批判される可能性もあります。公表時のこの期間中の取組みを可能な限り積極的に開示したり、あるいは複数回の公表にわけたり、または、社会的に影響の大きい深刻な被害が発覚した時点で第一報を行うなどの選択肢が考えられます。（Q17（76 頁）参照）

ケース１－１：初動フェーズ

図 79

状況：

・製品 A に関する注意喚起を受け、また、参加している情報共有活動（○○協議会）から共有された「製品 A の脆弱性を悪用する攻撃に関するインディケータ情報」にあっ

た「不正アクセス元」の IP アドレスからの通信有無を調査していたところ、自社で使用している製品 A サーバに対して不審なアクセスが行われていたことが発覚した。
・製品 A のサーバを調査したところ、不審なファイルが見つかった
・○県警察に通報するとともに、セキュリティベンダに調査を依頼したところ、マルウェア X であるとの速報結果を得られた

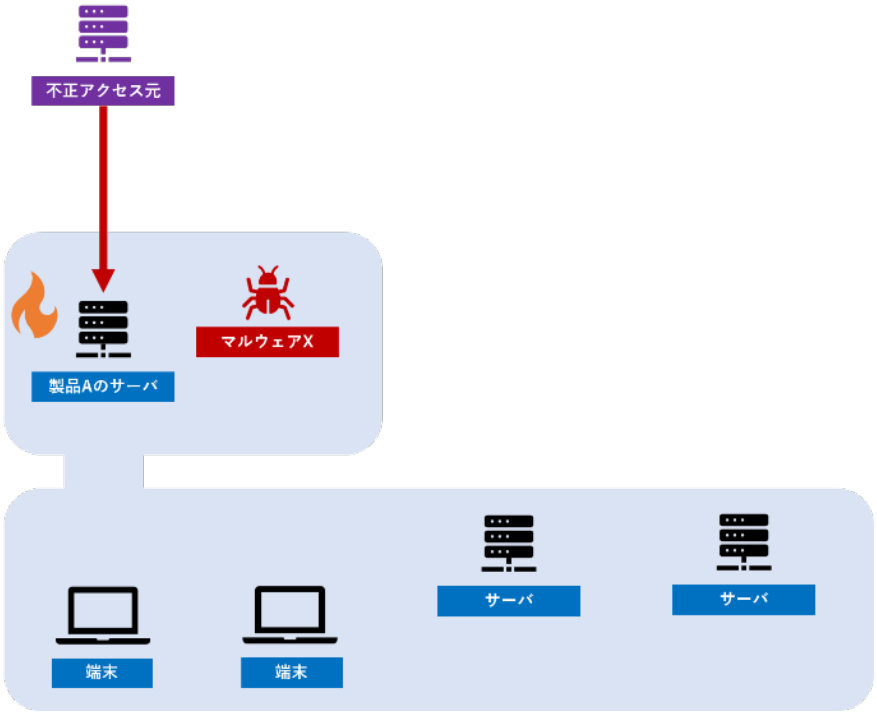


図 80

【ポイント解説】

・標的型サイバー攻撃の場合、攻撃者は製品／サービスによる監視／検知を回避しようとするため、外部から提供されたインディケータ情報によるログの調査にて発覚する場合が想定されます。

次に行った対応：

・○○協議会の窓口組織に以下の情報を提供し、情報共有によるフィードバックが欲しい旨を伝えた。

下記情報について、弊社名は 匿名 にて、TLP：AMBER にて、共有をお願いします。

＜概要＞
○月×日頃、製品 X のサーバに対して不正なアクセスが行われ、マルウェア X が設置されていたことが判明した。現在セキュリティベンダによる調査を開始しているが、どの程度侵害されたのか、マルウェア X 以外の感染有無等は現時点で不明。

対象のシステム：
製品 X が稼働する Windows サーバ。製品 X のバージョンは 1.2.x にて、○月△日に注意喚起があった脆弱性の影響を受けるバージョンであったことがわかっている。

不正アクセス元：
198.51.100[.]***　（○月×日 23:05～23:50 までに複数回アクセス）
その他の不正アクセス有無については現在調査中。

マルウェア：

ファイル名：
SHA256:
設置日時：○月×日 23:45
セキュリティベンダの速報的な解析結果ではマルウェア X ではないかとのことで、現在詳細を分析中。

ケース１－２：調査フェーズ

図 81

状況：

・○○協議会の窓口組織に情報を提供したところ、フィードバック情報として、自社が発見した不正アクセス元とは異なる IP アドレスからの不審なアクセスが他の被害組織に対して行われていたとの情報を得ることができた。この情報を元に調査したところ、マルウェア X のダウンロード元であることが判明した。

・また、マルウェア X について、マルウェア X が通信を行う C2 サーバに関する情報を得ることができ、通信ログを調査したところ、マルウェア X が別のサーバから発見された。

・セキュリティベンダからは、マルウェア X の挙動に関する詳細な解析結果が報告された。

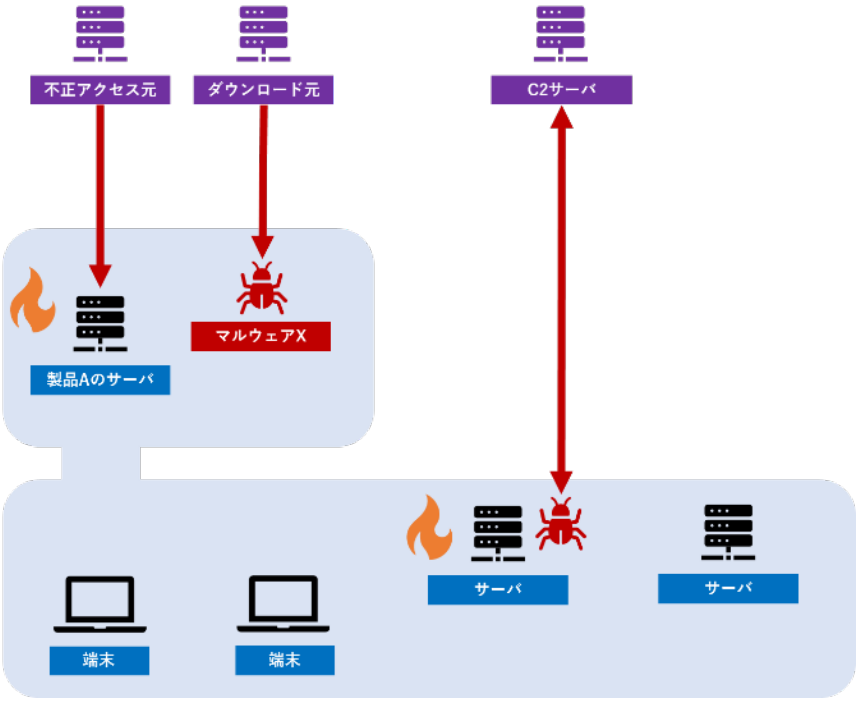


図 82

【ポイント解説】

・情報共有活動では、①早期に発見できた被害組織で見つかった情報を共有活動にインディケータ情報として展開、②受信組織で別の不正通信先情報を発見しフィードバック、③②の情報により被害が見つかった別の被害組織でさらに別の不正通信先が見つかる、というようなやりとりにより、攻撃者が使用している（使用していた）攻撃インフラの全容が徐々に判明していきます。

・標的型サイバー攻撃では一つの標的組織への攻撃に対して、複数の C2 サーバがマルウェア毎あるいは攻撃フェーズ別に使用されることから、情報共有活動を通じて、攻撃者が使っている（使っていた）攻撃インフラに関する情報をなるべく多く得ることが必要になります。

次に行った対応：

・侵害された「製品 A のサーバ」と「マルウェア X が見つかった別のサーバ」のフォレンジック調査を行い、製品 A のサーバからどのように社内に侵害が拡大したのか、他に侵害されたサーバ、端末がないか調査を進めた。

ケース１－３：報告／連絡フェーズ

図 83

状況：

・セキュリティベンダによる詳細な調査により、製品 A の脆弱性を突いて侵入した攻撃者がシステム管理用の端末を踏み台にして社内の他のサーバに侵害拡大していたことが判明した。
・機微な情報 B が保存されたサーバが侵害されており、ファイルを持ち出そうとした痕跡（ファイルの圧縮と外部に対して大きなサイズの通信）が見つかったが、持ち出そうとした圧縮ファイルや通信は暗号化されており内容を把握することはできなかった。
・〇〇協議会の窓口組織やセキュリティベンダからは、今回の攻撃はグループ Y という標的型攻撃グループが行った攻撃であるとの報告を受けているところ、同時期に海外において確認された、グループ Y の攻撃に関するレポートが発信されたとの連絡を受けた。

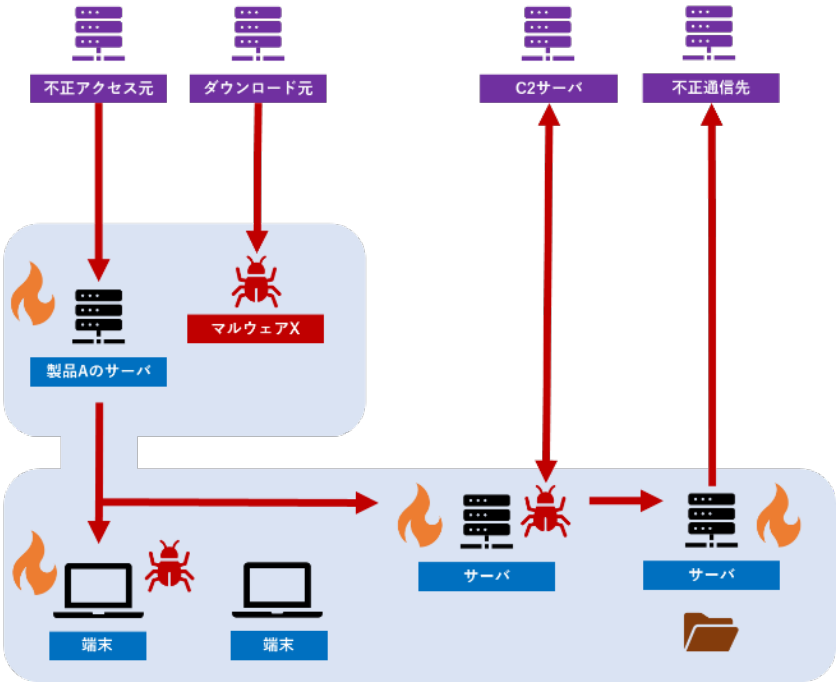


図 84

【ポイント解説】

・標的型サイバー攻撃では、攻撃発覚まで相当の期間を経ていることに対して、調査に必要な期間／種類のログが十分に確保できなかったり、攻撃インフラとの通信が暗号化されていたり、攻撃者が様々な活動痕跡を消去する場合などがあるため、窃取されたデータの特定については、調査自体が困難なケースが大半です。

・また、同時期に国内外で複数の被害組織がインシデント対応を行っていることが多く、自組織で外部への報告や公表を準備しているタイミングで、先行して他組織の被害公表や、セキュリティベンダからのレポートが発信される場合があります。攻撃被害について連絡をした相手方がそうした公開情報と照らし合わせて、連絡内容を解釈／評価する可能性も考慮しておく必要があります。

次に行った対応：

・機微な情報Ｂの取り扱いについて、所管省庁からＢ保護に関するガイドラインが示されており、漏洩被害があった場合について二次被害防止の観点等から所管省庁への報告のほか、公表を行うことが推奨されており、所管省庁への報告のほか公表に向けた準備を開始した。 ・専門機関やセキュリティベンダからのアドバイスとして、被害公表をした場合に、海外のセキュリティベンダが公表したグループＹの攻撃に関するレポートなどの情報から、公開情報の検索によって侵害原因が製品 A のサーバであることが容易に推測可能である旨が伝えられた。

ケース１－４：公表準備フェーズ

図 85

状況：

・以下の内容の公表文を用意し、社内各部門での調整のほか、セキュリティベンダや専門機関にも意見を求めた。
・また、公表を行う予定である旨を所管省庁に報告した。

・○月×日に製品 A の脆弱性を突いた不正アクセスを受けた。
・セキュリティベンダによる調査と並行し、○○協議会を通じた情報共有を行った。
・調査の結果、複数台のサーバが侵害を受け、このうち機微な情報 B が窃取された可能性が確認されたため、所管省庁への報告を行った。
・現時点で機微な情報 B の漏えいによると思われる関係先の二次被害は確認されていないが、引き続き注意を呼び掛けている。

【ポイント解説】

・標的型サイバー攻撃では、被害範囲の調査、被害内容の精査にかなりの期間を要する場合が多く、また、そもそも侵入されてから発覚までの間に相当の期間が経過している場合があるため、公表した際に「公表までの期間の長さ」に対して指摘がなされる場合があります。公表までの期間内にどのような調査や専門機関との連携、情報共有活動を行ったのか対外的に説明することも適切な評価を得るためのポイントとなります。

次に行った対応：

・セキュリティベンダや専門機関に対しては、攻撃の詳細をどこまで書くべきか、用いられたマルウェア名や攻撃グループ名、類似の攻撃に関するレポートが発信されていることに触れるか否かなどについて相談を行った。
・上記のような詳細を記載せず公表する場合、外部から同様の内容を指摘する問い合わせが来た場合にどのように回答するか想定問答等の準備を進めた。

ケース２：脆弱性等を突いた Web サーバへの不正アクセス

【共有・公表のポイント】

・下記に紹介する情報漏えいの可能性がある不正アクセス事案や Web サイト改ざんによるマルウェア設置の事案などの場合、「いつからいつまでの間、侵害されていたのか」速やかに特定し、影響を受ける範囲（情報の種類、件数、影響ユーザー数など）を調査し、二次被害防止のための通知・公表を行う必要があります。

・脆弱性が悪用されている場合、脆弱なままであった期間の特定、「当該脆弱性を悪用されると、どの箇所をどこまで侵害される可能性があるのか」といった情報や不正アクセス元に関する情報を専門組織や情報共有活動から得ることで、「いつからいつまで侵害されたのか／侵害されていた可能性があるのか」推測することができ、ある程度調査範囲を絞り込むことができます。

ケース２－１：発覚～初動対応フェーズ①

図 86

状況：

・外部から「御社が管理しているとみられる情報が外部に漏えいしているのではないか」という指摘を受け、当該情報を扱っていたシステムを調査したところ、不審な操作の痕跡が見つかった。

・運用保守ベンダに調査を依頼したところ、外部のユーザーが利用する Web サーバに不審なファイルが見つかった。

・当該システムについては直ちに運用を停止し、緊急のメンテナンスを行う旨の告知を行った。

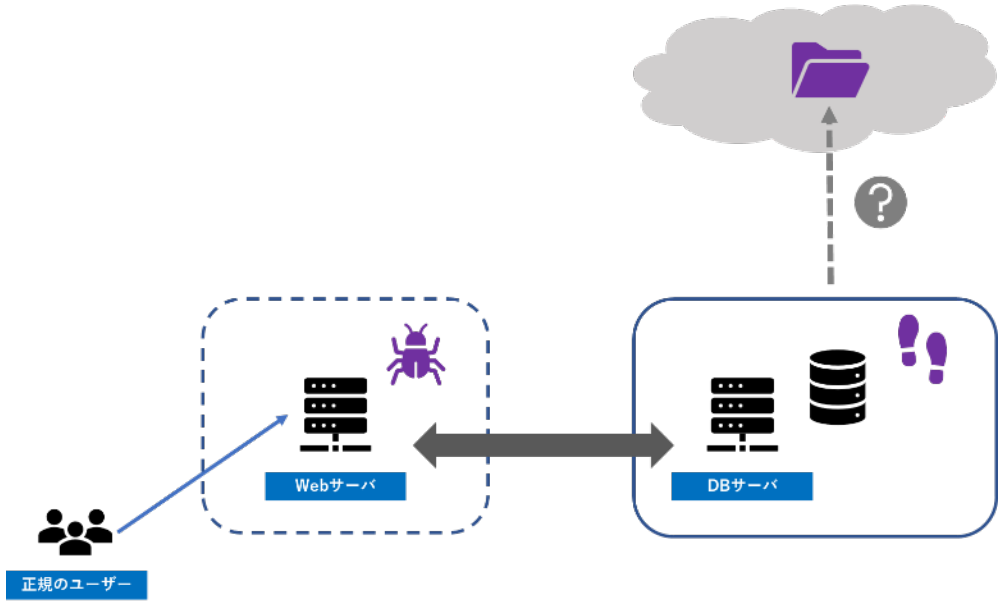


図 87

【ポイント解説】

・調査をしてみなければ確定できませんが、既に漏えいした情報が広く拡散している可能性があり、不特定の者が未公表の被害事実を既に知っている可能性があります（Q21（89 頁）参照）

・外部からの指摘について、漏えいしたと思われるデータが保全されており、これが提供された場合や、情報源の信頼性などから、本来外部には出ることがないはずのデータが漏えいしている蓋然性が極めて高い状況であれば、調査を待たず、対外サービスの緊急メンテナンス告知と同時に、第一報として不正アクセス疑義の調査を開始した旨を公表する選択肢もあります。

次に行った対応：

・〇〇協議会の窓口組織に以下の情報を提供し、情報共有によるフィードバックが欲しい旨を伝えた。また、〇県警察に被害に関する相談を行った

図 88

下記情報について、弊社名は 匿名 にて、TLP：AMBER にて、共有をお願いします

＜概要＞
○月×日頃、外部から「御社の情報が漏えいしている」と指摘があり調べたところ、○月□日頃に、△△△サービスのデータベースサーバに不審な操作の痕跡が見つかり、また、Web サーバ上に不審なファイルが見つかった。侵害原因については現時点で不明であり、運用保守ベンダで調査を進めている。

対象のシステム：
製品Ｙが稼働するサーバ。製品 Y のバージョンは 2.1.x にて、△月×日に注意喚起があった脆弱性の影響を受けるバージョンであったことがわかっている

不正アクセス元：
現時点で見つからず

Web サーバに設置されていた不審なファイル：
ファイル名：～
SHA256:～
設置日時：○月△日 01:30
セキュリティベンダの速報的な解析結果では Webshell ではないかとのことで、現在詳細を分析中。

ケース２－２：初動対応フェーズ②

図 89

状況：

・情報共有活動の窓口（専門組織）から回答があり、以下の不正な通信がないがログを調査するよう案内があった。

TLP:AMBER（※運用保守ベンダまで共有可）

直近において、以下のような攻撃が国内で観測されていますので、下記情報を参考に当該 Web サーバのアクセスログや操作ログについて調査を行ってください。

＜概要＞
○月○日頃から、国内の Y 製品が稼働する Web サーバに対して XXX の脆弱性(CVE-2022-*****）を悪用した不正アクセスが観測されています。下記情報を元に、不審なアクセスがないか調査と対処を行ってください。

影響をうける製品：
Y 製品 2.1.x 以前のバージョン

悪用される脆弱性：
CVE-2022-*****
Y 製品の影響を受けるバージョンを使用している場合、認証されていない第三者が悪意あるファイルを＊＊＊領域に設置することが可能です。

攻撃が観測された期間：
○月○日以降～

不正アクセス元：
192.0.2[.]***
203.0.113[.]***

調査方法：
上記不正アクセス元からのアクセスがないかアクセスログを調査するほか、当該サーバの××操作ログに以下の痕跡がないかご確認ください。
（省略）

・情報共有活動（またはその窓口の専門機関）から得たフィードバック（インディケータ情報）を元に、Web サーバの各種ログを調査したところ、○月○日に製品Ｙの脆弱性を突いた不正アクセスがあったことが判明した。

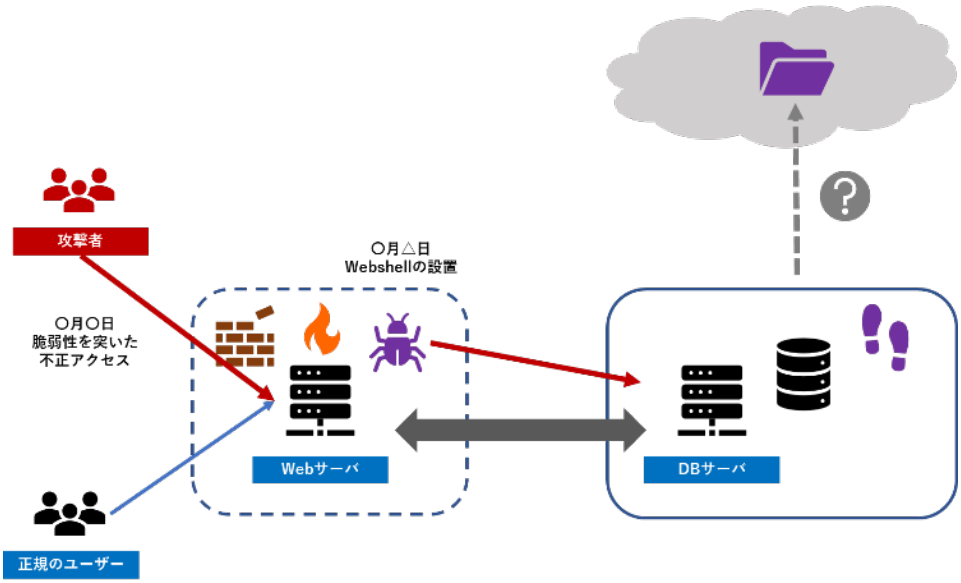


図 90

・不正アクセス被害に関する被害公表（第一報）を行うとともに、△△サービスの利用者に対する通知を行った。

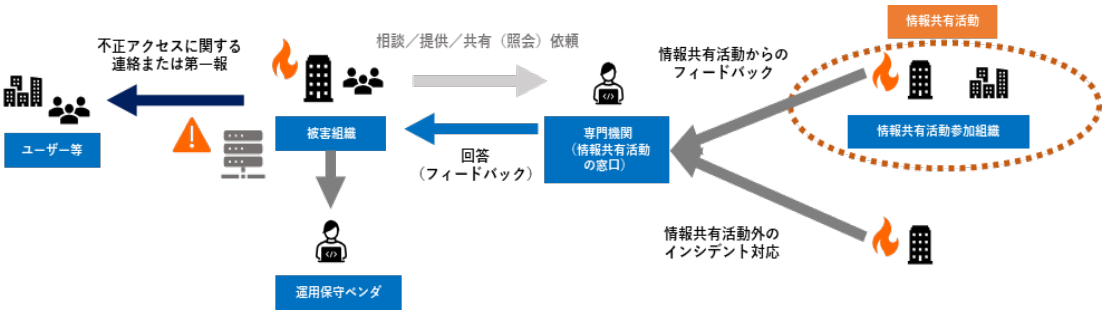


図 91

【ポイント解説】

・自組織（あるいは委託先）でヒントのない状態でアクセスログを調査し、不正アクセスを探し出す方法もありますが、このケースのように外部の専門組織や情報共有活動からイン

ディケータ情報（不正アクセス元に関する情報、攻撃のおおよその時期）を得ることで速やかに不正アクセスの痕跡を探すことが可能になります。
・悪用されている脆弱性情報を得ることで、当該製品のどこに不正なファイルが設置される可能性があるのか、既に見つけた不審なファイルがまさにそうした脆弱性悪用により設置されたのかどうかを絞り込むことができます。

次に行った対応：

・また、提供情報で示された操作ログ上の痕跡を調査したところ、提供された不正アクセス元以外の IP アドレスからの不審なアクセスも見つかったため、追加の共有情報として、専門組織に返答した。

ケース２－３：初動対応フェーズ③

図 92

状況：

・情報共有活動の窓口（専門機関）から以下のフィードバックがあり、不正アクセス元情報を注意喚起に使用することの連絡があった。

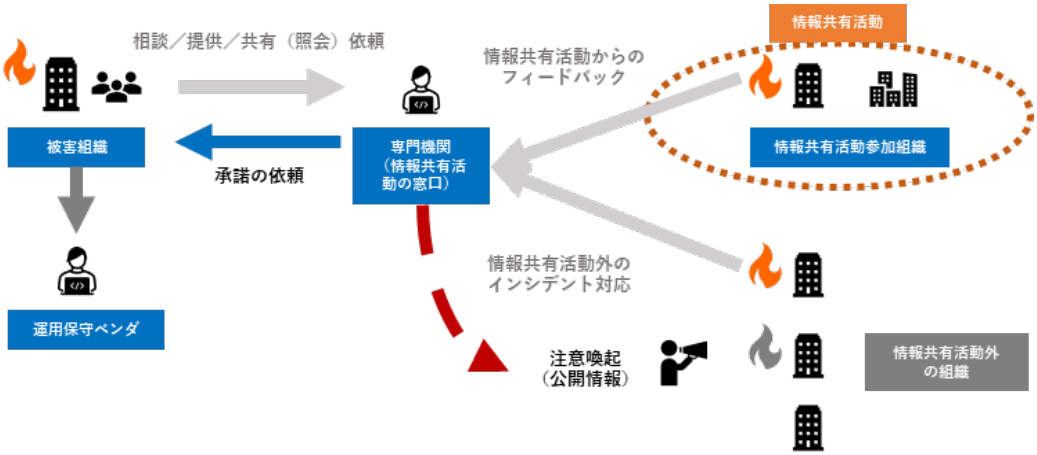


図 93

TLP:AMBER（※運用保守ベンダまで共有可）

提供いただいた、別の不審な IP アドレスですが、情報共有活動に展開したところ、他の被害組織への不正アクセスにも使用されていたことが判明しました。
御社のほか、複数の国内組織での被害が確認されているため、注意喚起を出す準備を進めていますが、ご提供いただいた不正アクセス元の IP アドレス情報（　　）を IoC 情報として記載したいと考えています。下記に注意喚起予定の文案を記載しておりますので、ご確認ください。

＜注意喚起文案＞

（省略）

【ポイント解説】

・専門機関を始めとした専門組織では、個別のインシデント対応に加えて、情報共有活動で得られた情報を元に、攻撃が広範囲に及ぶ蓋然性が高いと判断した場合、注意喚起を行います。そうした場合、被害組織で見つかった IoC 情報を掲載し、通信のブロックや調査を促します。IoC 情報は基本的に個別の被害組織と結びつく情報ではありませんので、提供した IoC 情報が公開情報として扱われることに積極的に協力することが望まれます。

次に行った対応：

・これまでに情報共有活動によって得られた情報を元に判明した不正アクセスが行われた期間や、既に見つかっている Webshell 経由での不審な操作が行われていたと思われる期間を踏まえて、どの時点の当該データが不正にアクセスされた可能性があるか調査を開始した（被害範囲の特定調査）。

ケース２－４：最終報フェーズ

図 94

状況：

（※詳細な調査フェーズや、所管省庁等への報告は図では省略）

・調査が終了したため、以下の最終報の公表を行った。

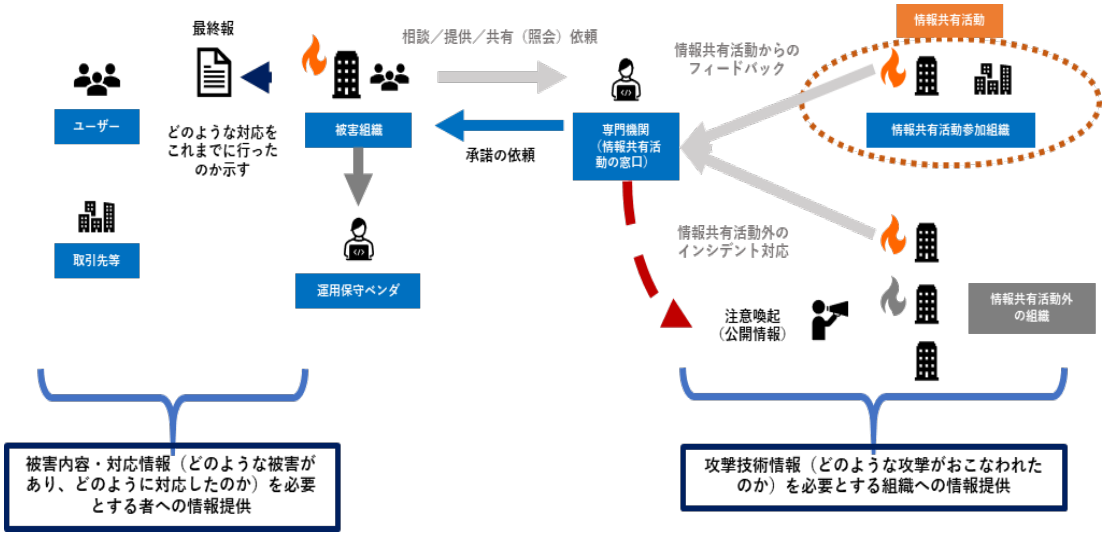


図 95

弊社システムに対する不正アクセスについて

×月１日

＊＊＊＊＊株式会社

弊社の△△△サービスのシステムが外部からの不正アクセスを受けたことが判明しました。

専門組織とともに調査を行い、原因特定や被害情報の確認を行うとともに、影響のあった利用者の方への連絡のほか、関係各所への報告を行っております。

引き続き、再発防止に向けた対策・体制強化に取り組んでまいります。

1．経緯

□月○日	製品Ｙの脆弱性（CVE-2022-*****）がメーカーから公表される
○月○日	製品Ｙの脆弱性（CVE-2022-*****）を悪用した不正アクセスが行われる
○月△日	△△△サービスの提供に使用している製品Ｙが稼働する Web サーバに不正プログラム（Webshell）が設置される △△△サービスに関するデータを保存したデータベースで不正な操作が行われる
○月×日	△△△サービスに関するデータの一部がインターネット上で見つかり、発見者から弊社に連絡が行われた
○月×日	△△△サービスのシステムを管理する運用保守ベンダに依頼し、調査を開始
○月＊日	専門機関Ａに相談を行い、見つかった不正プログラムに関する情報などを情報共有活動に共有し、追加の情報提供を求めた。また、Ｂ県警に相談を行うとともに、個人情報保護委員会へ速報（※）を行った ※報告対象事態の発生を知った時点から概ね３～５日以内
○月＆日	専門機関Ａからの提供情報を元に調査を進めたところ、製品Ｙの脆弱性を悪用した不正アクセスであったことが判明。 第一報を公表し、利用者に二次被害のおそれ等に関する注意を呼びかけた 追加で見つかった不正アクセス元などに関する情報を専門機関Ａに情報提供 個人情報保護委員会へ確報（※）を行った。Ｂ県警への連絡のほか、所管省庁への報告も実施（※※） ※報告対象事態の発生を知った日から 60 日以内 ※※Q20（86 頁）記載のとおり、社会的な影響が大きい事案のような場合、法令に基づく報告以外であっても、所管省庁に任意の報告をすることも想定されます
○月％日	専門機関Ａなどから製品Ｙの脆弱性を悪用した攻撃に関する注意喚起が公表される
○月　日～	被害範囲の詳細調査と漏えい情報の件数や漏えい経路に関する詳細調査を実施

２．被害内容
・△△△サービスのシステム内には個人情報が保存されており、今回の侵入した攻撃者によって情報が外部に漏えいし、なんらかの経緯でインターネット上に拡散したものと推測していますが、拡散した経緯は現時点で不明です。

（省略：個人情報の内訳、件数等～）

３．原因と再発防止策
△△△サービスのシステム上で稼働するソフトウェア製品 Y の脆弱性（CVE-2022-*****）が悪用されたものであったと判明しています。当該脆弱性は侵入の○週間前に修正プログラムが公開されていましたが、定期的なメンテナンス時にアップデート作業をする予定であったため、侵入時点でバージョンアップがなされていませんでした。
今後、専門機関等が出される脆弱性に関する情報を精査し、速やかに対応が必要なものについて優先度を設けて対処するよう、社内ルールや体制整備を進めてまいります。
また、攻撃者に侵入された後の侵害拡大については、ネットワーク設定やサーバの設定で防ぐことが可能だった点が認められたため、これら設定の変更による対策強化をすすめてまいります。

【ポイント解説】
・対応時系列の中で、相談・連絡した先の各組織名を記載しています。この脆弱性悪用については専門機関 A が注意喚起を出していることから、リリースを見た関係者が「(被害組織が) 当該攻撃について詳しい知見のある専門組織に相談できている」と評価することができます。
・また、情報共有活動のフィードバックとして自組織で新たに見つかった技術情報（不正アクセス元）を専門機関／情報共有活動側に提供していることを示しており、そうした動きの後に専門機関 A から注意喚起がなされた経緯が見えるため、リリースを見た関係者が「(被害組織が）情報共有活動や注意喚起などの他の被害拡大予防のための活動に貢献していた」と評価することができます。

ケース３：侵入型ランサムウェア攻撃

【共有・公表のポイント】

・侵入型ランサムウェア攻撃の初動対応においては、予防的措置としてネットワーク停止等を行いますが、業務への影響を最小限にとどめるためには速やかにランサムウェアの特定や侵入経路の特定が必要であり、インシデント対応の初期段階においてそれらの情報を入手することが必要です。

・他方で、すぐに専門企業と契約を結ぶことも難しいため、暫定的には専門機関や情報共有活動に照会をかけて、上記の情報を入手することが望まれるます。

・二重の脅迫型攻撃によりリークサイト上に犯行声明等が掲載されたり、対外向けサービスが停止したりするなど、ただちに被害が不特定多数の者に認知される場合があるため、速やかに第一報を公表する必要があるケースが想定されます。

ケース３－１：発覚～初動対応フェーズ①

図 96

状況：

・当日朝、社内の○○○サーバにアクセスできない、とする社内からのトラブル相談に対応して調査をしたところ、○○○サーバ内に保存されたデータの多数が暗号化されていることが判明した。

・同時に、出勤した複数の社員から、端末上のファイルが開けないとの問い合わせがあり確認したところ、同じく多数のファイルが暗号化されていたことが判明し、デスクトップ上に身代金脅迫のメッセージが表示されていることを確認した。

・JPCERT/CC が公開している「侵入型ランサムウェア攻撃を受けたら読む FAQ」などの情報を参考に初動対応を開始した。

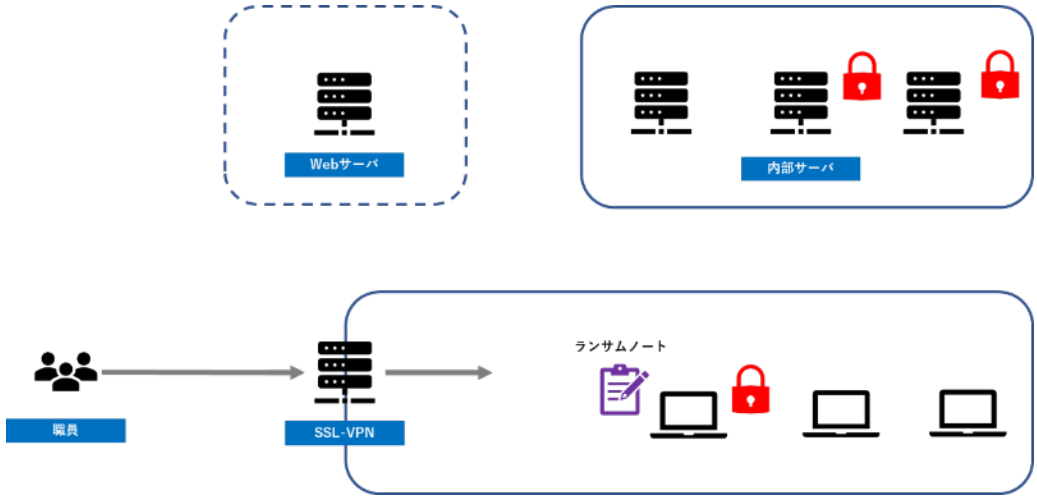


図 97

【ポイント解説】

この想定ケースでは、リークサイトへの掲載は当該時点ではまだなされておらず、また、被害が確認された○○○サーバは社内向けのものであり、対外向けサービスには用いていないことから、ただちに攻撃被害が外部の不特定多数に知られるという状況ではありません。しかし、Q17（75 頁）等で示したとおり、既にリークサイトに犯行声明が掲載されていたり、外部へのサービス提供に支障をきたしたりする場合、ランサムウェア攻撃の被害が不特定多数の者から推測される状況になる場合があります。その場合は、Q17（76 頁）のとおり、対外説明のための第一報などを急ぎ用意する必要があります。

次に行った対応：

・以前もインシデント調査を依頼したことのあるセキュリティベンダ A に調査依頼の相談を行うとともに、専門機関 B への相談と情報提供依頼を以下のとおり行った。また、B 県警察に被害に関する相談を行った。

ランサムウェア攻の撃被害が確認され、現在調査を開始していますが、不明な点が多く、調査に必要な情報の提供をお願いします。
下記情報について、情報共有の必要があれば、弊社名は 匿名 及び、TLP：AMBER にて、共有をお願いします

＜概要＞
○月×日頃、サーバ○台と端末×台がランサムウェア感染と思われる被害に遭っていることを確認。
侵入原因等は現在調査中で不明。

ランサムウェアについて：
被害に遭った端末上のファイルの拡張子が「.*****」に変えられていた。
デスクトップ上に表示されていた身代金要求の脅迫メッセージのテキストは別添でお送りします。

被害範囲について：
被害に遭ったのは社内向けサーバ〇台と端末X台で、いずれも外部から直接アクセスすることはできず、端末については、SSL-VPN 経由でのリモートデスクトップ接続のみ許可している。サーバについては RDP 含め外部から接続はできず、社内の端末からのみアクセスが可能。
サーバはすべて Windows サーバで、最新のセキュリティパッチを適用済み。

ケース３－２：初動対応フェーズ②

図 98

状況：

・情報共有活動の窓口（専門機関）から回答があり、以下の不正な通信がないがログを調査するよう案内があった。

TLP:AMBER（※運用保守ベンダまで共有可）

＜概要＞
暗号化されたファイルの拡張子や脅迫メッセージの特徴から、○×□ランサムウェアを用いた侵入型ランサムウェア攻撃と思われます。
このランサムウェアを用いた攻撃活動について、主に海外の被害においては、SSL-VPN 製品の製品Ｚの脆弱性を悪用した初期侵入が確認されていますので、下記情報を元にご確認ください。

推測されるランサムウェア：
いただいた情報から、○×□ランサムウェアのビルダーを用いて作成された○×□ランサムウェアの亜種ではないかと思われます。
基本的に○×□ランサムウェアの既知の検体では、自動で感染拡大するような挙動は確認されていません。

推測される初期侵入経路：
SSL-VPN 製品の製品 Z の脆弱性を悪用したものや、管理不備の RDP 経由の被害が海外においては確認されています。
外形上の調査から、以下の御社管理の IP アドレスで製品 Z が稼働しているのではないかと思われますので、ソフトウェアバージョンの確認や不審なアクセスがないかご確認ください。

vpn1.＊＊＊＊.co[.]jp　192.0.2[.]112
vpn2.＊＊＊＊.co[.]jp　192.0.2[.]113

影響をうける製品：
製品Z のファームウェアが 3.1.2.x 以前のバージョン

悪用される脆弱性：
CVE-2022-*****

調査方法：
SSL-VPN での不審なアクセスがないかご確認ください。また、ランサムウェア○×□を用いる海外の攻撃では、攻撃者が侵入後に AD サーバを侵害しているケースがあるため、AD サーバに不審なアクセスや操作がなかったか確認することを推奨します。

参考情報：
製品Z のメーカーからの公式情報
　URL：（省略）

○×□ランサムウェアに関する海外の専門企業の調査レポート
URL：（省略）

（省略）

・提供情報を元に確認したところ、SSL-VPN 製品のファームウェアのバージョンが脆弱なバージョンのまま稼働しており、今回の被害が発覚する前日に不審なアクセスがあったことが判明した。
・被害を受けていないサーバについても一時的に停止させていたが、提供情報から、被害拡大のおそれがないと判断し使用を再開した。

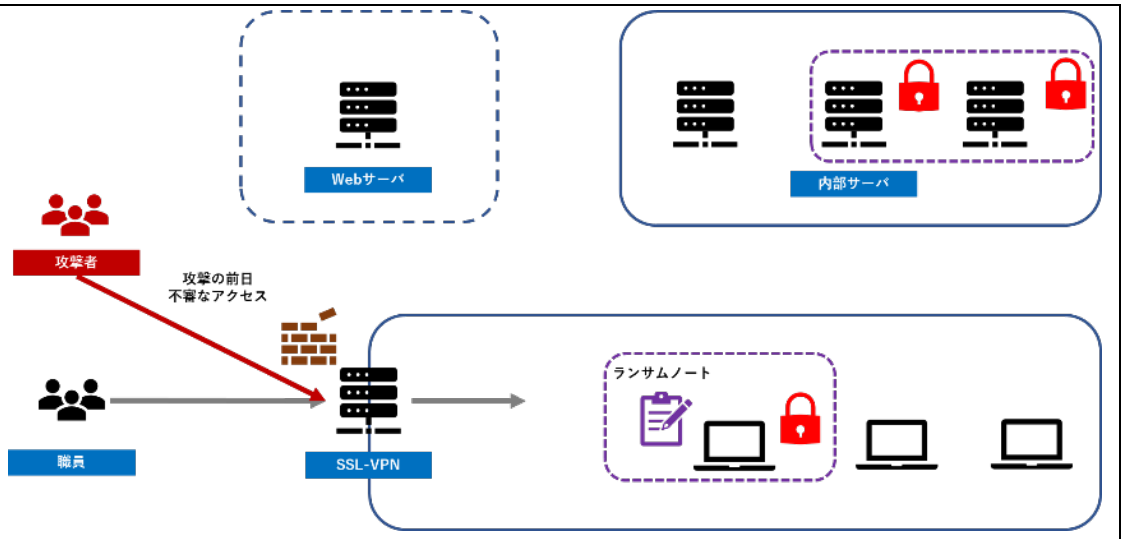


図 99

【ポイント解説】

・ランサムウェア感染時の対応として、かつての Wannacry2.0 などを念頭に、自己拡散するタイプのマルウェアを想定した、ネットワーク遮断や感染端末以外のサーバ／端末の利用停止などの初動対応が予防的措置として行われることが多く見られます。、こうした予防措置的対応は業務に支障をきたすため、上記のやりとりのように、ランサムウェアの種別を速やかに特定して、予防的措置を最小限の範囲とすることが必要です。

・一刻を争う対応が必要な場合、ランサムウェア検体の確保や専門組織への解析依頼やそのための手続を行う時間的猶予がない場合もあるため、今回のケースのように暗号化後の拡張子やランサムノートなど「外形上すぐにわかる情報」を専門機関や情報共有活動に伝えることで、ランサムウェアの種別特定に必要な情報を得ることが有効です。

・ランサムウェア感染事案の場合、調査対象端末自体や調査に必要なログを保存したサーバなども被害に遭っているため、通常のインシデント対応における調査がそもそもできないケースがあります。そのため、上記のような攻撃動向に関する情報を得ることで、ある程度侵害原因箇所／調査対象を絞り込むことで、速やかなインシデント対応につなげられる可能性があります。

次に行った対応：

・SSL-VPN 経由での不正アクセス以降 2 日間の範囲で、SSL-VPN から社内端末／サーバへの不正なアクセス有無や、AD サーバの侵害有無、被害にあったサーバに対する不審なアクセスがなかったかなど、攻撃者の侵入後の侵害範囲に関する調査を開始した。

・上記侵害範囲に関する調査のほか、外部へのファイルの持ち出しなどが行われていないか調査を進めた。

・上記調査の過程で見つかった技術情報について情報共有活動への提供を行った。

いただいた情報を元に調査したところ、以下の情報が見つかりましたので、共有します。

共有指定： 匿名希望にて、以下の情報は TLP：AMBER

共有情報：

不正アクセス元：
198.51.100[.]***
○月△日 0:32 ~ 1:10 まで複数回の不正なアクセス

ケース３－３：初動対応フェーズ③

図 100

状況：

・情報共有活動の窓口（専門機関）から以下の情報を情報共有活動内に共有しているとの参考情報が共有された。

TLP:AMBER（※運用保守ベンダまで共有可）

＜攻撃の概要＞
○×□ランサムウェアを用いた侵入型ランサムウェア攻撃が国内で観測されています。
このランサムウェアを用いた攻撃活動につい、SSL-VPN 製品の製品Ｚの脆弱性を悪用した初期侵入が国内外で確認されているため、以下の情報を参考に対応を行ってください。

○×□ランサムウェアについて：
○×□ランサムウェアのビルダーを用いて作成された○×□ランサムウェアの亜種が攻撃に用いられます。
基本的に○×□ランサムウェアの既知の検体では、自動で感染拡大するような挙動は確認されていません。

確認された初期侵入経路について：
以下の不正アクセス元からの SSL-VPN 製品の製品 Z の脆弱性（CVE-2022-*****）を悪用した侵入による攻撃被害が確認されています。

＜不正アクセス元に関する情報＞
IP アドレス：203.0.113[.]***
攻撃時期：○月△日～

影響を受ける製品：
製品Ｚ のファームウェアが 3.1.2.x 以前のバージョン

悪用される脆弱性：
CVE-2022-*****

調査方法：
SSL-VPN での不審なアクセスがないかご確認ください。また、ランサムウェア○×□を用いる海外の攻撃では、攻撃者が侵入後に AD サーバを侵害しているケースがあるため、AD サーバに不審なアクセスや操作がなかったか確認することを推奨します。

参考情報：
製品 Z のメーカーからの公式情報
URL：（省略）

○×□ランサムウェアに関する海外の専門企業の調査レポート
URL：（省略）

【ポイント解説】
・情報共有活動に参加している場合、自組織から専門機関や情報共有活動を実施する団体や組織に提供した情報がインディケータ情報として掲載されて展開されてくることがあります。自組織が提供した情報がどのように使われているのか知る機会であると同時に、どのような情報を提供すると、情報共有活動で活用されやすいのか知る機会にもなります。

次に行った対応：

（詳細調査フェーズや公表フェーズについてはケース１、２と同様）

5．チェックリスト／フローシート

情報共有と被害公表における情報の種類のチェックリスト

情報共有や被害公表では、取り扱う情報の種類が異なるため、以下を参考にしてください。

情報の種類	情報共有活動	留意点	被害公表	留意点
被害組織名	－	ハブ組織／専門組織を介した共有活動においては匿名であることが大半であるが、業種について付記することで情報が必要な組織に共有情報が伝達しやすくなる	○	
業種／規模	△		○	
被害内容	－		○	
タイムライン（対応状況）	－		○	被害組織内の対応のほか、どのような対外対応（二次被害防止のための顧客通知や専門組織への相談等）を行ったのか示すことが望ましい
タイムライン（技術情報）	△	攻撃経路や侵入後の攻撃者の動きに関する技術的情報の共有は有益だが、調査により判明するまで時間がかかるため、インディケータ情報が優先する	○	どのようなタイムラインで、どのような手順を踏み攻撃が行われたのか示すことで、“広義の”共有効果として有益になる（Q16（72 頁）参照）
攻撃対象システム	△	匿名を希望する場合、被害組織が特定されうるような個別システムに関する情報の共有は避けなければならないが、標的となっている対象が汎用的な製品／システムの場合、ソフトウェア名やバージョン、簡単なシステム構成などに関する情報は共有活動に有益	○	どのような構成／運用／対策を行っていたシステムが被害にあったのか具体的に示すことで、“広義の”共有効果として有益になる（Q16（72 頁）参照）
（攻撃対象の）対策状況	△	どのような対策をしていたにも関わらず、当該攻撃手法により突破されてしまったのか、という情報は共有に有益であるが、調査により判明するまで時間がかかるため、インディケータ情報の共有を優先する	○	
攻撃主体に関する情報	△	特定には専門的知見が必要であり、また専ら専門組織が特定の攻撃活動を識別するために便宜上用いるため、被害組織側で用意することが必ずしも求められるものではない	△	被害組織から個別に公表されるよりも、複数の被害組織で見つかった情報を元に、攻撃の全容が解明され、専門組織から技術的なレポートとして公表することが望ましいケースもある。
脆弱性関連情報等	○	特に未知の脆弱性悪用の場合、まず脆弱性修正対応への協力が求められる（Q23（94 頁）参照）	△	
その他 TTP	△	ある程度調査期間を経なければ判明しないため、インディケータ情報の共有を優先する（Q7（51 頁）参照）	△	
マルウェア	○		△	
通信先	○		△	

○：主な内容となる情報　△：内容／状況による　—：基本的に対象外　表 10

情報共有判断のためのフロー

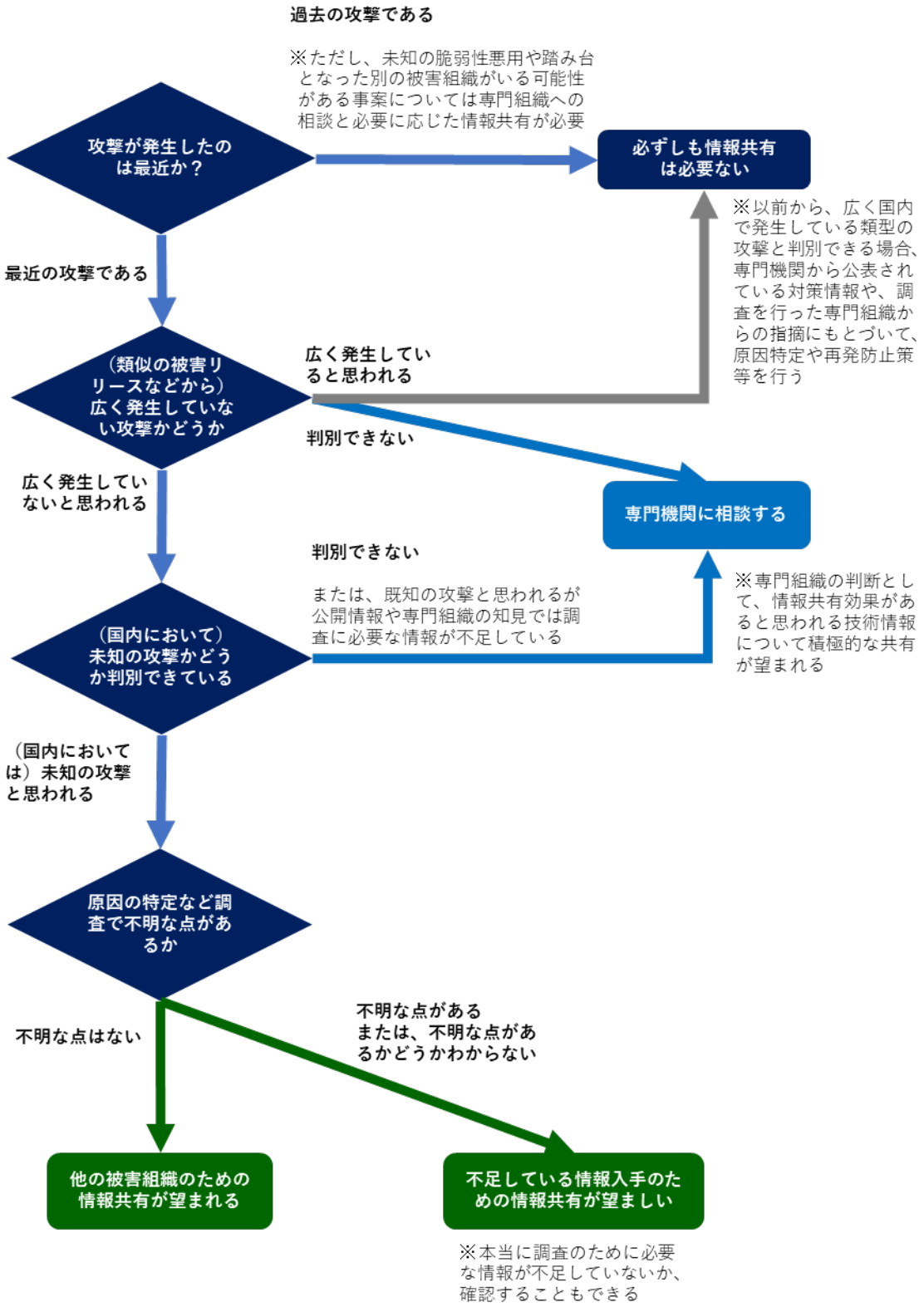


図 101

被害公表判断のためのフロー

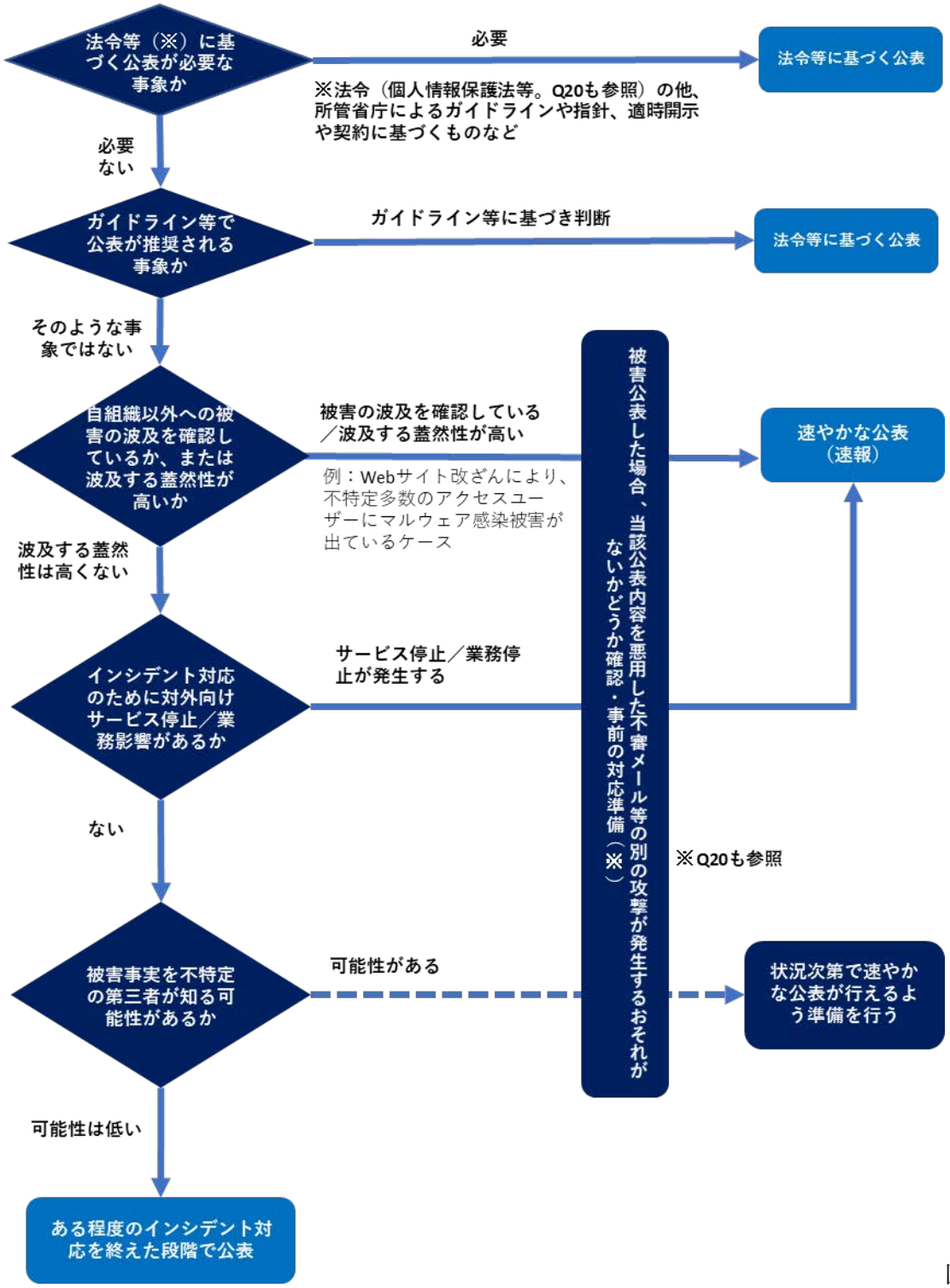


図 102

◇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（令和４年４月時点、敬称略）

新井　悠	（株）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	（一財）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）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）　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）　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（座長）	東京都立大学法学部　教授
松坂　志	（独）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
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）読売新聞東京本社　編集委員

◇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　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/CC）