攻撃技術情報の取扱い・活用手引き

2024 年 3 月 11 日

サイバー攻撃による被害に関する情報共有の促進に
向けた検討会事務局

第１章 はじめに

本手引きの目的

本手引きでは、サイバー攻撃の被害組織から相談・依頼を受け、インシデント対応支援にあたる専門組織等（本手引きでは「ファーストレスポンダー」と定義しています（☛第 1 章 14 頁参照））が、他の専門組織又は情報共有活動との間で情報共有を行い、調査に必要な情報を入手するなどして、効率的、的確にインシデントをクローズすることを目指すものです。
こうした、被害組織に代わっての情報共有活動は、被害組織自身のインシデント対応コストを低減するだけでなく、攻撃技術情報に適切な知見を持つ専門組織同士が情報を取り扱うことで伝達効率が上がるとともに、攻撃技術情報を正確に伝えるためのミスコミュニケーション防止にもなると考えます。

他方で、被害組織の CSIRT チーム同士などによる、直接の情報共有活動や被害組織自身による専門組織等のハブ組織を通じた被害組織間の情報共有活動も引き続き有効な取組であり、こちらは共有・公表ガイダンスで扱っていますので、ご参照ください。

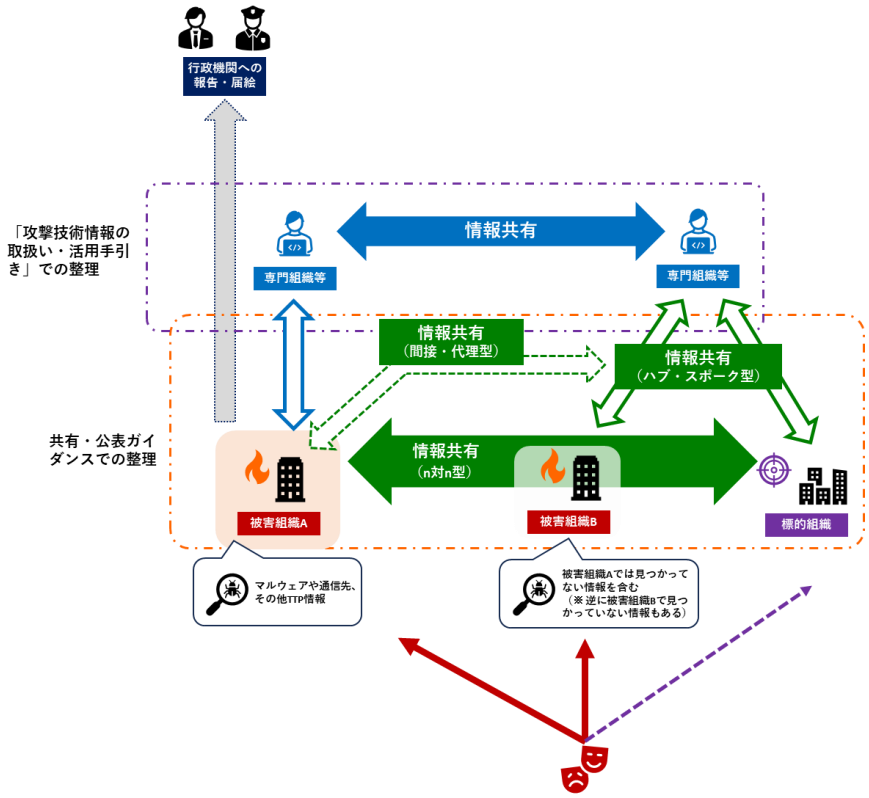


図 1

スコープとしている「情報共有活動」：時間軸の観点から

本手引きでスコープとしている「情報共有活動」は、主に短期的・中期的なタイミングにおける、主に専門組織同士の情報共有活動です。被害組織同士、被害組織と専門組織（又は情報共有活動のハブ組織）との間の情報共有活動については、後述のとおり、サイバー攻撃被害に係る情報の共有・公表ガイダンス[1]（以下、「共有・公表ガイダンス」という。）で解説されていますので、そちらをご覧ください。

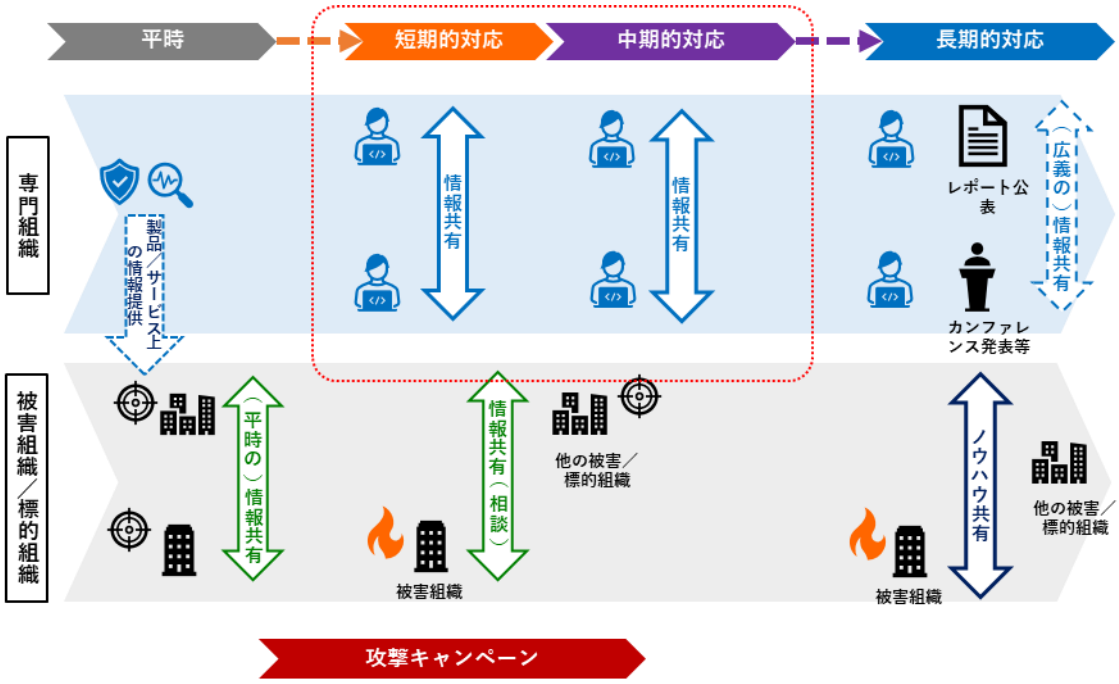
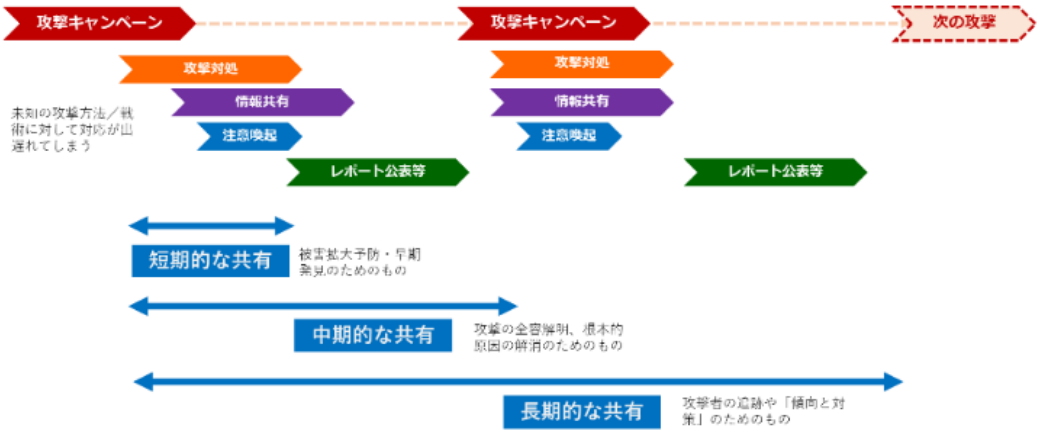


図 2

インシデント対応や情報共有活動における「短期的」「中期的」「長期的」という区分については、同じく共有・公表ガイダンスに下記のとおり解説がありますので、ご参考ください。

本手引きでは専門組織同士の短期的～中期的対応を主なスコープとしており、平時からの情報共有活動や、レポート公表やカンファレンス発表などを通じた長期的な情報共有活動については詳細には触れませんが、いずれも攻撃対処全体の中で重要な役割を担っています。

[1] https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf



（共有・公表ガイダンスより（図 73））

図 3

情報共有のメリットについて

情報共有の目的としては、

A 被害現場間の情報格差解消のための情報共有
B 専門組織間の情報共有

があり、A については、共有・公表ガイダンスで扱っています。被害組織又は他の標的組織が情報共有によってどのようなメリットを受けることができるのか等は共有・公表ガイダンスをご覧ください。
本手引きでは、B を扱っています。専門組織同士が情報共有する目的・必要性については後述の「何のために専門組織は攻撃技術情報を共有するのか」（第 2 章 20 頁参照）にて詳細を記載していますので、ご覧ください。

基本的に現場対応にあたる専門組織等も被害組織と同じく、原因特定、被害範囲特定に必要な情報を十分に得られていない状況にあります。（参考：サイバー攻撃による被害に関する情報共有の促進に向けた検討会最終報告書 8 頁）専門組織等の間で情報共有することで、インシデント対応支援先のインシデント対応を適切にクローズさせることができ、情報不足に起因する調査不足による調査の手戻り[2]などを未然に防ぐことができます。
また、クライアント（被害組織）に対しても、自組織が適切な調査能力を有していることを示す一助になります。

[2] 一通りのインシデント対応が済んだのち、被害組織が所管省庁等に（任意のものを含めた）報告を行った際に、所管省庁側から別途専門機関のセカンドオピニオンを受けるよう指示されたり、あるいは被害組織自身の判断でセカンドオピニオンとして専門機関に追加の相談をするケースがあります。そうした場合に、専門機関から調査不足を指摘され、調査のやり直し、手戻りが発生するケースがあります。

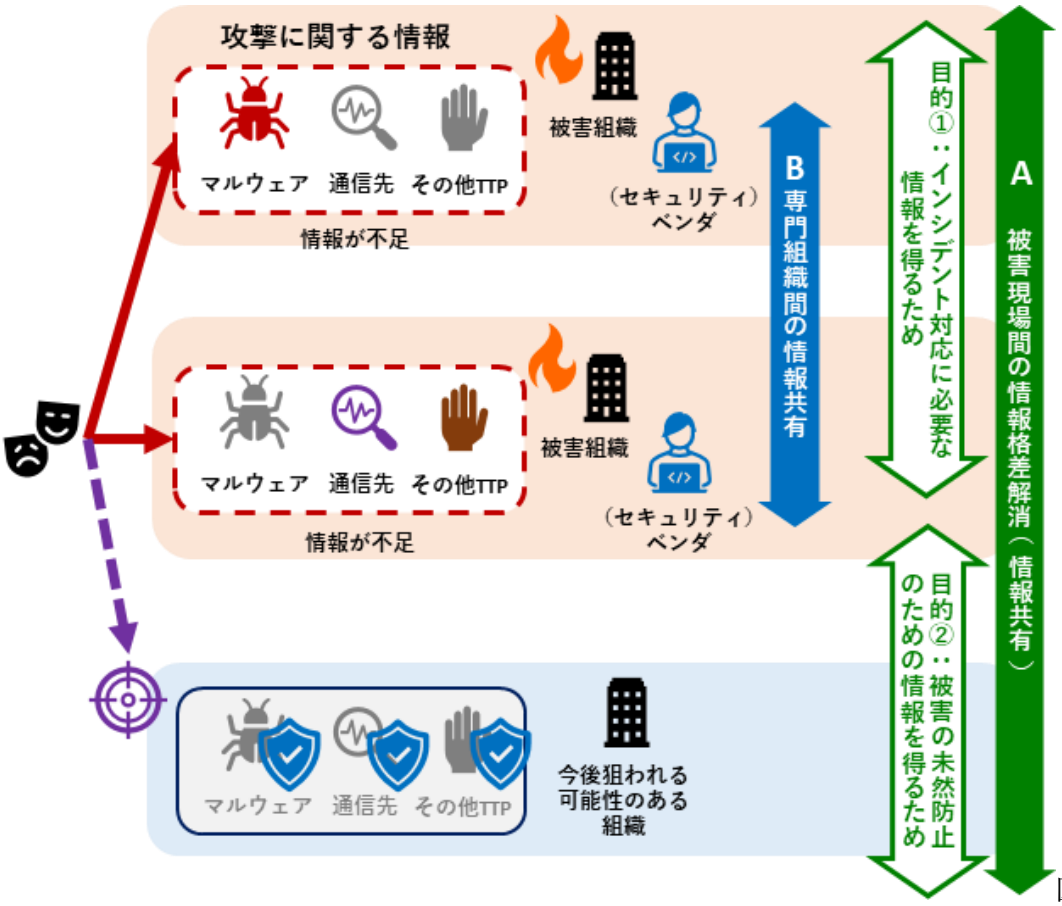

攻撃に関する情報
マルウェア
通信先
その他TTP
情報が不足
被害組織
（セキュリティ）ベンダ
マルウェア
通信先
その他TTP
情報が不足
被害組織
（セキュリティ）ベンダ
マルウェア
通信先
その他TTP
今後狙われる可能性のある組織
B 専門組織間の情報共有
目的①：インシデント対応に必要な情報を得るため
目的②：被害の未然防止のための情報を得るため
A 被害現場間の情報格差解消（情報共有）

図４

情報共有を被害組織―専門組織間で分担することのメリット

インシデント対応の内容・順番は攻撃類型や被害内容によって様々であり、被害組織は必ずしも教科書通りの順番で対応できるわけではありません。現状では、所管省庁等への報告や被害公表、取引先や顧客への連絡に加えて情報共有活動との連携も被害組織自身が行っており、リソースの消耗もさることながら、本来、インシデント対応の初期段階のタイミングで有効な情報共有や外部専門機関との連携が後回しになるケースがあります。情報共有のための作業を“分担”できることで、被害組織は被害公表や報告等に注力でき、専門組織等の側は調査に必要な情報の把握に努めることができます。

攻撃技術情報について、どの情報は情報共有効果を得られるもので、どの情報は不要なのか、被害組織側に知見がないことも多いため、より知見のある専門組織等が情報の精査や共有作業を行うことは効率性だけでなく、意図しない情報の開示といった事故の防止にも有効です。

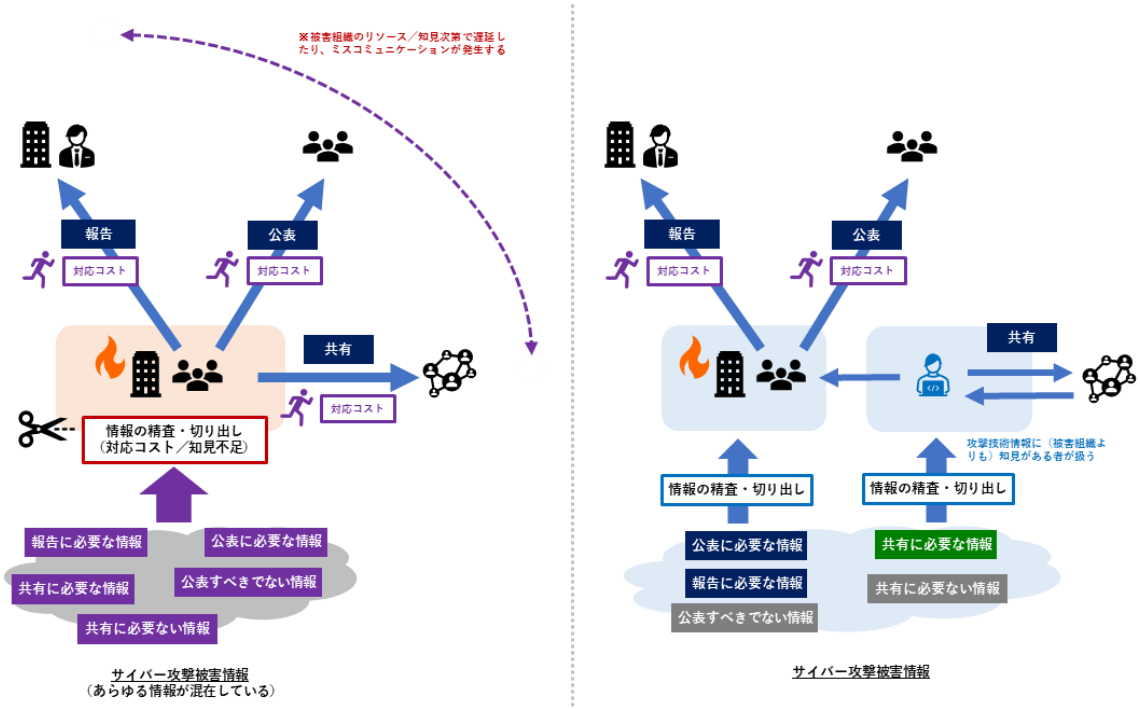


図 5

参考：本来必要な技術的対応や情報共有が行えないケースの例

APT 事案等で侵害の橋頭堡的に、又は横展開上の通過点として侵害された端末／サーバ内に個人情報が格納されていた場合、APTアクターの目的が当該個人情報の窃取でなかったとしても、漏えいしていないことが確認されない以上、個人情報漏えい事故としての対応に迫られる場合があります。個人情報漏えい事故における 3～5 日以内の速報や速やかな影響先への通知作業に多大なリソースが必要になるため、個人情報漏えい事故対応が優先され、本来の APT 事案対応に必要な情報入手のための情報共有等の外部連携が後回しになるケースがあります。

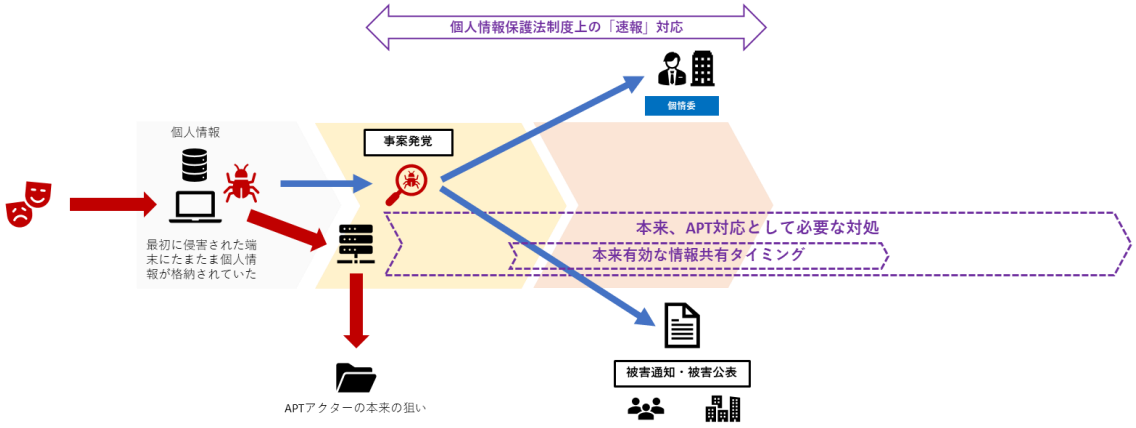


図 6

用語集

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。
攻撃グループ／アクター※	サイバー攻撃を行う組織又は個人そのもの。また、攻撃を行った者を便宜上グルーピングし、それを呼称するもの。
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）等の通信先及び踏み台としたサーバ。
TTP 情報／TTPs	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。
脆弱性情報※	脆弱性の性質及び特徴を示す情報。 （※「ソフトウェア製品等の脆弱性関連情報に関する取扱規程」（平成二十九年経済産業省告示第十九号に基づく。))
脆弱性関連情報※	「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」。 （出典は同上。）
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（「サイバー攻撃被害に係る情報の共有・公表ガイダンス」Q4（38頁）参照のこと)。
攻撃技術情報	マルウェア情報、攻撃インフラ、TTP 情報など攻撃者による攻撃活動又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又は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又は攻撃インフラを明らかにすること、もしくは、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」、「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」、「通信の発生日時」などの情報。
脅威情報	組織又は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、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、被害予防に必要な侵入経路などの TTP 情報を共有する。
情報展開※	（主に非公開の）情報共有活動において主に情報共有のハブ組織から参加組織に対して、又は参加組織から他の参加組織に対してインディケータ情報をはじめとした攻撃技術情報を提供すること。
（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又は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。
注意喚起	主に専門機関が、既に発生している攻撃活動又は今後悪用される蓋然性が高い脆弱性に関して、影響を受ける対象者に対して注意を呼びかけ、具体的な対策方法を伝達するために行う情報発信。
（分析）レポート公表※	専門組織がインシデント対応や攻撃の観測結果を基に、新たな攻撃手法及び攻撃活動に関する技術的分析と考察をまとめた情報発信。
通知※	侵害されているサーバ／端末の管理組織／個人に対して

	専門機関から直接、又は ISP、運用保守ベンダ等を通じてその事実や対応方法が伝達されること。
（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。
届出	ある行為を行うこと又は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又は、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。
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、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。
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。
運用保守ベンダ※	ユーザー組織が利用しているネットワーク、システム、アプリケーション、サーバ等の基盤について、運用保守を委託されたベンダ。
（販売）代理店※	IT 製品のメーカーや IT サービスの提供事業者に代わり、当該商品をユーザーや SIer／NIer 等に販売する事業者。
SIer/NIer※	IT システム全体の設計・構築・導入等を行う SIer と、特にネットワーク／ネットワーク機器の構築・導入を行う NIer のこと。
（製造）メーカー	ソフトウェア等の製造元。

ファーストレスポンダー※	攻撃の検知／被害認知を受けて被害組織から初動対応や調査を依頼された者。ネットワーク運用保守ベンダやインシデントレスポンスまで受けている SOC 事業者やアンチウイルスベンダ、別途インシデントレスポンス対応依頼を受けたセキュリティベンダ、初動対応の相談を受けた専門期間など案件によりこれを担う組織は様々。
調査ベンダ※	上記のファーストレスポンダーに加えて、フォレンジックベンダやアンチウイルスベンダなど、個別のシステム／個別の検体の調査を依頼された者。 また、ファーストレスポンダーの調査が一通り終えた段階で、「セカンドオピニオン」的に調査／精査依頼を受けた者も想定される。
テイクダウン	不正サイト、C&C サーバなどの攻撃インフラの無害化のこと。
Abuse／Abuse 窓口※	インターネットサービス上における迷惑行為／不正利用のこと。ISP、クラウドサービス、レジストリ／レジストラなどが設けている、迷惑行為／不正利用の通報窓口のこと。

※印のあるものは本稿作成にあたって新規に定めたもの。印がないものは「共有・公表ガイダンスから引用。

本手引きの想定読者

本手引きの想定読者は以下のとおりです。

〇専門組織

インシデント対応や専門組織同士の情報共有活動に取り組む、セキュリティベンダ（インシデントレスポンス対応を行う事業者など)、SOC 事業者、アンチウイルスベンダ、専門機関や、情報共有活動のハブ組織を担っている専門機関等が含まれます。

〇ファーストレスポンダー

攻撃の検知／被害認知を受けて被害組織から初動対応や調査を依頼された者。ネットワーク運用保守ベンダやインシデントレスポンスまで受けている SOC 事業者やアンチウイルスベンダ、別途インシデントレスポンス対応依頼を受けたセキュリティベンダが想定されます。初動対応の相談を受けた専門機関（相談窓口）も含まれます。

〇調査ベンダ

上記のファーストレスポンダーに加えて、フォレンジック調査や検体調査を個別に依頼された者。フォレンジックベンダやアンチウイルスベンダが想定されます。
また、ファーストレスポンダーの調査が一通り終えた段階で、「セカンドオピニオン」的に調査／精査依頼を受けた者も想定されます。

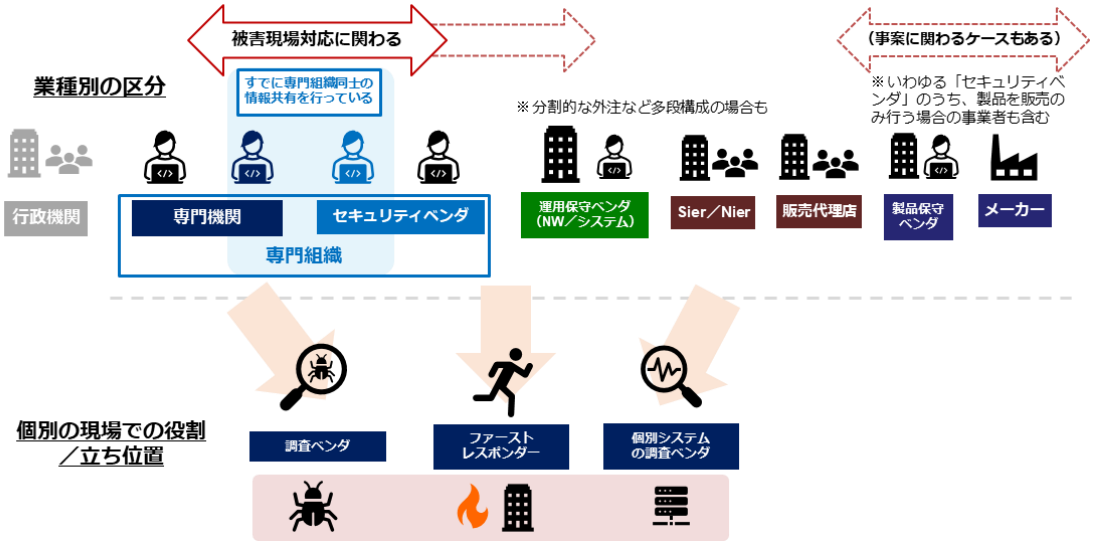


図 7

第２章 専門組織間の情報共有について

脅威情報を扱う大原則

石川朝久著「脅威インテリジェンスの教科書」では、脅威インテリジェンス（※本稿では「脅威情報」という用語で呼称します。「良いインテリジェンスの四要件（４A)」として、インテリジェンスに関する様々な先行研究やサイバーセキュリティにおける様々なアプローチを踏まえ、

- Accurate　（正確であること）
- Audience Focused　（利用者目線であること）
- Actionable　（アクショナブル＝次のアクションにつながること）
- Adequate Timing　（適切なタイミングで提供されること）

を示しています。
この手引きが目指す攻撃技術情報も上記の４条件を満たすものであり、専門組織間の情報共有や連携を通じて、各専門組織が**受信組織（被害組織やその他標的となっている組織）に対して作成・発出する情報**において以下が達成されることを目指します。

Accurate　（正確であること）

技術的に誤った情報や未精査な情報が流通しないこと

Audience Focused　（利用者目線であること）

情報の受信組織側に過度な情報共有活動の負担（応答義務や調査結果の“刈り取り”など）を強いたり、警戒や調査対応の必要がない情報を展開しないこと

Actionable　（アクショナブル＝次のアクションにつながること）

具体的な対策が示されていなかったり、対策的なものが示されていても非現実的な内容であったり、実施に必要以上のコスト負担を強いるものにしないこと

Adequate Timing　（適切なタイミングで提供されること）

既に終了してしばらく経つ攻撃に関する情報を発出したり、いつの攻撃なのか判然としないまま情報を発出しないこと

脅威情報と攻撃技術情報の整理について

本稿では、サイバー攻撃に関する情報のうち、通信先情報やマルウェア情報、TTP 情報等、攻撃者による攻撃手法やその痕跡を示す「攻撃技術情報」を主な情報共有の促進対象としています。
こうした、サイバー攻撃に関する情報は「脅威情報」「脅威インテリジェンス」「Threat Information」「Threat Intelligence」といった用語で示されることがありますが、こうした用語は多義的であり、用語の定義として引用されることのある海外文献上の表現ぶりについていくつか比較をしたのが下記の表です。

Threat 「Intelligence」となると、ある程度の被害傾向や標的分野に関する情報まで含まれ得るところ、本稿では、被害組織が特定されないように加工した情報を速やかに専門組織間で共有することを目指していますので、「脅威情報」や「Threat Intelligence」とは別に「攻撃技術情報」を共有することをスコープとしています。

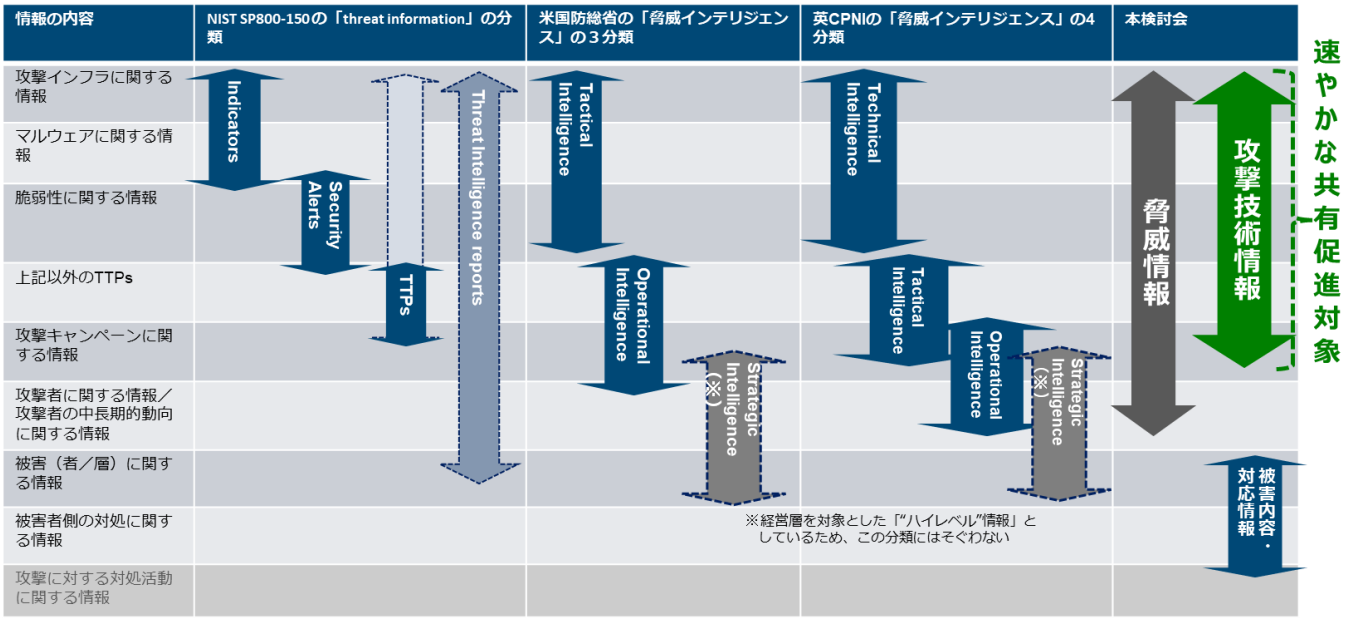


図 8

どのような情報を共有するのか

基本的には、**「攻撃者が限定的な範囲内で攻撃インフラや攻撃手法を使いまわす攻撃」**について、情報共有の効果が見込まれます（☛共有・公表ガイダンス 34 頁、48 頁、113 頁、116 頁、参照）。
他方で、広範囲への無差別攻撃や、単一アクターであっても攻撃インフラと攻撃手法をまったく使いまわさない攻撃の場合、情報共有効果はほとんど見込めません。広範囲への攻撃が行われている場合、非公開による情報共有ではなく、公開による注意喚起が行われたり、多数のセキュリティ製品／サービスで既に観測・対応可能な状況であったり、公開情報として TTPs、IoC 情報が流通していることが想定されます。

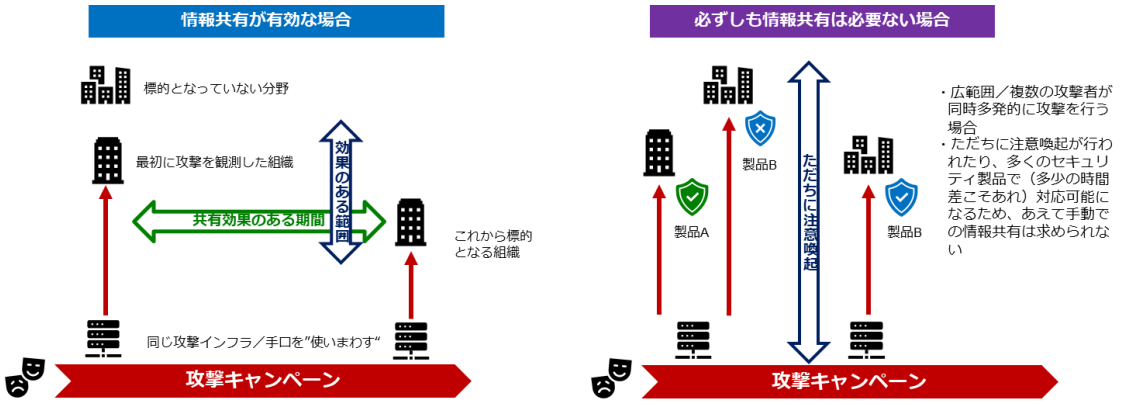


図 9

共有対象となる攻撃技術情報を選ぶポイントとしては、

① （基本的に）当該時点で非公開情報である
② 既存の製品・サービス上で広範囲に情報が流通していない／対応できていないと推測される
③ 限定的な範囲内で攻撃が行われている／行われていると推測される
④ 攻撃手口／攻撃インフラを使いまわしている／使いまわしていると推測される
⑤ 国内組織で利用されている製品の脆弱性や特定のサービスが悪用されている／悪用されている可能性がある

となります。①について、攻撃技術情報の一部、例えばマルウェア検体については VirusTotal などのサービスにアップロードされているなど、部分的に公開情報であるケースも想定されますが、攻撃活動の詳細など攻撃技術情報全体としてはまだ公開されていな

い／流通していない状態であることが想定されます。また、脆弱性悪用事案などでベンダレポートが既に公開されていても、その悪用事案の詳細について情報が公開されていない状態である、あるいは公表済みのレポートに誤りや不足があるようであれば、専門組織同士の情報共有で取り扱い、追加情報や修正情報を作出していく意味があります。⑤についてですが、②と同じような条件ですが、既知の脆弱性の悪用であっても検知が困難なケースが多く、さらに、第 3 章 71 頁（＜脆弱性悪用に関する情報はどうハンドリングされるべきか＞）解説のとおり、脆弱性悪用を示す情報は流通しにくい事情があるため、広範囲の被害拡大、あるいは認知が遅れる深刻な事案につながりやすく、実際の悪用現場を確認した専門組織同士の情報共有における早期の流通が望まれます。

何のために専門組織は攻撃技術情報を共有するのか

専門組織（専門機関やセキュリティベンダ）同士が情報共有する目的としては、主に以下の五つがあります。実際にはどれか一つ、ということではなく、複数の目的が組み合わさり（例：正規のサービスが悪用されている可能性があるが情報が不足している場合に、情報共有を通じてその確証を高めつつ、コーディネーション依頼を行う場合（A＋D））、行われています。

A：支援する被害組織における事案の対処及び全容解明や再発防止策のため、自組織では不足している情報を情報共有活動で補うこと

B：関与する情報共有活動の参加組織内に被害組織や標的組織がいる場合（あるいは想定される場合）、被害の未然予防や被害拡大防止、また被害の早期認知に必要な情報を得ること

C：被害組織への支援や調査を行う上で、自組織の知見が不足していないかについて知ること（平時からの取組として）

D：脅威アクターを中長期間にわたり追跡するために、自組織では不足している情報を情報共有活動で補うこと

E：攻撃要素（脆弱性や攻撃インフラ）への対処のため、対処ができる適切な専門組織等へ対応依頼をするために、必要な情報を提供すること

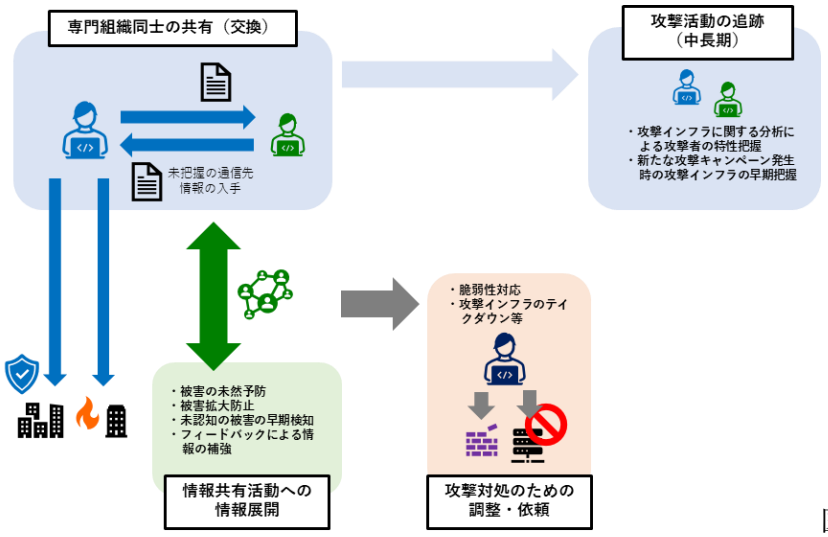


図 10

A：支援する被害組織における事案の全容解明や再発防止策のため、自組織では不足している情報を情報共有活動で補うこと

攻撃の高度化／複雑化により、**もはや単独の組織であらゆる事案に対応することは困難です**。攻撃者により、痕跡の消去や解析妨害、その他攪乱等が行われることから、専門組織間の情報共有を通じて、断片的な情報を収集し、攻撃の全容を解明しなければ、個別の事案のインシデント対応をクローズさせることが難しくなってきています。

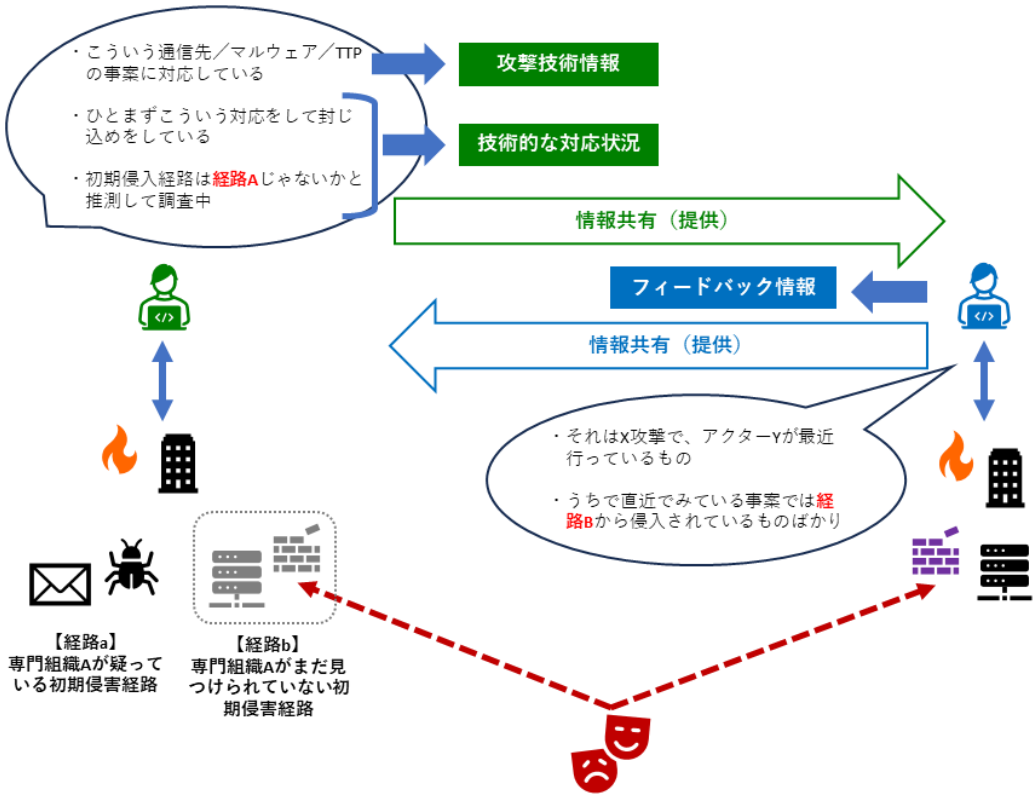


図 11

B：関与する情報共有活動の参加組織内に被害組織や標的組織がいる場合（あるいは想定される場合）、被害の未然予防や被害拡大防止、また被害の早期認知に必要な情報を得ること

専門組織は、相談等のあった被害組織への対応だけでなく、セキュリティベンダであれば、平時から自社製品／サービスを利用しているユーザー組織、（主に）専門組織であれば、情報共有のハブ組織を担当している情報共有活動の参加組織といった、現時点で被害は確認されていないが今後被害を受けるかもしれないといった、潜在的／将来の被害組織との関りがあります。こうした組織に対して、平時から製品・サービスや情報共有活動上の情報展開を通じて攻撃技術情報を提供しているわけですが、A に同じく、自らの知見不足により攻撃技術情報が提供されずに被害が発生したり、被害拡大を防止できないことが繰り返されれば、長期的にはユーザーや活動参加者を失うこと（≒大きな情報源を失うこと）につながります。そのため、こうした状況を防ぐべく、最新の攻撃技術情報を外部から得ることが重要です。

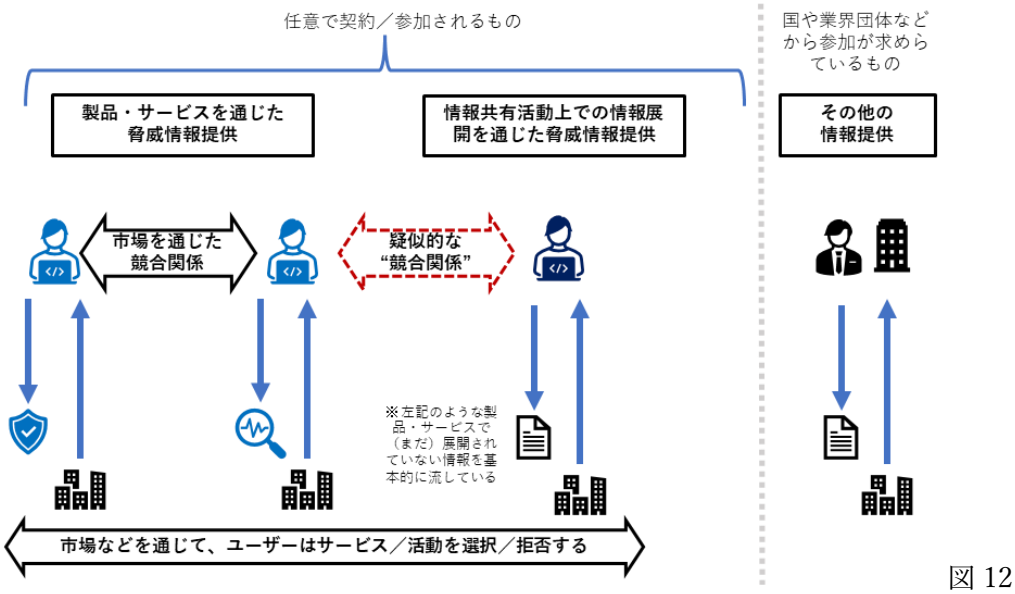


図 12

C：被害組織への支援や調査を行う上で、自組織の知見が不足していないかについて知ること（平時からの取組として）

A にて解説した通り、検知回避や解析妨害といった攻撃の「高度化」や、さらに脆弱性の悪用や正規の IT サービス／プラットフォームの悪用など複数の利害関係者が絡み「複雑化」する中において、あらゆる攻撃類型に対して最適な対処を行うための知見や機能を単独組織で維持し続けることが困難になっています。他方で被害組織の立場からすると、どの相談先が当該攻撃に最適な知見／能力を有しているのか事前に知ることはできません。さらに、被害組織から相談を受けて事案に最初に対応する「ファーストレスポンダー」である専門組織に当該攻撃に対する十分な知見がない場合でも、当該組織自身が自ら

の初動対応内容に知見的な不足があること自体を認識できていないため、結局対応に不備があるまま放置されてしまいます。「ファーストレスポンダー」組織も、偶然、当該事案の相談が来ただけであり、そもそも日頃から情報共有を行っていなければ、「自組織が何を知らないか」知る術がありません。

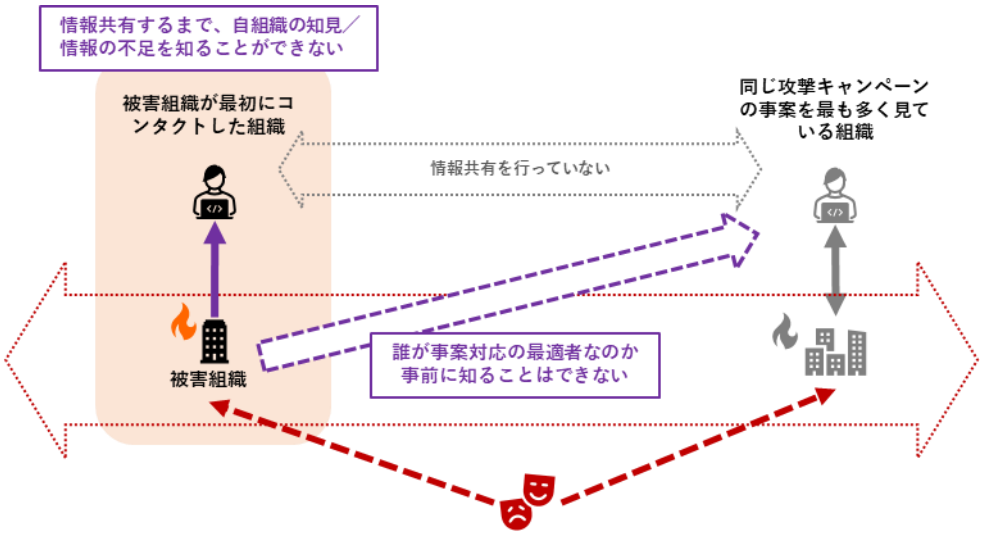


図 13

そこで、平時から他の専門組織と情報共有活動を行い、当該時点において自組織に足りない知見を認識するとともに、被害組織より十分な対応経験がない事案に関する相談が来た場合に、現在進めている対応内容で十分なのか照会をかけることが必要になります（A にて解説した通り）。

D：脅威アクターを中長期間にわたり追跡するために、自組織では不足している情報を情報共有活動で補うこと

特定の脅威アクターを追跡し、これへの最新の知見を備え、提供する製品・サービスで速やかな検知・対処ができることは当該専門組織の優位性を示すものとなり、また、各専門組織に所属するアナリストにとってもコミュニティ内外における成果となるため、いずれにせよ、専門組織では積極的な情報の入手が行われています。ただ、これも A や B に同じく、単独のアナリスト、単独の専門組織だけでは情報の入手に限界があるため、競合性を損なわない範囲において、専門組織同士の情報共有が行われることが有益となります。

E：攻撃要素（脆弱性や攻撃インフラ）への対処のため、対処ができる適切な専門組織等へ対応依頼をするために、必要な情報を提供すること

フィッシングサイトやマルウェアサイトのテイクダウンについて、専門組織であれば、自ら国内外のホスティング事業者／ISP 等の Abuse 窓口に申告して対応するケースもありま

すが、水飲み場型攻撃における改ざんサイトや Abuse 窓口のない IT インフラ、調整経験のない Abuse 申請などの場合は、専門機関へ依頼を行う場合があり、この際に停止に必要な情報やその他状況説明として攻撃技術情報を提供することがあります。

＜参考：被害組織はなぜ情報共有活動に参加するのか＞

共有・公表ガイダンスで解説がなされていますが、攻撃者はセキュリティ製品での検知回避など攻撃を高度化させる中で、既存のセキュリティ製品・サービスで検知が間に合わないケース／タイミングが発生してしまうところ、製品・サービス間で差が発生してしまいます。ユーザー側は「自分の組織は、使用しているセキュリティ製品・サービスを通じて必要な脅威情報を入手できていないのか」知ることはできません。そのため、平時から情報共有活動に参加するニーズ／必要性が発生するのです。

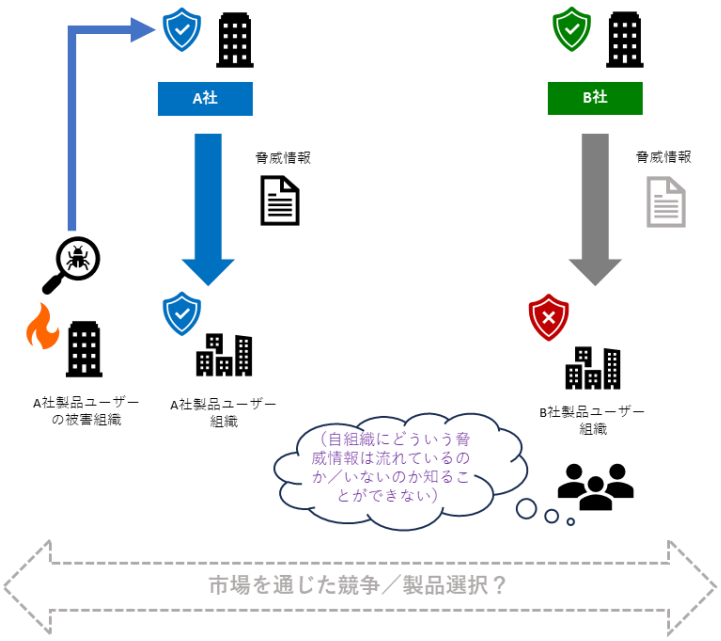


図 14

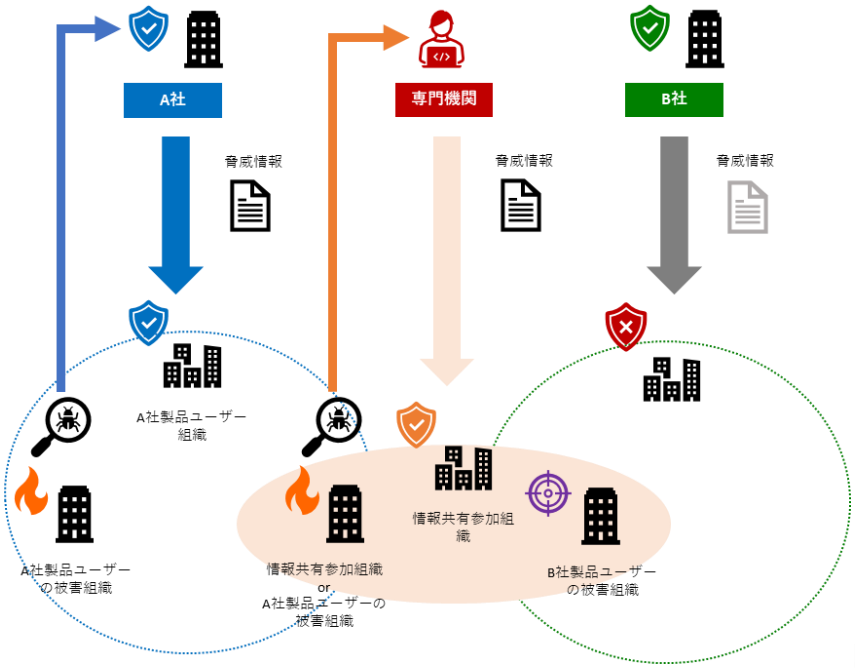

A社
専門機関
B社
脅威情報
脅威情報
脅威情報
A社製品ユーザー
組織
情報共有参加組織
A社製品ユーザー
の被害組織
情報共有参加組織
or
A社製品ユーザーの
被害組織
情報共有参加組
織
B社製品ユーザー
の被害組織

図 15

専門組織間の共有が有効でない場合と成功させる方法

＜情報共有が有効でない例：共有対象の選定の課題（1）＞

まず、大前提として、情報共有効果が見込まれるのは、限定された範囲に攻撃手法や攻撃インフラが使いまわされる攻撃活動に対してであり、

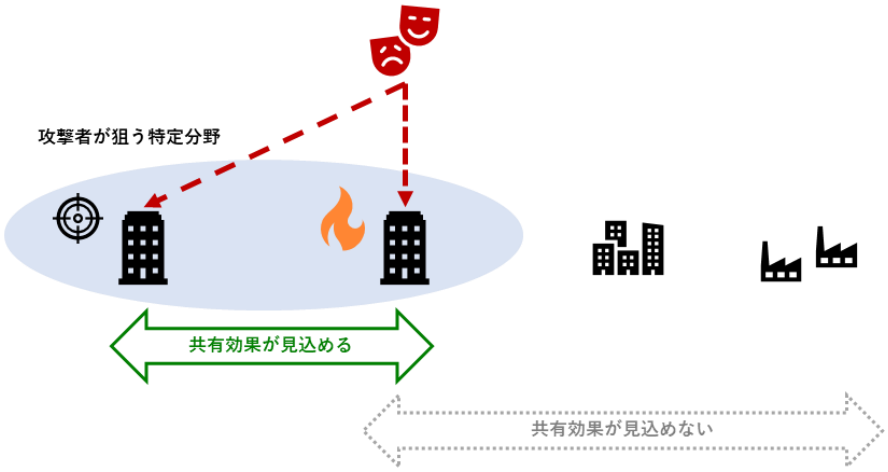


図 16

下記図のとおり、既に広範囲に攻撃や攻撃試行が発生していたり、複数の攻撃者により広く同様の攻撃手法が用いられている場合は、既に多くのセキュリティ製品／サービスで対処が可能であったり、あるいは、攻撃機関から注意喚起が発出されたり、レポート公表などの公開情報が流通し始めていることが想定されるため、被害組織同士や専門組織を介した非公開による情報共有はそれほど効果が見込めません。

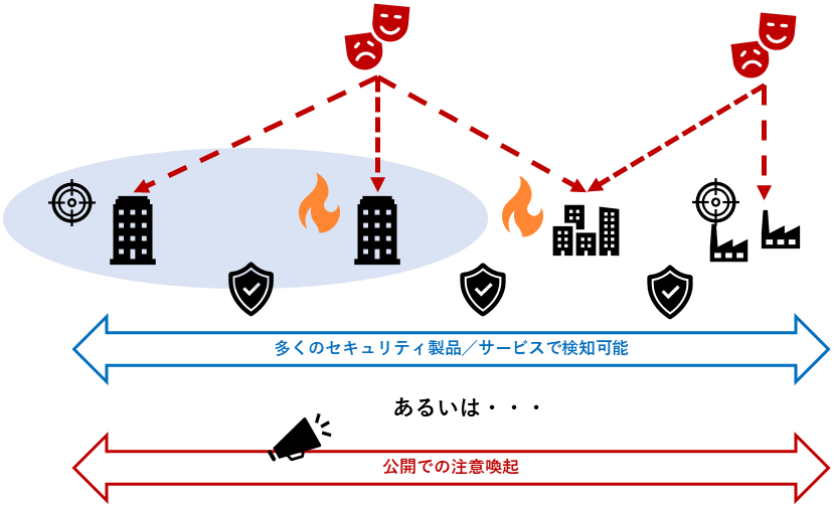


図 17

＜情報共有が有効でない例：共有対象の選定の課題（２）＞

専門組織同士の情報共有において、共有対象とする攻撃を受ける／受けている可能性のある分野や攻撃対象システムのユーザーの範囲をそれぞれ見ている専門組織間では情報共有効果が見込めますが、標的となっていない分野や標的となっていないシステムのユーザーの範囲を主に見ている専門組織との間では共有効果は見込めません。

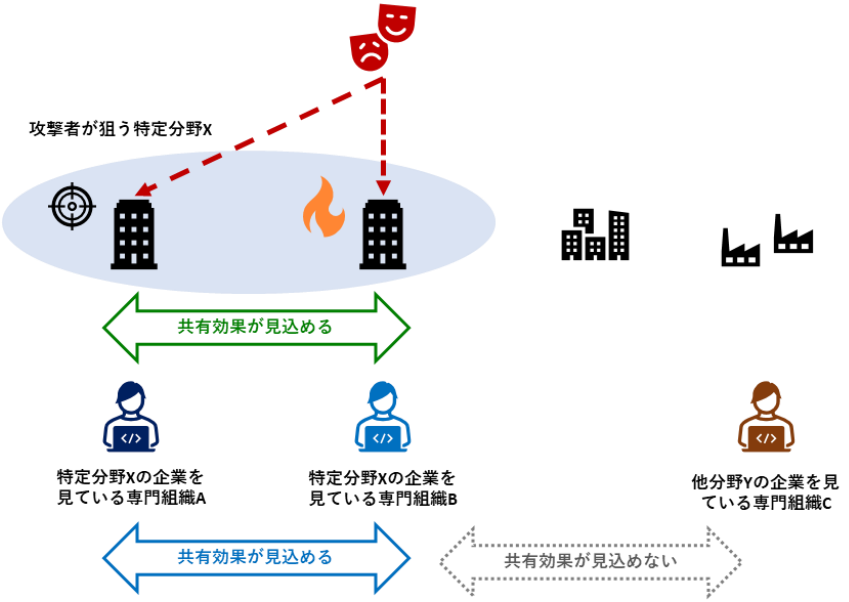


図 18

また、共有対象／共有効果の見込める類型の攻撃をそもそも観測／対応できる専門組織間でなければ、共有活動が成立しません。

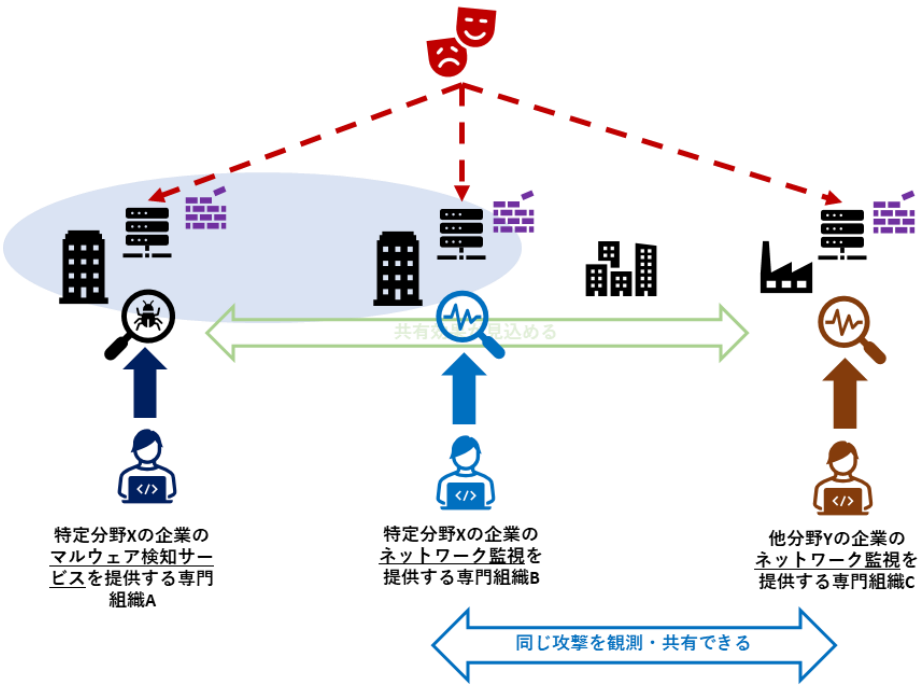


図 19

＜情報共有が有効でない例：共有先地域の選定の課題＞

なお、本稿のスコープは国内組織ですので参考となりますが、異なる地域間での情報共有の場合、そもそも活動する攻撃者／攻撃活動がまったく異なっているケースも多いため、情報共有が有効なケースが少ないという事情があります。
地域を跨いで被害が発生する APT キャンペーンなどもありますが、複数地域に攻撃が行われるものの多くは広範囲／無差別な攻撃が多く、情報共有するまでもなく注意喚起やレポート公表などの公開情報での情報流通やセキュリティ製品／サービスを通じた情報展開が行われます。

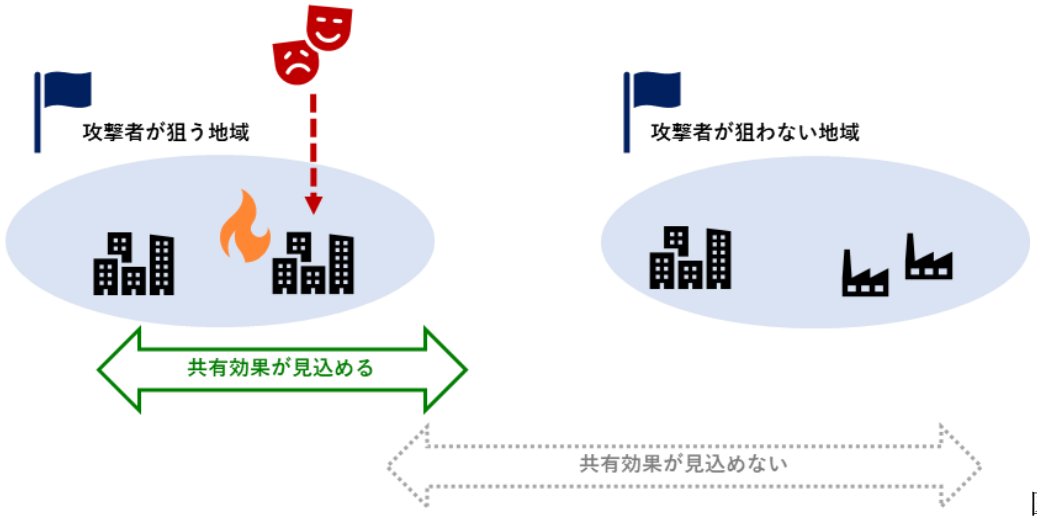


図 20

＜情報共有が有効でない例：伝達方法の課題＞

また、以下も主に地域間の情報伝達で想定されるケースですが、ある地域／分野内の情報共有活動で得た情報を地域外／分野外の専門組織に伝達する場合、当該情報提供元である専門組織と地域外／分野外の専門組織との間（専門組織 A-C 間）で直接のやりとりが行えないため、技術的な質疑や情報の精査が行えない問題が発生します。
組織 B が当該情報を専門組織 C に伝達すべき技術的理由や攻撃動向などを把握できていれば、さほどの問題は発生しませんが、本来、共有効果がない／共有の必要性が必ずしもない情報を組織 B が専門組織 C に伝達した場合、事情等がわからない専門組織 C は当該情報にどのように反応し、また、自ら受け持つ地域／顧客等にどのような対応を行えばよいのか判断できなくなるのです。

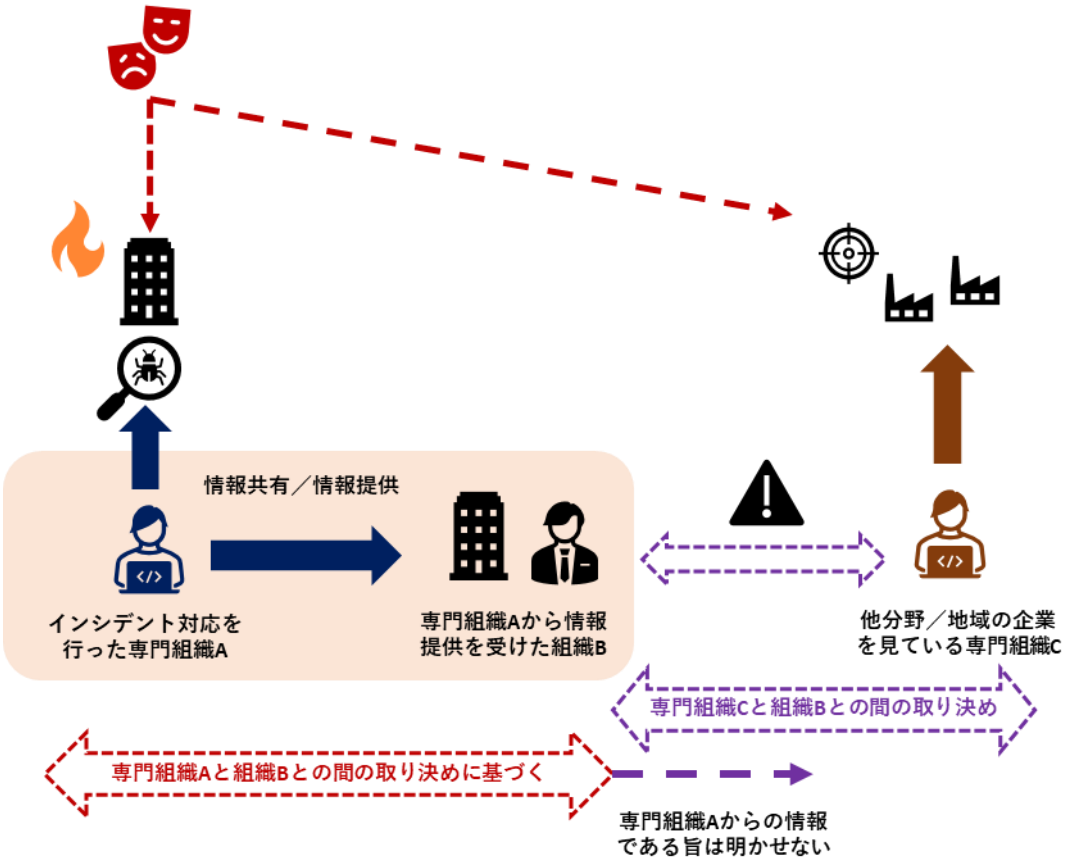


図 21

＜専門組織同士の情報共有を成功させるために＞

上記のような状況を回避する方法としては、

A：攻撃類型別／製品・サービス別／地域別に共有活動を行う
B：ハブ組織を通じた間接的な情報共有を行う

といった方法が考えられます。

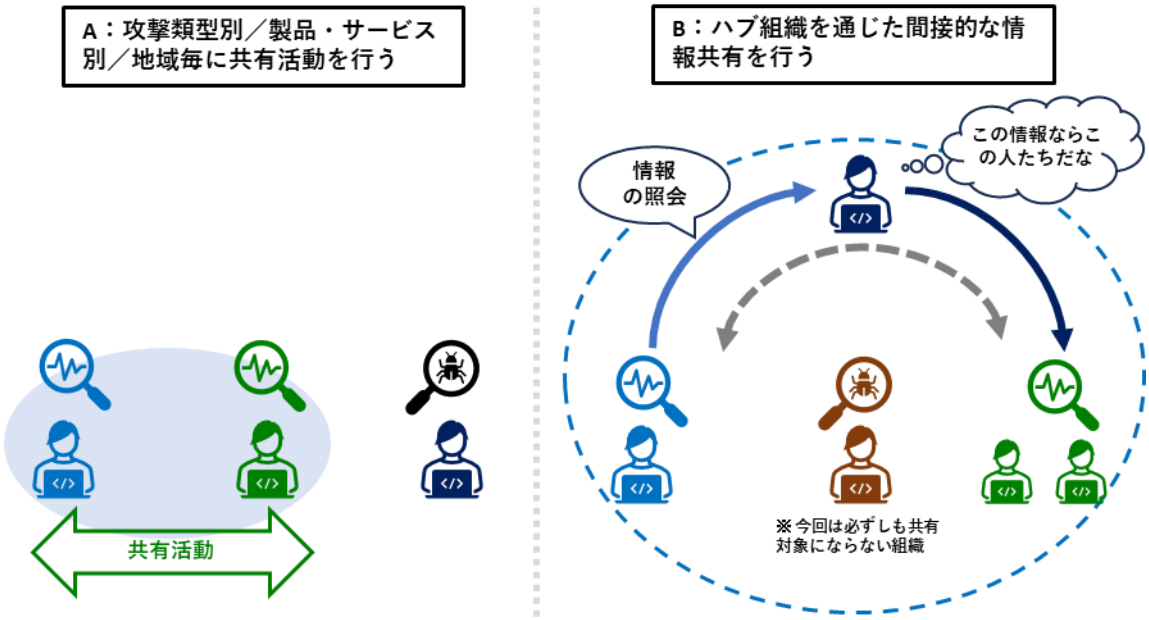


図 22

A のメリットとしては、前述のようなミスマッチを減らせる点がありますが、デメリットとして、幅広い攻撃類型に対応している専門組織や、複数の製品・サービスを通じて攻撃技術情報を扱っている専門組織からすると、攻撃類型別や製品・サービス別に複数の活動に参加しなければならない点が挙げられます。

B のメリットとしては、A のデメリットのように複数の活動に参加しなくてよいという点がありますが、デメリットとしては、共有活動の活性が当該情報のハンドリングを行うハブ組織の知見／能力に依存する点があります。

どうやって共有するのか

専門組織同士が情報共有する方法としては、

(a) 組織として情報共有活動に参加する

(b) アナリスト単位でコミュニティ活動を行う

(c) ハブとなっている組織に情報提供する

(d) その他個別に連携を行う

(e)（不）特定多数向けの情報発信を通じて間接的に行う

が挙げられます。

(a)組織として情報共有活動に参加する

例えば、サイバーセキュリティ協議会の「第一類」と呼ばれるグループには、セキュリティベンダや専門組織が参加しており、「自組織単独ではまだ確証を得るに至っていない専門的な分析内容等を積極的に提供し合い具体的な対策情報等を作出していく」[3]ことが役割として規約等で定められています。

(b)アナリスト単位でコミュニティ活動を行う

専門組織のアナリストの中には、ある程度個人として対外的に活動している場合があり、こうしたアナリストが組織から裁量として認められた範囲において他組織のアナリストと情報交換を行う場合があります。こうした活動は(a)のような場を通じて行われることもあれば、非公式なアナリスト同士のクローズドコミュニティにて行われる場合もあります。

(c)ハブとなっている組織に情報提供する

国内外の複数の専門組織／アナリストコミュニティと接点を有する専門組織を通じて、同

[3] https://www.nisc.go.jp/pdf/council/cs/kyogikai/kyogikai_gaiyou.pdf

じ事案に対応／脅威を追跡している、面識のない個々の専門組織／アナリスト間で間接的な情報交換が行われる場合があります。これは最初から専門組織／アナリストがそのように希望してコンタクトするものではなく、下記(d)で解説する、個別による情報連携の過程で、同じ脅威に関する複数の専門組織／アナリストから情報を受けったハブ組織側で調整を行うことで実現されます。

また、こうしたハブ組織を通じた「非特定化」のメリットもあります。
例えば、被害組織と当該専門組織の関係性が第三者に容易に推測されるような場合（子会社であったり資本関係があったり、そのほか当該事案に当該専門組織が調査にはいっていることが知られている／推測される場合)、当該専門組織が専門組織同士の情報共有活動やその他情報共有活動に情報提供した時点で、当該被害組織の存在が推測されてしまう可能性があります。
こうした推測を避けたい、という場合、情報共有ハブ組織を介した情報共有活動への情報提供を行うことで、さらなる非特定化への配慮を行うことができます。

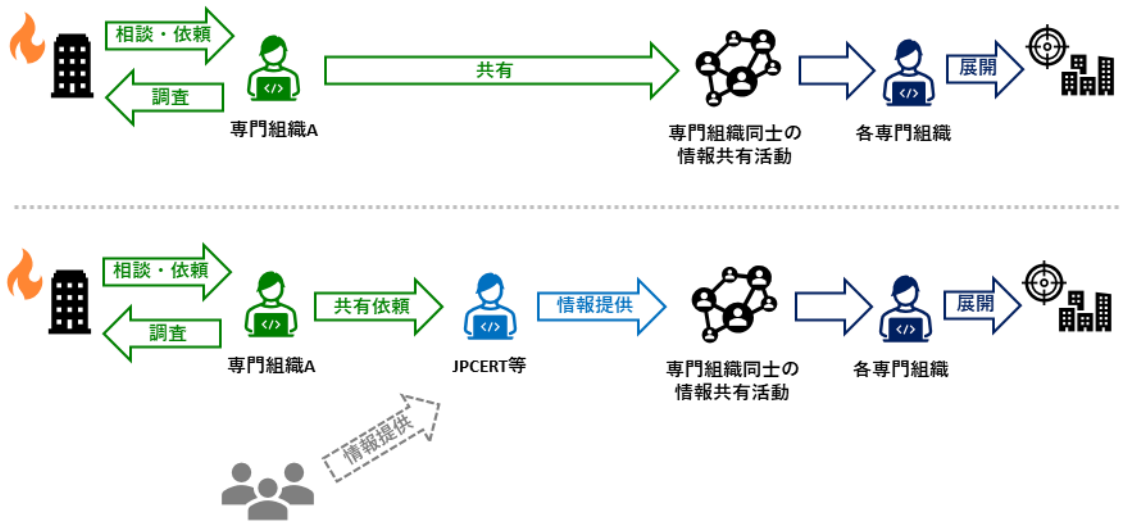


図 23

(d)その他個別に連携を行う

(a)や(b)のような活動に参加していない専門組織／アナリストや、当該脅威に関する情報をどこ／誰と情報共有すればあらたな知見が得られるのかわからない場合、ひとまず(c)の可能性を想定してハブ組織に情報提供する場合があります。そこからフィードバックを得たり、あるいはハブ組織が代行として(a)(b)を積極的に行うことでフィードバックが来る場合があります。

(e)（不）特定多数向けの情報発信を通じて間接的に行う

レポート公表や国際カンファレンスでの発表等を通じて、攻撃技術情報が公開されますが、こうした情報発信も中長期的な専門組織間の（間接的な）情報共有の一つであり、間接的な情報の交換と知見の補完だけでなく、これらの発表前後に個別にコンタクトを取ったり、あるいは(a)(b)の活動と併用して用いることで、特に脅威アクターの追跡に関する知見を補完することになります。
レポート発表だけでは、情報の共有まで時間がかかってしまうので、より早い段階での(a)～(d)での情報共有と組み合わせることが必要です。

＜担当者に必要な権限／情報が与えられているか？＞

専門組織間の情報共有活動に限らず、情報共有活動は専ら参加各組織の担当者同士が対面又はハブ組織を通じて、ポータルシステムやメール、会合等を通じて情報交換を行う活動です。

各担当者が自社で持っている情報を外部に示す権限がなければなりませんし、そもそも必要な情報が情報共有活動の窓口担当者に伝達されていなければ意味がありません。
さらに、自社で持っている情報について他の参加組織（の担当者）から問われたときにどこまで回答してよいのか、ある程度権限が与えられていなければ速やかな応答ができず、情報共有に有効なタイミングを失してしまう可能性があります。

例えば、ある企業ではSOC部門とインシデント対応支援を行う部門の2部門で顧客先の事案に対応しているところ、情報共有活動には SOC 部門の担当者を参加させているとします。この時に、SOC 監視で見た統計的な情報や被害組織が非特定化された個別の攻撃観測情報について情報共有できる権限を担当者に与えていましたが、他の情報共有活動参加組織から「こういう攻撃は観測していますか？どのくらい観測していますか？」という質問が来た際には一度、自社に持ち帰って回答可否を検討する、という手順になっていた場合、タイムリーな共有ができません。また、インシデント対応支援部門で得た情報はこの担当者が扱えないままであると、共有可能な情報、フィードバックを得られる攻撃類型／分野等が制限されてしまいます。

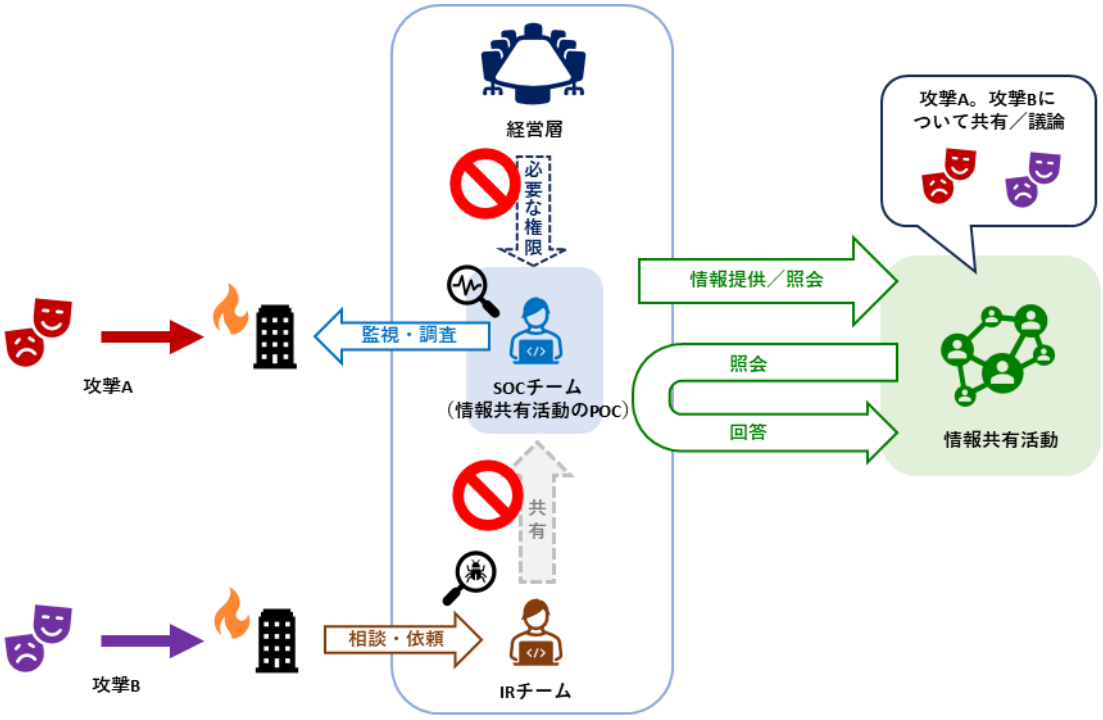

経営層
必要な権限
攻撃A。攻撃Bについて共有／議論
情報提供／照会
監視・調査
攻撃A
SOCチーム
（情報共有活動のPOC）
照会
回答
情報共有活動
共有
相談・依頼
攻撃B
IRチーム

図 24

いつ共有するのか

専門組織同士の情報共有の目的として、自組織では不足する情報を補い、支援先被害組織の速やかな初動対応を進めたり、あるいはこれから攻撃を受ける可能性のある他の顧客等の被害未然防止／被害拡大防止を意図する場合、可能な限り早期に情報共有することが必要になります。

他方で、共有・公表ガイダンスの 73 頁でも解説があり、また、ISOG-J「セキュリティ対応組織(SOC/CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」」[4]15 頁でも紹介されていますが、速報性と正確性はトレードオフの関係であるため、調査の初期段階での外部との情報共有に躊躇するケースも少なくありません。専門組織／アナリストであればこそ、「技術的に正確な情報を外部に提供したい」を考えてしまいがちです。

とはいえ、正確性を期すための調査／精査を待ったことで、情報共有に適したタイミングを逃し、攻撃技術情報の“鮮度”（共有効果を参加組織がお互いに得られる期限）が落ちてしまっては本末転倒です。

また、ある程度のタイミングを過ぎると、様々な被害現場で見つかった情報が VirusTotal への検体アップロードやこれを見つけた研究者などによる解析といった形で攻撃技術情報として流通／拡散を始めます。

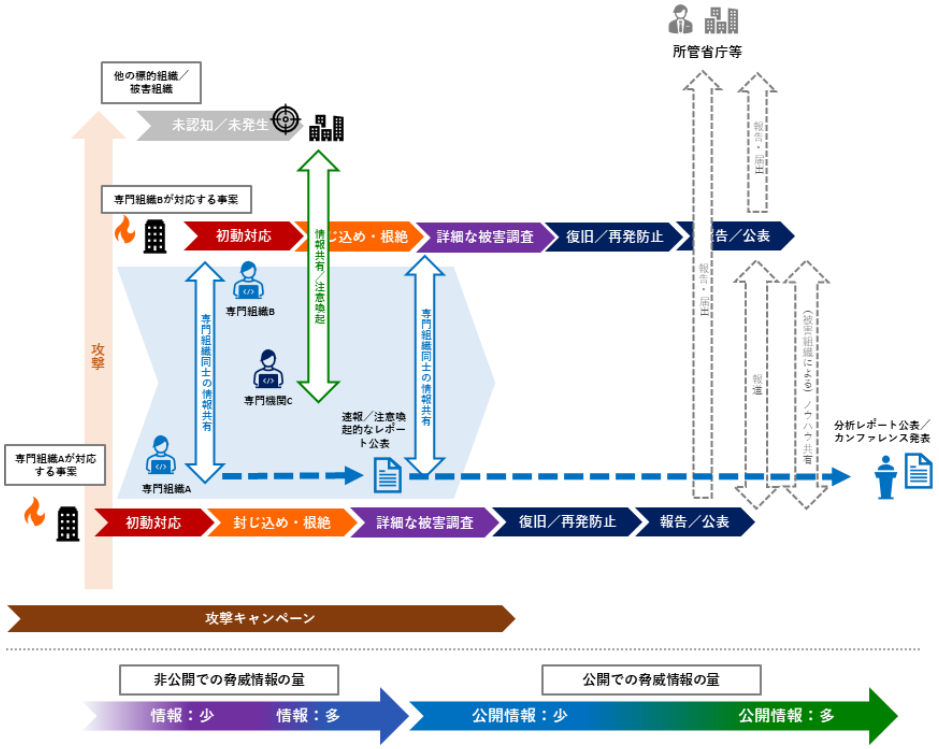
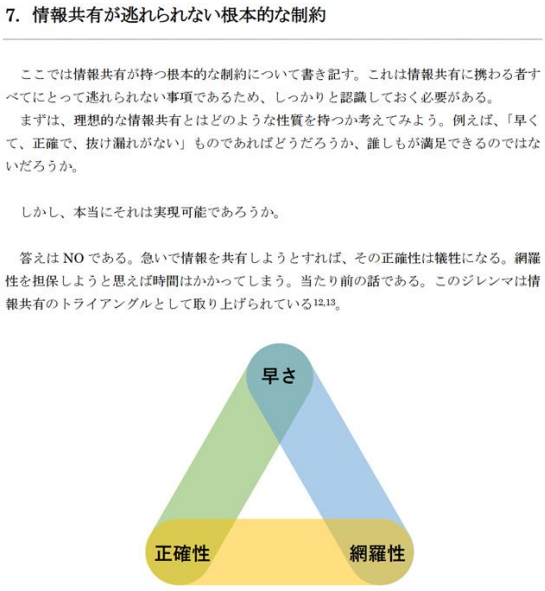


図 25

[4] https://isog-j.org/output/2017/5W1H-Cyber_Threat_Information_Sharing_v1.html

正確性を優先すべきか、スピードを優先すべきか

先に紹介した、ISOG-J「セキュリティ対応組織(SOC/CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」」でも解説されているとおり、より早く情報共有しようとすれば、正確性や網羅性が確保できない状態での情報共有／提供を行わざるを得ません。



7. 情報共有が逃れられない根本的な制約

ここでは情報共有が持つ根本的な制約について書き記す。これは情報共有に携わる者すべてにとって逃れられない事項であるため、しっかりと認識しておく必要がある。

まずは、理想的な情報共有とはどのような性質を持つか考えてみよう。例えば、「早くて、正確で、抜け漏れがない」ものであればどうだろうか、誰しもが満足できるのではないだろうか。

しかし、本当にそれは実現可能であろうか。

答えは NO である。急いで情報を共有しようとすれば、その正確性は犠牲になる。網羅性を担保しようと思えば時間はかかってしまう。当たり前の話である。このジレンマは情報共有のトライアングルとして取り上げられている[12,13]。

図 4　情報共有のトライアングル

図 26

（ISOG-J、「セキュリティ対応組織 (SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」」、2017 年 10 月 27 日）[5]

とはいえ、前項のとおり、専門組織同士の情報共有として効果が得られる大半は攻撃キャンペーンが継続している事案対処初期の段階であるため、「正確性／網羅性が担保できないが、速報性を優先した情報共有」が求められます。この場合、正確性／網羅性が担保されないことを補いながら、特に誤った情報が拡散しないようにするために以下の対策を行うことが求められます。

対策１：情報共有（提供）の際に当該情報のソースを明らかにする

対策２：（専門組織同士の）情報共有活動に提供する情報について、「正規サービス／正規ファイル」情報のコンタミネーションが起きないように最低限のチェックを行う

[5] https://isog-j.org/output/2017/5W1H-Cyber_Threat_Information_Sharing_v1.0.pdf

対策３：（専門組織同士の）情報共有活動に提供した情報が未精査のまま、第三者へインディケータ情報として展開されないようにする

対策４：情報共有活動におけるフィードバックを通じて網羅性を補っていく

対策１：
情報共有（提供）の際に当該情報のソースを明らかにする

本手引きが主なスコープとする速やかな情報共有においては、情報提供としての被害組織名を明かすことはできませんので、以下のいずれかのような表現で情報のソースを示します。

・直接被害現場で確認した情報である旨を示す
・直接被害現場で確認した情報ではなく、公開情報で得た情報（VirusTotal 上の検体など）である場合、直接の悪用被害を確認していない旨などを示す
・自組織が直接対応している被害先からの情報でない場合や自組織のセンサーによる情報ではなく、第三者から提供された情報を情報共有する場合は、第三者から提供された旨を示す
・直接被害現場で確認しているが、（当該時点で）当該ソース元の被害組織由来の情報を共有できない場合、その旨を示しつつ、公開情報として存在する同じ情報を使って伝達する（こうした場合の具体的な共有／伝達方法については、「通信先情報の共有のポイント」を参考）

対策２：
（専門組織同士の）情報共有活動に提供する情報について、「正規サービス／正規ファイル」情報のコンタミネーションが起きないように最低限のチェックを行う
※特に、対策１のように、自組織で直接悪用被害（現場）を確認できていない場合

マルウェアの隠蔽／検知回避戦術として、プロセスハロウィングや DLL ハイジャッキングなどの方法が多用されるようになったため、インディケータ情報や TTPs 情報に正規のファイル名／プログラム名が掲載されることが多くなりました。また単純にアンチウイルスソフトが誤検知したファイル等の情報が未精査のまま共有情報として流れてしまう場合もあります。精査する時間よりも共有のスピードを優先するとはいえ、こうした情報のコンタミネーションは最低限避けるべきであり、展開すべき情報と判断しつつも、未精査であるため、正規ファイルやグレーなプログラムを誤検知しているだけの可能性も考えられる場合は、その旨を付記して共有することが望まれます。

対策３：
（専門組織同士の）情報共有活動に提供した情報が未精査のまま、第三者へインディケータ情報として展開されないようにする

自組織では未精査な情報であっても、専門組織同士の情報共有効果として、「他の組織は既に調査・分析が先行しているかもしれない」ことへの期待とフィードバック（精査される効果）があるわけですが、必ずしもすべてのケースでこうした効果を得られるわけではありません。
その場合、自組織が提供した情報にそれ以上の追加情報が得られないまま、あるいは精査されないまま、共有先の専門組織を通じて第三者に情報展開がされる場合があります。

情報の未精査により、誤った情報のコンタミネーションが発生してしまった場合、自組織の情報展開先（製品・サービス提供先など）だけでなく、自組織が関与しない第三者にも影響が及ぶ可能性があるため、他の項目にあるコンタミネーション回避の対策だけでなく、情報共有活動内のプロセスとして、未精査情報の再展開を避ける手順／ルールの構築や、他の専門組織によるチェックを明示的に刈り取るなどの運用上の工夫が求められます。

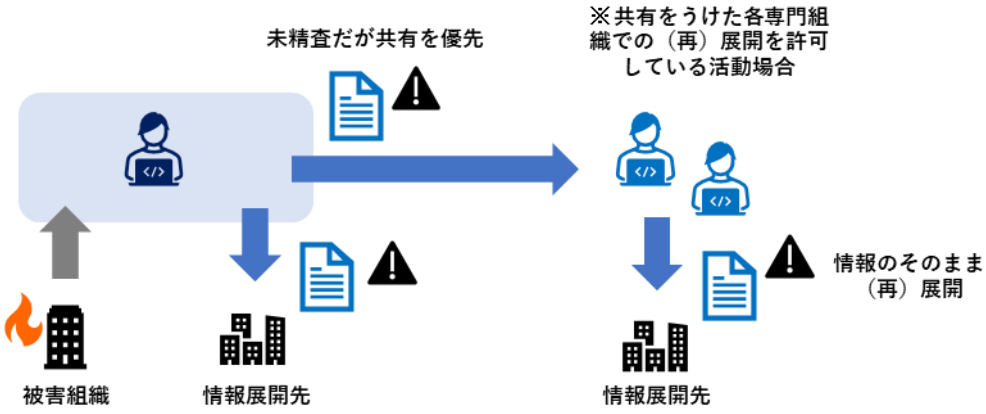


図 27

対策４： 情報共有活動におけるフィードバックを通じて網羅性を補っていく

本手引きの基本的なテーマですが、攻撃の高度化・複雑化により、そもそも単独組織だけで攻撃の全容を解明することが困難な事情があります。そのため、情報の網羅性も単独組織で達成しようとするのではなく、専門組織間の情報共有を通じて情報が補われることで、ある程度の網羅性が担保されれば十分と考えられます。

情報受信者側の対応コストを減らすためのポイント

＜問題＞

「サイバー攻撃による被害に関する情報共有の促進に向けた検討会」（以下、「検討会」という。）で取り上げたとおり、公開情報を始め攻撃技術情報の流通が増え、様々なプレイヤーが攻撃技術情報に触れたり、情報発信したりする機会が増える中で、既に公開されている情報や製品・サービスを通じて流通している情報が別途情報共有活動に流れて、受信者側（潜在的な被害組織／標的組織）にログ確認等の二度手間を発生させているケースがあります。

あるいは、公開情報ベースの情報で不正確であったり誤っている情報が混在して展開されるケースもあり、「情報共有活動の活性化」の一報で、受信者側のコスト負担も問題になっています。

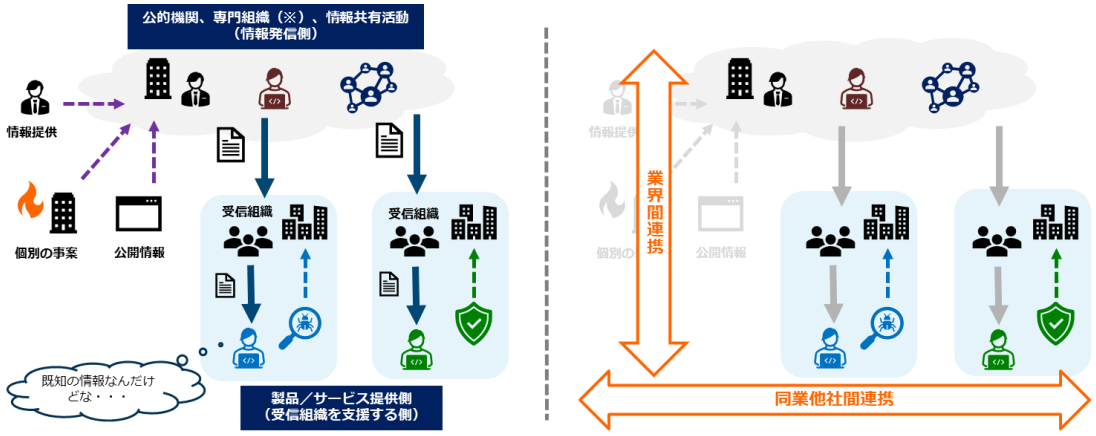


図 28

＜対策のポイント＞

上記のような受信者側のコスト負担を増やさないために、情報展開を行う専門組織側、あるいは情報展開前の専門組織同士の情報共有においては、以下のような対策が求められます。

ポイント１：公開情報や多数の製品・サービスで既に流通している攻撃技術情報の「再展開」はなるべく減らす

ポイント２：攻撃が確認されている時期やログ上の調査を推奨する期間を示す

ポイント３：具体的な対応方法をセットで示す

ポイント４：基本的には自組織あるいは共有先の他の専門組織が被害を確認している情報を展開する

ポイント１：
公開情報や多数の製品・サービスで既に流通している攻撃技術情報の「再展開」はなるべく減らす

VirusTotal 上での各エンジンの検知状況情報や、その他公開情報としてどの程度当該攻撃技術情報が拡散しているのか把握することが必要です。
他方で、例えば、新たなマルウェアについて SNS 上で研究者や海外セキュリティ専門企業が情報発信したり、あるいは VirusTotal 等の公開解析サービス上に検体がアップロードされていたとしても、その直後ではまだ多くの製品・サービスで検知が間に合っていなかったり、当該検体を用いた攻撃の初期侵害経路などの TTPs を取り急ぎ伝えなければ、被害拡大防止を図れないケースもあります。そういった場合は攻撃技術情報の大半が既に公開状態であるとはいえ、別途、情報共有活動を通じた情報展開もなお有効と考えられます。

また、上記のとおり、公開されている攻撃技術情報だけでなく、これに関連する非公開情報をセットにしたものであれば、なお情報共有／情報展開の対象として価値があると考えられます。

ポイント２：
攻撃が確認されている時期やログ上の調査を推奨する期間を示す

インディケータ情報を展開する場合、受信者側の対応コストを最小限にするためにも、「どの期間の侵害有無を調査すればいいのか」示すことが必要です。

これは、ポイント１とも大きく関係します。
既に通信先やマルウェアに関する情報が事案対応に当たった専門組織からレポート公表されているにもかかわらず、いまだ検知／被害認知ができていない被害組織が存在するケースが多く存在しています。これは、ファイルレス攻撃などによりエンドポイント側でのマルウェア検知だけで被害認知できないケースが増えていることや SOC 監視がない他、プロキシ／FW 側での不正通信のモニタリングを行っていない組織や対応に不足がある組織が存在するためです。
そうした、「既に公開情報も出ているが過去／直近の攻撃をまだ検知できていない組織（層）」向けには、公開情報であったとしても、過去／直近のいつからいつまでの期間を調査せよ、とインディケータ情報を、情報共有活動を通じて展開する必要が出てきます。

ポイント３：
具体的な対応方法をセットで示す

攻撃方法だけを示して、具体的にどのような対応／調査をすればいいのか、受信組織側で考えなければならないような情報発信は控えるべきです。
脆弱性情報であれば修正方法や、修正方法が未提供の場合の暫定的な回避策を示し、インディケータ情報であればどのログをどのくらいの期間、調査すべきか示すことが必要です。
また、対策や調査方法が現実的に困難なものと思われる場合、そのまま情報を流すのではなく、専門組織同士の情報共有活動を通じてさらなる知見を得て、より実施可能なレベルまで検討した上で情報展開をすることが求められます。

ポイント４：
基本的には自組織あるいは共有先の他の専門組織が被害を確認している情報を展開する

第三者から提供された情報を他の組織に共有すると、技術的に正しいコミュニケーションが取れなかったり、共有／展開情報に不正確な情報のコンタミネーションが起きるなど、問題になりやすい傾向があります。基本的には自組織自身で確認した情報を展開するようにするとともに、匿名希望の第三者の情報を代理的に展開するのであれば、前述のとおり、情報展開前に専門組織同士の情報共有などを通じて内容の精査を行うことが望まれます。

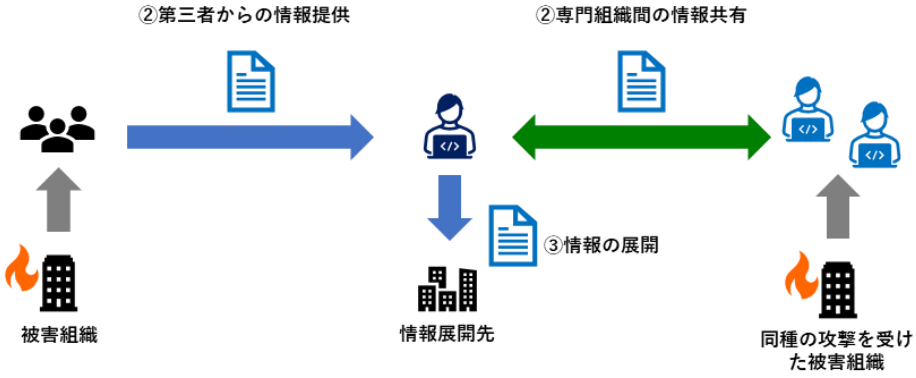


図 29

攻撃技術情報共有時の被害組織との間の問題点は何か

専門組織が他の専門組織や情報共有活動との間で情報共有を行う際に被害組織との間で問題になるのは

（1） 共有しようとする情報が秘密保持契約（以下、「NDA」という。）上の「秘密情報」に当たるとして共有許可が得られない（又は、そのように解釈して共有を行わない）

（2）共有した情報から被害組織が推測されてしまうことへの懸念が被害組織から上がる

の 2 点です。

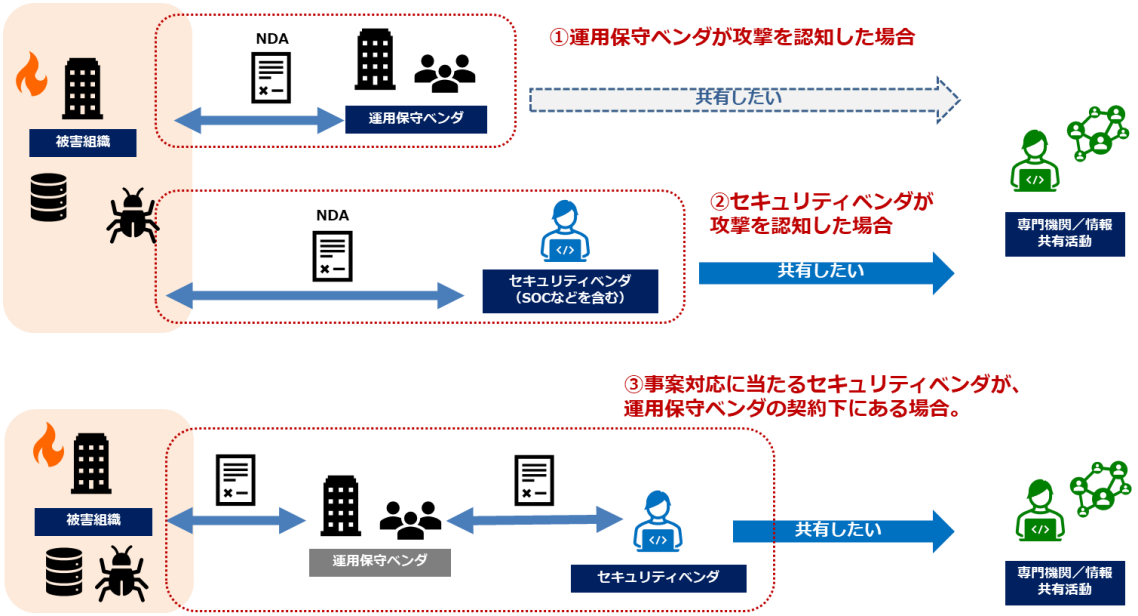


図 30

検討会では、まず（1）について、情報共有対象となる「攻撃技術情報」（☛定義は 6 項参照）について、基本的に被害組織が特定される情報は含まれないため、専門組織の判断で他の専門組織への速やかな情報共有が可能な対象となり得ると整理しました。詳細は次項をご覧ください。

また、（2）については、被害個社名等を推測可能な情報を除いた、非特定化加工した情報についても、情報共有対象とできると整理し、本手引きにより、被害組織が特定／推測されないための非特定化加工のポイントについて解説することとしました。

攻撃技術情報の性質

本手引きでは、検討会の検討結果を踏まえ、攻撃技術情報の取扱いについて以下のような整理を行っています。

被害組織から専門組織が受領したフォレンジック調査対象のデータや専門組織が被害組織に提供するセキュリティ製品・監視サービス等を通じて得たデータを分析したことで得られる攻撃技術情報のうち、被害組織が判明しないように非特定化加工された情報については基本的に第三者への提供を行うことができるものである。

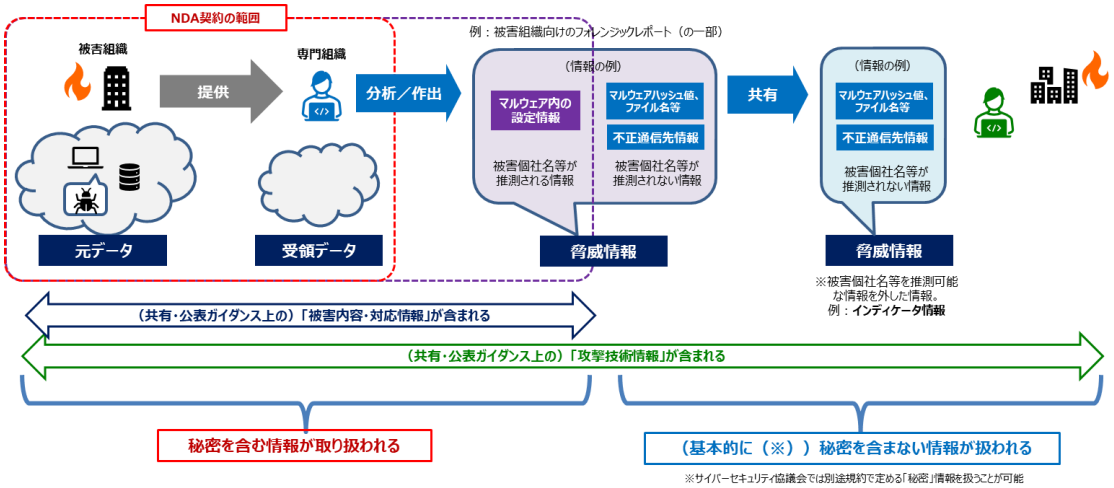


図 31

（サイバー攻撃による被害に関する情報共有の促進に向けた検討会最終報告書より抜粋）

＜公知の情報について＞

既に分析レポート等を通じて通信先やマルウェア等に関する情報が公知となっている場合は、専門組織の判断で第三者と攻撃技術情報を共有することができます。
他方で、「公知」とまでは言えないものの、インターネット上で「公開」されてしまっている情報については、基本的に公知の情報と同じ扱いができるものの、後述のとおり、被害組織が特定されてしまう情報を含んでいる場合が存在するため、これらの留意点を踏まえた取扱いが必要になります。

○公開情報ではあるが公知の情報ではない例：C2 サーバ上のペイロード検体

C2 サーバ上にマルウェアのペイロードなどが蔵置されており、被害現場の調査で当該 C2 サーバの存在に気付いた専門組織がアクセスすると当該ペイロードを入手できる場合があります。

多くのケースではその前段のダウンローダー等の解析結果をもとに何らかの認証情報を含むなど、一定条件のアクセスを行わなければ当該ペイロードをダウンロードすることができないケースが多いため、広く不特定多数の者がこれを入手できるものではありませんが（公知ではない）、インターネット上の公開サーバ上にある公開情報であり、当該専門組織以外の者がアクセスする可能性が十分にあります。

また、C2 ハンティングであったり、他の通信先情報を認知した他の専門組織が PassiveDNS 情報等をともに関連のある当該通信先を探し出し、同様の方法でペイロードを入手するということも想定されます。

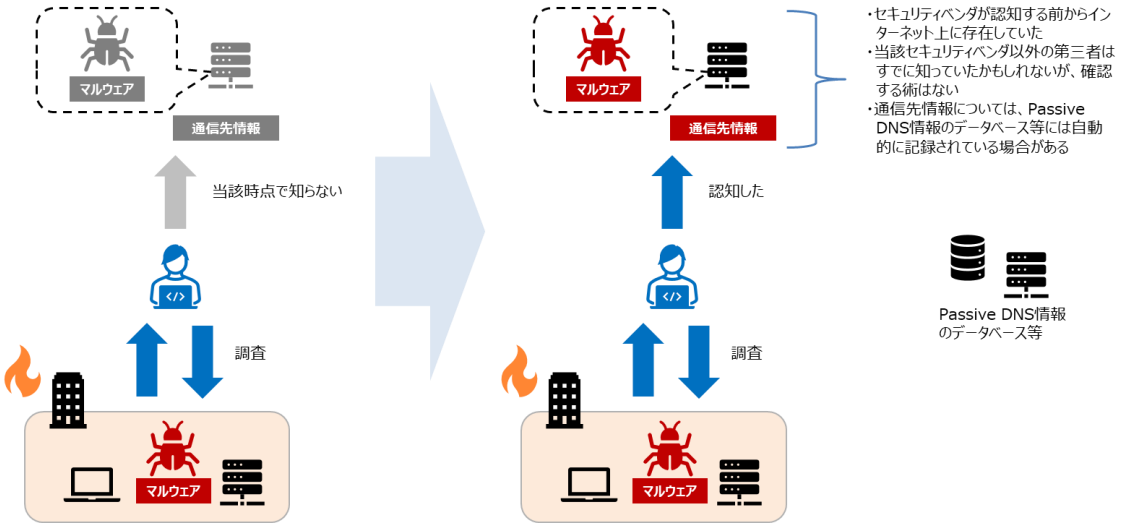


図 32

攻撃被害を示す情報の取扱いについて

「被害組織を推測させる情報」の他に、「攻撃被害を示す情報」があります。

① 不正アクセスにより漏えいした認証情報やその他内部情報
② 外形上認知可能なマルウェアが設置されたホストに関する情報や、改ざんされた Web サイト等に関する情報
③ 正規の Web サーバが改ざんされ、マルウェア配布サイトや C2 サーバとして使われていたり、正規のサービスが侵害されて、他の被害組織への攻撃の“踏み台”として用いられている場合

基本的な考え方については共有・公表ガイダンス「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 頁)、「“漏えい情報”は本当に現在の危険を示しているのか（93 頁）をご覧ください。①や②については、まず当該被害組織に情報が伝達される必要があり、被害組織への通知と被害対応支援に適切な専門組織への伝達以外に、必要のない組織に当該情報を正当な目的なく共有することは避けるべきです。③については、本稿第 3 章 56 頁「通信先が正規の Web サーバ等が改ざんされ悪用されたものである場合」をご覧ください。

通信先情報

通信先情報について

攻撃に関する通信先というのは基本的に
　A：不正な（不審な）アクセス元
　B：不正な（不審な）通信先
のいずれかであり、それぞれ、
　C：攻撃者が用意したサーバ
　D：正規のサーバ／機器を改ざんやマルウェア感染で悪用しているもの
　E：プロキシサービス等
のいずれかである。

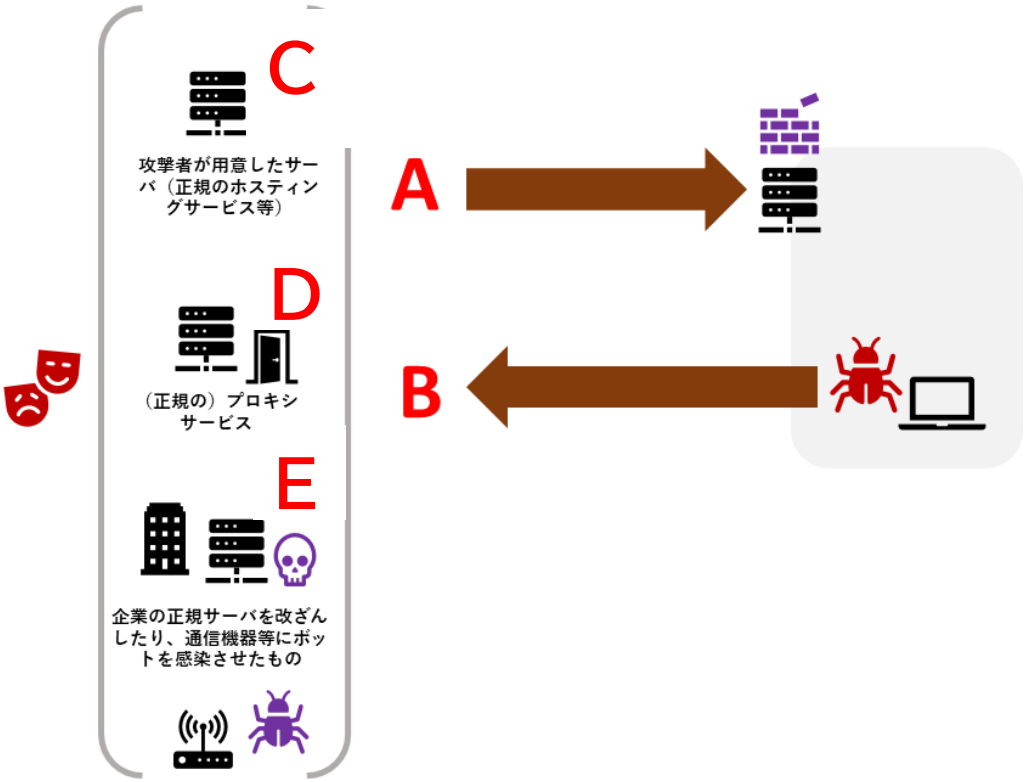


図 33

より早期に不正なアクセス元情報（A）を共有することで、他の標的組織によってはタイミングが間に合えば被害の未然予防につながり、マルウェアからの不正な通信（B）を共有することで、検知できていなかった攻撃を検知できるようになる可能性がある。

通信先情報の特性

下記図のとおり、通信先情報のうち、IP アドレスとこれに紐づくドメインに関する情報は大半が公開情報として流通しているため、完全な秘密性を有する情報とはならない。通信先情報を示す情報（IP アドレス、ドメイン（FQDN）、URL、通信が確認された時刻）というのは基本的に、第三者に知られたからといって、ただちに被害組織に不利益を与える情報ではない。したがって、基本的に秘密保持契約における秘密情報に含まれずに、委託先組織が外部との情報共有を行う際に当該情報を用いることはなんら問題ない。

ただし、後述のとおり、被害組織が特定又は推測し得るケースが存在するため、注意が必要である。

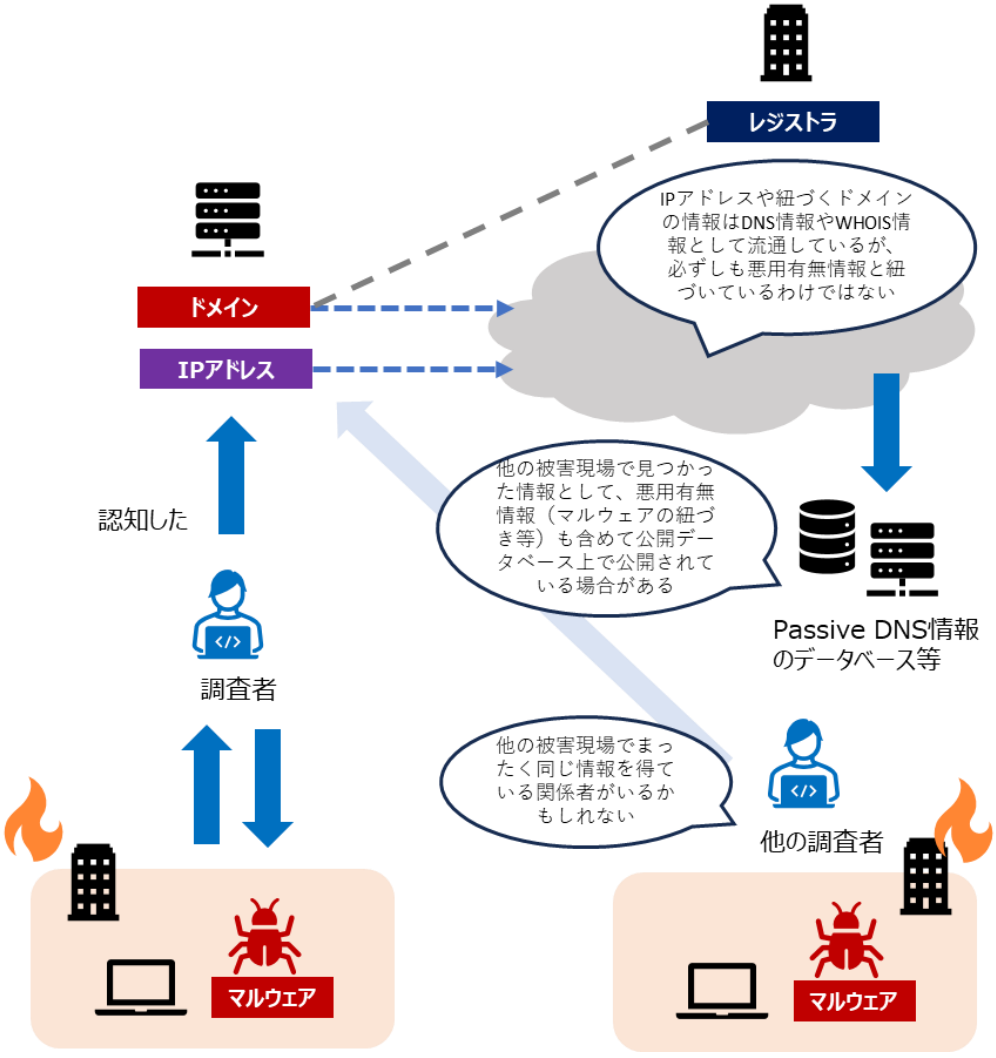


図 34

通信先情報の共有のポイント

＜通信先情報を何の目的で共有するのか＞

通信先情報を共有する目的としては、

目的１：他の専門組織に「どの事案／攻撃を自組織で見ているのか伝える」ための“識別子”的なものとして

目的２：自組織では把握できていない他の通信先情報や関連検体に関する情報を入手／交換するため

目的３：（目的１、目的２を通じて）自社顧客等にインディケータ情報を展開するため

目的１：
他の専門組織に「どの事案／攻撃を自組織で見ているのか伝える」ための“識別子”的なものとして

情報共有を行う場合、「どの攻撃に関する情報を共有（情報交換）したいのか」相手方に示す必要があります。
また、一つの事案／被害現場に間接的に重複して関与しているケースもあるため、「今から共有しようとしている情報の出所が相手と重複していないか」確認する必要も出てきます。
他方で、被害組織名を示して明示することもできず、また、事案対応初期の段階では情報も断片的で攻撃キャンペーン／グループの特定／命名も定まっていないため、「これから共有ようとしている、「自組織が対応する事案／攻撃活動を示す識別子」的な情報が必要になります。「識別子」的なものとしては、マルウェア情報、通信先情報、悪用された脆弱性情報、特徴的な攻撃手法、が想定されます。

後述のとおり、マルウェア検体は被害組織を特定できてしまう情報が含まれるケースがあるため、交換できないこともあり、また、VirusTotal 等にアップロードされていない場合、受け渡しが面倒であったり、解析結果のみを交換しても、被害組織ごとに検体のハッシュ値やファイル名、関連するプロセス名などが異なる場合もあり、同一の攻撃を特定するための情報としては役割不足な場合があります。

また、脆弱性の悪用や、攻撃手法に何らかの特徴（イニシャルアクセスで用いられる特徴的な侵害方法など）もない場合、残る「通信先情報」が「識別子」的情報の候補となります。

以下は、上記のような理由で検体情報を「識別子」として用いることができない場合を想定したものです。「通信先情報」を示すことで、同じ攻撃キャンペーンの異なる事案（被害組織）をそれぞれ見ていることを照会することができます。

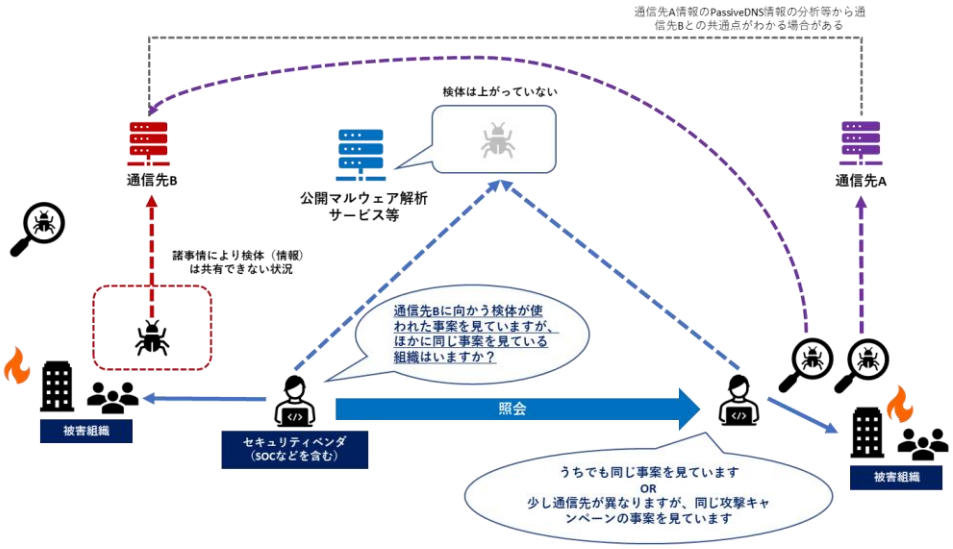


図 35

目的２： 自組織では把握できていない他の通信先情報や関連検体に関する情報を入手／交換するため

インシデント対応において、ネットワークフォレンジックを行っていても、すべての不審な通信を捕捉できないケースがあります。プロキシサーバがなく、IP アドレスベースで記録される FW ログしかなかったり、あるいは設定不備で感染端末からの不正な通信自体を記録できていないケースなども想定されます。

そこで、断片的であっても、現時点で把握している通信先情報を共有し、より多くの情報を先に把握している他の専門組織からのフィードバックにより、把握できていない通信先、さらには当該通信を発生させているマルウェア等を見つけていくことになります。

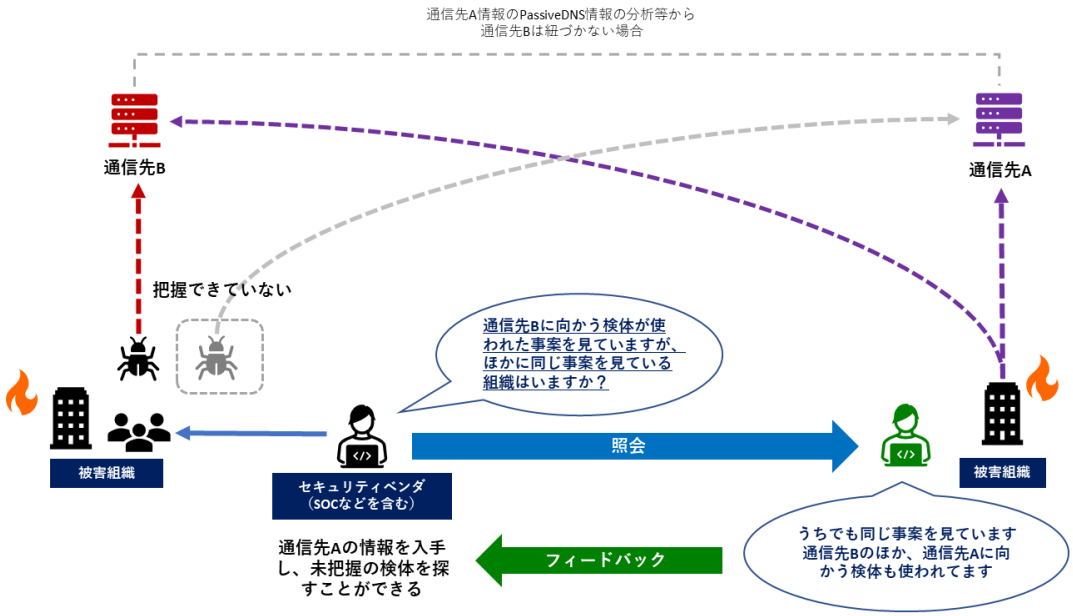


図 36

目的３：（目的１、目的２を通じて）自社顧客等にインディケータ情報を展開するため

情報共有活動を通じて得た、「自組織で把握できていなかった通信先情報」について、対応中の被害組織の調査に活用するだけでなく、この被害組織以外の顧客に対するサービス提供上でも活用することが想定されます。

ただし、情報共有活動によっては、情報共有活動を通じて入手した情報の商用利用を禁じていたり、特定の条件下でしか認めていない活動もありますので、規約等の確認が必要です。

どのタイミングで共有するのか

共有・公表ガイダンスのＱ８（下記）で示されているとおり、情報共有の一般論として、共有タイミングは「攻撃活動が行われているうちに速やかに」ということになります。
他方で、既に攻撃活動が収束したと思われるタイミングであっても、被害を認知できていない組織における早期認知のためのインディケータ展開はなおも有効ですので、ログが消えていかないうちに、やはり早期に共有されることが望まれます。
また、第１章５頁「スコープとしている「情報共有活動」」で解説のとおり、本稿では短期的な専門組織同士の情報共有活動をスコープとしていますが、攻撃全容解明のための中期的な情報共有、アクターや攻撃活動の長期的な追跡のための長期的情報共有も必要ですので、短期的タイミングを過ぎたものであっても、専門組織同士の情報共有としてはなお有効です。
他方で、目的とタイミングを逸した共有はむしろ逆効果になりますので、注意が必要です。
（参考：共有・公表ガイダンス Q8（57 頁））

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。

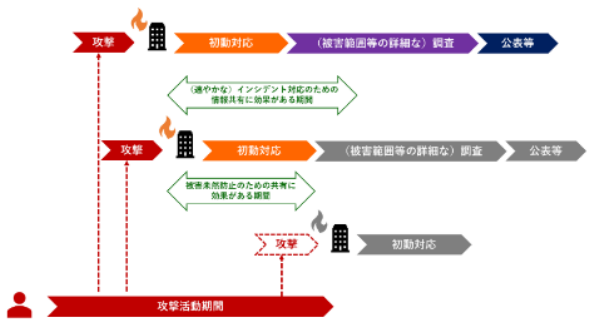


図 39

（共有・公表ガイダンスより）図 37

速報性と正確性の観点から

正確性が担保できない通信先情報も早めに共有することが効果的と考えます。その理由として、「情報共有をしてはじめて全容を把握できる」という事情があります。多くの攻撃活動では、複数の攻撃インフラ（通信先）を用いるため、単一の被害現場の調査だけではすべての攻撃インフラを把握できないケースが多く、専門組織同士で情報交換してはじめて、攻撃に使われた通信先をすべて把握することができます。

他方で、最低限の正確性の担保、特に誤情報のコンタミネーションを避けるためには、第2章37頁の解説のとおりですが、特に通信先情報については、以下の配慮が必要です。

〇どのような経緯で当該通信先を把握したのか説明する

被害現場の通信ログ分析から見つけた情報なのか、実際に現場で回収した検体を分析した結果なのか、あるいは直接被害現場から得た情報ではないのか示します。

例えば、「VirusTotal上にアップロードされていた検体を解析したところ、ある通信先情報が設定されていた」という場合、当該検体は実際には攻撃には使われておらず、攻撃者がテストとして公開解析サービス上での検知率を見るためにアップロードしたものである可能性も考えられます。実際の攻撃で使われていない可能性のある通信先情報をインディケータ情報として展開し、各受信組織にログ調査を行わせたり、本来不要なブロック設定を行われることは可能な限り回避することが望ましいため、当該情報を精査せずに拡散することは避けるべきです。

〇タイムスタンプの必要性

上記とも関係しますが、通信先はIPアドレス、やドメイン（FQDN）、URLのパスだけでなく、「いつ（からいつまで）そのアクセスがあったのか／通信が発生していたのか」というタイムスタンプ情報が必要となります。（☛共有・公表ガイダンス49頁参照）

被害組織が特定されてしまうケース

①被害組織が推測されるケース

攻撃者は被害組織に感染させたマルウェアから C2 サーバへの通信を検知されないように、通信方法の偽装や内容の秘匿のほか、通信先を正規の通信先であるかのように錯覚させる手法も取るケースがあります。例えば、クラウドサービスの利用が増えていることを利用し、正規のクラウドサービス名に酷似したドメインの C2 サーバを運用し、そのサブドメインに被害組織名／利用しているサービス名に酷似した文字列を用いることで、当該通信先を被害組織が利用しているクラウドサービスであるかのように見せるのです。
また、サブドメインではなくて、URL のパス名の一部に標的組織名（被害組織名）などを示す文字列が含まれているケースも稀ながら存在します。

したがって、当該通信先の FQDN の文字列を見た第三者が、サブドメイン上の文字列から被害組織（のドメイン名など）を推測する可能性があるわけですが、あくまでも「推測」であって、被害事実そのものを示す情報ではありません。しかしながら、その他の情報と結びつくことで、その確度が上がる可能性があります。

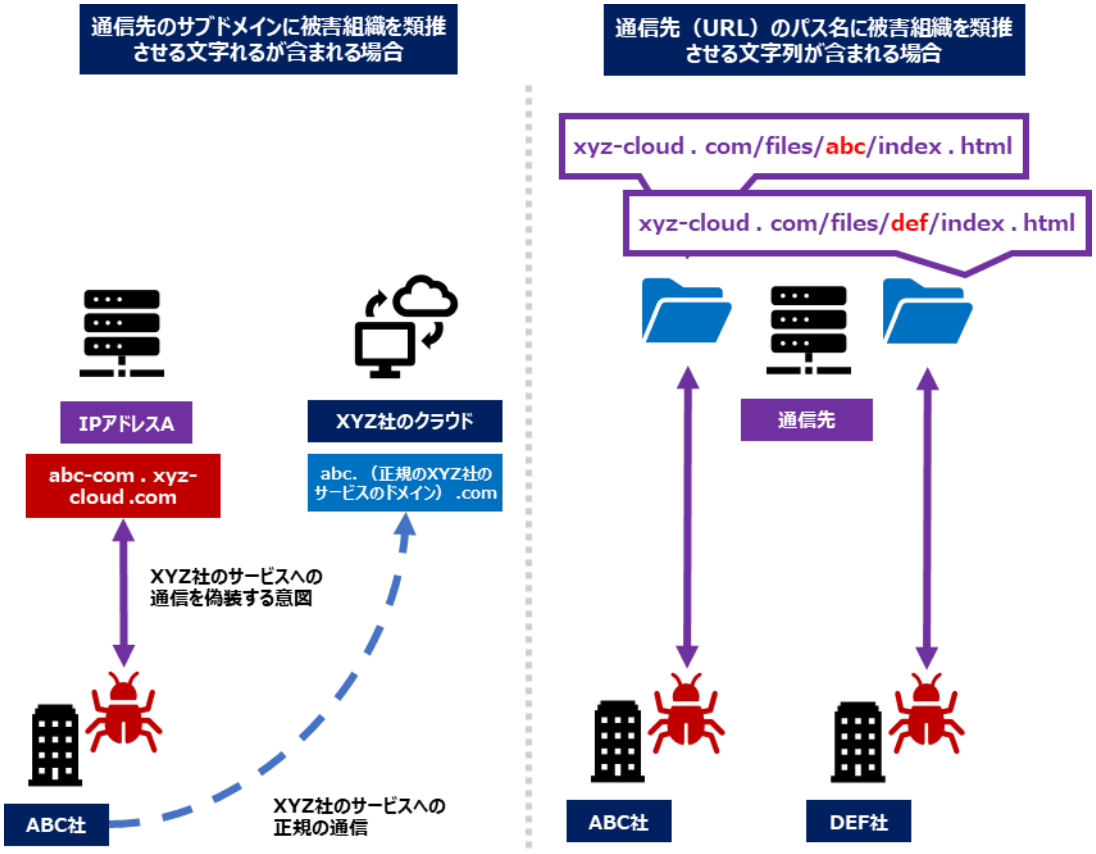


図 38

＜非特定化加工のポイント＞

①のケースに対しては、その他既に公表／流通している情報と組み合わせた場合に、当該被害組織をどこまで特定し得るのか確認した上で、被害組織と結びつきやすい文字列についてはマスキングして情報共有活動に展開する方法が考えられます。

（元情報） abc-com.example[.]com

（加工後の情報） ******.example[.]com

情報共有活動に展開するということは、他の標的組織を狙った C2 サーバの FQDN でも同じ事象（当該他の標的組織を示すような文字列が含まれている）が起きている可能性が想定されるため、

******.example[.]com 注：サブドメインの箇所に被害組織を示す文字列が入る

のように説明を加えることで、情報提供元（被害組織）を秘匿しながらも、より共有効果が高いように情報を展開することが可能になります。

②被害事実を示す情報が C2 サーバ上に閲覧可能な状態で蔵置されているケース

C2 サーバ上のファイルの一部がオープンディレクトリになっており、不特定多数の者が外部からアクセス可能になっている場合があります。こうした状況で当該 C2 サーバや当該ディレクトリを示す URL 情報が流通した場合、不特定多数の者が当該ディレクトリにアクセスし、蔵置されている、被害組織からの通信を示す情報を閲覧できる可能性があります。

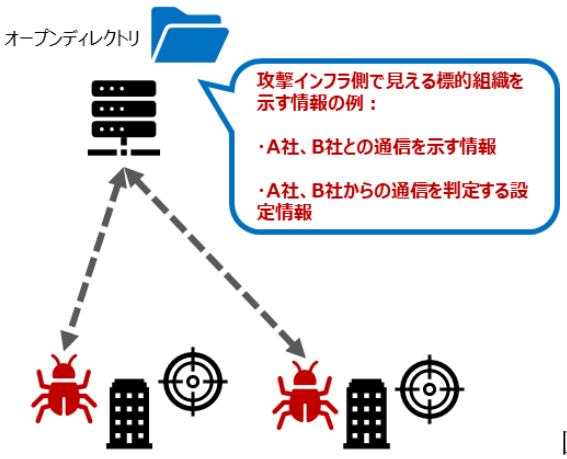


図 39

＜非特定化加工化のポイント＞

②のケースはそもそも当該通信先情報を広く情報共有する必要がない場合が想定されます。当該 C2 サーバ上に被害組織又は標的としていた組織を示す情報が蔵置されているのであれば、当該情報をもとにそれぞれの被害組織／標的組織に通知をすれば、情報共有と同じ効果を得られます。これについては、当該データの入手だけでなく、被害組織／標的組織への通知作業も必要になるため、広く被害組織への通知を日頃から行っている知見のある専門機関に相談することが望まれます。

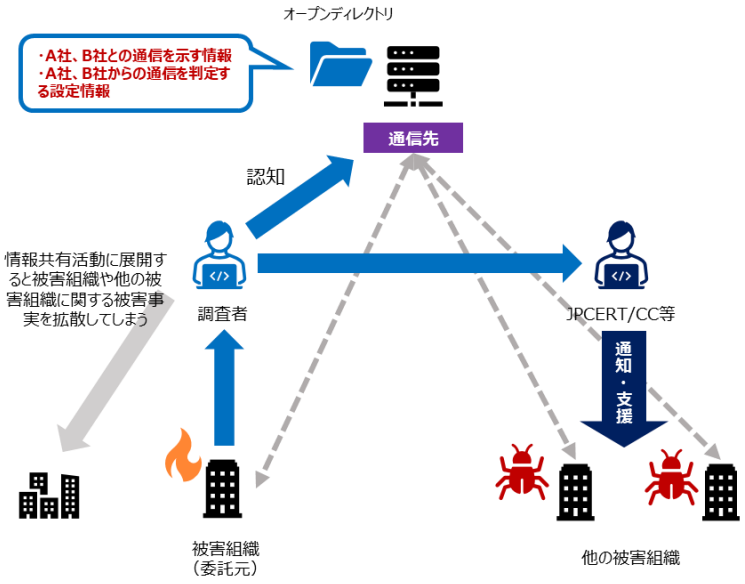


図 40

③通信先が正規の Web サーバ等が改ざんされ悪用されたものである場合

先述の通信先の類型 D のように、正規組織の Web サーバ等が何らかの侵害を受けて改ざんされるなどして不正な通信先として悪用されている場合があります。C2 サーバとして使われるほか、水飲み場攻撃など、マルウェアの配布元として使用される場合もあります。この場合、当該通信先を情報共有活動上で展開するということは、当該踏み台となった組織やその被害事実を類推させる情報を展開することになってしまいます。他方で、当該通信先情報が展開されなければ被害が拡大するおそれがあります。

＜非特定化加工の視点＞

「他の被害組織の被害に関する情報を見つけた場合」の対応としては、共有・公表ガイダンスの「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？」を参照ください。

この場合、当該通信先を情報共有活動上で展開するということは、当該踏み台となった組織やその被害事実を類推させる情報を展開することになってしまいます。他方で、当該通信先情報が展開されなければ被害が拡大するおそれがあるということで、当該情報を情報共有活動に展開すべきかジレンマに陥ることになります。

他方で、例えば水飲み場攻撃のように、改ざんサイトにアクセスしてきた特定の標的にだけマルウェア感染させるなどのターゲティングが行われている可能性が考えられるため、先述の②のケースのように、まずは当該サーバ内の情報確認を行うことで、必ずしも特定多数への情報展開が必要なのではなく、個別に標的となった可能性のある組織への通知をすれば済む場合が想定されます。

また、これ以外のケースでも、当該改ざんサーバ等には被害組織を示す何らかの情報が残っている可能性が考えられるため、いずれにせよ、当該踏み台となった組織への支援を優先することで、他の被害組織への情報展開も適切な方法で行える選択肢が見えてくる可能性があることから、まずは専門組織等を通じた当該踏み台組織へのコンタクト・支援を優先させる必要があります。

ただし、攻撃活動が現在進行形で進んでおり、当該踏み台組織へのコンタクト・支援によって当該攻撃インフラが停止する見込みよりも、被害拡大の蓋然性が高いと見込まれる場合、緊急的に当該通信先情報を情報共有活動へ展開したり、専門組織が注意喚起として情報発信することが想定されます。

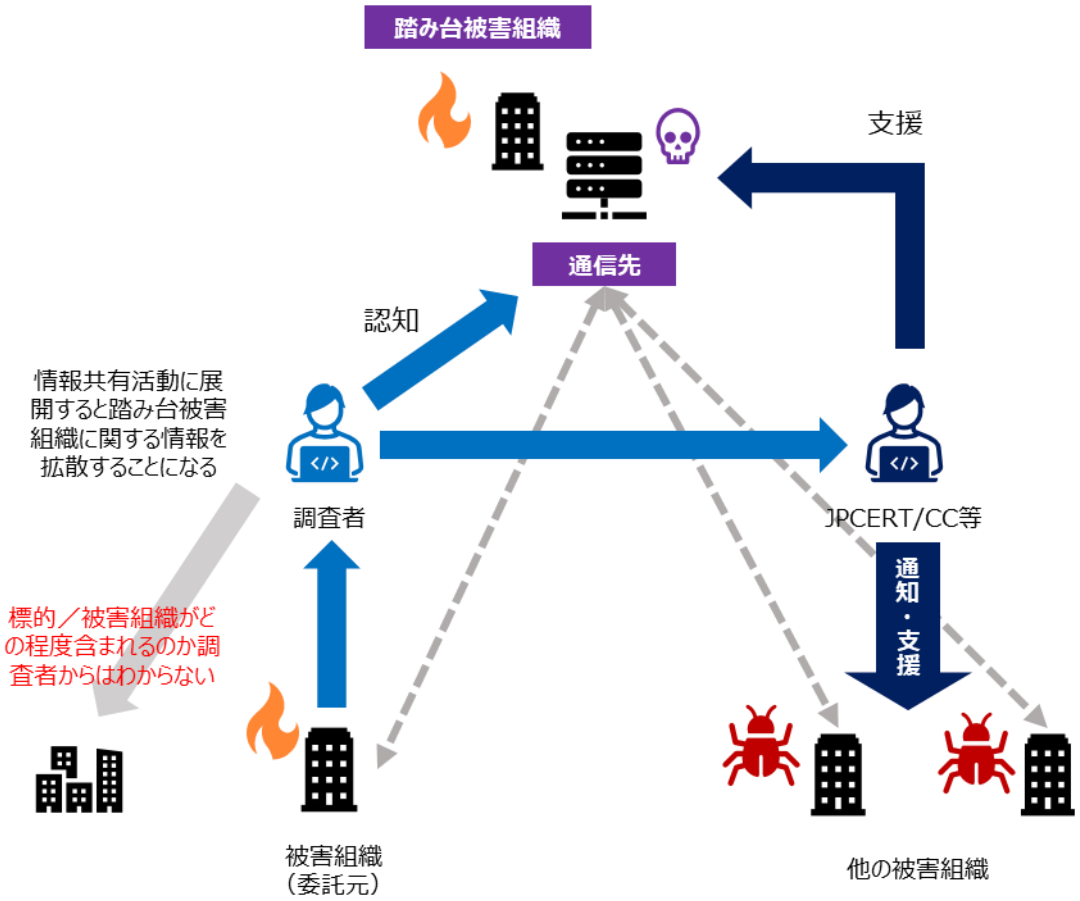

踏み台被害組織
支援
通信先
認知
情報共有活動に展開すると踏み台被害組織に関する情報を拡散することになる
調査者
JPCERT/CC等
通知・支援
標的／被害組織がどの程度含まれるのか調査者からはわからない
被害組織
（委託元）
他の被害組織

図 41

マルウェア情報

専門組織同士のマルウェア情報の共有

マルウェア情報は、マルウェアそのもの（検体）と、マルウェア検体を解析した結果得られた情報の二つがあり、情報共有活動ではこのうち「マルウェア検体を解析した結果」が扱われます。
一般的な情報共有活動においては、スキルの差がバラバラな組織同士が検体を安全に扱うことができないため、共有・公表ガイダンスでは、検体そのものではなく、マルウェアを解析した結果を扱うことが示されています（共有・公表ガイダンス 102 頁参照)。
他方で専門組織同士の場合、共有対象となるマルウェアについても既に当該情報提供元である専門組織がインシデント対応等で解析済みであることが多いため、やはり検体そのものではなく、解析結果を共有することが専らです。

また、前述の「専門組織が情報共有する目的」のうち、

A：支援する被害組織における事案の全容解明や再発防止策のため、自組織では不足している情報を情報共有活動で補うこと

B：関与する情報共有活動の参加組織内に被害組織や標的組織がいる場合（あるいはその想定される場合)、被害の未然予防や被害拡大防止、また被害の早期認知に必要な情報を得ること

C：被害組織への支援や調査を行う上で、自組織の知見が不足していないかについて知ること（平時からの取組として）

D：脅威アクターを中長期間にわたり追跡するために自組織では不足している情報を情報共有活動で補うこと

E：攻撃要素（脆弱性や攻撃インフラ）への対処のため、対処ができる専門機関等へ対応依頼をするために、必要な情報を提供すること

A、B、E は一刻も早く取り組むことが求められるため、場合によっては表層解析レベルの情報がやりとりされることもあります。情報共有活動を通じて検体そのものを入手し、詳細な分析を新たに行っている時間的猶予はないため、やはり、検体そのものを情報共有活動で取り扱わなければならない理由はありません。

他方で、D については検体の詳細解析による情報が重要である場合もあるため、検体そのものを入手するニーズがあるわけですが、中長期的活動であることから、当該分析を行うタイミングでは既に公開サンドボックスサービス上などに検体がアップロードされていたり、最初に当該検体を見つけたアナリストによる詳細な解析結果がレポート公表された後であることが想定されます。

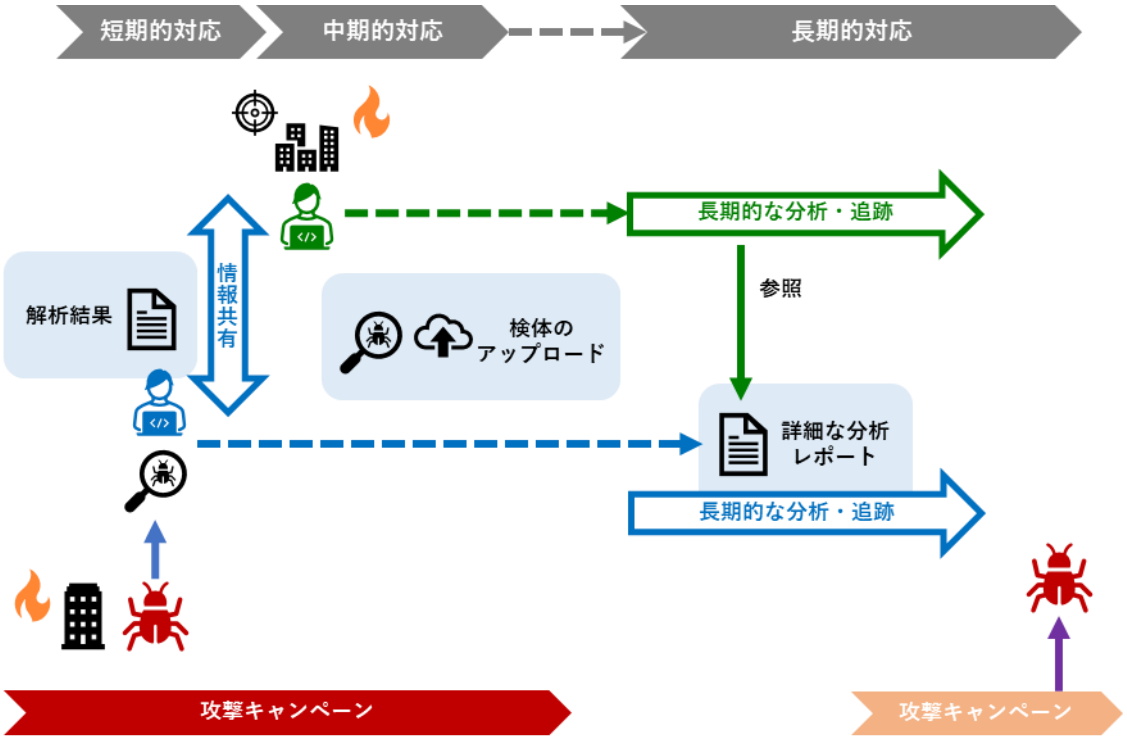


図 42

どの情報を共有するのか：マルウェア解析情報

マルウェアの解析には主に「表層解析」「動的解析」「静的解析」の 3 種類がありますが、それぞれに必要な時間（横軸）と得られる情報の量／質（縦軸）を整理したものが以下の図です。

前述の「専門組織が情報共有する目的」のうち、目的 A、目的 B として最低限必要な情報は表層解析である程度得ることができ、この両目的は「スピード」が重要である点からも、静的解析がまだ不十分であっても先に情報共有に供されます。

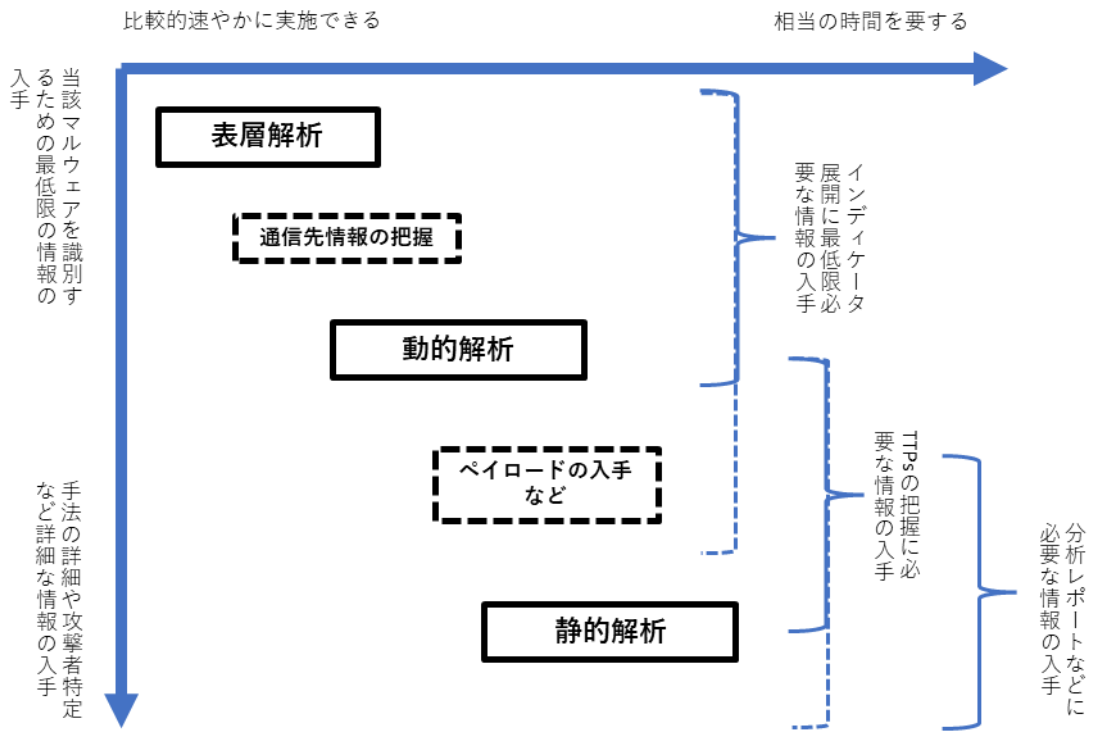


図 43

専門組織同士がマルウェア情報を共有する場合、ダウンローダーなどは入手できているが、その次のペイロードが入手できていない状況で他の組織に照会をかけるケースがあります。関連検体を入手したタイミングで既に C2 サーバが活動を停止していたり、あるいは特定の条件（認証コードの必要など）を満たさないとペイロードが DL できないことがあるため、条件を満たしてペイロードを入手できた他の専門組織がいないか照会をかけます。

各解析で得られる情報と共有タイミングについて

通信先情報のパートでも解説しましたが（第 3 章 46 頁参照)、本稿でスコープとする短期的対応だけでなく、専門組織同士の情報共有活動としては、中期的・長期的なものまであります。

マルウェア解析の特に静的解析にはある程度の時間がかかるところ、短期的には、表層解析や動的解析ですぐに判明する情報が必要とされます。他方で長期的な動きの中では静的解析により判明する情報が重要になりますが、これは必ずしも情報共有活動を通じた情報共有だけでなく、セキュリティ専門組織が行っているレポート公表や、国際カンファレンス等でのアナリストによる発表といった公開情報を通じて広く共有されていくことも想定されます。特に静的解析については解析方法や分析結果自体が当該専門組織の競争優位性の基盤であったり、アナリストの成果を示すものでもあるため、こうした成果としての情報発信が尊重されながら、長期的情報共有として知見が社会全体でも蓄積されていることができます。

対応フェーズ／タイミング		短期的対応	中期的対応	長期的対応
目的		・他の専門組織への紹介／突合 ・インディケータ展開	・過去の攻撃キャンペーンとの関連分析／攻撃グループ区分 ・攻撃（キャンペーン）の全容解明	・詳細なレポート公表 ・次の攻撃の早期検知？
表層解析	ファイル名、ファイルの種類（拡張子）	✓		
	ハッシュ値	✓		
	インポートハッシュ値などのその他のハッシュ値		✓	
	プロパティ情報、証明書情報		✓	
	通信先	✓		
動的解析	通信の種類	✓		
	通信先から得られるペイロード等の追加検体	✓		
	各プロセスの挙動			
静的解析	全体の構造やアルゴリズム		✓	
	動的解析では見えなかった挙動／機能			✓
	マルウェア／作成者固有の箇所			✓

どの種類のマルウェア情報を共有すべきなのか

「マルウェア」と一言に言っても、ダウンローダー、ドロッパー、ボット、RAT、キーロガー、Webshell と様々です。インディケータ情報で取り上げられたり、速報的なレポート公表で比較的取り上げられるのは、外部への通信が発生し、インディケータにもなりやすいダウンローダーやペイロードに関する情報です。

他方で、特徴的なローダーから攻撃グループ／攻撃活動を特定できるケースもあり[6]、特に、攻撃グループ特定により侵害原因を速やかに推測／特定できるケースにおいては、重要な情報となります。

いわゆるユーザー組織側でのインディケータ展開にはそこまで有効でなくても、専門組織同士の情報共有では有効であることが想定されるため、無理に共有対象の種別を絞らず、広めに共有することが望まれます。ただし、見つかったマルウェアについて、既に公開情報として流通しているものがあれば、後述のとおり、その旨を示しながら、効率的に伝達されるよう工夫する必要があります。

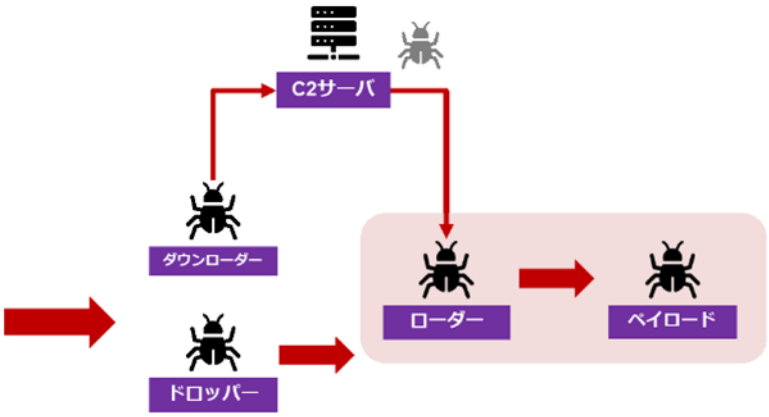


図 44

[6] https://blogs.jpcert.or.jp/ja/2022/05/HUILoader.html

被害組織が特定されてしまうケース

被害組織以外の第三者とマルウェア情報を共有する際に留意が必要なケースとしては、

ケース①：感染後の検体が公開サービスにアップロードされている場合

ケース②：検体に内包されている通信先情報から標的組織／被害組織を推測できるような検体が公開サービスにアップロードされている場合

ケース③：標的組織に関する情報を内包する検体が公開サービスにアップロードされている場合

ケース④：未修正の脆弱性に関する情報を含む検体が公開サービスにアップロードされている場合

があり、いずれも当該検体が VirusTotal などの公開サービスにアップロードされており、不特定多数の第三者が当該検体自体に触れられる状態で発生します。

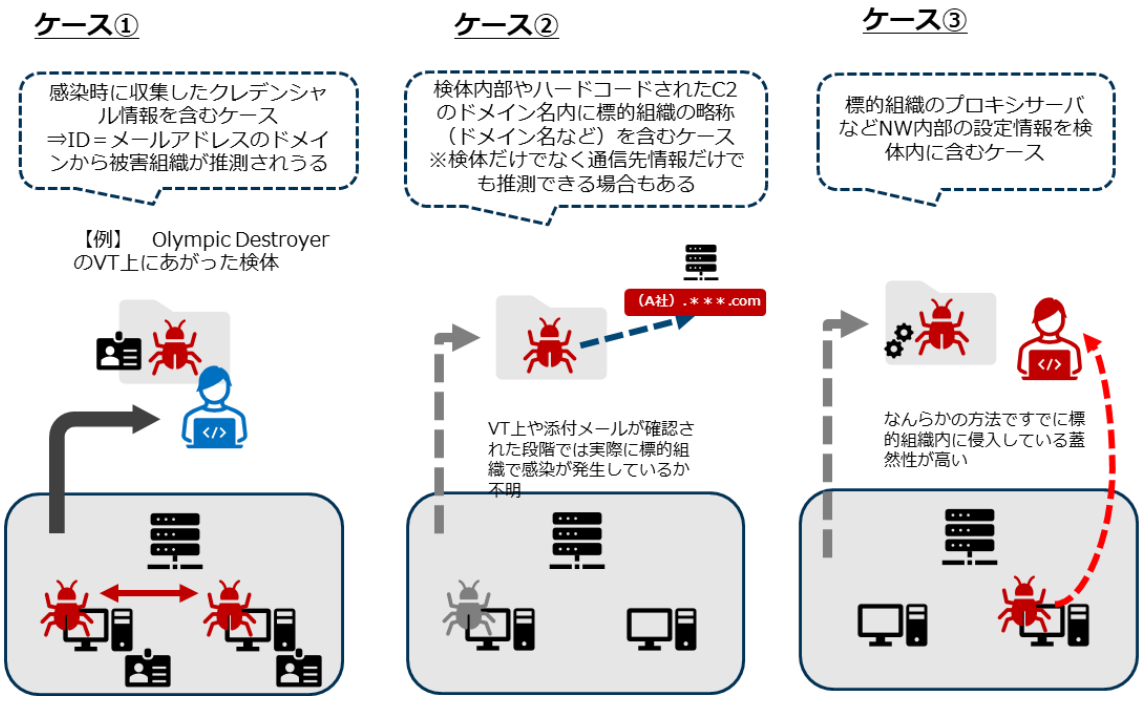


図 45

ケース①：感染後の検体が公開サービスにアップロードされている場合

下記は、2018 年 2 月に発見された OlympicDestroyer 検体の VirusTotal 上での解析結果です。OlympicDestroyer は感染後に感染端末から視覚情報を窃取し、横展開や権限昇格のために悪用する仕組みを持っています。下記検体は感染後に被害現場で回収された検体が何らかの経緯でアップロードされたと考えられ、感染端末から窃取した資格情報が内包されたままになっていました。そのための VirusTotal の strings 情報で見ることが可能になっており（※strings 情報は有償会員でなければ利用できない）、そこから感染組織が推測されてしまいました。
他の専門組織に情報共有しようとする専門組織自身がアップロードしていなくても、被害組織自身や事案対応に当たった他のベンダなどが VirusTotal などにアップロードしてしまっている場合、同様の事象が発生する場合もあり、注意が必要です。

資格情報単体であれば、「過去何らかの経緯（フィッシングや雑多なマルウェア感染等）で漏えいした情報」程度の意味合いしか示しませんが、検体の機能（感染した組織から視覚情報を窃取し内包する）や検体の出現時期（コンパイルタイムなど）、地域等（アップロード地域）の情報が加わることで「直近で未公表の攻撃被害が発生していることを示す」情報となってしまいます。

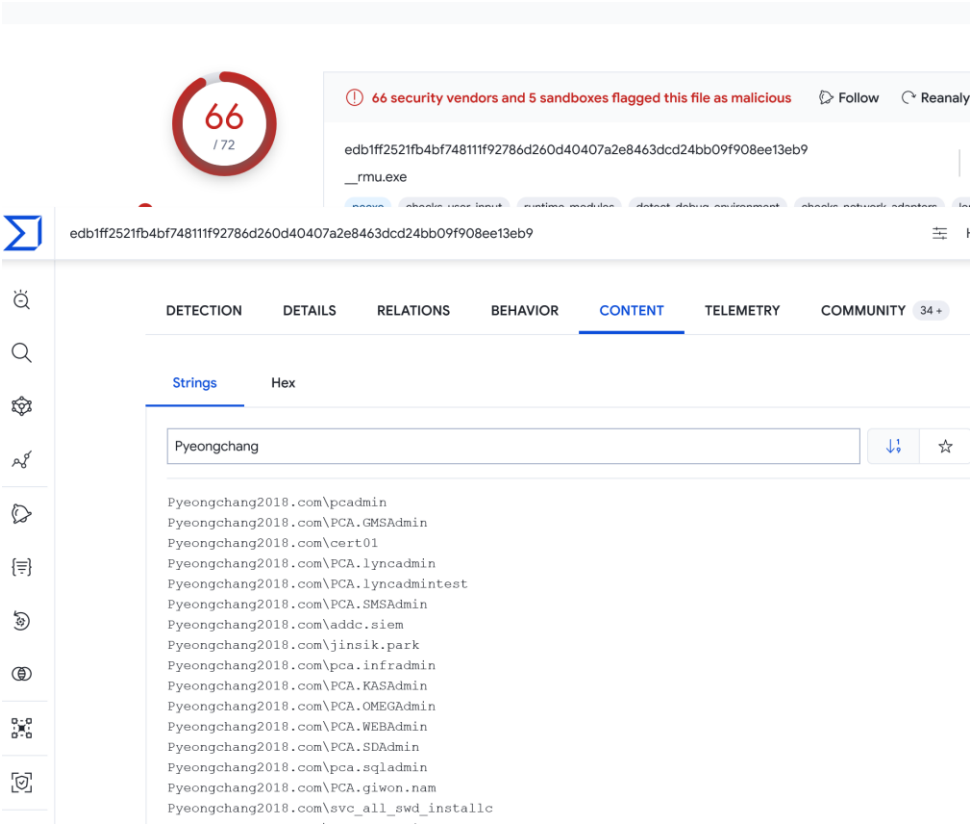


図 46

＜非特定化加工のポイント＞

上記のような、実際に各被害組織で実行され、資格情報等を多く内包した検体は実行前の検体からハッシュ値等が変化しているため、非特定化加工化のために資格情報を含まない実行前の検体のハッシュ値をインディケータ展開しても調査に有効でない可能性があります。

したがってこの場合は、実行前の検体のハッシュ値だけでなく、ファイル名や実行後に関連プログラムが稼働する箇所やプロセス名など、ハッシュ値以外のインディケータ情報を組み合わせて提供する必要があります。

他方で、資格情報を持たない実行前の検体も既に公開解析サービス上に上がっている場合、ハッシュ値 A の情報を情報共有活動を通じて知った者は公開解析サービス上の検索で、同じ特徴（通信先や特徴的な文字列など）を持つハッシュ値 B の検体にたどり着く場合があります。

自組織の被害を第三者が推測し得る検体を公開解析サービスにアップロードしてしまっている以上、被害組織について非特定化し続けることはそもそも困難です。他方で実行前の検体も既にどこからかアップロードされている状況では、既に複数の被害がある程度の範囲で発生していることが想定され、近いうちに各アンチウイルス製品やセキュリティ監視サービスで既に検知可能な状態になっていくことが想定されます。この場合、情報提供元の被害組織が特定されるリスクを冒してまで情報共有活動に当該検体情報を流す必要性がない状況である可能性があります。

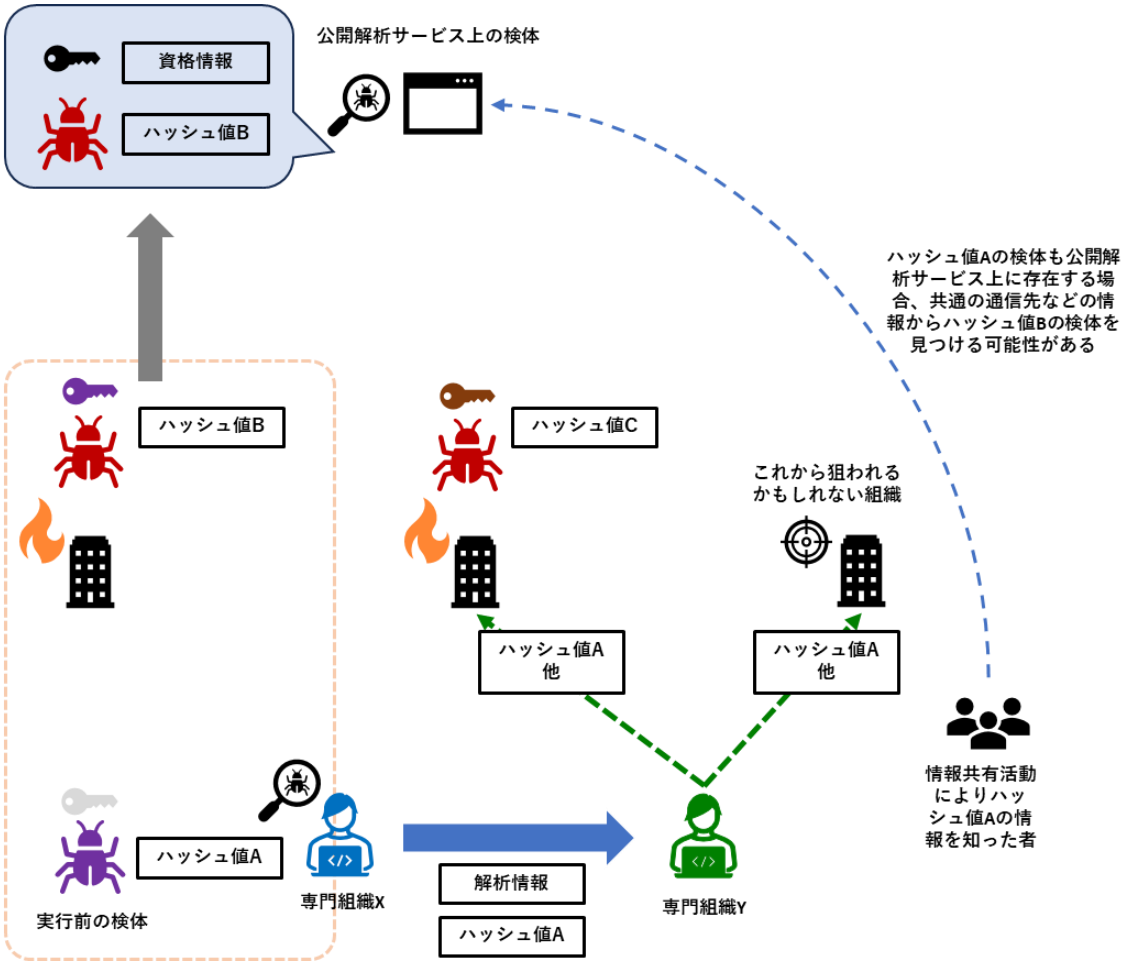


図 47

ケース②：検体に内包されている通信先情報から標的組織／被害組織を推測できるような検体が公開サービスにアップロードされている場合

（※通信先情報の項目で解説済みのため省略）

ケース③：標的組織に関する情報を内包する検体が公開サービスにアップロードされている場合

マルウェアの中には、ランサムウェアのように何らかの理由で特定地域を標的としない攻撃や、防御側の解析／攻撃解明を回避するために、特定言語環境下や、特定通信先への通信成功可否を動作条件として組み込まれるものがあります。これに加えて、標的組織のネットワーク内でのみ確実に動作し、標的組織以外のネットワーク内では実行されないように設計されたものがあります。
下記 VirusTotal にアップロードされた検体は通信先の一つに標的組織の内部サーバと思われるドメインが設定されており、攻撃者の想定通り、標的組織のネットワーク内に設置され、当該ドメインへ通信が成功する場合、検体の主機能が作動するようになっていました。

ケース①と同じくこうした検体が公開サービスにアップロードされている場合、不特定多数の者が「特定の組織が当該検体を用いた攻撃で狙われている／既に攻撃されているかもしれないことを示す」情報に触れることになります。
ただ、ケース①とは異なり、実際の感染被害を示すものではなく、何らかの経緯で攻撃者が攻撃前にアップロードした可能性や、攻撃試行はされたが当該標的組織で早期に認知し、感染等の実害が発生していない可能性があるため、あくまでも「攻撃／被害の可能性を推測させる情報」ということになります。

この場合、当該検体の存在をもってして、「既に日本の組織が標的となっていることを示す情報も確認されているため、このようなマルウェアの攻撃に注意してほしい／感染していないか調査を推奨する」という主旨／温度感で当該マルウェアに関する情報を展開することも想定されます。ただ、当該検体に内包された情報については基本的にはある程度の専門知見や VT ハンティングなどの積極的な公開検体探しをしている組織／研究者が見つけても限定的な範囲で知られる情報であり、公開サービスにアップロードされ「公知」になっているからといってただちに不特定多数の者に知れ渡るわけではないため取扱いに注意が必要です。前述のとおり、「推測させる情報」とはいえ、特定の被害組織や被害事実に関する情報であるため、当該検体の存在や当該内包されている設定情報から、当該標的／被害組織について広く情報発信することは必ずしも望まれるものではありません。まずは被害組織への個別通知や対応支援が必要になります。

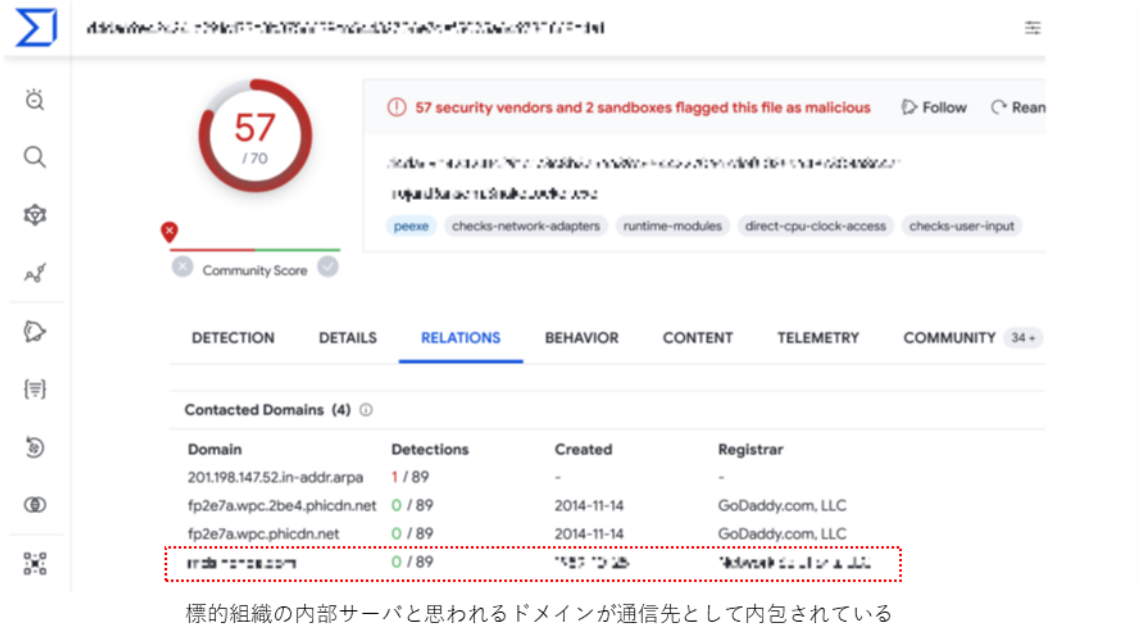


図 48

＜非特定化加工化のポイント＞

ケース①とほぼ同じような対応になりますが、特に上記のような標的組織ごとに設定値が異なる場合、検体ごとにハッシュ値が異なるため、ハッシュ値を共有情報として展開しても効果は見込めません。通信先やファイル名、保存先／永続先などの情報を中心に展開するしかありません。

ケース④：未修正の脆弱性に関する情報を含む検体が公開サービスにアップロードされている場合

遭遇する可能性は比較的低いと思われますが、検体内の情報から、当該時点で未修正の脆弱性が判明するケースが想定されます。この場合は、未知の脆弱性情報の取扱い（第 3 章 71 頁参照）にしたがって対応することが求められます。

脆弱性情報

脆弱性情報の性質

国内における脆弱性関連情報の取扱いについて定めた、「ソフトウェア製品等の脆弱性関連情報に関する取扱規程」（平成二十九年経済産業省告示第十九号。以下、「脆弱性取扱告示」という。）[7]では、

> (4) 脆弱性情報
> 脆弱性の性質及び特徴を示す情報をいう。
> (5) 脆弱性関連情報
> 次に掲げるものをいう
> ①脆弱性情報
> ②脆弱性が存在することを検証する方法
> ③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

と定めています。

また、脆弱性情報はその「状況」に応じて、以下のように整理することもできます。

① 未修正の脆弱性に関する情報
② 公表された脆弱性情報
③ 悪用された脆弱性に関する情報（既知の脆弱性の場合）
④ 悪用された脆弱性に関する情報（ゼロデイ攻撃の場合）

[7] https://www.meti.go.jp/policy/netsecurity/vul_notification.pdf

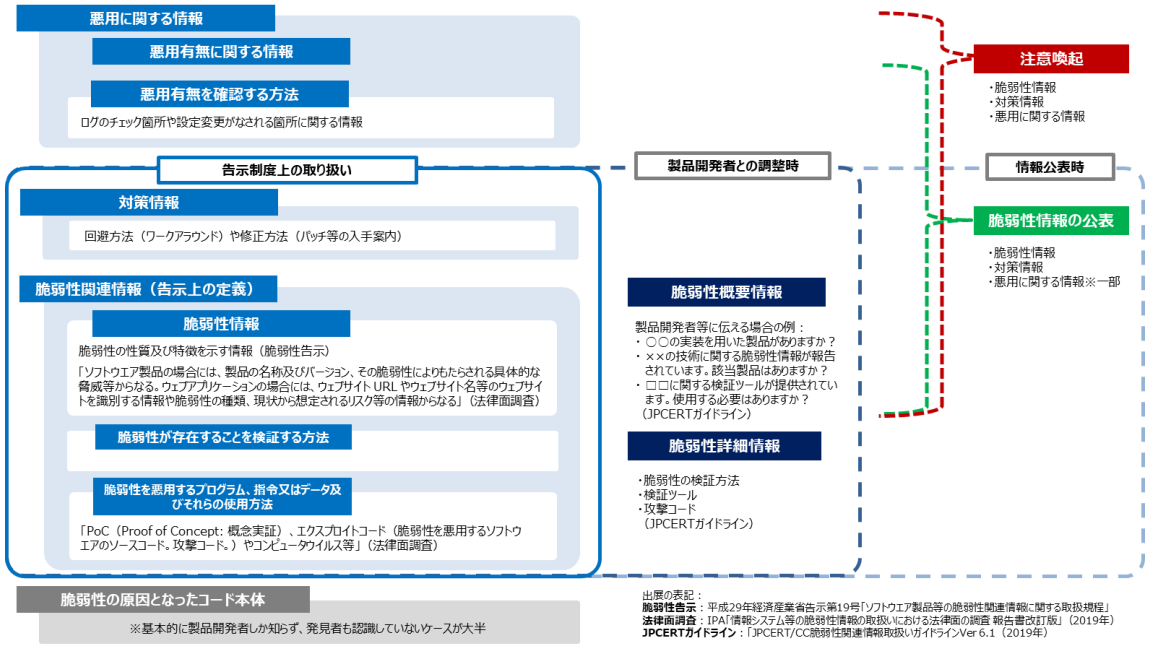


図 49

（サイバー攻撃による被害に関する情報共有の促進に向けた検討会最終報告書より抜粋）

脆弱性情報の多くは国内の場合、脆弱性取扱告示に基づく早期警戒パートナーシップ制度に基づいて公表や注意喚起などが行われており、専門組織同士の情報共有で扱われるものとしては、「悪用に関する情報」が主に想定されます。
この「悪用に関する情報」は上記の整理のとおり、

・既知の脆弱性に関する情報
・ゼロデイ攻撃に関する情報

の二つが想定されます。
基本的に扱い方については、共有・公表ガイダンス 121 頁「脆弱性の悪用に関する情報について」にて解説がなされていますのでご参照ください。また、被害公表時の想定ですが、共有・公表ガイダンスの「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？」という項目にも関連する解説があります。

脆弱性悪用に関する情報はどうハンドリングされるべきか

専門組織が被害現場への調査において、脆弱性悪用を確認した場合の対応については、共有・公表ガイダンス 121 頁にて解説されているとおり、既知の脆弱性であれば「製品 A の脆弱性が悪用された」という情報を情報共有活動に展開することは可能であり、未知の脆弱性が悪用されている可能性があれば、脆弱性の発見者として脆弱性取扱告示に基づく届出を行うことで、専門機関へ情報提供することができます。

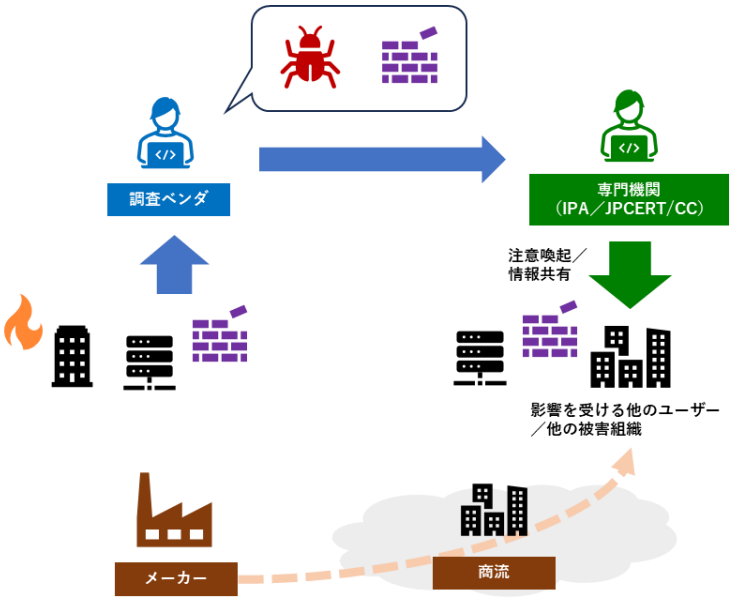


図 50

ここで問題になるのは、既知の脆弱性であっても、その「悪用情報」について（不）特定多数の者に伝達されることに対して、メーカーが消極的になるケースです。

共有・公表ガイダンス 98 頁では、IT ベンダのシステムが“踏み台”となって多数のユーザーが侵害されたケースを例示していますが、脆弱性についても同じ問題点が指摘できます。脆弱性が悪用されている情報について、特に法人向け製品においてメーカーからユーザー個別にコンタクト可能な場合、公表による伝達ではなく、メーカーは非公開での個別通知を行うことを希望する場合があります。ただし、この場合、個別通知では対応リソースの都合上、どうしても時間がかかるため、さらなる被害拡大や新たな攻撃活動への対応に間に合わない場合が懸念されます。また、通知先が増えるにしたがって、当該脆弱性悪用に関する情報が意図せず拡散していくことも想定されます。そのため、公表での注意喚起や情報共有活動を通じた情報展開の活用が望まれます。

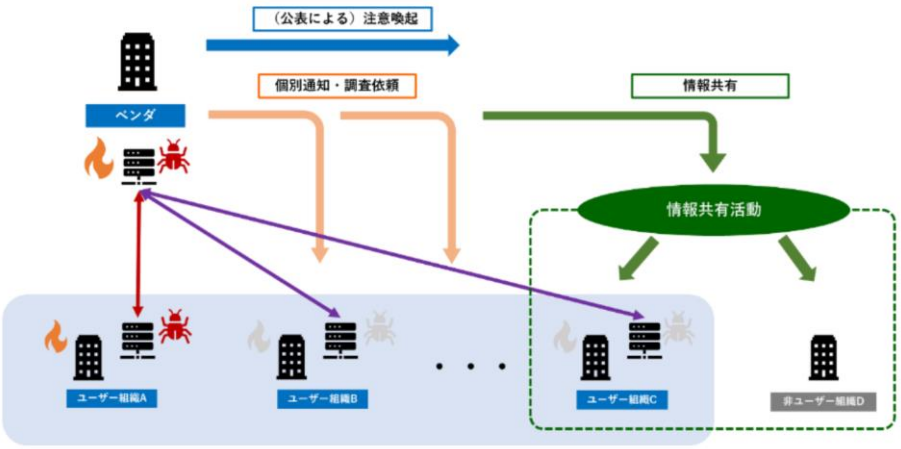


図 51

情報伝達の「スピード」の観点だけでなく、ユーザーへ伝達される「内容」の観点も重要です。特定製品の脆弱性が悪用された攻撃への対応や攻撃有無の確認を行う場合、そもそも当該製品ついて知見が無ければ適切な調査ができない場合があります。そうすると、被害現場ではメーカーや製品の保守ベンダの支援が必要になります。当該製品／サービスについて最も知見があるのはメーカー／保守ベンダであるものの、他方で、当該攻撃自体について最も知見があるのは当該事案を追跡している専門組織ですので、被害組織／ユーザーには双方の知見が情報として伝達されなければなりません。

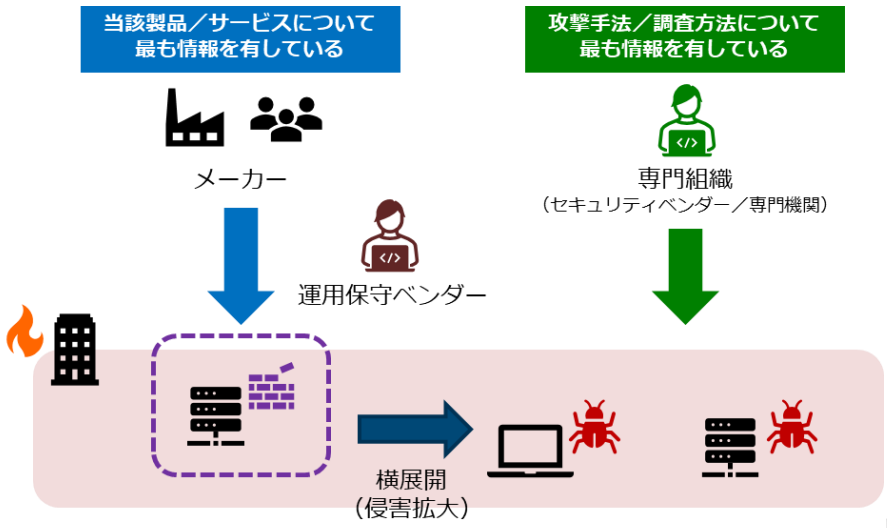


図 52

したがって、脆弱性悪用に関する情報は、メーカー／運用保守ベンダによる伝達だけではなく、専門組織同士の情報共有や、攻撃の活動状況によっては注意喚起などを通じて、攻撃手法や調査ポイントなどに関する攻撃技術情報もセットとなって伝達されるべきですので、当該情報を見つけた専門組織は積極的な情報共有や専門機関との連携が望まれます。

被害組織が特定されてしまうケース

既知の脆弱性に関する悪用情報を情報共有活動に展開したことで、情報提供元である被害組織が特定されるケースがあります。
以下のケースでは、情報共有前に既に被害組織が第一報的な被害公表をしており、個別の脆弱性や特定製品名までは当該時点で公表していないものの、その後に共有・展開される情報と Shodan/Censys などのヒストリーデータが組み合わさることで、当該情報提供元が第一報を公表した被害組織ではないかと推測することが可能になります。

ただし、このケースでは被害組織自体は既に被害を公表しており、また、複数の被害組織が存在していれば、必ずしも当該情報提供元が当該被害組織と一意に結びつくものではないため、他の事例のような「意図しない被害組織情報／被害事実」の漏示とまでは言えません。
とはいえ、このような経緯で（不）特定多数の第三者に推測されるであろう点について被害組織自身がまったく認知していないか、認知しているかでは対応の温度感が変わりますので、あらかじめそのような可能性があり得る点を専門組織側から被害組織に伝えておくことが推奨されます。

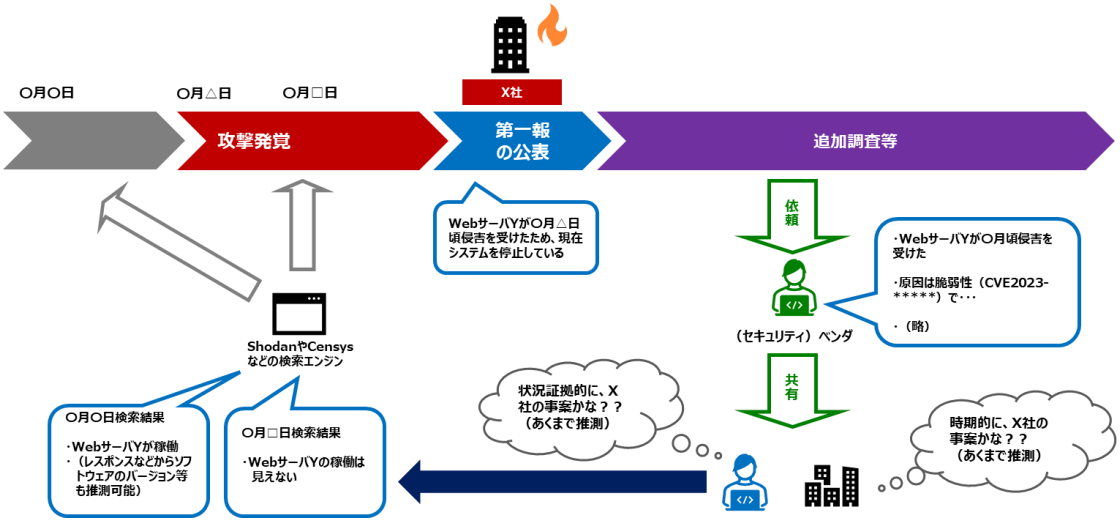


図 53

その他 TTPs

ケースバイケースであり、攻撃類型によりますが、マルウェア情報や通信先情報、脆弱性情報は比較的早期の時点で情報が見つかる一方で、横展開や権限昇格の手段などのその他の TTPs については、ある程度フォレンジック調査等を進めたのちに判明するものが多いため、早期の情報共有対象として扱われにくい性質があります。したがって、ある程度後ろの時点での分析レポート公表やカンファレンス発表のタイミングなどで開示されることが多い情報です。

被害組織が特定されてしまうケース

TTPs 情報から、被害組織が特定／推測されるケースを想定した場合、利用組織がほぼ一意に特定されるようなシステムが侵害されているため、マルウェア情報、通信先情報、脆弱性情報以外の TTPs から、当該システムが特定／推測されることで、被害組織が特定／推測されるケースが想定されます。
そのようなかなり特殊なシステムへの侵害事案の場合、むしろ利用組織はある程度限定されるため、必ずしも情報共有活動に情報展開することが、当該攻撃技術情報を伝達する最適な方法とは限らなくなります。例えば、メーカーから個別に通知することが想定されるため、第三者に被害組織が特定／推測されるリスクは基本的になくなります。

ケース１：バッドケース
ファーストレスポンダーの情報不足により被害組織の対応コストが増えてしまったケース

①初動対応フェーズ

被害組織 A が運用するあるシステムに関係する端末上でアンチウイルス製品がマルウェア X を検出したとアラートを上げたため、システムや関連するネットワークの運用保守を委託している IT ベンダ B 社に調査を依頼したところ、ほかにも複数の端末やサーバからマルウェア X が見つかった。

マルウェア X が見つかったシステムには官公庁を含む取引先に関する情報や顧客の個人情報が保存されており、フォレンジック調査や通信データの量などから、当該端末／サーバに保存されていた情報が漏えいした可能性が否定できないとして、影響を受ける取引先や所管省庁等への報告、被害公表を行うこととなった。

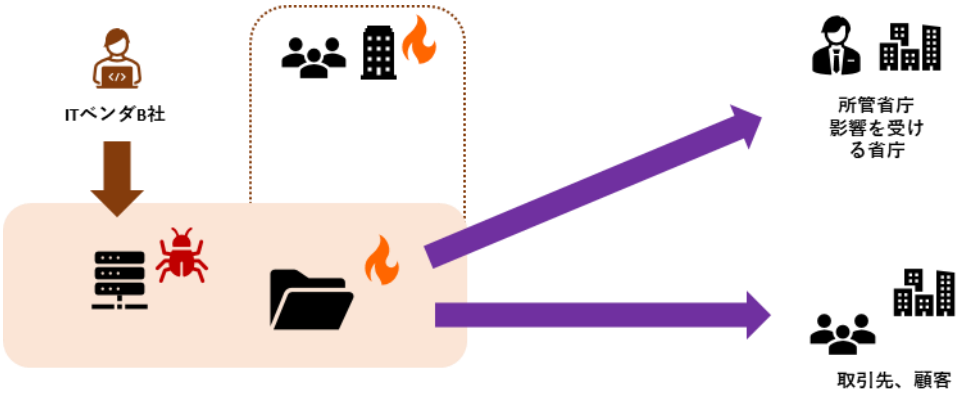


図 54

②対外応答フェーズ

所管省庁への報告のほか、他の行政機関からの情報提供の依頼に対応するなどあわただしくなる中、被害組織 A のセキュリティ担当者が念のため、通信ログのチェックを行ったところ、従業員のいない深夜帯に特定の通信先へ通信が多数発生していることが判明し、IT ベンダ B に問い合わせたが、少なくとも正規の通信ではないもののマルウェア感染によるものなのかは断定できず、また、アンチウイルスのスキャンでは不審なプログラム等は発見されなかった。コンタクトのあった行政機関等にも問い合わせたところ、当該不正通信先に関する情報が得られなかったが、専門組織 C への相談を推奨されたため、面識はこれまでなかったが、コンタクトすることとした。

被害組織 A は専門組織 C に相談をしたところ、この通信がマルウェア Y によるものではないかと回答があり、また、マルウェア Y を用いる攻撃活動で使われた通信先の一覧情報が提供され、通信ログを調べるようにアドバイスがなされた。

これに従い調べたところ、マルウェア Y の感染が複数見つかり、また、上記とは異なる別の不正通信先への通信も見つかった。

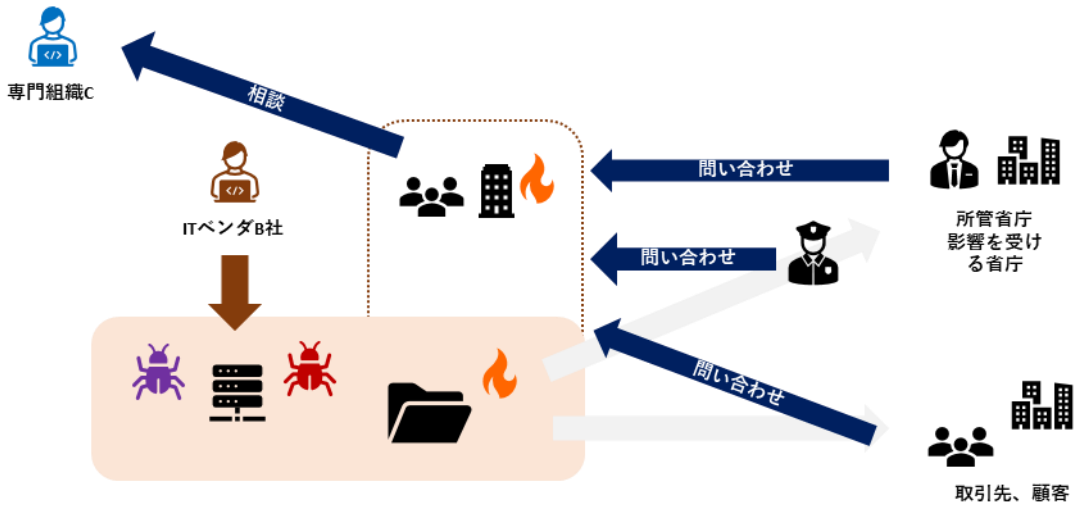


図 55

【初動対応が失敗に終わった原因】

・特に標的型サイバー攻撃では、マルウェアの高度化や複雑化、living off the land 戦術などの登場により、簡易な初動調査では痕跡が見つけられなかったり、本格的な調査を行っても断片的な情報しか得られないケースが増えている（※本稿公表時）。

・そのため、一現場だけで攻撃手法や使われた攻撃インフラを網羅的に把握することが難しいケースが増えており、複数事案で見つかった断片的な情報を組み合わせなければ、IoC の把握すらままならない場合がある。

・断片的な IoC 情報は、当該被害に気付くことはできても、網羅性がないため、攻撃者の追い出しに失敗したり、マルウェアの取りこぼしや被害範囲の調査不足を招く恐れがある。

〇どうするべきだったのか

初動段階で IT ベンダ B 社が専門組織 C など、外部の専門組織との間で情報共有を行うことができていれば当初の段階からマルウェア Y や他の通信先に関する IoC 情報を入手出来ていた。

他方で、IT ベンダ B 社は秘密保持契約が念頭にあり、外部に照会が行えないと考えて単独での調査を行っていた可能性もあり、事前に被害組織 A と IT ベンダ B 社との間で、インシデント発生時の外部連携の手はずや外部に照会可能な情報の範囲などに対する合意があるべきだったともいえる。
結果として、被害組織 A 自身が各方面への照会作業を行うこととなったが、専門組織 A は必ずしも当該システムに技術的に詳しいわけではなく、IT ベンダ B 社が専門組織 C 社とやりとりができた方がスムーズであった。

この事案では、

・IT ベンダ B 社が外部専門組織と連携できていなかった
・（初動対応ミスの後の）専門組織 C とのやりとりと被害組織 A が行うことになってしまった
・専門組織 C とのやりとりを被害組織 A が行ったことでスムーズな連携ができず追加調査やこれに必要な情報の入手・理解に時間／手間がかかってしまった

と、繰り返し、被害組織 A に対応コストが発生してしまったことになる。

【（本来のやるべきだった）ポイント】
・平時から、IT ベンダ B 社との間で、外部専門組織との情報共有について合意や契約上の必要な措置を行っておく。
・インシデント発生時に問い合わせるべき専門組織（調査に必要な知見を持つ組織）が見つかったが、IT ベンダ B 社が普段連携してない組織であったとしても、IT ベンダ B 社と当該専門組織間でスムーズな情報共有が行えるよう許可する。

※以下のケース 2 では、ランサムウェア攻撃の事例について、ケース 2 －A：バッドケース、ケース 2 －B：通常の対応ケース、ケース 2 －C：ベストケース、の 3 パターンにわけてケーススタディを示します。

ケース２―A：バッドケース
ファーストレスポンダーの知見が不足していたため、被害組織側の追加負担が発生したもの

①初動対応フェーズ

被害組織 A でランサムウェア攻撃が発生し、セキュリティ事故対応やフォレンジックも行っているという IT ベンダ B 社に調査依頼を行った。

B 社は攻撃に使われたランサムウェア X を発見したが、ランサムウェア X がランサムウェア Y の亜種であるということまで特定したものの、ランサムウェア X は大量の亜種があり、当該事案で見つかった特徴（ランサムノートや暗号化後の拡張子）を持つ亜種やこれを用いる攻撃グループに関する情報は有しておらず、また、公開情報で調査した範囲でもこれ以外の情報は見つからなかった。

他方で、直近で B 社が対応したランサムウェア攻撃では SSL-VPN 製品から侵入したと思われる事案があり、また、ランサムウェア攻撃の一般的な傾向としても当該侵入経路について取りざたされていたこともあり、本事案についても侵入経路の可能性があるのではないかと推測し、調査を進めた。

調査を進めたところ、当該 SSL-VPN 製品のＯＳのバージョンが古く、悪用が確認されている複数の脆弱性が残留したままの状態であることが判明した。当時のアクセスログ等は保存されていなかったため、当該製品が侵入経路となった直接の証拠は得られなかったものの、ランサムウェアに限らず、当該脆弱性を悪用した攻撃が海外で発生したケースについて公開情報もあったことから、当該　SSL-VPN 製品の脆弱性を悪用されて侵入されたのではないかと推測し、B 社から被害組織 A に報告がなされた。

図 56

②セカンドオピニオンフェーズ

IT ベンダ B 社による調査報告を踏まえて、被害組織 A は再発防止策（SSL-VPN の認証情

報リセットや二要素認証の導入、脆弱性対応体制の見直し）を検討し、被害公表のほか、所管省庁への報告を行った。

所管省庁からは、「似たようなランサムウェア攻撃被害事案の報告を受けたのだが、侵入原因が異なっている。本件、専門機関 C にセカンドオピニオン的に相談してはどうか？」と連絡があったことから、専門機関 C に改めて相談を行った。

専門機関 C からは、本件はランサムウェア X を使う攻撃グループ Z によるものであり、侵入原因は SSL-VPN 製品の脆弱性悪用ではなく、まったく別の Web サーバの脆弱性悪用ではないかと指摘された。
本件事案発生時には当該 Web サーバのバージョンが古く、悪用可能な脆弱性が残留していたことが分かったため、再度、当該 Web サーバの調査を行うこととなった。

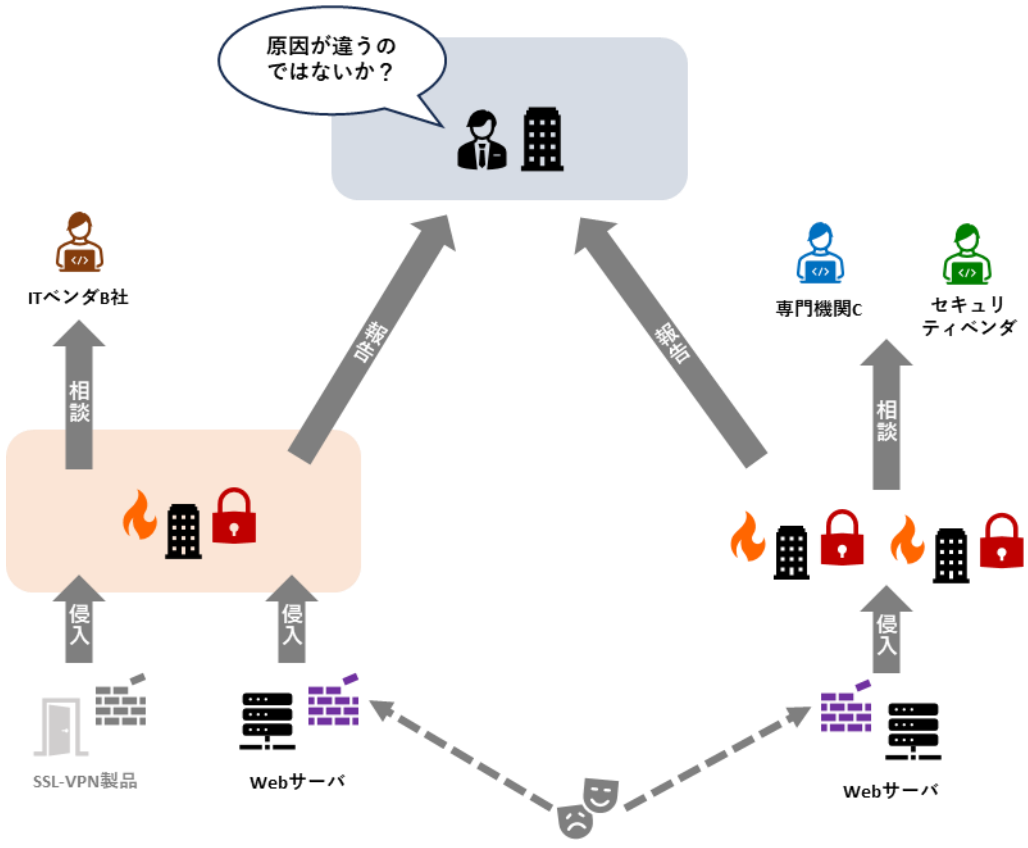


図 57

③再調査フェーズ

あらためて、セキュリティベンダ D 社に依頼を行い、Web サーバの調査を行ったところ、当該攻撃時期の直前に不審な IP アドレスから脆弱性を突くためと思われる通信がなされていたことが判明した。

また、Web サーバのほか、当該 Web サーバからアクセス可能な他のサーバにマルウェアが残留しており、不審な通信が出ていたことも判明した。

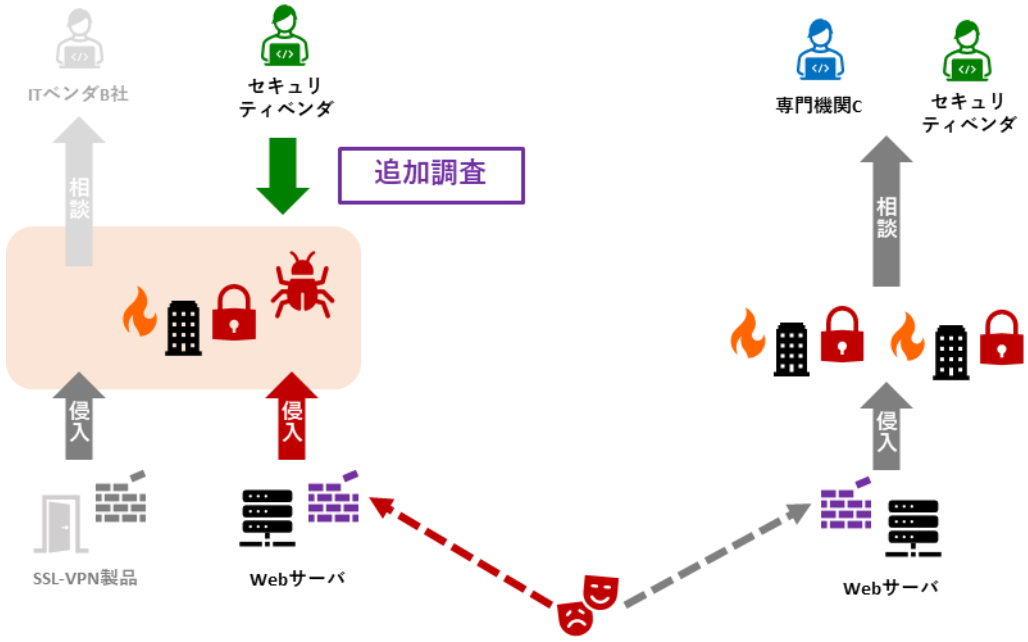


図 58

【初動対応が失敗に終わった原因】

・ランサムウェア攻撃対応では、侵害原因や侵害範囲（横展開）の調査に必要なログデータやツール等も棄損している場合があるため、調査が困難なケースも多く、また、侵害経路として多用されている。SSL-VPN 製品まわりは調査に必要なログが保存されていないか極めて少ない場合が多いため、原因特定は推測程度で終わることが多い。

・他方で Web サーバの脆弱性を突いたり、侵害後にいわゆる標的型攻撃で用いられるようなマルウェアやテクニックを利用するような、ある程度のスキルを有するランサムウェアの攻撃者もいるため、標的型攻撃と同程度の調査が必要なケースもある。

・今回のケースでは初動対応支援にあたった、ファーストレスポンダーである IT ベンダ B 社に上記のような想定もなく、また、ランサムウェア X を用いる攻撃グループ Z に関する情報がなかったため、適切な原因特定やマルウェアの駆除が行えなかったものである。

○【解説】バッドケース回避のためにどうするべきだったのか

IT ベンダ B は、ランサムウェア X がランサムウェア Y の亜種であるところまで特定できていたが、攻撃グループ Y の特定まで至れなかった。
その際に、自らの知見にないことと、公開情報に該当するような情報がないことの 2 点をもって、これ以上の調査を行っていないが、この時点で専門機関 C やそのほか攻撃グループ Y の他の被害事案を見ているセキュリティベンダ等との間で情報共有が行えていれば、必要な情報を初動段階で入手できていたのである。

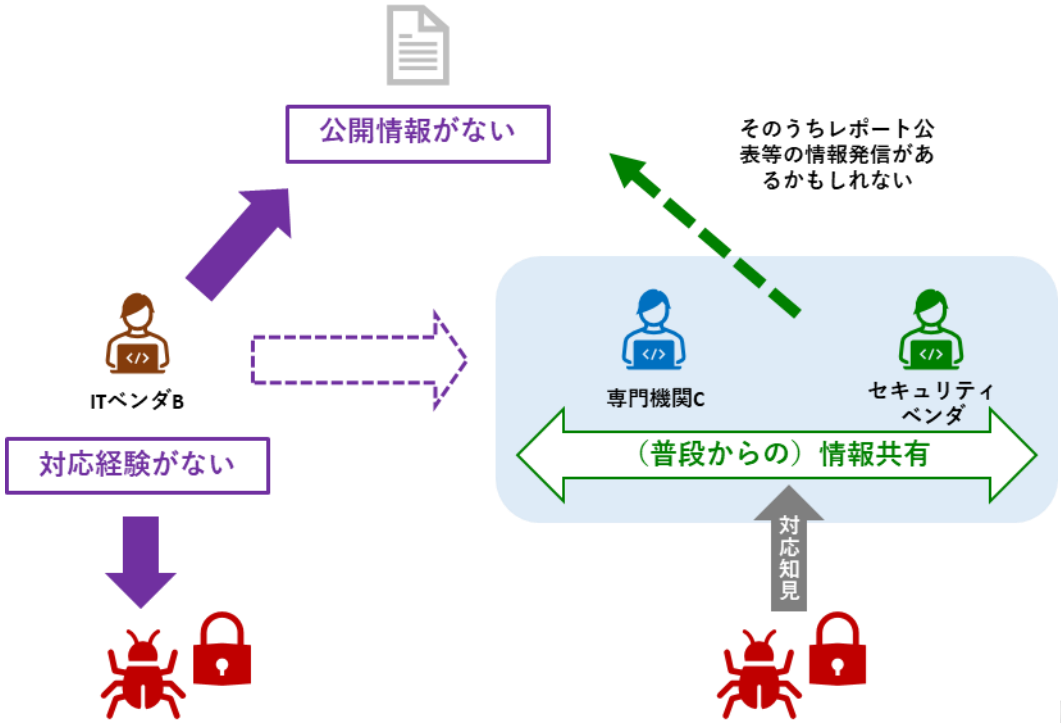


図 59

【(本来のやるべきだった) ポイント】

・ランサムウェア攻撃については事案が多く、例えば標的型サイバー攻撃ほどセキュリティベンダによるインシデント対応事例の詳細レポートが公開されにくい傾向にある（※本稿公開時点）。そのため、「公開情報がなかった」ことをもってして、ランサムウェアの特定や攻撃グループの特定に関する調査を終えるのは不十分であり、専門組織間の情報共有から、非公開情報としての攻撃活動や TTPs 等の情報入手をすべきである。

・とはいえ、今回のケースのような（比較的）特異な侵害経路やマルウェア投入等を行うアクターと比較的スキルが低く、そこまでの調査／追い出し等を必要としないアクターによる被害事例と初動対応初期に峻別することは難しいため、平時から情報共有を行っておく必要がある。

ケース２―B：通常の対応ケース
被害組織が情報共有コストを負担しているもの

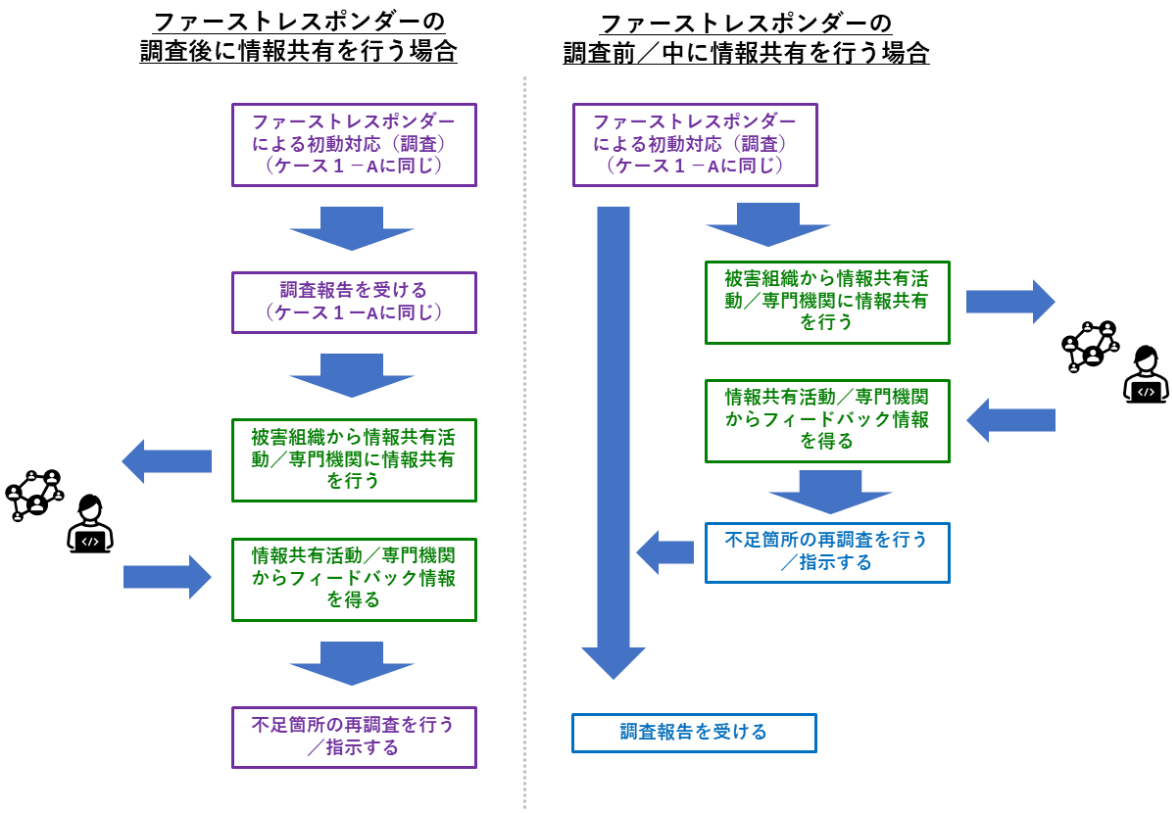


図 60

＜選択肢１＞ファーストレスポンダーの調査後に情報共有を行う場合

（初動対応については前述のケース２－A：バッドケースと同じ。）
IT ベンダ B 社から報告を受けたのち、被害組織 A は報告の内容をもとに、参加している情報共有活動へ（又は、情報共有活動のハブ組織である専門機関へ）、情報共有を行った。

ある情報共有活動では、ランサムウェア X によく似た被害事案について、調査中ではあるものの、侵入原因はある Web サーバ a の脆弱性を突いたものではないか、と推測する情報を得ることができた。その後、専門機関Cからは、ランサムウェアXを使うのは攻撃グループZであり、この攻撃グループはこれまでも度々、様々な Web サーバの脆弱性を突いて侵害しているとの回答があった。
このフィードバック情報を踏まえて、被害組織A は Web サーバ a を中心に IT ベンダ B 社又はセキュリティベンダ D 社に追加調査／再調査を依頼することとなった。
（初動対応については前述のケース２－A ：バッドケース③再調査フェーズと同じ。）

＜選択肢２＞ファーストレスポンダーの調査前／調査中に情報共有を行う場合

IT ベンダ B 社に初動対応の依頼を行うとともに、並行して被害組織 A から参加している情報共有活動へ（又は、情報共有活動のハブ組織である専門機関へ）、情報共有を行った。

ある情報共有活動では、ランサムウェア X によく似た被害事案について、調査中ではあるものの、侵入原因はある Web サーバの脆弱性を突いたものではないか、とする情報を得ることができた。その後、専門機関Ｃからは、ランサムウェアＸを使うのは攻撃グループＺであり、この攻撃グループが直近の攻撃活動である Web サーバの脆弱性を突いて侵害しているとの回答があった。

このフィードバック情報を踏まえて、被害組織 A は IT ベンダ B に Web サーバ側を追加調査するよう依頼を行った。

しばらくの後、調査の結果、当該攻撃時期の直前に不審な IP アドレスから Web サーバの脆弱性を突くためと思われる通信がなされていたことが判明した。また、Web サーバのほか、当該 Web サーバからアクセス可能な他のサーバにマルウェアが残留しており、不審な通信が出ていたことも判明した。

【問題点】

・被害組織 A 自身からのアクションで照会をかけていなかった場合、必要な情報や調査のヒントを得るまでに相当の時間がかかり、ケース２－A のような結果になっていた可能性もある。

・あるいは必要な情報について情報共有活動／専門組織から得るにあたって、被害組織の知見不足やインシデント対応に不慣れなことなどから、情報の入手に時間がかかったり、伝達ミスが発生する恐れもある。

ケース２―C：ベストケース
専門組織同士の情報共有により適切な初動対応を行えたもの

①初動対応フェーズ

被害組織 A でランサムウェア攻撃が発生し、セキュリティ事故対応やフォレンジックも行っているという IT ベンダ B 社に調査依頼を行った。B 社は攻撃に使われたランサムウェア X を発見したが、ランサムウェア X がランサムウェア Y の亜種であるということまで特定したものの、ランサムウェア X は大量の亜種があり、当該事案で見つかった特徴（ランサムノートや暗号化後の拡張子）を持つ亜種やこれを用いる攻撃グループに関する情報は有しておらず、また、公開情報で調査した範囲でもこれ以外の情報は見つからなかった。
他方で、直近で B 社が対応した別のランサムウェア攻撃では SSL-VPN 製品から侵入したと思われる事案があり、また、ランサムウェア攻撃の一般的な傾向としても当該侵入経路について取りざたされていたこともあり、本事案についても侵入経路の可能性があるのではないかと推測し、調査を進めた。
調査を進めたところ、当該 SSL-VPN 製品のＯＳのバージョンが古く、悪用が確認されている複数の脆弱性が残留したままの状態であることが判明した。当該脆弱性を悪用した攻撃が海外で発生したケースについて公開情報もあったことから、当該　SSL-VPN 製品の脆弱性を悪用されて侵入されたのではないかと推測したが、当時のアクセスログ等は保存されておらず、また、これ以外に調査に使えそうな関連機器のログデータは暗号化されたサーバ内にあったため調査に使うことができなかった。
そこで IT ベンダ B 社は自組織が参加する専門組織同士の情報共有活動（又は、専門組織同士の情報共有活動に参加する専門機関）に情報共有することとした。

図 61

【ポイント】
・ランサムウェア攻撃事案対応では、どうしても復旧対応が優先されがちであり、また、ログデータの毀損などもあり、侵入原因調査が手薄になるケースが多く、封じ込め／攻撃者の追い出しができておらず、初動対応後も攻撃者が侵入したままであったり、同じ経路から別の攻撃を受ける恐れがある。
・APT と異なり、アクターの追跡やグルーピングも不足しているため、攻撃グループの特定からおおよその侵害経路を絞り込むアプローチも難しく、上記のように「〇〇経由で侵入したのではないか」と推測程度で結論づけてしまう事案も多い。
・自組織で対応知見がなく、また関連する公開情報がないというだけで判断せず、当該時点では「非公開の情報を持っている専門組織がいるかもしれない」という前提で情報共有を行うことが必要である。

②情報照会フェーズ

IT ベンダ B 社は情報共有活動に当該事案対応の状況について情報提供した。

情報照会のポイント：

・どのような証拠／推測から、マルウェア（ランサムウェア）や侵害経路の特定を行ったのか／行っている最中なのか記す。

・ログの不足などフォレンジック対象の消失／棄損等のため、あくまで状況証拠的な推測であるのであれば、その旨を明示的に示す。

＜実際の提供情報（イメージ）＞

種類：
ランサム＊＊＊だと思われますが、分析中です。

ランサムウェア：
MD5： 1126a5562a3e 04103e2e7f **********
SHA256：1a7b03257a34ce9edf**********eb44d022c4215438a23ee76d27c1b4569c8c

暗号化後の拡張子名：
＊＊＊＊

ランサムノート：
添付のとおり。内容からすると、過去のランサム＊＊＊＊の文面に酷似しています。

侵害原因等について：
当該被害組織は SSL-VPN 製品 A を使っており、最後に OS のアップデートが行われたのが、2022 年〇月であったことから、CVE-2022-*****が残留したままでした。ランサム＊＊＊＊が CVE-2022-*****を悪用したという海外レポートもあるため、この脆弱性が悪用されて侵害されたのではないかと推測していますが、アクセスログ等が保存されていないため、確証はありません。

まったく同じランサムウェアではないが、元々同じランサムウェアのビルダーを用いて作られた「別ブランド」のランサムウェア Y による事案を対応していた専門組織 C からフィードバックがあり、以下の情報提供がなされた。

＜専門組織 C からのフィードバック＞

・攻撃グループ Z が何度か「リブランド」的にランサムウェアを変えながら攻撃活動をしており、ランサムウェア X のビルダーを用いている。ランサムウェア Y は攻撃グループ Z が用いているのではないかと思われる。

・攻撃グループ Z は SSL-VPN 経由で侵入することはなく、毎回何らかの Web サーバの脆弱性を突いて侵入してくる。攻撃時期や標的によって、どの Web サーバを狙うかは異なる。

また、別の専門組織 D からは

＜専門組織 D からのフィードバック＞

・ランサムウェア Y が使われた被害現場では、マルウェア W も見つかっている。直近で見た事案では、ファイル名から推測するに Web サーバ a のコンポーネントを偽装したファイルがいつくか見つかっており、DLL サイドローディングによりマルウェア W を読み込んでいると思われる。

・Web サーバ a については最近脆弱性（CVE-2023-*****）が公表されており、海外ベンダのレポートでは悪用事案が報告されている。これを悪用された可能性もあるのではないか。

とのコメントがなされた。

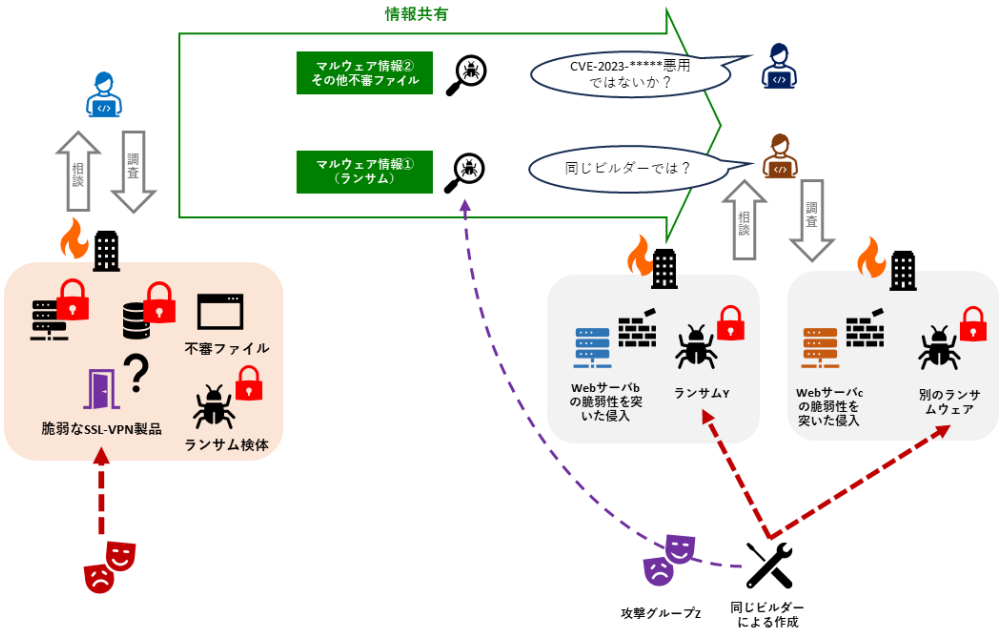


図 62

③フィードバックフェーズ

専門組織 C と D の情報から、専門組織 C が追跡している攻撃グループ Z が Web サーバ a の脆弱性を悪用して侵害し、その後 DLL サイドローディングによりマルウェア W を投入して侵害拡大していった攻撃シナリオが想定された。
IT ベンダ B が事案対応している被害組織では Web サーバ a の脆弱性（CVE-2023-*****）が残留する状態で稼働していたことから、これが侵害経路だった可能性が強まった。

その後の調査により、ランサムウェア被害の発生前に Web サーバ a に不審なアクセスや Web サーバ a の脆弱性（CVE-2023-*****）を悪用したアクセス試行の痕跡が見つかり、また、想定通り、マルウェア W もみつかった。ここを橋頭保として AD サーバや暗号化被害のあったサーバに不審なアクセスがなされていたことが判明し、侵害原因や侵害後の横展開の経路が判明したとして、被害組織 A に報告を行った。

マルウェア W が外部と通信していた痕跡も見つかり、マルウェア W の情報のほか、新たに見つかった不正通信先やその他 TTPs 情報について、被害組織 A への報告とともに、情報共有活動にフィードバックを行った。

フィードバック情報提供のポイント：
・事前に情報共有活動からもらった情報以外に新規に発見した情報を提供する。
・追加で提供したフィードバック情報の情報共有（再展開）可否について示す。

＜実際の提供情報（イメージ）＞

TLP：AMBER　（※他各共有活動で定めた方法で記載する。）

調査をすすめたところ、以下の情報が見つかりましたので、共有します。
Web サーバ a に CVE-2023-*****悪用の痕跡が残っており、海外セキュリティベンダ D 社が先日公表した CVE-2023-*****に関する検証レポートに記載されたものと同じファイルパスへのアクセスがありました。今回のランサムウェア Y を用いた攻撃は、Web サーバ a の脆弱性を突かれたことが侵害原因だったと考えられます。

（省略）

マルウェア W：
ファイル名：

MD5： 1126a5562a3e 04103e2e7f **********
SHA256：1a7b03257a34ce9edf**********eb44d022c4215438a23ee76d27c1b4569c8c

通信先／通信元：
① Web サーバ a の脆弱性（CVE-2023-*****）を悪用した不正アクセス元
（略）

② マルウェア W の通信先
（略）

【ポイント】

・調査で見つかった攻撃技術情報については可能な範囲で「フィードバック」として当該情報共有活動に共有を行う。

・情報共有により得られた情報で個別の被害現場の調査が適切に行われるだけでなく、共有活動全体として新たな情報が更新されることが必要である（次頁を参照）。

○『解説』専門組織間の情報共有と事案対応現場からのフィードバックによる情報の更新

一連の情報共有（被害現場からの照会⇒応答）とこれを踏まえた調査結果のフィードバックにより、元々専門組織 C、D が有していた情報や既に公開情報として流通していた情報に加えて、新たな IoC や TTP 情報を追加・更新できたのである。こうした新たにみつかった情報が情報共有活動や注意喚起、分析レポートを通じて拡散することで攻撃者の手法を陳腐化させたり、被害拡大予防に活用されることになる。

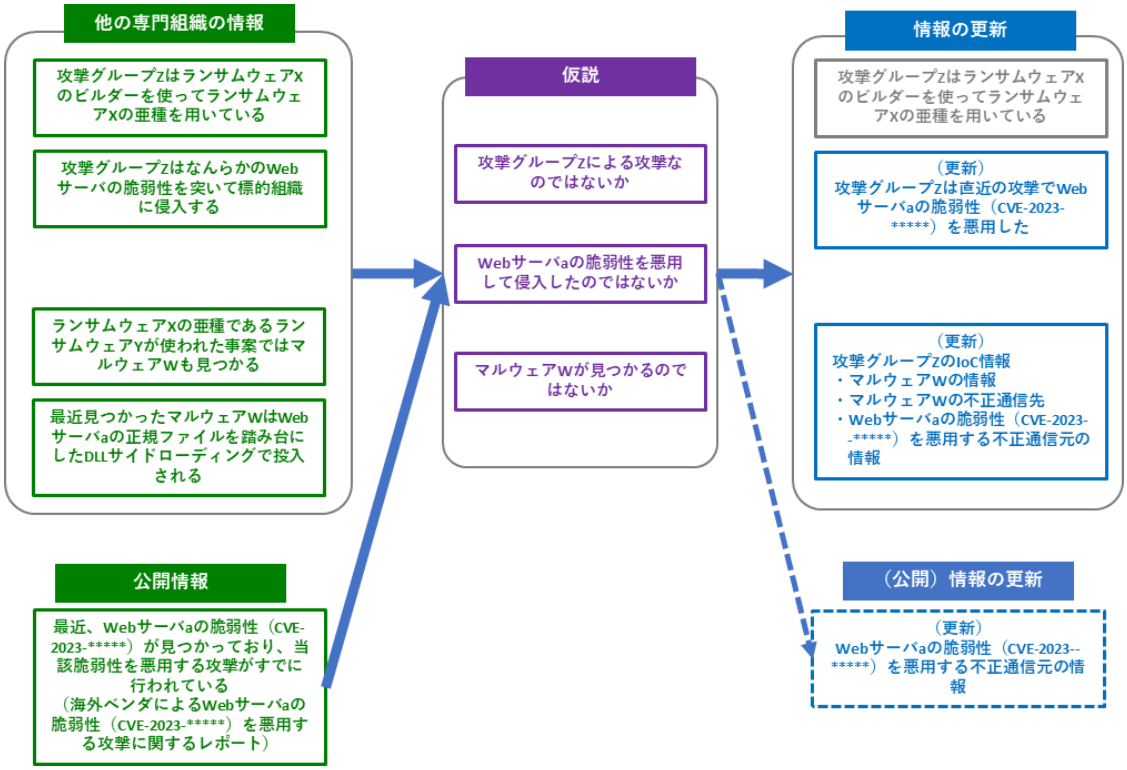


図 63

【ポイント】

・攻撃者は分析レポート等を通じて情報が拡散しはじめると、該時点での攻撃手法の有効性が下がり、手口を変更する場合がある。長期間攻撃キャンペーンを行う場合、マルウェアやいくらかの TTPs が変更されるが、基本的な戦術やスキルは大きく変わらないため、引き続き攻撃活動／グループの追跡・対処がなお有効である。

・ただし、マルウェアやその他のツール変更や、（今回のケースであれば）初期侵害経路として悪用する脆弱性／対象ホストの変更により、次の攻撃の検知が遅れる可能性があるため、事案ごと／攻撃キャンペーンごとにどのような TTPs の変化があったのか、フィードバック情報をもとに「検証」していくことが求められる。

・こうした「検証」は、専ら個別の専門組織からの分析レポートの公表やカンファレンス発表などの場を通じて、間接的に行われていくことが多いが、それでは次の攻撃への対処のタイミングが間に合わなかったり、公開情報としては出せない情報が存在する可能性もあるため、こうしたクローズドな場での情報共有を通じた「検証」も並行して行われるべきである。

○【解説】ケース２―A～C を通じて、被害組織の「コスト」はどう変わったのか

まず、ケース２―A：バッドケースでは、再調査が発生しており、追加の調査費用負担のほか、既に被害公表を行ってしまっている場合、公表内容の修正やステークホルダーへの報告のやり直しなど、レピュテーションリスクや対応リソースの追加負担が発生します。

ケース２－B：通常の対応ケースでは、ケース２―A ほどのコスト負担は発生していないものの、ランサムウェア被害からの復旧や業務への影響、対外応答へのリソース負担がある中で、さらに外部情報共有活動／専門機関とのコミュニケーションをという対応コストが重なることになります。また、被害組織自身が外部専門組織とコミュニケーションをやること自体の効率の問題やデメリットも発生します。
さらに、並行して IT ベンダによる調査が行われていますが、被害組織が情報共有活動から調査に必要な情報を得るまでの間に、並行する調査が見当違いな調査（ケース２－A）を進めてしまっていた場合、相当の「手戻り」が発生することになります。

被害組織における各種対応コストの変化

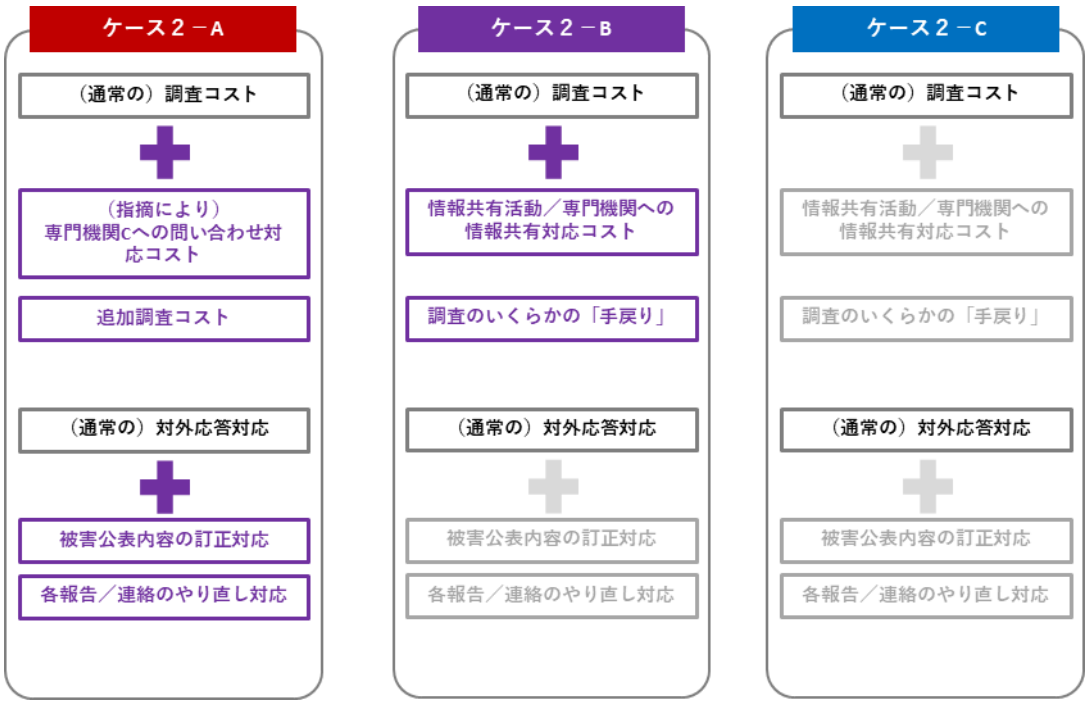


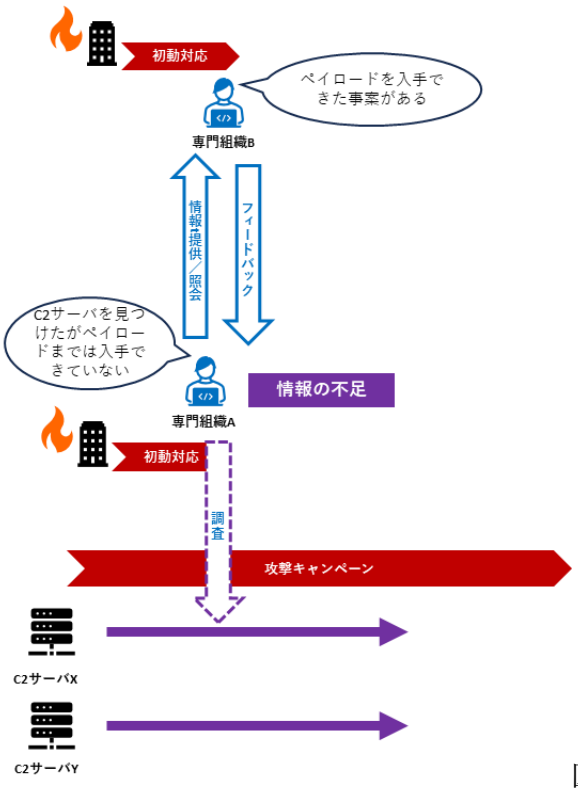
図 64

ケース３：
APT 攻撃キャンペーン初期の段階で、複数の事案に対応している専門組織同士の情報共有により攻撃キャンペーン途中の攻撃活動を捕捉し攻撃技術情報の展開を行えたケース

①情報提供／照会フェーズ

ある APT 事案の初期侵害（の試み）を見つけた専門組織 A は、通信先 X への通信を見つけたものの、通信先 X からダウンロードされると見られるペイロードらしきものを被害組織では確認されず、また、通信先 X を調査したが、ペイロードの取得までにはいたらなった。ダウンロードされるであろうペイロードが最終的なペイロードなのかも不明なため、現時点で攻撃が途中で終わったのか、それともなおも侵害されているのか判断をすることができない状態にある。

そこで、専門組織同士の情報共有活動に対して、通信先 X の情報や、既に見つかっているダウローダーなどの情報を共有したところ、同じ攻撃によるインシデント対応を行っていた専門組織 B から、ペイロードのハッシュ値や、次に感染するマルウェアの通信先Yの情報を得ることができた。



【ポイント】

・それぞれ対応している事案のコンテクスト情報は明かしていない。

・この時点で専門組織 B はペイロードまで入手できており、情報共有活動に積極的に参加する必然性がないように見えるが、今回の攻撃キャンペーンで使用されている通信先をすべて把握できているか専門組織B自身が確認することはできないため、情報共有活動上でのやりとりを踏まえて自組織の情報の不足を知るほかない。

図 65

(専門組織 A から他の専門組織への情報照会のイメージ)

情報照会のポイント：

・どの時点の通信を確認していて、それ以前の状況をそこまで把握しているのか／できていないのか記す。
・通信先／マルウェア情報が当該時点において公開情報として流通しているものなのかどうか記載する。
・本事例のように C2 サーバからのペイロード取得を試みたのであれば、いつ調査を行ったのか日時を記す。

＜実際の提供情報（イメージ）＞

攻撃時期：
下記通信先への通信が〇月×日頃に発生しているのを確認しているが、それ以前の侵害状況については不明。

通信先情報：
198.51.100[.]***

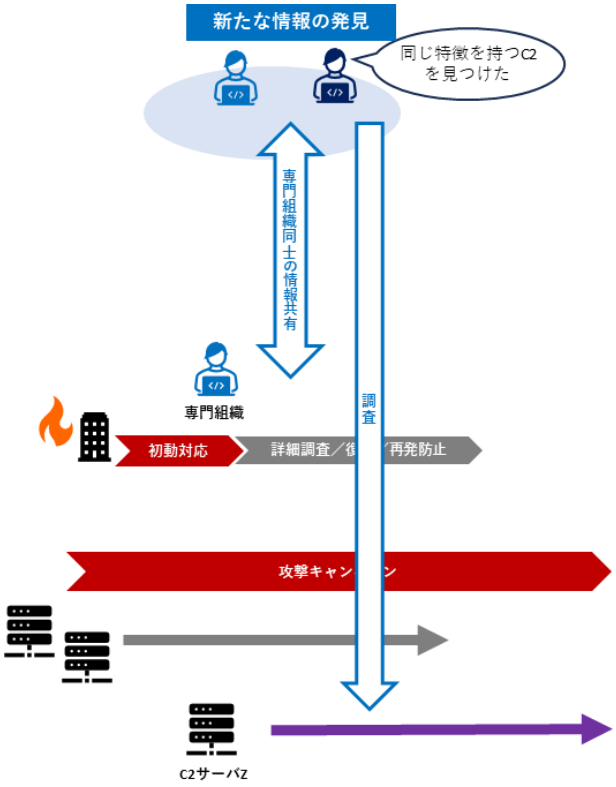
マルウェア情報：
下記ダウンローダーを思われるマルウェアが上記通信先に通信しており、何らかのペイロードを落として来ると思われるが、ペイロードは確認できていない。

MD5：～
VirusTotal に同種の検体がいくつか上がっていますが、現時点で分析レポート等の公開情報は確認できていません。

攻撃インフラについて：
弊社で上記 C2 サーバを確認した時点（△月〇日）では既に C2 サーバは稼働しておらず、ペイロードの入手はできませんでした。

②新たな情報の作出フェーズ

同じ専門組織間の情報共有活動に参加する専門組織 C は、専門組織 A、B から提供された C2 サーバ X と Y に関する情報から、同じ特徴を持つ C2 サーバ Z が稼働していることを発見した。紐づくドメインの取得状況や当該 C2 サーバの稼働開始時期などの情報から、C2 サーバ Z は構築されたばかりにて、本攻撃キャンペーンにおいてこれから本格的に使用されるのではないかと推測された。



【ポイント】

・専門組織 C は①のフェーズでは情報提供をしていないが、専門組織 A と B が提供した情報をもとに、C の知見が活用されたことで A、B、C の 3 者が未認知だった通信先 Z を新たに見つけることができた。

・また、この稼働直後の C2 サーバを捕捉できたのは、フェーズ①が攻撃キャンペーンの初期の段階で行われたからであり、専門組織 A が「もう少し調べてから共有しよう」と考えていた場合、C2 サーバ Z が攻撃に使われた後、あるいは既にある程度被害が出てからの捕捉タイミングになっていたかもしれない。

図 66

③情報展開フェーズ

専門組織 C は情報共有活動のハブ組織として活動しており、新たに見つけた通信先 Z を含めた、一連の情報をインディケータ情報として情報共有活動に展開した。また、専門組織 A や B も自社製品・サービスを提供するユーザー組織に当該情報を同じく展開した。

その結果、専門組織 C がハブ組織として活動する情報共有活動参加組織のいくつかにおいて、通信先 Z を用いた攻撃の試みを早期に検知することができ、そのフィードバック情報が寄せられた。

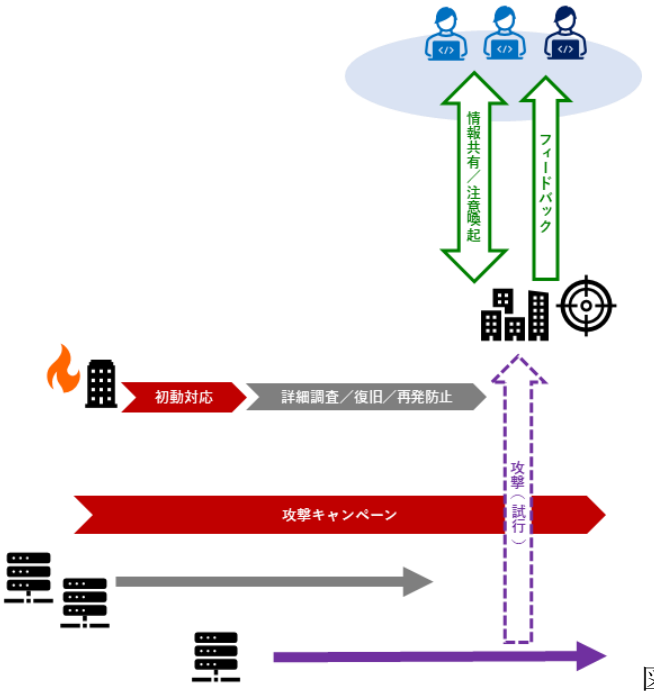


図 67

【ポイント】

・この情報共有活動では共同で作出した情報をそれぞれの情報共有活動外の目的（営利目的を含む）で活用することが認められている。

・他方で、当該情報の展開で得たフィードバック（のうち技術的な情報や統計的情報）については積極的に情報共有活動側に共有することが期待されている。

＜本ケース全体のポイント＞

・本ケースは攻撃キャンペーン初期の段階で複数の専門組織が情報共有・連携することで、攻撃キャンペーンの途中で被害組織／標的組織の早期認知／被害拡大防止につながった事例であるが、前述のとおり、専門組織 A がインシデント対応の早い段階、特に情報が少なく、技術的分析が不十分な段階でも情報共有を行ったことで、全体として早いタイミングでの攻撃対処が行えたものである。専門組織 A が情報不足を理由にさらに長い期間、自組織だけでの調査分析を進めていたが場合、その後情報共有が行えたとしても既に通信先 Z を使った被害が多発した後であったかもしれない。

・また、これらの情報共有活動は非公開で行われており、③での情報展開も非公開の情報共有活動や各組織が提供する製品／サービスを通じて行われたことで、情報の公開などにより攻撃者に対処動向が気づかれることなく、攻撃キャンペーンを中断させることが

できたものである。本稿の主たるスコープから外れるものの、専門組織同士の連携の中で、攻撃キャンペーンの進捗状況や、自らの情報展開先である程度十分な標的範囲にリーチできるのか（※非公開・直接通知でなく、公表による注意喚起の方が必要なのではないかといった検討）について共同で検討が行われたことも重要なポイントである。非公開での専門組織間連携にこだわりすぎ、自分たちがリーチできない標的組織への攻撃被害を見逃してしまっていては元も子もないからである。

ケース４：
製品の脆弱性を悪用したと思われる攻撃キャンペーンを特定し、脆弱性が残留するホストの利用者への対応を行うケース

①情報提供／照会フェーズ

製品 X の何らかの脆弱性を悪用したと思われる被害事案を対応した専門組織 A から攻撃に関する情報共有が行われた。

専門組織 A は様々な調査を行っているものの、初動対応支援の時点では具体的な脆弱性の特定に至れておらず、他の専門組織に照会が行われた。専門組織 A が対応した被害現場では当該製品のソフトウェアバージョンが 1 年前のもので数バージョン古く、この間に数件の脆弱性情報が公表されており、うちいくつかはメーカーや専門組織から注意喚起が出されているものであった。

同タイミングで類似の事案の対応を開始した専門組織 B からの情報共有があり、また、これまで当該製品の脆弱性を調整してきた専門機関も加わり、悪用された脆弱性の特定（CVE-2023-*****）が行われた。

専門組織 B が見ている被害組織では当該製品はひとつ前のバージョンで稼働していたことから、悪用された脆弱性を一つに絞ることができた。また、被害組織 A が行ったその他の侵害状況の調査結果が、CVE-2023-*****が悪用された場合に想定される攻撃シナリオとも一致していたことから、本件は CVE-2023-*****悪用による攻撃であると特定された。

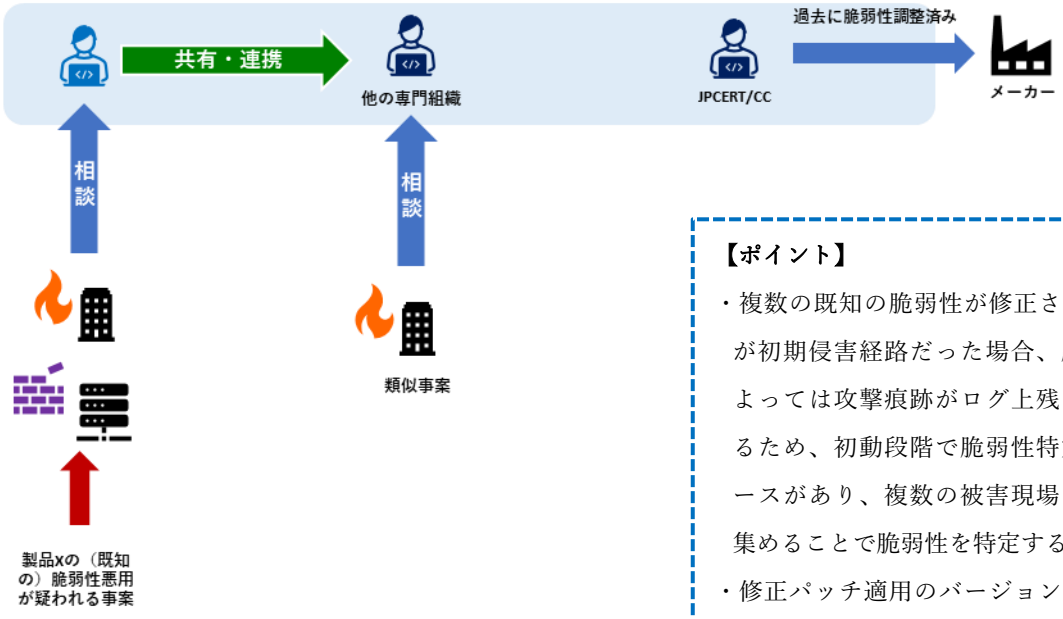


図 68

【ポイント】

・複数の既知の脆弱性が修正されていない製品が初期侵害経路だった場合、脆弱性の種類によっては攻撃痕跡がログ上残らないものもあるため、初動段階で脆弱性特定に至れないケースがあり、複数の被害現場における情報を集めることで脆弱性を特定することがある。

・修正パッチ適用のバージョン／タイミングがそれぞれ異なる侵害ホスト／事案を比較することでどの脆弱性が悪用された可能性があるのか絞り込むことが可能である。

②対処検討フェーズ

今回の攻撃活動で悪用された脆弱性が残留しているホストを Shodan/Censys 等で検索したところ、国内に多数存在していることが判明した。また、当該脆弱性が残留するホストを探す目的と思われるスキャンや不正アクセス試行が他の専門組織が運用するセンサーにて観測されたことから、攻撃活動がなおも継続中か、他の攻撃者が同様の攻撃を行っている可能性があると考えられた。

当該脆弱性が公表された際にも注意喚起が行われていたが、多くのホストが修正されていない状況であり、また、当該製品はメーカーからユーザーに直接コンタクトするパスを有していないことが判明しているため、注意喚起やメーカーからの連絡以外の方法でこれら脆弱性なホストの利用組織への情報伝達や専門組織 A や B が観測した不正アクセス元の IP アドレスや設置されるマルウェア情報をインディケータ情報として展開することを検討した。

各専門組織が顧客に攻撃技術情報の提供サービスを行っている場合はこのパスを用いて伝達するほか、情報共有活動のハブ組織を担っている専門組織では活動の加盟組織への伝達を行うこととした。

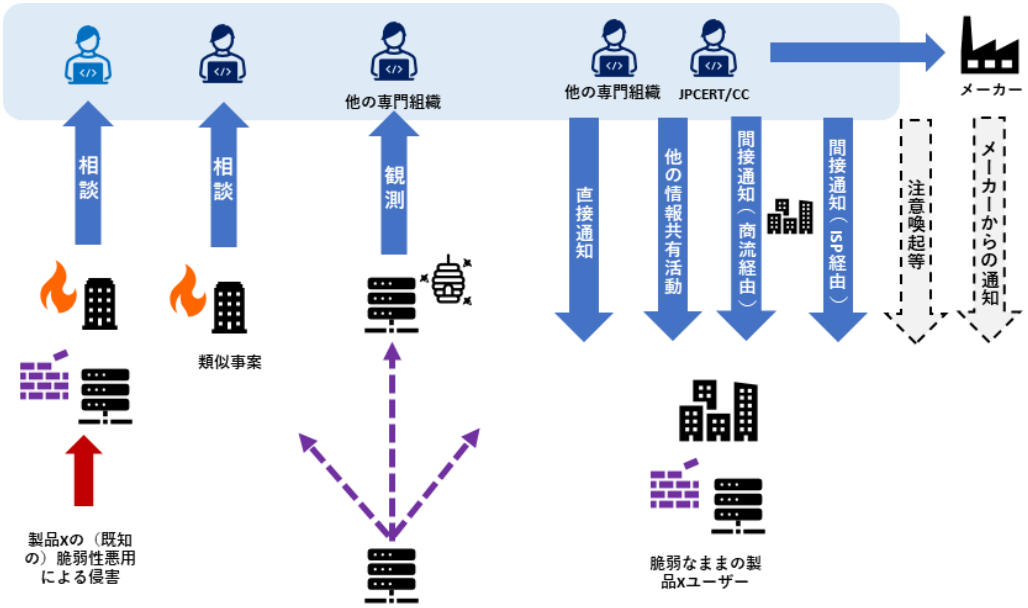


図 69

【ポイント】

・新たな攻撃活動を見つけた場合、自組織の製品・サービスを通じて対策を顧客に提供するだけでなく、レポート公表などを通じて広く注意を呼びかける活動もよく行われている。

・他方で注意喚起等の公開情報の発信は広範囲に伝達できるものの、「到達率」は低いため、情報共有活動や個別通知／間接通知など非公開での情報伝達も組みわせる必要がある。

・こうしたオペレーションを行うには、情報共有活動のハブ組織である組織、メーカー、代理店、運用保守ベンダ、ISP など様々な伝達ルート／機能を持つ事業者等との連携が必要であることから、こうした事業者との調整を行っている専門機関等との連携が必要となる。

③通知・フィードバックフェーズ

共有した情報をもとにしたインディケータ情報を各情報共有活動上に展開したり、脆弱なホストを運用している利用組織への通知をすすめ、被害未認知の組織での早期検知や被害拡大防止のための対応を行った。その結果、これまでに専門組織Ａ、Ｂが把握していなかった不正アクセス元や設置されたマルウェア等の情報を新たに得ることができた。

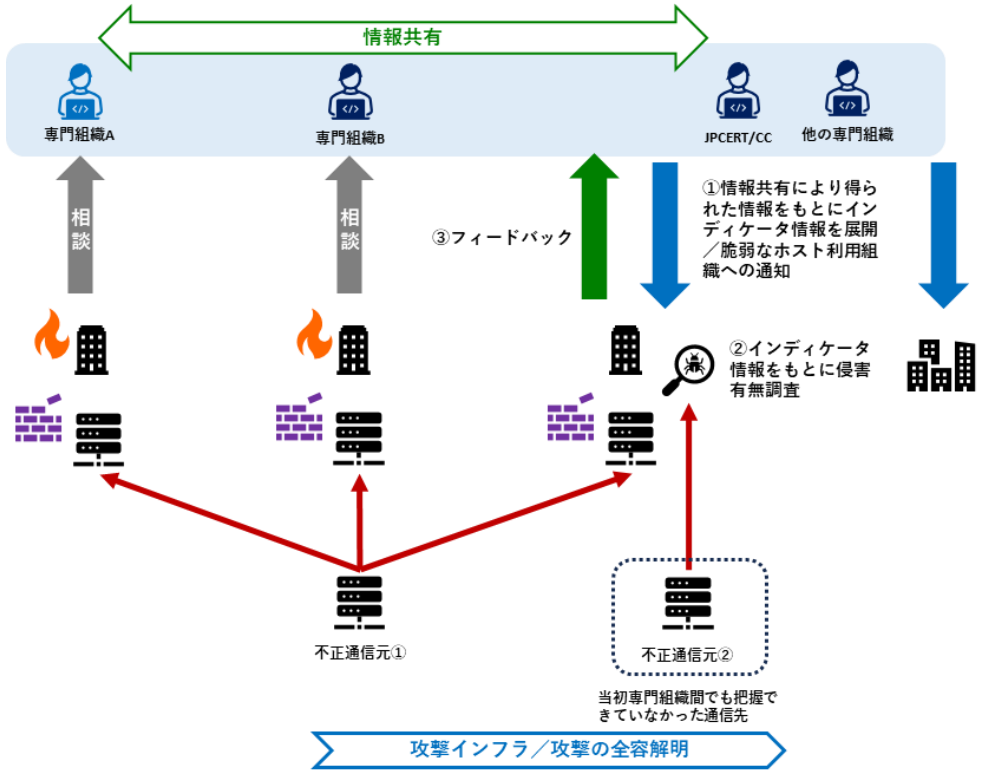


図 70

【ポイント】

・攻撃キャンペーンを終わらせることや、各被害組織の復旧・再発防止とともに、攻撃キャンペーンの全容を解明し、「次の攻撃」に備える必要がある。そのためにある程度の粒度で攻撃グループを特定したり、過去の攻撃キャンペーンとの紐づけたりと攻撃の傾向の分析が必要になる。

・攻撃グループ固有の特徴が残りやすい、マルウェアや TTPs の分析も重要であるが、攻撃インフラの解析も重要である。C2 サーバの認証をかけそこねていたり、本来は見せてはいけないレスポンスを返してしまったりと攻撃者側のミスにより、攻撃者をより特定できる情報を攻撃インフラから得ることができるケースがある。

・攻撃手法の解明だけでなく、「実際に使われた攻撃インフラ」を網羅的に洗い出すことも攻撃者特定に重要な役割を持っているのである。