サイバー攻撃被害の公表、果たして「正解」なんてあるのか？

今日の登壇メンバー

- 佐々木 勇人

  脅威アナリスト JPCERTコーディネーションセンター

  攻撃手法／活動の解明、情報共有活動側の立場

- 蔦 大輔

  弁護士 森・濱田松本法律事務所

  被害組織の被害公表等を支援する側の立場

- 福田 陽平

  記者 NHK科学文化部

  被害組織等を取材し情報を発信する側の立場

登壇者

JPCERT/CC　佐々木

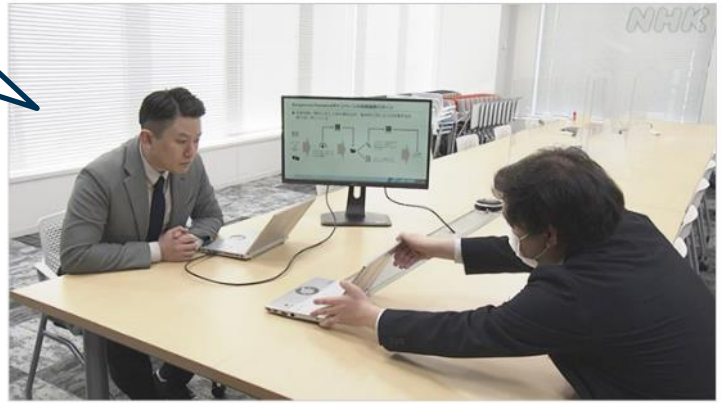
脅威アナリストとして、Lazarusの攻撃活動の分析やインシデント対応支援を行う

“北朝鮮”から届いてました

この偽メール、単なるフィッシング詐欺の類いなのか。

それにしては、社長のアドレスも本物など、手が込んでいる。

私たち（NHK取材班）は、橋本さんの許可を得て、メールをセキュリティーの専門機関に分析してもらった。



サイバー攻撃を受けた企業の支援を数多く手がけているJPCERTコーディネーションセンター。

NHK　福田記者

サイバー攻撃被害企業への取材や専門化への取材を行う

https://www3.nhk.or.jp/news/html/20230117/k10013950641000.html

Lawyer profile

蔦　大輔

Daisuke Tsuta

カウンセル

東京弁護士会所属

TEL: 03-6266-8769

daisuke.tsuta@mhm-global.com

主要な取扱分野

サイバーセキュリティ、個人情報保護、IT・ICT

- サイバーセキュリティ、個人情報保護・データ利活用、電気通信事業等のインターネット事業に関するサポートに取り組む
- サイバー攻撃の予防、攻撃を受けた後の対応に関する助言、サポート、従業員による内部不正についての対応（訴訟を含む）
- 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」、「サイバーセキュリティ関係法令Q&Aハンドブック ver2.0」の策定に関与

著作・論文

- 『類型別　不正・不祥事への初動対応』（中央経済社、2023年、共著）
- 『情報刑法Ⅰ　サイバーセキュリティ関連犯罪』（弘文堂、2022年、共著）
- 『60分でわかる！改正個人情報保護法超入門』（技術評論社、2022年、共著）
- 『法律実務のためのデジタル・フォレンジックとサイバーセキュリティ』（商事法務、2021年、共著）
- 『事例に学ぶサイバーセキュリティ 多様化する脅威と法務対応』（経団連出版、2020年、共著）

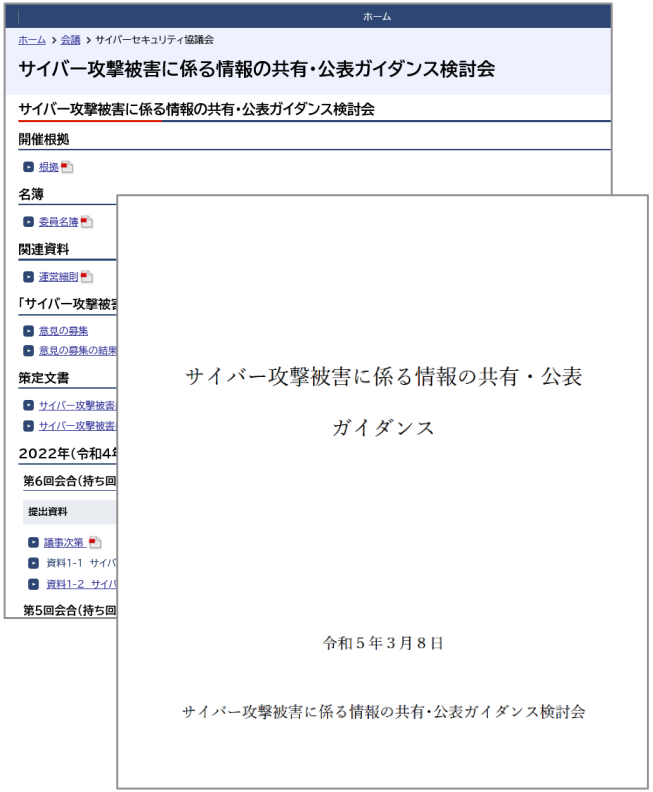
その他、著書・論文・講演多数

経歴

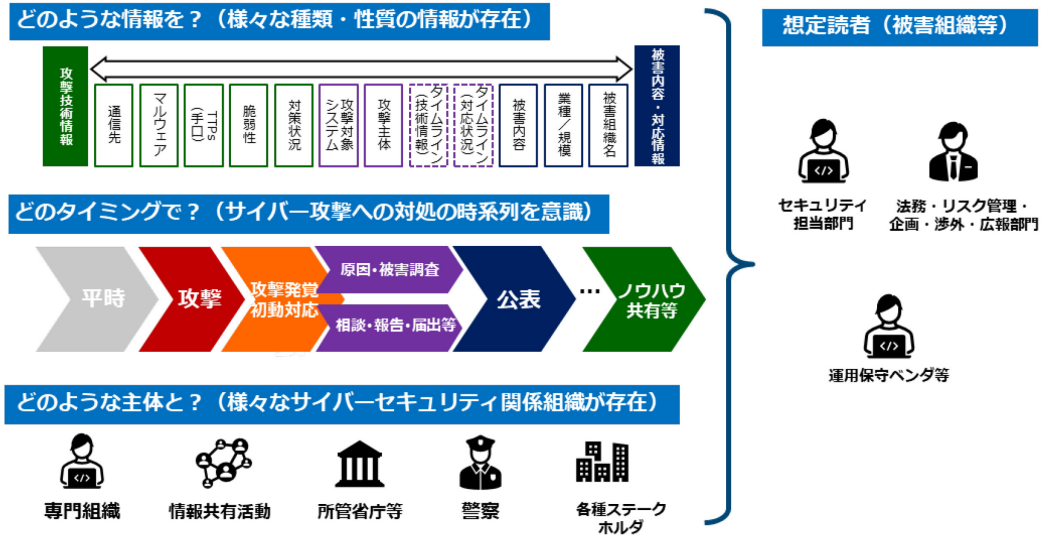
2007年　京都大学法学部卒業
2009年　神戸大学法科大学院修了
2011年　法律事務所勤務弁護士（大阪弁護士会）
2014年　財務省近畿財務局 統括法務監査官 法務監査官
2015年　総務省行政管理局 情報公開・個人情報保護推進室 副管理官
2016年　情報ネットワーク法学会理事（～2020年）
2017年　内閣官房内閣サイバーセキュリティセンター(NISC)　上席サイバーセキュリティ分析官
2019年　東京工業大学キャリアアップMOT(CUMOT) サイバーセキュリティ経営戦略コース 講師
2021年　総務省 IPネットワーク設備委員会 事故報告・検証制度等タスクフォース　構成員
2022年　筑波大学大学院 人文社会ビジネス科学学術院 ビジネス科学研究群 非常勤講師
2022年　サイバーセキュリティ協議会 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
2022年　警察庁 サイバー被害の潜在化防止に向けた検討会 委員
2023年　慶應義塾大学大学院政策・メディア研究科 特任准教授
2023年　日本弁護士連合会 弁護士業務における情報セキュリティに関するワーキンググループ 委員
2023年　経済産業省 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 委員

オンライン名刺

「サイバー攻撃被害に係る情報の共有・公表ガイダンス」



- 2022年5月よりサイバーセキュリティ協議会に設置された「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」（事務局：警察庁、総務省、経済産業省、NISC、JPCERT/CC）にて検討を行ったもの
- パブリックコメント実施の後、2023年3月に同ガイダンスを公表



出典：内閣サイバーセキュリティセンター
「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」
https://www.nisc.go.jp/council/cs/kyogikai/guidancekentoukai.html

被害公表後の「オーディエンス」の反応


【独自】三菱電機にサイバー攻撃　防衛などの情報流出か

大手総合電機メーカーの三菱電機が大規模なサイバー攻撃を受け、機密性の高い防衛関連、電力や鉄道といった重要な社会インフラ関連など官民の取引先に関する情報が広く流出した恐れがあることがわかった。本社や主要拠点のパソコンやサーバーが多数の不正なアクセスを受けたことが社内調査で判明した。同社は不正アクセスの手口などから、防衛関連の機密情報を主に狙う中国系のサイバー攻撃集団「Tick（ティック）」が関与した可能性があるとみている。

出典：朝日新聞デジタル
https://www.asahi.com/articles/ASN1M6VDSN1MULFA009.html


日本経済新聞

この記事は会員限定です

富士通の政府クラウドにサイバー攻撃相次ぐ　情報流出も

富士通が政府に提供するクラウドサービスへのサイバー攻撃が相次いでいる。2021年以降、3度にわたって攻撃を受けたが同社はいずれも詳しい原因や影響範囲を公開していない。その間、サイバー犯罪者が集う闇サイトで富士通の顧客や社内のものとされるデータが少なくとも2度暴露されている。

22年12月、富士通はインターネット回線サービス「フェニックス」に不正アクセスがあったと公表した。これまでに京セラ、東京海...

出典：日経電子版
https://www.nikkei.com/article/DGXZQOUC263TJ0W3A320C2000000/

- 2020年1月に報道された三菱電機不正アクセス事案
  - インシデント対応初期の段階で外部と情報共有
  - しばらくの調査期間の後、公表前に報道が先行
    ⇒被害公表や取引先への通知の遅れについて批判的な報道がなされる

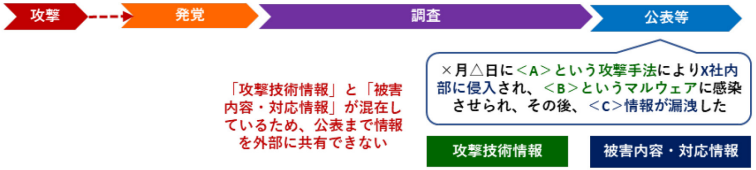
- 運用保守ベンダーが“踏み台”になる事案や脆弱性悪用事案における共有・公表の問題
  - 日立システムズ運用監視サービス事案（2020年）、Filezen事案（内閣府事案）（2021年）、富士通ProjectWeb事案（2021年）、Fjcloud・ニフクラへの不正アクセス事案（2022年）、富士通FENICS不正アクセス事案（2022年）
  - 公表されない情報や対外連携有無に対するメディアからの追及

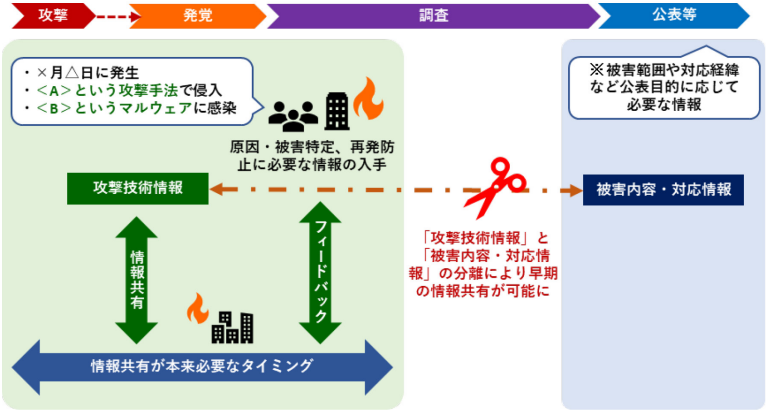
⇒ 前者：「公表前の早い段階で情報共有していたが、その後の公表において評価されない」事案、後者：「発覚後に公表はしていたが、情報共有等の外部連携対応が評価されない」事案

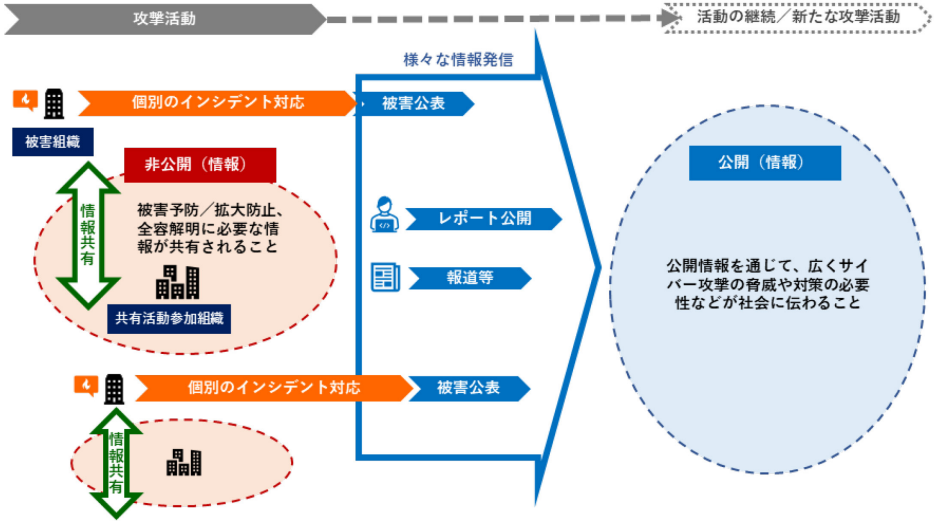
⇒ サイバー攻撃に対する認識が広まったことで、被害組織のインシデント対応の内容やスピード感について、ステークホルダーやメディアからの厳しい評価を受けることに

ガイダンスのコンセプト：「情報共有」と「被害公表」の分離

- タイミングの違い：被害公表時では情報共有として有効なタイミングを失している
- 目的の違い：情報共有の目的と被害公表の目的は違う
- 手段／対象の違い：情報共有→非公表で他の標的／被害組織に対して行う　被害公表→ステークホルダーなど影響を受ける関係者に広く伝える

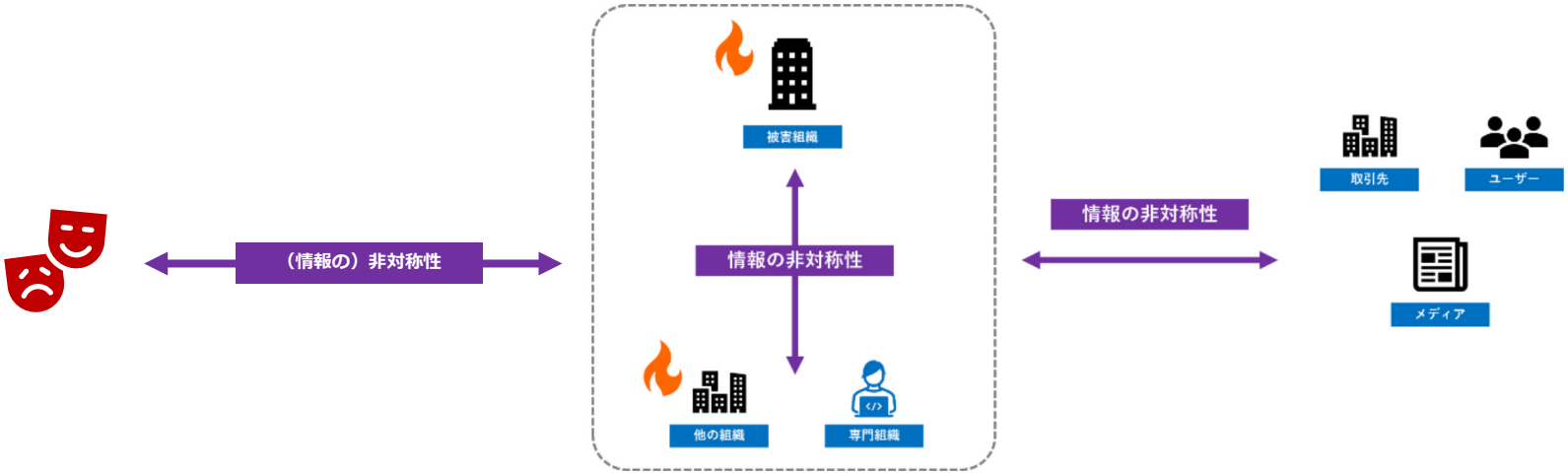




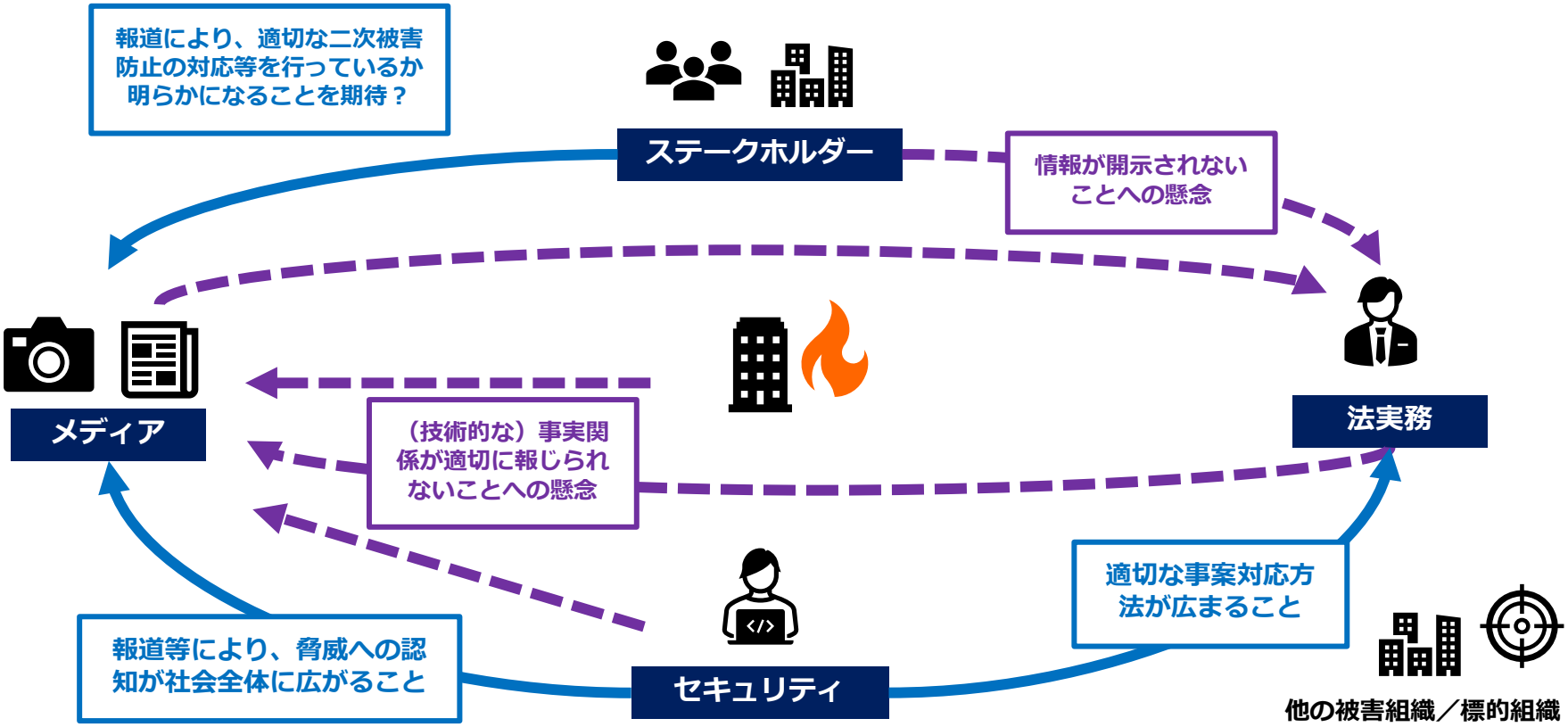


「情報の非対称性」という問題

- サイバー攻撃
  ⇒攻撃者と被害／標的組織との間の「非対称性」
- 情報共有
  ⇒被害組織と他の標的組織、専門組織との間の情報の非対称性を埋める活動
- 被害公表
  ⇒被害組織（＋被害現場に関わる関係者）とステークホルダー等との間の情報の非対称性を埋める活動



それぞれの「ジレンマ」



被害公表の目的

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。

平時・有事における公表・開示（法制度を中心に）

平時	組織のセキュリティ対策やリスク管理体制、ガバナンス等の公表・開示	● **個人情報保護法** 保有個人データの安全管理措置の公表等（問い合わせへの回答でもよい）（2022年4月1日～）
		● **金融商品取引法** ① 有価証券報告書等におけるサステナビリティ情報の開示（2023年3月期～） ※「サステナビリティ情報」には、サイバーセキュリティやデータセキュリティ等が含まれうる ② 内部統制報告制度（J-SOX法）の改訂：サイバーリスクの高まりを踏まえたセキュリティ確保の重要性を記載（2024年4月1日～）
有事	サイバー攻撃を含むインシデントに関する公表・開示	● **個人情報保護法** 公表自体は「望ましい措置」だが、本人通知義務の履行が困難な場合の代替措置として公表が必要となる場合がある（2022年4月1日～）
		● **有価証券上場規程** 上場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の適時開示 参考：財政に著しい影響：臨時報告書（金融商品取引法） ※サイバーインシデントが特出しされているわけではない

米国証券取引委員会：セキュリティ関連の開示ルール

■ 米国証券取引委員会（SEC）による開示ルールの採択

SECは、2023年7月26日付で、上場登録会社に対し、主に以下の2つを義務付ける規則を採択

（1）サイバーセキュリティ体制に関する定期開示（年次）

- ✓ サイバーセキュリティに関するリスク管理、戦略、ガバナンスの開示

（2）重大なサイバーセキュリティインシデントの臨時開示

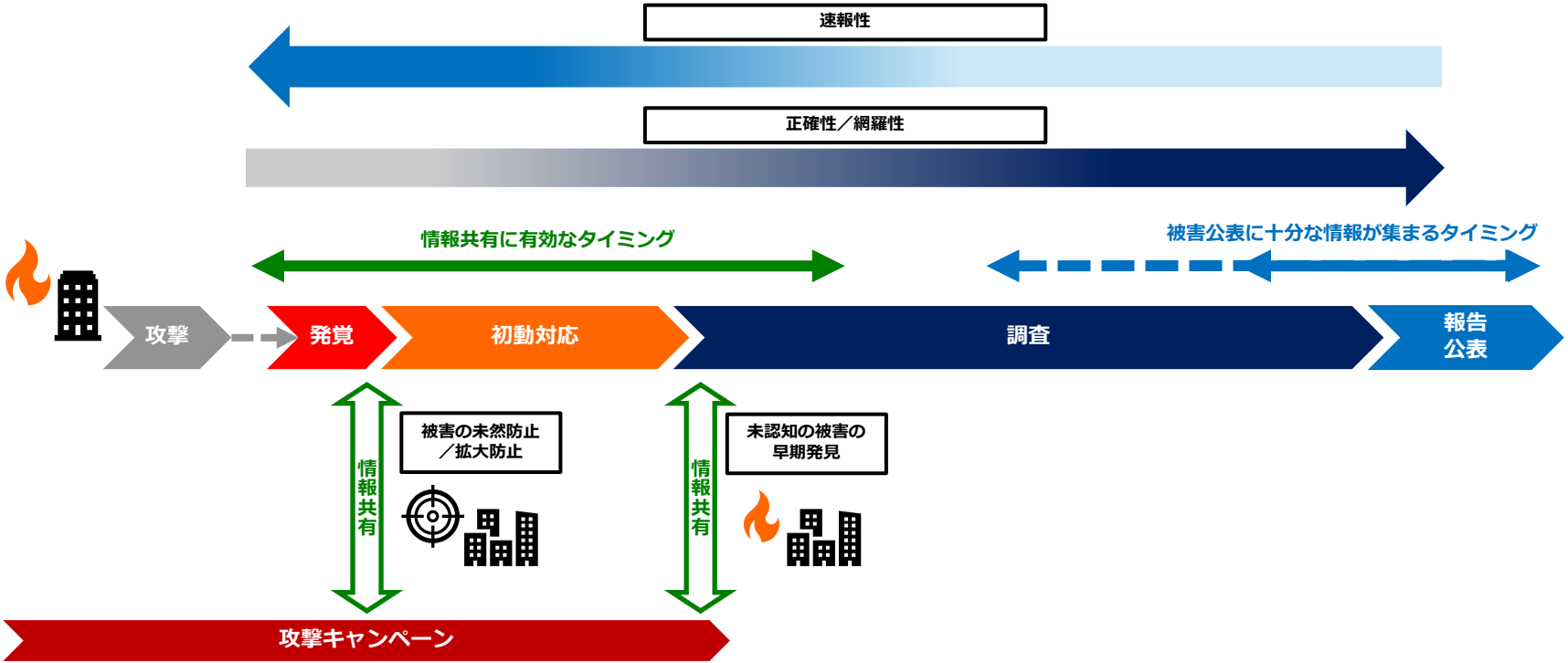
- ✓ サイバーセキュリティインシデントが重大であると**判断してから４営業日以内**に提出
- ✓ インシデント発見から不当な遅延なく重大性を判断

■ 制度の観点からの日本への影響

日本においても同種の制度導入に向けての議論の可能性

情報の速報性／正確性から見た情報共有と被害公表

- 情報共有：多少不正確／網羅性がなくても早期に共有しなければ共有効果は得られない
- 被害公表：（速報的なものを除き）ある程度情報が明らかにならなければ目的（説明責任など）を達成できない



ガイダンスにおける「原因情報」の取り扱いの解説①

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。

ガイダンスにおける「原因情報」の取り扱いの解説②

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。

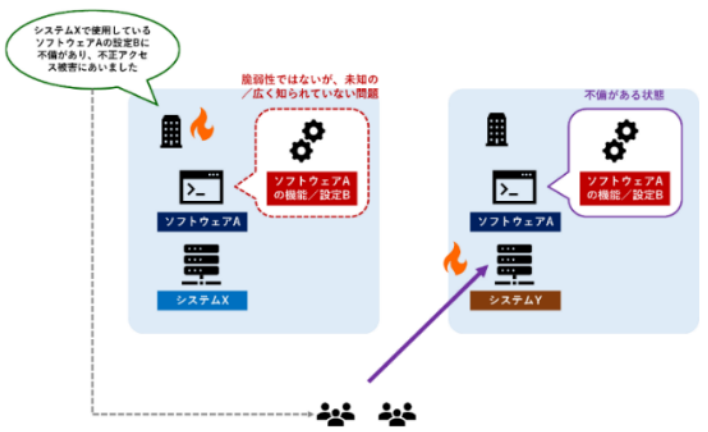


図 63

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。

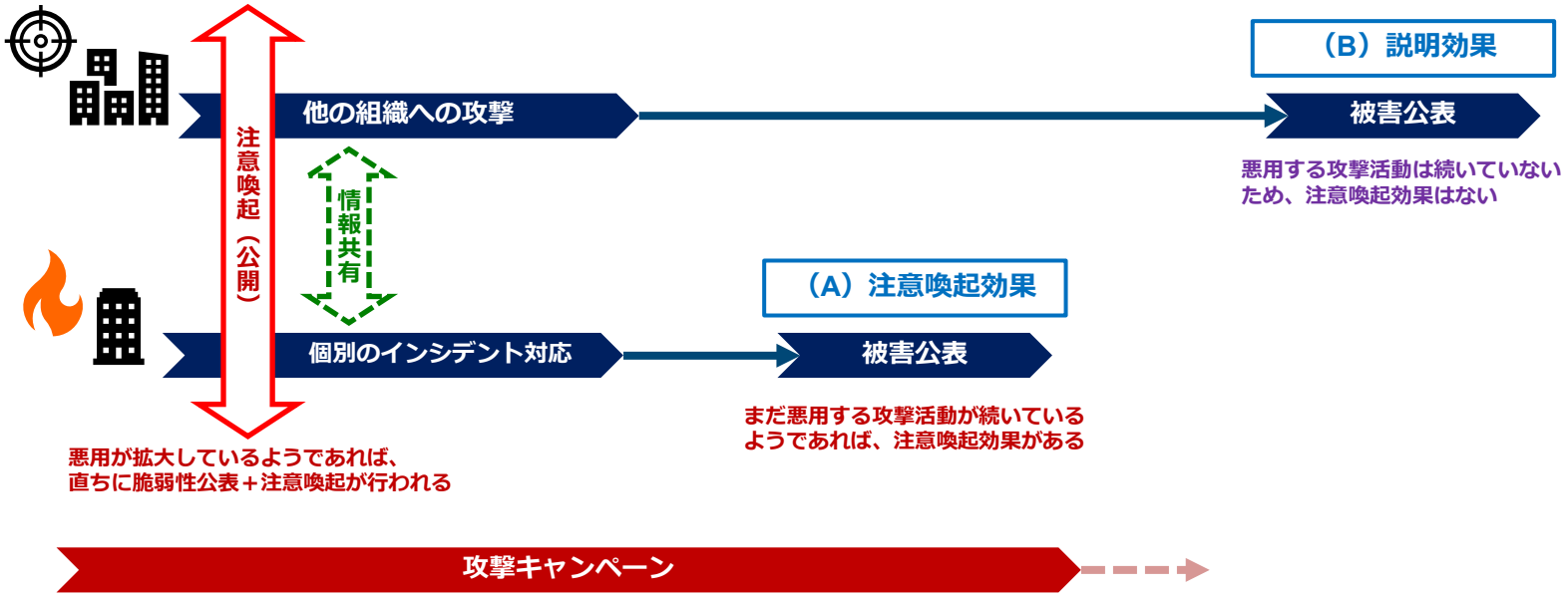
一方で、フィッシングサイトやマルウェアサイトではない偽サイト、「多くのユーザーがアクセスすること自体を不法行為の目的」としているような偽サイトの場

被害公表時になぜ「原因」を説明するのか

■ 被害公表時に「原因」を示す目的

A：他の利用組織など広く社会全体に注意喚起効果を持つ

B：侵害原因を可能な範囲で示すことで自組織の運用・管理上の問題だったのかゼロデイ攻撃など事前の予防が困難なものだったのか示す



「特定の製品／サービスが悪用された」という情報

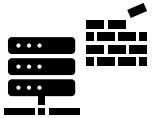
- 同じ情報であっても、「その情報をどう扱いたいか」という点においてそれぞれ利害の異なるプレーヤーが複雑に関係する状態にある ⇒ 情報を扱うにあたって利害の衝突が発生してしまう

消極的な背景／動機を持つ

メーカー

Sier／運用保守ベンダー

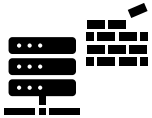
原因：製品／サービス
⇒自組織の“責任”を
増やす情報



積極的な背景／動機を持つ

被害組織

原因：製品／サービス
⇒自組織の“責任”を
減らす情報



積極的な背景／動機を持つ

他のユーザー

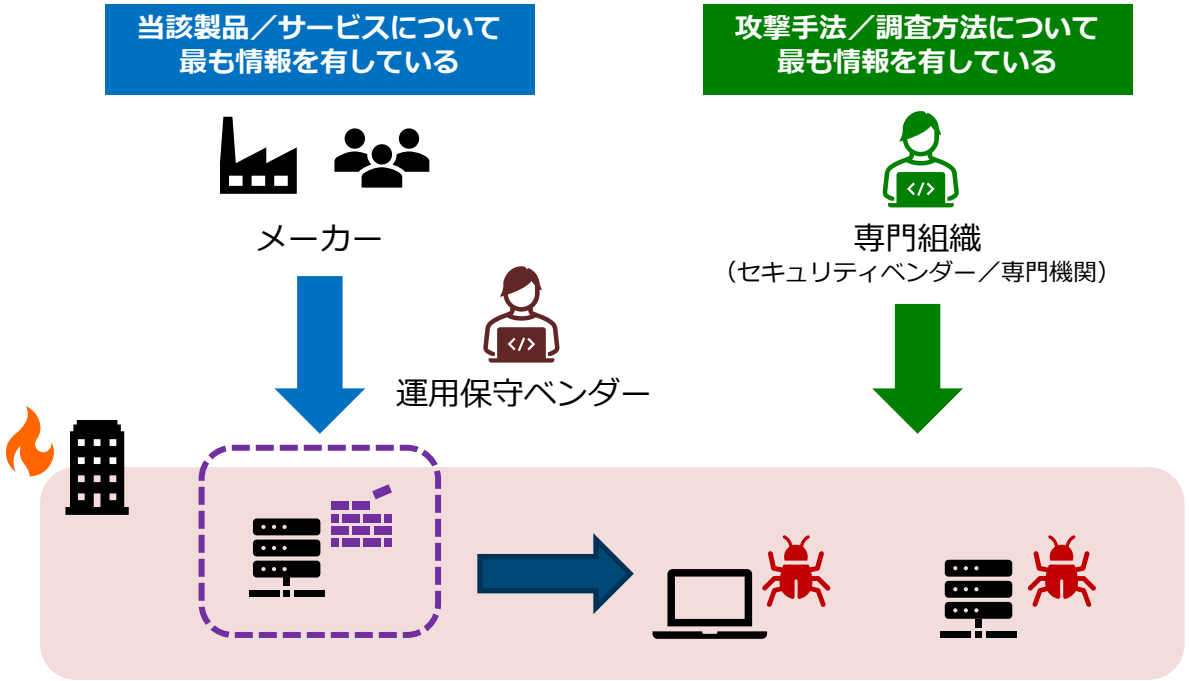
専門組織

メディア

顧客、取引先

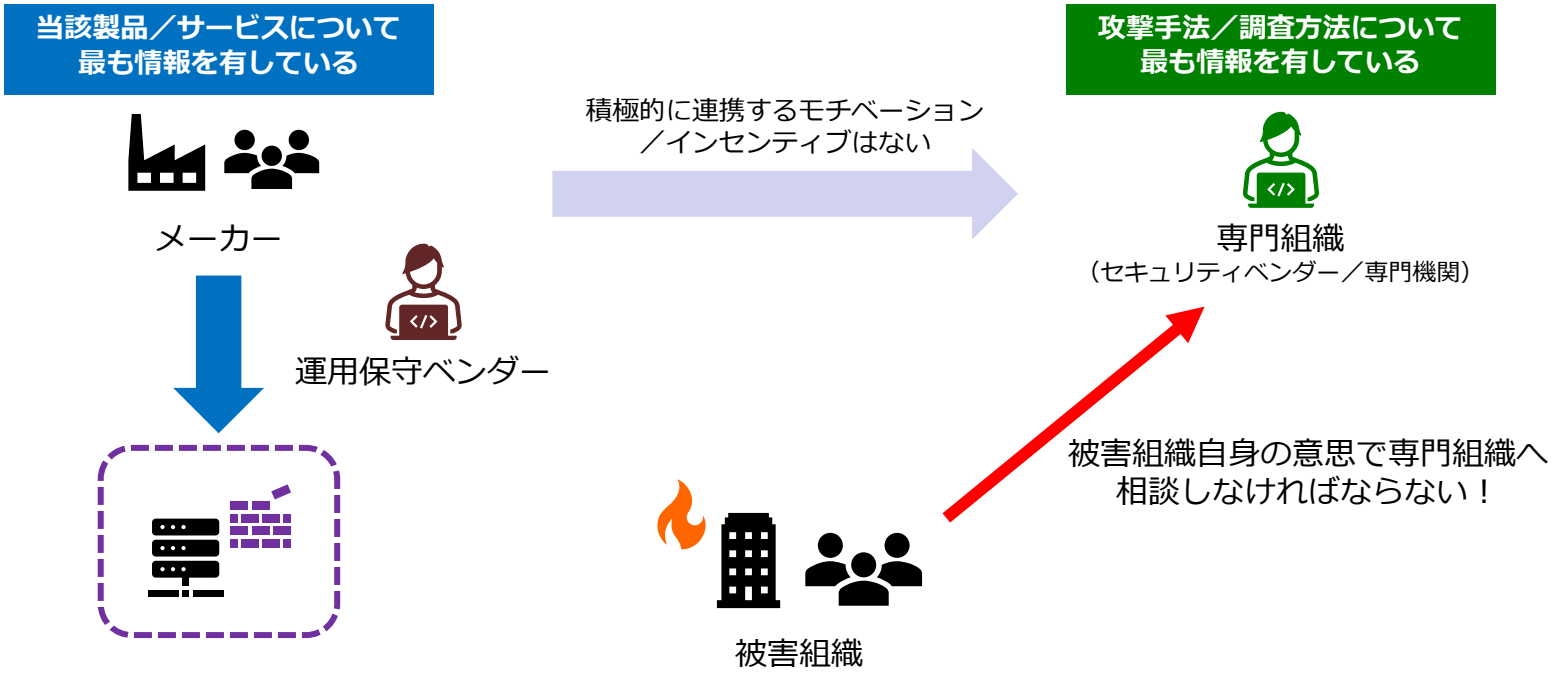
なぜメーカーからの情報だけでは不十分か

- 脆弱性の悪用事案が発生している場合、「脆弱性情報」を伝えるだけでは足りない
- 当該脆弱性悪用はあくまでInitinal Accessでしかないため、その後のラテラルムーブメントの調査をどうフォローできるかが重要



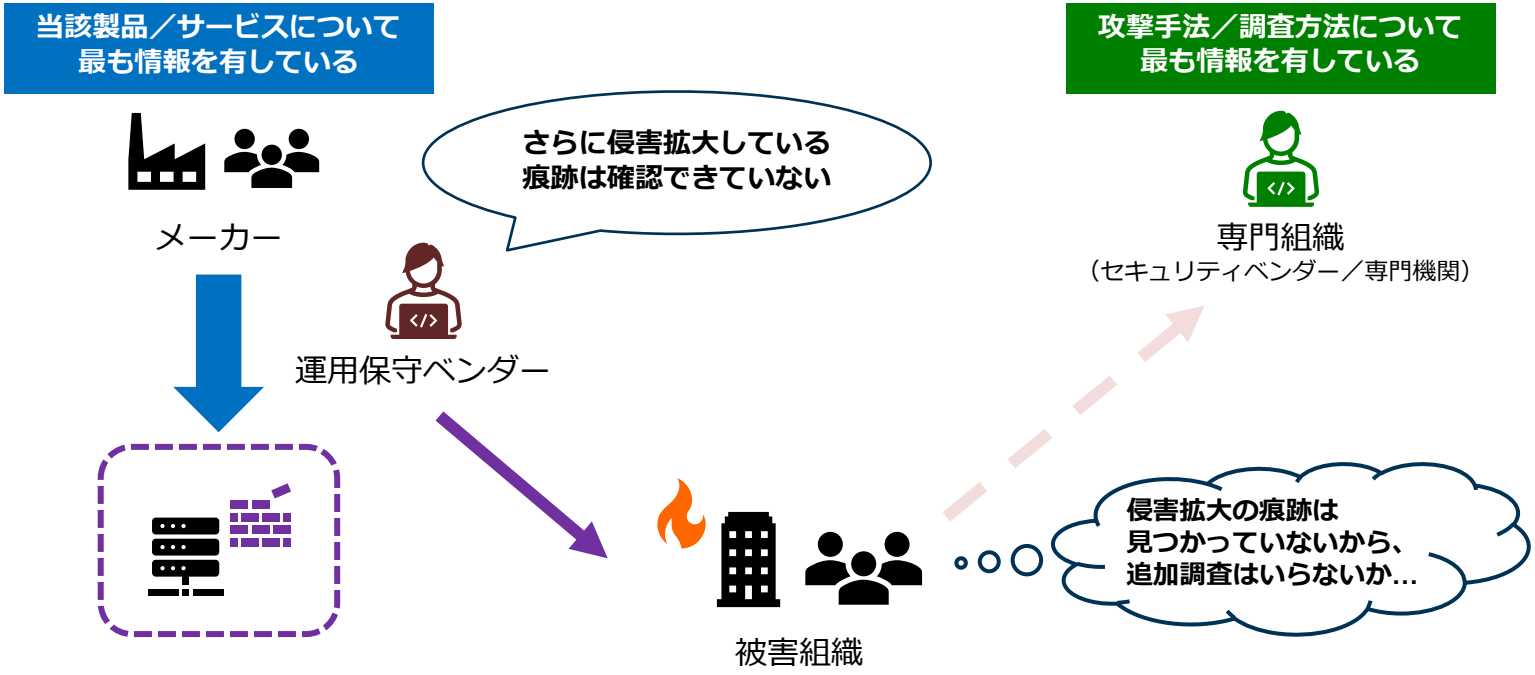
インシデント対応をどこまでフォローできるのか

- 専門組織への相談を積極的に推奨されるケースは少ない
- 基本的に被害組織自ら判断しないといけない



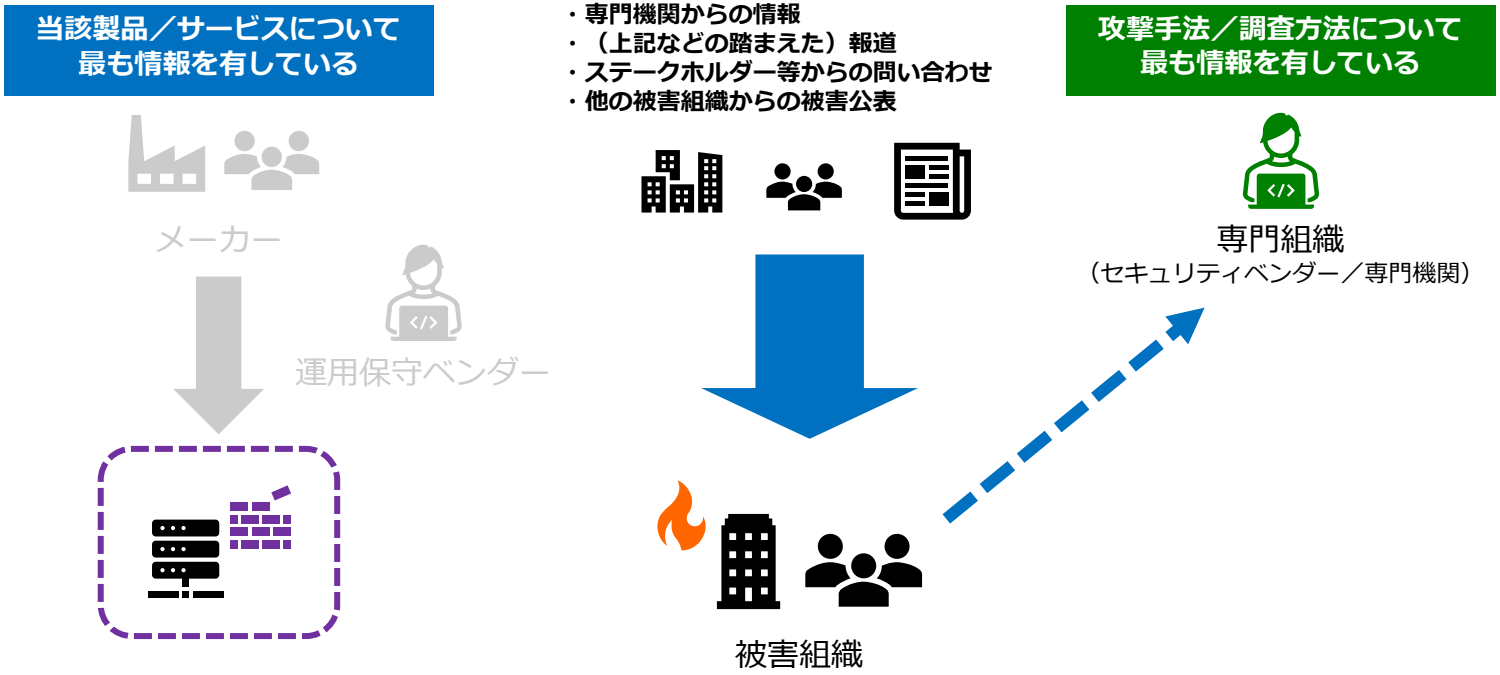
インシデント対応をどこまでフォローできるのか

- 運用保守ベンダーとして”守備範囲”外の調査まで積極的にユーザーを説得しづらい
- メーカー、運用保守ベンダー、被害組織それぞれ、積極的な侵害有無調査を行うインセンティブ／モチベーションを有しにくい



インシデント対応をどこまでフォローできるのか

- 「外からの情報」によって、被害組織が対応の温度感を認識・判断できる場合がある
- 他方で外部が”無風“であれば、対応の温度感を認識することができなくなる



ガイダンスが目指すもの：「情報の非対称性」をいかに埋めていくか

- 攻撃被害拡大を防げないのも、被害組織に（見当違いの）厳しい評価がなされてしまうのも、すべて「情報の非対称性」が存在するから（情報共有の問題だけ解消すればいいわけではない）
- いかにそれぞれのプレイヤーが必要とする／伝えるべき情報が効率的に伝えられるかが重要
- ガイダンスなどに基づいて「ルール」「規範」が広がることで、情報の非対称性が解消していけば、**お互いに無駄な衝突や機会損失をしない関係性**になれる

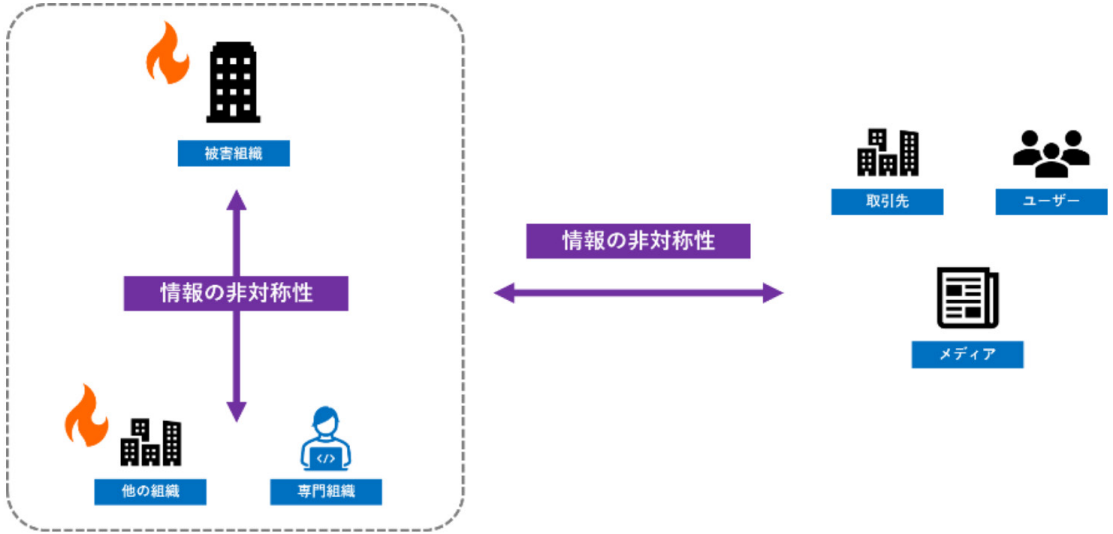


図 9

以下、参考資料（適宜投影）

初期侵害経路となる脆弱性公表／注意喚起の増加

2019年
・Pulse Connect Secure（CVE-2019-11510）
・Fortigate（CVE-2018-13379）

2020年
・Citrix（CVE-2019-19781）
・BIG-IP（CVE-2020-5902）
・Trend Micro製品の複数の脆弱性

2021年
・Filezen（CVE-2021-20655）
・SonicWall（CVE-2021-20016）
・Proxyshell（Exchange Serverの複数の脆弱性）
・Trend Micro 製品の脆弱性（CVE-2020-24557等）
・Pulse Connect Secure（CVE-2021-22893）
（・Confluence脆弱性（CVE-2021-26084））
（・ManageEngine ADSelfService Plusの脆弱性（CVE-2021-40539））
（・Vmware Horizon Log4j脆弱性）

2022年
・Sonicwall SMA100シリーズの複数の脆弱性
・BIG-IP（CVE-2022-1388）
・Trend Micro Apex Central製品の脆弱性（CVE-2022-26871）
・FortiOS等の脆弱性（CVE-2022-40684）
・FortiOS（CVE-2022-42475）

2023年
（・MOVEit File Transferの複数の脆弱性）
・Citrix ADCおよびCitrix Gatewayの脆弱性（CVE-2023-3519）
・Proself の複数の脆弱性（CVE-2023-39415等）
・FortiOS等の脆弱性（CVE-2023-27997）
（・Ivanti Endpoint Manager Mobileの複数の脆弱性）
・BarracudaESG（CVE-2023-2868）
・Citrix ADCおよびCitrix Gatewayの脆弱性（CVE-2023-3519）
・Array Networks Array AGシリーズの脆弱性
・ProselfのXML外部実体参照（XXE）に関する脆弱性
・Cisco IOS XEのWeb UIにおける権限昇格の脆弱性（CVE-2023-20198）

括弧付は国内で注意喚起が発行されなかったもの

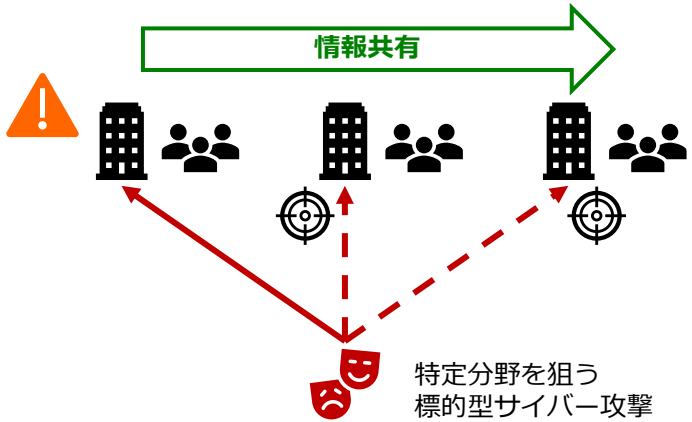
- 標的型サイバー攻撃や侵入型ランサムウェア攻撃の初期侵入経路（Attack Vector／Initial access）として悪用される脆弱性が多く見つかった3年間
- 引き続きメール経由で侵入を試みる標的型サイバー攻撃も存在するところ、特に侵入型ランサムウェア攻撃を中心に、インターネットに面したソフトウェア製品の脆弱性を突く攻撃が相次ぐ
- 他方で、Emotetのテイクダウン（※その後断続的に活動再開）、Trickbotの活動停止など、マルウェアディストリビューターが拡散させるマルウェア経由での侵害事案は想定的に減ったのではないかと推測

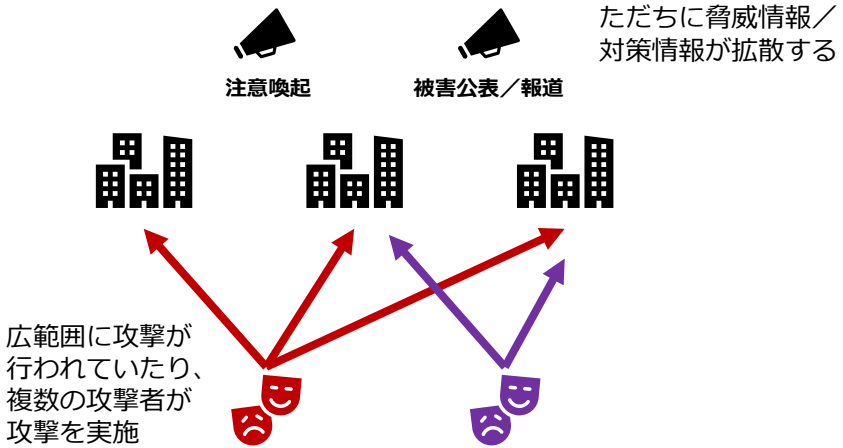
＜傾向＞

- ランサムアクターによるゼロデイ攻撃での悪用
- 特定製品分野でクリティカルな脆弱性が度々見つかる＆悪用される
（例：SSL-VPN製品、オンラインストレージ）
- 特定製品で度々クリティカルな脆弱性が見つかる＆悪用される（例：Fortigate、Sonicwall、Proself）

どう対策していけばいいか

- ゼロデイ攻撃はユーザー側で気付きようがない
- ゼロデイ攻撃であろうが、既知の脆弱性を悪用する攻撃であろうが、限定的な範囲を狙う攻撃キャンペーンは発覚しにくい
- どこからいつ来るかわからない攻撃に対して、あらゆるアプライアンス等に対策リソースを大量に張り付けることも現実的ではない
- 「脅威ベースアプローチで対処！」と言っても、”脅威情報“が巷にあふれている。。。
  ⇒適切な脅威情報を入手して、「正しく怖がる／備える」
- 例：特定の業界（の情報）／業界固有のシステムを狙う限定的な攻撃に関する情報を情報共有活動を通じて入手する／専門組織から得る





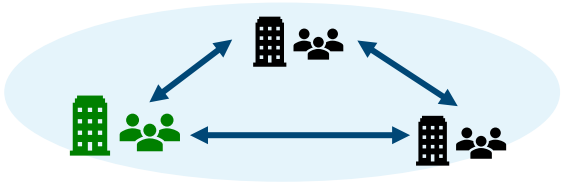
公開情報以外の脅威情報の入手方法／情報共有方法

「脅威インテリジェンスサービス」等の購入

例：
・脅威情報収集・提供サービス
・ASM関連の各種サービス

情報共有：n対n方式

例：
・業界単位でのISAC活動
・業界横断的な連携活動（例：日本シーサート協議会（NCA））

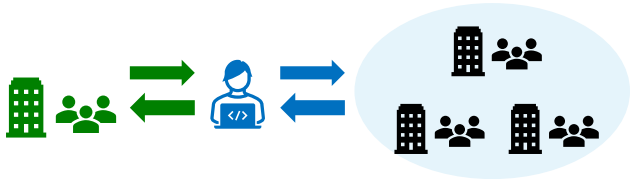


専門機関からの情報

例：
・JPCERT/CC、IPAからの注意喚起、メールニュース
・JPCERT/CCからの個別通知

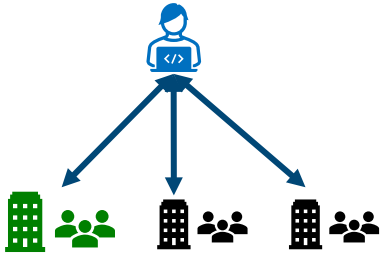
情報共有：間接／代理型

例：
・サイバーセキュリティ協議会
（の一般相談窓口：JPCERT/CC）
・その他、情報共有活動に参加している各専門組織

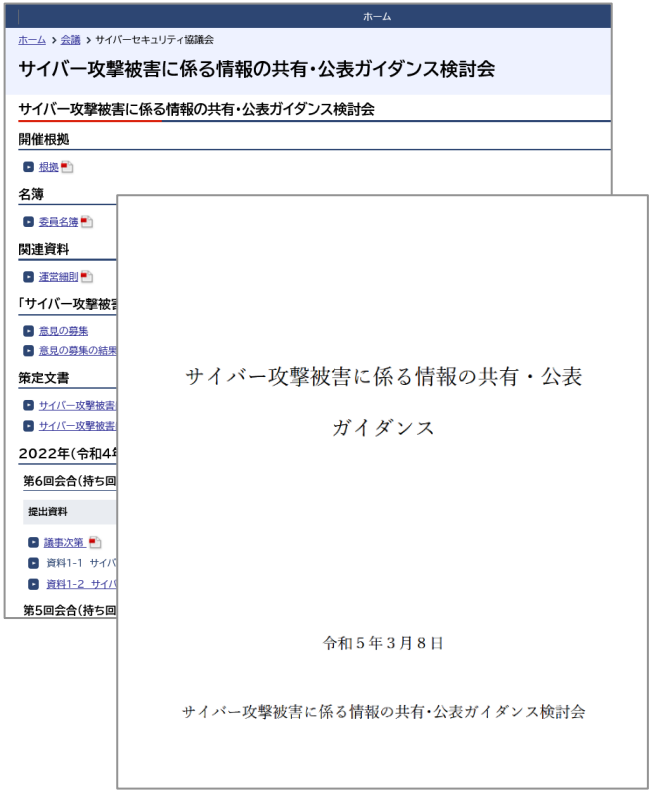


情報共有：ハブ・スポーク型

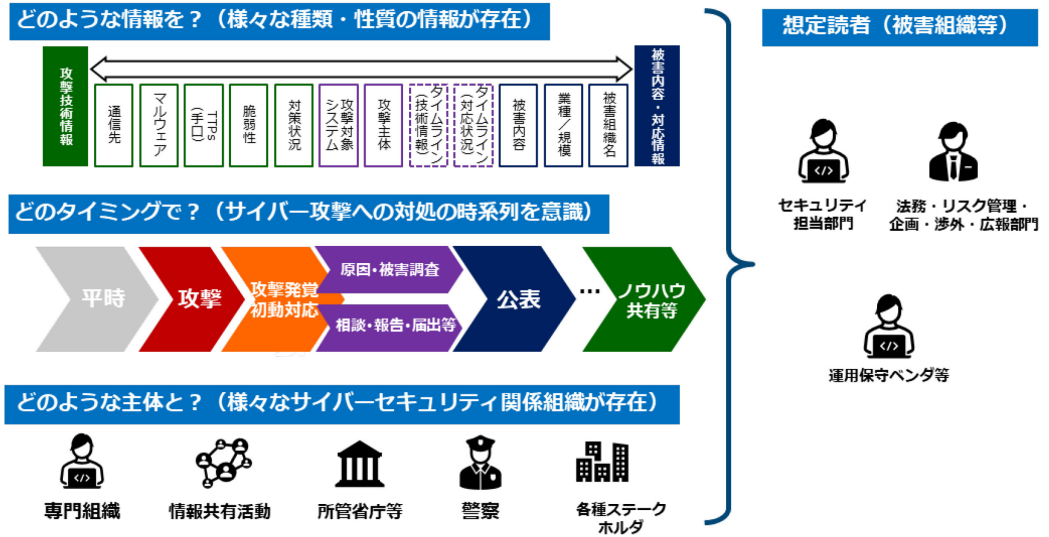
例：
・JPCERT/CC　CISTA
・IPA　J-CSIP
・サイバーセキュリティ協議会
（の一般構成員）



「サイバー攻撃被害に係る情報の共有・公表ガイダンス」



- 2022年5月よりサイバーセキュリティ協議会に設置された「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」（事務局：警察庁、総務省、経済産業省、NISC、JPCERT/CC）にて検討を行ったもの
- パブリックコメント実施の後、2023年3月に同ガイダンスを公表



出典：内閣サイバーセキュリティセンター
「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」
https://www.nisc.go.jp/council/cs/kyogikai/guidancekentoukai.html

本ガイダンスの目次

サイバー攻撃被害に係る情報の共有・公表ガイダンスの構成

- FAQ形式で構成されており、各問と回答が1ページにまとめられています
  その他補足説明等の解説が次の1ページに載っています
- FAQのほか、3事例のケーススタディや判断フローチャート、チェックリストがあります

目次構成

目次

FAQパート

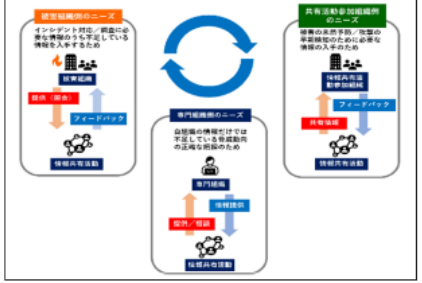
＜情報共有の方法等について＞

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。



各FAQの解説等

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、対応が網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。下記図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。

被害公表をめぐってよくある議論

■ 本当にそうなのか？

・情報共有のために被害公表すべき

・原因／手口についても公表することで注意喚起効果がある

・情報共有のために攻撃手口についても公表します

・他の組織の被害予防に役立てば幸いです

被害公表

被害公表後の「オーディエンス」の反応


【独自】三菱電機にサイバー攻撃　防衛などの情報流出か

大手総合電機メーカーの三菱電機が大規模なサイバー攻撃を受け、機密性の高い防衛関連、電力や鉄道といった重要な社会インフラ関連など官民の取引先に関する情報が広く流出した恐れがあることがわかった。本社や主要拠点のパソコンやサーバーが多数の不正なアクセスを受けたことが社内調査で判明した。同社は不正アクセスの手口などから、防衛関連の機密情報を主に狙う中国系のサイバー攻撃集団「Tick（ティック）」が関与した可能性があるとみている。

出典：朝日新聞デジタル
https://www.asahi.com/articles/ASN1M6VDSN1MULFA009.html


日本経済新聞

この記事は会員限定です

富士通の政府クラウドにサイバー攻撃相次ぐ　情報流出も

富士通が政府に提供するクラウドサービスへのサイバー攻撃が相次いでいる。2021年以降、3度にわたって攻撃を受けたが同社はいずれも詳しい原因や影響範囲を公開していない。その間、サイバー犯罪者が集う闇サイトで富士通の顧客や社内のものとされるデータが少なくとも2度暴露されている。

22年12月、富士通はインターネット回線サービス「フェニックス」に不正アクセスがあったと公表した。これまでに京セラ、東京海...

出典：日経電子版
https://www.nikkei.com/article/DGXZQOUC263TJ0W3A320C2000000/

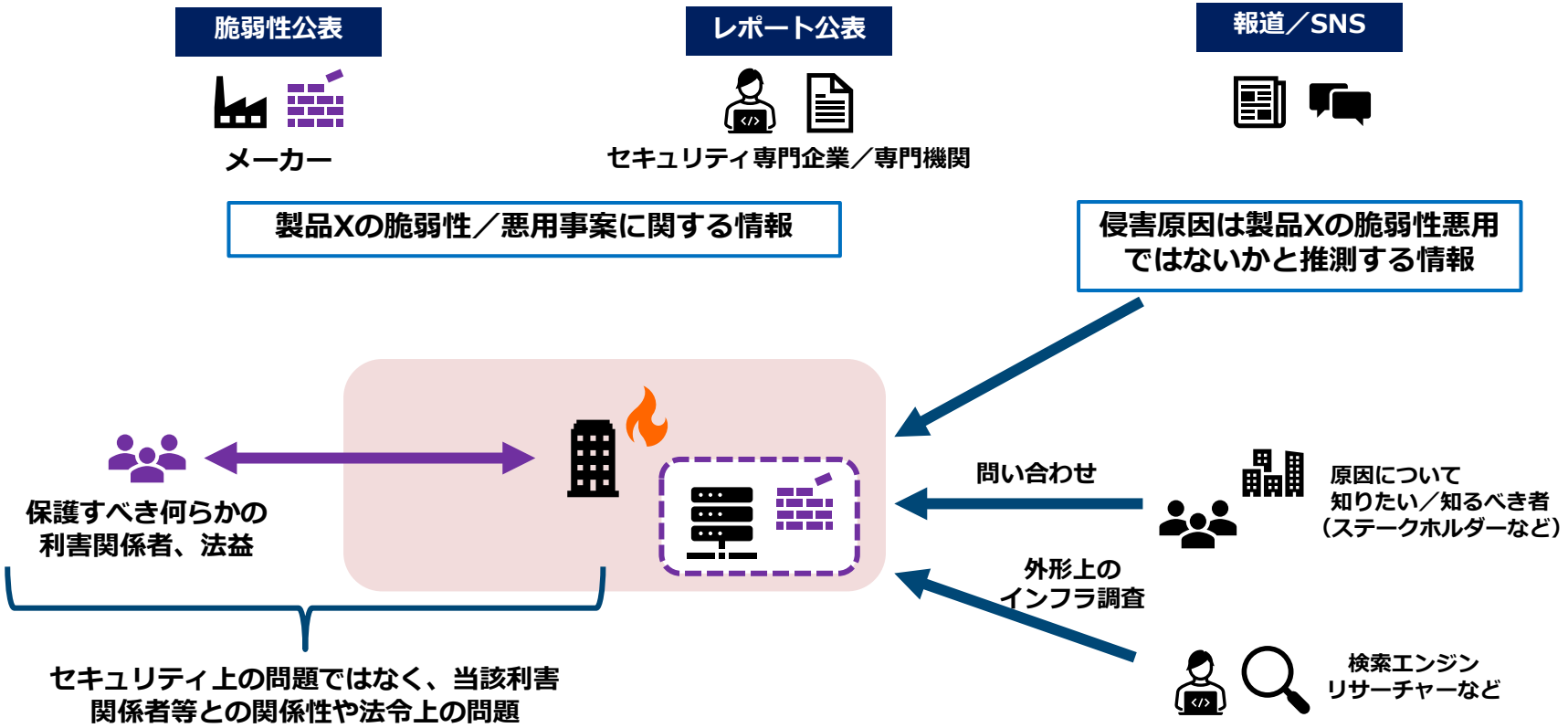
- 2020年1月に報道された三菱電機不正アクセス事案
  - インシデント対応初期の段階で外部と情報共有
  - しばらくの調査期間の後、公表前に報道が先行
    ⇒被害公表や取引先への通知の遅れについて批判的な報道がなされる

- 運用保守ベンダーが“踏み台”になる事案や脆弱性悪用事案における共有・公表の問題
  - 日立システムズ運用監視サービス事案（2020年）、Filezen事案（内閣府事案）（2021年）、富士通ProjectWeb事案（2021年）、Fjcloud・ニフクラへの不正アクセス事案（2022年）、富士通FENICS不正アクセス事案（2022年）
  - 公表されない情報や対外連携有無に対するメディアからの追及

⇒ 前者：「公表前の早い段階で情報共有していたが、その後の公表において評価されない」事案、後者：「発覚後に公表はしていたが、情報共有等の外部連携対応が評価されない」事案

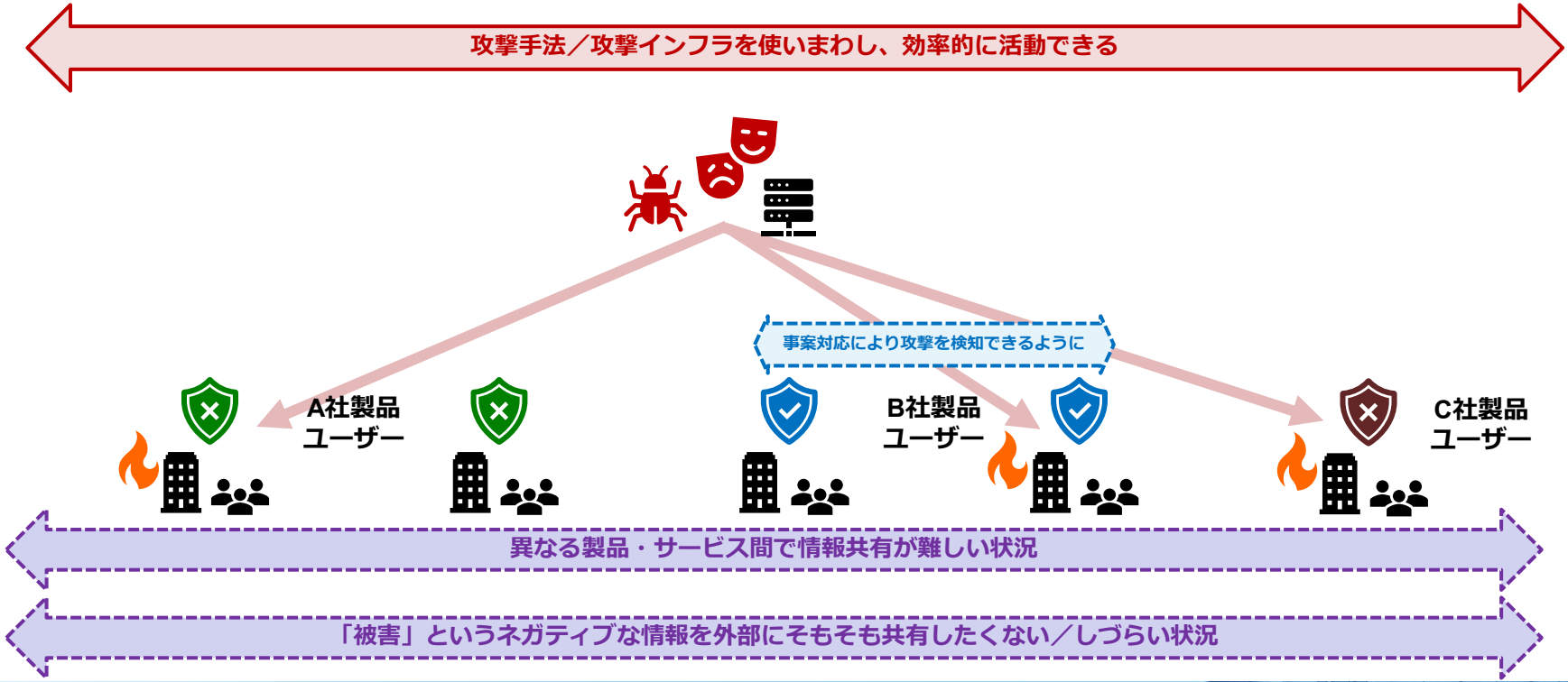
⇒ サイバー攻撃に対する認識が広まったことで、被害組織のインシデント対応の内容やスピード感について、ステークホルダーやメディアからの厳しい評価を受けることに

「セキュリティ上の理由で答えられない」という回答で耐えられるのか・・・



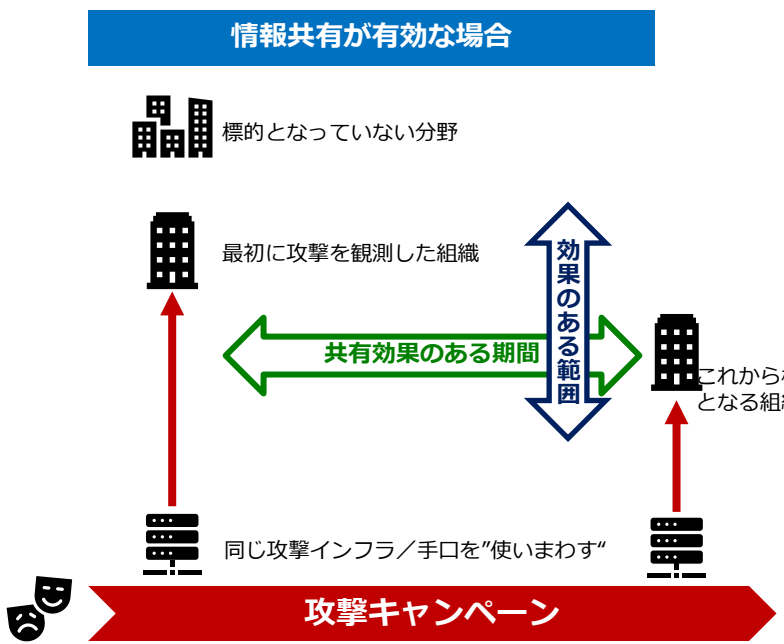
議論の前提：なぜ「共有」しなければならないのか

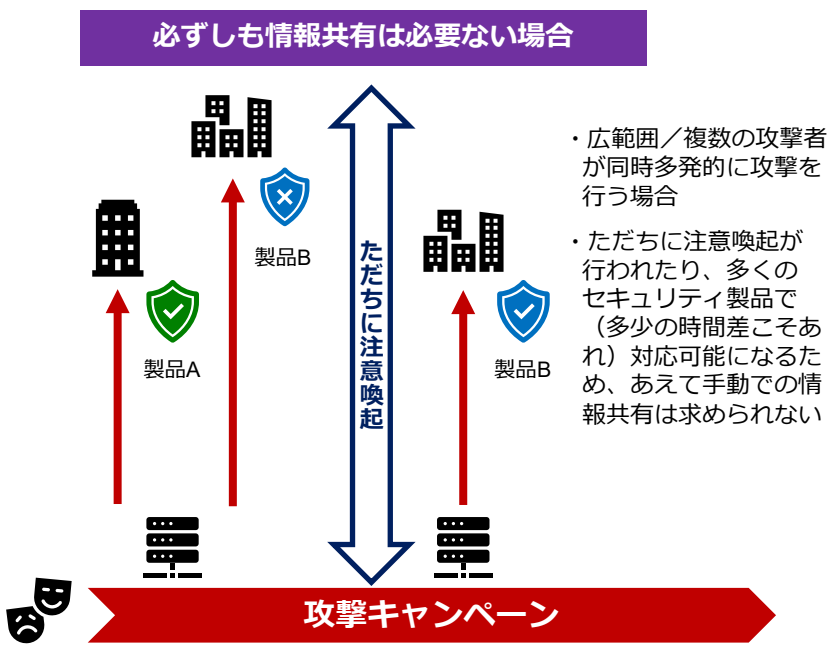
- 多くの攻撃では、攻撃側と防御側にある非対称性を利用して、攻撃者優位に立っている



なぜ「共有」が有効なのか

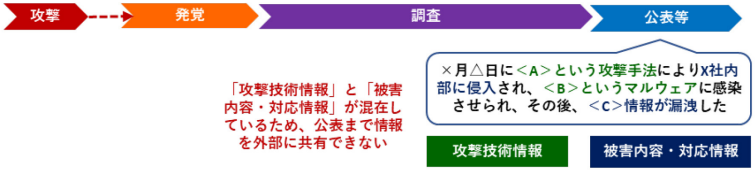
- 基本的に「攻撃者が攻撃インフラや攻撃手口を使いまわす」場合、情報共有が有効である
- 攻撃インフラを標的ごとに使い捨てる場合や、ごく限定的な範囲しか狙わない攻撃、逆に広範囲を狙う攻撃に対しては情報共有は効果がない（あるいは対応コストの方が高くついてしまう）
- ※もちろん、こうした話もガイダンスで解説しています

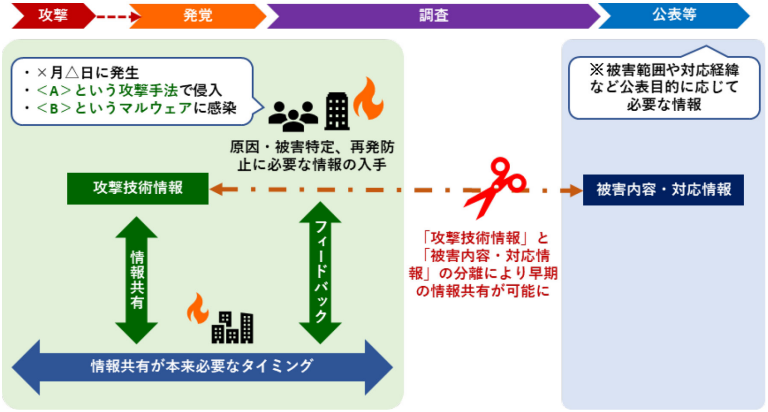


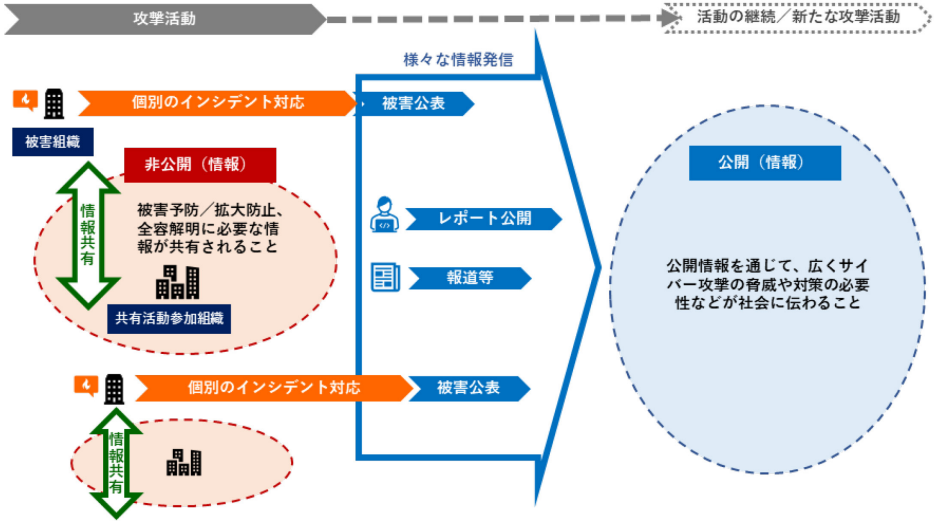


ガイダンスのコンセプト：「情報共有」と「被害公表」の分離

- タイミングの違い：被害公表時では情報共有として有効なタイミングを失している
- 目的の違い：情報共有の目的と被害公表の目的は違う
- 手段／対象の違い：情報共有→非公表で他の標的／被害組織に対して行う　被害公表→ステークホルダーなど影響を受ける関係者に広く伝える

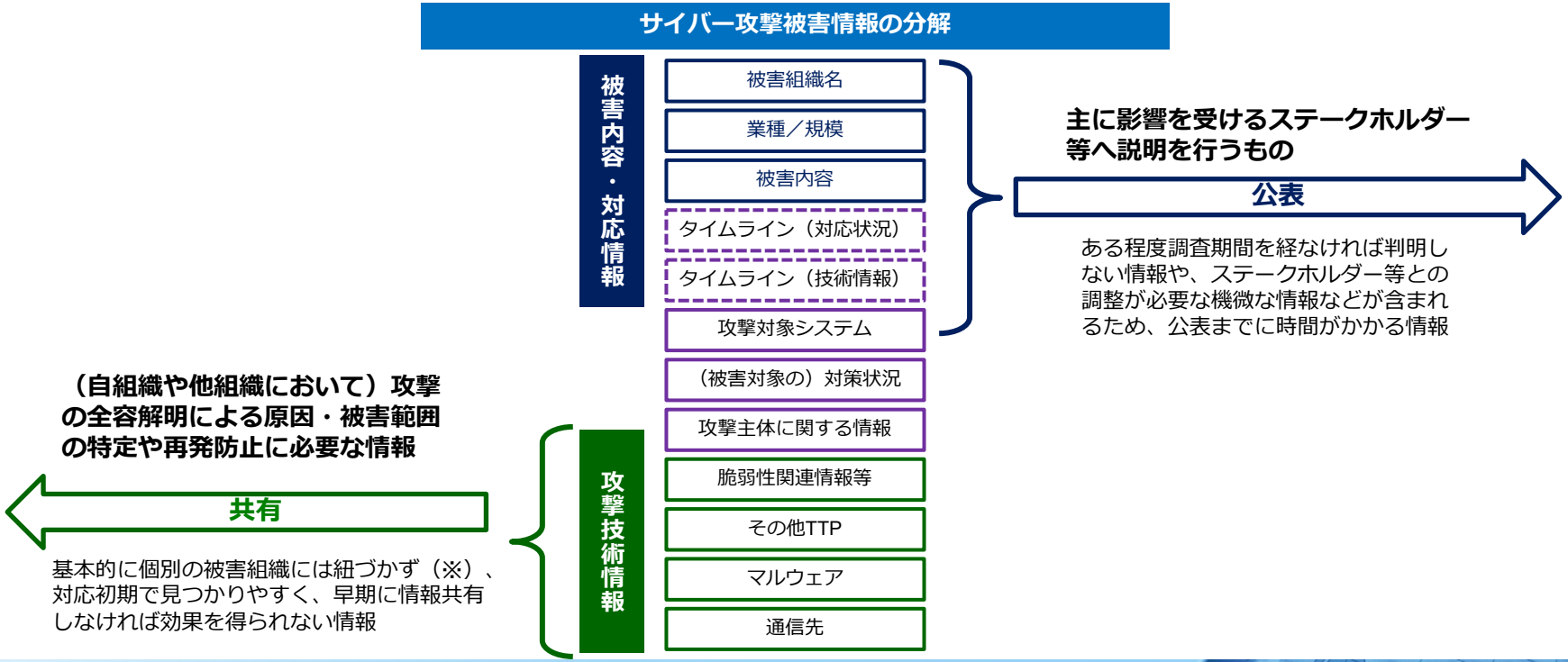




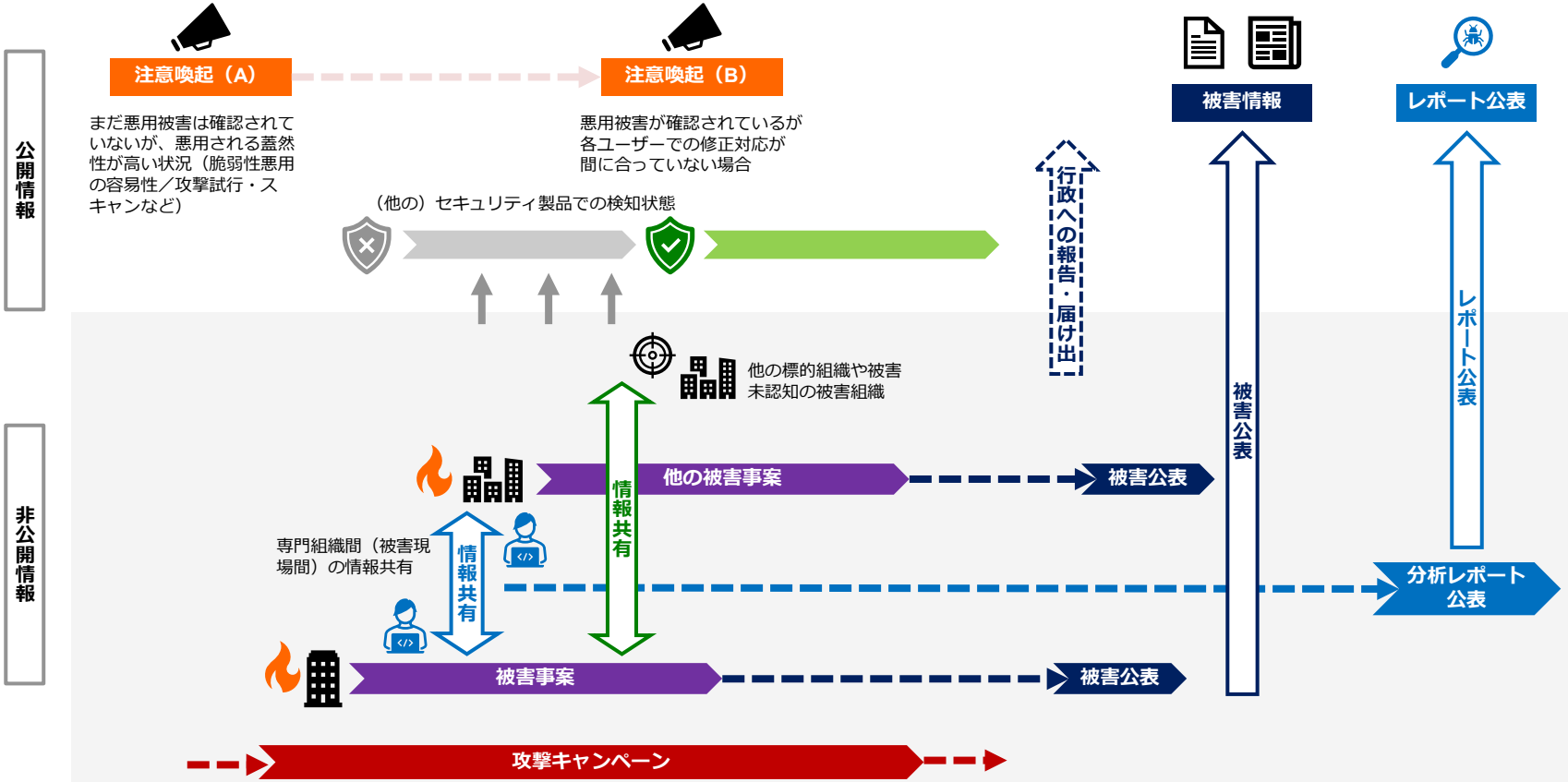


ガイダンスのコンセプト：攻撃技術情報と被害内容・対応情報の分離

- 情報を整理し切り分けることで、被害組織の匿名化や速やかな情報共有を行うことができる
- ただ、厳密な切り分けが難しい情報／ケースもある（特定製品の脆弱性や特定サービスが“踏み台”となった事案など）
- 攻撃技術情報であっても、被害組織が推測し得る情報もあるため注意が必要（※ガイダンスで解説）

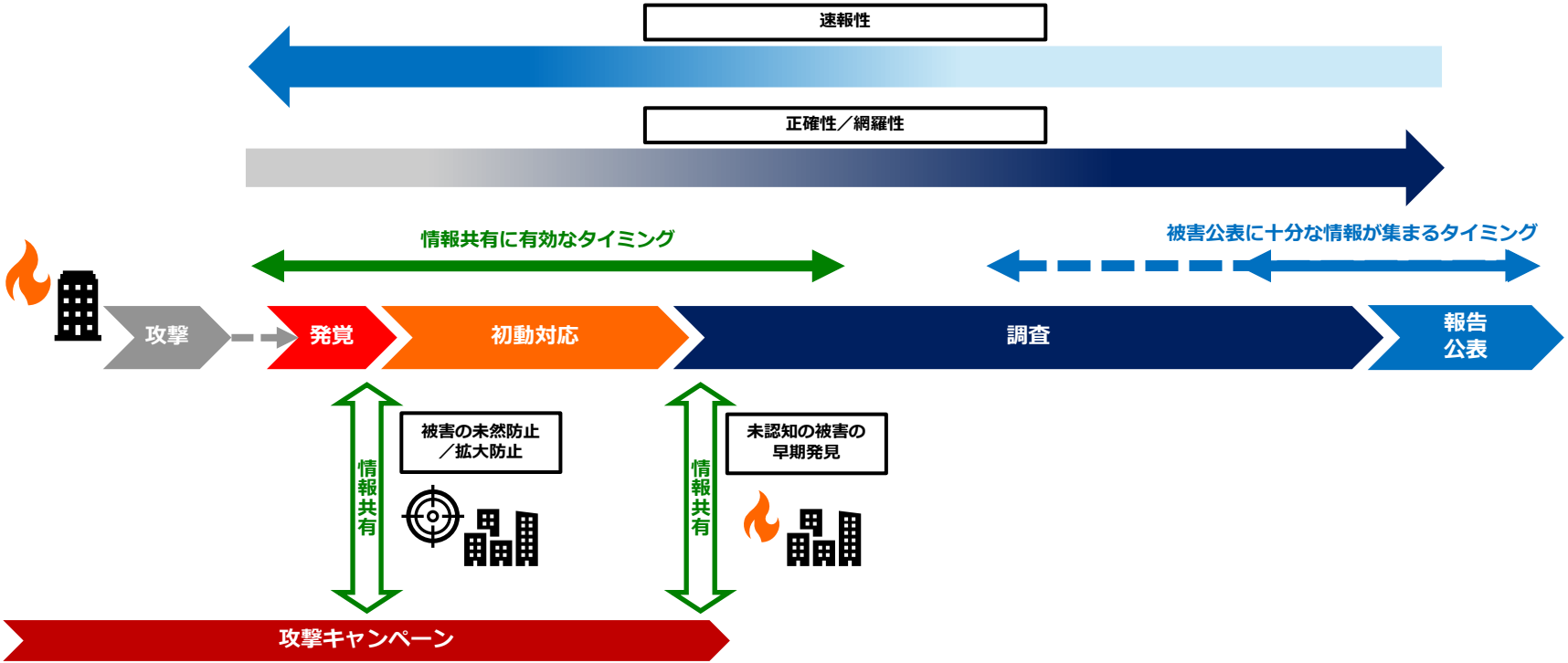


脅威情報の流通



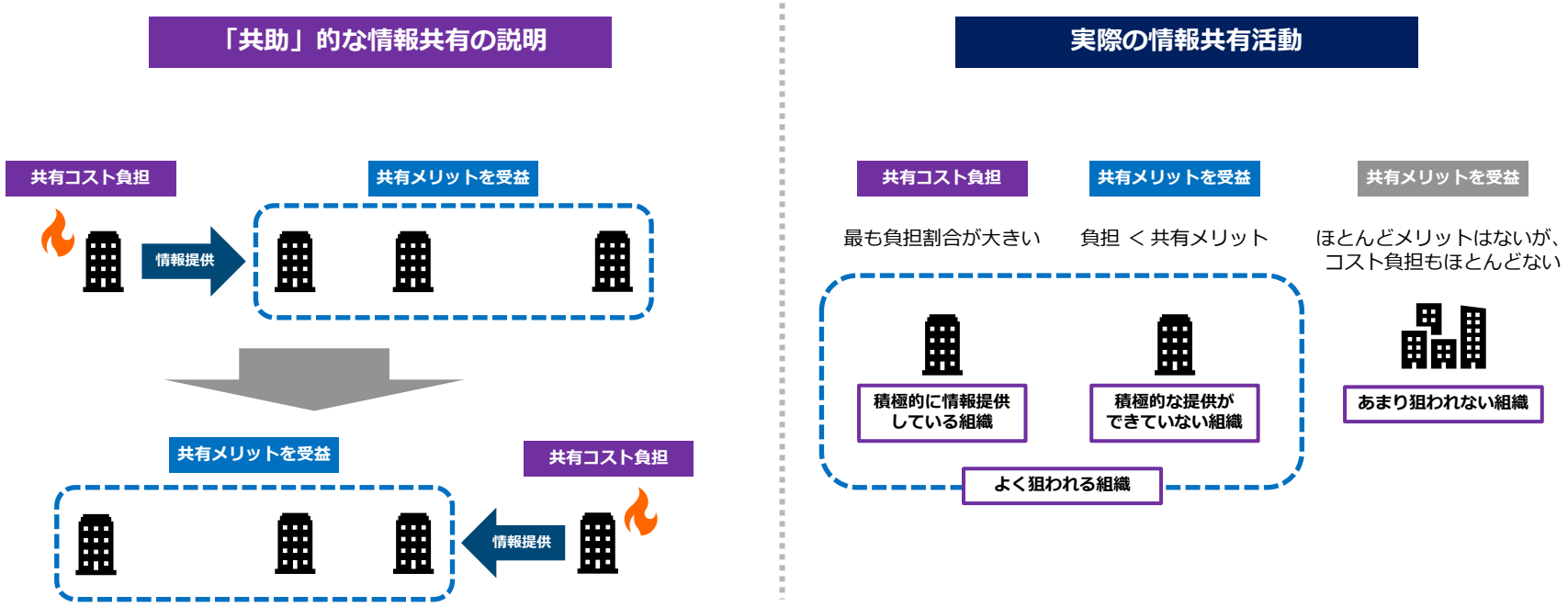
情報の速報性／正確性から見た情報共有と被害公表

- 情報共有：多少不正確／網羅性がなくても早期に共有しなければ共有効果は得られない
- 被害公表：（速報的なものを除き）ある程度情報が明らかにならなければ目的（説明責任など）を達成できない

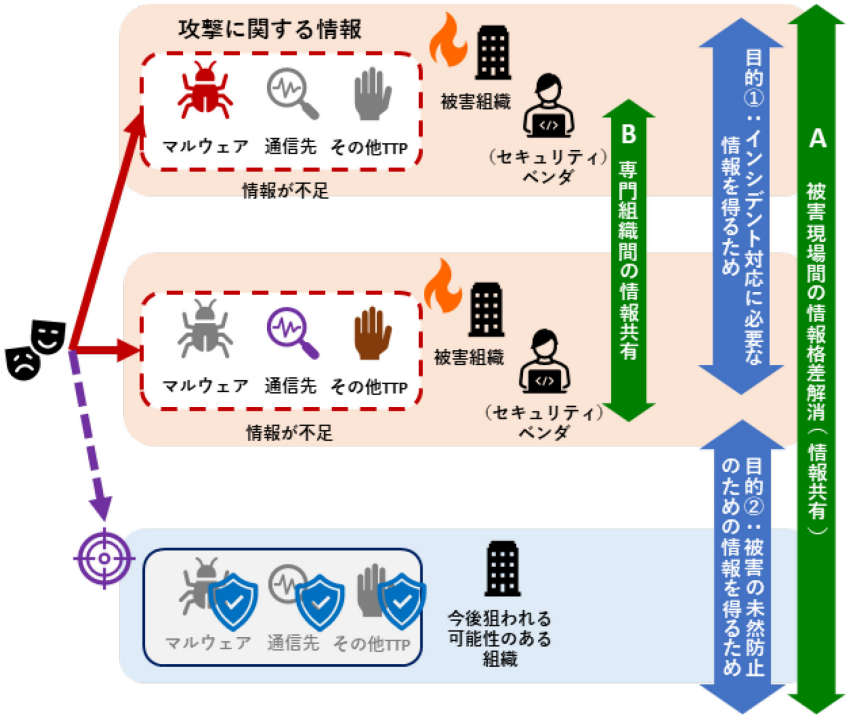


情報共有は本当に「共助」なのか

- 「自助」「共助」「公助」のうち、情報共有活動は「共助」的な活動として説明されることがあるが、果たしてそうなのだろうか？



目的の再定義：なぜ情報共有「しなければならない」のか



- サイバーセキュリティサービスにおける「市場の失敗」の是正措置としての情報共有の必要性

⇒共有の目的①：

調査に必要な情報を得るため
（インシデントをクローズさせるため）

- 主に①の目的のために情報が流通することで、副産物的に、他の共有活活動参加組織が恩恵を受ける

⇒共有の目的②：

被害予防／早期認知のため
※最初から被害予防目的に特化して共有活動をしているケースもある

- 情報の非対称性解消のための情報共有の必要性（情報共有してみなければ、「自組織にどういう情報が不足しているのか」知ることができない）

⇒共有の目的①

⇒共有の目的③：※今回のガイダンスではスコープ外

被害組織同士だけでなく、インシデント対応にあたる専門組織／ベンダー間でも必要なこと

被害公表の目的

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。

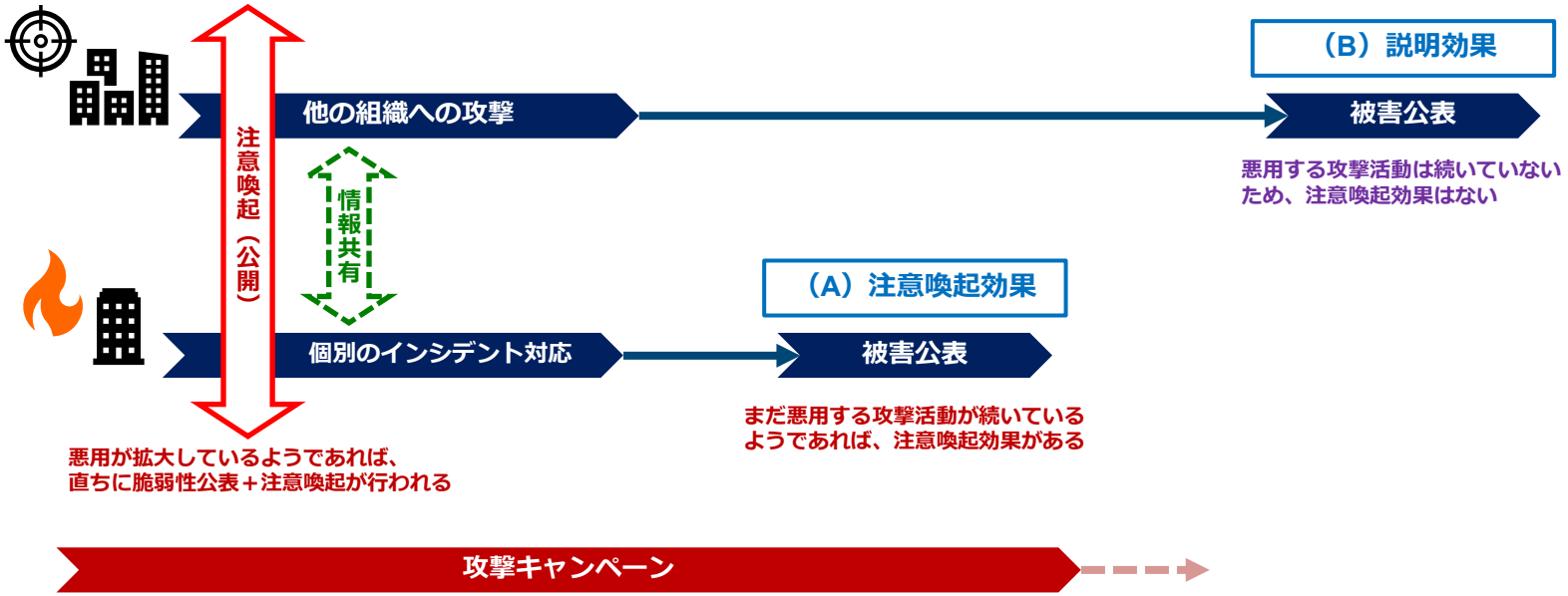
本ガイダンスの「はじめに」で述べたとおり、被害組織から自主的に公表される情報が広く伝わることで、サイバー攻撃の脅威に対する社会的な認知が向上し、社会全体での対策が進む可能性や同様の被害公表を行う被害組織のインシデント対応への理解が向上する可能性につながります。

被害公表時になぜ「原因」を説明するのか

■ 被害公表時に「原因」を示す目的

A：他の利用組織など広く社会全体に注意喚起効果を持つ

B：侵害原因を可能な範囲で示すことで自組織の運用・管理上の問題だったのかゼロデイ攻撃など事前の予防が困難なものだったのか示す



「特定の製品／サービスが悪用された」という情報

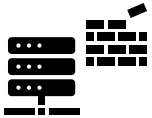
- 同じ情報であっても、「その情報をどう扱いたいか」という点においてそれぞれ利害の異なるプレーヤーが複雑に関係する状態にある ⇒ 情報を扱うにあたって利害の衝突が発生してしまう

消極的な背景／動機を持つ

メーカー

Sier／運用保守ベンダー

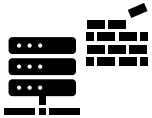
原因：製品／サービス
⇒自組織の“責任”を
増やす情報



積極的な背景／動機を持つ

被害組織

原因：製品／サービス
⇒自組織の“責任”を
減らす情報



積極的な背景／動機を持つ

他のユーザー

専門組織

メディア

顧客、取引先

ガイダンスにおける「原因情報」の取り扱いの解説①

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。

ガイダンスにおける「原因情報」の取り扱いの解説②

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。

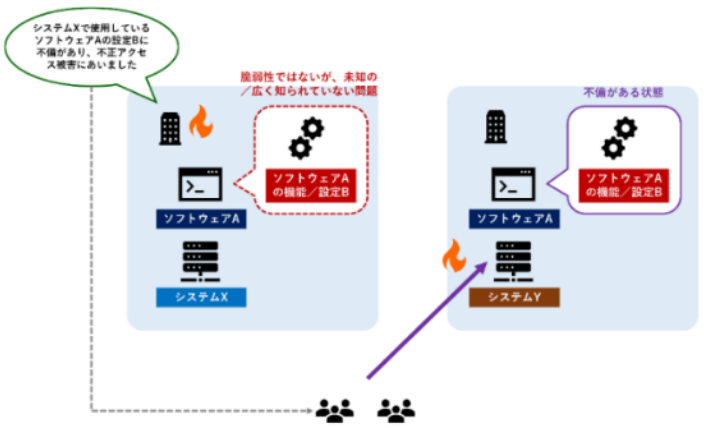


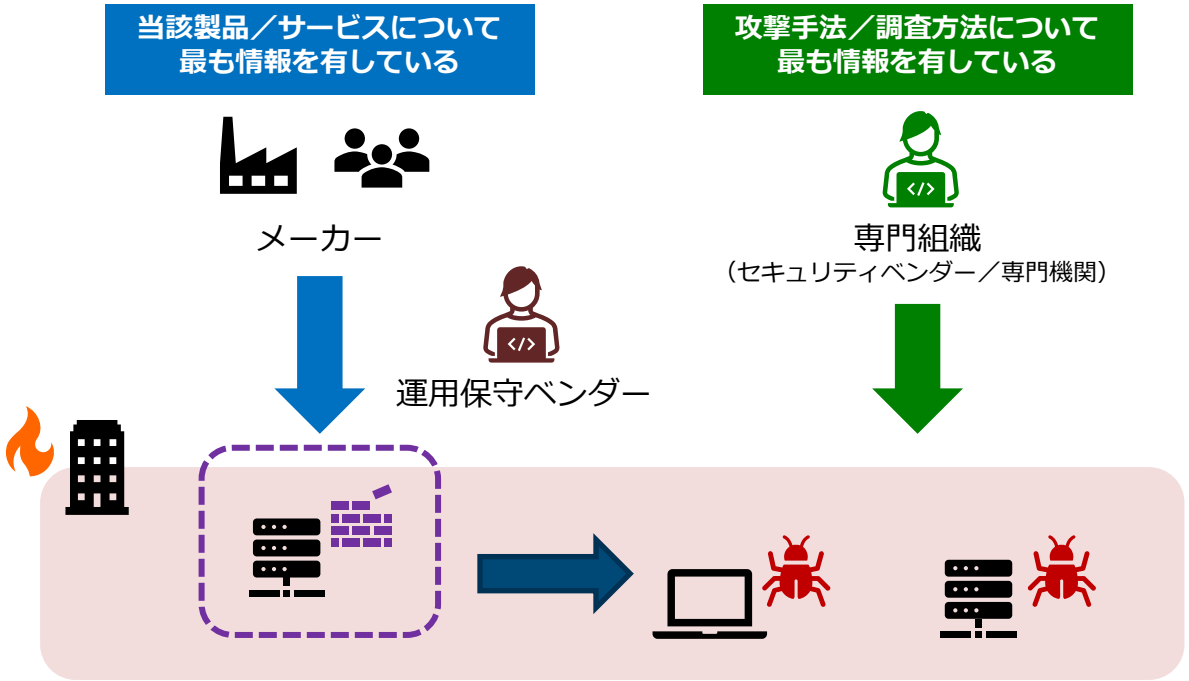
図 63

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

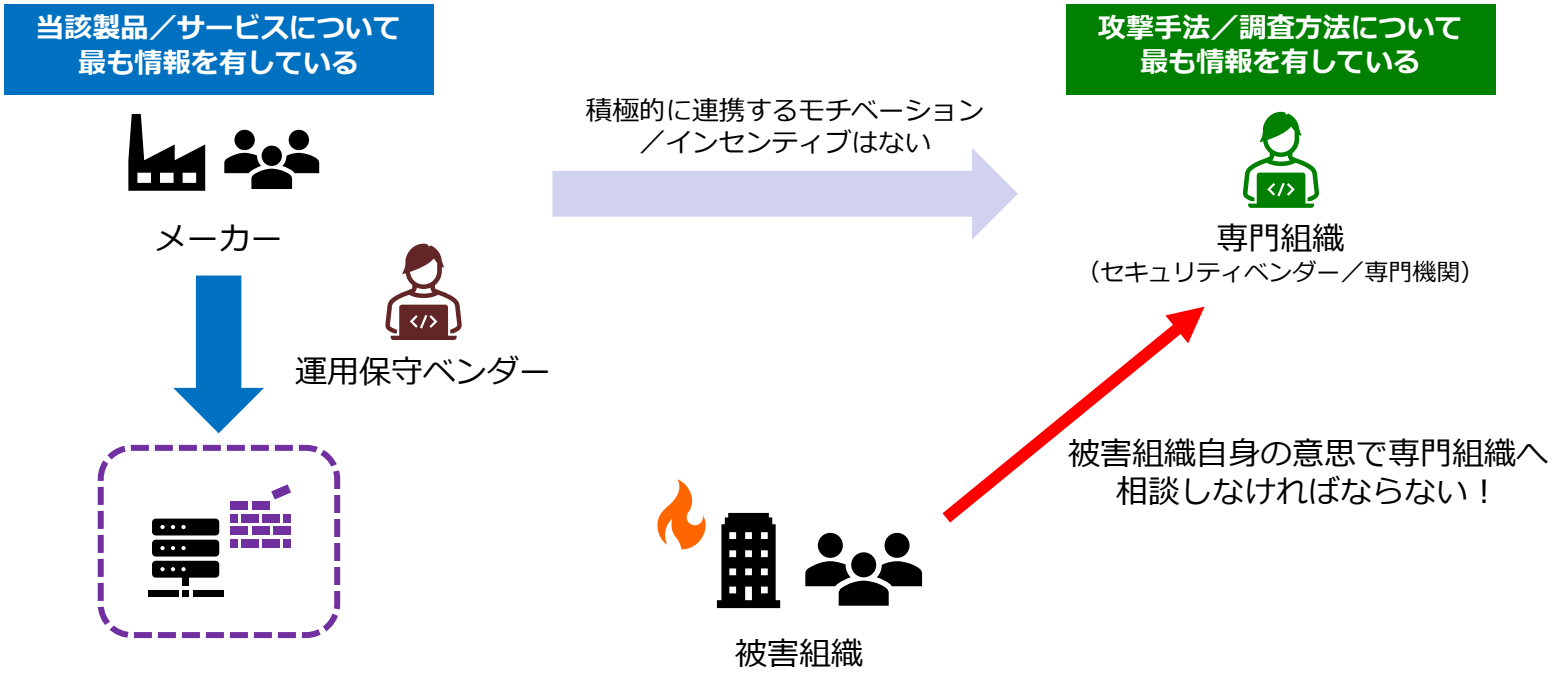
なぜメーカーからの情報だけでは不十分か

- 脆弱性の悪用事案が発生している場合、「脆弱性情報」を伝えるだけでは足りない
- 当該脆弱性悪用はあくまでInitinal Accessでしかないため、その後のラテラルムーブメントの調査をどうフォローできるかが重要



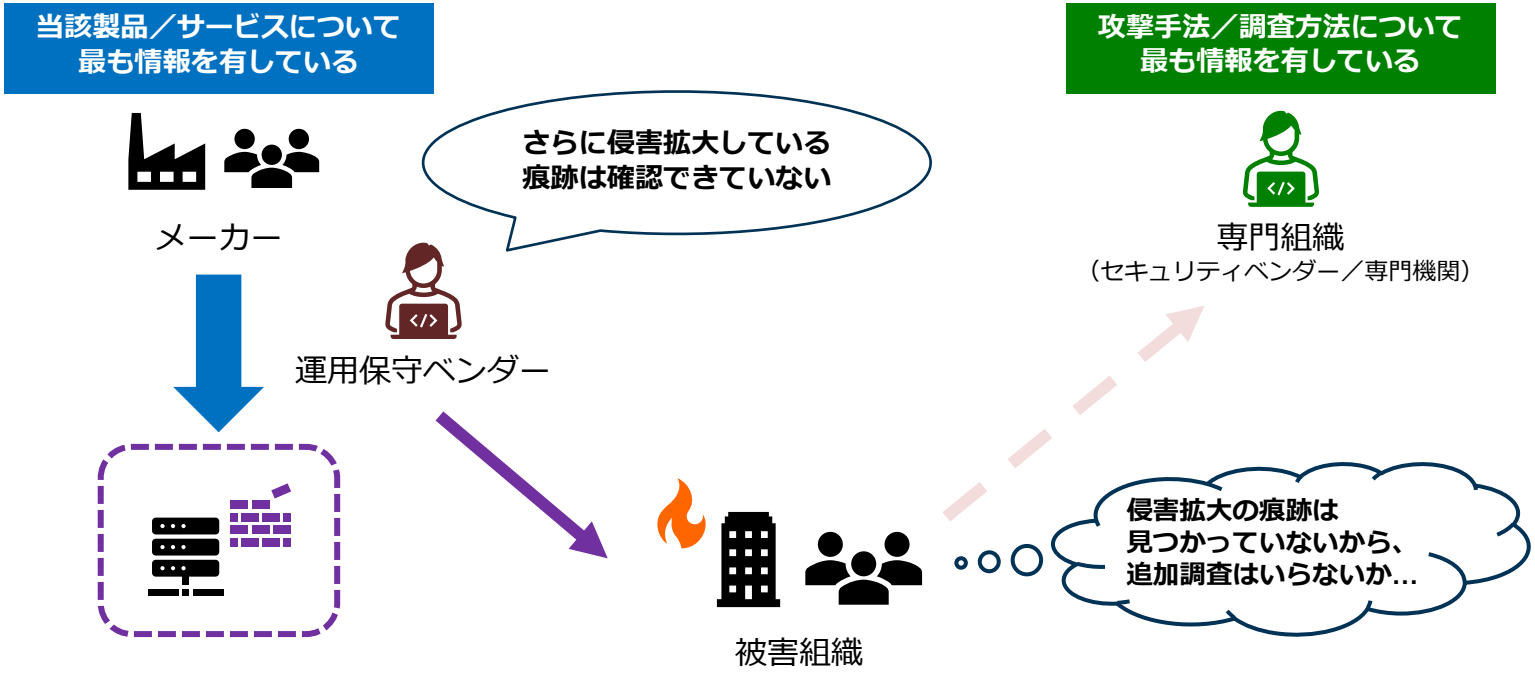
インシデント対応をどこまでフォローできるのか

- 専門組織への相談を積極的に推奨されるケースは少ない
- 基本的に被害組織自ら判断しないといけない



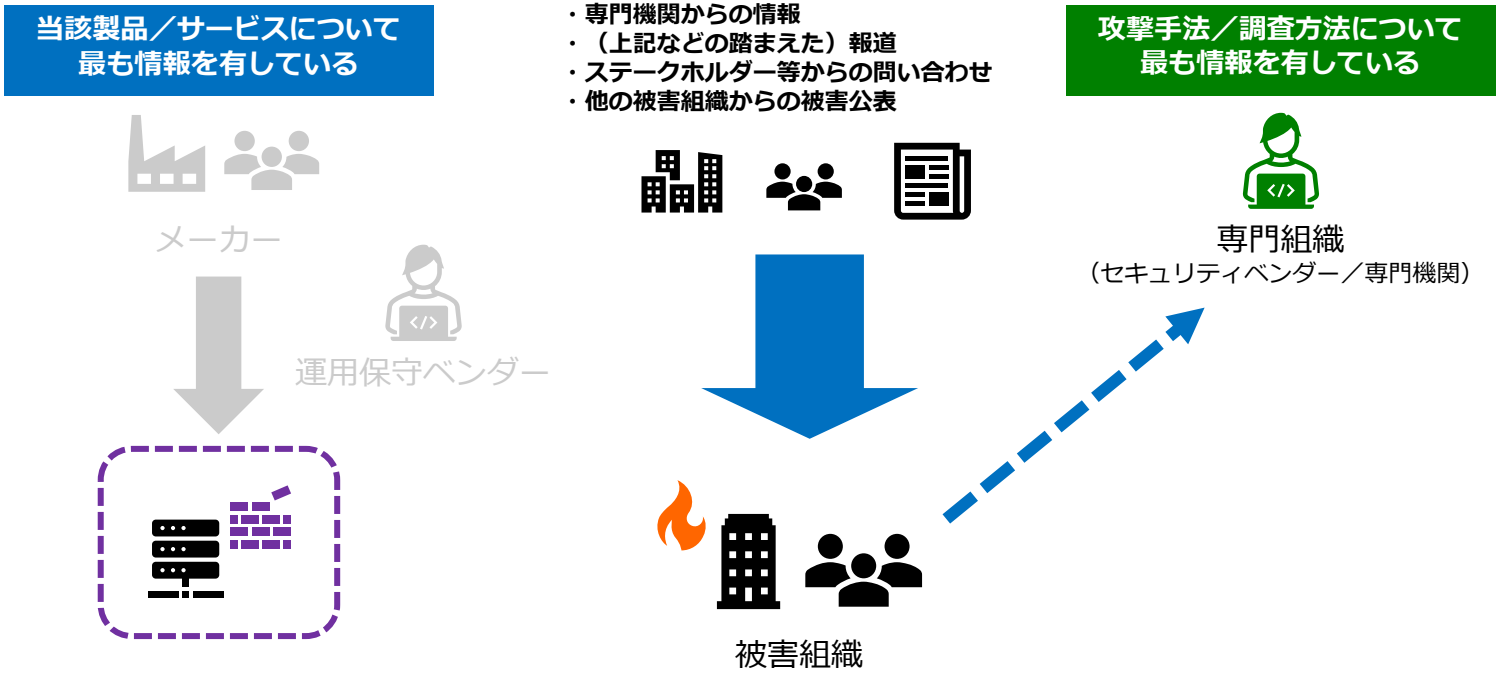
インシデント対応をどこまでフォローできるのか

- 運用保守ベンダーとして”守備範囲”外の調査まで積極的にユーザーを説得しづらい
- メーカー、運用保守ベンダー、被害組織それぞれ、積極的な侵害有無調査を行うインセンティブ／モチベーションを有しにくい



インシデント対応をどこまでフォローできるのか

- 「外からの情報」によって、被害組織が対応の温度感を認識・判断できる場合がある
- 他方で外部が”無風“であれば、対応の温度感を認識することができなくなる



ガイダンスが目指すもの：「情報の非対称性」をいかに埋めていくか

- 攻撃被害拡大を防げないのも、被害組織に（見当違いの）厳しい評価がなされてしまうのも、すべて「情報の非対称性」が存在するから（情報共有の問題だけ解消すればいいわけではない）
- いかにそれぞれのプレーヤーが必要とする／伝えるべき情報が効率的に伝えられるかが重要
- ガイダンスなどに基づいて「ルール」「規範」が広がることで、情報の非対称性が解消していけば、お互いに無駄な衝突や機会損失をしない関係性になれる

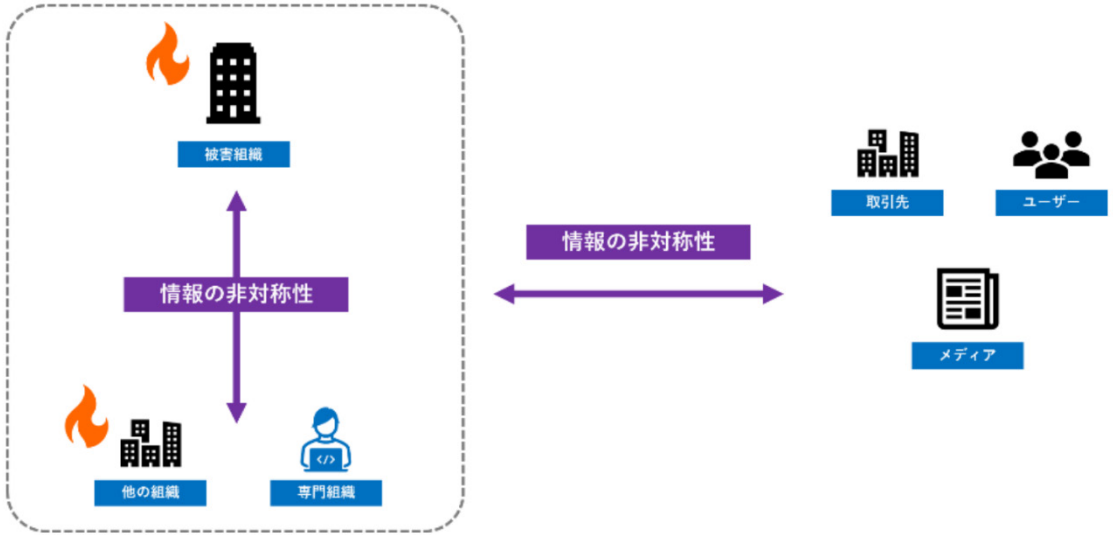


図 9

情報の非対称性問題：対応の温度感／相場観を作るために必要なことは

- 大多数の組織は情報共有活動に参加しておらず、対応の相場観などを「他の被害組織の被害公表」から推測している
- 他方で、被害公表の内容からは「適切な初動対応、再発防止が行えているのか」分からないケースが多い
  例：被害リリースにおける「外部の専門機関に相談しました」という記載　⇒本当に当該事案に適切に対応できる組織が対応のしかたを示す情報ではない

共有・公表ガイダンスQ16補足（74頁）

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。

共有・公表ガイダンスQ4補足（40頁）

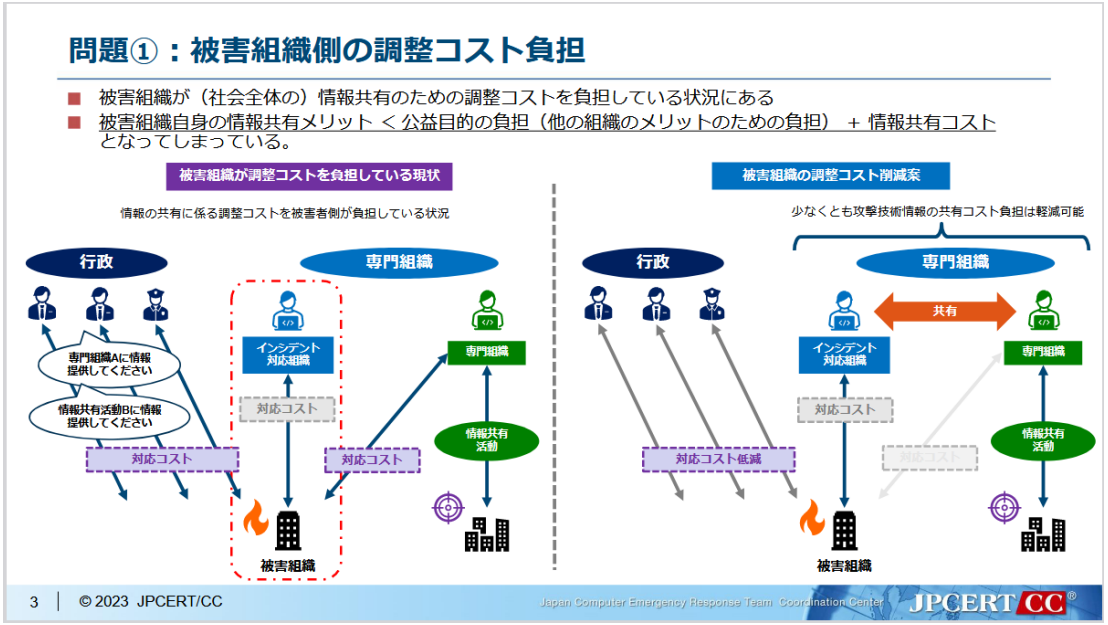
1．　経緯と対応の流れ

○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

“NDA問題”検討会

出典：経済産業省
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/cyber_attack/pdf/001_02_02.pdf

- 共有・公表ガイダンスの”フェーズ２”
- 被害組織から委託を受けた専門組織同士の情報共有活動を促進を目指す
- 被害組織の「対応コスト」を減らしながら、関係者間の「情報の非対称性」を解消することを目指す
- ファーストレスポンダー（初動対応にあたるベンダー等の組織）の知見向上



お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：ew-info@jpcert.or.jp
- https://www.jpcert.or.jp/reference.html

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

脆弱性に関するお問い合わせ

- Email：vultures@jpcert.or.jp
- https://jvn.jp/