サイバー攻撃被害の公表、果たして「正解」なんてあるのか？（ver.1.2）

一般社団法人JPCERTコーディネーションセンター
政策担当部長 兼 早期警戒グループマネージャー
脅威アナリスト
佐々木 勇人

「InternetWeek2023」でのセッション

講演者


佐々木 勇人


蔦 大輔


福田 陽平

- 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)
- 蔦 大輔(弁護士 森・濱田松本法律事務所)
- 福田 陽平(記者 NHK科学文化部)

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

- 専門機関、弁護士、メディア／記者の3つの立場・視点から、サイバー攻撃被害公表の論点、あり方について議論
- 「被害情報」を巡って、極めて複雑で利害関係が衝突し合う状況が存在する点について要素分解しながら解説
- 「答えがない」課題に対して、いかに漸次的に問題を解消していくか

前回のおさらい

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

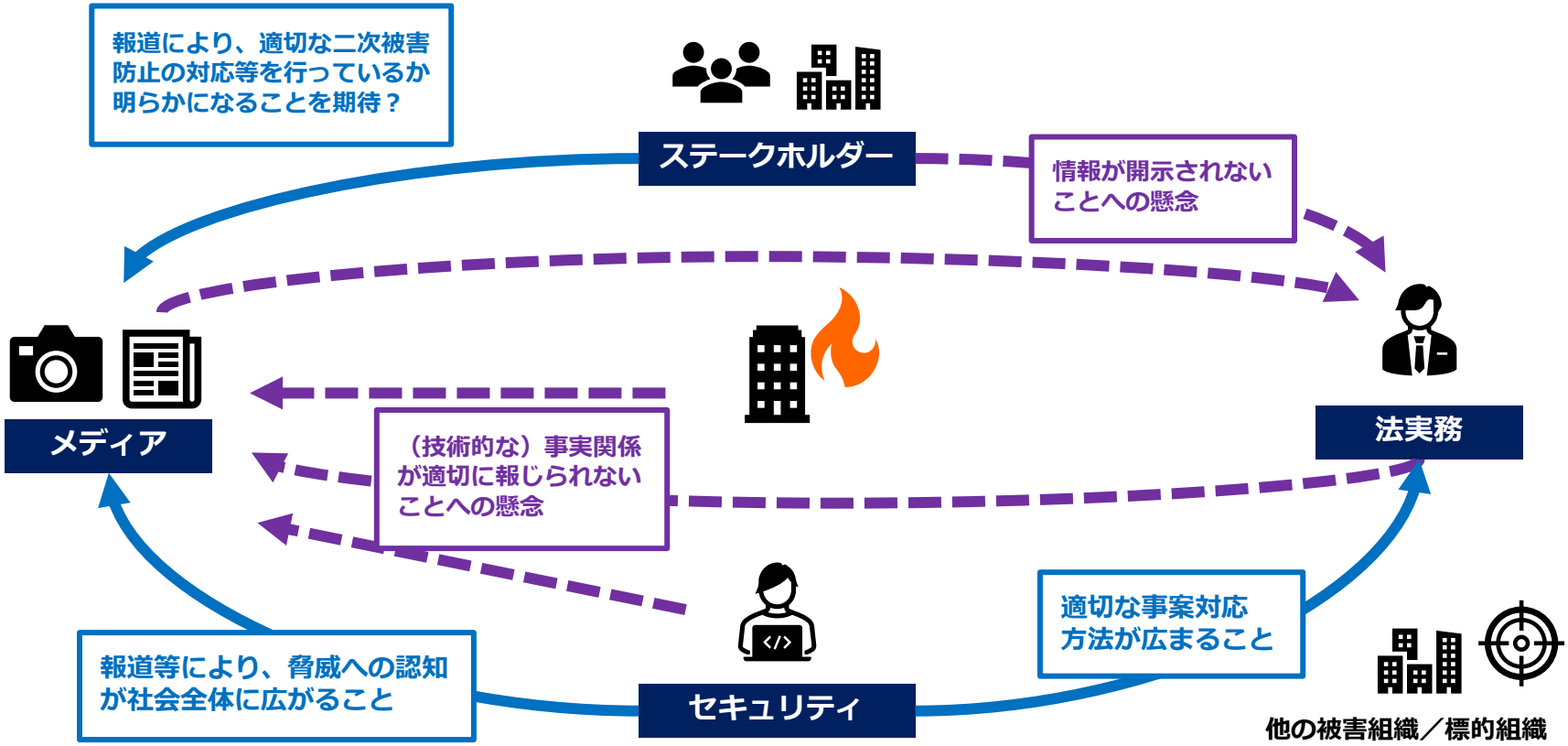
・原因／手口についても公表することで注意喚起効果がある

・情報共有のために攻撃手口についても公表します

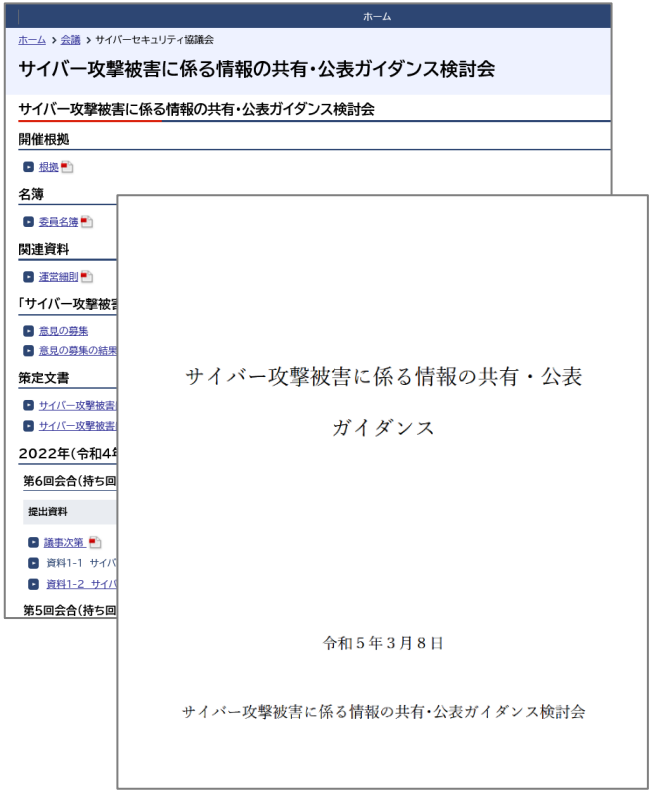
・他の組織の被害予防に役立てば幸いです

被害公表

それぞれの「ジレンマ」

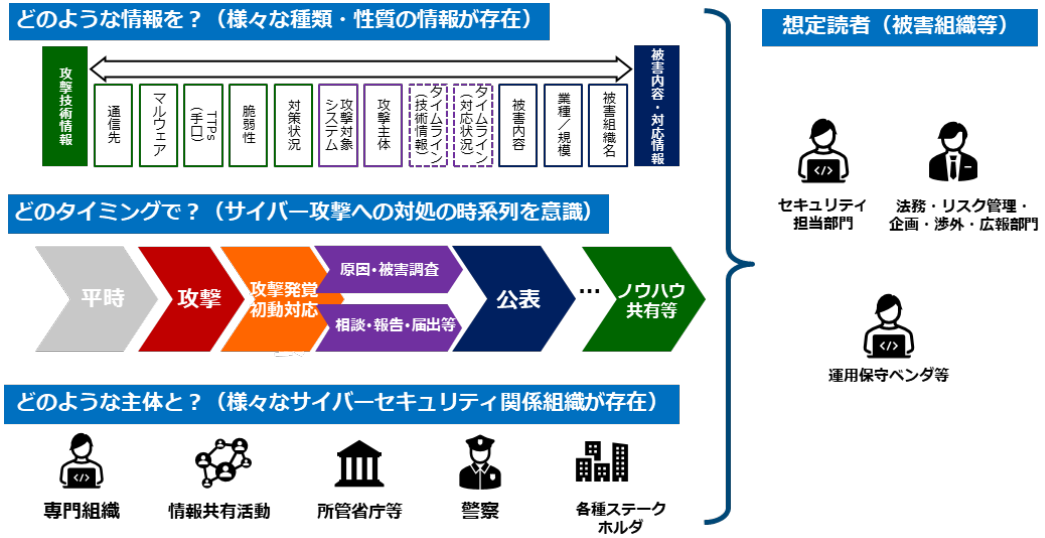


「サイバー攻撃被害に係る情報の共有・公表ガイダンス」



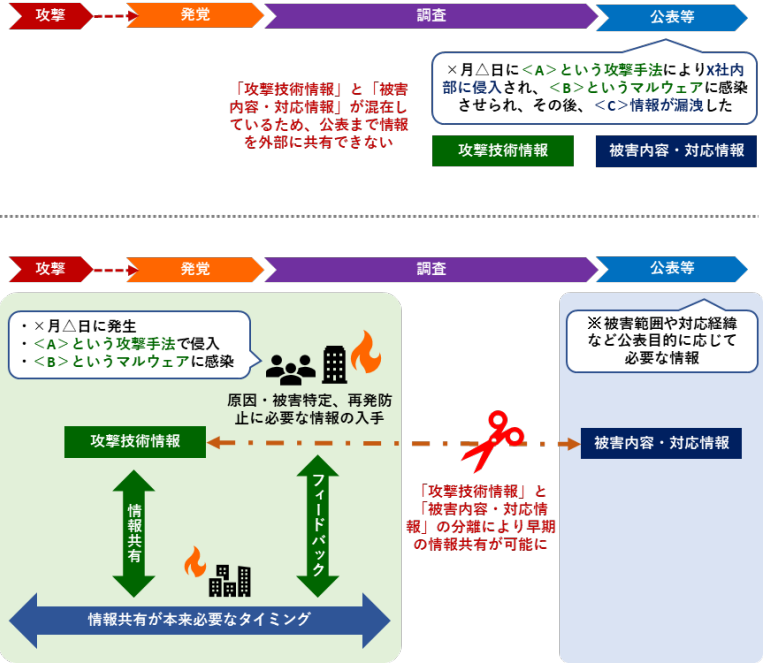
出典：内閣サイバーセキュリティセンター
「サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会」
https://www.nisc.go.jp/council/cs/kyogikai/guidancekentoukai.html

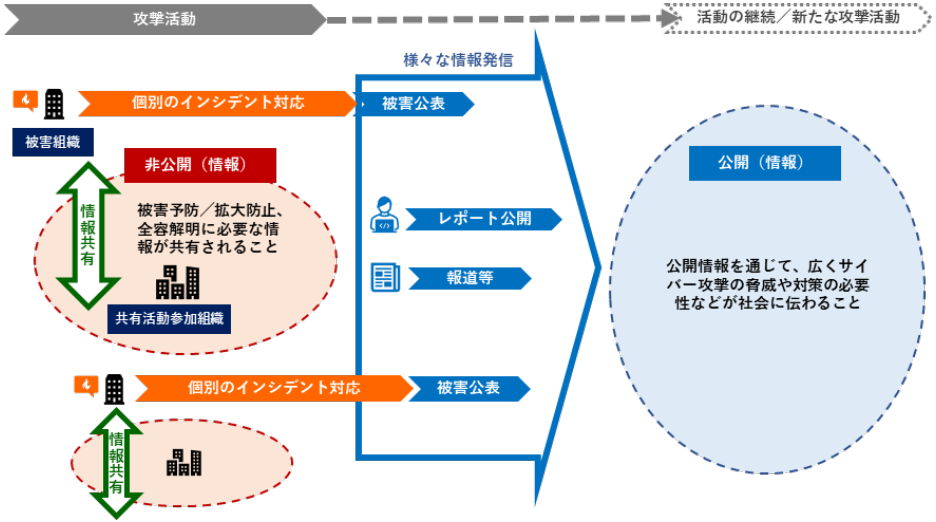
- 2022年5月よりサイバーセキュリティ協議会に設置された「サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会」（事務局：警察庁、総務省、経済産業省、NISC、JPCERT/CC）にて検討を行ったもの
- パブリックコメント実施の後、2023年3月に同ガイダンスを公表



ガイダンスのコンセプト：「情報共有」と「被害公表」の分離

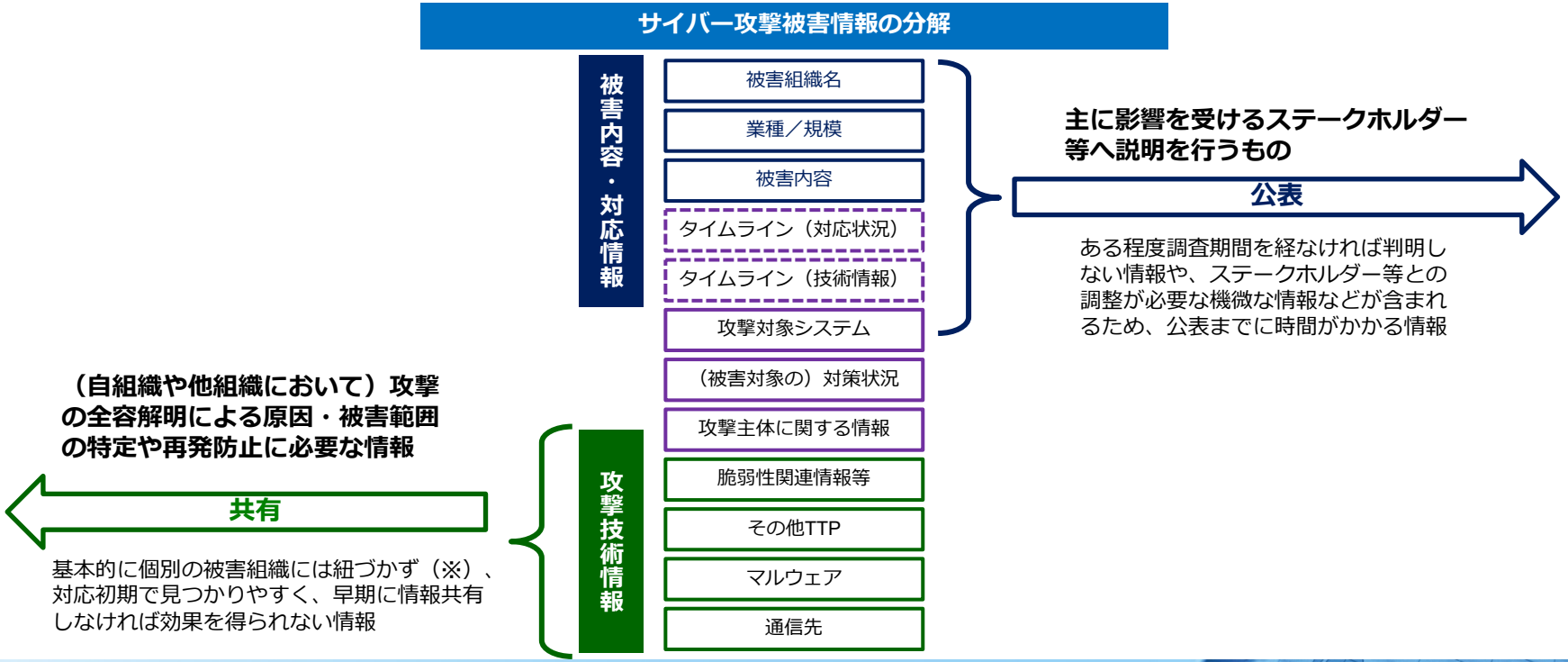
- タイミングの違い：被害公表時では情報共有として有効なタイミングを失している
- 目的の違い：情報共有の目的と被害公表の目的は違う
- 手段／対象の違い：情報共有→非公表で他の標的／被害組織に対して行う　被害公表→ステークホルダーなど影響を受ける関係者に広く伝える





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）



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

出典：InternetWeek 2023 「サイバー攻撃被害の公表、果たして「正解」なんてあるのか？」パネル登壇の森・濱田松本法律事務所 蔦大輔先生投影資料より

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

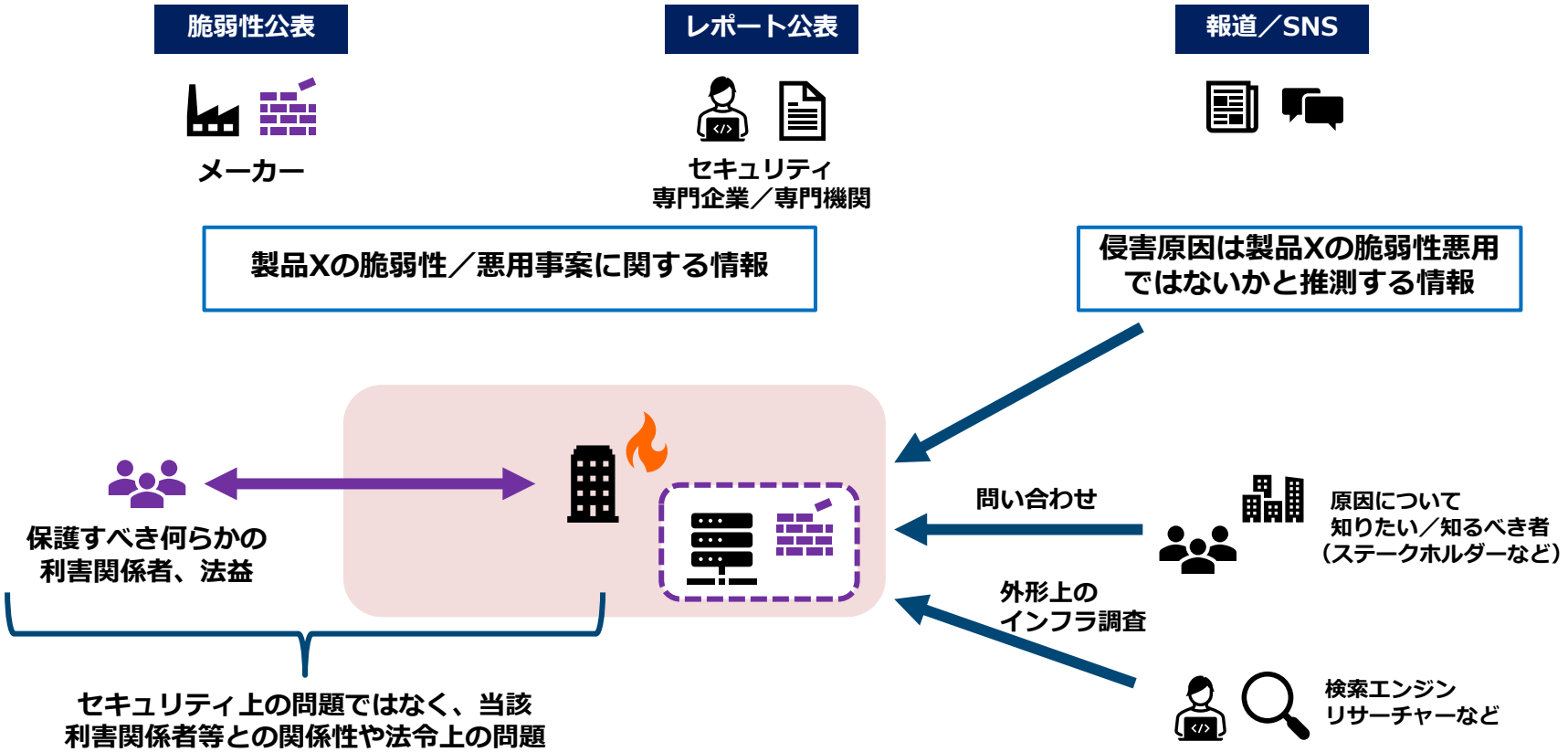
- ✓ サイバーセキュリティインシデントが重大であると**判断してから４営業日以内**に提出
- ✓ インシデント発見から不当な遅延なく重大性を判断

■ 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

出典：InternetWeek 2023 「サイバー攻撃被害の公表、果たして「正解」なんてあるのか？」パネル登壇　森・濱田松本法律事務所 蔦大輔先生　投影資料より

「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・・・



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。

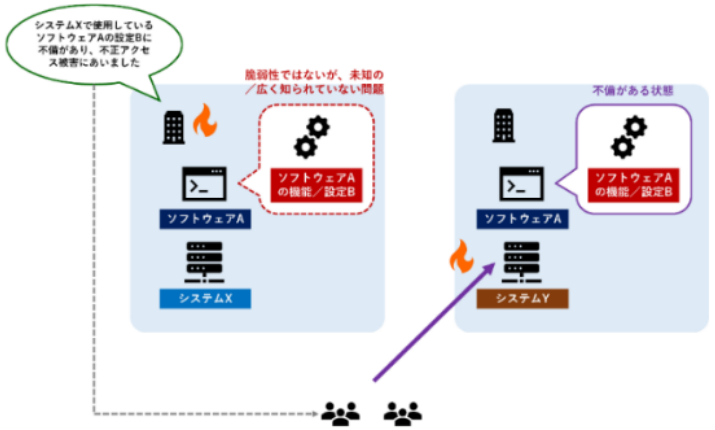


図 63

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。

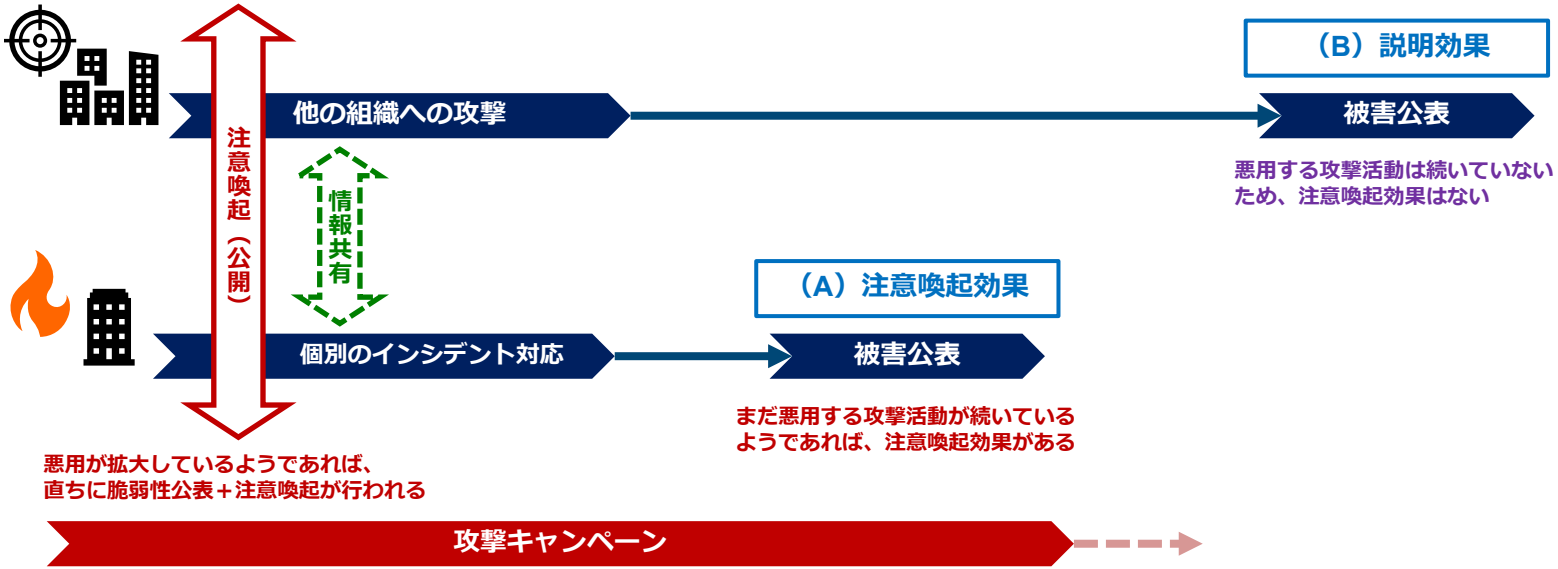
一方で、フィッシングサイトやマルウェアサイトではない偽サイト、「多くのユーザーがアクセスすること自体を不法行為の目的」としているような偽サイトの場

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



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）

外形上「見える」侵害経路からの被害事例

情報セキュリティインシデント調査委員会報告書について

大阪急性期・総合医療センターは令和4年10月31日早朝に発生したサイバー攻撃により電子カルテを含めた総合情報システムが利用できなくなり、救急診療や外来診療、予定手術などの診療機能に大きな支障が生じました。地域における中核的な役割を担う病院として、府民の皆様、とくに患者さんをはじめとする関係者の皆様に多大なるご迷惑、ご心配をおかけいたしましたことを、改めて深くお詫び申し上げます。また、さまざまな形でご支援をいただいた多くの皆様に厚く御礼申し上げます。

事件発生当日、電子カルテの異常を覚知し、ランサムウェアによる重大なシステム障害が発生していることが判明したため、幹部職員を招集して状況把握と紙カルテの運用など当面の診療体制の方針を決定しました。また、大阪府立病院機構本部、大阪府、大阪府警、大阪市保健所、内閣サイバーセキュリティセンター、厚生労働省医政局などの各方面に連絡をしました。特に厚生労働省からはサイバーセキュリティ初動対応支援チームの専門家が派遣され、発災当日からWEBを通じて多くの支援・有益な助言をいただき、ベンダーの方々の協力を得て、原因の究明に努めるとともに、職員および関係者が一丸となって復旧に取り組みました。

出典：大阪急性期・総合医療センター
「情報セキュリティインシデント調査委員会報告書について」
https://www.gh.opho.jp/important/785.html

報道資料

NISC

令和５年８月４日
内閣官房内閣サイバーセキュリティセンター

内閣サイバーセキュリティセンターの電子メール関連システムからの
メールデータの漏えいの可能性について

今般、内閣サイバーセキュリティセンター（NISC）の電子メール関連システムに対し、不正通信があり、個人情報を含むメールデータの一部が外部に漏えいした可能性があることが判明しました。

これは、メーカーにおいて確認できていなかった電子メール関連システムに係る機器の脆弱性を原因とするものであると考えられ、同様の事案は国外においても確認されています。

NISCにおける本事案の経緯及び講じた措置は以下のとおりです。

- ６月13日　電子メール関連システムに係る不正通信の痕跡を発見。
- ６月14～15日　当該システムの状況を確認するため、速やかに運用を停止。不正通信の原因と疑われる機器を交換するとともに、他の機器等に異常がないことの確認や、内部監視の強化等の対策を実施の上で、当該システムを再稼働。
- ６月21日　保守運用事業者の調査により、不正通信が当該機器の脆弱性を原因とするものであることを示す証跡を発見（本事案について個人情報保護委員会に報告）。

出典：内閣官房内閣サイバーセキュリティセンター
「内閣サイバーセキュリティセンターの電子メール関連システムからのメールデータの漏えいの可能性について」
https://www.nisc.go.jp/pdf/news/houdousiryou_20230804.pdf

「特定の製品／サービスが悪用された」という情報

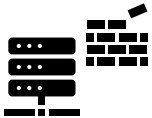
- 同じ情報であっても、「その情報をどう扱いたいか」という点においてそれぞれ利害の異なるプレーヤーが複雑に関係する状態にある ⇒ 情報を扱うにあたって利害の衝突が発生してしまう

消極的な背景／動機を持つ

メーカー

Sier／運用保守ベンダー

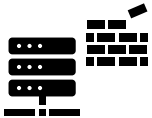
原因：製品／サービス
⇒ 自組織の“責任”を増やす情報



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

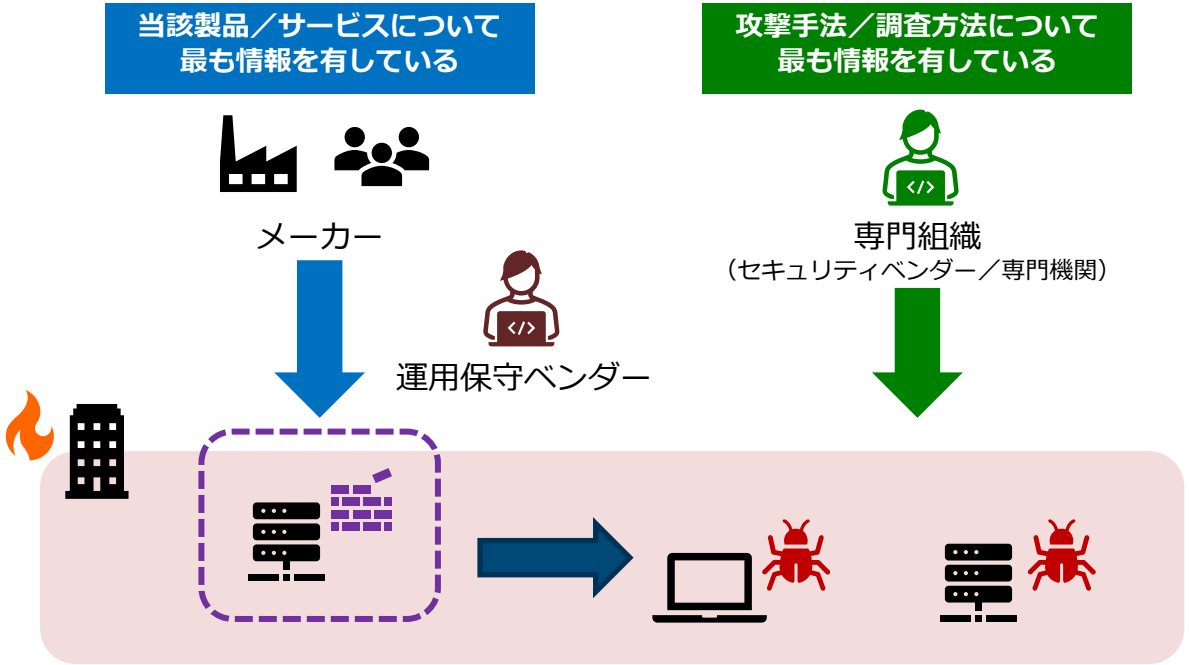
専門組織

メディア

顧客、取引先

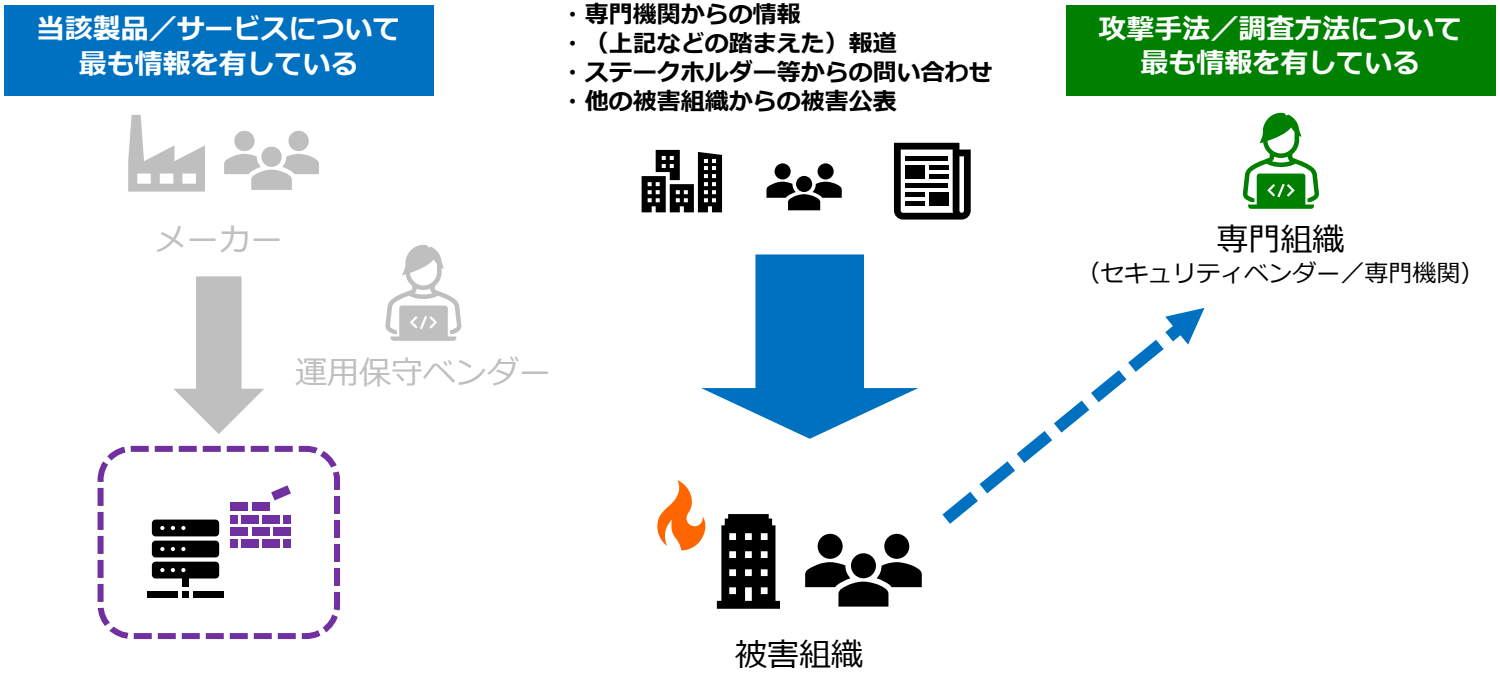
なぜメーカーからの情報だけでは不十分か

- 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

- 「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

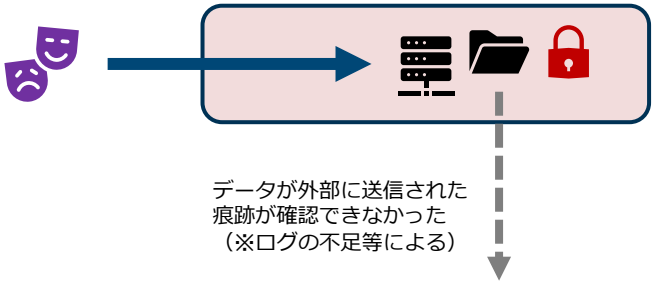


その後の論点・議論

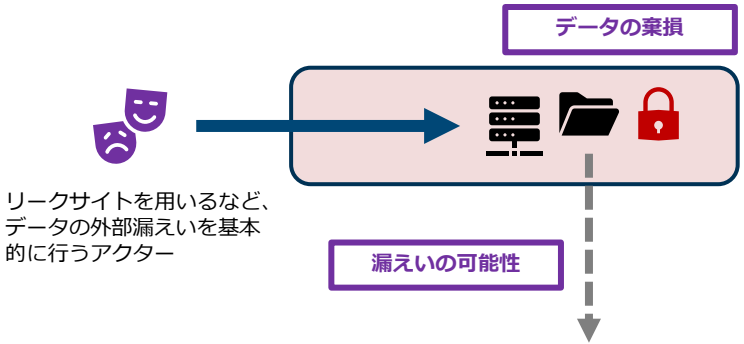
「被害公表／報道が増えた気がする」の背景

- 令和2年改正の全面施行（2022年4月～）以降の変化
- 「棄損」や「可能性」での報告義務化
- 3～5日以内の速報対応が必要に
- これまで「個人情報漏えい」として明確に扱われてこなかった事案も事故報告対象になり、被害公表対象としても増加している（特に、ランサムウェア攻撃被害）

これまで被害組織が想定していたもの

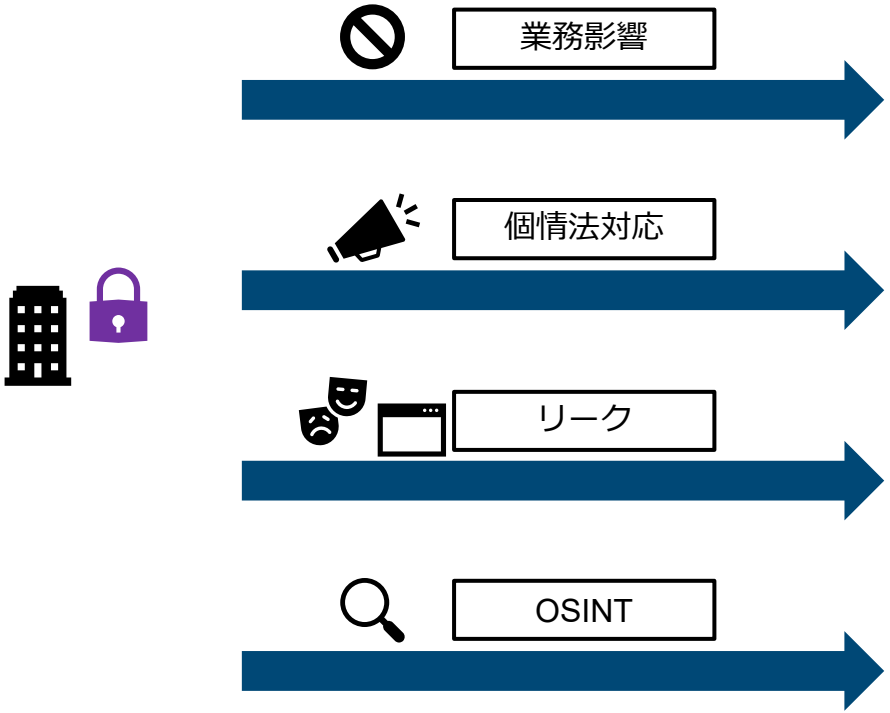


改正保護法の施行以降



ランサムウェア攻撃被害の特性

■ 他の不正アクセス事案に比べ、外部に被害事実が早期に認知されやすい



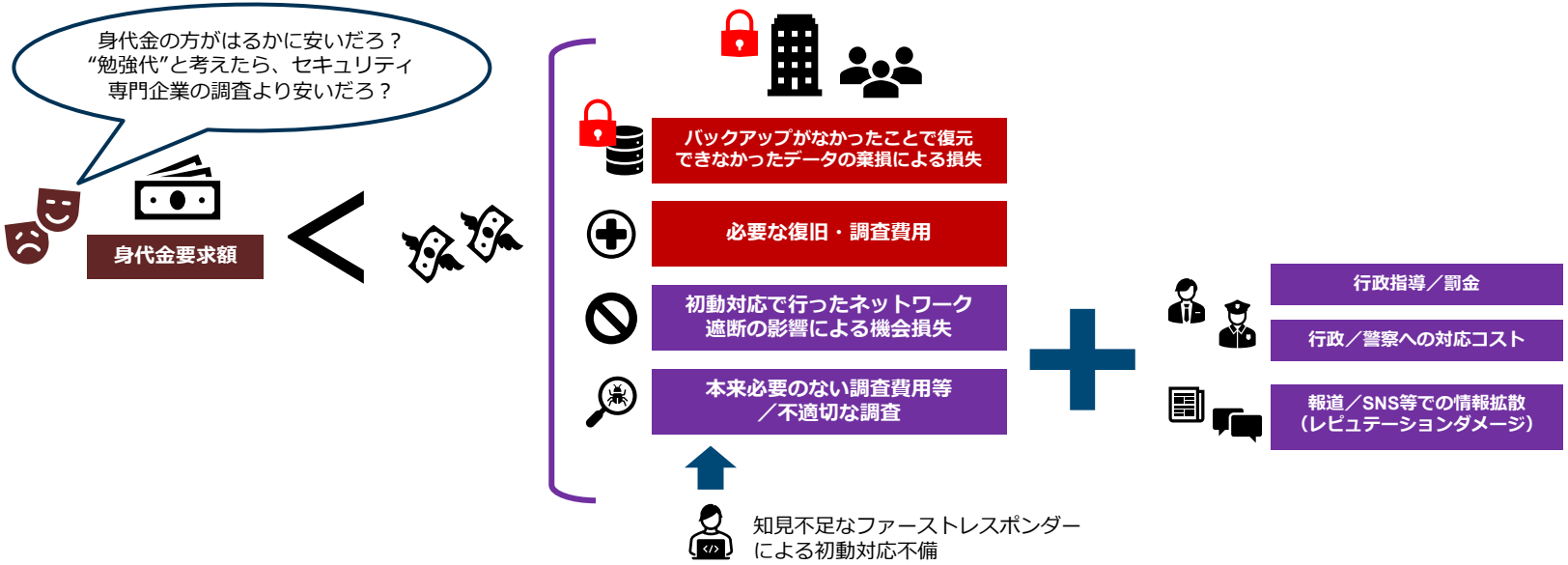
・顧客／取引先への連絡により被害を推測させる情報が拡散
・生産ライン停止時などに従業員等がSNS上でつぶやいてしまう、等

・漏えい等の恐れが高い時点で顧客等への通知と被害公表が行われる（原因が「ランサム」と明かさなくても、上記／下記等の事情から容易に推測されてしまう）

・（特に海外事案で）検体がVirustotalなどにアップロードされ、脅迫文から被害組織が推測されてしまうケース
・Webサーバー等外部からアクセス可能なシステムが暗号化されたり、ランサムノートが設置されてしまうことで、被害が検索可能なケース

ランサムウェア犯罪者の経済合理性

- 身代金支払いという選択肢は決して非合理的に選択されているわけではなく、極めて合理的に選択されている。攻撃者側も経済的に合理的な要求をしている
- 他方で、被害組織を取り巻く環境は被害組織に非合理的なコストを負担させてしまっている
- 本来必要のない調査や初動対応不備による機会損失の発生、インシデント対応における当局対応コストやレピュテーションリスクなど、「避けられるはずの損失・コスト」が“加算”されてしまっている



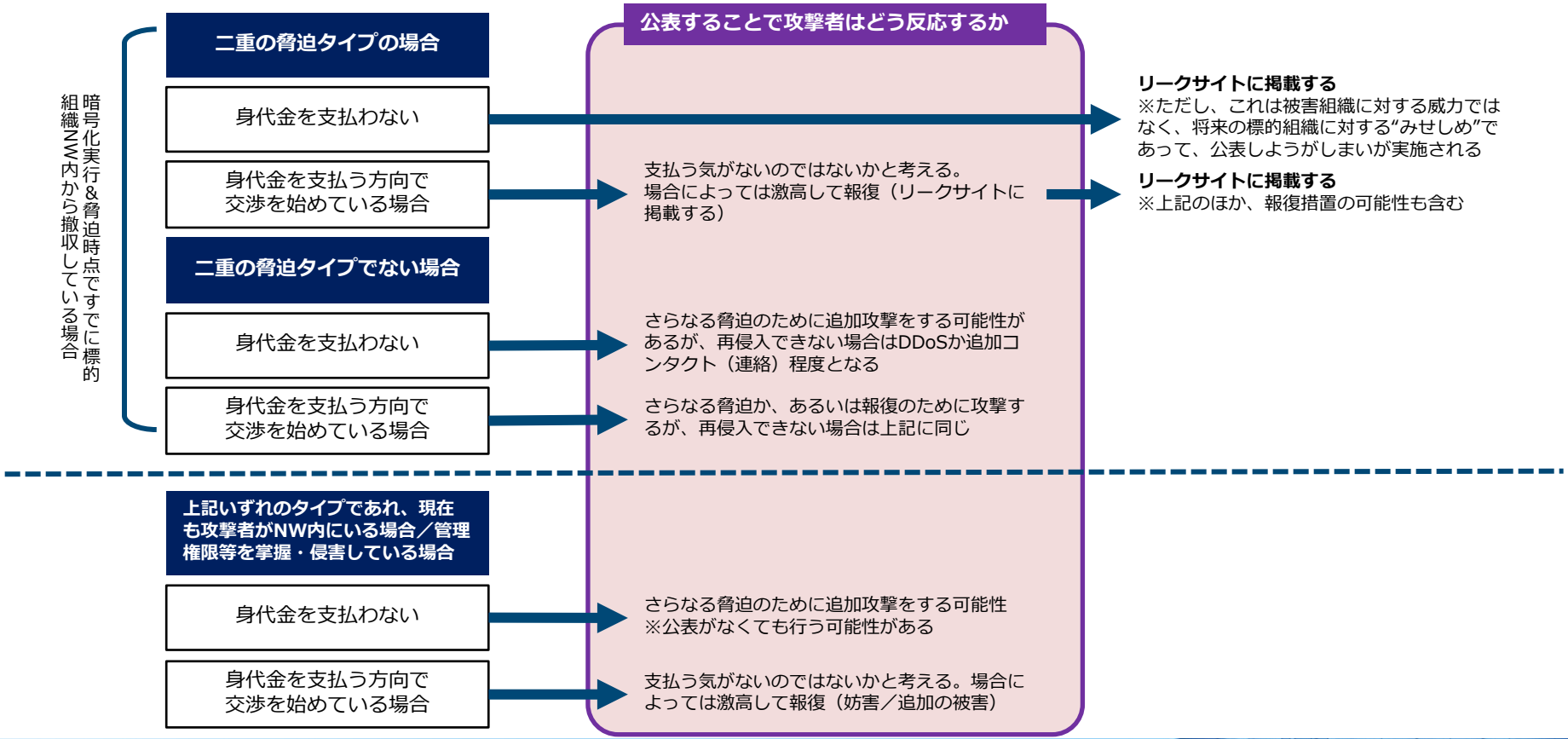
最近いただいた質問

- 「最近のランサムウェア攻撃の被害リリースにおいて、『ランサムウェア（攻撃）』と明記しないものが散見される。被害公表に『ランサムウェア／ランサム攻撃による～』と書かない理由はあるのか？」

- 結論から言えば、「書かない合理的理由はない」

- ただし、直近の報道事案等を踏まえて、「注目されたくない」と考える被害組織も多いと推察

ランサム攻撃であると公表することで攻撃はどう変化するか（※暫定的な考察）



報道と被害公表

- 被害組織からの公表前の“スクープ”記事再び・・・

出典：読売新聞オンライン「ＪＡＸＡにサイバー攻撃か、宇宙開発の「機微」閲覧の恐れ…警察から連絡受けるまで気づかず」
https://www.yomiuri.co.jp/politics/20231128-OYT1T50242/

出典：朝日新聞デジタル
「JAXAに複数回サイバー攻撃、機密流出か　NASA、トヨタ情報も」
https://www.asahi.com/articles/ASS6N40X6S6NUTIL02GM.html

被害組織だけの問題ではない


JPCERT CC

JPCERT/CC Eyes

Top > "インシデント"の一覧 > サイバー攻撃被害に係る情報の意図しない開示がもたらす情報共有活動への影響について

佐々木 勇人（Hayato Sasaki） 2023/12/05

サイバー攻撃被害に係る情報の意図しない開示がもたらす情報共有活動への影響について

ポスト メール

はじめに

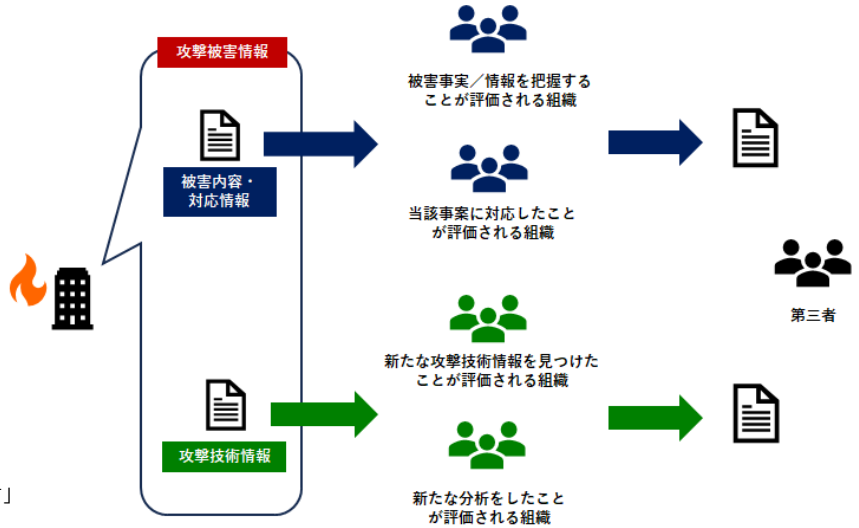
先日、JPCERT/CCが事務局として参加した、専門組織向上の情報共有活動の活性化に向けた「サイバー攻撃による被害に関する情報共有の促進に向けた検討会」の報告書が公開され、関連成果物のパブリックコメントが始まりました。

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
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/cyber_attack/index.html

JPCERT/CCはこれまでに下記の取り組みを通じて、情報共有活動の促進に向けたルール整備に取り組んできました。

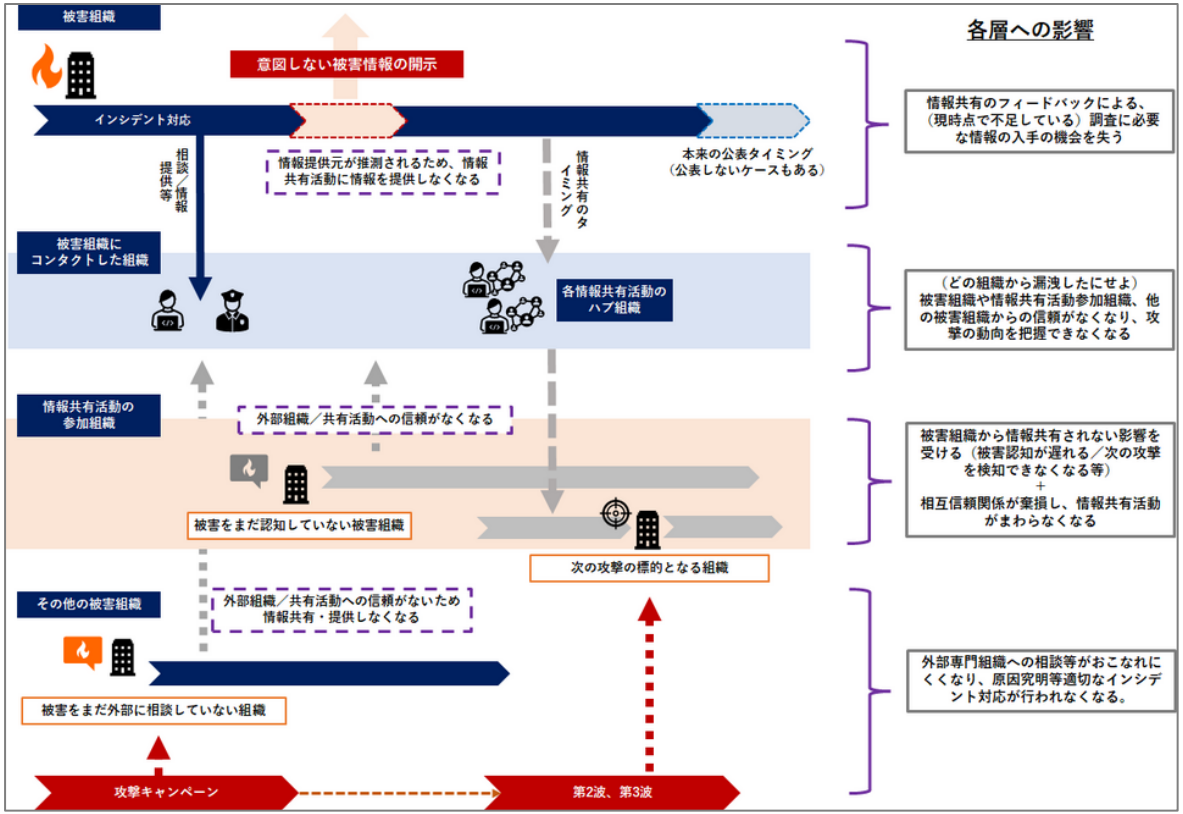
- 令和２年度総務省「サイバー攻撃の被害に関する情報の望ましい外部への提供のあり方に係る調査・検討の請負」の調査報告（2021年7月公開）[1]
- 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（2023年3月公開）の検討会事務局（内閣官、総務省、経済産業省、サイバーセキュリティ協議会事務局（NISC、JPCERT/CC））[2]

- 被害情報に触れる各プレーヤーは極めて利己的に被害情報を扱いやすい構造にある
- 被害組織側がコントロールできない情報開示が発生すると、同じ攻撃を受けている他の被害組織からの相談・情報提供が委縮してしまい、全体として攻撃対処に失敗する



出典：JPCERT/CC Eyes
「サイバー攻撃被害に係る情報の意図しない開示がもたらす情報共有活動への影響について」
https://blogs.jpcert.or.jp/ja/2023/12/leaks-and-breaking-trust.html

「攻撃キャンペーン」という観点の欠如



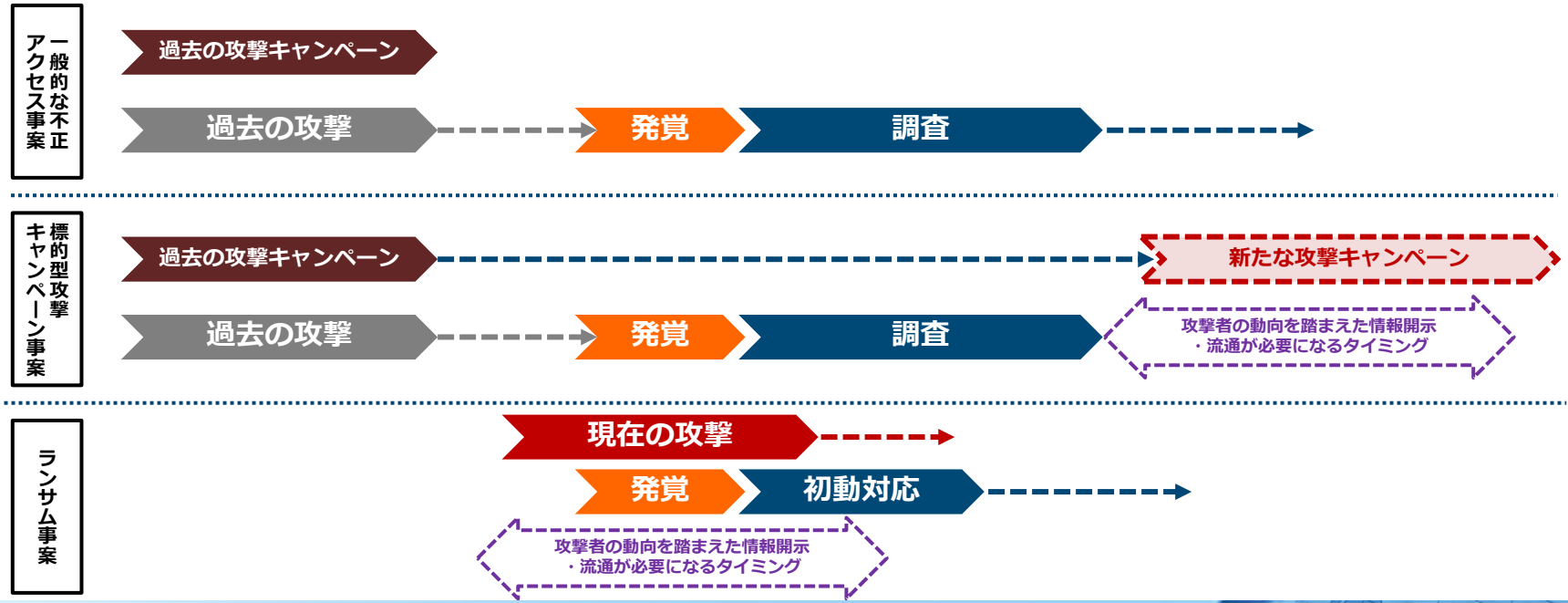
- 攻撃活動をミクロな観点だけで見ていると、「被害情報を開示すべきか否か」という極論に陥る
- 「攻撃キャンペーン」という観点から、他の被害組織、そして、次の標的組織の関係性というマクロな観点で見た場合、「被害情報を開示すべきか否か」という単純な議論ではなくなる

出典：JPCERT/CC Eyes
「サイバー攻撃被害に係る情報の意図しない開示がもたらす情報共有活動への影響について」
https://blogs.jpcert.or.jp/ja/2023/12/leaks-and-breaking-trust.html

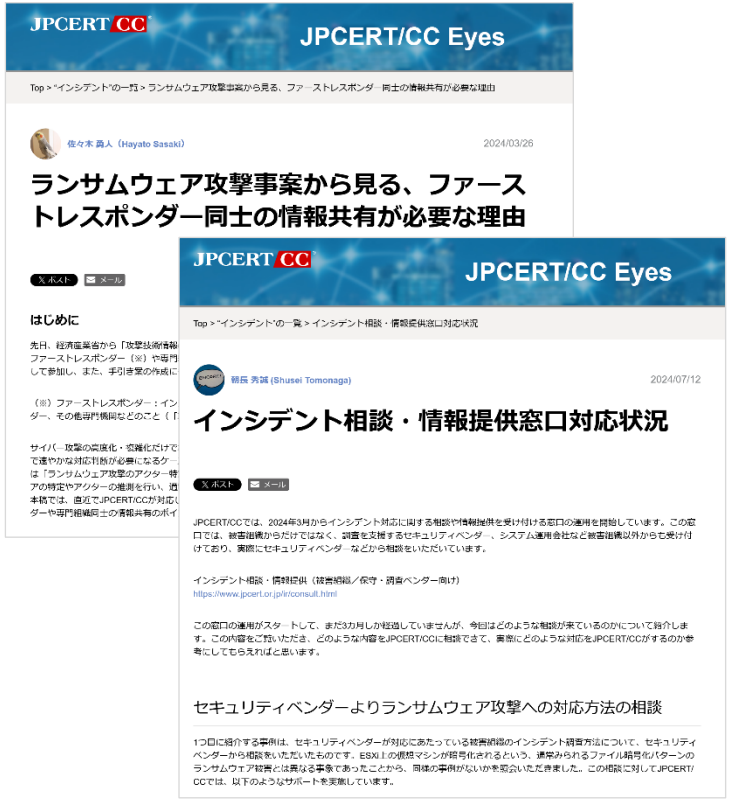
攻撃活動と被害組織保護という観点の欠如

- 「現在進行形」の事案に対する関係者の意識の欠如
- 被害組織自身が被害開示をコントロールしにくい事案であるランサムウェア攻撃の増加
- 被害が外部に知られること自体が攻撃者を利することに

⇒ 被害組織以外の関係者の「配慮」が必要



被害「事実」は周知されるのか？



出典：JPCERT/CC Eyes
（上）https://blogs.jpcert.or.jp/ja/2024/03/ransom_incident_and_infosharing.html
（下）https://blogs.jpcert.or.jp/ja/2024/07/ir_consult.html

- インシデント対応現場は被害組織と調査ベンダーの間の「閉鎖空間」
- 第三者の眼が入りづらいため、初動対応やその後調査等に失敗していても、修正されにくい構造
- 攻撃や被害の全容について調査不足・対応不足のまま被害公表やステークホルダーへの通知が行われてしまっていても、誰もそのミスに気付けない
- セカンドピニオン的相談やファーストレスポンダー同士の平時から情報共有（知見の補強）が必要