脅威情報共有・活用を巡る現場の課題

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

自己紹介

佐々木 勇人

【肩書】
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

【経歴】
2010年～ 情報処理推進機構（IPA）
2013年～ 経済産業省 情報セキュリティ政策室
（課室名は当時）
2016年～ JPCERT/CC

■ **脅威アナリストとしての活動**

—注意喚起などの情報発信、インシデント対応支援
—APTグループの追跡（特にLazarusの各サブグループ）
・2021年 CODEBLUE、HITCON、JSAC2023,2024での発表、専門誌への寄稿など
—ランサムウェア攻撃対処
・侵入型ランサムウェア攻撃を受けたら読むFAQ（2022年1月）作成
—講演／取材対応など
—関心事項の解説ブログ／寄稿
・能動的サイバー防御、被害公表のあり方、SSL-VPN製品のサプライチェーン問題

■ **政策渉外？的な活動**

—サイバーセキュリティ協議会の立ち上げ
—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」（2020年～2021年）
—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（2022年）、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の執筆
—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（2023年）、「攻撃技術情報の取扱い・活用手引き」の執筆

■ **学会活動／研究活動**

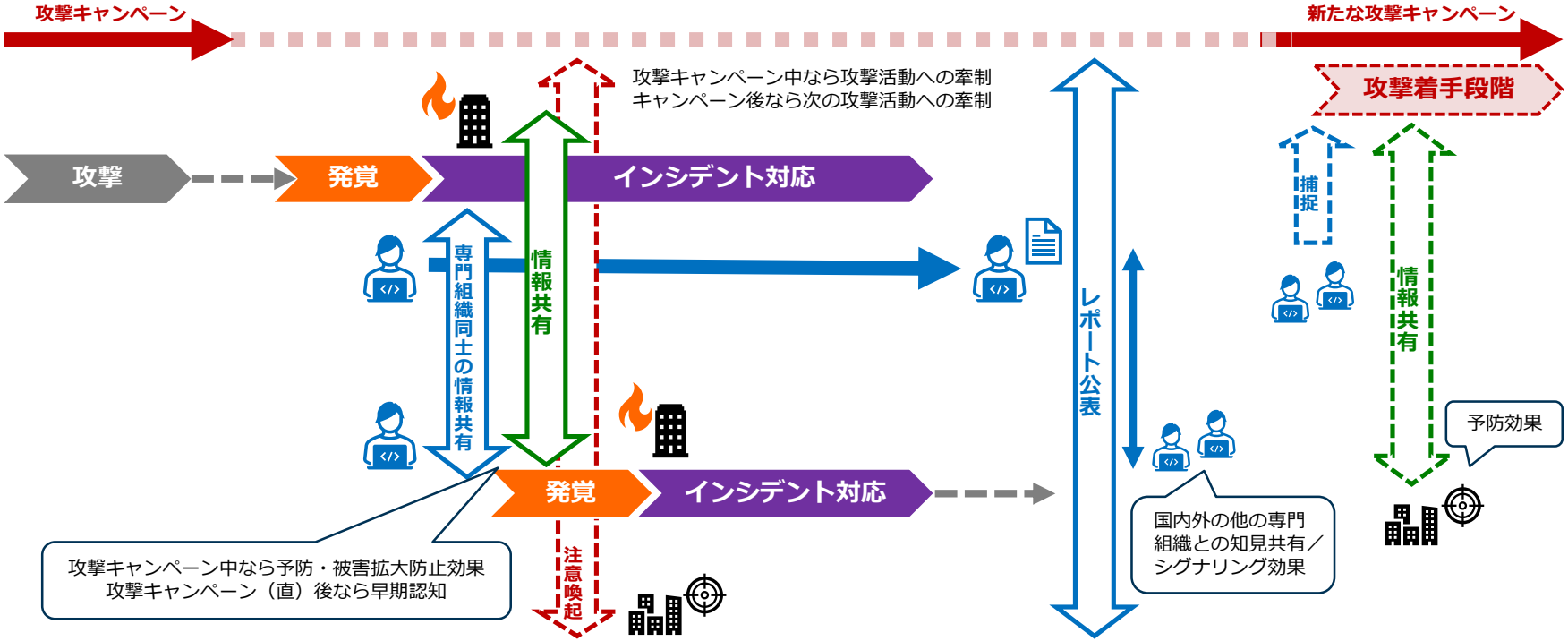
—サイバーセキュリティ法制学会理事（2023年～）
—情報ネットワーク法学会サイバーセキュリティ分科会
—安全保障専門誌への寄稿など

今日ご紹介すること

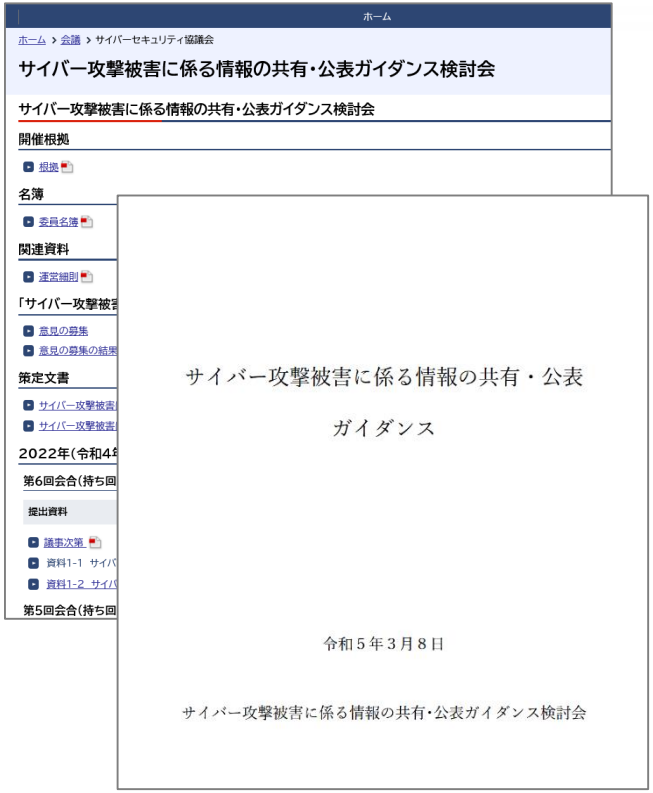
- 脅威情報は現場でどのように作出され、展開、利用されているのか（脅威情報の流通サイクル）
- 「被害組織同士」「被害組織⇔専門組織間」の情報共有の課題
- 国への国内外からの「情報提供」の課題
- 専門組織同士の情報共有の課題
- 官民間の情報共有の課題
- 脅威情報流通の活性化に向けて

それぞれの情報をどのタイミングで何の目的に使うのか

- 横軸：時間軸、縦軸：情報の流れ
- 攻撃類型／タイミングごとに目的と効果（被害防止、被害認知、知見共有、成果発信、攻撃者への牽制）が併存したり別々になったりしている

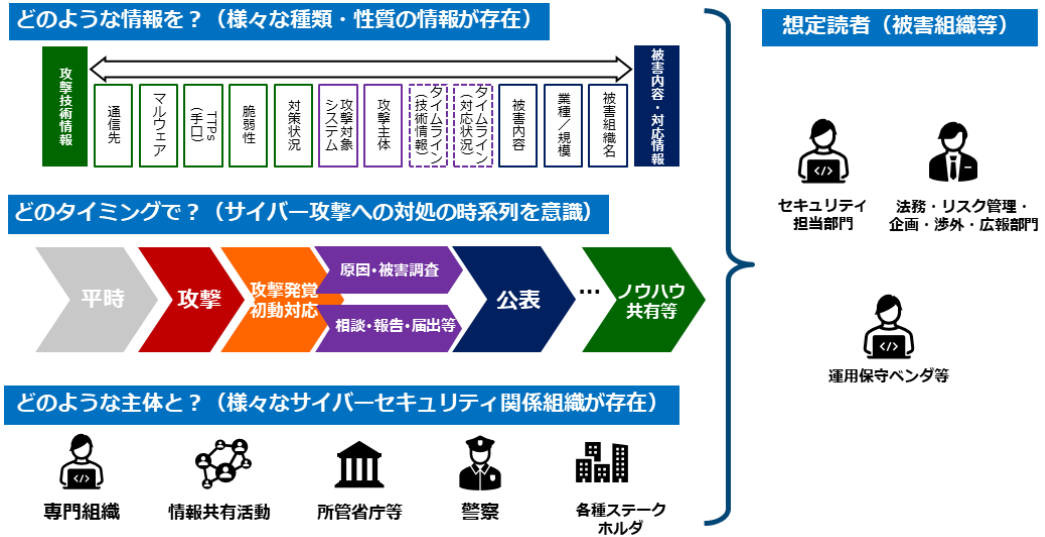


「サイバー攻撃被害に係る情報の共有・公表ガイダンス」

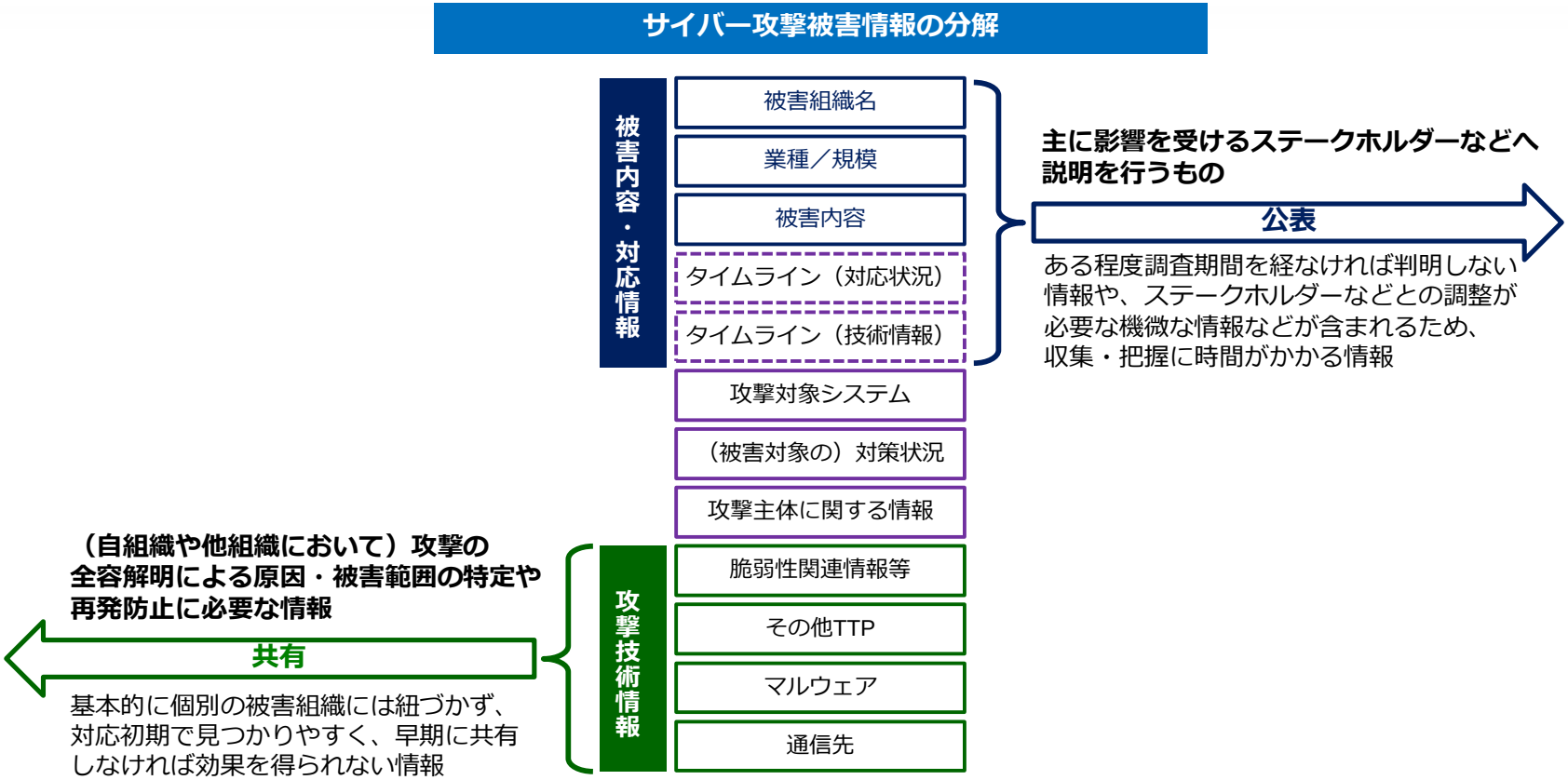


出典：内閣サイバーセキュリティセンター
「サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会」
https://www.nisc.go.jp/council/cs/kyogikai/guidancekentoukai.html

- 2022年5月から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



「サイバー攻撃被害情報」の定義

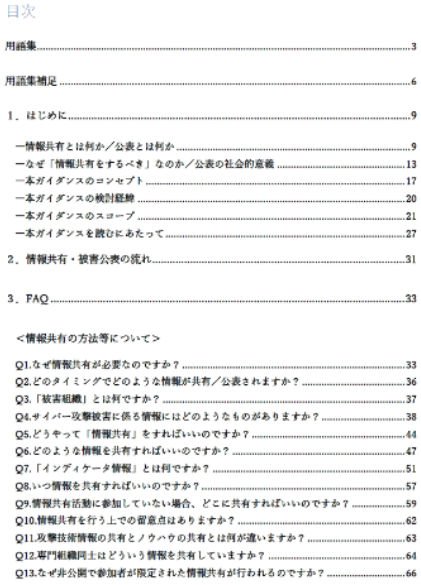


「共有・公表ガイダンス」の目次

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＞

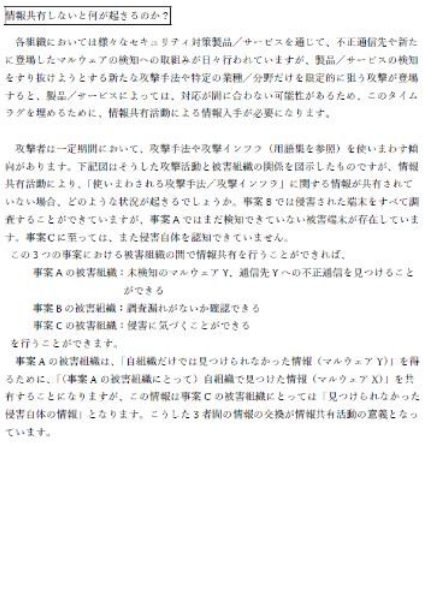
Q1. なぜ情報共有が必要なのですか？

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。

前者は被害組織固有の目的として、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、対応が個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。

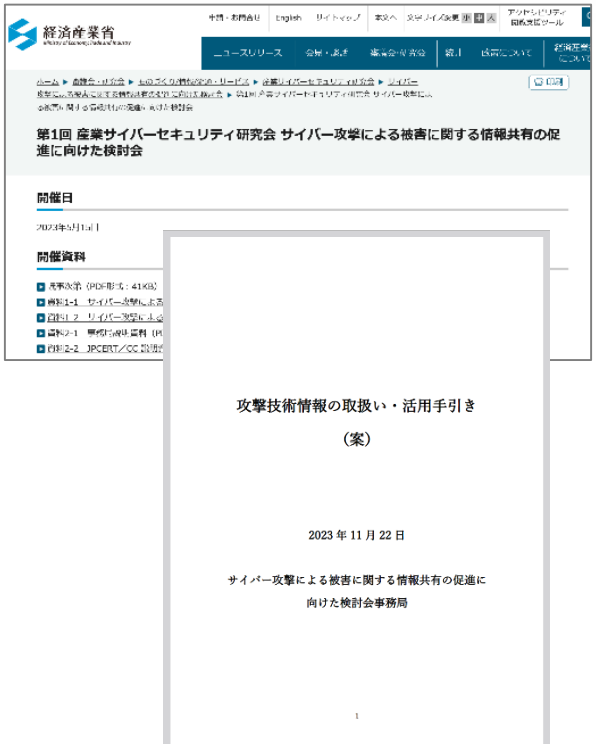
この３つの事案における被害組織の間で情報共有を行うことができれば、

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。

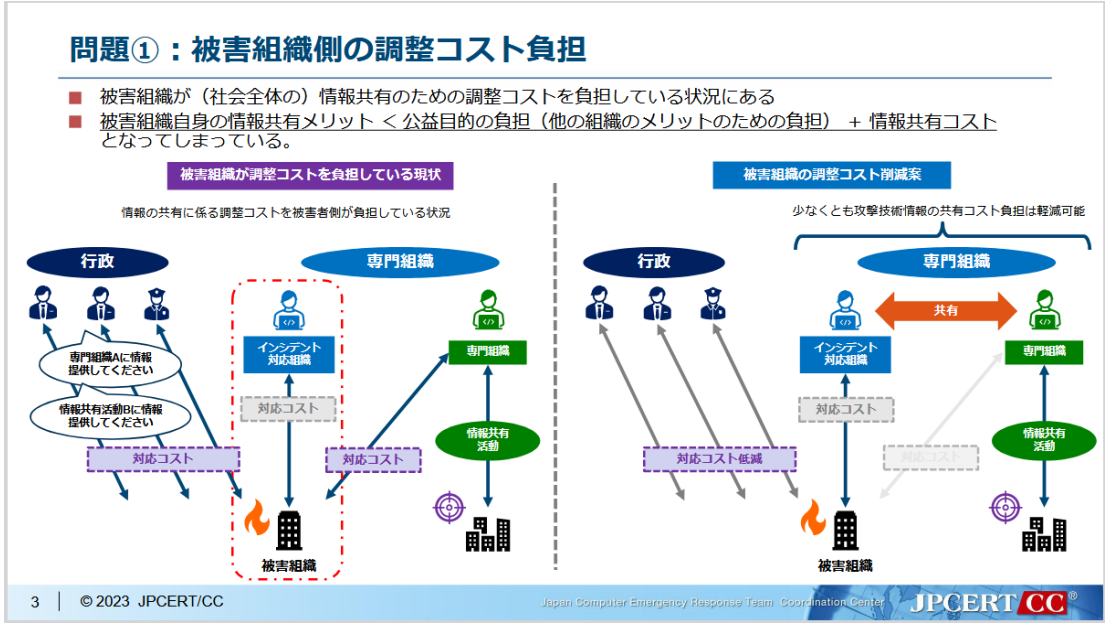
事案Ａの被害組織は、「自組織だけでは見つけられなかった情報（マルウェアＹ）」を得るために、「（事案Ａの被害組織にとって）自組織で見つけた情報（マルウェアＸ）」を共有することになりますが、この情報は事案Ｃの被害組織にとっては「見つけられなかった侵害自体の情報」となります。こうした３者間の情報の交換が情報共有活動の意義となっています。

「攻撃技術情報の取扱い・活用手引き」



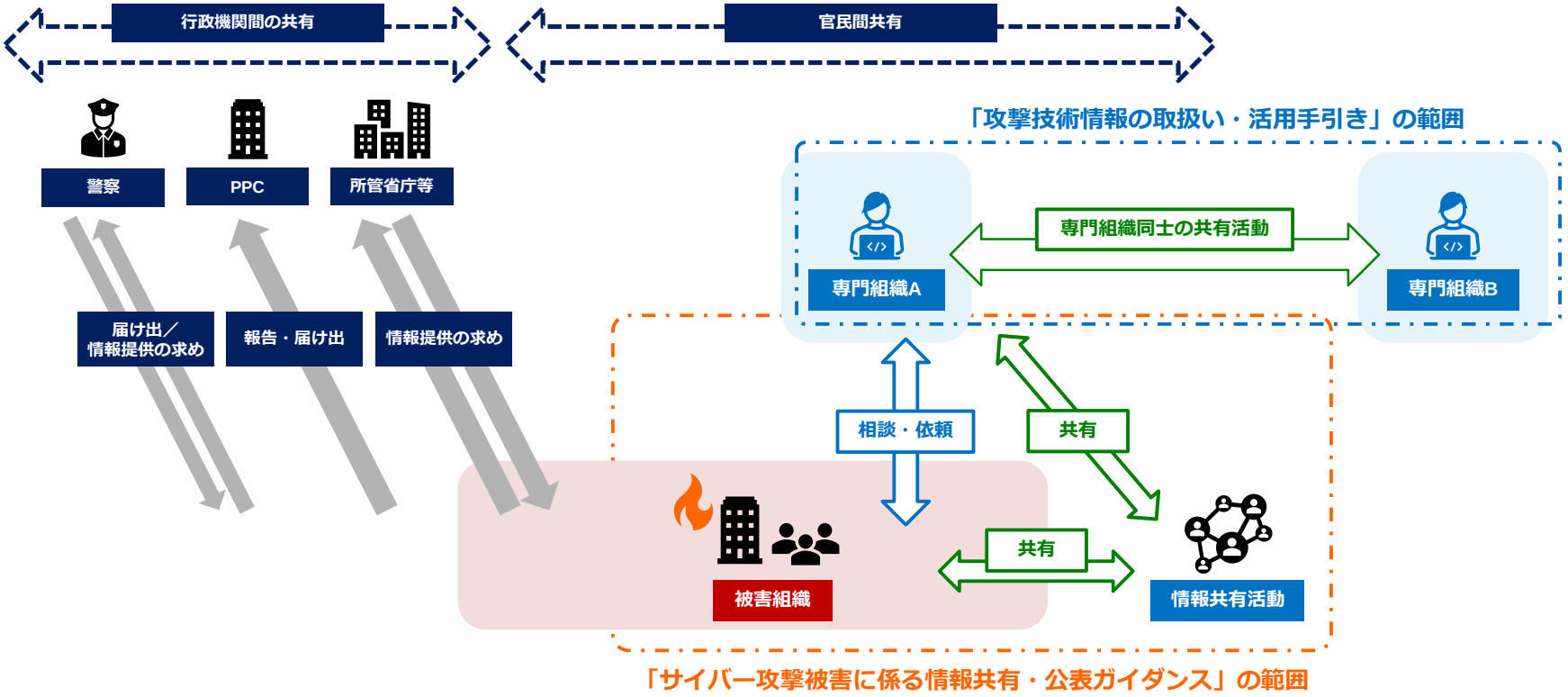
出典：経済産業省
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/cyber_attack/pdf/001_02_02.pdf

- 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
- 情報共有により、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）の知見が向上することで、被害組織のインシデント対応コストを減らすことが目的

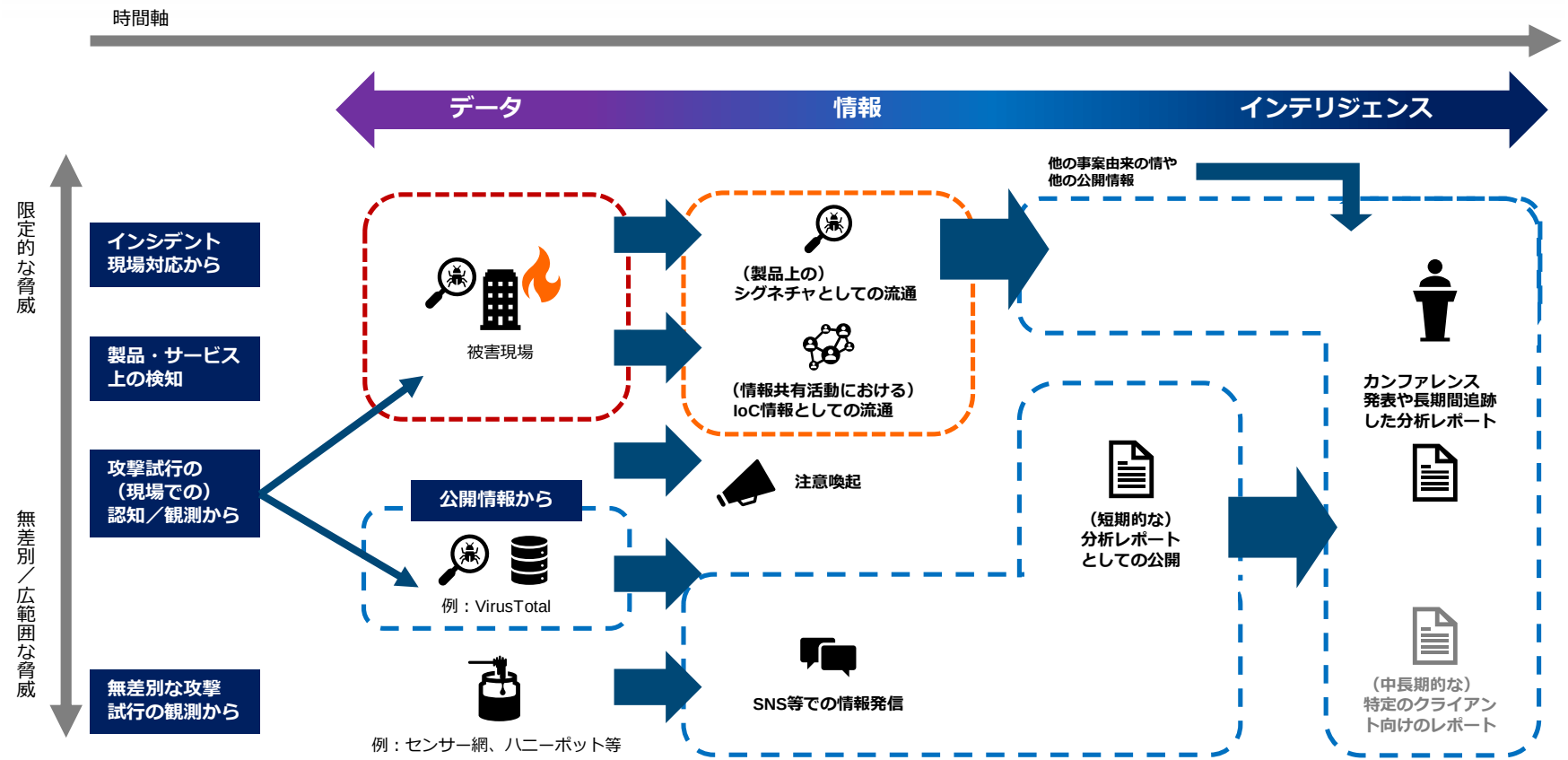


各ガイダンスのスコープ

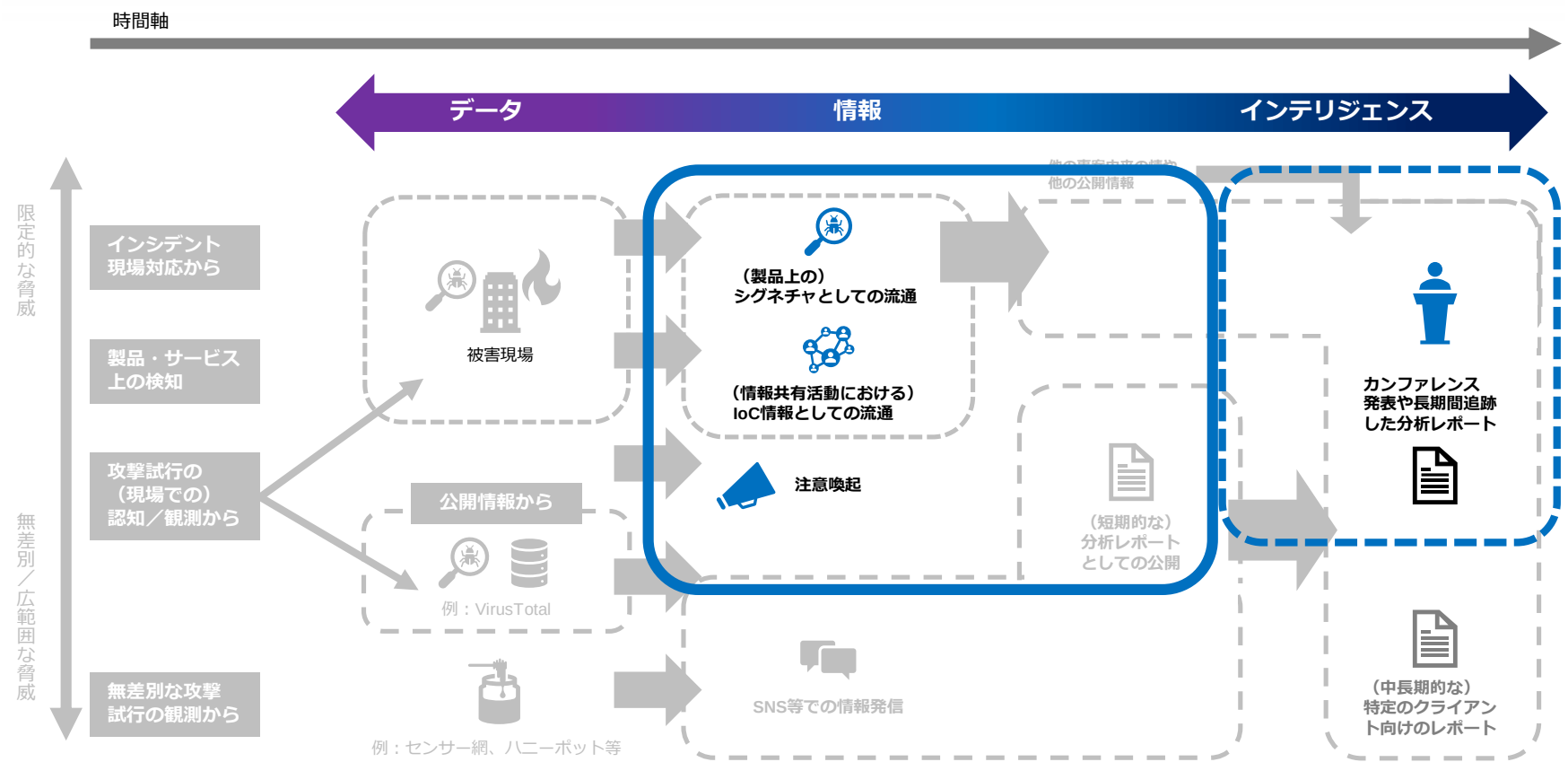
【用語に関する補足】
専門組織：専門機関やセキュリティベンダー（「サイバー攻撃被害に係る情報の共有・公表ガイダンス」における用語定義を準用）



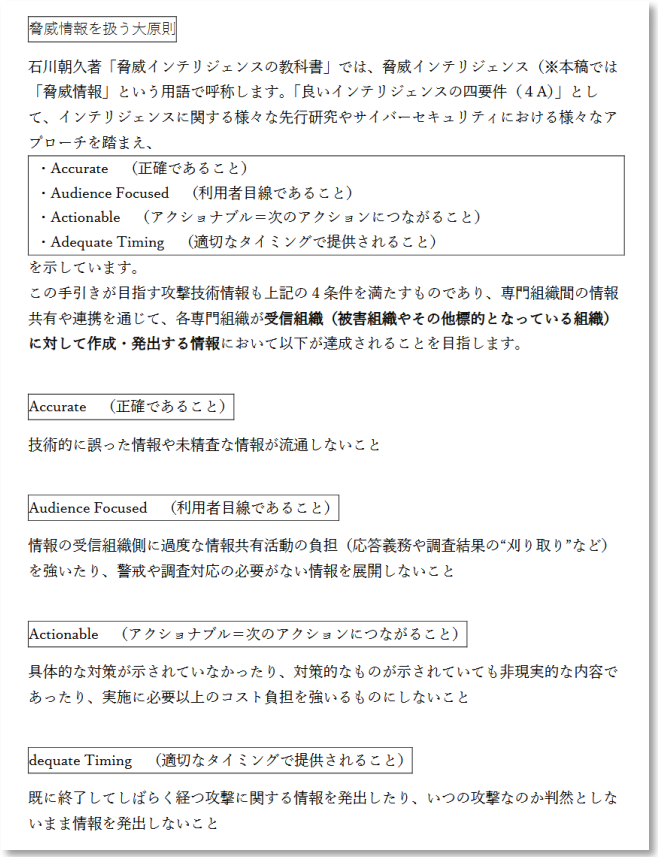
「脅威情報」はどこからやってくるのか



主に事案対応現場側が扱う脅威情報／タイミング



脅威情報を「出す」側の心構え・方法論



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

dequate 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

- 情報提供という「正しいこと」も「正しい方法」で行わなければ意味がない。むしろ、受信者側、被害組織側に不要な対応コストを強いてしまう

⇒「攻撃技術情報の取扱い・活用手引き」11ページほか

出典：経済産業省「攻撃技術情報の取扱い・活用手引き」
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/cyber_attack/pdf/20231122_3.pdf

注意喚起の例：脆弱性悪用に関するもの

Ivanti Connect SecureおよびIvanti Policy Secureの脆弱性（CVE-2023-46805およびCVE-2024-21887）に関する注意喚起

最終更新: 2024-02-14

X ポスト　メール

JPCERT-AT-2024-0002
JPCERT/CC
2024-01-11（公開）
2024-02-14（更新）

I. 概要

2024年1月10日（現地時間）、IvantiはIvanti Connect Secure（旧: Pulse Connect Secure）およびIvanti Policy Secureゲートウェイにおける脆弱性に関するアドバイザリを公開しました。認証バイパスの脆弱性（CVE-2023-46805）とコマンドインジェクションの脆弱性（CVE-2024-21887）が対象で、脆弱性が組み合わされて悪用されると、遠隔の第三者が認証不要で任意のコマンドを実行する可能性があります。

Ivantiは本脆弱性を悪用する攻撃を確認しており、JPCERT/CCは本脆弱性を悪用したとみられる攻撃が国内組織に対しても行われた可能性があることを確認しています。また、1月16日に本脆弱性を実証するコード（Proof-of-Concept）が公開されて以降、本脆弱性を悪用するさまざまな攻撃が発生しています。本脆弱性の影響を受ける製品を利用している場合、後述「III. 対策」以降に記載の情報およびIvantiが提供する最新の情報を確認の上、回避策の適用や侵害有無を確認する調査などを推奨します。

Ivanti
CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways
https://forums.ivanti.com/s/article/CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways

Ivanti
KB CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways
https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways

更新: 2024年2月14日追記

2024年1月31日（現地時間）以降に公開された脆弱性の内容を参考に、「III. 対策」「IV. 回避策」の記載を修正しました。Ivantiが提供する最新の情報を確認の上、最新のパッチの適用や回避策の適用を検討してください。

II. 対象

本脆弱性の対象となる製品は次のとおりです。

- Ivanti Connect Secure
- Ivanti Policy Secure

サポート対象の22系や9系のバージョンが影響を受けるとのことです。すでにサポートが終了しているバージョンにおける影響は評価されておらず、Ivantiはリポート対象のバージョンへの移行を推奨しています。リポート対象バージョンの最新の状況はIvantiの次の情報をご確認ください。

Ivanti
Granular Software Release EOL Timelines and Support Matrix
https://forums.ivanti.com/s/article/Granular-Software-Release-EOL-Timelines-and-Support-Matrix

III. 対策

Ivantiが提供する最新の情報を確認の上、最新のパッチの適用や回避策の適用を検討してください。

2024年1月31日（現地時間）、Ivantiは権限昇格の脆弱性（CVE-2024-21888）およびSSRFの脆弱性（CVE-2024-21893）を含め、本脆弱性を修正するパッチを公開しました。その後、2024年2月8日（現地時間）、Ivantiは同製品におけるXML外部実体参照（XXE）の脆弱性（CVE-2024-22024）に関するアドバイザリを公開しました。1月31日に公開された修正パッチを適用したバージョンが影響を受けますが、1月31日に公開された回避策を適用している場合は脆弱性の影響を受けないとのことです。

Ivanti
CVE-2024-21888 Privilege Escalation for Ivanti Connect Secure and Ivanti Policy Secure
https://forums.ivanti.com/s/article/CVE-2024-21888-Privilege-Escalation-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure

Ivanti
CVE-2024-22024 (XXE) for Ivanti Connect Secure and Ivanti Policy Secure
https://forums.ivanti.com/s/article/CVE-2024-22024-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure

IV. 回避策

2024年1月10日（現地時間）、本脆弱性の影響を緩和する回避策として、XMLファイルをインポートする方法をIvantiが案内しています。ファイルや適用方法に関する情報は該当向けのポータルで提供されています。

2024年1月31日（現地時間）、Ivantiは権限昇格の脆弱性（CVE-2024-21888）およびSSRFの脆弱性（CVE-2024-21893）の影響を緩和する新たな回避策となるxmlファイルを公開しています。Ivantiが提供する最新の情報をご確認の上、すぐに対策を適用できない場合は影響を緩和するため、回避策の適用をご検討ください。

V. 侵害検出方法

脆弱性を悪用されて機器が侵害された可能性を調べる方法や、侵害が疑われる場合の対処および復旧方法については、Ivantiが提供するアドバイザリなどの最新の情報をご確認ください。

https://www.jpcert.or.jp/at/2024/at240002.html

インディケータ情報の例（IoC：Indicator of compromise）

（参照：共有・公表ガイダンスQ7（51ページ～））

****

情報の共有範囲

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

****

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

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

1）攻撃が行われた期間

202x 年 x 月以降

2）攻撃の特徴

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

[メールの件名]

（※メールの件名を記載）

3）攻撃に使用された検体

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

ファイル名：（※実際のファイル名）.zip

File Type ：

MD5 ：

SHA-1 ：

SHA-256 ：

ファイル名：（※実際のファイル名）.lnk

File Type ：

MD5 ：

SHA-1 ：

SHA-256 ：

4）攻撃に使用された通信先

[メールの文中に掲載される URL のドメイン]

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

[lnk ファイルの通信先]

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

※安全のため通信先の一部を、[.] に置き換えています。

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

・JPCERT/CC Eyes

〇〇〇に感染させるショートカットファイルを用いた攻撃

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

（以下略）

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

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

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

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

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

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

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

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

図 36

注意喚起とIoCを組み合わせた例：攻撃キャンペーンに関するもの

- 過去（数カ月前）から現在までの複数の攻撃キャンペーン（の継続）に関するもの
- 予防効果だけでなく、被害をまだ認知できていない組織における事案の認知のためと攻撃活動への牽制を狙ったもの

日本の組織を標的にした外部からアクセス可能なIT資産を狙う複数の標的型サイバー攻撃活動に関する注意喚起

最終更新: 2023-11-16

X ポスト　メール

JPCERT-AT-2023-0029
JPCERT/CC
2023-11-16

公開: 2023年11月16日

複数の被害組織での調査や攻撃活動の追跡が並行して行われており、今後、記載したもの以外の製品の脆弱性や通信先等のインディケータ情報を追記、更新する見込みですので、今後の情報更新もご確認ください。

I. 概要

JPCERT/CCは、2022年5月以降におけるArray Networks Array AGシリーズの脆弱性を悪用する標的型サイバー攻撃に対する侵害調査を進めてきました。

Array Networks Array AGシリーズの脆弱性を悪用する複数の標的型サイバー攻撃活動に関する注意喚起
https://www.jpcert.or.jp/at/2023/at230020.html

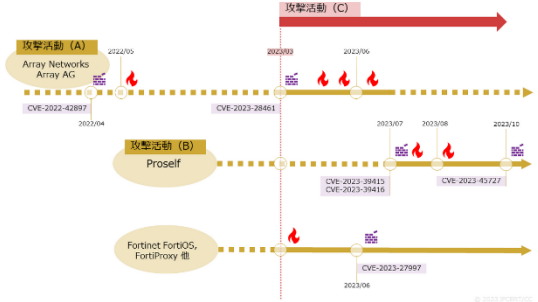
JPCERT/CCでは注意喚起に対するフィードバックや、サイバーセキュリティ協議会の活動を通じて、注意喚起に掲載した攻撃活動に関連すると考えられる活動を認識しました。「II. 攻撃活動の概要」の概要やインディケータ情報をもとに、侵害調査や、「III. 対象および対策」をもとに悪用が確認されている脆弱性への対応等の対策を進めることを推奨します。

II. 攻撃活動の概要

https://www.jpcert.or.jp/at/2023/at230029.html

攻撃時期：2023年3月以降
インディケータ情報：不正アクセス元のIPアドレス
- 154[.]31[.]112[.]129
- 173[.]249[.]201[.]243
- 35[.]229[.]146[.]251
- 45[.]32[.]49[.]130
- 45[.]32[.]252[.]239
- 45[.]66[.]217[.]106
- 45[.]32[.]33[.]120
- 95[.]85[.]91[.]15
- 139[.]162[.]127[.]90
- 167[.]71[.]207[.]51
- 176[.]97[.]70[.]81
- 194[.]102[.]36[.]128

インディケータ情報：ネットワーク内部からの接続先IPアドレス
- 45[.]66[.]217[.]106
- 95[.]85[.]91[.]15
- 207[.]148[.]97[.]235
- 45[.]77[.]12[.]212



分析レポートの例：攻撃手法／マルウェアの技術的解析

- 注意喚起目的で行われるものは少数であり、もっぱら、アナリストの成果・情報共有として、また、企業のPRとして行われる

JPCERT CC

JPCERT/CC Eyes

Top > "インシデント"の一覧 > 日本の組織を狙った攻撃グループLazarusによる攻撃オペレーション

園部 勇誠 (Shusei Tomonaga) 2021/03/22

日本の組織を狙った攻撃グループLazarusによる攻撃オペレーション

Lazarus

メール

これまでJPCERT/CC Eyesでは、攻撃グループLazarus（Hidden Cobraとも呼ばれる）が攻撃時に使用するマルウェアやツール名、被害に関わる[illegible]が、この攻撃グループによる攻撃オペレーションは[illegible]。今回は、[illegible]。なお、[illegible]。

VSingleの概要

VSingleは、リモートからPEのコードを実行する機能を持ったHTTPボットです。このマルウェアは、その後にプラグインをダウンロードして実行する機能なども持っています。
このマルウェアは[illegible]、Explorerを実行し、[illegible]をインジェクションしようとして、実行します（DLLインジェクションを行わない検体も確認されています）。なお、メインコードの[illegible]。

[illegible]

以降では、VSingleの文字列難読化、通信方式および機能について記述します。

VSingleの文字列難読化

VSingleは、検体内で使用する文字列の多くを暗号化しています。例1は、文字列暗号化を解除するコードです。元の[illegible]を使用して、XORや[illegible]。

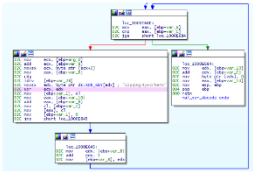


図2にプラグインを実行するコードの一部を示します。

```
65  LODWORD(v12) = 255;
66  memset(&v24, 0, v12);
67  switch ( HIBYTE(word_10088AC4) )
68  {
69    case 0u:
70      tmp = mal_xor_decode(enc_string_10072DE0);// .tmp
71      mal_generate_temp_filename(&FileName, (int)tmp);
72      flag_create_file = 1;
73      break;
74    case 1u:
75      lpAddress = VirtualAlloc(0, dwSize, 0x1000u, 0x40u);
76      LODWORD(v13) = a1 - 18;
77      memmove_0(lpAddress, Buffer, v13);
78      ((void (*)(void))lpAddress)();
79      VirtualFree(lpAddress, dwSize, 0x8000u);
80      break;
81    case 2u:
82      lpAddressa = VirtualAlloc(0, dwSize, 0x1000u, 0x40u);
83      LODWORD(v13) = a1 - 18;
84      memmove_0(lpAddressa, Buffer, v13);
85      ((void (*)(void))lpAddressa)();
86      break;
87    case 3u:
88      vbs = mal_xor_decode(enc_string_10072DEC);// .vbs
89      mal_generate_temp_filename(&FileName, (int)vbs);
90      flag_create_file = 1;
91      break;
92    case 5u:
93      bat = mal_xor_decode(enc_string_10072DF8);// .bat
94      mal_generate_temp_filename(&FileName, (int)bat);
95      flag_create_file = 1;
96      break;
97    default:
98      break;
99  }
100 if ( flag_create_file )
101 {
102   mal_sleep(30);
103   fopen_s(&Stream, &FileName, "a+b");
```

図2: VSingleのプラグインを実行するコードの一部

シェルコード形式のプラグインに関しては、メモリ上で展開し、実行されます。それ以外のプラグインは、%TEMP%フォルダーに一時的に保存されて実行されます。なお、シェルコード形式のプラグインに関しても、一時ファイルとして%TEMP%フォルダーに保存されます。
マルウェア情報送信コマンド（コマンド番号6）の際には、図3のような情報が送信されます。バージョン情報には、1.0.1以外にも4.1.1や3.0.1などが使用された検体も確認しており、マルウェアのバージョンではなく、何らかの検体識別子の可能性があります。

```
1  Version: 1.0.1
2  Loggedon User: test-user
3  Stub Path:
4  Persistence Mode:
5  Persistence name:
6  Mutex Name: sonatelr
```

図3: マルウェア情報送信コマンドで送信される情報の例

Appendix B: 通信先

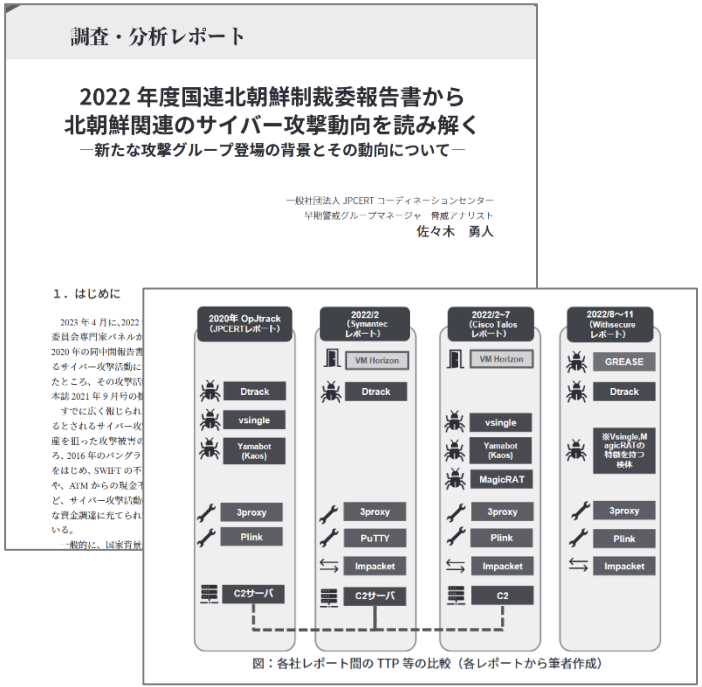
- http://aquagoat.com/customer
- http://blacktiger.com/input
- http://bluedog.com/submit
- http://coraltiger.com/search
- http://goldtiger.com/find
- http://greentiger.com/submit
- http://industryarticleboard.com/evolution
- http://industryarticleboard.com/view
- http://maturicafe.com/main
- http://purplefrog.com/remove
- http://whitedragon.com/search
- https://coralcameleon.com/register
- https://industryarticleboard.com/article
- https://maturicafe.com/polo
- https://salmonrabbit.com/login
- https://whitecameleon.com/find
- https://whiterabbit.com/input
- http://toysbagonline.com/reviews
- http://purewatertokyo.com/list
- http://pinkgoat.com/input
- http://yellowlion.com/remove
- http://salmonrabbit.com/find
- http://bluecow.com/input
- http://www.karin-store.com/data/config/total_manager.php
- http://katawaku.jp/bbs/data/group/group-manager.php
- http://3.90.97.16/doc/total.php

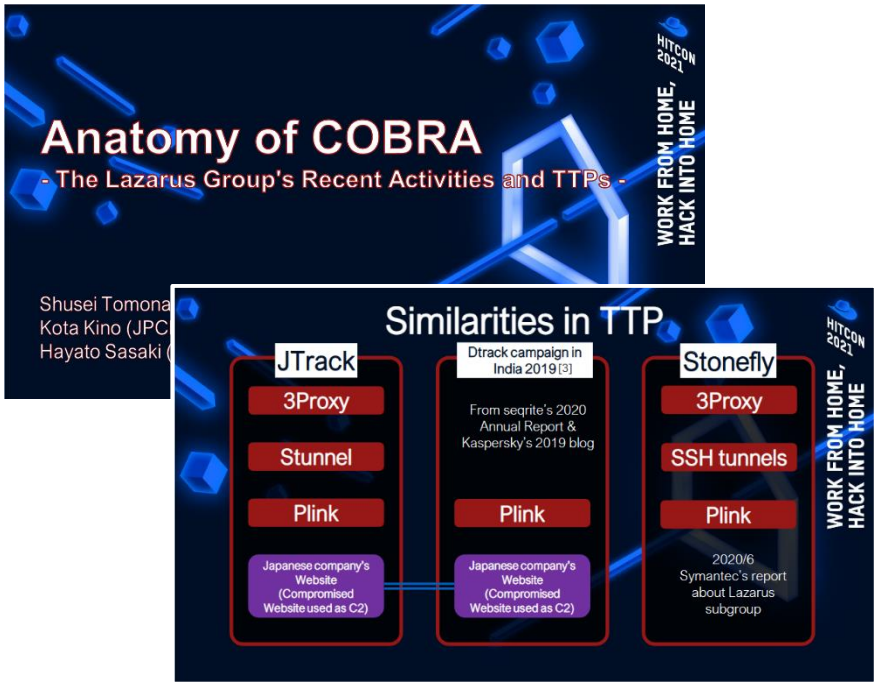
Appendix C: マルウェアのハッシュ値

- 487c1bdb65634a794fa5e359c383c94945ce9f0806fcad46440e919ba0e6166e
- eb846bb491bea698b99eab80d58fd1f2530b0c1ee5588f7ea02ce0ce209ddb60

分析レポートの例：ソフトなアトリビューションを含むもの

- 対応した事案（非公開）の分析結果＋公開情報の分析から、攻撃グループの特定まで行うもの



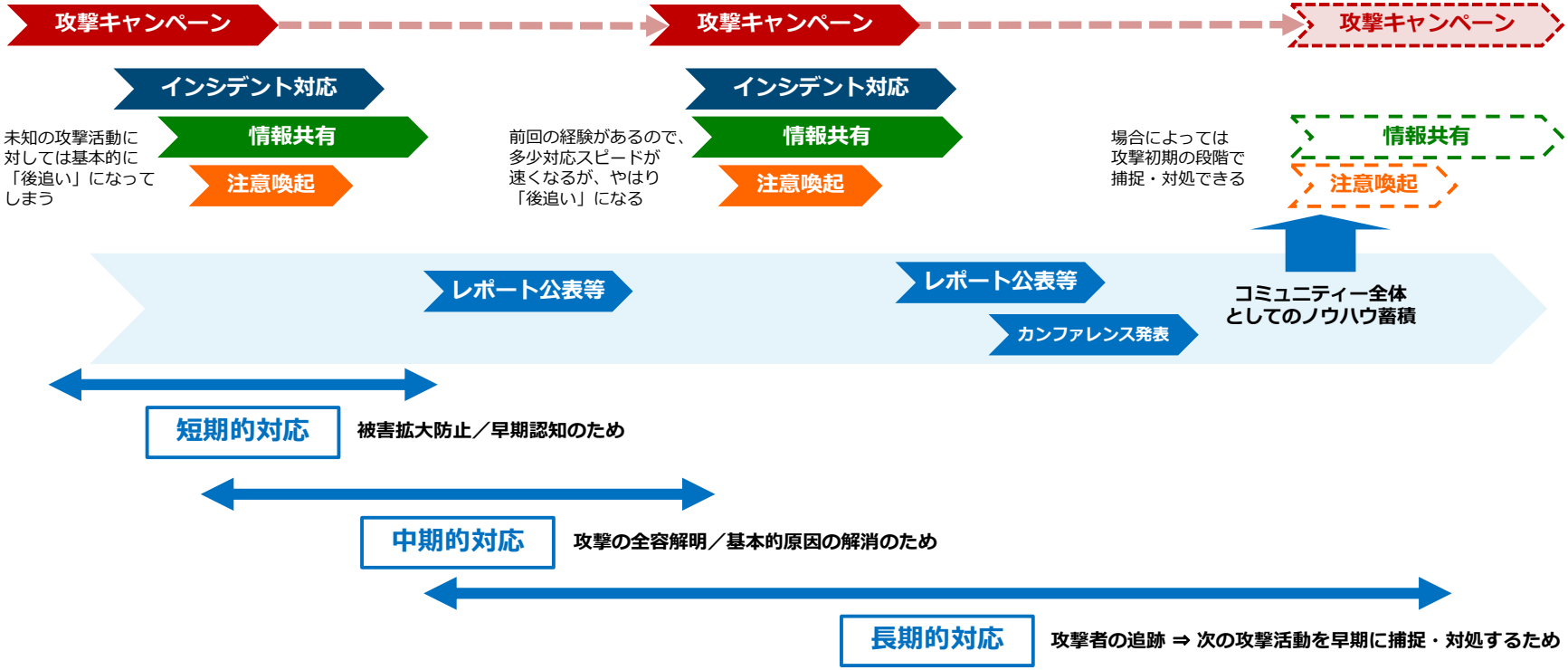


出典：安全保障貿易情報センター「CISTECジャーナル2023年5月号」調査・分析レポート
佐々木勇人「2022年度国連北朝鮮制裁委報告書から北朝鮮関連のサイバー攻撃動向を読み解く―新たな攻撃グループの登場の背景とその動向について―」

https://github.com/JPCERTCC/Lazarus-research/blob/main/slides/HITCON2021_Anatomy-of-COBRA.pdf

参考：専門組織はなぜアトリビューションを含めた分析を行うのか

- 基本的には便宜上、特定グループを明示的に追跡し続ける必要性・効果があるから



参考：（パブリック）アトリビューションの「粒度」

- 「粒度」の異なるさまざまなアトリビューションと公表が行われている
- “ソフト”なアトリビューション：バーチャネルな「攻撃グループ」の分類 ← セキュリティアナリストが行っているもの
- “ハード”なアトリビューション：実行犯／背景主体の特定 ← 行政機関等で行っているもの

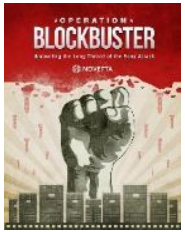
背後関係（所属組織、政府）まで特定しているもの

実行犯（人物）特定まで至っているもの

「攻撃グループ」特定（＋関係のある国／地域）

Sandworm

・ロシアのAPTグループと推測・特定されている
・2020/10にGRU要員の刑事訴追を公表



Lazarus

・北朝鮮のAPTグループと推測・特定されている
・2018/9、2021/2に関係者の刑事訴追を公表

APT1

・中国のAPTグループと推測・特定されている
・2013/1にマンディアント社が実行者まで特定
・2014/5に米司法省が刑事訴追を公表

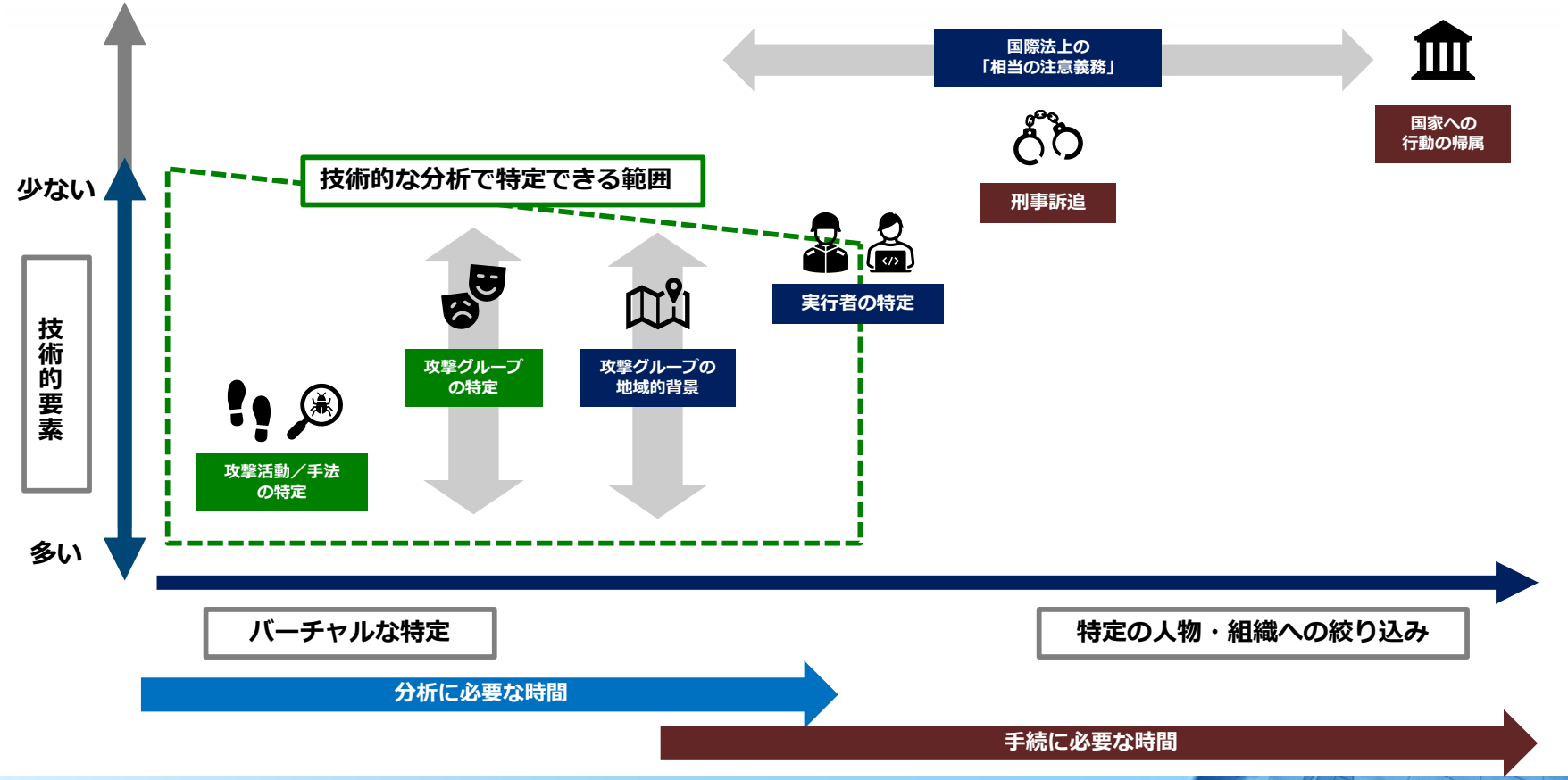
Kimsuky

・北朝鮮のAPTグループと推測されている
・標的が主に韓国
・これまでに実行犯個人の特定や、背後関係（どの組織に所属しているか）は明らかになっていない

SideCopy

・パキスタンのAPTグループと推測されている
・標的がインド、アフガニスタンの組織
・「パキスタン」を明示するセキュリティベンダーもいれば、明示しないベンダーも

参考：アトリビューションの全体像



基本的にその多くは「後追い」情報であるということ

- APTほか、情報共有すべき脅威ほど、基本的には「過去の攻撃」に関する情報を後追いで入手しているに過ぎないケースが多い（※なぜ、APT事案等では「後追い」にならざるを得ないのかについては本稿での解説は省略）

広範囲／無差別な攻撃のケース

PoC、攻撃（試行）元情報、攻撃時のログ等
⇒ **現在の情報**。いち早く共有できれば攻撃予防・被害拡大防止効果が見込める

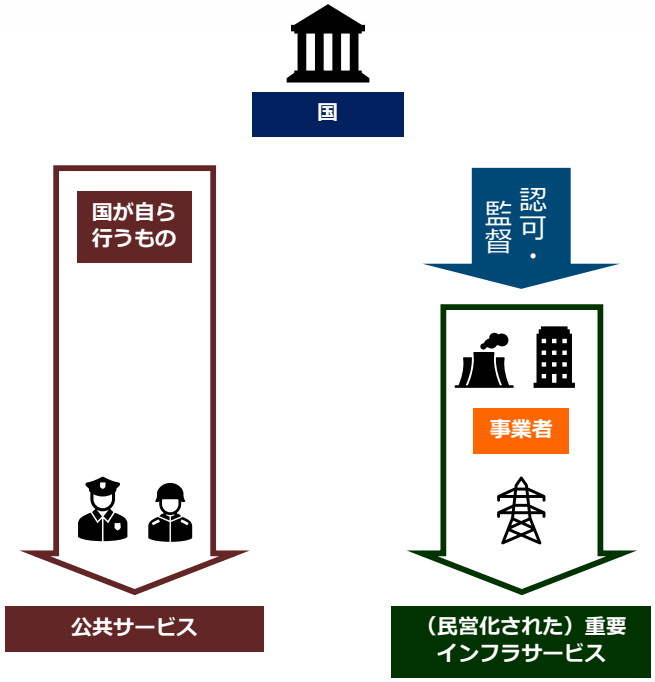
APT等、限定的範囲を狙うケース

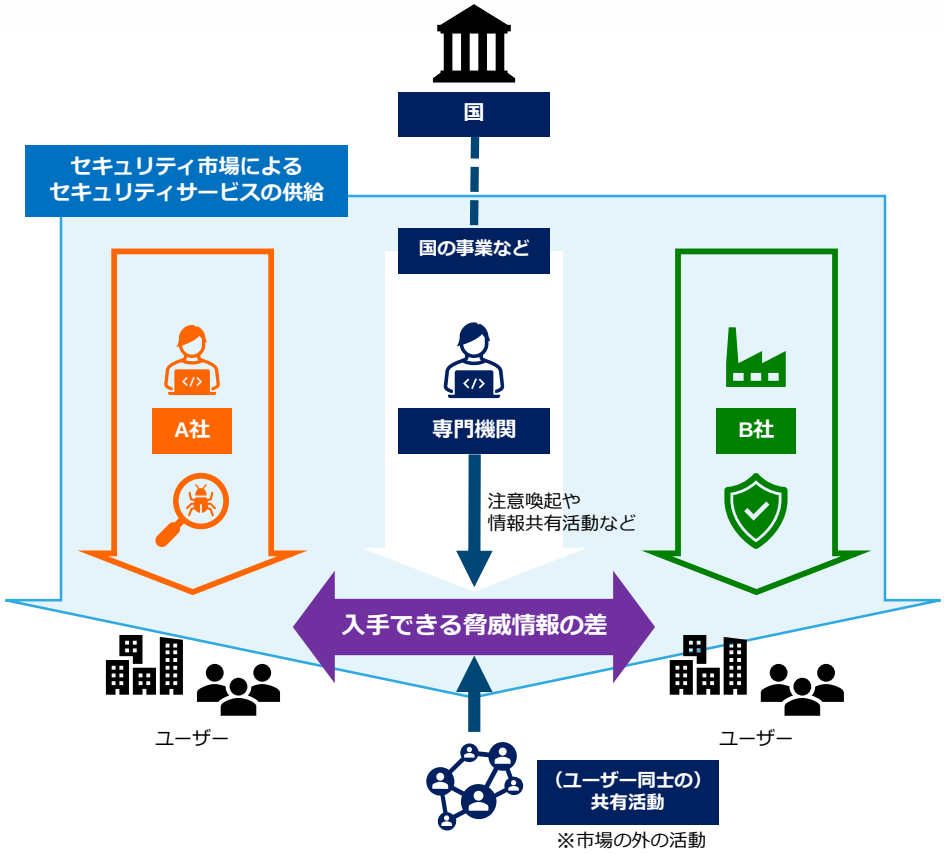
通信先、マルウェア情報等
⇒ **過去の情報**。基本的に共有の目的は
被害の“掘り起こし”と全容解明のため

スピアフィッシングメール等
⇒ いち早く共有できれば攻撃予防・被害拡大
防止　効果が見込める

脅威情報の「情報共有」の観点から

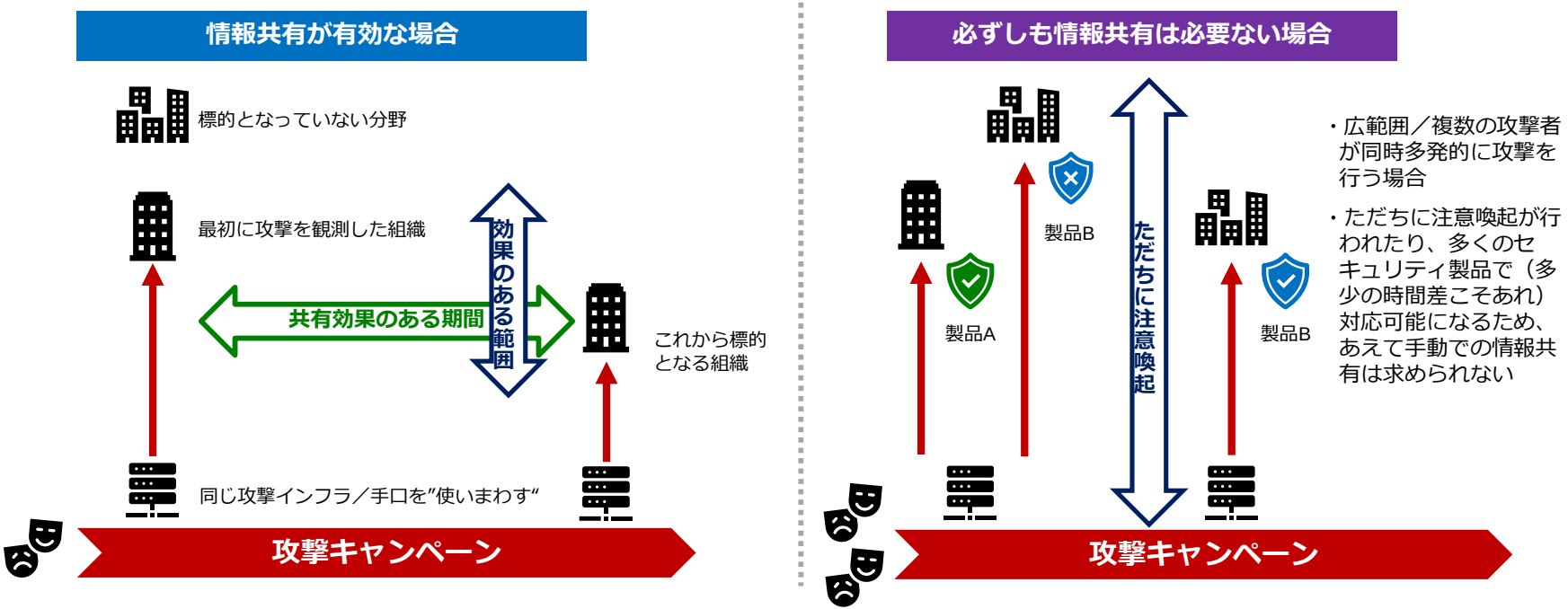
セキュリティサービスの“市場の失敗”の是正措置としての情報共有





必ずしも共有に適さない情報も多い

- 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）



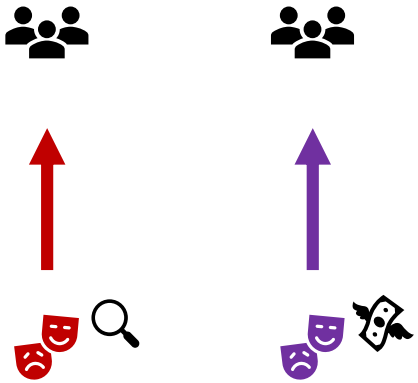
情報共有活動参加組織間のミスマッチ

- 共有活動の設計段階から構造的問題を組み込んでしまうケースが多い
- 業界単位、業界横断、国内に限らず、海外との情報共有活動でも同じ問題がある（次項参照）

被害／標的組織同士の共有

・被害組織／標的組織がそれぞれ主に得たい情報／攻撃類型が異なっている

・被害組織／標的組織がそれぞれ狙われている攻撃類型が大きく異なっている



専門組織ー被害／標的組織間の共有

・立場／役割が大きく異なる組織が同じ枠内に参加してしまっている

・それぞれが必要／関心事項とする情報の種類や内容、タイミングにズレがある

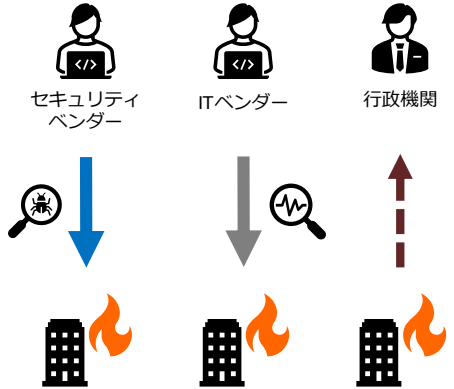
・ハッシュ値
・通信先情報
・ファイルパス
・構造・アルゴリズム
・他のマルウェア、過去のマルウェアとの共通点、変更点
・今後拡張される可能性のある機能

・ハッシュ値
・通信先情報
・ファイルパス
・構造・アルゴリズム
・他のマルウェア、過去のマルウェアとの共通点、変更点
・今後拡張される可能性のある機能

専門組織等同士の共有

・知見／技術レベルが異なる参加組織が混在している

・扱っている情報の種類／粒度が異なっている

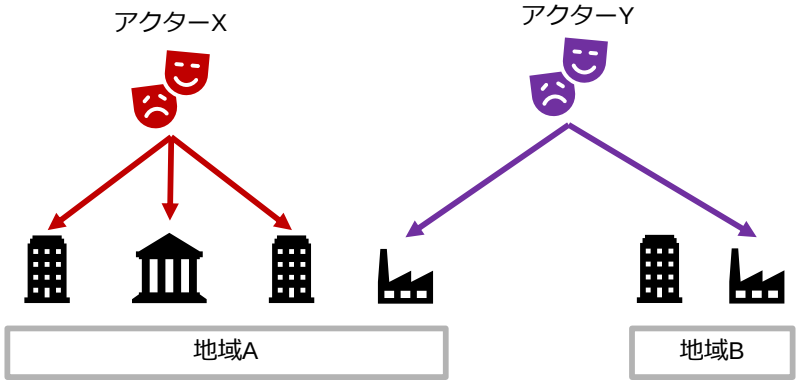


海外組織との共有活動はなぜそこまで振るわないのか

■ 海外組織と共有が必須なケースはそこまで多くはない
（※テイクダウン等の各種コーディネーション依頼を除く）

APTの場合

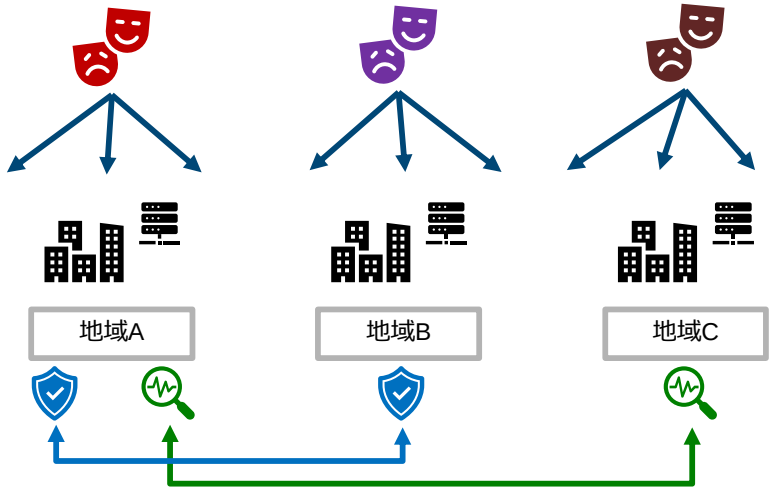
・特定地域を集中的に狙うアクターが多い。サプライチェーン攻撃を行う場合は地域に関係なく広範囲を狙うケースがある（例：CCleaner事案）
・同じAPTグループに区分していても、攻撃インフラや手口が必ずしも地域間で一致しない場合もある（例：APT10とOperation Cloud Hopper）



アクターXは特定地域を狙うため、地域間で情報共有をしてもほとんど効果はない
アクターYについては特定業種を狙い地域横断的に活動するため情報共有効果がある

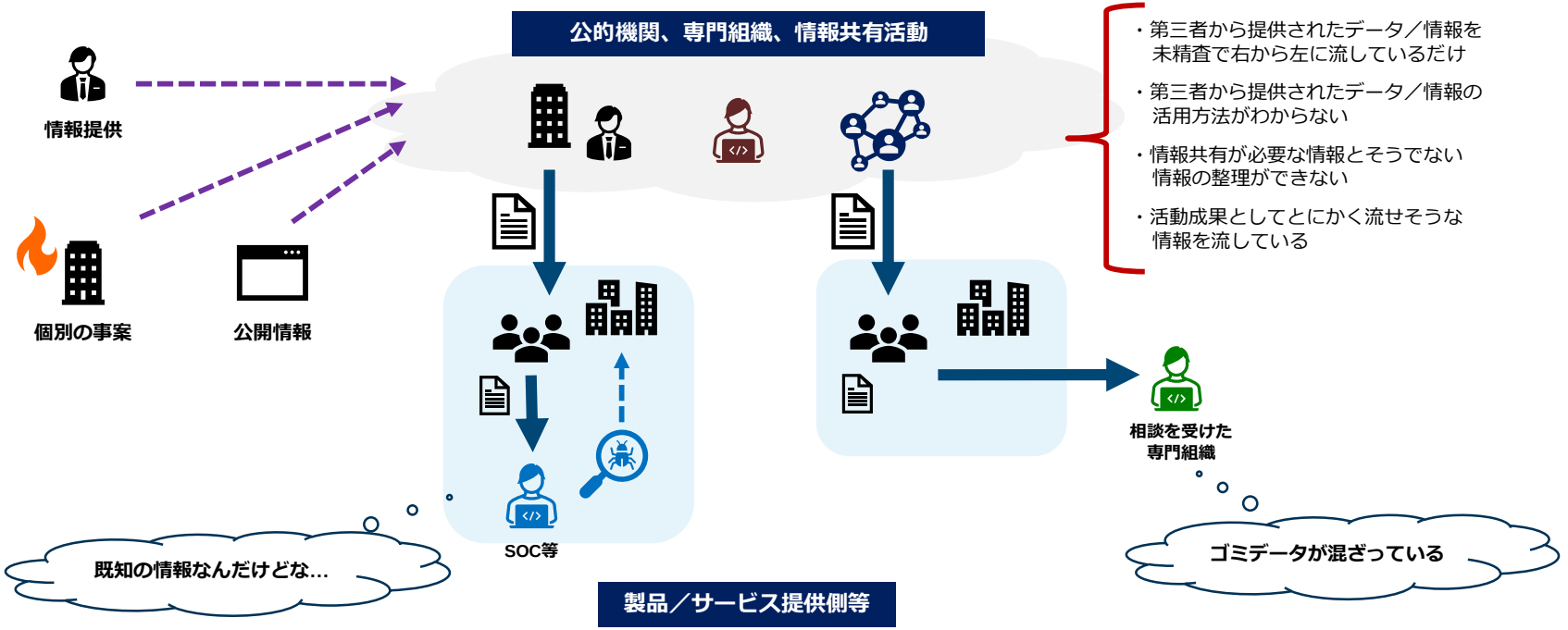
広範囲を狙う攻撃の場合

・（ゼロデイ含む）脆弱性を狙い特定製品を広範囲で狙う攻撃などは、世界中でほぼ同時多発的に観測される
・情報共有するよりも、各商用製品上の情報流通や公開情報での情報拡散の方が早いケースが多い



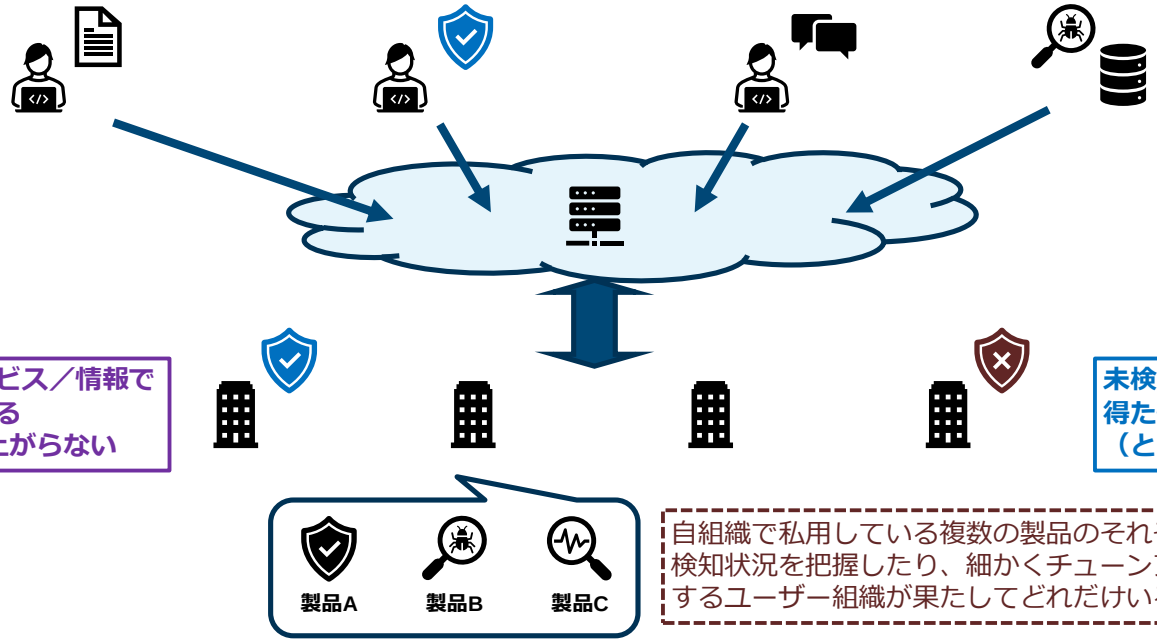
情報共有が“空回り”しているケース

- 本来、「必ずしも情報共有活動に流さなくてもよい情報」や未精査な情報が流れることによる「対応コスト」が発生してしまっているもの（セキュリティ製品／サービス側で対応できている状況を情報発信側が把握できていない）
- 情報を「流すこと」が自己目的化してしまっている



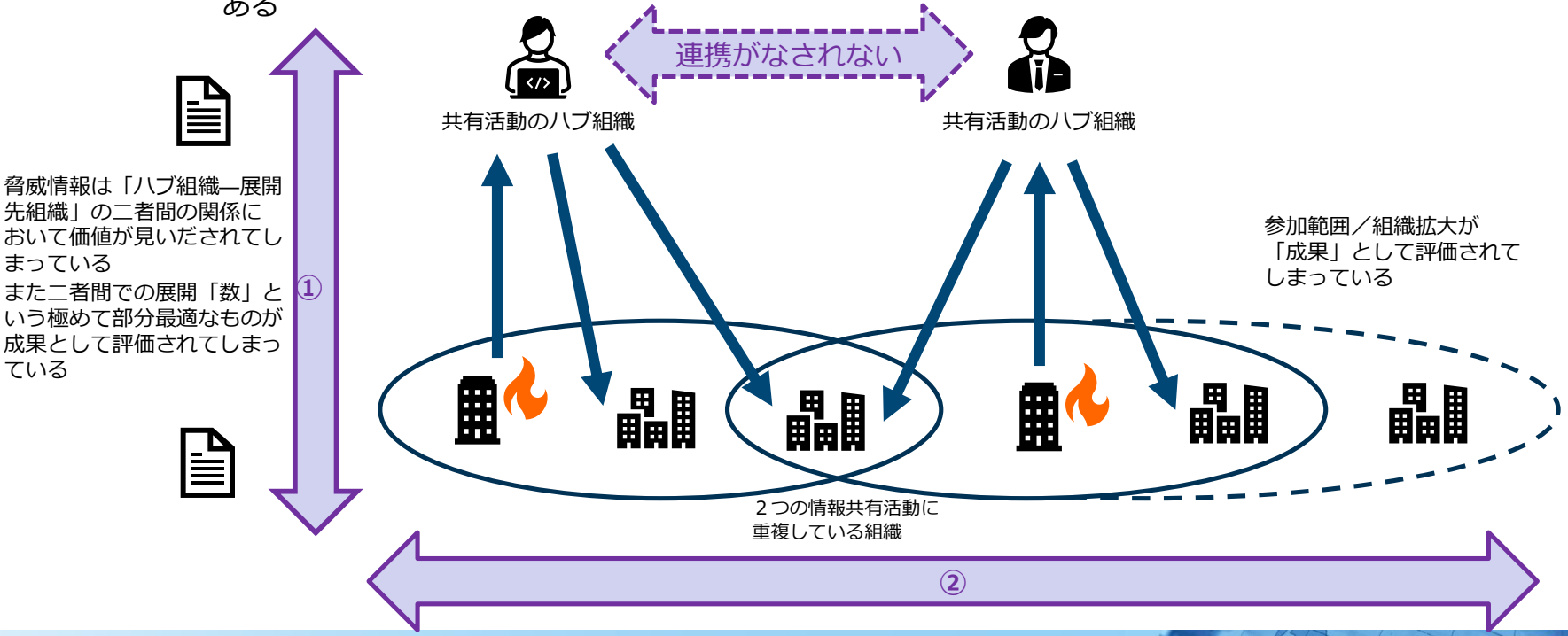
自動化は必要なのか？

- 複数ソースの情報を“自動化”で集めるということ ⇒ 情報源間で共有・調整していないため、既知・未知の情報の重複やノイズ情報などが混在することになる
- 「自動化するためのコスト」が発生しているため、自動化は情報の配信元（調整役）も受信側も高度な知見・リソースがあって初めて成立する仕組みである



情報共有「活動」自体の失敗

- ジレンマ①：情報共有ハブ組織にとって共有情報（脅威情報）は展開先組織（情報共有活動参加組織）との関係において価値が見いだされてしまっているので、部分最適＝自身が受け持つ範囲にしか情報を展開しない
- ジレンマ②：果てしなく巨大な活動体組むことは困難であり、また、分野横断共有活動自身のジレンマ（前述）がある

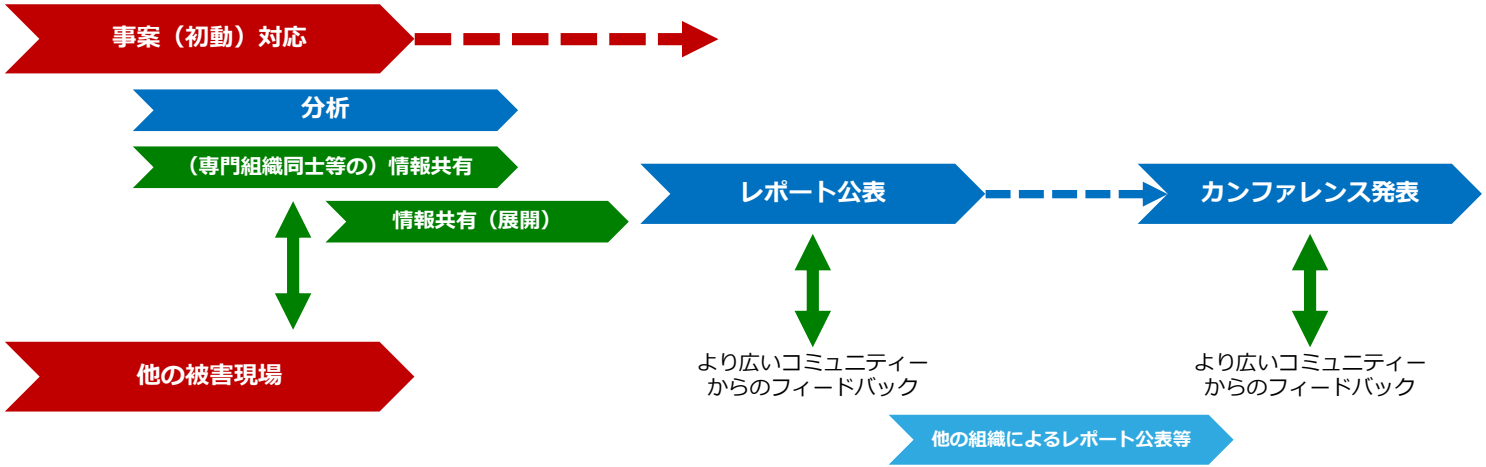


脅威情報の「提供」の観点から

専門組織の情報サイクル

- かつては情報の囲い込みや、成果としてPRするための”利己的”な情報開示が多かったが（部分最適な情報の消費）、専門家コミュニティーにおける活動の積み重ねにより、全体最適な情報の流通が行われるようになってきている
- 事案対応⇒分析⇒共有／サービス上での展開⇒レポート公表⇒カンファレンス発表、という一連のサイクルの中に、現状としては、「情報消費者／カスタマーとしての国」への情報提供がほどんと登場しない

セキュリティ専門組織の情報サイクル



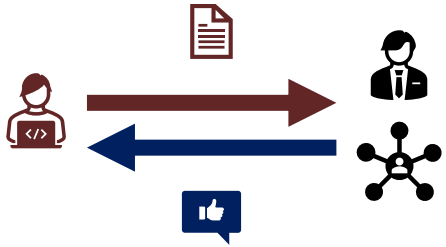
国へ“情報提供”されるケース

- 当該情報を適切／効率的に活用できる専門機関や行政機関への情報提供／届け出とは別に、国に自主的に（国内外から）セキュリティベンダーやITベンダー、研究者等から情報提供されるケースにおいては、問題が多い
- 提供者、受領側、双方に悪意や不作為があるわけではないが、情報共有としては適切／効果的ではない

アピールのため①

・国が主導する情報共有スキームに対して、企業としてPRのために行われる情報提供

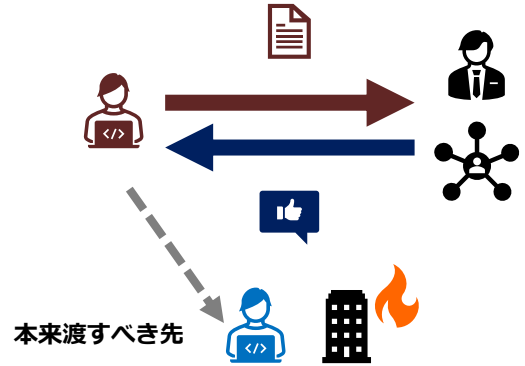
・レポートとして公開する前の事前提供などが多い（右記の「アリバイのため」とほぼ同様）



アピールのため②

・研究者、”リサーチャー“などが活動“成果”として提供するもの

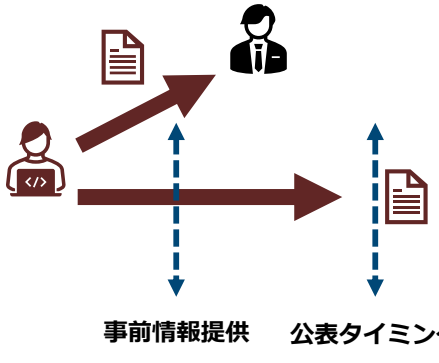
・本来は、専門機関や警察など、より適切／効率的に当該情報を活用できる窓口への提供が望ましいもの



アリバイのため

・国との関係を考慮して、公開前のレポートの内容を事前に提供するもの

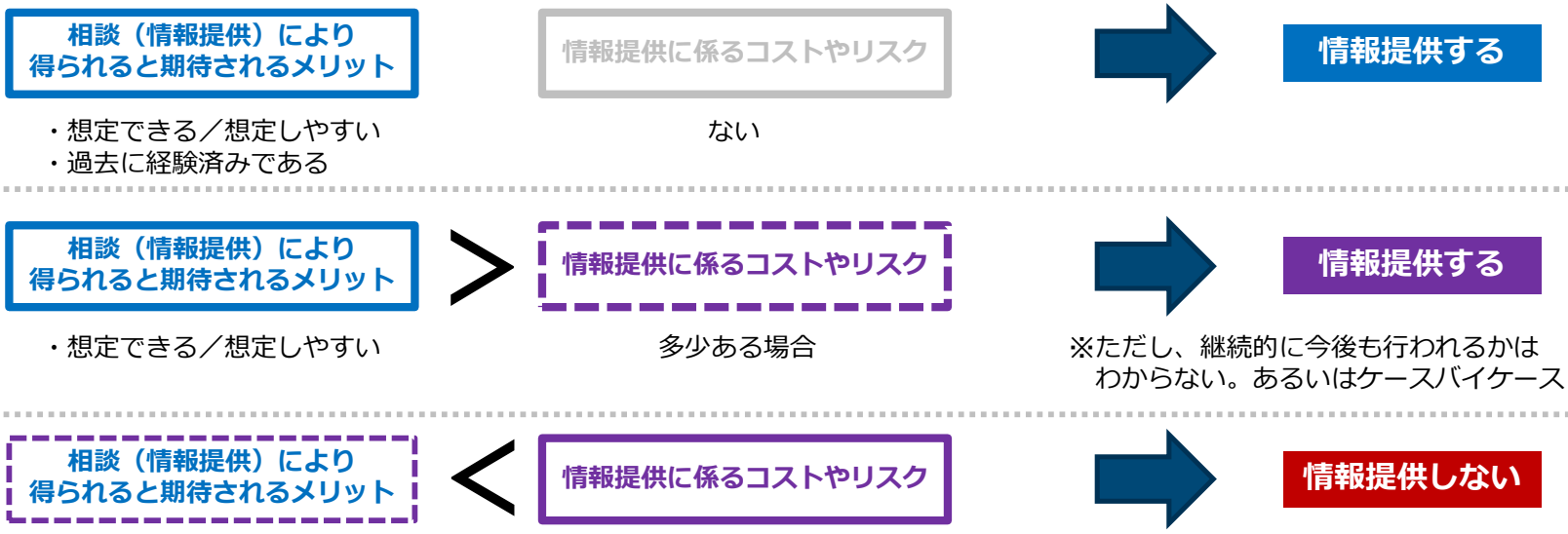
・当該情報を自組織だけで抱えておくには リスクがあるが、適切な提供先／依頼先が不明にて、提供されるもの



情報提供の経済学的力学

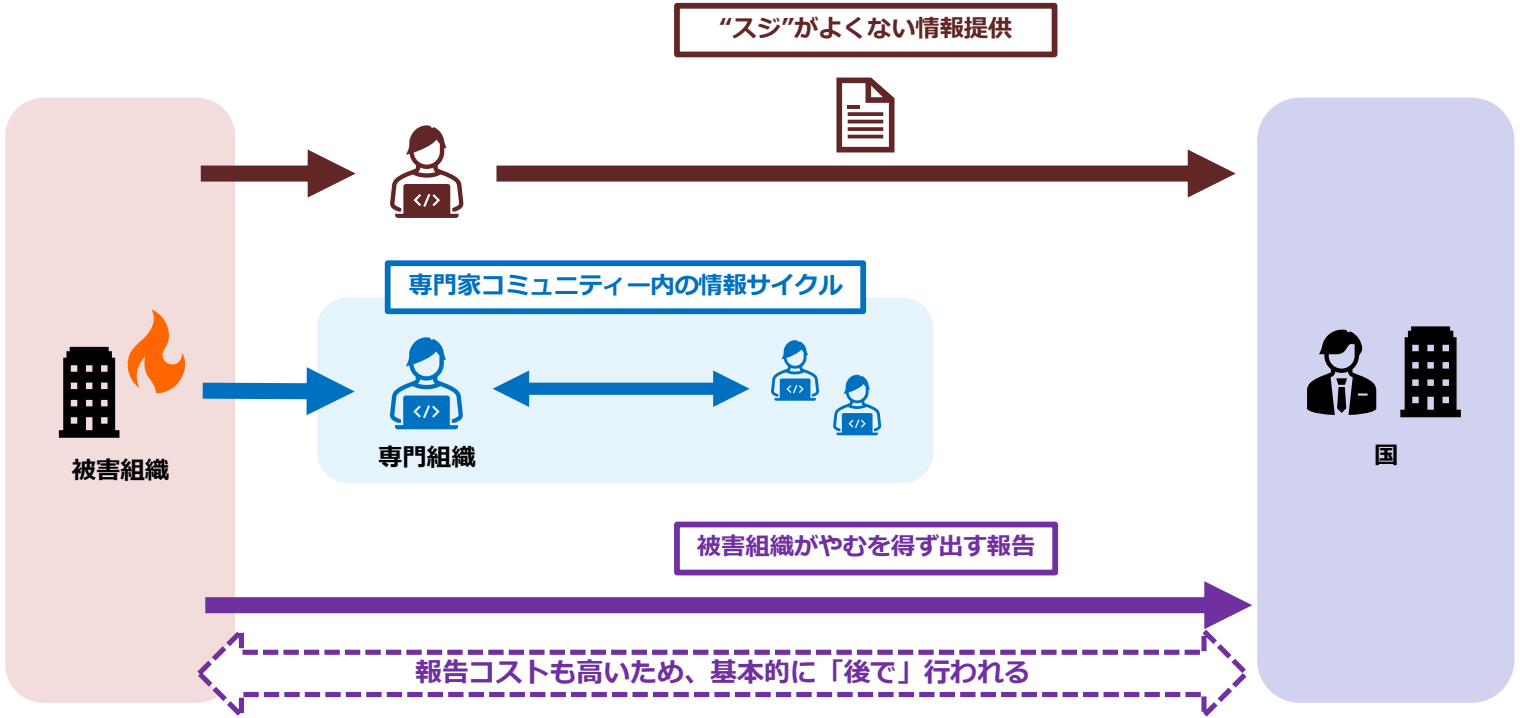
- 被害組織をはじめとした情報提供者がなぜ公的機関等に情報を出すのか
- 情報を「出してもらうメリット」のことばかり注目されがちだが、「情報提供コスト」が見逃されている

例：窓口側に知見がないため、技術的用語が使えず、説明を求められる　←行政に対しては企業の渉外・法務部門が対応することから、被害組織側がIT／セキュリティの知見が少ないように行政側から見えてしまう。また、行政向けに「平易な言葉」で報告内容を書いているに過ぎない。



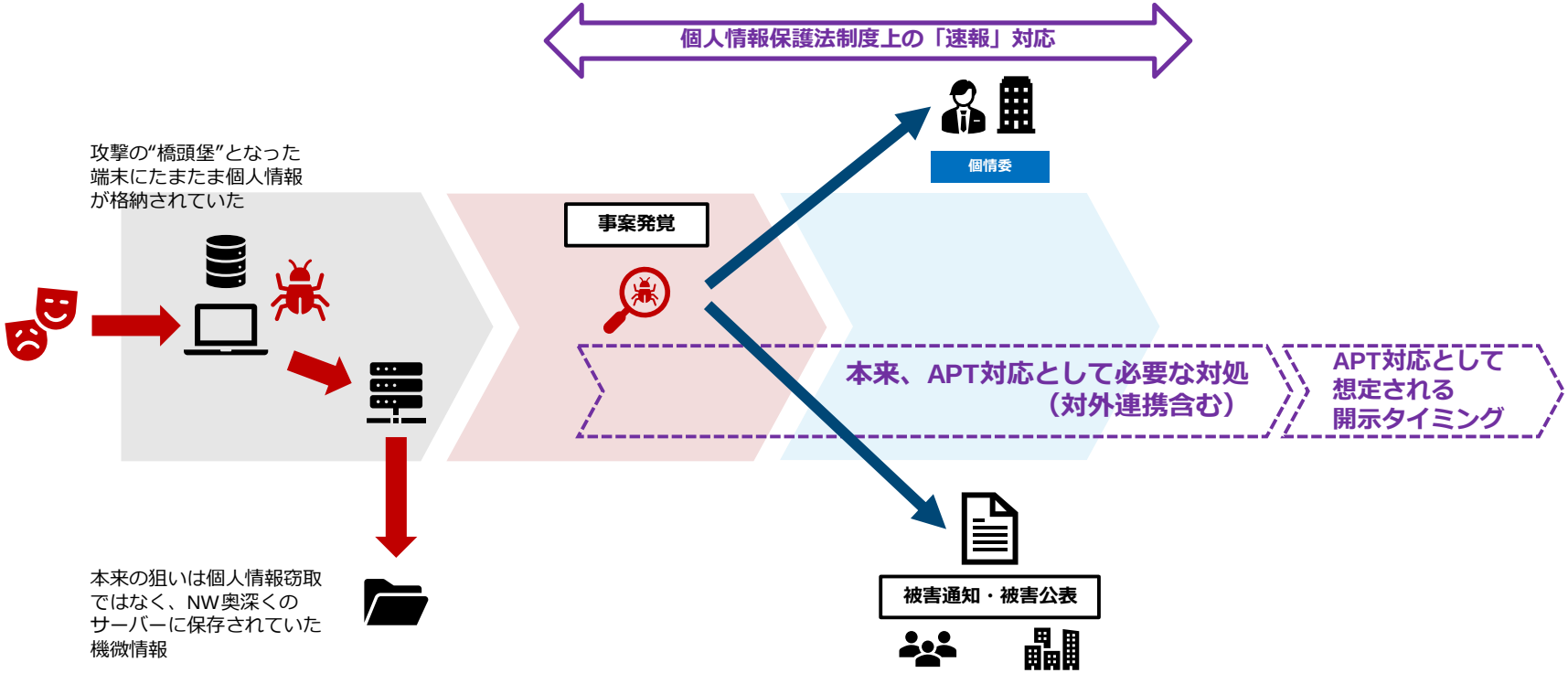
国側に情報が提供されない構造的背景①

- （ここまでの解説のとおりの状況であるため）スジがよくない情報提供やタイムリーではない情報提供ばかりになり、他方で、脅威情報の流通経路にはタッチできていない



国側に情報が提供されない構造的背景②

- 個人情報保護法制度上の「速報」対応や被害個別通知対応に追われ、被害組織は本来の事案対応リソースを消耗（報告対応や公表・対外応答対応）してしまっている。本来その攻撃類型に対して必要な外部連携はなされない



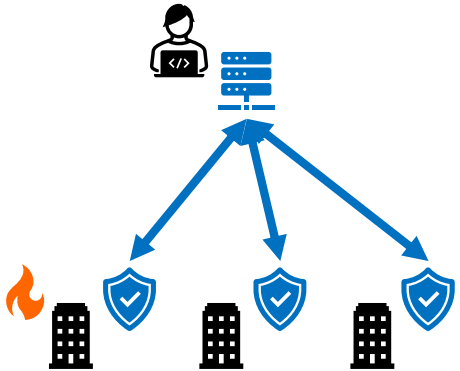
脅威情報ハンドリングをしようとする者の陥りやすい罠

- 他組織が知らない「情報を持っていること」自体が優位性／価値であると勘違いしてしまう
- 情報源の「囲い込み」によって入手できる情報源のパイを増やそうとするが、必ずしも上手くはいかない

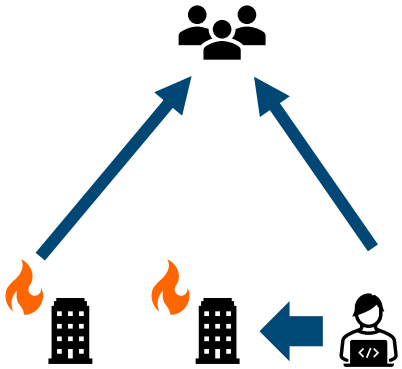
専門組織の優位性（と勘違いされること）

より広い／深い“センサー”を持っていること

例：アンチウイルスベンダー、SOC

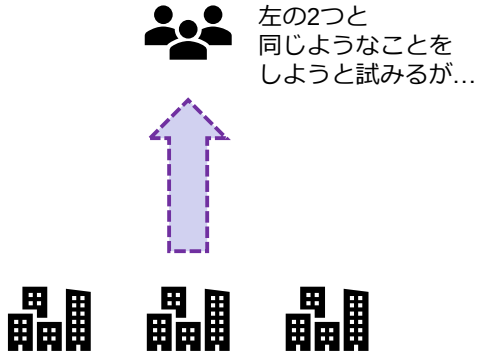


広い情報網を持っていること



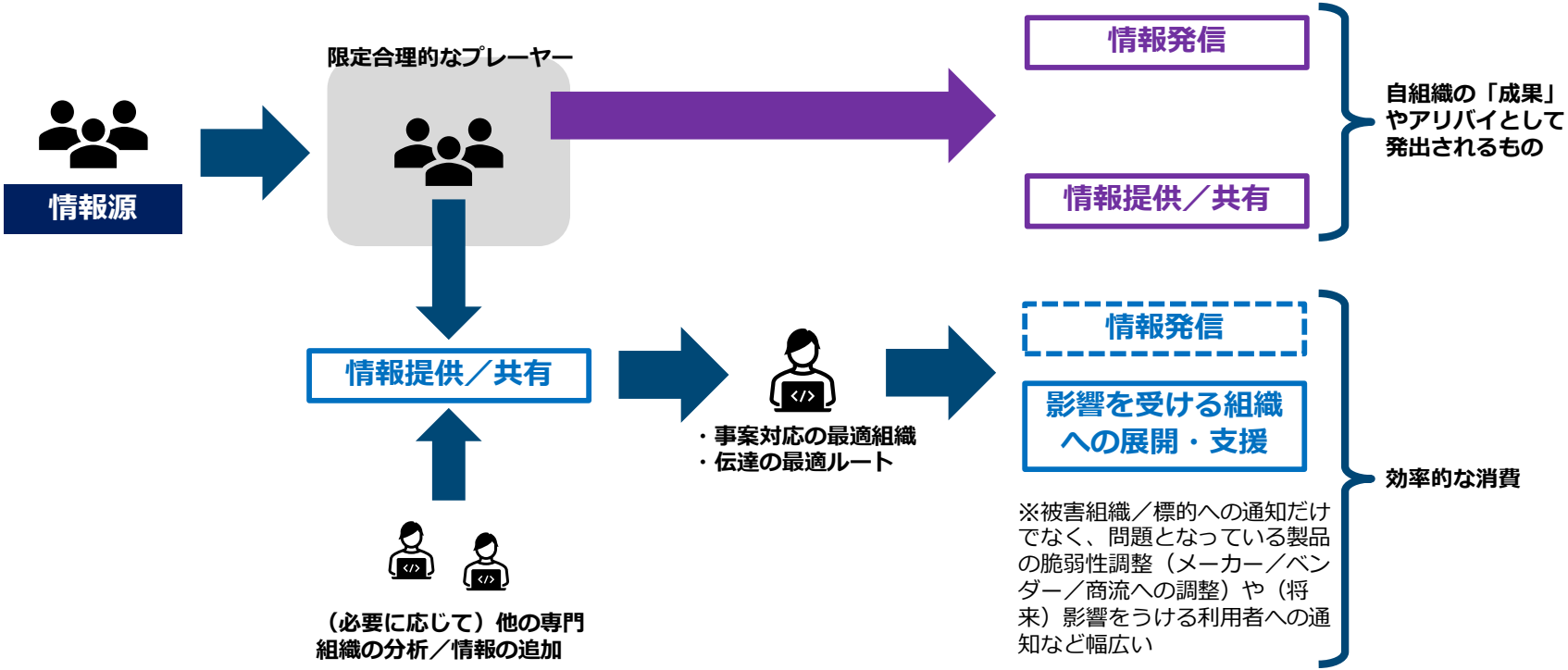
被害組織から直接情報が来なくても、（セキュリティ）ベンダーやISP等から相談が来る

広い情報網を持っているが機能しないもの



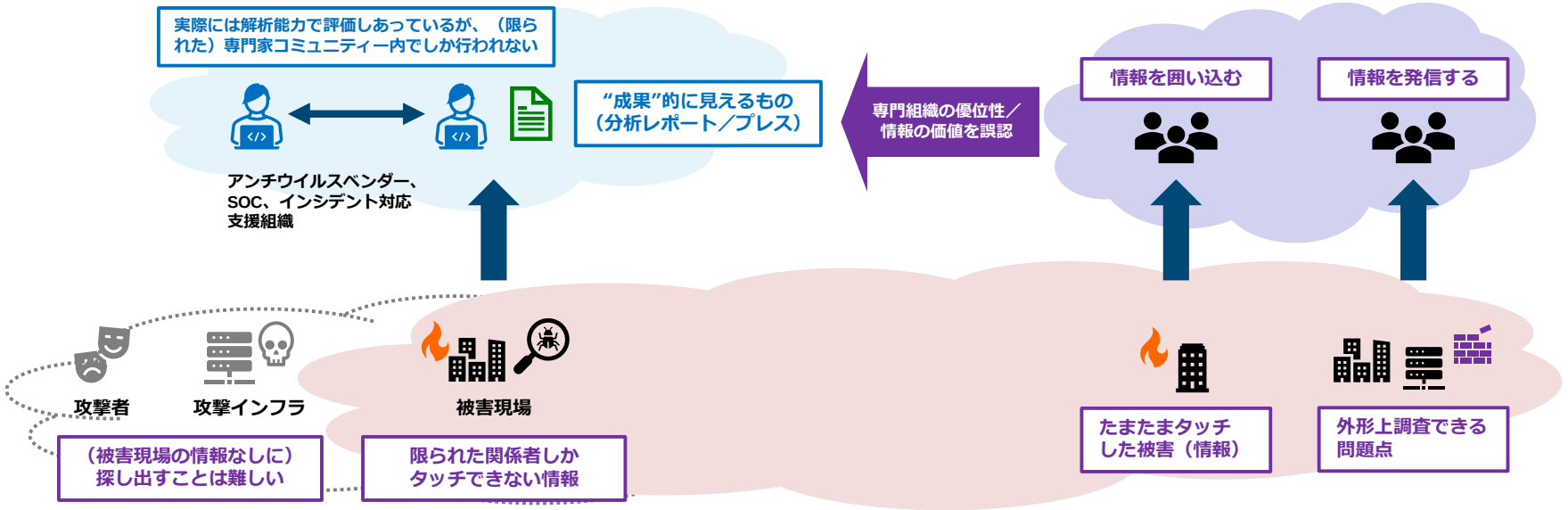
脅威情報の非効率な“消費”と効率的な“消費”

- 限定合理的なプレーヤーは脅威情報を活用しきれない
- 非効率的な”消費”を見た情報提供元は以降、情報を提供しなくなる



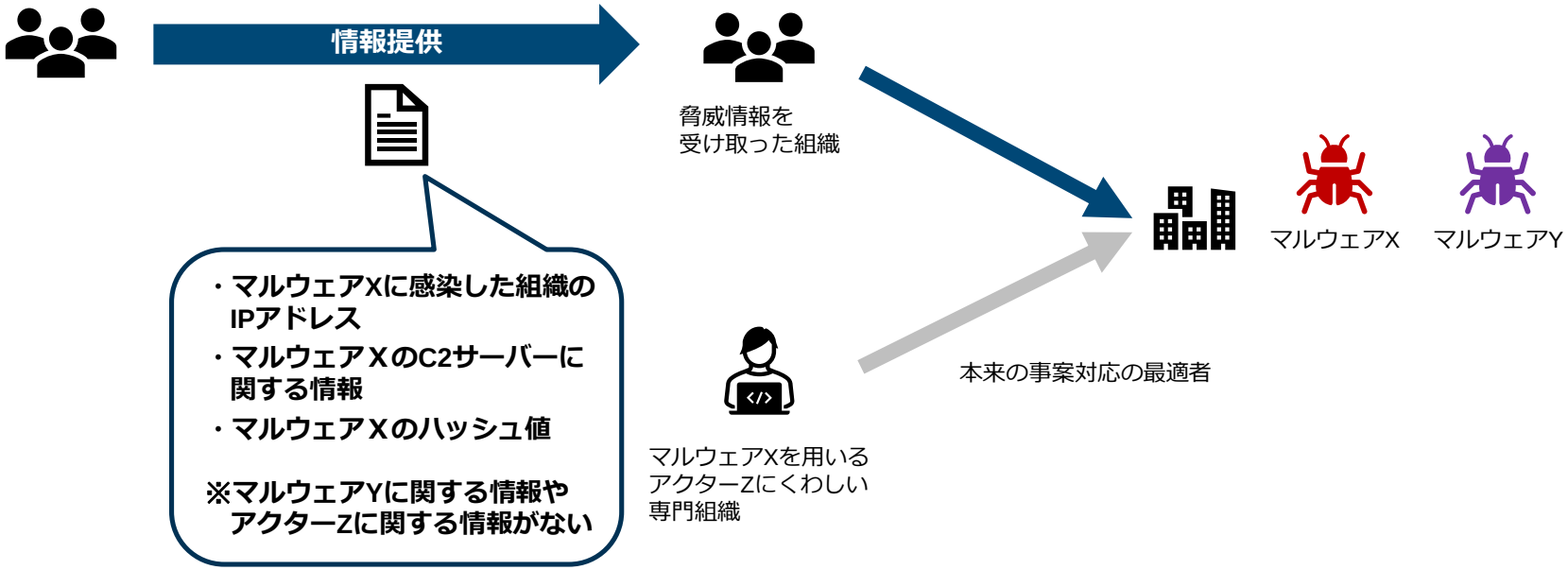
なぜ、情報を囲いこんだり「成果」として扱ったりしてしまうのか

- 専門家／専門組織同士の評価は極めてクローズドなコミュニティー内で行われており、それ以外の者からすると、分析レポートやメディア露出が“成果”として見えてしまう
- 「先行する専門組織は多くの「顧客」（営利／非営利問わず）を囲っているから」成果が出るのだと見てしまうプレーヤー
  ⇒ 自分がたまたまタッチした案件に関する情報は囲い込む（被害情報／件数が優位性であると、価値を誤認してしまうため）
- “成果”≒レポートをたくさん出していることだと評価しているプレーヤー ⇒ OSINT調査などで見つけた情報をすぐに開示してしまう



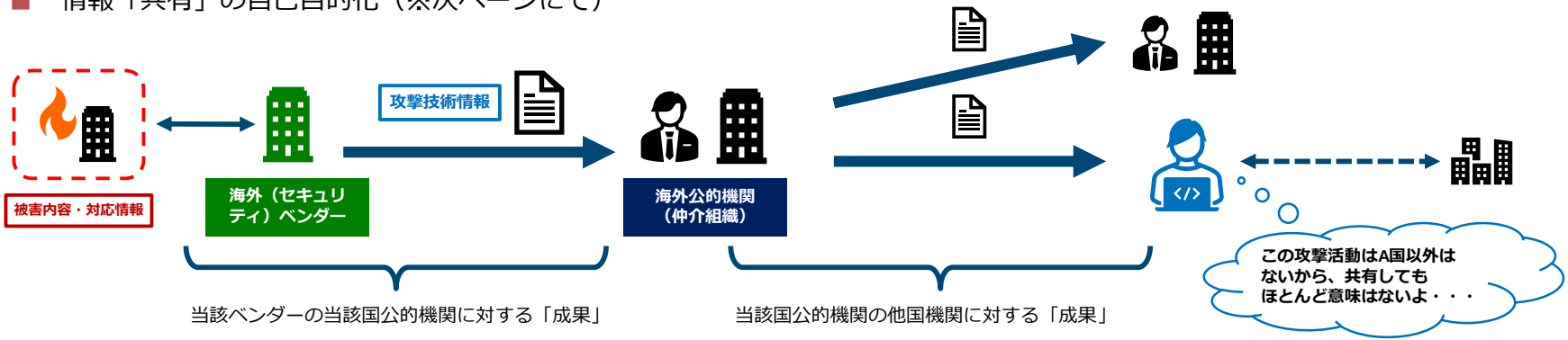
脅威情報を適切に「消費」できる者／できない者

- 脅威情報を最初に受け取った者が必ずしも当該事案対応の最適者とは限らない



海外組織との情報共有がうまくできないケース

- よくも悪くも「担当次第」である
  - —窓口になっている担当者判断で情報を切り出して提供していることが多い
    - ⇒個人的信頼関係で運よく情報を得られることもあるが、極めて属人的な営みであるため、当該担当者の異動／転職でそのルートは消えてしまう（本来的には組織間で情報伝達ができ、信頼性が担保されるようにすることが必要）
  - —他方で、組織全体での統制がとれておらず、外部への情報提供が意図しないトラブルになる場合もある
    - ⇒例：日本の製品を含む脆弱性情報が発見した海外セキュリティ企業から調整前に各国に拡散されてしまったケース
- 情報源からの提供情報にはPR目的、アリバイ目的の情報が多い
  - —公表直前での「仁義切り」的な事前情報提供を受けても、時間的余裕がなく、対応のしようがないケースも
  - —PR目的情報の「バケツリレー」
- 情報「共有」の自己目的化（※次ページにて）



海外情報連携の失敗事例から見えること①

- 専門組織同士の情報共有の間に別の組織（仲介組織）が挟まると情報共有・連携がうまくいかなくなることが多い
- 専門組織同士の情報共有において評価されるのは
  「（自組織にない）情報を持っていること」ではなく、「その組織しかできないこと」をやっているかどうか

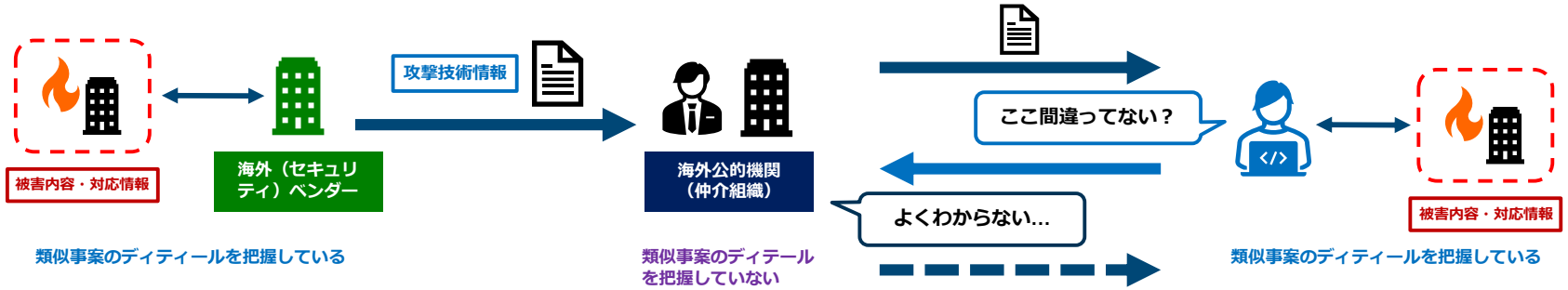
  例：攻撃に関する問い合わせのために情報提供をしてくるケース ⇒ 相手方には自分たちより「知見」があるから相談してくる

  例：テイクダウンで見つかった被害組織データを提供してくるケース ⇒ 相手方には当該被害組織へ適切な対応をしてくれる（≒当該データを効果的に消費してくれる）と考えるから提供してくる

- バッドケース：（仲介組織だけでなく、情報提供元の海外専門組織自身も含め）

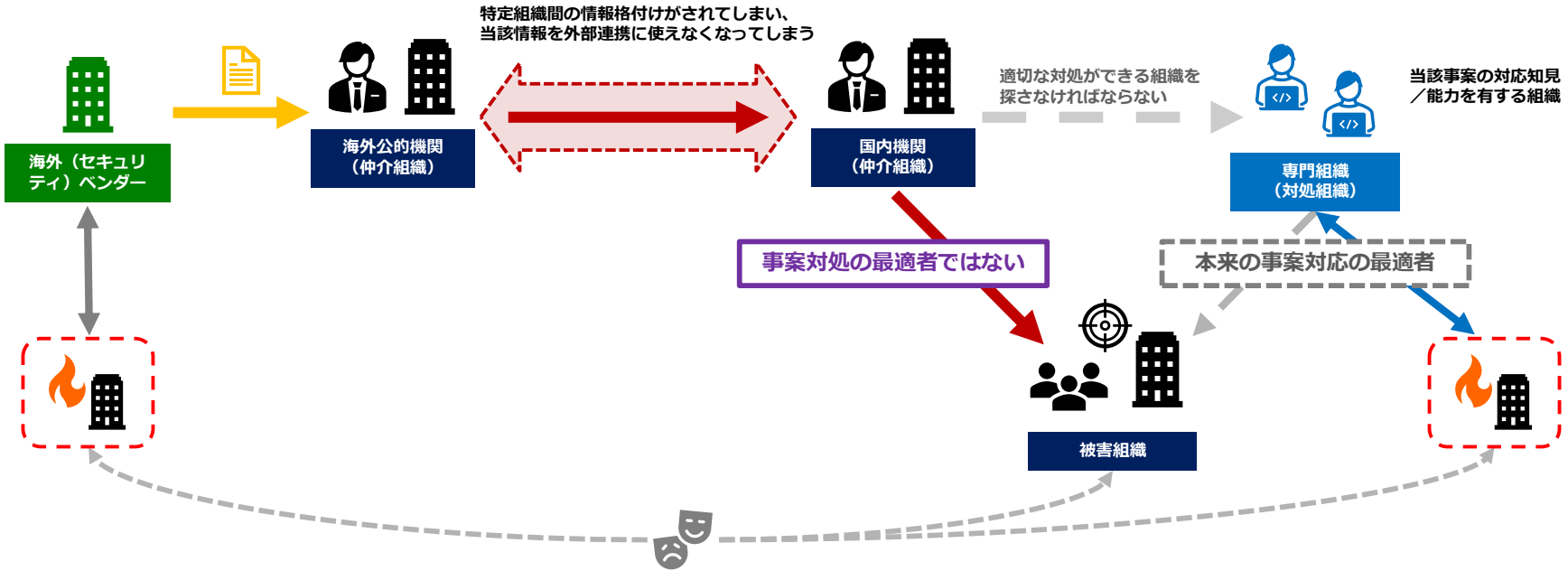
  —「相手が知らない情報を持っているかどうか」を価値／優位性と勘違いしているため、「情報を見せる／渡す」行為しかしない。また、仲介組織は情報提供源から得た情報をそのまま右から左に流す

  —利害関係者への調整が不十分なのに成果としての「情報を第三者に渡す」「情報を公表する」ことが優先されてしまい、“事故”を起こす



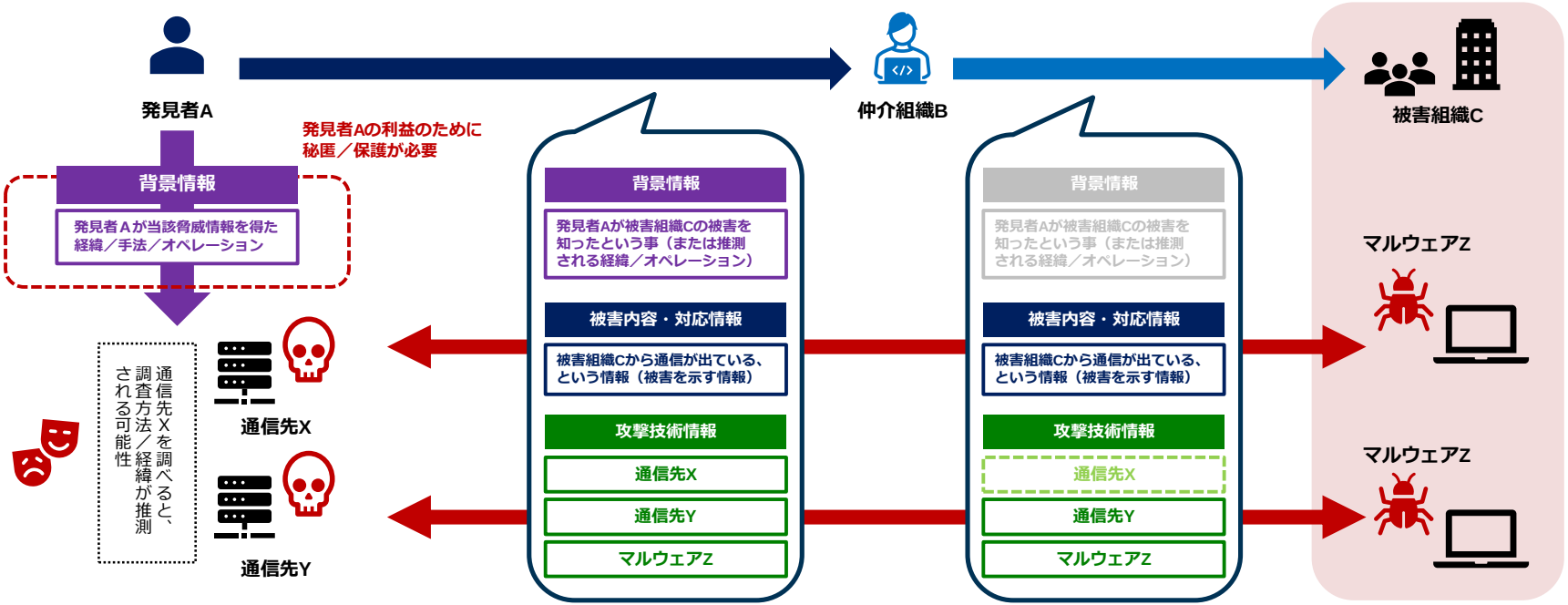
海外情報連携の失敗事例から見えること②

- 海外情報連携のマズさが、「事案対処の最適者が調整されない問題」に繋がっている
- 情報伝達の仲介組織が必ずしも「事案対処の最適者」とは限らないため、適切な対処組織を探さなければならないが、仲介組織間で情報格付けの縛りをかけてしまうため、適切な対処組織に当該情報を伝えられなくなってしまっている
（本来の窓口CERT間連携ではそのようなことが無いように適切なTLP設定や情報の分離を行っている）

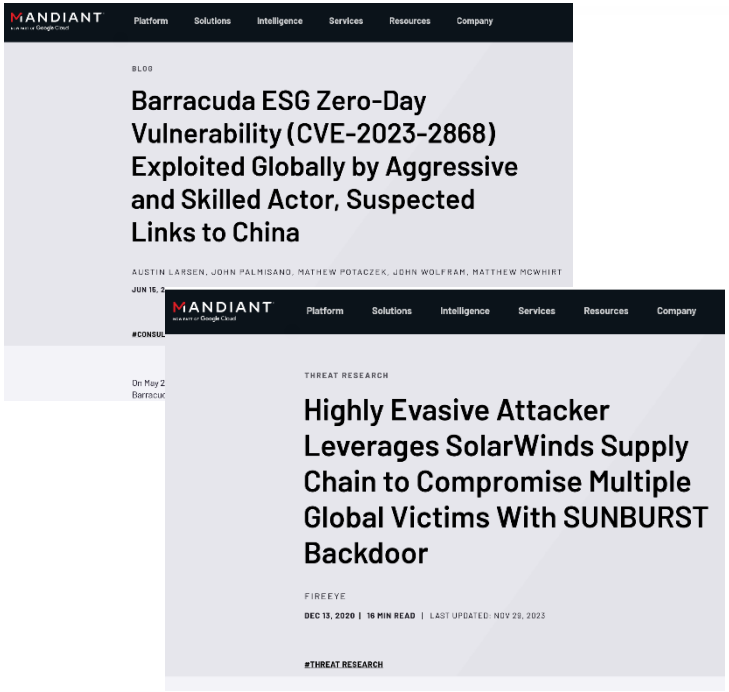


情報の分離・加工と「仲介者」の効果

- 当該脅威情報を発見した経緯／手法／オペレーションといった背景情報は“ある期間まで”発見者や他の被害組織の利益保護のために秘匿される。ただし、しばらくの後、当該背景情報は開示されることが多い（テイクダウンオペレーションの公表、刑事訴追の公表等）
- 背景情報以外の秘匿の必要性のない情報・調査に必要な情報を分離・加工・選択して「情報を伝えるべき相手」に伝達する
- 発見者から被害組織に直接伝えるのではなく、仲介組織を挟むのは必ずしも便宜上、あるいは支援のための専門知見の都合だけではなく、発見者を匿名化する効果もある



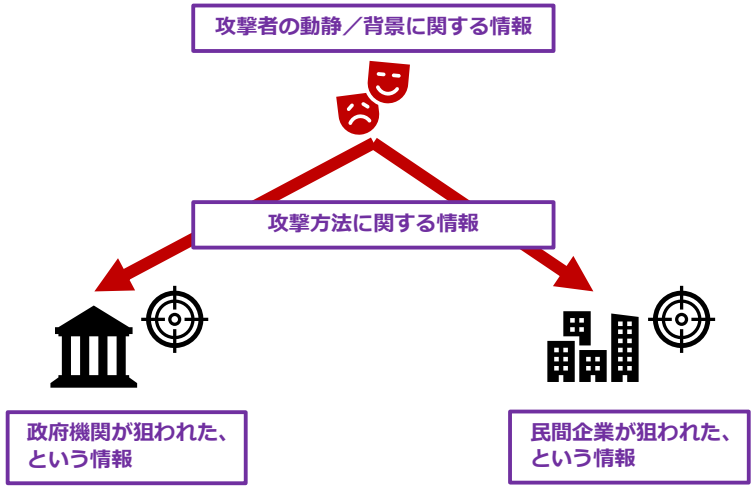
頭の体操・・・



出典（上）：MANDIANT
https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

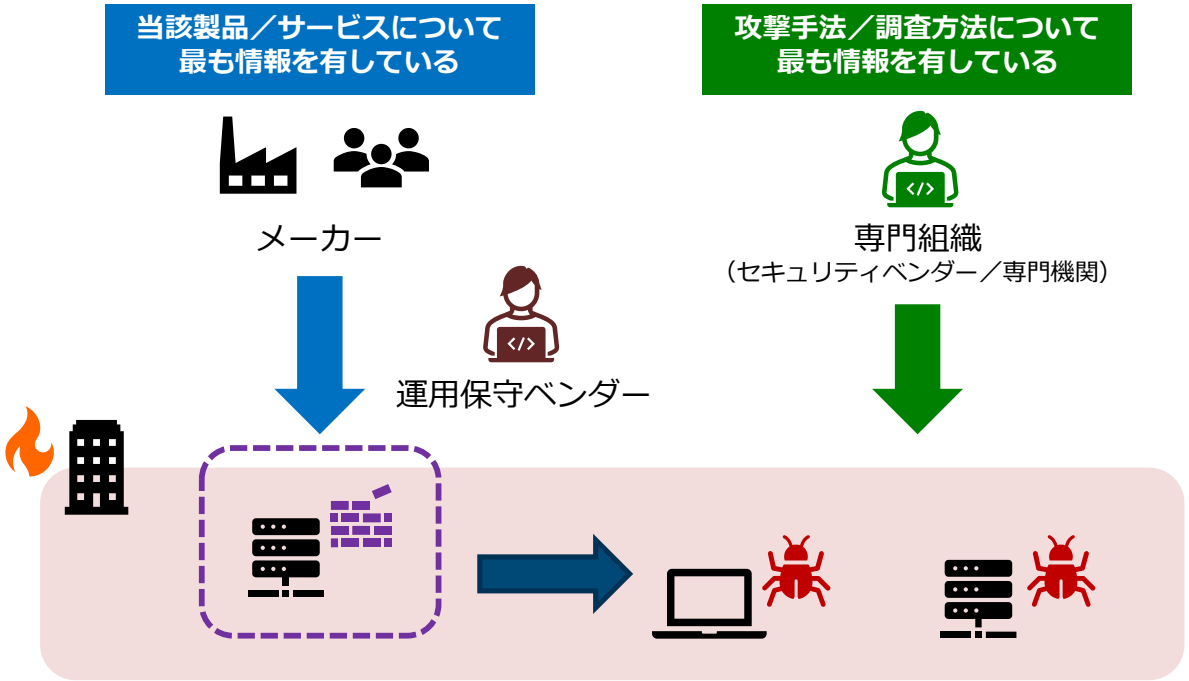
出典（下）：MANDIANT
https://www.mandiant.com/resources/blog/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

- SolarWinds事案（2020年）、BarracudaESG事案（2023年）、いずれもMandiantが速やかなレポート公表をしなかったらどうなっていたか…
- 「公的機関にも被害が出ている」ということで、もし当該国が情報の取り扱い全体に制限をかけてしまっていたら…



参考：なぜメーカーからの通知だけでは不十分か

- 特定製品のゼロデイ事案において「メーカーから（非公開で）対象者に個別通知がされればよい」という主張を度々聞くが…
- 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Initial 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



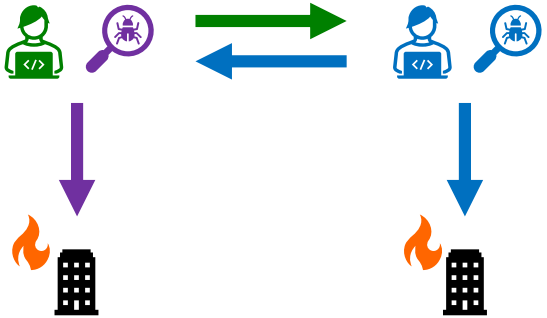
専門組織同士の情報共有の観点から

専門家同士の情報共有の動機

- 基本的にはセキュリティアナリスト（個人）単位で行われている
- 過去においては、民間のセキュリティベンダー同士の情報共有は難しく、情報の“囲い込み”もあったが、徐々に専門組織／アナリスト同士の情報共有が浸透した（そういう文化が醸成された）
- ただし、これができているのは（国内外ともに）業界の一部に過ぎない

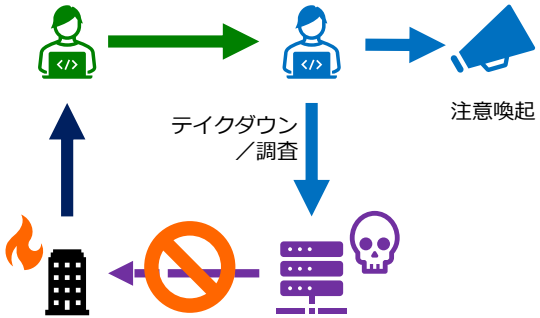
情報が不足しているので共有（により補充）する

攻撃の高度化により単一組織での解明が困難なケースが多い（例：APT事案）



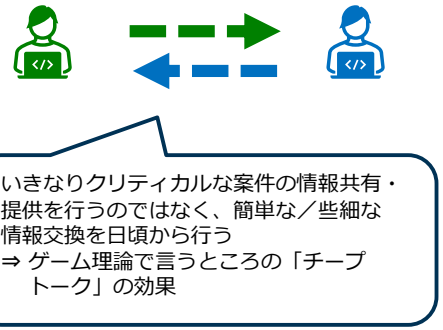
最適に「消費」できる組織へ渡すため

自組織では当該事案を解消できないため、最適に対処できる専門組織に依頼することが事実上の情報共有・情報提供になっている



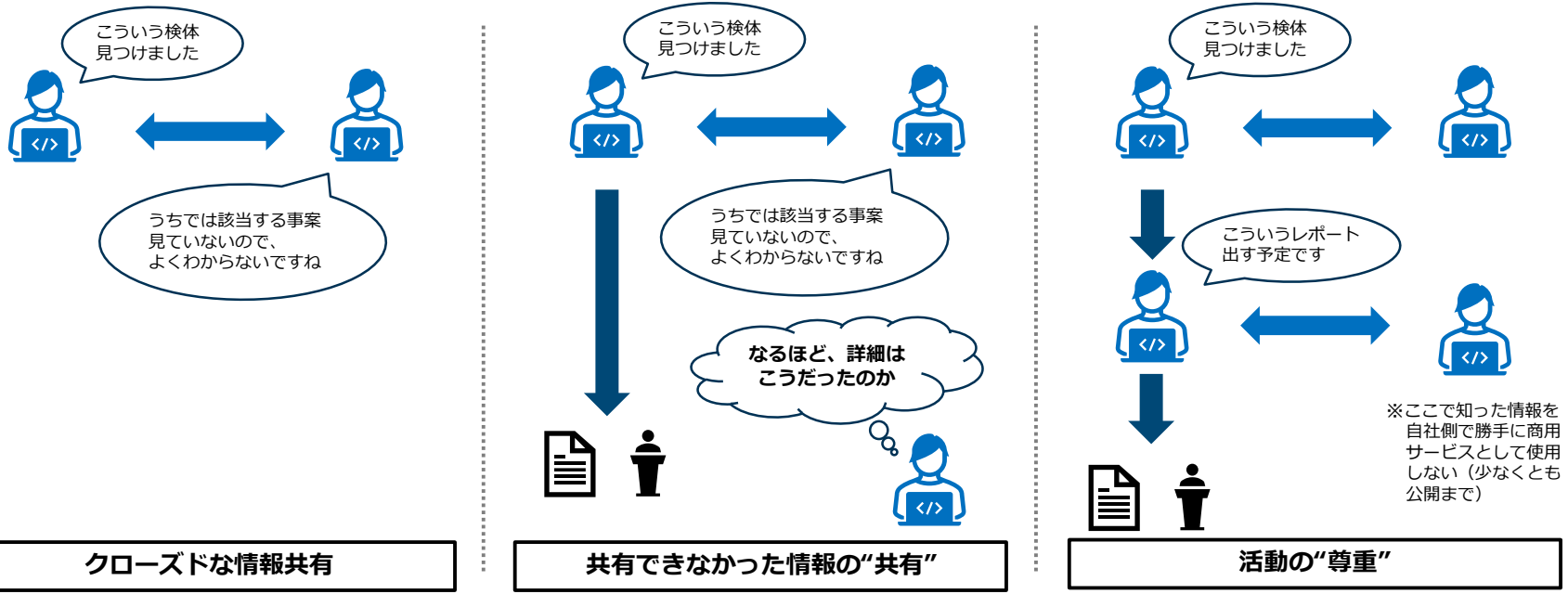
信頼関係維持のため

信頼に足る相手であるか、同じレベルの会話ができる相手が確認するために、日頃からクリティカルではない案件の情報交換を行う



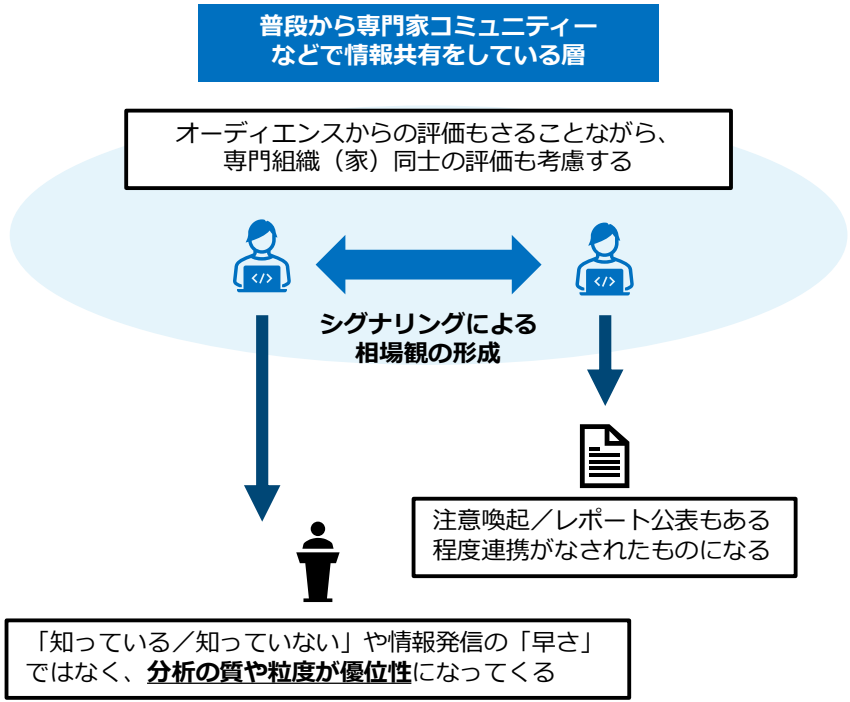
専門組織／専門家同士の共有メカニズムを支えるもの

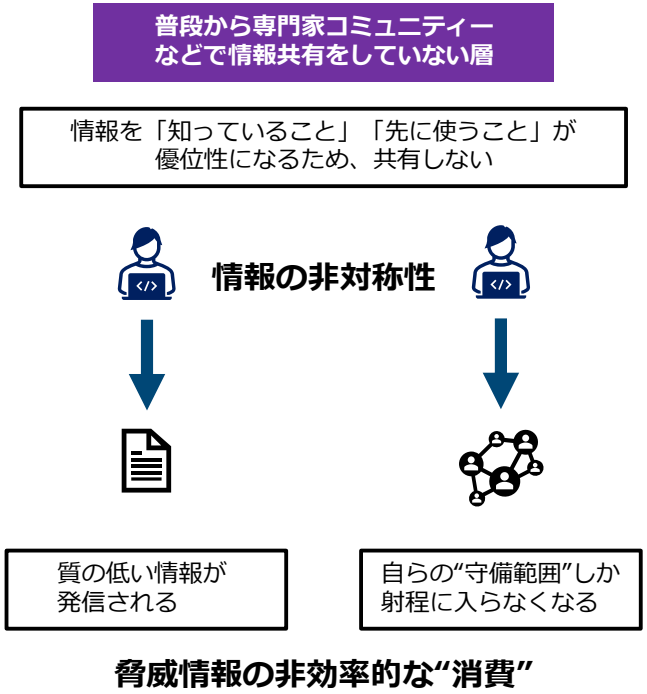
- 「レポート発表」の重要性 ⇒ 分析のために相互参照することだけでなく、信頼関係維持のために重要である
- 共有（提供）した情報をどう使ったのか「見える化」される ← 民間ベンダーから専門機関に提供される場合は、「注意喚起発信」や「脆弱性調整・公表」や「テイクダウン」という形態で「見える」。
  では、国に提供した情報がどう使われたのか、「見える化」されているのか…？



専門組織（家）間の共有を通じた脅威情報の効率的な消費

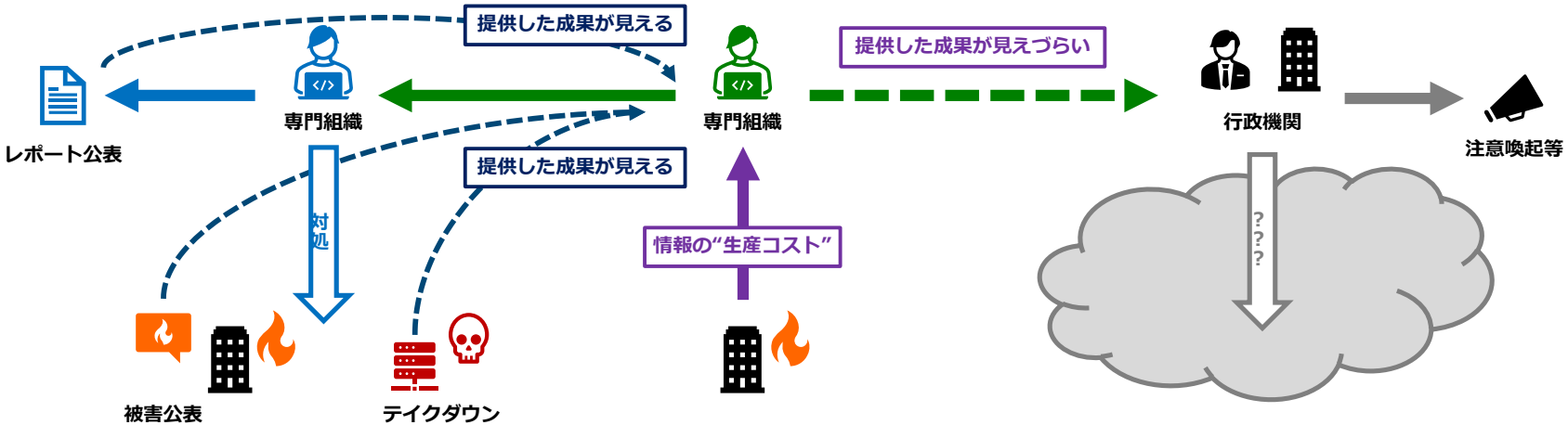
- 「鶏が先か卵が先か」論であるが、普段から専門組織同士で情報共有しない層は、「知っていること」「先に情報を使うこと」が優位性になったままであるため、共有を避け、情報を非効率的に“消費”してしまう





専門組織同士から見た「専門性」の源は脅威情報か、経験か

- 「情報（源）を多く持っているかどうか」≒「珍しい事案を経験する確率が高いか否か」ということであるため、時間の経過とともに希薄化する＆知見としてすぐ古くなる（個人としての経験（年）数にも同じことが言える）
- 専門家同士が互いの能力を評価する場であるレポートやカンファレンス ⇒ 当該時点で他人・他社にはない切り口での分析や行動ができているかどうか
- 「他人・他社にはない切り口での分析」⇒ 基本的にはアナリスト個人の分析能力
- 「他人・他社にはない行動」⇒ テイクダウン、脆弱性調整、（公益性の高い）情報発信、刑事手続き等の法的措置
- 情報の入手には“生産コスト”がかかっている以上、相手に渡す（取り引き）には、「渡す相手に相応の能力／専門性」があることが示されなければならない。「相応の能力／専門性」があるかどうかは、情報共有活動に加えて、共有活動を通じた情報発信（レポート／カンファレンス）や攻撃対処（テイクダウン、注意喚起、脆弱性調整、捜査等）による「見える化」も必要



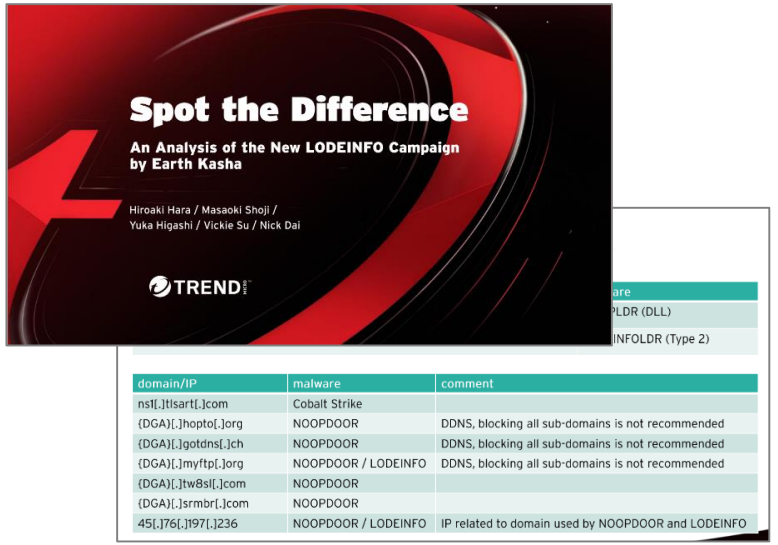
専門組織同士の情報共有とそれぞれの成果物の例

- 2023年9月、11月のJPCERT/CCからの標的型サイバー攻撃キャンペーンに関する注意喚起については「サイバーセキュリティ協議会の活動などを通じて」情報共有を受けた情報をもとに行われた
- 関連する攻撃キャンペーンに関する分析レポートは複数のセキュリティベンダーが分析レポートを公表／カンファレンス発表している

JPCERT/CCからの注意喚起

https://www.jpcert.or.jp/at/2023/at230029.html

セキュリティベンダーからのレポート例



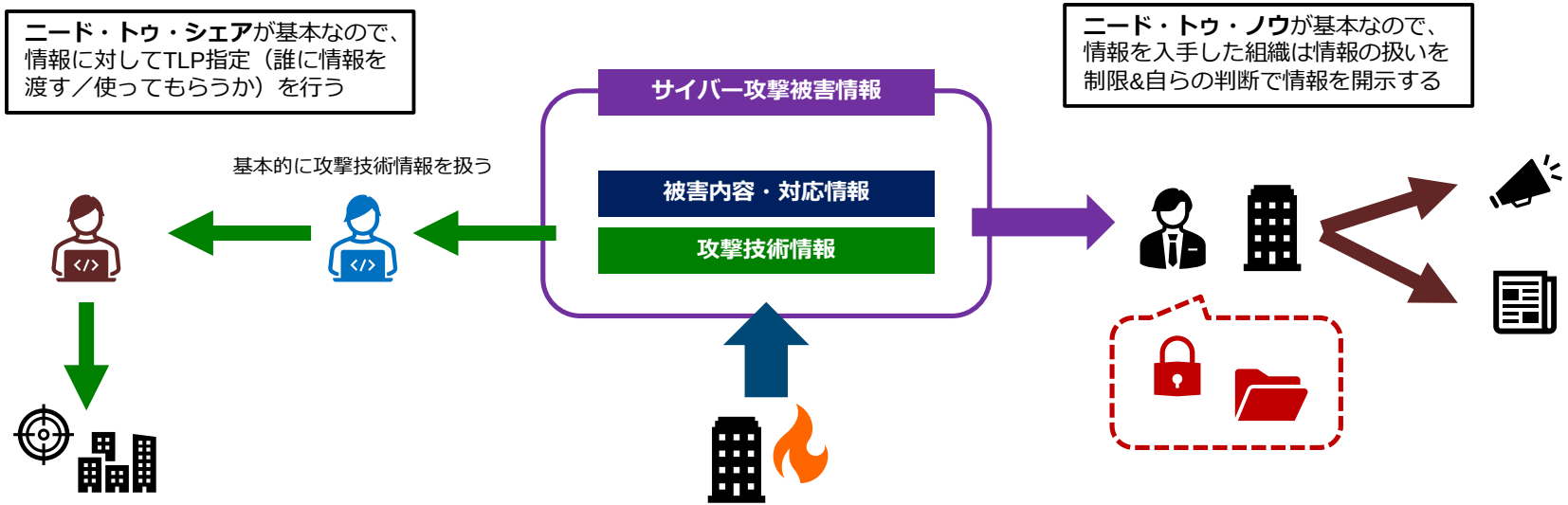
domain/IP	malware	comment
ns1[.]tlsart[.]com	Cobalt Strike	
{DGA}[.]hopto[.]org	NOOPDOOR	DDNS, blocking all sub-domains is not recommended
{DGA}[.]gotdns[.]ch	NOOPDOOR	DDNS, blocking all sub-domains is not recommended
{DGA}[.]myftp[.]org	NOOPDOOR / LODEINFO	DDNS, blocking all sub-domains is not recommended
{DGA}[.]tw8sl[.]com	NOOPDOOR	
{DGA}[.]srmbr[.]com	NOOPDOOR	
45[.]76[.]197[.]236	NOOPDOOR / LODEINFO	IP related to domain used by NOOPDOOR and LODEINFO

出典：トレンドマイクロ「Spot the Difference」
https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_2_7_hara_shoji_higashi_vickie-su_nick-dai_en.pdf

官民間情報共有の観点から

官民間の脅威情報の取り扱いの根本的ギャップ

- （国内はさておき）国側は「インテリジェンス情報」として扱うことが多い。専門組織は「被害情報」として扱う。根本的に考え方が違っている
- 国側：基本的に第三者への提供や開示は前提にない。ただし、公益性が高いと判断すればインテリジェンス情報は「開示」（注意喚起／報道対応）される
- 専門組織側：基本的に攻撃技術情報を扱うため、効率的な方法として非公開での伝達／共有が使われるが、しばらく経てば公開されると想定している



サイバー脅威情報に適した取り扱い制限のかけ方

参考：「共有・公表ガイダンス」Q30

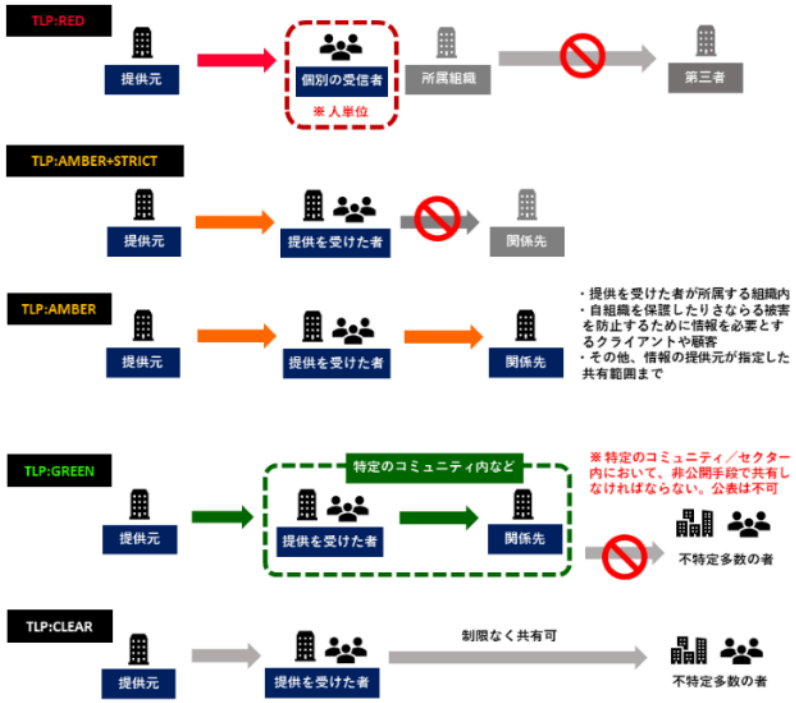


図 72

- 情報自体に「静的な」制限・指定かけるのではなく、共有範囲／期限／活用が許可される場合・目的といった、「動的な」制限・指定をかけることの重要性
- 当該情報を「何に使うのか」が定まっていないと、TLP設定を適切にかけることができない
- 必ずしも秘密性のない技術的な情報（攻撃技術情報）と、第三者を保護するために秘匿しなければならないコンテキスト情報（被害内容・対応情報）とを分けて、それぞれTLP設定する必要性

例：被害を受けている組織に攻撃技術情報（マルウェア情報、不正通信先情報等）を伝えなければならない場合

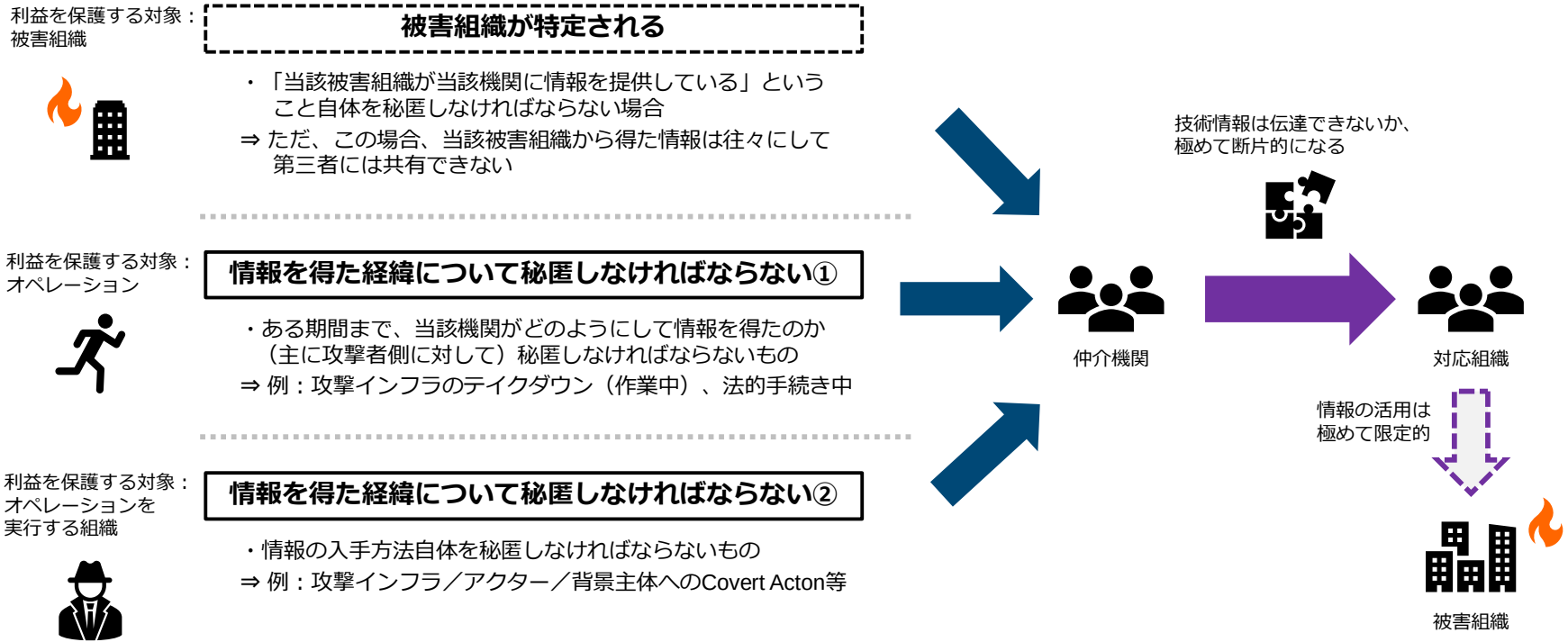
「機微な情報だから」ということでTLP：REDを設定

⇒ 被害組織に直接伝達するしかないが、ツテがなければ伝達できない

⇒ 被害組織に直接伝達できても、実際に作業する運用保守ベンダーに伝達できない

共有できない脅威情報、活用できない脅威情報

■ 情報源／情報の入手方法を秘匿しなければならないケースの大半では、第三者に開示できる情報が極めて断片的になるため、実際のインシデント対応支援や情報共有では活用できないことが多い

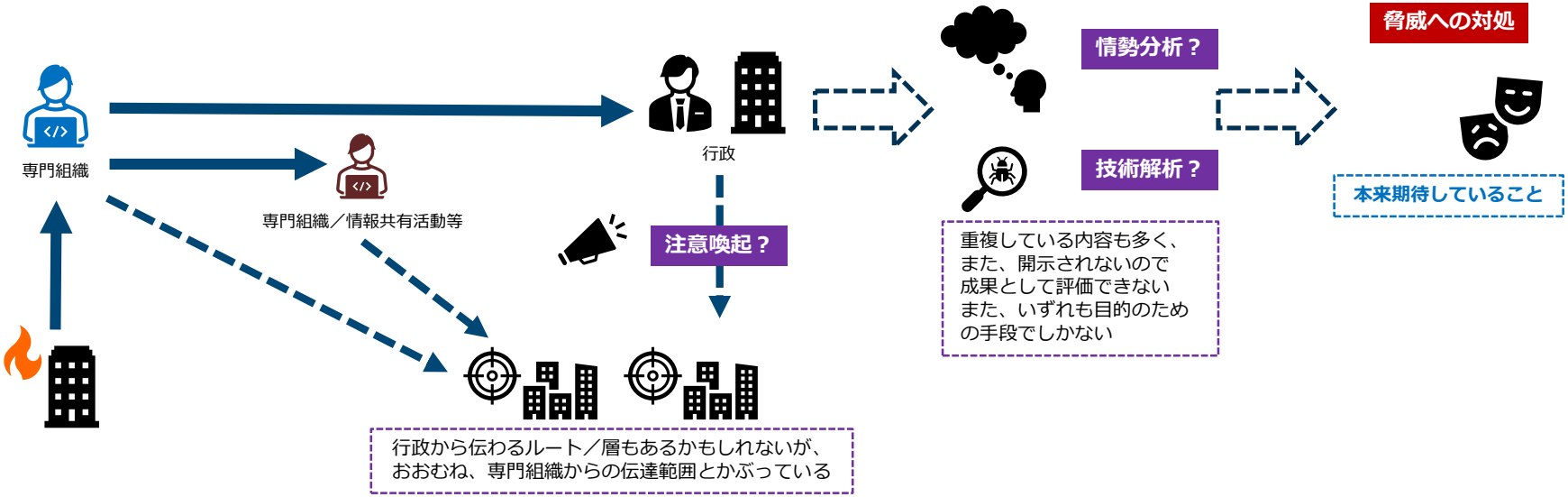


民⇒官へ：情報を何に使ってもらうのか？

- ※刑事捜査は別として
- よく遭遇するケース：「国から注意喚起するため／国から広く（経営層を対象に）注意を呼びかけることも効果があるので、情報を国へ出してほしい」

  ⇒ 本当に効果があるのか？タイミングはあっているのか？
- よく遭遇するケース：「我々も解析できる／国が持っているソースを使い情勢分析できる」

  ⇒ 技術解析：民側と重複orタイミングがあわない　情勢分析：開示されないので本当に活用されたのか評価できない



脅威情報流通の活性化に向けて

議論の前提：脅威情報の流通について

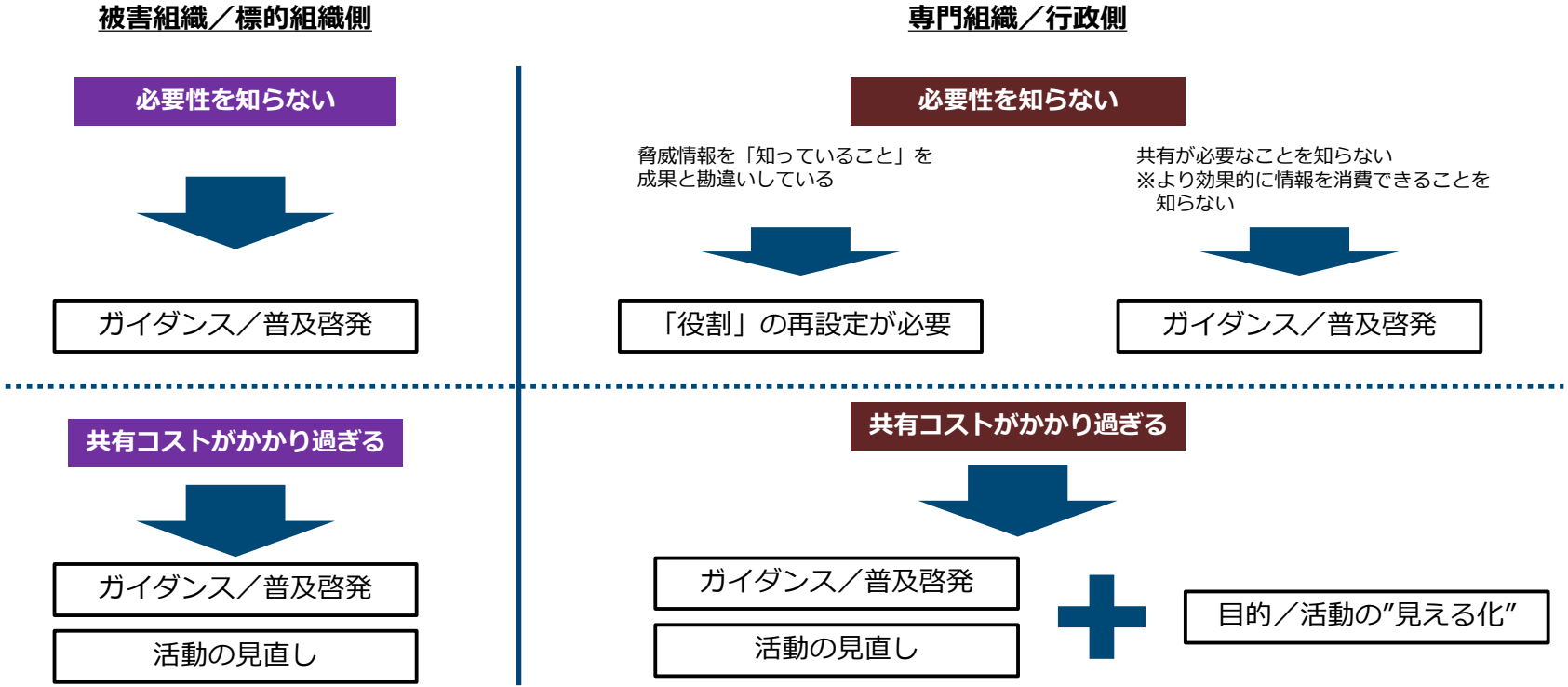
- 脅威情報を取引可能な「財」として捉えることができるのではないか
- 色々と整理しようと試みるも、なんともしっくりこない…（引き続き検討中です）

		消費において競合的か	
		競合する	競合しない
排除可能か	可能	**【私的財】** ・食品、衣服等	**【クラブ財】** （準公共財） **脅威情報：** **・消費が増えても追加費用なしで維持できる（非競合）** **・情報を囲い込むことで対価を支払わない消費を排除できる（排除性）**
	不可能	**【共有資源】** ・漁業資源 ・環境	**【公共財】** ・国家防衛、警察

出典：「マンキュー経済学Ⅰミクロ編（第4版）」や松村良之「財としての情報とその法的保護－「法と経済学」からのアプローチ」（田村善之編「情報・秩序・ネットワーク」収録）などから筆者作成

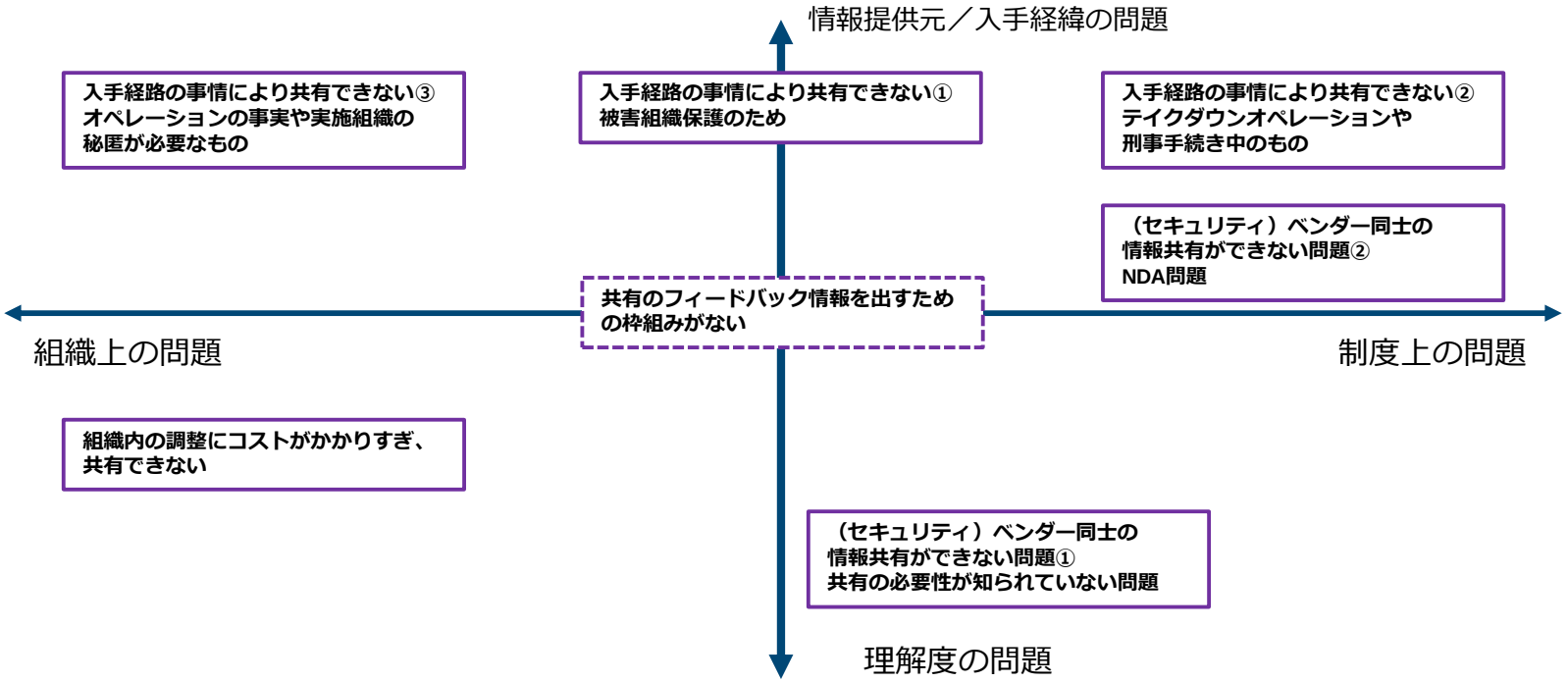
情報共有の活性化に向けて

- 脅威情報が「財」として取引できるのであれば、ゲーム理論などの情報とインセンティブに係る経済学的アプローチで改善可能ではないか？



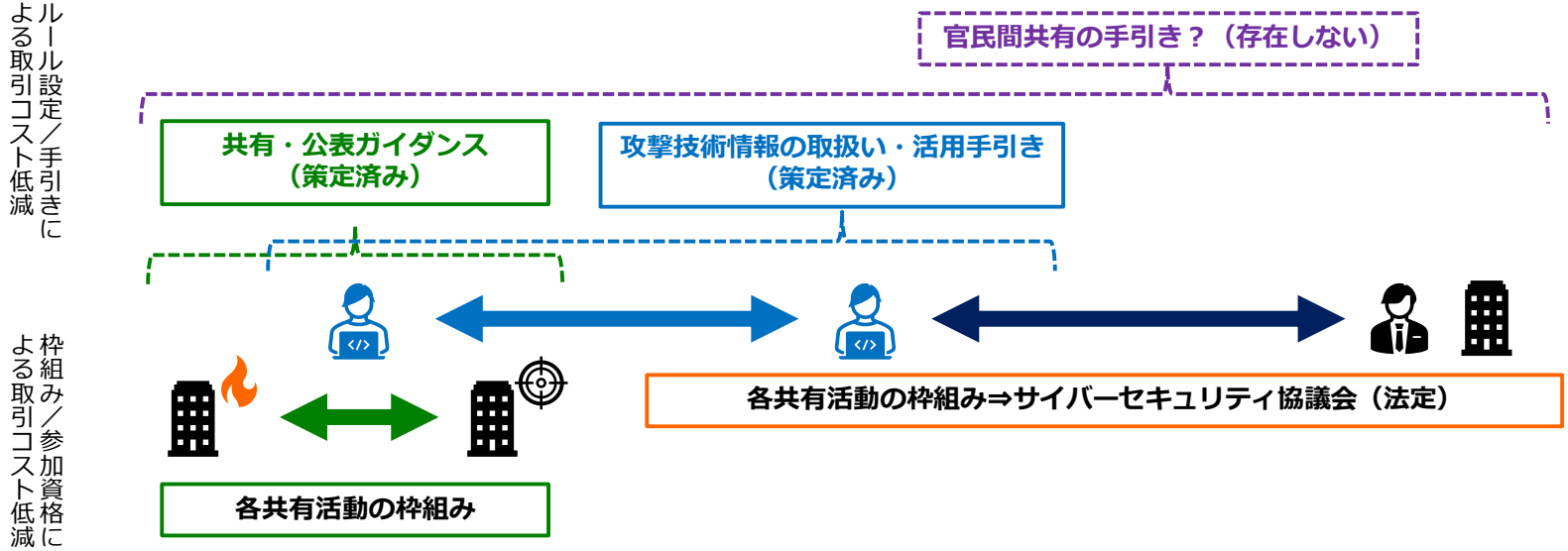
「共有できない理由」の各レベル感

- 脅威情報が「共有されない」理由を「（その組織が）情報共有できないから」としてしまっている（頭の悪い整理）
- 当該組織や当該脅威情報が「共有できない」理由／背景にはかなりの幅がある。それぞれにあった「処方箋」が必要。
- 被害組織への処方箋⇒「共有・公表ガイダンス」　専門組織への処方箋 ⇒「攻撃技術情報の取扱い・活用の手引き」



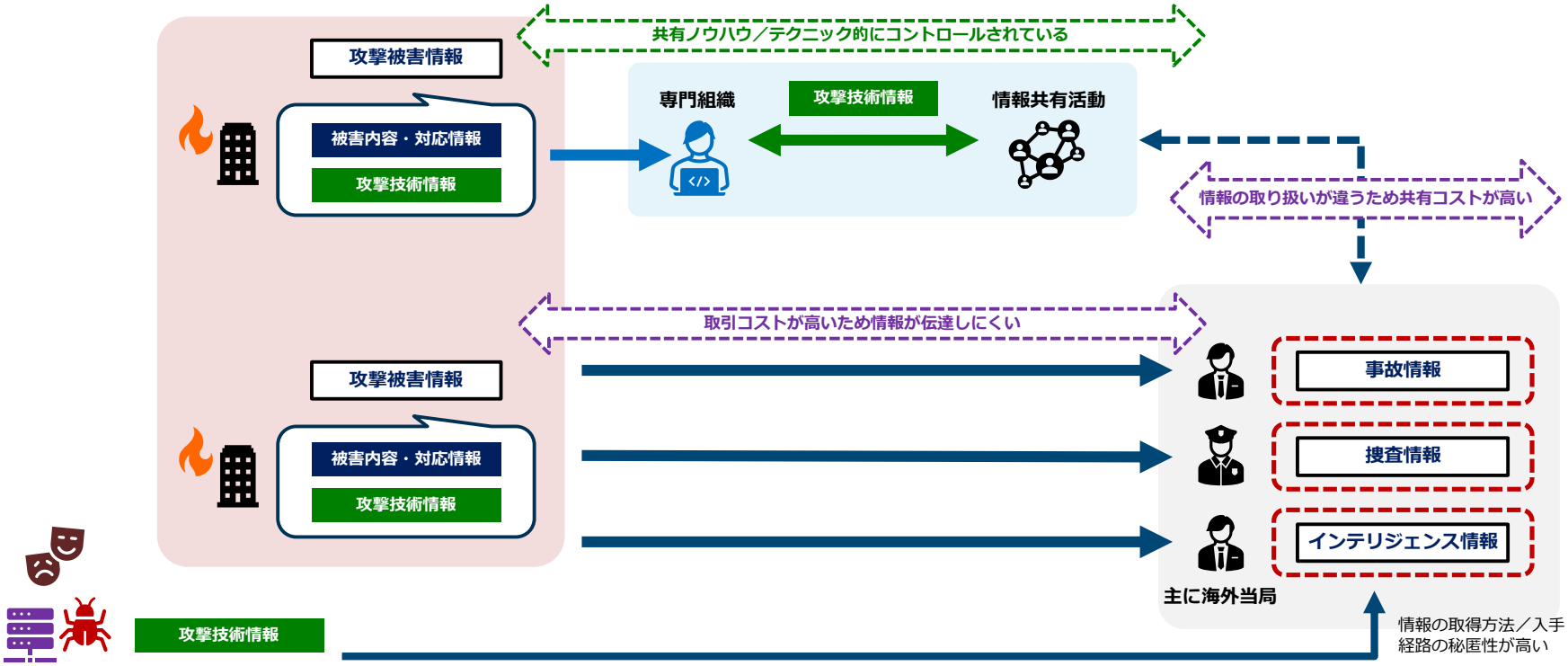
どう解消していくのか

- 脅威情報を経済学上の「財」としてみなせるのではないか
- 情報共有／情報提供のための「コスト」が見逃されている
- 情報の加工やルール設定により、「『財』として取引可能」な状態にすればよい
- 情報共有活動の設計段階の工夫（どういうメンバー／目的で行うか等）や、取り扱いルールの明示化、守秘義務制度、クリアランス制度等はすべて「取引コスト」を下げるためのもの



脅威情報の取り扱いギャップ

■ 同じ情報でも扱うプレーヤー次第で情報の取り扱いが変わってしまい、流通が滞る原因となっている



今後、取り組んでいこうと考えていること

■ **サイバーセキュリティの“大衆化”／“民主化”への対応**

—誰でも「分析」（らしきもの）ができてしまう時代
（例：Virustotal等の検体DB、Shodan／Censys等の検索エンジン等）

—「OSINT」と「OSINT＋α（非公開情報　例：事案対応による分析情報）」との違いや
その理論的整理の必要性

—質の悪い脅威情報（もどき）を市場から適切にはじくための仕組み
（セキュリティ市場の”自浄作用“）

■ **官民連携による脅威情報の作出・活用**

—例：ウクライナにおけるサイバー戦解説について、Microsoftレポート等の「輸入」「翻訳」
だけの情報が流れていて、それでいいのか？

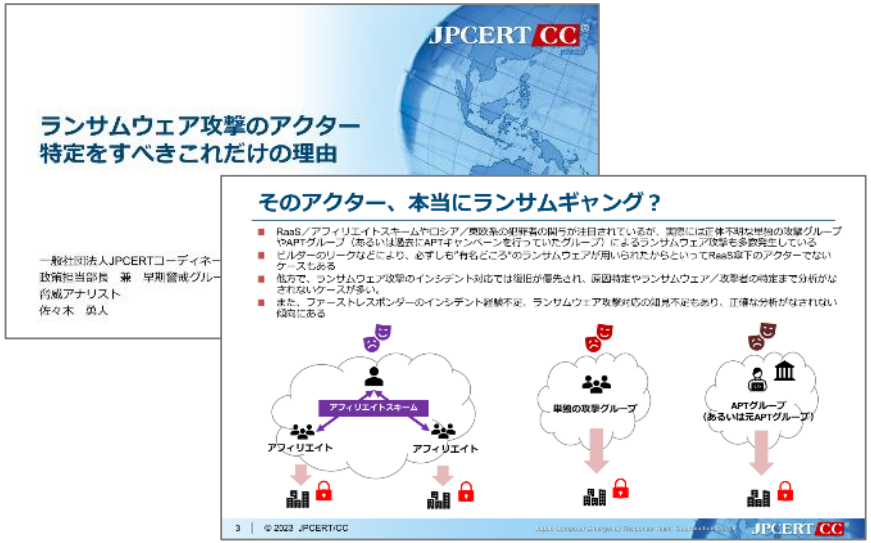
—本当にロシアによるサイバー戦の効果があったのかどうか検証し、今後の日本における備えとして学ぶことや、脅威認識を広く社会全体で共有するために、独自の分析（とのその情報発信）が必要ではないか？

※自分たちの手で分析する、というのは必ずしも「現地にいること」や「一次検体を入手しなければならない」ということではない

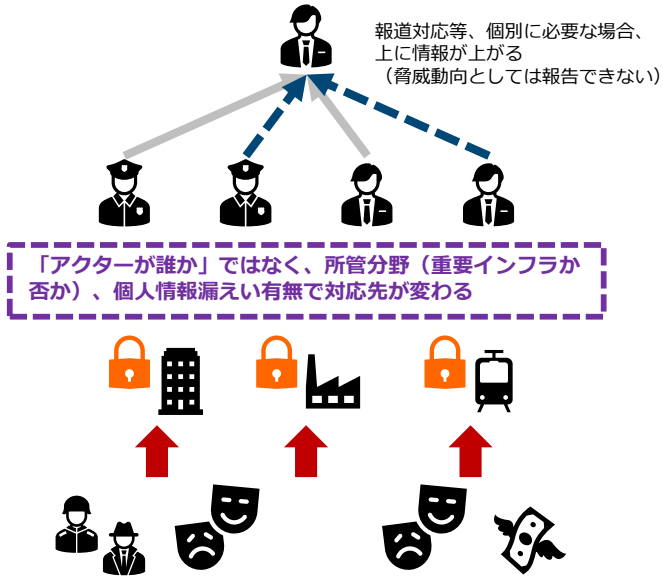
■ **ドクトリン作り（次項）**

ドクトリンの必要性

- リークサイトを用いたり、アフィリエイトスキームを組む、「目立つランサムウェアギャング」が注目されがちである一方、過去のAPTに関与したグループによる活動や現在活動中のAPTグループによる、自己活動資金調達のためのランサムウェア攻撃を“見逃している”可能性が高い
- APTはじめ、サイバー脅威に対する国としての対処指針／ドクトリンがないため、最初に情報を受け取った窓口組織で当該情報を（本来は）どこに共有／報告すべきか否か判断ができない
- “戦術” レベルでは部分最適な対応ができているかもしれないが、 “キャンペーン”単位、戦略単位では失敗している

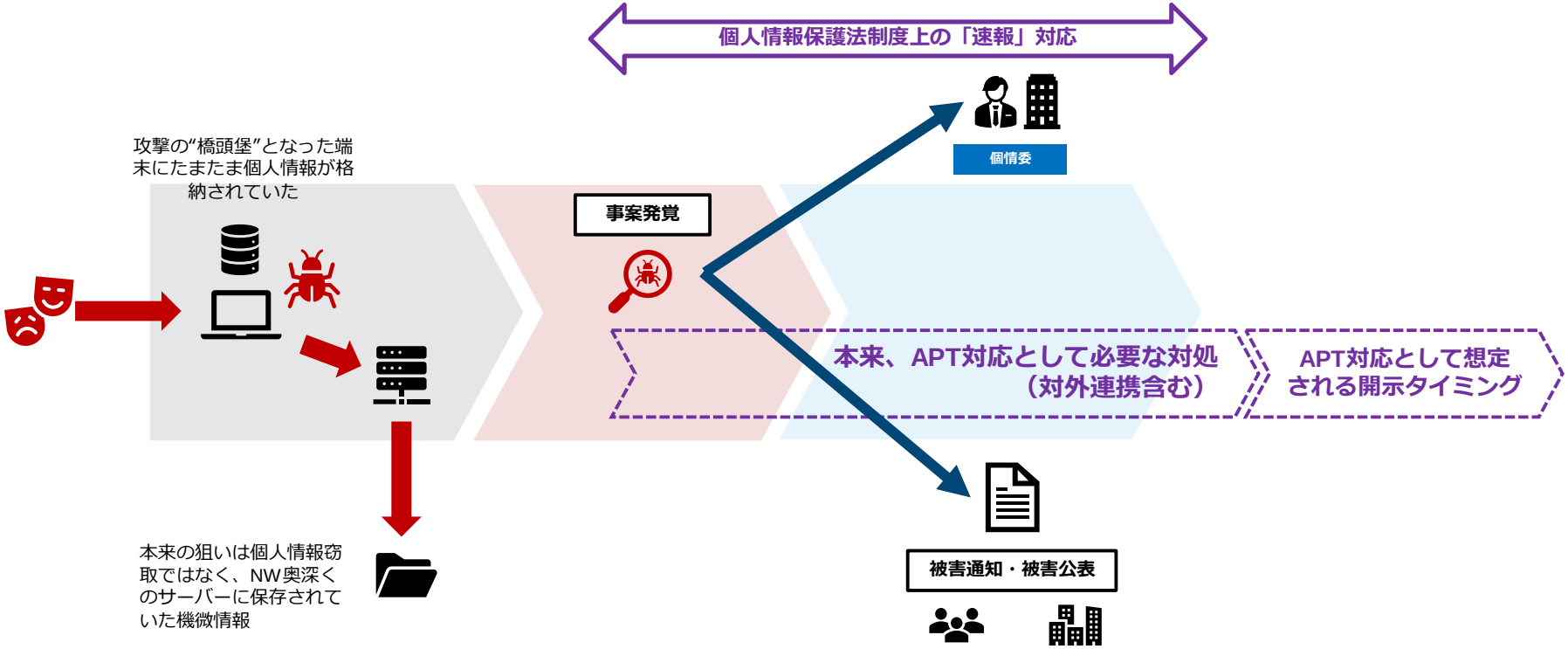


https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_2_6_hayato_sasaki_jp.pdf



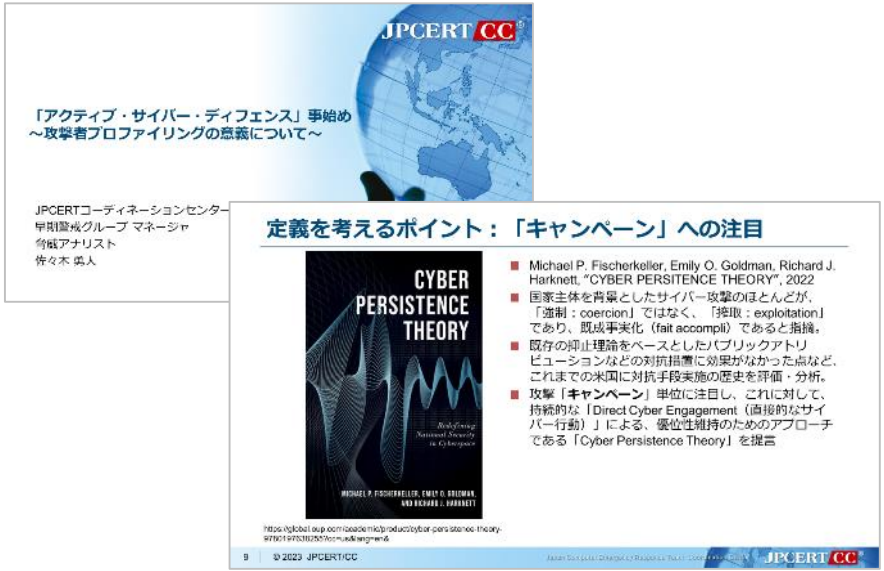
（再掲）国側に情報が提供されない構造的背景②

- 個人情報保護法制度上の「速報」対応や被害個別通知対応に追われ、被害組織は本来の事案対応リソースを消耗（報告対応や公表・対外応答対応）してしまっている。本来その攻撃類型に対して必要な外部連携はなされない

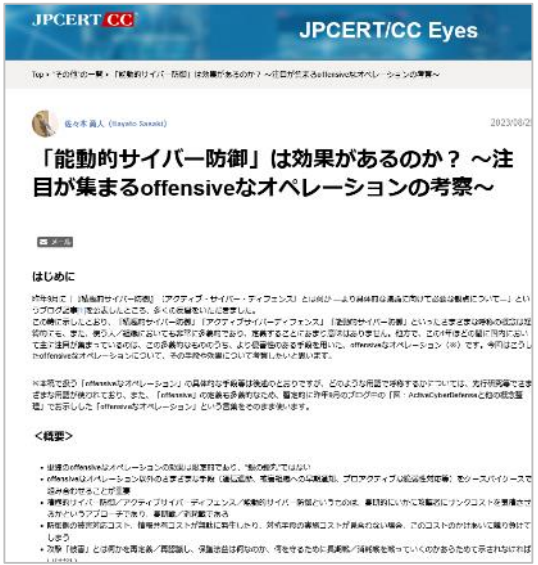


参考：サイバー脅威に対抗するためのドクトリン

- 米サイバー軍など組織／所管範囲内で「ドクトリン」を整備している国はあるものの、国全体としてサイバー攻撃に対処するためのドクトリンを包括的に整備している国はないと認識
- ドクトリン構築にあたっては、アクター／背景国家別に検討することも必要であるが、何よりも「攻撃キャンペーン」単位での作戦術の検討が必要
- 参考：攻撃キャンペーン単位でのドクトリンの必要性に関する先行研究としては、
  Michael P. Fischerkeller, Emily O. Goldman, Richard J. Harknett, “CYBER PERSITENCE THEORY”, 2022

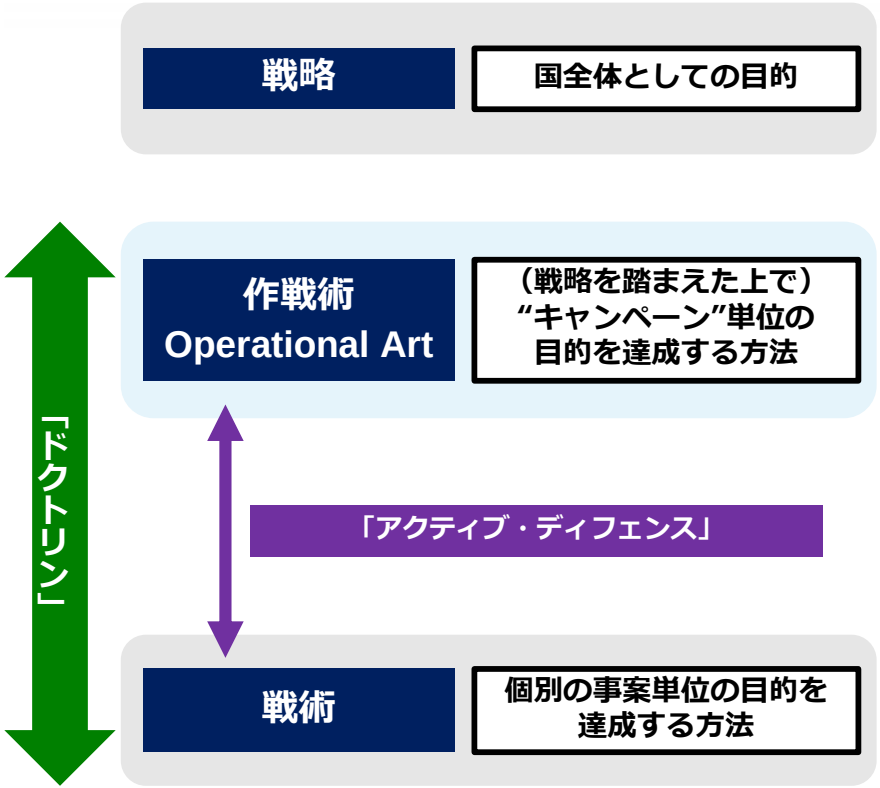


JSAC2023「アクティブ・サイバー・ディフェンス」事始め ～攻撃者プロファイリングの意義について～
https://jsac.jpcert.or.jp/archive/2023/pdf/JSAC2023_2_2_sasaki_jp.pdf



JPCERT/CC Eyes
https://blogs.jpcert.or.jp/ja/2023/08/effectiveness-of-active-cyber-defense.html

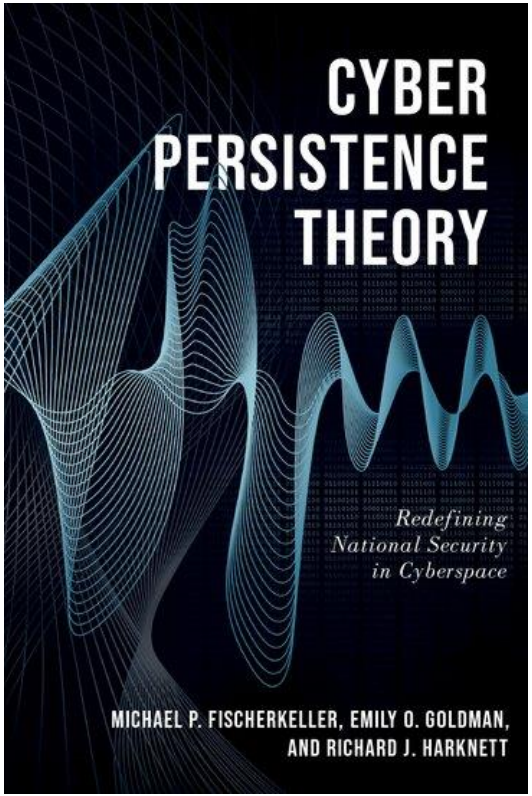
参考：「アクティブ・サイバー・ディフェンス」とドクトリン



- アメリカ陸軍戦闘教義FM100-5（1976年版）に登場する「**アクティブ・ディフェンス**」のコンセプト
- 作戦術（Operational Art）
  - 作戦術は戦役の術（“operational art is the art of **campaign**”（John English, 1996））
  - 作戦術は戦術的成功と戦略的達成点との間をつなぐもの（英統合ドクトリン）
- 「アクティブ・ディフェンス」の概念は戦術レベルに焦点が置かれているとの批判があり、その後、作戦レベルでの克服に向けた改訂が行われていく
- もともと“戦術”レベルである「アクティブ（・サイバー・）ディフェンス」を“作戦”レベルに拡張適用するための改良が必要

参考文献： 北川敬三「軍事組織の知的イノベーション ドクトリンと作戦術の想像力」、デイヴィッド・M・グランツ「ソ連軍＜作戦術＞ 縦深会戦の追及」 ほか

参考：ドクトリンを考えるポイント：「キャンペーン」への注目

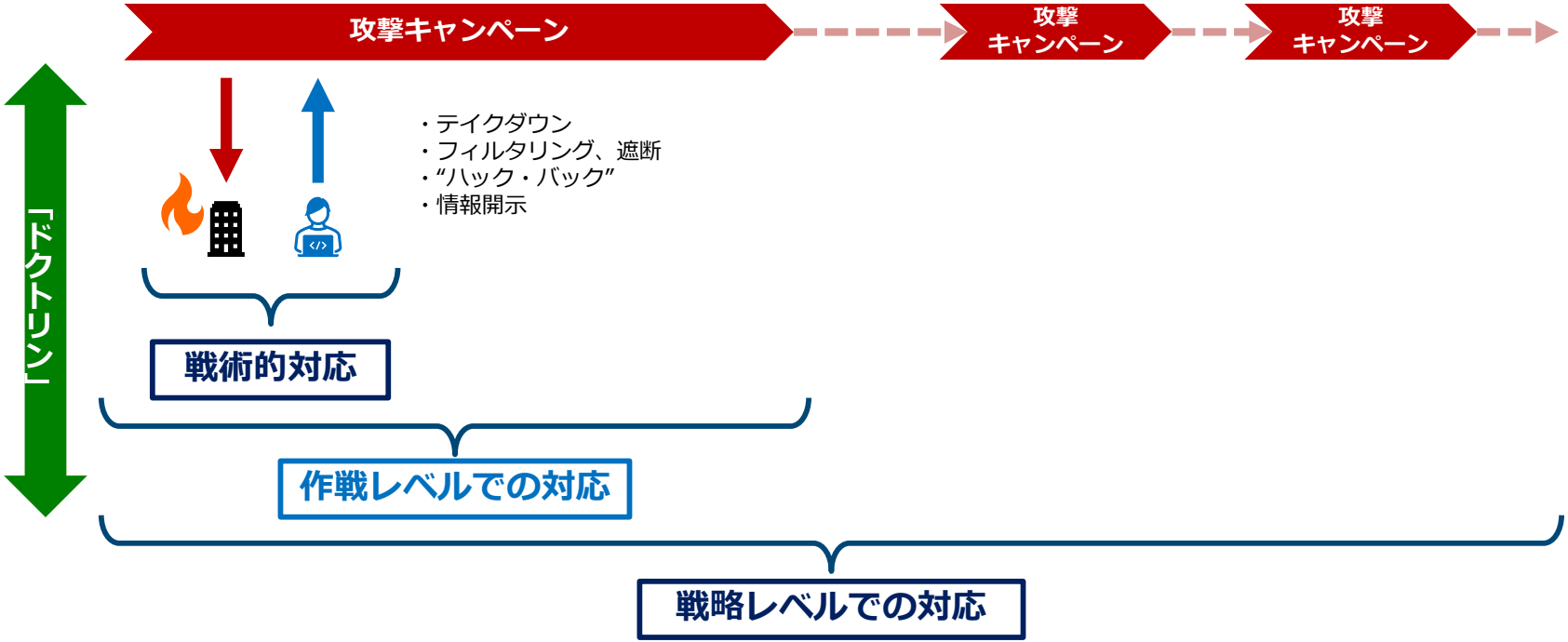


出典：Oxford University Press
https://global.oup.com/academic/product/cyber-persistence-theory-9780197638255?cc=us&lang=en&

- Michael P. Fischerkeller, Emily O. Goldman, Richard J. Harknett, “CYBER PERSITENCE THEORY”, 2022
- 国家主体を背景としたサイバー攻撃のほとんどが、「強制：coercion」ではなく「搾取：exploitation」であり、既成事実化（fait accompli）であると指摘
- 既存の抑止理論をベースとしたパブリックアトリビューションなどの対抗措置に効果がなかった点など、これまでの米国に対抗手段実施の歴史を評価・分析
- 攻撃「**キャンペーン**」単位に注目し、これに対して、持続的な「Direct Cyber Engagement（直接的なサイバー行動）」による、優位性維持のためのアプローチである「Cyber Persistence Theory」を提言

参考：ドクトリンとしての「アクティブ・サイバー・ディフェンス」

- 「縦軸：何に対して、何をするのか」に対して、キャンペーン単位における「横軸：何を目的としていつやるのか」が必要になる



参考：2020年10月 Trickbotへの対抗オペレーションへの評価

KrebsonSecurity
In-depth security news and investigation

HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

Report: U.S. Cyber Command Behind Trickbot Tricks

October 10, 2020 55 Comments

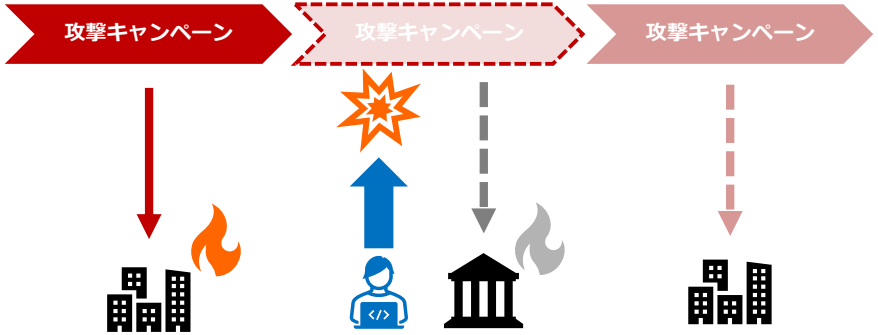
A week ago, KrebsOnSecurity broke the news that someone was attempting to disrupt the **Trickbot botnet**, a malware crime machine that has infected millions of computers and is often used to spread ransomware. A new report Friday says the coordinated attack was part of an operation carried out by the U.S. military's **Cyber Command**.

Image: Shutterstock.

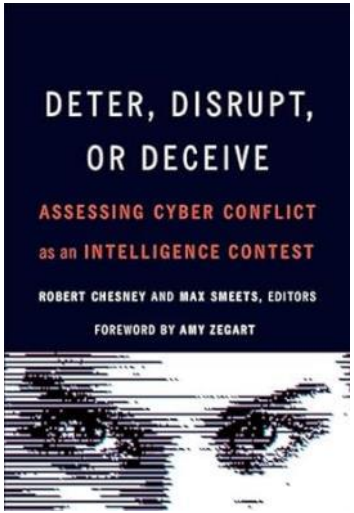
On October 2, KrebsOnSecurity reported that twice in the preceding ten days, an unknown entity that had inside access to the Trickbot botnet sent all infected systems a command telling them to disconnect themselves from the Internet servers the Trickbot overlords used to control compromised **Microsoft Windows** computers.

出典：KrebsOnSecurity
https://krebsonsecurity.com/2020/10/report-u-s-cyber-command-behind-trickbot-tricks/

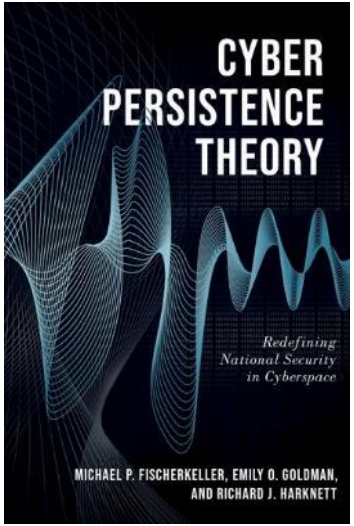
- Microsoftによるドメイン差止手続きの実施
- 加えて、米サイバー軍による「攪乱」作戦が行われた可能性の指摘
- 一連の対応実施後もTrickbotが完全に活動を停止しなかったことから、米サイバー軍の作戦に対しては否定的な見方が相次いだ
- 一方で、この対応は2020年11月の米大統領選挙への事前対応として行われたものであり、当該期間中に大統領選に影響があるような大規模攻撃に悪用されなかったことを評価する見方もある



さいごに



Robert Chesney, Max Smeets, “Deter, Disrupt, or Deceive: Assessing Cyber Conflict As an Intelligence Contest”, 2023



Michael P. Fischerkeller, Emily O. Goldman, Richard J. Harknett, “CYBER PERSITENCE THEORY”, 2022

- いろいろ悲観的なことばかり申し上げましたが…
- 「日本のサイバーセキュリティは世界〇位！」「海外にはあるのに／できるのに、日本ではできていない」といった声と、（非公開の）現場で起きていることとの間には大きなギャップを感じている。（ランキング自体が悪いのではなく、評価軸／評価理論の不在や評価のブレの問題）
- こうした場で官民の有志が集まって議論できているだけ日本は十分にやれている（と思う）
- 脅威インテリジェンスの本当の意味での活用はまだどの国／組織もできていない。包括的な対抗ドクトリンも整備できておらず、また、これまでの理論的な再評価も始まったところ（左記先行研究等）。まだまだこれから議論と実践が成熟していく分野であり、今の時点でランキングもへちまもない