経済産業省

一部非公開

事務局説明資料

（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）

これまでの論点の振り返り及び今後議論すべき論点の整理に向けて

経済産業省
サイバーセキュリティ課

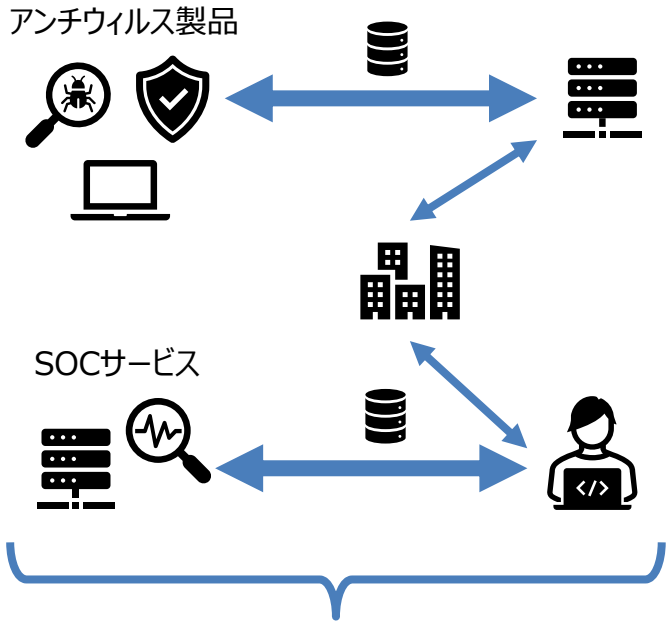
各組織におけるデータの取り扱われ方

- データに適法にアクセスし、その利用をコントロールできる事実上の地位がある場合、または契約によってデータの利用権限を取り決めた場合は、そのような地位をもって、データの利活用が可能とする。
- 組織によってデータの取り扱われ方は異なる。

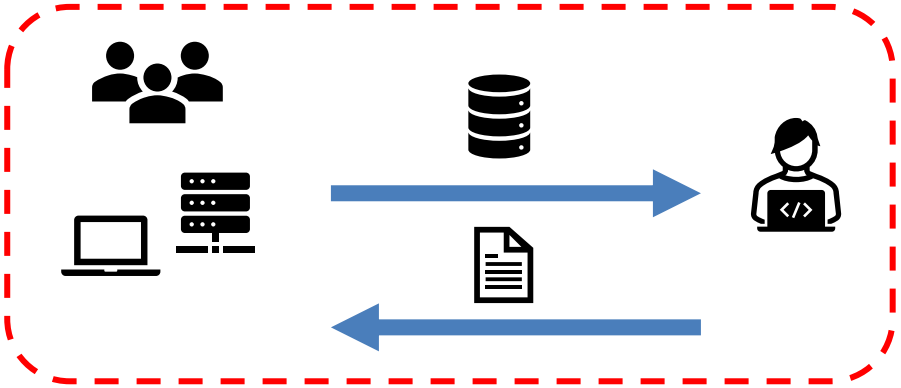
（例）

ーSOC業務は、同時に複数の顧客に対してサービスを提供する。あるデータを分析し、匿名化した場合、SOC事業者において当該匿名化したデータの利活用が可能と言える。

ーインシデント業務においては、契約を基に顧客に対して1対1でサービスを提供する。契約において、データの利用権限を得た場合を除き、被害組織に帰属される情報と整理しうる。



収集したデータの取り扱いは契約／ラインセンスで定めており、取り決めの範囲内でベンダ側が適宜利用可能



基本的に第三者提供等の外部利用を想定していない

情報共有のメリット・デメリット

● （第４回における意見等も踏まえながら、引き続き整理）

●これまでの議論のまとめ

メリット
- アナリスト間で情報共有を行うことで、調査が迅速に進められる。
- 組織のアナリストから受けたフィードバックと、関連する攻撃キャンペーンとのデータの紐付けによりその後の被害防止拡大に役立つ。
- 共有活動参加者が事前に包括的なNDA契約を結んでおくことで、情報展開毎の確認（社内調整など）を省略することができる。
- 事業者にとって、初動対応の参考となる情報を入手できる。

デメリット
- 被害組織が特定されてしまうおそれがあり、その結果情報の隠蔽を疑われる場合もある。例えば、情報共有より先に被害公表が行われていると、いくら匿名化してもその後に共有された情報と、先の被害公表内容とを突き合わせると、ある程度被害組織が絞り込めてしまう場合がある。
- データの共有をするためのコストが発生するおそれがある。

分析対象の「データ」と抽出される「情報」について

- 各事業者が被害組織との間で取り扱う「データ」と、分析の結果として抽出し、外部提供（情報共有など）する「情報」は異なる

データ	種類		共有効果が見込まれる情報	機微な情報を含むか？	（左記以外で）被害組織が推測可能な情報が含まれるか？
各種ログデータ	アクセスログ／イベントログ	元データ		○	
		抽出情報	例：Webサーバへの不正アクセス元情報 例：Webサーバの脆弱性を狙った通信の種類（パス、ポート番号等）	×	
	プロキシログ	元データ		○	
		抽出情報	○ 例：マルウェアの通信先情報	×	△ 標的組織名を模したC2ドメイン名が使われる場合
	FWログ	元データ		○	
		抽出情報	○ 例：マルウェアの通信先情報	×	△ 標的組織名を模したC2ドメイン名が使われる場合
調査対象端末（のデータ）		元データ		○	
		抽出情報	TTPs	×	
マルウェア ※同一検体が公開情報として流通していない場合		元データ			△ 標的組織のシステム情報を事前に内容していたり、感染先で窃取した認証情報を内包する場合
		抽出情報	ハッシュ値、保存先／永続先情報、ファイルサイズ、ファイル名等	×	

サイバー脅威情報の類型

● サイバー脅威情報は以下のとおり整理可能。

脅威情報の種類	情報の内容					各事業者			
	通信先情報	マルウェア情報	左記以外の攻撃手法について	脆弱性情報	攻撃者に関する情報	アンチウィルスベンダ	SOCベンダ	SOC＋インシデント対応	フォレンジックベンダ
						再配信可能だが自社サービス範囲		調整コストがかかる	
インディケーター	○	△ ハッシュ値やファイル名、設置／永続化箇所について	△ 特徴的なイニシャルアクセス方法など、調査が必要な個所について	△ ※左記に同じ	△ ※攻撃グループ名が注意喚起的に、また識別の便宜上用いられる場合があるが限定的	被害組織で検知した情報をもとにサービス上で展開する	左に同じ	※個別のインシデント対応側での利用条件に影響される	被害現場で得た情報をもとにレポート公表したり、情報共有活動に提供される
TTP		○ マルウェアの挙動に関する詳細など	○	△ 脆弱性の詳細が示されるのではなく、脆弱性を悪用してどのように不正な操作をしたのかについて		（被害組織で検知した情報や個別のインシデント対応をもとに脅威インテリジェンスレポートとして公表される）			
セキュリティアラート			△ 右記の補助的に記載される場合がある	△ 脆弱性の詳細が示されるのではなく、概要と影響範囲、修正方法について示される		（※JPCERT/CCから）			
						公表までの相手方等との調整に時間がかかる			
脅威インテリジェンスレポート	上記のIoC、TTP情報がAppendixとして示される				○	被害組織で検知した情報や個別のインシデント対応をもとに脅威インテリジェンスレポートとして公表される			

【参考】「脆弱性（関連）情報」について

悪用に関する情報

悪用有無に関する情報

悪用有無を確認する方法

ログのチェック箇所や設定変更がなされる箇所に関する情報

告示制度上の取り扱い

対策情報

回避方法（ワークアラウンド）や修正方法（パッチ等の入手案内）

脆弱性関連情報（告示上の定義）

脆弱性情報

脆弱性の性質及び特徴を示す情報（脆弱性告示）

「ソフトウエア製品の場合には、製品の名称及びバージョン、その脆弱性によりもたらされる具体的な脅威等からなる。ウェブアプリケーションの場合には、ウェブサイト URL やウェブサイト名等のウェブサイトを識別する情報や脆弱性の種類、現状から想定されるリスク等の情報からなる」（法律面調査）

脆弱性が存在することを検証する方法

脆弱性を悪用するプログラム、指令又はデータ及びそれらの使用方法

「PoC（Proof of Concept：概念実証）、エクスプロイトコード（脆弱性を悪用するソフトウエアのソースコード。攻撃コード。）やコンピュータウイルス等」（法律面調査）

脆弱性の原因となったコード本体

※基本的に製品開発者しか知らず、発見者も認識していないケースが大半

製品開発者との調整時

脆弱性概要情報

製品開発者等に伝える場合の例：
- ○○の実装を用いた製品がありますか？
- ××の技術に関する脆弱性情報が報告されています。該当製品はありますか？
- □□に関する検証ツールが提供されています。使用する必要はありますか？

（JPCERTガイドライン）

脆弱性詳細情報

- 脆弱性の検証方法
- 検証ツール
- 攻撃コード

（JPCERTガイドライン）

情報公表時

注意喚起

- 脆弱性情報
- 対策情報
- 悪用に関する情報

脆弱性情報の公表

- 脆弱性情報
- 対策情報
- 悪用に関する情報※一部

出展の表記：
脆弱性告示：平成29年経済産業省告示第19号「ソフトウエア製品等の脆弱性関連情報に関する取扱規程」
法律面調査：IPA「情報システム等の脆弱性情報の取扱いにおける法律面の調査 報告書改訂版」（2019年）
JPCERTガイドライン：「JPCERT/CC脆弱性関連情報取扱いガイドラインVer 6.1（2019年）

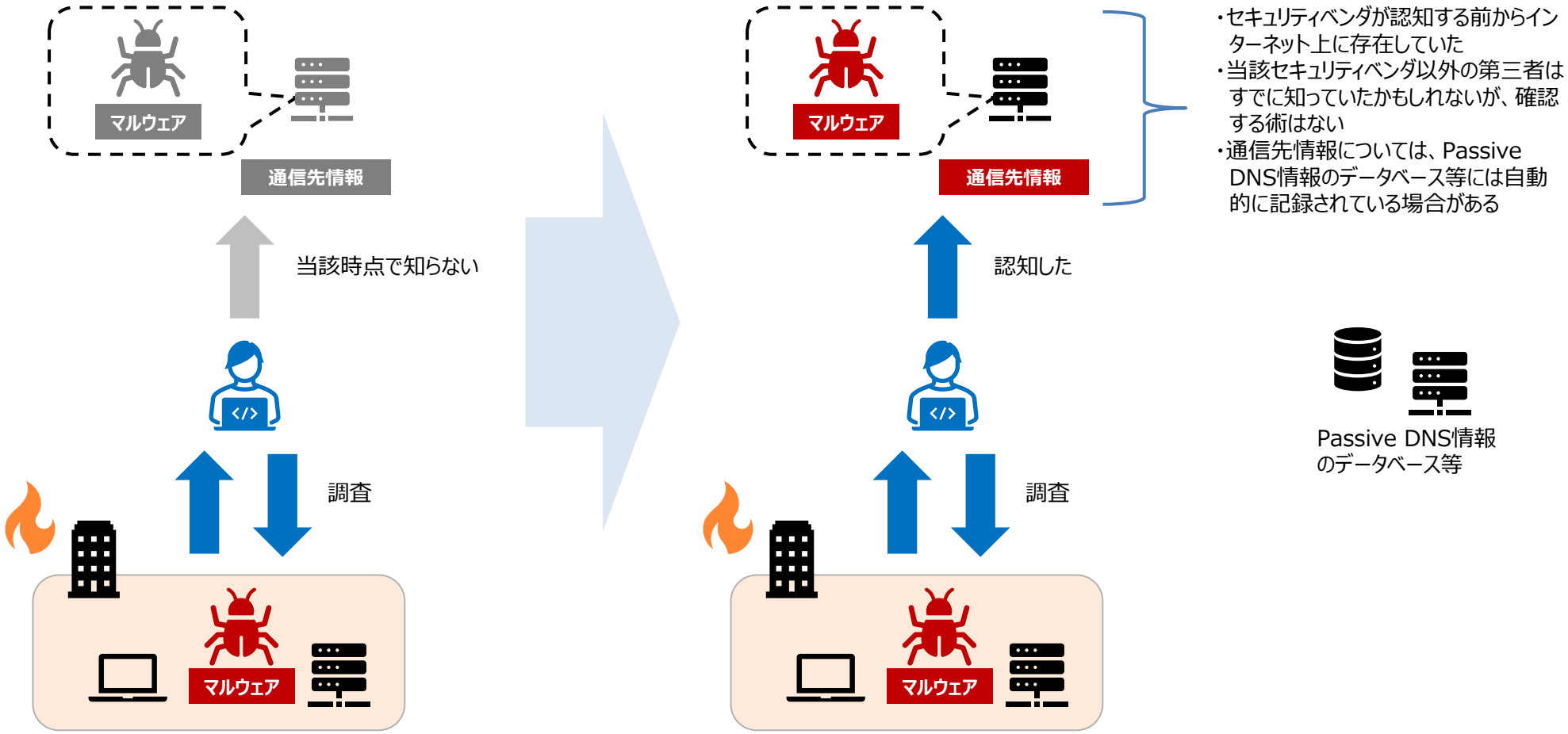
情報共有の対象となり得る情報

- 既にレポートが発出されている等、「公知」となっている場合は、共有可能。

※「公知」の情報：公開レポートが発信されている、オンライン解析サービス上に公開されているといった、正当なルートを通じて、既に公になっている情報

- 一方、「公知」ではないものの、インターネット上等で「公開」されてしまっている情報については、整理が必要。

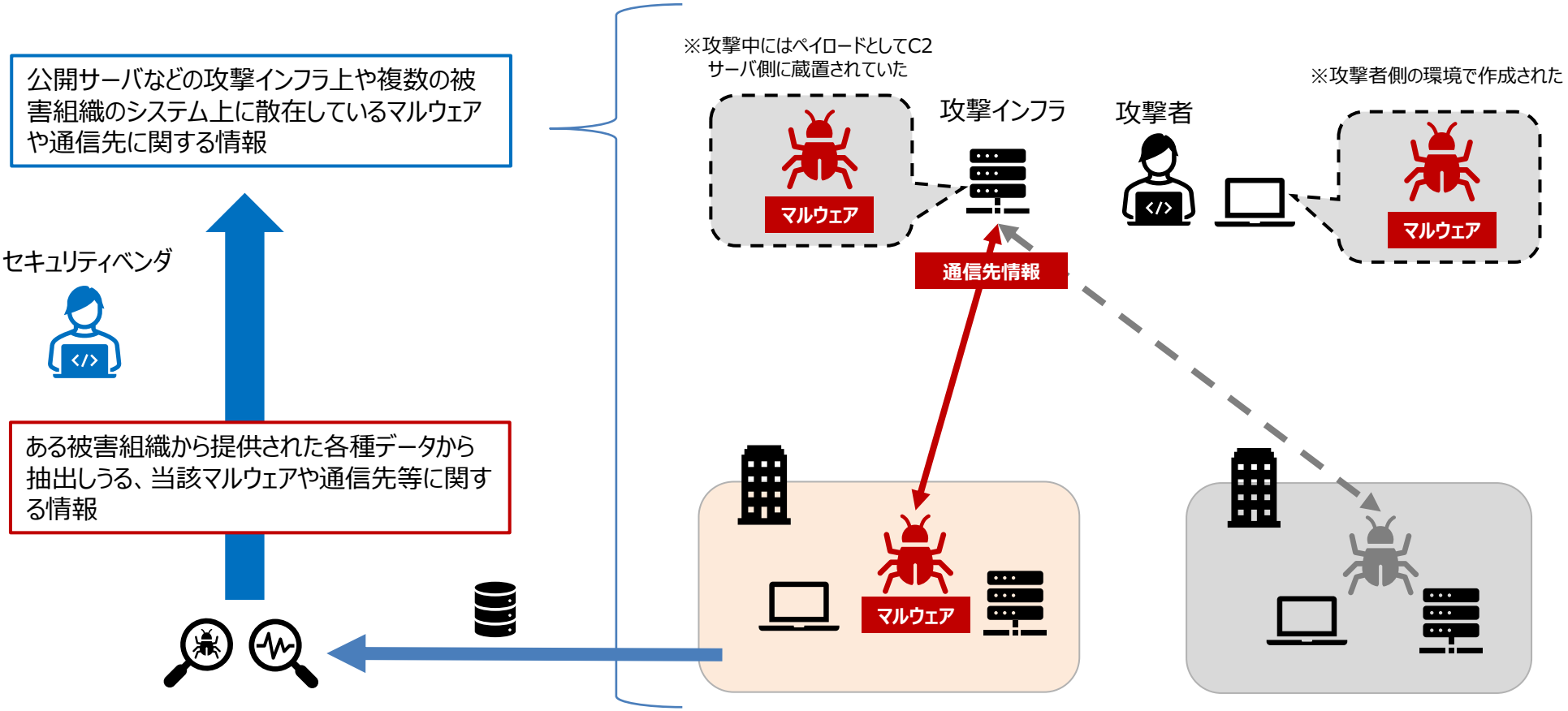
・インターネット上に存在している攻撃インフラに関する情報について、セキュリティベンダは被害対応を通じて認知することになるが、当該情報はそれ以前から公開状態で稼働していた場合、この情報は必ずしも被害組織に帰属される情報ではないのではないか



情報共有の対象となり得る情報

● 「公開」されてしまっている情報について、
ー被害企業を特定し得る情報は、秘密情報であり、情報共有の対象外
ー他方、匿名情報については、秘密情報の例外として、情報共有可能か

・脅威情報が示す情報の大半は、必ずしも、被害現場のデータからのみ生成され得るものではない
・公開情報や、他所でも複数存在している情報をある被害組織から提供されたデータから“発見”しているに過ぎない

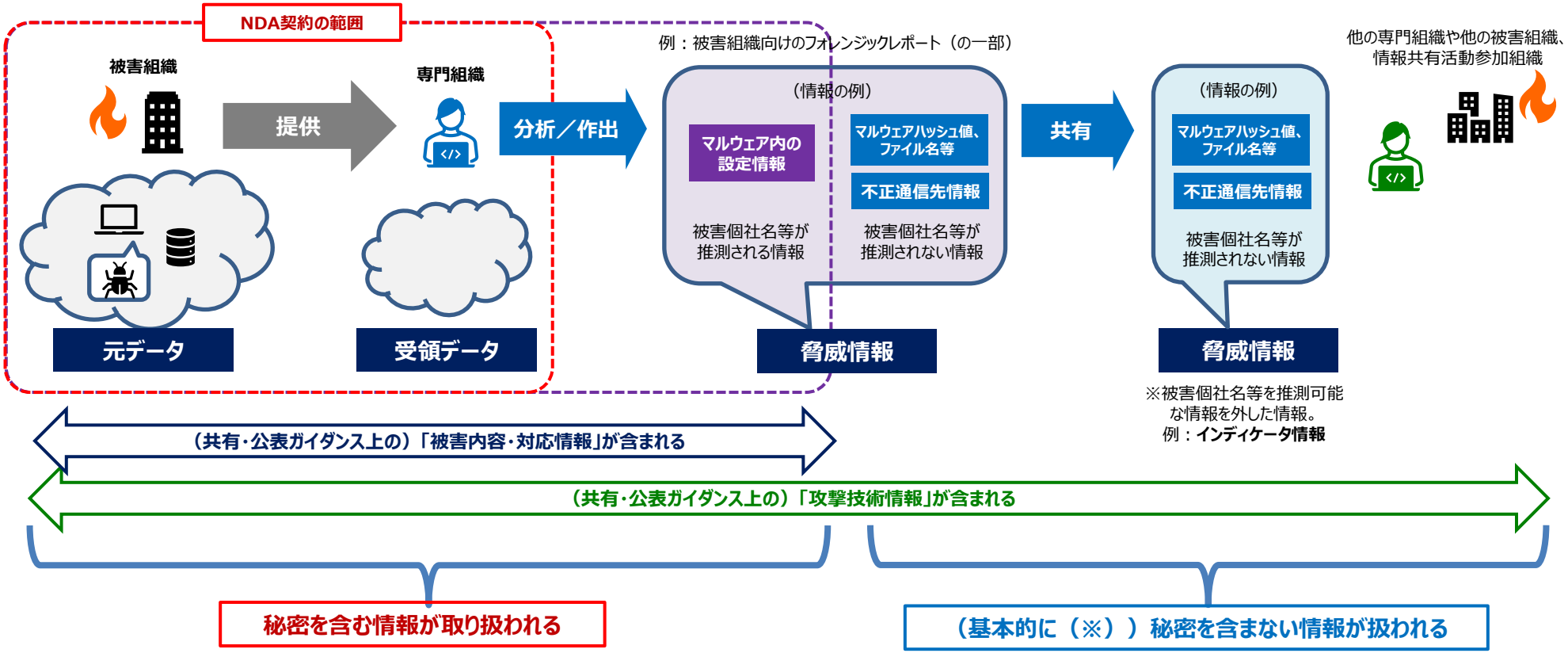


情報共有の対象となり得る情報と情報提供元の匿名化について

		公知でないケース		公知のケース		公開インフラ上に存在する場合		登録制サービス上に当該情報がある場合	
		匿名情報	被害組織を特定しうる場合があるか	匿名情報	被害組織を特定しうる場合があるか	匿名情報	被害組織を特定しうる場合があるか	匿名情報	被害組織を特定しうる場合があるか
通信先		共有可 ※基本的に第三者への共有が可能であるが、現状では便宜上、被害組織の了解を取っていることが多い	推測可能な場合がある ※被害組織名／ドメイン名類似のドメイン名をC2サーバに割り当てるなど、あくまでも「推測／憶測」の範囲内	共有可（※既知の情報であるため共有効果は限定的）	共有可（※既知の情報であるため共有効果は限定的）	※通信先情報の大半は基本的に公開情報として流通している			
						共有可	推測可能な場合がある ※被害組織名／ドメイン名類似のドメイン名をC2サーバに割り当てるなど、あくまでも「推測／憶測」の範囲内	※当該サービスの利用規約情報の情報の利用範囲制限による	
マルウェア	検体そのもの	共有可能であるが、一般体に検体そのものを共有活動上で展開しない							
			推測可能な場合がある ※標的組織のNW設定情報などかなりの確度で「特定組織が狙われている／いた」ことを示す情報が内包されている場合がある		推測可能な場合がある ※標的組織のNW設定情報などかなりの確度で「特定組織が狙われている／いた」ことを示す情報が内包されている場合がある		推測可能な場合がある ※標的組織のNW設定情報などかなりの確度で「特定組織が狙われている／いた」ことを示す情報が内包されている場合がある		
	抽出した情報	共有可 ※基本的に第三者への共有が可能であるが、現状では便宜上、被害組織の了解を取っていることが多い	特定できないように情報を選別して共有するのが一般的	共有可	特定できないように情報を選別して共有するのが一般的	共有可	特定できないように情報を選別して共有するのが一般的		
脆弱性（悪用）情報		脆弱性の修正・公表に係る調整がまず行われる		共有可	推測可能な場合がある ※被害事実が公になっており、侵害経路となった製品が外形上判別できる場合など	共有可 ※Exploitツールが攻撃インフラ上で見つかるケースなど	推測可能な場合がある ※Exploitツールが攻撃インフラ上で見つかり、かつ、攻撃インフラ上に標的組織を示す情報も見つかる場合		
			推測可能な場合がある ※被害事実が公になっており、侵害経路となった製品が外形上判別できる場合など						
脆弱性情報		同上		共有可 ※悪用した攻撃シナリオの概要や侵害調査方法の情報など	同上	同上	同上		
TTPｓ		共有可	推測可能な場合があるが、当該情報を外したうえで共有可 ※個別の製品／サービスを踏み台にしていたり、利用者がごく限定されるようなシステムを攻撃に悪用している場合　→ただ、そのようなケースでは広く情報共有する必要性もなくなる	共有可	推測可能な場合があるが、当該情報を外したうえで共有可 ※個別の製品／サービスを踏み台にしていたり、利用者がごく限定されるようなシステムを攻撃に悪用している場合　→ただ、そのようなケースでは広く情報共有する必要性もなくなる	想定されるケースがない？			

匿名加工された脅威情報の取り扱いについて

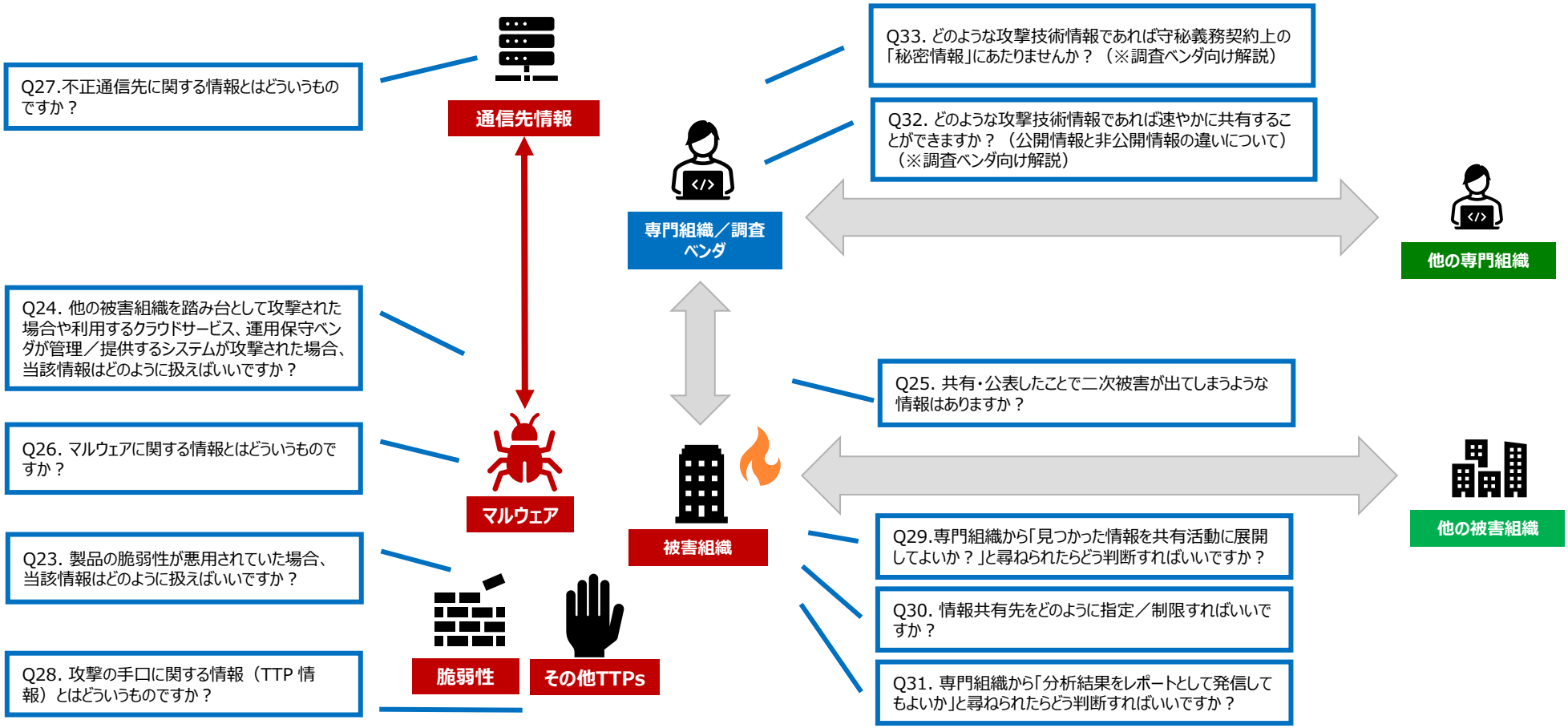
- 被害組織から専門組織に渡される調査対象のデータ（ログデータやフォレンジック対象のイメージコピーなど）と、これの分析により抽出／作出される脅威情報に分けることができる
- 脅威情報は基本的に個別の被害に関する情報は含まれないが、場合によっては攻撃技術情報（※）から被害個社名等を推測可能なケースが想定される（※サイバー攻撃被害に係る情報の共有・公表ガイダンス参照）
- 上記のような被害個社名等を推測可能な情報を除いた、匿名化した情報については、NDA契約における秘密情報とは別に取り扱いができるのではないか



※サイバーセキュリティ協議会では別途規約で定める「秘密」情報を扱うことが可能

共有・公表ガイダンスで示したもの

- 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月公表）において、被害組織やその調査・支援を行う専門組織、調査ベンダを想定した、共有対象情報の概要や取り扱い時の留意点等を示した
- 主に、「どのような情報が共有活動に効果的か」という観点で解説しているため、「どのような情報は被害組織を特定してしまう恐れがあるか」という被害者保護の観点や、秘密性／匿名性の観点は限定的な記載にとどまっている（例：Q32内の＜通信先情報について＞における被害組織を特定可能な情報がC2サーバから入手できてしまう可能性への言及（ガイダンス116ページ））



ケース：マルウェア情報

- 検体そのものは下記の通り、被害組織を特定できる情報が含まれていることがあるため、基本的には解析後の情報を共有する
- インディケータとして共有される場合：マルウェア名（検知名）、（感染先で確認された）ファイル名、検体のハッシュ値、ファイルサイズ、通信先
- 専門組織同士で共有する場合（※上記に加えて）挙動に関する簡単な解説（通信プロトコル、次に生成する／ダウンロードするファイルなど）、VirusTotal等公開情報有無、既知の類似検体の有無（類似の検体に言及しているレポートなど）

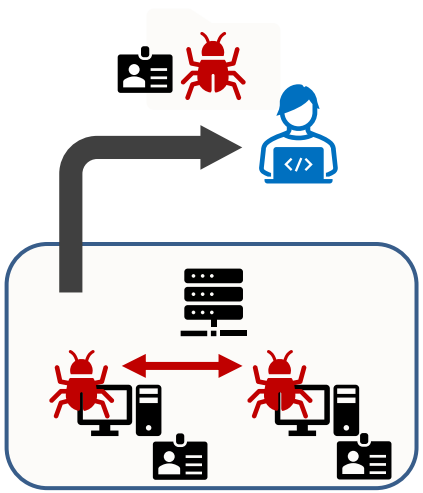
検体そのものが流通することで被害組織が特定／推測されるケース

参照：第1回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　資料2-2 JPCERT/CCからの論点提示資料

ケース①

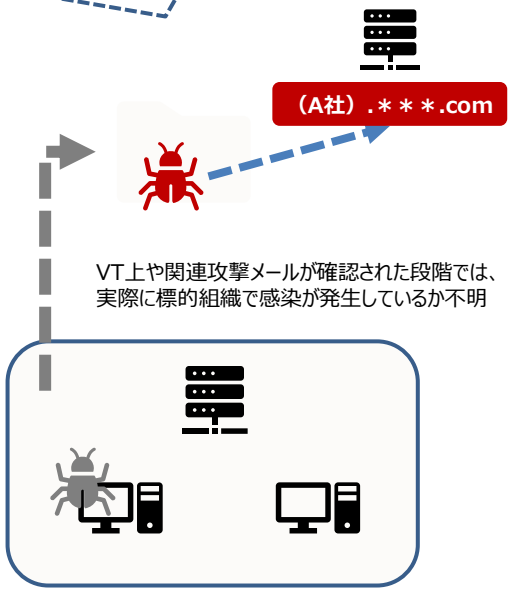
感染時に収集したクレデンシャル情報を含むケース
⇒ID＝メールアドレスのドメインから被害組織が推測されうる

【例】 Olympic DestroyerのVT上にあがった検体



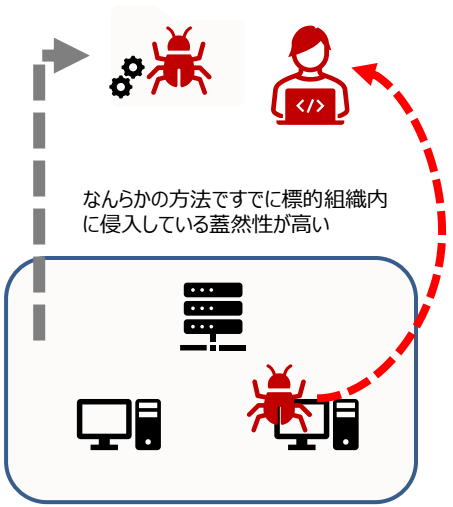
ケース②

検体内部やハードコードされたC2のドメイン名内に標的組織の略称（ドメイン名など）を含むケース
※検体だけでなく通信先情報だけでも推測できる場合もある



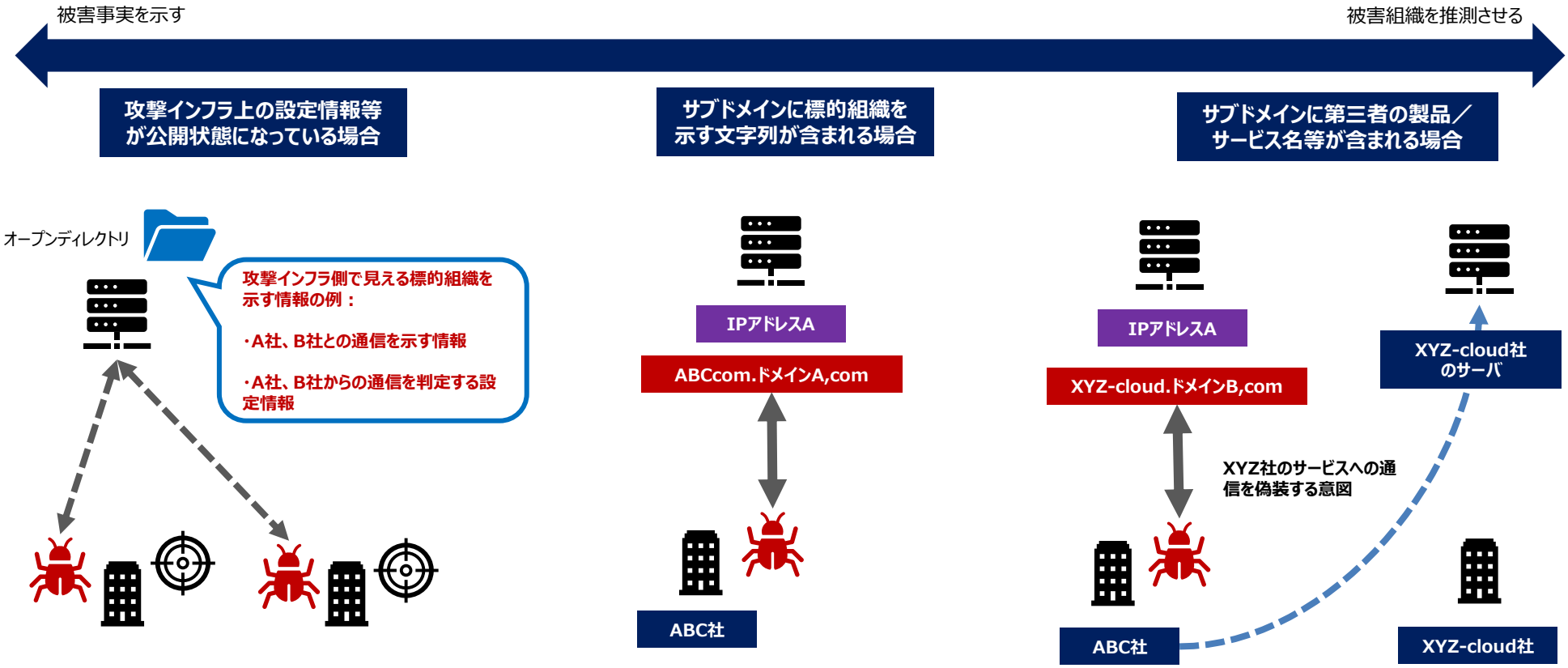
ケース③

標的組織のプロキシサーバなどNW内部の設定情報を検体内に含むケース



ケース：通信先情報

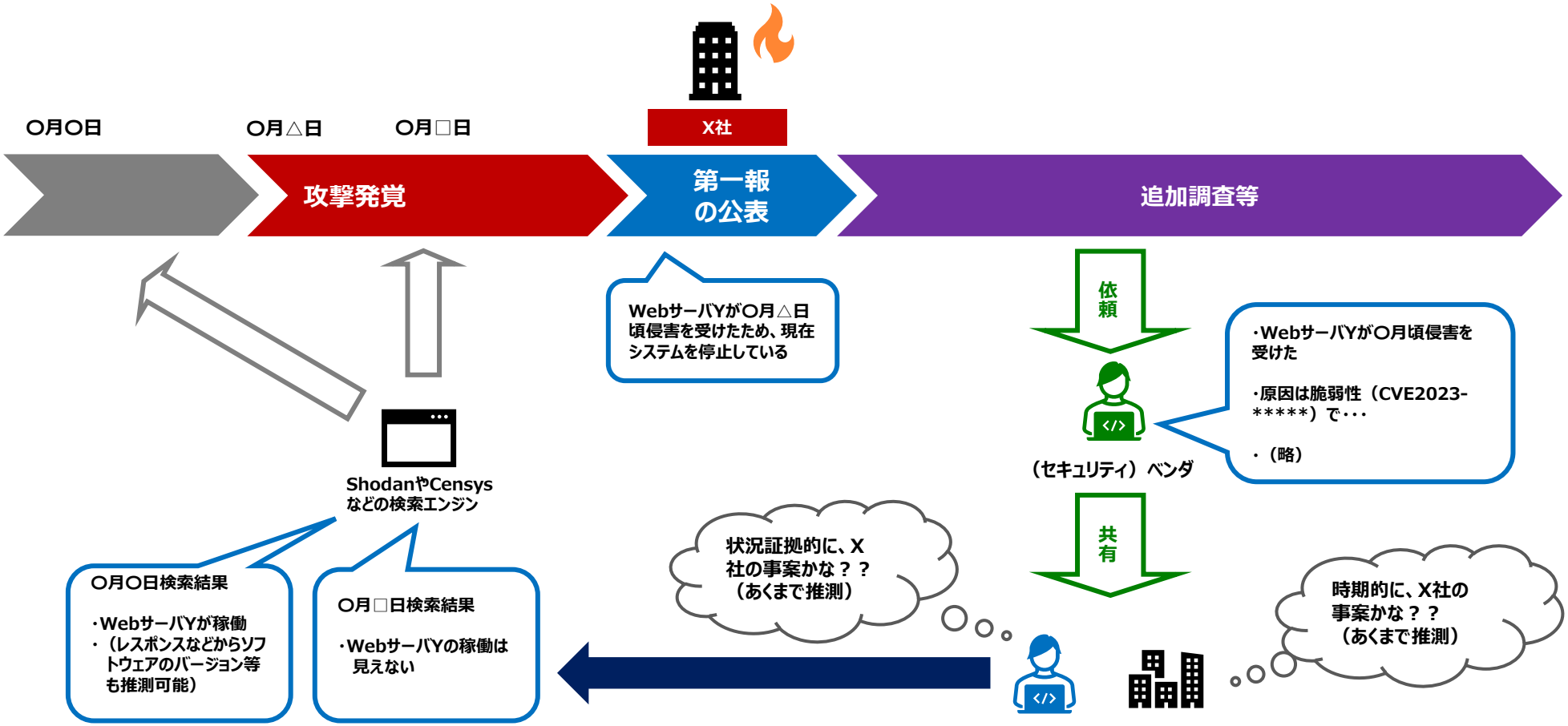
- 通信先情報そのものや通信先情報を共有することで通信先を調査する者が増えたことで、被害組織が特定されたり、あるいは推測されたりする状況が発生する
- あくまで推測するに過ぎない情報が大半であるところ、他の情報（攻撃時期／被害分野／当該被害組織固有のシステム／サービスに関する情報等）と組み合わさることでその“精度”があがることはあるが、あくまで「推測」に過ぎない



参照（右半分）：第1回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　資料2-2 JPCERT/CCからの論点提示資料

ケース：先に公表されている被害組織と結びつく情報

- 被害組織からの公表が共有より先に行われている場合、匿名化した情報を共有したとしても、先に行われた公表内容と結びつき、被害組織を推測させる場合がある。（※ただし、同種の攻撃被害が複数発生している場合、かならずしも特定になるわけではない）
- Webサーバなどのインターネット検索エンジンに情報が残るシステム等が侵害を受けた場合、過去の検索結果なども紐づき、被害組織の推測に至る場合がある（※この場合も、上記と同じく、推測でしかないケースが大半）
- 公表内容（使用しているシステム／サービスなど）から、当該組織が一意に特定される場合、公表前の速やかな共有や、他にも（非公表）被害組織が存在していないか情報共有活動を通じて情報を得るなどの配慮が必要

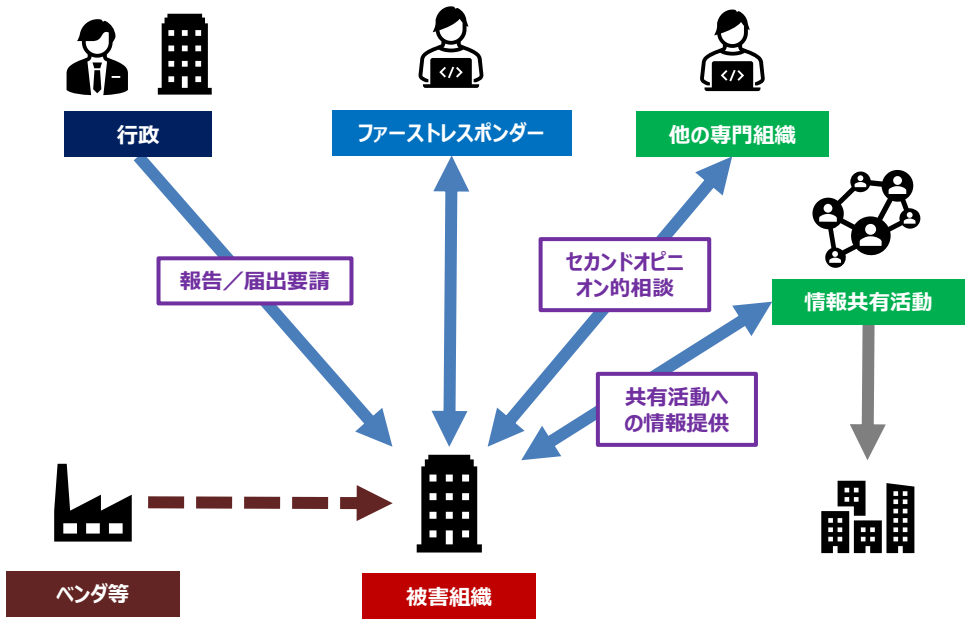


情報共有の目指すべき在り方

- 被害組織自体が情報共有を行う場合、その調整コストの負担が大きく、また、情報共有するか否かについての判断が各被害組織では難しいため、情報の共有がされにくくなる可能性がある。
- 様々な事案を対応し、より専門的知見のある専門組織が情報共有を行うことで、社会全体で効率的な情報の活用がなされる。

情報共有等のコスト負担の現状

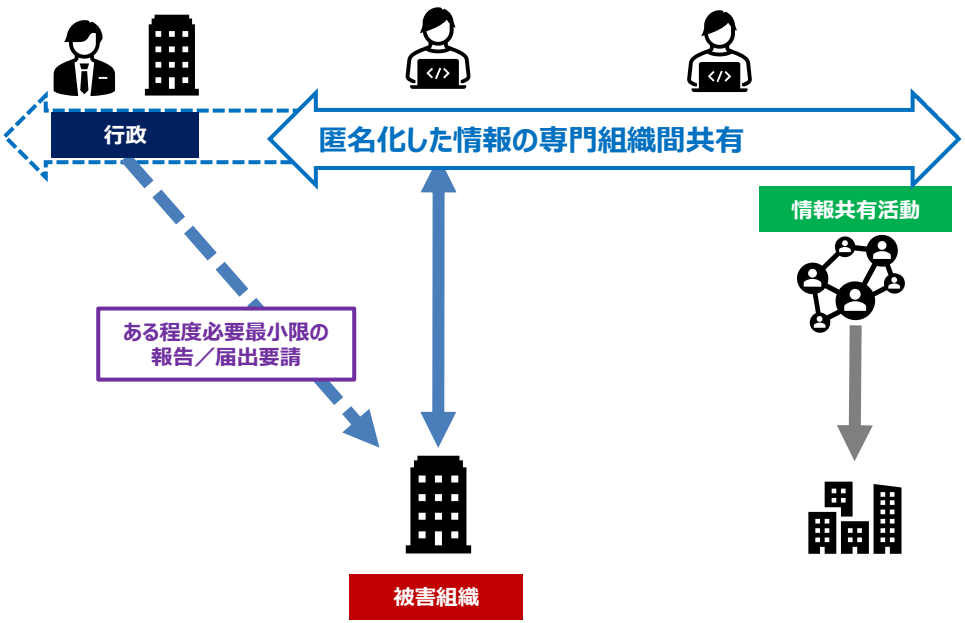
・被害組織による調整コスト負担が大きい状況
・脅威情報の効果的な使い方ができるかどうかは被害組織の知見／判断次第になってしまっている
・特定サービス／製品の悪用情報については極めて流通しにくい構造になっている



特定のサービス／製品の悪用情報の共有ついて、被害組織単独で判断できない

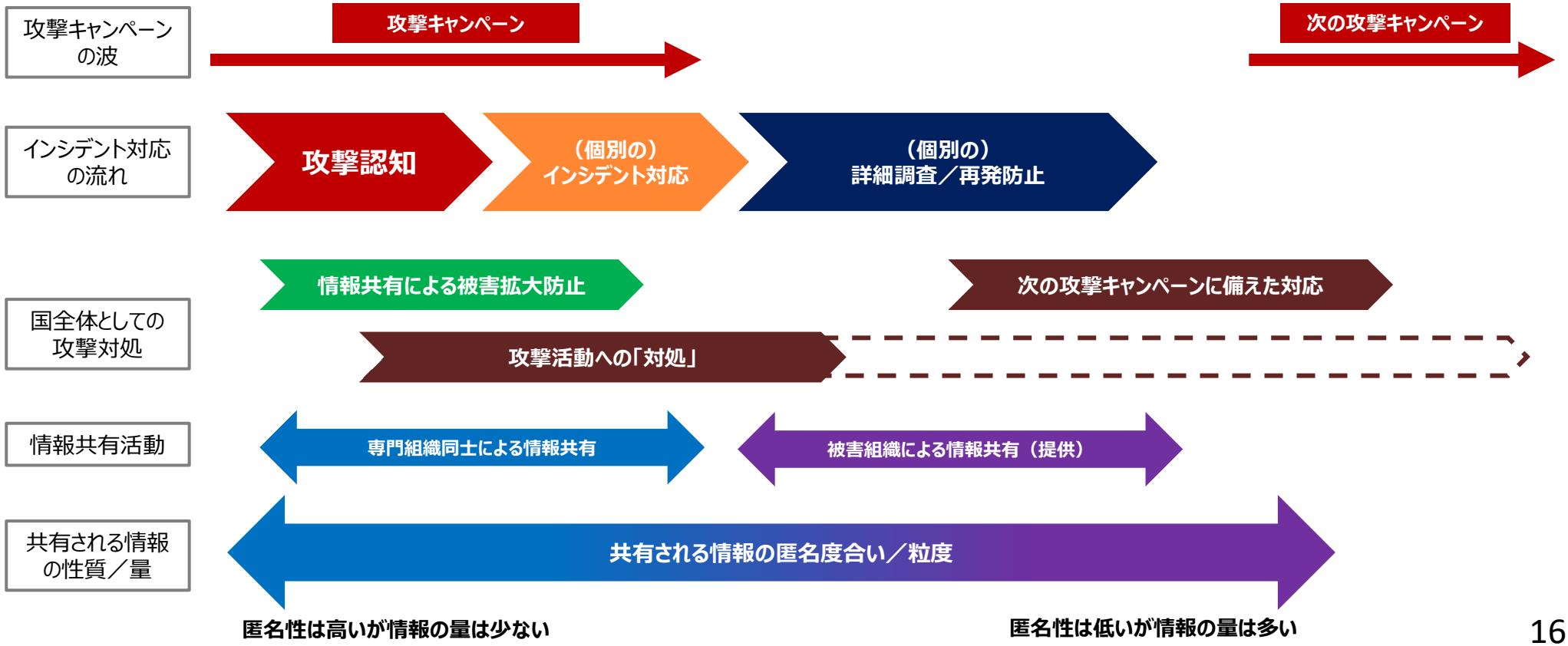
被害者組織のコスト負担を軽減する情報共有

・匿名化した攻撃技術情報については専門組織同士が速やかに共有を行い、被害調査のための追加情報作出や被害拡大防止のための共有活動、注意喚起等に活用する
・少なくとも個別の被害組織よりは専門的知見のある専門組織等が脅威情報をハンドリングすることで社会全体として効率的な情報の活用がなされる



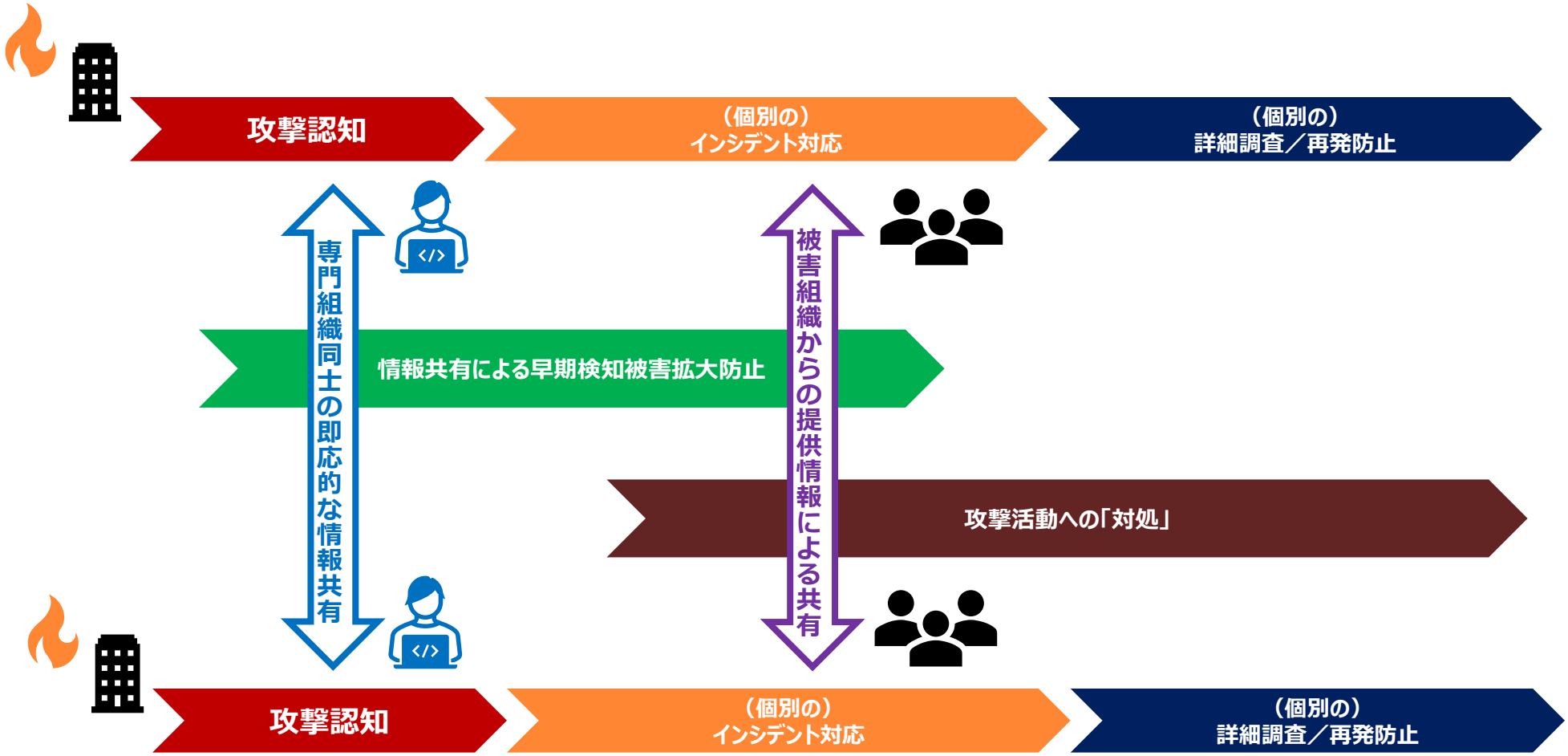
情報共有範囲（１）

- 専門組織同士が即応的に行える情報共有で共有できる情報の種類には限界があり、基本的に攻撃の早期検知や被害拡大防止フェーズまでにおいて有効な取組となる
- 攻撃の全容解明や中長期的な攻撃への対抗のためには詳細な攻撃情報が必要になり、匿名性の低い情報も必要になってくる



情報共有範囲（２）

- 匿名性が高い情報を専門組織が扱う即応的な情報共有と、匿名性が薄れるが詳細な情報を被害組織または専門組織が代理となって情報共有活動等に情報提供される情報共有活動の2段構えが必要なのではないか？



専門組織同士で共有する場合の例

- 実際には口頭やプレゼンテーション資料を用いて説明されることが多い
- 被害組織（情報提供元）が特定されない情報に限定しつつ、他組織での被害調査や、共有先の他の専門組織の対応事案との照合が可能な情報が記される

アクターXによるものと思われる□□□SSL-VPN製品の脆弱性を悪用した攻撃事案を国内で確認したので共有します。他に情報がありましたら是非共有お願いします。

【 概要 】

攻撃発生日時：2023年〇月頃と思われる（※詳細は現在調査中）

□□□SSL-VPN脆弱性を悪用して侵入したのち、侵害端末にマルウェアYを感染させ、通信先Zに通信をし追加のマルウェアをダウンロードするとおもわれるが、調査時点ではペイロードの取得はできなかった。また、その後の横展開でどこまで侵害拡大するかは現在のところ不明にて、調査中。

初期侵害経路：
□□□SSL-VPNのログに以下の痕跡があり、同製品の×月に公表した脆弱性（CVE-2023-＊＊＊＊＊）を悪用したものと思われる。

（痕跡が残る先のパス）
（アクセス時のユーザー名や記録されるイベントなどその他ログ上に残る特徴）

【 IoC 】

〇マルウェアY
MD5：
SHA-256：
ファイル名：
備考：下記通信先から追加のマルウェアをDLすると思われるが、調査時点でペイロードは取得できず。×××機能などの箇所がマルウェア***に酷似しているが、現時点で関連性は不明
参考情報：202×年△月　〇〇〇セキュリティ　***マルウェアに関するレポート
URL：（省略）

〇通信先Z
sslvpnconnect.*******[.]biz　443/TCP(HTTPS)
203.0.1113[.]***（攻撃発生時期に上記FQDNが紐づいていたIPアドレス）

【共有のポイント】
攻撃発生時期
国内事案か海外事案か

【共有のポイント】
自組織でどこまで把握できていて、どこから先は調査でわからなかったのかを示す

【共有のポイント】
既知（過去）の公開情報との関連性や、これまでの同種事案の分析の蓄積からの見解を示す

【共有のポイント】
どういった初期侵害経路だったのか、だけでなく、他の被害組織における調査に資する調査ポイントを示す

【共有のポイント】
取り急ぎの共有が求められる場合、速報的に動的解析等で判明した断片的な情報を記す場合もある

今後の論点

●情報共有に向けた官民連携について

・民間事業者の予防措置や適切な初動対応含め、サイバー攻撃に対して国全体の被害を最小化するためには、重要事案について適切に情報共有されるよう官民での連携が必要ではないか。その際、民間事業者からの効率的な情報提供のあり方も考慮（標準的なフォーマットの整備等）しつつ、被害組織がアプローチしやすい適切な窓口の設定・活用・周知等が必要ではないか。

・また、民間事業者からの情報収集のみならず、政府から民間事業者にとって有益な情報提供を行う等の支援が可能な環境を整備すべきではないか。

●国への情報提供のあり方の整理

・政府が重要な事案を把握し対応を検討するためには、攻撃技術情報、被害情報等の共有を受ける必要がある場合がある。この際、被害組織が迅速に必要な情報を提供できない等の場合には、被害組織ではなく、当該組織からの委託先（セキュリティベンダやSOC事業者等）から代理として情報共有を受けることが有効な場合があり得る。こうした場合において、委託先から行政への円滑な情報共有が可能なようにすべきではないか。

●サプライチェーンにおけるベンダ等の役割について

・サイバー攻撃の被害拡大防止のためには、システム等を販売した事業者等を通じて脆弱性等が迅速かつ確実にユーザーに共有されることが重要。そのため、事業者等がサプライチェーン上流からの脆弱性等の情報を把握したうえで、当該情報を必要なステークホルダーに提供することを推進するような施策の検討も必要ではないか。