サイバー攻撃による被害に関する情報共有の促進に向けた検討会最終報告書

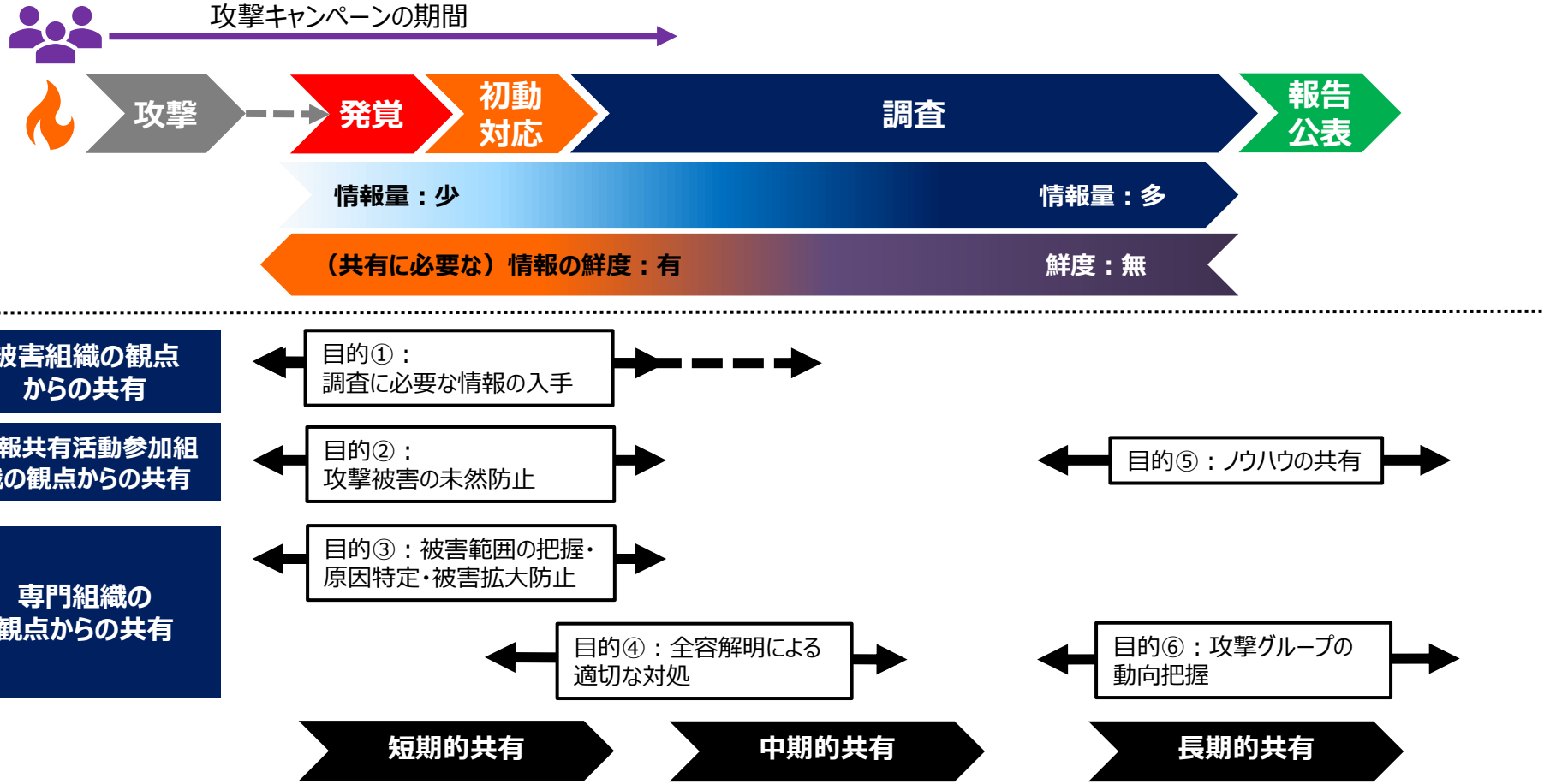
令和５年11月22日

サイバー攻撃による被害に関する情報共有の促進に向けた検討会事務局

１．情報共有の重要性と現状の課題

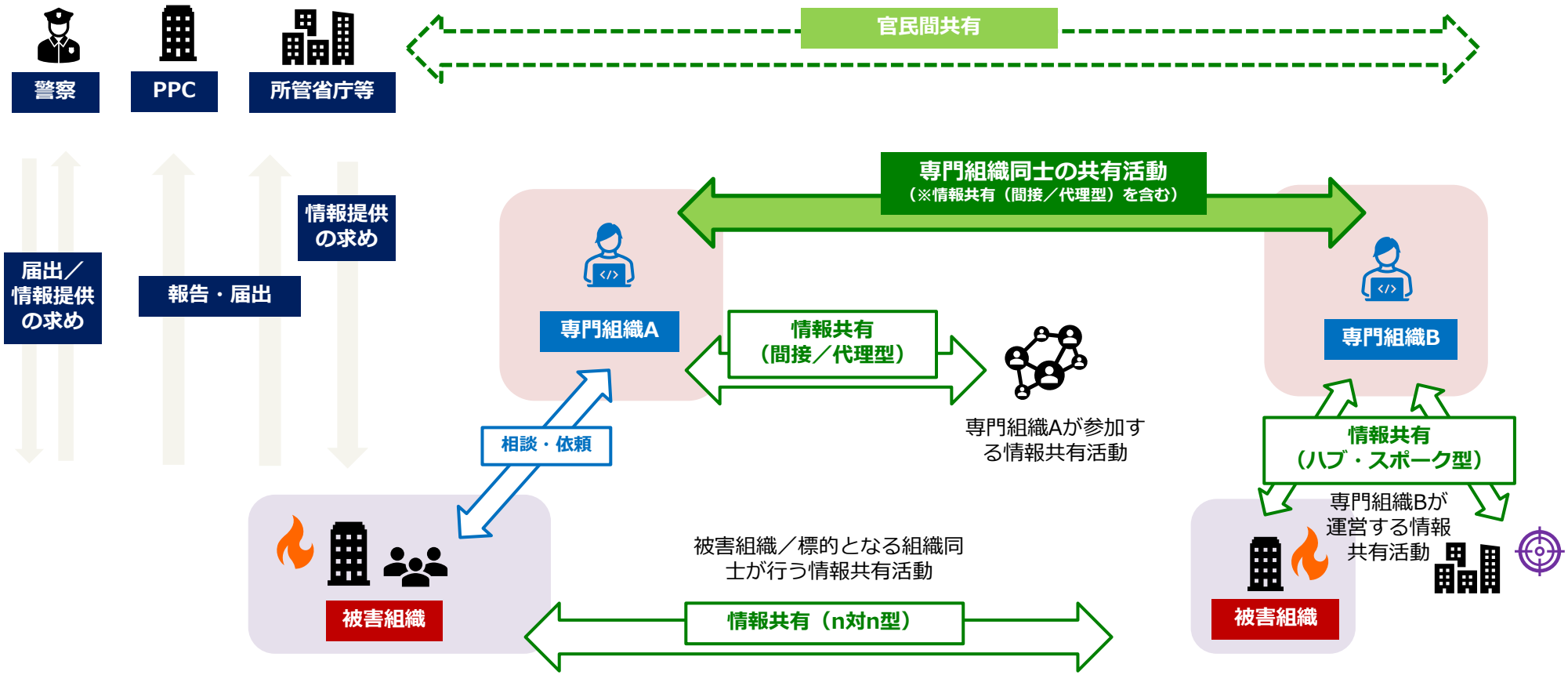
サイバー被害に係る情報共有の重要性

- サイバー攻撃が高度化する中、単独組織による攻撃の全容解明は困難となっている。そのため、攻撃の全容の把握や被害の拡大を防止する等の観点からサイバー攻撃に関する情報共有は極めて重要。
- 情報共有については、短期的には一つの機関だけでは情報量が少ない間に、情報の鮮度がある早期に行うことで効果を最大化することが可能。さらに、中期的、長期的な観点でも情報共有が重要。
- 情報共有の実施により、①被害組織の観点からは原因究明調査に必要な情報の入手【短期】、②情報共有活動参加組織の観点からは攻撃被害の未然防止【短期】やノウハウの共有【長期】、③専門組織の観点からは被害範囲の把握・原因特定・被害拡大防止【短期】、全容解明による適切な対処【中期】、攻撃グループの動向把握【長期】といったことが可能になる。



各組織間での情報共有の全体像

- 情報共有については、主に①被害組織／標的となる組織同士が行う共有、②被害組織と専門組織（専門機関やセキュリティベンダ）間での共有、③専門組織同士で行われる共有、さらには④官民間での共有などが挙げられる。



被害組織からの行う情報共有・公表のメリット・デメリット

- 被害組織が自ら情報共有や公表を行うことに対しては、レピュテーションリスクを懸念する声が聞かれるものの、情報共有や公表により、被害組織における被害拡大防止や、事案対応コストの軽減につながるといった利点もある。

＜メリット＞

- ステークホルダーへの説明責任を果たすことができる。
- 被害組織が情報を公表することで、広報対応等の負荷が軽減され得る
- 事業者にとって、初動対応の参考や攻撃被害の未然防止につながる情報を入手できる。

＜デメリット＞

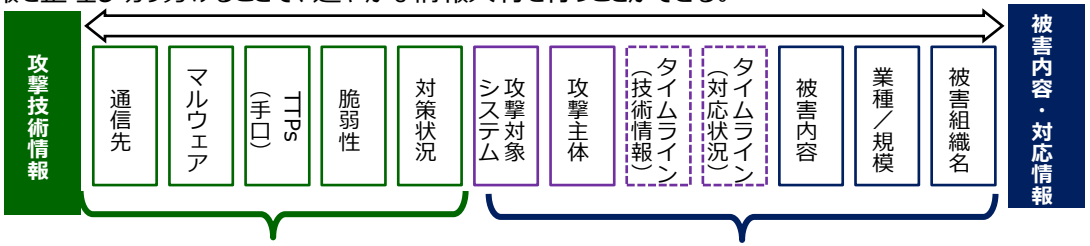
- 被害組織が特定されてしまうおそれがあり、その結果情報の隠蔽を疑われる場合もある。例えば、情報共有より先に被害が意図せずに公表が行われていると、いくら非特定化してもその後に共有された情報と、先の被害公表内容とを突き合わせると、ある程度被害組織が絞り込めてしまう場合がある。
- データの共有をするためのコストが発生する可能性がある。

サイバー被害に係る情報共有ガイダンスの策定と現状の課題

- 主に被害組織の担当部門向けに、被害組織を保護しながら、如何に速やかな情報共有や目的に沿ったスムーズな被害公表が行えるのか、実務上の参考となるポイントFAQ形式で整理した「サイバー被害に係る情報共有ガイダンス」を令和５年３月に公表。
- しかし、サイバー攻撃被害組織等における情報共有に関して複数の課題が存在。

どのような情報を？（様々な種類・性質の情報が存在）

情報を整理し切り分けることで、速やかな情報共有を行うことができる。



基本的に個別の被害組織には紐づかず、対応初期で見つかりやすく、早期に情報共有しなければ効果を得られない情報

ある程度調査期間を経なければ判明しない情報や、ステークホルダー等との調整が必要な機微な情報などが含まれるため、公表までに時間がかかる情報

どのタイミングで？（サイバー攻撃への対処の時系列を意識）

どのような主体と？（様々なサイバーセキュリティ関係組織が存在）

専門組織　情報共有活動　所管省庁等　警察　各種ステークホルダ

想定読者（被害組織等）

セキュリティ担当部門　法務・リスク管理・企画・渉外・広報部門

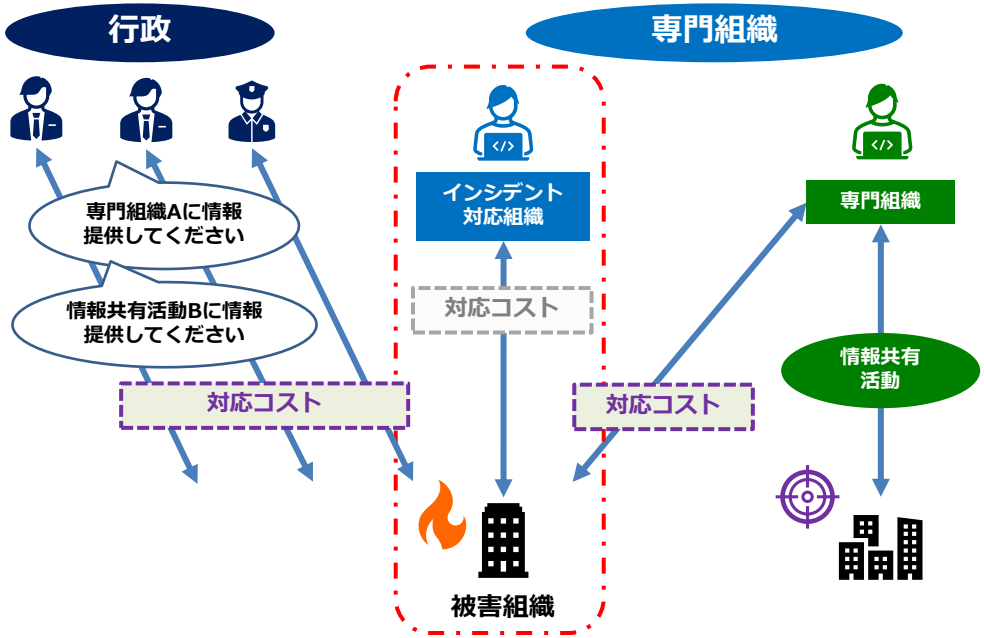
運用保守ベンダ等

問題①：被害組織側の調整コスト負担

- 被害組織が（社会全体の）情報共有のための調整コストを負担している状況にある。被害組織自身の情報共有メリット ＜ 公益目的の負担（他の組織のメリットのための負担） ＋ 情報共有コスト となってしまっている。
- 本来、情報共有により様々なメリットを得られるところ、現状は被害組織（あるいは標的となり得る組織）側の対応コスト／調整コストの負担が大きいため、情報共有活動そのものへのハードルが高い状態になっている。
- インシデント対応や情報共有活動のハブ組織として活動している専門組織同士の情報共有が行えれば、被害組織による情報共有コストを軽減することができるのではないか。
- 同様に行政機関への情報提供等についても何等かの対応コスト低減が望まれる。

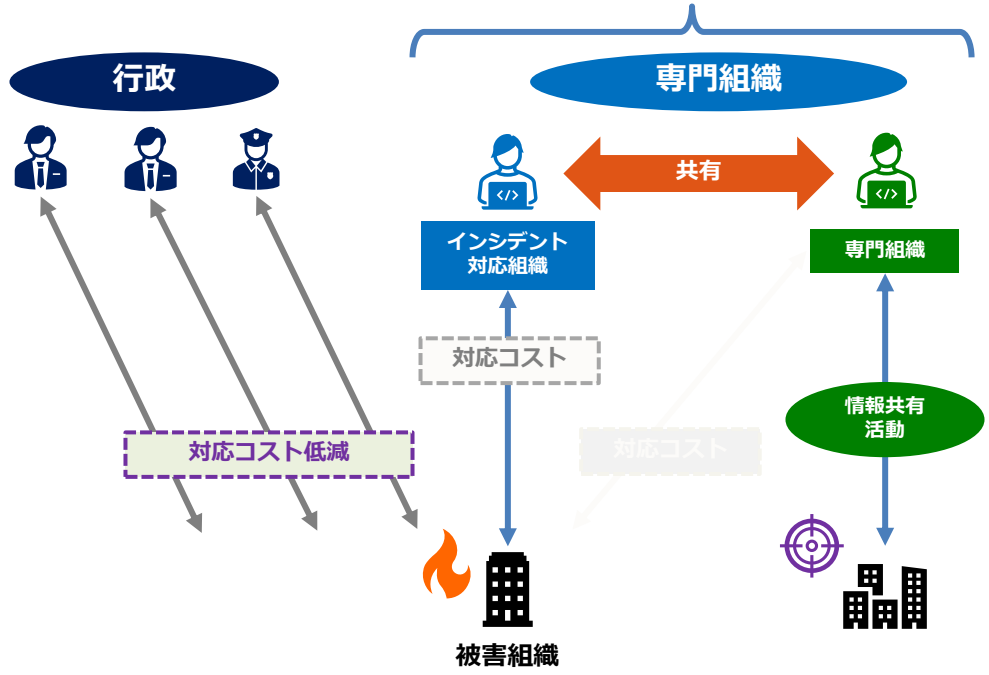
被害組織が調整コストを負担している現状

情報の共有に係る調整コストを被害者側が負担している状況



被害組織の調整コスト削減案

少なくとも攻撃技術情報の共有コスト負担は軽減可能



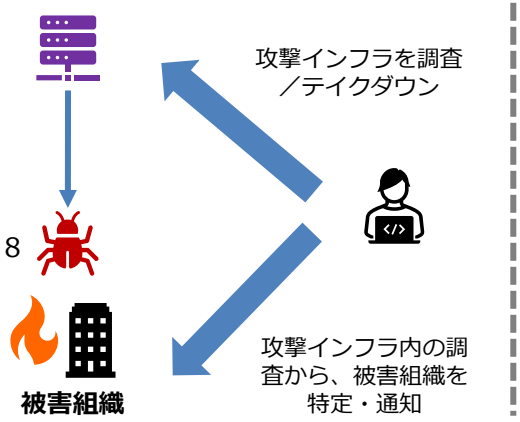
問題②：最適者が事案対応を行わない懸念

- ファーストレスポンダー（「最初に被害組織から相談を受けた組織」や「最初に被害組織にコンタクトした組織」）が当該攻撃に十分な知見を有する事案対処の最適組織とは限らない。
- ファーストレスポンダーは自組織に知見が不足しているかどうか知ることが難しい（他組織と共有して初めて知ることができる）。事案対処にあたる組織間の情報共有により知見が”補充”されるか、最適な対処組織に“交代”するかの調整／修正が必要。

事案対処の最適者である例

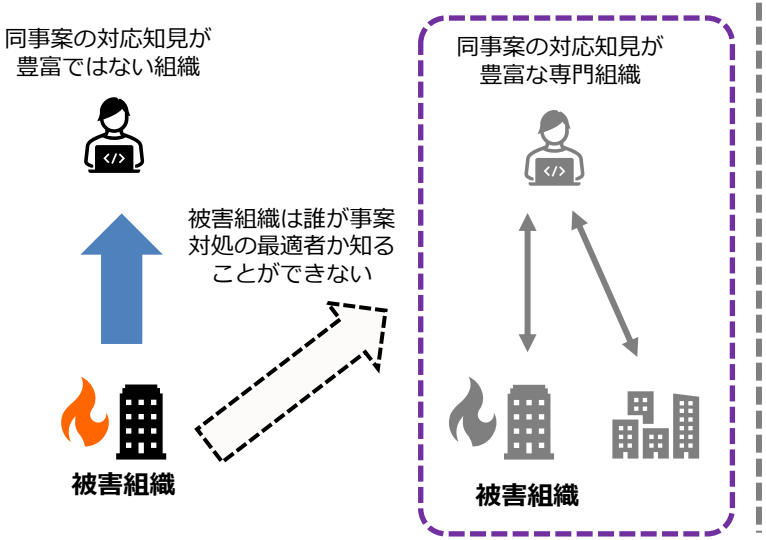
・攻撃インフラを調査／テイクダウンした組織が被害組織に通知するケース
・対処組織は当該攻撃に関する十分な情報／知見を有しているので、個別被害組織の支援に十分対応できる

※ただし、当該組織も「テイクダウンした別の組織から断片的な情報提供を受けただけ」であれば最適者とは限らない



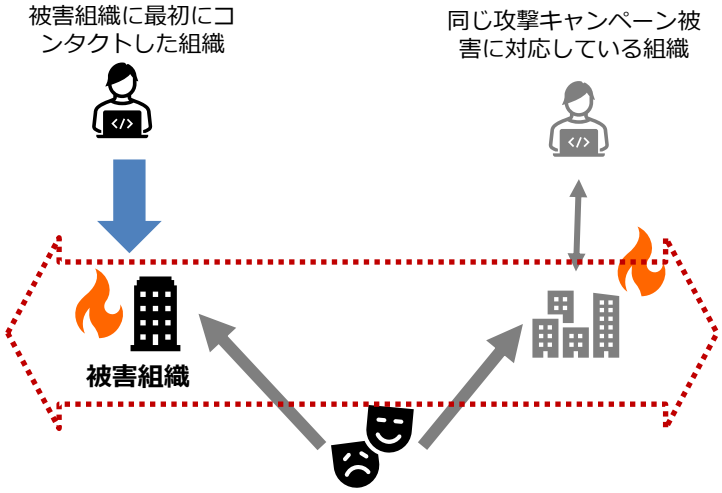
事案対処の最適者でないケース

・相談窓口を設けているからといって、あらゆる事案対応の知見をすべて有しているとは限らない
・被害組織から最も“近い”相談先組織（（セキュリティ）ベンダ、専門機関等）が事案対応の最適者とは限らない



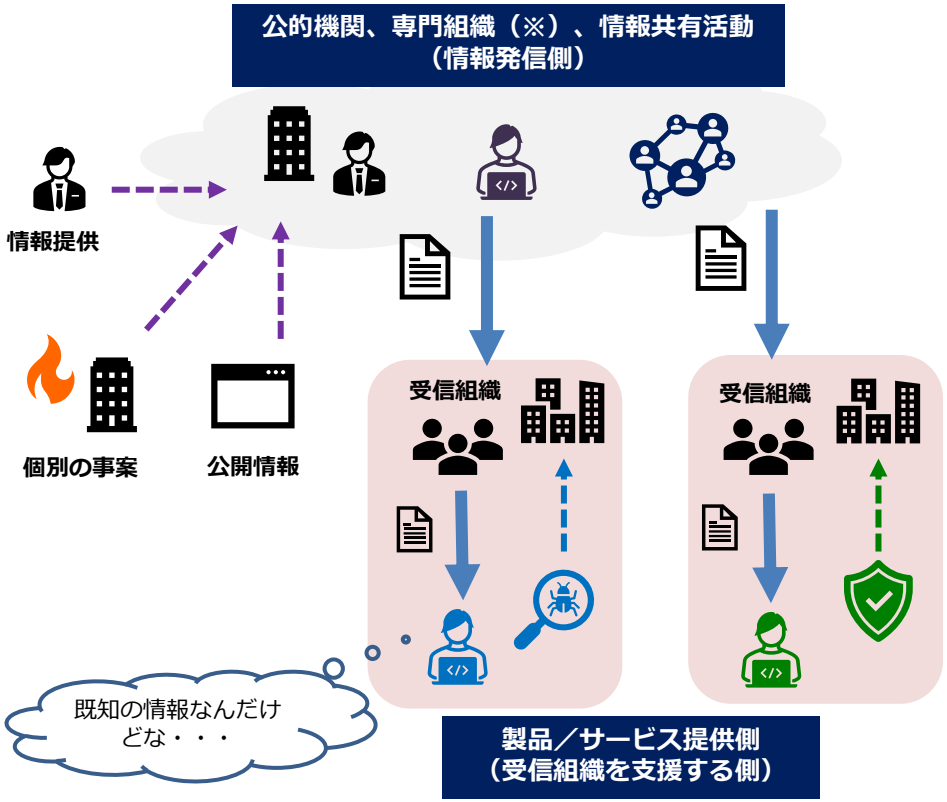
事案対処の最適者でないケース

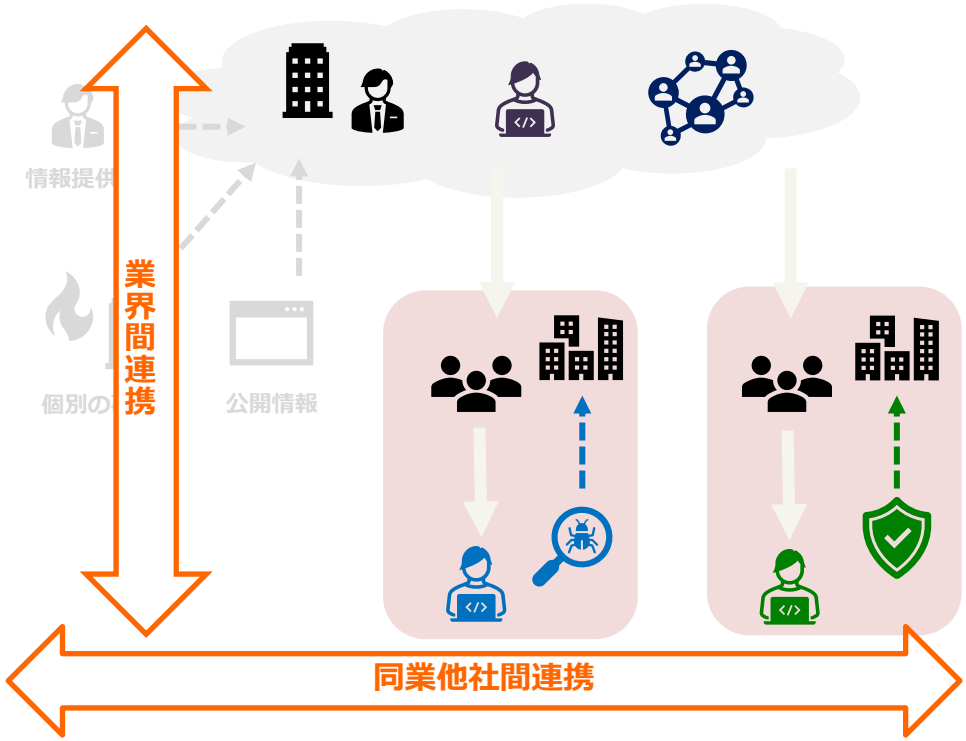
・単独の専門組織だけでは、攻撃キャンペーン全体の範囲を知ることは困難なため、そもそも十分な知見を持っているのかどうか知ることができない



問題③：処理コストのかかる情報提供

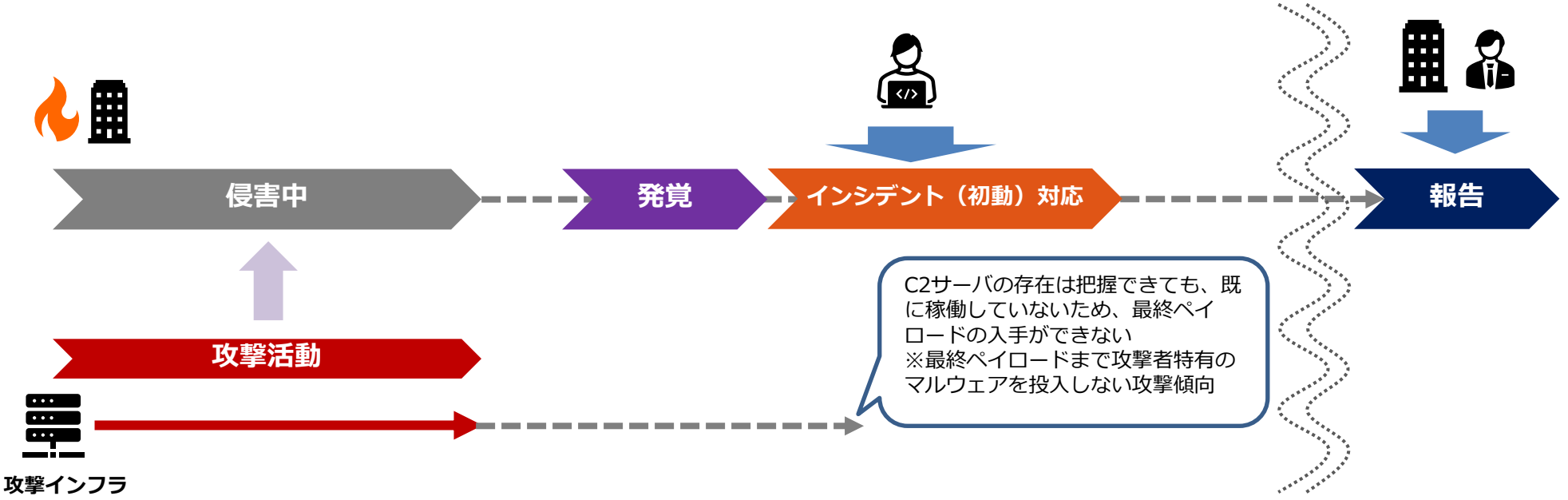
- 本来、情報共有活動に必ずしも流さなくても良い情報も流れることによる受信組織側の対応コストが発生しているおそれがある（セキュリティ製品／サービス側で対応できている状況を情報発信側が把握できていない）。





問題④：「被害現場」依存からの脱却の必要性

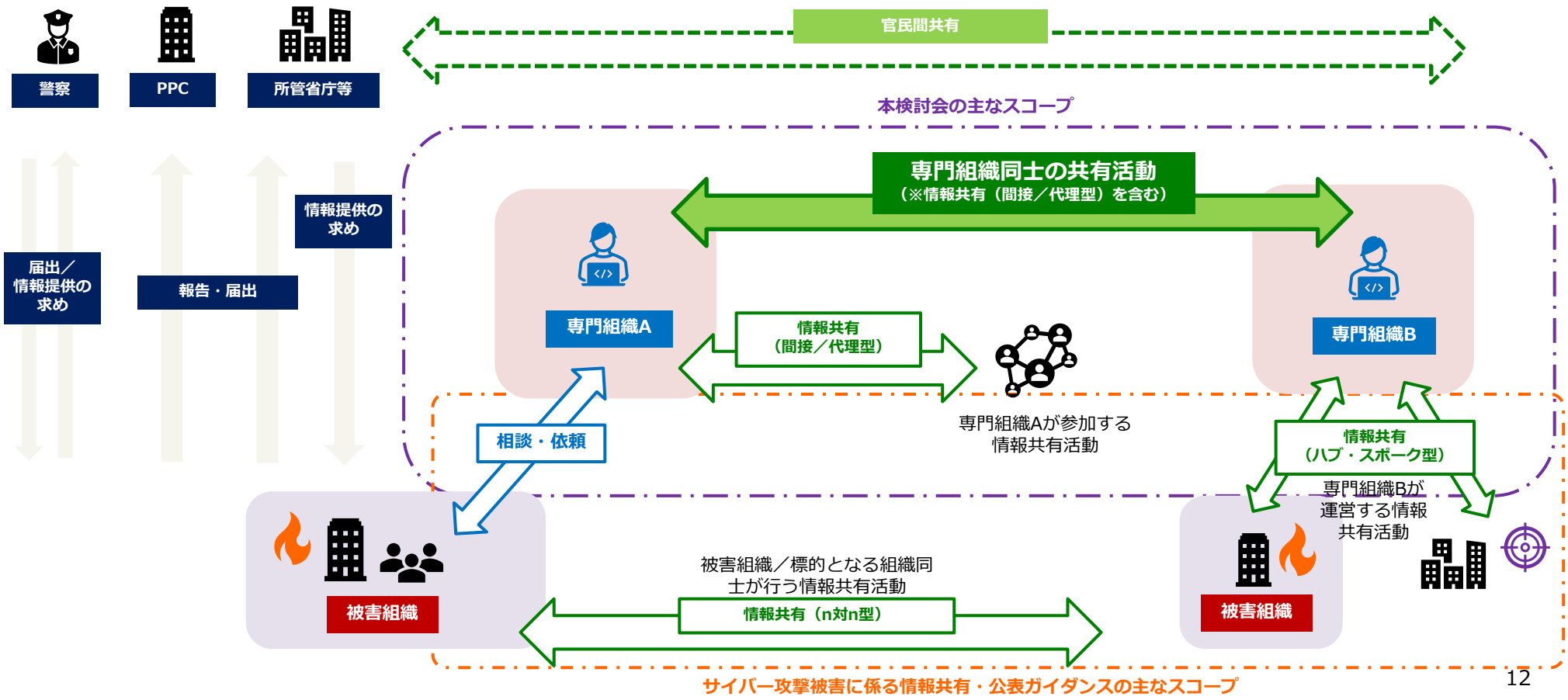
- 高度な攻撃の大半は攻撃活動後に認知されるため、その後のタイミングで専門組織が被害現場に情報を取りに行っても、攻撃インフラの全容や攻撃の全容（※最終ペイロードなど）が判明しないケースが多い。
- かつ、インシデント対応の初動段階で複数の組織が現場に“殺到”することで、被害組織の対外対応コスト負担が増えてしまい、被害組織自身の調査が進まなかったり、各組織との連携による調査・分析が進まず、全体として非効率化する。
- （製品）検知情報やファーストレスポンダーが得た技術情報の複数（専門）組織間での共有の活用が必要。



２．本検討会における提言
(専門組織同士による情報共有)

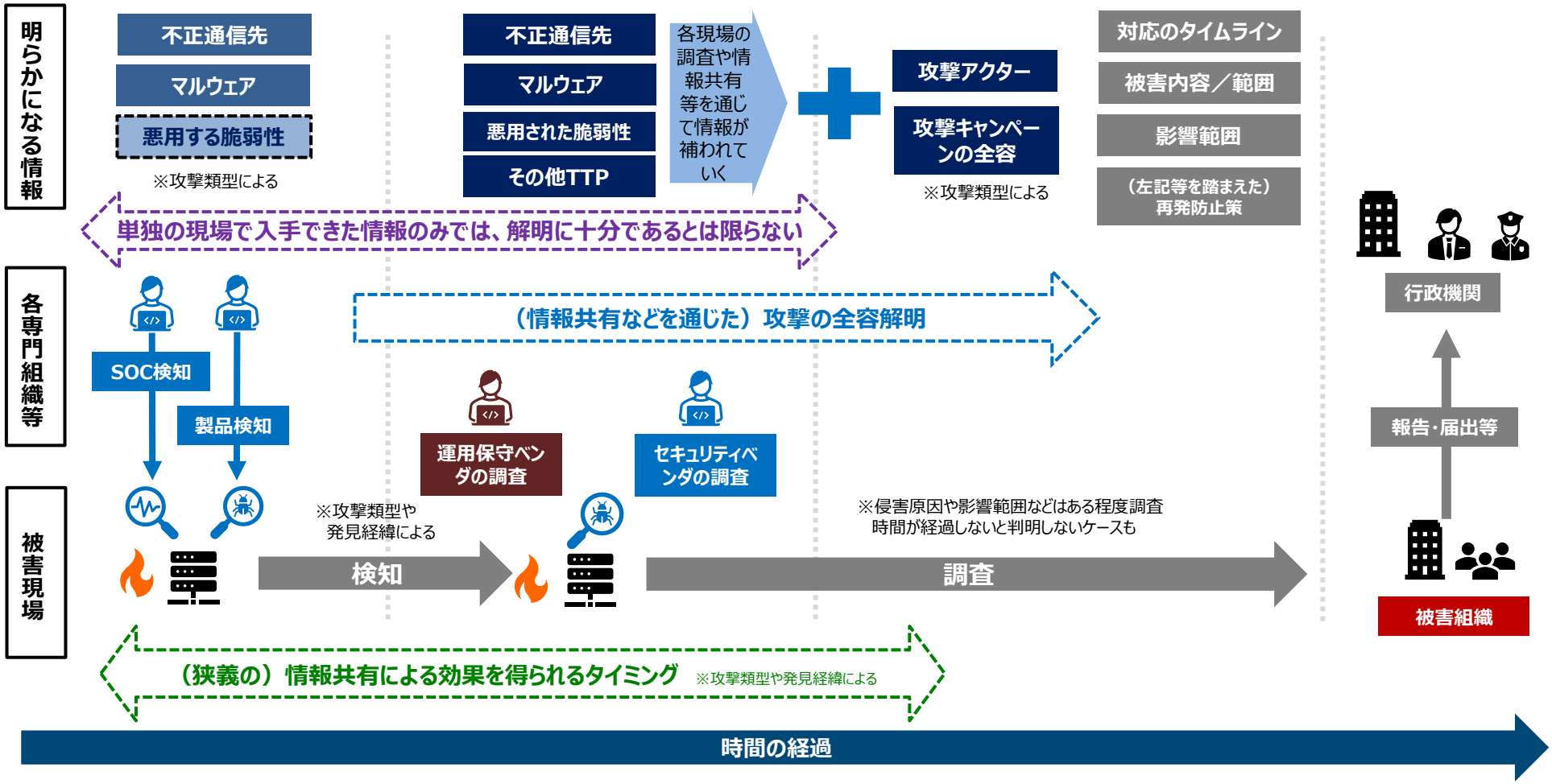
各組織間の情報共有の全体像と本検討会の主なスコープ

- 被害組織を直接支援する専門組織を主体とした情報共有により、被害組織も含め他の組織における被害の拡大防止や、被害組織にとっての情報共有に必要な社内調整コスト等の軽減につながり、また、事案対応の最適者が調整され得るといった利点が見込まれる。
- そのため、**本検討会では**、情報共有公表ガイダンスで主なスコープとしていた被害組織自身による情報共有ではなく、**被害組織を直接支援する専門組織間での情報共有の促進を主なスコープとして、情報共有を促進するための必要事項を検討**。
- 専門組織が被害者組織との間において事前に共有可能な情報について共通の認識を持ち、共有した情報の取扱いについて、事後に不要なトラブル等を防ぐことが可能となる。



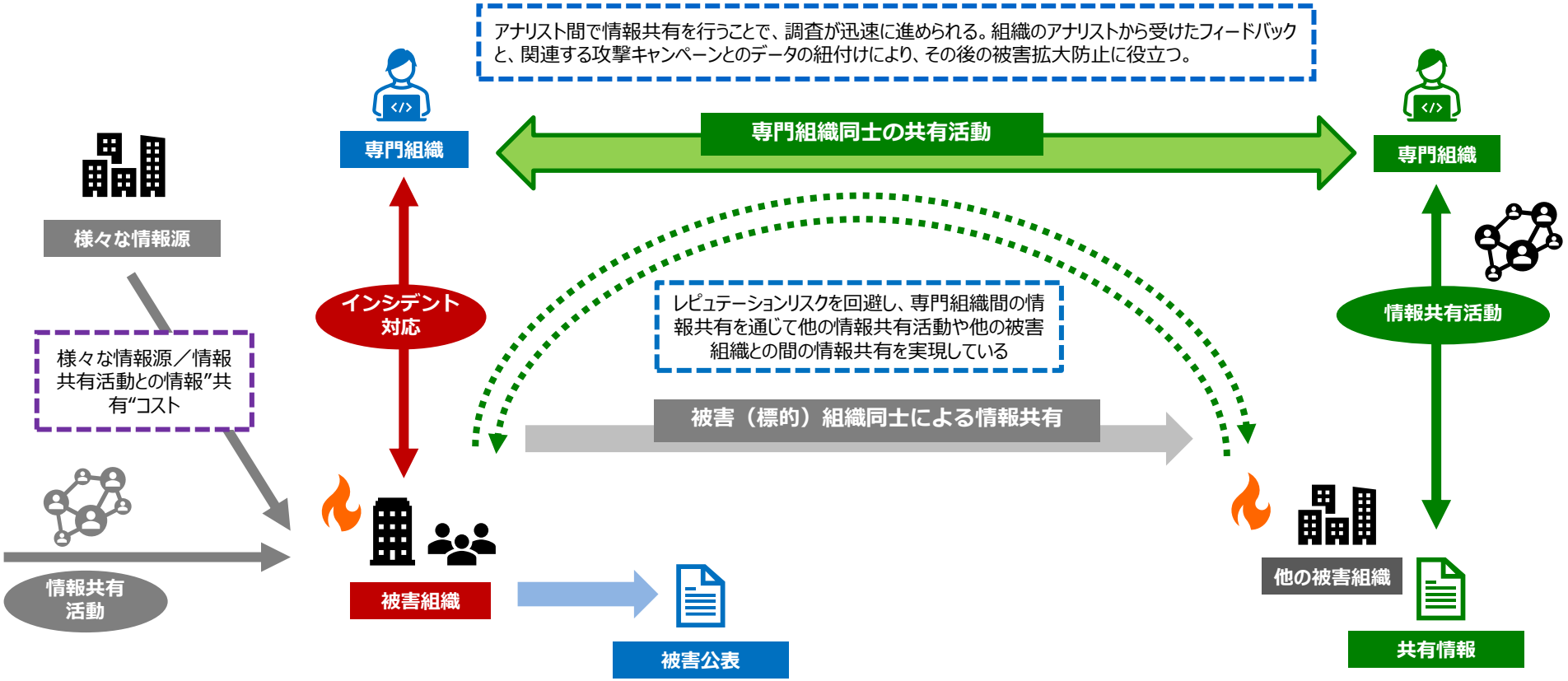
専門組織による情報共有活動の重要性①：全体像の解明

- 被害企業においては、セキュリティ監視をしている運用保守ベンダ等により不正通信先やマルウェア等が検知される、もしくは初動対応に当たった段階での調査で、悪用された脆弱性等が把握されることがある。
- しかし、それらの情報のみでは、被害の原因究明・再発防止に十分な情報を得られているとは限らず、専門組織による情報共有により、他者でも同様の攻撃が起きている状況を把握しながら、被害拡大防止と攻撃の全容が解明されていく必要がある。



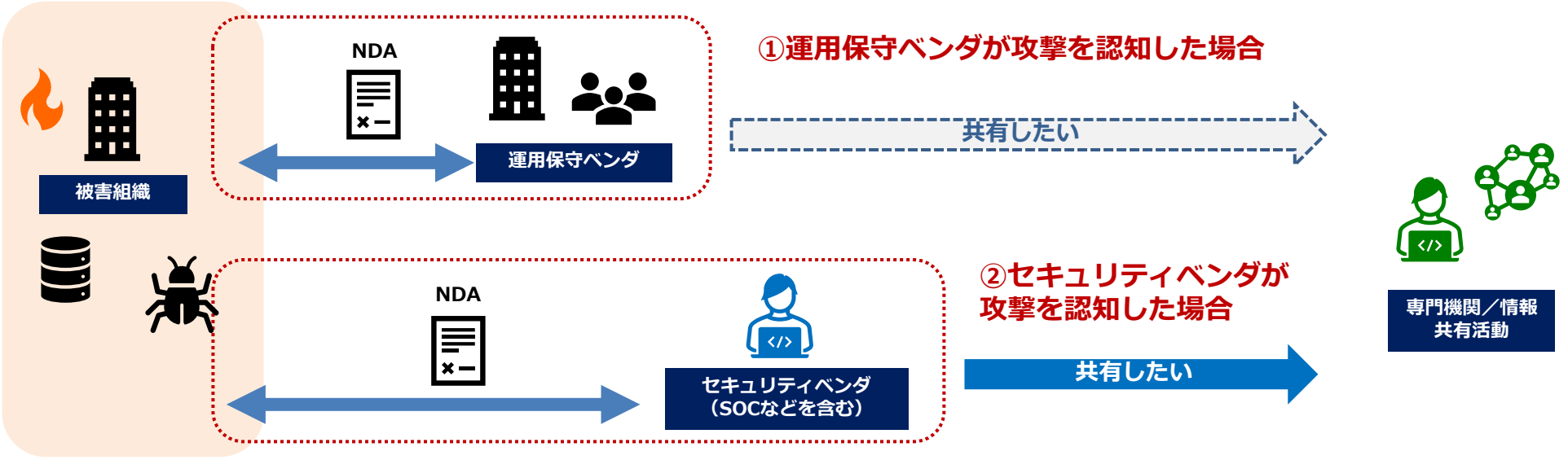
専門組織を通じた情報共有の重要性②：被害者組織のコスト低減

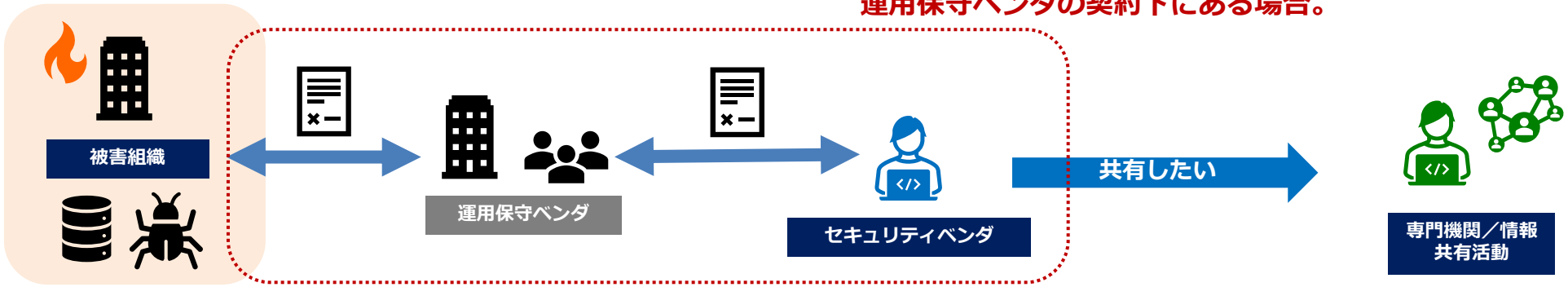
- 情報が必要に応じて「非特定化」され、専門組織を通じて他の情報共有活動に提供されることで、被害組織は、情報共有対応コストを軽減できるだけでなく、 レピュテーションリスクも低く保ちながらフィードバックを得ることができ、調査に資する情報を得ることができる。その結果、調査が迅速に進められる等、被害拡大防止につながる。



専門組織を通じた情報共有の課題①：秘密保持契約（NDA）との関係

- 専門組織を通じた情報共有は重要であるが、**専門組織が共有したい情報が、秘密保持契約上の「秘密情報」扱いとされ、共有できない可能性**がある。
- 基本的に「共有して情報交換をしたい」動機を持つ下記②、③のケースが多く、①のケースは少ない。（③のケースではセキュリティベンダは被害組織の運用保守ベンダのコントロール下にある。）





専門組織を通じた情報共有の課題②：非秘密情報から被害組織を特定/推測するおそれ

ケース１ ：マルウェア情報

- マルウェアの検体には下記の通り、**被害組織を特定や推測できる情報が含まれていることがある**ため、そのままでの情報共有は不適切な場合がある。

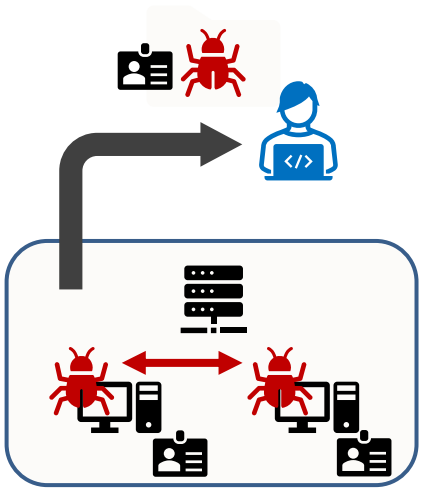
検体そのものが流通することで被害組織が特定／推測されるケース

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

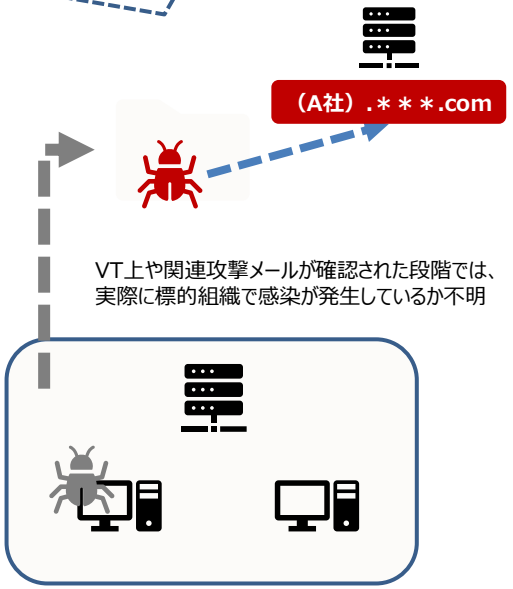
感染時に収集したクレデンシャル情報を含むケース
⇒ID＝メールアドレスのドメインから被害組織が推測されうる

【例】 Olympic DestroyerのVT上にあがった検体



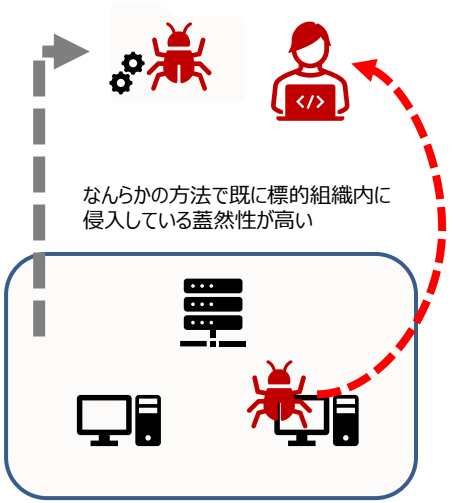
ケース②

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



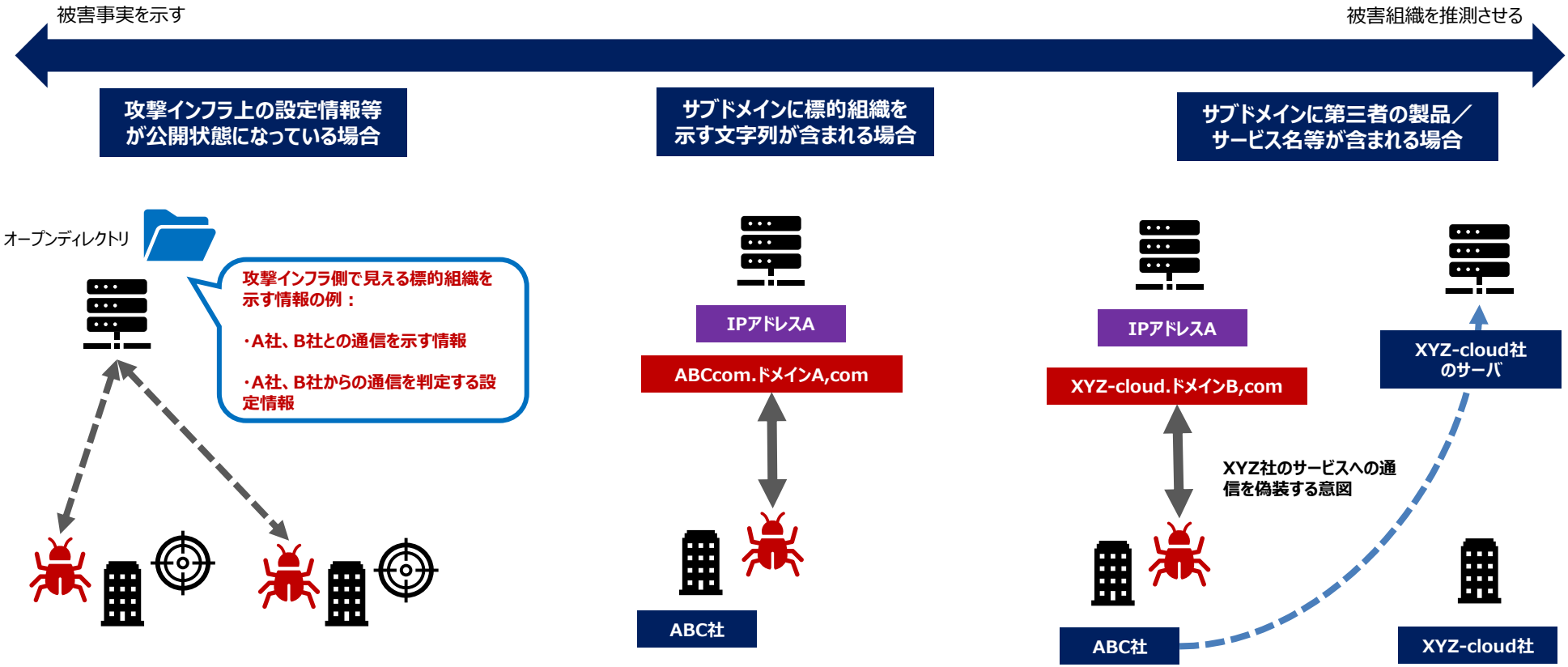
ケース③

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２：通信先情報

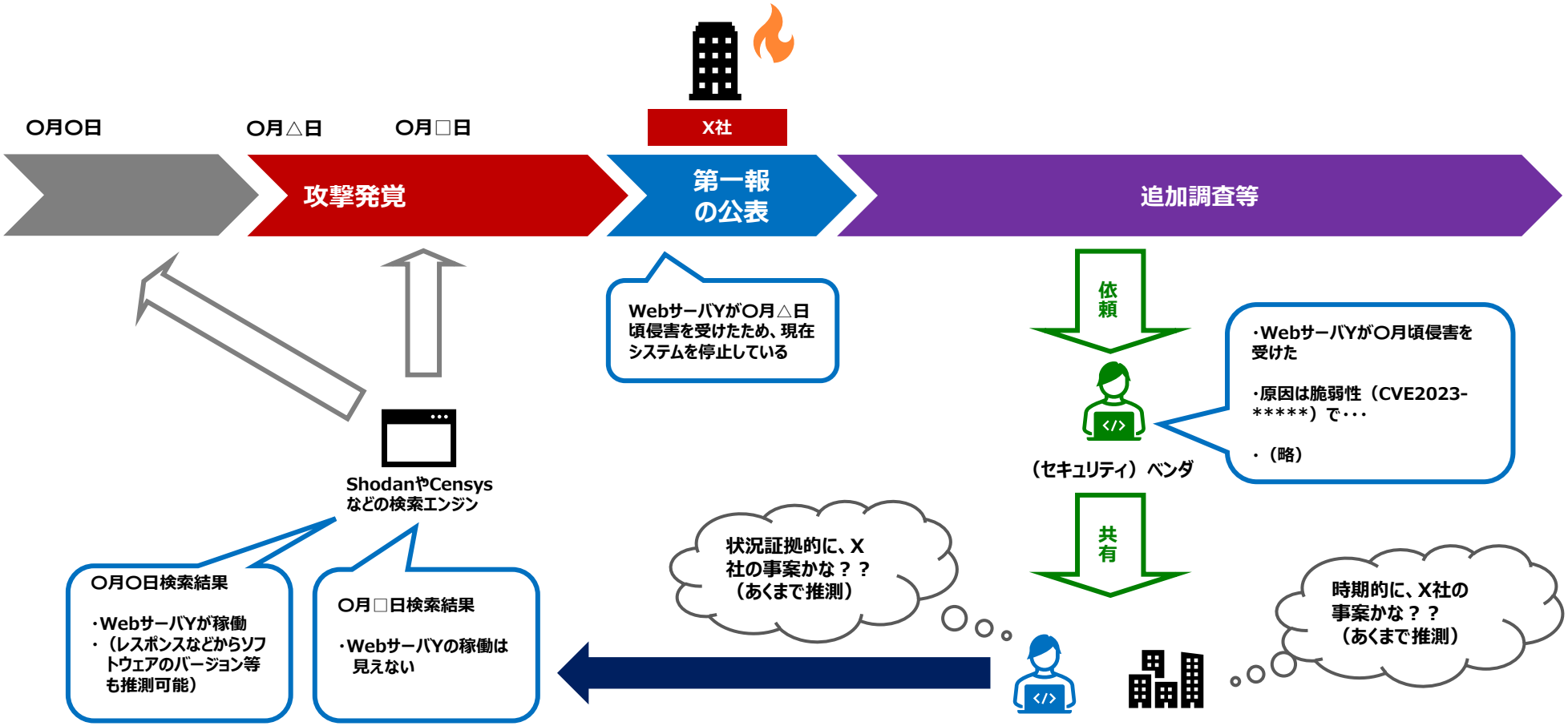
- **<u>通信先情報そのものや通信先情報を共有することで通信先を調査する者が増えたことで、被害組織が特定されたり、あるいは推測されたりする状況が発生</u>**する。
- ただし、あくまで推測するに過ぎない情報が大半であるところ、他の情報（攻撃時期／被害分野／当該被害組織固有のシステム／サービスに関する情報等）と組み合わさることでその“精度”が上がることはあるが、あくまで「推測」に過ぎない。



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

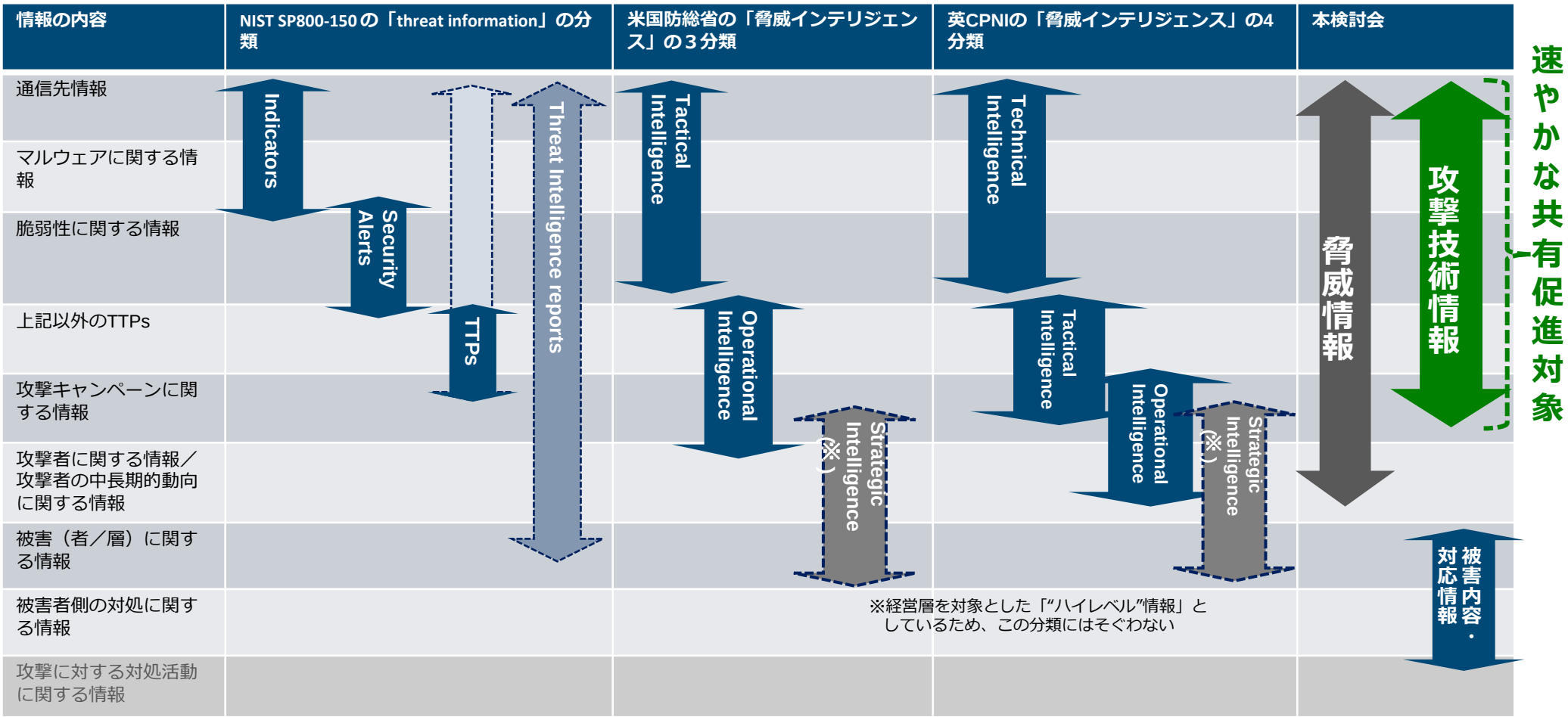
ケース３：先に公表されている被害組織と結びつく情報

- 被害組織からの公表が共有より先に行われている場合、**非特定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、必ずしも特定になる訳ではない。）
- 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。



速やかな共有促進の対象となる「攻撃技術情報」について

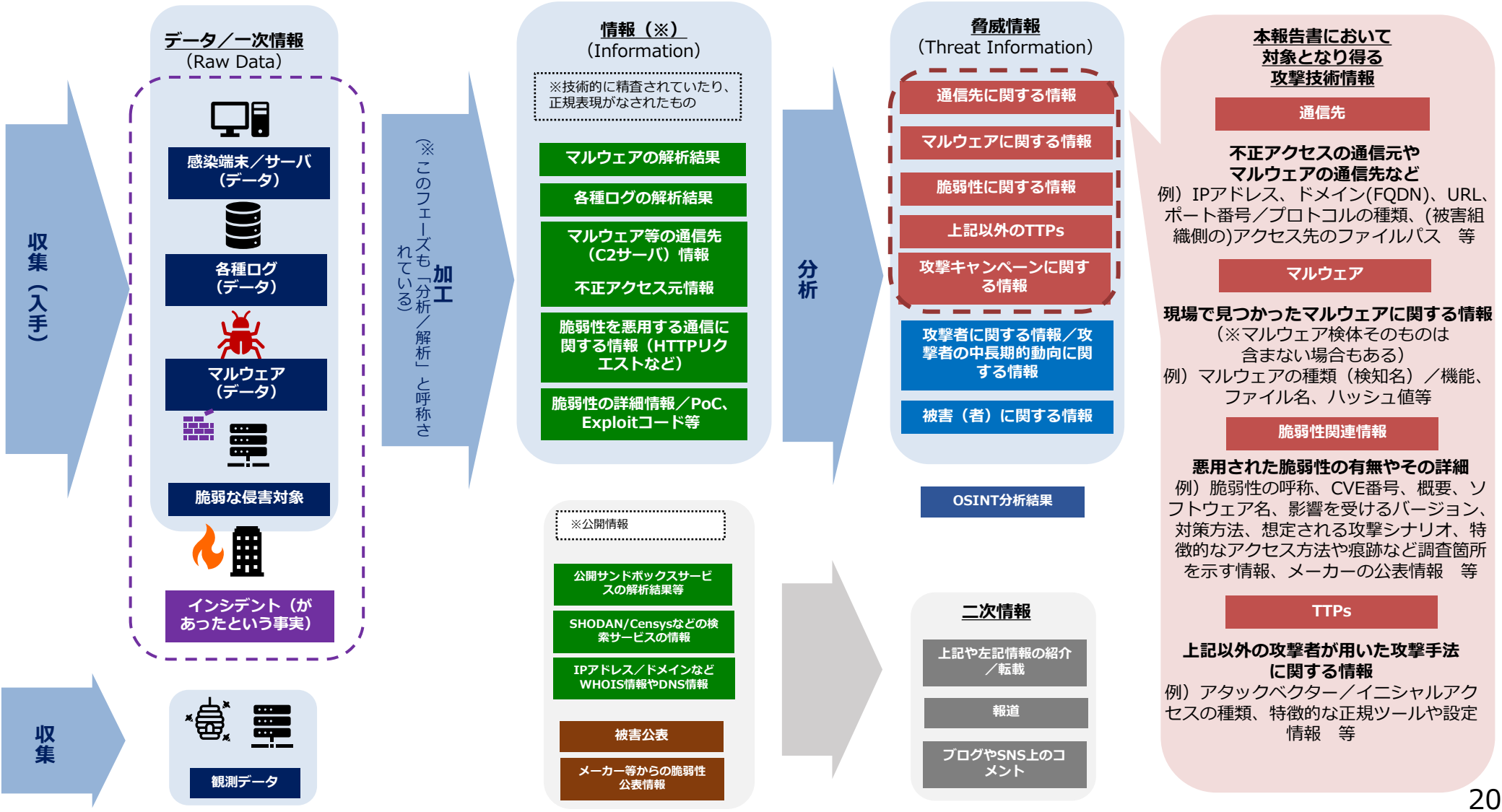
- 脅威情報のうち、**攻撃技術情報には基本的に被害組織が特定される情報は含まれないため、専門組織の判断で他の専門組織への速やかな情報共有が可能な対象となり得る**。ただし、場合によっては被害個社名等を推測可能なケースが想定されるため、留意が必要。



脅威情報：被害組織から専門組織に提供等される調査対象の「データ」を加工し、技術的に精査等した「情報」を分析したもの。

（参考）「データ」、「情報」、「脅威情報」、「攻撃技術情報」について

- 脅威情報は、被害組織から専門組織に提供等される調査対象の「データ」を加工し、技術的に精査等した「情報」を分析したもの。
- 「攻撃技術情報」とは「脅威情報」のうち、通信先情報やマルウェア情報、TTP情報等、攻撃者による攻撃手法やその痕跡を示すもの。



被害組織が推測され得る攻撃技術情報と各専門組織における取扱い

- 各事業者が各データから抽出した攻撃技術情報において、どのような情報／条件では被害組織が推測され得る可能性があるのかは以下のとおり整理される。

マルウェア情報：インディケーターとして展開する場合、マルウェアの挙動などの詳細解説ではなく、ハッシュ値や設置／永続化箇所など「感染を見つけるための」最小限の情報となる。
脆弱性情報：脆弱性の詳細が課されるのではなく、TTPsの場合は、脆弱性を悪用してどのような不正な操作がされるのかについて簡単に示され、インディケーターとして展開される場合は悪用された場合の痕跡（アクセスログ上の特徴的な痕跡など）や調査個所が示される。

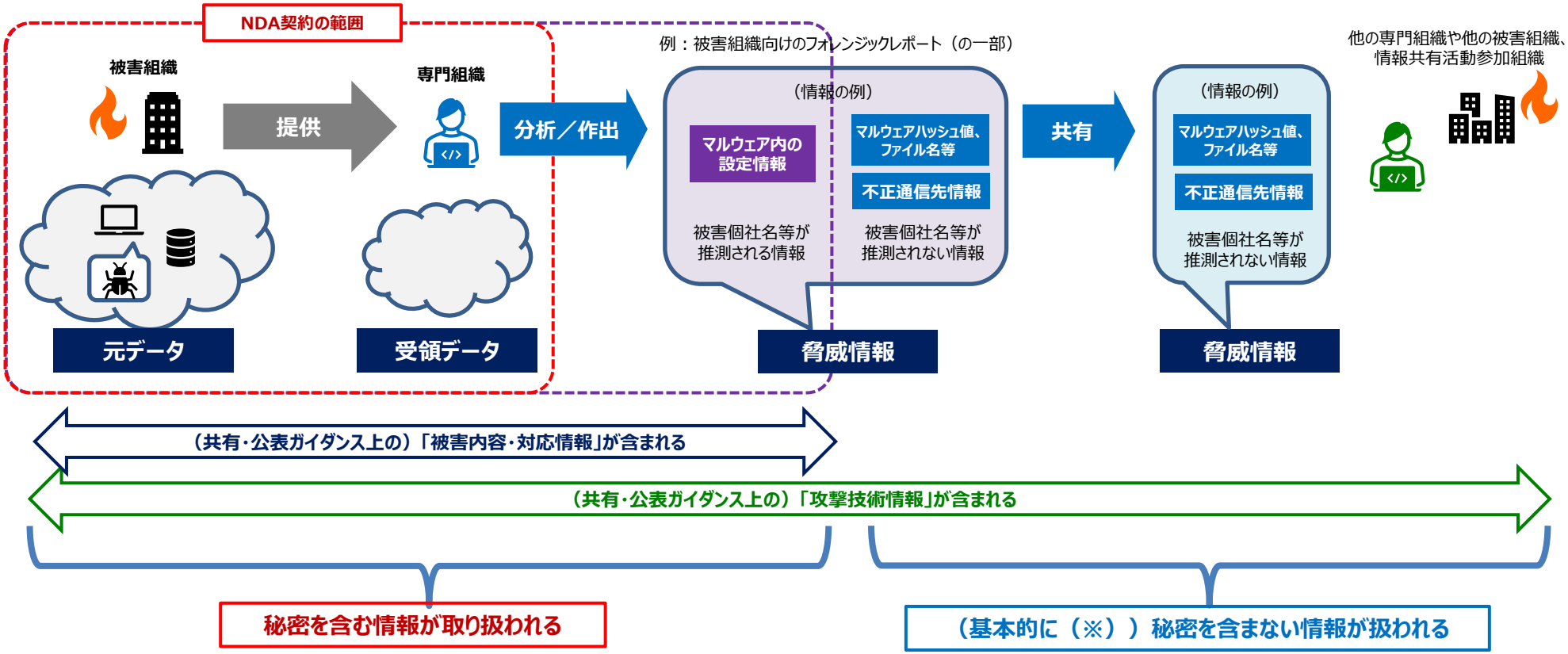
緑枠：各情報が主に扱う内容の範囲　　紫枠：活用範囲が限定的になっているもの　　赤枠：調整に時間／コストがかかるもの

把握・展開まで比較的早いもの ↑ ↓ 調査・公表まである程度時間がかかるもの

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	脆弱性情報	TTP s	攻撃キャンペーンに関する情報	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
インディケーター	サブドメイン名から被害組織が推測できる場合がある	公開サービス上に検体がある場合、当該検体内に内包された情報から被害組織が推測される場合がある				基本的に自社サービス範囲 【自社サービス内での展開】 基本的に被害組織で検知した情報をもとに自社サービス上で展開する	左に同じ	調整コストがかかる ※個別のインシデント対応側での利用条件に影響される	左に同じ
						【レポート公表や専門組織同士の共有】 現状では被害組織に個別の了解を得ている			
TTP		同上	先に被害公表が行われており、かつ、外形上、脆弱なホストが不特定多数に見えている場合、被害組織が推測される場合がある	侵害を受けたシステムが被害組織固有のものであった場合、下記ぶり次第では被害組織が推測される場合がある		【自社から公表する場合】 ※基本的には下記の脅威インテリジェンスレポートに内包される			
						【専門組織間で共有する場合】 現状では被害組織に個別の了解を得ている 調整コストがかかる			
セキュリティアラート			同上			（主に専門機関（JPCERT/CC等）から発出されるが、各ベンダが発見者となり、専門機関に届け出ることで注意喚起がなされるケースもある）			
脅威インテリジェンスレポート	・IoC,TTPs情報がAppendixとして示されることが多い ・攻撃インフラの特徴、マルウェアの機能、脆弱性悪用のプロセス等に関する詳細な解説が行われる				標的となった地域／業種が示される場合、既に公表されている被害情報と紐づく場合がある	公表までの相手方等との調整に時間がかかる 基本的には事後（被害公表後、あるいは攻撃キャンペーン後）において、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			

情報の非特定化加工による情報共有の実現

- 攻撃技術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、被害個社名等を推測可能なケースが想定される。
- このため、上記のような被害個社名等を推測可能な情報を除いた、非特定化した情報であれば、秘密情報の例外として整理できる。



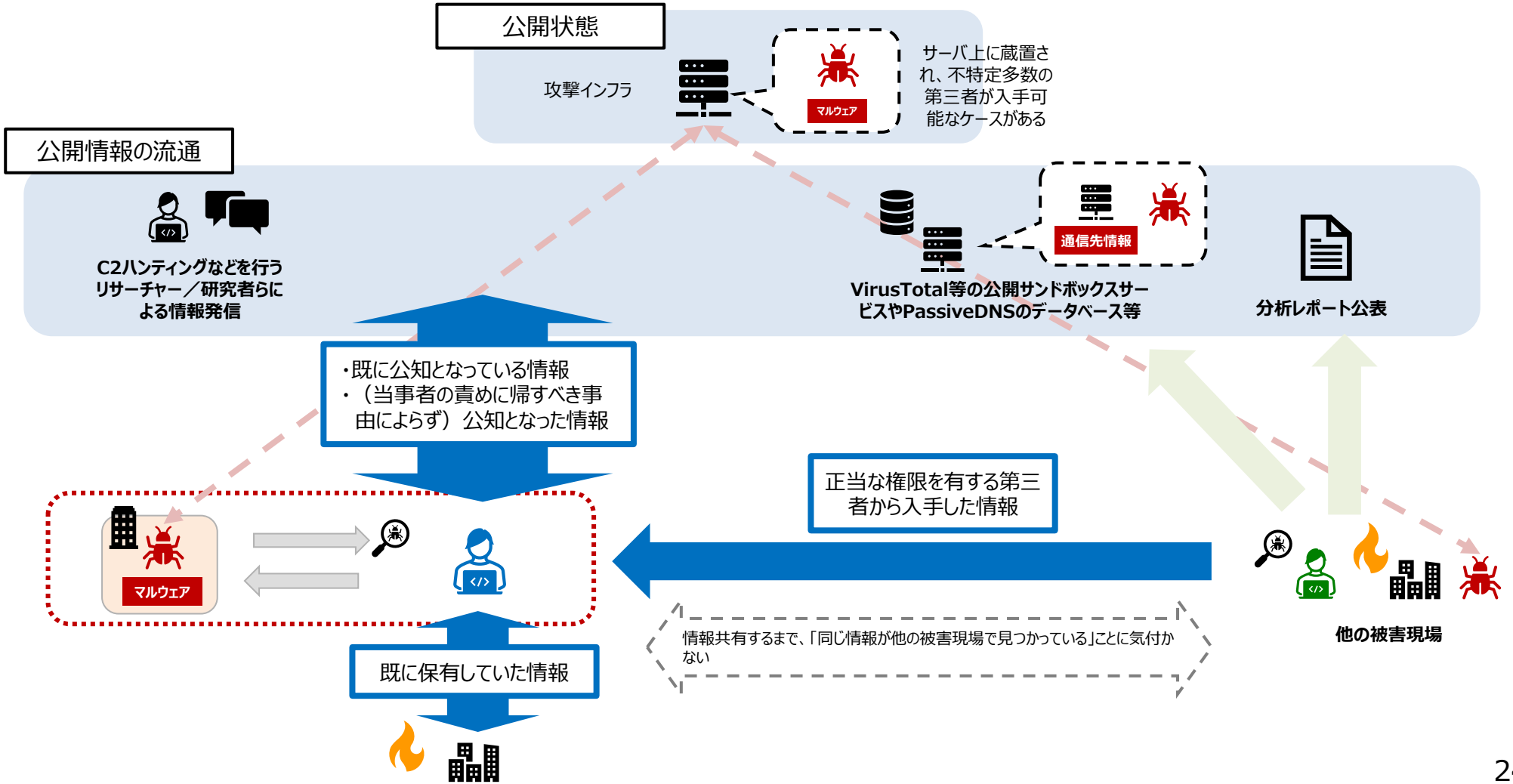
※サイバーセキュリティ協議会では別途規約で定める「秘密」情報を扱うことが可能

（参考）情報共有の対象となり得る攻撃技術情報と情報提供元の非特定化について

情報の内容		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	
		非特定情報	被害組織を特定しうる場合があるか	非特定情報	被害組織を特定しうる場合があるか	非特定情報	被害組織を特定しうる場合があるか	非特定情報	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？			

（参考）公開情報、公知の情報、第三者から入手した情報の整理

- 多くの秘密保持契約では、開示された時点で「受領当事者が既に了知していた情報」「既に公知であった情報」「開示された後に受領当事者の責めに帰すべき事由によらず公知となった情報」「開示当事者に対して秘密保持義務を負わない正当な権限を有する第三者から、受領当事者が秘密保持義務を負うことなく適法に取得した情報」については秘密情報に含まれないと定義されることが多い。



攻撃技術情報の取扱い・活用手引き（案）について

- どのような情報が速やかに専門組織同士で共有できるのか、そもそもどのような情報を共有すべきなのか、どのような情報は被害組織（情報提供元）が特定／推測されるおそれがあるのか、どのように非特定化加工すれば良いのか、どのように共有すれば良いのか、といった専門組織同士の情報共有における各論点や方法について解説。

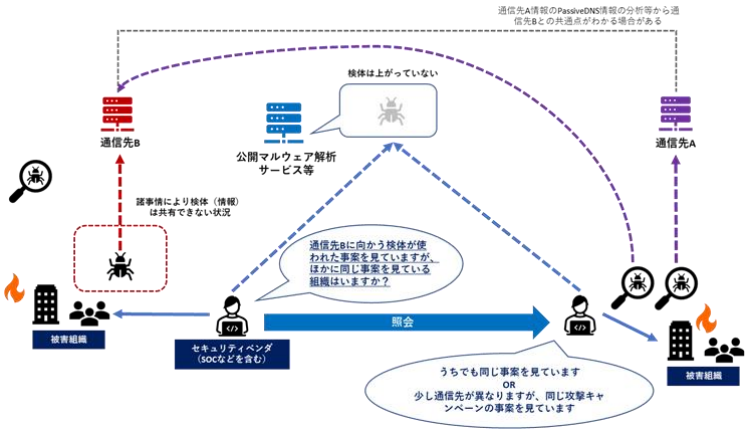
目次構成案

はじめに
・スコープとしている情報共有活動
・用語の定義
・本手引きの想定読者
第１章　専門組織間の情報共有について
・脅威情報を扱う大原則
・脅威情報と「攻撃技術情報」について
・どのような情報を共有するのか
・何のために専門組織は攻撃技術情報を共有するのか
・専門組織間の共有が有効な場合と有効でない場合
・どうやって共有するのか
・いつ共有するのか
・正確性を優先すべきか、スピードを優先すべきか
・情報受信側の対応コストを減らすためのポイント
・攻撃技術情報共有時の被害組織との間の問題点は何か
・NDAについて

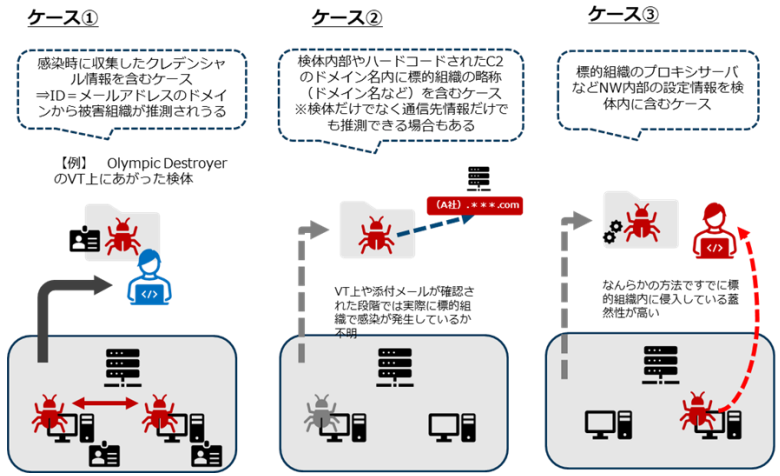
第２章　各攻撃技術情報の解説
・通信先情報
―通信先情報について
―通信先情報の特性
―通信先情報の共有のポイント
―被害組織が特定されてしまうケース
・マルウェア情報
―専門組織同士のマルウェア情報の共有
―その情報を共有するのか：マルウェア解析情報
―被害組織が特定されてしまうケース
・脆弱性情報
―被害組織が特定されてしまうケース
・その他TTPs
―被害組織が特定されてしまうケース

第３章　ユースケース

解説例：公開検体情報を用いた情報共有（照会）の方法の解説



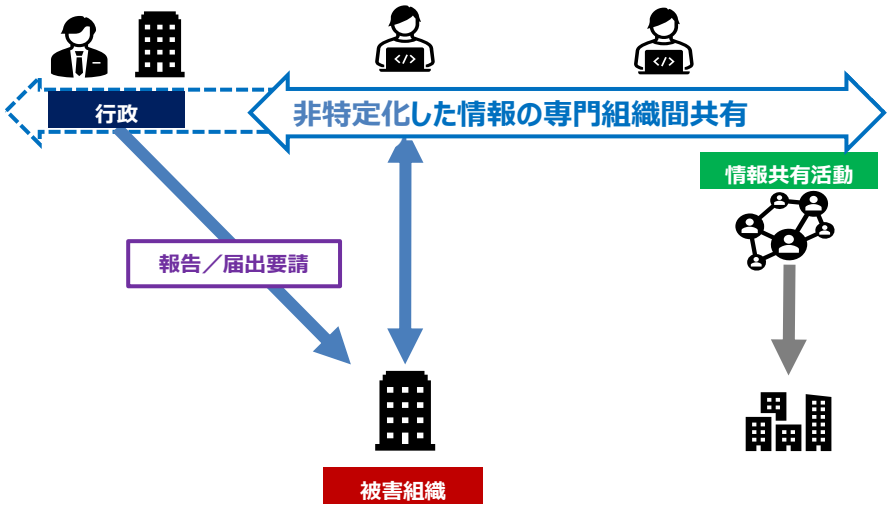
解説例：検体に内包する情報から被害組織が特定／推測されるケースの解説



情報共有の目指すべき在り方

- より専門的知見のある専門組織が、一定程度の信頼関係のある組織が集まったり、必要な安全管理措置を講じるなど、情報の漏えいリスクを軽減しつつ、積極的な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、全体像の解明による被害拡大防止や被害組織の対応コスト軽減に資する。
- そのためには**本報告書・活用手引きに基づき、非特定化加工された攻撃技術情報を整理することにより、既存の情報共有活動の枠組みも活用しながら、更に円滑な情報共有が可能**となる。
- なお、**専門組織が情報共有を行った場合には、故意又は重過失による場合を除き、その共有した情報に基づく法的責任を負わないことを合意するなどの対応をすることが望ましい**（秘密保持契約に盛り込むべき攻撃技術情報等の取扱いに関するモデル条文案参照）　。
- 今後、社会全体で効率・効果的な被害軽減・防止につながるように情報共有が促進されることを目指し、情報共有の重要性はもとより、**本検討会の成果について社会全体の理解促進と活用促進を図る**べく、**専門組織やユーザー企業の経営層への意識啓発も含めた周知・啓発活動**を進めるとともに、**関連ガイドラインへの反映等の環境整備に取り組むことが重要**。

被害者組織のコスト負担を軽減しつつ、社会全体での効率的な活用のための情報共有

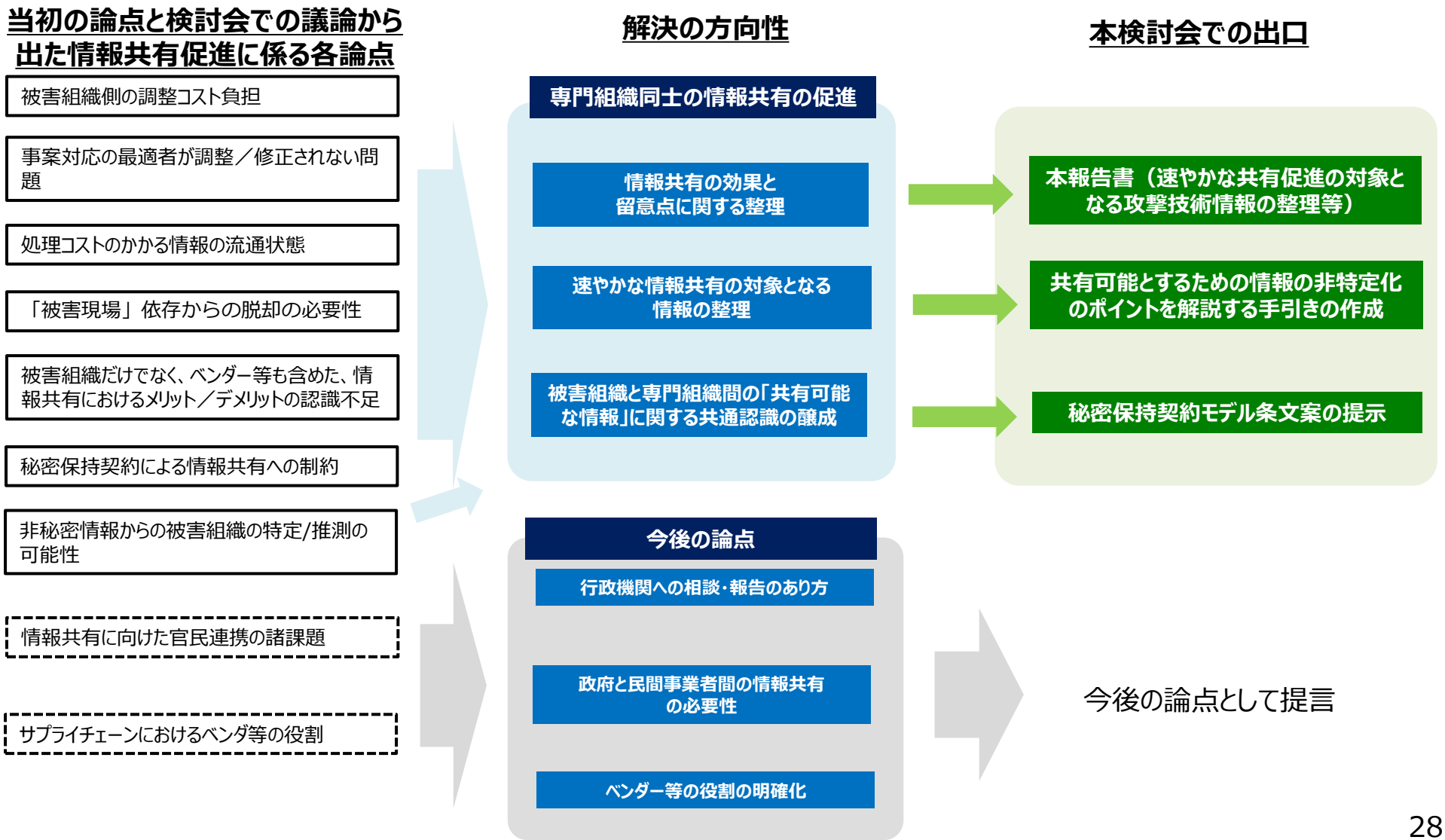


・主に非特定化加工した攻撃技術情報については専門組織同士が速やかに共有を行い、被害調査のための追加情報作出や被害拡大防止のための共有活動、注意喚起等に活用する。
・少なくとも個別の被害組織よりは専門的知見のある専門組織等が脅威情報をハンドリングすることで社会全体として効率的な情報の活用がなされる。

３．今後の論点

検討会での議論で出た各論点と出口について

- 本検討会では、専門組織同士の情報共有の促進に向けて、速やかな共有促進の対象となる攻撃技術情報の整理や秘密保持契約案の提示等を行ったが、専門組織同士の情報共有促進だけでは解消されない課題が「今後の論点」としてなお残る。



今後の論点

（１）情報共有に向けた官民連携等について

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、専門組織間の情報共有だけではなく、重要事案について被害者情報含めて、適切に情報共有されるような官民での連携が不可欠。具体的に、以下の点について今後検討していくことが必要ではないか。

①行政機関への相談・報告のあり方

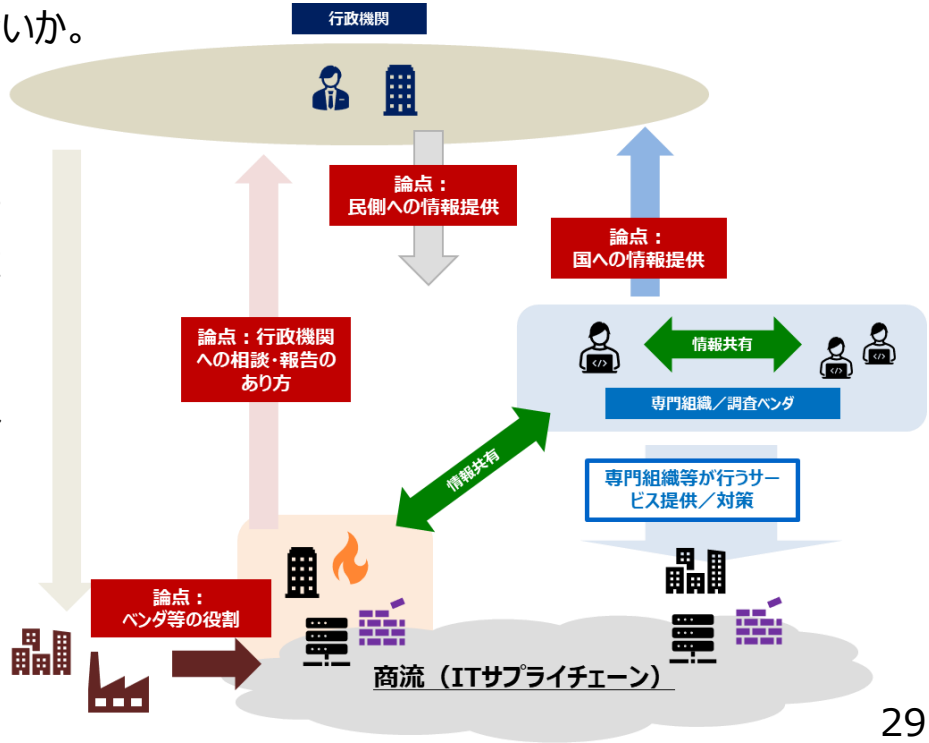
- 被害組織が行政機関に報告する際、行政機関ごとに報告事項が異なるなど、被害組織の負担が大きいため、対応コスト軽減に向けた取組の検討が必要ではないか。

②政府と民間事業者間の情報の共有

- 民間事業者の予防措置の観点から、政府の役割を明確化し、被害組織の支援等にあたる専門組織（セキュリティベンダやSOC事業者等）から政府への情報共有を促進するとともに、政府が持つ有益な情報等を民間事業者に提供する等、政府と民間事業者間の情報共有をさらに推進することが必要ではないか。

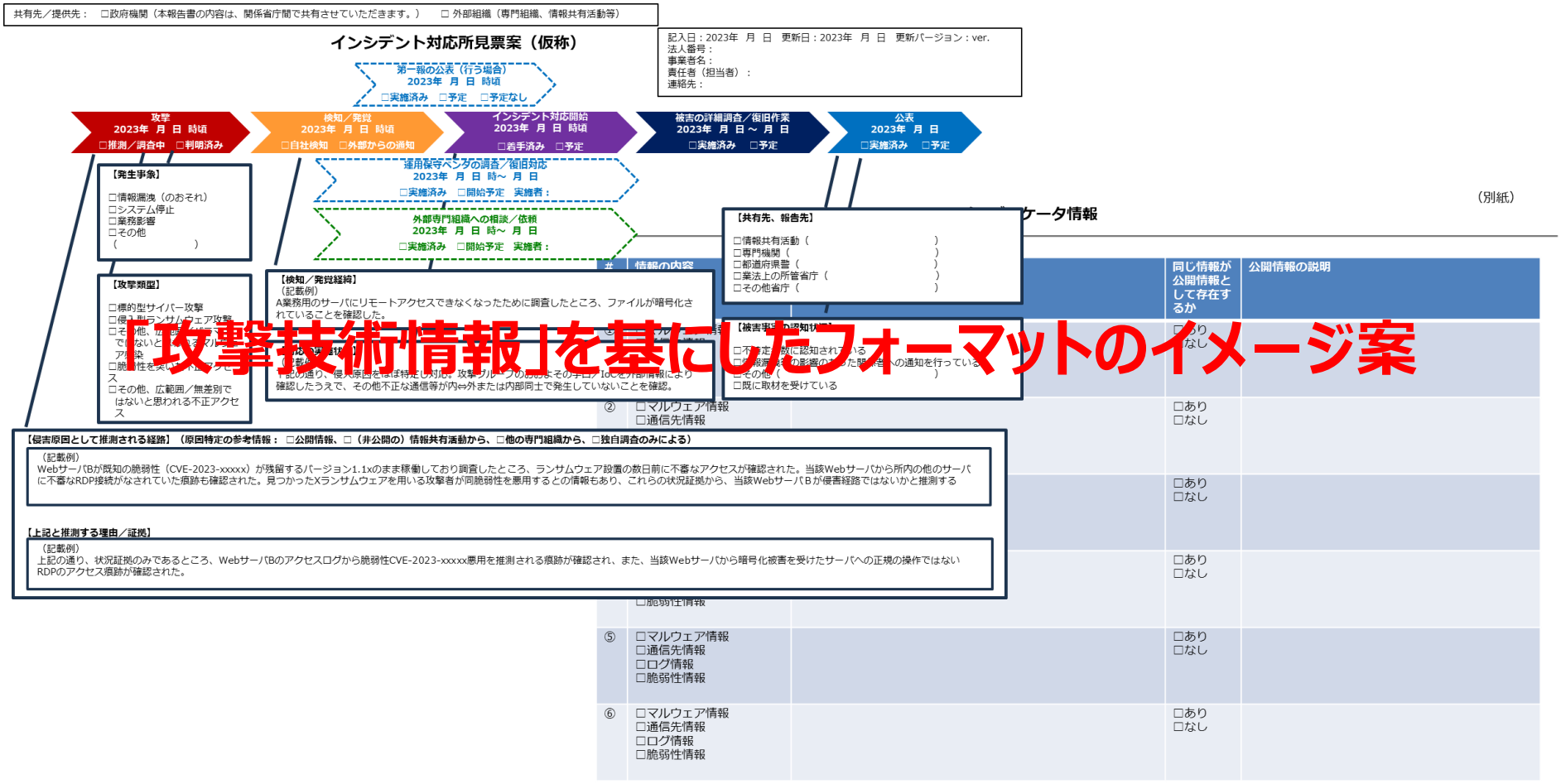
（２）サプライチェーンにおけるベンダ等の役割について

ユーザーとベンダー間の責任範囲が不明確であることや、両者に情報の非対称性が存在することに起因し、本来早急に対応すべき重大な脆弱性が放置され、結果としてサイバー事故につながってしまう事例が増えてきている。こうした事例を防止する観点から、ベンダーからユーザーへの情報提供のあり方やベンダーの役割の明確化などの検討が必要ではないか。



（参考）情報共有・報告の更なるコスト削減等に向けた方策案

- 今後の論点のうち、（１）①行政機関への相談・報告において、各行政機関が共通して参照できるフォーマット等を活用することで、報告等を行う被害組織のコストが低減され得るのではないか。
- 各行政機関における役割や求める情報等は異なるため、行政機関への報告・相談に係るフォーマットについては更なる検討や議論が必要。



４．参考（海外事例）

Cybersecurity Information Sharing Act of 2015

- 米国においては、連邦政府と非政府機関との脅威情報に関する情報共有について、2015年サイバーセキュリティ情報共有法で一定のルール化。

SEC. 102. Definitions.

SEC. 103. Sharing of information by the Federal Government.

(a) In general
(b) Development of procedures.

SEC. 104. Authorizations for preventing, detecting, analyzing, and mitigating cybersecurity threats.

(a) Authorization for monitoring.
(b) Authorization for operation of defensive measures.
(c) Authorization for sharing or receiving cyber threat indicators or defensive measures.
(d) Protection and use of information.
(e) Antitrust exemption.

SEC. 105. Sharing of cyber threat indicators and defensive measures with the Federal Government.

SEC. 106. Protection from liability.

SEC. 107. Oversight of Government activities.

SEC. 108. Construction and preemption.

SEC. 109. Report on cybersecurity threats.

SEC. 110. Conforming amendment.

国が機密扱いの脅威情報を民間へ情報提供することについて定めた箇所

(a) 一般に、機密情報、情報源および方法、ならびにプライバシーおよび市民の自由の保護と矛盾しないように、国家情報長官、国土安全保障長官、国防長官および司法長官は、適切な連邦機関の長と協議して、以下を促進および推進する手順を開発し、公布するものとする。

(1)連邦政府が保有する機密扱いのサイバー脅威指標を、関連団体の代表者と適時に共有すること。
(2) 機密解除され、非分類レベルで共有される可能性のある、連邦政府が所有するサイバー脅威指標または情報を関連する団体と適時に共有すること。
(3)連邦政府が保有する、管理された非分類を含む非分類サイバー脅威指標を、関連する主体又は適切な場合には一般大衆と共有すること。
(4) 必要に応じて、連邦政府が保有する、当該主体に対するサイバーセキュリティの脅威に関する情報を、当該サイバーセキュリティの脅威による悪影響を防止または軽減するために、当該主体と共有すること。
(5) 小企業関係者（Small Business Act (15 U.S.C. 632)の第3条に定義されている）が直面するアクセス可能性と実施上の課題に注意を払い、サイバー脅威指標と連邦政府が保有する情報の継続的分析に基づいて開発されたサイバーセキュリティベストプラクティスを、出版とターゲットアウトリーチを通して定期的に共有すること。

システムを管理する事業体が脅威情報を利用することを定めた箇所

(d)(1) 情報の安全性：情報システムを監視し、防御手段を運用し、又は本節に基づきサイバー脅威指標若しくは防御手段を提供若しくは受領する事業体は、当該サイバー脅威指標又は防御手段への不正なアクセス又は取得から保護するための安全管理を実施及び利用するものとする。

独禁法との関係について定めた箇所

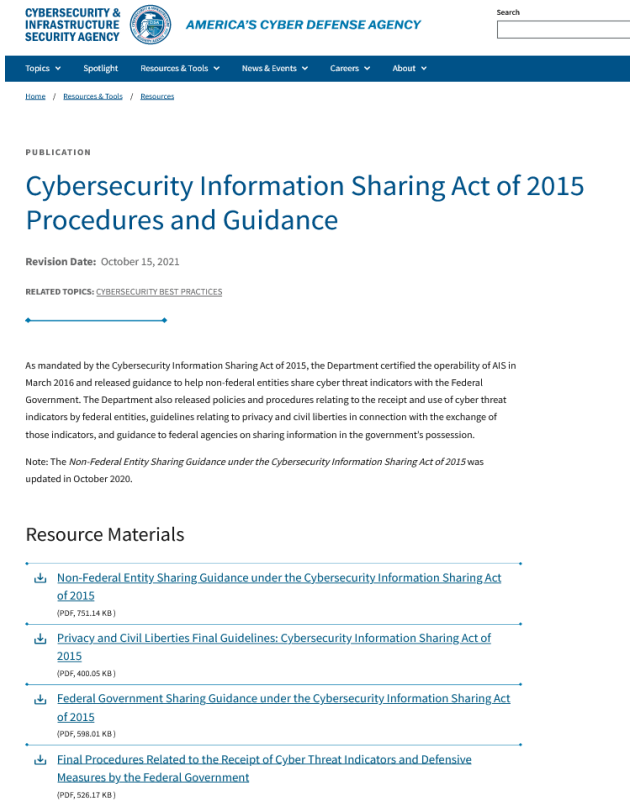
(e)(1) 一般に、第 108 条(e)に規定される場合を除き、2 以上の民間団体が、本タイトルに基づくサイバーセキュリティ目的のために、サイバー脅威指標、またはサイバーセキュリティ脅威の防止、調査、もしくは軽減に関する支援を交換または提供することは、独禁法のいかなる条項の違反とも見なされないものとする。

国と事業体が共有するための手続きやガイドラインを整備することを定めた箇所

出典：CYBERSECURITY INFORMATION SHARING
https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Information%20Sharing%20Act%20of%202015.pdf

2015CISA法施行後の動き／取組の評価①

- 連邦政府向け／非連邦政府向けの共有ガイダンスが公表され、主に法的免責やプライバシーデータへの配慮などに対する見解が解説されている。
- 2022年8月国土安全保障省監察官室が2015CISA法下でのDHSが行っている官民間情報共有活動について監査報告を行った。AIS（Automated Indicator Sharing）による情報共有の問題点として、サイバー脅威指標が意思決定者が行動を起こすのに役立つ十分なコンテキスト情報を含んでいないことや、展開される情報には不要なアップグレードや誤検知のアラートを発生させるような誤った情報が含まれている点が指摘された。


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
AMERICA'S CYBER DEFENSE AGENCY
Search
Topics Spotlight Resources & Tools News & Events Careers About
Home / Resources & Tools / Resources

PUBLICATION

Cybersecurity Information Sharing Act of 2015 Procedures and Guidance

Revision Date: October 15, 2021

RELATED TOPICS: CYBERSECURITY BEST PRACTICES

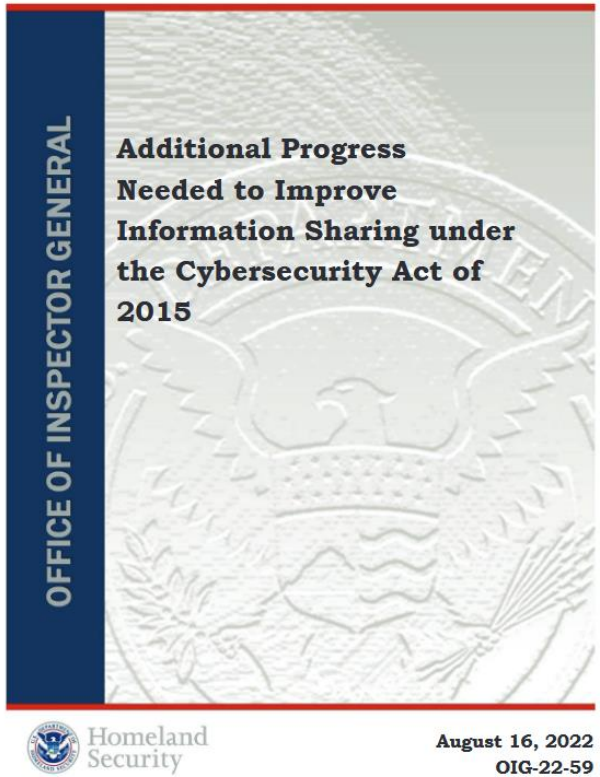
As mandated by the Cybersecurity Information Sharing Act of 2015, the Department certified the operability of AIS in March 2016 and released guidance to help non-federal entities share cyber threat indicators with the Federal Government. The Department also released policies and procedures relating to the receipt and use of cyber threat indicators by federal entities, guidelines relating to privacy and civil liberties in connection with the exchange of those indicators, and guidance to federal agencies on sharing information in the government's possession.

Note: The *Non-Federal Entity Sharing Guidance under the Cybersecurity Information Sharing Act of 2015* was updated in October 2020.

Resource Materials

- Non-Federal Entity Sharing Guidance under the Cybersecurity Information Sharing Act of 2015 (PDF, 751.14 KB)
- Privacy and Civil Liberties Final Guidelines: Cybersecurity Information Sharing Act of 2015 (PDF, 400.05 KB)
- Federal Government Sharing Guidance under the Cybersecurity Information Sharing Act of 2015 (PDF, 598.01 KB)
- Final Procedures Related to the Receipt of Cyber Threat Indicators and Defensive Measures by the Federal Government (PDF, 526.17 KB)

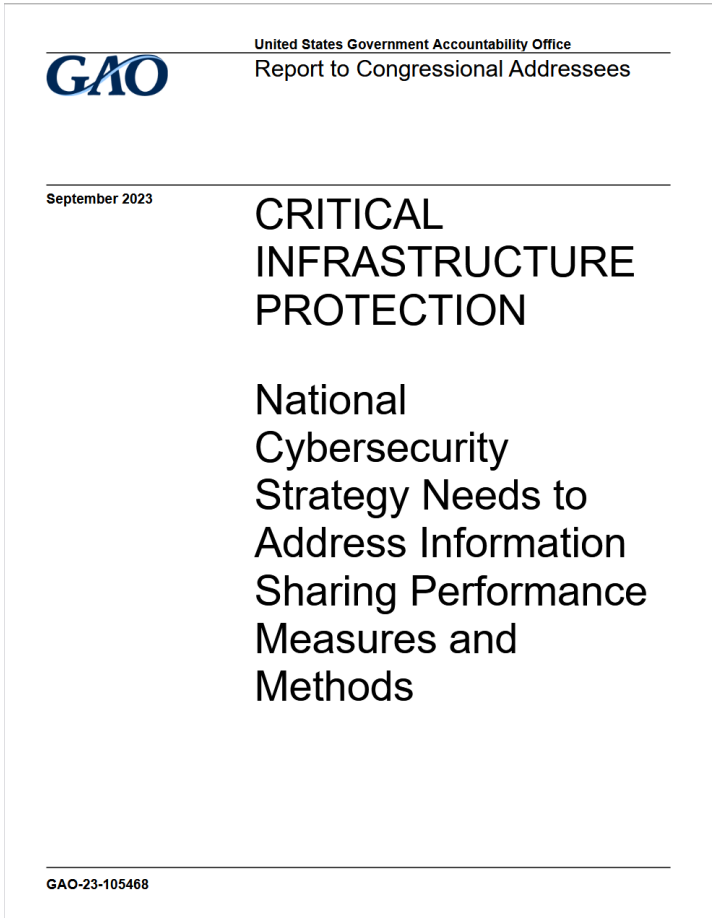
出典：Cybersecurity Information Sharing Act of 2015 Procedures and Guidance
https://www.cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015-procedures-and-guidance



出典：Additional Progress Needed to Improve Information Sharing under the Cybersecurity Act of 2015
https://www.oig.dhs.gov/sites/default/files/assets/2022-08/OIG-22-59-Aug22.pdf

2015CISA法施行後の動き／取組の評価②

- 重要インフラ防護における情報共有活動に対する各行政側の取り組みへの評価について、米会計検査院（GAO）が評価結果を公表（2023年9月）。これまでもGAOは国が進めるサイバー情報共有活動への評価報告を度々公表。


GAO

United States Government Accountability Office

Report to Congressional Addressees

September 2023

CRITICAL INFRASTRUCTURE PROTECTION

National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods

GAO-23-105468

出典：Critical Infrastructure Protection: National Cybersecurity Strategy Needs to Address Information Sharing Performance Measures and Methods
GAO-23-105468
https://www.gao.gov/products/gao-23-105468

指摘のあった課題例：タイムリーな共有の欠如
FBIは2021年10月に発生した選挙管理者を狙ったサイバー攻撃に関する情報について、2022年3月に共有していたとあるセクター調整協議会の関係者が指摘（29頁）

指摘のあった課題例：アクショナブルな情報の欠如
CISAのAISは、セクターごとの情報のカスタマイズがされていないとあるISACの関係者が指摘（31頁）
連邦政府機関が共有するサイバー脅威情報は曖昧／漠然としているとあるセクター調整協議会関係者が指摘（同頁）

指摘のあった課題例：情報共有活動の方式について
Centralized sharing approachとFederated sharing approachの併用が最適なのか評価を行うべき／どちらかを優先すべきかのか検討すべきとGAOが提言

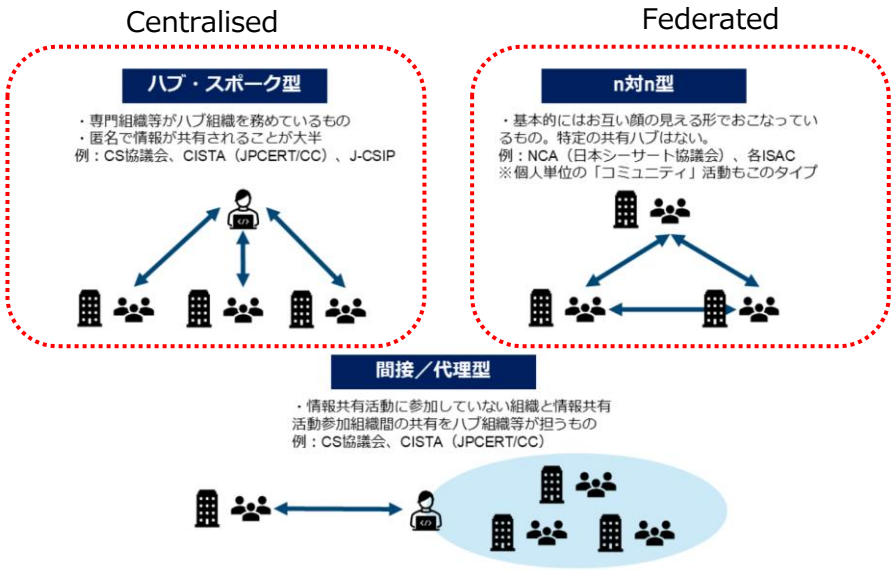


図 32

参考：サイバー攻撃被害に係る情報の共有・公表ガイダンス 図32

NIS2 Directiveにおける情報共有活動促進への言及

● CHAPTER Ⅵ Article 29 Cybersecurity information-sharing arrangements

法案元文	仮訳
1.Member States shall ensure that entities falling within the scope of this Directive and, where relevant, other entities not falling within the scope of this Directive are able to exchange on a voluntary basis relevant cybersecurity information among themselves, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks, where such information sharing: (a)aims to prevent, detect, respond to or recover from incidents or to mitigate their impact; (b)enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative cyber threat research between public and private entities.	1.加盟国は、サイバー脅威、ニアミス、脆弱性、技術及び手順、侵害の指標、敵対的手口、脅威要因固有の情報、サイバーセキュリティ警告、サイバー攻撃を検知するためのサイバーセキュリティツールの構成に関する推奨を含むサイバーセキュリティ関連情報を、本指令の適用範囲に含まれるエンティティ及び関連する場合は本指令の適用範囲に含まれないその他のエンティティが自主的に交換できるようにするものとする： (a)インシデントの予防、検知、対応、回復、またはその影響の軽減を目的とする場合； (b)特に、サイバー脅威に関する意識の向上、当該脅威の拡散能力の制限又は阻害、様々な防御能力、脆弱性の是正及び開示、脅威の検知、封じ込め及び防止技術、緩和戦略、又は対応及び復旧段階の支援、又は官民間のサイバー脅威に関する共同研究の促進を通じて、サイバーセキュリティのレベルを向上させる場合。
2. Member States shall ensure that the exchange of information takes place within communities of essential and important entities, and where relevant, their suppliers or service providers. Such exchange shall be implemented through cybersecurity information-sharing arrangements in respect of the potentially sensitive nature of the information shared.	2. 加盟国は、必要不可欠かつ重要な事業体、および関連する場合にはその供給者またはサービス提供者の共同体内において情報交換が行われることを確保するものとする。このような交換は、共有される情報の潜在的に機微な性質に関して、サイバーセキュリティ情報共有の取り決めを通じて実施されるものとする。
3. Member States shall facilitate the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 of this Article. Such arrangements may specify operational elements, including the use of dedicated ICT platforms and automation tools, content and conditions of the information-sharing arrangements. In laying down the details of the involvement of public authorities in such arrangements, Member States may impose conditions on the information made available by the competent authorities or the CSIRTs. Member States shall offer assistance for the application of such arrangements in accordance with their policies referred to in Article 7(2), point (h).	3. 加盟国は、本条第2項にいうサイバーセキュリティ情報共有の取決めの確立を促進するものとする。当該取決めは、専用のICTプラットフォームおよび自動化ツールの使用、情報共有取決めの内容および条件を含む運用要素を規定することができる。このような取決めにおける公的機関の関与の詳細を定めるにあたり、加盟国は、所轄官庁又は CSIRT が利用可能とする情報に条件を課すことができる。加盟国は、第 7 条(2)の(h)に言及された政策に従って、そのような取決めの適用のための支援を提供する。
4. Member States shall ensure that essential and important entities notify the competent authorities of their participation in the cybersecurity information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.	4. 加盟国は、不可欠かつ重要な主体が、第2項で言及されたサイバーセキュリティ情報共有の取決めに参加する場合、当該取決めを締結した時点で、または、場合によっては、当該取決めから脱退する場合、当該脱退が発効した時点で、当該主体が所管当局に通知することを確保するものとする。
5. ENISA shall provide assistance for the establishment of cybersecurity information-sharing arrangements referred to in paragraph 2 by exchanging best practices and providing guidance.	5. ENISA は、ベストプラクティスを交換し、ガイダンスを提供することにより、第 2 項で言及されるサイバーセキュリティ情報共有取決めの確立を支援するものとする。

出典：DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32022L2555

海外における情報共有活動成功例と課題

○成功例

- ニューヨーク州立大学オールバニ校のCEHC(The College of Emergency preparedness, Homeland security and Cybersecurity)とCIS(Center for Internet Security)、MS-ISAC(Multi-State Information Sharing & Analysis Center）が共同で発表した情報共有の成功事例紹介の取り組みによると、**分野毎に編成されたISAC内での情報共有に効果がある**こと（※既に国内でもその前提で各ISACの活動などの情報共有活動が行われている）に加えて、**ISAC単位で政府や外部専門組織、他のISACと外部連携することの効果**が各紹介事例から読み取れる。

（例）

ー標的でない分野のISACが、外部情報提供を基に追加調査を行い、特定分野への攻撃キャンペーンを発見。

ーMS-ISACがある不審な通信元を調査したことをきっかけに、ISAC外との連携により、航空分野を狙ったAPTキャンペーンを発見。

○課題例

- 2020年12月13日、SolarWinds社は同社のネットワーク監視ソフトウェア「Orion Platform」に、正規のアップデートを通じてマルウェアが仕込まれたことを公表。
- 攻撃は2019年9月には始まっていたとみられ、2020年3月～6月のアップデートファイルが侵害されたことで、**米政府機関等を含む最大約18,000組織が影響を受けた**とされる。
- 事案発覚の半年前に米司法省が（自組織への）侵害に気付いており、またいくつかの事案に複数のセキュリティベンダが事案調査を始めていたが、**全体としての連携・共有が行われていなかった**のではないかとの指摘あり。

出典：
Success Stories in Cybersecurity Information Sharing
https://www.albany.edu/sscis
Kim Zetter, “The DOJ Detected the SolarWinds Hack 6 Months Earlier Than First Disclosed”, WIRED, April 28, 2023
https://www.wired.com/story/solarwinds-hack-public-disclosure/
「最近の産業サイバーセキュリティに関する動向について」, 経済産業省（令和3年11月, 4ページ）
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_uchu_sangyo/pdf/003_03_00.pdf