経済産業省

資料３－４

経済産業省におけるサイバーセキュリティ施策の取組状況について

令和５年１２月２０日

経済産業省

サマリ

- 令和5年11月22日に「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」を公表。同時に「攻撃技術情報の取扱い・活用手引き（案）」及び「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」を公表。同案について、令和5年11月22日から令和5年12月22日までの期間で意見募集を実施中。

- 令和5年12月21日に、高圧ガス保安法等の一部を改正する法律（令和四年法律第七十四号）が施行。

経済産業省の情報共有促進の検討会HP：
https://www.meti.go.jp/press/2023/11/20231122002/20231122002.html

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概要

１．情報共有の重要性と現状の課題

- 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**。他方で、被害組織自らが情報共有を行うことについては、①被害組織側の調整コスト負担、②最適者が事案対応を行わない懸念、③処理コストのかかる情報共有、④被害現場依存の脱却の必要性などの課題が存在。

２．本検討会における提言

- **被害組織を直接支援する専門組織を通じた速やかな情報共有の促進が重要。**これにより、①全体像の解明による被害拡大の防止や②被害組織のコスト低減などが実現できる。
- 他方で、専門組織を通じた情報共有を促進するためには、**①秘密保持契約による情報共有への制約、②非秘密情報からの被害組織の特定/推測の可能性の課題に対応をする必要がある。**
- このため、本検討会では、これらの課題を乗り越え、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を可能とするために、被害者の同意を個別に得ることなく速やかな情報共有が可能な情報の考え方を整理。具体的には、通信先情報やマルウェア情報、脆弱性関連情報等の**「攻撃技術情報」から被害組織が推測可能な情報を非特定化加工した情報が対象となり得る**と整理。
- さらに、本報告書の提言を補完する観点から、**「攻撃技術情報の取扱い・活用手引き（案）」についてもとりまとめ**。本手引きでは、専門組織間で効果的な情報共有を行うために、どのような形で非特定化加工を行えばよいか、またどのように情報共有をおこなえばよいのかなど**専門組織として取るべき具体的な方針について整理**。
- 加えて、円滑な情報共有を促進すべく、上記考え方について**ユーザー組織と専門組織が共通の認識**を持ち、専門組織が非特定化加工済みの攻撃技術情報を共有したことに基づく**法的責任を原則として負わないことを合意するため**の**秘密保持契約に盛り込むべきモデル条文案を提示。**今後、本検討会の成果の**周知・啓発に取り組む**。

３．今後の課題

- 専門組織同士の情報共有促進だけでは解消されない**今後の課題**としては、**（１）情報共有に向けた官民連携のあり方**（行政機関への相談・報告のあり方や政府と民間事業者間の情報の共有など）、**（２）サプライチェーンにおけるベンダ等の役割**を挙げた。

(参考)「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」構成員

１．委員

阿部　慎司	GMOサイバーセキュリティ　byイエラエ（株） 執行役員・SOCイノベーション事業部長
石川 芳浩	（株）ラック
神林　彰	富士フイルムビジネスイノベーション（株） CP＆RM部 情報セキュリティセンター センター長
庄子　正洋	トレンドマイクロ（株） サイバーセキュリティ・イノベーション研究所スレットリサーチャ
武井 滋紀	NTTテクノクロス（株）セキュアシステム事業部　エバンジェリスト
武智　洋	サプライチェーンサイバーセキュリティコンソーシアム(SC3)運営委員 日本電気（株）サイバーセキュリティ戦略統括部　エグゼクティブエキスパート
辻　伸弘	SB テクノロジー（株）　プリンシパルセキュリティリサーチャー
蔦　大輔	森・濱田松本法律事務所　弁護士
名和　利男	サイバーディフェンス研究所　専務理事/上級分析官
北條　孝佳	西村あさひ法律事務所・外国法共同事業　パートナー弁護士
星　周一郎	東京都立大学法学部　教授
和田　昭弘	（一社）日本経済団体連合会サイバーセキュリティ委員会　サイバーセキュリティ強化WG主査 全日本空輸株式会社 デジタル変革室 専門部長

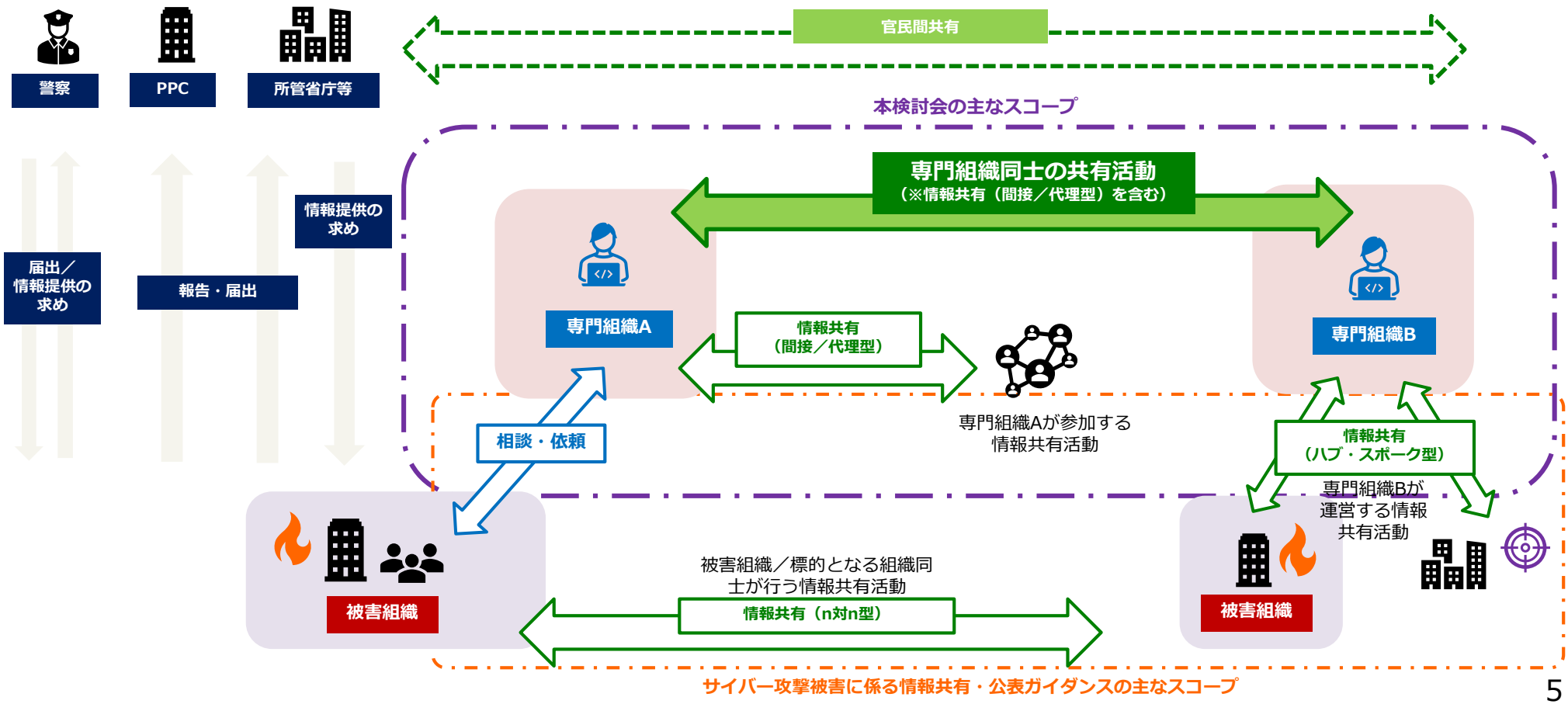
座長

２．オブザーバー

内閣官房内閣サイバーセキュリティセンター、内閣官房サイバー安全保障体制整備準備室、警察庁、
個人情報保護委員会、総務省、最高検察庁

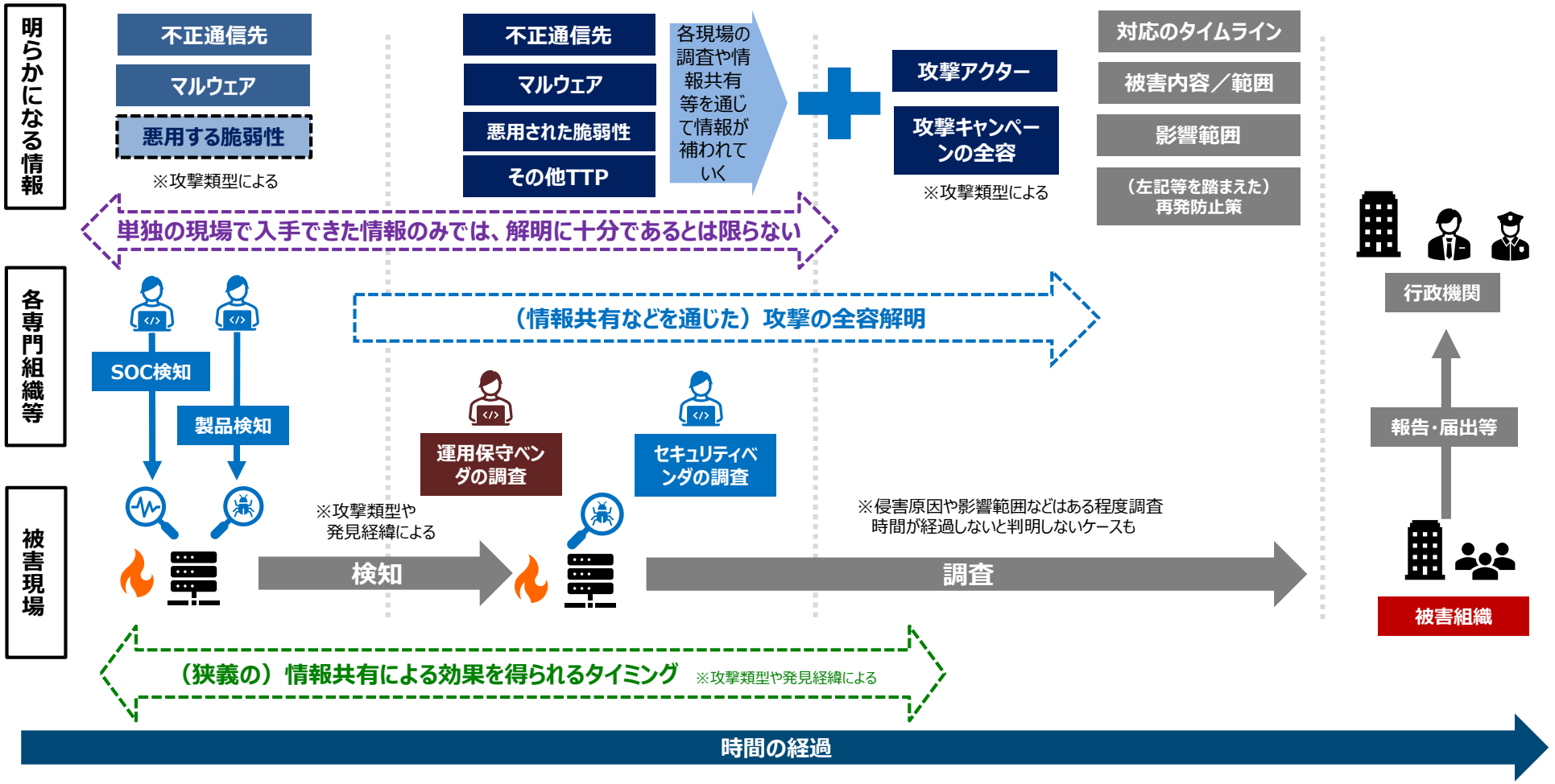
(参考)各組織間の情報共有の全体像と本検討会の主なスコープ

- 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。



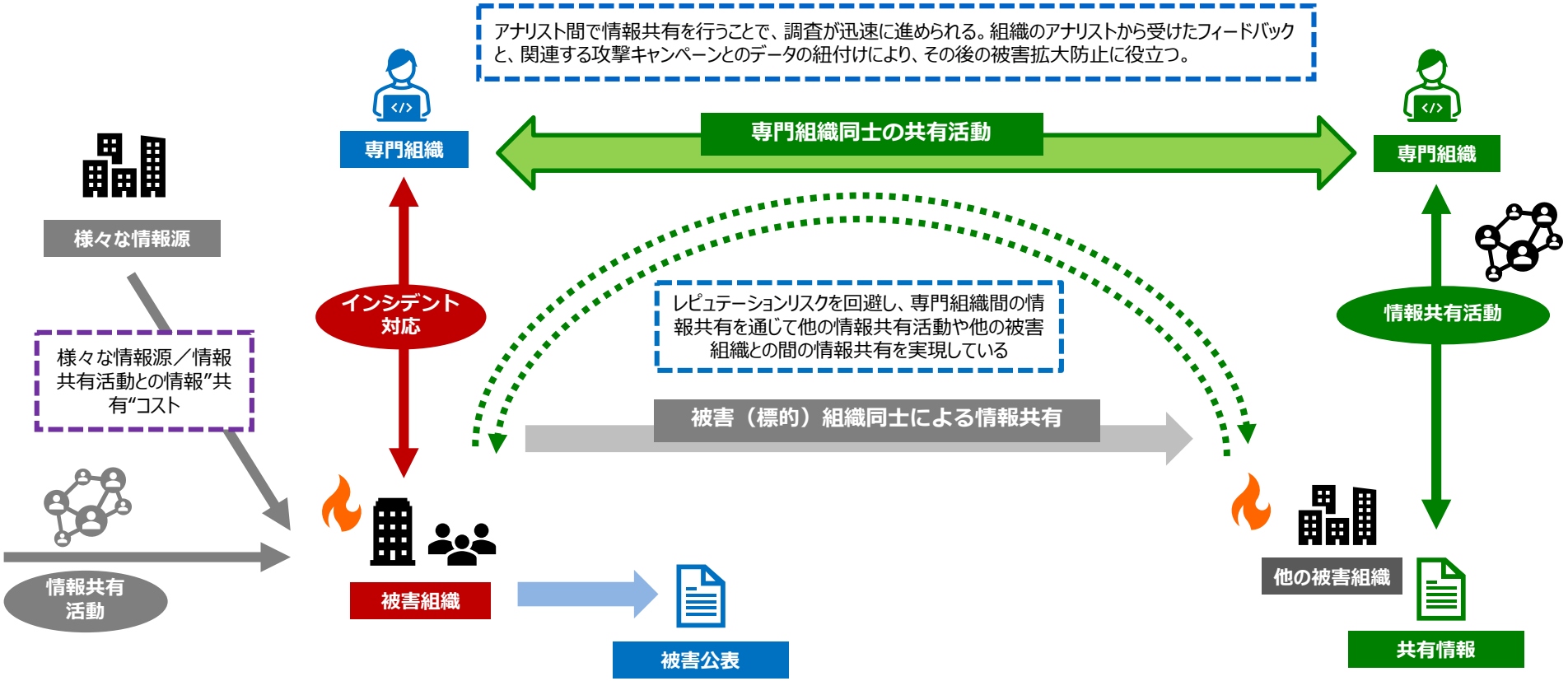
(参考)専門組織による情報共有活動の重要性①：全体像の解明

- 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。



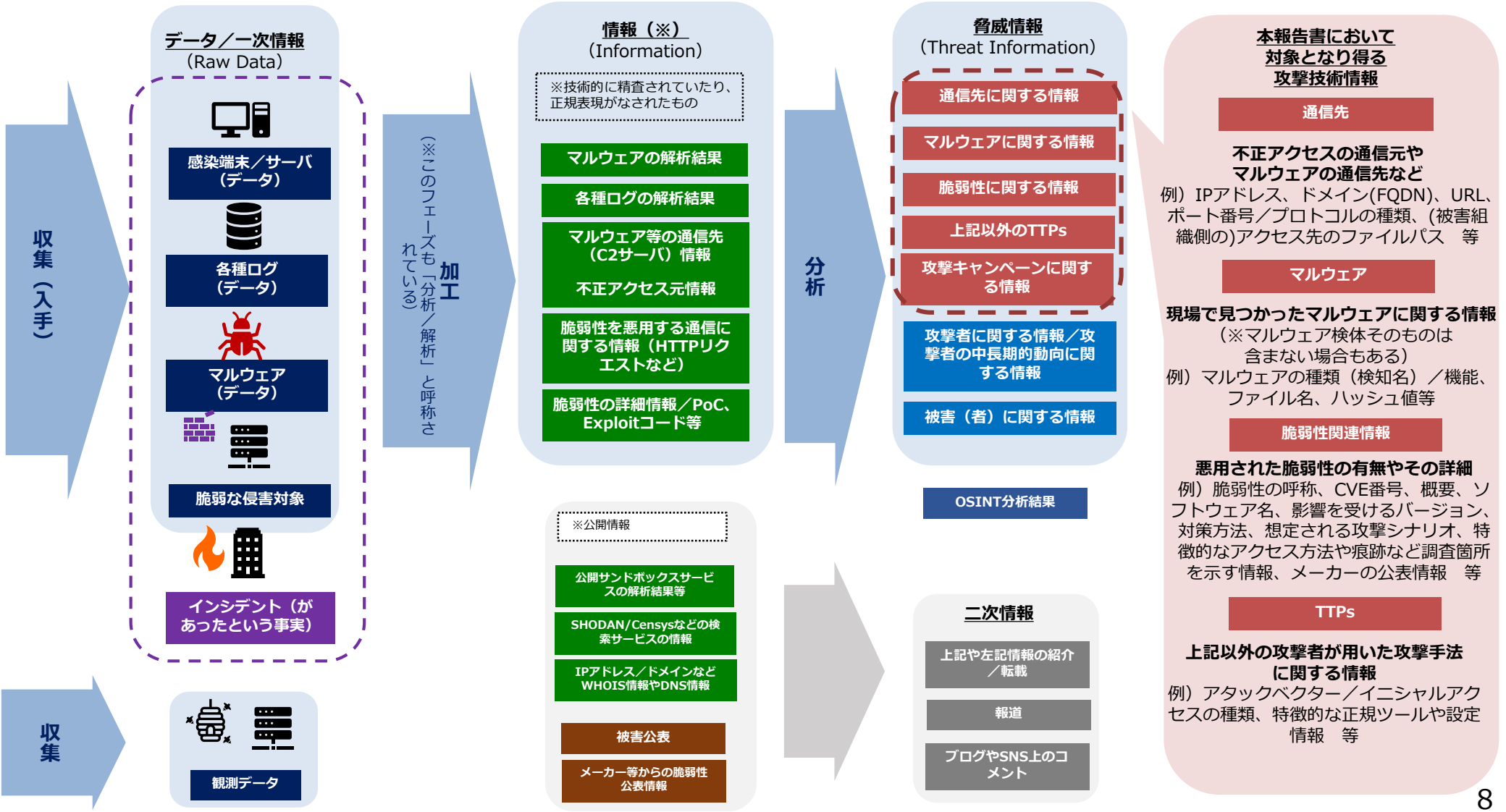
(参考)専門組織を通じた情報共有の重要性②：被害者組織のコスト低減

- 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。



（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。



(参考)攻撃技術情報の取扱い・活用手引き（案）

- 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

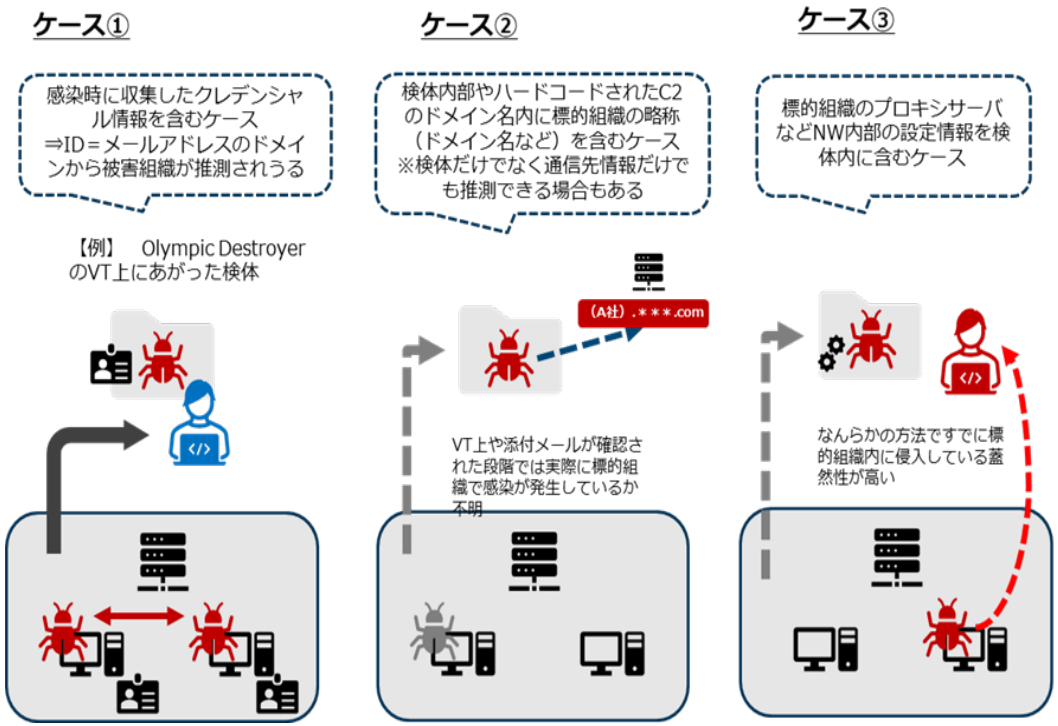
はじめに
・スコープとしている情報共有活動
・用語の定義
・本手引きの想定読者

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」いついて
・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：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



(参考)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

- 専門組織を通じた情報共有を促進し、被害組織の被害に対する迅速な調査や被害拡大防止等を目的として、あらかじめ被害組織（ユーザー組織。甲）と専門組織（乙）間で合意しておく攻撃技術情報等の取扱いや円滑な情報共有のための関連事項（保有情報に対する安全管理措置や免責事項など）を示すもの。

１．乙は、本サービスの遂行過程において、乙の知見により得られたサイバー攻撃に関する通信先、マルウェア、脆弱性その他の情報（以下この条において「攻撃技術情報」という。）について、甲の被害に対する迅速な調査、被害拡大の防止及び甲乙以外の組織に対するサイバー攻撃の未然防止を目的としてこれを保有又は利用し、また、甲を識別及び特定できないように加工した攻撃技術情報（以下この条において「攻撃技術情報」及び「甲を識別及び特定できないように加工した攻撃技術情報」を合わせて「攻撃技術情報等」という。）を作成、保有、利用又はサイバーセキュリティに関する専門組織に対して開示することができる。

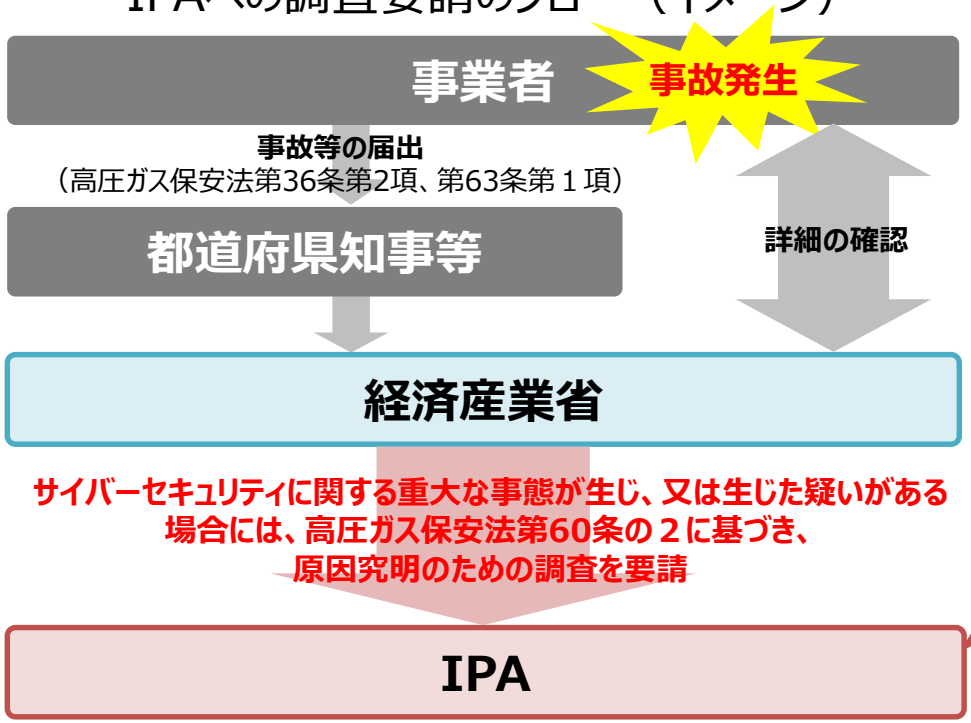
２．乙は、保有する攻撃技術情報等について、必要かつ適切な安全管理措置を講じなければならず、前項の目的を達成するために必要な範囲を超えて攻撃技術情報等を開示してはならない。

３．乙は、第１項及び第２項の攻撃技術情報等の利用又は開示に関連して、甲に生じた損害については一切の法的責任を負わないこととする。ただし、乙に故意又は重過失がある場合は、この限りでない。

サイバーインシデントに係る事故調査

- 諸外国においては、サイバー攻撃による石油パイプラインの操業停止や、電力関連施設へのサイバー攻撃による停電といった事案が発生しており、我が国においても、**産業保安関連設備に対するサイバー攻撃のリスクが懸念**。
- 昨年公布された改正保安3法（令和5年12月21日施行）に基づき、**電気、高圧ガス、ガス分野においてサイバーセキュリティに関する重大な事態が生じ、又は生じた疑いがある場合**には、国は、**独立行政法人情報処理推進機構（以下「IPA」という。）に原因究明調査を要請。**
- 事故調査は、**原因究明による再発防止を目的に実施**。調査結果を踏まえ、サイバーセキュリティ水準の向上を図るための対策を講じることを想定。

IPAへの調査要請のフロー（イメージ）



IPAによる調査のイメージ

- ✓ IPAは対象システムのログ等を確認することによって、サイバーセキュリティに関する重大な事態が生じた原因を究明するための調査を行う。
- ✓ IPAによる調査は、書面審査と現地調査の二段階で構成する。
  ※ただし、書面調査のみで十分に原因を特定できた場合には、現地調査は行わない。
- ✓ 調査日数や調査内容等は、IPAと事業者で相談の上、決定する。

改正高圧ガス保安法
第六十条の二　経済産業大臣は（中略）**保安に係るサイバーセキュリティ（中略）に関する重大な事態が生じ、又は生じた疑いがある場合**において、必要があると認めるときは、**独立行政法人情報処理推進機構に対し、その原因究明のための調査を要請することができる**。