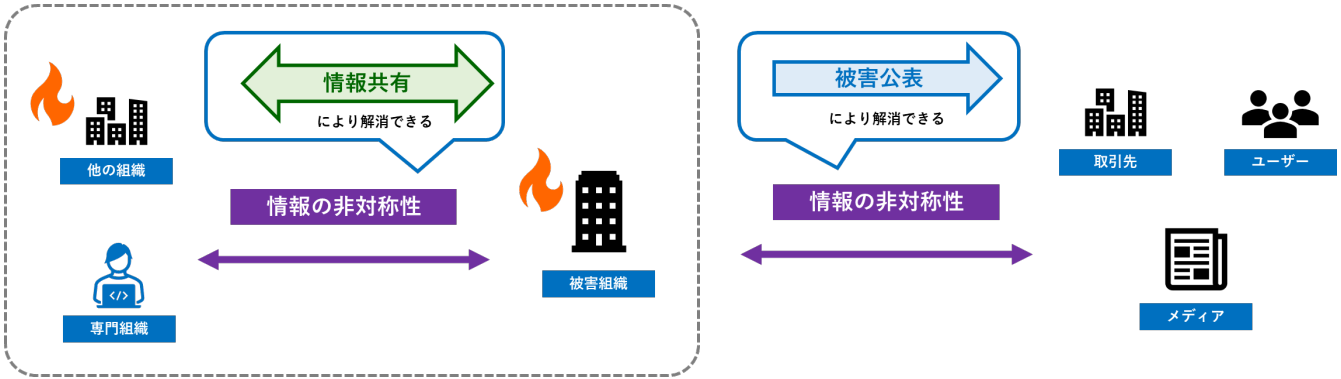
サイバー攻撃被害に係る情報の共有・公表ガイダンスの概要

令和５年３月８日
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

本ガイダンス検討における問題意識

- 攻撃手法が高度化する中で、単独組織による攻撃の全容解明はより困難になっている。他方で、被害組織はお互いに「他にどのような情報が存在するかを知ることができない」ため、情報共有がなかなか行われにくく、また、共有タイミングも遅いケースが多い。
- 第三者との関係などサイバー攻撃被害が複雑化する中で、被害組織のインシデント対応が適切になされているかどうかが外部から確認できず、また、被害組織も被害公表を通じた情報の開示に消極的なため、被害組織によるインシデント対応（結果）に不安や警戒を募らせるような状況になっている。

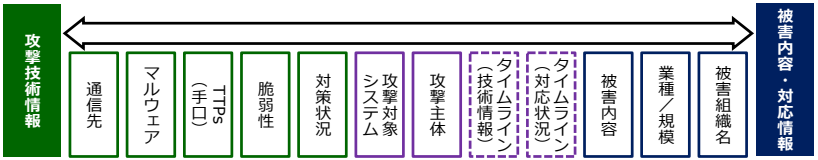
⇒ こうした情報の非対称性を解消する手段である**「情報の共有」「被害の公表」のポイントを示した参考資料がない**



本ガイダンスの目的・概要

- 被害組織の担当部門（例：セキュリティ担当部門、法務・リスク管理部門等）を主な想定読者とし、被害組織を保護しながら、いか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形式でまとめたものです。

どのような情報を？（様々な種類・性質の情報が存在）



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）

想定読者（被害組織等）

本ガイダンスの構成

- 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

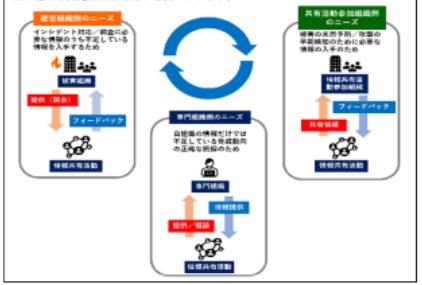
＜情報共有の方法等について＞

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。

前者は被害組織個別の目的として、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、対応が間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。

本ガイダンスで示す情報共有・被害公表のポイント

本ガイダンスは、被害組織で見つかった情報を「何のために」「どのような情報を」「どのタイミングで」「どのような主体に対して」共有／公表するのか、ポイントを整理したものです。

1.情報共有

- **(1)目的：**被害調査に必要な情報の提供や被害の未然防止に資する【→概要8ページ】
- **(2)タイミング：**情報共有と被害公表を分離し、迅速な情報共有を図る【→概要9ページ】
- **(3)情報の整理：**攻撃に関する情報（攻撃技術情報）と被害に関する情報（被害内容・対応情報）を分離し、迅速な攻撃技術情報の共有を図る【→概要10ページ】

2.被害公表

- **(1)目的：**レピュテーションリスク低下やインシデント対応上の混乱の回避に資する【→概要11ページ】
- **(2)タイミング：**攻撃の種類や被害の状況から、効果的な公表タイミングを選ぶ【→概要12ページ】
- **(3)情報の整理：**専門組織との連携や情報共有活動の状況など対応の経緯等を含めて示すことで、ステークホルダーの不安等を解消することができる【→概要13ページ】

3.外部組織との連携

- 専門組織との連携、警察への通報・相談、所管官庁への報告等を実施することで、正確な情報共有や注意喚起、捜査を通じた犯罪抑止や広く国民に影響する事案への対処等につなげることができる【→概要14ページ】

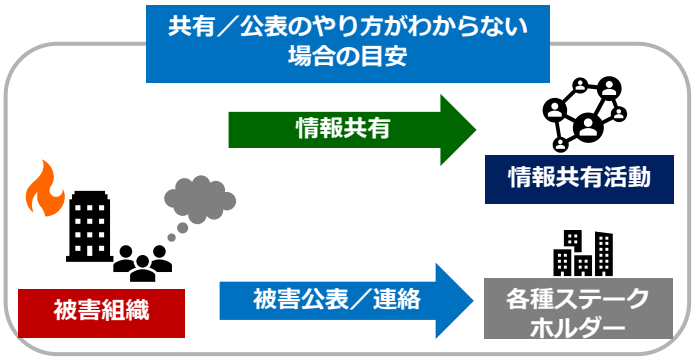
4.機微な情報への配慮

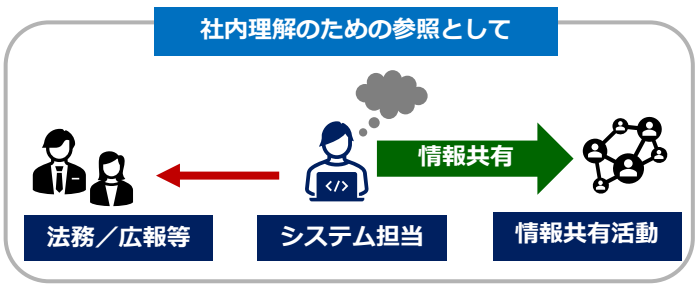
- 被害者への保護や機微な情報への配慮が必要な情報の取扱いを知ることで、スムーズな情報共有、被害公表を行うことができる【→概要15ページ】

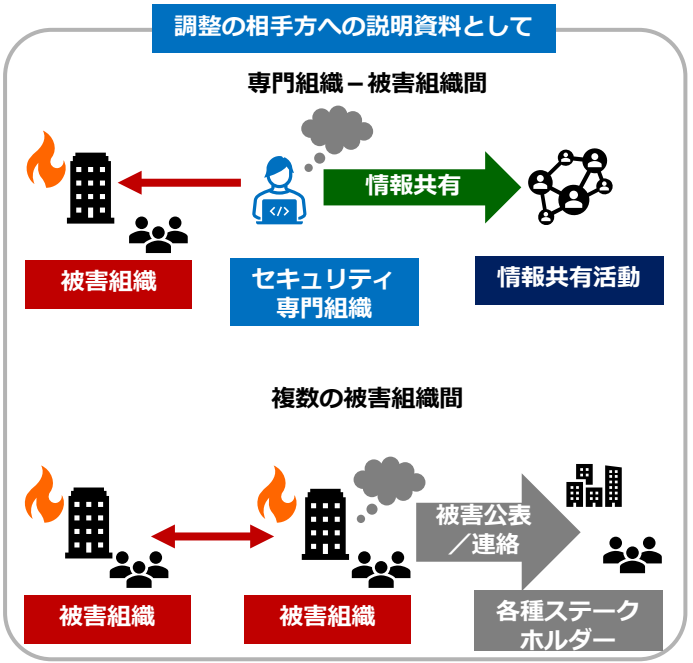
本ガイダンスの目次

本ガイダンスの使い方

- 被害組織の担当部門が情報共有／被害公表を行うにあたっての参考とするだけでなく、情報共有／被害公表に関わる関係者間の共通理解促進のために活用することができます。



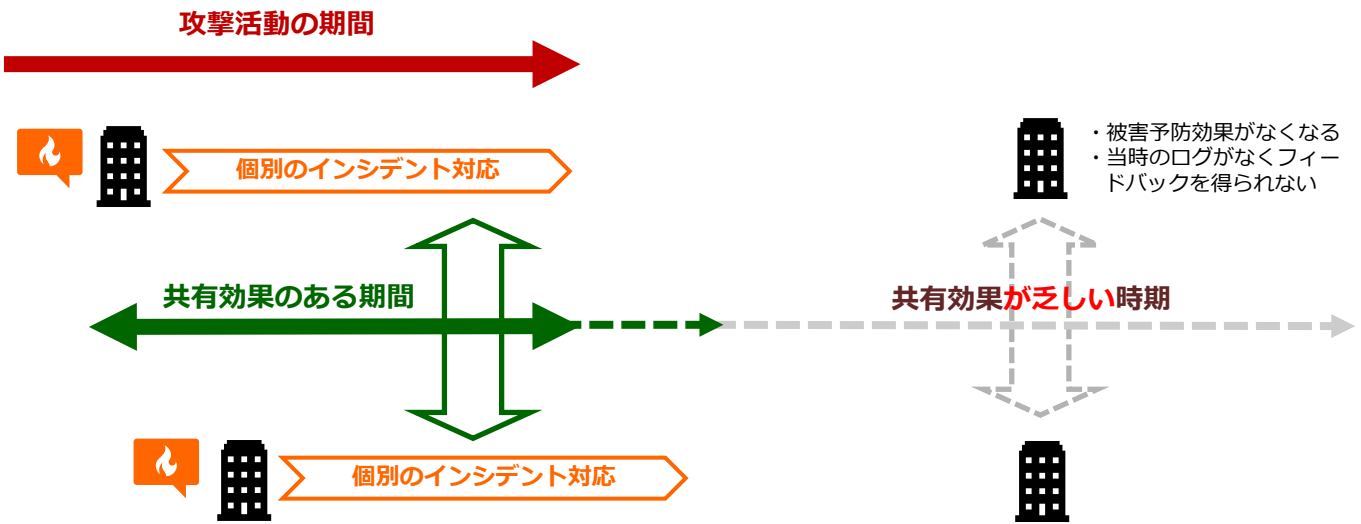




以下、本ガイダンスで示すポイントの詳細

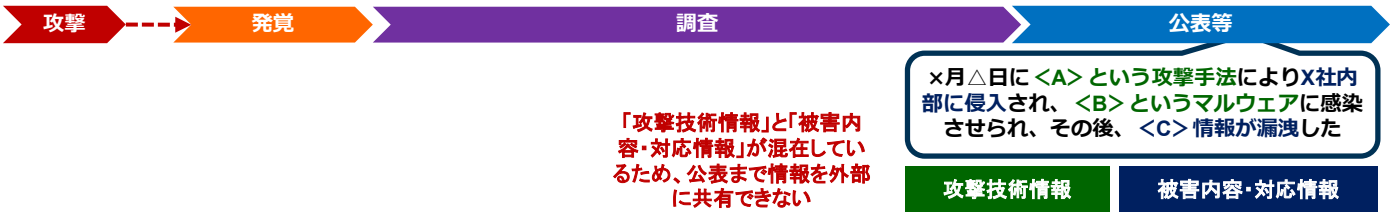
1.(1) 情報共有の目的：速やかな情報共有の必要性

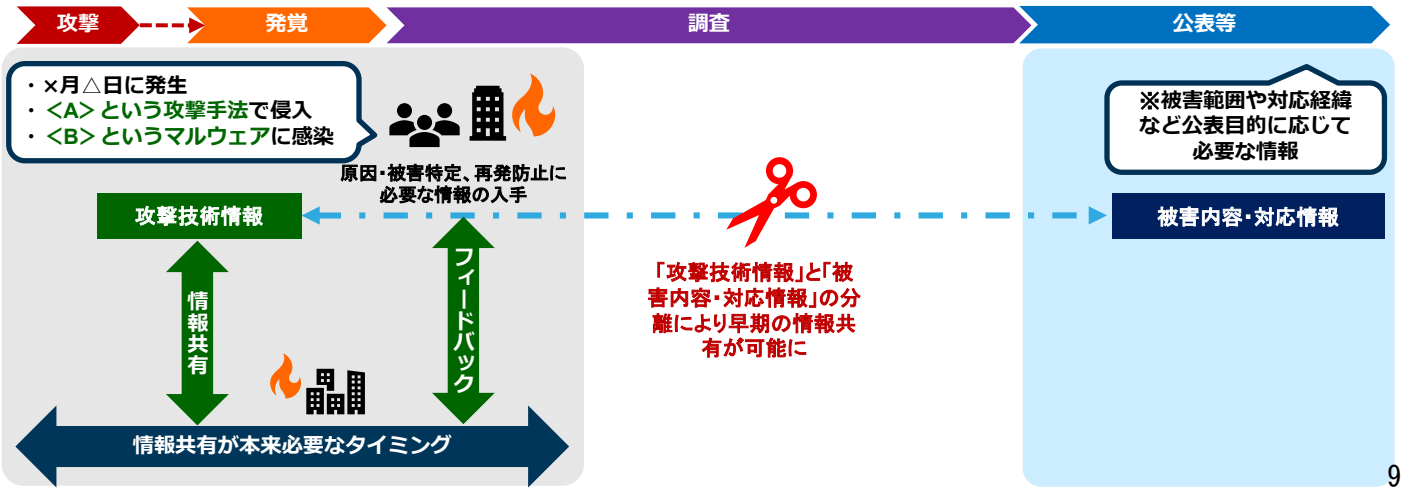
- 被害予防や攻撃の全容把握（インシデント対応や調査に必要な情報の入手）を目的とした情報共有活動において、攻撃に関する情報（技術情報）の共有は早ければ早いほど効果的である
- 速やかな技術情報の共有により、情報共有効果（フィードバック情報を得ることや被害を未然に防ぐこと）を得ることができる



1.(2) 情報共有のタイミング：「共有」と「公表」の分離

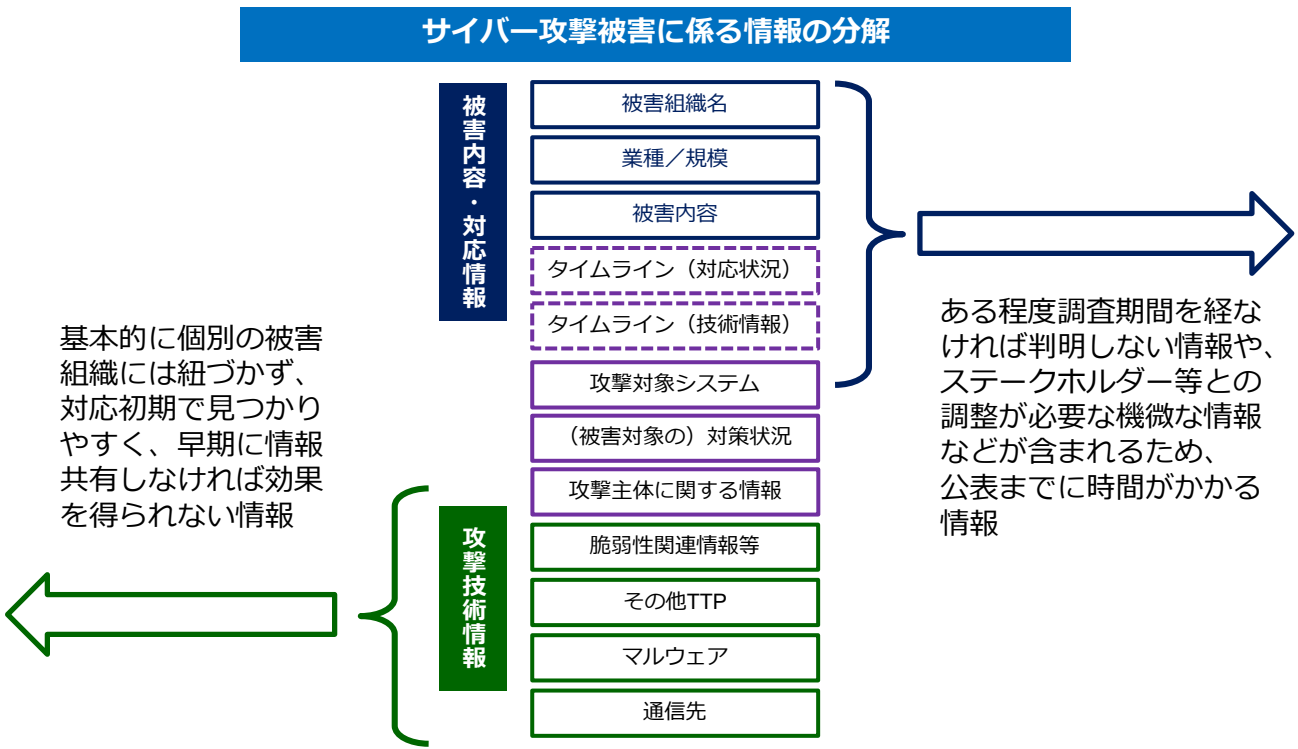
- すべての情報発信が公表タイミングに集中してしまうと、効果的なタイミングでの共有ができなくなってしまう
- 非公開での情報共有と、被害情報の公表を切り分けることで、速やかな情報共有を行うことができる





1.(3) 共有情報の整理：攻撃技術情報と被害内容・対応情報の分離

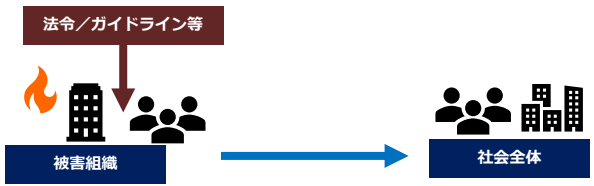
■ 情報を整理し切り分けることで、速やかな情報共有を行うことができる



2.(1) 被害公表の目的

- 目的を整理することで、公表を行うべきタイミング、公表に必要な情報を決めることができる

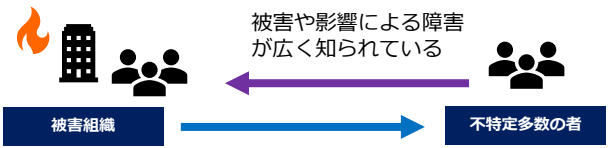
法令／ガイドライン等で求められるもの



注意喚起の目的で行うもの

※専門組織を通じて行われることが望ましいケースもある。

発生事象に対する対外説明として行うもの

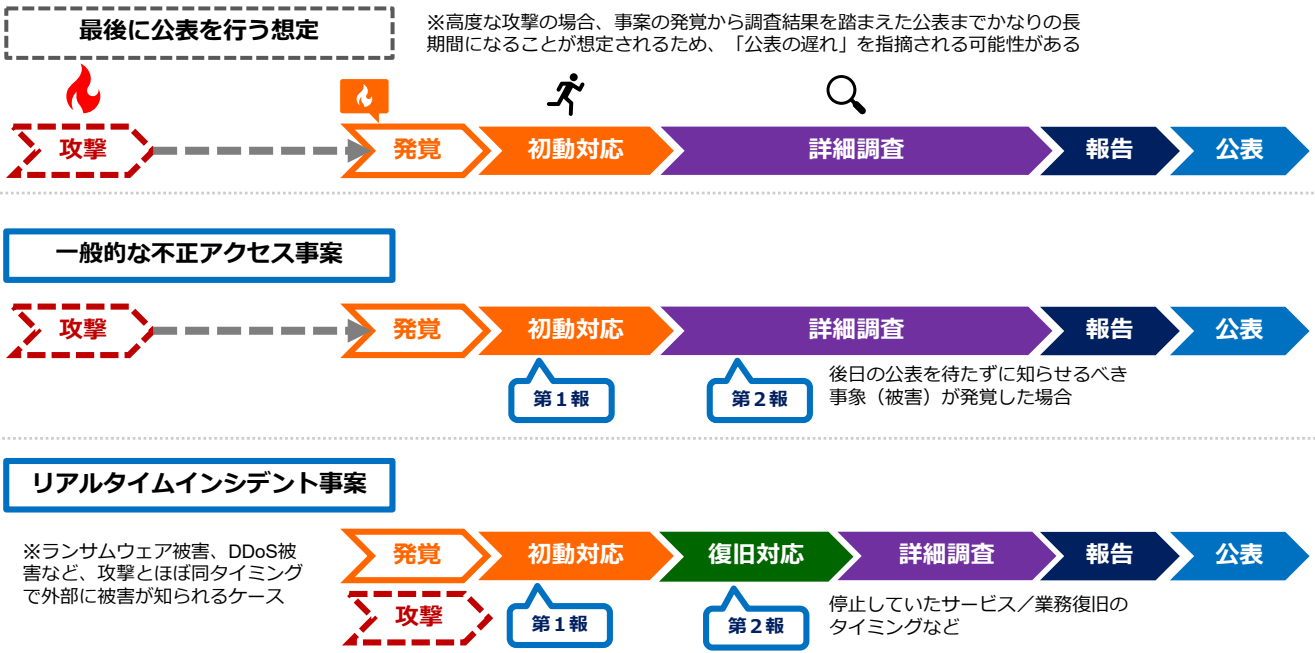


広報／リーガルリスク対応として行うもの

なんらかの経緯で発覚した場合、問い
合わせが多数来ることが想定される

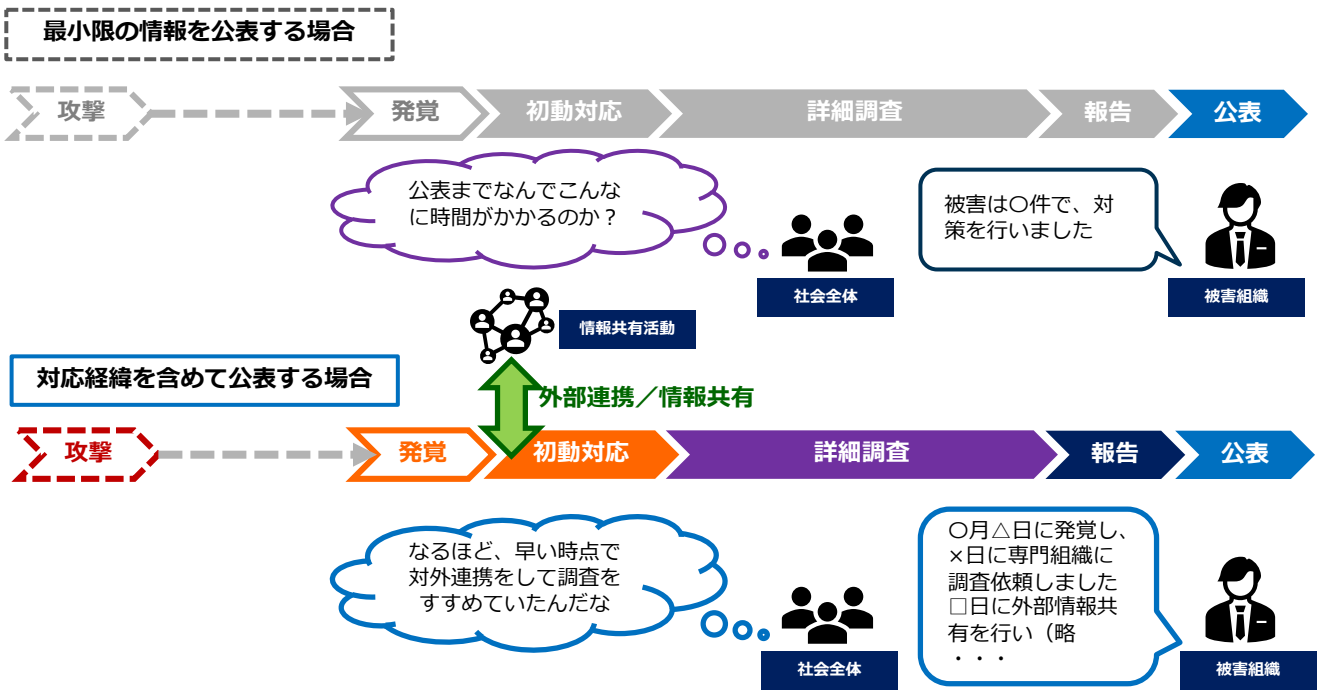
2.(2) 被害公表のタイミング

- すべての調査を終えてから最後に公表を行うだけでなく、二次被害が発生するおそれや社会的にインパクトの大きな被害が判明した時点で、適宜第一報的な公表を検討することが望ましい
- このほか任意／適宜の公表をこまめに行うことで、正確な情報をステークホルダー等に伝えることができる



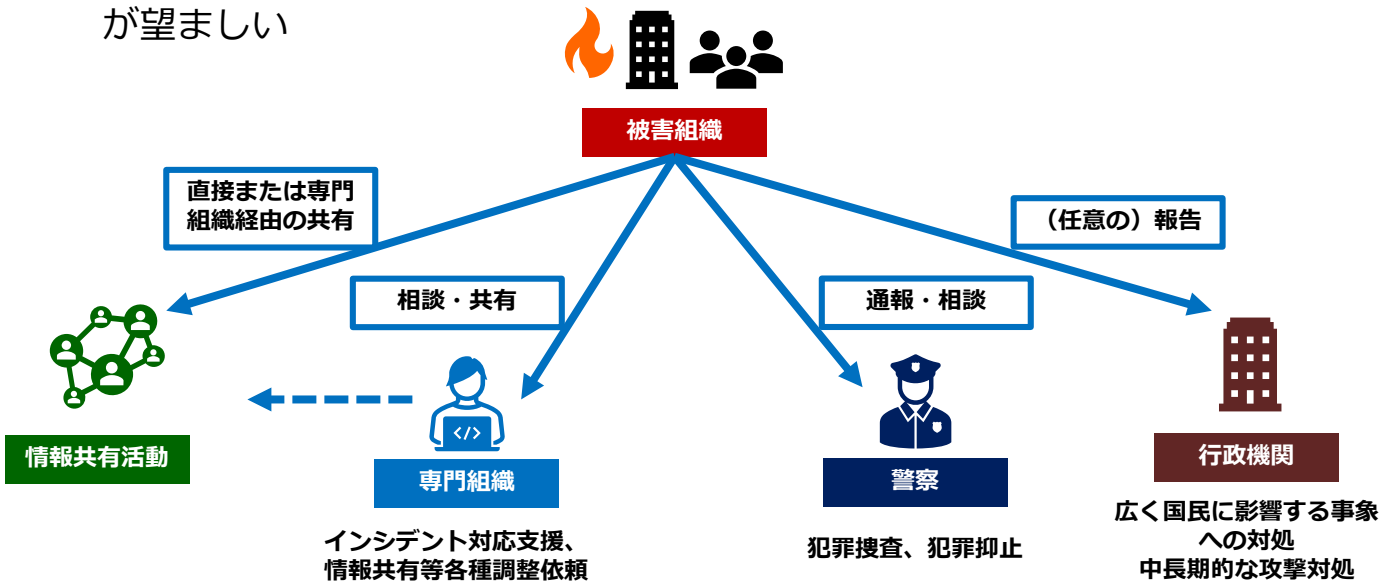
2.(3) 被害公表内容の整理

- 公表まである程度の期間が経過する場合は、「公表までにどのような対応を行ったのか」を示すことで、インシデント対応に対する不安や警戒の解消につなげることができる



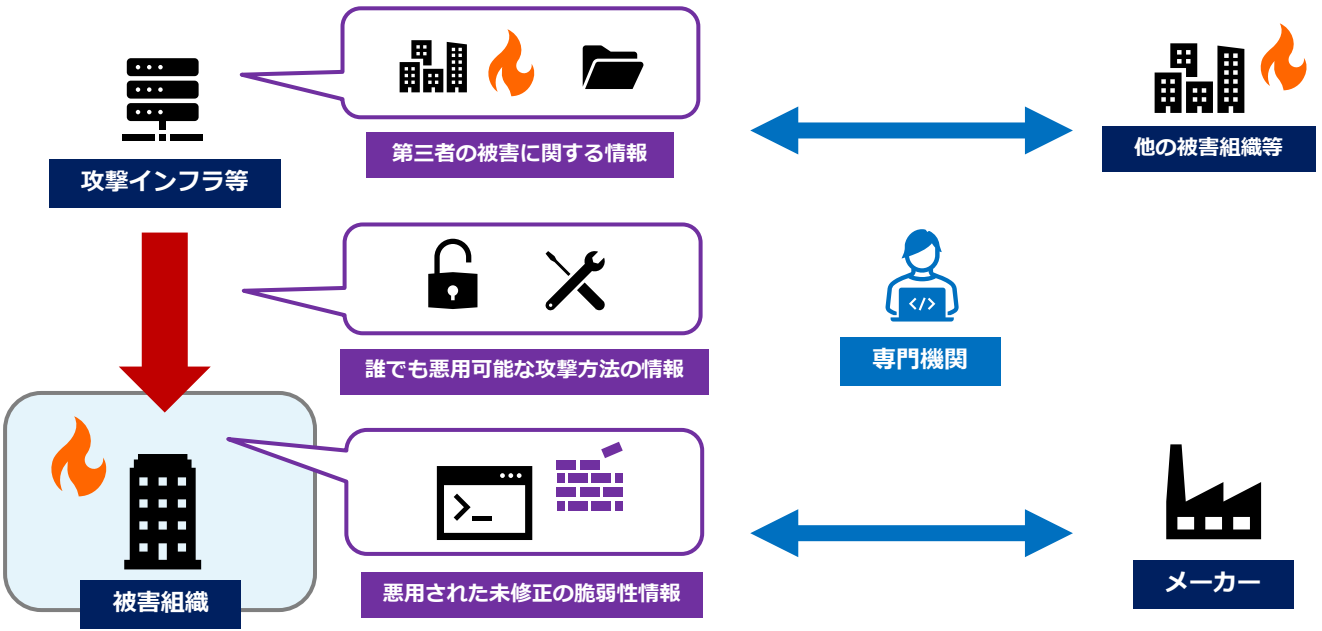
3. 外部組織（専門組織、警察、行政機関等）との連携

- 情報共有活動に元々参加していない被害組織は情報共有活動のハブ組織／窓口である専門組織経由で情報共有に参加することができる
- 情報共有や調査に必要な情報の入手のためだけでなく、テイクダウン依頼や脆弱性修正に向けた調整依頼を行うことができる
- 犯罪捜査を通じた抑止力の向上や広く国民に影響する事象への対処につなげるため、警察への通報・相談及び所管省庁への報告などを行うことが望ましい



4. 機微な情報への配慮

- 悪用された未修正の脆弱性情報や、攻撃インフラ等に存在する「第三者の被害を示す情報」（被害企業を示す情報や漏洩データなど）に対しては、専門機関を通じた関係者間の調整を行うことができる
- 第三者の不利益になるような機微な情報の取扱いについては、専門機関等を通じた関係者間の調整と情報の精査を経て、共有／公表することができる

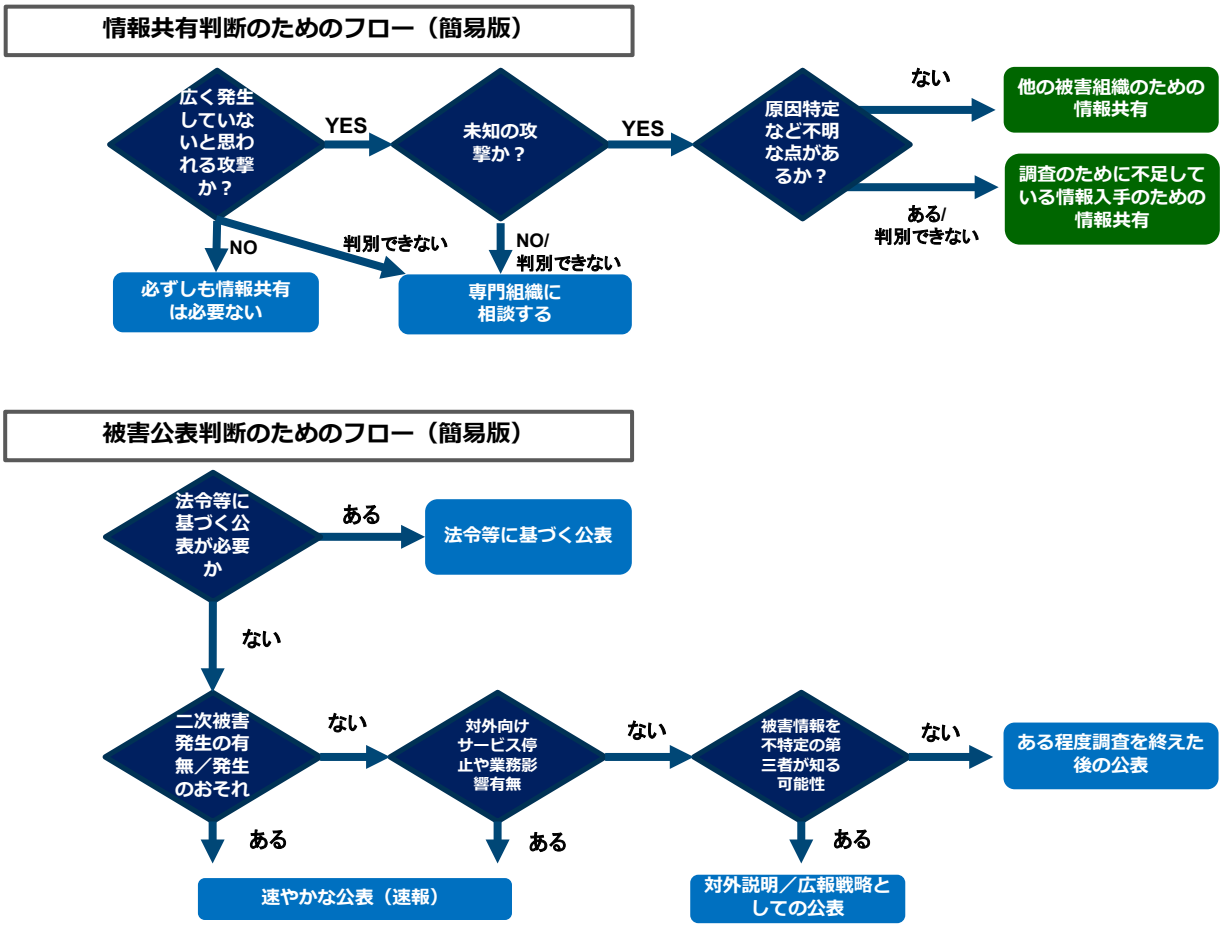


情報共有と被害公表における情報の種類のチェックリスト（簡易版）

	情報共有	被害公表
タイミング	可能な限り早期のタイミング	ケースバイケース ※二次被害発生のおそれなど注意喚起を目的とする速報が必要な場合はただちに公表
被害内容・対応情報 ・被害組織名 ・被害業種／規模 ・被害内容 ・対応のタイムライン	―	○
中間の情報 ・攻撃のタイムライン ・攻撃対象システムについて ・脆弱性悪用の情報等	△ ※共有に必要なものは専門機関への相談等を踏まえて共有することが望ましい	○
攻撃技術情報 ・マルウェア ・不正通信先 ・その他攻撃手法に関する情報	○	△

○：主な内容となる情報　△：内容／状況による　―：基本的に対象外

フローシート（簡易版）


情報共有判断のためのフロー（簡易版）
広く発生していないと思われる攻撃か？
YES
未知の攻撃か？
YES
原因特定など不明な点があるか？
ない
他の被害組織のための情報共有
ある/判別できない
調査のために不足している情報入手のための情報共有
NO
必ずしも情報共有は必要ない
判別できない
NO/判別できない
専門組織に相談する
被害公表判断のためのフロー（簡易版）
法令等に基づく公表が必要か
ある
法令等に基づく公表
ない
二次被害発生の有無／発生のおそれ
ない
対外向けサービス停止や業務影響有無
ない
被害情報を不特定の第三者が知る可能性
ない
ある程度調査を終えた後の公表
ある
速やかな公表（速報）
ある
ある
対外説明／広報戦略としての公表