

# 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

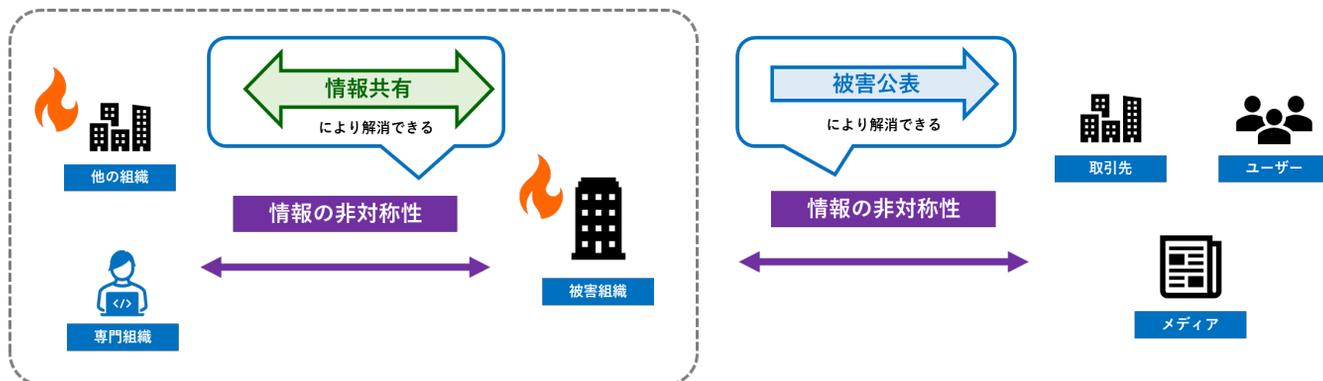
令和5年3月8日

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

# 本ガイド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



# 本ガイドンスの目的・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）



## 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



運用保守ヘンダ等

## 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

# 本ガイドンスの構成

- 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

用語集	3
用語集補足	6
1. はじめに	9
—情報共有とは何か/公表とは何か	9
—なぜ「情報共有をすべし」なのか/公表の社会的意義	13
—本ガイドンスのコンセプト	17
—本ガイドンスの検閲経緯	20
—本ガイドンスのスコープ	21
—本ガイドンスを讀むにあたって	27
2. 情報共有・被害公表の流れ	31
3. FAQ	33

### <情報共有の方法等について>

Q1. なぜ情報共有が必要なのか？	33
Q2. どのタイミングでどのような情報が共有/公表されますか？	36
Q3. 「被害組織」とは何ですか？	37
Q4. サイバー攻撃被害に係る情報にどのようなものがありますか？	38
Q5. どうやって「情報共有」をすればいいのですか？	44
Q6. どのような情報を共有すればいいのですか？	47
Q7. 「インディケータ情報」とは何ですか？	51
Q8. いつ情報を共有すればいいのですか？	57
Q9. 情報共有活動に参加していない場合、どこに共有すればいいのですか？	59
Q10. 情報共有を行う上での留意点がありますか？	62
Q11. 攻撃技術情報の共有とノウハウの共有とは何が違いますか？	63
Q12. 専門組織同士はどういう情報を共有していますか？	64
Q13. なぜ非公開で参加者が限定された情報共有が行われるのですか？	66

## FAQパート

### <情報共有の方法等について>

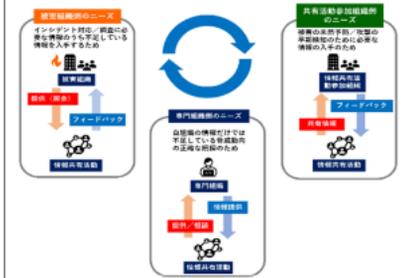
#### Q1. なぜ情報共有が必要なのか？

##### 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

前者は被害組織識別の目的として、後者は攻撃者に警戒とされ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、被害組織単体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）を使いやすくなる傾向があります。下図にはそうした攻撃活動と被害組織の関係を示したのですが、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。事例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、事例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。事例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つの事例における被害組織間で情報共有を行うことができれば、

- 事例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
- 事例Bの被害組織：調査漏れがないか確認できる
- 事例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。

事例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、「(事例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、この情報は事例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。

# 本ガイドンスで示す情報共有・被害公表のポイント

本ガイドンスは、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】

# 本ガイドスの目次

## 用語集

### 用語集補足

## 1. はじめに

- 情報共有とは何か／公表とは何か
- なぜ「情報共有をするべき」なのか／公表の社会的意義
- 本ガイドスのコンセプト
- 本ガイドスの検討経緯
- 本ガイドスのスコープ
- 本ガイドスを読むにあたって

## 2. 情報共有・被害公表の流れ

## 3. FAQ

### <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？
- Q2.どのタイミングでどのような情報が共有／公表されますか？
- Q3.「被害組織」とは何ですか？
- Q4.サイバー攻撃被害に係る情報にはどのようなものがありますか？
- Q5.どうやって「情報共有」すればいいのですか？
- Q6.どのような情報を共有すればいいのですか？
- Q7.インディケータ情報とはなんですか？
- Q8.いつ共有すればいいのですか？
- Q9.情報共有活動に参加していない場合、どこに共有すればいいのですか？
- Q10.情報共有を行う上での留意点はありますか？
- Q11.攻撃技術情報の共有とノウハウの共有とは何が違いますか？
- Q12.専門組織同士はどういう情報を共有していますか？
- Q13.なぜ非公開で参加者が限定された情報共有が行われるのですか？

### <被害の公表や法令等に基づく報告・届出について>

- Q14.公表の目的は何ですか？
- Q15.公表のタイミングはどのようなものがありますか？
- Q16.公表の内容としてはどのようなものがありますか？
- Q17.公表する際の留意点はありますか？
- Q18.警察への通報・相談は、行った方が良いでしょうか？
- Q19.警察に通報・相談することによる業務への影響はあるのでしょうか？
- Q20.所管省庁への任意の報告は、行った方が良いでしょうか？

### <被害組織の保護の観点について>

- Q21.公表していないのに自組織の被害が知られて公開されてしまうのはなぜですか？
- Q22.他組織の被害に関する情報を見つけた場合、どうしたらよいですか？
- Q23.製品の脆弱性が悪用されていた場合、当該情報はどのように扱えばいいですか？
- Q24.他の被害組織を踏み台として攻撃された場合、当該情報はどのように扱えばいいですか？
- Q25.共有・公表したことで二次被害が出てしまうような情報はありますか？

### <技術情報の取扱いについて>

- Q26.マルウェアに関する情報とはどういうものですか？
- Q27.不正通信先に関する情報とはどういうものですか？
- Q28.攻撃の手口に関する情報とはどういうものですか？
- Q29.専門組織から「見つかった情報を共有活動に展開してよいか？」と尋ねられたらどう判断すればいいですか？
- Q30.情報共有先をどのように指定／制限すればいいですか？
- Q31.専門組織から「分析結果をレポートとして公表してもよいか？」と尋ねられたらどう判断すればいいですか？
- Q32.どのような攻撃技術情報であれば速やかに共有することができますか？（公開情報と非公開情報の違いについて）（※調査ベンダ向け解説）
- Q33.どのような攻撃技術情報であれば守秘義務契約上の「秘密情報」にあたりませんか？（※調査ベンダ向け解説）

## 4. ケーススタディ

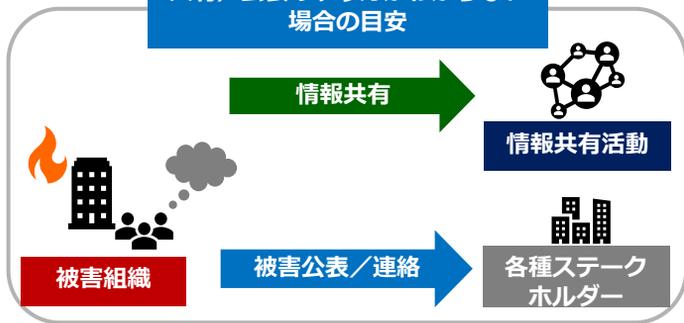
- ケース1：標的型サイバー攻撃
- ケース2：脆弱性を突いたWebサーバ等への不正アクセス
- ケース3：侵入型ランサムウェア攻撃

## 5. チェックシート／フローシート

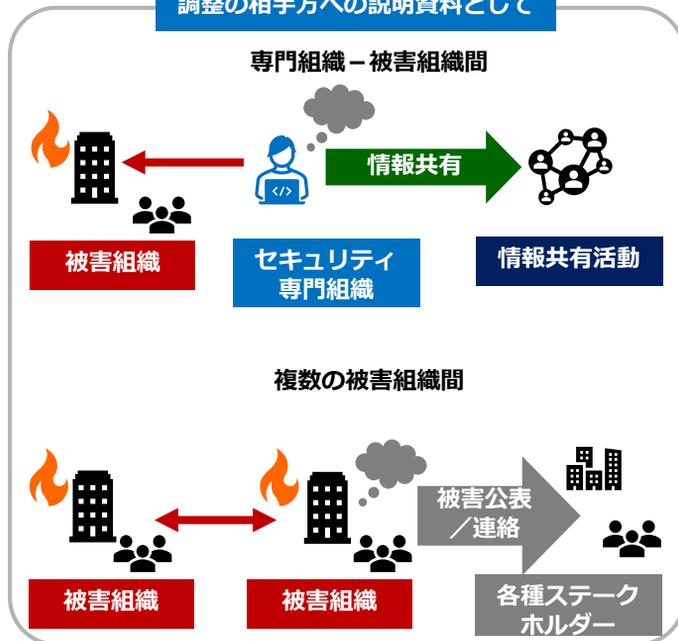
# 本ガイドンスの使い方

- 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。

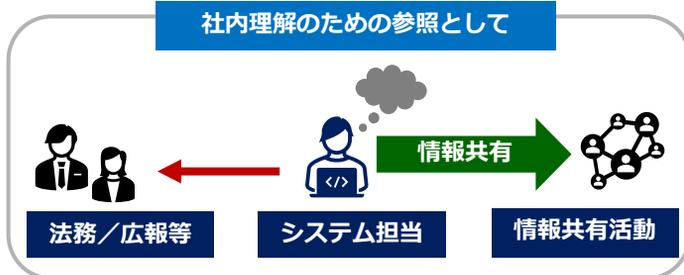
共有／公表のやり方がわからない  
場合の目安



調整の相手方への説明資料として



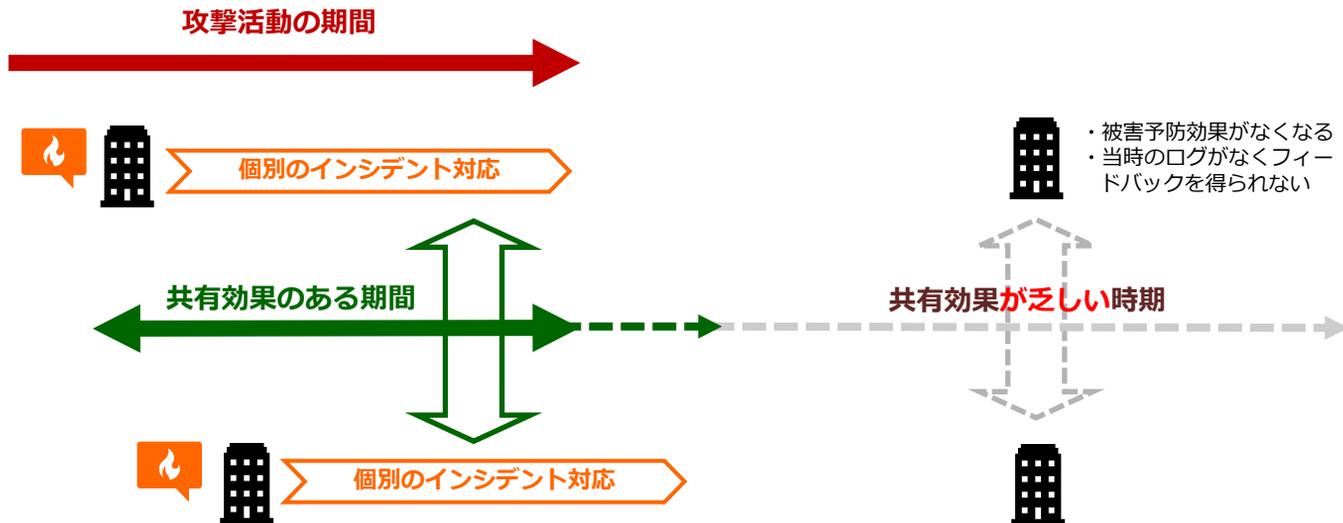
社内理解のための参照として



**以下、本ガイダンスで示すポイントの詳細**

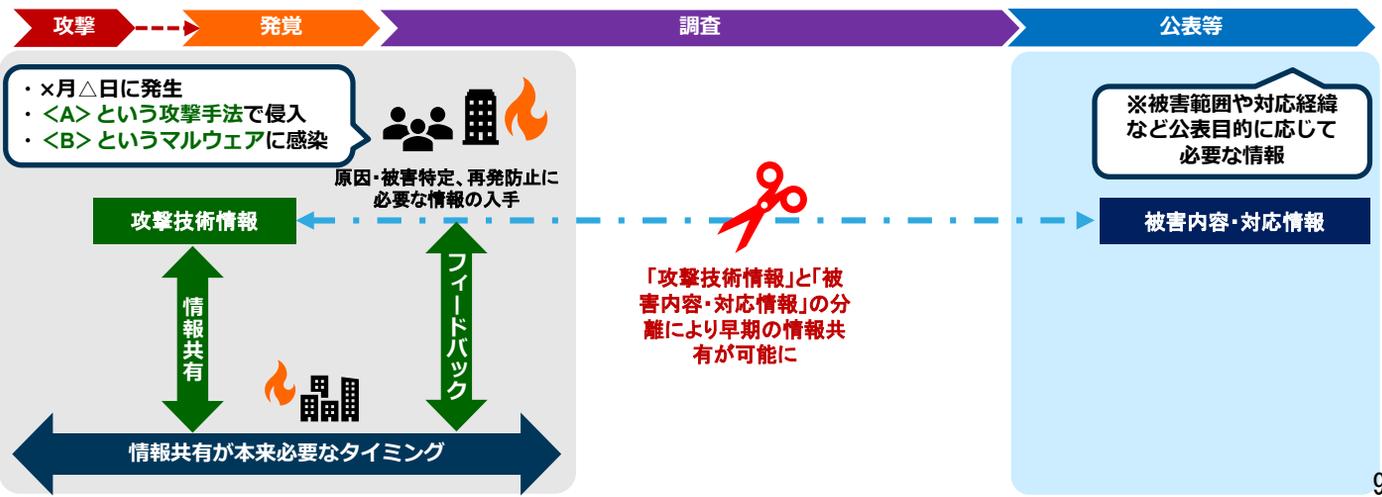
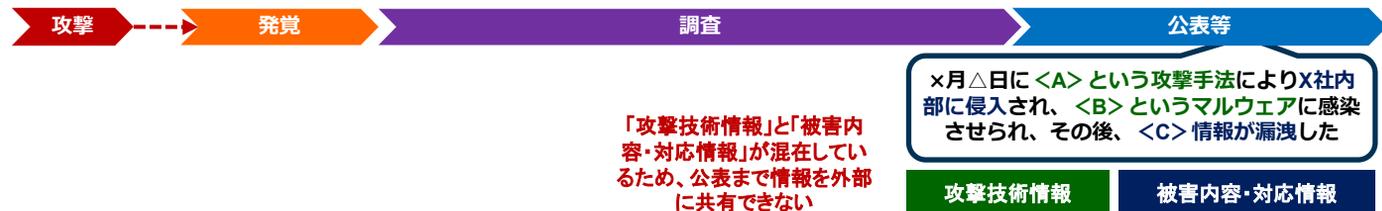
# 1.(1) 情報共有の目的：速やかな情報共有の必要性

- 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

## サイバー攻撃被害に係る情報の分解

被害内容・対応情報

被害組織名

業種／規模

被害内容

タイムライン（対応状況）

タイムライン（技術情報）

攻撃対象システム

（被害対象の）対策状況

攻撃主体に関する情報

脆弱性関連情報等

その他TTP

マルウェア

通信先

攻撃技術情報

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

## 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

### 最後に公表を行う想定

※高度な攻撃の場合、事案の発覚から調査結果を踏まえた公表までかなりの長期間になることが想定されるため、「公表の遅れ」を指摘される可能性がある



### 一般的な不正アクセス事案



### リアルタイムインシデント事案

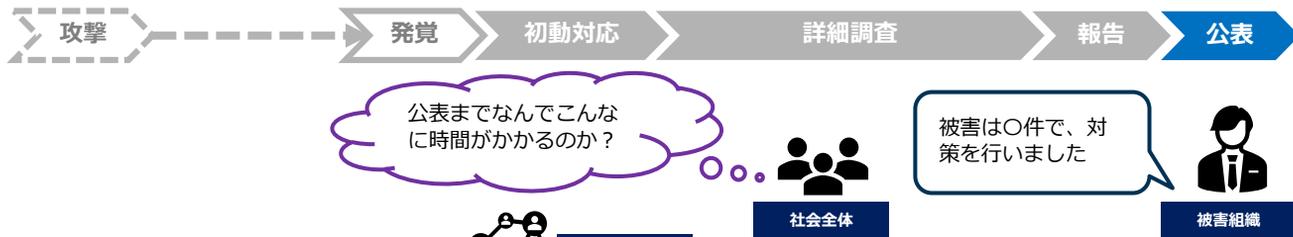
※ランサムウェア被害、DDoS被害など、攻撃とほぼ同タイミングで外部に被害が知られるケース



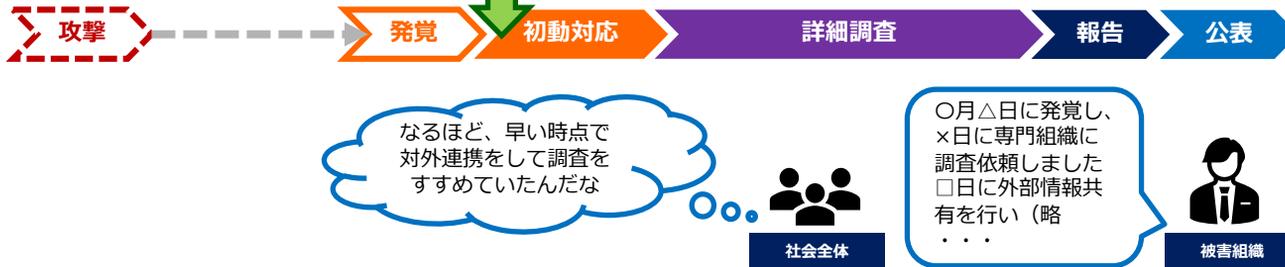
## 2.(3) 被害公表内容の整理

- 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

### 最小限の情報を公表する場合

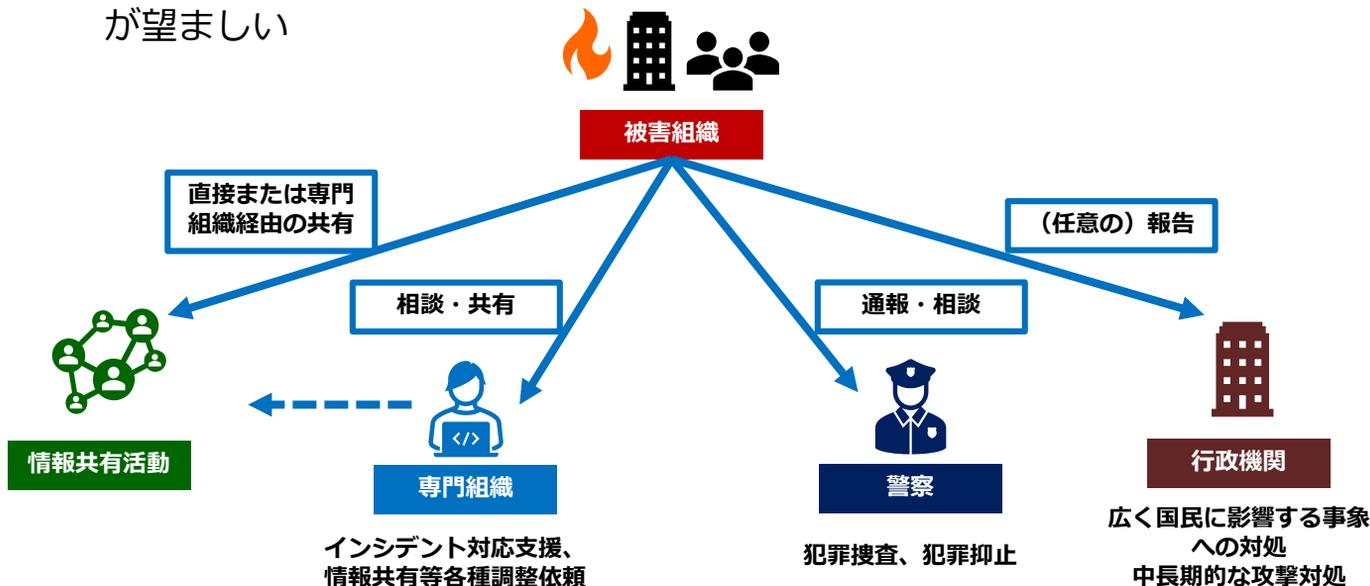


### 対応経緯を含めて公表する場合



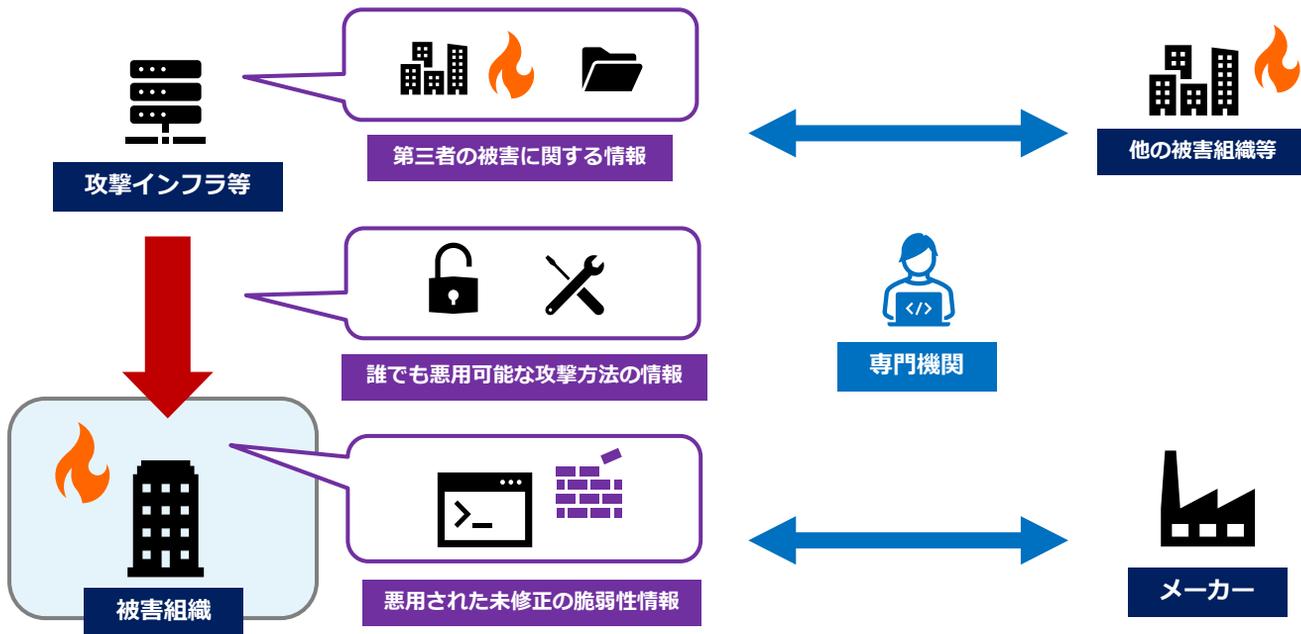
### 3. 外部組織（専門組織、警察、行政機関等）との連携

- 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がるため、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



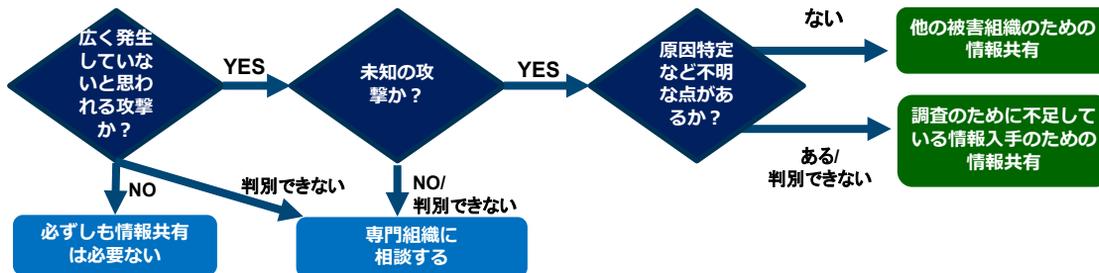
# 情報共有と被害公表における情報の種類のチェックリスト（簡易版）

	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）



## 被害公表判断のためのフロー（簡易版）

