NTTデータ先端技術のセキュリティ

NTT DATA
Trusted Global Innovator

INTELLILINK セキュリティ情報配信サービス
注目されているセキュリティ事故・事件に関する情報
＜2023年06月版 (第45号)＞(選り抜き版)

2023年6月29日
ＮＴＴデータ先端技術株式会社
サイバーセキュリティ事業本部

今回のサマリー

サイバー攻撃被害に係る情報の共有・公表ガイダンスの解説
2023年3月8日、内閣サイバーセキュリティセンター(NISC)のサイバーセキュリティ協議会運営委員会は、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を公開しました。本ガイダンスは、サイバー攻撃を受けた被害組織がサイバーセキュリティ関係組織とサイバー攻撃被害に係る情報を共有する際の実務上の参考となるポイントをFAQ形式でまとめたものです。本記事では、本ガイダンスのポイントを解説します。

サイバー攻撃被害に係る
情報の共有・公表ガイダンスの解説

1. 本ガイダンスについて

2023年3月8日、内閣サイバーセキュリティセンター(NISC)のサイバーセキュリティ協議会運営委員会は「サイバー攻撃被害に係る情報の共有・公表ガイダンス(以下、本ガイダンス)」を公開しました。

本ガイダンスは組織間の情報共有が行われない実態を踏まえて策定されました。サイバー攻撃を受けた**被害組織自身が攻撃・被害の全容を解明し、組織自身の対策や、他組織への攻撃・被害を未然に防止できる状態を実現する**ために、速やかな情報共有や目的に沿ったスムーズな被害公表を行うための実務上のポイントがまとめられています。

サイバー攻撃を受けた被害組織が得た情報や被害の情報が公開されることから、本ガイダンスの**対象読者はセキュリティ担当部門だけでなく、法務・リスク管理・広報部門、保守ベンダも含まれます**。本ガイダンスは33件のFAQ・解説とケーススタディ・チェックリストで構成されており、情報共有・被害公表の考え方を整理する際の参考となります。

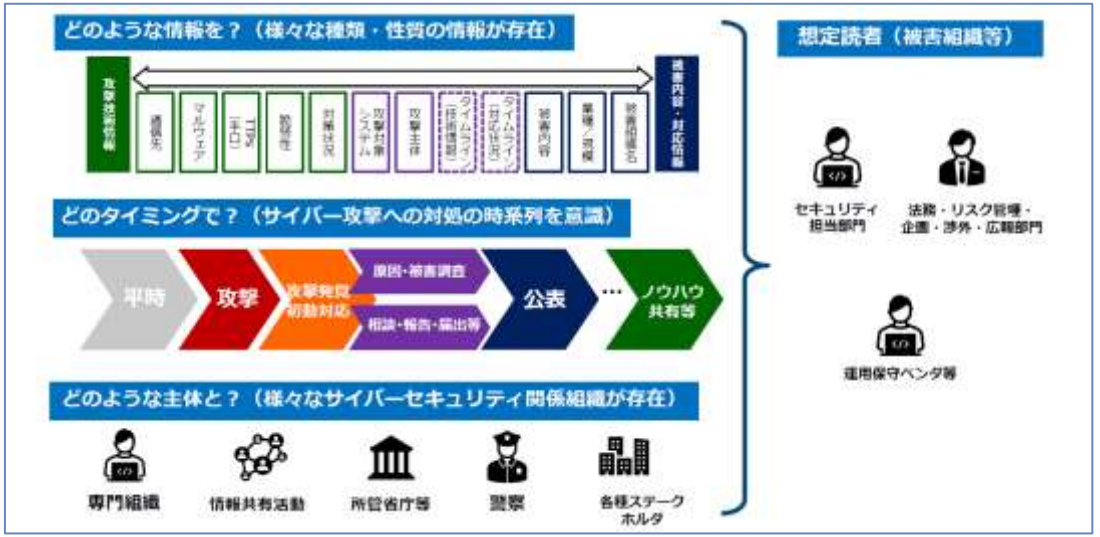


図1．本ガイダンスの概要
出典：サイバー攻撃被害に係る情報の共有・公表ガイダンス（概要）
<https://www.meti.go.jp/press/2022/03/20230308006/20230308006-3.pdf>

2. 情報共有の目的と必要性

本ガイダンスは情報共有・被害公表を行うためのものですが、被害組織が自身のネガティブな情報を外部へ提供したくないと考えるのは当然であり、組織間の情報共有がされない理由の1つであると言えます。

被害組織は、ある攻撃キャンペーンで被害を受けた複数組織の内の1つであると考えるべきです※。そのため、1つの被害組織の調査で得られた情報のみで攻撃・被害の全容を明らかにすることは困難であり、情報共有を行わない場合、調査可能な範囲でインシデント対応をクローズせざるを得ないことになります。

攻撃手法が高度化する中で、情報共有は自組織だけの力では対応できないサイバー攻撃に対抗するための必要な手段となります。情報共有を行うことで、他の被害組織からの情報共有が期待できます。

図2．攻撃キャンペーン全体の情報と単独組織の調査で得られる情報のイメージ
出典：サイバー攻撃被害に係る情報の共有・公表ガイダンス
<https://www.meti.go.jp/press/2022/03/20230308006/20230308006-2.pdf>

※自組織のみを標的としたサイバー攻撃の場合も「自組織のみを標的としている」ことの特定は困難なため、インシデント対応の初期では同様の対応を行うことになります。

3. 攻撃・被害に係る情報の種類と分類

情報共有を行うためには、**共有する情報が被害を受けた組織を特定できないことが大切であるため、**本ガイダンスでは被害組織が確認した攻撃・被害に係る情報を「攻撃技術情報」と「被害内容・対応情報」の2つに切り離して扱う配慮がされています。

攻撃技術情報は通信先・マルウェア・TTP(攻撃の手口の情報)などの攻撃手法や攻撃者の活動を示す情報です。被害組織に紐づく情報は殆ど含まれていません。情報の共有先は、JPCERT/CCや分野毎のISACなどが行っている**非公開の情報共有活動**※が挙げられます。**情報共有を行うことで他の被害組織から自組織では得られない攻撃技術情報を共有され、更に詳細な調査をできる**ことが期待できます。

被害内容・対応情報は被害そのものを示す情報です。外部に知られることで風評リスクとなる情報や、自組織の過失・責任に関する情報、第三者の不利益となるような情報を含む場合があるため、被害公表を行うまでは非公開にしたい情報です。

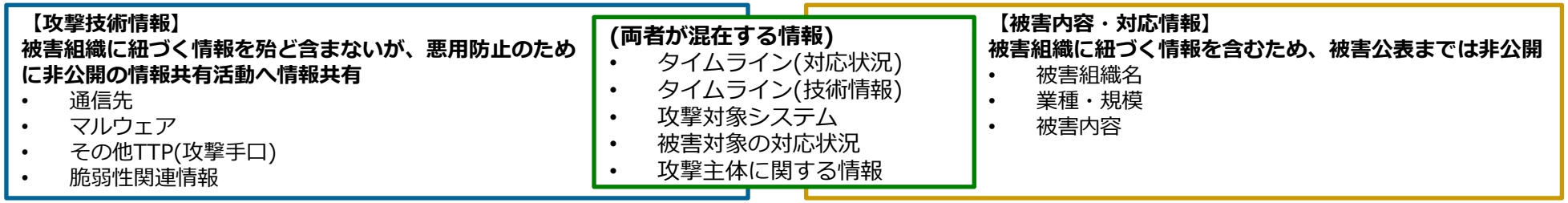


図3. サイバー攻撃被害に係る情報の種類と分類

FAQの「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？」で解説されています。

※攻撃技術情報は広く公開されることで悪用などの二次被害を生む可能性のある情報があるため、情報共有活動は非公開で行われています。
FAQの「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？」で解説されています。

4. 被害公表の目的

情報共有に対して、被害公表の目的は複数の種類に分けられます。いずれも、**積極的に情報を開示することにより、被害組織のインシデント対応における評価を得る効果**があります。

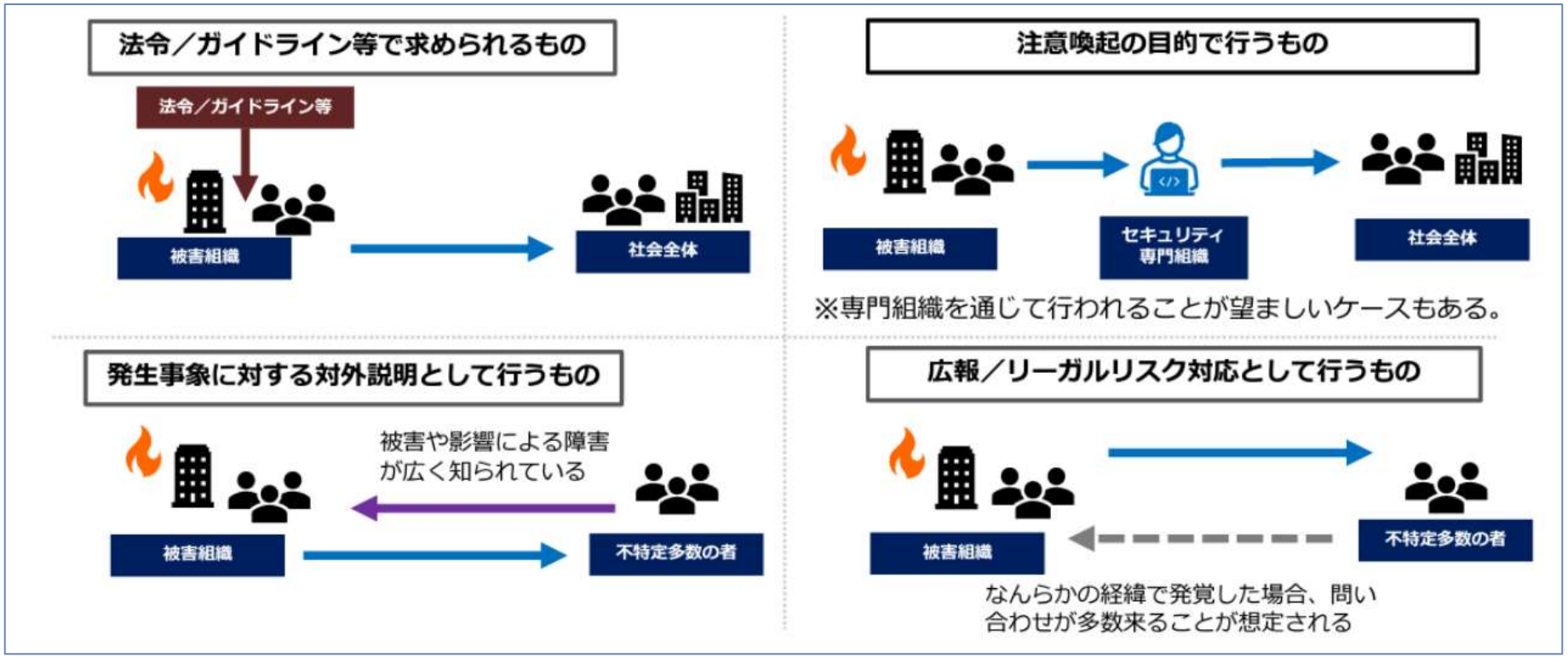


図4．被害公表の目的
出典：サイバー攻撃被害に係る情報の共有・公表ガイダンス（概要）
<https://www.meti.go.jp/press/2022/03/20230308006/20230308006-3.pdf>

5. サイバー攻撃被害に備えて

本ガイダンスは**サイバー攻撃を受けた際に初めて内容を確認するものではなく、インシデント対応時の情報共有・被害公表をスムーズに行えるような体制や対応に関する文書を事前に整備しておくために活用**するとよいと考えられます。

体制の整備は2章「情報共有・被害公表の流れ」が参考になります。情報共有・被害公表における情報の種類が整理されており、更に情報共有・被害公表の判断のためのフローチャートも示されているため、自組織の体制や対応に関する文書の整備に使用しやすくなっています※。

図5.情報共有判断のためのフロー(簡易版)
出典：サイバー攻撃被害に係る情報の共有・公表ガイダンス
<https://www.meti.go.jp/press/2022/03/20230308006/20230308006-2.pdf>

また、4章「ケーススタディ」は昨今のサイバー攻撃被害でよく見られる「標的型サイバー攻撃」「脆弱性等を突いたWebサーバへの不正アクセス」「侵入型ランサムウェア攻撃」の対応事例を紹介しており、情報共有・被害公表の具体的な実施内容の参考になります。

※2章のチェックリストとフローチャートは簡易版となっており、詳細版は5章「チェックリスト／フローシート」に記載されています。

6. まとめ

「サイバー攻撃被害に係る情報の共有・公表ガイダンス」は、本ガイダンスは組織間の情報共有が行われない実態を踏まえて、サイバーセキュリティ協議会運営委員会の下に設置された「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」で策定されました。

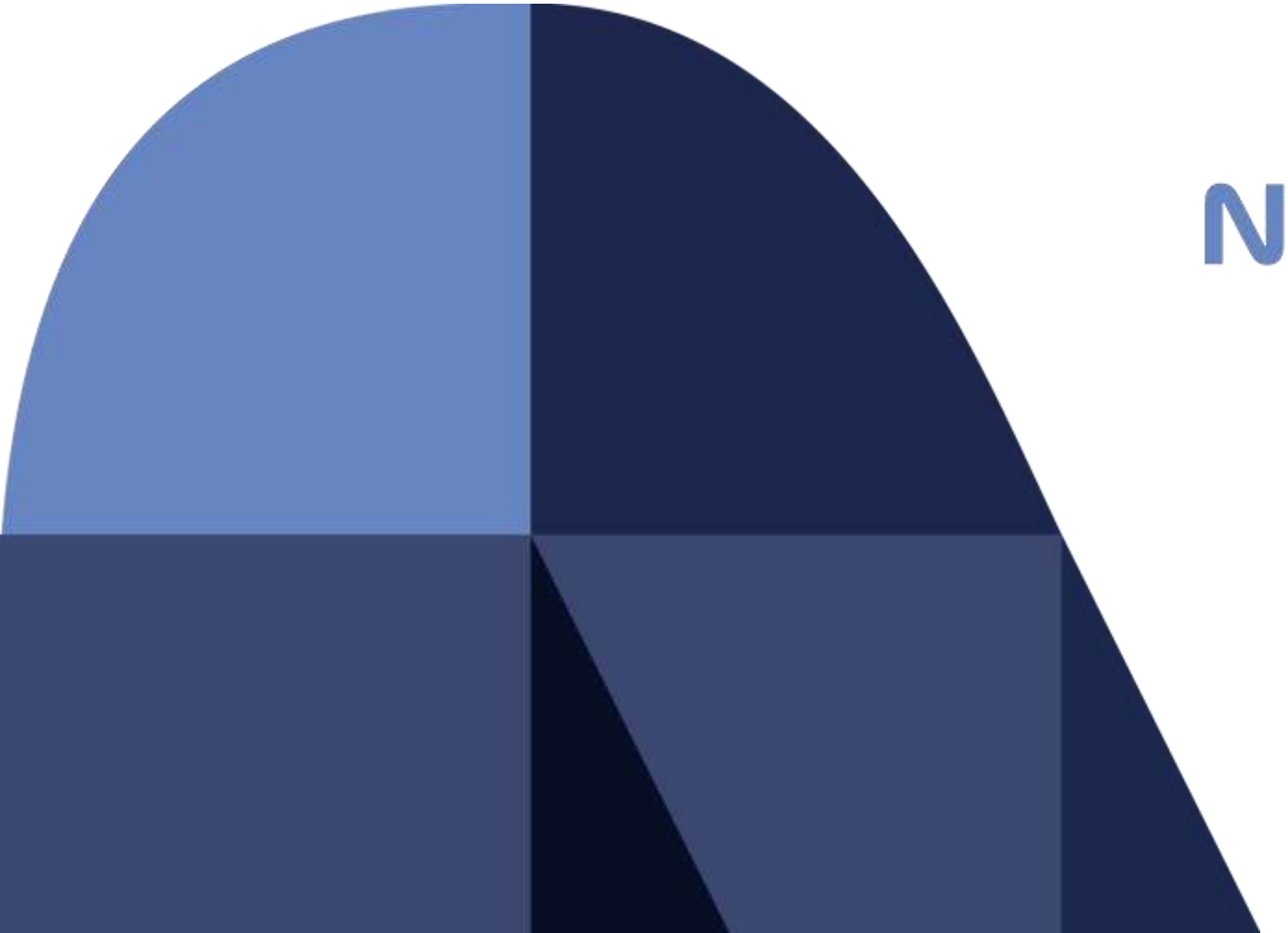
本ガイダンスはサイバー攻撃を受けた被害組織向けに、速やかな情報共有や目的に沿ったスムーズな被害公表を行うためのポイントがまとめられており、33件のFAQ・解説とケーススタディ・チェックリストで構成されています。

本ガイダンスの内容は、自身のネガティブな情報を外部へ提供したくないと考える組織のために、被害組織が確認した攻撃・被害に係る情報を「攻撃技術情報」と「被害内容・対応情報」の2つに切り離して扱う配慮がされています。

本ガイダンスを活用してインシデント対応時に情報共有・被害公表をスムーズに行えるような体制や対応に関する文書を整備しておくことをお勧めします。

7. 参考URL

- 「サイバー攻撃被害に係る情報の共有・公表ガイダンス（案）」に対する意見募集の結果及び「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の公表 （METI/経済産業省）
  https://www.meti.go.jp/press/2022/03/20230308006/20230308006.html
- 「サイバー攻撃被害に係る情報の共有・公表ガイダンス（案）」に対する意見募集の結果及び「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の公表
  https://www.jpcert.or.jp/tips/2023/wr230315.html
- サイバー攻撃被害に係る情報の共有・公表ガイダンス（概要）
  https://www.meti.go.jp/press/2022/03/20230308006/20230308006-3.pdf
- サイバー攻撃被害に係る情報の共有・公表ガイダンス
  https://www.meti.go.jp/press/2022/03/20230308006/20230308006-2.pdf
- サイバーセキュリティ協議会
  https://www.nisc.go.jp/council/cs/kyogikai/index.html



NTT DATA

Trusted Global Innovator