報道資料

令和４年４月２０日
総務省
経済産業省
警察庁
内閣官房内閣サイバーセキュリティセンター

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の開催について

サイバー攻撃被害を受けた民間主体やその受託者等（以下「サイバー攻撃被害組織等」という。）が、その被害に係る情報をサイバーセキュリティ関係組織等と共有することは、発生したサイバー攻撃の全容を解明し、更なる対策の強化を可能とせしめるものであり、サイバー攻撃被害組織等自身にとっても、社会全体にとっても非常に有益です。しかし、現状、サイバー攻撃被害組織等の現場にとって、自組織のレピュテーションに影響しかねない情報共有には慎重であるケースも多く、被害に係る情報のうち、どのような情報を、どのタイミングで、どのような主体と共有すればよいかの検討にあたり、実務上の参考とすべきものがないため、適切に判断することが難しいとの声も聞かれます。

そこで、サイバー攻撃被害に係る情報を取り扱う様々な担当者の判断に資することを目的として、サイバー攻撃被害組織等の立場にも配慮しつつ、技術情報等組織特定に至らない情報の整理を含めた、サイバー攻撃被害に係る情報の共有・公表ガイダンスを策定すべく、官民の多様な主体が連携する協議体である「サイバーセキュリティ協議会」の運営委員会の下に、「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」を開催することとしました。

◆スケジュール
令和4年4月 20 日　サイバーセキュリティ協議会運営委員会において、検討会の開催を決定
令和4年中に3回程度、検討会を開催し、成案を得る

（別紙）関連資料
別紙１　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の開催について
（サイバーセキュリティ協議会運営委員会決定）
別紙２　「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の検討会について
（説明資料）

（連絡先）
総務省サイバーセキュリティ統括官室
担 当:佐々木統括補佐、広瀬主査
電 話:03-5253-5357

経済産業省商務情報政策局サイバーセキュリティ課
担 当:石巻総括補佐、村上係長
電 話:03-3501-1253 FAX:03-3580-6239

警察庁サイバー警察局
担 当:田中企画官
電 話:03-3581-0141(内線:3511) FAX:03-3503-1194

内閣官房内閣サイバーセキュリティセンター
担 当:扇企画官、福田参事官補佐、
桑原上席サイバーセキュリティ分析官
電 話:03-6205-4648 FAX:03-3581-7652

別紙１

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の開催について

令和４年４月 20 日
サイバーセキュリティ協議会運営委員会決定

サイバー攻撃被害を受けた民間主体やその受託者等（以下「サイバー攻撃被害組織等」という。）が、その被害に係る情報をサイバーセキュリティ関係組織等と共有することは、発生したサイバー攻撃の全容を解明し、更なる対策の強化を可能とせしめるものであり、サイバー攻撃被害組織等自身にとっても、社会全体にとっても非常に有益である。しかし、現状、サイバー攻撃被害組織等にとって、自組織のレピュテーションに影響しかねない情報共有には慎重であるケースも多く、被害に係る情報のうち、どのような情報を、どのタイミングで、どのような主体と共有すればよいかの検討にあたり、実務上の参考とすべきものがないため、適切に判断することが難しいとの声も聞かれる。

そこで、サイバー攻撃被害に係る情報を取り扱う様々な担当者の判断に資することを目的として、サイバー攻撃被害組織等の立場にも配慮しつつ、技術情報等組織特定に至らない情報の整理を含めた、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「ガイダンス」という。）を策定すべく、協議会規約第４条第１項第３号に規定する、サイバーセキュリティに関する脅威情報等の共有及び分析に資する関係者間の連携の促進のための活動として、以下のとおりサイバーセキュリティ協議会運営委員会として決定する。

１　サイバーセキュリティ協議会運営委員会の下で、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（以下「検討会」という。）を開催する。

２　検討会は、サイバー攻撃被害組織等にとって、被害に係る情報をサイバーセキュリティ関係組織等と共有する際等に参考とすることのできるリファレンス文書として、ガイダンスの案を策定する。なお、ガイダンスは、協議会構成員以外においても有益なものとなるよう配慮する。

３　検討会の事務局は、警察庁、総務省、経済産業省及び協議会事務局（内閣官房内閣サイバーセキュリティセンター及び政令指定法人 JPCERT/CC）が担う。

４　検討会の委員は、２に掲げた内容を行うための優れた見識を有する者のうちから検討会の事務局が委嘱する。

５　検討会に座長を置く。検討会の座長は、その委員の互選により決する。

６　検討会の座長は、必要があると認めるときは、検討会の委員以外の者に対し、検討会議の会に出席して意見を述べることを求めることができる。

７　前各項に掲げるもののほか、検討会の運営に関する事項その他必要な事項は、検討会の座長が定める。

別紙2

「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の検討会について

背景及び目的

- サイバー攻撃被害を受けた組織が、サイバーセキュリティ関係組織等と攻撃被害に係る情報を共有することは、発生したサイバー攻撃被害の全容解明や、更なる対策の強化に寄与するものであり、被害組織自身にとっても、社会全体にとっても非常に有益。
- しかし、現状、サイバー攻撃被害を受けた組織にとって、自組織のレピュテーションに影響しかねない情報共有には慎重であるケースも多く、被害に係る情報のうち、どのような情報を、どのタイミングで、どのような主体と共有することが適当なのか等を検討するための参考資料等が乏しく、この点が情報共有が円滑かつ効果的に進まない一因となっていると考えられる。
- このため、サイバー攻撃被害を受けた組織の立場にも配慮しつつ、技術情報等組織特定に至らない情報の整理を含め、サイバー攻撃被害に係る情報を取り扱う担当者を対象とした、攻撃被害に係る情報を取り扱う際の実務上の参考となるガイダンス文書を策定し、これを普及していくことで、円滑かつ効果的な情報共有を促進する。

検討体制

- サイバーセキュリティ協議会運営委員会の下で、有識者からなる「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の検討会を開催。
- 検討会事務局は、警察庁、総務省、経済産業省及びサイバーセキュリティ協議会事務局（内閣官房内閣サイバーセキュリティセンター及び政令指定法人JPCERT/CC）が担う。

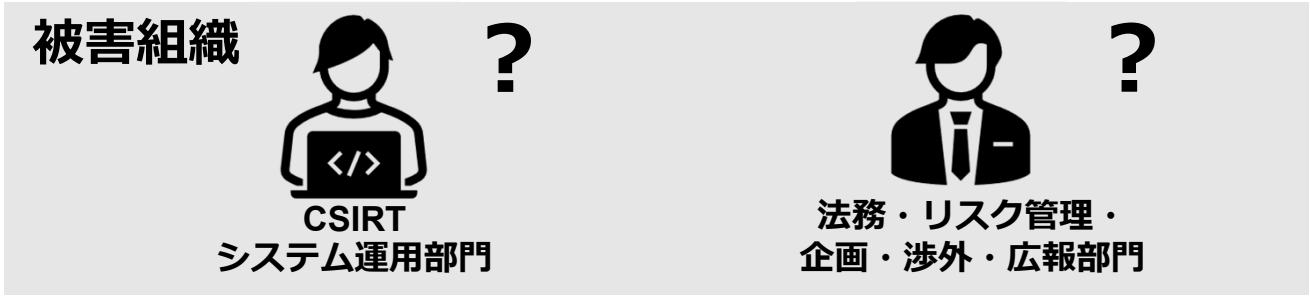
スケジュール

- 令和４年４月中に運営委員会にて開催を決定。
- 令和４年中に３回（論点整理、素案、成案）程度、検討会を開催し、成案を得る。

「サイバー攻撃被害に係る情報の共有・公表ガイダンス」（イメージ）

■ サイバー攻撃被害を受けた組織にとって、どのような情報を、どのタイミングで、どのような主体と共有することが適当なのか等を検討するための実務上の参考となるガイダンス文書

※　本ガイダンスでは、サイバーセキュリティ関係組織等の間の情報共有については対象としない



● どんな情報を？

コンテクスト情報

様々な種類・性質の情報が存在

- 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）
- 攻撃主体に関する情報
- 攻撃対象システム
- 対策状況
- 脆弱性
- その他TTP
- マルウェア
- 通信先

技術情報

● どのタイミングで？

サイバー攻撃への対処の時系列

● どんな主体と？

「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 委員

氏名	所属	役職
新井 悠	（株）NTTデータ	エグゼクティブ・セキュリティ・アナリスト
板橋 功	日本サイバー犯罪対策センター（JC3）	シニアセキュリティフェロー
勝村 幸博	（株）日経BP	日経NETWORK編集長
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
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
花岡 圭心	三菱電機（株）	情報セキュリティ統括室 セキュリティ技術部長
北條 孝佳	西村あさひ法律事務所	弁護士
星 周一郎	東京都立大学法学部	教授
松坂 志	（独）情報処理推進機構（IPA）	セキュリティセンター セキュリティ対策推進部 標的型攻撃対策グループ グループリーダー
山岡 裕明	八雲法律事務所	弁護士
吉岡 克成	横浜国立大学大学院環境情報研究院/ 先端科学高等研究院	准教授
若江 雅子	読売新聞東京本社	編集委員

参考 技術情報とコンテクスト情報（イメージ）

攻撃 → 発覚 → 調査 → 公表等

「技術情報」と「コンテクスト情報」が混在しているため、公表まで情報を外部に共有できない

×月△日に**<A>という攻撃手法**により**X社内部に侵入**され、**<B>というマルウェア**に感染させられ、その後、**<C>情報が漏えい**した。

技術情報　**コンテクスト情報**

攻撃 → 発覚 → 調査 → 公表等

・**×月△日**に発生
・**<A>という攻撃手法**で侵入
・**<B>マルウェア**に関する情報

全容解明に必要な情報の入手

技術情報

情報共有

フィードバック

情報共有が本来必要なタイミング

「技術情報」と「コンテクスト情報」の分離により早期の情報共有が可能に

コンテクスト情報

※被害範囲や対応経緯など公表に必要な情報