

「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。

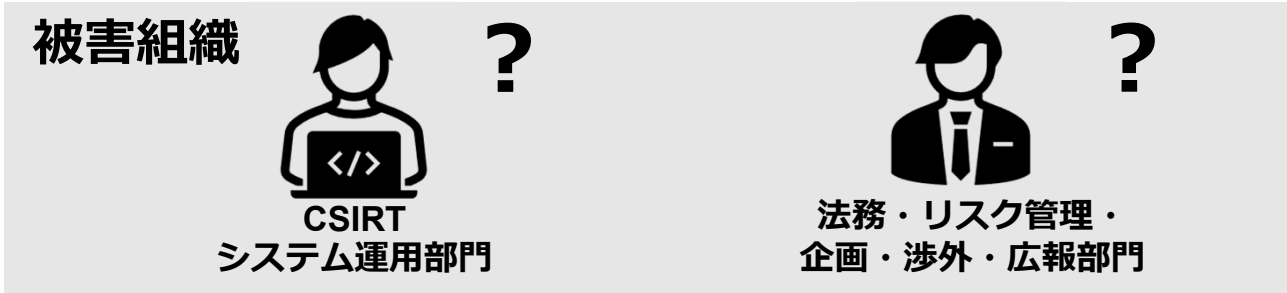
スケジュール

- 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・公表ガイドンス」(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ドンス文書

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



● どんな情報を？

コンテキスト情報

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

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



● どんな主体と？



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

「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ト情報（イメージ）



「技術情報」と「コンテクト情報」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、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

コンテクト情報



- ・ ×月△日に発生
- ・ <A>という攻撃手法で侵入
- ・ 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

※被害範囲や対応経緯など公表に必要な情報

コンテクト情報

「技術情報」と「コンテクト情報」の分離により早期の情報共有が可能に