資料37－１

サイバーセキュリティを巡る最近の動向

令和４年４月

サイバーセキュリティタスクフォース事務局

サイバーセキュリティ対策の強化について の注意喚起

サイバーセキュリティ対策の強化についての注意喚起

○ 現下の情勢を踏まえ、サイバー攻撃事案のリスクは高まっていると考えられることから、総務省では、関係省庁と連携して、電気通信事業者、放送事業者及び地方公共団体等に対して、サイバーセキュリティ対策の強化について、令和４年２月23日及び３月１日に続き、３月24日にも注意喚起を実施。

「現下の情勢を踏まえたサイバーセキュリティ対策の強化について（注意喚起）」

（令和4年3月24日　経済産業省、総務省、警察庁、内閣官房内閣サイバーセキュリティセンター）

昨今のサイバー攻撃事案のリスクの高まりを踏まえ、政府においては、２月 23 日に「昨今の情勢を踏まえたサイバーセキュリティ対策の強化について（別添１）」、３月１日に「サイバーセキュリティ対策の強化について（別添２）」注意喚起を行っております。

その後も、国内では、ランサムウェアによる攻撃をはじめとするサイバー攻撃事案の報告が続いており、また、エモテットと呼ばれるマルウェアの増加も見られるところです。また、米国では、３月 21 日に、バイデン大統領が、国内の重要インフラ事業者等に対して、ロシアが潜在的なサイバー攻撃の選択肢を模索しており警戒を呼びかける声明を発表するとともに、企業等に対してサイバーセキュリティ対策を強化する具体策を提示しています。

このような現下の情勢を踏まえ、政府機関や重要インフラ事業者をはじめとする各企業・団体等においては、組織幹部のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、上記の２月 23 日及び３月１日の注意喚起にある対策（①リスク低減のための措置、②インシデントの早期検知、③インシデント発生時の適切な対処・回復）の徹底をあらためてお願いいたします。また、ランサムウェアやエモテットについては、これまで専門機関等において公表している情報・サイトを確認の上、対応を講じるようお願いいたします。あわせて、不審な動き等を検知した場合は、速やかに所管省庁、セキュリティ関係機関に対して情報提供いただくとともに、警察にもご相談ください。

https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000472.html

「サイバー攻撃被害に係る情報の共有・公表ガイダンス」の検討会の設置について

「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し、その旨を報道発表。
- 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・公表ガイダンス検討会の開催について」

（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

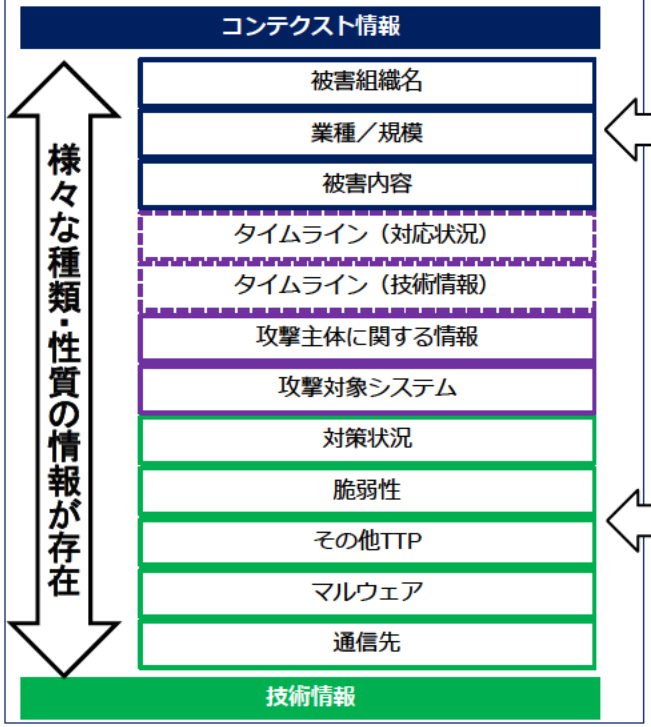
令和4年中に3回程度、検討会を開催し、成案を得る

https://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00136.html

「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？



● 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

※被害範囲や対応経緯など公表に必要な情報

技術情報 ⇔ コンテクスト情報

「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

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