National center of Incident readiness and Strategy for Cybersecurity

サイバーセキュリティ協議会について

サイバーセキュリティ分野における
従来の枠を超えた
情報共有・連携体制の構築・推進

内閣官房 内閣サイバーセキュリティセンター
対処・外部連携ユニット
令和６年7月

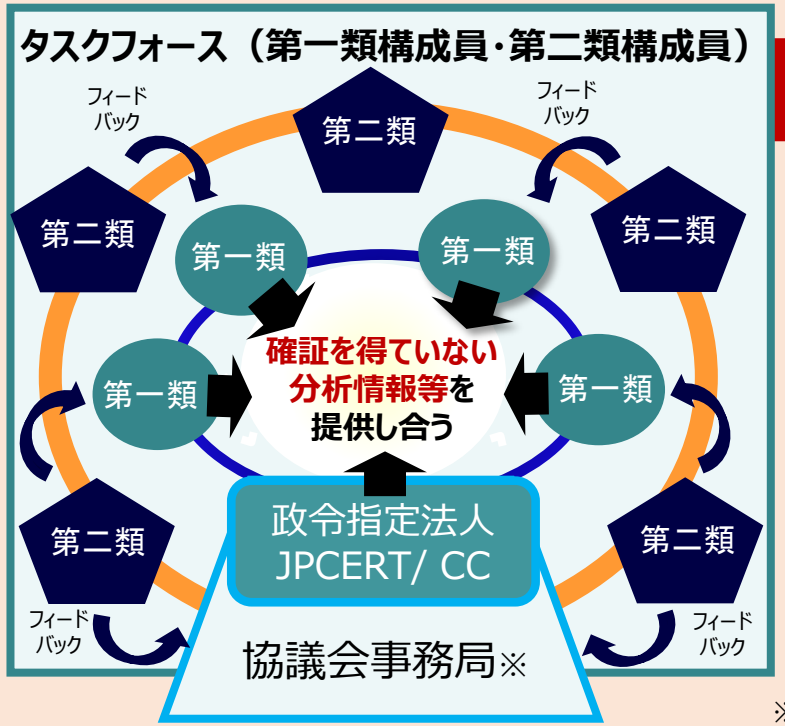
サイバーセキュリティ協議会の概要

目的

我が国のサイバーセキュリティに対する脅威に積極的に対応する意思を有する多様な主体が相互に連携して、サイバーセキュリティに関する施策の推進に関し必要な協議を行う

➡ 主として、**脅威情報等の共有・分析、対策情報等の作出・共有等**を**迅速に**行う（原則システムを活用）

サイバーセキュリティ協議会（CS戦略本部長等により組織）



作出した対策情報等の共有 ➡ **一般の構成員**

総会

全構成員により構成（各構成員に１の議決権）
・総会は毎年開催（電子的手段の開催も可）
・規約の改正　等を実施

運営委員会

運営委員は、CS戦略本部長等
・構成員の入会の承認、除名
・**情報提供等協力の求め**
等に関することを担当

※事務局の庶務はNISC対処・外部連携ユニットが担当

協議会の特徴

①官民、業界といった従来の枠を越えた**オールジャパンによる**情報共有体制

②システムを用いて情報共有等を行う「**バーチャル協議会**」

③直感的な違和感といった**早期の段階からの情報提供、相談等を促進**
構成員には、法律に基づく守秘義務※、情報提供義務が適用　※罰則付き

④**ギブアンドテイクルールを徹底し、積極的な情報提供者へのメリットを増加**　※積極的な情報提供に意欲と能力のある構成員を「**タスクフォース**」としてグループ化

我が国のサイバーセキュリティを確保する観点から、構成員になるためには、右の要件を満たし、**運営委員会の承認**を得なければならない

（加入は任意）

申込みを行うことのできる者

◆国の関係行政機関　◆地方公共団体　◆重要インフラ事業者
◆サイバー関連事業者（主にセキュリティ関連事業者を想定）◆大学・教育研究機関　等
であり、協議会の活動に賛同する者（事業者の団体等も含む）
※協議会の目的達成または活動に支障を生じるおそれがある場合は承認しない場合がある

協議会の運用状況

（平成31.4.1～）

（１）協議会の取組状況

平成31年

４月１日：サイバーセキュリティ協議会を組織（平成30年12月改正サイバーセキュリティ基本法施行）
協議会規約の制定、第一期構成員の入会申込受付開始

令和元年

５月17日：第一期の構成員を決定（全91者）

５月下旬：協議会における情報共有活動を開始

10月24日：第二期の構成員を決定→第一期構成員を含め全155者

令和２年

６月５日：第三期構成員を決定→第一期及び第二期構成員を含め全225者

令和３年

３月26日：第四期の構成員を決定→第一期～第三期構成員を含め全266者

令和４年

４月１日：第五期構成員を決定→第一期～第四期構成員を含め全303者

４月20日：運営委員会において、サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会の開催を決定

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」の公表

4月28日：第六期構成員を決定→第一期～第五期構成員を含め全315者

令和６年

6月13日：第七期構成員を決定→第一期～第六期構成員を含め全322者

（２）令和５年度における活用件数

■協議会において取り扱った情報の件数　全５２件（うち継続案件１７件）

→対策情報等を広く公開等するに至った回数　３６回（令和６年３月３１日時点）

○協議会における情報共有活動が開始されて以降、これまで各組織に散らばって存在し、協議会がなければ早期に共有されることがなかったであろう機微な情報が、組織の壁を越えて共有されてきています。

○令和５年度に協議会において取り扱った情報の件数（注）は５２件であり、これらはいずれも協議会がなければ早期に共有されることがなかった機微な情報です。

○これらの案件について、令和６年３月３１日までに、協議会以外の場を含め、対策情報等を広く公開し、又は一定の範囲に限定して共有するに至った回数は３６回でした。

※協議会では、他の情報共有体制では拾えていなかった情報を早期に発見・共有したり、他の情報共有体制で既に共有されている情報を補完する機微な追加情報を関係者に限定して共有すること等を主眼としており、共有情報を真に有益で、他では得られないものに絞り込んでいることから、共有の件数を追及しておりません。

○協議会タスクフォースにおいて取り扱った情報を踏まえたサイバー攻撃の情勢や、タスクフォースが注視している攻撃活動の動向をレポートとして、協議会構成員に限定して配信しており、令和５年度にはレポートを２９回配信しました。

○上記のほか、問い合わせ窓口・相談体制の充実を行っています。

＜注１＞「取り扱った情報の件数」
○一般論として、情報提供の件数は「攻撃活動の数」「攻撃の種類の数」「被害報告の数」などのうち、何に着目してカウントするかによって数値が変化します。
○例えば、ある攻撃グループが、１回の攻撃活動（例「2017年５月12日頃に広がったWannaCryによる一連の攻撃活動」）において、３種類のマルウェアを使用して、１０組織を攻撃した場合、「攻撃活動の数」は１件、「攻撃の種類の数」は最大３件、「被害報告の数」は最大１０件となります。
○この協議会では、その活動の目的に照らし、「攻撃活動の数」に着目して件数をカウントしています。したがって、ある構成員等から提供いただいた案件が、他の構成員等から提供いただいた案件と重複・関連すると認められる場合には、併せて１件として計上することとしています。
＜注２＞上記件数に関して、具体的な攻撃の態様、時期、対策の手法などの情報は一切お答えできませんので、ご容赦ください。

（３）協議会へのご相談･情報提供
（令和５年３月31日時点）

●協議会へのご相談・情報提供はメール又はお電話にてご連絡ください。具体的な被害が発生してなくても、例えば、通信量の急激な増加、サーバ等のハングアップ、特定のサイトへの接続が遅いなど**「いつもとは何か違う」といった段階であっても、お気軽にご相談**ください。

✓メール

- csc-anken@jpcert.or.jp（事案発生の疑いが生じた場合等）
- csc-info@jpcert.or.jp（その他）

✓電話

- 03-3270-3560

※情報のやりとりにあたっては、メール等の電子媒体でお願いすることになります。

※現在、新型コロナ感染症への対応としてお電話での受付を中止しています。

タスクフォース第一類グループからの助言・フィードバックが得られます！

・違和感のあるアクセス等、**サイバー攻撃として断定できない事象についての相談**を受けた。
・相談の内容や相談者の意向を鑑み、**第一類グループへの照会を実施**し、**当該相談者にフィードバック**を行った。

協議会構成員でない方からのご相談・情報提供もお待ちしています！

・**協議会の構成員でない者**から**サイバー攻撃に関する相談**を受けた。
・提供された情報の特徴が協議会で取り扱い中の攻撃活動に合致したため、定められた共有範囲に基づいて**協議会が有する情報を当該相談者に共有**した。

<注>上記は特定の個別事例ではなく、これまでに相談や情報提供いただいたものを踏まえモデルケースとして示したものであり、上記に記載されている情報以上の情報は一切お答えできませんので、ご容赦ください。

（参考）サイバー攻撃被害に係る情報の共有・公表ガイダンス

・本ガイダンスは、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、被害組織から見た意義・具体的な方法を示すことで、効果的な情報共有・被害公表等を促進を図るもの。

背景及び目的

- サイバー攻撃の脅威が高まる中、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被害に係る情報を共有することは、攻撃の全容解明や対策強化を図る上で、被害組織・社会全体にとって有益。しかし、実際には、被害組織は、被害情報の共有に慎重であるケースが多い。
- 当協議会運営委員会の下に、有識者からなる検討会（※）を開催し、被害組織の担当部門(システム運用部門、セキュリティ担当、法務・リスク管理部門等)が被害情報を共有する際の実務上の参考となるガイダンスを策定。

※： 事務局：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（NISC 及び JPCERT/CC）

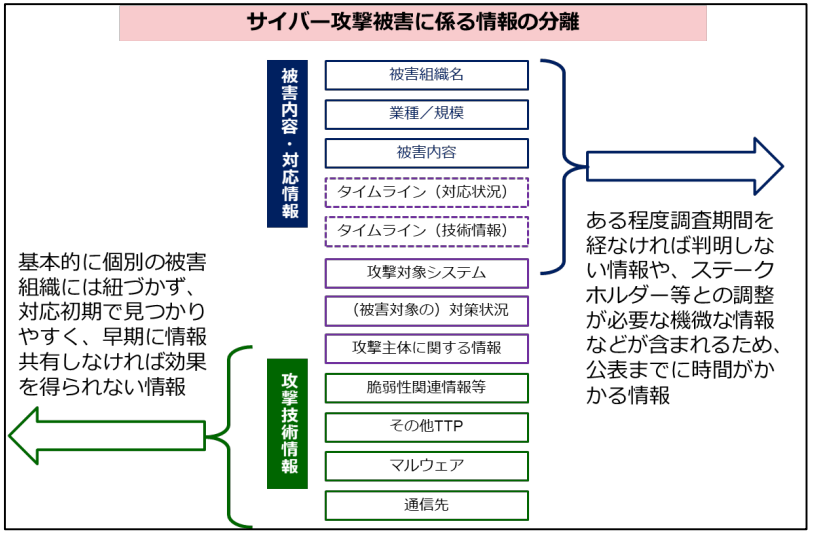
ガイダンスの概要

情報共有

- **何のために：**
  速やかな情報共有によるインシデント対応等に必要な情報の入手や被害拡大防止等。
- **どのような情報を：**
  被害情報を、「攻撃技術情報」と「被害内容・対応情報」に分離。「攻撃技術情報」の共有が被害拡大防止等に効果的。（右図参照）
- **どのタイミングで：**
  他組織が活用できるだけの「攻撃技術情報」が集まった段階での、一連の攻撃活動が行われているうちの速やかな共有を推奨。
- **どのような主体に対して：**
  サイバーセキュリティ協議会等の情報共有活動のハブ組織等。（情報共有活動に参加していない場合、専門組織に依頼しての提供を推奨）

被害公表

- **何のために：**
  顧客や取引先への正確な情報の伝達によるレピュテーションリスクの低減やインシデント対応上の混乱回避。（関係者等の自組織に対する不安等を解消）
- **どのような情報を：**
  通常求められる「被害内容・対応情報」に加え、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推奨。
- **どのタイミングで：**
  攻撃の種類や被害の状況（二次被害発生のおそれ、社会的なインパクトの大きさ等）から、効果的な公表タイミングを選択。（速報としての公表、注意喚起を目的とした公表、調査等を全て終えてから行われる公表等）



情報共有等の際の推奨事項

- 情報共有や被害公表に加えて、警察への通報・相談、所管官庁への報告等の実施。（捜査を通じた犯罪抑止、業界等の特性に応じた的確な情報共有、業界横断的な注意喚起や広く国民に影響する事案への対処等につながる）
- 円滑な情報共有・被害公表を行うため、他の被害組織や機微な情報の取扱いに対する配慮。

ガイダンスの普及啓発等

- 令和５年３月、サイバーセキュリティ協議会総会において、協議会構成員はガイダンスの積極的な活用に努める旨決議。
- NISCから関係府省庁に対し、所管の法人、団体等へガイダンスの積極的な活用を促すなどのガイダンスの普及啓発への協力を依頼する事務連絡を発出。
- サイバーセキュリティ協議会外の情報共有活動においても積極的な活用を奨励すべく、関係者への説明等を実施。

（参考）活用事例
（令和６年３月31日時点）

（事例１）

・特定のネットワーク製品について、攻撃者によりリモートから任意のコード実行や認証情報等の機微な情報を窃取される可能性がある脆弱性が公開され、政令指定法人JPCERT/CC等が当該脆弱性に関する注意喚起を公開した。
・その後、政令指定法人JPCERT/CCは、協議会タスクフォース（第一類グループ）に対して関連情報の照会を行ったところ、グループメンバーから当該脆弱性を悪用する攻撃活動について**追加の情報提供を受けた**ので、**当初、注意喚起を行った公開ルートにより追加の情報発信**を行った。

（事例２）

・政令指定法人JPCERT/CCが、ある標的型攻撃が生じているという事実等を把握したが、**攻撃活動が始まった初期の段階である可能性**があり、国内への攻撃状況（どのくらいの組織が狙われているのか、いつから攻撃が発生しているのか、過去のどういった攻撃と関連があるのか等）について単独では分析を迅速に行うことができなかった。
・このため、緊急に協議会タスクフォース（第一類グループ）に相談を行い、グループメンバーから直ちに関連情報の提供を受けるとともに、ほぼ同時並行で**第二類構成員及び一般の構成員に対し当該攻撃を受けたか否かの調査に資する情報といった対策情報を迅速に共有**し、**併せてフィードバックを任意の協力ベースで求めた**。
・今回共有された対策情報は協議会以外の場では共有されていない独自の情報であったが、これらの対策情報が外部に漏えいすると攻撃者に対し対策の手の内を明らかにしてしまうおそれがあること等を考慮し、今回の**情報共有範囲は原則として当初の情報提供者と協議会構成員に限定**した。

<注> 上記事例に関する具体的な攻撃の態様、時期、対策の手法など、上記に記載されている情報以上の情報は一切お答えできませんので、ご容赦ください。

（参考資料）

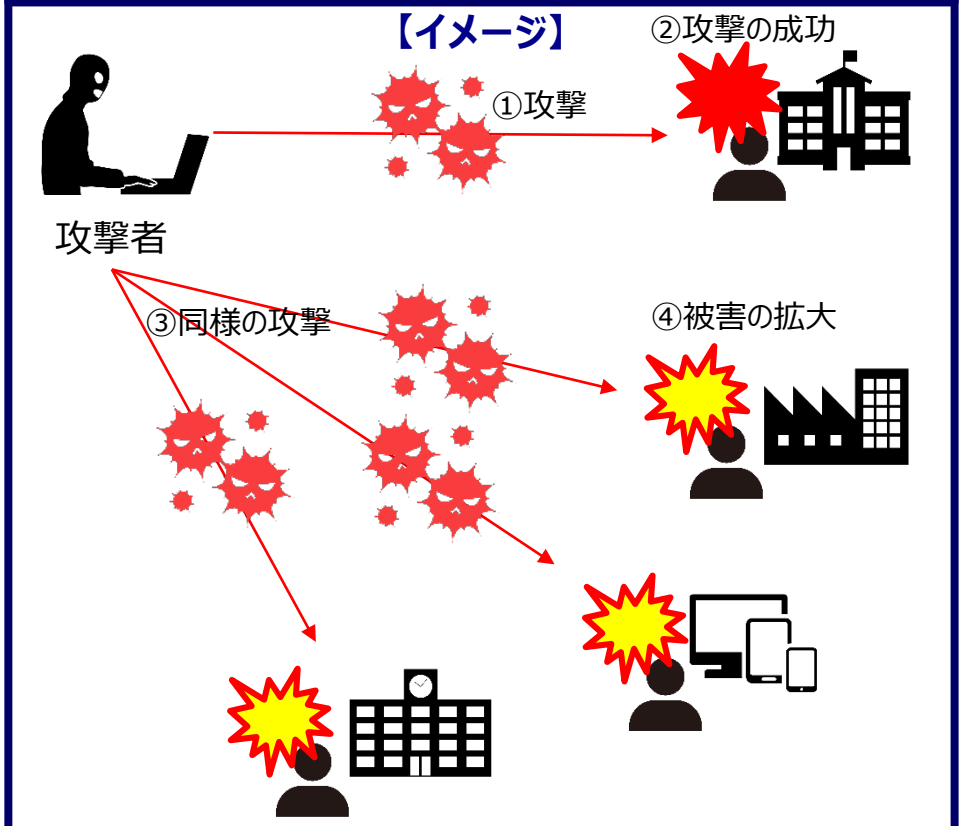
協議会創設の目的と
協議会の基本的な枠組み
～安心して参加できる情報共有体制を目指して～

今回新たに創設したサイバーセキュリティ協議会では、これまでサイバーセキュリティ分野における既存の様々な情報共有体制において**活動の活性化を妨げていた要因**を洗い出し、これを**法律改正等によって改善を図る**ことにより、**既存の情報共有体制の活動を補完**し、これらと**有機的に連携**しつつ、従来の枠を超えた情報共有・連携体制を構築していくことを目標としています。

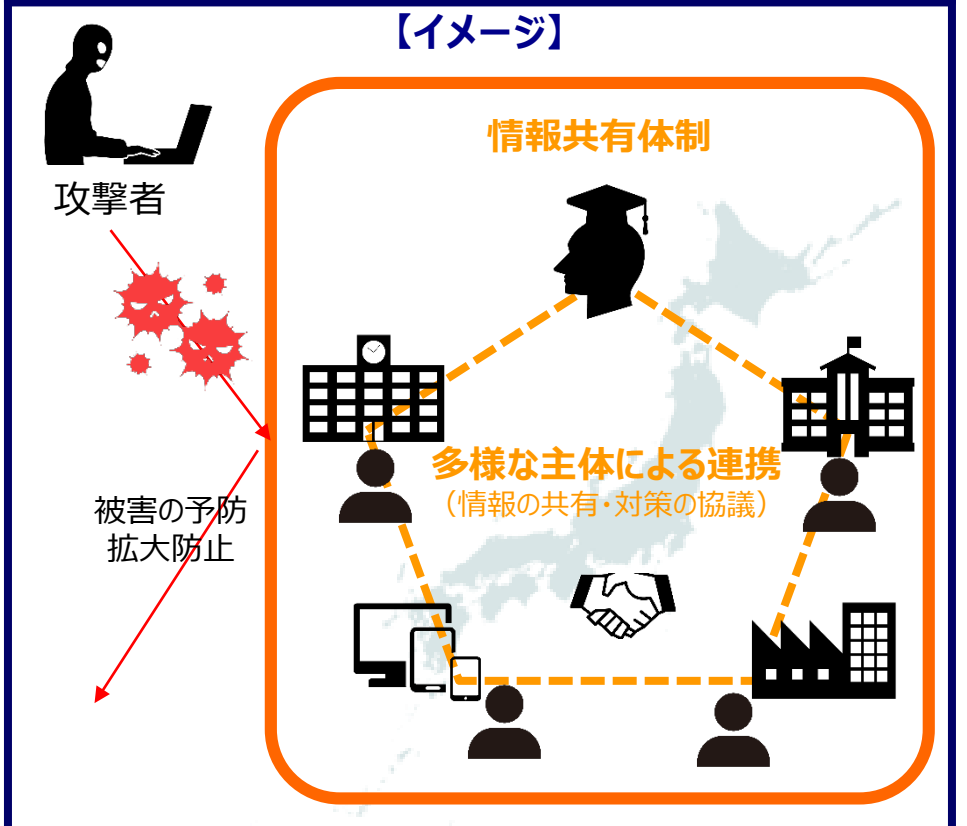
サイバーセキュリティに関する情報共有の効果とその重要性（単独で行う対策の限界）

- サイバーセキュリティの確保は、本来、各組織が自主的に取り組むべきもの
- しかし、サイバー攻撃の複雑化、巧妙化により、被害組織（被害組織から相談を受けるセキュリティベンダ・専門機関等を含む）が単独で有効な分析を行い、確証をもって効果的な対策を迅速に講じることに限界が生じてきている
- また、被害組織等から他の組織へ迅速な情報共有が行われなければ、攻撃手口や対策手法等を他組織が知ることができず、同様の手口によるサイバー攻撃の被害がいたずらに拡大するおそれ

個社単独での対策の限界



情報共有の効果



（参考１） ランサムウェア「WannaCry」（ワナクライ）事案
～早期の段階における迅速な情報共有の必要性と課題～

事案の概要

平成29年５月、政府機関や病院、銀行、大手企業等のコンピュータが、マイクロソフト製品の脆弱性を悪用したランサムウェア（身代金要求型の不正プログラム）「WannaCry」（ワナクライ）に感染

海外：約**150カ国**以上で感染。英国の病院では**診療・手術の中止**等、業務に支障を及ぼす被害が発生

日本：**自治体、鉄道、病院といった重要な機関**を含む幅広い分野において被害が発生

H29.3月 | H29.4月 | H29.5月

3/15
Microsoft製品の脆弱性修正プログラム公開

5/12(金)
Ａ社 システム異常発生

5/13(土)
Ａ社 対策チーム立ち上げ、状況把握開始

5/15(月)
Ａ社がサイバー攻撃を受けた旨報道

5/15 (月)
B市、C市、D社にて感染確認

5/16 (火)
E社感染確認

5/17 (水)
Ａ社 復旧・ニュースリリース

当時、被害拡大を防ぐために迅速な共有が必要であった情報は何か

◆修正プログラム未適用のPCは、起動した瞬間にネットワーク経由で感染し、ロックされるおそれ
→各職員は出勤後、不用意にPCを起動してはならない。
この旨を、国内の各組織に、（職員出勤時刻までに）一刻も早く周知する必要があった。

しかし、

当時の被害企業にとっての情報提供リスク

・個社単独では自らの分析内容に確証が持てない状況
・情報提供先の他組織で秘密の保持が十分に担保されていない

情報提供の結果、誤った情報が世間に漏れることで、
・**責任追及を受けるリスク**
・**風評被害を受けるリスク**

（１）情報の取扱いに関するきめ細やかなルールの整備

協議会では、事業者等の皆様が**相談や情報提供を安心して**行うことができるよう、
情報の取扱いに関するきめ細やかなルールを整備しています。

事業者等の皆様が持ちうる懸念や不安

- 提供した情報が適切に取り扱われず、提供者名等が漏れてしまうおそれはないか。
- 任意の相談・情報提供は、信頼する相手にしか見せたくない。
- 任意の相談をしたせいで、監督官庁等に処分されてしまうおそれはないか。
- 情報提供した場合のメリットが分からない。
- 秘密とすべき情報をどのように扱えばいいかわからず不安がある。

協議会におけるルール整備（主なもの）

- 罰則※により担保された**高度な守秘義務**
  ※　一年以下の懲役又は五十万円以下の罰金
  （平成30年12月改正サイバーセキュリティ基本法により措置）
- 活動の中核となる連絡調整事務は**政令指定法人JPCERT/CC**が担当（注）
- 「情報提供者は、情報の共有範囲を設定可」
  「当該共有範囲は、勝手に変更されない」
- 「情報提供者は、監督官庁等を情報の共有範囲から除外可」
- 「協議会から、対策手法の助言や周辺状況のフィードバックが得られる」
- 「事務局は提供する情報の秘密の範囲を明示」
  「情報提供者は提供に際して秘密の有無を明示」
  ※登録した事務従事者のみが秘密を取り扱う

（注）協議会における情報共有活動の核となる連絡調整事務を**政令指定法人JPCERT/CC**が担当することについて

情報共有体制の参加者が安心して情報共有活動を行うためには、その結節点となる連絡調整事務を誰が担うのかが重要な問題となります。具体的には、脅威の性質や潜在的な標的の種類等に応じて連絡調整の内容及び相手方を適切に選定し、迅速かつ的確に実施する必要があります。このような考え方を踏まえ、平成30年12月改正サイバーセキュリティ基本法に基づき、この分野における連絡調整事務について長年の経験・実績を有し、海外の専門機関との連絡調整を行う日本の窓口として国際的にも認知されている「一般社団法人JPCERT/CC」が政令で指定され、協議会の事務局として連絡調整事務を安定的・継続的に担当することとなりました。

協議会の事務局を務めるのは①内閣官房（NISC）と②前述の政令指定法人JPCERT/CCですが、このうち構成員等から提供されたインシデント情報等の内容を取扱うのは後者②の政令指定法人JPCERT/CCであり、前者①の協議会事務局としてのNISCは、構成員間で発生した紛争を法令に基づき裁定する必要がある場合等例外的なケースを除いては、インシデント情報等の内容には一切アクセスしないことになっています。

（２）協議会への参加に伴い発生する義務や負担の明確化

協議会への参加に伴い発生する**義務や負担は最小限のもの**にとどめるとともに、
協議会の規約等でそれらの**具体的範囲を明確化**しています。

事業者等の皆様が持ちうる懸念や不安

- 機微な情報を法的根拠なく提供すると、他法に抵触するおそれがある。
- 情報提供義務が適用され、情報を何でも吸い上げられることにならないか。
- あとで規約が改正されて、情報を何でも吸い上げられることにならないか。
- 協議会に一度入ったら、もう脱会できなくなるのか。
- 会費等を求められるか。会議等で頻繁に出向く必要があるのか。
- 他の情報共有体制にも参加しており、無駄な重複作業等が発生する。

協議会におけるルール整備（主なもの）

- 法律に規定された**情報提供義務**を創設
  （平成30年12月改正サイバーセキュリティ基本法により措置）
- 情報提供義務の発動要件を「大規模なサイバー攻撃」「同意がある場合」等に限定
- 規約の改正は、総会（民間企業等を含む全構成員で構成）における多数決で決定
- 届出により、いつでも協議会を脱退可
- 会費等は無料（国費で運営）。
  また、できるだけリアルタイムでの情報共有を実現するため、協議会は逐一対面で集まるのではなく、政令指定法人が管理するシステム等を活用（総会等も同様）。
- 主要な情報共有体制は当初から協議会にご参加いただいているため、適切な連携※が可能。

※　他の情報共有体制との関係については次ページをご参照ください。

（３）他の情報共有体制との関係

○　協議会は、既存の様々な情報共有体制において**活動の活性化を妨げていた要因**を洗い出し、これを**法律改正等によって改善を図る**ことにより、**既存の情報共有体制の活動を補完**し、これらと**有機的に連携**しつつ、従来の枠を超えた情報共有・連携体制を構築していくことを目標としています。

○　**主要な情報共有体制の多くは既に協議会に参加**いただいています。協議会において作出された対策情報等は、本来はできるだけ多くの関係組織に共有され活用されることが望ましいとの考えに立ち、機微な情報を除いては他の情報共有体制においても展開可能（＝配信ルートを協議会システムに限定しない）としているため、これらの情報共有体制に既にご参加いただいている主体は、**必ずしも協議会に直接参加しなくても**、協議会から発信される情報のうち機微なもの等を除いた一定の範囲のものを、これらの情報共有体制を経由して取得することができます。

○　逆に、他の情報共有体制の場で既に共有されている情報のコピーを重ねて協議会の場でも共有することは想定していません。協議会は、**他の情報共有体制では拾えていなかった情報を早期に発見し共有**したり、他の情報共有体制で既に共有されている情報を**補完する機微な追加情報（被害発生業種など）を関係者を限定して共有**すること等に主眼があり、**真に有益で、他では得られない情報にしぼりこんで**共有を行っています。

※そもそも協議会は他の情報共有体制と比べ、①協議会の強い守秘義務等のルールを信頼して情報提供いただいた方の信頼を傷つけることがないよう、情報の共有の際には特に慎重な配慮が必要、②かなり早い段階から相談をいただくため、当初は断片的な情報が多く、関連情報の収集や分析を慎重に進めることが必要、といった特徴があり、現時点では、大量の情報を機械的に共有するような活動にはなっていません。

○　また、情報を任意にご提供いただく場合についても、**基本的に、他の情報共有体制に対し既にご提供いただいた情報と同一の情報を重ねて協議会に対してもご提供いただくよう協議会からお願いすることは想定していません。**

【主要な情報共有体制の例】

- 早期警戒情報の提供システム「CISTA」（JPCERT/CC）
- 「重要インフラの情報セキュリティ対策に係る第４次行動計画」に基づく情報共有体制（NISC）
- サイバー情報共有イニシアティブ「J-CSIP」（IPA）
- 日本サイバー犯罪対策センター（JC3）による情報共有
- サイバーセキュリティ対処調整センター（NISC）
- 重要インフラ分野の各セプター、ISAC　等（民間事業者等）

（参考２）サイバーセキュリティ基本法 抜粋（義務規定）

◆ **守秘義務関係（第17条第4項、第38条）**

✓ 第17条第4項

協議会の事務に従事する者又は従事していた者は、正当な理由がなく、当該事務に関して知り得た秘密を漏らし、又は盗用してはならない。

✓ 第38条

第十七条第四項又は第三十一条第二項の規定に違反した者は、一年以下の懲役又は五十万円以下の罰金に処する。

◆ **情報提供義務関係（第17条第３項）**

協議会は、第一項の協議を行うため必要があると認めるときは、その構成員に対し、サイバーセキュリティに関する施策の推進に関し必要な資料の提出、意見の開陳、説明その他の協力を求めることができる。この場合において、当該構成員は、正当な理由がある場合を除き、その求めに応じなければならない。

（４）核となる「タスクフォース」（TF）の結成
～サイバーセキュリティのプロのニーズにも応え、対策情報の迅速な作出を実現～

○サイバー攻撃の複雑化、巧妙化により、プロのセキュリティベンダ・専門機関等でさえ、早いタイミングで、自社単独で有効な分析を行い、確証をもって効果的な対策情報等を迅速に作出することには限界が生じてきています。
○本来は、プロ同士、もっと早いタイミングで、お互いに信頼し合って分析を提示し合い、答え合わせをすることができれば、確度の高い対策情報等をより迅速に作出し、国の行政機関、地方公共団体、重要社会基盤事業者等に対し、より早いタイミングで、有用な情報の共有が可能となるはずです。

専門機関・ベンダが直面する課題

まだ確証が得られていない分析内容等を自社の外部に提供するのは難しい

貴重な情報を提供するのだから、
こちらから情報を出すばかりでは不公平

せっかく貴重な情報を提供したので、
きちんとフィードバックが欲しい

協議会におけるルール整備（概要）

- ✓ 罰則により担保された強い守秘義務が適用されるという協議会の特徴を最大限に活かし、協議会内部に、高度な信頼関係を前提とする少数の有志による特別なタスクフォース（TF）を設置。
- ✓ TF参加者の中だけで、未確証の分析内容等、密度の濃い情報を相互に情報交換

（公的な取組としては、世界的に見てもほぼ前例なし）

TF内では、「ただ乗り」を防止し、
ギブアンドテイクの情報共有

TF内では、提供した情報に対し
必ずフィードバックを得られる仕組み

タスクフォース（TF）を中心に、**協議会発の対策情報等の迅速な作出、共有を実現**

（参考３）サイバーセキュリティ協議会の活動イメージ

第一類構成員等（第一類構成員及び政令指定法人 ） （主にセキュリティ専門機関・セキュリティベンダ等）		第二類構成員、一般の構成員 （主に国の行政機関、地方公共団体、重要インフラ、教育研究機関、一般企業等）
①第一類構成員等は、マルウェア検体や、自組織単独ではまだ確証を得るに至っていない専門的な分析内容（マルウェアの挙動に関する分析など）を、必要に応じて強い守秘義務をかけて内々に持ち寄り、お互いにフィードバックし合い、分析の確度を急速に高め、端的で分かりやすい対策情報等（特定のパッチの適用など）をすみやかに他の構成員に広く提供。	①：対策情報等の提供（確度：高）	※　協議会へのご参加は、あくまで各主体の任意のご判断 ①一般の構成員及び第二類構成員は、協議会から迅速に提供された、確度の高い対策情報等を受領し、自らの組織の対策に迅速に役立てる。
②第一類構成員等は、まだ確証を得るに至っていない対策情報等を、第二類構成員（フィードバックについては積極的に貢献する意欲と能力を有する有志の構成員）に対してのみ、必要に応じて強い守秘義務をかけて内々に提供し、そこから得られたフィードバックを参考に、更に分析の確度を急速に上げる。 ※第一類構成員にとっては、第二類構成員等からのフィードバックにより、当該サイバー攻撃がどの分野や地域に行われているかといった全体的な傾向等を早期に把握することが可能となる。	②：対策情報等の提供（確度：低） ②フィードバック	②これに加え、第二類構成員は、更に早い段階の対策情報等を受領することができる。 （ただし確度は十分でない。また、必要に応じて強い守秘義務が適用。） そして、これに対するフィードバックを行う。
③第一類構成員等は、このほか、問題が生じている企業等からの内々の相談にも丁寧に対応することで、社会全体として、今、何が起きているのか、すばやく察知する機会を得ることができる。	③-1：内々に相談 ③-2：内々に助言	③一般の構成員及び第二類構成員は、自組織で問題が生じた場合は、必要に応じて強い守秘義務をかけて第一類構成員等に内々に相談（任意）し、対策手法の助言や周辺状況のフィードバックを取得 ※「いつもと何か違う…」といった、直感的な違和感が生じただけの段階でも、気軽に相談可能。
※　要件を満たし、希望すれば、専門機関やベンダ以外の主体も第一類構成員となることが可能。 ※　第一類構成員となった後、求められる貢献をしない者は、その地位を維持できない。		※　国の行政機関、地方公共団体、重要インフラ、教育研究機関、一般企業等のいずれの主体であっても、要件を満たし、希望すれば、第二類構成員となることが可能。 ※　第二類構成員となった後、求められる貢献をしない者は、その地位を維持できない。

【参考４】構成員の分類と、それらの相違点について

タスクフォースを構成

構成員の分類	役割	要件	義務の適用 守秘義務	義務の適用 情報提供義務	メリット
第一類構成員 ※ 政令指定法人JPCERT/CCとともに「**第一類構成員G**」を構成	自組織単独ではまだ確証を得るに至っていない専門的な分析内容等を積極的に提供し合い、**具体的な対策情報等を作出していく。**	他の第一類に対する専門的な見地からのフィードバックに加え、**自らも、自組織で収集・分析したオリジナル情報（まだ他には提供していないもの）を積極的に提供する意欲と能力を有する**こと	◎ （次頁参照）	◎ 大規模サイバー攻撃等に限らず、専門的な見地からのフィードバックに加え、自らもオリジナル情報を提供する義務が適用	①**他では得ることができない機微な情報を**入手できる。 ②TFで入手した情報は**自らの顧客等のサイバーセキュリティ確保のために活用**することができる。 （②は第一類のみ認められる特例）
第二類構成員	**第一類構成員から共有された対策情報等に対してフィードバックを行い、**第一類構成員による対策情報等の精度向上等に積極的に協力する。	第一類構成員Gからの対策情報等に対して、**迅速にフィードバックを行う**こと （「来ている」「来ていない」「わからない」といった端的なもので可）	○ （次頁参照）	○ 大規模サイバー攻撃等に限らず、端的なフィードバックを行う義務が適用	一般の構成員より対策情報を早く受領するので、**早期に対策を行う**ことができる。 （ただし、確度が低いため、自己責任での判断となる。一定の分析力や知見が必要。）
一般の構成員	**通常は、専らタスクフォースからの情報を受領し、自組織の対策に活用する。** ※例外的に、大規模なサイバー攻撃等の場合は、情報提供にも協力する	協議会の目的及び活動内容に賛同すること等	△ （次頁参照）	△ 大規模サイバー攻撃等の場合等限定的に適用 基本的に第二類と同様の端的なフィードバックで可とする運用を想定	タスクフォースが作出した**対策情報等**が得られる また、直感的な違和感といった早期の段階であっても、希望すれば、守秘義務の下、**安心して情報提供や相談を行う**ことが可。**対策手法の助言や周辺状況のフィードバック**が得られる。

タスクフォースには、
原則、**外資系法人**等は参加できない
（長年にわたり高度の信頼関係等を有するものとして特別の承認を得たものを除く）

【参考５】構成員の分類と、共有する情報のイメージ（典型例）

政令指定法人＋第一類構成員に限定

攻撃キャンペーンの動向、攻撃の手口、マルウェアの情報やその解析結果（ハッシュ値、接続先情報や具体的な挙動等）、踏み台サーバーの情報、攻撃対象業種等、様々な攻撃の痕跡を専門的に分析し、対策情報を作出

※いずれも自組織で収集・分析したオリジナル情報、かつ未確定情報

・通常は、被害組織名等は伏せたうえで、原則秘密指定し、第一類グループ限定で共有する。

タスクフォース（ＴＦ）構成員に限定（＝第二類構成員を含む）

接続先情報（未確定情報）

・通常は、秘密指定せずにTF限定で共有する。
・例外的に、接続先のドメイン名の中に被害組織名が類推され得る情報が含まれている場合等において、情報提供者の了解が得られた場合には、秘密指定して共有することがある。

このほか、
・攻撃の特定（ハッシュ値等）
・マルウエアの挙動の特徴
・攻撃に利用されている脆弱性の識別子
・攻撃に利用されている踏み台サーバーのURL
などの様々な攻撃の痕跡や対策情報
※いずれもある程度精査されているものの、なお未確定段階の情報

被害発生業種等に関する情報（未確定情報）

・通常は、秘密指定せずにTF限定で共有する。
・例外的に、当該業種に属する事業者数が少数である等、被害組織名が類推され得るおそれがある場合において、情報提供者の了解が得られた場合には、秘密指定して共有することがある。

全ての構成員　（＝一般の構成員を含む）

端的で分かりやすい対策情報（確定情報）

・通常は純粋な技術的情報であり、 秘密指定せずに共有する。
　※特定のパッチの適用の推奨、新種マルウェアのハッシュ値、接続先IPアドレスなど
・内容に応じて、公開したり、他の情報共有体制を通じて幅広く共有することがあるが、他方、当該対策情報が外部に漏洩すると攻撃者に対策の手の内を明らかにしてしまうおそれがある場合等においては、協議会構成員等に限定して共有することがある。

被害発生業種等に関する情報（確定情報）

・被害発生業種等は、通常はタスクフォースの内部のみで共有し、一般の構成員には共有しない。
・例外的に、当該情報を付加しなければ受け手が当該対策の緊急性等を理解できず、有効な対策を迅速に講じることが期待できない場合等において、情報提供者の了解が得られた場合には、必要に応じて秘密指定した上で、必要な範囲に限って共有することがある。

【参考６】協議会において共有される情報の内容について

協議会では、基本的に、**被害を受けた組織の名称や被害内容は伏せた上で**、
攻撃手法等に係る技術的な情報や対策情報を共有していくこととなります。

○　サイバーセキュリティ協議会は、同様の手口によるサイバー攻撃の被害がいたずらに拡大することがないよう、既に被害を受けた組織の名称や被害内容（具体的にどのような情報が漏えいしたか等）は伏せた上で、攻撃手法に係る技術的な情報等を早期に共有していく場です。（やむを得ず、被害組織名が類推され得る情報等を共有せざるを得ない事情がある場合においては、情報提供者の了解を得ることを前提とした上で、原則として守秘義務を適用し、かつ、限られた範囲においてのみ共有することになります。）

○　原則として被害組織の名称や被害内容を共有しないこととしているのは、
（１）「同様の手口による被害の拡大を防ぐ」という観点からは、当該攻撃の技術的手法等を分析・共有し、同種の攻撃に備えることができるようにすれば十分であり、必ずしも、先行被害組織が具体的に誰であり、その攻撃によってその組織から具体的に何が漏えいしたのかまでを第三者間で一般的に共有する必要はないこと（※）、
（２）対策を講じるうえで必要性の低い情報を（欲張って）付加しようとし、それに伴って、技術的情報の部分を含めた全体の共有範囲が狭くなってしまうと、より多くの組織に対策情報を共有し被害の拡大を防ぐ観点からかえって望ましくないことになること
（３）任意でなされた情報提供に対し、被害組織の名称や被害内容の開示を無理に促すと、情報提供そのものの意欲を萎縮させるおそれがあること、
といった理由によるものです。

※　例えば、家屋の空き巣対策に関し、ピッキングに強いシリンダーが普及したことにより、建物への新たな侵入手法としてサムターン回しが出現した、といった場合には、新たな手口であるサムターン回しの技術的な対策情報や、一般的な対策方法を早期に共有できれば十分であり、サムターン回しで既に被害に遭った方が誰で、何を盗まれたかまで第三者間で共有する必要は無い、ということと同じです。
　この協議会は、既に被害を受けた組織に係る個別の事案対処を行うことを目的とする場ではなく、また、この協議会に事業者等の皆様が安心して相談等を行うことができるようにするためには、情報提供者の名称が外部に漏れることは、決してあってはならないことと考えます。

【参考７】一般の構成員の協議会への参加に関するメリット及び留意点について

メリット	留意点
●協議会ならではの、秘密を含む情報など機微な情報を受領し、自組織の対策に活用することが可能 ※機微な情報は構成員限り（転送禁止）として共有することがある。（【参考５】参照）	●秘密を含む情報が共有されうることから、秘密の保持を確保するための環境整備等が求められる。 ⇒一般の構成員に対し、秘密を含む情報を頻繁に共有することは想定しておらず、また、予め構成員側で秘密を含む情報を受領しない設定を行うことも可能
●直感的な違和感といった早期の段階であっても、希望すれば、守秘義務の下、安心して情報提供や相談を行うことが可能。対策手法の助言や周辺状況のフィードバックが得られる。 ※協議会規約において、協議会タスクフォースから情報の原提供者へのフィードバック情報の提供に関する規定を明文化 ※協議会は、非構成員からも相談を受け付けるが、複数から相談を受けるなど業務がひっ迫している場合には、構成員からの相談を優先	●大規模サイバー攻撃の場合等、限定した形で情報提供を求められる。 ⇒情報提供としては、攻撃が「来ている」「来ていない」「分からない」といった端的なもので可能 ⇒原則として、夜間・休日の対応を求めるものではない。