National center of Incident readiness and
Strategy for Cybersecurity

情報共有のすすめ

～行う利点、持続的な活動のために重要なこと～

内閣官房
内閣サイバーセキュリティセンター
副センター長　内閣審議官
山内 智生
2019年11月7日

1　なぜ、協議会を作ったのか？

安心して参加できる情報共有体制の構築

既存の様々な情報共有体制※
　活発に活動し、セキュリティ対策の向上に寄与しているものが増加
　活動の活性化を妨げていた要因も存在

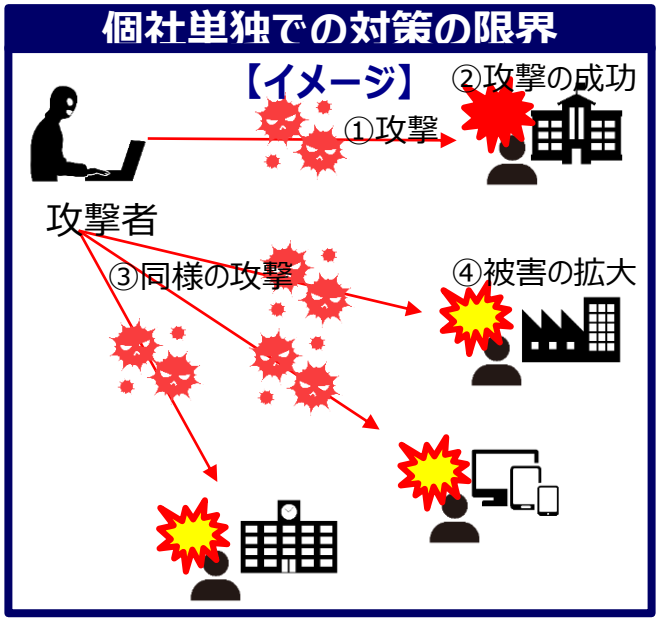
これらの要因を洗い出し

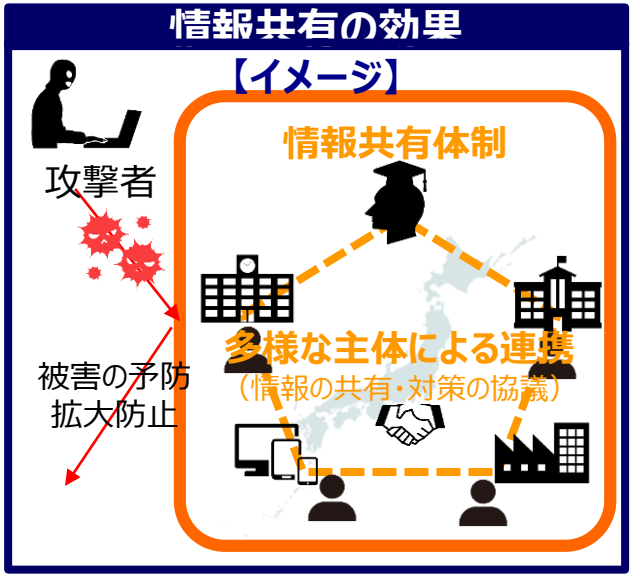
従来の枠を超えた情報共有・連携体制を構築
　サイバーセキュリティ基本法の改正によって**改善を図る**
　既存の情報共有体制の活動を補完し、これらと**有機的に連携**

これだけではイメージが湧かないと思いますので詳細は後ほど・・・

2　情報共有とは何か？

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





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**べきものだが・・・

⇩サイバー攻撃の複雑化、巧妙化

狙われた組織（相談された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**

攻撃手口や対策手法等を知らないと、**同様の手口**によるサイバー攻撃にあい、**被害が拡大するおそれ**

車の運転に例えると・・・

車の運転そのものはドライバー（システム運用者）が行っている。
別段、外部から情報を入手しなくても運転（運用）はできる・・・

しかし、どの道が事故で渋滞している、積雪でチェーン規制が行われているなどの情報を外部からもらうことができれば、迂回したりチェーンを持参する（トラフィック監視やDDoS対策を講じる）などの事前の対応ができて有益である・・・

いざという時に誰に聞けばいいかわからない、とか何をすればいいのかわからない、といったことにならないよう、普段から共有される情報に接していて、慌てず対処ができることが理想。

3　今までの情報共有はどうだったのか？

2005年12月 「重要インフラの情報セキュリティ対策に係る行動計画」（第１次行動計画）決定

※IT障害
重要インフラの各事業において発生する障害（サービスの停止や機能の障害）のうち、ITの機能不全が引き起こすもの

情報共有体制の強化

IT障害※の
①**未然防止**
②**拡大防止**・迅速な**復旧**
③要因の分析・検証等による**再発防止**
の3つの側面が重要

政府等は**重要インフラ事業者**等に適宜・適切に**提供**

事業者間、**相互依存性**のある**分野間**で適切に**情報共有**

事業者からの情報連絡があることが前提だが・・・

2011年7月～ 官民の様々な組織に標的型攻撃

三菱重工

ニュース 採用情報 | GLOBAL SITE MITSUBISHI HEAVY INDUSTRIES GROUP

企業情報 実績紹介 製品情報 CSR IR情報 グローバルネットワーク

HOME - 重要なお知らせ - 本日の一部報道について

重要なお知らせ

本日の一部報道について

2011-09-19

三菱重工業株式会社

本日、当社のコンピューターがウイルスに感染しているとの一部報道がありました。
8月中旬にウイルス感染の可能性が判明し、その後ウイルスの特性により情報漏えいの危険性も判明したことを受け、その旨を警察当局に報告、相談するとともに、以後、外部の専門家と共同で調査、対応を進めております。
現時点ではウイルス感染による被害拡大は止まったものと考えております。
また過去に社内一部のコンピューターのシステム情報（ネットワークアドレス等）が流出した可能性があることは判明しているものの、当社の製品や技術に関する情報の社外へのデータ流出は現在確認されておりません。
これまでウイルス駆除などの被害拡大防止策を講じておりますが、今後とも引き続き調査を進め、対策強化をはかってまいります。

三菱重工業報道発表

https://www.mhi.com/jp/notice/notice_110919.html

政府機関における情報セキュリティに係る年次報告（平成23年度）

https://www.nisc.go.jp/active/general/pdf/h23_report.pdf

ア）政府機関等への標的型攻撃

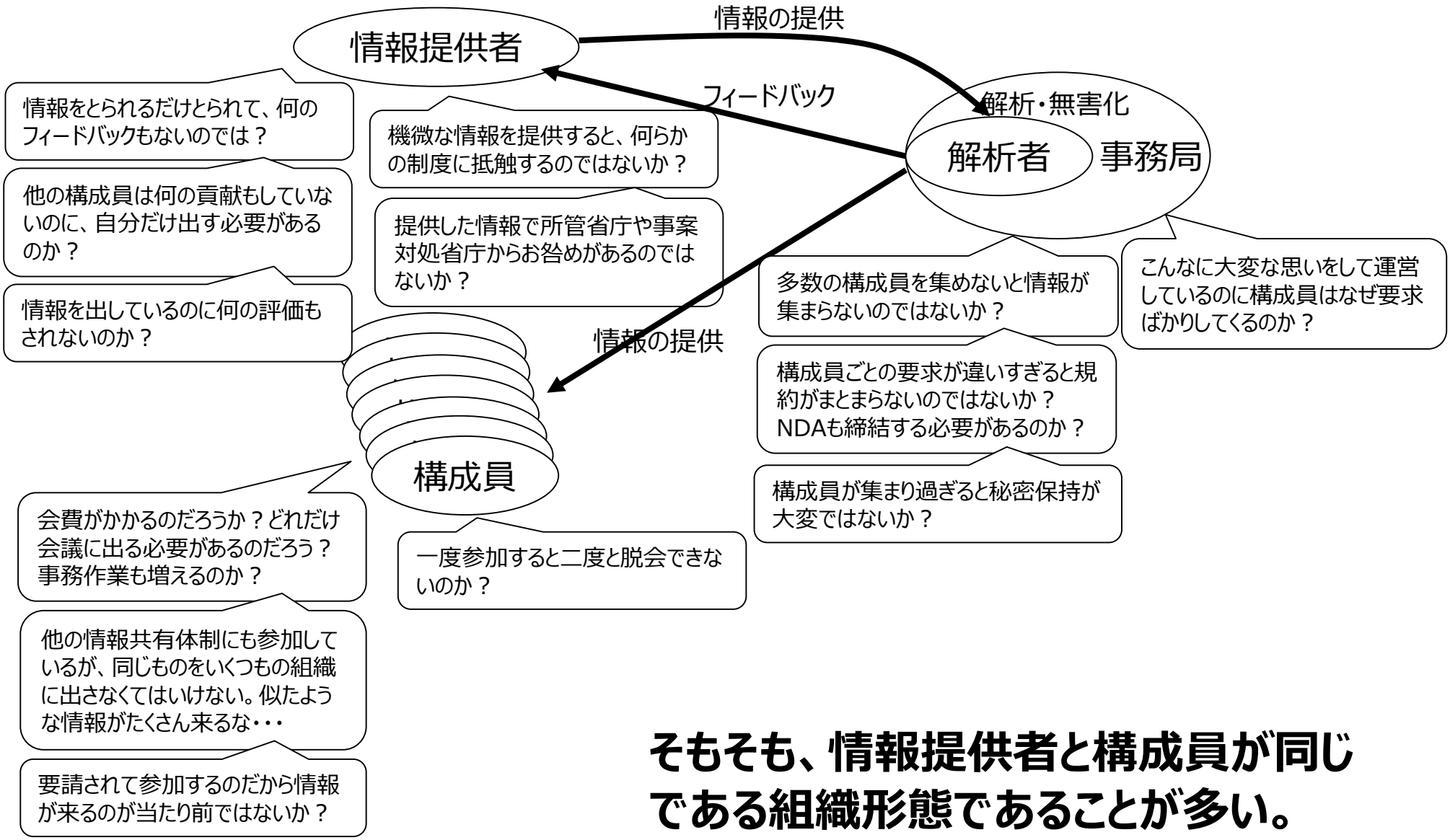
標的型攻撃（複数の攻撃手法を組み合わせ、ソーシャルエンジニアリングにより特定の組織や個人を狙い執拗に行われる攻撃）については、かねてから海外で発生事例が報告されていたが、平成 23 年度は、これらが我が国の政府機関等も標的になっていたことが顕在化した年となった。

現在、標的型攻撃の主な手法はメール（以下「標的型攻撃メール」という。）によるものであり、複数の府省庁から標的型攻撃メールが届いていると報告されている。そのうち、総務省及び外務省等では標的型攻撃メールに添付されたファイルを開封し、マルウェアに感染してしまうという事案も発生している。また、行政機関だけでなく、立法府である衆議院及び参議院の公務用メールアドレス宛にも標的型攻撃メールが送信され、院内のシステムがマルウェアに感染してしまうという事案も発生した。

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）

情報共有の際の様々な不安と懸念



そもそも、情報提供者と構成員が同じである組織形態であることが多い。

2017年　ランサムウェア「WannaCry」（ワナクライ）事案

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**

４　サイバーセキュリティ協議会の設立

サイバーセキュリティ基本法の一部を改正する法律案

趣旨

サイバーセキュリティに対する脅威が一層深刻化する中、我が国におけるサイバーセキュリティの確保を促進し、2020年東京オリンピック・パラリンピック競技大会の開催に万全を期すため、官民の多様な主体が相互に連携し、サイバーセキュリティに関する施策の推進に係る協議を行うための協議会を創設する等の措置を講ずる。

概要

1．サイバーセキュリティ協議会の創設

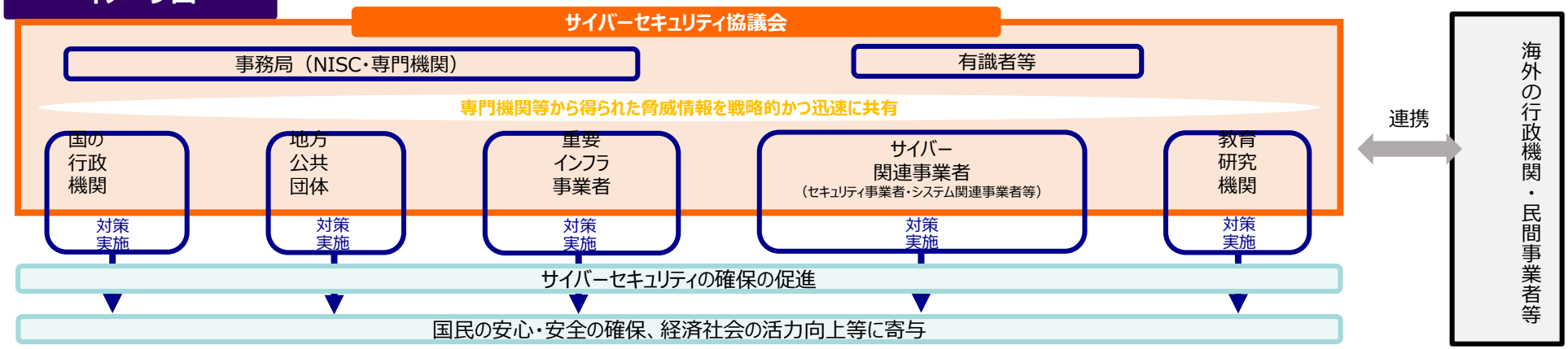
- 官民の多様な主体が相互に連携して情報共有を図り、必要な対策等について協議を行うための協議会を、サイバーセキュリティ戦略本部長等が創設する。
- 協議会の構成員（事務局：NISC、専門機関）
  国の行政機関、地方公共団体、重要インフラ事業者、サイバー関連事業者、
  教育研究機関、有識者　等
- 構成員の遵守事項
  秘密保持、協議会への情報提供の協力

2．サイバーセキュリティ戦略本部による連絡調整の推進

- サイバーセキュリティ戦略本部の所掌事務に、サイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整に関する事務を追加する。
- 上記事務の一部を政令で定める法人に委託することができることとするとともに、当該法人に対して秘密保持義務等を定める。

3．施行期日　公布の日から起算して一年を超えない範囲内において政令で定める日

イメージ図



昨年12月の臨時国会で成立
しかし、法律の規定だけで協議会の運営が成り立つ訳ではない・・・

1　情報の取扱いに関するきめ細やかなルールの整備

構成員が**相談や情報提供を安心して**行うことができるためのルール

構成員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。

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

「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」

「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

2　協議会への参加に伴い発生する義務や負担の最小化・明確化

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。

3　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～

○　セキュリティベンダ・専門機関等でさえ、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が困難状況。
○　これらの機関が、相互信頼の下、お互いの分析結果の「答え合わせ」ができれば、確度の高い対策情報等をより迅速に作出できる構成員に対して、より早いタイミングで、有用な情報の共有が可能となることを期待。

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**

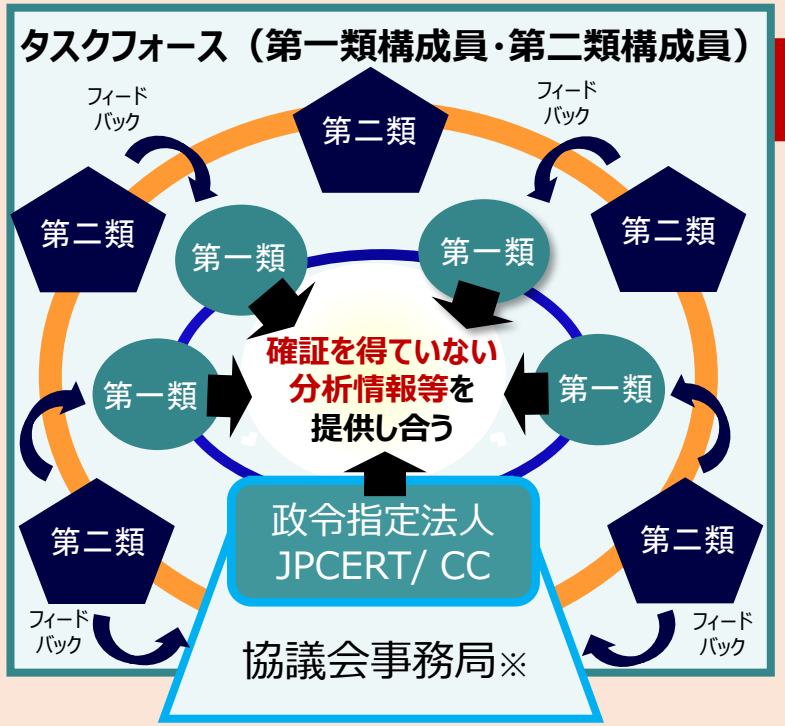
（全体像）サイバーセキュリティ協議会の概要

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基本戦略２G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

サイバーセキュリティ協議会の活動イメージ

NISC

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、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を、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、対策情報等をただちに他の構成員に広く提供。 ※専門的な分析内容の例： ・攻撃に利用されている脆弱性の識別子 ・マルウェアの挙動　等 ※対策情報等の例 ・特定のメーカーから出ている特定のパッチを当てる ・PCを立ち上げない　等	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、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、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、強い守秘義務をかけて第一類構成員等に内々に相談し、助言を受けることが可能（任意） ※「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。

最後に　協議会への参加をご検討いただく際に

○　協議会の事務局を担当するNISCとしては、ぜひとも協議会の趣旨に心よりご賛同いただき、**幅広い主体からご参加いただきたいと希望**するものの、参加はあくまで各主体の任意のご判断であり、**協議会事務局たるNISCが、協議会への参加にメリットを感じていない各主体のご意向に反してまで加入をお願いするようなことはいたしません**。

※そもそも、協議会への参加にメリットを感じていない主体に無理にご参加いただいても、活動の実態を得られず、かえって協議会全体の活動を停滞させるおそれがあります。

○　実際のところ、**既存の主要な情報共有体制の多くは既に協議会の活動にご参加**いただいているため、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、守秘義務等に反しない範囲であれば、協議会から発信される情報を、自らが参加する情報共有体制を経由して取得することが既に可能になっています。

○　他方、「協議会限りで共有される機微な情報も取得したい」「協議会から発信される情報を直接、漏れなく迅速に取得したい」といったニーズがある場合は、併せて協議会にも自らダイレクトに加入されることをお勧めいたします。

※実際に、これまでのところ、自組織の迅速な対策のためいち早く情報を取得しようとする意識が強い主体ほど、協議会へのご参加やお問合せを積極的にいただいている傾向があるようです。

○　サイバー攻撃の複雑化、巧妙化に伴い、情報共有の必要性が増しています。協議会に加入すれば、**協議会でしか得られない情報を得て、いち早く対策を講じる**ことができます。そのような**情報共有活動について意欲を有する主体からの積極的なご参加をお待ち**しています。

NISC

National center of Incident readiness and
Strategy for Cybersecurity

ご清聴ありがとうございました

https://www.nisc.go.jp