

## サイバーセキュリティ協議会について

資料 6 - 1 サイバーセキュリティ協議会の創設（概要）

資料 6 - 2 サイバーセキュリティ協議会について（詳細資料）

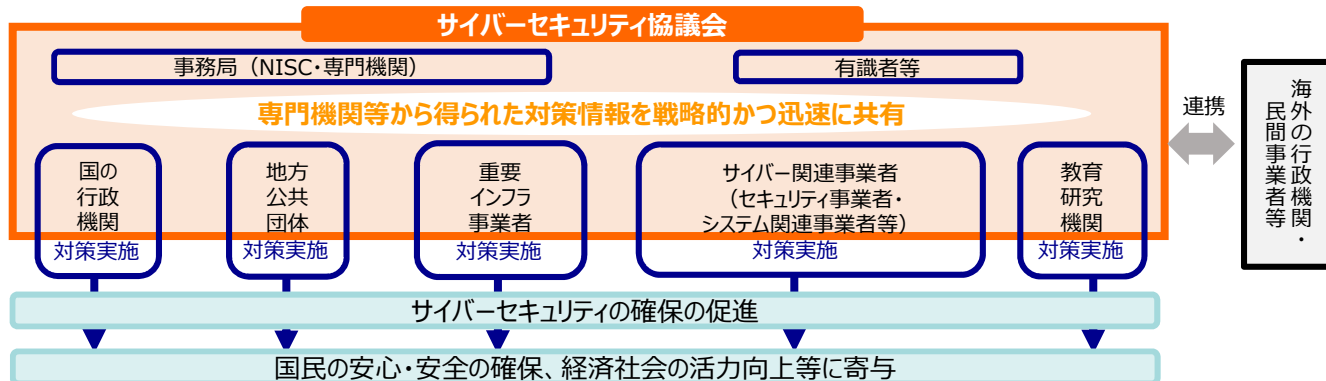
## サイバーセキュリティ基本法の一部を改正する法律が成立

～民間企業等が情報共有をためらう要因となっているデメリットを、法律上の措置によって除去～

※ 平成31年（2019年）4月1日施行

概要

- ・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**※
- ・**構成員に対して守秘義務及び情報提供義務を適用する等の措置を講ずる。** ※サイバーセキュリティ戦略本部長及びその委嘱を受けた国務大臣が組織

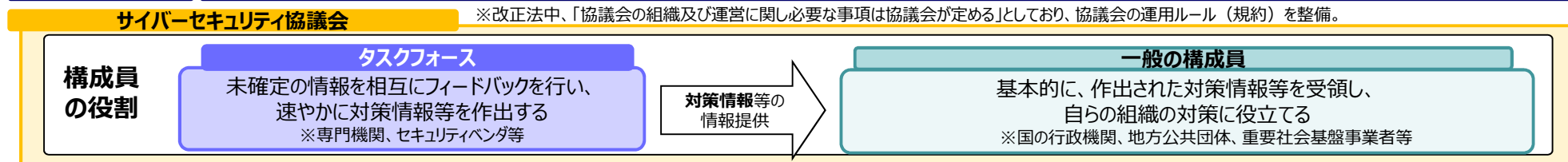


### ○情報共有のデメリット除去のために必要な規定を措置

- 1 罰則（※）により担保された**守秘義務**  
※ 1年以下の懲役又は50万円以下の罰金
- 2 法律に規定された**情報提供義務**

## サイバーセキュリティ協議会の運用ルール案 ～デメリットの除去に加え、協議会の運用ルールにより情報提供を行うメリットを付加～

背景	デメリット除去を法改正によって措置することは不可欠だが、それだけでは情報提供を促進するインセンティブにならないため、情報提供を行う <b>メリットを増加させることも重要</b>
解決策 (運用ルール案)	提供者の <b>モチベーション</b> と提供される <b>情報の質</b> を維持するため、積極的な情報提供に <b>能力と意欲</b> を有する者を、一般の構成員と別に、 <b>タスクフォース</b> としてグループ化
タスクフォース の <b>メリット</b>	<ul style="list-style-type: none"> <li>○ 提供した未確定の情報に対して<b>相互にフィードバック</b>を行うことで、<b>提供した情報の確度を高めることができる。</b></li> <li>○ 各主体がフィードバックだけでなく、自らも積極的に情報を提供する<b>ギブアンドテイクの原則</b>を徹底することで、<b>タスクフォースのみに共有される情報を得ることができる。</b></li> </ul>



➡ 2019年4月1日、サイバーセキュリティ協議会が組織され、同日から10日にかけて、構成員の募集を行い、5月17日、構成員を決定



**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

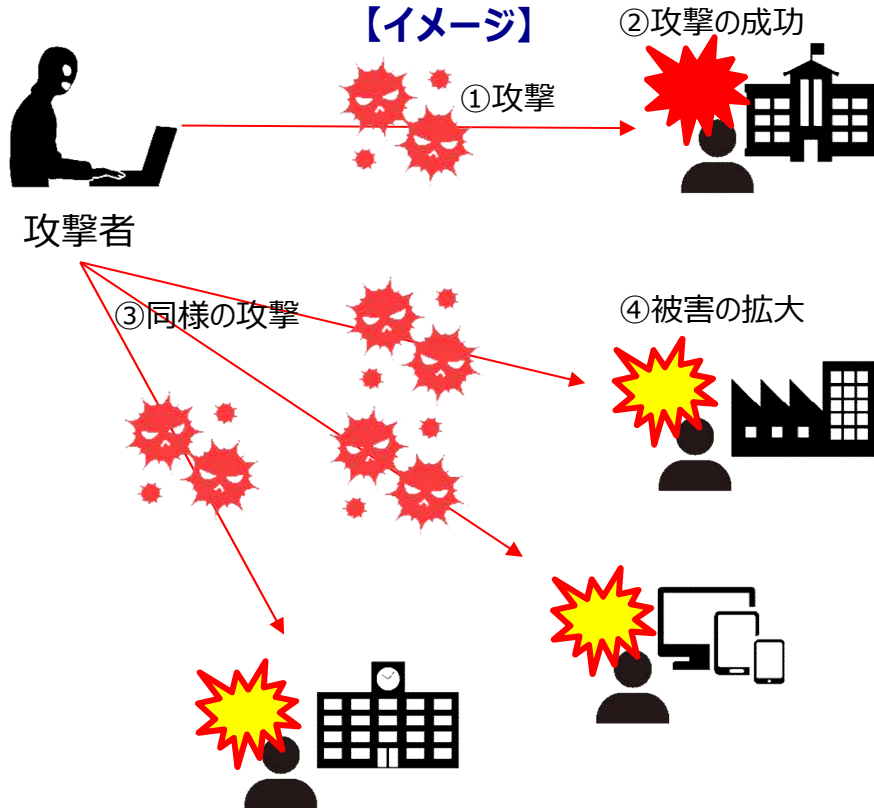
内閣官房 内閣サイバーセキュリティセンター  
基本戦略第2グループ  
令和元年5月

# 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

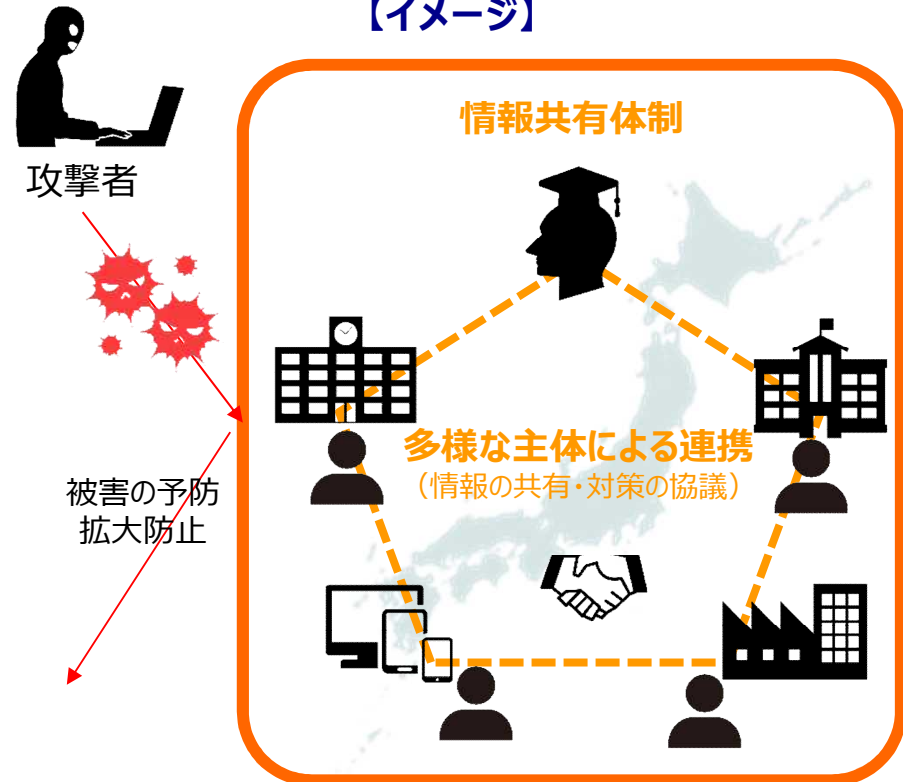
## 個社単独での対策の限界

【イメージ】



## 情報共有の効果

【イメージ】



## (参考) 既存の情報共有体制の具体例

- 現在、NISCをはじめとする政府機関や民間において、以下のような情報共有体制が活動している（代表的なものを紹介）。
- これらの活動が有効に機能している面もあるが、一部、まだ課題がある。

- 早期警戒情報の提供システム「CISTA」(JPCERT/CC)

※CISTA : Collective Intelligence Station for Trusted Advocates

- 「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)

※J-CSIP : Initiative for Cyber Security Information sharing Partnership of Japan

- 日本サイバー犯罪対策センター (JC3) による情報共有

- ICT-ISAC、金融ISAC、電力ISAC等 (民間事業者)

※ISAC : Information Sharing and Analysis Center

# (参考) 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 協議会の活動の「基礎」の確立

サイバーセキュリティ基本法の改正

# サイバーセキュリティ基本法改正により**協議会活動の基礎**を確立

2018.12  
サイバーセキュリティ基本法改正

「サイバーセキュリティ協議会」を創設し、その活動の**基礎**を確立

① 構成員が相互に**安心して情報共有を行うために必要不可欠な遵守事項**等を法定化

## 事業者等が直面する課題

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**

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

## 協議会構成員の遵守事項

罰則（1年以下の懲役又は50万円以下の罰金）により担保された  
**守秘義務**

法律に規定された  
**情報提供義務**

② 協議会における情報共有活動の核となる業務を**政令で指定する専門機関が担当**

協議会構成員等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**を担う機関が極めて重要であり、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ことについて、**長年にわたって経験・実績を有し、国内外の関係者との間で高度の信頼関係を構築している者が担当する必要がある。**

サイバーセキュリティ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」が政令指定法人として、協議会の連絡調整事務を担当**



## 2 安心して参加できる 運用ルールの整備



# 協議会の組織及び運営は、原則として、協議会自身が定める

## 改正 サイバーセキュリティ 基本法

罰則により担保された守秘義務等を直接規定する一方、それ以外の協議会の運用ルールは原則として協議会自身が定めるものとし、協議会の情報共有活動での実際の運用経験等を踏まえつつ、協議会自ら継続的に、かつ柔軟に運用ルールを見直していくことができるようにしている。

※改正サイバーセキュリティ基本法第17条第6項

(前各項に定めるもののほか、)  
協議会の組織及び運営に関し必要な事項は、協議会が定める。



我が国のサイバーセキュリティに対する脅威に連携して対応していく意思を有する多様な主体が、それぞれ安心して協議会に加入し、情報共有活動に参加することができるように、きめ細やかな運用ルール（協議会規約等）を整備

# 安心して参加していただくための運用ルール例

協議会では、**安心して、積極的に情報共有活動に参加していただけるよう**、事業者等の皆様が持ちうる懸念や不安を解消するための様々な運用ルールを協議会規約等に明文で盛り込んでいるところ（例えば以下のとおり）

## 事業者等の皆様が持ちうる懸念や不安

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。

## 運用ルール（規約等）における措置

「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」

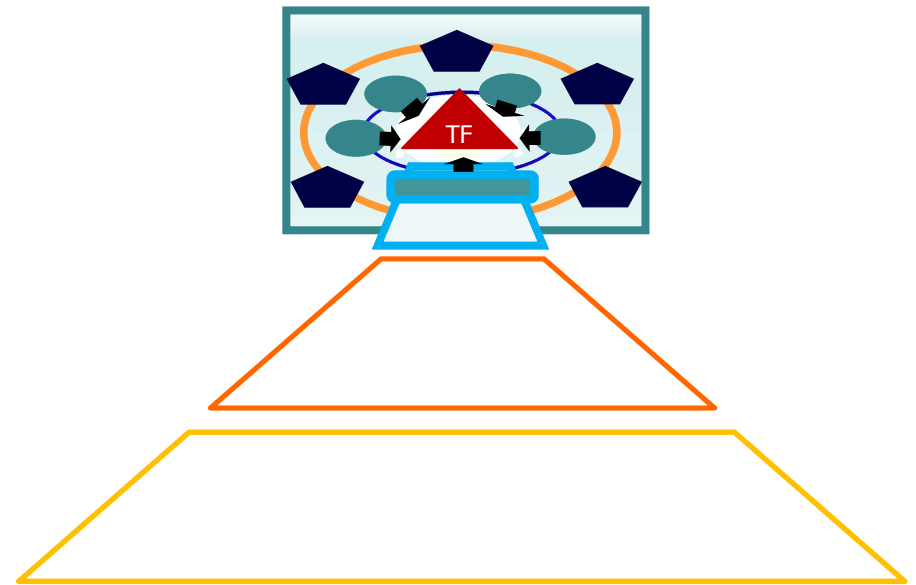
「情報提供者は、監督官庁等を情報の共有範囲から除外可」

情報提供義務の発動要件を「大規模なサイバー攻撃」等に明文で限定

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

### 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

## 協議会の 更なる 目標

- 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る。
- 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ある。

## 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

## 今回の協議会での解決の方向性

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  
今回の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）を設置し、その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  
（公的な取組みとしては、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、共有を実現していく。

# 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、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

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。

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。

※ 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。

①：対策情報等の提供  
（確度：高）

②：対策情報等の提供  
（確度：低）

②フィードバック

③-1：内々に相談

③-2：内々に助言

※ 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 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 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。

※ 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。

# (全体像) サイバーセキュリティ協議会の概要

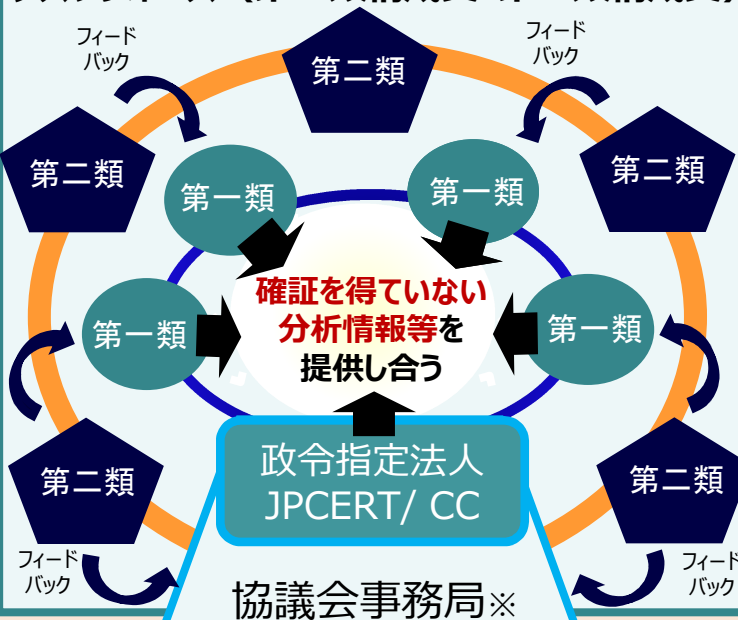
## 目的

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）

### タスクフォース（第一類構成員・第二類構成員）



## 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）

# 【参考1】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		メリット
			守秘義務	情報提供義務	
<b>第一類構成員</b>  <small>※ 政令指定法人 JPCERT/CC とともに「第一類構成員G」を構成</small>	自組織単独ではまだ確認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、 <b>具体的な対策情報等</b> 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、 <b>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</b>	◎ 被害組織名が判別できないようマスキングの上、被害状況や攻撃手法等は濃密に情報共有	◎ 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 <b>他では得ることができない機微な情報</b> を入手できる。 ② TFで入手した情報は <b>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</b> することができる。 （②は第一類のみ認められる特例）
<b>第二類構成員</b>	<b>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、</b> 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、 <b>迅速にフィードバックを行うこと</b> （「来ている」「来ていない」「わからない」といった端的なものでも可）	○ 被害状況の詳細は開示せず被害の有無のみ、攻撃手法等についても対策に必要な情報のみに絞り込んで情報共有	○ 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、 <b>早期に対策を行う</b> 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。）
<b>一般の構成員</b>	<b>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。</b>  <small>※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</small>	協議会の目的及び活動内容に賛同すること等	△ 一般の構成員に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、またあらかじめ構成員側で秘密情報を受領しない設定も可能	△ 大規模サイバー攻撃等の場合等限定的に適用	タスクフォースが作出した <b>対策情報</b> が得られる ・バッチの適用 ・注意メール 等  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、 <b>安心して情報提供や相談を行うことが可</b>

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2】 協議会の実務イメージ（その他）

## 1 利用システム

協議会の事務局はNISCが担い、その事務の一部をJPCERT/CCに委託。

できるだけリアルタイムでの情報共有を実現する観点から、協議会は逐一对面で集まるのではなく、システムを通じて実施。（総会、運営委員会の開催についても同様。）

JPCERT/CCは、以前から、早期警戒情報提供システム（以下「CISTA」という。）を構築し、幅広く内外から情報を収集し、登録者あてに早期警戒情報の発信を行っているため、協議会のシステムは、CISTAに、協議会に必要な機能（構成員間の情報交換を行うためのポータルサイト等）を追加する改修を行ったものを基盤としている。

## 2 他の情報共有体制との連携（関係者の事務負担増への配慮）

協議会構成員等のうち、既存の他の情報共有体制にも既に参加している皆様において、無駄な重複作業等が発生することのないよう、協議会としては、今後、既存の様々な情報共有体制との連携を積極的に進めていく予定。

実際に、2ページ目に挙げた主要な情報共有体制は全て、当初から協議会にご参画いただくこととなり、また、重要インフラ事業者のセプター事務局等も半分以上が当初からご参画いただくこととなったため、協議会と他の情報共有体制との連携の道筋は、かなり具体的に見えてきていると考えているところ。

## 【参考3】 協議会活動開始後の当面のスケジュール

	4月	5月	6月	7月	8月	9月	10月	11月	12月
マスターイベント			★ 6/28・29 G20サミット				★ ← (9/20~11/2) → ラグビーW杯		
協議会関係	★ 4/1 改正法施行 協議会設立	★ 5/17 第1期 構成員確定			★ 8月ごろ 第2期構成員 確定 (予定)				★ 12月ごろ 第3期構成員 確定 (予定)
	▲ 第1期 申込み受付期間 (4/1~4/10)				▲ 第2期 申込み開始 (予定)				▲ 第3期 申込み開始 (予定)
		▲ 暫定稼働開始 (システム既利用者を中心に)		▲ 必要に応じて、 総会・規約等の改正				▲ 必要に応じて、 総会・規約等の改正	