資料８

サイバーセキュリティ協議会の取組状況

資料８－１　サイバーセキュリティ協議会の取組状況（概要）

資料８－２　サイバーセキュリティ協議会の取組状況（詳細資料）

資料８－３　サイバーセキュリティ協議会の取組に対する現時点の評価及び今後の方向性について

サイバーセキュリティ協議会の取組状況

資料8-1

概要

・サイバーセキュリティ基本法の一部を改正する法律に基づき、平成31年４月にサイバーセキュリティ協議会が組織され、同年５月下旬から情報共有活動が開始されている。

・本協議会は、国の行政機関、重要社会基盤事業者、サイバー関連事業者等、官民の多様な主体が相互に連携し、より早期の段階で、サイバーセキュリティの確保に資する情報を迅速に共有することにより、サイバー攻撃による被害を予防し、また、被害の拡大を防ぐことなどを目的としている。

サイバーセキュリティ協議会

事務局（NISC・政令指定法人JPCERT/CC）

✓積極的な情報提供に能力と意欲を有する者を**タスクフォース**としてグループ化

タスクフォースにおいて作出された対策情報等を迅速に共有

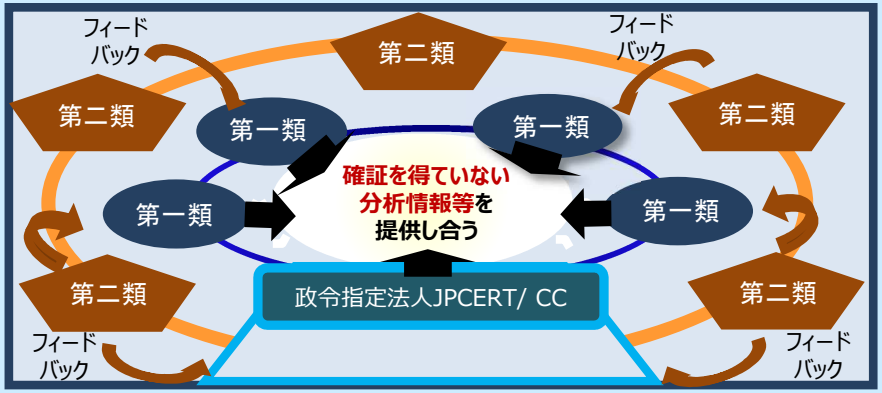
国の行政機関	地方公共団体	重要インフラ事業者	サイバー関連事業者（セキュリティ事業者・システム関連事業者等）	教育研究機関
対策実施	対策実施	対策実施	対策実施	対策実施

サイバーセキュリティの確保の促進

国民の安心・安全の確保、経済社会の活力向上等に寄与

タスクフォース（第一類構成員・第二類構成員）

✓未確定の情報を相互にフィードバックを行い、速やかに対策情報等を作出
✓活動の中核となる第一類構成員は、主に専門機関・セキュリティベンダ等から構成
✓第二類構成員は第一類構成員に対して主にフィードバックを積極的に行う



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）
○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
　　→協議会の特性を活かした迅速な情報共有を実施するなど、**一定の成果**が出始めている。
　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
　３月10日：第三期構成員の入会申込受付開始（３月10日～27日まで）
　６月 ５日：第三期の構成員を決定→第一期及び第二期構成員を含め**全225者**
（今後の予定）
　令和２年内：第四期構成員の入会申込受付開始（予定）
　※具体的な時期については、新型コロナウイルスの収束動向等を踏まえ、決定する予定

資料8-２

NISC

National center of Incident readiness and Strategy for Cybersecurity

サイバーセキュリティ協議会の取組状況

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
基本戦略第２グループ
令和２年７月

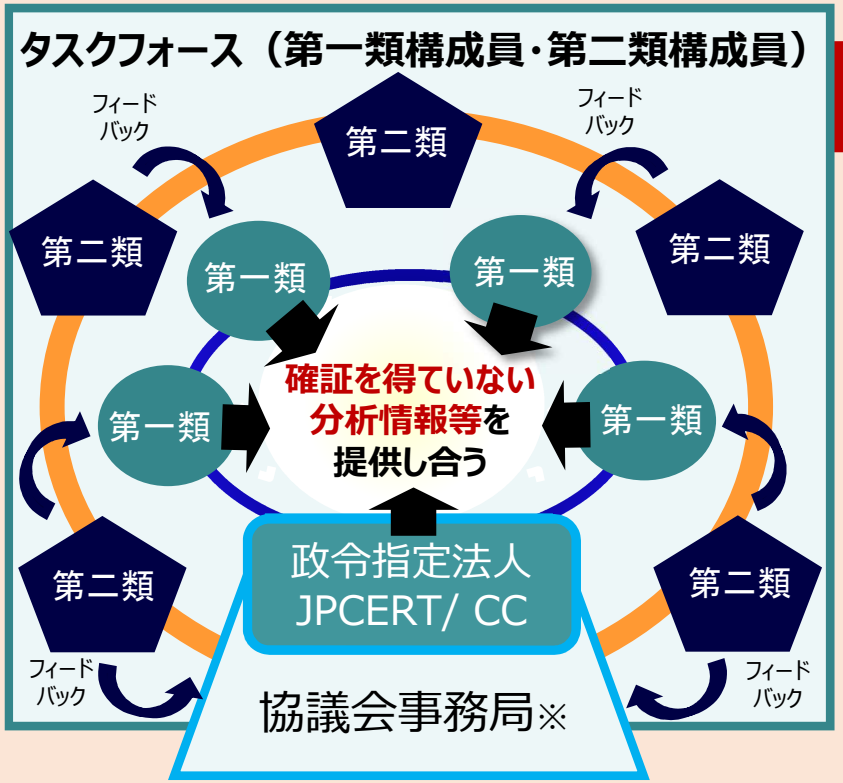
サイバーセキュリティ協議会の概要

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

協議会の運用状況

（平成31.4.1～）

（１）参加者の拡大

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

３月10日：第三期構成員の入会申込受付開始（３月10日～27日まで）

６月 ５日：第三期の構成員を決定→第一期及び第二期構成員を含め全225者
一覧は次頁参照

（今後の予定）

令和２年内：第四期構成員の入会申込受付開始（予定）

※具体的な時期については、新型コロナウイルスの収束動向等を踏まえ、決定する予定

サイバーセキュリティ協議会構成員名簿（令和2年6月5日時点）

1	国の関係行政機関の長等【75】							
①	国の関係行政機関の長等【26】	1	内閣官房内閣サイバーセキュリティセンター（解析担当）	8	公正取引委員会委員長	18	財務大臣
				9	国家公安委員会委員長	19	文部科学大臣
		2	内閣官房長官	10	個人情報保護委員会委員長	20	厚生労働大臣
		3	情報通信技術(IT)政策担当大臣	11	カジノ管理委員会委員長	21	農林水産大臣
		4	東京オリンピック・東京パラリンピック競技大会担当大臣（サイバーセキュリティ戦略本部に関する事務を担当する国務大臣）	12	金融庁長官	22	経済産業大臣
				13	消費者庁長官	23	国土交通大臣
				14	復興庁統括官	24	環境大臣
		5	内閣法制局長官	15	総務大臣	25	防衛大臣
		6	人事院総裁	16	法務大臣	26	日本銀行
		7	宮内庁長官	17	外務大臣		
②	独立行政法人等【49】（※3）	1	（独）情報処理推進機構	18	（独）国立女性教育会館	35	（独）日本学術振興会
		2	（独）奄美群島振興開発基金	19	（独）国立青少年教育振興機構	36	（独）日本芸術文化振興会
		3	（国研）医薬基盤・健康・栄養研究所	20	国家公務員共済組合連合会	37	（独）日本高速道路保有・債務返済機構
		4	（国研）宇宙航空研究開発機構	21	（国研）産業技術総合研究所	38	（独）日本スポーツ振興センター
		5	（国研）海上・港湾・航空技術研究所	22	（独）自動車事故対策機構	39	日本年金機構
		6	（国研）科学技術振興機構	23	（独）住宅金融支援機構	40	（国研）農業・食品産業技術総合研究機構
		7	（独）環境再生保全機構	24	（独）酒類総合研究所	41	（独）農林水産消費安全技術センター
		8	（独）勤労者退職金共済機構	25	（国研）新エネルギー・産業技術総合開発機構	42	（独）福祉医療機構
		9	（独）経済産業研究所	26	（国研）森林研究・整備機構	43	（国研）物質・材料研究機構
		10	（国研）建築研究所	27	（独）造幣局	44	（国研）防災科学技術研究所
		11	（独）高齢・障害・求職者雇用支援機構	28	（独）中小企業基盤整備機構	45	（独）水資源機構
		12	（独）国際観光振興機構	29	（独）駐留軍等労働者労務管理機構	46	（独）郵便貯金簡易生命保険管理・郵便局ネットワーク支援機構
		13	（独）国際協力機構	30	（独）鉄道建設・運輸施設整備支援機構		
		14	（独）国際交流基金	31	（独）統計センター	47	（国研）量子科学技術研究開発機構
		15	（国研）国際農林水産業研究センター	32	（独）都市再生機構	48	（独）労働政策研究・研修機構
		16	（独）国立印刷局	33	（国研）土木研究所	49	【非公表】
		17	（独）国立重度知的障害者総合施設のぞみの園	34	（国研）日本医療研究開発機構		
2	地方公共団体等【3】	1	地方公共団体情報システム機構	2	地方税共同機構	3	宮城県サイバーセキュリティ協議会
3	重要社会基盤事業者等【50】（※4）						
①	情報通信【13】	1	（一社）ICT-ISAC	6	東日本電信電話（株）	11	（一社）日本ケーブルテレビ連盟
		2	（株）インターネットイニシアティブ	7	楽天モバイル（株）	12	放送セプター事務局
		3	ソフトバンク（株）	8	KDDI（株）	13	スカパーJSAT（株）
		4	西日本電信電話（株）	9	NTTコミュニケーションズ（株）		
		5	日本電信電話（株）	10	（株）NTTドコモ		
②	金融【10】	1	銀行等セプター事務局	5	（一社）金融ISAC	10	Japan Digital Design（株）
		2	証券セプター事務局（日本証券業協会）	6	第一生命保険（株）		
		3	生命保険セプター事務局	7	第一フロンティア生命保険（株）		
		4	損害保険セプター事務局（（一社）日本損害保険協会）	8	ネオファースト生命保険（株）		
				9	auカブコム証券（株）		
③	航空【1】	1	定期航空協会（航空セプター事務局）				
④	空港【9】	1	空港・空港ビル協議会（空港セプター事務局）	4	中部国際空港（株）	7	成田国際空港（株）
		2	関西エアポート（株）	5	東京国際空港ターミナル（株）	8	日本空港ビルデング（株）
		3	新千歳空港ターミナルビルディング（株）	6	那覇空港ビルディング（株）	9	福岡国際空港（株）
⑤	鉄道【1】	1	（一社）日本鉄道電気技術協会				
⑥	電力【1】	1	電力ISAC				
⑦	ガス【1】	1	（一社）日本ガス協会				
⑧	医療【6】	1	（公社）日本医師会（医療セプター事務局）	3	（国研）国立国際医療研究センター	5	（国研）国立精神・神経医療研究センター
		2	（国研）国立がん研究センター	4	（国研）国立循環器病研究センター	6	社会保険診療報酬支払基金
⑨	水道【1】	1	水道セプター事務局（（公社）日本水道協会）				
⑩	物流【3】	1	（一社）日本物流団体連合会	2	山九（株）	3	（株）DOHO
⑪	化学【1】	1	石油化学工業協会				
⑫	クレジット【1】	1	（一社）日本クレジット協会				
⑬	石油【2】	1	石油連盟	2	JXTGエネルギー（株）		

サイバーセキュリティ協議会構成員名簿（令和2年6月5日時点）

4	サイバー関連事業者等【62】	1	トレンドマイクロ（株）	22	サイファーマ（株）	43	（株）プロット
		2	（一財）日本サイバー犯罪対策センター	23	シスコシステムズ（同）	44	（株）ベルウクリエイティブ
		3	（株）ラック	24	情報セキュリティ（株）	45	マクニカネットワークス（株）
		4	NTTセキュリティ・ジャパン（株）	25	（株）セキサ	46	丸紅情報システムズ（株）
		5	日本電気（株）	26	（株）セキュアベース	47	三菱電機インフォメーションシステムズ（株）
		6	ネットワンシステムズ（株）	27	（株）セキュリティア	48	三菱電機インフォメーションネットワーク（株）
		7	富士ソフト（株）	28	（株）ソリトンシステムズ	49	ALSOK（綜合警備保障（株））
		8	富士通（株）	29	大日本印刷（株）	50	（株）Blue Planet-works
		9	三井物産セキュアディレクション（株）	30	（株）デジタルハーツ	51	eGIS（株）
		10	（株）FFRI	31	（株）東芝	52	FCAサイバーセキュリティチーム
		11	NRIセキュアテクノロジーズ（株）	32	トラストウェーブジャパン（株）	53	ITbook（株）
		12	SOMPOリスクマネジメント（株）	33	（特非）日本セキュリティ監査協会	54	i-3c（株）
		13	アクモス（株）	34	日本タタ・コンサルタンシー・サービシズ（株）	55	NECネッツエスアイ（株）（EOSC）
		14	（株）アズジェント	35	（特非）日本ネットワークセキュリティ協会	56	（株）RSコネクト
		15	（株）アルファ・ウェーブ	36	日本プルーフポイント（株）	57	SCSK（株）
		16	（株）イズム	37	日本ユニシス（株）	58	Strategic Cyber Holdings LLC(CYBERGYM TOKYO)
		17	ヴイエムウェア（株）	38	（株）バルクホールディングス	59	TIS（株）
		18	ウイングアーク1st（株）	39	（株）ファイブドライブ	60	（株）YONA
		19	（株）大塚商会	40	富士ゼロックス（株）	61	（株）ZenmuTech
		20	グーグル・クラウド・ジャパン（同）	41	ブリッジシップ（株）	62	【非公表】
		21	（株）ケイテック	42	（株）ブロードバンドセキュリティ		
5	教育研究機関等【11】	1	（国研）情報通信研究機構	5	（国研）理化学研究所	8	滋慶学園グループ
		2	（国研）海洋研究開発機構	6	大学共同利用機関法人 情報・システム研究機構　国立情報学研究所	9	（学）順正学園
		3	（独）国立高等専門学校機構			10	（大）東京海洋大学
		4	（国研）日本原子力研究開発機構	7	（公社）私立大学情報教育協会	11	（学）福岡大学
6	その他【24】	1	（一社）医療ISAC	9	（一社）日本士業協会	17	三菱化工機（株）
		2	外国人技能実習機構	10	（株）日本製鋼所	18	三菱電機（株）
		3	（株）システムエンタープライズ	11	（一財）日本品質保証機構	19	（株）ユーデンテクノ
		4	情報システム監査（株）	12	（一社）日本防衛装備工業会	20	（株）Bloom
		5	全国社会保険労務士会連合会	13	（株）日立製作所	21	BOLDLY（株）
		6	千代田化工建設（株）	14	古野電気（株）	22	（株）LIXIL
		7	（株）デンソー	15	（公財）防衛基盤整備協会	23	（株）SUBARU
		8	（一社）日本航空宇宙工業会	16	（株）三井E＆Sホールディングス	24	【非公表】
計		225					

※1　構成員名及び区分等については、サイバーセキュリティ協議会加入申込書等に基づき、第一類、第二類、一般の構成員の順で五十音順等に基づき記載している。
　　タスクフォース構成員について、第一類は　　、第二類は　　を参照。
※2　協議会の事務局として内閣官房内閣サイバーセキュリティセンター（NISC）及び政令指定法人JPCERTコーディネーションセンターが務める。
※3　独立行政法人及び指定法人の総数は1②以外の欄に記載されている10者を含め、計59者である。
※4　「重要社会基盤事業者等」欄において、複数の事業分野にまたがる重要社会基盤事業者等については、主たる事業分野で分類している。

（２）活用件数（令和２年３月31日時点）

■協議会に持ち込まれた攻撃活動の件数　全４６件

→対策情報等を広く公開等するに至ったものは１３件（令和２年３月３１日時点）

○昨年５月下旬に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、徐々に組織の壁を越えて共有され始めています。

○令和２年３月末までの間に協議会に提供された攻撃活動の件数（注）は４６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。

○このうち同日までに、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ものは１３件でした。

（参考）令和元年５月下旬～令和２年３月末　対策情報等を広く公開等するに至らなかった３３件（＝４６件－１３件）の内訳

（１）協議会における分析の結果、共有の必要性が低いと判断したもの	２７件
（ア）協議会における分析の結果、既知の脅威であるなど、第三者にとって目新しい情報はないと判断したもの	２件
（イ）協議会における分析の結果、一過性の脅威とみられるなど、既に脅威度が低下していると判断したもの	２５件
（ウ）上記（ア）・（イ）以外の理由により、共有の必要性が低いと判断したもの	０件
（２）共有の必要性が低いとは判断していないが、共有を断念したもの	０件
（ア）共有することについて情報提供者等の了解が得られず、共有を断念したもの	０件
（イ）サンプル不足等により分析が行き詰まり、共有を断念したもの	０件
（ウ）上記（ア）・（イ）以外の理由により、共有を断念したもの	０件
（３）分析作業中のもの（令和２年３月３１日時点）	６件
（合計）	**３３件**

＜注１＞「攻撃活動の件数」
○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＞「協議会における分析の結果、一過性の脅威とみられるなど、既に脅威度が低下していると判断したもの」
○例えば、「各組織の単独の分析では、当該攻撃が一過性のものか、まだ攻撃活動が継続しており他分野にも広がっているものかが判然としなかったが、協議会において各組織が持ちこんだ情報を横断的に照合・分析したことにより、当該攻撃の脅威度は既に低下していると判断できるようになったもの」などが挙げられます。
○このように、各組織の単独の分析では判然としなかったものについて、協議会の場で専門機関同士が早期に情報を共有することができたからこそ、結果的に「既に脅威度が低下している」という判断を行うことができたものであり、このような情報共有活動を通じて、今後各組織の単独の分析では「打ち漏らしていた」おそれのあるものを未然に防止していくことが期待されるところです。

＜注３＞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。

（参考）活用事例①
（令和２年６月30日時点）

（事例１）

G20大阪サミットが開催される直前に、協議会タスクフォースから第一類構成員を経由して、サミットの関係機関に対して、迅速に、サミットの運営上リスクとなりうる情報が提供された。

（事例２）

ある第一類構成員からの情報提供に対し、他の第一類構成員から、**他の情報共有体制ではまだ共有されていない有益な情報**が、**極めて短時間のうちに**追加で提供され、協議会タスクフォースから他の関係機関へ対策情報を提供するための分析の確度が急速に高まった。

（事例３）

・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４）

国内で確認された標的型サイバー攻撃（注：１月下旬以降、関連する報道あり）について、昨年より一定の関係組織※から攻撃手法等に係る技術的な情報の提供を受け、既に分析、情報共有等を行った。

※なお、サイバーセキュリティ協議会は、罰則により担保された守秘義務等を適用することにより、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ことを目的として創設されたものであり、具体的にどの組織から情報提供を受けたか等については、情報提供者との信頼関係等の観点から、協議会側からは一切お答えできません。ご容赦ください。

＜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）活用事例②
（令和２年６月30日時点）

（事例５）

・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。

（事例６）

・政令指定法人JPCERT/CCにおいて、新たな標的型攻撃が生じている事実等を把握し、当該攻撃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、本攻撃に関する分析等をさらに深めるため、協議会タスクフォース（第一類グループ）に相談を行ったところ、グループメンバーから当該攻撃に関する関連情報の提供を受けた。
・**本標的型攻撃は、新型コロナウイルスに関連したファイル名を用いるなど攻撃の手口等に変化**が見られた。こうした**刻々と変化している状況**であったため、対策情報を迅速に共有し、当該攻撃の動向を把握する観点から、ほぼ同時並行で**第二類構成員及び一般の構成員に対し共有し、併せてフィードバックを任意の協力ベースで求めた**。
・**当該対策情報は未確証の情報を含む**ものであったため、今回の**情報共有範囲は協議会構成員及びその共助対象組織に限定**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。

サイバーセキュリティ協議会の取組に対する現時点の評価及び今後の方向性について

資料8-３

協議会の取組に対する現時点の評価

●2019年４月に協議会が組織されて以降、これまでの実際の運用の経験や各主体の意見を丁寧に踏まえ、サイバーセキュリティ協議会規約等の運用ルールの見直しを行ってきた。

●2019年度中に協議会構成員の募集を３回行い、現在の協議会構成員総数は225者と漸次拡大しており、計画どおりの進捗が図られた。

●2019年５月下旬に協議会における情報共有活動が開始されて以降、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徐々に共有され始めており、2019年度末時点で対策情報等を広く公開等するに至ったものは13件と、協議会の特性を活かした迅速な情報共有が実施されるなど、一定の成果が得られたところである。

協議会の取組に対する現時点の評価としては、一定の成果をあげているものと評価できるが、
サイバー攻撃による被害やその拡大を防止するためには、協議会の運用を充実・強化していくことが必要不可欠

◆そこで、現在の協議会の運用における課題や改善をする余地がないかなどを把握するべく、まずは協議会の情報共有活動の中核となる政令指定法人JPCERTコーディネーションセンター及び第一類構成員に対してアンケート調査を実施。
　本アンケート調査の結果を踏まえ、運用面の改善策等について検討していく。

今後の協議会の方向性

○本協議会の実際の運用の経験やアンケート調査を行うなどして各主体の意見を丁寧に踏まえ、必要に応じて運用ルールやシステムを不断に見直していく。

○協議会の取組や参加に関するメリット等がより伝わるよう広報し、協議会への参加を呼び掛けるなど、引き続き、より多くの主体が協議会に参加する重厚な体制を構築していく。

○真に有益で、他では得られない協議会ならではの情報が共有されるよう、引き続き、より多様かつ重要なサイバーセキュリティの確保に資する情報を迅速かつ確実に共有していく。