資料10

NISC

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

平成31年４月
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

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）　既存の情報共有体制の具体例

〇現在、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）。

〇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	協議会構成員の遵守事項
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	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**
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	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	運用ルール（規約等）における措置
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。	「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」
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。	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
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。	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
協議会に一度入ったら、もう脱会できなくなるのか。	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

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）

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
（事業者等の団体や個人も含む）

【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 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	◎ 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**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）	○ 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、**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	△ 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**対策情報**が得られる ・パッチの適用 ・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、**安心して情報提供や相談を行う**ことが可

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　利用予定のシステム

協議会の事務局はNISCが担い、その事務の一部をJPCERT/CCに委託する予定。

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、協議会は逐一対面で集まるのではなく、システムを通じて行っていく予定。（総会、運営委員会の開催についても同様。）

JPCERT/CCは、現在も、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する。

2　協議会構成員からの情報提供について

協議会構成員等の皆様のご負担をできるだけ増加させないよう、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、協議会における情報の受付は基本的には関係者が既に参画している枠組みなどをできるだけ活用していく考え。（ただし、強い守秘義務が確保される協議会に対するダイレクトの情報提供を構成員等の皆様が自発的に希望される場合は、協議会へのダイレクトのご相談についても、丁寧に対応していく予定）

【参考３】 発足当初の構成員のイメージ

サイバーセキュリティ協議会

タスクフォース

第一類構成員

現在、国内の有力な専門機関、ベンダから参加の希望をいただいており、運用ルールの細部を調整中

第二類構成員

現在、国内の重要インフラ分野の共助組織等から参加の希望をいただいており、運用ルールの細部を調整中

政令指定法人JPCERT/ CC

協議会事務局

一般の構成員

・国の関係行政機関

・地方公共団体又はその共助組織

・重要インフラ事業者又はその共助組織
（個社、セプター、セプター事務局、ISAC　等）

のうち、協議会の趣旨にご賛同いただいた主体

※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

発足当初は、G20等に万全を期す観点から優先度の高い主体に対し、参加を呼びかけ

協議会の発足時点（2019年４月）における構成員の申込みについては、**同年6月のG20等に万全を期す観点から優先度の高い主体**に対し呼びかけを行うこととし、発足後、協議会の実際の運営状況等を踏まえつつ、**2020年東京大会等に万全を期す観点から漸次拡大**していくこととする予定。

【参考４】　協議会活動開始後の当面のスケジュール（予定）

	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 （本部長等、事務局により運営開始） バーチャル総会の開催、プレスリリース	☆ 5月中旬 第１期 構成員確定 （構成員が参加） 構成員リスト公開 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		★ ８月ごろ 第２期構成員確定				★ １２月ごろ 第３期構成員確定
	▲ 第１期 申込み開始 （4/1～4/10）			▲ 第２期 申込み開始				▲ 第３期 申込み開始	

NISC

National center of Incident readiness and Strategy for Cybersecurity

資料10－2

重要インフラから見た協議会のメリット

平成31年４月
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

（１）一般の企業・団体等（重要インフラ事業者に該当しない企業・団体等）から見たサイバーセキュリティ協議会に加入するメリット

※用語等については３ページ目を参照

（２）一般の重要インフラ事業者から見たサイバーセキュリティ協議会に加入するメリット

※用語等については３ページ目を参照

（３）東京大会を支える重要サービス事業者である重要インフラ事業者から見た サイバーセキュリティ協議会に加入するメリット

※「情報インシデント状態」：ここでは、サイバー攻撃の存在を検知・認知できた場合における情報システムの被害の確認の調査等を目的とする対応を行っている状態をいう。

※「サービスレベル低下状態」：ここでは、平常時（情報システムによるサービスが安全かつ持続的に提供されている状態）よりサービスレベルが低下し、サービスの継続等を目的とするコンティエンジェンシープラン等に基づく対応を行っている状態をいう。なお、情報システムの被害を確認する前の段階（そもそも攻撃の存在を検知・認知していないケースを含む。）で既に対外的なサービス障害等が生じて外形的に事象が公知となっているような場合（上記「例２」）においては、事実上、情報インシデント状態での対応が完了する前にサービスレベル低下状態への対応が（並走して）始まることとなる。

※「CISTA」：経済産業省予算事業「CISTA・検体分析機能の実用性調査及び開発」事業で運用する、情報共有・検体解析ポータルシステムをいう。

※「行動計画に基づく情報連絡」：ここでは、重フラ行動計画「2.1 情報連絡を行う場合」の対象となる情報のうち、事業者における事案発生の疑いの段階での事案の連絡、相談を気兼ねなく安心して行うことができる情報共有体制における取扱いが適すると考えられる情報（例：事業者等が検知した情報で非公知のもの、特定分野間に限定されるもの、機微性が高いもの、詳細な内容のものなどをいう。）を除いたものの情報連絡をいう。

※協議会が重要インフラ以外の主体から得られた情報等に基づき重要インフラ分野においても早期対処が必要と判断した場合には、提供者の同意を得た上で行動計画側等に提供することがあり得る。これに対し、行動計画側等から協議会側に早期対処の情報連絡を行う必要が生じるケースは、現実的にほぼ想定されない。

※図中「①行動計画」と「②ＣＳ対処調整センター」に関し、東京大会を支える重要サービス事業者である重要インフラ事業者については、①②それぞれに情報連絡を行うことも可能であるが、事業者側における業務負担の軽減を図る観点から、いずれか一方のみにご連絡いただくことも可能とする。いずれか一方のみにご連絡いただいた場合には、ＮＩＳＣ側の処理で、その提供された情報を他方にも共有することとする。この場合において、事業者がどちらに情報連絡を行うべきかの判断の目安として、東京大会の期間中及びその直前期（現時点では来年５月ごろ以降を想定）は②に対し連絡を行い、それ以外の期間は①に対し連絡を行うものとする。

資料１０－３

サイバーセキュリティ協議会の「規約」等の概要

Ⅰ　骨格

○　全ての構成員を対象とした「協議会規約」と、一部の構成員を対象とした「タスクフォース規則」とに分かれる。

Ⅱ　協議会全体の通則（協議会規約）

1　協議会の運営関係

（１）協議会の内部組織は、「総会」、「運営委員会」「事務局」の３つ（第４章）

（２）総会は、全ての構成員で構成

①規約の改正は総会議決事項（10②Ⅰ）

②電子的手段による開催も可（10⑦）

（３）運営委員会は、「本部長等」（CS 戦略本部長（内閣官房長官）及びその委嘱を受けた国務大臣）により運営（11②）

①電子的手段による開催も可（11⑦）

②実際の業務は NISC 副センター長及び戦略本部員閣僚の課長級の専決事項とすることを想定

（４）事務局は、NISC（協議会の庶務）及び政令指定法人 JPCERT/CC（連絡調整）により運営（12）

2　協議会の構成員

（１）協議会の構成員は、「本部長等」及び「加入構成員」に分かれる（２Ⅲ・Ⅳ、５）

（２）構成員になろうとする者は、運営委員会の承認を得て、加入構成員となる（６①、11③Ⅰ）

第 1GSOC 加盟機関については、通知で足りる（６⑤）

（３）構成員は、協議会の情報を取り扱う「事務従事者」を全て登録しなければならない（２Ⅴ、６⑥）

（４）構成員は、その協議会事務従事者に対し緊急時の迅速な対応の権限をあらかじめ付与するよう努める（６⑦）

（５）構成員の名簿は公表される。ただし、公表を望まない加入構成員については記載しない（25）

3　情報提供等協力の求め（第７章等）

（１）法第 17 条第 3 項の規定に基づく情報提供等の協力の求めは、大規模なサイバー攻撃の発生等の場合に限定（23）

（２）協力の求めは、運営委員会の議決により行う（11③Ⅳ）

4　情報共有活動

（１）協議会における情報共有は、JPCERT/CC が指定する協議会システム（CISTA システム）を利用（２XIII、14①）

（２）協議会の庶務を処理する NISC 基本戦略第２グループは、原則として、協議会システムへの投稿にアクセスしない（14③）

（３）事務局は、その取扱う情報を、協議会の活動目的以外の目的で利用してはならない（19①）

構成員は、原則として、協議会から提供された情報を、自らのサイバーセキュリティを確保する目的以外の目的で利用してはならない（19②）

ただし、共助等を目的とする法人その他の団体（ISAC やセプター事務局等）は、守秘義務に反

しない範囲で、共助等の対象となる組織（ISAC 会員、セプター構成員等）のサイバーセキュリティ確保目的で利用可能（19④、22②、③）

（４）構成員は、任意に行う情報の提供に際し、共有範囲を指定することができる（17①、19②）
　事務局を含め、何人も、当該構成員の同意を得ることなく、当該共有範囲を超えて情報の共有を行ってはならない（17①）

（５）事務局は、構成員への情報の提供に際し、共有範囲を指定することができる（17②、③）

（６）構成員は、秘密情報の受領を希望しない場合は、受領拒否の設定を行うことができる（18⑤）

（７）構成員のうち特定連携構成員（第 1GSOC、第 2GSOC 加盟機関）は、政府機関横断構成員（GSOC）を経由して、協議会における情報共有活動を行う（２XI、21）

（８）構成員（特定連携構成員を除く。）は、原則として、構成員となったとき、併せて、協議会とは別の事業として JPCERT/CC が提供する早期警戒情報提供サービス（JPCERT/CC 脅威情報分析支援サービスを想定）の登録を受けたものとみなす（２XIV、15）

Ⅲ　タスクフォースの特則（協議会規約第 24 条等、タスクフォース規則）

（１）協議会に、協議会の活動に積極的に貢献する意欲と能力を有する構成員のみが参加するタスクフォースを置く。

（２）外国の法人等は、原則として 24 条タスクフォースには参加できない。

（３）タスクフォースの内部の取り決めはタスクフォースに参加する構成員による自治運営に委ねられる。

（４）タスクフォースに参加する構成員は、以下の２つに分類される。

①第一類構成員
　他の第一類構成員等から提供される情報に対するフィードバックを積極的に行うことに加え、自らも積極的に情報を提供する。

②第二類構成員
　第一類構成員等から提供される情報に対するフィードバックを積極的に行う。

（５）タスクフォースに参加する構成員になろうとする者は、タスクフォースの承認を得て、第一類構成員又は第二類構成員となる。

以上

資料１０－４

サイバーセキュリティ協議会規約

平成 31 年４月１日制定

第１章　総論

第１条　サイバーセキュリティ基本法（平成 26 年法律第 104 号、以下「法」という。）第 17 条第１項の規定に基づき、サイバーセキュリティ協議会を組織する。

（定義）

第２条　本規約において使用される用語の定義は、次のとおりとする。

一　協議会　法第 17 条第１項に規定するサイバーセキュリティ協議会

二　本部長等　法第 28 条第１項に規定す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

三　加入構成員　法第 17 条第２項及び本規約第６条の規定に基づき加えられた構成員

四　構成員　本部長等たる構成員及び加入構成員

五　協議会事務従事者　法第 17 条第４項にいう協議会の事務に従事する者（従事する可能性がある者を含む。）

六　NISC　内閣官房内閣サイバーセキュリティセンター

七　JPCERT/CC　一般社団法人 JPCERT コーディネーションセンター

八　重要社会基盤事業者　法第３条第１項に規定する重要社会基盤事業者（国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものに関する事業を行う者）

九　サイバー関連事業者　法第７条に規定するサイバー関連事業者（インターネットその他の高度情報通信ネットワークの整備、情報通信技術の活用又はサイバーセキュリティに関する事業を行う者）

十　政令指定法人 JPCERT/CC　法第 31 条第１項第２号及びサイバーセキュリティ基本法施行令（平成 26 年政令第 400 号）第５条に基づき事務の委託を受けた法人としての JPCERT/CC

十一　政府機関横断構成員　政府横断的な情報収集、攻撃等の分析・解析、各政府機関への助言及び各政府機関の相互連携促進及び情報共有等の業務を行う者として運営委員長が指定する構成員

十二　特定連携構成員　構成員のうち、国の関係行政機関の長（当該国の関係行政機関の長が内閣総理大臣の場合にあっては、担当する部局の長）、独立行政法人の長、指定法人の代表者であって、政府機関横断構成員と連携する者

十三　協議会システム　協議会における情報共有を行うために用いられる情報システム

として政令指定法人 JPCERT/CC が指定するもの

十四　早期警戒情報提供サービス　JPCERT/CC が協議会システムと互換性がある情報システムを用いて協議会とは別の事業として行う早期警戒情報の提供サービスであって、政令指定法人 JPCERT/CC が指定するもの

（目的）

第３条　協議会は、国、地方公共団体、重要社会基盤事業者、サイバー関連事業者、大学その他の教育研究機関等のうち、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ことを目的とする。

（活動）

第４条　協議会は、前条の目的を達成するため、次の各号に掲げる活動を行う。

一　サイバーセキュリティに関する脅威情報等の共有及び分析

二　前号の共有及び分析に基づき我が国のサイバーセキュリティを確保するために必要な情報の作出及び共有

三　前各号の活動に資する関係者間の連携の促進

四　前三号に掲げるもののほか、前条の目的を達成するために必要な活動

２　協議会は、前項に規定する活動を行うにあたって、次の各号に掲げる情報その他のサイバーセキュリティの確保に資する情報を取り扱うものとする。

一　サイバー攻撃による被害発生の動向等に関する情報

二　サイバー攻撃の攻撃手法等に関する情報

３　協議会は、特に、協議会事務従事者には法第 17 条第４項及び法第 38 条に基づき罰則により担保された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、国、地方公共団体、重要社会基盤事業者、サイバー関連事業者、大学その他の教育研究機関等の多様な主体が、サイバーセキュリティに関する事象発生前の疑いの段階においても、協議会に対し、これに関する連絡、相談等を気兼ねなく安心して行うことができるよう、運用において特に配慮するものとする。

第２章　構成員の加入等

（協議会の構成員）

第５条　協議会は、構成員をもって構成する。

（構成員の加入等）

第６条　構成員になろうとする者は、本規約に同意の上、運営委員会が定めるところにより、

運営委員会に対して入会の申込みを行い、運営委員会の承認を得たときに構成員となるものとする。何人も、自らの意に反して、入会の申込みを行うことを強要されることはない。

2　前項の申込みを行うことができる者は、次の各号のいずれにも該当する者（法人その他の団体又は個人を含む。）とする。

一　法第 17 条第２項各号に掲げる者（国の行政機関に関しては、府省に限るものではなく、庁、委員会等も含む。）

二　第３条に規定する協議会の目的及び第４条第１項に規定する活動内容に賛同する者

3　運営委員会は、第３条に規定する協議会の目的の達成又は第４条第 1 項に規定する協議会の活動に支障を生じるおそれがあると認める場合は、第１項の申込みを行った者に対して入会の承認をしない場合がある。この場合において、承認をしなかった理由等を開示することが我が国のサイバーセキュリティ確保に支障を生じるおそれがあると認められる場合等には、理由等を開示しないことがある。

4　次のいずれかに該当する加入構成員は、第 24 条に規定する 24 条タスクフォースに参加することができない。ただし、我が国におけるサイバーセキュリティの確保にとって特に重要な貢献をなす意欲及び能力並びに長年の我が国におけるサイバーセキュリティに関する官民の様々な公益的取組みへの積極的な協力の実績を有するものであり、かつ、協議会の事務に関して知り得た秘密の保持について高度の信頼をおくことができるものとして運営委員会が特別に承認したものについては、この限りでない。

一　日本の国籍を有しない人

二　外国政府又はその代表者

三　外国の法人又は団体

四　法人又は団体であって、第一号から第三号までに掲げる者（以下この号において「外国法人等」という。）がその議決権の過半数を有するものその他これに準ずる事情があると認められるもの（当該外国法人等が当該加入構成員の経営等を支配しているとは明らかに認められないものを除く。）

5　国の関係行政機関の長（当該国の関係行政機関の長が内閣総理大臣の場合にあっては、担当する部局の長）であって、政府機関横断構成員と連携する者は、構成員になろうとするときは、本規約に同意の上、運営委員会の定めるところにより、運営委員会に対して入会の通知を行い、運営委員会が当該通知を受領したときに、第１項に基づき運営委員会から承認されたものとみなす。

6　加入構成員は、協議会への入会にあたって、運営委員会が定めるところにより、当該加入構成員及びその受託者（再受託者等を含む。）の役職員（派遣労働者を含む。）であって、協議会の情報（法第 17 条第４項に基づく守秘義務の対象となる秘密情報に限る。）を取り扱う（取り扱う可能性がある場合を含む。）協議会事務従事者を全て登録しなければならない。

７　加入構成員は、協議会事務従事者に対し、必要性及び緊急性が生じた場合において当該協議会事務従事者の判断で協議会に対して情報提供及び相談を迅速に行う権限をあらかじめ付与するよう努めるものとする。

８　加入構成員は、第６項に規定する協議会事務従事者を変更しようとするときは、予め協議会事務局に対しその旨を届け出るものとする。ただし、予め届け出ることが困難である特別の理由がある場合は、協議会事務従事者の変更後速やかに協議会事務局に対し届け出るものとする。

第３章　構成員の脱退等

（協議会からの脱退）

第７条　加入構成員は、運営委員会が定めるところにより、事務局に対し退会の届出を行うことで、協議会を脱退することができる。

（加入構成員の除名）

第８条　運営委員会は、加入構成員（当該構成員の第６条第６項に規定する協議会事務従事者を含む。）が次の各号に掲げるいずれかの事由に該当すると認めた場合、運営委員全員の同意を得て、当該加入構成員を除名することができる。

一　法又は本規約その他協議会が定める規則等に違反した者

二　協議会もしくは構成員の名誉を傷つけ、または協議会の目的に反する行為をした者

三　法令又は公序良俗に違反した者

四　反社会的勢力や団体又はその関係者であると認められる者

五　協議会の目的と協調しがたい事業等に関与したと認められる者

六　その他除名すべき特別の理由があると認められる者

２　運営委員会は、構成員（当該構成員の協議会事務従事者及び当該構成員から第 22 条第２項又は第３項に基づき情報提供を受けた非構成員（当該非構成員の協議会事務従事者を含む。）を含む。）が次の各号に掲げるいずれかの事由に該当すると認めるときは、直ちに、運営委員会が定めるところにより、運営委員の４分の３以上の賛成をもって、当該構成員に対する情報共有等を制限することができる。

一　協議会の事務遂行上取得した情報を漏えいした疑いがあると認められる者

二　前項各号のいずれかに該当する疑いがあると認められる者

（構成員たる資格の喪失）

第９条　前条の場合のほか、加入構成員は、死亡し若しくは失踪宣告を受け又は解散したときは、その資格を喪失する。

第４章　協議会の運営等

（総会）

第 10 条　協議会は、原則として毎年、構成員による定時総会を開催するものとする。また、運営委員会が必要と認めるときは、臨時総会を開催することができる（以下、定時総会及び臨時総会をあわせて「総会」という。）。

２　総会においては、以下の事項を実施する。

一　本規約（別表１を除く。）又は第 18 条第６項に基づき規定する情報管理規定の改正の決議

二　本協議会の活動・運営に関する報告

三　運営委員会において総会に付議すべきものと決議した事項

３　総会の招集及び議事進行は、運営委員長が行う。

４　総会における議決権は、構成員１名につき１個とする。

５　総会は、すべての構成員の議決権の過半数を有する構成員の出席もしくは委任状の提出をもって成立する。

６　第２項のうち、議決が必要な事項については、総会に出席した構成員の過半数の賛成をもって成立するものとする。ただし、運営委員全員が反対した場合はこの限りではない。

７　総会は、必要に応じて、電子的手段により開催することができる。

（運営委員会）

第 11 条　協議会に運営委員会を置く。

２　運営委員会は、本部長等が法第 17 条第１項及び第２項に基づき、協議会を組織すること及び構成員を加えることができることに鑑み、別表１に掲げる本部長等を運営委員として構成する。なお、運営委員である国の関係行政機関の長において、当該行政機関自身のサイバーセキュリティの確保を担当する部局が第６条の規定に基づき協議会への入会を別に行うことは妨げない。

３　運営委員会は、協議会の運営上必要な事項として次に掲げる事項に関する業務を行う。ただし、政令指定法人 JPCERT/CC が行う構成員間の連絡調整に関すること及び 24 条タスクフォースの業務に関すること（第６条第４項に関することを除く。）を除く。

一　加入構成員の入会の承認及び退会申込みの受付に関すること

二　加入構成員の除名及び加入構成員たる資格の喪失に関すること

三　構成員に対する情報共有等の制限に関すること

四　第 23 条に基づく情報提供等協力の求めに関すること

五　本規約（別表１に限る。）の改正に関すること

六　前各号に定めるもののほか、協議会の組織及び運営に関すること

４　運営委員会は、前項の業務を行うにあたって必要があると認めるときは、政令指定法人

JPCERT/CC その他当該業務に関して十分な知識又は経験を有する者等の意見を聴くことができる。

5　運営委員会に、運営委員長を置き、サイバーセキュリティ戦略本部長をもって充てる。

6　運営委員会の定足数は運営委員の過半数とし、決議は、出席した運営委員の過半数をもって行うこととする。運営委員は、各１個の議決権を有するが、議決について特別の利害関係を有するときは、議決権を有しないものとする。

7　運営委員会は、必要に応じて、電子的手段により開催することができる。

8　運営委員長は、運営委員会の業務を総理し、運営委員会を招集する。

9　運営委員長は、協議会の目的及び活動に照らし必要があると認めるときは、第６項に基づく運営委員会の議決を拒否することができる。

10　前各項に定めるもののほか、運営委員会の運営及び手続に関し必要な事項は、運営委員会において定める。

（事務局）

第 12 条　協議会に事務局を置く。

2　事務局は、NISC 及び政令指定法人 JPCERT/CC が務める。

3　NISC 基本戦略第２グループは、事務局として、協議会の庶務を処理する。なお、NISC において基本戦略第２グループ以外のグループが第６条の規定に基づき協議会への入会を行うことは妨げない。

4　政令指定法人 JPCERT/CC は、第４条第１項第１号に基づく情報共有等を行うため、構成員を含む関係者間の連絡調整を行うものとする。

（準用）

第 13 条　第６条第６項から第８項までの規定については、本部長等たる構成員及び事務局に対して準用する。

第５章　情報共有システムの利用

（情報共有システムについて）

第 14 条　構成員（特定連携構成員を除く。）は、協議会における情報共有について協議会システムを利用することとし、当該システムの利用にあたり、当該システムに適用される利用規約を遵守しなければならない。

2　協議会システムの管理権限は、政令指定法人 JPCERT/CC が有する。管理権限を有する政令指定法人 JPCERT/CC に限り、第 17 条第１項及び第２項の規定にかかわらず、協議会システムにおける全ての投稿にアクセスすることができる。

3　協議会の庶務を処理する NISC 基本戦略第２グループは、協議会システムの利用者間

で発生した紛争等を裁定する必要がある場合、又は、協議会の庶務を処理する上で必要な場合に、当該目的を達成するために当該システムにおける必要最小限度の投稿にアクセスすることができる。この場合において、NISC 基本戦略第２グループは、運営委員会に付議すべき案件があると思料するときは、運営委員会に対し、必要最小限度の情報を提供することができる。

４　協議会における情報共有に当たって、本規約と第１項の利用規約との間に矛盾・抵触する規定がある場合は、本規約の規定が優先するものとする。

（早期警戒情報提供サービスについて）

第 15 条　構成員（特定連携構成員を除く。）は、構成員となったときに、併せて、早期警戒情報提供サービスの登録を受けたものとみなし、JPCERT/CC から早期警戒情報の提供を受けるものとする。ただし、当該構成員が構成員となるにあたって、運営委員会が定めるところにより別段の意思表示を行った場合はこの限りではない。

第６章　情報共有活動

（事務局と構成員との情報共有）

第 16 条　事務局は、JPCERT/CC から提供される情報、構成員から直接提供される情報、構成員以外の者から直接提供される情報を取り扱うこととする。

２　事務局は、構成員に対し、サイバーセキュリティの確保に資する情報を随時提供するものとする。

３　構成員は、事務局に対し、サイバーセキュリティの確保に資する情報を任意に提供することができる。構成員は、第４条第３項の規定の趣旨に鑑み、自組織内において収集・分析した情報のみでは情報システムの被害の内容・範囲を検知または認知するに至っておらず、平常時に比して直感的な違和感があるといった程度にとどまる早期・初動の時点においても、国内外における類似関連情報その他の有益な助言や情報を、専門的知見を有する政令指定法人 JPCERT/CC や他の構成員から得ることを目的として、事務局に対する相談に伴い、情報を提供することができる。

（情報の共有範囲の指定）

第 17 条　構成員は、事務局に対し任意に情報を提供するに際し、当該情報の共有範囲を指定することができる。事務局を含め、何人も、当該構成員の同意を得ることなく、当該共有範囲を超えて情報の共有を行ってはならない。

２　事務局は、構成員に対し情報を提供するに際し、当該情報の共有範囲を指定することができる。何人も、事務局の同意を得ることなく、当該共有範囲を超えて情報の共有を行っ

てはならない。

3　事務局は、前条第２項の規定に基づき提供する情報の中に、同条第３項の規定に基づき任意に提供された情報が含まれるときは、当該情報を提供した構成員の同意を得ることなく、第１項の規定に基づき当該構成員が指定した共有範囲を超えて、前項に規定する情報の共有範囲を指定してはならない。

（秘密の管理）

第 18 条　構成員は、事務局に対し任意に情報を提供するに際し、法第 17 条第４項に規定する秘密の有無を明示することとする。

2　事務局は、構成員に対し情報を提供するに際し、法第 17 条第４項に規定する秘密の範囲を明示することとする。

3　事務局は、法第 17 条第４項に規定する秘密を含む情報については、前条の規定に基づき指定する当該情報の共有範囲に、第６条第６項及び第８項（第 13 条に基づき準用する場合を含む。）の規定によりあらかじめ協議会事務従事者を登録した構成員以外の構成員を含めてはならない。

4　事務局及び構成員は、法第 17 条第４項に規定する秘密を含む情報を、第６条第６項及び第８項（第 13 条に基づき準用する場合を含む。）の規定によりあらかじめ協議会事務従事者として登録した者以外に取り扱わせてはならない。

5　構成員は、法第 17 条第４項に規定する秘密の受領を希望しない場合にあっては、運営委員会が定めるところにより、事務局に対し秘密の受領を拒否する旨届け出ることができる。

6　事務局及び構成員は、前各項に定めるもののほか、別途協議会が定める情報管理規定に基づき法第 17 条第４項に規定する秘密を取り扱うものとする。

（情報の利用の目的）

第 19 条　事務局は、協議会の事務を通じて知り得た情報を、第４条第１項に規定する協議会の活動目的以外の目的で利用してはならない。政令指定法人 JPCERT/CC は、協議会の事務を通じて知り得た情報を、協議会とは別の事業（早期警戒情報提供サービスを除く。）の活動目的で利用してはならない。

2　構成員は、協議会の事務を通じて知り得た情報を、自らのサイバーセキュリティを確保する目的以外の目的で利用してはならない。第 16 条第３項の規定に基づき情報を提供する構成員は、自ら任意に提供する情報が自ら又は情報の原提供者に対する犯罪捜査、行政処分、行政調査又は行政指導のために用いられるおそれがあると思料するときは、該当する捜査機関、監督官庁等を、第 17 条第１項の規定に基づき指定する情報の共有範囲からあらかじめ除外することができる。

3　構成員は、前項の規定にかかわらず、第 17 条に規定する情報の共有範囲が指定されて

いない情報について、普及啓発の目的で利用することができる。

４　複数の組織間の共助等を目的とする非営利の法人その他の団体である構成員は、第２項の規定にかかわらず、協議会の事務を通じて知り得た情報を、法第 17 条第４項に規定する守秘義務に反しない範囲で、かつ、第 17 条に規定する情報の共有範囲の指定の範囲で、当該法人その他の団体が共助等の対象とする組織（法第 17 条第２項第１号、第２号、第３号又は第５号に該当する者に限る。）のサイバーセキュリティを確保する目的で利用することができる。

（事務局を介さない情報共有）

第 20 条　構成員が協議会の事務の一環として他の構成員との間で情報の共有を行おうとするときは、事務局を通じて行うこととし、構成員の間における直接の情報共有は、特別の理由がある場合に限って行うこととする。この場合において、第 16 条から第 19 条までの規定（第 16 条第１項及び第２項、第 17 条第２項及び第３項、第 18 条第２項及び第３項並びに第 19 条第１項を除く。）は、構成員の間における直接の情報共有について準用する。

（特定連携構成員との情報共有）

第 21 条　特定連携構成員は、協議会の事務の一環として事務局又は他の構成員との間で情報の共有を行おうとするときは、政府機関横断構成員を経由してこれを行うものとする。

（非構成員との情報共有）

第 22 条　第 16 条第３項の規定は、構成員以外の者（以下「非構成員」という。）について準用する。この場合において、第 17 条から第 19 条までの規定は、非構成員から事務局に対し任意に提供された情報の取り扱いについて準用する。

２　事務局は、第 19 条第４項の規定に基づき非構成員のサイバーセキュリティを確保する必要がある場合その他構成員を介して非構成員に対して情報を提供する必要があると認める場合には、法第 17 条第４項に規定する守秘義務に反しない範囲で、第 17 条第２項に規定する情報の共有範囲に、当該非構成員を追加することができる。

３　事務局は、第 19 条第４項の規定に基づき非構成員のサイバーセキュリティを確保する必要がある場合その他構成員を介して非構成員に対して情報を提供する必要があると認める場合であり、かつ、当該非構成員に対し法第 17 条第４項に規定する秘密を含む情報を提供する緊急の必要があると認めるときは、第 18 条第３項及び第４項の規定にかかわらず、第 17 条第２項に規定する情報の共有範囲に、当該非構成員を追加することができる。なお、当該追加を行った場合には、当該非構成員は、当該情報を取り扱った協議会事務従事者を当該構成員を介して全て事務局に事後すみやかに届け出るものとし、事務局は、当該非構成員に情報を提供するにあたって、当該届出が必要となる旨を当該構成員を

介して予め通知するものとする。また、当該非構成員は、届け出た協議会事務従事者以外の者に当該情報を取り扱わせてはならない。

4　第 17 条第３項（第１項の規定により準用する場合を含む。）の規定は、第２項又は前項の規定に基づき事務局が情報の共有範囲の追加を行う場合における当該情報の中に第 17 条第１項（第１項の規定により準用する場合を含む。）の規定に基づき任意に提供された情報が含まれる場合について準用する。

5　第 17 条第２項及び第 19 条第２項から第４項までの規定は、第２項の規定により事務局から情報の提供を受けた非構成員について準用する。

6　第 17 条第２項、第 18 条第６項並びに第 19 条第２項及び第４項の規定は、第３項の規定により事務局から情報の提供を受けた非構成員について準用する。

第７章　情報提供等協力の求め

（協議会からの協力の求め）

第 23 条　協議会は、次の各号に掲げる場合に限り、構成員に対して、法第 17 条第３項に基づく情報提供等の協力の求めを行うものとする。

一　大規模なサイバー攻撃が発生するなど、情報提供等の協力を求める特別の必要性が認められる場合又はこれに準ずる状況であると認められる場合

二　構成員にとって協議会による求めがなければ提供することができない情報を提供する場合であって、当該構成員が協議会による協力の求めを受けることについて同意している場合

2　協議会は、前項の規定に基づき情報提供等の協力の求めを行うにあたっては、必要に応じて、当該協力の求めの目的及び当該求めに基づき取得した情報の共有範囲を明示するものとする。

第８章　タスクフォースに関する特則

（タスクフォース）

第 24 条　協議会に、24 条タスクフォース（以下「タスクフォース」という。）を置く。

2　タスクフォースは、政令指定法人 JPCERT/CC 及び次項に基づき追加された者をもって構成する。

3　タスクフォースは、第４条第１項第１号及び同項第２号に規定する活動に積極的に貢献する意欲と能力を有する者として承認した者をタスクフォースに加えることができる。何人も、自らの意に反して、当該承認の申込みを行うことを強要されることはない。

4　タスクフォースを構成する者（タスクフォースが定める要件に該当する者に限る。）は、第 19 条第１項及び同条第２項の規定にかかわらず、タスクフォースが定めるところによ

り、タスクフォースの事務の遂行上取得した情報について、法第 17 条第４項に規定する守秘義務に反しない範囲で、第三者のサイバーセキュリティ確保のために用いることができる。

５　タスクフォースの組織及び運営に関することは、タスクフォースにおいて定める。タスクフォースは、タスクフォースを構成する者に対してのみ適用されるものに限り、本規約の特則を設けることができる。当該特則は、タスクフォースを構成する者以外の構成員に対しては効力を生じない。

第９章　雑則

（構成員の公表）

第 25 条　協議会は、運営委員会が定めるところにより、本規約及び構成員の名簿を公表するものとする。この場合において、協議会は、公表を望まない加入構成員の名称等を、当該公表する名簿に記載してはならない。

（サイバーセキュリティ戦略本部との連携）

第 26 条　協議会は、必要があると認めるときは、我が国のサイバーセキュリティ確保に関する事項について、サイバーセキュリティ戦略本部との連携を図るものとする。

（協議会における議事等について）

第 27 条　総会、運営委員会及びタスクフォースの議事は原則非公開とする。

２　構成員の間で共有される情報のうち、情報共有の範囲が指定されているものについては、非公開とする。

（免責）

第 28 条　協議会及び構成員は、協議会の活動として提供した情報の正確性を保証しないものとする。

２　協議会及び構成員は、協議会の活動として提供した情報に基づき、情報提供者以外の者に損害が発生したとしても、当該損害について一切の法的責任を負わないものとする。ただし、故意又は重過失による場合はこの限りではない。

３　政令指定法人 JPCERT/CC は、協議会システムの利用又は協議会システムの利用の停止、休止、中断、制限若しくは通信回線の障害等によりシステムを利用した構成員又は他の第三者が被った損害について一切の法的責任を負わないものとする。

（違反に関する報告）

第 29 条　構成員は、協議会において取り扱われる情報の漏えい、共有範囲の逸脱、目的外

利用をはじめとする法令、本規約その他関係規則の違反があると思料するときは、NISC基本戦略第２グループに対してその旨連絡することができる。

（個人情報の取扱い）

第 30 条　協議会の庶務を処理するにあたって NISC が取得する個人情報（行政機関の保有する個人情報の保護に関する法律第２条第２項に規定する個人情報をいう。）の取扱いに関しては、別途 NISC が定めるプライバシーポリシーに従うものとする。

附　則

１　この規約は、平成 31 年４月１日から施行する。

２　平成 33 年４月１日までの協議会への入会申込みについては、運営委員会が定めるところにより、運営委員会が定める期間に限って協議会への入会申込みの募集を実施することとし、構成員になろうとする者は、当該期間中に限り、入会の申込みを行うことができるものとする。この場合において、運営委員会は、当該期間を、あらかじめ運営委員会の定めるところにより公表しなければならない。

別表１　運営委員一覧

サイバーセキュリティ戦略本部長（内閣官房長官）
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
国家公安委員会委員長
総務大臣
外務大臣
経済産業大臣
防衛大臣
情報通信技術（ＩＴ）政策担当大臣
東京オリンピック・パラリンピック競技大会担当大臣

資料１０－５

24 条タスクフォース規則

平成 31 年４月１日　24 条タスクフォース決定

（タスクフォース参加者の区分）

第１条　24 条タスクフォース（以下「タスクフォース」という。）に参加する者は、政令指定法人 JPCERT/CC のほか、第一類構成員及び第二類構成員の２つの区分により構成する。

一　第一類構成員　構成員のうち、他の情報共有体制に参加又は運営する主体であって、サイバーセキュリティ協議会規約（以下「規約」という。）第４条第１項第１号及び同項第２号に定める活動に積極的に貢献する能力と意欲を有する者として、サイバーセキュリティの確保に資する情報を積極的に提供することができる者

二　第二類構成員　構成員のうち、第一類構成員等（政令指定法人 JPCERT/CC 及び第一類構成員をいう。以下同じ。）から提供される情報に対し一定の応答を行うことができる能力と意欲を有する者

（タスクフォースの業務）

第２条　タスクフォースは、規約第４条第１項第１号及び同項第２号に掲げる協議会の活動として、サイバーセキュリティに関する脅威情報等の積極的な共有及び分析を行い、我が国のサイバーセキュリティを確保するために必要な情報の作出及び共有を積極的に行うものとする。

２　前項に規定するものの他、タスクフォースの運営に関する事項は、別途タスクフォースにおいて定める。

（地位の取得）

第３条　第一類構成員又は第二類構成員になろうとする構成員は、別途タスクフォースが定めるところにより、タスクフォースに対して申込みを行い、タスクフォースの承認を得たときに第一類構成員又は第二類構成員となるものとする。

（情報提供等の協力の求め）

第４条　協議会は、規約第 23 条第１項の規定にかかわらず、第一類構成員又は第二類構成員に対して情報提供等の協力を求める必要があると認められる場合には、別途タスクフォースが定めるところにより、法第 17 条第３項に基づく情報提供等の協力の求めを行うものとする。

（情報提供の範囲に関する留意事項）

第５条　タスクフォース参加者は、タスクフォースが高度な信頼関係に基づき機微性の高い情報をタスクフォースの中で共有することに鑑み、タスクフォース参加者以外の構成員にとって不要な情報を当該構成員に対し提供しないよう留意しなければならない。

（第一類グループ）

第６条　タスクフォースに、第一類グループを置く。

２　第一類グループは、第一類構成員等をもって構成する。

３　第一類グループによる情報の提供に関することその他第一類グループの運営に関することは、第一類グループが定める。

（情報提供等の協力の求め）

第７条　協議会は、規約第 23 条第１項の規定にかかわらず、第一類構成員に対して情報提供等の協力を求める必要があると認められる場合には、別途第一類グループが定めるところにより、法第 17 条第３項に基づく情報提供等の協力の求めを行うものとする。

（規約第 24 条に基づきタスクフォースが定める要件）

第８条　規約第 24 条第４項に規定するタスクフォースが定める要件は、第一類構成員等であることとする。

（タスクフォース等の庶務）

第９条　タスクフォース及び第一類グループの庶務は、NISC 基本戦略第２グループが務める。この場合において、NISC 基本戦略第２グループは、規約第 12 条第３項及び規約第 14 条第３項の規定の適用を除外されるものではない。