サイバーセキュリティ協議会 Q&A(Ver1.1)

2020 年 12 月 1 日
2021 年３月 31 日一部改正

内閣官房内閣サイバーセキュリティセンター
政令指定法人 JPCERT コーディネーションセンター

【目次】

Q20. どのような場合に情報提供等の協力が求められるのか。

５．情報の共有範囲について

Q21. TLP（Traffic Light Protocol）でREDが付された情報は、秘密を含む情報に該当するのか。

Q22. どのような情報が秘密として指定されるのか。

Q23. 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が、共助等の対象とする組織（ISAC会員、セプター構成員等）に対して協議会からの情報を展開してもよいか。

６．協議会への相談について

Q24. サイバーセキュリティ協議会は、協議会構成員だけでなく、非構成員からの相談や情報提供等も受け付けているとのことであるが、どのように相談等すればよいのか。

１．協議会への入会について

Q1.　協議会ではどういったことを行っているのか。
サイバーセキュリティ協議会は、サイバーセキュリティ基本法第 17 条に基づき、2019 年４月に組織された法定の情報共有体制です。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や教育研究機関など官民の多様な主体が相互に連携し、より早期の段階で、対策情報等を迅速に共有することにより、サイバー攻撃による被害の拡大を防ぐことなどを目的としています。 例えば、時々の話題やイベントに乗じた標的型攻撃が疑われるような事象について、その確証が得られない段階から取り扱い、確認や予防に資するような対策情報として協議会構成員等に共有する活動を行っています。 また、具体的な被害が発生していなくても、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、罰則により担保された守秘義務の下、安心して情報提供や相談を行うことが可能です。情報提供いただいた場合には、協議会から対策手法の助言や周辺状況等のフィードバックが得られます。 本協議会の詳しい資料や運用ルール（規約）等は、内閣官房内閣サイバーセキュリティセンター（NISC）のウェブサイトの協議会ページ https://www.nisc.go.jp/conference/cs/kyogikai/index.html に掲載していますので、そちらをご参照ください。
Q2.　協議会への入会の申込みはいつでも受け付けているのか。
協議会への入会の申込みは、運営委員会において定める募集期間に限って受け付けています。募集時期については、社内決裁などお時間を要することなどを踏まえ、事前に次回の募集時期の目安等も含め NISC のウェブサイトの協議会ページ https://www.nisc.go.jp/conference/cs/kyogikai/index.html に掲載することとしていますので、そちらをご参照ください。

Q3.　一般の構成員として協議会に加入したいが、どのようにすればよいか。

サイバーセキュリティ協議会の募集期間内に、協議会への入会のお申込みを行っていただき、運営委員会において加入が承認された場合には、一般の構成員として入会いただくことになります。

具体的には、NISC のウェブサイトの協議会ページに掲載されています「サイバーセキュリティ協議会加入申込書（申込み事項変更届）」に必要事項を記載の上、協議会事務局（NISC）の kyogikai-shomu@nisc.go.jp 宛てに電子メールでご送付ください。

また、協議会から秘密を含む情報の受信を希望する場合には、上記加入申込書と併せて、秘密を含む情報を取り扱う可能性がある方等を「サイバーセキュリティ協議会事務従事者登録届」に記載の上、上記宛先まで電子メールでご送付ください。

この点、本加入申込書又は事務従事者登録届を提出するにあたっては、以下の点にご留意ください。

① ファイル名を以下のとおり変更してください。

- 加入申込書

[yymmdd（提出年月日：西暦下 2 桁、月日各 2 桁）]_協議会加入申込書（組織・団体名）

（例）201201_協議会加入申込書（○○株式会社）

- 事務従事者登録届

[yymmdd（提出年月日：西暦下 2 桁、月日各 2 桁）]_事務従事者登録届（組織・団体名）

（例）201201_事務従事者登録届（○○株式会社）

② PDF 形式等に変換せず、Word 形式のままご提出ください。

③ 暗号化の措置を行った上でご提出ください。パスワードについては、メールではなく、お電話等でお知らせください。

なお、タスクフォース第一類構成員又は第二類構成員としての参加を希望される場合には、別途、事務局（NISC）までご連絡をお願いします。

Q4.　中小企業や法人格を持たない団体でも協議会への入会の申込みを行うことは可能か。

可能です。ただし、組織に属さない個人の方からのお申込みは想定していません。

Q5.　組織全体ではなく組織内の一つの部署で、協議会への入会の申込みを行うことは可能か。

可能です。ただし、複数の部署それぞれからのお申込みは想定していません。

Q6.　協議会への入会にあたり、入会費、年会費などは発生するのか。

入会費、年会費などの会費は発生しません。

Q7.　協議会システムの ID 発行の連絡は、どのような形でくるのか。

一般の構成員については、ご登録いただいた POC（point of contact）の方宛てに協議会システムの利用者全員分の ID 等がまとめて通知されます。POC の方から各システム利用者にご案内ください。

タスクフォース構成員については、システム利用者に対して個別に通知が行われます。

ご不明な点等ございましたら、協議会事務局（JPCERT/CC）の csc-sec@jpcert.or.jp までお問い合わせください。

２．加入申込書及び事務従事者登録届について

Q8.　「サイバーセキュリティ協議会加入申込書（申込み事項変更届）」の３（２）で、秘密を含む情報の受信を希望しない場合、「サイバーセキュリティ協議会事務従事者登録届」の提出は不要か。

秘密を含む情報が共有されませんので、お見込みのとおり、「サイバーセキュリティ協議会事務従事者登録届」をご提出いただく必要はありません。

Q9.　「サイバーセキュリティ協議会加入申込書（申込み事項変更届）」の３（３）の「早期警戒情報提供サービス」と協議会における情報共有はどのような関係にあるのか。

協議会からの情報は、本来はできるだけ多くの関係組織に共有・活用されることが望ましいとの考えに立ち、情報は広く公開されるか、又は早期警戒情報提供サービスを中心に他の情報共有体制において共有されます（ただし、秘密を含む情報や機微な情報は協議会システムでのみ共有されます。）。そのため、早期警戒情報提供サービスの新規登録を希望されない場合、協議会から共有される情報の一部を受け取ることができなくなる可能性があります。

Q10.　「サイバーセキュリティ協議会加入申込書（申込み事項変更届）」の４（１）の「担当者代表（POC）」について、どのような役職の者を登録する必要があるか。

協議会に参加される組織の業態や規模等によって、ご登録いただく方も異なることから、役職の指定などは設けていません。そのため、担当者代表（POC）のご登録にあたっては、協議会システム上の組織の担当者代表として、また、協議会事務局からご連絡を行う際の窓口となる方をご登録ください。

協議会から秘密を含む情報を受信することを希望する場合には、POC の方について「サイバーセキュリティ協議会事務従事者登録届」においてもご登録いただくとともに、（10）の「POC としての登録」欄には「する」にチェックを入れてください。POC として登録していない方は、「しない」にチェックを入れてください。

Q11. 登録事務従事者について、どのような役職の者を登録する必要があるか。

協議会に参加される組織の業態や規模等によって、ご登録いただく方も異なることから、役職の指定などは設けていません。そのため、登録事務従事者のご登録にあたっては、協議会において秘密を含む情報を取り扱う可能性がある方をご登録ください。

Q12.　「サイバーセキュリティ協議会事務従事者登録届」（７）の「電子メール」欄について、メーリングリストを登録することは可能か。

サイバーセキュリティ基本法（平成 26 年法律第 104 号）第 17 条第４項に基づく守秘義務の対象となる秘密を含む情報を取り扱う可能性がある方については、個別にご登録いただいているところ、メーリングリストでは外形的に誰が受信しているかが特定できないため、メーリングリストの登録はご遠慮ください。

Q13. 上司として報告を受けるなど、秘密を含む情報を取り扱う可能性はあるが、協議会システムを通じた受信を希望しない場合は、どのようにすればよいか。

秘密を含む情報を取り扱う可能性はあるものの、協議会システムを通じた受信を希望しない方については、「サイバーセキュリティ協議会事務従事者登録届」に氏名等を記載の上、（９）「協議会システム登録」欄の「不要」にチェックを入れてください。

Q14. 登録事務従事者は、変更することは可能か。

登録事務従事者の変更登録は、随時、承っております。変更内容を「サイバーセキュリティ協議会事務従事者登録届」に記載の上、協議会事務局（NISC）の kyogikai-shomu@nisc.go.jp 宛てに電子メールでご送付ください。本事務従事者登録届を提出するにあたっては、以下の点にご留意ください。

① ファイル名を以下のとおり変更してください。

[yymmdd（提出年月日：西暦下 2 桁、月日各 2 桁）]_事務従事者登録届（組織・団体名）

（例）201201_事務従事者登録届（○○株式会社）

② PDF 形式等に変換せず、Word 形式のままご提出ください。

③ 暗号化の措置を行った上でご提出ください。パスワードについては、メールではなく、お電話等でお知らせください。

なお、登録の申請から実際の協議会システムへの登録までは約５営業日ほどいただいております。

Q15. 例えば、登録事務従事者のうち１人の者の登録を外し、新たに１人の者を追加する場合、どのように記載すればよいか。

前回、ご提出いただいた「サイバーセキュリティ協議会事務従事者登録届」のうち、登録事務従事者として引き続きご登録いただく方の記載は残したままにしていただき、記載内容に変更等があれば修正の上、「（８）申請区分」欄の「継続」にチェックを入れてください。

登録を外す方については、「（８）申請区分」欄の「廃止」にチェックを入れてください。

新たに登録する方については、登録欄を追加し、氏名等の必要事項を記載の上、「（８）申請区分」欄の「新規」にチェックを入れてください。

なお、次回以降の登録事務従事者の変更の際には、前回、「廃止」にチェックを入れていただいた方の登録欄は削除願います。

３． 協議会構成員名簿の公開について

Q16. 協議会構成員の名簿を公開するとあるが、どの範囲まで公開されるのか。

NISC のウェブサイト上に公開される協議会構成員名簿には、組織・団体名の名称のほか、区分、分野やタスクフォースへの参加の有無（第一類構成員、第二類構成員、一般の構成員のいずれに該当するか）が記載されます。本名簿については、NISC のウェブサイトの協議会ページ https://www.nisc.go.jp/conference/cs/kyogikai/index.html の「サイバーセキュリティ協議会構成員名簿」をご参照ください。

上記公開する協議会構成員名簿への登載は任意であり、協議会への入会の申込時に、登載の是非を選択することが可能です。なお、「サイバーセキュリティ協議会事務従事者登録届」にて個別にご登録いただいた登録事務従事者等の個人の氏名等の個人情報は公開されません。

Q17. 協議会構成員であることを自社のウェブサイトで周知することは可能か。

可能です。協議会構成員であることを自社のウェブサイトで周知する際の記載例としては、以下のようなものが挙げられますので、参考になさってください。

【記載例（プレスリリース等）】

・20××年〇月△日に、サイバーセキュリティ協議会の構成員として加入することとなりましたので、お知らせいたします。

【記載例（組織紹介等）】

・当社はサイバーセキュリティ協議会の構成員として、協議会の活動に参加しています。

※なお、例えば、「内閣サイバーセキュリティ協議会（NISC）」といった記載は、誤りですので、ご注意ください。

４． 協議会の運用について

Q18. 総会は実際に集まって開催されるのか。

全ての構成員から構成される総会については、実際にお集まりいただくことを想定しておらず、電子的な開催となります。

Q19. どの位の頻度で対策情報等が共有されるのか。

対策情報等の共有の頻度については、サイバー攻撃の動向や脅威の深刻さなどの影響を受けることから、一概にお答えすることは困難ですが、協議会は、他の情報共有体制で既に共有されている情報を重ねて共有することを想定しておらず、真に有益で、他では得られない情報に絞り込んで共有を行っています。そのため、現時点では大量の情報を機械的に共有するような活動は行っていません。

ご参考までに、2020 年３月末時点で、協議会に持ち込まれた攻撃活動の件数は 46 件でした。そのうち、対策情報等を広く公開等するに至ったものは 13 件でした。

Q20. どのような場合に情報提供等の協力が求められるのか。
協議会がサイバーセキュリティ基本法第 17 条第３項に基づく情報提供等の協力の求めを行う場合は、大規模なサイバー攻撃が発生した場合や協議会構成員自身が情報提供等の協力の求めを受けることに同意している場合等に限定されています（サイバーセキュリティ協議会規約第 23 条第１項）。情報提供等の協力の求めを行う場合には、依頼に際してその旨を明記します。 大規模なサイバー攻撃としては、2017 年 5 月に発生したランサムウェア「WannaCry」のようなケースを想定しています。大規模なサイバー攻撃の発生時には事態が急速に展開する状況も予想されますので、ご協力をお願いします。 なお、通常の情報共有に際しても、任意でのフィードバックを依頼する場合がありますが、情報提供を行うかどうかは各構成員のご判断となります。

５． 情報の共有範囲について

Q21. TLP（Traffic Light Protocol）で RED が付された情報は、秘密を含む情報に該当するのか。
TLP は情報の共有範囲を視覚的に分かりやすい形で付与したもので、秘密を含む情報か否かとは別の観点の分類です。TLP が RED であり、当該情報の共有範囲が協議会事務従事者（当該構成員に係る登録事務従事者を含む。）に限られる場合、通常は秘密を含む情報であると想定されますが、場合によっては、秘密を含まない機微な情報ということもありえます。協議会から共有される情報には、秘密の有無を明示することとしていますので、そちらをご参照ください。
Q22. どのような情報が秘密として指定されるのか。
情報提供者の要望、協議会の規約・情報管理規程やタスクフォース構成員等の見解などを総合的に勘案し、協議会事務局（JPCERT/CC）において秘密指定の要不要を検討し、情報提供者との合意のもと判断します。 なお、一般的に、あるいは個別の契約や法律等により守秘が求められる情報については、協議会の判断に関係なく適切に扱ってください。
Q23. 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が、共助等の対象とする組織（ISAC 会員、セプター構成員等）に対して協議会からの情報を展開してもよいか。
協議会から情報を共有するにあたっては、情報の共有範囲が指定され、TLP を付与することとなりますので、本共有範囲をご確認願います。共助等対象組織に対して共有することが可能な場合であっても、共助等対象組織は、国の関係行政機関、地方公共団体又はその組織する団体、重要社会基盤事業者又はその組織する団体、大学その他の教育研究機関又はその組織する団体に限られていますので、ご留意願います。この点、該当する情報共有に際しては、その旨を共有範囲として明記しますので、ご確認ください。 なお、協議会構成員からの任意のフィードバックなどを踏まえ、改めて共有範囲等が見直される場合もありますので、情報の共有範囲についてご不明な点等ありましたら、協議会事務局（JPCERT/CC）までお問い合わせ願います。

６． 協議会への相談について

Q24. サイバーセキュリティ協議会は、協議会構成員だけでなく、非構成員からの相談や情報提供等も受け付けているとのことであるが、どのように相談等すればよいのか。

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いなくても、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）

【お電話】

■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。

協議会にご相談・情報提供していただくにあたり、以下の点を事前にご確認ください。

確認①：秘密指定の有無

（例：被害組織名又は被害内容は秘密に指定してほしいなど）

確認②：情報の共有範囲の設定

（例：タスクフォース第一類グループ限り、協議会構成員限りなど）

確認③：協議会事務局外への対応調整の要否

（例：協議会構成員において同様の報告がないか確認してほしい、不審メールの送信元に通知してほしいなど）

※ご連絡いただいた際には、上記確認事項を含めて幾つか質問させていただきますので、お含みおき願います。

なお、協議会へのご相談・情報提供いただくにあたっては、NISC のウェブサイトの協議会ページ https://www.nisc.go.jp/conference/cs/kyogikai/index.html の「サイバーセキュリティ協議会へのご相談・情報提供」も併せてご参照ください。