攻撃技術情報の取扱い・活用手引き（案）及び、秘密保持契約に盛り込むべき攻撃技術情報等の取扱いに関するモデル条文案に寄せられた御意見及び御意見に対する考え方

No.	提出者			該当箇所	御意見	ご意見に対する考え方
	提出者番号	枝番	組織・個人			
1	1	1	個人	手引き	・８５ページの４行目「おこなわれた」と、８６ページの枠外の３行目「行われた」とは、どちらかに字句を統一したほうがよい。 ・８６ページの枠外の９行目「タイミグ」とは何か？ ・６ページの表に表頭、表側を記載したほうがよい。 ・８ページのベンダの定義の文末に句点を記載したほうがよい。 ・４４ページの４行目「すでに」と、４７ページの２行目「既に」とは、どちらかに字句を統一したほうがよい。	御意見のとおり、当該箇所を修正いたします。
2	2	1	-		モデル条文を経産省が示してくれることは非常に有用であり賛意を表明します。	本案に対する肯定的な御意見として承ります。
3	3	1	個人		1.「専門組織を通じた速やかな情報共有」に関して、非常に良い考え方で基本は賛成します。その上で、善意な専門組織を考慮すれば問題ないとは思いますが、悪意のある(専門)組織を想定した場合は、被害のあった乙の意向なしに、情報が漏洩する可能性をもう少し低くしておく必要があるのではないかと考えます。例えば、情報共有等にあたるものを唯一の情報セキュリティの国家資格である情報処理安全確保支援士の指示のもとだけに限るといいのではないかと考えます。昨今、情報セキュリティが社会問題化されており、多くのいろいろな専門組織、専門家だと名乗る場合が多くなり、場合によっては能力、知識、経験が十分ではないとか、さらには悪意を持っている場合もある。情報処理安全確保支援士でもいろいろな知識、経験のレベルはありますが、倫理を学び、最低限の知識を持っていることを国が認めている資格なのでいいのではないかと考えます。	今後の検討の参考にいたします。
4	3	2	個人		2.ドキュメントの体裁 今回、91ページのドキュメントをPDFで提供されています。せめて、PDFで提供するにしても"しおり付きPDF"にしてデジタルでの可読性を高めた提供がいいのではないかと思います。またはdocx, pptx,xlsxでの提供で、案といいつつ各組織で活用(各組織内で引用してその組織にあった資料にする)しやすくするとかを考慮してもいいのではないかと考えます。 さらに、章番号を記載することにより、他の文書からの引用、参照がより容易で明確に実施可能になると考えます。 また、図には、図番号とタイトルを記載すべきだと考えます。	御意見を踏まえ修正いたします。 また、しおり付きのPDF形式で公開予定です。
5	3	3	個人	モデル条文案	3.「甲を識別及び特定できないように加工した攻撃技術情報」としていますが、甲のレピュテーションは重要ではありますが、それだけではないと思います。甲の顧客の情報及びレピュテーションも十分考慮して、契約に含める必要があると考えます。例えば、情報に個人のクレジットカード情報、要配慮個人情報が含まれていて、かつ、その情報が攻撃の特徴を表しているとき、その情報の開示に関しての責任は十分注意する必要があると考えます。	本手引き及びモデル条文案では、通信先やマルウェア情報等攻撃者による攻撃手法やその痕跡を示す攻撃技術情報を、専門組織間の情報共有の対象としており、個人のクレジットカード情報等の被害者に関する情報は対象としておりません。
6	3	4	個人		4. 契約条文案「３．乙は、第１項及び第２項の攻撃技術情報等の利用又は開示に関連して、甲に生じた損害については一切の法的責任を負わないこととする。ただし、乙に故意又は重過失がある場合は、この限りでない。」としています。乙が情報共有を躊躇しないためには良いのですが、元の被害を受けた甲が、乙の故意、重過失以外の場合にさらなる被害を受ける可能性が否定できないのかと思います。このような場合、乙の情報共有を躊躇しないで、甲のさらなる被害の可能性を減らすために、国としてこの部分に何かしらの補償制度を設ける必要があるのではないかと考えます。	今後の検討の参考にいたします。
7	3	5	個人		5. P7 インディケータ情報／IoC(Indicator of Compromise：侵害指標)の用語の定義において、「ＩＰアドレス」や「ドメイン名」、「通信プロトコル／ポート番号」や「通信の発生日時」などで助詞の「や」が使われている。助詞の「や」は、「及び」「又は」又は「及び/又は」のどれを示すのか不明確になるので、日本産業規格(JIS)では、使用禁止になっている。本書はJISではないですが、用語の定義など、より厳格さが求められる記載では避けたほうが望ましいかと思います。	御意見を踏まえ修正いたします。

8	3	6	個人		6. P11　誤記 「dequate Timing （適切なタイミングで提供されること）」となって最初の“A”が欠落。 8. P39　誤記？ 　図の中にBが2つある。図の左側のB、C、Dは、C、D、Eの間違いでは。 9. P45 誤記？ 「他方で、最低限の正確性の担保、特に誤情報のコンタミネーションを避けるためには、30頁の解説のとおりですが、特に通信先情報については、以下の配慮が必要です。」と記載されていますが、30頁ではなく31頁の間違いでは。特に頁を指定した参照は、文書を更新された場合にずれる場合が多く、章、節の番号を適切に記載してそれを用いた参照にすべき。 10 P74 誤記？　ポイント囲み内 「初動対後も攻撃者が侵入したままで」の「初動対後」は「初動対応後」の間違いでは。 11 P86 誤記？ 「同タイミグで類似の事案の対応を？」の「タイミグ」は「タイミング」の誤記かと思われます。 12 P14 誤記？ 「？主に四つがあります。？(A+D)？」と記載されていますが、その下にはA？Eの5つがリストされています。	御意見のとおり、当該箇所を修正いたします。
9	3	7	個人		7.　本書は、被害組織ではなく、その対応にあたる専門組織がその他の専門組織との情報共有を躊躇せず実施するためのガイドライン、契約条文案だと認識しています。その専門組織が共有することにより、自身の専門組織及び/又は被害組織が得られるメリットをもっと明記したほうがいいのではないかと考えます。さらに、その専門組織が共有した情報をどのように他の専門組織が活用できるかも記載すべきかと考えます。これらの記載により、被害組織及びその対応する専門組織が、より情報共有に理解が進むものと考えます。 特に専門組織が情報共有する場の法律上の位置付け、ガイドライン等を整備する必要があるのではないかと思います。国で実施する点、民間で実施する場合等など。つまり24ページ以降に記載しているものに対して、どのような法的な建付けなのかを明確に記載すべき。これが明確でないと、契約で被害組織の被害に関する攻撃技術情報をどこに開示されるかが不明確になる。	本手引き及びモデル条文案は、専門組織による自主的な情報共有の促進を対象としております。お寄せいただいた御意見も参考に、修正いたします。
10	3	8	個人		13. 本書において、情報共有組織において、被害組織との秘密保持契約上の取扱いに関してのモデル条文案が提示されています。それ以外の情報共有の際に気をつけるべき法とその考え方などの整理を検討、公表していただけるといいのかと思いました。例えば、独占禁止法上、不正競争防止法、電気通信事業法、著作権法など。さらに、今回、公表されたモデル条文案を使用した場合に、さらに秘密保持契約及び/又は不正競争防止法上で何をした場合に違反となるかなども記載していただくといいかと思います。	その他情報の開示や共有において留意すべき法令等においては、サイバー攻撃被害に係る情報の共有・公表ガイダンスや内閣官房内閣サイバーセキュリティセンター（ＮＩＳＣ）が公表している「サイバーセキュリティ関係法令 Q&Aハンドブック Ver2.0」をご参照ください。 サイバー攻撃被害に係る情報の共有・公表ガイダンス： https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf サイバーセキュリティ関係法令 Q&Aハンドブック Ver2.0： https://security-portal.nisc.go.jp/guidance/pdf/law_handbook/law_handbook_2.pdf
11	4	1	個人		議論の前提として脆弱性の悪用による被害やマルウェア感染による被害になっていると理解しています。 それ以外のいわゆるサイバー犯罪 (Cyber Crime)に関する情報共有についても今後議論をお願いしたいです。 例えば、不審なクレジットカード番号や電話番号の共有を想定しています。EC事業者はチャージバックなどの作業から第3者が悪用したと思われる不審なクレジットカード番号やその会員情報を把握していると思います。また電話番号も最近はSMS代行を謳っている電話番号もあり、そのような電話番号での下院登録は不正利用の可能性を考えなければならないと思われます。 このような不審なクレジットカード番号や電話番号のDBは各会社で持っている可能性があり、このDBを何かの枠組みの中でゼロ知識証明などの仕組みを使って照会できる仕組みを議論できると良いと思います。	今後の検討の参考にいたします。
12	5	1	-		サイバー空間が国家安全保障で取り扱われる現在において、国家安全保障視点での攻撃者情報の扱いへの言及が少ないように感じられる。 特に、中露朝イと想定されるようなサイバー攻撃などについては、政府の判断で情報が利活用されるべきで、民間主導ではない立場を明確にしないと、他国との関係においても問題を生じるのではないか？（例えば、政府の戦略的立場を無視して、被害組織が個別に独自の考えで被害情報を出したり、被害組織を支援した組織や個人が独自の判断で発表タイミングを恣意的に決めるなど） 特に、攻撃技術情報といっても、システム部門が扱う情報と、国家安全保障視点で使う情報は視点の違いで異なると推測できると思われるため、攻撃技術情報の取扱い・活用手引きでは「ナショナルサイバーセキュリティ、ナショナルインタレストに関わるものを除く」といった免責を入れるべきではないか。	今後の検討の参考にいたします。
13	6	1	個人		本件のスコープが「専門組織間での情報共有の促進」となっているが、被害組織が攻撃情報を共有するメリットが存在しないように見えます。その為、被害組織と専門組織での秘密保持契約を更新することに異議を見いだせず、専門組織が攻撃情報を公開できないのではと考えます。その為、経済産業省自身が強制力を含めた「被害組織が攻撃情報を(専門組織に)共有する束縛」が必要と考えます。おそらく、専門組織間の共有よりも、被害組織と専門組織間での秘密保持契約による情報公開不可の部分に焦点を当てたほうが、情報共有は進むと考えらえられます。 また、スコープ全体を一気に進めるように見受けられますが、段階的に一部から始めるような形の方が良いと考えます。	御意見を踏まえ情報共有のメリットを追記いたします。

14	7	1	-		冒頭に、手引きの目的が記載されていないのが気になります。 「想定読者」の記載とあわせて、誰のために何の目的で作成したか書いた方がいいと思います。 また、資料作成の基本的な部分で粗があるように思います。 例えば、p.35では被害組織との間で生じる問題を1、2の2つに分けています。 一方、その下の図では「1 運用保守ベンダが攻撃を認知した場合」等と、別の事象についても同様に1？3を用いています。 読者からすると、そのあとの文に出た1、2がどちらを示しているのか分かりません。 少なくとも同一ページ上では、番号分けは重複しないようにすべきではないでしょうか。	御意見を踏まえ、目的を追加する等修正いたします。
15	8	1	組織		「攻撃技術情報の取扱い・活用手引き（案）」において＜非特定化加工のポイント＞をお示しいただいているが、非特定化加工された攻撃技術情報と被害組織から開示された情報を組み合わせることで、被害組織が特定できてしまう可能性も考えられる。 検討会にユーザー組織が参加したり、手引案をパブコメに付していただくなど、ユーザー組織を含め広く意見を募集いただいているところではあるが、意図せず特定された場合にリスクを被るのは被害組織であることから、今後進めていただく手引きの周知・啓発や手続きの詳細化を検討いただく過程で、ユーザー組織へのヒアリングを行うなど、ユーザー組織の意見を踏まえた非特定化加工がおこなわれるよう、ご対応いただきたい。	今後の検討の参考にいたします。
16	9	1	組織	手引き p.33	「既に通信先やマルウェアに関する情報が事案対応に当たった専門組織からレポート公表されているにもかかわらず、いまだ検知／被害認知ができていない被害組織が存在するケースが多く存在しています。これは、ファイルレス攻撃などによりエンドポイント側でのマルウェア検知だけで被害認知できないケースが増えていることや SOC監視がない他、プロキシ／FW側での不正通信のモニタリングを行っていない組織や対応に不足がある組織が存在するためです。そうした、「既に公開情報も出ているが過去／直近の攻撃をまだ検知できていない組織（層）」向けには、公開情報であったとしても、過去／直近のいつからいつまでの期間を調査せよ、とインディケータ情報を情報共有活動を通じて展開する必要が出てきます。」との記載があるが、このような対象組織では十分なログ取得すら行われていないケースも考えられるため、デフォルトで取得されているログ（OS のイベントログ等）など、確実性の高い検知方法などへの言及もあると良いと考える。	今後の検討の参考にいたします。
17	9	2	組織	手引きp.35	「攻撃技術情報共有時の被害組織との間の問題点」について、情報共有活動（XXX-ISAC等）へ参加している企業の場合、自身が被害情報を共有せずとも専門機関などから情報が入手できる、フリーライドの可能性がある。 ガイドラインや本手引き案の趣旨は、広く情報を収集し共有することがあると思われるので、契約条項だけでなく、積極的に情報提供する環境の醸成が必要と考える。	情報共有が促進される環境が醸成されるように周知・啓発活動等を実施して参ります。

18	9	3	組織	手引き	このようなガイドをもとに実際に取り組みが行われた事例を国内企業や組織へ積極的に公開・共有することで、インシデント情報共有への理解を促進し、被害企業を含めた社会としてインシデント情報の共有があたりまえとして行われるよう意識の醸成が必要と考える。	情報共有が促進される環境が醸成されるように周知・啓発活動等を実施して参ります。
19	9	4	組織	秘密保持契約に盛り込むべき攻撃技術情報等の取扱いに関するモデル条文案 第3項	該当箇所について共有した攻撃技術情報等被害組織が推測されてしまった場合における被害組織のリスクは、被害組織が責任を負うと理解した。 「サイバー攻撃被害に係る情報の共有・公表ガイダンス」に言及のある「積極的に被害公表を行った組織に対して、より適切な評価がなされるようになる」、「説明責任を果たす観点から、積極的に情報を開示することにより、インシデント対応における評価を得る効果がある」といった社会からの適切な評価が担保されていれば妥当と思われるが、現状は被害企業が公表した際の社会からの無理解や誤解に基づく批判などを加味したうえで、これらの活動に取組むことが一般的と思われる。 そのため、「どの範囲／どの組織／誰にまで情報を共有すべきか」といった利用範囲を限定したり、専門組織にも一定の責任を問えるようなモデルの方が被害組織の理解を得られやすいと考える。	今後の検討の参考にいたします。
20	9	5	組織		専門組織については、攻撃技術情報等悪用が可能な情報を取り扱うことから、情報管理体制を適切に整備する必要があると考える。また専門組織の情報管理体制や情報共有状況について、公的機関などの第三者が適宜検証可能な仕組みを整備することも必要と考える。	今後の検討の参考にいたします。
21	10	1	組織		産業横断サイバーセキュリティ検討会では「攻撃技術情報の取扱い・活用手引き（案）」及び、「秘密保持契約に盛り込むべき攻撃技術情報等の取扱いに関するモデル条文案」を会員企業において共有し、その取り組みの必要性及び重要性を確認しております。 本取り組みにおいて共有される情報は、法人組織名と組み合わせると、企業信用及び株価等にも影響する重要な情報となるため、事業部門やIT部門が独自に判断できるものではない場合も考えられます。 法人組織が外部に提供する情報が悪用され経営にインパクトを与えることが無いよう、まさに「サイバーセキュリティは経営課題」であるとの観点から、情報を慎重に取り扱うことを示す「手引き（案）」及び「モデル条文案」となっているものと思いますが、今後も継続的に、この情報を提供する先の信頼性、漏洩した場合の補償、取扱事業者や取扱者の認定など、法人組織がこの取り組みに安心して関与できる枠組みの検討を続けて頂きたいと考えております。	今後の検討の参考にいたします。
22	11	1	個人		攻撃技術情報の取扱い・活用手引き（案）の12ページ以降に驚異情報の取り扱いについて言及されているとお見受けしております。 情報共有の重要性を始めとした様々な項目が記載されている中で、昨今のセキュリティーに関する情勢を鑑みて「情報のトリアージ」も 重要であると考えております。 それはすなわち競技情報は様々なところから入手可能であるが、その量が膨大であるため、 １：自分たちに本当に必要な情報は何なのか ２：自分たちに関係する事象が起こった際に、そこから先の行政機関へのシームレスな報告体制 の2点がさらに考慮すべき内容であると考えております。 「サイバー攻撃による被害に関する情報共有の促進に向けた検討会最終報告書」内29ページに記載がありますが、 １：行政機関への相談・報告のあり方、害組織が行政機関に報告する際、行政機関ごとに報告事項が異なるなど、被害組織の負担が大きいため、対応コスト軽減に向２：けた取組の検討が必要ではないか。 政府と民間事業者間の情報の共有、民間事業者の予防措置の観点から、政府の役割を明確化し、被害組織の支援等にあたる専門組織（セキュリティベンダやSOC事業者等）から政府への情報共有を促進するとともに、政府が持つ有益な情報等を民間事業者に提供する等、政府と民間事業者間の情報共有をさらに推進することが必要ではないか。 この部分が非常に近いものであり、 情報を共有するだけではなく、必要な情報を取捨選択するところと事案発生時におけるセキュリティ関連プラットフォームとインシデントを共有するプラットフォームが統一されていることが望ましいと考えております。	今後の検討の参考にいたします。
23	12	1	組織		専門組織が「攻撃技術情報の取扱い・活用手引き」に沿った対応を行う為の手順・体制を整備している事を示す認定制度や監査を設ける等、被害組織が専門組織の信頼性を判断可能とする為の制度についてご検討頂きたい。	今後の検討の参考にいたします。
24	12	2	組織		「モデル条文」および「取扱い・活用手引き」施行までのスケジュールを提示いただきたい。	頂いた御意見を踏まえ修正した手引き及びモデル条文を速やかに公表し、活用いただく想定です。