サイバー攻撃被害に係る情報の共有・公表ガイダンス　意見募集の結果一覧

	提出者	該当箇所	御意見の概要	御意見に対する主な考え方及び修正
1	個人1	はじめに―情報共有とは何か／公表とは何か	11頁　第三者による情報発信中央の図について 被害組織自身の匿名欄に何も入力されていないが「匿名による相談」を追加して「情報の共有」を専門組織から企業へ促すようにしてはどうでしょう。 ＩＳＭＳ２７００１を取得している企業で情報セキュリティ関係を専門に行う部門（部署）では、情報セキュリティ被害（インシデント）が発生した際に上長や上司に報告したりインシデント報告書を作成したりする。その後「情報の共有」が行われれば問題ないが、勉強不足や本ガイダンスの存在を知らないなどの理由で「情報の共有」が行われないケース（内部隠蔽含む）があります。 この「情報の共有」が行われないで被害を拡大させないために、企業内からのリークから専門組織より「Ａ社で情報セキュリティ被害が発生しています。御社も被害にあわれてませんか。」や「外部から提供されたログ情報から御社が攻撃された可能性があります。被害に会われてませんか。」等のアクションから被害を減らす取り組みを行ってはいかがでしょうか。	今後の検討の参考に致します。

2	個人2	その他、本ガイダンス全体について	ページ数の追記、用語の言い換え、誤植等の修正 ・Q〇〇とある箇所等は、ページ数も付記してほしい。 ・わかりやすい語、言い回しに置き換えて欲しい －ケーススタディ　→　事例研究 －企図する　→　企てる －授受　→　受け渡し －突合　→　照合 －リーガルリスク　→　法的リスク －アカウンタビリティ　→　説明責任 －インシデント　→　事例 －FAQ　→　よくある質問とそれに対応する回答 －インディケータ　→　指標 －ベンダ　→　販売者　等 ・誤植等 －おそれ　が　おそ　になっている箇所がある　等	ケーススタディ、リーガルリスク、アカウンタビリティは専門用語でもあり、日本語に置き換えるとニュアンスが変わってしまうところがあります。 インシデント、FAQ、インディケータ、ベンダは、情報共有の現場では定着している用語でもあります。 突合は、照合に置き換えると、データベースで照合することを想起させます。 したがいまして、これらにつきましては、原案のとおりとさせて頂ければと思います。 その他は、分かりやすくするため、ご指摘のように修正致します。
3	個人2	その他、本ガイダンス全体について	58頁　情報共有のタイミングを逃すとどうなるのか、政府が示す目安の期間を皆知りたいと思うのです。例えば3ヶ月～半年みたいな感じで目安を示して頂けると助かります。	ご質問の点は、攻撃キャンペーンや攻撃グループごとに異なってくるため、事案によりけりであり、一概にはお示しすることは困難ですのでご了承下さい。被害組織におかれましては、早期に専門組織（セキュリティベンダ、専門機関）に情報共有して頂ければと思います。
4	個人3	はじめに―情報共有とは何か／公表とは何か	21頁　下部の図では、それぞれの範囲の意味するところを赤・紫・橙・紺の色分けによって区別していますが、このような表現は色覚異常の方にとって不便であるので、番号を振るなど色分けに依存しない表現での区別を追加することが望ましいと考えます。あくまで「図の本質に関わる要素を」「色分けによってのみ」表現している点に問題があるのであって、色彩を用いた図の表現自体には異論ありません。	ご指摘のとおり修正致します。

5	個人3	その他、本ガイダンス全体について	111.222.***.***、123.211.***.***、213.111.***.***、123.***.***.231、223.***.***.112、213.***.***.*** といった IP アドレスがインディケータの例として掲載されていますが、これらは実在するグローバルアドレスなので、一部を伏字にしても例示に用いるのは不適切だと考えます。 111.222.***.***、123.211.***.*** に至っては (意見提出時点で) 該当するすべての IP アドレスが特定の AS (Autonomous System) に属しており、まるで当該 AS が悪性であるかのような誤った印象を与えかねず、なおさら適切でないと考えます。 RFC5737 によってドキュメント用に予約されているアドレスである、192.0.2.0/24、198.51.100.0/24、203.0.113.0/24 のいずれかを使用するべきです。	ご指摘のとおり修正致します(Q7、16、28、ケーススタディ)。
6	個人3	その他、本ガイダンス全体について	本ガイダンスの英語版を作成・公表し、その宣伝を英語で行うことを要望します。 海外のＩＴ系ニュースを複数購読していますが、我が国のサイバーセキュリティ政策が取り上げられたのはほとんど見たことがありません。 実際には様々な事業を行っており公開資料も多数あるにもかかわらず、海外メディアでは米国・英国・ＥＵなどと比べてまったく存在感がありません。 その理由のひとつは公開資料を日本語でしか提供していないことが多いことにあると考えます。海外の方からすれば日本語でしか出ていないものは存在しないも同然です。 有用な資料を作成したならば、英語で公表して、かつ各種媒体やソーシャルメディアを通じて積極的にその宣伝を行うことが、サイバーセキュリティに関する国際協力関係における我が国のプレゼンスを高めるうえで決定的に重要だと考えます。	今後の検討の参考に致します。

7	個人4	Q7.「インディケータ情報」とはなんですか？	重要インフラ分野「クレジット」の重要システムであるクレジットカード決済システムついて、意見を述べさせていただきます。 主に各クレジットカード会社単位で決済システムを利用していますが、不正作出にて作り出したデータと思われる情報により日々万件単位のリスト型攻撃を受けていると想定されます。不正オーソリを受け取るだけで、提示いただいたような「インディケータ情報」及び「攻撃技術情報」等の分析・対策をカード会社では行っていない状況です。 オーソリ情報の元（手前）にあるテクニカルな情報を読み取り、対策を講じることが必要と思われます。その点をケアしないと将来もっと重大な事故が起こる可能性が潜在的あると考えます。 クレジット業界では2022年度の不正被害金額は過去最高値を計上しようとする状況です。その三大要因は①不正作出によるリスト型攻撃、②フィッシング、③情報漏洩等です。それらの対策にも役立つ深堀した現状把握、原因分析、対策立案、実行、検証が緊喫の重要課題であると思料します。	賛成のご意見として承ります。
8	個人4	Q13.なぜ非公開で参加者が限定された情報共有が行われるのですか？	攻撃に関する情報を共有するにあたって、留意点として３点に言及されていますが、この点は当然であり、全面的に賛成です。 攻撃の早期段階で攻撃情報を公表してしまうと、攻撃者が即手法を変化させてくるのは必然です。重要インフラ「クレジット」に関する点で考えれば、攻撃に関する情報を対策対応ができる大手会社のみに共有限定することにより、対策の検証を行うことが必要です。そのうえで、同一パターンの攻撃が収束後（三か月、六か月程度）に内容を公表する形がいいと思料します。	賛成のご意見として承ります。

9	法人1	はじめに一本ガイダンスのコンセプト	北朝鮮ミサイル被弾、台湾有事、南海トラフ大地震などの危惧されている非常時を狙って、人的、設備的な脆弱性を衝いて、国家的関与のサイバー攻撃を受ける可能性は否定できない。平時のみを前提としたコンセプトに対して、非常時を前提としたコンセプトも並行して議論しておくべきではないかと考える。	本ガイダンスは、被害組織におけるサイバー攻撃被害に係る情報の共有・公表のポイントの整理を目的に策定するものとなります。ご指摘のような特定の状況下での情報共有については、今後の検討の参考に致します。
10	法人1	はじめに一なぜ「情報共有をするべき」なのか／公表の社会的意義	経済協力開発機構（ＯＥＣＤ）は、コンピューターシステムへのサイバー攻撃が、ほかの災害や惨事と同時に行われた場合、「最悪の事態」を引き起こす可能性があるとの報告書を発表している。非常時においては、「最悪の事態」を防ぐために、若干の業務効率は低下するとしても、関係組織において、ネットワークの制限を極度に強化するための情報としての社会的意義もあろう	本ガイダンスは、被害組織におけるサイバー攻撃被害に係る情報の共有・公表のポイントの整理を目的に策定するものとなります。ご指摘のような特定の状況下での情報共有については、今後の検討の参考に致します。
11	法人1	Q8.いつ情報を共有すればいいのですか？	平時においては、「インディケータ情報としての情報が集まった段階」で情報共有することは合理的であろう。しかし、非常時（武力攻撃事態、緊急対処自体、大規模災害時）をねらって、国家的関与するサイバー攻撃が日本のインフラ等に向けて行われることが危惧される。そのような攻撃があれば、標的になった企業の数千台のサーバーと数万台のＰＣとが、わずか7分間で全面停止すると言われている。そのため、非常時における情報共有については、サイバー攻撃の技術情報整理を待たず、迅速性を最優先に、別途ルールを設定すべきであろう。非常時の認識としては、全国瞬時警報システム（J-アラート）の活用も考えられる。	本ガイダンスは、被害組織におけるサイバー攻撃被害に係る情報の共有・公表のポイントの整理を目的に策定するものとなります。ご指摘のような特定の状況下での情報共有については、今後の検討の参考に致します。

12	法人1	Q32.どのような攻撃技術情報であれば速やかに共有することができますか？（公開情報と非公開情報の違いについて）（※調査ベンダ向け解説）	コンテクスト情報を秘匿し、技術情報のみを共有するにしても、国家主体を背景とするサイバー攻撃が複数の脆弱性を同時に狙ってきた場合、文書の起案を待つ余裕はない。瞬時にすべてのセキュリティ機器のポリシー変更や保護設定変更を行うような対処に必要な情報共有としては、短時間で判断し、行動を起こせるような、「コードE」とか「コードZ」などの重大度や特徴をあらわす記号での情報発信もご検討いただきたい。	本ガイダンスは、被害組織におけるサイバー攻撃被害に係る情報の共有・公表のポイントの整理を目的に策定するものとなります。ご指摘のような特定の状況下での情報共有については、今後の検討の参考に致します。
13	個人5	その他、本ガイダンス全体について	脆弱性情報公表の際、ゼロデイ攻撃がすでに確認されている場合には、最初に攻撃が観測された日付をいっしょに公表してほしいです。 公表してもらえるとログ確認の際に日付で絞り込めるので手間が少なくなって助かります。	本ガイダンスは、専門機関による脆弱性情報の公表について述べるものではありませんが、ご意見として承ります。
14	個人6	その他、本ガイダンス全体について	日本のサイバーセキュリティを担う皆様の苦労を軽減する意味でも、共有や公表は進めてただきたいところです。しかし、いかんせん、何らかのコストもかかるものは、二の次、三の次になりがちです。うやむやにするのが一番ということになりがちです。諸外国のように、攻撃を受けた側に、厳しい対応を求めるようにしないと、なかなか情報共有が進まないのではと思ったりします。（重荷にはなりますが、それでセキュアになるなら、厳しくする価値はあると思いますし、組織の判断としても、セキュリティにお金を使うほうが得であると思うようになるでしょう。）	今後の検討の参考に致します。
15	法人2	チェックシート／フローシート	150頁　情報共有判断のためのフロー 「（類似の被害リリースなどから）広く観測されている攻撃かどうかを判断」の部分について、その時点で広く観測されているとわかる状況であれば、すでに情報は出回っているのではないか？その前段階の情報共有が重要だと考える。	「広く発生していないと思われる」に修正致します。

16	法人2	チェックシート／フローシート	151頁 下記の方がより適切な表現でないか確認されたい。 　変更前：「自組織以外で被害が発生しているか、または発生する蓋然性が高いか」 　変更後：「自組織以外への被害の波及を確認しているか、または波及する蓋然性が高いか」 （主旨）「発生」だと一般公開情報（例えばマスメディアによる公開情報等）と混同し、自組織インシデントに起因しているもののみを指し示しているのか理解しづらいと感じた。	ご指摘のとおり修正致します。
17	法人2	Q22.他組織の被害に関する情報を発見した場合、どうしたらよいですか？	91頁 被害情報は、専門組織ないしは専門機関の仲介による連絡を推奨とされているが、そもそもこれらの組織は漏洩が疑われる組織へ個別に連絡を取るような事は行われるものか。 難しい場合の代替手段として、例えば入手した侵害・漏洩情報のデータ・リストを協議会内で共有することは検討されているか。	専門機関により、認証情報等が漏えいした組織へ個別通知を行うことは日頃から行われており、例えば、（一社）JPCERT/CCのサイトで紹介されている下記通知事例があります。 https://blogs.jpcert.or.jp/ja/2022/07/ssl-vpn.html ご指摘の専門組織／専門機関による個別通知が難しい場合における協議会内での共有ですが、協議会構成員を通じて漏えいが疑われる組織に通知が行えるのであれば共有することも選択肢としてありうると考えますが、その場合は通知を仲介可能な構成員に限定したデータ／リストの共有が現実的であり、協議会における守秘義務があるとはいえ、基本的に無関係な第三者へのデータ／リスト共有は必要最小限であることが望ましいと考えます。

18	法人2	Q24.他の被害組織を踏み台として攻撃された場合、当該情報はどのように扱えばいいですか？	96頁 セキュリティベンダやクラウド業者・保守業者が侵害され感染の流通経路となっているケース。全ての利用者に適切な情報が行き届くよう、複数の経路を使った速報が求められるのは当然ながら、事案が落ち着いた後には広く顛末を共有し、国全体のセキュリティ向上につなげるべき。ベンダや業者は、これらの可能性も想定したシミュレーションの重要性をあらためて周知するとよいと考える。	ご指摘のとおり、注意喚起目的だけでなく、同業他社を含めた「顛末の共有」目的として行われ、広く同業他社のインシデント対応知見が向上することが望ましいと考えますので、その旨、修正いたします。
19	法人2	ケーススタディ	124頁 説明文と挿絵に項番があると、より分かりやすいと感じた。(124頁以外も同様)	ご指摘のとおり修正致します。
20	個人7	Q20.所管省庁への任意の報告は、行った方が良いでしょうか？	国の安全保障に関わる事案の情報は、須らく政府機関に報告するように求めた方がよいのではないでしょうか。	本ガイダンスでは、所管官庁への任意の報告を推奨しているところですので（Q20）、ガイダンスの普及に積極的に取り組んでいきます。
21	法人3	はじめに一本ガイダンスのスコープ	本文書の位置づけですが、今後各社が任意で参考とするものという点を確認したいと思います。 また、文書のタイトルも「情報の共有・公表ガイダンス」はよりも内容にそった形で「情報の共有・公表時の考慮ポイント」というタイトルがより正確ではないでしょうか。	本ガイダンスは、ご指摘のとおり、あくまでも各社が任意で参考とするものですので、タイトルにつきましては、原案のとおりとさせて頂きます。

22	法人3	チェックシート／フローシート	公表の要否については、法令に従う部分もあると記載されていますが、そういった法令の確認がフローチャート等では見えにくくなっている様に思われます。 日本の個人情報保護法では、被害者に連絡出来ない場合は公表が必要になる等、法的に公表が必要な場合については、フローチャートでも分かり易く記述したほうが良いのではないでしょうか。 また、Q25で記載されていますが、公表することで、被害が拡大することも多々あります。例えば、不正アクセスを公表することで弊社を装う不審メールが頻発する可能性があります。そのような点もフローチャートでも分かり易く記述したほうが良いのではないでしょうか。	フローチャートに、個人情報保護法を明記するとともに、Q20への誘導を付加致します。 フローチャートの中に「被害公表した場合、当該公表内容を悪用した不審メール等の別の攻撃が発生するおそれがないかどうか確認・事前の対応準備」と記載しております。合わせて、Q25への誘導を付加致します。
23	法人3	その他、本ガイダンス全体について	現状は情報を出す側には負担が大きい状況です。サイバー攻撃を受けた事実を公開すると、当該会社へのマイナスイメージがつきまといます。この点を払拭しない限り、情報共有に躊躇する会社が大多数と思います。本取組みと並行して、サイバー攻撃事案の被害公表を社会的に受容する環境の醸成（取組み/啓発）をお願いしたいと思います。	今後の検討の参考に致します。

24	法人3	その他、本ガイダンス全体について	受け手側にとっては、匿名化され、もしかすると間違っているかもしれない情報が届いたときに、どこまで情報を信じて活用できるか？など、判断が難しい点が残ります。 間違った情報でシステム遮断してしまった際に周りからの批判を受けにくいようにする、あるいは、受け側も安心して対処できるために、情報の信頼をどのように担保するのかについても説明が必要ではないでしょうか。	ご指摘のとおり、特に脆弱性対応や、現在発生中の攻撃への対応に関する情報においては、技術的に誤った情報が伝わることにより、本来不要なシステム停止／ネットワーク遮断が発生することで企業の顧客／取引先等に多大な影響が及ぶ可能性が懸念されます。そのため、広く社会全体に対する注意喚起目的の情報発信については、Q14、Q31で記載のとおり、専門機関を通じた情報発信が望ましい旨を示しています。専門機関自身が情報を誤って発信してしまうおそれもありますが、これを防ぐためにも、Q9後段でお示ししたとおり、サイバーセキュリティ協議会のような専門機関、専門組織同士の共有／連携の場が必要であると考えています
25	法人3	その他、本ガイダンス全体について	情報共有活動におけるフィードバック情報については、本ガイダンスの中で多く言及されており、情報を出す側には、受け側から何等かのフィードバックをいただけることがモチベーションになります。 そのための仕掛けとして、共有情報の「深刻度」があれば良いのではと考えます。深刻度がわからないと、受け側として「優先度」が分からず、詳細な調査を後回しにする、あるいは実施しない、となります。結果として、フィードバックにまで至らないことが想定されます。 フィードバック情報の内容については（ケースの一部に記述されていますが）詳しく言及されてないように見受けられます。どのようなフィードバックがあり得るのかについての説明があると良いのではないでしょうか。	ご指摘のとおり、共有時に対応の優先度を検討しやすい目安となる情報／レベル分けが示されることは有効と考えます。 示し方は個別の情報共有活動毎のルールや、情報の発信元の専門組織によって、また攻撃類型毎にケースバイケースでありますが、どのような示し方がありうるか例示するよう修正させていただきます（Q10に「フィードバック」を得やすい情報共有について」を追記）。

26	法人3	その他、本ガイダンス全体について	技術情報の共有の仕方についても具体化が必要です。信頼できるコミュニティでの共有は既にできています。これを一歩進めるためには米DHS/CISAのように、政府機関が情報を受け取り、裏取り・匿名化を行った上で情報開示するような仕組みも必要ではないか。	本ガイダンスの主眼は、被害組織におけるサイバー攻撃被害に係る情報の共有・公表のポイントの整理にあります。政府からの情報発信のあり方については、今後検討が進められると思われます。
27	法人3	その他、本ガイダンス全体について	本ガイダンスの対象には中小企業・小規模企業が含まれると想定しています。 本ガイダンスの主な想定読者は被害を受けた組織の担当部門（セキュリティ担当部門、法務・リスク管理部門等）と述べられています。一方で、IPAの調査によれば、セキュリティの専門部署を置いたり兼務で担当者が任命されている中小企業は39.2%であり、担当部門がない企業が6割を超えています。 本ガイダンスには、企業規模にかかわらず参考にすべき点が多数盛り込まれていると思いますが、多くの中小企業にとっては145ページのガイダンスを読むだけでも二の足を踏んでしまうのではと想像されます。 本ガイダンスのうち、上記担当部門がなくても実施可能なことに絞り込んだポイントを、例えば、現在、IPAが研究会を実施して改定準備中の中小企業セキュリティガイドラインに盛り込むなど、せっかくのガイダンスを中小・小規模企業も活用できる方策をご検討いただけるようお願いしたい。	情報の共有・公表を促進するにあたり重要なご指摘ですので、情報処理推進機構（IPA）やサプライチェーン・サイバーセキュリティ・コンソーシアム（SC3）等とも連携しながら検討を進めていきます。

28	法人3	その他、本ガイダンス全体について	企業の情報システムの構築、運用では、自社だけでなく委託先を活用するケースが多くあります。インシデント発生時に情報共有や公表を行う際に、委託元と委託先の望ましい役割分担や連携方法について、ガイダンスを示していただけると、多くの企業でも参考になるのではないでしょうか。	Q24「他の被害組織を踏み台として攻撃された場合や利用するクラウドサービス、運用保守ベンダが管理／提供するシステムが攻撃された場合、当該情報はどのように扱えばいいですか？」において、「両者の利害が衝突する可能性や、未知の脆弱性悪用の可能性などもあるため、第三者としての専門機関への相談が推奨されます。」と記載したところです。 ご指摘の役割分担、連携方法につきましては、今後の検討課題とさせて頂きます。

29	個人8	その他、本ガイダンス全体について	・３頁の表に表側頭（たとえば「用語」）と表題（たとえば「用語意味」）を記載したほうがよい。 ・３頁の「マルウェア検体」の解説の記載内容は、解説になっていない。 ・３頁の「インディケータ情報」の解説の文末「のこと」は削除したほうがよい。他の箇所の例と同様に。 ・４頁の「情報提供」の解説の文末「。」は削除したほうがよい。 ・５頁の「窓口組織」の解説の文頭「上記」はどこの記載を指しているのか？ ・５頁の「窓口組織」の解説の２行目の「組織。」は「組織」のほうがよい。 ・５頁の「届出窓口」の解説の文末「。」は削除したほうがよい。 ・５頁の「ベンダ」の解説の「SIer」とは何か？ ・９頁の１１行目「という」と、６８ページの７行目「と言う」とは、どちらかに字句を統一したほうがよい。 ・９頁の２１行目「とおり」と、７３ページの３行目「通り」とは、どちらかに字句を統一したほうがよい。 ・１７頁の最下行から上に１行目「分かる」と、５５頁の最下行から上に２行目「わかりません」とは、どちらかに字句を統一したほうがよい。 ・５７頁の回答の５行目の文頭は一字下げたほうがよい。 ・６５頁の１２行目「ひとつ」は「１つ」のほうがよい。９ページの例と同様に。 ・８９頁の１５行目、１９行目の文頭は全角分字下げしたほうがよい。半角分ではなく	字句の修正につきましては、ご指摘のとおり修正致します。 SIerにつきましては、用語として定着しておりますので、原案のとおりとさせて頂きます。

30	個人9	その他、本ガイダンス全体について	取り組み自体や、取り組みの方向性は賛同します。一方で、投げっぱなしにならないように、以下の点に留意して進めてほしいです。 ・利用者からのフィードバックをもとに、わかりやすく実用的な内容へとブラッシュアップを継続する。 ・具体的な活用事例をもとにして、役に立った点や、判断に困った点、逆効果だった点などを継続的に評価する。(PDCA) ・公表によっておこることへの対処も含めた、もう少し広い範囲での説明になるとなお良いです。 ・利用者側、公表を見る側への啓もうも行ってほしいです。 ・また、拡散者への啓もうも重要です。切り取り報道の抑制のほか、情報源となる組織の公表サイトなどへの誘導などについて、きちんと協力的に振舞うことが重要です。	賛成のご意見として承ります。
31	法人4	はじめに一情報共有とは何か／公表とは何か	サイバー攻撃被害に係る情報の共有・公表ガイダンスによって情報を共有が促進されることを歓迎します。このガイダンスにおいて厳密には「公表」ではない匿名情報が、Disinformationであった場合の検知・訂正等の仕組み作りが今後必要だと考えます。	賛成のご意見として承ります。
32	法人4	情報共有・被害公表の流れ	サイバー攻撃被害に係る情報の共有・公表ガイダンスによって情報を共有が促進されることを歓迎します。実名で行う公表においてガイダンスでは、攻撃技術情報の専門機関へ情報開示と、所管官庁への報告は別個に行うとなっています。事案の経験では、攻撃技術情報と所管官庁への報告は一本化が望ましいと考えます。現場にて事案対処に追われている状況を考えると、例えば監督省庁へ届けの一本化が届け出の促進に繋がると考えます。	今後の検討の参考に致します。
33	法人5	その他、本ガイダンス全体について	図表については、関係性の図、プロセスの図、手順・作業の図等の整理がなされていないように見えており、被害組織の立場に立った時、それぞれを業務に生かすことが難しい。自身の立ち位置、作業手順、望まれる成果等、もう少し整理して図表に反映して頂きたい。	図表は、本文の理解の手助けという位置づけでもありますので、本文と合わせて参照して頂ければと思います。

34	法人5	はじめに―情報共有とは何か／公表とは何か	【本ガイダンスはサイバー攻撃の被害に係る情報のうち、どのような情報を、どのタイミングで、どのような主体と共有すれば、被害組織自身がサイバー攻撃の全容を解明し、被害組織自身の対策強化や他組織への攻撃被害の未然防止、被害拡大防止に効果を発揮することができるのか、実務上の参考とすべきものを具体的に示すことを目的として検討を行ったものです。】について 被害組織自身がサイバー攻撃の全容を解明することは難しく、自組織が狙われる又は攻撃を受けてなんらかの被害が発生した状況についてのみ解明を試みることができるのではないか。	ご指摘のとおり、単独の組織だけでは攻撃の解明が困難であることから、本ガイダンスにおいて情報共有の重要性を示しているところです。
35	法人5	はじめに―情報共有とは何か／公表とは何か	【前者は被害者個別の目的であり、高度な攻撃手法に対して不足する情報を補うことを目的としています。後者は情報共有活動全体としての目的であり、①の目的で提供された情報が別の参加組織の②のための情報となることで、情報共有活動を通じた相互の利益につながっていると言えます。】について 情報共有した相手が信頼に足りるか、攻撃者に情報が渡った場合にどのようなリスクがあるのかについての検討が少ないのではないか。どこまで攻撃されているかという被害組織の認知の範囲を公表してしまうことで、攻撃者はどこまで成功しているのか予測・計測できるのではないか。	ご指摘のとおり、関係者を限定し、非公開で行う情報共有活動のメリット等をガイダンス中でも解説しています。

36	法人5	はじめに―情報共有とは何か／公表とは何か	【被害企業への過度な批判ではなく、攻撃の脅威や対策の必要性に対する社会的な問題意識の共有が進むことを目指します】について 積極的な公表を推奨するのであれば、上記箇所について具体的な取り組みの内容が示されるべきではないか。また、各企業に公表を求めるだけでなく、公的機関が収集した「被害内容を示す情報」を匿名化し広くタイムリーに開示する仕組みを本ガイドラインの中で明示すれば、「公表」による社会的意義をより果たせるのではないか。	攻撃の脅威や対策の必要性に対する社会的な問題意識の共有が進むために、被害の公表に際して参考となる文書として、本ガイダンスを策定したところです。本ガイダンスの積極活用を期待します。 「タイムリーに開示する」という観点では、基本的には被害予防／被害拡大防止を目的とした、専門機関からの注意喚起情報の発信が想定されます。 なお、IPAでは、被害の状況 把握や対策検討を目的とし、一般利用者の方や企業・組織の方から、広くコンピュータウイ ルス・不正アクセスに関する届出を受け付けており、この事例を紹介することで、同様被害の早期発見や未然防止といったセキュリティ上の取組の促進につなげています。

37	法人5	はじめに―なぜ「情報共有をするべき」なのか／公表の社会的意義	【サイバー攻撃被害に係る情報の公表 により社会全体に対して情報が提供されることで、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と考えます。】について とても重要な視点だと考えています。この根拠を詳しく明示して頂きたい。	16頁において触れたとおりです。 被害公表を行った組織と、情報の受け手側（ステークホルダーだけでなく、メディアなどを含めた社会全体）との間に情報の非対称性があることにより、被害組織のインシデント対応の内容に適切な評価がなされていないと考えます。「鶏が先か、卵が先か」というジレンマではありますが、まずは積極的な被害公表による情報発信により、両者間の情報の非対称性が解消されていくことを目指し、本ガイダンスでは情報の共有だけでなく、被害公表時のポイントも示した次第です。
38	法人5	はじめに―本ガイダンスのスコープ	【これら取組の推進に当たっては、被害を潜在化させないことが何より重要であり、被害組織からの警察への通報・相談及び捜査協力は社会的に極めて重要な意義を持つものであるといえます。なお、仮に被害組織の内規等において、被害に係る情報の取扱いが厳格に定められていたとしても、警察への通報・相談及び捜査協力については、その社会的意義に鑑み、積極的に行われることが望ましく、これにより、更なる被害の防止を期待できます。】について 企業としては、内規等を無視した社内の機密情報の漏洩は、内部統制上の重大なインシデントとなるため、上記記載を残すのであれば、今後、新たに法規制を制定すること、または監査法人の監査項目として当該漏洩が問題の無いことを事前に確認頂いてから、ガイダンスとして発表して頂く必要があると考えます。	一般的に、企業における機密情報の管理に係る規程は、知的財産、情報セキュリティ、法務等の多様な観点から適切な行動がとられるよう整備されているべきものと承知しておりますが、外部への報告の適否はその必要性等に照らして個別に判断されるものと考えます。 本記載については、あくまで被害組織からの警察への通報・相談及び捜査協力に係る社会的意義等をお示しするものであることから、原案のとおりとさせていただきます。

39	法人5	はじめに―本ガイダンスを読むにあたって	【本ガイダンスは、主にサイバー攻撃を受けた被害組織を想定読者としています。サイバー攻撃を受けた場合、どのような情報をどのタイミングで、どのような主体と情報共有することが適当なのか検討するために実務上参考となるポイントを解説しています。被害を認知した後に参考としていただくだけではなく、平時からのインシデント対応体制の整備や訓練にあたって参考としてお使いいただくことも想定しています。】について 実務上参考となるポイントとありますが、被害を受けた組織が対応すべき手順、社内外の関係性の整理の仕方、情報共有や公表の考え方などについて、被害組織に寄り添った内容となっているのか、やや不明なところがあります。記述としては、情報を公表させたい意図が強く出ている印象を受けました。	ご指摘頂いたような点を含め、被害組織に寄り添った内容にするべく、公表を行おうとしているが判断ポイントや留意点が不明な状況において参考となるように、＜被害の公表や法令等に基づく報告・届出について＞（Q14～）、＜被害組織の保護の観点について＞(Q21～)などの解説を示しているところです。
40	法人5	Q21.公表していないのに自組織の被害が知られて公開されてしまうのはなぜですか？	【一般的な不正アクセス事案の場合、基本的には被害組織自身からの公表まで、外部に被害事実が知られることはありません】について これは内部ネットワークを想定した一面的な見方ではないか。たとえば公開ウェブサイトが改竄された場合、SNS公式アカウントが乗っ取られた場合なども考えていただきたい。	ご指摘のような、攻撃発生とほぼ同時に攻撃被害が広く知られてしまう／その可能性がある場合も含め、インシデントの被害の公表のタイミングにつきましては、Q14に記載がございます。
41	法人5	チェックシート／フローシート	【150頁、151頁】 フローの説明については、ユーザ企業の実務からの目線では、判断すべき順番が異なっている可能性があります。被害組織が観測できる範囲、被害であることを認識できる情報源など、もう少しポイントを整理して頂きたい。	ポイントにつきましては、QAの本文で解説しております。

42	法人6	情報共有・被害公表の流れ	平時からのインシデント対応体制の整備の一環として、SBOMの準備が注目を集めています。SBOMとは、製品に含むソフトウェアを構成するコンポーネントや互いの依存関係、ライセンスデータなどをリスト化した一覧表です。OSSのライセンス管理や脆弱性の管理、ソフトウェアサプライチェーンのリスク管理等の用途で利用されており、「情報共有判断のためのフロー」に沿った判断をする際、有用な手がかりになると考えられます。しかしながら、作成作業が煩雑であることから準備が見送られがちです。ぜひ、平時からのインシデント対応体制の整備の一環として、日頃からSBOMを作成・更新することを推奨することをご検討いただけますと幸いです。	SBOMの活用については、政府内で別途検討が進められております。

43	個人10	用語集	3頁 インディケータ情報報／IoC(Indicator of Compromise：侵害指標) IPアドレスと並んで重要なポート番号・プロトコルについての記述が無いが、IPアドレスよりも重要性が高い事もあるものであり、また関与者について調査を行う場合に必須的である場合も多いので（NAT利用の場合などそうであるが、近年のISP・VNEを利用したインターネットとの通信の際に用いられる接続方法であるIPoEは基本として複数の利用者でNATを用いる使用が基本的であるので、常時必須的である。）、ちゃんとポート番号やプロトコルについての記述を行うようにされたい。 国の書類は、総務省も含めて、セキュリティ関係の書類でポート番号についての記述が無い書類が多いように思われるのであるが、意図的に問題ある振る舞いをしているようにしか国民には見えない。ちゃんとポート番号については記載を行うようにされたい （そもそも、昔から、実務者の間ではIP・ポート番号がセットで基本的な情報として扱われていたはずであるが、それが文系である行政組織の官僚達が言及するようになってからポート番号についての記載が取れてしまった事が多いように思われる。ポート番号についての記述を省く様な懈怠を発生させないようにされたい。）。 6頁 情報共有 「後者の場合は匿名で行われることが専らです」とあるが、これはものによって異なると思われるので、そこまで言わなくてよいと考える。 匿名で行われる事が多い、くらいでよいのではないか。	ご指摘のとおり修正致します。

44	個人10	その他、本ガイダンス全体について	問題事態についての公表を行う事については、ちゃんと国民・市民自身が公表を行う事について、権利がある事について明言されたい。（攻撃者側は通信・情報処理についての窃視等も行えたりする場合が多く組織的である場合も多いので、政府やメーカーが対応を行うまで公表を強制的に控えさせるなどという事は不適切となると考える。むしろ、セキュリティホールなどについての存在を公に示して各種事業者等の速やかな対応を求めるのが適切と考える（ログの強制的な取得がちゃんと行われているのであれば、カジュアル犯に対しての対応はそれだけでかなり出来ているはずであるので、それで良いのではないかと考える。）。）	本ガイダンスは、あくまでも、公表をするに際して、考慮要素をお示しして、現場での参考にして頂く文書という位置づけです。
45	個人11	その他、本ガイダンス全体について	サイバー攻撃被害に係る情報の共有・公表ガイダンスにおける司令塔機能たる、サイバーセキュリティ人材の育成について意見を述べたい。 デジタルスキル標準において、人材類型としてサイバーセキュリティが公表されたところである。これを認定する国家資格が情報処理安全確保支援士試験であるなら、デジタル技術を活用して競争力を向上させる企業等に所属する人材にも合格者数、登録者数を増やしていく必要があるのではないかと感じている。 国家試験である情報セキュリティマネジメント・略称SG試験の紹介ページには『さらにステップアップしたい方の試験はこちら！』とリンク先は、情報処理安全確保支援士試験の紹介ページとなっている。SG試験からの順当なステップアップを明示していながら情報処理安全確保支援士試験の午前1試験は、応用情報技術者の午前試験からの抜粋30問となっており、実質的に応用情報技術者試験の全範囲の学習を求むることと同義であり、SG試験からのステップアップには過大な負担となっているため、受験しやすさの向上に資するとは言い難い実状である。 情報処理安全確保支援士試験は情報処理技術者試験とは別格なので、IPAの試験体系図が示すところの高度試験区分から切り分け、レベル対応もITパスポート試験同様に無くして、ITを利活用する者と情報処理技術者の間に位置付けて、午前1試験についてもSG試験からスムーズにステップアップができるよう出題をSG試験の特別措置試験問題からの抜粋30問の出題としてはどうか。	本ガイダンスでは、サイバー攻撃被害に係る情報の共有・公表を対象としており、人材育成についてまでは対象としておりませんので、何卒ご了承下さい。

46	個人11	その他、本ガイダンス全体について	登録セキスペを「セキュリティ専門人材」に位置付けて、デジタルスキル標準のユーザー企業および多数を占める中小企業の側に属している「プラス・セキュリティ人材」を「セキュリティマネジメント・セキュリティリーダー」に位置付け、登録セキスペとは切り分けた上で情報セキュリティマネジメント試験のキャッチコピーを“デジタル時代のプラス・セキュリティリーダー”として、QCサークル活動のリーダー的な立ち位置の名称独占による「国家資格」へ格上げしてはどうか。 内閣官房 内閣サイバーセキュリティセンター（NISC）で示されている「プラス・セキュリティ人材」が修得する知識や学習の補充講座プログラム カリキュラム例について、令和５年度から年間を通じての試験実施となる「情報セキュリティマネジメント試験」の合格者をNISCが「プラス・セキュリティ人材」として位置付けを明確に示したり、「情報セキュリティマネジメント試験のシラバス」を「プラス・セキュリティ知識」および、修得する学習の補充講座プログラム カリキュラムとして参照してはどうか。 応募者の平均年齢、男女比なども鑑みるならば、同試験の広報活動においてインフルエンサー並みの著名人、イチ推しは女子プロレス界きってのデジタルスキル(在宅ワークでCAD設計をやっていた)を有しているSTARDOM所属の「ウナギ・サヤカ」選手を起用してはどうか。	本ガイダンスでは、サイバー攻撃被害に係る情報の共有・公表を対象としており、人材育成についてまでは対象としておりませんので、何卒ご了承下さい。