「サイバー攻撃による重要インフラサービス障害等の深刻度評価基準（試案）」に関する意見の募集について

結果一覧

整理番号	提出者	該当箇所		御意見	反映の有無	御意見に対する考え方
		ページ	対象			
1	個人	2	深刻度評価の概要	深刻度レベルの判断基準が曖昧であるため、ぜい弱性の深刻度のようにスコアによる数値化で、レベルを１０段階程度に設定するべきである。 誰が深刻度レベルを決定するのかによって客観的な判断ができない。	無	本取組の目的は、事業者、政府関係機関、国民等がサイバー攻撃の深刻さに関する共通の理解を得て、冷静かつ適切な対応を行えるようになることです。共通の理解を得るためには、尺度が詳細過ぎることがデメリットになる可能性があり、取組の第一段階としては、諸外国の取組も参考にし、まずこの５段階程度で分類することから始めることを考えています。なお、今後、検討を進めていく中で、更なる細分化が必要になることも考えられますので、その際には、ご意見も踏まえ検討させていただきます。
2	マカフィー株式会社	1	評価対象	本深刻度評価の対象範囲が、サイバー攻撃のみに限られていますが、特にレベル３以上の事象の場合、物理的な攻撃との複合で行われるケースが想定されます。 例えば、物理的なテロを成功させるために、事前に物理セキュリティに関する情報を窃取したり、攻撃中に連絡システムにDoSを仕掛けることで、テロの把握を遅らせるといった攻撃は、単体では深刻度が低いと考えられますが、結果として大きな被害をもたらす事象をどう評価するのかという点をご考慮いただきたいです。結果事象で評価する場合には、物理的な攻撃も含めた方が良いと考えます。	無	現案は、取組の第一段階として、サイバー攻撃の結果として生じたサービス障害の国民社会への影響の度合のみで評価を行う手法を採用していますので、複合事案であるか否かが評価結果に影響を与えないものとなっています。今後も、過去事例等を用いた試行的な評価を行うなど、本評価基準の継続的な改善に努めることとしておりますので、その際には、必要に応じ、結果に与えたサイバー攻撃の役割を踏まえるなど、ご意見を踏まえ検討させていただきます。
3	マカフィー株式会社	2	評価の観点及び評価手法	「サービスに対する信頼低下」を評価指標に加えていますが、他の評価指標である人命や社会インフラの安全性、持続性の被害との比較は難しいかと考えます。「サービスに対する信頼低下」に関しても、事象の総被害額（対処にかかった人的工数含む、株価低下等）を深刻度を決める際の指標としてはいがかでしょうか。	無	サービスに対する信頼の低下を定量的に評価することが理想であると考えていますが、現時点では、信頼の低下の度合いと総被害額との関係を表すスキームが存在しておらず、尺度として用いることは困難であると考えています。今後も、過去事例等を用いた試行的な評価を行うなど、本評価基準の継続的な改善に努めることとしております。試行的な評価により事例を蓄積する中で、評価手法や指標についても検討していきたいと考えています。その際には、ご意見を参考にさせていただきます。
4	株式会社ＩＣＳ研究所	1	今後の取組	サイバー攻撃による重要インフラサービス障害等の深刻度評価基準は、火山などの深刻度基準と同じくあってしかるべきと考えます。また、地震速報のように緊急警戒の速報性も考慮しておく必要があると思います。 さらに、深刻度を公共機関や企業に促すことで、重要インフラ系の国民生活に影響を及ぼすところは、重要な制御システムについては各企業判断で、ネットワークから切り離して、スタンダロンで操業継続するなどの処置をすることも可能になります。そういう考えで、その深刻度を促すことは重要かつ活用面はあると考えます。	無	緊急警戒の速報性が重要であることは、ご意見のとおりと考えています。現案は、取組の第一段階として、事後に評価するための尺度を検討しておりますが、今後は、次の段階として、この基準を事案が発生した時点での国民社会への影響の予測的評価に活用し、政府の対応を判断する基準とすることなどを継続的に検討し、ご期待に添えるよう取り組んでいく所存です。

整理番号	提出者	該当箇所		御意見	反映の有無	御意見に対する考え方
		ページ	対象			
5	石油連盟	2	深刻度評価の概要	・評価対象について ① 「国民社会に与えた影響全体の深刻さ」を評価するものとされているが、試案では供給者における重要インフラサービスの提供状況のみに基づいている。国民社会、すなわちサービスの享受者が被った影響の実態を、この一面的な情報により評価することは極めて困難である。 ② また、政府機関であるNISCがこのような評価を「国民社会への影響」として国民に周知した場合、国民が過大な事象であるとの印象を受け、かえって社会に大きな混乱を招く恐れがある。 ③ 更には、今回評価内容を「国民社会への影響」とすると、サイバー攻撃による事象以外の大規模災害等他の事象によって生じた事象の評価に影響を与えることは避けられず、これらも考慮した慎重な検討が必要。 ④ 従って、今回検討する評価対象はより正確を期し、「重要インフラサービスの提供への影響」とすべき。	無	深刻さを表現するに当たり、主体によって受け取る深刻さが異なることは理解していますが、サイバーセキュリティ戦略本部で決定された重要インフラの情報セキュリティ対策に係る第４次行動計画で「国民生活や社会経済活動に重大な影響を及ぼすことなく」と示すとおり、その視点は「国民社会への影響」であるべきだと考えています。 NISCが評価した結果をどのように公表するかについては、今後の課題として検討を継続することとしており、評価の手法や指標を含め慎重に議論を重ねていく所存です。
6	石油連盟	2	深刻度評価の概要	・観点ごとに独立した評価とすべき ① 試案においては、「持続性」「安全性」「信頼性」の観点から「それぞれ独立して評価し、その最も高い値を深刻度とする」とあるが、各分野が提供する重要インフラサービスの特性や発生した障害の性質により、各観点が国民社会に与える影響に及ぼす寄与度は異なると考えられる。 ② 殆どの重要インフラ事業者においては、共通的に、安全性・信頼性の確保は当然の前提として、サービス提供の持続性の確保が特に重要となると考えられる。 ③ 例えば、石油分野においては「石油の供給」を提供すべき重要インフラサービスと位置付けており 、石油業界としても安全性・信頼性の確保は当然の前提として「石油の安定供給」を最大の社会的使命として取り組むなど、国民生活への影響評価の観点の中では「持続性」の寄与度が相対的に大きいと考えられる。 ④ 一方で仮に製油所で事故が発生し重傷者が出た場合、「安全性」についてはレベル2となるが、在庫の活用、他拠点からの転送、他社からの融通等により石油製品の供給への支障を回避できれば「持続性」についてはレベル0となる。 この場合、試案に従えば、石油製品の供給は継続されたにも関わらず全体の深刻度は両者の最大値である「安全性」のレベル2となり、「重要インフラサービスの提供への影響」はもとより、「国民社会への影響」であったとしても、国民の実感と必ずしも合致しないのではないか。 ⑤ 従って全ての重要インフラサービス分野において一律に試案の示す「全体評価」を実施することはやめ、観点ごとに独立した評価とするべき。（上述の例では、「持続性：レベル0、安全性：レベル2」という評価）	無	本取組の目的は、事業者、政府関係機関、国民等がサイバー攻撃の深刻さに関する共通の理解を得て、冷静かつ適切な対応を行えるようになることです。共通の理解を得るためには、評価の結果をシンプルに伝えることが必要だと考えていますので、取組の第一段階としては、最終的に一つの評価となることを目指したいと思います。ただし、評価結果の公表方法や内容については今後の課題としておりますので、ご意見も踏まえ検討させていただきます。

整理番号	提出者	該当箇所		御意見	反映の有無	御意見に対する考え方
		ページ	対象			
7	石油連盟	―	情報提供	・NISCへの報告については各分野の自主性を確保すべき ① 各分野（業界）が自主的に深刻度評価基準を策定した分野（特に法令等に基づく事故報告基準が存在しない分野）においては、NISCでの深刻度評価のために行う報告の内容・様式については各分野（業界）に委ねるべき。 ② また、評価後に追加的な情報提供を求めるなど、事業者に過重な負担が生じないよう配慮すべき。	無	本取組は、事象が発生した際に、現場において必要なリソースを必要な行動に充てることができる環境作りに寄与することを目的にしており、情報入手に関しては、第４次行動計画を含めた現行の制度体系（※）をベースとして検討しております。事業者に過重な負担が生じることは、この目的にも反することになりますので、そのようなことにならないよう取り組んでいく所存です。 ※情報連絡を行う場合（第４次行動計画別添より） ①法令等で重要インフラ所管省庁への報告が義務付けられている場合。 ②関係主体が国民生活や重要インフラサービスに深刻な影響があると判断した場合であって、重要インフラ事業者等が情報共有を行うことが適切と判断した場合。 ③そのほか重要インフラ事業者等が情報共有を行うことが適切と判断した場合。
8	個人	2	評価の観点及び評価手法	サイバー攻撃的なものとはならないかもしれないが、重要インフラの情報セキュリティにおいて非常に重要なものとして、行政機関が委託を行いホストの運用等を実際に行っている行政機関外あるいは国外の事業者内部における、行政機関及び国民に関係する情報の漏洩等についても、安全度の評価を行うべきであると考える。 現状、多くの省庁において、国民の個人情報が含まれる重要情報が、*.go.jpとなるドメインで提供される、シンガポールや香港のホスト（CDN事業者等がそれらのホストを用いているのである。なお、仮想通貨NEM（シンガポールに運営者の本拠地がある。）の流出事件で有名なコインチェック株式会社の査察等を行いまた報告書等の提出も受けている関東財務局が意見等（相談や通報等が行われる事もあるであろう。）のためのフォームからの送信先ホストとしているlfb.mof.go.jpは、概ね香港のホストでの提供が多く行われていた。場合によりアメリカのホストが用いられる事もあるのであるが、しかし結局CDN事業者のさじ加減でどの国にも情報が送られてしまうのであるから問答無用レベルで悪（「真面目に」ネットワークエンジニアリングやセキュリティについて考える者にとっては、であるが。（嘘を吐くネットワークエンジニアやセキュリティ専門家など溢れすぎているので、狐狸に騙されない様に眉に唾する様に注意をしていたいものである。省庁の無軌道なCDN利用についての注意もまともにしないNISCについてもまともな組織とは到底思われない。NISCは一体何をやっているわけです？））と言える。）に、送信されているのであるが、それらのホストについて及び通信回線については、通信が国内のみで完結する場合と比べて危険性が高いと言えるものであるので、そういう事が今後基本として発生しないように、（事業者等からの）情報の漏洩等に関する安全性の評価も行う事を求める。	有	サイバーセキュリティ戦略本部で決定された重要インフラの情報セキュリティ対策に係る第４次行動計画において、重要インフラ防護の目的を「重要インフラサービスの安全かつ持続的な提供を実現すること」と規定しています。現案では、この考え方に基づき、サービスの持続性への影響、サービスに関する安全性への影響という２点を中心に評価の観点を整理しました。ただし、サービスの提供に直接的な影響を与えるものではない重要な要素があるとして、別途、「その他（サービスに対する信頼低下）」という評価の指標を設けました。情報の漏えい等の要素はこの項目で評価したいと考えておりますので、ご指摘を踏まえ、情報の漏えい等を含む旨を追記します。