「被害報告一元化に関するDDoS事案及びランサムウェア事案報告様式」（案）に関する
意見募集の結果及び意見に対する考え方

■意見募集期間 ： 令和7年7月 10 日（木）から同年8月9日（土）まで
■意見提出数 ： 28 件（法人又は団体：11 件、個人：17 件）
■意見提出者 ： ※以下、提出順に記載

No.	提出された意見	意見に対する考え方	修正の有無
1	「DDoS 事案共通様式」および「ランサムウェア事案共通様式（案）」について、以下の意見を申し上げます。 今回の様式案を拝見し、確かに専門用語が極力少なくされている印象を受けました。しかしその一方で、「具体的に何をどこまで書けば良いのか」「どのレベルの情報まで求められているのか」が曖昧で、現場としては逆に迷いやすいと感じました。 現場対応者やセキュリティ担当者からすると、ある程度の専門用語や業界で通じる表現がないと、 ・本来報告すべき重要な情報が抜けてしまう ・逆に曖昧な記述しかできず、情報の正確性や再現性が損なわれる ・後から行政側や第三者に説明が必要になったときに混乱が起きる といった問題が出てくる恐れがあります。 「分かりやすさ」と「現場の実情に即した情報の精度・具体性」は両立すべきであり、 ・最低限、現場が使う基本的な専門用語には補足説明を添える ・抽象的すぎる設問には「記入例」や「想定する用語例」を明示する ・不明点があれば問い合わせできる窓口を明記する など、現場・実務サイドが“困らない”様式に再設計していただきたいです。 現場が書きやすく、かつ正確な情報収集につながる報告様式となるよう、再度ご検討をお願いいたします。	本意見募集においては、あくまで様式本体についての意見募集を行っているものであり、今後、本様式の運用を開始する際、ご指摘も踏まえ記入例を公表するなど、分かりやすい対応に努めてまいります。	－
2	趣旨は理解できるも、被害を受けた企業が冷静にかつ正確に報告出来るか、実効性に疑問がある。本報告は即時性を求めているのか、正確性を求めているのか。まずどちらを求めているのか明確に提示いただき、その上で、例えば、一の社内様式でも可とするといった方策を取らないと実効性に乏し	様式内に記載のとおり、本統一様式は、官公署への報告が必要な場合等において共通して利用可	－

	いのではないかと思料。 もちろん被害を受けないのが前提ではあるが、被害を受けてしまった場合 ・社内様式による社内報告 ・社内様式による社外報告 ・これ と三重苦の報告責め苦を負うことになる。少しでも報告者の負担を軽減し、迅速に鎮火させるにはもう少し工夫が必要ではないか。報告のための余計な仕事を作らせたいのか疑問である。	能なものであり、新たな手続きを創設するものではありません。	
3	マスコミに対する報道発表にも利用できるようにすべき。	今後の施策の参考とさせていただきます。	－
4	本様式で収集される情報は、国際的な脅威情報共有の標準形式である STIX 等との親和性が高く、国内のサイバーセキュリティ向上に大きく貢献する可能性を秘めていると高く評価いたします。 この価値あるデータが持つ可能性を最大限に引き出すためには、データ収集のプロセスが極めて重要です。現在の PDF や電子メールを前提とした手動の報告方法では、情報の即時性や正確性が損なわれる懸念があります。そのため、ウェブフォーム等を活用した自動化された報告プロセスの導入を強く推奨いたします。 理由: 本様式案で示された「攻撃技術情報」の各項目、例えばランサムウェア事案における「ランサムウェアの類型」、「侵入方法」、「インディケータ情報」や、DDoS 攻撃事案における「攻撃類型」、「送信元情報」などは、STIX のような標準化された形式で脅威情報を記述するための基本的な要素です。 これは、報告されたデータを国内の関係機関で即座に共有し、分析や対策に活用できる素地が既にあることを意味します。 しかし、このポテンシャルは、報告プロセスが自動化されて初めて活かされます。まさに「データそのものだけでなくプロセスも同様に重要である」と言えます。 現在の PDF や電子メールでの報告では、受け取った側での手作業によるデータ転記が必要となり、対応の遅延や入力ミスの原因となりかねません。これでは、せっかくの価値ある情報が迅速に活用されず、被害拡大防止の機会を逸する可能性があります。 そこで、例えば米国 CISA が提供するインシデント報告フォーム（https://myservices.cisa.gov/irf）のような、ウェブベースの報告システムを導入することを提案いたします。このシステムには、以下のような利点があります。 情報の即時性と標準化: 報告された STIX 互換データがリアルタイムでデータベースに登録され、機械的な処理や関係機関への迅速な共有が可能になります。 インシデント管理の効率化: 報告時に一意のインシデント番号が自動で割り当てられ、対応状況の正確な追跡が容易になります。 データ品質の向上: 必須項目や入力形式をシステム側で制御することで、報告内容の標準化が図ら	今後、報告窓口の一元化に向け、所要のシステム整備を進める予定です。	－

	れ、データの品質と一貫性が確保されます。 貴重な脅威インテリジェンスの価値を最大化し、日本のサイバーセキュリティ全体の強化に繋げるため、報告プロセスの見直しとシステムの導入が"被害組織の負担軽減と政府の対応迅速化を図る"との目的に合致すると考えます。		
5	1.「内閣サイバーセキュリティセンター」と様式にあるが、「国家サイバー統括室」に組織は変更されているのではないか。少なくとも本パブリックコメント開始時点で明らかになっているこのような重要な変更について反映せず、パブリックコメントを行うとは、行政手続法を軽視しているのではないかと批判されても仕方がないとともに、サイバーセキュリティの強化を推進すべき立場であるはずの国家サイバー統括室自身が民間事業者等を含めて幅広い立場のものに使用させる様式をこのような不完全な形で提示する見識を疑わざるを得ない。 2.「政府機関等の対策基準策定のためのガイドライン」の対象となる政府機関等とされている省庁や法人等についてもこの様式で報告するということとなるのか明らかにしていただきたい。	1. 本意見募集では、「サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ」（令和 7 年 5 月 28 日）における様式を対象としており、運用開始に当たってご指摘のような点については修正を行います。 2. 本様式は、「記載の手引き」に揚げる法令、ガイドライン等に基づく報告を対象としています。	○
6	当社は主に独立行政法人や自治体などのCIO補佐や最高情報セキュリティアドバイザーを担当しております。 DDoS 事案及びランサムウェア事案報告様式において、インシデント時にはその団体の内部ネット環境が影響を受けている可能性などもあり、様式をメールで送付できない場合なども考慮して、外部通信回線を利用しての報告、ならびに共通様式を PC やスマホ等でもアクセスし伝達できるように、記入内容をWEB化したものにアクセスさせる等、臨機応変な伝達手段が選択できるように配慮いただけると良いのではないかと思います。	今後、報告窓口の一元化に向け、所要のシステム整備を進める予定です。	－
7	主に「DDoS 攻撃事案共通様式」に関する意見です。 ランサムウェアの被害と異なり、より頻度が高いおそれがあるため、様式についてその前提での仕組みが肝要と考えています。 具体的には、 ・DDoS 攻撃を受けたと考える時間や量を、資料の冒頭や指針として開示する →突発的なアクセス増加、F5 連打やサーバーの不調によるケースを誤認あるいは報告対象とするかしないか判断しやすくなる。 例）15 分以上の継続し、サービスに不調を伴うもので明らかに分散型の攻撃と推測できる事例を報告する、など ・攻撃類型への補足情報付与 直接ネットワークフラッド　Direct Network Flood（TCP ベースの大量アクセス） 反射増幅　Reflection Amplification（UDP ベースの大量アクセス） エンドポイントサービス拒否攻撃（ログインなど処理負荷の高い機構への大量アクセス）	頂いたご意見も踏まえ、攻撃類型の記載について修正いたしました。また、通信量の例示につきましては、ご指摘に沿って追記いたしました。その他のご意見については、今後の施策の参考とさせていただきます。	○

	OS 枯渇フラッド　OS Exhaustion Flood（CPU 処理誘引） サービス枯渇フラッド　Service Exhaustion Flood（ポートリソース枯渇） アプリケーション枯渇フラッド　Application Exhaustion Flood（システムリソース消費枯渇） アプリケーション又はシステムの窃取　Application or System Exploitation（その他攻撃を含む） →MITRE の分類は申告時には判断が難しいためガイドが必要。 ・送信元情報の記載配慮を追記する →UDP 通信の場合には、送信元詐称の可能性が高く、情報を収集しても意味をなさないことが多いため「観測 IP 数」などで簡潔に回答できる項目が適当。 ・通信量 →HTTP の場合は HTTP Request/sec が情報を収集しやすいため、その例も許容させる。Gbps は集計が手間がかかり、pps ではネットワークレイヤで観測をし直す必要があり正確な値を出すことが困難である。		
8	入力された情報のデータベース化や API 連携を視野に入れ、pdf や word 形式でのファイルでの提出ではなく、G ビズ ID と連携した web form での申請とし、諸事情で G ビズ ID が使えない時のみ pdf や word 形式を受け付けるなどとするのが望ましいと考える。	今後、報告窓口の一元化に向け、所要のシステム整備を進める予定です。	－
9	僭越ながら、小職の意見を本フォームにて提出させていただきます。 本意見の背景は、先日、Cloudflare 社が開示したレポートになります。 https://blog.cloudflare.com/ddos-threat-report-for-2025-q2/ 本レポートでは、「ランサム DDoS 攻撃」に関する統計情報として、’25 年度第 2 四半期では、全体の 14%の企業から同攻撃の被害に遭ったとデータが掲載されております。 特定のベンダーが公表する統計情報の引用になりますが、ランサムウェア DDoS 攻撃が一定の割合で継続されて確認されているため、本意見公募の対象となっている事案報告様式に、同攻撃の要素を入れるべきではないかと思っております 具体的には以下を提示します。 ●「DDoS 攻撃事案共通様式」について 4.(2) 攻撃類型の選択項目に「ランサム攻撃」の項目を追加 ご検討をいただければ幸いです。よろしくお願いいたします。	ランサム DDoS 攻撃として脅迫を受けている場合には、（1）事案の概要や（3）事実経過にその旨を記載いただく方法で対応できると考えています。	－

10	DDoS 事案及びランサムウェア事案報告様式はベースはこのようなフォーマットでも致し方ないと思うが、運用は電子フォーマット（XML や JSON）で機械的に処理され、天気予報のように政府機関や国民が自由に閲覧・情報取得できるべきであり、そのための電子フォーマットやデータスペースなどを活用した流通手段をて整えるべきである。	今後、報告窓口の一元化に向け、所要のシステム整備を進める予定です。	－
11	フォーマットを出すのは構わないが、一体何に利用するのかもう少し詳細に記載してほしい。何に利用するのか意図がわかれば回答も正確性が増すのではないだろうか？また、IP を出せプロトコルを出せというのも、主要ベンダのログ出力から抽出できるようなスクリプトを AI に作成させ、それを攻撃を受けた会社に利用してもらえば、国側が受け取った際にある一定のフォーマットで受領できるのではないだろうか？そうすることによって送信側（攻撃を受けた会社）の負担軽減にも、受信側（国側）の集計負担軽減にもなるのではないだろうか？	今後の施策の参考とさせていただきます。	－
12	1 この様式を使用する報告者側のメリットがわからない。詳細な事項が多すぎて、報告する期限が求められている個人情報保護法などにおいては、迅速な報告の障害となるのではないか。そもそも速報の段階での使用が想定されているのか。事後での報告に使用することを想定しているのか。 2 なぜランサムウェアのみが、本様式の対象となるのか。その他のウイルス等の不正指令電磁記録による被害についてはなぜ対象とならないのか。報告者から見て複雑ではないか。 3 この様式による報告した情報がどこで、どのように取り扱われているか報告者からのトレーサビリティに欠けている。提出した情報がどのような範囲で利用され、だれが閲覧し、いつまで保管されているのか全く分からないのは問題ではないのか。 4 本様式により報告したのち、折り返しの連絡についても一本化されるということでよいのか。共有先の各機関から同じ内容の問い合わせが個別にあることはないということでよいのか。 5 この様式にて報告したのち、共有先の各機関から何らかの様式で追加の報告が求められることはないということでよいのか。 6 なぜこの様式は NISC であるのか。国家サイバー統括室に変更されないのか。 7 本様式でおこなった報告について情報開示請求行う場合、どの機関に問い合わせればよいのか。訂正の請求についても一本化されているということでよいのか。 8 本様式を使用しなかった場合の罰則などはあるのか。 9 PDF のみで様式は提供されるのか。Office などのデータ形式での提供もあるのか。その場合 Office がない場合はどうしたらよいのか。印刷したものに手書きしてスキャンするなどの運用が想定されているのか。 10 本報告はなぜ PDF での報告様式であるのか。フォームで入力するホームページなどは作成されないのか。	1. 様式中に記載のとおり、報告時点で判明している内容について記載を求めております 2. DDoS 攻撃事案及びランサムウェア事案については、サイバー攻撃であることがインシデント発生時から明白であることが多く、その件数も多いため、これらの攻撃を対象としているものです。 3. 提出先の機関において、行政文書として適切な取り扱いが行われるものと考えます。 4. 各行政機関において、把握すべき事柄は異なっており、個別の問い合わせはあり得るものと考えます。 5. 各行政機関において、把握すべき事柄は異なっており、追加での問い合わせはあり得るものと考えます。 6. 本意見募集では、「サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ」（令和 7 年 5 月 28 日）における様式を対象としており、運用開始に当たってご指摘のような点については修正を行います。	○

		7. 提出先の機関に対して必要な手続きを行っていただくこととなります。 8. あくまで本様式も使用可能であることを申し合わせています。 9. エクセル様式での公表を想定しています。 10. 今後、報告窓口の一元化に向け、所要のシステム整備を進める予定です。	
13	■DDoS 攻撃報告様式について 1. 項目(3)影響を受けたシステムの稼働状況の選択肢について ・経験上、そもそも「影響なし」なら報告(＝情報共有)の必要はない、と考える組織が多いので、「影響が実質的になかったとしても、サイバー攻撃を受けて対応が必要になった場合は報告すること」など、表現を工夫する必要があると感じています。 また、影響た対処状況について暫定対処と根本対処の区別ができない組織が多いので、選択肢も下記のような分類があると、IT に疎い人でも整理・回答しやすくなるのではないかと思います。 ------ (1)システムへの影響 i.システムのスローダウン(性能は低下したが機能自体は使える)→ 一部 or 全部 ii.システムの機能不全(動作不良・機能不全)→ 一部 or 全部 iii.システム全体の停止(データの損壊や処理場の不整合などは無し) iv. システム全体の停止(データの損壊や処理場の不整合などを伴う) (1)システムの稼働・復旧状況 i.稼働継続中(特段の措置等も無く、自然復旧) ii. システムの一部を停止中 iii. システムの全体を停止中 iv. 復旧済み(正常稼動中) ------ 2. 項目(4)送信元情報 について ・IT に疎い組織だと src と dst の区別を間違って回答することがあるので、「送信元」とするよりも「攻撃元」としたほうが、何を書くべきか直感的に伝わるのではないでしょうか。 また、(3)の「通信プロトコル」も、「攻撃に使われたプロトコル」として本項に纏めたほうが整理しやすいのではないでしょうか。 ・「送信元の機器・ボットネットワーク」を記述せよ、と言われても、何をどう調べてどう書けばよいのかまで分からない人が多いと思います。	今後、本様式の運用を開始する際、ご指摘も踏まえ記入例を公表するなど、分かりやすい対応に努めてまいります。また、項目については、関係法令で報告を求めている事項との整合も踏まえ、政府としての対処・分析に必要十分な情報を設定しているものであり、実際の運用状況やいただいたご意見も踏まえ、適宜見直しを行ってまいります。その他のご意見については、今後の施策の参考とさせていただきます。	－

	具体的に何をどう調べ、どう書けばよいのか、例示など丁寧なガイドが必要ではないでしょうか。 3. 報告事項について ・DDoS 攻撃は、本質的・究極的には防御・予防は不可能な攻撃ではありますが、対策ノウハウの共有のためには下記の情報も求めた方が良いのではないでしょうか。 a. 暫定対処の内容（当該システムに対する対症療法） b. 根本対処の内容（当該システムに対する根治療法） c. 再発防止策（今後に向けた被害の予防策や、自社内での横展開の内容） 一方で、根本対処や再発防止策は「なし」や「暫定対処で包括」なども有り得えるので、それらも選択肢にいれるなどしてはいかがでしょうか。 4. 今後の対応/(3)本様式の届出先・報告の根拠規定等 ・自由記述ではなく、手引1・（1）に有る選択肢を並べ該当するものを■やvにする方式の方が記入しやすいのではないでしょうか （ランサムウェアの報告様式はそうなっているようでしたので）。 ・また、法令も業種・業態ごとの分類（インデックス）を付けるなどして、ひと目見て選別しやすくしていただけると幸いです。 ・業種・業態ごとに見る必要がある法令も異なってくるので、選択肢が多くなりすぎるようであれば別紙等で選択しやすくナビゲートするのが良いのではないでしょうか。 ■ランサムウェア攻撃報告様式について 1. 項目 4.(2)ランサムウェアの類型の記述要領について ・暗号化の有無などの前に、「推定あるいは特定されたランサムウェアの名称・種別」の記載を求めたほうが、記述する側も思考を整理しやすくなると感じました。 経験則として、ランサムウェアの種別特定もしないまま対症療法的にバックアップからレストアしてしまい、真因を確認・根絶することができないままになってしまうことがあります。 基本的にはランサムノートや暗号化されたファイルの拡張子、対策ツールによる解析などで分かるはずの情報なので、欄として独立させたほうが漏れが出にくくなると思います。 ・後段の(5)ランサムウェアの特長との重複感もあるので、項目としてまとめた上で、記入を求めるべき事項を箇条書きにしておく（記入欄として独立させておく）などしたほうが、書き手の抜け漏れを防ぎやすいのではないでしょうか。 2.「今後の予定」について ・項題に対し、選択肢に違和感と分かりにくさを感じました。例えば下記のようにしたほうが、IT に疎い人でも理解しやすくなるのではないでしょうか。 --- （2）現在の状況：事象（障害）継続中、暫定復旧済み/恒久策を継続中、恒久策まで完了、再発防止		

	策まで完了、 （3）今後の予定：暫定復旧見込み：_____頃、恒久復旧見込み：_____頃 --- 3.（8）再発防止のための措置　について ・経験的に、「根本措置」と「再発防止策」の区別が適切に付けられておらず、場当たり的対症療法の事を発防止策と称している業者が非常に多いと常々感じています。 正しい理解を促すためにも「根本措置：事象から復旧させるための措置」と「再発防止策：今後、類似の事案を当該システムだけでなく他のシステムでも起こさなくするための組織的・構造的な対処」との2欄に分けて記入を求めるのがよろしいのではないでしょうか。 4. 別紙 3.（5）発生原因 / 原因の選択肢について ・選択肢が「不正アクセス」の 1 つだけであれば、必ず■になってしまうので、意味がない項目担ってしまうのではないでしょうか。 基本的に、マルウェアの送り込みも脆弱性をついた攻撃もアカウントジャックも全て「不正アクセス」に該当しますので、統括室が定める不正アクセスとは〇〇行為のことである、という定義があるのであれば、それを明記していただくのがよろしいかと思います。 例えば、攻撃箇所/攻撃手法の自由記述欄のみにするか、下記のように具体的・端的な選択肢を列挙するほうが良いのではないでしょうか。 --- □PC へのマルウェア汚染 □PC やサーバ、ネットワーク機器の脆弱性を突いた侵害 □各種機器やクラウドサービスへのなりすましログイン(アカウントジャック)、 □フィッシング等による認証情報の窃取 □サポート詐欺による遠隔操作 等々 ---- ■共通 4. その他全般について ・基本的に、担当監督省庁への報告内容との重複が非常に多く、内容的にはコピー（流用）で済むとはいえ、様式・書式が異なってくると結局打ち込みのし直しとなります。 そのため、報告する側としては二度手間・無駄手間を取らされてしまう感があります。業種ごとの監督省庁（当局）に提出する際も、すべてこの様式で統一されることを望みます。 ・この報告をすることで、報告者（被害者）が得られるインセンティブについて、強くアピールしていただけないでしょうか。		

	明確なインセンティブが何もなく、「社会貢献」「社会的義務」は重要ですが、それだけだと「単に負担を強いられているだけだ」と感じる組織も少なくありません。 報告をすることで統括室から適切なアドバイスや支援が受けられる/対処の適切性を評価してもらえる、などといった「利点」を強調・明確化していただくことで、率先して報告しようとする気になってはもらえないのではないでしょうか。 以上、よろしくご査収・ご検討のほどお願い申し上げます。		
14	◯両書式について、不明なものについては不明と記載して良い事を明示願いたい。 ◯様式に報告期限（決定後）も明示願いたい。 ◯DDoS 発生時には他のサイバー攻撃も発生している可能性もあり、それらを考慮したフォーマットとする必要があり、自由記入欄を追加してもらいたい。	1．様式中に記載のとおり、報告時点で判明している内容について記載を求めております。 2．報告期限は提出先の機関の手続き毎に異なります。 3．その他の攻撃を受けている場合には（1）事案の概要や（3）事実経過にその旨を記載いただく方法で対応できると考えています。	－
15	(1) DDoS 攻撃に関しては、複数の組織に対して同時または連続して被害が及ぶ可能性が十分に考えられる。そのため、注意喚起を目的とした速やかな情報共有が強く求められる。しかし、現行の報告様式では実質的に即時性の高い報告が困難な状況にあることから、速報用と事後報告用の二つの報告様式を明確に分けて運用することが望ましい。 (2) 現在の報告様式は紙での運用を前提として設計されており、報告先機関の長の記載やチェックマーク、囲い枠の記入など、入力の負担が大きくなっている。デジタル庁等の専門家を交え、より効率的かつ実用的な様式への見直しを検討いただきたい。	今後、報告窓口の一元化に向け、所要のシステム整備を進める予定です。その他のご意見については、今後の施策の参考とさせていただきます。	－
16	1．段階的な報告プロセスと柔軟な訂正の仕組みの導入について サイバーセキュリティインシデントにおいては、被害の拡大防止と迅速な注意喚起のため、発生早期の情報共有が極めて重要です。しかし、インシデント覚知の初動段階では不明な点が多く、報告様式の全項目を正確に埋めることは困難です。 そこで、運用開始時における報告プロセスについて、段階的運用を提案いたします。まず「第一報」では、共有すべき最低限の項目（例：攻撃の発生日時、検知した事象、想定される攻撃種別など）に限定して迅速な報告を可能とし、その後の調査の進展に応じて「第二報」「第三報」として詳細情報を追加報告できる仕組みが望ましいと考えます。 また、初期の報告内容がその後の調査で覆ることは少なくありません。報告内容を訂正する場合も、報告者が簡便に対応できるような柔軟な仕組み（運用解釈など分かりやすい解説）を公表に併せて整備して頂けると幸甚です。	1．様式中に記載のとおり、報告時点で判明している内容について記載を求めております 2(1)．代表者名は法人番号と同様に基本的に公表情報であり、個人情報保護委員会の報告においても報告事項とされています。 その他のご意見については、今後の施策の参考とさせていただきます。	－

	2. 報告者の定義に関する柔軟な運用について 報告の迅速性と正確性を担保するため、報告者の定義について以下の点を考慮いただくよう申し上げます。 (1) 報告責任者の定義の柔軟化 報告者概要欄に「代表者名」の記載を必須とした場合、多くの企業では代表取締役等の署名に時間を要する社内承認プロセスが必要となり、報告の遅延につながる懸念があります。 インシデント報告における「代表者」とは、法的な代表権を持つ者に限定せず、「本報告に関する責任者」と位置づけ、情報セキュリティ担当役員（CISO）や担当部署の責任者等の名義でも提出可能とすることが、迅速な報告を実現する上で効果的と考えます。 (2) 調査担当事業者による代理・連名報告の許容 インシデントの原因究明等、技術的な詳細については、調査を担う外部のサイバーセキュリティ専門事業者が最も正確に状況を把握しています。 そのため、報告様式に、被害企業とは別に「調査担当事業者」の名称や担当者名を併記する欄を設け、技術的な項目については当該事業者が代理で記載・報告することも許容するような運用をご検討頂けると幸甚でございます。 3. 報告の信頼性向上と専門人材の活用について 報告内容の正確性と信頼性を担保するための方策として、「情報処理安全確保支援士（登録セキスペ）」の活用を提案いたします。情報処理安全確保支援士は、法律に基づく国家資格であり、最新の知識・技能の維持や高い倫理観が求められます。報告書の確認者として同資格保有者の署名を求めることで、報告内容の信頼性が向上すると考えます。また、これは同資格保有者にとって具体的な役割を創出することにもつながり、我が国全体のサイバーセキュリティ人材の育成・確保にも資する施策となり得ると理解しております。 4. その他 本制度の検討にあたっては、経済産業省「産業サイバーセキュリティ研究会 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」の報告書等で示されている「攻撃情報の早期共有」の理念も参考に、より実効性のある制度設計が進められることを期待いたします。		
17	1. ランサムウェア事案共通様式 「ランサムウェア事案共通様式」では、内閣サイバーセキュリティセンターへの共有等を希望しない選択が可能となっているが、当該希望をしないケースとしてどのような場面が想定されているか。 （理由） 「ランサムウェア事案共通様式」で設定された設問の趣旨を確認したい。 2. ランサムウェア事案共通様式 「ランサムウェア事案共通様式」冒頭にある「2. ランサムウェア感染時のお願い」において、初期対応のみならず例えば以下のような形で復旧までの対応を記載いただきたい。	1. 例えば別紙 1,2 の個人情報保護委員会への報告項目を NCO への共有を希望しない場合が想定されます。 2. 本様式はあくまで報告様式であり、ランサムウェア感染への各対処については他のガイドラインを参照すべきところ、被害を拡散させないように初期対応についてのみ留意事項を記載しているところです。	－

	また、現時点で初期対応についてのみ記載されている背景について、ご教示いただきたい。 「封じ込め（被害拡大防止）」 ・感染が疑われる機器類を速やかにネットワーク（有線・無線）から切り離すこと ・感染が疑われる機器類や、当該機器類からアクセス可能なシステム（特に個人情報を含むもの）について、認証情報の変更または一時的なアカウントロックを実施すること（ネットワークから切り離してしまい対応不可の場合は、復旧時に対応すること） 「証拠保全」 ・後続の詳細な調査（フォレンジック調査）において、十分な調査をするために証拠保全をする必要がある。以下の操作を行うと、証拠が保全できない可能性がある。 −感染端末等の再起動や電源オフ、既に感染端末等の電源がオフの場合はオン −ウイルス対策ソフトによる感染端末等のフルスキャン −ネットワーク機器の再起動や電源オフ −ファームウェアや OS のアップデート 「フォレンジック調査」 ・ランサムウェア攻撃に関する詳細な調査（フォレンジック調査）は、自社のみでの対応は困難であるため、信頼できる外部の専門機関に依頼すること。 「接続再開方針策定・復旧」 ・フォレンジック調査の結果をもとに根本原因を特定し、再発防止策を策定したうえで、自社および接続先の合意を得てからネットワーク接続を再開すること。 （理由） ランサムウェア感染時においては、初期対応のみならずその後の対応においても速やかな対応が必要であり、その明示をすることで被害組織の対応が円滑となると考えるもの。		
18	項番 1 該当する様式:DDoS 事案共通様式およびランサムウェア事案共通様式 意見・質問等:被害組織の報告負担の低減という目的に鑑みると、本様式で報告した事象については、障害発生等報告書（金商業者向け監督指針　別紙様式3−1）で報告すべき事案であっても、障害発生等報告書の提出は不要となる認識でよいか。 項番 2 該当する様式:DDoS 事案共通様式およびランサムウェア事案共通様式　1ページ 意見・質問等:本様式に基づいて報告すべき事象であるかを判断するにあたっては、「金商業者向け監督指針−11 システムリスク管理態勢−報告すべきシステム障害等」に記載される以下を基準に考え	1. 記載の手引きの通り、追加的な報告事項の有無については、各法令等に従う必要があります。 2. 記載の手引きの「本様式の対象となる手続」が報告の対象となります。 3. スローロリス攻撃や RUDY 攻撃は(2)攻撃類型の Network Denial of Service（T1498）として報告するものと考えます。	−

	てよいか。 （なお、障害が発生していない場合であっても、サイバー攻撃の予告がなされ、又はサイバー攻撃が検知される等により、顧客や業務に影響を及ぼす、又は及ぼす可能性が高いと認められる時は、報告を要するものとする。） 項番 3 該当する様式:DDoS 事案共通様式　3ページ 意見・質問等:3ページ目の攻撃類型の分類のとおり、本様式の報告対象となるのはあくまで DDoS 攻撃のみと考えてよいか。たとえば通常の DoS 攻撃やスローロリス攻撃、RUDY 攻撃のように DDoS 攻撃ではないがサービス不能攻撃に分類される攻撃は本様式の対象外と考えて良いか。 項番 4 該当する様式:DDoS 事案共通様式およびランサムウェア事案共通様式 意見・質問等:例えば SQL インジェクション攻撃など、DDoS 攻撃およびランサムウェア攻撃のいずれにも該当しない類型のサイバー攻撃については本様式の対象外であり、従来の報告様式に沿った報告が必要と考えて良いか。	4. DDoS 攻撃事案及びランサムウェア事案については、サイバー攻撃であることがインシデント発生時から明白であることが多く、その件数も多いため、これらの攻撃を対象としているものです。その他の攻撃については、必要な場合には従前の方法で報告いただくこととなります。	
19	【該当箇所】 ランサムウェア事案共通様式 4. 攻撃技術情報 に関して 【意見概要】 重要インフラ、基幹インフラにおいては、4. 攻撃技術情報に関して、後述の詳細な報告を求めるようにして頂きたい。 詳細な報告を基に、内閣サイバー統括室から広く国民にランサムウェア対策案を公表し、被害の低減につながるよう広報活動をして頂きたい。 【意見内容】 サイバー攻撃に係る被害組織の負担を軽減し、政府の対応迅速化を図るため、報告のあり方について検討がなされていることについて、大いに賛同するところです。 一方で、過去のランサムウェア事案においては、ランサムウェア事案防止の観点での、侵入経路、攻撃手法、復旧対策等に関する詳細な共有がなされておらず、国、所轄官庁等からも、明確な指針、対策も明示されていません。一部、政府関連組織では、ネットワークの即時遮断に関して、慎重な検討を要する等、ミスリーディングな広報を行っている状況にあり、国としての統一的な対応措置や復旧における注意点を早急に共有すべき事態にあります。 他方、フォレンジック調査はサーバー1 台 400 万円との見積実績もあり、詳細なフォレンジック調査を求めた場合、中小～中堅企業にとっては、経営上の大打撃となるところです。 そこで、重要インフラ、基幹インフラに限っては、 金銭的な被害額と技術的な詳細な報告を求め、国が公表することで、	項目については、関係法令で報告を求めている事項との整合も踏まえ、政府としての対処・分析に必要十分な情報を設定しているものであり、実際の運用状況やいただいたご意見も踏まえ、適宜見直しを行ってまいります。その他のご意見については、今後の施策の参考とさせていただきます。	－

	1.具体的な被害額の共有による、国民のサイバーセキュリティに関する関心を高め、かつ自分事とすること、 2.広く国民に向けて、実際の侵入方法を基にした実効性の高い対策の呼びかけや、注意喚起の広報ができること、 3.重要インフラ、基幹インフラにあたっては、他山の石をもって、具体的かつ即効性のある対策が講じられる効果が期待できる、 と考えます。 特に具体的な侵入方法の共有は、ランサムウェア攻撃に即効的効果が期待でき、システムやネットワークの設計において重要な指針となり、全国の SIer、ネットワークベンダー、IT 事業者、サイバーインフラ事業者にとって極めて有益な情報となります。 【要望内容】 重要インフラ、基幹インフラにおけるランサムウェア攻撃については、最低限、以下の内容の報告を求めるようにして頂きたいと要望致します。 被害内容と影響範囲　暗号化されたデータの種類　ファイルサーバー、バックアップ、Active Directory など 被害内容と影響範囲　暗号化対象の台数　PC、サーバー、NAS、クラウドサービス、制御機器、医療機器等含む 被害内容と影響範囲　データ漏洩有無（ダブルエクストーション）　データ流出の有無と種類（顧客情報、機密など） 被害内容と影響範囲　業務停止の有無・時間　可用性被害の影響評価 被害内容と影響範囲　復旧にかかった時間・費用　経済的損失評価のため 被害内容と影響範囲　ランサム要求額　要求ビットコイン量 or 日本円換算額 被害内容と影響範囲　支払の有無・支払額　傾向や再被害リスク分析に使用 感染経路・攻撃手法　初期侵入ベクター　フィッシング、RDP、VPN、ゼロデイ、USB など 感染経路・攻撃手法　攻撃者の持続手法　C2 通信、レジストリ常駐、タスクスケジューラー、Auto Run など 感染経路・攻撃手法　lateral movement 手法　PsExec、WMI、RDP 横展開、AD 認証悪用など 感染経路・攻撃手法　エクスプロイト対象　CVE 番号、脆弱な製品名（例：Citrix、FortiGate） 感染経路・攻撃手法　感染した OS やバージョン　被害の多いプラットフォームの把握用 技術的情報　ランサムウェア名／ファミリー名　LockBit、BlackCat、Clop、Conti 等 技術的情報　ランサムノート　TOR リークサイトの URL 等 技術的情報　使用されたファイル名／拡張子　lockbit、8base など		

	技術的情報　通信先（C2 サーバーIP／ドメイン）　通信分析と封じ込め対策に重要 技術的情報　残存ツールの言語　使用言語、攻撃者属性 運用　エンドポイント対策状況　EDR/AV 導入状況と挙動ログ取得有無 運用　セグメントの有無・状態　横展開の抑止度評価 運用　バックアップの有無・被害状況　被害からの復元可能性の指標 運用　被害端末・サーバーでの脆弱性管理状況　悪用された脆弱性 運用　被害端末・サーバーでの管理者権限の付与状況　特権の使用状況、脆弱性による特権昇格の可能性 運用　管理者 ID とパスワードの使いまわし状況　水平展開の原因		
20	1 DDoS 事案共通様式（案）・ランサムウェア事案共通様式（案） 報告対象事案の範囲 委託先システムについて、攻撃技術情報等の情報は持ち得ていない場合が多く、報告することが困難である。 2 DDoS 事案共通様式（案）・ランサムウェア事案共通様式（案） 報告様式・手段 迅速な情報連携を目的に、当該様式で提示されている項目について電子メール本文で報告することを許容いただきたい。また、当該方法での報告が許容される場合、メールにて報告する場合のメールの件名などの指定があれば提示いただきたい。 3 DDoS 事案共通様式（案）・ランサムウェア事案共通様式（案） 予備報告手段 報告手段については、当面は現状通りメール、将来的には「報告受付システム」で行う形が想定されていると認識しているが、ランサムウェア攻撃等によりメールや Web ブラウザが利用できない状況も想定し、そのような場合でも報告ができる予備手段（電話など）も準備することも有効ではないか。 4 DDoS 事案共通様式（案）・ランサムウェア事案共通様式（案） 報告回数の表記欄の新設 報告回数の明確化の観点から、何回目の報告かを表記する欄（第 1 報、第 2 報など）を設けてはどうか。 5 DDoS 事案共通様式（案）・ランサムウェア事案共通様式（案） 1.記載の手引き 「記載の手引き」が様式の１頁目にあることで、迷わずに記載可能となるかもしれないが、記載後に1頁目を見ても報告者がわからないなど、内容把握の支障になることも考えられる。「記載の手引き」については、例えば最終頁におくなど、記入領域と明確に分けた方が把握しやすいのではないか。	1．様式中に記載のとおり、報告時点で判明している内容について記載を求めております。 2　具体的な使用方法は、それぞれの手続きに係る法令、ガイドラインや各省庁が公表する方法に従うこととなります。 3．具体的な使用方法は、それぞれの手続きに係る法令、ガイドラインや各省庁が公表する方法に従うこととなります。 4．提出先の機関において、適切に報告回数は管理されると考えています。 5．内容を確認する提出先の機関において、円滑に把握できると考えています。 6．項目については、関係法令で報告を求めている事項との整合も踏まえ設定しており、様式によって差分が生じているものもございます。 7．項目については、関係法令で報告を求めている事項との整合も踏まえ設定しており、様式によって差分が生じているものもございます	○

	6 DDoS 事案共通様式（案）・ランサムウェア事案共通様式（案） 1. 報告者の概要 「報告者の概要」の記載粒度が DDoS 事案共通様式（案）とランサムウェア事案共通様式（案）で異なるが、記載内容を統一いただきたい。 7 ランサムウェア事案共通様式（案） 5.今後の対応 (2)今後の予定 当該欄の選択肢のうち「事象継続中」の意味がイメージしにくい。「今後の予定」としては対応策が開始される（している）ことが通常と考えられるので、「事象継続中」を削除するか、「対応策を検討中」等に変更してはどうか。 8 ランサムウェア事案共通様式（案） 別紙1 (1)報告の種別 「別紙 1 個人情報取扱事業者における個人データの漏えい等に係る項目」には、「(1)報告の種別」において「速報」「中間報」「確報」の 3 種類が記載されている一方、「ランサムウェア事案共通様式」においては、そのような区分はないので、統一いただきたい。 9 DDoS 事案共通様式（案） 4.攻撃技術情報 MITRE ATT&CK のテクニックについて唐突に記載されている印象がある。記載の分類は ATT&CK のテクニックから抜粋等の補記が必要ではないか。	8. 項目については、関係法令で報告を求めている事項との整合も踏まえ設定しており、様式によって差分が生じているものもございます。 9. 頂いたご意見も踏まえて、MITRE ATT&CK を参照している旨を追記いたしました。	
21	【意見】 〇サイバー攻撃を受けた際、「公表の実施状況」に関して、二次被害等抑止のセキュリティの観点から、サイバー攻撃ではなく、 システム障害として公表することで、公表済みと整理することは可能との理解で良いか。 〇（DDoS 攻撃・ランサムウェア 両方の共通様式について） 官公署への報告事項として記入が必要な項目と NISC への情報共有として任意で記入する項目が明確に判別できるようにしていただきたい。 〇（ランサムウェア共通様式について） 記載の手引き「2.ランサムウェア感染時のお願い」で「（初期対応時に）再起動や電源オフをしない」「フルスキャンをしない」等 記載されている。感染時の対応手順は組織やシステム環境等で異なるので、「お願い」ではなく、一般的な「留意事項」とした記載いただきたい。	1. 個別の事案について一概には申し上げられませんが、その旨をご記載いただくといった運用が考えられます。 2. 具体的な使用方法は、それぞれの手続きに係る法令、ガイドラインや各省庁が公表する方法に従うこととなります。 3. ご意見を踏まえて修正いたしました。	〇

22	サイバー対処能力強化法の趣旨に則り、官民連携強化の一歩として、以下の通り意見を申し上げます。 1.報告様式はシンプルかつ直感的な UI 設計とし、報告率向上と将来的な一元化への発展的基礎となることを期待します。 2.攻撃元 IP、手法、痕跡情報など、被害企業が重要と考える脅威情報を容易に共有できるよう、任意記入欄を十分に確保してください。初期報告は必要最低限の情報を必須とし、詳細報告は脅威インテリジェンスとして有用な情報を任意項目として後日追記・修正可能な仕組みとすることで、迅速性と確実性を両立できることを期待します。 3.被害報告後にフィードバックが得られる体制を整備し、報告者が積極的かつ継続的に協力できる仕組み形成を期待します。 4.報告窓口の一元化においては、情報共有の迅速化のため、民間の SOC や CSIRT と政府機関との自動連携を可能とする API の整備と標準化を検討してください。主要なセキュリティ製品やクラウドサービスとの連携を想定した API 標準仕様の策定・公開をお願いします。 5.報告時のプライバシー・機密情報の取り扱いに関する明確なガイドライン提示と、匿名化・非特定化に関する技術的基準や手続きの明示、信頼性の政府担保により、企業が安心して報告できる環境整備を期待します。 6.サイバー対処能力強化法に基づく無害化措置と収集情報との連携を踏まえ、情報が即時対応に活用される仕組みの構築を提案します。米国 CIRCIA 等を参考に、報告組織に対する法的保護・免責措置の導入、風評被害への対応も検討ください。 7.今後の様式拡張に備え、インシデント種別に関する分類枠（taxonomy）の策定・共通化を進めてください。 8.各報告項目に対し標準的なタイムライン情報（発見・報告・初動対応など）の付与項目を設定いただくと、初動分析や対応評価の精度向上に資するものと考えます。 9.報告された情報の政府内での共有範囲や、分析・研究等での二次的な利用方針についても透明性を持って示してください。	今後、報告窓口の一元化に向け、所要のシステム整備を進める予定です。その他のご意見については、今後の施策の参考とさせていただきます。	－
23	DDoS 攻撃事案共通様式（案） ランサムウェア事案共通様式（案） 記載の手引1.（1）本様式の対象となる手続き 現在、事務ガイドライン第三分冊：金融会社関係(5前払式支払手段発行者関係)Ⅱ－3－1－2に基づき、障害発生時には所管省庁へ障害発生等報告書を提出しているが、ランサムウェア事案共通様式及びDDoS攻撃事案共通様式を用いれば、現行提出している報告書は不要という認識でよいか。	関連資料「サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ」の通り、本様式は、各報告等を用い、又は別途法令等で定める様式に添付する形での報告を可能とするものです。具体的な使用方法は、それぞれの手続きに係る法令、ガイドラインや各省庁が公表する方法に従うこととなります。	－
24	＜要旨＞ ・該当文書： 全体 ・該当箇所： 全体	1．いずれも、各ページの冒頭に「報告をしようとする時点で把握している範囲で、その内容を記載すること。」と記載しています。また、今後、本様式の	－

	・意見内容: 統一フォーマット案の提示ありがとうございます。 今回の統一フォーマットはこの先の報告一元化に向けた第一ステップとして、現行の複数ルール・複数報告先のもとで、まずフォーマットのみを共通化するものと理解します。 しかし、提示案は現行の異なるフォーマットの「寄せ集め・和集合」となっているため、企業側にとっては負担減となりません。 加えて、報告目的とフォーマットの齟齬が生じるため誤解を招きやすくなっています。 結果として、現案のままでは、企業の実運用の現場では現状よりも利便性が悪化する恐れがあります。 今回はあくまで第一ステップではありますが、その先にある報告一元化を見込んだフォーマット統一として頂くことをお願い致します。 そのため、まず、報告一元化に向けては以下の 2 点が重要な考慮点となることをご理解ください。 ①報告内容が意味のある官民情報連携に繋がること。具体的には、報告を受けて分析を行う政府側の分析ケーパビリティを念頭に置いた内容とすること。現状の政府の分析ケーパビリティを越えた情報の収集は避けて頂きたく思います。 無論、政府の分析ケーパビリティも徐々に向上しますので、それに伴って報告情報もリッチにしていくこととなりますが、まずは現状に即した内容としていただくことが企業の現場に不要な負荷を与えない点で肝要です。 ②報告のタイミング。おそらくは初報、続報など時系列の中で充実した報告内容とする工夫が必要と想定致します。 初報は軽く、続報は内容詳細に、などのメリハリが必要と思われます。これもサイバー攻撃対処に追われる企業の現場の負荷を考慮したものとする必要があります。 今回のフォーマット統一の先においては、上記2点を考慮した報告一元化を進めて頂きたく存じます。 以上2点を念頭に置いた時、今回第一ステップにおいても、以下の改善点を提案いたします。 ・「すべての項目を報告しなくて良い」という注記を目立つ場所におくことで、「全部を埋めなくて良い」ことを認知されやすくする ・報告の対象となるインシデントをより具体的に明示すること ・今回の統一フォーマットが先々の報告一元化後の「初報用」になる可能性が高いことを考えると、出来る限り簡素にすること ・理由: せっかくの「報告一元化」の取組み第一歩が、企業側に失望を生むものとなることを避け、先々に期待を抱かせるものとするため 以上を全体要旨としまして、今回第一ステップとしての各文書に関してご意見いたします（4つ）。 ＜意見1＞	運用を開始する際には、分かりやすい対応に努めてまいります。 2. 政府としての対処・分析に必要十分な情報を設定しているものであり、実際の運用状況やいただいたご意見も踏まえ、適宜見直しを行ってまいります。 3. 本様式は、各報告等を用い、又は別途法令等で定める様式に添付する形での報告を可能とするものであり、具体的な対象事案等は、それぞれの手続きに係る法令、ガイドラインや各省庁が公表する方法に従うこととなります。 4. 本様式は、各報告等を用い、又は別途法令等で定める様式に添付する形での報告を可能とするものであり、具体的な対象事案等は、それぞれの手続きに係る法令、ガイドラインや各省庁が公表する方法に従うこととなります。	

	・該当文書：ランサムウェア事案共通様式　および　DDoS 攻撃事案共通様式 ・該当箇所：「※1　いずれの項目も、全ての項目を記入する必要はなく、報告をしようとする時点で把握している範囲で、その内容を記載すること。」 ・意見内容：文書の途中でなく、初めのわかりやすいところに明示してほしい。 ・理由： この前提条件をはじめに読み込めなければ、被害組織の大幅な負担増となるため。 ＜意見2＞ ・該当文書：ランサムウェア事案共通様式　および　DDoS 攻撃事案共通様式 ・該当箇所：文書全般 ・意見内容：初動報告として、必要最低限の項目に絞ってほしい。 ・理由：既存様式を単純に足し合わせた結果、報告ボリュームが増えており、かえって被害組織の負担増となるため。（従前は初動で必須としなかった項目が増えており、初動時の被害組織の負担増となるため。） 初動以外の部分（技術的に詳細なヒアリング事項群）については、必要となるタイミングも区々であると思われるため一律のヒアリングとせずに、削除してしまうか、参考などに切り出してはどうか。 ＜意見3＞ ・該当文書：ランサムウェア事案共通様式　および　DDoS 攻撃事案共通様式 ・該当箇所：文書全般（様式を用いる状況について） ・意見内容：報告対象となるインシデントの条件を明確にしてほしい。 ・理由：例えば、電気通信事業者の場合、本施策の対象が以下のどの場合に適用されるか不明確。 ①「特定重要設備（および特定重要電子計算機）」 ②それ以外の電気通信設備 ③電気通信事業以外のシステムやビジネス インシデントが発生した箇所により、様式や報告ルートが異なった場合、現場は大混乱となる。報告すべき対象が一元化（同じルート・手順で報告を行う）されていることが理想。 ＜意見4＞ ・該当文書：DDoS 攻撃事案共通様式 ・該当箇所：文書全般 ・意見内容：報告対象となる条件（意義やメリット、タイミング）を明確にしてほしい。特に電気通信事業者は、DDoS を対象とする報告様式とルートが別に既にあり混乱するため、必要とされる報告のみに絞ってほしい。 ・理由：・電気通信設備につながらない事象（故障等）が発生した場合、その原因に依らず総務省に報告することになっているが、その原因が DDoS と判明した場合に、本様式を追加で用いるのであれば、かえって現場の負荷があがり混乱すると思われる。 　全ての DDoS について、NCO が詳細調査を行う稼働は割けないと想定され、であれば詳細報告は		

	求めるべきでない。本様式で DDoS 報告することの意義やメリットがわかると、いつ・何を報告すべきかが理解されるのでは。 　なお、通信の秘密に抵触するため電気通信事業者の立場で通信内容（DDoS か）を判断することはできず、通信事業者の立場で　本様式が用いられることは無いと考えます。		
25	いずれも、特別の言及がない限り、いずれの様式案に対しても共通して意見する次第です。 ・関係各省申し合わせにて「特に、DD o S攻撃事案及びランサムウェア事案については、サイバー攻撃であることがインシデント発生時から明白であることが多く、初動対応中の報告となり、その件数も多いことから、被害組織の報告負担が極めて大きいと考えられる」と記載されているように、両類型は攻撃が現在進行形で行われている状況での報告が求められるケースが多いため、初報、続報と細切れ・断続的な報告にならざるを得ないところ、フォーマットの注書きにもその旨記載があるが、報告のタイムラインを示すなど、もう少しわかりやすくその旨示す必要があると考えます。 ・「外部機関による調査の実施状況」項目があるところ、より正確な記載を行うべきと考えます。具体的には、専門組織名（セキュリティ専門企業、JPCERT/CC 等）、公的機関名（IPA 等）の記載や、初動対応相談なのか、フォレンジック調査なのか、情報共有（のための調整依頼）先なのか、あるいはセカンドオピニオン調査なのかといった区分の記載が必要と考えます。インシデント対応は多くの組織が初めての経験であるところ、場合によっては当該攻撃類型に対して適切な対応知見を持たない組織に相談してしまっているケースも多く、行政側の第一報報告の段階で軌道修正することが可能であると考えます。 （ただし、被害組織がこれを望まない場合は除きます。） （本論点は「産業サイバーセキュリティ研究会 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」にて検討しており、ご参考ください） ・被害組織の負担を増やしているポイントの一つとして、報告先窓口機関が当該攻撃類型／事象について、知らない／理解が至っていない技術的な点について、当該被害組織に問い合わせてしまうことが挙げられます。個別の被害内容については別として、当該攻撃手法等に関する情報については、同様の報告を受けて対応している他の公的機関や専門機関（JPCERT/CC）に問い合わせる方が推奨されます。よって、当該攻撃類型について、どこに問い合わせればよいかを報告受付機関側が把握できるよう、上記の通り、相談・届出先組織名の記載が必要と考えます。 ・ランサムウェア攻撃については、行政機関への報告だけ行われ、情報共有活動への照会／共有がなされず、当該被害調査に係る情報が不足したまま調査が行われたり、情報共有不足にて他の攻撃被害が放置されるケースが散見されており、情報共有活動への対応有無についても上記同様、記載がなされ、行政機関側で対応状況を把握できるようにするべきと考えます。（ただし、被害組織がこれを望まない場合は除く）	今後、本様式の運用を開始する際、ご指摘も踏まえ記入例を公表するなど、分かりやすい対応に努めてまいります。その他のご意見については、今後の施策の参考とさせていただきます。	－

	また、被害組織がこの報告記載内容をもってして、受付機関または内閣サイバーセキュリティセンターを通じて、サイバーセキュリティ協議会等への情報共有を希望する場合は、その旨を記載する項目が必要と考えます。 ・上記、情報共有等については、そのための情報の加工方法や手順等、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」、「攻撃技術情報の取扱い・活用手引き」に記載があり、これらの案内の記載が必要と考えます。 ・被害情報を各所管省庁が収集する点については別として、攻撃に関する情報を集約して、これを公的機関側はどのように活用するのか示されていません。被害組織側の納得感を得て、よりタイムリーな情報のやりとりが行えるよう、「なぜ攻撃情報を集めるのか。情報をどのようの加工・分析・活用するのか」という点についてより具体的に示すべきと考えます。 ・IPA の「コンピュータウイルス・不正アクセスに関する届出」について今回の対象外とした旨の説明をなんらか示すべきではないかと考えます。 （IPA 側ホームページにおいて、情報セキュリティ安心相談窓口への相談とは別として掲載がなされています） ・攻撃技術情報、特に IP アドレスやログ情報等については、記載時の誤操作や受領側での扱いによる事故等を考慮して、多数かどうかにかかわらず、別ファイル（様式外）での提出を可能にすべきと考えます。		
26	掲題の件、「被害報告一元化に関する DDoS 事案及びランサムウェア事案報告様式」（案）に関する意見の募集について、弊社の意見を提出させていただきます。 現在の情報連絡様式では NISC さま→事業者への情報共有の役割も担っていると考えております。 被害報告一元化に移行するにあたって、国からの情報共有の方法についても整理をいただけますと幸いです。 移行期間中の国からの情報提供について明確にしていただき、混乱が生じないようご配慮をお願いいたします。 意見対象の文書、該当ページ、該当箇所はございませんが、ご了承ください。	今後の施策の参考とさせていただきます。	
27	1.「ランサムウェア攻撃事案共通様式」に関して （1）「ランサムウェア感染時のお願い」に記載の対応策については、オンプレの機器を想定した対策が記載されているとの理解でよいでしょうか。想定している環境下を明記するとともに、事業者によっては記載の対応策が必ずしも該当しない（例：クラウド事業者の場合はオンプレ環境のための対応策は該当しないなど）場合もあるため、事業者の判断で柔軟な適用が認められるような記載ぶりについてご検討いただけますよう希望します。	1. ご意見も踏まえて、「お願い」を「留意事項」に修正しています。 2（1）. 本様式は、各報告等を用い、又は別途法令等で定める様式に添付する形での報告を可能とするものであり、具体的な対象事案等は、それぞれ	○

	2.「DDoS 攻撃事案共通様式」と「ランサムウェア攻撃事案共通様式」の双方に関して （1）本様式自体は、それぞれ「（1）本様式の対象となる手続」に挙げられる各業法やガイドライン等に規定される報告手続のタイミングや報告事項を変更させるものではないことを確認させてください。 （2）「具体的な提出先や提出方法、追加的な報告事項の有無については、各法令、ガイドラインや、各省庁が公表する方法に従うこと。」とありますが、各省庁がこの様式も踏まえて所管の報告手続の運用方法を変更する場合は、特に初動対応においては事業者がインシデントそのものへの対応に全力を挙げる必要があることも念頭に、円滑な官民連携が可能な運用としていただくことが重要です。そのため、検討にあたっては関係業界とも十分な双方向の議論を実施するよう、国家サイバー統括官室から各省庁にも周知いただくことを要望します。 （3）グローバルに事業を営む企業においては、インシデントレポートはまずは英語で作成され、その後に影響があった各国の言語への翻訳版を至急作成するという流れも一般的です。そのため、本様式は速やかに英語版も公表されることを希望するとともに、特にインシデントの初動対応中において、できるだけ迅速に報告が実施できるよう、英語による報告も容認いただくことを要望します。 （4）今後、サイバー対処能力強化法及び同整備法の施行規則による特別社会基盤事業者（及び間接的にそれへの重要電子計算機等供給者）や重要電子計算機等供給者に対する報告義務の制度設計に伴い、報告様式の再改定（本様式の再修正と新たな様式の作成）が予定されているとの理解でよろしいでしょうか。その場合、既存の報告義務含めた報告制度全体において官民連携の円滑化が実現するよう、国家サイバー統括官室から重要電子計算機等供給者含む関係者に対して制度設計の全体像を示し、双方向の議論を実施していただけるよう要望します。 3. 報告受付システムの運用に関して （1）報告内容の漏洩はさらなる被害拡大や各社機密情報の漏洩に繋がりうるため、万が一にも漏洩が無いようシステム・関連制度ともに綿密に設計していただくことを要望します。特に、報告受付システムで受け付けた各種報告は、担当部局の業務上当該報告へのアクセスが真に必要な正規職員（臨時職員や民間企業所属者を除く）のみが限定的にアクセス可能となるようにアクセス権限を厳格に設計・運用いただくことも非常に重要と考えられます。 （2）報告受付システムは、想定されるいかなるサイバー攻撃や災害の発生時でも稼働し真正の事業者からの報告を受け付けられるよう極めて堅牢なシステムとして（万が一正常に稼働しない場合の代替手段も含めて）構築・運用されることが非常に重要である一方、事業者側が過度な負担なく円滑に報告を提出できることとの両立も重要と理解しております。そのためには設計段階においてシステムのユーザーである事業者の声を踏まえることも重要と考えられるため、検討段階において事業者との双方向の議論が継続的に実施されることを要望します。	の手続きに係る法令、ガイドラインや各省庁が公表する方法に従うこととなります。 （4）関連資料「サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ」の「（2）サイバー対処能力強化法に基づく報告」に記載の通り共通様式を整備することを予定しています。 その他のご意見は、今後の施策の参考とさせていただきます。	
28	様式本体の1. 、5. 、6. について、ランサムウェアと DDOS で様式（回答項目）が異なっているが、それぞれ簡素な方の設問に統一でないでしょうか。	項目については、関係法令で報告を求めている事項との整合も踏まえ設定しており、様式によって差分が生じているものもございます	－