「重要電子計算機に対する不正な行為による被害の防止に関する法律に基づく特別社会基盤事業者による特定侵害事象等の報告等に関する命令第四条第二項の特別社会基盤事業所管大臣及び内閣総理大臣が定める様式案」等に関する意見の募集の結果一覧

No.	御意見の要旨	御意見に対する主な考え方
1	【意見1】 対象箇所：各共通様式（別添様式1、別添様式2、別添様式3）の「記載の手引き」-「(2) 記載事項」 意見の趣旨：続報時における手動での下線引きの要求を緩和し、システムの活用や柔軟な変更箇所の明示を認める文言への修正、または初動時の負担軽減のための考慮を提案します。 意見の理由：インシデント発生時の緊迫した状況において、前回の報告書との差分を手動で確認し、下線を引き直す作業は報告者に過度な事務負担を強いることになります。デジタル化や官民連携基盤の整備を進める一方で、アナログな修正管理を必須とすることは、迅速な報告を阻害する要因となります。 修正案： 現行：「前回の報告から記載を変更した箇所に下線を引くなど、変更箇所が分かるようにしてください。」 修正案：「前回の報告から記載を変更した箇所が分かるようにしてください（下線や色付けのほか、システム上の差分管理機能による明示も可とします。ただし、初動対応中等で対応が困難な場合は、この限りではありません）。」 【意見2】 対象箇所：各共通様式（別添様式1、別添様式2、別添様式3）の「内閣官房国家サイバー統括室への共有等を希望しない」に関する注記部分 意見の趣旨：「希望しない」とした場合でも共有される例外的なケースについて、法的根拠やセキュリティ担保措置を具体的に明記し、報告者の懸念を払拭することを提案します。 意見の理由：「希望しないとした場合でも共有されることがある」という現在の表記は、報告者に対して政府の情報管理に対する不安や不信感を与える恐れがあり、自主的な報告（任意報告）を躊躇させる要因になりかねません。どのような場合に、どのような安全措置をもって共有されるのかを明示することが、信頼関係に基づく情報共有の促進につながります。 修正案： （注）の末尾に、以下の趣旨の文言を追記する。 「なお、共有が行われる場合であっても、法令に基づく秘密保持義務および適切なアクセス制御のもとで厳重に管理され、被害組織の同意なく公表されることはありません。」 【意見3】 対象箇所：各共通様式（別添様式2、別添様式3）の「記載の手引き」-「(2) 記載事項」 意見の趣旨：個人情報等の漏えい報告に関する「別紙1から3」について、速報段階では「把握している範囲の最小限の項目」の記載で足りる旨を、手引きに明記することを提案します。 意見の理由：ランサムウェア被害等の初動対応において、個人データの詳細な漏えい件数や項目、原因の特定には時間がかかります。一元化された様式内に膨大なチェックボックス（別紙）が含まれているため、報告者がすべての項目を即座に埋める必要があると誤認し、報告が遅れるリスクがあります。 修正案： 手引きの共通事項に以下の文言を追記する。 「※別紙1から3に記載の個人情報等に係る報告項目については、速報段階においては、すべての項目を記入する必要はなく、その時点で把握できている範囲で記入してください。」 【意見4】 対象箇所：申合せ案 2. 対象とする手続（第2ページ） 意見の趣旨：関係省庁が本共通様式を受理する際、電子的な手段（専用オンラインフォームや電子メールなど）を原則として整備・公表する旨の努力義務規定を追記することを提案します。 意見の理由：様式が統一されても、提出方法が省庁ごとに郵送、FAX、窓口持参などアナログな方法に依存したままであれば、被害組織の負担軽減や政府の対応迅速化という目的を達成できません。受け手側のデジタル対応を促す文言が必要です。 修正案： 第2項の「具体的な提出先及び提出方法については、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する。」の後に以下を追記する。 「その際、各省庁は、被害組織の負担軽減および迅速な情報共有のため、電子メールや専用フォーム等の電子的手段による受付窓口を速やかに整備し、公表するものとする。」	【意見1】共通様式の利用にあたり、「前回の報告から記載を変更した箇所に下線を引くなど」と記載しているとおり下線を引く方法は例示となりますので、変更箇所が分かれば、お示しいただいた色付けなどの方法で問題ございません。また、整備を進めている官民連携基盤においても、前回の報告に追記いただくことで、更新された項目が自動で明示される仕様となっております。 【意見2】重要電子計算機に対する不正な行為による被害の防止に関する法律（令和７年法律第42号。以下「強化法」という。）第５条に基づく報告に関する御指摘の「法的根拠」については、強化法の各条項であり、また、御指摘の「セキュリティ担保措置」につきましては、強化法第８条（安全管理措置）の規定に基づき取り扱うなど、関係法令等の規定に基づき適切に取り扱います。 【意見3】御指摘については、別紙１から３までの冒頭に、「いずれの項目も、報告をしようとする時点で把握している内容を記載すること」明記しております。 【意見4】御指摘については、本申合せ２．対象とする手続において、「サイバー対処能力強化法の施行に併せ、官民連携基盤の整備により報告の窓口を一元化する」及び「サイバー対処能力強化法の対象以外の被害組織についても官民連携基盤等の整備により報告先が一元化されるよう所要の調整を進める」と記載しております。
2	ランサムウェア事案共通様式における別紙１、２、３において、個人情報流出の媒体確認があるが、ランサムウェア攻撃で物理的な媒体流出は考えられない。 その他サイバー攻撃等事案共通様式では、「等」に物理的な窃盗などが含まれていると考えられているのであれば、上記は対象とならないが、想定されていないのであれば、同様に媒体を確認することに意味がない。	御指摘の箇所の媒体につきましては、報告される事案について、漏えい等が発生し、又は発生したおそれがある項目を選択していただくこととなります。例えば、電子媒体に不正アクセスを受けた場合であれば、電子媒体をご選択いただくこととなります。
3	該当箇所 「重要電子計算機に対する不正な行為による被害の防止に関する法律に基づく特別社会基盤事業者による特定侵害事象等の報告等に関する命令第四条第二項の特別社会基盤事業所管大臣及び内閣総理大臣が定める様式案」及び「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一部改正案」全体。 特に、速報、続報、詳報、報告先、共有先、官民連携基盤、国家サイバー統括室への共有、注意喚起、終了判断、再評価、見直しに関する部分。 意見内容 本案は、サイバー攻撃を受けた組織の報告負担を減らし、政府の対応を早くするためのものだと理解しています。申合せ案でも、報告件数の増加や報告先の多さにより、被害組織に過度な報告負担がかかっていること、また政府対応の迅速化が必要であることが示されています。 この目的自体には賛成です。 また、DDoS攻撃、ランサムウェア、その他のサイバー攻撃等について3つの様式を設けることにも、一定の合理性があると考えます。 ただし、速報を単に各省庁の所管窓口へ流すだけで終わらせると、同じような攻撃を受ける可能性がある他の事業者への注意喚起や、被害拡大の防止に十分つながらないおそれがあります。 この制度は、サイバー攻撃があったことを政府が早く知るだけでなく、その情報を関係機関に共有し、注意喚起や被害拡大防止、制度改善につなげるためのものだと考えます。 そのため、3様式を維持する場合でも、速報、続報、詳報、終了判断、再発、追加攻撃、再評価を、同じ事案として追える仕組みが必要です。 1. 共通番号付きの事案共有ページを設けるべきです 速報を受けたら、その事案に共通受付番号を付け、関係機関や必要な事業者が確認できる「事案共有ページ」又はそれに相当する共有機能を設けるべきです。 ここでいう事案共有ページは、必ずしも新しい大規模システムを意味しません。既存の官民連携基盤の中に作る共有画面でも、限定共有できる電子的な共有機能でもよいと考えます。 重要なのは、共通受付番号ごとに、速報、続報、詳報、終了判断、再評価情報を同じ場所で確認できることです。 速報を受けた管轄省庁又は受付機関は、速やかに次の情報を付した事案共有ページを作成することが望ましいと考えます。	9.につきまして、御指摘の暫定所感は、「６．その他（特記事項等）」に記載いただくことが可能です。 13.につきまして、御指摘の「随時検証」及び「不断の見直し」は、本申合せの関係省庁が行うものです。検証及び見直しの時期及びその基準については、各省庁等の適用状況や、サイバー攻撃の傾向を踏まえ、適時適切に判断してまいりますが、今後の見直しの際は、本申合せにおいて当該見直しを適用する期日を明示した上で公表する予定です。 その他、頂いた御意見は、今後の制度の運用における参考と致します。

No.	御意見の要旨	御意見に対する主な考え方
	・共通受付番号 ・初回受付時刻 ・受付機関 ・暫定分類 ・確認済み事実 ・影響を受けたサービス ・緊急連絡先 ・続報先 ・警戒区分又は影響度区分 ・関係機関 ・終了判断を行う主体 これにより、速報が個別メールや複数様式に分散せず、同じ事案として管理できます。 2. 事案共有ページの運営主体を明確にすべきです 事案共有ページを設ける場合、誰がその基盤を管理し、誰が個別事案を管理するのかを明確にすべきです。 共通受付番号、権限管理、アクセスログ、更新通知、再評価履歴などの基盤管理は、横断的な情報共有を担う内閣官房国家サイバー統括室又は同室が関与する官民連携基盤が担うのが適当だと考えます。 一方で、個別事案の初回受付、報告者への更新権限の付与、詳報の確認、終了判断については、その事案を受け付けた管轄省庁又は受付機関が担うべきです。 ただし、複数省庁にまたがる事案、重要インフラへの波及が疑われる事案、再発又は追加攻撃が確認された事案については、国家サイバー統括室が関係省庁と連携し、共有範囲、警戒区分、再評価の要否を調整できるようにすべきです。 3. 報告者が続報・詳報を更新できるようにすべきです 報告を受けた管轄省庁又は受付機関は、事案共有ページを作成した後、報告者に対して、共通受付番号、参照先、期限付きの認証情報、更新権限を付与すべきです。 報告者は、攻撃状況に変化があった場合、同じ事案共有ページに続報を記録できるようにするべきです。続報には、記録時刻が自動で残る必要があります。 各様式には、速報、続報、詳報を区別し、続報では前回報告からの変更点が分かるようにする考え方があります。　この考え方を、個別の提出書類だけでなく、同じ事案を更新していく仕組みにも広げるべきです。 攻撃が収束した後、報告者は詳報を同じ事案共有ページに記録する。詳報が記録された場合には、管轄省庁や必要な関係機関へ更新通知が届く仕組みとすべきです。 これにより、報告者は別様式で最初から出し直すのではなく、同じ事案の続報又は詳報として更新できます。 4. 各省庁は共通番号と参照先で注意喚起できるようにすべきです 各省庁は、自らの所管する事業者又は関係機関に対し、必要に応じて、共通受付番号と事案共有ページの参照先を通知できるようにすべきです。 その後の続報、詳報、警戒区分の変更、終了判断、再評価情報は、同じ事案共有ページで確認できるようにします。 これにより、各省庁が毎回、個別に詳細な通知文を作成しなくても、共通受付番号と参照先を使って、同種攻撃への注意喚起や被害拡大防止に必要な情報共有を行うことができます。 申合せ案では、報告を受けた官公署が、報告者の同意がある場合に内閣官房国家サイバー統括室へ共有すること、また官民連携基盤により窓口一元化を進めることが示されています。 　この方向性を、所管事業者への注意喚起や被害拡大防止にもつなげるべきです。 5. 更新通知機能を設けるべきです 事案共有ページは、作るだけでは不十分です。 続報、詳報、警戒区分の変更、終了判断、再評価、再発又は追加攻撃があった場合には、関係省庁や必要な対象事業者へ更新通知が届く仕組みを設けるべきです。 更新通知がなければ、重要な続報が記録されても、関係者が気付かないままになるおそれがあります。 同種攻撃への注意喚起や被害拡大防止のためには、情報を置くだけでなく、更新されたことを知らせる仕組みが必要です。 6. 再発又は追加攻撃があった場合は、終了済み事案を再開できるようにすべきです サイバー攻撃は、一度終わったように見えても、再発したり、追加攻撃が続いたりすることがあります。 そのため、終了済みの事案について再発又は追加攻撃が確認された場合には、新規事案として最初から報告させるのではなく、既存の共通受付番号又は同じ事案の管理記録を再開し、同じ事案の続報として記録できるようにすべきです。 再発又は追加攻撃が確認された場合、報告者は最初と同じ管轄省庁又は受付機関へ連絡し、受付機関は終了済み事案の管理記録を再開した上で、報告者に再度更新権限を付与する。報告者は、再発又は追加攻撃として続報を記録し、関係機関等へ更新通知が送られる仕組みとすべきです。 終了は記録の削除ではなく、暫定的な終了状態として扱い、再発又は追加攻撃が確認された場合には、同じ事案として再開又は再評価できるようにすべきです。 7. 再発、追加攻撃、重要更新は分かりやすく表示すべきです 再発、追加攻撃、警戒区分の変更、終了後の再評価があった場合には、通常の続報と区別できるよう、事案共有ページ上で目立つ表示を設けるべきです。 例えば、次のような表示です。 ・再発あり ・追加攻撃あり ・詳報更新 ・警戒区分変更 ・終了後再評価 ・緊急更新 これにより、関係者が再発又は重要な状態変更を見落とすリスクを下げることができます。 8. 警戒区分を設ける場合は、発動条件・解除条件・再評価条件を明確にすべきです 事案共有ページでは、攻撃の規模や影響に応じて、警戒区分又は影響度区分を設けることが有用です。例えば、通常受付、注意、警戒、緊急といった区分です。 ただし、報告者に攻撃規模を判断させるのではなく、サービス停止、障害継続、利用者影響、情報漏えい疑い、暗号化表示、身代金要求、他事業者への波及可能性など、報告時点で確認できる事実に基づいて、行政側が暫定的に付与すべきです。 小規模事案まで一律に警戒又は緊急として扱えば、警戒情報が形だけになったり、関係機関の確認負担が増えたりするおそれがあります。その一方で、小規模に見える事案が後から拡大する可能性もあります。 したがって、警戒区分又は影響度区分を設ける場合には、発動条件、維持条件、解除条件、再評価条件を明確にし、運用しながら見直すべきです。	

No.	御意見の要旨	御意見に対する主な考え方
	9. 報告者の暫定所感欄を設けるべきです 速報時には、確認済み事実とは別に、報告者の暫定所感を300字程度で記載できる任意欄を設けることを検討すべきです。 現場担当者の経験則に基づく違和感や、過去事案との類似点は、初動確認の参考となる場合があります。 ただし、この欄は攻撃類型の確定判断ではなく、あくまで報告者の所感として扱うべきです。事実確認欄とは分離し、後に所感と異なる結果が判明した場合でも、直ちに誤報又は虚偽報告として扱わないことを明示すべきです。 また、所感欄には、感情的表現、責任追及、根拠のない断定、個人情報、詳細なシステム構成、脆弱性の詳細、攻撃元情報等の機微情報を記載しないよう、入力上の注意を設けるべきです。 報告者所感は、断定ではなく、初動確認の参考情報として扱うべきです。 10. 事案共有ページのセキュリティ対策を明確にすべきです 事案共有ページは、同種攻撃への注意喚起や被害拡大防止に有用ですが、それ自体が攻撃対象になる可能性があります。 そのため、参照先情報だけで閲覧可能とするのではなく、限定共有を前提とすべきです。 少なくとも、次の対策が必要です。 ・期限付き認証情報 ・期限付き認証 ・閲覧権限管理 ・更新権限管理 ・アクセスログ ・権限失効機能 ・更新通知先の管理 ・代替連絡経路 また、被害事業者名、個人情報、システム構成、脆弱性の詳細、攻撃元情報等の機微情報は、必要に応じて非表示又は共有範囲を制限すべきです。 通報窓口や事案共有ページそのものがサイバー攻撃や障害の対象となる可能性もあるため、通常の共有基盤が利用できない場合の代替連絡経路も整備すべきです。 11. 終了判断者、終了根拠、再評価条件を記録すべきです 詳報が記録され、報告書として十分であると判断された場合には、終了判断主体が終了を宣言できる仕組みは有用です。 ただし、終了する場合には、必ず次の事項を記録すべきです。 ・終了判断者 ・終了判断機関 ・終了時刻 ・終了根拠 ・終了後の再評価条件 ・終了通知先 終了通知を関係機関等へ一括送信できる仕組みは有用ですが、何をもって終了としたのかが記録されなければ、後から受付後の処理が適切であったかを確認できません。 終了は、単なる削除や放置ではなく、根拠付きの暫定的な状態確定として扱うべきです。 12. 判断ログは、合理的に対応した担当者を守るためにも必要です 事案共有ページに判断記録を残す目的は、単に後日の責任追及を容易にするためではありません。 サイバー攻撃対応では、速報時点で情報が不完全であることが通常であり、後日の詳報、再発又は追加攻撃によって、攻撃類型、被害範囲、重要度が変わる場合があります。 そのため、当時把握できた情報、判断者、判断時刻、判断根拠、共有範囲、警戒区分又は影響度区分、終了判断、再評価条件を記録することは、当時の判断が合理的であったかを確認し、合理的に対応した担当者を守るためにも必要です。 記録がなければ、後から結果だけを見て担当者の判断を評価することになります。これは、初動段階で不完全な情報に基づいて判断せざるを得ないサイバー攻撃対応の実態に合いません。 判断ログは、未処理を可視化するだけでなく、当時の合理的判断を保護するための制度的安全装置として位置付けるべきです。 13. 見直しは、判断主体・基準・期限・完了確認を明確にすべきです 申合せ案では、各省庁等の適用状況やサイバー攻撃の傾向を随時検証し、不断の見直しを行うとされています。 この方針自体は重要です。 しかし、「随時検証」「不断の見直し」だけでは、誰が、いつ、どの基準で見直しの必要性を判断し、修正をいつまでに行い、誰が修正完了を確認するのかが明確ではありません。 ・事案共有ページを採用する場合には、少なくとも次の事項を検証すべきです。 ・事案共有ページの作成又は開始までの時間 ・続報の記録までの時間 ・詳報の記録までの時間 ・更新通知の到達状況 ・再発又は追加攻撃時の再開又は再評価件数 ・終了後の再評価件数 ・警戒区分又は影響度区分の過剰発動件数 ・見逃し又は過小評価が疑われる件数 ・通常業務への支障 ・関係者が更新を確認したか これらを確認し、一定以上の問題が生じた場合には、様式、入力項目、事案共有ページの運用、通知範囲、警戒区分又は影響度区分、終了判断手順を見直すべきです。 結論 本案の目的である報告負担軽減と政府対応迅速化には賛同します。 ただし、速報を単に管轄省庁へ連絡するだけで終わらせるのではなく、同種攻撃への注意喚起及び被害拡大防止に使える形で接続する必要があります。 そのため、3様式を維持する場合でも、共通受付番号を付した事案共有ページ又は同等の仕組みを設け、速報、続報、詳報、終了判断、再発又は追加攻撃、再評価を同一事案として管理できるようにすべきです。 各省庁は、所管事業者又は関係機関に対し、共通受付番号及び当該事案の参照先を通知することで、個別に詳細な通知文を作成し続けなくても、同種攻撃への注意喚起及び被害拡大防止に必要な情報共有を行うことができます。 一方で、事案共有ページ自体が攻撃対象となる可能性もあるため、限定共有、期限付き認証、権限管理、アクセスログ、権限失効、代替連絡経路を設けるべきです。 また、終了判断者、終了根拠、再評価条件を記録し、再発又は追加攻撃が確認された場合には、終了済み事案の管理記録を再開又は再評価して、同一事案の続報として管理できるようにすべきです。 さらに、判断ログは後日の責任追及のためだけではなく、速報時点の不完全な情報に基づき合理的に対応した担当者を守るためにも必要です。	

No.	御意見の要旨	御意見に対する主な考え方
4	【意見(1)】 ■ 該当箇所: 「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(案)」 2. 対象とする手続(第2段落) および 各共通様式(別添様式1、別添様式2、別添様式3)における「内閣官房国家サイバー統括室への共有」に関する記載 ■ 意見内容: 申合せ本文における「被害報告を行う者の同意がある場合は」という表現と、実際の様式における「共有等を希望しない場合は、その旨を記載(チェック)してください」というオプトアウト方式の表現に齟齬があるため、表現の整合性を図る修正を提案します。 具体的には、以下のいずれかの修正を提案します。 修正案A(申合せ本文の修正): 「被害報告を行う者が共有を拒否(オプトアウト)しない場合は、各様式に基づいて報告を受けた官公署は、当該内容を内閣官房国家サイバー統括室に共有するものとする。」 修正案B(各共通様式の修正): 様式側の記述を「[ ] 内閣官房国家サイバー統括室への情報共有に同意する」というオプトイン方式のチェックボックスに改める。 ■ 理由・効果: 現行案では、申合せ本文が「同意ベース(オプトイン)」を前提としているのに対し、実際の様式フォーマットは「拒否ベース(オプトアウト)」を求める形になっており、手続き上の法的・実務的な解釈に不整合が生じる懸念があります。被害組織が安心してスムーズに報告を行えるよう、両者のプロセス定義を一致させることで、実務上の混乱や法的解釈のブレを未然に防ぐことができます。 【意見(2)】 ■ 該当箇所: 「別添様式2(ランサムウェア事案共通様式)」および「別添様式3(その他サイバー攻撃等事案共通様式)」 「2. マルウェア感染時(ランサムウェア感染時)の留意事項」 ■ 意見内容: 初期対応に関する具体的な手順(「電源オフをしない」「LANケーブルを抜く」など)の冒頭に、被害組織の環境や専門ベンダーの判断を尊重する以下の免責・補足注記を追加することを提案します。 修正案: 「(注)以下の事項は一般的な初期対応における推奨事項であり、被害組織のシステム環境、保守契約、セキュリティ専門ベンダー等の具体的な指示や状況が異なる場合は、当該専門的判断や対応を優先してください。」 ■ 理由・効果: 様式に記載されている留意事項は初期対応のガイドラインとして極めて有益です。しかし、クラスタ構成やクラウド仮想化環境、特殊な産業用制御システムなど、環境によっては「電源オフ」や「ネットワーク切断」の判断が被害を拡大させたり、ハードウェア保守契約のサポート対象外となったりするリスクがあります。 本注記を追加することで、被害組織が独自の合理的な専門判断で初期対応を行った際に、様式の指示に反したかのような誤解が生じるのを防ぎます。また、国が提供する様式による指示が原因で予期せぬトラブルが生じた場合の責任の所在をクリアにし、官民双方が安心して利用できる様式となります。 【意見(3) ■ 該当箇所: 「別添様式3(その他サイバー攻撃等事案共通様式)」 2. 事案の概要(業務への影響) (3) 個人データ、保有個人情報又は特定個人情報の漏えい等について ■ 意見内容: 別紙1から別紙3のチェックボックス部分について、インシデント発生時の混乱した現場でも判断に迷わないよう、各別紙を添付すべき法的要件(報告義務)をわかりやすく併記することを提案します。 修正案: 「(3) 個人データ、保有個人情報又は特定個人情報の漏えい等について (※以下の該当する事態が発生した、またはそのおそれがある場合はチェックし、各別紙を記載の上、本様式と同時に提出してください) [ ] 別紙1(個人データの漏えい等):民間事業者等で、個人情報保護法第26条第1項に基づく報告等に該当する場合 [ ] 別紙2(保有個人情報の漏えい等):行政機関等で、個人情報保護法第68条第1項に基づく報告等に該当する場合 [ ] 別紙3(特定個人情報の漏えい等):民間・行政共通で、番号法第29条の4第1項に基づく報告等に該当する場合」 ■ 理由・効果: 様式3は不正アクセスや情報窃取など多岐にわたるサイバー攻撃を網羅する優れた共通フォーマットですが、インシデント対応の最中にある担当者は極度の混乱の中にあります。どの別紙を埋めて、どこに提出すればよいのかを明確に示すガイド(導線)を様式自体に持たせることで、記入の手戻りを防ぎ、被害組織の過度な報告負担の軽減という本申合せの「目的」をより実効性の高いものにできます。 【意見(4)】 ■ 該当箇所: 各共通様式(別添様式1、別添様式2、別添様式3)の「手引き」 「(1) 本様式の対象となる手続等」における「固有の報告項目については、様式本体の『6. その他特記事項』に記載すること」の指示	【意見(1)】御指摘を踏まえ、申合せ本文を修正しました。 【意見(2)】御指摘を踏まえ、申合せの別添様式２・３を修正しました。 【意見(3)】原案において、別紙１から別紙３を用いる報告者を正確に示していることから、原案を維持させていただきます。 【意見(4)】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。

No.	御意見の要旨	御意見に対する主な考え方
	■ 意見内容: 各業法等における固有の報告項目について、被害組織が漏れなく的確に記載できるよう、ポータルサイト(内閣官房ウェブサイトなど)における「分野別固有項目・記載ガイドライン」への具体的なURLや参照先情報を様式上に明記することを提案します。 修正案: 「...また、業法等の固有の報告項目については、様式本体の『6. その他特記事項』に記載すること。各分野における主要な固有の報告項目や具体的な記載例については、以下のウェブサイト(URL:[※具体的なポータルサイトのURL])に掲載されている『分野別報告ガイド』等を参照すること。」 ■ 理由・効果: 「その他特記事項」という自由記述欄への記載を現場に丸投げする場合、記入内容の過不足が発生しやすく、結果として各省庁からの再確認(聞き取り)の手間が増えてしまいます。これでは「政府の対応迅速化」という目的が十分に達成されません。容易に参照できるWeb上のガイドへのリンクを様式に直接配置することで、報告の一発書き・品質均一化が図られ、被害組織と政府双方のやり取りの往復コストを大幅に削減できます。	
5	件名：外国資本が関与する特別社会基盤事業者への報告義務違反に対する罰則強化と、実質的支配者情報の届出義務化を求める意見 内閣府 御担当者様 「サイバー対処能力強化法に基づく特別社会基盤事業者による特定侵害事象等の報告等に関する制度の解説」（案）について、以下のとおり意見を申し上げます。 意見の要旨 特別社会基盤事業者のうち、外国資本が経営権の一部または全部を保有する事業者について、特定侵害事象の報告義務違反に対する罰則を、他の事業者よりも重く設定すること、および実質的支配者（外国資本の出資比率、意思決定への関与の程度）の届出を義務化することを求めます。 問題意識 通信インフラをはじめとする重要インフラ事業者の中には、その経営権の一部を外国資本が保有している事業者が存在します。実際に、日本国民が広く利用する通信基盤において、外国企業が親会社の株式を50%保有する状態が継続し、その基盤上で複数回の情報漏えい事案（2023年、2026年）が発生してきました。 こうした事業者において、サイバー攻撃や情報漏えいの発生を把握しながら、報告を遅延させる、あるいは報告内容を実態より軽微に見せかけるといった行為があった場合、単なる過失報告義務違反として扱うのではなく、意図的な隠蔽・虚偽報告の可能性を含めて厳格に調査・処罰する必要があります。特に、報告義務違反に対する罰則が軽微であれば、事業者にとって「罰則を受け入れてでも報告を遅らせる、あるいは行わない」という判断が経済合理的になりかねません。 具体的な要請 第一に、特定侵害事象の報告義務に違反した特別社会基盤事業者に対する罰則について、違反によって生じた社会的損害の大きさ（利用者数、情報の機微性等）に応じた、実効性のある金額水準（違反によって事業者が得た利益、または回避した対応コストを大きく上回る水準）に設定してください。 第二に、外国資本が一定割合以上（例えば20%以上）を保有する特別社会基盤事業者については、その資本構成・実質的支配者情報を、届出制度に組み込んでください。これにより、報告義務違反が発生した際に、その背景に外国資本の意思決定関与があったかどうかを検証できる体制を整えてください。 第三に、悪質な虚偽報告・報告遅延が繰り返される事業者については、罰則にとどまらず、特別社会基盤事業者としての指定取消しを含む、事業継続に影響する厳格な措置を検討してください。 第四に、報告義務違反への罰則水準について、諸外国（EUのNIS2指令等）における同種の制度と比較し、日本の罰則が国際的に見て実効性を持つ水準であるかを検証し、必要に応じて強化してください。 日本国民の生活基盤を担う重要インフラの安全性を守るため、実効性のある報告義務制度の構築を求めます。	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。
6	全体のフォーマットについて： デジタルフォレンジックの調査には長い時間がかかるため、維持レベルの逸脱の有無・他の事業者への波及の可能性は有り・無しではなく、「わからない」という回答もあるべきではないでしょうか。 また全般的に枠欄が狭すぎます。記入するべき事項を列挙したうえで、様式自由の別紙での提出をデフォルトとするべきと考えます。 DDoSの技術情報について： 「通信プロトコル」が指示している内容も曖昧ですので、明確にすべきです。TCPやUDPのことを指すのか、アプリケーションレイヤーでのプロトコルを指すのかなど。プロトコルというよりは、攻撃を受けたサーバ内部でのルーティング（通信経路）などの情報のほうが有用ではないでしょうか。 ランサムウェア技術情報について： ランサムウェアについては、ゼロデイ攻撃を使うような高度なものだけではなくて、単に事業者がOSのアップデートを怠ったために発生するものも多いです。したがって、OSを最後にアップデートした日付（及び攻撃発生時の日付との差分）や、OSのバージョンなども重要な情報ではないでしょうか。これについても、技術情報の欄に書くべきと考えます。	全体のフォーマットについて： 記載の手引きに「報告をしようとする時点で把握している範囲で、１から６までの内容を記載してください。」と記載するとともに、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。」又は、「報告時点で記入可能な項目を記載してください。不明箇所は空白で構いません。」と記載しております。 また、御指摘の全般的に枠欄が狭いとの点について、現在も記載例は「セルが小さいときは、①セル幅を調整、②フォントサイズを調整、③「別紙〇のとおり」と記載し別紙を別ファイルで添付の順で対応」と枠欄を拡張する方法を明記しております。 DDoSの技術情報について： 御指摘の「通信プロトコル」に関して記入すべき事項については、今後公表する記入例においてお示しする予定です。 ランサムウェア技術情報について： 「OSを最後にアップデートした日付」及び「OSのバージョン」の記載につきましては、被害防止に一定程度有用な場合もあるものの、報告者における調査に係る負担が過大となることから、現時点において欄を設けて一律に記載を求める考えはございません。

No.	御意見の要旨	御意見に対する主な考え方
7	様式2および様式3における「悪用された脆弱性」のセクションについて、記載内容の例示として、見出しの横に「（悪用された脆弱性に係るCVD ID 等）」などのような括弧書きを行うのがよいのではないか。 また、製品開発者への報告のほかに、「ソフトウエア製品等の脆弱性関連情報に関する取扱規程（平成29年経済産業省告示第19号）」によるIPAへの届出有無についてもチェック欄を設けるべきではないか。 また、「製品開発者への報告の有無」については、修正・公開済みの脆弱性について悪用された場合に、その悪用の事実を報告した際に「有」とすべきか(そのような報告を推奨する趣旨か)を明らかにされたい。また、未修正・非開示の脆弱性が悪用された場合に、悪用の事実を伏せ、未修正の脆弱性の技術的詳細について報告した場合に「有」とすべき(報告内容として意図しているのは悪用の事実か、それとも脆弱性修正依頼としての内容か)について、明らかにされたい。	御指摘の「悪用された脆弱性」に関して記入すべき事項については、今後公表する記入例においてお示しする予定です。 御指摘の「IPAへの届出有無」の記載につきましては、被害防止に一定程度有用な場合もあるものの、報告者における調査に係る負担が過大となることから、現時点において欄を設けて一律に記載を求める考えはございません。 御指摘の「製品開発者への報告の有無」につきましては、修正済みか、公開済みかに関わらず、脆弱性の悪用の事実を報告したか否かを記載してください。国における対応の参考とする趣旨であり、必ずしも報告を推奨する趣旨のものではありません。
8	本様式案は、サイバー攻撃被害時の報告様式を一元化し、報告負担を軽減するものとして有用であると考えます。 一方で、実際の初動対応時には、攻撃原因、影響範囲、技術的詳細、個人情報漏えいの有無等が未確定であることが多く、全項目を確認してから報告しようとすると、速報が遅れるおそれがあります。 そのため、各様式の冒頭に「速報時に最低限記載すべき項目」を明示することを提案します。例えば、報告者情報、発覚日時、被害または影響の概要、現在の対応状況、連絡先、攻撃類型の仮分類等を最低項目として示し、技術的詳細や別紙事項は続報・詳報で補完できることを明確にすべきです。 また、各項目について「不明」「調査中」「該当なし」を明示的に選択または記載できるようにすることを提案します。未確定情報を無理に記載させるのではなく、速報段階では未確定であること自体を適切に示し、続報で補完できる構造にすることで、報告の迅速性と正確性の両立が図りやすくなると考えます。	記載の手引きに「報告をしようとする時点で把握している範囲で、１から６までの内容を記載してください。」と記載するとともに、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。」又は、「報告時点で記入可能な項目を記載してください。不明箇所は空白で構いません。」と記載しております。
9	本様式案では、内閣官房国家サイバー統括室等への情報共有に関する希望を記載する欄が設けられています。一方で、特定の法令報告や重要インフラ関係では、共有を希望しない場合でも共有され得る旨の注記があります。 この点は制度上必要な扱いであるとしても、報告者から見ると、「共有を希望しない」とした場合に何が制限され、どの情報は例外的に共有されるのかが分かりにくいおそれがあります。サイバー攻撃被害に関する情報には、脆弱性、侵入経路、業務影響、公表予定、個人情報に関する情報など、事業者にとって機微性の高い情報が含まれる可能性があります。 そのため、共有同意欄について、少なくとも以下の事項を様式本文または記載要領において明確化することを提案します。 * 同意により共有される情報の範囲 * 同意しない場合に共有されない情報の範囲 * 同意の有無にかかわらず共有され得る場合 * 匿名化または加工後に活用される場合の扱い * 共有先および共有目的の概要 報告者が過度に萎縮せず、正確な情報提供を行えるようにするためには、公益目的の情報共有と報告者保護の境界を、より分かりやすく示すことが重要であると考えます。	御指摘の「同意により共有される情報の範囲」及び「同意しない場合に共有されない情報の範囲」につきまして、「記載内容の全部又は一部について、内閣官房国家サイバー統括室との共有等を希望しない場合は、その旨及び共有等を希望しない内容について以下に記載してください」と記載しているとおり、共有を希望しない場合はその範囲を「共有等を希望しない内容：」の欄に記載してください。 御指摘の「同意の有無にかかわらず共有され得る場合」は（注）に記載しているとおりです。詳細につきましては、強化法第５条及び行動計画別添2. 重要インフラ事業者等からの情報連絡において明記されております。 御指摘の「匿名化または加工後に活用される場合の扱い」及び「共有目的」については、「報告された内容を整理分析の上、被害者が分からないようにした上で、被害の拡大防止のため、注意喚起等に活用することがあります」と記載しております。「共有先」は、（注）に記載している場合を除き、内閣官房国家サイバー統括室です。
10	本様式案では、速報、続報、詳報の区分が設けられており、続報等において変更箇所を分かるようにする運用が想定されています。 しかし、下線等によって変更箇所を示す方法は、文書ベースの運用としては理解できるものの、複数回の続報が発生した場合に、どの時点で何が変更されたのかを追跡しにくくなるおそれがあります。また、今後の電子申請、フォーム入力、機械処理、データ連携を考えると、変更箇所を文章上の装飾で示すだけでなく、構造化された欄として管理できることが望ましいと考えます。 そのため、様式内に「前回報告からの主な変更点」欄、または「版管理欄」を設けることを提案します。例えば、報告回数、報告日時、変更項目、変更内容、未確定から確定に変わった事項、削除または訂正した事項を記載できる構造にすることが考えられます。 これにより、報告者と受領側の双方にとって続報管理が容易になり、情報の取り違え、確認漏れ、過去報告との差分把握の負担を減らせると考えます。	御指摘の「前回報告からの主な変更点」及び「版管理欄」につきましては、各別添様式１頁目の【報告の区分】欄において、速報・続報・詳報の別のほか、報告の版、前回報告の時点の日時を記載することとしており、また、下線等で明示いただく箇所は前回の報告からの変更箇所であるため、御指摘のように「複数回の続報が発生した場合に、どの時点で何が変更されたのかを追跡しにくくなるおそれ」はなく、追加で別途記載を求める考えはございません。
11	本様式案は、サイバー攻撃被害時の報告様式を一元化し、被害組織の報告負担を軽減する方向性として重要であると考えます。 さらに将来的には、報告者が初動状況を比較的自由な文章で入力し、電子申請システムやAI等を用いた対話型入力支援により、不足情報の確認、用語の整理、該当欄への転記補助を行う仕組みも検討に値すると考えます。 ただし、この場合でもAI等に判断を委ねるのではなく、あくまで報告者の入力支援、確認支援、様式整理支援に限定すべきです。最終提出前には、人間が内容を確認、修正、承認する設計が必要です。また、サイバー攻撃被害に関する情報は機微性が高いため、外部AIへの不用意な送信禁止、入力データの保存範囲の明確化、学習利用の禁止、推定補完と本人入力の区別、応答ログや補完履歴の保存等も併せて検討すべきです。 その前提として、今回の様式についても、紙やPDFでの記載だけでなく、将来的な電子申請、フォーム入力、対話型記載支援に対応しやすい項目構造とすることを提案します。 直ちにAI導入を求めるものではありませんが、今後の運用高度化を見据え、項目の構造化、未確定情報の状態区分、変更履歴、確認ログ等に対応しやすい様式としておくことが、報告の迅速性と正確性の両立に資すると考えます。	本申合せの別添様式は、電子申請いただく場合も想定し、定めております。

No.	御意見の要旨	御意見に対する主な考え方
12	報告様式及び報告手続は、事業者が行政へ提供する情報の内容や報告方法を具体的に定めるものであるため、実務上の運用が分かりやすく、制度目的に照らして必要な範囲に整理されていることが重要であると考えます。 以上を踏まえ、以下の点について要望します。 １．第一報と詳細報告の役割を明確にしてください。 第一報は初動対応に必要な事項を迅速に報告することを目的とし、詳細な原因分析や再発防止策などは詳細報告で整理するなど、それぞれの報告の目的と記載範囲を分かりやすく示してください。 ２．報告基準及び記載基準を具体的にしてください。 どのような事案で報告が必要となるのか、また各記載項目についてどの程度まで記載すれば足りるのかを、記載例や具体例を用いて分かりやすく示してください。 判断基準が明確になることで、報告漏れや過大な報告を防ぎ、制度の円滑な運用につながると考えます。 ３．報告された情報の取扱いを明確にしてください。 報告された情報について、利用目的、保存期間、安全管理の考え方などを分かりやすく示してください。 報告制度への信頼を高めるためにも、情報がどのように管理・利用されるのかを明確にすることを要望します。 ４．制度運用後の検証及び見直しを実施してください。 制度開始後は、報告手続及び報告様式について、制度目的に照らして適切に機能しているか、事業者に過度な負担が生じていないかなどを定期的に検証し、その結果を踏まえて必要に応じて見直しを行うことを要望します。 制度の実効性と事業者の協力を両立させるため、分かりやすい運用と継続的な改善をお願いいたします。	１．について 御指摘の「報告の目的」については、速報は、政府の初動における被害の拡大防止に向けた対応、続報・詳報は、その後の被害の拡大防止に向けた対応に活用いたします。また、御指摘の「記載範囲」につきましては、各別添様式の１．記載の手引き（２）①に「報告をしようとする時点で把握している範囲で、１から６までの内容を記載してください。」と記載するとともに、各別添様式及び別紙の冒頭に「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。」又は、「報告時点で記入可能な項目を記載してください。不明箇所は空白で構いません。」と記載しております。 ２．について 御指摘の「報告基準」につきましては、報告の根拠となる法令、ガイドライン等により異なるため、それぞれの法令、ガイドライン等を参照してください。御指摘の「記載基準」につきましては、今後記入例を公表する予定です。 ３．について 御指摘の「利用目的」については、各別添様式１頁目において「国家サイバー統括室は、報告された内容を整理分析の上、被害者が分からないようにした上で、被害の拡大防止のため、注意喚起等に活用することがあります」と記載しております。御指摘の保存期間については、官公署等において公表している標準文書保存期間基準に基づき取り扱います。御指摘の「安全管理」につきましては、政府機関等のサイバーセキュリティ対策のための統一基準（令和７年度版）第3部等に基づき取り扱うほか、強化法第５条に基づき報告いただいた情報については、強化法第８条（安全管理措置）の規定に基づき取り扱います。 ４．について 御指摘の検証及び見直しについては、本申合せ３．において、「本申合せは、各省庁等の適用状況や、サイバー攻撃の傾向を随時検証し、不断の見直しを行う」としており、頂いた御意見は、当該検証及び見直しの際の参考と致します。
13	・各様式において、記入の具体例を明示いただくことを希望します。特に、別添様式3　「４（１）攻撃の手口・侵入経路・攻撃の時系列」と「４（２）サイバー攻撃等の類型」は記入内容が重複することが想定されるため、具体例を示していただくことを希望します。 ・共通様式への記載において、時系列や詳細など、報告の粒度次第では別紙での提出が許容されると理解しておりますが、この認識で正しければ、その旨を記載いただけますと幸甚です。	御指摘の別添様式３の４．（１）及び（２）に関して記入すべき事項については、今後公表する記入例においてお示しする予定です。また、御指摘の時系列については、様式は必要に応じて欄を拡張いただけるよう、エクセルで公表する予定です。御指摘の詳細につきましては、４．（４）に記載頂ければと存じますが、こちらも適宜欄を拡張いただけるようにする予定であるほか、別ファイルで提出可能な旨注記しております。
14	・各共通様式の記載の手引き内に「報告根拠」を記載する欄がありますが、こちらには旧様式の手引きに列挙されていたものから選択して記載することでよいでしょうか。 ・各共通様式の記載の手引き内に「https://www.cyber.go.jp/policy/group/cyber/policy.html」がありますが、具体的にどこを参照するのか記載いただけますと幸いです。 ・各共通様式の本体シートにある「発生日時」は「攻撃が始まった日時（サイバー攻撃の被害が発生した日時）」を記載する理解でよいでしょうか。今後記載要領を開示いただく際は、各項目においてどんな記載を求めているか分かりやすいものを開示いただけますと幸いです。 ・各共通様式の本体シートにある「発覚日時」は「サイバー攻撃を受けていると気づいた日時（つまり、認知した日時）」を記載する理解でよいでしょうか。今後記載要領を開示いただく際は、各項目においてどんな記載を求めているか分かりやすいものを開示いただけますと幸いです。 ・共通様式２の本体シート4.（６）悪用された脆弱性は、CVEや対象製品、バージョンを記載する理解でよいでしょうか。今後記載要領を開示いただく際は、各項目においてどんな記載を求めているか分かりやすいものを開示いただけますと幸いです。 ・共通様式３の本体シート4.（２）サイバー攻撃等の類型は、様式２の記載例を踏まえ、「・リークサイトやSNS当を通じた情報漏えいが行われた旨の公表の有無/身代金要求の有無といった被害の方式」を記載することでよいでしょうか。今後記載要領を開示いただく際は、各項目においてどんな記載を求めているか分かりやすいものを開示いただけますと幸いです。 ・共通様式３の本体シート4.（３）サイバー攻撃等の特徴（インディケータ情報）は、様式２の記載例を踏まえ、「・マルウェア情報/通信先のIPアドレスの通信情報等/判明した事案に係るログ情報等の技術的に識別できるランサムウェアの特徴や痕跡」を記載することでよいでしょうか。今後記載要領を開示いただく際は、各項目においてどんな記載を求めているか分かりやすいものを開示いただけますと幸いです。	御指摘の「報告根拠」につきましては、御指摘の旧様式の手引きに列挙されていたものを更新した上で内閣官房国家サイバー統括室ウェブサイトに掲載しますので、その中から選択して記載してください。そのほか、警察への相談を行う場合や、所管省庁から本様式により報告を 行うよう要請等があった場合についても本様式を利用することができます。その際は要請等の内容に沿って報告根拠を記載してください。 その他の御指摘につきましては、今後記入例を公表する予定です。
15	まず、重要インフラ事業者の「サイバーセキュリティ基本法」におけるインシデント報告（セプター等）と「サイバー対処能力強化法」における基幹インフラ事業者のインシデント報告について、 「重要インフラ事業者かつ基幹インフラ事業者」の場合、「重要インフラ事業者の指定分野」に関係する部分のみでインシデントが発生した場合でも、（重要インフラ事業者としての情報共有だけを行い）基幹インフラ事業者のインシデント報告をしなくても良い、という訳ではないと認識しているがそれで良いか。 （※あるいは、特定社会基盤事業者として指定された、特定重要設備に対する攻撃でなければ、「能力強化法」におけるインシデント報告義務とは直接紐付かない、ということになるのか？） 上記を前提とすると、 報告様式を統一頂いたこと、官民連携基盤を10/1に合わせてリリース頂くことは非常に良いと考える。一方で、「重要インフラ事業者かつ基幹インフラ事業者」の場合、「重要インフラ事業者としての情報共有体制」も、官民連携基盤を通じてできるよう対象が拡大されれば、一度で済むのではないか。省庁横断、法律横断的に対応頂けるのは非常に良いと考える。官民連携基盤の活用を今後、できる限り広げて頂きたいと考える。	御指摘の「重要インフラ事業者かつ基幹インフラ事業者」である場合であって、強化法第２条第２項に規定する特定重要電子計算機以外において発生した事案につきましては、強化法第５条に基づく報告は不要です。なお、強化法第５条に基づく届出範囲は、特定重要設備において発生した事象ではなく、特定重要電子計算機において発生した事象です。 また、御指摘の「重要インフラ事業者かつ基幹インフラ事業者」は、強化法第５条に基づく報告及び行動計画に定める重要インフラ事業者等による報告を一度で行うことが可能です。

No.	御意見の要旨	御意見に対する主な考え方
16	意見1 【該当箇所】 申合せ別添様式案 各様式「１．記載の手引き（２）記載事項」 【意見】 「本様式に記載いただいた内容は、報告先機関から、内閣官房国家サイバー統括室に共有されます。」との記載を、共有が報告者の同意を条件とすることが分かる表現に改めるべきである。あわせて「共有等」の「等」に含まれる行為を具体的に示すべきである。 【理由】 申合せ案２．は「被害報告を行う者の同意がある場合は、…共有するものとする」と定め、共有を同意の存在にかからしめている。しかし様式の記載の手引きは条件を付さない断定形で記載されているため、報告者は共有が既定の取扱いであると理解するおそれがあり、上位文書の定めと様式の記載が一致していない。 　また、報告者は「共有等を希望しない内容」を特定して記載することを求められるが、「等」に含まれる行為が示されていないため、何について拒否の意思表示をしているのかを判断できない。同意の対象が特定されない限り、同意は実質的な意思決定を伴わないものとなる。 意見2 【該当箇所】 申合せ案 １．目的／申合せ別添様式案 各様式「１．記載の手引き（２）記載事項」 【意見】 報告を受けた官公署又は内閣官房国家サイバー統括室から被害組織に対して情報の提供等が行われる場合があるのであれば、その内容、時期及び条件を明示すべきである。提供が予定されていないのであれば、その旨を明らかにすべきである。 【理由】 申合せ案１．は「官民双方向の情報共有を促すことが必要不可欠である」との認識を出発点としている。しかし本申合せが定めるのは、被害組織から官公署への報告及び官公署から内閣官房国家サイバー統括室への共有に限られ、被害組織に対する情報の提供については何らの定めも置かれていない。 　また、様式の記載の手引きにおいて共有された内容の用途として示されているのは、被害者が分からないようにした上で被害の拡大防止のため注意喚起等に活用することがある旨の記載のみである。報告者は、共有等に同意するか否かを判断するに当たり、自らに何が生じ又は生じないかを知る手がかりを持たない。目的として双方向性を掲げる以上、報告者が判断し得る程度に、報告者への還元の有無及び内容を明らかにすべきである。 意見3 【該当箇所】 申合せ案 ３．本申合せの適用開始時期及び見直し 【意見】 「２（１）に定める様式の適用開始から１年後を目途に必要な見直しを行う」との現行規定を維持し、又はこれに代わる期限を付した検証規定を置くべきである。 【理由】 現行規定による見直しの目途は、別添様式１及び２の適用開始（令和７年10月１日）から１年後、すなわち令和８年10月１日である。他方、改正案は別添様式３の適用開始日を同じ令和８年10月１日と定めている。期限付き見直しが到来する時点と、対象事案を拡大する時点が一致している。 　改正案はこの期限を「不断の見直し」に置き換えるものであり、先行して適用された様式１及び２の運用実績が検証されないまま対象が拡大される結果となりかねない。検証を行うのであれば、報告件数、重複報告の削減状況、報告に要する時間、共有等を希望しない旨の申出の状況等の指標をあらかじめ定め、その結果を公表すべきである。 意見4 【該当箇所】 申合せ案 ２．対象とする手続／別添様式案「その他サイバー攻撃等事案共通様式」１．記載の手引き（２）記載事項 【意見】 別添様式３を用いるべき事案の判断基準及び判断時点を示すとともに、原因が判明していない段階における様式選択の取扱い、及び事後に他の様式によるべきであったことが判明した場合の取扱いを明示すべきである。 【理由】 申合せ案２．は様式３の対象を「１，２の事象以外の事象」と定めるのみで、積極的な定義を置いていない。他方、別添様式３には「２から４までの報告を行う場合においては、サイバー攻撃事案に伴う漏えい等事案に伴う報告であることに留意する」との記載があり、様式の使用に当たり当該事案がサイバー攻撃に起因するとの判断が前提とされている。 　個人情報の保護に関する法律第26条第１項の規定による報告のうち速報は、事態を知った後速やかに行うこととされ、通常は原因の特定に先立って提出される。原因が判明しない段階で様式を選択せざるを得ない場面が生じるが、その取扱いは本改正案及び関係資料のいずれにも示されていない。判断を報告者に委ねたまま基準を示さないことは、報告の遅延又は様式の不統一を招き、負担軽減という目的に反するおそれがある。 意見5 【該当箇所】 申合せ別添様式案「その他サイバー攻撃等事案共通様式」４．事案に関する技術的な事項（２）サイバー攻撃等の類型 【意見】 別添様式１と同様に、既存の分類体系に基づく選択肢を設けるべきである。 【理由】 別添様式１（ＤＤｏＳ攻撃事案）の「（２）攻撃類型」は、MITRE ATT&CKのTechniquesを参照した選択式とされ、該当が不明な場合の選択肢も設けられている。これに対し別添様式３の「（２）サイバー攻撃等の類型」には選択肢がなく、自由記述による。 　様式３が対象とする事案は「不正アクセス、情報窃取等」と範囲が広く、記述の粒度が報告者ごとに異なることが想定される。情報集約及び整理分析を目的とするのであれば、様式３においてこそ分類軸を統一する必要性が高い。選択式とすることは、初動対応中における記載負担の軽減にも資する。 意見6	（意見１） 御指摘の「共有が報告者の同意を条件とすることが分かる表現」は「本様式に記載いただいた内容は、報告先機関から、内閣官房国家サイバー統括室に共有されます。」の次の段落で「記載内容の全部又は一部について、内閣官房国家サイバー統括室との共有等を希望しない場合は、その旨及び共有等を希望しない内容について以下に記載してください。」としており、共有等を希望しない場合にはその旨記載できることは明らかであると考えます。また、御指摘の「等」は、直前の「国家サイバー統括室は、報告された内容を整理分析の上、被害者が分からないようにした上で、被害の拡大防止のため、注意喚起等に活用することがあります。」を指しますが、「等」の内容を書き下した場合、文章が冗長になることから書き下してはおりません。 （意見２） 御指摘の官公署等からの情報提供は、頂いた情報を整理分析の上、適時適切に行うものであり、予めその内容、時期及び条件を予見して規定することは困難です。 （意見３） 今後の見直しの時期につきましては、各省庁等の適用状況や、サイバー攻撃の傾向を踏まえ、適時適切に判断してまいります。 （意見４） 御指摘については、報告の根拠となる法令やガイドライン等ごとに異なる場合があるため、報告の根拠となる法令やガイドライン等を参照してください。 （意見５） 別添様式３は対象となる事象が多岐にわたるため、御指摘のサイバー攻撃の類型を網羅的に選択肢として示すことは困難ですが、記入すべき事項の例については、今後公表する記入例においてお示しするとともに、報告されるサイバー攻撃の傾向を踏まえ、適宜見直しを行ってまいります。 （意見６） 御指摘の「マルウェア感染を伴わない事例」について、発生原因は多岐に渡ることから網羅的に示すことは困難であることから主要な発生原因として考えられるマルウェア関連時の留意事項を記載しております。また、「これらは事案の発覚直後、報告書の作成に着手する前に採られるべき措置である」との御指摘についてはその通りですが、マルウェア感染時にどのように対応すべきかにつきましては、それぞれの組織において、自組織の環境に合わせた手順を準備しておくことが好ましいと考えます。 （意見７） 御指摘の「既存の法令上の報告様式・提出先・期限がどの範囲で代替されるのか」につきましては、当該既存の法令の規定によるため、当該各法令の規定を参照してください。また、本申合せ２．の「サイバー対処能力強化法の対象以外の被害組織についても官民連携基盤等の整備により報告先が一元化されるよう所要の調整を進める」との記載については、所要の調整を進めることを記載したものであり、令和８年10月１日にサイバー対処能力強化法の対象以外の被害組織についても報告先の一元化を行うことを記載したものではありません。当該被害組織の報告先を一元化する時期については、現時点において予見することは困難ですが、関係する事業者には当該一元化を行う前に適切に周知してまいります。

No.	御意見の要旨	御意見に対する主な考え方
	【該当箇所】 申合せ別添様式案「その他サイバー攻撃等事案共通様式」２．マルウェア感染時の留意事項 【意見】 マルウェア感染を伴わない事案における証跡保全の取扱いを明示すべきである。また、これらの留意事項は報告様式のみに掲載するのではなく、事案発生前に参照される媒体において周知すべきである。 【理由】 様式３が対象とする「不正アクセス、情報窃取等」には、マルウェア感染を伴わない事案が含まれる。しかし当該項目は「マルウェア感染時」と題され、「感染端末」を前提とした記述となっているため、マルウェア感染が確認されていない不正アクセス事案において同様の措置を採るべきかが不明である。 　また、記載されている措置（再起動及び電源オフを行わないこと、ウイルス対策ソフトによるフルスキャンを行わないこと、ファームウェア及びＯＳのアップデートを行わないこと）は、平時に推奨される対応と方向を異にする。これらは事案の発覚直後、報告書の作成に着手する前に採られるべき措置であるが、現状では報告様式の中にのみ記載されている。様式を参照する前に措置が採られてしまう可能性が高く、周知の手段として適切とは言い難い。 意見7 【該当箇所】 申合せ案 ２．対象とする手続 【意見】 共通様式を用いた場合に既存の法令上の報告様式・提出先・期限がどの範囲で代替されるのかを明示すべきである。また、サイバー対処能力強化法の対象以外の被害組織について、官民連携基盤等を利用できる時期の見通しを示すべきである。 【理由】 改正案は共通様式を「用い、又は別途法令等で定める様式に添付する形で報告等を行うことを可能とする」とし、「具体的な提出先及び提出方法については、各法令、ガイドラインや、各省庁が公表する方法に従う」と定めている。この定めによれば、共通様式は既存様式の代替ではなく選択肢の追加にとどまり、提出先及び期限は従前どおり各法令に従うこととなるため、どの範囲で重複が解消されるのかが明らかでない。 　また、対象以外の被害組織については「所要の調整を進める」とされるにとどまるため、様式３の適用が開始される令和８年10月１日の時点でこれらの組織が窓口一元化の対象となるかが判然としない。	
17	今回、これまでの意見を踏まえて、改正案である主務省令に定められております各様式案及び報告手続等に関する申し合わせの一部改正案について、弊社として賛同いたします。 特に申合せ一部改正案にあります「３．本申合せの適用開始時期及び見直し」の修正案については、極めて変化の早いサイバーセキュリティを取り巻く現下の状況をかんがみると、大変時宜を得た改正案であると認識しております。運用にあたっては、その判断に迷うことも多々考えられることから、例えば、NCOホームページ上で判断しやすい解説を付すなど、ご配慮いただきますようよろしくお願いいたします。	賛同の御意見として承ります。 また、運用にあたっては、記載内容について判断に迷うことのないよう、今後記入例を公表する予定です。

No.	御意見の要旨	御意見に対する主な考え方
18	【AIによる自律的サイバー攻撃を想定した制度設計を求める意見】 本意見募集の対象となっているサイバー攻撃による被害の報告制度について、強い懸念を表明します。 現在、AI技術は急速に高度化しています。AIエージェントが、人間から一つ一つの操作を指示されなくても、与えられた目的を達成するために情報収集、分析、外部システムへのアクセスなどを自律的に行い、サイバー攻撃につながる行動まで実行する事例が現実に報告されています。 このような状況で、従来型の「サイバー攻撃を受けた後に被害を報告する」という考え方だけでは、到底十分とは言えません。 AIによる攻撃は、人間が一つ一つ操作する攻撃とは異なり、短時間で大量の情報を探索・取得・分析し、攻撃方法を変化させながら継続する可能性があります。 特に、AIが個人情報や機密情報を扱うシステムへアクセスできる環境が広がれば、一度侵入を許した場合の被害規模は従来以上に深刻になる可能性があります。 したがって、単に被害発生後の報告手続を整備するだけではなく、「AIが自律的に攻撃を実行する」ことを明確な脅威として想定し、攻撃を未然に防止するための技術的・制度的措置を義務化すべきです。 具体的には、AIシステムに対する個人情報・機密情報へのアクセス権限を必要最小限に限定すること、人間による監督を必須とすること、異常なアクセスや大量取得をリアルタイムで検知・遮断すること、AIによる目的外利用を防止すること、アクセス履歴を保存し監査可能にすることなどを制度として明確にしてください。 また、AIによって取得・複製・分析された情報は、後から完全に回収することが困難です。 特に個人情報については、ひとたび漏えいすれば、氏名や住所だけでなく、複数の情報をAIが組み合わせることで、本人が意図していなかった生活状況、行動、属性等まで推測される危険があります。 この点からも、現在進められている個人情報保護法改正との整合性について重大な疑問があります。 一方では本人同意なしの第三者提供等を可能とする方向へ個人情報の利活用を広げながら、他方ではサイバー攻撃による情報流出への対策を整備するという制度設計では、根本的な矛盾があります。 「情報を広く利用できるようにする」ことと「情報を安全に守る」ことは別問題です。 AIが自律的に情報を処理・取得できる時代に、個人情報の流通範囲を拡大することは、サイバー攻撃時の被害をさらに深刻化させる可能性があります。 したがって、政府には、AIによる自律的なサイバー攻撃を前提とした抜本的な安全対策を講じることを求めます。 さらに、個人情報保護法改正についても、AIによる自律的な情報処理・サイバー攻撃という最新のリスクを十分に検証した上で、施行を強行せず、撤回・廃止を含めて根本から見直してください。 「攻撃されたら報告する」だけでは国民の情報は守れません。 攻撃されても被害を最小限に抑えられる仕組み、そもそもAIが容易に個人情報へ到達できない仕組み、そして本人の意思なく個人情報が広範に利用・流通されない仕組みを構築してください。 AIの自律化が進む今こそ、利便性やデータ利活用を優先するのではなく、国民の個人情報と安全を最優先とする制度へ転換することを強く求めます。	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。

No.	御意見の要旨	御意見に対する主な考え方
19	<KEV該当有無の追加> 「悪用された脆弱性」の記載欄に、Known Exploited Vulnerabilities（KEV）該当有無を追記することを提案する。 実際に攻撃者による悪用が確認されている脆弱性かどうかは、被害拡大の可能性や優先対応要否を判断する上で有用な情報である。 特に初動対応段階における脆弱性の危険度評価や、関係機関による状況把握の高度化に資すると考える。 <ラテラルムーブメント有無の追加> 「不正アクセス」に関する項目として、「横展開（ラテラルムーブメント）の有無」を追加することを提案する。 近年のランサムウェア事案や高度なサイバー攻撃においては、初期侵害後の横展開により被害が拡大するケースが多く見られる。 横展開の有無を把握することは、影響範囲の評価や重要システムへの波及状況の把握に有用であり、 我が国全体のサイバーセキュリティ対策の高度化に資すると考える。 <生成AI関連影響有無の追加> 「生成AI関連影響の有無」を把握できる項目を追加することを提案する。 近年、生成AIを活用したシステムやサービスの利用が拡大しており、プロンプトインジェクション、 機密情報の不適切な参照・出力、AIサービスを経由した情報漏えい等の新たなリスクが顕在化しつつある。 生成AI利用環境がインシデントに関係しているかを把握することは、事案分析や影響範囲の評価に有用であり、 我が国全体のサイバーセキュリティ対策の高度化に資すると考える。 <初報における暫定記載の明確化> 「影響範囲」の記載について、初報時点では暫定的な記載を許容し、 続報にて補完可能である旨を記載例や解説書において明確化することを提案する。 近年のサイバー攻撃事案においては、インシデント発生直後に被害範囲や影響範囲を正確に把握することが困難なケースが多く見られる。 初報において確定情報を求めることは、事業者の初動対応や被害拡大防止対応の負担増加につながる可能性があるため、 暫定的な記載を許容し、継続的な報告により情報を補完できることを明確化することが有用であると考える。 <「その他サイバー攻撃等事案」の具体例提示> 「その他サイバー攻撃等事案」の対象範囲について、具体例を示すことを提案する。 近年のサイバー攻撃は多様化しており、「その他サイバー攻撃等事案」に該当する範囲が必ずしも明確ではないケースが想定される。対象となる事案の具体例を示すことにより、 事業者による様式選択の判断を容易にし、報告内容の均質化及び報告品質の向上に資すると考える。 <サイバー攻撃類型の選択式項目の追加> 「その他サイバー攻撃等事案」の「サイバー攻撃等の類型」について、選択式の記載項目を追加することを提案する。 近年のサイバー攻撃は多様化しているものの、事業者ごとに攻撃類型の記載粒度や表現が異なる場合が想定される。ランサムウェア、不正アクセス、情報窃取、DDoS等の代表的な 類型を選択肢として例示することにより、報告内容の均質化及び集計・分析の高度化に資すると考える。 <インディケータ（IoC）情報の記載例追加> インディケータ情報について、IPアドレス、ドメイン、URL、ファイル名、ハッシュ値、マルウェア名等の記載例を示すことを提案する。 インディケータ情報は被害状況の把握や類似事案との関連分析において有用な情報である。一方で、記載対象が明示されていない場合、事業者によって報告内容に差異が生じる可能性がある。記載例を示すことにより、報告内容の均質化及び分析精度の向上に資すると考える。	<KEV該当有無の追加><ラテラルムーブメント有無の追加>及び<生成AI関連影響有無の追加>は、被害防止に一定程度有用な場合もあるものの、報告者における調査に係る負担が過大となることから、現時点において一律に記載を求める考えはございません。 <初報における暫定記載の明確化>につきましては、各別添様式の１．記載の手引き（２）①に「報告をしようとする時点で把握している範囲で、１から６までの内容を記載してください。」と記載するとともに、各別添様式及び別紙の冒頭に「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。」又は、「報告時点で記入可能な項目を記載してください。不明箇所は空白で構いません。」と記載しております。 <「その他サイバー攻撃等事案」の具体例提示>につきましては、別添様式３の名称に「（不正アクセス、情報窃取等）」と付しております。なお、報告対象の範囲の詳細につきましては、報告の根拠となる法令やガイドライン等を参照してください。 <サイバー攻撃類型の選択式項目の追加>につきまして、別添様式３は対象となる事案が多岐にわたるため、御指摘のサイバー攻撃の類型を網羅的に選択肢として示すことは困難ですが、記入すべき事項の例については、今後公表する記入例においてお示しするとともに、報告されるサイバー攻撃の傾向を踏まえ、適宜見直しを行ってまいります。 <インディケータ（IoC）情報の記載例追加>につきましては、今後公表する記入例においてお示しいたします。

No.	御意見の要旨	御意見に対する主な考え方
20	提出者：一般社団法人　日本貿易会　情報システム委員会 要旨：商社自体は「特別社会基盤事業者」に該当しないが、商社も事業者へ重要設備を納入する中間業者（サプライヤー）として介在し、事前審査や届出の対象となり影響が想定されることから、以下の意見を提出する。 １．意見内容：本様式案の方向性に賛成する。DDoS攻撃、ランサムウェア、その他サイバー攻撃等について共通様式を用い、又は別途法令等で定める様式に添付する形で報告できる取扱いは、被害組織の報告負担軽減と政府側の対応迅速化に資するため、制度化を進めるべきである。 【理由】申告せ案では、報告先となる官公署が多いこと等により被害組織に過度な報告負担がかかっているとした上で、報告先や様式の一元化、簡素化を進める趣旨が示されている。また、告示案・概要では、DDoS攻撃事案、ランサムウェア事案、その他事案の区分ごとに関係省庁申合せ別添様式1から3を用いることが示されている。 ２．意見内容：具体的な提出先、提出方法、追加的な報告事項の有無について、施行前に、事業者が実務で参照できる一覧表、Q&A又はフローチャートとして公表いただきたい。特に、複数の法令・ガイドライン、警察相談、所管省庁への報告等が重なる場合に、共通様式を提出した後の別途報告の要否、提出先の優先順位、同一内容の再提出が不要となる範囲を明確にしていただきたい。 【理由】様式案では、具体的な提出先や提出方法、追加的な報告事項の有無は、各法令、ガイドライン、各省庁が公表する方法に従うものとされている。この記載のままでは、平時の準備やインシデント初動時に、どの窓口へ、どの様式で、どの範囲まで報告すべきかを事業者側で判断しにくく、結果として重複報告や報告遅延につながる懸念がある。 ３．意見内容：速報提出時の記載負担を抑えるため、各様式について「必須項目」「任意項目」「不明又は調査中でも差し支えない項目」を記載要領上で明示いただきたい。また、IPアドレス、ログ情報、IoC、システム構成図、フォレンジック結果等を別ファイルで提出する場合のファイル形式、容量、暗号化・送付方法も明確にしていただきたい。 【理由】様式案では「報告をしようとする時点で把握している範囲」で記載すること、ランサムウェア及びその他サイバー攻撃等の技術情報については不明箇所は空白でよいこと、IPアドレスやログ情報など記載内容が多数になる場合は別ファイルで提出することが示されている。一方、速やかな初動対応中は未確定情報が多いため、運用上の許容範囲を明示することで、報告品質の確保と初動対応への支障回避を両立できると考える。 ４．意見内容：報告内容の内閣官房国家サイバー統括室等への共有、匿名化された注意喚起等への活用、及び「共有等を希望しない」場合の取扱いについて、営業秘密、技術情報、個人情報、取引先情報が含まれる場合の保護措置と共有範囲を具体化いただきたい。特に、法令に基づき共有される場合と、任意報告・同意に基づく共有の場合の違いを明確にしていただきたい。 【理由】様式案では、報告内容が報告先機関から内閣官房国家サイバー統括室に共有され、被害者が分からないようにした上で注意喚起等に活用される旨が記載されている。また、共有等を希望しない場合でも、重要電子計算機に対する不正な行為による被害の防止に関する法律第5条に基づく報告や重要インフラのサイバーセキュリティに係る行動計画に基づき、共有されることがある旨も示されている。提出側が安心して正確な情報を出せるよう、共有範囲と保護措置の明確化が必要と考える。	１．賛同の御意見として承ります。 ２．御指摘の具体的な提出先や提出方法、追加的な報告事項の有無、共通様式を提出した後の別途報告の要否については、報告の根拠となる各法令・ガイドラインにより異なることから、各法令・ガイドラインを参照してください。 御指摘の提出先の優先順位につきまして、特段根拠となる法令・ガイドライン等に優劣はございません。また、御指摘の同一内容の再提出が不要となる範囲につきましては、各法令・ガイドライン等の規定に基づき、本様式により提出いただく範囲については、再提出いただく必要はございません。 ３．御指摘の必須項目等につきまして、各別添様式の１．記載の手引き（２）①に「報告をしようとする時点で把握している範囲で、１から６までの内容を記載してください。」と記載するとともに、各別添様式及び別紙の冒頭に「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。」又は、「報告時点で記入可能な項目を記載してください。不明箇所は空白で構いません。」と記載しております。 また、別ファイルで提出する場合は、報告者の報告負担を軽減する観点から任意の形式で提出いただけます。 ４．御指摘の「保護措置」につきましては、政府機関等のサイバーセキュリティ対策のための統一基準（令和７年度版）第3部等に基づき取り扱うほか、強化法第５条に基づき報告いただいた情報については、強化法第８条（安全管理措置）の規定に基づき取り扱います。御指摘の「共有範囲」につきましては、強化法第５条に基づく報告については、強化法の各規定の定めるところにより、それ以外の報告については、内閣官房国家サイバー統括室です。
21	「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「別添様式３」は、なぜ『サイバー攻撃「等」事案』なのでしょうか。 「等」が示すものが案を読んでも分からないため、「等」の字は削除すべきです。	本様式では、サイバー攻撃によらない不正アクセス、情報窃取等においても報告に使用されることから、『サイバー攻撃「等」事案』という名称としています。
22	本案に強く反対する。 サイバー攻撃への対処を口実として、民間事業者が保有するシステム情報や被害情報を政府が広範に把握する仕組みを拡大することには、重大なプライバシー・情報管理上の問題がある。 特に、報告内容に個人情報、顧客情報、通信に関する情報、企業秘密、システムの脆弱性情報等が含まれる可能性がある以上、政府がそれらを取得することによる二次的な情報漏えいリスクまで考慮しなければならない。 サイバー攻撃を防ぐための制度によって、新たな巨大な情報集中リスクを生み出すようなことがあってはならない。 また、複数の行政機関が関与する制度である以上、どの機関がどの情報にアクセスできるのか、情報をどこまで共有できるのか、目的外利用をどのように禁止するのかを明確にすべきである。 「必要な場合」「適切に」「関係機関と共有する」といった曖昧な運用によって、行政機関の裁量が過度に広がることは絶対に避けるべきである。 国民の個人情報や企業の機密情報を政府に集中させるのであれば、それに見合うだけの厳格な監督、第三者による監査、利用目的の限定、保存期間の制限、目的外利用の禁止、漏えい時の責任を法律上明確にすべきである。 これらの保障が十分でないまま本制度を拡大することには断固反対する。政府の情報収集権限を拡大するのではなく、国民の権利と情報の安全を最優先とした制度に根本的に改めることを求める。	御指摘の個人情報及び顧客情報につきまして、報告者の特定や報告者に連絡を行うため、法人等の代表者の氏名並びに事務連絡者の氏名及び連絡先を記載いただくこととしておりますが、一般の顧客の個人情報を求めるものではございません。 その他の情報につきましても、各様式において「報告された内容を整理分析の上、被害者が分からないようにした上で、被害の拡大防止のため、注意喚起等に活用することがあります」等と記載しているところです。また、報告いただいた情報の取扱いにつきましては、政府機関等のサイバーセキュリティ対策のための統一基準（令和７年度版）第3部等に基づき取り扱うほか、強化法第５条に基づき報告いただいた情報については、強化法第８条（安全管理措置）の規定に基づき取り扱います。

No.	御意見の要旨	御意見に対する主な考え方
23	本案に強く反対する。 サイバー攻撃への対処を口実として、民間事業者が保有するシステム情報や被害情報を政府が広範に把握する仕組みを拡大することには、重大なプライバシー・情報管理上の問題がある。 特に、報告内容に個人情報、顧客情報、通信に関する情報、企業秘密、システムの脆弱性情報等が含まれる可能性がある以上、政府がそれらを取得することによる二次的な情報漏えいリスクまで考慮しなければならない。 サイバー攻撃を防ぐための制度によって、新たな巨大な情報集中リスクを生み出すようなことがあってはならない。 また、複数の行政機関が関与する制度である以上、どの機関がどの情報にアクセスできるのか、情報をどこまで共有できるのか、目的外利用をどのように禁止するのかを明確にすべきである。 「必要な場合」「適切に」「関係機関と共有する」といった曖昧な運用によって、行政機関の裁量が過度に広がることは絶対に避けるべきである。 国民の個人情報や企業の機密情報を政府に集中させるのであれば、それに見合うだけの厳格な監督、第三者による監査、利用目的の限定、保存期間の制限、目的外利用の禁止、漏えい時の責任を法律上明確にすべきである。 これらの保障が十分でないまま本制度を拡大することには断固反対する。政府の情報収集権限を拡大するのではなく、国民の権利と情報の安全を最優先とした制度に根本的に改めることを求める。	御指摘の個人情報及び顧客情報につきまして、報告者の特定や報告者に連絡を行うため、法人等の代表者の氏名並びに事務連絡者の氏名及び連絡先を記載いただくこととしておりますが、一般の顧客の個人情報を求めるものではございません。 その他の情報につきましても、各様式において「報告された内容を整理分析の上、被害者が分からないようにした上で、被害の拡大防止のため、注意喚起等に活用することがあります」等と記載しているところです。また、報告いただいた情報の取扱いにつきましては、政府機関等のサイバーセキュリティ対策のための統一基準（令和７年度版）第3部等に基づき取り扱うほか、強化法第５条に基づき報告いただいた情報については、強化法第８条（安全管理措置）の規定に基づき取り扱います。
24	「DDoS攻撃事案共通様式」について、PCで編集可能なpdfファイルまたはWordファイルの提供があることが望ましい。また、（送信側、受取側双方の）データ活用の観点とプロプライエタリソフトウェアへの依存の排除の観点から、中長期的にはjsonまたはyamlで提出項目の構造を定義し（validatorの提供も含め）、回答できるようにすることを検討頂きたい。	本様式は編集可能なエクセルでの公表を想定しております。その他、頂いた御意見は、今後の制度運用の参考とさせていただきます。
25	ランサムウェアによるインシデント報告は、様式１と様式３どちらにも当てはまる可能性があると説明されているが、どちらの様式で報告優先すべきか明示いただきたい	ランサムウェアによるインシデント報告は、様式２において報告を行ってください。ランサムウェア攻撃か不明な事象に係るインシデント報告は様式３で報告することも可能です。
26	1、（参考）新旧対照表 P１下部、P２ 意見 サイバー攻撃に伴う個人データ漏えい等が発生した際、本共通様式を用いて報告を行うことで、個人情報保護法第２６条第１項に基づく個人情報保護委員会等への従来の個別報告は不要となる（本様式での一回の報告にて手続きが賄える）という認識で正しいか確認させてください。 実務上の報告漏れや重複手続きを防止するため、本様式提出による法的手続きの補填範囲を規定等でより明確に示していただくよう要望いたします。 ２、申合せ別添様式案 DDoS攻撃事案共通様式 P３ 意見 DDoS攻撃の初動対応時において、攻撃の「波」の区切り方や「別種」の判定基準に事業者の迷いが生じると、報告様式の記述方法を巡って手続きの受理が停滞する懸念があります。 つきましては、「別種の攻撃（波）」の分割基準を例示いただくか、または「速報段階では事業者の判断で一括・分割のいずれで記載しても不備とはしない」旨の運用上の柔軟性を明記いただくようお願いいたします。 ３、申合せ別添様式案 ランサムウェア事案共通様式 P７、その他サイバー攻撃等事案共通様式P１６ 意見 初動対応時に抽出したIoC（IPアドレス等）について、誤検知の可能性が残る未確証の情報であっても本欄に記載すべきか、あるいは確証が得られた情報のみに限定すべきかについての記載基準をご教授ください。 報告遅延を防ぎ迅速な速報を担保する観点から、「未確定情報であってもその旨を併記して報告可能であり、後の精査で除外・補正された場合でも手続上の不備とは扱わない」旨を運用の手引き等へ明確に追記いただくことを要望いたします。	１．につきましては、別添様式２及び３を用いて行う報告を個人情報の保護に関する法律（平成15年法律第57号）第26条第１項に基づく報告として取り扱うことが可能です。御指摘の「補填範囲」につきましては、報告の根拠となる法令、ガイドライン等により異なるため、それぞれの法令、ガイドライン等を参照してください。 ２．攻撃の「波」の区切り方や「別種」であるかの判断については、当該攻撃の発生状況を踏まえ、設定いただいて問題ありません。 ３．記載いただくIoCなどの攻撃技術情報は、報告時点で記入可能な項目かつ未確証の情報であっても問題ありません。また、情報収集等に時間を要する場合にはインシデント報告と別のタイミングで既に行った報告との関連がわかるように情報提供いただいても問題ございません。ただし、既に行った報告に誤報箇所があった場合は、続報等で訂正・補足いただくようにお願いします。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。

No.	御意見の要旨	御意見に対する主な考え方
27	○項目 報告様式 ○確認 関係政府機関への報告様式が統一されることは報告時の負荷軽減に繋がるものとして賛同いたします。 その中で、統一される様式の対象について確認させてください。 生命保険会社においては、本法令の適用対象事業者（経済安全保障推進法に基づく「特定社会基盤事業者」）以外の会社も含め、平成18年9月に発出された報告徴求命令（金監1853号）※に基づきシステム障害等に係る報告が求められているところ、今回の報告様式統一を受け、当該命令に基づく報告に係る様式は廃止され、"関係省庁申合せ別添様式3"に統合される、との認識でよいでしょうか。 ※登録金融機関業務を営む場合は平成19年9月発出の報告徴求命令（金監2420号）に基づく報告も求められる。 ○項目 各様式冒頭及び各記入項目ページ ○意見 初報は最小限、続報・詳報で詳細化する段階報告を明文化いただきたい。そのために各様式又は記載要領に以下を明記いただきたい。 ---- 初報は、発生又は検知日時、影響を受けた又は受けたおそれのある業務・システム、現時点の影響、実施済みの封じ込め措置、連絡先、不明事項に限定して提出できる。攻撃手法、侵入経路、漏えい有無、詳細IoC、復旧見込み、再発防止策等は、続報又は詳報において調査進展に応じて報告できる。 ---- ○項目 申合せ案「1.目的」、「2.対象とする手続」 ○意見 既存報告との「形式的一元化」にとどまらず、重複照会を抑制する「実質的一元化」を実現いただきたい。そのために、申合せに以下を追記いただきたい。 また、同一内容の重複提出や重複照会が極力生じない運用となることを期待します。 ---- 共通様式により提出された項目については、各行政機関間で共有済みの情報については重複照会を避ける。追加照会が必要な場合も、官民連携基盤上で照会内容及び回答状況を共有し、同趣旨の質問が複数機関から重複して行われないよう運用する。 ---- ○項目 申合せ案「NCOへの共有」「官民連携基盤」 ○意見 報告情報の共有先、利用目的及び二次利用の考え方について明確化いただきたい。 ○項目 ランサムウェア事案共通様式 ○意見 ランサムウェア復旧実務に即し、調査・封じ込め・復旧準備が並行して進むことを前提に様式を整備いただきたい。そのために復旧状況を段階的に記載できるよう、記載例の充実をお願いしたい。 ○項目 別添様式1、別添様式2、別添様式3、対象手続 ○意見 DDoS、ランサムウェア、その他攻撃の分類について、複合事案・未確定事案の扱いを明示いただきたい。そのために、各様式に以下の選択肢又は自由記載欄を設けていただきたい。 ---- 「分類未確定」「データ窃取のみ」等。報告後に分類を変更又は追加できることを明記する。 ----	（１つ目）現在、金融庁においては、当該関係省庁申合せの改定を踏まえ、「主要行等向けの総合的な監督指針」等の一部改正（案）についてパブリックコメント手続を実施しているものと承知しております。御指摘の点は、これらの改正内容に関する事項であることから、当該手続の実施期間中である現時点において、確定的な回答を行うことは差し控えさせていただきます。 その上で、金融庁が公表している改正案の概要においては、「関係省庁申合せの改正を踏まえ、従来の報告様式から関係省庁申合せに基づく共通様式へ移行することとする」とされており、従来の報告様式については、関係省庁申合せに基づく共通様式へ移行する方向で検討が進められているものと承知しております。なお、御指摘の報告徴求命令に基づく報告様式の取扱いについては、金融庁における検討及びパブリックコメント手続の結果を踏まえて整理されるものと承知しております。 （２つ目及び５つ目）御指摘については、各別添様式１頁目１．（２）①に「報告をしようとする時点で把握している範囲で、１から６までの内容を記載してください。」と記載するとともに、各別添様式の４及び各別紙の冒頭に「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。」又は「報告時点で記入可能な項目を記載してください。不明箇所は空白で構いません。」と記載しております。 （３つ目）御指摘を踏まえ、申合せ本文を修正しました。 （４つ目）各別添様式において「本様式に記載いただいた内容は、報告先機関から、内閣官房国家サイバー統括室に共有されます。内閣官房国家サイバー統括室は、報告された内容を整理分析の上、被害者が分からないようにした上で、被害の拡大防止のため、注意喚起等に活用することがあります」等と記載しております。 （６つ目）御指摘の具体的な提出先や提出方法、追加的な報告事項の有無、共通様式を提出した後の別途報告の要否については、報告の根拠となる各法令・ガイドラインにより異なる可能性があることから、各法令・ガイドラインを参照してください。

No.	御意見の要旨	御意見に対する主な考え方
28	本様式においては、個人情報の保護に関する法律等に理解の深い法務部門ではなく、サイバーセキュリティ担当者が起票することを想定する場合に、平易な表現または補足の説明があった方が良いと考えます。以下は例です。 【ランサムウェア事案共通様式】 「強化法第５条による報告の場合」自社が該当するのかしないのか判断する際の補足があると良い。 【その他サイバー攻撃等事案共通様式　（不正アクセス、情報窃取等】 ●「サイバー攻撃等の類型」　「不正アクセス／マルウェア感染／フィッシングによる情報窃取／脆弱性の悪用／内部不正　などを指すと思われるので例として記載するのが良い。 以下は今回の改正案対象ではないが、今後のご参考として意見を提出させてください。 【ランサムウェア事案共通様式】 「３）個人データ、保有個人情報又は特定個人情報の漏えい等について（報告を行う様式にチェックすること。）の箇所の１～３について、以下の例のような平易な表現が良い。 例） -民間事業者が、通常の個人データを漏えいした場合→別紙１ -行政機関等が、保有個人情報を漏えいした場合→別紙２ -民間・行政問わず）漏えいした情報にマイナンバーが含まれていた→別紙３（別紙１または２に加えて記入） 【別紙１～３】 ●個人番号利用事務と個人番号関係事務の違い 　民間は個人番号関係事務がほとんどかと思われるためその点を記載してほしい。 ●基礎項目評価、重点項目評価　とは何を指しているのか？→民間企業は関係ないのであればそのように明記したほうがよい。 ●滅失・毀損の簡易解説 ●法第9条・19条違反の簡易解説 ●規則第２条各号該当性の記載粒度例 第１号（情報提供ネットワークシステム等）→情報提供ネットワークシステム等又は個人番号利用事務を処理するために使用する情報システム等で管理される特定個人情報の漏えい等 第２号（不正の目的）→不正の目的をもって行われたおそれがある、特定個人情報の漏えい等、又は不正の目的をもって利用・提供されたおそれがある事態 第３号（不特定多数の者に閲覧）→特定個人情報ファイルに記録された特定個人情報が電磁的方法により不特定多数の者に閲覧され、又は閲覧されるおそれがある事態 第４号（百人超）→本人の数が100人を超える事態非該当→上記いずれにも該当しない場合	御指摘の強化法第５条の報告の対象は特別社会基盤事業者であり、特別社会基盤事業者に対しては、様々な機会を捉え、制度を周知しております。御指摘の「サイバー攻撃等の類型」につきましては、記入すべき事項の例を今後公表する記入例においてお示しいたします。 「（３）個人データ、保有個人情報又は特定個人情報の漏えい等について」に関するご意見については、今後の施策の参考とさせていただきます。
29	１.攻撃技術情報の記載粒度統一 該当箇所： 別添様式1「4. (2) 攻撃類型」 様式2「4. (3) ランサムウェアの類型」 様式3「4. (2) サイバー攻撃等の類型」 意見： 様式2及び様式3の類型欄にも、MITRE ATT&CK（サイバー攻撃の手口を体系化した知識ベース）のTechnique IDを付した選択肢を例示し、参照バージョンを明記すべきである。なお、選択は任意とし、自由記述との併用を可能とすることが望ましい。 理由： 様式1のみ構造化されている一方、様式2及び様式3は自由記述であるため、報告先機関における横断的な集計や経年比較が困難である。 ２.機械可読形式による別ファイル提出の推奨明示 該当箇所： 各様式のインディケータ情報に関する別ファイル提出注記 意見： 別ファイル提出時の推奨形式として、STIX 2.1等の機械可読形式（他形式も選択可）を手引きに例示すべきである。 理由： インディケータ情報は数百件から数千件に及ぶ場合があり、形式が不統一であると機械処理が困難となり、注意喚起や情報共有が遅延するおそれがある。 ３.論理的隔離の取扱い明確化 該当箇所： 様式2及び様式3「感染時の留意事項」 意見： 技術的手段により感染端末を論理的に隔離し、物理的遮断と同等以上の安全性を確保できる場合には、物理的な抜線を行わないことができる旨、及び専門事業者の助言に従って差し支えない旨を追記すべきである。なお、原則として物理的遮断を優先する考え方は維持する。 理由： 論理的隔離は、横展開防止と遠隔調査の継続を両立できるため、法令の目的である原因究明及び再感染防止を、より高い水準で達成し得る。	１．の御指摘の箇所につきましては、記載されうるMITRE ATT&CKのTechniqueが多岐にわたるため、網羅的に選択肢として示すことは困難ですが、記入すべき事項の例については、今後公表する記入例においてお示しするとともに、報告されるサイバー攻撃の傾向を踏まえ、適宜見直しを行ってまいります。 ２．別ファイルで提出する場合は、報告者の報告負担を軽減する観点から任意の形式で提出いただけます。 ３．御指摘の「感染時の留意事項」につきましては、一般的に推奨される事項を示したものであり、これによらない合理的な理由がある場合には、問題ありませんので、その趣旨を明確化する修正を行いました。 ３．御指摘の「感染時の留意事項」につきましては、一般的に推奨される事項を示したものであり、これによらない合理的な理由がある場合には、問題ありませんので、その趣旨を明確化する修正を行いました。

No.	御意見の要旨	御意見に対する主な考え方
30	報告様式の一元化によって被害組織の負担軽減や政府対応の迅速化を図る趣旨自体には合理性があると考えます。一方で、今回の共通様式では、内閣官房国家サイバー統括室への共有を希望しない旨を記載できる一方、サイバー対処能力強化法第5条に基づく報告の場合には、共有を希望しないとしても同室等へ情報提供される場合があるとされています。報告者にとって、どの情報が共有拒否の対象となり、どの情報が拒否の意思にかかわらず共有されるのか、その共有先、法的根拠及び利用目的が十分に明確とはいえません。 また、共通様式では、報告者や担当者の情報、影響を受けたシステム、攻撃に関する技術情報等に加え、場合によっては個人情報保護法や番号利用法に基づく漏えい報告とも接続し、氏名、住所、連絡先、パスワード等の情報を扱うことになります。 こうした情報を一元的に取り扱う以上、単に報告様式を共通化するだけでなく、情報共有の範囲を必要最小限に限定し、目的外利用及び不必要な横断利用を防ぐための明確な歯止めを設ける必要があります。 具体的には、少なくとも以下を明確にしてください。 ＊ 「共有等を希望しない」とした場合でも共有される情報の範囲、共有先、法的根拠及び利用目的 ＊ 国家サイバー統括室その他の機関におけるアクセス権限及び再共有の範囲 ＊ 情報の保存期間及び削除基準 ＊ 個人情報、特定個人情報及び重要システムに関する技術情報の目的外利用の禁止 ＊ アクセス記録の保存及び監査の仕組み ＊ 情報共有の必要性及び範囲を定期的に検証し、その結果を公表する仕組み 申合せでは、各省庁等の適用状況やサイバー攻撃の傾向を随時検証し、不断の見直しを行うとされています。 この見直しには、情報収集・共有の必要性だけでなく、共有拒否の実効性、保存期間、利用実態、再共有、アクセス状況等の検証も明示的に含めるべきです。 報告窓口の一元化が、必要性・相当性が十分検証されないまま行政機関における情報集約や利用範囲の拡大につながることがないよう、共通様式の導入と同時に、必要最小限性、目的限定、透明性、監査及び削除に関する具体的な保障を、本告示及び関連する省令・ガイドライン等を通じて明確にすることを求めます。	御指摘の「「共有等を希望しない」とした場合でも共有される情報の範囲、共有先、法的根拠及び利用目的」及び「国家サイバー統括室その他の機関におけるアクセス権限及び再共有の範囲」につきましては、各様式１頁目の（注）にお示ししており、その詳細については、強化法の各条項及び重要インフラ行動計画別添２．に記載されております。 御指摘の「情報の保存期間及び削除基準」につきましては、報告先となる各官公署等において公表している標準文書保存期間基準に基づき取り扱います。 また、報告いただいた情報については、政府機関等のサイバーセキュリティ対策のための統一基準（令和７年度版）第3部等に基づき取り扱うほか、強化法第５条に基づき報告いただいた情報については、強化法第８条（安全管理措置）の規定に基づき取り扱います。各別添様式は、事務連絡者の氏名等を記載いただく箇所はございますが、これらにつきましては、個人情報の保護に関する法律に基づき適切に管理いたします。なお、各別添様式は、御指摘の特定個人情報の記載を求めるものではありません。 御指摘の検証につきましては、本申合せ３．に記載しておりますとおり、各省庁等の適用状況や、サイバー攻撃の傾向を随時検証し、不断の見直しを行ってまいります。
31	**減税派・日本人ファーストの立場からの意見書（是々非々）** 内閣府政策統括官（サイバー安全保障担当）付 御中 関係各省庁 御中 令和8年8月15日 件名：「重要電子計算機に対する不正な行為による被害の防止に関する法律に基づく特別社会基盤事業者による特定侵害事象等の報告等に関する命令第四条第二項の特別社会基盤事業所管大臣及び内閣総理大臣が定める様式案」等に関する意見 私は、減税を重視し、日本人の生命・財産・国家主権を最優先する立場から、本件について是々非々で意見を述べます。サイバー攻撃被害報告の様式一元化・簡素化自体は、被害組織の負担軽減と政府の迅速対応を図る点で評価できますが、現行案では中国由来のサプライチェーンリスク・人的リスク・データ持ち出しリスクへの対処が不十分であり、実効性に欠けます。以下、具体的に指摘します。 ### 1. 基本的な評価（賛同する点） - **報告様式の一元化・簡素化** DDoS攻撃・ランサムウェア・その他サイバー攻撃事案について共通様式を定め、報告先の整理を進める方向は妥当です。被害組織が複数の官公署に重複報告する負担を減らし、初動対応に集中できる点は、民間の効率性を高め、結果として無駄な行政コスト（税金）の抑制につながります。減税派として支持します。 - **内閣官房国家サイバー統括室への情報集約** 同意に基づく情報共有を原則としつつ、重要電子計算機関連では法に基づき集約する仕組みは、被害拡大防止に資するものです。 これらは「日本人ファースト」の観点からも、国内インフラの迅速な防衛に寄与する限りで意義があります。 ### 2. 是正を強く求める点（批判的指摘と追加要望） 中国は国家主導でサイバー攻撃・産業スパイ・技術窃取を体系的に行っていることが国際的に明らかであり、特別社会基盤事業者（重要インフラ）における中国産製品・中国人職員・データ持ち出しは、日本国民の安全を直接脅かす最大のリスクです。様式案や申合せ改正ではこの点を無視しており、報告義務を形骸化させます。以下を明確に盛り込むことを求めます。 **(1) 中国産製品の原則廃止・使用禁止の明記** 報告様式に「使用している重要電子計算機・関連機器・ソフトウェアの製造国・調達先」を必須記載項目として追加し、中国産（中国企業製または中国資本関与製品）を原則禁止する運用基準を併せて策定すること。 理由：サプライチェーンを通じたバックドア・マルウェア混入リスクは極めて高く、事後報告だけでは被害防止に不十分です。日本人ファーストの立場から、国家安全保障上の脅威国製品を排除することは当然の措置です。減税派としても、一度の大規模被害で発生する復旧・補償コスト（最終的に税金負担）を未然に防ぐ方が財政的に合理的です。 **(2) 中国人職員・アルバイトの禁止** 様式に「特定重要電子計算機の運用・管理に関与する職員・アルバイトの国籍・在留資格」を必須記載項目とし、中国国籍者（永住者を含む）の関与を原則禁止すること。	１．につきましては、賛同の御意見として承ります。 ２．及び３．につきましては、今後の施策の参考と致します。

No.	御意見の要旨	御意見に対する主な考え方
	理由：人的スパイ・内部犯行のリスクが現実に存在します。日本人の雇用を優先し、国家機密・重要インフラに外国人（特に脅威国国籍者）を近づけないことは、日本人ファーストの核心です。経済合理性（減税）の観点からも、安価な労働力に依存してリスクを抱えるより、国内人材育成に投資する方が長期的に国益に叶います。 **(3) 書類・データの持ち出し禁止と厳罰化** 報告様式に「重要データ・設計情報・運用ログの外部持ち出し（USB・クラウド・紙媒体を含む）の有無と経路」を必須記載とし、中国を含む国外への持ち出しを原則禁止する規定を追加すること。違反した場合の刑事罰（懲役・罰金）をサイバー対処能力強化法または関連法令に創設すること。 理由：データ持ち出しは被害拡大の主因です。現状の報告義務だけでは抑止力が弱く、実効性ある刑罰が必要です。日本人の個人情報・産業データ・国家インフラ情報を守ることは、日本人ファーストの最低条件です。減税派としても、事後の損害賠償や行政対応コストを抑える予防措置として支持します。 **(4) 是々非々のバランス** - 過度な規制で民間の自由を奪い、行政コストを肥大化させることには反対です。中国リスクに特化した最小限の禁止・罰則とし、他の友好国製品や日本人職員への規制拡大は避けるべきです。 - 様式追加による報告負担増は、デジタル提出の徹底と自動入力支援で最小限に抑えること。 - 罰則は「故意・重大な過失による持ち出し・隠蔽」に限定し、軽微な違反にまで広げないこと。 ### 3. 結論 本件の様式案・申合せ改正は、報告負担軽減の点で方向性は正しいものの、中国由来のリスクを直視せず、日本人の安全を守る実効性に欠けるため、このままでは不十分です。中国産製品の原則廃止、中国人職員・アルバイトの禁止、書類・データの持ち出し禁止と刑罰創設を明確に盛り込むよう強く求めます。 税金を無駄にせず、日本人の生命と国家主権を最優先する制度設計を実現してください。過剰な行政肥大ではなく、真に必要な安全保障措置を講じることが、減税と日本人ファーストの両立です。 以上、意見として提出いたします。	
32	対象：申合せ案、申合せ別添様式案 意見及び質問： 1　申合せ案、申合せ別添様式案において、国家サイバー統括室への情報共有を行うにあたり、一定の場合（5条報告及び行動計画に基づくもの。以下同様）を除き、報告者の同意を要件としているのはなぜか。 2　様々なサイバー脅威に適切かつ迅速に対処するには、事案に応じて国家サイバー統括室に当該対処に必要な情報が適時適切に共有される必要があり、一定の場合を除き、報告者の同意にその共有を行うかどうかをかからしめるのは不適切である。こういう文案が出てくると、政府のサイバー脅威への認識が甘いのではないかという疑いを抱きざるを得ない。 実際のところ、報告者が不同意としても、所掌事務の範囲内で、法令の規定や内閣の調整機能等により各府省に報告を求めるのではないか。そうだとすると、現状の記載では一定の場合を除きここで不同意とすれば報告府省以外には共有されないとの印象を抱かせる点において報告者の意思に反することとなりかねない。 以上の点から、報告者の同意に係る部分については極めて不適切であり、削除を強く求めたい。	１．御指摘の一定の場合を除き、報告者の同意なく内閣官房国家サイバー統括室に情報を共有する根拠がないためです。 ２．我が国全体のサイバーセキュリティを強化するためには、官民双方向の情報共有を促すことが必要不可欠です。そのためには、内閣官房国家サイバー統括室への情報共有にあたり、報告者の意思を確認することなどを通じ、官民の信頼関係の醸成を図る必要があると考えております。

No.	御意見の要旨	御意見に対する主な考え方
33	【意見】 特定侵害事象等の報告様式において、情報漏えいが発生し、又は発生したおそれがある場合、「どのような情報が何件流出したか」だけでなく、流出したデータが実際に復元・閲覧・悪用可能な状態であったかを確認できる項目を追加することを要望します。 具体的には、次の事項を報告項目として検討していただきたいです。 1. 流出したデータが平文その他そのまま内容を読み取れる状態であったか、暗号化、秘密分散、データ無意味化等の技術的保護が講じられていたか。 2. 流出したデータ単体で、本人情報、機密情報、システム情報等の内容を復元・利用できる状態であったか。 3. 暗号化されていた場合、復号鍵、認証情報その他の復元に必要な情報も侵害された可能性があるか。 4. 秘密分散、データ無意味化又は分散保管等が行われていた場合、取得されたデータ片だけで内容を復元できる状態であったか。他のデータ片や復元に必要な情報が安全に保たれているか。 5. 情報保護措置が、利用者による個別の判断・操作を必要とする仕組みであったか、それとも所定の保存領域への保存等により、システム側で自動的に保護が適用される仕組みであったか。 6. 端末ローカル、クラウド、共有フォルダ、委託先、バックアップ、外部記憶媒体等に、保護されていないデータが残っていなかったか。 7. 以上を踏まえ、取得された情報が第三者によって実際に悪用される可能性及び、利用者・取引先・国民等への二次被害の程度。 【理由】 サイバー攻撃による被害の大きさを適切に判断するためには、「侵入された」「データが外部に出た」という事実だけではなく、攻撃者が取得したデータが実際に利用できる状態であったかを確認することが重要だと考えます。 例えば、同じ100万人分の情報が外部へ取得された事案であっても、平文のデータが取得された場合と、秘密分散等によって取得されたデータ片単体では内容を復元できない場合では、実際の被害リスクは大きく異なります。 そのため、報告様式にデータの保護状態、復元可能性、悪用可能性を明示する項目を設けることで、政府が事案の重大性をより正確に評価し、必要な対策や注意喚起を判断できると考えます。 また、暗号化や情報管理ルールが存在していても、その保護措置を適用するために職員や従業員がその都度判断・操作しなければならない仕組みでは、操作漏れ、設定漏れ、誤保存、緊急時の例外的取扱い等が発生する可能性があります。 特に重要インフラや社会基盤を担う事業者では、サイバー攻撃時には通常とは異なる対応が増え、平時に定めた運用ルールを完全に守ることが難しい場面も想定されます。 そのため、報告様式において、 「保護措置が人の判断・操作に依存していたか」 「通常どおり保存することでシステム側が自動的に保護する設計となっていたか」 という点についても確認することには意味があると考えます。 今後のサイバーセキュリティでは、「侵入を防ぐ」「検知する」「復旧する」という対策に加えて、 「侵入される可能性もある」 「人は誤操作する可能性がある」 「委託先やクラウドから流出する可能性もある」 ことを前提として、万一取得された場合でも、データそのものを復元・悪用されにくい状態にしておくことが重要だと考えます。 秘密分散、データ無意味化及び分散保管等は、そのような「侵害後の被害最小化」を実現するための技術的選択肢の一つです。 例えば、データを複数に分散し、それぞれのデータ片単体では意味を持たない状態にしておけば、一部のデータが端末、クラウド、委託先等から取得された場合でも、直ちに元の情報を利用されるリスクを低減できる可能性があります。 また、利用者が特別な暗号化操作等を行わなくても、所定の保存領域へ通常どおり保存することで、システム側が自動的にデータを保護する設計であれば、人為的な操作漏れや判断の違いを減らすことにもつながります。 こうした対策が行われていたかを報告様式で確認することは、単に事故後の被害把握に役立つだけでなく、企業側に「流出した後の被害まで考慮したシステム設計」を促す効果も期待できると考えます。 なお、秘密分散や暗号化等が実施されていたことだけを理由として、直ちに報告義務を免除することを求めるものではありません。 他のデータ片、復号鍵、認証情報等の管理状況も含め、実際の復元可能性・悪用可能性を評価するための情報として報告項目に加えていただきたいという趣旨です。 特定の企業や製品の採用を求めるものではありません。 暗号化、秘密分散、データ無意味化、分散保管及びシステムによる自動的な保護等を、「侵害時の被害最小化」という観点から評価できる報告様式としていただくことを要望します。	御指摘の１．から６．までにつきましては、被害防止に一定程度有用な場合もあるものの、報告者における調査に係る負担が過大となることから、現時点において一律に記載を求める考えはございません。 御指摘の７．につきましては、別添様式２及び別添様式３の各別紙において「（６）二次被害又はそのおそれの有無及びその内容」として記載いただくこととしております。