資料３－１：別紙

個人情報の保護に関する法律施行規則第八条第三項第一号及び第二号並びに第四十四条第三項並びに行政手続における特定の個人を識別するための番号の利用等に関する法律第二十九条の四第一項及び第二項に基づく特定個人情報の漏えい等に関する報告等に関する規則第三条第三項に規定する個人情報保護委員会が別に定める場合及びその方法を定める件の一部を改正する告示（案）に関する意見募集結果

番号	寄せられた御意見等	御意見等に対する考え方
1	サイバー攻撃に関して報告書の様式の追加や官民連携基盤を創設する趣旨は理解しました。ただ、今期で採決された個人情報保護法の改正案にて個人の情報は企業に勝手に流されるという報道を聞きまして、このサイバー攻撃にて仮に個人が打撃を受けた場合、その対策はなされるのでしょうか。これはただ報告書の追加や創設するだけ、という提案なのか、どうにも理解できませんでした。個人情報は文字通り個人が個人でもっているべきものです、官民連携基盤においても徹底して個人を保護するようにしてください。 【匿名】	本改正案は、サイバー攻撃等事案に関する個人情報保護委員会又は事業所管大臣への個人情報の漏えい等報告について、関係省庁申合せ別添様式３を提出する方法及び官民連携基盤を用いる方法によることを可能とするものです。今後の官民連携基盤の運用については国家サイバー統括室において適切に対応されるものと考えます。
2	件名：「個人情報の保護に関する法律施行規則第八条第三項第一号及び第二号並びに第四十四条第三項並びに行政手続における特定の個人を識別するための番号の利用等に関する法律第二十九条の四第一項及び第二項に基づく特定個人情報の漏えい等に関する報告等に関する規則第三条第三項に規定する個人情報保護委員会が別に定める場合及びその方法を定める件の一部を改正する告示（案）」に対する意見 １．意見の趣旨 本改正は、サイバー攻撃事案に係る官公署への報告手続を一元化・簡素化し、報告を行う事業者・行政機関等（以下「報告組織」という。）の負担軽減を図るものと理解する。この目的自体には異論はないが、本改	（１）について、本改正案は、サイバー攻撃等事案に関する個人情報保護委員会又は事業所管大臣への個人情報の漏えい等報告について、関係省庁申合せ別添様式３を提出する方法及び官民連携基盤を用いる方法によることを可能とするものであり、それ

	正及びその基礎となる「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」は、一貫して報告組織側の手続負担軽減に焦点を当てており、漏えい等により実際に被害を受ける本人（顧客・従業員・国民等）への通知・説明・救済の迅速化という観点が、制度設計上明確に位置付けられていないのではないか。 ２．具体的な懸念点 第一に、「その他サイバー攻撃等事案共通様式」（別添様式３）の別紙１「（７）本人への対応の実施状況」は、「対応済（対応中)」「対応予定」「予定なし」の選択式であり、「予定なし」を選んだ場合も理由の記載のみで足りる構成となっている。本人通知について標準的な期限や最低限の実施内容が定められないまま、行政への報告様式のみが整備・一元化されることは、報告組織にとっての手続的な利便性が先行し、本人保護の実効性が置き去りにされる結果を招きかねない。 第二に、官民連携基盤の整備により、内閣官房国家サイバー統括室への情報集約は制度的に強化される一方、集約された情報がどのように本人への注意喚起や被害拡大防止に活用されるか、その運用上の担保が本様式・本改正案からは明らかでない。行政側の情報収集体制の強化と、本人の知る権利・救済を受ける権利の強化とが、対をなす形で整理されるべきである。 ３．要望事項 以上を踏まえ、以下を要望する。 （１）共通様式における「本人への対応の実施状況」について、「予定なし」とする場合の理由記載を求めるだけでなく、本人通知を行うべき標準的な期限（例：漏えい発覚後速やかに、又は具体的な日数）についてのガイドライン上の目安を別途明示すること。 （２）官民連携基盤を通じて集約された情報が、本人への注意喚起や二次被害防止にどのように活用されるかについて、運用ルールを明確化し、公表すること。 （３）報告手続の一元化・簡素化を進める場合であっても、それが本人保護の後退につながらないよう、施行後一定期間を経て、本人対応の実施状況（特に「予定なし」の選択割合や理由）について検証・公表を行うこと。	以外の従前の取扱いについて変更するものではありません。 （２）、（３）について、頂いた御意見は今後の執務の参考とさせていただきます。

	以上 【匿名】	
3	意見 本改正案には反対します。 個人情報及び特定個人情報（マイナンバー）は、一度漏えいすると本人に重大かつ長期的な被害を及ぼすおそれがあるため、その取扱いには最大限の慎重さが求められます。 今回の改正案は、サイバー攻撃等に係る報告手続の見直しを目的としているとされていますが、報告対象や報告方法、例外規定の運用について、国民に十分理解できる説明がなされているとは言えません。制度の簡素化や効率化を優先するあまり、漏えい事案の把握や監督が不十分になることを懸念します。 特に、報告を要しない場合の取扱いについては、例外が拡大していると受け取られるおそれがあり、事業者等による報告が抑制されることがないよう慎重な制度設計が必要です。国民の信頼を維持するためにも、透明性を損なうおそれのある改正は避けるべきです。 また、改正によって実際にどのような運用変更が生じるのか、国民が理解しやすい形で具体例を示した説明が不足しています。制度改正に先立ち、十分な情報提供と丁寧な説明を行うべきです。 以上の理由から、本改正案には反対し、現行制度を維持するか、少なくとも報告義務や透明性が後退しないことを明確に担保した上で再検討することを求めます。 【個人】	本改正案は、サイバー攻撃等事案に関する個人情報保護委員会又は事業所管大臣への個人情報の漏えい等報告について、関係省庁申合せ別添様式３を提出する方法及び官民連携基盤を用いる方法によることを可能とするものであり、それ以外の従前の取扱いについて変更するものではありません。

4	1. ゲノム情報（DNA 等）および病歴情報等の「要配慮個人情報」に対する AI 学習・収集プロセスの厳格な規制および漏えい報告基準の強化について 【理由・背景】 今回の改正において、個人情報保護委員会が別に定める漏えい等の報告義務基準が議論されているが、とりわけ個人の尊厳やプライバシーに直結する DNA（ゲノムデータ）や病歴、特定個人情報（マイナンバー関連情報）といった極めて機微な「要配慮個人情報」の扱いについて、国民の不安は極めて大きい。 昨今、本人の明確かつ個別具体的な同意を得ることなく、AI の機械学習やデータ収集のプロセスにおいてこれらの要配慮個人情報が事実上取り込まれ、処理されるリスクが顕在化している。AI による不透明なデータ収集およびプロファイリング（分析）行為自体が、広義の「不適切な取り扱い」および「漏えい・毀損の予兆」に該当し得る。 したがって、AI 技術を用いた要配慮個人情報の収集・学習プロセスにおける不正な取得や管理不備については、従来のデータ漏えい基準よりも遥かに厳格なしきい値を設け、極めて微細な検知であっても委員会への即時報告および本人告知を義務付けるよう、本件告示において明確な基準を規定することを強く求める。 2. 国外移転（外国の第三者へのデータ売却・提供）および海外事業者への委託に伴う漏えいリスクに対する、徹底的な監視と厳罰化について 【理由・背景】 我が国の国民のプライバシー権、および国家的な情報安全保障の観点から、国内で収集された DNA 情報や特定個人情報が、不透明な形で外国の第三者（AI 開発企業、クラウド事業者、データブローカー等）に提供・売却、あるいは実質的にアクセス可能な状態に置かれることは断じて容認できない。 外国政府の法制度（例えば、国家情報法などの政府によるデータ強制提出義務）が適用される地域への情報	本意見募集は本改正案について意見を求めるものであり、御意見は本意見募集の対象外であると考えます。

	移転や、海外の委託先における管理不備による実質的な情報流出は、国民生活の安全・安心を根底から揺るがす深刻な事態である。 本件告示で定める「漏えい等の報告義務」においては、「外国の第三者への提供、または海外委託先における漏えい・漏えいのおそれ」が発生した（またはその疑いが生じた）場合について、国内案件よりも迅速かつ網羅的な詳細報告を義務付ける厳格な特別基準を設けるべきである。また、流出が発覚した事業者に対しては、単なる報告の徴収にとどまらず、即座に移転差し止めや強力な是正措置・行政処分を下す根拠となるような、極めて厳格な執行基準をあわせて策定・明文化することを強く要望する。 【匿名】	
5	その他サイバー攻撃等事案共通様式において、本人への対応への実施状況が　対応済み　対応予定　予定なし　とありますが、予定なしに関して理由を聞くべきです。個人情報を扱っているのです。予定なしがチェック項目だけなのは、個人情報をないがしろにしているように見受けられます。 【匿名】	本改正案は、サイバー攻撃等事案に関する個人情報保護委員会又は事業所管大臣への個人情報の漏えい等報告について、関係省庁申合せ別添様式３を提出する方法及び官民連携基盤を用いる方法によることを可能とするものです。今後、当該申合せや共通様式の改定等については国家サイバー統括室において適切に対応されるものと考えます。
6	該当箇所 改正概要「4. 改正の概要」及び告示案中、「その他サイバー攻撃等事案共通様式」を提出する方法並びに官民連携基盤を使用する方法を追加する部分 意見	本改正案に賛成の御意見として承ります。 共通様式又は官民連携基盤を利用した場合の漏えい等報告の運用につ

	本改正案の方向性に賛成します。 その上で、本告示の施行時までに、個人情報保護法第 26 条第 1 項及び第 68 条第 1 項並びに番号法第 29 条の 4 第 1 項に基づく報告について、共通様式又は官民連携基盤を利用した場合の取扱いを、個人情報保護委員会のウェブサイト、FAQ 又は利用案内で明示してください。 少なくとも、次の事項を確認できるようにすることが必要と考えます。 1. 官民連携基盤又は共通様式による提出をもって、個人情報保護委員会又は事業所管大臣への報告が完了すると扱われる時点 2. 従来の電子報告フォーム又は報告書への重複提出の要否 3. 速報後の続報、確報及び訂正を、先に提出した報告と接続する方法 4. 受付番号又はこれに相当する識別情報の取扱い 5. 官民連携基盤を利用できない場合の代替提出方法 これらを告示本文へ詳細に規定することを求めるものではありません。運用変更に応じて更新可能な FAQ 又は利用案内による対応で足りると考えます。 理由 今回の改正案は、従来の電子情報処理組織を使用する方法等に加え、その他サイバー攻撃等事案共通様式を提出する方法及び官民連携基盤を使用する方法を追加するものです。 一方、共通様式の記載の手引きでは、具体的な提出先、提出方法及び追加的な報告事項について、各法令、ガイドライン又は各省庁が公表する方法に従うとされています。 このため、報告者が、官民連携基盤又は共通様式による提出だけで個人情報保護法等に基づく報告が完了したのか判断できなければ、期限徒過を避けるため、従来の電子報告フォーム等にも同じ内容を重複して提出する可能性があります。 また、速報後に調査結果が更新された場合、どの受付番号を用いて続報又は確報を提出するかが分からなければ、同一事案が別件として受け付けられ、報告者と行政の双方に照合作業が発生する可能性があります。 本改正の目的である報告負担の軽減を実際の運用へ接続するには、個人情報保護委員会が所管する報告に	いては、当委員会ウェブサイト等において適切に周知してまいります。頂いた御意見は今後の執務の参考とさせていただきます。

	限って、追加された報告方法と従来の報告方法との関係を明示することが必要です。 この提案は、新たな報告義務、審査制度又は恒久的な調査事務を追加するものではありません。既に予定されている報告方法の取扱いを FAQ 等で整理するものであり、比較的軽い行政対応によって、重複提出及び受付上の混乱を防止できると考えます。 【個人】	
7	サイバー攻撃等事案の共通様式に賛成です。この様式の保護にも力を入れてください。報告書がまた流出した、などということにならないようにお願いします。個人情報保護法の改正によって、国から勝手に情報が企業へ渡されることを懸念している国民としては、これらのデータも外部へ流されるのではという危機感しかありません。 【匿名】	本改正案に賛成の御意見として承ります。 なお、提出された報告については、個人情報保護委員会又は事業所管大臣、更には共有を受けた場合には国家サイバー統括室においても行政文書として適切に管理します。
8	該当箇所 改正概要「4. 改正の概要」及び「その他サイバー攻撃等事案共通様式（別添様式 3)」のうち、個人データ、保有個人情報及び特定個人情報の漏えい等に関する報告項目 意見 「その他サイバー攻撃等事案共通様式」において、漏えい等が発生し、又は発生したおそれのある個人データ、保有個人情報及び特定個人情報について、情報の種類や人数だけでなく、流出したデータの保護状態、復元可能性及び悪用可能性を確認できる項目を設けることを要望します。	本改正案は、サイバー攻撃等事案に関する個人情報保護委員会又は事業所管大臣への個人情報の漏えい等報告について、関係省庁申合せ別添様式３を提出する方法及び官民連携基盤を用いる方法によることを可能とするものです。本意見募集は本改正案について意見を求めるものであり、御意見は本意見募集の対象外であると考えます。

	具体的には、次の事項を報告項目に加えることを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た状態であったか。 2. 流出したデータ単体で、本人を識別し、内容を復元し、又は悪用することが可能な状態であったか。 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流出した可能性があるか。 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、流出したデータ片だけで内容を復元できる状態であったか。また、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. 暗号化その他の技術的保護措置が、利用者による個別の判断、操作又は保存先の選択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適用される仕組みであったか。 6. 端末ローカル、共有フォルダ、クラウド、外部記憶媒体等への保存について、システムによる技術的な制御が行われていたか。操作漏れ、設定漏れ、誤保存又は例外的な取扱いにより、保護されていないデータが残っていなかったか。 7. これらの保護状態を踏まえ、本人への二次被害、なりすまし、詐欺、差別その他の権利利益侵害が、具体的にどの程度生じるおそれがあるか。 速報の段階で判明していない事項については、「確認中」又は「不明」として報告し、調査の進展に応じて	

	続報又は確報で更新できる仕組みとすることが適切だと考えます。 理由 同じ種類、同じ人数の個人情報が流出した事案であっても、平文のデータが流出した場合と、暗号化や秘密分散等により、流出したデータ単体では内容を復元・悪用することが困難な場合とでは、本人に生じる実際の危険性が異なります。 そのため、漏えいした情報の種類や人数だけでなく、データの保護状態、復元可能性、本人識別可能性及び悪用可能性を報告項目として確認することにより、行政機関が事案の緊急性や本人への影響を、より正確に評価できると考えます。 また、暗号化機能や情報管理ルールが用意されていても、利用者が暗号化する情報を選択し、暗号化操作を行い、適切な保存先を選び、パスワードや暗号鍵を管理しなければ保護されない仕組みでは、操作漏れ、設定漏れ、誤保存及び緊急時の例外的な取扱いが生じる可能性があります。 規程、研修及び注意喚起は重要ですが、人が常に正しく判断し、定められた操作やルールを完全に守ることだけを前提とした安全管理措置には限界があります。特に、業務上の利便性、通信環境、処理速度、作業負荷等の事情により、現場で端末ローカルへの一時保存や例外的な取扱いが必要になる場合があります。 この点に関連して、2025 年 12 月に、VDI・DaaS を利用する企業の情報システム部門担当者 270 人を対象として実施された民間調査では、次の結果が示されています。 ・VDI・DaaS を利用している企業でも、端末ローカルへのデータ保管をシステム的にできないよう制御し	

	ている企業は約 3 割にとどまり、約 7 割の企業では端末ローカルにデータが保管される可能性がある。 ・セキュリティを VDI・DaaS の導入理由として挙げた企業でも、端末へのデータ保管をシステム的に制御している企業は約 4 割にとどまる。 ・VDI・DaaS を利用している企業の約 7 割が、業務上、端末へのデータ保管が必要であると回答している。 ・約 9 割の企業が、端末の盗難・紛失時のセキュリティに何らかの不安を感じている。 この調査は、セキュリティルールへの違反率を直接測定したものではありません。しかし、セキュリティを目的として VDI・DaaS を導入していても、業務上の利便性やネットワーク環境等の事情から、端末へのデータ保存を完全には排除できず、方針や運用ルールだけでは情報を保護しきれない場合があることを示唆しています。 したがって、漏えい等の報告においては、「暗号化機能やルールが存在していたか」だけでなく、実際に対象データへ保護措置が適用されていたか、その適用が人の判断や操作に依存していたか、システム側で自動的に適用される設計であったかを確認することが重要です。 例えば、所定の保存領域に通常どおり保存することにより、暗号化、秘密分散又はデータ無意味化等の保護措置がシステム側で自動的に適用される仕組みであれば、利用者による操作漏れや判断の違いを減らすことができます。 報告項目に「保護措置が自動的に適用される仕組みであったか」「保護されていない保存先や例外的な取扱いが存在していなかったか」という観点を設けることにより、単に保護機能が導入されていたかだけでな	

	く、実際の業務において保護が確実に適用される設計であったかを評価できます。 なお、暗号化、秘密分散又はデータ無意味化が行われていたことだけを理由として、直ちに報告義務や本人通知を免除することを求めるものではありません。暗号鍵、認証情報、他のデータ片の管理状況、再識別可能性等を含め、事案ごとに実質的な危険性を評価するための情報として報告を求める趣旨です。 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といった技術・設計上のカテゴリを、漏えい時の被害を適切に評価するための共通項目として位置付けていただきたいという趣旨です。 参考とした調査 「VDI/DaaS の利用に関するアンケート調査」 調査対象：VDI・DaaS を利用する企業の情報システム部門担当者 270 人 調査方法：日経クロステック Active リサーチによるインターネット調査 調査時期：2025 年 12 月 なお、この調査は特定製品の採用を求める根拠としてではなく、情報保護を人的な判断や運用ルールだけに依存することの課題を示す民間調査の一例として引用するものです。 【個人】	
9	意見 1	意見 1 について、今後の当該関係省庁申合せや共通様式の改定等に係る

	【該当箇所】 改正の概要（報告の方法に関する部分） 【意見】 告示が申合せの別添様式を引用する形式を採る場合、当該様式の改定に当たっても意見募集又は事前の公表を行う旨を明らかにすべきである。 【理由】 改正案は、報告の方法として「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」の別添様式を提出する方法を定めるものである。この構成では、様式の記載事項が変更されても告示の文言は変わらないため、報告者が記載すべき事項が告示の改正を経ることなく変更され得る。当該申合せは「随時検証し、不断の見直しを行う」と定めており、様式の変更が予定されている。報告義務の実質的な内容に変更が生じる場合には、手続の透明性を確保する必要がある。 意見２ 【該当箇所】 改正の概要（報告の方法に関する部分） 【意見】 新たに追加される報告方法と、現行の報告方法との関係を明示すべきである。 【理由】改正案は既存の報告方法に加えて共通様式及び官民連携基盤による方法を追加するものであるが、報告者がいずれかの方法を選択した場合に他の方法による報告が不要となるのか、また受付番号の通知や続報の提出をどの経路で行うのかが明らかでない。別添様式には個人情報保護委員会から通知された受付番号を記載する欄が設けられており、経路をまたぐ運用が想定されるが、その手順は示されていない。 【匿名】	意見募集については、国家サイバー統括室において対応されているものと考えます。 意見２について、共通様式又は官民連携基盤を利用した場合の漏えい等報告の方法については、当委員会ウェブサイト等において適切に周知してまいります。頂いた御意見は今後の執務の参考とさせていただきます。
10	AI による自律的サイバー攻撃時代を踏まえた個人情報保護・漏えい対策の抜本的強化を求める意見】	本改正案は、サイバー攻撃等事案に

	今回の告示改正案について、強い懸念を表明します。 現在、AI 技術は急速に高度化しており、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を収集・分析し、外部システムへアクセスし、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。 このような状況において、個人情報保護を「漏えいが起きた後に報告する」という事後対応だけで考えることは不十分です。 AI が大量の個人情報を高速で処理し、複数の情報を組み合わせ、本人が提供した情報から本人が想定していなかった情報まで推測できる時代になっています。 さらに、AI が自律的に外部システムへアクセスできるようになれば、ひとたび個人情報への不正アクセスが発生した場合、人間が手作業で行う場合とは比較にならない速度と規模で情報が取得・複製・分析される危険があります。 一度漏えいした個人情報を完全に回収することはできません。AI によって複製・分析・推測された情報を、後から「なかったこと」にすることもできません。 したがって、本当に必要なのは、漏えい後の報告手続を整備するだけではなく、そもそも AI を含む高度なシステムから個人情報を不正に取得・利用されないための予防措置を徹底することです。 特に、AI に個人情報へのアクセス権限を与える場合には、目的外利用を防止する技術的措置、最小限の権限設定、人間による監督、アクセス記録の保存、異常なアクセスの即時検知・遮断等を義務化すべきです。 「AI が勝手にサイバー攻撃をすることは想定していなかった」という事後的な説明では、国民の個人情報は守れません。 AI の能力が今後さらに高度化することを前提に、最悪の事態を想定した制度設計を行うべきです。 また、現在進められている個人情報保護法改正では、本人同意なしの第三者提供等、個人情報の利活用を拡大する方向が示されています。しかし、個人情報を利用・流通させる範囲を広げるのであれば、それに比例して漏えい時の被害リスクも高まります。 AI による自律的な情報処理やサイバー攻撃が現実のものとなっている現在、個人情報の利用範囲を拡大す	関する個人情報保護委員会又は事業所管大臣への個人情報の漏えい等報告について、関係省庁申合せ別添様式３を提出する方法及び官民連携基盤を用いる方法によることを可能とするものです。 本意見募集は本改正案について意見を求めるものであり、御意見は本意見募集の対象外であると考えます。

	ることを先行させるのは危険です。 個人情報は単なる「データ」ではありません。国民一人ひとりの生活、人格、プライバシーそのものです。 本告示案については、AI による自律的なサイバー攻撃・情報取得・情報分析まで想定した安全対策が十分に盛り込まれているのか、根本から再検討してください。 そして、個人情報保護法改正についても、こうした最新の AI リスクを十分に検証した上で、施行を強行するのではなく、撤回・廃止を含めて抜本的に見直すべきです。 「漏えいしたら報告する制度」だけでは国民の個人情報は守れません。 漏えいそのものを防ぐこと、AI による不正利用を防ぐこと、本人の同意なく個人情報が広範に利用されることを防ぐことを最優先にしてください。 国民の個人情報を AI 時代の無制限な利活用やサイバー攻撃のリスクにさらさない制度へ転換することを強く求めます。 【匿名】	
11	本改正案に強く反対する。 個人情報やマイナンバーを含む特定個人情報は、ひとたび漏えいすれば本人が取り返すことのできない極めて重要な情報である。行政や事業者が扱う情報量が増え続けている現在、必要なのは情報を広く収集・共有する方向ではなく、情報を必要最小限にとどめ、漏えいそのものを防止する仕組みを徹底することである。 特にサイバー攻撃等を理由として、個人情報を含む情報の報告・共有範囲が拡大する場合には、誰が、何の目的で、どの範囲まで情報を取得し、どのように保存・共有・利用するのかを明確にしなければならない。 「安全保障」「サイバー対策」「被害把握」を理由にすれば、個人情報の取扱いが無制限に拡大してよいわけではない。行政機関間での情報共有についても、目的外利用や二次利用が起こらないことを法的に明確に担	本改正案は、不正アクセス事案等に関する個人情報保護委員会又は事業所管大臣への個人情報の漏えい等報告について、関係省庁申合せ別添様式３を提出する方法及び官民連携基盤において報告する方法によることを可能とするものであり、どの機関に対して報告を行うかは、報告者が選択することとされています。 提出された報告については、個人情報保護委員会又は事業所管大臣、更には共有を受けた場合には国家サイバ

	保すべきである。 個人情報は行政の都合で扱ってよい情報ではなく、国民一人一人の人格と私生活に直結するものである。 本改正案について、情報収集・報告・共有の範囲、保存期間、第三者提供、目的外利用、漏えい時の責任を十分に明確化できていないのであれば、安易に施行すべきではない。 国民のプライバシーを犠牲にして利便性や行政効率を優先する制度変更には反対する。拙速な改正は撤回し、国民の権利を最優先にした制度として改めて検討することを強く求める。 【匿名】	一統括室においても行政文書として適切に管理します。
12	**個人情報の保護に関する法律施行規則等に基づく特定個人情報の漏えい等報告に係る告示改正案等に対する意見書** 個人情報保護委員会 御中 標記の意見募集（個人情報の保護に関する法律施行規則第八条第三項第一号及び第二号並びに第四十四条第三項並びに行政手続における特定の個人を識別するための番号の利用等に関する法律第二十九条の四第一項及び第二項に基づく特定個人情報の漏えい等に関する報告等に関する規則第三条第三項に規定する個人情報保護委員会が別に定める場合及びその方法を定める件の一部を改正する告示（案）並びに関連する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・共通様式等）について、是々非々の立場から以下のとおり意見を提出します。	意見１について、本改正案に賛成の御意見として承ります。 意見２について、本意見募集は本改正案について意見を求めるものであり、御意見は本意見募集の対象外であると考えます。

	### 1. 改正案の基本的方向性に対する評価（是とする点） 本改正案の趣旨である、ランサムウェア事案その他サイバー攻撃等事案における個人データ・特定個人情報の漏えい等報告について、電子情報処理組織・官民連携基盤の利用や関係省庁申合せに基づく共通様式（別添様式2・3等）の活用を可能とし、被害組織の報告負担を軽減しつつ政府の対応迅速化を図る点は、適切かつ時宜を得たものと評価します。 サイバー攻撃件数が増加し、初動対応中の多重報告負担が指摘されている現状を踏まえ、報告様式の一元化・簡素化を進めることは、被害組織が本来注力すべき復旧・再発防止に資源を振り向けやすくするものであり、官民双方のサイバーセキュリティ強化に資します。施行期日を令和8年10月1日頃と想定し、関係省庁申合せの改定を踏まえた整理を行う点も合理的です。これらの方向性自体は支持します。 ### 2. 改正案に対する補完的指摘と懸念（非とする点・改善提案） 一方で、報告方法の整備のみでは不十分です。サイバー攻撃の多くがサプライチェーンや人的要因、物理的拠点を経由して発生している実態を踏まえれば、報告手続の円滑化と同時に、攻撃の「入口」そのものを封じる措置を講じなければ、本質的なリスク低減にはつながりません。特に国家安全保障上の観点から、以下の点を強く求めます。 #### （1）中国産製品の国家機関・地方自治体における使用禁止 サイバー攻撃（不正アクセス、情報窃取、ランサムウェア等）の技術的基盤として、ハードウェア・ソフトウェアのサプライチェーンリスクが極めて大きいことは周知の事実です。中国産の情報通信機器、サーバー、ネットワーク機器、ソフトウェア等については、バックドアや脆弱性の意図的・非意図的な混入が国際	

	的に指摘されており、重要インフラや行政機関での使用は国家安全保障上重大な脅威となります。 よって、国家機関および地方自治体において、中国産（中国企業・中国資本関連を含む）の情報システム関連製品・サービスの新規調達・使用を原則禁止する措置を、関連法令・ガイドラインの改正や本告示の運用指針等に盛り込むべきです。既存導入分についても、計画的な段階的排除を求めます。報告様式の整備だけでは「事後対応」に止まり、予防に欠けるためです。 #### （2）職員の日本人限定 行政機関等における個人情報・特定個人情報の取扱いは、国家の根幹に関わる業務です。外国人職員（特に特定の国・地域出身者）の配置は、スパイ活動や内部不正のリスクを高めます。サイバー攻撃事案の報告・対応過程でも、人的信頼性が極めて重要です。 よって、国家機関・地方自治体の情報システム関連部署、個人情報取扱業務、サイバーセキュリティ対応部署の職員については、原則として日本国籍を有する者に限定する人事運用を明確化し、関連規則・告示に反映させることを求めます。これは差別ではなく、国家安全保障上の合理的な制限です。 #### （3）外国人の土地取得禁止および既存取得分の収用 サイバー攻撃はデジタル空間に限らず、重要施設近傍の土地取得を通じた物理的監視・妨害・情報収集と連動するケースが懸念されています。外国人（特に中国等特定国の個人・法人）による土地取得が、防衛施設・重要インフラ・行政施設周辺で進んでいる現状は、報告手続の整備以前の問題です。 よって、国家安全保障上重要な土地について、外国人による新規取得を原則禁止し、既に取得されたものに	

	ついては、公共の安全を理由とする適正な補償を伴う収用手続を可能とする法整備を速やかに進めるべきです。本告示・申合せの対象であるサイバー対処能力強化法や個人情報保護関連制度とも整合する安全保障措置として位置づけてください。 ### 3. 総合的な意見（是々非々のまとめ） 報告負担軽減と様式一元化という「是」の部分は積極的に推進すべきです。しかし、それだけに止まり、サプライチェーン（中国産製品）、人的管理（職員の国籍制限）、物理的拠点（外国人土地取得）という根本的な脆弱性への対応を欠くのであれば、改正の実効性は半減します。サイバー攻撃の多くが特定の国家主体やその影響下にある主体と関連づけられる国際情勢を直視し、予防的な安全保障措置を合わせて講じることが不可欠です。 以上の点を踏まえ、告示案の最終化および関連する運用・他制度との連携において、上記提案を十分に検討・反映されるよう強く要望します。意見の採否にかかわらず、国民の個人情報と国家の安全を守る観点から、是々非々の真摯な対応を期待します。 以上 【個人】	
13	個人情報保護委員会 御中 「個人情報の保護に関する法律施行規則第八条第三項第一号及び第二号並びに第四十四条第三項並びに行政手続における特定の個人を識別するための番号の利用等に関する法律第二十九条の四第一項及び第二項に基づく特定個人情報の漏えい等に関する報告等に関する規則第三条第三項に規定する個人情報保護委員	本改正案は、サイバー攻撃等事案に関する個人情報保護委員会又は事業所管大臣への個人情報の漏えい等報告について、関係省庁申合せ別添様式３を提出する方法及び官民連携基盤

	会が別に定める場合及びその方法を定める件の一部を改正する告示（案）」について、以下のとおり意見を提出します。 本件は、個人情報保護法上の漏えい等報告に加え、番号利用法第 29 条の 4 に基づく特定個人情報の漏えい等報告制度に関わる重要な改正です。特に、関連資料として「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）」及び「その他サイバー攻撃等事案共通様式（別添様式 3）（案）」が示されていることから、本改正は単なる告示上の報告方法の整理ではなく、マイナンバーを含む特定個人情報ファイルがサイバー攻撃等の対象となった場合に、本人保護、被害拡大防止、行政横断的な情報共有、再発防止をどのように実効化するかという制度設計の問題です。 番号利用法第 29 条の 4 は、個人番号利用事務等実施者に対し、特定個人情報ファイルに記録された特定個人情報の漏えい、滅失、毀損その他の安全確保に係る事態であって、個人の権利利益を害するおそれが大きいものが生じた場合、個人情報保護委員会への報告及び本人通知を求めています。また、委託を受けた者が委託元に通知した場合の例外も設けています。したがって、本制度の中心は、特定個人情報ファイル単位で、どのような事態が、いつ、どの範囲で、誰の管理下で発生し、本人の権利利益にどの程度のリスクを生じさせたかを、迅速かつ正確に把握することにあります。 第一に、特定個人情報の漏えい等報告様式は、機械可読な形式で整備すべきです。サイバー攻撃発生時には、初動対応、封じ込め、証拠保全、本人対応、委託先・再委託先との調整、関係機関への報告が同時並行で発生します。報告様式が PDF、Excel、自由記述、メール添付中心である場合、事業者側では転記・再入力・重複報告の負担が大きく、行政側でも横断分析、重複排除、時系列把握、攻撃手法の共有、被害拡大防止が困難になります。共通様式は、人間が読む文書であると同時に、システムが処理できるデータであるべきです。	を用いる方法によることを可能とするものであり、それ以外の従前の取扱いについて変更するものではありません。 　なお、御意見の報告手続・共通様式に関しては、国家サイバー統括室において当該申合せや共通様式の改定等、適切に対応されるものと考えます。

	具体的には、PDF 又は表計算形式に加え、JSON Schema、CSV、OpenAPI、必要に応じて STIX/TAXII 等と連携可能な形式を提供すべきです。構造化すべき項目としては、事案 ID、発生日、検知日、報告日、初報・続報・確報の区分、特定個人情報ファイルの名称又は識別子、記録されていた情報の種別、推定対象者数、個人番号そのものの漏えい有無、本人確認情報との結合可能性、侵害経路、攻撃手法、利用された脆弱性、影響を受けたシステム、委託先・再委託先の関与、国外アクセスの有無、暗号化の有無、鍵漏えいの有無、認証方式、アクセスログ保全状況、封じ込め措置、本人通知状況、再発防止策等が考えられます。 第二に、報告制度は、件数や形式的な漏えい有無だけでなく、特定個人情報に対する実質的リスクを評価できる構造にすべきです。マイナンバーを含む特定個人情報は悪用時の影響が大きいため、厳格な管理が必要です。一方で、全ての事案を同一に扱うと、重要度の高い事案への対応資源が分散します。例えば、暗号化済みデータが外部に流出したが鍵は漏えいしていない場合、ログ上閲覧又は取得が確認されていない場合、バックアップの毀損であって外部流出がない場合、仮名化又はマスキングにより個人番号への到達が制限されている場合などは、本人リスクの性質が異なります。報告様式では、個人番号の露出可能性、本人識別性、他情報との結合可能性、攻撃者による取得可能性、鍵管理状況、ログ上のアクセス事実を区別して記録できるようにすべきです。 第三に、委託先・再委託先・クラウド・開発保守事業者が関与する場合の責任分界を明確化すべきです。番号利用法第 29 条の 4 は、委託を受けた者が委託元に通知した場合の例外を設けています。しかし実務上、特定個人情報ファイルは、クラウド、SaaS、BPO、システム保守、セキュリティ監視、バックアップ、ログ管理等を通じて複数の主体が関与します。サイバー攻撃時に、誰が初報を行い、誰がログを保全し、誰が本人通知の判断資料を作成し、誰が再委託先から情報を収集するのかが曖昧であると、報告遅延や証拠散逸を招きます。告示又は関連 Q&A において、委託契約に含めるべき報告条項、再委託先からの通知期限、ログ保全義務、事故時連絡経路、初報・続報・確報の役割分担を例示すべきです。	

	第四に、海外フリーランスエンジニア等の形式的排除ではなく、特定個人情報への実アクセス有無に基づくリスク管理を明確化すべきです。現場では、個人情報保護法、番号利用法、越境移転規制への過度な恐れから、「海外在住である」「外国人である」「国外からアクセスする可能性がある」という理由だけで、海外エンジニアや海外フリーランスを一律に排除する例があります。しかし、ソフトウェア開発、保守、脆弱性診断、AI モデル開発、ログ分析等では、世界中の専門人材を活用することが実務上必要です。重要なのは、国籍や居住地そのものではなく、特定個人情報ファイル又は本番データに実アクセスできるか、アクセス権限が最小化されているか、監査ログが残るか、契約上の秘密保持・再委託制限・削除義務があるかです。 特定個人情報については、原則として開発・検証・AI 学習・デバッグに本番データを使わないこと、ダミーデータ又は合成データを用いること、必要な場合でも個人番号をマスキング又はトークナイズすること、本番環境へのアクセスを JIT 方式で限定すること、多要素認証、端末制御、画面録画又は操作ログ、アクセスレビューを行うことが重要です。これらの統制がある場合、海外人材の利用を一律に不適切と扱うべきではありません。個人情報保護委員会は、海外在住者又は外国にある委託先の利用が直ちに違法又は不適切となるものではなく、特定個人情報への実アクセスの有無と技術的・組織的措置に基づき判断すべきであることを、Q&A 又はガイドラインで明確化すべきです。 第五に、生成 AI・クラウド・分散処理時代における特定個人情報の取扱いを明確化すべきです。生成 AI、クラウド、分散ログ分析、監視基盤、外部 API 等の利用が進む中で、特定個人情報がプロンプト、ログ、ベクトルデータベース、監視イベント、エラー通知、バックアップ、チケット管理システム等に混入するリスクがあります。本告示及び関連様式では、特定個人情報ファイルそのものだけでなく、派生ログ、エクスポート、バックアップ、分析用データ、AI 入力データ、サポートチケット等に特定個人情報が含まれ得ることを前提に、事故時の調査範囲を整理すべきです。特に、生成 AI サービスへの入力、AI 学習への利用、RAG 用データベースへの格納、外部チケット管理ツールへの貼付け等は、明示的に禁止又は厳格管理すべき場面を例示すべきです。	

	第六に、中小事業者に過剰負担をかけない制度設計が必要です。特定個人情報の保護は重要ですが、報告項目が過度に複雑で、提出先が複数に分散し、同じ内容を何度も入力させる制度では、中小事業者は本来行うべき封じ込め、復旧、本人対応、再発防止に十分なリソースを割けません。初報段階では不確実な情報が多いため、「不明」「調査中」「推定」の入力を許容し、続報・確報で差分更新できる設計とすべきです。共通様式、記載例、業種別テンプレート、API 連携、ワンスオンリー入力、簡易報告モード、チェックリストを整備すべきです。 以上の理由から、本告示改正及び関連する報告手続・共通様式においては、番号利用法第 29 条の 4 の趣旨に即し、1. 特定個人情報漏えい等報告様式の機械可読化、2. 特定個人情報ファイル単位での影響範囲・本人リスク・技術的保護措置の構造化、3. 委託先・再委託先・クラウド・保守事業者の責任分界の明確化、4. 海外エンジニア等の形式的排除ではなく実アクセス有無と監査可能性に基づくリスク管理、5. 生成 AI・クラウド・分散処理における派生データ混入リスクの整理、6. 中小事業者にも実装可能な初報・続報・確報の差分提出と共通テンプレート整備を明記又は推進することを求めます。 以上。 【個人】	
14	一元化は賛成だが、国家サイバー統括室への情報共有について、利用目的・保存期間・アクセス管理・目的外利用禁止を明文化してほしいです。 【匿名】	提出された報告については、個人情報保護委員会又は事業所管大臣、更には共有を受けた場合には国家サイバー統括室においても行政文書として適切に管理します。
15	私は、本改正案に賛成します。	本改正案に賛成の御意見として承

	サイバー攻撃の被害報告は、現場の負担が非常に大きく、特にランサムウェアや不正アクセスのような緊急性の高い事案では、複数の省庁へ個別に報告する必要があり、初動対応を妨げる要因となっていました。 今回の改正案で示されている 共通様式の導入 官民連携基盤による報告窓口の一元化 個人情報保護委員会告示との整合性確保 は、被害組織の負担軽減と迅速な情報共有の両立に寄与するものであり、実務上の改善効果が大きいと考えます。 特に、その他サイバー攻撃等事案共通様式（別添様式 3）の追加は、従来の制度では扱いづらかった不正アクセス・情報窃取などの事案にも対応でき、現場の実態に即した改正だと評価します。 以上の理由から、本改正案の早期施行を支持します。 【個人】	ります。
16	**個人情報の保護に関する法律施行規則等に基づく漏えい等報告方法を定める告示の一部改正案に対する意見書** 個人情報保護委員会事務局 御中	本意見募集は本改正案について意見を求めるものであり、意見１及び意見２は本意見募集の対象外であると考えます。

	標記告示改正案（ランサムウェア事案その他サイバー攻撃等事案における個人情報・特定個人情報の漏えい等報告について、共通様式の追加や官民連携基盤の利用を可能とし、報告負担を軽減するもの）について、減税派・日本人ファーストの立場から是々非々で意見を提出します。 **評価できる点** 被害組織の報告負担軽減と政府対応の迅速化は、無駄な行政コストを抑え、国民負担（税金）の増大を防ぐ観点から賛成です。サイバー攻撃が増加する中、報告の一元化・簡素化は実務上合理的です。 **要望・指摘（特に刑事罰の整備）** しかし、これまで日本国内で繰り返されてきた個人情報・特定個人情報の紛失・漏えい事案（企業・自治体・行政機関による過失を含む）に対し、現行の行政処分や報告義務だけでは抑止力が不十分です。日本人の個人情報を守ることは「日本人ファースト」の基本であり、被害者である国民の権利保護を最優先すべきです。 よって、以下を強く要望します。 1. 個人情報・特定個人情報の漏えい・紛失について、重大な過失や管理不備が認められる場合に、明確な刑事罰（罰金・懲役を含む）を新たに創設・強化すること。報告の簡素化だけを進め、責任追及を曖昧にすることは本末転倒です。 2. 漏えい発生時の報告義務違反や隠蔽に対する罰則も厳格化し、抑止効果を高めること。 3. 官民連携基盤の利用に際しても、データ共有時のセキュリティ基準を厳格に定め、国民の個人情報が二次被害を受けないよう担保すること。 報告負担の軽減は支持しますが、個人情報保護の実効性を高めるための刑事罰整備を並行して進めなけれ	意見３について、官民連携基盤については、今後国家サイバー統括室において適切に運用されるものと考えます。

	ば、国民の信頼は得られません。是々非々の観点から、効率化は認めつつ、日本人の個人情報を守るための罰則強化を最優先で検討してください。 【個人】	
17	サイバー攻撃を受けた組織の報告負担を軽減し、共通様式及び官民連携基盤によって報告窓口を一元化する方向には賛成いたします。 攻撃への初動対応中に複数の官公署へ同様の内容を繰り返し報告することは、被害組織に大きな負担を生じさせ、復旧や被害拡大防止の妨げになる可能性もあります。 一方、共通様式及び官民連携基盤には、個人情報や特定個人情報だけでなく、攻撃経路、IP アドレス、悪用された脆弱性、システム構成、ログ情報及びフォレンジック調査結果等、機密性の高い情報が集約されることになります。 このような情報を集約する基盤は、それ自体がサイバー攻撃の重要な標的となる可能性があります。 そのため、官民連携基盤について、通信時及び保存時の暗号化、アクセス権限の最小化、操作履歴の保存及び監査、情報の分離管理、保存期間、削除基準、再委託先を含む管理体制並びに基盤自体で漏えい等が発生した場合の通知及び公表基準を明確にしていただきたいです。 また、報告内容を国家サイバー統括室その他の機関へ共有する場合には、共有される情報の範囲、共有先、利用目的、保存期間及び第三者への再共有の可否を、報告者が事前に理解できる形で明示する必要があると考えます。 あわせて、一元的な報告を行った場合に、どの官公署に対する、どの法令上の報告義務が、いつ履行された	本改正案に賛成の御意見として承ります。 官民連携基盤については、今後国家サイバー統括室において適切に運用されるものと考えます。 また、提出された報告については、個人情報保護委員会又は事業所管大臣、更には共有を受けた場合には国家サイバー統括室においても行政文書として適切に管理します。

	ものとして扱われるのかを確認できる受領記録を報告者へ交付する仕組みも必要です。 報告負担の軽減だけでなく、集約された機密情報の保護及び法令上の報告義務を確実に履行できる仕組みを併せて整備することを要望いたします。 【匿名】	
18	本改正案に賛成します。 個人情報及び特定個人情報の漏えい等は、被害が確定してからの対応では遅く、特にサイバー攻撃事案では初動の遅れが被害拡大につながります。そのため、報告対象は広めに定め、おそれ段階であっても迅速に報告を求める制度とするべきです。あわせて、報告の要否を事業者の広い裁量に委ねるべきではなく、報告不要と判断できる範囲は限定的に解することを明確にすべきです。さらに、報告様式の記載事項を明確化し、影響範囲、原因、再発防止策等を漏れなく報告させることで、制度の実効性を高めるべきと考えます。 【匿名】	本改正案に賛成の御意見として承ります。頂いた御意見は今後の執務の参考とさせていただきます。
19	質問１　報告情報の利用目的 その他サイバー攻撃等事案共通様式によって取得した情報について、個人情報保護委員会、内閣サイバー統括室その他の行政機関が、それぞれどの情報項目をどの目的で利用することを想定しているのか、情報項目ごとに明示されたい。 質問２　官民連携基盤の管理主体 「官民連携基盤」に提出された情報について、具体的な管理主体はどの行政機関なのか。また、当該情報にアクセスできる行政機関の範囲を明示されたい。 質問３　行政機関間の共有 当該情報を他の行政機関、捜査機関、外国政府機関、民間事業者等に提供する場合には、１提供先、２提供	本改正案は、サイバー攻撃等事案に関する個人情報保護委員会又は事業所管大臣への個人情報の漏えい等報告について、関係省庁申合せ別添様式３を提出する方法及び官民連携基盤を用いる方法によることを可能とするものであり、それ以外の従前の取扱いについて変更するものではありません。 また、官民連携基盤においてどの機関に対して報告を行うかは、報告者が

	する情報項目、3 提供目的、4 法的根拠、5 保存期間、6 提供後の利用制限について明示されたい。 質問 4　警察捜査への利用 共通様式によって取得された情報が、犯罪捜査、犯人の特定、捜索・差押え等の刑事司法目的に利用されることはあるのか。その場合の法的根拠を明示されたい。 質問 5　情報の保存期間 共通様式及び官民連携基盤によって取得された情報について、保存期間、保存期間経過後の削除方法、バックアップを含む複製データの管理方法を明示されたい。 質問 6　個人情報に該当しない技術情報についての扱いについて 共通様式 3 によって報告された情報のうち、個人情報に該当しない技術情報についても、行政機関が保有・分析・共有することになる場合、その利用範囲及び保存期間を明示されたい。 つまり民間企業から取得したサイバーインシデント情報を、国家はどこまで収集し、誰が分析し、誰に提供し、いつまで保有するのか。その法的根拠と利用範囲を明らかにされたい。 【個人】	選択することとされています。 　提出された情報は、個人情報保護委員会又は事業所管大臣、更には共有を受けた場合には国家サイバー統括室においても行政文書として適切に管理します。

※　御意見はとりまとめの都合により整理・要約して掲載しております。

※　上記意見のほか、改正案の内容とは関係がないと考えられる御意見が 11 件ありました。