コメントの概要及びコメントに対する金融庁の考え方

No.	コメントの概要	金融庁の考え方
監督指針全般について		
1	今回の「主要行等向けの総合的な監督指針」等の一部改正では、既往の「障害発生等報告書」に代えて「DDoS 攻撃事案」「ランサムウェア事案」「その他サイバー攻撃等事案」を各共通様式で報告することとされていますが、「障害発生等報告書」で従来報告してきたハードウェアの故障やソフトウェアの不具合による、サイバー攻撃によらないシステム障害を報告できる様式が廃止されているように思われます（「その他サイバー攻撃等事案」の様式では、システム障害の報告に適さない）。 サイバー攻撃によらないシステム障害で監督指針の報告基準に該当するものを報告できるよう、従来の「障害発生等報告書」による報告を認めていただけませんでしょうか。	今回の改正において、DDoS攻撃事案及びランサムウェア事案以外のコンピュータシステムの障害及びサイバーセキュリティの事案の全般的な報告様式として、「その他サイバー攻撃等事案共通様式」を提供しています。これにより、事象の起因等が、明らかになっていない状況であっても、「その他サイバー攻撃等事案共通様式」により報告いただくことが可能です。 なお、「その他サイバー攻撃等事案共通様式」における「等」にはコンピュータシステム障害も含まれるものとして、サイバー攻撃によらないシステム障害についても当該様式により報告いただくことになります。
2	1. 提出の趣旨 改正案による関係省庁申合せに基づく共通様式への移行及び報告プロセスの標準化・効率化に賛同する。その上で、制度の実効性向上及び障害発生時の円滑な対応の観点から、運用面における明確化や支援策の充実を求める。 2. 具体的な改善提案 （1）初動報告（第一報）における様式選択に関する運用の明確化 発生原因が特定できない初動段階における様式選択の取扱いを明確化し、暫定的な様式による報告及び原因判明後の差替え・再提出を認める旨を示すよう求める。 （2）事前の「予告・検知段階」における記載項目の見直し・記載要領の提示	1. いただいた御意見は、今後の金融行政の参考とさせていただきます。 2.（1）について、監督指針等における「直ちに、その事実を当局宛てに報告」とは、基本的に連絡方法や様式等を問わず迅速な報告を求めるものであり、その時点において様式の選択は、必要ありません。 また、その後の様式を用いた報告においても、DDoS 攻撃事案共通様式又はランサムウェア事案共通様式は、その時点で該当する事案であることが明らかな場合に使用を求めるものであり、その他の状況において「その他サイバー攻撃等事案共通様式」を選択いただくことで支障ありません。また、その後の報告において、他の様式を用いるべき事案であることが判明した場合であっても、様式の切り替えを求めるものではありません。このため、差替・再提出は、必要ありません。 なお、「その他サイバー攻撃等事案共通様式」における「等」にはコンピュータシステム障害も含まれるものとして、当該様式により報告いただくことになります。

No.	コメントの概要	金融庁の考え方
	サイバー攻撃の予告又は検知段階での報告について、被害未発生時に記載すべき項目を明確化し、必要最小限の情報による報告を可能とする記載要領等を示すよう求める。 (3)個人データ漏えい報告の兼任手続きに関する Q&A の拡充 共通様式による報告と個人情報保護法上の報告との関係を明確化するため、兼用可能な項目や対応関係に関する Q&A 等の充実を求める。 (4)経過措置期間(令和9年3月末まで)における中小事業者向けガイドの提供 経過措置期間中の円滑な移行を支援するため、中小規模事業者向けに記載例、Q&A及び移行手順等を示したガイドの整備・周知を求める。 3. まとめ 改正案の基本的な方向性を支持した上で、Q&A や記載要領の整備等の運用面での対応により、金融機関の実務負担軽減と監督当局による迅速かつ的確な状況把握の両立を図るよう求める。	2.(2)について、いただいた御意見は、今後の金融行政の参考とさせていただきます。 2.(3)について、関係省庁申合せの改正を踏まえて、「金融機関における個人情報保護に関するQ&A」(以下、「金融分野Q&A」という。)の改正を予定しており、頂いた御意見は、今後の金融行政の参考とさせていただきます。 2.(4)について、いただいた御意見は、今後の金融行政の参考とさせていただきます。共通様式は、従来様式と比較して様式の構成や記載項目の粒度等が異なることから、共通様式への移行及び記載実務における習熟に資するため、「関係省庁申合せ共通様式による障害等発生報告等に関する補足事項」を提供いたします。なお、当該資料には、新旧の項目の対応関係等も含まれます。 3. いただいた御意見は、今後の金融行政の参考とさせていただきます。
3	※環境依存文字により〇に数字や英数字の項番は使用できないため、「数字(〇数字)」や「数字(英数字)」と表記。 ・2(英数字)ー3ー14　監督手法・対応　(1) 障害発生時 (〇1) 「令和 7 年 5 月 28 日関係省庁申合せ」以降も、サイバー攻撃による漏えい発生報告は初動対応時に攻撃種類の判別ができないことも多いことから現行様式である「別紙	1点目について、御認識の通り、個人データ等の漏えい等報告については、引き続き金融分野Q&Aの別紙様式1・別記様式第一を用いて御報告いただくことも可能です。 2点目について、御認識の通りです。 なお、「ランサムウェア事案共通様式」及び「その他サイバー攻撃等事案共通様式」による個人データ等の漏えい等の報告は、コンピュータシステムの障害又はサイバーセキュリティ事案と共に個人データ等の漏えい等が発生した場合に、一つの様式で障害等発生報告等と併せて漏えい等報告を可能とすることで、事業者負担の軽減を図ることを想定したものとなります。

No.	コメントの概要	金融庁の考え方
	様式1・別記様式第一」にて報告しているが、今後も同様の理由で現行様式の「別紙様式1・別記様式第一」の報告も許容されるとの理解でよいか。 ・2（英数字）ー3ー14　監督手法・対応　（1）障害発生時　（〇1）　c. 「その他サイバー攻撃等」の「等」は、後述の（注2）の記述にある報告すべきシステム障害等に合致する事象を指しているとの理解でよいか。その場合、（注2）が様式3に含まれることを明示していただきたい。	個人データ等の漏えい等報告については、関係省庁申合せ改正を踏まえて、改正予定の金融分野Q＆Aをご確認願います。
4	1. 今回の取組は、サイバー攻撃発生時の報告様式を共通化し、被害組織の報告負担を軽減することを目的としたものであり、その趣旨に賛同いたします。 一方で、新設される「その他サイバー攻撃等事案（別添様式3）」については、既存の報告制度との関係が必ずしも明確ではなく、例えば、不正アクセスの試行のみの事案、SOC 等で検知・遮断した事案、API への不正アクセス、個人情報等の漏えいが確認されていない段階での侵害事案等について、報告対象となるかどうか判断に迷うケースがあります。 そこで確認ですが、本申合せは各業法で定める既存の報告基準（例：資金決済法における「障害発生等報告書」等）を変更するものではなく、従来の報告対象事案について共通様式での報告を可能とする趣旨との理解でよいでしょうか。 その上で、別添様式 3 を利用する代表的なケースについて FAQ 等で示していただけると、事業者間で判断が統一され、円滑な制度運用につながるものと考えます。 2. サイバーセキュリティ事案以外のシステム障害についても、「その他サイバー攻撃等事案共通様式」（関係省庁申合せ別添様式 3）を使用する認識で相違ないか。	1. 今回の各監督指針等の改正は、報告要否の基準について、特段の変更は行っておらず、御認識の通り、主に様式の移行に関するものとなります。 2. 及び3.　「その他サイバー攻撃等事案共通様式」における「等」にはコンピュータシステム障害も含まれるものとして、当該様式により報告いただくことになります。 4. 御認識の通りとなります。 5. 金融庁長官等から特定社会基盤事業者として指定された者については、従前の障害等発生報告に加えて、サイバー対処能力強化法のインシデント報告の義務が課されることから、これらを簡便に御報告いただくため、従前の電子申請・届出システムではなく、官民連携基盤を用いていただくこととしております。官民連携基盤のインシデント報告機能においては、共通様式の Excel ファイルをインポートする方法の他ウェブフォームへの入力により報告いただくことも可能ですが、令和8年 10 月1日時点では、個人情報の漏えい等報告は、ウェブフォームではなく、共通様式を添付いただく形で御報告いただくこととなります。 （個別の様式等はございません）

No.	コメントの概要	金融庁の考え方
	上記相違ない場合、様式を見るとサイバーセキュリティ事案を想定した項目が多く、それ以外のシステム障害を記載する場合、関連しない項目も多いと思われるが、その点はどのように考えれば良いか、また記載例などは提供される予定はあるか。 3. 関係省庁申合せ別添様式 3(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)。)は、従来の障害発生等報告書様式にあった、システム障害の発生原因、事後改善策を記載する欄がなく、逆にシステム障害では、「該当なし」と記載せざるを得ないと思われる「4. 事案に関する技術的な事項(攻撃技術情報)」の欄があることから、サイバー攻撃以外の原因によるシステム障害の報告には用いにくいのではないかと思料する。 そのため、サイバー攻撃以外の原因によるシステム障害の報告には、従来の障害発生等報告書を用いたほうが良いのではないか。 4. サイバー攻撃以外の原因によるシステム障害の場合、関係省庁申合せ別添様式 3 の「4. 事案に関する技術的な事項(攻撃技術情報)」等、記載できない部分については「該当なし」と回答すればよいのか。 5. 官民連携基盤での提出では、個人情報漏えい等報告を個人情報保護委員会に対して行う場合における「漏えい等報告のフォーム」のように、Web 上のフォームに入力する形になるのか。 もしその場合、個人情報漏えい等報告同様、フォームに入力前に社内での報告等に用いることができるようにするため、参考様式として Word の報告様式等を展開いただきたい。	なお、金融分野では統一的な事務手続きを行う観点から、当面の間、障害等発生報告について、ウェブフォームは使用せず、あらかじめ共通様式の Excel ファイルに報告内容を記入頂いたうえで、官民連携基盤に当該ファイルをインポートし、添付ファイルとして提出いただくこととしております。 6. いただいた御意見は、今後の金融行政の参考とさせていただきます。また、共通様式は、従来様式と比較して様式の構成や記載項目の粒度等が異なることから、共通様式への移行及び記載実務における習熟に資するため、「関係省庁申合せ共通様式による障害等発生報告等に関する補足事項」を提供させて頂きます。なお、当該資料には、新旧の項目の対応関係等も含まれます。 7. 内閣官房国家サイバー統括室への共有について、当庁では、従前よりコンピュータシステムの障害やサイバーセキュリティ事案のいずれかに関わらず、「重要インフラのサイバーセキュリティに係る行動計画」に沿って対応してきたところとなります(※)。 また、上記に加えて、関係省庁申合せにおいて、「被害報告をおこなう者が共有等を希望しない旨の意思表示をした場合を除き、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。」とあることから、共通様式を用いた報告については、原則として内閣官房国家サイバー統括室への共有対象となります。なお、共通様式において「内閣官房国家サイバー統括室への共有等を希望しない。」欄等が設けられております。 その上で、「直接照会を受けるような場合は想定されるか。」とのご質問について、今回の各監督指針等の対象である障害等発生報告について、現時点において、内閣官房国家サイバー統括室による直接の照会は想定しておりません。 ※サイバーセキュリティ基本法に規定する重要社会基盤事業者(重要インフラ事業者)に関する重要インフラ所管省庁の情報共有に関しては、以下もご参照ください。

No.	コメントの概要	金融庁の考え方
	6. 各様式について、記載例を示していただけないか。 特にサイバー攻撃以外の原因によるシステム障害の場合、関係省庁申合せ別添様式3で記載することになると考えられるので、関係省庁申合せ別添様式3でどのように記載するのが適切か、記載例を示していただけるとありがたい。 7. 今後は、サイバーセキュリティ事案以外についても、「その他サイバー攻撃等事案共通様式」(関係省庁申合せ別添様式 3)を通じて内閣官房国家サイバー統括室へ共有がなされるものとなるのか。 上記相違ない場合、報告した内容について内閣官房国家サイバー統括室より直接照会を受けるような場合は想定されるか。 8. 将来的な報告窓口の一元化についても示されておりますが、資金移動業者では同一インシデントについて金融庁、個人情報保護委員会、警察等へ複数報告が必要となる場合があります。 制度趣旨である報告負担の軽減を実現するため、今後は提出内容・提出方法・提出窓口のさらなる共通化・一元化についても検討をお願いいたします。	「重要インフラのサイバーセキュリティに係る行動計画」(2025 年6月 27 日) https://www.cyber.go.jp/pdf/policy/infra/cip_policy_2025.pdf ・V. 関係主体において取り組むべき事項 ＞2. 重要インフラ所管省庁 ＞ (3)「情報共有体制の強化」に関する事項 (P34) ・別添:情報連絡・情報提供について(P43-P59) 8. 頂いた御意見は、今後の金融行政の参考とさせていただきます。
5	1. 報告制度の共通化について サイバー攻撃等発生時の報告様式を政府共通様式へ移行し、情報共有の迅速化及び金融機関・行政双方の負担軽減を図る方向性に賛同する。一方で、報告制度の整備に加え、予防、早期検知及び被害の局限化といった事前対策を重視するよう求める。	いただいた御意見は、今後の金融行政の参考とさせていただきます。

No.	コメントの概要	金融庁の考え方
	2. AIを悪用したサイバー攻撃への対策 AIの活用によるサイバー攻撃の高度化・高速化・大規模化を前提とし、金融機関に対して脆弱性管理、多要素認証、多層防御、異常検知、復旧訓練等の対策を求めるとともに、防御側においてもAI等の新技術を活用した対応体制の強化を求める。また、高度な攻撃を想定した訓練、脆弱性診断及び侵入テストの実施を重視すべきとする。 3. 外国勢力及びサプライチェーンへの対策 外国政府、外国情報機関、犯罪組織等による攻撃や情報取得のリスクを想定するとともに、クラウドサービス、通信機器、ソフトウェア、保守事業者等の委託先・再委託先を含めたサプライチェーン全体のリスク管理を求める。また、安全保障上の観点から、データ保存場所、国外移転、遠隔アクセス及び実質的支配関係等を踏まえたリスク評価を行うよう求める。 4. 政府に集約される報告情報の保護 報告制度の共通化により行政機関に集約される情報について、新たな攻撃対象となる可能性を踏まえ、アクセス管理、暗号化、保存期間の管理、委託先管理及び国外移転の制限等の情報管理措置を徹底するよう求める。また、情報漏えい発生時の調査、原因究明、責任の所在及び再発防止措置の明確化を求める。 5. 対策不足を放置しないこと 重大な脆弱性の放置や同種事故の反復など、サイバーセキュリティ管理上の問題が認められる金融機関に対しては、原因分析及び改善計画の提出を求めるとともに、必要に応じて監督上の措置を講じるよう求める。また、金融機関で判明した攻撃手法や	

No.	コメントの概要	金融庁の考え方
	脆弱性に関する情報を、機密性に配慮しつつ業界内で迅速に共有する仕組みの強化を求める。 6. 総括 サイバー攻撃発生後の報告体制の整備だけでなく、AIを活用した攻撃、外国勢力による攻撃及びサプライチェーン経由の攻撃等を想定した予防的対策を一体的に強化するよう求める。また、行政機関における情報管理体制の強化を通じて、国民の資産、個人情報及び金融インフラの保護を最優先とした制度運用を求める。	
6	今回の改正案におけるDDoS攻撃事案、ランサムウェア事案及びその他のサイバー攻撃等事案に係る共通様式の導入並びに金融分野横断での報告様式の統一化について賛同する。共通様式により、業態横断的なサイバー攻撃の実態把握や分析が促進され、金融分野全体のサイバーレジリエンス向上につながることを期待する。 その上で、インシデント分析及び監督上の評価に当たっては、攻撃者による侵入やデータの持出しの有無だけでなく、流出した情報が第三者にとって実際に利用可能な状態であったか、暗号化・秘密分散・データの分散管理等の保護措置により被害がどの程度抑制されたかといった観点についても把握・分析するよう求める。 また、共通様式を通じて収集した情報を活用し、攻撃経路、悪用された脆弱性、被害状況及び有効な防御措置等を分析することで、金融分野全体のサイバーセキュリティ対策の高度化につなげるよう求める。 さらに、人的ミスの発生を前提としたセキュリティ対策の重要性を踏まえ、従業員の注意や手作業への過度な依存を低減し、通常業務の中で重要情報が自動的に保護され	いただいた御意見は、今後の金融行政の参考とさせていただきます。

No.	コメントの概要	金融庁の考え方
	る仕組みについて、インシデント分析及び今後の監督上の評価の対象として取り入れることを求める。	
7	1. KPI（成果指標）の設定について 改正案には制度改正の効果を検証するための成果目標や KPI が示されていないとして、重大インシデント把握率、報告までの平均時間、報告内容の不備率、行政による注意喚起発出までの時間、再発防止策の実施率及び新興金融分野における報告遵守率等の指標を設定し、継続的に評価・公表するよう求める。 2. KPI 算出に必要なデータの収集・分析体制について 金融庁、各金融機関、内閣官房及びデジタル庁等が保有するインシデント情報、報告状況及びシステム運用情報等を活用し、関係機関が連携してデータの収集・分析を行うことで、制度の効果を客観的に検証するよう求める。 3. 制度の透明性及び行政手続法との関係について 成果目標、検証方法及び達成期限が示されていない点を踏まえ、制度の透明性及び説明責任を確保する観点から、政策効果の評価方法や目標設定を明確化するよう求める。 4. 関係省庁との連携について サイバー攻撃が金融分野にとどまらず重要インフラ全体に影響することを踏まえ、内閣官房、デジタル庁、総務省及び経済産業省等との連携体制を明確化し、省庁横断的な取組を推進するよう求める。	いただいた御意見は、今後の金融行政の参考とさせていただきます。

No.	コメントの概要	金融庁の考え方
	5. AI・AX・DX の活用について AI を活用したインシデント分析、DX による報告手続の効率化及び横断的なデータ連携等を推進し、デジタル技術を活用した監督・報告体制の高度化を図るよう求める。 6. 情報共有の対象及び連携内容の明確化について どの行政機関と連携し、どのような情報を共有するのかについて監督指針等で明確化するとともに、省庁間の役割分担や情報共有の枠組みを示すよう求める。 7. EBPM の観点からの効果検証について EBPM（証拠に基づく政策立案）の観点から、成果指標、基準値、目標値、達成期限及び予算との関係を設定・公表するとともに、定期的な見直しを実施するよう求める。 8. 海外事例の活用について 米国・欧州におけるサイバーインシデント報告制度や KPI 設定、省庁間連携及び情報共有の取組を参考とし、我が国においても透明性の高い効果検証及び協調体制を整備するよう求める。 9. 総括 金融機関におけるサイバー事故対応の実効性向上のため、KPI による効果検証、関係省庁との連携強化、AI・DX の活用及び情報共有体制の明確化等を通じて、透明性及び客観性の高い制度運用を行うよう求める。	