令和８年９月 18 日

関係省庁申合せ共通様式による障害等発生報告に関する補足事項

金融庁　経済安全保障室

「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 日関係省庁申合せ。以下「関係省庁申合せ」という。）が令和８年９月 15 日に改正され、従前の「ＤＤｏＳ攻撃事案共通様式」（別添様式１）及び「ランサムウェア事案共通様式」（別添様式２）に加え、「その他サイバー攻撃等事案共通様式」（別添様式３）が新たに整備された（以下、これらを総称して「共通様式」という。）。

金融庁では、「主要行等向けの総合的な監督指針」等（以下「監督指針等」という。）において、コンピュータシステム障害又はサイバーセキュリティ事案を認識した場合に監督当局への報告を行う際の様式を示しているところ、関係省庁申合せの改正を踏まえ、従来の障害等発生報告書様式（以下「従来様式」という。）から共通様式へ移行することとした。

監督指針等に記載のとおり、共通様式においても、障害原因、被害状況、対処状況及び事後改善策等の報告を求めることとしており、その取扱いは従来様式と同様である。他方で、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、本資料を作成したものである。

なお、障害等の内容、規模その他の事情に応じて、監督当局より個別に報告内容等について指示を行う場合がある。その場合には、本資料の記載にかかわらず、当該指示に従うこと。

（記載要領）

１．第１報については、障害等の全容が判明する前の断片的なものであっても差し支えないものとする。第２報以降については、第１報後の状況の変化の都度適時にその状況を記載すること。なお、「報告日時」（共通様式前文右上）には、各報告を行った時点での日時を記載すること

２．サービスへの影響や原因等が多岐に亘る場合、又は補足説明資料等がある場合については、本様式にその旨記載した上で、別紙に記載し添付することも可能とする（様式任意）

３．共通様式の「２．（１）」欄には「事案の概要」、「発生場所」、「原因内容等」、「障害分類（コード番号）」、「復旧見込」、「被害状況」、「復旧までの影響」、「復旧までの対応」及び「その他の連絡先等」を記載すること

４．共通様式の「２．（２）」欄には「サービスの概要」、「サービスへの影響」及び「他事業者への影響等」を記載すること

５．共通様式の「３.」欄には「システム名称」及び「システムの概要」を記載すること
６．共通様式の「６.」欄には「事後改善策」を記載すること
７．共通様式の「２．（１）」欄における「発生場所」については、障害が発生しているシステムの設置場所等（市町村名まで）及び店舗等の名称を記載すること
８．共通様式の「２．（１）」欄における「障害分類」については、報告時点において障害分類表で示した原因の中で分類可能なものを記載すること
なお、障害の原因が多岐に亘る場合は、該当し得るものを複数記載することを可とする。また、「災害」を起因とするシステム障害については、通信障害による遠隔地での通信スループット低下等のように被災地以外で発生したものに限り、本様式に記載すること（被災地で発生しているシステム障害は本様式に記載する必要はない）
９．共通様式の「２．（１）」欄における「被害状況」については、被害（顧客への影響等）が確認されている場合には、必要に応じその状況を記載すること
１０．共通様式の「２．（１）」欄における「復旧までの対応」については、応急措置や抜本的対応（代替措置等の状況・方針)、抜本的対応の準備に要する時間等を記載すること
１１．共通様式の「２．（１）」欄における「その他の連絡先等」については、警察、セキュリティ関係機関、他省庁等に対して、既に本障害等を報告している場合に、その内容を記載すること
１２．共通様式の「２．（２）」欄における「他の事業者等への影響等」については、他の事業者等に対して攻撃・障害等が波及する可能性、現況等が確認されている場合には、その内容を記載すること
１３．共通様式の「３.」欄における「システム名称」については、障害が発生しているシステムの名称、又は当該システムが担っている業務名（勘定系、対外接続系等）を記載すること
１４．共通様式の別添様式１又は別添様式２については、第１報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すること。また、その他の状況（コンピュータシステム障害含む）においては別添様式３を使用すること。なお、第２報以降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、様式の切り替えは必要ない
１５．コンピュータシステム障害について報告する場合、共通様式の「４．事案に関する技術的な事項」の記入は必要ない
１６．コンピュータシステム障害やサイバーセキュリティ事案に伴う個人情報等漏えい等事案の場合、共通様式の「報告根拠」欄に報告根拠への記入及び「２．（３）」欄の「別紙１」のチェックを行った上で、「別紙１」を用い、あわせて個人情報等漏えい等報告を行うことが可能である。詳細は、「金融機関における個人情報保護に関するＱ＆Ａ」を確認すること

（障害分類表）

共通様式の「２．（１）」欄における「障害分類」には、下記表のコード番号を記載すること

報告時点において障害原因が不明である場合は、障害分類は空白であっても差し支えない

脅威の類型	コード番号	原因の分類	説明
サイバー攻撃をはじめとする意図的要因	１－１	外部からの不正アクセス、DoS 攻撃	外部からのサイバー攻撃による障害
	１－２	コンピュータウイルスへの感染	コンピュータウイルスへの感染による障害
	１－３	その他の意図的要因	その他の意図的要因による障害
非意図的要因	２－１	ソフトウェア障害	ソフトウェアの不具合等による障害
	２－２	ハードウェア障害	ハードウェア等物理的な不具合等による障害
	２－３	管理面・人的要因	設定ミス、操作ミス、外部委託管理上の問題等による障害
	２－４	その他の非意図的要因	その他の非意図的要因による障害
災害や疾病	3	災害や疾病	災害や疾病による障害
他分野の障害からの波及	４－１	情報通信分野（電気通信）からの波及	利用する電気通信サービスからの波及による障害
	４－２	電力分野からの波及	利用する電力利用からの波及による障害
	４－３	水道分野からの波及	利用する水道供給からの波及による障害
	４－４	上記以外の他分野からの波及	上記以外の他分野からの波及による障害
その他	5	その他	上記の脅威の類型以外の理由による障害

（ 従来様式の記載事項に対応する共通様式での記載箇所 ）

従来様式の各項目の記載事項について、共通様式における対応する記載箇所を下記のとおり示す。なお、参考として、従来様式及び共通様式の項番並びに項目名について、それぞれの様式上の該当箇所を赤枠で示している。(項番及び項目名は、本資料において便宜的に付したものである。)

項番	従来様式-項目名１	従来様式-項目名２	共通様式での記載箇所（項番、項目名等）
(1)	（届出先）	（金融庁長官等）	②（報告先機関の長）　※複数ある場合、すべてを記載
(2)	（報告者）	金融機関名	1. ⑬報告者の名称
(3)		代表者名	1. ⑰代表者の氏名
(4)	（担当者情報）	所属	1. ⑲事務連絡者-所属部署
(5)		氏名	1. ⑱事務連絡者-氏名
(6)		電話番号	1. ⑳事務連絡者-電話番号
(7)		E-mail	1. ㉑事務連絡者-E-mail
(8)	（前文等）	（報告根拠）	③にチェック、④報告根拠内に記載　※複数ある場合、すべてを記載
(9)		第〇報	⑦報告の版
(10)		連絡日時（年月日時分）	①報告年月日／報告時分
(11)	障害発生の日時・場所	発生日時	2.(1) ㉒発生日時
(12)		発生場所	2.(1) ㉔内に「**発生場所**」として記載
(13)	障害の発生したサービス	サービスの概要	2.(2) ㉗内に「**サービスの概要**」として記載
(14)		サービスへの影響	2.(2) ㉗内に「**サービスへの影響**」として記載 ※時系列の事実経過は、2.(3)又は 2.(4)の㉛に記載
(15)	障害原因	障害分類	2.(1) ㉔内に「**障害分類**」として記載
(16)		原因内容等	2.(1) ㉔内に「**原因内容等**」として記載
(17)	対象システム	システム名称	3.㉜ 内に「**システム名称**」として記載
(18)		システムの概要	3.㉜ 内に「**システムの概要**」として記載
(19)	被害状況等	復旧見込	2.㉔ 内に「**復旧見込**」として記載
(20)		被害状況	2.㉔ 内に「**被害状況**」として記載 ※時系列の事実経過は、2.(3)又は 2.(4)の㉛に記載 ※技術的な事項は、4.㉝に記載
(21)		復旧までの影響	2.(1) ㉔ 内に「**復旧までの影響**」として記載
(22)	他の事業者への影響等		2.(2) ㉗ 内に「**他の事業者への影響等**」として記載
(23)	対処状況	復旧までの対応	2.(1) ㉔内に「**復旧までの対応**」として記載
(24)		対外説明	5.(1) 公表の実施状況（㉞、㉟）に記載
(25)		その他の連絡先等	2.(1) ㉔内に「**その他の連絡先等**」として記載
(26)	事後改善策		6.㊳ 内に「**事後改善策**」として記載

【参考１】従来様式における項番及び項目名の該当箇所　（様式４－４６使用）

コンピュータシステムに障害等が発生した場合
様式４－４６

金融庁長官　○○○○　殿
（１）

金融機関名　（２）
代　表　者　（３）

担当者情報
所属　（４）
氏名　（５）
電話番号　（６）
E-mail　（７）

（８）
今般、以下のように障害等が発生したので、　（文書番号）　に基づき報告します。

障害発生等報告書

（第（９）報）　（10）（連絡日時：　年　月　日　時　分）

項目		内容
障害の発生日時・場所	発生日時	（11）年　月　日　時　分頃
	発生場所	（12）
障障害の発生したサービス	サービスの概要	（13）
	サービスへの影響	（14）
障害原因	障害分類	（15）
	原因内容等	□ 未確認　□ 確認済 （16） 内容（　）
対象システム	システム名称	（17）
	システムの概要	（18）
被害状況等	復旧見込	□ 復旧済み　（　日　時頃） □ 復旧見込み　（　日　時頃） □ 不明 （19）
	被害状況	（20）
	復旧までの影響	（21）
他の事業者等への影響等		（22）
対処状況	復旧までの対応	（23）
	対外説明	（24）
	その他の連絡先等	（25）
事後改善策		（26）

【参考２】共通様式における項番及び項目名の該当箇所　（別添様式３使用）

（別添様式３）その他サイバー攻撃等事案共通様式

その他サイバー攻撃等事案共通様式

①　年　月　日
　　時　分

②（報告先機関の長）殿

以下の報告根拠に基づき、別添のとおり報告いたします。

報告根拠：

③ □法令等に基づく報告（「本様式の対象となる手続等」から該当手続名を記載すること。）

④

⑤ □上記選択肢以外（自主判断による情報提供を目的とした任意報告等）

※任意報告の同報先がある場合は、以下に同報先機関を記載すること。

⑥

【報告の区分】

（１）報告の版：第　⑦　報

（２）速報/続報/詳報の別：

⑧ □速報(新規)　□続報　□詳報(確報)

⑨（前回報告：　年　月　日　時　分）

⑩（受付番号※：　）

※個人情報保護委員会より通知されている場合

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。

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。

⑪ □　内閣官房国家サイバー統括室への共有等を希望しない。

共有等を希望しない内容：

⑫

（注）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条に基づく報告である場合は、「共有等を希望しない」とした場合でも、内閣府（及び所管省庁）への報告として取り扱われます。

（注）報告を行う者が、重要インフラのサイバーセキュリティに係る行動計画（2022年６月17日サイバーセキュリティ戦略本部決定）に定める重要インフラ事業者等である場合は、同行動計画に基づき、「共有等を希望しない」とした場合でも、別紙１から別紙３までの内容を除き、内閣官房国家サイバー統括室に共有されることがあります。

１．記載の手引き

（１）本様式の対象となる手続等

報告根拠に記載する法令、ガイドライン等（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おいて重要インフラ分野として指定されている分野の法令、ガイドライン等を含む）については、次のウェブサイトに記載。ただし、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。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。このほか、警察への相談を行う場合や、その他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る。

https://www.cyber.go.jp/policy/group/cyber/policy.html

（２）記載事項

①共通

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。また、続報として提出する場合には、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。

（1／4）

１．報告者の概要

報告者の氏名 又は名称	（フリガナ） ⑬ （氏名は旧姓での記載を可とする）
法人番号（13桁）	⑭
業種・業種番号	⑮
報告者の住所 又は居所	〒 － ⑯
代表者の氏名 （報告者が法人等の場合に限る。）	（フリガナ） ⑰ （氏名は旧姓での記載を可とする）
事務連絡者の氏名	（フリガナ） ⑱ （氏名は旧姓での記載を可とする） 所属部署 ⑲　電話番号 ⑳ E-mail ㉑

２．事案の概要（業務への影響）

（１）事案の概要

㉒ 発生日時：　　年　　月　　日　　時　　分
㉓ 発覚日時：　　年　　月　　日　　時　　分

㉔

事案の概要：

発生場所：

原因内容等：

障害分類（コード番号）：

復旧見込：

被害状況：

復旧までの影響：

復旧までの対応：

その他の連絡先等：

（２）重要インフラサービス維持レベルについて（重要インフラのサイバーセキュリティに係る行動計画（2022年６月17日サイバーセキュリティ戦略本部決定）に定める重要インフラ事業者等に該当する場合に記載すること。該当しない場合は記載を要さない。）

・重要インフラサービスのサービス維持レベルの逸脱の有無：　㉕ □ 有　□ 無
・他の事業者等への波及の可能性：　㉖ □ 有　□ 無

㉗

サービスの概要：

サービスへの影響：

他事業者への影響等：

（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。個人情報の保護に関する法律及び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に基づく漏えい等報告を同時に行う場合は、両方チェックし、それぞれの様式に記載すること。）

㉘□ 別紙１（個人情報取扱事業者における個人データ等の漏えい等報告）【民間事業者・個人情報の保護に関する法律第58条第１項各号に掲げる法人等（いわゆる規律移行法人）の方】

㉙□ 別紙２（行政機関等における保有個人情報の漏えい等報告）【行政機関等の方】

㉚□ 別紙３（特定個人情報の漏えい等報告）【民間事業者・行政機関等共通】

（４）事実経過（時系列）

㉛

３．影響のあるシステム（強化法第５条による報告の場合、特定侵害事象等が発生した特定重要電子計算機について記載）

㉜

システム名称：

システムの概要：

４．事案に関する技術的な事項（攻撃技術情報）

㉝**（※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。）**

（１）攻撃の手口・侵入経路・攻撃の時系列

※システム構成が分かる図やフォレンジック結果報告書を提出する場合は別ファイルとしてください。

（２）サイバー攻撃等の類型

（３）サイバー攻撃等の特徴（インディケータ情報）

※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御提出ください。

（４）悪用された脆弱性

・製品開発者への報告の有無：□ 有 □ 無

５．事案への対応に関する事項

（１）公表の実施状況

㉞ 事案の公表：
- ☐ 実施済　【公表日：　年　月　日】
  公表URL：
- ☐ 実施予定　【公表予定日：　年　月　日】
- ☐ 検討中
- ☐ 予定無し

㉟ 公表の方法：
- ☐ ホームページに掲載
- ☐ 記者会見
- ☐ 報道機関等への資料配付
- ☐ その他：（　）

公表文：

（２）今後の予定

㊱
- ☐ 事象継続中
- ☐ 対応策を継続中
- ☐ 対応完了

（３）外部機関による調査の実施状況

㊲
- ☐ 実施済又は実施中
- ☐ 実施予定
- ☐ 検討中
- ☐ 予定なし

（詳細：　）

６．その他（特記事項等）

㊳

事後改善策：

【参考３】共通様式における項番及び項目名の一覧

項番	項目名１	項目名２	入力方式	備考欄
①	（前文等）	報告年月日／報告時分		
②		（報告先機関の長）		
③	（報告根拠等）	法令に基づく報告（か否か）	[チェック]	
④		該当手続き名等	[自由記述欄]	
⑤		上記選択肢以外-任意報告（か否か）	[チェック]	
⑥		任意報告の同報先機関	[自由記述欄]	
⑦	（報告の区分等）	第〇報		
⑧		速報/続報/詳報の別		
⑨		前回報告日時（年月日時分）		
⑩		受付番号		
⑪	（情報共有）	NCO への共有等を希望しない	[チェック]	
⑫		NCO への共有等を希望しない内容	[自由記述欄]	
⑬	１．報告者の概要	報告者の名称又は氏名		
⑭		法人番号（13 桁）		
⑮		業種・業種番号		
⑯		報告者の住所又は居所		
⑰		代表者の氏名		
⑱		事務連絡者の氏名		
⑲		所属部署		
⑳		電話番号		
㉑		E-mail		
㉒	２．事案の概況（業務への影響）	発生日時		
㉓		発覚日時		
㉔		（１）事案の概要	[自由記述欄]	
		「事案の概要」	**[上記欄内記述]**	
		「発生場所」	**[上記欄内記述]**	
		「原因内容等」	**[上記欄内記述]**	
		「障害分類（コード番号）」	**[上記欄内記述]**	
		「復旧見込」	**[上記欄内記述]**	
		「被害状況」	**[上記欄内記述]**	
		「復旧までの影響」	**[上記欄内記述]**	
		「復旧までの対応」	**[上記欄内記述]**	
		「その他の連絡先等」	**[上記欄内記述]**	

項番	項目名１	項目名２	入力方式	備考欄
		（２）重要インフラサービス維持レベルについて		
㉕		重要インフラサービスのサービス維持レベルの逸脱の有無	[チェック]	
㉖		他の事業者等への波及の可能性	[チェック]	
㉗		（その内容） **「サービスの概要」** **「サービスへの影響」** **「他事業者への影響等」**	[自由記述欄] **[上記欄内記述]** **[上記欄内記述]** **[上記欄内記述]**	
		（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		※様式２及び様式３のみ
㉘		別紙１	[チェック]	※様式２及び様式３のみ
㉙		別紙２	[チェック]	※様式２及び様式３のみ
㉚		別紙３	[チェック]	※様式２及び様式３のみ
㉛		（４）事実経過（時系列）	[自由記述欄]	※様式１では（３）
㉜	３．影響のあるシステム	（その内容）	[自由記述欄]	
		「システム名称」 **「システムの概要」**	**[上記欄内記述]** **[上記欄内記述]**	
㉝	４．事案に関する技術的な事項（攻撃技術情報）	（１）観測期間		※様式１の場合のみ
		（２）攻撃類型－①分類（複数選択）		※様式１の場合のみ
		②詳細	[自由記述欄]	※様式１の場合のみ
		（３）通信プロトコル	[自由記述欄]	※様式１の場合のみ
		（４）送信元情報	[自由記述欄]	※様式１の場合のみ
		（５）送信先情報	[自由記述欄]	※様式１の場合のみ
		（６）通信量	[自由記述欄]	※様式１の場合のみ
		（１）ランサムノート（身代金を要求する文言等）		※様式２の場合のみ
		（２）暗号化されたファイルの拡張子		※様式２の場合のみ
		（３）ランサムウェアの類型		※様式２の場合のみ

項番	項目名１	項目名２	入力方式	備考欄
		（４）攻撃の手口・侵入経路・攻撃の時系列		※様式２の場合のみ
		（５）ランサムウェアの特徴（インディケータ情報）		※様式２の場合のみ
		（６）悪用された脆弱性		※様式２の場合のみ
		（１）攻撃の手口・侵入経路・攻撃の時系列	[自由記述欄]	※様式３の場合のみ
		（２）サイバー攻撃の類型	[自由記述欄]	※様式３の場合のみ
		（３）サイバー攻撃の特徴（インディケータ情報）	[自由記述欄]	※様式３の場合のみ
		（４）悪用された脆弱性	[自由記述欄]	※様式３の場合のみ
		・製品開発者への報告有無	[チェック]	※様式３の場合のみ
	５．事案への対応に関する事項	（１）公表の実施状況		
㉞		事案の公表（実施状況、公表日、公表予定日等）	[チェック]等	
㉟		公表の方法（公表先、公表文）	[チェック]、[自由記述欄]	
㊱		（２）今後の予定（事象継続中、対応策を継続中、対応完了[チェック]）	[チェック]	
㊲		（３）外部機関による調査の実施状況（実施済、実施中、予定無し等、詳細	[チェック]、[自由記述欄]	
㊳	６．その他特記事項	（その内容） **「事後改善策」**	[自由記述欄] **[上記欄内記述]**	
―	別紙１（個人情報取扱事業者）	別紙１（個人情報取扱事業者における個人データ等の漏えい等報告）【民間事業者・個人情報の保護に関する法律第 58 条第１項各号に掲げる法人等（いわゆる規律移行法人）の方】		※様式２及び様式３のみ
―	別紙２（行政機関等）	別紙２（行政機関等における保有個人情報の漏えい等報告）【行政機関等の方】		※様式２及び様式３のみ
―	別紙３（特定個人情報）	別紙３（特定個人情報の漏えい等報告）【民間事業者・行政機関等共通】		※様式２及び様式３のみ