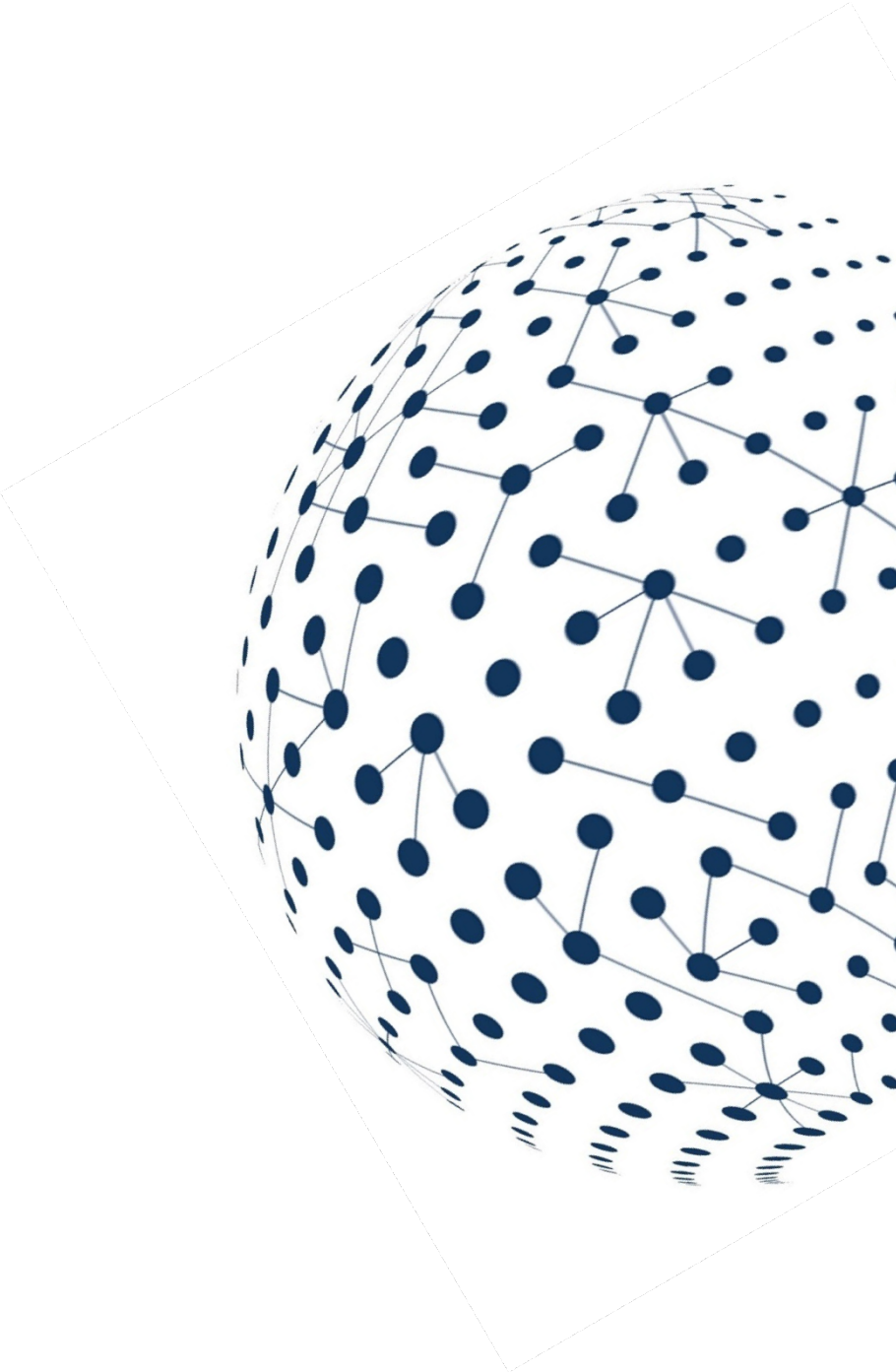
インシデント報告交換（FIRE）のフォーマット

最終報告

2025 年 4 月 15 日



金融安定理事会（FSB）は、効果的な規制・監督・その他の金融セクター政策の策定と実施を促進するため、各国金融当局と国際標準設定団体の作業を国際レベルで調整する。FSB のマンデートは FSB 憲章に定められており、FSB の政策立案と関連活動をガバナンスしている。これらの活動は、その中で下された決定を含め、拘束力を持つものではなく、いかなる法的権利や義務も生じさせないものとする。

金融安定理事会に連絡する

E メールアラートに登録する www.fsb.org/emailalert

X/Twitter で FSB をフォローする：FSB に E メールを送る：

著作権 © 2025 金融安定理事会.諸条件を参照のこと

目次

エグゼクティブサマリー **5**
序文 **6**
FIRE の範囲 7
FIRE の開発 8
本文書の構成 8
実施のためのガイダンス 9
構造化データモデル 9
FIRE レポートの基本要素 11
金融機関主導の報告 12
1. 報告内容 **14**
1.1. 報告事業体 **14**
事業体タイプ 15
事業体の国名 16
1.2. 受入事業体 **16**
例 16
1.3. 連絡先 **18**
2. インシデントの詳細 **20**
2.1. 参考文献 **20**
2.2. インシデント **21**
フェーズとインシデントの状況を報告する。 21
インシデントのタイトルと説明 24
インシデント・タイプ 25
インシデント痕跡 26
インシデント発見手法 26
インシデント報告トリガー 26
解決までの推定期間 28
2.3. 前回報告書からの変更点 **28**
2.4.日付／時刻マーカー **30**
3. 影響アセスメント **32**
3.1. 重大度評価 **32**
3.2. 影響を受ける当事者 **33**
3.3. サービスとリソース **35**
サービス 35
顧客／消費者ベース 37
影響を受ける取引 37
リソース 38

3.4. 影響 **39**
地理的な広がり 40
4. インシデントのクローズ **42**
4.1. 原因 **42**
4.2. レッスン **44**
4.3. 補足文書 **45**
附属書 A：標準化されたフィールドタイプ **47**
附属書 B：機関主導の報告における報告段階の選択性 **48**
附属書 C：インシデントの種類 **52**
附属書 D：インシデント発見の方法 **53**
附属書 E：標準化された重症度 **54**
附属書 F：サービス中断の種類 **54**
附属書 G：ISO 20022 事業分野 **56**
附属書 H：資源の種類 **57**
附属書 I：資源特性 **58**
附属書 J：財務的影響尺度 **59**
附属書 K：事業影響尺度 **60**
附属書 L：風評影響尺度 **60**
附属書 M：外部影響尺度 **62**
附属書 N：原因の種類 **63**
附属書 O：発生源 **66**

エグゼクティブサマリー

2017 年以降、金融安定理事会（FSB）は、金融システムの安定性に対するサイバーインシデントの脅威を強調してきた。効果的なインシデント対応と復旧は、金融安定リスクを緩和する上で極めて重要である。FSB は、そのようなショックを悪化させる可能性のある弱点を特定し、対処するために取り組んでいる。

インシデント報告は、金融当局が規制事業体内の混乱を監視するための重要な金融機関である。国・地域によって報告アプローチが異なるため、要件が分断され、連携に課題がある。規制当局による報告のより一層の調和は、企業の効率的なインシデント対応と回復を支援し、効果的な監督と回復機関間の協力を促進する。FIRE（Format for Incident Reporting Exchange）は、インシデント報告のための共通の情報要素を促進する一方で、柔軟な実施方法を可能にすることを目的としている。認可当局は、FIRE を採用する範囲を選択し、その特徴や定義を活用することで、コンバージェンスを促進し、既存の枠組み間の翻訳を容易にすることができる。

FIRE は、サイバーインシデントを含むオペレーショナルインシデントをカバーするよう設計されており、FSB のサイバーレジリエンスに関するこれまでの作業を超えるものである。FIRE は、インシデントを報告するための一連の共通情報項目を提供するが、共通の報告トリガー、期限、緩和アプローチについては定義していない。金融セクター参加者の認可当局への報告に焦点を当てた設計となっており、規制対象事業体がサービス・プロバイダとの関係において FIRE を活用できるよう柔軟性を持たせている。FIRE の特徴は、この書式の全部または一部を採用する認可当局の柔軟性を支えている。定義された 87 の情報項目のうち、39 項目は任意であり、当局はニーズに応じてどの項目を導入するかを決めることができる。認可当局は、運用上の課題を複雑にしないよう配慮しつつ、報告フェーズのベースラインビューをカスタマイズすることができる。非構造化フィールドの追加仕様を提供することもできる。さらに、フィールド名と許容入力は、概念的な同等性を維持しつつ、現地の言語ニーズをサポートするように調整することができる。FIRE との完全な整合を選択する事業体は、必須情報項目をすべて含み、基本的な任意性 要件を満たし、互換性のあるフィールド型を使用し、列挙リストを遵守すべきである。部分的な実装であっても、一貫性と相互運用性の利点はある。

FIRE のグローバルな採用を促進するため、FSB はデータ・ポイント・モデル（DPM）方式を用いたデータ・モデルも公表しており、これにより eXtensible Business Reporting Language（XBRL）などの機械可読バージョンの FIRE が可能となる。機械読み取り可能なフォーマットは、インシデント報告の効率性、正確性、透明性を高め、金融認可当局が事業体や法域を超えて一貫して定義されたデータを収集し、リスクの分析とモニタリングをサポートすることを可能にする。DPM はまた、異なるシステムやソフトウェア間の相互運用性と柔軟性を促進し、シームレスなデータ交換を可能にする。FSB は、FIRE が最終化された 2 年後（例えば 2027 年）に、産業界や当局とワークショップを開催し、導入上の課題を含め、FIRE の経験を把握する。

序文

2017 年以降、FSB は金融システムの安定性に対するサイバーインシデントの脅威を強調し、そのようなショックを悪化させる可能性のある弱点や非効率性を特定し、対処し始めた。インシデントへの効率的かつ効果的な対応とインシデントからの回復は、関連する金融安定リスクを抑制するために不可欠である。規制報告のより一層の調和は、金融機関の効果的な監督を支え、こうしたリスクの監視と対処における当局間の協力と協調を促進する。

インシデント報告は、金融当局がその規制対象事業体で発生した混乱を可視化し、個々の必須要件に沿って維持するために使用する主要な金融機関のひとつと考えられている。しかし、インシデント報告へのアプローチは時代とともに独自に発展してきたため、報告要件が断片化し、当局間や管轄区域間の調整が困難になっている。

FIRE は、民間セクターの参加者との協議により開発された。このプロセスには、インシデント報告ニーズの共通点を特定するための発見段階と、FIRE の構成要素を開発するための設計段階が含まれた。さまざまなインシデントタイプやシナリオを用いて、FIRE の設計と堅牢性を確認するためのテスト段階が実施された。2027 年にワークショップを開催し、これまでの経験を検討し、改訂の必要性を判断する予定である。

FIRE は、インシデント報告のための共通の情報要素と要件を推進するアプローチであり、同時に、様々な実施慣行に柔軟に対応するものである。FIRE は、FSB の報告書[1] に基づき、各認可当局の情報要件や、企業のインシデント報告における最も顕著な実務上の問題に対処することを目的としている。FIRE は企業に直接的な要件を課すものではなく、FSB がインシデント報告を収集することもない。むしろ、FIRE が利用可能となるためには、個々の当局による導入、または当局が FIRE に沿った報告を受け入れることを示すことが必要となる。認可当局は、個々の状況に応じて、FIRE をどの程度採用するか決定することができる。例えば、認可当局は FIRE の特徴や定義のサブセットを活用することで、限定的なコンバージェンスを促進することができる。単一の法域で採用されなかったとしても、FIRE は、金融金融機関が様々な報告要件に照らし合わせ、既存の枠組み間の変換を支援するための共通フォーマットとして機能する可能性がある。

FSB のサイバーインシデント報告に関する作業において、[2] 3 つの異なる報告タイプが特定され、それぞれの情報要件がこのフォーマットに反映されている：

- **金融機関主導**の報告、インシデントが 1 つまたは複数の金融当局の報告規準を満たした場合、または自発的に報告された場合に発生す報告で、エンド・ツー・エンドのインシデント・ライフサイクルに関連する初期報告、中間報告、最終報告が含まれる
- **規制当局主導**の報告、インシデント情報は、セクター全体のインシデントの影響をよりよく理解するために、1 つ以上の規制当局から要請を受けて報告される。
- **定期的**な報告、規制対象機関から**定期的に**収集したインシデント関連情報を報告する（イベントドリブンではない）。

金融機関主導の報告が最も一般的であり、金融機関にとって業務上の最大の課題であることから、FIRE の設計では、金融機関主導の報告に共通する情報項目を定義することに重点を置いている。

FIRE の設計は、インシデントを報告するための一連の共通情報項目に限定されている。共通の報告トリガー、報告期限、緩和アプローチ、あるいはサイバーインシデント対応と復旧の他の側面を定義するものではない。

人間が読める」フォーマットの設計に加え、言語にとらわれない DPM[3] メソッドを用いて、柔軟性と相互運用性を最大化する FIRE のデータモデルが開発された。このデータモデルにより、本パッケージの一部を構成する XBRL を使用してエンコードされた FIRE のような、機械可読バージョンの FIRE を誰でも作成できるようになった。FIRE は、認可当局に対し

---

[1]FSB (2023a)、インシデント報告交換フォーマット（*FIRE*）：*A possible way forward*, April.

[2]FSB (2023b)、サイバーインシデント報告におけるより大きな収束を達成するための提言、4 月

[3]ISO 511 6 詳細は国際標準化金融機関（ISO）の ISO/TC 68「DPM とは」を参照のこと。

て、事前に開発された XBRL 分類法を活用する（xBRL-CSV の提出を義務付けるなど）か、別の報告言語でインシデント報告を FIRE するか、いずれかの柔軟性を提供する。

FIRE の範囲

FIRE の設計は、主に金融機関から金融当局へのオペレーショナルインシデント（サイバーインシデントを含む）の報告を対象としている。[4]これまでの FSB のストックテイクでは、多くの認可当局はサイバーインシデントに特化した別のアプローチや報告金融機関を有していないことが確認されている。むしろ、多くの枠組みは、サイバーインシデント報告をより広範なオペレーショナルインシデント報告の一部として扱っている。そのため、FIRE の対象範囲は、FSB のサイバーレジリエンスに関するこれまでの作業の範囲を超えている。

FIRE の範囲内でインシデントの種類と根本的な原因の境界を確立するため、FSB サイバー用語集にある同等のサイバー用語を補完する 3 つの追加用語と関連する定義を**表 1 に示す**。[5]

表 1：追加用語と関連する定義

用語	定義
オペレーション	1 つまたは複数の活動、機能またはサービスを提供するために使用される人、プロセス、情報、情報システム、施設、または外部依存関係に関するもの。 出典 BCBS およびジョイント・フォーラムより引用
オペレーション・イベント	オペレーション・ドメイン内で、特定の状況の観察可能な発生または変化。運用上の事象は、運用上のインシデントが発生していることを示すことがある。 出典 ISO と NIST（「イベント」の定義）から引用した。
オペレーション・インシデント	事業体に悪影響を及ぼすと判断された業務上の事象で、対応と復旧の必要性を促す。 出典 NIST CSF（「サイバーセキュリティインシデント」の定義）から引用した。

これらの用語の関係を**図 1 に**示す。この図では、これらの用語を「報告すべき業務上の事故」という概念に相互に関連付けている。この「報告すべき業務上の事故」は、個々の報告義務を引き起こす業務上の事故のさまざまなサブセットを表している。

非金融機関による詳細な報告は、FIRE の設計の主要な範囲には含まれないが、個々の法域の非金融機関や認可当局が利用できるよう、設計には十分な柔軟性がある。

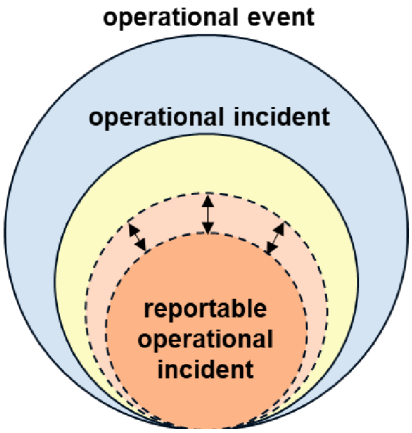
[4]本段落で概説した中核概念間の関係のより詳細な説明については、FSB (2023c), *Cyber Lexicon の 2023 年更新*附属書 B を参照のこと：、4 月）を参照のこと。

[5]FSB（2023c）

金融機関はまた、当局の導入決定とは無関係に、第三者のサービスプロバイダーとの関係で FIRE を活用することを選択することもできる。金融機関は、（一連の）サービスプロバイダーとの間で、サービスプロバイダーが、合意されたサービスやその他の義務を提供する能力に影響を与えるオペレーション上のインシデント を金融機関に報告するために FIRE を利用することに合意することができる。[6]。

出典 ISO/TC

図 1：オペレーション用語



FIRE の開発

FIRE の開発は、いくつかの段階を経て、官民の参加者が 1 年半にわたって協力しながら進められた。

FSB メンバー当局および産業界から代表者を集め、リソースを特定するための初期段階を経て、ワーキンググループは、ステークホルダーからのフィードバックに基づいてインシデント報告のニーズを特定し、FIRE の前提条件と実現可能性を決定するための発見段階を開始した。個々の情報項目に対する支持の度合いを判断するため、情報収集演習が実施され、これらの項目に関するコンセンサスを形成し、プロジェクト実施のための推定労力と複雑さをより明確に把握した。

ワーキンググループの目的を達成するのに十分なコンセンサスと実現可能性が示されたため、プロジェクトは FIRE コンセプトの構成要素を開発する設計フェーズに入った。設計の労力は 2 つに分けられた。80%以上の情報項目は、ほとんどあるいは中間の設計労力を必要としないと見積もられ（総称して「労力の少ない」情報項目）、残りの情報項目は「多大な労力」を必要とすると考えられた。前者は即座に設計段階に移され、一方、多大な労力を要する情報項目の設計には、設計要件についての相互理解を深めるために、規制当局と業界参加者の間で複数回にわたるバーチャル・ワークショップが行われた。

FIRE の設計作業と並行して、いくつかの既存および将来的な国内または地域のインシデント報告の枠組みとの比較作業が行われ、FIRE の設計にさらなる情報項目を盛り込んだり、調整したりする必要性がある可能性を特定した。

本文書の構成

FIRE のフォーマットは、本文書では以下の構造で記述されている：

- 金融機関主導する報告書の書式を詳述したセクション：
  - 共通の目的を持つ情報項目ごとにグループ化された複数のサブセクション（金融機関が主導する報告については**図 4 に**示すとおり）。
  - 各情報項目、その目的、構文、規則または制約、および少なくとも 1 つの例を説明するテキストを添付した表。
  - 各情報項目の色分けは、その項目が**必須**（赤みがかったオレンジ）であり、ローカルな実装に含まれるべきものであるか、またはオプション（薄い黄色）であり、含めるかどうかが任意であることを示す。
- 附属書には、報告段階ごとのオプションの詳細（**附属書 B**）と、特定の情報項目に関する参照表（**附属書 C～O**）が含まれている。

[6]FSB (2023d), *Final Report on Enhancing Third-party Risk Management and Oversight - A Toolkit for Financial Institutions and Financial Authorities*, December, Section 3.3.

実施のためのガイダンス

FIRE の設計には、整合性のある結果を達成しつつも、当局の柔軟性をサポートするためのいくつかの機能が含まれている：

- **情報項目**：FIRE に定義された 87 の情報項目のうち、39 項目はどの報告段階においても「必須」とマークされていないため、認可当局は、特定の状況に基づいて、これらの追加情報項目のうちどれ（もしあれば）を実施するかを決定することができる。
- **報告段階**：FIRE は、各報告段階に対する個々の情報項目の報告に関する基本的な見解を定義している。ある情報項目が報告フェーズにおいて「任意」とされている場合、認可当局は、報告ニーズに沿ってそれを「必須」とすることを決定することができる。ただし、FSB の「サイバーインシデント報告に関する勧告」に従い、インシデント発生当初に報告事業 体がすでに直面している運用上の課題を複雑化させないよう注意する必要がある[7]。
- **言語のカスタマイズ**：認可当局は、情報項目の名称と定義、および関連するタクソノミを、管轄区域内の現地の言語 ニーズまたは既存の用語をサポートするように調整することができる。ただし、規制当局が国際獣疫事務 所との整合性を維持することを望む場合、調整された内容は、本文書の内容との概念上の等価性を保たなければならない。
- **非構造化フィールドに関する補足指針**：FIRE フォーマット内のいくつかの情報項目は、フィールドの長さ以外に使用上の制約がない、短い または長いテキストフィールドを使用している。規制当局は、これらの情報項目を通じて受け取ることを望む記述情報の性質に関する補足ガイダンスを含めることができる。

FIRE の設計は、より大きな収斂と柔軟な成果を達成するために、利用可能な選択肢の下限と上限の範囲内で柔軟性を提供している。とはいえ、FIRE と完全に整合することを選択する事業体は、以下を行うべきである：

- すべての必須情報項目を含む
- すべての報告フェーズにおいて、ベースラインの任意性要件を満たす（または上回る）インシデント報告書を生成および／または収集する
- 同じまたは互換性のあるフィールドタイプを使用して、FIRE 内で情報項目を実装する
- FIRE 内で定義されている列挙リスト（またはそのサブセット）を使用する。
- FIRE の設計に含まれていない追加的な情報項目は、地域の特殊性をもたらし、報告事業 体が直面する課題を悪化させるため、含めない。

これらのアライメント前提条件のサブセットのみを順守する実装は、他の FIRE アライ メント・ソリューションとの一貫性と相互運用性はある程度達成できるかもしれないが、コンバージェ ンスのメリットを完全に享受することはできない。

FIRE 報告書に含まれうる情報の機密性（重要インフラの詳細、IP アドレス、重要脆弱性など）を考慮すると、当局は、金融機関や他の当局から受領する他の機密情報と同レベルの保護をもって、報告書が処理、保管され、（該当する場合には）転送されることを保証すべきである。当局が受け取った情報を、その機密性を保護するための適切な措置で保護することを金融機関に保証することは、この点に関する金融機関の懸念を軽減するのに役立つであろう。

構造化データモデル

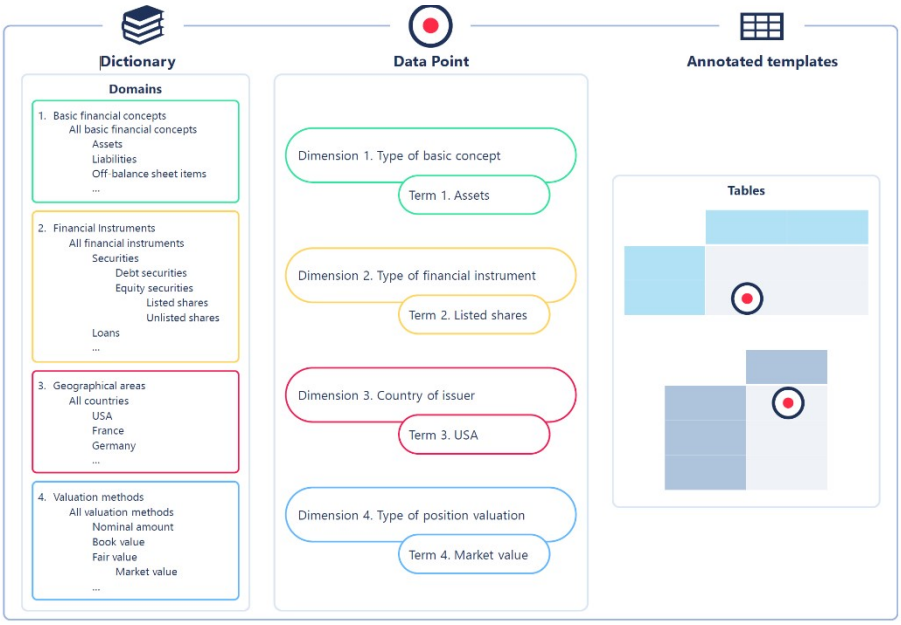
FIRE は、インシデント報告を合理化するために設計された標準化された報告フォーマットである。導入を促進するため、FSB はテクニカル・アネックスを通じて、DPM 1.0 における FIRE フォーマットの構造化された表現をプロバイダとして提

[7]FSB (2023b), 勧告 4.

供している。この附属書には、DPM モデルに基づく XBRL のタクソノミーのサンプルも含まれており、FIRE に沿った機械可読のインシデント報告ソリューションの開発に関する洞察を提供している。

DPM は、ビジネス用語や概念を階層的に整理するデータ中心の手法である（**図 2** 参照）。基礎となる法的要件から導き出される様々な報告シナリオにおいて、ビジネスフレンドリーかつ非技術的な方法でデータを提示する。DPM は、必要な共通理解をプロバイダとして提供することで、ビジネスと IT のコミュニケーションギャップを埋める。ビジネスコンセプトは、IT 専門家が必要とする正式なルールに従って DPM で指定される一方、ポリシーの専門家や他のデータ利用者が管理しやすい状態に保たれる。

図 2：DPM 法によるビジネス用語（データポイント）の分解



出典 ISO/TC

DPM 法は、用語や概念の正確で完全かつ曖昧性のない定義を提供する。これにより、ビジネスユーザーと技術ユーザーの両方が理解できる、基礎となるビジネス辞書に基づく情報要件（メッセージ、テーブル、データセット、キューブなど）の論理構造を構築することができる。欧州の関係者の協力により開発された DPM は、現在 ISO 5116 に含まれ、様々な国内外の規制当局で使用されている。[8]

XBRL は、財務、業績、リスク、コンプライアンス情報をデジタルで報告するための標準である。XBRL は、すべての人が利用可能なフリーライセンスのオープン標準である。[9]

プロバイダが提供する XBRL タクソノミはその一例である。このタクソノミーを各国当局が導入すれば、事業体による XBRL-XML や xBRL-CSV といった形式での報告が容易になる。既に XBRL に基づく報告金融機関を持っている法域もあれば、別の方法を選択する法域もある。

最終的な公表の一部として、FIRE の報告要件とともに、以下の技術支援標準も公表される：

- **DPM データ辞書：**これは、FIRE 報告に必要なデータの構造化された表現を提供するデータ辞書である。
- **妥当性確認ルール：**妥当性確認ルールとは、報告されたデータの一貫性を確認するために適用されるテストである。データセットに対する妥当性確認ルールの結果が真であれば、報告されたデータはそのルールに従って一貫している。結果が偽の場合、報告された情報にはチェックまたは修正すべき矛盾がある。

[8]ユーロファイリング（2021 年）、ISO 5116 標準として発行された DPM（8 月）を参照のこと。

[9]XBRL

- **XBRL タクソノミ：**報告書提出をサポートするために XBRL タグ付けされた FIRE 報告書。

XBRL レポートの妥当性確認や作成を容易にするために、金融機関が利用できる XBRL ツールは、オープンソースからエンタープライズまで様々なものがある。[10]

最も単純な形では、エクセルのプラグインが FIRE テンプレートを提供し、更新後、提出可能な XBRL ファイルの生成とともに妥当性確認ルールを実行することができる。金融機関は、XBRL 報告要件を効果的に管理するために、オープンソースソフトウェアを含め、それぞれのニーズに合った様々なソフトウェアソリューションを検討することができる。

FIRE レポートの基本要素

FIRE フォーマット内で定義されているすべての情報項目の根底には、16 の基本フィールドタイプ（附属書 A に記述）があり、関連する国際条約や標準に沿ったデフォルトの構文規則が定められている。

報告事業体と受信事業体との間で共通の解釈を容易にするために、この書式は、報告されるインシデントには直接関係しないが、交換される情報の性質を特定する以下の情報項目を定義している：

- **バージョン**：インシデントを記述するために使用される FIRE フォーマットのバージョンを記述し、送信者および取得者がこの報告書がどのバージョンに準拠するかを理解できるようにする。
- **レポートタイプ**：交換されるインシデント報告のタイプを記述する。バージョン 1.0 では institution initiated のみが実装されている。
- **報告言語**：最大 3 つの情報項目の組み合わせが使用され、言語コード（例：英 語の "en"）と国コード（例：グレートブリテン島の "GB"）を組み合わせることで、情報項目とその基礎となる定義の言語ローカライズを記述する。カスタムタグを使用することで、さらに言語をカスタマイズすることも可能である。
- **レポート通貨**：レポート内のすべての通貨参照に使用される通貨を記述する。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
FIRE	メッセージが準拠して FIRE フォーマットのバージョン	10 進数	**構文** • 小数点以下 1 桁の 10 進数で代表者を表す。 **妥当性確認** • ゼロより大きくなければならない **例**（架空） • *1.0*
FIRE レポート	FIRE インシデント報告のタイプ。メッセージの残りの部分に含まれるフィールドを決定する。	列挙	**構文** • テキスト（短い）列挙リストで、以下のいずれかの値を持つ： 金融機関主導 **例(架空)** • 金融機関主導型
FIRE レポート言語	ローカリゼーションをサポートするためにレポートが使用する言語	列挙	**構文**

[10]認証されたツールやソフトウェアは、XBRL インターナショナルのウェブサイトで見ることができる。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
			• ISO 639 言語コードの値を列挙したリスト。[11] **例** • en
FIRE レポート言語 国	ローカリゼーションをサポートするために、報告書に使用されている言語の国別バリエーション	列挙	**構文** • テキスト（短い） ISO 3166 alpha-2 エンコーディング国コードからの列挙リスト [12] **例** • GB
FIRE レポート言語のカスタマイズ	レポートで使用されるオプションのラベルカスタマイズの識別（ローカル実装者によって指定される）。	テキスト（短文）	**例** *BOE*（これは *FIRE* のバージョンであることを示す *BOE* カスタムラベル）
FIRE レポート通貨	使用通貨 報告書内のすべての金額参照	テキスト（短文）	**構文** • ISO 4217[13] で定義されているアルファベットコードの列挙リストから単一通貨を選択する。 **例** • 米ドル

金融機関主導の報告

インシデント報告導入の大部分は、金融機関主導の報告が代表者となっている。

つまり、事業体がインシデントを経験し、自発的に報告することを選択するか、状況によっては、インシデントが 1 つ以上の報告義務者に報告するきっかけとなる。

情報の流れは**イベントドリブンであり**、報告事業体から受信事業体への**一方向で**ある（**図 3 に**示す）。各受信事業体の個々の報告要件によっては、同じインシデントに対して複数のインシデント報告を発行する必要がある場合もある。

機関主導の報告に関する情報要件は、（**図 4 に**示すように）4 つの異なるコレクションに分類され、以下のような特徴がある：

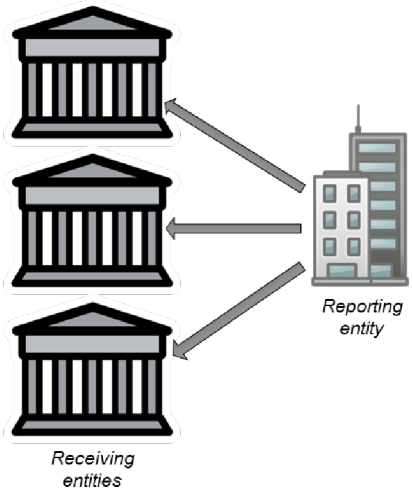
- **報告書の詳細**：誰が、誰に対して報告書を発行したのか？
- **インシデントの詳細**：何が起きたか／起きているか？
- **影響アセスメント**：どのような悪影響があるか？
- **インシデントのクローズ**：何がインシデントの原因となり、どのような改善措置が取られるのか？

[11] ISO (2002), *ISO 639 言語コード*

[12] ISO (2020), *ISO 3166 国コード*

[13] ISO (2015), *ISO 4217 通貨コード*

図 3：金融機関主導の報告



これらの情報項目を総合すると、受信事業体は、インシデントが発生したときにそれを理解し、それに応じて行動するために必要な情報を得ることができる。

図 4：金融機関主導の報告における情報項目のグループ分けの内訳

1. 報告内容	2. インシデントの詳細	3. 影響アセスメント	4. インシデントのクローズ
1.1 報告事業体	2.1 参考文献	3.1 重大度評価	4.1 原因
1.2 受入事業体	2.2 インシデント	3.2 影響を受ける当事者	4.2 レッスン
1.3 連絡先	2.3 前回報告書からの変更点	3.3 サービスとリソース	4.3 補足文書
	2.4 日付／時刻マーカー	3.4 影響	

1. 報告内容

報告事業体に関連する情報項目は以下の通りである：

(i) 属性は事業体に関連する；

(ii) どの受理事業体がこの報告インスタンスを受理すべきかの詳細、および、必要であれば、受理事業体がインシデントに関して連絡することができる報告事業体の個人の連絡先情報。

1.1. 報告事業体

これらの情報項目には、報告事業体の基本的な参照および分類フィールドが含まれる。**事業**体の法的名称または最も一般的に使用される名称（およびその親会社の名称）を反映する**事業体**名と**最終的な親会社名を**除けば、残りの項目は、受信事業体による報告事業体データセット全体の分析をサポートするように構成されている。

一意な事業体識別子に関しては、2 つの情報項目が定義されている：

- **グローバル識別子**：報告情報が取得者間で共有される可能性がある場合、LEI コード（ISO 174421:2020[14] に定義される）のようなグローバルに認知された識別スキームは、FIRE がどこで実施されるかにかかわらず、同一の事業体の報告を整合させるメカニズ ムを提供する。しかしながら、いかなるグローバルな識別スキームの使用も普遍的でない可能性があるため、 実施の裁量及び報告事業体による情報項目の入力方法の両面において、柔軟性がプロバイダとして 提供される必要がある。
- **ローカル識別子（複数可）**：法域や超国家金融機関によっては、報告事業体を一意に識別するた めに、既存の識別スキームがすでに使用されている。報告事業体には、関連する受信事業体によって定義されたスキーム名と対応する識別子を含める。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
事業体名	報告書を提出した事業体の名称（正式な法的名称または最も一般的に使用される呼称など）	テキスト（短文）	**例**（架空） 株式会社メガバンク
グローバル識別子	事業体ごとにユニークでグローバルに一貫した識別子を持つ。	配列（キー値）	**構文** • 識別子の名前, 識別子の値]の形式の（1 つ以上の）テキスト（短文）ペアの配列。 **妥当性確認** • LEI]識別子が使用される場合には、ISO17442-1:2020 に沿った固有の 20 文字の英数字コードの妥当性確認ルールを適用する。 番号 1-4 は常に LEI を発行した LOU の ID を示す。 ○ 5-6 の数値は常に 0 である。

[14]ISO (2020), *ISO 17442-1:2020 金融サービス-事業体識別子（LEI）第 1 部：割り当て*

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
			○ 番号／手紙 7～18 は事業体ごとに固有のものである。 ○ 19-20 は検証のためである。 • ""（空白／識別 子なし）の場合、フリーテキスト可 **例**（架空のもの） • レイ, • 自由
ローカル識別子（複数可）	ユニーク 受信側事業体の管轄区域内でローカルに使用される報告事業体の識別子（複数可	配列（キー値）	**構文** • 1 つ以上の）テキスト（短文）ペアの配列。 [識別子の名前、識別子の値]。 **妥当性確認** • もし""（空白／識別子がない）なら、フリーテキストが許される。 **例(架空)** • *FRN,* • *ABI,* • 自由
最終親名	報告事業体が属するグループの最終親会社の名称（該当する場合	テキスト（短文）	**例**（架空） グループ

事業体タイプ

報告事業体の性質に基づいて報告データのサブセットを調査する能力をサポートするため、**事業体 の種類を**示す情報項目がフォーマットとともに含まれている。設計に関しては、列挙をサポートする潜在的な参照点として様々な既存の産業分類スキーム（ISIC、NAICS など）が検討されたが、適切な一致点はないと判断された。さらに、多くの管轄区域では、インシデント報告以外の用途で、事業体タイプの定義がすでに地域の法律や規制の中で成文化されている。

したがって、事業体種別のアプローチは事業体識別子と同様であり、使用するスキーマに ついて完全な裁量が与えられ、そのスキーマから関連する列挙が選択される。この方法は、個々の実装者のニーズに合わせて複数のスキーマの使用をサポートし、既存および将来のスキーマとの後方互換性と前方互換性の両方を提供する。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
事業体タイプ	選択したスキーマに従って事業体のタイプを指定する。	配列（キー値）	**構文** • スキーマの名前、選択された列挙]という形式の（1 つ以上の）テキスト（短文）ペアの配列。 **妥当性確認** • ""（空白／スキーマなし）の場合、フリーテキスト可 **例**（架空） • *スキーマ 1、エンティティタイプ 1*

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
			• スキーマ 2、タイプ *A*

事業体の国名

管轄区域を越えた受信事業体へのインシデント報告をサポートするために、報告事業体の所在 地は、**事業体の国**情報項目を使用して把握される（影響を受ける場所は、影響地理的広がりの下で 別々に把握される）。この項目を支えるために、ISO 3166 国別コード標準が活用され、特に広く使用されている**アルファ 2 の** 2 文字の国別コード（例：インターネットの国別コードトップレベルドメイン）が活用される。このオプションは、簡潔でエンコードの長さが最適化されるという利点があるが、人間が読んでもすぐには判別できないかもしれない。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
事業体 国	報告事業体が所在する国	列挙	**構文** • ISO 3166 alpha-2 エンコーディングを使用した、テキスト（短い）ベースの列挙リスト国コード • *ES*

1.2. 受入事業体

このセクションは、インシデント報告の配信とルーティングに関するいくつかのシナリオを可能にするように設計されている：

- **取得者識別子：**情報項目は、報告主体が同じインシデント報告を複数の受信事業体に同時に送信することを可能にし、それによって一対多の効率性を促進する。この項目はまた、インシデント報告の受信を一元化し、その後配布するための、規制当局間の取り決めをサポートすることができる。しかし、このプロセスは、すべての受信規制当局がインシデント報告ライフサイクルの同じ段階にあることを必要とする（セクション 2.2 のインシデントステータスを参照）。受信した事業体は、報告事業体から同じインシデント報告を受信した他のすべての事業体を認識する。金融機関へのサプライチェーン内のインシデント報告を促進するために FIRE に整合したソ リューションが使用されている場合、サードパーティは、(i)特定の外部エンドユーザーにカスタムコンテ ンツを含む個別のインシデント報告を送信するか、(ii)特定のコホートを特定するために本情報項目内のフ リーテキストオプションを使用して、そのユーザーベースの全て又は の一部に広範なインシデント報告を送信することを選択することができる。
- **取得者履歴：**情報項目は、同じインシデントに関するレポートを以前に受信した事業体を表示するために使用されるが、現在発行されているインシデント レポート インスタンスは表示されない。この項目は、インシデントのライフサイクルの後半に報告トリガーが有効になる追加の受信事業体に最初のインシデント報告を送信するために使用できる。
- **転送：**情報項目は、報告事業体には公開されない。その代わり、この項目は、受信事業体がインシデント報告を、インシデントを直接知らされていない他の事業体に転送するための機能を提供する（適切な情報共有の取り決めが行われていることが前提である）。

例

シナリオステップ		受信事業体の情報項目
1	最初のインシデント報告が認可 AAA に送られる。	取得者識別子： AAA

シナリオステップ		受信事業体の情報項目
2	最初のインシデント報告は、その後、報告事業体から BBB に伝達される。	取得者識別番号：BBB 取得者履歴：AAA
3	AAA と BBB の両認証機関は、報告事業体から同じ中間報告を同時に受け取る。	取得者識別番号：AAA、BBB 取得者履歴：AAA, BBB
4	規制当局 AAA は規制当局 CCC と情報共有の取り決めをしており、ステップ 3 の中間報告を転送する。CCC は、取得者識別子の情報項目に記載されていないため、報告事業体からではなく AAA からこの報告書を受領していることを知っている。	受信者識別子：AAA、BBB 受信者履歴：AAA, BBB 転送元：AAA 転送先取得者：CCC

受信事業体が、受信者識別子にも転送先にも参照されていない報告書を受信した場 合、この報告書インスタンスはその事業体向けではない。このような場合、受信事業体は受信した情報を削除し、この報告書の宛先が間違って送信され たことを発信者に通知すべきである。しかし、報告事業体および転送送信者は、誤った取得者宛名による偶発的なデータ損失を防ぐため に、適切な管理者を導入すべきである。独立に発動する可能性のある多数の報告義務が存在する場合、インシデント・ライフサイクル全体 を通じたインシデント報告の順序は、各報告の相対的な日付／タイムスタンプによって決定される （セクション 2.4 参照）。

これらの情報項目で受入及び転送事業体を一意に参照するため、LEI コードの使用がサポートされるが、 他のスキームやフリーテキストも使用可能である。

裁量的インシデント転送機能を導入する場合、受信側事業体は、まず、自らのインシデント報告 の目的に沿って転送機能の利用が発動される状況、及びインシデントについて直接報告された情報を、 他の義務に抵触することなく共有できる範囲を決定すべきである。また、取得者は、当事者間のインシデント報告情報の移転を保護するために、適切な情報共有の取 り決めが行われていることを確認し、 、転送先が「知る必要がある」ベースで当該情報を取扱うための措置を講じていることを確認すべきである（MoU 条項、技術管理、アクセス管理、身元審査等を含むが、これらに限定されない） 。最後に、取得者は、規制・監督上の慣行に基づいて転送が行われる際に、発信元報告主体に通知するための仕組みを設けるべきである。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
取得者識別子	報告事業体が選択した、本報告書の宛先となる受信事業体の識別子を指定する。	配列（キー値）	**構文** • 1 つ以上の）テキスト（短文）ペアの配列。 [識別子の名前、識別子の値]。 **妥当性確認** • LEI」識別子を使用する場合は、ISO17442-1:2020 に沿った妥当性確認ルールを実施する。 • もし""（空白／識別子がない）なら、フリーテキストが許される。 **例**（架空） • *レイ, 123400abc123def45699* • 認可 *X*
取得者履歴	報告主体が同じインシデントに関する過去の報告を送信した受信	配列（キー値）	**構文** • 1 つ以上の）テキスト（短文）ペアの配列。 [識別子の名前、識別子の値]。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
	事業体の識別子を指定する。		**妥当性確認** • LEI」識別子を使用する場合は、ISO17442-1:2020 に沿った妥当性確認ルールを実施する。 • もし""（空白／識別子がない）なら、フリーテキストが許される。 **例**（架空） • *レイ, 123400abc123def45699* • 認可 *X*
転送元 *(*該当なし）	インシデント報告のオンワード共有を行うレポート取得者の識別子を指定する。	配列（キー値）	**構文** • 1 つ以上の）テキスト（短文）ペアの配列。 [識別子の名前、識別子の値]。 **妥当性確認** • LEI」識別子を使用する場合は、ISO17442-1:2020 に沿った妥当性確認ルールを実施する。 • もし""（空白／識別子がない）なら、フリーテキストが許される。 **例**（架空） • *レイ, 123400abc123def45699* • 認可 *X*
転送先取得者 *(*該当なし）	このレポート がレポート受信者によって転送される受信事業体の識別子を指定する。	配列（キー値）	**構文** • 1 つ以上の）テキスト（短文）ペアの配列。 [識別子の名前、識別子の値]。 **妥当性確認** • LEI」識別子を使用する場合は、ISO17442-1:2020 に沿った妥当性確認ルールを実施する。 • もし""（空白／識別子がない）なら、フリーテキストが許される。 **例**（架空） • *レイ, 123400abc123def45699* • 認可 *X*

1.3. 連絡先

インシデント報告書の提出後、受理側事業体が報告側事業体からのさらなる情報を必要とする場合、 報告側事業体は、連絡窓口として機能する少なくとも一人の主要代表者を指名するよう要請される。単一の連絡先または複数の連絡先の使用は、既存のインシデント報告体制によって異なるため、**事業体連絡先**情報項目は、受理側事業体がその地域のニーズに合わせて実施できるように、1 つまたは複数の連絡先をサポートするように設計されている。連絡先の

E メールと電話番号は、事業体代表者と連絡を取るための 2 つのコミュニケーションチャネルを持つために、両方とも必須情報項目とされている。

情報項目	目的 / 内容	フィールド	追加の構文と妥当性確認ルール、およびデータの例
事業体の連絡先	報告されたインシデントに関連する 1 人または複数の事業体代表者の氏名および連絡先情報	コンテナ	**構文** • 各事業体のコンタクトインスタンスのラッパー **妥当性確認** • コンタクト・タイプ = "プライマリー "のコンタクト・エントリーが少なくとも 1 つなければならない。
コンタクトタイプ	各連絡先の優先順位を示す。	列挙	**構文** • テキスト（短い）列挙リスト： o プライマリー O **例** • プライマリー
連絡先	報告事業体の連絡担当者の姓名	テキスト（短文）	**例**（架空） ジョン・
連絡先メールアドレス	報告事業体の担当者の E メールアドレス	テキスト（E メール）	**例**(架空) *john.smith@email.com*
連絡先電話番号	報告事業体の連絡担当者の電話番号（国番号を含む	テキスト (電話)	**例**(架空)
連絡役	報告事業体の担当者の役割	テキスト（短文）	**例**(架空) 上級役員（*CISO* など
連絡先	報告事業体の担当者の部署名	テキスト（短文）	**例**(架空) 規制
連絡先取得者	事業体とのコンタクトが適切な取得者	配列（リスト）	**構文** • **取得者識別子の**リストを用いて動的に入力される**。** **妥当性確認** • 取得者は 1 人以上でなければならない。 選択されている場合、識別子のリスト。空白の場合、連絡先はすべての取得者に妥当性確認される。 **例**(架空) • 認可 *X*

2. インシデントの詳細

報告されたインシデントに関連する情報項目は以下の通りである：

(i) 報告事業体は、インシデントまたは関連する可能性のある他のインシデントについて、固有の識別子を生成した；

(ii) インシデントの性質と状況は、インシデントが進展するにつれて拡大され、洗練されていく；

(iii) 前回のインシデント報告以降に起こった、そのインシデントに対して取られた措置や反応。

(iv) インシデントの主要なマイルストーンのタイミング情報。

2.1. 参考文献

個々のインシデント、およびインシデント間の可能性のある関係の追跡をサポートするために、フォーマットは、異なる目的を果たす 2 つの識別参照フィールドを使用する：

- **事業体内部インシデント ID** 情報項目は、報告事業体がインシデントを参照するために組織内部で使用する一意の識別子を捕捉する。受信側の事業体は、同じインシデントに関連するすべての報告を識別し、照合するために、この項目を使用する。
- **事業体関連インシデント ID（複数可）** 情報項目は、内部参照スキームを使用して、このインシデントを、その事業体が経験した以前のインシデント（以前に報告されたか否かを問わない）に関連付ける能力を、報告事業体に提供する。これにより受信事業体は、報告事業体と同じ関係情報にアクセスできる。

事業体提供 ID は、受信事業体間のオンワード・フォワーディングと組み合わせると、個人または集団ベースで報告事業体に関与する際、取得者間で一意のキーとして機能する。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
事業体内インシデント ID	報告事業体が発行した、インシデントを明確に特定する固有の参照コード	テキスト（短文）	**例**（架空） *INC123456789*
事業体関連インシデント ID（複数可）	報告事業体は、関連する可能性のある他の現在または過去に解決されたインシデントとの関係を作成することができる。	配列（リスト）	**構文** • テキストの配列（ショート） **妥当性確認** • ゼロ、1 つ、またはそれ以上のエントリーを持つことができる **例**（架空） • *INC11111111* • *INC22222222* • *INC3333333333*

2.2. インシデント

このセクションでは、インシデントの基本属性を記述し、何が発生したかを把握する。インシデント情報の他の要素と同様に、対処すべき競合要件がある：

- インシデント報告情報の共通の解釈、表現、処理、分析を促進するなど、あらかじめ定義された構造化された情報項目を最大限に活用することで、**一貫性を高める**。
- **柔軟性を維持**し、インシデントの質的な詳細を記録する能力を**維持することで**、あらかじめ用意されたオプションでは容易に反映させることができない。

フェーズとインシデントの状況を報告する。

インシデントを説明する前に、報告書が生成されるフェーズを、受信事業体のインシデント報告トリガー規準、インシデントのステータス、および以前の報告書が発行されたかどうかに基づいて決定する必要がある。

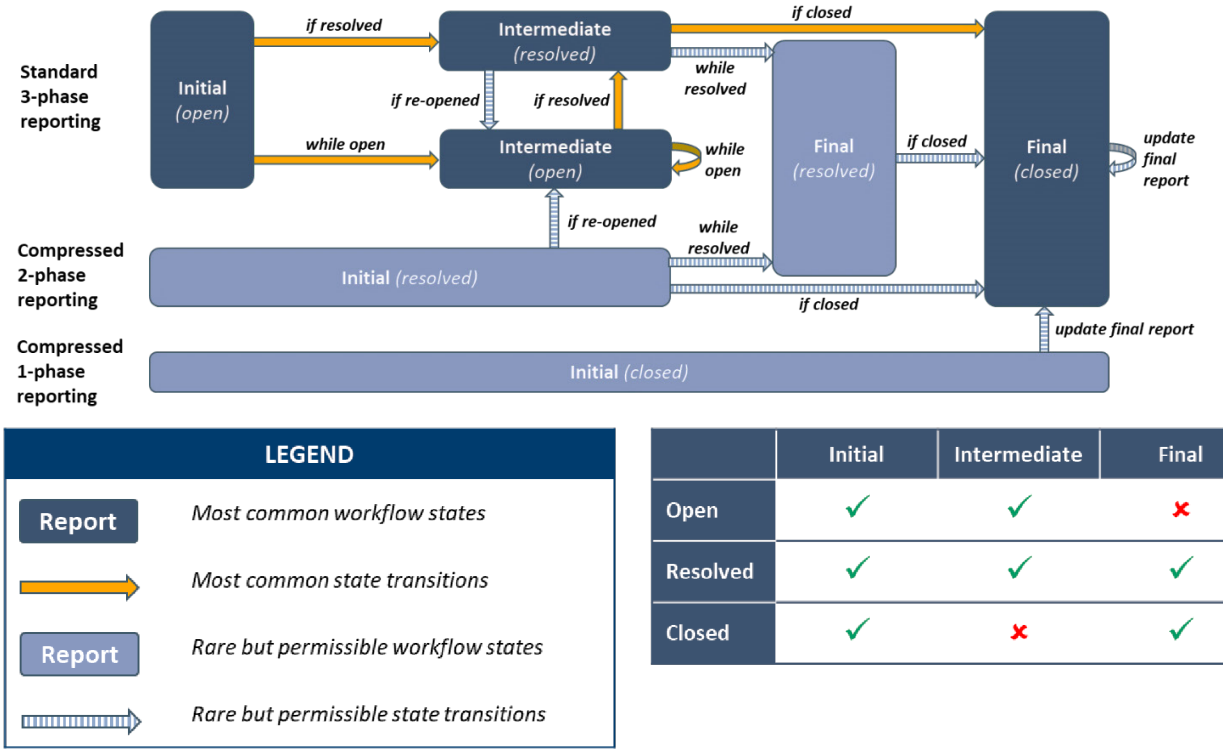
この書式は、**報告段階の**情報項目に反映された 3 段階のワークフローを採用しており、FSB のサイバーインシデント報告に関する作業に反映されているように、（用語は異なるものの）認可当局が現在使用している最も一般的なアプローチを反映している[15]。

- **初回**：取得者の報告トリガー規準に基づいて、1 つ以上の取得事業体に発行された最初のインシデント報告。
- **中間報告**：インシデントが解決されるまで、また解決されたときを含め、さらなる取得者報告トリガー規準に基づき、同じインシデントに関して報告事業体により発行される可能性のある追加報告。
- **最終報告書**：受入事業体の期待に沿い、インシデント発生後の所見と是正措置を含む最終報告書を提出する。

図 5 は、状態間の遷移と**インシデントステータス**情報項目との相互作用を示す。FIRE フォーマットは、3 相報告の最も一般的なユースケースをサポートするが、ローカルなアプローチが望ましい場合は、2 相報告や 1 相報告もサポートすることができる。

[15]FSB (2023b)

図 5：レポート段階のワークフローと妥当性確認状態



	Initial	Intermediate	Final
Open	✓	✓	✗
Resolved	✓	✓	✓
Closed	✓	✗	✓

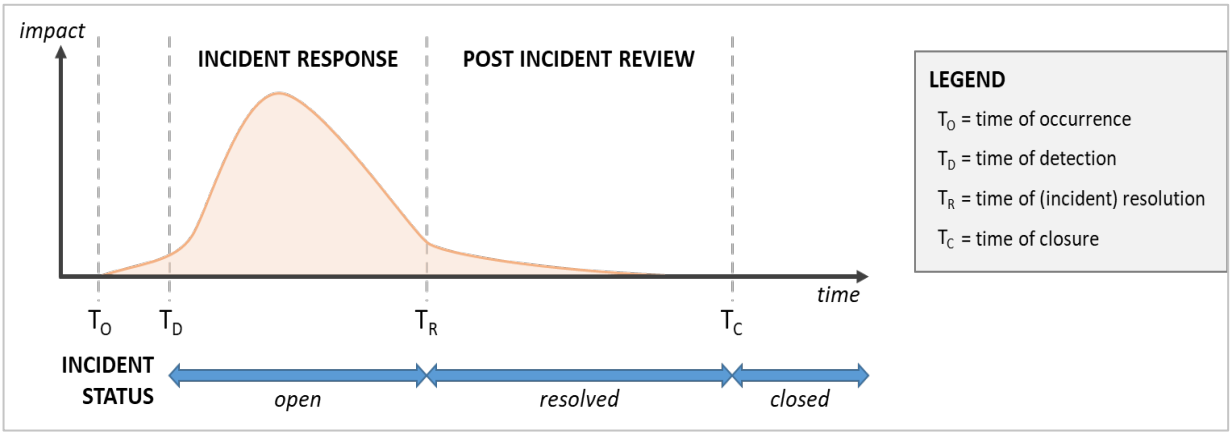
ほとんどの場合、トリガーされると、インシデント報告ワークフローはこれら 3 つの段階を順番に通過し、複数の中間報告または最終報告が発行される可能性がある。しかし、許容されるエッジケースの組み合わせもある：

- **初回／解決済み**：初回報告の規準は満たしているが、インシデントがすでに解決済みである場合（圧縮された 2 段階報告）。解決された状態であれば、中間フェーズで規定されたデータ要件が適用される。
- **初回／クローズ**：初回報告の規準は満たしているが、インシデントがすでにクローズされている場合（圧縮された 1 フェーズ報告）。クローズされた状態であれば、最終フェーズで定められたデータ要件が適用される。
- **最終／解決**：インシデント発生後のレビューが終了する前に最終報告のトリガーが発生し、インシデントのクローズに関連する情報項目に関する最初の見解が必要とされる場合。このユースケースはまた、以前に発行された報告書を補強または調整するために、複数の最終報告書が提出される可能性があることを意味する。

インシデントのステータスは、3 つの可能な状態に単純化され、それらは（**図 6 に**示すように）主要なインシデント時間マーカーに関連して定義される：

- **オープン**：検知時点（T_D）から解決時点（T_R）までの期間であり、報告事業体がインシデントへの対応に集中し、影響を制御下に置き、おそらく正常ではないが安定した状態に戻るまでの期間である。
- **解決済み**：解決時（T_R）からクローズ時（T_C）までの期間であり、インシデントの直接的な悪影響が対処されたときであるが、長期的な影響からの回復には時間がかかる場合がある。インシデント後の正式なレビューは、通常この期間に実施される。
- **クローズ**：インシデント後のレビューが終了し（T_C）、所見と改善活動が特定された場合に想定される状態。

図 6：ライフサイクルの状態遷移に対するインシデント状況



インシデントの状態間の移行は、ほとんどの状況において、オープンから解決、または解決からクローズというように、本質的に一方向であることが意図されていることに留意することが重要である。しかしながら、最初に解決済みとみなされたインシデントがまだ進行中であると判断され、そのため新たなインシデント報告ワークフローを開始する追加的な負担を避けるためにオープン状態に戻す機能が必要となる場合がまれにあるかもしれない。インシデントが繰り返し発生した場合は、新しいインシデントとして扱われ、関連するインシデント ID を使用してインシデントの前回の発生が参照され、新しいワークフローが開始されることが期待される。

金融機関主導の報告においては、インシデントの状況もまた、**報告段階の任意性と**呼ばれる報告形式のもう一つの重要な特徴の原動力となる。インシデントが発生した当初は、2 つの重要な初期アセスメントの課題を考慮する必要がある：

- **情報の信頼性**：状況認識が低い初期段階では、インシデントの根本的な性質を判断できないことがある。
- **過度の初期負担**：報告事業体にとっての優先事項は、インシデントに対応し、その影響を制御下に置くことである。この時期の過度な報告要件は、報告事業体がこの成果を達成するのを妨げたり、気を散らしたりする可能性がある。

したがって、当初に必要とされる報告情報の規模は、可能な限り最小である必要があるが、受入事業体がそのマンデートを実行するための要件を満たすには十分である。インシデントが終息に至るまで進行するにつれて、フォーマットは、各移行時点で期待される情報を反映するために、報告フェーズの任意性を調整する（すべての金融機関主導の報告情報項目とその任意性の内訳については、附属書 B を参照）。この書式は、報告段階の任意性のための最小限の情報セットを反映したものであり、受理側事業 体は、その地域のニーズを反映するために、任意の情報項目の収集を追加的に要求することができる ことに留意されたい。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
報告	報告書が発行されたインシデントのフェーズを記述する。	列挙	**構文** • 以下のいずれかの値を持つテキスト（短い）リスト： o 初期 o 中間 o 最終 例 • 初回

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
インシデントステータス	インシデントのライフサイクルを 3 つの段階に分けて代表者を示す。	列挙	**構文** • テキスト（短い）リスト。 o オープン o 解決済み o 解決済み **妥当性確認** • レポート段階との互換性のない組み合わせは却下する： o 中級＋クローズド o 最終＋オープン 例 • オープン

インシデントのタイトルと説明

異なる粒度レベルでインシデントの全体的な反映を提供する 2 つの重要な質的情報項目は、インシデントタイトルとインシデント説明である。これらはそれぞれ異なる目的を果たす：

- **インシデントタイトル：**情報項目は、インシデントを簡潔に反映し、広範な（場合によっては専門外の）聴衆がアクセスでき、解釈できることを意図している。これらの情報項目にとって有用な例えは、インシデントタイトルが主要メディアの見出しを表すのに対し、インシデント記述には根本的なストーリーが含まれ、インシデントを区別するために十分に特徴的であることを目的とする、というものである。インシデントタイトルは、インシデントの発生時にそのような具体性を提供することができない場合があるため、（参照識別子がインシデントのライフサイクルを通じて 追跡を維持するように）インシデントが進展するにつれて、インシデントの性質をより正確に反映するために、同じインシデントのレポート間で異なる場合がある。
- **インシデント記述：**情報項目は、報告事業体が、追加の制約を課すことなく、インシデントのより広範な質的記述を提供することを可能にする。タイトルと同様に、説明の内容は、インシデントの現在の理解を反映するために、時とともに発展させることができる。この項目は、フォーマット内の他のインシデント関連情報項目に反映されていない、特異な認可報告要件のためのキャッチオールとしても使用できる。報告事業体によって取られた、または計画された行動は、別に捕捉されることに留意すべきである。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
インシデントタイトル	報告事業体が記載したインシデント名または見出し	テキスト（短文）	**例**（架空） オンライン・バンキング・プラットフォームへの断続的なアクセス
インシデント記述	構造化された情報項目を補足するために、インシデントの最も関連性の高い側面を要約して説明する。	テキスト（長文）	**例**（架空） 報告されたインシデントに関する詳細な説明

インシデント・タイプ

インシデントを分類するために認可当局が使用する最も一般的な方法の一つは、タイプに基づくものである。しかし、このデータフィールドの使用はほぼ普遍的であるが、当局間での実装は一般的に特注である。より収束させることを目的として、この仕様は、**インシデントタイプ**分類への一貫したアプローチを提案することによって、この断片化の原因に対処しようとするものである。

既存のインシデント報告慣行を比較すると、インシデントタイプの割り当てによって、**イベントとその因果関係が混同される**ことがよくあった。例えば、既存のインシデントタイプの分類には、「ソーシャルエンジニアリング」や「フィッシング」が含まれるかもしれないが、これらのタイプは、発生したオペレーション上のイベント（例えば、データ侵害）ではなく、手法やベクトルを記述している。インシデントの根本的な原因を記述する際には、これらの要素を捉える方がより正確であろう。

この問題を考慮するため、FIRE の設計では、ボウタイ方式（[16]）に基づき、原因（インシデント・クロージングの柱）、インシデント・タイプ、結果としての影響（影響アセスメントの柱）を区分している（**図 7**）。附属書 C にあるインシデントタイプの列挙は**、原因にとらわれず**、様々な脅威やハザードから発生する可能性がある。この アプローチ（[17]）により、インシデントをより簡潔かつ一貫性をもって分類することができる。一方、考えられる原因はより広範かつ精巧なものとなる可能性がある。

図 7：仕様内でのボウタイ工法の適用

場合によっては、インシデントの根本的な原因が**完全に理解される**のは、インシデントの後期になるか、場合によってはインシデント後のレビューが行われるまで理解されないこともある。したがって、報告の初期段階で原因／事象を分離しておくことは有益である。また、マルウェアの展開とデータの流出など、状況によっては複数のインシデントタイプが該当する可能性もある。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
インシデント・タイプ	因果関係ではなく）事象の種類に基づくインシデントの分類を提供する。	配列（リスト）	**構文** • 列挙されたテキスト（短文）型の配列 • 附属書 C のリストから複数選択する。 **妥当性確認** • 複数のインシデント・タイプを持つことができる • インシデントの種類は当初は完全にはわからないが、インシデントが解決したときに「必須」となる。

[16]ボウタイ・メソッドは、リスクシナリオを分析し、伝達するために使用できるリスクアセスメント手法であり、ボウタイに似た図の形状からその名が付けられた。

[17]このアプローチは、「イベント・タイプ」で提案された同様の方法を反映し、適応させたものである：

リッチモンド連邦準備銀行（2020 年）、Curti 他、金融リスクマネジメントのためのサイバーリスクの定義と分類

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
			• データ漏洩

インシデント痕跡

インシデントに対応している間、報告事業体は、原因および/またはインシデントの発生源に関する情報を発見する可能性があり、受信事業体に関連する可能性がある。インシデント痕跡情報項目は、非構造化ロングテキストデータタイプを使用することで、そのような情報を任意に報告する柔軟な金融機関を提供する。この情報項目が使用される可能性のある痕跡のタイプには、以下に限定されないが、以下が含まれる：IP アドレス、URL アドレス、ドメイン、ファイルハッシュ、マルウェアデータ、ネットワーク活動データ、電子メールメッセージデータ、DNS 要求およびレジストリ構成、ユーザーアカウントアクティビティ、またはデータベーストラフィック。

情報項目	目的／内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
インシデント痕跡	インシデントの原因究明に役立つ具体的な詳細を記載する施設	テキスト（長文）	**例** • *IP アドレス、1.1.1.1* • ドメイン、*example.com*

インシデント発見手法

各インシデントに関連する**発見方法は**、報告事業体にとっても受信事業体にとっても有用な属性である。このデータポイントは、事業 体がインシデントを認識するさまざまな経路に関する洞察を提供し、将来のインシデント検知能力開 発に情報を提供することができる。リストのオプションは、VERIS[18] にプロバイダとして提供された同様のリストの調整版に基づいており、いくつかの項目が追加・統合されている。可能性のある発見方法をすべて説明することは不可能な場合があるため、インシデント記述情報項目を使用して補足的な方法詳細を反映できるように、「その他」オプションが含まれている。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
インシデント発見手法	報告事業体がインシデントをどのように発見したかを示す。	列挙	**構文** • 附属書 D からの単一選択を含むテキスト（短い）リスト **例** • 社外 - 法執行機関

インシデント報告トリガー

報告トリガー：規準は各受領事業体によって独自に定義されるため、報告主体がインシデント報告書を発行する根本的な理由は大きく異なる。従って、この情報項目は、報告義務の引き金となり得る影響タイプ（セクション 3.4 による）または取られた行動を反映するために一般化されている。

すべての可能なシナリオを考慮するために、報告事業体は、どのトリガー規準が適用されるかを示すか（前 に識別された取得者識別子を用いて、各取得事業体について）、または報告はトリガーに関連しないことを記 述することができる。追加オプションは、発生または検知に基づく報告規準の使用をサポートするために提供される。

[18]Verizon (2019), *Vocabulary for Event Recording and Incident Sharing (VERIS)* (Discovery_method 列挙)

- **オペレーション**
- **財務**
- **評判**
- **法的／規制的**規制当局の報告義務違反など）
- **外部**
- **地理的広がり**
- **インシデントタイプ**（データ損失など）
- **社内エスカレーションのレベル**（インシデントの重大性に反映される可能性がある）
- **被認定団体**（その他の認定機関／規制当局）
- **時間ベースの要件**（すなわち、特定のタイムマーカーから定められた期間内に報告する義務）
- **目的に対するリスク**（インシデントに起因する影響が、1 つまたは複数の受入事業体の目的をリスクにさらす可能性がある場合）。
- **トリガーとされなかった**（プロアクティブまたはレトロスペクティブに報告された）
- **その他**

複数の取得者認可にまたがる同時トリガーをサポートするために、取得者識別子は、関連するトリガーのそれぞれに対して反映される。

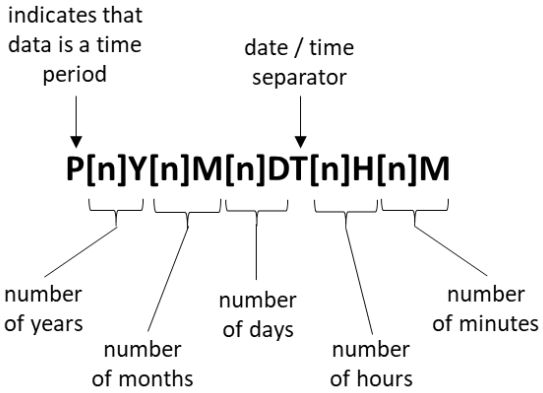
情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
インシデント報告トリガー	報告事業体に対して、報告規準のどの側面が発動されたか、またどの報告取得者について発動されたかを宣言する機能を提供する。	配列（リスト）	**構文** • 1 つ以上のトリプレットの配列： [テキスト（短）列挙リスト、テキスト（短）、テキスト（長）]。 • 以下の値から列挙リストを選択する： ○ オペレーション上 ○ 財務 ○ 評判 ○ 法律/規制 ○ 外部 ○ 地理的広がり ○ インシデント・タイプ ○ 内部エスカレーションのレベル ○ 被認定団体 ○ 時間ベースの要件 ○ 目的に対するリスク ○ トリガーされない ○ その他

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
			• 取得者識別子の値を持つテキスト(short) • さらなる文脈を提供するオプションのテキスト（長文 妥当性確認 • 以前にプロバイダから提供されたエントリーから選択された事業体を受け取る 例 • 金融、認可 X、100 万ドル超の損失が見込まれる

解決までの推定期間

インシデント解決の推定期間を提供するための情報項目は、報告事業体が受信事業体に対して、いつインシデントが管理下に入るかを示すことができるように、フォーマット内に含まれる。ISO 8601 標準[19]は、一貫した方法で期間を記録するために使用される。各時間要素は、報告事業体が分、時間、日、月、あるいは年単位で見積もりを提供できるように、オプションで表現することができる。**図 8 を**参照のこと。

図 8 : ISO 8601 標準



情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
解決までの推定期間	事業体に対して、インシデント解決までの期間を示す機能を提供する。	期間	**構文** • ISO 8601 標準に従って、シンタックスのサブセットを提供することができる。 • *3 時間 30 分は次のように表される。PT3H30M*

2.3. 前回報告書からの変更点

インシデントの詳細に関する前のセクションが、インシデントの進展する性質を捉えようとするものであったのに対し、このセクションの情報項目は、報告書と報告書の間に（またはインシデントがあれば最初の報告書の一部として）生じた新たなインシデントの進展を反映するために、グループ化されたものである。このセクションの 6 つの情報項目は、構造化されたフォーマットと構造化されていないフォー マットが混在している。この書式を導入する受理側事業体は、自由記述欄で受理したい特定の内容についての追加ガイダンスを提供することを選択できる。

[19]ISO (2019), *ISO 8601-1:2019 日付及び時刻-情報交換のための表現-第 1 部：基本*

- **取られた措置**：インシデントを管理下に置くために報告事業体が取った措置。この情報項目は、取り得るすべての行動を先取りするのではなく、意図的にフリーテキストとしている。記録される行動は、報告書固有のものであることを意図している。しかし、同じインシデントに関連するすべての報告書にわたって、この の情報項目の項目を統合することにより、インシデントの過程における行動の完全なタイムラインを最終報告書で再構成することができる（報告書のタイミング情報と並行して）。
- **計画されている行動**：報告事業体がインシデントを管理下に置くためにとることを計画しているステップ（報告事業体は、計画されている行動が特定されていない、または必要でない場合も示すことができる）。
- **一般大衆の反応**：主流メディアやソーシャル・メディア・チャンネルから生じた報道、声明、感情の要約。
- **発行されたコミュニケーション**：報告事業体が、プレスリリース、ソーシャルメディアへの投稿、影響を受けたすべての関係者に送信された電子メールなど、公的または私的に、インシデントに対応した広範な外部コミュニケーションを発行または更新したかどうかを示す。したがって、この情報項目は、当局に対する個々の影響当事者との特注の二者間交流を含むことを意図していない。
- **被認証団体**：インシデント報告の直接の取得者である金融当局とは別に、この情報項目は、インシデントを被認証した他の当局や認定機関の名称を取得する。これらの団体には、関連する国家安全保障局（例：サイバーセキュリティ機関）、法執行機関、またはインシデントに関心を持つ利害関係者グループ（国内外）が含まれる可能性がある。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
行動	インシデントを管理下に置くために報告事業 体が取った措置の説明	テキスト（長文）	**例**（架空） • 事業体はインシデントを解決するためにこの措置をとった。
行動計画	インシデントを管理下に置くために報告事業体が計画している措置の説明	テキスト（長文）	**例**（架空） • 事業体は、インシデントを解決するために以下の行動をとる予定である。
世間の反応	インシデントに起因するメディアまたは世論の現在の言論レベルの説明	テキスト（長文）	**例**（架空） • インシデントは以下のようにメディアに取り上げられ、ソーシャルメディア上でも存在感を示している。
通信発行	外部のステークホルダーに対するインシデントに関するコミュニケーションの記述	テキスト（長文）	**例**（架空） • 事業体はこのインシデントに関して、以下の正式なコミュニケーションを発表した。
被認定団体	、インシデントの通知を受けたすべての非金融当局または関連機関（国内外）のリスト。	配列（リスト）	**構文** • テキストの配列（ショート） **妥当性確認** • ゼロ、1 つ、またはそれ以上のエントリーを持つことができる。 **例**（架空） • 国家サイバー • 法執行

2.4.日付／時刻マーカー

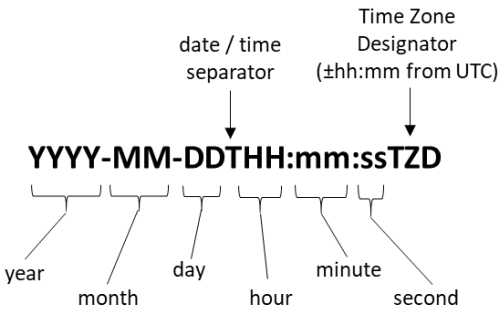
インシデント情報には、インシデント内のマイルストーンの特定のタイミングを反映する日付／時間マーカーが含まれることが多い。これらのマーカーのうち 4 つはすでに**図 8 で**言及したが、さらに 2 つのマーカーが補足されている：

- **報告時刻**：特定の報告がいつ発行されたかを記録する。受信事業体は、同じインシデントに関連する報告の順序を決定するために、この情報を必要とする。
- **次の報告の時期**：次の報告がいつ発行されるかの期待値を管理するために、報告事業 体がプロバイダとして提供する推定値。これは、報告間の一定期間、状況の変化に基づく中間報告、インシデント解決時にのみ要求される中間報告など、報告を受ける事業体によって定義される中間報告の報告トリガーにある程度依存する。

セクション 2.2 の期間の取り扱いと同様に、日付／時間マーカーの構文も ISO 8601:2019 標準を使用し、**図 9 に**示すように、時間に関して 2 つの注記がある：

- 精度が要求される場合は、**秒を**含める
- **タイムゾーン・デジグネータ（TZD）**により、ローカル・タイムゾーンを使用してタイミング情報をエンコードし、その後 UTC（協定世界時）に相対的にシフトすることができる。

図 9：ISO 8601 標準



情報項目	目的 / 内容	フィールド	追加の構文と妥当性確認ルール、およびデータの例
報告時期	報告書がれた日時	日付	**妥当性確認** • 日時は過去のものでなければならない。 例 • *2024-06-15T12:32:20+00:00*
発生時期	インシデントが発生した日時（判明している場合）	日付	**妥当性確認** • 日時は過去のものでなければならない。 • 検知時よりも早く、または検知時と同等でなければならず、解決やクローズよりも早くなければならない。 例 • *2024-06-15T12:32:20+00:*
検知時刻	インシデントが検知された日時	日付	**妥当性確認** • 日時は過去のものでなければならない。 • 発生時刻より後、または発生時刻と同じでなければならない（プロバイダがある場合） • 閉店時間より早くなければならない 例 • *2024-06-15T12:32:20+00:*

情報項目	目的 / 内容	フィールド	追加の構文と妥当性確認ルール、およびデータの例
解決時期	サービス、活動、および／または業務がインシデントから復旧した日時	日付	**妥当性確認** • 日時は過去のものでなければならない。 • 発生時刻より後でなければならない（プロバイダの場合） • 閉店時間より早くなければならない 例 • *2024-06-15T12:32:20+00:*
終了時間	インシデントが終了した日付と時刻、および特定された原因	日付	**妥当性確認** • 日時は過去のものでなければならない。 • 検知・解決時刻より後でなければならない。 例 • *2024-06-15T12:32:20+00:*
次回更新時期	報告事業体が次の報告書を発行すると予想される日時	日付	**妥当性確認** • 日時は未来でなければならない。 例 • *2024-06-15T12:32:20+00:*

3. 影響アセスメント

インシデントから生じる結果は、通常、影響という形で表現される。この影響は、ISO[20] 、「目標に影響を及ぼす混乱の結果」と定義されている。しかし

影響の測定には、インシデントが発生した後にしか収集できず、すぐには判別できないかもしれない遅行指標の研究が含まれる。

したがって、インシデント報告を目的とした影響の評価と明確化は、特に初期の段階では、既知のもの、または容易に観察可能なものに基づかなければならない。報告事業体にとって、影響の認識は通常、報告事業体内（ ）で経験されるか、利害関係者からなる直接的なコミュニティに発せられる一次的影響に限定される。その結果、個々の報告主体から得られる影響情報の範囲は、事業体が下流 の影響について知っていることや、金融システムの他の部分やより広範な経済への伝染の可能 性によって制約されることになる。多くの規制機関に影響を及ぼすセクター全体またはクロスボーダーのインシデントの場合、 金融当局は、市場セクター参加者のターゲットとなるサブセットに対する影響評価を実施するため、 および／または法域レベルの評価を実施するために、規制当局主導の報告を促すことを望むかもしれない。

したがって、影響に関連する情報項目は、報告事業体がアセスメントを行う順序を反映するようにグループ化され、順序付けされている：

- 報告事業体による**重大性の**分類
- インシデントの**影響を**受けた**当事者たちで**
- インシデントによって影響を受ける事業体**サービスおよびリソース**。
- 正規化された尺度を用いた、**影響の**定性的表現である。

3.1. 重大度評価

影響度アセスメントがインシデントの影響を外向きに評価しようとするのに対し、**重大性の**概念は、報告事業体がインシデントへの対処にどの程度の重要性と緊急性を置いているかを示すものである。金融機関や規制当局が使用する重大性へのアプローチは、一般的に各組織に合わせたものであり、したがって特異なものである。

これは 2 つの相反するドライバーとのジレンマをもたらす：

- 事業体間の比較可能性を高めるために、より大きなコンバージェンスを達成する。
- 個々の金融機関の選択とエコシステム全体の多様性を尊重する。

適切なバランスをとるため、このフォーマットの中で、深刻度に関連する 2 つの情報項目は、以下のように実装されている：

- **事業体の深刻度**情報項目は、報告事業体が内部的にインシデントの深刻度をどのように参照し ているかを把握する。深刻度レベルは、インシデントの経過を通じて変化する可能性がある。最終報告書に記録されるレベルは、インシデントのライフサイクルの中で報告事業 体が割り当てた最も深刻なレーティングを表すことが期待される。
- **標準化された重大度**情報項目は、共通の基準尺度に照らして評価された、報告事業体の重大度の正規化された解釈を反映する。一貫性のある尺度を導入することで、報告されたインシデントデータセットの重大度を相対的に比較することが可能になる。先の情報項目と同様、最終報告書で報告される標準化された

[20]ISO (2021), *ISO 22300:2021* - セキュリティとレジリエンス - 用語集

深刻度は、インシデント全体を通じて、報告を受けた事業体によって割り当てられた最も深刻な評価を反映する。

このアプローチは、報告事業体間で同質性を強制することなく、ある程度の標準化を促進しようとするものである。重要度の割り当ては、インシデント検知およびインシデント管理手順の開始時点から、報告事業体（ ）によって行われるため、標準化された重要度は、すべての機関が開始したインシデント報告において必須項目である。標準化された重大度は、インシデントの重大度に応じて内部エスカレーションに関連する概念も組み込んでいる。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
事業体の重大性	内部インシデント分類に従った報告事業体の重大度レーティングを記述する。	テキスト（短文）	**例**（架空） 重要度 *2*
標準重症度	報告されたインシデント全体における重大性の一貫した分類を促進するために、観察された影響に関連付けられた重大性の標準化された見解。	列挙	**構文** • テキスト（短い）列挙リストで、以下の値を持つ（詳細は附属書 E を参照）： o なし o ごくわずか o 低い o 中位 o 高い o 極めて高い **例** • 中位

3.2. 影響を受ける当事者

報告されたインシデントにより、金融セクターの内外を問わず、他の関係者がどの程度影響を受けるかを伝えるため、**影響を受ける関係**者の種類を説明する情報項目がフォーマット内に含まれ、以下のオプションがある：

- **報告事業体**：報告書を発行した事業体は、インシデントによって直接的な影響を受ける（報告事業体が、同じ組織内の別の事業体に代わって報告義務を果たすことは可能だが、影響を受けないことに注意）。
- **その他の関連事業体**：同じ組織内の影響を受ける他の事業体
- **ビジネス・カウンターパーティ**：既存の取引関係がある別の金融機関
- **その他の金融市場参加者**：これまでの選択肢で説明されていない、インシデントの影響を受けるその他の金融機関 **サードパーティ・ベンダーまたはサービスプロバイダー**：金融セクターをサポートする非金融事業体
- **非金融部門**：金融部門以外の影響を受ける事業体
- **顧客／消費者**：報告事業体（または関連事業体）から金融サービスを消費する、影響を受ける個人または法人顧客

- **脆弱な顧客／消費者**：前述の選択肢のサブセットで、個人的な事情により特に危害を受けやすい個人を指す。
- **一般大衆**：報告事業体またはその関連会社と関係のない社会の人々

同じインシデントによって、他の当事者は 2 つの影響を受ける可能性がある：

(i) 報告事業体において影響を受けるサービスの直接的または間接的な結果として。

(ii) なぜなら、同じインシデントが報告事業体だけでなく、他の事業体にも影響を及ぼしているからである。

関連する影響を受けた事業体」情報項目は、報告事業体がインシデントの影響を受けた組織内の事業体を特定するための仕組みを提供する。

影響を受けた注釈」情報項目は、どの当事者が影響を受けたかを補足的に説明するために含まれている。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
当事者タイプ	報告事業体からサービス中断の直接的な影響を受けた当事者、または同じインシデントの結果、報告事業体を経由しなかった当事者のタイプを記述する。	配列（リスト）	**構文** • テキスト（短文）列挙型の配列： o 報告事業体 o その他の関連事業体 o 取引先 o その他の金融市場参加者 o サードパーティ・ベンダーまたはサービスプロバイダ o 非金融部門 o 顧客／消費者 o 脆弱性顧客／消費者 一般 **妥当性確認** • 同じインシデントで複数の当事者が影響を受ける可能性がある。 **例** • 報告事業体 • その他の事業体 • その他の金融市場参加者 • 顧客／消費者
¥関連事業体	同じ組織内でインシデントの影響を受けたすべての事業体のリスト。	配列（キー値）	**構文** • 1 つ以上の）テキスト（短文）ペアの配列。 [識別子の名前、識別子の値]。 **妥当性確認** • LEI」識別子を使用する場合は、ISO17442-1:2020 に沿った妥当性確認ルールを実施する。 • もし""（空白／識別子がない）なら、フリーテキストが許される。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
			例（架空） • *レイ, 123400abc123def45699* • 自由
特記事項	影響を受ける当事者について、より広範な説明を提供する。	テキスト（長文）	**例**（架空） 複数のリテール銀行とその顧客基盤に影響を与えた市場全体のインシデント

3.3. サービスとリソース

インシデントが発生した当初は、状況を完全に理解できないかもしれないが、報告事業体は、そのサービスや基礎的なリソースに対する技術的な影響について合理的な理解を迅速に深めることができる可能性が高い。この情報は、包括的な影響アセスメントに向けて構築できる情報項目の次のグループを形成する。

サービス

この書式における「サービス」という用語の使用は、合同フォーラムが 2006 年に発表した「事業継続のためのハイレベル原則」（[21]）における定義に沿って、「業務」と同義であることを意図している。しかし、アセスメントの焦点は主に外部化された影響であるため、「サービス」の優先順位は、報告事業体内の影響を受ける業務ではなく、外部の当事者が報告事業体とどのように相互作用するかに基づいている。サービスの重要性の概念も切り離され、個別に評価される。このような区分により、外部への影響を伴わない内部サービスに関わるインシデントも報告することができる。

同じインシデント中に複数のサービスが中断される可能性があるため、フォーマットでは、影響を受ける各サービスについて 9 つの属性を捕捉するように設計されており、最初の 4 つは、影響を受ける各サービスの性質と中断のタイプを記述している：

- **サービス名**：サービスを識別するために会社が使用する記述的用語。
- **サービスタイプ**：影響を受けるサービスの一貫した分類の使用をサポートするために、この情報項目は、（事業体タイプと同じ方法を使用して）選択されたスキーマに対してサービスをマッピングする金融機関を提供する。
- **サービスクリティカル（service critical）**：重要度（severity）と同様に、各報告事業体 は、サービスの重要度（criticality）のレベルを定義する独自のアプローチを持つ。この情報項目には、スカラーを実装するのではなく、報告主体が判断した、重要または重要なサービスの規準が満たされる受信事業体のリストが含まれる。
- **サービス中断の種類**：サービスは様々な方法で中断される可能性があるため、附属書 F に記載されているように、様々な中断の種類に対応する形式となっている。この形式は、FSB サイバーレキシコン（FSB Cyber Lexicon）の「サイバーセキュリティ」の定義（[22]）（附属書 I にも記載されている）に記載されて

[21]バーゼル銀行監督委員会（2006）、ジョイント・フォーラム、事業ためのハイレベル原則

重要な業務またはサービス」という用語は、「金融業界参加者、金融認可、および／または関係する金融システムの継続的なオペレーションにとって重大な損失となる活動、機能、プロセス、またはサービス」と定義されている。

特定の業務やサービスが「重要」かどうかは、関連する組織や金融システムの性質による。

[22]FSB (2018), *Cyber Lexicon*, November.

サイバーセキュリティ」という用語は、「サイバー媒体を通じて、情報および／または情報システムの機密性、完全性、可用性を保持すること」と定義されている。さらに、認証性、説明責任、否認防止、信頼性など、その他の特性も含まれる。

いる特性を活用している。障害の種類は、まず、これらの特性の損失、すなわち、可用性の損失、完全性の損失、機密性の損失、及び残りの特性の統合体としての信頼の損失に沿ってグループ化される。破壊のタイプをさらに区別するために、第二レベルの粒度がフォーマットで提供されている。

- **サービス停止時間**：この情報項目には、完全または部分的なサービス停止時間が記録される。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
影響を受けるサービス	インシデントの影響を受けた報告事業体が提供するサービスについて説明する。	コンテナ	**妥当性確認** サービスに影響を与えずにインシデントが発生する可能性がある。
サービス	報告事業体がサービスを識別するために使用する記述的用語	テキスト（短文）	**例**（架空） プッシュ（クレジット）払い
サービスタイプ	1 つ以上の関連スキーマを使用してサービスを分類する方法を提供する。	配列（キーベール）	**構文** • スキーマの名前、選択された列挙]という形式の（1 つ以上の）テキスト（短文）ペアの配列。 **妥当性確認** • ""（空白／スキーマなし）の場合、フリーテキスト可 **例**（架空） • *Schema1, ServiceType1* • *Schema2, ServiceTypeA*
サービス・クリティカル	サービスとみなされる受信事業体のリストをキャプチャする。 報告事業体が判断し、（各取得者の定義に沿って）重要または重要であると判断したもの。	配列（リスト）	**構文** • **取得者識別子の**リストを用いて動的に入力される**。** • 空白のままであれば、サービスはすべての受信事業体レジームに関してノンクリティカルとみなされる。 **例**（架空） • 認可 *X*
サービス停止タイプ	サービス中断の異なるタイプを一貫して分類する方法を提供する。	配列（リスト）	**構文** • テキスト（短文）列挙型の配列で、附属書 F のリストから選択する。 **妥当性確認** • 少なくとも 1 つのタイプが選択されていなければならない **例**（架空） • 稼働率低下：的
サービス停止時間	外部エンドユーザーがサービスを完全にまたは部分的に利用できなくなってから、通常の	期間	**構文** • ヌル値は、ダウンタイムがゼロであるか、または代表者がいないことを表す。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
	活動または業務が回復するまでの期間。(該当する場合)		**例** • *4* 時間は *PT4H* と表される

影響を受ける各サービスに含まれる後続の情報項目は、影響を受ける顧客又は消費者基盤及びトランザクショ ン量（適切な場合）に焦点を当て、インシデントの規模の一貫した表現を提供するために使用される。この情報は、このセクションの最後にある補足的な**サービス／リソース注記**情報項目を用いて定性的に補強することができる。

顧客／消費者ベース

金融セクターの参加者のビジネスモデルの大半は、B2B（企業対企業）または B2C（企業対消費者）の関係を伴う。これらの関係は、（財・サービスの購入者としての）顧客と（財・サービスのエンドユーザーとしての）消費者を区別しているが、本書式では、報告事業体のサービスの「外部エンドユーザー」として、これらの外部当事者を組み合わせている。外部エンドユーザー」の概念には、金融市場インフ ラの参加者など、関連する他の取引相手も含まれる。このフォーマットは、関係するサービスごとに影響を受けるユーザーベースの規模を記述するのではなく、簡略化したアプローチをとっている：

- **影響を受けた外部エンドユーザー数**：インシデントにより影響を受けた直接の顧客または消費者の合計を反映する。
- **影響を受けた外部エンドユーザーの割合**：純粋な数字だけでは規模感がすぐに伝わらないため、影響を受けたユーザーベースが典型的な総ユーザーベースの文脈で考慮されるように、割合の数字も含まれる。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
影響を受けるエンドユーザー	特定のサービスにおいて影響を受けた外部エンドユーザーの数	整数	**妥当性確認** • 値は負であってはならない。 • *50000*
影響を受けたエンドユーザーの割合	特定のサービスのユーザーベースが影響を受ける割合（全体に対する割合	パーセント	**例** *0.25*（*25%*に等しい）

影響を受ける取引

特定のサービスに関連する、影響を受けるトランザクションフローへの影響を報告するために、 報告事業体は、どの情報項目がローカルに実装されたかに応じて、影響を受けるトランザク ションの数、割合、及び／又は金額を示すことができる。場合によっては、ユーザー数ではなく、**トランザクションのパーセンテージを使って**規模感を伝えるのが最良かもしれない。例えば、高度にクリティカルなサービスにはダウンストリームユーザー（例えば別の規制対象取引先）が 1 人しかいないかもしれないが、ユーザーベース指標は 1 人の外部エンドユーザーが影響を受けたことを明らかにするだけであり、単独では特に有益ではない。異なる状況においては、影響を受けた**トランザクション数**または**トランザクション金額に関する**知識もまた、問題の大きさを測るために重要かもしれない。

加えて、**影響を受ける取引の種類は**、ISO 20022 の金融業界共通のメッセージングスキーム[23] に基づき、附属書 G に定義されたビジネスエリアのグルーピングを用いて任意に記録される。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
影響を受けるトランザクション・	ISO20022 のビジネスエリアに沿った、特定のサービスに対して影響を受けるトランザクションの種類	配列（リスト）	**構文** • 列挙されたテキスト（短文）タイプの配列（附属書 G のリストから選択）。 **例** • 支払いと現金管理
対象取引番号	特定のサービスで影響を受けたトランザクション数	整数	**例** *50000*
影響を受けた取引の割合	特定のサービスの典型的な総量に対する、影響を受けたトランザクションの割合。	パーセント	**例** *0.6（60%に等しい）*
影響を受けた取引額	特定のサービスにおいて影響を受けた取引額	10 進数	**例** *1000000*

リソース

リソース」という用語の使用は、オペレーショナル・レジリエンスに関する BCBS の原則で定義されている「支援資産」の概念により合致するよう、FSB サイバー・レキシコン（[24] ）で定義されている「資産」の種類のサブセットであることを意図している。[25]。

インシデントは、リソースの特性が悪影響を受け、それがサポートするサービスの中断につながる場合に発生する。インシデント報告の目的のために、この書式は、影響を受ける**リソースのタイプ**（附属書 H）、およびそれらに関連する**特性**（附属書 I）を捕捉するためのデータ構造を定義することによって、比例的なアプローチをとる。

しかし、影響を受けた個々のリソースの規模や相対的な割合を把握することは、構造化された方法で実施することは非現実的であり、インシデントの真の程度を明らかにするインシデント後のレビューの後にのみ、完全に理解され、関連することができるであろう。その代わりに、影響を受けたサービスまたはリソースに関連する補足情報のための**注釈**情報項目が、フォーマット内に含まれる。受信事業体は、ローカルな実装の一部として、この項目の内容要件に関するガイダンスを発行することができる。

[23]ISO (2013), *ISO 20022 ユニバーサル金融業界メッセージング標準*

[24]FSB (2018).

資産」とは、「人、情報、インフラ、財政、評判を含む、保護する価値のある有形または無形の価値あるもの」と定義されている。

[25]バーゼル銀行監督委員会（2021 年）、オペレーショナル・レジリエンス原則、3 月

支援資産」とは、「重要な業務を遂行するために必要な人、技術、情報、施設」と定義されている。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
影響を受ける資源	インシデントによって全体として影響を受けたリソースを記述する。	コンテナ	
リソース	インシデントによって影響を受ける、基本的なリソースのタイプを記述する。	列挙	**構文** • テキスト（短い）列挙リスト。附属書 H から 1 つ選択する。 • テクノロジー*ICT* ハードウェア
資源の影響を受ける物件	影響を受ける各資源の関連特性が、どのように影響を受けたかを記述する。	配列（リスト）	**構文** • 附属書 I の列挙から選択されたテキスト（短文）タイプのエントリーの配列。 • 室状況
サービス／リソースノート	影響を受けるサービスおよび/またはリソースについて、より広範な説明を提供する。	テキスト（長文）	**例（**架空） 決済処理システムに関連する修復不可能なネットワークカードハードウェアの故障により、ネットワークトラフィックの断続的な再ルーティングが発生し、顧客向け取引承認サービスに下流の影響が出た。

3.4. 影響

影響のアセスメントは、短期（1 日以内）から長期（数カ月、数年）にわたる複数の時間軸でインシデントの影響を評価する必要があり、自明な作業ではない。定量的アプローチは、一般に、個々の金融機関がインシデント対応の一環として使用するための正確でタイムリーなデータを最初に定義し、入手することがより困難である。そのため、この書式では、あらゆる種類の報告事業体に対してより容易に適用できる定性的な影響を評価するアプローチを採用している。

この判断に基づく方法は、記述的な記述を使用して、様々な影響カテゴリーにわたって、深刻度が増すレベルを定義するものである。インシデントが発生するまでの間、報告事業体はこれらの定性的尺度に照らした評価を定期的に行い、影響の概算を行い、適切な組織的対応を推進する。しかし、このアプローチは、個人の一貫した解釈と判断に依存するため、バイアスや主観が入る可能性がある。

したがって、報告事業体または受入事業体のいずれかによって定義された既存のレベルに取って代わ ることを意図しているわけではないが、正規化された一連の影響尺度を使用することが必要である。その代わりに、この尺度は、インシデント間の影響の比較可能性を可能にする共通の仲介形式を提供する。アセスメントされる影響カテゴリーのうち 3 つは、報告事業体が経験する影響という文脈で、4 つ目のカテゴリー（外部）は、金融システムやより広範な経済への影響を反映しようとするものである。外部への影響は、報告事業体がインシデントの下流への影響について判断する能力に基づいて正確に評価することがより困難である可能性があるが、正規化された尺度はその大きさを概算する手段を提供する。追加的な記述の詳細は、セクションの最後にある**影響に関する注記**情報項目を通じてプロバイダが提供することもできる。

4 つの影響カテゴリーはすべて、報告事業体によって 5 段階のリッカート尺度（影響がないことを示す「なし」の選択肢も追加）でアセスメントされ、現在観察されている影響レベルを記録する：

- **財務**：罰金、違約金、逸失利益、市場シェア低下による財務的損失

- **運用**：サービスレベルの中断または低下、ワークフローの混乱、サプライチェーンの混乱
- **風評被害**：否定的な意見やブランドへのダメージ
- **外部**：前の 4 つの尺度が内部への影響を表すのに対し、外部への影響はインシデントが生態系の他の部分に及ぼす影響を反映する。

さらに、財務上の影響の大きさを表現するための補足情報として、**財務上の影響損失**では、インシデントに関連する総損失またはコストの見積もり定量化を金銭的に含めるオプションが提供される。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、、データ例
財務上の損失に影響する	インシデントに起因する直接的、間接的な総費用および 損失の総額	10 進数	**構文** • FIRE の報告通貨で設定された額面で、財務上の損失を表現するために使用される。 **例** • *250000*
影響ファイナンシャル	報告事業体が経験している現在の財務的影響について説明する。	列挙	**構文** テキスト（短い）列挙リスト。附属書 J に記述されている値から選択する。
影響	報告事業体が経験した業務上の影響を説明する。	列挙	**構文** テキスト（短い）列挙リスト。附属書 K に記述されている値から選択する。
風評への影響	報告事業体が経験した評判への影響について記述する。	列挙	**構文** テキスト（短い）列挙リスト。附属書 L に記載されている値から選択する。
外部への影響	インシデントが外部に及ぼした影響について説明する。 エコシステム	列挙	**構文** テキスト（短い）列挙リスト。附属書 M に記述されている値から選択する。

地理的な広がり

フォーマット内に含まれる 5 つ目の影響指標は、インシデントによって影響を受けるすべての当事者を包含する**地理的広がりに**基づくものである。このフォーマットにおける影響の広がりは、5 段階の地理的スケールで正規化されている：

- **地元**：影響を受ける当事者が同じ都市中心部に住んでいる。
- **地域的**：影響を受けるのは、管轄区域内のディビジョン（郡など）の一部に限られる。
- **国内**：影響を受ける当事者が単一の管轄区域全体で特定されている。
- **複数の管轄区域**：影響を受ける当事者は複数の管轄区域にまたがる。
- **グローバル**：影響を受ける当事者は、複数の大陸にまたがる大半の司法管轄区に存在する。

国または複数管轄のオプションが選択されている場合、インシデントの影響が発生した管轄区域を、ISO 国コード標準を使用して「影響地理的国」フィールドに報告することができる。

各選択肢には、特定のロケールや地域を説明するための追加情報をプロバイダとして提供することができる。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
地理的広がりに影響を与える	インシデントの影響がどの程度経験されているかを、地理的スケールの拡大を通して記述する。	列挙	**構文** • テキスト（短い）列挙リスト。以下の値から選択する： o ローカル o リージョナル o ナショナル o 複数管轄 o グローバル **例** • 地域
影響を与える地理的な国々	インシデントの影響が発生している 1 つ以上の管轄区域を記述する（拡散が全国的または複数の管轄区域に及ぶ場合にのみ適用される）。	配列（リスト）	**構文** • ISO 国コードから生成された、テキスト（短い）列挙リストの配列。 **妥当性確認** • この値は、ISO 3166 alpha-2 エンコーディングを使用した国コードのリストに準拠する。 • "national "スプレッド "が選択された場合は 1 つの値のみが期待され、"multi "jurisdictional "が選択された場合は複数の値が期待される（情報項目が実施される報告事業体および／または受信事業体のみが実施可能）。 **例** • *[GB]* • *[es、de、fr、it]*。
影響ノート	影響のより広範な説明を提供する。	テキスト（長文）	**例** このインシデントはメディアで大きく取り上げられ、ソーシャルメディアのチャンネルを通じて否定的な顧客感情を抱いた。

4. インシデントのクローズ

インシデントがクローズし、インシデント後のレビューが実施された時点で、金融機関主導の報告に関連する 4 つ目の情報項目と最後の情報項目が確認される。したがって、これらの情報要件は主に最終報告書の内容に関するものであるが、インシデントの初期段階であっても、特定の要素が疑われたり、知られていたりする場合がある。重要な要素は 3 つある：

- これは、インシデントがなぜ起こったのか、誰が、あるいは何がその原因を作ったのかを説明するものである；
- **識別された教訓と改善活動**（脆弱性とそれに対処するための行動を詳述する）。
- ファイルベースの補足資料を含めることができるようにする。

4.1. 原因

インシデント対応段階では、事態を収束させ、サービス提供を許容レベルまで回復させることに主眼が置かれる。したがって、インシデント発生後のレビューまで、因果関係の詳細な分析は通常行われない。しかし、報告事業体は、その対応の一環として、インシデントの原因について十分な理解を深めている可能性があり、したがって、インシデントがまだ進行中である間に、受信事業体に早期の洞察を提供できる可能性がある。

オペレーショナル・リスクの領域内で想定される原因の列挙を容易にするため、**図 10 に**示すように、BCBS の「オペレーショナル・リスク」の定義（[26]）に沿うような 2 層構造を採用している。レベル 2 では、さらに 27 の根本的な原因が附属書 N に記載されており、報告事業体が選択するにも、その後の原因分析を支援するにも、妥当なレベルの粒度を提供している。レベル 2 の原因項目は、多くの信頼できる情報源（例：UNDRR、SEI、米海軍[27]）から引用されているが、原因の選択を簡素化するために大幅に統合されている。報告事業体がインシデントの原因を反映する適切なレベル 2 の原因を特定できない場合、報告事業体は（「その他」の使用を避けるために）それ以上の特定をせずにレベル 1 の原因ファミリーを使用することができる。

図 10：「オペレーショナル・リスク」の定義とレベル 1 の原因タイプの整合性

可能性のある各原因に対して、報告事業体は、識別された各原因に関連する因果関係の強さを示すことができる：

- **ルート**：インシデントにつながったに違いない
- **寄与的**：他の過失と組み合わさった場合にのみ、インシデントにつながる可能性がある。

[26]バーゼル銀行監督委員会（2004）『バーゼルⅡ：資本測定と資本国際的収斂：改訂された枠組み』6 月。

[27]以下のような情報源から得たものである：国連災害リスク軽減事務所(UNDRR)、災害リスクのための仙台枠組みを含む。削減；ソフトウェア工学金融機関（SEI）（2014）『運用上のサイバーセキュリティリスクの分類法（*A Taxonomy of Operational Cyber Security Risks Version 2*）』；米海軍 *HFACS（Human Factors Analysis and Classification System）*枠組み；

因果関係を把握することに加えて、このフォーマットには、インシデントを引き起こした当事者または勢力（本書では「発生源」と呼ぶ）の身元を記録するための要素も含まれている。起源」という用語の使用は、脅威アクター（[28]）の概念よりも範囲が広く、「悪意を持って活動していると思われる個人、グループ、組織」を表し、意図を持っていない当事者、例えば不可抗力も含まれる。

- **発生源：**報告事業体におけるインシデントにつながる発生源の種類に関するその後の分析を支援するための 2 段階の分類スキーム。カテゴリーレベルでは、原産地は 3 つのグループに分けられ、タイプは附属書 O でさらに詳しく説明されている
  - **内部**：報告事業体が雇用または契約している組織資源または関連事業体（通常は個人）であり、当該事業体内の脅威源を表す。
  - **サードパーティ**：報告企業と既存の関係を有する事業体
  - **外部：**[29] 事業体は報告企業と既存の関係を持たない。
- **発生源アイデンティティ**：オリジンを指定するオプションの属性で、フリーテキスト・フィールドとしてプロバイダから提供される。適切な場合、報告事業体は、既知のエンティティへの一貫した参照を維持するために、認 識された脅威アクタープロファイルリポジトリを活用することができる。

原因に関するメモのための追加情報項目は、原因または関連する起源の性質のより広範な記述をサポートするために含まれている。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
識別された原因	インシデントにつながった、または寄与したすべての原因を把握する。	コンテナ	**妥当性確認** 少なくとも 1 つの原因が因果的強度を持たなければならない。 ルート
原因	ハザード、人的要因、情報システムおよびプロセスの障害、外部依存の障害、悪意ある行為に及ぶ原因の分類	列挙	**構文** • テキスト（短い）列挙リスト。附属書 N の値から選択する。 • 悪意ある行為 - ランサムウェア
因果強度	識別された原因がインシデントにどの程度寄与したかを記述する。	列挙	**構文** • テキスト（短い）列挙リスト。以下の値から選択する o ルート o 未拠出 •
起源	インシデントを引き起こした、あるいはインシデントの一因となった、誰の、あるいはどのような	列挙	**構文** • テキスト（短い）列挙リスト。附属書 O の値から選択する。

[28]FSB（2018）、脅威アクターの定義）。

[29]ベライゾン（2019 年）、外部アクターの多様性。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
	行為かについて、高いレベルで分類する。		• アウトソーシング・サービス・プロバイダ
発生源アイデンティティ	主にサードパーティまたは外部の出所について説明することを目的とした、各出所の疑いのある名称または識別子（判明している場合）。	配列（キー値）	**構文** • 1 つ以上の）テキスト（短文）ペアの配列。 [識別子の名前、識別子の値]。 **妥当性確認** • LEI識別子を使用する場合は、ISO17442-1:2020 に沿った妥当性確認ルールを実施する。 • もし""（空白／識別子がない）なら、フリーテキストが許される。 **例**（架空） • *HAL*
注意事項	原因および/または起源について、より広範な説明を提供する。	テキスト（長文）	**例(架空)** 原因の詳細

4.2. レッスン

根本原因分析に続き、インシデント後のレビューでは、報告事業体が対策を講じるべき 1 つ以上の教訓を特定することが期待される。インシデント後のレビューの成果として、より一般的に使用される「教訓」ではなく、「識別された教訓」が使用されていることに留意されたい。識別された教訓は、その後、実施または適用され、教訓とみなされる前に金融機関内に定着する必要がある。識別された教訓の細かさについては、各地域の実施者が判断することであるが、改善と再発防止に焦点を当て、改善活動を追跡するために使用される詳細レベルに匹敵するものでなければならない。

この形式では、識別されたレッスンは 2 つの部分で構成されている：

- **教訓の記述**：インシデント後のレビューから得られた個々の所見を記述する。
- ISO8601:2019 のフォーマット（YYYY-MM-DD）を用いて日付を表現する。

これらの情報項目の組み合わせは、報告事業体と受領事業体の双方に、進捗状況を監視し、その後、原因が適切に対処されたかどうかを評価するために必要な改善計画情報を提供する。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
識別レッスン	報告事業体の事故後のレビューから特定された（「学んだ」ではない）各教訓を記録する。	コンテナ	
レッスン	事故後のレビューから得られた個々の所見について説明する。	テキスト（長文）	**例** インシデントから識別された教訓 *1*

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
改善措置	指摘事項に対処するために報告事業体が実施している 1 つ以上の措置と、各措置の改善完了予定日を記載する。	配列（キー値）	**構文** • 日付, テキスト（Long）]形式の（1 つ以上の）ペアの配列。 • 日付は ISO 8601 形式を使用する：YYYY-MM-DD **妥当性確認** • 日付スタンプは省略可能で、未来でも過去でもよい（例えば、最終報告書が発行される頃には完了している可能性がある）。 • *2024-09-13*、レッスン *1* にリンクした行動 *1* の説明 • *2025-03-22*、アクション *2* にリンクした説明 課

4.3. 補足文書

すべての情報が構造化されたテキストベースの情報項目で把握できるわけではないので、このフォーマットには、インシデント報告の一部としてファイルベースの資料を組み込むための金融機関が含まれている。主にインシデント発生後のレビューに関連する詳細情報をサポートするためであるが、インシデントのライフサイクルの他の時点で、受信事業体が追加コンテンツを提出することを望むことも考えられる。

このプロセスを可能にするために、この書式は、FIRE メッセージ自体の中、あるいは補完的なプロセスとして、以下の情報項目を使用した補足情報の交換のための様々な方法をサポートする：

- **添付方法**：補足情報を交換するために報告事業体が選択した方法

  embedded(埋め込み): メッセージに含まれる添付ファイル

  電子メール：FIRE メッセージとは別に電子メールで受信事業体に伝達される添付ファイル

  ファイル転送：FIRE メッセージとは別に、ファイル転送（FTP/SFTP など）により受信 事業体に伝達される添付ファイル。

  外部でホストされる：受信事業体が、指定された場所から個別にダウンロードできるようにした添付ファイル。添付ファイルの参照は、、ホスティング場所（URL など）、関連するアクセス認証情報の場所、およびファイル名の参照を指定するために使用される。

- **添付ファイルの説明**：各添付ファイルと、選択した方法で非埋め込みファイルをどのように取得/アクセスできるかを説明する、構造化されていない長いテキストフィールド

- **添付ファイル埋め込み(attachment embedded)**: 受信事業体との間で交換される FIRE メッセージ内への添付ファイルのアップロードと包含をサポートするために使用される、Base64 バイナリエンコードされたファイルの配列。

情報項目	目的 / 内容	フィールドタイプ	追加の構文と妥当性確認ルール、およびデータの例
アタッチメント方式	インシデントに関する補足情報を提供するために採用された方法を説明する。	列挙	**構文** • テキスト（短い）列挙リスト。以下の値から選択する： ○ 埋め込まれた ○ 電子メール ○ ファイル転送 ○ 外部ホスト **例** • 埋め込まれた
添付文書	のファイル名と追加の検索方法を説明する。 添付ファイルの非エンベデッド交換	テキスト（長文）	**例** 添付ファイルは、以下の *E* メールの詳細とともに、すべてのレポート取得者にコミュニケーションされる ***From**: contact@reporting-entity.com* タイトルインシデント報告 *ID123456789* **添付**ファイルファイル *1.pdf*、ファイル *2.pdf*、ファイル *3.pdf*
添付ファイル埋め込み	オーダーメイドの書類をアップロードすることで、詳細を追加できるオプションを提供する。	配列（リスト）	**構文** • Base64 エンコーディングで格納された、Attachment 型の 1 つ以上のファイルの配列。 **妥当性確認** • 最大ファイルサイズを考慮する必要があるかもしれないが、この制約は個々のローカルな実装にリンクされるだろう。 **例** • 一般的に使用されているファイル形式（*DOC*、*PDF*、*PPT* など）をエンコードして表現する。

附属書 A：標準化されたフィールドタイプ

フィールド	タイプ	説明	制限／形式	例
配列（キー・バリュー）	リスト	キーと値のペアのリスト		[("整数", "テキスト（短文）")]。
配列（リスト）	リスト	複数の要素を特定の順序で並べたリスト。		["Enum1","Enum2","Enum3"]
アタッチメント	バイナリ	バイナリ・エンコードされたファイルを Base64（または同等のもの）に変換する。		
ブーリアン	ブーリアン	真または偽の値	0（偽）、1（真）	1
コンテナ	コンテナ	関連する 1 つまたは複数のフィールドのコレクション 目的		
日付	日時	ISO 8601 フォーマットによる日付	YYYY-MM-DD	2023-12-12
日付	日時	ISO 8601 形式を使用した日付と時刻の組み合わせ	YYYY-MM DDTHH:mm:	2024-01-25T14:17+00:00
10 進数	数値	ISO/IEC に準拠した、分数を含む数値のための数値データ型。 60559:2020	binary32 形式	7.04
期間	日時	を使った時間間隔である。 ISO 8601 フォーマット	P[n]Y[n]M[n]DT[n]H[n]M	PT3H15M
列挙	ストリング	小さなセットから単一の値を選択する 事前に定義された固有の値 (要素または列挙子）で、文字列ベースである。	リストからの単一選択	列挙 1
整数	数値	分数を含まない数値を表す数値データ型	符号付きロング（32 ビット）フォーマット	13
パーセント	数値	値が限定された 10 進数（0 から 1 を含む）	>=と<=1	0.46
テキスト（E メール）	ストリング	に準拠した文字列である。 RFC5322 フォーマット	ローカルパート "@" ドメイン	john.smith@email.com
テキスト（ロング）	ストリング	段落の長いテキストフィールド。 UTF-8 エンコーディング	65,535 文字	複数の段落...
テキスト（短文）	ストリング	UTF-8 エンコーディングのタイトルと名前用の短いテキスト・フィールド	255 文字、改行なし	短い文章

フィールド	タイプ	説明	制限／形式	例
テキスト（電話）	ストリング	E.164 標準に準拠した文字列：+[国番号][加入者番号] 最大 15 番号	正規表現：/^¥+[1-9]¥d14$/	+14151234567

附属書 B：機関主導の報告における報告段階の選択性

情報項目名	**イニシャル**（オープン）	**初期**（解決済み） **中級**（オープン） **中級**（解決済み）	**イニシャル**（クローズ） **最終**（解決済み） **最終**（クローズ）
メッセージ・			
FIRE バージョン	必須	必須	必須
FIRE レポートタイプ	必須	必須	必須
FIRE レポート言語コード	必須	必須	必須
FIRE レポート言語 国	必須	必須	必須
FIRE レポート言語のカスタマイズ	オプション	オプション	オプション
FIRE レポート通貨	必須	必須	必須
報告			
報告事業体			
事業体名	必須	必須	必須
グローバル識別子	オプション	オプション	オプション
ローカル識別子（複数可）	オプション	オプション	オプション
最終親名	オプション	オプション	オプション
事業体タイプ	必須	必須	必須
事業体 国	オプション	オプション	オプション
受信事業体			
取得者識別子	必須	必須	必須
取得者履歴	オプション	オプション	オプション
転送元	該当なし	該当なし	該当なし
転送先取得者	該当なし	該当なし	該当なし
連絡			

情報項目名	イニシャル（オープン）	初期（解決済み） 中級（オープン） 中級（解決済み）	イニシャル（クローズ） 最終（解決済み） 最終（クローズ）
事業体の連絡先	必須（1 つ以上）	必須（1 つ以上）	必須（1 つ以上）
コンタクトタイプ	必須	必須	必須
連絡先	必須	必須	必須
連絡先メールアドレス	必須	必須	必須
連絡先電話番号	必須	必須	必須
連絡役	オプション	オプション	オプション
連絡先	オプション	オプション	オプション
連絡先取得者	オプション	オプション	オプション
インシデント詳細			
文献			
事業体内インシデント ID	オプション	オプション	オプション
事業体関連インシデント ID（複数可）	オプション	オプション	オプション
インシデント			
報告段階	必須	必須	必須
インシデントステータス	必須	必須	必須
インシデントタイトル	必須	必須	必須
インシデント記述	必須	必須	必須
インシデント・タイプ	オプション	必須	必須
インシデント痕跡	オプション	オプション	オプション
インシデント・ディスカバリー方式	オプション	必須	必須
インシデント報告トリガー	オプション	必須	必須
インシデントの解決予定期間	オプション	オプション	該当なし
前回変更点			
行動	オプション	必須	必須
行動計画	オプション	必須	該当なし
世間の反応	オプション	オプション	必須

情報項目名	イニシャル（オープン）	初期（解決済み） 中級（オープン） 中級（解決済み）	イニシャル（クローズ） 最終（解決済み） 最終（クローズ）
通信発行	オプション	オプション	必須
被認定団体	オプション	オプション	必須
日付／時刻			
報告時期	必須	必須	必須
発生時期	オプション	オプション	オプション
検知時刻	オプション	オプション	必須
解決時期	該当なし	必須	必須
閉店時間	該当なし	該当なし	必須
次回更新時期	オプション	オプション	該当なし
影響アセスメント			
深刻度			
事業体の重大性	オプション	オプション	オプション
標準重症度	必須	必須	必須
関係			
当事者タイプ	オプション	オプション	必須
関連事業体	オプション	オプション	必須
特記事項	オプション	オプション	オプション
サービスと			
影響を受けるサービス	オプション	必須	必須
サービス名	オプション	必須	必須
サービスタイプ	オプション	必須	必須
サービス・クリティカル	オプション	オプション	オプション
サービス停止タイプ	オプション	必須	必須
サービス停止時間	オプション	必須	必須

情報項目名	イニシャル（オープン）	初期（解決済み） 中級（オープン） 中級（解決済み）	イニシャル（クローズ） 最終（解決済み） 最終（クローズ）
影響を受けるエンドユーザー番号	オプション	必須	必須
影響を受けたエンドユーザーの割合	オプション	必須	必須
影響を受けるトランザクション・タイプ	オプション	オプション	オプション
対象取引番号	オプション	オプション	オプション
影響を受けた取引の割合	オプション	オプション	オプション
影響を受けた取引額	オプション	オプション	オプション
影響を受ける資源	オプション	オプション	必須
リソースタイプ	オプション	オプション	必須
資源の影響を受ける物件	オプション	オプション	必須
サービス／リソースノート	オプション	オプション	オプション
財務上の損失に影響する	オプション	オプション	オプション
影響ファイナンシャル	オプション	オプション	オプション
影響	オプション	オプション	オプション
風評への影響	オプション	オプション	オプション
外部への影響	オプション	オプション	オプション
地理的広がりに影響を与える	オプション	必須	必須
影響を与える地理的な国々	オプション	オプション	オプション
影響ノート	オプション	オプション	オプション
インシデントクローズ			
識別された原因	オプション	オプション	必須
原因タイプ	オプション	オプション	必須

情報項目名	イニシャル（オープン）	初期（解決済み） 中級（オープン） 中級（解決済み）	イニシャル（クローズ） 最終（解決済み） 最終（クローズ）
因果強度	オプション	オプション	オプション
起源	オプション	オプション	必須
オリジン・アイデンティティ	オプション	オプション	オプション
注意事項	オプション	オプション	オプション
識別レッスン	該当なし	該当なし	必須
レッスン内容	該当なし	該当なし	必須
改善措置	該当なし	該当なし	必須
補足			
アタッチメント方式	オプション	オプション	オプション
添付文書	オプション	オプション	オプション
添付ファイル埋め込み	オプション	オプション	オプション

附属書 C：インシデントの種類

インシデント・タイプ	定義	例
事業の中断、システムまたは実行の失敗	事業体の活動、機能またはサービスの提供を妨害する、あらゆる種類の業務上のインシデント。	技術障害、第三者サービスの損失、サービス拒否（DoS）、マルウェア、自然災害
侵害 （非破壊的）	(非破壊的）情報システムのセキュリティ侵害	アカウント侵害、侵入、改ざん、リソースハイジャック
データ漏洩	偶発的または違法な破壊、紛失、改ざん、不正な開示、あるいは送信、保存、あるいはその他の方法で処理されたデータへのアクセスにつながるセキュリティの侵害。	データ漏洩、データ損失、データ操作
金融窃盗／詐欺	不正な金銭的利益を得るための故意の行為	デジタル・チャネルを通じた資金の窃盗
情報障害	悪意の有無にかかわらず、虚偽または現実に基づいた情報を広めること。	誤情報、偽情報、悪情報

*FSB サイバー・レキシコンの定義

附属書 D：インシデント発見の方法

ディスカバリー・メソッド		説明
外部	俳優の情報開示	脅威アクターから発表/通知される
	認可／作成機関	金融規制当局、サイバーセキュリ ティ作成機関などの（国家）所轄庁から報告される。
	法執行機関	国内または国際的な法執行機関（LEA）（警察、国家犯罪捜査機関、インターポールなど）から報告された。
	サードパーティ	報告事業体の外部依存関係（マネージドサービス・プロバイダー、ベンダーなど）のいずれかによって報告された
	顧客	報告事業体のサービスの消費者（複数可）により報告されたもの。
	競合他社	他の規制対象事業体から報告された（例：共同情報共有プラットフォーム経由）。
	外部監査	外部監査人（例：ペリメーター・スキャン・サービス・プロバイダ）によるレビュー後に発見された。
	モニタリング・サービス	外部の監視プロバイダ（例：セキュリティ・イベント監視サービス）から報告される。
	非関連当事者	報告事業体とは無関係の者からの報告 例：バグの賞金稼ぎ
	不明	匿名または身元不明の外部事業体からの報告
内部	インシデント対応	別のインシデント対応中に発見された。
	セキュリティ・オペレーションセンター	セキュリティ専門機能が、通常業務の一環として発見した。
	既存の検知技術	既存の監視ツール（侵入検知、ログ監視など）を使用して検知する。
	内部監査	内部監査人によるレビュー後に発見された
	スタッフ	報告事業体の契約スタッフによって報告される
	不明	匿名または正体不明の事業体による報告
不明		情報源不明
		(インシデントの説明に含める）。

附属書 E：標準化された重症度

重大度レベル説明と段階的変更の移行ステートメントを含む）		**その他の状況**（観察されるかもしれない）
なし	いかなる形のインシデント対応も必要としない	
▼インシデント対応は、通常業務の一環として管理される。		
ごくわずか	局所的なインシデントは、特注の介入を必要とすることなく、標準業務手順に沿ってハンドリングされている。	- インシデントが発生した場合、特別な対応や補足的なリソースを必要とせず、確立された手順でハンドリングされる。
▼インシデントを管理するために必要な具体的かつ協調的な対応		
低い	関連する機能ユニット内でインシデント対応モードをエスカレートさせる	- 影響を受ける機能部門（オペレーション／テクノロジー／SOC など）内でエスカレーションを行えば、十分な対応が可能である。 - 指名されたインシデントコーディネーターまたはインシデント対応チーム（IRT）を指名することができる。 - 危機のエスカレーション手順が発動されていない
▼危機管理体制の		
ミディアム	危機管理体制が発動される	- 組織として協調した対応の必要性 - 絶え間ない社内コミュニケーションの流れ - 危機コミュニケーション戦略の活性化
▼最高幹部レベルへの危機のエスカレーション		
高い	インシデントのハンドリングと結果について最終的な責任を負う、最も上級の危機指揮組織にエスカレーションされる。	- 戦略的な危機対応は、被害を受けた事業体内の最上位の指揮系統が主導する。 - 影響を受ける事業体の安全性と健全性に対する重大な脅威
▼危機管理は集団の責任となる		
エクストリーム	インシデントは、影響を受ける事業体の存続またはセクターの秩序ある機能が危機に瀕している場合、最大限の厳しさで扱われる。	- セクター別の危機対応取り決めが発動された - 影響を受ける事業体の安全性と健全性に対する現実的かつ差し迫ったリスク

附属書 F：サービス中断の種類

サービス中断の		**説明**
可用性損失	合計	サービスが外部のエンドユーザーからまったく利用できない。

	部分的	サービスの機能／コンポーネントのサブセットが、外部のエンドユーザーから利用できない。
	断続的	サービスが定期的または不定期に（全体的または部分的に）利用できなくなることがある。
	劣化	サービスが事前に定義された許容サービスレベルを下回っている
完全性の喪失	マニピュレーション	サービスに関連する情報の作成、追加、重複、変更、順序の入れ替えまたは削除
	汚職	サービスに関する情報は読めないが、復元可能、または再構成可能である。
	破壊	サービスに関連する情報が取り返しのつかない形で失われた
守秘義務喪失	意図しない／許可されていない開示	情報へのアクセスを許可されていない事業体に情報がエクスポージャーされる（例：データ漏洩）。
	不正取得	妥当性確認なしに情報へのアクセスおよび/または情報を取得する（例：データ流出、傍受）。
信頼の喪失	なりすまし	サービス ID が、権限のない事業体によって想定または模倣される（クローン ID、マン・イン・ザ・ミドルなど）。
	偽情報	聴衆を誤解させ、混乱させ、操ることを最終目的として、意図的に虚偽の情報を流布すること。
	噂 憶測	情報の信憑性を確認せずに拡散する
不明		サービス中断の内容についてはまだ確認されていない
その他		サービス中断のタイプが事前に定義されたカテゴリーと一致しない

附属書 G：ISO 20022 事業分野 [30]

ビジネスエリア（BA）グループ	ISO 20022 における事業分野
カード決済と関連取引	アクセプタからアクワイアラーへのカード取引、アクワイアラーから発行者へのカード取引、セールから POI へのカード取引、ATM カード取引、カード管理、POI 管理、ATM 管理、手数料徴収、ペイメントトークン管理、ネットワーク管理、ファイル管理、決済報告、不正報告、処分
支払いと現金管理	支払開始、支払決済、キャッシュ・マネジメント、支払送金通知
貿易サービス	貿易サービス開始、貿易サービス、貿易サービス管理
証券	証券発行、証券取引開始、証券取引、証券清算、証券決済、証券管理、証券イベント
外国為替	外国為替取引の開始、外国為替取引、外国為替管理
銀行ローン/預金	銀行ローン取引開始、銀行ローン取引、銀行ローン管理
デリバティブ	デリバティブ取引開始, デリバティブ取引, デリバティブ管理
商品	商品取引開始、商品取引、商品管理
シンジケート・ローン	シンジケート・ローン開始、シンジケート・ローン、シンジケート・ローン管理
雑多な/一般的な	口座管理、認可、担保、参照データ
該当なし	影響を受けるサービスに関連するトランザクションタイプがない
その他	ISO20022 でカバーされていないその他の取引タイプ

[30] ISO（2017）、*ISO 20022 事業分野*（該当しない、その他の種類で補強）。

附属書 H：資源の種類

リソース		説明／例非網羅的）
人々		従業員（およびそれに関連する技能、才能または能力）
プロパティ		建物、設備、機械、車両、土地、オフィススペース、事務機器、備品
テクノロジー	ICT（情報通信技術）ハードウェア	ストレージ機器、サーバー、メインフレーム、バックアップ設備、デスクトップ機器、ネットワーク機器、コミュニケーション、音声サービス
	OT（オペレーション・テクノロジー）ハードウェア	ビル管理制御システム、SCADA システム、産業制御システム（ICS）、分散制御システム、侵入検知システム、物理アクセス制御システム、緊急事態管理システム
	ソフトウェア	オペレーティングシステム（仮想を含む）、アプリケーション（内部開発またはサードパーティ開発）、ミドルウェアコンポーネント、ウェブコンポーネント
インフォメーション	データストア	永続的かつ構造化された情報のリポジトリ（RDBMS、キー／バリューストア、ドキュメントストアなど）
	ファイルベースのデータ	情報を電子的または物理的に保存する
	コード	自社開発
	サードパーティ・ライブラリ	報告事業体が使用している購入済みまたはオープンソースのライブラリ
	アーカイブ情報	長期保存のためにリポジトリ内に保持されるデータの収集

附属書 I：資源特性 [31]

	説明
空室状況	認可された事業体が要求に応じてアクセスでき、使用できること。
誠実さ	正確性と完全性
守秘義務	許可されていない個人、事業体、プロセス、またはシステムに情報が提供されたり、開示されたりしないようにする。
認証	事業体がそのように主張するものであるという性質
説明責任	ある事業体の行動が、その事業体に固有に追跡できることを保証するプロパティである。
否認防止	主張された出来事または行為の発生とその発生源となった事業体を証明する能力
信頼性	意図した行動と結果が一貫している

[31] FSB (2018).サイバーセキュリティの定義より

附属書 J：財務的影響尺度

影響レベル説明とステップ変更の推移を含む）		**その他の状況**（観察されるかもしれない）
なし	財務上の影響は見られない	
▼財務上の影響が見られた、または予想された		
重要ではない	重要でない財務上の損失を計上	- 既存の予算内で吸収できる最小限の費用で済む場合もある。
▼損失が、影響を受ける事業ラインの典型的な営業パラメーターを超えて拡大する。		
マイナー	インシデントに関連する直接的または間接的な費用から生じる経済的損失は限定的である。	- 事業体全体のオペレーショナル・リスク損失引当金で財務的影響を吸収できる - 事業体全体の収益性を損なうものではない
▼損失は組織的な懸念となり、利用可能な資金源に影響を及ぼす。		
中程度	財務上の懸念はあるが、吸収可能である。	- 事業体の収益性にマイナスの影響を与える - 損失はコスト削減策で抑えることができる - 流動性の妥当性および／または資本ポジションが悪化している
▼事業体はもはや拡大する損失を吸収することはできない。		
相当なものだ	事業体が経営難に陥り、流動性リスクやもはや吸収できない損失へのエクスポージャーが増大している。	- 事業体が流動性要件を満たすために外部（中央銀行など）からの資金調達を利用したり、ビジネスモデルに重大な調整を加えたりするリスクが高まる - 復旧計画が失敗した場合、資本要件に抵触する可能性がある。
▼事業体が外部からの介入なしに十分な機能を果たせなくなった。		
厳しい	事業体が**財政難または債務超過に**陥り、その債務を履行または弁済することができない。	• 事業体が存続不可能になりかけている（懸念がなくなった） • 1 つまたは複数の当局が認可を取り消し、および／または破綻処理、清算、倒産が引き起こされる可能性が差し迫っている。

附属書 K：事業影響尺度

影響レベル説明とステップ変更の推移を含む）		**その他の状況**（観察されるかもしれない）
なし	操業への影響は見られない	
▼観測された、または予想される業務上の影響		
ではない	重要でないサービスや資源の提供や保護が低下する	- 事業体の既存の復旧手段を用いて管理される基礎的資源への混乱 - 永続的な影響のない情報の漏洩
▼致命的でない故障		
マイナー	重要でないサービスまたはリソースの障害または結果的な危殆化、あるいは重要なサービスまたはリソースの提供の限定的な低下	- 重要でないサービスやリソースが影響を受ける - 重要なサービスの提供および/または資源の利用可能性の悪化は限定的である。 - 情報漏洩の影響は限定的である
▼重要なサービスやリソースの中断		
中程度	1 つまたは複数の重要なサービスまたは資源の提供または保護に悪影響が及ぶ	- 重要なサービスの提供および／または資源の利用可能性の悪化 - 影響を受ける資源の割合から見て、大規模な影響はない - 情報の漏洩は、機密性や情報量の点で顕著な影響を及ぼす。
▼実質的に耐えられない機能障害		
相当なものだ	重要なサービスやリソースが影響を受け、主要な事業目標が達成されない	重要なサービスに対する許容可能な中断レベルが破られた。 - 復旧は可能だが、不確実性、複雑性、労力がある。 - 影響を受ける資源の割合から見て大規模な影響 - 情報の漏洩が、機密性や量の点で広範囲に及ぶ。
▼中核となる事業機能をオペレーションできなくなった。		
	事業体が**その使命を達成することを**妨げる、持続的な事業上の影響	• 事業体のオペレーションを妨げるような重要なサービスやリソースの取消不能な喪失（オペレーション麻痺など）。 • すべての回復オプションを使い果たした

附属書 L：風評影響尺度

影響レベル説明とステップ変更の推移を含む）		**その他の状況**（観察されるかもしれない）
なし	評判への影響はない　観察される	
▼インシデントに関連した副作用が識別される		

重要ではない	少数の社外関係者から批判／否定的な反応を受けた孤立した事例がある。	- 限定的または局地的なネガティブ報道、顧客の不満・苦情 - 報道エクスポージャーなし - 評判／イメージに特筆すべき影響はない - 事業体の標準コミュニケーション・プロトコルまたは苦情処理プロセスで処理できる。
▼ネガティブな勢いが強まり、地元の主流報道へと広がっている。		
マイナー	複数の地域で、外部からの批判／否定的な反応があった。	- 地元メディアによる一時的な報道 - 地元世論の認識 - ソーシャルメディアのトレンド - 短期的だが回復可能な軽微な評判への影響 - インシデントに対して影響を受けた事業体が発行した特定のコミュニケーション - 顧客からの苦情はほとんどない
▼国益や公的批判を引き起こす懸念の高まり		
中程度	利害関係者の信頼悪化を反映した、社会、金融機関、または市場の懸念の高まり	- 事業体の主な活動地域内において、地元または全国規模のメディアによる報道が拡大する。 - 中程度のエンゲージメントと知名度を持つソーシャルメディア・トレンド - 代表者（政治家や認可者など）からの否定的なコメントや関心 - コア顧客からの信頼は失われていないが、顧客から繰り返し苦情が寄せられている。
▼ブランド価値、見込み、市場シェアの損失		
相当なものだ	社会的、全国的、主流メディアによる**広範な**報道または世間の監視によって、風評被害が生じる可能性がある。	• ネガティブな報道が執拗に続き、一面を飾ったり、国際的なメディアの関心を集めたりする。 • 顧客、同業者、投資家の信頼を失う • 代表者からの公的非難 • さまざまな顧客層から大量の苦情が繰り返し寄せられている。
影響レベル説明とステップ変更の推移を含む）		**その他の状況**（観察されるかもしれない）
▼事業体が外部のエンドユーザーや市場の期待に応える能力に対する信頼や信用を大きく失う。		
	社会的、全国的、主流メディアによる報道、または世間の詮索が長引いた結果、**風評被害が生じた**。	• ブランドや市場価値に長期的または深刻な影響を及ぼし、修復不可能となる可能性がある。 • 顧客の信頼を大きく失い、株主や規制当局から訴訟を受ける可能性がある。 • 関連事業体、市場または地域に及ぶ評判への影響

附属書 M：外部影響尺度

影響レベル説明とステップ変更の推移を含む）		**その他の状況**（観察されるかもしれない）
なし	外部への影響は見られない	
▼インシデントにより一時的に迷惑を被った外部関係者		
重要ではない	影響を受ける事業体の義務に対する瞬間的な不満の表明	- 短期的な消費者の不便 -外部エンドユーザーの成果を達成するために利用可能な代替チャネルまたは金融機関
▼望ましい活動が損なわれるような、直接的または間接的に影響を受ける外部の関係者		
マイナー	インシデントにより、外部の関係者に不釣り合いなレベルの混乱や困難がもたらされる。	- 観測された障害にもかかわらず、許容範囲内で重要なサービスの提供を継続すること。
▼利害関係者のニーズを満たせず、利害関係者の利益を守れなかった。		
中程度	影響を受けた事業体が、1 つまたは複数の利害関係者グループの期待に応えられなくなった。	- サービスレベル義務の不履行 - 消費者の不利益（不利益および／または不満）が増大する - 金融サービスへのアクセスが制限される
▼他の事業体に対して二次的（またはそれ以上）の伝染効果をもたらす影響		
相当なものだ	インシデントが、結果として、依存するステークホルダーの失敗、障害、または損害をもたらす。	- より広範な生態系に影響を及ぼす可能性がある - 消費者、顧客、または市場の整合性や競争力に対する実際の損害 - 保険契約者保護にリスクをもたらす - 金融システムの安定性、完全性、信頼性のリスク
▼インシデントが影響を受ける事業体の手に負えないものである。		
	影響を受ける事業体、その取引相手、または金融システム全体の秩序あるオペレーションに対する**差し迫ったリスク**	• 消費者または顧客の利益を著しく損なう • 金融システム、他の市場参加者、より広範な経済に深刻な財務的影響を及ぼす。

附属書 N：原因の種類

原因タイプレベル 1 およびレベル 2）		**説明**
内部プロセスの失敗	プロセスの設計と保守	エンド・ツー・エンドのプロセス（インプット、アウトプット、フロー、測定を含む）を適切に設計、文書化、または実施し、その後、利害関係者の期待に沿って定期的に見直し、維持することができなかった。
	役割、責任、プロセス・オーナーシップ	プロセスの利害関係者の役割と責任の定義と理解が不十分で、プロセスのオーナーシップの定義が不十分である、またはガバナンスが不十分である。
	プロセスの監視と問題のエスカレーション	適切な人員による対処のために、プロセスの運用に関する異常または予期せぬ状況を適切に通知、確認、対応、またはエスカレーションしなかったこと。
	サービス・レベル契約	プロセス関係者の間で、期待されるサービスに関する合意が得られず、期待されるアクションを完了できないこと。
		特定できない内部プロセスの故障
人的要因	ヒューマンエラー	実行に失敗した： • 誤った行動（ミス） • 正しい知識がない（無知） • 不適切な選択（誤った判断） • 性急なパフォーマンス（中略） • 行動しなかった（不作為） • 不利な個人的条件（職務適性）、または • 期待される行動から意図的に逸脱する（違反）
	劣悪な労働環境	人的パフォーマンスに悪影響を及ぼす、事業環境や組織文化の欠陥
	経営の失敗	適切な監督を行わず、既知の問題を是正せず、業務を支援するために必要な適切な人的、金銭的、設備的資源を供給しなかった。
		特定できない人的要因
情報システムの障害	設計、開発、テスト	不適切または不十分な要件定義、開発中の要件不履行、実装/設定の誤り、非効率的または非定型的なテストに起因する不具合。
	変更管理	適切な権限、レビュー、厳格さを欠くプロセスによって、情報システムまたはその構成に加えられた変更。
	容量と性能	与えられた負荷や情報量を処理できない、あるいは許容されるパラメータ（速度、消費電力、熱負荷など）内で指示や情報処理を完了できない。
	保守と陳腐化	情報システム・コンポーネントの保守が不適切または不十分であること、またはサポートされる耐用年数を超えて運用されていることに起因する障害

原因タイプレベル 1 およびレベル 2）		**説明**
	システムの複雑性や統合性	システムの機能が複雑であったり、コンポーネント間の相互関係が多かったり、システムのさまざまなコンポーネントが一緒に機能しなかったり、正しくインターフェイスできなかったりすること。
		特定不能の情報システム障害
外部依存の失敗	オペレーション上の失敗 (セキュリティーを除く)	社内のプロセス、人材、管理、またはシステムが効果的でない、あるいは機能していないことが原因で、サービスや商品の提供に対する期待や契約上の義務を満たすことができない。
	セキュリティ障害	機関にとって価値のある資産に悪影響を及ぼすような、サードパーティまたはサプライチェーン内での危殆化またはデータ漏洩
	ビジネス主導の失敗	プロバイダの財務上の不備、法律や規制の不遵守、風評被害につながる不利益な行為、またはサービス提供に関する戦略的意思決定が相容れないことに起因する外部依存の失敗。
		特定できない外部依存の失敗
ハザード	自然災害	人命の損失、負傷またはその他の健康への影響、物的損害、生活およびサービスの損失、社会的・経済的混乱、または環境破壊を引き起こす可能性のある自然の過程または現象（気象学的、水文学的、地質学的、および自然発生的な生物学的・化学的災害、ならびに宇宙気象を含む。）
	人為的ハザード	人間の活動や選択によって完全に、または主にもたらされたハザードで、曝露された人々や環境を危険にさらす可能性のあるもの（環境的、技術的、社会的ハザードを含む）。
		特定不能の危険
悪意ある行為	DoS / DDoS	**サービス拒否（DoS）**：情報または情報システムへの認可されたアクセスを阻止すること、または情報システムの運用と機能を遅延させ、その結果、認可されたユーザーの可用性を失わせること。 **分散型サービス拒否（DDoS）**：多数のソースを同時に使用して実行されるサービス拒否。
	個人情報の盗難	詐欺や欺瞞を伴う何らかの方法で、通常は経済的利益を得るために、他人の個人データを不正に取得・使用すること。
	インサイダーの脅威	内部脅威者による意図的な行為で、資産に損害を与えたり、混乱させたり、不正にアクセスしたりすること。
	マルウェア	悪意を持って設計されたソフトウェアで、事業体やその情報システムに直接的または間接的に危害を与える可能性のある機能や機能を含む。
	物理的な操作、損傷、盗難、紛失	事業体の現物資産に不利な影響を与える行為（すなわち、「現物資産」、「現物資産」、「現物資産」、「現物資産」、「現物資産」、「現物資産」、「現物資産」）。 具体的で現実的な）環境
	ランサムウェア	身代金の要求が満たされるまで、情報システムやその情報の利用を妨害し、恐喝を行うために使用されるマルウェア。

原因タイプレベル 1 およびレベル 2）		**説明**
	リソースのハイジャック	システムおよび/またはホストサービスの可用性に影響を与える可能性のある、リソース集約的なタスクを完了するために、共同利用される情報システムのリソースを活用する。
	ソーシャル・エンジニアリング (フィッシングを含む)	**ソーシャル・エンジニアリング**：人をだまして情報を開示させたり、特定の行動をとらせようとする行為の総称。 **フィッシング**：ソーシャル・エンジニアリングのデジタル形態で、電子コミュニケーションにおいて信頼できる事業体のふりをして個人情報や機密情報を取得しようとする行為。
	スパム	電子メッセージングシステムを悪用し、無差別に迷惑なバルクメッセージを送信すること。
	ウェブアプリケーション・ターゲティング	ウェブベースのアプリケーションやサービスのサイバーセキュリティを侵害する行為（例：水飲み場攻撃、ウェブサイトの悪用、インターネットにアクセス可能なアプリケーションやリモートアクセスサービスの侵害）。
		不特定の悪意ある行為

附属書 O：発生源

原産地（適切な場合はサブタイプも	
内部	
サードパーティ	グループ内事業体
	アウトソーシング・サービス・プロバイダ
	外部委託していないサードパーティ
	サプライチェーン - 第 4 者（またはそれ以上
	重要インフラ／プロバイダ
外部	不可抗力（自然および偶然）
	脅威アクター（悪意者）
	金融市場参加者
	顧客／消費者
不明	
その他	