AFCブリーフィング

セクターを越えた詐欺情報の共有

行動への道

2026年3月

ACAMS

このレポートは、2026年2月にACAMS国際詐欺対策および技術タスクフォースに提出されました。

エグゼクティブサマリー

詐欺は金融犯罪対策における世界最大の脅威として浮上しており、組織が多額の投資を行っているにもかかわらず、損失は増加し続けています。根本的な課題は明確です。詐欺スキームは、通信、テクノロジープラットフォーム、ソーシャルメディア、銀行、暗号通貨取引所にまたがる広大なエコシステムで機能しているにもかかわらず、こうしたスキームに関する情報は個々のセクターや組織内にとどまっています。どの組織も全体像を把握していないため、詐欺をリアルタイムで阻止するのはほぼ不可能になっています。

ACAMS国際詐欺対策および技術タスクフォースは、民間部門の情報共有について検証し、業務に対する短期の潜在的影響を特定することを決定しました。詐欺を効果的に阻止するには、実用的な情報を、詐欺に介入できる立場と意思を持った当事者に提供することが必要です。そのため、強固な情報共有インフラストラクチャは、協調的な詐欺防止と対応に必要不可欠です。

タスクフォースの主な検討事項と議論のポイント

- **重要なイニシアティブ:** 特定された行動機会に基づいて、タスクフォースのメンバーが優先的に取り組むべきだと提案する具体的なイニシアティブ（セクター、プライバシー、法的責任に関する現在の許可と保護について法令や指針を詳細に検証するなど）は存在するか？こうしたイニシアティブの推進に最適なのは誰か？
- **協力の支援:** 国際的な情報共有基準枠組みの策定を開始するにあたり、提携するのに最適な組織はどれか？
- **今後の展望:** (1) 詐欺ライフサイクルの各段階における情報の可用性、共有、行動に焦点を当てた机上演習の主催、および (2) セクター別の具体的な高付加価値データのユースケース・テンプレートや優先度の高い詐欺シナリオ（防止、阻止、回収など）といった詐欺データツールキットの開発において、ACAMSがタスクフォースを支援するうえで最も重要な要素は何か、そして参加させるべきステークホルダーは誰か？

既存のフレームワークと重要な障壁

米国、欧州、アジア太平洋のステークホルダーのエンゲージメントは、一貫したパターンを示しています。それは、適切な仕組みがあれば効果的な情報共有は実現可能だが、体系的な障壁によって拡大が妨げられているというものです。情報共有が機能している分野、例えば金融セクターのコンソーシアム（**早期警戒サービス [EWS]**、**金融サービス情報共有分析センター [FS-ISAC]** など）、テクノロジー連合（**グローバルシグナル交換所**、子供の安全を守るための**テック・コーリションのランタン**プログラムなど）、香港の**FINEST**プラットフォームや**シンガポールの詐欺防止センター**といったセクター横断的なイニシアティブ、および二者間のパートナーシップでは、明確なガバナンス、的を絞ったユースケース、互恵的な価値、信頼関係が成功の要因になっています。

しかし、ほとんどの組織は詐欺情報を効果的に共有していません。ACAMSとタスクフォースのメンバーは、一連のエンゲージメントやラウンドテーブルで、詐欺対策のための情報共有の速度、洗練性、実行性、導入を改善するうえで特に重要な障壁を特定しました。こうした障壁には、法務顧問の既定の回答が「ノー」であること、法的責任を負うリスクの認識、規制上の明確な許可の欠如、技術的な互換性の欠如、データの質に関する懸念、風評被害などがあります。最も根本的な障壁は、組織にとって多大なコストがかかり、潜在的な法的責任が生じ、競合他社を利する可能性さえあると感じられる自主的な情報共有に対して、リソースを投資するインセンティブは限定的だと認識されていることです。

- **法令および規制上の問題：**政府は大規模な情報共有を実現するために、法的責任が適用されないセーフ・ハーバー（米国愛国者法第314(b)条、サイバーセキュリティ情報共有法など）を認めていますが、既存のセーフ・ハーバーは十分に活用されていません。一部では政府が広範な権限と保護を与えているという評価もあるものの、こうしたセーフ・ハーバーのさまざまな要素は、低速、煩雑、特定のセクターにしか適用されない、ユースケースや応用が限定的、あるいは広範な利用を促進するために必要なインセンティブがないといった批判を受けています。プライバシー法（GDPR、CCPA、GLBA、ECPAなど）は、主観的な制約や実際の制約を生み出し、解釈も法域やセクターによって大きく異なっており、国境を越えた情報共有をさらに困難にしています。組織は、法務・コンプライアンス部門がリスク回避的であり、情報共有イニシアティブの開始を阻止すると報告しています。
- **速度と適時性：**詐欺インフラは常に変化しています。犯罪者はリストを継続的にモニタリングし、ドメインや電話番号などのインフラを絶えず入れ替えています。こうした行動パターンに対して、情報共有のスピードが遅いと効果が乏しくなります。特に詐欺やそれによる収益獲得を短期的に防止および阻止するために**タイムリーな行動**を必要とする場合はなおさらです。
- **技術的な互換性と基準の欠如：**組織はさまざまなデータ形式、識別情報、システムを使用しているため、現在、詐欺対策に有用な情報を大規模に共有することは困難です。詐欺のライフサイクルにおいて有用な情報は組織によって異なります。メッセージ形式とデータ基準は国、ネットワーク、データの種類（金融、デジタルフットプリントなど）によって異なり、効果的な情報交換には課題があります。
- **データの質と実用性：**組織は、十分な背景情報が欠如した情報を受け取ることが頻繁にあります。信頼スコア、調査の詳細、または実用的なガイダンスがなければ、受け手は共有された情報に基づいて業務上の決定を正当化できません。さらに根本的な問題として、多くの組織は、他のセクターのパートナー組織にとってどのような情報が最も有用であるかが分からないと報告しています。多くの組織は、過去に情報が共有された際に、情報に基づいて行動していない、あるいは有意義な成果を達成していないように見えたのではないかという懸念を表明しました。
- **風評リスクと競争上の懸念：**組織は、正当な顧客を拒否すること、「デバンキング」を助長していると認識されること、あるいはコミュニケーションプラットフォームやソーシャルメディアプラットフォームへのアクセスを遮断しようとしていると認識されることによる風評被害や法的責任を恐れています。
- **縦割りとカバレッジのギャップ：**一部では効果的な情報共有が行われていますが、詐欺犯罪者がセクターや国境を越えて技術、通信、金融インフラを悪用しているにもかかわらず、セクターを越えた情報共有は最小限にとどまっています。組織内だけでなく、特に業界や国の垣根を解消することは、タイムリーで実用的な情報共有の実現に必要不可欠です。
- **組織としてのインセンティブの欠如：**ほとんどの地域とセクターは、組織がセクターを越えて情報を共有するインセンティブが非常に乏しい状況にあります。多くの組織は、リソースの消費、法的責任を負う可能性、風評リスクによるデメリットがメリットを上回るため、情報共有の意欲が妨げられていると報告しています。

次のステップ

上記の障壁に対処するには、短期的な業務改善と長期的な構造変革の両方が必要です。以下の複数の短期的な行動は、セクターを越えた詐欺情報の共有を促進できる可能性があります。(1) 既存の権限をより効果的に活用する。これには、セクター、プライバシー、法的責任の枠組み全体で、現在の許可と保護について正式な法務レビューを追求することを含む。(2) さまざまなセクターにとって有用な情報の種類を特定する。(3) 詐欺犯罪者の行動と同等の速度の自動化システムを通じて、犯罪類型アラートやハッシュ化された識別情報など、スムーズに共有できる種類の情報を共有する。(4) 背景情報を有する高付加価値データに焦点を当て、データを実用的な情報に転換する。および (5) 詐欺スキームや詐欺の防止、阻止または被害回復に関する具体的なユースケースに基づいて、優先度の高いシナリオのユースケース・テンプレートとパイロット試験を導入する。タスクフォースのメンバーは、長期の構造的課題に対処するため、公共セクターと民間セクターのステークホルダーを示し、エンゲージメントを実施するという的を絞った取り組みを検討することができます。これは、成功した国際モデルに基づき、法令を明確化し、セーフ・ハーバーのギャップに対処することを目的としています。

ACAMSはタスクフォースを支援するため、有用で優先度の高いデータ要素とその有用性を示す**詐欺データツールキット**を開発しています。また、有用なデータ、ユースケース・テンプレート、詐欺や不正行為のライフサイクル全体で詐欺を防止および阻止するために実施できる行動をより完全に示すための**机上演習**を主催する予定です。またACAMSは、タスクフォースや外部の専門家との協力を通じて、**詐欺情報共有標準フレームワークの策定**を開始する予定です。そのために、優先度の高いユースケースとデータ要素の要件を定め、より広範な技術的および非政府的な標準化組織、運用組織、専門家と連携し、当該フレームワークを導入するための正式な技術仕様への移行を目指します。

セクターを越えた詐欺情報共有
– 行動への道筋

背景

詐欺は近年劇的に増加しており、**ACAMSグローバルAFC脅威レポート2026**では金融犯罪対策における世界最大の脅威に挙げられています。ACAMS国際詐欺対策および技術タスクフォースの初回会合において、メンバーは民間部門間の情報共有を、協調的な詐欺防止の基盤を成す優先事項として認識しました。

現代の詐欺対策における基本的な課題の一つは、詐欺スキームのさまざまな部分が、通信、テクノロジープラットフォーム、ソーシャルメディア、銀行、暗号通貨取引所などのセクターを含む広大な詐欺エコシステム全体に分散していることです。このような情報の断片化により、個々の企業は事件の不完全な全体像しか把握できず、詐欺をリアルタイムで特定および阻止することが困難になっています。

個々の組織による多額の投資にもかかわらず、犯罪ネットワークが急速に適応し、組織や法域の境界を越えて活動する中で、詐欺による損失は増加し続けています。金融機関、決済プロバイダー、テクノロジープラットフォーム、通信会社などの民間企業はそれぞれ、詐欺のパターン、加害者のインフラストラクチャ、標的とされる被害者に関する貴重な情報を保有していますが、こうした情報は依然としてほとんどサイロ化されています。情報共有は一貫しておらず、詐欺を適時に阻止するには遅すぎることが多く、往々にして詐欺がすでに発生した後にのみ情報が共有されています。

既存のパートナーシップから得られる一貫した教訓は、組織がどのようなデータを、誰と、どの程度の速度で、どのような業務上の目的で共有する必要があるかを明確にすると、進歩が加速するということです。このような明確さがない場合、情報共有は法的リスクが高い、業務上の負担が大きい、競争面でセンシティブである、または範囲が広すぎると認識され、組織は協力ではなく警戒を基本姿勢とすることになります。

現状：何が成功し、何が失敗しているか

既存の情報共有メカニズム

複数のセクターからのエビデンスは、適切な仕組みがあれば、民間部門の効果的な情報共有が実現できることを証明しています。

- **EWS、オーストラリア金融犯罪情報交換所（AFCX）、FS-ISAC**などの**金融セクターのコンソーシアム**は、脅威に関する情報を共有することで、競争上の境界線を尊重しつつ、詐欺による損失を減らせることを示しています。コンソーシアムの有効性は、顧客データではなく特定の脅威の兆候に焦点を当てた設計、明確なガバナンス構造、参加者の相互価値を生み出すインセンティブなど、いくつかの設計上の共通の特徴に起因しています。

> **注目のユースケース – 政府が支援するパートナーシップ：**
>
> アジア太平洋地域の政府が支援するプラットフォームは、セクターを越えた大規模な情報共有モデルを提供しています。香港の**FINEST**プラットフォームは、警察が一元管理し、現在はリテール銀行や仮想銀行もメンバーとなっています。このプラットフォームは、マネーミュールや詐欺口座に関する情報の多対多の自動共有を実現し、大きな影響をもたらしています。試験運用の開始以来、支払い停止の要求が減少したと報告されています。こうしたプラットフォームの成功の理由は、明示的な規制承認、一元化された技術インフラ、明確な運用プロセスです。

- **テクノロジープラットフォームのパートナーシップ**は、組織的攻撃ネットワークを妨害するために、口座情報とコンテンツ情報を共有する二者間協定を策定しています。プラットフォームは、詐欺口座、詐欺コンテンツのパターン、組織的な不正行為に関するシグナルを共有し、詐欺がさらに拡大する前にパートナーが積極的に行動することを可能にします。

> **注目のユースケース – セクターを越えたテクノロジー連合：**
>
> テック・コーリションのランタンプログラムなど、子供の安全を守るためのセクターを越えたテクノロジー連合は、共通の使命と規制要件（児童の性的虐待コンテンツ［CSAM］は世界全体で厳しく非難されるとともに、法令で対処が義務付けられている）が、金融機関とソーシャルメディアプラットフォームを結びつける効果的な協力関係を大きく推進することを示しています。**グローバル詐欺対策連合**と**グローバルシグナル交換所（GSE）**は、GSEを通じてコンテンツハッシュやURLなどの技術的指標を共有するなど、消費者詐欺情報に関する国際協調を促進しています。こうしたモデルが機能している理由は、問題の深刻さと世界全体からの厳しい非難に加え、特に法令上の義務によって問題がさらに困難になり、参加が促進されたためです。

- 英国の**合同マネー・ローンダリング・インテリジェンス・タスクフォース（JMLIT）**や**国家経済犯罪センター（NECC）**などの**マネー・ローンダリング対策パートナーシップ**は、信頼関係に基づく、狭い範囲におけるユースケース主導の情報共有が大きな影響をもたらすことを示しています。これらのイニシアティブが機能している理由は、包括的なデータ共有よりも実用的な情報に重点を置いているためです。

> **注目のユースケース – 暗号通貨に関する違法金融取引の情報共有：**
>
> 業界全体でいくつかのパートナーシップが設立され、その一部は政府機関と提携しています。こうしたパートナーシップは、情報共有や、速やかな回収のために暗号通貨建てとなっている違法収益や詐欺収益に関連する資産回復を開始することを目的としています。例えば、**違法な仮想資産通知（IVAN）**パートナーシップ、**セキュリティ・アライアンス（SEAL 911）**、**オペレーション・シャムロックおよびクリプト・コーリション**、T3金融犯罪対策部門グローバル・コラボレーター・プログラムなどが挙げられます。

- 個々の組織間の**非公式な二者間協定**は、正式な枠組みではなく個々の関係と明確な相互利益に依拠しており、具体的な詐欺の脅威が発生した場合に最も速く行動できる傾向にあります。

情報共有が失敗するケース

上記の成功にもかかわらず、以下のような重大な障壁によって、広範な情報共有の導入は妨げられています。

- **競争上の懸念と信頼の欠如：**ラウンドテーブル参加者の一人が説明したように、「信頼を拡大するのは困難」です。組織は詐欺情報を共有することで、独自の検知方法、顧客の行動パターン、またはビジネスの脆弱性が競合他社に知られる可能性を懸念しています。セクター間およびセクター内の信頼の欠如は、特に組織が異なる規制上の義務やビジネス上のインセンティブを持つ場合、情報共有への参加意欲を妨げます。
- **法令および規制上の問題：**プライバシー法規（EU一般データ保護規則［GDPR］、カリフォルニア州消費者プライバシー法［CCPA］、グラムリーチ・ブライリー法［GLBA］、金融プライバシー権法［RFPA］、電子通信プライバシー法［ECPA］など）や反トラスト法に関する考慮事項は、共有が可能な情報に関して、主観的な制約や実際の制約を生み出しています。ステークホルダーはエンゲージメントにおいて、法務・コンプライアンス部門がリスク回避的で、情報共有イニシアティブの開始を阻止していると一貫して報告しました。たとえセーフ・ハーバーが存在しても、こうした仕組みは低速かつ煩雑で、インセンティブが限られており、実務上の阻害要因があると組織は報告しています。多くの組織は、誤った情報を共有すると規制や風評上の影響を受けるが、情報共有に成功しても組織にメリットがないと感じています。しかし、他のステークホルダーは、一部の法域では広範なユースケースについて幅広い免責が既に業界で認められていることを強調しました。例えば米国には、金融機関がマネー・ローンダリングに対抗するための情報共有を認める**米国愛国者法第314(b)条**や、サイバー脅威情報を民間部門で共有するための**サイバーセキュリティ情報共有法**などがあります。参加者の一人が指摘したように、技術的な能力と、情報を共有したいという業務上の要請が存在しても、規制の保守的な解釈によって「法務顧問が共有を止めている」状況があります。法的責任の枠組みやセーフ・ハーバーの適用の明確性と範囲に関してステークホルダー間で意見が異なっていることに加え、不正確な恐れがある情報の共有や、情報共有が少なすぎることや遅すぎることによって法的責任を負う懸念も、躊躇を強める要因となっています。さまざまなセクターやユースケースにおける免責は、こうした主観的な制約や実際の制約、限定的なインセンティブなどが理由で、十分に活用されていません。セクターごとに直面している法的制約は異なるため、セクターを越えた情報共有は特に困難になります。

- **技術的な互換性の欠如：**法律や信頼性の障壁を克服した場合でも、データ形式の不整合、API統合コスト、共通した標準の欠如によって、情報共有は業務上困難になっています。組織ごとに、同一の事業体の識別情報や、保有データの詳細度は異なっており、システムの互換性も欠如しています。互換性を巡る課題は、世界中にセクターを越えて広がっています。クレジットカードのような単一セクター内であっても、カード保有者側の銀行と加盟店側の銀行間のデュアルメッセージ・システムの形式は異なります。さらに、各国が独自のネットワークと基準を定めており、カードネットワークの基準とも整合していません。小規模な地方銀行にとって有用なものと、大規模な金融機関が必要とするものは大きく異なります。また、通信会社やソーシャルメディアプラットフォームのニーズも金融機関のそれとは異なっています。
- **データの質、信頼性、実用性に関する懸念：**組織は、共有された情報について、情報の統合と活用に必要な業務上の労力に値する正確性、適時性、具体性を有するかどうかを疑問視しています。ステークホルダーは、背景情報のない生の指標は、往々にして価値が限定的であると強調しました。例えば、あるカンボジアのメールアドレスについて情報共有を受けたとしても、そのメールアドレスがなぜ疑わしいのか、どのような行動を取るべきかが分からなければ、ほとんど実務の助けになりません。組織は、受け手が情報を評価し、対応の優先順位を付けられるように、信頼スコアなどの明確な信頼性指標を付与することの重要性を強調しました。こうした背景情報がなければ、テクノロジープラットフォームから情報を受け取る銀行は、それをどのように使用すべきか確信が持てない可能性があります。誤検知は、共有された情報に対する信頼を損ないます。一方、結果に関するフィードバックがないと、情報共有を継続するインセンティブが低下します。
- **タイミングの遅延：**既存の情報共有枠組みの多くは日次または週次のサイクルで運用されており、詐欺を防止するには遅すぎます。情報が共有されるまでに、詐欺犯罪者はすでに資金を移動したり、口座を閉鎖したり、戦術やインフラを転換したりしています。単に損失を文書化するだけでなく、詐欺防止に効果的な情報共有を行うためには、情報を自動的に、犯罪活動と同等の速度と規模で共有する必要があります。
- **カバレッジのギャップ：**セクター内で情報共有が機能している場合でも、セクターを越えた情報交換は依然として限定的です。銀行は他の銀行と、プラットフォームは他のプラットフォームと情報を共有していますが、詐欺のエコシステムはあらゆるセクターに同時に広がっています。
- **風評リスクの懸念：**組織は、不完全または不正確な恐れがある共有情報に基づいて、顧客を拒否またはデバンキングすることによる風評の毀損を懸念しています。誤って取引を終了された顧客が、ソーシャルメディアでネガティブな注目を喚起するリスクは、規制や民事責任と同等に重大な懸念事項です。この問題が特に顕著になるのは、個人が被害者と加害者のどちらであるかについての完全な情報がない状態で、組織が独自の調査を実施せずに行動することを躊躇するケースです。こうした懸念は、金融排除に対する国民の関心が高まっている法域で増大しています。
- **組織的インセンティブの欠如：**情報共有が技術的に可能であり、個々の社員が共有を望んでいたとしても、組織は根本的なインセンティブの不一致に直面しています。一部のステークホルダーは、「規制当局が情報共有を義務付けるならば共有するが、そうでなければ共有しない」と報告しました。自主的な情報共有には、リターンが不確実なものにリソース（法務レビュー、技術的な統合、業務プロセスなど）を投じる必要があり、情報を共有する組織が法的リスクや風評リスクにさらされる一方で、競合他社を利する可能性があります。株主は、金融機関が自主的なイニシアティブにリソースを費やす理由を疑問視しています。明確な義務や競争上の優位性がないため、組織は積極的な情報共有ではなく、最小限のコンプライアンスを既定路線としています。

共有すべき情報の優先順位付け

すべての種類の情報が同じ価値を持つ、または共有が困難であるとは限りません。組織は業務への影響と実行可能性に基づき、抽出および共有すべき情報を優先順位付けする必要があります。

最も価値の高い種類の情報

以下の種類の情報は、ステークホルダーとのエンゲージメントに基づき、業務への影響、セクター間の適用可能性、および詐欺を適時に阻止できる可能性の観点から、セクターを越えて優先的に共有すべき情報として特定されました。

- **口座および送金先の識別情報：**銀行口座番号、送金人および受取人の名前、暗号通貨ウォレットのアドレス、詐欺収益を受け取る口座の支払いアプリの識別情報。こうした識別情報は、積極的なブロックと協調的な口座閉鎖を可能にします。
- **電話番号：**通信プロバイダーが提供し、詐欺通話、テキストメッセージ、または口座確認に使用される電話番号は、取引の拒否や、他のセクターのリスクシグナルとして使用できます。
- **連携口座ネットワーク：**プラットフォームの口座識別情報と行動シグナルは、ソーシャルメディア、マッチングアプリなどのサービスにまたがる詐欺行為を明らかにします。
- **詐欺犯罪の類型と戦術：**現在の詐欺スキーム、ソーシャルエンジニアリングの戦術、および標的パターンの説明は、組織が検知ルールを更新し、潜在的な被害者に警告することを可能にします。
- **ドメインとインフラストラクチャ：**詐欺ウェブサイトやフィッシングインフラストラクチャのURL、ドメイン、IPアドレス、ホスティング情報を削除またはブロックすることができます。
- **デバイス識別情報とデジタルフットプリント：**デバイスID、疑わしいIPアドレスの範囲、ブラウザのフィンガープリント、画面解像度、タイピング圧力パターンなどのデバイス特性は、ネットワーク分析を可能にします。
- **取引パターン：**行動指標と取引シーケンスから、顧客の身元を明らかにすることなく、詐欺と正当な活動を区別できます。
- **氏名と国民識別番号：**顧客名や、パスポートなどの公式識別番号は、法律によって認められる場合、データベース間の照合に使用できます。

名前と国の識別情報に関するメモ：組織は、これらのコア識別情報（一部の組織は組織データベース間の照合にとって「最も有用なデータポイント」と認識）から始めることの価値を強調する一方、法域ごとのプライバシー法によって共有の可否が大きく変わるという認識を示しました。こうしたデータポイントはプライバシーへの影響が大きく、法的に正当な強い理由が必要です。他の組織は、有意義でタイムリーな名寄せをサポートするうえで、地域や言語間の互換性に課題があることを強調しました。

情報の種類別の法的影響

さまざまな種類の情報の法務リスク特性を理解することは、組織が最初に共有すべき情報と、より慎重な法的分析が必要な情報を優先順位付けするのに役立ちます。あらゆる詐欺関連情報のプライバシー上または規制上の影響が同じとは限りません。調査やステークホルダーとのエンゲージメントに基づく初期レビューは、具体的な情報の種類のリスク階層に関する議論を可能にします。

- **プライバシーリスクが低い:** ドメインやIPアドレス、詐欺犯罪類型の説明、集計されたパターン情報などの詐欺インフラストラクチャ指標は、通常、個人データと関連せず、法的障壁も最小限となっています。
- **プライバシーリスクが中程度:** ハッシュ化またはトークン化された口座識別情報、確認済みの詐欺に関連する電話番号、暗号通貨ウォレットアドレスには個人データが含まれますが、これらはプライバシー法の詐欺防止規定の下で、適切な保護措置を講じた上で頻繁に共有されています。
- **プライバシーリスクが高い:** 暗号化されていない顧客口座の詳細、コミュニケーションの内容、取引履歴、および複数の識別情報と個人の関連付けには、必要性と比例性の原則に基づき、慎重な法的分析と、より強い正当な理由が必要です。

法域やセクターによって、国境を越えてさまざまな当局と情報を共有するための基準となる許可が異なります。米国のグラムリーチ・ブライリー法（GLBA）に基づき業務を運営している金融機関は、他の多くのセクターよりも詐欺関連の情報共有をより明確に許可されている一方で、通信プロバイダーは電子通信プライバシー法（ECPA）の下でより厳格な制限に直面しています。欧州連合（EU）のGDPR第6条第1項(f)は、セクターを越えて適用される正当な利益の根拠について規定していますが、条文の解釈は加盟国やデータ保護当局によって大きく異なります。シンガポールの枠組みは、詐欺防止センターを通じた銀行と通信プロバイダー間の情報共有を明示的に許可していますが、オーストラリアのプライバシー法における詐欺防止関連の例外規定は、依然としてセクター間で解釈が異なっています。これらの法域およびセクター間の差異が存在するため、たとえ英国の通信プロバイダーと米国の金融機関が同じ詐欺スキームを防止するために行動していても、前者が電話番号を共有する際に、後者が同じ番号を共有する際とは異なる法的考慮事項に直面する可能性があります。

情報共有による最高の投資収益率（ROI）

優先度の高い情報共有では、以下のような情報に焦点を当てるべきです。

- **詐欺を阻止するうえで時間が極めて重要:** 現行の詐欺インフラストラクチャについての情報をリアルタイムまたは1時間ごとに共有することで、被害者が重大な被害を受ける前にブロックすることができます。
- **複数のセクターに関連:** 電話番号、ウォレットアドレス、ドメインは複数のセクターにとって有用で、情報共有の価値を最大化します。
- **実用性が明確:** 支払いの拒否、口座の削除、顧客への警告など、具体的な保護措置を可能にする情報には、業務に投資する正当な理由があります。
- **既に収集済み:** 組織が自社の詐欺防止のために維持する情報は、共有に必要な追加コストが最小限に抑えられます。
- **法的に明確:** 低リスクな種類の情報から始めることで、自信と運用能力を深めたうえで、より複雑なシナリオに対処できます。
- **完全な背景情報の存在:** 信頼スコア、調査の詳細、受取人が実施できる行動（支払いの拒否、口座の凍結、コンテンツの削除、顧客への警告など）に関する明確なガイダンスなど、実用的な背景情報とともに共有される情報は、生のデータポイントに比べて、業務への投資を非常に効果的に正当化します。

最も価値があり、法的に共有可能な種類の情報を優先することで、組織は既存の権限とスムーズなアプローチを活用し、即座に行動を起こすことができます。

短期的な機会

新たな立法や大規模な技術投資を必要とせずに、情報共有を改善できる可能性がある複数の機会について議論がなされました。

既存の法的権限の利用を改善する

多くの組織は、詐欺に関する特定の情報や関連情報の共有について、さまざまな法的保護や許可を提供する既存の法的権限を十分に活用していません。

- **米国愛国者法第314(b)条**は、金融機関が詐欺関連情報を共有するためのセーフ・ハーバーを提供していますが、認識不足や過度に慎重な解釈のため、依然として十分に活用されていません。
- **2015年サイバーセキュリティ情報共有法**は、サイバー脅威と保護措置に関連する情報の共有について、セクター横断的な免責事項を規定しています。主に金融機関に適用される第314(b)条とは異なり、同法はサイバー脅威情報を共有するあらゆる業界の成員を対象としています。現代の詐欺の大半はサイバー対応型犯罪であるため、この既存のセーフ・ハーバーは、組織が現在認識しているよりも、セクターを越えた詐欺情報の共有を幅広く認めている可能性があります。
- **GDPR第6条第1項(f)に定める「正当な利益」の根拠**は、詐欺防止のための情報処理を許可していますが、組織は許容性を確認する法的意見を求めることなく、不必要に保守的なアプローチを取ることが頻繁にあります。
- 通信詐欺規制、決済システム規則（カードネットワーク運用規制など）、プラットフォーム利用規約における**セクター別規定**は、往々にして組織の理解よりも広範な情報共有を許可していますが、それぞれのセクター以外では十分に理解されていない可能性があります。
- **契約メカニズム**（秘密保持契約［NDA］、二者間データ共有契約、コンソーシアムの会員構造など）は、効果的な交渉と導入に法的リソースが必要であるものの、新たな立法を必要とせず、機密性と法的責任に関する多くの懸念に対処できます。

組織は、すべての関連法域の法務顧問を交えた部門横断的な法務レビューを実施することで、情報共有の可否の基準を確立し、既存の枠組みの下で現在共有可能な情報を文書化できる可能性があります。規制ファシリテーションは、既存の権限の活用を加速させることができます。香港では、銀行規制当局が、プライバシー法の改正が確定する前であっても、詐欺防止のための情報共有が許可されていることを確認する明示的なレターを参加銀行に提供しました。これにより、FINESTプラットフォームの設立に必要な法的安心感が生み出されました。このことは、規制当局が法律の改正を待たずに、明確なコミュニケーションと明示的な承認を通じて、既存の枠組みの範囲内で行動を起こせることを示しています。

即時かつスムーズに共有できる種類の情報

組織は、法令または業務上の障壁が極めて小さい種類の情報から、情報共有をただちに始めることができます。こうした情報には以下が含まれます。

- **詐欺犯罪類型アラート：**現在の詐欺スキーム、戦術、標的パターンの説明には個人データが含まれておらず、既存のコミュニケーションチャネルを通じて自由に共有できます。
- **ハッシュ化された識別情報：**一般的なアルゴリズムを使用してハッシュ化された電話番号、口座番号、ウォレットアドレスは有意義な照合機能を提供します。プライバシーが保護されており、技術的な複雑性も極めて低水準です。
- **インフラストラクチャ指標：**確認済み詐欺サイトのドメイン、URL、IPアドレス、ホスティング情報を共有し、協力してブロックおよび削除することができます。
- **集計されたパターン：**詐欺の傾向、地理的な集中、タイミングのパターンに関する統計情報により、個々の記録を明らかにすることなく、検知を改善できます。

組織は、詐欺犯罪類型アラート、インフラストラクチャ指標、集計されたパターンなど、個人を識別できない情報（非PII）について、犯罪者の活動と同等の速度で情報を自動的に共有すべきであると強調しました。ドメイン、IPアドレス、犯罪類型情報の共有を検証および承認するための手作業のプロセスは、情報を陳腐化させる遅延につながります。自動化されたシステムは、こうした低リスクな種類の情報を、必要な速度と規模で共有できます。こうした低リスクな種類の情報は、非公式のチャネルやシンプルな二者間協定を通じて即座に共有でき、より複雑な情報共有シナリオに向けた運用能力と信頼を高めます。

パイロット試験とテンプレート

パイロット試験やより広範な導入の一環として、具体的なテンプレートやガイドを策定し、導入を促進することで、詐欺対策の最前線で戦う人々にとって短期的な実用性があるツールを提供できる可能性があります。例えば、以下のようなツールが考えられます。

- **ユースケース・テンプレート：**3〜5つの優先的な情報共有シナリオ（銀行間で共有されるミュール口座、銀行と暗号通貨ウォレット間で共有されるアドレス、通信会社と全当事者間で共有される詐欺関連の電話番号、プラットフォーム間で共有される連携口座、マッチングアプリと銀行間で共有されるロマンス詐欺師）に関する詳細な文書。共有すべきデータ要素、法的根拠、タイミング要件、実現できる行動を定めます。
- **法的ガイダンス文書：**既存の情報共有の許可に関する法域ごとの分析、データ共有契約のテンプレート、セーフ・ハーバー条項の説明。
- **技術的なガイド：**ハッシュ化された識別情報交換の簡単な仕様、二者間共有のためのAPI構造、実用最小限のデータスキーマ。
- **ガバナンステンプレート：**二者間、コンソーシアム、仲介を通じた情報共有取り決めのモデル契約。標準的な相互性、使用制限、説明責任についての条項を定めます。
- **パイロットプログラム：**3〜5つの協調的なパイロットプログラムを立ち上げ、自発的な参加者とともに優先度の高い情報共有シナリオをテストし、実施における課題と教訓を文書化し、より広い範囲での再現を図ります。

長期の構造的課題

既存の権限による短期的な進歩が可能である一方、いくつかの障壁を打破するには、より正式な枠組みや立法または規制上の措置が必要です。

セーフ・ハーバーと免責

現在のギャップ:既存のセーフ・ハーバーはセクター別で、主に金融機関向けであり、セクターを越えた情報共有を明示的に対象としていません。組織は、不正確な情報の共有、情報共有が過少であること、または遅すぎることに対して法的責任を負う可能性を恐れています。

ニーズ:明示的なセーフ・ハーバー条項は、銀行、プラットフォーム、通信会社、小売業者、暗号通貨取引所など、特定の条件下におけるセクターを越えた詐欺情報の共有を許可しなければなりません。組織の躊躇を減らすためには、善意の情報共有について、十分に明確かつ強固な免責を定める必要があります。

既存のアプローチの例:

- **米国:**米国愛国者法**第314(b)条**は金融機関にセーフ・ハーバーを提供していますが、プラットフォーム、通信プロバイダーや金融機関以外とのセクターを越えた情報共有には明示的に適用されていません。**2015年サイバーセキュリティ情報共有法**は、サイバー脅威や保護措置に関連する情報共有について、業界のあらゆる成員に免責を提供しています。これはサイバー対応型犯罪の指標にも適用される可能性があります。
- **オーストラリア:**オーストラリアの**プライバシー法**には詐欺の防止に関する例外規定が定められていますが、その解釈はさまざまで、セクターを越えて適用できるかどうかは依然として不透明です。
- **香港:**金融情報調査局は香港警察を通じてFINESTプラットフォームを運営しています。香港金融管理局は、詐欺防止のための情報共有が許可されていることを確認するレターを参加銀行に送付しており、同プラットフォームに規制上の明示的な承認を与えています。FINESTプラットフォームでは現在、すべてのリテール銀行と仮想銀行が、マネーミュールと詐欺口座情報に関する自動化された一元的な多対多の情報共有システムに参加しており、導入以来、詐欺が大幅に減少しています。
- **シンガポール:****フィッシング対策の責任共有枠組み**は、通信プロバイダーや銀行が詐欺防止センターを通じて情報を共有することを明示的に承認しています。
- **韓国:**法執行機関と金融規制当局が主導する包括的な**詐欺防止フレームワーク**は、銀行、ノンバンク金融機関（NBFI）、フィンテック企業、通信プロバイダーが協力し、詐欺が特定された際に口座をただちに凍結することを認めています。この枠組みは、立法措置が、明確な権限、強力な執行メカニズム、セクターを越えた協力関係を生み出し、組織的な参加をいかに促進するかを示しています。

主な考慮事項:セクターを越えたセーフ・ハーバーを策定することで、適切なガバナンスの下で、口座識別情報、電話番号、ウォレットアドレス、インフラ指標などの特定の詐欺指標を指定セクター間で共有することを可能にし、所定の基準を満たす善意の情報共有を免責する。

プライバシー法および反トラスト法の明確化

プライバシー法が明確化される可能性:

- GDPRおよび同様の枠組みに基づき、詐欺防止が正当な利益またはその他の法的根拠とみなされることを明示したガイダンス。
- 金融サービス、通信、テクノロジープラットフォーム、小売など、さまざまなセクターで詐欺防止規定がどのように適用されるかについての明確な方向性。
- データ移転規制に基づく、国境を越えた詐欺情報の共有の明示的な許可。
- さまざまな詐欺シナリオにおいて、どのデータ要素を共有するのが合理的であるかを定めた、比例原則に基づくガイダンス。
- 共有の遅延によって情報が無意味になる可能性があることを考慮した、情報共有の速度と適時性に関する規定。

反トラスト法が明確化される可能性:

- 詐欺脅威情報の共有が、反競争的な情報交換とみなされないことの確認。
- 業界コンソーシアムの適切なガバナンス構造に関するガイダンス。
- 許可されている詐欺指標の共有と、許可されていないビジネス情報の交換の明確な区別。

例:

- **欧州連合(EU):データ保護当局**は、新型コロナウイルス(COVID-19)のデータ処理に関して発行されたガイダンスと同様に、詐欺防止のための情報共有に関する協調的なガイダンスを発行する可能性があります。

- **米国:**連邦取引委員会と司法省は、詐欺情報共有コンソーシアムのために、反トラスト法で認められる情報共有とそうでない情報共有の境界を明確にする可能性があります。

主な考慮事項:データ保護当局や競争規制当局と協力し、詐欺情報の共有に関する既存の許可と境界を明確化した具体的なガイダンスを策定する。これにより、既存の枠組みの下での行動を妨げる主観的な法務リスクを軽減できる。

国境を越えたデータ共有権限

現在のギャップ: 国境を越えた詐欺情報の共有は、データ転送制限（GDPRの十分性要件、Schrems II判決の影響、セクター別のデータのローカライズ要件など）に基づく不確実性に直面しています。組織は、業務上重要であっても、国際的な情報共有を行わないことが多く、それが既定路線となっています。こうした課題にもかかわらず、国境を越えた合法な情報共有を支援する枠組みや、共有を義務付ける条約も存在します（**金融情報機関（FIU）によって構成されるエグモントグループ**、**国連サイバー犯罪防止条約**、**刑事共助条約（MLAT）**など）。

ニーズ: 情報共有の仕組みは、リアルタイムの国際的な詐欺情報交換を実現し、それを既存のデータ保護枠組みにおいて機能させることが必要です。これには、詐欺防止を適切な保護措置として相互に承認すること、詐欺情報に関する標準的な契約条項、またはAPEC越境プライバシー規則と同様の多国間枠組みが含まれる可能性があります。

例:

- **APAC:** FRONTIER+イニシアティブは、国境を越えた詐欺情報の共有が可能であることを証明していますが、包括的な法的枠組みが欠如しています。
- **欧州-米国:** データプライバシーフレームワークは、大西洋を越えたデータ転送の枠組みを定めていますが、詐欺情報の共有に適用されるかどうかは依然として不明です。

主な考慮事項: データ保護要件を満たしつつ、業務上必要な速度を確保した方法で、国境を越えて詐欺情報を共有するためのモデルフレームワークを策定する。これは政府間の多国間協定や規制当局間の相互承認協定などを通じて行われる可能性がある。金融活動作業部会（FATF）などの組織に対し、金融犯罪やマネー・ローンダリングとの闘いに不可欠な措置として、勧告16改訂のように、国境を越えた取引情報と補助情報のタイムリーな共有をポリシーに盛り込むための文言を提案する。

法的責任、義務、規制要件

いくつかの法域では、自主的な情報共有を超える規制上の義務が課されており、情報共有に参加するインセンティブが根本的に変化しています。

課題: 競争圧力により行動が妨げられる場合、自主的なアプローチでは十分な参加や投資が実現しない可能性があります。

手段: 法令および規制上の要件により、各業界の企業に対して詐欺防止および情報共有の義務が課され、基準を満たさなかった場合に重大な罰則と法的責任が生じます。

意図する効果: 企業は詐欺対策とセクターを越えた情報共有イニシアティブへの投資を増加させ、詐欺の特定と阻止の推進、詐欺による損失全体の減少、被害者の資産回復の促進につながります。企業は、重大な罰則に直面する可能性を踏まえ、リスクを軽減するために、自社の統制措置に投資し、上流と下流の他の参加者が情報を共有していることを確認します。

例:

- **シンガポール:** フィッシング対策の責任共有枠組みは、所定の詐欺防止および情報共有義務を遵守しない銀行や通信事業者に法的責任を負わせ、詐欺防止センターへの積極的な参加を促しています。
- **英国:** 「承認されたプッシュ決済(APP)」詐欺に対する払い戻し義務は、決済サービスプロバイダー(PSP)が詐欺防止に投資し、法的責任へのエクスポージャーを軽減するために情報共有に参加する金銭的インセンティブを生み出しています。
- **欧州連合(EU):** 第2次決済サービス指令(PSD2)の強力な顧客認証(SCA)要件と詐欺モニタリング義務は、基準のベースラインを構成しています。ただし、依然としてほとんどの情報共有は自主的に行われています。

トレードオフ: 義務は投資と参加を促進しますが、画一的になるリスクがあります。また、進化する詐欺の手口に迅速に適応できない可能性があります。義務が最も大きな効果を発揮するには、組織が成果ベースの要件を遵守するための方法を選択できるように、導入と柔軟性に関して業界の意見を取り入れることが必要です。

主な考慮事項: 自主的なアプローチが不十分である法域では、画一的な義務ではなく成果ベースの規制要件(詐欺による損失の削減、応答時間の改善、情報共有への参加など)を検討し、組織が柔軟に導入できるようにしながら、結果に対する明確な説明責任を負わせる。

自主的なインセンティブメカニズム

規制上の義務以外にも、法的要件によらずに情報共有への参加を促進するアプローチは複数存在します。

自主的な業界標準とコミットメント

課題: 詐欺対策の強化と情報共有への参加は、同一セクターの他の企業が同様の措置を取らない場合、競争上の不利になる可能性があります。

手段: 企業は、詐欺情報の共有を促進するための基準や要件に自主的にコミットします。こうした基準は、セクター内またはセクター間で適用され、業界団体、政府の奨励、または主要な組織の集団行動によって促進することができます。

意図する効果: 参加企業が十分に多い場合、競争上の不利が軽減されます。その結果、セクター全体の基準が向上します。また、元来は詐欺対策を強化する意向がなかった企業に対しても、政府、規制当局や一般の人々から「詐欺対策や顧客保護に取り組んでおらず、業界内で孤立している」というイメージを持たれることを避けるという理由で、圧力をかけることができます。これは、より大規模な情報共有イニシアティブへの第一歩となり得ます。

例:

- **英国:** 通信詐欺防止セクター憲章は、通信プロバイダーを団結させ、具体的な詐欺防止策と情報共有への取り組みを促進しています。
- **米国:** 米国銀行協会などの業界団体は、EWSやFS-ISACのようなイニシアティブを通じて、詐欺情報の共有を促進しています。
- **グローバル:** ペイメントカードネットワークの詐欺防止規則は、参加金融機関にとっての事実上の基準となっています。また、グローバル組織は技術的指標(GSEなど)の共有を可能にしています。

民間セクターのイニシアティブ

課題: セクターを越えた連携は困難です。法律、規制および業務上の課題への対処には時間とリソースが必要であり、個々の組織はそれを正当化するのに苦労しています。

手段: 民間セクターは、セクターを越えた詐欺情報の共有を促進および実行するための組織、団体またはグループを形成しています。政府はこうしたイニシアティブを認識、奨励または支持することができ、イニシアティブに参加する可能性もあります。

意図する効果: 組織はメンバーに代わり、課題をより効果的かつ効率的に共同で解決できます。これにより、詐欺をより迅速かつ正確に特定し、銀行口座の閉鎖、電話番号のブロック、オンライン口座やサイトの削除など、セクターを越えて詐欺を阻止するための行動を迅速化することが可能です。

例:

- **英国:** CIFASは、銀行、保険会社、通信会社、小売企業、政府から成る非営利会員組織で、詐欺リスクに関するデータと情報をリアルタイムで共有するための枠組みを提供します。
- **英国:** Stop Scams UKは、銀行、テクノロジー企業、通信企業をメンバーとする組織で、詐欺対策のためのセクターを越えた協力を促進しています。
- **米国:** NCFTAは、産業界、法執行機関、学界間のパートナーシップで、サイバー犯罪と詐欺に関する情報の共有を目的としています。

政府主導のイニシアティブ

課題: 民間セクターのイニシアティブは、詐欺の迅速な阻止と資産回復を可能にするための十分な権限、専門的な洞察、または法執行機関との連携が欠如している可能性があります。

手段: 政府は、公共セクターと民間セクターを結びつけ、多くの場合において物理的に同じ場所に配置し、詐欺関連の情報、洞察、インテリジェンスを共有するフュージョンセルとインテリジェンスハブを構築します。

意図する効果: 政府のリーダーシップは、信頼性の高い仲介者として、法令および規制上の不確実性を軽減できます。こうしたイニシアティブにより、政府は情報をより効率的に受け取り、共有し、政府の優先事項に沿って活動することが可能です。その結果、詐欺の阻止と資産回復の速度が向上し、政府が民間企業にフィードバックを提供しやすくなります。

例：

- **オーストラリア：全豪詐欺防止センター（NASC）**は、政府機関、法執行機関、銀行、通信プロバイダー、テクノロジープラットフォームを結びつけ、リアルタイムで情報を共有し、対応を調整しています。
- **シンガポール：詐欺防止センター（ASC）は、**銀行、通信プロバイダー、法執行機関の代表者が一堂に会する官民共同のイニシアティブとして活動しており、即時の情報共有と、詐欺を阻止するための協力を可能にしています。
- **英国：**JMLITと詐欺対策合同タスクフォースは、官民のインテリジェンス融合モデルを提供しています。

各アプローチにはそれぞれ強みと限界があります。政府主導のイニシアティブは、優先順位の向上と権限の拡大という利点をもたらし、より永続的な効果を持つことが多い一方で、適応性の高い短期的な脅威への対処に必要な俊敏性と適時性に欠けるという課題に直面しています。特に成功しているモデルは、セーフ・ハーバー条項によって基本的な法律を明確化し、業界が基準の策定や民間セクターのイニシアティブに取り組んで自主的にリーダーシップを発揮し、政府がフュージョンセンターを通じて取り組みを円滑化し、自主的なアプローチが不十分である場合に的を絞って法律上の義務を課すといった重要な要素を組み合わせています。

技術およびガバナンス要件

技術的なインフラストラクチャ

組織には、業務上の有用性、セキュリティ、プライバシー保護、導入の実現性のバランスが取れたインフラストラクチャが必要です。例えば：

- **短期的な情報共有の取り組みに関するいくつかの重要な要件：**
    - 安全な伝送チャネル（TLS、VPNなど）
    - 重要な識別情報の基本的な照合機能
    - フィールドの形式と意味を定義する明確なデータスキーマ
    - 権限のある担当者のみが情報を照会または受領できるようにするアクセス管理
    - 説明責任をサポートするための監査記録
    - 実施した行動を報告するためのフィードバックメカニズム
- **情報共有インフラストラクチャを支える可能性がある優先的な技術標準：**
    - 口座番号、電話番号、暗号通貨ウォレットアドレス、ドメイン、IPアドレスの一般的な識別情報フォーマット
    - セクター共通の一般的な詐欺犯罪類型のタクソノミー
    - 情報共有の信頼性と品質の指標
    - 行動と結果を報告するためのフォーマット
    - 二者間共有のためのAPI仕様
    - プライバシー保護手法に関するガイダンス（ハッシュ化、トークン化、各手法をいつ使用するかなど）

情報共有をただちに開始する機会：組織は、共通アルゴリズムの利用を追求し、単純なハッシュ化された識別情報からただちに情報共有を始めることができます。これにより、有意義なプライバシー保護が提供され、高度なインフラストラクチャや法務レビューを必要とすることなく、組織間の照合が可能です。

ガバナンス要件

中核的なガバナンス原則：情報共有の取り決めが最も効果的に機能するのは、共有環境全体で信頼性とセキュリティを促進する一連の原則に従う場合です。

- **相互性：**情報を受け取る組織は、情報を提供し、共有の際に適切な行動を取ることにコミットする必要があります。段階的な参加モデルは、小規模な組織にとっての公平性とアクセス性のバランスに寄与する可能性があります。
- **データの処理と保持：**情報共有の取り決めでは、共有された情報が保持される期間、その情報がどのように保持されるか、誰がアクセスできるか、いつ削除する必要があるかについて、明確な要件を定める必要があります。
- **使用時およびその後の共有に関する制限：**共有された情報は、詐欺防止および関連する目的にのみ使用されるべきです。その後の共有は、明示的な同意がある場合、または所定の共有コミュニティ内でのみ許可される必要があります。
- **監査と説明責任：**参加組織は、受け取った情報と実施した行動の記録を維持し、コンプライアンスを検証するための定期的なレビューを受け、参加者が取り組みの有効性を評価するのに役立つ全体的な結果を報告する必要があります。
- **フィードバックループ**情報の受領者は、共有情報に基づいて実施した行動と、達成した成果について報告する必要があります。
- **目的の明確性：**情報共有の取り決めは、その業務上の目的（詐欺防止、進行中の詐欺の阻止、資産回収、特定の前提犯罪に対する起訴の支援など）を明示的に定める必要があります。

ガバナンスモデルの選択肢：

- **二者間/ピアツーピア：**このモデルはシンプルで直接的な信頼関係に依拠していますが、拡張性は限定的です。
- **コンソーシアム：**このアプローチは、より広い範囲をカバーし、パターン検知を拡大できますが、より複雑なガバナンスを必要とします。
- **第三者の仲介者：**この選択肢は競争上の懸念を解消できますが、運用上の依存関係が生じます。

組織は単一の規範的なアプローチを追求するのではなく、具体的なユースケース、既存の関係性、セクターのダイナミクス、競争上の感応度に基づいてモデルを選択する必要があります。

主な考慮事項とロードマップ

タスクフォースは、組織が大規模な変革を経ることなく、意思を成果に転化するための実用的な取り組みに重点を置き、責任ある組織と協力して有意義な進歩を遂げるための基盤を築き、詐欺対策イニシアティブの持続的な拡大に必要な長期のシステミックな課題に対処しなければなりません。

タスクフォースが実施する可能性がある行動

1. 3つから5つの優先的な情報共有シナリオについて、**データ共有契約とユースケースのテンプレートを策定**し、正確なデータ要素、法的根拠、タイミング要件、保護措置、背景情報要件、実施可能な行動を文書化する。
2. 詐欺犯罪類型アラート、ハッシュ化された識別情報、インフラ指標、集計されたパターンの**迅速でスムーズな共有を促進**する。
3. **詐欺データツールキットと情報共有シナリオを開発**し、優先度の高い詐欺データ要素、その有用性とソース、情報共有のためのメカニズムとベクトル、相互運用性のための既存標準または必要な標準を示す。
4. 国境やセクターを越えた情報共有のために、**法的な明確化やセーフ・ハーバー条項が不足している点**を示し、その課題に対処するための取り組みを支援できるように政策立案者を関与させる。

おわりに

民間セクターの詐欺情報の共有は、新たな法的枠組みや大規模な技術変革を待たずに実現可能です。その進歩は、業務上の明確な価値を持つインパクトの大きいユースケース、組織が既存の法的枠組みの下で現実的に共有できる具体的なデータ要素、および透明性と相互性を通じて信頼を構築するガバナンスモデルに、当初の重点事項として取り組めるかどうかに左右されます。

組織は、スムーズに共有できる種類の情報と、シンプルな二者間の取り決めからただちにスタートし、より複雑な情報共有シナリオに向けた運用能力と信頼を構築する必要があります。タスクフォースの勧告は、現在の情報が分断された状況から、より体系的かつ拡張的で持続可能な情報交換へと移行し、詐欺による損失を大幅に削減するための道筋を提示しています。

ACAMSについて

ACAMSは、金融犯罪対策（AFC）教育、ベストプラクティス、ピアツーピア・ネットワーキングの機会を世界中のAFC専門家に提供する国際的な主要会員組織です。ACAMSは、マネー・ローンダリング/テロ資金供与対策、制裁措置に関する知識の共有、ソート・リーダーシップ、リスク軽減サービス、ESGイニシアティブ、官民対話のためのプラットフォームの提供を通じて、金融犯罪を撲滅するという使命に取り組んでおり、200以上の法域に11万人以上の会員を擁しています。

ACAMSのCAMS認定資格はAFCプロフェッショナルのためのグローバル・ゴールドスタンダードです。同時に、CGSS認定資格は、制裁のプロフェッショナルのためのプレミア・スペシャリスト資格です。ACAMSの世界で60を超える支部は、教育やネットワーキングのイニシアティブを通じて、協会の使命をさらに追及しています。