半期脅威動向レポート（2026年春期）

決済セキュリティに関する戦略的視点

Visa Network Defense

チーフ・リスクアンドクライアントサービス・オフィサー

ポール・ファバラ（Paul Fabara）からのメッセージ

不正対策は、防御側と攻撃側で繰り広げられる継続的な戦いです。ある領域で防御が強化されると、攻撃者は防御の手薄な領域へと攻撃の矛先を移します。その対象はインフラではなく、「人」であることが少なくありません。

過去6か月において、Visaはネットワークレベルでユニークな列挙攻撃のブロック件数を13%増加させるとともに、コアとなるセキュリティ指標においても明確な改善を達成し続けています。これは、ネットワーク規模での防御が機能していることを示す明確な証拠です。

しかしながら、セキュリティ施策が機能する一方で、脅威の性質自体が変化しています。攻撃者は標的を移しており、スキャム（詐欺）は消費者にとって最も急速に拡大しているリスクとなっています。これは高度ななりすましやAIを活用したソーシャルエンジニアリングによって加速しています。不正は、人を騙す手口の高度化、エコシステムの分断、そしてAIによって加速する攻撃サイクルといった課題へと変化しています。

今後、優位性を維持するためには、単なる個別のコントロール強化では不十分です。金融機関、加盟店、テクノロジープラットフォーム、政策立案者など、金融エコシステム全体にわたるシステムレベルでの共通アプローチが求められます。レジリエンスは、すべての参加者が関わるシステム全体の強さによって決まります。

本レポートでは、決済セキュリティを再構築しつつある構造的な変化と、それがデジタルコマースにおける信頼を守る責任を担うリーダーにとって何を意味するのかを提示します。

ポール・ファバラ（Paul Fabara）
チーフ・リスクアンドクライアントサービス・オフィサー

エグゼクティブサマリ

不正の性質は「技術侵害」から「行動操作」へと移行しており、決済セキュリティの在り方そのものの再定義を迫っています

認証の高度化、トークナイゼーションの普及、ネットワークレベルでの防御強化により、従来型の不正手口は抑止されています。しかし、こうした防御が強化されるほど、攻撃者は人、プロセス、サードパーティとの連携といった比較的防御の手薄な領域へと急速にシフトし、AIが活用され、欺瞞行為の拡大や攻撃サイクルの高速化が進んでいきます。

2025年後半においては、以下の4つの変化が決済セキュリティにおいて世界的な潮流を示しています。

攻撃件数は増加が続く中、基本的なセキュリティ対策は引き続き成果を上げている

詐欺が消費者被害の主たる要因となってきた

AIが攻撃と防御の双方を加速させている

ランサムウェアは依然として蔓延しているが、支払いに関する経済性は変化している

その結果、企業はトランザクション単位での不正検知に加えて、エコシステム全体での管理を強化する必要があります。その中核となるのは、スピード、連携、そしてAIを活用した異常検知です。

データが示すもの

- **コアセキュリティは改善：**デバイストークンの不正は前年比で9.6%減少し、列挙攻撃による損失は16%減少しました。これは、VisaのRisk Operation Centerが数千万件規模の不正の疑いがある取引をブロックしたことによるものです。
- **詐欺は主要な脅威に：**2025年7月から12月の間に、約10億ドル規模の詐欺関連の不正試行が確認されました。
- **AIが攻撃と防御の双方を再構築：**犯罪者はAIを用いて詐欺を大規模化し、攻撃プロセスを自動化しています。Visaを含む防御側もAIの活用を拡大し、より早い段階で攻撃を阻止し、被害の軽減に取り組んでいます。
- **ランサムウェア：攻撃は増加、支払いは減少。**2025年7月から12月にかけて、グローバルでのランサムウェアの活動は前年同期比で26%増加した一方で、身代金支払い率は23%と過去最低となりました。これは、多くの企業が「支払ってもデータ漏洩を防げない」という認識を持つようになったことによるものです。

それが意味するもの

- **セキュリティ上の失敗は、エコシステムの“境界”で発生するケースが増えています。**特に重大なものほど、目的や情報共有が分断されている組織間の境界で発生する傾向が強まっています。
- **不正はもはや主に認証情報の問題ではなく、行動の問題となっています。**認証の精度が向上するにつれ、攻撃者は正規の利用者を巧みに誘導して不正な取引を承認させる傾向を強めています。対策は「盗まれた認証情報を検知する」から、「**欺瞞を見抜き、阻止する」ことへと転換が求められています。**
- **AIの進展により、防御における「スピード」は、競争上、決定的な差を生む要素となっています。**手作業によるレビューや変化の遅いパターン分析に基づいて構築された防御モデルでは、機械の速度で動く攻撃者に対して十分な効果を発揮できません。
- **レジリエンスは予防と同等に重要です。**ランサムウェアの攻撃が増加している一方で、身代金の支払い率は低下していることから、事業継続性や復旧対応は、後付けの対応ではなく、主要なセキュリティ対策として位置付ける必要があります。

戦略的脅威ランドスケープ：決済セキュリティを再構築する4つの変化

SHIFT #1

セキュリティ対策は機能している。しかし、攻撃者はリソース配分を変えている

決済エコシステムは着実な進展を遂げています。攻撃活動が増加する中でも、トークナイゼーションの進展、認証の改善、ネットワークレベルでの検知高度化によって、測定可能な成果が出ています。トークン不正は、2025年7月から12月は、前年同期比で **9.6%減少**し、列挙攻撃による損失は **16%減少**しました。

示唆：

コアとなる対策が成果を上げているからといって、リスクが縮小しているわけではありません。むしろ、攻撃者が人やサードパーティ依存といった、より防御の手薄な領域へ移行していることを意味します。したがって、過去の結果を示す指標（不正損失額）から、次に不正がどこへ移行するかを示す先行シグナルへと軸足を移す必要があります。最も重要な問いは、もはや「どれだけ不正が発生したか」ではなく、「不正はどこへ移行しているのか、そしてそのスピードはどの程度か」です。結果として、今後はエコシステム全体の脆弱性、サードパーティ依存、そしてプロセスや設定上のギャップに焦点があてられることになります。

経営層にとっての戦略的検討事項：

- ✓ パフォーマンス指標は、単なる損失削減ではなく、リスクの移行に重点を置く形へと再設計する。すなわち、不正の試行と損失がチャネル、ユースケース、地域間でどのようにシフトしているかを把握する。
- ✓ 「境界」に重点を置いたコントロールを優先する：加盟店オンボーディング管理、プラットフォームの健全性確保、本人確認、そしてパートナー間の連携強化。
- ✓ 将来を見据えた脅威インテリジェンスおよび分析を、不正対策オペレーションの中核機能として組み込む。

SHIFT #2

詐欺が消費者向け脅威の中心となっている

詐欺は現在、消費者向け不正の中で最大かつ最も急成長しているカテゴリーです。2025年7月から12月には、**約10億ドル規模**の詐欺関連活動が確認されました。AIはこの動きをさらに加速させており、攻撃者は欺瞞的な手口を拡大し、かつ高度化させることが可能になっています。AI生成コンテンツ、音声のなりすまし、ディープフェイクといった技術は、悪意ある攻撃者によって利用された場合、詐欺の到達範囲と信頼性の双方を高める可能性があります。

示唆：

詐欺対策は、オーソリゼーションレベルでのコントロールだけでは解決できません。取引の観点ではユーザーの行動が「正当」に見える場合、詐欺対策は本人確認、意図の評価、操作・誘導の検知を組み合わせることが必要不可欠となります。さらに、多くの場合、単一機関の枠を超えた連携した対応が必要となります。

経営層にとっての戦略的検討事項：

- ✓ なりすましのパターン、詐欺に関与する加盟店エコシステム、高リスクの流入経路（検索、広告、SNS等）を特定することを目的とした「欺瞞防御」能力を構築する。
- ✓ 顧客とのコミュニケーション自体をセキュリティコントロールの一部として位置付け、信頼できる連絡手段の確立、確実な本人確認、および顧客対応における明確なルールの設定を徹底する。
- ✓ エコシステム全体のパートナー間でインセンティブおよびエスカレーション経路を整合させ、詐欺ネットワークの迅速なテイクダウン（排除）を可能にする体制を構築する。

戦略的脅威ランドスケープ：決済セキュリティを再構築する4つの変化

SHIFT #3

AIにより、不正の発生から検知・対応に至るまでのサイクルが短縮している（攻撃側・防御側の双方で）

AIは、不正の攻撃と防御の双方に変革をもたらしています。攻撃者はAIを用いて、個々の対象に合わせた説得力の高い詐欺を生成し、プロセスを大規模に自動化し、手口を迅速に反復・適応させています。防御側はAIを用いて、より早い段階で異常を検知し、攻撃が消費者や加盟店に到達する前に阻止し、検知の精度を向上させています。

戦略的な変化の鍵は「スピード」です。攻撃はより速く反復し、より速く拡大し、より速く適応します。ランサムウェア領域では、AIツールによって攻撃タイムラインが「数日」から「数分」へと圧縮されています。

示唆：

手作業かつ分断されたレビューモデルに依存する組織は、構造的に不利になります。優位性を持つのは、リアルタイムに対応でき、パートナー間で迅速に連携でき、検知、優先度判断、対応のプロセスを自動化できる組織です。

経営層にとっての戦略的検討事項：

- ✓ 機械レベルのスピードに対応した統制へと刷新する：検知・優先度判断・対応の自動化、引き継ぎ工程の削減、迅速な介入を可能にするための明確な権限付与。
- ✓ 音声・映像の合成、ならびに高度に個別化された誘導に耐性を持つ認証および検証手法への投資を強化する。
- ✓ 主要なステークホルダー間で連携し、組織横断（クロスパートナー）で共同の意思決定と対応を行う体制を構築する。

SHIFT #4

ランサムウェアは増加しているが、経済性は変化している

ランサムウェアのインシデントは引き続き増加しています（2025年7月から12月は、前年同期比で 26%増加）。一方で、被害者が身代金を支払う頻度は低下しています（同期間の支払い率は 23% と過去最低）。さらに、平均支払い額も減少しています（2025年7月から9月は、2025年4月から6月と比べて 66%減少）。これは、企業の対応力（レジリエンス）の向上に加え、「支払いを行ってもデータ公開を確実に防げない」という認識の広がりを反映しています。

示唆：

ランサムウェアは、単なる予防の問題ではなく、レジリエンスおよび復旧の課題として捉える必要性をますます強めています。迅速に復旧し、被害の拡大を抑えることができる組織は、被害の大きさと攻撃者の交渉力の双方を実質的に低減できます。

経営層にとっての戦略的検討事項：

- ✓ 復旧目標時間(RTO)およびバックアップの完全性を、取締役会レベルで管理すべき重要指標として位置付ける。
- ✓ セキュリティ基準の徹底、外部との連携・接続の監視、および迅速な通知体制の整備を通じて、サードパーティ起因の影響範囲を最小化する。

Visaはどのように支援するか — 規模で決済エコシステムを守る

デジタル決済における信頼の保護には、規模を伴う取り組みと、組織および地域を超えた連携が不可欠です。Visaは、ネットワーク全体を俯瞰したインテリジェンス、リアルタイムの防御機能、そしてエコシステム全体での連携を組み合わせることで、決済エコシステムの保護において独自の役割を果たしています。

Visaは以下を通じて決済エコシステムを保護しています：

リアルタイムの取引モニタリング

ネットワーク全体にわたる継続的かつAIを活用したモニタリングにより、新たに出現する脅威を検知・遮断し、不正が消費者、加盟店、金融機関に到達する前に防止します。

大規模攻撃のネットワークレベルでの遮断

集中化された可視性により、Visaは加盟店・国境をまたぐ組織的な攻撃パターンを特定し、ネットワーク全体で防御策を適用することが可能です。これは単一の機関では実現できない対応です。

専任の詐欺対策機能

詐欺ネットワークの特定・調査・解体に特化した専門チームが、わずか6か月で約10億ドル規模の詐欺活動を特定するとともに、不正に関与する加盟店や関連インフラの排除を加速させています。

エコシステム全体での連携

銀行、加盟店、テクノロジーパートナー、そして各国の法執行機関との継続的な連携により、世界中で多数の被害に関連する犯罪ネットワークを阻止し、攻撃の再発を抑制するとともに、被害の拡大を防ぎます。

主要指標および定義（方法論抜粋）

本エグゼクティブ版は、2025年後半の動向に基づき、ネットワークレベルでの攻撃遮断、詐欺の特定活動、ランサムウェアの動向のモニタリング結果を反映しています。主要指標には、トークン不正の推移、列挙攻撃による被害及び遮断の動向、2025年7月から12月に特定された詐欺活動、ならびにランサムウェアの発生および支払いに関する動向が含まれます。