

RSA eFRAUDNETWORK

不正データのグローバルリポジトリにより、検出件数が増加

世界的な金融機関の事例で、以下のことが示されました。

- 四半期で250万ドルを超える不正の削減を、eFraudNetworkだけで実現しました。*
- eFraudNetworkの偽陽性率は低く、0.4%でした。**
- 介入率はわずか0.12%でした（取引のチャレンジまたは拒否）。

RSA eFraudNetworkは、組織が150以上の国で不正（または不正未遂）に関与していたIPアドレス、ミュール アカウント、デバイス（モバイルを含む）、業者、その他のインジケーターやパターンをプロアクティブに特定できるように支援します。RSA eFraudNetworkは、業界初で最大規模の組織間、プラットフォーム間、国際的な共有オンライン不正防止ネットワークです。このネットワークは数年前から存在しており、金融機関、クレジットカードやデビットカードの発行会社、医療機関、通信会社、小売業者、ISP、ワイヤレス プロバイダー、ハイテク企業、政府機関、法執行機関など、何千もの組織や機関が世界中で貢献しています。

共有不正インテリジェンスを使用すると、組織は既知のサイバー犯罪者に対してプロアクティブに対策を立てて、損失の発生を防ぐことができます。RSAは、お客様、ISP、サードパーティーの協力者による広範なネットワークを通じて、不正および不正の試行を監視および追跡します。ある組織で不正が確認されると、不正取引のさまざまな要素（IP、ハッシュ化された国際銀行口座番号（IBAN）、デバイス要素など）がeFraudNetworkで共有されます。eFraudNetworkの不正インテリジェンス情報はIPブラックリストよりもはるかに多く、eFraudNetworkの貢献的なパートナー、RSA Fraud and Risk Intelligenceのお客様、RSA Anti-Fraud Command Center（AFCC）のアナリストによって継続的に更新されます。

eFraudNetworkのインテリジェンスは複数のソースから提供されるだけでなく、IPアドレス、デバイスフィンガープリント、cookie、ミュール アカウント、モバイル デバイスIDなど、さまざまなタイプのデータ要素も含まれます。これらの要素は、eFraudNetworkの情報が適時かつ正確であることを保証するために、最新のリスクレベルに従って継続的に特定、評価、スコア付けされます。

eFraudNetworkアルゴリズムは、確認された（および偽の）不正に関するケース管理フィードバック、独自の認証フィードバック ループ、頻度に基づいて、これらすべてのデータ要素の有効期限とリスク スコアを動的に設定します。このインテリジェントなスコアリング方法は、機械学習アルゴリズムを使用した不正対正規の比率と頻度に基づいており、eFraudNetworkの有効性を高めます。

eFraudNetworkは信頼性の高いデータ ソースです。個人を特定できる情報は共有されず、すべてのデータはリポジトリに追加される前に消去されます。

* eFraudNetworkに含まれていた要素を含む不正取引

** eFraudNetworkの要素が含まれているが、最終的に「confirmed genuine（正規として確認）」とマークされた取引

「RSA eFraudNetworkサービスとの提携により、不正防止テクノロジーに関する収益と包括的な不正戦略の開発が加速されました。実際、1つのプロジェクトとして始まったことが、現在では銀行の他の分野にまで広がり、さらに発展していくのは、非常に大きな成果です。」

— 不正戦略マネージャー

数字で見るeFRAUDNETWORK

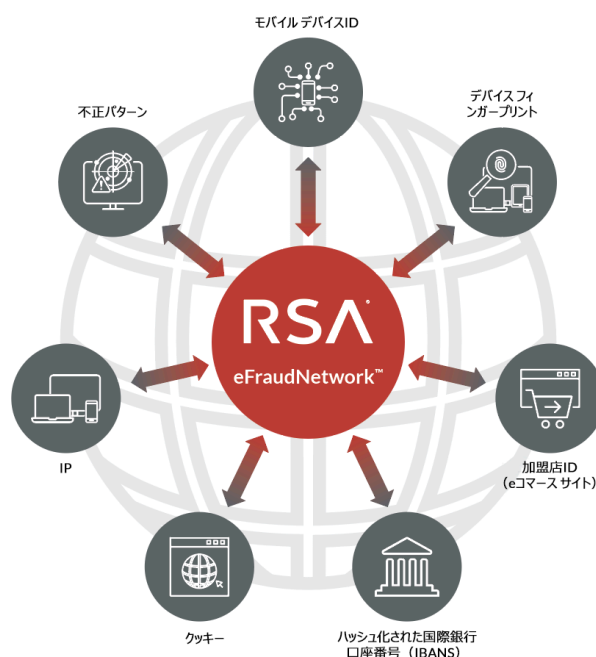


*お客様をマーキングする主要な不正行為における平均

** 2018年のデータに基づく

- RSA eFraudNetworkに貢献している数千もの直接的および間接的なお客様が、不正インテリジェンスを毎日確認しています。
- 確認された900万件の不正取引からの不正な要素が毎日提供されています。
- 32万を超える要素が日次フィードにマーキングされ、お客様間の不正取引の重要な相関関係が示されます（異なるお客様からの取引に同じ不正要素が存在すると、これらが実際に不正に関連している可能性が高くなるため）。
- 年間5,500万件を超える取引には、eFraudNetworkで共有された要素が含まれています。
- RSA eFraudNetworkは、RSA Fraud & Risk Intelligenceの顧客ベースを対象に、年間3億5,000万ドルを削減しました。
- eコマースのお客様向けのRSA Adaptive Authenticationでは、平均誤検知率はわずか0.6%です（eFraudNetworkの要素を含むが、「Confirmed Genuine（正規として確認）」としてマークされた取引）。

集会的不正インテリジェンスのパワー



eFraudNetworkエコシステムのパワーは、すでに発生した不正のデータ要素を取得し、ネットワーク全体でそのインテリジェンスを利用できるようにする能力を根源としています。

RSA Fraud and Risk Intelligenceのお客様は、eFraudNetworkに自動的に登録することができます。リアルタイムの不正の脅威に関する直接フィードがRSAリスク エンジンによって活用され、RSA Adaptive Authentication、RSA Adaptive Authentication for eCommerce、RSA Transaction Monitoringを駆動します。eFraudNetworkに不正として表示されているデバイス、IPアドレス、その他の要素によってトランザクションまたはアクティビティが試行された場合、全体的なリスク スコアに反映されます。さらに、eFraudNetworkの要素は、それぞれのソリューションのポリシー マネージャーで直接参照できます。

接続し、共有された情報は、サイロ化および切断された環境よりも優れたセキュリティを提供します。RSA eFraudNetworkを使用すると、世界中の何千もの組織のコミュニティーから収集された累積的な詐欺インテリジェンスの恩恵を受けることができます。

RSAについて

RSAはBusiness-Driven Securityソリューションを提供し、さまざまな組織が、統合的な可視性、自動化されたインサイト、および組織的なアクションを使用してデジタル リスク管理のための統合的なアプローチを採用できるようサポートしています。RSAのソリューションは、高度な攻撃の効果的な検出と対応、ユーザー アクセス制御の管理、さらにビジネス リスク、不正行為、サイバー犯罪の削減を目的として設計されています。RSAは、世界中の数百万人のユーザーを保護し、Fortune 500の企業の90%以上が成功し、革新的な変化に継続的に適応できるように支援しています。詳細はrsa.com/ja-jpをご覧ください。