LexisNexis®
RISK SOLUTIONS

ホワイトペーパー

LexisNexis® Risk Solutionsを使用して、3Dセキュアのカスタマージャーニーにおけるリスク判定を強化

オンライントランザクションを利用する顧客が急増

デジタルコマースはグローバル経済を成長させた主な推進要因の一つであり、オンライン消費者はデジタルコマースを通じて、場所や時間を問わず、商品やサービスにアクセスすることができます。これは世界的規模でインクルージョンを促進する一方で、販売業者、イシュアー、アクワイアラーに対し、競争の激しいオンライン市場で顧客に負担をかけることなく、本人確認と取引認証を行うという課題をもたらします。

タイミングの悪いステップアップ認証や過度に厳しい認証戦略により、得意客や時々利用する消費者が別のオンラインサイトに乗り換えてしまうリスクが生じます。しかし、堅牢なセキュリティ手順を設けなければ、企業は手に負えないほど不正率が上がる可能性があります。

オンラインジャーニー全体にわたり、正規の顧客と潜在的なサイバー犯罪者を確実に識別する能力を活かして、効果的かつ顧客に負担をかけないバランスの取れた不正制御戦略を実現することが、ビジネス成長にとって必要不可欠です。

3Dセキュア（3DS）認証プロトコルにデジタルアイデンティティ・インテリジェンスを導入

3DSプロトコルは、eコマース取引中にカード所有者を認証するために、アクワイアラーをイシュアーにリンクする安全なフレームワークを提供します。2018年に更新され、モバイルコンポーネントが含まれるようになりました。これにより、セキュリティを損ねることなく、顧客体験がさらに合理化されました。

3DS 2.xのメリット

- 顧客の負担が少ない認証プロセス
- モバイルブラウザおよびモバイルアプリの両方と統合したモバイルフレンドリーな仕様
- 販売業者がイシュアーと共有できるデータポイントは、従来の15ポイントから150ポイントに増加
- 柔軟なオプトアウト・ポリシー

3DS　2.xの適用範囲の拡大により、、販売業者は150のデータポイントをイシュアーと共有できるようになり、イシュアーはより多くの情報に基づいたリスク判定ができるようになりました。この拡大範囲を十分に活用するカギは、業界、チャネル、プラットフォーム全体にわたり、世界的規模で最も関連性の高い最新のインテリジェンスを利用することです。

ほぼリアルタイムで更新されるグローバルインテリジェンスのネットワークを活用

これまで、不必要な手間とパスワードへの過度な依存が非難の的となっていたため、イシュアーは現在、高い承認率の維持と顧客体験の合理化とのバランスをいかに取るかという課題に直面しています。

したがって、イシュアーとACSプロバイダはカード所有者をほぼリアルタイムで認証するために、最も包括的で適切なインテリジェンスにアクセスし、追加のステップアップ認証を最小限に抑え、必要に応じて顧客に手間をかけない認証戦略の使用を最適化する必要があります。

LexisNexis® Risk Solutionsは、数千社の企業から、500億件を超えるグローバル・トランザクションに関する情報を活用し、ほぼリアルタイムで更新されるデジタルアイデンティティ・インテリジェンスを介して、競争上の優位性を提供します。

LexisNexis® Digital Identity Network®

3DS 2.xとの初めてのインタラクション時でも、カード所有者のデバイス、場所、メールアドレス、オンライン行動に履歴コンテキストを添付できることが、成功のためには不可欠です。

LexisNexis® Digital Identity Network®から入手可能なインテリジェンス

デジタルアイデンティティ・インテリジェンス

- 信用、リスク、異常、関連付けられたアイデンティティ、デジタルアイデエティティの経年、メールのリスク評価、アイデンティティデータ

デバイス・インテリジェンス:

- 3種類の異なるデバイス識別子、オペレーションシステム、モデル、ブラウザ、プラグインなどのデバイスの特徴

ロケーションインテリジェンス:

- 国、都市、接続タイプ、VPN、TOR、プロキシの有無

スレット・インテリジェンス:

- マルウェア、リモートアクセス型トロイの木馬（RAT）、エミュレータ、クローンデバイス
- 確認された不正行為のグローバルリスト、ブロックリスト、マネーミュール

行動インテリジェンス:

- 身ぶり、行動上の変化、マウスの動き、特殊キー
- 金額、速度、受益者の詳細、時間などのトランザクションの詳細

LexisNexis® Risk SolutionsとACSプロバイダーの統合を通じて、より多くの情報に基づくリスク判定を実現

Digital Identity Network®からのインテリジェンスは、非対面（Card-not-Present, CNP）の3DSカスタマージャーニー全体にわたる信用とリスクに関するより明確な全体像を提供します。一連のアクセス・コントロール・サービス（ACS）プロバイダーとの協力により提供されるこれらの不正検出　認証機能は既に、多くの発行銀行/ 金融機関が一連のアクセス・コントロール・サービス（ACS）プロバイダーと提携して、効果的に使用されています。

以下の3つの統合オプションをご提供：

1. LexisNexis® Risk Solutionsが（LexisNexis® ThreatMetrix®製品を介して）第三者のACSに対する主要不正リスク判定エンジンとしての役割を果たす
2. LexisNexis® Risk Solutionsがリスク判定を補強するために、既存のACS不正リスク判定エンジンに対する追加データフィードとしての役割を果たす
3. LexisNexis® Risk Solutionsが3DSチャレンジジャーニー に基づくソリューション内の認証レイヤーとしての役割を果たす

1. 主要な不正リスク判定エンジンとしての役割を果たす

LexisNexis® ThreatMetrix®は、3DSエコシステム内で、ACSプロバイダーに対する不正リスク判定エンジンとして使用することができます。ThreatMetrixは、オンラインのカスタマージャーニー全体にわたり機能するID検証/ 不正防止/ 認証ソリューションです。これは、新規口座開設の検証やアカウントのライフサイクル管理トランザクションの認証を行い、信頼できるユーザーと潜在的な脅威を確実に識別することができます。

メリット

- イシュアーは3DSジャーニー中にThreatMetrixテクノロジーを利用することで、ほぼリアルタイムで更新されるグローバル・デジタルアイデンティティ・インテリジェンスからメリットが得られます。
- 販売業者からACSに送信されるデータ（Areq：認証要求）を消費する機能に加えて、ThreatMetrixはDigital Identity Networkからの専有データを利用して、意思決定プロセスを補強します。上述のように、このデータには詳細なデバイス、位置情報、行動、脅威に関するインテリジェンスが含まれています。
- ThreatMetrixはこのデータを使用して、トランザクションを行うすべてのユーザーに対する個々のデジタルアイデンティティを作成し、各カード所有者が通常オンラインでインタラクションを行う方法を詳細に把握することができます。
- ユーザーのデバイスの傾向、場所の傾向、平均的な決済金額、通常の配送先、IP近接などを把握することで、全体的かつ完全な不正リスクと信頼性の評価が可能になります。
- さらに、イシュアーはThreatMetrix Decision Management Portalを使用して、3DSトランザクションのリスクを管理するための独自の戦略を構築および設定することができます。これらの戦略は一連のルールで構成され、トランザクション内で特定の情報を検索し、定量条件が満たされる場合は、リスク加重を適用するか、一定の措置を講じます。

ACSサービスとThreatMetrixを連携させるメリットは一目瞭然です。リスク評価中に生成された追加データを利用することで、不正検出の可能性を高めると同時に、正規のユーザーには余分な手間のかからないチェックアウト体験を提供することができます。

2. 既存のACS不正リスク判定エンジンに対する追加データフィードとしての役割を果たす

3DS CNPリスク判定は通常、販売業者から発行銀行に提供されるデータであるAreq（認証要求）内で提供されるデータポイントを使用して行われます。また3DS 2.x仕様ではAreqの範囲が拡大され、よりコンテキスト化されたデータ交換が可能になり、イシュアーが確実に不正判断を下せる可能性がさらに高まっています。

これに加えて、3DS 2.xプロトコルはクレジットカード会社に対し、メソッドURLプロトコルを介してカスタムデータを収集する絶好の機会を提供しています。このデータは、リスク評価判定能力をさらに強化するために使用できます。メソッドURLでは、ブラウザを介して、強化されたデバイス認識、デジタルIDのプロファイリング、位置情報分析、脅威/ 異常検出の利用が可能になります。

メリット

- メソッドURLを介してThreatMetrixの機能を導入することで、ThreatMetrixはThreatMetrixルールエンジンを通じて分析可能な何百もの追加データポイント（上記に説明した通り）を生成することができます。
- このデータは、イシュアーのACSの全体的なCNP判定能力を補強するために使用することができ、不正検出率の向上と誤検出の低減を実現します。
- ThreatMetrixはACSプロバイダーの既存の不正検出エンジンに対し、生データだけではなく、最適化されたスコア付きのリスク評価も提供することができます。
- ThreatMetrixのデータを既存のACSエンジンに入力することを選択した場合、イシュアーはよりコンテキスト化されたリスク判定を行い、カード所有者に余分な手間をかけずに、不正検出率を向上させることができます。

3. 3DSチャレンジジャーニー内の認証レイヤー

LexisNexis Risk Solutionsは、3DSチャレンジジャーニーをサポートする一連の認証戦略を備えています。これらを階層化することで、コスト効率的で顧客に余分な手間をかけない認証ジャーニーを最適化し、比較的コストのかかる高リスクのトランザクションに対するステップアップ認証に備えることができます。

デバイスバインディング: ThreatMetrix Strong IDはエンドユーザーのウェブ/モバイルブラウザ/アプリとThreatMetrix間の暗号化ビッドを生成して、持続的かつ安全なデバイス認識を実現します。これは現在、SCAワークフローの一環として、数社の組織で使用されています。

- **最初のバインド後の静的な低摩擦**
- **大量のトランザクションの場合に非常に高いコスト効率性**

SMS OTP: 帯域外（OTP）認証方式は、SMS、メール、電話を介した時間依存の一意のランダムなパスコードを提供します。これはSIMスワップ/リダイレクトおよびデータ移植により保証されます。

- **安全**
- **モバイルアプリを登録していない顧客も使用可能**
- **動的リンクを含めることが可能**

プッシュ通知: ブラウザベースのトランザクション中の帯域外認証として、エンドユーザーのモバイルデバイス、特にモバイルアプリを利用します。これは、標準のiOSまたはAndroidの安全なプッシュ通知サービスを使用します。

- **モバイルアプリを登録している顧客に余分な手間をかけない**
- **動的リンクを含めることが可能**

ナレッジベースの認証（KBA）: インテリジェントなアルゴリズムを使用して構築され、数十億件もの消費者の記録にアクセスするKBAは、ユーザーの身元を認証するために、個人的な質問と複数の回答を動的に作成します。

- **パスワードを思い出す必要がない、個人的な知識による認証**

LexisNexis® TrueID®: ユーザーの身分証明書をスキャンした後に、その身元が検証され、TrueIDデータベースに登録されます。

- **信頼できる物理的エンティティの認証**

行動バイオメトリクス: SMS　OTPのインプット時に収集された行動バイオメトリクスデータを使用して、3DS 2.xワークフローでカード所有者の二要素認証を提供します。

- **別の準拠認証戦略と重ね合わせた静的な低摩擦アプローチ**
- **大量のトランザクションの場合に非常に高いコスト効率性**

ホワイトペーパー

結論

LexisNexis® Risk Solutionsと連携することで、不正判定の際にACSプロバイダーが利用できるデータを強化することができます。またThreatMetrix製品は、必要に応じて、主要なトランザクションリスク評価エンジンになり得ます。オンラインバンキングセッションを保護するために世界中の多くの金融サービス組織で既に導入されているソリューションとして、ThreatMetrixをACSフロー内に組み込むことで、すべてのデジタルバンキングチャネルにわたってより緊密にインテリジェンスを共有し、銀行全体で顧客の全体像を一元化することができます。

LexisNexis® RISK SOLUTIONS

LexisNexis® Risk Solutionsの不正/アイデンティティ管理ソリューションの詳細については、risk.lexisnexis.co.jp/products/digital-identity-networkにアクセスしてください。