





3DS 2.xの対象範囲が拡大したために、販売業者は150のデータポイントをイシューアと共有し、より多くの情報に基づく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、世界的規模で、業界、チャネル、プラットフォーム全体にわたり、最も適切かつ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的となっていたため、イシューアは現在、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。

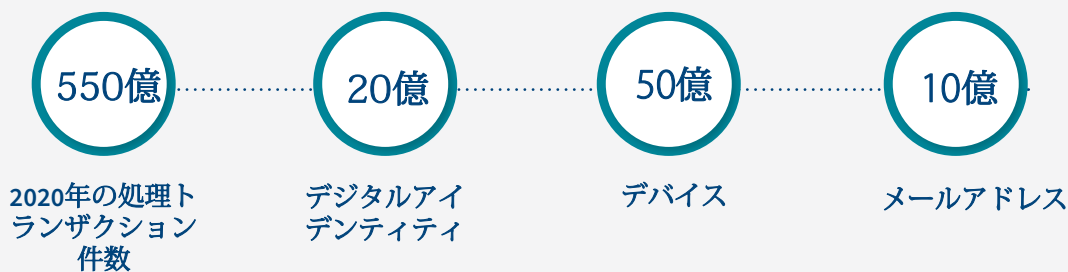
したがって、イシューアとACSプロバイダーは最も包括的で適切なインテリジェンスにアクセスして、ほぼリアルタイムでカード所有者を認証し、追加的なステップアップ認証を最小限に抑え、必要に応じて顧客に手間をかけない認証戦略の使用を最適化する必要があります。

LexisNexis® Risk Solutionsは、数千社のグローバルなデジタル企業からの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追加する能力は、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、変則性、関連付けられたアイデンティティ、デジタルアイデンティティの経年、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、オペレーティングシステム、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の存在、TORとプロキシ



### 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（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 金融機関により効果的に使用されています。

### The Three Integration Options Are:

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アイデンティティ検証 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

- イシューアは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、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、場所、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、イシューアは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構成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、イシューア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、デジタルアイデンティティのプロファイリング、ロケーション分析、脅威 変則性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、イシューアの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ます。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、イシューア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、比較的成本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



## 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ン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](https://risk.lexisnexis.co.jp/products/digital-identity-network)にアクセスしてください

### LexisNexis Risk Solutionsについて

LexisNexis® Risk Solutionsは、データの力と高度な分析を活用して、企業や政府機関がリスクの軽減と意思決定の向上を通じて世界中の人々の利益を守るために役立つ洞察を提供します。当社は保険、金融サービス、医療、政府部門を含む広範な業界にデータとテクノロジーソリューションを提供しています。ジョージア州アトランタの都市圏に本社を置く当社は世界各地に事務所を擁しており、あらゆる業界のプロフェッショナルな法人顧客向けの情報ベースの分析と意思決定ツールのグローバルプロバイダであるRELX Group (LSE: REL/NYSE: RELX) の一部門です。詳細については、[www.risk.lexisnexis.com](http://www.risk.lexisnexis.com)および[www.relx.com](http://www.relx.com)にアクセスしてください。

本文書は教育目的のためにのみ作成されたものであり、特定されたLexisNexis製品の機能または特長を保証するものではありません。LexisNexisは、本文書が完全である、または誤植がないことを保証いたしません。

LexisNexisおよびKnowledge BurstのロゴはRELX Inc.の登録商標です。その他の製品およびサービスは各企業の商標または登録商標である場合があります。 .  
© copyright © 2021 LexisNexis Risk Solutions Group. NXR14848-01-0122-JP