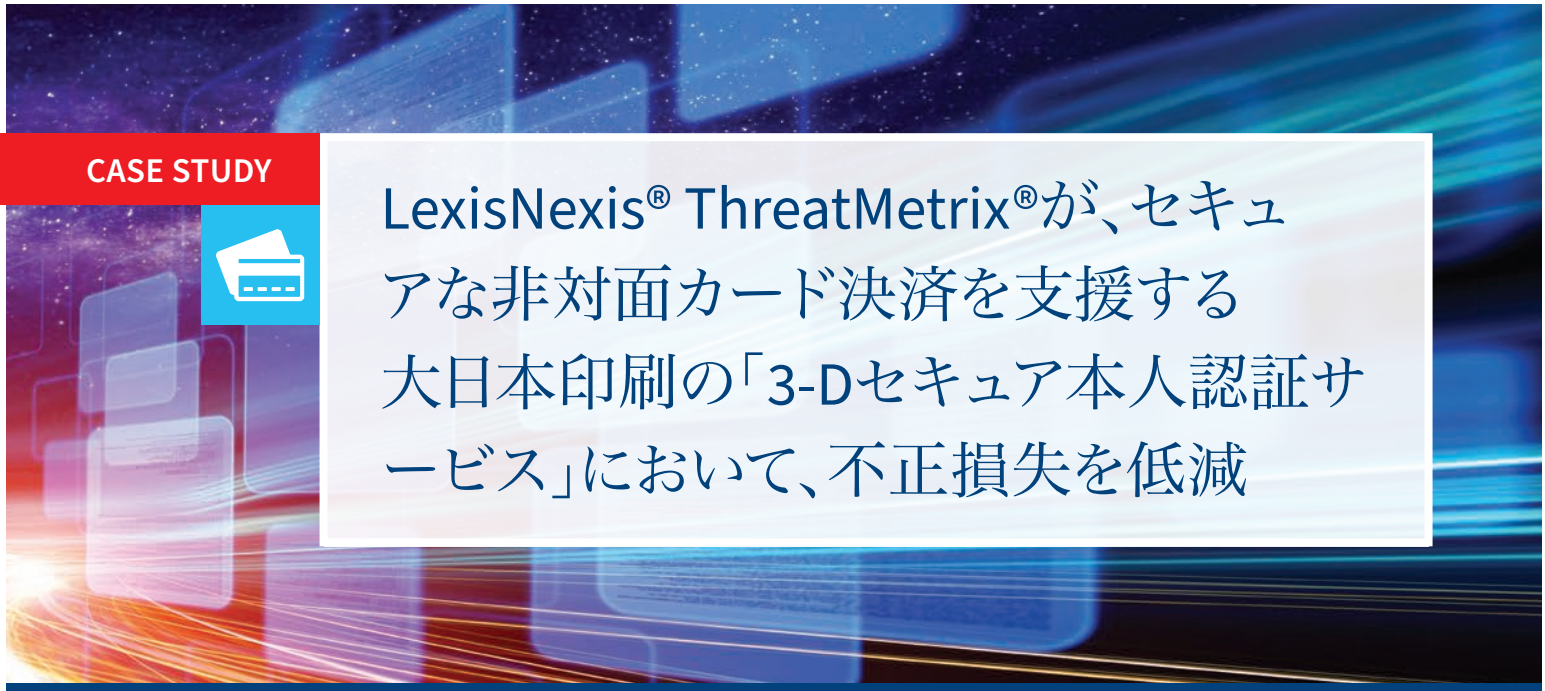
LexisNexis®
RISK SOLUTIONS



CASE STUDY

LexisNexis® ThreatMetrix®が、セキュアな非対面カード決済を支援する大日本印刷の「3-Dセキュア本人認証サービス」において、不正損失を低減

概要

顧客

DNP

大日本印刷 (DNP)

要件

- 非対面カード決済における不正取引の低減
- クレジットカード会社に対する不正損失の低減
- カスタマイズが簡単で、強力なルールエンジンの導入
- 他の3-DセキュアACSプロバイダとの差別化要因となる機能強化

ソリューション

DNPは、LexisNexis® ThreatMetrix®のリスクベース認証を使用して、自社の3-Dセキュア(3DS)ワークフローの一部であるリスク判定の強化を図っています。日本のカード会社に対してアクセス制御サーバ(ACS)としての機能を提供しているDNPは、ほぼリアルタイムで高リスクの取引を特定することができ、カード会社が非対面カード決済取引を承認、拒否またはステップアップするかどうかの判断を支援しています。DNPはカード会社に対して LexisNexis® ThreatMetrix®サービスを提供しており、各カード会社は自社の決済ワークフローにリスクベース認証を実装し、ルールとリスク許容度を調整することができます。

重要点

- 信頼できるカード会員からの低リスクの決済取引は、余分な手間をかけずに認証することができる。不要な認証を減らすことにより、真に高リスクのケースに集中できるよう、不正対策部門の作業負荷を最適化することができる。
- カードが初めて使用されたか、または3DSパスワードが登録されているかどうかを問わず、オンライン決済に対する信頼できるリスク評価を提供することができる。
- LexisNexis ThreatMetrixソリューションでは、カード会社はグローバル・デジタル・アイデンティティ・インテリジェンスを利用し、DNPとのパートナーシップを介して、取引認証の基準をそれぞれのニーズに合わせて変更できる。
- 各カード会社は、それぞれの事業戦略に合った不正対策を反映させた、柔軟でカスタマイズされたルールを導入することができる。
- カード会社はLexisNexis® Risk Solutions Consortiumの機能を使用して、確認された不正に関する情報を、DNPとパートナーシップ関係にある他のカード会社との間で共有することができる。
- これらにより、不正の割合と不正による損失額が大幅に減少した。

CASE STUDY

「*ThreatMetrix*のソリューションにより、新たに出現する不正の脅威の特定を支援し、効果的なリスク低減、戦略を提示することで、当社はカード会社に最適なサービスを提供することができます」— DNP

概要

DNPは1876年創業の総合印刷会社です。P&I（印刷と情報）の強みを活かして包材や建材、エレクトロニクスなど、さまざまな分野に事業領域を拡大し、環境やエネルギー、ライフサイエンスなどの事業にも注力しています。情報イノベーション事業部では、デジタルマーケティングの推進やキャッシュレス決済関連の事業の拡大に注力するほか、人手不足や働き方改革の対策のひとつとして、企業等の業務を代行するBPO事業などを推進しており、マーケティング・決済・認証サービス事業において、国内で多くの実績を誇ります。

決済・認証サービス事業の一部として、DNPは3DS認証ソリューションを提供しており、3DSプロトコルを使用して非対面カード決済取引を認証するクレジットカード会社向けのACSプロバイダとしての役割を果たしています。顧客企業との対話の中で、DNP、カード会社がより多くの情報に基づきリスクを判断し、不正による損失を減らす必要性があり、効果的なリスクベース認証機能により支援できると考えました。これは特に、非対面でのカード決済取引で不正行為が世界的に拡大していることを鑑みると、時宜にかなったものでした。

DNPはLexisNexis ThreatMetrixが提供するサービスを採用することで、以下を実現しています。

- **クレジットカード番号やパスワードに加えて、デバイスの情報、現在および過去のユーザーの行動、位置データ、取引の詳細に関するデジタル・アイデンティティ・インテリジェンスを利用して、取引のリスク評価を行う。**
- **ほぼリアルタイムで、信頼できる取引と高リスクの取引を区別する。**
- **市場の要件と進化する脅威に合わせて、ルールとリスクスコアを調整する。**

CASE STUDY

ビジネス上の問題

電子決済は消費者の取引方法を抜本的に変え、今では日本市場におけるキャッシュレス取引の割合は増加の一途をたどっています。しかし、不正利用者はデジタル決済がもたらす機会を悪用しようとするため、この消費者行動の変化に伴ってリスクも高まります。

カード会社は、ますます高度化するなりすまし手法(多くの場合は盗難によりなりすまされた認証情報一式)を使って、正規のカード会員になりすまそうとしている不正利用者の存在に関する懸念を、ACSプロバイダとしてのDNPに対して表明していました。

カード会社は深刻化する不正取引問題とそれによる損失の増大に直面していました。主な課題は、盗まれたパスワードおよびクレジットカード情報を所有している不正利用者が、標準的な認証チェックをすり抜けてしまうことでした。

DNPは、静的データのみではなく動的でほぼリアルタイムのデジタルアイデンティティデータを活用して、カード会社による高リスク取引の検出をサポートする手段を必要としていました。DNPは、盗まれたクレジットカードを使用した支払い、以前に特定の消費者と関連付けられていなかったデバイスの利用、疑わしい取引または行動などについて、カード会社に警告を発することができます。

「ThreatMetrixソリューションでは、信頼できる行動と疑わしい行動 を区別し、真にリスクが高い決済に不正対策のリソースを集中できるため、より多くの取引を受け入れ、かご落ちを低減することができます」— DNP

グローバル・デジタル・アイデンティティ・インテリジェンスを使用した3DSリスク判断の強化

LexisNexis ThreatMetrixソリューションは、数千件のウェブサイトにわたる数十億件の世界的取引を活用したデジタル・アイデンティティ・インテリジェンスのクラウドソース・リポジトリをベースとして構築されています。LexisNexis® Digital Identity Network®は、処理されたあらゆる取引によってさらに強力になり、消費者のデジタルアイデンティティに関する情報へのほぼリアルタイムのアクセスを実現します。

つまり、不正利用者が盗まれたクレジットカード情報を使用した可能性があったとしても、カード会社はDigital Identity Networkを使用して、当該クレジットカード情報を使った一連の取引行動によって、新しいデバイスで異なる場所から使用されているのか、または情報が流出したのか、マルウェアに感染した可能性があるデバイスから使用されているのかを把握することができます。

LexisNexis ThreatMetrixソリューションでは、数百項目ものデータを使用してあらゆるデジタル決済のリスクを評価しているため、カード会社は非対面カード決済の信頼性とリスクをほぼリアルタイムで把握することができます。

CASE STUDY

ソリューションを拡大して個々のカード会社に合わせてカスタマイズした実装を可能にし、コンソーシアムを介して確認された不正事例を共有

3DS決済に対するリスクベースの認証アプローチが成功した後、DNPは個々のカード会社に合わせたルールの最適化を提供しました。これにより、カード会社は自社のオンライン決済プロセス全体に合わせたリスクベースの認証を実装し、特定の不正被害の許容値に合わせてルールとリスクスコアを調整することができます。DNPは現在、十社以上の日本のカード会社に対してLexisNexis ThreatMetrixプラットフォームを導入しており、日本国内におけるクレジットカード不正防止ソリューションの構築を支援しています。

「当社は日本市場で多くのカード会社と取引を行っています。それらの会社にはそれぞれ異なる不正対策の課題と攻撃パターンがあります。当社はThreatMetrixを使用して、個々のカード会社に合わせてカスタマイズしたソリューションを提供することができます。そしてこれが、LexisNexis Risk Solutionsを選ぶ際の大きな差別化要因でした」— DNP

これらのパートナーシップの成功を拡大するために、DNPはLexisNexis Risk Solutions Consortiumの機能を使用して、不正決済対策コンソーシアムを構築しました。これにより、コンソーシアムのメンバーとなったカード会社は、一定の組織グループ内で、より高い確度で不正と認定された事例に関するデータを共有することができます。

そのメリットは以下の通りです。

- **確認された不正事例に関連する何万もの要素がコンソーシアム内の組織間で共有された。**
- **不正の防止により毎月多額の損失を免れ、コンソーシアムのメンバーに大きな投資回収率をもたらした。**
- **パスワードだけでは完全に保護できない不正取引の検出能力を高めた。**

「コンソーシアムは当社にとって革新的なものでした。これにより、コンソーシアムメンバー間で起きたことを共有し、協力して共通の不正の属性と新たな攻撃ベクトルを特定することができます」— DNP

不正取引による損失の低減をサポートするLexisNexis ThreatMetrix Solutionの特定機能

- **ThreatMetrix SmartID®**は、Cookie を消去したり、プライベートブラウジングを使用したり、その他のパラメータを変更したりして、従来のデバイスのフィンガープリントツールをバイパスするリピートユーザーを識別することを可能にします。こうして、Smart ID はユーザー検出を改善し、誤検知を削減します。多数のブラウザ、プラグイン、TCP/IP 接続の属性の分析から派生したSmart ID は、同一デバイスからの複数の不正アカウント登録を検出する信頼性スコアを生成します
- **スマートルール**は、真の顧客行動への理解を深めるとともに、実際の不正を確実に検出するのに役立ちます。ThreatMetrixは詳細な行動評価を実行するために、行動、年齢および場所を使用して、所定の取引に関する履歴データを調査します。これにより、実際の不正と正当な行動の変化をより確実に区別し、全体的なリスクを高めることなく、ステップアップの頻度を減らすことができます。
- **LexisNexis ThreatMetrix** コンソーシアムでは、共通の目標、課題または不正のリスクを有している企業が、合意済みの一連のコンソーシアムのメンバーとの間で、ネガティブ情報およびポジティブ情報をほぼリアルタイムで共有することができます。この知識共有により、複数の組織にわたるネットワークで活動している不正行為者、あるいは盗まれた認証情報をいくつかのオンラインプロバイダにわたってテストしている不正を検出およびブロックすることができます。
- **チャンピオンチャレンジャー** は、DNPをはじめとする多くの企業に、ポリシー変更の効果を判断するために使用されています。テストポリシー（チャレンジャー）は稼働中のポリシー（チャンピオン）に影響を与えることなく、並行して実行することができます。両ポリシーを同じ事例に対して同時に実行して、効果を比較することができます。

詳細については、risk.lexisnexis.jp/products/threatmetrixにアクセスしてください。

LexisNexis® RISK SOLUTIONS

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判断力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インサイトを提供します。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、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および意思決定ツールのグローバルプロバイダであるRELX（LSE: REL/NYSE: RELX）の一部門です。 www.risk.lexisnexis.com and www.relx.com

ThreatMetrix について

LexisNexis® Risk Solutions CompanyであるThreatMetrix®は、妥協することなく確実に利益が出るように世界経済を力づけます。14億のトークン化されたデジタルアイデンティティに対する深いインサイトにより、LexID® Digitalは、本物の顧客と不正顧客をほぼリアルタイムで区別するための、1.1億件の日々の認証ならびに信頼決定の背後にあるインテリジェンスをお届けします。