LexisNexis® Risk Solutions

2021年6月　決済セキュリティセミナー

LexisNexis®
RISK SOLUTIONS

目次

- 会社紹介
- サイバー犯罪報告書
- 他社事例のご紹介
  - カード会社のコンソーシアムネットワーク
  - 不正ポイント交換
  - なりすまし
  - アカウント乗取り
  - カードの不正利用
- ThreatMetrixのメリット
  - 金融庁のガイドラインについてQ&A
  - 不正対策

LexisNexis Risk Solutions - ThreatMetrixご紹介

正規のユーザーと、不正アクセスをリアルタイムに識別する為のグローバルネットワークを運営

精度の高いデバイス認識とフレキシブルなルールの設定が可能なリスクベース認証サービス

FORRESTER® **Leader among risk-based authentication (RBA) providers**	CNP AWARDS **Best Anti-fraud Solution** (Established)	FINTECH BREAKTHROUGH AWARD 2021 BEST FRAUD PREVENTION COMPANY **Overall Fraud Prevention Solution Provider of the Year** (2020)	2020 ASIAN PRIVATE BANKER 6th TECHNOLOGY AWARDS **Best Cybersecurity Solution** (2019 & 2020)	JAVELIN **Leader in Identity** Among Enterprise Identity Proofing Vendors
cyber secured AWARDS 2020 **Best Fraud Protection** and **Threat Intelligence**	TOP 25 Cybersecurity Company 2020 TSR **Top Cybersecurity Company** Ranking 3rd in the Top 25 Cybersecurity Companies	FINTECH BREAKTHROUGH AWARD 2021 BEST FRAUD PREVENTION COMPANY **Best Fraud Prevention Company** (2021)	CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2021 **LexisNexis® Threatmetrix** Financial Services	AWARD WINNERS 2021 11TH YEAR Finance **Best Anti-Fraud/Security Solutions Provider 2021** United States, Europe, Asia Pacific, Latin America

LexisNexis®
RISK SOLUTIONS

変化し続ける サイバー犯罪の様相

グローバル目線でAPACを比較

世界の数値と比較したAPAC（アジア太平洋地域）の状況

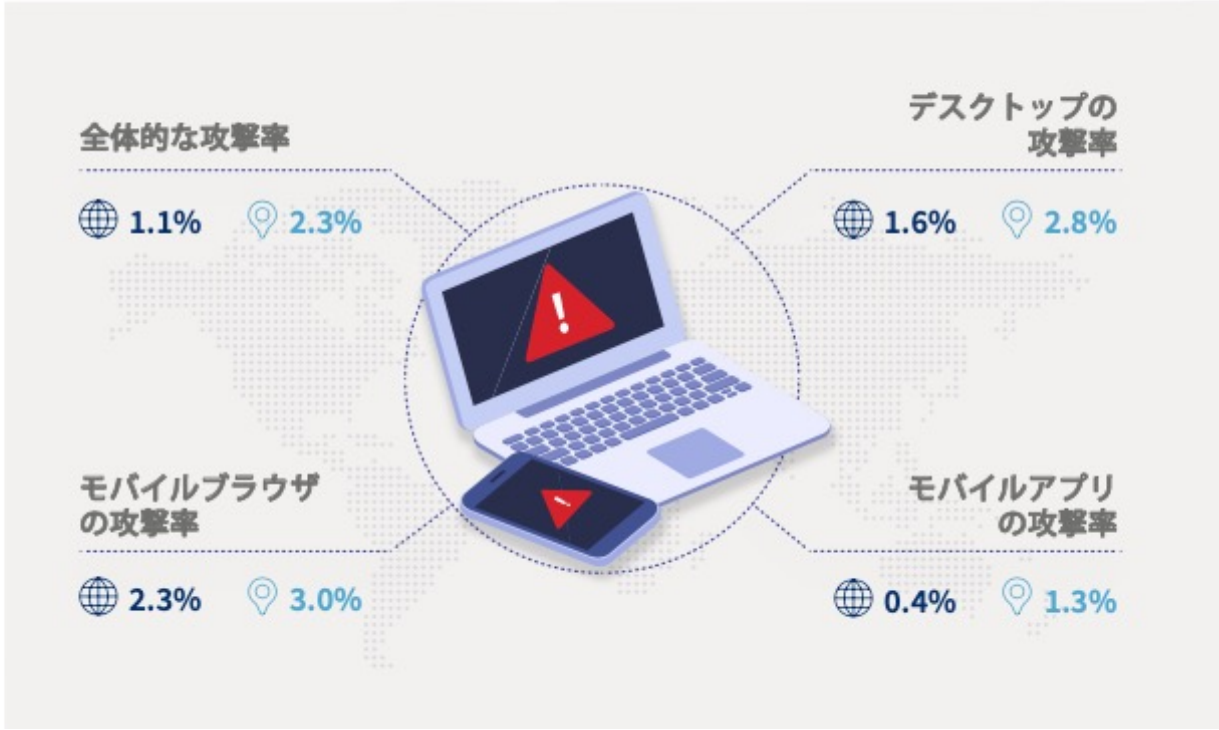
あらゆるチャネルにおいて世界の数値よりも高い攻撃率を示しているAPAC

	世界	APAC

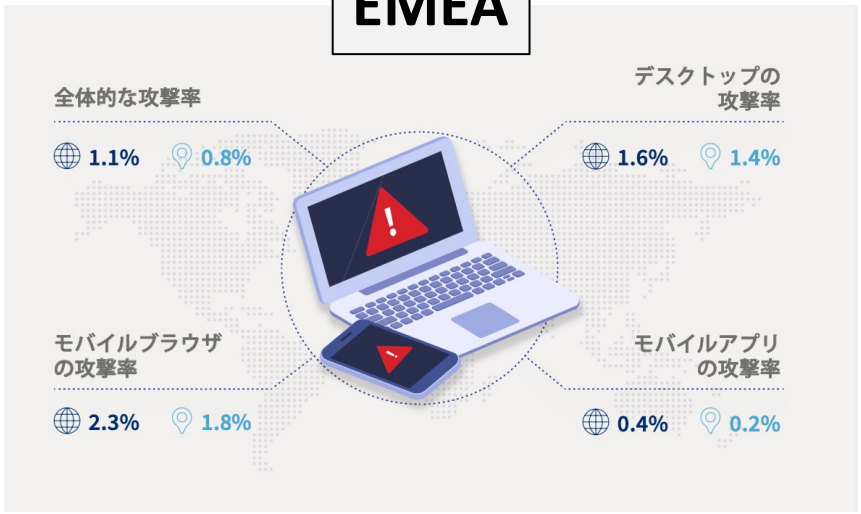
APACにおける攻撃率は、前年比ですべてのチャネルにわたり減少傾向にあるものの、依然として世界平均よりも高くなっています。

APAC地域は引き続き世界的なボット攻撃の主要発生源となっており、日本、インド、オーストラリアはすべて世界の上位攻撃発生国のリストに載っています。

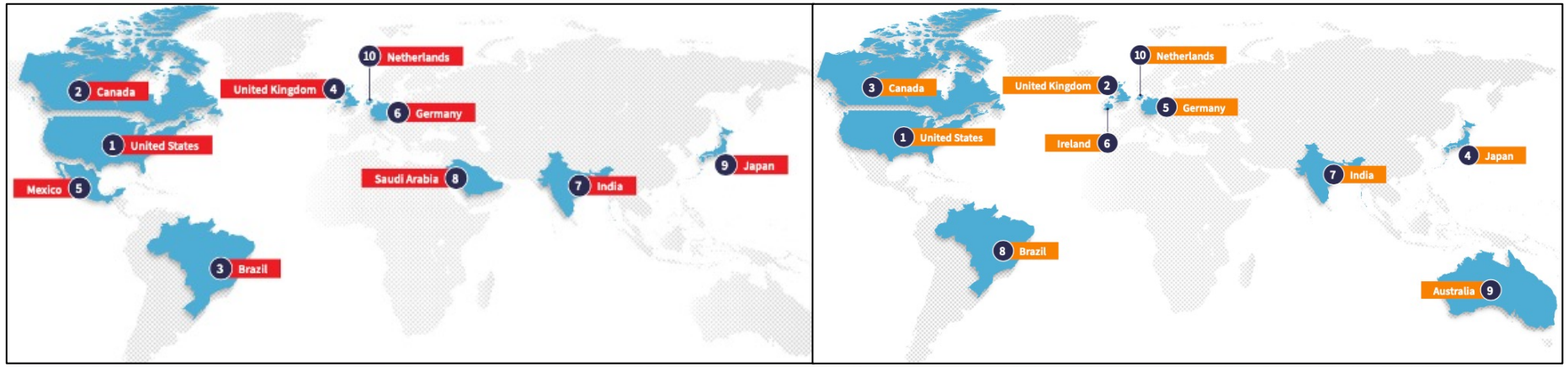
APACからの自動ボット攻撃量は、前年比でほぼ同様です。



EMEA



APAC攻撃パターン



上位5の攻撃発進国

1. India
2. Japan
3. Bangladesh
4. Philippines
5. Malaysia

上位5の攻撃対象国

1. U.S.
2. UK
3. Australia
4. Japan
5. Malaysia

取引および攻撃パターン

17億件 処理済み取引件数

人為的攻撃件数 **3,300万件**

自動ボット攻撃件数 **1.42億件**

チャネル別の取引の内訳

44% デスクトップ　56% モバイル

40% モバイルブラウザ　60% モバイルアプリ

チャネル別の攻撃の内訳

48% デスクトップ　52% モバイル

-15% ▼ 前年比によるモバイルデバイスからの攻撃の減少率

LexisNexis® RISK SOLUTIONS

CONFIDENTIAL

出典: The LexisNexis Risk Solutions サイバー犯罪報告書 – 2020年7月～12月

デスクトップvsモバイル

デスクトップ 対 モバイル

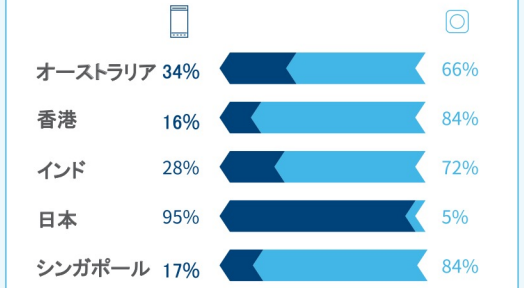
チャネル別トランザクションを概ね反映した数値となっており、
リスクが顧客の利用法に関連していることがわかる。

	オーストラリア	香港	インド	日本	シンガポール
全般	0.60%	1.00%	2.90%	1.20%	2.70%
デスクトップ	0.80%	2.00%	2.20%	1.40%	3.40%
モバイルブラウザ	0.70%	1.90%	7.80%	0.90%	3.40%
モバイルアプリ	0.40%	0.30%	1.70%	3.40%	2.00%

取引
チャネル別

攻撃
チャネル別

モバイル取引
ブラウザ/アプリ別



攻撃先　上位5カ国

業界別の攻撃パターン

金融サービスの決済時の攻撃件数は
どの業界よりも高い

モバイルアプリよりもデスクトップや
モバイルブラウザからの攻撃の方が高い

どの業界も正規ユーザーの増加により
攻撃の割合は減少している。

Eコマースの人為的攻撃率は下がったが
ボットによる攻撃は他の業界よりも増加

Eコマースのモバイルアプリで行われる
決済の攻撃率がどの業界よりも高く、
今後攻撃の対象になるリスクが最も高い

金融サービスの概要	アカウントの新規作成	ログイン	決済
リスク動向	2019年12月/2020年1月にモバイルアプリのアカウントの新規作成をターゲットとした大規模なボット攻撃により、この期間に攻撃の大きなピークを迎えたために、攻撃量/モバイルアプリの攻撃率が大幅に減少。ただし、デスクトップとモバイルブラウザによるトランザクションにおける攻撃率の増加が記録された。	信頼できる顧客からの定期的なトランザクション量が多いために、ログイン取引の全体的な攻撃率は低い水準を維持している。. ただし、アカウント乗っ取りの試みが3,600万件もあったことから、正規の顧客のアカウントが重大なリスクにさらされていることが明らかになっている。デスクトップとモバイルブラウザによるトランザクションの攻撃率は最も高かったが、前年比では攻撃率が減少している。	決済取引量は前年比で増加し、これに伴い攻撃量も増加した。ただし、攻撃量の増加はトランザクション量の増加よりも顕著ではなかったため、全体的には攻撃率が減少した。
攻撃量	500万件 (9400万件)	3600万件 （4800万件）	6900万件 （5800万件）
攻撃率			
△ 全体	4.1% (18.3%)	0.3% (0.5%)	3.6% (4.5%)
デスクトップ	**7.1%** (5.0%)	**0.7% (1.2%)**	4.1% (4.2%)
モバイルブラウザ	3.4% (3.1%)	**0.7%** (1.0%)	**4.9% (6.3%)**
モバイルアプリ	2.3% **(20.8%)**	0.1% (0.2%)	1.0% (2.2%)

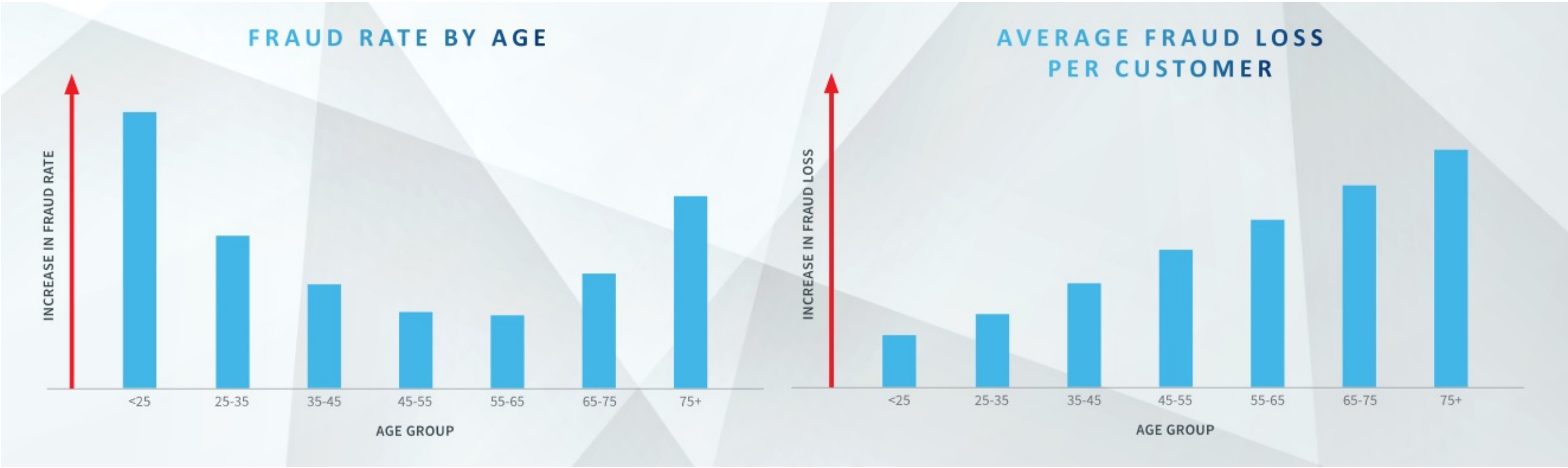
Eコマースの概要	アカウントの新規作成	ログイン	決済
リスク動向	デスクトップからのアカウントの新規作成が他のユースケースよりも引き続き高い率で攻撃を受けており、トランザクション10件あたり2件以上が潜在的な攻撃として特定されている。 これにもかかわらず、攻撃率はすべてのチャネルにわたり減少している。	Eコマース業者は金融サービス組織と比べると、比較的高い割合でアカウント乗っ取りに直面しているが、全体的な攻撃率は比較的低い水準を維持しており、すべてのチャネルにおいて前年比で減少している。	Eコマースのカスタマージャーニーにおける決済取引は、サイバー犯罪者にとって、盗まれた認証情報を換金して現金化するうってつけの機会を与えている。 攻撃率もすべてのチャネルにわたり減少しているが、Eコマース業者に対するモバイルアプリの攻撃率は他の業種よりも高くなっている。
攻撃量	600万件 （800万件）	1900万件 （4900万件）	3600万件 （4400万件）
攻撃率			
△ 全体	5.2% (11.3%)	1.0% (3.4%)	2.3% (3.8%)
デスクトップ	**10.7% (25.9%)**	**1.3%** (3.3%)	**2.7% (4.7%)**
モバイルブラウザ	2.7% (4.5%)	0.8% (2.9%)	1.6% (2.9%)
モバイルアプリ	1.3% (4.0%)	0.2% **(4.3%)**	**2.7%** (3.8%)

LexisNexis® RISK SOLUTIONS

出典: The LexisNexis Risk Solutions サイバー犯罪報告書 – 2020年7月～12月

年齢層別のリスク

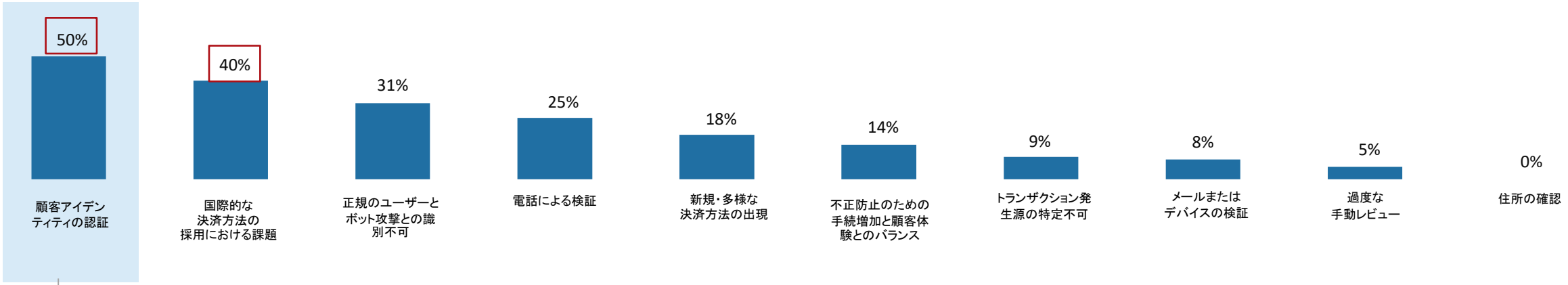
- 2020年には、オンライン上で取引をする顧客が増えた（オンライン初心者）
- 分析結果では、25歳未満が最も詐欺被害件数が高いことが示されています
- 75歳以上が次に詐欺件数が多く、かつ被害額は最も高い



非対面決済の主な課題となっているアイデンティティの認証と国際決済の採用

過半数がこれらの両方を上位3つの課題として挙げています。アイデンティティの検証に対する主な障壁として、リアルタイムのトランザクション追跡ツールの欠如、注文場所の特定の難しさ、合成アイデンティティが挙げられます。そのすべてが、顧客の余分な手続増加と離脱率増加の要因となる可能性があります。

オンライン上で商品を販売する際の課題*（上位3位）



ID検証が課題となる主な要因

- リアルタイムのトランザクション追跡ツールが限定的である、または入手できない（74%）
- 注文の発生場所を特定する機能が限定的である（59%）
- 認証速度と顧客の認証手続増加とのバランス（50%）
- 偽造のアイデンティティ（なりすまし）の増加（48%）

= その他のほとんどのまたはすべての課題よりも大幅にまたは方向的に高い

調査質問：
Q19a_1:顧客にデジタル商品を販売する際に貴社が直面している上位3つの不正に関する課題を挙げてください。
Q19a_2:デジタル商品を販売する際に顧客のアイデンティティ検証が課題となる上位3つの要因を挙げてください。
* 小売業者とEコマース業者のみに質問

他社事例のご紹介

LexisNexis®
RISK SOLUTIONS

大日本印刷 - 日本のカードコンソーシアム

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

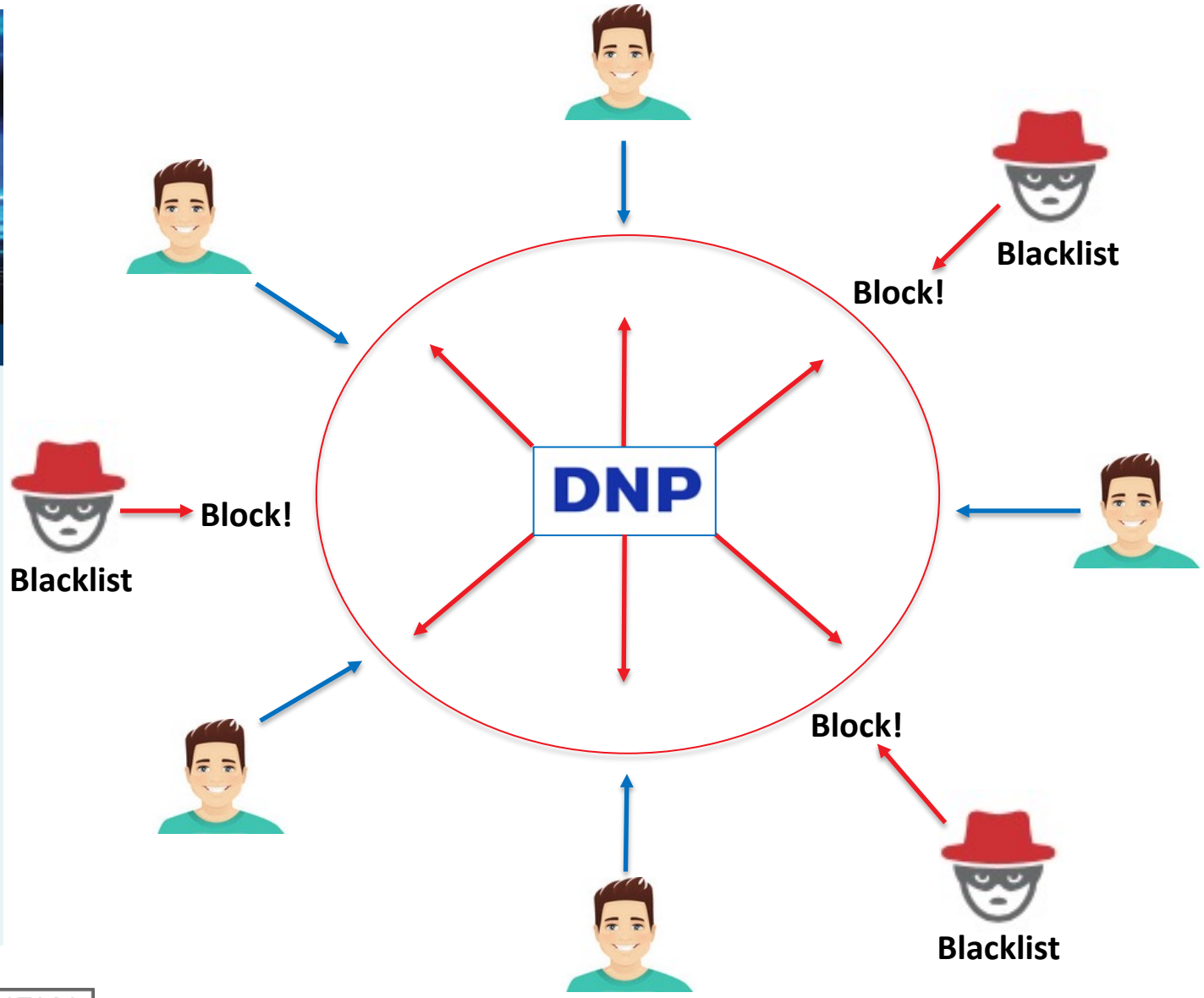
- 非対面カード決済における不正取引の低減
- クレジットカード会社に対する不正損失の低減
- カスタマイズが簡単で、強力なルールエンジンの導入
- 他の3-Dセキュア ACSプロバイダとの差別化要因となる機能強化

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。



エミレーツ航空 – 不正ポイント交換

ビジネスにおける課題

エミレーツ・スカイワーズは、以下を可能にするソリューションによるロイヤリティ・プログラムのマイル価値の維持を必要としていました。

- **エミレーツ・スカイワーズ会員アカウントを不正アクセスから保護し、優良なリピート顧客の余分な手続を最小化**
  ロイヤリティ・プログラムは、実在の顧客が獲得したマイルを不正に交換することを目的とするサイバー犯罪者にとって収益性の高い機会とみなされています。会員のアカウントを乗っ取ったサイバー犯罪者は、無料航空券、アップグレード、その他の提供される特典、場合によっては会員データから金銭的利益を得ようとします。 エミレーツ・スカイワーズは、不正なアクセスから顧客アカウントを保護するだけでなく、会員の旅程における主なタッチポイントでの余分な手続のいらない会員体験の維持も可能にするソリューションを必要としていました。
- **事前対応型不正モニタリングを推進**
  不正モニタリングは、事実上事後対応型アプローチの例外報告に基づいて行われていました。そのためエミレーツ・スカイワーズは、不正モニタリングを事後対応型のアプローチから事前対応型のアプローチへと強化するソリューションを求めていました。

なりすまし・アカウント乗取り・非対面決済の不正

日本の大手証券会社

〜FATF等の指定国からのアクセス〜

要件：

顧客がログインしてくる位置情報を確認し、サンクション国からのアクセスをブロックする必要があった。

システム導入後の結果：

顧客がログインする時の位置情報をThreatMetrixが識別、サービスを展開していない国からのアクセスを完全ブロック。さらに、VPN、TOR、Proxyを使った高リスクのアクセスも識別。

日本の金融機関

〜アカウント乗取り（ATO）〜

要件：

口座に不正アクセスする犯罪者から顧客の個人情報を保護する。デバイスの位置情報だけでは足らない。

システム導入後の結果：

デバイスや位置情報は簡単に偽造される為、ThreatMetrixを導入する事によって、デバイスや位置情報の偽造行為を検知する事に成功。

グローバル企業

〜非対面決済のカード不正利用（CNP）〜

要件：

カードの不正利用によるチャージバックに悩まされていた。

システム導入後の結果：

利用されているカードといくつもの情報を紐付けする事によって、関係性を瞬時にThreatMetrixが分析。リスクの高いトランザクションを拒否や追加認証を要求する事で追加認証のコスト削減とチャージバック数を大幅にダウン。

ThreatMetrixのメリット

LexisNexis®
RISK SOLUTIONS

金融庁のガイドラインについてQ&A

金融庁のガイドラインについてよくある質問	FATFの方針に沿った対応

インターネットバンキングについて、マネロン・テロ資金供与リスク評価、低減措置の観点から留意すべき事項を教えてください。

【A】

インターネットバンキングについては、乗っ取り、なりすましや取引時確認事項の偽りの可能性があることなど、非対面取引のリスクを踏まえた対応が必要であり、例えば、IPアドレスやブラウザ言語、時差設定等の情報、User Agentの組み合わせ情報（例えば、OS/ブラウザの組み合わせ情報）等の端末情報や画像解析度等を活用することにより、不審・不自然なアクセスを検知するといった対応が考えられます。

https://www.fsa.go.jp/news/r2/2021_amlcft_faq/2021_amlcft_guidelines_FAQ.pdf

ThreatMetrixによるリスク判定の仕組み

アクセス元のデバイス/ネットワークの情報、サイトからの情報、世界中の他のユーザーからの情報をもとに
「新規登録」、「ログイン」、「送金・決済」時の「不正リスク」を判定し、不正なトランザクションを検知します。

デバイスの情報

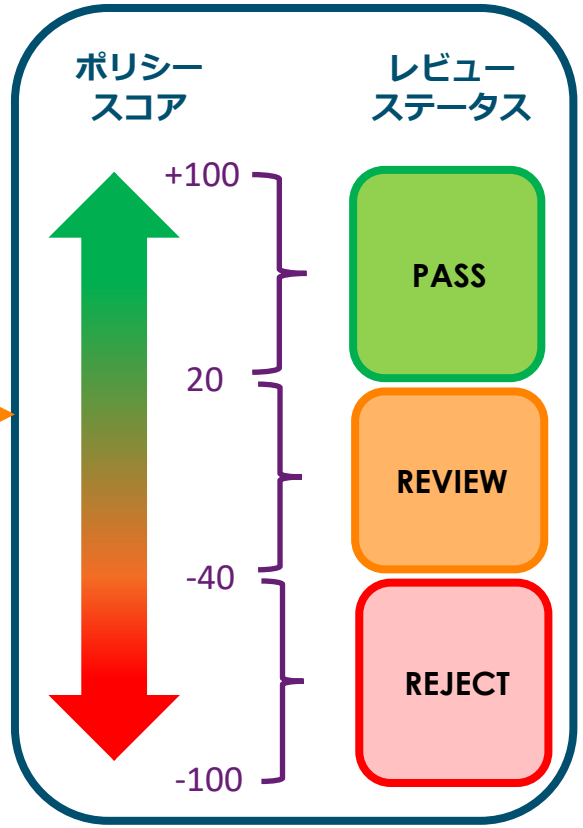
サイトからの入力情報

世界中の情報

ルールは容易に
カスタマイズ可能

ルール

1,000以上の要素を使って
リスク値を計算



スコアをPASS/REVIEW/REJECTの3つのステータスに分け、それぞれ具体的なアクションを実装

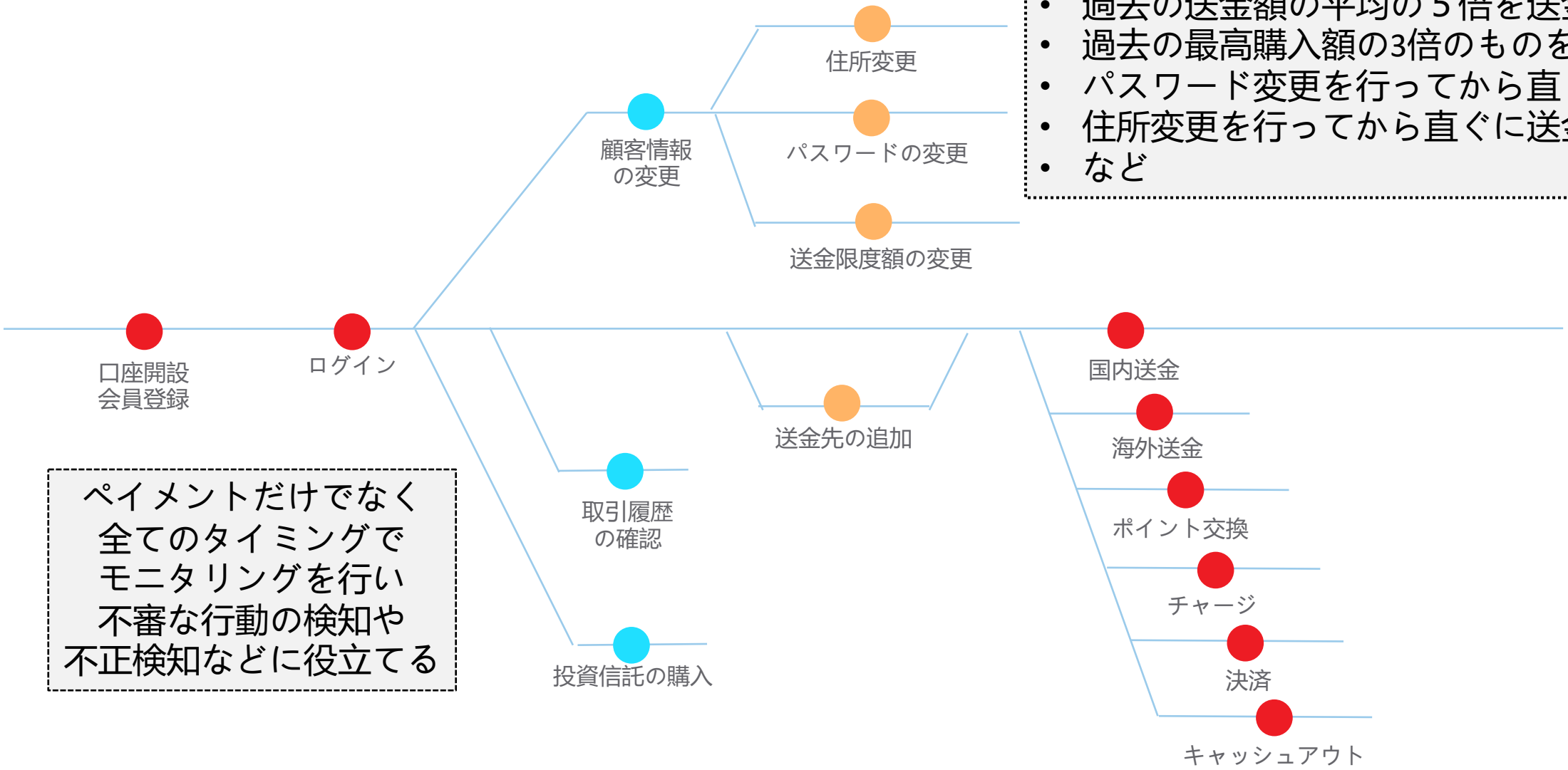
【PASS判定時の例】
- スムースにアクセスを許可

【REVIEW判定時の例】
- 追加認証（OTP等）の実装
- 後で改善の為、確認

【REJECT判定時の例】
アクセスを拒否したうえで
- ユーザーにメール送信
- ユーザーに照会

不正対策 - サイト全体でモニタリング

変数などを使ったスマートルールの例
- 過去の送金額の平均の５倍を送金
- 過去の最高購入額の3倍のものを購入
- パスワード変更を行ってから直ぐに送金
- 住所変更を行ってから直ぐに送金
- など



ペイメントだけでなく
全てのタイミングで
モニタリングを行い
不審な行動の検知や
不正検知などに役立てる

不正対策 - デバイスにふる三つのID

デバイスID① ExactID

クッキーベースのID

とは？	クッキーに対してのデバイスID
どのように使用する？	デバイスを識別する上で重要不可欠
どんな価値がある？	信頼の構築を支援し、誤検知を20%以上減少

デバイスID② SmartID

デバイスのプロファイリングで生成するID

とは？	400以上のデバイス属性をプロファイリングして生成するクッキーに依存しないデバイスID
どのように使用する？	クッキーワイプされているデバイスを識別する
どんな価値がある？	クッキーワイプされてもデバイスの識別が可能な唯一無二のID

デバイスID③ StrongID

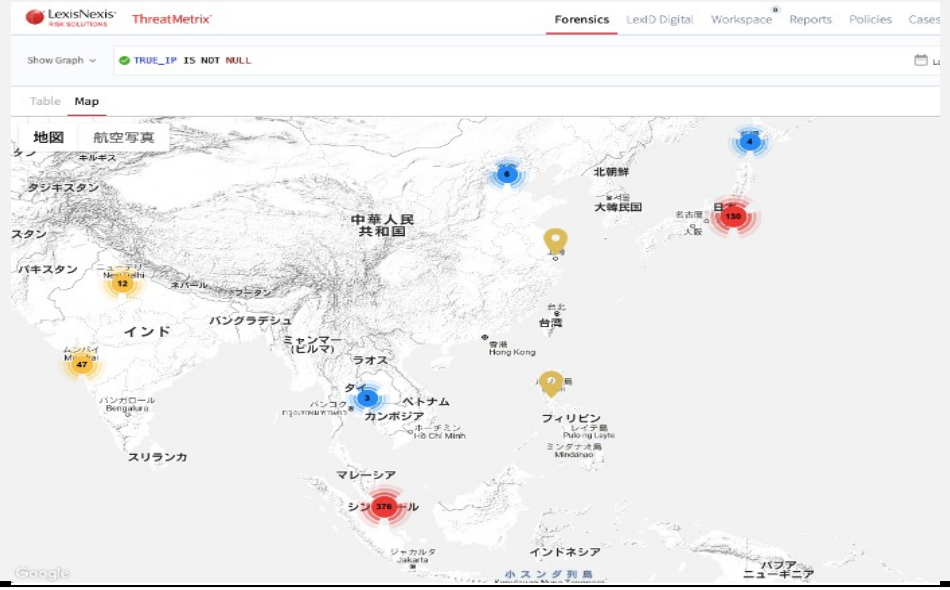
顧客の信頼性に応じて振るID

とは？	信頼性の高い顧客にふるID
どのように使用する？	トランザクション時の追加認証を無くしたりより良いユーザーエクスペリエンスを提供
どんな価値がある？	SCAの「Posession」要求を満たす

不正対策 – IPアドレス検知の正確性・デジタルIDの重要性

実IPアドレス

- VPN、TOR、プロキシの使用を検知
- プロキシピアシングで実IPを検知
- IPアドレス確実に検知する事によってサンクション国からのアクセスを未然に防ぐ

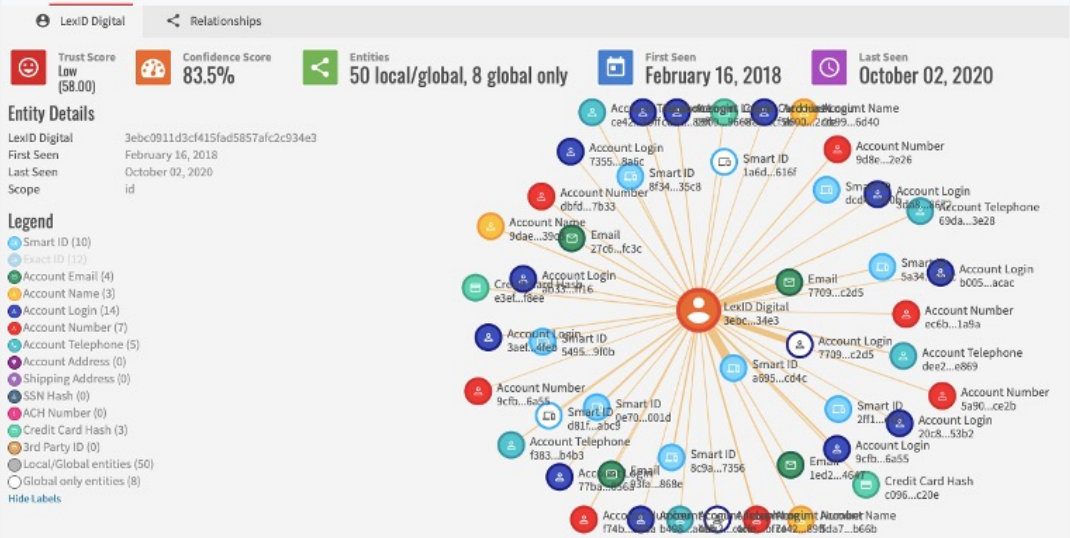


LexID® Digital

- デバイスのその先にIDを振る事によって、様々な要素との関係性を深堀

（例：電話番号、メールアドレス、カード情報、デバイスの数、など）

- デジタルIDの過去の振る舞いを検知
- デバイスからだけでは得られない情報を獲得



不正対策 – 行動バイオメトリクスで更なる防御

デバイスの振る舞い検知機能

デスクトップ

- キーボードの入力パターン
- マウスの操作方法

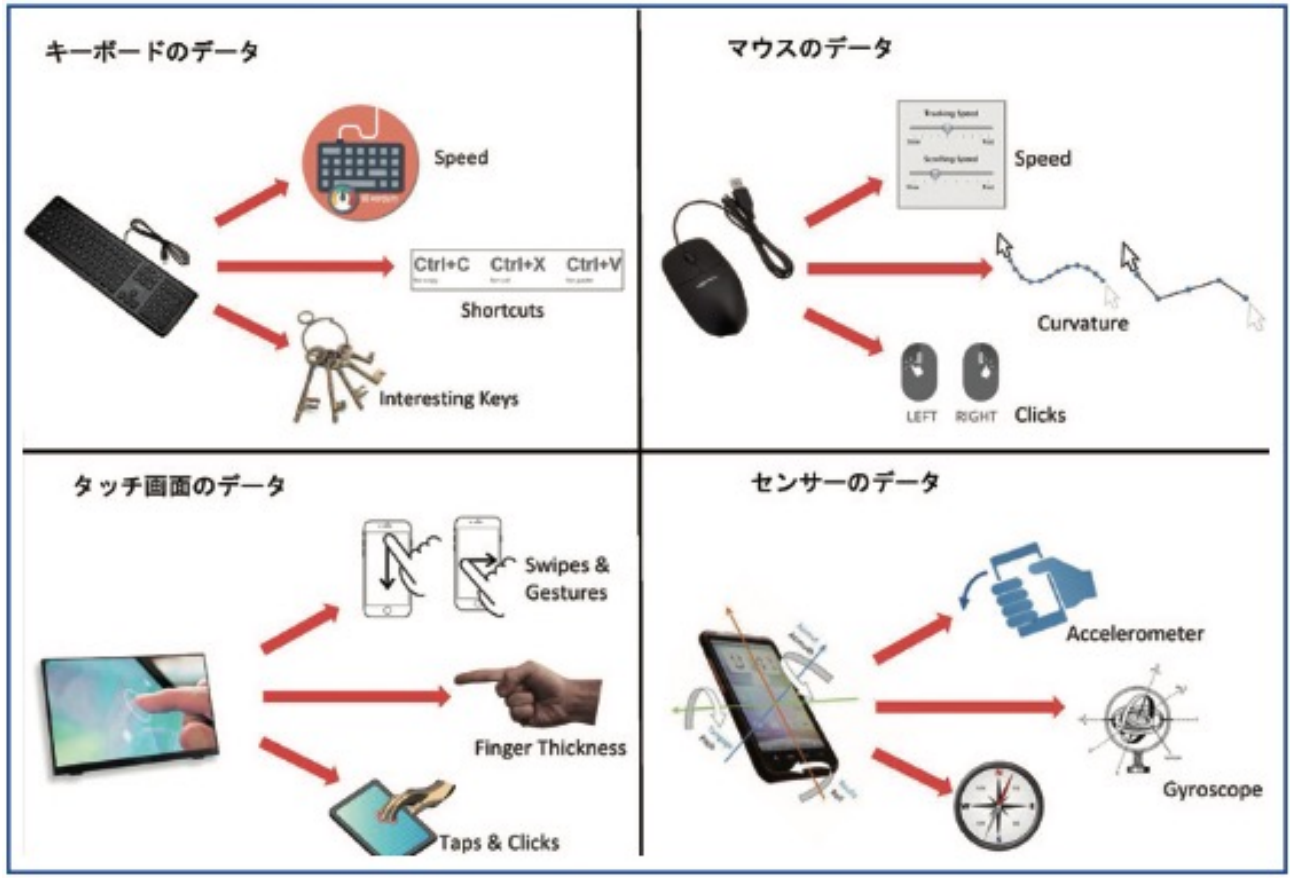
携帯端末

- タッチ画面操作
- 端末の角度検知

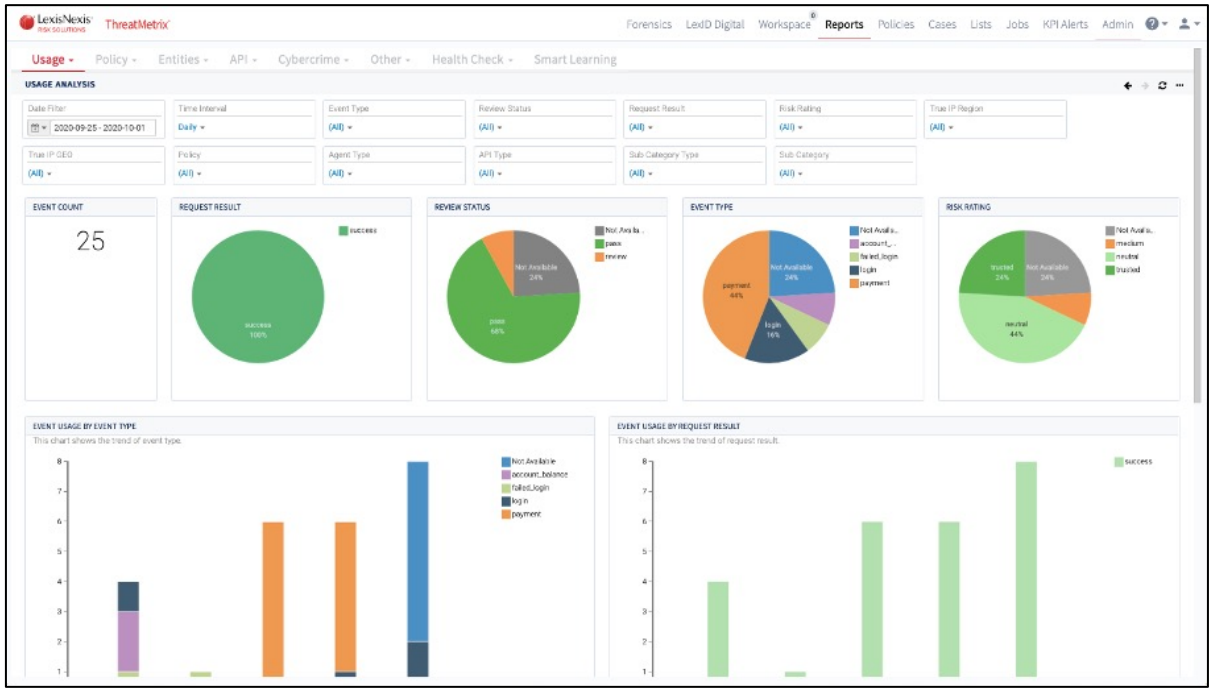
検知できるリスクの例：

- 名前や電話番号をコピペ
- マウスの動きに人間味が無い
- 指の太さやスワイプ方法が変わった
- 端末が一定の角度で固定されている

過去のパターンと比較してルールに反映



ユーザビリティ向上



お客様へのメリット

- 顧客に余分な手間をかけさせずに認証
- 不正アクセスから顧客の個人情報を保護
- 顧客の口座・アカウント・カード等を不正アクセスから保護する

ThreatMetrixユーザーのメリット

- チャージバックを大幅に削減
- 不正対策部門やコールセンターの作業効率アップ
- 追加認証・OTPなどのコストダウン
- 様々なレポートを出力して監査に対応
- 過去のレポートを使ってAI分析を行いルールに反映させて、誤検知数を大幅にダウン
- 実装やサポート日本語対応・ 24時間サポート体制