

# 支払いに関するオンライン詐欺

IPインテリジェンスはオンライン詐欺の**検出と防止**に使用されるトップ5のテクニックの一つ



digital element   
Location is Elemental™

## 目次

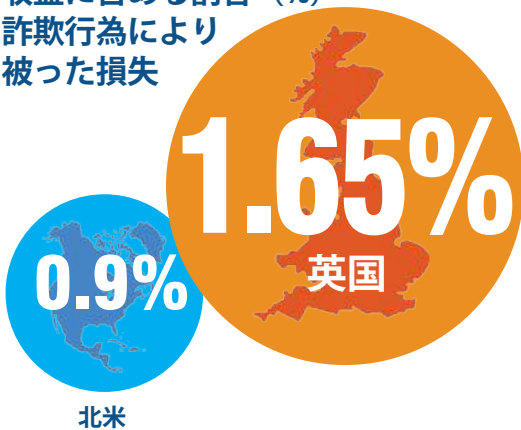
IPインテリジェンスはトップ5の不正防止ツールの一つ	3
すべてのIPベンダーが同じではない	4
より洗練されたルールへの投資	5
モバイルトランザクション	7
トラフィックの詳細を知るべきもっともな理由	7
クライアントを保護するために提供されるデータの一部	8



## IPインテリジェンスはトップ5の不正防止ツールの一つ



収益に占める割合 (%)  
詐欺行為により  
被った損失



eMarketerによると、世界のeコマース売り上げは、2014年に1.5兆ドルに達することが予想されており、さらに、2017年までには57%の急成長を遂げるものと予想されます。この急激な成長のマイナス面は、オンライン詐欺のケースが増えることです。詐欺行為により被った損失は、英国で収益の1.65%、北米で収益の0.9%で、合計では35億ドルと推測されます (Cybersource report)。相当数の、しかも慎重に管理される認証プロセスと適切なツールを採用することにより、詐欺の減少につながる大きな成果をもたらすことができます。

Digital Elementは、もっぱらIPアドレスに基づきオンラインユーザーに関する情報を提供するIPインテリジェンステクノロジー業界におけるパイオニアとして、世界をリードしています。Digital ElementのIPインテリジェンスソリューションであるNetAcuityは、中立的な立場の検証により、最も精度の高いIPデータセットの提供が可能であるとされていて、ユーザーの認証と監視を行い、オンライン詐欺を防止して、オンライン詐欺から保護してくれます。

IP情報の運用は、自動スクリーニングシステムを使う小売業者が採用するあらゆるツールの中でトップ5にランクされますが、すべてのIPソリューションが同じというわけではありません。一般に利用可能なデータをリパッケージするだけのプロバイダーと、複数の方法を採用してIPルーティングのインフラストラクチャ分析を行うトップクラスのプロバイダーとの間には、大きな隔たりがあります。

### ECBによる新たなカード不正使用の報告が示すオンライン詐欺の増加

クレジットカードおよびデビットカードで支払われる2,635ユーロ中の1ユーロが詐欺による損失を被っています

「単一ユーロ決済圏 (SEPA) におけるカード不正使用は、インターネット上の詐欺行為が増えたことが主な理由で、2012年に2008年以降初めて増加しました。欧州中央銀行 (ECB) が発表したカード不正使用に関する第三回報告から、インターネットによる購入が増え続ける中、オンラインのカード支払いのセキュリティを保証するために、さらなる努力が必要であることが分かっています。」

産業界は、とりわけオンライン販売に関して、継続的にセキュリティ対策の強化を図っていかねばなりません

オンライン販売の力強い成長に伴い、インターネットでの不正取引が増加

## すべてのIPベンダーが同じではない



IPアドレスの所在地を判別できるサービスを提供する業者やシステムはいくつかあり、わずかな費用で答えを得ることができますが、果たしてそれは適切なものでしょうか？IPアドレスの正しい所在地を判断して、プロキシなどの詐欺防止に役立つ他の重要なデータを見つけるためには、高度なインフラストラクチャ分析が必要になり、これは、インターネットのレジストリをチェックするだけだったり、一般に利用可能な無料データをリパッケージするだけのケースとはまったく異なります。

Digital Elementの質の高いIPアドレスデータは、最も高いレベルの粒度で、個人を特定することなく、ユーザーの現在地を都市／郵便番号レベルにまで正確に特定することができます。カバー範囲は全世界におよび、精度は国レベルで99.99%に達し、データは定期的に更新されています。重要なのは、ユーザーがどのように接続しているのかも判断できることで、VPN、衛星経由情報、アノニマイザー、Tor、モバイルデバイス、ISP、ドメイン、ホスティングセンターなど、詐欺を効果的に防ぐために小売業者が必要とするデータを特定することができます。

これは、IPルーティングのインフラストラクチャ分析に、世界の商業パートナーのネットワークを使って匿名位置を見抜く技術を組み合わせることにより達成されます。

NetAcuityは一元管理の効果的なソリューションで、小売業者のシステムへの統合と社内管理が簡単に行えます。それとは対照的に、一般に利用可能なデータは、世界的にカバーされる範囲が一様ではなく、更新されることはまれで、識別されるデータのパラメーターに制限がかかっていて、本質的に不正確です。

## 詐欺のタイプにはどのようなものがありますか？

電子取引を行う小売業者にとって最大の脅威は、クリーン詐欺、なりすまし、フレンドリー詐欺、フィッシング、ボットネットです。Digital ElementのNetAcuity IPインテリジェンスは、匿名をあばいたり、詐欺師の偽装を見抜くことができるテクノロジーを提供します。

クリーン詐欺

なりすまし

フレンドリー  
詐欺

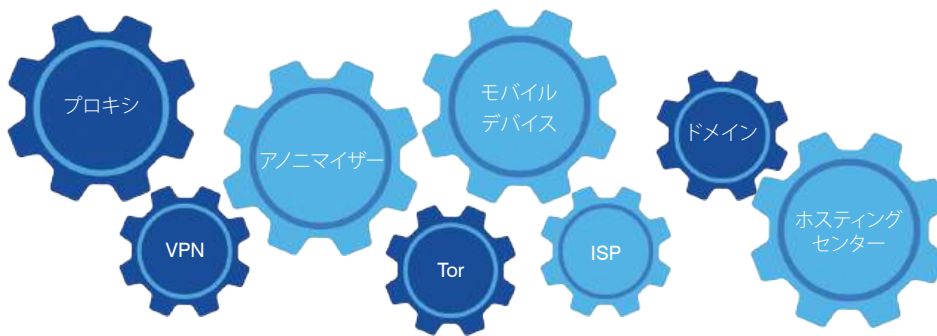
フィッシング

ボットネット

## より洗練されたルールへの投資

検出率とユーザーの使用感を向上しながら、誤検出を低減するためには、より洗練された詐欺検出ルールを整備し、プロセスを自動化することが有効であることが立証されています。IPインテリジェンスを使用した場合には、疑われるトラフィックを自動的にブロックしたり、検証をリクエストしたり（EメールまたはSMSで）、不正が疑われるトランザクションとして追加内部審査に送るようにフラグをつけることができます。

詐欺防止には現在地が活用されていますが、賢い小売店であれば、それをさらに突き進め、NetAcuityの高度インテリジェンスパラメーターを使用して、プロキシ、VPN、アノマイザー、Tor、モバイルデバイス、ISP、ドメイン、ホスティングセンターを特定することができます。現在地以上の情報を提供するNetAcuityのIPインテリジェンスを使用することで、より多くの疑わしい接続トラフィックを検出できるようになります。



## どのようなルールを採用すべきでしょうか？



### IPアドレスの所在国の確認

国際商取引を行う企業では、ナイジェリア、インド、パキスタン、ロシアなどの高いリスクがつきまとう国をブロックすることがあります。さらに、ユーザーが特定の国に住んでいることがわかっている場合に、別の国からアカウントにアクセスすると、疑わしいものとして検出されます。レジストリのみをチェックする基本的なシステムでは、ユーザーの現在地を正確に判断することができません。また、無料のIPデータでは、ユーザーがインターネットにアクセスしている国を偽っているかどうか（プロキシやアノマイザーを使用して）を特定できず、詐欺行為を見逃すことになりかねません。



### 請求先、出荷先、IPアドレスの所在地

請求先、出荷先、IPアドレスが一致しない場合は、自動的に赤いフラグをつけて更なる審査に回すか、アカウントの持ち主にEメールかSMSで検証を行うようにリクエストすることができます。



### ドメイン名

判明している不正ドメインや、公衆Wi-Fiホットスポット、インターネットカフェ、大学やキャンパスなどの疑わしいインターネットロケーションは再審査の対象となります。

## どのようなルールを採用すべきですか？

(続き)



### プロキシ

匿名、透過型、企業、公衆、教育機関、AOLなど、ユーザーがインターネット接続に使用しているプロキシのタイプを把握することで、詐欺警告を出すことができます。各タイプのプロキシへの対応はそれぞれ異なり、例えば匿名には企業プロキシよりも高いスコアがつくことがあります。現在では、エンドユーザーの現在地を偽装する接続や「容認性」の高い都市や国からのように装っている接続を、簡単に分類できるようになっています。



### ホスティング

エンドユーザーのトラフィックは、通常ホスティングセンターやデータセンターではわからないようになっています。その理由は、この種のセンターがトラフィックを通過させるように設計されており、トラフィックが発信されないためです。一部のクラウドブラウザはこれらのセンターを使用していますが、サービスは一様でなく、広範な開発が行われていません。受注確認を行う前に、他のCRM（顧客関係管理）データとの照合を行うことをお勧めします。



### 家庭、企業、ISP

接続が家庭で行われているのか企業で行われているのか、また、ISPを特定するために、別のインテリジェンスレイヤーを追加できます。このデータを使用して接続履歴情報を徐々に構築することで、いつもと異なる行動や異常な行動を検出することができます。

## ルールはいつ採用すべきですか？

認証または支払いシステムで重要なのは、サインアップ、ログイン、購入、金銭の預け入れまたは引き出し中のセッションです。

理想的には、セッションがハイジャックされていないことを確認できるように、購入プロセスのあらゆる段階で継続的な確認を怠らないことです。



## モバイルトランザクション



Gartnerの報告によれば、世界のモバイルデバイスを使った支払い額は年度末までに2,350億ドルを超えるということです。2012年に比べて44%の大幅増で、今後4年間にわたり年間平均で35%の成長が予想されます。

eコマースにモバイルデバイスを使って購入を完了させる際は、やはり、IP接続が行われます。ユーザーは、接続速度、利便性、コスト的な理由から、Wi-Fiネットワークを利用する可能性が80%高くなり、約20%が、3G、4G、LTE接続です。

Wi-Fi接続はデスクトップ設定と同様で、NetAcuityがWi-Fiロケーションと使用されているプロキシのタイプを正確に判断するため、同じルールが適用されます。3G、4G、LTEを使用している場合は、サービスプロバイダーとその接続ハブを示す固有のネットワーク特性を確認できます。

## トラフィックの詳細を知るべきもっともな理由

90%

不正行為を  
減少

ユーザーがどこでどのようにサイトに接続するかを把握することが、注文を受けやすくし、誤検出を少なくし、不正行為を減少させることにつながります。自動化は鍵で、NetAcuityのIPインテリジェンスは一元管理のシンプルなソリューションを提供し、デジタルビジネスの世界で不正行為を90%も減少させることができます。

NetAcuityは20分以内に社内サーバーに簡単にデプロイでき、様々な形で提供されるAPIによるクエリに対する応答時間は0.3ミリ秒以下の高速かつ信頼できるもので、毎秒最大30,000件のリクエストを処理することができます。

Digital Elementは、IPインテリジェンスに特化する世界で唯一のプロバイダーです。15年以上にわたる経験とノウハウを備える欧州および米国の専門チームは、オンライン詐欺の防止方法についてアドバイスを提供することができます。

顧客がどこからアクセスしているのか、また重要なことですが、その接続方法を詳しく知ることは、取引システムに必要な多くの改善の実現につながります。

20分以内に  
サーバーにデプロイ

## クライアントを保護するために提供されるデータの一部

国	接続形式	時間帯	ASN
都市、地域、州、都道府県	携帯/Wi-Fi	プロキシ	確実性
移動体通信事業者	緯度/経度	ISP	家庭/企業
郵便番号	電話地域コード	ドメイン	産業コード
カスタム地域	会社名	組織名	人口統計情報

## NetAcuityの小話とテクニカルニュース

クライアントプラットフォームをあらゆるオペレーティングシステムとアプリケーションに統合可能	データベースを毎週更新	わずか20分で運用可能！
待ち時間 - わずか0.03ミリ秒	毎秒30,000件以上のIP解決を実現	大部分のプログラミング言語とクライアントプラットフォームでカスタムサポートの利用が可能
サポート - 一日24時間、週7日体制のテクニカルサポート	32/64ビットのコンピューティングプラットフォーム、Red Hat Enterprise、Linux 4+、Solaris、10-Intel、Solaris 8-SPARC、Windows 2003 & 2008 Serverのサポート	API C、C++、C#、Perl、Java、PHP、.NET、Ruby、Python

## クライアント例



JPMORGAN CHASE & CO.



競争力に優れたオンライン活動を展開するために提供できるサービスについてご説明しますので、弊社までお問い合わせください。

UK | +44 (0)2033 184 702 USA | +1 678.258.6327

[www.digitalelement.com](http://www.digitalelement.com)