ThreatMetrix®
The Digital Identity Company™

グローバル化する不正は集合知で迎え撃つ

～不正のトレンドと最新のリスクベース認証のご紹介～

2016年11月25日

リスクベース認証の背景

既存の3Dセキュアと連動するリスクベース認証機能や、国際機関(EMVCo)　で検討中の　3Dセキュア　2.0へのバージョンアップは、**取引内容等の高リスク取引のみ本人認証**を行う等の制御が可能になるため、販売機会の逸失等の懸念が相当程度緩和されることが期待されることから、サービス内容やサービス開始時期等について関係事業者や国際ブランドからの情報収集に努めるとともに、できる限り早期に導入できるように検討を進める。

（抜粋）
クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画
－２０１６－【公表版】
２０１６年2月２３日　クレジット取引セキュリティ対策協議会

アジェンダ

- スレットメトリックス会社概要
- サイバー攻撃のトレンドと予測
  （2016 ThreatMetrix サイバークライム レポートより）
- 不正対策への最新のアプローチ
- Q&A

ThreatMetrixの会社概要

- 本社：シリコン バレー(サンノゼ)
- CEO： Reed Taussig
- 従業員：約２００人
- オフィス： ニューヨーク、ロンドン、パリ、シドニー、アムステルダム、香港、東京
- 顧客数：4000社 以上
- ウェブサイト数：30,000サイト以上
- トランザクション数：月間18億を超える
- 顧客層：ECサイト、銀行、クレジットカード、ソーシャルサイト、保険、政府系など

サイバー脅威を防止する先進的セキュリティプロバイダー

グローバルな顧客実績

>80M
日次トランザクション

30K
ウェブサイト

4,000+
顧客

電子商取引

ebay
BEST BUY
StubHub!
NETFLIX
Microsoft
hp
tickets.com
Яндекс
Найдётся всё
Walmart
Target.
markt.de
Der Marktplatz für Deutschland.
n11.com
mercado libre
Alibaba.com 阿里巴巴
Office DEPOT
COSTCO WHOLESALE
GoPro
tripadvisor
badoo
EBATES
EDGE LOYALTY
QUAKES
SuperRewards
global sources
Reliable exporters: find them and meet them
FANDANGO
Redbubble
VILLAGE ROADSHOW
gcp GIFT CARD PLANET

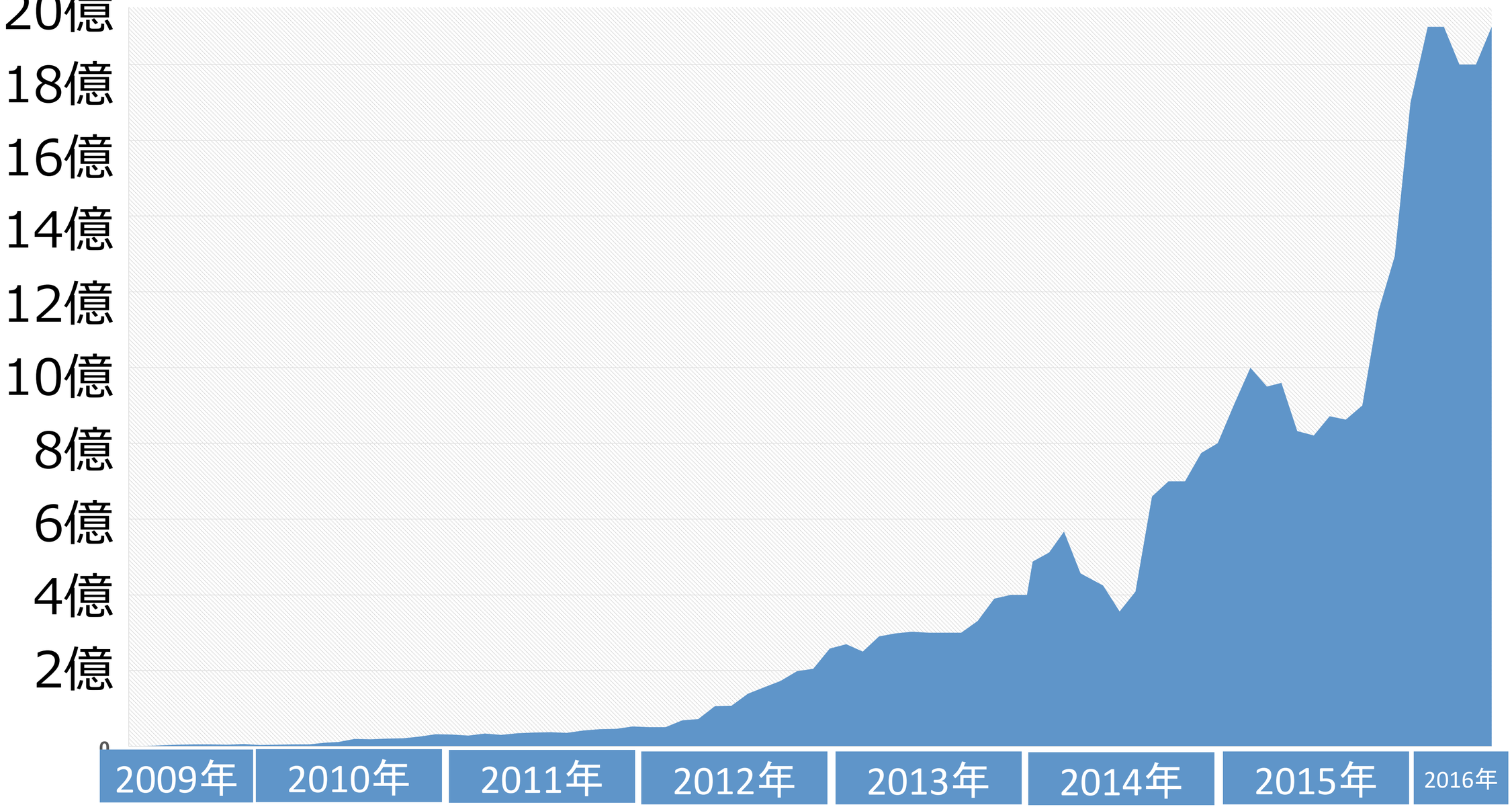
電子決済

VISA
AMERICAN EXPRESS
支付宝 ALIPAY
DISCOVER
PayU
worldpay
eMerchantPay
Yandex money
First Data.
OFX
CARDINAL COMMERCE
vantiv
RewardsPay
paysafecard pay cash. pay safe.
Moneris SOLUTIONS
Skrill
nets
Paysafe
BILLPAY
CyberSource
Accertify AN AMERICAN EXPRESS COMPANY
ACI UNIVERSAL PAYMENTS

ThreatMetrix®

2016 ThreatMetrix サイバークライム レポート

2009年から現在までの月間トランザクション数の推移



2016年のグローバル・トレンド

認証件数

月間約18億の
トランザクションを認証

攻撃検知数

1.3億の攻撃を検知。
前年比40%の増加
（第三四半期）

なりすまし被害

不正取得したIDを利用し自動攻撃するBot攻撃となりすまし被害が継続して高く、流通業をターゲット

モバイル割合

43%がモバイル端末のネイティブ アプリケーション

国境間取引

5分の1のトランザクションが国境間。
グローバル取引の承認/拒否において従来よりもより重要な判断

データ販売

ID情報は自動化された攻撃に利用される価値の高い情報として
売買されている

ホリデイシーズン

2016年の第4四半期はホリデイシーズンでありトランザクション量は約10倍になると予測

リスクベース認証

リスクベース認証はグローバルに継続して大きなユースケースとなる

攻撃の起点グローバルマップ

ThreatMetrix®

中国でのサイバー攻撃状況

中国を攻撃する国 トップ5
中国
米国
北朝鮮
香港
英国

中国から攻撃される国 トップ5
中国
米国
香港
日本
シンガポール

ThreatMetrix®

2013年度より約40億にも及ぶユーザ情報の漏洩

信用情報の漏洩

様々な国での数億、数千万単位での情報漏洩
例）2014年韓国での1億以上のクレジットカード、銀行口座情報漏洩

Eメールアドレスの漏洩

アシュレイ・マディソンサイトでの4千万のeメールアドレスが公開される

GoogleとYahooでの情報漏洩

ロシアのハッカーによる2.7億の認証情報取得

ヘルスケア・データ漏洩

アンセム（米国医療保険会社）での8千万の患者情報漏洩

リスト攻撃の被害を公表されている企業/サイト

電子商取引		
発表日	企業名	サービス名
H28.3.3	ビックカメラ	ビックカメラドットコム
H27.9.28	トイザらス	トイザらス オンラインストア
H27.7.6	タミヤ	タミヤショップオンライン
H27.7.16	ディノス・セシール	セシールオンラインショップ
H27.07.28	シャトレーゼ	オンラインショップ
H27.04.17	楽天	楽天市場
H26.09.29	佐川急便	会員制Webサービス
H26.09.26	ヤマト運輸	クロネコメンバーズ
H26.09.08	リクルート	ポンパレモール
H26.08.13	良品計画	無印良品ネットストア
H26.06.13	ドワンゴ	ニコニコ動画
H26.06.02	楽天	楽天ダウンロード
H26.04.23	パナソニック	CLUB Panasonic
H26.01.22	スタイライフ	Stylife
H25.12.21	ドスパラ	ドスパラ通販WEBサイト
H25.10.23	セブンネットショッピング	セブンネットショッピング
H25.08.29	WebMoney	WebMoneyファンクラブ
H25.06.19	ニッセン	ニッセンオンラインショッピング
H25.06.03	ハピネット	ハピネット・オンライン
H25.05.29	阪急・阪神百貨店	阪急・阪神オンラインショッピング
H25.05.25	三越伊勢丹	三越オンラインショップ
H25.05.17	資生堂	ワタシプラス
H25.05.08	ディノス	ディノス オンラインショッピング
H25.04.22	エムティーアイ	mopita
H25.04.05	イーブックイニシアティブジャパン	eBookJapan

ポイント交換		
発表日	企業名	サービス名
H27.7.6	ニフティ・ライフメディア	ライフメディア
H27.7.28	オリエントコーポレーション	会員Webサイト「e-Orico」
H26.12.24	キューデンインフォコム	ヒアコン
H26.11.10	マーシュ	D STYLE WEB
H26.07.04	イード	あんぱら
H26.06.26	CPP	CAPAT
H26.05.09	ジャックス	インターコムクラブ
H26.05.02	ソニーマーケティング	ソニーストア
H26.03.27	JCB	MyJCB
H25.09.02	GMOメディア	ポイントタウン
H25.07.26	カルチュア・コンビニエンス・クラブ	Tサイト
H25.04.06	カルチュア・コンビニエンス・クラブ	Tサイト

2013年より37件

Amebaに不正ログイン5万件　リスト型攻撃受け、全ユーザーにパスワード変更呼び掛け

「Ameba」がリスト型攻撃を受け、約5万件の不正ログインがあったという。全ユーザーにパスワードの変更を呼び掛けている。

サイバーエージェントは5月11日、「Ameba」がリスト型攻撃を受け、7日までに約5万件の不正ログインがあったと発表した。不正ログインの試行回数は223万回にのぼるといい、全ユーザーにパスワードの変更を呼び掛けている。

リスト型攻撃は、流出したID、パスワードのリストを使い、別のサービスに不正ログインを試みる攻撃。Amebaは4月29日夜から断続的に攻撃を受けているという。

不正ログインを受けたアカウントのパスワードはリセットし、ユーザーに報告した。対象のアカウントは、ニックネームやメールアドレス、生年月日などが第三者に閲覧された可能性がある。クレジットカード情報はシステムで保有していないという。

同社は、不正ログインを受けていないユーザーも含め、全ユーザーにパスワード変更を呼び掛けている。他社サービスと異なるID・パスワードにしたり、パスワードに同じ文字の連続を使わない――などをすすめている。

情報漏洩による攻撃の兆候

情報漏洩が発生した後、高リスクのトランザクションが急激に増加

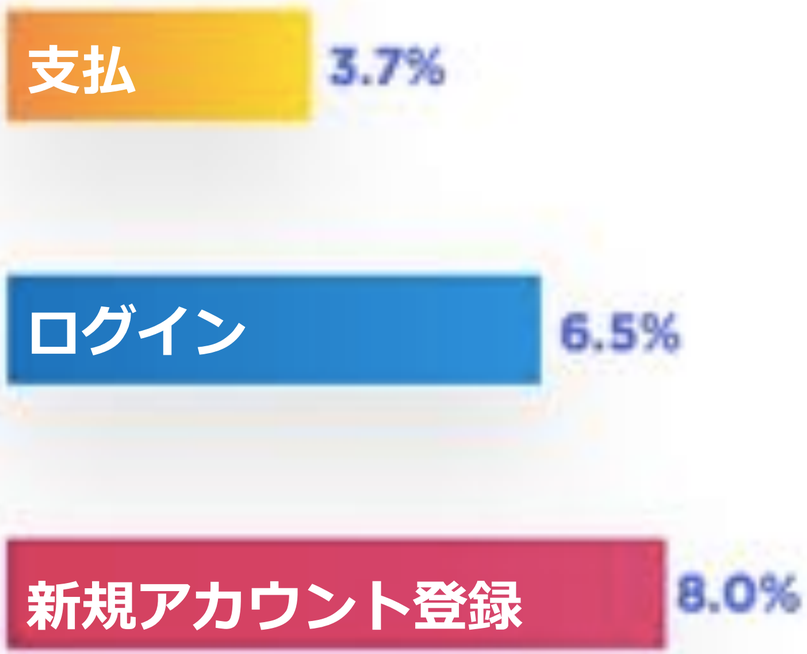
ThreatMetrix®

ECサイトにおける攻撃対象ユースケース

支払　ログイン　新規アカウント登録

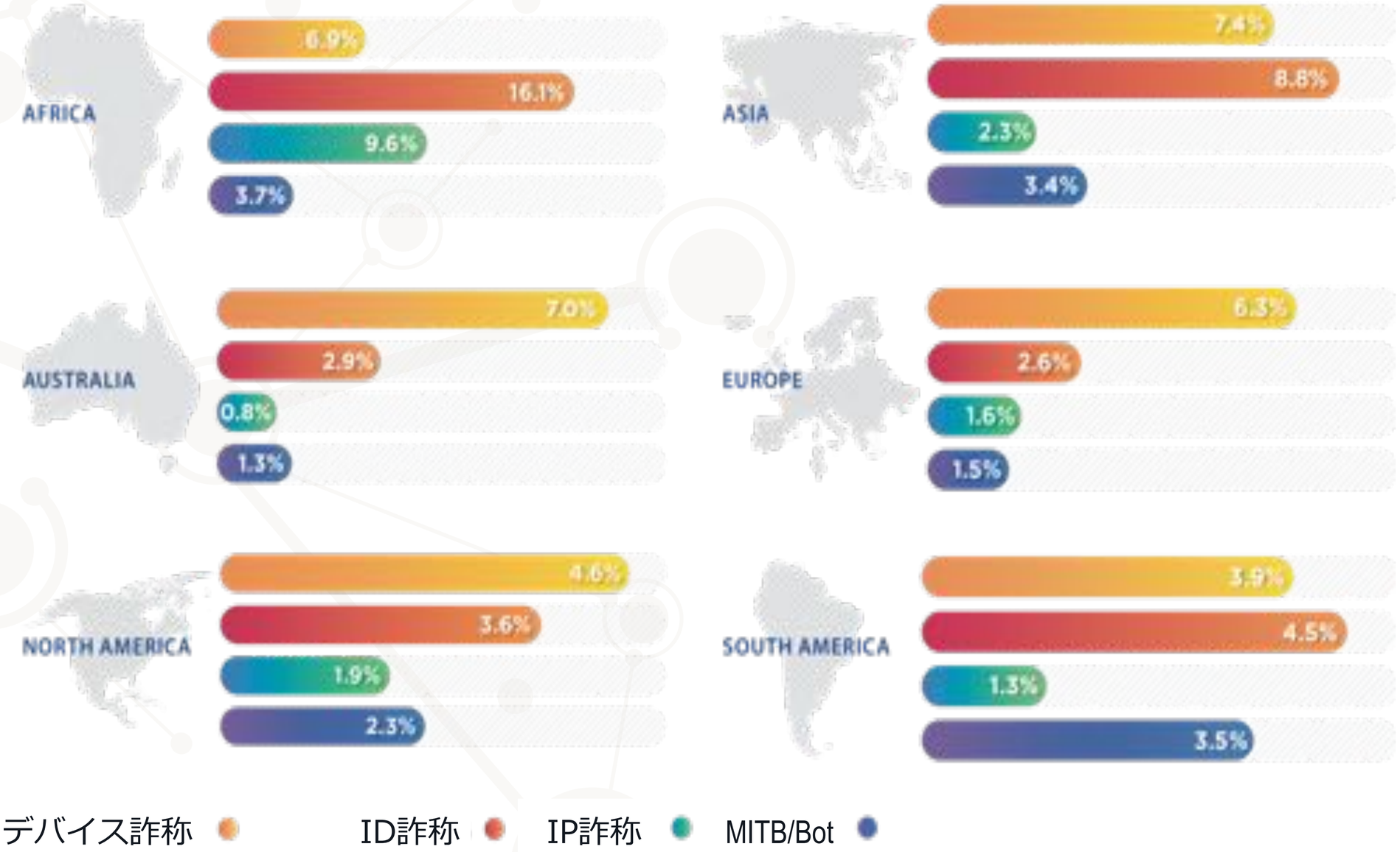
トランザクションのタイプと量

トランザクションのタイプと攻撃率



ThreatMetrix®

ID詐称がグローバルに増加兆候



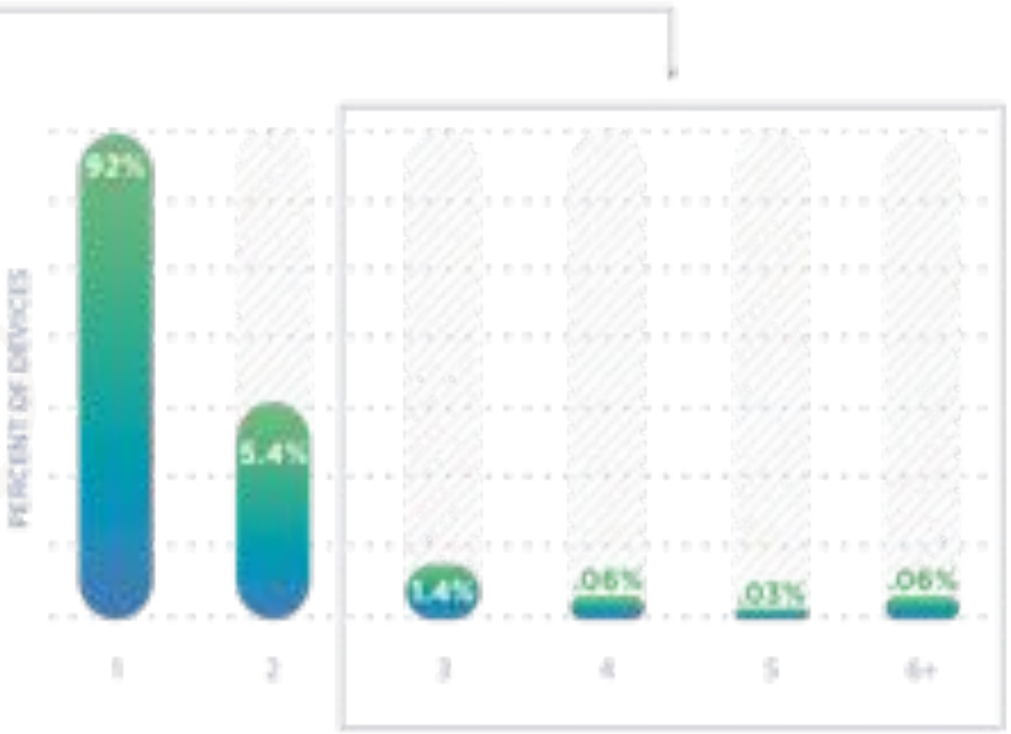
ThreatMetrix®

デバイスとID詐称

Bot？ アグリゲータ？詐欺行為？

一つのデバイスにおける複数のID

1 週間内で一つのデバイスから複数の
eメールアドレスでの操作



一つのデバイスにおける永続的なマーカーの消去

“新デバイス”として現れる数

- 不正行為者は、一つのデバイスから複数のIDをテストする
- cookie / cacheの頻繁な消去は疑わしい行為の顕著な兆候

ThreatMetrix®

米国における攻撃の事例

20分間に米国のProxyを利用し１２の
クレジットカードから5ドルの小額購入

ブラジルからの攻撃者

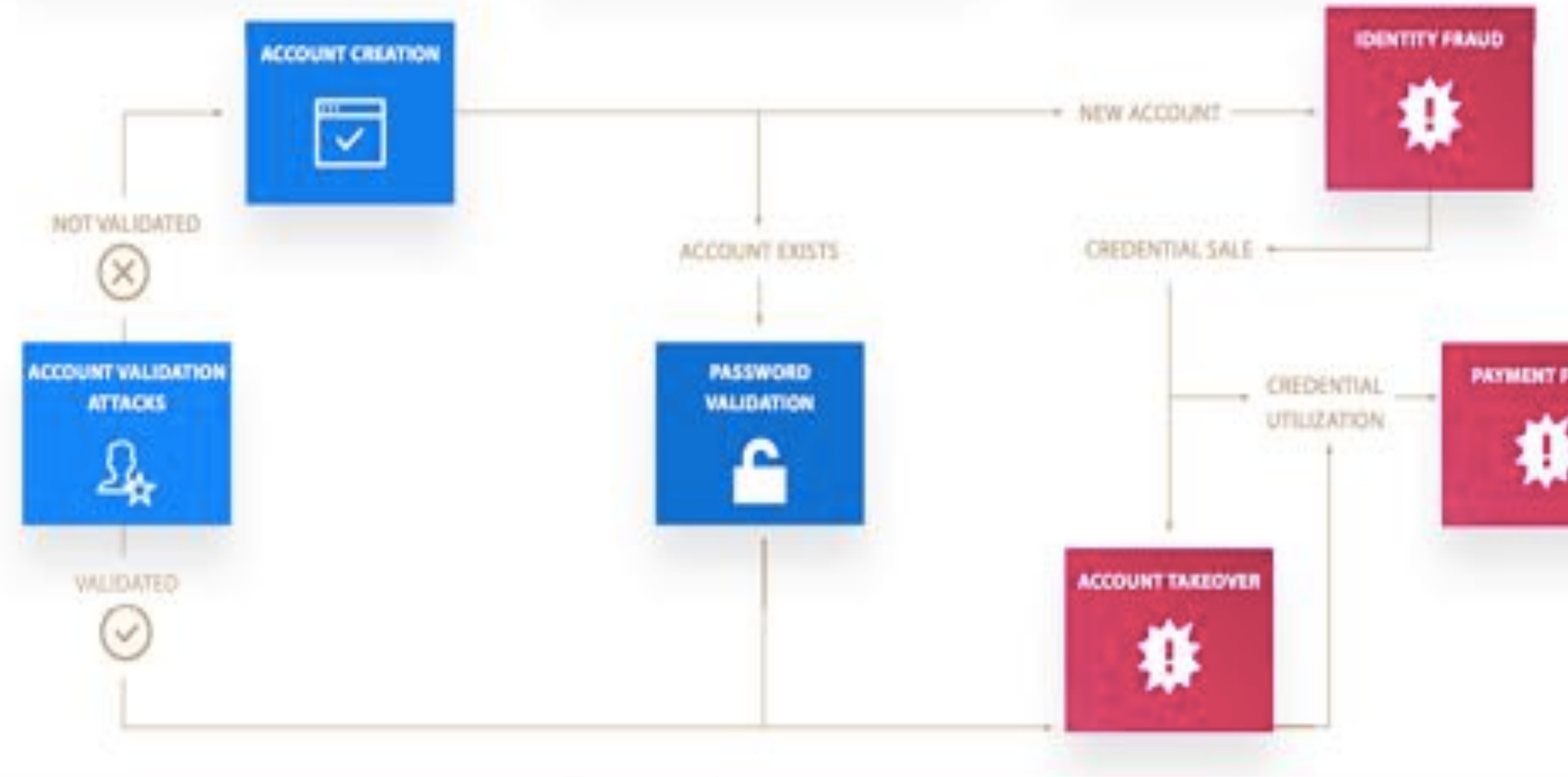
ThreatMetrix®

最新のbot攻撃の手法

大量のID検証する
基本的なボット

大量のパスワードの組み合
わせを試す複雑なボット

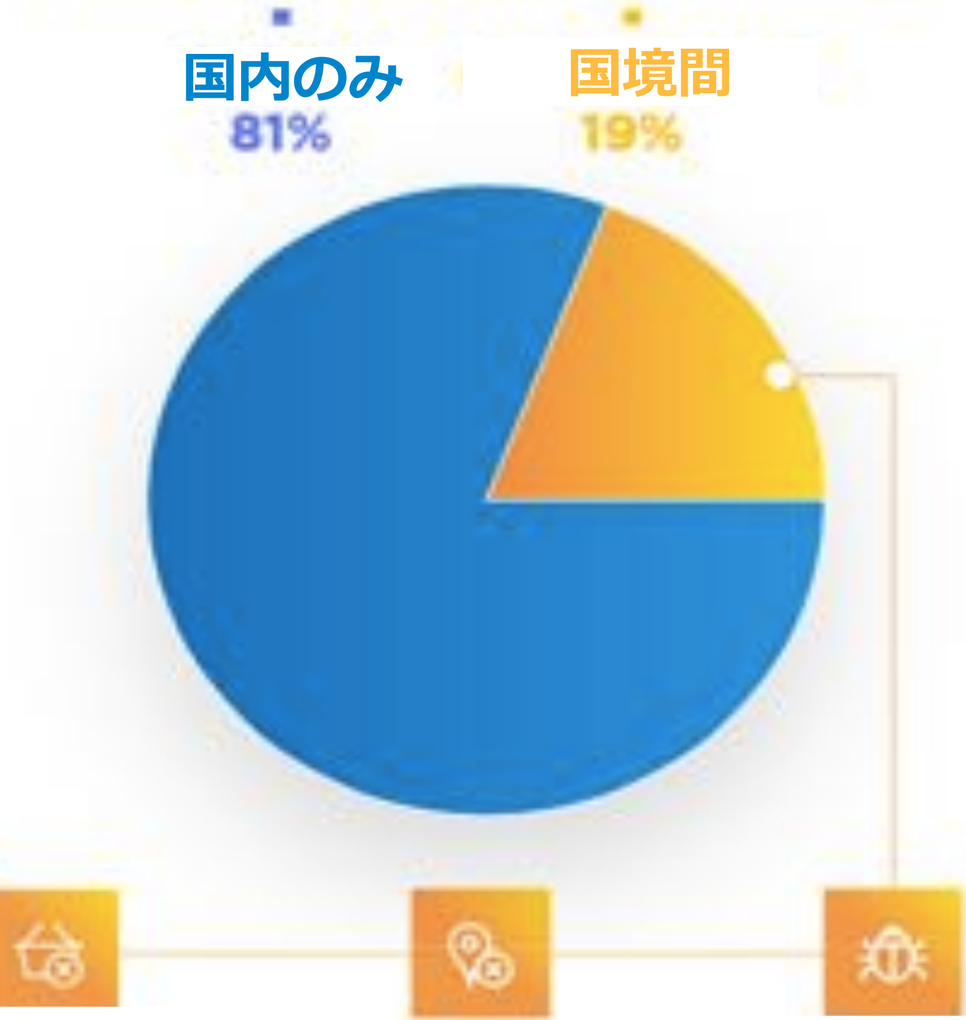
正規の人によるアクセス
として見せかけるボット



ThreatMetrix®

国境間取引の分析

国境間と国内のみのトランザクション比較



国境間での攻撃は自国内での攻撃に比べて２倍以上

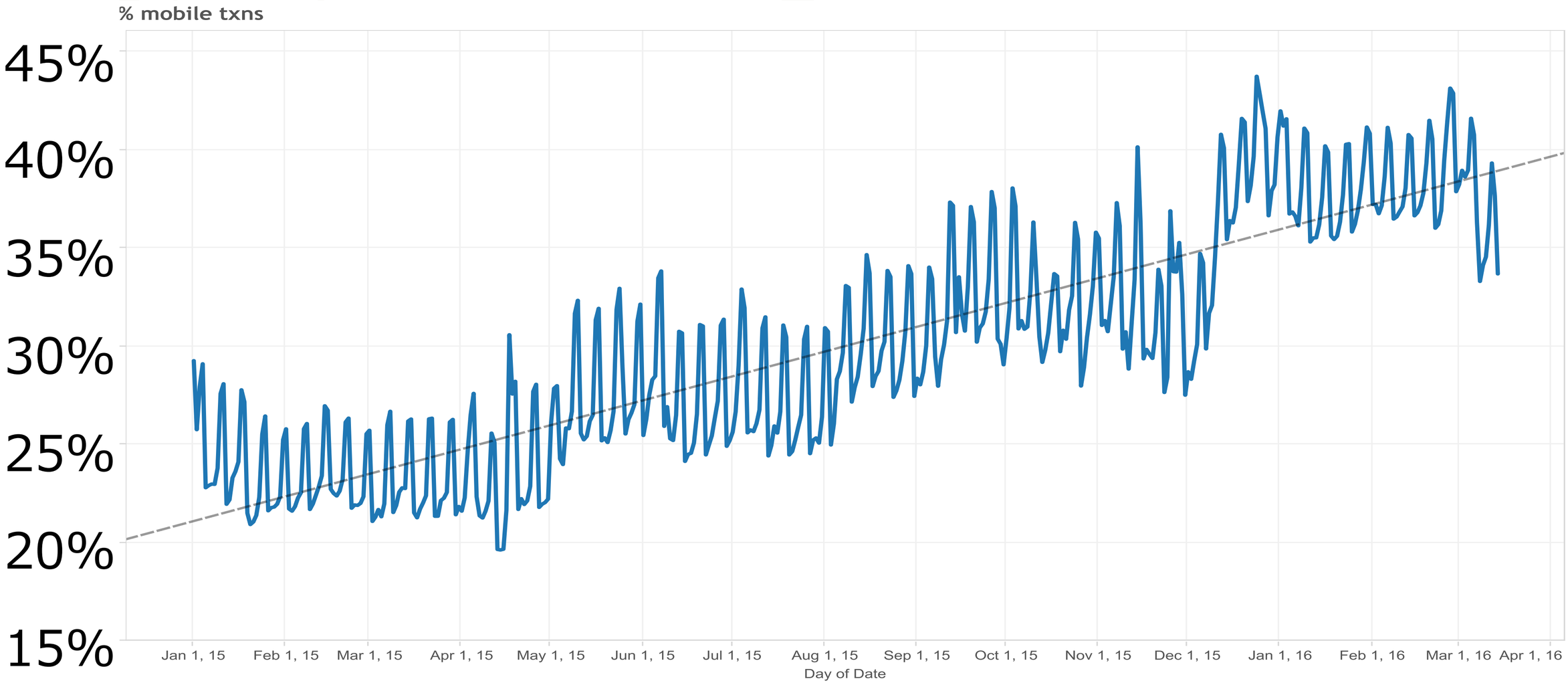
国境間でのIP詐称は自国内と比べて25%高い

国境間でのbot攻撃は自国内での攻撃に比べて70%高い

ThreatMetrix®

モバイル・ファーストのビジネスの増加

昨年より **160%** 伸張



ThreatMetrix®

今後の予測と対策

- Bot攻撃は継続して増加しており尚、セキュリティ対策を回避するように進化している
- なりすまし（ID詐称)は主要な課題
- モバイル利用の増加

- グローバルに攻撃がどのようにされているか分析が必要
- 包括的に対応可能な単一プラットフォームが必要
- 詳細に分析可能なソリューションが必要

ThreatMetrix®

ThreatMetrix®

不正対策への最新のアプローチ

ThreatMetrix リスクベース認証について

信頼できるユーザ？ それとも サイバー脅威？

“インターネット上では、俺が犬だなんて誰も知らない”

ThreatMetrix®

リピート顧客は売り上げ向上に最大の貢献

金融サービス

91%

Eコマース

84%

全デバイスにおける
リピート顧客率

ThreatMetrix®

ThreatMetrixインテリジェンスの優位性:

善良な顧客と不正行為者をグローバルに特定します

70% 誤検知削減

90% 詐欺 削減

グローバル デジタル アイデンティティ

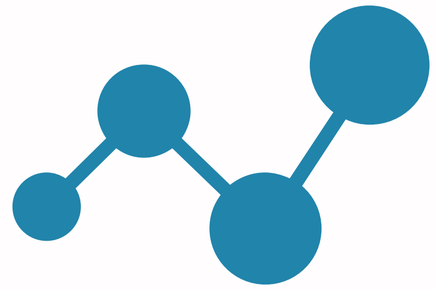
非摩擦の認証・解析

約300要素のデバイス
プロファイリングと
端末特定技術、行動分析

グローバル 共同利用型 インテリジェンス

世界相互情報

月間２０億を超える
トランザクションと
相互化されるデータベース



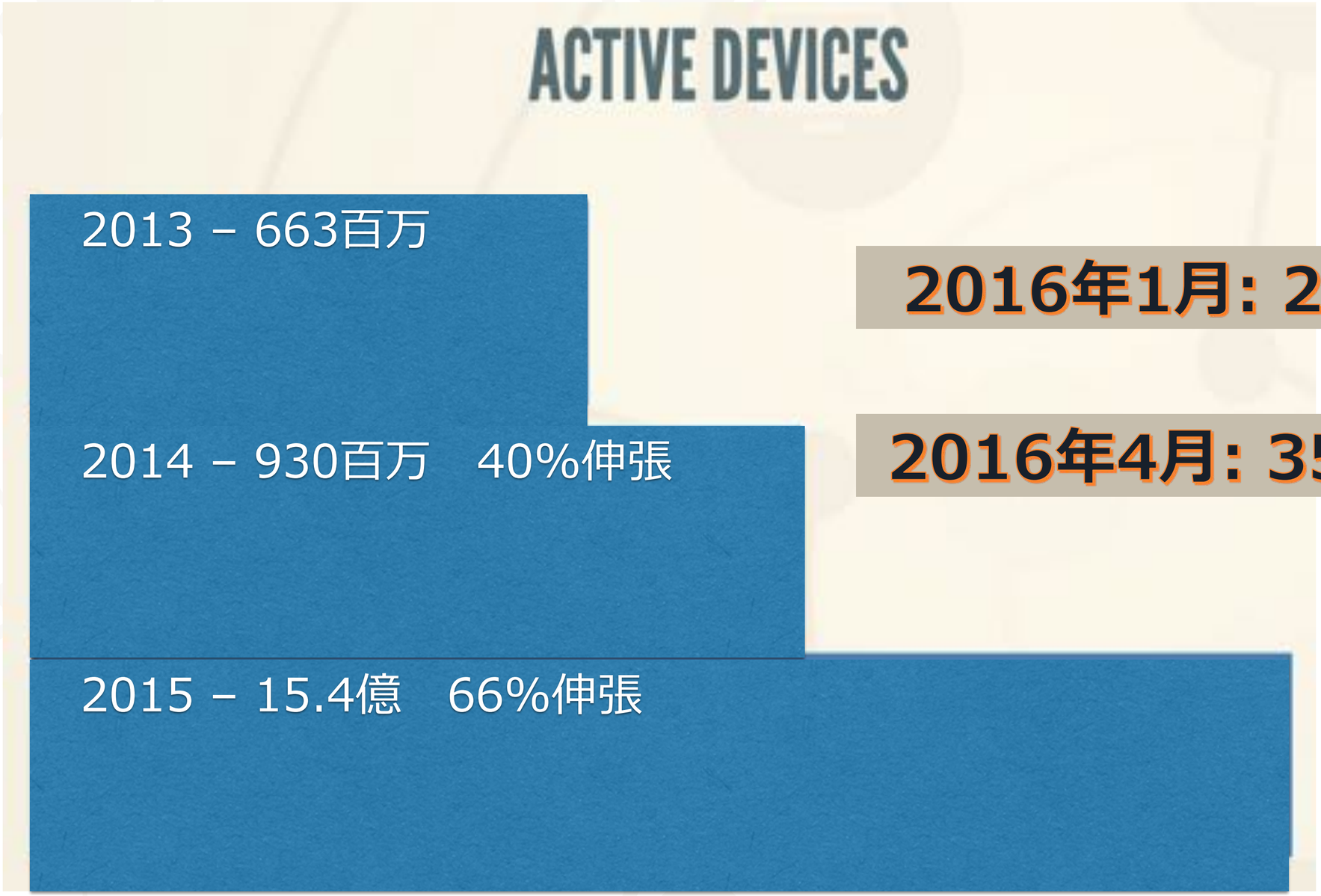
グローバル リアルタイム 意思決定

瞬間的な判断

顧客に合わせた
ルールカスタマイズと
リアルタイムスコアリング

ThreatMetrix®

ThreatMetrixネットワークでのアクティブなデバイス数

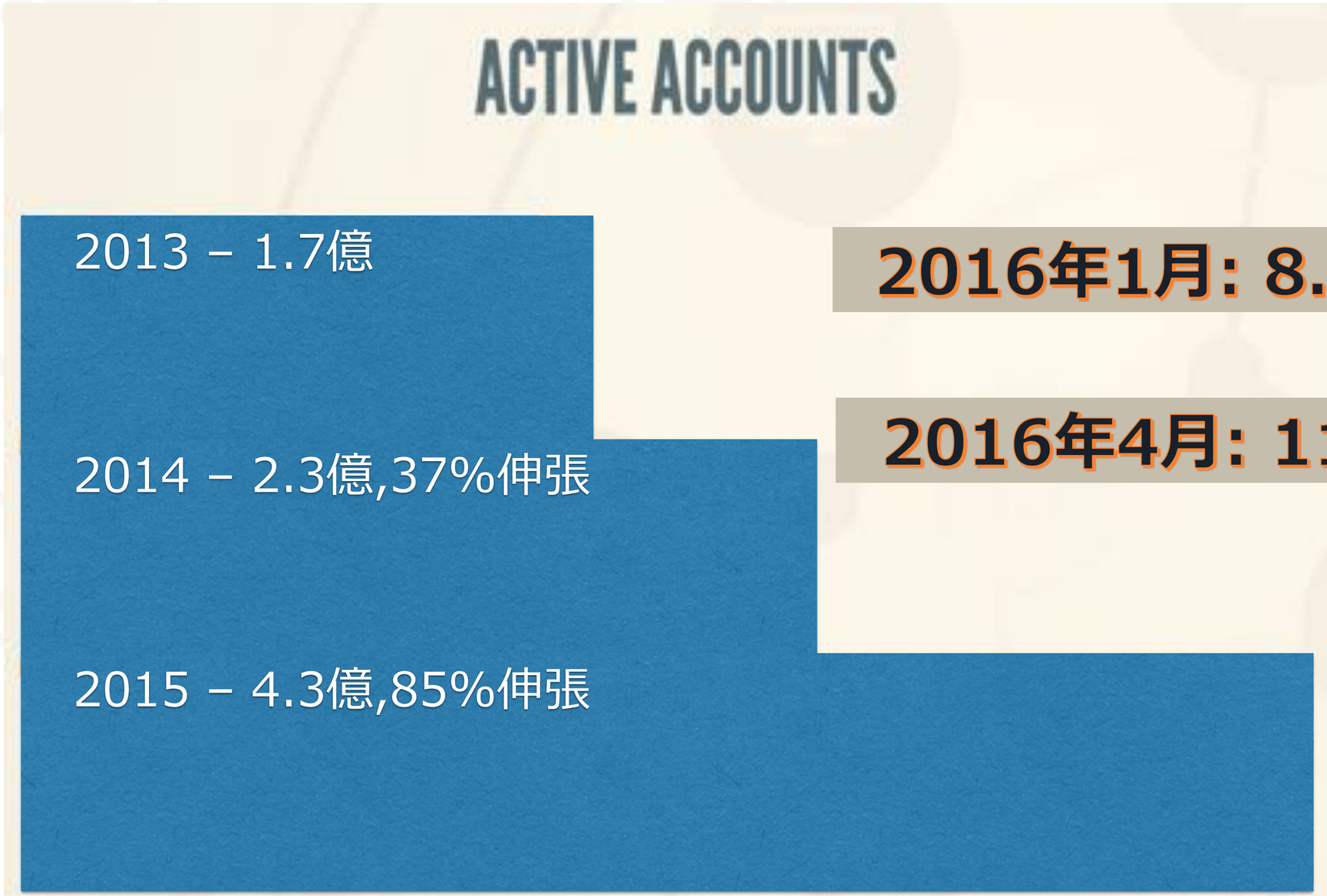


2016年1月: 25億デバイス

2016年4月: 35億デバイス

ThreatMetrix®

ThreatMetrixネットワークでのアクティブなアカウント数



2016年1月: 8.7億アカウント

2016年4月: 11億アカウント

ThreatMetrix®

共同型グローバル・インテリジェンス

サイト毎にカスタマイズされたルール

マシンラーニング

デフォルトテンプレート

共同利用

暗号化

信頼

デバイス
IPアドレス
匿名化ID

不正

デバイス
IPアドレス
匿名化ID

Microsoft

DISCOVER

Walmart

LLOYDS BANKING GROUP

airbnb

NETFLIX

VISA

BEST BUY

TARGET

TD Bank

tripadvisor

ThreatMetrix

利用事例 – VISA

課題

“Verified by VISA”の3DSecure決済代行サービスを提供したが、パスワード入力のユーザフリクション（利便性低下）による転換率が向上しない課題。

解決策

ThreatMetrixによるリスクベース認証導入により、信頼できる正規ユーザにはパスワード認証を行わず、疑わしいアクセスのみパスワード要求を行うように変更。

販売機会の逸失等の懸念が相当程度緩和
高リスク 取引のみ本人認証

VISA

カード認証の
219%増加

購買量の40%増加

不正購買を80%削減

ThreatMetrix®

利用事例 – 国内オンラインストア

課題

海外からの不正購買を最小化するため利用限度額を設定。

解決策

ThreatMetrixによるリスクベース認証導入によりアクセスを分析。
不正検知を行うことにより、海外からの購入に利用限度額を無くし売上を向上。

大手米国Eコマースサイトへの適用事例

サイバー攻撃

✓ボット攻撃や不正取得パスワードによるなりすまし購買被害
✓デジタルコンテンツ販売サービスの停止

課題

✓不正利用カード番号、なりすまし、ボット攻撃など
様々なサイバー攻撃を包含的に対策が必要
✓追加認証負担によるユーザ購買低下を回避

ThreatMetrix利用による効果

-端末特定による善良なユーザと不正ユーザを検知し、ボット攻撃となりすまし攻撃、盗難カード番号ブラックリストより不正検知
-デジタルコンテンツ販売の再開
-年間合計数十億のコスト削減

デジタル・アイデンティティ・グラフをマッピングします

個人とデバイス、認証情報、脅威のふるまいなどの様々な関係性をグラフ化し真のユーザと不正行為者を識別

各顧客がこのネットワークに参加することにより他の顧客の参加によって蓄積された知見を相互に活用することができます

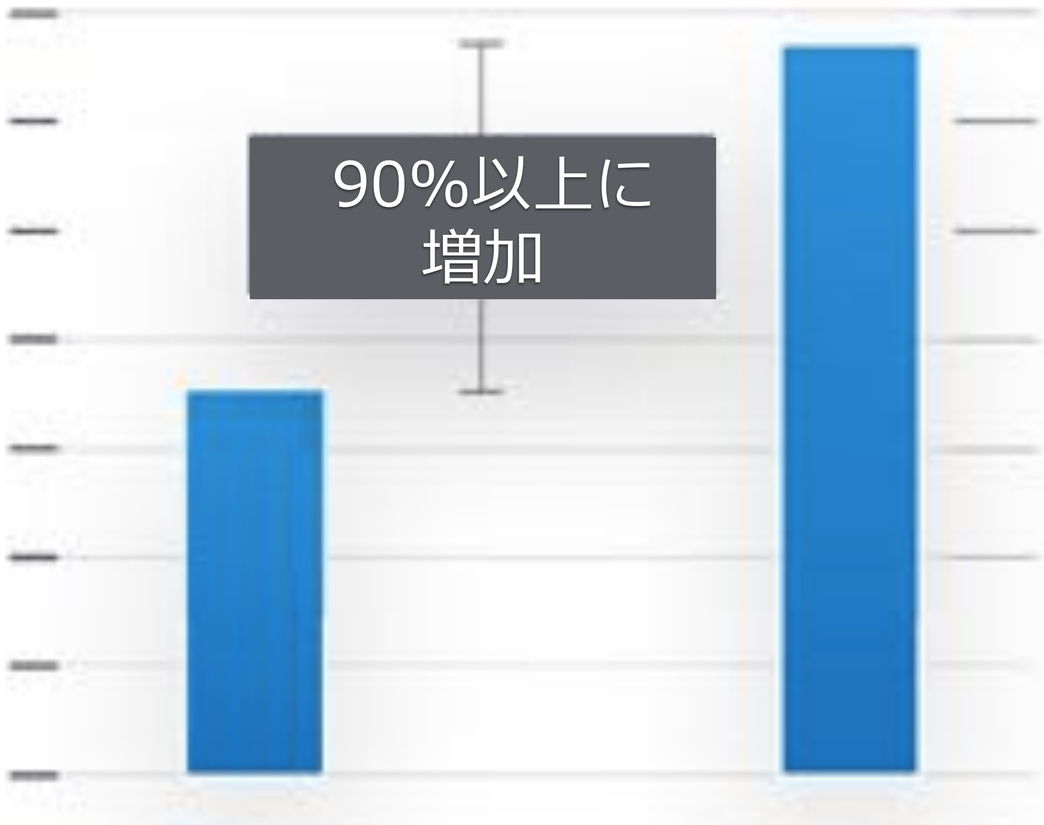
ThreatMetrix®

デジタル・アイデンティティ特定の手法

ThreatMetrix®

デジタル・アイデンティティとは

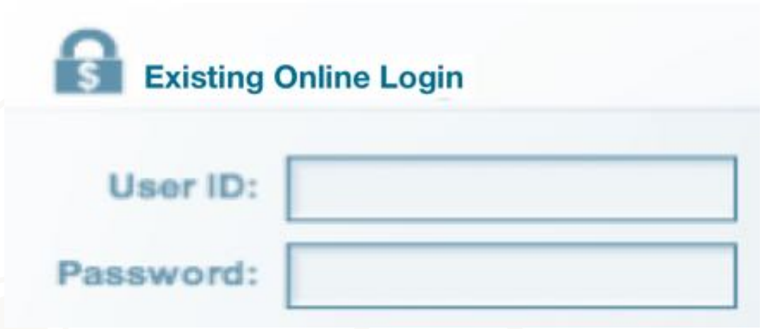
トランザクションにおける“信頼”できるユーザとして識別する率



デバイス識別には、単純なデバイス情報だけでは不十分です。
ロケーション情報、匿名化されたID 情報報、アクセス履歴などを総合的に分析しデジタル・アイデンティティを特定します。
これによって、正規のユーザにはフリクションレスを与え、転換率を向上します。

ThreatMetrix®

ThreatMetrixの適用局面



新規アカウント登録 → PASS / REVIEW / REJECT

ログイン → PASS / REVIEW / REJECT

決済・送金 → PASS / REVIEW / REJECT

匿名トランザクション & ユーザー属性

判定, スコアリング, 理由コード, 行動分析 & 属性

不正履歴参照, ポリシーエンジンのカスタマイズ　& 管理ポータル

共同利用型インテリジェンス

ThreatMetrix デジタルアンデンティティ

ThreatMetrix®

ThreatMetrix アーキテクチャー

利用者

ウェブサイト

1 利用者がページを読み込む

利用者がトランザクションを実行する 2

3 トランザクションの結果

1

利用者のデバイスを
プロファイルング
(セッション ID と
非個人情報)

ThreatMetrix の
API を呼び出す
(セッション ID と
暗号化された任意の
個人情報)

2

ThreatMetrix
Digital Identity Network

3 **リスクスコア**
が返される

- **PASS**
- **REVIEW**
- **REJECT**

正常な活動と異常な活動とを
見分ける

- ページ改竄
- 隠されたプロキシー
- 同一デバイスからの複数のログイン
- 過剰なトランザクション額
- マルウェア検出
- プロファイルングデータ

属性データからルールによるスコア

プロファイリング

(属性：約300要素)

直検知（非個人情報）

- 攻撃データ
- 行動データ
- ペルソナデータ
- デバイスデータ

API経由

（匿名化される個人情報）

- メールアドレス
- 住所
- 電話番号
- カード番号
- BIN番号
- その他

ルール
エンジン

リスクスコアリング

リスク判定

PASS

REVIEW

REJECT

キャプチャ率を増加させるために
ルールもスコアも調整

ThreatMetrix®

透過的な認証機能付通過型決済

クレジットカード番号を保持

消費者

加盟店サイト

ショッピング画面

1 ショッピング

2 画面遷移通過

9 カード情報

4 プロファイリング

ThreatMetrix
Digital Identity Network

5 API 呼出

6 リスクスコア返付

<TAGS>

加盟店サイト

カード番号

有効期限

決済画面

7

ACCEPT
REVIEW
DENY

10 オーソリ

カード会社

VISA
MasterCard
Diners Club INTERNATIONAL
JCB
AMERICAN EXPRESS
DISCOVER

¥ $ €

ThreatMetrix®

透過的な認証機能付非通過型決済

クレジットカード番号を非保持

消費者

加盟店サイト

ショッピング画面

1 ショッピング

2 画面遷移リンク

4 プロファイリング

ThreatMetrix
Digital Identity Network

5 API 呼出

6 リスクスコア返付

カード情報

9

決済代行

カード番号

有効期限

決済画面

7

ACCEPT
REVIEW
DENY

10 オーソリ

カード会社

VISA MasterCard Diners Club JCB DISCOVER

¥ $ €

<TAGS>

ThreatMetrix

透過的な認証機能付本人認証

購入者

加盟店サイト

ショッピング画面

1 ショッピング

2 画面遷移

3

4 プロファイリング

5 API 呼出

6 リスクスコア返付

ThreatMetrix
Digital Identity Network

イシュアーACS

クベース認証
ポップアップ

ACCEPT
CHALLENGE
DENY

7 認証要求

イシュアーACS

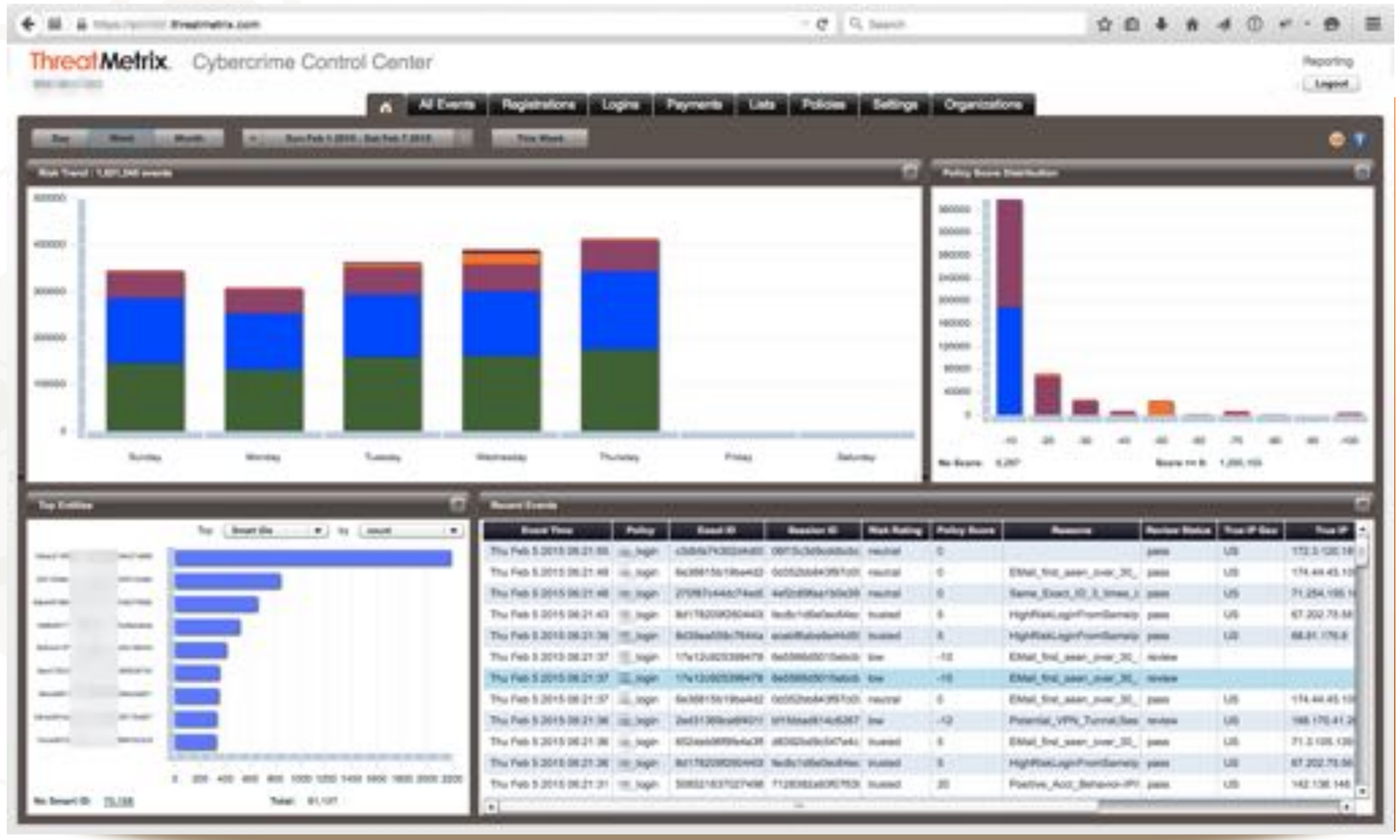
ユーザーID

パスワード

本人認証画面

ThreatMetrix

管理ポータルからのカスタマイズ、分析、レポート



- データの可視化による分析支援
- Eメールによるレポートとアラート
- 標準レポートとカスタマイズレポート

- トランザクションと端末の詳細情報
  - ルールの適用とカスタマイズ
    - データのエキスポート

ThreatMetrix®

セキュリティとプライバシー

個人情報を暗号化

- ThreatMetrix の API に渡される個人情報はユニークなプライベートキーで暗号化

個人情報は非共有

- プライベートキーで暗号化するのに先立って ThreatMetrix は一方行の暗号学的ハッシュ値を作成

Global Trust Intelligence Network

ThreatMetrix®

ThreatMetrixの製品歴史

2009
グローバル インテリジェンス
- デバイス ID
- プロキシー
- ピアシング

2010
意思決定管理
- ポリシーエンジン

2011
暗号化 & 匿名化
- アイデンティティ解析

2012
脅威 インテリジェンス
- マルウェア検知

2013
アイデンティティ & ペルソナ
- ペルソナID
- つながり分析
- モバイルSDK

2014
モバイル ファースト戦略
- モバイルマルウェア
- ジェイルブレイク検知
- アプリ改ざん検知

2015
オムニチャネル 保護
- 連携ハブ
- 暗号化データベース
- RAT検知

2016
動的意思決定
- ふるまい分析
- インテリジェンス拡張

リアルタイム分析
デジタル意思決定プラットフォーム

ThreatMetrix® デジタル・アイデンティティ・ネットワーク

ThreatMetrix®

ThreatMetrix®

Q&A

ThreatMetrix®
The Digital Identity Company™

THANK YOU

ThreatMetrix.com | sales@threatmetrix.com | partners@threatmetrix.com
1.408.200.5700 (Americas) | +61 2 9411 4499 (Asia Pacific) | +31 (0)20 800 0638 (EMEA)