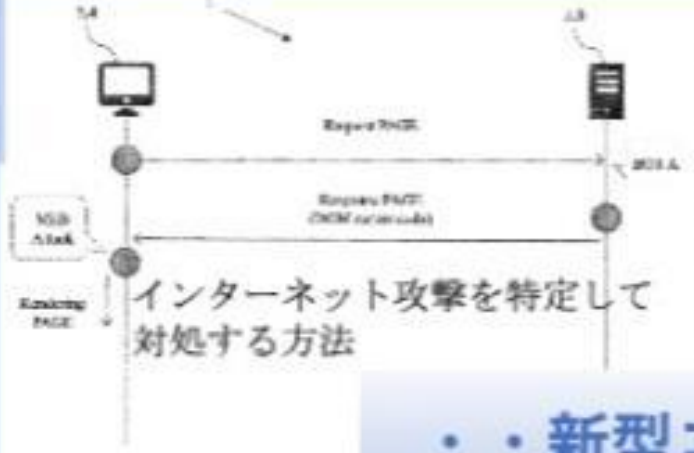
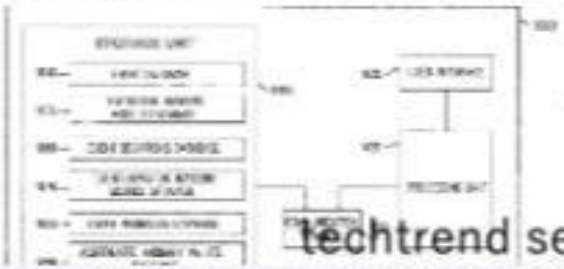


インターネット攻撃を特定して
対処する方法

ユーザー行動の再帰的異常検出による
内部脅威のインシデントの特定

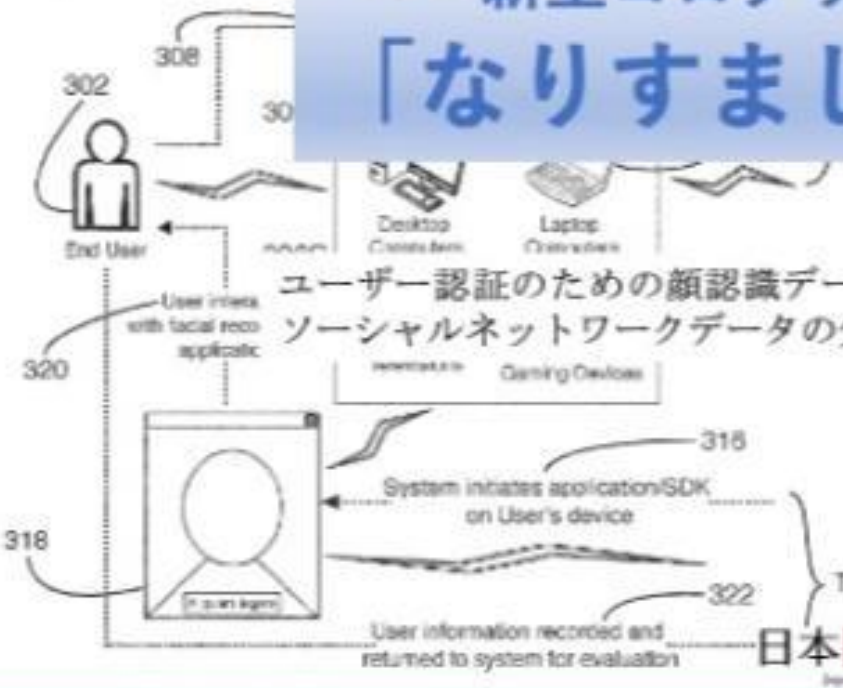


techtrend semimar

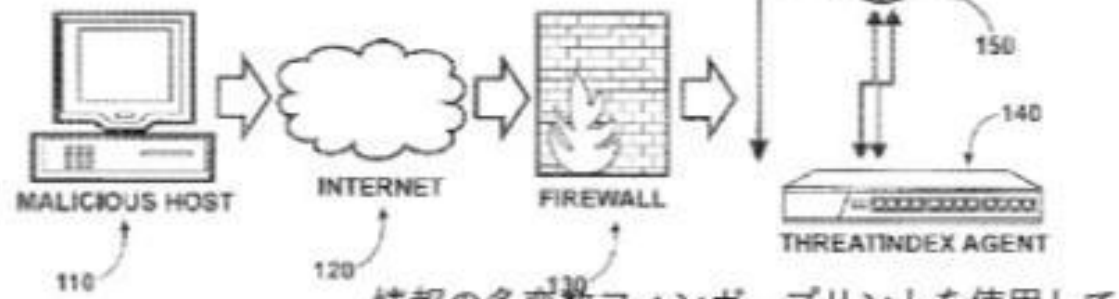
不正行為を特定するための詳細電話記録分析

・・新型コロナウイルスを悪用する詐欺の横行が続く・・

「なりすまし詐欺」対策システムと特許



ユーザー認証のための顔認識データと
ソーシャルネットワークデータの分析



情報の多変数フィンガープリントを使用して
ネットワーク上のマシンを追跡する方法

日本IT特許組合

河野特許事務所

講師紹介

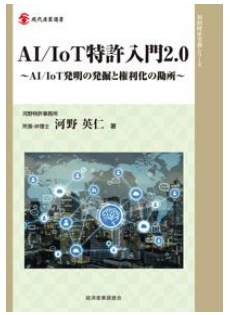
1996年立命館大学理工学部電気電子工学科卒業。
1998年立命館大学大学院理工学研究科情報システム学博士前期課程修了。
1999年弁理士登録。
2003年Birch,Stewart,Kolasch,&Birch,LLP(米国Virginia州)勤務。
2005年Franklin Pierce Law Center (米国New Hampshire州)知的財産権法修士修了。
2007年特定侵害訴訟代理人登録、清華大学法学院（北京）留学。中国知的財産権法夏期講習修了。
2009年～日本国際知的財産権保護協会(AIPPI)「コンピュータ・ソフトウェア関連およびビジネス分野等における保護」に関する研究会委員。
2010年北京同達信恒知識産権代理有限会社にて実務研修。
2011年~東京都知的財産総合センター専門相談員。
2012年~日本IT特許組合パートナー
2016年MIT(マサチューセッツ工科大学) Fintechコース受講
2018年MITコンピュータ科学・AI研究所 AIコース修了

言語：英語、中国語

著書

中国特許法と実務
経済産業調査会

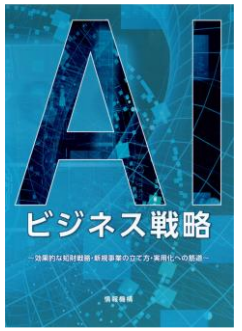
FinTech特許入門
経済産業調査会



AI/IoT特許入門2.0
経済産業調査会

世界のソフトウェア
特許改訂版(共著)
発明推進協会

パテントダイジェスト(Kindle版)
AI編、ブロックチェーン編、サイバーセキュリティ編



AIビジネス戦略
～効果的な知財戦略・新規事業の立て方・実用化への筋道～」(共著)
情報機構

インターネット攻撃を特定して対処する方法:　Cleafy

IVRシステム詐欺検出:　Pindrop Security

ID詐欺防止ソリューション:　Socure

デバイス指紋認証:　ThreatMETRIX

オーバーレイマルウェアを検出するデバイス、システム、および方法:
BioCatch

タッチ面にかかる力を推定するシステム、デバイス、および方法
BioCatch

ご紹介特許のタイトルと権利者

「なりすまし詐欺」対策システムとその特許

新型コロナウィルスを悪用する「なりすまし詐欺」が増えています。WHOやCDCにもなりすました詐欺目的のメールが横行していると言われています。
この「なりすまし詐欺」の主な手口は、偽サイトに誘導してログインIDやパスワードなどを奪うフィッシング詐欺、パスワードを搾取するため考えられる文字列を片っ端から試すアカウントリスト攻撃、SNS乗っ取り、なりすましメール、チケットなどの通販詐欺、有名人のアカウントなりすまし、など多岐にわたっています。
この講座では、この「なりすまし詐欺」に対するシステム面の対策とその特許について先進企業の事例をご紹介します。

【インターネット攻撃を特定して対処する方法】Cleafy

【IVRシステム詐欺検出】　Pindrop Security

【ID詐欺防止ソリューション】　Socure

【デバイス指紋認証】　ThreatMETRIX

【オーバーレイマルウェアを検出するデバイス、システム、および方法】BioCatch

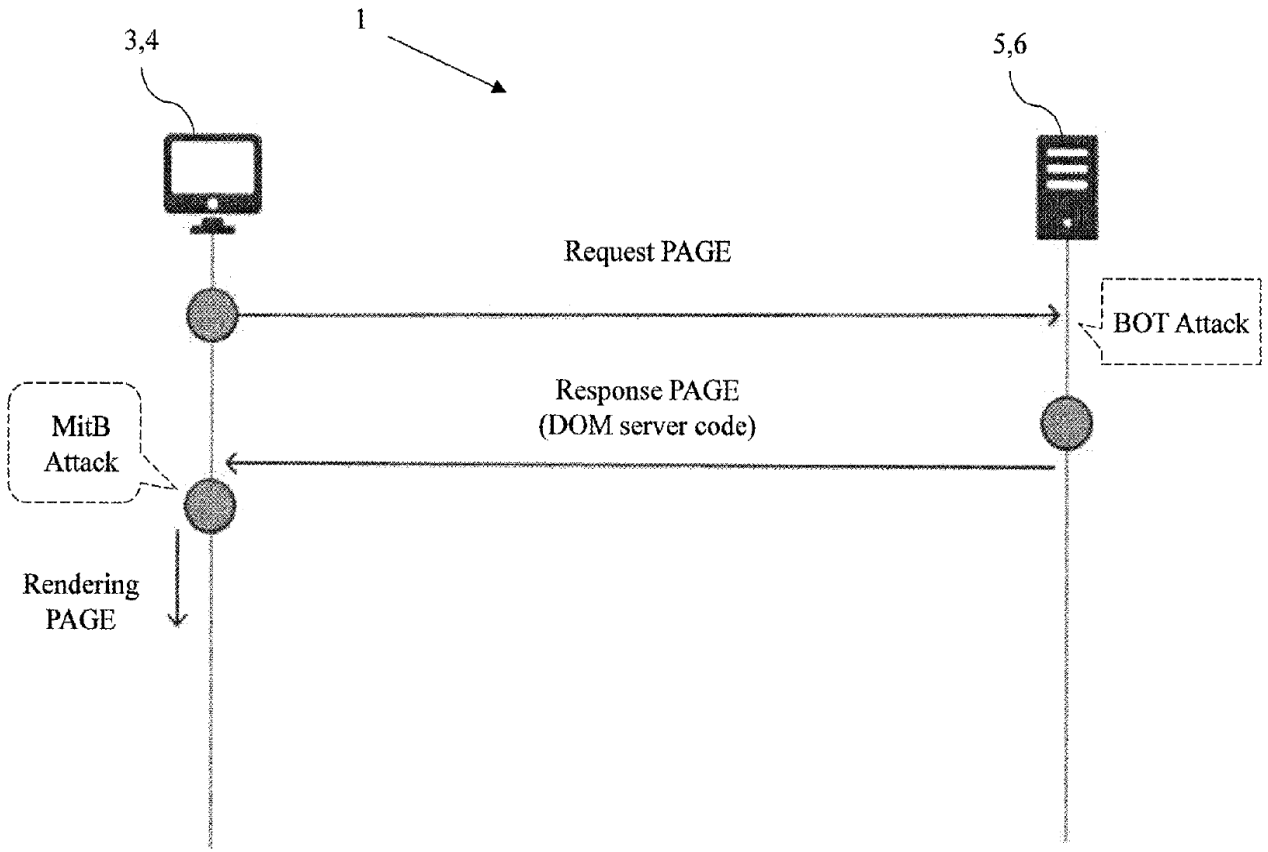
【タッチ面にかかる力を推定するシステム、デバイス、および方法】BioCatch

02701

【インターネット攻撃を特定して対処する方法】

マルウェアの検出

特許権者 Cleafy
出願日　2015年4月10日
登録日　2017年7月25日
登録番号 US9716726



本特許は、Man-in-the-Browser、Man-in-the-Middle、Bot攻撃を含むコンピュータセキュリティ攻撃に対抗するウイルス対策ソフトウェアに関する

Man-in-the-Browser（MitB）攻撃は、Webブラウザを直接操作して、ユーザーがWebサイトにアクセスしたときに表示されるコンテンツを変更する攻撃の一種である

Man-in-the-Browser攻撃は、ユーザーの知らないうちにコンピューターにインストールされたマルウェアを使用して実行される

このようなマルウェア（プロキシトロイの木馬など）は、Webブラウザープロセスのメモリと相互作用して、（Webブラウザーで使用される）システムコールの通常のフローを、追加のHTMLをダウンロードしたWebページに挿入するなどの目的を持つ特定のマルウェア機能にリダイレクトする

HTML/ScrInjectが最も多く検出されている。HTMLに埋め込まれた不正スクリプトであり、Webサイト閲覧時に実行される。

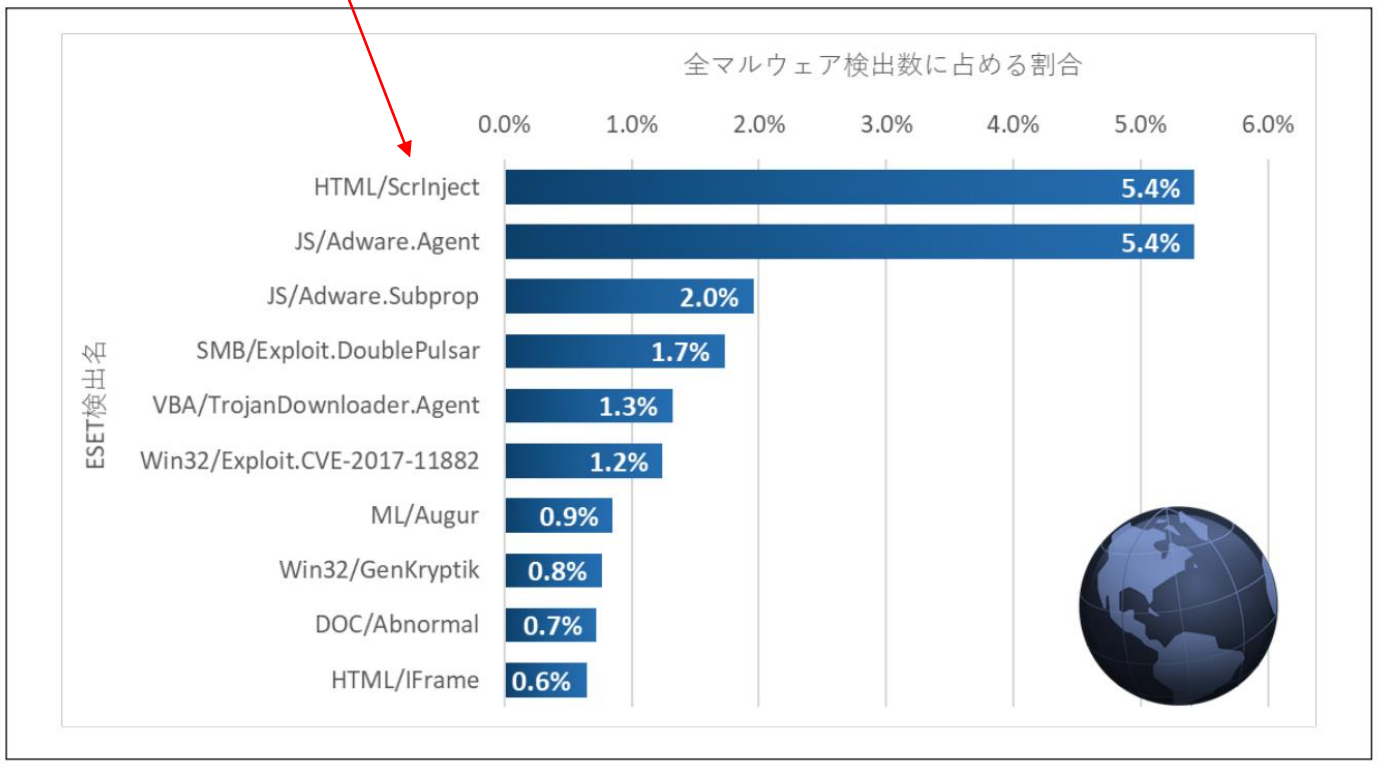


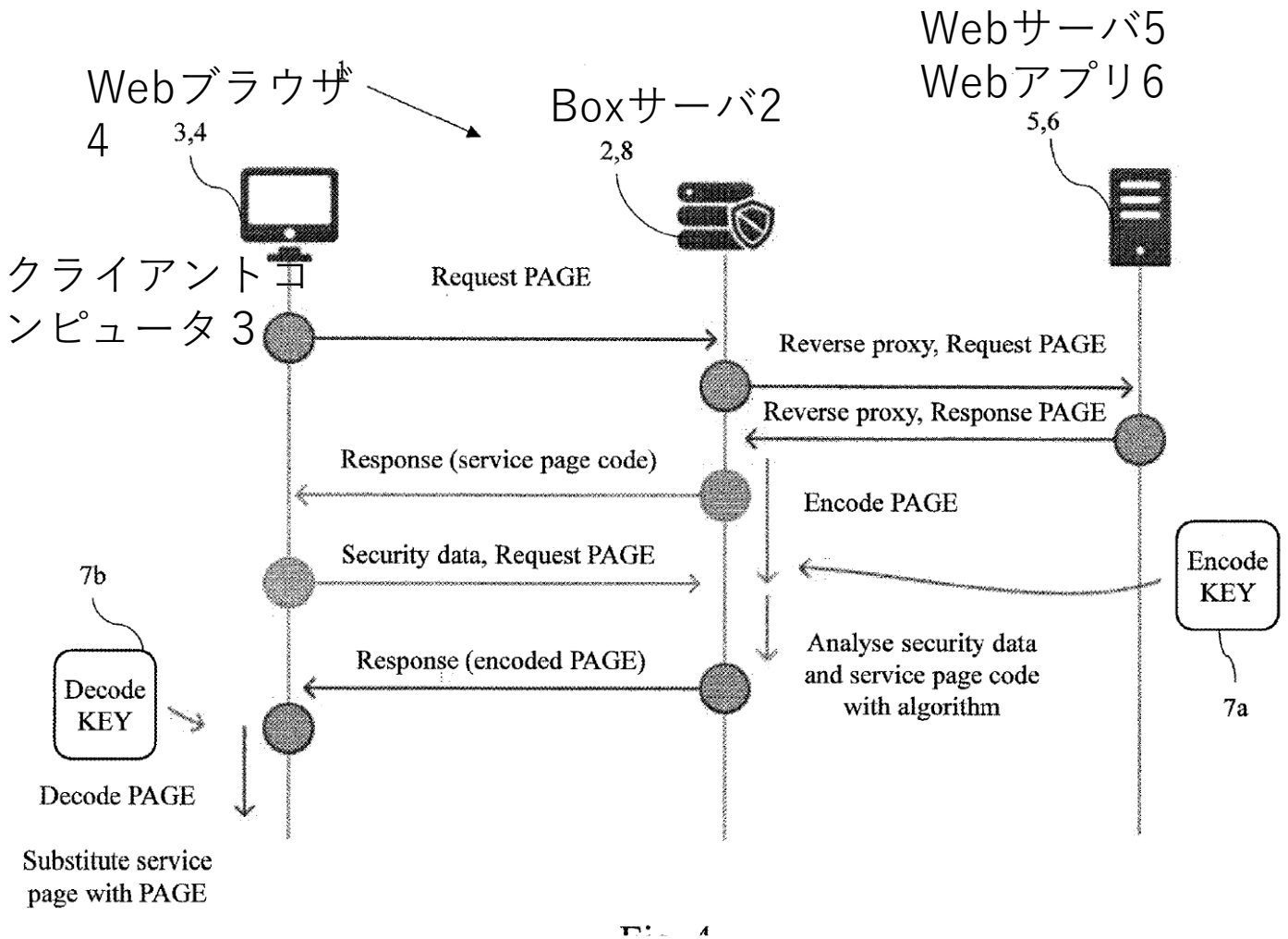
図1.2.2　世界全体におけるマルウェア検出の割合（2019年）

マルウェアレポート2019　キヤノンマーケティングジャパン株式会社

eバンキングおよびeコマースサイトからのクレジットカードデータの盗難や、ユーザーとの対話なしで自動的に開始されることが多い詐欺的なトランザクションなど、さまざまなMan-in-the-Browser攻撃が認められている。

ユーザーがWebブラウザーを介してWebページ（つまり、Webアプリケーション）を要求すると、そのWebページをホストするWebサーバーは、HTMLソースコード（Document Object Model、DOM）をWebブラウザーに送信する。

DOMコードは、ユーザーに表示するためにWebブラウザーのレンダリングエンジンに転送される。たとえば、マルウェアに感染したPCでは、WebブラウザがWebサーバーから受信したDOMコードは、Webブラウザのレンダリングエンジンで処理される前に、マルウェアによって変更される。
例）
ユーザーが実際に注文した送金を他の受信者にリダイレクトする
クレジットカードデータを要求する
ユーザーが追加データを入力するフィールドを追加する



Webブラウザー4は、Webサーバー5に常駐するWebアプリケーション6に関する要求を生成する

Webブラウザ4は、Webサーバ5と通信しているボックスサーバ2に、生成した要求を送信する

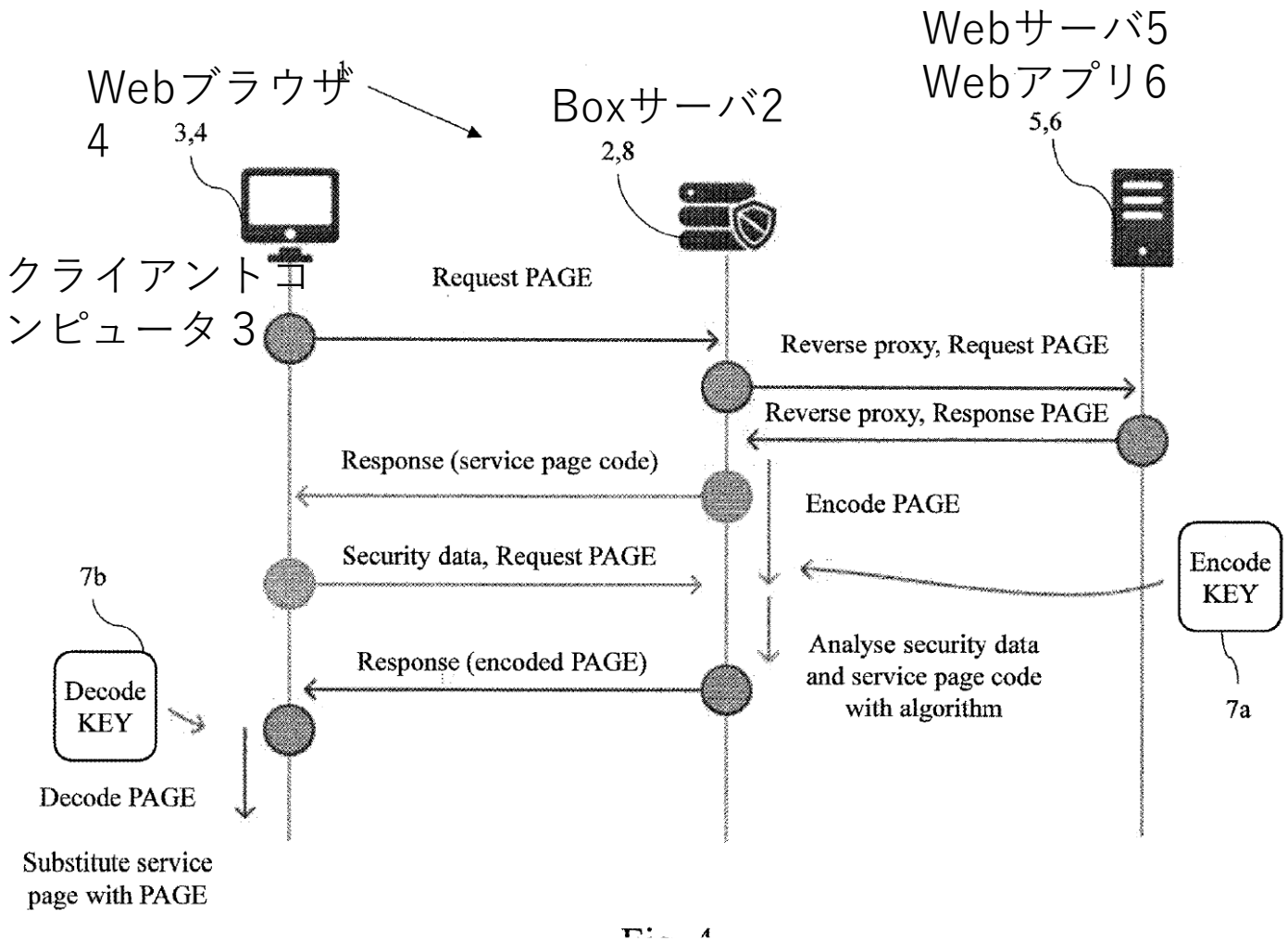
ボックスサーバー2はWebサーバ5から送信されたサーバー文書オブジェクトモデル（DOM: document object model）コードを受信する

要求に応答して、ボックスサーバ２によってWebブラウザ４にサービスページコードを送信する

サービスページコードは、難読化された多形のJavaScriptコードおよびHTMLコードを含む

Webブラウザ４はサービスページコードを受信してレンダリングする

Webブラウザ4によりレンダリングされたサービスページコードはボックスサーバー2に送信される



レンダリングされたサービスページコードと、元のサービスページコードとを、少なくとも1つのコードの違いが識別されるように、ボックスサーバー２にあるアルゴリズムアプリケーションによって処理および比較する

元のサービスページコードがレンダリングされたサービスページコードと互換性がない場合に、Man-in-the-Browser攻撃を示す信号を生成する

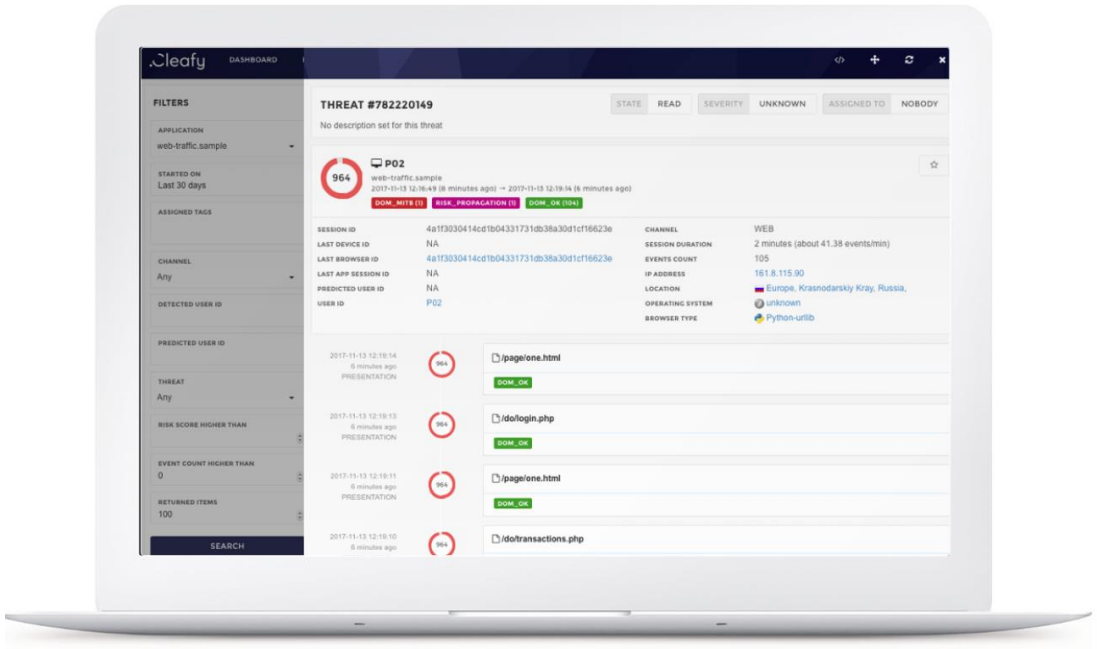
Cleafy社　2014年設立　本社イタリアミラノ
米国ボストンに子会社
詐欺検出ソリューションを金融機関に提供している

Cleafy

SOLUTIONS TECHNOLOGY RESOURCES WEBINARS PARTNERS JOBS ABOUT CONT

ADVANCED THREAT DETECTION & PROTECTION

Real-time, continuous application monitoring and risk assessment
for adaptive threat detection & protection against today advanced attacks from unmanaged endpoints



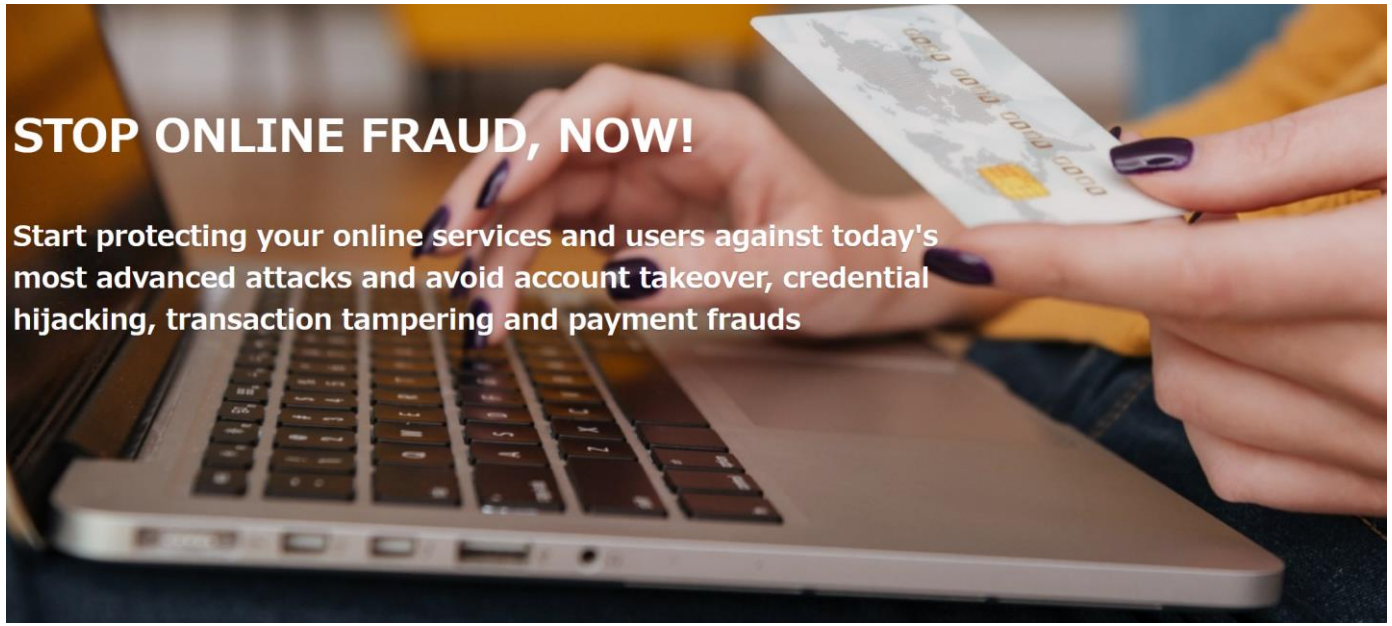
We had a great experience with Cleafy - both the company and the solution.

CISO
European Bank
Gartner Peer Insights review

Gartner peerinsights™ | How satisfied is your organization with the value the product provides for the money spent? ★★★★★

[Cleafy] is able to continuously monitor and assess the risk of the application behaviors using cumulative session risk

Cleafy社HPより2020年9月5日https://www.cleafy.com/



Cleafyの使用により、高度な脅威とアカウント乗っ取り、 IDの乗っ取り、トランザクションの改ざん、支払い詐欺のシナリオをリアルタイムで検出できる。

Cleafyは、Gartner Market Guide for Online Fraud Detection 2020の代表ベンダーとしてリストされている（「デバイスの評価、エンドポイントマルウェアの検出と行動分析」部門）。

【不正行為を特定するための詳細記録分析の呼び出し】

IVRシステム詐欺検出

特許権者 Pindrop Security Inc
出願日 2016年10月14日
登録日 2018年3月27日
登録番号 US9930186

Timestamp	Step	Status
7:39am	Language Menu	SUCCESS
7:39am	Account Entity	SUCCESS
7:41am	PIN Entry	FAIl
7:42am	PIN Entry	SUC
7:42am	Balance Check	SUC

Timestamp	Step	Status
7:39am	Language Menu	SUCCESS
7:39am	Account Entry	SUCCESS
7:41am	PIN Entry	FAILURE
7:41am	PIN Entry	FAILURE
7:41am	PIN Entry	FAILURE
7:42am	SSN Entry	FAILURE
7:43am	SSN Entry	FAILURE
7:43am	SSN Entry	SUCCESS
7:44am	Balance Check	SUCCESS
7:44am	PIN Change	SUCCESS

特許権者　Pindrop Security Inc
出願日　2016年10月14日
登録日　2018年3月27日
登録番号 US9930186

不正行為を特定するための詳細記録分析の呼び出し

IVR(Interactive Voice Response自動音声応答装置)システムにおける操作記録を機械学習により分析し、詐欺の有無を検出するアイデア

左側：真正ユーザのIVRコールフロー

右側：フィッシングの試み：ユーザーはPINの入力を数回試行して失敗し、次に別の認証方法を試行してアカウントへのアクセスに成功。

　アカウントの残高を確認した後、ユーザーはPINを変更してアカウントを乗っ取ろうとしている。

通常はノード（送信元）から１－３の宛先

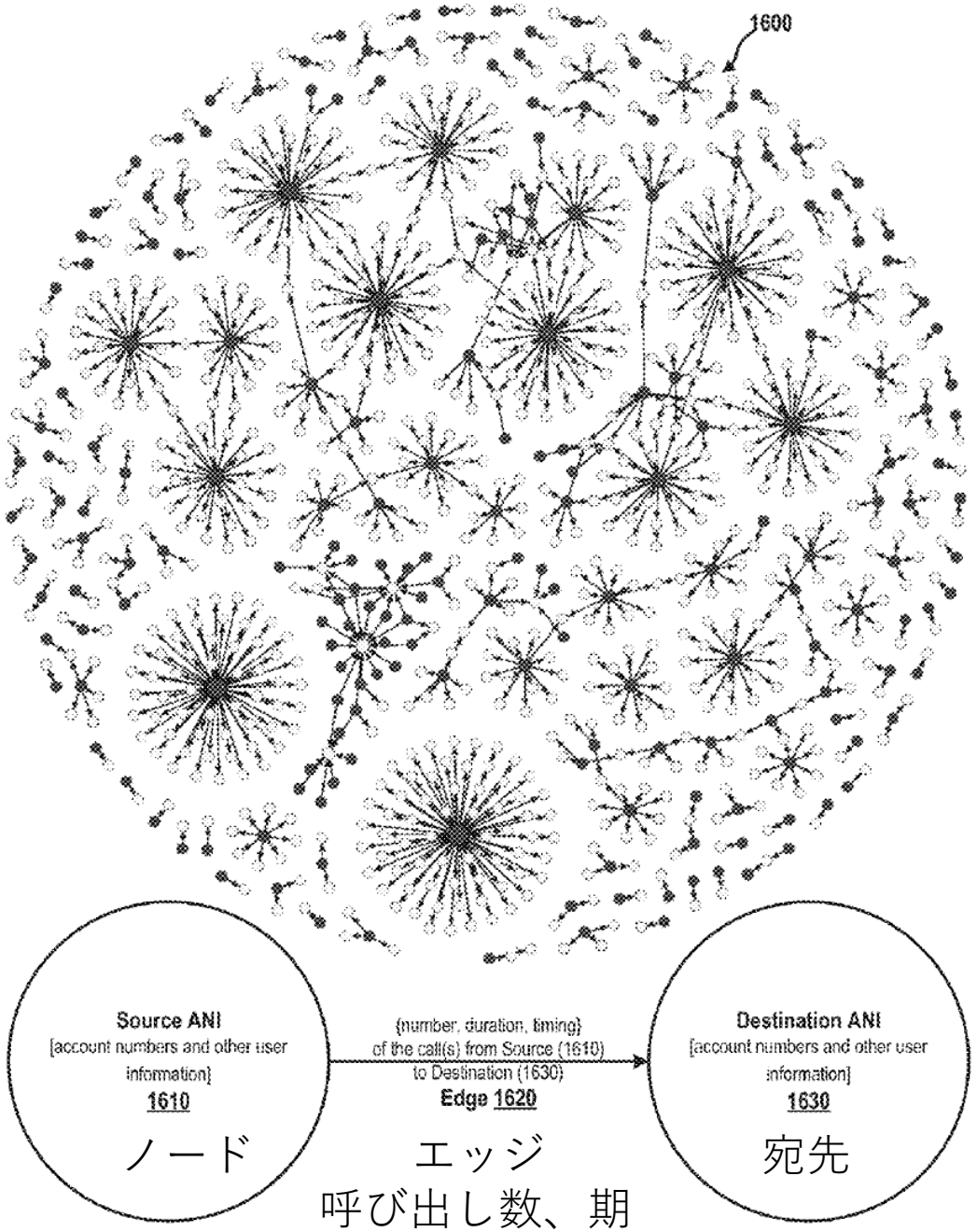
呼び出し数、期間、タイミングによりグラフが特徴づけられる

多数の宛先の場合、スパマーマーケティングの可能性

送信元・送信先のいずれをも示す場合、プレミアムレート詐欺（ワン切り詐欺）

トラフィックポンピング・・・フリーダイヤル番号への通話中に可能な限り多くの時間を使用することや、フリーダイヤル番号への異常に高い回数の通話を行うことが含まれる。トラフィックポンピングにおける悪いアクターの目的は、発信者のローカル交換キャリアの料金を増やすことである可能性がある。

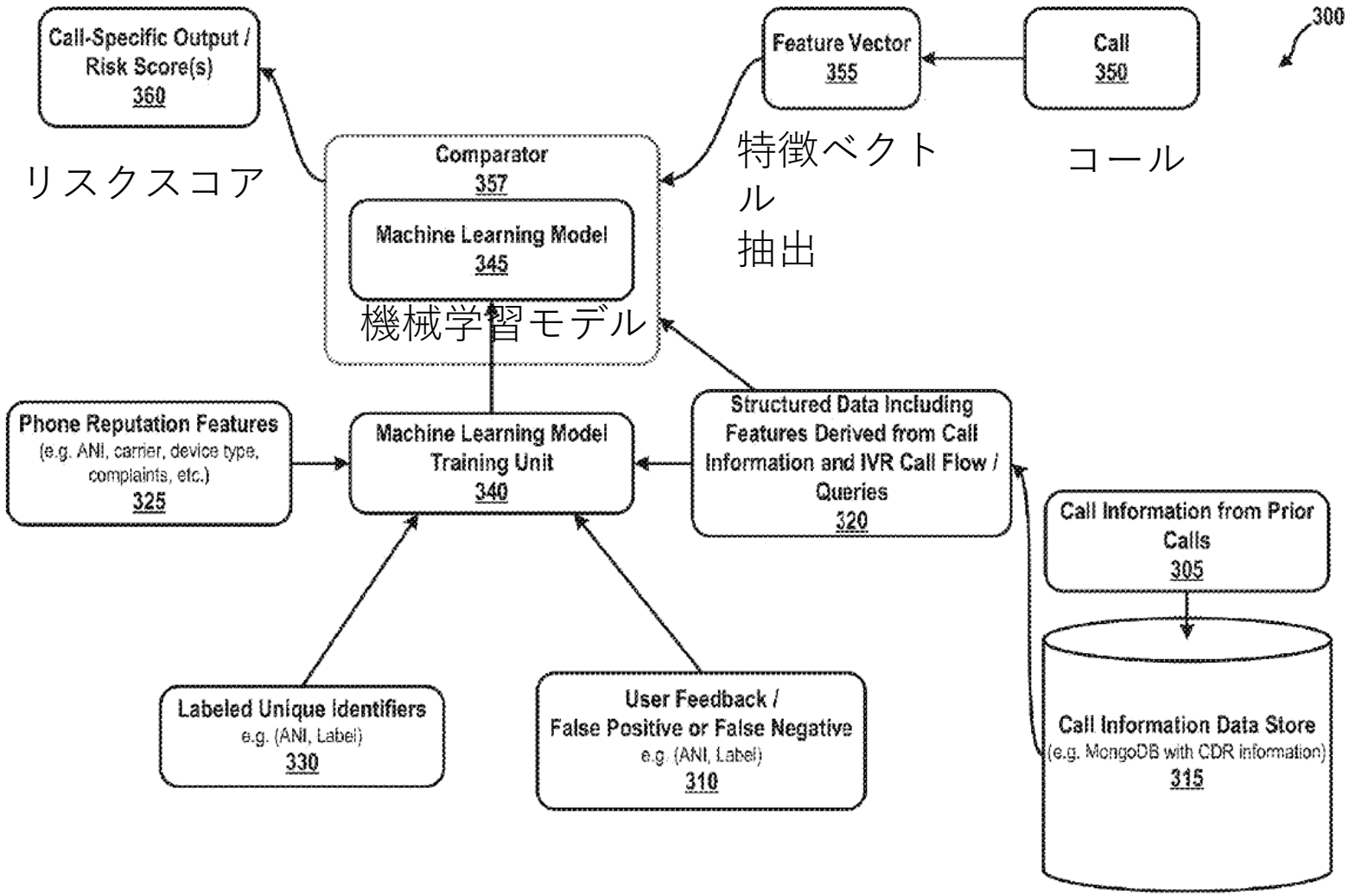
機械学習によりこれらの詐欺を検出する。



ノード

エッジ
呼び出し数、期間、タイミング

宛先



リスクスコア

特徴ベクトル抽出

コール

機械学習モデル

特徴ベクトル

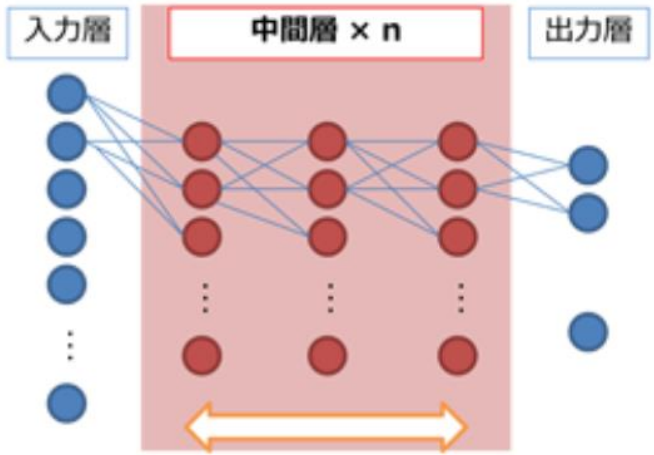
評判特徴ベクトル・・・キャリア、デバイスの種類（固定電話、携帯電話、VoIP、ソフトフォン、特定の電話モデルなど）、発信者の電話に関連する苦情など

速度特徴ベクトル・・・ソースが呼び出した宛先の数、コールの平均頻度、コールのインターバルなど

動作特徴ベクトル・・・DTMF(Dual-Tone Multi-Frequency:トーン信号)トーンの音量や持続時間、DTMFトーン、音声ナビゲーションなど

コール

特徴ベクトル生成
評判特徴
速度特徴
動作特徴



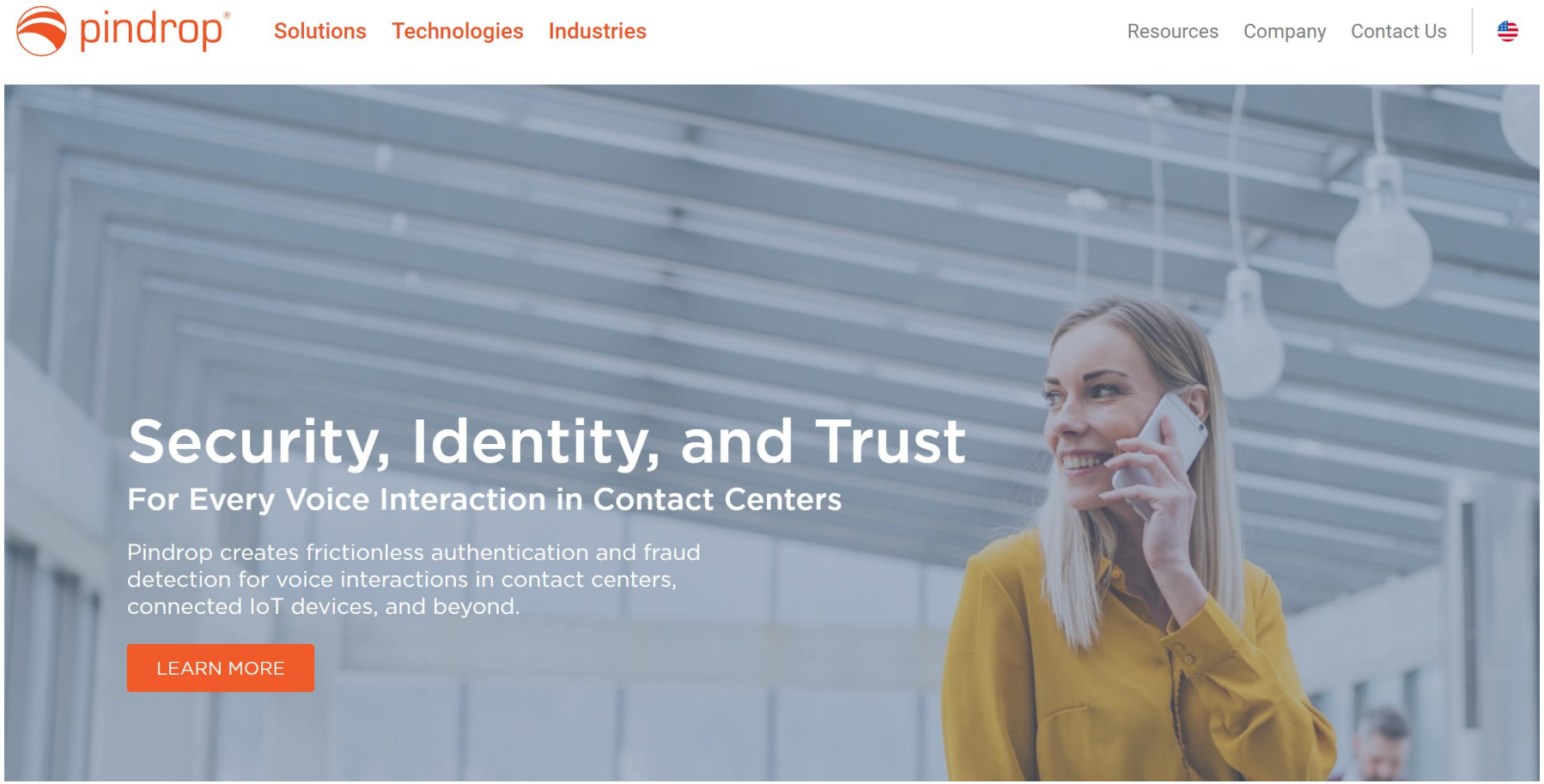
ディープラーニングモデル

詐欺スコア

Pindrop Security社　米国の情報セキュリティ会社　　2015年設立

電話をリスクスコアリングして詐欺を検出し、発信者を認証する

147の異なる通話機能をAIで分析する



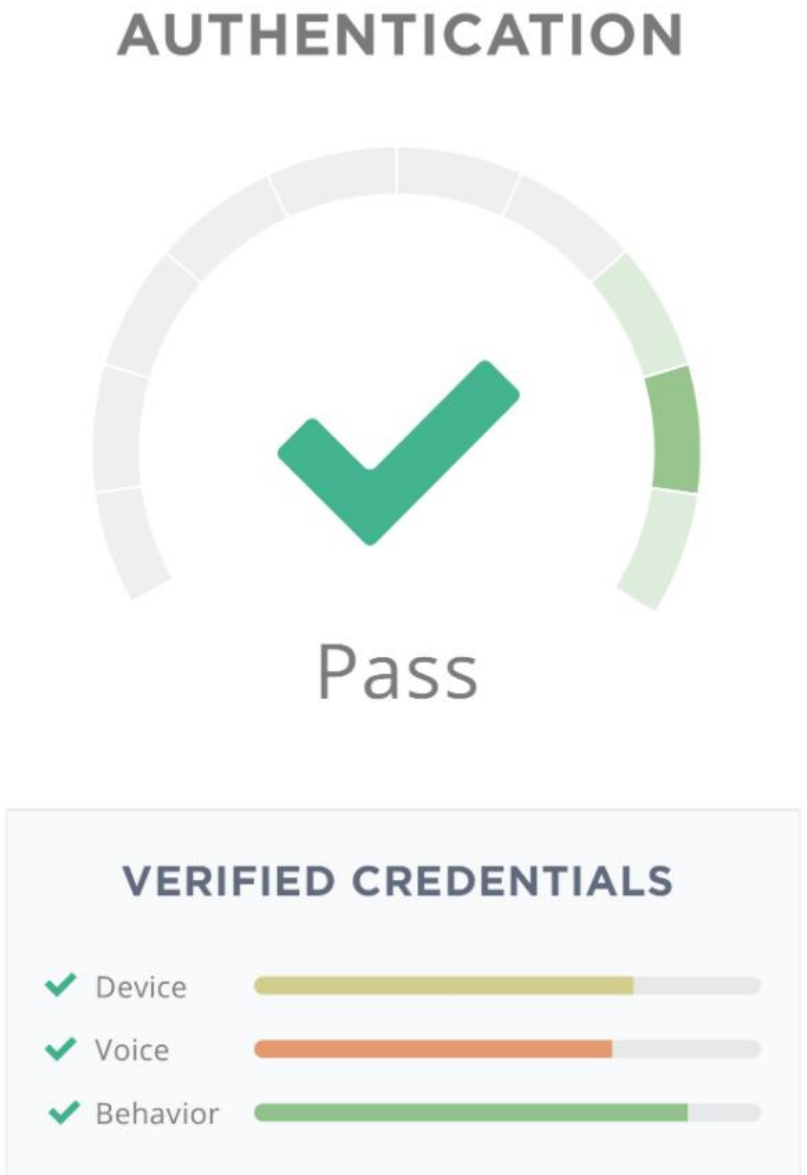
Pindrop Security社HP2020年9月6日
https://www.pindrop.com/

電話の受付

AIによる認証
電話番号、音声、
デバイス、行動から
スコアリング

AIによる認証
後、エージェ
ントに接続

平均ハンドリング
時間の減少



Pindrop Passportソリューション

Pindrop Passportは、コールセンターの相互作用をリアルタイムで評価して、正当な顧客を受動的に認証する。

Passportはすべての通話のバックグラウンドで実行され、特許取得済みのPhoneprinting®テクノロジーと独自のDeep Voice™生体認証を組み合わせて、発信者がアカウントにアクセスするための適切なデバイス、音声、および動作を持っているかどうかを判断する。

導入事例
保険会社　保険会社はクレーム詐欺に対し対策を強化しているが、アカウントの乗っ取り等の新たな詐欺が増加、巧妙化している。被害額は一般の金融機関の約３倍。大手７社の内５社が導入。

小売　Shop Direct(英国のデジタル小売業者)　不正行為の増加に対するソリューションとして導入

02703

【ユーザー認証のための顔認識データとソーシャルネットワークデータの分析】

ID詐欺防止ソリューション

Socure
出願日　2015年6月11日
登録日　2018年12月11日
登録番号 US10154030

オンラインでのID詐欺が急激に増加している

米国では毎年約1,300万人のID盗難が生じている

これにより金融機関は年間170億ドル、小売業では年間1千億ドルもの損害が生じている

顔認証に加えて、SNSを通じたインターネットデータをも用いて総合的に認証するアイデア

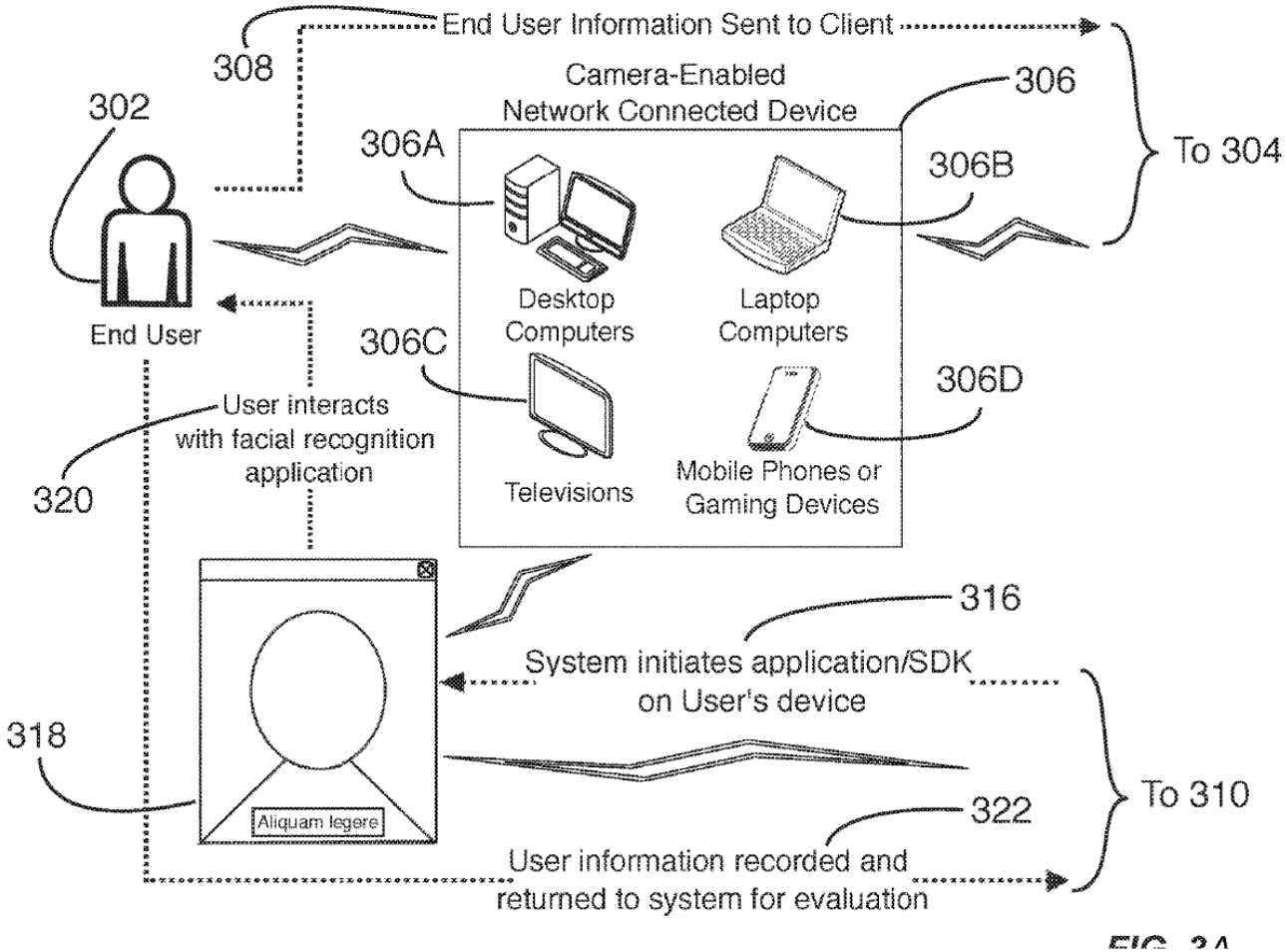
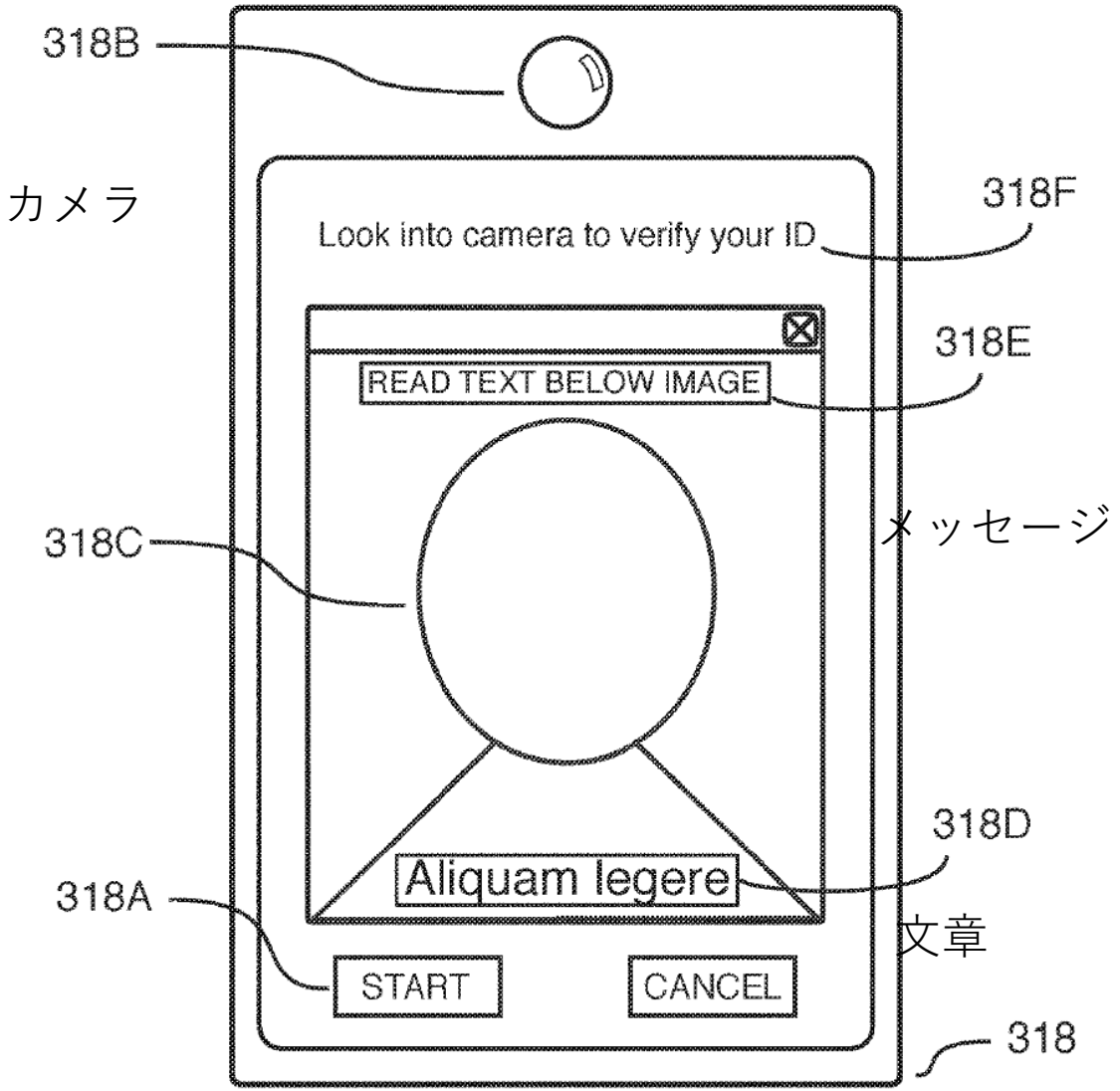


FIG. 3A



顔認証時に、活気(liveliness)スコアを算出する

顔を撮影し、表示された文章を読ませる、ジェスチャーをとらせる

解剖学的に適切な動きを行っているか、動きベクトルを機械学習モデルを用いてスコアを求める

本人でない、写真を用いている等の不正を排除する

その他の入力データ、デバイスから得られるデータ（OS、ブラウザ、IPアドレス等）を考慮して認証スコアを求める

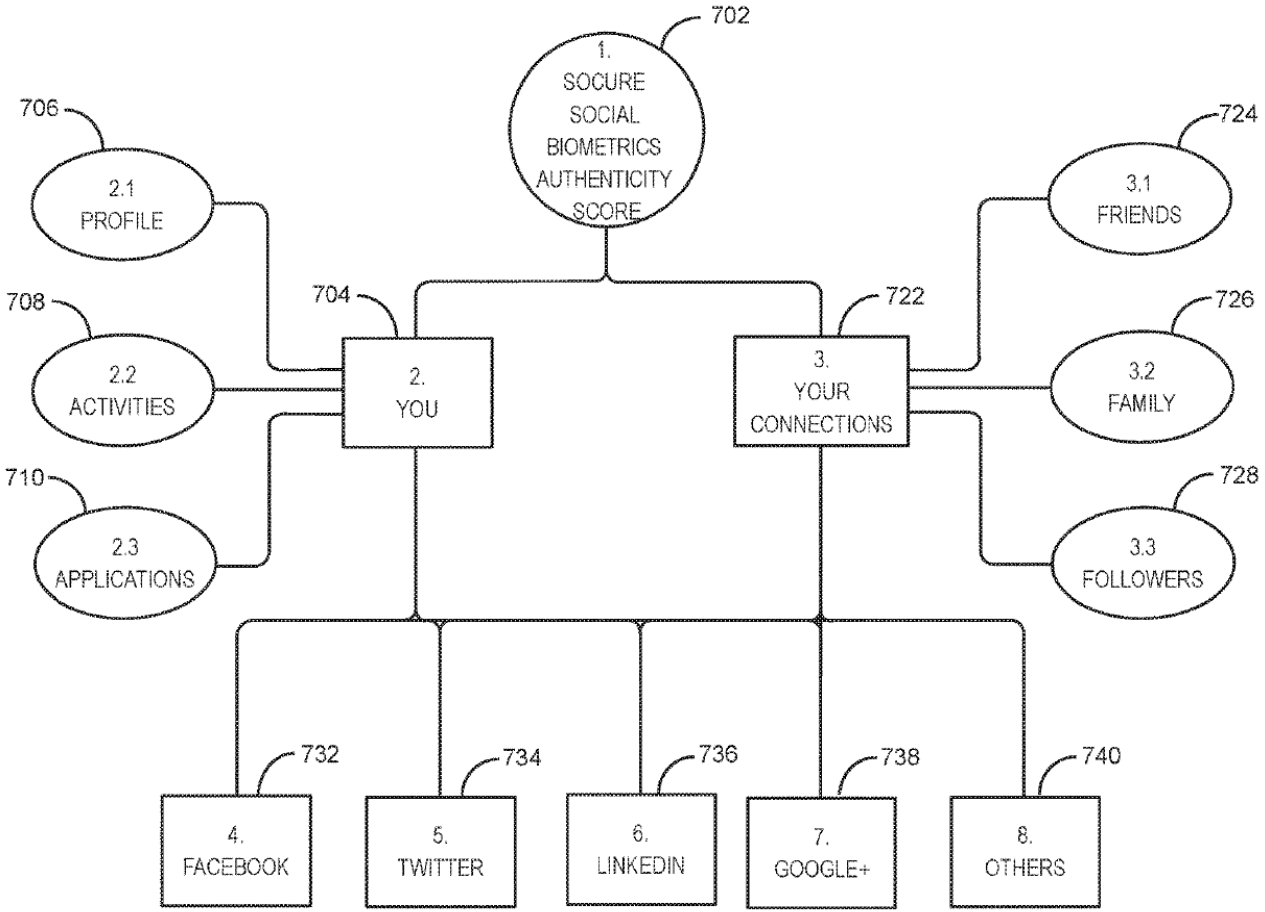


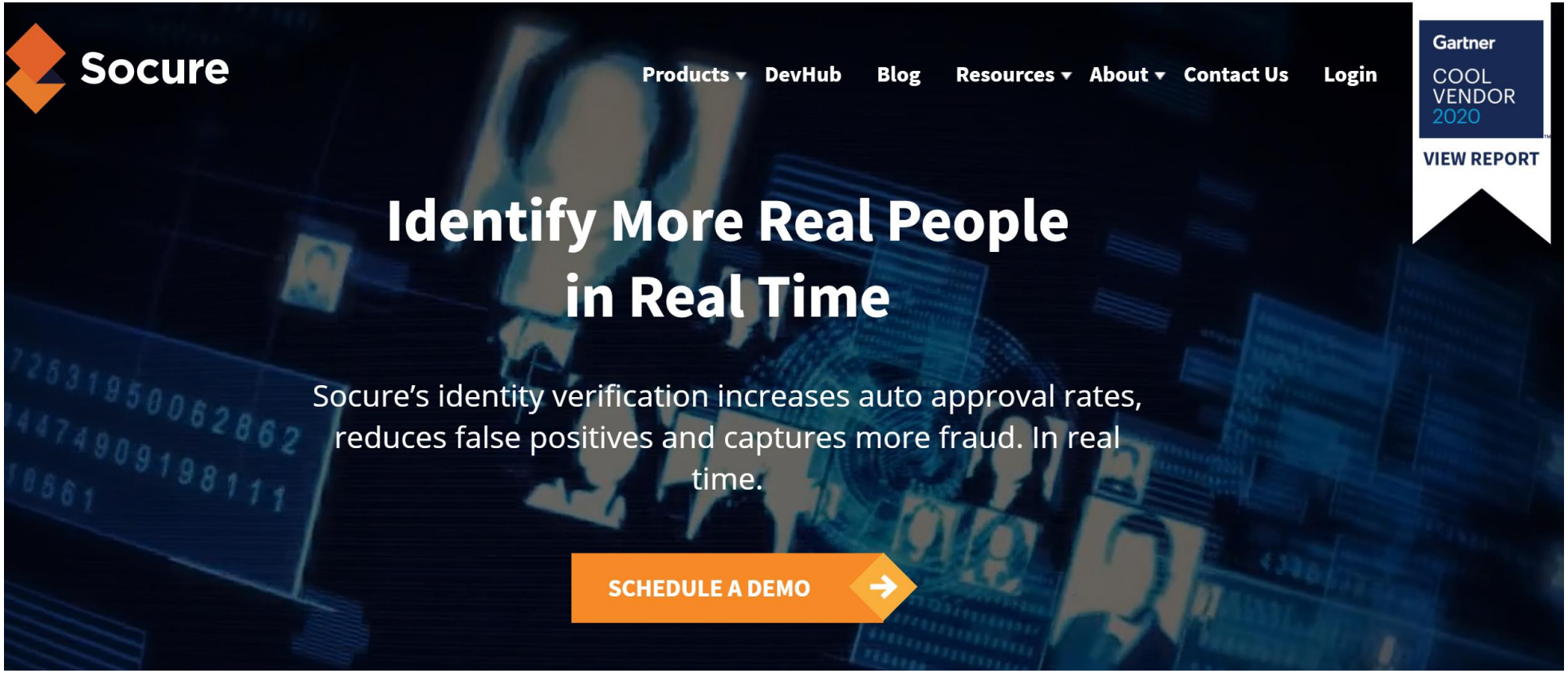
FIG. 7

Facebook、ツイッター等のSNS、専門職のネットワークから抽出されるデータを機械学習モデルに入力し、ユーザスコアを求める

本人だけでなくSNSのつながりを追跡し、情報を収集し、ユーザスコアを求める・・友人、家族、フォロワー

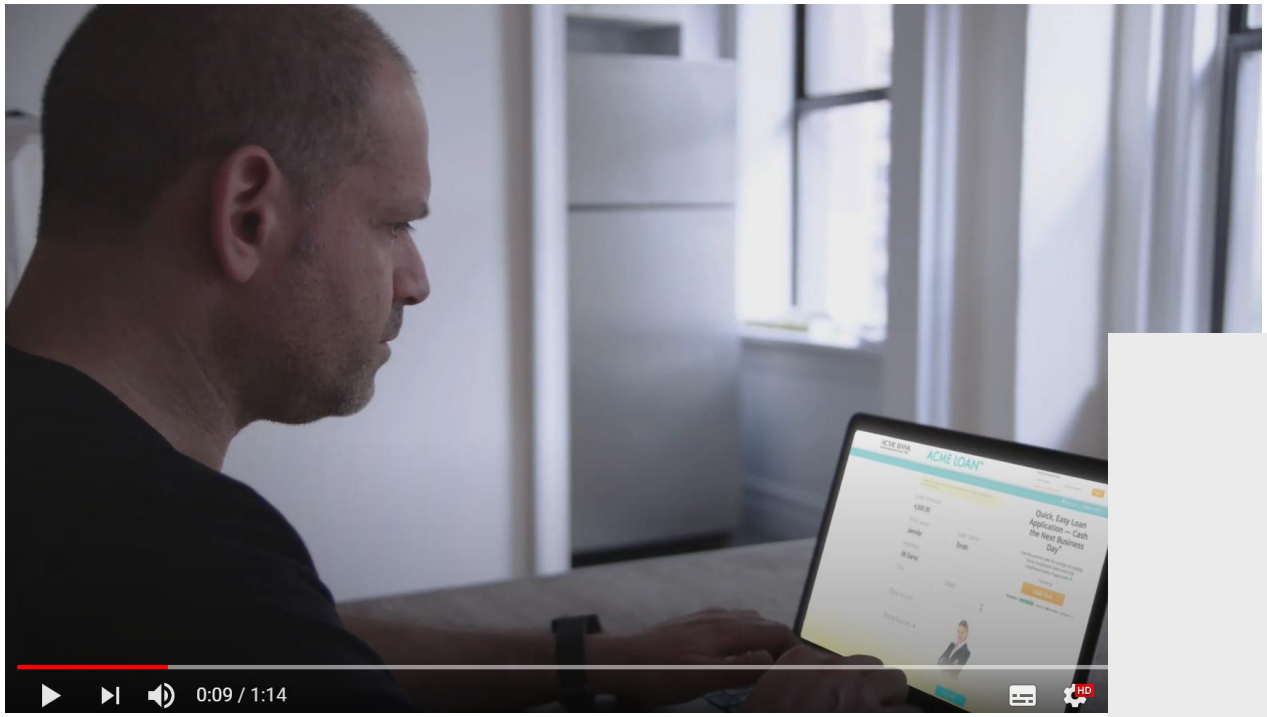
投稿の頻度、投稿した位置等のデータもスコアを求める際に考慮される

ユーザスコア、認証スコアを総合的に考慮して本人認証を行う

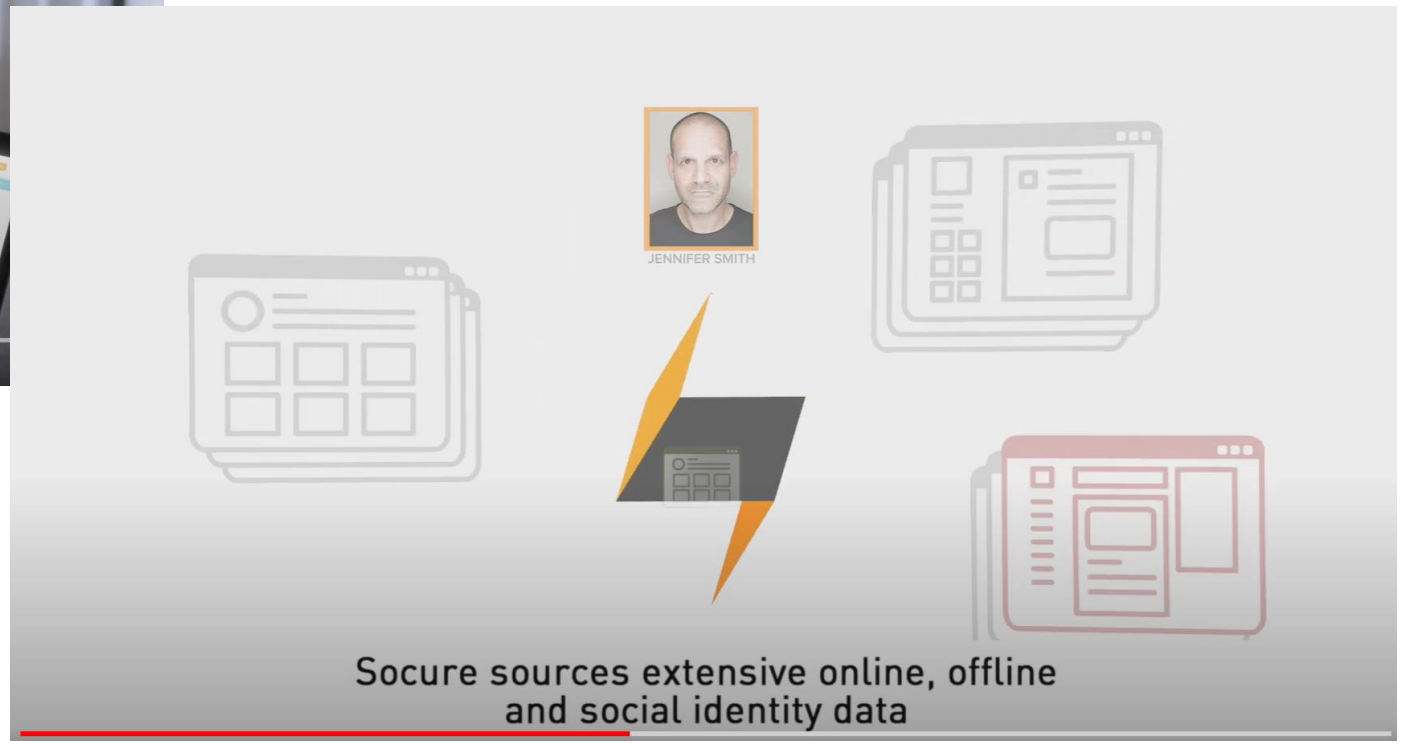


Socure社HPより2020年9月10日
https://www.socure.com/

Socure社　2012年設立　本社米国ニューヨーク
金融取引時における本人認証ソリューションを提供している。
95％の予測精度を持つAI「Aida」
信用調査機関、電子メールの履歴、電話の記録、IPアドレス、ソーシャルネットワークなど、数百のオンラインおよびオフラインのデータソースからデータを取り込み、AIモデルを学習し、顧客からのフィードバックを得て精度向上



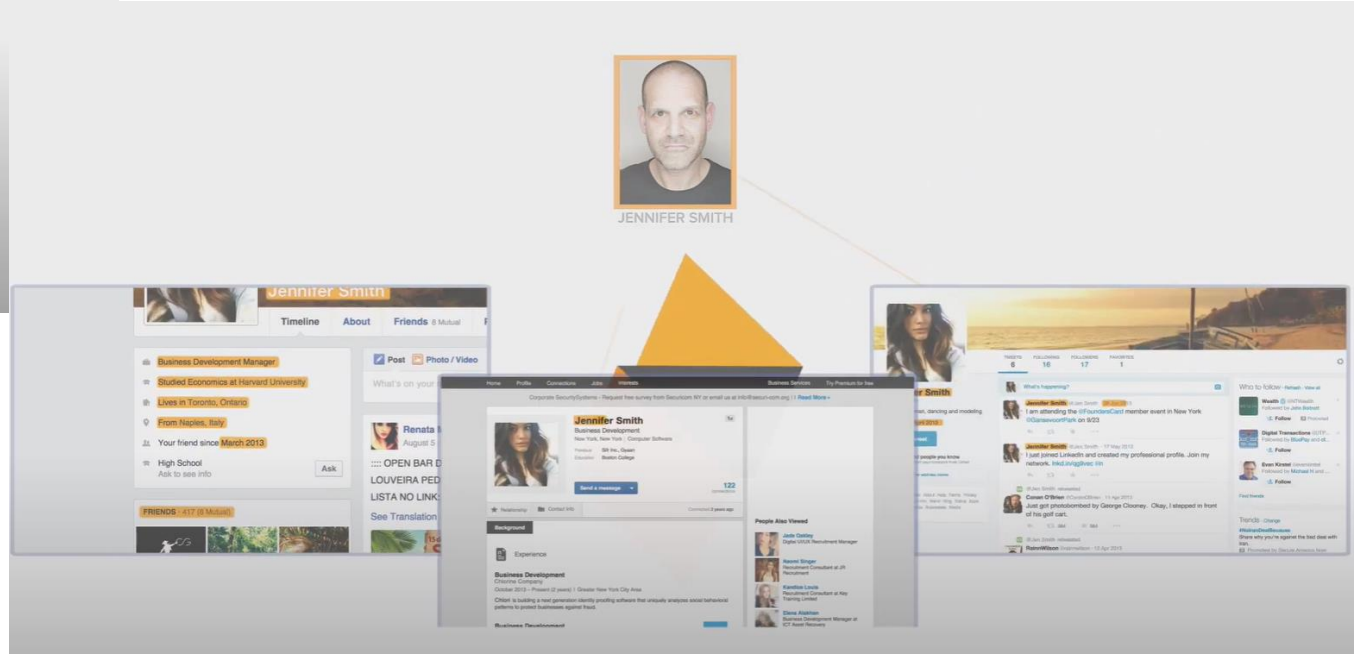
不正ログインの試みが増加



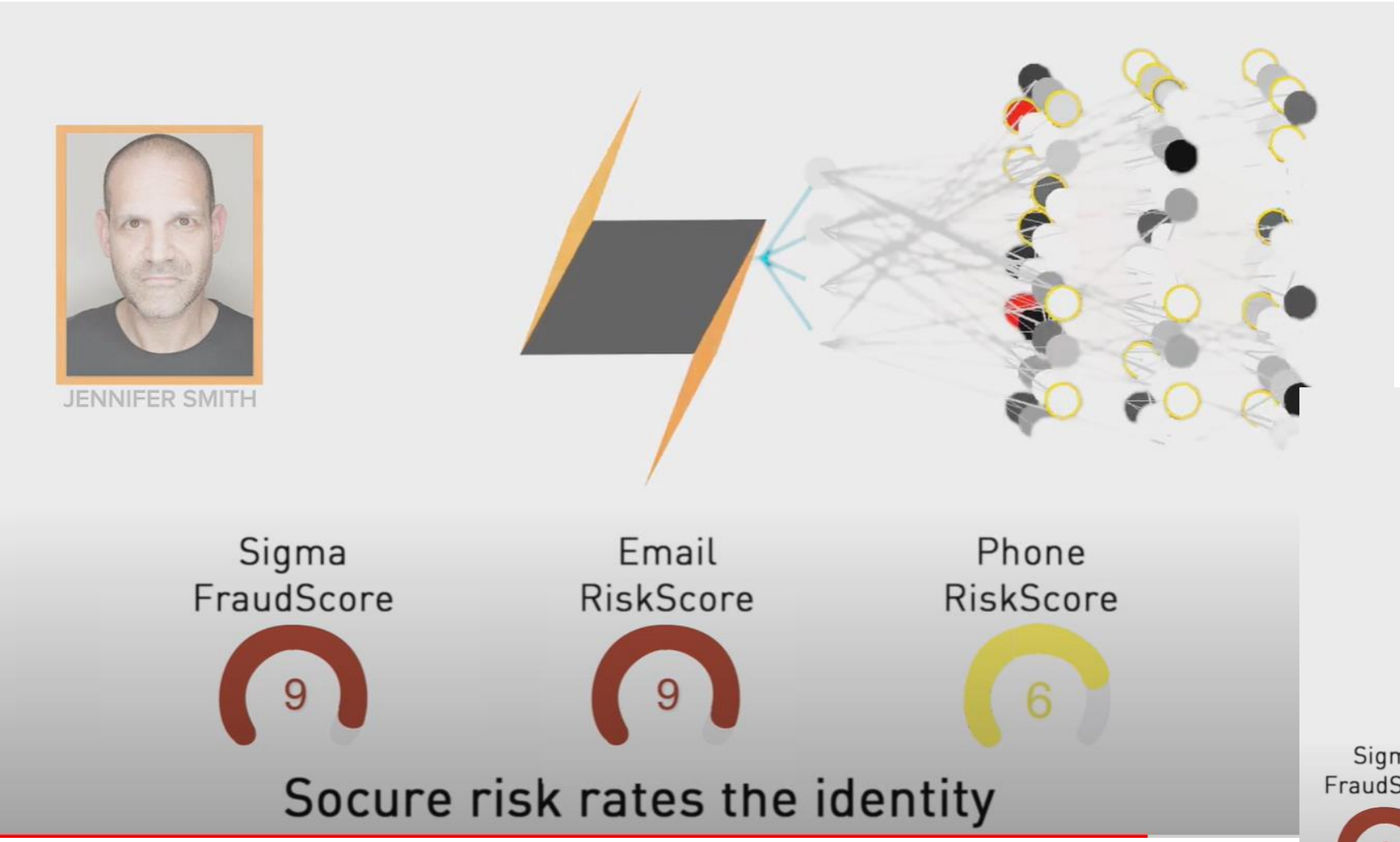
顔認証、活性認証に加えて、オンライン、オフライン、SNS等のデータを収集する

YouTubeより2020年9月10日
https://www.youtube.com/watch?v=kjpUv7a7JvI

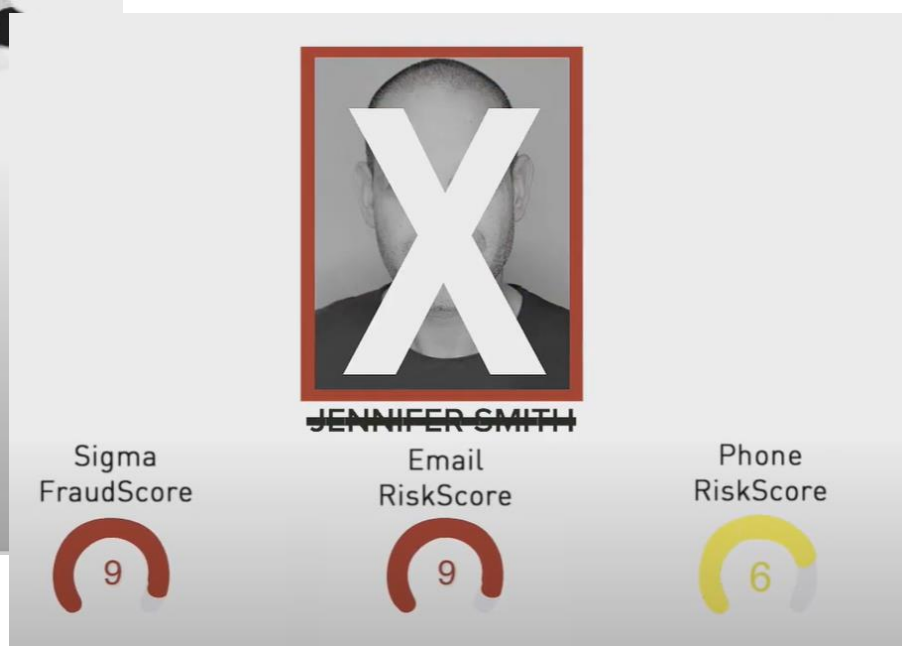
様々なインターネットデータを取り込む



SNSのデータをつながりをもたどって収集



ディープラーニングモデルにデータを入力し、詐欺スコア、リスクスコア等を導出する

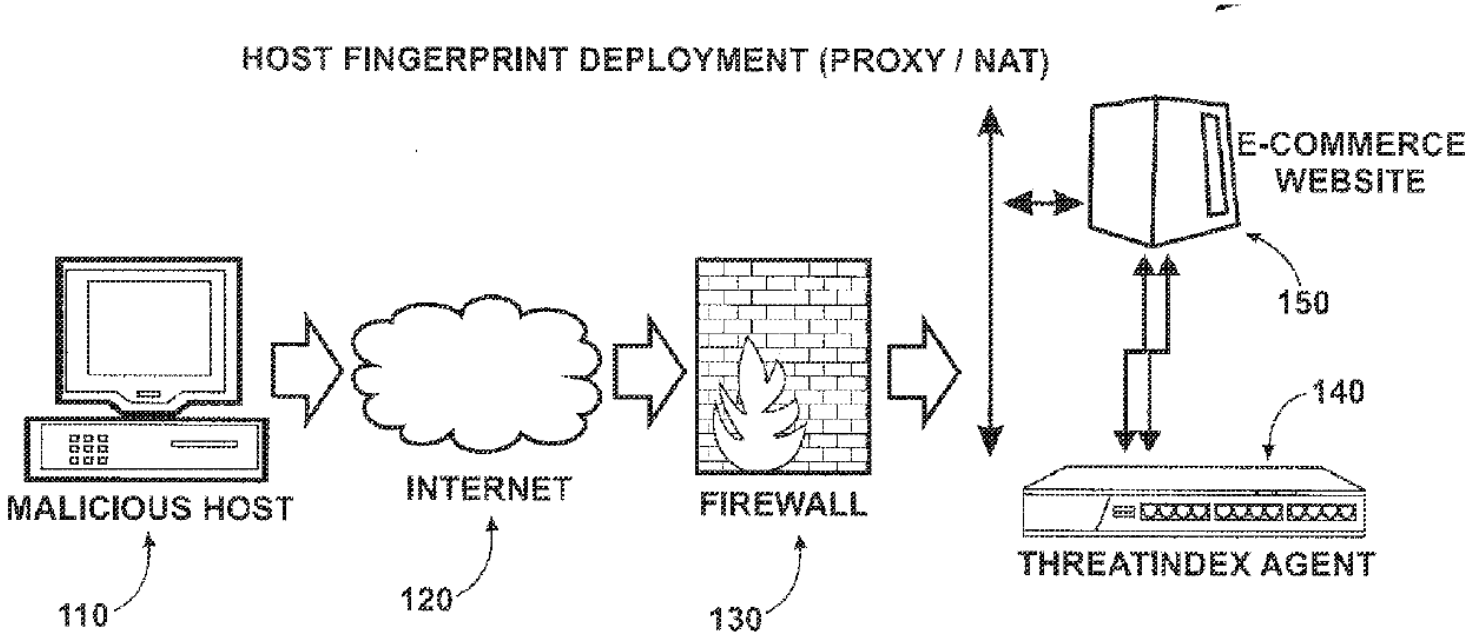


スコアが低いと認証拒否

【デバイス指紋認証】

ThreatMETRIX
出願日　2014年8月8日
登録日　2016年9月13日
登録番号 US9444835

出願日　2018年9月14日
登録日　2020年9月10日
登録番号 US10764297

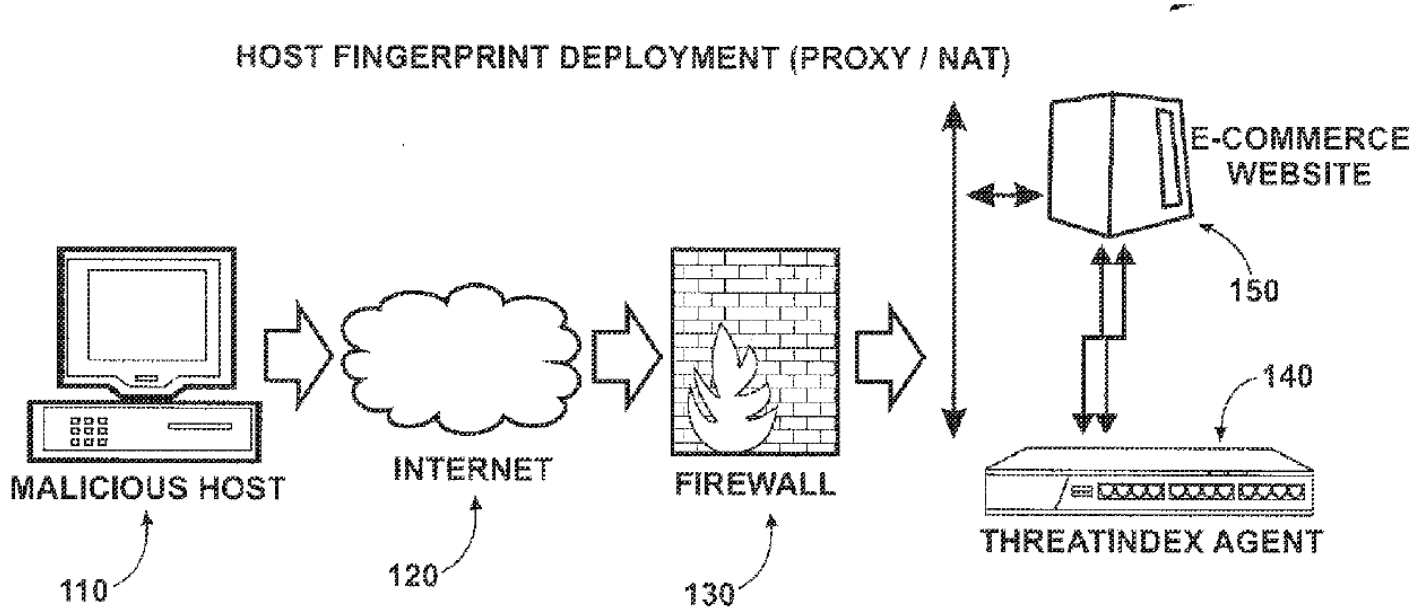


「受動的に利用可能な情報の多変数指紋を使用してネットワーク上のマシンを追跡する方法」、「匿名化されたペルソナ識別子」

世界中の企業がデジタル通信とトランザクションについてインターネットへの依存度を高めており、同時にサイバー犯罪による危険性が高まっている
信頼できる顧客とサイバー犯罪者を区別するための戦略が必要となる

技術的な知識が豊富な詐欺犯は、かつて安全であると考えられていたオンライントランザクションおよび認証システムを標的とする高度な詐欺スキームを開発し続けている

デバイス指紋と、ペルソナIDを活用して不正を防止する



コンピュータとWebサイトとの通信を監視する

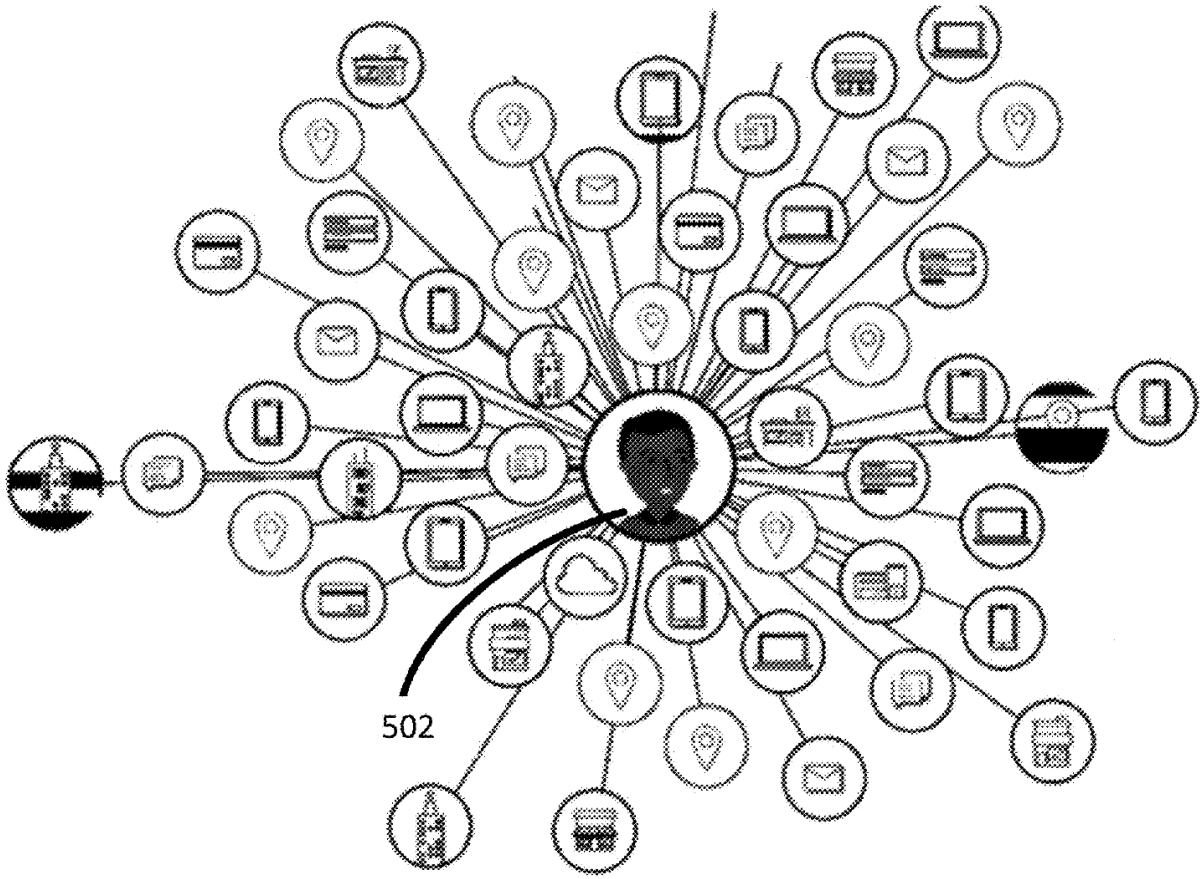
IPアドレス及びデバイス指紋を取得する

デバイス指紋：TCPウィンドウサイズ、最大転送単位、接続タイプ、接続速度、画面解像度等の情報を組み合わせてデジタル指紋を生成する

悪意のあるコンピュータを特定した場合、IPアドレス、デバイス指紋をブラックリストに登録しておく

他のコンピュータと他のWebサイトとのトラフィックを監視

デバイス指紋がブラックリストに登録されている場合、悪意のあるコンピュータであると特定



名前、電子メールアドレス、物理アドレス、電話番号、IPアドレス、デジタルデバイス識別子、イベント、およびトランザクション等の複数の属性表示を受信する

複数の属性表示のそれぞれの時間情報を抽出する。

複数の属性表示のそれぞれについて、ユーザ502に対応するリンケージスコアを決定する

ユーザ502についての複数の属性変数の異常スコアを決定する。異常スコアは、通常の動作からの逸脱を表す

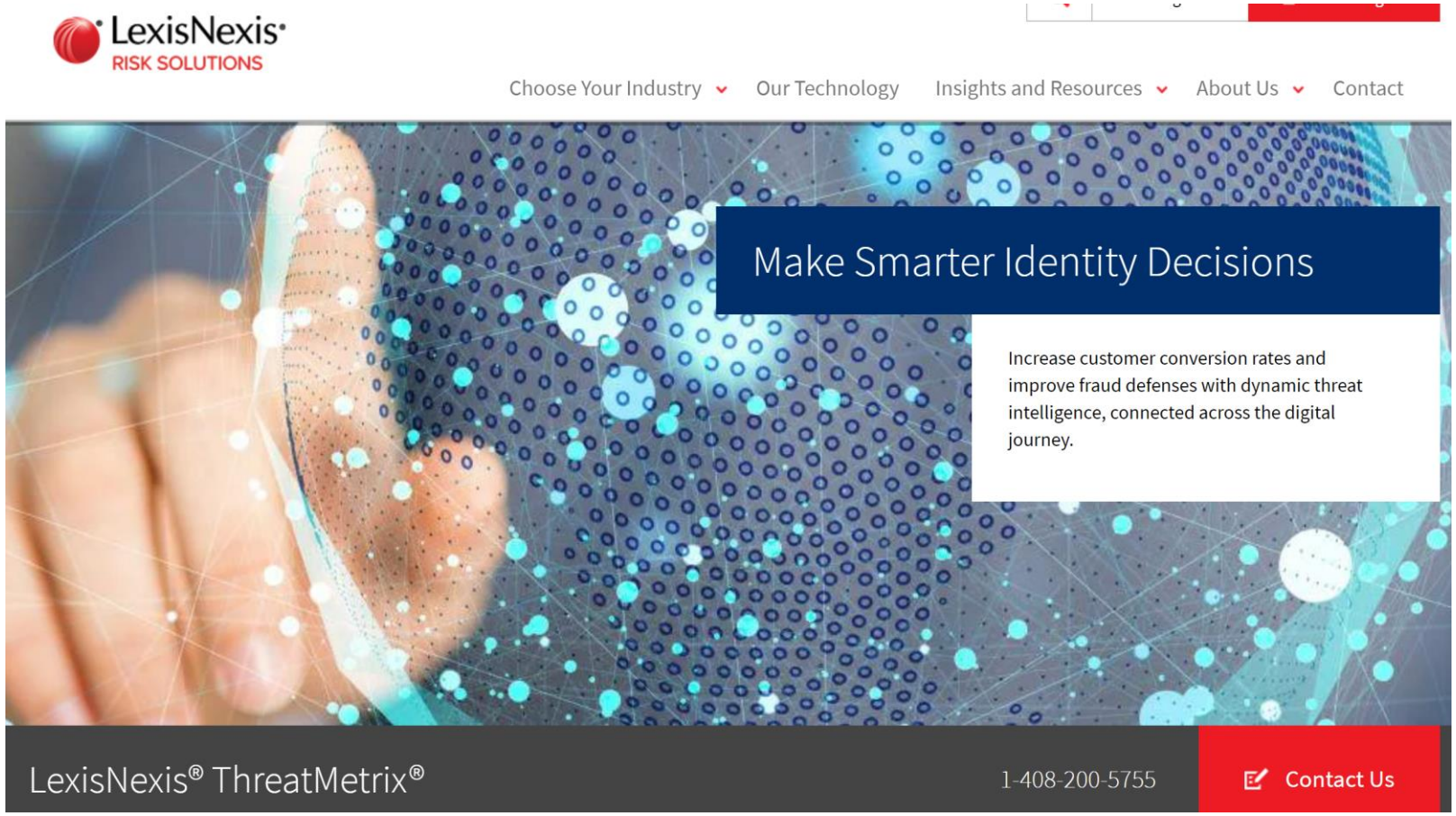
リンケージスコア、異常スコア、および時間情報に基づく時間ベースの減衰の重み付けに基づいて、ユーザの脅威スコアの集計を求める。時間が古くなるほど重みを減衰させる

決定された総脅威スコアが閾値スコアより大きい場合、アクセスをブロックする

ThreatMETRIX社　オーストラリア本社　2005年設立

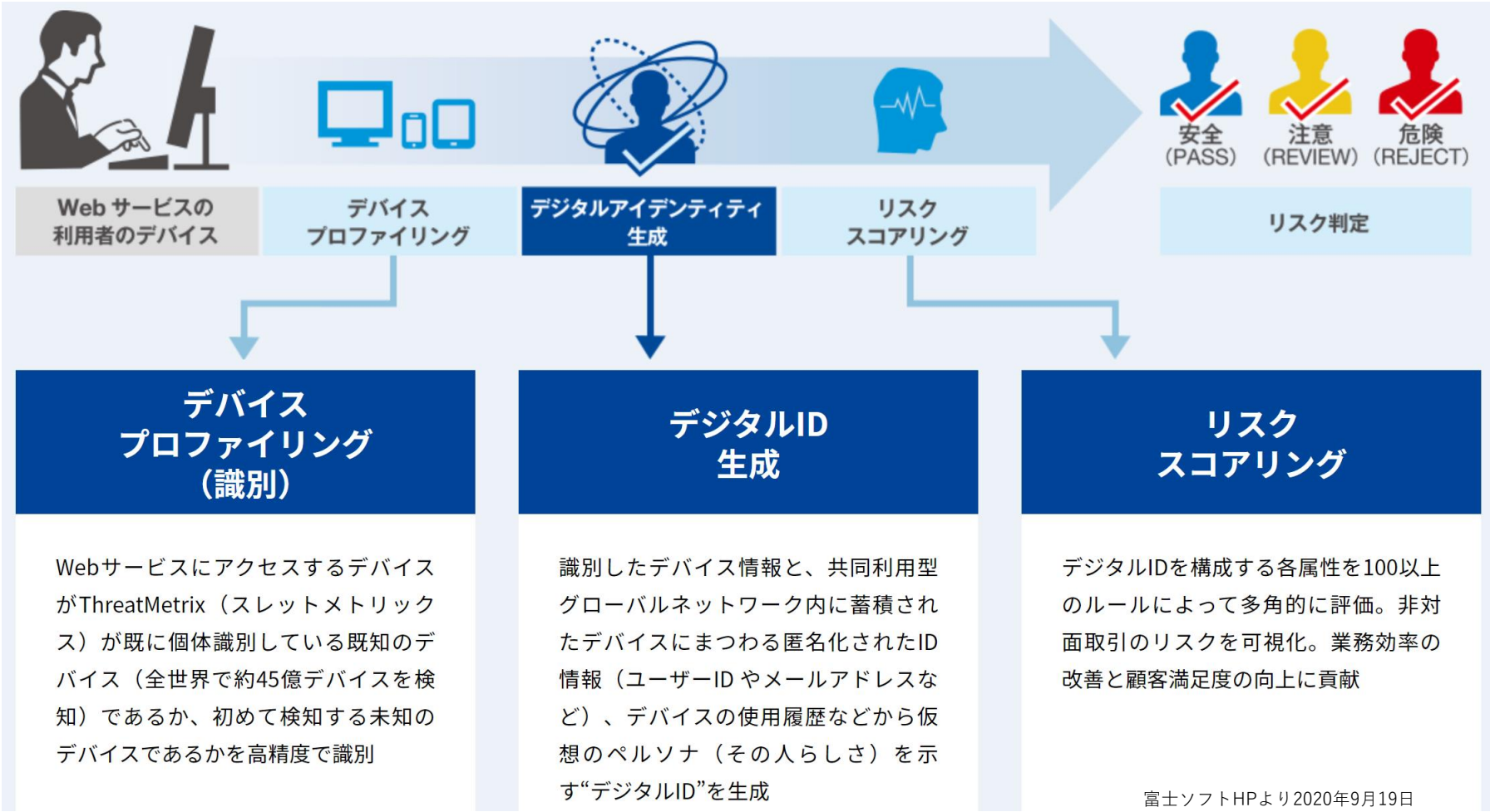
全世界で5000社が導入

日本では富士ソフトがサービス提供



ThreatMetrix紹介HPより2020年9月19日
https://risk.lexisnexis.com/products/threatmetrix

45億のデバイス情報
約300要素のデバイス情報を収集・蓄積。既知のデバイスは付与済みのデバイスIDで認識し、
未知のデバイスには新たなデバイスIDを付与。
年240億のトランザクション監視
ThreatMetrix（スレットメトリック）を利用する世界で5,000社、年間約240億トランザクションの取引を解析する

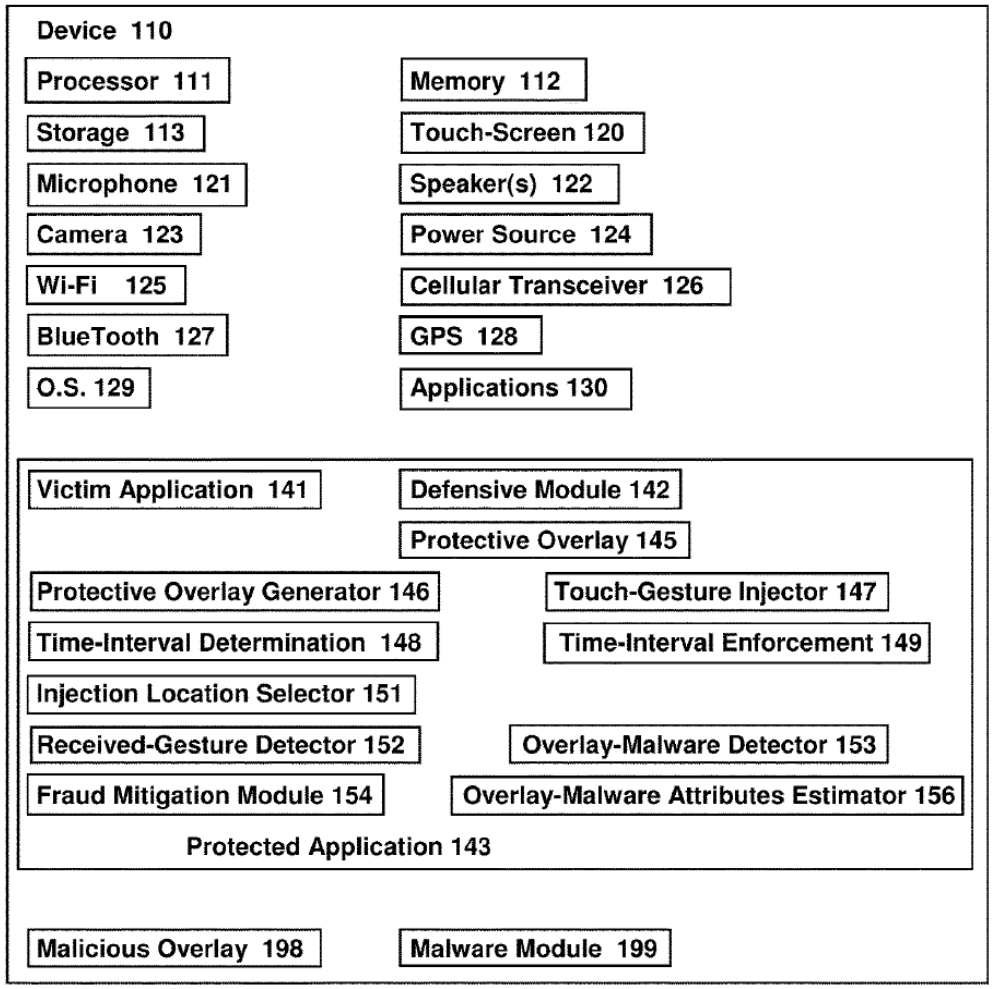


富士ソフトHPより2020年9月19日
https://www.fsi.co.jp/tmx/

02705

【オーバーレイマルウェアを検出するデバイス、システム、および方法】

BioCatch
出願日　2017年7月20日
登録日　2019年8月27日
登録番号 US10397262



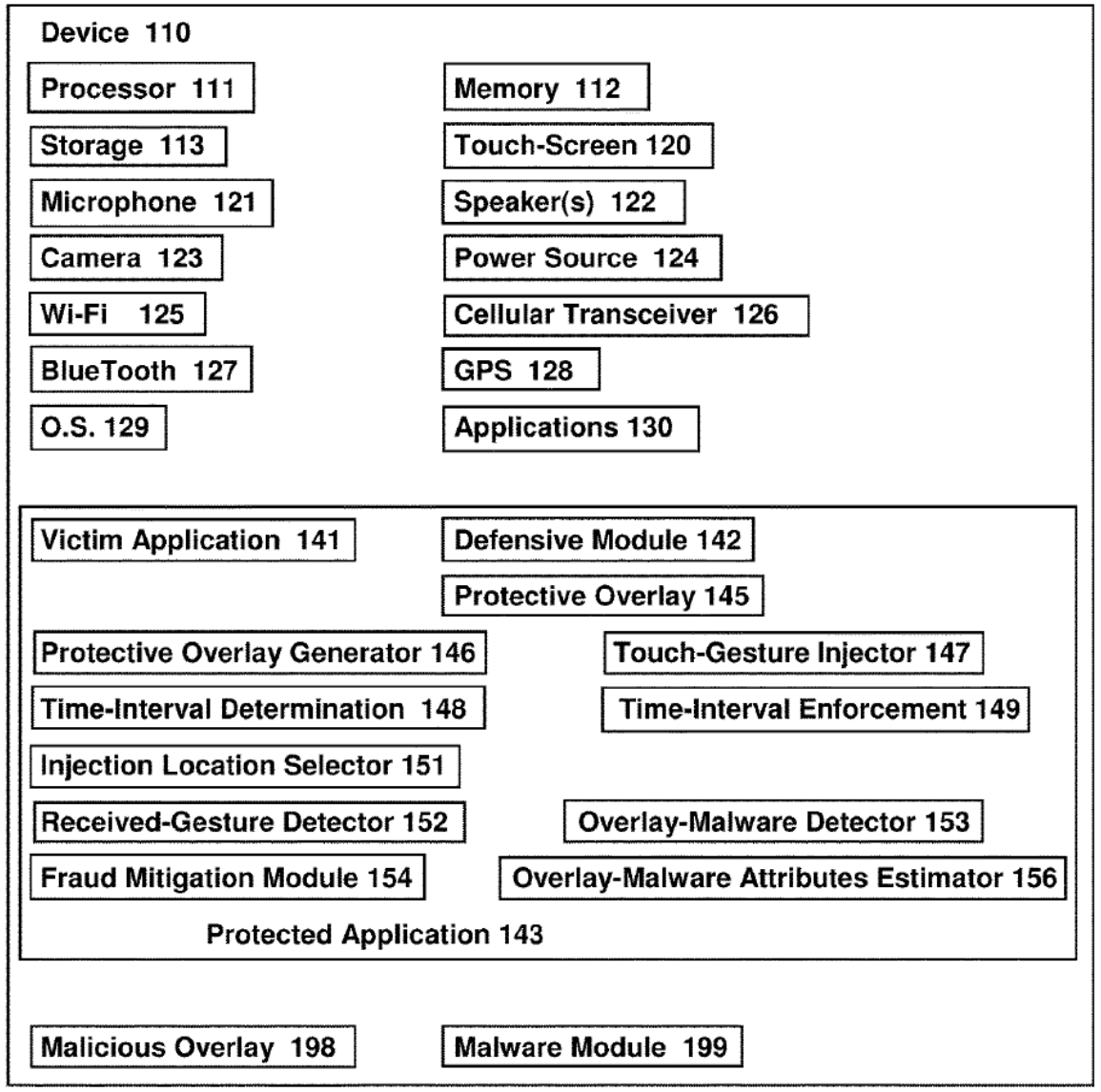
スマホ、タブレットでの金融取引が増加している。
Androidオペレーティングシステム（OS）を使用すると、開発者は、Always-On-Top要素を使用できる

画面の最上層にオーバレイマルウェアが仕込まれ、他のアプリケーションがマスクされ、または、非表示となる

CitiBankのアプリを起動すると、その上に、そっくりの偽のページがオーバーレイされる

偽のページにてログインID,パスワードを入力させ、偽のサイトにID、パスワードを送信させる

偽のページはログインに失敗しましたと表示しID、パスワードを不正に取得する

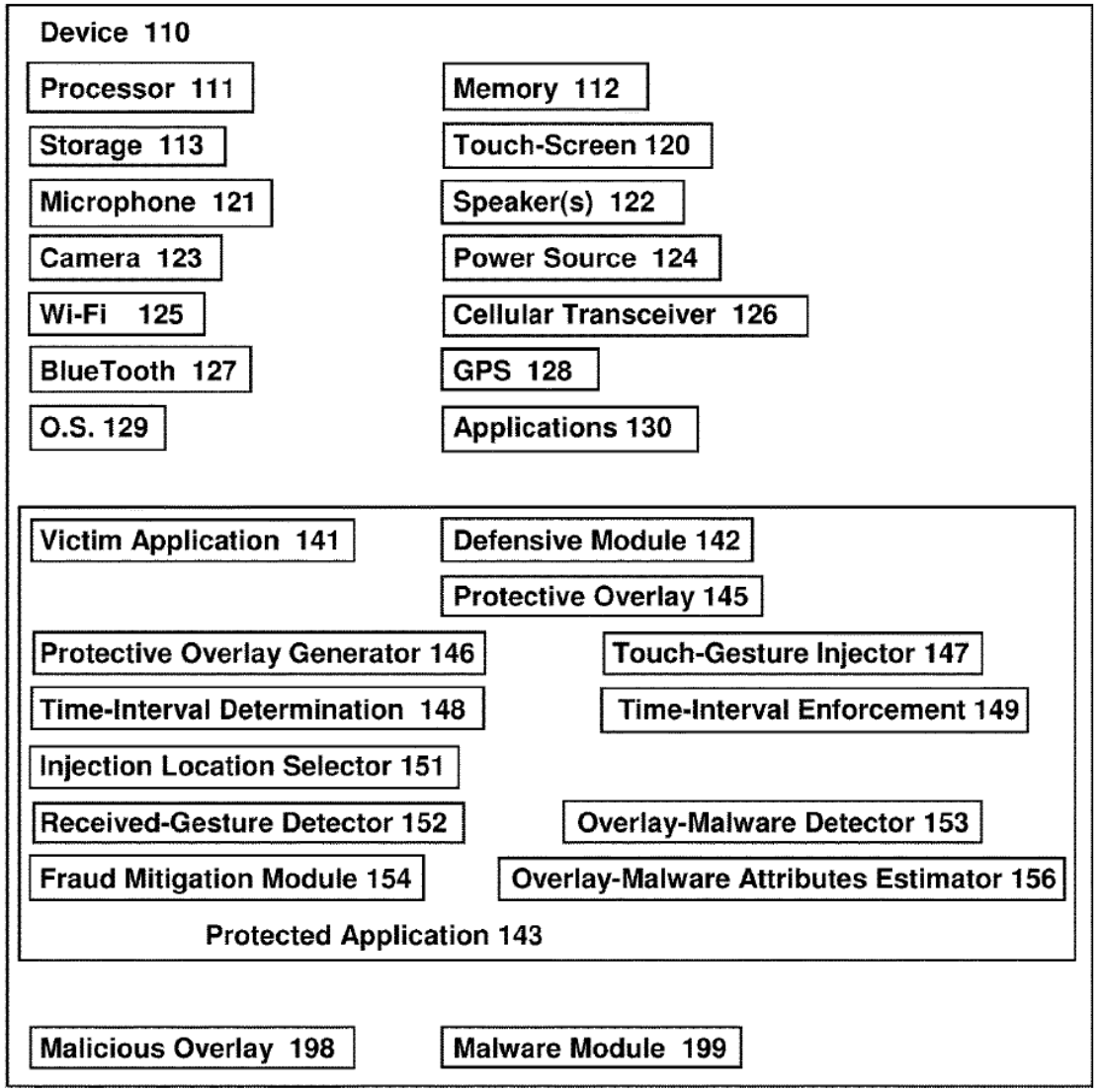


人間のユーザーには見えない保護用の常時最上層を生成する

タッチスクリーンの画面上の所定位置で人間以外のタッチイベントを自動的に注入する

数ミリ秒以内に、非人間タッチイベントが保護用の常時最上位層で実際に受信されたか否かを検出する

注入してから数ミリ秒以内に、人間以外のタッチイベントが保護用の常時最上位層で受信されなかった場合、オーバーレイマルウェアモジュールが電子デバイス上でアクティブであると判断する



Ｋミリ秒毎に所定座標をタップする。
　Ｋ＝100～500ms、疑似ランダムでもよい

注入後Ｍミリ秒以内で、システムのわずかな処理遅延を検出する。ここで、Ｍはたとえば、1ms,5msまたは10ms
K>M
（10%以下の遅延を検出）

タップ後、すぐに(１ｍｓ以内)タップ操作を受信しない場合、オーバレイマルウェアに乗っ取られていると判断する
最上位に配置したはずの透明最上位層よりも更に上にオーバレイマルウェアが配置されている

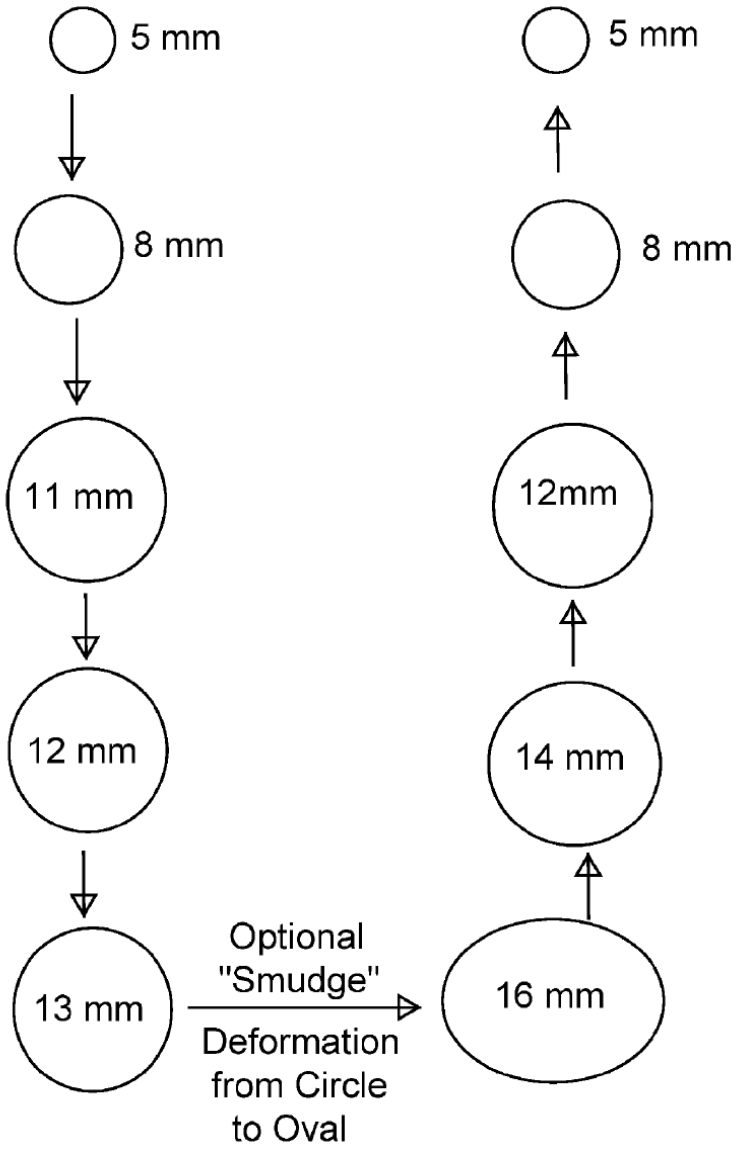
この場合、ユーザに乗っ取られていることを警告する

処理遅延を適切に検出できている場合、アクティブな攻撃は存在しないと判断

02706

【タッチ面にかかる力を推定する システム、デバイス、および方法】

BioCatch
出願日　2016年9月30日
登録日　2019年2月5日
登録番号 US10198122



タッチパネルへのタップ時のSmudge（汚れ）の時系列変化を分析する

タップ面積の時系列変化と、その時の加速度センサのデータを取得する　（大きさと強さがわかる、人により特徴がある）

タップ操作をモデル化することができる

認証時に、なりすましユーザがタップ操作した場合、元のユーザのタップ操作と異なることを検出できる

BioCatch社　2011年にイスラエルにて設立

行動バイオメトリクスを用いた認証

ニューヨーク、ロンドンに支社

月40億のトランザクションを監視

BIOCATCH社HPより2020年10月3日
https://www.biocatch.com/

2020年5月29日　みずほ銀行、SCSK株式会社、BioCatch社が、行動的生体AI認証技術を用いた金融詐欺の防止に関する共同実証実験を開始

みずほ銀行のバンキングアプリケーションを模した、疑似アプリケーションにBioCatch社のテクノロジーを実装し、複数のテスターで送金シナリオを実行することで、なりすまし対策およびその他金融詐欺の対策ソリューションとしての有効性を分析、検証

SCSK株式会社HP2020年10月3日プレスリリースより
https://www.scsk.jp/news/2020/press/product/20200529.html