

インダストリアルIoT（IIoT）とサイバーセキュリティ 注目スタートアップの特許

講師  河野特許事務所 所長 弁理士 河野英仁

企画・運営 日本IT特許組合

現在、IoT機器の活用は、多くの新しいサービスや重要インフラなどの監視設備として、広く活用されている。しかしながら、簡易なIoT機器へのセキュリティ機能の未配備やIoT利用者におけるセキュリティ意識が低いことが原因で、IoTがサイバー攻撃に加担していることが多く確認されている。

本講座ではインダストリアルIoT (IIoT) 分野のサイバーセキュリティとして注目されるスタートアップ企業の特許をとり上げ、解説する。

【産業用制御システムへのサイバー攻撃を軽減する方法】 Cyberx Israel

【ビッグデータマシンを訓練して防御する方法とシステム】 PatternEx

【グローバルな自動車安全システム】 Argus Cyber Security

【大量のVPN接続をなくすためのゲートウェイデバイス】 Blue Cedar Networks

【モバイルデバイスでのアプリケーションの使用に関する地理的制限】 Blue Cedar Networks

【グループ認証のシステムと方法】 iovation

【アクティブなクエリを使用した産業用制御ネットワークでの設定ミスと敵対的な攻撃の検出】 indegy

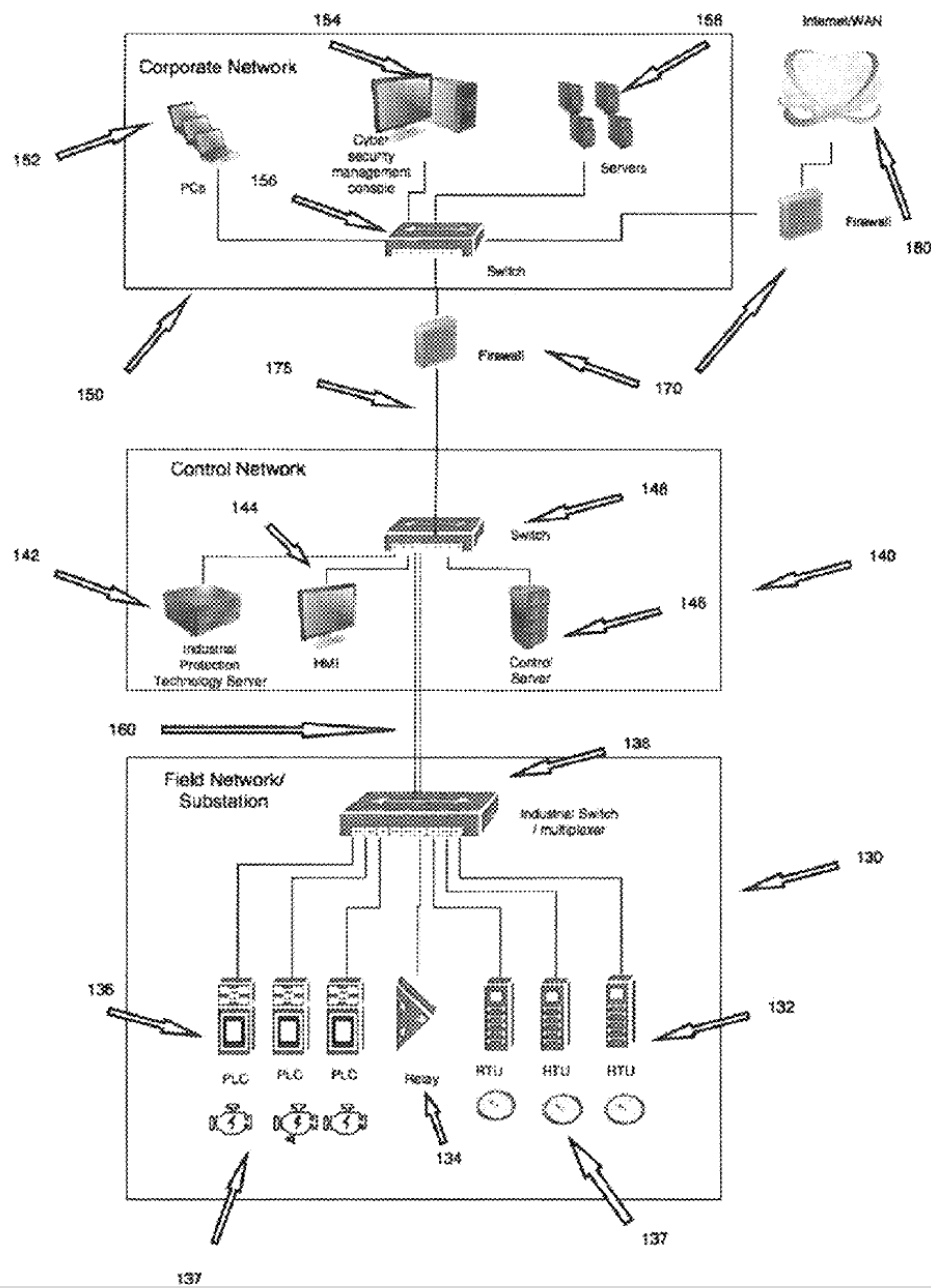
【産業用制御システムへのサイバー攻撃を軽減する方法】

Cyberx Israel

出願日 2015年8月20日

登録日 2018年7月3日

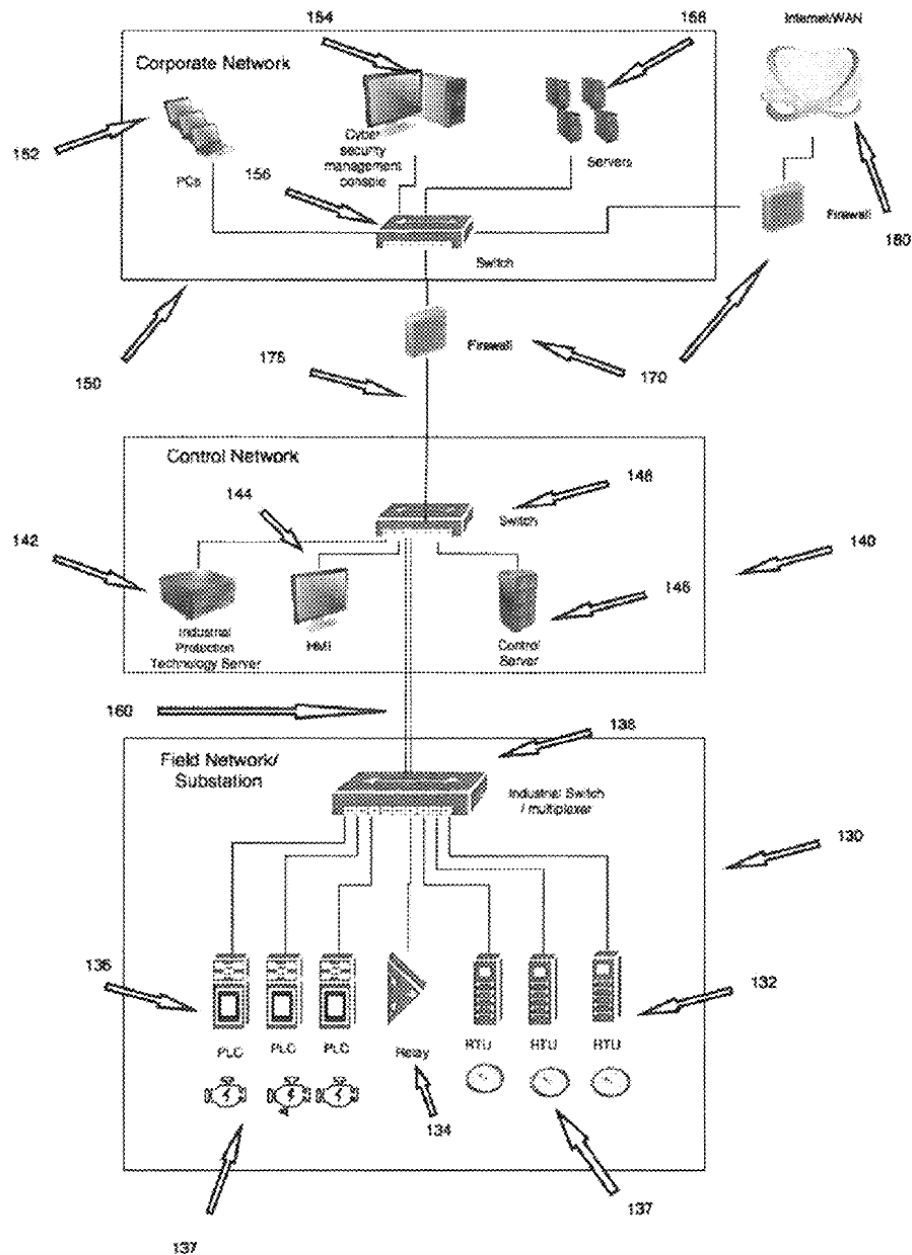
登録番号 US10015188



産業用機器のプログラマブルロジックコントローラ（PLC）の
 パケットデータを解析することによりサイバー攻撃を検出するア
 イデア

産業用制御システムに対する悪意のある攻撃が懸念されている
 特に、プログラマブルロジックコントローラ（PLC）になりす
 まし、産業用制御システムに損害を与えるトラフィックを送信す
 るウイルスが増加している

学習モードと保護モードに大別される



学習モードでは、パケットデータに基づき第1状態(正常状態)と、第2状態(異常状態)とをクラスタリングする

保護モードでは、学習済みモデルを用いてPLCの状態を推定する

第1状態から第2状態へ遷移する遷移確率を算出する

遷移確率を随時算出し、遷移確率が閾値を超える場合、防護措置をとる

防護措置：アラート、ノードの無効化、パケットのブロック

再度学習モードでの学習が行われる

CyberX社 産業用制御システムのセキュリティに特化した企業
米国イリノイ州本社
機械学習を用いた分析
米国政府機関、エネルギー、化学プラント等350社以上に導入



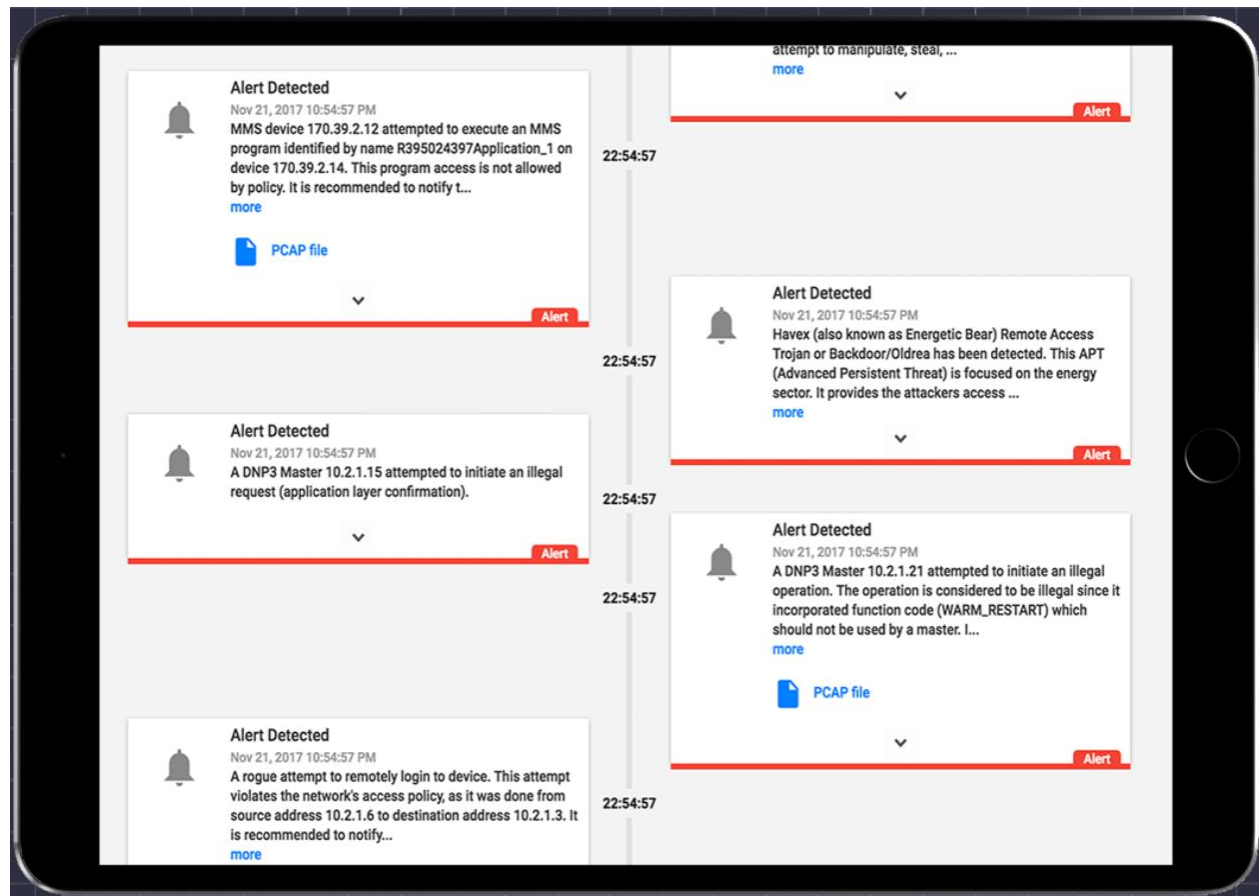
CYBERX BATTLE-TESTED INDUSTRIAL CYBERSECURITY [REQUEST A DEMO](#)

PROTECT YOUR PEOPLE, PRODUCTION & PROFITS

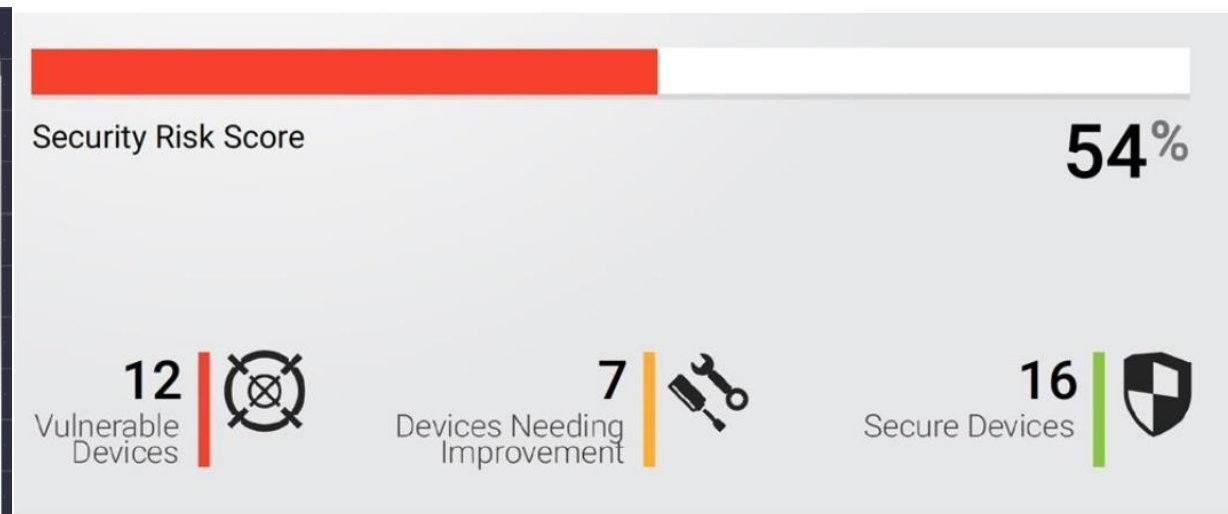
CyberX delivers the only IoT/ICS cybersecurity platform built by blue-team experts with a track record defending critical national infrastructure — and the only platform with patented M2M-aware threat analytics and machine learning.

CyberX社HP2019年8月11日 <https://cyberx-labs.com/>

Cyberx Israel特許 産業用ネットワークのサイバーセキュリティ



アラート表示



CyberX provides detailed information about each device including device type, manufacturer, open ports, and known vulnerabilities (CVEs) ranked by severity.

セキュリティリスクスコア表示

【ビッグデータマシンを訓練して防御する方法とシステム】

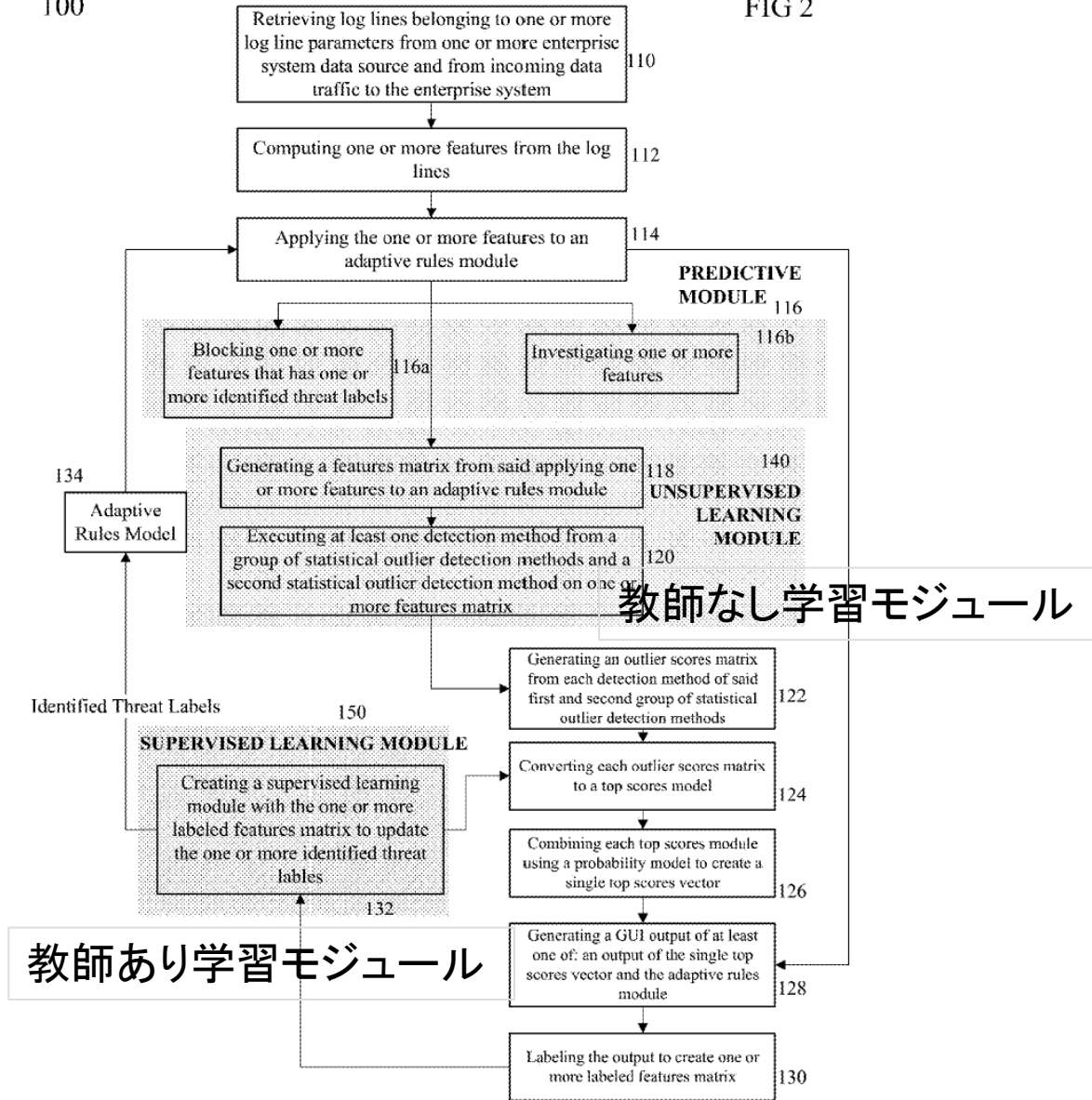
PatternEx

出願日 2016年12月16日

登録日 2018年2月27日

登録番号 US9904893

FIG 2



教師なし学習モジュールと、セキュリティアナリストによる教師あり学習モジュールを用いてビッグデータ中の脅威を検出するアイデア

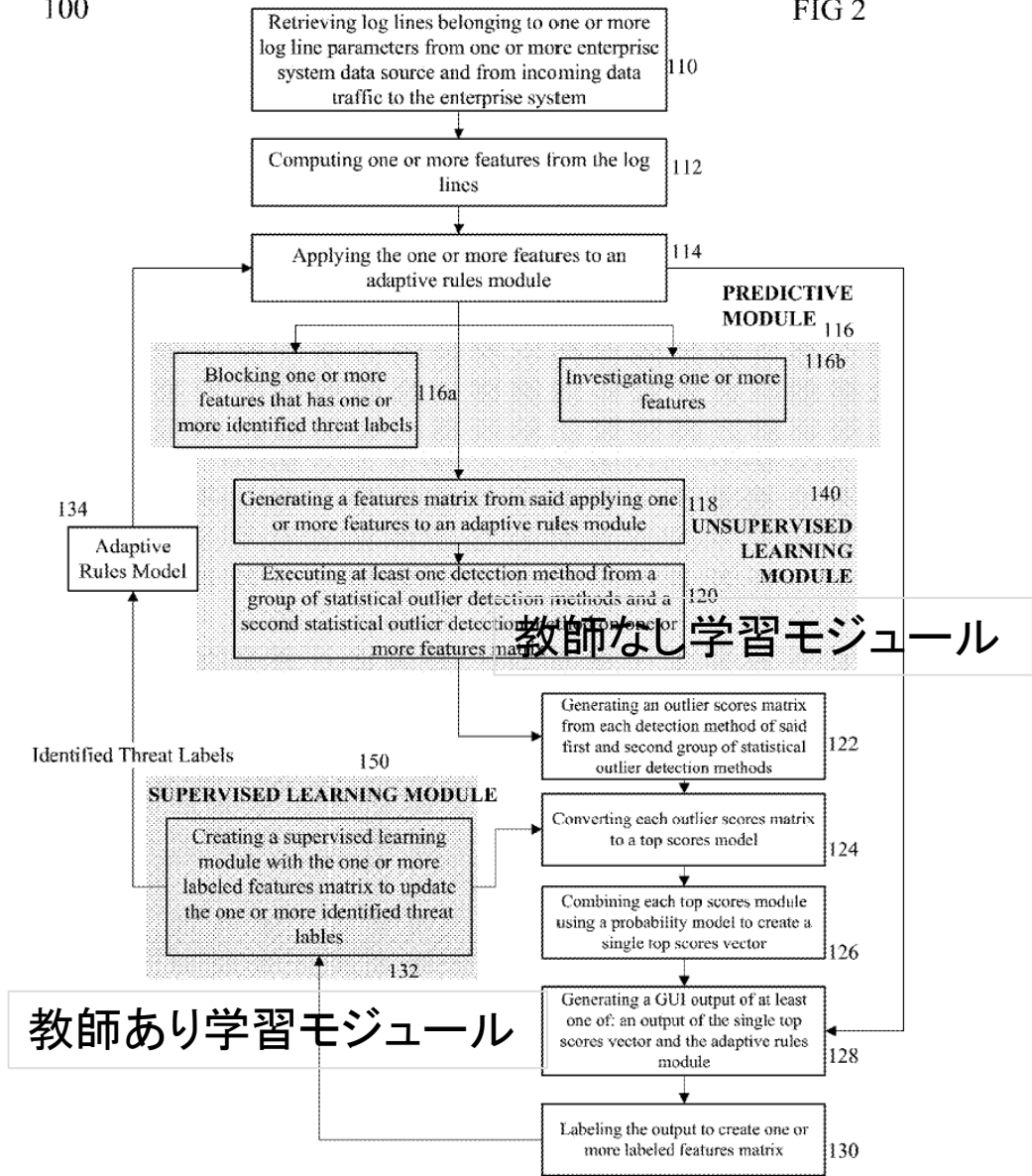
電子商取引システムはセキュリティの脅威にさらされている

教師なし学習モジュール

教師なしの機械学習ソリューションは、異常パターンの検出につながるが、誤検知も多い

教師あり学習モジュール

FIG 2



ログデータから特徴マトリックスを生成する

複数の異なる方法により、統計的外れ値の検出を行う（レアなケースを検出する）

教師なし学習モジュール

統計的外れ値検出方法の第1および第2グループの各検出方法から外れ値スコアマトリックスを生成し、各外れ値スコアマトリックスからトップスコアベクトルを生成する

トップスコアベクトルの出力と適応モデルのGUIを出力し、セキュリティアナリストがラベル付けする

適応モデルに対し教師あり学習により学習させる

適応モデルの性能が学習により徐々に向上する。適応モデルにより、脅威の検出・ブロックを行う

「アクティブ・コンテクスチュアル・モデリング」システム：
セキュリティアナリストがリスク検出とコンピュータ学習を監督するシステム



[SOLUTIONS](#) [PRODUCT](#) [THRETEX LABS](#) [RESOURCES](#) [ABOUT US](#)

[CUSTOMER SUPPORT](#) [CONTACT US](#)

[DEMO](#)

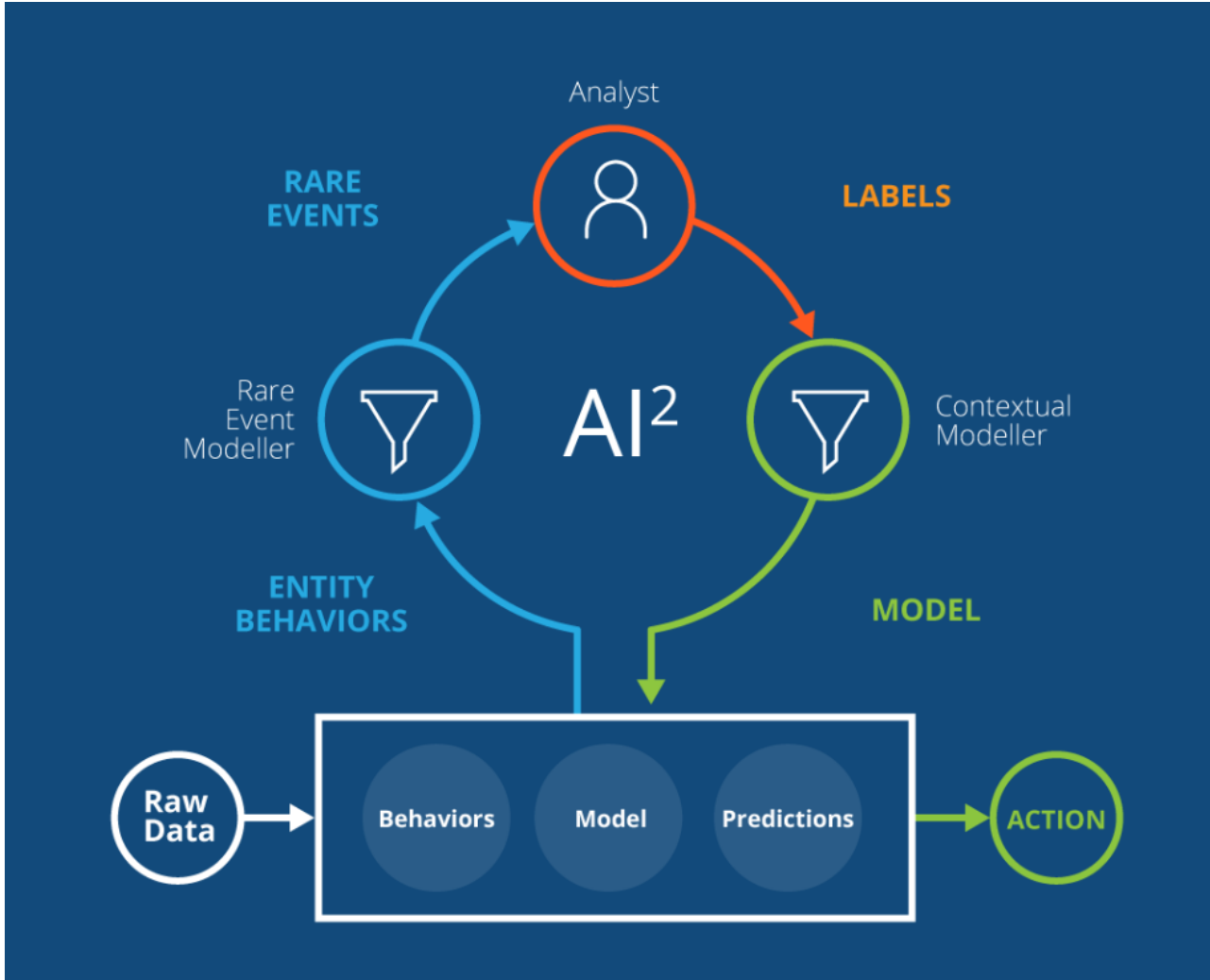
[THRETEX LABS](#)

Transform SecOps with Virtual Analysts

5x Fewer False Positives
10x Better Detection
20x Faster Investigations

Live Webinar: Learn how Proficio architected the next generation of a security analytics SOC with PatternEx Virtual Analyst Platform AI technology.

[RESERVE YOUR SEAT](#)



生データが取り込まれ、行動に変換される

行動からレアイベントが発見され、アナリストがレビューする

レビュー後、アナリストによって各イベントに適切なラベルが付与される

システムはこれらのラベルから学習し、脅威の検出効率を自動的に改善する

【グローバルな自動車安全システム】

Argus Cyber Security
出願日 2015年1月6日
登録日 2017年4月11日
登録番号 US9616828

サイバー攻撃に対するセキュリティを車載通信システムに搭載した技術

センサ、ECU、アクチュエータ等、車載機器が増加し続けており、サイバー攻撃の対象になりやすくなっている

グローバル自動車安全システム（G A S S）20は、サイバーハブ22と、車両にインストールされるサイバーウォッチマン40とを備え

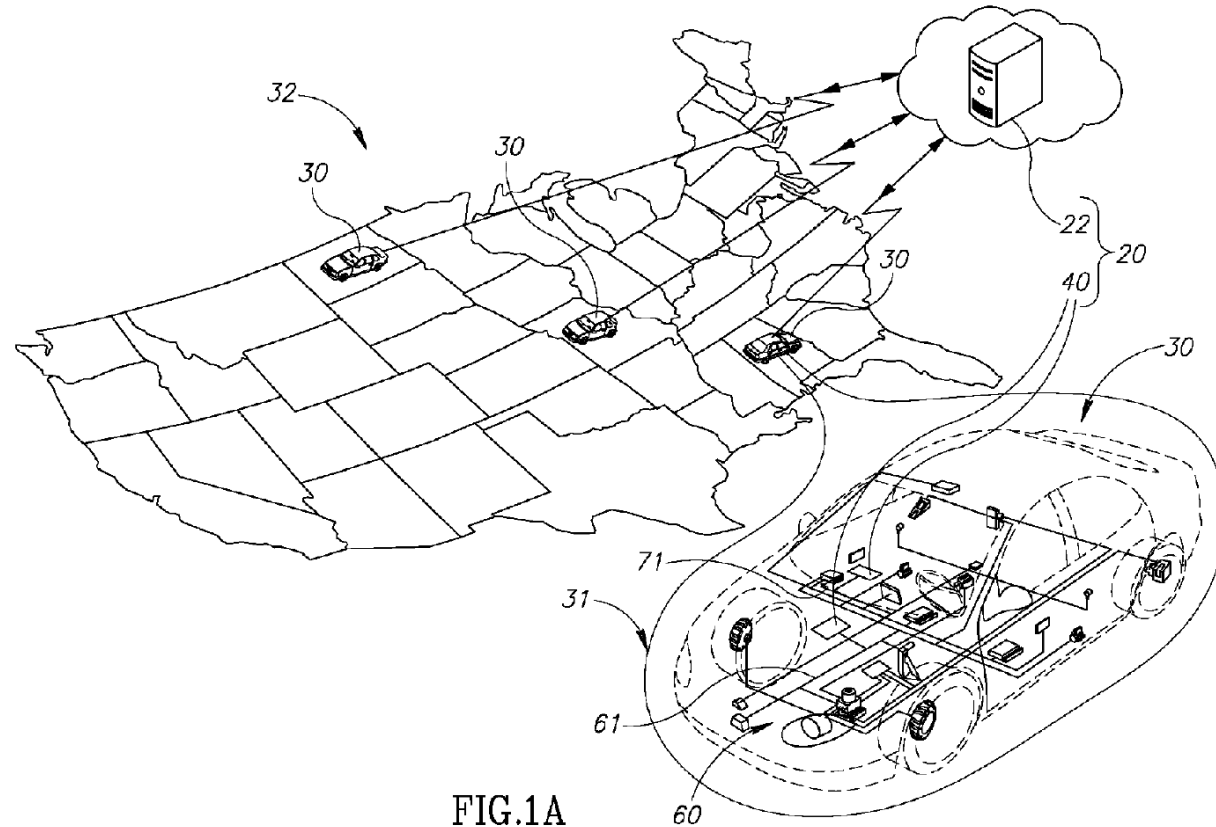


FIG.1A

サイバーウォッチマン40A-40Dは、車両の車載通信ネットワークの通信トラフィックを監視し、ネットワークまたは車両の通常の動作の妨害する通信トラフィックの異常を識別する

サイバーウォッチマンは、異常を識別した場合、異常を報告、軽減、制御するための多様なアクションをとる。ウォッチマン40Bのプロセッサは、高速バス61の上に任意選択で「ポイズンビット」と呼ばれるドミナントビットを送信させ、高速バス61で伝搬する望ましくないメッセージを壊す

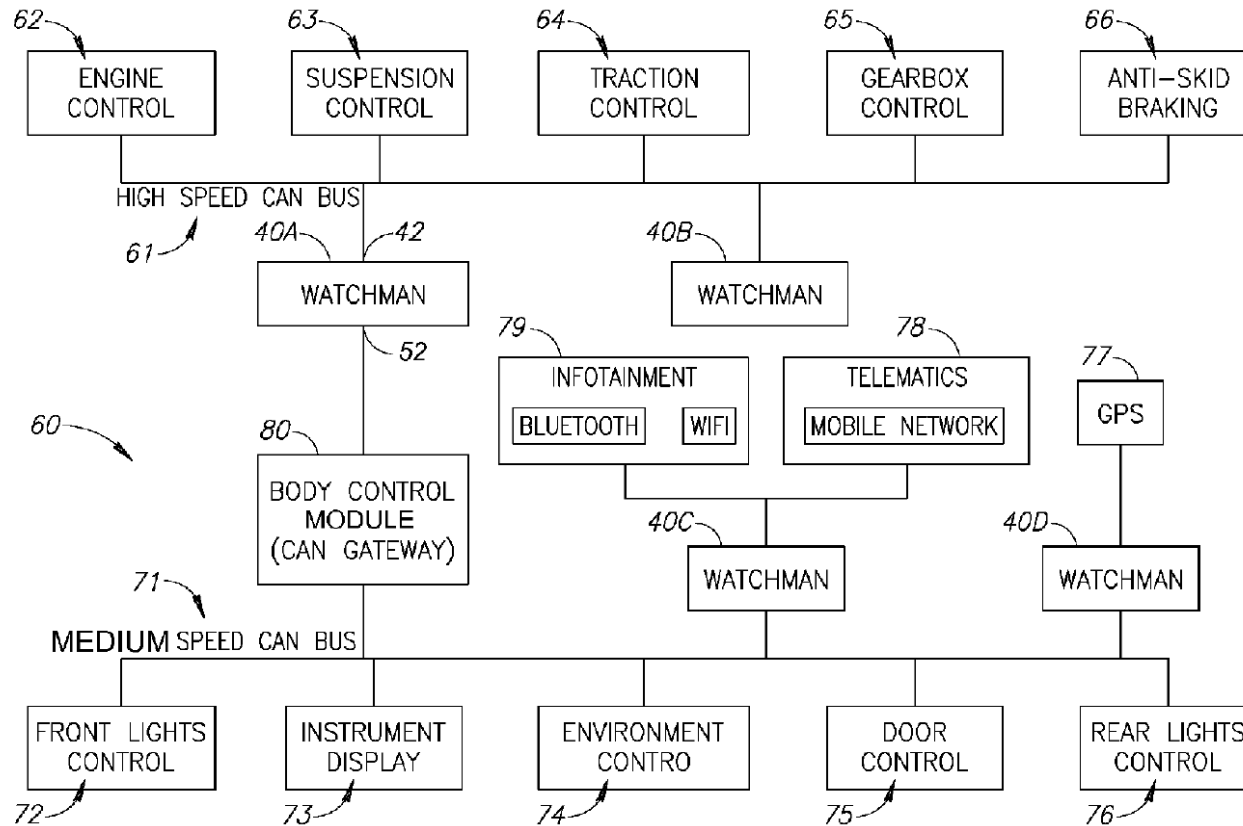


FIG.1B

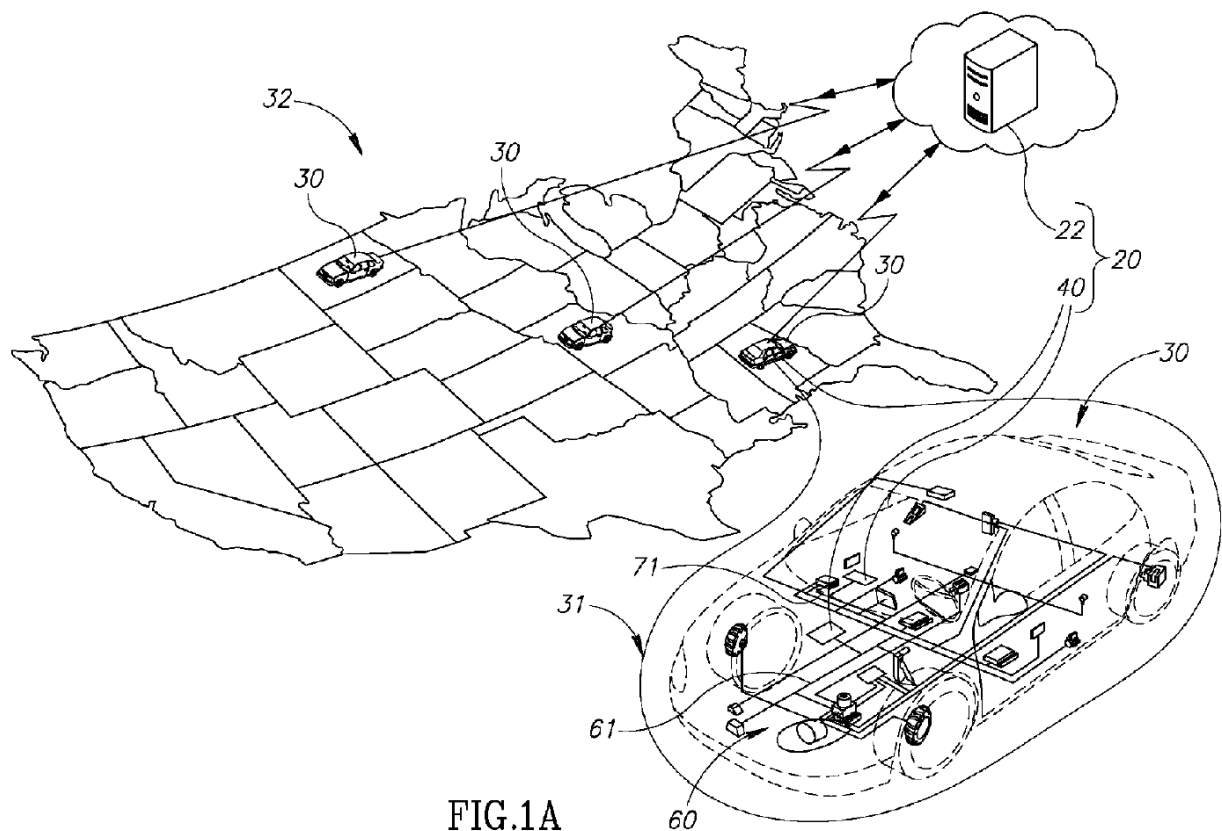


FIG.1A

サイバーウォッチマン40は、ウォッチマンデータと呼ばれるデータをサイバーハブ22に送信する。サイバーハブ22は加入者車両からのウォッチマンデータを処理する。サイバーハブ22は複数の加入者車両からのウォッチマンデータを処理して、車両または車両の集団が差し迫ったサイバー攻撃の脅威にさらされている可能性があるのか、サイバー攻撃を受けているのか、またはサイバー攻撃に対する脆弱性を有しているのかを判断する。

サイバーハブ20は、CANデータのホワイトリスト、ブラックリスト、グレーリストを生成する。ウォッチマン40はリストに応じて機能を制限する。

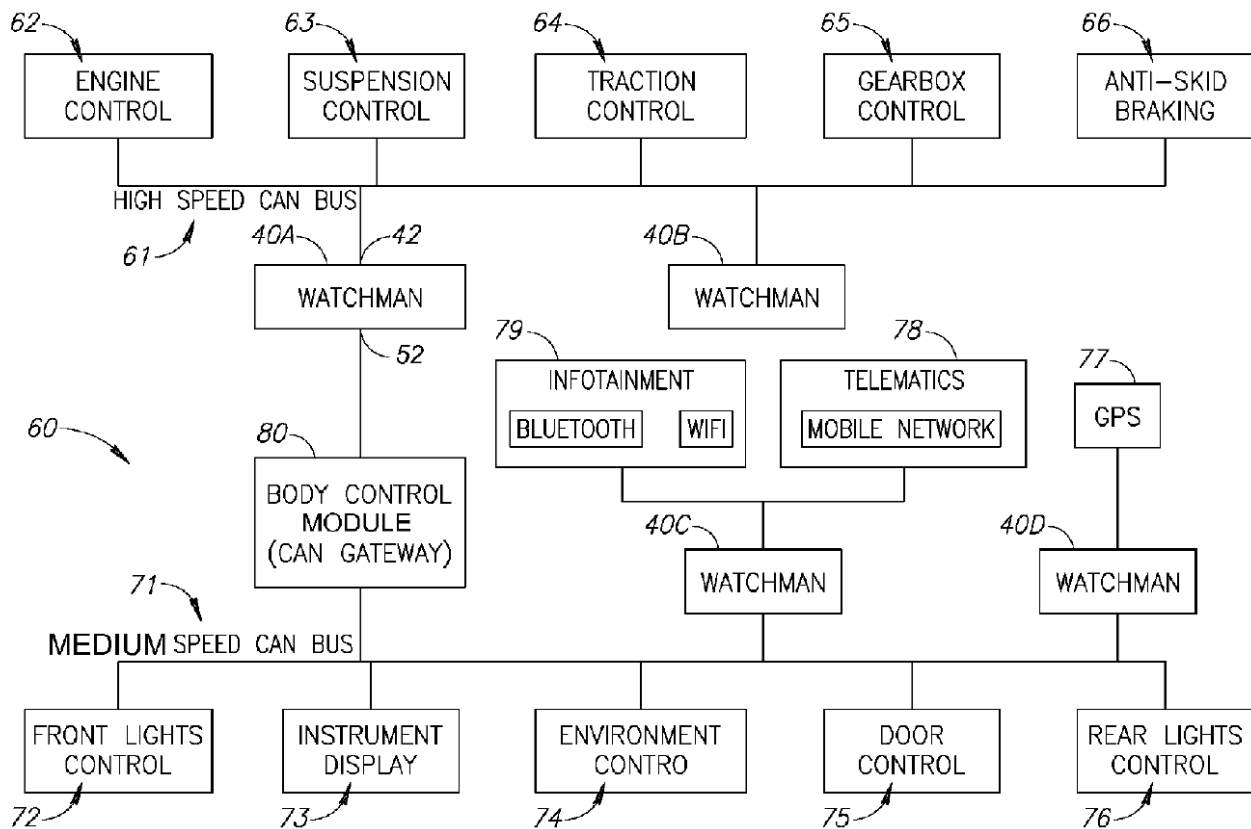


FIG.1B

ファームウェアを更新（例えばエンジンの制御プログラムを更新）する場合、テレマティックシステム78から更新データをダウンロードするウォッチマン40は適切に暗号化されているか否かを判断する

適切に暗号化されている場合、更新データを復号し、その後、車両のコンテキストデータ（例えば車速）にアクセスする

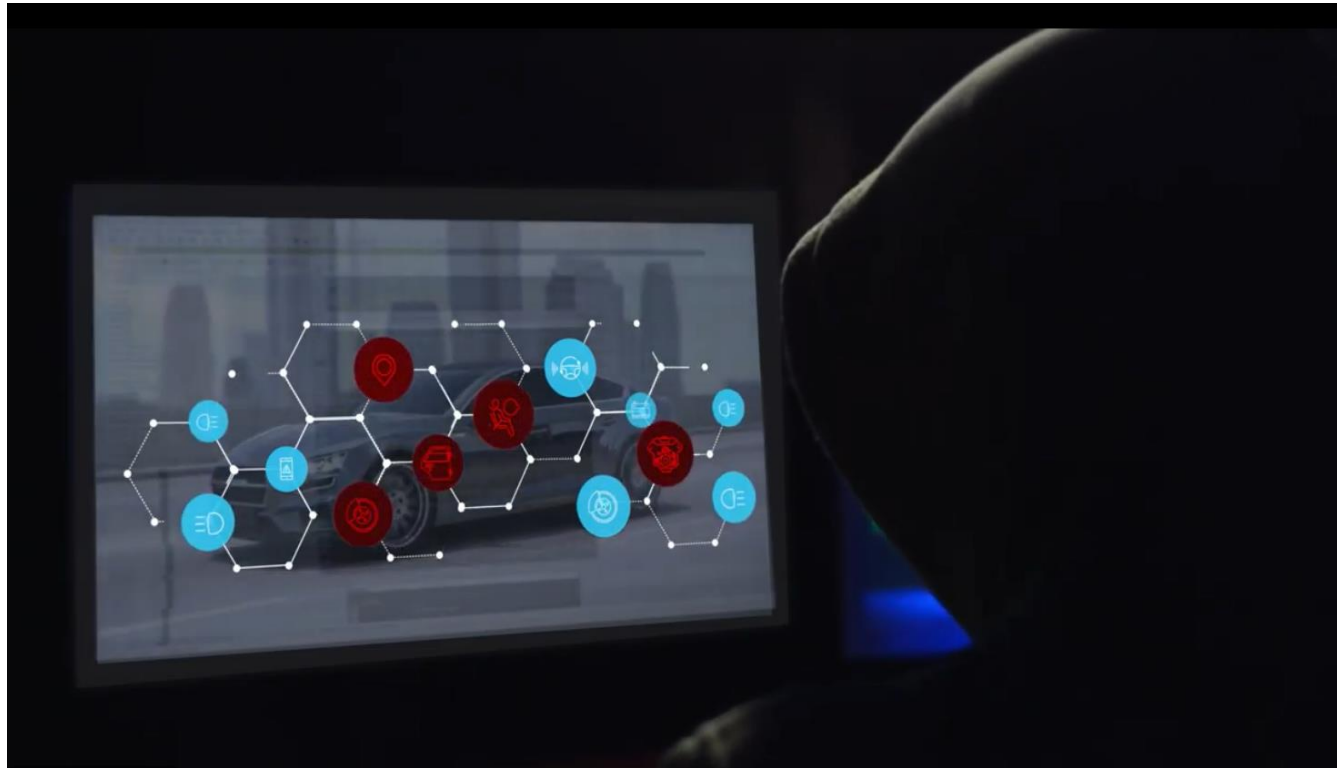
車速が10km/h以上の場合、更新しない

車速が10km/h以下となった場合に更新する

Argus Cyber Security 2013年設立

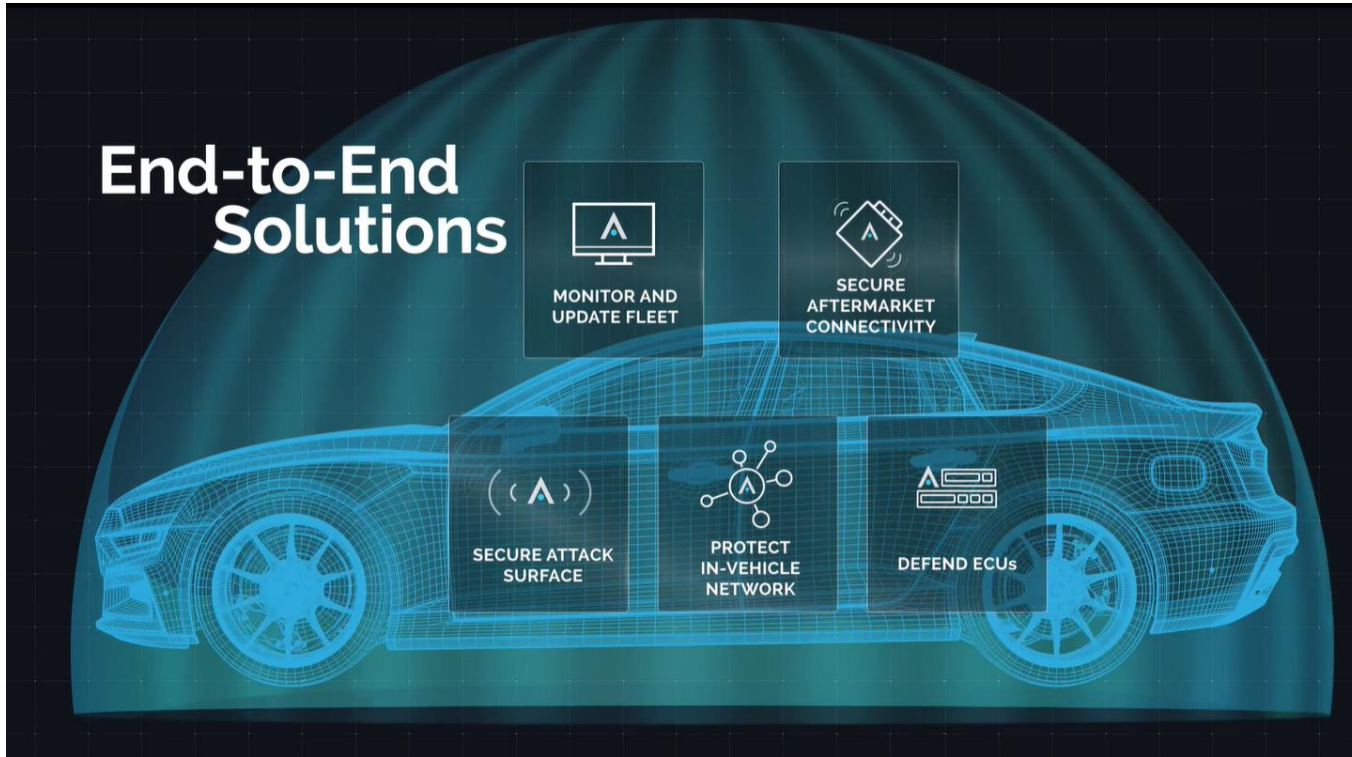
イスラエルの自動車向けサイバーセキュリティ会社

2017年にコンチネンタルが買収



コネクテッドカーの増加によりハッキングリスクが日々高まっている

自動車に対するサイバー攻撃防止



数多くの特許技術によりセキュリティ対策を行っている

世界中のハッキング状況をリアルタイムで収集・対策



その他の動画

遠隔での監視



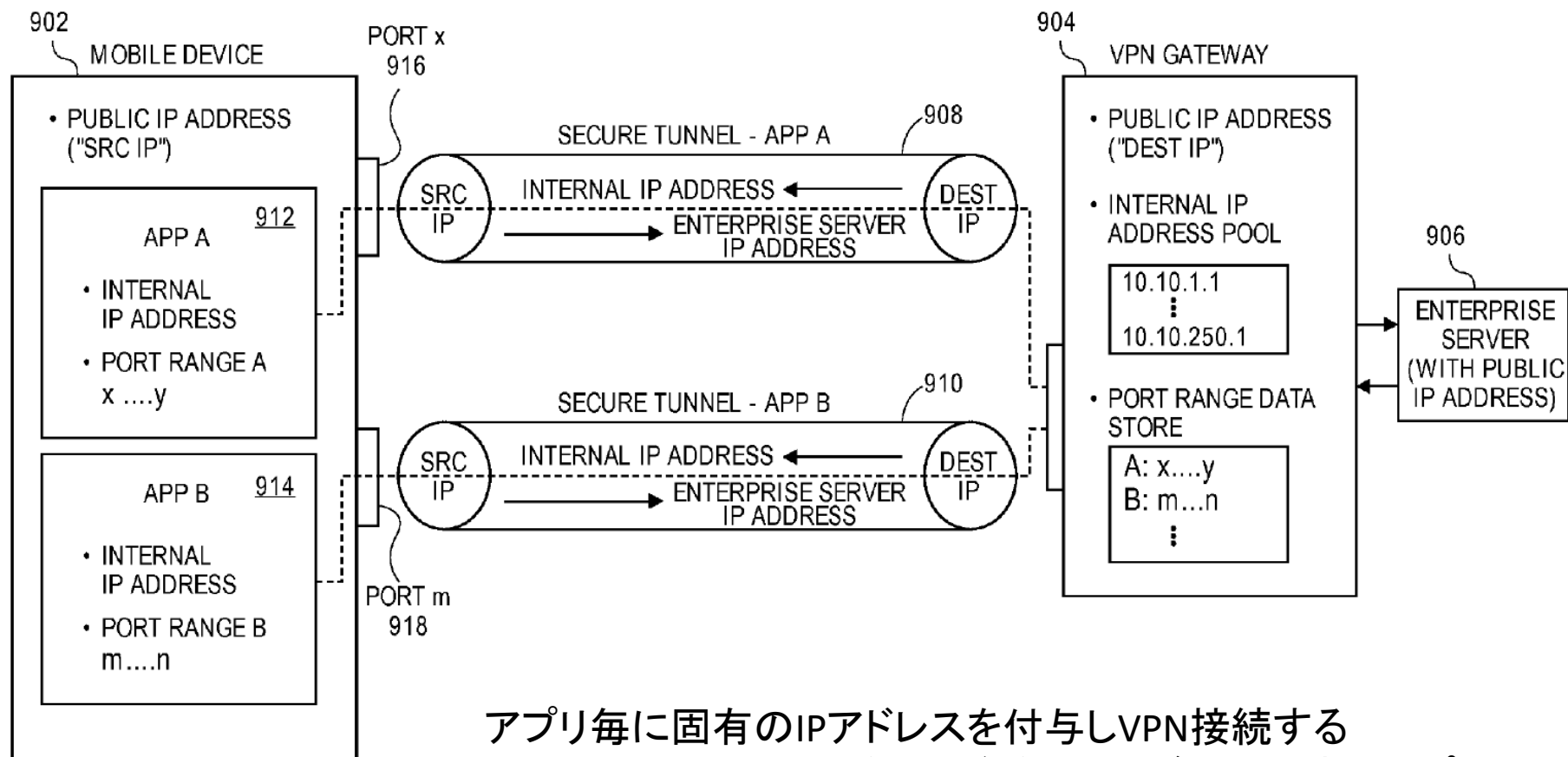
【大量のVPN接続をなくすためのゲートウェイデバイス】

Blue Cedar Networks
出願日 2014年8月14日
登録日 2015年3月31日
登録番号 US8997208

モバイルデバイスに対するセキュリティ維持が重要

会社が付与するモバイルデバイスは会社へのアクセスのために使用するアプリの他、プライベート使用のアプリも存在する
プライベートでの使用時に、セキュリティ上の問題が発生する事が多い

従来、モバイルデバイスを、VPNトンネルを通じてVPNゲートウェイに接続していた



アプリ毎に固有のIPアドレスを付与しVPN接続する
ただしこの場合、IPアドレスが増加しすぎるため連合アプリの概念を導入する

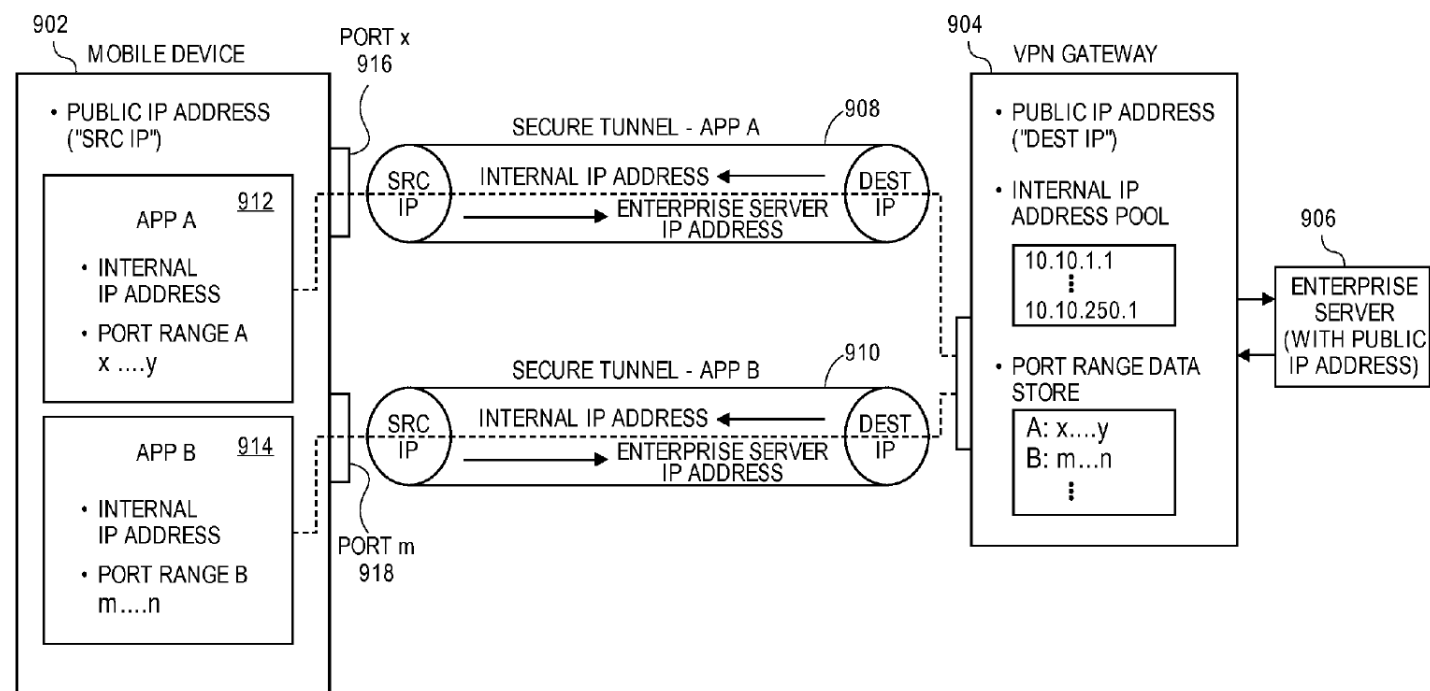
第1アプリにVPNゲートウェイから内部的に固有のIPアドレスを伝送する

VPNゲートウェイから第1アプリにアプリ連合クッキーを伝送する

アプリ連合クッキーを第2アプリと共有する。第2アプリに同一のIPアドレスを付与する

VPNゲートウェイは、第1アプリに第1ポート範囲を設定し、第2アプリに第2ポート範囲を設定し、VPNトンネルを通じて通信する

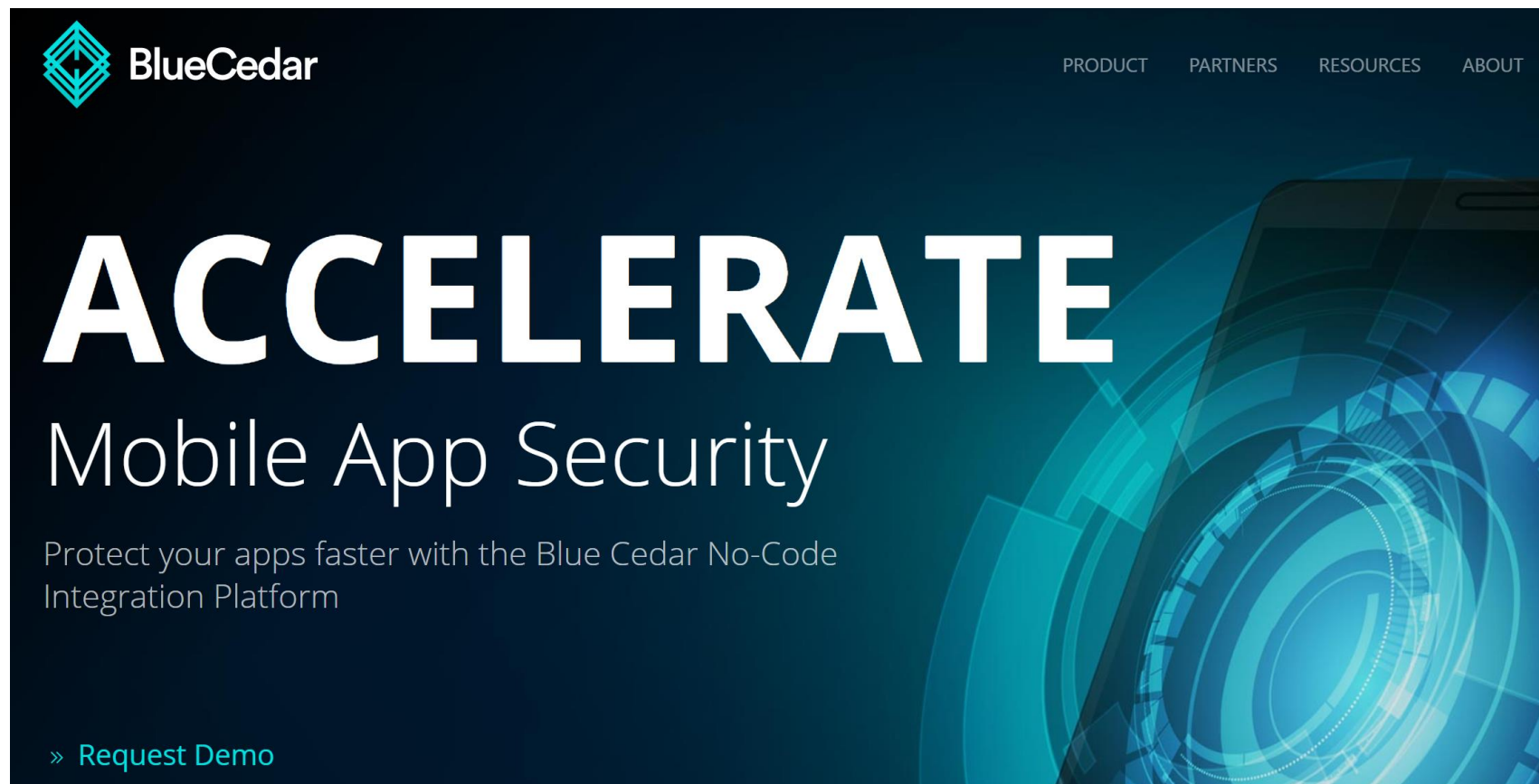
連合アプリには、固有のIPアドレスを割り当てず、共通のVPNを利用させる



Blue Cedar Networks 米国カリフォルニア州本社 2016年設立

モバイルアプリのセキュリティサービスを提供

Mocana社（2006年設立 産業用制御システムのIoTプラットフォームを提供）から分離した会社

The image shows a website banner for Blue Cedar. In the top left corner is the Blue Cedar logo, which consists of a stylized blue diamond shape made of lines, followed by the text 'BlueCedar'. In the top right corner, there are four navigation links: 'PRODUCT', 'PARTNERS', 'RESOURCES', and 'ABOUT'. The main text of the banner is 'ACCELERATE' in large, bold, white capital letters, followed by 'Mobile App Security' in a smaller white font. Below this, there is a subtitle: 'Protect your apps faster with the Blue Cedar No-Code Integration Platform'. At the bottom left of the banner, there is a call to action: '» Request Demo'. The background of the banner is dark blue with abstract, glowing blue circular patterns and a faint image of a smartphone on the right side.

BlueCedar

PRODUCT PARTNERS RESOURCES ABOUT

ACCELERATE

Mobile App Security

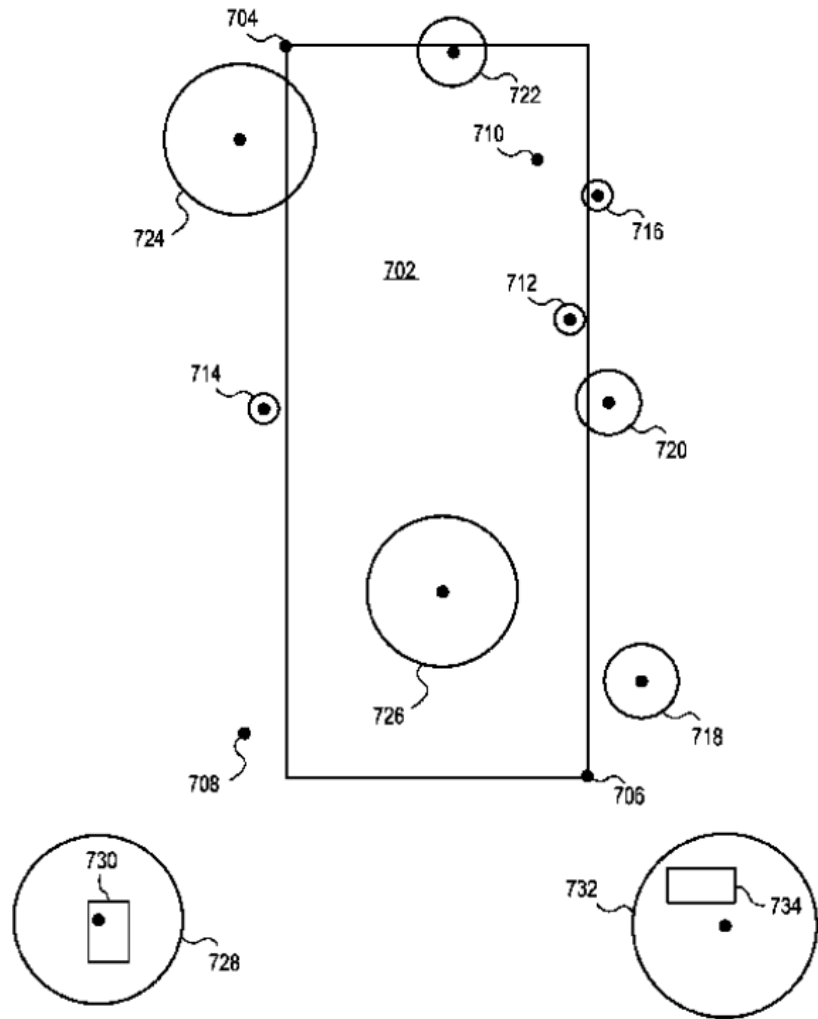
Protect your apps faster with the Blue Cedar No-Code Integration Platform

» [Request Demo](#)

Blue CedarHPより2019年8月26日
<https://www.bluecedar.com/>

【モバイルデバイスでのアプリケーションの 使用に関する地理的制限】

Blue Cedar Networks
出願日 2014年3月24日
登録日 2017年1月3日
登録番号 US9537869

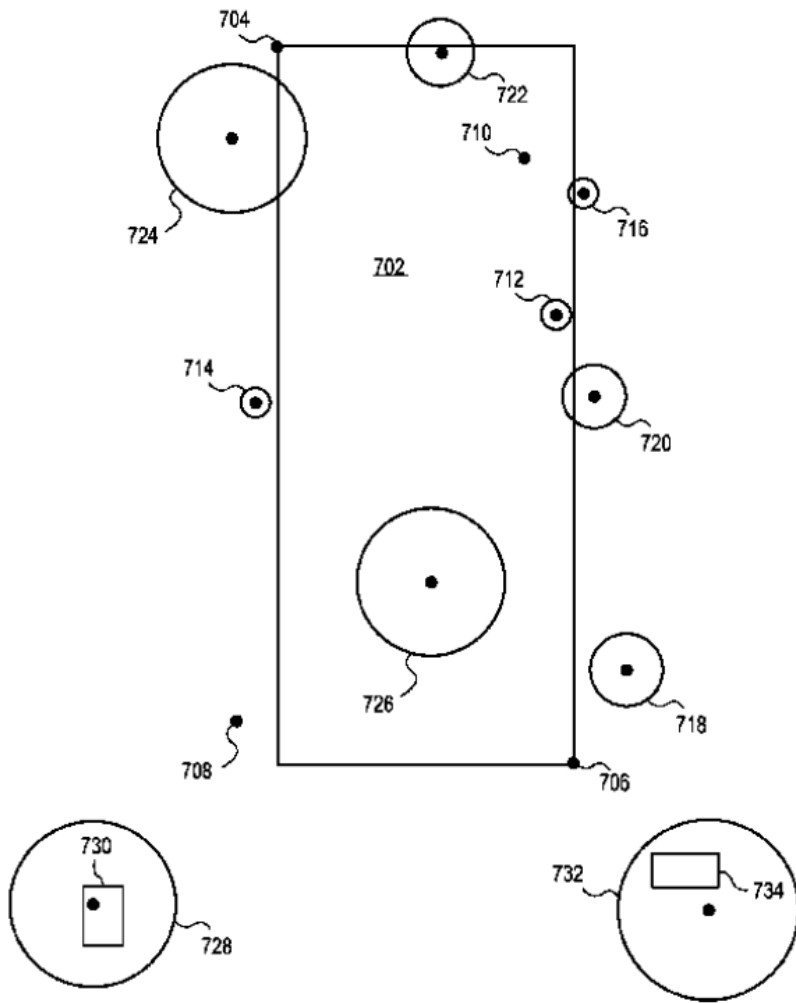


自社従業員、顧客、パートナー向けに自社アプリを提供する機会が増加している

自社アプリはスマホ、タブレットなどのハンドヘルドデバイスにインストールされるがセキュリティ上の問題がある

アプリは、ハンドヘルドデバイスに重大な損傷を引き起こす可能性があり、データの損失や意図しないデータの送信を引き起こす可能性がある

アプリに対し、位置情報に基づくセキュリティラッピングを施すアイデア



- (1) 地理的ポリシーが規定されたアプリケーションセキュリティプログラム用のJavaクラスファイルを生成する
- (2) アプリケーションのJavaクラスファイル(アプリと、デバイスOSとの間のプロキシ)をアプリケーションセキュリティプログラムのJavaクラスファイルに置き換える
これによりアプリのセキュリティラッピングが完了する
- (3) デバイスのGPSデータ、ユーザが指定した精度値(円形領域の半径)を取得する
- (4) デバイスの円形エリアが許可エリアと交差するか、許可エリア内に完全に収まるかを決定する
- (5) 円形領域が許可領域と交差するか、完全に許可領域内にある場合に、アプリケーションの実行を有効にする

【ネットワーク接続認証のシステムと方法】

～デバイスとのペアリング～

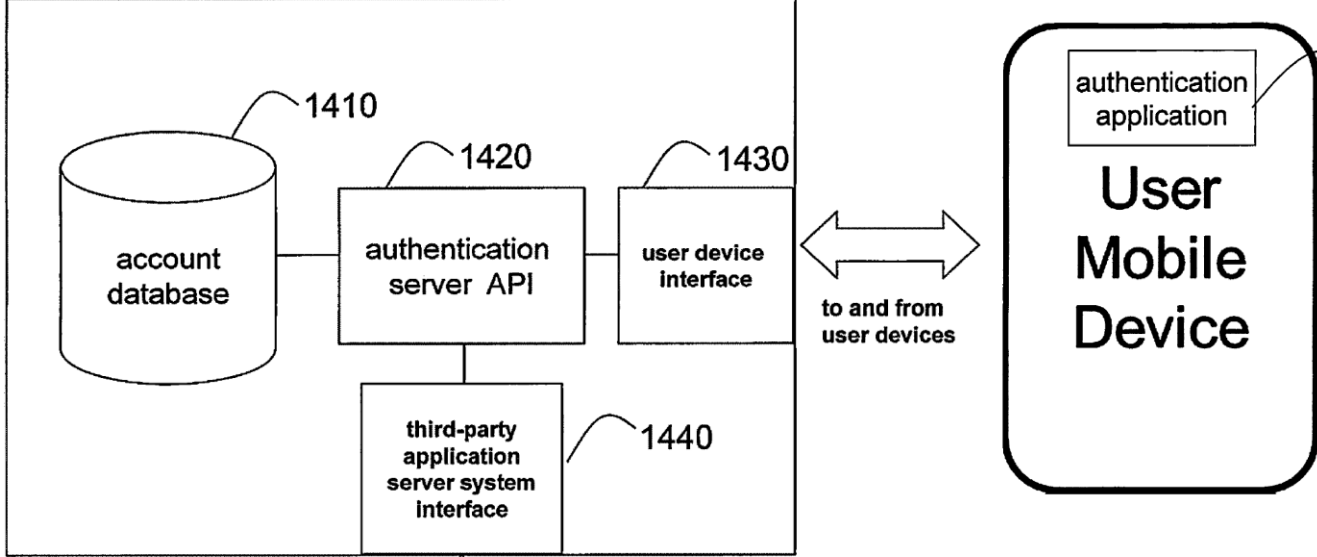
iovation

出願日 2013年8月7日

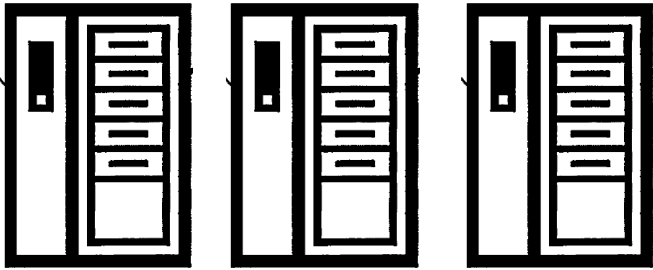
登録日 2017年5月2日

登録番号 US9641521

認証サーバ



to and from third-party
application server
systems



サードパーティーアプリケーション
サーバ

アプリ使用時の認証は一般にID、パスワードを用いる

その他、生体認証等も用いるが、生体認証、パスワードを用いずに安全な認証を行いたい

世界中のデバイス情報を取得し、ユーザとデバイスとをペアリングし、様々なアプリでの認証を容易にするアイデア

ユーザのモバイルデバイスにより、サードパーティーアプリケーションサーバを使用する場合、認証サーバが認証を行う

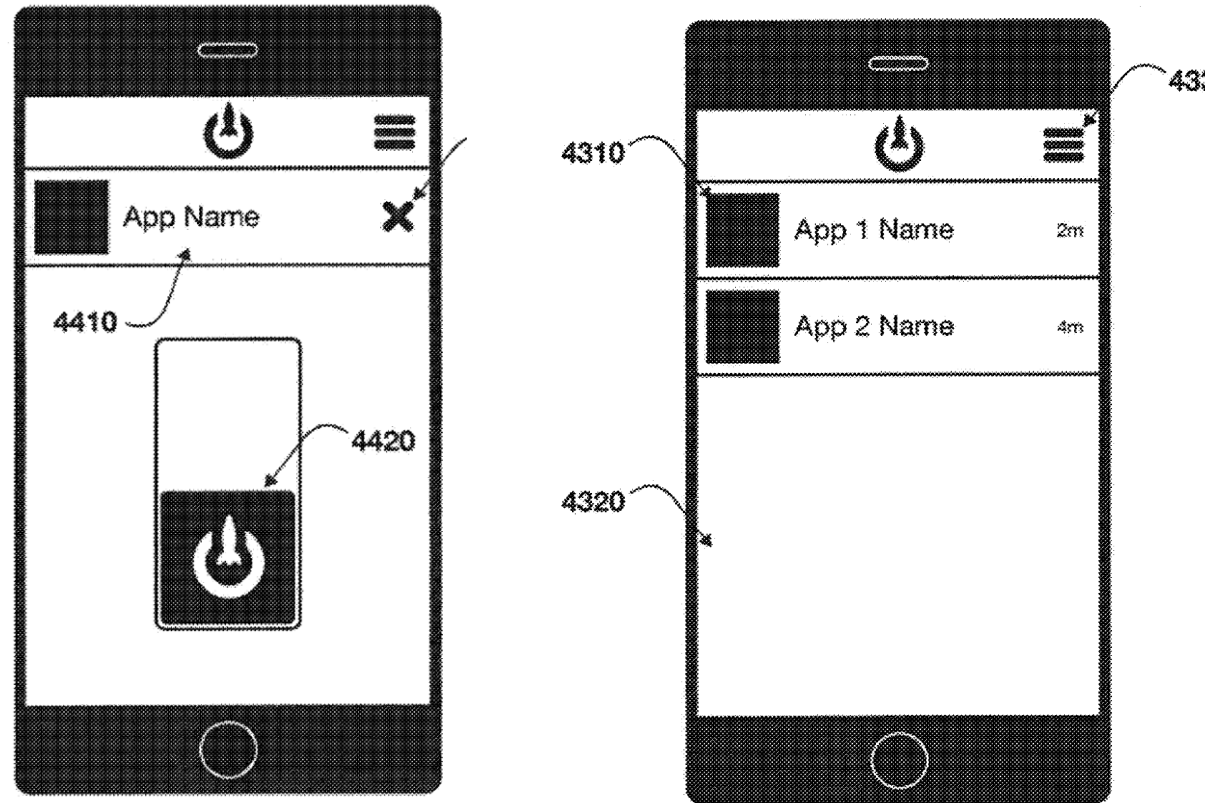
アプリを起動し、認証アイコン4420を上側にスワイプする

ユーザ名と、デバイス名を用いた認証処理が実行される

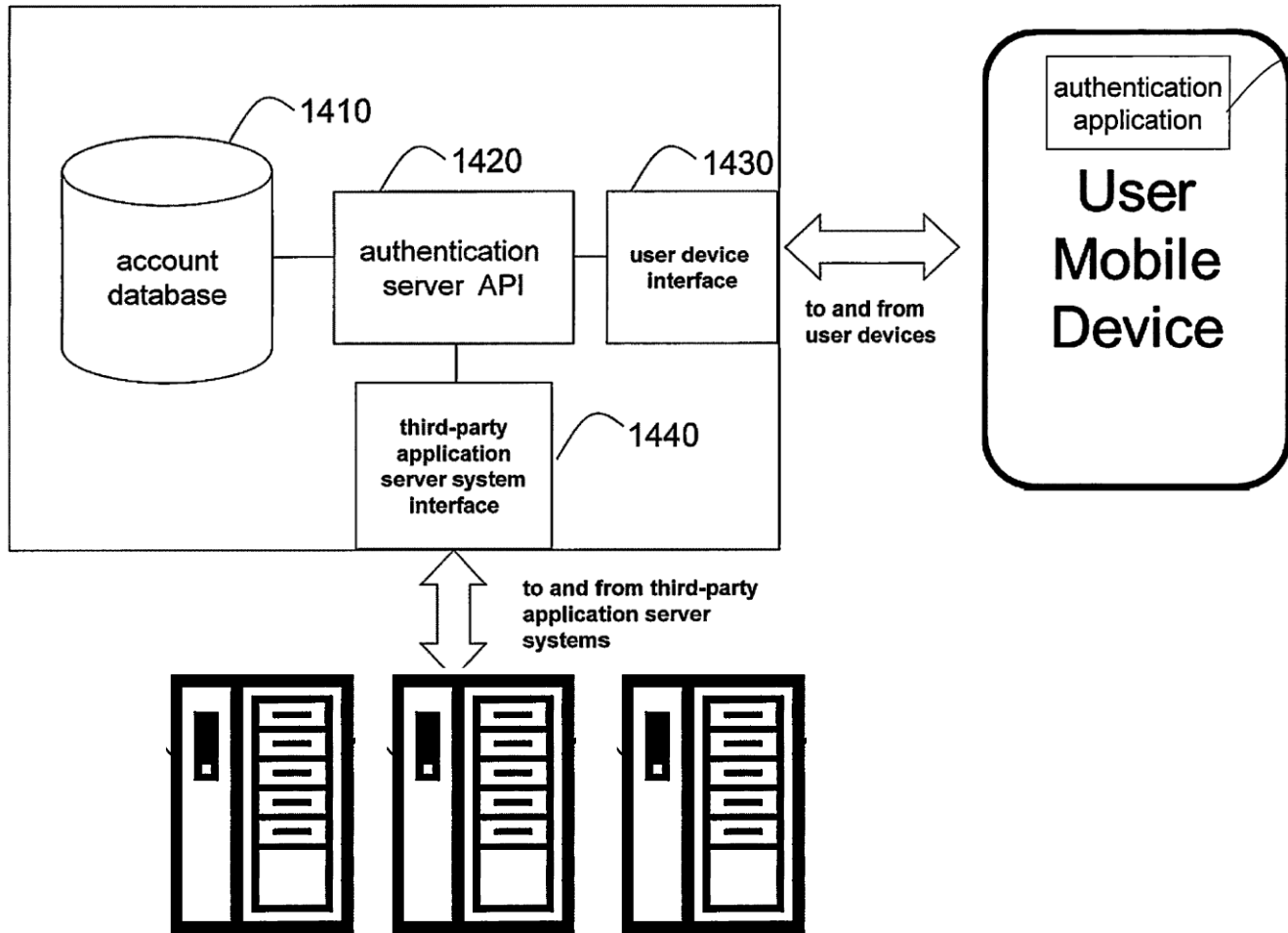
アクティブログ4320に、認証済みのアプリが追加される

全てのサードパーティーアプリはユーザ名と、ペアリングされた
デバイス名で認証が行われる

アプリごとのID、パスワードを用いた認証は不要



認証サーバ



サードパーティーアプリケーションサーバ

ユーザ名とモバイルデバイスとをペアリングする

サードパーティーアプリケーションサーバから第1認証要求を受け付ける

第1認証要求が有効であれば、モバイルデバイスに認証要求(ユーザ名を含む)を通知する

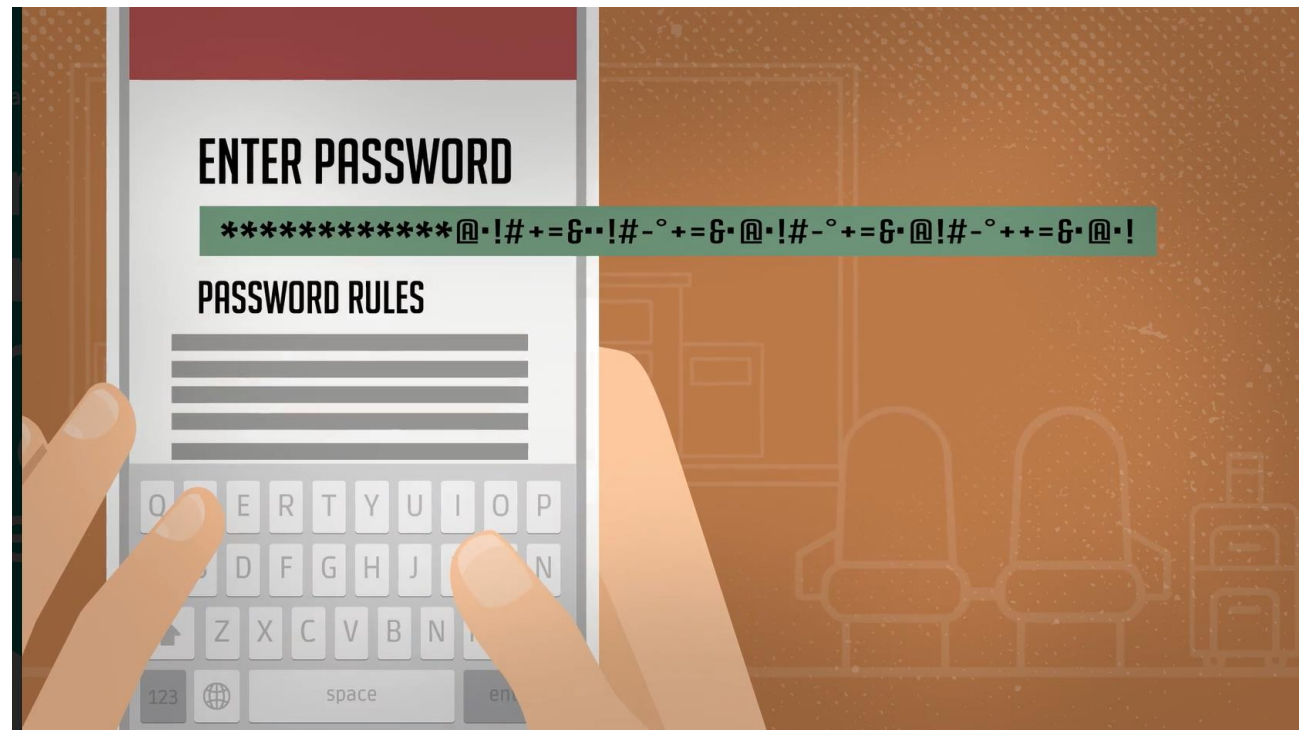
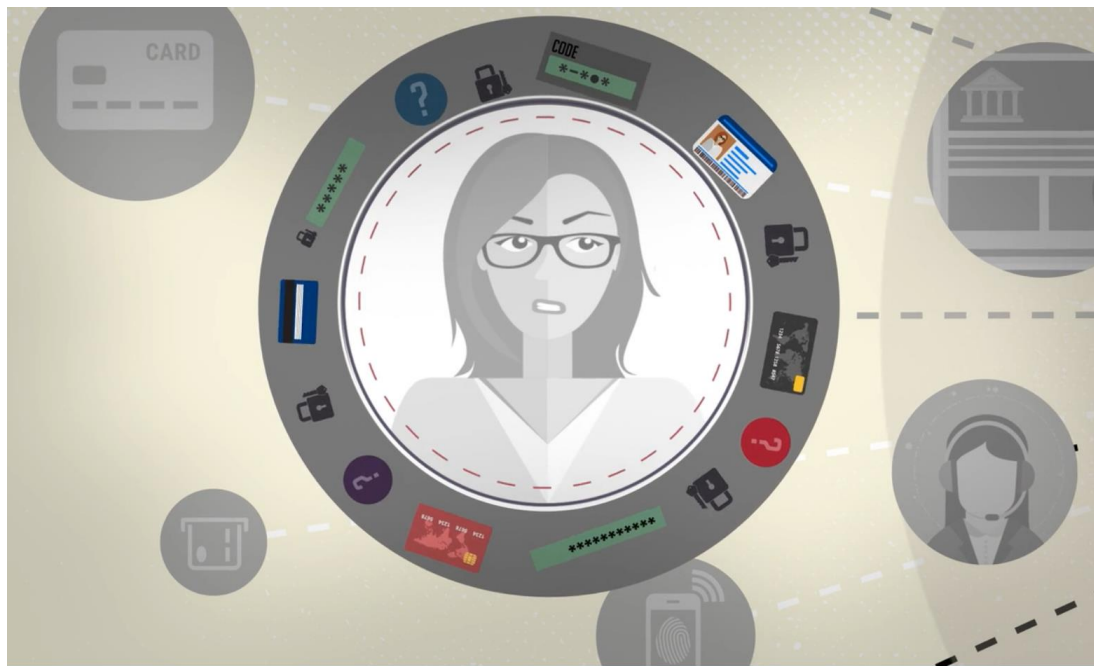
モバイルデバイスから、モバイルデバイスが暗号化した暗号化データ及び第2検証データを受信する

第2検証データが有効である場合、暗号化データをサードパーティーアプリケーションサーバへ送信する

暗号化データは特定のサードパーティーアプリケーションサーバのみが復号可能

認証が完了する

パスワード、ID、ペットの名前、生体認証・・・アプリごとの管理が大変 パスワードも長い、しかも複雑化



デバイス情報を取得し認証を行う。



iovation社 2004年設立 本社米国ポートランド

世界No.1の誤認知率0.0028%を誇る、デバイス認証システムを提供

パソコン、スマートフォン、ゲーム機器などのデバイスからデバイス情報を取得する
デバイスの情報を取得したいページに、タグを挿入するだけで簡単にデバイス情報を取得

デバイス情報の取得率は業界平均を上回る、平均97%

世界中の様々な業界のデバイス情報を30億台分保有。また3,000万台以上の不正デバイス情報を所有している。

1 高いデバイス認識率



デバイス情報の取得率は業界平均を上回る、平均97%を誇ります。

2 圧倒的デバイス数



世界の様々な業界のデバイスを30億台分保有し、3,000万台以上の不正デバイス情報も有しており、日々増え続けています。

3 低い誤認識率



誤検知によって優良顧客を排除してしまうリスクは、業界トップレベルの0.0028%です。

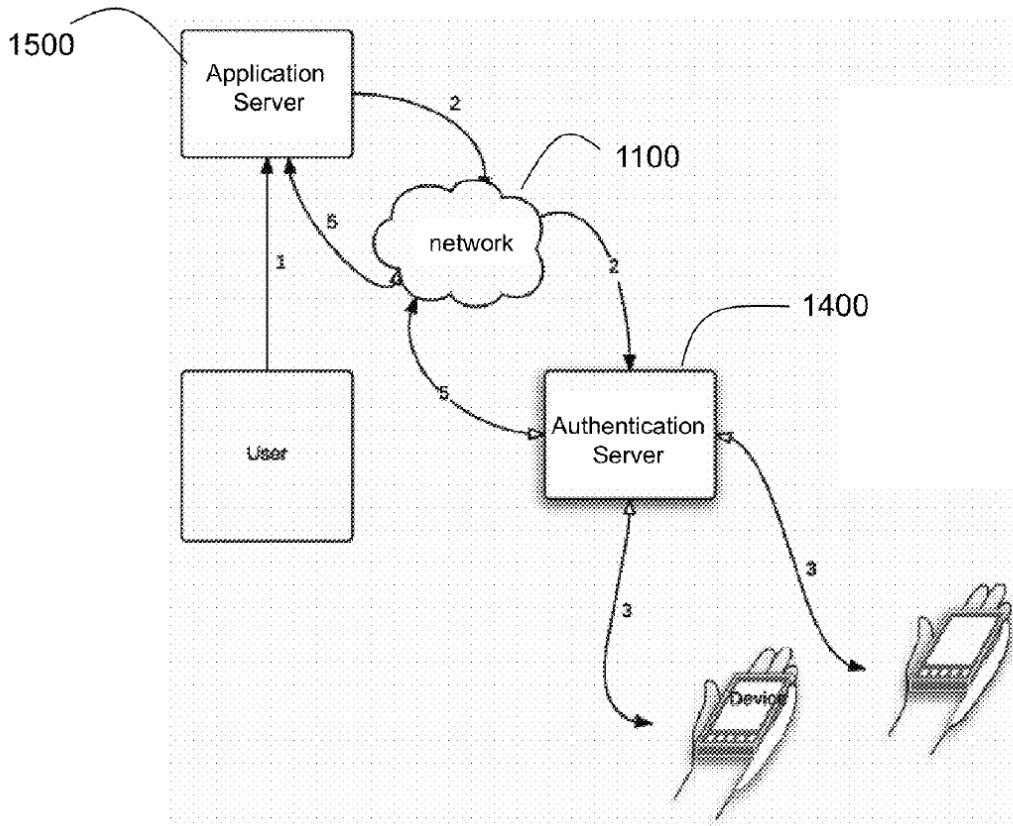
【グループ認証のシステムと方法】

iovation

出願日 2014年11月6日

登録日 2016年10月11日

登録番号 US9467445



グループとしての認証の必要性が増加している

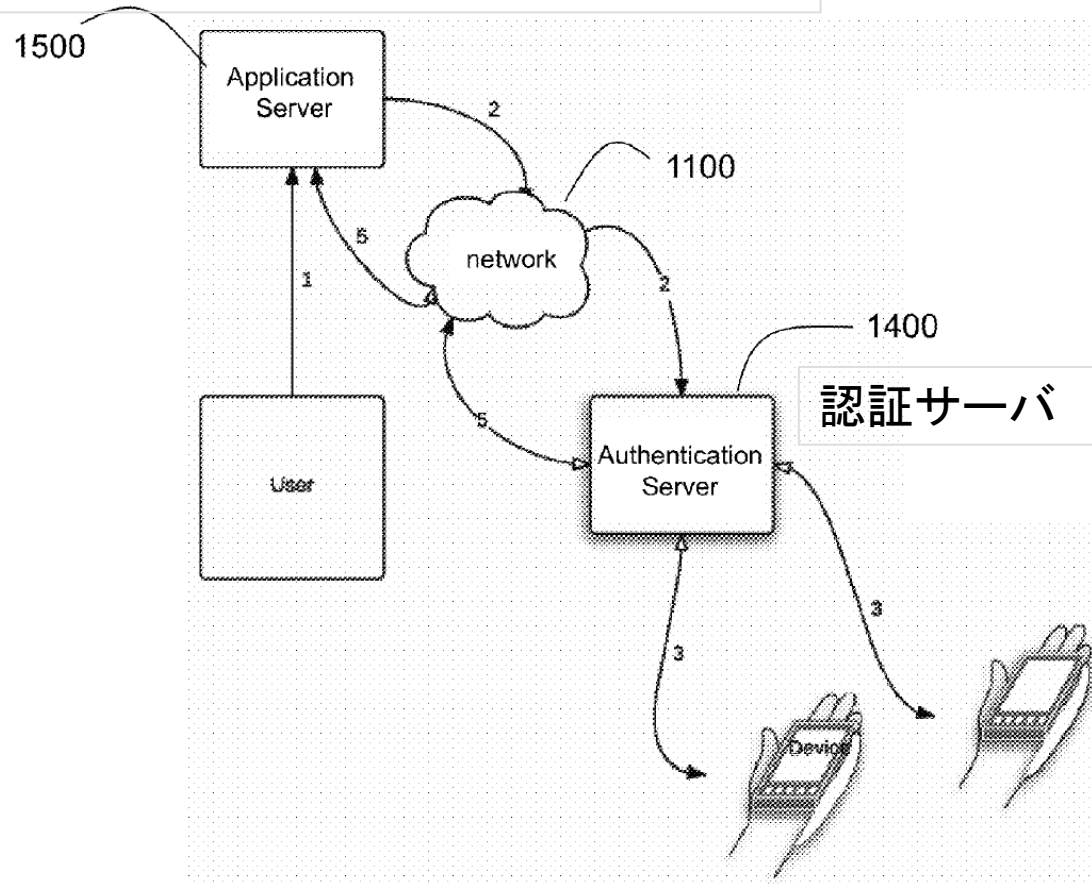
子供が2人の親から映画を見る許可を受け取りたいが、両親のどちらもいない場合がある

ビジネスパートナーが大規模な金融取引を互いにリモートで作業しながら一緒にサインオフしたい場合

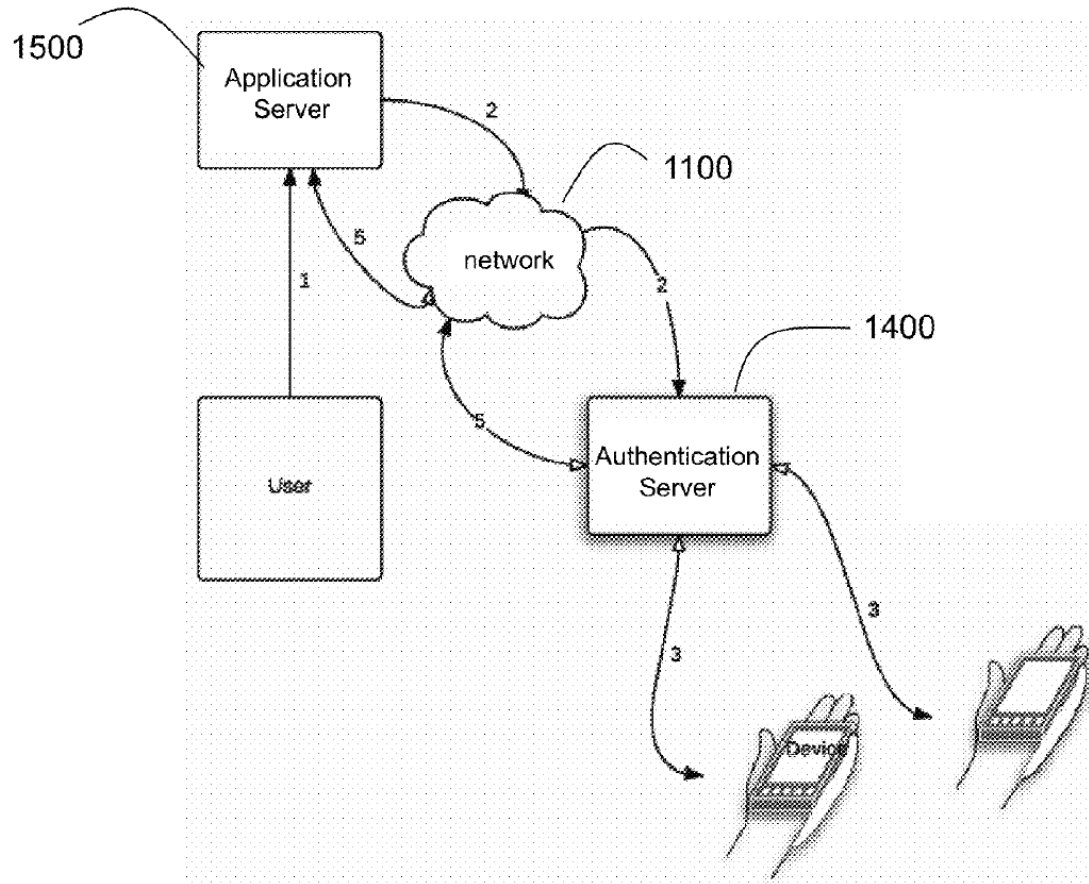
さまざまな場所にいる別々の個人が、同じアカウントの同じWebページに同時にアクセスしたい場合

少数派であっても、すべての関係者の承認ではなく、一定の割合が必要な場合。たとえば、ソフトウェアの更新には、一部の開発者と1人のプロジェクトマネージャーのみの承認が必要な場合がある

サードパーティアプリケーションサーバ



- 1 : ユーザはグループID及び認証要求をサードパーティアプリケーションサーバ1500へ送信する
- 2 : サードパーティアプリケーションサーバ1500は、グループID及びサードパーティアプリケーションサーバIDを認証サーバ1400へ送信する
- 3 : 認証サーバ1400は、DBを参照し、サードパーティアプリケーションサーバにより規定されたルールに基づきグループIDに対応するユーザIDを抽出する
ルールには、ポリシーが規定されている
例) グループ内のユーザの内、何人に認証を要求する、どのユーザに認証を要求するかのポリシー
- 4 : 認証サーバ1400は、ユーザデバイスに認証要求を出力する



5 : 各ユーザデバイスはユーザ応答を認証サーバ1400
に出力する

認証サーバ1400は、ユーザ応答をサードパーティアプ
リケーションサーバ1500へ送信する

サードパーティアプリケーションサーバ1500はグルー
プごとのポリシーに従い、認証を許可するか否かを判断
する

厳しいポリシー 60%の同意が必要

【アクティブなクエリを使用した産業用制御ネットワークでの設定ミスと敵対的な攻撃の検出】

indegy

出願日 2015年4月15日

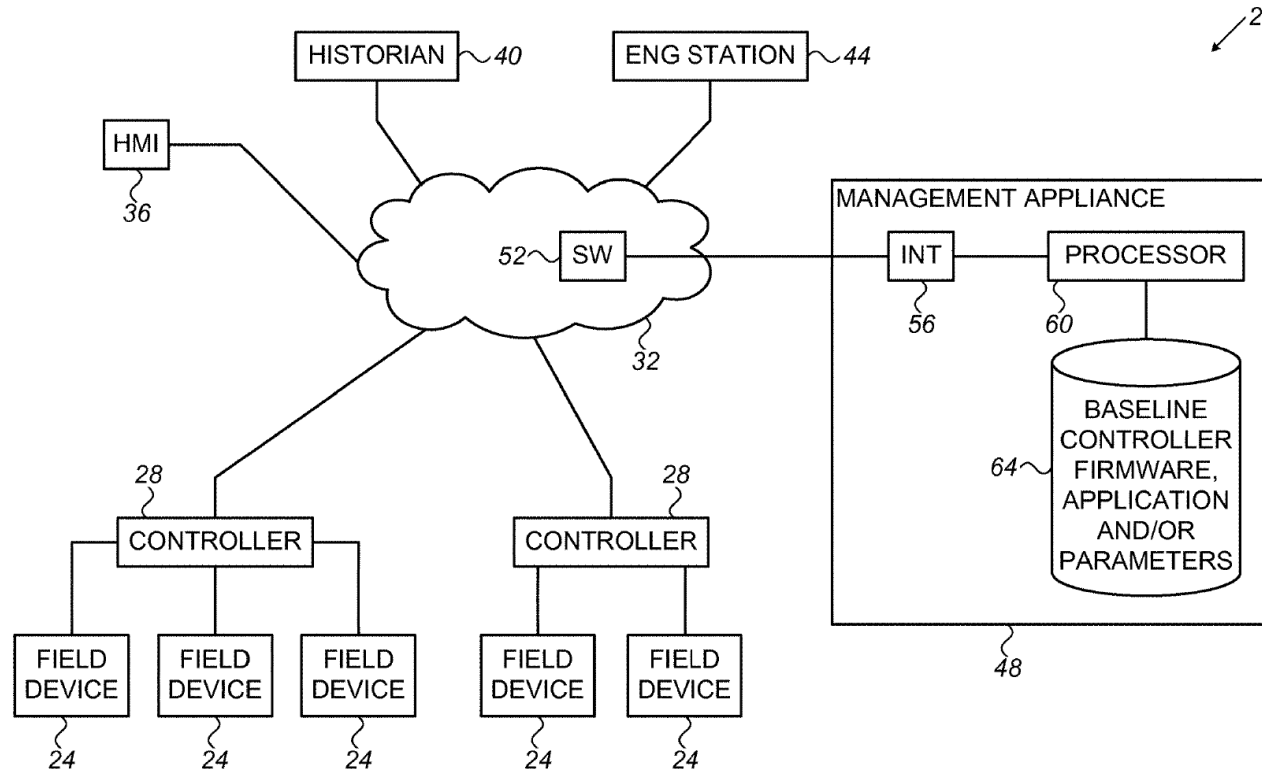
登録日 2019年4月16日

登録番号 US10261489

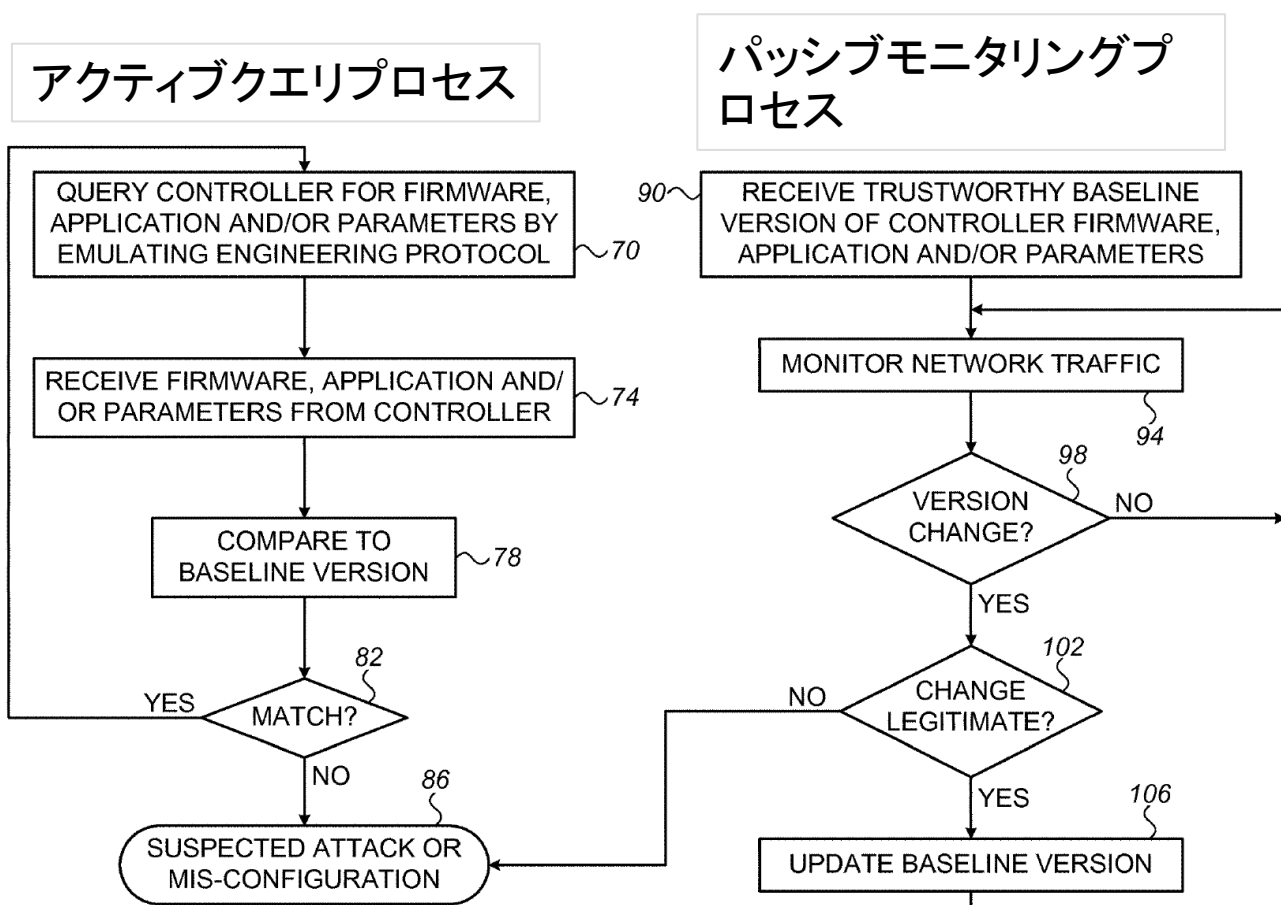
従来の産業制御システム（以下、ICS：Industrial Control System）は、外部のネットワークや情報系のシステムとは接続されていない。しかしながら、IoT導入に伴い産業制御ネットワーク内のコントローラ（PLC）に対する敵対的な攻撃リスクが高まる。またネットワークの設定ミスにより障害が発生するリスクもある

2つのプロセスにより、産業用制御ネットワークのトラフィック内のコードを監視するアイデア

コントローラ28は、フィールドデバイス24,24,24・・・を制御する。マネージメント装置48は、ネットワークトラフィック中のコードを監視する



パッシブモニタリングプロセス



(i) コントローラのファームウェア、アプリ、パラメータ等のベースラインバージョン(ベースラインコード)を取得

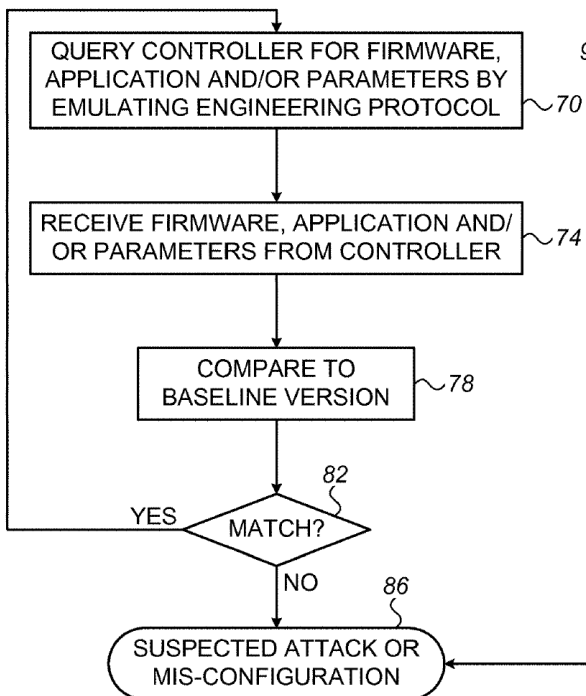
(ii) 産業用制御ネットワークを介して交換されるトラフィックを継続的にインターセプトする

(iii) インターセプトされたトラフィックがコード更新トランザクションで構成されているか否かを判断

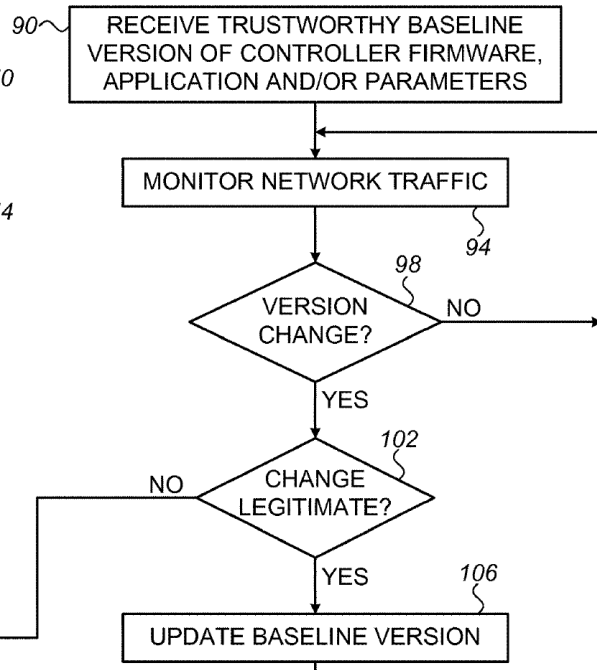
(iv) コード更新トランザクションを含む場合、コード更新トランザクションが正当であるかどうかを確認

(v) コード更新トランザクションが正当である場合、コードの最新の信頼できるベースラインバージョンを更新

アクティブクエリプロセス



パッシブモニタリングプロセス



アクティブクエリプロセス

(i) コントローラを構成するために使用されるエンジニアリングプロトコルをエミュレートすることにより、コントローラが現在使用しているコードの報告を要求

(ii) 報告されたコードをコードのベースラインバージョンと比較

ハッキング・設定ミス判断

(i) アクティブクエリプロセスが、パッシブモニタリングプロセスによって継続的に更新されているベースラインバージョンとの不一致を検出した場合、または、
(ii) 前記パッシブモニタリングプロセスが、コード更新トランザクションが違法であることを検出した場合、ハッキング、または、設定ミスと判断する。

Indegy社 イスラエル本社

産業機器向けのサイバーセキュリティソリューションを提供している



Products & Technology

Solutions

Partners

Resources

Company

Request a Demo



Indegy Industrial Cybersecurity Suite

Get end-to-end visibility, security and control for all OT activities by analyzing your industrial security posture at the network and device levels.

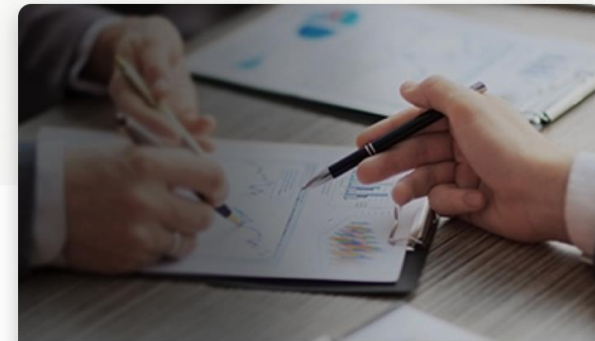
Learn More [→](#)



Indegy Device Integrity

Go beyond passive network monitoring with active detection checks that automatically and safely discover all changes related to ICS devices.

Learn More [→](#)



Indegy Risk Assessment

Understand which assets are at risk, where your OT network is most vulnerable and how to secure your environment with this customized service.

Learn More [→](#)



イスラエル、アメリカに続き、2017年から日本でも製品販売

1. OT(Operational Technology)環境のサイバーリスクを可視化

一般的なIT資産管理ツールでは、OT環境の資産情報を収集することは不可能。Indegy Spは、PLCやDCS(Distributed Control System)など、制御システムの最新情報を自動的に定例集計。制御システムなどに存在するサイバーリスクを可視化

→特許技術：PLCの状態変更・コードの書き換え・構成情報など、これまでの監視ツールでは取得できなかった情報を取得できる

2. AI脅威検出機能

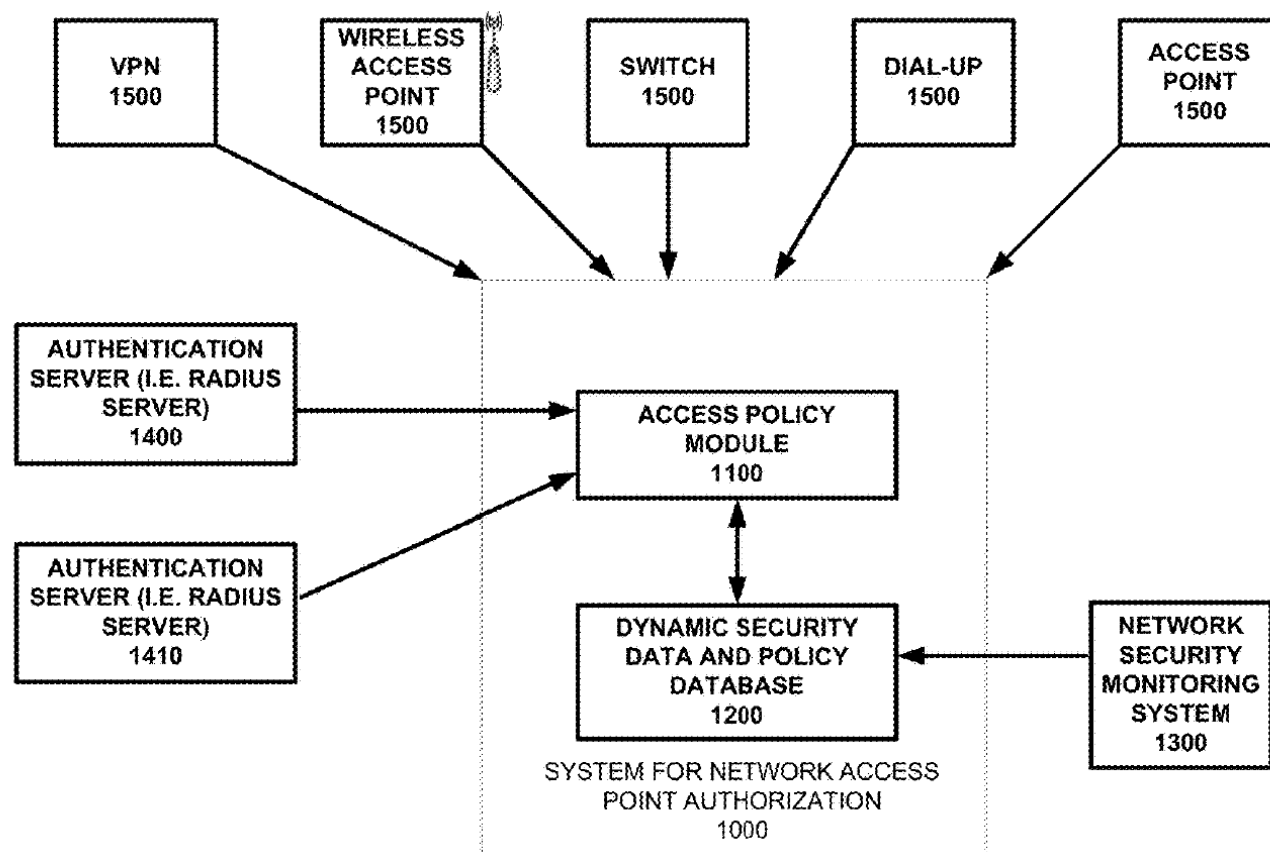
Indegy SPにOT環境の通信パターンを学習させ、パターンから逸脱した通信を自動検知

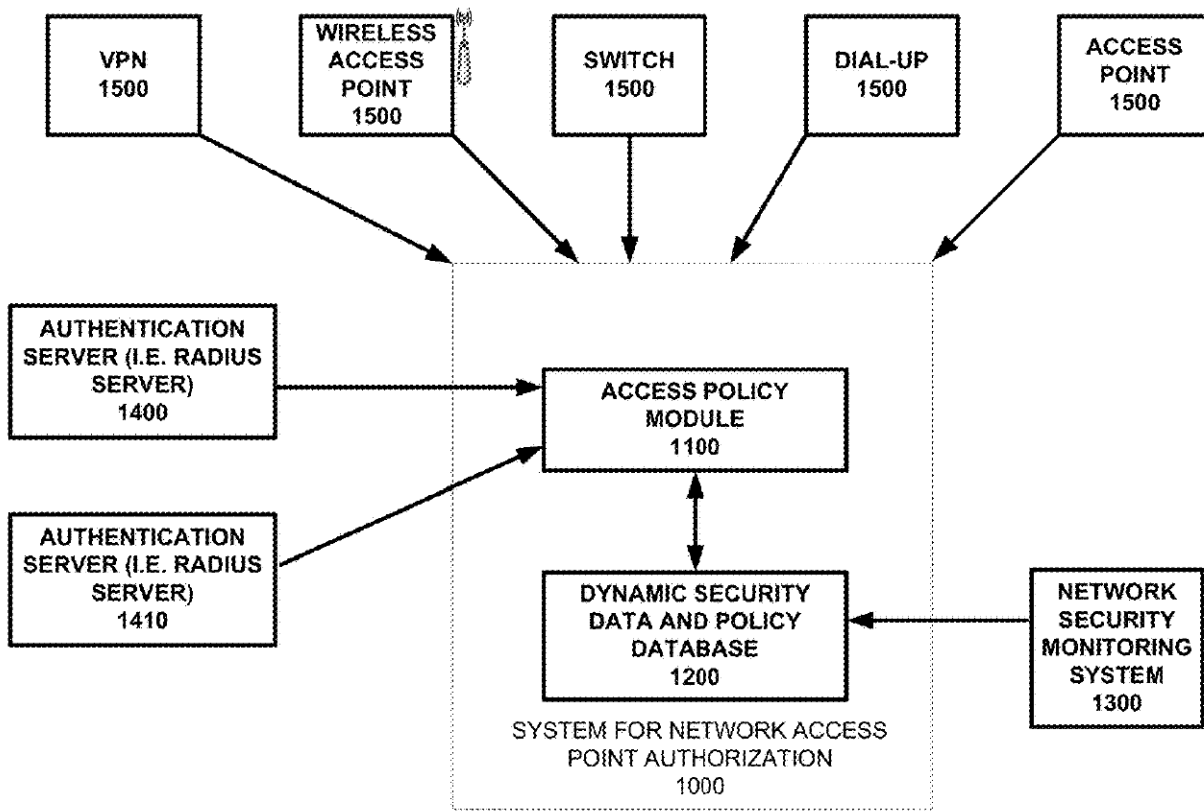
【認証サーバを用いたダイナミック セキュリティ方法及びシステム】

ForeScout Technologies
出願日 2013年11月18日
登録日 2015年3月5日
登録番号 US9027079

従来のITセキュリティアーキテクチャの大部分は、最新のハッキング状況进行处理するように構築されていない。そのため、ハッカーは多重に防御されたネットワークに繰り返し侵入を試みる

アクセスのあったデバイスを隔離し、セキュリティポリシーを満たすか否か判断する





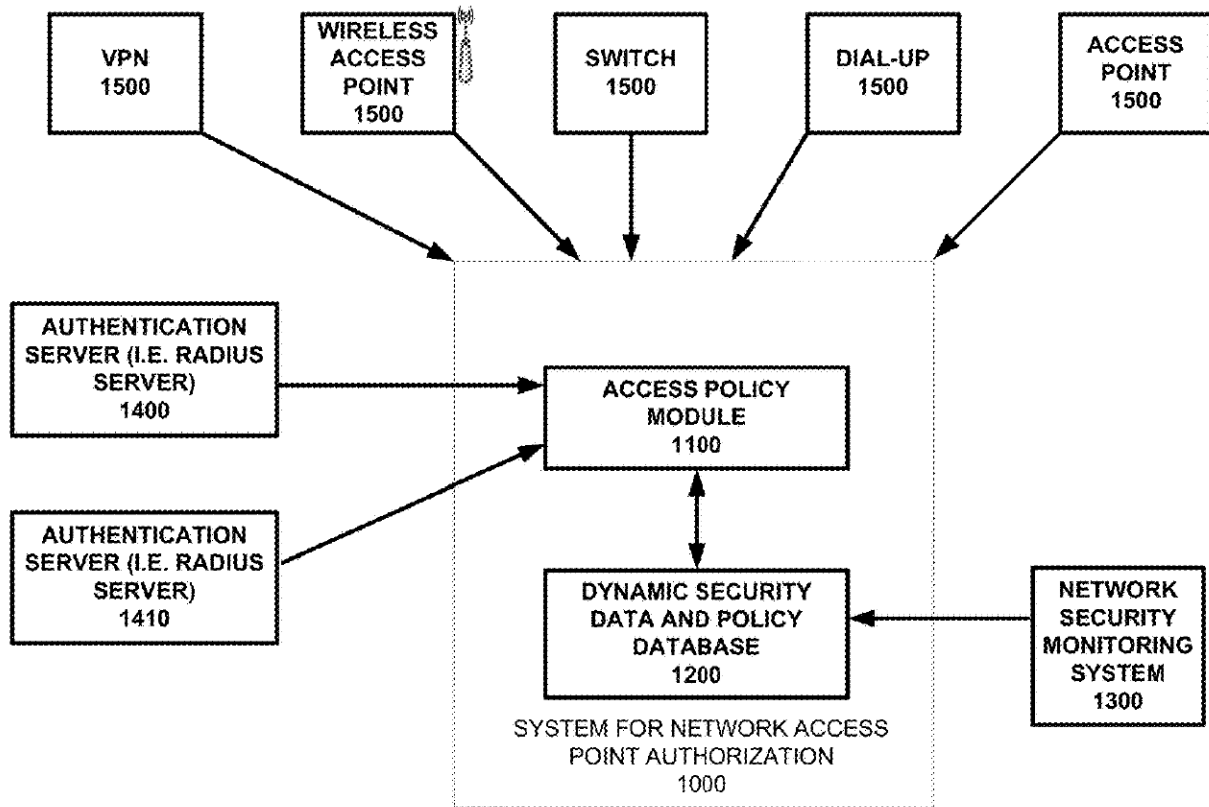
ネットワークセキュリティ・監視システムはダイナミックセキュリティ認証サービスサーバー (DSASS : Dynamic Security Authentication Service Server) を備える。

ダイナミックセキュリティ認証サービスサーバー (DSASS)はダイナミックセキュリティデータ・ポリシーデータベースDSDPD1200(Dynamic Security Data & Policy Database)を備える。

データベース1200には、

- (a) デバイス毎にセキュリティポリシーコンプライアンス
- (b) 監視システムから受信したセキュリティ情報
- (c) 認証サーバー1400から受信した認証情報が記憶されている。

様々なデバイスがアクセスポイント1500を通じてネットワークにアクセスするが、以下の認証処理を行う



(1) ユーザーが第1デバイスを使用してネットワークリソースに接続しようとしているアクセスポイント1500から、ユーザーの認証資格情報を受信する

(2) (i) 認証資格情報に関連して認証サーバー1400から受信したデータと (ii) DSDPD1200から受信した第1デバイスに関連付けられたコンプライアンスデータに基づいて、まず第1デバイスにネットワークへの隔離されたアクセスを許可する

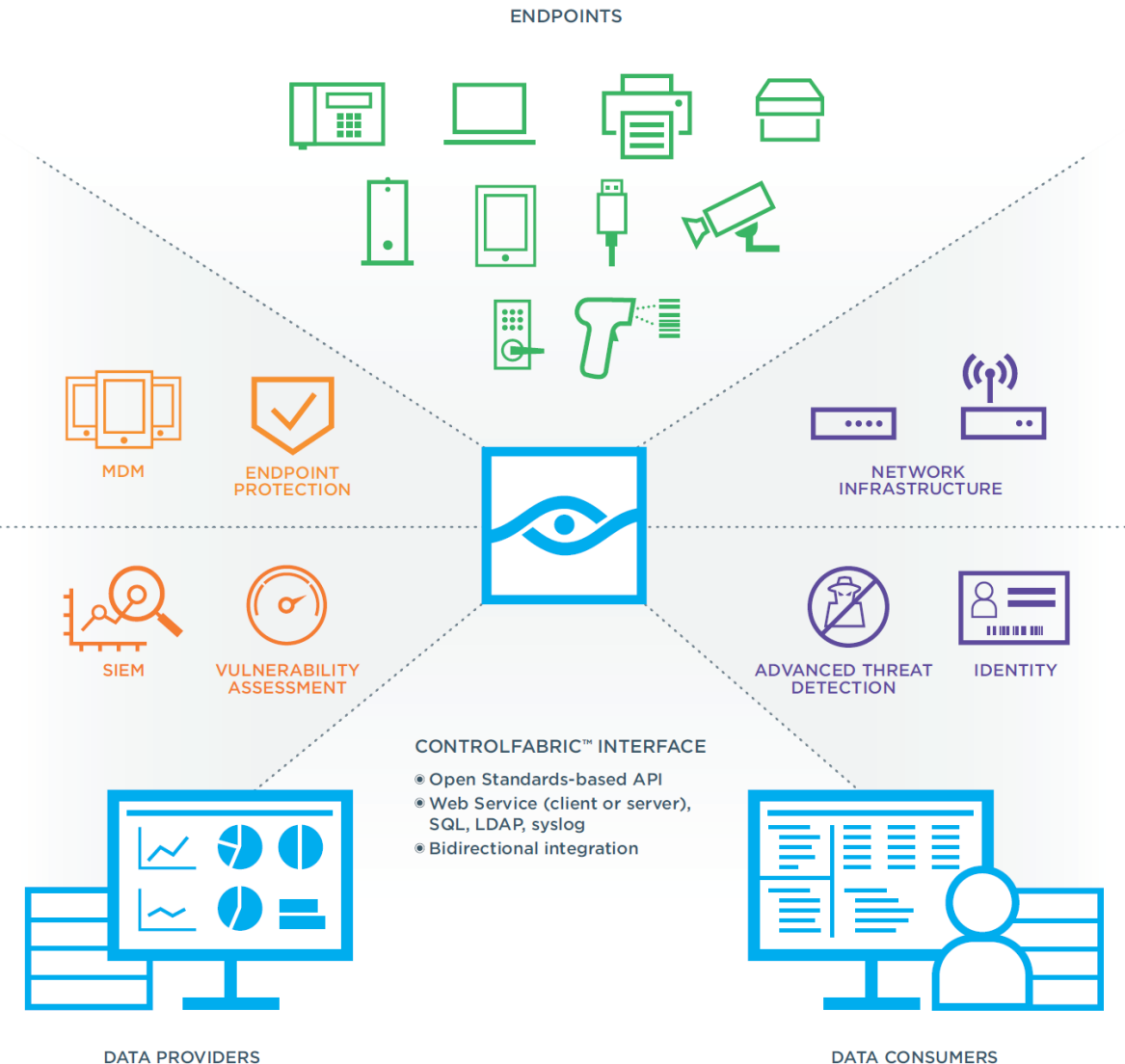
(3) 第1デバイスに隔離されたアクセスが許可された後、隔離されたアクセスを介した第1デバイスのさらなるコンプライアンステストを実施する。

(4) コンプライアンステストの結果に応じて、第1デバイスのアクセスが許可されるネットワークリソースを決定。

(5) アクセスポイント1500は、第1デバイスに、許可されたネットワークリソースへのアクセスを認める。

Forescout Technologies社

2000年設立 本社米国カリフォルニア州



デバイスがネットワークに接続した瞬間に監視するユニークなソリューションを、Global 2000企業および政府機関に提供している

Advanced Threat Detection (ATD)

本特許の一機能・・・デバイスからアクセスがあった場合、隔離されたアクセスを許可し、コンプライアンステストを行う

ForeScout ControlFabric™ Architectureカタログより 2019年9月7日