特集《IoT と知財》

IoT セキュリティ特許と査証制度

会員　河野　英仁

要　約

多くの企業が IoT デバイスを用いたデジタルトランスフォーメーション（DX）への取り組みを開始し，単なる「モノ」の販売にとどまらず，AI（人工知能）を活用した様々な「コト」サービスビジネスによる収益モデルを追求する時代となっている。

自動車，スマートフォン，工場内のセンサ・コントローラ，家電機器等ありとあらゆるデバイスがネットワークにつながるようになった。この傾向は AI 技術の進化及び 5G の本格普及に伴い更に加速するであろう。

その一方で IoT セキュリティの脆弱性が指摘されており産業機器に対する攻撃のほか，脆弱な IoT デバイスを踏み台にした DDos（Distributed Denial of Service（分散型サービス妨害））攻撃等が頻繁に行われている。本稿では産業用途向け IoT セキュリティ技術に注目し，米国及びイスラエル企業の IoT セキュリティ特許とビジネスについて紹介し，更に侵害立証が困難とされる IoT 技術分野における査証制度の活用について検討を加える。

目次

1．はじめに

第 4 次産業革命と 5G の普及によりこれまでインターネットにつながっていなかった工場のセンサ，アクチュエータ，ロボット，車載装置等が続々と IoT 機器としてインターネットにつながり，生産管理，故障予測，生産効率の向上，自動運転等の新たなサービスが次々と生まれている。

その一方でインターネットにつながりだした IoT 機器はサイバー攻撃に対し非常に脆弱であり，IoT 機器が搭載される機器自身が攻撃対象となるほか，ハッキングされた大量の IoT 機器が踏み台として利用され，他の機器に対しサイバー攻撃を行う事態も発生している。

本稿では，IoT 機器の脆弱性について解説するとともに，米国及びイスラエルのスタートアップ企業の IoT セキュリティに関する特許及びビジネスを解説する。また法改正により導入された査証制度の IoT 特許訴訟における活用を検討する。

2．IoT 機器に対するセキュリティが脆弱な理由

（1） IoT 機器に対するハッキング

2010 年 6 月イラン核施設内のウラン濃縮用遠心分離機の PLC（Programmable Logic Controller）が，Windows 上で動作するコンピュータワーム Stuxnet（スタンクスネット）に乗っ取られ，動作不能となる事件が発生した。この事件では 8,400 台もの遠心分離機が攻撃された。

また産業機械だけではなくコネクテッドカーもハッキングの対象となっている。クライスラー社の Jeep

が外部からハッキングが可能であると指摘されリコール対象となった。これはセキュリティ企業であるIOActive 社の Charlie Miller 氏らが Jeep の車載システム「Uconnect」の脆弱性を見つけエアコンの操作，エンジンの停止等が遠隔より可能であることを動画で公開した事により明らかとなった。

これらのケースはいずれも IoT 機器自身が攻撃された事例であるが，IoT 機器自体がハッキングにより踏み台にされ，他のサーバの攻撃に用いられることもある。2016 年 9 月には「Mirai」と称するマルウェアにルータ，ネットワークカメラ等の様々な IoT 機器が感染し，特定のサーバに大量のパケットを送信する DDoS 攻撃が行われた。Mirai ウィルスに感染した IoT 機器は世界中で約 50 万台にものぼるという。

（2） IoT 機器のセキュリティが脆弱である理由

読者が使用されている PC では，セキュリティアップデート，OS のアップデートが頻繁に行われており，セキュリティレベルは高いと言える。しかしながら，IoT 機器は PC と異なり人が操作・監視しないことが多く，ハッキングされていても気づかない事が多い。またネットワークに常時接続されていないこともあり，遠隔監視ができない，ソフトウェアを適時にアップデートできないという問題もある。IoT 機器数が多いため，個人のスマートフォンでは気を使う ID 及びパスワードについても初期設定のままであることが多い。初期設定では一般に ID は「Admin」，パスワードは「Pass」等となっていることが多い。ハッカーは代表的な初期設定の ID 及びパスワードの組合せリストを有しており，これらを逐次入力するだけで簡単にログインされてしまう。

Insecam.org では世界中の Web カメラのうち，セキュリティ対策がおろそかで誰もが自由に見ることができる Web カメラの映像を公開している。残念なことに日本は下記図 1[(1)] に示すように米国に次いで第 2 位という脆さである。

Japan（2070）の表示をクリックすると，セキュリティ対策がなされていない日本各地の Web カメラ画像が表示される。Web カメラ一つをとっても如何にセキュリティが脆弱であるかが理解できる。

第 4 次産業革命により今後も IoT 機器が爆発的に増加するであろうし，より深刻な問題に発展していく可能性がある。次章ではこのような IoT 機器に対するセキュリティソリューションを提供し，また特許についても積極的に取得している米国及びイスラエルのスタートアップを紹介する。

3．米国及びイスラエルの注目 IoT セキュリティスタートアップ特許とビジネス

IoT セキュリティといえども数多くの分野に分類される。本稿では主に工場・自動車等の産業用途向け IoT セキュリティに着目し，米国及びイスラエル企業の特許及び各社の IoT セキュリティを用いたビジネスについて紹介する。

（1） CyberX Israel 特許

(i) 特許の概要

CyberX Israel は，「産業用制御システムへのサイバー攻撃を軽減する方法」と称する米国特許第 10015188 号（188 特許）を所有している。188 特許は 2015 年 8 月 20 日に出願され，2018 年 7 月 3 日に登録された。

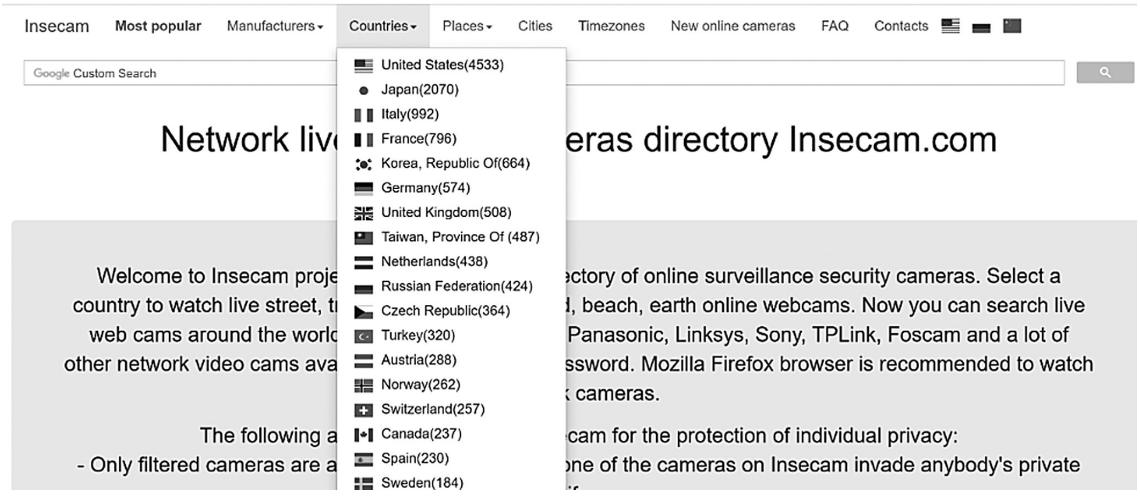

図 1　Insecam.org の HP

188 特許は AI（人工知能）を用いて産業用機器のプログラマブルロジックコントローラー（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である。

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おり，特に，プログラマブルロジックコントローラー（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。188 特許における監視方法は，機械学習を用いた学習モードと保護モードとに大別される。

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。そして保護モードでは，完成した学習済みモデルを用いて PLC の状態を推定する。保護モードでは第 1 状態から第 2 状態へ遷移する遷移確率を随時算出し，算出した遷移確率が閾値を超える場合，アラート，ノードの無効化，パケットのブロック等の防護措置をとる。ここで新たなデータが取得できた場合，再度学習モードでの学習が行われる。以上の処理を繰り返すことにより，学習モデルによる推定精度が向上することとなる。

(ii) ビジネスの紹介

CyberX Israel 社は，産業用制御システムのセキュリティに特化した企業であり，機械学習を用いた分析を得意としている。主に米国政府機関，エネルギー，化学プラント等 350 社以上に製品を導入している。図 2[(2)] に示すように，リアルタイムで PLC のセキュリティに関する情報が担当者に通知される。

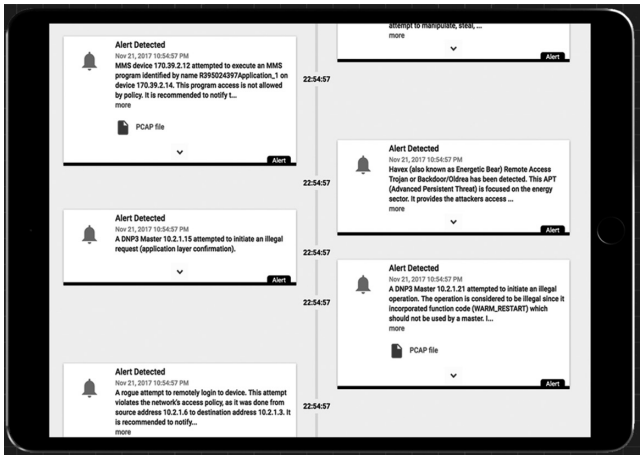

図 2　セキュリティアラートの表示

（2） PatternEx 特許

(i) 特許の概要

PatternEx 社は，「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」と称する米国特許第 9904893 号（893 特許）を有している。893 特許は 2016 年 12 月 16 日に出願され，2018 年 2 月 27 日に登録された。

893 特許はダブル AI，すなわち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である。

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。そこで，893 特許は教師なし学習と，教師あり学習との双方を用いて精度向上を図るものである。

ログデータから特徴マトリックスを生成し，異なる複数の方法により，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は，統計的外れ値検出方法である第 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。

そして，生成したトップスコアベクトルと適応モデルの GUI とを出力し，セキュリティアナリストがラベル付けを行い，適応モデルに対し教師あり学習により学習させる。これにより，適応モデルの性能が学習により徐々に向上することとなる。

(ii) ビジネスの紹介

PatternEx 社は米国カリフォルニア州に本社をおき，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を提供している。

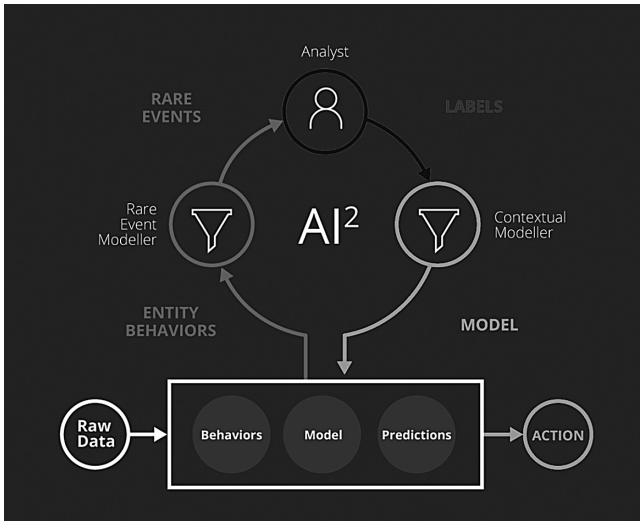

図 3　PatternEx のビジネスモデル

これは図 3[(3)] に示すように，生データが取り込まれ，行動に変換される。そして変換された行動からレアイ

ベントが発見され，アナリストがレアイベントについてレビューを行う。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を行い，脅威の検出効率を自動的に改善する。

（3） Argus Cyber Security 特許

(i) 特許の概要

Argus Cyber Security 社は，グローバルな自動車安全システムと称する米国特許第 9616828 号（828 特許）を所有している。828 特許は 2015 年 1 月 6 日に出願され，2017 年 4 月 11 日に登録された。828 特許はサイバーアタック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である。

自動運転への移行が進むに連れセンサ，ECU，アクチュエータ等の車載機器が増加し，サイバーアタックの対象になりやすくなっている。828 特許のグローバル自動車安全システム（GASS）20 は，図 4 に示すようにサイバーハブ 22 と，車両にインストールされるサイバーウオッチマン 40 とを備える。

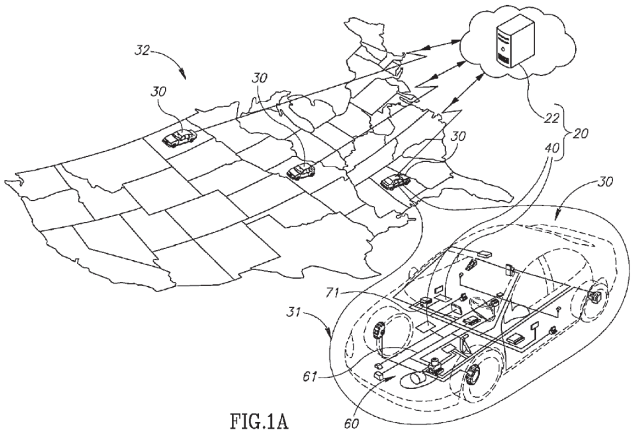

FIG.1A

図 4　828 特許の図 1.A

下記図 5 に示すように車内のサイバーウオッチマン 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動作を妨害する通信トラフィックを識別する。

サイバーウオッチマン 40 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。例えばウオッチマン 40B のプロセッサは，高速バス 61 上に「ポイズンビット」と呼ばれるドミナントビット（2 進数データの「0」）を送信させ，高速バス 61 上で伝搬する望ましくないメッセージを破壊する。またサイバーウオッチマン 40 は，ウオ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。

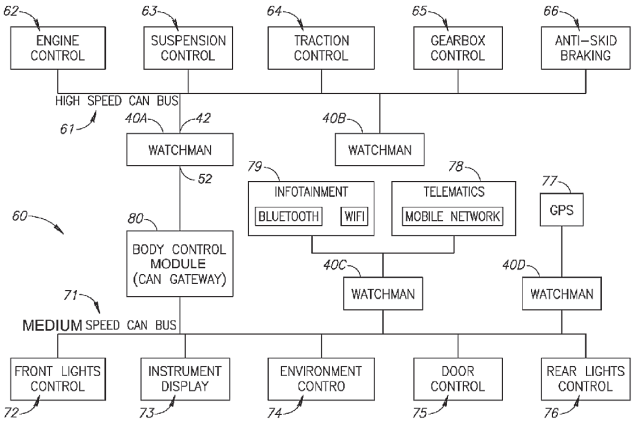

FIG.1B

図 5　828 特許の図 1.B

サイバーハブ 22 は複数の加入者車両からのウオ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アタックの脅威にさらされている可能性があるのか，サイバーアタックを受けているのか，またはサイバーアタック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。

ウオッチマン 40 はリストの内容に応じて機能を制限する。また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，車両のコンテキストデータ（車速等）を考慮する。最初に，ウオッチマン 40 は，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し，更新データが適切に暗号化されているか否かを判断する。

更新データが適切に暗号化されていると判断した場合，更新データを復号し，その後，車両のコンテキストデータ（車速）にアクセスする。ここで，車速が 10km/h 以上の場合，安全性を考慮して更新を行わず，車速が 10km/h 以下となった場合，ファームウェアの更新を行う。

(ii) ビジネスの紹介

Argus Cyber Security 社はイスラエルにて 2013 年に設立され，主に自動車向けサイバーセキュリティサービスを提供している。2017 年独コンチネンタル社が Argus Cyber Security 社を買収している。

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。Argus Cyber Security 社は数多くの特許技術によりセキュリティ対策を行っており，図 6[(4)] に示すように，世界中のハッキング状況をリアルタイムで監視・収集し，カーハッキングに対する対

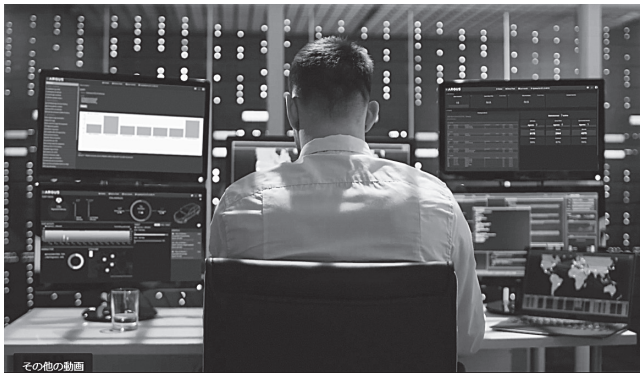

図 6　Argus Cyber Security 社の監視システム

策を行っている。

（4） Indegy 特許

(i) 特許の紹介

Indegy 社は「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」と称する米国特許第 10261489 号（489 特許）を所有している。489 特許は 2015 年 4 月 15 日に出願され，2019 年 4 月 16 日に登録された。

従来の産業制御システムは，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。

489 特許は 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である。

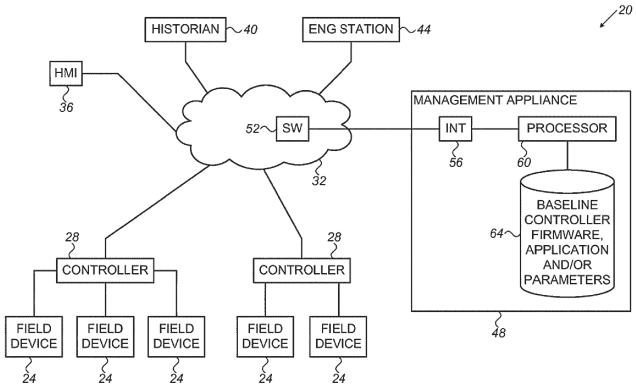

図 7　489 特許の図 1

図 7 に示すように，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。

監視プロセスにおいては，図 8 に示すようにパッシブモニタリングプロセスとアクティブクエリプロセスとが同時進行で行われる。パッシブモニタリングプロセスでは以下の（a）～（e）の処理が行われる。

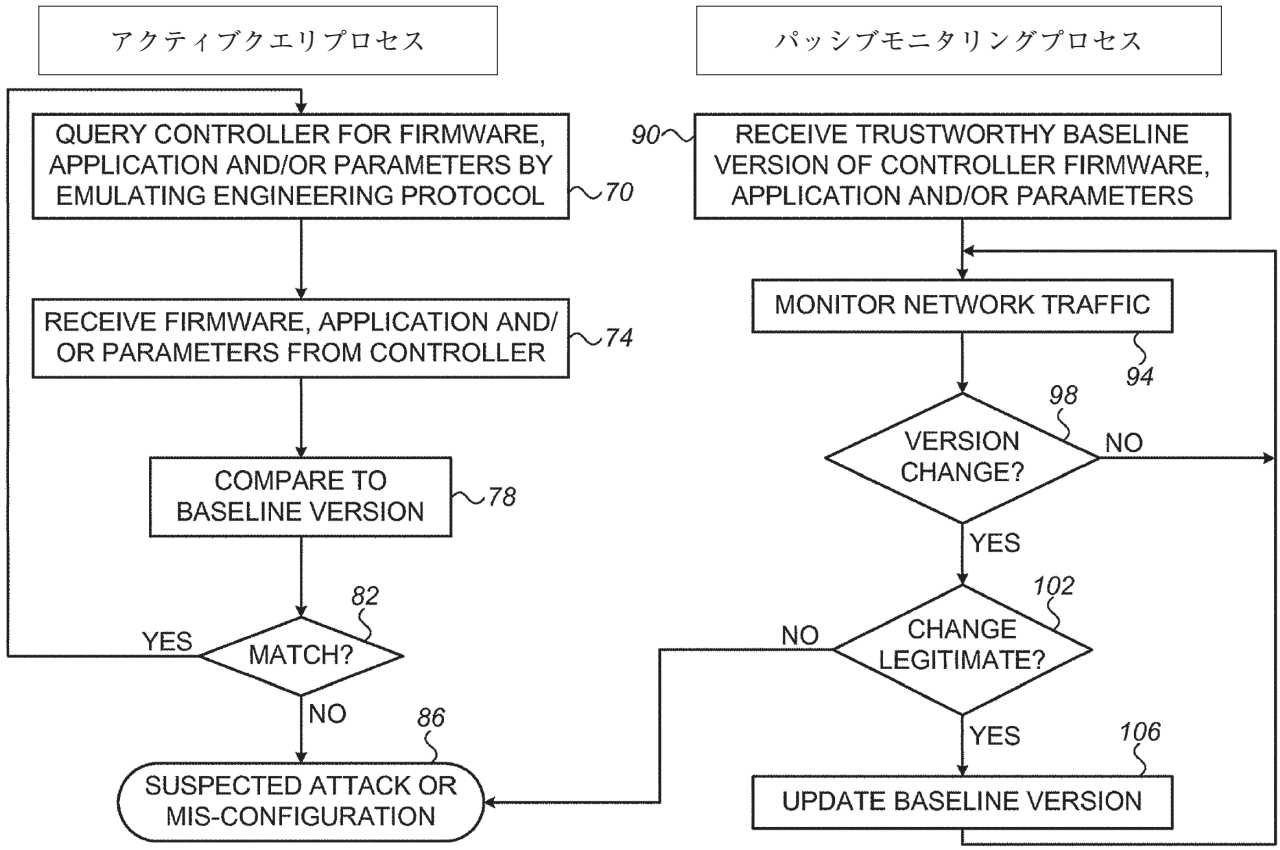

図 8　489 特許の図 2

(a)　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）を取得する。
(b)　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。
(c)　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する。
(d)　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否かを確認する。
(e)　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する。

アクティブクエリプロセスは以下の（a）及び（b）の処理が行われる。
(a)　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し，コントローラが現在使用しているコードの報告を要求する。
(b)　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する。

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，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。つまりパッシブモニタリングプロセスでは更新コードをインターセプトし，更新が適切に行われているか否かを監視し，アクティブクエリプロセスではエミュレートを行うことで更新コードのバージョンの一致性を監視し，相互のプロセスで不一致が発生しないかを監視する。

(ii) ビジネスの紹介

Indegy 社は，イスラエルに本社をおき主に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。

イスラエル，アメリカに続き，2017 年から図 9 に示す Indegy センサ[5]を日本でも製品販売している。Indegy センサは，PLC や DCS（Distributed Control System）など，制御システムの最新情報を自動的に

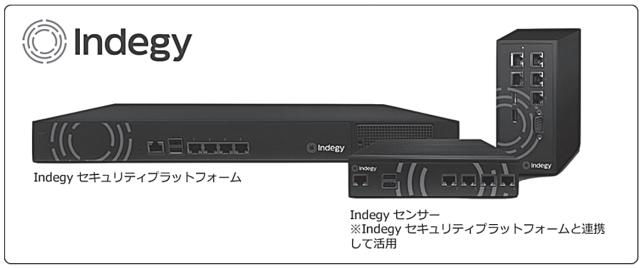

図 9　Indegy センサ

定例集計し，制御システムなどに存在するサイバーリスクを可視化することができる。具体的には，489 特許に示すように，PLC の状態変更，コードの書き換え状態，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することができる。

また，AI 脅威検出機能をも備えている。具体的には，OT（Operational Technology）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することができる。

（5）　ForeScout 特許

(i) 特許の概要

ForeScout Technologies 社は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と称する米国特許第 9027079 号（079 特許）を所有している。079 特許は　2013 年 11 月 18 日に出願され，2015 年 3 月 5 日に登録された。

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を処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。079 特許ではアクセスのあったデバイスを隔離し，隔離した状態でセキュリティポリシーを満たすか否か判断し，判断の結果に応じてデバイスにリソースを割り当てるアイデアである。

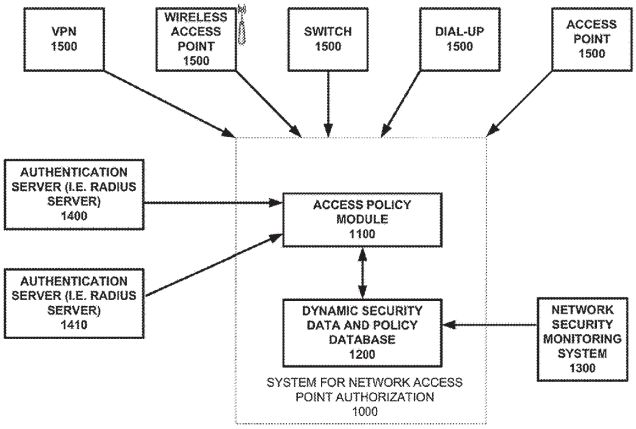

図 10　078 特許の図 1

図 10 に示すようにネットワークセキュリティ・監視システム 1000 はダイナミックセキュリティ認証サービスサーバ（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（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 1400 から受信した認証情報

が記憶されている。

様々な IoT 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，本システムでは以下の認証処理を行う。

(a)　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。

(b)　認証資格情報に関連して認証サーバ 1400 から受信したデータと 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，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。

(c)　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。

(d)　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する。

(e)　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。

(ii) ビジネスの紹介

米国カリフォルニア州を拠点とする Forescout Technologies 社は 2000 年に設立され，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。

図 11[6] に示す Advanced Threat Detection（ATD）は，本特許の一機能であり，様々な IoT デバイスからアクセスがあった場合，隔離された状態でのアクセスを許可し，コンプライアンステストを行う。

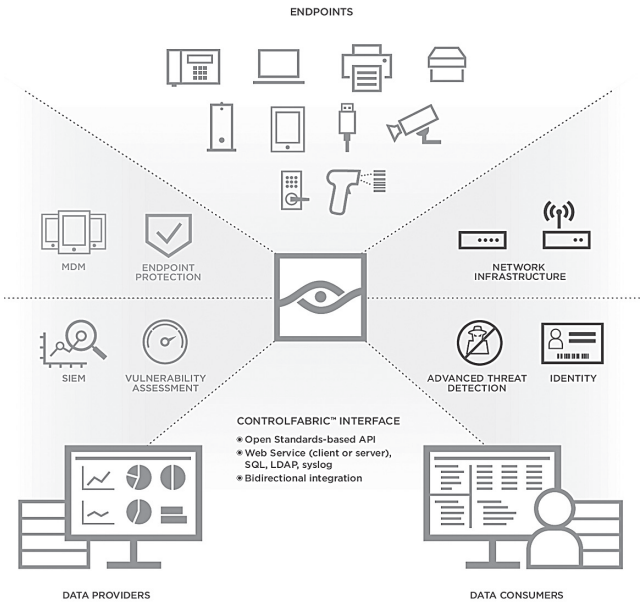

図 11　Advanced Threat Detection（ATD）の概要

4．IoT 特許の権利化と訴訟における査証制度の影響

（1）　侵害特定が容易なクレームの作成

ソフトウェア関連発明を専門とする弁理士であれば，できるだけ外部からの侵害特定が容易なクレームの作成を試みるであろう。侵害特定を容易にする方法としては一般的には以下の 2 つのアプローチがある。

1 つ目には，入力と出力とだけをクレームに記載することである。イ号製品の侵害確認に際しては振る舞いテストが行われる。すなわち，ある入力をイ号製品に対して行い，その際イ号製品から出力される結果を検証することで，プログラムのアルゴリズムに立ち入ることなく技術的範囲の属否判断を行うことができる。

2 つ目には，UI（User Interface）/UX（User Experience）をクレームに記載することである。製品・アプリがヒットするか否かの重要な要素の一つとして UI/UX が挙げられる。Apple 社の iPhone には分厚いマニュアルは同梱されていない。それでも優れた UI/UX のおかげで容易に操作方法を直感的に理解することができる。この UI/UX に関するアイデアをクレームに記載すれば，画面をみながら技術的範囲の属否判断を行うことができる。

（2） IoT セキュリティ発明のクレーム困難性

しかしながら，本稿で解説した各社の IoT セキュリティ特許は，クラウドまたは工場内サーバで処理される詳細なアルゴリズムまで記載せざるを得ないことが多く，単に入出力を記載するだけで特許を取得することができるケースは少ないであろう。

また，IoT デバイスに対するセキュリティ判断アルゴリズムに関する技術自体が UI/UX に関連することも少なく，また特許権者が立ち入ることができない他社工場内で表示処理が実行されるため，UI/UX に依拠したクレームも活用し難い。

（3） 米国での IoT 特許訴訟[7]

このように侵害特定が困難な IoT セキュリティ特許ではあるが，訴訟件数の多い米国では下記図 12 に示すとおり，IoT 特許訴訟の中でも一定の割合を占めている。これは米国特許訴訟においてはディスカバリ制度が採用されており，ディスカバリを通じて被告イ号製品の具体的なアルゴリズムを特定することができることも要因の一つであろう。

（4） 特許法改正に伴う査証制度の導入

IoT/AI の普及により，外部から侵害の特定が困難な状況が増加していることから平成 31 年特許法改正により査証制度が導入された（特許法第 105 条の 2）。

すなわち，図 13 に示すように裁判所が査証人を選定し，選定された査証人は侵害が疑われる施設へ立ち入り証拠収集を行った上で査証報告書を作成して裁判所に提出する。

本稿では上述した米国特許が日本でも同様に特許として成立しており，特許権者が，日本企業に対し特許訴訟を提起し，特許権者が査証の申立を裁判所に行った場合に，特許権者としてどのような主張が必要か，また被告日本企業としてはどのような対応，準備が必要であるか検討する。

(i) Indegy 特許訴訟における査証

特許事例として Indegy 社の下記クレームが，日本においても特許が成立しており，原告特許権者に特許

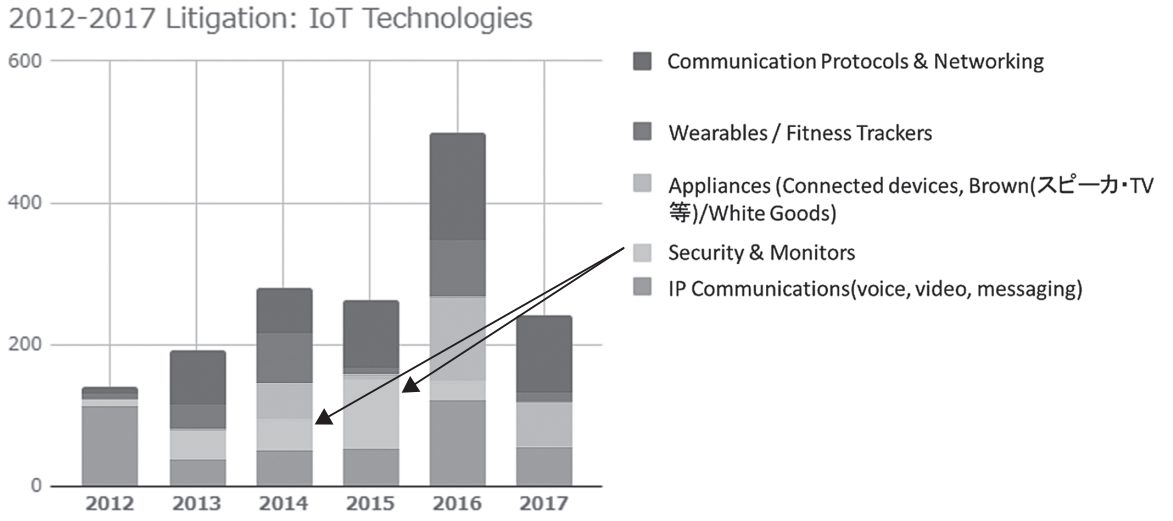

図 12　米国における IoT 技術に関する特許訴訟件数の推移

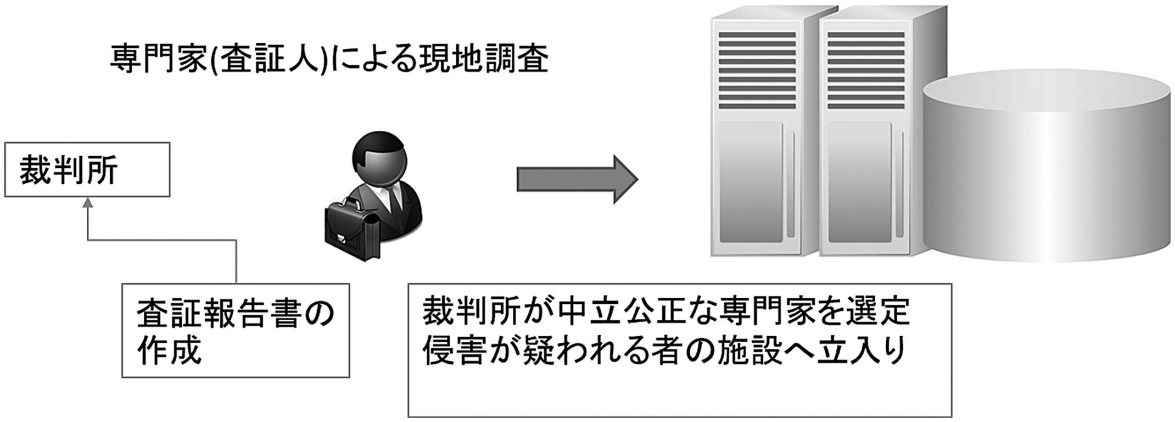

図 13　査証制度概要

権侵害で提訴された被告日本企業が，被告監視サーバを通じてクレームに記載された方法（被告方法）を使用しているものとして説明する。

1. 方法において，

コントローラーが１つ以上のフィールドデバイスを制御する産業用制御ネットワークに接続された管理アプライアンスにて，パッシブモニタリングプロセスとアクティブクエリプロセスとを並行して実行し，

前記パッシブモニタリングプロセスは，(i) 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し，(ii) インターセプトされたトラフィックが，コントローラーに送信され，コントローラがフィールドデバイスの制御に現在使用されているコードを更新することに基づく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確認し，(iii) トラフィックが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し，(iv) コード更新トランザクションが正当である場合，管理アプライアンスに保存されている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するためにコード更新トランザクションを使用し，

前記アクティブクエリプロセスは，(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，コントローラによって現在使用されているコードを報告するようにコントローラに要求し，(ii) コントローラによって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することを含み

(i) 前記アクティブクエリプロセスが，コントローラによって報告されたコードと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，前記パッシブモニタリングプロセスと前記アクティブクエリプロセスとの間で通知の発行を含むインタラクトを行う。

また被告方法を紹介する Web ページまた原告による調査によれば，被告方法は２つのプロセスが協同しながら並行して処理を実行しており，また第１のプロセスで検出されたベースラインバージョンと第２のプロセスおいて検出されたベースラインバージョンとの比較が行われることまでは把握できている。

しかしながら，図７に示したように被告方法の監視プログラムは被告サーバ（Management Appliance48 に相当）で実行されているため，原告特許権者は，被告の実施する方法が，クレームに記載された全ての構成要件を具備するか否か立証しきれていないものとする。特に第２のプロセスにおいてエミュレートすることにより取得したコードに基づきベースラインバージョンと比較しているか否かは原告は立証することができないものとする。

(ii) 査証の申立

このような場合，査証人にどのような証拠を確保してもらうべきかを事前検討する必要がある。本事例では，２つの監視プロセスが並行して行われることから，各プロセスのソフトウェア処理内容が把握できる証拠を押さえればよいことがわかる。具体的には，各プロセスのソースコード，本監視システムの仕様書，顧客マニュアル等を入手する必要がある。

申立書の記載内容については特許法第 105 条の２第２項に規定されており，各号において記載すべき事項を検討する。

(a) 特許権又は専用実施権を相手方が侵害したことを疑うに足りる相当な理由があると認められるべき事由（一号）

被告カタログ，原告側での侵害調査等に基づき，侵害の蓋然性が極めて高いことを示す理由を記載する。具体的には査証申立に関するクレームの構成要件以外の構成要件は全て被告方法が充足していることを主張する必要がある。また査証申立に関する構成要件についても，充足している可能性が高いことを示す理由を記載する方がよい。

(b) 査証の対象とすべき書類等を特定するに足りる事項及び書類等の所在地（二号）

上述した各プロセスのソースコード，本監視システムの仕様書，顧客マニュアルが査証の対象とすべき書類等となる。また，本事例では被告本社または被告製品が設置されたデータセンターが書類等の所在地となる。ここで問題となるのが，被告が外国企業の日本法人子会社であり，肝心のソースコード及び仕様書等が外国本社に存在する場合である。この場合，外国本社での査証は実行できないと考える。

(c)　立証されるべき事実及びこれと査証により得られる証拠との関係（三号）

ソースコード及び仕様書等の証拠により，被告方法が構成要件を充足することを記載する。

(d)　申立人が自ら又は他の手段によつては，前号に規定する証拠の収集を行うことができない理由（四号）

被告方法の行為は全て被告サーバ内で行われており，また被告方法の内容を規定するソースコードも開示されていないため，原告自身では収集することができないことを記載する。

(e)　第百五条の二の四第二項（装置の作動，計測，実験その他査証のために必要な措置）の裁判所の許可を受けようとする場合にあつては，当該許可に係る措置及びその必要性（五号）

検出したコードとベースラインバージョンとが一致しない場合の動作検証，コード更新トランザクション（ベースラインを更新するためのコードのトランザクション）が違法である場合の動作検証等が必要な措置に該当する。これらの動作検証を行うことで被告方法がクレームの構成要件を充足するか判断することができるからである。

(iii) 査証を受ける被告側の注意点

査証を受ける被告側の注意点は以下の通りである。

(a)　査証への協力と，立ち入りを拒んだ場合の効果

査証を受ける被告は，査証人及び執行官に対し，査証に必要な協力をしなければならない。査証を受ける被告が査証人の工場等への立入りの要求若しくは質問若しくは書類等の提示の要求又は装置の作動，計測，実験その他査証のために必要な措置として裁判所の許可を受けた措置の要求に対し，正当な理由なくこれらに応じないときは，裁判所は，立証されるべき事実に関する申立人の主張を真実と認めることができる（第105 の 2 の 5)。

このように被告が正当な理由なく査証に応じない場合，原告の主張が真実として認められてしまうペナルティを負う。

(b)　非開示要求

査証を受けた被告は，査証報告書の写しの送達を受けた日から二週間以内に，査証報告書の全部又は一部を申立人に開示しないことを申し立てることができる（第 105 条の 2 の 6)。被告側としては特許訴訟に関連のないソースコードの一部，仕様書の一部でありノウハウ的要素を含む事項等については開示しないことを 2 週間以内に申し立てる事が必要である。

(c)　証拠の保存（事前措置）

ソフトウェア機能の拡張，AI のハイパーパラメータの変更等，IoT システムは随時更新される。将来的に査証を受ける可能性があることに鑑み更新の度にソースコード，仕様の変更箇所，更新日時を記録しておくことが重要である。例えば IoT セキュリティシステムに関し，Ver1 と，Ver1 に機能を追加した Ver2 とが存在している場合に，Ver2 に対し特許権侵害訴訟を提起され損害賠償請求されたものとする。この際，査証を通じて Ver2 が侵害していることが明らかとなるが，いつの時点から Ver2 に切り替えたかが損害賠償額発生の起算日認定上重要となる。

ここで，Ver1 の仕様，及び，Ver2 に更新した日時を適切に記録していないと，Ver1 が非侵害であることを立証できず Ver1 についてまで損害賠償請求の対象となってしまう恐れがある。特にソフトウェアは有体物と異なりデジタルデータであり書き換え容易であるという特性を有する上に，頻繁にマイナーな修正・時に大規模なバージョンアップが行われるため，どの時点でどのようなソースコード・仕様であったのかを記録しておくことが重要である。

5．最後に

本稿では IoT セキュリティに関するスタートアップの技術を紹介するとともに，侵害立証困難性に鑑みた査証制度の活用について検討を加えた。モノからコトサービスへとビジネスモデルが変化していく中で IoT 技術に関する発明抽出，クレームドラフティング，及び，侵害立証の実務も今後変化していくであろう。本稿が IoT 関連発明を取り扱う実務者の参考となれば幸いである。

以上

(注)

(1) Insecam.orgHP より 2019 年 9 月 28 日 http://www.insecam.org/

(2) CyberX 社 HP より 2019 年 8 月 11 日 https://cyberx-labs.com/

(3) PatternEx 社 HP より 2019 年 8 月 14 日 https://www.patternex.com/product

(4) Argus Cyber Security社HPより2019 年 9 月 28 日 https://argus-sec.com/

(5) Security&LabHP より 2019 年 9 月 7 日 https://toyo-slc.com/indegy_sp/
(6) ForeScout ControlFabricTM Architecture カタログより 2019 年 9 月 7 日
(7) Unified PatentsHP より 2018 年 11 月 17 日 https://www.unifiedpatents.com/news/2018/3/28/internet-of-things-2017-litigation-update

（原稿受領 2019.9.28）