(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7071034号
(P7071034)

(45)発行日　令和4年5月18日(2022.5.18)

(24)登録日　令和4年5月10日(2022.5.10)

(51)国際特許分類			FI		
G06F	*21/55*	*(2013.01)*	G06F	21/55	
G05B	*23/02*	*(2006.01)*	G05B	23/02	G
F02C	*9/00*	*(2006.01)*	G05B	23/02	302Z
			F02C	9/00	B

請求項の数　7　外国語出願　（全30頁）

(21)出願番号　特願2017-226395(P2017-226395)
(22)出願日　平成29年11月27日(2017.11.27)
(65)公開番号　特開2018-139101(P2018-139101A)
(43)公開日　平成30年9月6日(2018.9.6)
審査請求日　令和2年11月17日(2020.11.17)
(31)優先権主張番号　15/371,905
(32)優先日　平成28年12月7日(2016.12.7)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　390041542
ゼネラル・エレクトリック・カンパニイ
アメリカ合衆国、ニューヨーク州　１２３４５、スケネクタデイ、リバーロード、１番
(74)代理人　100105588
弁理士　小倉 博
(74)代理人　100129779
弁理士　黒川 俊久
(74)代理人　100113974
弁理士　田中 拓人
(72)発明者　コーディー・ジョー・ブシェイ
アメリカ合衆国、ニューヨーク州・１２３０９、ニスカユナ、ワン・リサーチ・サークル

最終頁に続く

(54)【発明の名称】　産業資産制御システムにおける脅威検出のための特徴および境界の調整

(57)【特許請求の範囲】

【請求項１】

産業資産制御システムを保護するシステム（１００，３００，８００）であって、

複数の監視ノード（１３０）の各々について、前記産業資産制御システムの正常動作を表す経時的な一連の正常監視ノード値（１７０４）を格納する正常空間データソース（１１０）と、

前記複数の監視ノード（１３０）の各々について、前記産業資産制御システムの脅威を受けている動作を表す経時的な一連の脅威監視ノード値（１７０４）を格納する脅威空間データソース（１２０）と、

前記正常空間データソース（１１０）および前記脅威空間データソース（１２０）に結合された脅威検出モデル作成コンピュータ（１４０）であって、

（ｉ）前記一連の正常監視ノード値（１７０４）を受信し、一組の正常特徴ベクトル（５１２，１７０８）を生成し、

（ｉｉ）前記一連の脅威監視ノード値（１７０４）を受信し、一組の脅威特徴ベクトル（５１２，１７０８）を生成し、

（ｉｉｉ）前記一組の正常特徴ベクトル（５１２，１７０８）、前記一組の脅威特徴ベクトル（５１２，１７０８）、および少なくとも１つの初期アルゴリズムパラメータ（１５０４，１６０４）に基づいて、脅威検出モデル（１５５，１４１４）のための少なくとも１つの潜在的判定境界を自動的に計算し、

（ｉｖ）脅威検出の速度に関連付けられる性能メトリック（１５０６，１６０６）に基づ

いて前記少なくとも１つの潜在的判定境界の性能を自動的に評価し、
（ｖ）前記評価の結果に基づいて前記少なくとも１つの初期アルゴリズムパラメータ（１５０４，１６０４）を自動的に調整し、前記少なくとも１つの潜在的判定境界を再計算する、
脅威検出モデル作成コンピュータ（１４０）と
を含む、システム（１００，３００，８００）。
【請求項２】
前記自動的な評価、調整、および再計算は、最終調整アルゴリズムパラメータおよび最終判定境界が決定されるまで実行される、請求項１に記載のシステム（１００，３００，８００）。
【請求項３】
前記自動的な評価、調整、および再計算は、ローカル特徴ベクトル（５１２，１７０８）およびローカル判定境界に関連付けられ、
前記ローカル特徴ベクトル（５１２，１７０８）の抽出は、最小値、最大値、平均値、分散、整定時間、高速フーリエ変換スペクトル、極、浅い特徴、主成分解析、独立成分解析、ｋ－平均クラスタリング、スパース符号化、およびディープラーニングの特徴のうちの少なくとも１つに関連付けられる、請求項１または２に記載のシステム（１００，３００，８００）。
【請求項４】
複数のローカル特徴ベクトル（５１２，１７０８）およびローカル判定境界は、結合されてグローバル特徴ベクトル（８５０，１７１０）およびグローバル判定境界を形成し、前記自動的な評価、調整、および再計算は、前記グローバル特徴ベクトル（８５０，１７１０）および前記グローバル判定境界に関連付けられ、
前記グローバル特徴ベクトル（８５０，１７１０）および前記グローバル判定境界の少なくとも一方は、次元縮退、カーネル選択、いくつかのサポートベクトル、正常データ（３１０）に関連するコスト、および異常データに関連するコストに使用されるいくつかの重みに関連付けられる、請求項１乃至３のいずれかに記載のシステム（１００，３００，８００）。
【請求項５】
前記性能メトリック（１５０６，１６０６）は、受信者操作特性（「ＲＯＣ」）メトリックを含み、
前記ＲＯＣメトリックは、真陽性（１１１０）、真陰性（１１２０）、偽陽性（１１３０）、偽陰性（１１４０）、曲線下面積、ＲＯＣ精度、陽性予測値、偽発見率、偽省略率、陰性予測値、有病率、真陽性率、偽陽性率、陽性尤度比、陰性尤度比、偽陰性率、真陰性率、および診断オッズ比のうちの少なくとも１つに関連付けられる、請求項１乃至４のいずれかに記載のシステム（１００，３００，８００）。
【請求項６】
前記アルゴリズムパラメータは、一組の潜在的アルゴリズムパラメータから自動的に選択され、特徴（１７０６）のタイプ、いくつかのローカル特徴、いくつかのグローバル特徴、次元縮退の方法、主成分解析、主成分回帰、フィッシャーディスクリミネータ解析、サポートベクトルマシン、境界構築方法、境界方法特定調整器、カーネル機能、ボックス制約、コスト、および入力バッチサイズのうちの少なくとも１つに関連付けられる、請求項１乃至５のいずれかに記載のシステム（１００，３００，８００）。
【請求項７】
前記産業資産制御システムの現在の動作を表す、経時的な監視ノード信号値のストリームを受信するための複数のリアルタイム監視ノード信号入力と、
前記複数のリアルタイム監視ノード信号入力および前記脅威検出モデル作成コンピュータ（１４０）に結合された脅威検出コンピュータプラットフォームであって、
（ｉ）監視ノード信号値の前記ストリームを受信し、
（ｉｉ）監視ノード信号値の各ストリームについて、現在の監視ノード特徴ベクトル（５

１２，１７０８）を生成し、
（ｉｉｉ）各監視ノード（１３０）について適切な判定境界を選択し、前記適切な判定境界は、前記現在の協調モードにおいてその監視ノード（１３０）の異常状態から正常状態を分離し、
（ｉｖ）各生成された現在の監視ノード特徴ベクトル（５１２，１７０８）を前記選択された対応する適切な判定境界と比較し、
（ｖ）前記比較の結果に基づいて脅威警報信号を自動的に送信する、
脅威検出コンピュータプラットフォームと
をさらに含む、請求項１乃至６のいずれかに記載のシステム（１００，３００，８００）。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、産業資産制御システムにおける脅威検出のための特徴および境界の調整に関する。
【背景技術】
【０００２】
物理的システム（例えば、動力タービン、ジェットエンジン、機関車、自律車両など）を操作する産業資産制御システムは、インターネットに接続されることが多くなっている。その結果、これらの制御システムは、電力の発生と分布を妨げたり、エンジンを損傷したり、車両の誤動作を招くなどの可能性のあるサイバー攻撃（例えば、コンピュータウイルス、悪意のあるソフトウェアなど）などの脅威に対して脆弱であり得る。現在の方法は、主に、情報技術（「ＩＴ」、例えば、データを格納、検索、送信、操作するコンピュータ）および操作技術（「ＯＴ」、例えば直接監視装置および通信バスインターフェース）における脅威検出を考慮する。サイバー脅威は、Ｓｔｕｘｎｅｔ攻撃を受けた２０１０年に見られるように、これらの保護レイヤーに侵入し、物理的な「ドメイン」に到達する可能性がある。そのような攻撃は、制御システムのパフォーマンスを低下させ、プラントの総停止または破局的な損傷さえも引き起こすおそれがある。現在、ＦＤＩＡ（Ｆａｕｌｔ Ｄｅｔｅｃｔｉｏｎ Ｉｓｏｌａｔｉｏｎ ａｎｄ Ａｃｃｏｍｍｏｄａｔｉｏｎ）アプローチはセンサデータを解析するだけであるが、他のタイプの脅威監視ノードと関連して脅威が発生する可能性がある。また、ＦＤＩＡは、一度に１つのセンサにおいて自然に発生する障害にのみ限定されることに留意されたい。ＦＤＩＡシステムは、悪意のある攻撃の場合のように同時に発生する複数の障害には対処しない。さらに、脅威検出システムの性能を測定するいくつかの方法がある（例えば、脅威が存在しない場合の誤警報、脅威が実際に存在する場合の警報作成の失敗、脅威検出の迅速さなど）。結果として、適切な脅威検出システムの作成が困難になることがあり、特に、かなりの数の異なるタイプの監視ノードが評価され、様々な性能メトリックを考慮する必要がある場合にはそうである。したがって、産業資産制御システムをサイバー脅威から自動的かつ正確に保護するための適切な脅威検出システムの作成を容易にすることが望ましい。
【先行技術文献】
【特許文献】
【０００３】
【文献】米国特許第９４０５９００号明細書
【発明の概要】
【０００４】
いくつかの実施形態によれば、脅威検出モデル作成コンピュータは、一連の正常監視ノード値（産業資産制御システムの正常動作を表す）を受信し、一組の正常特徴ベクトルを生成することができる。脅威検出モデル作成コンピュータはまた、一連の脅威監視ノード値（産業資産制御システムの脅威を受けている動作を表す）を受信し、一組の脅威特徴ベクトルを生成することもできる。脅威検出モデルのための少なくとも１つの潜在的判定境界は、一組の正常特徴ベクトル、一組の脅威特徴ベクトル、および少なくとも１つの初期ア

ルゴリズムパラメータに基づいて計算されてもよい。少なくとも１つの潜在的判定境界の性能は、性能メトリックに基づいて評価されてもよい。次に、少なくとも１つの初期アルゴリズムパラメータは、評価の結果に基づいて調整されてもよく、少なくとも１つの潜在的判定境界は再計算されてもよい。

【０００５】

いくつかの実施形態は、一連の正常監視ノード値を受信し、一組の正常特徴ベクトルを生成する手段であって、経時的な一連の正常監視ノード値は、産業資産制御システムの正常動作を表す、手段と、一連の脅威監視ノード値を受信し、一組の脅威特徴ベクトルを生成する手段であって、経時的な一連の脅威監視ノード値は、産業資産制御システムの脅威を受けている動作を表す、手段と、一組の正常特徴ベクトル、一組の脅威特徴ベクトル、および少なくとも１つの初期アルゴリズムパラメータに基づいて、脅威検出モデルのための少なくとも１つの潜在的判定境界を計算する手段と、性能メトリックに基づいて少なくとも１つの潜在的判定境界の性能を評価する手段と、評価の結果に基づいて少なくとも１つの初期アルゴリズムパラメータを調整し、少なくとも１つの潜在的判定境界を再計算する手段と、を含む。

【０００６】

本明細書に開示するいくつかの実施形態のいくつかの技術的利点は、産業資産制御システムをサイバー脅威から自動的かつ正確に保護するための適切な脅威検出システムの作成を容易にする改良されたシステムおよび方法である。

【図面の簡単な説明】

【０００７】

【図１】いくつかの実施形態により提供することができるシステムの高レベルブロック図である。

【図２】いくつかの実施形態による方法を示す図である。

【図３】いくつかの実施形態による脅威警報システムを示す図である。

【図４】いくつかの実施形態による様々な監視ノードパラメータの境界および特徴ベクトルを示す図である。

【図５】いくつかの実施形態による様々な監視ノードパラメータの境界および特徴ベクトルを示す図である。

【図６】いくつかの実施形態による様々な監視ノードパラメータの境界および特徴ベクトルを示す図である。

【図７】いくつかの実施形態によるサイバー攻撃検出システムのブロック図である。

【図８】いくつかの実施形態によるグローバル脅威保護システムの一例を示す図である。

【図９】いくつかの実施形態による三次元のセンサ出力を示す図である。

【図１０】いくつかの実施形態による脅威検出のための特徴および境界調整の方法を示す図である。

【図１１】いくつかの実施形態による受信者操作曲線測定を示す図である。

【図１２】いくつかの実施形態による最適化フローチャートを示す図である。

【図１３】いくつかの実施形態によるディスプレイを示す図である。

【図１４】本発明のいくつかの実施形態による産業資産制御システム保護プラットフォームのブロック図である。

【図１５】いくつかの実施形態によるローカルデータベースのテーブル部分を示す図である。

【図１６】いくつかの実施形態によるグローバルデータベースのテーブル部分を示す図である。

【図１７】いくつかの実施形態による監視ノードデータベースのテーブル部分を示す図である。

【発明を実施するための形態】

【０００８】

以下の詳細な説明では、実施形態の完全な理解を提供するために、多数の特定の詳細が述

べられる。しかしながら、これらの具体的な詳細なしで実施形態を実施できることは、当業者には理解されるであろう。他の例では、周知の方法、手順、構成要素、および回路は、実施形態を不明瞭にしないように詳細には記載していない。

【０００９】

物理システムを操作する産業制御システムは、インターネットに接続されることが多くなっている。その結果、これらの制御システムは、脅威に対して脆弱になる可能性があり、場合によっては、複数の攻撃が同時に発生するおそれがある。ＦＤＩＡアプローチなどの産業制御システムを保護する既存のアプローチでは、これらの脅威に適切に対処できない場合があり、特に、かなりの数の異なるタイプの監視ノードが評価され、様々な性能メトリックを考慮する必要がある場合にはそうである。したがって、産業資産制御システムをサイバー脅威から自動的かつ正確に保護するための適切な脅威検出システムの作成を容易にすることが望ましい。図１は、いくつかの実施形態によるシステム１００の高レベルアーキテクチャである。システム１００は、「正常空間」データソース１１０および「脅威空間」データソース１２０を含むことができる。正常空間データソース１１０は、複数の「監視ノード」１３０のそれぞれに対して、（例えばモデルによって生成された、または、図１に破線で示すように実際の監視ノード１３０のデータから収集された）産業資産制御システムの正常動作を表す一連の正常値を経時的に格納することができる。本明細書で使用されるように、「監視ノード」という語句は、例えば、センサデータ、アクチュエータ、モータ、ポンプ、および補助機器に送信される信号、補助機器に送信される信号ではなく直接センサ信号ではない中間パラメータ、および／または制御論理を意味することができる。これらは、例えば、脅威監視システムからのデータを連続的な信号またはデータストリームまたはそれらの組み合わせの形で連続的に受信する脅威監視ノードを表すことができる。さらに、それらのノードは、サイバー脅威または異常事象の発生を監視するために使用されてもよい。このデータパスは、暗号化または他の保護メカニズムで特に指定されるので、情報を保護することができ、サイバー攻撃によって改ざんされることはない。脅威空間データソース１２０は、監視ノード１３０のそれぞれに対して、（例えば、システムがサイバー攻撃を受けている場合に）産業資産制御システムの脅威を受けている動作を表す一連の脅威値を格納することができる。

【００１０】

正常空間データソース１１０および脅威空間データソース１２０からの情報は、このデータを使用して判定境界（すなわち、正常挙動と脅威挙動とを分離する境界）を生成する脅威検出モデル作成コンピュータ１４０に提供することができる。その場合、判定境界は、脅威検出モデル１５５を実行する脅威検出コンピュータ１５０によって使用することができる。脅威検出モデル１５５は、例えば、センサノード、アクチュエータノード、および／または任意の他の重要な監視ノード（例えば、監視ノードMN_1～MN_N）からのデータを含む監視ノード１３０からのデータストリームを監視し、受信したデータに基づいて各監視ノードについて「特徴」を計算し、適切な場合に（例えば、ユーザへの表示のために）、１つまたは複数の遠隔監視装置１７０に脅威警報信号を「自動的に」出力することができる。いくつかの実施形態によれば、脅威警報信号は、ユニットコントローラ、プラントヒューマンマシンインターフェース（「ＨＭＩ」）、またはいくつかの異なる送信方法により顧客に送信することができる。脅威警報信号の１つの受信者は、幅広いプラント資産に対する複数の攻撃を相関させるクラウドデータベースである可能性があることに留意されたい。本明細書で使用する「特徴」という用語は、例えば、データの数学的特徴付けを意味することができる。データに適用される特徴の例としては、最大値および最小値、平均値、標準偏差、分散、整定時間、高速フーリエ変換（「ＦＦＴ」）スペクトル成分、線形および非線形主成分、独立成分、スパース符号化、ディープラーニングなどを挙げることができる。さらに、「自動的に」という用語は、例えば、人の介入をほとんどまたは全く伴わずに行うことができる動作を意味することができる。いくつかの実施形態によれば、検出された脅威に関する情報は、産業制御システムに送り返すことができる。

【００１１】

本明細書で使用されるように、システム１００および本明細書に記載された他の任意のデバイスに関連するデバイスを含むデバイスは、ローカルエリアネットワーク（「ＬＡＮ」）、メトロポリタンエリアネットワーク（「ＭＡＮ」）、ワイドエリアネットワーク（「ＷＡＮ」）、専用ネットワーク、公衆交換電話網（「ＰＳＴＮ」）、無線アプリケーションプロトコル（「ＷＡＰ」）ネットワーク、ブルートゥース（登録商標）ネットワーク、無線ＬＡＮネットワーク、および／またはインターネット、イントラネット、もしくはエクストラネットなどのインターネットプロトコル（「ＩＰ」）ネットワークの１つまたは複数とすることができる任意の通信ネットワークを介して情報を交換することができる。本明細書で説明する任意のデバイスは、１つまたは複数のそのような通信ネットワークを介して通信することができることに留意されたい

脅威検出モデル作成コンピュータ１４０は、正常空間データソース１１０および／または脅威空間データソース１２０などの、様々なデータストアに情報を格納し、および／または様々なデータストアから情報を検索することができる。様々なデータソースは、脅威検出モデル作成コンピュータ１４０（例えば、オフラインまたはオンライン学習に関連してもよい）からローカルに格納されてもよいし、遠隔地に存在してもよい。単一の脅威検出モデル作成コンピュータ１４０が図１に示されているが、任意の数のそのようなデバイスを含めることができる。さらに、本明細書に記載された様々なデバイスは、本発明の実施形態に従って組み合わせることができる。例えば、いくつかの実施形態では、脅威検出モデル作成コンピュータ１４０および１つまたは複数のデータソース１１０、１２０は、単一の装置を含むことができる。脅威検出モデル作成コンピュータ１４０の機能は、分散処理またはクラウドベースのアーキテクチャにおいて、ネットワーク化された装置の組み合わせによって実行することができる。

【００１２】

ユーザは、本明細書に記載された実施形態のいずれかに従って脅威情報に関する情報を閲覧および／または管理するために、監視装置１７０（例えば、パーソナルコンピュータ（「ＰＣ」）、タブレット、またはスマートフォン）の１つを介してシステム１００にアクセスすることができる。場合によっては、インタラクティブなグラフィカル・ディスプレイ・インターフェースにより、ユーザが特定のパラメータ（例えば、脅威検出トリガレベル）を定義および／または調整すること、ならびに／もしくは脅威検出モデル作成コンピュータ１４０および／または脅威検出コンピュータ１５０から自動的に生成された勧告または結果を提供または受信することができる。

【００１３】

例えば、図２は、図１に関して記載されたシステム１００の要素のいくつかまたは全てによって実行することができる方法を示す。本明細書で説明するフローチャートは、ステップの順序を固定することを意味するものではなく、本発明の実施形態は、実行可能な任意の順序で実施することができる。本明細書で説明する方法のいずれかは、ハードウェア、ソフトウェア、またはこれらの手法の任意の組み合わせによって実行することができることに留意されたい。例えば、コンピュータ可読記憶媒体は、機械によって実行された場合、本明細書に記載の実施形態のいずれかによるパフォーマンスをもたらす命令を格納することができる。

【００１４】

Ｓ２１０において、複数のリアルタイム監視ノード信号入力は、産業資産制御システムの現在の動作を表す経時的な監視ノード信号値のストリームを受信することができる。少なくとも１つの監視ノード（例えば、コントローラノードなど）は、例えば、センサデータ、補助機器入力信号、制御中間パラメータ、および／または制御論理値と関連付けられてもよい。

【００１５】

Ｓ２２０において、脅威検出コンピュータプラットフォームは、監視ノード信号値のストリームを受信し、監視ノード信号値の各ストリームについて、現在の監視ノード特徴ベクトルを生成することができる。いくつかの実施形態によれば、現在の監視ノード特徴ベク

トルの少なくとも１つは、主成分、統計的特徴、ディープラーニング特徴、周波数領域特徴、時系列解析特徴、論理的特徴、地理的または位置に基づく場所、および／または相互作用特徴に関連付けられる。

【００１６】

Ｓ２３０において、各生成された現在の監視ノード特徴ベクトルは、その監視ノードの対応する判定境界（例えば、線形境界、非線形境界、多次元境界など）と比較され、判定境界はその監視ノードの異常状態から正常状態を分離することができる。いくつかの実施形態によれば、少なくとも１つの監視ノードが複数の多次元判定境界に関連付けられ、Ｓ２３０での比較がそれらの境界のそれぞれに関連して実行される。判定境界は、例えば、特徴ベースの学習アルゴリズムおよび高忠実度モデル、あるいは産業資産制御システムの正常動作に従って生成されてもよいことに留意されたい。さらに、少なくとも１つの判定境界が多次元空間に存在し、動的モデル、完全な要因設計、田口スクリーニング設計、中央合成手法、Ｂｏｘ－Ｂｅｈｎｋｅｎ手法、現実の動作条件手法などの実験の設計から生成されたデータと関連付けることができる。さらに、判定境界に関連する脅威検出モデルは、いくつかの実施形態によれば、過渡条件、産業資産制御システムの定常状態モデル、および／または着信データストリームからの自己学習システムにおけるように、システムを動作させている間に取得されたデータセットに基づいて動的に適応させることができる。

【００１７】

Ｓ２４０において、システムは、Ｓ２３０で実行された比較の結果に基づいて脅威警報信号（例えば、通知メッセージなど）を自動的に送信することができる。この脅威は、例えば、アクチュエータ攻撃、コントローラ攻撃、監視ノード攻撃、プラント状態攻撃、なりすまし、金融損害、ユニット利用可能性、ユニットトリップ、ユニット寿命の喪失、および／または少なくとも１つの新しい部品を必要とする資産損害に関連付けることができる。いくつかの実施形態によれば、脅威警報信号が送信されると、１つまたは複数の応答動作を実行することができる。例えば、システムは、（例えば、検出された潜在的なサイバー攻撃をさらに調査させるために）産業資産制御システムの全部または一部を自動的に停止することができる。他の例として、１つまたは複数のパラメータを自動的に変更してもよく、ソフトウェアアプリケーションを自動的にトリガして、データを捕捉してもよく、および／または潜在的な原因などを分離してもよい。脅威警報信号は、ＰＲＥＤＩＸ（商標）フィールドエージェントシステムなどのクラウドベースのシステムを介して送信されてもよいことに留意されたい。いくつかの実施形態によれば、情報をアーカイブし、および／または境界に関する情報を格納するために、クラウドアプローチを使用することもできることに留意されたい。

【００１８】

いくつかの実施形態によれば、システムは、脅威の起点を特定の監視ノードにさらにローカライズすることができる。例えば、１つの監視ノードに関連する判定境界が、別の監視ノードに関連する判定境界が交差した時間と比較して交差した時間に従って、ローカライズを行うことができる。いくつかの実施形態によれば、特定の監視ノードの表示が脅威警報信号に含まれてもよい。

【００１９】

本明細書で説明するいくつかの実施形態は、システムに対する１つまたは複数の同時の敵対的脅威を検出するために、調整された高忠実度機器モデルおよび／または実際の「オンザジョブ」データから先験的に学習することによって、制御システムの物理特性を利用することができる。さらに、いくつかの実施形態によれば、全ての監視ノードデータは、高度な特徴ベースの方法を使用して特徴に変換することができ、制御システムのリアルタイム動作は、実質的にリアルタイムで監視することができる。異常は、監視されたデータを「正常」または障害（もしくは、劣化）として分類することによって検出することができる。この判定境界は、動的モデルを使用して構築することができ、オペレータが制御システムを直ちに正常動作に戻すことを可能にする脆弱性の早期検出（および壊滅的な障害の潜在的回避）を可能にする補助をすることができる。

【００２０】
自動的に（例えば、アルゴリズムを介して）抽出され、および／または手動で入力することができる多次元特徴ベクトルの適切な組は、低次元ベクトル空間における測定データの良好な予測子を含むことができることに留意されたい。いくつかの実施形態によれば、ＤｏＥ技術に関連する科学的原理を介して得られるデータセットを使用して、多次元空間に適切な判定境界を構築することができる。さらに、複数のアルゴリズム方法（例えば、サポートベクトルマシンまたはマシンラーニング技術）を使用して、判定境界を生成することができる。境界は測定データ（または、高忠実度モデルから生成されたデータ）によって駆動することができるので、定義された境界マージンは、多次元特徴空間に脅威ゾーンを作成するのに役立つことができる。さらに、マージンは、本質的に動的であり、機器の過渡状態または定常状態モデルに基づいて適合され、および／または入力データストリームから自己学習システムのようにシステムを動作させながら得ることができる。いくつかの実施形態によれば、トレーニング方法は、判定境界を教えるための教師付きの学習のために使用されてもよい。このタイプの教師付きの学習は、システム動作（例えば、正常動作と異常動作との間の相違）に関するオペレータの知識を考慮に入れることができる。
【００２１】
主成分（自然基底集合を用いて構築された重み）および統計的特徴（例えば、時系列信号の平均、分散、歪度、尖度、最大値、最小値、最大値および最小値の位置、独立成分など）を含む、本明細書に記載された実施形態のいずれかに従って多くの異なるタイプの特徴を利用できることに留意されたい。他の例には、深層学習特徴（例えば、実験的および／または履歴的データセットを採掘することによって生成される）および周波数領域特徴（例えば、フーリエ変換またはウェーブレット変換の係数に関連する）が含まれる。また、実施形態は、相互相関、自己相関、自己回帰の順序、移動平均モデル、モデルのパラメータ、信号の微分および積分、立ち上がり時間、整定時間、ニューラルネットワークなどの時系列解析特徴に関連付けることができる。さらに、他の例には、論理的な特徴（「はい」および「いいえ」などの意味論的抽象化を含む）、地理的／位置的場所、および相互作用特徴（複数の監視ノードおよび特定の場所からの信号の数学的組み合わせ）が含まれる。実施形態は、任意の数の特徴を組み込むことができ、システムが物理的処理および脅威についてより多くを学習するにつれて、手法がより正確になることを可能にするより多くの特徴を含むことができる。いくつかの実施形態によれば、監視ノードからの異なる値は、単位のない空間に対して正規化され、出力と出力の強度とを簡単な方法で比較することを可能にすることができる。
【００２２】
したがって、いくつかの実施形態は、例えばキーガスタービン制御センサに対するサイバー攻撃を検出する高度な異常検出アルゴリズムを提供することができる。アルゴリズムは、監視ノード特有の判定境界を使用してどの信号が攻撃されているかを特定し、制御システムに適応する動作をとるように通知することができる。特に、検出および位置特定アルゴリズムは、センサ、補助機器入力信号、制御中間パラメータ、または制御論理が正常状態または異常状態にあるかどうかを検出することができる。解析され得るガスタービン監視ノードのいくつかの例には、臨界制御センサ（例えば、発電機出力変換器信号、ガスタービン排気温度熱電対信号、ガスタービン速度信号など）、制御システムの中間パラメータ（例えば、発電機出力、ガスタービン排気温度、圧縮機吐出圧力、圧縮機吐出温度、圧縮機圧力比、燃料流量、圧縮機入口温度、ガイドベーン角、燃料ストローク基準、圧縮機抽気バルブ、入口抽気熱バルブなど）、補助機器の入力信号（例えば、アクチュエータ、モータ、ポンプなどに送られる信号）、および／またはコントローラへの論理コマンドが含まれる。
【００２３】
アルゴリズムのいくつかの実施形態は、高い忠実度の物理モデルおよび／または（アルゴリズムを任意のシステムに配備することを可能にする）機械操作データに基づく特徴ベースの学習技術を使用して、高次元の判定境界を確立することができる。その結果、複数の

信号を使用してより正確に検出が行われ、偽陽性の少ない正確な検出を行うことができる。さらに、実施形態は、監視ノードデータに対する複数の攻撃を検出し、根本原因攻撃が起きた場所を合理的に説明することができる。例えば、アルゴリズムは、以前の信号攻撃のために信号が異常であるかどうか、またはそれが代わりに独立して攻撃されているかどうかを判定することができる。これは、例えば、特徴の進化を監視することによって、および攻撃間の時間遅延を考慮することによって達成することができる。

【００２４】

サイバー攻撃検出および位置特定アルゴリズムは、リアルタイムのタービン信号データストリームを処理し、次にセンサ特有の判定境界と比較することができる特徴（複数の識別子）を計算することができる。いくつかの実施形態によるセンサ特有のガスタービンサイバー攻撃検出および位置特定アルゴリズムを利用するシステム３００のブロック図が図３に示されている。特に、発電プラント３３２は、電子機器およびプロセッサを備えたコントローラ３３６がアクチュエータ３３８を調整するのを助ける情報をセンサ３３４に提供する。脅威検出システム３６０は、正常データ３１０および／または脅威データ３２０を生成するために、発電プラント３３２に関連する１つまたは複数の高忠実度物理に基づくモデル３４２を含むことができる。正常データ３１０および脅威データ３２０は、特徴発見コンポーネント３４４によってアクセスされ、オフライン（例えば、必ずしも発電プラント３３２が動作している間ではない）の間に判定境界アルゴリズム３４６によって処理され得る。判定境界アルゴリズム３４６は、様々な監視ノードの判定境界を含む脅威モデルを生成することができる。各判定境界は、各監視ノード信号（例えば、センサ３３４、コントローラ３３６、および／またはアクチュエータ３３８からの）に対して正常データ３１０と脅威データ３２０を用いたサポートベクトルマシンなどの、バイナリ分類アルゴリズムを実行することによって構築された高次元空間内の２つのデータセットを分離することができる。

【００２５】

リアルタイム脅威検出プラットフォーム３５０は、監視ノードからのデータストリームと共に境界を受信することができる。プラットフォーム３５０は、各監視ノード要素３５２上の特徴抽出と、センサ特有の判定境界を使用して個々の信号内の攻撃を検出し、複数の信号に対する攻撃を合理的に説明し、どの信号が攻撃されたか、および位置特定モジュール３５６を介したシステムに対する以前の攻撃のためにどれが異常になったかを宣言するアルゴリズムを有する正常判定３５４と、を含むことができる。収容要素３５８は、異常判定表示（例えば、脅威警報信号）、コントローラ動作、および／または取り付けられた監視ノードのリストなどの出力３７０を生成することができる。

【００２６】

リアルタイム検出の間、監視ノードデータの連続バッチがプラットフォーム３５０によって処理され、正規化され、特徴ベクトルが抽出されてもよい。次に、高次元の特徴空間における各信号のベクトルの位置を、対応する判定境界と比較することができる。それが攻撃領域内にある場合には、サイバー攻撃が宣言され得る。アルゴリズムは、攻撃が最初に発生した場所を決定することができる。攻撃は、時にはアクチュエータ３３８上にあってもよく、センサ３３４のデータに現れてもよい。攻撃がセンサ、コントローラ、またはアクチュエータ（例えば、監視ノードのどの部分を示すか）のいずれかに関連しているかどうかを分離するために、攻撃判定が後判定モジュール（例えば、位置特定要素３５６）において実行されてもよい。これは、判定境界に関する特徴ベクトルの位置を経時的に個別に監視することによって行うことができる。例えば、センサ３３４が偽装されている場合、攻撃されたセンサ特徴ベクトルは、図４から図６に関して説明したように、残りのベクトルより早く判定境界を横切る。センサが異常であると宣言され、補助機器への負荷コマンドが異常であると後で判定された場合には、信号偽装などの元の攻撃がセンサ３３４上で発生したと判定することができる。逆に、補助機器への信号が異常であると最初に判定され、その後センサ３３４のフィードバック信号に現れた場合には、機器への信号が最初に攻撃されたと判定することができる。

【００２７】
いくつかの実施形態によれば、局在化された判定境界の使用および特定の信号特徴のリアルタイム計算を介して信号が正常動作空間（または異常空間）にあるか否かを検出することができる。さらに、アルゴリズムは、攻撃されているセンサと、攻撃されている補助機器への信号とを区別することができる。制御中間パラメータおよび制御論理も同様の方法を用いて解析することができる。アルゴリズムは、異常になる信号を合理的に説明することができることに留意されたい。その後に、信号に対する攻撃を特定することができる。
【００２８】
図４は、いくつかの実施形態による、様々な監視ノードパラメータに対する境界および特徴ベクトルを示す４００。特に、各パラメータについて、グラフは、値の重み１（「ｗ１」）、すなわち特徴１を表す第１の軸、および値の重み２（「ｗ２」）、すなわち特徴２を表す第２の軸を含む。ｗ１およびｗ２の値は、例えば、入力データに対して実行される主成分解析（ＰＣＡ）からの出力と関連付けられてもよい。ＰＣＡは、データを特徴付けるアルゴリズムによって使用され得る機能の１つであってもよいが、他の特徴を活用してもよい。
【００２９】
圧縮機吐出温度４１０、圧縮機圧力比４２０、圧縮機入口温度４３０、燃料流量４４０、発電機出力４５０、およびガスタービン排気温度４６０のグラフが提供される。各グラフは、各監視ノードパラメータについて、ハード境界４１２（実線の曲線）、最小境界４１６（点線の曲線）、および最大境界４１４（破線の曲線）、ならびに現在の特徴位置に関連する表示（グラフ上に「Ｘ」で示されている）を含む。図４に示すように、現在の監視ノード位置は、最小境界と最大境界との間にある（すなわち、「Ｘ」は点線と破線の間にある）。結果として、システムは、産業資産制御システムの動作が正常である（システムが現在攻撃中であることを示す脅威が検出されていない）と判断することができる。
【００３０】
図５は、これらのパラメータについて、その後の境界および特徴ベクトルを示す５００。例えば、圧縮機吐出圧力に対する特徴ベクトルの移動５１２を考える。特徴ベクトル５１２が移動したとしても、それは依然として最大および最小境界内にあり、その結果、その監視ノードの正常動作であると判定することができる。これは、図５の最初の５つのグラフの場合である。この例では、ガスタービン排気温度の特徴ベクトルの移動５６２が最大境界を超えており、その結果、その監視ノードの異常動作が判定される可能性がある。例えば、修正値である排気温度スケールファクタについての脅威が存在する可能性がある。その結果、図５に示す中間監視ノード信号の特徴ベクトルに対する特徴は、それが異常であるように移動する（符号５６２）。このアルゴリズムはこのサイバー攻撃を検出し、２つの並行動作を開始することができる。１つの動作は、何が攻撃されたかを発見するための信号の後処理であってもよく、この場合、システムが各排気熱電対を監視していれば、いずれも現在異常ではないと結論付けることができる。したがって、この特徴を計算するために使用されたものが攻撃されたと判定することができる。もう１つの動作は、さらなる攻撃を継続的に監視して検出することである。そのようなアプローチは、複数の信号攻撃の検出を容易にすることができる。
【００３１】
図５の例が与えられると、ガスタービン排気温度信号が攻撃されたと仮定する。これにより、システムは他の信号を異常な状態にするように応答する可能性がある。これは、攻撃が既に検出されており、他の信号が異常であることが示されている図６に示されている６００。特に、圧縮機吐出圧力６１２、圧縮機圧力比６２２、圧縮機入口温度６３２、および燃料流量６４２の特徴移動は全て異常になる（ガスタービン排気温度６６２の特徴ベクトルに加わる）。発電機出力の特徴ベクトルは異常にならないことに留意されたい。これらの信号６１２、６２２、６３２、６４２が本当に現在攻撃を受けているか否かを判定するために、関連する特徴ベクトル情報を有する履歴バッチを、ある程度の時間持続させることができる。次に、別の信号で攻撃が検出されると、このバッチが検査され、ガスター

ビン排気温度およびいくつかの後続の要素に対する確認された攻撃の時間が解析される。
【００３２】
１つの信号の合理化は、システムの時間遅延に関連する可能性があることに留意されたい。つまり、センサが攻撃された後に、システムが定常状態に戻るまでの期間があり得る。この遅延の後に、異常になる信号は、システムが応答するのとは対照的に、攻撃によるものである可能性がある。
【００３３】
監視ノードにおける異常状態を検出する現在の方法は、ＦＤＩＡ（それ自体は非常に限定されている）に限定されている。本明細書に記載されているサイバー攻撃検出および位置特定アルゴリズムは、センサの異常信号を検出することができるだけでなく、補助機器に送信された信号、制御中間パラメータおよび／または制御論理を検出することもできる。このアルゴリズムは、複数の信号攻撃を理解することもできる。サイバー攻撃の脅威を正しく識別する１つの課題は、複数のセンサがマルウェアの影響を受けて発生する可能性があることである。いくつかの実施形態によれば、アルゴリズムは、攻撃が発生したこと、どのセンサに影響を与えたかをリアルタイムで識別して、障害応答を宣言することができる。このような結果を得るためには、システムの詳細な物理的応答を知って、許容可能な判定境界を作成する必要がある。これは、例えば、忠実度の高いモデルで実験設計（「ＤｏＥ」）の実験を実行して、正常領域と異常領域のデータセットを構築することで実現することができる。各センサのデータセットは、所与の脅威値（例えば、タービン速度、熱電対スケールファクタなど）に対する特徴ベクトルを含むことができる。完全な要因、田口スクリーニング、中央合成、Ｂｏｘ－Ｂｅｈｎｋｅｎは、攻撃空間の作成に使用される既知の設計手法の一部である。モデルが利用できない場合、これらのＤｏＥ方法は実世界の発電システムからデータを収集するためにも使用される。実験は、同時攻撃の種々の組み合わせで実行することができる。いくつかの実施形態では、システムは、サイバー攻撃とは対照的に、劣化／欠陥動作を検出することができる。そのような判定は、劣化／欠陥動作空間に関連するデータセットを利用することができる。このプロセスの最後に、システムは、判定境界を構築する際に使用するために、「攻撃ｖ／ｓ正常」および「劣化ｖ／ｓ正常」などのデータセットを作成することができる。さらに、特徴空間内のデータセットを使用して各信号について判定境界を作成することができることに留意されたい。様々な分類方法を用いて判定境界を計算することができる。例えば、バイナリ線形および非線形監視分類器は、判定境界を得るために使用できる方法の例である。
【００３４】
場合によっては、複数のベクトル特性を調べることができ、図４～図６に関して説明した情報を処理して、攻撃が検出されたときに信号が特定の方向に動いているかどうか（または、ノイズのために移動したかどうか）を判定することができる。攻撃が行われたときに信号が一様に増加していた場合には、この信号は元の攻撃に対する応答であり、独立した攻撃ではない。
【００３５】
産業資産制御システムは、動作パラメータの範囲（例えば、負荷、温度など）にわたる非線形動作に関連し得ることに留意されたい。その結果、データの変動が大きくなり、サイバー脅威がいつ制御システムの動作に基づいて存在するかを判断することが困難になる可能性がある。図７は、いくつかの実施形態によるサイバー攻撃検出システム７００のブロック図を示す。具体的には、システム７００は、負荷（例えば、ガスタービン負荷、適応リアルタイムエンジンシミュレーション「ＡＲＥＳ」負荷など）に関する情報を、負荷正規化機能７２０に送信するガスタービン７１０（例えば、ガスタービンユニットコントローラに関連する）を示す。ガスタービン７１０はまた、モード処理７３０（例えば、ガスタービンの報告された動作モード）および特徴処理７４０（例えば、ガスタービンユニットデータ）に情報を送信してもよい。後述するように、負荷正規化機能７２０は、正規化された監視ノード信号を特徴処理７４０に送信することができる。後処理７５０は、特徴処理７４０から情報を受信し、判定処理７７０（正常／攻撃データセット記憶装置７６０

から受信したデータセットに少なくとも部分的に基づいてサイバー攻撃警報を自動的に生成することができる）にデータを送信することができる。したがって、いくつかの実施形態は、タービン負荷もしくは温度レベルおよび時間的な時系列信号に動的に基づいて、正規化された監視ノード信号を計算することができる。この正規化は、異なる負荷条件に対して攻撃検出を実行する能力を提供することができる。

【００３６】

実施形態は、時間的および／または空間的正規化を利用できることに留意されたい。時間的正規化は、時間軸に沿った正規化を提供することができる。空間的正規化を使用して、複数のノード（例えば、センサ軸）に沿って信号を正規化することができる。いずれの場合でも、正規化された信号は、特徴抽出および判定境界との比較を使用して攻撃検出を実行するために使用することができる。センサ、アクチュエータ、およびコントローラノードの時系列データは、実質的にリアルタイムで処理され、このデータから「特徴」を抽出することができる。次に、特徴データを判定境界と比較して、サイバー攻撃がシステムに生じたかどうかを判定することができる。空間的に正規化されたデータにおける攻撃を検出するために同様の手法を用いることができる。

【００３７】

リアルタイムデータの処理は、ガスタービン７１０の正常動作点を利用することができる。この正常動作点は、例えば、システム動作モード、外部条件、システム劣化要因、燃料入力などに基づいて決定することができる。実際に測定されたセンサデータ、アクチュエータデータ、およびコントローラノードのデータは、実際の値と公称値との間の差が計算され、この差、すなわちデルタが予想動作条件係数で正規化されるように処理することができる。タービン負荷レベル（例えば、メガワット（「ＭＷ」）で表される）は、複数の測定値に基づいて計算することができ、負荷は、適応リアルタイムエンジンモデルから推定することができることに留意されたい。

【００３８】

いくつかの実施形態によれば、以下をオフラインで（リアルタイムではなく）実行することができる。所与のタービンモードに対して、ガスタービン７１０の動作は、高忠実度モデルを用いてシミュレートすることができる。負荷レベルは、最低動作点から最高動作点まで変化させることができる（例えば、予め定められた時間間隔ごとにステップを変化させる）。このシミュレートされたデータは、様々な負荷レベルでいくつかの作動データファイルを生成する。これらのファイルの１つを取ると、負荷レベルは平均化され、予め規定された負荷レベル分解能に分類される（例えば、最も近い０．２５ＭＷに平均される）。これらの正規化パケットを時系列信号の処理への入力として使用することにより、リアルタイムで動作するときの動的正規化が容易になる。次いで、動的正規化プロセスからのこれらの出力は、特徴発見プロセスにおいて使用することができる。

【００３９】

図８は、いくつかの実施形態によるグローバル脅威保護システム８００の一例である。特に、システムは、３つの発電機（Ａ、Ｂ、およびＣ）を含み、脅威ノードからの値８１０のバッチが、ある期間（例えば３０～５０秒）にわたって生成された各々について収集される。いくつかの実施形態によれば、脅威ノードからの値８１０のバッチは時間的に重複する。脅威ノードからの値８１０は、例えば、時間（t_1、t_2など）および脅威ノードのタイプ（S_1、S_2など）によって配列された行列８２０に格納することができる。特徴量設計コンポーネント８３０は、３つの発電機（例えば、発電機Ｃに対する特徴ベクトル８４０は、FS_{C1}、FS_{C2}などを含む可能性がある）ごとに特徴ベクトル８４０を作成するために、各行列８２０内の情報を使用することができる。次いで、３つの特徴ベクトル８４０は、システム８００に対して単一のグローバル特徴ベクトル８５０に組み合わせることができる。相互作用特徴８６０を適用してもよく（例えば、Ａ×Ｂ×Ｃ、Ａ＋Ｂ＋Ｃなどに関連付けられる）、異常検出エンジン８７０は、その結果を判定境界と比較し、適切な場合に脅威警報信号を出力することができる。説明するように、実施形態は、脅威検出システム８００の性能を改善するために、ローカル特徴ベクトル８４０およびグローバ

ル特徴ベクトル８５０の両方について、特徴および境界パラメータを調整することができる。

【００４０】

図９は、いくつかの実施形態による三次元の脅威ノード出力を示す９００。特に、グラフ９１０は、主要成分特徴（「ＰＣＦ」）に関連付けられた次元、例えば、ｗ１、ｗ２、およびｗ３などの３次元の脅威ノード出力（「＋」）をプロットする。さらに、グラフ９１０は、正常動作空間の判定境界９２０の表示を含む。単一の連続境界９２０が図９に示されているが、実施形態は複数の領域に関連付けられてもよい。ＰＣＦ情報は、低下次元で重みとして表すことができることに留意されたい。例えば、各脅威ノードからのデータは、低次元の特徴（例えば、重み）に変換することができる。いくつかの実施形態によれば、脅威ノードデータは、以下のように正規化され、

【００４１】

【数１】

$$S_{normalized}(k) = \frac{S_{nominal}(k) - S_{original}(k)}{\bar{S}_{nominal}}$$

ここで、Ｓは、「ｋ」時点の脅威ノード量を表す。さらに、その場合、出力は、以下のように、基底関数の加重線形結合として表現することができ

【００４２】

【数２】

$$S = S_0 + \sum_{j=1}^{N} w_i \Psi_j$$

ここで、S_0は全ての脅威を伴う平均脅威ノード出力であり、w_jはｊ番目の重みであり、Ψ_jはｊ番目の基底ベクトルである。いくつかの実施形態によれば、脅威ノードのデータ行列の共分散を用いて自然基底ベクトルが得られる。基底ベクトルが分かれば、以下の式を用いて重みを求めることができる（基底集合が直交すると仮定する）。

【００４３】

$w_j = (S - S_0)^T \Psi_j$

重みは、特徴ベクトルで使用される特徴の例であり得ることに留意されたい。

【００４４】

いくつかの実施形態によれば、脅威検出のための特徴および境界調整に関連して、脅威ノード出力を使用することができる。例えば、図１０は、いくつかの実施形態による脅威検出のための特徴および境界調整の方法１０００である。Ｓ１０１０において、一連の正常監視ノード値を、脅威検出モデル作成コンピュータによって受信することができる。次いで、脅威検出モデル作成コンピュータは、一組の正常特徴ベクトルを生成することができ、経時的な一連の正常監視ノード値は、産業資産制御システムの正常動作を表す。Ｓ１０２０において、一連の脅威監視ノード値が受信され、産業資産制御システムの脅威を受けている動作を（表す）一組の脅威特徴ベクトルを生成することができる。いくつかの実施形態によれば、一連の正常監視ノード値および／または一連の脅威監視ノード値は、高忠実度機器モデルと関連付けられてもよい。

【００４５】

Ｓ１０３０において、システムは、一組の正常特徴ベクトル、一組の脅威特徴ベクトル、および少なくとも１つの初期アルゴリズムパラメータに基づいて、脅威検出モデルのための少なくとも１つの潜在的判定境界を計算することができる。いくつかの実施形態によれば、アルゴリズムパラメータは、一組の潜在的アルゴリズムパラメータから自動的に選択

される。例えば、予測モデルは、多数の潜在的なアルゴリズムパラメータを検討して、システムの性能を最適化するための「キー」としてパラメータのサブセットを特定することができる。

【００４６】

Ｓ１０４０において、システムは、性能メトリックに基づいて少なくとも１つの潜在的判定境界の性能を評価することができる。図１１に関して説明したように、性能メトリックは、例えば、受信者操作曲線メトリックに関連付けられてもよい。いくつかの実施形態によれば、性能メトリックは、脅威検出の速度と関連付けられてもよい。Ｓ１０５０において、システムは、Ｓ１０４０での評価の結果に基づいて少なくとも１つの初期アルゴリズムパラメータを調整し、少なくとも１つの潜在的判定境界を再計算することができる。いくつかの実施形態によれば、Ｓ１０４０およびＳ１０５０の自動的な評価、調整、および再計算は、最終調整アルゴリズムパラメータおよび最終判定境界が決定されるまで継続的に実行される。

【００４７】

いくつかの実施形態によれば、Ｓ１０４０およびＳ１０５０の自動的な評価、調整、および再計算は、ローカル特徴ベクトルおよびローカル判定境界に関連付けられる。この場合、ローカル特徴ベクトルの抽出は、例えば、最小値、最大値、平均値、分散、整定時間、高速フーリエ変換スペクトル、極、浅い特徴、主成分解析、独立成分解析、ｋ－平均クラスタリング、スパース符号化、および／またはディープラーニングの特徴に関連付けることができる。

【００４８】

いくつかの実施形態によれば、（例えば、図８に関して説明したように）複数のローカル特徴ベクトルおよびローカル判定境界は、結合されてグローバル特徴ベクトルおよびグローバル判定境界を形成する。この場合、Ｓ１０４０およびＳ１０５０の自動的な評価、調整、および再計算は、グローバル特徴ベクトルおよびグローバル判定境界に関連付けることができる。さらに、グローバル特徴ベクトルおよびグローバル判定境界の少なくとも一方は、次元縮退、カーネル選択、いくつかのサポートベクトル、正常データに関連するコスト、および／または異常データに関連するコストに使用されるいくつかの重みに関連付けられてもよい。

【００４９】

潜在的判定境界の性能（したがって、脅威検出システムの性能）を評価するために使用される性能メトリックは、いくつかの実施形態によれば、受信者操作曲線（「ＲＯＣ」）測定であってもよい。本明細書で使用されるＲＯＣ測定は、識別しきい値が変更されると、バイナリ分類器システムの性能を反映することができる。例えば、図１１は、いくつかの実施形態による全母集団のＲＯＣ測定１１００を示す。特に、「陽性」および「陰性」の予測条件は、「陽性」および「陰性」の真の（すなわち実際の）条件と比較することができる（例えば、「陽性」はサイバー脅威を示し、「陰性」）はサイバー脅威を示さない）。このようなシステムの結果には、真陽性１１１０（脅威が予測され、実際に存在した場合）、真陰性１１２０（脅威が予測されず、脅威が存在しない場合）、偽陽性１１３０（脅威が予測されたが実際には脅威が存在しなかった場合）、および偽陰性１１４０（脅威が予測されなかったが、実際には脅威が存在した場合）が含まれる。

【００５０】

ＲＯＣ測定１１００は、サイバー脅威検出アルゴリズムの最適化および調整に関連して、例えば、低い偽陽性を達成するために使用することができる。そのようなアルゴリズムは、例えば、産業資産の複数の監視ノードからの時系列データを表すために特徴を使用する脅威検出アルゴリズムを含むことができる。特徴は、ローカル監視ノードについて構成することができ、これらの特徴は、次いで、グローバル特徴ベクトルに結合することができる（そして、グローバル特徴境界を計算することができる）。調整パラメータは、グローバル特徴ベクトルおよびグローバル特徴の境界の両方の作成のために選択することができる。最適化は、検出時間メトリックと併せて目的関数である堅牢な統計的ＲＯＣ出力を用

いて実行することができる。最適化は、アルゴリズムのパラメータを、より少ない偽陽性、より少ない偽陰性、または様々な調整パラメータの使用による迅速な検出に向けてバイアスするために実行することができることに留意されたい。

【００５１】

図１１に示すように、特定のＲＯＣ測定１１００の例は、脅威検出システムの性能を測定するために使用することができ、ＲＯＣ精度、陽性予測値、偽発見率、偽省略率、陰性予測値、有病率、真陽性率、偽陽性率、陽性尤度比、陰性尤度比、偽陰性率、真陰性率、および／または診断オッズ比を含むことができる。最適化の目的関数としてＲＯＣ測定１１００を使用することによって、アルゴリズムを様々な所望の結果に最適化する柔軟性を提供することができる。入力は、評価集合の真理値ラベルであってもよく、アルゴリズムは、各評価実行に対してスコアを提供してもよい。

【００５２】

目的関数が所定の位置（例えば、ＲＯＣ測定１１００または検出時間）にある場合、アルゴリズムの調整を行うことができる。アルゴリズムは、最初に監視ノードデータから特徴を抽出する必要があり得る。これは、どの特徴が所望の結果に従って最も有用な情報を抽出するかに関連して、１つの調整パラメータが存在する可能性がある場合である。これらの特徴は、例えば、最大値、最小値、平均値、分散、整定時間、または高速フーリエ変換スペクトルデータ、極などの知識ベースの特徴であってもよい。特徴は、いくつかの実施形態によれば、主成分解析（「ＰＣＡ」）、独立成分解析（「ＩＣＡ」）、ｋ－平均クラスタリング、スパース符号化、および／またはディープラーニング特徴に関連する特徴などの「浅い」特徴であってもよい。これは、例えば、最初の調整「ノブ」と考えることができる。適用可能であれば、特徴についてのいくつかの重み付けもあり得る。この場合、次元縮退が行われる場合に使用される重み付けの数の調整もあり得る。実施形態は、グローバルな特徴境界の調整に移動することができ、そこでは、どのモデルが最良に動作するか、どのカーネルか、またはサポートベクトルの数、または正常もしくは異常データに関連するコストなどを見つけるために境界を調整することができる。アルゴリズムは、例えば、調整ノブを選択し、目的関数を設定して性能を測定することによって、調整することができる。その結果、（停滞しているシステムとは対照的に）ユーザのニーズに合わせることができる自己調整型サイバー検出アルゴリズムを提供することができる。

【００５３】

例えば、図１２は、いくつかの実施形態による最適化フローチャート１２００である。１２１０において、システムは、パラメータの調整を停止するかどうか（例えば、満足のいくレベルの性能に達しており、プロセスが終了してもよい）を決定することができる。システムが１２１０で継続することを決定した場合（さらなる最適化が行われるように）には、評価アルゴリズムは、１２２０でＲＯＣメトリックを目的関数として利用することができる。次いで、システムは、ローカル特徴を作成するために使用される特徴のタイプおよび数の調整ノブを使用するなどして、１２３０で特徴を作成することができる（調整ノブの選択および／または設定は、手動および／または自動であってもよいことに留意されたい）。１２４０において、境界構築のための調整ノブを使用してローカル境界を作成することができる。１２５０において、グローバル特徴ベクトルは、次元縮退のタイプおよびグローバル特徴の数についての調整ノブを使用して作成することができる。１２６０において、グローバル境界構築のための調整ノブを使用して、１つまたは複数のグローバル境界を作成することができる。システムは１２２０の評価アルゴリズムに戻り、１２１０で最適化を続行するか否かを決定することができる。したがって、最適化プロセスは、アルゴリズムを一組の定義された要件に合わせることを可能にすることができる。要件は、偽陽性、真陽性、偽陰性、真陰性、特異性、精度、感度、またはグローバル異常を検出する時間、異常を局在化する時間などの検出時間メトリックなどの、ＲＯＣメトリックであってもよい。

【００５４】

いくつかの実施形態は、ユーザのニーズに合うようにアルゴリズムの性能および挙動を変

更する能力を提供することができる。これは、産業制御システム（「ＩＣＳ」）セキュリティの成長分野で多くの用途が発生しているサイバーセキュリティ空間において特に重要となり得る。いくつかの製造工場などのサイバー攻撃の影響がより低い用途では、生産を妨げる可能性があるので、ユーザは正常な動作を「異常」として識別することを望まない場合がある。発電や商業輸送などの別の用途では、サイバー攻撃の発生時期を知ることが重要であり得る。この場合、オペレータが状況を確認し修復するためのプロセスを実行することができるので（また、誤って攻撃を逃した結果が相当なものになる可能性があるので）、場合によっては正常動作を攻撃として誤って通知することも許容され得る。いくつかの実施形態では、最適化および調整方法は、単純化のためにアルゴリズムで使用される重み（特徴）の数だけを調整することができる。１つまたは複数のＲＯＣ測定の曲線下面積（「ＡＵＣ」）解析は、本明細書に記載の実施形態に従って実施することができることに留意されたい。

【００５５】

調整パラメータは、システムによって自動的に選択されてもよく、および／またはユーザ入力に基づいてもよいことに留意されたい。例えば、図１３は、１つまたは複数の調整ノブを選択するために使用できるユーザ入力領域１３２０と共に監視ノード情報（例えば、現在の特徴ベクトル１３１０および判定境界を含む）を表示することができる対話型グラフィカル・ユーザ・インターフェース（「ＧＵＩ」）・ディスプレイ１３００を示すディスプレイ１３００である。例えば、ユーザは、特徴のタイプ、いくつかのローカル特徴、いくつかのグローバル特徴、次元縮退の方法（例えば、ＰＣＡ、主成分回帰（「ＰＣＲ」）、フィッシャーディスクリミネータ解析（「ＦＤＡ」など）、境界構築方法（例えば、サポートベクトルマシン（「ＳＶＭ」））、境界方法特定調整器（例えば、カーネル機能、ボックス制約、またはコスト）、入力バッチサイズなどを用いて選択することができる。

【００５６】

本明細書で説明する実施形態は、任意の数の異なるハードウェア構成を使用して実現することができる。例えば、図１４は、例えば、図１のシステム１００に関連することができる産業資産制御システム保護プラットフォーム１４００のブロック図である。産業資産制御システム保護プラットフォーム１４００は、通信ネットワーク（図１４では図示せず）を介して通信するよう構成される通信デバイス１４２０に結合される、１チップマイクロプロセッサの形式の１つまたは複数の市販の中央処理装置（「ＣＰＵ」）などの、プロセッサ１４１０を含む。通信デバイス１４２０を使用して、例えば、１つまたは複数の遠隔監視ノード、ユーザプラットフォームなどと通信することができる。産業資産制御システム保護プラットフォーム１４００は、入力デバイス１４４０（例えば、調整ノブ選択および／または予測型モデリング情報を入力するコンピュータマウスおよび／またはキーボード）および／または出力デバイス１４５０（例えば、表示をレンダリングし、警報を送信し、推奨事項を送信し、および／またはレポートを作成するためのコンピュータモニタ）をさらに含む。いくつかの実施形態によれば、モバイル機器、監視物理システム、および／またはＰＣを使用して、産業資産制御システム保護プラットフォーム１４００と情報を交換することができる。

【００５７】

プロセッサ１４１０はまた、記憶装置１４３０と通信する。記憶装置１４３０は、磁気記憶装置（例えば、ハードディスクドライブ）、光学記憶装置、携帯電話、および／または半導体メモリデバイスの組み合わせを含む、任意の適切な情報記憶装置を含むことができる。記憶装置１４３０は、プロセッサ１４１０を制御するためのプログラム１４１２および／または脅威検出モデル１４１４を格納する。プロセッサ１４１０は、プログラム１４１２、１４１４の命令を実行し、それにより、本明細書で説明する実施形態のいずれかに従って動作する。例えば、プロセッサ１４１０は、一連の正常監視ノード値（産業資産制御システムの正常動作を表す）を受信し、一組の正常特徴ベクトルを生成することができる。プロセッサ１４１０はまた、一連の脅威監視ノード値（産業資産制御システムの脅威を受けている動作を表す）を受信し、一組の脅威特徴ベクトルを生成することもできる。

脅威検出モデルのための少なくとも１つの潜在的判定境界は、一組の正常特徴ベクトル、一組の脅威特徴ベクトル、および初期アルゴリズムパラメータに基づいてプロセッサ１４１０によって計算することができる。少なくとも１つの潜在的判定境界の性能は、性能メトリックに基づいてプロセッサ１４１０によって評価することができる。その後に、初期アルゴリズムパラメータを評価の結果に基づいてプロセッサ１４１０によって調整することができ、少なくとも１つの潜在的判定境界を再計算することができる。

【００５８】

プログラム１４１２、１４１４は、圧縮フォーマット、未コンパイルフォーマット、および／または暗号化フォーマットで格納することができる。プログラム１４１２、１４１４は、さらに、オペレーティングシステム、クリップボードアプリケーション、データベース管理システム、および／または周辺機器とインターフェースするためにプロセッサ１４１０によって使用されるデバイスドライバなどの、他のプログラム要素を含むことができる。

【００５９】

本明細書で使用される場合、情報は、例えば、（ｉ）別のデバイスから産業資産制御システム保護プラットフォーム１４００によって「受信される」か、もしくは別のデバイスから産業資産制御システム保護プラットフォーム１４００に「送信する」ことができ、または（ｉｉ）別のソフトウェアアプリケーション、モジュール、もしくはソースから産業資産制御システム保護プラットフォーム１４００内のソフトウェアアプリケーションもしくはモジュールによって「受信される」か、もしくは別のソフトウェアアプリケーション、モジュール、もしくはソースから産業資産制御システム保護プラットフォーム１４００内のソフトウェアアプリケーションもしくはモジュールに「送信する」ことができる。

【００６０】

いくつかの実施形態（図１４に示すものなど）では、記憶装置１４３０は、ローカルデータベース１５００、グローバルデータベース１６００、および監視ノードデータベース１７００をさらに格納する。ここで、産業資産制御システム保護プラットフォーム１４００に関連して使用することができるデータベースの一例を、図１５～図１７に関して詳細に説明する。本明細書で説明するデータベースは例に過ぎず、追加のおよび／または異なる情報をそこに格納してもよいことに留意されたい。さらに、様々なデータベースは、本明細書に記載された実施形態のいずれかに従って分割または結合することができる。

【００６１】

図１５を参照すると、いくつかの実施形態による産業資産制御システム保護プラットフォーム１４００に格納することができるローカルデータベース１５００を表すテーブルが示されている。テーブルは、例えば、産業資産制御システムのローカル特徴および境界に関連するエントリを含むことができる。テーブルはまた、各エントリに対してフィールド１５０２、１５０４、１５０６、１５０８、１５１０を定義することもできる。フィールド１５０２、１５０４、１５０６、１５０８、１５１０は、いくつかの実施形態によれば、産業資産識別子１５０２、初期アルゴリズムパラメータ１５０６、性能メトリック１５０６、調整されたアルゴリズムパラメータ１５０８、およびローカル特徴および境界１５１０を指定することができる。ローカルデータベース１５００は、例えば、新しい物理システムが監視またはモデル化されたときに、オフライン（非リアルタイム）で作成および更新することができる。

【００６２】

産業資産識別子１５０２は、例えば、監視される産業資産（例えば、ジェットタービンシステム、製造プラント、風力発電所など）を識別する固有の英数字コードであってもよい。初期アルゴリズムパラメータ１５０４は、例えば（例えば、正常特徴ベクトルおよび脅威特徴ベクトルに基づいて）ローカル判定境界を計算するために使用される値を含むことができる。性能メトリック１５０６は、例えば、判定境界の性能（例えば、ＲＯＣ測定、検出速度など）を評価するために使用される値であってもよい。調整されたアルゴリズムパラメータ１５０８は、（例えば、性能メトリック１５０６に関連付けられた）調整ノブ

に従って初期アルゴリズムパラメータ１５０４に対してなされた更新を反映することができる。ローカル特徴および境界１５１０は、最適化プロセスが完了した後の最終的な解を表すことができる。

【００６３】

図１６を参照すると、いくつかの実施形態による産業資産制御システム保護プラットフォーム１４００に格納することができるグローバルデータベース１６００を表すテーブルが示されている。テーブルは、例えば、産業資産制御システムのグローバル特徴および境界に関連するエントリを含むことができる。テーブルはまた、各エントリに対してフィールド１６０２、１６０４、１６０６、１６０８、１６１０を定義することもできる。フィールド１６０２、１６０４、１６０６、１６０８、１６１０は、いくつかの実施形態によれば、産業資産識別子１６０２、初期アルゴリズムパラメータ１６０６、性能メトリック１６０６、調整されたアルゴリズムパラメータ１６０８、およびグローバル特徴および境界１６１０を指定することができる。グローバルデータベース１６００は、例えば、新しい物理システムが監視またはモデル化されたときに、オフライン（非リアルタイム）で作成および更新することができる。

【００６４】

産業資産識別子１６０２は、例えば、監視される産業資産を識別する固有の英数字コードであってもよく、ローカルデータベース１５００の産業資産識別子１５０２に基づいてもよく、または関連してもよい。初期アルゴリズムパラメータ１６０４は、例えば、グローバル判定境界を計算するために使用される値を含むことができる。性能メトリック１６０６は、例えば、判定境界の性能（例えば、ＲＯＣ測定、検出速度など）を評価するために使用される値であってもよい。調整されたアルゴリズムパラメータ１６０８は、（例えば、性能メトリック１６０６に関連付けられた）調整ノブに従って初期アルゴリズムパラメータ１６０４に対してなされた更新を反映することができる。グローバル特徴および境界１６１０は、最適化プロセスが完了した後の最終的な解を表すことができる。

【００６５】

図１７を参照すると、いくつかの実施形態による産業資産制御システム保護プラットフォーム１４００に格納することができる監視ノードデータベース１７００を表すテーブルが示されている。テーブルは、例えば、物理システムに関連する監視ノードを識別するエントリを含むことができる。テーブルはまた、各エントリに対してフィールド１７０２、１７０４、１７０６、１７０８、１７１０、１７１２を定義することもできる。フィールド１７０２、１７０４、１７０６、１７０８、１７１０、１７１２は、いくつかの実施形態によれば、監視ノード識別子１７０２、監視ノード値１７０４、特徴１７０６、特徴ベクトル１７０８、グローバル特徴ベクトル１７１０、および判定１７１２を指定することができる。監視ノードデータベース１７００は、例えば、新しい物理システムが監視またはモデル化され、脅威ノードが値を報告し、動作条件が変化するなどした場合、作成および更新することができる。

【００６６】

監視ノード識別子１７０２は、例えば、一連の監視ノード値１７０４を経時的に（例えば、データの３０～５０秒のバッチで）検出する産業資産制御システム内の脅威ノードを識別する固有の英数字コードであってもよい。監視ノード値１７０４は、（例えば、最適化された調整パラメータに従って）特徴１７０６および特徴ベクトル１７０８を作成するために使用することができる。複数の監視ノード識別子１７０２に関連する特徴ベクトル１７１０は、（例えば、最適化された調整パラメータに従って）産業資産制御システム全体の全体的なグローバル特徴ベクトル１７１０を生成するために使用することができる。次いで、グローバル特徴ベクトル１７１０を判定境界と比較して、判定１７１２（例えば、「攻撃」または「正常」の表示）を生成することができる。

【００６７】

したがって、実施形態は、ユーザの特定のニーズ（例えば、所望の偽陽性率）に従って、産業資産にサイバー攻撃保護を提供することができる。さらに、実施形態は、監視ノード

からのリアルタイム信号を使用して、マルチクラス異常動作の指標を受動的に検出することを可能にすることができる。またさらに、検出フレームワークは、複数の地理的位置における様々なシステム（すなわち、ガスタービン、蒸気タービン、風力タービン、航空エンジン、機関車エンジン、電力網など）への本発明の展開を容易にするツールの開発を可能にすることができる。いくつかの実施形態によれば、（複数タイプの機器およびシステムにわたる）この技術によって可能になる分散型検出システムは、多点攻撃を検出するのに役立つ協調データの収集を可能にする。本明細書に記載した特徴ベースの手法は、データの新しい学習および代替的なソースが利用可能になると、拡張された特徴ベクトルを可能にし、および／または既存のベクトルに新しい特徴を組み込むことができることに留意されたい。その結果、実施形態は、システムがそれらの特性についてより多くを学習するにつれて、比較的広い範囲のサイバー脅威（例えば、ステルス、リプレイ、隠密、インジェクション攻撃など）を検出することができる。実施形態はまた、システムが有用で重要な新しい特徴を組み込み、冗長またはそれほど重要でないものを除去するので、偽陽性率を低減する可能性がある。本明細書に記載した検出システムは、攻撃を阻止することができる（または攻撃の影響を鈍化させることができる）ように、産業資産制御システムのオペレータに早期の警報をもたらし、機器の損傷を軽減することができることに留意されたい。

【００６８】

サイバーセキュリティは、発電プラント機器などの資産の保護に必要な重要な機能であることに留意されたい。この空間における動的正規化は、検出の分解能を向上させることができる。産業資産に関連する機械は非常に複雑である可能性があり、本明細書に記載した実施形態は、検出を迅速かつ確実に行うサイバーセキュリティアルゴリズムの実施を可能にすることができる。負荷変動（例えば、真陽性検出、偽陽性検出、真陰性検出および偽陰性検出の表示を含む）に対する動的正規化の使用を評価するために、受信者操作特性（「ＲＯＣ」）曲線を使用できることに留意されたい。

【００６９】

以下に、本発明の様々な追加の実施形態を示す。これらは全ての可能な実施形態の定義を構成するものではなく、当業者は、本発明が他の多くの実施形態に適用可能であることを理解するであろう。さらに、以下の実施形態は、明瞭にするために簡潔に記載されているが、当業者であれば、これらのおよび他の実施形態ならびに用途に対応するための上述の装置および方法に、必要に応じて任意の変更を加える方法を理解するであろう。

【００７０】

特定のハードウェアおよびデータ構成について本明細書で説明してきたが、本発明の実施形態に従って任意の数の他の構成を提供することができることに留意されたい（例えば、本明細書に記載のデータベースに関連する情報の一部は、外部システムと組み合わせるか、または外部システムに格納することができる）。例えば、いくつかの実施形態はガスタービン発電機に焦点を当てているが、本明細書に記載された実施形態のいずれも、ダム、電力網、軍用機などの他のタイプの資産に適用することができる。

【００７１】

いくつかの実施形態は、予め選択された調整ノブおよび／または調整ノブパラメータの使用を記載している。いくつかの実施形態によれば、調整手法は、アルゴリズムパラメータを最適化し、ＲＯＣ統計を改善するために、適応調整のためにオンラインデータを使用することができる。このような必要性は、例えば、システム構成要素が交換され、新しい資産が導入され、新しい特徴が導入され、カーネル機能が変更されるなどの場合に生じる可能性がある。最新のモデルを使用してオンラインで調整する場合、評価ランを実行するのに十分なケースが生成され得る。モデルパラメータは、それらがシステムの現在の挙動を表すようにオンライン調整アルゴリズムを使用して調整することができる。このようなアプローチでは、ユーザの目的に応じて性能測定（ＲＯＣ統計など）を使用することができる。実装されたプラントモデルが実際の産業資産の状態と一致しなくなった場合には、正常動作データだけが消費される「ワンクラス」学習（半監督下の学習）を使用して新しい

判定境界を作成することができる。ワンクラスの学習では、他のＲＯＣ統計ではなく、偽陽性が性能測定として使用されてもよい。

【００７２】

いくつかの実施形態によれば、攻撃状態に関する情報は、異なる産業資産プラント間で織り込まれてもよい。例えば、１つの発電プラントが（他の発電プラントの）他のノードの状態を認識することができ、そのようなアプローチは、協調サイバー脅威を阻止するのにさらに役立つことができる。自動的な脅威検出に加えて、本明細書に記載したいくつかの実施形態は、防衛のさらなるサイバー層をシステムに提供し、（例えば、動作データを使用する際に）カスタムプログラミングなしで展開可能とすることができる。いくつかの実施形態は、ライセンスキーと共に販売され、監視サービスとして組み込むことができる。例えば、工業用資産プラントの機器をアップグレードする場合に、境界を定期的に更新することができる。

【００７３】

本発明は、説明目的のみのために、いくつかの実施形態の観点から記載されている。当業者であれば、本発明は記載された実施形態に限定されるものではなく、添付の特許請求の範囲の精神および範囲によってのみ限定される修正および改変によって実施できることを認識するであろう。

［実施態様１］

産業資産制御システムを保護するシステム（１００，３００，８００）であって、

複数の監視ノード（１３０）の各々について、前記産業資産制御システムの正常動作を表す経時的な一連の正常監視ノード値（１７０４）を格納する正常空間データソース（１１０）と、

前記複数の監視ノード（１３０）の各々について、前記産業資産制御システムの脅威を受けている動作を表す経時的な一連の脅威監視ノード値（１７０４）を格納する脅威空間データソース（１２０）と、

前記正常空間データソース（１１０）および前記脅威空間データソース（１２０）に結合された脅威検出モデル作成コンピュータ（１４０）であって、

（ｉ）前記一連の正常監視ノード値（１７０４）を受信し、一組の正常特徴ベクトル（５１２，１７０８）を生成し、

（ｉｉ）前記一連の脅威監視ノード値（１７０４）を受信し、一組の脅威特徴ベクトル（５１２，１７０８）を生成し、

（ｉｉｉ）前記一組の正常特徴ベクトル（５１２，１７０８）、前記一組の脅威特徴ベクトル（５１２，１７０８）、および少なくとも１つの初期アルゴリズムパラメータ（１５０４，１６０４）に基づいて、脅威検出モデル（１５５，１４１４）のための少なくとも１つの潜在的判定境界を自動的に計算し、

（ｉｖ）性能メトリック（１５０６，１６０６）に基づいて前記少なくとも１つの潜在的判定境界の性能を自動的に評価し、

（ｖ）前記評価の結果に基づいて前記少なくとも１つの初期アルゴリズムパラメータ（１５０４，１６０４）を自動的に調整し、前記少なくとも１つの潜在的判定境界を再計算する、

脅威検出モデル作成コンピュータ（１４０）と

を含む、システム（１００，３００，８００）。

［実施態様２］

前記自動的な評価、調整、および再計算は、最終調整アルゴリズムパラメータおよび最終判定境界が決定されるまで実行される、実施態様１に記載のシステム（１００，３００，８００）。

［実施態様３］

前記自動的な評価、調整、および再計算は、ローカル特徴ベクトル（５１２，１７０８）およびローカル判定境界に関連付けられる、実施態様１に記載のシステム（１００，３００，８００）。

［実施態様４］
前記ローカル特徴ベクトル（５１２，１７０８）の抽出は、最小値、最大値、平均値、分散、整定時間、高速フーリエ変換スペクトル、極、浅い特徴、主成分解析、独立成分解析、ｋ－平均クラスタリング、スパース符号化、およびディープラーニングの特徴のうちの少なくとも１つに関連付けられる、実施態様３に記載のシステム（１００，３００，８００）。
［実施態様５］
複数のローカル特徴ベクトル（５１２，１７０８）およびローカル判定境界は、結合されてグローバル特徴ベクトル（８５０，１７１０）およびグローバル判定境界を形成し、前記自動的な評価、調整、および再計算は、前記グローバル特徴ベクトル（８５０，１７１０）および前記グローバル判定境界に関連付けられる、実施態様１に記載のシステム（１００，３００，８００）。
［実施態様６］
前記グローバル特徴ベクトル（８５０，１７１０）および前記グローバル判定境界の少なくとも一方は、次元縮退、カーネル選択、いくつかのサポートベクトル、正常データ（３１０）に関連するコスト、および異常データに関連するコストに使用されるいくつかの重みに関連付けられる、実施態様５に記載のシステム（１００，３００，８００）。
［実施態様７］
前記性能メトリック（１５０６，１６０６）は、受信者操作特性（「ＲＯＣ」）メトリックを含む、実施態様１に記載のシステム（１００，３００，８００）。
［実施態様８］
前記ＲＯＣメトリックは、真陽性（１１１０）、真陰性（１１２０）、偽陽性（１１３０）、偽陰性（１１４０）、曲線下面積、ＲＯＣ精度、陽性予測値、偽発見率、偽省略率、陰性予測値、有病率、真陽性率、偽陽性率、陽性尤度比、陰性尤度比、偽陰性率、真陰性率、および診断オッズ比のうちの少なくとも１つに関連付けられる、実施態様７に記載のシステム（１００，３００，８００）。
［実施態様９］
前記性能メトリック（１５０６，１６０６）は、脅威検出の速度に関連付けられる、実施態様１に記載のシステム（１００，３００，８００）。
［実施態様１０］
前記アルゴリズムパラメータは、一組の潜在的アルゴリズムパラメータから自動的に選択される、実施態様１に記載のシステム（１００，３００，８００）。
［実施態様１１］
前記初期アルゴリズムパラメータ（１５０４，１６０４）は、特徴（１７０６）のタイプ、いくつかのローカル特徴、いくつかのグローバル特徴、次元縮退の方法、主成分解析、主成分回帰、フィッシャーディスクリミネータ解析、サポートベクトルマシン、境界構築方法、境界方法特定調整器、カーネル機能、ボックス制約、コスト、および入力バッチサイズのうちの少なくとも１つに関連付けられる、実施態様１に記載のシステム（１００，３００，８００）。
［実施態様１２］
前記一連の正常監視ノード値（１７０４）および前記一連の脅威監視ノード値（１７０４）のうちの少なくとも一方が、高忠実度機器モデルに関連付けられる、実施態様１に記載のシステム（１００，３００，８００）。
［実施態様１３］
前記自動的な計算、評価、および調整の少なくとも１つは、遠隔産業資産制御システム情報源から受信したオンライン更新に少なくとも部分的に基づいて実行される、実施態様１に記載のシステム（１００，３００，８００）。
［実施態様１４］
前記産業資産制御システムの現在の動作を表す、経時的な監視ノード信号値のストリームを受信するための複数のリアルタイム監視ノード信号入力と、

前記複数のリアルタイム監視ノード信号入力および前記脅威検出モデル作成コンピュータ（１４０）に結合された脅威検出コンピュータプラットフォームであって、
（ｉ）監視ノード信号値の前記ストリームを受信し、
（ｉｉ）監視ノード信号値の各ストリームについて、現在の監視ノード特徴ベクトル（５１２，１７０８）を生成し、
（ｉｉｉ）各監視ノード（１３０）について適切な判定境界を選択し、前記適切な判定境界は、前記現在の協調モードにおいてその監視ノード（１３０）の異常状態から正常状態を分離し、
（ｉｖ）各生成された現在の監視ノード特徴ベクトル（５１２，１７０８）を前記選択された対応する適切な判定境界と比較し、
（ｖ）前記比較の結果に基づいて脅威警報信号を自動的に送信する、
脅威検出コンピュータプラットフォームと
をさらに含む、実施態様１に記載のシステム（１００，３００，８００）。
［実施態様１５］
前記脅威警報信号の送信は、クラウドベースのシステム、エッジベースのシステム、無線システム、有線システム、保護されたネットワーク、および通信システムのうちの少なくとも１つを使用して実行される、実施態様１４に記載のシステム（１００，３００，８００）。
［実施態様１６］
前記脅威は、アクチュエータ攻撃、コントローラ攻撃、監視ノード攻撃、プラント状態攻撃、なりすまし、金融損害、ユニット利用可能性、ユニットトリップ、ユニット寿命の喪失、および少なくとも１つの新しい部品を必要とする資産損害のうちの少なくとも１つに関連付けられる、実施態様１４に記載のシステム（１００，３００，８００）。
［実施態様１７］
産業資産制御システムを保護するコンピュータ化された方法であって、
脅威検出モデル作成コンピュータ（１４０）によって、一連の正常監視ノード値（１７０４）を受信し、一組の正常特徴ベクトル（５１２，１７０８）を生成するステップであって、前記経時的な一連の正常監視ノード値（１７０４）は、前記産業資産制御システムの正常動作を表す、ステップと、
前記脅威検出モデル作成コンピュータ（１４０）によって、一連の脅威監視ノード値（１７０４）を受信し、一組の脅威特徴ベクトル（５１２，１７０８）を生成するステップであって、前記経時的な一連の脅威監視ノード値（１７０４）は、前記産業資産制御システムの脅威を受けている動作を表す、ステップと、
前記一組の正常特徴ベクトル（５１２，１７０８）、前記一組の脅威特徴ベクトル（５１２，１７０８）、および少なくとも１つの初期アルゴリズムパラメータ（１５０４，１６０４）に基づいて、脅威検出モデル（１５５，１４１４）のための少なくとも１つの潜在的判定境界を計算するステップと、
性能メトリック（１５０６，１６０６）に基づいて前記少なくとも１つの潜在的判定境界の性能を評価するステップと、
前記評価の結果に基づいて前記少なくとも１つの初期アルゴリズムパラメータ（１５０４，１６０４）を調整し、前記少なくとも１つの潜在的判定境界を再計算するステップと、
を含む方法。
［実施態様１８］
前記評価、調整、および再計算は、最終調整アルゴリズムパラメータおよび最終判定境界が決定されるまで実行される、実施態様１７に記載の方法。
［実施態様１９］
産業資産制御システムを保護する方法を実行するためにプロセッサ（１４１０）によって実行される命令を格納する非一時的なコンピュータ可読媒体であって、前記方法は、
一連の正常監視ノード値（１７０４）を受信し、一組の正常特徴ベクトル（５１２，１７０８）を生成するステップであって、前記経時的な一連の正常監視ノード値（１７０４）

は、前記産業資産制御システムの正常動作を表す、ステップと、
一連の脅威監視ノード値（１７０４）を受信し、一組の脅威特徴ベクトル（５１２，１７０８）を生成するステップであって、前記経時的な一連の脅威監視ノード値（１７０４）は、前記産業資産制御システムの脅威を受けている動作を表す、ステップと、
前記一組の正常特徴ベクトル（５１２，１７０８）、前記一組の脅威特徴ベクトル（５１２，１７０８）、および少なくとも１つの初期アルゴリズムパラメータ（１５０４，１６０４）に基づいて、脅威検出モデル（１５５，１４１４）のための少なくとも１つの潜在的判定境界を計算するステップと、
性能メトリック（１５０６，１６０６）に基づいて前記少なくとも１つの潜在的判定境界の性能を評価するステップと、
前記評価の結果に基づいて前記少なくとも１つの初期アルゴリズムパラメータ（１５０４，１６０４）を調整し、前記少なくとも１つの潜在的判定境界を再計算するステップと、
を含む、非一時的なコンピュータ可読媒体。
［実施態様２０］
前記評価、調整、および再計算は、最終調整アルゴリズムパラメータおよび最終判定境界が決定されるまで実行される、実施態様１９に記載の媒体。
【符号の説明】
【００７４】
１００　システム
１１０　正常空間データソース
１２０　脅威空間データソース
１３０　監視ノード
１４０　脅威検出モデル作成コンピュータ
１５０　脅威検出コンピュータ
１５５　脅威検出モデル
１７０　遠隔端末
３００　システム
３１０　正常データ
３２０　脅威データ
３３２　発電プラント
３３４　センサ
３３６　電子機器およびプロセッサを備えたコントローラ
３３８　アクチュエータ
３４２　高忠実度物理に基づくモデル
３４４　特徴発見コンポーネント
３４６　判定境界アルゴリズム
３５０　リアルタイム脅威検出プラットフォーム
３５２　監視ノード要素
３５４　正常判定
３５６　位置特定モジュール、位置特定要素
３５８　収容要素
３６０　脅威検出システム
３７０　出力
４１０　圧縮機吐出温度
４１２　ハード境界
４１４　最大境界
４１６　最小境界
４２０　圧縮機圧力比
４３０　圧縮機入口温度
４４０　燃料流量

４５０　発電機出力
４６０　ガスタービン排気温度
５１２　特徴ベクトル、特徴ベクトルの移動
５６２　特徴ベクトルの移動
６１２　圧縮機吐出圧力、信号
６２２　圧縮機圧力比、信号
６３２　圧縮機入口温度、信号
６４２　燃料流量、信号
６６２　ガスタービン排気温度
７００　サイバー攻撃検出システム
７１０　ガスタービン
７２０　負荷正規化機能
７３０　モード処理
７４０　特徴処理
７５０　後処理
７６０　正常／攻撃データセット記憶装置
７７０　判定処理
８００　脅威検出システム、グローバル脅威防止システム
８１０　値
８２０　行列
８３０　特徴量設計コンポーネント
８４０　ローカル特徴ベクトル
８５０　グローバル特徴ベクトル
８６０　相互作用特徴
８７０　異常検出エンジン
９１０　グラフ
９２０　連続境界、判定境界
１１００　ＲＯＣ測定
１１１０　真陽性
１１２０　真陰性
１１３０　偽陽性
１１４０　偽陰性
１２００　最適化フローチャート
１３００　対話型グラフィカル・ユーザ・インターフェース・ディスプレイ
１３１０　現在の特徴ベクトル
１３２０　ユーザ入力領域
１４００　産業資産制御システム保護プラットフォーム
１４１０　プロセッサ
１４１２　プログラム
１４１４　プログラム、脅威検出モデル
１４２０　通信デバイス
１４３０　記憶装置
１４４０　入力デバイス
１４５０　出力デバイス
１５００　ローカルデータベース
１５０２　産業資産識別子、フィールド
１５０４　初期アルゴリズムパラメータ、フィールド
１５０６　性能メトリック、初期アルゴリズムパラメータ、フィールド
１５０８　調整されたアルゴリズムパラメータ、フィールド
１５１０　ローカル特徴および境界、フィールド

１６００　グローバルデータベース
１６０２　産業資産識別子、フィールド
１６０４　初期アルゴリズムパラメータ、フィールド
１６０６　初期アルゴリズムパラメータ、性能メトリック、フィールド
１６０８　アルゴリズムパラメータ、フィールド
１６１０　グローバル特徴および境界、フィールド
１７００　監視ノードデータベース
１７０２　監視ノード識別子、フィールド
１７０４　監視ノード値、フィールド
１７０６　特徴、フィールド
１７０８　特徴ベクトル、フィールド
１７１０　グローバル特徴ベクトル、フィールド
１７１２　判定、フィールド

【図面】

【図１】

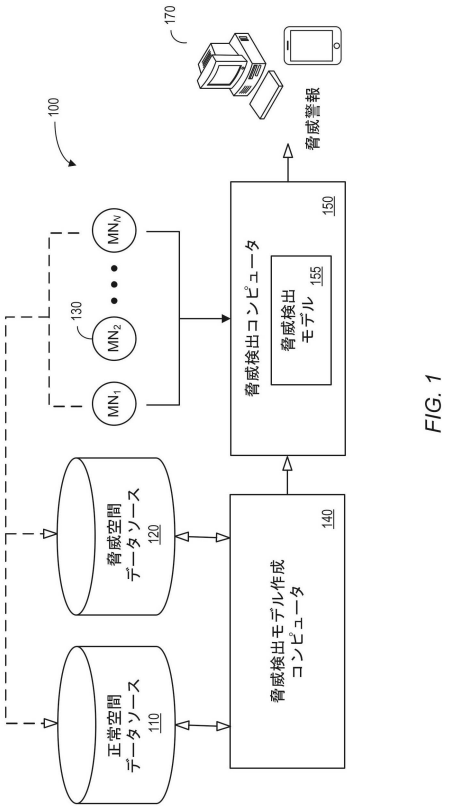


FIG. 1

【図２】

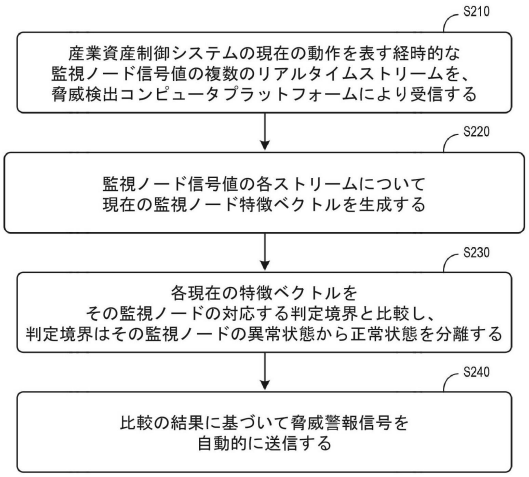


FIG. 2

【図３】

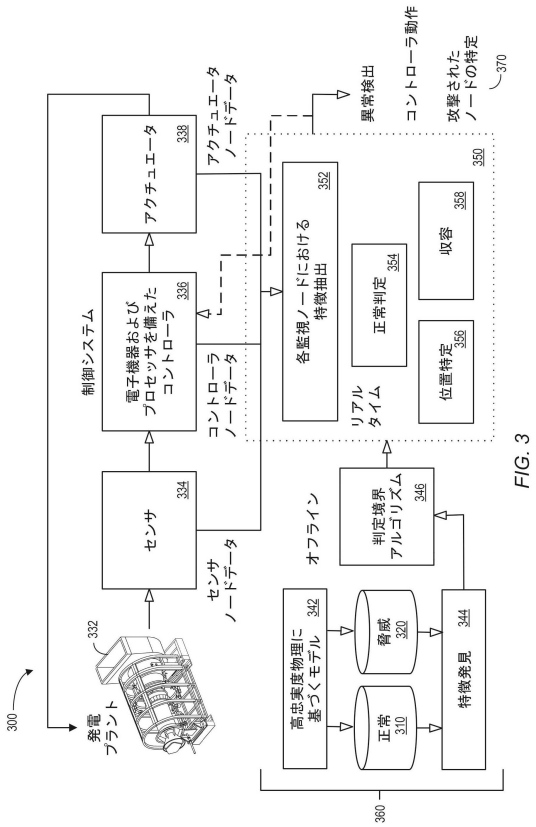


FIG. 3

【図４】

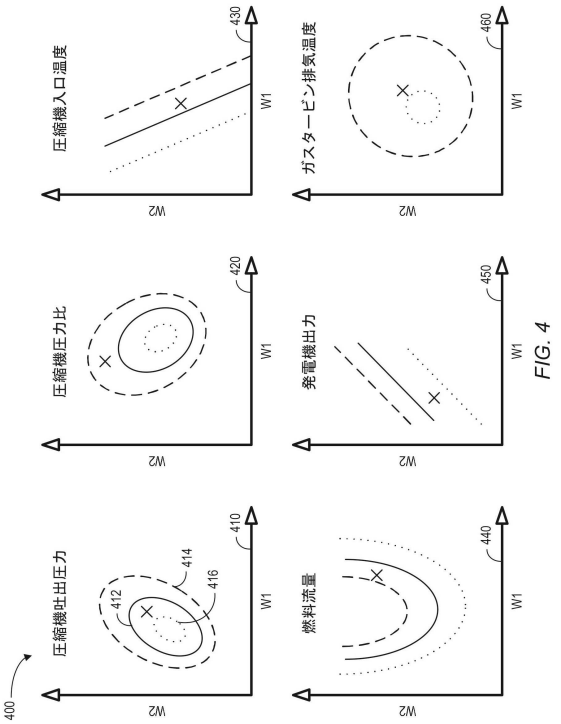


FIG. 4

【図５】

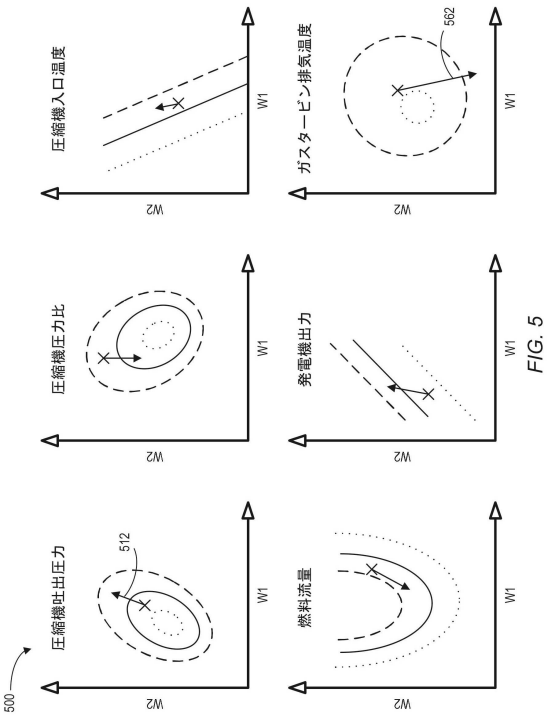


FIG. 5

【図６】

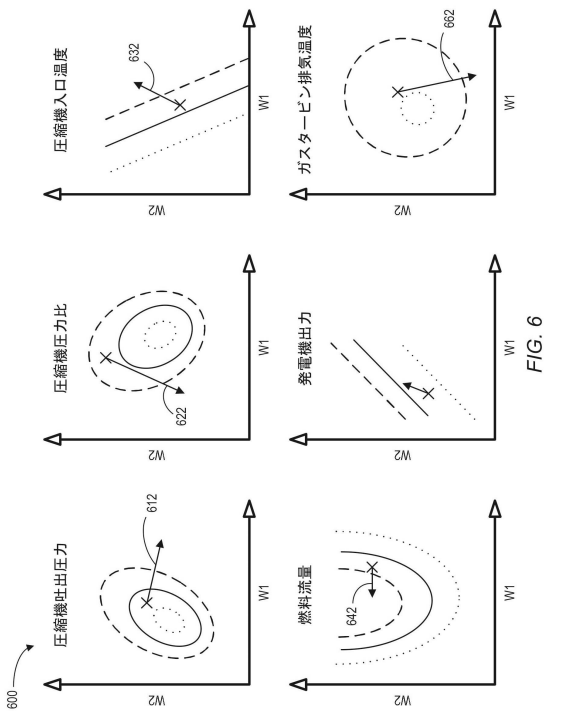


FIG. 6

【図７】

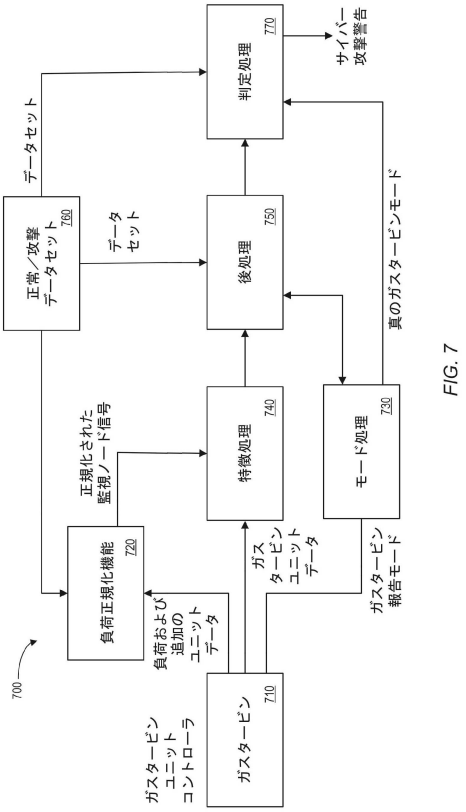


FIG. 7

【図８】

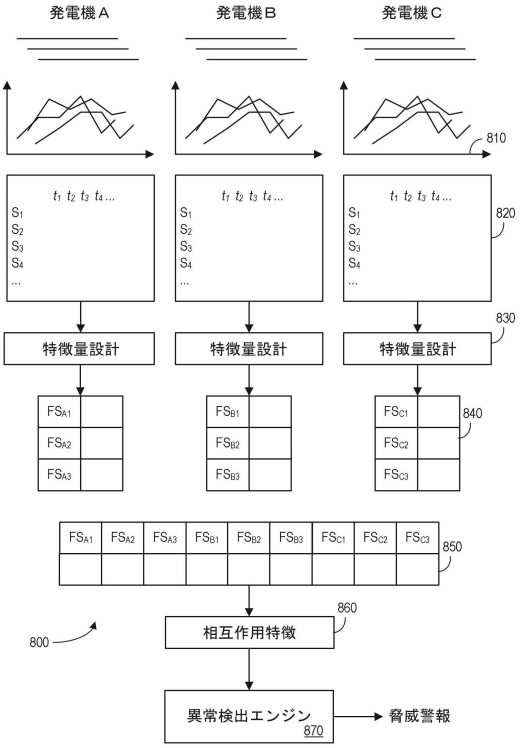


FIG. 8

【図９】

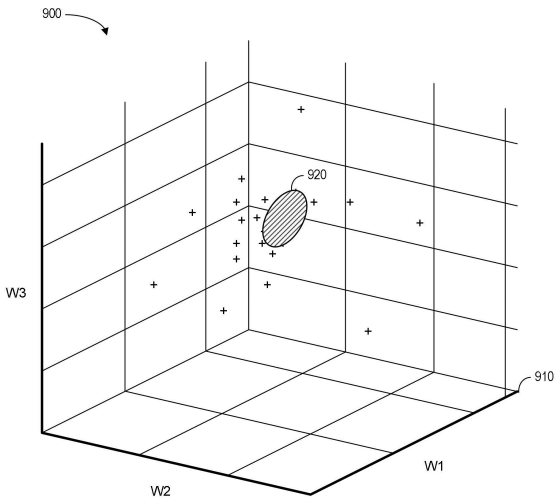


FIG. 9

【図１０】

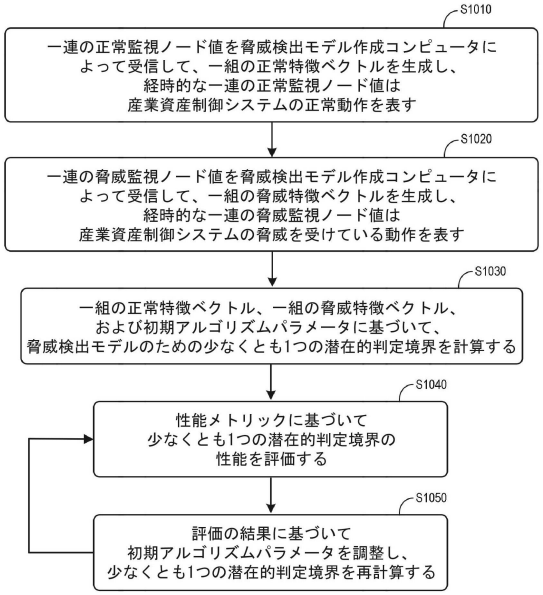


FIG. 10

【図１１】

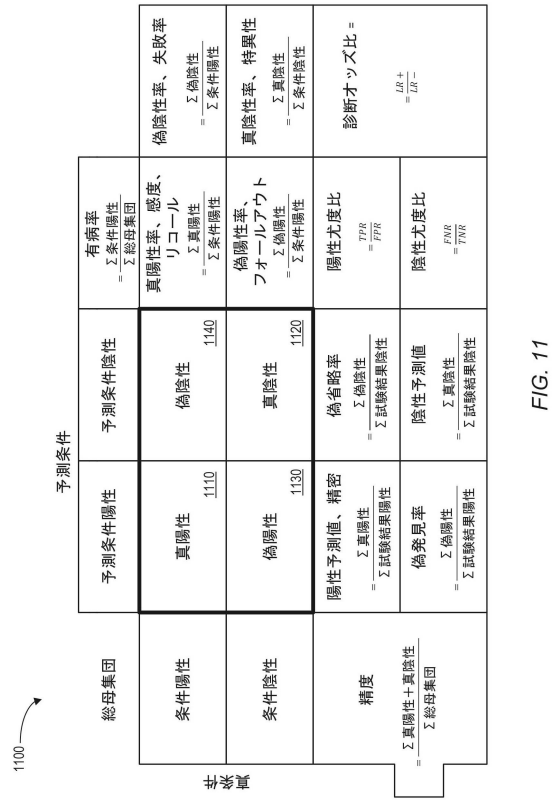


FIG. 11

【図１２】

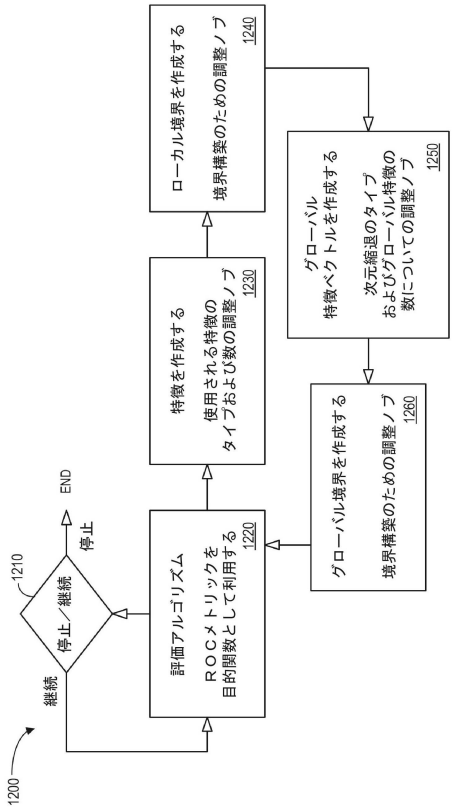


FIG. 12

【図１３】

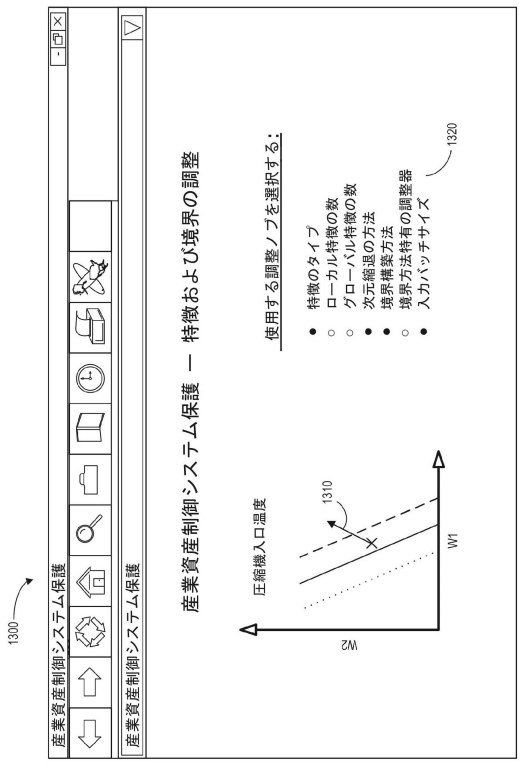


FIG. 13

【図１４】

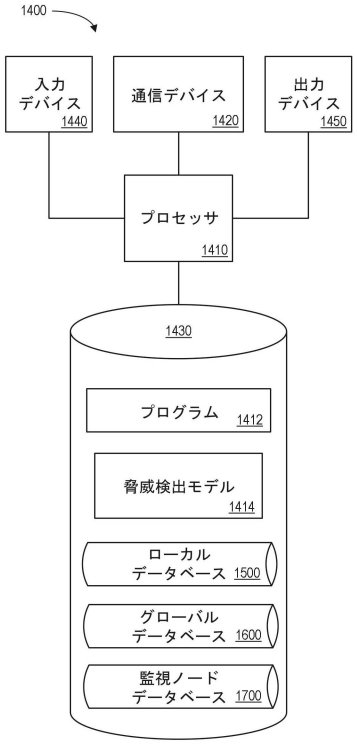
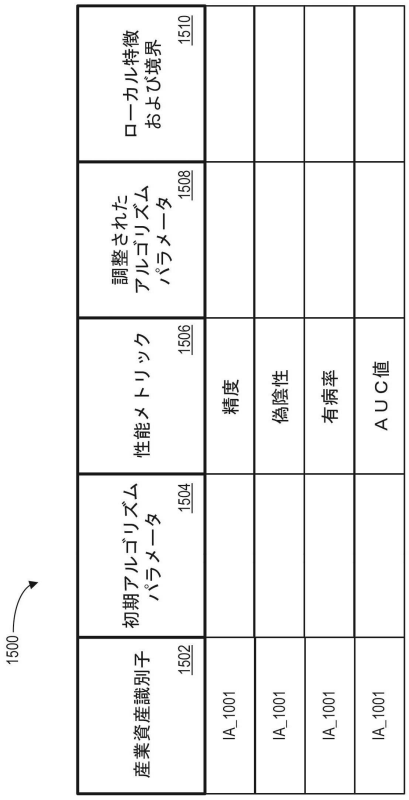


FIG. 14

【図１５】

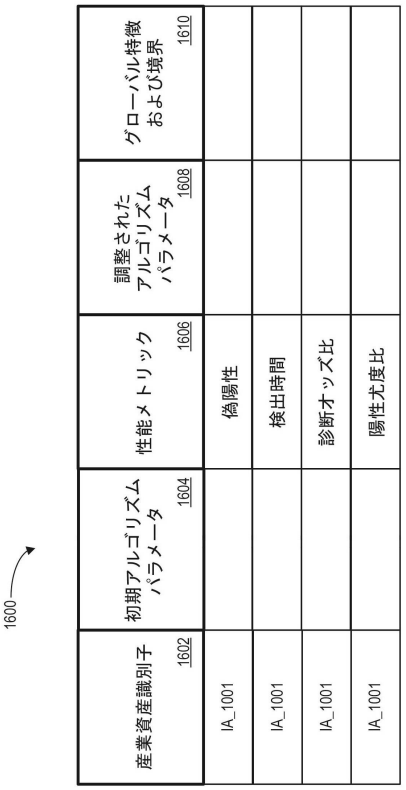


産業資産識別子 1502	初期アルゴリズムパラメータ 1504	性能メトリック 1506	調整されたアルゴリズムパラメータ 1508	ローカル特徴および境界 1510
IA_1001		精度		
IA_1001		偽陰性		
IA_1001		有病率		
IA_1001		AUC値		

1500

FIG. 15

【図１６】

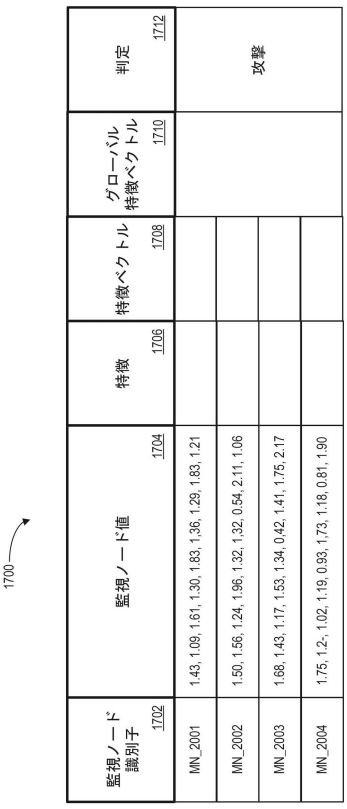


産業資産識別子 1602	初期アルゴリズムパラメータ 1604	性能メトリック 1606	調整されたアルゴリズムパラメータ 1608	グローバル特徴および境界 1610
IA_1001		偽陽性		
IA_1001		検出時間		
IA_1001		診断オッズ比		
IA_1001		陽性尤度比		

1600

FIG. 16

【図１７】



監視ノード識別子 1702	監視ノード値 1704	特徴 1706	特徴ベクトル 1708	グローバル特徴ベクトル 1710	判定 1712
MN_2001	1.43, 1.09, 1.61, 1.30, 1.83, 1.36, 1.29, 1.83, 1.21				攻撃
MN_2002	1.50, 1.56, 1.24, 1.96, 1.32, 1.32, 0.54, 2.11, 1.06				
MN_2003	1.68, 1.43, 1.17, 1.53, 1.34, 0.42, 1.41, 1.75, 2.17				
MN_2004	1.75, 1.2., 1.02, 1.19, 0.93, 1.73, 1.18, 0.81, 1.90				

1700

FIG. 17

フロントページの続き

(72)発明者　ラリト・ケシャブ・メスタ
アメリカ合衆国、ニューヨーク州・１２３０９、ニスカユナ、ワン・リサーチ・サークル
(72)発明者　ジャスティン・バーキー・ジョン
アメリカ合衆国、ニューヨーク州・１２３０９、ニスカユナ、ワン・リサーチ・サークル
(72)発明者　ダニエル・フランシス・ホルツハウアー
アメリカ合衆国、ニューヨーク州・１２３０９、ニスカユナ、ワン・リサーチ・サークル

審査官　宮司 卓佳
(56)参考文献　特表２００７－５０３０３４（ＪＰ，Ａ）
特開２０１４－０９６１４５（ＪＰ，Ａ）
特開２００２－０９０２６７（ＪＰ，Ａ）
特開２０１６－１９２０００（ＪＰ，Ａ）
特開平０２－２７２３２６（ＪＰ，Ａ）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５５
Ｇ０５Ｂ　２３／０２
Ｆ０２Ｃ　９／００