(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7358564号
(P7358564)

(45)発行日　令和5年10月10日(2023.10.10)

(24)登録日　令和5年9月29日(2023.9.29)

(51)国際特許分類
Ｇ０６Ｆ　21/55　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/55

請求項の数　15　外国語出願　（全65頁）

(21)出願番号　特願2022-93754(P2022-93754)
(22)出願日　令和4年6月9日(2022.6.9)
(62)分割の表示　特願2019-514755(P2019-514755)の分割
原出願日　平成29年9月15日(2017.9.15)
(65)公開番号　特開2022-126712(P2022-126712A)
(43)公開日　令和4年8月30日(2022.8.30)
審査請求日　令和4年6月24日(2022.6.24)
(31)優先権主張番号　62/396,016
(32)優先日　平成28年9月16日(2016.9.16)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　62/447,759
(32)優先日　平成29年1月18日(2017.1.18)
最終頁に続く

(73)特許権者　502303739
オラクル・インターナショナル・コーポレイション
アメリカ合衆国カリフォルニア州９４０６５レッドウッド・シティー，オラクル・パークウェイ５００
(74)代理人　110001195
弁理士法人深見特許事務所
(72)発明者　ジョセフ，アジ
アメリカ合衆国、９５１２０ カリフォルニア州、サン・ノゼ、ミノルー・ドライブ、１０７０
(72)発明者　ラオテ，パレシュ
アメリカ合衆国、９４５３８ カリフォルニア州、フリーモント、シャトー・パ
最終頁に続く

(54)【発明の名称】　脅威を検出するための動的ポリシーの導入およびアクセスの可視化

(57)【特許請求の範囲】
【請求項１】
システムであって、
１つ以上のプロセッサおよび非一時的機械可読記憶媒体と、
１つ以上のライブ情報フローを監視するためのプログラム命令とを含み、前記ライブ情報フローは、複数のソースから複数の宛先へのデータフローを含み、
複数のバケットを含むユーザインターフェイスを提供するためのプログラム命令を含み、各バケットは、異なる実行措置に関連し、各バケットは、リアルタイムでトリガされ、前記関連する実行措置を含む現在の実行ポリシーの総数を表示し、
実行ポリシーのトリガに基づいて、前記１つ以上のライブ情報フロー内のセキュリティイベントの発生を判断するためのプログラム命令を含み、前記実行ポリシーは、ソース、宛先、および実行措置の指定を含み、前記１つ以上のライブ情報フロー内の前記データが少なくとも前記実行ポリシーの前記ソースおよび前記宛先と一致する場合、前記実行ポリシーがトリガされ、前記実行措置が適用され、
前記セキュリティイベントの発生を反映するように、（ｉ）前記複数のバケットから、前記実行ポリシーによって適用された前記実行措置に関連するバケットを特定することおよび（ｉｉ）前記実行措置によってリアルタイムでトリガされ、前記特定されたバケットに表示されている現在の実行ポリシーの総数を増やすことによって、前記ユーザインターフェイスを更新するためのプログラム命令を含み、
前記プログラム命令は、前記非一時的機械可読記憶媒体に格納され、前記１つ以上のプ

ロセッサによって実行される、システム。
【請求項２】
前記セキュリティイベントの発生に基づいて、前記特定されたバケットのトレンドインジケータを更新するためのプログラム命令をさらに含み、
前記トレンドインジケータを更新することは、前記特定されたバケットに上向き矢印を表示することを含む、請求項１に記載のシステム。
【請求項３】
前記実行ポリシーの総数を増やすことは、前記実行ポリシーの総数のカウント数ｎをカウント数ｎ＋１に増分することを含む、請求項１または２に記載のシステム。
【請求項４】
前記複数のバケットからバケットの選択に対応するユーザ入力を受け取るためのプログラム命令と、
前記選択されたバケットに対応する前記複数のソースおよび前記複数の宛先を含む前記ライブ情報フローを前記ユーザインターフェイスに表示するためのプログラム命令とをさらに含む、請求項１から３のいずれか１項に記載のシステム。
【請求項５】
前記複数のソースをタグクラウドとして前記ユーザインターフェイスに表示するためのプログラム命令をさらに含み、
前記タグクラウドは、各ソースの使用率に比例して、前記選択されたバケットに対応する前記複数のソースを示す、請求項４に記載のシステム。
【請求項６】
前記データに基づいて動的実行ポリシーを作成するための要求を受け取るためのプログラム命令を含み、前記動的実行ポリシーは、ソース、宛先、実行措置、および前記動的実行ポリシーがアクティブになる期間の指定を含み、
複数のエージェントが前記動的実行ポリシーにアクセスできるように、前記動的実行ポリシーをポリシーバス上に公開するためのプログラム命令と、
前記動的実行ポリシーに基づいて、前記１つ以上のライブ情報フロー内の別のセキュリティイベントに対して前記実行措置を実行するためのプログラム命令とを含み、前記複数のエージェントのうち少なくとも１つのエージェントは、前記実行措置を実行し、
前記別のセキュリティイベントに対して前記実行措置の実行を反映するように、（ｉ）前記複数のバケットから、前記実行ポリシーによって適用された前記実行措置に関連するバケットを特定することおよび（ｉｉ）前記実行措置によってリアルタイムでトリガされ、前記特定されたバケットに表示されている現在の実行ポリシーの総数を増やすことによって、前記ユーザインターフェイスを更新するためのプログラム命令をさらに含む、請求項１から５のいずれか１項に記載のシステム。
【請求項７】
前記動的実行ポリシーがアクティブになる前記期間中に、前記動的実行ポリシーは、前記動的実行ポリシーに含まれた前記ソースおよび前記宛先と同じ指定を含む静的実行ポリシーを上書きする、請求項６に記載のシステム。
【請求項８】
方法であって、
コンピューティングシステムを用いて、１つ以上のライブ情報フローを監視するステップを含み、前記ライブ情報フローは、複数のソースから複数の宛先へのデータフローを含み、
前記コンピューティングシステムを用いて、複数のバケットを含むユーザインターフェイスを提供するステップを含み、各バケットは、異なる実行措置に関連し、各バケットは、リアルタイムでトリガされ、前記関連する実行措置を含む現在の実行ポリシーの総数を表示し、
前記コンピューティングシステムを用いて、実行ポリシーのトリガに基づいて、１つ以上のライブ情報フロー内のセキュリティイベントの発生を判断するステップを含み、前記

実行ポリシーは、ソース、宛先、および実行措置の指定を含み、前記１つ以上のライブ情報フロー内の前記データが少なくとも前記実行ポリシーの前記ソースおよび前記宛先と一致する場合、前記実行ポリシーがトリガされ、前記実行措置が適用され、

前記コンピューティングシステムを用いて、前記セキュリティイベントの発生を反映するように、（ｉ）前記複数のバケットから、前記実行ポリシーによって適用された前記実行措置に関連するバケットを特定することおよび（ｉｉ）前記実行措置によってリアルタイムでトリガされ、前記特定されたバケットに表示されている現在の実行ポリシーの総数を増やすことによって、前記ユーザインターフェイスを更新するステップを含む、方法。

【請求項９】

前記コンピューティングシステムを用いて、前記複数のバケットからバケットの選択に対応するユーザ入力を受け取るステップと、

前記選択されたバケットに対応する前記複数のソースおよび前記複数の宛先を含む前記ライブ情報フローを前記ユーザインターフェイスに表示するステップとをさらに含む、請求項８に記載の方法。

【請求項１０】

前記コンピューティングシステムを用いて、前記複数のソースから特定のソースの選択に対応するユーザ入力を受け取るステップと、

前記コンピューティングシステムを用いて、前記特定のソースから始まる前記ライブ情報フローを表示するステップとをさらに含む、請求項９に記載の方法。

【請求項１１】

前記コンピューティングシステムを用いて、前記複数の宛先から特定の宛先の選択に対応するユーザ入力を受け取るステップと、

前記コンピューティングシステムを用いて、前記特定の宛先で終わる前記ライブ情報フローを表示するステップとをさらに含む、請求項９に記載の方法。

【請求項１２】

前記コンピューティングシステムを用いて、前記複数のソースおよび前記複数の宛先を含む前記ライブ情報フローを前記ユーザインターフェイスに表示するステップと、

前記複数のソースから前記複数の宛先に流れるデータ量に基づいて、一組の上位ソースを示すインジケータを提供するステップとをさらに含む、請求項８から１１のいずれか１項に記載の方法。

【請求項１３】

前記コンピューティングシステムを用いて、前記複数のソースおよび前記複数の宛先を含む前記ライブ情報フローを前記ユーザインターフェイスに表示するステップと、

前記複数のソースから前記複数の宛先に流れるデータ量に基づいて、一組の上位宛先を示すインジケータを提供するステップとをさらに含む、請求項８から１１のいずれか１項に記載の方法。

【請求項１４】

前記コンピューティングシステムを用いて、前記複数のソースおよび前記複数の宛先を含む前記ライブ情報フローを前記ユーザインターフェイスに表示するステップと、

前記複数のソースから前記複数の宛先に流れるデータ量およびポリシーバス上に公開された一組のアクティブな実行ポリシーに基づいて、一組の上位実行ポリシーを示すインジケータを提供するステップとをさらに含む、請求項８から１１のいずれか１項に記載の方法。

【請求項１５】

請求項８から１４のいずれか１項に記載の方法をコンピュータに実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

関連出願の相互参照

本願は、２０１７年１月１８日に出願され、「脅威を検出するためのアクセスの可視化」と題された米国仮出願第６２／４４７７５９号および２０１６年９月１６日に出願され、「脅威を検出するためのアクセスの可視化」と題された米国仮出願第６２／３９６０１６号の優先権および利益を主張し、これらの出願の内容の全体は、あらゆる目的のために参照によって本明細書に組み込まれる。

【背景技術】

【０００２】

背景

本開示は、一般的に脅威検出に関し、より詳しくは動的ポリシーを用いてセキュリティイベントを分析し、能動的脅威と、ユーザ活動と、能動的脅威およびユーザ活動によってトリガされた動的ポリシーとを含む統合ビューを表示するための技術（例えば、システム、方法、１つ以上のプロセッサによって実行可能なコードまたは命令を格納するためのコンピュータプログラム製品）に関する。

【０００３】

コンピュータネットワークは、現代のビジネスにとって重要なツールとなっている。現在では、大量の情報は、このようなネットワークに格納されており、世界中のユーザによって利用されている。殆どの情報がある程度に秘密または機密であるため、情報の保護が必要である。驚くことではないが、権限のない人物および／または装置がコンピュータネットワークおよびコンピュータネットワークに格納されている情報にアクセスする試みを検知するために、様々なネットワークセキュリティ監視装置が開発されている。

【０００４】

ネットワークセキュリティ製品は、主に侵入検知システム（ＩＤＳ）を含み、このような侵入検知システムは、ネットワークベースの侵入検知システム（ＮＩＤＳ）であってもよく、ホストベースの侵入検知システム（ＨＩＤＳ）であってもよい。他のネットワークセキュリティ製品は、ファイアウォール、ルータログ、および様々な他のイベントレポート装置を含む。ネットワークの規模によって、多くの企業は、これらの製品を何百または何千もネットワークに配置している。したがって、ネットワークセキュリティ担当者は、可能なセキュリティ脅威を表すアラームの対応に追われている。殆どの企業は、受け取った全てのアラームを個別に対応できるリソースまたは有資格者を有しない。

【０００５】

したがって、セキュリティイベントを分析し、エンドユーザにとって容易に理解可能な方法でリアルタイムのデータ分析を提示するための脅威視覚化を提供するための技術が望まれている。

【発明の概要】

【課題を解決するための手段】

【０００６】

概要

ユーザ活動が極めて大量（１日あたり数十億のイベント）である場合、静的セキュリティルールは攻撃されやすいユーザ、アプリケーションおよびホストから生じる脅威に対応できないため、脅威インテリジェンスプラットフォームを提供する必要がある。いくつかの実施形態は、リアルタイムの脅威検出および分析を提供することができる。特定の実施形態は、ユーザ、アプリケーションの使用および性能の可視化を提供することができる。いくつかの実施形態は、既存のアクセス制御を利用して、リアルタイムの実行を提供することができる。特定の実施形態は、コンプライアンスを実行し、認可されていないアプリケーションに対するユーザのアクセスをブロックし、ポリシーに基づいて適応型認可およびユーザの認証を行い、プライバシーおよび漏洩を防ぐためにコンテンツ検査を実行することができる。特定の実施形態は、ルールおよび分析論を用いて、リアルタイムの実施を実行することができる。いくつかの実施形態は、リアルタイムで大量のセキュリティデータ（すなわち、１日当たり数十億のイベント）を収集、監視および視覚化することができ、対応する措置を講じることができる。

【０００７】
特に、分散環境内のアクセス可能なリソースへのアクセスを制御するためのシステム、方法、およびコンピュータ可読メモリが開示される。セキュリティイベントを動的に分析し、分散環境内のアクセス可能なリソースへのアクセスを制御し、能動的脅威およびユーザ活動の統合ビューを表示するように構成されたアクセス管理および脅威検出システム並びに情報管理システムを用いて、ＩＤ管理ソリューションを提供するための特定の技術が開示される。様々な実施形態において、システムおよび方法は、（検査ポリシーおよび実行ポリシーを含む）動的なポリシーを作成する能力、動的ポリシーを複数の実行実体に導入および伝達するためのポリシーバスの構想および潜在的には異なる方法でポリシーに動的に対応する実体の能力を含むネットワークアーキテクチャに関する。例えば、様々な実施形態において、脅威検出に基づいて動的アクセスポリシーの用意および実行を行い、リアルタイム脅威モデルに基づいてリアルタイム異常検出を行い、検査ポリシー配信に基づいて動的イベントおよびデータの収集を行い、および脅威レベルに基づいて動的アクセスポリシーの分類を行うための方法およびシステムが提供される。
【０００８】
様々な実施形態において、１つ以上のプロセッサおよび非一時的機械可読記憶媒体と、ユーザ装置、複数のエージェント、収集バス、ポリシーバス、およびリソースを有するターゲットシステムを含む分散環境と、セキュリティイベントに関するデータを収集するためのプログラム命令とを含むシステムが提供される。データは、（ｉ）ユーザまたはユーザ装置を特定するためのソース、および（ｉｉ）ターゲットシステムまたはリソースを特定するための宛先を含み、データは、収集バスによって複数のエージェントのうち少なくとも１つのエージェントから収集される。システムは、データに基づいて動的実行ポリシーを作成するためのプログラム命令をさらに含む。動的実行ポリシーは、ソース、宛先、実行措置、および動的実行ポリシーがアクティブになる期間の指定を含む。システムは、複数のエージェントが動的実行ポリシーにアクセスできるように、動的実行ポリシーをポリシーバス上に公開するためのプログラム命令をさらに含む。動的実行ポリシーがアクティブになる期間中に、動的実行ポリシーは、ソースおよび宛先の指定を含む静的実行ポリシーを上書きする。プログラム命令は、非一時的機械可読記憶媒体に格納され、１つ以上のプロセッサによって実行される。
【０００９】
いくつかの実施形態において、システムは、動的実行ポリシーに基づいて、セキュリティイベントに対して実行措置を実行するためのプログラム命令をさらに含む。複数のエージェントのうち少なくとも１つのエージェントは、実行措置を実行する。
【００１０】
いくつかの実施形態において、期間は、少なくとも５分という所定期間であり、動的実行ポリシーは、所定期間が終了した後に非アクティブになり、ポリシーバスから削除され、静的実行ポリシーは、所定期間中に非アクティブであり、静的実行ポリシーは、所定期間が経過した後にアクティブになる。
【００１１】
いくつかの実施形態において、データの収集は、ポリシーバス上に公開された検査ポリシーによってトリガされ、検査ポリシーは、セキュリティイベントの一組の基準が定義済みパターンと一致するときに、セキュリティイベントに関する一組の定義済み属性であるデータをリアルタイムで収集するためのルールを含む。
【００１２】
いくつかの実施形態において、分散環境は、分析サーバおよび機械学習コンポーネントをさらに含み、検査ポリシーおよび動的実行ポリシーは、分析サーバおよび機械学習コンポーネントによって作成される。
【００１３】
いくつかの実施形態において、システムは、ターゲットシステムまたはリソースの履歴データまたは指定に基づいて検査ポリシーを作成するためのプログラム命令と、複数のエ

ージェントが検査ポリシーにアクセスできるように、検査ポリシーをポリシーバス上に公開するためのプログラム命令とをさらに含む。

【００１４】

いくつかの実施形態において、動的実行ポリシーの作成は、リアルタイムで収集されたデータおよび履歴データを１つ以上のデータクラスタに分類することと、１つ以上のデータクラスタを用いて、一組の定義済み属性を分析することと、分析に基づいて、ソース、宛先、実行措置、および動的実行ポリシーがアクティブになる期間を作成することとを含む。

【００１５】

いくつかの実施形態において、１つ以上のデータクラスタは、教師ありまたは教師なし機械学習またはクラスタリング技術を用いて生成され、分析は、１つ以上のデータクラスタの重心から一組の定義済み属性までの距離を計算することを含み、実行措置は、距離に基づいて決定される。

【００１６】

様々な実施形態において、命令を格納する非一時的機械可読記憶媒体が提供される。これらの命令は、１つ以上のプロセッサによって実行されると、１つ以上のプロセッサにセキュリティイベントに関するデータを収集するステップを含む方法を実行させる。データは、（ｉ）ユーザまたはユーザ装置を特定するためのソース、および（ｉｉ）ターゲットシステムまたはリソースを特定するための宛先を含み、データは、複数のエージェントのうち少なくとも１つのエージェントから収集バスによって収集される。方法は、データに基づいて動的実行ポリシーを作成するステップをさらに含む。動的実行ポリシーは、ソース、宛先、実行措置、および動的実行ポリシーがアクティブになる期間の指定を含む。方法は、複数のエージェントが動的実行ポリシーにアクセスできるように、動的実行ポリシーをポリシーバス上に公開するするステップをさらに含む。方法は、動的実行ポリシーに基づいて、セキュリティイベントに対して実行措置を実行するステップをさらに含み、複数のエージェントのうち少なくとも１つのエージェントは、実行措置を実行する。動的実行ポリシーがアクティブになる期間中に、動的実行ポリシーは、ソースおよび宛先の指定を含む静的実行ポリシーを上書きする。

【００１７】

いくつかの実施形態において、期間は、少なくとも５分という所定期間であり、動的実行ポリシーは、所定期間が終了した後に非アクティブになり、ポリシーバスから削除され、静的実行ポリシーは、所定期間中に非アクティブであり、静的実行ポリシーは、所定期間が経過した後にアクティブになる。

【００１８】

いくつかの実施形態において、データの収集は、ポリシーバス上に公開された検査ポリシーによってトリガされ、検査ポリシーは、セキュリティイベントの一組の基準が定義済みパターンと一致するときに、セキュリティイベントに関する一組の定義済み属性であるデータをリアルタイムで収集するためのルールを含む。

【００１９】

いくつかの実施形態において、検査ポリシーおよび動的実行ポリシーは、分析サーバおよび機械学習コンポーネントによって作成される。

【００２０】

いくつかの実施形態において、方法は、ターゲットシステムまたはリソースの履歴データまたは指定に基づいて、検査ポリシーを作成するステップと、複数のエージェントが検査ポリシーにアクセスできるように、検査ポリシーをポリシーバス上に公開するステップとをさらに含む。

【００２１】

いくつかの実施形態において、動的実行ポリシーを作成するステップは、リアルタイムで収集されたデータおよび履歴データを１つ以上のデータクラスタに分類することと、１つ以上のデータクラスタを用いて、一組の定義済み属性を分析することと、分析に基づい

て、ソース、宛先、実行措置、および動的実行ポリシーがアクティブになる期間を作成することとを含む。

【００２２】

いくつかの実施形態において、１つ以上のデータクラスタは、教師付きまたは教師なし機械学習またはクラスタリング技術を用いて生成され、分析は、１つ以上のデータクラスタの重心から一組の定義済み属性までの距離を計算することを含み、実行措置は、距離に基づいて決定される。

【００２３】

様々な実施形態において、コンピューティングシステムを用いて、セキュリティイベントに関するデータを収集するステップを含む方法が提供される。データは、ｉ）ユーザまたはユーザ装置を特定するためのソース、および（ｉｉ）ターゲットシステムまたはリソースを特定するための宛先を含み、データは、複数のエージェントのうち少なくとも１つのエージェントから収集バスによって収集される。方法は、データに基づいて、動的実行ポリシーを作成するステップをさらに含む。方法は、コンピュータシステムを用いて、データに基づいて動的実行ポリシーを作成するステップをさらに含む。動的実行ポリシーは、ソース、宛先、実行措置、および動的実行ポリシーがアクティブになる期間の指定を含む。方法は、複数のエージェントが動的実行ポリシーにアクセスできるように、コンピューティングシステムを用いて、動的実行ポリシーをポリシーバス上に公開するステップをさらに含む。方法は、コンピューティングシステムを用いて、動的実行ポリシーに基づいてセキュリティイベントに対して実行措置を実行するステップをさらに含み、複数のエージェントのうち少なくとも１つのエージェントは、実行措置を実行する。動的実行ポリシーがアクティブになる期間中に、動的実行ポリシーは、ソースおよび宛先の指定を含む静的実行ポリシーを上書きする。

【００２４】

いくつかの実施形態において、期間は、少なくとも５分という所定期間であり、動的実行ポリシーは、所定期間が終了した後に非アクティブになり、ポリシーバスから削除され、静的実行ポリシーは、所定期間中に非アクティブであり、静的実行ポリシーは、所定期間が経過した後にアクティブになる。

【００２５】

いくつかの実施形態において、データの収集は、ポリシーバス上に公開された検査ポリシーによってトリガされ、検査ポリシーは、セキュリティイベントの一組の基準が定義済みパターンと一致するときに、セキュリティイベントに関する一組の定義済み属性であるデータをリアルタイムで収集するためのルールを含む。

【００２６】

いくつかの実施形態において、方法は、コンピューティングシステムを用いて、ターゲットシステムまたはリソースの履歴データまたは指定に基づいて検査ポリシーを作成するステップと、複数のエージェントが検査ポリシーにアクセスできるように、検査ポリシーをポリシーバス上に公開するステップとをさらに含む。

【００２７】

いくつかの実施形態において、動的実行ポリシーを作成するステップは、リアルタイムで収集されたデータおよび履歴データを１つ以上のデータクラスタに分類することと、１つ以上のデータクラスタを用いて、一組の定義済み属性を分析することと、分析に基づいて、ソース、宛先、実行措置、および動的実行ポリシーがアクティブになる期間を作成することとを含む。

【００２８】

様々な実施形態において、システムおよび方法は、能動的脅威カテゴリ、各脅威カテゴリに対してトリガされたポリシーの数、および関連するトレンドの統合ビューを提供することに関する。特定の実施形態において、１つ以上のプロセッサおよび非一時的機械可読記憶媒体と、１つ以上のライブ情報フローを監視するためのプログラム命令とを含むシステムが提供される。ライブ情報フローは、複数のソースから複数の宛先へのデータフロー

を含む。システムは、複数のバケットを含むユーザインターフェイスを提供するためのプログラム命令をさらに含む。各バケットは、異なる実行措置に関連し、各バケットは、リアルタイムでトリガされ、関連する実行措置を含む現在の実行ポリシーの総数を表示する。システムは、実行ポリシーのトリガに基づいて、１つ以上のライブ情報フロー内のセキュリティイベントの発生を判断するためのプログラム命令をさらに含む。実行ポリシーは、ソース、宛先、および実行措置の指定を含み、１つ以上のライブ情報フロー内のデータが少なくとも実行ポリシーのソースおよび宛先と一致する場合、実行ポリシーがトリガされ、実行措置が適用される。システムは、セキュリティイベントの発生を反映するように、（ｉ）複数のバケットから、実行ポリシーによって適用された実行措置に関連するバケットを特定することおよび（ｉｉ）実行措置によってリアルタイムでトリガされ、特定されたバケットに表示されている現在の実行ポリシーの総数を増やすことによって、ユーザインターフェイスを更新するためのプログラム命令をさらに含む。プログラム命令は、非一時的機械可読記憶媒体に格納され、１つ以上のプロセッサによって実行される。

【００２９】

いくつかの実施形態において、システムは、セキュリティイベントの発生に基づいて、特定されたバケットのトレンドインジケータを更新するためのプログラム命令をさらに含み、トレンドインジケータを更新することは、特定されたバケットに上向き矢印を表示することを含む。

【００３０】

いくつかの実施形態において、実行ポリシーの総数を増やすことは、実行ポリシーの総数のカウント数ｎをカウント数ｎ＋１に増分することを含む。

【００３１】

いくつかの実施形態において、システムは、複数のバケットからバケットの選択に対応するユーザ入力を受け取るためのプログラム命令と、選択されたバケットに対応する複数のソースおよび複数の宛先を含むライブ情報フローをユーザインターフェイスに表示するためのプログラム命令とをさらに含む。

【００３２】

いくつかの実施形態において、システムは、複数のソースをタグクラウドとしてユーザインターフェイスに表示するためのプログラム命令をさらに含む。タグクラウドは、各ソースの使用率に比例して、選択されたバケットに対応する複数のソースを示す。

【００３３】

いくつかの実施形態において、システムは、データに基づいて動的実行ポリシーを作成するための要求を受け取るためのプログラム命令をさらに含む。動的実行ポリシーは、ソース、宛先、実行措置、および動的実行ポリシーがアクティブになる期間の指定を含む。

【００３４】

いくつかの実施形態において、システムは、複数のエージェントが動的実行ポリシーにアクセスできるように、動的実行ポリシーをポリシーバス上に公開するためのプログラム命令をさらに含む。システムは、動的実行ポリシーに基づいて、１つ以上のライブ情報フロー内の別のセキュリティイベントに対して実行措置を実行するためのプログラム命令をさらに含み、複数のエージェントのうち少なくとも１つのエージェントは、実行措置を実行する。システムは、別のセキュリティイベントに対する実行措置の実行を反映するように、（ｉ）複数のバケットから、動的実行ポリシーによって適用された実行措置に関連するバケットを特定することおよび（ｉｉ）実行措置によってリアルタイムでトリガされ、特定されたバケットに表示されている現在の実行ポリシーの総数を増やすことによって、ユーザインターフェイスを更新するためのプログラム命令をさらに含む。

【００３５】

いくつかの実施形態において、動的実行ポリシーがアクティブになる期間中に、動的実行ポリシーは、動的実行ポリシーに含まれた、ソースおよび宛先と同じ指定を含む静的実行ポリシーを上書きする。

【００３６】

様々な実施形態において、命令を格納する非一時的機械可読記憶媒体が提供される。これらの命令は、１つ以上のプロセッサによって実行されると、１つ以上のプロセッサに１つ以上のライブ情報フローを監視するステップを含む方法を実行させる。ライブ情報フローは、複数のソースから複数の宛先へのデータフローを含む。方法は、複数のバケットを含むユーザインターフェイスを提供するステップをさらに含む。各バケットは、異なる実行措置に関連し、各バケットは、リアルタイムでトリガされ、関連する実行措置を含む現在の実行ポリシーの総数を表示する。方法は、複数のバケットを含むユーザインターフェイスを提供するステップをさらに含む。各バケットは、異なる実行措置に関連し、各バケットは、リアルタイムでトリガされ、関連する実行措置を含む現在の実行ポリシーの総数を表示する。方法は、実行ポリシーのトリガに基づいて、１つ以上のライブ情報フロー内のセキュリティイベントの発生を判断するステップをさらに含む。実行ポリシーは、ソース、宛先、および実行措置の指定を含み、１つ以上のライブ情報フロー内のデータが少なくとも実行ポリシーのソースおよび宛先と一致する場合、実行ポリシーがトリガされ、実行措置が適用される。方法は、セキュリティイベントの発生を反映するように、（ｉ）複数のバケットから、実行ポリシーによって適用された実行措置に関連するバケットを特定することおよび（ｉｉ）実行措置によってリアルタイムでトリガされ、特定されたバケットに表示されている現在の実行ポリシーの総数を増やすことによって、ユーザインターフェイスを更新するステップをさらに含む。

【００３７】

いくつかの実施形態において、方法は、複数のバケットからバケットの選択に対応するユーザ入力を受け取るステップと、選択されたバケットに対応する複数のソースおよび複数の宛先を含むライブ情報フローをユーザインターフェイスに表示するステップとをさらに含む。

【００３８】

いくつかの実施形態において、方法は、複数のソースをタグクラウドとしてユーザインターフェイスに表示するステップをさらに含み、タグクラウドは、各ソースの使用率に比例して、選択されたバケットに対応する複数のソースを示す。

【００３９】

いくつかの実施形態において、方法は、データに基づいて動的実行ポリシーを作成するための要求を受け取るステップをさらに含む。動的実行ポリシーは、ソース、宛先、実行措置、および動的実行ポリシーがアクティブになる期間の指定を含む。方法は、複数のエージェントが動的実行ポリシーにアクセスできるように、動的実行ポリシーをポリシーバス上に公開するするステップをさらに含む。方法は、動的実行ポリシーに基づいて、１つ以上のライブ情報フロー内の別のセキュリティイベントに対して実行措置を実行するステップをさらに含み、複数のエージェントのうち少なくとも１つのエージェントは、実行措置を実行する。方法は、別のセキュリティイベントに対する実行措置の実行を反映するように、（ｉ）複数のバケットから、実行ポリシーによって適用された実行措置に関連するバケットを特定することおよび（ｉｉ）実行措置によってリアルタイムでトリガされ、特定されたバケットに表示されている現在の実行ポリシーの総数を増やすことによって、ユーザインターフェイスを更新するステップをさらに含む。

【００４０】

いくつかの実施形態において、動的実行ポリシーがアクティブになる期間中に、動的実行ポリシーは、動的実行ポリシーに含まれた、ソースおよび宛先と同じ指定を含む静的実行ポリシーを上書きする。

【００４１】

いくつかの実施形態において、期間は、少なくとも５分という所定期間であり、動的実行ポリシーは、所定期間が終了した後に非アクティブになり、ポリシーバスから削除され、静的実行ポリシーは、所定期間中に非アクティブであり、静的実行ポリシーは、所定期間が経過した後にアクティブになる。

【００４２】

様々な実施形態において、コンピューティングシステムを用いて、１つ以上のライブ情報フローを監視するステップを含む方法が提供される。ライブ情報フローは、複数のソースから複数の宛先へのデータフローを含む。方法は、コンピューティングシステムを用いて、複数のバケットを含むユーザインターフェイスを提供するステップをさらに含む。各バケットは、異なる実行措置に関連し、各バケットは、リアルタイムでトリガされ、関連する実行措置を含む現在の実行ポリシーの総数を表示する。方法は、コンピューティングシステムを用いて、実行ポリシーのトリガに基づいて、１つ以上のライブ情報フロー内のセキュリティイベントの発生を判断するステップをさらに含む。実行ポリシーは、ソース、宛先、および実行措置の指定を含み、１つ以上のライブ情報フロー内のデータが少なくとも実行ポリシーのソースおよび宛先と一致する場合、実行ポリシーがトリガされ、実行措置が適用される。方法は、コンピューティングシステムを用いて、セキュリティイベントの発生を反映するように、（ｉ）複数のバケットから、実行ポリシーによって適用された実行措置に関連するバケットを特定することおよび（ｉｉ）実行措置によってリアルタイムでトリガされ、特定されたバケットに表示されている現在の実行ポリシーの総数を増やすことによって、ユーザインターフェイスを更新するステップを含む。

【００４３】

いくつかの実施形態において、方法は、コンピューティングシステムを用いて、複数のバケットからバケットの選択に対応するユーザ入力を受け取るステップと、選択されたバケットに対応する複数のソースおよび複数の宛先を含むライブ情報フローをユーザインターフェイスに表示するステップとをさらに含む。

【００４４】

いくつかの実施形態において、方法は、コンピューティングシステムを用いて、複数のソースから特定のソースの選択に対応するユーザ入力を受け取るステップと、コンピューティングシステムを用いて、特定のソースから始まるライブ情報フローを表示するステップとをさらに含む。

【００４５】

いくつかの実施形態において、方法は、コンピューティングシステムを用いて、複数の宛先から特定の宛先の選択に対応するユーザ入力を受け取るステップと、コンピューティングシステムを用いて、特定の宛先で終わるライブ情報フローを表示するステップとをさらに含む。

【００４６】

いくつかの実施形態において、方法は、コンピューティングシステムを用いて、複数のソースおよび複数の宛先を含むライブ情報フローをユーザインターフェイスに表示するステップと、複数のソースから複数の宛先に流れるデータ量に基づいて、一組の上位ソースを示すインジケータを提供するステップとをさらに含む。

【００４７】

いくつかの実施形態において、方法は、コンピューティングシステムを用いて、複数のソースおよび複数の宛先を含むライブ情報フローをユーザインターフェイスに表示するステップと、複数のソースから複数の宛先に流れるデータ量に基づいて、一組の上位宛先を示すインジケータを提供するステップとをさらに含む。

【００４８】

いくつかの実施形態において、方法は、コンピューティングシステムを用いて、複数のソースおよび複数の宛先を含むライブ情報フローをユーザインターフェイスに表示するステップと、複数のソースから複数の宛先に流れるデータ量およびポリシーバス上に公開された一組のアクティブな実行ポリシーに基づいて、一組の上位実行ポリシーを示すインジケータを提供するステップとをさらに含む。

【００４９】

様々な実施形態において、システムおよび方法は、ユーザ、ユーザによってアクセスされているアプリケーション、およびアクセスに関連する可能なアクセスポリシーの統合ビューを提供することに関する。特定の実施形態において、１つ以上のプロセッサおよび非

一時的機械可読記憶媒体と、ライブ情報フローを監視するためのプログラム命令とを含むシステムが提供される。ライブ情報フローは、ソースから宛先へのデータフローを含む。システムは、回線を介して接続されたソースおよび宛先を含むユーザインタフェースを提供するためのプログラム命令と、実行ポリシーのトリガに基づいて、ライブ情報フロー内のセキュリティイベントの発生を判断するためのプログラム命令とをさらに含む。実行ポリシーは、ソース、宛先、および実行措置の指定を含み、１つ以上のライブ情報フロー内のデータが少なくとも実行ポリシーのソースおよび宛先と一致する場合、実行ポリシーがトリガされ、実行措置が適用される。システムは、セキュリティイベントの発生を反映するように、（ｉ）実行ポリシーのインジケータを特定すること、および（ｉｉ）実行ポリシーのインジケータを通過するソースと宛先を接続する回線を表示することによって、ユーザインタフェースを更新するためのプログラム命令をさらに含む。プログラム命令は、非一時的機械可読記憶媒体に格納され、１つ以上のプロセッサによって実行される。

【００５０】

いくつかの実施形態において、ソースは、ユーザインターフェイスのウィンドウの一方側に表示され、宛先は、ソースを有する側と反対するウィンドウの他方側に表示され、実行ポリシーのインジケータは、ソースと宛先との間の回線上に表示される。

【００５１】

いくつかの実施形態において、システムは、１つ以上のライブ情報フローを監視するためのプログラム命令をさらに含む。ライブ情報フローは、（ｉ）複数のソースから複数の宛先へのデータフロー、および（ｉｉ）データによってトリガされた１つ以上の実行ポリシーを含み、ユーザインターフェイスは、（ｉ）複数のソースの各ソースを対応する複数の宛先の各宛先に接続するための１つ以上の回線、および（ｉｉ）各ソースと各宛先との間に流れるデータによってトリガされる実行ポリシーを示す各回線上のインジケータをさらに含む。

【００５２】

いくつかの実施形態において、システムは、複数のソースから特定のソースの選択に対応するユーザ入力を受け取るためのプログラム命令と、ライブ情報フロー内のデータによってトリガされた１つ以上の実行ポリシーを含む特定のソースから始まるライブ情報フローを表示するためのプログラム命令とをさらに含む。

【００５３】

いくつかの実施形態において、システムは、複数の宛先から特定の宛先の選択に対応するユーザ入力を受け取るためのプログラム命令と、ライブ情報フロー内のデータによってトリガされた１つ以上の実行ポリシーを含む特定の宛先で終わるライブ情報フローを表示するためのプログラム命令とをさらに含む。

【００５４】

いくつかの実施形態において、システムは、データに基づいて動的実行ポリシーを作成するための要求を受け取るためのプログラム命令をさらに含む。動的実行ポリシーは、ソース、宛先、実行措置、および動的実行ポリシーがアクティブになる期間の指定を含む。システムは、複数のエージェントが動的実行ポリシーにアクセスできるように、動的実行ポリシーをポリシーバス上に公開するためのプログラム命令をさらに含む。システムは、動的実行ポリシーに基づいて、１つ以上のライブ情報フロー内の別のセキュリティイベントに対して実行措置を実行するためのプログラム命令をさらに含み、複数のエージェントのうち少なくとも１つのエージェントは、実行措置を実行する。システムは、別のセキュリティイベントに対する実行措置の実行を反映するように、（ｉ）実行ポリシーのインジケータを特定することおよび（ｉｉ）実行ポリシーのインジケータを通過するソースと宛先とを接続する回線を表示することによって、ユーザインターフェイスを更新するためのプログラム命令をさらに含む。

【００５５】

いくつかの実施形態において、動的実行ポリシーがアクティブになる期間中に、動的実行ポリシーは、動的実行ポリシーに含まれた、ソースおよび宛先と同じ指定を含む静的実

行ポリシーを上書きする。

【００５６】

様々な実施形態において、命令を格納する非一時的機械可読記憶媒体が提供される。これらの命令は、１つ以上のプロセッサによって実行されると、１つ以上のプロセッサにライブ情報フローを監視するステップを含む方法を実行させる。ライブ情報フローは、ソースから宛先へのデータフローを含む。方法は、回線を介して接続されたソースおよび宛先を含むユーザインタフェースを提供するステップと、実行ポリシーのトリガに基づいて、ライブ情報フロー内のセキュリティイベントの発生を判断するステップとをさらに含む。実行ポリシーは、ソース、宛先、および実行措置の指定を含み、１つ以上のライブ情報フロー内のデータが少なくとも実行ポリシーのソースおよび宛先と一致する場合、実行ポリシーがトリガされ、実行措置が適用される。方法は、セキュリティイベントの発生を反映するように、（ｉ）実行ポリシーのインジケータを特定すること、および（ｉｉ）実行ポリシーのインジケータを通過するソースと宛先を接続する回線を表示することによって、ユーザインタフェースを更新するステップをさらに含む。

【００５７】

いくつかの実施形態において、ソースは、ユーザインターフェイスのウィンドウの一方側に表示され、宛先は、ソースを有する側と反対するウィンドウの他方側に表示され、実行ポリシーのインジケータは、ソースと宛先との間の回線上に表示される。

【００５８】

いくつかの実施形態において、方法は、１つ以上のライブ情報フローを監視するステップをさらに含む。ライブ情報フローは、（ｉ）複数のソースから複数の宛先へのデータフロー、および（ｉｉ）データによってトリガされた１つ以上の実行ポリシーを含み、ユーザインターフェイスは、（ｉ）複数のソースの各ソースを対応する複数の宛先の各宛先に接続するための１つ以上の回線、および（ｉｉ）各ソースと各宛先との間に流れるデータによってトリガされる実行ポリシーを示す各回線上のインジケータをさらに含む。

【００５９】

いくつかの実施形態において、方法は、複数のソースから特定のソースの選択に対応するユーザ入力を受け取るステップと、ライブ情報フロー内のデータによってトリガされた１つ以上の実行ポリシーを含む特定のソースから始まるライブ情報フローを表示するステップとをさらに含む。

【００６０】

いくつかの実施形態において、方法は、複数の宛先から特定の宛先の選択に対応するユーザ入力を受け取るステップと、ライブ情報フロー内のデータによってトリガされた１つ以上の実行ポリシーを含む特定の宛先で終わるライブ情報フローを表示するステップとをさらに含む。

【００６１】

いくつかの実施形態において、方法は、データに基づいて動的実行ポリシーを作成するための要求を受け取るステップをさらに含む。動的実行ポリシーは、ソース、宛先、実行措置、および動的実行ポリシーがアクティブになる期間の指定を含む。方法は、複数のエージェントが動的実行ポリシーにアクセスできるように、動的実行ポリシーをポリシーバス上に公開するするステップをさらに含む。方法は、動的実行ポリシーに基づいて、１つ以上のライブ情報フロー内の別のセキュリティイベントに対して実行措置を実行するステップをさらに含み、複数のエージェントのうち少なくとも１つのエージェントは、実行措置を実行する。方法は、別のセキュリティイベントに対する実行措置の実行を反映するように、（ｉ）実行ポリシーのインジケータを特定することおよび（ｉｉ）実行ポリシーのインジケータを通過するソースと宛先とを接続する回線を表示することによって、ユーザインターフェイスを更新するステップをさらに含む。

【００６２】

いくつかの実施形態において、動的実行ポリシーがアクティブになる期間中に、動的実行ポリシーは、動的実行ポリシーに含まれた、ソースおよび宛先と同じ指定を含む静的実

行ポリシーを上書きする。

【００６３】

様々な実施形態において、コンピューティングシステムを用いて、ライブ情報フローを監視することを含む方法が提供される。ライブ情報フローは、ソースから宛先へのデータフローを含む。方法は、コンピューティングシステムを用いて、回線を介して接続されたソースおよび宛先を含むユーザインタフェースを提供するステップと、コンピューティングシステムを用いて、実行ポリシーのトリガに基づいて、ライブ情報フロー内のセキュリティイベントの発生を判断するステップとをさらに含む。実行ポリシーは、ソース、宛先、および実行措置の指定を含み、１つ以上のライブ情報フロー内のデータが少なくとも実行ポリシーのソースおよび宛先と一致する場合、実行ポリシーがトリガされ、実行措置が適用される。方法は、コンピューティングシステムを用いて、セキュリティイベントの発生を反映するように、（ｉ）実行ポリシーのインジケータを特定すること、および（ｉｉ）実行ポリシーのインジケータを通過するソースと宛先を接続する回線を表示することによって、ユーザインタフェースを更新するステップをさらに含む。

【００６４】

いくつかの実施形態において、ソースは、ユーザインターフェイスのウィンドウの一方側に表示され、宛先は、ソースを有する側と反対するウィンドウの他方側に表示され、実行ポリシーのインジケータは、ソースと宛先との間の回線上に表示される。

【００６５】

いくつかの実施形態において、方法は、コンピューティングシステムを用いて、１つ以上のライブ情報フローを監視するステップをさらに含む。ライブ情報フローは、（ｉ）複数のソースから複数の宛先へのデータフロー、および（ｉｉ）データによってトリガされた１つ以上の実行ポリシーを含む。ユーザインターフェイスは、（ｉ）複数のソースの各ソースを対応する複数の宛先の各宛先に接続するための１つ以上の回線、および（ｉｉ）各ソースと各宛先との間に流れるデータによってトリガされる実行ポリシーを示す各回線上のインジケータをさらに含む。

【００６６】

いくつかの実施形態において、方法は、コンピューティングシステムを用いて、複数のソースから特定のソースの選択に対応するユーザ入力を受け取るステップと、コンピューティングシステムを用いて、ライブ情報フロー内のデータによってトリガされた１つ以上の実行ポリシーを含む特定のソースから始まるライブ情報フローを表示するステップとをさらに含む。

【００６７】

いくつかの実施形態において、方法は、コンピューティングシステムを用いて、複数の宛先から特定の宛先の選択に対応するユーザ入力を受け取るステップと、コンピューティングシステムを用いて、ライブ情報フロー内のデータによってトリガされた１つ以上の実行ポリシーを含む特定の宛先で終わるライブ情報フローを表示するステップとをさらに含む。

【００６８】

いくつかの実施形態において、方法は、コンピューティングシステムを用いて、データに基づいて動的実行ポリシーを作成するための要求を受け取るステップをさらに含む。動的実行ポリシーは、ソース、宛先、実行措置、および動的実行ポリシーがアクティブになる期間の指定を含む。方法は、コンピューティングシステムを用いて、複数のエージェントが動的実行ポリシーにアクセスできるように、動的実行ポリシーをポリシーバス上に公開するするステップをさらに含む。方法は、コンピューティングシステムを用いて、動的実行ポリシーに基づいて、１つ以上のライブ情報フロー内の別のセキュリティイベントに対して実行措置を実行するステップをさらに含み、複数のエージェントのうち少なくとも１つのエージェントは、実行措置を実行する。方法は、コンピューティングシステムを用いて、別のセキュリティイベントに対する実行措置の実行を反映するように、（ｉ）実行ポリシーのインジケータを特定することおよび（ｉｉ）実行ポリシーのインジケータを通

過するソースと宛先とを接続する回線を表示することによって、ユーザインターフェイスを更新するステップをさらに含む。

【図面の簡単な説明】

【００６９】

【図１】いくつかの実施形態に従って、高レベル脅威インテリジェンスプラットフォームを示す簡略ブロック図である。

【図２】いくつかの実施形態に従って、情報管理システムの詳細アーキテクチャを示す簡略ブロック図である。

【図３】いくつかの実施形態に従って、脅威視覚化システムの一部の機能要素を示す簡略ブロック図である。

【図４Ａ】いくつかの実施形態に従って、能動的脅威カテゴリを表示するためのユーザインターフェイス（ＵＩ）を示す図である。

【図４Ｂ】いくつかの実施形態に従って、能動的脅威カテゴリを表示するためのユーザインターフェイス（ＵＩ）を示す図である。

【図５】いくつかの実施形態に従って、能動的脅威カテゴリを表示するための追加ＵＩを示す図である。

【図６】いくつかの実施形態に従って、能動的脅威カテゴリを表示するための追加ＵＩを示す図である。

【図７】いくつかの実施形態に従って、能動的脅威カテゴリを表示するための追加ＵＩを示す図である。

【図８】いくつかの実施形態に従って、能動的脅威カテゴリを表示するための追加ＵＩを示す図である。

【図９】いくつかの実施形態に従って、能動的脅威カテゴリを表示するための追加ＵＩを示す図である。

【図１０】いくつかの実施形態に従って、能動的脅威カテゴリを表示するための追加ＵＩを示す図である。

【図１１】いくつかの実施形態に従って、能動的脅威カテゴリを表示するための追加ＵＩを示す図である。

【図１２Ａ】いくつかの実施形態に従って、管理者が１つ以上のポリシーを作成することを可能にするためのＵＩを示す図である。

【図１２Ｂ】いくつかの実施形態に従って、管理者が１つ以上のポリシーを作成することを可能にするためのＵＩを示す図である。

【図１３】いくつかの実施形態に従って、能動的脅威カテゴリを表示するための追加ＵＩを示す図である。

【図１４】いくつかの実施形態に従って、能動的脅威カテゴリを表示するための追加ＵＩを示す図である。

【図１５】いくつかの実施形態に従って、能動的脅威カテゴリを表示するための追加ＵＩを示す図である。

【図１６】いくつかの実施形態に従って、能動的脅威カテゴリを表示するための追加ＵＩを示す図である。

【図１７】いくつかの実施形態に従って、トリガされたポリシーに基づいて能動的脅威を表示するためのＵＩを示す図である。

【図１８】いくつかの実施形態に従って、様々なソースの追跡活動を表示するためのＵＩを示す図である。

【図１９】いくつかの実施形態に従って、分散環境において動的実行ポリシーをポリシーバス上に公開するためのプロセスを示すフローチャートである。

【図２０】いくつかの実施形態に従って、能動的脅威カテゴリ、各脅威カテゴリのためにトリガされたポリシーの数および関連するトレンドの統合ビューを提供するためのプロセスを示すフローチャートである。

【図２１】ユーザ、ユーザによってアクセスされたアプリケーション、およびアクセスに

関連する可能なアクセスポリシーの統合ビューを提供するためのプロセスを示すフローチャートである。
【図２２】本開示のいくつかの実施形態を実施するために使用され得る分散システムを示す簡略ブロック図である。
【図２３】いくつかの実施形態に従って、サービスをクラウドサービスとして提供することができるシステム環境の１つ以上の構成要素を示す簡略ブロック図である。
【図２４】本開示のいくつかの実施形態を実施するために使用され得る例示的なコンピュータシステムを示す図である。
【発明を実施するための形態】
【００７０】
詳細な説明
Ｉ．序論
以下の開示は、リアルタイムの脅威検出および分析を提供することができる脅威インテリジェンスプラットフォームを説明する。様々な実施形態において、提供されたシステムは、プロセッサと、命令を格納するメモリとを含む。これらの命令は、プロセッサによって実行されると、エージェントから、少なくとも宛先とソースとを含むセキュリティイベントを受信することと、セキュリティイベントがポリシーと一致するときに当該ポリシーをトリガすることとをプロセッサに実行させ、当該ポリシーは、ソース、宛先および実行措置の指定を含み、当該ポリシーに基づいてセキュリティイベントに対して実行措置を実行することと、トリガされたポリシーを介してセキュリティイベントのソースと宛先とをリンクするようにユーザインターフェイスを更新することとをプロセッサに実行させる。しかしながら、ある実体（例えば、会社、国）において、数千または数十万の従業員および他の個人（例えば、ユーザ、顧問、ゲスト）は、常にネットワークを通じて様々なサービス（例えば、ソース）にアクセスしているため、セキュリティイベントを引き起こす。人々が多種多様なサービスにアクセスしようとするときに、様々なアクセス違反およびパスワードエラーなどが生じるため、監視を行う必要がある。現在では、セキュリティポリシー内の静的セキュリティルールは、攻撃されやすいユーザ、攻撃されやすいアプリケーションおよび攻撃されやすいホストに対して進化し続ける脅威には対応できない。ユーザ活動が極めて大量（例えば、１日当たり数十億のイベント）である場合、ユーザインターフェイスを用いた手動分析または自家製分析は、費用上非常に高くなる。また、非常に多くのユーザに対して、非常に正確な自動パターン検出を行い、権限のないユーザがサービスにアクセスすることを防ぐことは、困難であろう。
【００７１】
これらの問題に対処するために、様々な実施形態は、動的ポリシーを用いてセキュリティイベントを分析し、能動的脅威と、ユーザ活動と、能動的脅威およびユーザ活動によってトリガされた動的ポリシーとを含む統合ビューを表示するための技術（例えば、システム、方法、１つ以上のプロセッサによって実行可能なコードまたは命令を格納するコンピュータプログラム製品）を提供する。いくつかの実施形態は、ユーザアクセスを追跡し、リアルタイムで情報を収集することによって、パターンを特定し、分析を生成し、対応する修正措置を講じることができる。リアルタイムまたはほぼリアルタイムでデータを収集することによって、これらのデータに基づいて決定された修正措置を直ちに適用することができる。例えば、アプリケーションに対してユーザを認証する時に、権限のないユーザがコンテンツにアクセスすることを防ぐための措置を講じるための時間が短い（例えば、ミリ秒）であろう。追加または代替の実施形態において、リアルタイムまたはほぼリアルタイムでデータを収集し、これらのデータの履歴を保存することによって、リアルタイムデータおよび履歴データに基づいて決定された修正措置を適用することによって、ユーザを認証した後でも、権限のないユーザがアクセスできないように防ぐことができ、そのユーザをネットワークから追い出すことができる。
【００７２】
いくつかの実施形態は、ユーザＩＤ、リソースの使用パターンおよび性能特性を可視化

することができる。特定の実施形態は、特定のアクセス制御を利用して、リアルタイムの実施を提供することができる。例えば、特定の実施形態は、コンプライアンスを実行しまたは認可されていないアプリケーションに対するユーザのアクセスをブロックし、適応型認可を実行し、ポリシーに基づいてユーザの認証を行い、およびプライバシーおよび漏洩を防ぐためのコンテンツ検査を実行することができる。特定の実施形態は、動的ルールおよび分析を使用してリアルタイムの実行を提供することができる。いくつかの実施形態は、エンドユーザにとって容易に理解可能な方法でリアルタイムのデータ分析を提示するための脅威視覚化を提供することができる。大量のデータを要約し、分析データをリアルタイム且つ有意義な方法で提示することによって、エンドユーザは、実行可能な項目を特定することができ、適切なポリシーを確実に更新すると共に、特定のポリシーを確実に実行することができる。

【００７３】

一例において、ユーザがユーザ名およびパスワードをログインページに入力して、これらのユーザ認証情報を送信すると、これらのユーザ認証情報は、リアルタイムまたはほぼリアルタイムでデータ収集バスに送信される。いくつかの例において、チューニングパラメータ（例えば、収集バスがクラウドに位置するか否か）に応じて、１秒または３０ミリ秒未満でデータの収集および送受信を行うことができる。ネットワークの遅延（例えば、エージェントが情報を収集するホストマシンに位置し、データ収集バスが別のマシン、例えばクラウドに位置する場合）を除いて、データの転送は、殆ど遅延なく（すなわち、ほぼリアルタイムで）行われる。しかしながら、ユーザが認証情報を入力するときに、システムは、これらの認証情報が特定のサーバから来たものか否かを判断し、疑わしい活動がある場合に、追加認証をユーザに提示する必要があるか否かを判断することができる。ユーザがページにアクセスしている時に、システムは、認証情報が有効であってもユーザが認可されるべきではないと判断した場合、そのページにアクセスできないようにユーザを追い出すことができる。

【００７４】

いくつかの実施形態において、ユーザがアカウントにログインした後に、ウエブプロキシは、ユーザの活動および行動を絶えず監視および学習することができ、異常をトリガすることができる（それによって、ユーザに追加認証を提示する）。例えば、ユーザは、多額の資金を送金しようとする。この動作は、システムをトリガして、ユーザに追加認証を提示する。特定の実施形態において、プロキシは、別の情報源（例えば、トラフィックフロー）を提供することができ、収集されたデータは、リアルタイムで供給され、分析される。ユーザが保護されたアプリケーションまたはエージェントによって保護されていないクラウドアプリケーションにアクセスする場合、プロキシサーバは、ユーザの活動、例えばユーザが特定のウエブサイトにアクセスして情報をダウンロードすることを判断することができる。プロキシサーバは、ユーザの活動を監視し、収集されたデータに基づいてユーザがブラックリストに登録されているという情報を提供することができる。さらに、プロキシは、履歴情報を提供することができる。これによって、ユーザが新しいサイトにアクセスする場合、ユーザにアクセス権を付与するときにそのユーザに関する履歴情報を考慮することができる。

【００７５】

いくつかの実施形態は、利用可能なリアルタイムデータをリアルタイム可視化サーバに供給し、リアルタイムで分析結果を顧客に提示することができる。リアルタイムでデータを顧客に提供する場合、リアルタイム分析結果に応じて、迅速に措置を決定することができる。いくつかの実施形態は、データを記憶し、記憶されたデータまたは履歴データを用いて、リアルタイムで適用できる追加のルールおよびポリシーを作成することができる。履歴データをマイニングすることによって、特定の実施形態は、履歴データに基づいて実行ポリシーを作成することができる。特定の実施形態は、履歴データおよびリアルタイムで得られた分析結果の両方を用いて、異常をトリガすることができる。有利には、これらの手法は、リアルタイムで非常に大量のセキュリティデータ（すなわち、数十億のストリ

ーミングイベント）を収集、監視および視覚化することができ、対応する措置を講じることができる。

【００７６】

ＩＩ．脅威を検出するためのシステムアーキテクチャ

図１は、本開示の少なくとも１つの実施形態に従って、ユーザからの異常アクセス要求を検出することによって、リアルタイムで脅威を検出するためのシステム１００の態様を示している。いくつかの実施形態において、システム１００は、分散環境においてネットワーク１２０を介してユーザ装置１１５に通信可能に接続されたアクセス管理および脅威検出システム１０５と情報管理システム１１０とを含む。アクセス管理および脅威検出システム１０５と情報管理システム１１０とは、ＩＤアクセスマネージャの一部である。ＩＤアクセスマネージャの一部として様々な種類のエージェントが存在しており、これらのエージェントは、ウエブサーバまたはアプリケーションへのアクセスを保護する。例えば、ユーザがメールサーバまたはドキュメントサーバにアクセスしようとするときに、サーバ（例えば、ＯＡＭ（Oracle Access Manager）サーバ）と通信する保護エージェントが存在する。このエージェントは、例えば、ＩＤに関連する認証情報を検証することによって、そのユーザがこのサーバにアクセスできるか否かを検証する。特定の実施形態は、拡張エージェントおよびアクセスマネージャサーバを有することができる。したがって、ユーザがデータを要求しているときに、誰かが何かにアクセスしている情報は、情報管理システム１１０のデータ収集エンジンにリアルタイムで送信される。

【００７７】

ネットワーク１２０は、ユーザ装置１１５と、アクセス管理および脅威検出システム１０５と、情報管理システム１１０との間の通信およびデータ交換を容易にすることができる。ネットワーク１２０は、ＴＣＰ／ＩＰ、ＳＮＡ、ＩＰＸ、AppleTalkなどを含むがこれらに限定されない様々な市販プロトコルのいずれかを使用してデータ通信をサポートすることができ、当業者に知られている任意種類のネットワークであってもよい。単なる一例として、ネットワーク１１５は、イーサネット（登録商標）ネットワーク、トークンリングネットワークなどのローカルエリアネットワーク（ＬＡＮ）、広域ネットワーク、仮想プライベートネットワーク（ＶＰＮ）を含むがこれに限定されない仮想ネットワーク、インターネット、イントラネット、エクストラネット、公衆交換電話ネットワーク（ＰＳＴＮ）、赤外線ネットワーク、無線ネットワーク（たとえば、ＩＥＥＥ８０２．１Ｘプロトコルスイート、当該分野に知られているBluetooth（登録商標）プロトコル、および／または任意の他の無線プロトコルの下で動作するネットワーク）および／またはこれらのネットワークと他のネットワークの組み合わせであってもよい。

【００７８】

ユーザ装置１１０は、（例えば、様々なバージョンのMicrosoft Windows（登録商標）および／またはApple Macintosh（登録商標）オペレーティングシステムを実行するパーソナルコンピュータおよび／またはラップトップコンピュータを含む）汎用パーソナルコンピュータ、（例えば、Microsoft Windows Mobile（登録商標）などのソフトウェアを実行し、インターネット、電子メール、ＳＭＳ、ブラックベリー（登録商標）または他の通信プロトコルが有効化された）携帯電話またはＰＤＡ、（様々なＧＮＵ／Ｌｉｎｕｘ（登録商標）オペレーティングシステムを含むがこれに限定されない）市販のＵＮＩＸ（登録商標）またはＵＮＩＸに類似する様々なオペレーティングシステムを実行するワークステーションコンピュータ、または他のコンピューティング装置であってもよい。例えば、ユーザ装置１１０は、ネットワーク（例えば、ネットワーク１１５）を介して通信可能なシンクライアントコンピュータ、インターネット対応ゲームシステム、および／またはパー
ソナルメッセージング装置などの他の電子装置であってもよい。例示的なシステム環境１００は、１つのユーザ装置を備えると示されているが、他の実施形態において、任意の数のユーザ装置および／またはクライアントコンピューティング装置をサポートすることができる。

【００７９】
アクセス管理および脅威検出システム１０５は、１つ以上のコンピュータおよび／またはサーバを含んでもよい。これらのコンピュータおよび／またはサーバは、汎用コンピュータ、（例示として、ＰＣサーバ、ＵＮＩＸ（登録商標）サーバ、ミッドレンジサーバ、メインフレームコンピュータ、ラックマウントサーバを含む）専用サーバコンピュータ、サーバファーム、サーバクラスタ、または任意の他の適切な構成および／または組み合わせであってもよい。アクセス管理および脅威検出システム１０５を構成するコンピューティング装置は、任意のオペレーティングシステムまたはＨＴＴＰサーバ、ＦＴＰサーバ、ＣＧＩサーバ、Ｊａｖａ（登録商標）サーバ、データベースサーバなどを含む様々な追加のサーバアプリケーションおよび／または中間層アプリケーションを実行することができる。例示的なデータベースサーバは、Oracle（登録商標）、Microsoft（登録商標）、Sybase（登録商標）、IBM（登録商標）などの会社から市販されているものを含むがこれらに限定されない。
【００８０】
様々な実施形態において、アクセス管理および脅威検出システム１０５は、組織の１つ以上のターゲットシステム１３０によって提供されたリソース１２５を保護するように動作可能な１つ以上の要素を含むことができる。いくつかの実施形態において、「ターゲットシステム」は、１つ以上のリソースを提供するまたは含む任意のシステムを指すことがある。ターゲットシステム１３０によって提供されたローカルまたはリモートにアクセス可能なリソース１２５は、ソフトウェア製品、アプリケーション（例えば、クラウドアプリケーション、エンタープライズアプリケーションまたは他のアプリケーション）、クラウドサービス、様々な種類のデータ（例えば、ネットワークファイル、ディレクトリ情報、データベースなど）および他のリソースを含む様々な種類のものであってもよい。ターゲットシステム１３０は、１つ以上のデータベース、ライトウェイトディレクトリアクセスプロトコル（ＬＤＡＰ）サーバ、アクティブディレクトリ（ＡＤ）システム、電子メールシステム、ＵＮＩＸシステムなどを含むことができる。例えば、ターゲットシステム１３０は、アクティブディレクトリサーバにアクセスするように、アクティブディレクトリサービスへのアクセスを提供するアクティブディレクトリ（ＡＤ）システムであってもよい。いくつかの例において、ターゲットシステム１３０は、会議室にアクセスを提供するコンピューティングシステム、例えばバッジを使用して会議室にアクセスを提供するコンピューティングシステムであってもよい。いくつかの実施形態において、ターゲットシステム１３０は、アプリケーションインスタンスとして呼ばれてもよい。
【００８１】
特定の実施形態において、ターゲットシステム１３０によって提供されたリソース１２５へのアクセスは、ターゲットシステム１３０内の様々な種類のアカウントを用いて管理することができる。ターゲットシステム１３０によって提供されたリソース１２５に基づいて、ターゲットシステム１３０にアカウントを作成することができる。アカウントは、ユーザアカウント、管理アカウント、アプリケーションアカウントなどの様々な種類のアカウントを含んでもよい。各種類のアカウントは、ターゲットシステム１３０によって提供された１つ以上のリソース１２５に対して特定のアクセスレベルを付与する。ユーザがターゲットシステム１３０にアクセスまたはログインすることを可能にするために、ターゲットシステム１３０は、各々のアカウント（例えば、ユーザアカウント、管理アカウントおよび／またはアプリケーションアカウント）を含むことができる。ユーザまたはユーザグループ（例えば、組織）のＩＤに基づいて、ユーザまたはユーザグループにアカウントを作成または用意することができる。特定種類のリソースにアクセスするように、ユーザまたはユーザグループに特定種類のアカウントを与えることができる。例えば、ユーザに与えられたExchangeサーバ上の電子メールアカウントは、Exchangeリソース用のアカウントである。ユーザに複数のアカウントを与えることができ、各種類のアカウントが各種類のリソースに対応する。例えば、ユーザは、ターゲットシステム１３０にログインして、異なる種類の操作を行うために、２つの異なるアカウントを有することができる。例

えば、ターゲットシステム１３０は、電子メール交換サーバをホストし、電子メールアカウントを提供することができる。また、同じターゲットシステム１３０は、人事（ＨＲ）システムをホストし、ＨＲシステムに関連する管理機能を実行するためのＨＲ管理アカウントを提供することができる。特定のユーザは、ターゲットシステム１３０上に電子メールアカウントを有すると共に、ターゲットシステム１３０上にＨＲ管理アカウントを有することができる。電子メールアカウントでログインする場合、ユーザは、電子メールにアクセスすることができる。ＨＲ管理アカウントでログインする場合、ユーザは、組織のリソース管理に関連する管理作業を行うことができる。

【００８２】

少なくともいくつかの実施形態によれば、ユーザ装置１１５のユーザは、ユーザ装置１１５上のウエブベースの要求ユーザインターフェイス（ＵＩ）にアクセスすることによって、ターゲットシステム１３０と通信して、リソース１２５（例えば、電子メールアプリケーション）を要求することができる。例えば、要求ＵＩは、ユーザ装置１１５上のクライアントアプリケーション（例えば、ブラウザ）を介して見ることができるグラフィカルユーザインターフェイスを含むことができる。ユーザがターゲットシステム１３０上のリソースにアクセスしたいときまたはターゲットシステム１３０上のリソースに対して操作を実行しようとするときに、アクセス管理および脅威検出システム１０５は、ユーザからのアクセス要求を傍受し、ユーザを認証／認可しようとする。例えば、アクセス管理および脅威検出システム１０５は、ユーザにログインページを提供することによって、ユーザの認証情報（例えば、ログインＩＤおよびパスワード）を取得することができる。その後、アクセス管理および脅威検出システム１０５は、ユーザのログイン認証情報に基づいて、そのユーザが認可されたユーザであるか否かを判断することができる。アクセス管理および脅威検出システム１０５は、様々なチャネル（ＨＴＴＰ、ＯＡＰ）を介してユーザから、様々なイベント／動作（例えば、認証（authN）、認可（authZ）、ポリシー検証、ステップアップ認証、ＳＳＯ、トークン発行）を行うための様々な種類のアクセス要求、例えば、ウエブ要求、ＳＤＫ要求、プログラム要求を受信するように構成されてもよい。

【００８３】

様々な実施形態において、アクセス管理および脅威検出システム１０５は、１つ以上のエージェント１３５、１つ以上のプロキシ１４０（例えば、フォワードプロキシまたはリバースプロキシ）、１つ以上のアクセスマネージャ１４５、および／または１つ以上のウエブゲート１５０を含む。アクセス管理および脅威検出システム１０５は、リソース１２５に対するアクセス制御機能を提供するように、ユーザ装置１１５とターゲットシステム１３０（例えば、分散環境サーバ）との間の通信を可能にするためのエージェント－サーバモデルに従って、システム１００に実装されてもよい。エージェント－サーバモデルは、エージェント要素（例えば、シングルサインオンエージェントまたはポリシー実行エージェントとしても知られている１つ以上のエージェント１３５、１つ以上のプロキシ１４０、および／または１つ以上のウエブゲート１５０）およびサーバ要素（例えば、シングルサインオンサーバまたはポリシーサーバとしても知られている１つ以上のアクセスマネージャ１４５）を含むことができる。例えば、１つ以上のアクセスマネージャ１４５は、リソース１２５へのアクセスを制御するための判断要素として機能することができ、１つ以上のエージェント１３５、１つ以上のプロキシ１４０および／または１つ以上のウエブゲート１５０は、リソース１２５へのアクセスを制御するための実行要素として実装または動作することができる。いくつかの実施形態において、１つ以上のエージェント１３５、１つ以上のプロキシ１４０および／または１つ以上のウエブゲート１５０は、リソース１２５のプラグインまたはその一部として、リソース１２５と共に配置されてもよく、１つ以上のエージェント１３５、１つ以上のプロキシ１４０または１つ以上のウエブゲート１５０は、例えばリソース１２５の前のウエブサーバ上に実行するように、リソース１２５から独立して配置されてもよい。１つ以上のアクセスマネージャ１４５は、ＩＤアクセスマネージャの一部として配置されてもよい。

【００８４】

アクセス管理および脅威検出システム１０５は、分散環境内でＳＳＯ機能を提供することができ、分散環境内のリソースに対するアクセスを管理するために様々なアクセス制御関連機能を実行することができる。例えば、１つ以上のエージェント１３５、１つ以上のプロキシ１４０、１つ以上のアクセスマネージャ１４５および／または１つ以上のウエブゲート１５０は、ユーザ装置１１５を操作しているユーザの認証を実行することができる。認証とは、ユーザが自分自身が主張した人物であることを判断するためのプロセスである。ユーザを認証するために、アクセス管理および脅威検出システム１０５は、（例えば、ユーザのウエブブラウザを介して）チャレンジの形で認証情報を要求するためのリクエストをユーザに提示することができる。実行ポリシー（例えば、認証ポリシー）は、所定のリソースに対するアクセス権を付与すべきユーザを認証するために使用される認証方法を指定することができる。これらのポリシーは、リソースに対するアクセスを保護すべき方法（例えば、暗号化の種類など）を定義する。１つ以上のアクセスマネージャ１４５は、リソース１２５にアクセスするユーザの認可を決定することができる。認可とは、ユーザが要求されたリソースに対するアクセス権を有するか否かを判断するためのプロセスである。実行ポリシー（例えば、認可ポリシー）は、ユーザまたはユーザグループがあるリソースに対してアクセス権を有する条件を指定するように定義されてもよい。例えば、管理者は、特定のリソースに対するアクセス権を有するようにグループ内の特定のユーザを認可することができる。

【００８５】

１つ以上のエージェント１３５は、リソース要求のフィルタとして機能するポリシー実行エージェントであってもよい。１つ以上のエージェント１３５は、リソース要求を傍受し、静的実行ポリシーおよび動的実行ポリシーを適用することによって、要求されたリソースがアクセス管理および脅威検出システム１０５によって保護されているか否かを判断することができる。保護されている場合、リソース要求は、１つ以上のアクセスマネージャ１４５に転送され、保護されたリソースを要求しているユーザが保護されたリソースにアクセスできるか否かを判断することができる。特定の実施形態において、Oracle社によって開発された革新的なソリューションである１つ以上のウエブゲート１５０は、エージェントとして使用され、リソース要求をフィルタリングすることができる。いくつかの実施形態によれば、１つ以上のエージェント１３５および１つ以上のウエブゲート１５０は、ハードウェア構造またはハードウェア実装とソフトウェア実装の組み合せであってもよい。

【００８６】

１つ以上のプロキシ１４０は、リソース要求のフィルタとして機能するポリシー実行エージェントであってもよい。例えば、１つ以上のプロキシ１４０は、リソースに対するユーザ認証を処理するための認証プロキシであってもよい。認証プロキシは、認証機能を提供するように、ウエブアプリケーションまたはリソースによって呼び出される（例えば、インスタンス化される）ことができる。いくつかの実施形態において、認証プロキシは、基礎となる認証方式から独立して、認証に依存するプログラムを設計および作成することを可能にするように、１つ以上の低レベル認証方式を統合した高レベルＡＰＩを含むことができる。１つ以上のプロキシ１４０は、リソース要求を傍受し、静的実行ポリシーおよび動的実行ポリシーを適用することによって、要求されたリソースがアクセス管理および脅威検出システム１０５によって保護されているか否かを判断することができる。保護されている場合、リソース要求は、１つ以上のアクセスマネージャ１４５に転送され、保護されたリソースを要求しているクライアントが保護されたリソースにアクセスできるか否かを判断することができる。認証プロキシの一例として、リナックスシステムに使用されたプラグ可能な認証モジュール（ＰＡＭ）が挙げられる。いくつかの実施形態によれば、１つ以上のプロキシ１４０は、ハードウェア構造またはハードウェア実装とソフトウェア実装の組み合せであってもよい。

【００８７】

１つ以上のアクセスマネージャ１４５は、認証および／または認可プロセスを行うため

の複数の要素を有することができる。また、１つ以上のアクセスマネージャ１４５は、１つ以上の認証方式を含むことができる。認証方式は、１つ以上のアクセスポリシー（例えば、本明細書に説明されている静的実行ポリシーおよび動的実行ポリシー）を用いてリソースを保護するように構成されてもよい。認証方式は、認証情報収集メカニズムに関する詳細および認証情報を収集するために使用された認証情報収集装置の種類を含むことができる。例えば、認証情報の収集は、リモートユーザからのＨＴＴＰ（Ｓ）要求を処理するためのＨＴＴＰ（Ｓ）トランスポートチャネルを使用して行われてもよい。特定の実施形態において、認証方式は、認証および／または認可プロセスの成功または失敗をユーザ装置１１５に通知するために使用されるリダイレクトＵＲＬ（Uniform Resource Locator：ユニフォームリソースロケータ）を特定することができる。また、認証方式は、ユーザ装置１１５からの認証情報の転送を保護するための信頼レベルを表す認証レベルを特定することができる。例えば、ＬＤＡＰ（Lightweight Directory Access Protocol：ライトウ
ェイトディレクトリアクセスプロトコル）方式は、フォーム認証方法に基づいてＵＲＬなどのマネージャ関連リソースを保護するように、ＬＤＡＰ認証モジュールを使用した第２レベルの認証であってもよい。フォーム認証方法において、１つ以上のテキスト入力フィールドを有するＨＴＭＬフォームを使用して、認証情報を収集することができる。いくつかの実施形態において、フォーム認証は、ユーザ名、パスワード、社会保障番号、生年月日、ワンタイムパスワード、または他の一般的なパラメータの組み合わせなどの認証情報を収集することができる。

【００８８】

図１は、１つ以上のエージェント１３５、１つ以上のプロキシ１４０、１つ以上のアクセスマネージャ１４５および／または１つ以上のウエブゲート１５０を含むアクセス管理および脅威検出システム１０５を実装する分散環境に管理されたＳＳＯセッションの一例をさらに示している。例えば、ユーザは、ユーザ装置１１５を操作して、ターゲットシステム１３０によって制御されているリソース１２５に対するアクセスを要求することができる。この要求は、リソース１２５に対するアクセスを制御する１つ以上のエージェント１３５、１つ以上のプロキシ１４０および／または１つ以上のウエブゲート１５０にルーティングされまたは傍受される。いくつかの実施形態において、１つ以上のエージェント１３５、１つ以上のプロキシ１４０および／または１つ以上のウエブゲート１５０によって管理されているいくつかのリソースは、保護されていないことがある。この場合、１つ以上のエージェント１３５、１つ以上のプロキシ１４０および／または１つ以上のウエブゲート１５０は、１つ以上のアクセスマネージャ１４５に照会することによって、要求されたリソースが保護されているか否かを判断することができる。１つ以上のアクセスマネージャ１４５は、リソース１２５に関連する実行ポリシーをチェックすることによって、リソース１２５にアクセスするために認証を行う必要があるか否かを判断する。要求されたリソースが保護されており且つ使用時に認証を行う必要がある場合、１つ以上のアクセスマネージャ１４５は、ユーザ用のセッションが存在しているか否かを判断することができる。ユーザ用のセッションが存在していないと判断した場合、１つ以上のアクセスマネージャ１４５は、このユーザをＩＤアクセスマネージャのログインサービス（例えば、認証サービス）に転送する。認証サービスは、ユーザから認証情報（例えば、ユーザ名／パスワードなど）を要求することができる。認証サービスは、適切な認証情報を受信すると、受信した認証情報をユーザディレクトリまたはＩＤ記憶装置に記憶されているものと比較することによって、ユーザを認証することができる。

【００８９】

受信したユーザの適切な認証情報に基づいて、１つ以上のアクセスマネージャ１４５は、ユーザを１つ以上のエージェント１３５、１つ以上のプロキシ１４０および／または１つ以上のウエブゲート１５０に戻して、１つ以上のエージェント１３５、１つ以上のプロキシ１４０および／または１つ以上のウエブゲート１５０は、認証を確認し、認証したユーザのために第１セッションを確立することができる。その結果、ユーザは、ターゲット

システム１３０（例えば、分散環境サーバ）上のそのセッションにログインする。ログインすると、ユーザは、異なるアプリケーションの実行、クラウドストレージの利用など、アクセスを許可したリソースを利用することができる。ユーザがターゲットシステム１３０にログインすると、１つ以上のアクセスマネージャ１４５は、ユーザのセッション活動を追跡するためのクッキーを作成することができる。このクッキーは、ユーザが当該セッション上にアクティブであった時間を含むことができる。このクッキーは、セッション活動データとして情報管理システム１１０に記憶されてもよい。

【００９０】

ユーザがＳＳＯセッションに認証されていると判断した場合、１つ以上のエージェント１３５、１つ以上のプロキシ１４０および／または１つ以上のウエブゲート１５０は、認可クエリを１つ以上のアクセスマネージャ１４５に転送することによって、リソース１２５に対する原始要求を処理する。１つ以上のアクセスマネージャ１４５は、リソース１２５に関連する実行ポリシーをチェックすることによって、リソース１２５に対するユーザのアクセスが許可されているか否かを判断する。１つ以上のアクセスマネージャ１４５は、実行ポリシーに基づいて、許可メッセージまたは拒否メッセージを１つ以上のエージェント１３５、１つ以上のプロキシ１４０および／または１つ以上のウエブゲート１５０に送信する。リソース１２５に対するユーザのアクセスが許可されていると判断した場合、１つ以上のエージェント１３５、１つ以上のプロキシ１４０および／または１つ以上のウエブゲート１５０は、ユーザ装置１１５からリソース１２５にアクセスする要求を許可する。これによって、ユーザは、ユーザ装置１１５から、ターゲットシステム１３０上のリソース１２５にアクセスすることができる。リソース１２５に対するユーザのアクセスが拒否されていると判断した場合、１つ以上のエージェント１３５、１つ以上のプロキシ１４０および／または１つ以上のウエブゲート１５０は、リソース１２５に対するユーザのアクセスが許可されていないことをユーザ装置１１５に通知する。

【００９１】

情報管理システム１１０は、１つ以上のコンピュータおよび／またはサーバを含んでもよい。これらのコンピュータおよび／またはサーバは、汎用コンピュータ、（例示として、ＰＣサーバ、ＵＮＩＸ（登録商標）サーバ、ミッドレンジサーバ、メインフレームコンピュータ、ラックマウントサーバを含む）専用サーバコンピュータ、サーバファーム、サーバクラスタ、または任意の他の適切な構成および／または組み合わせであってもよい。情報管理システム１１０を構成するコンピューティング装置は、任意のオペレーティングシステムまたはＨＴＴＰサーバ、ＦＴＰサーバ、ＣＧＩサーバ、Ｊａｖａ（登録商標）、データベースサーバなどを含む様々な追加のサーバアプリケーションおよび／または中間層アプリケーションを実行することができる。例示的なデータベースサーバは、Oracle（登録商標）、Microsoft（登録商標）、Sybase（登録商標）、IBM（登録商標）などの会社から市販されているものを含むがこれらに限定されない。　様々な実施形態において、情報管理システム１１０は、リソース１２５に対するユーザのアクセスを保護および認可するために、アクセス管理および脅威検出システム１０５をサポートする。情報管理システム１１０は、ターゲットシステム１３０に対するユーザのアクセスを認証／認可するために、ユーザのアクセス要求に関連する追加情報を取得するように構成されてもよい。この情報は、例えば、要求を送信したクライアントのＩＰアドレス、装置情報、ユーザ情報、要求されたリソース、および要求を送信した時間を含むことができる。また、情報管理システム１１０は、これらの情報を分析して、所定期間に亘って静的ポリシーを上書きするための新たなポリシー（例えば、動的検査および実行ポリシー）を作成および公開するように構成されてもよい。いくつかの実施形態において、利用可能なリアルタイムデータは、システム脅威分析結果の一部として顧客に視覚的に提示される。リアルタイムでデータを顧客に提供する場合、リアルタイム脅威分析結果に応じて、迅速に措置を決定することができる。様々な実施形態は、データを格納し、格納されたデータ（すなわち、履歴データ）を用いて、リアルタイムで適用できる追加のルールおよびポリシーを作成することができる。特定の実施形態は、履歴データをマイニングすることによって、履歴データに基

づいて動的検査ポリシーおよび実行ポリシーを作成することができる。他の実施形態において、履歴データとリアルタイムで得られた情報の分析結果との両方を用いて、動的検査ポリシーおよび実行ポリシーを作成することができる。

【００９２】

図２は、リソースにアクセスするユーザの情報を収集し、情報の分析結果に基づいてポリシーを公開し、および情報の分析結果を視覚化するための情報管理システム２００（例えば、図１を参照して説明した情報管理システム１１０）の態様を示している。いくつかの実施形態において、情報管理システム２００は、ネットワーク（すなわち、図１を参照して説明したネットワーク１２０）を介して、アクセス管理および脅威検出システム２１５（例えば、図２を参照して説明したアクセス管理および脅威検出システム１０５）に通信可能に接続された収集バス２０５およびポリシーバス２１０を含む。また、情報管理システム２００は、収集バス２０５およびポリシーバス２１０に通信可能に接続された分析サーバ２２０、機械学習コンポーネント２２５、視覚化サーバ２３０、１つ以上のエージェント２３５、１つ以上のプロキシ２４０、１つ以上のアクセスマネージャ２４５、１つ以上のウエブゲート２５０、およびシステムメモリ２５５をさらに含むことができる。

【００９３】

収集バス２０５およびポリシーバス２１０は、ネットワークトポロジを含む。このネットワークトポロジにおいて、分析サーバ２２０、機械学習コンポーネント２２５、視覚化サーバ２３０、１つ以上のエージェント２３５、１つ以上のプロキシ２４０、１つ以上のアクセスマネージャ２４５および／または１つ以上のウエブゲート２５０などのノードは、バスまたはエンタープライズサービスバスと呼ばれる共通の線形（または分岐）リンクに接続される。収集バス２０５およびポリシーバス２１０は、分散コンピューティングを行うためのソフトウェアアーキテクチャを実装する。分散コンピューティングは、様々なノード間でメッセージおよびデータのルーティング、様々なポリシー（検査および実行ポリシー）の配置の管理、検査ポリシーに基づいてデータの収集を容易にするためのサービスの提供、およびリスナー（すなわち、エージェント）に対して様々なポリシー（検査ポリシーおよび実行ポリシー）の公開を含む。

【００９４】

分析サーバ２２０、機械学習コンポーネント２２５および視覚化サーバ２３０は、１つ以上のコンピュータおよび／またはサーバを含んでもよい。これらのコンピュータおよび／またはサーバは、汎用コンピュータ、（例示として、ＰＣサーバ、ＵＮＩＸ（登録商標）サーバ、ミッドレンジサーバ、メインフレームコンピュータ、ラックマウントサーバを含む）専用サーバコンピュータ、サーバファーム、サーバクラスタ、または任意の他の適切な構成および／または組み合わせであってもよい。分析サーバ２２０、機械学習コンポーネント２２５および視覚化サーバ２３０を構成するコンピューティング装置は、任意のオペレーティングシステムまたはＨＴＴＰサーバ、ＦＴＰサーバ、ＣＧＩサーバ、Ｊａｖａ（登録商標）、データベースサーバなどを含む様々な追加のサーバアプリケーションおよび／または中間層アプリケーションを実行することができる。例示的なデータベースサーバは、Oracle（登録商標）、Microsoft（登録商標）、Sybase（登録商標）、IBM（登録商標）などの会社から市販されているものを含むがこれらに限定されない。

【００９５】

システムメモリ２５５は、例えば、フラッシュメモリなどの非一時的機械可読記憶媒体、読取専用メモリ（ＲＯＭ）などの永久メモリ、ランダムアクセスメモリ（ＲＡＭ）などの半永久メモリ、他の適切な種類の非一時的記憶装置、またはそれらの任意の組み合せを含む１つ以上の記憶媒体であってもよい。異なる態様によれば、メモリ２５５は、システム２００の動作に関連するコンピュータ可読プログラム命令、データ構造、プログラムモジュールおよび他のデータを記憶する。特定の態様によれば、メモリ２５５は、実施形態において、オペレーティングシステム、応用プログラム、ポリシー、ユーザの活動およびアクセス要求に関連するデータ情報、およびプログラムデータを格納することができる。

【００９６】

図２のシステムが配置されると、（図１を参照して説明したように、１つ以上のエージェント２３５、１つ以上のプロキシ２４０、１つ以上のアクセスマネージャ２４５および／または１つ以上のウエブゲート２５０によって構成された）アクセス管理および脅威検出システム１０５は、静的実行ポリシーおよび動的実行ポリシー内のルールに基づいて、ターゲットシステム上のリソースに対するエンドユーザのアクセスが認証および／または認可されている否かを判断することができる。ルールは、宛先（例えば、アプリケーションまたはサービスなどのターゲットシステムまたはリソースのＵＲＬ、ホスト名、宛先ＩＰアドレスまたはポート）、ソース（例えば、ユーザＩＤ、ユーザグループの指定、クライアント装置のＩＰアドレス）、期間（例えば、ポリシーが有効になっている所定の時間）、および実行措置（例えば、ユーザによるアクセスのブロック、認証／認可ファクタの要求、活動の監視）の指定を含むことができる。ネットワークトラフィックまたはユーザ活動パターンがポリシー内のルールと一致する場合、このポリシーがトリガされ、実行措置が適用される。静的実行ポリシーおよび動的実行ポリシーは、各々静的ポリシーのキャッシュ２６５および動的ポリシーのキャッシュ２７０としてメモリ２５５に格納されてもよい。

【００９７】

特定の実施形態において、一般的な方法は、以下のように行われる。エンドユーザは、保護されたポリシードメイン上のリソースを要求するためのＵＲＬまたはＩＤを入力する。ユーザのブラウザは、ＵＲＬをＨＴＴＰ要求の一部としてウエブサーバに送信する。１つ以上のエージェント２３５、１つ以上のプロキシ２４０および／または１つ以上のウエブゲート２５０は、要求を認識して傍受する。エンドユーザがまだ認証されていない場合、１つ以上のエージェント２３５、１つ以上のプロキシ２４０および／または１つ以上のウエブゲート２５０は、ブラウザにログイン情報を求めるチャレンジを発行するように、ウエブサーバに要請する。受信されたログイン情報は、その後、ウエブサーバに戻され、１つ以上のエージェント２３５、１つ以上のプロキシ２４０および／または１つ以上のウエブゲート２５０に渡される。１つ以上のエージェント２３５、１つ以上のプロキシ２４０および／または１つ以上のウエブゲート２５０は、認証要求を１つ以上のアクセスマネージャ２４５に送信し、１つ以上のアクセスマネージャ２４５は、ユーザが提供したログイン情報が本物であるか否かを判断する。１つ以上のアクセスマネージャ２４５は、ユーザのＩＤ情報の属性およびメモリ２５５に格納されているリソースの認証基準を利用して認証を行う。ユーザが提供したログイン情報が認証基準を満たす場合、プロセスは、以下のように進み、そうでない場合、要求されたリソースへのアクセスが拒否されることをエンドユーザに通知し、プロセスは、終了する。

【００９８】

ユーザを認証した後、１つ以上のエージェント２３５、１つ以上のプロキシ２４０および／または１つ以上のウエブゲート２５０は、要求されたリソースに対するユーザのアクセスが許可されているか否かについて１つ以上のアクセスマネージャ２４５に照会する。したがって、１つ以上のアクセスマネージャ２４５は、要求されたリソースの適切な認可基準について情報管理システム２００に照会する。１つ以上のアクセスマネージャ２４５は、リソースの認可基準を検索し、リソースの認可基準およびユーザのＩＤ情報に基づいて、１つ以上のエージェント２３５、１つ以上のプロキシ２４０および／または１つ以上のウエブゲート２５０の認可クエリに応答する。ユーザが認可されている場合、リソースに対するユーザのアクセスが許可される。それ以外の場合、ユーザの要求が拒否される。上述したフローに対する様々な代替案も本発明の精神および範囲に含まれる。

【００９９】

認証および認可の判断は、ポリシードメインおよびポリシー（例えば、静的実行ポリシーおよび動的実行ポリシー）に基づいて行われてもよい。ポリシードメインは、ウエブサーバのホストＩＤ、ホスト名、ＵＲＬプレフィックス、およびルールを含む論理グループである。ホスト名およびＵＲＬプレフィックスは、特定のポリシードメインによって保護されるウエブネームスペースの粗い部分（course-grain portion）を指定する。ポリシ

ードメインのルールは、要求されたリソースへのアクセスを許可または拒否する条件、およびこれらの条件を適用するエンドユーザを指定する。ポリシードメインは、ポリシーに含まれている第１レベルのデフォルトルールと第２レベルのルールとの２つのレベルのルールで構成される。第１レベルのデフォルトルールは、ポリシーに関連付けられていないポリシードメイン内の任意のリソースに適用することができ、第２レベルのルールは、ポリシーに関連付けられているポリシードメイン内の任意のリソースに適用することができる。ポリシーとは、ＵＲＬパターン、リソース種類、操作種類（要求メソッドなど）、およびユーザごとに特定のリソースに対するアクセスを制限するためのルール、静的または動的なグループメンバーシップ、時刻または曜日、ＩＰ（インターネットプロトコル）アドレスなどを含むグループである。ポリシーは、ポリシードメインに関連付けられた静的または動的ポリシーであってもよく、ポリシーによって保護されるウエブネームスペースの細かい部分（fine-grain portion）を指定する。実際には、ポリシードメインのホスト名およびＵＲＬプレフィックスは、ポリシーのＵＲＬパターンと論理的に関連している。得られたパターンの全体は、受信したＵＲＬと比較される。一致した場合、ポリシーの様々なルールを評価することによって、要求を認可するか拒否するかを決定する。一致しなかった場合、デフォルトポリシードメインルールが使用される。

【０１００】

静的実行ポリシーおよび動的実行ポリシーは、許可されているものおよび許可されていないものを表現するための属性をまとめるステートメントである。実行ポリシーは、任意種類の属性（ユーザ属性、リソース属性、オブジェクト、アクション、環境属性など）を使用することができ、ブール論理などの論理を含む。この場合、ルールは、属性を評価し、許可されているものおよび許可されていないもの（例えば、要求を出したユーザが認証されたか否か、要求を出したユーザが要求したリソースに対するアクセスが認可されているか否か、要求を出したユーザが要求したリソースに対して要求を出す行動が認可されているか否か）を判断するためのステートメント（例えば、「IF、THEN」）を含む。例えば、要求元がマネージャである場合、機密データへの読み取り／書き込みアクセスが許可される。静的実行ポリシーは、デフォルトルール、または進化するシステムの動態または属性を評価するためにシステムの寿命に亘って書き込まれる／書き直される（例えば、システムの管理者によって作成される）ルールを含む。しかしながら、静的ポリシー内に含まれるルールは、リアルタイムで書かれる／書き直されることはない。これによって、ポリシーは、進化するシステムの動態または属性をリアルタイムで評価することができる。一方、動的実行ポリシーは、進化するシステムの動態または属性をリアルタイムで評価するように、書き込まれる／書き直される（例えば、機械学習技術またはシステムの管理者によって作成される）ルールを含む。

【０１０１】

様々な実施形態において、脅威の検出に基づいて静的ポリシーおよび動的ポリシーの作成および実行を行うためのシステムおよび方法が提供される。静的実行ポリシーおよび動的実行ポリシーは、様々なエージェント（例えば、１つ以上のエージェント２３５、１つ以上のプロキシ２４０および／または１つ以上のウエブゲート２５０）によって、実行経路に沿って実行されてもよい。これらのポリシーは、実行経路におけるエージェントの位置にそれぞれ適用されるものとして理解されてもよい。いくつかの実施形態において、動的ポリシーは、管理者によって手動で作成されてもよく、または機械学習コンポーネント２２５によってシステムに自動的に導入されてもよい。また、特定の実施形態において、動的ポリシーの実行期間（例えば、所定期間）を指定することができる。例えば、所定期間（例えば、５分、１０分、４時間、１日、２週間など）にポリシーを設定することによって、分析サーバ２２０および／または管理者は、その所定期間内のデータに基づいて、異常を監視およびトリガすることができる。所定期間が経過した後に、ポリシーは無効になる。したがって、いくつかの実施形態は、動的ポリシーを新たに追加したシステムの挙動を監視することができ、システムの安定性を保証することができる。監視されている動的ポリシーは、ソリッドまたは永久（すなわち、所定期間によって制限されない）ポリシ

ーになるように変更されてもよい。いくつかの実施形態は、機械学習機能を使用して、所定期間（例えば、次の３０分）の間に動的ポリシーを作成し、最終的にはこの動的ポリシーを用いて、システムに設定された静的ポリシーを永久に上書きする。なお、完全な承認プロセスを行う必要があるか否かに関わらず、視覚化アプリケーションを見ているセキュリティ管理者がこれらのポリシーを迅速に生成してシステムに導入することは、非効率的であり、リソースを浪費する。

【０１０２】

いくつかの実施形態において、機械学習コンポーネント２２５がポリシーに影響を与えない場合、スティッキーポリシー（すなわち、上書きできない静的ポリシー）を作成することができる。他の実施形態において、機械学習コンポーネント２２５は、デフォルトポリシーまたは管理者によって作成されたポリシー（例えば、上書き可能な静的ポリシー）を学習することができ、これらのポリシーを変更するまたは動的ポリシーを用いてこれらのポリシーを上書きすることができる。特定の実施形態において、機械学習は、追加のデータに基づいて、システム管理者によって以前に作成されたデフォルトポリシーまたは静的ポリシーを変更することができ、デフォルトポリシーまたは静的ポリシーを上書きすることができる。例えば、ブロックポリシーに対応する特定のカテゴリに異常を分類することができる。このブロックポリシーは、高警告ポリシーであり、第２ファクタ認証などの別のカテゴリを上書きすることができる。これによって、ユーザが有効セッションにいても、ユーザが何らかの行動を行った場合に、追加認証を行うためのフォームまたは質問をユーザに提示することができる。他の実施形態において、ブロックポリシー（例えば、ユーザまたはユーザグループがリソースに対する読み取り／書き込みなどの動作をブロックするように構成されたロジックを有するポリシー）を作成しないように指定することができる。これによって、管理者は、機械学習によってトリガされたポリシーの種類を監視することができる。例えば、管理者は、最初の数ヶ月間、特定の状況下または特定のパターンがある場合に機械学習が複数の高警告を作成することを監視し、これらの警告を検証し、機械学習が大量の偽陽性警告を作成していないことを判断する。次に、管理者は、ポリシーを調整し、あるパターンに対して高警告を作成するのではなく、当該パターンに対して第２ファクタ認証ポリシーを作成することができる。

【０１０３】

一例において、ユーザは、毎日の午前７時から９時まで自宅または別の場所からサーバ（例えば、ターゲットシステム）にアクセスし、毎日の午前１０時から午後４時まで職場または本部からサーバにアクセスすることがある。ユーザが別の場所に移動してサーバにアクセスしようとする場合、システムは、位置データが履歴データと一致しないときに第２ファクタ認証をトリガするという異常時のデフォルトポリシーまたは静的ポリシーで構成されているため、分析サーバ２２０は、そのアクセスが異常であると判断し、第２ファクタ認証をトリガする。一定の時間が経過した後、システムは、デフォルトまたは静的ポリシーから学習して適応し、ユーザの行動パターンに基づいて、ユーザが別の場所に移動しているときに異常をトリガしないように判断することができる。また、システムは、ユーザの行動パターンを識別することができる。システムは、履歴データおよび更新されたリアルタイムデータに基づいて、異常をトリガすべきであるか否かを知能的に判断することができる。機械学習コンポーネント２２５は、履歴データおよびリアルタイムデータから絶えずに学習することによって、エンドユーザのＩＤ情報または行動モデルおよび行動を管理するためのポリシーを作成および修正することができる。これらのＩＤ情報およびポリシーは、毎週または隔週に更新されるのではなく、リアルタイムで更新される。これによって、次の異常検出には、ユーザ活動の全ての履歴データおよびリアルタイムデータが考慮される。したがって、次回の判断には、異常として特定され得るものを速やかに考慮に入れることができる。よって、この例において、新しい位置がメモリ２５５に更新されているため、次回にユーザがこの地理的位置にいるときにログインした場合、システム上の活動が異常検出をトリガしない。実質的には、過去のポリシーを上書きする新しい動的ポリシーが作成された。

【０１０４】
図２は、イベント／データの収集を行うためのメカニズムをさらに示している。いくつかの実施形態において、機械学習がより多くの処理データを有する場合、機械学習コンポーネント２２５は、より多くの実行ポリシーを生成することができ、より多くおよびより複雑なパターンを見出すことができる。特定の実施形態において、イベント／データの収集は、動的であり、検査ポリシーメカニズムは、データの収集を容易にすることができる。収集されたデータは、機械学習に与えることができる。これによって、さらに多くの実行ポリシーを作成することができ、実行ポリシーによってトリガされる異常をトリガすることができる。例えば、新しいアプリケーションをインストールするときに、システムは、（収集バス２０５および分析サーバ２２０を介して自動的にまたは管理者を介して手動で）検査ポリシーを起動して、アプリケーションがどのように機能するかを理解することができる。検査ポリシーは、アプリケーションに対するユーザ活動を調べることによって、検査ポリシーのルールを考慮して、データを生成することができる。収集バス２０５、分析サーバ２２０および機械学習コンポーネント２２５は、収集されたデータに基づいて活動を自動的に分類し、データから特定されたパターンに基づいて活動が低警告活動、中警告活動または高警告活動であるかを判断することができる。その後、分析サーバ２２０および機械学習コンポーネント２２５は、収集バス２０５によって収集されたデータに基づいて、動的検査および実行ポリシーを自動的に生成することができ、生成されたポリシーは、ポリシーバス２１０上に公開され、所定期間中にエージェントによって使用され、静的ポリシーを上書きすることができる。

【０１０５】
特定の実施形態において、企業内で（例えば、企業のネットワーク上に）公開された全てのデータは、収集バス２０５を介してリアルタイムで収集可能であり、分析サーバ２２０によって使用および分析されてもよい。いくつかの実施形態において、分析サーバ２２０は、イベント相関を行い、レポートを生成し、レポートバス２７５上にレポートを公開することができる。機械学習コンポーネント２２５は、レポートバス２７５からリアルタイムで情報を継続的に受信し、視覚化サーバ２３０を介してユーザインターフェイスに情報を提供する。また、機械学習コンポーネント２２５は、収集バス２０５、メモリ２５５およびレポートバス２７５からのリアルタイムイベントおよび履歴データを使用する。したがって、機械学習コンポーネント２２５は、異常を発見し、ポリシー（検査ポリシーまたは実行ポリシー）をポリシーバス２１０に公開することができる。

【０１０６】
従来の技術において、エージェントは、データを収集し、そのデータをログアスキーデータ名と値の対として記録し、そのログを定期的に（例えば、５分または１０分ごとに）サーバに送信するように構成されている。エージェントがクラウドに位置し、サーバが企業内または企業外に位置する可能性があるため、これらのログの転送には費用がかかる可能性がある。また、ログを蓄積してまとめて送信する場合、時間がかかる。様々な実施形態は、ログアスキーデータ名と値の対を収集して送信する代わりに、データを高度に圧縮するように、バイナリデータを用いて、様々なエージェントから収集バス２０５にデータをリアルタイムに転送する。特定の実施形態は、データをマッピングするために値およびメカニズムを転送する。例えば、エージェントは、値を収集バス２０５に送信し、収集バス２０５は、エージェントから送信されたフォーマット（例えば、スキーマ１）を判断することができる。フォーマットが特定されると、値は、翻訳される。これは、データを圧縮して効率的に転送する方法である。

【０１０７】
様々な実施形態において、システムは、１つ以上のエージェント２３５、１つ以上のプロキシ２４０、１つ以上のアクセスマネージャ２４５および１つ以上のウエブゲート２５０を含むエージェントによって捕捉および送信されたデータに基づいて、脅威を検出およびトリガすることができる。エージェントがより新しいターゲットシステム、アプリケーションおよび既存のアプリケーションインターフェイスの変更をサポートする必要がある

ときに、一組の定義済み属性（例えば、ユーザ属性、リソース属性、オブジェクト、アクション、環境属性など）は十分ではない場合がある。したがって、システムは、動的検査ポリシーを用いて、動的ルールをエージェントに送信することによって、様々なペイロード（例えば、ＨＴＴＰ）内のデータなどの追加の情報または属性の収集／検査をエージェントに要請することができる。この情報は、通常のアクセス要求イベントの一部として報告される。その後、機械学習コンポーネント２２５は、この新しいデータまたは情報の異常を検出し、動的実行ポリシーを挿入することによって、より多くの異常をトリガすることができる。より多くの異常がトリガされると、特定の種類のトラフィックを防ぐために追加の実行ポリシーを作成することができる。これによって、収集、検出および実行サイクルが完了する。

【０１０８】

収集バス２０５は、エンドユーザからのアクセス要求などのセキュリティイベントに関連する情報を取得し、その情報またはデータをレポートバス２７５に報告するように構成されてもよい。収集バス２０５は、特定の基準が満たされたときに、一組の定義済み属性（例えば、ユーザ属性、リソース属性、オブジェクト、アクション、環境属性など）を収集するためのルールを含むデフォルト検査ポリシーまたは静的検査ポリシーに基づいて構成されてもよい。特定の実施形態において、検査ポリシーは、データを監視し、特定の基準が定義済みパターンと一致するときに管理者に通知する。検査ポリシーは、パターンが存在するときに警告をトリガしないが、パターンが存在するときに一組の定義済み属性を収集する。例えば、システムは、一組の基準が満たされたとき（例えば、閾値時間帯にヘッダデータが一致する場合）に、管理者がトリガされる特定の検査ポリシーを指定できるように、検査ポリシーユーザインターフェイス（ＵＩ）を提供することができる。他の態様によれば、収集は、データまたは属性を収集するためのルールを含む動的検査ポリシーに基づいて構成されてもよい。例えば、収集バス２０５および分析サーバ２２０は、協働して一組の定義済み属性を収集し、過去に設定されたルール（デフォルトポリシー、静的ポリシー、または動的検査および実行ポリシー）に基づいて異常をトリガすることができる。検査ポリシーは、収集される一組の定義済み属性および特定されるデータ内のパターンの基準を指定することができる。収集バス２０５を介して属性およびパターンを収集した後、分析サーバ２２０は、データ内の属性およびパターンを検査し、これらの属性およびパターンが実行ポリシー内に定義されたルールと一致するか否かを判断することができる。データは、収集バス２０５に入ると、メモリ２５５に格納され、履歴データの一部になる。機械学習コンポーネント２２５は、履歴データおよびリアルタイムデータから絶えずに学習することによって、システム上のユーザ活動の脅威評価に必要な情報を効率的に収集するように検査および実行ポリシーを作成および修正することができる。

【０１０９】

イベントに関連する情報は、（図１を参照して説明した）１つ以上のエージェント２３５、１つ以上のプロキシ２４０、１つ以上のアクセスマネージャ２４５および／または１つ以上のウエブゲート２５０を含む１つ以上のエージェントから収集され、例えば、要求を送信したクライアントのＩＰアドレス、装置情報、ユーザ情報、要求されたリソース、および要求を送信した時間を含むことができる。特定の実施形態において、情報は、クライアント装置内のＧＰＳアプリケーション、天気アプリケーション、監視ソフトウェア、ハードウェアセンサ、負荷分散ソフトウェアなどを含む第３者エージェントからさらに収集される。情報は、収集バス２０５によって非同期に収集されてもよい。例えば、収集バス２０５は、情報の処理、リアルタイムで情報のインデクス付け、情報に対してデータ集約および照会動作を実行するように構成された待ち行列（queue）を含むことができる。いくつかの例において、収集バス２０５は、ユーザから受信したアクセス要求に関する情報を、例えばクライアントコンテキスト、リソースコンテキスト、ユーザコンテキスト、サーバコンテキスト、タイムスタンプ、セッション情報および要求を処理するためのサーバインスタンスなどの様々なカテゴリに編成するように構成されてもよい。様々な実施形態において、収集バス２０５は、ユーザ活動から取得および編成された情報またはデータ

をメモリ２５５内の情報データベース２６０に格納するように構成される。
【０１１０】
図２は、収集されたイベント／データに基づいて動的実行ポリシーを作成し、ポリシーバス２１０を介してエージェント（例えば、１つ以上のエージェント２３５、１つ以上のプロキシ２４０、１つ以上のアクセスマネージャ２４５および１つ以上のウエブゲート２５０を含む１つ以上のエージェント）によって実行される動的実行ポリシーを公開するためのメカニズムを示している。いくつかの実施形態において、分析サーバ２２０および機械学習コンポーネント２２５は、一定期間において、（例えば、メモリ２５５に格納された）ユーザまたはユーザグループから受信されたアクセス要求に関するリアルタイム着信データおよび履歴データを分析することによって、ユーザまたはユーザグループ用の動的実行ポリシーを作成するように構成される。一実施形態において、分析サーバ２２０および機械学習コンポーネント２２５は、ユーザまたはユーザグループによるアクセス要求のリアルタイム着信データおよび履歴データに関連するパラメータサブセットを特定することによって、ユーザまたはユーザグループ用の動的実行ポリシーを生成し、パラメータサブセットに対照してアクセス要求のリアルタイム着信データおよび履歴データを分析することによって、動的実行ポリシーを作成するように構成されてもよい。例えば、分析サーバ２２０および機械学習コンポーネント２２５は、一定期間において、ユーザまたはユーザグループが通常ターゲットシステムに格納された１つ以上のアプリケーションにアクセスする時間パラメータ（例えば、時間）に基づいて、ユーザまたはユーザグループのアクセス要求を分析し、ユーザのアクセス時間を監視することによって、実行ポリシーを作成するように構成されてもよい。ユーザまたはユーザグループが通常の時間パラメータ以外の時間に１つ以上のアプリケーションにアクセスしようとする場合、実行ポリシーは、第２ファクタ認証を要請するルールもしくはユーザまたはユーザグループをブロックするルールを含むことができる。
【０１１１】
いくつかの実施形態において、監視されるパラメータのサブセットは、ユーザがアクセスするターゲットシステム上のリソース（例えば、ターゲットアプリケーション）によって特定／定義されてもよく、ターゲットアプリケーションは、この情報を分析サーバに提供してもよい。例えば、ターゲットアプリケーション（例えば、金融アプリケーション）は、ユーザＩＤ、アクセス時刻およびアクセス期間などのパラメータに基づいて、ユーザのアクセス要求を追跡したい場合がある。これらのパラメータは、分析サーバ２２０を用いて設定され、機械学習コンポーネント２２５は、これらのパラメータに対照して、一定期間においてアクセス要求のリアルタイム着信データおよび履歴データを分析することによって、ユーザまたはユーザグループのために実行ポリシーを作成することができる。特定の実施形態において、監視されるパラメータサブセットを満たすデータが収集されていない場合、分析サーバ２２０および機械学習コンポーネント２２５は、特定の基準が満たされたとき（例えば、ユーザまたはユーザグループがシステムにログインするとき）に、パラメータサブセットを満たすデータを取得するようにトリガされる動的検査ポリシーを作成するように構成されてもよい。
【０１１２】
特定の実施形態において、分析サーバ２２０および機械学習コンポーネント２２５は、ユーザまたはユーザグループのために複数のポリシーを生成するように構成されてもよい。これらのポリシーは、アクセス要求に関連する異なるパラメータセットに対照して、ユーザまたはユーザグループによるアクセス要求のリアルタイム着信データおよび履歴データを分析することによって生成されてもよい。例えば、上述したように、分析サーバ２２０および機械学習コンポーネント２２５は、ユーザまたはユーザグループが通常ターゲットシステムに格納されている様々なアプリケーションにアクセスする時間に基づいて、ユーザまたはユーザグループのアクセス要求を分析することによって、ユーザまたはユーザグループのために時間依存性ポリシーを生成するように構成されてもよい。別の例において、分析サーバ２２０および機械学習コンポーネント２２５は、ユーザがターゲットシス

テムに格納されている様々なアプリケーションにアクセスするパターンを分析することによって、ユーザのためにアプリケーションアクセスパターンポリシーを生成するように構成されてもよい。分析サーバ２２０および機械学習コンポーネント２２５は、アクセス要求からのセキュリティ脅威、侵入、サービス拒否（ＤＯＳ）攻撃の特徴を取得することによって、ユーザのためにポリシーを生成するように構成されてもよい。

【０１１３】

いくつかの実施形態において、分析サーバ２２０および機械学習コンポーネント２２５は、ユーザまたはユーザグループに関連するアクセス要求のリアルタイム着信データおよび履歴データを１つ以上のデータクラスタに分類することによって、ポリシーを生成するように構成されてもよい。特定の実施形態において、分析サーバ２２０および機械学習コンポーネント２２５は、教師ありまたは教師なし機械学習または他のクラスタリング（例えば、Ｋ平均）技法を用いて、１つ以上のデータクラスタを生成するように構成されてもよい。様々な実施形態において、機械学習コンポーネント２２５は、密度ベースのクラスタリングアルゴリズムおよびユークリッド距離を使用した教師なし学習を用いて、クラスタの重心からアクセス要求までの距離を計算するように構成されてもよい。特定の例において、クラスタの半径は、クラスタ内の各点の重心からの距離の平均値に基づいて計算される。標準偏差に基づいて、半径の外側に位置する点のリスクが高くなる。企業ネットワーク上のユーザ活動が重心に近ければ、アクセスのリスクが低くなる。

【０１１４】

特定の例において、分析サーバ２２０、機械学習コンポーネント２２５および／または統合アプリケーション（例えば、ユーザがアクセスしようとするアプリケーション）によって構成されたパラメータのリアルタイム着信データおよび履歴データは、クラスタを構築するためのデータポイントになる。分析サーバ２２０および機械学習コンポーネント２２５は、クラスタを構築した後、１つ以上のデータクラスタに関するルールを含むポリシーを生成するように構成されてもよい。例えば、ユーザまたはユーザグループによる要求の特定のパラメータ（ｘ、ｙおよびｚ）がクラスタのパラメータ（ｘ、ｙおよびｚ）と一致しない場合、行動を実行する、例えば第２ファクタ認証を実行するまたはユーザまたはユーザグループをブロックするように、ルールを構築することができる。その結果、ユーザまたはユーザグループから新しい要求を受信する場合、要求から得られたパラメータの値を、既に確立されたクラスタのパラメータを含むポリシー内のルールと照合することによって、ユーザまたはユーザグループからのアクセス要求が異常であるか否かを判断することができる。

【０１１５】

いくつかの実施形態において、分析サーバ２２０および機械学習コンポーネント２２５は、クラスタを確立した後、脅威レベルに基づいてポリシーを分類するようにさらに構成されてもよい。脅威レベルは、クラスタの中心からの距離に基づいて決定されてもよい。一例として、企業ネットワーク上のトラフィックパターンは、基準に設定されたルール、例えば１つ以上のクラスタからトラフィックパターンまでの距離に従ってポリシーを生成するために使用される属性を有することができる。距離が１倍（例えば、平均から１つの標準偏差）である場合、ポリシーは、低程度リスクとして分類され、関連するトラフィックパターンは、低警告をトリガする。距離が２倍（例えば、平均から２つの標準偏差）である場合、ポリシーは、中程度リスクとして分類され、関連するトラフィックパターンは、中警告をトリガする。距離が３倍を超える（例えば、平均から３つの標準偏差を超える）場合、ポリシーは、ブロックとして分類され、関連するトラフィックパターンは、活動のブロックをトリガする。したがって、顧客は、トラフィックパターンが異常なパターンであるか否かを心配する必要はない。代わりに、顧客は、トラフィックパターンが低警告、中警告、高警告、第２ファクタ認証、またはブロックのいずれを作成したか否かに集中することができる。

【０１１６】

本明細書に記載されたように、ポリシーは、分析サーバ２２０および機械学習コンポー

ネント２２５または管理者（異常の発生を見ている人）によって生成されてもよい。いくつかの実施形態は、ポリシーを宣言する標準として、ＳＴＩＸ（Structured Threat Information eXpression）を使用する。様々な実施形態において、ポリシー（例えば、新しい動的実行ポリシー）は、確立または生成されると、ポリシーバス２１０に公開され、エージェント（例えば、１つ以上のエージェント２３５、１つ以上のプロキシ２４０、１つ以上のアクセスマネージャ２４５および／または１つ以上のウエブゲート２５０）によって実行される。ポリシーがエージェントによって実行されているときに、エージェントは、実行エコシステムの一部になる。例えば、ユーザまたはユーザグループから新しいアクセス要求を受信したときに、１つ以上のエージェント２３５、１つ以上のプロキシ２４０、１つ以上のアクセスマネージャ２４５および／または１つ以上のウエブゲート２５０は、実行ポリシー（デフォルト、静的または動的ポリシー）に対照して、アクセス要求に関連する情報を分析することによって、ユーザまたはユーザグループのアクセス要求が異常であるか否かを判断するように構成されている。

【０１１７】

いくつかの実施形態において、１つ以上のエージェント２３５、１つ以上のプロキシ２４０、１つ以上のアクセスマネージャ２４５および／または１つ以上のウエブゲート２５０は、先ず、ポリシーバス２１０上に公開される複数の実行ポリシーから、ユーザまたはユーザグループのためにポリシーを選択するように構成されてもよい。特定の実施形態において、ポリシーは、ユーザまたはユーザグループに特異的に関連付けられてもよい。選択は、例えば、ユーザまたはユーザグループがアクセスを要求しているアプリケーションの種類に基づいて行われてもよい。例えば、ユーザまたはユーザグループがターゲットシステム上の金融アプリケーションに対するアクセスを要求している場合、１つ以上のエージェント２３５、１つ以上のプロキシ２４０、１つ以上のアクセスマネージャ２４５および／または１つ以上のウエブゲート２５０は、複数のポリシーから、金融アプリケーションによって定義されたパラメータのサブセットを分析するためのポリシーを選択するように構成されてもよい。例えば、上述したように、金融アプリケーションは、ユーザＩＤ、アクセス時刻およびアクセス期間などのパラメータに基づいて、ユーザまたはユーザグループからのアクセス要求を分析したい場合がある。他の実施形態において、１つ以上のエージェント２３５、１つ以上のプロキシ２４０、１つ以上のアクセスマネージャ２４５および／または１つ以上のウエブゲート２５０は、ポリシーバス２１０上に公開された複数の実行ポリシーの全てを取得し、全てまたは一部のポリシーからのパラメータに基づいて、ユーザまたはユーザグループからのアクセス要求を分析するように構成されてもよい。

【０１１８】

１つ以上のエージェント２３５、１つ以上のプロキシ２４０、１つ以上のアクセスマネージャ２４５および／または１つ以上のウエブゲート２５０は、特定のポリシーを選択または取得した後、当該ポリシーに対照して、アクセス要求に関連する情報を分析することによって、ユーザのアクセス要求が異常であるか否かを判断するように構成されてもよい。いくつかの実施形態において、１つ以上のエージェント２３５、１つ以上のプロキシ２４０、１つ以上のアクセスマネージャ２４５および／または１つ以上のウエブゲート２５０は、分析サーバ２２０および機械学習コンポーネント２２５によって生成された１つ以上のデータクラスタからアクセス要求の偏差を判断することによって、異常要求を判断するように構成されてもよい。偏差が所定の閾値を超える場合、要求が異常であると判断される。閾値は、システムのユーザ（例えば、管理者）によって決定されてもよく、分析サーバ２２０および機械学習コンポーネント２２５によって自動的に決定されてもよい。特定の実施形態において、閾値は、クラスタのデータセットの相関を考慮したマハラノビス（Mahalanobis）距離であってもよい。

【０１１９】

各エージェントは、公開されたポリシーに独自に反応して、同じ最終目標（例えば、保護されたリソースに対するアクセス権を未認可／未認証ユーザに付与しないこと）を達成することができる。特定の実施形態において、異常が検出され、ユーザをブロックするた

めのポリシーが（例えば、ＳＴＩＸフォーマットで）作成され、ポリシーバス２１０に公開されると、１つ以上のエージェント２３５、１つ以上のプロキシ２４０、１つ以上のアクセスマネージャ２４５および／または１つ以上のウエブゲート２５０は、当該ポリシーを選択または取得し、ユーザまたはユーザグループをブロックするときの役割を決定することができる。例えば、ユーザまたはユーザグループがアプリケーションにアクセスしているときに、１つ以上のアクセスマネージャ２４５は、ユーザの資格情報を検証し、ユーザを認証セッションの一部であることを認証するための実体になり、１つ以上のエージェント２３５、１つ以上のプロキシ２４０および／または１つ以上のウエブゲート２５０は、ユーザが実行エコシステムの任意部分のリソースにアクセスしているときに、いつでもユーザをチャレンジおよび認証することができるように、セッションを開始、維持または切断することができる。１つ以上のプロキシ２４０は、行われているユーザまたはユーザグループの活動を絶えずに監視および学習し、ポリシーに基づいて、異常をトリガし、活動をブロックする措置をとることができる。例えば、１つ以上のプロキシ２４０は、ポリシーからブロックされるユーザの情報を取得することができ、当該ユーザに対応するＩＰアドレスからセッション要求を受信する場合、１つ以上のプロキシ２４０は、セッションの作成をブロックすることができる。したがって、リソースが他のエージェントによって保護されていなくても、１つ以上のプロキシ２４０は、ポリシーバス２１０と同じポリシーを有するため、ユーザ活動に対して独自の行動をとることができる。

【０１２０】

追加的にまたは代替的に、１つ以上のエージェント２３５、１つ以上のアクセスマネージャ２４５および／または１つ以上のウエブゲート２５０は、ユーザまたはユーザグループが行っている（例えば、ユーザがログインページにユーザ名またはパスワードを入力しようとしている、ユーザが保護されたアプリケーションにアクセスしようとしている、または承認されたセッションから別のウエブサイトにアクセスしようとしている）活動を絶えずに監視および学習し、同じポリシーに基づいて、異常をトリガし、活動をブロックする措置をとることができる。例えば、１つ以上のエージェント２３５および／または１つ以上のウエブゲート２５０は、期間が満了したか否かに基づいて、セッションがまだ有効であるか否かをチェックすることができる。いくつかの例において、時間セッションは、所定期間、例えば、１時間または８時間に有効である。セッションが無効になったときに、ユーザが再度ログインするように要求される。１つ以上のエージェント２３５および／または１つ以上のウエブゲート２５０は、当該ポリシーを用いてセッションを検証し、セッションが無効になったときに当該セッションを切断することができる。また、１つ以上のアクセスマネージャ２４５は、同じポリシーを取得することができる。よって、次に同じユーザが正しいユーザ名およびパスワードを使用してログインしようとするときに、１つ以上のアクセスマネージャ２４５は、ユーザアクセスを許可しないことがある。したがって、リソースが１つ以上のエージェント、例えば１つ以上のプロキシ２４０によって保護されていなくても、１つ以上のエージェント２３５、１つ以上のアクセスマネージャ２４５および／または１つ以上のウエブゲート２５０は、ポリシーバス２１０と同じポリシーを有するため、ユーザ活動に対して独自の行動をとることができる。したがって、ルールが決定されるとエージェントがグループとして同様に反応する従来のシステムと異なって、各エージェントは、各々異なる方法でポリシーに反応することができる。

【０１２１】

図２はさらに、イベント／データの収集およびユーザ活動に対して静的ポリシーおよび動的ポリシーの実行に基づいて、ユーザインターフェイスを提供するためのメカニズムを示している。様々な実施形態において、統合ユーザインターフェイス２８０が、視覚化サーバ２３０から提供される。いくつかの実施形態において、統合ユーザインターフェイス２８０は、能動的脅威カテゴリ、各脅威カテゴリに対してトリガされたポリシーの数および関連するトレンドを含む。他の実施形態において、統合ユーザインターフェイス２８０は、ユーザ、ユーザによってアクセスされているソース、およびそのような活動に関連する可能なポリシーを含む。さらに他の実施形態において、リアルタイム統計値は、所定の

時間間隔（例えば、２秒、４秒、５秒、３０秒）で、５分または１５分などの異なる時間枠において統合ユーザインターフェイス２８０上に公開および表示される。これによって、セキュリティ管理者は、「リアルタイムのトレンド」に対して適切な措置を講じることができる。

【０１２２】

統合ユーザインターフェイス２８０は、セキュリティ管理者がシステムにログインするときに、セキュリティ管理者に提示されてもよい。統合ユーザインターフェイス２８０は、ネットワークトラフィックを生成しているトップユーザ、およびこれらのユーザがアクセスしているソースを提示することができる。収集バス２０５から収集されたリアルタイムデータは、システムに供給されてもよい。統合ユーザインターフェイス２８０は、一定の期間（例えば、５分または３０分）に、ユーザがネットワーク上の異なるソースにアクセスした頻度を提示することができる。統合ユーザインターフェイス２８０は、新しいデータが入ってくると、例えば「現在の時間－５分」を示すように絶えずに更新されてもよい。上位のアクティブＩＰアドレスを示すこともできる。いくつかの実施形態は、非常にアクティブであるＩＰアドレスと、人気であり且つトラフィックが多いソース（例えば、ＵＲＬ）との間の相関関係を示すことができる。また、特定の実施形態は、（例えば、星印を用いて）特定されていないユーザのＩＰアドレスを標記することができる。

【０１２３】

いくつかの実施形態は、ユーザ－アプリケーションマッピングに加えて、クライアントＩＰアドレス－アプリケーションマッピングを提示することができる。特定の実施形態は、特定のＩＰアドレスから多くの異なるソースにアクセスすることができること、またはその逆、全ての異なるユーザが特定のＵＲＬにアクセスすることができることを示すことができる。統合ユーザインターフェイス２８０は、一方側にエンドユーザ（またはクライアントのＩＰアドレス）を提示し、他方側にエンドソースを提示する。また、いくつかの実施形態は、色を用いて、グループを区別することができる。また、特定の実施形態は、各アプリケーションがアクセスされた回数などの情報を提示することもできる。いくつかの実施形態は、特定のユーザまたはクライアントのＩＰアドレスを選択することによって、特定のユーザまたはクライアントのＩＰアドレスからアプリケーションにアクセスした回数を提示することができる。

【０１２４】

いくつかの実施形態において、管理者は、統合ユーザインターフェイス２８０を介して、１つ以上の比較基準および基準値を指定することができる。また、特定の実施形態において、管理者は、統合ユーザインターフェイス２８０を介して、イベントの１つ以上の基準および基準値が管理者によって指定された基準および基準値と一致する場合に所望の警告および警告期間を指定することができる。例えば、いくつかの実施形態において、ユーザおよびクライアントＩＰアドレスが当該ユーザがアクセスしている宛先（例えば、ホスト名、特定のＩＰアドレス、サービス）と一致するまたはユーザの活動と一致するときに、管理者によって指定された対応の警告を提供することができる。

【０１２５】

ＩＩＩ．統合ユーザインターフェイス

図３は、様々な実施形態に従って、脅威視覚化システム３００の一部の機能要素を示すブロック図である。図示されたシステムは、３つの層、すなわち、プレゼンテーション層３０５、アプリケーション層３１０、およびデータベース層３１５を含む。プレゼンテーション層３０５は、複数のユーザインターフェイス（例えば、グラフィカルユーザインターフェイス（ＧＵＩ））を含む。ユーザ（例えば、顧客または管理者）は、リアルタイムで脅威を検出するために、複数のユーザインターフェイスを介して、企業のネットワーク上のユーザ活動を監視することができる。複数のユーザインターフェイスは、複数のＵＩ３２０、３２５、３３０および３３５（例えば、図２を参照して説明した統合ユーザインターフェイス２８０）を含む。いくつかの実施形態において、ＵＩ３２０、３２５、３３０および３３５は、１つ以上のワークステーションに存在する。他の実施形態において、

ＵＩ３２０、３２５、３３０および３３５は、１つ以上のパーソナルコンピュータに存在する。通常、ＵＩ３２０、３２５、３３０および３３５は、任意のコンピューティングシステムに存在することができる。なお、図３には４つのＵＩが示されているが、本明細書に記載の態様によれば、任意の数のＵＩを開発および提供することができる。

【０１２６】

ＵＩ３２０、３２５、３３０および３３５は、アプリケーション層３１０内の１つ以上のアプリケーションサーバ３４０および３４５（例えば、図２を参照して説明した分析サーバ２２０、機械学習コンポーネント２２５および視覚化サーバ２３０）に接続されている。アプリケーションサーバ３４０および３４５は、ＵＩ３２０、３２５、３３０および３３５と企業ネットワークとの間に情報を交換および処理することによって、企業基盤ネットワーク上のセキュリティおよび脅威のリアルタイム評価を容易にする動作を実行する。様々な実施形態において、アプリケーションサーバ３４０および３４５は、本明細書に記載された一組のメカニズムを介して、セキュリティおよび脅威の評価を容易にする。アプリケーションサーバ３４０および３４５は、計算サーバまたはデータベースサーバを含む分散コンピューティングシステム内のいくつかの場所に配置されることができ、プレゼンテーション層内の任意のＵＩと通信することができる。

【０１２７】

アプリケーションサーバ３４０および３４５は、データベース層３１５内のデータベース管理システム３５０（例えば、図２を参照して説明したメモリ２５５）に接続されている。データベース管理システム３５０は、データの保存および検索を管理できる任意種類の特製または市販のデータベースシステムであってもよい。いくつかの実施形態において、データベース管理システム３５０は、データベースサーバなどを含む。例示的なデータベースサーバは、Oracle（登録商標）、Microsoft（登録商標）、Sybase（登録商標）、IBM（登録商標）などの会社から市販されているものを含むがこれらに限定されない。データベース管理システム３５０は、キャッシュおよびデータベース３５５（例えば、図２を参照して説明したキャッシュ２６５、２７０およびデータベース２６０）に接続されている。キャッシュおよびデータベース３５５は、データを格納および検索することができる任意種類のキャッシュまたはデータベースであってもよい。データベースの例として、階層データベースおよびリレーショナルデータベースを含むがこれらに限定されない。

【０１２８】

様々な実施形態において、プレゼンテーション層３０５、アプリケーション層３１０およびデータベース層３１５は、能動的脅威カテゴリ、各脅威カテゴリに対してトリガされたポリシーの数および関連するトレンドを含むＵＩ３２０、３２５、３３０および３３５を提供するように動作する。図４Ａおよび図４Ｂに示すように、いくつかの実施形態は、脅威レベルの分類体系に基づいて、能動的脅威の統合ＵＩ４００を提供することができる。本明細書に説明したように、実行ポリシー（例えば、静的ポリシーおよび動的ポリシー）は、ブロックポリシー、ステップアップまたは第２ファクタポリシー、高警告ポリシー、中警告ポリシー、および低警告ポリシーに各々分類することができる。例えば、分析サーバ２２０および機械学習コンポーネント２２５は、例えば、１回のみのアクセスが観察された場合、低警告として、「異常なアプリケーションアクセス」ポリシーを動的に作成することができる。しかしながら、他の要因に基づいて、同じポリシーは、第２ファクタポリシーとして導入され、認証されていないユーザによるアクセスを阻止することができる。アプリケーション層３１０は、このようなポリシー実行措置の分類方式を使用して、ブロック４０５、ステップアップまたは第２ファクタ４１０、高警告４１５、中警告４２０および低警告４２５に対応する様々なバケットを含む統合ＵＩ４００のダッシュボード４０２を表示することができる。ポリシー実行措置の脅威レベルの分類体系によって、管理者は、ポリシーの評価および低レベルから高レベルへのレベルの上昇またその逆を行うことができる。また、いくつかの実施形態は、ポリシーの評価またはポリシーの脅威レベルの昇降を判断するときに、機械学習コンポーネント２２５を含むことができる。さらに、ポリシー名ではなく脅威レベルに基づいて能動的脅威の統合ＵＩ４００を提供すること

によって、セキュリティ管理グループは、ポリシー名に基づいて脅威レベルを解釈する代わりに、分類に基づいて異なる種類の脅威および措置に集中することができる。

【０１２９】

バケット４０５、４１０、４１５、４２０および４２５は、任意の時点で企業ネットワーク上のユーザ活動によってトリガされ、対応する分類を有するポリシーの総数「ｎ」４３０を含むことができる。バケット４０５、４１０、４１５、４２０および４２５は、分類ごとに、関連するトレンドをトリガされたポリシーの数「ｎ」４３０にさらに含むことができる。例えば、マーカ４３５およびグラフ４４０などの図形を用いて、トリガされたポリシーの数「ｎ」４３０に対応する履歴トレンドを示すことができる。いくつかの実施形態において、トリガされたポリシーの数「ｎ」４３０が増加している場合（例えば、ｎ＋１、５、１０、１５など）、上向き矢印を用いて、このようなトレンドを容易に示すことができる。対照的に、トリガされたポリシーの数「ｎ」４３０が減少している場合（例えば、ｎ－１、５、１０、１５など）、下向き矢印を用いて、このようなトレンドを容易に示すことができる。トリガされたポリシーの数「ｎ」４３０が実質的に同様である場合（例えば、＋／－５％、１０％、または１５％）、円を用いて、このようなトレンドを容易に示すことができる。特定の実施形態において、バケット４０５、４１０、４１５、４２０および４２５は、ドロップダウンボックス４４５をさらに含み、管理者は、このドロップダウンボックス４４５を利用して、企業ネットワーク上にトリガされたポリシーおよびユーザによって実行されている活動（アクセスされているソース）に関する詳細をさらに調査することができる。特定の実施形態において、統合ＵＩ４００は、任意の所定の時間に実行されているポリシーの総数「ｍ」（全ての分類グループ）を示すための追加のバケット４５０をさらに含む。

【０１３０】

本明細書に説明した様々な態様によれば、企業ネットワーク上のユーザ行動を監視することができ、ユーザに対して１つ以上の動的ポリシーを作成することができる。いくつかの実施形態において、管理者または機械学習コンポーネント２２５は、特定の行動によってブロック、第２ファクタ認証、低警告、中警告または高警告をトリガするための実行ポリシーを設定することができる。例えば、機械学習コンポーネント２２５は、履歴データから、リアルタイムデータの変動または逸脱（例えば、通常はユーザが午後７時または午後８時ごろ自宅からアクセスするが、今日はユーザが別の場所からアクセスしていること）を検出することができ、この異常なアクセスに対してポリシーを作成することができる。このポリシーは、当該アクセスに対して、警告レベル（例えば、低、中または高警告）、第２ファクタ認証、またはブロックを指定することができる。ユーザが第２ファクタ認証を介して提示されたチャレンジで認証されたか否かに基づいて、システムは、履歴データを利用してポリシーを修正することができる。ユーザのさらなる行動によって警告レベルが上がり、新しいポリシーがユーザの行動を高警告行動として指定した場合、統合ユーザインターフェイス４００は、ダッシュボード４０２を介して、高警告行動の提示を開始することができる。短期間（例えば、過去１０秒または過去２０秒）にこのユーザに対して複数回（例えば、１０回または２０回）の高警告があった場合、問題がある可能性があるため、機械学習コンポーネント２２５は、統合ユーザインターフェイス４００を介して管理者に警告することができる。

【０１３１】

いくつかの実施形態において、ダッシュボード４０２は、上位アクセス活動、ソースにアクセスしている上位ユーザ、ソースにアクセスするために使用されている上位ＩＰアドレス、およびアクセスされている上位ソースを含む情報を表示する様々なウィンドウ４５５を含むことができる。上位または下位は、例えば、上位または下位５、１０、１５、３５、または５０という閾値数として定義されてもよい。代替的には、上位または下位は、例えば、上位または下位５％、１０％、１５％、３５％、または５０％という閾値百分率として定義されてもよい。ウィンドウ４５５は、任意のグラフィック手段を用いて情報を表示することができる。例えば、上位アクセス活動は、各ユーザＩＤまたはＩＰアドレス

をアクセスされているリソースまたはターゲットシステムに連結する線を示すピクトグラムまたは線図４６０を用いて表示することができる。追加的にまたは代替的に、上位ユーザは、フォントのサイズまたは色などの印刷変更を伴う比例面積チャート、バブルチャートまたはタグクラウド４６５を用いて表示することができる。追加的または代替的に、上位ＩＰアドレスは、フォントのサイズまたは色などの印刷変更を伴う比例面積チャート、バブルチャートまたはタグクラウド４７０を用いて表示することができる。追加的にまたは代替的に、アプリケーションは、フォントのサイズまたは色などの印刷変更を伴う比例面積チャート、バブルチャートまたはタグクラウド４７５を用いて表示することができる。

【０１３２】

いくつかの実施形態において、プレゼンテーション層３０５、アプリケーション層３１０およびデータベース層３１５は、追加の機能または情報を管理者に提供するようにさらに動作することができる。例えば、図５に示すように、管理者は、マウスポインタなどの入力装置をダッシュボードのウィンドウ５１０内の特定のユーザ５０５上に置くことによって、その特定のユーザがアクセスしたリソース５１５を単独に表示することができる。また、図６に示すように、管理者は、マウスポインタなどの入力装置をダッシュボードのウィンドウ６１０内の特定のＵＲＬ６０５上に置くことによって、ユーザまたはＩＰアドレスがリソースにアクセスした特定のカウント数または回数６１５を見ることができる。図７に示すように、管理者は、マウスポインタなどの入力装置をダッシュボードのウィンドウ７１０内の特定のＵＲＬ７０５上に置くことによって、そのＵＲＬにアクセスしている様々なユーザ７１５を見ることができる。図８に示すように、管理者は、マウスポインタなどの入力装置を用いてダッシュボードのウィンドウ８１０から特定のユーザ８０５を選択することによって、特定のユーザ８０５を選択的に監視することができる。図９に示すように、管理者は、比例面積チャート９１５またはバブルチャートを用いて、特定のユーザ９１０の活動９０５を監視することができる。図１０に示すように、管理者は、マウスポインタなどの入力装置をＵＲＬ上に置くことによって、特定のユーザ１０１０が比例面積チャート１０２０またはバブルチャート内のＵＲＬ１０１５にアクセスした回数１００５を見ることができる。図１１に示すように、管理者は、複数の比例面積チャート１１１０またはバブルチャートを用いて、複数のユーザ１１０５の活動を監視することができる。

【０１３３】

いくつかの実施形態において、プレゼンテーション層３０５、アプリケーション層３１０およびデータベース層３１５は、１つ以上のポリシー（例えば、検査ポリシーまたは実行ポリシー）を作成するための追加の機能を管理者に提供するようにさらに動作することができる。図１２Ａおよび１２Ｂは、特定の実施形態に従って、管理者が１つ以上のポリシーを作成することを可能にするためのＵＩ１２０５の一例を示している。いくつかの実施形態において、管理者は、異常活動を観察した後に、本明細書に記載のＵＩのいずれかを用いて１つ以上のポリシーを作成することができる。管理者は、ユーザＩＤ、ＩＰアドレスまたはグループなどを指定することによって、ポリシーのソース１２１０を指定することができ、またはソース１２１０を空白にすることによって、任意のソースを指定することができる。管理者は、ホスト名、ターゲットシステム名またはＩＤ、ＩＰアドレス、リソース名などを用いて、ポリシーの宛先１２１５を指定することができ、または宛先１２１５を空白にすることによって、任意の宛先に指定することができる。管理者は、ポリシーの実行措置１２２０を指定することができる。実行措置１２２０は、低警告、中警告、高警告、第２ファクタ認証、またはブロックを含むことができる。なお、異常活動から検知された脅威レベルを用いて、ポリシーを低リスク、中リスク、高リスク、第２ファクタ認証リスク、またはブロックリスクに分類することもできる。管理者は、ポリシーがアクティブになる期間または所定期間１２２５を指定することができる。いくつかの実施形態において、期間１２２５は、５、１５、３０、または６０分とすることができる。これによって、管理者は、所定期間中に、本明細書に記載のＵＩのいずれかを介して、ネットワークトラフィックに対するポリシーの影響を見ることができる。その後、ポリシーが意

図した効果を持たなかった場合またはポリシーが異常活動に適用できなくなった場合に、管理者は、そのポリシーを失効させることができ、または期間１２２５を変更することによって、そのポリシーのアクティブ状態を延長することができる。特定の実施形態において、期間１２２５を永久にすることができる。これによって、管理者は、静的ポリシーを永久的に上書きすることができ、またはリアルタイムで企業ネットワーク上のセキュリティ戦略を変更することができる。

【０１３４】

いくつかの実施形態において、プレゼンテーション層３０５、アプリケーション層３１０およびデータベース層３１５は、追加の機能または情報を管理者に提供するようにさらに動作することができる。いくつかの実施形態は、特定の時間間隔に特定の種類のポリシー（例えば、ブロックポリシー）の数を管理者に示すことができる。特定の実施形態において、管理者は、（例えば、ＵＩ要素を選択することによって）特定の措置または警告（例えば、ブロック）を引き起こしたポリシーを見ることができる。例えば、図１３に示すように、特定の実施形態に従って、管理者は、対応のモード１３１５（例えば、上位ブロックポリシーモード）を選択することによって、ウィンドウ１３１０内の各分類の上位ポリシー１３０５の名前を見ることができる。また、いくつかの実施形態において、管理者は、ウィンドウ１３２５内で、上位ポリシー１３０５に関連し且つポリシーを複数回に違反した上位ユーザ１３２０を見ることができる。上位または下位は、例えば、上位または下位５、１０、１５、３５、または５０という閾値数として定義されてもよい。代替的に、上位または下位は、例えば、上位または下位５％、１０％、１５％、３５％、または５０％という閾値百分率として定義されてもよい。図１４に示すように、いくつかの実施形態に従って、管理者は、ウィンドウ１４１０内のリソース１４０５および上位ポリシー１３０５に基づいてとられた実行措置（例えば、ブロック）を見ることができる。これらの表示によって、管理者は、各分類または検知された脅威レベルに対してトリガされている上位ポリシーに関連するユーザ、リソース、ＩＰアドレスおよびポリシーを確認することができる。いくつかの実施形態において、管理者は、特定のユーザを選択して、その特定のユーザによって引き起こされた警告の数（例えば、そのユーザによって引き起こされた１５個のブロックおよび２つの第２ファクタ）を見ることができる。

【０１３５】

様々な種類の情報を管理者に提示することによって、管理者は、（例えば、異なるトレンドに応じて）適切な行動をとることができる。本明細書記載のＵＩが特定の警告に対して上昇トレンドを示すことによって、管理者は、警告の上昇トレンドを見たときに、上昇トレンドのみに応じて適切な行動をとることができる。いくつかの実施形態において、管理者は、特定のポリシーに従って高警告によってブロックされた、特定のアプリケーションにアクセスしているユーザ／クライアントＩＰアドレス／ソースを見ることができる。ポリシーを見るときに、一部の属性によって、管理者は、手動で導入されたポリシーと機械学習ポリシーとを区別することができる。いくつかの実施形態において、管理者は、機械学習ポリシーではなく、手動で作成されたポリシーのみを編集することができる。

【０１３６】

様々な実施形態において、管理者は、低、中および高警告を監視し、警告を引き起こした特定のポリシーを修正する必要がある推奨、例えば、ブロックポリシーのために高警告を修正する必要がある推奨を提供する。他のシステム管理者は、推奨された変更すべきポリシーの通知を受け、そのポリシーをブロックポリシーにアップグレードするか否かを判断することができる。図１５に示すように、特定の実施形態に従って、管理者は、対応のモード１５１５（例えば、高警告ポリシーモード）を選択することによって、ウィンドウ１５１０内の各分類（例えば、高警告）の上位ポリシー１５０５の名前を見ることができる。図１６に示すように、いくつかの実施形態に従って、管理者は、ウィンドウ１６１０内のリソース１６０５および上位ポリシー１５０５に基づいてとられた措置（例えば、高警告）を見ることができ、ウィンドウ１６２０内のＩＰアドレス１６１５および上位ポリシー１５０５に基づいてとられた措置（例えば、高警告）を見ることができる。

【０１３７】
様々な実施形態において、プレゼンテーション層３０５、アプリケーション層３１０およびデータベース層３１５は、ユーザ、ユーザによってアクセスされているリソース、およびアクセス活動に関連する可能なポリシーを含むＵＩ３２０、３２５、３３０および３３５を提供するように動作する。図１７に示すように、いくつかの実施形態は、トリガされたポリシーに基づいて、能動的脅威を示す統合ＵＩ１７００を提供することができる。例えば、特定の実施形態において、管理者は、特定の行動または警告（例えば、ブロック）を引き起こしたポリシーを見ることができる。図１７に示すように、管理者は、ポリシーをトリガしている企業ネットワーク上の活動のソース１７０５（例えば、ユーザＩＤ、グループ指定、ＩＰアドレス、クライアント装置ＩＤなど）、トリガされたポリシー１７１０（例えば、静的実行ポリシーおよび動的実行ポリシー）の名前または分類を示すインジケータ、およびソース１７０５からの活動の宛先１７１５（例えば、アクセスされているリソースまたはサービス）を示すウィンドウ１７０５を見ることができる。これらの表示によって、管理者は、各ユーザによってトリガされたポリシーおよびリソースを見ることができる。いくつかの実施形態において、管理者は、特定のユーザを選択して、その特定のユーザによってトリガされたポリシーに集中することができる（例えば、このユーザは、１５個のブロックポリシーおよび２つの第２ファクタポリシーをトリガした）。図１８に示すように、管理者は、様々なソース１８０５、クライアントＩＰアドレス１８１０、宛先ＩＰポート１８１５、宛先ホスト名１８２０、要求ＵＲＬ１８２５、トリガされた各ポリシー１８３０、およびポリシー１８３０に対して取られた措置を示すポリシー分類１８４０に関する追跡活動を見ることができる。いくつかの実施形態において、検索バー１８４５を用いて、追跡活動を検索することができる。

【０１３８】
ＩＶ．脅威知能プラットフォームを利用するためのプロセスおよび操作
図１９～２１は、いくつかの実施形態に従って、動的ポリシーを用いてセキュリティイベントを分析し、分散環境内の能動的脅威、ユーザ活動並びに能動的脅威およびユーザ活動によってトリガされた動的ポリシーを含む統合ビューを提供するための技術を示している。個々の実施形態は、フローチャート、流れ図、データ流れ図、構造図、またはブロック図として示されたプロセスとして説明されてもよい。フローチャートは、動作を逐次プロセスとして説明するが、多くの動作は、並行にまたは同時に実行されてもよい。また、動作の順序は、変更されてもよい。プロセスは、その動作が完了すると終了するが、図面に含まれていない追加のステップを含むことができる。プロセスは、方法、機能、手順、サブルーチン、サブプログラムなどに対応してもよい。プロセスが機能に対応する場合、プロセスの終了は、呼出し機能またはメイン機能に戻ることに対応してもよい。

【０１３９】
図１９～２１に示されたプロセスおよび／または動作は、１つ以上の処理ユニット（例えば、プロセッサコア）ハードウェア、またはそれらの組み合わせによって実行されるソフトウェア（例えば、コード、命令、プログラム）に実施することができる。ソフトウェアは、メモリ（例えば、メモリ装置、非一時的コンピュータ可読記憶媒体）に格納することができる。図１９～２１に示された一連の特定の処理ステップは、限定的であることを意図していない。代替的な実施形態に従って、他の一連のステップを実行することができる。例えば、代替的な実施形態において、異なる順序で上述したステップを実行してもよい。また、図１９～２１に示された各ステップは、各ステップに適切である様々な順序で実行され得る複数のサブステップを含むことができる。さらに、特定の用途に応じて、追加のステップを追加または削除してもよい。当業者は、多くの変形、修正および代替を認識するだろう。

【０１４０】
図１９は、様々な実施形態に従って、動的ポリシーを作成および公開するためのプロセスを示すフローチャート１９００である。いくつかの実施形態において、フローチャート１９００に示されたプロセスは、図１に示され、図２を参照して説明されたアクセス管理

および脅威検出システム１０５および情報管理システム１１０によって実施されてもよい。ステップ１９０５において、ユーザ装置、複数のエージェント、収集バス、ポリシーバス、およびリソースを有するターゲットシステムを含む分散環境を提供するまたはインスタンス化する。いくつかの実施形態において、分散環境は、分析サーバおよび機械学習コンポーネントをさらに含み、検査ポリシーおよび動的実行ポリシーは、分析サーバおよび機械学習コンポーネントによって作成される。特定の実施形態において、分散環境は、検査ポリシー、動的実行ポリシーおよび１つ以上の情報フローから受信した履歴データを格納するためのメモリをさらに含む。

【０１４１】

任意選択のステップ１９１０において、履歴データまたはターゲットシステムもしくはリソースの指定に基づいて、検査ポリシーを作成することができる。いくつかの実施形態において、データの収集は、ポリシーバス上に公開された検査ポリシーによってトリガされる。例えば、収集バスは、エンドユーザのアクセス要求などのセキュリティイベントに関連する情報を取得し、その情報またはデータをレポートバスに報告するように構成されてもよい。収集バスは、特定の基準が満たされたときに一組の定義済み属性（例えば、ユーザ属性、リソース属性、オブジェクト、アクション、環境属性など）を収集するためのルールを含むデフォルトまたは静的検査ポリシーに基づいて、構成されてもよい。特定の実施形態において、システムは、検査ポリシーＵＩを提供することができ、管理者は、この検査ポリシーＵＩを用いて、一組の基準が満たされたとき（例えば、特定の時間間隔においてヘッダデータが一致する場合）にトリガされる特定の検査ポリシーを指定することによって、検査ポリシーを作成することができる。他の実施形態において、収集バスは、データまたは属性を収集するためのルールを含む動的検査ポリシーに基づいて、構成されてもよい。例えば、収集バスおよび分析サーバは、連携して一組の定義済み属性を収集し、以前に構成されたルール（デフォルト、静的または動的検査および実行ポリシー）に基づいて、異常をトリガすることができる。この検査ポリシーは、セキュリティイベントに関する一組の基準が所定のパターンと一致するときにセキュリティイベントに関する一組の所定の属性であるデータをリアルタイムで収集するためのルールを含む。データは、収集バスによって収集された後、メモリに格納され、履歴データの一部になる。機械学習コンポーネントは、履歴データおよびリアルタイムデータを絶えずに学習することによって、システム上のユーザ活動の脅威評価に必要な情報を効率的に収集するように、検査ポリシーおよび実行ポリシーを作成および変更することができる。

【０１４２】

任意選択のステップ１９１５において、複数のエージェントが検査ポリシーにアクセスできるように、検査ポリシーをポリシーバス上に公開するまたはポリシーバスに導入することができる。検査ポリシーをポリシーバス上に公開することは、リスナ（すなわち、エージェント）がポリシーにアクセスし、以前に設定されたルールに基づいて一組の定義済み属性を収集するようにポリシーを実行することを可能にすることによって、データの収集を容易にする。ステップ１９２０において、セキュリティイベントに関するデータを収集することができる。様々な実施形態において、データは、（ｉ）ユーザまたはユーザ装置を特定するためのソース、および（ｉｉ）ターゲットシステムまたはリソースを特定するための宛先を含む。データは、収集バスによって、複数のエージェントのうち少なくとも１つのエージェントから収集されてもよい。いくつかの実施形態において、データは、デフォルト、静的または動的検査ポリシーに従って収集される。例えば、ソースから宛先へのデータフローを含むライブ情報フローの基準がデフォルト、静的または動的検査ポリシー内の事前定義パターンと一致する場合、検査ポリシーが起動され、１つ以上のエージェントが、情報フローの属性（例えば、ソースおよび宛先）または情報フロー内に発生したセキュリティイベントを収集することができる。その後、収集された属性は、さらなる処理を行うために、本明細書に記載された様々な態様に従って収集バスに送信されてもよい。

【０１４３】

ステップ１９２５において、データに基づいて動的実行ポリシーを作成することができる。動的実行ポリシーは、少なくともソース、宛先、実行措置、および動的実行ポリシーがアクティブになる期間の指定を含む。期間は、少なくとも５分、少なくとも１０分、少なくとも３０分、または少なくとも１時間、例えば１０分、３０分、１時間、５時間、１日、または３日という所定期間であってもよい。動的実行ポリシーがアクティブになる期間中に、動的実行ポリシーは、少なくとも同じソースおよび同じ宛先の指定を含む静的実行ポリシーを上書きする。例えば、静的実行ポリシーは、第１レベルの認証を必要とするＩＰアドレスからユーザが指定されたターゲットシステム上のリソースにアクセスしようとするたびに、そのＩＰアドレスからのユーザまたはユーザグループに対してデフォルトまたはアクティブである。動的実行ポリシーは、第２ファクタ認証を必要とする同じＩＰアドレスからユーザが指定された同じターゲットシステム上のリソースにアクセスしようとするたびに、そのＩＰアドレスからのユーザまたはユーザグループに対して公開されてもよい。動的実行ポリシーは、５時間の期間を有してもよい。したがって、所定期間（例えば、５時間）中に静的実行ポリシーが非アクティブである場合、所定期間（例えば、５時間）中に、動的実行ポリシーは、アクティブである（例えば、ＩＰアドレスから特定のターゲットシステムへのアクセス要求に対して、第２ファクタ認証が実行される）。所定期間（例えば、５時間）が経過した後、動的実行ポリシーは、非アクティブになり、ポリシーバスから除去され、静的実行ポリシーは、アクティブになる（例えば、ＩＰアドレスから特定のターゲットシステムへのアクセス要求に対して、第１レベル認証が実行される）。

【０１４４】

特定の実施形態において、システムは、実行ポリシーＵＩを提供することができ、管理者は、この実行ポリシーＵＩを用いて、一組の属性が満たされたとき（例えば、ライブ情報フローがポリシーのソースおよび宛先と一致する場合）にトリガされる特定の実行措置を指定することによって、動的実行ポリシーを作成することができる。他の実施形態において、分析サーバおよび機械学習コンポーネントは、動的実行ポリシーを作成する。動的実行ポリシーの作成は、リアルタイムで収集されたデータおよび履歴データを１つ以上のデータクラスタに分類することと、１つ以上のデータクラスタを用いて、一組の定義済み属性を分析することと、分析に基づいて、ソース、宛先、実行措置、および動的実行ポリシーがアクティブになる期間を作成することとを含む。１つ以上のデータクラスタは、教師付きまたは教師なし機械学習またはクラスタリング技術を用いて生成することができ、分析は、１つ以上のデータクラスタの重心から一組の定義済み属性までの距離を計算することを含むことができる。ブロック認証または第２ファクタ認証などの実行措置は、１つ以上のデータクラスタの重心から一組の定義済み属性までの距離に基づいて決定されてもよい。

【０１４５】

ステップ１９３０において、複数のエージェントが動的実行ポリシーにアクセスすることができるように、動的実行ポリシーをポリシーバス上に公開することができる。動的実行ポリシーをポリシーバス上に公開することは、リスナー（すなわち、エージェント）がポリシーにアクセスし、以前に構成されたルールに基づいてポリシーの実行措置を作動させることを可能にすることによって、例えば、企業ネットワーク上の脅威の検出を容易にする。ステップ１９３５において、動的実行ポリシーに基づいて、セキュリティイベントに対して実行措置を実施してもよい。いくつかの実施形態において、複数のエージェントのうち少なくとも１つのエージェントは、実行措置を実行する。実行措置は、情報フローの属性（例えば、ソースおよび宛先）または情報フロー内で発生するセキュリティイベントが指定された動的実行ポリシーの属性（例えば、ソースおよび宛先）と一致すると判断された場合、複数のエージェントのうち少なくとも１つのエージェントによって実施されてもよい。その後、例えば、（ｉ）ユーザのアクセスが認可される前に宛先へのユーザアクセスをブロックすること、（ｉｉ）ユーザと宛先との接続を切断すること、（ｉｉｉ）システム上のユーザの認証をブロックすること、（ｉｉｉ）第２ファクタ認証または認可

を要求すること、（ｉｖ）低警告、中警告または高警告を報告することによって、実行措置は、複数のエージェントのうち少なくとも１つのエージェントによって実施されてもよい。

【０１４６】

図２０は、能動的脅威カテゴリ、各脅威カテゴリのためにトリガされたポリシーの数および関連するトレンドの統合ビューを提供するためのプロセスを示すフローチャート２０００である。いくつかの実施形態において、フローチャート２０００に示されたプロセスは、図１に示され、図２を参照して説明されたアクセス管理および脅威検出システム１０５および情報管理システム１１０によって実施されてもよい。ステップ２００５において、ユーザ装置、複数のエージェント、収集バス、ポリシーバス、およびリソースを有するターゲットシステムを含む分散環境を提供するまたはインスタンス化する。いくつかの実施形態において、分散環境は、分析サーバおよび機械学習コンポーネントをさらに含み、検査ポリシーおよび動的実行ポリシーは、分析サーバおよび機械学習コンポーネントによって作成される。特定の実施形態において、分散環境は、検査ポリシー、動的実行ポリシー、および１つ以上の情報フローから受信した履歴データを格納するためのメモリをさらに含む。

【０１４７】

ステップ２０１０において、１つ以上のライブ情報フローを監視することができる。ライブ情報フローは、複数のソースから複数の宛先へのデータフローを含むことができる。いくつかの実施形態において、監視は、複数のエージェントによって実行される。監視は、様々なポリシー（例えば、検査ポリシーおよび実行ポリシー）に従って実行されてもよい。ステップ２０１５において、複数のバケットを含むユーザインターフェイスを提供することができる。各バケットは、異なる脅威レベルまたは実行措置に関連してもよく、各バケットは、関連する脅威レベルまたは実行措置を含み、リアルタイムでトリガされている現在の実行ポリシーの総数を表示する。図４Ａに示すように、バケットは、本質的に、脅威レベルまたは各ポリシーに宣言された実行措置に基づいて実行ポリシーに割り当てられた同じ分類体系（例えば、ブロック、第２ファクタ認証、低警告、中警告、高警告など）に従って分類されたグラフィカルサイロである。ポリシー名ではなく、脅威レベルまたは実行措置バケットに基づいて能動的脅威の統合ＵＩを提供することによって、セキュリティ管理グループは、ポリシー名に基づいて脅威レベルを解釈するのではなく、分類に基づいて様々な種類の脅威および措置に集中することができる。

【０１４８】

ステップ２０２０において、実行ポリシーのトリガに基づいて、１つ以上のライブ情報フロー内のセキュリティイベントの発生を判断する。実行ポリシーは、ソース、宛先、および実行措置の指定を含むことができ、１つ以上のライブ情報フロー内のデータが少なくとも実行ポリシーのソースおよび宛先と一致する場合、実行ポリシーがトリガされ、実行措置が適用される。ステップ２０２５において、セキュリティイベントの発生を反映するように、（ｉ）複数のバケットから、実行ポリシーによって適用された実行措置に関連するバケットを特定すること、および（ｉｉ）実行措置によってリアルタイムでトリガされ、特定されたバケットに表示されている現在の実行ポリシーの総数を増やすことによって、ユーザインターフェイスを更新することができる。いくつかの実施形態において、実行ポリシーの総数を増やすことは、実行ポリシーの総数のカウント数ｎをカウント数ｎ＋１に増分することを含む。任意選択のステップ２３０において、セキュリティイベントの発生に基づいて、特定されたバケットを示すトレンドインジケータを更新することができる。例えば、トレンドインジケータを更新することは、特定されたバケット内に上向き矢印、下向き矢印または無色円を表示させることを含むことができる。

【０１４９】

任意選択のステップ２０３５において、複数のバケットからバケットの選択に対応するユーザ入力を受け取ることができる。いくつかの実施形態において、選択に応じて、選択されたバケットに対応する複数のソースおよび複数の宛先を含むライブ情報フローをユー

ザインターフェイスに表示することができる。他の実施形態において、選択に応じて、選択されたバケットに対応する複数のソースをタグクラウドとしてユーザインターフェイスに表示することができる。タグクラウドは、各ソースの使用率に比例して、選択されたバケットに対応する複数のソースを示すことができる。

【０１５０】

任意選択のステップ２０４０において、複数のソースから特定のソースの選択に対応するユーザ入力を受け取ることができる。いくつかの実施形態において、選択に応じて、特定のソースから始まるライブ情報フローが表示される。任意選択のステップ２０４５において、複数の宛先から特定の宛先の選択に対応するユーザ入力を受け取ることができる。いくつかの実施形態において、選択に応じて、特定の宛先で終わるライブ情報フローが表示される。任意選択のステップ２０５０において、複数のソースおよび複数の宛先を含むライブ情報フローをユーザインターフェイスに表示することができる。いくつかの実施形態において、複数のソースから複数の宛先に流れるデータ量に基づいて、一組の上位ソースを示すインジケータを提供することができる。任意選択のステップ２０５５において、複数のソースおよび複数の宛先を含むライブ情報フローをユーザインターフェイスに表示することができる。いくつかの実施形態において、複数のソースから複数の宛先に流れるデータ量に基づいて、一組の上位宛先を示すインジケータを提供することができる。任意選択のステップ２０６０において、複数のソースおよび複数の宛先を含むライブ情報フローをユーザインターフェイスに表示することができる。いくつかの実施形態において、複数のソースから複数の宛先に流れるデータ量およびポリシーバス上に公開された一組のアクティブな実行ポリシーに基づいて、一組の上位実行ポリシーを示すインジケータを提供することができる。

【０１５１】

任意選択のステップ２０６５において、データに基づいて、動的実行ポリシーを作成するための要求を受け取ることができる。動的実行ポリシーは、ソース、宛先、実行措置、および動的実行ポリシーがアクティブになる期間の指定を含むことができる。任意選択のステップ２０７０において、複数のエージェントが動的実行ポリシーにアクセスすることができるように、動的実行ポリシーをポリシーバス上に公開することができる。本明細書に説明したように、期間は、少なくとも５分、少なくとも１０分、少なくとも３０分、または少なくとも１時間、例えば１０分、３０分、１時間、５時間、１日、または３日という所定期間であってもよい。動的実行ポリシーがアクティブになる期間中に、動的実行ポリシーは、少なくとも同じソースおよび同じ宛先の指定を含む静的実行ポリシーを上書きする。任意選択のステップ２０７５において、動的実行ポリシーに基づいて、１つ以上のライブ情報フロー内の別のセキュリティイベントに対して実行措置を実行することができる。複数のエージェントのうち少なくとも１つのエージェントは、実行措置を実行することができる。任意選択のステップ２０８０において、別のセキュリティイベントに対する実行措置の実行を反映するように、（ｉ）複数のバケットから、実行ポリシーによって適用された実行措置に関連するバケットを特定することおよび（ｉｉ）実行措置によってリアルタイムでトリガされ、特定されたバケットに表示されている現在の実行ポリシーの総数を増やすことによって、ユーザインターフェイスを更新することができる。

【０１５２】

図２１は、ユーザ、ユーザによってアクセスされたアプリケーション、およびアクセスに関連する可能なアクセスポリシーの統合ビューを提供するためのプロセスを示すフローチャート２１００である。いくつかの実施形態において、フローチャート２１００に示されたプロセスは、図１に示され、図２を参照して説明されたアクセス管理および脅威検出システム１０５および情報管理システム１１０によって実施されてもよい。ステップ２１０５において、ユーザ装置、複数のエージェント、収集バス、ポリシーバス、およびリソースを有するターゲットシステムを含む分散環境を提供するまたはインスタンス化する。いくつかの実施形態において、分散環境は、分析サーバおよび機械学習コンポーネントをさらに含む。検査ポリシーおよび動的実行ポリシーは、分析サーバおよび機械学習コンポ

ーネントによって作成される。特定の実施形態において、分散環境は、検査ポリシー、動的実行ポリシー、および１つ以上の情報フローから受信した履歴データを格納するためのメモリをさらに含む。

【０１５３】

ステップ２１１０において、ライブ情報フローを監視することができる。ライブ情報フローは、ソースから宛先へのデータフローを含むことができる。いくつかの実施形態において、監視は、複数のエージェントによって実行される。監視は、様々なポリシー（例えば、検査ポリシーおよび実行ポリシー）に従って実行されてもよい。任意選択のステップ２１１５において、１つ以上のライブ情報フローを監視することができる。例えば、１つ以上の追加のライブ情報フローを監視することができる。追加のライブ情報フローは、（ｉ）複数のソースから複数の宛先へのデータフロー、および（ｉｉ）データによってトリガされた１つ以上の実行ポリシーを含むことができる。ステップ２１２０において、回線を介して接続されたソースおよび宛先を含むユーザインターフェイスを提供することができる。例えば、図１７に示すように、ライブ情報フローに含まれた各ソースは、グラフィカルラインを介して、アクセスされている１つ以上の宛先に接続されてもよい。選択的に、追加のライブ情報フローを監視する場合、ユーザインターフェイスは、（ｉ）複数のソースの各ソースを対応する複数の宛先の各宛先に接続するための１つ以上の回線、および（ｉｉ）各ソースと各宛先との間に流れるデータによってトリガされる実行ポリシーを示す各回線上のインジケータをさらに含むことができる。

【０１５４】

ステップ２１２５において、実行ポリシーのトリガに基づいて、ライブ情報フロー内のセキュリティイベントの発生を判断することができる。実行ポリシーは、ソース、宛先、および実行措置の指定を含むことができ、１つ以上のライブ情報フロー内のデータが少なくとも実行ポリシーのソースおよび宛先と一致する場合、実行ポリシーがトリガされ、実行措置が適用される。ステップ２１３０において、セキュリティイベントの発生を反映するように、（ｉ）実行ポリシーのインジケータを特定すること、および（ｉｉ）実行ポリシーのインジケータを通過するソースと宛先を接続する回線を表示することによって、ユーザインタフェースを更新することができる。いくつかの実施形態において、ソースは、ユーザインターフェイスのウィンドウの一方側に表示され、宛先は、ソースを有する側と反対するウィンドウの他方側に表示され、実行ポリシーのインジケータは、ソースと宛先との間の回線上に表示される。

【０１５５】

任意選択のステップ２１３５において、複数のソースから特定のソースの選択に対応するユーザ入力を受け取ることができる。いくつかの実施形態において、選択に応じて、ライブ情報フロー内のデータによってトリガされた１つ以上の実行ポリシーを含む特定のソースから始まるライブ情報フローが表示される。任意選択のステップ２１４０において、複数の宛先から特定の宛先の選択に対応するユーザ入力を受け取ることができる。いくつかの実施形態において、選択に応じて、ライブ情報フロー内のデータによってトリガされた１つ以上の実行ポリシーを含む特定の宛先で終わるライブ情報フローが表示される。任意選択のステップ２１４５において、複数のソースおよび複数の宛先を含むライブ情報フローをユーザインターフェイスに表示することができる。いくつかの実施形態において、複数のソースから複数の宛先に流れるデータ量に基づいて、一組の上位ソースを示すインジケータを提供することができる。任意選択のステップ２１５０において、複数のソースおよび複数の宛先を含むライブ情報フローをユーザインターフェイスに表示することができる。いくつかの実施形態において、複数のソースから複数の宛先に流れるデータ量に基づいて、一組の上位宛先を示すインジケータを提供することができる。任意選択のステップ２１５５において、複数のソースおよび複数の宛先を含むライブ情報フローをユーザインターフェイスに表示することができる。いくつかの実施形態において、複数のソースから複数の宛先に流れるデータ量およびポリシーバス上に公開された一組のアクティブな実行ポリシーに基づいて、一組の上位実行ポリシーを示すインジケータを提供することがで

きる。

【０１５６】

任意選択のステップ２１６０において、データに基づいて、動的実行ポリシーを作成するための要求を受け取ることができる。動的実行ポリシーは、ソース、宛先、実行措置、および動的実行ポリシーがアクティブになる期間の指定を含むことができる。任意選択のステップ２１６５において、複数のエージェントが動的実行ポリシーにアクセスすることができるように、動的実行ポリシーをポリシーバス上に公開することができる。本明細書に説明したように、期間は、少なくとも５分、少なくとも１０分、少なくとも３０分、または少なくとも１時間、例えば１０分、３０分、１時間、５時間、１日、または３日という所定期間であってもよい。動的実行ポリシーがアクティブになる期間中に、動的実行ポリシーは、少なくとも同様のソースおよび同様の宛先の指定を含む静的実行ポリシーを上書きする。任意選択のステップ２１７０において、動的実行ポリシーに基づいて、１つ以上のライブ情報フロー内の別のセキュリティイベントに対して実行措置を実行することができる。複数のエージェントのうち少なくとも１つのエージェントは、実行措置を実行することができる。任意選択のステップ２１７５において、別のセキュリティイベントに対する実行措置の実行を反映するように、（ｉ）実行ポリシーのインジケータを特定することおよび（ｉｉ）実行ポリシーのインジケータを通過するソースと宛先とを接続する回線を表示することによって、ユーザインターフェイスを更新することができる。

【０１５７】

Ｖ．コンピューティング環境

図２２は、本開示の一実施形態を実施するための分散システム２２００を示す簡略図である。図示の実施形態において、分散システム２２００は、１つ以上のネットワーク２２１０を介して、ウェブブラウザまたは専用クライアント（例えば、オラクル（登録商標）フォーム）などのようなクライアントアプリケーションを実行および作動するように構成された１つ以上のクライアントコンピューティング装置２２０２、２２０４、２２０６および２２０８を含む。サーバ２２１２は、ネットワーク２２１０を介して、リモートクライアントコンピューティング装置２２０２、２２０４、２２０６および２２０８と通信可能に連結されてもよい。

【０１５８】

様々な実施形態において、サーバ２２１２は、１つ以上のサービスまたはソフトウェアアプリケーション、例えばサービスおよびＩＤ管理サービスを提供するためのアプリケーションを実行するように構成されてもよい。特定の実施形態において、サーバ２２１２は、他のサービスを提供することができ、ソフトウェアアプリケーションは、非仮想環境および仮想環境を含むことができる。いくつかの実施形態において、これらのサービスは、ウエブサービスまたはクラウドサービスとして、またはSaaS（Software as a Service）モデルに基づいて、クライアントコンピューティング装置２２０２、２２０４、２２０６および／または２２０８のユーザに提供されてもよい。クライアントコンピューティング装置２２０２、２２０４、２２０６および／または２２０８を操作するユーザは、１つ以上のクライアントアプリケーションを用いて、サーバ２２１２と情報を交換することによって、これらのコンポーネントによって提供されたサービスを利用することができる。

【０１５９】

図２２に示す構成において、システム２２００のソフトウェアコンポーネント２２１８、２２２０および２２２２は、サーバ２２１２に実装されている。他の実施形態において、システム２２００の１つ以上のコンポーネントおよび／またはこれらのコンポーネントによって提供されたサービスは、１つ以上のクライアントコンピューティング装置２２０２、２２０４、２２０６および／または２２０８によって実現されてもよい。クライアントコンピューティング装置を操作するユーザは、１つ以上のクライアントアプリケーションを用いて、これらのコンポーネントによって提供されたサービスを利用することができる。これらのコンポーネントは、ハードウェア、ファームウェア、ソフトウェア、またはこれらの組み合わせで実現されてもよい。理解すべきことは、分散システム２２００と異

なる様々なシステム構成が可能であることである。したがって、図２２に示された実施形態は、実施形態のシステムを実現するための分散システムの一例であり、限定を意図していない。

【０１６０】

クライアントコンピューティング装置２２０２、２２０４、２２０６および／または２２０８は、様々な種類のコンピューティングシステムを含むことができる。例えば、クライアント装置は、例えば、Microsoft Windows Mobile（登録商標）のようなソフトウェア、および／またはｉＯＳ、Windows（登録商標）フォン、アンドロイド（登録商標）、ブラックベリー（登録商標）１０およびパームＯＳなどの様々なモバイルオペレーティングシステムを実行することができる手持ち式携帯装置（例えば、iPhone（登録商標）、携帯電話、Ipad（登録商標）、タブレット、携帯情報端末（ＰＤＡ）または着用できる装置（Google Glass（登録商標）ヘッドマウントディスプレイ）を含むことができる。装置は、様々なアプリケーション、例えば様々なインターネット関連アプリケーション、電子メールアプリケーション、ショートメッセージサービス（ＳＭＳ）アプリケーションをサポートすることができ、様々な他の通信プロトコルを使用することができる。また、クライアントコンピューティング装置は、例示として、Microsoft Windows（登録商標）オペレーティングシステム、Apple Macintosh（登録商標）オペレーティングシステムおよび／またはリナックス（登録商標）オペレーティングシステムの様々なバージョンを実行するパーソナルコンピュータおよび／またはラップトップコンピュータを含む汎用のパーソナルコンピュータを含んでもよい。クライアントコンピューティング装置は、例えば、様々なＧＮＵ／リナックスオペレーティングシステム、例えば、Google Chrome OSを含むがこれに限定されない市販のＵＮＩＸ（登録商標）またはＵＮＩＸに類似する様々なオペレーティングシステムを実行するワークステーションコンピュータであってもよい。クライアントコンピューティング装置は、ネットワーク２２１０を介して通信可能なシンクライアントコンピュータ、インターネット対応のゲームシステム（例えば、Kinect（登録商標）ジェスチャ入力装置を備えるまたは備えないMicrosoft Xboxゲームコンソール）、および／またはパーソナルメッセージング装置などの他の電子機器を含んでもよい。

【０１６１】

図２２の分散システム２２００は、４つのクライアントコンピューティング装置を備えると示されているが、任意の数のクライアントコンピューティング装置をサポートすることができる。他の装置、例えばセンサを有する装置は、サーバ２２１２と情報を交換することができる。

【０１６２】

分散システム２２００のネットワーク２２１０は、ＴＣＰ／ＩＰ（伝送制御プロトコル／インターネットプロトコル）、ＳＮＡ（システムネットワークアーキテクチャ）、ＩＰＸ（インターネットパケット交換）、Apple Talkなどを含むがこれらに限定されない様々な市販プロトコルのいずれかを使用してデータ通信をサポートすることができ、当業者に熟知される任意種類のネットワークであってもよい。単なる例示として、ネットワーク２２１０は、ローカルエリアネットワーク（ＬＡＮ）、イーサネット（登録商標）に基づいたネットワーク、トークンリング、広域ネットワーク、インターネット、仮想プライベートネットワーク（ＶＰＮ）、イントラネット、エクストラネット、公衆交換電話ネットワーク（ＰＳＴＮ）、赤外線ネットワーク、無線ネットワーク（例えば、ＩＥＥＥ１００２．１１プロトコルスイート、Bluetooth（登録商標）および／または任意の他の無線プロトコルの下で動作するネットワーク）および／またはこれらのネットワークと他のネットワークの組み合わせを含むことができる。

【０１６３】

サーバ２２１２は、１つ以上の汎用コンピュータ、専用サーバコンピュータ（例示として、ＰＣ（パーソナルコンピュータ）サーバ、ＵＮＩＸ（登録商標）サーバ、ミッドレンジサーバ、メインフレームコンピュータ、ラックマウントサーバを含む）、サーバファー

ム、サーバクラスタ、または任意の他の適切な構成および／または組み合わせから構成されてもよい。サーバ２２１２は、仮想オペレーティングシステムを実行する１つ以上の仮想マシンまたは仮想化を含む他のコンピューティングアーキテクチャを含むことができる。論理記憶装置の１つ以上のフレキシブルプールを仮想化して、サーバの仮想記憶装置を維持することができる。仮想ネットワークは、ソフトウェア定義ネットワーキングを用いて、サーバ２２１２によって制御されてもよい。様々な実施形態において、サーバ２２１２は、前述の開示に記載された１つ以上のサービスまたはソフトウェアアプリケーションを実行するように構成することができる。例えば、サーバ２２１２は、本開示の実施形態に従って上記に説明した処理を実行するためのサーバに対応することができる。

【０１６４】

サーバ２２１２は、上述したものいずれかを含むオペレーティングシステム、および任意の市販サーバオペレーティングシステムを動かすことができる。また、サーバ１０９は、ＨＴＴＰ（ハイパーテキスト転送プロトコル）サーバ、ＦＴＰ（ファイル転送プロトコル）サーバ、ＣＧＩ（共通ゲートウェイインターフェイス）サーバ、Java（登録商標）サーバ、データベースサーバなどを含む様々な追加サーバアプリケーションおよび／または中間層アプリケーションのいずれかを動かすことができる。例示的なデータベースサーバは、Oracle（登録商標）、Microsoft（登録商標）、Sybase（登録商標）、IBM（登録商標）などの会社から市販されているものを含むがこれらに限定されない。

【０１６５】

いくつかの実現例において、サーバ２２１２は、クライアントコンピューティング装置２２０２、２２０４，２２０６、および２２０８のユーザから受信したデータフィードおよび／またはイベント更新を分析および統合する１つ以上のアプリケーションを含んでもよい。例示として、データフィードおよび／またはイベント更新は、Twitter（登録商標）フィード、Facebook（登録商標）更新または１つ以上の第３情報源および連続データストリームから受信したリアルタイム更新を含むがこれらに限定されない。リアルタイム更新は、センサデータアプリケーション、金融相場表示機、ネットワーク性能測定ツール（例えば、ネットワーク監視およびトラフィック管理アプリケーション）、ページ遷移（Clickstream）解析ツール、自動車交通監視装置などに関連するリアルタイムイベントを含
むことができる。また、サーバ２２１２は、クライアントコンピューティング装置２２０２、２２０４、２２０６および２２０８の１つ以上の表示装置を介して、データフィードおよび／またはリアルタイムイベントを表示するための１つ以上のアプリケーションを含むこともできる。

【０１６６】

また、分散システム２２００は、１つ以上のデータベース２２１４および２２１６を含むことができる。これらのデータベースは、様々な実施形態によって使用される情報、例えばユーザＩＤ情報および他の情報を格納するためのメカニズムを提供することができる。データベース２２１４および２２１６は、様々な場所に常駐することができる。例示として、１つ以上のデータベース２２１４および２２１６は、サーバ２２１２の近く（および／またはその中）の非一時記憶媒体に常駐することができる。代替的には、データベース２２１４および２２１６は、リモートサーバ２２１２から離れており、ネットワークに基づく接続または専用接続を介して、サーバ２２１２と通信している。一組の実施形態において、データベース２２１４および２２１６は、記憶領域ネットワーク（ＳＡＮ）に常駐することができる。同様に、サーバ２２１２に寄与する機能を実行するための任意の必要なファイルは、必要に応じて、サーバ２２１２上に／またはサーバ２２１２から離れた場所に保存されてもよい。一組の実施形態において、データベース２２１４および２２１６は、例えば、Oracleにより提供されるデータベースなどの関係データベースを含むことができる。これらの関係データベースは、ＳＱＬフォーマット命令に応じて、データを取得、保存および更新するように構成されている。

【０１６７】

いくつかの実施形態において、上述したＩＤ管理サービスは、クラウド環境を介したサービスとして提供されてもよい。図２３は、本開示の一実施形態に従って、サービスをクラウドサービスとして提供することができるシステム環境２３００の１つ以上のコンポーネントを示す簡略ブロック図である。図２３に示す実施形態において、システム環境２３００は、１つ以上のクライアントコンピューティング装置２３０４、２３０６および２３０８を含み、ユーザは、これらのクライアントコンピューティング装置を用いて、会社のターゲットシステムに格納された資格情報を管理するためのサービスを含むクラウドサービスを提供するクラウドインフラストラクチャシステム２３０２と情報を交換することができる。クラウドインフラストラクチャシステム２３０２は、サーバ２２１２に関して上述したものを含むことができる１つ以上のコンピュータおよび／またはサーバを含むことができる。

【０１６８】

理解すべきことは、図８に示されたクラウドインフラストラクチャシステム２３０２は、図示されたコンポーネント以外のコンポーネントを備えてもよいことである。さらに、図８に示された実施形態は、本発明の実施形態を組み込むことができるクラウドインフラストラクチャシステムの一例に過ぎない。いくつかの他の実施形態において、クラウドインフラストラクチャシステム２３０２は、図示よりも多いまたは少ないコンポーネントを有してもよく、２つ以上のコンポーネントを組み合わせてもよく、または異なる構成または配置のコンポーネントを有してもよい。

【０１６９】

クライアントコンピューティング装置２３０４、２３０６および２３０８は、上述した装置２２０２、２２０４、２２０６および２２０８と同様である。クライアントコンピューティング装置２３０４、２３０６および２３０８は、ウエブブラウザ、専用クライアントアプリケーション（例えば、オラクル（登録商標）フォーム）または他のアプリケーションなどのクライアントアプリケーションを作動するように構成されることができる。ユーザは、これらのクライアントアプリケーションを用いて、クラウドインフラストラクチャシステム２３０２と情報を交換することによって、クラウドインフラストラクチャシステム２３０２により提供されたサービスを利用することができる。例示的なシステム環境２３００は、３つのクライアントコンピューティング装置を備えると示されているが、任意の数のクライアントコンピューティング装置をサポートすることができる。他の装置、例えばセンサを有する装置は、クラウドインフラストラクチャシステム２３０２と情報を交換することができる。

【０１７０】

ネットワーク２３１０は、クライアント２３０４、２３０６および２３０８とクラウドインフラストラクチャシステム２３０２との間のデータの通信および交換を促進することができる。各ネットワークは、上記でネットワーク７１０に関して説明したプロトコルを含む様々な市販プロトコルのいずれかを用いてデータ通信をサポートすることができ、当業者に熟知する任意の種類のネットワークであってもよい。

【０１７１】

特定の実施形態において、クラウドインフラストラクチャシステム２３０２によって提供されたサービスは、需要に応じて、クラウドインフラストラクチャシステムのユーザに提供できる多くのサービスを含むことができる。ＩＤ管理に関連するサービスに加えて、オンラインデータストレージおよびバックアップソリューション、ウエブベースの電子メールサービス、ホストされたオフィススイートおよびドキュメントコラボレーションサービス、データベース処理、管理された技術サポートサービスを含むがこれらに限定されない様々な他のサービスを提供することもできる。クラウドインフラストラクチャシステムによって提供されるサービスは、ユーザのニーズを満たすように動的に拡張することができる。

【０１７２】

特定の実施形態において、クラウドインフラストラクチャシステム２３０２によって提

供されたサービスの特定のインスタンス化は、本明細書において、「サービスインスタンス」と呼ばれる。一般的には、インターネットなどの通信ネットワークを介して、クラウドサービスプロバイダのシステムからユーザに提供できる任意のサービスは、「クラウドサービス」と呼ばれる。典型的には、パブリッククラウド環境において、クラウドサービスプロバイダのシステムを構成するサーバおよびシステムは、顧客のオンプレミスサーバおよびシステムとは異なる。例えば、クラウドサービスプロバイダのシステムは、アプリケーションを提供することができ、ユーザは、必要に応じて、インターネットなどの通信ネットワークを介して、アプリケーションを注文し、使用することができる。

【０１７３】

いくつかの例において、コンピュータネットワーククラウドインフラストラクチャ内のサービスは、保護されたコンピュータネットワークのストレージアクセス、ホストされたデータベース、ホストされたウエブサーバ、ソフトウェアアプリケーション、またはクラウドベンダによってユーザに提供された他のサービス、または当該技術分野に知られている他のサービスを含むことができる。例えば、サービスは、インターネットを介して、クラウド上のリモートストレージに対して、パスワードにより保護されたアクセスを含むことができる。別の例として、サービスは、ウエブサービスにホストされている関係データベースおよびネットワーク上の開発者により私的使用のためのスクリプト言語ミドルウェアエンジンを含むことができる。別の例として、サービスは、クラウドベンダのウエブサイト上にホストされている電子メールソフトウェアアプリケーションに対するアクセスを含むことができる。

【０１７４】

特定の実施形態において、クラウドインフラストラクチャシステム２３０２は、セルフサービスのサブスクリプションに基づく、柔軟なスケーラビリティ、信頼性、高可用性および安全性を有する方法で、顧客に提供できる一連のアプリケーション、ミドルウェアおよびデータベースサービスを含むことができる。このようなクラウドインフラストラクチャシステムの例示として、本願譲受人により提供されたオラクルパブリッククラウドが挙げられる。

【０１７５】

また、クラウドインフラストラクチャシステム２３０２は、「ビッグデータ」関連の計算および分析サービスを提供することができる。「ビッグデータ」という用語は、一般的に極めて大きいデータセットを指す。分析者および研究者は、格納されたビッグデータを利用して、大量のデータを視覚化し、データからトレンドを検出しおよび／またはデータと対話することができる。ビッグデータおよび関連アプリケーションは、インフラストラクチャシステムによって、様々なレベルおよび様々な規模でホストおよび／または利用されてもよい。並列にリンクされた数十個、数百個または数千個のプロセッサは、このようなデータを計算することによって、データを提示したり、データに作用する外力またはデータの表現をシミュレートすることができる。これらのデータセットは、データベースに組織化されたデータまたは他の構造化モデルに従って組織化されたデータなどの構造化データおよび／または非構造化データ（例えば、電子メール、画像、データブロブ（バイナリラージオブジェクト）、ウエブページ、複雑なイベント処理）を含む。一実施形態に従って、クラウドインフラストラクチャシステムは、より多くの（またはより少ない）コンピューティングリソースを比較的迅速に目的に集中させることによって、企業、政府機関、研究機関、個人、個人同士または組織のグループ、または他の団体の需要に基づいて、大きなデータセットに対してタスクをよりよく実行することができる。

【０１７６】

様々な実施形態において、クラウドインフラストラクチャシステム２３０２は、顧客から申込んだクラウドインフラストラクチャシステム２３０２のサービスを自動的に提供、管理および追跡するように構成されることができる。クラウドインフラストラクチャシステム２３０２は、様々な展開モデルを介して、クラウドサービスを提供することができる。例えば、サービスは、クラウドサービスを販売する組織に所有された（例えば、オラク

ル社に所有された）クラウドインフラストラクチャシステム２３０２を有するパブリッククラウドモデルで提供され、一般人または異なる業界の企業に利用されることができる。別の例として、サービスは、単一の組織に専用されたクラウドインフラストラクチャシステム２３０２を有するプライベートクラウドモデルで提供され、組織内の１つ以上の実体に利用されることができる。また、クラウドサービスは、集団クラウドモデルで提供されてもよい。よって、クラウドインフラストラクチャシステム２３０２およびクラウドインフラストラクチャシステム２３０２により提供されたサービスは、関連する集団内の複数の組織によって共有される。また、クラウドサービスは、２つ以上の異なるモデルの組み合わせからなるハイブリッドクラウドモデルで提供されてもよい。

【０１７７】

いくつかの実施形態において、クラウドインフラストラクチャシステム２３０２によって提供されたサービスは、SaaS（Software as a Service）カテゴリ、PaaS（Platform as
a Service）カテゴリ、IaaS（Infrastructure as a Service）カテゴリ、またはハイブリッドサービスを含む他のカテゴリのサービスに準拠して提供された１つ以上のサービスを含むことができる。顧客は、サブスクリプション申込書によって、クラウドインフラストラクチャシステム２３０２によって提供された１つ以上のサービスを注文することができる。これに応じて、クラウドインフラストラクチャシステム２３０２は、顧客のサブスクリプション申込書に含まれたサービスを提供する処理を行う。

【０１７８】

いくつかの実施形態において、クラウドインフラストラクチャシステム２３０２によって提供されたサービスは、アプリケーションサービス、プラットフォームサービスおよびインフラストラクチャサービスを含むがこれらに限定されない。いくつかの例において、アプリケーションサービスは、SaaSプラットフォームを介して、クラウドインフラストラクチャシステムによって提供されてもよい。SaaSプラットフォームは、SaaSカテゴリに準拠するクラウドサービスを提供するように構成されてもよい。例えば、SaaSプラットフォームは、統合の開発および展開プラットフォーム上にオンデマンドアプリケーションのスイートを構築し、提供するように、機能することができる。SaaSプラットフォームは、SaaSサービスを提供するために、基礎のソフトウェアおよびインフラストラクチャを管理し、制御することができる。SaaSプラットフォームにより提供されたサービスを利用することによって、顧客は、クラウドインフラストラクチャシステム上に動作するアプリケーションを利用することができる。顧客は、別々のライセンスおよびサポートを購入する必要なく、アプリケーションサービスを取得することができる。様々な異なるSaaSサービスを提供することができる。例示としては、販売実績管理、企業統合、および大規模組織のビジネス柔軟性に対する解決策を提供するサービスを含むがこれらに限定されない。

【０１７９】

いくつかの実施形態において、プラットフォームサービスは、クラウドインフラストラクチャシステム２３０２によって、PaaSプラットフォームを介して提供されてもよい。PaaSプラットフォームは、PaaSカテゴリに準拠するクラウドサービスを提供するように構成されてもよい。プラットフォームサービスの例としては、共有されている共通アーキテクチャ上に既存のアプリケーションを統合する能力、およびプラットフォームにより提供された共有サービスを活用する新規アプリケーションを構築する能力を組織（例えば、Oracle社）に与えるサービスを含むがこれに限定されない。PaaSプラットフォームは、PaaSサービスを提供するために、基礎のソフトウェアおよびインフラストラクチャを管理し、制御することができる。顧客は、別々のライセンスおよびサポートを購入する必要なく、クラウドインフラストラクチャシステム２３０２によって提供されたPaasサービスを利用することができる。プラットフォームサービスの例としては、oracle Javaクラウドサービス（JCS）、Oracleデータベースクラウドサービス（DBCS）およびその他を含むがこれらに限定されない。

【０１８０】

PaaSプラットフォームにより提供されたサービスを利用することによって、顧客は、クラウドインフラストラクチャシステムにサポートされているプログラミング言語およびツールを利用することができ、展開されたサービスを制御することができる。いくつかの実施形態において、クラウドインフラストラクチャシステムによって提供されるプラットフォームサービスは、データベースクラウドサービス、ミドルウェアクラウドサービス（例えば、Oracle Fusionミドルウェアサービス）、およびJavaクラウドサービスを含むことができる。一実施形態において、データベースクラウドサービスは、データベースリソースを蓄積する能力を組織に与えることができる共有サービス展開モデルをサポートすることができ、DBaaS（Database as a Service）をクラウドデータベースとして顧客に提供することができる。ミドルウェアクラウドサービスは、クラウドインフラストラクチャシステム上に様々なビジネスアプリケーションを開発および展開するためのプラットフォームを顧客に提供することができ、Javaクラウドサービスは、クラウドインフラストラクチャシステム上にJavaアプリケーションを展開するためのプラットフォームを顧客に提供することができる。

【０１８１】

様々な異なるインフラストラクチャサービスは、IaaSプラットフォームによって、クラウドインフラストラクチャシステムに提供されてもよい。これらのインフラストラクチャサービスは、SaaSプラットフォームおよびPaaSプラットフォームにより提供されたサービスを利用する顧客のために、ストレージ、ネットワークおよびその他の基本的なコンピューティングリソースとしての基礎コンピューティングリソースの管理と制御を容易にする。

【０１８２】

特定の実施形態において、クラウドインフラストラクチャシステム１４０２はまた、クラウドインフラストラクチャシステムを利用する顧客に、様々なサービスを提供するために使用されるリソースを提供するためのインフラストラクチャリソース１４３０を含むことができる。一実施形態において、インフラストラクチャリソース１４３０は、PaaSプラットフォームおよびSaaSプラットフォームおよび他のリソースによって提供されたサービスを実行するために、事前に統合され且つ最適化されたサーバリソース、ストレージリソースおよびネットワークリソースなどのハードウェアの組み合わせを含んでもよい。

【０１８３】

いくつかの実施形態において、クラウドインフラストラクチャシステム２３０２内のリソースは、複数のユーザに共有されることができ、各々の需要に応じて動的に再割当てることができる。また、リソースは、異なるタイムゾーンでユーザに割当てることができる。例えば、クラウドインフラストラクチャシステム２３０２は、指定時間内でクラウドインフラストラクチャシステムのリソースを第１時間帯における第１グループのユーザに利用させ、その後、同様のリソースを異なる時間帯における別のグループのユーザに再配分することができ、リソースを最大に利用する。

【０１８４】

特定の実施形態において、提供された複数の内部共有サービス２３３２は、クラウドインフラストラクチャシステム２３０２の異なる構成要素またはモジュールに共有されることによって、クラウドインフラストラクチャシステム２３０２がサービスを提供することができる。これらの内部共有サービスは、安全性および識別サービス、統合サービス、企業リポジトリサービス、企業管理サービス、ウイルススキャンおよびホワイトリストサービス、高可用性のバックアップおよびリカバリサービス、クラウドサポートを可能にするサービス、メールサービス、通知サービス、およびファイル転送サービスなどを含むがこれらに限定されない。

【０１８５】

特定の実施形態において、クラウドインフラストラクチャシステム２３０２は、クラウドインフラストラクチャシステム内のクラウドサービス（例えば、SaaSサービス、PaaSサービスおよびIaaSサービス）を包括的に管理する機能を提供することができる。一実施形

態において、クラウド管理機能は、クラウドインフラストラクチャシステム２３０２などによって受信した顧客のサブスクリプションを提供、管理、および追跡する機能を含んでもよい。

【０１８６】

一実施形態において、図２３に示すように、クラウド管理機能は、１つ以上のモジュール、例えば、オーダー管理モジュール（order management module）２３２０、オーダー
調整モジュール（order orchestration module）２３２２、オーダー支給モジュール（order provisioning module）２３２４、オーダー管理および監視モジュール（order management and monitoring module）２３２６、およびＩＤ管理モジュール（identity management module）２３２８によって提供される。これらのモジュールは、１つ以上のコンピ
ュータおよび／またはサーバを含んでもよく、これらを用いて形成されてもよい。これらのコンピュータおよび／またはサーバは、汎用コンピュータ、専用サーバコンピュータ、サーバファーム、サーバクラスタ、または任意の他の適切な配置および／またはこれらの組み合わせであってもよい。

【０１８７】

例示的な操作２３３４において、顧客は、クライアント装置、例えば、クライアント装置２３０４、２３０６または２３０８を用いて、クラウドインフラストラクチャシステム２３０２により提供された１つ以上のサービスをリクエストし、クラウドインフラストラクチャシステム２３０２によって提供された１つ以上のサービスのサブスクリプションをオーダーすることによって、クラウドインフラストラクチャシステム２３０２と情報を交換することができる。特定の実施形態において、顧客は、クラウドユーザインターフェイス（ＵＩ）、例えば、クラウドＵＩ２３１２、クラウドＵＩ２３２３および／またはクラウドＵＩ２３１６にアクセスし、これらのＵＩを介して、サブスクリプションを申し込むことができる。顧客のオーダーに応答してクラウドインフラストラクチャシステム２３０２によって受信したオーダー情報は、顧客と、クラウドインフラストラクチャシステム２３０２により提供され、顧客が購入しようとする１つ以上のサービスとを識別する情報を含むことができる。

【０１８８】

２３３６において、顧客から受け取ったオーダー情報をオーダーデータベース２３１８に格納することができる。このオーダーが新しいオーダーである場合、このオーダーに新しいレコードを作成することができる。一実施形態において、オーダーデータベース２３１８は、クラウドインフラストラクチャシステム２３１８によって操作され、または他のシステム要素と連動して操作されるいくつかのデータベースのうち１つであってもよい。

【０１８９】

２３３８において、オーダー情報は、オーダー管理モジュール２３２０に転送される。オーダー管理モジュール２３２０は、オーダーに関連する請求および会計機能、例えば、オーダーの確認、および確認後、オーダーの記入を実行するように構成されてもよい。

【０１９０】

２３４０において、オーダーに関する情報は、顧客がオーダーしたサービスおよびリソースの提供を用意するように構成されたオーダー調整モジュール２３２２に伝達されてもよい。いくつかの例において、オーダー調整モジュール２３２２は、オーダー支給モジュール１４２４のサービスを用いて、サービスおよびリソースの提供を用意することができる。特定の実施形態において、オーダー調整モジュール２３２２は、各オーダーに関連するビジネスプロセスを管理することができ、ビジネスロジックを適用することによって、オーダーに対して支給をするか否かを判断することができる。

【０１９１】

図２３に示す実施形態に示されたように、２３４２において、新規サブスクリプションのオーダーを受信すると、オーダー調整モジュール２３２２は、リソースを割当て、サブ

スクリプションのオーダーを満たすために必要なリソースを構成するように、リクエストをオーダー支給モジュール２３２４に送信する。オーダー支給モジュール２３２４は、顧客がオーダーしたサービス用のリソースを割当てることができる。オーダー支給モジュール２３２４は、クラウドインフラストラクチャシステム２３００によって提供されたクラウドサービスと、リクエストされたサービスを提供するためのリソースを供給するために使用される物理的な実装層との間の抽象化レベルを形成する。このように、オーダー調整モジュール２３２２は、たとえば、サービスおよびリソースをその場で支給するかまたは事前に支給するか、リクエストに応じて割当てる／与えるかなどの実装詳細から単離することができる。

【０１９２】

２３４４において、サービスおよびリソースを支給した後、要求されたサービスが使用可能であることを示す通知を加入顧客に送信することができる。いくつかの例において、顧客が要求したサービスの使用を可能にするための情報（例えば、リンク）を顧客に送信してもよい。

【０１９３】

２３４６において、オーダー管理および監視モジュール２３２６は、顧客のサブスクリプションオーダーを管理および追跡することができる。いくつかの例において、オーダー管理および監視モジュール２３２６は、顧客が購入したサービスの使用に関するサービス使用の統計データを収集するように構成されることができる。統計データとして、例えば、ストレージの使用量、データの転送量、ユーザの数、システムの起動時間およびシステムの停止時間が収集されてもよい。

【０１９４】

特定の実施形態において、クラウドインフラストラクチャシステム２３００は、ＩＤ管理モジュール２３２８を含むことができる。ＩＤ管理モジュール２３２８は、クラウドインフラストラクチャシステム２３００に、識別サービス、例えば、アクセス管理および認可サービスを提供するように構成することができる。いくつかの実施形態において、ＩＤ管理モジュール２３２８は、クラウドインフラストラクチャシステム２３０２によって提供されたサービスを利用したい顧客に関する情報を制御することができる。このような情報は、顧客のＩＤを承認する情報、および様々なシステムリソース（例えば、ファイル、ディレクトリ、アプリケーション、通信ポート、メモリセグメントなど）に対して許可された顧客の実行権限を記載する情報を含むことができる。ＩＤ管理モジュール２３２８は、各顧客に関する記述情報、記述情報にアクセスおよび変更する方法、および記述情報にアクセスおよび変更した顧客に対する管理を含むことができる。

【０１９５】

図２４は、本開示の実施形態を実施するために使用され得る例示的なコンピューティングシステム２４００を示す。いくつかの実施形態において、コンピューティングシステム２４００を用いて、上記の様々なサーバおよびコンピューティングシステムのうちいずれかを実装することができる。図２４に示すように、コンピューティングシステム２４００は、バスサブシステム２４０２を介して、複数の周辺サブシステムと通信する処理サブシステム２４０４を含む様々なサブシステムを含む。周辺サブシステムは、処理加速ユニット２４０６、Ｉ／Ｏサブシステム２４０８、記憶サブシステム２４１８および通信サブシステム２４２４を含むことができる。記憶サブシステム２４１８は、有形のコンピュータ可読記憶媒体２４２２およびシステムメモリ２４１０を含むことができる。

【０１９６】

バスサブシステム２４０２は、コンピュータシステム２４００の様々な構成要素およびサブシステムが必要に応じて相互通信させるための機構を形成する。図示には、バスサブシステム２４０２を単一のバスとして概略的に示しているが、代替的な実施形態において、バスサブシステムは、複数のバスを利用してもよい。バスサブシステム２４０２は、メモリバスまたはメモリコントローラ、周辺バス、および様々なバスアーキテクチャのいずれかを使用するローカルバスを備えるいくつかの種類のバス構造のいずれかを有してもよ

い。例えば、このようなアーキテクチャは、業界標準アーキテクチャ（ＩＳＡ）バス、マイクロチャネルアーキテクチャ（ＭＣＡ）バス、拡張ＩＳＡ（ＥＩＳＡ）バス、ビデオエレクトロニクス規格協会（ＶＥＳＡ）ローカルバス、および周辺構成要素相互接続（ＰＣＩ）バスを含むことができる。これらのバスは、ＩＥＥＥ　Ｐ１３８６．１規格に準拠した製造されたメザニンバスとして実現することができる。

【０１９７】

処理サブシステム２４０４は、コンピューティングシステム２４００の動作を制御し、１つ以上の処理ユニット２４３２、２４３４などを含むことができる。処理ユニットは、１つ以上のプロセッサ、例えば、シングルコアプロセッサまたはマルチコアプロセッサ、１つ以上コアのプロセッサまたはそれらの組み合わせを含むことができる。いくつかの実施形態において、処理サブシステム２４０４は、１つ以上の専用コプロセッサ、例えば、グラフィックプロセッサ、デジタルシグナルプロセッサ（ＤＳＰ）などを含むことができる。いくつかの実施形態において、処理サブシステム２４０４の処理ユニットのいくつかまたは全ては、特定用途向け集積回路（ＡＳＩＣ）またはフィールドプログラマブルゲートアレイ（ＦＰＧＡ）などの特製回路を用いて実装することができる。

【０１９８】

いくつかの実施形態において、処理サブシステム２４０４の処理ユニットは、システムメモリ２４１０またはコンピュータ可読記憶媒体２４２２に格納された命令を実行することができる。様々な実施形態において、処理ユニットは、様々なプログラムまたはコード命令を実行することができ、同時に実行しているプログラムまたはプロセスを維持することができる。任意の時間に実行されているプログラムコードの一部または全部は、システムメモリ２４１０および／または１つ以上の記憶装置を含み得るコンピュータ可読記憶媒体２４１０に常駐することができる。適切なプログラミングによって、処理サブシステム２４０４は、上述したように、使用パターンに応じて文書（例えば、ウエブページ）を動的に修正するための様々な機能を提供することができる。

【０１９９】

特定の実施形態において、特定の処理を実行するまたは処理サブシステム２４０４によって実行される処理の一部をオフロードするように、処理加速ユニット２４０６を提供することによって、コンピューティングシステム２４００によって実行される全ての処理を加速することができる。

【０２００】

Ｉ／Ｏサブシステム２４０８は、情報をコンピューティングシステム２４００に入力するための装置および機構および／またはコンピューティングシステム２４００からまたはコンピューティングシステム２４００を介して情報を出力するための装置および機構を含むことができる。一般的に、「入力装置」という用語は、情報をコンピューティングシステム２４００に入力するための全ての可能な装置および機構を含む。ユーザインターフェイス入力装置は、例えば、キーボード、マウスまたはトラックボールなどのポインティング装置、ディスプレイに組み込まれたタッチパッドまたはタッチスクリーン、スクロールホイール、クリックホイール、ダイヤル、ボタン、スイッチ、キーパッド、音声命令認識システムを備える音声入力装置、マイクロフォン、および他の種類の入力装置を含んでもよい。また、ユーザインターフェイス入力装置は、例えば、ユーザが入力装置を制御することおよび入力装置と対話することを可能にするMicrosoft Kinect（登録商標）モーションセンサなどのモーション検知および／またはジェスチャ認識装置、Microsoft Xbox（登録商標）３６０ゲームコントローラ、ジェスチャおよび音声命令を使用した入力を受信するためのインターフェイスを提供するための装置を含むことができる。また、ユーザインターフェイス入力装置は、Google Glass（登録商標）瞬き検出器のような眼球ジェスチャ認識装置を含むことができる。Google Glass瞬き検出器は、ユーザの眼球活動（例えば、写真を撮るときおよび／またはメニューを選択するときの「瞬き」）を検出し、眼球活動を入力装置（例えば、Google Glass）に入力する入力に変換する。さらに、ユーザインターフェイス入力装置は、音声命令を介してユーザと音声認識システム（例えば、Siri（

登録商標）ナビゲータ）との対話を可能にする音声認識検出装置を含んでもよい。
【０２０１】
ユーザインターフェイス入力装置の他の例としては、三次元（３Ｄ）マウス、ジョイスティックまたはポインティングスティック、ゲームパッド、グラフィックタブレット、スピーカなどのオーディオ／ビジュアル装置、デジタルカメラ、デジタルビデオカメラ、ポータブルメディアプレーヤ、ウェブカメラ、イメージスキャナ、指紋スキャナ、バーコード読取器、３Ｄスキャナ、３Ｄプリンタ、レーザ距離計、および視線追跡装置を含むがこれらに限定されない。さらに、ユーザインターフェイス入力装置は、例えば、コンピュータ断層撮影装置、磁気共鳴像装置、超音波放射断層撮影装置、および医療用超音波装置などのような医用画像入力装置を含んでもよい。また、ユーザインターフェイス入力装置は、例えば、ＭＩＤＩキーボードおよび電子楽器などの音声入力装置を含むことができる。
【０２０２】
ユーザインターフェイス出力装置は、ディスプレイサブシステム、インジケータライト、またはオーディオ出力装置などの非視覚ディスプレイを含んでもよい。ディスプレイサブシステムは、例えば、陰極線管（ＣＲＴ）、液晶ディスプレイ（ＬＣＤ）またはプラズマディスプレイを使用するフラットパネル装置、投射装置またはタッチスクリーンであってもよい。一般に、「出力装置」という用語を使用する場合、コンピュータシステム２４００から情報をユーザまたは他のコンピュータに出力するためのすべての可能な種類の装置および機構を含むことを意図している。例えば、ユーザインターフェイス出力装置は、文字、画像およびオーディオ／ビデオ情報を視覚的に伝達する様々な表示装置、例えば、モニタ、プリンタ、スピーカ、ヘッドフォン、カーナビゲーションシステム、プロッタ、音声出力装置、およびモデムを含むがこれらに限定されない。
【０２０３】
記憶サブシステム２４１８は、コンピューティングシステム２４００によって使用される情報を格納するためのリポジトリまたはデータストアを提供する。記憶サブシステム２４１８は、いくつかの実施形態の機能を提供する基本的なプログラミングおよびデータ構造を格納するための有形のコンピュータ可読記憶媒体を提供する。処理サブシステム２４０４によって実行されると上述した機能を提供するソフトウェア（プログラム、コードモジュール、命令）は、記憶サブシステム２４１８に格納されてもよい。これらのソフトウェアは、処理サブシステム２４０４の１つ以上の処理ユニットによって実行されてもよい。また、記憶サブシステム２４１８は、様々な態様に従って使用されるデータを格納するためのリポジトリを提供することができる。
【０２０４】
記憶サブシステム２４１８は、揮発性メモリ装置および不揮発性メモリ装置を含む１つ以上の非一時的メモリ装置を含むことができる。図２４に示すように、記憶サブシステム２４１８は、システムメモリ２４１０およびコンピュータ可読記憶媒体２４２２を含む。システムメモリ２４１０は、プログラム実行中に命令およびデータを記憶するための揮発性メインランダムアクセスメモリ（ＲＡＭ）と、固定命令を記憶するための不揮発性読取専用メモリ（ＲＯＭ）またはフラッシュメモリとを含むいくつかのメモリを含むことができる。いくつかの実装形態において、例えば起動中にコンピューティングシステム２４００の要素間に情報を転送することを助ける基本ルーチンを含む基本入力／出力システム（ＢＩＯＳ）が、通常ＲＯＭに格納されてもよい。ＲＡＭは、通常、処理サブシステム２４０４によって現在操作および実行されているデータおよび／またはプログラムモジュールを含む。いくつかの実装形態において、システムメモリ２４１０は、複数の異なる種類のメモリ、例えば、スタティックランダムアクセスメモリ（ＳＲＡＭ）またはダイナミックランダムアクセスメモリ（ＤＲＡＭ）を含むことができる。
【０２０５】
限定ではなく一例として、図２４に示すように、システムメモリ２４１０は、クライアントアプリケーション、ウエブブラウザ、中間層アプリケーション、関係データベース管理システム（ＲＤＢＭＳ）などを含むことができる応用プログラム２４１２、プログラム

データ２４１４およびオペレーティングシステム２４１６を格納することができる。一例として、オペレーティングシステム２４１６は、マイクロソフトウィンドウズ（登録商標）、Apple Macintosh（登録商標）および／もしくはＬｉｎｕｘ（登録商標）オペレーティングシステムの様々なバージョン、様々な市販のＵＮＩＸ（登録商標）もしくはＵＮＩＸライクオペレーティングシステム（様々なＧＮＵ／Ｌｉｎｕｘオペレーティングシステム、Google Chrome（登録商標）ＯＳなどを含むが、これらに限定されるものではない）、ならびに／または、ｉＯＳ、Windows（登録商標）フォン、アンドロイド（登録商標）ＯＳ、ブラックベリー（登録商標）１０ ＯＳおよびパーム（登録商標）ＯＳオペレーティングシステムなどのモバイルオペレーティングシステムを含むことができる。

【０２０６】

コンピュータ可読記憶媒体２４２２は、いくつかの実施形態の機能を提供するプログラミングおよびデータ構造を格納することができる。処理サブシステム２４０４によって実行されると上述した機能を提供するソフトウェア（プログラム、コードモジュール、命令）は、記憶サブシステム２４１８に格納されてもよい。一例として、コンピュータ可読記憶媒体２４２２は、不揮発性メモリ、例えば、ハードディスクドライブ、磁気ディスクドライブ、ＣＤ－ＲＯＭ、ＤＶＤ、ブルーレイ（登録商標）ディスクなどの光ディスクドライブ、または他の光媒体を含むことができる。コンピュータ可読記憶媒体２４２２は、Ｚｉｐ（登録商標）ドライブ、フラッシュメモリカード、ユニバーサルシリアルバス（ＵＳＢ）フラッシュドライブ、セキュアデジタル（ＳＤ）カード、ＤＶＤディスク、デジタルビデオテープなどを含み得るが、これらに限定されない。また、コンピュータ可読記憶媒体２４２２は、フラッシュメモリに基づくＳＳＤ、企業向けフラッシュドライブ、ソリッドステートＲＯＭなどの不揮発性メモリに基づいたソリッドステートドライブ（ＳＳＤ）、ソリッドステートＲＡＭ、ダイナミックＲＡＭ、スタティックＲＡＭなどの揮発性メモリに基づくＳＳＤ、ＤＲＡＭベースのＳＳＤ、磁気抵抗ＲＡＭ（ＭＲＡＭ）ＳＳＤ、およびＤＲＡＭとフラッシュメモリベースのＳＳＤとの組み合わせを使用するハイブリッドＳＳＤを含み得る。ディスクドライブおよびそれらの関連のコンピュータ可読媒体は、コンピュータ可読命令、データ構造、プログラムモジュールおよび他のデータの不揮発性記憶装置をコンピュータシステム２４００に提供することができる。

【０２０７】

特定の実施形態において、記憶サブシステム２４００は、コンピュータ可読記憶媒体２４２２にさらに接続可能なコンピュータ可読記憶媒体読取器２４２０を含むことができる。コンピュータ可読記憶媒体２４２２は、システムメモリ２４１０と共にまたは必要に応じてシステムメモリ２４１０と組み合わせて、コンピュータ可読情報を格納するための記憶媒体に加えて、リモート記憶装置、ローカル記憶装置、固定的な記憶装置および／または取外し可能な記憶装置を包括的に表すことができる。

【０２０８】

特定の実施形態において、コンピューティングシステム２４００は、１つ以上の仮想マシンの実行をサポートすることができる。コンピューティングシステム２４００は、仮想マシンの構成および管理を容易にするために、ハイパーバイザなどのプログラムを実行することができる。各仮想マシンに、メモリ、計算（例えば、プロセッサ、コア）、Ｉ／Ｏ、およびネットワークリソースを割り当てることができる。各仮想マシンは、通常、独自のオペレーティングシステムを実行する。このオペレーティングシステムは、コンピューティングシステム２４００によって実行される他の仮想マシンによって実行されるオペレーティングシステムと同様であってもよく、異なっていてもよい。したがって、コンピューティングシステム２４００は、複数のオペレーティングシステムを同時に実行することができる。各仮想マシンは、通常、他の仮想マシンに独立して動作する。

【０２０９】

通信サブシステム２４２４は、他のコンピューティングシステムおよびネットワークへのインターフェイスを形成する。通信サブシステム２４２４は、他のシステムからデータを受信し、コンピュータシステム２４００から他のシステムにデータを送信するためのイ

ンターフェイスとして機能する。通信サブシステム２４２４によって、コンピューティングシステム２４００は、例えば、インターネットを介して１つ以上のクライアント装置との間に情報を送受信するための通信チャネルを確立することができる。例えば、図１に示すアカウント管理システム１１２は、通信サブシステム２４２４を用いて、トレーニングワードに関連する入力を含むユーザログイン情報をクライアント装置から受信することができる。さらに、通信サブシステム２４２４を用いて、成功したログインに関する通知またはアカウント管理システムからユーザへのパスワード再入力要求に関する通知を送信することができる。

【０２１０】

通信サブシステム２４２４は、有線通信プロトコルおよび／または無線通信プロトコルの両方をサポートしてもよい。例えば、いくつかの実施形態において、通信サブシステム２４２４は、（例えば３Ｇ、４ＧまたはＥＤＧＥ（enhanced data rates for global evolution）などの携帯電話技術、高度データネットワーク技術を用いて）無線音声および／またはデータネットワークにアクセスするための無線周波数（ＲＦ）トランシーバ要素、ＷｉＦｉ（ＩＥＥＥ８０２．１１ファミリ標準または他のモバイル通信技術またはそれらの任意の組み合わせ）、全地球測位システム（ＧＰＳ）レシーバ要素、および／または、他の要素を含むことができる。いくつかの実施形態において、通信サブシステム２４２４は、無線インターフェイスに加えてまたは無線インターフェイスの代わりに、有線ネットワーク接続（例えば、イーサネット）を提供することができる。

【０２１１】

通信サブシステム２４２４は、様々な形式のデータを送受信することができる。例えば、いくつかの実施形態において、通信サブシステム２４２４は、構造化および／または非構造化データフィード２４２６、イベントストリーム２４２８、イベント更新２４３０などの形式の入力通信を受信することができる。例えば、通信サブシステム２４２４は、ソーシャルネットワークおよび／または他の通信サービスのユーザから、ツイッター（登録商標）フィード、フェースブック（登録商標）更新、ＲＳＳ（Rich Site Summary）フィードなどのウエブフィードを含むデータフィード２４２６をリアルタイムで受信（または送信）するおよび／または１つ以上の第３者情報源からリアルタイム更新を受信（または送信）するように構成されてもよい。

【０２１２】

特定の実施形態において、通信サブシステム２４２４は、リアルタイムイベントのイベントストリーム２４２８および／または明確な結末を持たない連続的または本質的に無境界のイベント更新２４３０を含み得る連続的なデータストリーム形式のデータを受信するように構成されてもよい。連続的なデータを生成するアプリケーションの例としては、例えば、センサデータアプリケーション、金融ティッカ、ネットワーク性能測定ツール（例えば、ネットワーク監視およびトラフィック管理アプリケーション）、クリックストリーム分析ツール、自動車交通監視などを含むことができる。

【０２１３】

また、通信サブシステム２４２４は、構造化および／または非構造化データフィード２４２６、イベントストリーム２４２８、およびイベント更新２４３０などを、コンピュータシステム２４００に結合された１つ以上のストリーミングデータソースコンピュータと通信し得る１つ以上のデータベースに出力するように構成されてもよい。

【０２１４】

コンピュータシステム１５００は、手持ち式携帯機器（例えば、iPhone（登録商標）携帯電話、Ipad（登録商標）計算タブレット、ＰＤＡ）、ウェアラブル装置（例えば、Google Glass（登録商標）ヘッドマウントディスプレイ）、パーソナルコンピュータ、ワークステーション、メインフレーム、キオスク、サーバラックまたはその他のデータ処理システムを含む様々なタイプのうちの１つであってもよい。

【０２１５】

コンピュータおよびネットワークが絶え間なく進化し続けるため、図２４に示されたコ

ンピュータシステム２４００の説明は、特定の例として意図されているにすぎない。図２４に示されたシステムよりも多くのまたは少ない数の構成要素を有する多くの他の構成も可能である。例えば、ハードウェア、ファームウェア、（アプレットを含む）ソフトウェア、または組み合わせにおいて、カスタマイズされたハードウェアも使用されてもよく、および／または、特定の要素が実装されてもよい。さらに、ネットワーク入力／出力装置などの他の計算装置への接続が利用されてもよい。本明細書で提供される開示および教示に基づいて、当業者は、様々な実施例を実現するための他の手段および／または方法を理解するであろう。

【０２１６】

本実施形態を詳細に説明してきたが、本明細書に説明された実施形態の精神および範囲内の修正は、当業者にとって容易であり明らかであろう。上記および／または添付の特許請求の範囲に列挙された様々な実施形態の局面、様々な局面の一部および様々な特徴は、全体的にまたは部分的に組み合わせることができ、または交換することができる。当業者なら理解できるように、上記の様々な実施形態の説明において、他の実施形態を参照した実施形態は、他の実施形態と適切に組み合わせることができる。さらに、当業者であれば、上記の説明は、例示に過ぎず、本発明を限定することを意図していないことを理解するであろう。

【図面】

【図１】

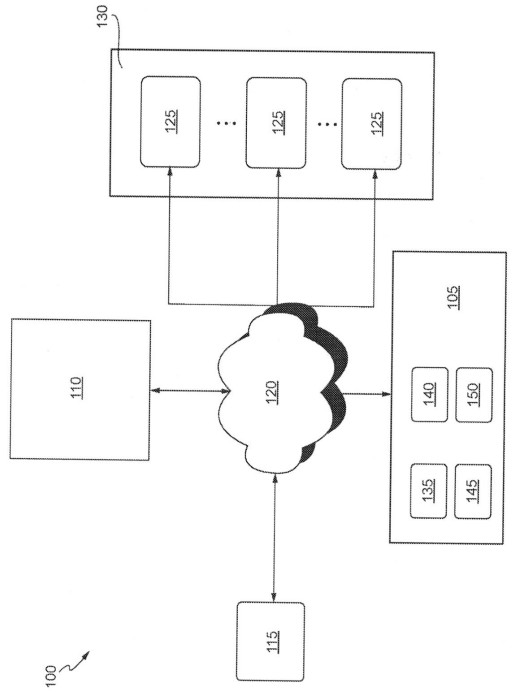

FIG. 1

【図２】

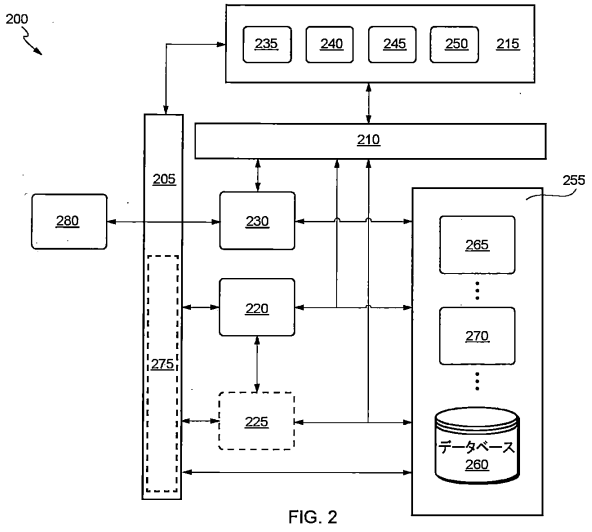

FIG. 2

【図３】

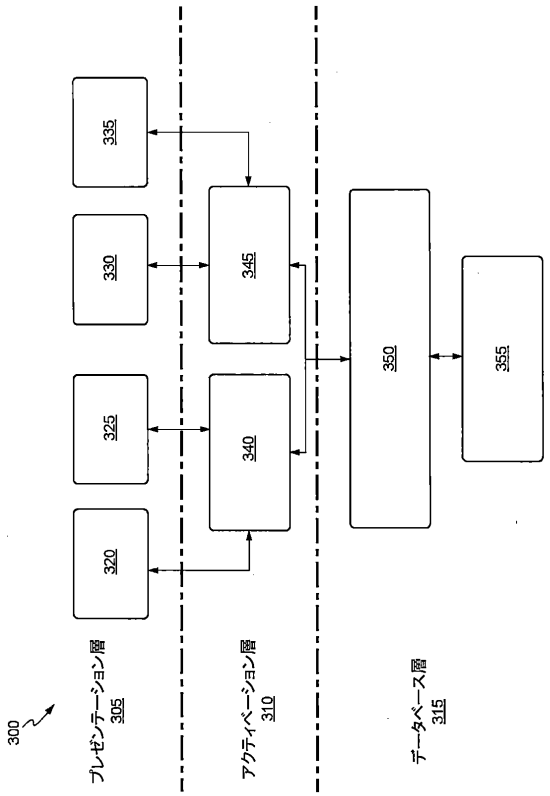

FIG. 3

【図４Ａ】

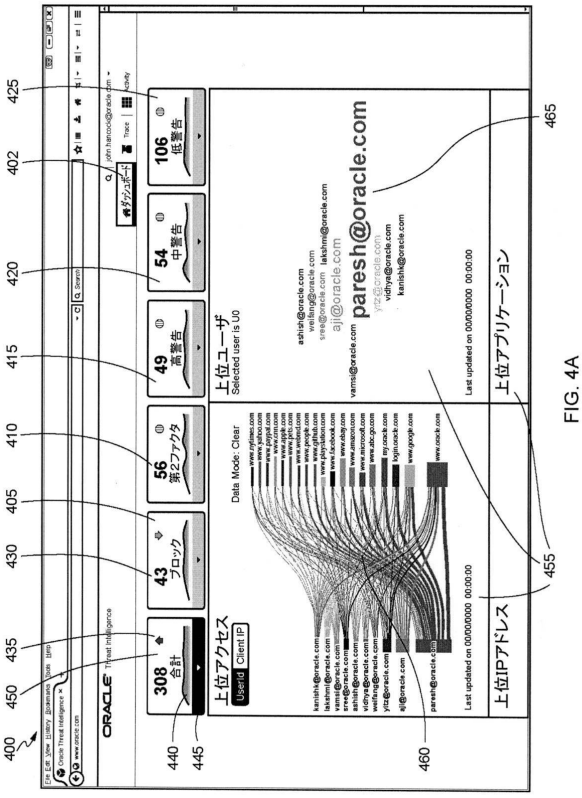

FIG. 4A

【図４Ｂ】

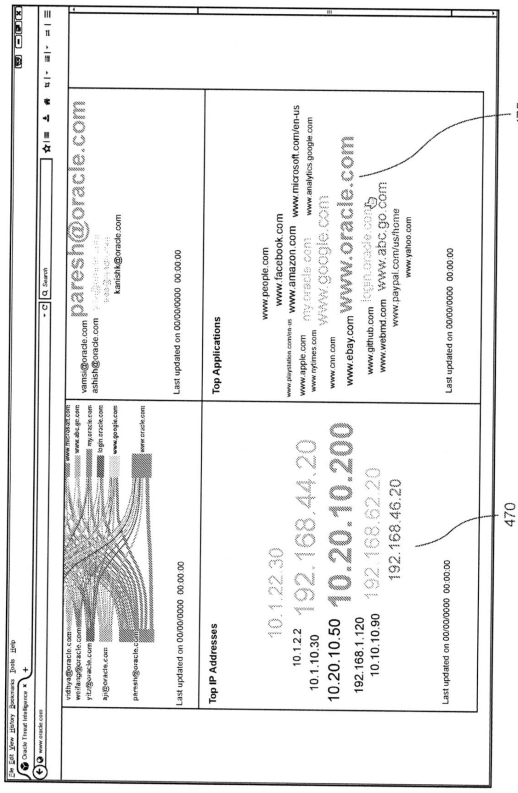

FIG. 4B

【図５】

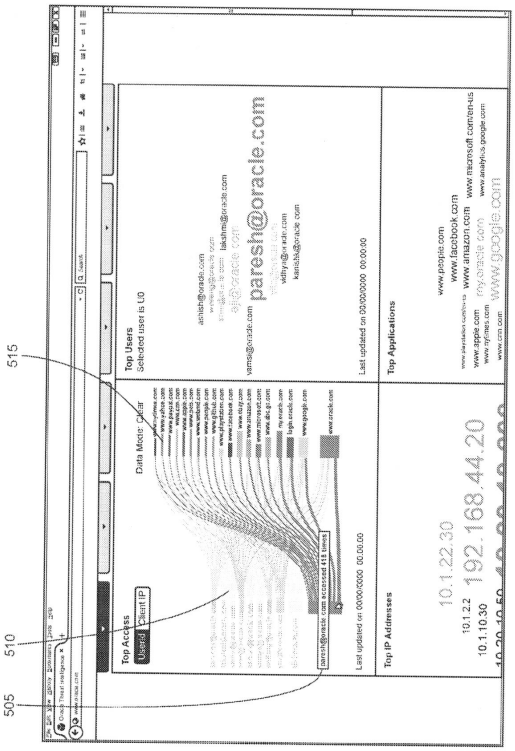

FIG. 5

【図６】

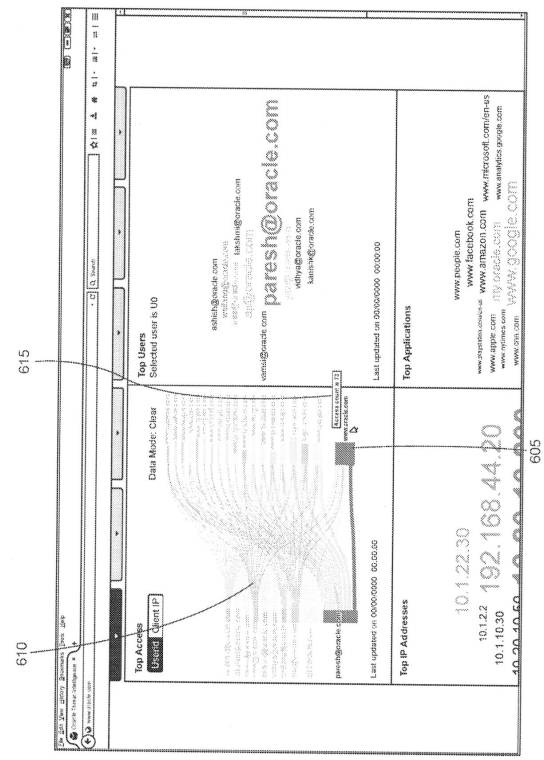

FIG. 6

【図７】

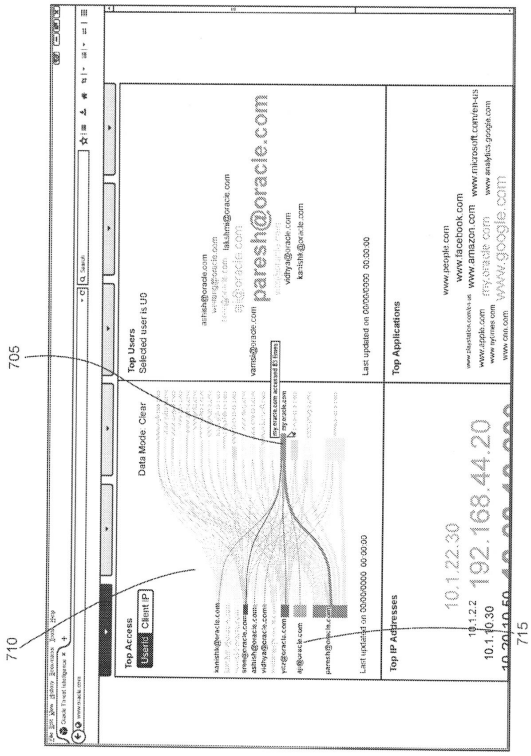

FIG. 7

【図８】

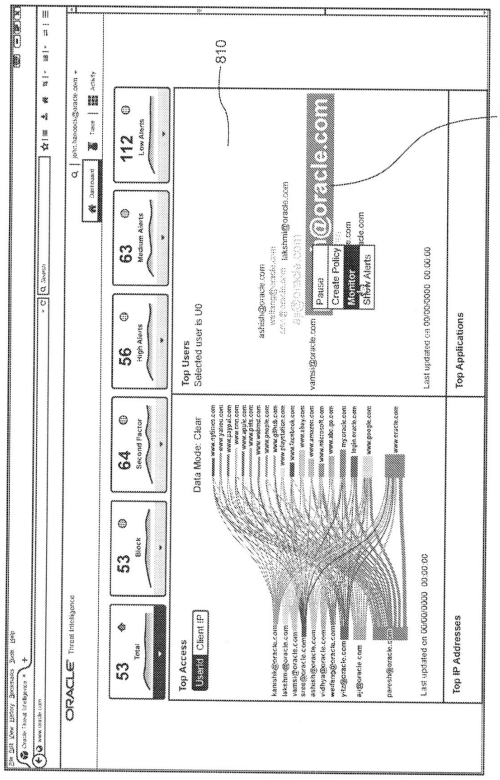

FIG. 8

【図９】

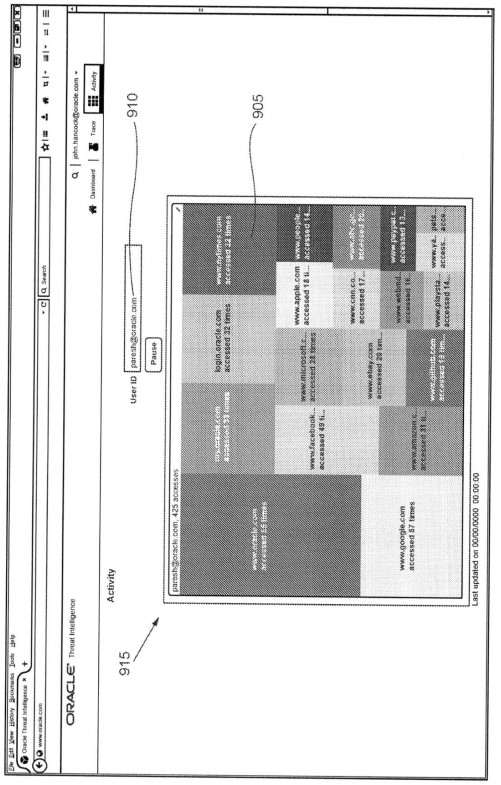

FIG. 9

【図１０】

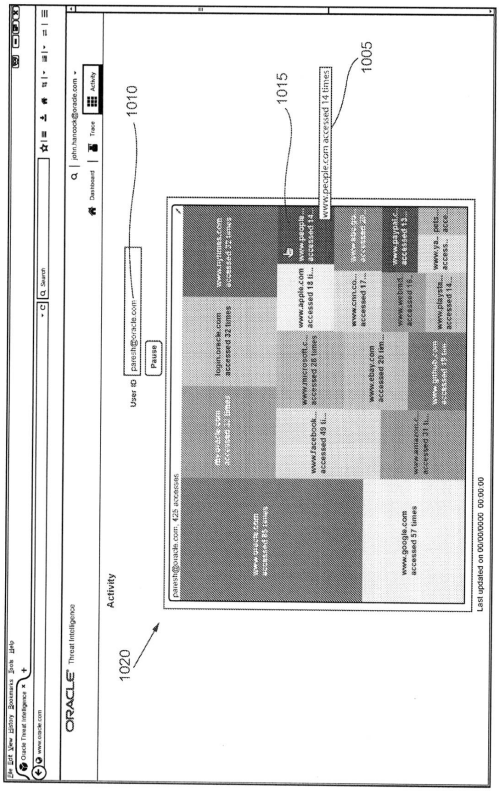

FIG. 10

【図１１】

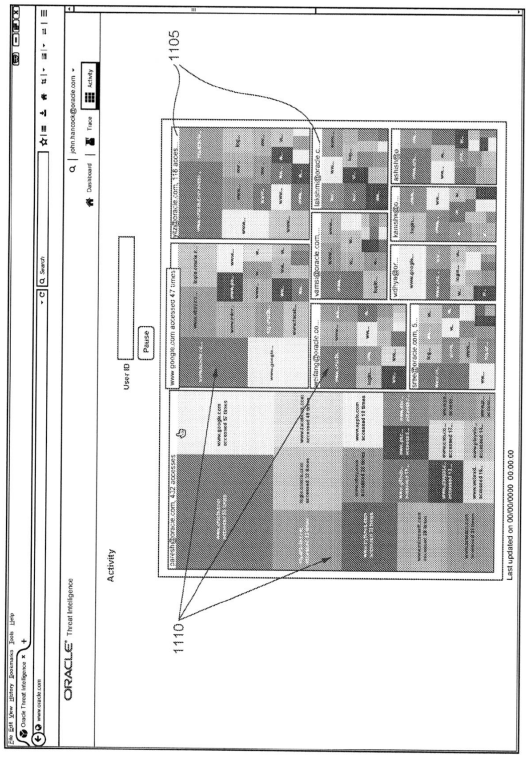

FIG. 11

【図１２Ａ】

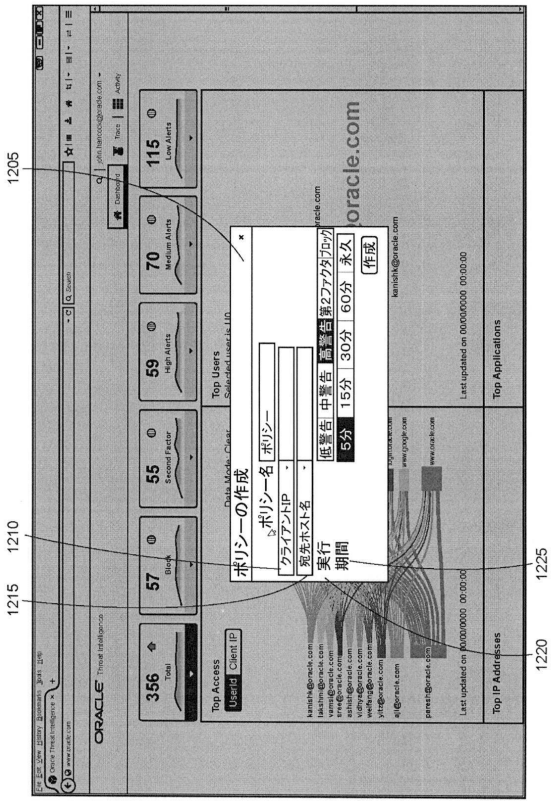

FIG. 12A

【図１２Ｂ】

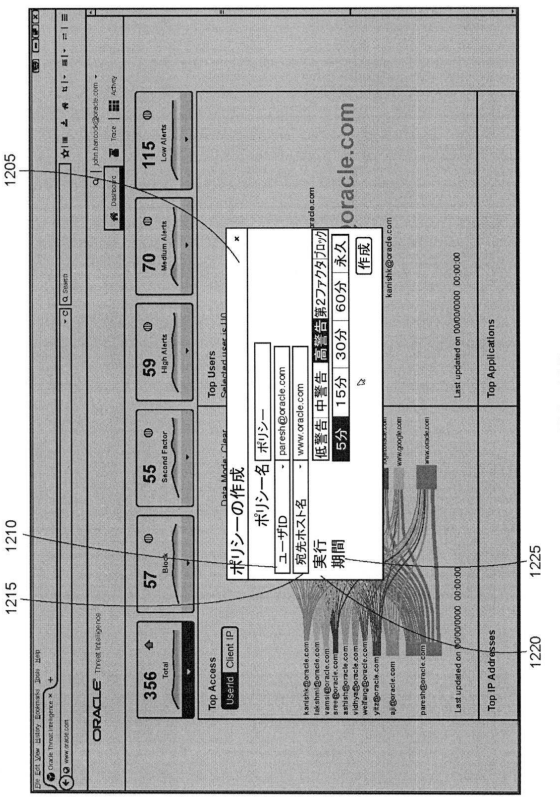

FIG. 12B

【図１３】

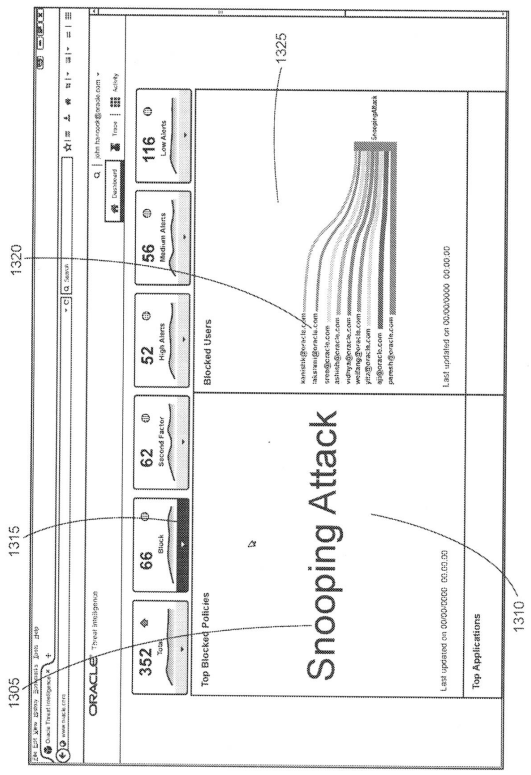

FIG. 13

【図１４】

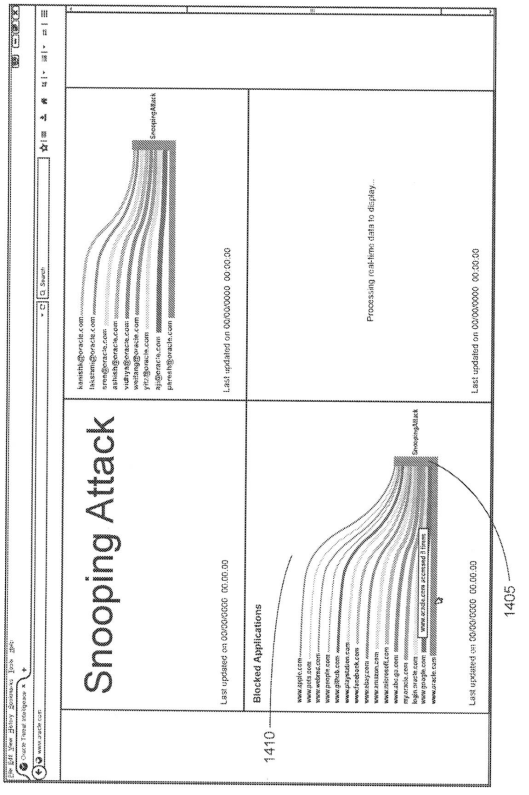

FIG. 14

【図１５】

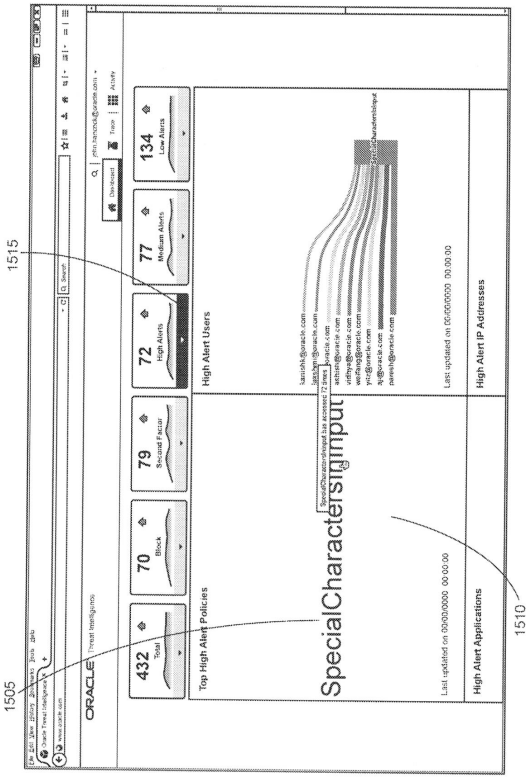

FIG. 15

【図１６】

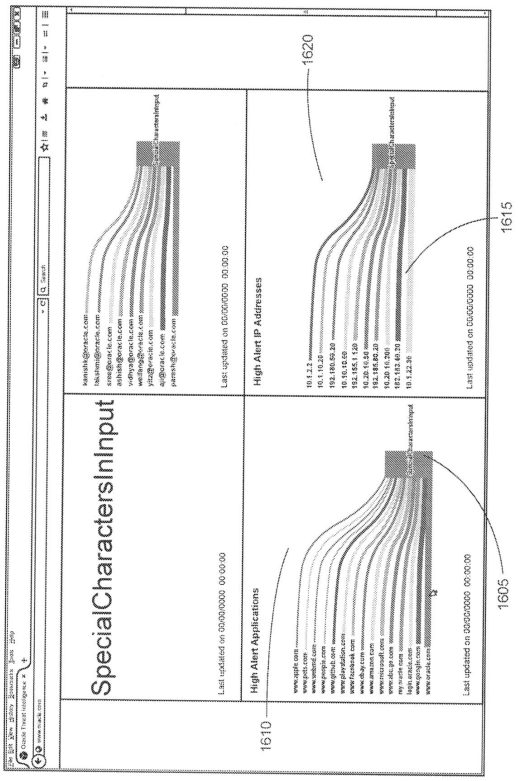

FIG. 16

【図１７】

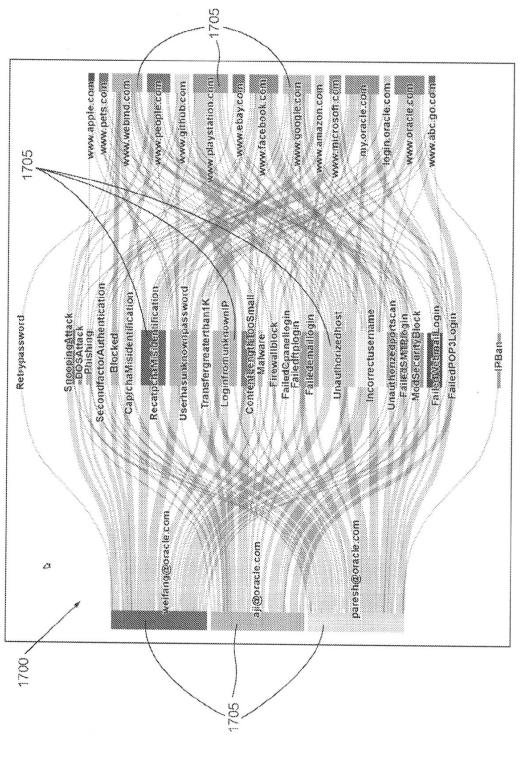

FIG. 17

【図１８】

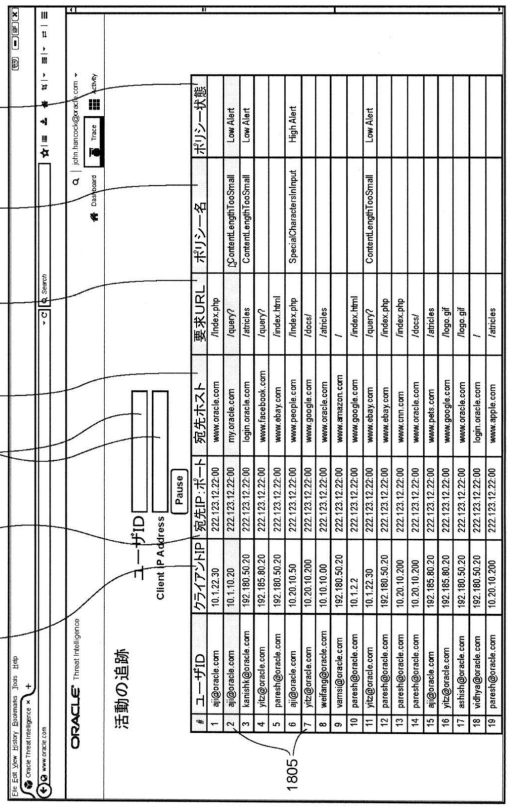

FIG. 18

【図１９】

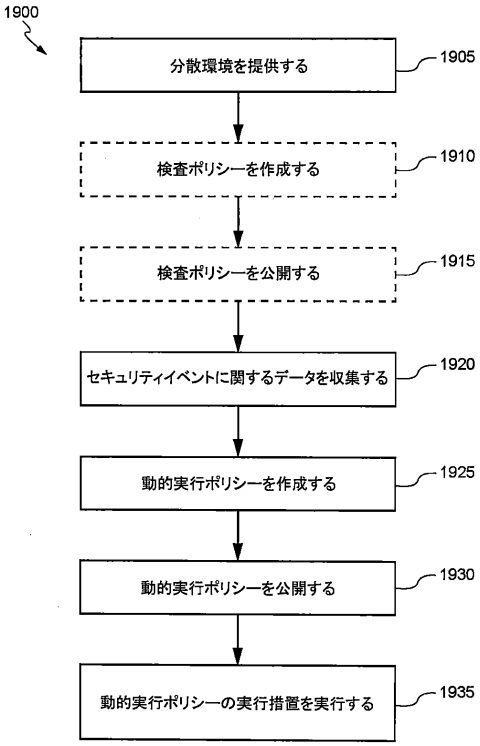

FIG. 19

【図２０】

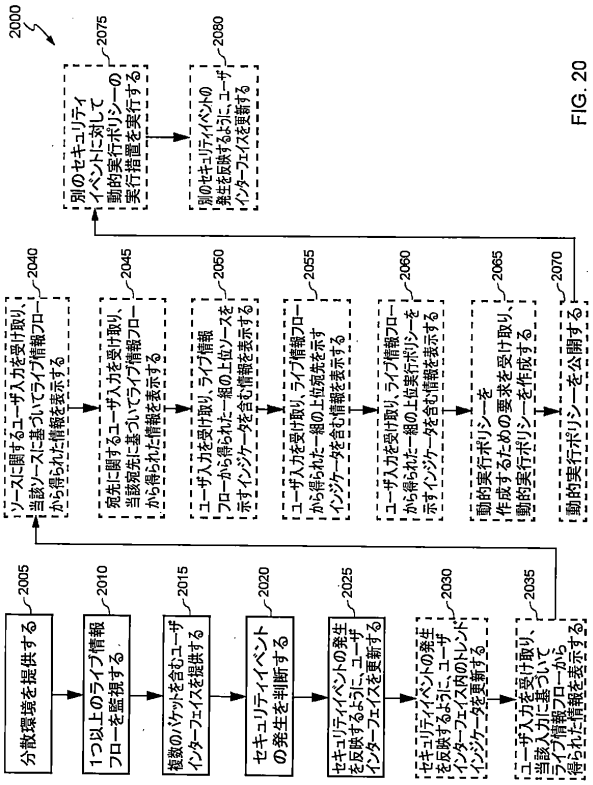

FIG. 20

【図２１】

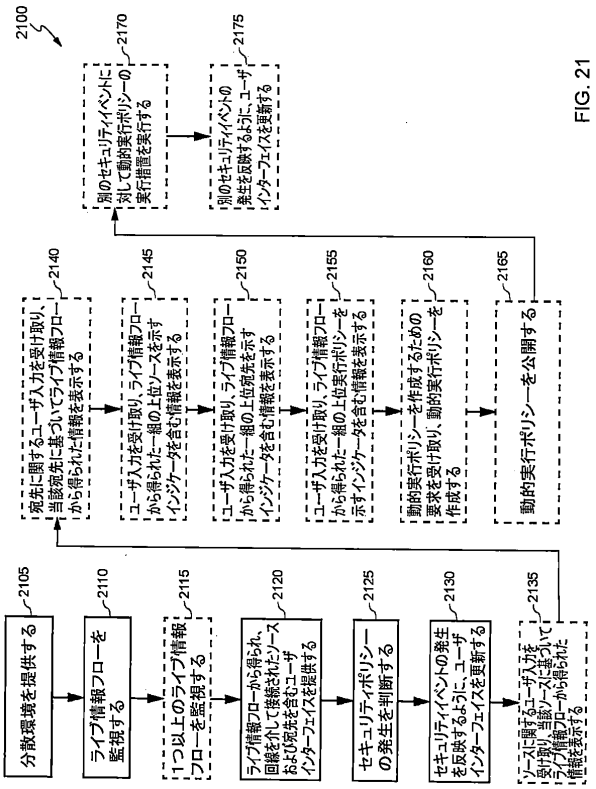

FIG. 21

【図２２】

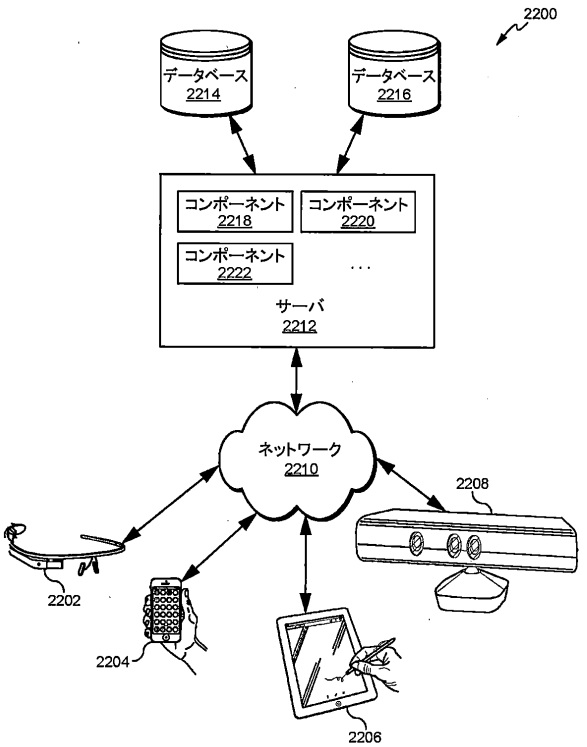

FIG. 22

【図２３】

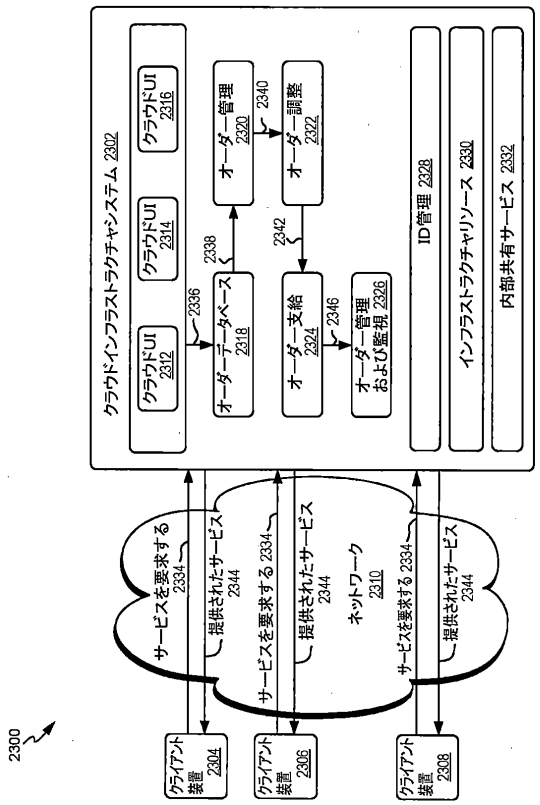

FIG. 23

【図２４】

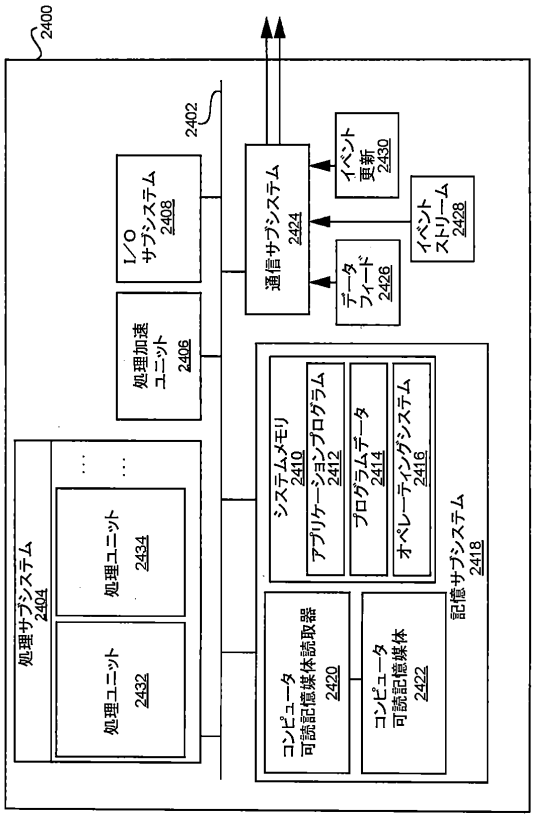

FIG. 24

フロントページの続き

(33)優先権主張国・地域又は機関
米国(US)
ーク・コート、４６３４
(72)発明者　ハリハラン，ラクシュミ
アメリカ合衆国、３００６８ ジョージア州、マリエッタ、プリンストン・ウォーク・ノース・イースト、１１２６
(72)発明者　マハジャン，カニシュク
アメリカ合衆国、９４５６８ カリフォルニア州、ダブリン、セントラル・パークウェイ、２０６２
(72)発明者　コリ，アシシュ
アメリカ合衆国、９５０１４ カリフォルニア州、クパチーノ、マドリッド・ロード、１０６５５
(72)発明者　バネルジー，モウシュミ
アメリカ合衆国、９５０１４ カリフォルニア州、クパチーノ、オログランド・プレイス、２１１７９
(72)発明者　ウィーザー，イサク
アメリカ合衆国、４４１１８ オハイオ州、ユニバーシティ・ハイツ、ブロムリー・ロード、２４２３
(72)発明者　シエ，ウェイファン
アメリカ合衆国、９５１２９ カリフォルニア州、サン・ノゼ、ジョンソン・アベニュ、１５９１
(72)発明者　キュイ，ジンユ
アメリカ合衆国、９５０５１ カリフォルニア州、サンタ・クララ、ビア・ローマ・プレイス、２９４１、ユニット・２９
審査官　打出 義尚
(56)参考文献　特開２０１５－２１６５４９（ＪＰ，Ａ）
中国特許出願公開第１０４０６５６２２（ＣＮ，Ａ）
米国特許出願公開第２００５／０１０８５６８（ＵＳ，Ａ１）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５５