(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2023-514989
(P2023-514989A)
(43)公表日　令和5年4月12日(2023.4.12)

(51)国際特許分類	FI	テーマコード（参考）
G06F 16/33 (2019.01)	G06F 16/33	5B175

審査請求　未請求　予備審査請求　未請求　（全30頁）

(21)出願番号　特願2022-548191(P2022-548191)
(86)(22)出願日　令和2年12月30日(2020.12.30)
(85)翻訳文提出日　令和4年8月24日(2022.8.24)
(86)国際出願番号　PCT/IB2020/062537
(87)国際公開番号　WO2021/161092
(87)国際公開日　令和3年8月19日(2021.8.19)
(31)優先権主張番号　16/789,884
(32)優先日　令和2年2月13日(2020.2.13)
(33)優先権主張国・地域又は機関
米国(US)
(81)指定国・地域　AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,
最終頁に続く

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ ＢＵＳＩＮＥＳＳ ＭＡＣＨＩＮＥＳ ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４ ニューヨーク州 アーモンク ニュー オーチャード ロード
Ｎｅｗ Ｏｒｃｈａｒｄ Ｒｏａｄ， Ａｒｍｏｎｋ， Ｎｅｗ Ｙｏｒｋ １０５０４， Ｕｎｉｔｅｄ Ｓｔａｔｅｓ ｏｆ Ａｍｅｒｉｃａ
(74)復代理人　110000420
弁理士法人ＭＩＰ
最終頁に続く

(54)【発明の名称】　構造化ログイベントを用いたワークフローの支援および自動化

(57)【要約】
例示のシステムは、ユーザインタフェースを監視して、ステップフローを含む活動ログを生成することを行うためのプロセッサを含む。プロセッサは、活動ログ内の非構造化データから特徴および共通変数を抽出し、抽出された前記特徴および前記共通変数に基づいて、構造化ログイベントを生成するためのものである。プロセッサは、構造化ログイベントに基づいてワークフロー・モデルを生成するためのものである。プロセッサは、生成されたワークフロー・モデルに基づいてワークフローを自動化または支援するためのものである。

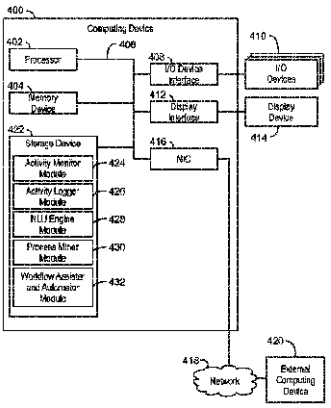


FIG. 4

【特許請求の範囲】
【請求項１】
プロセッサを含むシステムであって、前記プロセッサは、
ユーザインタフェースを監視して、ステップフローを含む活動ログを生成することと、
前記活動ログ内の非構造化データから特徴および共通変数を抽出し、抽出された前記特徴および前記共通変数に基づいて、構造化ログイベントを生成することと、
前記構造化ログイベントに基づいてワークフロー・モデルを生成することと、
生成された前記ワークフロー・モデルに基づいてワークフローを自動化または支援すること
を行うためのものである、システム。
【請求項２】
前記構造化ログイベントは、自然言語理解ユニットを介して生成され、前記プロセッサは、前記構造化ログイベントを、開始イベント、ステップフローおよび終了イベントに変換するためのものである、請求項１に記載のシステム。
【請求項３】
前記プロセッサが、
監視されるプロセスの中の共通の開始イベントを検出することと、
前記共通の開始イベントに基づいて前記プロセスを統合して最適化することと、
前記プロセスの中の共通のサブプロセスを検出することと、
統合された前記プロセスの中の各プロセスの遷移規則を検出することと、
分類を実行してコンテキストを検出することと、
前記開始イベント、前記遷移規則、前記共通のサブプロセスおよび前記コンテキストに基づいて、最適化されたフローモデルを生成することと
を行うためのものである、請求項１に記載のシステム。
【請求項４】
前記プロセッサは、ユーザフィードバックに基づいて最適化された前記フローモデルを調整するためのものである、請求項３に記載のシステム。
【請求項５】
前記プロセッサは、横断する顧客をクラスタ化し、クラスタにおける各顧客に提示すべき改良されたワークフローを生成するためのものである、請求項１に記載のシステム。
【請求項６】
前記プロセッサは、ユーザの手動プロセスのための次のステップを示唆する予測分析を対話的に実行するためのものである、請求項１に記載のシステム。
【請求項７】
前記自動化または支援されたワークフローは、セキュリティ上のベストプラクティスなワークフロー、フォレンジック・プロセス・ワークフロー、システム・チューニング・ワークフローまたはリスク緩和プロセス・ワークフローを含む、請求項１に記載のシステム。
【請求項８】
コンピュータ実装方法であって、
プロセッサを介して、ユーザインタフェースを監視して、ステップフローを含む活動ログを生成するステップと、
前記プロセッサを介して、前記活動ログ内の非構造化データから特徴および共通変数を抽出し、抽出された前記特徴および前記共通変数に基づいて、構造化ログイベントを生成するステップと、
前記プロセッサを介して、前記構造化ログイベントに基づいてワークフロー・モデルを生成するステップと、
前記プロセッサを介して、生成された前記ワークフロー・モデルに基づいてワークフローを自動化または支援するステップと
を含む、コンピュータ実装方法。

【請求項９】
前記構造化ログイベントを、開始イベント、ステップフローおよび終了イベントに変換するステップを含む、請求項８に記載のコンピュータ実装方法。
【請求項１０】
前記ワークフロー・モデルを生成するステップは、
監視されるプロセスの中の共通の開始イベントを検出するステップと、
前記共通の開始イベントに基づいて前記プロセスを統合して最適化するステップと、
前記プロセスの中の共通のサブプロセスを検出するステップと、
統合された前記プロセスの中の各プロセスの遷移規則を検出するステップと、
分類を実行してコンテキストを検出するステップと、
前記開始イベント、前記遷移規則、前記共通のサブプロセスおよび前記コンテキストに基づいて、最適化されたフローモデルを生成するステップと
を含む、請求項８に記載のコンピュータ実装方法。
【請求項１１】
前記ワークフロー・モデルを生成するステップは、
ユーザフィードバックに基づいて最適化された前記フローモデルを調整するステップを含む、請求項８に記載のコンピュータ実装方法。
【請求項１２】
横断する顧客をクラスタ化するステップと、クラスタにおける各顧客に推奨すべき改良されたワークフローを生成するステップとを含む、請求項８に記載のコンピュータ実装方法。
【請求項１３】
ユーザの手動プロセスのための次のステップを示唆する予測分析を対話的に実行するステップをさらに含む、請求項８に記載のコンピュータ実装方法。
【請求項１４】
前記構造化ログイベントに基づいて追加のワークフロー・モデルを生成するステップと、自動的に前記追加のワークフロー・モデルを実行して、提示すべき複数の結果を生成するステップとを含む、請求項８に記載のコンピュータ実装方法。
【請求項１５】
ワークフローを自動化または支援するためのコンピュータ・プログラム製品であって、前記コンピュータ・プログラム製品は、プログラムコードが具現化されたコンピュータ可読ストレージ媒体を含み、前記コンピュータ可読ストレージ媒体は、一時的な信号自体ではなく、前記プログラムコードは、プロセッサによって実行可能であり、前記プロセッサが、
ユーザインタフェースを監視して、ステップフローを含む活動ログを生成することと、
前記活動ログ内の非構造化データから特徴および共通変数を抽出し、抽出された前記特徴および前記共通変数に基づいて、構造化ログイベントを生成することと、
前記構造化ログイベントに基づいてワークフロー・モデルを生成することと、
生成された前記ワークフロー・モデルに基づいてワークフローを自動化または支援すること
を実行するためのものである、コンピュータ・プログラム製品。
【請求項１６】
前記プログラムコードは、前記プロセッサにより前記構造化ログイベントを開始イベント、ステップフローおよび終了イベントに変換するように実行可能である、請求項１５に記載のコンピュータ・プログラム製品。
【請求項１７】
前記プロセッサによって、
監視されるプロセスの中の共通の開始イベントを検出することと、
前記共通の開始イベントに基づいて前記プロセスを統合して最適化することと、
前記プロセスの中の共通のサブプロセスを検出することと、

統合された前記プロセスの中の各プロセスの遷移規則を検出することと、
分類を実行してコンテキストを検出することと、
前記開始イベント、前記遷移規則、前記共通のサブプロセスおよび前記コンテキストに基づいて、最適化されたフローモデルを生成することと
を実行するために実行可能なプログラムコードをさらに含む、請求項１５に記載のコンピュータ・プログラム製品。
【請求項１８】
前記プロセッサによって、ユーザフィードバックに基づいて最適化された前記フローモデルを調整するために実行可能なプログラムコードをさらに含む、請求項１５に記載のコンピュータ・プログラム製品。
【請求項１９】
前記プロセッサによって、横断する顧客をクラスタ化し、クラスタにおける各顧客に推奨すべき改良されたワークフローを生成するために実行可能なプログラムコードをさらに含む、請求項１５に記載のコンピュータ・プログラム製品。
【請求項２０】
前記プロセッサによって、ユーザ手動プロセスのための次のステップを示唆する予測分析を対話的に実行するために実行可能なプログラムコードをさらに含む、請求項１５に記載のコンピュータ・プログラム製品。
【発明の詳細な説明】
【技術分野】
【０００１】
本技術は、ワークフローに関する。より具体的には、本技術は、ワークフローの自動化に関する。
【発明の概要】
【０００２】
本明細書で説明される実施形態によれば、システムは、ユーザインタフェースを監視して、ステップフローを含む活動ログを生成することを行うためのプロセッサを含み得る。プロセッサは、また、活動ログ内の非構造化データから特徴および共通変数を抽出し、抽出された特徴および共通変数に基づいて、構造化ログイベントを生成してもよい。プロセッサは、また、構造化ログイベントに基づいてワークフロー・モデルを生成してもよい。プロセッサは、また、生成されたワークフロー・モデルに基づいてワークフローを自動化または支援してもよい。
【０００３】
本明細書で説明される別の実施形態によれば、方法は、プロセッサを介して、ユーザインタフェースを監視して、ステップフローを含む活動ログを生成するステップを含む。方法は、さらに、プロセッサを介して、活動ログ内の非構造化データから特徴および共通変数を抽出し、抽出された特徴および共通変数に基づいて、構造化ログイベントを生成するステップを含む。方法は、また、プロセッサを介して、構造化ログイベントに基づいてワークフロー・モデルを生成するステップを含む。方法は、また、プロセッサを介して、生成されたワークフロー・モデルに基づいてワークフローを自動化または支援するステップを含む。
【０００４】
本明細書で説明される別の実施形態によれば、ワークフローを自動化または支援するためのコンピュータ・プログラム製品は、プログラムコードが具現化されたコンピュータ可読ストレージ媒体を含む。コンピュータ可読ストレージ媒体は、一時的な信号自体ではない。プログラムコードは、プロセッサによって実行可能であり、プロセッサが、ユーザインタフェースを監視して、ステップフローを含む活動ログを生成することを実行するようにする。プログラムコードは、また、プロセッサが、活動ログ内の非構造化データから特徴および共通変数を抽出し、抽出された特徴および共通変数に基づいて、構造化ログイベントを生成するようにする。プログラムコードは、また、プロセッサが、構造化ログイベ

ントに基づいてワークフロー・モデルを生成するようにする。プログラムコードは、また、プロセッサが、生成されたワークフロー・モデルに基づいてワークフローを自動化または支援するようにする。

【図面の簡単な説明】

【０００５】

【図１】構造化ログイベントを使用してワークフローを自動化し、また、支援するための例示的なシステムのブロック図。

【図２】構造化ログイベントを用いてワークフローを自動化し、また、支援することができる例示的な方法のブロック図。

【図３】ワークフローを自動化または支援するためのワークフロー・モデルを生成することができる例示的な方法のブロック図。

【図４】構造化ログイベントを用いてワークフローを自動化し、また支援することができる例示的なコンピューティング・デバイスのブロック図。

【図５】本明細書で説明される実施形態によるクラウド・コンピューティング環境の例を示す図。

【図６】本明細書に記載の実施形態による例示的な抽象化モデル・レイヤの図。

【図７】構造化ログイベントを使用してワークフローを自動化し、また支援することができる、例示的な有形的、非一時的なコンピュータ可読媒体を示す。

【発明を実施するための形態】

【０００６】

セキュリティ動作は、非常に高コストであり、限定されている。セキュリティ調査において不審な全てのイベントを検討し、調査することは困難であり、一方で、これらのイベントの各々は、標的化された組織での深刻な含意を伴うセキュリティ・インシデントを示すかもしれない。加えて、全ての不審なイベントに対してブレイン・ストーミングおよびプロセス計画を行うことは、コストが法外となる可能性がある。さらに、所与の時間に実行する何千ものこのようなプロセスが存在する可能性もある。

【０００７】

いくつかの自動化されたイベント調査ソリューションが事前に構築される。例えば、セキュリティ専門家は、自動化されたイベント調査のために、「直ぐに使える（out-of-the box）」レシピを設計することができる。しかしながら、これらのアプローチは、非常に限定されており、今日の困難なサイバーセキュリティのランドスケープを満たさない可能性がある。例えば、攻撃者の迅速かつ動的な独創力が、検出を阻止する可能性がある。加えて、技術が頻繁に更新されると、このような設計が急速に無効になる可能性がある。さらに、ベンダからのドメイン専門知識の欠如により、そのような設計が最初から効果がない可能性がある。最後に、法人固有のケースが、他の状況でうまく機能しない可能性がある。例えば、攻撃者は、顧客に特有の脆弱性を利用する可能性がある。特定の顧客が特定のアーキテクチャ、構成またはコードを有し、ベンダがリリースしているプロセスがこれらのケースをカバーしない場合もある。加えて、シグネチャを有しない攻撃に対しては、このような攻撃を修正するための効率的な根かニズムを自動的に構築するための簡単な方法がない可能性がある。

【０００８】

本開示の実施形態によれば、システムは、ワークフローを自動的に支援し、またはワークフローを自動化するために、構造化ログイベントを使用することができる。例示的なシステムは、ユーザインタフェースを監視して、ステップフローを含む活動ログを生成するプロセッサを含む。プロセッサは、活動ログ内の非構造化データから特徴および共通変数を抽出し、抽出された特徴および共通変数に基づいて、構造化ログイベントを生成するためのものである。プロセッサは、構造化ログイベントに基づいてワークフロー・モデルを生成するためのものである。プロセッサは、生成されたワークフロー・モデルに基づいて、ワークフローを自動化または支援するためのものである。ひいては、本開示の実施形態は、監視されたユーザの活動から生成されたモデルワークフローに基づいてワークフロー

のサポートを自動化または支援することを可能とする。

【０００９】

ここで、図１を参照すると、ブロック図は、構造化ログイベントを使用してワークフローを自動化し、また支援するための例示的なシステムを示す。例示的なシステムは、概して、参照番号１００によって参照され、図２および図３の方法２００および３００を使用して、図４および図５のコンピューティング・デバイス４００またはコンピュータ可読媒体５００を使用して実装することができる。

【００１０】

図１の例では、システム１００は、複数のユーザ・アプリケーション・プログラミング・インタフェース（ＡＰＩ）１０２を含む。システム１００は、また、ユーザＡＰＩ１０２に通信可能に結合される、緩和プラットフォーム１０４と、インシデント調査プラットフォーム１０６と、セキュリティ警報システム１０８とを含む。システム１００は、さらに、ユーザＡＰＩ１０２に通信可能に結合される活動モニタ１１０を含む。システム１００は、また、活動モニタ１１０に通信可能に結合されるイベントログ・ストレージ１１２をさらに含む。システム１００は、イベントログ・ストレージ１１２に通信可能に結合される自然言語理解（ＮＬＵ）エンジン１１４も含む。システム１００は、ＮＬＵエンジン１１４に通信可能に結合されるプロセス・マイニング・エンジン１１６をさらに含む。システム１００は、また、プロセス・マイニング・エンジン１１６、ユーザＡＰＩ１０２およびインシデント調査プラットフォーム１０６に通信可能に結合されるサーバ１１８を含む。

【００１１】

さらに、図１を参照すると、システム１００は、ドメイン専門家の知識および熟練を活用することによって、セキュリティ・ベストプラクティス・ビルダー、フォレンジック・プロセス、システム・チューニングおよびリスク緩和プロセスを自動化するために使用することができる。特に、システム１００は、ＮＬＵおよびプロセス・マイニングの組み合わせを使用して、これらのプロセスを実行する際にドメイン専門家によって使用されるワークフローを構築する。システム１００は、次いで、これらのプロセスを適用する際にユーザを支援するために、構築ワークフローを利用することができる。例えば、システム１００は、到来する不審なイベントに対する緩和対策を、そのような緩和対策をサポートするための情報を含めて、提案することができる。システム１００は、イベント調査、システム・チューニングおよびリスク緩和プロセスを自動化するために、構築ワークフローを利用することもできる。

【００１２】

図１の例では、システム１００は、調査手順を適用するためにドメイン専門家によって使用されるユーザＡＰＩ１０２を含む。一例として、ドメイン専門家は、システム・オン・チップ（ＳｏＣ）アナリストであってもよい。種々の例では、これらのユーザＡＰＩ１０２は、単純なＳＱＬクエリを適用するためのシンプルなユーザインタフェースから、システムに自由な言語で質問をして回答を得ることが可能なＮＬＵベースのＵＩまでに及んでもよい。例えば、ユーザＡＰＩ１０２は、あらゆる不審なイベントを調査するために必要な作業を簡略化するための高度なＮＬＵ技術を備えたチャットボットを実装することができる。いくつかの例では、ユーザとのチャットは、基本的な遷移規則を設定するために使用され得る、データを照会するためのＲｅｓｔＡＰＩに変換されてもよい。本明細書で使用されるように、遷移規則は、プロセスのステップに対する、別のステップに移動するための１または複数の条件を含む。例えば、ユーザは、不審なユーザが過去３日のうちにＮ回以上ログインに失敗したか否かをシステムに尋ねることができる。ユーザは、「はいの場合には、ステップＡをとる」こと、「いいえの場合はステップＢを取る」ことを指定してもよい。よって、この例の遷移規則は、過去３日内の失敗したログインの数に基づいており、次のステップを決定するためにシステム１００によって使用される。種々の例では、ユーザとのチャットからのデータは、種々のアクションを実行するために使用されてもよい。例えば、アクションは、次のＮ時間、不審なユーザに対してアクセスをブロック

することを含んでもよい。いくつかの例では、アクションは、不審なユーザの上司に通知を送信することを含んでもよい。種々の例では、アクションは、不審なユーザに対する監査の分解能（resolution）を増大させることを含んでもよい。いくつかの例では、アクションは、不審なユーザのアクションをバイオレーション・システムにログ記録することを含んでもよい。いくつかの例では、アクションはチケットを開くことを含んでもよい。例えば、チケットは、マニュアルでのレビューのために不審なユーザのアクションにフラグを立てるために使用されてもよい。種々の例では、アクションは、不審なユーザの検出が偽陽性であったことを検出することに応答して、ケースを閉じることを含んでもよい。

【００１３】

セキュリティ警報システム１０８は、セキュリティ・イベントの検出に応答して、セキュリティ警報を発生してもよい。例えば、セキュリティ・イベントは、データ・ファイアウォール、侵入検出システム（ＩＤＳ）、セキュリティ情報およびイベント管理（ＳＩＥＭ）またはセキュリティ・イベント検出のための他の適切な技術を介して検出されてもよい。いくつかの例では、セキュリティ警報システム１０８は、複数のセキュリティ警報システムを含んでもよい。

【００１４】

インシデント調査プラットフォーム１０６は、セキュリティ・インシデントを調査するために使用してもよい。例えば、セキュリティ・インシデントは、ＳＩＥＭ、マルウェア分析エンジン、データベース活動分析エンジンなどから受信してもよい。種々の例では、インシデント調査プラットフォーム１０６は、ユーザが内部データベースおよび外部データベースを照会することを可能にする検索エンジンを含む。

【００１５】

緩和プラットフォーム１０４は、組織のセキュリティシステムに構成チューニングおよび緩和コマンドを適用するために使用してもよい。例えば、緩和プラットフォーム１０４は、ファイアウォールのブラックリストにインターネット・プロトコル（ＩＰ）アドレスを追加するために使用されてもよい。別の例として、緩和プラットフォーム１０４は、あるサービスについてユーザのクレデンシャルを無効にしてもよい。

【００１６】

活動モニタ１１０は、１または複数のシステムとのドメイン専門家のやり取りを監視し、ドメイン専門家によって実行されるステップフローを含む活動ログを生成してもよい。種々の例では、活動モニタ１１０の監視は、クライアント・サイドであってもよく、あるいは、サーバ・サイドであってもよい。いくつかの例では、最も包括的な監視される手順のレコードを取得ために、活動モニタ１１０は、プロセス中のすべてのドメイン専門家の活動を監視してもよい。したがって、いくつかの例では、活動モニタ１１０は、外部プラットフォームに適用されるクエリを監視してもよい。例えば、活動モニタ１１０は、ウェブ・プラットフォーム上のクエリを監視してもよい。加えて、いくつかの例では、活動モニタ１１０は、受動的モニタリングまたは能動的モニタリングを行ってもよい。例えば、受動的モニタリングは、ドメイン専門家のようなユーザに対して透過的であってもよい。能動的なモニタリングでは、活動モニタ１１０は、特定のワークフローについての洞察を得るためにユーザとやり取りをしてもよい。例えば、活動モニタ１１０は、調査手順における次のステップに導く、いくつかの応答の一部を強調表示ようにユーザに依頼してもよい。種々の例では、活動モニタ１１０は、プロセス・マイニングを改善するために、遷移規則を決定し、トークンを埋めるためにユーザに助けを求めるプロアクティブなモニタリングを適用してもよい。本明細書で使用されるように、トークンは、後続のステップで使用されて、よって格納されるパラメータおよびパラメータ値のリストを参照する。例えば、パラメータ値は、プロセスの後続のステップにおける実行時パラメータ値として使用されてもよい。よって、トークンは、後続のステップのためのコンテキストとして働き得る。種々の例では、活動モニタ１１０は、ユーザが、続くクエリに導かれるか、またはインシデント結論に導かれるシステム応答におけるアーチファクトを強調表示することを可能にしてもよい。

【００１７】
種々の例において、イベントログ・ストレージ１１２は、活動モニタ１１０によって生成された活動ログを格納するために使用されるデータベースである。例えば、イベントログ・ストレージ１１２は、内部データベースであっても、または外部データベースであってもよい。
【００１８】
ＮＬＵエンジン１１４は、活動ログ内の非構造化データから特徴および共通変数を抽出するために使用されるモデルであってもよい。例えば、特徴は、ユーザ、ファイルまたは監視されるシステムの他の特徴であってもよい。ＮＬＵエンジン１１４は、非構造化データを、プロセス・マイニング・エンジン１１６によって処理可能な構造化ログイベントに変換することができる。変数は、特定のエラータイプ、時間などであってもよい。ＮＬＵエンジン１１４は、構造化ログイベントを、イベントログ・ストレージ１１２のようなデータベースに格納してもよい。
【００１９】
プロセス・マイニング・エンジン１１６は、イベントログ・ストレージ１１２からドメイン専門家のログを受信し、ドメイン専門家のログに基づいて、ワークフロー・モデルを構築してもよい。ワークフロー・モデルを構築するために、プロセス・マイニング・エンジン１１６は、プロセス・マイニング手順を実行してもよい。プロセス・マイニング手順は、例えば、図３の方法３００を使用して実装することができる。例えば、プロセス・マイニング手順において、プロセス・マイニング・エンジン１１６は、プロセスを、開始－＞ステップフロー－＞終了に変換してもよい。プロセス・マイニング・エンジン１１６は、共通の「開始ステップ」を識別してもよい。例えば、共通の開始ステップは、複数の調査が開始した共通の開始不審イベントであってもよい。種々の例において、開始ステップは、プロセス・マイニング・エンジン１１６を実行して、開始ステップに関連するこれらのプロセスを統合し、最適化するために使用されてもよい。プロセス・マイニング・エンジン１１６は、次いで、全てのプロセスの中での共通のサブプロセスを識別してもよい。プロセス・マイニング・エンジン１１６は、すべてのプロセスの遷移規則をさらに識別してもよい。例えば、プロセス・マイニング・エンジン１１６は、すべてのプロセスの遷移規則を識別するための事前定義された構文を設定してもよい。種々の例では、プロセス・マイニング・エンジン１１６は、分類を実行してステップのコンテキストを識別してもよい。ステップのコンテキストは、トークンと参照され得る。分類の目的で、プロセス・マイニング・エンジン１１６は、どの部分が変数であり、どこから変数を抽出するかを学習することができる。どの部分が変数であり、どこから変数を抽出するかを学習することは、非常に複雑である可能性があるため、いくつかの例では、プロセス・マイニング・エンジン１１６は、ユーザに選択肢を提示して、手動での選択や変数の調整を可能にしてもよい。一例として、不審なイベントが特定のデータベースのテーブルに関連する場合、第２のステップは、このデータベース・テーブルに関連する症状（symptoms）を警告することができる。次のステップは、このデータベースに対する第１の調査ステップを実行することができる。分類の目的は、自動化が、＜ｔａｂｌｅ：”ｔａｂｌｅ　ｎａｍｅ”＞を定数ではなく実行パラメータとして設定することを知るように、＜ｅｎｔｉｔｙ：ｖａｌｕｅ＞のペアを識別することである。プロセス・マイニング・エンジン１１６は、次いで、最適化されたフローを生成してもよい。例えば、プロセス・マイニング・エンジン１１６は、最適化されたフローを生成する際に、開始イベント、遷移規則および共通サブプロセスを考慮に入れてもよい。種々の例では、フローの最適化は、同一の法人のユーザ内で行ってもよいし、複数の法人を横断して行ってさえもよい。いくつかの例では、プロセス・マイニング・エンジン１１６は、ユーザが、生産ワークフロー・モデルをカスタマイズしかつ強化することを可能にすることによって、ワークフロー・モデルを調整してもよい。種々の例では、プロセス・マイニング手順の結果は、ＮＬＵに基づいて自動的に生成される、自動化された最適な統合済みのプロセスフローである。いくつかの例では、結果として得られる最適な統合済みプロセスフローは、多くの顧客間で共有されてもよい。

【００２０】
種々の例において、サーバ１１８は、構築されたワークフローを入力として受信し、構築されたワークフローを使用して、ユーザがイベント調査手順を適用することを支援するか、または、全体的または部分的のいずれかにおいて調査手順を自動化するモデルを含んでもよい。いくつかの例では、自動化されたプロセスは、組織の警報システムの１つによって検出されたインシデントによってトリガされてもよいし、または定期的にトリガされてもよい。例えば、ユーザは、脅威分析プロセスをＥｘ２として記録し、脅威分析プロセスをＮ時間毎に自動的に実行するようにスケジュールしてもよい。種々の例では、サーバ１１８は、スクリプトからエンティティを識別し、次いで、プロセスの実行時パラメータに使用するためのトークンを探すための分類アルゴリズムを含んでもよい。いくつかの例では、プロセスは、その遷移規則およびトークンを用いて自動的に定義される。例えば、サーバ１１８は、ユーザが、第１のステップから動的に生成されるトークンに含まれるべきであり、その後のすべてのステップを通じて使用されることを識別することができる。追加のパラメータ値は、後続のステップで使用するべき、後のステップにおけるトークンに追加されてもよい。

【００２１】
種々の例では、ユーザがより多くのプロセスを実行することを継続する仮定すると、プロセス・マイニング・エンジン１１６は、同一の開始イベントに対するより多くのプロセスおよび共通のサブプロセスを識別するために定期的に動作することができる。プロセス・マイニング・エンジン１１６は、特定のプロセス・マイニング・アルゴリズムを実行して、多数のワークフロー・プロセスを、最適化されたプロセスに最適化してもよい。例えば、プロセス・マイニング・エンジン１１６は、フェーズ・マイニング・アルゴリズムを実行してもよい。プロセス・マイニング・エンジン１１６は、すべての可能な遷移規則でプロセスを識別し、最適化することができる。一例として、ユーザがＣＯＭＭＡＮＤ＝ＧＲＡＮＴに関係する外れ値（Outlier）を実行し、しばらくしてから、同一ユーザまたは別のユーザが、ＣＯＭＭＡＮＤ＝ＳＥＬＥＣＴに対して上記の脅威分析プロセスＥｘ２と同様のプロセスを実行する第１のプロセスの場合、次いで、２つのプロセスは、遷移規則を用いて、１つの最適化されたプロセスに統合され得る。

【００２２】
このようにして、サーバ１１８は、最も適合した最適化されたプロセスを適用するだけでなく、所与のインシデントのために使用されなかった他のプロセスを適用してもよい。種々の例において、サーバ１１８は、サーバとセキュリティ専門家との間の反復を容易にするユーザインタフェースを含む。例えば、ユーザインタフェースは、セキュリティ分析者に対する提案を提示してもよいし、または、自動化プロセスにセキュリティ分析者のフィードバックを提供するなどしてもよい。種々の例では、サーバ１１８は、横断する顧客をクラスタ化し、すべての顧客にかれらのプロセスの改善を推奨することができる。例えば、顧客は、最近傍アルゴリズムを実行することによってクラスタ化されてもよい。いくつかの例では、サーバ１１８は、ユーザのマニュアルでの処理に対する次のステップを示唆する予測分析を対話的に実行してもよい。

【００２３】
１つのプロセス例Ｅｘ１として、新たなコマンド外れ値”ＧＲＡＮＴ”が検出されてもよい。セキュリティ分析者は、要求：カテゴリ”Ｎｅｗ　Ｃｏｍｍａｎｄ”の最上位の外れ値を有するユーザを発見する（ｆｉｎｄ　ｔｈｅ　ｕｓｅｒ　ｗｉｔｈ　ｔｏｐ　ｏｕｔｌｉｅｒ　ｏｆ　Ｃａｔｅｇｏｒｙ　”Ｎｅｗ　Ｃｏｍｍａｎｄ”）、を送信してもよい。システムは、このユーザを表示することによって応答し、この外れ値コマンドに関する詳細を提供することができる。結果は、ＮＬＵエンジン１１４によって処理されて、特徴をトークンに抽出する。例えば、これらの特徴は、後続のステップの分析に使用され、ステップに共通の特徴を発見するために用いられる。ＮＬＵエンジン１１４は、ｃａｔｅｇｏｒｙ＝”Ｎｅｗ　Ｃｏｍｍａｎｄ”およびｕｓｅｒ＝＜ｕｓｅｒ　ｆｏｕｎｄ（見つかったユーザ）＞を識別してもよい。これら２つの動的パラメータは、後で使用するためにトーク

ンにコピーされてもよい。セキュリティ分析者は、次いで、このユーザに対する外れ値がタイプＧＲＡＮＴのＮｅｗ Ｃｏｍｍａｎｄである場合、ＧＲＡＮＴＥＥがＤＯＲＭＡＮＴ ＵＳＥＲ（休眠ユーザ）であるかどうかをチェックすることを要求してもよい。システムは、”Ｔｒｕｅ、ｔｈｉｓ ｕｓｅｒ ｉｓ ｄｏｒｍａｎｔ ｕｓｅｒ（真、このユーザは休眠ユーザである。）”を応答することができ、とりわけ、削除されたＧＲＡＮＴコマンドについての情報を提供することができる。ＮＬＵエンジン１１４は、次いで、特徴マッピングを実行し、関連するＡＰＩを実行し、トークンを実行時パラメータにマッピングし、ｃｏｍｍａｎｄ＝ＧＲＡＮＴ ＆ ｇｒａｎｔｅｅ＝＜ｕｓｅｒ ｗｈｏ ｒｅｃｅｉｖｅｄ ｔｈｅ Ｐｒｉｖｉｌｅｇｅ（特権を受領したユーザ）＞をトークンに追加することができる。セキュリティ分析者は、次に、ＧＲＡＮＴＥＥを取得し、ＧＲＡＮＴＥＥの活動を検索すること（Ｇｅｔ ｔｈｅ ＧＲＡＮＴＥＥ ａｎｄ ｓｅａｒｃｈ ｔｈｅ Ａｃｔｉｖｉｔｉｅｓ ｏｆ ｔｈｅ ＧＲＡＮＴＥＥ）を要求することができる。システムは、”ＧＲＡＮＴＥＥ ｉｓ Ｊｏｈｎ Ｓｍｉｔｈ（ＧＲＡＮＴＥＥはジョン・スミスである。）”を応答し、ユーザＪｏｈｎ Ｓｍｉｔｈのリストされた活動を提供することができる。このとき、ＮＬＵエンジン１１４は、それに応じて、トークンに、＜ｕｓｅｒ＝Ｊｏｈｎ Ｓｍｉｔｈ＞＆ａｃｔｉｖｉｔｉｅｓ＝＜ｌｉｓｔ ｏｆ ａｃｔｉｖｉｔｉｅｓ ｆｏｕｎｄ（発見された活動のリスト）＞を加えることができる。セキュリティ分析者は、さらに、機微なオブジェクトがあるかどうかをチェックする（Ｃｈｅｃｋ ｉｆ ｔｈｅｒｅ ｉｓ Ｓｅｎｓｉｔｉｖｅ Ｏｂｊｅｃｔ）ことを要求することができる（（フィルタ＜ＧＲＡＮＴＥＥ＞および＜ｓｅｎｓｉｔｉｖｅＯｂｊｅｃｔ＞でフリーテキスト形式の検索を実行するＲｅｓｔＡＰＩ））。システムは、”８ ｒｅｃｏｒｄｓ ｆｏｕｎｄ…（８レコードがみつかりました。）”と応答し、発見された結果を提供することができる。ＮＬＵエンジン１１４は、したがって、ｓｅｎｓｉｔｉｖｅＯｂｊｅｃｔ＝＜ｌｉｓｔ ｏｆ ｏｂｊｅｃｔｓ ｆｏｕｎｄ（発見されたオブジェクトのリスト）＞をトークンに追加することができる。セキュリティ分析者は、次に、”Ｃｈｅｃｋ ｉｆ ｔｈｅｒｅ ａｒｅ ｍｏｒｅ ｔｈａｎ １ ｏｃｃｕｒｒｅｎｃｅｓ ｏｆ ｔｈｉｓ ａｃｔｉｖｉｔｉｅｓ（１より多いこの活動の発生があるかどうかを確認する）（フィルタＣｏｕｎｔ＞１でフリーテキスト形式の検索を実行するＲｅｓｔＡＰＩ）”。システムは、”Ｆａｌｓｅ”で応答することができる。セキュリティ分析者は、次に、ＲＥＣＯＲＤ ＡＦＦＥＣＴＥＤの数が１より大きいかどうかをチェックする（フィルタ ＲｅｃｏｒｄＡｆｆｅｃｔｅｄ＞１およびＣｏｕｎｔ＞１でフリーテキスト形式の検索を実行するＲｅｓｔＡＰＩ）ことを要求してもよい。システムは、”Ｔｒｕｅ，ｎｕｍｂｅｒ ｏｆ ＲＥＣＯＲＤ ＡＦＦＥＣＴＥＤ ｉｓ ６（真、ＲＥＣＯＲＤ ＡＦＦＥＣＴＥＤの数は６である。）”と応答することができ、検索結果を提供する。このとき、ＮＬＵエンジン１１４は、パラメータＲｅｃｏｒｄｓＡｆｆｅｃｔｅｄ＝６をトークンに追加することができる。次いで、セキュリティ分析者は、コマンド”Ａｄｄ ｔｈｉｓ ＵＳＥＲ ｔｏ ｔｈｅ ＷＡＴＣＨ ＬＩＳＴ（このユーザをＷＡＴＣＨ ＬＩＳＴに加える）（ＷａｔｃｈＬｉｓｔに＜ｕｓｅｒ＞を加えるＲｅｓｔＡＰＩ）”を送信し、”Ｏｐｅｎ ａ ＴＩＣＫＥＴ ｉｎ ＳｅｒｖｉｃｅＮｏｗ ａｎｄ ａｓｓｉｇｎ ｔｈｅ ｕｓｅｒ’ｍａｎａｇｅｒ（ＳｅｒｖｉｃｅＮｏｗ内のＴＩＣＫＥＴを開き、ユーザの上司に割り当てる）”（ＳｅｒｖｉｃｅＮｏｗにおいてＴＩＣＫＥＴを開き、そのプロセスの出力スクリプトをテキストとしてチケットに加えるＲｅｓｔＡＰＩ）。ＮＬＵエンジン１１４は、したがって、ＳｅｒｖｉｃｅＮｏｗ．ｔｉｃｋｅｔＩｄをトークンに追加することができる。

【００２４】

第２の例示的なプロセスＥｘ２においては、新たなコマンド外れ値”ＳＥＬＥＣＴ”が検出されてもよい。例えば、セキュリティ分析者は、カテゴリ”Ｎｅｗ Ｃｏｍｍａｎｄ”の最上位の外れ値を有するユーザを発見する（ｆｉｎｄ ｍｅ ｔｈｅ ｕｓｅｒ ｗｉｔｈ ｔｏｐ ｏｕｔｌｉｅｒ ｏｆ Ｃａｔｅｇｏｒｙ ”Ｎｅｗ Ｃｏｍｍａｎｄ”）、要求をしてもよい。このシステムは、このユーザを表示し、この外れ値についての詳細を

提供することによって応答することができる。セキュリティ分析者は、次に、”ｒｅｔｒｉｅｖｅ ｔｈｅ ｏｕｔｌｉｅｒｓ ｗｈｅｒｅ ｔｈｅ Ｎｅｗ Ｃｏｍｍａｎｄ ｉｓ ＳＥＬＥＣＴ（ＮｅｗＣｏｍｍａｎｄがＳＥＬＥＣＴである外れ値を検索する）”を要求することができる。このシステムは、ＮｅｗＣｏｍｍａｎｄがＳＥＬＥＣＴである外れ値のリストに応答することができる。セキュリティ分析者は、”Ｒｕｎ ｇｅｎｅｒｉｃ Ｓｅａｒｃｈ ｆｏｒ ｔｈｉｓ ＵＳＥＲ ａｎｄ ｌｏｏｋ ｆｏｒ ｗｏｒｄ ＯＵＴ＿ＦＩＬＥ，ＵＴＬ＿ＨＴＴＰ（このユーザに対する汎用検索を実行し、単語ＯＵＴ＿ＦＩＬＥ，ＵＴＬ＿ＨＴＴＰを見つける）”を要求することができる。システムは、”Ｔｒｕｅ”と応答し、検索結果を提供することができる。セキュリティ分析者は、次いで、コマンド”Ｏｐｅｎ ａ ｔｉｃｋｅｔ ｆｏｒ ｔｈｉｓ ｕｓｅｒ，（このユーザに対するチケットを開き、）”、”ｓｅｔ ｐｒｉｏｒｉｔｙ ＨＩＧＨ ＳＥＶＥＲＩＴＹ，（優先度をＨＩＧＨ ＳＥＶＥＲＩＴＹに設定し、）”および”ｔｅｘｔ ｔｈｅ ｕｓｅｒ ｎａｍｅ ｆｏｕｎｄ ａｎｄ ｅｘｐｏｒｔ ｉｎｔｏ ａ ｆｉｌｅ ｏｒ ｈｔｔｐ．（見つかったユーザ名をテキスト化し、ファイルまたはＨＴＴＰにエクスポートする。）”のコマンドを送信することができる。

【００２５】

これらの２つの例示的なプロセスの場合、プロセス・マイニング・エンジン１１６は、ＮＬＵエンジン１１４から、２つの対応するワークフロー（ＷＦ）を受信し、２つのワークフローが共通の開始点を有することを検出することができる。プロセス・マイニング・エンジン１１６は、次いで、アルゴリズムを実行して、２つのワークフローを結合するための最適なワークフローを発見することができる。いくつかの例では、プロセス・マイニング・エンジン１１６のアルゴリズムは、ステップ１から開始する、両方のワークフローに共通である新しいワークフローを生成し、次いで、２つのユースケースをカバーするためのネストされたワークフローを生成することができる。

【００２６】

図１のブロック図は、システム１００が図１に示された全てのコンポーネントを含むものであることを示すことを意図するものではない。むしろ、システム１００は、図１に示されていない、より少ないまたは追加のコンポーネント（例えば、追加のクライアント・デバイス、または追加のリソース・サーバなど）を含んでもよいことを理解すべきである。

【００２７】

図２は、構造化ログイベントを使用してワークフローを自動化し、また支援することができる例示的な方法のプロセスフロー図である。方法２００は、図３のコンピューティング・デバイス３００のような任意の適切なコンピューティング・デバイスを用いて実装することができ、図１のシステム１００を参照して説明する。例えば、以下に説明する方法は、図４のコンピューティング・デバイス４００によって実装することができる。

【００２８】

ブロック２０２において、プロセッサは、ユーザインタフェースを監視し、ステップフローを含む活動ログを生成する。例えば、プロセッサは、ユーザとサーバ上のサービスとの間の双方向の会話を監視してもよい。例えば、サービスは、仮想アシスタント、ウェブサイトまたはアプリケーションを介してアクセスされるチャットボットであってもよい。チャットボットは、音声技術またはテキスト技術を介してユーザとの会話を行うことができる。種々の例では、ユーザは、セキュリティ・ワークフロー、フォレンジック・プロセス、システム・チューニングまたはリスク緩和プロセスの一部として、要求をサービスに送信してもよい。いくつかの例では、モニタリングは、受動的モニタリングまたは能動的モニタリングであってもよい。

【００２９】

ブロック２０４においては、プロセッサは、活動ログをデータベースに格納する。例えば、データベースは、プロセッサにとって直接アクセス可能な内部データベースであってもよいし、またはネットワークを介してアクセスし得る外部データベースであってもよい

。

【００３０】

ブロック２０６において、プロセッサは、活動ログ内の非構造化データから特徴および共通変数を抽出し、抽出された特徴および共通変数に基づいて構造化ログイベントを生成する。例えば、プロセッサは、訓練済み自然言語理解モデルを用いて特徴および共通変数を抽出してもよい。種々の例では、抽出された特徴は、トークン上に格納されてもよい。種々の例では、抽出された特徴は、他のタイプの中でも、ユーザ、サーバ、サービス、時間、コマンド、テーブル、フィールド、応答時間、影響を受けたレコード、クライアント・インターネット・プロトコル・アドレス、エラータイプ、エラーコード、違反タイプ、違反の重大性を含んでもよい。

【００３１】

ブロック２０８において、プロセッサは、構造化ログイベントに基づいてワークフロー・モデルを生成する。例えば、プロセッサは、種々のタイプのワークフローに対して最適化されたワークフロー・モデルを生成してもよい。いくつかの例では、プロセッサは、ワークフローのタイプに対して複数のワークフロー・モデルを生成してもよい。例えば、ワークフロー・モデルは、特定のタスクに実際に使用されなかった可能性のあるプロセスまたはサブプロセスを含む、異なるプロセスを統合してもよい。いくつかの例では、プロセッサは、横断する顧客をクラスタ化し、クラスタ内の各顧客に推奨されるべき改善されたワークフローを生成してもよい。例えば、プロセッサは、特定の顧客に対してまたは複数の顧客を横断してマイン（ｍｉｎｅ）の複数のワークフローを処理することができ、複数の顧客を横断してデータおよび学習を共有する。

【００３２】

ブロック２１０においては、プロセッサは、生成されたワークフロー・モデルに基づいて、ワークフローを自動化または支援する。いくつかの例では、プロセッサは、特定の生成されたワークフロー・モデルを自動的に実行してもよい。例えば、プロセッサは、特定のタスクに対して最適化されたワークフロー・モデルを実行してもよい。いくつかの例では、プロセッサは、特定のタスクのために複数のワークフロー・モデルを実行し、結果をユーザに提示してもよい。例えば、プロセッサは、構造化ログイベントに基づいて追加のワークフロー・モデルを生成し、追加ワークフロー・モデルを自動的に実行して、提示されるべき複数の結果を生成してもよい。種々の例においては、プロセッサは、最適化されたワークフローに基づいて、特定のタスクを実行するユーザを支援することができる。例えば、プロセッサは、ユーザがタスクの特定のステップにあることを検出し、次に実行するステップを示唆してもよい。種々の例では、プロセッサは、ユーザのマニュアルでの処理のための次のステップを示唆するために、対話的に予測分析を実行してもよい。いくつかの例では、ワークフローの自動化は、警報システムからの検出されたインシデントによってトリガされてもよい。種々の例では、ワークフローの自動化は、定期的に実行されてもよい。例えば、自動化されたワークフローは、所定の時間間隔で自動的に実行されるようにスケジュールされてもよい。

【００３３】

図２のプロセスフロー図は、方法２００の動作が任意の特定の順序で実行されるべきとか、あるいは、方法２００の全ての動作が全ての場合に含まれることを示すことを意図するものではない。さらに、方法２００は、任意の適切な数の追加の動作を含んでもよい。

【００３４】

図３は、ワークフローを自動化または支援するためのワークフロー・モデルを生成することができる例示的な方法のプロセスフロー図である。方法３００は、図３のコンピューティング・デバイス３００のような任意の適切なコンピューティング・デバイスで実装することができ、図１のシステム１００を参照しながら説明する。例えば、方法３００は、図１のプロセス・マイニング・エンジン１１６、図４のコンピューティング・デバイス４００のプロセス・マイナ・モジュール４３０または図７のプロセス・マイナ・モジュール７１２によって実装されてもよい。

【００３５】
ブロック３０２においては、プロセッサは、構造化ログイベントを、開始イベント、ステップフローおよび終了イベントに変換する。開始イベントは、特定の監視されるプロセスを開始するイベントである。例えば、開始イベントは、調査を開始する不審なイベントである可能性がある。ステップフローは、開始イベントから終了イベントへ接続する一連のステップを含んでもよい。終了イベントは、特定の監視されたプロセスを終了させるイベントを含んでもよい。
【００３６】
ブロック３０４において、プロセッサは、監視されるプロセスの中での共通の開始イベントを検出する。例えば、プロセッサは、２以上のプロセスの開始イベントによって共有される１または複数の特徴に基づいて、共通の開始イベントを検出することができる。一例として、２つのワークフロー・プロセスが、”Ｇｅｔ ｍｅ ｔｏｐ ａｎｏｍａｌｙ ｉｎ ｌａｓｔ Ｎ ｄａｙｓ（最後のＮ日に最上位の以上を取得）”コマンドを含むステップから開始する可能性がある。
【００３７】
ブロック３０６において、プロセッサは、共通の開始イベントに基づいて、プロセスを統合し、最適化する。例えば、プロセッサは、２つのプロセスを１つの最適化されたプロセスにマージすることによってプロセスを統合することができる。一例として、プロセッサは、２つの開始ステップを統合してもよい。プロセッサは、任意の適切なプロセス・マイニング技術によってプロセスを最適化してもよい。
【００３８】
ブロック３０８においては、プロセッサは、異なるプロセスの中で共通のサブプロセスを検出する。例えば、共通のサブプロセスは、共有される開始ステップ、特徴、変数などに基づいて検出されてもよい。
【００３９】
ブロック３１０において、プロセッサは、統合されたプロセスの中の各プロセスの遷移規則を検出する。いくつかの例では、プロセッサは、遷移規則を検出するために事前定義された構文を設定してもよい。事前定義された構文は、種々の単語または句を特定の特徴または変数に関連付けるためにプロセッサによって使用される辞書または例のセットであってもよい。
【００４０】
ブロック３１２において、プロセッサは、各プロセスの各ステップについてコンテキストを検出するための分類を実行する。例えば、プロセッサは、変数であり、また、そのような変数の位置である、各プロセスにおける各ステップの部分を識別するように訓練された分類器を使用してもよい。プロセッサは、可変パラメータをトークンに抽出することができる。トークンは、各プロセスのステップを横断して、抽出されたパラメータを追跡するために使用されてもよい。
【００４１】
ブロック３１４においては、プロセッサは、開始イベント、遷移規則、共通のサブプロセスおよびコンテキストに基づいて、最適化されたフローモデルを生成する。いくつかの例では、最適化されたフローモデルは、特定の組織の各ユーザに対して生成されてもよい。種々の例においては、最適化されたフローモデルは、特定の組織に対して生成されてもよい。いくつかの例では、プロセッサは、複数の組織によって使用できる最適化されたフローモデルを生成してもよい。
【００４２】
ブロック３１６においては、プロセッサは、ユーザフィードバックに基づいて最適化されたフローモデルを調整する。例えば、プロセッサは、ユーザが、生成された最適化済みフローモデルをカスタマイズし、強化することを可能とする。
【００４３】
図３のプロセスフロー図は、方法３００の動作が任意の特定の順序で実行されること、

あるいは、方法３００の全ての動作が全ての場合に含まれることを示すことを意図するものではない。加えて、方法３００は、任意の適切な数の追加の動作を含んでもよい。例えば、ユーザが追加のプロセスを実行することを継続すると仮定すると、プロセッサは、共通の開始イベントおよび共通のサブプロセスで、追加のプロセスを定期的に識別してもよい。プロセッサは、次いで、最適化されたフローモデルを更新し、これらの共通のサブプロセスのための追加の遷移規則を含めることができる。

【００４４】

いくつかのシナリオでは、本明細書で説明される技術は、クラウド・コンピューティング環境において実装されてもよい。以下、少なくとも図４～図７を参照しながら詳細を議論するように、構造化ログイベントを用いてワークフローを自動化するよう構成されたコンピューティング・デバイスは、クラウド・コンピューティング環境において実装されてもよい。この開示は、クラウド・コンピューティングについての説明を含み得るが、本明細書で詳述される教示の実装は、クラウド・コンピューティング環境に限定されないことに理解されたい。むしろ、本発明の実施形態は、現時点で知られた、またはこれから開発される他の任意のタイプのコンピューティング環境と併せて実装可能である。

【００４５】

クラウド・コンピューティングは、最小の管理労力またはサービス・プロバイダとの対話で迅速にプロビジョニングおよびリリースされ得る、構成可能なコンピューティング・リソース（例えば、ネットワーク、ネットワーク帯域、サーバ、処理、メモリ、ストレージ、アプリケーション、仮想マシンおよびサービス）の共有プールへの便利なオンデマンドのネットワーク・アクセスを可能とする、サービス配布のモデルである。このクラウド・モデルは、少なくとも５つの特性、少なくとも３つのサービス・モデルおよび少なくとも４つのデプロイメント・モデルを含む可能性がある。

【００４６】

特性は、以下の通りである。

【００４７】

オンデマンド・セルフ・サービス：クラウド・コンシューマは、サービス・プロバイダとの人的な対話を必要とせずに自動的に必要なだけ、サーバ時間およびネットワーク・ストレージなどのコンピュータ能力を一方的にプロビジョニングすることができる。

【００４８】

広帯域ネットワーク・アクセス：能力は、ネットワーク越しに利用可能であり、異種シン・クライアントまたはシック・クライアント・プラットフォーム（例えば、モバイルフォン、ラップトップ、ＰＤＡ）による使用を促進する標準的なメカニズムを介して、アクセスされる。

【００４９】

リソース・プーリング：プロバイダのコンピューティング・リソースは、マルチ・テナント・モデルを用いて複数のコンシューマに提供するためにプールされ、種々の物理的および仮想的リソースが需要に従って動的に割り当てられ、また、再割り当てられる。コンシューマは、一般的に、提供されるリソースの正確な場所を管理したり、知識を有したりせず、しかし、より高度な抽象レベル（例えば国、州、またはデータセンタ）にて場所を指定することが可能であるという意味で、場所の独立感がある。

【００５０】

迅速な弾力性：能力は、迅速かつ柔軟に、いくつかの場合では自動的に、プロビジョニングされて素早くスケール・アウトすることができ、また、迅速にリリースされて素早くスケール・インすることができる。コンシューマにとって、プロビジョニング利用可能な能力は、しばしば外面的には無制限のように見え、任意の時間に任意の量を購入することができる。

【００５１】

測量されたサービス：クラウドシステムは、サービスのタイプにとって適切なある抽象レベル（例えば、ストレージ、処理、帯域幅、アクティブ・ユーザ数）での計量能力を利

用することによって、自動的にリソース使用を制御し、また最適化する。リソース使用量は、監視され、制御されおよび報告されて、利用サービスのプロバイダおよびコンシューマの双方に対する透明性を提供する。

【００５２】

サービス・モデルは、以下の通りである。

【００５３】

ソフトウェア・アズ・ア・サービス（ＳａａＳ）：コンシューマに提供される能力は、クラウド・インフラストラクチャ上で稼働するプロバイダのアプリケーションを使用することである。アプリケーションは、ウェブ・ブラウザ（例えばウェブベースの電子メール）などのシン・クライアント・インタフェースを介して種々のクライアント・デバイスからアクセス可能である。コンシューマは、ネットワーク、サーバ、オペレーティング・システム、ストレージ、または、限定されたユーザ固有のアプリケーション構成設定の潜在的な例外を除いて個々のアプリケーション能力すらも含む下層のインフラストラクチャを管理または制御しない。

【００５４】

プラットフォーム・アズ・ア・サービス（ＰａａＳ）：コンシューマに提供される能力は、プロバイダによってサポートされるプログラミング言語およびツールを用いて作成された、コンシューマ作成または獲得のアプリケーションをクラウド・インフラストラクチャ上にデプロイすることである。コンシューマは、ネットワーク、サーバ、オペレーティング・システムまたはストレージを含む下層のクラウド・インフラストラクチャを管理または制御しないが、デプロイされたアプリケーションおよび場合によってはアプリケーション・ホスティング環境の構成への制御を有する。

【００５５】

インフラストラクチャ・アズ・ア・サービス（ＩａａＳ）：コンシューマに提供される能力は、処理、ストレージ、ネットワーク、および、コンシューマが、オペレーティング・システムおよびアプリケーションを含み得る任意のソフトウェアをデプロイし、稼働させることができる他の基本的なコンピューティング・リソースを提供することである。コンシューマは、下層のクラウド・インフラストラクチャを管理または制御しないが、オペレーティング・システム、ストレージ、デプロイされたアプリケーションに対する制御、および、場合によっては、選択したネットワーキング・コンポーネント（例えば、ホストファイアウォール）の限定された制御を有する。

【００５６】

デプロイメント・モデルは、以下の通りである。

【００５７】

プライベート・クラウド：クラウド・インフラストラクチャは、１つの組織のためだけに使用される。これは、組織または第三者によって管理されてもよく、オンプレミスまたはオフプレミスが存在し得る。

【００５８】

コミュニティ・クラウド：クラウド・インフラストラクチャは、いくつかの組織により共有され、共通の懸念（例えば、ミッション、セキュリティ要件、ポリシーおよびコンプライアンスに関する考慮事項）を有する特定のコミュニティをサポートする。これは、組織または第三者によって管理されてもよく、オンプレミスまたはオフプレミスが存在し得る。

【００５９】

パブリック・クラウド：クラウド・インフラストラクチャは、一般公衆、または、大きな業界団体が利用可能であり、クラウド・サービスを販売する組織によって所有される。

【００６０】

ハイブリッド・クラウド：クラウド・インフラストラクチャは、２以上のクラウド（プライベート、コミュニティまたはパブリック）の混成であり、これらのクラウドは、固有のエンティティのままであるが、しかし、データおよびアプリケーションのポータビリテ

ィを可能とする標準化されたまたは独自の技術（例えばクラウド間の負荷分散のためのクラウド・バースティング）によって結合される。

【００６１】

クラウド・コンピューティング環境は、ステートレス性、低結合、モジュール性および意味論的な相互運用性に重点を置いたサービス指向である。クラウド・コンピューティングの核心は、相互接続された複数のノードのネットワークを含むインフラストラクチャである。

【００６２】

図４は、構造化されたログイベントを用いてワークフローを自動化し、支援することができる一例のコンピューティング・デバイスのブロック図である。コンピューティング・デバイス４００は、例えば、サーバ、デスクトップ・コンピュータ、ラップトップ・コンピュータ、タブレット・コンピュータまたはスマートフォンであってもよい。いくつかの例では、コンピューティング・デバイス４００は、クラウド・コンピューティング・ノードであってもよい。コンピューティング・デバイス４００は、コンピュータ・システムによって実行されるプログラム・モジュールのようなコンピュータ・システム実行可能命令の一般的な文脈において説明され得る。一般に、プログラム・モジュールは、特定のタスクを実行するかまたは特定の抽象データタイプを実装する、ルーチン、プログラム、オブジェクト、コンポーネント、ロジック、データ構造などを含む。コンピューティング・デバイス４００は、通信ネットワークを介してリンクされた遠隔処理デバイスによってタスクが実行される分散型クラウド・コンピューティング環境で実施してもよい。分散型クラウド・コンピューティング環境では、プログラム・モジュールは、メモリ・ストレージ・デバイスを含むローカルおよび遠隔のコンピュータ・システム・ストレージ媒体の両方に配置されてもよい。

【００６３】

コンピューティング・デバイス４００は、格納された命令を実行するためのプロセッサ４０２と、動作中に前記命令の動作のための一時的メモリ空間を提供するためのメモリデバイス４０４とを含んでもよい。プロセッサは、シングルコアプロセッサ、マルチコアプロセッサ、コンピューティング・クラスタ、または任意の数の他の構成とすることができる。メモリ４０４は、ランダム・アクセス・メモリ（ＲＡＭ）、リード・オンリー・メモリ、フラッシュメモリまたは他の適切なメモリシステムを含んでもよい。

【００６４】

プロセッサ４０２は、コンピューティング・デバイス４００を１以上のＩ／Ｏデバイス４１０に接続するように適合された入出力（Ｉ／Ｏ）デバイス・インタフェース４０８にシステム相互接続４０６（例えば、ＰＣＩ（登録商標）、ＰＣＩ－Ｅｘｐｒｅｓｓ（登録商標）など）を介して接続されてもよい。Ｉ／Ｏデバイス４１０は、例えば、キーボードおよびポインティング・デバイスを含むことができ、ポインティング・デバイスは、これらの中でも、タッチパッドまたはタッチスクリーンを含んでもよい。Ｉ／Ｏデバイス４１０は、コンピューティング・デバイス４００の内蔵のコンポーネントであってもよいし、コンピューティング・デバイス４００に外部接続されたデバイスであってもよい。

【００６５】

プロセッサ４０２は、また、コンピューティング・デバイス４００をディスプレイ・デバイス４１４に接続するように適合されたディスプレイ・インタフェース４１２にシステム相互接続４０６を介してリンクされてもよい。ディスプレイ・デバイス４１４は、コンピューティング・デバイス４００の内蔵コンポーネントである表示スクリーンを備える。ディスプレイ・デバイス４１４は、コンピューティング・デバイス４００に外部接続されたコンピュータ・モニタ、テレビジョンまたはプロジェクタを含んでいてもよい。加えて、ネットワーク・インタフェース・コントローラ（ＮＩＣ）４１６は、システム相互接続４０６を介してコンピューティング・デバイス４００をネットワーク４１８に接続するように適合されてもよい。いくつかの実施形態では、ＮＩＣ４１６は、中でもインターネット・スモール・コンピュータ・システム・インタフェースのような任意の適切なインタフ

ェースまたはプロトコルを使用してデータを送信することができる。ネットワーク４１８は、セルラー・ネットワーク、無線ネットワーク、ワイド・エリア・ネットワーク（ＷＡＮ）、ローカル・エリア・ネットワーク（ＬＡＮ）、またはインターネットであってもよい。外部コンピューティング・デバイス４２０は、ネットワーク４１８を介してコンピューティング・デバイス４００に接続してもよい。いくつかの例では、外部コンピューティング・デバイス４２０は、外部ウェブ・サーバ４２０であってもよい。いくつかの例では、外部コンピューティング・デバイス４２０は、クラウド・コンピューティング・ノードであってもよい。

【００６６】

プロセッサ４０２は、また、ハードドライブ、光学ドライブ、ＵＳＢフラッシュドライブ、ドライブのアレイ、またはそれらの任意の組み合わせを含んでよいストレージ・デバイス４２２にシステム相互接続４０６を介してリンクされてもよい。いくつかの例では、ストレージ・デバイスは、活動モニタ・モジュール４２４、活動ロガー・モジュール４２６、自然言語理解（ＮＬＵ）モジュール４２８、プロセス・マイナ・モジュール４３０およびワークフロー・アシスタおよびオートメータ４３２を含むことができる。活動モニタ・モジュール４２４は、ユーザインタフェースを監視して、ステップフローを含む活動ログを生成することができる。例えば、ステップフローは、ユーザによって特定のタスクを完了するためにとられたステップを含む。活動ロガー・モジュール４２６は、データベースに活動ログを格納することができる。例えば、データベースは、内部データベースまたは外部データベースであってもよい。ＮＬＵモジュール４２８は、活動ログ内の非構造化データから特徴および共通変数を抽出し、抽出された特徴および共通変数に基づいて、構造化ログイベントを生成することができる。プロセス・マイナ・モジュール４３０は、構造化ログイベントに基づいてワークフロー・モデルを生成することができる。例えば、プロセス・マイナ・モジュール４３０は、構造化ログイベントを、開始イベント、ステップフローおよび終了イベントに変換することができる。プロセス・マイナ・モジュール４３０は、次いで、監視されるプロセスの中の共通の開始イベントを検出することができる。プロセス・マイナ・モジュール４３０は、共通の開始イベントに基づいて、プロセスを統合して最適化することができる。プロセス・マイナ・モジュール４３０は、さらに、プロセスの中の共通のサブプロセスを検出することができる。プロセス・マイナ・モジュール４３０は、また、プロセスの中の各プロセスの遷移規則を検出することができる。プロセス・マイナ・モジュール４３０は、分類を実行してコンテキストを検出することができる。プロセス・マイナ・モジュール４３０は、次いで、開始イベント、遷移規則、共通のサブプロセスおよびコンテキストに基づいて、最適化されたフローモデルを生成することができる。いくつかの例において、プロセス・マイナ・モジュール４３０は、ユーザフィードバックに基づいて最適化されたフローモデルを調整することができる。いくつかの例において、プロセス・マイナ・モジュール４３０は、また、横断する顧客をクラスタ化し、クラスタにおける各顧客に提示すべき改良されたワークフローを生成することができる。種々の例において、プロセス・マイナ・モジュール４３０は、ユーザ手動プロセスのための次のステップを示唆する予測分析を対話的に実行することができる。ワークフロー・アシスタおよびオートメータ４３２は、生成されたワークフロー・モデルに基づいて、ワークフローを自動化または支援することができる。例えば、自動化または支援されたワークフローは、セキュリティ上のベストプラクティスなワークフロー、フォレンジック・プロセス・ワークフロー、システム・チューニング・ワークフローまたはリスク緩和プロセス・ワークフローであってもよい。

【００６７】

図４のブロック図は、コンピューティング・デバイス４００が、図４に示された全てのコンポーネントを含むものであることを示すことを意図するものではない。むしろ、コンピューティング・デバイス４００は、より少ない、または、図４に示されていない追加のコンポーネント（例えば、追加のメモリ・コンポーネント、組み込みコントローラ、モジュール、追加のネットワーク・インタフェースなど）を含んでもよいことを理解すべきで

ある。さらに、活動モニタ・モジュール４２４、活動ロガー・モジュール４２６、ＮＬＵモジュール４２８、プロセス・マイナ・モジュール４３０およびワークフロー・アシスタおよびオートメータ４３２のうちの任意の機能は、部分的または完全に、ハードウェアもしくはプロセッサ４０２またはその両方においてで実装されてもよい。例えば、機能は、特定用途向け集積回路、組み込みコントローラで実現されるロジック、またはプロセッサ４０２内で実現されるロジックによって実現されてもよい。いくつかの実施形態では、活動モニタ・モジュール４２４、活動ロガー・モジュール４２６、ＮＬＵモジュール４２８、プロセス・マイナ・モジュール４３０およびワークフロー・アシスタおよびオートメータ４３２の機能は、ロジックで実装することができ、ロジックは、本明細書で参照されるように、任意の適切なハードウェア（例えば、プロセッサなど）、ソフトウェア（例えば、アプリケーションなど）、ファームウェア、または、ハードウェア、ソフトウェアおよびファームウェアの任意の適切な組み合わせを含んでもよい。

【００６８】

ここで、図５を参照すると、例示的なクラウド・コンピューティング環境５００が示されている。図示するように、クラウド・コンピューティング環境５００は、１以上のクラウド・コンピューティング・ノード５０２を含み、これと、例えば、ＰＤＡまたは携帯電話５０４Ａ、デスクトップ・コンピュータ５０４Ｂ、ラップトップ・コンピュータ５０４Ｃもしくは自動車コンピュータ・システム５０４Ｎまたはその組み合わせなどの、クラウド・コンシューマによって使用されるローカル・コンピューティング・デバイスが通信してもよい。ノード５０２は、互いに通信してもよい。これらは、プライベート、コミュニティ、パブリックもしくはハイブリッド・クラウドなど上述したような、またはその組み合わせなどの１以上のネットワークにおいて、物理的にまたは仮想的にグループ化（図示しない）されてもよい。これは、クラウド・コンピューティング環境５００が、インフラストラクチャ、プラットフォームもしくはソフトウェアまたはその組み合わせをサービスとして提供することを可能とし、これらについては、クラウド・コンシューマは、リソースをローカル・コンピューティング・デバイス上で維持する必要がない。図５に示されるコンピューティング・デバイス５０４Ａ～５０４Ｎのタイプは、説明する目的のみであり、コンピューティング・ノード５０２およびクラウド・コンピューティング環境５００が、任意のタイプのネットワーク、ネットワークアドレス可能な接続（例えば、ウェブ・ブラウザを使用して）またはこれらの両方を介して、任意のタイプのコンピュータ化されたデバイスと通信することができることが理解される。

【００６９】

ここで、図６を参照すると、クラウド・コンピューティング環境５００（図５）によって提供される機能抽象レイヤのセットが示される。図６に示すコンポーネント、層および機能は、説明する目的のみであり、本発明の実施形態は、これらに限定されないことを事前に理解されるべきである。示すように、以下の層および対応する機能が提供される。

【００７０】

ハードウェアおよびソフトウェア・レイヤ６００は、ハードウェアおよびソフトウェア・コンポーネントを含む。ハードウェア・コンポーネントの例には、メインフレーム、一例ではＩＢＭ（登録商標）ｚＳｅｒｉｅｓ（登録商標）Ｓｙｓｔｅｍｓ、ＲＩＳＣ（縮約命令セットコンピュータ）アーキテクチャに基づくサーバ、一例においてはＩＢＭ（登録商標）ｐＳｅｒｉｅｓ（登録商標）Ｓｙｓｔｅｍｓ，ＩＢＭ（登録商標）ｘＳｅｒｉｅｓ（登録商標）Ｓｙｓｔｅｍｓ，ＩＢＭ（登録商標）ＢｌａｄｅＣｅｎｔｅｒ（登録商標）Ｓｙｓｔｅｍｓ、ストレージ・デバイス、ネットワークおよびネットワーキング・コンポーネントを含む。ソフトウェア・コンポーネントの例は、一例では、ＩＢＭ（登録商標）ＷｅｂＳｐｈｅｒｅ（登録商標）アプリケーション・サーバ・ソフトウェアおよびデータベース・ソフトウェア、一例では、ＩＢＭ（登録商標）ＤＢ２（登録商標）データベース・ソフトウェアを含み得る。（ＩＢＭ，ｚＳｅｒｉｅｓ，ｐＳｅｒｉｅｓ，ｘＳｅｒｉｅｓ，ＢｌａｄｅＣｅｎｔｅｒ，ＷｅｂＳｐｈｅｒｅおよびＤＢ２は、世界中の多くの管轄地域で登録されたインターナショナル・ビジネス・マシーンズ・コーポレーションの商標

である。）

【００７１】

仮想化レイヤ６０２は、抽象化レイヤを提供し、そこから仮想化サーバ、仮想化ストレージ、バーチャル・プライベート・ネットワークを含む仮想化ネットワーク、仮想化アプリケーションおよびオペレーティング・システムおよび仮想クライアントなどの仮想化エンティティの例が提供される。一例においては、管理レイヤ６０４は、以下に説明する機能を提供してもよい。リソース・プロビショニングは、クラウド・コンピューティング環境内でタスクを実行するために利用されるコンピューティング・リソースおよび他のリソースの動的な調達を提供する。メータリングおよびプライシングは、リソースがクラウド・コンピューティング環境内で利用されるコストの追跡およびこれらのソースの消費に対する請求またはインボイスの送付を提供する。一例においては、これらのリソースは、アプリケーション・ソフトウェアのライセンスを含んでもよい。セキュリティは、クラウド・コンシューマおよびタスクについての本人確認、並びに、データおよび他のリソースに対する保護を提供する。ユーザポータルは、コンシューマおよびシステム管理者に対しクラウド・コンピューティング環境へのアクセスを提供する。サービス・レベル・マネジメントは、要求されるサービス・レベルを満たすようにクラウド・コンピューティング・リソースの割り当ておよび管理を提供する。サービス・レベル合意（ＳＬＡ）の計画と履行は、ＳＬＡに従って、将来の要求が予期されるクラウド・コンピューティグ・リソースの事前配置および調達を提供する。

【００７２】

ワークロード・レイヤ６０６は、クラウド・コンピューティング環境が利用される機能性の例を提供する。ワークロードおよびこのレイヤから提供される機能の例には、マッピングおよびナビゲーション、ソフトウェア開発およびライフサイクル管理、仮想クラスルーム教育配信、データ・アナリティクス処理、トランザクション処理、ワークフロー自動化が含まれる。

【００７３】

本発明は、任意の可能な統合の技術的詳細のレベルにおけるシステム、方法もしくはコンピュータ・プログラム製品またはその組み合わせであってよい。コンピュータ・プログラム製品は、プロセッサに本発明の側面を実行させるためのコンピュータ可読プログラム命令をその上に有するコンピュータ可読ストレージ媒体を含んでもよい。

【００７４】

コンピュータ可読ストレージ媒体は、命令実行デバイスによって使用するための命令を保持し格納する有形のデバイスであってよい。コンピュータ可読ストレージ媒体は、例えば、これに限定されるものではないが、電子的ストレージ・デバイス、磁気ストレージ・デバイス、光学ストレージ・デバイス、電磁気ストレージ・デバイス、半導体ストレージ・デバイスまたは上記の任意の適切な組み合わせであってよい。コンピュータ可読ストレージ媒体のより具体的な例示の非網羅的リストとしては、ポータブル・コンピュータ・ディスケット、ハード・ディスク、ランダム・アクセス・メモリ（ＲＡＭ）、リード・オンリー・メモリ（ＲＯＭ）、消去可能プログラマブル・リード・オンリー・メモリ（ＥＰＲＯＭまたはフラッシュメモリ）、スタティック・ランダム・アクセス・メモリ（ＳＲＡＭ）、ポータブル・コンパクト・ディスク・リード・オンリー・メモリ（ＣＤ－ＲＯＭ）、デジタル・バーサタイル・ディスク（ＤＶＤ）、メモリースティック、フロッピーディスク（登録商標）、パンチカードまたは記録された命令を有する溝内の隆起構造のような機械的エンコードされたデバイス、および上記の任意の適切な組み合わせが含まれる。コンピュータ可読ストレージ媒体は、本明細書で使用されるように、電波、自由伝搬する電磁波、導波路または他の伝送媒体を伝搬する電磁波（たとえば、ファイバ光ケーブルを通過する光パルス）または、ワイヤを通して伝送される電気信号のような、それ自体が一時的な信号として解釈されるものではない。

【００７５】

本明細書で説明されるコンピュータ可読プログラム命令は、コンピュータ可読ストレー

ジ媒体からそれぞれのコンピュータ／処理デバイスに、または、例えばインターネット、ローカル・エリア・ネットワーク、ワイド・エリア・ネットワークもしくは無線ネットワークまたはその組み合わせといったネットワークを介して外部コンピュータまたは外部ストレージ・デバイスにダウンロードすることができる。ネットワークは、銅伝送ケーブル、光伝送ファイバ、無線伝送、ルータ、ファイアウォール、スイッチ、ゲートウェイ・コンピュータもしくはエッジサーバまたはその組み合わせを含んでもよい。各コンピュータ／処理デバイスにおけるネットワーク・アダプタ・カードまたはネットワーク・インタフェースは、ネットワークからコンピュータ可読プログラム命令を受信し、コンピュータ可読プログラム命令を、それぞれのコンピューティング／処理デバイス内のコンピュータ可読ストレージ媒体に格納するために転送する。

【００７６】

本発明の動作を実行するためのコンピュータ可読プログラム命令は、アセンブラ命令、命令セットアーキテクチャ（ＩＳＡ）命令、機械語命令、機械依存命令、マイクロコード、ファームウェア命令、状態設定データ、または、１以上のプログラミング言語の任意の組み合わせで書かれたコードあるいはオブジェクト・コードであってよく、１以上のプログラミング言語は、Ｓｍａｌｌｔａｌｋ（登録商標）、Ｃ＋＋またはこれらに類するものなどのオブジェクト指向言語、Ｃプログラミング言語または類似のプログラミング言語などの従来型の手続型言語を含む。コンピュータ可読プログラム命令は、スタンド・アローンのソフトウェア・パッケージとして、全体としてユーザのコンピュータ上で、部分的にユーザのコンピュータ上で、部分的にユーザのコンピュータ上かつ部分的に遠隔のコンピュータ上で、または、完全に遠隔のコンピュータまたはサーバ上で実行されてもよい。後者のシナリオでは、遠隔のコンピュータは、ユーザのコンピュータに、ローカル・エリア・ネットワーク（ＬＡＮ）またはワイド・エリア・ネットワーク（ＷＡＮ）を含む任意のタイプのネットワークを通じて接続されてもよく、あるいは接続は、（例えば、インターネット・サービス・プロバイダを用いてインターネットを通じて）外部コンピュータになされてもよい。いくつかの実施形態においては、電気的回路は、本発明の側面を実行するために、コンピュータ可読プログラム命令の状態情報を利用して、電気的回路を個別化することによって、コンピュータ可読プログラム命令を実行してもよく、この電気的回路は、例えば、プログラマブル・ロジック回路、フィールド・プログラマブル・ゲート・アレイ（ＦＰＧＡ）、またはプログラマブル・ロジック・アレイ（ＰＬＡ）を含む。

【００７７】

本発明の側面は、本明細書において、本技術の実施形態に従った方法、装置（システム）およびコンピュータ・プログラム製品のフローチャート図もしくはブロック図またはその両方を参照しながら、説明される。フローチャート図もしくはブロック図またはその両方の各ブロック、および、フローチャート図もしくはブロック図またはその両方における複数のブロックの組み合わせは、コンピュータ可読プログラム命令によって実装されてもよいことが理解されよう。

【００７８】

これらのコンピュータ可読プログラム命令は、汎用コンピュータ、特定目的コンピュータのプロセッサまたは他のプログラマブル・データ処理装置に提供され、コンピュータのプロセッサまたは他のプログラマブル・データ処理装置を介して実行される命令が、フローチャート図もしくはブロックまたはその両方のブロックまたは複数のブロックにおいて特定される機能／作用を実装するための手段を作成するように、マシンを生成する。これらのコンピュータ可読プログラム命令は、また、コンピュータ、プログラマブル・データ処理装置もしくは他のデバイスまたはその組み合わせに特定のやり方で機能するよう指示できるコンピュータ可読ストレージ媒体に格納され、それに格納された命令を有するコンピュータ可読ストレージ媒体に、フローチャートもしくはブロックまたはその両方のブロックまたは複数のブロックで特定される機能／作用の側面を実装する命令を含む製品が含まれるようにする。

【００７９】

コンピュータ可読プログラム命令は、また、コンピュータ、他のプログラマブル・データ処理装置、または他のデバイスにロードされ、コンピュータ、他のプログラマブル・データ処理装置または他のデバイス上で一連の動作ステップを実行させて、コンピュータ、他のプログラマブル・データ処理装置または他のデバイス上で実行される命令が、フローチャートもしくはブロックまたはその両方のブロックまたは複数のブロックで特定される機能／作用の側面を実装するように、コンピュータ実装処理を生成することもできる。

【００８０】

図７を参照すると、構造化されたログイベントを用いてワークフローを自動化し、支援することができる一例の有形の非一時的なコンピュータ可読媒体７００のブロック図が示されている。有形の非一時的なコンピュータ可読媒体７００は、プロセッサ７０２によってコンピュータ相互接続７０４を介してアクセスされてもよい。さらに、有形の非一時的なコンピュータ可読媒体７００は、プロセッサ７０２に、図２および図３の方法２００および３００の動作を実行させるように指示するコードを含んでもよい。

【００８１】

本明細書で説明する種々のソフトウェア・コンポーネントは、例えば、図７に示すように、有形的、非一時的なコンピュータ可読媒体７００に格納されてもよい。例えば、活動モニタ７０６は、ユーザインタフェースを監視して、ステップフローを含む活動ログを生成するためのコードを含む。自然言語理解モジュール７１０は、活動ログ内の非構造化データから特徴および共通変数を抽出し、抽出された特徴および共通変数に基づいて、構造化ログイベントを生成するためのコードを含む。プロセス・マイナ・モジュール７１２は、構造化ログイベントに基づいてワークフロー・モデルを生成するためのコードを含む。いくつかの例において、プロセス・マイナ・モジュール７１２は、構造化ログイベントを、開始イベント、ステップフローおよび終了イベントに変換するためのコードを含む。種々の例において、プロセス・マイナ・モジュール７１２は、監視されるプロセスの中の共通の開始イベントを検出するためのコードを含む。プロセス・マイナ・モジュール７１２は、共通の開始イベントに基づいてプロセスを統合して最適化するためのコードを含んでもよい。プロセス・マイナ・モジュール７１２は、さらに、プロセスの中の共通のサブプロセスを検出するためのコードを含んでもよい。プロセス・マイナ・モジュール７１２は、また、プロセスの中の各プロセスの遷移規則を検出するためのコードを含んでもよい。プロセス・マイナ・モジュール７１２は、分類を実行してコンテキストを検出するためのコードを含んでもよい。プロセス・マイナ・モジュール７１２は、また、開始イベント、遷移規則、共通のサブプロセスおよびコンテキストに基づいて、最適化されたフローモデルを生成するためのコードを含んでもよい。いくつかの例において、プロセス・マイナ・モジュール７１２は、ユーザフィードバックに基づいて最適化されたフローモデルを調整するためのコードを含んでもよい。種々の例において、プロセス・マイナ・モジュール７１２は、また、横断する顧客をクラスタ化し、クラスタにおける各顧客に推奨すべき改良されたワークフローを生成するためのコードを含む。ワークフロー・アシスタおよびオートメータ７１４は、生成されたワークフロー・モデルに基づいてワークフローを自動化または支援するためのコードを含む。いくつかの例において、ワークフロー・アシスタおよびオートメータ７１４は、ユーザ手動プロセスのための次のステップを示唆する予測分析を対話的に実行するためのコードを含む。特定の用途に応じて、図７に示されない任意の数の追加のソフトウェア・コンポーネントが、有形の非一時的なコンピュータ可読媒体７００内に含まれてもよいことを理解されたい。

【００８２】

図面におけるフローチャートおよびブロック図は、本発明の種々の実施形態に従ったシステム、方法およびコンピュータ・プログラム製品の可能な実装のアーキテクチャ、機能および動作を示す。この点に関して、フローチャートまたはブロック図の各ブロックは、特定の論理機能を実装するための１以上の実行可能な命令を含む、モジュール、セグメントまたは命令の部分を表す可能性がある。いくつかの代替の実装では、ブロックにおいて言及された機能は、図面に示された順序から外れて生じる可能性がある。例えば、連続し

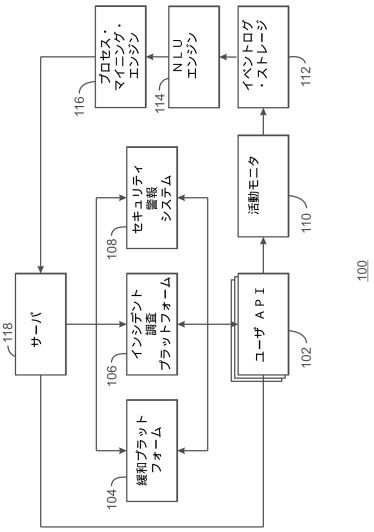
て示される２つのブロックは、実際には、実質的に同時に実行されてもよく、あるいは、複数のブロックは、関与する機能性に応じて逆の順序で実行されてもよい。ブロック図もしくはフローチャート図またはその両方の各ブロックおよびブロック図もしくはフローチャート図またはその両方の複数のブロックの組み合わせが、特定の機能または作用を実行し、または、特別な目的のハードウェアおよびコンピュータ命令の組み合わせを実施する、特定目的ハードウェアベースのシステムによって実装されてもよいことに留意されたい。特定の用途に応じて、図７に示されない任意の数の追加のソフトウェア・コンポーネントが、有形の非一時的なコンピュータ可読媒体７００内に含まれてもよいことを理解されたい。

【００８３】

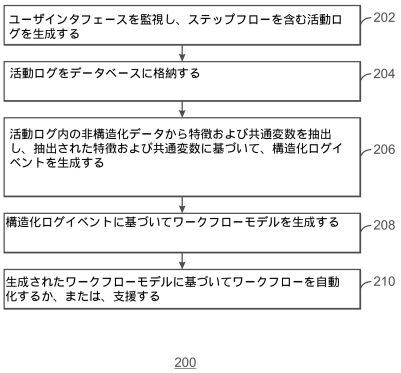
本技術の種々の実施形態の説明が、説明のために提示されたが、しかしながら、網羅的であること、または、開示される実施形態に限定されることを意図するものではない。説明される実施形態の範囲を逸脱することなく、多くの変更および変形が当業者にとって明らかであろう。本明細書で使用される用語は、実施形態の原理、実際の応用または市場で発見される技術に対する技術的改善を最もよく説明するために、あるいは、他の当業者が、本明細書で開示される実施形態を理解できるように選ばれたものである。

【図面】

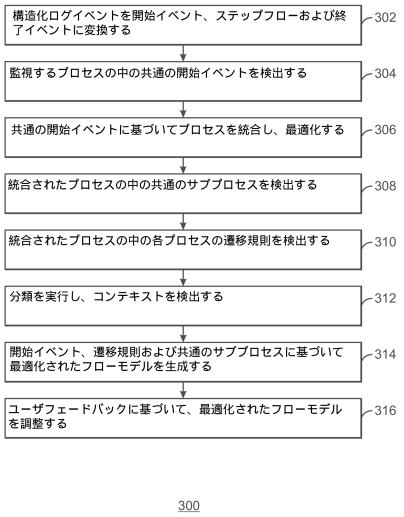
【図１】



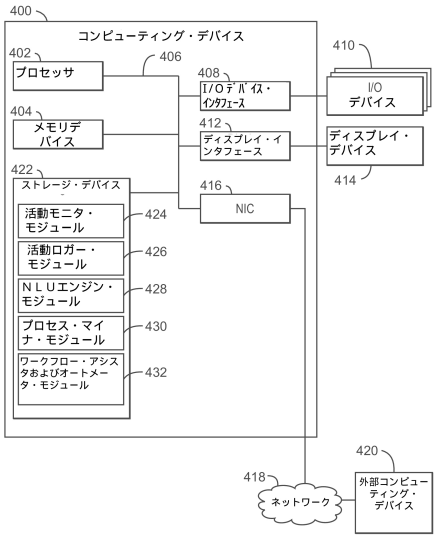
【図２】



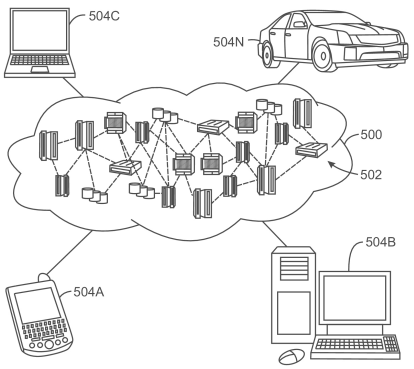
【図３】


構造化ログイベントを開始イベント、ステップフローおよび終了イベントに変換する
302
監視するプロセスの中の共通の開始イベントを検出する
304
共通の開始イベントに基づいてプロセスを統合し、最適化する
306
統合されたプロセスの中の共通のサブプロセスを検出する
308
統合されたプロセスの中の各プロセスの遷移規則を検出する
310
分類を実行し、コンテキストを検出する
312
開始イベント、遷移規則および共通のサブプロセスに基づいて最適化されたフローモデルを生成する
314
ユーザフェードバックに基づいて、最適化されたフローモデルを調整する
316
300

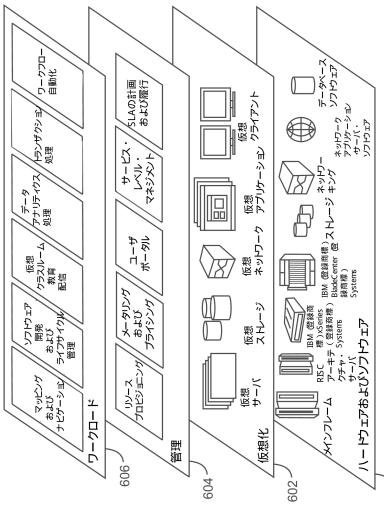
【図４】


400
コンピューティング・デバイス
402
プロセッサ
404
メモリデバイス
406
408
I/Oデバイス・インタフェース
410
I/Oデバイス
412
ディスプレイ・インタフェース
ディスプレイ・デバイス
414
422
ストレージ・デバイス
416
NIC
活動モニタ・モジュール
424
活動ロガー・モジュール
426
NLUエンジン・モジュール
428
プロセス・マイナ・モジュール
430
ワークフロー・アシスタおよびオートメータ・モジュール
432
418
ネットワーク
420
外部コンピューティング・デバイス

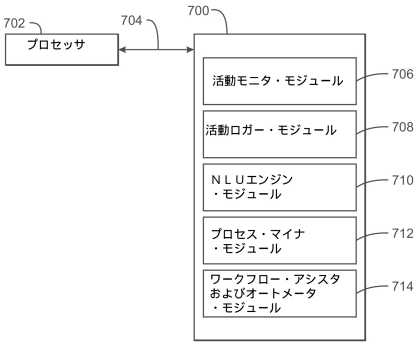
【図５】


504C
504N
500
502
504B
504A

【図６】


ワークロード
管理
仮想化
ハードウェアおよびソフトウェア
600
602
604
606

【図７】


702
プロセッサ
704
700
活動モニタ・モジュール
706
活動ロガー・モジュール
708
ＮＬＵエンジン
・モジュール
710
プロセス・マイナ
・モジュール
712
ワークフロー・アシスタ
およびオートメータ
・モジュール
714

【手続補正書】
【提出日】令和4年10月12日(2022.10.12)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
プロセッサを含むシステムであって、前記プロセッサは、
ユーザインタフェースを監視して、ステップフローを含む活動ログを生成することと、
前記活動ログ内の非構造化データから特徴および共通変数を抽出し、抽出された前記特徴および前記共通変数に基づいて、構造化ログイベントを生成することと、
前記構造化ログイベントに基づいてワークフロー・モデルを生成することと、
生成された前記ワークフロー・モデルに基づいてワークフローを自動化または支援すること
を行うためのものである、システム。
【請求項２】
前記構造化ログイベントは、自然言語理解ユニットを介して生成され、前記プロセッサは、前記構造化ログイベントを、開始イベント、ステップフローおよび終了イベントに変換するためのものである、請求項１に記載のシステム。
【請求項３】
前記プロセッサが、
監視されるプロセスの中の共通の開始イベントを検出することと、
前記共通の開始イベントに基づいて前記プロセスを統合して最適化することと、
前記プロセスの中の共通のサブプロセスを検出することと、
統合された前記プロセスの中の各プロセスの遷移規則を検出することと、
分類を実行してコンテキストを検出することと、
前記開始イベント、前記遷移規則、前記共通のサブプロセスおよび前記コンテキストに基づいて、最適化されたフローモデルを生成することと
を行うためのものである、請求項１または２に記載のシステム。
【請求項４】
前記プロセッサは、ユーザフィードバックに基づいて最適化された前記フローモデルを調整するためのものである、請求項３に記載のシステム。
【請求項５】
前記プロセッサは、横断する顧客をクラスタ化し、クラスタにおける各顧客に提示すべき改良されたワークフローを生成するためのものである、請求項１～４のいずれか１項に記載のシステム。
【請求項６】
前記プロセッサは、ユーザの手動プロセスのための次のステップを示唆する予測分析を対話的に実行するためのものである、請求項１～５のいずれか１項に記載のシステム。
【請求項７】
前記自動化または支援されたワークフローは、セキュリティ上のベストプラクティスなワークフロー、フォレンジック・プロセス・ワークフロー、システム・チューニング・ワークフローまたはリスク緩和プロセス・ワークフローを含む、請求項１～６のいずれか１項に記載のシステム。
【請求項８】
コンピュータ実装方法であって、
プロセッサを介して、ユーザインタフェースを監視して、ステップフローを含む活動ログを生成するステップと、

前記プロセッサを介して、前記活動ログ内の非構造化データから特徴および共通変数を抽出し、抽出された前記特徴および前記共通変数に基づいて、構造化ログイベントを生成するステップと、
前記プロセッサを介して、前記構造化ログイベントに基づいてワークフロー・モデルを生成するステップと、
前記プロセッサを介して、生成された前記ワークフロー・モデルに基づいてワークフローを自動化または支援するステップと
を含む、コンピュータ実装方法。
【請求項９】
前記構造化ログイベントを、開始イベント、ステップフローおよび終了イベントに変換するステップを含む、請求項８に記載のコンピュータ実装方法。
【請求項１０】
前記ワークフロー・モデルを生成するステップは、
監視されるプロセスの中の共通の開始イベントを検出するステップと、
前記共通の開始イベントに基づいて前記プロセスを統合して最適化するステップと、
前記プロセスの中の共通のサブプロセスを検出するステップと、
統合された前記プロセスの中の各プロセスの遷移規則を検出するステップと、
分類を実行してコンテキストを検出するステップと、
前記開始イベント、前記遷移規則、前記共通のサブプロセスおよび前記コンテキストに基づいて、最適化されたフローモデルを生成するステップと
を含む、請求項８または９に記載のコンピュータ実装方法。
【請求項１１】
前記ワークフロー・モデルを生成するステップは、
ユーザフィードバックに基づいて最適化された前記フローモデルを調整するステップを含む、請求項１０に記載のコンピュータ実装方法。
【請求項１２】
横断する顧客をクラスタ化するステップと、クラスタにおける各顧客に推奨すべき改良されたワークフローを生成するステップとを含む、請求項８～１１のいずれか１項に記載のコンピュータ実装方法。
【請求項１３】
ユーザの手動プロセスのための次のステップを示唆する予測分析を対話的に実行するステップをさらに含む、請求項８～１２のいずれか１項に記載のコンピュータ実装方法。
【請求項１４】
前記構造化ログイベントに基づいて追加のワークフロー・モデルを生成するステップと、自動的に前記追加のワークフロー・モデルを実行して、提示すべき複数の結果を生成するステップとを含む、請求項８～１３のいずれか１項に記載のコンピュータ実装方法。
【請求項１５】
ワークフローを自動化または支援するためのコンピュータ・プログラムであって、前記コンピュータ・プログラムは、プロセッサに、
ユーザインタフェースを監視して、ステップフローを含む活動ログを生成することと、
前記活動ログ内の非構造化データから特徴および共通変数を抽出し、抽出された前記特徴および前記共通変数に基づいて、構造化ログイベントを生成することと、
前記構造化ログイベントに基づいてワークフロー・モデルを生成することと、
生成された前記ワークフロー・モデルに基づいてワークフローを自動化または支援すること
を実行させるためのものである、コンピュータ・プログラム。
【請求項１６】
前記コンピュータ・プログラムは、前記プロセッサに、さらに、前記構造化ログイベントを開始イベント、ステップフローおよび終了イベントに変換することを実行させる、請求項１５に記載のコンピュータ・プログラム。

【請求項１７】
前記コンピュータ・プログラムは、前記プロセッサに、
監視されるプロセスの中の共通の開始イベントを検出することと、
前記共通の開始イベントに基づいて前記プロセスを統合して最適化することと、
前記プロセスの中の共通のサブプロセスを検出することと、
統合された前記プロセスの中の各プロセスの遷移規則を検出することと、
分類を実行してコンテキストを検出することと、
前記開始イベント、前記遷移規則、前記共通のサブプロセスおよび前記コンテキストに基づいて、最適化されたフローモデルを生成することと
を実行させる、請求項１５または１６に記載のコンピュータ・プログラム。
【請求項１８】
前記コンピュータ・プログラムは、前記プロセッサに、ユーザフィードバックに基づいて最適化された前記フローモデルを調整することを実行させる、請求項１７に記載のコンピュータ・プログラム。
【請求項１９】
前記コンピュータ・プログラムは、前記プロセッサに、横断する顧客をクラスタ化し、クラスタにおける各顧客に推奨すべき改良されたワークフローを生成することを実行させる、請求項１５～１８のいずれか１項に記載のコンピュータ・プログラム。
【請求項２０】
前記コンピュータ・プログラムは、前記プロセッサに、ユーザ手動プロセスのための次のステップを示唆する予測分析を対話的に実行することを実行させる、請求項１５～１９のいずれか１項に記載のコンピュータ・プログラム。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB2020/062537

A. CLASSIFICATION OF SUBJECT MATTER

G06F 7/00(2006.01)i; G06Q 10/00(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F; G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNPAT, WPI, EPODOC, IEEE: log?, events, step-flows, workflow, common, activity, feature?, variables, unstructured, structured, model

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 103218692 A (NANJING UNIVERSITY OF SCIENCE & TECHNOLOGY) 24 July 2013 (2013-07-24) description, paragraphs 0002-0048, figures 1-5	1-20
Y	US 9122694 B1 (LOGZILLA CORPORATION) 01 September 2015 (2015-09-01) claims 1-5, description, column 5, line 25 to column 10, line 4 and figures 1-2	1-20
A	CN 107909344 A (HANGZHOU DIANZI UNIVERSITY) 13 April 2018 (2018-04-13) the whole document	1-20
A	US 2018107529 A1 (NEC LABORATORIES AMERICA, INC.) 19 April 2018 (2018-04-19) the whole document	1-20
A	CN 102332125 A (NANJING UNIVERSITY) 25 January 2012 (2012-01-25) the whole document	1-20
A	US 2017344926 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 30 November 2017 (2017-11-30) the whole document	1-20

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 March 2021	**09 April 2021**
Name and mailing address of the ISA/CN **National Intellectual Property Administration, PRC** **6, Xitucheng Rd., Jimen Bridge, Haidian District, Beijing** **100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer **ZHANG,Wen** Telephone No. **86-(10)-53961314**

Form PCT/ISA/210 (second sheet) (January 2015)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/IB2020/062537

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	103218692	A	24 July 2013	None			
US	9122694	B1	01 September 2015	US	2016085452	A1	24 March 2016
				US	9195674	B1	24 November 2015
				US	2016085792	A1	24 March 2016
CN	107909344	A	13 April 2018	None			
US	2018107529	A1	19 April 2018	None			
CN	102332125	A	25 January 2012	None			
US	2017344926	A1	30 November 2017	None			

Form PCT/ISA/210 (patent family annex) (January 2015)

フロントページの続き

MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,KM,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DJ,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IR,IS,IT,JO,JP,KE,KG,KH,KN,KP,KR,KW,KZ,LA,LC,LK,LR,LS,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SA,SC,SD,SE,SG,SK,SL,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,WS,ZA,ZM,ZW

(74)代理人　100112690
弁理士　太佐 種一
(74)代理人　100120710
弁理士　片岡 忠彦
(72)発明者　ソフェー，オデッド
イスラエル ハイファ ３１９０５ マウント・カーメル ハイファ大学キャンパス
(72)発明者　マルガリット，オデッド
イスラエル ハイファ ３１９０５ マウント・カーメル ハイファ大学キャンパス
(72)発明者　アロウシュ，ヤイア
イスラエル ハイファ ３１９０５ マウント・カーメル ハイファ大学キャンパス

Ｆターム（参考）　5B175　DA01 FB04