

(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号

特許第7035096号

(P7035096)

(45)発行日 令和4年3月14日(2022.3.14)

(24)登録日 令和4年3月4日(2022.3.4)

(51)国際特許分類

F I

G 0 6 F 21/62 (2013.01)

G 0 6 F 21/62 3 1 8

G 0 6 F 21/57 (2013.01)

G 0 6 F 21/57 3 7 0

G 0 6 F 21/31 (2013.01)

G 0 6 F 21/31

請求項の数 17 (全74頁)

(21)出願番号 特願2019-570846(P2019-570846)
(86)(22)出願日 平成30年6月19日(2018.6.19)
(65)公表番号 特表2020-524855(P2020-524855
A)
(43)公表日 令和2年8月20日(2020.8.20)
(86)国際出願番号 PCT/US2018/038347
(87)国際公開番号 WO2018/236915
(87)国際公開日 平成30年12月27日(2018.12.27)
審査請求日 令和3年4月2日(2021.4.2)
(31)優先権主張番号 62/523,668
(32)優先日 平成29年6月22日(2017.6.22)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号 16/011,538
(32)優先日 平成30年6月18日(2018.6.18)
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940
65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
特許業務法人深見特許事務所
(72)発明者 キルティ、ガネーシュ
アメリカ合衆国、95054 カリフォ
ルニア州、サン・ノゼ、トレセル・ド
ライブ、6221
(72)発明者 ビスワス、カマレンドゥ
アメリカ合衆国、94582 カリフォ
ルニア州、サン・ラモン、マクラレン
最終頁に続く

(54)【発明の名称】 コンピューティング環境における特権ユーザの監視および異常なアクティビティの検出の
手法

(57)【特許請求の範囲】

【請求項1】

コンピュータにより実現される方法であって、セキュリティ管理システムのコンピュータシステムにおいて、
サービスプロバイダシステムからアクティビティデータを取得することを備え、前記アクティビティデータは、クラウドサービスの利用中に実行されるアクションを記述し、前記アクションは、テナントに関連付けられた1人以上のユーザによって実行され、前記サービスプロバイダシステムは前記テナントにテナントアカウントを提供し、前記テナントアカウントにより、前記1人以上のユーザは前記クラウドサービスにアクセスすることができ、前記方法はさらに、前記セキュリティ管理システムのコンピュータシステムにおいて、前記アクティビティデータにおいて、前記クラウドサービスに関して特権のある1つ以上のアクションを識別することと、
前記アクティビティデータを用いて、前記1つ以上のアクションを実行したユーザのセットを識別することとを備え、前記ユーザのセットは前記テナントに関連付けられた前記1人以上のユーザから判断され、前記方法はさらに、前記セキュリティ管理システムのコンピュータシステムにおいて、
前記ユーザのセットを、特権を有するとして分類することと、
前記アクティビティデータを用いて、前記1人以上のユーザの1つ以上のリスクスコアを判定することと、
前記ユーザのセット内におけるユーザのリスクスコアがしきい値より大きいと判断するこ

とと、

前記サービスプロバイダシステムのセキュリティ制御を判断することとを備え、前記セキュリティ制御は、前記クラウドサービスへのアクセスを構成するために前記サービスプロバイダシステムによって用いられ、前記方法はさらに、前記セキュリティ管理システムのコンピュータシステムにおいて、

前記サービスプロバイダシステムに送信するための1つ以上の命令を判断することと、前記1つ以上の命令を前記サービスプロバイダシステムに送信することとを備え、前記1つ以上の命令は前記セキュリティ制御を前記ユーザに関して変更させ、前記ユーザによる前記クラウドサービスへのアクセスは、前記セキュリティ制御の変更により変更される、コンピュータにより実現される方法。

10

【請求項2】

前記1つ以上のアクションは、前記クラウドサービスに関連付けられたアクションのリストを用いて識別され、前記アクションのリスト内のアクションは、前記クラウドサービスに関して特権を有するとして分類される、請求項1に記載のコンピュータにより実現される方法。

【請求項3】

前記1つ以上のアクションは、管理アクションのリストを用いて識別される、請求項1または2に記載のコンピュータにより実現される方法。

【請求項4】

前記1つ以上のアクションおよび過去のアクティビティデータを用いてモデルを生成することをさらに備え、前記モデルは、前記クラウドサービスに関して特権のある前記クラウドサービスの利用のパターンを記述し、前記方法はさらに、前記モデルを用いて前記ユーザのセットを識別することを備える、請求項1～3のいずれかに記載のコンピュータにより実現される方法。

20

【請求項5】

前記クラウドサービスの利用中に実行されるアクションをグループ化することと、特権のあるアクションを含むアクションのグループを識別することとをさらに備え、前記ユーザのセットは前記アクションのグループを用いて識別される、請求項1～4のいずれかに記載のコンピュータにより実現される方法。

【請求項6】

リスクスコアは、前記クラウドサービスの利用時にユーザが実行したアクションから前記テナントに対するセキュリティリスクの程度を示す、請求項1～5のいずれかに記載のコンピュータにより実現される方法。

30

【請求項7】

リスクスコアは、リスクインジケータの重みの合計として計算される、請求項1～6のいずれかに記載のコンピュータにより実現される方法。

【請求項8】

特権を有するとして分類されたユーザのリスクスコアは、非特権ユーザのリスクスコアよりも大きな重みで計算される、請求項1～7のいずれかに記載のコンピュータにより実現される方法。

40

【請求項9】

特権アクションは、第1のユーザによって実行されると、他のユーザによる前記クラウドサービスの利用に影響を与える態様で前記クラウドサービスを変更することができるアクションである、請求項1～8のいずれかに記載のコンピュータにより実現される方法。

【請求項10】

特権アクションは、第1のユーザによって実行されると、前記クラウドサービスの他のユーザのユーザアカウントに影響を与えることができるアクションである、請求項1～9のいずれかに記載のコンピュータにより実現される方法。

【請求項11】

セキュリティ管理システムのコンピューティングシステムであって、

50

1つ以上のプロセッサと、

前記1つ以上のプロセッサに結合され、前記1つ以上のプロセッサによって読み取り可能であるメモリとを備え、前記メモリは命令を含み、前記命令は、前記1つ以上のプロセッサによって実行されると、前記1つ以上のプロセッサに動作を実行させ、前記動作は、サービスプロバイダシステムからアクティビティデータを取得することを含み、前記アクティビティデータは、クラウドサービスの利用中に実行されるアクションを記述し、前記アクションは、テナントに関連付けられた1人以上のユーザによって実行され、前記サービスプロバイダシステムは前記テナントにテナントアカウントを提供し、前記テナントアカウントにより、前記1人以上のユーザは前記クラウドサービスにアクセスすることができ、前記動作はさらに、

10

前記アクティビティデータにおいて、前記クラウドサービスに関して特権のある1つ以上のアクションを識別することと、

前記アクティビティデータを用いて、前記1つ以上のアクションを実行したユーザのセットを識別することとを含み、前記ユーザのセットは前記テナントに関連付けられた前記1人以上のユーザから判断され、前記動作はさらに、

前記ユーザのセットを、特権を有するとして分類することと、

前記アクティビティデータを用いて、前記1人以上のユーザの1つ以上のリスクスコアを判定することと、

前記ユーザのセット内におけるユーザのリスクスコアがしきい値より大きいと判断することと、

20

前記サービスプロバイダシステムのセキュリティ制御を判断することとを含み、前記セキュリティ制御は、前記クラウドサービスへのアクセスを構成するために前記サービスプロバイダシステムによって用いられ、前記動作はさらに、

前記サービスプロバイダシステムに送信するための1つ以上の命令を判断することと、

前記1つ以上の命令を前記サービスプロバイダシステムに送信することとを含み、前記1つ以上の命令は前記セキュリティ制御を前記ユーザに関して変更させ、前記ユーザによる前記クラウドサービスへのアクセスは、前記セキュリティ制御の変更により変更される、セキュリティ管理システムのコンピューティングシステム。

【請求項12】

前記1つ以上のアクションは、前記クラウドサービスに関連付けられたアクションのリストを用いて識別され、前記アクションのリストは、前記クラウドサービスに関して特権を有するとして分類される、請求項11に記載のコンピューティングシステム。

30

【請求項13】

前記1つ以上のアクションは、管理アクションのリストを用いて識別される、請求項11または12に記載のコンピューティングシステム。

【請求項14】

前記メモリはさらに、命令を含み、前記命令は、前記1つ以上のプロセッサによって実行されると、前記1つ以上のプロセッサに動作を実行させ、前記動作は、

前記1つ以上のアクションおよび過去のアクティビティデータを用いてモデルを生成することを含み、前記モデルは、前記クラウドサービスに関して特権のある前記クラウドサービスの利用のパターンを記述し、前記動作はさらに、

40

前記モデルを用いて前記ユーザのセットを識別することを含む、請求項11～13のいずれかに記載のコンピューティングシステム。

【請求項15】

前記メモリはさらに、命令を含み、前記命令は、前記1つ以上のプロセッサによって実行されると、前記1つ以上のプロセッサに動作を実行させ、前記動作は、

前記クラウドサービスの利用中に実行されるアクションをグループ化することと、

特権のあるアクションを含むアクションのグループを識別することとを含み、前記ユーザのセットは前記アクションのグループを用いて識別される、請求項11～14のいずれかに記載のコンピューティングシステム。

50

【請求項 16】

請求項 1 ~ 10 のいずれか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。

【請求項 17】

請求項 16 に記載のプログラムを格納したメモリと、

前記プログラムを実行するためのプロセッサとを備える、コンピュータ。

【発明の詳細な説明】

【背景技術】

【0001】

関連出願への相互参照

本出願は、2017年6月22日に出願された米国仮出願番号第62/523,668号
および2018年6月18日に出願された米国出願番号第16/011,538号の優先
権を主張し、それぞれの全体を参照により本明細書に組み込む。

10

【0002】

背景

クラウドサービスプロバイダは、「クラウド」でさまざまなサービスを提供する。つまり、パブリックインターネットなどのネットワーク経由で、ネットワークに接続されたクライアントデバイスにリモートでアクセス可能である。クラウドサービスプロバイダ（以下、「クラウドプロバイダ」または「プロバイダ」とも呼ばれる）で用いられるサービスモデルの例には、サービスとしてのインフラストラクチャ（IaaS）、サービスとしてのプラットフォーム（PaaS）、サービスとしてのソフトウェア（SaaS）、サービスとしてのネットワーク（Naas）が含まれる。IaaSプロバイダは、顧客がソフトウェアを実行するために使用できる処理、ストレージ、ネットワーク、その他のコンピューティングリソースなどのインフラストラクチャリソースを顧客に提供する。顧客はインフラストラクチャを管理しないが、オペレーティングシステム、ストレージ、展開されたアプリケーションなどを制御し、ファイアウォールなどの一部のネットワーク接続コンポーネントを制御できる場合がある。PaaSプロバイダは、基盤となるコンピューティングインフラストラクチャを維持することなく、顧客がアプリケーションを開発、実行、管理することができるプラットフォームを顧客に提供する。SaaSは、ソフトウェアがサブスクリプションベースで顧客にライセンスされるソフトウェアライセンス付与および配信モデルであり、クラウドプロバイダによって中央でホストされる。このモデルでは、たとえばウェブブラウザを用いてアプリケーションにアクセスすることができる。Naasプロバイダは、たとえば、別のパーティが運営するネットワークインフラストラクチャ上で仮想ネットワークをプロビジョニングすることにより、ネットワークサービスを顧客に提供する。これらの各サービスモデルでは、クラウドサービスプロバイダが、サービスを提供するハードウェアやソフトウェアを維持および管理し、ユーザのデバイス上で実行されるソフトウェアは、あったとしてもほとんどない。

20

30

【0003】

ユーザまたはテナントと呼ばれ得るクラウドサービスプロバイダの顧客は、サービスプロバイダに加入して、サービスプロバイダが提供する特定のサービスにアクセスすることができる。サービスプロバイダは、ユーザまたはテナントのアカウントを維持することができる。ユーザおよび/またはテナントは、このアカウントを介してプロバイダのサービスにアクセスすることができる。サービスプロバイダは、個々のユーザのテナントのために、テナントに関連付けられているユーザアカウントをさらに維持することができる。サービスプロバイダの例には、Box、Dropbox、Microsoft、DocuSign、Google（登録商標）、Salesforce、Oracle、Amazonなどが含まれる。これらのようなサービスプロバイダは複数の異なるサービスを提供することができるが、異なるサービスプロバイダは、インフラストラクチャやセキュリティ境界を共有しないなど、相互に提携する必要はない。多くの場合、サービスプロバイダシステムは高度に保護されており、非テナントには閉鎖されている。

40

【0004】

50

組織がコンピューティング環境に依存しているため、コラボレーション、販売および顧客サービス、インフラストラクチャなどの運用にクラウドサービスが広く採用されている。クラウド環境を介して提供されるアプリケーションにより、組織はデータセンター、ハードウェア、ソフトウェア、展開プロジェクトに多くの先行投資をすることなく、サービスをより迅速に展開することができる。アプリケーションのアクセシビリティは、職場、自宅、ホテルなどの多くの場所からクラウド対応サービスを利用することができるため、従業員の生産性を向上させることができる。

【 0 0 0 5 】

組織および/または組織のユーザは多くの異なるクラウドサービスプロバイダのサービスに加入する可能性があるため、組織はクラウドサービスの利用によって組織自体のシステムが損なわれないようにする方法が必要になる場合がある。クラウドサービスを利用すると、組織が組織内でサービスをホストおよび管理する場合には存在しないセキュリティリスクにつながる可能性がある。

【 発明の概要 】

【 発明が解決しようとする課題 】

【 0 0 0 6 】

簡単な要約

さまざまな実現例において、クラウドサービスプロバイダが提供するアプリケーションまたはサービスに関して特権能力を有するユーザを特定することができるクラウドセキュリティシステムのためのシステムおよび方法が提供される。管理者ユーザまたは特権ユーザと呼ばれ得る特権能力を有するユーザは、クラウドサービスの操作方法および/または他のユーザがクラウドサービスを利用する方法を変更することができる、クラウドサービスにアクセスまたはクラウドサービスを変更することができる能力を有することができる。特権ユーザはクラウドサービスに関して通常のユーザよりも多くの能力を有するため、特権ユーザをより詳細に監視し、特権ユーザアカウントが侵害されているかどうかを迅速に判断することが望ましい場合がある。

【 0 0 0 7 】

しかしながら、クラウドサービスでは、どのユーザが特権を有し、どのユーザが一般ユーザであるかを知ることは簡単ではない場合がある。クラウドサービスごとに、ユーザに特権を与えるためのパラメータが異なる場合がある。さらに、クラウドサービスは、顧客のためにどのユーザアカウントに特権があるかを判断する方法を提供しない場合がある。

【 課題を解決するための手段 】

【 0 0 0 8 】

セキュリティ管理システムがクラウドサービスの特権ユーザを識別することを可能にするシステム、方法、およびコンピュータ可読媒体が提供される。さまざまな実現例において、セキュリティ管理システムは、クラウドサービスの特権ユーザを識別するための技術を含むことができ、その技術にはさまざまなステップを実行することが含まれる。ステップには、サービスプロバイダシステムからアクティビティデータを取得することが含まれる。アクティビティデータは、クラウドサービスの利用中に実行されるアクションを記述することができる。アクションは、テナントに関連付けられた1人以上のユーザによって実行することができる、サービスプロバイダシステムはテナントにテナントアカウントを提供する。テナントアカウントにより、1人以上のユーザはクラウドサービスにアクセスすることができる。ステップにはさらに、アクティビティデータにおいて、クラウドサービスに関して特権のある1つ以上のアクションを識別することが含まれ得る。ステップには、さらに、アクティビティデータを用いて、1つ以上のアクションを実行したユーザのセットを識別することが含まれ得る。ユーザのセットは、テナントに関連付けられている1人以上のユーザから判定することができる。このステップには、さらに、ユーザのセットを特権ユーザとして分類することが含まれ得る。ステップにはさらに、アクティビティデータを用いて、1人以上のユーザの1つ以上のリスクスコアを判定することが含まれ得る。ステップには、さらに、ユーザのセット内におけるユーザのリスクスコアがしきい値より

10

20

30

40

50

大きいことを判定することが含まれ得る。ステップには、さらに、サービスプロバイダシステムのセキュリティ制御を判定することが含まれ得、セキュリティ制御は、クラウドサービスへのアクセスを構成するためにサービスプロバイダシステムによって用いられる。ステップには、さらに、サービスプロバイダシステムに送信するための1つ以上の命令を判定することが含まれ得る。ステップには、さらに、1つ以上の命令をサービスプロバイダシステムに送信することが含まれ得る。1つ以上の命令により、セキュリティ制御をユーザに関して変更することができ、この場合、ユーザによるクラウドサービスへのアクセスは、セキュリティ制御の変更により変更される。

【0009】

さまざまな局面において、1つ以上のアクションは、クラウドサービスに関連付けられたアクションのリストを用いて識別される。アクションのリスト内のアクションは、クラウドサービスに関して特権を有するとして分類される。さまざまな局面において、1つ以上のアクションは、管理アクションのリストを用いて識別される。

10

【0010】

さまざまな局面において、上記のシステム、方法、およびコンピュータ可読媒体によって実現される技術は、1つ以上のアクションおよび過去のアクティビティデータを用いてモデルを生成するなどのステップをさらに含み、モデルは、クラウドサービスに関して特権のあるクラウドサービスの利用のパターンを記述する。ステップには、さらに、モデルを用いてユーザのセットを識別することが含まれ得る。

【0011】

20

さまざまな局面において、上述のシステム、方法、およびコンピュータ可読媒体によって実現される技術は、クラウドサービスの利用中に実行されるアクションをグループ化するなどのステップをさらに含む。ステップには、特権のあるアクションを含むアクションのグループを識別することがさらに含まれ得、アクションのグループを用いてユーザのセットが識別される。

【0012】

さまざまな局面において、リスクスコアは、クラウドサービスの利用時にユーザが実行したアクションからテナントに対するセキュリティリスクの程度を示す。さまざまな局面において、リスクスコアはリスクインジケータの重みの合計として計算される。さまざまな例では、特権ユーザとして分類されたユーザのリスクスコアは、非特権ユーザのリスクスコアよりも大きな重みで計算される。

30

【0013】

さまざまな局面において、特権アクションは、第1のユーザによって実行されると、他のユーザによるクラウドサービスの利用に影響を与える状態でクラウドサービスを変更することができるアクションである。さまざまな局面において、特権アクションは、第1のユーザが実行すると、クラウドサービスの他のユーザのユーザアカウントに影響を与えることができるアクションである。

【0014】

上記は、他の特徴および実現例とともに、以下の明細書、特許請求の範囲、および添付の図面を参照することでより明らかになるであろう。

40

【図面の簡単な説明】

【0015】

【図1】セキュリティ監視および制御システムを含むコンピューティング環境の例を示すブロック図を含む。

【図2】セキュリティ管理および制御システムによって実現することができる例示的なクラウドセキュリティシステムのブロック図を示す。

【図3】セキュリティ管理および制御システムの例示的な分析エンジンのブロック図を示す。

【図4】挙動分析エンジンのブロック図を示す。

【図5】表6のデータのグラフの例を示す。

50

【図 6】クラウドサービスの特権ユーザを判定し、特権ユーザのアクティビティが引き起こす可能性のあるセキュリティリスクを管理するためのプロセスの例を示すフローチャートを含む。

【図 7】上述のさまざまな例を実現することができる分散型システムの簡略図を示す。

【図 8】サービスがクラウドとして提供され得るシステム環境の 1 つ以上のコンポーネントの簡略化されたブロック図である。

【図 9】さまざまな例を実施するために使用され得るコンピュータシステムの例を示す。

【発明を実施するための形態】

【0016】

詳細な説明

以下の説明では、説明の目的で、さまざまな実現例および例を十分に理解するために、特定の詳細が示されている。しかしながら、これらの特定の詳細なしでさまざまな実現例を実施することができることは明らかである。たとえば、回路、システム、アルゴリズム、構造、技術、ネットワーク、プロセス、および他のコンポーネントは、不必要な詳細で実現例を不明瞭にしないために、ブロック図形式のコンポーネントとして示される場合がある。図および説明は、制限することを意図したものではない。

【0017】

本開示における図面を参照して開示される例など、いくつかの例は、フローチャート、フロー図、データフロー図、構造図、シーケンス図、またはブロック図として示されるプロセスとして説明される場合がある。シーケンス図またはフローチャートは、連続して起こるプロセスとして動作を示し得るが、動作の多くのは、平行して、または同時に行われてもよい。これに加えて、動作の順序は、並び替えられてもよい。プロセスは、その動作が完了したときに終了するが、図に含まれない追加のステップを有し得る。プロセスは、方法、関数、プロシージャ、サブルーチン、サブプログラムなどに相当してもよい。プロセスが関数に相当する場合、その終了は、呼び出し関数またはメイン関数へのこの関数の戻りに相当してもよい。

【0018】

本開示における図を参照して説明されるプロセスなど、本明細書に示すプロセスは、1 つ以上の処理装置（たとえば、プロセッサコア）、ハードウェア、またはそれらの組合せによって実行されるソフトウェア（たとえば、コード、命令、プログラム）で実現されてもよい。ソフトウェアは、（たとえば、メモリ素子上、非一時的なコンピュータ可読記憶媒体上の）メモリに格納されてもよい。いくつかの例において、本明細書においてシーケンス図およびフローチャートに示されるプロセスは、本明細書に開示のいずれのシステムによっても実現され得る。本開示における特定の一続きの処理は、限定を意図したものではない。また、他の一続きのステップが別の例に従って実行されてもよい。たとえば、本開示の別の例は、上に概要を述べたステップを異なる順序で実行してもよい。また、図に示す個々のステップは、個々のステップに応じてさまざまな順序で行なわれ得る複数のサブステップを含んでもよい。さらに、特定のアプリケーションに応じてさらなるステップが追加または削除されてもよい。当業者は、多くの変形例、変更例、および代替例が分かるだろう。

【0019】

いくつかの例において、本開示の図の各プロセスは、1 つ以上の処理装置によって実行され得る。処理装置は、1 つ以上のプロセッサを含んでもよく、1 つ以上のプロセッサは、シングルコアもしくはマルチコア・プロセッサ、プロセッサの 1 つ以上のコア、またはそれらの組合せを含む。いくつかの例において、処理装置は、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、1 つ以上の専用コプロセッサを含み得る。いくつかの例において、処理装置の一部またはすべては、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、カスタム回路を使用して実現され得る。

【0020】

10

20

30

40

50

さまざまな例において、クラウドサービスは、サービスの管理ユーザをサービスの一般ユーザから区別する特権を定義することができる。このコンテキストでの特権とは、ネットワーク、アプリケーション、サービスなどのコンピューティングリソースに変更を加える能力、および/または非特権ユーザによるアクセスが制限されているリソースに影響を与える能力のことである。通常のユーザは最小限の特権セットを有することができるが、管理ユーザはより高い特権を有するため、管理ユーザは、管理ユーザがより高い特権を有するコンピューティングリソースを構成および管理することができる。管理ユーザは、本明細書では特権ユーザとも呼ばれる。

【0021】

クラウドサービスは、クラウドサービスに固有のさまざまな方法で特権を細分化して割り当てることができる。たとえば、ファイル共有サービスBoxには、管理ユーザ、共同管理ユーザ、およびグループ管理ユーザを定義するアクセス制御モデルがある。この例では、管理ユーザは、ユーザおよびグループの管理、組織のすべてのファイルおよびフォルダの表示および編集、組織内の任意のユーザのユーザアカウントへのログイン、組織の設定の編集、ならびにレポートの実行またはレポートへのアクセスを行うことができる。共同管理ユーザは管理ユーザと同じ操作を実行することができるが、管理ユーザの許可を変更することはできない。グループ管理ユーザは、組織内のグループを管理し、これらのユーザが管理するグループにユーザを追加することができ、グループに割り当てられる新たなユーザを作成することができ、グループにアクセス権を割り当てることができるが、それ以外の場合はグループ外的能力はない。

【0022】

管理ユーザは通常のユーザよりも高い特権を有するため、管理ユーザのアクティビティには通常のユーザのアクティビティよりも高いレベルの監視が必要になる場合がある。さまざまな理由により、より高度な精査が必要になる場合がある。たとえば、コンプライアンス監査人は、クラウドサービスがさまざまな金融機密保護法に準拠していることを確認するために、管理アクティビティの監査証拠を要求することができる。別の例として、不正な管理者を特定することで、組織の機密データの誤用や改ざんを防ぐことができる。別の例として、管理ユーザアカウントは、管理ユーザアカウントで利用可能なより高い特権を取得しようとするネットワーク攻撃者によって頻繁に標的にされる。

【0023】

しかしながら、特定のサービスの特権ユーザを識別することは簡単ではない場合がある。企業ネットワーク内で実行される企業アプリケーションを用いると、組織はそれらのアプリケーションを組織の内部コーポレート識別管理システムと統合することができる場合がある。これにより、組織は企業アプリケーションのユーザ、およびユーザに割り当てられた特権を管理することができる。しかしながら、クラウドサービスの場合、ユーザおよびユーザの権限の管理は、企業ネットワークの外部のクラウドサービス内で処理される。さらに、各クラウドサービスは、クラウドサービスのユーザに特権を付与するために、異なるモデルを用いる場合があり、ユーザを管理ユーザにする特権がクラウドサービスごとに異なり得る。したがって、クラウドサービスの特権ユーザを識別するための統一された定義がない場合がある。

【0024】

さらに、組織のユーザは、管理されていないデバイス（たとえば、組織が所有するデバイスではなく個人所有のデバイス）を用いてクラウドサービスを利用したり、および/または管理されていないネットワーク（たとえば、自宅、空港、ホテル、またはその他の企業ネットワーク外インターネット接続）からクラウドサービスにアクセスするかもしれない。このような状況では、ユーザのクラウドサービスの利用が組織のネットワークにセキュリティ侵害を引き起こし、組織がネットワーク攻撃に対して脆弱になる可能性がある。

【0025】

Imperva、Lgrhythem、Cyberark、Oracleなどのさまざまなベンダーの製品は、特権ユーザの監視を実行することができる。しかしながら、これらの製品では、特権ユーザを

10

20

30

40

50

事前に識別し、監視のために製品に入力する必要がある。クラウドサービスの特権ユーザは、その情報の追跡が綿密ではなかった可能性があるため、事前に知られていない可能性がある。さらに、管理ユーザは、新たな管理ユーザが組織のユーザ、自動化ツール、API、および/または悪意のあるユーザによって作成されて、時間とともに変化する可能性もある。同様に頻繁に発生する可能性があるのは、管理アカウントを作成および使用した人の組織での雇用が終わる可能性があるため、どのアカウントが管理アカウントであったかに関する知識が時間とともに失われる可能性があることである。

【0026】

さまざまな実現例において、クラウドサービスのセキュリティを監視および管理するためのセキュリティ管理ならびに制御システムには、所与のクラウドサービスの特権ユーザを識別するための自動化された手法を含めることができる。さまざまな例では、セキュリティ管理および制御システムはクラウドサービスからログファイルを取得することができる。ここではアクティビティログと呼ぶ。アクティビティログには、クラウドサービスの利用中に組織のユーザが実行したアクションが記録される。さまざまな例では、セキュリティ管理および制御システムは、クラウドサービスに関して特権があるアクティビティログ内のアクションを識別することができる。たとえば、セキュリティ管理および制御システムは、教師あり学習手法と教師なし学習手法を用いて、組織のユーザがクラウドサービスを利用する方法を記述するモデルを開発することができる。この例および他の例では、セキュリティ管理および制御システムは、アクティビティログのアクションを用いて特権ユーザを識別することができる。特権ユーザが識別されると、セキュリティ管理および制御システムは特権ユーザをより詳細に監視することができる。

【0027】

図1は、セキュリティ監視および制御システム102（本明細書では「セキュリティ管理システム」および「セキュリティシステム」とも呼ばれる）を含むコンピューティング環境100の例を示すブロック図を含む。セキュリティ監視および制御システム102は、クラウドサービスプロバイダ110によって提供されるサービス112a～112bを用いる組織130に脅威分析および救済を提供することができる。サービス112a～112bは組織130のネットワークの外部で管理されるため、組織130のネットワークセキュリティシステムは、サービス112a～112bの利用が組織130にセキュリティリスクを生じさせないことを保証できない場合がある。さまざまな例では、組織130のユーザは、ネットワーク150またはネットワークの組み合わせを介してサービス112a～112bにアクセスし、用いることができる。ネットワーク150は、例えば、公衆インターネットを含むことができる。組織130は、ネットワーク150を介してセキュリティ監視および制御システム102のサービスに同様にアクセスし、用いることができる。さまざまな例では、セキュリティ監視および制御システム102は、クラウドサービスプロバイダによって管理されるクラウドサービスとして記述することもできる。セキュリティ監視および制御システムの一例は、Oracle Corporationが提供する製品およびサービスであるOracle CASBである。

【0028】

サービスプロバイダは、コンピューティングサービスを他に提供するように構成されたハードウェアとソフトウェアとの集まりである。コンピューティングサービスには、たとえば、ハードウェアリソース、処理リソース、データストレージ、ハードウェアプラットフォーム、ソフトウェアプラットフォーム、および/またはさまざまなレベルの複雑さのアプリケーションなど、コンピューティングリソースが含まれる。場合によっては、サービスプロバイダは、プロバイダのサービスを有効にするハードウェアおよびソフトウェアを運用する。場合によっては、サービスプロバイダは別のサービスプロバイダのハードウェアおよびソフトウェアを用いる。たとえば、第1のサービスプロバイダはデータセンターの運営者となり、ソフトウェアホスティングサービスリソースを第2のサービスプロバイダにリースし、第2のプロバイダは組織のユーザに共同ワープロアプリケーションなどのアプリケーションを提供する。

10

20

30

40

50

【 0 0 2 9 】

さまざまな例において、サービスプロバイダはサブスクリプションモデルに従い、サービスの利用を他にリースする。この場合、リースは一定期間継続することができる。本明細書ではテナントとも呼ばれる加入者には、サービスプロバイダおよび/またはテナントのアカウントを与えることができ、それを通じてテナントはサービスを利用する。テナントが組織の場合、テナントはサービスプロバイダのアカウント（ここではテナントアカウントまたは企業アカウントと呼ばれる）を有することができ、組織のユーザはサービスプロバイダおよび/または特定のサービスの個々のユーザアカウントを有することができる。場合によっては、ユーザアカウントはテナントのアカウントに関連付けられており、テナントアカウントはユーザアカウントを制御および管理することができる。

10

【 0 0 3 0 】

いくつかの例では、サービスプロバイダは、加入者からの直接報酬なしでサービスを提供することができる。たとえば、サービスプロバイダは無料の電子メールアプリケーションを提供し、広告などの他の手段を通じてサービスの収益を得ることができる。この例および他の例では、加入者はリースなしで、場合によっては無期限にサービスプロバイダのアカウントを取得することができる。

【 0 0 3 1 】

図 1 の例では、サービスプロバイダ 1 1 0 は、ネットワーク 1 5 0 を介してサービスプロバイダ 1 1 0 の顧客にアクセス可能な 2 つのサービス 1 1 2 a ~ 1 1 2 b を提供している。サービス 1 1 2 a ~ 1 1 2 b は、他のサービスの中でも、例えば、インフラストラクチャ、プラットフォーム、ネットワーク、およびアプリケーションを含むことができる。いくつかの例では、2 つのサービス 1 1 2 a ~ 1 1 2 b は相互に関連付けられることができ、たとえば、データを共有したり、シングルサインオンメカニズムを介してアクセスしたりすることができる（たとえば、1 セットのユーザクレデンシャルにより、ユーザーは、各サービスで個別に認証する必要なく、両方のサービス 1 1 2 a ~ 1 1 2 b にアクセスできる）。いくつかの例では、サービス 1 1 2 a ~ 1 1 2 b は完全に独立して動作する。例えば、第 1 のサービス 1 1 2 a は銀行業務アプリケーションであり得、第 2 のサービス 1 1 2 b はソフトウェア開発プラットフォームであり得る。この例では、サービスプロバイダ 1 1 0 は、別個の無関係な製品として 2 つのサービス 1 1 2 a ~ 1 1 2 b を提供しているてもよい。

20

30

【 0 0 3 2 】

サービスプロバイダ 1 1 0 の顧客は、個々のユーザおよび/または組織を含むことができ、組織は複数のユーザを含むことができる。組織とは、人とリソースとを結び付けて共通の目的を果たすエンティティである。組織の例には、とりわけ企業、大学、公益事業体、政府機関が含まれる。組織の人々は、組織内においてユーザとして表すことができる。コンピューティング環境 1 0 0 の文脈においては、ユーザは、組織のコンピューティングシステムにアクセスして用いるために用いることができるユーザ名、ユーザ識別子、ユーザアカウント、クレデンシャル（例えば、パスワード、セキュリティトークン、またはクレデンシャルの別の形態）、および/または他のデータを含むことができるデジタルエンティティである。1 人以上を同じユーザアカウントに関連付けることができ、または 1 人が複数のユーザアカウントを有することができる。たとえば、ネットワーク管理チームのあるメンバーは、ネットワーク管理チームの他のメンバーが用いるのと同じ管理ユーザアカウントを用いることができ、一方で、その 1 人のネットワーク管理者のみが用いるユーザアカウントも有することができる。いくつかの例では、ユーザのアクティビティは、人間によってドライブされる代わりに、またはそれに加えて、自動化されたプログラム（「ボット」など）によってドライブされ得る。

40

【 0 0 3 3 】

さまざまな例において、組織のユーザおよび組織のリソースは共通の管理下にあり、同じセキュリティ境界内で動作することができる。例えば、図 1 の例では、組織 1 3 0 のリソースは、企業ネットワーク 1 0 4 およびいくつかのクライアントデバイス 1 0 6 a ~ 1 0

50

6 cを含む。クライアントデバイス106 a~106 cは、例えば、デスクトップコンピュータ、ラップトップコンピュータ、スマートフォン、タブレット、および他のコンピューティングデバイスを含むことができる。いくつかの例では、クライアントデバイス106 a~106 cは組織130の従業員が個人的に所有することができるが、これらのデバイスは、企業ネットワーク104に接続される一方で、組織130によって管理される。企業ネットワーク104は、サーバ、プリンタ、ルータ、スイッチ、および他のネットワークデバイスなどの他のコンピューティングデバイスも含むことができる。組織130のリソースは、データ（例えば、ドキュメント、ウェブページ、ビジネスデータ、ユーザデータなど）、データベース、アプリケーション、処理容量、ストレージ容量、ネットワーク容量、および他のハードウェア、ソフトウェア、またはデジタルリソースも含むことができる。

10

【0034】

さまざまな例では、組織130のクライアントデバイス106 a~106 bは、企業ネットワーク104に接続され、その中で動作することができる。例えば、クライアントデバイス106 a~106 bは、企業ネットワーク104内のスイッチに接続することができ、これにより、クライアントデバイス106 a~106 bは企業ネットワーク104のファイアウォール108の背後に配置される。ファイアウォール108の背後にあることにより、クライアントデバイス106 a~106 bは企業ネットワーク104のセキュリティ境界内に配置される。セキュリティ境界内では、ファイアウォール108ならびにセキュリティ情報およびイベント管理（SIEM）アプリケーション、侵入検知システム（IDS）、侵入防止システム（IPS）などのネットワークセキュリティシステムが、ネットワークの脅威から企業ネットワーク104におけるデバイスを守ることができる。

20

【0035】

さまざまな例では、組織130のクライアントデバイス106 cは、企業ネットワーク104の外部から組織130に接続することができる。例えば、クライアントデバイス106 cは、インターネットサービスプロバイダ（ISP）を介してネットワーク150に接続することができ、ネットワーク150を介して、クライアントデバイス106 cは企業ネットワーク104の仮想プライベートネットワーク（VPN）または同様のメカニズムに接続することができてもよい。一旦VPNに接続されると、クライアントデバイス106 cは、企業ネットワーク104の一部として動作し、企業ネットワーク104のセキュリティ境界によって防御されることができる。しかしながら、この例では、クライアントデバイス106 cは、クライアントデバイス106 cと企業ネットワーク104との間にあるネットワーク150に同時に接続しているため、ネットワーク150から生じる可能性のあるセキュリティリスクに依然としてさらされ得る。さらに、いくつかの例では、クライアントデバイス106 cは、サービスプロバイダ110のサービス112 a~112 bにアクセスすることができるようにするために企業ネットワーク104に接続する必要がない場合がある。

30

【0036】

さまざまな例では、組織130のユーザは、組織130のリソース、および組織130が所有し組織130が組織のメンバーに提供することができるクライアントデバイス106 a~106 cを介して組織130が加入するサービス112 a~112 bを利用することができる。さまざまな例では、メンバーは組織130の任意のクライアントデバイスを使用でき、複数のクライアントデバイスを用いることができてもよい。例えば、企業ネットワーク104は、任意のメンバーがログインしてメンバーのユーザアカウントにアクセスするために用いることができるユーザワークステーションを含むことができる。別の例として、メンバーはラップトップコンピュータおよびスマートフォンにアクセスすることができ、いずれかのデバイスにログインして、同じユーザアカウントにアクセスすることができる。代替的または追加的に、メンバーは、メンバーが個人的に所有するクライアントデバイスを用いて、組織のネットワークに接続して、組織のリソースを利用することができる。

40

50

【 0 0 3 7 】

上述のように、サービスプロバイダのサービス 1 1 2 a ~ 1 1 2 b の加入者は、組織 1 3 0 に所属していないか、またはその一部ではない個人でもあり得る。その個人は、ネットワーク対応クライアントデバイス 1 0 6 d にアクセスを有してもよく、それを介してサービス 1 1 2 a ~ 1 1 2 b にアクセスすることができる。個人は、個人がネットワーク 1 5 0 にアクセスすることができるようにする I S P のユーザアカウントを有してもよい。代替的または追加的に、個人はサービス 1 1 2 a ~ 1 1 2 b の 1 つ以上のユーザアカウントを有してもよい。しかしながら、個人はクライアントデバイス 1 0 6 d を用いて企業ネットワーク 1 0 4 に接続することはできず、なぜならば、個人が、組織 1 3 0 のユーザアカウント、またはユーザアカウントが企業ネットワーク 1 0 4 に接続するための許可を得るためのクレデンシャルを有していないからである。

10

【 0 0 3 8 】

さまざまな例において、個人および組織は、異なるサービスプロバイダが提供するサービスに加入することができる。たとえば、組織は 1 つのサービスプロバイダからのメールサービス（例：Google（登録商標）からのGmail）と別のサービスプロバイダのファイル共有サービス（Dropboxなど）とを用いることができる。この例および他の例では、それぞれのサービスをサポートするための別個のコンピューティングシステムを有し、異なるエンティティによって制御されることを含むなど、異なるサービスプロバイダは無関係であることができる。いくつかの例では、ユーザは、各サービスプロバイダおよび/または各サービスプロバイダのサービスの、別々のアカウントを有することができる。一部の例では、ユーザは共通のユーザアカウントを用いて、異なるサービスプロバイダのサービスにアクセスすることができてよい。

20

【 0 0 3 9 】

いくつかの例では、クラウドサービスは、組織 1 3 0 内での利用について承認または未承認とされることができる。承認サービスとは、組織 1 3 0 が利用を承認したサービスである。承認には、たとえば、サービスが安全であることを保証するための認証プロセスを通じてサービスを審査すること、サービスプロバイダ 1 1 0 とのサービス契約を確立すること、承認されたサービスプロバイダのリストにサービスプロバイダ 1 1 0 を配置すること、サービスプロバイダ 1 1 0 を周知の信頼することができるサービスプロバイダとして識別すること、および/または組織 1 3 0 のユーザのためのサービスのユーザアカウントの生成を制御すること、その他のアクティビティが含まれ得る。例えば、サービスプロバイダ 1 1 0 は、サービスプロバイダ 1 1 0 によって「信頼することができる」サービスプロバイダとして分類されることができる。いくつかの例では、組織 1 3 0 は、他のサービスプロバイダを「信頼できない」として分類するか、信頼リストにないすべてのサービスプロバイダを信頼できないとして分類することができる。未承認サービスとは、組織が明確に承認していない可能性があり、ユーザがユーザ自身の裁量で用いているサービスである。例えば、ユーザは、組織 1 3 0 が特に承認していないファイル共有サービスを利用しているかもしれず、組織 1 3 0 はおそらくファイル共有サービスが利用されていることを認識していない。

30

【 0 0 4 0 】

いくつかの例では、サービスプロバイダ 1 1 0 のサービス 1 1 2 a ~ 1 1 2 b は、組織 1 3 0 内から実行でき組織 1 3 0 内での使用が承認されていてもよいアプリケーションを介して実行またはアクセスすることができる。例えば、組織 1 3 0 は、承認されたウェブブラウザアプリケーションを有することができ、それを介して、ユーザはファイル共有サービスまたはデータベースサービスなどのサービスにアクセスすることができる。この例および他の例では、ウェブブラウザアプリケーションを内部アプリケーションと呼ぶことができる。いくつかの例では、内部アプリケーションは、たとえば、クラウドサービス 1 1 2 a ~ 1 1 2 b が組織 1 3 0 内のデータ、ユーザアカウント情報、または他の情報にアクセスすることができるようにするなど、クラウドサービス 1 1 2 a ~ 1 1 2 b と連携して動作することができる。内部アプリケーションは組織 1 3 0 内で（たとえば、組織 1 3 0

40

50

のクライアントデバイス 106 a ~ 106 c 上で) 実行されているため、組織 130 は内部アプリケーションの使用を監視および制御することができる。しかしながら、組織 130 は、内部アプリケーションを介するサービスプロバイダ 110 のサービス 112 a ~ 112 b のユーザの利用を認識していないか、または監視することができないかもしれない。

【0041】

いくつかの例では、ユーザは、サードパーティのサービスプロバイダ 114 を介してサービスプロバイダ 110 のサービス 112 a ~ 112 b にアクセスすることができる。例えば、ユーザは最初にサードパーティのサービスプロバイダ 114 によって提供されるサービス 116 にアクセスし、このサービス 116 を介して、別のサービスプロバイダ 110 のサービス 112 b にアクセスすることができる(ここでは破線矢印で示す)。サードパーティサービスプロバイダ 114 のサービス 116 は、例えば、ユーザが他のクラウドサービスプロバイダのアプリケーションおよびサービスを見つけてアクセスすることを可能にするポータルサービスであり得る。いくつかの例では、サードパーティのサービスプロバイダのサービス 116 は、ネットワーク 150 を介して他のサービスへのアクセスを提供する(たとえば、他のサービス 112 b のためのサービス 116 との間のデータは、ネットワーク 150 を介して他のサービス 112 b との間で送受信される)が、そのアクセスは、ユーザの視点からは、直接的なように見え得る。いくつかの例では、サービス 116 は、ユーザが他のサービス 112 b とのサブスクリプションを確立することを可能にし、その後、ユーザは、サードパーティサービスプロバイダ 114 のサービス 116 にアクセスする必要なく、他のサービス 112 b に直接アクセスする。

【0042】

クラウドサービス 112 a ~ 112 b の利用は、サービス 112 a ~ 112 b の加入者にセキュリティリスクを生じさせる可能性がある。たとえば、組織内で動作しているハードウェア、プラットフォーム、およびソフトウェアは、ほとんどの場合、組織によって制御され、物理的な障壁および/またはネットワークセキュリティツールなどを用いて組織によって保護される。しかしながら、クラウドサービス 112 a ~ 112 b は、組織 130 の外部および組織 130 による直接制御の外部で動作する。組織 130 は、サービス 112 a ~ 112 b を用いるときにユーザが実行するアクティビティに対する可視性、またはユーザが実行するアクションを制御する能力をほとんどまたは全く有さない場合がある。さらに、組織 130 は、疑わしいデータまたは無許可のユーザをサービス 112 a ~ 112 b 経由で組織 130 に入れさせる、もしくはサービス 112 a ~ 112 b の利用を介して組織のデータを組織 130 から出させるユーザアクションを、監視または制御する能力をほとんどまたはまったく有さない場合がある。

【0043】

さまざまな実現例において、セキュリティ監視および制御システム 102 は、クラウドサービス 112 a ~ 112 b の加入者にネットワーク脅威検出および救済サービスを提供することができる。さまざまな実現例では、セキュリティ監視および制御システム 102 は、サービス 112 a ~ 112 b の利用を分析し、組織または個々の加入者に対する脅威となり得るアクティビティを識別することができる。いくつかの実現例では、セキュリティ監視および制御システム 102 は、さらに、救済アクションを提案および/または自動的に実行して、脅威を隔離または停止することができる。いくつかの例では、セキュリティ監視および制御システム 102 によって実行される分析は、ユーザアクティビティの正常および/または異常な挙動のモデルを判定すること、およびそれらのモデルを用いて不審なアクティビティのパターンを検出することを含み得る。いくつかの例では、セキュリティ監視および制御システム 102 は、異なるサービスおよび/または異なるサービスプロバイダからのデータを同時に分析することができる。これらの例では、セキュリティ監視および制御システム 102 は、異なるサービスで実行されるアクションが発生したときにのみ明らかな疑わしいアクティビティを検出することができてよい。さまざまな例において、セキュリティ監視および制御システム 102 は、疑わしいアクティビティが検出されたサービスプロバイダで、または他のサービスプロバイダでアクションが取られる必要

があるかもしれないと分析が判断したときに異なるサービスプロバイダで実行することができる救済措置を判断することができる。

【 0 0 4 4 】

いくつかの例では、セキュリティ管理および制御システム 1 0 2 は、組織 1 3 0 のコンピューティング環境に統合することができる。たとえば、セキュリティ監視および制御システム 1 0 2 は、企業ネットワーク 1 0 4 内のサーバ上で、組織 1 3 0 のファイアウォール 1 0 8 の背後で実行することができる。これらの例では、セキュリティ管理および制御システム 1 0 2 は、組織のネットワーク管理者、および / またはセキュリティ管理および制御システム 1 0 2 の開発者に関連する人員によって管理することができる。

【 0 0 4 5 】

代替的または追加的に、さまざまな例では、セキュリティ監視および制御システム 1 0 2 の機能は、個人および組織へのサービスとして提供することができる。例えば、セキュリティ監視および制御システム 1 0 2 のネットワークセキュリティサービスは、ウェブベースのクラウドサービスとして、および / またはサービスとしてのソフトウェア (S a a S) モデルの下で提供され得る。これらおよび他の例では、顧客はセキュリティ監視および制御システム 1 0 2 によって提供されるアプリケーションを使用でき、アプリケーションはさまざまな脅威検出および救済機能を提供する。サービスプロバイダ 1 1 0 のサービス 1 1 2 a ~ 1 1 2 b と同様に、個人および組織は、セキュリティ監視および制御システム 1 0 2 によって提供されるセキュリティサービスに加入することができる。いくつかの例では、組織 1 3 0 のグループユーザが管理ユーザとして指定され、組織 1 3 0 のセキュリティを監視する際にセキュリティ監視および制御システム 1 0 2 によって実行される操作を管理することができる。これらのユーザは、セキュリティ管理および制御システム 1 0 2 によって生成されるレポートなどのアクセス情報、ならびにセキュリティ管理および制御システム 1 0 2 によって提案された救済アクションを実行する能力などの機能を有する。

【 0 0 4 6 】

さまざまな実現例において、セキュリティ監視および制御システム 1 0 2 は、コンピューティングシステムを用いて実現することができる。これらの実現例では、コンピューティングシステムは 1 つ以上のコンピュータおよび / またはサーバ (たとえば、1 つ以上のアクセスマネージャサーバ) を含むことができ、それらは、汎用コンピュータ、専用サーバコンピュータ (デスクトップサーバ、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など)、サーバファーム、サーバクラスタ、分散サーバ、またはその他の適切なコンピューティングハードウェアの構成および / もしくは組み合わせであってもよい。セキュリティ監視および制御システム 1 0 2 は、ハイパーテキストトランスポートプロトコル (H T T P) サーバ、ファイルトランスポートサービス (F T P) サーバ、共通ゲートウェイインターフェース (C G I) サーバ、J a v a (登録商標) サーバ、データベースサーバ、その他のコンピューティングシステムを含むオペレーティングシステムおよび / またはさまざま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してもよい。データベースサーバの例には、Oracle、Microsoft、およびその他から市販されているものが含まれる。セキュリティ監視および制御システム 1 0 2 は、ハードウェア、ファームウェア、ソフトウェア、またはハードウェア、ファームウェアおよびソフトウェアの組み合わせを用いて実現することができる。

【 0 0 4 7 】

さまざまな実現例では、セキュリティ監視および制御システム 1 0 2 は、少なくとも 1 つのメモリ、1 つ以上の処理ユニット (たとえば、プロセッサ)、および / またはストレージを含み得る。処理ユニットは、ハードウェア (集積回路など)、コンピュータ実行可能命令、ファームウェア、またはハードウェアと命令との組み合わせで適切に実現することができる。いくつかの例では、セキュリティ監視および制御システム 1 0 2 は、いくつかのサブシステムおよび / またはモジュールを含むことができる。セキュリティ監視および制御システム 1 0 2 内のサブシステムおよび / またはモジュールは、ハードウェア、ハー

10

20

30

40

50

ドウェア上で実行されるソフトウェア（例えば、プロセッサによって実行可能なプログラムコードもしくは命令）、またはそれらの組み合わせで実現され得る。いくつかの例では、ソフトウェアは、メモリ（たとえば、非一時的なコンピュータ可読媒体）、メモリデバイス、または他の何らかの物理メモリに格納でき、1つ以上の処理ユニット（たとえば、1つ以上のプロセッサ、1つ以上のプロセッサコア、1つ以上のグラフィックスプロセスユニット（GPU）など）によって実行されてもよい。処理ユニットのコンピュータ実行可能命令またはファームウェア実現例は、任意の適切なプログラミング言語で記述されたコンピュータ実行可能命令またはマシン実行可能命令を含むことができ、本明細書で説明するさまざまな操作、機能、方法、および/またはプロセスを実行することができる。メモリは、処理ユニットでロード可能および実行可能なプログラム命令を、これらのプログラムの実行中に生成されたデータとならんで格納してもよい。メモリは、揮発性（ランダムアクセスメモリ（RAM）など）および/または不揮発性（読み取り専用メモリ（ROM）、フラッシュメモリなど）であってもよい。メモリは、コンピュータ可読記憶媒体などの任意のタイプの永続的記憶装置を用いて実現されてもよい。いくつかの例では、悪意のあるコードを含む電子通信からコンピュータを保護するようにコンピュータ可読記憶媒体を構成することができる。コンピュータ可読記憶媒体は、プロセッサ上で実行されるとセキュリティ監視および制御システム102の動作を実行する命令を格納することができる。

10

【0048】

さまざまな実現例において、セキュリティ監視および制御システム102は、セキュリティ監視および制御システム102の異なる機能を実現するさまざまなモジュールを含むことができる。図1の例では、これらのモジュールは、スキャナ174、パターン分析部176、学習システム178、データアクセス部182、データ分析システム136、情報ハンドラシステム138、マッピングジェネレータ170、制御マネージャ172、ログ収集システム134、およびインターフェース120を含む。セキュリティ監視および制御システム102は、セキュリティ監視および制御システム102が用いるさまざまなデータを格納するストレージ122をさらに含む。いくつかの例では、セキュリティ監視および制御システム102は、セキュリティ監視および制御システム102が必要とする可能性がある追加のデータを格納することができる追加のデータストア180に接続することもできる。

20

30

【0049】

さまざまな例では、セキュリティ監視および制御システム102のストレージ122は、テナント構成情報124、セキュリティ情報126、ドメイン情報128、およびアプリケーション情報132を格納する1つ以上のデータストアであり得る。さまざまな例において、ストレージ122は、1つ以上のデータベース（例えば、ドキュメントデータベース、リレーショナルデータベース、または他のタイプのデータベース）、1つ以上のファイルストア、1つ以上のファイルシステム、またはデータを格納するためのシステムの組み合わせを含むことができる。

【0050】

さまざまな例において、テナント構成情報124（「テナント構成情報」）は、テナントおよびテナントアカウント、ならびに各テナントアカウントに関連付けられたユーザアカウントの構成情報を含むことができる。例えば、組織130がセキュリティ管理および制御システム102のサービスに加入する場合、組織は、組織の、クラウドサービスプロバイダ110のテナントアカウントを識別する情報を、セキュリティ管理および制御システム102に提供することができる。この例では、セキュリティ管理および制御システム102は、テナント構成情報124にテナントアカウント情報を格納することができる。場合によっては、組織130は、サービスプロバイダ110のユーザアカウントのリストを提供することもでき、これもテナント構成情報124に格納することができる。代替的または追加的に、いくつかの例では、セキュリティ管理および制御システム102は、サービスプロバイダ110に問い合わせ、ユーザアカウントを判断することができる。いく

40

50

つかの例では、セキュリティ監視および制御システム 102 は、テナントに関連付けられたユーザのアクティビティに関する情報を取得するためなど、テナントアカウントとテナントのユーザのユーザアカウントと間の関連付けをさまざまな方法で用いることができる。

【0051】

いくつかの例では、組織 130 は、認証情報をセキュリティ管理および制御システム 102 に提供することもでき、認証情報を用いて、サービスプロバイダ 110 のサービス 112 a ~ 112 b にログインまたはアクセスすることができる。さまざまな例において、セキュリティ管理および制御システム 102 は、認証情報を用いて、組織の、サービスプロバイダ 110 のテナントアカウント 130 にアクセスすることができる。承認情報は、たとえば、トークン（OAuth トークンなど）、ユーザ名とパスワード、または別の形式のクレデンシャルをとることができる。いくつかの例では、組織 130 は、承認とともに許可または特権を指定することができる、セキュリティ管理および制御システム 102 が組織のテナントアカウントに対して有するアクセスのレベルを定義することができる。例えば、組織 130 は、セキュリティ管理および制御システム 102 はサービスプロバイダ 110 によって提供されるサービスのセキュリティ設定を変更することができるが、セキュリティ管理および制御システム 102 は新たなユーザアカウントを生成またはユーザアカウントを削除できないことを指定することができる。

【0052】

さまざまな例において、テナント構成情報 124 は、例えばセキュリティ、サービスプロバイダ 110 のサービス 112 a ~ 112 b にアクセスするための設定、ログ設定、および/またはアクセス設定（例えば、セキュリティポリシー、セキュリティ設定、ホワイトリストとブラックリストなど）など、組織 130 に関する他の情報を格納することができる。いくつかの例では、組織 130 は、レベルに基づいてサービスのセキュリティ設定を指定することができる。たとえば、高レベルのセキュリティ設定では、ユーザパスワードを「強力」にする必要があってもよい。つまり、パスワードには、大文字、小文字、数字、記号などのさまざまな文字を含める必要がある。同様に、さまざまなレベルのセキュリティ設定では、セッションの非アクティビティタイマーをより長い時間またはより短い時間に設定することができる。たとえば、非アクティビティタイマーが切れると、ユーザのセッションは自動的に終了する。

【0053】

いくつかの例では、ストレージ 122 は、セキュリティ監視および制御システム 102 によって実行されるセキュリティ分析を含むセキュリティ情報 126（「セキュリティ情報」）を含むことができる。いくつかの例では、セキュリティ情報 126 は、セキュリティ監視および制御システム 102 の異なる顧客に対する個別のエントリを含むことができる。いくつかの例では、セキュリティ情報 126 は履歴データ：必要なときに参照することができる過去（例えば、先月、過去 3 か月、昨年、または他の過去の期間）の分析の結果を含む。いくつかの例では、セキュリティ情報 126 は、過去のセキュリティインシデントの記録、過去のセキュリティインシデントが実際のインシデントまたは誤検知であったかどうかの判定、過去のインシデントに対して行われた救済アクションの記録、および/または救済アクションを実行した結果、その他のデータをさらに含むことができる。いくつかの例では、セキュリティ情報 126 は、たとえば、サードパーティの脅威インテリジェンスのアグリゲータおよびディストリビュータから取得したネットワーク脅威インテリジェンスデータをさらに含むことができる。

【0054】

いくつかの例では、ストレージ 122 は、サービスプロバイダ 110 および他のサービスプロバイダに関するドメイン情報 128（「ドメイン情報」）を含むことができる。ドメイン情報 128 は、例えば、サービスプロバイダ 110 のネットワークアドレスまたは位置、サービスプロバイダ 110 の所有者または運営者（例えば、サービスプロバイダ 110 を所有および/または運営する個人または組織）の識別情報、ならびにサービスプロバイダ 110 の素性を確認するための情報を含むことができる。ドメイン情報 128 は、例

10

20

30

40

50

えば、サービスプロバイダ 110 に問い合わせること、サービスプロバイダ 110 に証明書を要求すること、および/またはサービスプロバイダのISPもしくはサービスプロバイダのホスティングサービスに情報を要求することにより、取得することができる。

【0055】

いくつかの例では、ストレージ 122 は、サービスプロバイダのアプリケーションまたはサービスのユーザを記録するアプリケーション情報 132 (「アプリ情報」) を含むことができる。アプリケーション情報 132 は、例えば、組織 130 から収集されたデータログおよび/またはサービスプロバイダ 110 から取得されたアクティビティログを含むことができる。アプリケーション情報 132 は、例えば、サービスプロバイダ 110 のサービス 112a ~ 112b の利用中に実行されるアクション、アクションを実行したユーザの識別、アクションが実行されたときのタイムスタンプ、ユーザがアクションを実行したときのユーザについてのネットワークのネットワーク識別および/または地理的位置、アクションによって影響を受けるリソース、ならびにサービス 112a ~ 112b の利用に関連する他の情報を記録することができる。

10

【0056】

さまざまな実現例では、セキュリティ監視および制御システム 102 は、1つ以上のデータストア 180 に結合または通信することができる。データストア 180 は、メモリストレージデバイスまたは他の非一時的なコンピュータ可読記憶媒体などの任意のタイプの永続ストレージデバイスを用いて実現され得る。いくつかの例では、データストア 180 は、1つ以上のデータベース (たとえば、ドキュメントデータベース、リレーショナルデータベース、または他のタイプのデータベース)、1つ以上のファイルストア、1つ以上のファイルシステム、またはそれらの組み合わせを含むかまたは実現することができる。データストア 180 は、サービスプロバイダシステムによって提供されるサービスによって実現され、および/またはそのようなサービスとしてアクセス可能であってもよい。データストア 180 は、サービスまたはサービスのサービスプロバイダに関連するデータを要求するためのインターフェースを含んでもよい。

20

【0057】

いくつかの実現例では、セキュリティ監視および制御システム 102 は、セキュリティ監視および制御システム 102 が分析を実行することができるデータを取得するための操作を実行するログ収集システム 134 を含むことができる。さまざまな例において、セキュリティ監視および制御システム 102 は、脅威分析を行うために異なるタイプのデータまたはデータソースを用いることができる。例えば、セキュリティ監視および制御システム 102 は、サービス 112a ~ 112b が利用されるクライアントデバイス 106a ~ 106c を監視することにより取得されたデータ、および/またはルータもしくはファイアウォール 108 などの組織のネットワーク内のポイントを監視することにより取得されたデータを用いることができる。本明細書では、クライアントデバイスから、または組織のネットワーク内で取得されたデータは、ネットワークデータと呼ばれる。ネットワークデータを取得するために、いくつかの例では、監視エージェントをクライアントデバイス 106a ~ 106c および/または組織のネットワークのネットワークインフラストラクチャに配置することができる。これらの例では、監視エージェントは、ユーザがクラウドサービスを利用する際のユーザアクティビティをキャプチャすることができる。

30

40

【0058】

別の例として、セキュリティ監視および制御システム 102 は、サービスプロバイダ 110 からのデータログを用いることができる。さまざまな例では、サービスプロバイダ 110 は、サービスプロバイダ 110 のサービス 112a ~ 112b が利用されるときにユーザアクティビティを記録することができる。例えば、サービスプロバイダ 110 は、ユーザがサービスにログインした時間、ユーザがログインするときのユーザのネットワークおよび/または地理的位置、ユーザがサービスを利用するときユーザによって実行されるアクション、アクションによって影響を受けるリソース、ならびにサービスの利用に関連するその他の情報を記録することができる。ここでは、サービスプロバイダからのデータ

50

をアクティビティデータまたはアクティビティログと呼ぶ。

【 0 0 5 9 】

次の例は、サービスプロバイダから取得することができるアクティビティデータの例を示す。以下は、サービスプロバイダから取得することができるアクティビティデータ（監査ログレコードなど）の第 1 の例である。

【 0 0 6 0 】

【 数 1 】

```
“entries”: [  
  {  
    “source”: {  
      “type”: “user”,  
      “id”: “222853877”,  
      “name”: “Sandra Lee”,  
      “login”: “sandra@company.com”  
    },  
    “created_by”: {  
      “type”: “user”,  
      “id”: “222853866”,  
      “name”: “Mike Smith”,  
      “login”: “mike@company.com”  
    },  
    “created_at”: “2016-12-02T011:41:31-08:00”,  
    “event_id”: “b9a2393a-20cf-4307-90f5-004110dec233”,  
    “event_type”: “ADD_LOGIN_ACTIVITY_DEVICE”,  
    “ip_address”: “140.54.34.21”,  
    “type”: “event”,  
    “session_id”: null,  
    “additional_details”: null  
  }  
]
```

【 0 0 6 1 】

以下は、サービスプロバイダから取得することができるアクティビティデータ（共有ファイル監査ログレコードなど）の第 2 の例である。

【 0 0 6 2 】

【 数 2 】

```

“entries”: [
{
  “type”: “event”,
  “source”: {
    “parent”: {
      “type”: “folder”,
      “id”: “0”,
      “name”: “All Files”
    },
    “item_name”: “financial2017Q1.doc”,
    “item_type”: “file”,
    “item_id”: “159004949136”
  },
  “additional_details”: {
    “service_name”: “File Sharing App”
  },
  “event_type”: “SHARE”,
  “ip_address”: “140.191.225.186”,
  “event_id”: “234d2f55-99d0-4737-9c3b-1a5256fe7c67”,
  “created_at”: “2016-12-12T20:28:02-07:00”,
  “created_by”: {
    “type”: “user”,
    “id”: “238746411”,
    “name”: “John Smith”,
    “login”: “john@company.com”
  }
}
}

```

【 0 0 6 3 】

以下は、サービスプロバイダから取得することができるアクティビティデータ（監査レコードなど）の第3の例である。

【 0 0 6 4 】

【 数 3 】

```

{
  "Records": [
    {
      "eventVersion": "1.03",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "111122225533",
        "arn": "arn:aws:iam::111122223333:user/john",
        "accountId": "111122223335",
        "accessKeyId": "AKIAIOSFODNN7JOHN",
        "userName": "john"
      },
      "eventTime": "2016-12-26T20:46:31Z",
      "eventSource": "s3.amazonaws.com",
      "eventName": "PutBucket",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "[]",
      "requestParameters": {
        "bucketName": "myprodbucket"
      },
      "responseElements": null,
      "requestID": "47B8E8D397DCE7D6",
      "eventID": "cdc4b7ed-e171-4cef-975a-ad829d4123c7",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223344"
    }
  ]
}

```

【 0 0 6 5 】

以下は、サービスプロバイダから取得することができるアクティビティデータ（監査レコードなど）の第4の例である。

【 0 0 6 6 】

【 数 4 】

```

79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47efcde
myprodbucket [06/Feb/202017:00:01:57 +0000] 192.0.2.3 Mary DD6CC733AMARY
REST.GET.OBJECT s3-dg.pdf "GET /mybucket/financial2016Q4.pdf HTTP/1.1"
200 - - 4406583 4175428 "-" "S3Console/0.4" -

```

【 0 0 6 7 】

いくつかの例では、セキュリティ監視および制御システム 102 は、組織のネットワークまたはサービスプロバイダ 110 以外のネットワークソースからのサードパーティフィードなど、他のデータソースからのデータを用いることができる。他のネットワークソースの例には、ネットワークセキュリティデータアグリゲータおよびディストリビュータ、ソーシャルネットワーキングシステム、ニュース報告または集約システム、行政システム、評判システム、および他のシステムが含まれる。

【0068】

さまざまな実現例において、ログ収集システム 134 は、ネットワークデータおよび/またはアクティビティデータを取得するための操作を実行することができる。例えば、ログ収集システム 134 は、企業ネットワーク 104 に配置されたソフトウェアエージェントと通信して、これらのエージェントによって記録されたデータをネットワーク化するように構成することができる。この例では、ネットワークデータは、ユーザがサービスプロバイダ 110 のサービス 112a ~ 112b または別のサービスプロバイダのサービスを利用するときに生成されるネットワークトラフィックを含むことができる。いくつかの例では、ネットワークデータは、ユーザが組織 130 のリソースまたはウェブサイトなどのインターネット上のリソースなどの他のネットワークリソースを用いるときに生成されるネットワークトラフィックなど、他のネットワークトラフィックを含むことができる。別の例として、ログ収集システム 134 は、サービスプロバイダ 110 と通信して、サービスプロバイダ 110 からアクティビティログを取得するように構成することができる。サービスプロバイダ 110 は、例えば、ログ収集システム 134 がアクティビティログを要求することができるようにする API を有することができる。これらの例では、ログ収集システム 134 は、アクティビティログを要求するためにサービスプロバイダ 110 のテナントアカウントのクレデンシャルを用いることができてもよい。すなわち、ログ収集システム 134 は、サービスプロバイダ 110 のテナントを装い、テナントと同じ方法で要求を行うことができる。

【0069】

さまざまな実現例において、ログ収集システム 134 によって取得されたデータは、セキュリティ監視および制御システム 102 内のデータ分析システム 136 によって処理され得る。データ分析システム 136 は、ネットワークデータおよびアクティビティデータの分析を行って、他の動作の中でも、使用中のアプリケーションの発見、アクティビティパターン学習および認識、異常検出、ネットワーク脅威検出などの動作を実行することができる。データ分析システム 136 によって実行され得るこれらおよび他の操作は、以下でさらに論じられる。

【0070】

さまざまな実現例において、セキュリティ監視および制御システム 102 の情報ハンドラシステム 138 は、ストレージ 122 内のデータの管理を行ない、それは、例えば、データの格納、データの検索および取得、データの編成、データの更新などの操作を含む。いくつかの例では、情報ハンドラシステム 138 は、組織のユーザのリストおよびユーザに関するデータなどの情報を提供することができる管理ユーザなどの組織 130 のユーザからデータを受信する。ユーザに関するデータには、たとえば、ユーザの役割や権限を含めることができる。これらおよび他の例では、情報ハンドラシステム 138 は、ストレージ 122 内の適切なデータストアにおけるユーザデータの保存を管理することができる。

【0071】

さまざまな実現例において、マッピングジェネレータ 170 は、組織 130 またはセキュリティ監視および制御システム 102 の別の顧客のセキュリティ分析を実行する。例えば、マッピングジェネレータ 170 は、データ分析システム 136 の出力を処理し、サービス、ユーザ、テナント、またはサービス、ユーザ、および/もしくはテナントの組み合わせのセキュリティの尺度を計算することができる。いくつかの例では、マッピングジェネレータ 170 は、インターフェース 120 からデータを取得してセキュリティ分析を実行することができる。セキュリティ分析操作については、以下でさらに説明する。

【 0 0 7 2 】

さまざまな実現例において、セキュリティ監視および制御システム 1 0 2 内の制御マネージャ 1 7 2 は、組織 1 3 0 の代わりに機能して、組織のユーザによるサービスプロバイダ 1 1 0 のサービス 1 1 2 a ~ 1 1 2 b へのアクセスを管理することができる。さまざまな例では、制御マネージャ 1 7 2 は、複数のクラウドサービスまたは組織のユーザが利用するクラウドサービスにこのサービスを提供することができる。いくつかの例では、制御マネージャ 1 7 2 は、アクセスポリシーを用いて、サービス 1 1 2 a ~ 1 1 2 b へのユーザのアクセスを制御することができる。アクセスポリシーは、たとえば、サービスを利用できるまたはできないユーザのタイプまたはカテゴリ、サービスを利用できるまたはできない特定のユーザ、サービスを利用することができる時刻または曜日、サービスとの間で転送することができるデータの量、利用することができるデータ帯域幅、サービスの利用中に実行することができるまたはできないアクション、アクセスポリシーが適用されるユーザ、および/またはサービスに関するその他の制限または許可を定義することができる。さまざまな例において、制御マネージャ 1 7 2 は、セキュリティ管理および制御システム 1 0 2 のサービスに加入する各組織のポリシーのセットを維持することができる。いくつかの例では、制御マネージャ 1 7 2 は、異なるレベルのセキュリティでプリセットを提供することができ、プリセットを選択すると、1つ以上のサービスのセキュリティ構成が選択される。これらの例では、組織によるプリセットの選択は、組織のユーザがサービスを利用する能力の一部またはすべてに影響を与え得る。

10

【 0 0 7 3 】

いくつかの例では、制御マネージャ 1 7 2 は、組織 1 3 0 のセキュリティポリシーも維持することができる。セキュリティポリシーでは、検出された場合にセキュリティ違反もしくは注意が必要なイベントを構成するアクションまたはアクションのセットを定義することができる。一部の例では、ポリシーによってセキュリティ違反として定義されるアクションは、1つのサービスの利用を通じて発生する可能性がある。つまり、同じサービスを利用している間にすべてのアクションが実行されたことを意味する。いくつかの例では、複数のサービスの利用中にアクションが発生した可能性があり、サービスは1つのサービスプロバイダまたは複数のサービスプロバイダによって提供される。いくつかの例では、セキュリティポリシーは、ポリシーの違反が検出されたときに実行する1つ以上の救済アクションも定義することができる。救済アクションには、たとえば、違反の原因となったユーザ、組織 1 3 0 のネットワーク管理者、セキュリティ管理および制御システム 1 0 2 の管理者、ならびに/または別のエンティティへの通知の送信が含まれる。

20

30

【 0 0 7 4 】

いくつかの例では、救済には、サービスまたは複数のサービスへのアクセスの変更が含まれ得る。例えば、救済アクションには、特定のユーザによるサービスの利用の防止、または組織 1 3 0 のすべてのユーザによるサービスの利用の防止が含まれ得る。別の例として、救済アクションには、サービスの利用時に実行することができるアクションの制限が含まれ得る。いくつかの例では、救済アクションを実行することは、命令を企業ネットワーク 1 0 4 に送信することを含み得る。これらの例では、命令は、たとえば、クライアントデバイスまたはファイアウォール 1 0 8 などのネットワークインフラストラクチャデバイスを構成することができる。クライアントデバイス 1 0 6 a ~ 1 0 6 c および/またはネットワークインフラストラクチャデバイスは、いくつかの例では、制御マネージャ 1 7 2 が、デバイスと通信し、デバイスに対する変更を行なうことができるようにするソフトウェアエージェントを実行していてもよい。変更には、たとえば、ドメインまたはIPアドレスへのアクセスの制限、すべてのネットワークトラフィックのブロック、デバイスの無効化、デバイスへのその他の変更が含まれ得る。

40

【 0 0 7 5 】

いくつかの例では、救済アクションを実行することは、サービスプロバイダ 1 1 0 に命令を送信して、サービス 1 1 2 a ~ 1 1 2 b へのアクセスを変更することを含むことができる。これらの例では、救済アクションに、送信する命令の判定を含めることができる。例

50

例えば、制御マネージャ 172 は、サービスプロバイダ 110 および / またはサービスの API を検査して、サービスに所望の変更を引き起こすために実行することができる命令を識別することができる。この例では、API は、たとえば組織 130 のユーザまたはユーザのグループによるサービスへのアクセスを防止または制限することができる命令を定義することができる。別の例として、API は、サービスの特定の機能を無効化または有効化することができる命令を定義でき、無効化または有効化は組織 130 の 1 人以上のユーザに影響を与える。これらの例および他の例では、サービスの変更は、救済が関連付けられている組織のユーザに影響を与え、別の組織のユーザには影響しない。

【0076】

さまざまな実現例において、セキュリティ監視および制御システム 102 は、学習システム 178 を含むことができる。学習システム 178 は、セキュリティ監視および制御システム 102 によって収集されたデータにさまざまな機械学習アルゴリズムを適用することができる。次いで、データについて学習された情報は、例えば、データ分析システム 136 によって使用されて、サービスプロバイダ 110 によって提供されるサービスを利用する際のユーザアクティビティに関する判断を下すことができる。例えば、学習システム 178 は、組織のユーザの通常のまたは一般的な挙動のパターンを学習することができる。これらおよび他の例では、学習システム 178 は、学習システム 178 が学習したパターンをキャプチャするモデルを生成でき、それらは組織の他のデータとともにストレージ 122 に格納することができる。

【0077】

学習システム 178 をサポートするために、いくつかの実現例では、セキュリティ監視および制御システム 102 は、スキャナ 174 およびパターン分析部 176 を含む。これらの実現例では、スキャナ 174 は、例えば、特定のタイプの情報についてデータをスキャンすることができる。例えば、スキャナ 174 は、特定のユーザ、特定のユーザのグループ、特定のユーザのクラス、および / または特定のテナントに関連するすべてのユーザのアクティビティを抽出することができる。別の例として、スキャナ 174 は、特定のサービスまたはサービスのセットの利用に関連するアクティビティを抽出することができる。別の例として、スキャナ 174 は、特定のサービスプロバイダに関連するアクティビティを抽出することができる。さまざまな実現例では、パターン分析部 176 は、スキャナ 174 によって抽出されたデータを用いて、データ内のパターンを識別することができる。例えば、ユーザおよび / または組織は、反復的な態様または周期的な態様でサービスを用い得る。これらの例では、パターン分析部 176 は反復挙動を識別し、学習システム 178 に対するこれらの挙動パターンを識別することができる。

【0078】

いくつかの例では、セキュリティ監視および制御システム 102 内のデータアクセス部 182 は、サービスプロバイダと通信して、それらのサービスプロバイダからアクティビティデータを取得することができる。アクティビティデータは、ユーザアカウント、テナントアカウント、グループアカウント、または別のタイプのアカウントのものである。アクティビティデータは、サービス、特定のタイプのデータ（特定の属性のデータなど）、1 人以上のユーザ、またはサービス、サービスプロバイダ、属性、ユーザ、その他の要素の組み合わせについて取得することができる。いくつかの例では、データアクセス部 182 は、データを処理して、1 つ以上のサービス、特定のタイプのデータ（たとえば、特定の属性のデータ）、1 人以上のユーザ、またはそれらの組み合わせなど、1 つ以上の基準に関連するアクティビティを識別することができる。

【0079】

さまざまな実現例において、セキュリティ管理および制御システム 102 は、セキュリティ管理および制御システム 102 の顧客がセキュリティ管理および制御システム 102 のサービスを利用することができるインターフェース 120 を提供する。インターフェース 120 は、例えば、組織の管理ユーザがセキュリティ管理および制御システム 102 のサービスを構成することができるようにするコントロールパネルまたはダッシュボードを表

10

20

30

40

50

示することができるグラフィカルユーザインターフェース（GUI）を提供することができる。グラフィカルユーザインターフェースにより、管理ユーザは、さらに、サービスプロバイダ 110 のサービス 112 a ~ 112 b に関するユーザアクティビティのレポートを見ることができる。グラフィカルユーザインターフェースは、さらに、セキュリティイベントのレポートを提供し、救済アクションを提案し、および / またはセキュリティ管理および制御システム 102 が自動的に実行する救済アクションの結果について報告することができる。グラフィカルユーザインターフェースは、例えば、組織 130 のクライアントデバイス 106 a ~ 106 c で実行することができるソフトウェアアプリケーションとして実現することができる。代替的または追加的に、グラフィカルユーザインターフェースは、ウェブベースのインターフェース（ウェブサイトなど）として実現することができる。

10

【0080】

いくつかの例では、インターフェース 120 は、代替または追加として、セキュリティ管理および制御システム 102 によって提供されるサービスを組織 130 が管理することができる API を提供することができる。API は、たとえば、クラウドサービスの利用におけるユーザアクティビティに関するレポートのプル、セキュリティイベントに関するレポートのプル、救済アクションの命令の発行、ユーザアクティビティに関する統計の取得のためのアクション、および / またはセキュリティ管理および制御システム 102 のサービスに関連する他のアクションを定義することができる。インターフェース 120 の API により、組織は、例えば、セキュリティ管理および制御システム 102 の機能を組織 130 のセキュリティインフラストラクチャに統合することができる。

20

【0081】

さまざまな実現例において、セキュリティの監視および制御のためのシステムは、単一のハードウェアプラットフォームまたは相互に通信している複数のハードウェアプラットフォームに位置することができる複数のコンポーネントを含むことができる。コンポーネントは、セキュリティ管理および制御システム 102 の動作を実行するようにサーバもしくは他のコンピューティングデバイスを構成するソフトウェアアプリケーションおよび / またはモジュールを含むことができる。

【0082】

図 2 は、セキュリティ管理および制御システムによって実施することができる例示的なクラウドセキュリティシステム 200 のブロック図を示す。さまざまな実現例において、例示的なクラウドセキュリティシステム 200 は、サービスプロバイダ 230 のテナント 220 についてネットワーク脅威分析を実施し、サービスプロバイダ 230 のサービスを利用する際のテナント 220 のユーザによるアクションがネットワーク脅威を構成するかどうかを判定することができる。さまざまな実現例において、クラウドセキュリティシステム 200 は、テナント 220 とインターフェースするためのユーザインターフェースコンポーネント 215 と、サービスプロバイダ 230 とインターフェースするためのプロバイダインターフェースコンポーネント 201 とを含むことができる。バックエンドでは、クラウドセキュリティシステム 200 は、分析を行うためのさまざまなアプリケーションと、分析で用いられるデータを格納するためのデータストアとを含むことができる。

30

40

【0083】

図 2 の例の文脈では、テナント 220 はサービスプロバイダ 230 のテナントであり、テナント 220 がサービスプロバイダ 230 のサービスを利用していることを意味する。クラウドセキュリティシステム 200 がクラウドサービスとして提供される場合、テナント 220 はクラウドセキュリティシステム 200 のテナントであることもでき、テナント 220 はクラウドセキュリティシステム 200 のサービスを利用している。

【0084】

さまざまな例では、ユーザインターフェースコンポーネント 215 は、管理コンソール 214 および分析視覚化コンソール 216 を含む。管理コンソール 214 を用いて、テナント 220 は、サービスプロバイダ 230 のサービスのセキュリティ制御を構成することが

50

できる。セキュリティ制御の構成には、たとえば、テナントのユーザによるサービスへのアクセスの有効化または無効化または無効化、テナントのユーザが利用することができるサービスの機能の有効化または無効化、およびテナント 220 に利用可能な他の構成が含まれる。分析視覚化コンソール 216 を用いて、クラウドセキュリティシステム 200 によって生成された分析を見ることができる。たとえば、分析視覚化コンソール 216 を用いて、テナント 220 は、テナントのユーザおよびテナント 220 が加入しているサービスに関するセキュリティインシデントのレポートを閲覧することができる。さまざまな例では、管理コンソール 214 および分析視覚化コンソール 216 に表示される情報は、クラウドセキュリティシステム 200 のデータストアから取得することができる。

【0085】

さまざまな実現例において、管理コンソール 214 は、テナント 220 に、複数のクラウドサービスおよび/またはクラウドサービスプロバイダについて、正規化された制御のビューを提供することができる。管理コンソール 214 は、同じ画面上に異なるクラウドサービスについて簡略化された制御のビューを表示するユーザインターフェースを含むことができる。管理コンソール 214 に提供される情報は、メタデータベースのスキーママッピングを用いてアプリケーションカタログデータベース 208 から取得することができる。いくつかの例では、管理コンソール 214 を用いて、クラウドサービス全体で一貫したアクセスポリシーを割り当てることができる。これらの例では、管理コンソール 214 は、とりわけ標準、厳格、またはカスタムなどの指定された分類子に従って制御を表示および/または制御を設定することができる。この例では、より高いレベルの分類は、より厳格な制御に対応する。一部の例では、セキュリティ管理策の分類および/または指定は、米国国立標準技術研究所 (NIST)、国際標準化機構 (ISO)、および/または PCI データセキュリティスタンダード (PCI DSS) などの組織によって指定された基準、および/またはそのような組織が提供する特定の証明に準拠している。いくつかの例では、管理コンソール 214 は、SaaS、PaaS、およびネイティブアプリケーションと統合するプラグインインターフェースを提供することもできる。

【0086】

さまざまな実現例において、分析視覚化コンソール 216 は、セキュリティインジケータを (赤、緑、黄色などの) 色コード化されたリスク要因とともにライブラリ形式で表示することができる。たとえば、他のメトリックの中でも、ユーザのログイン試行、最も新たに追加されたユーザのグループ、削除されたファイル、最も削除されたファイルのユーザ、および/または最もファイルをダウンロードしたユーザなど、他の統計またはメトリックが表示されてもよい。情報のタイプによっては、特定のサービスプロバイダに固有のものがある。たとえば、Salesforce.com の場合、メトリックには、商談または予算データ、契約、または連絡先をダウンロードしているユーザの素性を含めることができる。いくつかの例では、分析視覚化コンソール 216 は、テナントのクラウドサービスのセキュリティ制御の統合されたビューを提供する。分析視覚化コンソール 216 は、異なるクラウドサービスに設定されたセキュリティ制御のいずれかまたはすべてに設定された値、および所定のポリシーまたは構成に関連付けられた値からの現在の値の偏差を表示してもよい。

【0087】

さまざまな例では、プロバイダインターフェースコンポーネント 201 は、クラウドセキュリティシステム 200 がサービスプロバイダ 230 とインターフェースするために用いることができるアプリケーションであり得る。これらのコンポーネントには、クラウドクローラーアプリケーション 202、クラウドシーダーアプリケーション 204、およびデータローダーアプリケーション 206 が含まれる。

【0088】

さまざまな例において、クラウドクローラーアプリケーション 202 は、セキュリティ制御に関する情報をサービスプロバイダ 230 から取得することができる。クラウドクローラーアプリケーション 202 によって取得されたデータは、アプリケーションカタログデータベース 208 に入力することができる。情報の取得は、例えば、サービスに利用可能

10

20

30

40

50

なセキュリティ制御およびセキュリティ制御に利用可能な設定をサービスプロバイダ 230 に求めるように定式化された要求をサービスプロバイダ 230 に送信することを含むことができる。代替的または追加的に、サービスプロバイダ 230 は、クラウドクローラアプリケーション 202 がサービスのセキュリティ制御を取得することができる A P I を含むことができる。さまざまな例において、クラウドクローラアプリケーション 202 は、サービスプロバイダ 230 からソフトウェア定義のセキュリティ構成データを取得することができる。ソフトウェア定義のセキュリティ構成データは、特定のサービスのセキュリティ制御の構成を記述することができる。セキュリティ制御は、クラウドサービスプロバイダが収容するアプリケーションおよび/またはデータへのアクセスを制限するメカニズムである。たとえば、ソフトウェア定義のセキュリティ構成データには、ユーザ、グループ、およびユーザのグループに対して定義されている役割を記述するデータ；暗号化キー；トークン；アクセス制御；許可；構成；認証ポリシーのタイプ；モバイルアクセスポリシー；ならびに他の多くのタイプのセキュリティ管理を含めることができる。

10

【0089】

さまざまな例において、クラウドクローラアプリケーション 202 は、ソフトウェア定義のセキュリティ構成データを取得するためにサービスプロバイダ 230 に接続することができる。サービスプロバイダ 230 は、サービスプロバイダのシステムへのアクセスに対する承認または他の何らかの同意の明示を必要としてもよい。承認は、トークン（承認のための Open Authorization (OAuth) オープン基準を用いるなど）またはクレデンシャル（ユーザ名およびパスワードなど）によって提供されてもよい。トークンまたはクレデンシャルは、テナント 220 のもの、またはクラウドセキュリティシステム 200 に関連付けられたトークンもしくはクレデンシャルであり得る。クラウドプロバイダのシステムおよびデータへのアクセスを承認するために、他のさまざまな手法を用いることができる。接続には、サービス URL の提供も含まれ得る。

20

【0090】

さまざまな例では、ソフトウェア定義のセキュリティ構成データは、サービスプロバイダ 230 の A P I を用いて収集することができる。A P I および A P I のクラスの例には、Representational State Transfer (REST)、Java 2 Platform、Enterprise Edition (J2EE)、Simple Object Access Protocol (SOAP)、およびネイティブプログラミングメソッド（Java のネイティブアプリケーション A P I など）などが含まれる。情報は、スクリプト言語（Python や PHP など）、展開記述子、ログファイル、Java Database Connectivity (JDBC) または REST を介したデータベース接続、および常駐アプリケーション（クラウドビーコンなど）などの他の手法を用いて要求することもできる。送受信される情報は、JavaScript Object Notation (JSON)、Extensible Markup Language (XML)、または（Comma Separated Values (CSV) などのさまざまな形式で表現することができる。

30

【0091】

以下の表 1 は、クラウドサービスプロバイダの Box および Amazon Web Services (AWS) が提供するセキュリティ制御の例を示す。他のクラウドサービスプロバイダも、同様のセキュリティ制御または他のセキュリティ制御を有することができる。

40

【0092】

【表 1】

表 1

セキュリティ制御	Box におけるサポート	Amazon Web Services (AWS) におけるサポート
ユーザ／グループ管理	REST (Representational State Transfer) API	AWS IAM (身元およびアクセス管理) APIs
クレデンシャルおよび識別子	N/A	アカウント、トークン、キーなどの保護および監視
ログイン／ログアウトイベント	REST API	AWS CloudTrail - イベント API およびログファイル
クライアントの IP アドレス	REST API	AWS CloudTrail - イベント API およびログファイル
クライアントによって用いられるデバイス (iphone, ipad など)	REST API	AWS CloudTrail - イベント API およびログファイル
パスワードポリシー	REST API	AWS IAM ポリシー
リソースアクセス許可	リソース: ファイル、フォルダ アクション: 編集、プレビュー、アップロード、コラボレーションイベント	リソース: EC2, S3, EBS アクション: 作成、アクセス、リスタート、終了など IP アドレスベースのアクセス制御
モバイルアクセスを制限または限定	オフラインアクセスについてコンテンツをセーブすることからユーザを制限する	AWS IAM ポリシー
役割	BOX は予め定義された管理役割を有する	役割は予め定義されたポリシーを用いて作成される

【 0 0 9 3 】

表 2 に、クラウドサービスプロバイダSalesforce.comのセキュリティ制御およびサポートされているアクセスの一部の例を示す。他のクラウドサービスプロバイダも、同様のまたは他のセキュリティ制御およびアクセス制御を用いることができる。

【 0 0 9 4 】

【表 2】

表 2

セキュリティ制御	Salesforce.comにおけるサポート
ユーザ／グループ管理	SalesForce ユーザ／グループ／プロフィール APIs
クレデンシャルおよび識別子	APIs: セットアップ変更
ログイン／ログアウトイベント	APIs: 監査アクティビティ
クライアントの IP アドレス	APIs: 監査アクティビティ
クライアントによって用いられるデバイス (iphone, ipad など)	セットアップ変更を管理する API
パスワードポリシー	APIs: セットアップ変更
リソースアクセス許可	オブジェクト履歴を用いる Salesforce オブジェクト監視
モバイルアクセスを制限または限定	セットアップ変更を管理する APIs
役割	Salesforce プロファイル

10

20

【 0 0 9 5 】

さまざまな例では、クラウドクローラーアプリケーション 2 0 2 は、サービスプロバイダ 2 3 0 から取得したソフトウェア定義のセキュリティ構成データからセキュリティ制御メタデータを生成することができる。セキュリティ制御メタデータは、アプリケーションカタログデータベース 2 0 8 などの共通データベースに情報を入力するための正規化された記述子である。セキュリティ制御メタデータは、分類（カテゴリへのマッピングなど）およびインデックス付けすることができる。この分類は、セキュリティ組織によって指定された基準に準拠していてもよく、ならびに／または第三者によって証明および／もしくは監査されていてもよい。さらに、セキュリティ制御メタデータおよび／またはメタデータの分類は、特定の規制または基準の要件に基づいて策定することができる。たとえば、医療保険の相互運用性と説明責任に関する法律（H I P A A）、サーベンス・オクスリー法、米国連邦リスクおよび承認管理プログラム（F e d R A M P）、および／または P C I データセキュリティスタンダード（P C I D S S）などの規制および基準は、報告および監査証跡が必要であっててもよい。セキュリティ制御メタデータは、規制および基準で必要な情報のタイプを表示し、必要なレポートの生成を容易にする方法でフォーマットすることができる。

30

40

【 0 0 9 6 】

セキュリティ制御メタデータは、アプリケーションカタログデータベース 2 0 8 に格納することができる。いくつかの例では、アプリケーションカタログデータベース 2 0 8 は、Apache Cassandraデータベースであり、多くのコモディティサーバにわたって大量のデータを処理するように設計されたオープンソースの N o S Q L データベース管理システムである。いくつかの例では、アプリケーションカタログデータベース 2 0 8 は、アプリケーションに適したタイプのデータベースを用いて実現される。いくつかの例では、さまざまなデータベースを用いて、後の取得、レポート生成、および分析生成のために、アプリ

50

ケーションカタログを格納することができる。

【 0 0 9 7 】

さまざまな実現例では、他の方法を用いて、ソフトウェア定義のセキュリティ構成データを取得し、セキュリティ制御メタデータを生成することができる。さらに、ソフトウェア定義のセキュリティ構成データを取得するためのさまざまなタイプの制御およびメカニズムが、さまざまなクラウドサービスプロバイダによってサポートされている場合がある。たとえば、Office 365、GitHub、Workday、およびさまざまなGoogleアプリケーションなどの他のクラウドアプリケーションは、サービスに固有の検索メカニズムを用いる。さらに、クラウドサービスプロバイダがサポートするものに依拠して、ソフトウェア定義のセキュリティ構成データを取得するプロセスを自動化することができる。

10

【 0 0 9 8 】

さまざまな実現例において、クラウドシードアプリケーション 2 0 4 を用いて、テナント 2 2 0 のセキュリティポリシーを実現することができる。クラウドシードアプリケーション 2 0 4 は、たとえば、テナントの、サービスプロバイダのサービスのアカウントのセキュリティ制御を設定することができる。セキュリティ制御は、たとえば、1つのユーザアカウント、複数のユーザアカウント、またはすべてのユーザアカウントに影響し得る。いくつかの例では、クラウドシードアプリケーション 2 0 4 は、さまざまな状況でセキュリティ制御を設定することができる。たとえば、クラウドシードアプリケーション 2 0 4 は、脅威の救済の一部として、またはテナント 2 2 0 から呼び出されたときに、セキュリティ制御を設定することができる。さまざまな例では、クラウドシードアプリケーション 2 0 4 を用いて、クラウドサービス全体で一貫したアクセスポリシーを調整することができる。一部の例では、組織がさまざまなサービスプロバイダに所有している複数のアカウント間でセキュリティ制御を調整することができる。たとえば、さまざまなレベルのセキュリティを定義して、より高いレベルまたはより低いレベルのセキュリティを選択すると、組織の、異なるクラウドサービスのアカウントのセキュリティ制御がすべて、より高いレベルまたはより低いレベルのセキュリティを反映するようにされる。このようにして、統一されたポリシーおよびセキュリティ制御の構成を実施することができる。さまざまなセキュリティレベルのさまざまなセキュリティ制御の値は、前述の制御管理プラットフォームなどのユーザインターフェイスへの入力によって定義でき、各セキュリティレベルのセキュリティ制御に関連付けられた値はデータベースに格納することができる。ユーザインターフェイスを提供して、組織の、クラウドサービスのアカウントのセキュリティ制御、およびセキュリティレベルでのセキュリティ制御値の割り当てを示すことができる。例として、「厳格な」セキュリティレベルのセキュリティ制御には、最小 1 0 文字、2つの数字、1つの特殊文字、1つの大文字、最後の 1 0 個のパスワードの再利用なしなど、ユーザアカウントのパスワード要件が含まれる。

20

30

【 0 0 9 9 】

さまざまな実現例において、データローダーアプリケーション 2 0 6 は、サービスプロバイダ 2 3 0 からテナント 2 2 0 のアクティビティデータを取得することができる。アクティビティデータは、テナントのユーザがサービスプロバイダサービスを利用するときにサービスプロバイダ 2 3 0 によって生成されたログから取得することができる。さまざまな例では、データローダーアプリケーション 2 0 6 は、サービスプロバイダ 2 3 0 にアクティビティデータを要求することにより、アクティビティデータを取得することができる。データローダーアプリケーション 2 0 6 によって取得されたデータは、ランディングリポジトリ 2 1 0 ならびに / または分析および脅威インテリジェンスリポジトリ 2 1 1 に入力することができる。ランディングリポジトリ 2 1 0 に入力されるデータは、例えば、異なるサービスプロバイダから収集されたために、異なるフォーマットであり得、および / または異なる範囲の値を有し得る。いくつかの例では、データローダーアプリケーション 2 0 6 からのデータは、例えば、データが一般的な形式になるように、分析および脅威インテリジェンスリポジトリ 2 1 1 に移動される前に再フォーマットおよび / または構造化することができる。

40

50

【 0 1 0 0 】

さまざまな例では、データローダーアプリケーション 2 0 6 は、サービスプロバイダ 2 3 0 に接続して通信することによりアクティビティデータを取得することができる。さまざまな例において、接続は暗号化された通信チャネルを介して行われる。一部の例では、トークンもしくはログインクレデンシャル、または別の認証方法を用いて接続を認証することができる。いくつかの例では、アクティビティデータの収集は定期的に（たとえば、4 時間ごと、6 時間ごと、または他の時間間隔で）発生するようにスケジュールされている。いくつかの例では、収集のスケジュールはテナント 2 2 0 によって構成可能である。いくつかの例では、データローダーアプリケーション 2 0 6 は、例えばオープンソースの分散リアルタイム計算システムである Apache Storm などのリアルタイム計算システムを用いて、イベントが発生するとリアルタイムでデータを収集する。データローダーアプリケーション 2 0 6 は、特定のイベントまたはアクティビティを高リスクイベントとして指定するように構成することができ、これらのイベントは、スケジュールされた取得間隔外でほぼリアルタイムで取得することができる。

10

【 0 1 0 1 】

さまざまな例では、アクティビティデータには、サービスプロバイダのサービスのユーザに関するさまざまなタイプの情報が含まれ得る。たとえば、ユーザアカウントに関連付けられたアクティビティデータには、サービスのユーザアカウントの使用および／またはそれで行ったアクションに関連する情報を含めることができる。この例では、アクティビティデータに、ユーザログや監査証跡などの情報ソースを含めることができる。より具体的なタイプのアクティビティデータには、たとえば、ログインおよびログアウト統計（試行および成功を含む）、ファイル操作、アクセスメトリック、ネットワークダウンロード／アップロードメトリック、アプリケーションメトリック（たとえば、使用、操作、機能など）、サービスへのアクセスに用いられる IP アドレス、サービスへのアクセスに用いられるデバイス、および／またはアクセスされたクラウドリソース（たとえば、ファイル管理クラウドアプリケーション（Box など）のファイルおよびフォルダ、ヒューマンリソースクラウドアプリケーション（Workday など）の従業員および請負業者、および／または顧客関係管理クラウドアプリケーション（Salesforce など）の連絡先およびアカウント）が含まれ得る。さまざまな例において、アクティビティデータには、イベントまたは統計に関連付けられたユーザのユーザアカウントまたは他のユーザ識別子を含めることができる。さまざまな例では、アクティビティデータには、サーバアクティビティ、サーバの再起動、サーバが用いるセキュリティキー、システムクレデンシャルなど、クラウドシステムのシステムステータスまたはアクティビティに関する情報を含めることができ、この情報は、承認されたクレデンシャルを用いてシステムに可視であるかまたはアクセス可能である。

20

30

【 0 1 0 2 】

いくつかの例では、アクティビティデータには、おそらくはテナントアカウントに関連付けられたユーザアカウントのセキュリティ構成を含む、テナントアカウントのセキュリティ構成に関する情報も含まれる場合がある。セキュリティ構成には、テナントおよび／またはテナントに関連付けられたユーザアカウントのセキュリティ制御が設定される値を含めることができる。

40

【 0 1 0 3 】

さまざまな例では、データローダーアプリケーション 2 0 6 は、検索されたアクティビティデータを分析および脅威インテリジェンスリポジトリ 2 1 1 に格納することができる。分析および脅威インテリジェンスリポジトリ 2 1 1 は、クエリ機能を備えた任意のデータベースまたはデータリポジトリにすることができる。一部の例では、分析および脅威インテリジェンスリポジトリ 2 1 1 は、Apache Cassandra または別の分散データ処理システムなどの NoSQL ベースのインフラストラクチャに構築されているが、アプリケーションに応じて任意のデータウェアハウスインフラストラクチャを適切に用いることができる。いくつかの例では、データは最初にランディングリポジトリ 2 1 0 に入力され、再フォ

50

ーマットおよび/または構造化されたのち、分析および脅威インテリジェンスリポジトリ 211 に移動される。

【0104】

一部の例では、アクティビティデータは、さまざまなサービスプロバイダまたはサービスで用いられるさまざまな形式で受信されてもよい。たとえば、データはJSONまたは他のデータ交換形式でフォーマットされていてもよく、またはログファイルもしくはデータベースエントリとして利用可能であってもよい。いくつかの例では、データローダーアプリケーション206は、データを正規化し、分析および脅威インテリジェンスリポジトリ211における格納および検索のためにデータを共通フォーマットに再フォーマットするための操作を実行する。データの再フォーマットには、データを共通フォーマットに分類および構造化することが含まれ得る。一部の例では、データベースは構造の変更や新たな値に適応し、自動化されたプロセスを実行して、変更されたデータをチェックすることができる。いくつかの例では、クラウドクローラーアプリケーション202は、取得したデータの構造または値の違いを認識し、アプリケーションカタログデータベース208ならびに/または分析および脅威インテリジェンスリポジトリ211に変更を適用することができる。

10

【0105】

いくつかの例では、データローダーアプリケーション206は、システムレポートを事前生成することができる。システムレポートは、定期的な間隔でデータセットで実行するようにスケジュールされているジョブ（例：プロセスなど）によって生成することができる。アプリケーションカタログデータベース208ならびに/または分析および脅威インテリジェンスリポジトリ211に格納されたデータを用いて、さまざまなレポートを生成することができる。レポートのカテゴリには、たとえば、認証と承認、ネットワークとデバイス、システムと変更データ、リソースアクセスと可用性、マルウェアアクティビティ、障害と重大なエラーなどが含まれ得る。レポートは、たとえば、アプリケーションごと、ユーザごと、保護されたリソースごと、アクセスに用いられるデバイスごとなど、さまざまな属性に基づくことができる。レポートでは、クラウドアプリケーションの更新された機能や新しく変更されたポリシーなどの最近の変更が強調表示される場合がある。レポートは、（パフォーマンス上の理由などのために）スケジュールされたジョブによって事前に生成されてもよく、またはユーザもしくは管理者によって要求されてもよい。

20

30

【0106】

一部の例では、レポートにはデータに対して生成された分析が含まれる。分析では、Hadoop、Hive、Spark、MahoutなどのApache Software Foundation技術、または用いられるデータストレージフレームワークで利用可能なその他の機能を用いてもよい。一部の例では、Rプログラミング言語を用いて分析を生成する。いくつかの例では、分析の生成には、機械学習アルゴリズム、所有アルゴリズム、および/またはFireEyeやNorseなどの外部商用ソースからの外部脅威インテリジェンスもしくはZeusやTorなどの公共脅威インテリジェンスコミュニティの使用が含まれる。

【0107】

さまざまな実現例において、アクセスパターンおよび他のイベント統計に関する、分析および脅威インテリジェンスリポジトリ211内のアクティビティ情報の集約により、システム200は挙動のベースラインを確立することが可能になる。たとえば、機械学習技術を適用して脅威を検出し、脅威への対応方法に関する推奨事項を提供することができる。既知または未知または新たに出現する脅威を検出するために、脅威モデルを開発することができる。脅威は、以下でさらに説明するように、アクティビティデータを、サードパーティプロバイダによって提供される情報などの外部の脅威インテリジェンス情報と比較することでも特定することができる。さまざまな例では、分析および脅威インテリジェンスリポジトリ211のデータを用いて、さらに、ユーザインターフェイスを介してシステム管理者に視覚的に提示することができるレポートを生成し、脅威レベルの判定、特定の脅威の検出、潜在的な脅威の予測などのための分析を生成することができる。

40

50

【 0 1 0 8 】

いくつかの例では、テナント 2 2 0 の単一のユーザは、サービスプロバイダ 2 3 0 および / またはサービスプロバイダ 2 3 0 によって提供されるサービスで複数のアカウントを有することができる。さまざまな例では、1 人のユーザのさまざまなユーザアカウントを、ユーザ素性リポジトリ 2 0 9 で関連付けることができる。いくつかの例では、ユーザ素性リポジトリ 2 0 9 は、ユーザが複数のサービスプロバイダで有するユーザアカウントをグループ化することができる。いくつかの例では、テナント 2 2 0 は、サービスプロバイダ 2 3 0 のテナントアカウントを有することができる。これらの例では、ユーザ素性リポジトリ 2 0 9 は、テナント 2 2 0 のユーザをテナントアカウントに関連付けることができ、それは、ユーザのユーザアカウントをテナントアカウントに関連付けることもできる。ユーザアカウントのテナントアカウントへの関連付けは、テナントのユーザのユーザアクティビティに関する情報の取得など、さまざまな方法で用いることができる。いくつかの例では、テナントアカウントの、サービスプロバイダ 2 3 0 のクレデンシャルを用いて、サービスプロバイダ 2 3 0 にログインし、テナントアカウントに関連付けられたユーザアカウントのアクティビティデータを取得することができる。

10

【 0 1 0 9 】

さまざまな実現例において、ユーザ素性リポジトリ 2 0 9 は、ユーザアクティビティの追跡およびプロファイルの生成を容易にするためにも使用でき、プロファイルは特定のユーザのクラウドサービスまたは複数のクラウドサービスの利用を記述することができる。いくつかの例では、クラウドセキュリティシステム 2 0 0 は、ユーザのプロファイルを用いて、複数のクラウドサービスに影響を与えるアクションを実行することができる。例えば、クラウドセキュリティシステム 2 0 0 は、いくつかのクラウドサービスを利用する際のユーザのアクティビティがセキュリティリスクである可能性がある場合、システム管理者に先制的に警告することができる。代替的または追加的に、別の例として、クラウドセキュリティシステム 2 0 0 は、認証に追加の手順を追加する、パスワードを変更する、特定の IP アドレスをブロックする、電子メールメッセージまたは送信者をブロックする、アカウントをロックするなどの是正措置を適用することにより、ユーザがデータを維持する他のサービスを予防的に保護することができる。

20

【 0 1 1 0 】

さまざまな実現例において、クラウドセキュリティシステム 2 0 0 は、クラウドセキュリティシステム 2 0 0 によって収集されたデータの分析を実行するアプリケーションまたはソフトウェアモジュールを含むことができる。アプリケーションまたはソフトウェアモジュールは、揮発性または不揮発性メモリに格納され、実行時に特定の機能またはプロセスを実行するようにプロセッサを構成することができる。これらのアプリケーションは、記述的分析アプリケーション 2 0 7 および予測分析アプリケーション 2 1 2 を含むことができる。いくつかの例では、記述的分析アプリケーション 2 0 7 は、ユーザに関する統計、ユーザアクティビティ、およびユーザが用いるリソースなどの分析を生成することができる。いくつかの例では、脅威検出および予測分析アプリケーション 2 1 2 は、機械学習および他のアルゴリズムを用いて分析を生成することができる。予測分析アプリケーション 2 1 2 によって実行される分析は、アクティビティおよび挙動モデルのパターンからセキュリティの脅威を識別および予測することを含むことができる。記述的分析アプリケーション 2 0 7 および予測分析アプリケーション 2 1 2 によって実行される分析は、分析および脅威インテリジェンスリポジトリ 2 1 1 に格納されたデータを用いて実行することができる。

30

40

【 0 1 1 1 】

さまざまな実現例において、クラウドセキュリティシステム 2 0 0 は、脅威に対応するための手動および / または自動化されたプロセスを提供する救済機能を含むことができる。いくつかの例では、分析は、テナントによって提供される脅威インテリジェンスを記述する、テナントシステムから受信した情報を用いることができる。例示的なシステム 2 0 0 においてテナントベースライン 2 1 7 と呼ばれるこれらのソースには、監視またはプロッ

50

クすべき特定のIPアドレス、監視またはブロックすべきユーザ、監視またはブロックすべき電子メールアドレス、監視すべきソフトウェア脆弱性、誤用の影響を受けやすいブラウザもしくはブラウザバージョン、および/またはモバイルハードウェアもしくはソフトウェアの脆弱なモバイルデバイスもしくはバージョンなどが含まれ得る。いくつかの例では、分析は外部のサードパーティフィード218から受信した情報を用いることができる。サードパーティフィード218のソースは、例えば、脅威インテリジェンスアグリゲータまたはディストリビュータであり得る。サードパーティフィード218からの情報を用いて、セキュリティ脅威に関する外部情報を提供することにより、クラウドセキュリティシステム200の脅威分析を強化することができる。外部情報には、たとえば、感染したノードポイントの識別、特定のソースIPアドレスからの悪意のあるアクティビティ、マルウェアに感染した電子メールメッセージ、脆弱なウェブブラウザバージョン、クラウドに対する既知の攻撃などが含まれ得る。

10

【0112】

さまざまな実現例において、インシデント救済アプリケーション213を用いて、検出された脅威に応じて救済アクションを調整および/または実行することができる。いくつかの例では、推奨される救済アクションが提示され、アラートで選択されたときに、インシデント救済アプリケーション213が呼び出されてもよい。インシデント救済アプリケーション213は、選択された救済アクションを実行するか、クラウドシードアアプリケーション204などの別のアプリケーションに選択された救済アクションを実行するよう指示することができる。選択した救済アクションが、手動で実行される場合、またはセキュリティシステム200の外部にある場合、インシデント救済アプリケーション213は救済アクションのステータスと救済アクションが完了したかどうかを追跡することができる。いくつかの例では、インシデント救済アプリケーション213を用いて、手動または自動救済アクションの結果を保存することができる。いくつかの例では、選択された救済アクションは、サードパーティまたはテナントのインシデント救済システムなど、セキュリティシステム200の外部のシステムによって実行される。これらの例では、インシデント救済アプリケーション213は、サードパーティまたはテナントのインシデント救済システムに指示するかまたはそれ呼び出して、アクションを実行することができる。例えば、インシデント救済アプリケーション213は、サードパーティまたはテナント220の自動化された統合プロセスにアクセスすることができる。

20

30

【0113】

図3は、セキュリティ管理および制御システムの例示的な分析エンジン300のブロック図を示す。さまざまな例では、分析エンジン300はさまざまなデータソースを分析して、ユーザがクラウドサービスを利用している組織のネットワーク脅威を識別することができる。さまざまな例では、分析エンジン300の動作を用いて、さまざまな脅威シナリオの検出および/または対処が可能である。

【0114】

脅威シナリオの1つの例は、IPホッピングである。IPホッピングのシナリオでは、攻撃者は1つ以上のプロキシサーバを用いて、攻撃を仕掛ける前に、攻撃者の実際の位置またはマシンIDを隠すことができる。このタイプのシナリオの検出には、クラウドアプリケーションへの接続に用いられる各IP接続の地理的解決（たとえば、IPアドレスに関連付けられた地理的位置の識別または検索）が含まれる。検出には、さらに、空間データ内の異常な特性を検出し、この情報から脅威を予測することが含まれ得る。検出に用いられるメトリックには、たとえば、ユーザが1日あたりに用いる一意のIPアドレスの数のカウントおよび/または速度が含まれ得、それは、異なるIPアドレスを使用した場合の時間差および/または各IPアドレスが用いた期間を指し得る。

40

【0115】

脅威シナリオのもう1つの例は、異常なジオロケーションのシナリオである。異常なジオロケーションのシナリオは、予期しない場所または確立されたパターン外の場所で発生したアクティビティを指してもよい。このシナリオには、異常なジオロケーションからの口

50

グインの成功またはファイルのアップロード/ダウンロードなどが含まれ得るが、これらに限定はされない。

【0116】

脅威シナリオの別の例は、ブルートフォース攻撃である。ブルートフォース攻撃の例としては、攻撃者が正しいパスワードを見つけてユーザアカウントを侵害するために多くのパスワードを試行する場合がある。検出には、ログイン試行の失敗の速度およびイベントアクティビティのパターンを評価して、ブルートフォース攻撃を予測することが含まれ得る。いくつかの例では、ブルートフォース攻撃は、遅い攻撃速度や速い攻撃速度など、異なる速度を有する場合がある。検出のメトリックには、たとえば、既存の有効なアカウントに対する異常な数のログイン失敗、および/または無効なユーザ名もしくは解雇/停職ユーザ名による異常な数のログイン試行が含まれ得る。

10

【0117】

脅威シナリオのもう1つの例は、インサイダー脅威である。インサイダー脅威とは、ネットワーク内から人が犯したセキュリティ侵害を指す。たとえば、組織の雇用過程で承認された組織の従業員が、承認を誤用し、意図的または意図せずにセキュリティ違反を起こす可能性がある。インサイダー脅威の検出には、ユーザの通常の挙動の追跡と、ユーザのアカウントに関連付けられたイベントまたはアクティビティが標準から逸脱した場合のアラートの生成とが含まれ得る。メトリックには、たとえば、ダウンロード数が多いなど、企業リソースの使用率が通常高いこと、および/または評価が低い従業員が、異常に多数のファイル/フォルダを共有またはダウンロードすること、ソースコード管理システムからコードを削除すること、もしくは顧客情報を変更することなどが含まれ得る。

20

【0118】

脅威シナリオの別の例は、アプリケーションの誤用である。アプリケーションの誤用とは、解雇または停職とされた従業員に関連するイベント（失効または停止されたユーザアカウントの使用、SSHキーなどの暗号キーの使用など）、または有効なクレデンシャルを用いているが、たとえば通常とは異なるジオロケーションまたはIPアドレスなどを用いて異常な数のファイルのダウンロード/アップロードを実行するマルウェア感染デバイスを含み得るシナリオである。

【0119】

これらのシナリオを識別するために用いることができる特定の脅威シナリオおよび情報のタイプについては上記で説明したが、当業者は、脅威の検出および予測がさまざまな情報および式のいずれかを利用することができることを認識するだろう。

30

【0120】

さまざまな例では、分析エンジン300は、さまざまな外部および内部データソースを調べることにより、前述の脅威シナリオを、他の脅威シナリオとならんで、検出することができる。外部データソースは、クラウドサービスプロバイダから取得したアクティビティデータ310を提供することができる。いくつかの例では、外部データはオプションでテナントベースライン317とサードパーティデータ318とを含むことができる。いくつかの例では、内部データソースは、挙動分析エンジン304によって判断されたデータモデルを含むことができ、セキュリティ管理および制御システムによって維持される脅威インテリジェンスデータ314をオプションで含むことができる。

40

【0121】

さまざまな例において、クラウドサービスは、ユーザがクラウドサービスを利用するときにユーザアクティビティを記憶することができる。たとえば、クラウドサービスは、サービスを利用するためのユーザのログイン、サービスの利用中にユーザが実行するアクション、アクションの影響を受けるリソース、サービスの内外に移動する、もしくはサービス内のデータ、および/またはセッションの終了時におけるユーザのログアウトなどの各発生を記憶することができる。これらおよびその他の例では、ユーザのアクティビティをログファイルに記憶することができる。ログファイルは、ここではアクティビティログと呼ぶ。アクティビティログのエントリには、たとえば、実行されたアクションもしくは実行

50

されたアクションの記述、アクションを実行したユーザの識別、アクションによって影響を受けたリソース、アクションが実行された時間またはアクションの開始時および/もしくは完了時、および/またはアクションを実行したユーザのネットワーク位置もしくはジオロケーションなどの情報が含まれ得る。図3の例では、アクティビティデータ310は、複数のサービスおよび/または複数のサービスプロバイダのアクティビティログを含むことができる。これらの例および他の例では、1つのアクティビティログに、1つのサービスまたは同じサービスプロバイダが提供する複数のサービスのユーザアクティビティを含めることができる。

【0122】

さまざまな例では、分析エンジン300は、更新されたアクティビティデータ310を1日1回、隔日、または別の時間間隔で定期的に受信する。いくつかの例では、イベントが発生したことを示すサービス（例えば、サービスが更新された、またはサービスがネットワーク脅威もしくはサービスで発生する別のイベントを検出した）、イベントが発生したことを示す組織（たとえば、サービスにユーザを追加した組織、更新された分析を要求するネットワーク管理者、または組織で発生する別のイベント）、またはイベントが発生したことを示すセキュリティ管理および制御システム（たとえば、新たな脅威インテリジェンスデータ314の受信またはセキュリティ管理および制御システムで発生する別のイベント）などの特定のイベントが発生すると、分析エンジン300はアクティビティデータ310を受信する。

【0123】

一部の例では、異なるクラウドサービスのアクティビティログの形式が異なる場合がある。たとえば、あるアクティビティログのエントリはコンマ区切り値として提供され、別のアクティビティログはJSON構文を用いる場合がある。これらおよび他の例では、アクティビティログ内のデータは、分析エンジン300によって、または分析エンジン300に提供される前に正規化されてもよい。アクティビティデータ310を正規化することは、異なるサービスおよび/またはサービスプロバイダからのデータが同等であり、同じ意味を有し、ならびに/または同じ有意性および関連性を有するように、アクティビティデータ310を再フォーマットすることを含む。正規化後、挙動分析エンジン304は、異なるクラウドサービスからのデータを意味のある方法で集約して比較することができる。たとえば、1人のクラウドサービスでの1人のユーザによる一連のログイン試行の失敗は、脅威ではないと見なされ得る。しかしながら、同じユーザによる複数の異なるクラウドサービスでの一連の失敗したログインは、ユーザのパスワードを解読するための計画的な労力を示しているため、アラームを作動させるべきである。

【0124】

さまざまな例において、アクティビティデータ310は、挙動分析エンジン304によって分析エンジン300に取り込むことができる。さまざまな実現例において、挙動分析エンジン304は、アクティビティデータ310から統計を収集し、アクティビティデータ310から挙動特性を識別することができる。統計には、たとえば、成功したログイン試行または失敗したログイン試行などのアクションのカウントを含めることができる。いくつかの例では、統計は、特定のサービスプロバイダ、特定のサービス、特定のユーザ、サービスの利用時に実行することができる特定のアクション、特定の時間枠、他の要因、および/または要因の組み合わせに関連付けることができる。

【0125】

さまざまな実現例では、挙動分析エンジン304は、アクティビティデータ310から生成された統計データを用いて、本明細書では挙動プロファイルとも呼ばれるアクティビティプロファイルを判断することができる。例えば、挙動分析エンジン304は、特定の組織のユーザによるサービスの一般的または典型的な利用パターンを記述するアクティビティプロファイルを生成することができる。別の例として、挙動分析エンジン304は、特定のユーザまたはユーザのグループのアクティビティプロファイルを生成することができる。この例では、アクティビティプロファイルは、1つ以上のサービスを利用する際のユ

10

20

30

40

50

ーザのアクティビティを記述することができる。さまざまな例では、サービス全体でユーザのアクティビティを識別するために、挙動分析エンジン 304 は、特定のユーザの、異なるクラウドサービスのアカウントをリンクすることができるユーザ素性データにアクセスすることができる。ユーザ素性データには、たとえば、ユーザの、各クラウドサービスのユーザ名またはその他の形式の識別が含まれ得る。さまざまな例では、ユーザ素性データは組織によって提供され得る。代替的または追加的に、いくつかの例では、セキュリティ管理および制御システムは、異なるユーザアカウントが関連していることを自動的に判断する。たとえば、セキュリティ管理および制御システムは、同じユーザ名を有するユーザアカウントまたは同じ IP アドレスもしくは MAC アドレスからのユーザアカウントをリンクすべきであることを想定することができる。

10

【0126】

いくつかの例では、挙動分析エンジン 304 は、ユーザのアクティビティプロファイルにコンテキストデータを含めることができる。コンテキストデータは、例えば、サードパーティデータ 318 から取得することができる。サードパーティデータ 318 のソースは、評判システム、ソーシャルメディアシステム、ニュースアグリゲータもしくはプロバイダ、またはユーザに関する情報を維持することができる別のシステムである。コンテキストデータの例には、旅行アプリケーションもしくは電子メールからの旅行の場所および旅程、ヘルスケア管理システムからの従業員ステータス、Salesforceアプリケーションからの重要な財務期間、ならびに / または電子メールサーバからの重要な電子メールなどのデータが含まれる。一部の例では、コンテキストデータは、ユーザが用いるクライアントデバイスから追加的または代替的に取得することができる。これらの例では、コンテキストデータには、たとえば、クライアントデバイスのタイプの識別、クライアントデバイスが用いる IP アドレス、クライアントデバイスの全地球測位システム (GPS) 受信機によって計算されるジオロケーションデータ、およびクライアントデバイスについてのその他の情報またはクライアントデバイスから取得することができるその他の情報が含まれ得る。

20

【0127】

さまざまな例において、アクティビティプロファイルはさまざまな期間をカバーすることができる。いくつかの例では、アクティビティプロファイルは、週単位で測定される期間をカバーする固定された移動ウィンドウを用いることができる。いくつかの例では、「新生プロファイル」を生成することができる。これは、先週または目標日付の 1 週間前など、比較的最近のイベントをキャプチャする。一部の例では、「安定したプロファイル」を生成することができる。これには、直近の 4 (または 8) 週間以内または目標日付の直前の 4 (または 8) 週間以内のイベントが含まれる。さまざまな例において、他のプロファイルまたはプロファイルタイプを生成することができる。

30

【0128】

一部の例では、固定された移動ウィンドウは重ならないようにすることができる。つまり、時間をさかのぼるウィンドウは、時間的により最近のウィンドウにおけるイベントを除外することができる。たとえば、8 週間のプロファイルには 4 週間のプロファイルまたは 1 週間のプロファイルのイベントは含まれず、同様に、4 週間のプロファイルには 1 週間のプロファイル内のイベントは含まれない。日次 (または定期) 集約プロセスは、日と日の間または日中に実行されてもよい。

40

【0129】

以下の表 3 は、一部のユーザアクティビティについて計算された統計の例を示す。ユーザアクティビティの例には、4 週間のウィンドウプロファイルの平均ログインカウント (「avglogcntday4wk」)、4 週間のウィンドウプロファイルの平均ログイン IP アドレスカウント (「avglogipcntday4wk」)、1 週間のウィンドウプロファイルのログインカウントの標準偏差 (「stdlogcntday1wk」) および 1 週間のウィンドウプロファイルのログイン IP アドレスカウントの標準偏差が含まれる (「stdlogipcntday1wk」)。利用可能なデータおよび / または予測される脅威に応じて、同様の統計および他の統計を計算することができる。

50

【 0 1 3 0 】

【 表 3 】

表 3

ユーザID	avglogcntday _4wk	avglogipcntday _4wk	stdlogcntday _1wk	stdlogipcntda y_1wk
ユーザ 1	5	4	3	2
ユーザ 2	6	2	2	1
ユーザ 3	4	3	2	2
ユーザ 4	4	4	2	1
ユーザ 5	5	5	1	1

【 0 1 3 1 】

上記のような統計は、特徴ベクトルに組み合わせることができる。特徴ベクトルには、たとえば、ログイン数のカウント、ログインに用いられる個別のIPアドレスの数のカウント、24時間以内にログインに用いられた2つのIPアドレス間の最大距離、24時間以内にクラウドアプリケーションへの接続に使用された異なるブラウザの数、および/またはその他のメトリックが含まれ得る。特徴ベクトルは、クラウドアプリケーションごと、および/またはクラウドアプリケーションごとのユーザごとに集約することができる。

【 0 1 3 2 】

以下の表4は、日次集計行列ベクトルの例を示す。1番目の列はアプリケーションプロバイダの例を提供し、2番目の列はプロバイダがサポートすることができるベクトル次元を示し、3番目の列は各次元に割り当てることができる値を示す。

【 0 1 3 3 】

10

20

30

40

50

【表 4】

表 4

アプリケーション	次元	記述
Amazon, Salesforce, Box	ログイン	(# of count, Avg, Stddev, Max)
Amazon, Salesforce, Box	失敗したログイン	(# of count, Avg, Stddev, Max)
Amazon, Salesforce, Box	ログインIP	(# of count, Avg, Stddev, Max)
Amazon, Salesforce, Box	失敗したログインIP	(# of count, Avg, Stddev, Max)
Box	ダウンロード	(# of count, Avg, Stddev, Max)
Box	ダウンロードIP	(# of count, Avg, Stddev, Max)
Salesforce	ブラウザ	(# of count, Avg, Stddev, Max)
Salesforce	一括削除、一括転送、データエクスポート	(# of count, Avg, Stddev, Max)
Salesforce	証明書およびキー管理	(# of count, Avg, Stddev, Max)
Salesforce	ネットワークアクセスおよびIPホワイトリスト変更	(# of count, Avg, Stddev, Max)
Salesforce	ユーザ変更管理	(# of count, Avg, Stddev, Max)
Salesforce	プラットフォーム	(# of count, Avg, Stddev, Max)
Salesforce	パスワードポリシー変更	(# of count, Avg, Stddev, Max)
Salesforce	共有設定変更	(# of count, Avg, Stddev, Max)
Amazon	EC2インスタンス変更	(# of count, Avg, Stddev, Max)
Amazon	セキュリティグループ変更	(# of count, Avg, Stddev, Max)
Amazon	SSHキーペア変更	(# of count, Avg, Stddev, Max)
Amazon	ネットワークACL変更	(# of count, Avg, Stddev, Max)
Amazon	VPN接続変更	(# of count, Avg, Stddev, Max)
Amazon	SAML変更	(# of count, Avg, Stddev, Max)
Amazon	VPC変更	(# of count, Avg, Stddev, Max)
Amazon	IAMアクセスキー変更	(# of count, Avg, Stddev, Max)

【0134】

以下の表 5 は、いくつかの可能な日次集計行列ベクトルの値の例を示す。ここに示す例のベクトルには、1日の1日あたりのログイン数（「logcntday_1dy」）、1日の1日あたりの失敗ログイン数（「logfailcntday_1dy」）、失敗ログインが1日にわたって発生したIPアドレスの1日あたりのカウント（「logfailipdisday_1dy」）、および1日にわたってログインに用いられたIPアドレスの1日あたりのカウント（「logipdisday_1dy」）が含まれる。

【0135】

10

20

30

40

50

【表 5】

表 5

ユーザID	logcntday_1dy	logfailcntday_1dy	logfailpdisday_1dy	logipdisday_1dy
ユーザ 1	5	4	3	2
ユーザ 2	6	2	2	1
ユーザ 3	4	3	2	2
ユーザ 4	4	4	2	1
ユーザ 5	5	5	1	1

10

【 0 1 3 6 】

さまざまな例では、挙動分析エンジン 3 0 4 によって判断されたアクティビティプロファイルを脅威検出エンジン 3 0 2 によって用いて、クラウドサービスを利用している組織に脅威を与える可能性があるクラウドサービスの利用を識別することができる。いくつかの例では、脅威検出エンジン 3 0 2 はセキュリティポリシーを適用して脅威を特定する。セキュリティポリシーは、発生すると組織ならびに / またはセキュリティ管理および制御システムに注意されるイベントを記述することができる。たとえば、セキュリティポリシーは、クレジットカード番号を含むファイルのダウンロード、暗号化キーのコピー、一般ユーザの特権の昇格など、組織の注意を引く必要があるアクションを指定することができる。一部の例では、セキュリティポリシーは、サービスへのアクセスのブロック、ユーザアカウントの無効化など、イベントが検出されたときに実行されるアクションを記述することもできる。

20

【 0 1 3 7 】

いくつかの例では、脅威検出エンジン 3 0 2 は、異常検出を実施して脅威を特定する。異常検出には、確立された標準からの統計的変動の検索が含まれ得る。いくつかの例では、脅威検出エンジン 3 0 2 の動作は、組織からの脅威インテリジェンスを含むことができるテナントベースライン 3 1 7 によって強化することができる。いくつかの例では、脅威検出エンジン 3 0 2 は、セキュリティ管理および制御システムによって維持される脅威インテリジェンスデータ 3 1 4、ならびに / または例えば脅威インテリジェンスアグリゲータもしくはディストリビュータからの脅威インテリジェンスを含むサードパーティデータ 3 1 8 を代替的または追加的に受信することができる。

30

【 0 1 3 8 】

以下に、異常検出に用いることができるさまざまなアルゴリズムの例を示す。これらのアルゴリズムは例として提供されており、他のアルゴリズムを用いることができる。

【 0 1 3 9 】

アルゴリズム 1 は、ログイン IP アドレス変動を判定するために用いることができるアルゴリズムの一例である。ログイン IP アドレス特徴ベクトルの Z スコアを、さまざまな期間にわたって計算することができる。次の例では、時間の異なる期間の例として 1 週間、4 週間、および 8 週間を用いており、3 つの Z スコアが得られる。

40

【 0 1 4 0 】

【数 5】

50

$$L1\ ZScore = \frac{\text{過去24時間のログインIP} - 1\text{週間平均ログインIP}}{1\text{週間標準偏差ログインIP}}$$

$$L2\ ZScore = \frac{\text{過去24時間のログインIP} - 4\text{週間平均ログインIP}}{4\text{週間標準偏差ログインIP}}$$

$$L3\ ZScore = \frac{\text{過去24時間のログインIP} - 8\text{週間平均ログインIP}}{8\text{週間標準偏差ログインIP}}$$

【0141】

Zスコアは、次のように、各スコアに割り当てられた重み（ $w_1 \dots w_3$ ）と組み合わせることができる。

【0142】

【数6】

$$L\ Combined = (w_1 \times L1\ ZScore) + (w_2 \times L2\ ZScore) + (w_3 \times L3\ ZScore)$$

【0143】

いくつかの例では、重みの合計は1である。適用される重みは、計算が実行されるタイミングに応じて動的に計算されてもよい。たとえば、1日目では、既存のデータに基づいて計算された値を用いてデフォルトのベースラインが適用され、デフォルトのAvg（平均）およびデフォルトのStddev（標準偏差）が含まれる。さらなる例として、2日目から始まる最初の週には、 $L1$ Zスコアが利用可能であるため、重みを $w_1 = 1$ 、 $w_2 = 0$ 、 $w_3 = 0$ に設定することができる。この例を続けると、5週間後、 $L1$ および $L2$ Zスコアが利用可能になり、重みを $w_1 = 0.4$ 、 $w_2 = 0.6$ 、 $w_3 = 0$ に設定することができる。14週間後、 $L1$ 、 $L2$ 、および $L3$ Zスコアが利用可能になり、重みを $w_1 = 0.2$ 、 $w_2 = 0.3$ 、 $w_3 = 0.5$ に設定することができる。ログインIPアドレスの変動の異常条件は、 $L_Combined > T$ として定義することができる。ここで、 T はしきい値である。しきい値は、以前のデータから判断することも、時間とともに変更することもできる。

【0144】

アルゴリズム2は、失敗したログインIPアドレスの変動を検出するために用いることができるアルゴリズムの例である。例として、1週間、4週間、および8週間として示されているさまざまな期間にわたって、ログインIPアドレス特徴ベクトルのZスコアを計算することができる。

【0145】

【数7】

$$L1\ ZScore = \frac{\text{過去24時間の失敗ログインIP} - 1\text{週間平均の失敗ログインIP}}{1\text{週間標準偏差の失敗ログインIP}}$$

$$L2\ ZScore = \frac{\text{過去24時間の失敗ログインIP} - 4\text{週間平均の失敗ログインIP}}{4\text{週間標準偏差の失敗ログインIP}}$$

$$L3\ ZScore = \frac{\text{過去24時間の失敗ログインIP} - 8\text{週間平均の失敗ログインIP}}{8\text{週間標準偏差の失敗ログインIP}}$$

10

20

30

40

50

【 0 1 4 6 】

失敗したログインIPアドレスのZスコアは、次のように、各スコアに割り当てられた重み ($w_1 \dots w_3$) と組み合わせることができる。

【 0 1 4 7 】

【 数 8 】

$$L_{Combined} = (w_1 \times L1_{ZScore}) + (w_2 \times L2_{ZScore}) + (w_3 \times L3_{ZScore})$$

【 0 1 4 8 】

さまざまな例において、適用される重みは、計算が実行されるタイミングに応じて動的に計算されてもよい。たとえば、1日目では、既存のデータに基づいて計算された値を用いてデフォルトのベースラインが適用され、デフォルトのAvg (平均) およびデフォルトのStddev (標準偏差) が含まれる。この例では、アルゴリズム1の例で示したように、週が進むにつれて重みを変えることができる。ログインIPアドレスの変動の異常条件は、 $L_{Combined} > T$ として定義することができる。ここで、Tはしきい値である。しきい値は、以前のデータから判断することも、時間とともに変更することもできる。

10

【 0 1 4 9 】

さまざまな例では、あるクラウドサービスのユーザについて検出された異常なアクティビティを脅威検出エンジン302が用いて、別のクラウドサービスの利用における脅威の可能性を計算または再計算することができる。このようにして、あるクラウドサービスの利用中に発生する新たなイベントを事前にスクリーニングして、別のクラウドサービスの利用における脅威を検出または予測することができる。さまざまな例において、さまざまなクラウドサービスにわたる複数のデータポイントを相互に関連付けて、脅威スコアの精度を高めることができる。

20

【 0 1 5 0 】

アルゴリズム3は、複数のアプリケーションの挙動の分析に用いることができるアルゴリズムの例を提供する。アルゴリズム3では、さまざまなクラウドサービスアクティビティ (ログインなど) に関連付けられたユーザIPアドレスが、ジオロケーション座標IP1 (緯度1、経度1)、IP2 (緯度2、経度2)、IP3 (緯度3、経度3) などに解決される。ユーザが異なるクラウドサービスで異なるユーザ名を有する場合、そのユーザに関連付けられているさまざまなユーザ名を、サービス全体でユーザを識別する一意のユーザ固有の素性にマッピングすることができる。いくつかのクラウドサービス (Amazon Web Services、Box、Salesforceなど) でのログイン (ログイン試行、ログイン成功、ログイン失敗など) に用いられる2つのIPアドレス間の距離を、さまざまな距離測定および/または数式を用いて計算することができる。いくつかの例では、距離dは、次のようにHaversine Distance式を用いて計算される。

30

【 0 1 5 1 】

【 数 9 】

40

$$Diff_{Long} = \text{経度}2 - \text{経度}1$$

$$Diff_{Latitude} = \text{緯度}2 - \text{緯度}1$$

$$a = \left(\sin\left(\frac{Diff_{Latitude}}{2}\right) \right)^2 + (\cos(\text{緯度}1) \times \cos(\text{緯度}2) \times \left(\sin\left(\frac{Diff_{Long}}{2}\right) \right)^2$$

$$c = 2 \times \text{atan2}(\sqrt{a}, \sqrt{1-a})$$

10

$$d = R \times c$$

【 0 1 5 2 】

d の方程式では、R は地球の半径である。

Z スコアを計算して、上記で計算した最大距離を用いて、さまざまな期間にわたるユーザの挙動の偏差を判断することができる。例として、1 週間、4 週間、および 8 週間の期間が示される。

【 0 1 5 3 】

【 数 1 0 】

20

$$L1 \text{ ZScore} = \frac{\text{過去 2 4 時間の最大距離 I P ログイン} - 1 \text{ 週間平均 (1 日あたりの最大距離 I P ログイン)}}{1 \text{ 週間標準偏差 (1 日あたりの I P ログイン I P 間の最大距離)}}$$

$$L2 \text{ ZScore} = \frac{\text{過去 2 4 時間の最大距離 I P ログイン} - 4 \text{ 週間平均 (1 日あたりの最大距離 I P ログイン)}}{4 \text{ 週間標準偏差 (1 日あたりの I P ログイン I P 間の最大距離)}}$$

$$L3 \text{ ZScore} = \frac{\text{過去 2 4 時間の最大距離 I P ログイン} - 8 \text{ 週間平均 (1 日あたりの最大距離 I P ログイン)}}{8 \text{ 週間標準偏差 (1 日あたりの I P ログイン I P 間の最大距離)}}$$

30

【 0 1 5 4 】

Z スコアは、次のように、各スコアに割り当てられた重み (w1 ... w3) と組み合わせることができる。

【 0 1 5 5 】

【 数 1 1 】

$$L \text{ Combined} = (w1 \times L1 \text{ ZScore}) + (w2 \times L2 \text{ ZScore}) + (w3 \times L3 \text{ ZScore})$$

【 0 1 5 6 】

さまざまな例において、適用される重みは、計算が実行されるタイミングに応じて動的に計算されてもよい。たとえば、1 日目では、既存のデータに基づいて計算された値を用いてデフォルトのベースラインが適用され、デフォルトの Avg (平均) およびデフォルトの Std dev (標準偏差) が含まれる。この例では、上で示したように、時間が進むにつれて重みを変えることができる。ログイン IP アドレスの変動の異常条件は、L Combined > T として定義することができる。ここで、T はしきい値である。しきい値は、以前のデータから判断することも、時間とともに変更することもできる。

40

【 0 1 5 7 】

アルゴリズム 4 は、クラウドアプリケーションへのアクセス時に用いられるブラウザまたはオペレーティングシステム (OS) の変動を判定するアルゴリズムの例を提供する。Z スコアは、さまざまな期間にアクセスが発生した、クラウドアプリケーションにアクセス

50

するときに用いられるさまざまなブラウザまたはオペレーティングシステムの数のカウントを表す特徴ベクトルを用いて計算することができる。例として、1週間、4週間、および8週間の期間を以下に用いる。

【 0 1 5 8 】

【 数 1 2 】

L1 ZScore

$$= \frac{\text{過去24時間の〔ブラウザ, OS〕カウント} - 1\text{週間平均 (1日あたりの〔ブラウザ, OS〕カウント)}}{1\text{週間標準偏差 (1日あたりの〔ブラウザ, OS〕カウント)}}$$

L2 ZScore

$$= \frac{\text{過去24時間の〔ブラウザ, OS〕カウント} - 4\text{週間平均 (1日あたりの〔ブラウザ, OS〕カウント)}}{4\text{週間標準偏差 (1日あたりの〔ブラウザ, OS〕カウント)}}$$

L3 ZScore

$$= \frac{\text{過去24時間の〔ブラウザ, OS〕カウント} - 8\text{週間平均 (1日あたりの〔ブラウザ, OS〕カウント)}}{8\text{週間標準偏差 (1日あたりの〔ブラウザ, OS〕カウント)}}$$

【 0 1 5 9 】

Zスコアは、次のように、各スコアに割り当てられた重み (w1 ... w3) と組み合わせることができる。

【 0 1 6 0 】

【 数 1 3 】

$$L\text{ Combined} = (w1 \times L1\text{ ZScore}) + (w2 \times L2\text{ ZScore}) + (w3 \times L3\text{ ZScore})$$

【 0 1 6 1 】

さまざまな例において、デフォルトのベースラインを最初に適用することができ、時間が経過するにつれて、利用可能なデータが増えるにつれて重みを変えることができる。ログインIPアドレスの変動の異常条件は、 $L\text{ Combined} > T$ として定義することができる。ここで、Tはしきい値である。しきい値は、以前のデータから判断することも、時間とともに変更することもできる。

【 0 1 6 2 】

アルゴリズム5は、クラウドアプリケーションからのダウンロード数の変動を判断するためのアルゴリズムの例を提供する。Zスコアは、次の例に示すように、1週間、4週間、8週間など、さまざまな期間にわたるユーザアカウントのダウンロード数のカウントを表す特徴ベクトルを用いて計算することができる。

【 0 1 6 3 】

【 数 1 4 】

$$L1\text{ ZScore} = \frac{\text{過去24時間のダウンロードカウント} - 1\text{週間平均 (1日あたりのダウンロードカウント)}}{1\text{週間標準偏差 (1日あたりのダウンロードカウント)}}$$

$$L2\text{ ZScore} = \frac{\text{過去24時間のダウンロードカウント} - 4\text{週間平均 (1日あたりのダウンロードカウント)}}{4\text{週間標準偏差 (1日あたりのダウンロードカウント)}}$$

$$L3\text{ ZScore} = \frac{\text{過去24時間のダウンロードカウント} - 8\text{週間平均 (1日あたりのダウンロードカウント)}}{8\text{週間標準偏差 (1日あたりのダウンロードカウント)}}$$

【 0 1 6 4 】

Zスコアは、次のように、各スコアに割り当てられた重み ($w_1 \dots w_3$) と組み合わせることができる。

【 0 1 6 5 】

【 数 1 5 】

$$L_{Combined} = (w_1 \times L_1 \text{ ZScore}) + (w_2 \times L_2 \text{ ZScore}) + (w_3 \times L_3 \text{ ZScore})$$

【 0 1 6 6 】

さまざまな例において、デフォルトのベースラインを最初に適用することができ、時間が経過するにつれて、利用可能なデータが増えるにつれて重みを変えることができる。ログインIPアドレスの変動の異常条件は、 $L_{Combined} > T$ として定義することができる。ここで、 T はしきい値である。しきい値は、以前のデータから判断することも、時間とともに変更することもできる。

10

【 0 1 6 7 】

さまざまな例では、上記のスコアなどのスコア、およびその他のインジケータを用いて、リスクスコアを計算することができ、それをここではセキュリティの尺度とも呼ぶ。さまざまな例では、脅威検出エンジン 3 0 2 は、ユーザ、ユーザのグループもしくはカテゴリ、サービス、および/またはサービスプロバイダのリスクスコアを計算することができる。リスクスコアは、セキュリティリスクの程度を示すことができる。たとえば、1 ~ 5 のスケールを定義することができる。値が大きいほど、ユーザまたはサービスが組織にとってより高いセキュリティリスクを呈することを示す。

20

【 0 1 6 8 】

リスクスコアの計算に用いられるインジケータは、特定のリスク要因をスコアの形式でも提供することができる。たとえば、異常検出の結果には、標準からの逸脱の程度および/または異常が組織にもたらすリスクの程度を示すスコア形式のインジケータを含めることができる。一部の例では、同じユーザまたは同じサービスに関連付けられた各異常を個別のインジケータとして用いることができる。さまざまな例において、リスクスコアの計算に用いることができる他のインジケータは、ユーザ、サービス、サービスプロバイダ、ユーザがいると思われるジオロケーション、ユーザがいると思われるドメイン、時刻もしくは曜日もしくは時節、または別の要因に関連付けられることができる。ユーザのインジケータは、たとえば、ユーザが関連付けられている組織、評判サイト、ソーシャルメディアサイト、ニュース組織、または別のソースから取得することができる。サービスまたはサービスプロバイダのインジケータは、たとえば、サービスもしくはサービスプロバイダの評判を追跡することができる脅威インテリジェンスアグリゲータまたはディストリビュータから取得することができる。他のインジケータは、内部脅威インテリジェンスデータ 3 1 4 によって提供されてもよい。

30

【 0 1 6 9 】

さまざまな例において、リスクスコアは、利用可能なインジケータの加重合計として計算することができる。たとえば、インジケータ「 I_1, I_2, \dots, I_n 」が与えられるとして、次の方程式を用いてリスクスコアを計算することができる。

40

【 0 1 7 0 】

【 数 1 6 】

$$\text{リスクスコア} = \frac{I_1 W_1 + I_2 W_2 + \dots + I_n W_n}{W_1 + W_2 + \dots + W_n}$$

【 0 1 7 1 】

上記の方程式では、「 W_1, W_2, \dots, W_n 」は重みである。さまざまな例において、重み値はインジケータの相対的な重要度を示し、重要度の低いインジケータは低い重み値を受

50

け取る。

【 0 1 7 2 】

いくつかの例では、分析エンジン 3 0 0 は、リスクスコアの有効性および / または精度に関するフィードバックを取得してもよい。例として、組織のネットワーク管理者はフィードバックを提供することができる。別の例として、セキュリティ管理および制御システムの管理者がフィードバックを提供することができる。代替的または追加的に、いくつかの例では、決定木およびニューラルネットワークなどの自動化された機械学習アルゴリズムを用いてフィードバックを取得することができる。いくつかの例では、分析エンジン 3 0 0 は、フィードバックを用いて、おそらくソースまたはインジケータを削除することを含めて、重み、インジケータ、および / またはソースを調整することができる。これらおよび他の例では、脅威検出エンジン 3 0 2 は、調整されたインジケータおよび重みを用いて新たなリスクスコアを計算することができる。

10

【 0 1 7 3 】

さまざまな例において、脅威検出エンジン 3 0 2 は、リスクスコアを計算するために用いられる各インジケータおよび / またはリスクスコアに対して回帰分析を実行することができる。回帰分析には、線形回帰モデルの構築および更新が含まれてもよい。線形回帰モデルは、 $S = c_1(I_1) + c_2(I_2) + \dots + c_n(I_n)$ などの出力を提供してもよい。回帰モデルによって計算される係数 c_i は、リスクスコアを計算するための初期の重みを置き換える新たな重みまたは修正された重みである可能性がある。モデルは、より多くのフィードバックおよびより多くのデータが収集されるにつれ、より高い精度を提供することができる。

20

【 0 1 7 4 】

さまざまな例では、分析エンジン 3 0 0 は、サービスプロバイダから取得したアクティビティデータ 3 1 0 に対してさまざまな他の分析 3 0 6 を実行することができる。いくつかの例では、さまざまなタイプのアルゴリズムがデータの分析に特に有用である。決定木、時系列、単純ベイズ分析、およびユーザ挙動プロファイルの構築に用いられる手法は、不審なアクティビティのパターンおよび / または外部データフィールドに基づいて予測を生成するために用いることができる機械学習手法の例である。クラスタリングなどの手法を用いて、外れ値や異常なアクティビティを検出することができる。たとえば、脅威は、1 つ以上のファイルにアクセスするアカウント、または (サードパーティのフィードなどによって) 悪意があるとフラグが付けられた IP アドレスからの一連のログイン試行に失敗したアカウントに基づいて識別することができる。同様に、脅威は、1 つのクラウドアプリケーションまたは複数のクラウドアプリケーションでのおそらくは経時的なアクティビティの異なるパターンに基づき得る。

30

【 0 1 7 5 】

生成され得る分析の 1 つのクラスに、記述的分析または統計的分析がある。統計データは、たとえば、MapReduce ジョブおよび Spark and Apache Hive クエリなど、システムクエリの事前定義されたセットを使用して生成できる。記述的分析は、1 つのサービス、または、相関分析技術を使用して複数のサービス間について生成できる。生成できるレポートには、たとえば、ログイン統計データ (たとえば、ログインに最も多く失敗したユーザ、IP アドレスの評判の考慮を含む IP アドレスベースのログイン履歴、地理的位置、および他の要因)、ユーザ統計データ (たとえば、最も多くのリソース [ファイル、EC2 マシンなど] を有するユーザ、クラウド間のエンタイトルメント、変更されたパスワードの数など)、アクティビティ統計データ (たとえば、クラウド間のユーザのアクティビティ)、キーローテーションについての統計データ (たとえば、過去 30 日以内に Secure Shell (SSH) キーがローテーションされたかどうかなど)、およびリソース統計データ (たとえば、ユーザがダウンロードしたフォルダ数、ファイル数、ローミングまたはモバイルユーザがダウンロードしたファイル数など) などが挙げられる。平均、標準偏差、回帰、サンプルサイズの決定、仮説検定など、さまざまな統計分析手法を用いることができる。特定の時間内のログインアクティビティ、パスワード関連のサポート問題の過去の履

40

50

歴に基づくこのような問題、または特定の時間内で最も多くのアクティビティを見たモバイル機器の識別タイプなどのトレンドが特定されてもよい。レポートに含まれるデータは、イベントビューアとして、イベントの「壁」を、ユーザがイベントに対して講ずることのできる操作またはイベントを救済するための操作とともに表示するユーザインタフェース上に表示され得る。具体的なイベントおよびしきい値を含み得る既定のルールに基づいて、アラートを構成できる。

【0176】

生成され得る別の部類の分析として、予測分析およびヒューリスティック分析がある。これらは、機械学習アルゴリズムを組み込んで、たとえば、基準となる期待値からの偏差、めったに起こらないイベント、およびユーザの怪しい挙動を得るための挙動分析などの脅威モデルを生成してもよい。普通でない挙動がセキュリティリスクであるかどうかをインテリジェントに予測するようにアルゴリズムおよびプロファイルを訓練できる。これらに限定されないが、IP (Internet Protocol) アドレスの評判、マルウェア、感染したノードポイントのID、脆弱なウェブブラウザのバージョン、ユーザによるプロキシサーバまたはVPNサーバの使用、およびクラウドに対する既知の攻撃など、潜在的なセキュリティ脅威の外部情報および潜在的なセキュリティ脅威に関する外部情報を提供することによって、これらに限られないが、MaxMind、FireEye、Qualys、Mandiant、AlienVault、およびNorse STIXなどのプロバイダからのサードパーティフィードを統合して、脅威インテリジェンスを強化することができる。これらのサードパーティフィードは、たとえば、IPアドレス評判、マルウェア、感染ノードポイントの識別、脆弱なウェブブラウザバージョン、ユーザによるプロキシまたは仮想プライベートネットワーク (VPN) サーバの使用、クラウドに対する既知の攻撃など、潜在的なセキュリティ脅威に関する外部情報を提供することができる。一部の例では、脅威情報は、Structured Threat Information eXpression (STIX) データフォーマットで表される。たとえば、1つ以上のサービスが、評判（たとえば、ソフトウェア脆弱性がある、悪意のあるソフトウェアのホストである、または攻撃のソースであると知られている）および/またはIPアドレスに対応付けられた地理的位置など、特定のIPアドレスに関する情報を提供してもよい。この情報は、何時にそのIPアドレスからログインが試みられたかなど、IPアドレスを伴う取り出されたアクティビティデータ、および、ログインの試みの間隔など、アクティビティデータから得られた情報と組み合わせることができる。これらの要因を用いて、「ログイン速度 (login velocity)」評価指標を決定することができる。ファイルアクセス、売買取引、または仮想マシンのインスタンスなど、他のアクティビティの評価指標を決定することができる。

【0177】

クラスタリングアルゴリズムおよび回帰アルゴリズムを使用して、データを分類して、共通のパターンを見つけることができる。たとえば、クラスタリングアルゴリズムは、モバイルデバイスからログインしているユーザのすべてのエントリを集約することによって、データをクラスタにすることができる。また、予測分析は、ユーザが特定のクラウドアプリケーションに数か月アクセスしていなかった後、翌月に高いアクティビティを示す、または、ユーザが過去数週間にわたって、毎週1つのファイルをダウンロードしているなど、潜在的なAPT攻撃 (Advanced Persistent Threat) のシナリオを示すアクティビティに基づいて脅威を特定することを含み得る。いくつかの例において、時間とともに収集されたデータを使用して、正常な挙動（たとえば、イベントおよびアクティビティのパターン）のモデルを作成し、通常から逸脱した挙動を異常挙動としてフラグを立てる。フラグが立てられている1つ以上のイベントまたはアクティビティが、（たとえば、ユーザフィードバックによって）真または偽陽性であるとみなされた後、情報を1つ以上の機械学習アルゴリズムに戻してシステムのパラメータを自動的に変更することができる。したがって、機械学習アルゴリズムを少なくとも上述の方法で利用して、推奨を作成し、偽警報（偽陽性）を減らすことができる。時間とともにさまざまなパラメータから収集されたアクティビティデータを機械学習アルゴリズムとともに使用して、ユーザ挙動プロファイ

10

20

30

40

50

ルと称されるパターンを生成することができる。アクティビティデータは、IPアドレスおよび地理的位置などの背景情報を含み得る。

【0178】

さまざまな実現例において、アルゴリズムは以前に取得したユーザアクティビティデータを用いて通常のユーザアクティビティをシミュレートすることができる。例えば、テナントベースライン317は、クラウドサービスのユーザによる過去の利用のレコードを含むことができる。シミュレーションを用いて、組織のユーザの通常の挙動を学習するよう、他の機械学習アルゴリズムをトレーニングすることができる。一般に、ある特定のセキュリティ問題が常に繰り返されるとは限らないかもしれないが、したがって、純粋に監視されたアルゴリズムでは検出されないかもしれない。しかしながら、外れ値の検出などの手法により、異常なアクティビティの検出に役立つベースラインを確立することができる。このような異常なアクティビティと状況に応じた脅威インテリジェンスにより、予測誤りの少ない、より正確な脅威予測を行なうことができる。

10

【0179】

さまざまな実現例において、他の分析306は、セキュリティ制御ドリフトの検出を含むことができる。セキュリティ制御ドリフトは、一見任意の方法で1つ以上のセキュリティ制御を変更することを指し得、それはセキュリティリスクを増大させ得る。いくつかの例では、リスクイベントは、クラウドサービスのセキュリティ制御の変更、およびリスクイベントに関連付けられるアクション可能なインテリジェンスに応答して生じ得る。脅威には、アプリケーションの使用に関して異常な、または準拠していない、アクティビティ、イベント、またはセキュリティ制御が含まれ得る。例として、クラウドアプリケーションでのテナントのパスワードポリシーが変更され、要件が少なくなっている場合がある（たとえば、文字のタイプおよび/または数）。これにより、リスクイベントが生じ、パスワードポリシーを元のパスワードポリシーに戻すことを推奨するアラートが生成される。

20

【0180】

さまざまな実現例において、分析エンジン300は、脅威検出エンジン302、挙動分析エンジン304、および他の分析306の出力を受け取る推奨エンジン308を含むことができる。さまざまな例において、推奨エンジン308は、アラート322を発し、推奨324を行い、アクション326を自動的に実行し、組織のクラウドサービスの利用、検出されたセキュリティリスク、およびセキュリティリスクの是正などを理解するために組織が利用することができる視覚化328を提供することができる。

30

【0181】

さまざまな例において、アラート322は、組織がアクセス可能なユーザインターフェースを用いて見ることができる視覚化328で提供され得る。代替的または追加的に、アラート322は、電子メール、テキストメッセージ、ショートメッセージサービス(SMS)メッセージ、ボイスメール、または別の通信方法などの他の通信チャネルを通じて提供することができる。いくつかの例では、アラート322は、安全なメッセージとして通信することができる（たとえば、安全な通信チャネルを介して、または見るためにキーもしくはログインクレデンシャルを要求する）。

【0182】

40

アラートは、たとえば、イベント識別子、日付、時間、リスクレベル、イベントカテゴリ、イベントに対応付けられたユーザアカウントおよび/もしくはセキュリティ制御、イベントに対応付けられたサービス、イベントの説明、救済タイプ（たとえば、手動または自動）、ならびに/またはイベントのステータス（たとえば、未解決、解決済み）など、検出されたイベントについての情報を含み得る。各リスクイベントについてのアラートに含まれる情報は、たとえば、影響を受けたクラウドサービスおよびインスタンスについての識別子(ID)、カテゴリ、優先事項、日時、記述、推奨される救済タイプ、ならびに/またはステータスなどの情報を含み得る。また、リスクイベントは、編集、削除、ステータスを完了にする、および/または救済アクションを実行するなど、ユーザが選択可能なアクションを有してもよい。救済アクションの選択によって、選択された救済を実行す

50

るために、インシデント救済アプリケーションおよび/またはクラウドシードアプリケーションなどのアプリケーションが呼び出されてもよい。セキュリティ監視および制御システムの外部のエンティティに、アラートおよび/または特定された脅威に関する他の情報を送信することができる。

【0183】

いくつかの例では、さまざまなイベントカテゴリのイベントの経時的なカウントをチャートなどのグラフィカルな視覚化として提供することができる。チャートには、たとえば、通常でない時間でのアクティビティ、営業時間外のダウンロード、ログインの失敗など、色分けされた各カテゴリにおける日付ごとのイベント数が表示されてもよい。イベントカテゴリの視覚的表現（線など）は、オンとオフとを切り替えることができる。いくつかの例では、脅威も概要ビューに表示することができる。

10

【0184】

いくつかの例では、組織のネットワーク管理者がアラート322を受信すると、ネットワーク管理者は組織のネットワーク内から救済アクションを実行してもよい。これらの例では、セキュリティ管理および制御システムは、ネットワーク管理者がアラートを閉じることができるまで、アラートを「作動」状態に維持してもよい。

【0185】

さまざまな例において、推奨エンジン308は、脅威検出エンジン302または他の分析306が注意を要するイベントにフラグを立てたときに推奨324を判断することもできる。推奨には、疑わしいイベントをさらに調査したり、疑わしいイベントを修正したりする（たとえば、是正措置を取る）ために実行することができるアクションが含まれる。さまざまな例において、推奨324は、ユーザインターフェースにおいて提示される視覚化328で組織のネットワーク管理者に提示することができる。代替的または追加的に、推奨324は、電子メール、テキストメッセージ、ショートメッセージサービス（SMS）メッセージ、ボイスメールなどのような他の通信形態を通じて提示することができる。さまざまな例において、組織のネットワーク管理者は、推奨されるアクションをアクティブにすることを選択することができる。これにより、セキュリティ管理および制御システムはアクションを実行することができる。

20

【0186】

さまざまな例において、推奨エンジン308は、関連ルール学習を用いて推奨を生成することができる。一部の例では、推奨エンジン308は、プロファイルリンクアルゴリズムを用いて、クロスサービス相関を見つけることにより、複数のクラウドアプリケーション全体のアクティビティをリンクすることができる。複数のクラウド全体で共通に用いられるプライマリユーザ識別子やシングルサインオン（SSO）認証メカニズム（Active Directory、Oktaなど）などの1つ以上の属性または識別要素を用いて、単一のユーザを複数のクラウドサービスにわたって識別することができる。アプリケーション間でのアクティビティの相関の例は、異なるIPアドレスから同時に2つのクラウドサービスにログインしているユーザ、複数回のログイン試行の失敗後にパスワードを変更したユーザ、2つ以上のクラウドサービスに対する多数のログイン失敗が頻繁にあるユーザを見つけるなどする。

30

40

【0187】

さまざまな例では、推奨エンジン308は、セキュリティ管理および制御システムが自動的に実行する救済アクションを含むアクション326を判断することもできる。さまざまな例において、組織は、分析エンジン300が特定のセキュリティイベントを検出したときに救済アクションを自動的に実行するように構成することができる。救済アクションの例には、アカウントの無効化、パスワードのリセット、またはより強力なセキュリティ制御の設定などが含まれる。これらの例および他の例では、救済アクションには、セキュリティインシデントの影響を受けるサービスまたは別のサービスのセキュリティ設定の変更が含まれてもよい。後者の場合、分析エンジン300は、セキュリティインシデントが検出されたときに他のサービスが影響を受ける可能性があるか、そうでなければセキュリテ

50

ィで保護する必要があると判断してもよい。

【0188】

一部の例では、組織は、たとえばServiceNowやIBM（登録商標）QRadarなどのサードパーティのインシデント管理自動化システムを用いる場合がある。これらの例では、セキュリティ管理および制御システムがサードパーティのインシデント管理システムとインターフェースして、セキュリティインシデントを救済することができてよい。たとえば、インシデント管理システムは、セキュリティ管理および制御システムがインシデント管理システムとインターフェースすることができるAPIを有してもよい。この例および他の例では、推奨エンジン308によって判断されるアクションは、セキュリティインシデントに関するアラートおよび/または他の情報をインシデント管理システムに送信することを含み、インシデント管理システムはインシデントを追跡し、場合によっては修正することもできる。インシデント管理システムは、セキュリティ管理および制御システムにステータスを返してもよい（たとえば、完了または未完了）。このようにして、救済が外部システムに委任され、結果がセキュリティ管理および制御システムに報告されて「ループを閉じる」。たとえば、ユーザアカウントのパスワードのリセットが所望される場合、アクションには、ユーザアカウントを管理する組織の内部ITシステムへのアラートまたはメッセージの送信が含まれ得る。管理者またはシステムはパスワードリセット操作を完了し、ステータスを完了としてクラウドセキュリティシステムに報告してもよい。

10

【0189】

さまざまな例において、クラウドサービスは、管理ユーザをサービスの一般ユーザと区別する特権を定義することができる。より大きな、またはより多くの特権を有することにより、管理ユーザは組織のクラウドサービスを構成および管理することができるが、通常のユーザはクラウドサービスを利用することしかできない。

20

【0190】

上記で説明したように、クラウドサービスの特権ユーザを識別することは簡単ではない場合がある。たとえば、各クラウドサービスには、1人のユーザを管理ユーザとして資格を与え、別のユーザを通常のユーザとする、特権の、異なる定義があり得る。別の例として、クラウドサービスの管理ユーザは時間の経過とともに変わる場合があり、新たな管理ユーザが、組織によって制御されない態様および時間で作成される場合がある。別の例として、組織の従業員が職務を辞任または変更すると、どのユーザアカウントが特権を有するかに関する知識が失われる可能性がある。

30

【0191】

さまざまな実現例において、セキュリティ管理および制御システムは、クラウドサービスの特権ユーザを識別するための技術を実現することができる。特権ユーザのアクティビティは、挙動分析、異常検出、機械学習技術など、上記で説明したような方法を用いて追跡することができ、特権アカウントが悪用された場合に発生し得る、より大きな被害に見合った、より高度な精査が適用される。

【0192】

さまざまな実現例において、特権ユーザの識別は、セキュリティ管理および制御システムの分析エンジンのコンポーネントになり得る。図4は、挙動分析エンジン404のブロック図を示し、これは特権ユーザの識別を実現することができる分析エンジンの1つのコンポーネントの例である。さまざまな例では、挙動分析エンジン404は、1つのクラウドサービスまたは複数のクラウドサービスのユーザアクティビティのレコードを含むことができるアクティビティデータ410を受け取ることができる。アクティビティデータ410は、例えば、実行されたアクションのリスト、アクションを実行したユーザ、アクションの影響を受ける1つ以上のオブジェクト、タイムスタンプなどのコンテキストデータ、および/またはユーザがアクション実行したネットワーク位置などを含むことができる。

40

【0193】

さまざまな例において、挙動分析エンジン404は、統計データ分析エンジン432を含むことができ、これはアクティビティデータ410の統計分析を行うことができる。さま

50

さまざまな例において、統計分析エンジン 4 3 2 は、組織のユーザがクラウドサービスまたは複数のクラウドサービスを利用する態様を記述することができる挙動モデル 4 4 2 を出力することができる。例えば、統計分析エンジン 4 3 2 は、特定のユーザによるクラウドサービスの利用、ユーザグループによるクラウドサービスの利用、および / または組織内のすべてのユーザによるクラウドサービスの利用を記述するモデルを出力することができる。別の例として、統計分析エンジン 4 3 2 は、クラウドサービスが組織のユーザによって利用される態様を記述するモデル、および / または複数のクラウドサービスが組織の 1 人以上のユーザによって用いられる態様を記述するモデルを出力することができる。さまざまな例において、統計分析エンジン 4 3 2 は、ユーザ、クラウドサービスの利用におけるユーザのアクション、および / またはクラウドサービスの利用の態様を記述する他のモデルを出力することができる。

10

【 0 1 9 4 】

さまざまな例では、挙動分析エンジン 4 0 4 は、クラウドサービスの特権ユーザ 4 4 4 のリストを生成することができる特権ユーザ識別エンジン 4 3 4 も含むことができる。さまざまな例では、特権ユーザ識別エンジン 4 3 4 は、異なる技術を、おそらく組み合わせて用いることにより、クラウドサービスの特権ユーザを識別することができる。

【 0 1 9 5 】

第 1 の例として、特権ユーザ識別エンジン 4 3 4 は、クラウドサービスの管理ユーザであるユーザのユーザ名のリストを含むことができるテナントベースライン 4 1 7 から特権ユーザの素性を学習することができる。さまざまな例では、組織は、クラウドサービスの管理ユーザのリストを有してもよい。たとえば、組織が Salesforce などのサービスに登録する場合、組織はどのユーザを管理ユーザにするかを Salesforce に指定することができる。場合によっては、組織はサービスの管理ユーザを変更し、セキュリティ管理および制御システムに管理ユーザの更新されたリストを提供することができる。しかしながら、多くの場合、組織にはクラウドサービスの管理ユーザを追跡するための適切なプロセスが適所になく、テナントベースライン 4 1 7 で正確なリストを提供できない場合がある。

20

【 0 1 9 6 】

第 2 の例として、特権ユーザ識別エンジン 4 3 4 は、サービスプロバイダから取得されるサービスプロバイダデータ 4 1 8 から特権ユーザの素性を学習することができる。サービスプロバイダは、セキュリティ管理および制御システムがサービスの特権ユーザのリストを要求することができるようにする機能を含むことができる API を有する。さまざまな例では、セキュリティ管理および制御システムは、サービスの特権ユーザが変わる場合に、この要求を定期的に行うことができる。しかしながら、多くのクラウドサービスはこの機能を提供しないかもしれない。代替的または追加的に、クラウドサービス自体の特権ユーザの定義が狭すぎて、サービスの他のユーザまたはサービスの操作に影響を与える可能性のある操作を除外するかもしれない。

30

【 0 1 9 7 】

さまざまな実現例では、テナントベースライン 4 1 7 および / またはサービスプロバイダデータ 4 1 8 に依存することに加えて、またはその代わりに、特権ユーザ識別エンジン 4 3 4 は学習技術を用いてクラウドサービスからのアクティビティデータ 4 1 0 から特権ユーザを判断することができる。これらの実現例では、特権ユーザ識別エンジン 4 3 4 は、教師あり学習エンジン 4 3 6 および / または教師なし学習エンジン 4 3 8 を含むことができる。

40

【 0 1 9 8 】

さまざまな実現例において、教師あり学習エンジン 4 3 6 は、組織ならびに / またはセキュリティ管理および制御システムのオペレータからトレーニングデータを受け取ることができる。さまざまな例において、トレーニングデータには、クラウドサービスで実行することができるアクションの一部またはすべて、およびアクションが特権であるかどうかを示すアクションのラベルを含めることができる。いくつかの例では、ラベルは異なるカテゴリの特権を示している場合がある。たとえば、ある特権セットは管理特権であり、別の

50

特権セットは共同管理特権である場合がある。さまざまな例において、教師あり学習エンジン 4 3 6 は、トレーニングデータを用いて、ニューラルネットワークまたはランダムフォレストまたは別の分類モデルなどの分類モデルを訓練することができる。

【 0 1 9 9 】

さまざまな例において、教師あり学習エンジン 4 3 6 は、サービスからのアクティビティデータ 4 1 0 に分類モデルを適用することができる。一般的に、分類モデルは、同じクラウドサービスのアクティビティデータに対応するトレーニングデータから生成される（たとえば、トレーニングデータは、クラウドサービスを利用して実行することができるアクションから開発される）。分類モデルを用いて、教師あり学習エンジン 4 3 6 は、たとえば、特権アクションを含むアクティビティログのイベントを抽出することができる。アクティビティログはユーザを各イベントとともにリストすることができるため、教師あり学習エンジン 4 3 6 は、そのイベントを開始したユーザが特権ユーザである可能性が高いと判断することができる。さまざまな例では、アクション以外の、またはアクションに加えて、基準を用いて、イベントが特権ユーザによって実行されたと判断することができる。たとえば、イベントの特権的な性質は、アクションによって影響を受けるリソース、アクションがリソースに影響を与える態様、アクションが実行された回数、アクションが実行された時間、イベントが開始された IP アドレス、およびその他の基準で示すことができる。

10

【 0 2 0 0 】

さまざまな例において、教師あり学習エンジン 4 3 6 によって行われた判定の精度は、組織ならびに / またはセキュリティ管理および制御システムのオペレータからフィードバックを取得することによって検証および改善することができる。例えば、挙動分析エンジン 4 0 4 は、教師あり学習エンジン 4 3 6 によって識別された特権ユーザ 4 4 4 のリスト、およびこれらのユーザを特権を有するとして識別した、特権ユーザが実行したアクションを出力することができる。レビューは、セキュリティ管理および制御システムに、ユーザおよび / またはユーザが特権を有すると特定したアクションが正しいかどうかを示すことができる。この情報は、教師あり学習エンジン 4 3 6 にフィードバックすることができ、それは、適切な分類モデルを更新することができる。

20

【 0 2 0 1 】

さまざまな実現例において、教師なし学習エンジン 4 3 8 は、特権のあるアクションの学習を試み、この学習から特権ユーザを特定することができる。教師なし学習エンジン 4 3 8 は、例えば、アクティビティデータ 4 1 0 内のイベントを解析し、イベントの成分を特徴セットとして保存することができる。たとえば、教師なし学習エンジン 4 3 8 は、「アクション」、「アクションタイプ」、「ユーザ ID」、「タイムスタンプ」、「影響を受けるリソース」などのフィールド、およびイベントの他の成分の他のフィールドを有するデータ構造を用いて、特徴セットを表すことができる。さらなる例として、教師なし学習エンジン 4 3 8 は、毎日、毎週、または異なる期間のイベントを集約し、このようにしてクラウドサービスの履歴イベントデータの本体を収集することができる。さまざまな例において、教師なし学習エンジン 4 3 8 は、とりわけ異常検出およびニューラルネットワークなどのさまざまな教師なし学習技術を、蓄積された特徴セットに適用することができる。

30

40

【 0 2 0 2 】

一例として、K - m e a n s クラスタを特徴セットに適用して、アクティビティデータ 4 1 0 内のクラスタを識別することができる。クラスタは特権ユーザおよび一般ユーザをグループ化することができる。いくつかの例では、教師なし学習エンジン 4 3 8 に、特権のあるアクションのリスト、特権ユーザのみがアクセスすべきリソースのリスト、または教師なし学習エンジン 4 3 8 が特権ユーザのクラスタを特定するために用いることができるその他の基準を提供することができる。代替的または追加的に、教師なし学習エンジン 4 3 8 は、セキュリティ管理および制御システムのオペレータに提示され、オペレータは、次いで、特権ユーザのクラスタを識別し、クラスタから特権ユーザの特性を記述するモデルを定義することができる。

50

【 0 2 0 3 】

以下の表 6 は、ユーザのグループによって毎日実行される平均カウントアクションの例を示す。この例では、アクションにはファイル共有が含まれ、ファイル共有アプリケーションでユーザアクションを作成する。

【 0 2 0 4 】

【表 6】

表 6

ユーザ	ファイル共有イベント#	ユーザ作成イベント#
John	3	0
Mary	6	0
Bill	2	0
Kumar	4	0
Chi	0	0
Jose	11	0
Colin	9	0
Sean	20	1
Mike	19	1
Steve	17	1
Alexi	18	3
Samantha	20	3
Josh	16	2
Jenny	21	2

【 0 2 0 5 】

図 5 は、表 6 のデータのグラフ 5 0 0 の例を示す。水平軸 5 0 2 はファイル共有イベントのカウントをマッピングし、垂直軸はユーザ作成イベントのカウントをマッピングする。表 6 のデータによると、第 1 のユーザのグループはファイル共有イベントのみを実行したため、これらのユーザのデータポイントはすべてゼロのユーザ作成イベントの行に沿っている。第 2 のユーザのグループは、ファイル共有イベントおよびユーザ作成イベントの両方を実行したため、これらのユーザのデータポイントは、水平方向および垂直方向の両方でゼロより大きい。

【 0 2 0 6 】

図 5 の例に示されるように、ユーザの 2 つのクラスタが明らかである。第 1 のクラスタは、ユーザ Sean、Mike、Steve、Alexi、Samantha、Josh、および Jenny を含み、同じアクションを実行したためにユーザの 1 つのグループを形成する。ユーザ John、Mary、Bill、Kumar、Chi、Jose、および Colin を含む第 2 のクラスタは、これも同じアクションを実行したことにより、ユーザの第 2 のグループを形成する。この例では、第 1 のグループのユーザは、ユーザ作成イベントを実行したために、特権ユーザであると識別することができる。さまざまな例において、特権ユーザのグループとしての第 1 のクラスタの識別は、特権と見なされるアクティビティの記述から、および / またはクラスタリングツールの出力の分析を担当するオペレータによって判定することができる。

【 0 2 0 7 】

さまざまな例では、アクションだけでは、アクションを実行したユーザが特権ユーザであるかどうかを示さない場合がある。たとえば、ファイル共有サービスでは、一部のファイルフォルダには「機密」などのキーワードがタグ付けされている場合があるが、他のファイルフォルダは、異なるタグを有するか、またはタグを有さない。この例では、「機密」とタグ付けされたフォルダに関連するイベントの一部またはすべてが特権イベントであり得る。たとえば、「機密」というタグが付いたフォルダ内のファイルを読み取るユーザは、特権ユーザと見なされてもよい。別の例として、「機密」とタグ付けされたフォルダ内

に新たなファイルを追加したり、ファイルを削除したりすることができるユーザのみを、特権を有すると見なしてもよい。別の例として、異なるタグを有するフォルダまたはタグのないフォルダにのみアクセスするユーザは、通常の特権ユーザと見なされてもよい。

【0208】

図6は、クラウドサービスの特権ユーザを判定し、特権ユーザのアクティビティが引き起こし得るセキュリティリスクを管理するプロセス600の例を示すフローチャートを含む。さまざまな例では、例示的なプロセス600は、セキュリティ管理システムのコンピューティングシステムによって実行することができる。さまざまな例において、プロセス600は、プロセス600のステップを実行するためにコンピューティングシステムの1つ以上のプロセッサによって実行され得る、非一時的なコンピュータ可読媒体に格納される命令として具現化され得る。

10

【0209】

ステップ602で、プロセス600は、サービスプロバイダシステムからアクティビティデータを取得することを含み、アクティビティデータは、クラウドサービスの利用中に実行されるアクションを記述し、アクションは、テナントに関連付けられた1人以上のユーザによって実行され、サービスプロバイダシステムはテナントにテナントアカウントを提供し、テナントアカウントにより、1人以上のユーザはクラウドサービスにアクセスすることができる。いくつかの例では、テナントは、共通の目的を果たすために人およびリソースをまとめる組織であることができる。組織の例には、企業、大学、病院、行政機関、その他の人々およびリソースのグループが含まれる。いくつかの例では、テナントはネットワークサービスを利用する個人である場合がある。さまざまな例において、組織または個人は、サービスプロバイダのサービスに加入し、加入により、サービスプロバイダが提供するサービスを利用することができる。クラウドサービスの例には、インフラストラクチャ、プラットフォーム、ネットワーク、ソフトウェアアプリケーションなどが含まれる。

20

【0210】

さまざまな例では、加入すると、テナントには、テナントがサービスにアクセスすることを可能にするテナントアカウントが提供される。一部の例では、テナントに関連付けられるユーザに、サービスの個別のユーザアカウントを付与することができる。これにより、各ユーザはサービスを利用することができるようになる。これらの例および他の例では、ユーザがサービスを利用すると、サービスプロバイダはユーザが実行したアクションを記録することができる。アクションには、たとえば、サービスへのログイン、ログアウト、データのアップロード、データのダウンロード、データの変更、実行可能ファイルの起動、その他の操作が含まれる。さまざまな例では、これらのアクションは、アクションを実行したユーザの識別、アクションが開始および/または完了した時間、アクションの影響を受けるリソース、またはユーザがアクションを実行したネットワーク位置もしくはジオロケーションなどの情報とともに、アクティビティデータに記録することができる。

30

【0211】

ステップ604で、プロセス600は、アクティビティデータにおいて、クラウドサービスに関して特権のある1つ以上のアクションを識別することを含む。特権アクションは、あるユーザが、すべてのユーザが実行を許可されるわけではない状態でリソースに影響を与えることができるアクションである。たとえば、特権アクションは、第1のユーザが実行したときに、他のユーザによるクラウドサービスの利用に影響を与える状態でクラウドサービスを変更することができるアクションである。別の例として、特権アクションは、第1のユーザによって実行されたときに、クラウドサービスの他のユーザのユーザアカウントに影響を与えることができるアクションである。

40

【0212】

一部の例では、特権のある1つ以上のアクションは、クラウドサービスに関連付けられたアクションのリストを用いて識別されることができ、リスト内のアクションは、クラウドサービスに関して特権を有するとして分類される。たとえば、1つのクラウドサービスの場合、ユーザアカウントの作成およびユーザアカウントの削除のためのアクションは特権

50

として分類することができる。別の例として、別のクラウドサービスの場合、特定のファイルフォルダを変更するためのアクションを特権として分類することができる。

【0213】

一部の例では、管理アクションのリストを用いて、特権を有する1つ以上のアクションを識別することができる。これらの例では、管理アクションのリストには、ユーザアカウントの作成または削除、アクセス制御またはセキュリティ設定の変更、クレデンシャルの変更など、より高い特権が必要なアクションが含まれ得る。

【0214】

ステップ606で、プロセス600は、アクティビティデータを用いて、1つ以上のアクションを実行したユーザのセットを識別することを含み、ユーザのセットはテナントに関連付けられた1人以上のユーザから判断される。

10

【0215】

一部の例では、ユーザのセットを識別することは、1つ以上のアクションおよび過去のアクティビティデータを用いてモデルを生成することを含む。これらの例では、モデルはクラウドサービスに関して特権のあるクラウドサービスの利用のパターンを記述することができる。たとえば、教師あり学習または教師なし学習を用いて、特定のクラウドサービスに関して特権のあるアクションまたは一連のアクションを認識するようにニューラルネットワークをトレーニングすることができる。教師あり学習の例では、特権のあるアクションまたは特権のないアクションを識別するラベル付きトレーニングデータをニューラルネットワークに提供することができる。教師なし学習の例では、コスト関数を最小化するようにニューラルネットワークを構成することができ、コスト関数はクラウドサービスへの変更をモデル化する。これらの例および他の例では、モデルを用いてユーザのセットを識別することができる。

20

【0216】

代替的または追加的に、ユーザのセットを識別することは、クラウドサービスの利用中に実行されるアクションをグループ化すること、および特権のあるアクションを含むアクションのグループを識別することを含む。たとえば、K-meansクラスタリング手法を用いて、アクティビティデータにおけるアクションをプロットし、アクションを実行したユーザをプロットして、同様のアクションを実行したユーザを特定することができる。プロットから、ユーザのグループを特定することができる。

30

【0217】

ステップ608で、プロセス600は、ユーザのセットを、特権を有するとして分類することを含む。さまざまな例では、特権を有するとして識別された1つ以上のアクションを実行したため、ユーザのセットは特権が与えられている。

【0218】

ステップ610で、プロセス600は、アクティビティデータを用いて、1人以上のユーザの1つ以上のリスクスコアを判定することを含む。さまざまな例において、リスクスコアは、クラウドサービスの利用中にユーザが実行したアクションからテナントに対するセキュリティリスクの程度を示す。リスクスコアは、個々のユーザ、ユーザのグループ、個々のサービス、複数のサービス、異なるサービスプロバイダのサービス、および/またはユーザとサービスとの組み合わせに対して計算することができる。いくつかの例では、リスクスコアはリスクインジケータの重みの合計として計算される。リスクインジケータは、実行されたアクション、アクションの影響を受けるリソース、特定のユーザ、ユーザのグループ、サービス、サービスプロバイダ、ユーザがいるネットワーク位置、サービスプロバイダもしくはサービスのネットワーク位置、ジオロケーション、時刻、曜日、月、その他の要因、または要因の組み合わせと関連付けられることができる。代替的または追加的に、リスクインジケータは、ネットワークの脅威インテリジェンスの外部アグリゲータおよび/またはディストリビュータから取得した脅威インテリジェンスから取得することができる。いくつかの例では、より重要なリスクインジケータに、より高い重み値が与えられる。

40

50

【 0 2 1 9 】

さまざまな例において、特権ユーザとして分類されたユーザのリスクスコアは、非特権ユーザのリスクスコアよりも大きな重みで計算される。したがって、たとえば、特権ユーザがアクションを実行する場合、特権ユーザのリスクスコアは、非特権ユーザが同じアクションを実行する場合よりも高くなり得る。代替的または追加的に、より多くの、または異なるインジケータを用いて、一般ユーザよりも特権ユーザのリスクスコアを判定することができる。代替的または追加的に、特権ユーザのリスクスコアはより頻繁に計算されるか、そうでなければ非特権ユーザのリスクスコアよりも高いレベルの精査が与えられてもよい。

【 0 2 2 0 】

ステップ 6 1 2 で、プロセス 6 0 0 は、ユーザのセット内のユーザのリスクスコアはしきい値より大きいと判定することを含む。さまざまな例において、しきい値は、しきい値を超えたときにテナントのセキュリティリスクを構成するアクティビティを示すことができる。さまざまな例では、しきい値を特定のテナント、特定のユーザ、ユーザのグループ、特定のサービスもしくはサービスプロバイダ、時刻もしくは曜日、別の要因、または要因の組み合わせに関連付けることができる。

【 0 2 2 1 】

ステップ 6 1 4 で、プロセス 6 0 0 は、サービスプロバイダシステムのセキュリティ制御を判断することを含み、セキュリティ制御は、クラウドサービスへのアクセスを構成するためにサービスプロバイダシステムによって用いられる。セキュリティ制御は、リスクスコアがしきい値を超えたアクション、アクションの影響を受けるリソース、脅威インテリジェンス、および/またはテナントに関連付けられた構成設定などの要因に依存する。判断することができるセキュリティ制御の例には、ユーザまたはユーザのグループによるサービスの利用をブロックすること、クラウドサービスの特定のユーザアカウントを無効にすること、特定のユーザがログインおよび/または特定のアクションを実行するたびにサービスにアラートを送信させること、サービスへの/からのデータのアップロードまたはダウンロードをブロックすることなどの制御が含まれる。

【 0 2 2 2 】

ステップ 6 1 6 で、プロセス 6 0 0 は、サービスプロバイダシステムに送信する 1 つ以上の命令を判断することを含む。さまざまな例では、サービスプロバイダに照会して適切な命令を要求し、所望の構成を達成することで命令を判断することができる。これらの例では、コンピューティングシステムにクエリを実行するための自動化されたプログラムを含めることができる。別の例として、命令は、クラウドサービスの A P I から判断することができる。A P I には、コンピューティングシステムがクラウドサービスの構成を変更することができるようにする操作を含めることができる。

【 0 2 2 3 】

ステップ 6 1 8 で、プロセス 6 0 0 は、1 つ以上の命令をサービスプロバイダシステムに送信することを含み、1 つ以上の命令は、ユーザに関してセキュリティ制御を変更させ、ユーザによるクラウドサービスへのアクセスがセキュリティ管理の変更により変更される。さまざまな例において、命令の送信には、テナントに割り当てられた承認（パスワード、トークン、またはその他の形式のクレデンシャルなど）を用いることが含まれ得る。これにより、セキュリティ管理システムはテナントに代わってクラウドサービスを構成することができる。一部の例では、命令はテナントまたはサービスプロバイダによる活性化のためにサービスプロバイダシステムに送信される。実行されると、特権ユーザに起因するセキュリティリスクを監視、軽減、および/または停止することができる。

【 0 2 2 4 】

図 7 は、上記のさまざまな例を実現することができる分散型システム 7 0 0 を簡略化した図を示す。図示した例において、分散型システム 7 0 0 は、1 つ以上のクライアントコンピューティングデバイス 7 0 2、7 0 4、7 0 6、および 7 0 8 を備える。1 つ以上のクライアントコンピューティングデバイス 7 0 2、7 0 4、7 0 6、および 7 0 8 は、1 つ

10

20

30

40

50

以上のネットワーク（複数可）710でウェブブラウザ、プロプライエタリ・クライアント（たとえば、Oracle Forms）などのクライアントアプリケーションを実行および操作するように構成される。サーバ712は、ネットワーク710を介して、リモートクライアントコンピューティングデバイス702、704、706、および708と通信可能に接続されてもよい。

【0225】

さまざまな例において、サーバ712は、1つ以上のサービスまたはソフトウェア・アプリケーションを実行するようになされてもよい。また、ある例において、サーバ712は、他のサービスまたはソフトウェア・アプリケーションを提供してもよく、非仮想環境および仮想環境を含み得る。いくつかの例において、これらのサービスは、クライアントコンピューティングデバイス702、704、706、708のユーザに対して、ウェブベースのサービスもしくはクラウドサービスとして提供されてもよく、または、SaaS（Software as a Service）モデル下で提供されてもよい。そして、クライアントコンピューティングデバイス702、704、706、708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利用して、サーバ712とやり取りして、これらのコンポーネントが提供するサービスを利用できる。

【0226】

図7に示す構成において、システム700のソフトウェアコンポーネント718、720、722が、サーバ712上に実装されたものとして示される。また、他の例において、システム700のコンポーネントのうちの1つ以上および/またはこれらのコンポーネントが提供するサービスのうちの1つ以上は、クライアントコンピューティングデバイス702、704、706、708のうちの1つ以上によって実現されてもよい。次に、クライアントコンピューティングデバイス702を操作しているユーザは、1つ以上のクライアントアプリケーションを利用して、これらのコンポーネントが提供するサービスを使用してもよい。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、またはそれらの組合せで実現されてもよい。さまざまな異なるシステム構成が可能であり、これらは、例示の分散型システム700とは異なってもよいことを理解されたい。よって、図7に示す例は、任意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、限定を意図したものではない。

【0227】

クライアントコンピューティングデバイス702、704、706、708は、さまざまな種類のコンピュータシステムを含んでもよい。たとえば、クライアントコンピューティングデバイスは、Microsoft Windows Mobile（登録商標）などのソフトウェアおよび/またはiOS、Windows（登録商標）Phone、Android、BlackBerry 10、Palm OSなどのいろいろなモバイルオペレーティングシステムを実行する手のひらサイズのポータブルデバイス（たとえば、iPhone（登録商標）、携帯電話、iPad（登録商標）、コンピューティングタブレット、携帯情報端末（PDA））またはウェアラブルデバイス（たとえば、Google Glass（登録商標）ヘッドマウントディスプレイ）を含んでもよい。デバイスは、さまざまなインターネット関連アプリ、電子メール、ショートメッセージサービス（SMS）アプリケーションなど、さまざまなアプリケーションをサポートしてもよく、さまざまな他の通信プロトコルを使用してもよい。また、クライアントコンピューティングデバイスは、一例として、さまざまなバージョンのMicrosoft Windows（登録商標）、Apple Macintosh（登録商標）、および/またはLinux（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を含んでもよい。クライアントコンピューティングデバイスは、これらに限定されないが、たとえば、Google Chrome OSなど、いろいろなGNU/Linux（登録商標）オペレーティングシステムを含む、流通している各種のUNIX（登録商標）またはUNIX（登録商標）に似た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り得る

10

20

30

40

50

。また、クライアントコンピューティングデバイスは、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ミングシステム（たとえば、Kinect（登録商標）ジェスチャ入力装置付きまたは無しのMicrosoft Xboxのゲーミングコンソール）、および/またはパーソナルメッセージングデバイスなど、ネットワーク（複数可）710で通信可能な電子機器を含んでもよい。

【0228】

図7の分散型システム700は、4つのクライアントコンピューティングデバイスとともに示されているが、任意の数のクライアントコンピューティングデバイスがサポートされてもよい。センサ付きデバイスなど、他のデバイスがサーバ712とやり取りを行ってもよい。

10

【0229】

分散型システム700におけるネットワーク（複数可）710は、これらに限定されないが、TCP/IP（Transmission Control Protocol/Internet Protocol）、SNA（Systems Network Architecture）、IPX（Internet Packet Exchange）、AppleTalkなどを含む、各種の利用可能なプロトコルを使用したデータ通信をサポートできる、当業者にとってなじみの任意の種類ネットワークであってもよい。単に一例として、ネットワーク（複数可）710は、LAN（Local Area Network）、Ethernet（登録商標）ベースのネットワーク、トークンリング、ワイドエリアネットワーク、インターネット、仮想ネットワーク、VPN（Virtual Private Network）、イントラネット、エクストラネット、PSTN（Public Switched Telephone Network）、赤外線ネットワーク、ワイヤレスネットワーク（たとえば、IEEE（Institute Of Electrical And Electronics）802.11スイートのプロトコル、Bluetooth（登録商標）、および/またはその他のワイヤレスプロトコルのうちのいずれかの下で動作するネットワーク）、および/またはこれらの任意の組合せならびに/もしくは他のネットワークで有り得る。

20

【0230】

サーバ712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（一例として、PC（Personal Computer）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、ラックマウント式のサーバなどを含む）、サーバファーム、サーバ・クラスタ、またはその他の適切な配置および/または組合せから構成されてもよい。サーバ712は、仮想オペレーティングシステムを実行している1つ以上の仮想マシン、または仮想化を伴う他のコンピューティングアーキテクチャを含み得る。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、サーバ用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使用して、サーバ712によって制御することができる。さまざまな例において、サーバ712は、上記の開示において説明した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なされてもよい。たとえば、サーバ712は、上述した処理を行うためのサーバに対応してもよい。

30

【0231】

サーバ712は、上述のオペレーティングシステムのいずれかおよび市販されているサーバオペレーティングシステムのうちのいずれかを含む、オペレーティングシステムを実行してもよい。また、サーバ712は、HTTP（Hypertext Transport Protocol）サーバ、FTP（File Transfer Protocol）サーバ、CGI（Common Gateway Interface）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、各種の追加のサーバアプリケーションおよび/またはミッドティア・アプリケーションを実行してもよい。例示的なデータベースサーバとして、Oracle、Microsoft、Sybase、IBM（International Business Machines）などから市販されているデータベースサーバが挙げられるが、これらに限定されない。

40

【0232】

いくつかの実装形態において、サーバ712は、クライアントコンピューティングデバイ

50

ス 7 0 2、7 0 4、7 0 6、および 7 0 8 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 1 つにまとめるための 1 つ以上のアプリケーションを含んでもよい。例として、データフィードおよび / またはイベント更新は、これらに限定されないが、1 つ以上のサードパーティ情報ソースおよび連続したデータストリームから受信する T w i t t e r (登録商標) フィード、F a c e b o o k (登録商標) 更新またはリアルタイム更新を含んでもよく、当該 1 つ以上のサードパーティ情報ソースおよび連続したデータストリームは、センサーデータアプリケーション、チックカー (financial ticker)、ネットワークパフォーマンス測定ツール (たとえば、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、自動車交通量監視などに関するリアルタイムイベントを含み得る。また、サーバ 7 1 2 は、クライアントコンピューティングデバイス 7 0 2、7 0 4、7 0 6、7 0 8 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んでもよい。

10

【 0 2 3 3 】

また、分散型システム 7 0 0 は、1 つ以上のデータベース 7 1 4 および 7 1 6 を含んでもよい。これらのデータベースは、ユーザインタラクション情報、使用パターン情報、適合規則情報、および上記のさまざまな例によって用いられる他の情報などの情報を格納するための機構を提供してもよい。データベース 7 1 4 および 7 1 6 は、いろいろな場所に存在してもよい。例として、データベース 7 1 4 および 7 1 6 のうちの 1 つ以上は、サーバ 7 1 2 にローカルな (および / または存在する) 非一時的な記憶媒体上に存在してもよい。これに代えて、データベース 7 1 4 および 7 1 6 は、サーバ 7 1 2 から遠隔の場所に存在し、ネットワークベースまたは専用の接続を通してサーバ 7 1 2 と通信していてもよい。ある例においては、データベース 7 1 4 および 7 1 6 は、S A N (Storage-Area Network) に存在してもよい。同様に、サーバ 7 1 2 に起因する機能を実行するための必要なファイルは、いずれも、サーバ 7 1 2 上のローカルな場所および / またはサーバ 7 1 2 から遠隔の場所に、適宜、格納されてもよい。ある例においては、データベース 7 1 4 および 7 1 6 は、S Q L フォーマットのコマンドに応答してデータ格納、更新、および取り出すようになされた O r a c l e が提供するデータベースなど、リレーショナルデータベースを含んでもよい。

20

【 0 2 3 4 】

いくつかの例において、クラウド環境は、1 つ以上のサービスを提供してもよい。図 8 は、サービスがクラウドとして提供され得るシステム環境 8 0 0 の 1 つ以上のコンポーネントを簡略化したブロック図である。図 8 に示す例において、システム環境 8 0 0 は、1 つ以上のクライアントコンピューティングデバイス 8 0 4、8 0 6、および 8 0 8 を含む。1 つ以上のクライアントコンピューティングデバイス 8 0 4、8 0 6、および 8 0 8 は、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 8 0 2 とやり取りするために、ユーザによって使用され得る。クラウドインフラストラクチャシステム 8 0 2 は、図 7 のサーバ 7 1 2 に関して上述したものを含み得る 1 つ以上のコンピュータおよび / またはサーバを備えてもよい。

30

【 0 2 3 5 】

図 8 に示すクラウドインフラストラクチャシステム 8 0 2 が、図示されたコンポーネント以外のコンポーネントを有し得ることを理解されたい。さらに、図 8 に示す実施形態は、上記のさまざまな例を組み込み得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。他の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 8 0 2 は、図に示すコンポーネント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、またはコンポーネントの構成または配置が異なってもよい。

40

【 0 2 3 6 】

クライアントコンピューティングデバイス 8 0 4、8 0 6、および 8 0 8 は、クライアントコンピューティングデバイス 7 0 2、7 0 4、7 0 6、および 7 0 8 に関して上述した

50

ものと同様のデバイスであってもよい。クライアントコンピューティングデバイス 804、806、および 808 は、ウェブブラウザ、プロプライエタリ・クライアントアプリケーション（たとえば、Oracle Forms）、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操作するように構成されてもよい。クライアントアプリケーションは、クライアントコンピューティングデバイスのユーザによって、クラウドインフラストラクチャシステム 802 とやり取りを行って、クラウドインフラストラクチャシステム 802 が提供するサービスを使用するために、使用されてもよい。例示的なシステム環境 800 は、3 つのクライアントコンピューティングデバイスとともに示されているが、任意の数のクライアントコンピューティングデバイスがサポートされてもよい。センサ付きデバイスなど、他のデバイスがクラウドインフラストラクチャシステム 802 とやり取りを行ってもよい。

10

【0237】

ネットワーク（複数可）810 は、クライアントコンピューティングデバイス 804、806、および 808 と、クラウドインフラストラクチャシステム 802 との間のデータの通信およびやり取りを容易にすることができる。各ネットワークは、図 7 のネットワーク（複数可）710 に関して上述したプロトコルを含む、各種の流通しているプロトコルを使用したデータ通信をサポートできる、当業者にとってなじみの任意の種類のネットワークであってもよい。

【0238】

ある例において、図 8 のクラウドインフラストラクチャシステム 802 が提供するサービスは、クラウドインフラストラクチャシステムのユーザが要求すると、ユーザで利用できるようになるサービスのホストを含んでもよい。また、オンラインのデータ記憶およびバックアップソリューション、ウェ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ドキュメント共同作業サービス、データベース処理、管理されたテクニカルサポートサービスなどを含むさまざまな他のサービスが提供されてもよいが、これらに限定されない。クラウドインフラストラクチャシステムが提供するサービスは、そのユーザのニーズを満たすために、動的にスケール変更できる。

20

【0239】

ある例において、クラウドインフラストラクチャシステム 802 が提供するサービスを具体的にインスタンス化したものは、本明細書において、「サービスインスタンス」と称される場合がある。一般に、クラウドサービスプロバイダのシステムからの、インターネットなどの通信ネットワークを介してユーザでできるようにされるいずれのサービスも、「クラウドサービス」と称される。通常、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、顧客所有のオンプレミス・サーバおよびシステムとは異なる。たとえば、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ホストしてもよく、ユーザは、インターネットなどの通信ネットワークを介して、要求に基づいてアプリケーションをオーダーして使用すればよい。

30

【0240】

いくつかの例において、コンピュータネットワークのクラウドインフラストラクチャにおけるサービスは、保護されたコンピュータネットワークのストレージへのアクセス、ホストされたデータベース、ホストされたウェブサーバ、ソフトウェア・アプリケーション、またはクラウドベンダーがユーザに提供するまたは当技術分野で周知の他のサービスを含んでもよい。たとえば、サービスは、インターネットを通じたクラウド上のリモートストレージへのパスワード保護されたアクセスを含み得る。別の例として、サービスは、ウェブサービスベースのホストされたリレーショナルデータベース、およびネットワークで結ばれた開発者が私的使用するためのスクリプト言語ミドルウェアエンジンを含み得る。別の例として、サービスは、クラウドベンダーのウェブサイト上にホストされた電子メールソフトウェア・アプリケーションへのアクセスを含み得る。

40

【0241】

ある例において、クラウドインフラストラクチャシステム 802 は、セルフサービスで、

50

サブスクリプション方式の、伸縮自在にスケーラブルで、信頼でき、高い可用性を持つセキュアな方法で顧客に届けられるアプリケーションのスイート、ミドルウェア、およびデータベースサービス提供物を含んでもよい。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が、本願の譲受人が提供するオラクルパブリッククラウド (Oracle Public Cloud) である。

【0242】

また、クラウドインフラストラクチャシステム802は、「ビッグデータ」ならびに関連の演算および分析サービスを提供してもよい。用語「ビッグデータ」は、一般に、大量のデータを可視化する、トレンドを検出する、および/またはデータとやり取りするためにアナリストおよび研究者によって格納および操作され得る極めて大きなデータセットを指す。このビッグデータおよび関連アプリケーションは、多くのレベルおよび異なる規模で、インフラストラクチャシステムによってホストおよび/または操作され得る。このようなデータを提示するために、またはこのデータに対する外力またはデータが表すものをシミュレーションするために、並列にリンクされた何十、何百、または何千ものプロセッサがこのデータに作用できる。これらのデータセットは、データベースにおいて、または構造化モデルに応じて編成されたもののような構造化データ、および/または非構造化データ(たとえば、Eメール、画像、データBLOB(binary large objects)、ウェブページ、複雑なイベント処理)を伴い得る。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素早く目標に集める能力を活用することによって、企業、政府関係機関、研究機関、私人、同じ意見を持った個人同士のグループもしくは組織、または他のエンティティからの要求に基づいて、大きなデータセットに対してタスクを実行するにあたり、クラウドインフラストラクチャシステムをより利用可能にできる。

【0243】

さまざまな例において、クラウドインフラストラクチャシステム802は、クラウドインフラストラクチャシステム802が提供するサービスへの顧客のサブスクリプションを自動的にプロビジョニング、管理、および追跡するようになされてもよい。クラウドインフラストラクチャシステム802は、それぞれ異なるデプロイメントモデルを介して、クラウドサービスを提供してもよい。たとえば、サービスは、パブリッククラウドモデル下で提供されてもよい。パブリッククラウドモデルでは、クラウドインフラストラクチャシステム802は、(たとえば、オラクルコーポレーション所有の)クラウドサービスを提供する組織が所有しており、一般大衆またはそれぞれ異なる産業企業でサービスが使用できるようになる。別の例として、サービスは、クラウドインフラストラクチャシステム802が1つの組織のためだけに動かされるプライベートクラウドモデル下で提供されてもよく、組織内の1つ以上のエンティティのためのサービスを提供してもよい。また、クラウドサービスは、コミュニティクラウドモデル下で提供されてもよい。コミュニティクラウドモデルでは、クラウドインフラストラクチャシステム802およびクラウドインフラストラクチャシステム802によって提供されるサービスが、関連コミュニティ内のいくつかの組織によって共有される。クラウドサービスは、ハイブリッドクラウドモデル下で提供されてもよい。ハイブリッドクラウドモデルとは、2つ以上の異なるモデルの組合せである。

【0244】

いくつかの例において、クラウドインフラストラクチャシステム802が提供するサービスは、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、または混合サービスを含む、他のカテゴリ下で提供される1つ以上のサービスを含んでもよい。顧客は、サブスクリプションのオーダーによって、クラウドインフラストラクチャシステム802が提供する1つ以上のサービスをオーダーしてもよい。次に、クラウドインフラストラクチャシステム802は、処理を実行して、顧客のサブスクリプションのオーダーにあるサービスを提供する。

【0245】

10

20

30

40

50

いくつかの例において、クラウドインフラストラクチャシステム 802 が提供するサービスは、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んでもよいが、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 サービス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 カテゴリに該当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。たとえば、SaaS プラットフォームは、オンデマンドアプリケーションのスイートを構築し、統合開発/デプロイメントプラットフォームに届けるための機能を提供してもよい。SaaS プラットフォームは、SaaS サービスを提供するための基礎となるソフトウェアおよびインフラストラクチャを管理および制御してもよい。SaaS プラットフォームが提供する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で実行されるアプリケーションを利用できる。顧客は、アプリケーションサービスを、別のライセンスおよびサポートを購入する必要なしに、入手できる。さまざまな異なる SaaS サービスが提供されてもよい。例として、大きな組織のための販売実績管理、エンタープライズ統合、およびビジネス上の柔軟性に対するソリューションを提供するサービスなどが挙げられるが、これに限定されない。

10

【0246】

いくつかの例において、プラットフォームサービスは、PaaS 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 802 によって提供されてもよい。PaaS プラットフォームは、PaaS カテゴリに該当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として、組織（Oracle など）が既存のアプリケーションを共有の共通アーキテクチャ上に 1 つにまとめることを可能にするサービス、およびプラットフォームが提供する共有サービスを活用する新しいアプリケーションを作る能力などが挙げられるが、これらに限定されない。PaaS プラットフォームは、PaaS サービスを提供するための、基礎となるソフトウェアおよびインフラストラクチャを管理および制御してもよい。顧客は、PaaS クラウドインフラストラクチャシステム 802 が提供するサービスを、ライセンスおよびサポートを別に購入する必要なしに、取得できる。プラットフォームサービスとして、JCS（Oracle Java Cloud Service）、DBCS（Oracle Database Cloud Service）など、およびその他が挙げられるが、これらに限定されない。

20

30

【0247】

PaaS プラットフォームが提供する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がサポートするプログラミング言語およびツールを採用することができ、また、デプロイされたサービスを管理することができる。いくつかの例において、クラウドインフラストラクチャシステムが提供す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（たとえば、Oracle Fusion Middleware サービス）、および Java クラウドサービスを含んでもよい。一例において、データベース・クラウドサービスは、共有サービスデプロイメントモデルをサポートしてもよい。共有サービスデプロイメントモデルは、組織が、データベースリソースをプールし、データベース・クラウドの形のサービスとしてデータベースを顧客に提供することを可能にする。ミドルウェアクラウドサービスは、顧客がさまざまな業務アプリケーションを開発およびデプロイするためのプラットフォームを提供してもよく、Java クラウドサービスは、顧客がクラウドインフラストラクチャシステムにおいて Java アプリケーションをデプロイするためのプラットフォームを提供してもよい。

40

【0248】

クラウドインフラストラクチャシステムにおいて、IaaS プラットフォームによって、さまざまな異なるインフラストラクチャサービスが提供されてもよい。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 プラットフォームが提供するサービスを利用している顧客のための、ストレージ、ネットワーク、および他の基本的な

50

コンピューティングリソースなど、基礎となるコンピューティングリソースの管理および制御を容易にする。

【0249】

また、ある例において、クラウドインフラストラクチャシステム802は、クラウドインフラストラクチャシステムの顧客にさまざま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830を含んでもよい。一例において、インフラストラクチャ・リソース830は、PaaSプラットフォームおよびSaaSプラットフォームが提供するサービスを実行するための、サーバなどのハードウェアと、ストレージと、ネットワーキング・リソースとの予め統合された最適な組合せ、および他のリソースを含んでもよい。

10

【0250】

いくつかの例において、クラウドインフラストラクチャシステム802におけるリソースは、複数のユーザによって共有され、要求に応じて、動的に再割り当てされてもよい。これに加えて、リソースは、それぞれ異なるタイムゾーンのユーザに割り当てられてもよい。たとえば、クラウドインフラストラクチャシステム802は、第1のタイムゾーンにいる第1セットのユーザが、指定された時間数、クラウドインフラストラクチャシステムのリソースを利用することを可能にした後、同じリソースを、異なるタイムゾーンに位置する別のセットのユーザへ再割り当てすることを可能にし、リソースの利用を最大限に活用することができる。

【0251】

20

いくつかの例において、クラウドインフラストラクチャシステム802のそれぞれ異なるコンポーネントまたはモジュールによって共有されて、クラウドインフラストラクチャシステム802によるサービスのプロビジョニングを可能にするいくつかの内部の共有サービス832が提供されてもよい。これらの内部の共有サービスは、セキュリティ/素性サービス、統合サービス、エンタープライズリポジトリサービス、エンタープライズマネージャサービス、ウイルススキャン/ホワイトリストサービス、可用性の高いバックアップ・リカバリサービス、クラウドサポート、Eメールサービス、通知サービス、ファイル転送サービスなどを可能にするためのサービスを含み得るが、これらに限定されない。

【0252】

いくつかの例において、クラウドインフラストラクチャシステム802は、クラウドインフラストラクチャシステムにおけるクラウドサービス（たとえば、SaaSサービス、PaaSサービス、およびIaaSサービス）の包括的な管理を提供してもよい。一例において、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802などが受信した顧客のサブスクリプションをプロビジョニング、管理、および追跡するための機能を含んでもよい。

30

【0253】

一例において、図8に示すように、クラウド管理機能は、オーダー管理モジュール820、オーダーオーケストレーションモジュール822、オーダープロビジョニングモジュール824、オーダー管理/監視モジュール826、および素性管理モジュール828など、1つ以上のモジュールによって提供されてもよい。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、または、これらを使用して提供されてもよい。1つ以上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、またはその他の適切な配置および/または組合せであり得る。

40

【0254】

例示的な動作において、ステップ834において、クライアントコンピューティングデバイス804、806、または808などのクライアントデバイスを使用している顧客は、クラウドインフラストラクチャシステム802が提供する1つ以上のサービスを要求し、クラウドインフラストラクチャシステム802が提供する1つ以上のサービスのサブスクリプションのオーダーをすることによって、クラウドインフラストラクチャシステム80

50

2とやり取りしてもよい。いくつかの例において、顧客は、第1のクラウドUI 812、第2のクラウドUI 814、および/または第3のクラウドUI 816などのクラウドユーザインタフェース(UI: User Interface)にアクセスし、これらのUIを介してサブスクリプションのオーダーを行ってもよい。顧客がオーダーをすることに応答してクラウドインフラストラクチャシステム802が受信したオーダー情報は、この顧客を特定する情報、および、顧客がサブスクリプションをする予定である、クラウドインフラストラクチャシステム802が提供する1つ以上のサービスを含んでもよい。

【0255】

ステップ836において、顧客から受けたオーダー情報を、オーダーデータベース818に格納してもよい。これが、新しいオーダーである場合、オーダーについての新しい記録を作成してもよい。一例において、オーダーデータベース818は、クラウドインフラストラクチャシステム802によって操作され、他のシステム要素と共に操作されるいくつかのデータベースのうちの1つであり得る。

10

【0256】

ステップ838において、オーダー情報が、オーダー管理モジュール820に転送されてもよい。オーダー管理モジュール820は、オーダーの確認、確認後のオーダーの登録など、オーダーに関する課金機能および会計機能を実行するように構成されてもよい。

【0257】

ステップ840において、オーダーに関する情報は、オーダーオーケストレーションモジュール822に伝送されてもよい。オーダーオーケストレーションモジュール822は、顧客が行ったオーダーに関するサービスおよびリソースのプロビジョニングをオーケストレーションするように構成される。場合によっては、オーダーオーケストレーションモジュール822は、オーダープロビジョニングモジュール824のサービスをプロビジョニングのために使用してもよい。いくつかの例において、オーダーオーケストレーションモジュール822は、各オーダーに対応付けられたビジネスプロセスの管理を可能にし、ビジネスロジックを適用して、オーダーがプロビジョニングに進むべきかどうかを判断する。

20

【0258】

図8に表した例に示すように、ステップ842において、新しいサブスクリプションのオーダーを受けると、オーダーオーケストレーションモジュール822は、オーダープロビジョニングモジュール824に、リソースを割り当て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、要求を送る。オーダープロビジョニングモジュール824は、顧客が申し込んだサービスのためのリソースの割り当てを可能にする。オーダープロビジョニングモジュール824は、クラウドインフラストラクチャシステム802が提供するクラウドサービスと、要求されたサービスを提供するためのリソースをプロビジョニングするために使用される物理実施層との間に、抽象度を提供する。これによって、サービスおよびリソースがオンザフライで実際にプロビジョニングまたは予めプロビジョニングされて、要求された場合にのみ割り当て/アサインされたかどうかなどの実施詳細から、オーダーオーケストレーションモジュール822を切り離すことが可能になる。

30

【0259】

ステップ844において、いったんサービスおよびリソースがプロビジョニングされると、要求されたサービスが使える用意が整ったことを示す通知を、サブスクリプションをしている顧客に送ってもよい。ある場合において、要求されたサービスを顧客が使用し始めることを可能にする情報(たとえば、リンク)が、顧客に送られてもよい。

40

【0260】

ステップ846において、顧客のサブスクリプションのオーダーが、オーダー管理/監視モジュール826によって管理および追跡されてもよい。場合によっては、オーダー管理/監視モジュール826は、顧客のサブスクリプションしているサービスの使用に関する使用統計データを収集するように構成されてもよい。たとえば、使用されたストレージの量、転送されたデータの量、ユーザの数、およびシステムの稼働時間およびシステムの休

50

止時間などについての統計データが収集されてもよい。

【0261】

ある例において、クラウド・インフラストラクチャ・システム800は、素性管理モジュール828を含んでもよい。素性管理モジュール828は、クラウド・インフラストラクチャ・システム800におけるアクセス管理および承認サービスなどの素性サービスを提供するように構成される。いくつかの例において、素性管理モジュール828は、クラウドインフラストラクチャシステム802が提供するサービスを利用したい顧客についての情報を制御してもよい。このような情報は、このような顧客の素性を認証する情報、および、さまざまなシステムリソース（たとえば、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）に対してそれらの顧客がどのような操作を行うことが承認されているのかを記述する情報を含み得る。また、素性管理モジュール828は、各顧客についての記述情報、およびその記述情報が誰によってどのようにアクセスおよび変更され得るかについての記述情報の管理を含んでもよい。

10

【0262】

図9は、上記のさまざまな例を実現するために使用され得るコンピュータシステム900の例を示す図である。いくつかの例において、コンピュータシステム900を使用して、上述のさまざまなサーバおよびコンピュータシステムのうちのいずれかを実現してもよい。図9に示すように、コンピュータシステム900は、バス・サブシステム902を介していくつかの周辺サブシステムと通信する処理サブシステム904を含むさまざまなサブシステムを備える。これらの周辺サブシステムは、処理高速化ユニット906と、I/Oサブシステム908と、ストレージサブシステム918と、通信サブシステム924とを備えてもよい。ストレージサブシステム918は、有形のコンピュータ読み取り可能な記憶媒体922と、システムメモリ910とを備えてもよい。

20

【0263】

バス・サブシステム902は、コンピュータシステム900のさまざまなコンポーネントおよびサブシステムを互いに意図した通りに通信させるための機構を提供する。バス・サブシステム902は、1つのバスとして図示されているが、バス・サブシステムの代替例は、複数のバスを利用してもよい。バス・サブシステム902は、メモリコントローラのメモリバス、周辺バス、および各種のバスアーキテクチャを使用するローカルバスを含む、いくつかの種類のバス構造のうちのいずれかであってもよい。たとえば、このようなアーキテクチャは、ISA (Industry Standard Architecture) バス、MCA (Micro Channel Architecture) バス、EISA (Enhanced ISA) バス、VESA (Video Electronics Standards Association) ローカルバス、およびPCI (Peripheral Component Interconnect) バスを含んでもよく、これらは、IEEE P1386.1 標準規格に準拠して製造されるMezzanineバスなどとして実現され得る。

30

【0264】

処理サブシステム904は、コンピュータシステム900の動作を制御し、1つ以上の処理装置932、934などを備えてもよい。処理装置は、シングルコア・プロセッサまたはマルチコア・プロセッサを含む1つ以上のプロセッサ、プロセッサの1つ以上のコア、またはそれらの組合せを含んでもよい。いくつかの例において、処理サブシステム904は、グラフィックスプロセッサ、デジタル・シグナル・プロセッサ(DSP)など、1つ以上の専用コプロセッサを含み得る。いくつかの例において、処理サブシステム904の処理装置の一部またはすべては、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、カスタム回路を使用して実現され得る。

40

【0265】

いくつかの例において、処理サブシステム904に含まれる処理装置は、システムメモリ910に、または、コンピュータ読み取り可能な記憶媒体922上に格納された命令を実行できる。さまざまな例において、処理装置は、いろいろなプログラムまたはコード命令を実行し、複数の同時に実行しているプログラムまたはプロセスを維持できる。いつでも

50

、実行されるプログラムコードの一部またはすべては、システムメモリ 910 に、および / または、1 つ以上の記憶装置上に潜在的に含む、コンピュータ読み取り可能な記憶媒体 922 上に存在し得る。適したプログラミングを通して、処理サブシステム 904 は、さまざまな機能を提供できる。

【0266】

いくつかの例において、カスタマイズされた処理を実行するための、または、コンピュータシステム 900 によって実行される全体的な処理が高速化するように、処理サブシステム 904 によって実行される処理のうちのいくつかの負荷を軽減させるための処理高速化ユニット 906 が提供されてもよい。

【0267】

I/O サブシステム 908 は、コンピュータシステム 900 に情報を入力するためのデバイスおよび機構、ならびに / またはコンピュータシステム 900 から、もしくはコンピュータシステム 900 を介して情報を出力するためのデバイスおよび機構を含んでもよい。一般に、用語「入力装置」の使用は、コンピュータシステム 900 に情報を入力するためのあらゆる種類のデバイスおよび機構を含む意図がある。ユーザインタフェース入力装置は、たとえば、キーボード、マウスもしくはトラックボールなどのポインティングデバイス、タッチパッドもしくはディスプレイに組み込まれたタッチスクリーン、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、ボイスコマンド認識システムを有する音声入力装置、マイクロホン、および他の種類の入力装置を含んでもよい。また、ユーザインタフェース入力装置は、ユーザが入力装置を制御するおよび入力装置とやり取り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動き検知デバイスおよび / またはジェスチャ認識デバイス、Microsoft Xbox (登録商標) 360 ゲームコントローラ、ジェスチャコマンドおよび音声コマンドを使用した入力を受信するためのインタフェースを提供するデバイスを含んでもよい。ユーザインタフェース入力装置は、ユーザからの目のアクティビティ (たとえば、写真を撮影しながらおよび / またはメニュー選択を行いながら「まばたきすること」) を検出し、アイ・ジェスチャを、入力装置 (たとえば、Google Glass (登録商標)) への入力として変形させる Google Glass (登録商標) まばたき検出装置などのアイ・ジェスチャ認識デバイスを含んでもよい。これに加えて、ユーザインタフェース入力装置は、ユーザが、ボイスコマンドを通して、音声認識システム (たとえば、Siri (登録商標) ナビゲータ) とやり取りすることを可能にする音声認識検知デバイスを含んでもよい。

【0268】

ユーザインタフェース入力装置の他の例に、3次元 (3D) マウス、ジョイスティックもしくはポインティングスティック、ゲームパッドおよびグラフィックタブレット、ならびに、スピーカ、デジタルカメラ、デジタルカムコーダー、ポータブルメディアプレーヤ、ウェブカム、イメージスキャナ、指紋スキャナ、バーコードリーダ3Dスキャナ、3Dプリンタ、レーザー測距器、および視線追跡装置などのオーディオ/ビジュアル装置などが挙げられるが、これらに限定されない。これに加えて、ユーザインタフェース入力装置は、たとえば、コンピュータ断層撮影法、磁気共鳴画像、ポジترون・エミッション・トモグラフィー、超音波検査デバイスなど、医用画像入力装置を含んでもよい。また、ユーザインタフェース入力装置は、たとえば、MIDI キーボード、デジタル楽器などの音声入力装置を含んでもよい。

【0269】

ユーザインタフェース出力装置は、表示サブシステム、インジケータライト、または音声出力装置などの非ビジュアル装置を含んでもよい。表示サブシステムは、ブラウン管 (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ものなどのフラットパネル表示装置、投影装置、タッチスクリーンなどであってもよい。一般に、用語「出力装置」の使用は、コンピュータシステム 900 からユーザまたは他のコンピュータに情報を出力するためのあらゆる種類のデバイスおよび機構を含むよう意図される。

10

20

30

40

50

たとえば、ユーザインタフェース出力装置は、モニタ、プリンタ、スピーカ、ヘッドホン、自動車ナビゲーションシステム、作図装置、音声出力装置、およびモデムなど、視覚的に文字、図形、および音声／映像情報を伝えるいろいろな表示装置を含み得るが、これらに限定されない。

【0270】

ストレージサブシステム918は、コンピュータシステム900が使用す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。ストレージサブシステム918は、いくつかの例の機能を提供する基本プログラミング構成体およびデータ構成体を格納するための、有形の非一時的なコンピュータ読み取り可能な記憶媒体を提供する。処理サブシステム904によって実行されると上述の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）が、ストレージサブシステム918に格納されてもよい。ソフトウェアは、処理サブシステム904の1つ以上の処理装置によって実行されてもよい。また、ストレージサブシステム918は、本開示に応じ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してもよい。

10

【0271】

ストレージサブシステム918は、揮発性および不揮発性メモリ素子を含む、1つ以上の非一時的なメモリ素子を含んでもよい。図9に示すように、ストレージサブシステム918は、システムメモリ910と、コンピュータ読み取り可能な記憶媒体922とを備える。システムメモリ910は、プログラムを実行中に命令およびデータを格納するための揮発性のメインRAM（Random Access Memory）、および、固定の命令が格納される不揮発性ROM（Read Only Memory）またはフラッシュメモリを含む、いくつかのメモリを含んでもよい。いくつかの実装形態において、起動中などで、コンピュータシステム900内の要素間で情報を転送することを助ける基本ルーチンを含むBIOS（Basic Input/Output System）は、通常、ROMに格納されてもよい。RAMは、通常、処理サブシステム904が現在操作および実行し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910は、SRAM（Static Random Access Memory）またはDRAM（Dynamic Random Access Memory）など、複数の異なる種類のメモリを含んでもよい。

20

【0272】

一例として、限定ではないが、図9に示すように、システムメモリ910は、クライアントアプリケーション、ウェブブラウザ、ミッドティア・アプリケーション、リレーショナルデータベース管理システム（RDBMS）などのアプリケーションプログラム912と、プログラムデータ914と、オペレーティングシステム916とを含んでもよい。例として、オペレーティングシステム916は、さまざまなバージョンのMicrosoft Windows（登録商標）、Apple Macintosh（登録商標）、および／もしくはLinuxオペレーティングシステム、いろいろな流通しているUNIX（登録商標）もしくはUNIXに似たオペレーティングシステム（いろいろな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、これらに限定されない）、ならびに／またはiOS、Windows（登録商標）Phone、Android（登録商標）OS、BlackBerry（登録商標）100S、およびPalm（登録商標）OSオペレーティングシステムなど、モバイルオペレーティングシステムを含んでもよい。

30

40

【0273】

コンピュータ読み取り可能な記憶媒体922は、いくつかの例の機能を提供するプログラミング構成体およびデータ構成体を格納してもよい。処理サブシステム904によって実行されると、プロセッサに上述の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）が、ストレージサブシステム918に格納されてもよい。例として、コンピュータ読み取り可能な記憶媒体922は、ハードディスクドライブなどの不揮発性メモリ、磁気ディスクドライブ、CD-ROM、DVD、Blu-Ray（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学媒体を含んでもよい。コンピュータ読み取り

50

可能な記憶媒体 9 2 2 は、Z i p (登録商標) ドライブ、フラッシュメモリーカード、U S B (Universal Serial Bus) フラッシュドライブ、S D (Secure Digital) カード、D V D ディスク、デジタルビデオテープなどを含んでもよいが、これらに限定されない。また、コンピュータ読み取り可能な記憶媒体 9 2 2 は、フラッシュメモリーベースの S S D、エンタープライズフラッシュドライブ、ソリッドステート R O M など、不揮発性メモリに基づく S S D (Solid-State Drives)、ソリッドステート R A M、動的 R A M、静的 R A M など、揮発性メモリに基づく S S D、D R A M ベースの S S D、磁気抵抗 R A M (M R A M) S S D、および D R A M の S S D とフラッシュメモリーベースの S S D との組合せを使用するハイブリッド S S D を含んでもよい。コンピュータ読み取り可能な記憶媒体 9 2 2 は、コンピュータ読み取り可能な命令、データ構造、プログラムモジュール、およびコンピュータシステム 9 0 0 用の他のデータのストレージを提供してもよい。

10

【0 2 7 4】

また、いくつかの例において、ストレージサブシステム 9 1 8 は、コンピュータ読み取り可能な記憶媒体 9 2 2 にさらに接続され得るコンピュータ読み取り可能な記憶媒体リーダー 9 2 0 を含んでもよい。システムメモリ 9 1 0 と合わせて、必要に応じてシステムメモリ 9 1 0 と組み合わせて、コンピュータ読み取り可能な記憶媒体 9 2 2 は、遠隔の記憶装置、ローカル記憶装置、固定記憶装置、および/またはリムーバブル記憶装置、ならびにコンピュータ読み取り可能な情報を格納するための記憶媒体を包括的に表してもよい。

【0 2 7 5】

いくつかの例において、コンピュータシステム 9 0 0 は、1 つ以上の仮想マシンを実行するためのサポートを提供してもよい。コンピュータシステム 9 0 0 は、仮想マシンの構成および管理を容易にするためのハイパーバイザなどのプログラムを実行してもよい。各仮想マシンには、メモリ、コンピュータ(たとえば、プロセッサ、コア)、I/O、およびネットワーク・リソースが割り当てられてもよい。各仮想マシンは、通常、それ自体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、コンピュータシステム 9 0 0 が実行す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じまたは異なってもよい。よって、複数のオペレーティングシステムは、コンピュータシステム 9 0 0 によって同時に実行される可能性があってもよい。各仮想マシンは、一般に、その他の仮想マシンとは別に実行される。

20

【0 2 7 6】

通信サブシステム 9 2 4 は、他のコンピュータシステムおよびネットワークへのインタフェースを提供する。通信サブシステム 9 2 4 は、コンピュータシステム 9 0 0 からデータを受信し、コンピュータシステム 9 0 0 から他のシステムにデータを送信するためのインタフェースとして機能する。たとえば、通信サブシステム 9 2 4 は、1 つ以上のクライアントコンピューティングデバイスと情報を送受信するためのクライアントコンピューティングデバイスへの通信チャンネルを、インターネットを介してコンピュータシステム 9 0 0 が確立することを可能にしてもよい。

30

【0 2 7 7】

通信サブシステム 9 2 4 は、有線通信プロトコルおよび/またはワイヤレス通信プロトコルの両方をサポートしてもよい。たとえば、いくつかの例において、通信サブシステム 9 2 4 は、ワイヤレス音声ネットワークもしくは/またはデータネットワークにアクセスするための R F (Radio Frequency) 送信コンポーネント(たとえば、携帯電話技術、3 G、4 G、もしくは E D G E (Enhanced Data Rates For Global Evolution) などの次世代データネットワークテクノロジー、W i F i (IEEE 8 0 2 . 1 1 ファミリー標準規格)、他の移動体通信技術、またはそれらの任意の組合せを使用する)、G P S (Global Positioning System) 受信コンポーネント、および/または他のコンポーネントを含んでもよい。いくつかの例において、通信サブシステム 9 2 4 は、ワイヤレスインタフェースに加えて、またはワイヤレスインタフェースの代わりに、有線ネットワーク接続性(たとえば、E t h e r n e t)を提供できる。

40

【0 2 7 8】

50

通信サブシステム 924 は、さまざまな形でデータを受送信できる。たとえば、いくつかの例において、通信サブシステム 924 は、入力通信文を、構造化および/または非構造化データフィード 926、イベントストリーム 928、イベント更新 930 などの形で受信してもよい。たとえば、通信サブシステム 924 は、Twitter (登録商標) フィード、Facebook (登録商標) の更新、RSS (Rich Site Summary) フィードなどのウェブフィード、および/または 1 つ以上のサードパーティ情報ソースからのリアルタイム更新など、ソーシャルメディアネットワークおよび/または他のコミュニケーションサービスのユーザから、データフィード 926 をリアルタイムで受信する (または送る) ように構成されてもよい。

【0279】

10

いくつかの例において、通信サブシステム 924 は、連続したデータストリームの形でデータを受信するように構成されてもよく、連続したデータストリームは、リアルタイムイベントのイベントストリーム 928 および/またはイベント更新 930 を含んでもよく、本質的に明らかな終端がない連続ストリームまた無限ストリームであってもよい。連続データを生成するアプリケーションとして、たとえば、センサーデータアプリケーション、チッカー、ネットワークパフォーマンス測定ツール (たとえば、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、自動車交通量監視などが挙げられてもよい。

【0280】

また、通信サブシステム 924 は、コンピュータシステム 900 に接続された 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中であり得る 1 つ以上のデータベースに、構造化および/または非構造化データフィード 926、イベントストリーム 928、イベント更新 930 などを出力するように構成されてもよい。

20

【0281】

コンピュータシステム 900 は、手のひらサイズのポータブルデバイス (たとえば、iPhone (登録商標) 携帯電話、iPad (登録商標) コンピューティングタブレット、PDA)、ウェアラブルデバイス (たとえば、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、さまざまな種類のうちの 1 つであり得る。

30

【0282】

変わり続ける、というコンピュータおよびネットワークの性質により、図 9 に示すコンピュータシステム 900 の説明は、具体例にすぎない。図 9 に示すシステムよりも多いまたは少ないコンポーネントを有する多くの他の構成が可能である。本明細書に記載の開示および教示に基づいて、当業者は、さまざまな例を実現するための他のやり方および/または方法が分かるだろう。

【0283】

具体的な実現例を説明したが、さまざまな変更例、代替例、代替的な構成、および均等物も本開示の範囲内に包含される。変更例は、開示された特徴の適切な組合せのいずれも含む。本開示に記載される実現例は、ある特定のデータ処理環境内の動作に制限されず、複数のデータ処理環境内で自由に動作することができる。これに加えて、特定の一続きのランザクションおよびステップを使用して本開示に記載される実現例を説明したが、本開示の範囲は、記載の一続きのランザクションおよびステップに限られないことは、当業者に明らかであるはずである。上述の実現例のさまざまな特徴および態様は、個々に、または共同で使用されてもよい。

40

【0284】

さらに、ハードウェアとソフトウェアとの特定の組合せを使用して本開示に記載される実現例を説明したが、ハードウェアとソフトウェアとの他の組合せも、本開示の範囲内であることを認識されたい。本開示に記載される実現例は、ハードウェアのみ、もしくは、ソフトウェアのみで実現されてもよく、またはそれらの組合せを使用して実現されてもよい

50

。本明細書に記載のさまざまなプロセスは、同じプロセッサまたは任意の組合せのそれぞれ異なるプロセッサ上で実現できる。よって、コンポーネントまたはモジュールが特定の動作を実行するように構成されると説明されている箇所では、このような構成は、たとえば、この動作を実行するように電子回路を設計することによって、この動作を実行するようにプログラム可能な電子回路（マイクロプロセッサなど）をプログラムすることによって、またはそれらの任意の組合せによって達成できる。プロセスは、プロセス間通信のための従来技術を含む、いろいろな技術を使用して通信できるが、これに限定されず、それぞれ異なるペアプロセスは、異なる技術を使用してもよく、プロセスの同じペアは、異なる技術を別々のタイミングで使用してもよい。

【0285】

明細書および図面は、厳密ではなく、一例にすぎないと適宜みなされるべきである。しかしながら、添付の特許請求の範囲に記載のより広義の趣旨および範囲から逸脱することなく、追加、減算、削除、および他の変更ならびに変形がそれらに対してなされてもよいということは明白であろう。したがって、具体的な実現例を説明したが、これらは、限定を意図しない。さまざまな変更例および均等物は、添付の特許請求の範囲内である。

【0286】

以下で用いられるように、一連の例への言及は、それらの例の各々への言及として分離的に理解されるべきである（例えば、「例1～4」は「例1, 2, 3, または4」として理解されるべきである）。

【0287】

例1は、コンピューターにより実現される方法であって、セキュリティ管理システムのコンピュータシステムにおいて実行されるステップを含む。上記のステップは、サービスプロバイダシステムからアクティビティデータを取得することを含み、上記アクティビティデータは、クラウドサービスの利用中に実行されるアクションを記述し、上記アクションは、テナントに関連付けられた1人以上のユーザによって実行され、上記サービスプロバイダシステムは上記テナントにテナントアカウントを提供し、上記テナントアカウントにより、上記1人以上のユーザは上記クラウドサービスにアクセスすることができる。上記のステップはさらに、上記アクティビティデータにおいて、上記クラウドサービスに関して特権のある1つ以上のアクションを識別することを含む。上記のステップはさらに、上記アクティビティデータを用いて、上記1つ以上のアクションを実行したユーザのセットを識別することを含み、上記ユーザのセットは上記テナントに関連付けられた上記1人以上のユーザから判断される。上記のステップはさらに、上記ユーザのセットを、特権を有するとして分類することを含む。上記のステップはさらに、上記アクティビティデータを用いて、上記1人以上のユーザの1つ以上のリスクスコアを判定することを含む。上記のステップはさらに、上記ユーザのセット内におけるユーザのリスクスコアがしきい値より大きいと判断することを含む。上記のステップはさらに、上記サービスプロバイダシステムのセキュリティ制御を判断することを含み、上記セキュリティ制御は、上記クラウドサービスへのアクセスを構成するために上記サービスプロバイダシステムによって用いられる。上記のステップはさらに、上記サービスプロバイダシステムに送信するための1つ以上の命令を判断することを含む。上記のステップはさらに、上記1つ以上の命令を上記サービスプロバイダシステムに送信することを含み、上記1つ以上の命令は上記セキュリティ制御を上記ユーザに関して変更させ、上記ユーザによる上記クラウドサービスへのアクセスは、上記セキュリティ制御の変更により変更される。

【0288】

例2は例1の方法であり、上記1つ以上のアクションは、上記クラウドサービスに関連付けられたアクションのリストを用いて識別され、上記アクションのリスト内のアクションは、上記クラウドサービスに関して特権を有するとして分類される。

【0289】

例3は例1～例2の方法であり、上記1つ以上のアクションは、管理アクションのリストを用いて識別される。

10

20

30

40

50

【 0 2 9 0 】

例 4 は例 1 ～ 例 3 の方法であり、上記ステップはさらに、上記 1 つ以上のアクションおよび過去のアクティビティデータを用いてモデルを生成することを含み、上記モデルは、上記クラウドサービスに関して特権のある上記クラウドサービスの利用のパターンを記述する。上記ステップはさらに、上記モデルを用いて上記ユーザのセットを識別することを含む。

【 0 2 9 1 】

例 5 は例 1 ～ 例 4 の方法であり、上記ステップはさらに、上記クラウドサービスの利用中に実行されるアクションをグループ化することを含む。上記ステップはさらに、特権のあるアクションを含むアクションのグループを識別することを含み、上記ユーザのセットは上記アクションのグループを用いて識別される。

10

【 0 2 9 2 】

例 6 は例 1 ～ 例 5 の方法であり、リスクスコアは、上記クラウドサービスの利用時にユーザが実行したアクションから上記テナントに対するセキュリティリスクの程度を示す。

【 0 2 9 3 】

例 7 は例 1 ～ 例 6 の方法であり、リスクスコアは、リスクインジケータの重みの合計として計算される。

【 0 2 9 4 】

例 8 は例 1 ～ 例 7 の方法であり、特権を有するとして分類されたユーザのリスクスコアは、非特権ユーザのリスクスコアよりも大きな重みで計算される。

20

【 0 2 9 5 】

例 9 は例 1 ～ 例 8 の方法であり、特権アクションは、第 1 のユーザによって実行されると、他のユーザによる上記クラウドサービスの利用に影響を与える態様で上記クラウドサービスを変更することができるアクションである。

【 0 2 9 6 】

例 1 0 は例 1 ～ 例 9 の方法であり、特権アクションは、第 1 のユーザによって実行されると、上記クラウドサービスの他のユーザのユーザアカウントに影響を与えることができるアクションである。

【 0 2 9 7 】

例 1 1 は、セキュリティ管理システムのコンピューティングシステムであって、1 つ以上のプロセッサと、上記 1 つ以上のプロセッサに結合され、上記 1 つ以上のプロセッサによって読み取り可能であるメモリとを含む。上記メモリは命令を含み、上記命令は、上記 1 つ以上のプロセッサによって実行されると、上記 1 つ以上のプロセッサに、例 1 ～ 例 1 0 の方法に従って動作を実行させる。

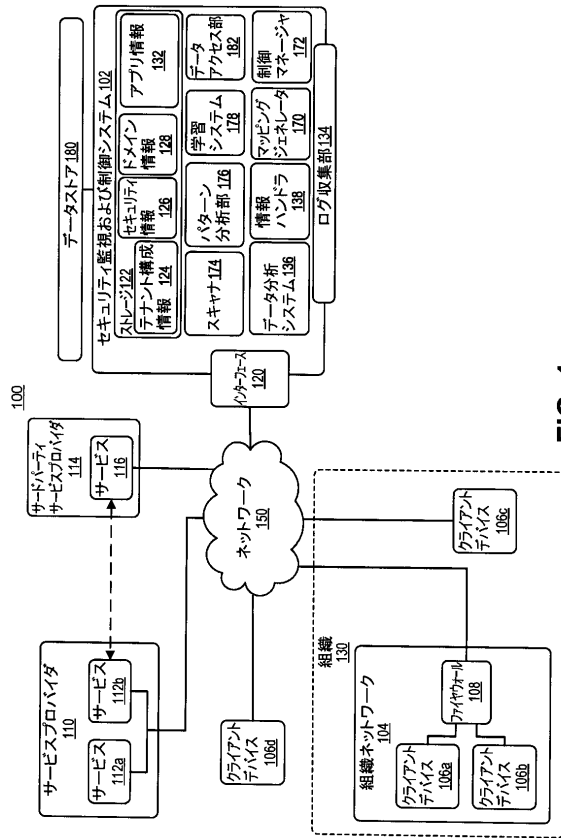
30

【 0 2 9 8 】

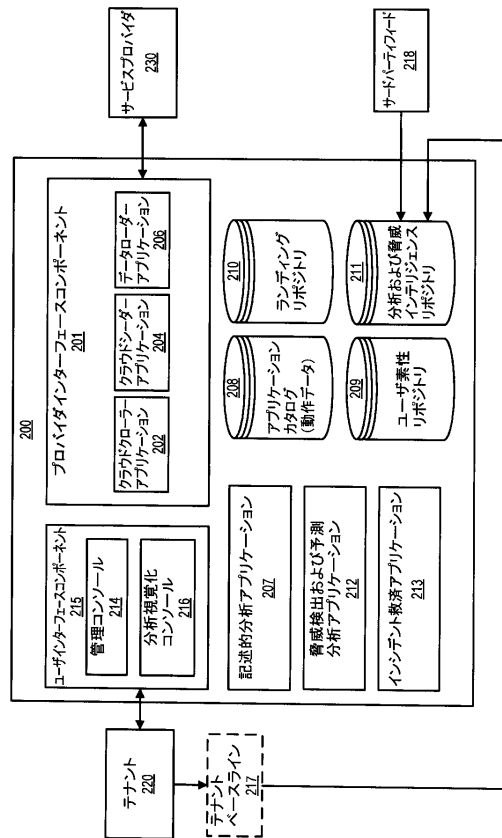
例 1 2 は、命令が格納された非一時的な機械可読記憶媒体であって、上記命令は、セキュリティ管理システムのコンピューティングシステムの 1 つ以上のプロセッサによって実行されると、上記 1 つ以上のプロセッサに、例 1 ～ 例 1 0 の方法に従ってステップを実行させる。

40

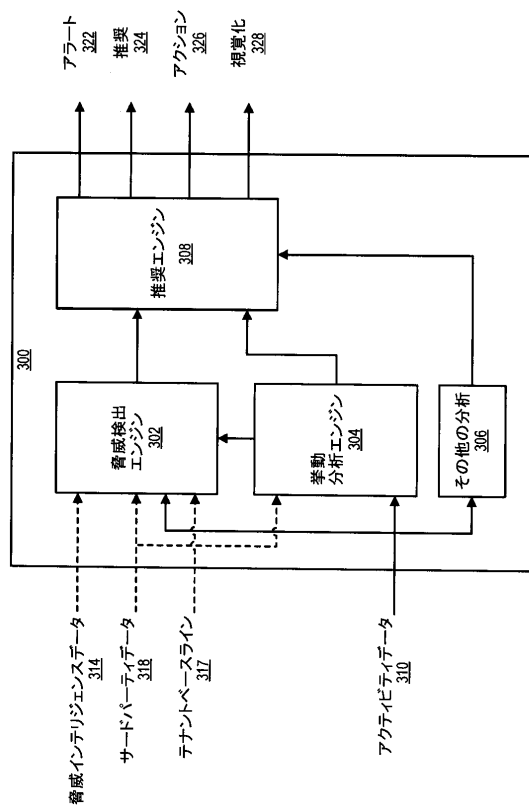
【 図面 】
【 図 1 】



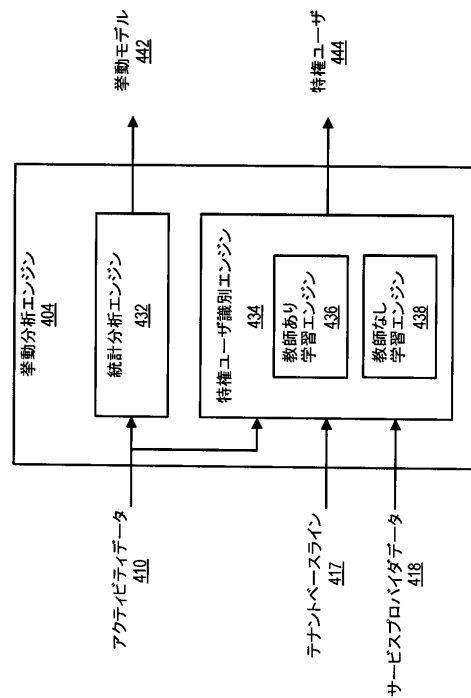
【 図 2 】



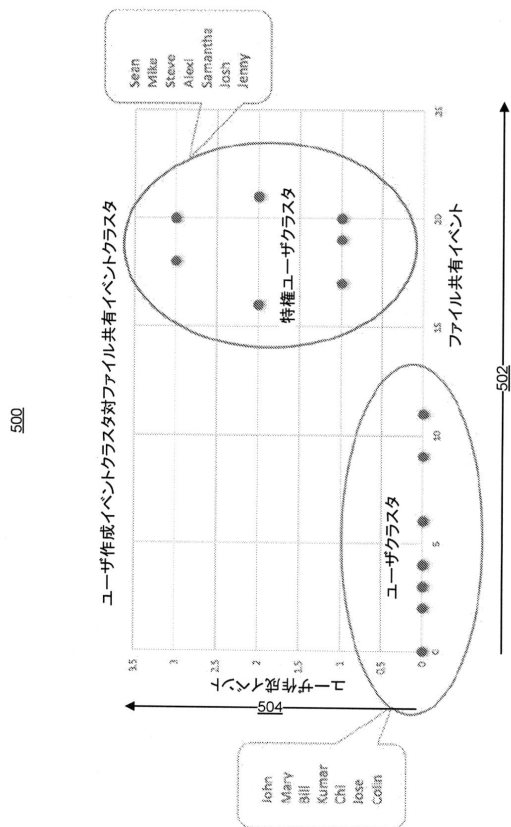
【 図 3 】



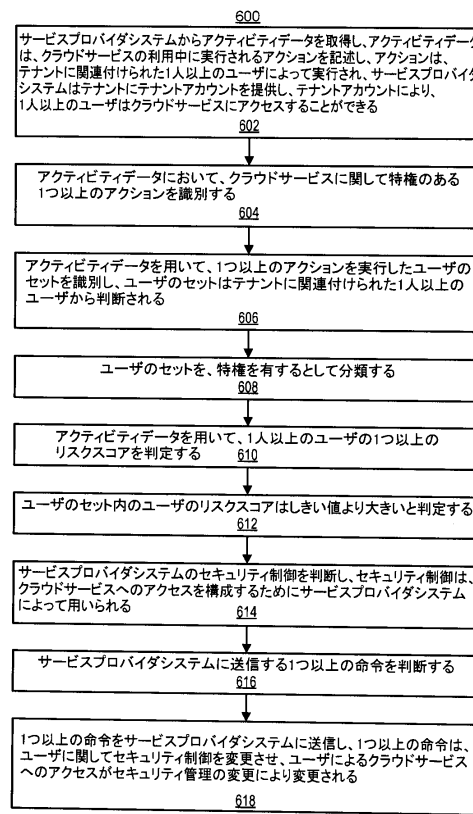
【圖 4】



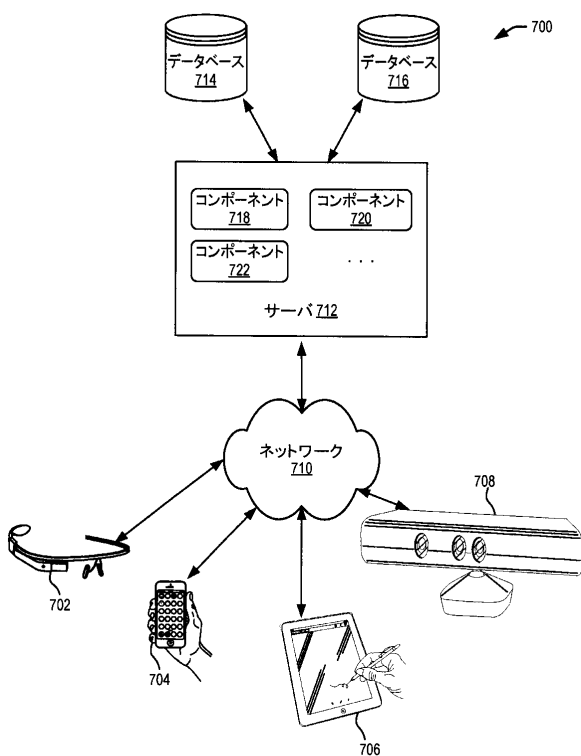
【図 5】



【図 6】



【図 7】



【図 8】

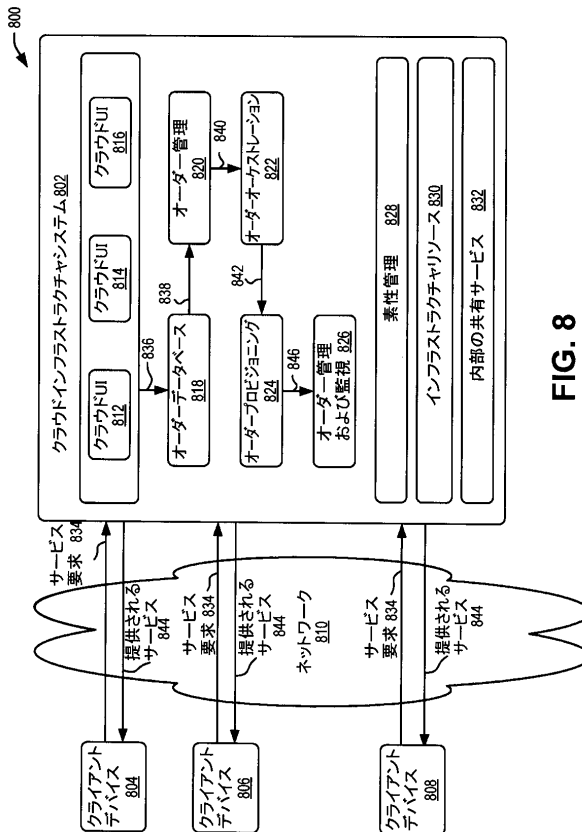


FIG. 7

FIG. 8

【図 9】

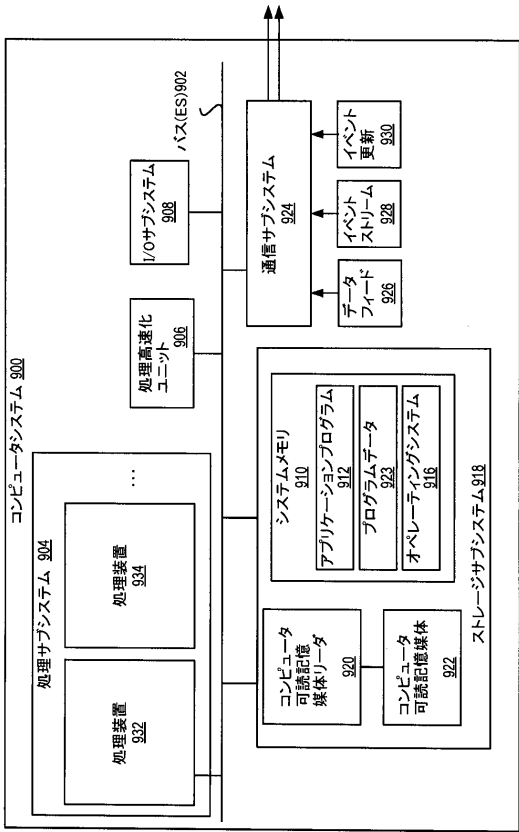


FIG. 9

10

20

30

40

50

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)

・レーン、 2 5 8 4

(72)発明者 ペレラ，メレンネ・スメーダ・ナリン

アメリカ合衆国、 9 4 4 0 2 カリフォルニア州、サン・マテオ、パーチ・アベニュー、 6 7 3

審査官 宮司 卓佳

(56)参考文献 特開 2 0 1 4 - 1 1 5 8 4 1 (J P , A)

特表 2 0 1 5 - 5 3 1 5 1 7 (J P , A)

(58)調査した分野 (Int.Cl. , D B 名)

G 0 6 F 2 1 / 0 0 - 2 1 / 8 8