(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)公開番号
特開2023-103341
(P2023-103341A)
(43)公開日　令和5年7月26日(2023.7.26)

(51)国際特許分類　FI
G06F 21/55 (2013.01)　G06F 21/55
G06F 21/62 (2013.01)　G06F 21/62 318

審査請求　有　請求項の数　12　OL　外国語出願　（全78頁）

(21)出願番号　特願2023-77773(P2023-77773)
(22)出願日　令和5年5月10日(2023.5.10)
(62)分割の表示　特願2022-31870(P2022-31870)の分割
原出願日　平成30年6月19日(2018.6.19)
(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)
(33)優先権主張国・地域又は機関
米国(US)

（特許庁注：以下のものは登録商標）
最終頁に続く

(71)出願人　502303739
オラクル・インターナショナル・コーポレイション
アメリカ合衆国カリフォルニア州９４０６５レッドウッド・シティー，オラクル・パークウェイ５００
(74)代理人　110001195
弁理士法人深見特許事務所
(72)発明者　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、トレーセル・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、マクラーレン
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)【要約】　（修正有）
【課題】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を可能とする方法、コンピュータシステム及び非一時的なコンピュータ可読媒体を提供する。
【解決手段】コンピューティング環境において、クラウドサービスのセキュリティを監視し、管理するためのセキュリティ監視および制御システムは、クラウドサービスからアクティビティログを取得する。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。セキュリティ監視および制御システムはまた、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し、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し、特権ユーザを特定すると、特権ユーザをより詳細に監視する。
【選択図】図６

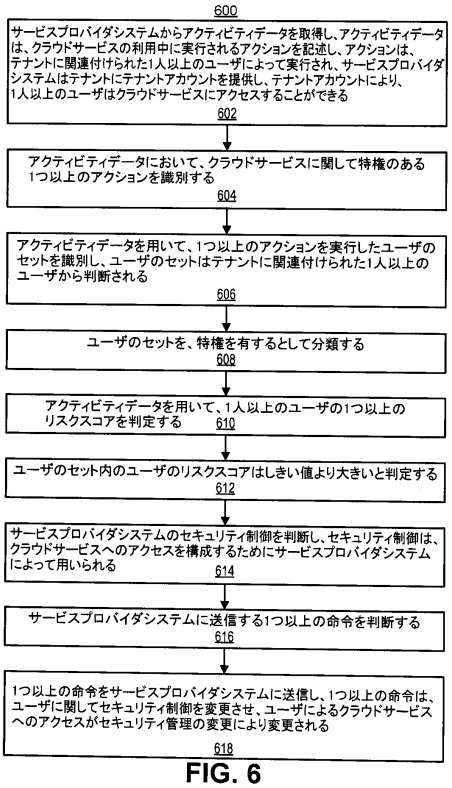

FIG. 6

【特許請求の範囲】
【請求項１】
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、
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、コンピューターにより実現される方法。
【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に記載のコンピュータにより実現される方法。
【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に記載のコンピュータにより実現される方法。
【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に記載のコンピュータにより実現される方法。
【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、
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、
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、
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。
【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、
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に記載のコンピューティングシステム。
【請求項１６】
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、前記命令は、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、前記１つ以上のプロセッサに、
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させ、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、前記命令は、さらに、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、
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させ、
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させ、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、前記命令は、さらに、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、
前記ユーザのセットを、特権を有するとして分類させ、
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させ、
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させ、
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させ、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、前記命令は、さらに、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、
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させ、
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させ、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、非一時的な

機械可読記憶媒体。
【請求項１７】
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１６に記載の非一時的な機械可読記憶媒体。
【請求項１８】
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１６に記載の非一時的な機械可読記憶媒体。
【請求項１９】
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、
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させてモデルを生成し、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、前記命令は、さらに、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、
前記モデルを用いさせて前記ユーザのセットを識別する、請求項１６に記載の非一時的な機械可読記憶媒体。
【請求項２０】
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、
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させ、
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させ、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１６に記載の非一時的な機械可読記憶媒体。
【請求項２１】
請求項１、２、３、４、５、６、７、８、９または１０に記載のコンピューターにより実現される方法。
【請求項２２】
請求項１、２、３、４、５、６、７、８、９または１０に記載の方法を実現するコンピュータシステム。
【請求項２３】
請求項１、２、３、４、５、６、７、８、９または１０記載の方法を実現する非一時的なコンピュータ可読媒体。
【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。
【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。

【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。

【０００４】

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。

【０００５】

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】

【０００６】

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。

【０００７】

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】

【０００８】

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、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。

【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】

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。

【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態様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。

【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。

【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充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】

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の能力はない。

【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跡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。

【００２９】

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。

【００３０】

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。

【００３１】

図１の例では、サービスプロバイダ１１０は、ネットワーク１５０を介してサービスプロバイダ１１０の顧客にアクセス可能な２つのサービス１１２ａ～１１２ｂを提供している。サービス１１２ａ～１１２ｂ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１１２ａ～１１２ｂ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１１２ａ～１１２ｂにアクセスできる）。いくつかの例では、サービス１１２ａ～１１２ｂは完全に独立して動作する。例えば、第１のサービス１１２ａは銀行業務アプリケーションであり得、第２のサービス１１２ｂ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１１０は、別個の無関係な製品として２つのサービス１１２ａ～１１２ｂを提供していてもよい。

【００３２】

サービスプロバイダ１１０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１００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。

【００３３】

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１３０のリソースは、企業ネットワーク１０４およびいくつかのクライアントデバイス１０６ａ～１０６ｃを含む。クライアントデバイス１０６ａ～１０６ｃ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１０６ａ～１０６ｃ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。

【００３４】

さまざまな例では、組織１３０のクライアントデバイス１０６ａ～１０６ｂ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１０６ａ～１０６ｂ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１０６ａ～１０６ｂ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１０６ａ～１０６ｂ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。

【００３５】

さまざまな例では、組織１３０のクライアントデバイス１０６ｃ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１０６ｃ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１０６ｃ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１０６ｃ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１０６ｃは、クライアントデバイス１０６ｃ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１０６ｃは、サービスプロバイダ１１０のサービス１１２ａ～１１２ｂ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。

【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１０６ａ～１０６ｃを介して組織１３０が加入するサービス１１２ａ～１１２ｂ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。

【００３７】

上述のように、サービスプロバイダのサービス１１２ａ～１１２ｂの加入者は、組織１３０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１０６ｄにアクセスを有してもよく、それを介してサービス１１２ａ～１１２ｂ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１５０にアクセスすることができるようにするＩＳＰ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１１２ａ～１１２ｂ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１０６ｄを用いて企業ネットワーク１０４に接続することはできず、なぜならば、個人が、組織１３０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１０４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。

【００３８】

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もよい。

【００３９】

いくつかの例では、クラウドサービスは、組織１３０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１３０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１１０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１１０を配置すること、サービスプロバイダ１１０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１３０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１１０は、サービスプロバイダ１１０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１３０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１３０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１３０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。

【００４０】

いくつかの例では、サービスプロバイダ１１０のサービス１１２ａ～１１２ｂは、組織１３０内から実行でき組織１３０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１３０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１１２ａ～１１２ｂが組織１３０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１１２ａ～１１２ｂ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１３０内で（たとえば、組織１３０のクライアントデバイス１０６ａ～１０６ｃ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１１２ａ～１１２ｂ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１１２ａ～１１２ｂ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１１２ｂ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１１２ｂ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１１２ｂ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１

１６は、ユーザが他のサービス１１２ｂ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１１２ｂに直接アクセスする。

【００４２】

クラウドサービス１１２ａ～１１２ｂの利用は、サービス１１２ａ～１１２ｂ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１１２ａ～１１２ｂ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１１２ａ～１１２ｂ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１１２ａ～１１２ｂ経由で組織１３０に入れさせる、もしくはサービス１１２ａ～１１２ｂ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１１２ａ～１１２ｂ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１１２ａ～１１２ｂ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もよい。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。

【００４４】

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、組織１３０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１０２は、企業ネットワーク１０４内のサーバ上で、組織１３０のファイアウォール１０８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１０２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１０２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。

【００４５】

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１０２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１０２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（ＳａａＳ）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１０２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１１０のサービ

ス１１２ａ～１１２ｂ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１０２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１３０のグループユーザが管理ユーザとして指定され、組織１３０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１０２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１０２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１０２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。

【００４６】

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、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１０２は、ハイパーテキストトランスポートプロトコル（ＨＴＴＰ）サーバ、ファイルトランスポートサービス（ＦＴＰ）サーバ、共通ゲートウェイインターフェース（ＣＧＩ）サーバ、Ｊａｖａ（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１０２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。

【００４７】

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、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１０２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１０２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。

【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。

【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に問い合わせて、ユーザアカウントを判断することができる。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１１２ａ～１１２ｂ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、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１１

０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１１２ａ～１１２ｂ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。

【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。

【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。

【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に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。

【００５９】
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。

【００６０】
【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
  }
```


【００６１】

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。

【００６２】

【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"
    }
}
```


【００６３】
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。
【００６４】
【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”
}
```


【００６５】

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。

【００６６】

【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” -
```

【００６７】

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。

【００７２】
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内の制御マネージャ１７２は、組織１３０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１１０のサービス１１２ａ～１１２ｂ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１７２は、複数のクラウドサービスまたは組織のユーザが用い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１７２は、アクセスポリシーを用いて、サービス１１２ａ～１１２ｂ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、用い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１７２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１７２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。

【００７３】
いくつかの例では、制御マネージャ１７２は、組織１３０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１３０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１０２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。

【００７４】
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１３０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１０４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１０８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１０６ａ～１０６ｃ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１７２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。

【００７５】
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１１０に命令を送信して、サービス１１２ａ～１１２ｂ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。たとえば、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１１２ａ～１１２ｂ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１０６ａ～１０６ｃ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。

【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。

【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。

【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係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、クラウドクローラーアプリケーション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ＡＰＩを含むことができる。さまざまな例において、クラウドクローラーアプリケーション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。

【００８９】

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、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。

【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ＡＰＩを用いて収集することができる。ＡＰＩおよびＡＰＩ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マティックメソッド（Javaのネイティブアプリケーションａｐｉ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。

【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。

【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

【００９３】

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。

【００９４】

【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／プロファイル 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

【００９５】

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２０２は、サービスプロバイダ２３０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２０８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（ＨＩＰＡＡ）、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（ＦｅｄＲＡＭＰ）、および／またはＰＣＩデータセキュリティスタンダード（ＰＣＩ　ＤＳＳ）などの規制および基準は、報告および監査証跡が必要であってもよい。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。

【００９６】

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２０８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２０８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ＮｏＳＱＬ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２０８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

プリケーションカタログを格納することができる。
【００９７】
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応じて、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。
【００９８】
さまざまな実現例において、クラウドシーダーアプリケーション２０４を用いて、テナント２２０のセキュリティポリシーを実現することができる。クラウドシーダーアプリケーション２０４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、クラウドシーダーアプリケーション２０４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、クラウドシーダーアプリケーション２０４は、脅威の救済の一部として、またはテナント２２０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、クラウドシーダーアプリケーション２０４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１０文字、２つの数字、１つの特殊文字、１つの大文字、最後の１０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。
【００９９】
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２０６は、サービスプロバイダ２３０からテナント２２０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２３０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２０６は、サービスプロバイダ２３０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２０６によって取得されたデータは、ランディングリポジトリ２１０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に入力することができる。ランディングリポジトリ２１０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２０６からのデータは、例えば、データが一様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２１１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。
【０１００】
さまざまな例では、データローダーアプリケーション２０６は、サービスプロバイダ２３０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２２０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２０６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２０６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。
【０１０１】
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／またはそれで実行し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。
【０１０２】
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。
【０１０３】
さまざまな例では、データローダーアプリケーション２０６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２１１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２１１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２１１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２１０に入力され、再フォーマットおよび／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。

【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。

【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。

【０１０８】

いくつかの例では、テナント２２０の単一のユーザは、サービスプロバイダ２３０および／またはサービスプロバイダ２３０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２０９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２０９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２２０は、サービスプロバイダ２３０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２０９は、テナント２２０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２３０のクレデンシャルを用いて、サービスプロバイダ２３０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。

【０１０９】

さまざまな実現例において、ユーザ素性リポジトリ２０９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２００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２００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２００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。

【０１１０】

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、クラウドセキュリティシステム２００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２０７および予測分析アプリケーション２１２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２０７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２１２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２１２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２０７および予測分析アプリケーション２１２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２１１に格納されたデータを用いて実行することができる。

【０１１１】

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、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２００においてテナントベースライン２１７と呼ばれるこれらのソースには、監視またはブロックすべき特定の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。

【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、クラウドシーダーアプリケーション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と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を呼び出して、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。

【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。
【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ロ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。
【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。
【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。
【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。
【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。

【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、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。

【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。

【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。

【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。

【０１３０】

【表３】

表３

ユーザID	avglogcntday_4wk	avglogipcntday_4wk	stdlogcntday_1wk	stdlogipcntday_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

【０１３１】

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。

【０１３２】

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。

【０１３３】

【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_ldy」）、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_ldy」）、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_

ｌｄｙ」）が含まれる。
【０１３５】
【表５】

表５

ユーザID	logcntday_1dy	logfailcntday_1dy	logfailipdisday_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

【０１３６】
さまざまな例では、挙動分析エンジン３０４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３０２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３０２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。
【０１３７】
いくつかの例では、脅威検出エンジン３０２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３０２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３１７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３０２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３１４、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３１８を代替的または追加的に受信することができる。
【０１３８】
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。
【０１３９】
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。
【０１４０】
【数５】

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

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

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

【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（ｗ１…ｗ３）と組み合わせることができる。

【０１４２】

【数６】

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

【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ｗ１＝１、ｗ２＝０、ｗ３＝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ｗｌ＝０．４、ｗ２＝０．６、ｗ３＝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ｗｌ＝０．２、ｗ２＝０．３、ｗ３＝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】

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

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

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

【０１４６】
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（ｗ１…ｗ３）と組み合わせることができる。
【０１４７】
【数８】

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

【０１４８】
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。
【０１４９】
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。
【０１５０】
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。
【０１５１】
【数９】

$$Diff_{Long} = 経度2 - 経度1$$

$$Diff_{Latitude} = 緯度2 - 緯度1$$

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

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

$$d = R \times c$$

【０１５２】

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。

【０１５３】

【数１０】

$$L1\ ZScore = \frac{過去２４時間の最大距離ＩＰログイン - １週間平均（１日あたりの最大距離ＩＰログイン）}{１週間標準偏差（１日あたりのＩＰログインＩＰ間の最大距離）}$$

$$L2\ ZScore = \frac{過去２４時間の最大距離ＩＰログイン - ４週間平均（１日あたりの最大距離ＩＰログイン）}{４週間標準偏差（１日あたりのＩＰログインＩＰ間の最大距離）}$$

$$L3\ ZScore = \frac{過去２４時間の最大距離ＩＰログイン - ８週間平均（１日あたりの最大距離ＩＰログイン）}{８週間標準偏差（１日あたりのＩＰログインＩＰ間の最大距離）}$$

【０１５４】

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

【０１５５】

【数１１】

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

【０１５６】

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、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。

【０１５７】

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。

【０１５８】

【数１２】

$$L1\ ZScore = \frac{過去２４時間の〔ブラウザ，ＯＳ〕カウント－１週間平均（１日あたりの〔ブラウザ，ＯＳ〕カウント）}{１週間標準偏差（１日あたりの〔ブラウザ，ＯＳ〕カウント）}$$

$$L2\ ZScore = \frac{過去２４時間の〔ブラウザ，ＯＳ〕カウント－４週間平均（１日あたりの〔ブラウザ，ＯＳ〕カウント）}{４週間標準偏差（１日あたりの〔ブラウザ，ＯＳ〕カウント）}$$

$$L3\ ZScore = \frac{過去２４時間の〔ブラウザ，ＯＳ〕カウント－８週間平均（１日あたりの〔ブラウザ，ＯＳ〕カウント）}{８週間標準偏差（１日あたりの〔ブラウザ，ＯＳ〕カウント）}$$

【０１５９】

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

【０１６０】

【数１３】

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

【０１６１】

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。

【０１６２】

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。

【０１６３】

【数１４】

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

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

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

【０１６４】

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

【０１６５】

【数１５】

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

【０１６６】

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。

【０１６７】

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３０２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。

【０１６８】

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３１４によって提供されてもよい。

【０１６９】

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「Ｉ１，Ｉ２，…Ｉｎ」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。

【０１７０】

【数１６】

$$リスクスコア = \frac{I_1W_1 + I_2W_s + \cdots + I_nW_n}{W_1 + W_2 + \cdots + W_n}$$

【０１７１】

上記の方程式では、「Ｗ１，Ｗ２，…Ｗｎ」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

受け取る。

【０１７２】

いくつかの例では、分析エンジン３００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３００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３０２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。

【０１７３】

さまざまな例において、脅威検出エンジン３０２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、$S = c_1(I_1) + c_2(I_2) + \cdots + c_n(I_n)$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。

【０１７４】

さまざまな例では、分析エンジン３００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３１０に対してさまざまな他の分析３０６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。

【０１７５】

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、Qualy、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ず、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。

【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。

【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用いることができる視覚化３２８を提供することができる。

【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】

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ーアカウントおよび／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ダー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。

【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と報告するまで、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得る。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。

【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。

【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もよい。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。

【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。

【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。

【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

。
【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。さまざまな例において、統計分析エンジン４３２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４４２を出力することができる。例えば、統計分析エンジン４３２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４３２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４３２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。
【０１９４】
さまざまな例では、挙動分析エンジン４０４は、クラウドサービスの特権ユーザ４４４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４３４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４３４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。
【０１９５】
第１の例として、特権ユーザ識別エンジン４３４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４１７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４１７で正確なリストを提供できない場合がある。
【０１９６】
第２の例として、特権ユーザ識別エンジン４３４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４１８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。
【０１９７】
さまざまな実現例では、テナントベースライン４１７および／またはサービスプロバイダデータ４１８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４３４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４１０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４３４は、教師あり学習エンジン４３６および／または教師なし学習エンジン４３８を含むことができる。
【０１９８】
さまざまな実現例において、教師あり学習エンジン４３６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４３６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。

【０１９９】

さまざまな例において、教師あり学習エンジン４３６は、サービスからのアクティビティデータ４１０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４３６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４３６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。

【０２００】

さまざまな例において、教師あり学習エンジン４３６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４０４は、教師あり学習エンジン４３６によって識別された特権ユーザ４４４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。レビューアは、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４３６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。

【０２０１】

さまざまな実現例において、教師なし学習エンジン４３８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４３８は、例えば、アクティビティデータ４１０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４３８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４３８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４３８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。

【０２０２】

一例として、Ｋ－ｍｅａｎｓ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４１０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４３８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４３８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４３８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。

【０２０３】

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。

【０２０４】

【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

【０２０５】

図５は、表６のデータのグラフ５００の例を示す。水平軸５０２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。

【０２０６】

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。

【０２０７】
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、通常の非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。

【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。

【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。

【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態様でリソースに影響

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態様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。

【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。

【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。

【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。

【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。

【０２１９】

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。

【０２２０】

ステップ６１２で、プロセス６００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。

【０２２１】

ステップ６１４で、プロセス６００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。

【０２２２】

ステップ６１６で、プロセス６００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ＡＰＩから判断することができる。ＡＰＩ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。

【０２２３】

ステップ６１８で、プロセス６００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。

【０２２４】

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７００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７００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７０２、７０４、７０６、および７０８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７０２、７０４、７０６、および７０８は、１つ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（Ｓ

ＭＳ）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。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。

【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の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。

【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７１

２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。

【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。

【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ス７０２、７０４、７０６、および７０８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Ｔｗｉｔｔｅｒ（登録商標）フィード、Ｆａｃｅｂｏｏｋ（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７１２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。

【０２３３】

また、分散型システム７００は、１つ以上のデータベース７１４および７１６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７１４および７１６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７１４および７１６のうちの１つ以上は、サーバ７１２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７１４および７１６は、サーバ７１２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７１２と通信していてもよい。ある例においては、データベース７１４および７１６は、ＳＡＮ（Storage-Area Network）に存在してもよい。同様に、サーバ７１２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７１２上のローカルな場所および／またはサーバ７１２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７１４および７１６は、ＳＱＬ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Ｏｒａｃｌｅ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。

【０２３４】

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８００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８００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８０４、８０６、および８０８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８０４、８０６、および８０８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８０２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８０２は、図７のサーバ７１２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。

【０２３５】

図８に示すクラウドインフラストラクチャシステム８０２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８０２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いてもよい。

【０２３６】

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、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に関して上述した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。

【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、ユーザで使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。

【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使用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。

【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し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。

【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、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８

０２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】

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。

【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。

【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。

【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。

【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】

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。

【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。

【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８０２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ＵＩ８１２、第２のクラウドＵＩ８１４、および／または第３のクラウドＵＩ８１６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。

【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。

【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。

【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。

【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。

【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。

【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。

【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。

【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、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を潜在的に含む、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、ポジトロン・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、インジケーターライト、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。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。

【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。
【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）１０ＯＳ、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。
【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可能な記憶媒体９２２は、Ｚｉｐ（登録商標）ドライブ、フラッシュメモリーカード、ＵＳＢ（Universal Serial Bus）フラッシュドライブ、ＳＤ（Secure Digital）カード、ＤＶＤ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９２２は、フラッシュメモリベースのＳＳＤ、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ＲＯＭなど、不揮発性メモリに基づくＳＳＤ（Solid-State Drives）、ソリッドステートＲＡＭ、動的ＲＡＭ、静的ＲＡＭなど、揮発性メモリに基づくＳＳＤ、ＤＲＡＭベースのＳＳＤ、磁気抵抗ＲＡＭ（ＭＲＡＭ）ＳＳＤ、およびＤＲＡＭのＳＳＤとフラッシュメモリベースのＳＳＤとの組合せを使用するハイブリッドＳＳＤを含んでもよい。コンピュータ読み取り可能な記憶媒体９２２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９００用の他のデータのストレージを提供してもよい。
【０２７４】
また、いくつかの例において、ストレージサブシステム９１８は、コンピュータ読み取り可能な記憶媒体９２２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９２０を含んでもよい。システムメモリ９１０と合わせて、必要に応じてシステムメモリ９１０と組み合わせて、コンピュータ読み取り可能な記憶媒体９２２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－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。
【０２７５】
いくつかの例において、コンピュータシステム９００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９００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、およびネットワーキング・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９００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９００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。

【０２７６】

通信サブシステム９２４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９２４は、コンピュータシステム９００からデータを受信し、コンピュータシステム９００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９２４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ネルを、インターネットを介してコンピュータシステム９００が確立することを可能にしてもよい。

【０２７７】

通信サブシステム９２４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９２４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ＲＦ（Radio Frequency）送信コンポーネント（たとえば、携帯電話技術、３Ｇ、４Ｇ、もしくはＥＤＧＥ（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、ＷｉＦｉ（ＩＥＥＥ　８０２．１１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）、ＧＰＳ（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９２４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、Ｅｔｈｅｒｎｅｔ）を提供できる。

【０２７８】

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ｗｅｂ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】

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。

【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。
【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、特定の一続きのト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、記載の一続きのト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。
【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。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。

【０２９０】

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。

【０２９１】

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。

【０２９２】

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。

【０２９３】

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。

【０２９４】

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。

【０２９５】

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。

【０２９６】

例１０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。

【０２９７】

例１１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１０の方法に従って動作を実行させる。

【０２９８】

例１２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１０の方法に従ってステップを実行させる。

【図面】

【図１】

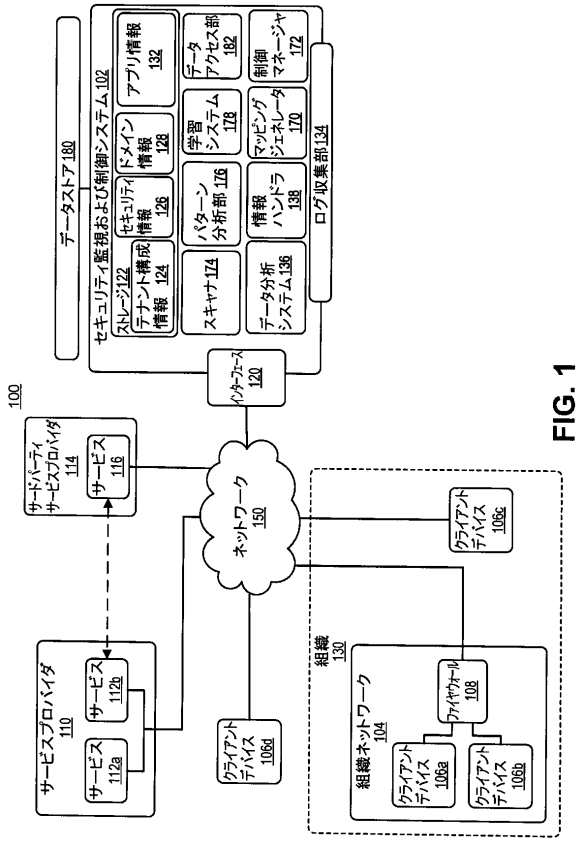

FIG. 1

【図２】

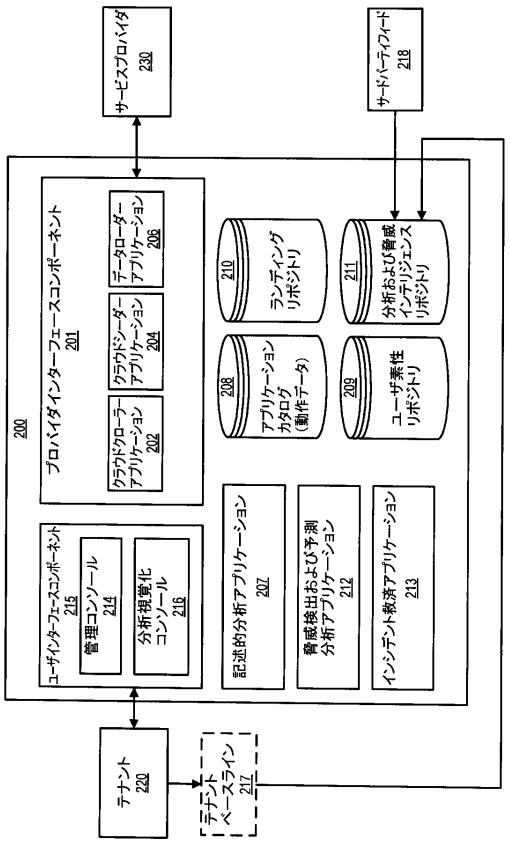

FIG. 2

【図３】

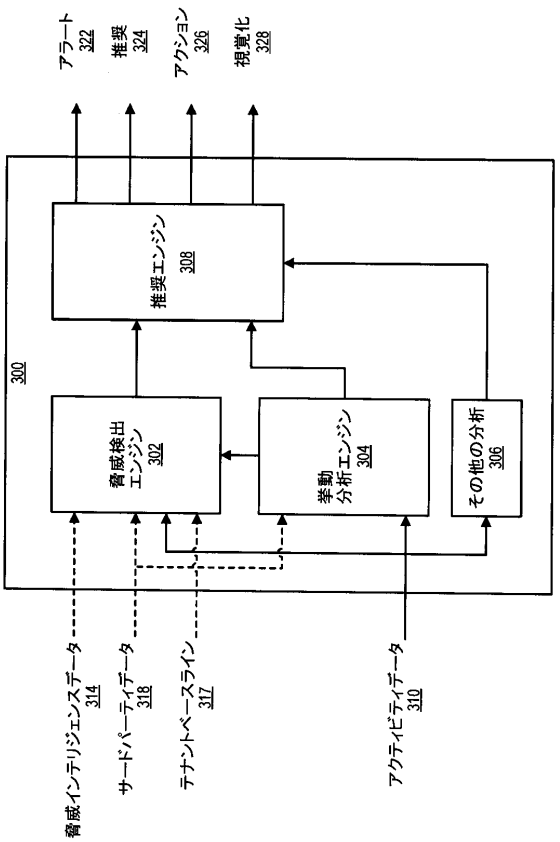

FIG. 3

【図４】

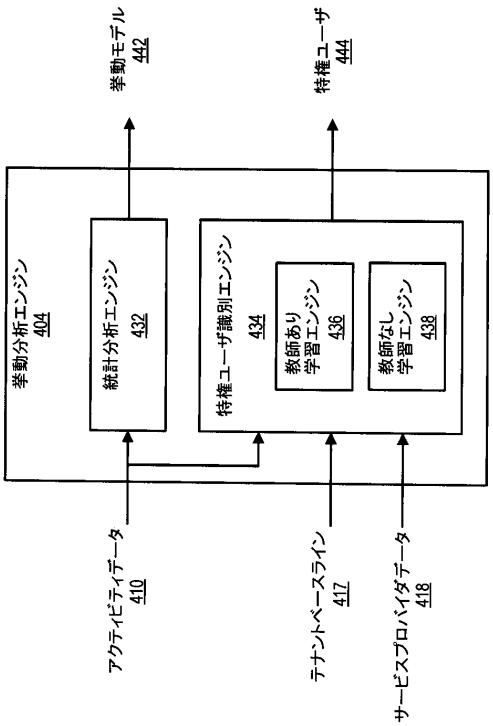

FIG. 4

【図５】

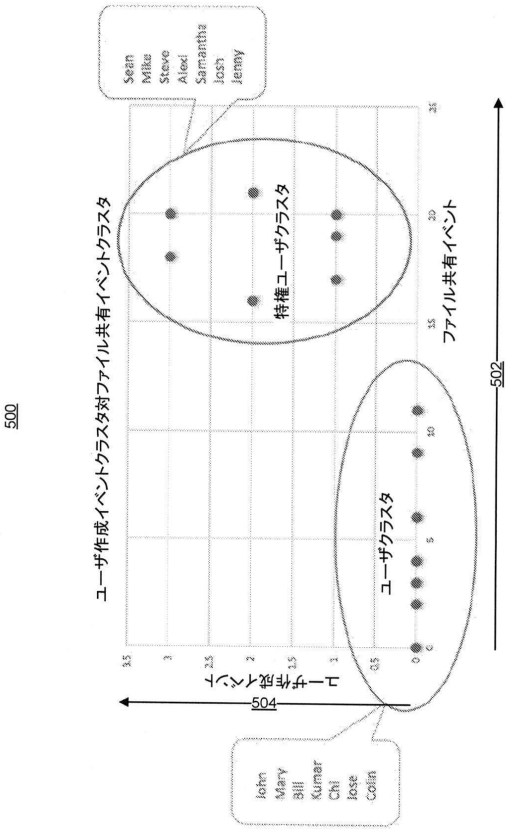

FIG. 5

【図６】

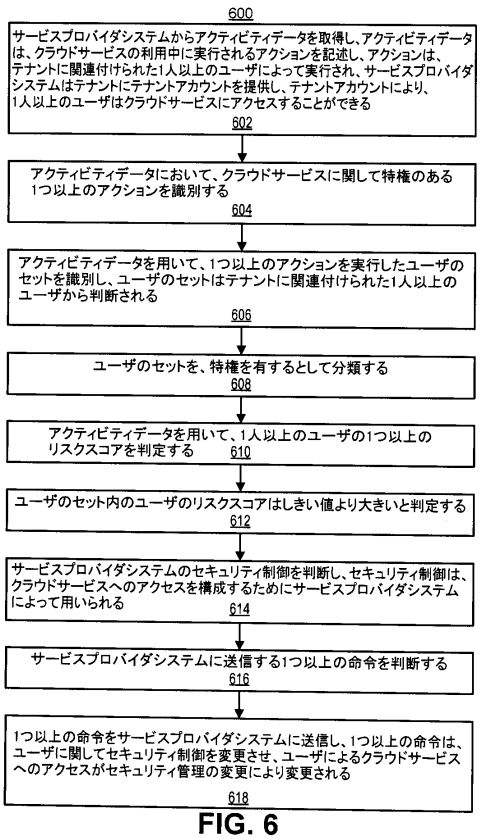

FIG. 6

【図７】

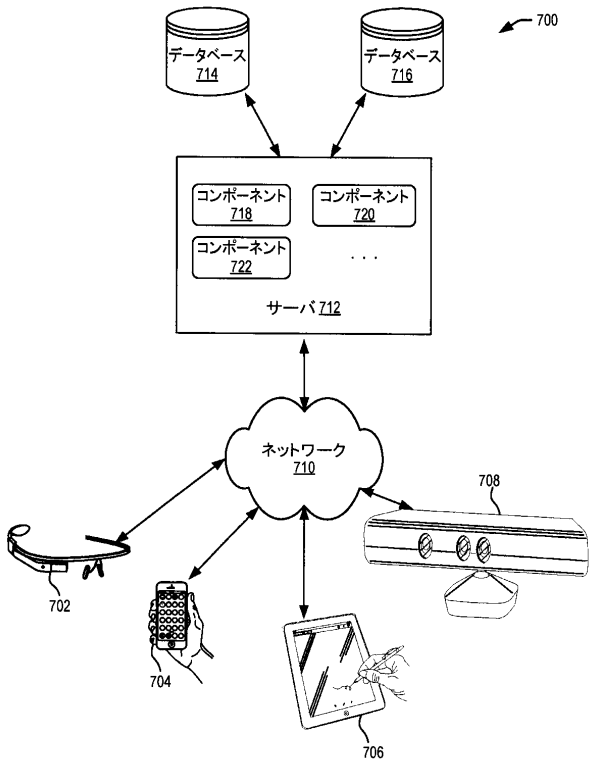

FIG. 7

【図８】

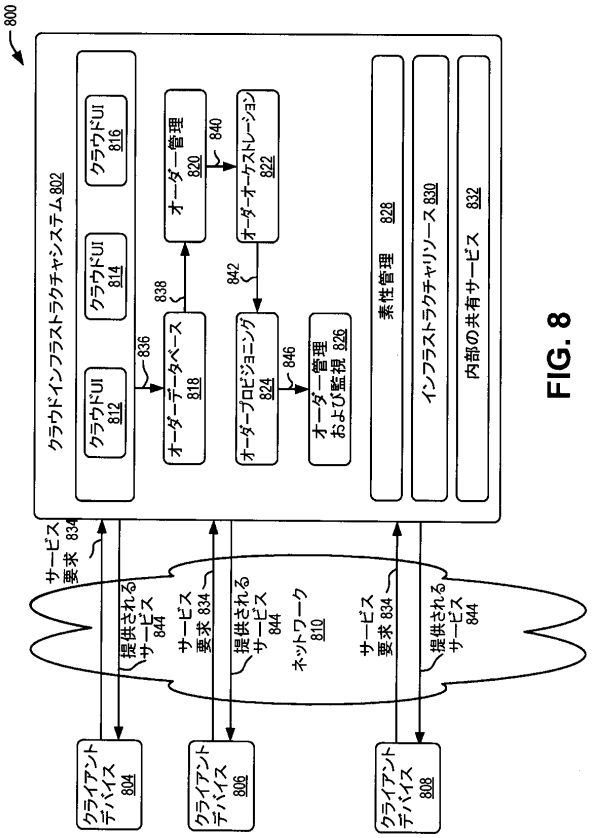

FIG. 8

【図９】

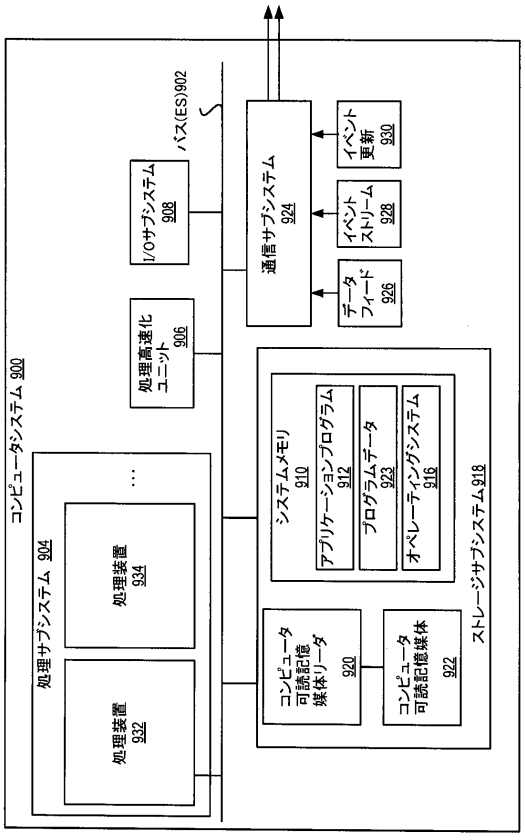

FIG. 9

【手続補正書】
【提出日】令和5年6月6日(2023.6.6)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
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ユーザによって実行されるアクションを記述し、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を受け、前記アクティビティデータにおけるアクションを実行したユーザから特権ユーザを分類するモデルに、前記アクティビティデータを提供することと、
前記モデルの出力に基づいて、前記サービスプロバイダシステムの特権ユーザのリストを生成することとを含む、コンピュータにより実現される方法。
【請求項２】
前記方法はさらに、
前記アクティビティデータを用いて、前記特権ユーザのリストについての１つ以上のリスクスコアがしきい値より大きいと判定することと、
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、前記方法はさらに、
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して、前記セキュリティ制御を前記ユーザに関して変更されるようにして、前記ユーザの前記クラウドサービスへのアクセスを修正することを含む、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つ以上のリスクスコアは、前記クラウドサービスの利用時に前記特権ユーザのリスト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、請求項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２に記載のコンピュータにより実現される方法。
【請求項５】
特権を有するとしてカテゴリ化されたユーザの前記１つ以上のリスクスコアは、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２に記載のコンピュータにより実現される方法。
【請求項６】
前記モデルは、教師あり学習モデルを含む、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。
【請求項７】
以前のアクティビティデータを用いて前記教師あり学習モデルをトレーニングすることをさらに含み、前記以前のアクティビティデータにおけるアクションは、特権アクションまたは非特権アクションとしてラベル付けされる、請求項６に記載のコンピュータにより実現される方法。
【請求項８】

前記サービスプロバイダシステムからの管理ユーザのリストを用いて前記教師あり学習モデルをトレーニングすることをさらに含む、請求項６に記載のコンピュータにより実現される方法。
【請求項９】
前記アクションは、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修正することができるアクションを含む、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】
前記アクションは、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を含む、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１１】
請求項１～１０のいずれかに記載の方法をシステムに実行させるための、プログラム。
【請求項１２】
請求項１１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１つ以上のプロセッサとを備える、システム。
【外国語明細書】
20231033410000033.pdf

フロントページの続き

１．ＰＹＴＨＯＮ
２．ＪＡＶＡＳＣＲＩＰＴ
３．ｉＯＳ
４．Ｐａｌｍ ＯＳ

・レーン、２５８４
(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、９４４０２ カリフォルニア州、サン・マテオ、バーチ・アベニュ、６７３