(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)公表番号
特表2024-540794
(P2024-540794A)
(43)公表日　令和6年11月6日(2024.11.6)

(51)国際特許分類　ＦＩ
Ｇ０６Ｆ　21/55　(2013.01)　Ｇ０６Ｆ　21/55　３２０

審査請求　未請求　予備審査請求　未請求　（全25頁）

(21)出願番号　特願2024-505476(P2024-505476)
(86)(22)出願日　令和4年10月6日(2022.10.6)
(85)翻訳文提出日　令和6年1月29日(2024.1.29)
(86)国際出願番号　PCT/IB2022/059544
(87)国際公開番号　WO2023/067425
(87)国際公開日　令和5年4月27日(2023.4.27)
(31)優先権主張番号　17/505,673
(32)優先日　令和3年10月20日(2021.10.20)
(33)優先権主張国・地域又は機関
米国(US)
(81)指定国・地域　AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,ST,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,
最終頁に続く

(71)出願人　523015600
パロ アルト ネットワークス （イスラエル アナリティクス） リミテッド
イスラエル国，６７８９１５５ テル アビブ，イーガル アロン ストリート ９４エイ，アロン １ タワー
(74)代理人　100107766
弁理士　伊東 忠重
(74)代理人　100229448
弁理士　中槇 利明
(72)発明者　ライマー，ネタネル
イスラエル国，７６３０８１０ レホボト，ピンスカー ストリート ８
(72)発明者　マイヤー，アビアド
イスラエル国，４５３４３２０ ホド ハ
最終頁に続く

(54)【発明の名称】　ユーザエンティティの正規化および関連付け

(57)【要約】
方法、装置、および電算プログラム製品は、単一のユーザエンティティに関連付けられた複数のユーザ識別子を識別することによってコンピュータシステムを保護することを含む、本発明の実施形態を実施する。ユーザ識別子のうち第１識別子を使用して実行される第１イベントが検出される。ユーザ識別子のうちの第１ユーザ識別子とは異なる、ユーザ識別子のうちの第２ユーザ識別子を使用して実行された第２イベントを検出すると、第１イベントおよび第２イベントの組み合わせに応答して、アラートを発行することができる。

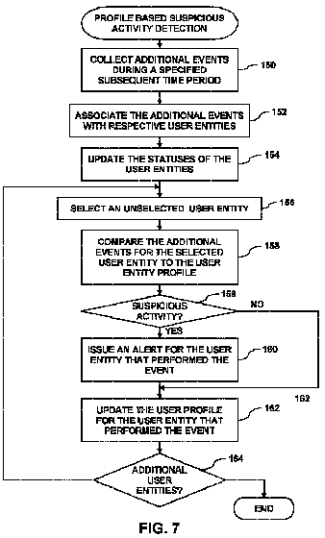

FIG. 7

【特許請求の範囲】
【請求項１】
コンピュータシステムを保護するための方法であって、
プロセッサによって、単一のユーザエンティティに関連付けられた複数のユーザ識別子を識別するステップと、
前記ユーザ識別子のうち第１ユーザ識別子を使用して実行される第１イベントを検出するステップと、
前記ユーザ識別子のうち前記第１ユーザ識別子とは異なる第２ユーザ識別子を使用して実行される第２イベントを検出するステップと、
前記第１イベントおよび前記第２イベントの組み合わせに応答して、アラートを発行するステップと、
を含む、方法。
【請求項２】
前記単一のユーザエンティティに関連付けられた複数のユーザ識別子を識別する前記ステップは、
前記第１イベントおよび前記第２イベントを含むイベントのセットを収集すること、
前記セット内のイベントからそれぞれのユーザ識別子を抽出すること、
抽出された前記ユーザ識別子をそれぞれのアカウントにマッピングすること、および、
前記アカウントをそれぞれのユーザエンティティに関連付けること、
を含み、
前記単一のユーザエンティティは、複数のユーザエンティティのうち１つを含む、
請求項１に記載の方法。
【請求項３】
所与の抽出されたユーザ識別子を所与のアカウントにマッピングすることは、
所与のユーザエンティティを特定のフォーマットに正規化することを含み、
前記所与のアカウントは、前記正規化されたユーザエンティティを含む、
請求項２に記載の方法。
【請求項４】
前記単一のユーザエンティティは、１つ以上のアカウントに関連付けられる、
請求項２に記載の方法。
【請求項５】
複数のユーザ識別子は、前記単一のユーザエンティティの所与のアカウントにマッピングされる、
請求項２に記載の方法。
【請求項６】
第１イベントを検出する前記ステップは、
第１ネットワーク化エンティティ上で前記第１イベントを検出すること、を含み、
第２イベントを検出する前記ステップは、
前記第１ネットワーク化エンティティとは異なる第２ネットワーク化エンティティ上で前記第２イベントを検出すること、を含む、
請求項１乃至５いずれか一項に記載の方法。
【請求項７】
第１イベントを検出する前記ステップは、
第１期間の最中に複数の第１イベントを検出すること、および、前記複数の第１イベントに応答して、プロファイルを生成すること、を含み、
第２イベントを検出する前記ステップは、
前記第１期間に続く第２期間の最中に１つ以上の第２イベントを検出すること、を含み、
前記第１イベントおよび前記第２イベントの組み合わせは、前記１つ以上の第２イベン

トが前記プロファイルに従っていないことを検出すること、を含む、
請求項１乃至５いずれか一項に記載の方法。
【請求項８】
前記第１イベントは、前記単一のユーザエンティティの時間ベースのステータスを含み、かつ、
前記第２イベントは、前記時間ベースのステータスに従わない、
請求項１乃至５いずれか一項に記載の方法。
【請求項９】
コンピュータネットワークを保護するための装置であって、
ネットワークインターフェイスカード(ＮＩＣ)と、
少なくとも１つのプロセッサと、を含み、
前記プロセッサは、
単一のユーザエンティティに関連付けられた複数のユーザ識別子を識別し、
前記ユーザ識別子のうち第１ユーザ識別子を使用して実行される第１イベントを検出し、
前記ユーザ識別子のうち前記第１ユーザ識別子とは異なる第２ユーザ識別子を使用して実行される第２イベントを検出し、かつ、
前記第１イベントおよび前記第２イベントの組み合わせに応答して、アラートを発行する、
ように構成されている、装置。
【請求項１０】
所与のプロセッサは、
前記第１イベントおよび前記第２イベントを含むイベントのセットを収集すること、
前記セット内のイベントからそれぞれのユーザ識別子を抽出すること、
抽出された前記ユーザ識別子をそれぞれのアカウントにマッピングすること、および、
前記アカウントをそれぞれのユーザエンティティに関連付けること、
によって、前記単一のユーザエンティティに関連付けられた複数のユーザ識別子を識別するように構成されており、
前記単一のユーザエンティティは、複数のユーザエンティティのうち１つを含む、
請求項９に記載の装置。
【請求項１１】
所与のプロセッサは、所与のユーザエンティティを特定のフォーマットに正規化することによって、所与の抽出されたユーザ識別子を所与のアカウントにマッピングするように構成されており、
前記所与のアカウントは、前記正規化されたユーザエンティティを含む、
請求項１０に記載の装置。
【請求項１２】
前記単一のユーザエンティティは、１つ以上のアカウントに関連付けられる、
請求項１０に記載の装置。
【請求項１３】
複数のユーザ識別子は、前記単一のユーザエンティティの所与のアカウントにマッピングされる、
請求項１２に記載の装置。
【請求項１４】
所与のプロセッサは、
ネットワークの第１ネットワーク化エンティティ上で前記第１イベントを検出することによって、前記第１イベントを検出し、かつ、
前記第１ネットワーク化エンティティとは異なる第２ネットワーク化エンティティ上で前記第２イベントを検出することによって、前記第２イベントを検出する、

ように構成されている、
請求項９乃至１３いずれか一項に記載の装置。
【請求項１５】
所与のプロセッサは、第１期間の最中に複数の第１イベントを検出することによって、前記第１イベントを検出するように構成されており、
前記所与のプロセッサは、さらに、前記複数の第１イベントに応答して、プロファイルを生成するように構成されており、
前記所与のプロセッサは、前記第１期間に続く第２期間の最中に１つ以上の第２イベントを検出することによって、第２イベントを検出するように構成されており、かつ、
前記第１イベントおよび前記第２イベントの組み合わせは、前記１つ以上の第２イベントが前記プロファイルに従っていないことを検出すること、を含む、
請求項９乃至１３いずれか一項に記載の装置。
【請求項１６】
前記第１イベントは、前記単一のユーザエンティティの時間ベースのステータスを含み、かつ、
前記第２イベントは、前記時間ベースのステータスに従わない、
請求項９乃至１３いずれか一項に記載の装置。
【請求項１７】
コンピュータプログラムであって、前記コンピュータプログラムは、コンピュータ命令を含み、非一時的コンピュータ可読媒体に保管されており、
前記コンピュータ命令は、プロセッサによって実行されると、前記コンピュータに、
単一のユーザエンティティに関連付けられた複数のユーザ識別子を識別し、
前記ユーザ識別子のうち第１ユーザ識別子を使用して実行される第１イベントを検出し、
前記ユーザ識別子のうち前記第１ユーザ識別子とは異なる第２ユーザ識別子を使用して実行される第２イベントを検出し、かつ、
前記第１イベントおよび前記第２イベントの組み合わせに応答して、アラートを発行する、
ようにさせる、コンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般的に、コンピュータセキュリティおよびネットワークに関する。そして、特には、イベントログ内のユーザ識別子をユーザエンティティに関連付けること、および、ログ内のイベントに基づいてユーザエンティティプロファイルを生成することに関する。
【背景技術】
【０００２】
多くのコンピュータおよびネットワークシステムにおいては、セキュリティ脅威の絶えず増大する範囲を検出し、かつ、撃退するために、多層のセキュリティ装置およびソフトウェアが配備されている。最も基本的なレベルにおいて、コンピュータは、不正プログラムがコンピュータ上で実行されているのを防止するために、アンチウイルスソフトウェアを使用する。ネットワークレベルにおいて、侵入検出および防止システムは、マルウェアがネットワークを通じて拡散することを検出および防止するために、ネットワークトラフィックを分析し、かつ、制御する。
【０００３】
上記の説明は、この分野における関連技術の一般的な概要として提示されているものであり、そして、それが含む情報のいずれかが本特許出願に対する先行技術を構成することを認めるものと解釈されるべきではない。
【発明の概要】

【０００４】
本発明の一つの実施形態に従って、コンピュータシステムを保護するための方法が提供される。本方法は、プロセッサによって、単一のユーザエンティティに関連付けられた複数のユーザ識別子を識別するステップと、前記ユーザ識別子のうち第１ユーザ識別子を使用して実行される第１イベントを検出するステップと、前記ユーザ識別子のうち前記第１ユーザ識別子とは異なる第２ユーザ識別子を使用して実行される第２イベントを検出するステップと、前記第１イベントおよび前記第２イベントの組み合わせに応答して、アラートを発行するステップとを含む。
【０００５】
いくつかの実施形態において、前記単一のユーザエンティティに関連付けられた複数のユーザ識別子を識別する前記ステップは、前記第１イベントおよび前記第２イベントを含むイベントのセットを収集すること、前記セット内のイベントからそれぞれのユーザ識別子を抽出すること、抽出された前記ユーザ識別子をそれぞれのアカウントにマッピングすること、および、前記アカウントをそれぞれのユーザエンティティに関連付けることを含む。ここで、前記単一のユーザエンティティは、複数のユーザエンティティのうち１つを含む。
【０００６】
第１実施形態において、所与の抽出されたユーザ識別子を所与のアカウントにマッピングすることは、所与のユーザエンティティを特定のフォーマットに正規化することを含む。ここで、記所与のアカウントは、前記正規化されたユーザエンティティを含む。
【０００７】
第２実施形態において、前記単一のユーザエンティティは、１つ以上のアカウントに関連付けられる。
【０００８】
第３実施形態において、複数のユーザ識別子は、前記単一のユーザエンティティの所与のアカウントにマッピングされる。
【０００９】
追加的な実施形態において、第１イベントを検出することは、第１ネットワーク化エンティティ上で第１イベントを検出することを含み、第２イベントを検出することは、第１ネットワーク化エンティティとは異なる第２ネットワーク化エンティティ上で第２イベントを検出することを含む。
【００１０】
さらなる実施形態において、第１イベントを検出する前記ステップは、第１期間の最中に複数の第１イベントを検出すること、および、前記複数の第１イベントに応答して、プロファイルを生成することを含む。ここで、第２イベントを検出する前記ステップは、前記第１期間に続く第２期間の最中に１つ以上の第２イベントを検出することを含み、そして、前記第１イベントおよび前記第２イベントの組み合わせは、前記１つ以上の第２イベントが前記プロファイルに従っていないことを検出することを含む。
【００１１】
補足的な実施形態において、前記第１イベントは、前記単一のユーザエンティティの時間ベースのステータスを含み、かつ、前記第２イベントは、前記時間ベースのステータスに従わない。
【００１２】
本発明の一つの実施形態に従って、コンピュータネットワークを保護するための装置が提供される。本装置は、ネットワークインターフェイスカード(NIC)と、少なくとも１つのプロセッサとを含む。前記プロセッサは、単一のユーザエンティティに関連付けられた複数のユーザ識別子を識別し、前記ユーザ識別子のうち第１ユーザ識別子を使用して実行される第１イベントを検出し、前記ユーザ識別子のうち前記第１ユーザ識別子とは異なる第２ユーザ識別子を使用して実行される第２イベントを検出し、かつ、前記第１イベントおよび前記第２イベントの組み合わせに応答して、アラートを発行するように構成されて

いる。
【００１３】
本発明の一つの実施形態に従って、コンピュータシステムを保護するためのコンピュータソフトウェア製品が追加的に提供される。本製品は、プログラム命令が保管された非一時的コンピュータ可読媒体を含む。本命令は、コンピュータによって読み取られると、前記コンピュータに、単一のユーザエンティティに関連付けられた複数のユーザ識別子を識別し、前記ユーザ識別子のうち第１ユーザ識別子を使用して実行される第１イベントを検出し、前記ユーザ識別子のうち前記第１ユーザ識別子とは異なる第２ユーザ識別子を使用して実行される第２イベントを検出し、かつ、前記第１イベントおよび前記第２イベントの組み合わせに応答して、アラートを発行するようにさせる。
【図面の簡単な説明】
【００１４】
本開示は、添付の図面を参照して、単なる例として、本明細書に記載されている。
【図１】図1は、本発明の一つの実施形態に従った、ネットワークイベントログから取り出されたイベントに基づいて、ユーザエンティティについてのアクティビティプロファイルを生成するように構成された、セキュリティサーバを備えるコンピューティングファシリティを概略的に示すブロック図である。
【図２】図2は、本発明の一つの実施形態に従った、所与のイベントログの一つの例を示すブロック図である。
【図３】図3は、本発明の一つの実施形態に従った、セキュリティサーバに保管された集約イベントログ（aggregated event log）の一つの例を示すブロック図である。
【図４】図4は、本発明の一つの実施形態に従った、ドメインデータベースサーバによって保管され得るデータベースレコードの一つの例を示すブロック図である。
【図５】図5は、本発明の一つの実施形態に従った、セキュリティサーバ上に保管されたユーザエンティティ情報の一つの例を示すブロック図である。
【図６】図6は、本発明の一つの実施形態に従った、アクティビティプロファイルを生成する方法を概略的に示すフローチャートである。
【図７】図7は、本発明の一つの実施形態に従った、疑わしいアクティビティを検出するために生成されたアクティビティプロファイルを使用する方法を概略的に示すフローチャートである。
【発明を実施するための形態】
【００１５】
コンピュータネットワークにわたり通信するネットワーク化エンティティ（networked entity）は、典型的に、ネットワーク化エンティティにおけるイベントを記録（record）するログを保管している。これらのログは、イベントについての識別子を含むことができるが、一方で、ユーザエンティティ(例えば、組織の従業員)は、ネットワーク上のデータにアクセスするときに、複数のアカウント(例えば、電子メールアカウント)を使用することができ、そして、各アカウントは、ネットワーク上のデータにアクセスするときに、複数の識別子を使用することができる。従って、ネットワーク上の異なるアカウントおよび異なるユーザ識別子を使用して、所与のユーザエンティティによって実行される疑わしい／悪意（suspicious/malicious）のあるアクティビティを検出することは困難であり得る。
【００１６】
本発明の実施形態は、単一のユーザエンティティに関連付けられた複数のユーザ識別子を識別することによって、コンピュータシステムを保護するための方法およびシステムを提供する。ユーザ識別子のうちの第１ユーザ識別子を使用して実行された第１イベントを検出し、かつ、ユーザ識別子のうちの第１ユーザ識別子とは異なるユーザ識別子のうちの第２ユーザ識別子を使用して実行された第２イベントを検出すると、第１イベントおよび第２イベントの組み合わせに応答して、アラートを発行することができる。いくつかの実施形態において、第１イベントは、第１ネットワーク化エンティティ上の第１ログから収

集され、そして、第２イベントは、第１ネットワーク化エンティティとは異なる第２ネットワーク化エンティティ上の第２ログから収集される。

【００１７】

一つの実施形態においては、コンピュータネットワークに結合されたネットワーク化エンティティ上の複数のイベントログから、複数のイベントを収集することができる。識別子は、イベントから抽出され得る。識別子は、イベントをアカウントにマッピングするように正規化され得る。そして、アカウントのサブセットは、単一のユーザエンティティに関連付けられ得る。ユーザエンティティプロファイルが、次いで、単一のユーザエンティティに関連付けられたイベントに基づいて生成され得る。この実施形態を使用して、本発明の実施形態を実施するシステムは、単一のユーザエンティティに関連付けられた任意の後続のイベントが、ユーザエンティティプロファイルに従っていないと判定された場合に、疑わしいアクティビティを検出し、かつ、フラグ付けすることができる。

【００１８】

システムの説明

図1は、本発明の一つの実施形態に従った、複数のネットワーク化エンティティによってそれぞれのイベントログ26に記録されたアクティビティに基づいて、ユーザエンティティアクティビティプロファイル24を生成するように構成された、セキュリティサーバ22を備えるコンピューティングファシリティ20の一つの例を概略的に示すブロック図である。図1に示される構成において、セキュリティサーバ22は、ローカルエリアネットワーク(データベースサーバ)32といったデータネットワークにわたり、複数のコンピューティングデバイス28(ホストまたはホストコンピュータとしても、また、知られるもの)、アカウントLAN　29、および人事(HR)サーバ30と通信するように構成されている。

【００１９】

アカウントデータベースサーバ29は、ドメインデータベース管理システム(DBMS)アプリケーション31およびドメインデータベース37を含み有み得る。アカウントデータベース33は、以下で図4を参照する記載において説明されているアカウントデータベースレコード35のセットを含んでいる。

【００２０】

コンピューティングファシリティ20は、また、インターネットゲートウェイ34を含み得る。これは、コンピューティングファシリティ20をインターネットといったパブリックネットワーク36に結合する。コンピューティングデバイス28を保護するために、コンピューティングファシリティ20は、LAN32に結合され、かつ、所定のセキュリティルールに基づいて、コンピューティングデバイス28と、１つ以上のクラウドサーバ42を含むデータクラウド40との間のデータトラフィックを制御する、ファイアウォール38も含み得る。

【００２１】

上述のように、セキュリティサーバ22は、複数のネットワーク化エンティティによって、それぞれのイベントログ26に記録されたアクティビティに基づいて、ユーザエンティティプロファイル24を生成するように構成され得る。図1の構成は、ネットワーク化エンティティがコンピューティングデバイス28、ファイアウォール38、およびクラウドサーバ42を含むことを示しているが、ネットワークにわたり通信する任意の他のタイプのネットワーク化エンティティは、本発明の趣旨および範囲内にあるものと考えられる。

【００２２】

図1に示される構成において、イベントログ26は、識別番号に文字を付加することによって区別することができ、その結果、ウェブページは、以下のようになる。

●オペレーティングシステム(OS)ログ26Aは、コンピューティングデバイス28上で実行されるオペレーティングシステム(マイクロソフト社によって製造されるWindows（登録商標）、およびLinux(登録商標)といったもの)、およびアプリケーションによって生成されるイベントに関する情報を保管する。

●エンドポイント検出および応答(endpoint detection and response、EDR)

ログ26Bは、コンピューティングデバイス28上で実行されるエンドポイントエージェント44(例えば、95054　米国カリフォルニア州、サンタクララ、タンナーウェイ3000のパルアルトネットワーク社によって製造されたXDR™)によって検出されたイベントに関する情報を保管する。

●ファイアウォールログ26Cは、コンピューティングファシリティ20(例えば、コンピューティングデバイス28)と、インターネット36に結合されたサーバ(例えば、クラウドサーバ42)との間の送信に関する情報を保管する。ファイアウォール38の一つの例は、パルアルトネットワーク社によって製造されたPA-3250 Next Generation Firewall™である。

●クラウドイベントログ26Dは、クラウドサーバ42によって生成されたイベントに関する情報を保管する。ログ26の例は、これらに限定されるわけではないが、アプリケーションログ、リソースログ、およびAmazon Web Service(98109　米国ワシントン州、ノースシアトル、テリーアベニュー410のアマゾンドットコム社によって提供されるもの)についてのサービスログを含む。

【００２３】

本明細書で説明される実施形態において、セキュリティサーバ22は、ログ26からユーザ識別子(ID)を抽出し、ユーザIDを正規化し、かつ、正規化されたユーザIDをユーザエンティティ(すなわち、従業員といった個々の人々)に関連付ける。いくつかの実施形態において、HRサーバ30は、各ユーザエンティティの情報を保管するHRデータベース46を保管している。いくつかの実施形態において、HRデータベース46は、組織のユーザエンティティ(すなわち、従業員)との一対一の対応を有するレコード47のセットを含んでいる。

【００２４】

セキュリティサーバ22は、プロセッサ48、メモリ50、および、セキュリティサーバをネットワークインターフェイスカード32に結合するローカルエリアネットワーク(NIC)51を含んでいる。いくつかの実施形態において、プロセッサ48は、ログ26を集約イベントログ52へと組み合わせることができる。イベントログ26および52は、それぞれに、以下で図2および図3を参照する記載において説明されている。

【００２５】

本明細書において説明される実施形態において、プロセッサ48は、イベントログ24A－24Dからイベントを収集し、そして、集約イベントログ52に保管するが、他のタイプのイベントログ26から集約イベントログへとイベントを集約することは、本発明の趣旨および範囲内にあるものと考えられる。１つ以上の追加のイベントログ26によって保管され得る情報の例は、これらに限定されるわけではないが、以下を含む。

●入力／出力(I/O)イベント(ファイルイベントとしても、また、知られる)。I/Oイベントの一つの例は、「local_file＼malicious.exe」という名前のファイルを書き込むドメインアカウント「Company＼jdoe」である。ドメインアカウントについては後述する。

●レジストリイベント。レジストリイベントの一つの例は、値「local_file＼malicious.exe」を有する、Autorunに関連するレジストリキーを修正するドメインアカウント「Company＼jdoe」である。

●プロセス実行イベント。プロセス実行イベントの一つの例は、ドメインアカウント「company＼jdoe」の許可を伴い「local_file＼malicious.exe」を自動的に実行するSYSTEMである。

●ネットワークイベント。ネットワークイベントの一つの例は、local_file＼malicious.exeという名前のプロセスを使用して、「www.malware_command_and_control.com」へのHTTP要求を実行したドメインアカウント「company＼jdoe」である。

●シングルサインオン(SSO)イベント。SSOサービス(例えば、Okta™、PingOne™、AzureAD™)は、典型的に、監査ログ（audit log）を提供する。プロセッサ48が収集できるイベントの一つの例は、ログインするSSOアカウント「john.doe@compan

y.com」である。

●電子メールイベント。電子メールイベントを保管する電子メールログは、Outlook™といったローカルシステム、ExchangerServer™といったサーバ(すなわち、企業)システム、および、ExchangeOnline™といったクラウドベースの電子メールサーバから収集され得る。ローカルシステムにおける電子メールイベントの例は、「john.doe@gmail.com」によって送信／受信される電子メールである。サーバシステムにおける電子メールイベントの一つの例は、「johndoe@company.com」によって送信／受信される電子メールである。クラウドベースのシステムにおける電子メールイベントの一つの例は、「john_doe@cloud_email_provider.com」によって送信／受信される電子メールである。

【００２６】

図1に示される構成において、メモリ50は、また、プロファイル24を保管する複数のユーザエンティティレコード54も保管する。いくつかの実施形態において、各所与のユーザエンティティレコード54は、HRデータベース46から所与のユーザエンティティについての情報を取り出し、そして、取り出された情報を所与のユーザエンティティレコードに保管することができる。

【００２７】

いくつかの実施形態において、イベントログ26からユーザIDを抽出すること、ユーザIDを正規化すること、正規化されたユーザIDをユーザエンティティに関連付けること、ログ26を集約イベントログ52へと集約すること、および、ユーザエンティティプロファイル24を生成すること、といった、本明細書で説明されるタスクは、コンピューティングファシリティ20内の、または、コンピューティングファシリティの外部の複数のコンピュータシステム22、28、および30(例えば、クラウドサーバ42)の間で分割され得る。追加的な実施形態において、コンピューティングデバイス28、セキュリティサーバ22、アカウントデータベースサーバ29、およびHRサーバ30の一部または全部の機能性は、物理的コンピューティングデバイス、仮想マシンまたはコンテナとして、コンピューティングファシリティ20及び／又はインターネット36内に配備され得る。

【００２８】

いくつかの実施形態において、クライアントコンピュータ28は、クライアントコンピュータのそれぞれを識別するために使用され得る、それぞれのホスト名56を有している。

【００２９】

プロセッサ48は、汎用中央処理装置(CPU)または専用組み込みプロセッサを含み、これらは、本明細書で説明される機能を実行するためにソフトウェアまたはファームウェアでプログラムされている。このソフトウェアは、例えば、ネットワークにわたり、電子形式でセキュリティサーバ22にダウンロードされ得る。追加的または代替的に、ソフトウェアは、光学、磁気、または電子メモリ媒体といった、有形の、非一時的コンピュータ可読媒体に保管され得る。さらに追加的または代替的に、プロセッサ48の機能の少なくともいくつかは、ハードワイヤードまたはプログラマブルデジタル論理回路によって実行され得る。

【００３０】

メモリ50の例は、ダイナミックランダムアクセスメモリ、不揮発性ランダムアクセスメモリ、ハードディスクドライブ、およびソリッドステートディスクドライブを含んでいる。

【００３１】

図2は、本発明の一つの実施形態に従った、イベントログ26に保管されたデータコンポーネントの一つの例を示すブロック図である。イベントログ26A－26Dは、異なるそれぞれのレイアウト(すなわち、フォーマットおよびスキーマ)で情報を保管することができるが、簡単にするために、本明細書におけるイベントログは単一のレイアウトを含んでいる。

【００３２】

図2に示される例において、各イベントログ26は、イベントログエントリ60のセットを含み、イベントログエントリのそれぞれは、日付62、時間64、および、イベントの記述を保管するイベントメッセージ66を含んでいる。所与のイベントログエントリ60内の所与のイベントについて、日付62は、所与のイベントの日付を含み、時間64は、所与のイベントの時間を含み、そして、イベントメッセージ66は、イベントを記述して、参加者のユーザ識別子をリストする。ユーザ識別子は、以下で図3を参照する記載において説明されている。

【００３３】

各イベントメッセージ66(すなわち、所与のイベントを参照するもの)は、１つ以上のユーザ識別子68(すなわち、対応するイベントの参加者)を有することができる。一つの実施例において、所与のイベントメッセージが、電子メールを送信するユーザエンティティを含むイベントに対応する場合に、所与のイベントメッセージ66は、単一の識別子(ID)68を含んでいる。別の実施例において、所与のイベントメッセージが、第２ユーザエンティティに関連付けられた第２アカウントに対して１つ以上のシステム許可（system permission）を与える、第１ユーザエンティティに関連付けられた第１アカウントを含むイベントに対応する場合に、所与のイベントメッセージは、2個の識別子68を含み得る。

【００３４】

本発明の実施形態において、１つ以上のそれぞれのアカウント69を使用してコンピューティングデバイスを操作する、複数のユーザエンティティ67(すなわち、個々の物理ユーザ)が存在している。以下で説明されるように、プロセッサ48は、各識別子68をそれぞれのアカウント69にマッピングし、そして、次いで、各アカウント69をそれぞれのユーザエンティティ67に関連付けることができる。アカウント69は、以下で図5を参照する記載において説明されている。

【００３５】

いくつかの実施形態において、プロセッサ48は、全てのイベントログ(例えば、イベントログ26A－26D)からイベントログエントリ60を取り出し、そして、取り出されたイベントログエントリ内のイベント情報を集約イベントログ52に保管することができる。以下で説明されるように、プロセッサ48は、集約イベントログ52に保管された情報を使用して、イベントをユーザエンティティにマッピングすることができる。

【００３６】

図3は、本発明の一つの実施形態に従った、集約イベントログ52に保管されたデータコンポーネントの一つの例を示すブロック図である。集約イベントログ52は、集約ログエントリ70のセットを含んでいる。いくつかの実施形態において、プロセッサ48は、各イベントログ26内の各イベントログエントリ60に対して新しい集約ログエントリ70を作成することができる。別の言葉で言えば、各集約ログエントリ70は、対応するイベントログエントリ60を有している。

【００３７】

各集約イベントログエントリ70は、イベントID　72、ソース74、日付76、時間78、イベントメッセージ80、および、識別子情報レコード82を含んでいる。対応するイベントログエントリ60について新しい集約ログエントリ70を作成すると、プロセッサ48は、以下を行うことができる。

●固有のイベントIDを作成する(72)。

●対応するイベントログエントリ60を保管しているイベントログを生成したデバイスの識別子を、ソース74に、保管する。識別子の実施例は、これらに限定されるわけではないが、所与のクラウドサーバ42のインターネットプロトコル(IP)アドレス、または、所与のコンピューティングデバイス28のメディアアクセス制御(MAC)アドレスを含む。

●対応するイベントログエントリ60の日付62を日付76にコピーする。

●対応するイベントログエントリ60内の時間64を時間78にコピーする。

●対応するイベントログエントリ60内のイベントメッセージ66をイベントメッセージ

80にコピーする。

【００３８】

いくつかの実施形態において、プロセッサ48は、イベントメッセージ80から１つ以上のユーザID 69を抽出し、ユーザIDを正規化し、そして、正規化されたユーザIDをユーザエンティティに関連付けることができる。図3に示される構成において、所与のイベントメッセージ80から抽出された各ユーザID 69は、抽出されたユーザ識別子84、識別子タイプ86、マッピングされたアカウントm、および、関連付けられたユーザエンティティ90といった情報を保管する、対応する識別子レコード82を有している。

【００３９】

新しい集約ログエントリを作成すると(すなわち、上述のように)、プロセッサ48は、イベントメッセージ80内のいくつかの(すなわち、１つ以上の)識別子68を識別し、各識別子68が対応する識別子情報レコード82を有するように、識別されたいくつかの識別子情報レコード82を新しい集約ログエントリに追加し、そして、以下のように各所与の識別子情報レコードをポピュレート（populate）することができる。

●対応する識別子68を抽出された識別子84に保管する。

●抽出された識別子84を分類し、そして、分類を識別子タイプ86に保管する。識別子の分類は、以下で説明される。

●対応する識別子を所定のアカウント69にマッピングするように、対応する識別子68を正規化し、そして、マッピングされたアカウントをマッピングされたアカウント88に保管する。正規化識別子68は、以下で図6を参照する記載において説明されている。

●マッピングされたアカウント88に関連付けられた所与のユーザエンティティ67を識別し、そして、識別されたユーザエンティティを関連付けられたユーザエンティティ90に保管する。関連付けられたユーザエンティティ90を識別することは、以下で図6を参照する記載において説明されている。

【００４０】

以下で説明される実施例においては、「John Doe」という名前の所与のユーザエンティティ67が、会社「Company」という、複数のマッピングされたアカウント88を有しており、それぞれが１つ以上の識別子84によって参照される、会社のために働いている。

【００４１】

識別子タイプ86の例は、これらに限定されるわけではないが、以下を含んでいる。

●ドメイン名は、「Company/jdoe」といったものである。ドメイン名は、典型的に、イベントログ26A、26B、および、26C内のイベントメッセージ66において見出すことができる。

●最終的に認可されたドメイン名(FQDN)は、てき「Company.com/jdoe」といったものである。FQDNは、典型的に、イベントログ26A、26B、および、26C内のイベントメッセージ66において見出すことができる。

●ユーザ名(すなわち、ドメインを有さない)は、「jdoe」といったものである。ユーザ名は、典型的に、イベントログ26A、26B、および、26C内のイベントメッセージ66において見出すことができる。

●セキュリティ識別子(SID)番号は、「S-1-5-21-1602811402-2595058921-120187713-502」といったものである。SID番号は、典型的に、イベントログ26Aおよび26B内のイベントメッセージ66において見出すことができる。

●グローバル一意識別子(GUID)番号は、「8c6bfd4a-4cb2-11ea-b67e-88e9fe502c1f」といったものである。GUID番号は、典型的に、イベントログ26Bおよび26D内のイベントメッセージ66において見出すことができる。

●ローカルユーザ名は、「host123＼jdoe」といったものであり、ここで、「host123」は所与のホスト名56を含んでいる。ローカルユーザ名は、典型的に、イベントログ26A、26B、および、26C内のイベントメッセージ66において見出すことができる。

●企業ユーザ名は、「john.doe@company.com」といったものである。これらのユ

ーザ名は、典型的に、SSOログ(図示なし)、電子メールログ(図示なし)、並びに、イベントログ26Cおよび26Dといった、イベントログ26内のイベントメッセージ66において見出すことができる。

●個人ユーザ名は、「john.doe@gmail.com」といったものである。これらのユーザ名は、典型的に、SSOログ(図示なし)、電子メールログ(図示なし)、並びに、イベントログ26Cおよび26Dといった、イベントログ26内のイベントメッセージ66において見出すことができる。

【００４２】

図4は、本発明の一つの実施形態に従った、所与のデータベースレコード35の構成の一つの例を示すブロック図である。各データベースレコード35は、イベント識別子92、および、所与のアカウント69を参照する対応するアカウント識別子94といった、情報を保管することができる。この構成を使用して、アカウントデータベースレコード33は、識別子68とアカウント67との間の既知の関係を保管することができる。

【００４３】

いくつかの実施形態において、アカウントデータベース33は、パルアルトネットワーク社によって製造されたDirectory Sync Service™(DSS™)を含み、かつ、エンドポイントエージェント44は、XDR™を含み得る。XDR™エンドポイントエージェントは、識別子68とアカウント67との間のマッピングを取り出すために、DSS™とインタラクションすることができる。

【００４４】

例えば、識別子68とアカウント67との間の関係は、Windows(登録商標)ドメインタイプネットワーク内の全てのユーザおよびコンピュータを認証、かつ、認可すること、全てのコンピュータについてセキュリティポリシー割当て、かつ、実施すること、および、ソフトウェアをインストール、かつ、更新すること、といった、動作を実行する、Active Directory™(米国ワシントン州、レッドモンドのマイクロソフト社によって製造されるもの)のような、ディレクトリサービスアプリケーション(図示なし)によって維持することができる。この実施例において、アカウントDBMS 31は、識別子68とドメインアカウントを含むアカウント67との間のマッピングを取り出すために、アクティブDirectory™をクエリ（query）することができる。

【００４５】

図5は、本発明の一つの実施形態に従った、ユーザエンティティレコード54に保管された情報の一つの例を示すブロック図である。図5に示される構成において、各ユーザ072レコード54は、ユーザエンティティID 100、ユーザエンティティプロファイル24、ステータス情報レコード104のセット、アカウント情報レコード106のセット、および、識別子－アカウントマッピングレコード108のセットといった、情報を保管している。

【００４６】

ユーザエンティティID 100は、所与のユーザエンティティ67について一意の識別子を含んでいる。いくつかの実施形態において、プロセッサは、アカウントデータベースレコード47と一対一の対応を有している、ユーザエンティティレコード54のセットを作成し、そして、セット内の各ユーザエンティティid 100に一意の識別子を保管することができる。従って、各所与のユーザエンティティ(すなわち、従業員)67は、対応するユーザエンティティレコード54を有している。ユーザエンティティID 100は、また、本明細書ではユーザエンティティ100としても称され得る。

【００４７】

ユーザエンティティプロファイル24は、対応するユーザエンティティの予想されるアクティビティを示すユーザプロファイルを含んでいる。本明細書において以下で図7を参照する記載において説明されるように、プロセッサ48は、コンピューティングファシリティ20内の対応するユーザエンティティによって実行されるアクションにおける任意の異常を検出するために、ユーザプロファイル24を使用することができる。

【００４８】
各ステータス情報レコードは、開始日110、終了日112、および、ステータス114を含んでいる。各所与のステータス114は、開始日110で始まり終了日112で終わる期間におよぶ。いくつかの実施形態において、開始日110および終了日112は、また、時間(例えば、2022年12月11日の13時30分)も含み得る。
【００４９】
ステータス114の実施例は、これらに限定されるわけではないが、以下を含む。
●雇用期間．プロセッサ48は、もはやユーザエンティティが組織によって雇用されていない場合に、対応するユーザエンティティによるアクティビティ(例えば、電子メール、ファイルアクセス)を疑わしいものとしてフラグ付けすることができる。
●休暇期間．プロセッサ48は、ユーザエンティティが休暇を取っている場合に、対応するユーザエンティティによるアクティビティ(例えば、電子メール、ファイルアクセス)を疑わしいものとしてフラグ付けすることができる。
●位置．組織は、複数の位置（location）を有することができ、そして、HRデータベースは、各ユーザエンティティが所与の時間に働く位置を追跡することができる。いくつかの実施形態において、プロセッサ48は、異常な位置から作業する所与のユーザエンティティによるアクティビティを検出するために、この情報を使用することができる。
●デバイス．ユーザエンティティ100は、異なるコンピューティングデバイス28(例えば、デスクトップ／ラップトップコンピュータ、および、モバイルデバイス)を使用し得る。プロセッサ48は、任意の所与の時間(すなわち、過去または現在)に、どのユーザエンティティがどのコンピューティングデバイス28を使用しているかを追跡するために、この情報を使用することができる。
●部門．任意の所与の時間に、各ユーザエンティティ100を特定の部門(例えば、金融、マーケティング)に割り当てることができ、それによって、各部門の従業員によって典型的にアクセスされるシステム(例えば、給与支払い、広告追跡)を示している。
●タイトル．所与のユーザエンティティ100の組織タイトル(例えば、マネージャ、スーパーバイザ)は、所与のユーザエンティティについて特権および典型的なシステム挙動を示すことができる。
【００５０】
各ユーザエンティティID100は、典型的に、１つ以上の電子メールアカウントを使用する。図5に示される構成において、各所与のユーザエンティティ100は、所与のユーザエンティティによって使用される電子メールアカウントのそれぞれについての対応するアカウント情報レコード106を保管する、対応するユーザエンティティレコード54を含んでいる。
【００５１】
各アカウント情報レコード106は、一意のアカウントID　116、アカウント名118(すなわち、「john.doe@company.com」およびjohn.doe@gmail.comといった電子メールアドレス)、および、アカウントタイプ120といった情報を保管することができる。本明細書の実施形態において、アカウントID　116は、また、アカウント116と称され得る。
【００５２】
アカウントタイプ120の実施例は、これらに限定されるわけではないが、以下を含む。
●「Company/jdoe」といったドメインアカウント。ドメインアカウントは、組織内のActive Directory™(マイクロソフト社によって製造されるもの)ドメインにわたり使用することができるアカウントを含んでいる。ドメインアカウントは、典型的に、以下の識別子タイプ86に関連付けられる。ドメイン名、FQDN、ユーザ名、SID番号、GUID番号、および、企業識別子。
●ローカルアカウントは、特定のそれぞれのネットワーク化エンティティに結び付けられた、「host123/jdoe」(すなわち、「host123」が所与のホスト名56を含む)といったアカウントを含んでいる。ローカルアカウントは、典型的に、以下の識別子タイプ8

6に関連付けられる。ユーザ名、SID番号、GUID番号、および、ローカルユーザ。

●「john.doe@company.com」といったクラウドアカウント。クラウドアカウントは、Google Cloud Platform™(カリフォルニア州、マウンテンビューのAlphabet社によって提供されるもの)、または、Azure™(Microsoft社によって提供されるもの)のように、クラウドインフラストラクチャにわたり使用され得る。クラウドアカウントは、典型的に、以下の識別子タイプ86に関連付けられる。GUID番号、企業識別子、および、個人識別子。

●組織の内側および外側の両方で使用できる「john.doe@gmail.com」といったアカウントを含むパーソナルアカウント。パーソナルアカウントは、典型的に、個人識別子に関連付けられる。

【００５３】

本発明の実施形態において、プロセッサ48は、イベントログエントリ0から識別子84を抽出し、そして、それぞれのマッピングされたアカウント88を識別するために、抽出された識別子を正規化する。対応するユーザエンティティレコード54内の所与のユーザエンティティ100について、プロセッサ48は、識別子－アカウントマッピングレコード108内に、抽出された識別子と、関連付けられたアカウントとの間の現在のマッピング(すなわち、両方とも所与のユーザエンティティに対するもの)を保管することができる。所与のユーザエンティティレコード54内の(すなわち、対応するユーザエンティティ100についての)各識別子－アカウントマッピングレコード108は、以下のような情報を保管することができる。

●対応するユーザエンティティによって使用される所与の識別子84を含むユーザ識別子122。

●識別子タイプ124。上述のように、識別子タイプ124は、ドメイン名、FQDN、ユーザ名、SID番号、GUID番号、ローカルユーザ名、企業識別子、および、個人識別子を含んでいる。

●関連付けられたアカウントID126は、プロセッサ48が識別子122と関連付ける、所与のアカウントID 116を保管する。

【００５４】

ユーザエンティティ識別

図6は、本発明の一つの実施形態に従った、イベントログ26内のアクティビティをユーザエンティティ100に関連付け、そして、コンピューティングファシリティ20内のユーザエンティティのアクティビティに基づいてプロファイル24を生成する方法を概略的に示すフローチャートである。

【００５５】

ステップ130において、プロセッサ48は、ユーザエンティティレコード54を初期化する。上述のようないくつかの実施形態において、各ユーザエンティティレコード54は、対応するユーザエンティティ100の所与のHRデータベースレコード47aに対応している。ユーザエンティティレコード54を初期化するとき、追加的に、ユーザエンティティレコード54を初期化するときに、プロセッサ48は、ユーザエンティティプロファイル24も、同様に初期化することができる。

【００５６】

ステップ132において、プロセッサ48は、イベントログ26を識別する。

【００５７】

ステップ134において、プロセッサは、所与のイベントログ26内で未マッピング（unmapped）イベントログエントリ60を選択する。本明細書の実施形態において、未マッピングイベントログエントリ60は、以下で説明されるように、ステップ134－136によって処理されないイベントログエントリのいずれかを含んでいる。

【００５８】

ステップ136において、プロセッサ48は、選択されたイベントログエントリを取り出す（retrieve）。選択されたログエントリを取り出すと、プロセッサ48は、新しい集約

ログエントリ70を集約イベントログ52に追加し、そして、本明細書で上記に説明した実施形態を使用して、新しい集約ログエントリ内に、イベントID72、ソース74、日付76、時間78、および、イベントメッセージ80をポピュレートすることができる。

【００５９】

ステップ138において、プロセッサ48は、イベントメッセージ80内の１つ以上の識別子68を識別し、そして、識別された識別子68を１つ以上の抽出された識別子84に(すなわち、１つ以上のそれぞれの識別子情報レコード82内に)保管する。

【００６０】

ステップ140において、プロセッサ48は、抽出された識別子のそれぞれをそれぞれのアカウント116にマッピングするために、１つ以上の抽出された識別子84を１つ以上の指定されたフォーマットに正規化する。いくつかの実施形態において、各アカウントタイプ120は、対応する指定されたフォーマットを有し得る。上述のアカウントタイプの実施例を使用すると、以下のようである。

●アカウントタイプ「domain account」のために指定されたフォーマットは、「CompanyName[/]UserName」であり得る。ここで、「CompanyName」および「UserName」は、自己記述的（self-descriptive）である。上述のように、ドメインアカウントの一つの例は「Company/jdoe」である。

●アカウントタイプ「local account」のために指定されたフォーマットは、「ComputerID/UserName」であり得る。ここで、「ComputerID」は、ネットワーク32上の所与のコンピューティングデバイス28に対する識別子を含み、そして、「UserName」は自己記述的である。上述のように、ローカルアカウントの一つの例は「host123/jdoe」である。

●アカウントタイプ「cloud account」のために指定されたフォーマットは、「UserName[@]CompanyDomain」であり得る。ここで、「UserName」は、自己記述的であり、ネットワーク32上の所与のコンピューティングデバイス28のための識別子を含む。そして、「UserName」は、自己記述的であり、かつ、「CompanyDomain」は、企業ドメイン名を含んでいる。上述のように、クラウドアカウントの一つの例は、「john.doe@company.com」である。

●アカウントタイプ「personal account」のために指定されたフォーマットは、「UserName[@]ProviderDomain」であり得る。ここで、「UserName」は、自己記述的であり、そして、「ProviderDomain」は、電子メールサービスプロバイダドメイン名を含む(例えば、Alphabet社によって提供されるGmail™)。上述のように、パーソナルアカウントの一つの例は、「john.doe@gmail.com」である。

【００６１】

いくつかの実施形態において、所与のイベントについてのフォーマットは、ソース(例えば、所与のイベントに対応するイベントログエントリをプロセッサ48が取り出したイベントログ、イベントタイプ、所与のイベントに対応するログエントリ内のフィールド)、または、所与のイベントに対応するログエントリのコンテンツに基づいている。例えば、以下のようである。

●所与の抽出された識別子84が電子メール識別子フォーマット(すなわち、「local-part[@]domain」、ここで、「local-part」は、ユーザ名および「domain」を含む)を有している場合に、プロセッサ48は、所与の識別子をクラウドアカウント(例えば、「john.doe@company.com」)またはパーソナルアカウント(例えば、「john.doe@gmail.com」)に正規化することができる。

●プロセッサ48が、電子メールサーバのログからの所与のログエントリ60から所与の識別子84を抽出し、かつ、ドメインが何らかのパブリックサービスである場合に、それは、プライベート電子メールアカウントを参照している可能性が最も高いことが分かる(例えば、コンテキストは、所与のログエントリが電子メールサーバの所与のログ26から来たことであり、そして、所与のログエントリのコンテンツは「@gmail」のようなパブリック電子メールドメインを含んでいた)。

●SIDフォーマットは、ローカルまたはドメインアカウントを参照することができ、そして、たいてい、コンテンツによって区別される。いくつかの実施形態において、SIDのプレフィックスは、ドメイン、またはローカルマシン(例えば、所与のコンピューティングデバイス28)を一意に識別する。

●GUIDは、異なるアカウントタイプを参照することができ、そして、コンテキスト(例えば、プロセッサ48がGUIDを抽出したログ26のそれぞれのタイプ)によって、または、プロセッサ48がアカウントデータベース33(例えば、DSS™)から抽出することができる「ground truths」にGUIDをマッチングすることによって認識することができる。

【００６２】

いくつかの実施形態において、１つ以上の抽出された識別子84(それぞれの識別子68に対応しているもの)から単一のアカウント116(所与のアカウント69に対応しているもの)へのマッピングが存在し得る。例えば、以下のようである。

●プロセッサ48は、以下の識別子84を、アカウントタイプ120がドメインアカウントを含む所与のアカウント116「Company/jdoe」にマッピングすることができる。

○「Company/jdoe」、識別子タイプ86がドメイン名を含むもの

○「Company.com/jdoe」、識別子タイプ86がFQDNを含むもの

○「jdoe」、識別子タイプ86がドメインを伴わないユーザ名を含むもの

○「S-1-5-21-1602811402-2595058921-120187713-502」、識別子タイプ86がSIDを含むもの

○「8c6bfd4a-4cb2-11ea-b67e-88e9fe502c1f」、識別子タイプ86がGUIDを含むもの

○「host123＼jdoe」、識別子タイプ86がローカルユーザ名を含むもの

○「john.doe@company.com」、識別子タイプ86が企業ユーザ名を含むもの。

●プロセッサ48は、以下の識別子84を、アカウントタイプ120がローカルアカウントを含む所与のアカウント116「host123/jdoe」にマッピングすることができる。

○「jdoe」、識別子タイプ86がドメインを伴わないユーザ名を含むもの

○「S-1-5-21-1602811402-2595058921-120187713-502」、識別子タイプ86がSIDを含むもの

○「8c6bfd4a-4cb2-11ea-b67e-88e9fe502c1f」、識別子タイプ86がGUIDを含むもの

○「host123＼jdoe」、識別子タイプ86がローカルユーザ名を含むもの

●プロセッサ48は、以下の識別子84を、アカウントタイプ120がクラウドアカウントを含む所与のアカウント116「john.doe@company.com」にマッピングすることができる。

○「8c6bfd4a-4cb2-11ea-b67e-88e9fe502c1f」、識別子タイプ86がGUIDを含むもの

○「john.doe@company.com」、識別子タイプ86が企業ユーザ名を含むもの

○「john.doe@gmail.com」、識別子タイプ86が個人ユーザ名を含むもの

●プロセッサ48は、以下の識別子84を、アカウントタイプ120がパーソナルアカウントを含む所与のアカウント116「john.doe@gmail.com」にマッピングすることができる。

○「john.doe@gmail.com」、識別子タイプ86が個人ユーザ名を含むもの

【００６３】

いくつかの実施形態において、プロセッサ46は、それぞれのアカウント116に対する抽出された識別子に対して、データベースレコード35をクエリすることができる。

【００６４】

所与の抽出された識別子84の各マッピングを実行すると、プロセッサ48は、マッピングされたアカウント(ID)116を、所与の抽出された識別子を保管している識別子情報レコード82内のマッピングされたアカウント88に保管する。ステップ140で検出された任意の所与のマッピングが未だユーザエンティティレコード54に保管されていない場合、

プロセッサ48は、新しい識別子－アカウントマッピングレコードを、マッピングされたアカウントを保管しているユーザエンティティレコード内に追加し、そして、それに応じて、識別子122、識別子タイプ124、および、関連付けられたアカウントID126をポピュレートすることができる。

【００６５】

第１正規化の実施形態においては、文字列操作（string manipulation）によって、所与の抽出された識別子84を正規化することができる(すなわち、プロセッサ48は、抽出された識別子をテキスト文字列として保管する)。この実施形態において、プロセッサ48は、相関およびクエリを可能にするために、抽出された識別子84を正規化することができる。例えば、プロセッサ48は、以下の両方を「company＼jdoe」に正規化するために、文字列操作を使用することができる。

●「jdoe@company[.]onmicrosoft[.]

●「domain=company.local, username=jdoe」

【００６６】

第２正規化の実施形態において、プロセッサ48は、ドメイン知識（domain knowledge）を使用することによって、所与の抽出された識別子84を正規化することができる。この実施形態において、特別な識別子は、所与の識別子にマッピングされたアカウントのタイプおよび範囲を(例えば、ホストまたはメインレベル)で示すことができる。以下の例において、プロセッサ48は、以下のことを行うためにドメイン知識を使用使用することができる。

●「AzureAD＼jdoe」をクラウドアカウントにマッピングする。

●「MicrosoftAccount＼jdoe」ドメインを個人Microsoft™アカウントにマッピングする。

●「company＼jdoe$」を所与のホスト名56「jdoe」のマシンアカウントにマッピングする。この例において、識別子における「$」は、マシンアカウント(すなわち、「$」+ユーザ名)を示す。

【００６７】

ドメイン知識は、プロセッサ48が、Active Domain™およびケルベロス領域（Kerberos realms）、並びに、様々なデータクラウド環境において、典型的には、異なって管理されるアカウントを区別することを可能にする。

【００６８】

第３正規化の実施形態において、プロセッサ48は、以前に学習された知識を使用することによって、所与の抽出された識別子84を正規化することができる。この実施形態において、プロセッサ48は、所与の抽出された識別子84のアカウントを決定するために、学習された役割（role）およびディレクトリ同期サービス(DSS™)を使用することができる。以下の例において、プロセッサ48は、ドメイン知識を以下のように使用することができる。

●ad_domain_roleが「company」を含む場合に、アカウントタイプ120はドメインアカウントである。

●internal_hostname_roleが「company」を含む場合に、アカウントタイプ120はローカルアカウントである。

●イベントメッセージがSID番号のみを有する場合に、プロセッサ48は、所与の抽出された識別子を「company＼jdoe」にマッピングするように、DSS.sidフィールドを介して(「sid」は、Active Directory™において「security identifier」の省略形である)ピボット（pivot）することができる。

●抽出された所与の識別子が「john.doe@gmail[.]com」を含む場合には、抽出された所与の識別子をドメインアカウントとして認識するように、DSS.upnフィールドを介して(「upn」は、Active Directory™において「user principal name」の省略形である)ピボットし、次いで、抽出された識別子を、正規化された識別子「company＼jdoe」にマッピングする。この例において、プロセッサ48は、文字列「john.doe@

gmail[.]com」をDSS.upnフィールドと比較し、そして、その値を有するレコードが見つかった場合に、それはドメインアカウントであると見なされ、プロセッサは、正規化された識別子「company＼jdoe」を返す。いくつかの実施形態において、対応するDSSレコード「DSS.netbios_domain＼DSS.sam_account_name」内の値は、「company＼jdoe」を含み得る。

【００６９】

フローチャートに戻ると、ステップ142においては、各所与のマッピングされたアカウント88に対して、プロセッサ48は、所与のユーザエンティティ100を所与のマッピングされたアカウント88に関連付ける。いくつかの実施形態において、各ユーザエンティティ100は、１つ以上のアカウント116に関連付けられ得る。例えば、上述のように、マッピングされたアカウントは、「Company/jdoe」、「host123/jdoe」、「john.doe@company.com」、および「john.doe@gmail.com」を含み得る。これら全てのマッピングされたアカウント88は、「John　Doe」と名付けられた所与のユーザエンティティに関連付けられ得る。

【００７０】

第１関連付け実施形態において、プロセッサ46は、所与のアカウント69を所与のユーザエンティティ67に関連付けるように、HRデータベース46及び／又はアカウントデータベース33に保管された情報を使用することができる。例えば、プロセッサ46が、所与の識別子68を所与のアカウント69「john.doe@gmail.com」にマッピングするためにアカウントデータベース33を使用し、そして、HRデータベース46内で「John　Doe」と名付けられた所与のユーザエンティティ67を識別した場合には、それらが同じ名前を有するので、プロセッサは、所与のアカウントを所与のユーザエンティティと関連付けることができる。

【００７１】

第２関連付けの実施形態において、プロセッサ48は、所与のユーザエンティティを所与のマッピングされたアカウントに関連付けるために、ヒューリスティック（heuristics）を使用することができる。例えば、「john.doe@gmail[.]com」がDSS表示名「John　Doe」と一致する場合に、それらは、同じユーザエンティティ100を参照する可能性が高い。

【００７２】

第３関連付けの実施形態において、プロセッサ48は、所与のユーザエンティティを所与のマッピングされたアカウントに関連付けるために、プロファイリング（profiling）および属性を使用することができる。１つのプロファイリングの例において、プロセッサ48は、ホスト名「host_123」を有しているコンピューティングデバイスが、大部分は、単一のユーザエンティティ100「company＼jdoe」によって使用されていると判定することができる。第２のプロファイリング例において、プロセッサ48は、アカウント「john.doe@gmail[.]com」が、常に、ホスト名「host_123」を有しているコンピューティングデバイスからログエントリ60を発する（originate）と判定することができる。

【００７３】

第１属性の例において、プロセッサ48は、ホスト名「host_123」を有しているコンピューティングデバイスが、ユーザエンティティ「jdoe」によって使用されるパーソナルエンドポイントであると判定することができる。第２属性の例において、プロセッサ48は、「john.doe@gmail[.]com」が、ユーザエンティティ「jdoe」の個人電子メールであると判定することができる。第３属性の例において、プロセッサ48は、ユーザエンティティ「jdoe」が、アカウント「host_123＼Administrator」へのアクセスを有する可能性が高いと判定することができる。

【００７４】

フローチャートに戻ると、ステップ144において、プロセッサ48は、選択されたログエントリに対応しているイベントに参加した、ユーザエンティティのうちの１つ以上を識

別する。
【００７５】
ステップ146において、プロセッサ48は、選択されたログエントリ内のイベントメッセージによって示されるイベントを用いて、ステップ144において識別されたユーザエンティティのそれぞれのユーザエンティティプロファイルを更新する。いくつかの実施形態において、プロセッサ48は、指定された期間(例えば、過去30日)内にイベントがあった場合にのみ、選択されたログエントリ内に示されるイベントを用いて、ユーザエンティティプロファイル24を更新することができる。
【００７６】
ステップ148において、未マッピング（unmapped）のログエントリ60がある場合に、方法は、ステップ132に進む。本方法は、未マッピングのログエントリ60が存在しないときに終了する。
【００７７】
一旦、プロセッサ48がプロファイル24を作成すると、プロセッサは、コンピューティングファシリティ20内で悪意のあるアクティビティを実行するために複数の識別子122を使用している単一のユーザエンティティ100を検出するために、プロファイルを使用することができる。例えば、プロセッサ48は、以下を行うことができる。
１．GoogleDrive™(カリフォルニア州、マウンテンビューのAlphabet社によって提供されるもの)からファイル「confidential.pdf」をダウンロードした、クラウドアカウント「jdoe@company[.]com」を検出する。
２．ドメインアカウント「Company＼jdoe」がファイル「confidential.pdf」を「obscured.zip」にリネームしたことを検出する。
３．obscured.zipという名前の添付ファイルを伴うパーソナル電子メール「john.doe@gmail[.]com」に対して電子メールが送信されたことを検出する。
【００７８】
これらの個々のイベントのそれぞれは正当であるように見えるが、本発明の実施形態は、これら３つのイベントを単一のユーザエンティティ100「John　Doe」に相関させる（correlating）ことを可能にする。複数の識別子122を有している複数のイベントを相関させることは、プロセッサ48が、単一のユーザエンティティ100に結び付けられた疑わしいイベントシーケンスを検出することを可能にする。
【００７９】
図7は、本発明の一つの実施形態に従った、疑わしいアクティビティを検出するためにユーザエンティティアクティビティプロファイル24を使用する方法を概略的に示すフローチャートである。
【００８０】
ステップ150では、上記で図6を参照する記載において説明されたようにプロファイル24を生成した後の時点で、プロセッサ48は、ログ26から、追加的なイベントログエントリ60のセットを収集する。いくつかの実施形態において、プロセッサ48は、特定の期間(例えば、10分または丸1日)の最中に追加的なイベントログエントリを収集することができる。
【００８１】
ステップ152において、プロセッサ48は、上記で図6のステップ140－142を参照する記載において説明された実施形態を使用して、追加的なイベントログエントリ内のイベントメッセージにおけるイベントのそれぞれを、それぞれのユーザエンティティ100に関連付ける。
【００８２】
ステップ154において、プロセッサ48は、HRデータベース46に対する任意の更新を用いてステータス情報レコード104を更新し、そして、それに応じて、ユーザエンティティプロファイル24を更新する。例えば、ユーザエンティティ「John　Doe」は休暇中であり得る。

【００８３】
ステップ156において、プロセッサ48は、未選択（unselected）のユーザエンティティ100を選択する。
【００８４】
ステップ158において、プロセッサ48は、選択されたユーザエンティティの追加的なイベントを、選択されたユーザエンティティのユーザエンティティプロファイル24と比較する。
【００８５】
ステップ158において、プロセッサ48は、ユーザエンティティプロファイルに基づいて、追加的なイベントが疑わしいアクティビティを含むか否かを判定する。いくつかの実施形態において、各ユーザプロファイル24は、対応するユーザエンティティ100のステータスレコード104からの情報を含むことができる。例えば、所与のユーザエンティティ100についての所与のステータス114が、所与のユーザエンティティが退職していることを示しており、かつ、プロセッサ48が、退職の後でユーザエンティティに関連付けられたイベントを検出した場合には、イベントがユーザエンティティプロファイルにおける退職ステータスに従っていないので、プロセッサは、それらのイベントを疑わしいものとして分類することができる。
【００８６】
追加的なイベントが疑わしいアクティビティを含む場合には、ステップ160において、プロセッサ48は、選択されたユーザエンティティに対してアラートを発行する。一つの実施形態において、疑わしいアクティビティは、ユーザエンティティプロファイルを生成するためにプロセッサ48が使用した、第１所与のイベントログエントリ60内の第１イベントと、ステップ150でプロセッサ48が収集した、第２所与のイベントログエントリ60内の第２イベントとを組み合わせることができる。この実施形態において、第１および第２所与のイベントログエントリは、同じユーザエンティティ100に関連付けられた異なる識別子122にマッピングされた。
【００８７】
アラートを発行するために、プロセッサ48は、システム管理者(図示なし)にメッセージを送信すること、または、選択されたユーザエンティティに関連するアカウントのいずれかへのアクセスを制限すること、といった動作を実行することができる。
【００８８】
ステップ162において、プロセッサ48は、選択されたユーザエンティティに関連する追加的なイベントを用いて、選択されたユーザエンティティのユーザエンティティプロファイルを更新する。
【００８９】
ステップ164において、未選択のユーザエンティティ100が存在する場合に(すなわち、ステップ156)、方法は、ステップ156に進む。未選択のユーザエンティティ100が存在しない場合に、方法は、終了する。
【００９０】
ステップ158に戻って、プロセッサ48が、ユーザエンティティプロファイルに基づいて、追加的なイベントにおける疑わしいアクティビティを検出しなかった場合に、方法は、ステップ162に進む。
【００９１】
上述の実施形態は、実施例として引用されていること、および、本発明は、上記で、特に、示され、かつ、説明されてきたものに限定されないことが理解されるだろう。むしろ、本発明の範囲は、上述の様々な特徴の組合せ、および、部分的組合せ両方、並びに、上述の説明を読めば当業者には思い浮かぶであろう、先行技術に開示されていない、それらの変形および修正を含んでいる。

【図面】

【図１】

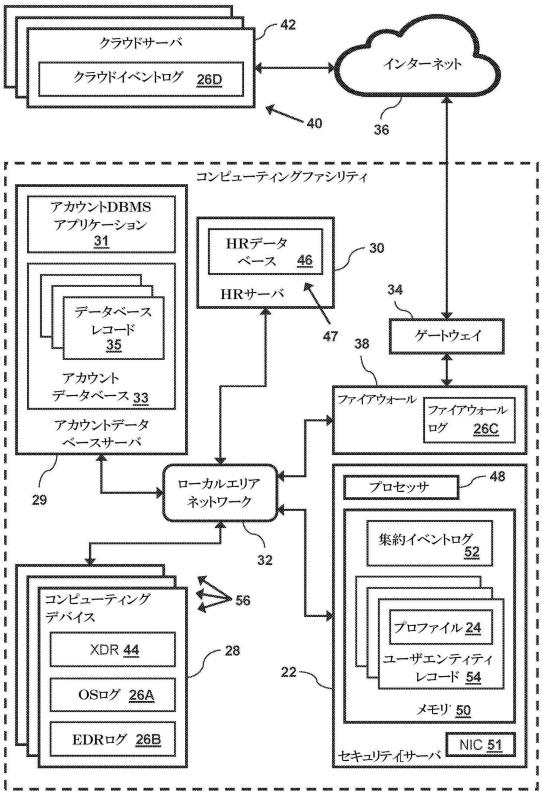

FIG. 1

【図２】

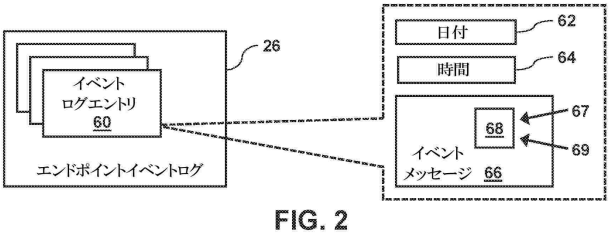

FIG. 2

【図３】

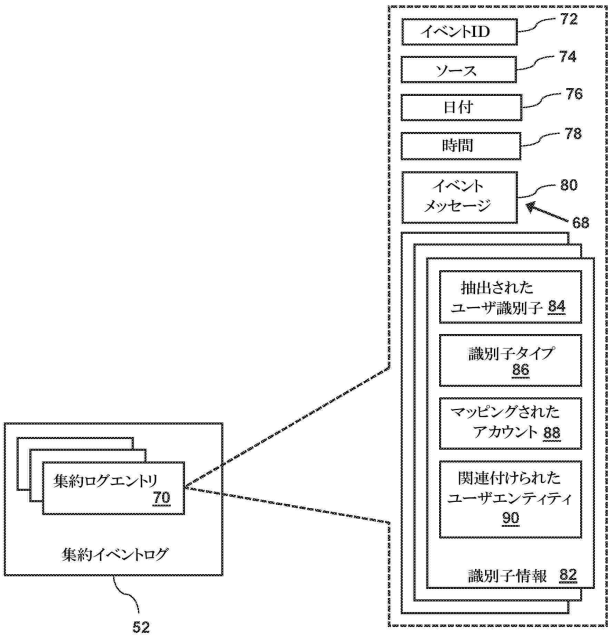

FIG. 3

【図４】

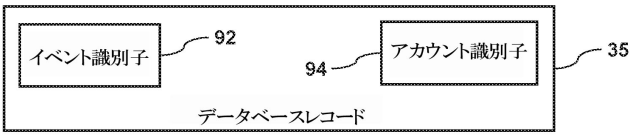

FIG. 4

【図５】

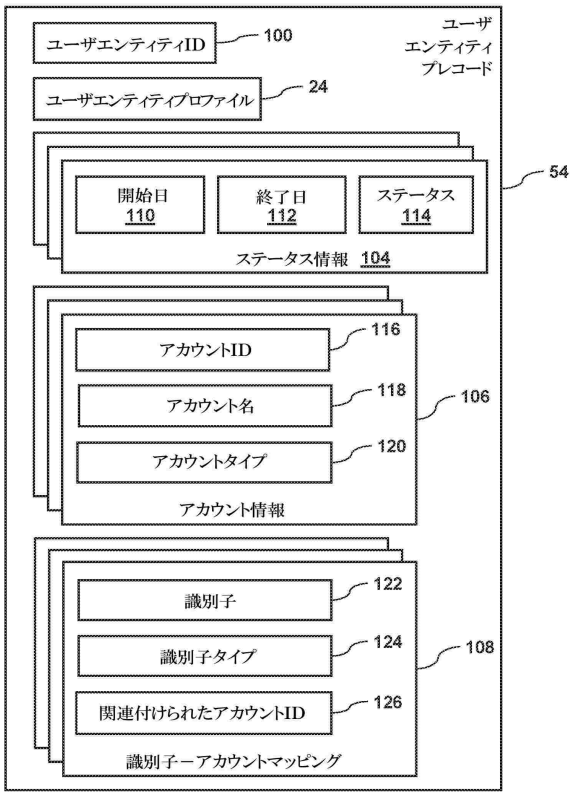

FIG. 5

【図６】

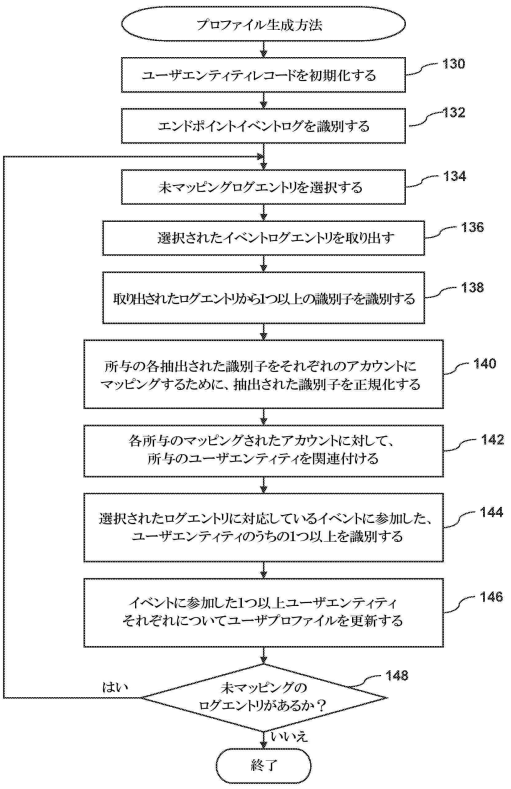

FIG. 6

【図７】

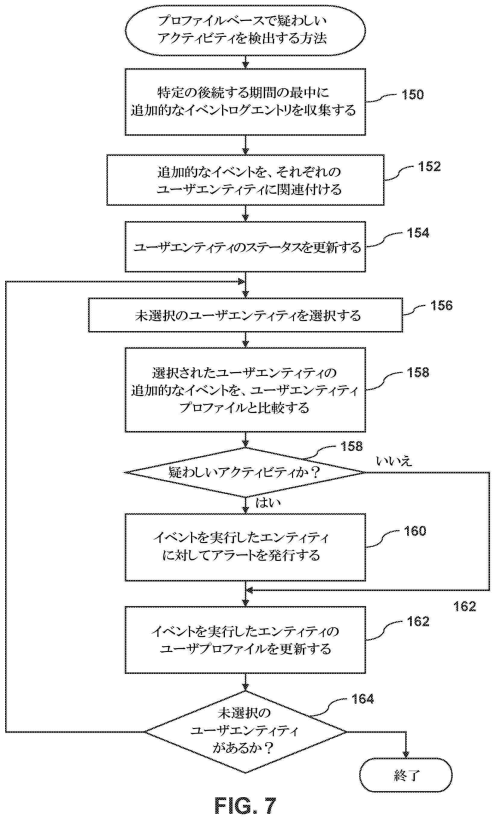

FIG. 7

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2022/059544

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/55 H04L9/40
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F H04L

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/073519 A1 (LONG KURT J [US]) 29 March 2007 (2007-03-29) abstract paragraph [0006] - paragraph [0008] paragraph [0015] - paragraph [0067] -----	1-17
A	US 6 347 374 B1 (DRAKE DAVID L [US] ET AL) 12 February 2002 (2002-02-12) abstract column 1, line 1 - column 4, line 48 column 11, line 25 - column 19, line 11 -----	1-17
A	US 2020/285737 A1 (KRAUS NAAMA [IL] ET AL) 10 September 2020 (2020-09-10) abstract paragraph [0004] - paragraph [0008] paragraph [0025] - paragraph [0038] paragraph [0243] - paragraph [0326] -----	1-17

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

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance;; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance;; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 January 2023	20/01/2023

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Jakob, Gregor

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IB2022/059544

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007073519 A1	29-03-2007	NONE	
US 6347374 B1	12-02-2002	NONE	
US 2020285737 A1	10-09-2020	EP 3935542 A2	12-01-2022
		US 2020285737 A1	10-09-2020
		WO 2020219134 A2	29-10-2020

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

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

シャロン，エッシュコル ストリート １７エー
(72)発明者 ノイマン，ヤロン
イスラエル国，４２８２３００ ツォラン，ハゲフェン ストリート ６５
(72)発明者 アロン，ヨナタン
イスラエル国，３４９１２７９ ハイファ，スウェーデン ストリート ２６