(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6888109号
(P6888109)
(45)発行日　令和3年6月16日(2021.6.16)　(24)登録日　令和3年5月21日(2021.5.21)

(51)Int.Cl.		F I	
G06F 21/62	(2013.01)	G06F	21/62
G06N 3/02	(2006.01)	G06N	3/02
G06F 21/55	(2013.01)	G06F	21/55
G06N 20/00	(2019.01)	G06N	20/00

請求項の数 14　(全 31 頁)

(21)出願番号　特願2019-546873 (P2019-546873)
(86)(22)出願日　平成30年2月8日(2018.2.8)
(65)公表番号　特表2020-510926 (P2020-510926A)
(43)公表日　令和2年4月9日(2020.4.9)
(86)国際出願番号　PCT/US2018/017420
(87)国際公開番号　WO2018/156359
(87)国際公開日　平成30年8月30日(2018.8.30)
審査請求日　令和1年9月11日(2019.9.11)
(31)優先権主張番号　15/443,801
(32)優先日　平成29年2月27日(2017.2.27)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　506223509
アマゾン・テクノロジーズ、インコーポレイテッド
アメリカ合衆国、ネバダ州　８９５０７、レノ、ピー．オー．ボックス　８１０２
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100103034
弁理士　野河　信久
(74)代理人　100179062
弁理士　井上　正
(74)代理人　100199565
弁理士　飯野　茂
(74)代理人　100153051
弁理士　河野　直樹

最終頁に続く

(54)【発明の名称】インテリジェントセキュリティ管理

(57)【特許請求の範囲】
【請求項１】
訓練用文書のセットを使用してトピックモデルを訓練することであって、前記セットの各訓練用文書が、少なくとも１つの識別されたトピックと割り当てられたリスクスコアとを有する、前記トピックモデルを訓練すること、
訓練用文書の前記セットを使用して、ランダムフォレストリグレッサを訓練すること、
電子リソース環境全体にわたってエンティティ用に格納されている複数の文書をクロールし、前記複数の文書にインデックスを付けること、
少なくとも前記トピックモデルを使用して、前記複数の文書の各文書の１つ以上のトピックを判定すること、
少なくとも前記ランダムフォレストリグレッサを使用して、前記複数の文書の各文書のリスクスコアを判定すること、
前記電子リソース環境内の前記複数の文書に関する履歴アクティビティを使用して、再帰型ニューラルネットワークを訓練すること、
前記再帰型ニューラルネットワークを使用して、少なくとも１つの決められた期間にわたって前記複数の文書に関して指定されたユーザの予想されるアクティビティを判定すること、
前記複数の文書のうちの少なくとも指定された文書に関するユーザアクティビティを検出することであって、前記ユーザアクティビティが前記指定されたユーザに関連付けられる、前記ユーザアクティビティを検出すること、

前記再帰型ニューラルネットワークを使用して前記アクティビティを処理し、前記ユーザアクティビティが前記予想されるタイプのアクティビティから逸脱しているかどうかを判定することであって、前記判定がさらに、前記指定された文書に対して判定された少なくとも１つのトピックに少なくとも部分的に基づいている、前記アクティビティを処理すること、及び

前記ユーザアクティビティが、前記予想されるアクティビティから許容できないほど逸脱すると判定され、前記ユーザアクティビティまたは前記指定された文書の少なくとも１つに対するリスクスコアが、少なくともアラート閾値を満たしている場合に、セキュリティアラートを生成すること

を含む、コンピュータ実施方法。

【請求項２】

前記再帰型ニューラルネットワークによる前記処理の結果を、カルマンフィルタを用いて処理して、複数の期間にわたる前記ユーザアクティビティを分析し、前記ユーザアクティビティが、前記予想されるアクティビティから許容量を超えて逸脱しているかどうかをさらに判定すること

をさらに含む、請求項１に記載のコンピュータ実施方法。

【請求項３】

前記指定されたユーザを含むピアグループ内のピアのピアアクティビティと前記ユーザアクティビティとをさらに比較すること、及び

前記ピアアクティビティに関する前記ユーザアクティビティの第２の逸脱にさらに基づいて、前記ユーザアクティビティが前記予想されるアクティビティから許容できないほど逸脱しているかどうかを判定すること

をさらに含む、請求項１に記載のコンピュータ実施方法。

【請求項４】

前記電子リソース環境の前記複数の文書及び複数のユーザに関して監視されたアクティビティデータを使用して訓練された教師なし分類器を使用して、前記指定されたユーザを含む前記ピアグループを判定すること

をさらに含む、請求項３に記載のコンピュータ実施方法。

【請求項５】

電子リソース環境で、エンティティのために格納された複数の文書に関する履歴アクティビティを使用してニューラルネットワークを訓練すること、

前記ニューラルネットワークを使用して、少なくとも１つの決められた期間にわたって前記複数の文書に関して指定されたユーザの予想されるアクティビティを判定すること、

前記複数の文書のうちの少なくとも指定された文書に関するユーザアクティビティを、少なくとも決められた期間にわたって検出することであって、前記ユーザアクティビティが前記指定されたユーザに関連付けられる、前記ユーザアクティビティを検出すること、

前記指定された文書に関連する少なくとも１つのトピックを判定すること、

前記少なくとも１つのトピックを、前記予想されるアクティビティに関連するトピックと比較すること、

前記ユーザアクティビティを、前記ニューラルネットワークを使用して処理して、前記ユーザアクティビティが、前記予想されるタイプのアクティビティから逸脱しているかどうかを判定すること、前記判定は、前記少なくとも１つのトピックと前記予想されるアクティビティに関連する前記トピックとの間のトピックベクトル空間におけるトピック距離に少なくとも部分的に基づいており、及び

前記ユーザアクティビティが前記予想されるタイプのアクティビティから許容できないほど逸脱すると判断された場合に、決められたアクションを実行すること

を含むコンピュータ実施方法。

【請求項６】

判定されたリスクスコアに少なくとも部分的に基づいて、実行すべき前記アクションを判定することであって、少なくとも１つのリスク閾値が実行される可能性のあるアクショ

ンに関連付けられており、前記アクションは、それぞれがリスクスコアの範囲にそれぞれ関連付けられた複数の可能なアクションの１つであり、前記可能なアクションが、セキュリティアラートの生成、異常なアクティビティデータの記録、または前記指定されたユーザもしくは前記指定された文書の少なくとも１つに関連付けられたアクセス権の調節のうちの少なくとも１つを含む、前記アクションを判定すること
をさらに含む、請求項５に記載のコンピュータ実施方法。
【請求項７】
前記指定されたユーザを含むピアグループ内のピアのピアアクティビティと前記ユーザアクティビティとをさらに比較すること、
前記ピアアクティビティに関する前記ユーザアクティビティの第２の逸脱に少なくとも部分的に基づいて、前記ユーザアクティビティが前記予想されるユーザアクティビティから許容できないほど逸脱しているかどうかを判定すること、及び
前記電子リソース環境の前記複数の文書及び複数のユーザに関して監視されたアクティビティデータを使用して訓練された教師なし分類器を使用して、前記指定されたユーザを含む前記ピアグループを判定すること
をさらに含む、請求項５に記載のコンピュータ実施方法。
【請求項８】
前記ユーザアクティビティには、アクセスの種類、アクセスの頻度、一定期間のアクセス試行の合計数、アクセスの送信元アドレス、アクセスされたトピック、アクセスされた文書の種類、アクセスの場所、前記アクセスの日もしくは時間、または前記アクセスを取得するために使用されるアプリケーションプログラミングインタフェース（ＡＰＩ）呼出しのうちの少なくとも１つが含まれる、請求項５に記載のコンピュータ実施方法。
【請求項９】
システムであって、
少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサによって実行されるとき、前記システムに、
訓練用文書のセットを使用してトピックモデルを訓練することであって、前記セットの各訓練用文書が、少なくとも１つの識別されたトピックと割り当てられたリスクスコアとを有する、前記トピックモデルを訓練すること、
電子リソース環境全体にわたってエンティティ用に格納されている複数の文書をクロールし、前記複数の文書にインデックスを付けること、
少なくとも前記トピックモデルを使用して、前記複数の文書の各文書の１つ以上のトピックを判定すること、
前記複数の文書の各文書のリスクスコアを判定すること、及び
前記エンティティに関連付けられた許可ユーザによるアクセスのためのセキュリティ情報を提供することであって、前記セキュリティ情報には、前記識別されたトピックの情報と、前記エンティティ用に格納されている前記複数の文書のリスクスコアとが含まれる、前記セキュリティ情報を提供すること
を行わせる命令を含むメモリと
を備えた前記システム。
【請求項１０】
前記命令が、実行されると、前記システムにさらに、
前記電子リソース環境の前記エンティティ用に格納された新たな文書または文書の変更のうちの少なくとも１つに対応する更新された文書データを検出すること、及び
前記更新された文書データのインスタンス毎に前記トピックモデルをさらに訓練すること
を行わせる、請求項９に記載のシステム。
【請求項１１】
前記命令が、実行されると、前記システムにさらに、
自然言語理解（ＮＬＵ）を利用して前記複数の文書を分析し、前記複数の文書の各文書

に関連付けられた１つ以上のトピックを判定すること
を行わせる、請求項９に記載のシステム。
【請求項１２】
前記命令が、実行されると、前記システムにさらに、
前記複数の文書に含まれる複数の要素を判定することであって、前記複数の要素の各要素が、前記エンティティに潜在的なセキュリティリスクをもたらす、前記複数の要素を判定すること、
前記複数の要素の各要素にそれぞれリスクスコアを割り当てること、及び
指定された文書に関連付けられた前記要素の１つに対する最高のそれぞれのリスクスコアに少なくとも部分的に基づいて、前記複数の文書のうちの前記指定された文書の前記リスクスコアを判定すること
を行わせる、請求項９に記載のシステム。
【請求項１３】
前記命令が、実行されると、前記システムにさらに、
前記電子リソース環境の前記エンティティ用に格納された新たな文書を検出すること、
前記新たな文書に関連する１つ以上のトピックを判定すること、
前記新たな文書の前記１つ以上のトピックを有する他の文書に関連付けられた文書バケットに前記新たな文書を割り当てること、及び
前記文書バケットのバケットリスクスコアに少なくとも部分的に基づいて、前記新たな文書にリスクスコアを割り当てること
を行わせる、請求項９に記載のシステム。
【請求項１４】
前記命令が、実行されると、前記システムにさらに、
前記訓練されたトピックモデルを使用して、前記複数の文書を処理することにより、新しいトピックを学習させること
を行わせる、請求項９に記載のシステム。
【発明の詳細な説明】
【背景技術】
【０００１】
ユーザは、共有リソース環境を通じて提供され得るリモートコンピューティングリソースを用いて、ますます多くのタスクを実行するようになっている。ユーザは専用のハードウェアやソフトウェアを購入して保守する必要がなく、代わりに、いつでも利用できるリソースに対してのみ支払いをすることが可能であり、それらのリソースは、通常はリソースプロバイダによって管理されることになるので、このことは多くの利点を有する。ユーザは、リソースプロバイダが提供する各種のリソースを用いて、データの格納やアプリケーションの実行などのタスクを実行することができる。様々な組織では、それらの組織用に格納されたデータ及び文書の非常に大きなコーパスが存在し得る。特にユーザが何らかの手動分類プロセスを経ずして文書を作成し、それをリモートデータストアに格納する場合には、このような文書のそれぞれの文脈を判定することは非常に困難となり得る。さらに、このような文書の適切なセキュリティを確保することは、これらの文書毎に許可されるべきアクセスの種類に精通すること、及び要求されるアクセス許可と矛盾する可能性のあるアクセスを検出することが難しいので、困難となり得る。
【０００２】
本開示による様々な実施形態について、図面を参照しながら説明する。
【図面の簡単な説明】
【０００３】
【図１】様々な実施形態を実施することができる環境の例を示す図である。
【図２】様々な実施形態に従って利用できる、１人以上の顧客のために格納された文書及びデータを分析するのに使用できるシステムの例を示す図である。
【図３】様々な実施形態に従って利用できる、顧客文書に関しての異常行動を検出するの

に使用できるシステムの例を示す図である。
【図４】様々な実施形態に従って判定されたユーザピアに関するユーザの異常行動を検出するのに使用できるシステムの例を示す図である。
【図５】様々な実施形態に従って利用できる、文書を見つけて分類するためのプロセスの例を示す図である。
【図６】様々な実施形態に従って利用できる、異常行動を検出するためのプロセスの例を示す図である。
【図７】様々な実施形態に従って利用できる、検出された行動が異常であるかどうかを判定するためのプロセスの例を示す図である。
【図８】様々な実施形態の態様を実施するために使用できるコンピューティングデバイスの構成要素の例を示す図である。
【発明を実施するための形態】
【０００４】
以下の記載では、様々な実施形態を説明する。説明のために、実施形態の理解の徹底を期すよう具体的構成及び詳細を述べる。しかしながら、この具体的な詳細がなくても本実施形態を実施できることが、同様に、当業者には明らかになるであろう。なお、周知の特徴事項は、説明される実施形態を不明瞭にしないために、省略し、または簡略化する場合がある。
【０００５】
様々な実施形態によるアプローチは、エンティティ用に格納された文書のコーパス、及び他のデータオブジェクトのデータ損失防止を提供する。コーパスを分析して、それらの文書のそれぞれについて１つ以上のトピックを判定することができる。分析には、各文書にリスクスコアを割り当てるために使用できる要素または態様の検出も含まれる。トピック及びセキュリティ要素の種類、ならびに関連リスクスコアは、例えば、トピックモデル及びランダムフォレストリグレッサを使用して、経時的に学習させ、適合させることができる。様々な文書へのアクセスを監視することができ、例えば、訓練された再帰型ニューラルネットワーク分類器または他のニューラルネットワーク分類器を使用して、ユーザの予想される行動を判定できる。実際のユーザアクティビティを監視し処理して、アクティビティが異常であるかどうか、または過度に逸脱しているかどうかを、予想されるユーザアクティビティを基準にして判定することができる。アクティビティを、経時的に学習させることもできるユーザピアのアクティビティと比較して、このアクティビティがまた、ユーザピアグループの中で異常なものであるかどうかを判定することもできる。異常行動の場合には、このアクセスに対してアラートを生成するかどうかを判定するために、アクセスされた文書（複数可）のリスクスコア（複数可）を分析することができる。生成されるセキュリティアラートの数を制限するために、リスクスコアが十分に低い場合には、リスクスコアの低い文書への異常なアクセスはログに記録するか、無視する場合さえある。トピックの割り当て、リスクスコアの判定、及びアクティビティ分類器の精度を、他のそのような態様の中でも特に向上させるために、各アクティビティ及び結果を使用してモデルを訓練し、更新することができる。
【０００６】
他の様々な機能を、本明細書の他の箇所で説明し、提案するのみならず、様々な実施形態の範囲内で実施することもできる。
【０００７】
図１は、様々な実施形態の態様を実施することができる環境１００の例を示す。この例では、ユーザがクライアントデバイス１０２を利用して、少なくとも１つのネットワーク１０４越しに、リソースプロバイダ環境１０６に要求を送信することができる。クライアントデバイスは、適切なネットワークを通じて要求、メッセージ、または他のそのような情報を送受信し、デバイスのユーザに情報を伝達し返すように動作可能ないずれかの適切な電子デバイスを含み得る。上記のクライアントデバイスの例としては、パーソナルコンピュータ、タブレット型コンピュータ、スマートフォン、ノート型コンピュータなどがあ

る。少なくとも１つのネットワーク１０４は、イントラネット、インターネット、セルラネットワーク、ローカルエリアネットワーク（ＬＡＮ）、または他のいずれかのそのようなネットワークもしくは組合せを含む、いずれかの適切なネットワークを含んでもよく、ネットワークを通じた通信は、有線接続及び／または無線接続を介して可能にすることができる。リソースプロバイダ環境１０６は、要求を受信し、それらの要求に応答して情報を返し、またはアクションを実行する、いずれかの適切な構成要素を含み得る。一例を挙げると、プロバイダ環境は、要求を受信し、処理し、次いでその要求に応答して、データ、ウェブページ、ビデオ、音声、または他のそのようなコンテンツもしくは情報を返すためのウェブサーバ及び／またはアプリケーションサーバを含んでもよい。

【０００８】

様々な実施形態では、プロバイダ環境は、多種多様な目的のために、複数のユーザが利用できる各種のリソースを含み得る。少なくとも一部の実施形態では、所与のリソースの全部もしくは一部、またはリソースセットが、少なくとも定められた期間にわたって特定のユーザに割り当てられ、または特定のタスクのために割り当てられ得る。プロバイダ環境からのこれらのマルチテナントリソースの共有は、他にも同様の用語はあるが特に、リソース共有、ウェブサービス、または「クラウドコンピューティング」と呼ばれることが多く、特定の環境及び／または実施態様に依存する。この例では、プロバイダ環境は、１種類以上の複数のリソース１１４を含む。これらの種類には、例えば、ユーザによって提供された命令を処理するように動作可能なアプリケーションサーバ、またはユーザ要求に応答して１つ以上のデータストア１１６に格納されたデータを処理するように動作可能なデータベースサーバが含まれ得る。そのような目的について知られているように、ユーザは、所与のデータストア内のデータストレージの少なくとも一部を確保しておくこともできる。ユーザが、様々なリソース及びリソースインスタンスを確保できるようにする方法は、当技術分野ではよく知られており、したがって、処理全体の詳細な説明、及び可能な全ての構成要素の説明については、本明細書では詳しく扱わないことにする。

【０００９】

少なくとも一部の実施形態では、リソース１１４の一部を利用したいユーザが要求を送信することができ、この要求はプロバイダ環境１０６のインタフェース層１０８に受信される。インタフェース層は、ユーザがプロバイダ環境に要求を送信できるようにするアプリケーションプログラミングインタフェース（ＡＰＩ）または公開された他のインタフェースを含み得る。この例のインタフェース層１０８は、少なくとも１つのウェブサーバや、ルーティング構成要素、負荷分散装置などの他の構成要素を含むこともできる。リソースを提供させる要求がインタフェース層１０８に受信されるとき、その要求のための情報は、リソースマネージャ１１０、またはユーザアカウント及びユーザ情報、リソースプロビジョニング及びリソース使用状況、ならびに他のそのような態様を管理するように構成された他のそのようなシステム、サービス、もしくは構成要素に向けられ得る。要求を受信するリソースマネージャ１１０は、要求を送信するユーザの本人認証を行うと共に、そのユーザがリソースプロバイダに既存のアカウントを有しているかどうかを判定するなどのタスクを実行することができ、そこでアカウントデータは、プロバイダ環境内の少なくとも１つのデータストア１１２に格納され得る。ユーザは、ユーザの本人認証を行うために、プロバイダに各種の認証情報のいずれかを提供することができる。それらの認証情報には、例えば、ユーザ名及びパスワードの組、生体データ、デジタル署名、または他のそのような情報が含まれ得る。プロバイダは、この情報をユーザ用に格納された情報と照らし合わせて検証することができる。ユーザが適切なアクセス許可、状態などを付与されたアカウントを有する場合に、リソースマネージャは、ユーザの要求に適合し得る十分なリソースが有るかどうかを判定することができ、リソースが有る場合は、リソースを提供するか、または別の方法で、それらのリソースの要求によって指定された量のリソースをユーザが使用できるように、リソースの対応する部分へのアクセスを許可することができる。この量としては、例えば、他にも同様の値はあるが、単一の要求を処理する記憶容量、もしくは単一のタスクを実行する記憶容量、指定された期間、または繰返し期間／更新可

能期間があり得る。ユーザがプロバイダに有効なアカウントを持たず、ユーザアカウントが、要求内に指定された種類のリソースにアクセスできるようにせず、または別のそのような理由により、ユーザにそのようなリソースへのアクセスを取得させないようにしている場合には、他にも同様の選択肢はあるが、とりわけ、ユーザがアカウントを作成しもしくは修正し、または要求で指定したリソースを変更したりできるようにする通信がユーザに送られてもよい。

【００１０】

ユーザが認証され、アカウントが検証され、リソースが割り当てられると、ユーザは、指定された容量、データ転送の量、期間、または他のそのような値の割り当てられたリソース（複数可）を利用することができる。少なくとも一部の実施形態では、ユーザは、後続の要求がユーザセッション上で処理されることを可能にするために、セッショントークンまたは他のそのような認証情報をそれらの要求と共に提供してもよい。ユーザは、リソース識別子、特定アドレス、またはクライアントデバイス１０２が、リソースマネージャ１１０と通信する必要なしに、割り当てられたリソースと通信することを可能にする他の情報を、少なくとも、ユーザアカウントの関連する態様が変更されるか、ユーザがリソースへのアクセスをもはや許可されなくなるか、または別のそのような態様が変更されるかといった時まで受信することができる。

【００１１】

この例のリソースマネージャ１１０（または別のそのようなシステムもしくはサービス）は、管理アクションに加えて、プロビジョニング、スケーリング、レプリケーションなどを含み得る制御機能を取り扱うハードウェア構成要素及びソフトウェア構成要素の仮想層として機能することもできる。リソースマネージャは、インタフェース層１０８内の専用ＡＰＩを利用することができ、そこでは各ＡＰＩが、インスタンスのプロビジョニング、スケーリング、クローニング、またはハイバネーションを行うなどのために、データ環境に関して実行すべき少なくとも１つの特定のアクションについての要求を受信するように提供され得る。ＡＰＩのうちの１つへの要求を受信すると、インタフェース層のウェブサービス部分は、呼出しに対応し、または呼出しを処理するために必要なステップまたはアクションを判定する要求を構文解析し、または別の方法で分析することができる。例えば、データリポジトリを作成する要求を含むウェブサービス呼出しが受信されてもよい。

【００１２】

少なくとも１つの実施形態のインタフェース層１０８は、様々なＡＰＩを提供し、ＡＰＩ仕様に基づいて適切な応答を返すことができるスケーラブルな顧客対応サーバのセットを含む。インタフェース層は、１つの実施形態では、外的に対面している顧客ＡＰＩを処理するステートレスな複製サーバで構成される少なくとも１つのＡＰＩサービス層を含むこともできる。インタフェース層は、認証情報に基づいた顧客の認証、顧客の承認、ＡＰＩサーバへの顧客要求の制限、ユーザ入力の検証、ならびに要求及び応答のマーシャリングまたはアンマーシャリングなどのウェブサービスフロントエンド機能を担当することができる。ＡＰＩ層は、ＡＰＩ呼出しに応答して、管理データストアからのデータベース構成データの読取り／管理データストアへのデータベース構成データの書込みを担当することもできる。多くの実施形態では、ウェブサービス層及び／またはＡＰＩサービス層は、外部から見える唯一の構成要素であり、または制御サービスの顧客に見え、制御サービスの顧客によってアクセス可能な唯一の構成要素である。ウェブサービス層のサーバは、当技術分野で知られているように、ステートレスであり、水平方向にスケーリングすることができる。例えば、サーバが単一のデータセンタの障害に対応できるように、ＡＰＩサーバと永続データストアとを地域内の複数のデータセンタに散在させることができる。

【００１３】

すでに述べたように、そのような環境により、組織が、インターネットなどのネットワークを通じて、コンピューティングリソースを取得し構成して、様々な種類のコンピューティング操作を実行できるようになる（例えば、スレッド、プログラム、ソフトウェア、ルーチン、サブルーチン、プロセスなどを含むコードを実行する）。したがって、開発者

は、物理マシンを入手することを心配することなく、必要な量のコンピューティングリソースを迅速に購入するか、または別の方法で入手することができる。そのようなコンピューティングリソースは、通常、仮想コンピューティングリソースまたは仮想マシンインスタンスの形で購入される。これらの仮想マシンのインスタンスは、独自のオペレーティングシステムと他のソフトウェア構成要素とを備えた物理コンピューティングデバイスでホストされ、物理コンピュータと同じようにして利用できる。

【００１４】

大規模な組織では、そのような環境全体に何百万もの（またはそれ以上の）文書及びデータオブジェクトが格納されている場合がある。そのような組織では、様々な文書及びオブジェクトの、特にそれらが更新されたときのコンテンツ、ならびに各文書及びオブジェクトに適用されるアクセスポリシ、アクセス許可ポリシ、またはセキュリティポリシを判定するなど、文書を管理することが困難な場合がある。さらに、組織にとって潜在的に危険または有害である可能性のある異常行動がいつ発生するかを判定するために、これらの文書について適切なユーザ行動を判定することは非常に困難であり得る。特定のキーワードまたはパターン（例えば、社会保障番号、クレジットカード番号、または医療記録）を検索するなど、利用できる従来の様々なセキュリティ機構があるが、その機構は限定的であり、誤検知や失敗の傾向がある。

【００１５】

そのため、様々な実施形態によるアプローチは、顧客または他のそのようなエンティティのために格納された様々な文書、データオブジェクト、及び他のそのようなオブジェクト（以降、簡略化するためにしばしば単に「文書」と呼ぶ）を自動的に分析して、それらの文書のそれぞれについて１つ以上のトピックを判定しようと試みることができる。分析には、各文書にリスクスコアを割り当てるために使用できるセキュリティ要素の検出も含まれる。トピック及びセキュリティ要素の種類、ならびに関連リスクスコアは、例えば、ニューラルネットワーク、モデルセット、訓練されたリグレッサ、または他のそのような機構を使用して、経時的に学習させ、適合させることができる。様々な文書へのアクセスを監視することもでき、例えば、再帰型ニューラルネットワークを使用して、ユーザの予測される行動または予想される行動を判定できる。実際のユーザアクティビティを監視し処理して、アクティビティが異常であるかどうかを、予想されるユーザアクティビティを基準にして判定することができる。アクティビティを、経時的に学習させることもできるユーザピアのアクティビティと比較して、このアクティビティがまた、ユーザピアグループの中で異常なものであるかどうかを判定することもできる。異常行動の場合には、このアクセスに対してアラートを生成するかどうかを判定するために、アクセスされた文書（複数可）のリスクスコア（複数可）を分析することができる。生成されるセキュリティアラートの数を制限するために、リスクスコアが十分に低い場合には、リスクスコアの低い文書への異常なアクセスをログに記録するか、無視する場合さえある。トピックの割り当て、リスクスコアの判定、及びアクティビティ分類器の精度を、他のそのような態様の中でも特に向上させるために、各アクティビティ及び結果を使用してモデルを訓練し、更新することができる。

【００１６】

様々な実施形態に則った実施形態は、文書、データ、及び他の知的財産を侵害及び盗難から保護するのに役立ち得るデータ損失防止サービスを提供することができる。そのようなサービスプロバイダのアカウントを有した、少なくとも一部の実施形態ではマルチテナントリソース環境を提供するリソースプロバイダでもある顧客は、格納されている顧客の文書に関する情報を取得するために、様々なツールとインタフェースとを利用することができ、それらの文書に関して検出された異常行動または危険行動に関するレポートまたはアラートを受け取ることができる。これは、多くの場合「クラウド」のストレージと呼ばれる、そのようなマルチテナント環境またはリソースプロバイダ環境に格納されている文書を保護するのに役立ち得る。

【００１７】

いくつかの実施形態では、そのようなサービスは、電子メール、文書、及びスプレッドシートなどの顧客の知的財産、ならびに関連データ及び他のオブジェクトを探して追跡するために、人工知能（ＡＩ）または機械学習を利用することができる。いくつかの実施形態では、これには、顧客ネットワークを介して格納される文書もまた含まれ得る。そのようなサービスでは、各文書またはデータのトピック、ビジネス関連性、及び価値などの情報を理解するために、自然言語処理（ＮＬＰ）を活用することができる。サービスは、各文書のリスクレベルまたはリスクスコアを判定することもできる。サービスは、異常行動またはデータとの異常な関わりを識別して表面化させ、潜在的な侵害または攻撃を顧客に警告することができる。例えば、顧客サービス担当者が外部ＩＰアドレスから機密の人事ファイルにアクセスしようとすると、サービスはこのアクティビティを異常であると識別し、アラートを生成し得る。少なくとも一部の実施形態では、サービスは、そのような各文書にリスクスコアまたはセキュリティレベルを割り当てることもできる。これにより、アラートを生成するかどうかの判定を、アクセスされた文書（複数可）のリスクスコア（複数可）に少なくとも部分的に基づかせることができる。

【００１８】

様々な実施形態では、データ損失防止システムまたはサービスは、トピックモデリングを利用することができる。利用されまたは生成されるトピックモデルは、文書及びトピックのクラスタを見つけることができる潜在的ディリクレ配分法（ＬＤＡ）などのいずれかの適切な技術に基づくことができる。トピックモデリングでは、観測されていないグループによって観測の結果セットが説明されるようにするために、様々な生成統計手法を活用することができ、これはデータの一部が類似していると判定される理由を説明するのに役立ち得る。これは、データの大きなコーパスにわたってトピックのセットを識別する教師なし分類器としての従来の使用法とは異なり、代わりに、ユーザが通常アクセスする種類のデータを個別に、ユーザのピアに関して分類するために使用される。そのようなアプローチは、組織のデータに関する特定の知識を必要とせず、代わりに、特定のユーザまたはピアグループがコーパス全体のサブセットとして通常アクセスするトピックのセットを作成し、維持することができるという利点をもたらす。同様に、後に処理される文書のリスクスコアを判定することができるようにするために、リスクスコアが割り当てられた訓練用文書を使用して、ランダムフォレストリグレッサなどの分類器を訓練することができる。訓練されたリグレッサは、ラベル付きデータセットを含む文書を受信し、本明細書の他の箇所で説明されているように、対応するリスクスコアを提供することができる。

【００１９】

上記のデータ損失防止サービスは、一定の期間にアクセスされた文書の量、頻度、またはその他のメトリック（複数可）を、ユーザ及び少なくとも一部の実施形態ではユーザのピアに合わせて訓練される再帰型ニューラルネットワークへの入力として利用することができる。少なくとも一部の実施形態では、ピアグループは、組織構造（すなわち、組織図）に基づいて自動的に判定され、及び／またはアクセスされた文書またはトピックの種類、それらのアクセスの頻度などの情報を分析することによって学習され得る。ピアグループの例には、例えば、特定の方法でリソースにアクセスする可能性が高いソフトウェア開発者または人事担当者のグループが含まれ得る。このピアのアクティビティと、ユーザが頻繁に対話する他のピアのアクティビティとは、アラートを生成すべき不審なアクセスを判断するために、ユーザが対話するであろうトピックの種類や文書の量などの情報を予測するのに役立ち得る。

【００２０】

一実施形態では、就業日にユーザがアクセスする文書を、追跡し、監視し、または別の方法で判定することができる。トピックモデルは、組織全体のデータコーパスの処理に基づいて、訓練され、更新される。組織全体にわたって各文書には、１つ以上のトピックで構成されるラベルを付けることができる。ユーザは、対話するデータの種類、及び組織構造やその他の情報に少なくとも部分的に基づいて、ピアグループにクラスタ化することができる。ユーザが様々な文書と対話するとき、アクセスされる文書及びトピックの数は、

過去の基準値に基づいて将来のアクティビティを予測できる逆伝播を用いた教師なし分類器への入力として送り込まれる。ユーザが、予測されるアクセスの種類または頻度、及び少なくとも一部の実施形態でのピアグループのアクセスの種類または頻度から、判定された量よりも大きく逸脱した（すなわち、閾値または最大許容量を超えた）場合、ニューラルネットワークは、逸脱を検出し、セキュリティグループまたは他の適切なエンティティ向けにアラートを生成することができる。

【００２１】

いくつかの実施形態では、再帰型ニューラルネットワーク（ＲＮＮ）を使用して、ユーザ行動をモデル化し、組織のリスクを示す基準に設定されたアクティビティの増加または減少に対して警告することができる。このようなＲＮＮベースのアプローチ（または階層型時間メモリベースのアプローチなどの他のアプローチ）は、個別に、及び１つ以上のユーザピアグループに関して、数百以上のユーザアクティビティの特徴を同時に評価するなどの利点を提供することができる。ただし、様々な状況で従来のニューラルネットワークは、重要な洞察（モデルのイントロスペクション）や、または特定のユースケースの性能を向上させるように結果の出力を容易に調整する能力をユーザに提供しない。したがって、様々な実施形態によるアプローチは、ＲＮＮによって一緒に評価される個々の入力を視覚化する能力、及びニューラルネットワークがその入力の経時的な変化に大方反応するように出力を平滑化する能力を提供する。少なくとも一部の実施形態では、平滑化は、ニューラルネットワークからの個々の特徴予測に適用することができるカルマンフィルタベースの平滑化関数の使用により達成することができ、その後、それらの予測を、関数が異常であるかどうかを判定する上位の分類器によって評価することができる。そのようなアプローチは、重み付けを調節する能力と、ユーザアクティビティを予測するためにニューラルネットワークに入る特徴毎の組合せの応答とを提供する。これは、精度及びリコールの性能を劇的に向上させるとともに、普通なら性能に影響を与え得るノイズの多い特徴やコーナーケースの影響を特定して軽減するのに役立つことができる。

【００２２】

図２は、様々な実施形態による、クローリングや文書分析などの機能を実行するのに利用できるシステム２００の例を示す。参照番号は、説明を簡略化する目的で、図面間で同様のオブジェクトを表すために持ち越される場合があるが、そのような使用法は、特に別段の指示が無い限り、様々な実施形態の範囲の制限として解釈されるべきではない。図１の環境と同様に、顧客は、ここでは顧客コンソール１０２を操作するクライアントデバイスを利用して、少なくとも１つのネットワーク１０４越しに、リソースプロバイダ環境１０６のリソースにアクセスすることができる。すでに述べたように、これは、他にも同様の選択肢はあるが、とりわけ、顧客データを少なくとも１つのデータリポジトリ２１４に格納することや、文書を少なくとも１つの文書ストア２１２に格納することなどに使用できる。いくつかの実施形態では顧客は、顧客のために格納された様々なデータ及び文書へのアクセスを制御するために、顧客コンソール１０２を利用して、アクセスマネージャ２０８または他のそのようなシステムもしくはサービスによって利用できるセキュリティ設定を指定することができる。本明細書の別の箇所で詳細に説明するように、ユーザが特定のデータまたは文書にアクセスできるようになる前に、様々なセキュリティポリシを実施して、特定のアクセス許可、認証情報、ロール、または他のアクセス基準を満たす必要がある。アクティビティモニタ２０４などのサービスは、様々なユーザによる様々な文書及びデータへのアクセスを監視し、アクティビティログ２０６または他のそのようなリポジトリなどの場所に情報を格納することができる。セキュリティマネージャ２０２は、アクセスマネージャ２０８及び／またはアクティビティモニタ２０４と連携して、潜在的に不審な行動の存在を判定することができ、次いでそれを顧客コンソール１０２に報告するか、さもなければアラートまたは通知として提供することができる。少なくとも一部の実施形態では、生成されるアラートの種類、アラートを生成する行動の種類、及び他のそのような情報を判定するために、顧客コンソール１０２を使用して、セキュリティマネージャ２０２にセキュリティ設定またはセキュリティ選択を提供することもできる。

【００２３】
少なくとも一部の実施形態では、組織などの顧客のために、データストア２１４及び／または文書ストア２１２に格納された任意のコンテンツが存在し得る。少なくとも一部の実施形態では、このコンテンツを分析して、顧客のために格納されたデータ、文書、及び他のオブジェクトの種類を可視化することが望ましい場合がある。この例では、クローラ２１０を使用して、顧客のために格納されている様々な文書（及び他のデータなど）を探し出して分析することができる。クローラは、データの内容を探し出し、解析し、評価する目的で、データに含まれる単語、数字、文字列、またはパターンを分析するなど、様々なデータクロールアルゴリズムを含むことができる。クローラ２１０はまた、各文書に１つ以上のトピックを割り当てるなど、様々な文書を分類することができる分類器アルゴリズムを含むか、またはそれと連携することができる。クローラ２１０はまた、文書毎（または少なくとも文書のサブセット）にリスクスコアを判定することができる１つ以上のリスク評価アルゴリズムを含むか、またはそれと連携することができる。少なくとも一部の実施形態では、リスクスコアは、正規表現の様々なメトリックの複合物であり得、文書内の様々なトピック及びテーマの存在に少なくとも部分的に基づいたものであり得る。そのようなアプローチの１つの利点は、顧客が顧客コンソール１０２または別のそのような機構を利用して、顧客用に格納されているコンテンツの種類、及びそのコンテンツと関連したリスクを可視化できることである。少なくとも一部の実施形態では、顧客は、コンテンツ、ならびに割り当てられたトピック及びリスクスコアを調べ、顧客が適切と考える調節を行う能力を有することもできる。その場合、これらの調節を用いて、特徴分類及びスコア判定を改善するために、ニューラルネットワークをさらに訓練することができる。少なくともいくつかの実施形態では、顧客は、様々な文書へのアクセスのパターンまたは種類、特定の文書またはトピックにアクセスするユーザまたはピアグループのリスト、特定のリスクスコア付きの文書などを調べることもできる。

【００２４】
一実施形態では、クローラ２１０は、既知の文書と教師なし分類との組合せを用いて、全コンテンツを分類する。分類された文書の初期セットを、初期訓練セットとして提供することができる。これらの文書には、リスクスコアを割り当てることもでき、または他の同様の選択肢の中でも特に、訓練用の初期リスク基準を提供することができる。初期データを用いてニューラルネットワークを訓練し、その後、データのコーパスを用いて教師なし分類を提供することができる。そのようなアプローチにより、業界固有のコンテンツを認識し、分類できるようにし、適切なリスクスコアを判定することができるようになる。文書を分類するための従来のアプローチでは、社会保障番号やクレジットカード番号などの特定のコンテンツを探し、ユーザがその情報にアクセスするといつでも警告することができる。様々な実施形態によるアプローチは、代わりに、以前に遭遇したことがなく、または分類されていない、医薬品データなどの業界固有のコンテンツデータを含み得るコンテンツを、動的に分類する能力を提供する。コンテンツについて学んだこと、及び他の関連コンテンツがどのように採点されるかに基づき、トピックを判定し、リスクスコアを割り当てることができる。例えば、類似した頻度でピアによってアクセスされる文書のスコアを使用して、これらの文書のリスクスコアを推定することもできる。分類器は、特定のコンテンツの分離とラベル付けとを試み、その後、割り当てるべき適切なリスクスコアを判定することができる。少なくとも一部の実施形態では、様々な行動分析を利用して、文書に関する基準のユーザアクティビティを判定することができ、これを使用してリスクスコアを判定することができる。様々な実施形態は、製薬文書を企業内のごく少数の人々のみがアクセスできるものとして認識することなどにより、企業のリスクを示す文書の特徴を分離させることもできる。これは、リスクスコアやアクセスパターンなどを生成する際に使用するデータの種類と関連トピックとを学習するのに役立ち得る。

【００２５】
一例では、クローラ２１０は、顧客と関連した全ての文書（及び他のデータ）にインデックスを付けることができる。クローラ２１０は、文書のコンテンツ、及びそれらの文書

のアクセスパターン履歴を分析することもできる。アクセスパターン履歴には、オープン、読取り、更新、ログイン、管理イベントなどに関する情報が含まれ得る。いくつかの実施形態では、文書を分類し、及び／またはそのような他の分類を実行するのに使用できるトピックモデルを構築するために、過去６ヶ月などのある期間にわたって判定された全てのアクセスデータを利用することができる。この例では、クローラは、トピックモデリングを利用し、テキストコンテンツの様々なインスタンスを分類する方法に関しての洞察を提供する。いくつかの実施形態では、分類を容易に判定できるように、トピックデータをトピックデータストア２１６に格納し、一方様々な文書の分類データを、文書自体に格納し、または文書を参照する分類データストア２１８もしくはテーブルに格納する。

【００２６】

図３は、様々な実施形態による、分類された文書に対しての異常行動を判定するために使用できるシステム３００の例を示す。前の例と同様に、このシステムは、システムのユーザによる様々な文書、データ、及び他のオブジェクトへのアクセスを監視できるアクティビティモニタ２０４を含み得る。情報は、ログデータストア２０６などの場所か、またはそのような他の場所に格納することができる。各アクティビティの情報は、他にも同様の選択肢はあるが、とりわけ、分類器サービス３０２に送り込まれるか、または分類器サービスによってアクティビティキューから取り出され得る。いくつかの実施形態では、アクティビティデータを個別に処理することができるが、他の実施形態では、ニューラルネットワークの訓練が過剰にリソースを消費することなどを防ぐために、データを３２個のアクティビティエントリのバッチに分けるなど、数回に分けて処理してもよい。いくつかの実施形態では、ある期間にわたるユーザアクティビティの集合または集約を処理することができ、これは、生データを使用するよりもコスト及びリソースを効率化し得る。例えば、ユーザの全てのサービスインタラクションは、オープンソースのクラスタコンピューティングフレームワークであるＡｐａｃｈｅ　Ｓｐａｒｋなどの技術を使用して集約することができる。

【００２７】

この例では、アクティビティデータが分類器サービスに受信され、再帰型ニューラルネットワーク（ＲＮＮ）によって処理される。様々な実施形態の範囲内で、他のタイプのニューラルネットワーク（すなわち、畳み込みネットワークまたは敵対的生成ネットワーク）も同様に使用できることを理解されたい。アクティビティデータは、最初に分類器サービスのＲＮＮによって処理されて、判定された将来の期間にわたる様々なユーザのアクティビティを予測することができる。この情報は、訓練を受けたＲＮＮにより、他にも同様の選択肢はあるが、とりわけ、ユーザの過去の行動やユーザのピアの行動などの情報に基づいて判定され得る。予測または予想される行動データは、行動データストア３１０またはそのような他の場所に格納することができる。再帰型ニューラルネットワークを使用する利点は、ネットワークが多数のユーザ及び文書にわたる経時的な使用パターンを認識し、それらのパターンに基づいてユーザが今後どのように行動し得るかを予測するように学習できることである。再帰型ニューラルネットワークは、特定のデータへの頻繁なアクセスまたは不定期のアクセスに対して、誤検知アラートが生成されないことを確実にするために、通常なら不審であるように見える正常なアクティビティパターンを学習することもできる。ＲＮＮは、パターンからの逸脱を不審なものとして、より正確にフラグを立てることができるように、それらのパターンを非常に良く認識することができる。ＲＮＮは、多数の特徴を同時に分析することもでき、したがって、データソースの特徴のセットを分析のために一緒に組み合わせることができる。ＲＮＮは監視なしの設備能力で利用できるので、ネットワークはデータに適応できる。これは、アクセスパターンの変化に適応し、通常なら検出されない可能性のある様々な種類の攻撃を特定するのに役立ち得る。

【００２８】

後続のアクティビティが検出されると、その情報を分析のために分類器サービス３０２に送り込むことができる。アクティビティデータをＲＮＮで処理して、アクティビティのいずれかが予想された行動から外れているかどうかを、不審であるとラベル付けされるよ

うな方法で、識別することができる。いくつかの実施形態では、予想された行動から逸脱した場合に、アクティビティが不審であると判定されるための様々な閾値、値、または範囲があり得、一方、他の実施形態では、ＲＮＮは、他の同様の選択肢の中でも特に、変動分を予想し、こうした種類のアクティビティのみを不審であるとしてフラグを立てるように訓練することができる。また一方、特定の期間での使用が不審なように見えるが、別の時間帯では不審に見えない場合があり得る。例えば、ユーザは通常、特定の文書に１時間に１０回アクセスするが、通常は５分間に１０回、その文書にアクセスすることはない。５分間の使用が不審な場合であっても、必ずしも長期間の使用が不審であるとは限らない。したがって、様々な実施形態によるアプローチは、カルマンフィルタまたはそのような他のアルゴリズムを利用することなどにより、ＲＮＮの結果を平滑化しようと試みてもよい。カルマンフィルタは、ノイズ及び他の不正確さを含み得る経時的に観測された測定のセットに基づき、線形２次推定を生成するのに使用されて、単一期間のみに基づき得る、より正確な推定を生成する。カルマンフィルタは、他にも同様の選択肢はあるが特に、ユーザ行動を予測するとき、及び特定のアクティビティが不審なものか、それとも予測された行動の許容範囲外であるかを判定するときに使用できる。一例では、カルマンフィルタは、複数の期間にわたって、ダウンロードした文書の数、またはＡＰＩ呼出しの数など、特定ユーザのアクティビティの時系列を取得する。多少の訓練をすれば、異なる時系列にわたる結果をカルマンフィルタで平滑化して、普通ならＲＮＮのみで生成されるであろうよりも有効な予測を生成することができる。少なくとも一部の実施形態では、ＲＮＮ及びカルマンフィルタを同時に使用することができ、ＲＮＮは、カルマンフィルタによって平滑化される個々の特徴予測を生成する。その後、平滑化された結果を訓練された（高レベル）分類器アルゴリズムに提供することができ、最終的にこの分類器アルゴリズムは、アクティビティが、アラームを生成すべきか、またはそのような他のアクションを実行すべきかのような、不審なものであるのかどうかを判定することができる。

【００２９】

予測は、過去及び予想された行動、またはユーザ及びユーザのピアに基づいて、特定のステップまたは時点で行うこともできる。平滑化プロセスは信頼区間を提供することもでき、これにより、期待値からの合理的な逸脱を判定して、誤検知をさらに抑えるのに役立つ。いくつかの実施形態では、ユーザの予想されるアクティビティと実際のアクティビティとの間のエラーを累積し、時系列にわたるエラーの集計を分析して、不審なアクティビティを表し得る過度に大きなエラー値を有したユーザを特定することができる。したがって、アラートを、特定の不審なアクティビティか、またはユーザの全体に対して、個々に対して、もしくはそのユーザのピアに関して不審と思われるアクティビティに対して生成することができる。いくつかの実施形態では、ピアのグループによって経験され、したがってそのピアグループの個々のユーザに代わる不審なアクティビティとなる可能性が低い、予想しない変動分を説明するために、エラースコア総計がユーザのピアと比較され、ピアスコアから閾値を超えて逸脱したエラースコアが不審なものであると報告されてもよい。いくつかの実施形態のセキュリティコンソール３１２は、他の同様の選択肢の中でも特に、後続の分析のためにアラートまたは少なくともストア情報をアラートデータストア３１４に提供するために、不審なアクティビティについての通知を受けることができる。

【００３０】

図４は、図３のシステムの構成要素のサブセットを含むシステム４００を示しており、これは様々な実施形態に従ってピアグループを判定するのに使用することができる。すでに述べたように、少なくとも一部の実施形態では、ユーザのアクティビティは、ユーザのピアのアクティビティ、及びピアグループ内の他のユーザの行動に関して判定された不審な行動に少なくとも部分的に基づいて予測できる。これらのピアグループは、組織構造などの既知の情報に基づいて判定できるが、ピアは、アクセスされる文書の種類、そのアクセスのパターン及び頻度、ならびにそのような他の情報を学習することによって、経時的に判定することもできる。例として、分類器またはクローラは、Ｗｉｎｄｏｗｓ（登録商標）イベントデータ、ＡＷＳ　ＣｌｏｕｄＴｒａｉｌ、ＶＰＣフロー、Ａｐａｃｈｅ、及

びＩＩＳなどの複数のソースコード言語及びログ形式を識別できる場合がある。分類器またはクローラは、ＭｙＳＱＬ、ＭＳＳＱＬ、及びＭｏｎｇｏＤＢなどの様々なデータベースバックアップ形式、ならびにＳＥＣ文書やＦＤＡ届出書などの規定形式を識別することもできる場合がある。

【００３１】

いくつかの実施形態では、組織構造からのマッピング及び判定を、ＲＮＮへの初期入力として使用することができる。利用実態に即したアクティビティデータを分析するＲＮＮは、システム内に見られる行動の種類に関してピアであるユーザを判定することもできる。したがって、ユーザは、複数のピアグループに属す場合もあれば、経時的に学習される特定のピアグループ、及びいずれかの特定の組織構造または組織呼称の外部に属す場合もある。一部の実施形態では、ピアグループは重み付けされてもよく、他の実施形態では、任意のピアグループに対して不審なアクティビティがアラームを生成し得る一方で、他の実施形態では、アクティビティはアラームが生成される前に全てのピアグループに対して不審な（他の要因がない）必要がある。すでに述べたように、分類器サービス３０２の一部としてアクティビティデータに合わせて訓練を受けた分類器は、経時的な観察された行動に基づいてピアグループを判定し、更新することができる。アクティビティの類似性により、特定のユーザ４０２を、ピア４０４と共に第１のピアグループにグループ化するが、実質的に異なる行動のアクティビティパターンを持つ別個のピアグループのピア４０８とは関連付けないようにすることができる。ピアグループの数は、制限される場合もあれば無制限の場合もあり、これは、判定の精度に影響を与える可能性がある。ただし、比較のために確実に安定したアクセスパターンを得するためには、グループ内に少なくとも最小数のユーザが必要になる場合がある。さらに、特にユーザが無制限の数のグループに属している場合に、多数のピアグループは、潜在的に過剰なリソース使用を引き起こす可能性がある。

【００３２】

評価されるアクティビティパターンは、少なくとも一部の実施形態では、アクセスされる文書とアクセス数とに限定されず、アクセスのパスや種類などの情報を含むこともできる。例えば、読取りアクセスと書込みアクセスとを区別することができる。さらに、特定のリソース、またはＩＰアドレス、またはアドレス範囲からの呼出しも分析できる。少なくとも一部の実施形態では、ＲＮＮは、アクティビティの追加の態様または他の態様を考慮して調整することができ、場合によっては、ＲＮＮは、予想されるアクセスまたはアクティビティの種類を表し得るアクティビティに関する情報を学習することが可能とされる。少なくとも一部の実施形態では、これらの特徴のそれぞれの信頼レベルを個別に調整することもでき、その結果、特定のＩＰアドレスまたは地理的領域からの要求の要件は、ユーザが通常はアクセスしないような文書の種類以上に変化する可能性がある。これにより、このアクティビティが異常である可能性があり、購入がユーザ基盤全体で頻繁に発生する可能性があり、さもなければ誤検出のアラームが多数発生する可能性があるときに、ユーザはアラートを生成することなく、少なくとも特定の範囲内でＩＰアドレスを変更できる。ユーザは、特定の特徴に対して生成されるアラートの数を調節するために、個々の特徴の信頼値または閾値を調節することができる。したがって、ユーザが実際には問題のない特定の種類のアラートを、あまりにも多く受け取る場合には、ユーザは、その特定の特徴についての極端な逸脱のみがアラームを生成するように、閾値または信頼水準を調節することができる。

【００３３】

いくつかの実施形態では、文書をバケットにグループ化することができ、それによって、重要度及びリスク値を、様々なバケットに割り当てることができる。たとえば、人事（ＨＲ）文書を、あるバケットにグループ化してもよく、一方、医療記録を別のバケットにグループ化してもよい。このグループ化は、オフラインでかつ手動で実行することができ、またはグループ化は、他の選択肢や組合せの中でも特に、経時的に学習させることができる。そのようなアプローチにより、バケット内の全ての文書に、同様のリスクまたは重

要度の値が割り当てられるようにすることができるが、それぞれの適切なリスクまたは重要度のスコアを個別に判定することは困難であり得る。いくつかの実施形態では、バケットスコアは、各文書内に含まれる高スコアの情報を用いて個々の文書スコアを判定することができるため、その中に含まれる各文書の最小リスクスコアとすることができる。少なくとも一部の実施形態では、文書に割り当てられたリスクスコアは、文書内のいずれかの要素について判定された最高のリスクスコアに等しい。例えば、リスクスコアは、１（低リスク）から１０（非常に高リスク）の間で割り当てることができる。ＨＲバケット内のＨＲ文書のリスクスコアは５であるが、特定の文書にリスクスコア８の社会保障番号が含まれている場合は、その特定の文書のスコアは８になる。そして、その文書に５つの社会保障番号が含まれ、それぞれのリスクスコアが８である場合は、その例の文書のリスクスコアは引き続き８になる。いくつかの実施形態では、リスクスコアは、他の同様の選択肢の中でも特に、多くの社会保障番号を有する文書が、単一のリスクスコアを含む文書よりも高いリスクスコアを有するように集計され得るか、または重み付けされ得る。すでに述べたように、リスクスコアを使用して、不審なアクティビティに対して実行するアクションを判定できる。リスクスコアに対して実行されるアクションは、顧客が変更したり、顧客からのフィードバックに基づいて経時的に適合させたりすることもできる。いくつかの実施形態では、最初はリスク分析アルゴリズムの出力に対応することができるが、その後は顧客からのフィードバックと重要性に関するそのような他の情報とに基づき更新することができる特徴の複合セットを受け入れるランダムフォレストリグレッサを使用することができる。

【００３４】

顧客は、特定のリスクスコアに対するアクションを設定するだけでなく、他の様々な閾値またはトリガを設定し、または調整することもできる。例えば、ユーザが、通常アクセスするトピックとは異なるトピックを含む文書にアクセスしているときに、不審なアクティビティを判定することができる。顧客は、アラートまたは同様のアクションが実行される前に許可されるべき差異の水準を指定することができる。例えば、トピック間の距離を計算して、２つのトピック間に関連する差異を生成することができ、顧客は、アラームが生成される前に満たす必要のある最小の差異を指定できる。顧客は、異なる範囲に対して異なるアクションを指定することもできる。例えば、第１の閾値よりも小さい差異は無視されるが、第１の閾値と第２の閾値との間の差異はログに記録され、第２の閾値を超えるトピック間の差異に対してのみアラームが生成される。いくつかの実施形態では、自然言語理解（ＮＬＵ）を使用して、トピック及び概念、またはそれらの概念に関連する単語を判定でき、これをベクトル空間にベクトル化してトピックを組み立て、ベクトル空間でのそれらの距離を判定することができる。ベクトル及び空間は、他にも同様の選択肢があるが特に、例えば、線形判別分析（ＬＤＡ）または主成分分析（ＰＣＡ）を用いて生成できる。

【００３５】

したがって、様々な実施形態によるＤＬＰサービスは、データの不注意な露出、インサイダー脅威、または標的型攻撃などのビジネスへのリスクを示唆する機密データに関連するユーザ、アプリケーション、及びサービスアカウントのアクティビティを分析することができる。そのようなサービスは、異常なＩＰアドレスから大量の機密コンテンツを列挙してダウンロードする侵害されたユーザアカウントや、または通常この種の機密コンテンツにアクセスしないユーザアカウントによる大量のソースコードのダウンロードなどの不審なアクティビティを警告することができる。コンプライアンスに焦点を当てた例としては、個人を特定できる情報、知的財産、法律、または財務データを含むファイルなど、公的に、または会社全体で共有されている大量のハイリスク文書の検出が含まれる。さらに、顧客はまた、顧客用ダッシュボードを使用して、機密コンテンツにアクセスする必要があるサードパーティ製アプリケーションをホワイトリスト及びブラックリストに登録するなど、独自のアラート及びポリシ定義を定義することができる。

【００３６】

いくつかの実施形態では、１つ以上のトピックモデルを用いて、コンテンツが作成及び／または格納されるときに、既存コンテンツ及び新規コンテンツの両方を自動的に発見、分類、及びラベル付けすることによって、自動化されたコンテンツ分類及びラベル付けを提供することができる。このテーマスライシング機能は、潜在ディリクレ配分法（ＬＤＡ）、名前付きエンティティ抽出、文書の類似性、及びクラスタリングを含むトピックモデリングからの要素を利用して、既知の文書テンプレートと一致しないコンテンツについて人間が理解できる意味とビジネス価値とを推測することができる。すでに述べたように、文書の類似性を利用して、同じトピックを扱う可能性のある異なるファイルタイプ間の類似性を確実に評価することができる。この機能は、ＬＤＡトピック空間、ｄｏｃ２ｖｅｃ、またはＴＦ－ＩＤＦバッグオブワーズ空間からの文書ベクトルを利用できる。この機能は、ファイルの種類、ファイルの所有者、ファイルが外部で共有されているかどうかに関する情報、及びファイルの可視性レベルなどを含み得る文書メタデータの特徴を利用することもできる。これらの異なる「類似性のタイプ」は、異なるタイプが最終的な類似性スコアに異なる影響を与えるように、加重平均を使用するなどによって一緒に組み合わせることができる。

【００３７】

様々な実施形態に従って使用される異常検出サービスまたは分類器は、生のアクティビティイベント記録から抽出された情報に基づいてその状態を更新することができ、その後、様々な独立したデータセットを調べることによって、及びアラートを生成し、これらのデータセットにわたる異常で危険なアクティビティが観察された場合にアラートが作成された理由の説明を生成することによって、ユーザアカウント及びシステムアカウントに関連付けられた「リスクレベル」に関するクエリに答えることができる。利用される異常検出アルゴリズムには、カルマンフィルタと長期短期記憶（ＬＳＴＭ）再帰型ニューラルネットワーク（ＲＮＮ）とが含まれ得、これらは、ユーザの一時的なアクセスパターンに基づいて異常を識別するのに効果的であることが証明されている。さらに、従来のブラックボックス行動分類に対する洞察を提供する統計的手法を使用して、検出された異常の説明を提供する「説明する」機能を提供することができる。このような異常検出フレームワークは、自身を継続的に訓練することができ、シミュレートされた攻撃シナリオを入力イベントストリームに注入することにより、適合度関数を利用して自身の性能を継続的に改善することができる。

【００３８】

図５は、様々な実施形態に従って利用することができる１つ以上の割り当てられたリソースインスタンスを使用して、イベントのために登録された関数を処理するためのプロセス４００の例を示す。本明細書で説明するこのプロセス及び他のプロセスについては、別段の指示が無い限り、様々な実施形態の範囲内で、類似もしくは代替の順序で、または並行して、追加のステップ、代替のステップ、またはより少ないステップを実行できることを理解されたい。この例では、トピックラベル及びリスクスコア基準の初期セットが判定される（５０２）。これらには、例えば、他にも同様の選択肢はあるが特に、特定の顧客が関心を持つ特定のトピック、及び特定の文書から検出され得る特定の要素に割り当てるべきリスクスコアが含まれ得る。これらのトピックに従って分類され、リスクスコアを割り当てられた文書の初期セットを判定し（５０４）、訓練データとして使用することができる。初期訓練データを用いて、トピックモデル及びリスクスコアに対するランダムフォレストリグレッサを訓練することができる（５０６）。クローラ、またはそのような他のシステムもしくはサービスはまた、様々なリポジトリまたは他の格納場所をクロールして（５０８）、データ損失防止サービスの顧客である可能性のある組織のために格納され、アクセスが可能な文書を判定することができる。クローラ、またはクローラと連携するサービスは、リスクスコアや他のそのような値とともに、１つ以上のトピックを各文書（またはデータオブジェクトなど）に割り当てることができる（５１０）。顧客または他の権限を付与されたエンティティは、いくつかの実施形態では、意図されたトピックの知識または文書の実際のリスクに少なくとも部分的に基づいて、これらの判定を無効にし、また

は更新する能力を持ち得る。トピックモデル及びリグレッサは、組織の更新された文書または新たに格納された文書のデータなど、追加の文書データを使用して、さらに訓練を続けることができる（５１２）。このサービスは、組織の文書のコーパスに対する報告及び他の種類の可視性を有効にすることができ（５１４）、それによって組織は、利用可能な文書の種類及び関連するリスク、ならびにアクセスのパターン、識別されたトピックなどの潜在的な他の情報を判定することができる。このサービスはまた、リポジトリのクロールを（定期的な間隔などで）続行して、組織で利用可能な新規または変更された文書を判定し（５１６）、それらの文書のスコアを分類し生成したり、最新の利用可能な文書データを組み込むようにモデルをさらに訓練したりすることができる。

【００３９】

図６は、様々な実施形態に従って利用することができる異常なアクティビティを識別するためのプロセス６００の例を示す。この例では、組織の文書、データ、及び他のそのようなオブジェクトに関して、ユーザのアクティビティを監視できる（６０２）。すでに述べたように、様々な実施形態の範囲内で、全てのユーザもしくはユーザのサブセットのアクティビティ、またはそのアクティビティのサブセットを監視することができる。アクティビティデータを、トピックモデルを使用して処理し（６０４）、ユーザに適切なピアグループを判定することができる。すでに述べたように、これは、訓練されたＲＮＮまたは分類器サービスを使用して判定することができ、他にも同様の選択肢はあるが特に、類似の履歴アクセスパターン及び／または予測アクセスパターンを示すピアグループを判定する。ユーザのアクティビティは、分類器サービスを使用して処理し（６０６）、ユーザの将来のアクティビティを予測することができる。本明細書の他の箇所でより詳細に説明するように、これには、ＲＮＮを使用して生データまたは要約データを処理し、予測を生成することが含まれ、その後、カルマンフィルタまたはそのような他のアルゴリズムを使用して平滑化することができる。その後、平滑化された結果を高レベル分類器に送り込み、アクティビティが不審であるか否か、またはセキュリティアラートを生成するなどのアクションを起こすべきかどうかを判定できる。ユーザの最近のアクセスまたはアクティビティデータを、顧客または組織用に格納された特定の文書に関して受信することができる（６０８）。アクセスまたはアクティビティのデータを、分類器サービス（ＲＮＮ及びカルマンフィルタを含む）を使用して処理し（６１０）、アクティビティに関する何かが異常であるかどうか、少なくとも許容範囲を超える逸脱があるかどうかを判定できる。アクティビティが異常でないと判定（６１２）された場合、プロセスを継続することができる。また一方、アクティビティが異常であると判定された場合は、異常なアクセス（及びその他の要因）のリスクスコアを判定することができ（６１４）、これを特定のアクションを実行するための様々なルール、基準、または閾値と比較することができる。リスクスコアが指定された閾値を超えるなど、異常行動のリスクスコアがアラートを必要とすることが判定（６１６）された場合、セキュリティチームに対してアラートを生成できる。本明細書の他の箇所で説明及び示唆されるように、他の様々なアクションを行うことができる。アクティビティがアラームを必要としない場合は、異常行動のイベントデータを記録し、アクティビティの監視を続けるなど、別のアクションを実行できる。ネットワークをさらに訓練するために、任意のアクティビティデータをＲＮＮにフィードバックすることもできる。

【００４０】

図７は、図６に関して説明したアクセスデータを処理するために使用できる別のプロセス７００の例を示す。この例では、前述の監視プロセスの一部として、ユーザアクティビティが検出される（７０２）。アクティビティが異常であるかどうかを適切に評価するために、ユーザの過去のアクティビティとユーザのピアグループのアクティビティとの両方を、少なくとも最近の期間にわたって判定することができる（７０４）。次いでアクティビティデータは、例えば、再帰型ニューラルネットワーク（または他のニューラルネットワーク分類器）を使用して処理し、アクティビティが異常であるかどうか、または別の方法で、予想されるユーザアクティビティ及び／またはピアアクティビティから逸脱してい

るかどうかを判定できる（７０６）。少なくとも一部の実施形態では、複数の期間にわたってデータを分析するカルマンフィルタを使用して、ＲＮＮの結果を平滑化することができる（７０８）。この平滑化された結果は、教師なし分類器及び／または半訓練分類器を用いて処理し、異常の説明を試みることができる（７１０）。分類器は、異常の理由を統計的に判定し、異常の範囲を判定するために使用できるフィードバックを提供し、さらに分類器またはＲＮＮを訓練しようと試みることができる。次に、提供された説明に少なくとも部分的に基づいて、適切なアクションを判定することができる（７１２）。すでに述べたように、アクションには、他にも同様の選択肢があるが特に、ユーザインタフェース、メッセージングサービス、またはその他の機構を使用したセキュリティチーム用のアラームの生成が含まれ得る。

【００４１】

図８は、様々な実施形態の態様を実装するために利用することができるコンピューティングデバイス７００の例の基本構成要素のセットを例示する。この例では、本デバイスは、メモリデバイスまたはメモリ要素８０４に格納することができる命令を実行する少なくとも１つのプロセッサ８０２を含む。当業者には明らかなように、本デバイスは、少なくとも１つのプロセッサ８０２によって実行されるプログラム命令のための第１のデータ記憶装置など、多くのタイプのメモリ、データ記憶装置、またはコンピュータ可読媒体を含むことができ、画像またはデータに対して同一または別個の記憶装置を使用してもよく、他のデバイスと情報を共有するために着脱可能のメモリを利用することができ、他のデバイスと共有するために任意数の通信アプローチを利用することができる。デバイスは、タッチスクリーン、電子インク（ｅインク）、有機発光ダイオード（ＯＬＥＤ）、または液晶ディスプレイ（ＬＣＤ）など、少なくとも１つのタイプのディスプレイ要素８０６を含んでもよいが、サーバなどのデバイスは、光及びデータ伝送のシステムを通じてなど、他の手段を介して情報を搬送してもよい。デバイスは典型的には、少なくとも１つのネットワークを通じた通信を可能にするポート、ネットワークインタフェースカード、または無線送受信機など、１つ以上のネットワーキング構成要素８０８を含む。デバイスは、ユーザから従来の入力を受信することができる少なくとも１つの入力デバイス８１０を含むことができる。この従来の入力は、例えば、プッシュボタン、タッチパッド、タッチスクリーン、ホイール、ジョイスティック、キーボード、マウス、トラックボール、キーパッド、またはいずれかの他のそのようなデバイスもしくは要素を含むことができ、それによって、ユーザは、デバイスにコマンドを入力することができる。いくつかの実施形態では、これらのＩ／Ｏデバイスは、ワイヤレス赤外線もしくはブルートゥース（登録商標）、または他のリンクによっても同じようにして接続され得る。また一方、いくつかの実施形態では、このようなデバイスはボタンをまったく含まず、ユーザがデバイスと接触する必要なしにデバイスを制御できるように、視覚コマンド及び音声コマンドの組合せによってのみで制御されてもよい。

【００４２】

本開示の一態様では、コンピュータ実施方法は、訓練用文書のセットを使用してトピックモデルを訓練することであって、セットの各訓練用文書が、少なくとも１つの識別されたトピックと割り当てられたリスクスコアとを有する、トピックモデルを訓練すること、訓練用文書のセットを使用して、ランダムフォレストリグレッサを訓練すること、電子リソース環境全体にわたってエンティティ用に格納されている複数の文書をクロールし、複数の文書にインデックスを付けること、少なくともトピックモデルを使用して、複数の文書の各文書の１つ以上のトピックを判定すること、少なくともランダムフォレストリグレッサを使用して、複数の文書の各文書のリスクスコアを判定すること、電子リソース環境内の複数の文書に関する履歴アクティビティを使用して、再帰型ニューラルネットワークを訓練すること、再帰型ニューラルネットワークを使用して、少なくとも１つの決められた期間にわたって複数の文書に関して指定されたユーザの予想されるアクティビティを判定すること、複数の文書のうちの少なくとも指定された文書に関するユーザアクティビティを検出することであって、ユーザアクティビティが指定されたユーザに関連付けられる

、ユーザアクティビティを検出すること、再帰型ニューラルネットワークを使用してアクティビティを処理し、ユーザアクティビティが予想されるタイプのアクティビティから逸脱しているかどうかを判定することであって、判定がさらに、指定された文書に対して判定された少なくとも１つのトピックに少なくとも部分的に基づいている、逸脱を判定すること、及びユーザアクティビティが、予想されるアクティビティから許容できないほど逸脱すると判定され、ユーザアクティビティまたは指定された文書の少なくとも１つに対するリスクスコアが、少なくともアラート閾値を満たしている場合に、セキュリティアラートを生成することを含む。

【００４３】

本開示の他の態様では、コンピュータ実施方法は、再帰型ニューラルネットワークによる処理の結果を、カルマンフィルタを用いて処理して、複数の期間にわたるユーザアクティビティを分析し、ユーザアクティビティが、予想されるアクティビティから許容量を超えて逸脱しているかどうかをさらに判定することをさらに含む。他の態様では、コンピュータ実施方法は、指定されたユーザを含むピアグループ内のピアのピアアクティビティとユーザアクティビティとをさらに比較すること、及びピアアクティビティに関するユーザアクティビティの第２の逸脱にさらに基づいて、ユーザアクティビティが予想されるアクティビティから許容できないほど逸脱しているかどうかを判定することを含む。さらに他の態様では、コンピュータ実施方法は、電子リソース環境の複数の文書及び複数のユーザに関して監視されたアクティビティデータを使用して訓練された教師なし分類器を使用して、指定されたユーザを含むピアグループを判定することを含む。

【００４４】

本開示の別の態様では、コンピュータ実施方法は、電子リソース環境で、エンティティのために格納された複数の文書に関する履歴アクティビティを使用してニューラルネットワークを訓練すること、再帰型ニューラルネットワークを使用して、少なくとも１つの決められた期間にわたって複数の文書に関して指定されたユーザの予想されるアクティビティを判定すること、複数の文書のうちの少なくとも指定された文書に関するユーザアクティビティを、少なくとも決められた期間にわたって検出することであって、ユーザアクティビティが指定されたユーザに関連付けられる、ユーザアクティビティを検出すること、ユーザアクティビティを、ニューラルネットワークを使用して処理して、ユーザアクティビティが、予想されるタイプのアクティビティから逸脱しているかどうかを判定すること、及びユーザアクティビティが予想されるタイプのアクティビティから許容できないほど逸脱すると判断された場合に、決められたアクションを実行することを含む。

【００４５】

本開示の別の態様では、コンピュータ実施方法は、判定されたリスクスコアに少なくとも部分的に基づいて、実行すべきアクションを判定することであって、少なくとも１つのリスク閾値が実行される可能性のあるアクションに関連付けられている、実行すべきアクションを判定することをさらに含む。本コンピュータ実施方法のアクションは、それぞれがリスクスコアの範囲にそれぞれ関連付けられた複数の可能なアクションの１つであり、可能なアクションが、セキュリティアラートの生成、異常なアクティビティデータの記録、または指定されたユーザもしくは指定された文書の少なくとも１つに関連付けられたアクセス権の調節のうちの少なくとも１つを含む。本コンピュータ実施方法は、ニューラルネットワークによる処理の結果を、カルマンフィルタを用いて処理して、複数の期間にわたるユーザアクティビティを分析し、ユーザアクティビティが、予想されるアクティビティから許容できないほど逸脱しているかどうかをさらに判定することをさらに含む。本コンピュータ実施方法は、訓練された分類器を使用してカルマンフィルタ処理の結果を処理し、ユーザアクティビティが予想されるアクティビティから許容できないほど逸脱しているかどうかを判定することを更に含む。本コンピュータ実施方法は、指定されたユーザを含むピアグループ内のピアのピアアクティビティとユーザアクティビティとをさらに比較すること、及びピアアクティビティに関するユーザアクティビティの第２の逸脱に少なくとも部分的に基づいて、ユーザアクティビティが予想されるユーザアクティビティから許

容できないほど逸脱しているかどうかを判定することをさらに含む。本コンピュータ実施方法は、電子リソース環境の複数の文書及び複数のユーザに関して監視されたアクティビティデータを使用して訓練された教師なし分類器を使用して、指定されたユーザを含むピアグループを判定することをさらに含む。本コンピュータ実施方法は、指定された文書に関連する少なくとも１つのトピックを判定すること、少なくとも１つのトピックを、予想されるアクティビティに関連するトピックと比較すること、及び少なくとも１つのトピックと予想されるアクティビティに関連するトピックとの間のトピックベクトル空間におけるトピック距離に少なくとも部分的に基づいて、ユーザアクティビティが、予想されるユーザアクティビティから許容できないほど逸脱するかどうかを判定することをさらに含む。本コンピュータ実施方法は、アクセスの種類、アクセスの頻度、一定期間のアクセス試行の合計数、アクセスの送信元アドレス、アクセスされたトピック、アクセスされた文書の種類、アクセスの場所、アクセスの日もしくは時間、またはアクセスを取得するために使用されるアプリケーションプログラミングインタフェース（ＡＰＩ）呼出しのうちの少なくとも１つが含まれる、ユーザアクティビティを開示する。

【００４６】

本開示の別の態様では、システムは、少なくとも１つのプロセッサと、少なくとも１つのプロセッサによって実行されるとき、システムに、訓練用文書のセットを使用してトピックモデルを訓練することであって、セットの各訓練用文書が、少なくとも１つの識別されたトピックと割り当てられたリスクスコアとを有する、トピックモデルを訓練すること、電子リソース環境全体にわたってエンティティ用に格納されている複数の文書をクロールし、複数の文書にインデックスを付けること、少なくともトピックモデルを使用して、複数の文書の各文書の１つ以上のトピックを判定すること、複数の文書の各文書のリスクスコアを判定すること、及びエンティティに関連付けられた許可ユーザによるアクセスのためのセキュリティ情報を提供することであって、セキュリティ情報には、識別されたトピックの情報と、エンティティ用に格納されている複数の文書のリスクスコアとが含まれる、セキュリティ情報を提供することを行わせる命令を含むメモリとを備える。本システムは、命令が、実行されると、システムにさらに、電子リソース環境のエンティティ用に格納された新たな文書または文書の変更のうちの少なくとも１つに対応する更新された文書データを検出すること、及び更新された文書データのインスタンス毎にトピックモデルをさらに訓練することを行わせることを開示する。本システムは、命令が、実行されると、システムにさらに、自然言語理解（ＮＬＵ）を利用して複数の文書を分析し、複数の文書の各文書に関連付けられた１つ以上のトピックを判定することを開示する。本システムは、命令が、実行されると、システムにさらに、複数の文書に含まれる複数の要素を判定することであって、複数の要素の各要素が、エンティティに潜在的なセキュリティリスクをもたらす、複数の要素を判定すること、複数の要素の各要素にそれぞれリスクスコアを割り当てること、及び複数の文書のうちの指定された文書のリスクスコアを、指定された文書に関連付けられた要素の１つに対する最高のそれぞれのリスクスコアに少なくとも部分的に基づいて、判定することを行わせることを開示する。本システムは、命令が、実行されると、システムにさらに、電子リソース環境のエンティティ用に格納された新たな文書を検出すること、新たな文書に関連する１つ以上のトピックを判定すること、新たな文書の１つ以上のトピックを有する他の文書に関連付けられた文書バケットに新たな文書を割り当てること、及び文書バケットのバケットリスクスコアに少なくとも部分的に基づいて、新たな文書にリスクスコアを割り当てることを行わせることを開示する。本システムは、命令が、実行されると、システムにさらに、訓練されたトピックモデルを使用して、複数の文書を処理することにより、新しいトピックを学習させることを行わせることを開示する。本システムは、命令が、実行されると、システムにさらに、エンティティの業界に特有であり、あらかじめトピックに関連付けられたコンテンツを含まない種類の文書を、トピックモデルによって分類できるようにすることを行わせることを開示する。

【００４７】

既に述べたように、説明した実施形態に従って、様々な環境で異なるアプローチを実施

することができる。認識されるように、本明細書で提示されるいくつかの例の説明を目的としてウェブに基づく環境が使用されるが、様々な実施形態を実施するために、必要に応じて異なる環境を使用してもよい。システムは、電子クライアントデバイスを含み、電子クライアントデバイスは、適切なネットワークを通じて要求、メッセージ、または情報を送信及び受信し、デバイスのユーザに情報を再度搬送するように動作可能ないずれかの適切なデバイスを含むことができる。そのようなクライアントデバイスの例には、パーソナルコンピュータ、携帯電話、ハンドヘルドメッセージングデバイス、ラップトップコンピュータ、セットトップボックス、携帯情報端末、及び電子ブックリーダなどが含まれる。ネットワークには、イントラネット、インターネット、セルラネットワーク、ローカルエリアネットワーク、もしくは任意の他のそのようなネットワーク、またはそれらの組合せを含む、任意の適切なネットワークが含まれ得る。そのようなシステムに使用される構成要素は、選択されるネットワーク及び／または環境の種類に少なくとも部分的に依存し得る。そのようなネットワークを介して通信するためのプロトコル及び構成要素は周知であり、本明細書では詳細に説明しない。ネットワークを介した通信は、有線または無線接続、及びそれらの組合せを介して可能にされてもよい。この例では、ネットワークは、要求を受信し、それに応答してコンテンツをサービスするためのウェブサーバを含む環境のように、インターネットを含むが、他のネットワークについて、当業者に明らかなように、類似の目的をサービスする代替的なデバイスが使用されてもよい。

【００４８】

例示的な環境は、少なくとも１つのアプリケーションサーバ及びデータストアを含む。いくつかのアプリケーションサーバ、層もしくは他の要素、処理、または構成要素が存在することができ、それらは、つながれ、または他に構成されてもよく、適切なデータストアからデータを取得することなどのタスクを実行するようにやりとりすることができることが理解されるべきである。本明細書で使用される場合、「データストア」という用語は、データを記憶し、データにアクセスし、及びデータを取り出す能力を有するいずれかのデバイスまたはデバイスの組合せを指し、いずれかのデバイスまたはデバイスの組合せは、いずれかの標準、分散、またはクラスタ化された環境内の、データサーバ、データベース、データ記憶装置、及びデータ記憶媒体のいずれかの組合せ及びいずれかの数のそれらを含んでもよい。アプリケーションサーバは、クライアントデバイスに対して１つ以上のアプリケーションの態様を実行するために必要に応じてデータストアとやりとりし、アプリケーションについてのデータアクセス及びビジネスロジックの大多数を取り扱うためのいずれかの適切なハードウェア及びソフトウェアを含むことができる。アプリケーションサーバは、データストアと連携してアクセス制御サービスを提供し、ユーザに転送されることになるテキスト、グラフィック、音声、及び／またはビデオ等のコンテンツを生成することができ、コンテンツは、この例では、ＨＴＭＬ、ＸＭＬ、または別の適切な構造化言語の形式でウェブサーバによってユーザにサービスされ得る。全ての要求及び応答と共に、クライアントデバイスとアプリケーションサーバとの間のコンテンツの配信を取り扱うことは、ウェブサーバによって取り扱われ得る。本明細書で考察される構造化コードを、本明細書で他に考察されるいずれかの適切なデバイスまたはホストマシン上で実行することができるので、ウェブ及びアプリケーションサーバは必要とされず、これらは例示的な構成要素にすぎないことが理解されるべきである。

【００４９】

データストアは、いくつかの別個のデータテーブル、データベース、または特定の態様に関連するデータを記憶するための他のデータ記憶機構及び媒体を含むことができる。例えば、図示されているデータストアは、コンテンツ（例えば、制作データ）及びユーザ情報を保存するためのメカニズムを含み、これらは、制作側にコンテンツを提供するために使用されてもよい。データストアはまた、ログまたはセッションデータを記憶するための機構を含むとして示される。必要に応じて上記記載された機構のいずれか、またはデータストア内の追加の機構に記憶することができる、ページ画像情報及びアクセス権情報など、データストアに記憶される必要があることがある多くの他の態様が存在することができ

ることが理解されるべきである。データストアは、それと関連付けられたロジックを通じて、アプリケーションサーバから命令を受信し、それに応答して、データを取得、更新、または他に処理するように動作可能である。一例では、ユーザは、ある特定のタイプの項目についての検索要求を送信してもよい。この場合、データストアは、ユーザの識別を検証するために、ユーザ情報にアクセスしてもよく、そのタイプの項目に関する情報を取得するために、カタログ詳細情報にアクセスすることができる。ユーザデバイス上のブラウザを介してユーザが見ることが可能なウェブページ上の結果リストなどの情報が次いで、ユーザに返されてもよい。専用ページまたはブラウザのウインドウ内で、関心の特定の項目についての情報を見ることができる。

【００５０】

各々のサーバは典型的には、そのサーバの全体的な統治及び操作のための実行可能なプログラム命令を提供するオペレーティングシステムを含み、典型的には、サーバのプロセッサによって実行されるとき、サーバがその意図された機能を実行することを可能にする命令を記憶したコンピュータ可読媒体を含む。サーバのオペレーティングシステム及び汎用機能性についての適切な実施態様は、既知であり、または商業的に利用可能であり、特に、本明細書における開示を考慮して、当業者によって容易に実施される。

【００５１】

１つの実施形態における環境は、１つ以上のコンピュータネットワークまたは直接接続を使用して、通信リンクを介して相互接続された、いくつかのコンピュータシステム及び構成要素を利用した分散コンピューティング環境である。しかしながら、そのようなシステムは、例示されるよりも少ないまたは多くの数の構成要素を有するシステム内でも等しく良好に動作することができることが当業者によって認識されるであろう。よって、本明細書におけるシステムの記述は、本質的に例示的であり、開示の範囲を限定しないと見なされるべきである。

【００５２】

様々な実施形態は更に、幅広い種類の動作環境内で実施されてもよく、オペレーティング環境は、一部の場合では、いくつかのアプリケーションのいずれかを動作させるために使用することができる１つ以上のユーザコンピュータまたはコンピューティングデバイスを含むことができる。ユーザデバイスまたはクライアントデバイスは、標準オペレーティングシステムを実行するデスクトップコンピュータまたはノート型コンピュータ等の任意の数の汎用パーソナルコンピュータと、モバイルソフトウェアを実行し及びいくつかのネットワーキングプロトコル及びメッセージプロトコルをサポートすることが可能である、セルラデバイス、無線デバイス、及びハンドヘルドデバイスを含み得る。イベントまたはリクエストを生成できるデバイスは、ウェアラブルコンピュータ（例えば、スマートウォッチまたはスマートグラス）、ＶＲヘッドセット、モノのインターネット（ＩｏＴ）デバイス、音声コマンド認識システムなどを含むこともできる。そのようなシステムはまた、開発及びデータベース管理などの目的により、様々な商業的に利用可能なオペレーティングシステム及び他の既知のアプリケーションのいずれかを稼働させるいくつかのワークステーションを含むことができる。それらのデバイスはまた、ダミー端末、シンクライアント、ゲーミングシステム、及びネットワークを介して通信する能力を有する他のデバイスなどの他の電子デバイスを含むことができる。

【００５３】

ほとんどの実施形態は、ＴＣＰ／ＩＰ、ＦＴＰ、ＵＰｎＰ、ＮＦＳ、及びＣＩＦＳなどの様々な商業的に利用可能なプロトコルのいずれかを使用して通信をサポートする、当業者によく知られた少なくとも１つのネットワークを利用する。ネットワークは、例えば、ローカルエリアネットワーク、ワイドエリアネットワーク、仮想プライベートネットワーク、インターネット、イントラネット、エクストラネット、公衆交換電話網、赤外線ネットワーク、無線ネットワーク、及びそれらのいずれかの組合せとすることができる。

【００５４】

ウェブサーバを利用する実施形態では、ウェブサーバは、ＨＴＴＰサーバ、ＦＴＰサー

バ、ＣＧＩサーバ、データサーバ、Ｊａｖａ（登録商標）サーバ、及びビジネスアプリケーションサーバを含む、様々なサーバまたは中間階層アプリケーションのいずれかを稼働させることができる。サーバ（複数可）はまた、Ｊａｖａ（登録商標）、Ｃ、Ｃ＃、もしくはＣ＋＋などのいずれかのプログラミング言語、またはＰｅｒｌ、Ｐｙｔｈｏｎ、もしくはＴＣＬなどのいずれかのスクリプト言語、ならびにそれらの組合せで記述された１つ以上のスクリプトまたはプログラムとして実施することができる１つ以上のウェブアプリケーションを実行することによってなど、ユーザデバイスからの要求に応答して、プログラムまたはスクリプトを実行する能力を有してもよい。サーバ（複数可）はまた、Ｏｒａｃｌｅ（登録商標）、Ｍｉｃｒｏｓｏｆｔ（登録商標）、Ｓｙｂａｓｅ（登録商標）、及びＩＢＭ（登録商標）から商業的に利用可能なサーバ、ならびにＭｙＳＱＬ、Ｐｏｓｔｇｒｅｓ、ＳＱＬｉｔｅ、ＭｏｎｇｏＤＢ、及び構造化または非構造化データを記憶し、取り出し、及びアクセスする能力を有するいずれかの他のサーバなどのオープンソースサーバを含むがそれらに限定されない、データベースサーバを含んでもよい。データベースサーバは、テーブルベースサーバ、文書ベースサーバ、非構造化サーバ、関係サーバ、非関係サーバ、もしくはそれらの組合せ、及び／または他のデータベースサーバを含んでもよい。

【００５５】

環境は、上記考察された様々なデータストア、及び他のメモリ及び記憶媒体を含むことができる。それらは、コンピュータのうちの１つ以上にローカルな（及び／またはそれに存在する）、またはネットワークにわたってコンピュータのいずれかもしくは全てにリモートな記憶媒体など、様々な位置に存在することができる。実施形態の特定のセットでは、情報は当業者によく知られているストレージエリアネットワーク（ＳＡＮ）に存在してもよい。同様に、コンピュータ、サーバ、または他のネットワークデバイスにあるとする機能を実行するために必要なファイルは、必要に応じてローカル及び／またはリモートに格納することができる。システムがコンピュータ化されたデバイスを含む場合、各々のそのようなデバイスは、ハードウェア要素を含むことができ、ハードウェア要素は、バスを介して電気的に結合されてもよく、要素は、例えば、少なくとも１つの中央処理装置（ＣＰＵ）、少なくとも１つの入力デバイス（例えば、マウス、キーボード、コントローラ、タッチ感知表示要素、またはキーパッド）、及び少なくとも１つの出力デバイス（例えば、ディスプレイデバイス、プリンタ、またはスピーカ）を含む。このようなシステムはまた、ディスクドライブ、光学記憶デバイス、ならびに、ランダムアクセスメモリ（ＲＡＭ）または読み出し専用メモリ（ＲＯＭ）、ならびに取り外し可能記憶デバイス、メモリカード、フラッシュカード等のソリッドステート記憶デバイス等、１つ以上の記憶デバイスを含み得る。

【００５６】

そのようなデバイスはまた、上記説明されたコンピュータ可読記憶媒体リーダ、通信デバイス（例えば、モデム、ネットワークカード（無線または有線）、赤外線通信デバイス）、及びワーキングメモリを含むことができる。コンピュータ可読記憶媒体リーダは、リモート、ローカル、固定、及び／または着脱可能記憶装置を表すコンピュータ可読記憶媒体と共に、コンピュータ可読情報を一時的及び／または更に永続的に包含し、記憶し、伝送し、及び取り出すための記憶媒体と接続されてもよく、またはそれらを受信するように構成されてもよい。システム及び様々なデバイスはまた、典型的には、オペレーティングシステム及びクライアントアプリケーションまたはウェブブラウザなどのアプリケーションプログラムを含む、少なくとも１つのワーキングメモリデバイス内に位置するいくつかのソフトウェアアプリケーション、モジュール、サービス、または他の要素を含む。代替的な実施形態が上記説明された実施形態からの多数の変形形態を有してもよいことを認識されるべきである。例えば、カスタマイズされたハードウェアも使用されてもよく、及び／または特定の要素がハードウェア、ソフトウェア（アプレットなどのポータブルソフトウェアを含む）、もしくはその両方で実施されてもよい。さらに、ネットワーク入力／出力デバイスなどの他のコンピューティングデバイスへの接続を使用することができる。

【００５７】
コードまたはコードの一部を包含する記憶媒体及び他の非一時的コンピュータ可読媒体は、限定されないが、コンピュータ可読命令、データ構造、プログラムモジュール、または他のデータなどの情報の記憶のためのいずれかの方法または技術において実施された揮発性及び不揮発性、着脱可能及び着脱不能メディアなど、本分野において既知であり、または使用されるいずれかの適切な媒体を含むことができ、それらは、ＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ（登録商標）、フラッシュメモリもしくは他のメモリ技術、ＣＤ－ＲＯＭ、デジタル多用途ディスク（ＤＶＤ）もしくは他の光学式記憶装置、磁気カセット、磁気テープ、磁気ディスク記憶装置もしくは他の磁気記憶装置、または所望の情報を記憶するために使用することができ、システムデバイスによってアクセスすることができるいずれかの他の媒体を含む。本明細書で提供される開示及び教示に基づいて、当業者は、様々な実施形態を実施するための他の方式及び／または方法を認識するであろう。

【００５８】
したがって、明細書及び図面は、限定的な意味ではなく例示的であると見なされることになる。しかしながら、特許請求の範囲において示されるような発明のより広い趣旨及び範囲から逸脱することなく、それらに様々な修正及び変更が行われてもよいことが明白であろう。

以下に、本願の出願当初の特許請求の範囲に記載された発明を付記する。

［Ｃ１］
訓練用文書のセットを使用してトピックモデルを訓練することであって、前記セットの各訓練用文書が、少なくとも１つの識別されたトピックと割り当てられたリスクスコアとを有する、前記トピックモデルを訓練すること、
訓練用文書の前記セットを使用して、ランダムフォレストリグレッサを訓練すること、
電子リソース環境全体にわたってエンティティ用に格納されている複数の文書をクロールし、前記複数の文書にインデックスを付けること、
少なくとも前記トピックモデルを使用して、前記複数の文書の各文書の１つ以上のトピックを判定すること、
少なくとも前記ランダムフォレストリグレッサを使用して、前記複数の文書の各文書のリスクスコアを判定すること、
前記電子リソース環境内の前記複数の文書に関する履歴アクティビティを使用して、再帰型ニューラルネットワークを訓練すること、
前記再帰型ニューラルネットワークを使用して、少なくとも１つの決められた期間にわたって前記複数の文書に関して指定されたユーザの予想されるアクティビティを判定すること、
前記複数の文書のうちの少なくとも指定された文書に関するユーザアクティビティを検出することであって、前記ユーザアクティビティが前記指定されたユーザに関連付けられる、前記ユーザアクティビティを検出すること、
前記再帰型ニューラルネットワークを使用して前記アクティビティを処理し、前記ユーザアクティビティが前記予想されるタイプのアクティビティから逸脱しているかどうかを判定することであって、前記判定がさらに、前記指定された文書に対して判定された少なくとも１つのトピックに少なくとも部分的に基づいている、前記アクティビティを処理すること、及び
前記ユーザアクティビティが、前記予想されるアクティビティから許容できないほど逸脱すると判定され、前記ユーザアクティビティまたは前記指定された文書の少なくとも１つに対するリスクスコアが、少なくともアラート閾値を満たしている場合に、セキュリティアラートを生成すること
を含む、コンピュータ実施方法。

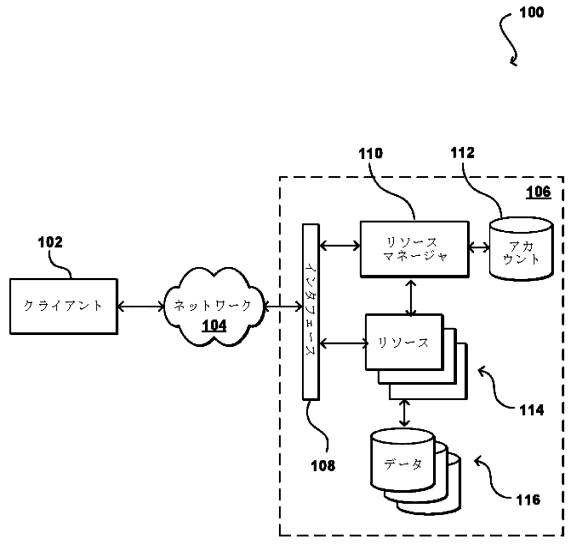
［Ｃ２］
前記再帰型ニューラルネットワークによる前記処理の結果を、カルマンフィルタを用いて処理して、複数の期間にわたる前記ユーザアクティビティを分析し、前記ユーザアクテ

ィビティが、前記予想されるアクティビティから許容量を超えて逸脱しているかどうかをさらに判定すること
をさらに含む、Ｃ１に記載のコンピュータ実施方法。
［Ｃ３］
前記指定されたユーザを含むピアグループ内のピアのピアアクティビティと前記ユーザアクティビティとをさらに比較すること、及び
前記ピアアクティビティに関する前記ユーザアクティビティの第２の逸脱にさらに基づいて、前記ユーザアクティビティが前記予想されるアクティビティから許容できないほど逸脱しているかどうかを判定すること
をさらに含む、Ｃ１に記載のコンピュータ実施方法。
［Ｃ４］
前記電子リソース環境の前記複数の文書及び複数のユーザに関して監視されたアクティビティデータを使用して訓練された教師なし分類器を使用して、前記指定されたユーザを含む前記ピアグループを判定すること
をさらに含む、Ｃ３に記載のコンピュータ実施方法。
［Ｃ５］
電子リソース環境で、エンティティのために格納された複数の文書に関する履歴アクティビティを使用してニューラルネットワークを訓練すること、
前記再帰型ニューラルネットワークを使用して、少なくとも１つの決められた期間にわたって前記複数の文書に関して指定されたユーザの予想されるアクティビティを判定すること、
前記複数の文書のうちの少なくとも指定された文書に関するユーザアクティビティを、少なくとも決められた期間にわたって検出することであって、前記ユーザアクティビティが前記指定されたユーザに関連付けられる、前記ユーザアクティビティを検出すること、
前記ユーザアクティビティを、前記ニューラルネットワークを使用して処理して、前記ユーザアクティビティが、前記予想されるタイプのアクティビティから逸脱しているかどうかを判定すること、及び
前記ユーザアクティビティが前記予想されるタイプのアクティビティから許容できないほど逸脱すると判断された場合に、決められたアクションを実行すること
を含むコンピュータ実施方法。
［Ｃ６］
判定されたリスクスコアに少なくとも部分的に基づいて、実行すべき前記アクションを判定することであって、少なくとも１つのリスク閾値が実行される可能性のあるアクションに関連付けられており、前記アクションは、それぞれがリスクスコアの範囲にそれぞれ関連付けられた複数の可能なアクションの１つであり、前記可能なアクションが、セキュリティアラートの生成、異常なアクティビティデータの記録、または前記指定されたユーザもしくは前記指定された文書の少なくとも１つに関連付けられたアクセス権の調節のうちの少なくとも１つを含む、前記アクションを判定すること
をさらに含む、Ｃ５に記載のコンピュータ実施方法。
［Ｃ７］
前記指定されたユーザを含むピアグループ内のピアのピアアクティビティと前記ユーザアクティビティとをさらに比較すること、
前記ピアアクティビティに関する前記ユーザアクティビティの第２の逸脱に少なくとも部分的に基づいて、前記ユーザアクティビティが前記予想されるユーザアクティビティから許容できないほど逸脱しているかどうかを判定すること、及び
前記電子リソース環境の前記複数の文書及び複数のユーザに関して監視されたアクティビティデータを使用して訓練された教師なし分類器を使用して、前記指定されたユーザを含む前記ピアグループを判定すること
をさらに含む、Ｃ５に記載のコンピュータ実施方法。
［Ｃ８］

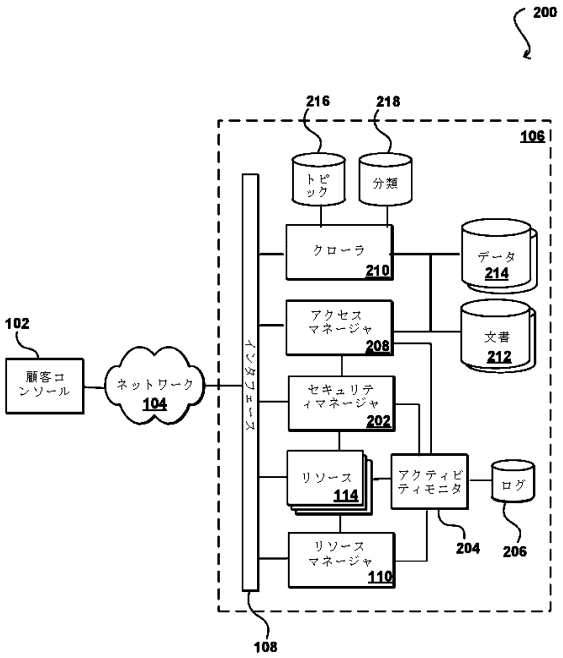
前記指定された文書に関連する少なくとも１つのトピックを判定すること、
前記少なくとも１つのトピックを、前記予想されるアクティビティに関連するトピックと比較すること、及び
前記少なくとも１つのトピックと前記予想されるアクティビティに関連する前記トピックとの間のトピックベクトル空間におけるトピック距離に少なくとも部分的に基づいて、前記ユーザアクティビティが、前記予想されるユーザアクティビティから許容できないほど逸脱するかどうかを判定すること
をさらに含む、Ｃ５に記載のコンピュータ実施方法。
［Ｃ９］
前記ユーザアクティビティには、アクセスの種類、アクセスの頻度、一定期間のアクセス試行の合計数、アクセスの送信元アドレス、アクセスされたトピック、アクセスされた文書の種類、アクセスの場所、前記アクセスの日もしくは時間、または前記アクセスを取得するために使用されるアプリケーションプログラミングインタフェース（ＡＰＩ）呼出しのうちの少なくとも１つが含まれる、Ｃ５に記載のコンピュータ実施方法。
［Ｃ１０］
システムであって、
少なくとも１つのプロセッサと、
前記少なくとも１つのプロセッサによって実行されるとき、前記システムに、
訓練用文書のセットを使用してトピックモデルを訓練することであって、前記セットの各訓練用文書が、少なくとも１つの識別されたトピックと割り当てられたリスクスコアとを有する、前記トピックモデルを訓練すること、
電子リソース環境全体にわたってエンティティ用に格納されている複数の文書をクロールし、前記複数の文書にインデックスを付けること、
少なくとも前記トピックモデルを使用して、前記複数の文書の各文書の１つ以上のトピックを判定すること、
前記複数の文書の各文書のリスクスコアを判定すること、及び
前記エンティティに関連付けられた許可ユーザによるアクセスのためのセキュリティ情報を提供することであって、前記セキュリティ情報には、前記識別されたトピックの情報と、前記エンティティ用に格納されている前記複数の文書のリスクスコアとが含まれる、前記セキュリティ情報を提供すること
を行わせる命令を含むメモリと
を備えた前記システム。
［Ｃ１１］
前記命令が、実行されると、前記システムにさらに、
前記電子リソース環境の前記エンティティ用に格納された新たな文書または文書の変更のうちの少なくとも１つに対応する更新された文書データを検出すること、及び
前記更新された文書データのインスタンス毎に前記トピックモデルをさらに訓練すること
を行わせる、Ｃ１０に記載のシステム。
［Ｃ１２］
前記命令が、実行されると、前記システムにさらに、
自然言語理解（ＮＬＵ）を利用して前記複数の文書を分析し、前記複数の文書の各文書に関連付けられた１つ以上のトピックを判定すること
を行わせる、Ｃ１０に記載のシステム。
［Ｃ１３］
前記命令が、実行されると、前記システムにさらに、
前記複数の文書に含まれる複数の要素を判定することであって、前記複数の要素の各要素が、前記エンティティに潜在的なセキュリティリスクをもたらす、前記複数の要素を判定すること、
前記複数の要素の各要素にそれぞれリスクスコアを割り当てること、及び

指定された文書に関連付けられた前記要素の１つに対する最高のそれぞれのリスクスコアに少なくとも部分的に基づいて、前記複数の文書のうちの前記指定された文書の前記リスクスコアを判定すること
を行わせる、Ｃ１０に記載のシステム。
［Ｃ１４］
前記命令が、実行されると、前記システムにさらに、
前記電子リソース環境の前記エンティティ用に格納された新たな文書を検出すること、
前記新たな文書に関連する１つ以上のトピックを判定すること、
前記新たな文書の前記１つ以上のトピックを有する他の文書に関連付けられた文書バケットに前記新たな文書を割り当てること、及び
前記文書バケットのバケットリスクスコアに少なくとも部分的に基づいて、前記新たな文書にリスクスコアを割り当てること
を行わせる、Ｃ１０に記載のシステム。
［Ｃ１５］
前記命令が、実行されると、前記システムにさらに、
前記訓練されたトピックモデルを使用して、前記複数の文書を処理することにより、新しいトピックを学習させること
を行わせる、Ｃ１０に記載のシステム。

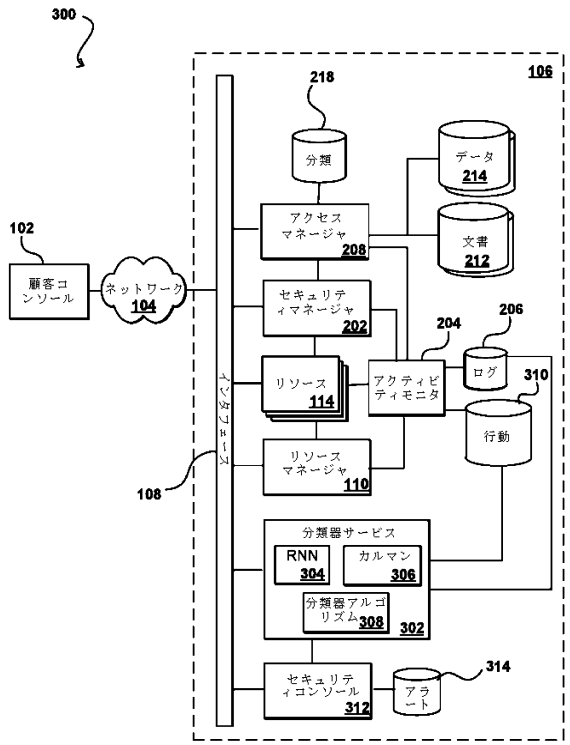
【図１】



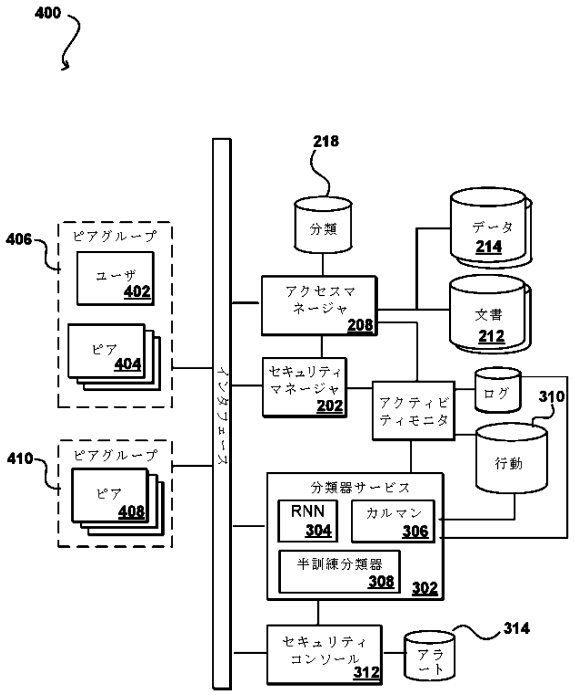
【図２】



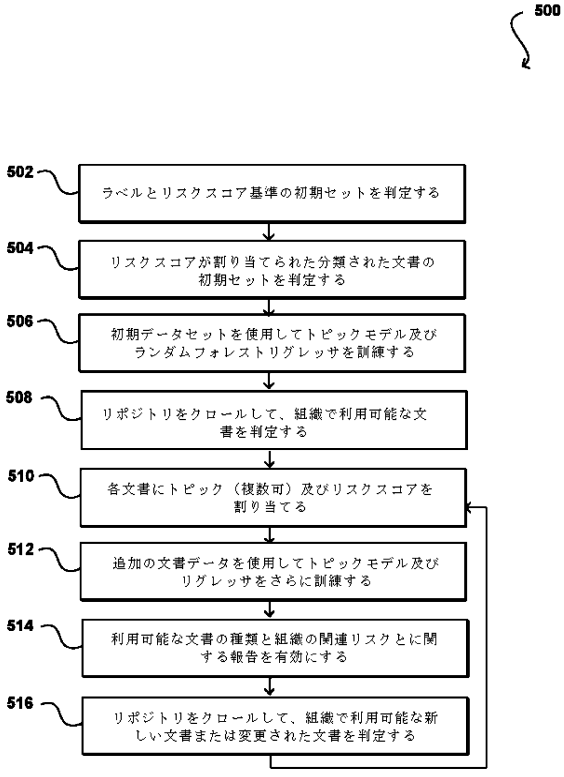
【図３】


300
106
218
分類
データ
214
アクセス
マネージャ
208
文書
212
102
顧客コンソール
ネットワーク
104
セキュリティ
マネージャ
202
204
206
ログ
310
リソース
114
アクティビティモニタ
行動
インターフェース
リソース
マネージャ
110
108
分類器サービス
RNN
304
カルマン
306
分類器アルゴリズム
308
302
セキュリティ
コンソール
312
314
アラート

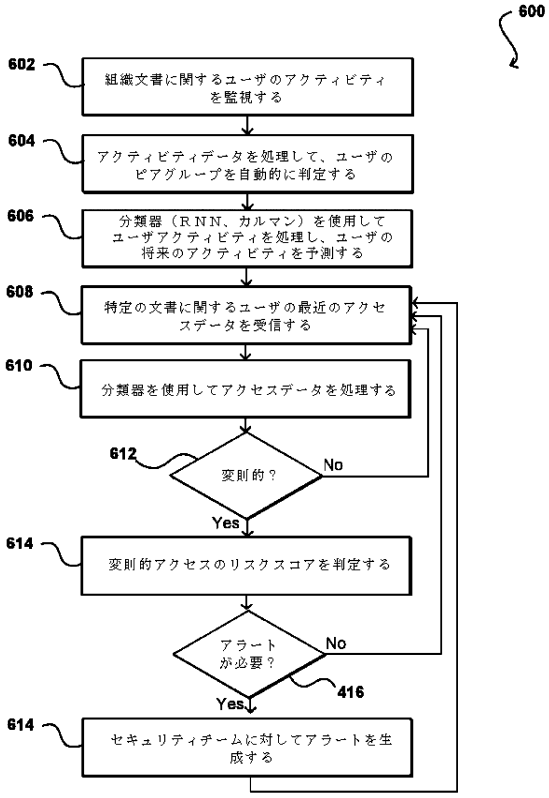
【図４】


400
218
分類
データ
214
406
ピアグループ
ユーザ
402
アクセスマネージャ
208
文書
212
ピア
404
セキュリティマネージャ
202
アクティビティモニタ
ログ
310
インターフェース
行動
410
ピアグループ
ピア
408
分類器サービス
RNN
304
カルマン
306
半訓練分類器
308
302
セキュリティコンソール
312
314
アラート

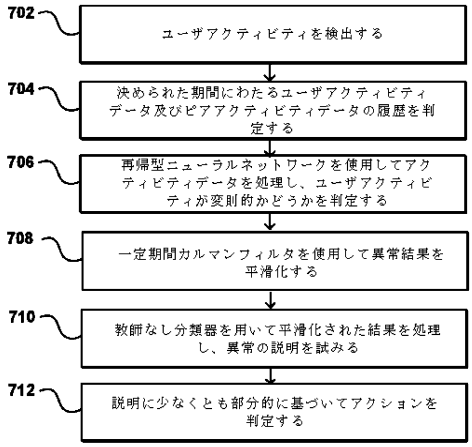
【図５】


500
502
ラベルとリスクスコア基準の初期セットを判定する
504
リスクスコアが割り当てられた分類された文書の初期セットを判定する
506
初期データセットを使用してトピックモデル及びランダムフォレストリグレッサを訓練する
508
リポジトリをクロールして、組織で利用可能な文書を判定する
510
各文書にトピック（複数可）及びリスクスコアを割り当てる
512
追加の文書データを使用してトピックモデル及びリグレッサをさらに訓練する
514
利用可能な文書の種類と組織の関連リスクとに関する報告を有効にする
516
リポジトリをクロールして、組織で利用可能な新しい文書または変更された文書を判定する

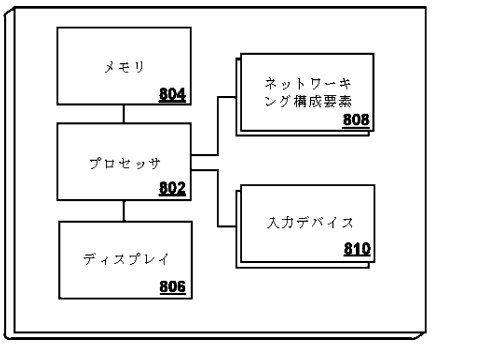
【図６】


600
602
組織文書に関するユーザのアクティビティを監視する
604
アクティビティデータを処理して、ユーザのピアグループを自動的に判定する
606
分類器（ＲＮＮ、カルマン）を使用してユーザアクティビティを処理し、ユーザの将来のアクティビティを予測する
608
特定の文書に関するユーザの最近のアクセスデータを受信する
610
分類器を使用してアクセスデータを処理する
612
変則的？
No
Yes
614
変則的アクセスのリスクスコアを判定する
アラートが必要？
No
Yes
416
614
セキュリティチームに対してアラートを生成する

【図７】


700
702
ユーザアクティビティを検出する
704
決められた期間にわたるユーザアクティビティデータ及びピアアクティビティデータの履歴を判定する
706
再帰型ニューラルネットワークを使用してアクティビティデータを処理し、ユーザアクティビティが変則的かどうかを判定する
708
一定期間カルマンフィルタを使用して異常結果を平滑化する
710
教師なし分類器を用いて平滑化された結果を処理し、異常の説明を試みる
712
説明に少なくとも部分的に基づいてアクションを判定する

【図８】


800
メモリ
804
ネットワーキング構成要素
808
プロセッサ
802
入力デバイス
810
ディスプレイ
806

フロントページの続き

(74)代理人 100162570
弁理士 金子 早苗
(72)発明者 ワトソン、アレキサンダー
アメリカ合衆国、ワシントン州 ９８１０９－５２１０、シアトル、テリー・アベニュー・ノース ４１０
(72)発明者 ブリム、ダニエル
アメリカ合衆国、ワシントン州 ９８１０９－５２１０、シアトル、テリー・アベニュー・ノース ４１０
(72)発明者 シモンズ、クリストファー
アメリカ合衆国、ワシントン州 ９８１０９－５２１０、シアトル、テリー・アベニュー・ノース ４１０
(72)発明者 ラドゥロビック、ポール
アメリカ合衆国、ワシントン州 ９８１０９－５２１０、シアトル、テリー・アベニュー・ノース ４１０
(72)発明者 ブレイ、テイラー・スチュアート
アメリカ合衆国、ワシントン州 ９８１０９－５２１０、シアトル、テリー・アベニュー・ノース ４１０
(72)発明者 ブリンクレイ、ジェニファー・アン
アメリカ合衆国、ワシントン州 ９８１０９－５２１０、シアトル、テリー・アベニュー・ノース ４１０
(72)発明者 ジョンソン、エリック
アメリカ合衆国、ワシントン州 ９８１０９－５２１０、シアトル、テリー・アベニュー・ノース ４１０
(72)発明者 チン、ビクター
アメリカ合衆国、ワシントン州 ９８１０９－５２１０、シアトル、テリー・アベニュー・ノース ４１０
(72)発明者 ラスガイティス、ジャック
アメリカ合衆国、ワシントン州 ９８１０９－５２１０、シアトル、テリー・アベニュー・ノース ４１０
(72)発明者 ツァイ、ナイチン
アメリカ合衆国、ワシントン州 ９８１０９－５２１０、シアトル、テリー・アベニュー・ノース ４１０
(72)発明者 ゴフ、マイケル
アメリカ合衆国、ワシントン州 ９８１０９－５２１０、シアトル、テリー・アベニュー・ノース ４１０
(72)発明者 エンガー、マックス
アメリカ合衆国、ワシントン州 ９８１０９－５２１０、シアトル、テリー・アベニュー・ノース ４１０

審査官 和平 悠希

(56)参考文献 特開２００４－１４７０６７（ＪＰ，Ａ）
特開平０９－０７３４４０（ＪＰ，Ａ）
特開２０１６－１２２２７３（ＪＰ，Ａ）
国際公開第２０１７／０１９７３５（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／６２

G06F　21/55
G06N　3/02
G06N　20/00