

(19) 日本国特許庁(JP)

再公表特許(A1)

(11) 国際公開番号

W02017/065070

発行日 平成30年8月16日 (2018.8.16)

(43) 国際公開日 平成29年4月20日 (2017.4.20)

(51) Int.Cl.	F I	テーマコード (参考)
G06F 21/55 (2013.01)	G06F 21/55 320	
G06F 21/62 (2013.01)	G06F 21/62 309	
G06N 99/00 (2010.01)	G06N 99/00 153	

審査請求 有 予備審査請求 未請求 (全 36 頁)

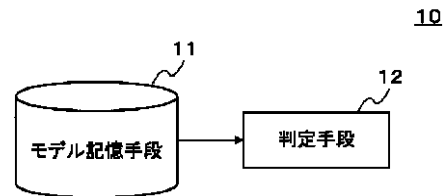
出願番号	特願2017-545169 (P2017-545169)	(71) 出願人	000004237 日本電気株式会社 東京都港区芝五丁目7番1号
(21) 国際出願番号	PCT/JP2016/079637	(74) 代理人	100103090 弁理士 岩壁 冬樹
(22) 国際出願日	平成28年10月5日 (2016.10.5)	(74) 代理人	100124501 弁理士 塩川 誠人
(31) 優先権主張番号	特願2015-202280 (P2015-202280)	(72) 発明者	友永 康之 東京都港区芝五丁目7番1号 日本電気株式会社内
(32) 優先日	平成27年10月13日 (2015.10.13)		
(33) 優先権主張国	日本国 (JP)		

最終頁に続く

(54) 【発明の名称】 不審行動検知システム、情報処理装置、方法およびプログラム

(57) 【要約】

情報処理装置は、データに対する利用者の行動であるデータアクセス行動に関するアクセス情報であって、データにアクセスする利用者に由来する第1の情報と、アクセスされるデータに由来する第2の情報とを含むアクセス情報と、不審行動または正常行動との関係を示すアクセス行動モデルを記憶するモデル記憶手段11と、アクセス行動モデルに基づいて、任意のデータアクセス行動が不審行動であるか否かを判定する判定手段12とを備える。



11 Model storage means
12 Determination means

【特許請求の範囲】**【請求項 1】**

データに対する利用者の行動であるデータアクセス行動に関するアクセス情報であって、データにアクセスする利用者由来の第 1 の情報と、アクセスされるデータ由来の第 2 の情報とを含むアクセス情報と、不審行動または正常行動との関係を示すアクセス行動モデルを記憶するモデル記憶手段と、

前記アクセス行動モデルに基づいて、任意のデータアクセス行動が不審行動であるか否かを判定する判定手段とを備えた

ことを特徴とする情報処理装置。

【請求項 2】

アクセス情報は、第 1 の情報として、アクセスする利用者、アクセスされる時間、アクセス種別もしくはアクセス方法に関する情報を含む、または、第 2 の情報として、データ自体もしくはデータの格納場所に関する情報を含む

請求項 1 に記載の情報処理装置。

【請求項 3】

アクセス情報は、アクセスする利用者に関する情報として、当該利用者が生成したテキストに関する情報もしくは当該利用者が所定のデータに対して行ったアクセス行動に関する統計値を含む、または、データ自体に関する情報として、当該データの内容に関する情報もしくは当該データに対して行われたアクセス行動に関する統計値を含む

請求項 2 に記載の情報処理装置。

【請求項 4】

アクセス情報と、前記アクセス情報が示すデータアクセス行動が不審行動であるか否かを示す情報とを学習データに用いて、機械学習によりアクセス行動モデルを生成する学習手段を備えた

請求項 1 から請求項 3 のうちのいずれか 1 項に記載の情報処理装置。

【請求項 5】

ファイルサーバによって管理されているファイルを、対象データとする情報処理装置であって、

モデル記憶手段は、所定のファイルに対するアクセス履歴に含まれるアクセス行動のうち指定された期間におけるアクセス行動に関するアクセス情報と、前記アクセス行動が不審行動か否かを判別可能な情報とを用いて機械学習されたアクセス行動モデルを記憶する

請求項 1 から請求項 4 のうちのいずれか 1 項に記載の情報処理装置。

【請求項 6】

アクセス情報から、各々が多次元の数値からなる 2 以上の数値ベクトルを生成する数値ベクトル生成手段を備え、

モデル記憶手段は、前記 2 以上の数値ベクトルの組と、不審行動または正常行動との関係を示すアクセス行動モデルとの関係を示すアクセス行動モデルを記憶し、

判定手段は、前記アクセス行動モデルを用いて算出される、指定されたアクセス情報から生成される 2 以上の数値ベクトルの組に対する不審行動または正常行動の確度に基づいて、前記アクセス情報によって示されるデータアクセス行動が不審行動であるか否かを判定する

請求項 1 から請求項 5 のうちのいずれか 1 項に記載の情報処理装置。

【請求項 7】

数値ベクトル生成手段として、

アクセス情報に含まれる第 1 情報から、多次元の数値からなる第 1 数値ベクトルを生成する第 1 数値ベクトル生成手段と、

アクセス情報に含まれる第 2 情報から、多次元の数値からなる第 2 数値ベクトルを生成する第 2 数値ベクトル生成手段とを備え、

モデル記憶手段は、前記第 1 数値ベクトルと前記第 2 数値ベクトルとの組と、不審行動または正常行動との関係を示すアクセス行動モデルを記憶し、

10

20

30

40

50

判定手段は、前記アクセス行動モデルを用いて算出される、指定されたアクセス情報に含まれる第1情報および第2情報から生成される前記第1数値ベクトルと前記第2数値ベクトルの組に対する不審行動または正常行動の確度に基づいて、前記アクセス情報によって示されるデータアクセス行動が不審行動であるか否かを判定する

請求項6に記載の情報処理装置。

【請求項8】

アクセス行動モデルに基づいて、不審行動に該当するアクセス行動が行われる危険性があるデータを予測する危険データ予測手段を備えた

請求項1から請求項7のうちのいずれか1項に記載の情報処理装置。

【請求項9】

アクセス行動モデルに基づいて、不審行動に該当するデータアクセス行動を行う危険性がある利用者を予測する危険利用者予測手段を備えた

請求項1から請求項8のうちのいずれか1項に記載の情報処理装置。

【請求項10】

判定手段による判定結果に基づいて、アクセス権限を変更するアクセス権限変更手段を備えた

請求項1から請求項9のうちのいずれか1項に記載の情報処理装置。

【請求項11】

判定手段による判定結果を基に、実際に行われたデータアクセス行動から不審行動を検知する不審行動検知手段と、

不審行動が検知されると、管理者に通知を行う通知手段とを備えた

請求項1から請求項10のうちのいずれか1項に記載の情報処理装置。

【請求項12】

データに対する利用者の行動であるデータアクセス行動に関するアクセス情報であって、データにアクセスする利用者に由来する第1の情報と、アクセスされるデータに由来する第2の情報とを含むアクセス情報と、前記アクセス情報が示すデータアクセス行動が不審行動か否かを判別可能な情報とを学習データに用いて、機械学習により、任意のアクセス情報と不審行動または正常行動との関係を示すアクセス行動モデルを生成する学習手段と、

前記アクセス行動モデルを記憶するモデル記憶手段と、

前記アクセス行動モデルに基づいて、任意のデータアクセス行動が不審行動であるか否かを判定する判定手段と、

前記判定結果を基に、実際に行われたデータアクセス行動から不審行動を検知する不審行動検知手段とを備えた

ことを特徴とする不審行動検知システム。

【請求項13】

情報処理装置が、データに対する利用者の行動であるデータアクセス行動に関するアクセス情報であって、データにアクセスする利用者に由来する第1の情報と、アクセスされるデータに由来する第2の情報とを含むアクセス情報と、不審行動または正常行動との関係を示すアクセス行動モデルに基づいて、任意のデータアクセス行動が不審行動であるか否かを判定する

ことを特徴とする不審行動検知方法。

【請求項14】

コンピュータに、

データに対する利用者の行動であるデータアクセス行動に関するアクセス情報であって、データにアクセスする利用者に由来する第1の情報と、アクセスされるデータに由来する第2の情報とを含むアクセス情報と、不審行動または正常行動との関係を示すアクセス行動モデルに基づいて、任意のデータアクセス行動が不審行動であるか否かを判定させる処理

を実行させるための不審行動検知プログラム。

10

20

30

40

50

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、不審行動を検知するための不審行動検知システム、それに用いられる情報処理装置、不審行動検知方法および不審行動検知プログラムに関する。

【背景技術】

【0002】

近年、企業データの情報漏えい対策が特に注目されている。特に、データに対する有効なアクセス権限を有する関係者が契機となって生じる情報漏えいに対する対策が注目されている。

10

【0003】

企業データの情報漏えい事例の分析により、企業データに対して有効なアクセス権限を有する社内関係者や当該企業の外部委託先の担当者が契機となっているケースが多いことがわかってきたためである。

【0004】

情報漏えい対策の代表的な例としては、全てのデータを暗号化する手法や、ルールベースで利用者の不審行動を検知して禁止する手法や、統計ベースで利用者の不審行動を検知して禁止する手法が挙げられる。なお、本発明では、データに対して正当な権限を有する利用者が権限を悪用して当該データにアクセスする行為を不審行動と呼ぶ。また、以下では、データに対して正当な権限を有する利用者が当該権限を正当に利用して（権限を設定した目的の範囲内で）当該データにアクセスする行為を正常行動と呼ぶ場合がある。この場合、あるデータに対して正当な権限を有する利用者の当該データに対するアクセス行動は、正常行動か不審行動のいずれかに分類される。

20

【0005】

例えば、特許文献1には、上記の統計ベースで利用者の不審行動を検知する手法の例が記載されている。より具体的には、特許文献1に記載のシステムは、ユーザの操作ログから、所定の時間帯における所定の操作について、ユーザ毎に、操作状況の推移を演算する。そして、演算された操作状況の推移を示す数値から構成されるモデルを生成し、それらの平均値を求める。そして、各ユーザの操作状況の推移を示す数値と平均値との乖離計算により、特異な操作を行った利用者を検知する。

30

【0006】

また、データから特徴量を得る技術に関連して、非特許文献1には、数値のみからなる多次元ベクトルに対して特徴抽出を行って、特徴ベクトルを生成する方法が記載されている。

【先行技術文献】

【特許文献】

【0007】

【特許文献1】特開2008-192091号公報

【非特許文献】

【0008】

【非特許文献1】Bespalov, Dmitriy and Qi, Yanjun and Bai, Bing and Shokoufandeh, Ali, "Sentiment Classification with Supervised Sequence Embedding", Machine Learning and Knowledge Discovery in Databases, vol.7523, 2012, p.159-174

40

【発明の概要】

【発明が解決しようとする課題】

【0009】

上記の全てのデータを暗号化する手法は、利用者がデータをそのまま持ち出しても専用ソフトウェアを使用しないと暗号化を解除できないため、情報漏えい対策として有効である。しかし、この手法は、通常の業務等で取引先企業にデータを送付する際に、都度当該データの暗号化を解除する権限を有する特権管理者に暗号化の解除を依頼する必要がある

50

、生産性が低下する問題がある。また、この手法は、特定ファイルを暗号化対象から除外するなど抜け穴が生じる問題がある。また、この手法は、特権管理者がその権限を悪用してデータの暗号化を解除するケースを防止できない問題がある。

【0010】

アクセスログ等を分析し、アクセスパターンに関するルールを設定して不審行動を検知するなどのルールベースの手法は、特権管理者を含む全ての利用者に適用できるため、特権管理者の権限悪用による情報漏えいを防止できる可能性が高い。しかし、この手法は、予めルールを設定することが非常に困難であるという問題がある。また、この手法は、設定したルールのメンテナンスに手間がかかる等の問題がある。

【0011】

なお、統計ベースの手法としては、特許文献1に記載されているような、利用者の通常行動と相関のある特徴量（例えば、1分間のファイルサーバアクセス数など）を計算し、この特徴量が予め設定した閾値を超過した場合に不審行動を検知する手法がある。しかし、特許文献1に記載の手法は、利用者の不審行動または通常行動と相関のある特徴量を決めるためにアクセスログを統計分析する必要があり、導入時の敷居が高いという問題がある。また、アクセスログの統計分析の対象とされる利用者およびデータに関する情報は、大量かつ多様なテキストを含むことが多い。この場合、特許文献1に記載の手法では、上記の特徴量が高次元となるが、統計分析でこのような高次元の特徴量を扱うのは困難である。このため、特許文献1に記載の手法は、不審行動の検知精度が低い問題がある。

【0012】

そこで、本願発明は、上記に鑑み、予めルールを設定することなく、高精度に不審行動を検知できる不審行動検知システム、それに用いられる情報処理装置、不審行動検知方法および不審行動検知プログラムを提供することを目的とする。

【課題を解決するための手段】

【0013】

本発明による情報処理装置は、データに対する利用者の行動であるデータアクセス行動に関するアクセス情報であって、データにアクセスする利用者に由来する第1の情報と、アクセスされるデータに由来する第2の情報とを含むアクセス情報と、不審行動または正常行動との関係を示すアクセス行動モデルを記憶するモデル記憶手段と、アクセス行動モデルに基づいて、任意のデータアクセス行動が不審行動であるか否かを判定する判定手段とを備えたことを特徴とする。

【0014】

本発明による不審行動検知システムは、データに対する利用者の行動であるデータアクセス行動に関するアクセス情報であって、データにアクセスする利用者に由来する第1の情報と、アクセスされるデータに由来する第2の情報とを含むアクセス情報と、アクセス情報が示すデータアクセス行動が不審行動か否かを判別可能な情報とを学習データに用いて、機械学習により、任意のアクセス情報と不審行動または正常行動との関係を示すアクセス行動モデルを生成する学習手段と、アクセス行動モデルを記憶するモデル記憶手段と、アクセス行動モデルに基づいて、任意のデータアクセス行動が不審行動であるか否かを判定する判定手段と、判定結果を基に、実際に行われたデータアクセス行動から不審行動を検知する不審行動検知手段とを備えたことを特徴とする。

【0015】

本発明による不審行動検知方法は、情報処理装置が、データに対する利用者の行動であるデータアクセス行動に関するアクセス情報であって、データにアクセスする利用者に由来する第1の情報と、アクセスされるデータに由来する第2の情報とを含むアクセス情報と、不審行動または正常行動との関係を示すアクセス行動モデルに基づいて、任意のデータアクセス行動が不審行動であるか否かを判定することを特徴とする。

【0016】

本発明による不審行動検知プログラムは、コンピュータに、データに対する利用者の行動であるデータアクセス行動に関するアクセス情報であって、データにアクセスする利用

10

20

30

40

50

者に由来する第 1 の情報と、アクセスされるデータに由来する第 2 の情報とを含むアクセス情報と、不審行動または正常行動との関係を示すアクセス行動モデルに基づいて、任意のデータアクセス行動が不審行動であるか否かを判定させる処理を実行させることを特徴とする。

【発明の効果】

【0017】

本発明によれば、予めルールを設定することなく、精度良く不審行動を検知できる。

【図面の簡単な説明】

【0018】

【図 1】第 1 の実施形態の不審行動検知システムの構成例を示すブロック図である。 10

【図 2】第 1 の実施形態の不審行動検知システムの動作例を示すフローチャートである。

【図 3】第 1 の実施形態の不審行動検知システムの他の構成例を示すブロック図である。

【図 4】第 1 の実施形態の不審行動検知システムの他の動作例を示すフローチャートである。

【図 5】第 1 の実施形態の不審行動検知システムの他の構成例を示すブロック図である。

【図 6】数値ベクトル生成手段 16 のより詳細な構成例を示すブロック図である。

【図 7】第 2 の実施形態の不審行動検知システムの構成例を示すブロック図である。

【図 8】利用者データ記憶部 101 が保持する利用者データのデータ構造の一例を示す説明図である。

【図 9】文書データ記憶部 102 が保持する文書データのデータ構造の一例を示す説明図である。 20

【図 10】アクセスログ記憶部 105 が保持するアクセスログのデータ構造の一例を示す説明図である。

【図 11】予測スコア記憶部 112 が保持する予測結果のデータ構造の一例を示す説明図である。

【図 12】不審行動検知システム 100 のアクセス行動学習ステップの動作例を示すフローチャートである。

【図 13】不審行動検知システム 100 のアクセス行動予測ステップの動作例を示すフローチャートである。

【図 14】不審行動検知システム 100 の不審行動通知ステップの動作例を示すフローチャートである。 30

【図 15】第 2 の実施形態の第 1 変形例の不審行動検知システムの構成例を示すブロック図である。

【図 16】第 2 の実施形態の第 1 変形例の不審行動検知システムの動作例を示すフローチャートである。

【図 17】第 2 の実施形態の第 2 変形例の不審行動検知システムの構成例を示すブロック図である。

【図 18】アクセス権限制御画面の例を示す説明図である。

【図 19】第 2 の実施形態の第 2 変形例の不審行動検知システムの動作例を示すフローチャートである。 40

【図 20】第 2 の実施形態の第 3 変形例の不審行動検知システムの構成例を示すブロック図である。

【図 21】第 2 の実施形態の第 3 変形例の不審行動検知システムの動作例を示すフローチャートである。

【発明を実施するための形態】

【0019】

実施形態 1 .

以下、本発明の実施形態について図面を参照して説明する。図 1 は、本発明の第 1 の実施形態にかかる不審行動検知システムの構成例を示すブロック図である。図 1 に示す不審行動検知システム 10 は、モデル記憶手段 11 と、判定手段 12 とを備える。 50

【 0 0 2 0 】

モデル記憶手段 1 1 は、アクセス情報と不審行動との関係またはアクセス情報と正常行動との関係を示すアクセス行動モデルを記憶する。アクセス情報は、データに対する利用者の行動であるデータアクセス行動に関する情報であって、データにアクセスする利用者に由来する第 1 の情報と、アクセスされるデータに由来する第 2 の情報とを含む。

【 0 0 2 1 】

判定手段 1 2 は、モデル記憶手段 1 1 に記憶されているアクセス行動モデルに基づいて、任意のデータアクセス行動が不審行動であるか否かを判定する。

【 0 0 2 2 】

ここで、第 1 の情報は、例えば、データにアクセスする利用者に関する情報や、該利用者がデータにアクセスする際の時間（アクセス時間）、種別（アクセス種別）または方法（アクセス方法）に関する情報であってもよい。また、第 2 の情報は、アクセスされるデータ自体に関する情報（いわゆるデータの属性情報や、特徴量といったデータの内容に関する情報等）であってもよい。第 2 の情報は、データ自体に関する情報に限られず、例えば、該データの格納場所に関する情報や、該データに対して行われたアクセス行動に関する統計値であってもよい。

10

【 0 0 2 3 】

また、データにアクセスする利用者に関する情報は、一般に利用者の属性情報とされる情報に限られず、例えば、当該利用者が生成したテキストに関する情報や、当該利用者が所定のデータに対して行ったアクセス行動に関する統計値であってもよい。

20

【 0 0 2 4 】

また、図 2 は、本実施形態の動作例を示すフローチャートである。図 2 に示す例では、まず、判定手段 1 2 は、モデル記憶手段 1 1 からアクセス行動モデルを読み出す（ステップ S 1 1）。次に、判定手段 1 2 は、読み出されたアクセス行動モデルに基づいて、指定されたアクセス情報に対して、該アクセス情報が示すデータアクセス行動が不審行動であるか否かを判定する（ステップ S 1 2）。

【 0 0 2 5 】

アクセス情報の取得方法としては、例えば、管理者が直接入力してもよいし、システムが、所定のデータに対するアクセス履歴に含まれる指定された期間やデータや利用者等の情報を基に生成してもよい。

30

【 0 0 2 6 】

このような構成によれば、データにアクセスした利用者に由来する情報と、アクセスされたデータに由来する情報という少なくとも 2 つの観点による情報の組からデータアクセス行動が不審行動か否かを判別可能なアクセス行動モデルを基に、任意のアクセス行動が不審行動か否かを判定できるため、予めルールを設定することなく、不審行動を高精度に検知できる。

【 0 0 2 7 】

また、図 1 に示す構成において、データは、ファイルサーバによって管理されているファイルであってもよい。そのような場合に、モデル記憶手段 1 1 は、所定のファイルに対するアクセス履歴に含まれるアクセス行動のうち指定された期間におけるアクセス行動に関するアクセス情報と、該アクセス行動が不審行動か否かを判別可能な情報とを用いて機械学習されたアクセス行動モデルを記憶してもよい。

40

【 0 0 2 8 】

また、図 3 は、不審行動検知システム 1 0 の他の構成例を示すブロック図である。図 3 に示すように、不審行動検知システム 1 0 は、図 1 に示す構成に加えて、例えば、アクセス情報と、該アクセス情報が示すデータアクセス行動が不審行動か否かを判別可能な情報とを学習データに用いて、機械学習によりアクセス行動モデルを生成する学習手段 1 3 を備えていてもよい。

【 0 0 2 9 】

そのような学習手段 1 3 を備えることによって、学習手段に与えるデータの次元数が膨

50

大であっても学習が可能になる。なお、データの次元数は、例えば、1000以上であってもよいし、10000以上であってもよい。

【0030】

また、図3に示すように、不審行動検知システム10は、例えば、判定手段12による判定結果を基に、実際に行われたデータアクセス行動から不審行動を検知する不審行動検知手段14をさらに備えていてもよい。

【0031】

また、図4は、不審行動検知システム10の図3に示す構成における動作例を示すフローチャートである。図4に示す例では、まず、学習手段13が、アクセス情報と、該アクセス情報が示すデータアクセス行動が不審行動か否かを判別可能な情報とを学習データに用いて、機械学習によりアクセス行動モデルを生成する(ステップS21)。また、学習手段13は、生成したアクセス行動モデルをモデル記憶手段11に書き込む(ステップS22)。

10

【0032】

次に、判定手段12が、モデル記憶手段11からアクセス行動モデルを読み出し、読み出されたアクセス行動モデルに基づいて、指定されたアクセス情報に対して不審行動か否かを判定する(ステップS11、ステップS12)。

【0033】

判定手段12による判定の結果、不審行動であった場合(ステップS23のYes)、不審行動検知手段14は、指定されたアクセス情報が示すアクセス行動が不審行動であるとして、所定の検知処理を行う(ステップS24)。検知処理は、例えば、検知した不審行動に関する情報を記憶したり、管理者に通知する処理であってもよい。

20

【0034】

一方、不審行動でなかった場合(ステップS23のNo)、システムは、次のアクセス情報が指定されるのを待つ(ステップS12に戻る)。

【0035】

ステップS12~ステップS24までの動作を、例えば、アクセス情報が指定される度に繰り返す。

【0036】

また、図5は、不審行動検知システム10の他の構成例を示すブロック図である。図5に示すように、不審行動検知システム10は、例えば、通知手段15や、数値ベクトル生成手段16や、危険利用者予測手段17や、危険データ予測手段18や、アクセス権限変更手段19をさらに備えていてもよい。

30

【0037】

通知手段15は、不審行動が検知されると、管理者に通知を行う。

【0038】

数値ベクトル生成手段16は、アクセス情報から、各々が多次元の数値からなる2以上の数値ベクトルを生成する。

【0039】

数値ベクトル生成手段16を備える構成において、モデル記憶手段11は、数値ベクトル生成手段16が生成した数値ベクトルの組と、不審行動または正常行動との関係を示すアクセス行動モデルとの関係を示すアクセス行動モデルを記憶してもよい。また、判定手段12は、そのようなアクセス行動モデルを用いて算出される、指定されたアクセス情報から生成される2以上の数値ベクトルの組に対する不審行動または正常行動の確度に基づいて、当該アクセス情報によって示されるデータアクセス行動が不審行動であるか否かを判定してもよい。

40

【0040】

また、図6は、数値ベクトル生成手段16のより詳細な構成例を示すブロック図である。図6に示すように、数値ベクトル生成手段16は、第1数値ベクトル生成手段161と、第2数値ベクトル生成手段162とを含んでいてもよい。

50

【 0 0 4 1 】

第 1 数値ベクトル生成手段 1 6 1 は、アクセス情報に含まれる第 1 情報から、多次元の数値からなる第 1 数値ベクトルを生成する。

【 0 0 4 2 】

第 2 数値ベクトル生成手段 1 6 2 は、アクセス情報に含まれる第 2 情報から、多次元の数値からなる第 2 数値ベクトルを生成する。

【 0 0 4 3 】

第 1 数値ベクトル生成手段 1 6 1 および第 2 数値ベクトル生成手段 1 6 2 を備える構成において、モデル記憶手段 1 1 は、第 1 数値ベクトルと第 2 数値ベクトルの組と、不審行動または正常行動との関係を示すアクセス行動モデルを記憶してもよい。また、判定手段 1 2 は、そのようなアクセス行動モデルを用いて算出される、指定されたアクセス情報から生成される第 1 数値ベクトルと第 2 数値ベクトルの組に対する不審行動または正常行動の確度に基づいて、当該アクセス情報によって示されるデータアクセス行動が不審行動であるか否かを判定してもよい。

10

【 0 0 4 4 】

危険利用者予測手段 1 7 は、アクセス行動モデルに基づいて、データに対して、不審行動に該当するデータアクセス行動を行う危険性がある利用者を予測する。

【 0 0 4 5 】

危険データ予測手段 1 8 は、アクセス行動モデルに基づいて、利用者に対して、不審行動に該当するアクセス行動が行われる危険性があるデータを予測する。

20

【 0 0 4 6 】

アクセス権限変更手段 1 9 は、判定手段 1 2 による判定結果、不審行動検知手段 1 4 による検知結果、危険データ予測手段 1 8 による予測結果または危険利用者予測手段 1 7 による予測結果に基づいて、アクセス権限を変更する。

【 0 0 4 7 】

このような構成によれば、不審行動を高精度に検知できるだけでなく、検知した不審行動の情報（検知の対象となったアクセス情報など）を管理者に通知できる。また、不審行動が検知された利用者（不審行動者）が、当該不審行動が検知されたデータ（対象データ）を不正に取得できないよう、当該利用者に対する対象データのアクセス権限を自動的に変更できる。また、事前に、そのような不審行動を行う可能性のある利用者や対象データを予測できるので、不審行動を未然に防ぐことができる。また、データのアクセス権限の設定に穴があってもその穴を塞ぐことができる。

30

【 0 0 4 8 】

本実施形態において、モデル記憶手段 1 1 は、例えば、記憶装置によって実現される。また、判定手段 1 2、学習手段 1 3、不審行動検知手段 1 4、通知手段 1 5、数値ベクトル生成手段 1 6、危険利用者予測手段 1 7、危険データ予測手段 1 8 およびアクセス権限変更手段 1 9 は、例えば、プログラムに従って動作する情報処理装置によって実現される。なお、通知手段 1 5 が、ディスプレイ装置等を介して管理者に情報の通知を行う場合、通知手段 1 5 は、例えば、プログラムに従って動作する情報処理装置と、ディスプレイなどの表示装置または該表示装置とのインタフェース部とによって実現されてもよい。

40

【 0 0 4 9 】

実施形態 2 .

次に、本発明の第 2 の実施形態について説明する。なお、以下では、不審行動の検知対象とするデータが、ファイルサーバによって管理されるファイルである場合を例に用いて説明を行うが、データはファイルサーバによって管理されるファイルに限定されない。例えば、データは、データベースシステム等に格納される任意の単位のデータであってもよい。

【 0 0 5 0 】

まず、本実施形態の特徴を簡単に説明する。本実施形態の不審行動検知システムは、（ 1 ）ファイルサーバの利用者データ、（ 2 ）ファイルサーバが格納する文書データ、（ 3

50

）ファイルサーバのアクセスログ、の3つのデータを用いて、各ファイルサーバ利用者の通常時におけるファイルサーバに対するアクセス行動を機械学習（教師あり学習）でモデル化する。そして、各ファイルサーバ利用者の実際のファイルサーバに対するアクセス行動と上記のモデルで予測されるアクセス行動の乖離を常時監視することにより、乖離の大きいファイルサーバ利用者を不審行動者として自動検知する。

【0051】

ここで、（1）利用者データは、例えば、氏名、年齢、性別、学歴、担当業務、役職、部署、管理スパン（スパンオブコントロール）、異動履歴、保有資格、職務経歴、業績評価、健康診断結果などを含んでいてもよい。また、（2）文書データは、例えば、文書名、ファイルパス、アクセス権限、更新日時などのプロパティ設定、文書の内容に関する情報（テキスト、画像など）などを含んでいてもよい。また、（3）アクセスログは、ファイルサーバに対するアクセス履歴を保存したファイルであってもよい。なお、いずれのデータにおいても、大量かつ多様なテキストデータ（非構造化データ）が含まれていてもよい。

10

【0052】

また、本実施形態の不審行動検知システムが行う不審行動検知方法には、前処理ステップ、特徴抽出ステップ、学習ステップ、予測ステップ、通知ステップ、の5つのプロセスを含まれる。

【0053】

前処理ステップでは、上記の3つのデータ（利用者データ、文書データ、アクセスログ）から＜利用者属性、文書属性、アクセス実績＞のデータ組（tuple）を生成する。ここで、利用者属性は、ファイルサーバの利用者データから、利用者の特徴を表現するデータ項目の内容を抜き出したものであればよい。文書属性は、ファイルサーバが格納する文書データから、文書の特徴を表現するデータ項目の内容を抜き出したものであればよい。アクセス実績は、ファイルサーバのアクセスログで示される、当該利用者が当該文書にアクセスした実績の有無を判別可能な情報であればよい。例えば、アクセス実績は、アクセスした実績がある場合は1、ない場合は0等として2値化された情報であってもよい。

20

【0054】

特徴抽出ステップでは、上記のデータ組のうち利用者属性および文書属性からそれぞれ特徴ベクトルを生成する。

30

【0055】

学習ステップでは、上記のデータ組の集合から学習対象期間に該当するデータ組を切り出した上で、それらデータ組を用いて要素間の関係性（より具体的には、＜利用者属性、文書属性＞ペアとアクセス実績の関係性）を機械学習して予測モデルを生成する。機械学習アルゴリズムには、米国特許第8341095号明細書に記載された方法（Supervised Semantic Indexing（以下、SSIという））を用いることを想定するが、その他、一般的な機械学習手法を組み合わせてもよい。

【0056】

予測ステップでは、上記のデータ組の集合から予測対象期間に該当するデータ組を切り出した上で、それらデータ組に対して予測モデルを適用する。より具体的には、それらデータ組の各々が示す＜利用者属性、文書属性＞ペアに対してアクセス行動の予測スコアを計算する。本実施形態では、予測スコアを[0.0～1.0]の実数値とする。なお、予測スコアが1.0に近いほど、当該＜利用者属性、文書属性＞ペアはアクセス確度が高いすなわち正常行動である可能性が高いことを表す。一方、予測スコアが0.0に近いほど、当該＜利用者属性、文書属性＞ペアはアクセス確度が低いすなわち不審行動である可能性が高いことを表す。

40

【0057】

通知ステップでは、予測ステップで計算した＜利用者属性、文書属性＞ペアのうち、予測スコアが閾値（例えば0.1など）より低いもの（つまり当該利用者属性が示す利用者が当該文書属性が示す文書にアクセスする確度が低いと予測されるもの）を不審行動とし

50

て抽出する。そして、抽出された不審行動の対象とされた利用者のリストを管理者等に通知する。

【0058】

以下、より具体的な構成について説明する。図7は、本実施形態の不審行動検知システムの構成例を示すブロック図である。

【0059】

図7に示す不審行動検知システム100は、利用者データ記憶部101と、文書データ記憶部102と、利用者データ前処理部103と、文書データ前処理部104と、アクセスログ記憶部105と、アクセスログ前処理部106と、利用者属性特徴抽出部107と、文書属性特徴抽出部108と、アクセス実績学習部109と、予測モデル記憶部110と、予測スコア算出部111と、予測スコア記憶部112と、不審行動通知部113とを備える。

10

【0060】

不審行動検知システム100は、例えば、パーソナルコンピュータやサーバ装置等の情報処理装置と、該情報処理装置がアクセス可能なデータベースシステム等の記憶装置群とによって実現される。このとき、利用者データ前処理部103、文書データ前処理部104、アクセスログ前処理部106、利用者属性特徴抽出部107、文書属性特徴抽出部108、アクセス実績学習部109、予測スコア算出部111および不審行動通知部113は、例えば、情報処理装置が備えるCPUによって実現されてもよい。その場合、該CPUは、所定の記憶装置に記憶された各処理部の動作を記述したプログラムを読み出し、該プログラムに従って動作することによって各処理部の機能を実現する。また、利用者データ記憶部101、文書データ記憶部102、アクセスログ記憶部105、予測モデル記憶部110および予測スコア記憶部112は、例えば、情報処理装置がアクセス可能な記憶装置群によって実現されてもよい。なお、記憶装置は1つであっても複数であってもよい。

20

【0061】

利用者データ記憶部101は、ファイルサーバの利用者の利用者データを保持する。ファイルサーバの利用者データの項目例としては、氏名、年齢、性別、学歴、担当業務、役職、部署、管理スパン、異動履歴、保有資格、職務経歴、業績評価、健康診断結果などが挙げられる。

30

【0062】

図8は、利用者データ記憶部101が保持する利用者データのデータ構造の一例を示す説明図である。図8に示すように、利用者データ記憶部101は、利用者データとして、例えば、利用者を識別する利用者IDと対応づけて、利用者の氏名、年齢、性別、役職、担当業務、業績評価等の情報を記憶してもよい。利用者データは、さらに利用者の人物像や勤務態度に関する説明等がテキスト形式で記載された情報を含んでいてもよい。また、利用者データは、さらに健康診断結果を含んでいてもよい。なお、図8において、網掛けは一人分の利用者データに相当するレコードの例を示している。

【0063】

文書データ記憶部102は、ファイルサーバが格納する文書の文書データを保持する。文書データの項目例としては、文書名、文書の種別、ファイルパス、アクセス権限、更新日時などの当該文書に付随するプロパティ設定などが挙げられる。

40

【0064】

図9は、文書データ記憶部102が保持する文書データのデータ構造の一例を示す説明図である。図9に示すように、文書データ記憶部102は、文書データとして、例えば、文書を識別する文書IDと対応づけて、文書の種別、アクセス権限の設定内容、作成日時、更新日時等のプロパティ情報を記憶してもよい。また、文書データは、さらに文書の内容に関する説明等がテキスト形式で記載された情報を含んでいてもよい。なお、図9において、網掛けは一ファイル分の文書データに相当するレコードの例を示している。

【0065】

50

利用者データ前処理部 103 は、利用者データ記憶部 101 を参照して、指定された利用者に関するレコードを読み込む。また、利用者データ前処理部 103 は、読み込んだレコードに含まれる指定された利用者に関する情報（以下、利用者属性情報という場合がある）を用いて、利用者ベクトルを生成する。ここで、利用者ベクトルは、利用者属性情報が示す内容を、数値からなる多次元ベクトルで表現したものである。利用者データ前処理部 103 は、例えば、上記処理を利用者属性特徴抽出部 107 の命令に応じて行う。

【0066】

文書データ前処理部 104 は、文書データ記憶部 102 を参照して、指定された文書に関するレコードを読み込む。また、文書データ前処理部 104 は、読み込んだレコードに含まれる指定された文書に関する情報（以下、文書属性情報という場合がある）を用いて、文書ベクトルを生成する。ここで、文書ベクトルは、文書属性情報が示す内容を、数値からなる多次元ベクトルで表現したものである。文書データ前処理部 104 は、例えば、上記処理を文書属性特徴抽出部 108 の命令に応じて行う。

10

【0067】

アクセスログ記憶部 105 は、所定のファイルサーバのアクセスログを保持する。ファイルサーバのアクセスログには、ファイルサーバ利用者がファイルサーバにアクセスする度に、アクセス日時、アクセス者、アクセス文書等のアクセス行動に関する情報が記録される。

【0068】

図 10 は、アクセスログ記憶部 105 が保持するアクセスログのデータ構造の一例を示す説明図である。

20

【0069】

アクセスログ前処理部 106 は、アクセスログ記憶部 105 を参照して、指定期間のアクセス日時をもつレコードを読み込む。また、アクセスログ前処理部 106 は、読み込んだレコードに含まれるアクセス者 ID およびアクセス文書 ID を基に、ラベル情報を生成する。例えば、アクセスログ前処理部 106 は、アクセスログの指定期間中のレコードに含まれているアクセス者 ID とアクセス文書 ID の組を用いて、該アクセス者 ID に対応する利用者 ID と該アクセス文書 ID に対応する文書 ID の組に対して、正否ラベルを正解（1）とするラベル情報〈利用者 ID、文書 ID、正否ラベル（0 / 1）〉を生成してもよい。また、アクセスログ前処理部 106 は、例えば、アクセスログの指定期間中にアクセス実績のない利用者と文書の組をランダムに選択し、その利用者の利用者 ID とその文書の文書 ID の組に対して、正否ラベルを不正解（0）とするラベル情報を生成してもよい。なお、アクセスログ前処理部 106 は、正解ラベル情報として、正常行動を行った利用者と文書の組を示すラベル情報〈利用者 ID、文書 ID〉を生成したり、不正解ラベル情報として、不審行動を行った利用者と文書の組を示すラベル情報〈利用者 ID、文書 ID〉を生成してもよい。以下、正解ラベル情報と不正解ラベル情報とを特に区別せず、不審行動が否かを判別可能なラベル情報という意味で正否ラベル情報と呼ぶ場合がある。アクセスログ前処理部 106 は、例えば、上記処理をアクセス実績学習部 109 の命令に応じて行う。

30

【0070】

利用者属性特徴抽出部 107 は、利用者データ前処理部 103 が生成した利用者ベクトルに対して特徴抽出を行い、利用者特徴ベクトルを生成する。ここで、利用者特徴ベクトルは、利用者ベクトルの次元数よりも少ない次元数の数値ベクトルであればよい。利用者属性特徴抽出部 107 は、例えば、上記処理をアクセス実績学習部 109 または予測スコア算出部 111 の命令に応じて行う。

40

【0071】

文書属性特徴抽出部 108 は、文書データ前処理部 104 が生成した文書ベクトルに対して特徴抽出を行い、文書特徴ベクトルを生成する。ここで、文書特徴ベクトルは、文書ベクトルの次元数よりも少ない次元数の数値ベクトルであればよい。文書属性特徴抽出部 108 は、例えば、上記処理をアクセス実績学習部 109 または予測スコア算出部 111

50

の命令に応じて行う。

【0072】

アクセス実績学習部109は、利用者属性特徴抽出部107が生成した利用者特徴ベクトルと、文書属性特徴抽出部108が生成した文書特徴ベクトルと、アクセスログ前処理部106が生成したラベル情報とから、学習データとして<利用者特徴ベクトル、文書特徴ベクトル、正否ラベル(1/0)>を生成する。なお、ラベル情報は、正否ラベルを含むラベル情報(<利用者ID、文書ID、正否ラベル>)であっても、正否ラベルを含まない正否ラベル情報(<利用者ID、文書ID>)であってもよい。また、アクセス実績学習部109は、生成された学習データを用いて、利用者特徴ベクトルと文書特徴ベクトルと正否ラベルの間の関係性を機械学習し、予測モデルを生成する。

10

【0073】

予測モデル記憶部110は、アクセス実績学習部109が生成した予測モデルを保持する。

【0074】

予測スコア算出部111は、指定された利用者と文書のペアについて、予測データ<利用者特徴ベクトル、文書特徴ベクトル>を生成する。また、予測スコア算出部111は、生成した予測データに予測モデル記憶部110が保持する予測モデルを適用して、当該予測データに対するアクセス行動の予測スコアを算出する。予測スコア算出部111は、例えば、利用者と文書を指定して、利用者データ前処理部103、利用者属性特徴抽出部107、文書データ前処理部104および文書属性特徴抽出部108に命令をすることにより、予測データの要素を生成してもよい。

20

【0075】

予測スコア記憶部112は、予測スコア算出部111による予測結果(予測スコアの算出結果)を、予測に用いた利用者と文書の情報とともに保持する。

【0076】

図11は、予測スコア記憶部112が保持する予測結果のデータ構造の一例を示す説明図である。図11に示すように、予測スコア記憶部112は、例えば、アクセスする利用者を識別するアクセス者IDと、アクセスされたデータを識別されるアクセス文書IDとともに、算出された予測スコアを記憶してもよい。

30

【0077】

不審行動通知部113は、予測スコア記憶部112を参照し、予測スコアが閾値(例えば0.1など)より低いレコード(つまりアクセス確度が低いと予測されるレコード)を不審行動として抽出する。また、不審行動通知部113は、抽出した不審行動の対象とされた利用者のリストを、管理者等に所定の方法を用いて通知する。

【0078】

次に、本実施形態の動作について説明する。本実施形態の不審行動検知システム100の動作は、大きく、アクセス行動学習ステップ、アクセス行動予測ステップ、不審行動通知ステップ、の3つのステップに分類される。

【0079】

アクセス行動学習ステップでは、アクセス実績学習部109が、利用者属性特徴抽出部107が生成した利用者特徴ベクトルと、文書属性特徴抽出部108が生成した文書特徴ベクトルと、アクセスログ前処理部106が生成したラベル情報とに基づいて、学習データを生成し、学習データの要素間の関係性、より具体的には利用者特徴ベクトルと文書特徴ベクトルの組に対する成否ラベルの関係性を機械学習して予測モデルを生成する。また、アクセス実績学習部109は、生成した予測モデルを予測モデル記憶部110に書き込む。

40

【0080】

行動予測ステップでは、予測スコア算出部111が、指定された利用者および文書について、利用者特徴ベクトルと文書特徴ベクトルの組に対して予測モデルを適用し、当該利用者が当該文書にアクセスする確度を予測スコアとして計算する。また、予測スコア算出

50

部 1 1 1 は、算出した予測スコアを、算出に用いた利用者と文書の情報とともに予測スコア記憶部 1 1 2 に書き込む。

【 0 0 8 1 】

不審行動通知ステップでは、不審行動通知部 1 1 3 が、予測スコア記憶部 1 1 2 から、予測スコアが閾値より低いレコードを不審行動として抽出し、抽出された不審行動に関する情報のリストを出力する。

【 0 0 8 2 】

図 1 2 は、不審行動検知システム 1 0 0 のアクセス行動学習ステップの動作例を示すフローチャートである。図 1 2 に示す例では、まず、アクセス実績学習部 1 0 9 が、アクセスログ前処理部 1 0 6 を駆動し、アクセスログのうち指定した期間（つまり学習期間）のアクセス日時を有するレコードを読み出させる（ステップ S 1 0 1 ）。

10

【 0 0 8 3 】

ステップ S 1 0 1 で、アクセスログ前処理部 1 0 6 は、例えば、アクセスログ記憶部 1 0 5 より、アクセス日時が条件にマッチするレコードをアクセス実績として読み込み、正解ラベル<利用者 ID、文書 ID、正解ラベル(1)>を生成してもよい。また、アクセスログ前処理部 1 0 6 は、例えば、読み込んだレコードに含まれる利用者 ID に対して、アクセス実績のない文書 ID をランダムに選択して、不正解ラベル<利用者 ID、文書 ID、不正解ラベル(0)>を生成してもよい。

【 0 0 8 4 】

次に、アクセス実績学習部 1 0 9 は、アクセス実績の件数分、ステップ S 1 0 3 ~ ステップ S 1 0 8 の動作を繰り返す（ステップ S 1 0 2、ステップ S 1 0 9 ）。

20

【 0 0 8 5 】

ステップ S 1 0 3 では、アクセス実績学習部 1 0 9 が、利用者データ前処理部 1 0 3 を駆動し、ステップ S 1 0 1 で読み出されたアクセス実績の利用者 ID の利用者データである利用者属性情報を読み出させる。また、利用者データ前処理部 1 0 3 は、読みだされたレコードの内容（利用者属性情報）をベクトル形式に変換し、利用者ベクトルを生成する。

【 0 0 8 6 】

利用者属性情報のベクトル化（数値化）は、例えば次のように実施される。すなわち、利用者データ前処理部 1 0 3 は、利用者属性情報のうち、年齢、年齢、最終学歴、資格などの値域が予め定まっている項目であるコード項目のデータであれば、予め定めたベクトル要素の値として当該コード項目の内容が所定の範囲に該当すれば 1 とし、該当しなければ 0 としてもよい（2 値化）。

30

【 0 0 8 7 】

また、利用者データ前処理部 1 0 3 は、例えば、利用者属性情報のうち、テキスト形式の項目であるテキスト項目のデータであれば、当該テキスト項目の内容とされたテキストを形態素解析等を用いて単語に分解し、テキスト全体における単語または単語群の頻度等を計数してもよい。頻度は、一単語ごとではなく、二単語から五単語程度の単語群をひとまとめにして数えてもよい。最適な単語数は、学習対象となる利用者の数や文書の量によって異なる。また、利用者データ前処理部 1 0 3 は、例えば、計数された頻度を、当該単語または当該単語群に対応するベクトル要素の値としてもよい。

40

【 0 0 8 8 】

モデル学習ステップでは、後述する機械学習パラメータの更新時に、学習対象のデータ（文書特徴ベクトルと利用者特徴ベクトルの組）の一部を学習対象から外したデータでモデルを学習しなおして精度を検証する動作が行われる場合がある。そのとき、利用者データ前処理部 1 0 3 は、単語数を変えて検証することで、最適な単語数を定めてもよい。また、利用者データ前処理部 1 0 3 は、すべての文書において高頻度の単語、例えば助詞を除外するなど、頻度を数える対象となる単語を制限してもよい。そのようにして、テキストの特徴、つまりそのテキストを書いた利用者の特徴が表現された数値ベクトル（数値のみからなるデータ羅列）を生成する。

50

【0089】

なお、利用者がWebサイトやSNSに投稿したテキスト等も、利用者の特徴を表すデータ(数値)に変換可能である。昨今では、多くの人に興味を持った事柄について、SNSやブログ等へ書き込んでいるため、それらの情報を用いることで、利用者の特徴を多く含む数値ベクトルを生成できる。

【0090】

また、利用者データ前処理部103は、上記のテキストを数値化する方法と同様の方法で、アクセス先のURL名等を分解し、それらに含まれる単語や単語群の頻度または滞留時間をカウントしたり、URL先のHTTP文書を分解して、含まれる単語や単語群の頻度をカウントしてもよい。そのようなWebアクセス履歴に関する計数の結果も、ベクトル(数値)化できる。

10

【0091】

ステップS104では、アクセス実績学習部109が、利用者属性特徴抽出部107を駆動し、ステップS103で生成された利用者ベクトルに対して特徴抽出を行わせて、利用者特徴ベクトルを生成させる。

【0092】

一般に、ステップS103で生成される利用者ベクトルは、非常に大きいベクトル長のデータである。このため、そのままでは後段の学習および予測への適用が困難である。そこで、本実施形態では、利用者属性特徴抽出部107を用いて、利用者属性情報のうち特徴となるデータ項目のみを選択させ、データ長が圧縮されたベクトルを生成する。

20

【0093】

利用者属性特徴抽出部107は、例えば、上述した非特許文献1に記載されている方法を利用して、特徴ベクトルを生成してもよい。なお、非特許文献1に記載された方法は全て自動で特徴ベクトルを生成するが、その方法以外にも、主成分分析などにより重要なベクトル項をまず手動で分析した上で、そのようなベクトル項を指定してもよい。そのような場合、利用者属性特徴抽出部107は、そのベクトル項の内容を表現した特徴ベクトルを生成してもよい。

【0094】

ステップS105では、アクセス実績学習部109が、文書データ前処理部104を駆動して、ステップS101で読み込まれたアクセス実績の文書IDの文書データ(文書属性情報)を読み出させる。文書データ前処理部104は、文書データ記憶部102より文書IDがマッチするレコードを読み出して、ベクトル形式に変換して文書ベクトルを生成する。文書属性情報のベクトル化(数値化)は、ステップS103で示した利用者属性情報のベクトル化と同様の方法が適用可能である。

30

【0095】

ステップS106では、アクセス実績学習部109が、文書属性特徴抽出部108を駆動し、ステップS105で生成された文書ベクトルに対して特徴抽出を行って、文書特徴ベクトルを生成させる。文書ベクトルからの特徴抽出は、ステップS104で示した利用者ベクトルからの特徴抽出方法と同様の方法が適用可能である。

【0096】

ステップS107では、アクセス実績学習部109が、学習の前処理として、ステップS104で生成された利用者特徴ベクトルと、ステップS106で生成された文書特徴ベクトルのコサイン類似度を計算する。なお、本例では、2つのベクトルの類似度を測定するメトリックとしてコサイン類似度を用いているが、その他にも、任意のノルム(L1ノルム、L2ノルム、等)を用いることも可能である。

40

【0097】

ステップS108では、アクセス実績学習部109が、ステップS107で計算された類似度と、ステップS101で生成されたラベル情報とを用いて、機械学習パラメータを調整する。

【0098】

50

なお、本例では、機械学習の手段として、上述した S S I を想定しているが、任意の教師あり機械学習分類器が適用可能である。任意の教師あり機械学習分類器の例として、サポートベクタマシン、ニューラルネット、ベイズ分類器などが広く知られている。

【0099】

不審行動検知システムは、アクセス実績の件数分だけ上記の処理を繰り返すと、ステップ S 1 1 0 に進む。

【0100】

ステップ S 1 1 0 では、アクセス実績学習部 1 0 9 が、ステップ S 1 0 8 で調整された機械学習パラメータを予測モデル記憶部 1 1 0 に書き込む。

【0101】

また、図 1 3 は、不審行動検知システム 1 0 0 のアクセス行動予測ステップの動作例を示すフローチャートである。

【0102】

図 1 3 に示す例では、まず、予測スコア算出部 1 1 1 が、ステップ S 1 1 0 で書き込まれた調整済みの機械学習パラメータを予測モデル記憶部 1 1 0 から読み出す（ステップ S 2 0 1 ）。

【0103】

次に、予測スコア算出部 1 1 1 は、アクセスログ前処理部 1 0 6 を駆動し、アクセスログのうち指定した期間（予測期間）のアクセス日時を有するレコードを読み出させる（ステップ S 2 0 2 ）。ステップ S 2 0 2 で、アクセスログ前処理部 1 0 6 は、読み出したレコード群を基に、ラベル情報<利用者 ID、文書 ID、正否ラベル>のリストを生成する。以下、ここで生成されたラベル情報のリストを、アクセス行動予測対象リストと呼ぶ場合がある。

【0104】

次に、予測スコア算出部 1 1 1 は、ステップ S 2 0 2 で生成されたリストに含まれるレコードの件数分だけ、ステップ S 2 0 4 ~ ステップ S 2 0 9 の処理を繰り返す（ステップ S 2 0 3、ステップ S 2 1 0 ）。

【0105】

ステップ S 2 0 4 では、予測スコア算出部 1 1 1 が、アクセス行動予測対象リストに含まれるラベル情報を順次取り出す。そして、予測スコア算出部 1 1 1 は、利用者データ前処理部 1 0 3 を駆動し、取り出したラベル情報に含まれる利用者 ID が示す利用者の利用者データを読み出させる。ステップ S 2 0 4 で、利用者データ前処理部 1 0 3 は、指定された利用者 ID にマッチするレコード（利用者属性情報）を利用者データ記憶部 1 0 1 から読み出し、ベクトル形式に変換して利用者ベクトルを生成する。利用者属性情報のベクトル化（数値化）の方法は、ステップ S 1 0 3 で示した方法と同様でよい。

【0106】

ステップ S 2 0 5 では、予測スコア算出部 1 1 1 は、利用者属性特徴抽出部 1 0 7 を駆動して、ステップ S 2 0 4 で生成された利用者ベクトルに対して特徴抽出を行わせて利用者特徴ベクトルを生成させる。利用者ベクトルの特徴抽出の方法は、ステップ S 1 0 4 で示した方法と同様でよい。

【0107】

ステップ S 2 0 6 では、予測スコア算出部 1 1 1 は、文書データ前処理部 1 0 4 を駆動し、ステップ S 2 0 4 で取り出したラベル情報に含まれる文書 ID が示す文書の文書データを読み出させる。ステップ S 2 0 6 で、文書データ前処理部 1 0 4 は、指定された文書 ID にマッチするレコード（文書属性情報）を文書データ記憶部 1 0 2 から読み出し、ベクトル形式に変換して文書ベクトルを生成する。文書属性情報のベクトル化（数値化）の方法は、ステップ S 1 0 3 に示す方法と同様でよい。

【0108】

ステップ S 2 0 7 では、予測スコア算出部 1 1 1 は、文書属性特徴抽出部 1 0 8 を駆動し、ステップ S 2 0 6 で生成された文書ベクトルに対して特徴抽出を行わせて文書特徴ベ

10

20

30

40

50

クトルを生成させる。文書ベクトルの特徴抽出の方法は、ステップ S 1 0 4 に示す方法と同様でよい。

【 0 1 0 9 】

ステップ S 2 0 8 では、予測スコア算出部 1 1 1 は、ステップ S 2 0 5 で生成された利用者特徴ベクトルと、ステップ S 2 0 7 で生成された文書特徴ベクトルとを用いて、ステップ S 2 0 1 で読み出された機械学習パラメータに基づき、該利用者特徴ベクトルと该文書特徴ベクトルの組に対するアクセス確度を予測スコアとして算出する。既に説明したように、本例では、予測スコアを [0 . 0 ~ 1 . 0] の実数値とする。予測スコアは、例えば、サポートベクタマシンのprobability (確信度、信頼度) と呼ばれる数値であってもよい。

10

【 0 1 1 0 】

ステップ S 2 0 9 では、予測スコア算出部 1 1 1 が、ステップ S 2 0 8 で算出された予測スコアと予測スコアの算出対象とされた利用者および文書の組とともに、予測結果を予測スコア記憶部 1 1 2 に書き込む。予測スコア算出部 1 1 1 は、< 利用者 I D、文書 I D、予測スコア > の形式で予測結果を予測スコア記憶部 1 1 2 に書き込んでよい。

【 0 1 1 1 】

アクセス行動予測対象リストに含まれるレコードの件数分、上記処理を繰り返すと、当該行動予測ステップを終了する。

【 0 1 1 2 】

また、図 1 4 は、不審行動検知システム 1 0 0 の不審行動通知ステップの動作例を示すフローチャートである。

20

【 0 1 1 3 】

図 1 4 に示す例では、まず、不審行動通知部 1 1 3 が、予測結果 < 利用者 I D、文書 I D、予測スコア > のリストである予測結果リストを読み出す (ステップ S 3 0 1) 。

【 0 1 1 4 】

次に、不審行動通知部 1 1 3 は、予測結果リストに含まれる予測結果の件数分、ステップ S 3 0 3 ~ ステップ S 3 0 4 の処理を繰り返す (ステップ S 3 0 2、ステップ S 3 0 5) 。

【 0 1 1 5 】

ステップ S 3 0 3 では、不審行動通知部 1 1 3 が、ステップ S 3 0 1 で読み出されたレコードの予測スコアとあらかじめ設定した閾値 (例えば 0 . 1 など) とを比較する。ここで、読み出したレコードの予測スコアが所定の閾値未満であれば、不審行動通知部 1 1 3 は、そのレコードが示す利用者と文書の組によるアクセス行動は不審行動であると判定する (ステップ S 3 0 3 の Y e s) 。そして、不審行動通知部 1 1 3 は、ステップ S 3 0 4 に進む。一方、所定の閾値以上であれば、不審行動通知部 1 1 3 は、その組によるアクセス行動は不審行動に該当しないすなわち正常行動であると判定する (ステップ S 3 0 3 の N o) 。不審行動通知部 1 1 3 は、その後は特に処理は行わず、リストの次のレコードに処理を移すべくステップ S 3 0 3 に戻る

30

【 0 1 1 6 】

ステップ S 3 0 4 では、不審行動通知部 1 1 3 が、不審行動とされた利用者と文書の組における少なくとも利用者の情報 (利用者 I D) を、一時記憶に記憶する。なお、不審行動通知部 1 1 3 は、利用者の情報だけでなく文書の情報 (文書 I D) や算出された予測スコアなども併せて記憶してもよい。このとき、不審行動通知部 1 1 3 は、繰り返し処理により同じ情報が登録済みの場合は、再度の登録をしなくてよい。

40

【 0 1 1 7 】

予測結果リストの件数分、上記処理を完了すると、不審行動通知部 1 1 3 は、ステップ S 3 0 4 で一時記憶に登録された情報を読み出し、不審行動として管理者等に通知する (ステップ S 3 0 6) 。不審行動通知部 1 1 3 は、例えば、一時記憶に登録された情報に含まれる利用者 I D が示す利用者を、不審行動者として通知してもよい。また、不審行動通知部 1 1 3 は、例えば、一時記憶に登録された情報に含まれる文書 I D が示す文書を、通

50

常時とは異なるアクセス行動が行われている危険文書として通知してもよい。

【0118】

以上のように、本実施形態では、データにアクセスする利用者の情報である利用者データ、データそのものの情報である文書データおよびアクセスログを用いて、不審行動の予測モデルを生成し、生成された予測モデルを基に、不審行動を検知している。このため、統計ベースで生成されるモデル等と比べて、扱えるデータ量を多く出来るので、より高精度な検知が可能となる。

【0119】

変形例1

上記の実施形態では、検知した不審行動を通知するまでを実施する構成を示したが、不審行動検知システムは、不審行動が検知された利用者に対する対象データのアクセス権限の設定を自動で変更することも可能である。そのようにして、アクセス権限の穴を自動的に塞ぐことにより、ファイルサーバの利用者がデータを不正に持ち出す行為をプロアクティブに抑止することができる。

10

【0120】

図15は、本変形例による不審行動検知システムの構成例を示すブロック図である。図15に示す不審行動検知システム100は、図7に示した構成に比べて、アクセス権限制御部114、アクセス権限記憶部115をさらに備えている点で異なる。

【0121】

アクセス権限制御部114は、不審行動の検知対象とされたデータを含む所定のデータに適用されるアクセス権限の設定、変更等の制御を行う。

20

【0122】

アクセス権限記憶部115は、不審行動の検知対象とされたデータを含む所定のデータに適用される現在のアクセス権限の情報を少なくとも保持する。

【0123】

図16は、本変形例による不審行動検知システムの動作例を示すフローチャートである。本変形例では、上記の構成に比べて、さらに、アクセス権限制御ステップを含む。なお、図16は、本変形例による不審行動検知システム100のアクセス権限制御ステップの動作例を示している。

【0124】

アクセス権限制御ステップでは、アクセス行動予測ステップによる予測スコアの算出結果に基づいて検知された不審行動の情報を基に、当該不審行動を行った利用者が同様のアクセス行動を行うことができなくなるようアクセス権限を制御する。アクセス権の制御は、例えば、検知された不審行動の対象とされたデータに対して、該不審行動が検知された利用者のアクセスを禁止するものであってもよい。例えば、アクセス権限制御部114が、不審行動の情報から利用者IDと文書IDとを取得し、該利用者IDが示す利用者が該文書IDが示す文書(データ)にアクセスできなくなるよう、該文書を格納するファイルサーバのホスト名を取得してアクセス権限を設定してもよい。

30

【0125】

図16に示す例では、まず、アクセス権限制御部114が、不審行動通知部113より、検知された不審行動に関する情報を取得する(ステップS401)。

40

【0126】

次に、アクセス権限制御部114は、不審行動の対象文書を格納するファイルサーバのホスト名を取得する(ステップS402)。

【0127】

次に、アクセス権限制御部114は、不審行動者に対する当該ファイルサーバもしくは不審行動の対象文書のアクセス権限設定を変更する(ステップS403)。なお、アクセス権限設定の変更方法は、特に問わない。例えば、一般的に行われている方法を用いればよい。一例として、ディレクトリサービス(Windows(登録商標)の場合はActive DirectoryやLDAP)により管理される場合には、当該サービスを経由して、ファイルサーバ等の

50

アクセス権限設定を変更する方法が挙げられる。

【0128】

変形例2.

また、第1変形例では、検知された不審行動に基づいて、アクセス権限設定の穴を自動的に塞ぐ例を示したが、システムは、運用担当者等の特定ユーザに、不審行動の情報とともに当該不審行動にかかるアクセス権限の設定変更を提案し、応答を待った上でアクセス権限の制御を行うことも可能である。そのようにすれば、実運用において、データやファイルサーバのアクセス権限設定が自動的に変更されてしまうことで、現場の業務が混乱することを防止できる。

【0129】

図17は、本変形例の不審行動検知システムの構成例を示すブロック図である。図16に示すよう不審行動検知システム100は、図15に示した構成に比べて、アクセス権限制御画面部116をさらに備えている点で異なる。

【0130】

アクセス権限制御画面部116は、後述するアクセス権限制御画面の制御を介して、特定ユーザに、特定ユーザに、不審行動にかかるアクセス権限の設定変更を行うか否かを問い合わせる。

【0131】

図18は、アクセス権限制御画面の例を示す説明図である。図18に示すように、アクセス権限制御画面は、ユーザに、不審行動者に対する当該ファイルサーバもしくは不審行動の対象文書のアクセス権限設定として、現状のアクセス許可設定を削除する(塞ぐ)か否(見逃す)かを選択させるものであってもよい。

【0132】

また、図19は、本変形例による不審行動検知システムの動作例を示すフローチャートである。なお、図19は、本変形例による不審行動検知システム100のアクセス権限制御ステップの動作例を示している。

【0133】

図19に示す例は、図16に示した第1変形例における動作に、アクセス権限設定の制御を行うか否かの判定ステップ(ステップS501)が加わっている。

【0134】

例えば、ステップS501では、アクセス権限制御画面部116が、検知された不審行動者の利用者IDと、当該不審行動者による不審行動の対象とされた文書を格納するファイルサーバのホスト名が少なくとも表示されており、かつ、「塞ぐ」および「見逃す」ボタン等、アクセス権限の制御を行うか否かを指示するUI(ユーザインタフェース)部品を含むアクセス権限制御画面を表示してもよい。このとき、ファイルサーバの運用担当者等の特定ユーザは、画面の表示内容を確認した上で、当該人物が当該ファイルサーバにアクセスできなくなるようアクセス権限を制御するかどうかを判断すればよい。

【0135】

特定ユーザが[塞ぐ]ボタンを押下すると、アクセス権限制御画面部116は、ステップS403に進めばよい。一方、[見逃す]ボタンが押下されると、何も処理をせず終了してもよい。

【0136】

なお、不審行動が複数検知された場合は、その各々について上記の処理を行う。例えば、アクセス権限制御画面部116は、複数の不審行動の各々について、不審行動者の利用者IDと、当該不審行動者による不審行動の対象とされた文書を格納するファイルサーバのホスト名が少なくとも表示されており、かつ、「塞ぐ」および「見逃す」ボタン等、アクセス権限の制御を行うか否かを指示するUI(ユーザインタフェース)部品を含むアクセス権限制御画面を表示してもよい。

【0137】

なお、図18に示す例では、不審行動者の利用者IDと、当該不審行動者による不審行

10

20

30

40

50

動の対象文書を格納するファイルサーバのホスト名の両方を表示しているが、いずれか一方の情報のみを表示してもよい。例えば、不審行動者の利用者IDのみを取得・表示して、当該利用者IDの利用者は不審行動を行う危険性があるとし、当該利用者に対するすべてのデータのアクセスを禁止するような、アクセス権限の設定を提案してもよい。また、例えば、不審行動の対象とされた文書を格納するファイルサーバのホスト名のみを取得・表示して、当該ファイルサーバもしくは当該文書は不審行動が行われる危険性があるとし、当該ファイルサーバに対するすべての利用者のアクセスを禁止するようなアクセス権限の設定を提案してもよい。

【 0 1 3 8 】

なお、上記のアクセス権限の設定は、システムが自動設定する場合においても適用が可能である。

10

【 0 1 3 9 】

変形例 3 .

また、本実施形態および各変形例では、アクセス行動学習ステップ、アクセス行動予測ステップ、不審行動通知ステップ、の3つのステップをすべて同一装置で実施する例を示したが、ネットワーク経由で（例えば、インターネット上に公開された予測モデルの配信サーバなどから）で予測モデルを受信する構成であれば、アクセス行動学習ステップを省略することも可能である。

【 0 1 4 0 】

図 20 は、本変形例の不審行動検知システムの構成例を示すブロック図である。図 20 に示す構成は、図 7 に示す第 1 変形例の構成と比べて、上記のアクセス行動学習ステップでのみ用いられる要素（より具体的には、アクセスログ記憶部 105、アクセスログ前処理部 106 およびアクセス実績学習部 109）を省略し、新たに予測モデル受信部 117 が追加されている点が異なる。なお、これらの変更点を、例えば、他の変形例に適用することも可能である。

20

【 0 1 4 1 】

予測モデル受信部 117 は、外部から予測モデルを受信する。予測モデルは、例えば、当該システムを構成する装置以外の装置によって生成された予測モデルであってもよい。受信する予測モデルは、当該システムが不審行動の検出対象とするデータに対するアクセス行動に基づいて学習されたものでなくてもよい。例えば、稼働実績が十分あったり、アクセス権限等による情報漏えい対策が十分な他のファイルサーバ等において蓄積されたアクセスログによって示されるアクセス情報を基に学習されたものであってもよい。

30

【 0 1 4 2 】

また、図 21 は、本変形例による不審行動検知システムの動作例を示すフローチャートである。図 21 に示す例は、図 13 に示したアクセス行動予測ステップの動作例に比べて、最初の予測モデル読み出し動作（ステップ S201）が、予測モデルの受信・読み出し動作（ステップ S601）に変わっている点を除き、図 13 に示したアクセス行動予測ステップの動作と同じである。すなわち、本変形例では、予測モデルを読み出しに際し、予測モデル受信部 117 で受信した予測モデルを読み出せばよい。

【 0 1 4 3 】

例えば、ステップ S601 では、予測モデル受信部 117 は、ネットワーク経由で予測モデルを受信し、予測モデル記憶部 110 に書き込む。そして、予測スコア算出部 111 が、その予測モデルを予測モデル記憶部 110 から読み出す。

40

【 0 1 4 4 】

本変形例によれば、自システムにおけるアクセスログの蓄積が十分でない場合やモデル生成に必要な処理能力が十分でない場合等であっても、精度のよい予測モデルを用いることができる。

【 0 1 4 5 】

変形例 4 .

次に、本実施形態の第 4 変形例について説明する。これまで、学習・予測に用いる入力

50

データとして、利用者データと、文書データの2つの入力データを想定して説明をしたが、アクセス行動学習ステップおよびアクセス行動予測ステップにおいて、3つ以上の入力データ(N入力データ)を処理させることも可能である。

【0146】

例えば、利用者データとして、次の3つのデータが存在するとする。すなわち、利用者データが、(a)いわゆる属性データ(図8に示した情報等の利用者自身に関するデータ)、(b)SNS等において生成されたデータであるSNSデータ、(c)当該利用者が所定のデータに対して行ったアクセス行動に関する統計値等の統計データ、に大別されるとする。

【0147】

このような場合に、システムは、上記3つのデータ各々から、上記のベクトル化と同じ方法で利用者特徴ベクトルを生成し、生成された3つの利用者特徴ベクトルをマージ(A次元ベクトルとB次元ベクトルとC次元ベクトルと、・・・とをつなげて $A + B + C + \dots$ 次元のベクトルに合成)して、1つの利用者特徴ベクトルとすればよい。文書データに関しても同様である。

【0148】

これにより、N個の入力データであっても、利用者とデータのどちらにより由来するかによって利用者データか文書データに分類し、マージを行うことで、2入力データに落とし込むことができる。

【0149】

変形例5.

次に、本実施形態の第5変形例について説明する。本実施形態のこれまでの説明では、アクセスログの特に指定した期間(予測期間)から抽出されるアクセス行動における<利用者ID、文書ID>の組に対して、不審行動か否かを判定した。しかし、予想対象とするアクセス行動は、このようなアクセスログによって示されるものに限定されない。例えば、実際に行われたアクセス行動に対してだけでなく、事前に、危険文書や危険利用者を予測することも可能である。ここで、危険文書は、ある特定の利用者または利用者群にとって不審行動の対象となりやすい文書または文書群、より具体的には当該特定の利用者または利用者群がアクセスする可能性の低い文書または文書群をいう。また、危険利用者は、ある特定のデータまたはデータ群にとって不審行動の主体となりやすい利用者または利用者群、より具体的には当該特定のデータまたはデータ群にアクセスする可能性の低い利用者または利用者群をいう。危険文書や危険利用者を予め予測することにより、例えば、危険文書への特定利用者によるアクセスや、危険利用者による特定文書へのアクセスをあらかじめ制限する等の事前予防を実施できる。

【0150】

本変形例における危険利用者の予測方法は、例えば、アクセス行動予測ステップのステップS202で、アクセス行動予測対象リストを生成する際に、検査対象の利用者の利用者ID(特定利用者ID)に対して全ての文書IDを組み合わせたものを、アクセス行動予測対象リストに含ませればよい。なお、予測に用いる入力データとして、利用者IDおよび文書IDから得られる情報以外の情報(例えば、アクセス時間帯等)を含む場合には、特定利用者IDに対して利用者データ以外の入力データが取り得る全ての値のパターンを組み合わせたものを、アクセス行動予測対象リストに含ませればよい。

【0151】

そして、そのようにして生成したアクセス行動予測対象リストを用いて、ステップS203以降を実行すればよい。その結果、1つでも不審行動と判定された組があれば、その組に含まれる特定利用者IDが示す利用者を、少なくともその組が示すアクセス行動における危険利用者とし、みなしてもよい。

【0152】

同様に、本変形例における危険文書を予測するには、例えば、アクセス行動予測ステップのステップS202で、アクセス行動予測対象リストを生成する際に、検査対象の文書

10

20

30

40

50

の文書ID（特定文書ID）に対して全ての利用者IDを組み合わせたものを、アクセス行動予測対象リストに含ませればよい。なお、予測に用いる入力データとして、利用者IDおよび文書IDから得られる情報以外の情報（例えば、アクセス時間帯等）を含む場合、該特定文書IDに対して文書データ以外の入力データが取り得る全ての値のパターンを組み合わせたものを、アクセス行動予測対象リストに含ませればよい。

【0153】

そして、そのようにして生成したアクセス行動予測対象リストを用いて、ステップS203以降を実行すればよい。その結果、1つでも不審行動と判定された組があれば、その組に含まれる特定文書IDが示す文書を、少なくともその組が示すアクセス行動における危険文書とみなしてもよい。

10

【0154】

また、システムは、危険利用者や危険文書が検出された場合、不審行動通知ステップの動作を実行してもよい。

【0155】

以上、本実施形態および実施例を参照して本願発明を説明したが、本願発明は上記実施形態および実施例に限定されるものではない。本願発明の構成や詳細には、本願発明のスコープ内で当業者が理解し得る様々な変更をすることができる。

【0156】

例えば、本願発明の特徴の1つは、データアクセスに関する過去の利用者の行動を示すデータをもとに、機械学習を行い、未知のデータアクセス行動に対して不審行動か否かを判定する点にある。上記の説明の多くでは、2入力（アクセスログから得られる、利用者データと文書データの1対1の組合せ）に対して成否のラベルを付けて学習を行う例を示している。しかし、本願発明の目的の1つとして、機械学習による行動ベースのアクセス制御ができればよいので、学習に用いる入力は上記に限られない。また、監視対象も、一企業等の情報システム部門で管理されるようなファイルサーバに限られない。

20

【0157】

入力データに含まれるとして好ましい項目の一例として、データアクセス行動に関する下記の5W1Hに相当する情報が挙げられる。

【0158】

WHO：利用者のプロフィール（氏名、年齢、役職、職務、健康状態、上司評価、など）

30

WHEN：利用者がデータにアクセスした日時（平日、休日、日中、夜間、など）

WHERE：利用者がデータにアクセスした場所（ファイルサーバ、データベース、SNS、など）

WHAT：利用者がアクセスしたデータ（タイトル、プロパティ、内容、など）

WHY：利用者がデータにアクセスした理由（読込、書込、コピー、削除、など）

HOW：利用者がデータにアクセスした方法（アクセス端末、アクセス経路、など）

【0159】

また、例えば、第2の実施形態において利用者データ前処理部103や文書データ前処理部104が生成するベクトルの次元数がそれほど大きくない場合は、特徴抽出部（利用者属性特徴抽出部107、文書属性特徴抽出部108）を省略してもよい。

40

【0160】

また、上記の各実施形態は以下の付記のようにも記載できる。

【0161】

（付記1）データに対する利用者の行動であるデータアクセス行動に関するアクセス情報であって、データにアクセスする利用者に由来する第1の情報と、アクセスされるデータに由来する第2の情報とを含むアクセス情報と、不審行動または正常行動との関係を示すアクセス行動モデルを記憶するモデル記憶手段と、アクセス行動モデルに基づいて、任意のデータアクセス行動が不審行動であるか否かを判定する判定手段とを備えたことを特徴とする情報処理装置。

【0162】

50

(付記2) アクセス情報は、第1の情報として、アクセスする利用者、アクセスされる時間、アクセス種別もしくはアクセス方法に関する情報を含む、または、第2の情報として、データ自体もしくはデータの格納場所に関する情報を含む付記1に記載の情報処理装置。

【0163】

(付記3) アクセス情報は、アクセスする利用者に関する情報として、当該利用者が生成したテキストに関する情報もしくは当該利用者が所定のデータに対して行ったアクセス行動に関する統計値を含む、または、データ自体に関する情報として、当該データの内容に関する情報もしくは当該データに対して行われたアクセス行動に関する統計値を含む付記2に記載の情報処理装置。

10

【0164】

(付記4) アクセス情報と、アクセス情報が示すデータアクセス行動が不審行動であるか否かを示す情報とを学習データに用いて、機械学習によりアクセス行動モデルを生成する学習手段を備えた付記1から付記3のうちのいずれかに記載の情報処理装置。

【0165】

(付記5) ファイルサーバによって管理されているファイルを、対象データとする情報処理装置であって、モデル記憶手段は、所定のファイルに対するアクセス履歴に含まれるアクセス行動のうち指定された期間におけるアクセス行動に関するアクセス情報と、アクセス行動が不審行動か否かを判別可能な情報とを用いて機械学習されたアクセス行動モデルを記憶する付記1から付記4のうちのいずれかに記載の情報処理装置。

20

【0166】

(付記6) アクセス情報から、各々が多次元の数値からなる2以上の数値ベクトルを生成する数値ベクトル生成手段を備え、モデル記憶手段は、2以上の数値ベクトルの組と、不審行動または正常行動との関係を示すアクセス行動モデルとの関係を示すアクセス行動モデルを記憶し、判定手段は、アクセス行動モデルを用いて算出される、指定されたアクセス情報から生成される2以上の数値ベクトルの組に対する不審行動または正常行動の確度に基づいて、アクセス情報によって示されるデータアクセス行動が不審行動であるか否かを判定する付記1から付記5のうちのいずれかに記載の情報処理装置。

【0167】

(付記7) 数値ベクトル生成手段として、アクセス情報に含まれる第1情報から、多次元の数値からなる第1数値ベクトルを生成する第1数値ベクトル生成手段と、アクセス情報に含まれる第2情報から、多次元の数値からなる第2数値ベクトルを生成する第2数値ベクトル生成手段とを備え、モデル記憶手段は、第1数値ベクトルと第2数値ベクトルとの組と、不審行動または正常行動との関係を示すアクセス行動モデルを記憶し、判定手段は、アクセス行動モデルを用いて算出される、指定されたアクセス情報に含まれる第1情報および第2情報から生成される第1数値ベクトルと第2数値ベクトルの組に対する不審行動または正常行動の確度に基づいて、アクセス情報によって示されるデータアクセス行動が不審行動であるか否かを判定する付記6に記載の情報処理装置。

30

【0168】

(付記8) アクセス行動モデルに基づいて、不審行動に該当するアクセス行動が行われる危険性があるデータを予測する危険データ予測手段を備えた付記1から付記7のうちのいずれかに記載の情報処理装置。

40

【0169】

(付記9) アクセス行動モデルに基づいて、不審行動に該当するデータアクセス行動を行う危険性がある利用者を予測する危険利用者予測手段を備えた付記1から付記8のうちのいずれかに記載の情報処理装置。

【0170】

(付記10) 判定手段による判定結果に基づいて、アクセス権限を変更するアクセス権限変更手段を備えた付記1から付記9のうちのいずれかに記載の情報処理装置。

【0171】

50

(付記 1 1) 判定手段による判定結果を基に、実際に行われたデータアクセス行動から不審行動を検知する不審行動検知手段と、不審行動が検知されると、管理者に通知を行う通知手段とを備えた付記 1 から付記 1 0 のうちのいずれかに記載の情報処理装置。

【 0 1 7 2 】

(付記 1 2) データに対する利用者の行動であるデータアクセス行動に関するアクセス情報であって、データにアクセスする利用者に由来する第 1 の情報と、アクセスされるデータに由来する第 2 の情報とを含むアクセス情報と、アクセス情報が示すデータアクセス行動が不審行動か否かを判別可能な情報とを学習データに用いて、機械学習により、任意のアクセス情報と不審行動または正常行動との関係を示すアクセス行動モデルを生成する学習手段と、アクセス行動モデルを記憶するモデル記憶手段と、アクセス行動モデルに基づいて、任意のデータアクセス行動が不審行動であるか否かを判定する判定手段と、判定結果を基に、実際に行われたデータアクセス行動から不審行動を検知する不審行動検知手段とを備えたことを特徴とする不審行動検知システム。

10

【 0 1 7 3 】

(付記 1 3) 情報処理装置が、データに対する利用者の行動であるデータアクセス行動に関するアクセス情報であって、データにアクセスする利用者に由来する第 1 の情報と、アクセスされるデータに由来する第 2 の情報とを含むアクセス情報と、不審行動または正常行動との関係を示すアクセス行動モデルに基づいて、任意のデータアクセス行動が不審行動であるか否かを判定することを特徴とする不審行動検知方法。

20

【 0 1 7 4 】

(付記 1 4) コンピュータに、データに対する利用者の行動であるデータアクセス行動に関するアクセス情報であって、データにアクセスする利用者に由来する第 1 の情報と、アクセスされるデータに由来する第 2 の情報とを含むアクセス情報と、不審行動または正常行動との関係を示すアクセス行動モデルに基づいて、任意のデータアクセス行動が不審行動であるか否かを判定させる処理を実行させるための不審行動検知プログラム。

【 0 1 7 5 】

この出願は、2015年10月13日に出願された日本特許出願2015-202280を基礎とする優先権を主張し、その開示の全てをここに取り込む。

【産業上の利用可能性】

30

【 0 1 7 6 】

本発明は、入力データから利用者およびデータに関する特徴量を抽出してモデル学習を行う特徴から、例えば、不審行動の検知に高い精度を有する予測モデルのみを提供するといったビジネスモデルも考えられる。

【符号の説明】

【 0 1 7 7 】

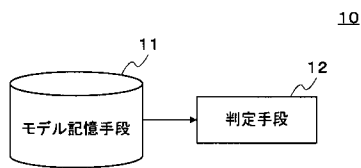
- 1 0、1 0 0 不審行動検知システム
- 1 1 モデル記憶手段
- 1 2 判定手段
- 1 3 学習手段
- 1 4 不審行動検知手段
- 1 5 通知手段
- 1 6 数値ベクトル生成手段
- 1 6 1 第 1 数値ベクトル生成手段
- 1 6 2 第 2 数値ベクトル生成手段
- 1 7 危険利用者予測手段
- 1 8 危険データ予測手段
- 1 9 アクセス権限変更手段
- 1 0 1 利用者データ記憶部
- 1 0 2 文書データ記憶部
- 1 0 3 利用者データ前処理部

40

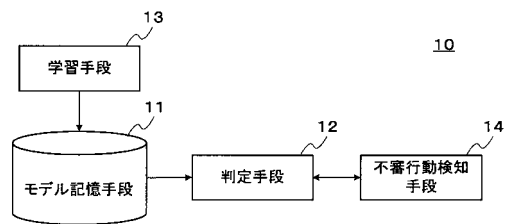
50

- 1 0 4 文書データ前処理部
- 1 0 5 アクセスログ記憶部
- 1 0 6 アクセスログ前処理部
- 1 0 7 利用者属性特徴抽出部
- 1 0 8 文書属性特徴抽出部
- 1 0 9 アクセス実績学習部
- 1 1 0 予測モデル記憶部
- 1 1 1 予測スコア算出部
- 1 1 2 予測スコア記憶部
- 1 1 3 不審行動通知部
- 1 1 4 アクセス権限制御部
- 1 1 5 アクセス権限記憶部
- 1 1 6 アクセス権限制御画面部
- 1 1 7 予測モデル受信部

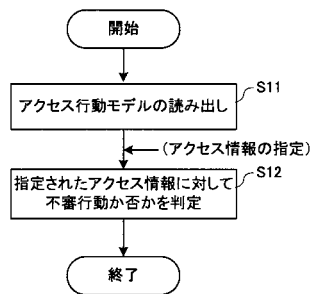
【 図 1 】



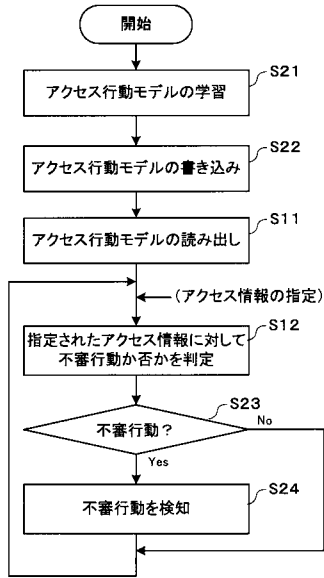
【 図 3 】



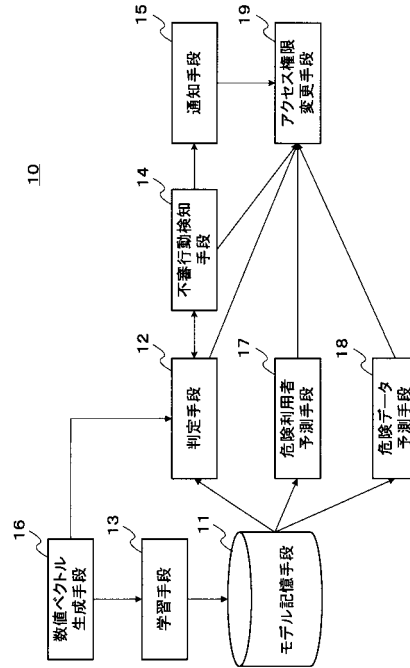
【 図 2 】



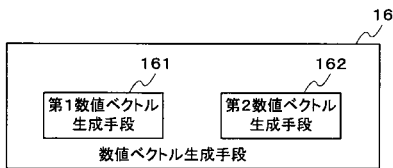
【 図 4 】



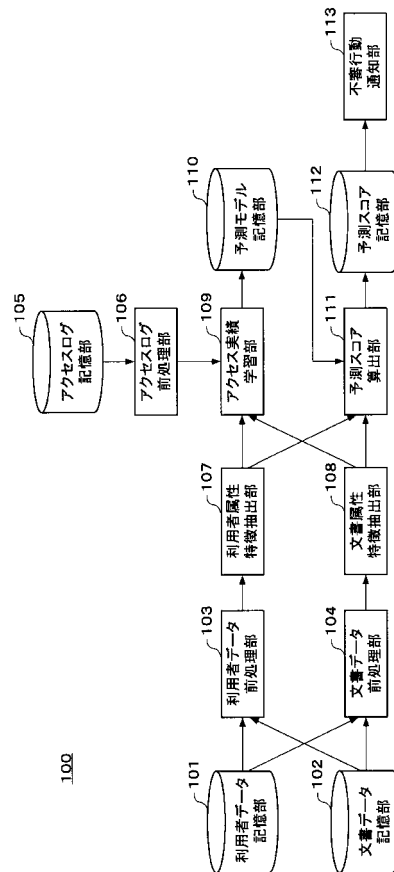
【 図 5 】



【 図 6 】



【 図 7 】



【 図 8 】

利用者ID	氏名	年齢	性別	役職	担当業務	業績評価	キャリア面接結果
U01	山田 一郎	22	男	担当	開発	A	現在の担当業務にやりがいを感じている。
U02	山下 花子	28	女	担当	営業	S	強い情熱を持って、担当業務に取り組んでいる。
U03	山本 二郎	48	男	前長	経理 財務	C	近年、担当業務一筋でマンネリ化。専門スキルを活かしてキャリアチェンジを志向。30歳の節目に強腰に転職して以来、担当業務一筋。日々楽しく業務している。
U04	松田 三郎	36	男	課長	法務	A	30歳の節目に係長に昇格。仕事の量も増えて毎日忙しく仕事をこなしている。
U05	松下 紀子	30	女	係長	知財	B	

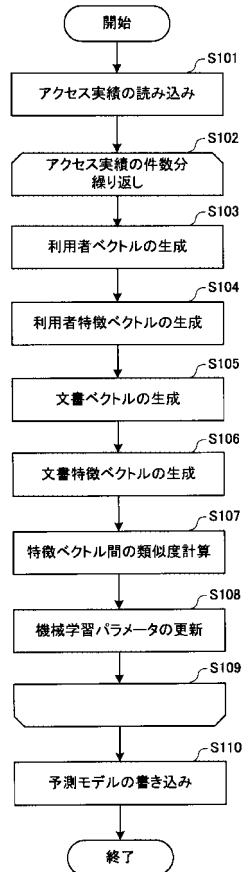
【 図 9 】

文書ID	文書種別	アクセス権	作成日時	更新日時	文書内容
D01	営業資料	営業職かつ担当以上は閲覧可能	2015/04/01	2015/05/01	顧客であるA社向けの営業リーフレットです。...
D02	技術資料	技術職かつ担当以上は閲覧可能	2013/04/01	2015/04/01	2015年6月リリースのB製品の基本設計書です。...
D03	決算資料	財務職かつ担当以上は閲覧可能	2000/01/01	2015/03/30	2014年度の決算報告書です。企業秘密です。...
D04	顧客資料	前長以上は閲覧可能	2000/01/01	2015/05/18	顧客一覧を言ひます。企業秘密、取扱注意です。...
D05	広報資料	担当以上は閲覧可能	2014/02/01	2014/04/01	2014年4月に社外公表した広報資料です。...

【 図 1 0 】

アクセス利用者ID	アクセス文書ID	アクセス日時
U01	D02	2015/05/16
U02	D01	2015/05/16
U03	D03	2015/05/16
U04	D05	2015/05/16
U01	D02	2015/05/17
U02	D01	2015/05/17
U03	D03	2015/05/17
U04	D05	2015/05/17
U01	D02	2015/05/18
U02	D01	2015/05/18
U03	D04	2015/05/18
U04	D05	2015/05/18

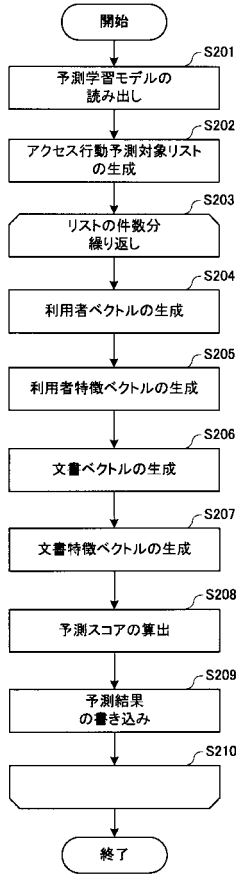
【 図 1 2 】



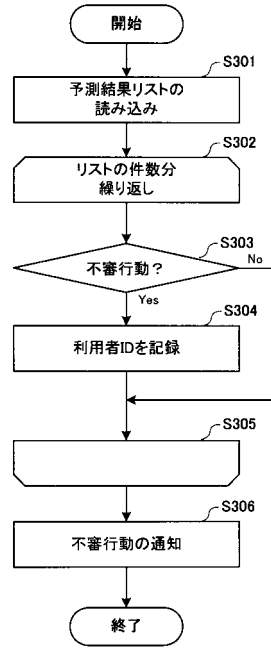
【 図 1 1 】

アクセス者ID	アクセス文書ID	予測スコア
U01	D02	0.9
U02	D01	0.8
U03	D04	0.1
U04	D05	0.7

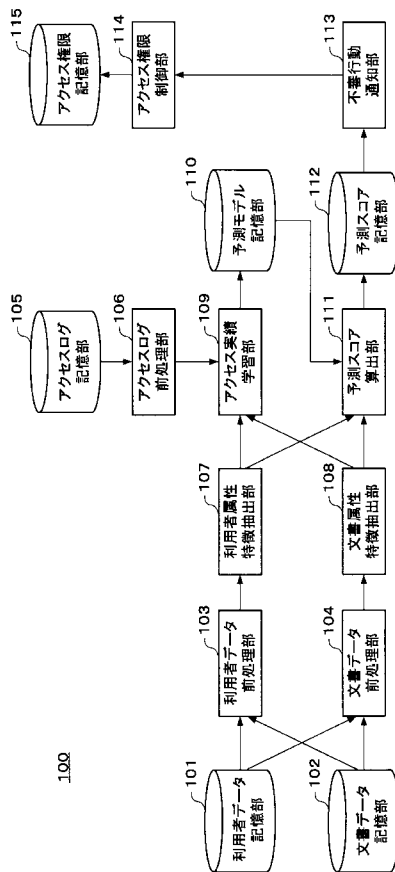
【図13】



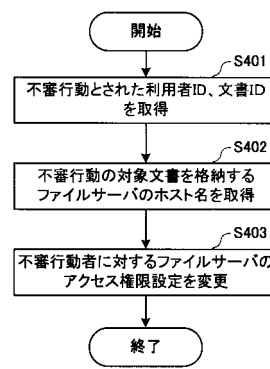
【図14】



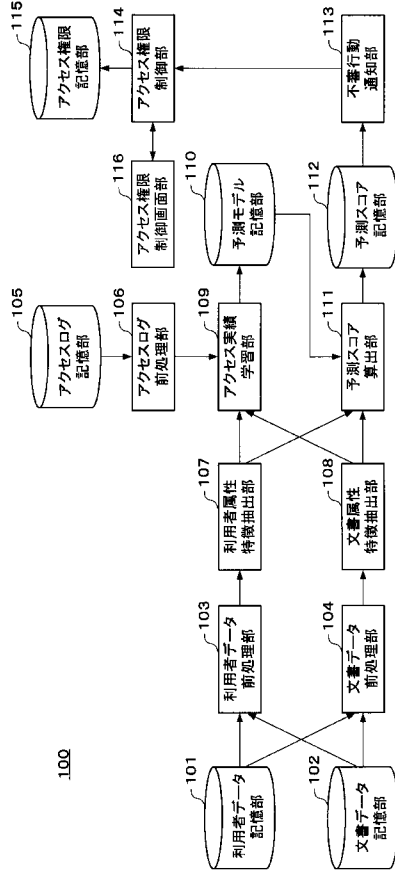
【図15】



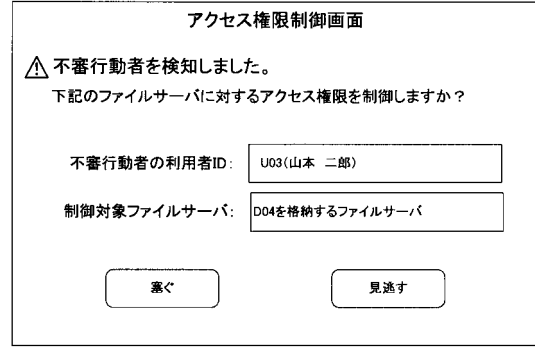
【図16】



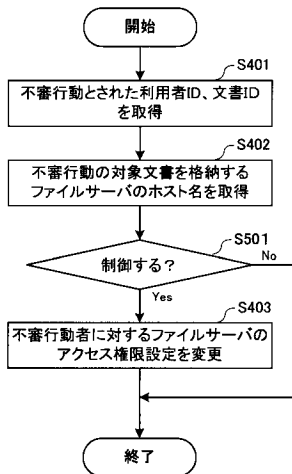
【図17】



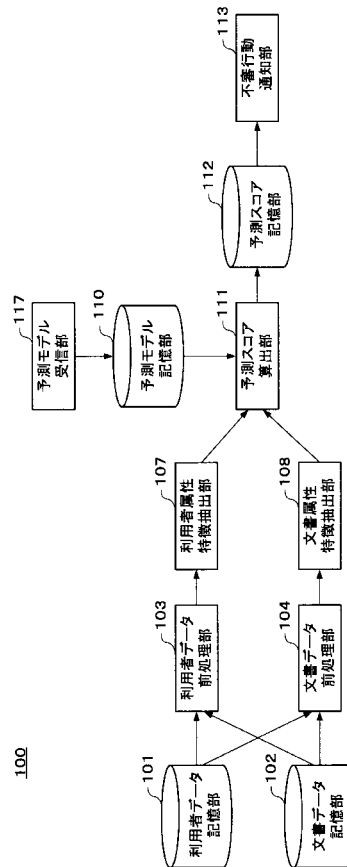
【図18】



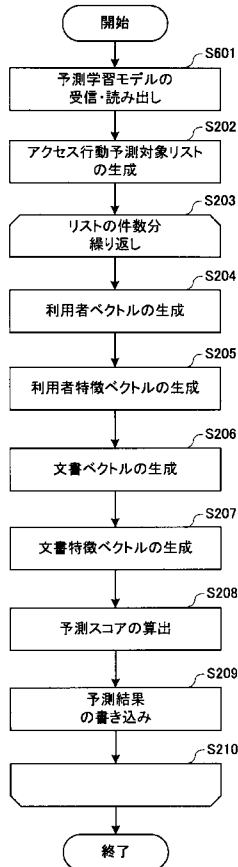
【図19】



【図20】



【 図 2 1 】



【 手続補正書 】

【 提出日 】平成30年4月4日 (2018.4.4)

【 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 】

データに対する利用者の行動であるデータアクセス行動に関するアクセス情報であって、データにアクセスする利用者由来の第1の情報と、アクセスされるデータ由来の第2の情報とを含むアクセス情報と、不審行動または正常行動との関係を示すアクセス行動モデルを記憶するモデル記憶手段と、

前記アクセス行動モデルに基づいて、任意のデータアクセス行動が不審行動であるか否かを判定する判定手段とを備えた

ことを特徴とする情報処理装置。

【 請求項 2 】

アクセス情報は、第1の情報として、アクセスする利用者、アクセスされる時間、アクセス種別もしくはアクセス方法に関する情報を含む、または、第2の情報として、データ自体もしくはデータの格納場所に関する情報を含む

請求項1に記載の情報処理装置。

【 請求項 3 】

アクセス情報は、アクセスする利用者に関する情報として、当該利用者が生成したテキストに関する情報もしくは当該利用者が所定のデータに対して行ったアクセス行動に関する統計値を含む、または、データ自体に関する情報として、当該データの内容に関する情

報もしくは当該データに対して行われたアクセス行動に関する統計値を含む

請求項 2 に記載の情報処理装置。

【請求項 4】

アクセス情報と、前記アクセス情報が示すデータアクセス行動が不審行動であるか否かを示す情報とを学習データに用いて、機械学習によりアクセス行動モデルを生成する学習手段を備えた

請求項 1 から請求項 3 のうちのいずれか 1 項に記載の情報処理装置。

【請求項 5】

ファイルサーバによって管理されているファイルを、対象データとする情報処理装置であって、

モデル記憶手段は、所定のファイルに対するアクセス履歴に含まれるアクセス行動のうち指定された期間におけるアクセス行動に関するアクセス情報と、前記アクセス行動が不審行動か否かを判別可能な情報とを用いて機械学習されたアクセス行動モデルを記憶する

請求項 1 から請求項 4 のうちのいずれか 1 項に記載の情報処理装置。

【請求項 6】

アクセス情報から、各々が多次元の数値からなる 2 以上の数値ベクトルを生成する数値ベクトル生成手段を備え、

モデル記憶手段は、前記 2 以上の数値ベクトルの組と、不審行動または正常行動との関係を示すアクセス行動モデルとの関係を示すアクセス行動モデルを記憶し、

判定手段は、前記アクセス行動モデルを用いて算出される、指定されたアクセス情報から生成される 2 以上の数値ベクトルの組に対する不審行動または正常行動の確度に基づいて、前記アクセス情報によって示されるデータアクセス行動が不審行動であるか否かを判定する

請求項 1 から請求項 5 のうちのいずれか 1 項に記載の情報処理装置。

【請求項 7】

数値ベクトル生成手段として、

アクセス情報に含まれる第 1 情報から、多次元の数値からなる第 1 数値ベクトルを生成する第 1 数値ベクトル生成手段と、

アクセス情報に含まれる第 2 情報から、多次元の数値からなる第 2 数値ベクトルを生成する第 2 数値ベクトル生成手段とを備え、

モデル記憶手段は、前記第 1 数値ベクトルと前記第 2 数値ベクトルとの組と、不審行動または正常行動との関係を示すアクセス行動モデルを記憶し、

判定手段は、前記アクセス行動モデルを用いて算出される、指定されたアクセス情報に含まれる第 1 情報および第 2 情報から生成される前記第 1 数値ベクトルと前記第 2 数値ベクトルの組に対する不審行動または正常行動の確度に基づいて、前記アクセス情報によって示されるデータアクセス行動が不審行動であるか否かを判定する

請求項 6 に記載の情報処理装置。

【請求項 8】

アクセス行動モデルに基づいて、不審行動に該当するアクセス行動が行われる危険性があるデータを予測する危険データ予測手段を備えた

請求項 1 から請求項 7 のうちのいずれか 1 項に記載の情報処理装置。

【請求項 9】

アクセス行動モデルに基づいて、不審行動に該当するデータアクセス行動を行う危険性がある利用者を予測する危険利用者予測手段を備えた

請求項 1 から請求項 8 のうちのいずれか 1 項に記載の情報処理装置。

【請求項 10】

判定手段による判定結果に基づいて、アクセス権限を変更するアクセス権限変更手段を備えた

請求項 1 から請求項 9 のうちのいずれか 1 項に記載の情報処理装置。

【 国際調査報告 】

INTERNATIONAL SEARCH REPORT		International application No. PCT/JP2016/079637
A. CLASSIFICATION OF SUBJECT MATTER G06F21/55(2013.01)i, G06F21/62(2013.01)i, G06N99/00(2010.01)i According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) G06F21/55, G06F21/62, G06N99/00 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2016 Kokai Jitsuyo Shinan Koho 1971-2016 Toroku Jitsuyo Shinan Koho 1994-2016 Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP 2008-158959 A (Sky Co., Ltd.), 10 July 2008 (10.07.2008), paragraphs [0016] to [0028]; fig. 1 to 4 (Family: none)	1-3, 6-7, 10-11, 13-14 4-5, 12 8-9
X Y A	JP 2010-9239 A (The Kansai Electric Power Co., Inc.), 14 January 2010 (14.01.2010), claim 1; paragraphs [0015] to [0039]; fig. 1 to 4 (Family: none)	1-3, 9, 13-14 4-5, 12 6-8, 10-11
Y A	JP 2004-312083 A (KDDI Corp.), 04 November 2004 (04.11.2004), paragraphs [0016] to [0035]; fig. 1 to 4 (Family: none)	4-5, 12 6-11
<input checked="" type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> 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 31 October 2016 (31.10.16)		Date of mailing of the international search report 08 November 2016 (08.11.16)
Name and mailing address of the ISA/ Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan		Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2016/079637

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-148276 A (Fujitsu Ltd.), 26 May 2000 (26.05.2000), claims 1, 7; paragraphs [0017] to [0027] & EP 999490 A2 paragraphs [0019] to [0030]	3
A	JP 2011-138298 A (NTT Data Corp.), 14 July 2011 (14.07.2011), paragraphs [0018] to [0027] (Family: none)	8

国際調査報告		国際出願番号 PCT/J P 2 0 1 6 / 0 7 9 6 3 7									
A. 発明の属する分野の分類 (国際特許分類 (IPC)) Int.Cl. G06F21/55(2013.01)i, G06F21/62(2013.01)i, G06N99/00(2010.01)i											
B. 調査を行った分野 調査を行った最小限資料 (国際特許分類 (IPC)) Int.Cl. G06F21/55, G06F21/62, G06N99/00											
最小限資料以外の資料で調査を行った分野に含まれるもの <table border="0"> <tr> <td>日本国実用新案公報</td> <td>1922-1996年</td> </tr> <tr> <td>日本国公開実用新案公報</td> <td>1971-2016年</td> </tr> <tr> <td>日本国実用新案登録公報</td> <td>1996-2016年</td> </tr> <tr> <td>日本国登録実用新案公報</td> <td>1994-2016年</td> </tr> </table>				日本国実用新案公報	1922-1996年	日本国公開実用新案公報	1971-2016年	日本国実用新案登録公報	1996-2016年	日本国登録実用新案公報	1994-2016年
日本国実用新案公報	1922-1996年										
日本国公開実用新案公報	1971-2016年										
日本国実用新案登録公報	1996-2016年										
日本国登録実用新案公報	1994-2016年										
国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)											
C. 関連すると認められる文献											
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号									
X Y A	JP 2008-158959 A (S k y株式会社) 2008.07.10, 段落 [0016]-[0028], 図 1-4 (ファミリーなし)	1-3, 6-7, 10-1 1, 13-14 4-5, 12 8-9									
X Y A	JP 2010-9239 A (関西電力株式会社) 2010.01.14, 請求項 1, 段落 [0015]-[0039], 図 1-4 (ファミリーなし)	1-3, 9, 13-14 4-5, 12 6-8, 10-11									
<input checked="" type="checkbox"/> C欄の続きにも文献が列挙されている。 <input type="checkbox"/> パテントファミリーに関する別紙を参照。											
* 引用文献のカテゴリー		の日の後に公表された文献									
「A」特に関連のある文献ではなく、一般的技術水準を示すもの		「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの									
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの		「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの									
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)		「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの									
「O」口頭による開示、使用、展示等に言及する文献		「&」同一パテントファミリー文献									
「P」国際出願日前で、かつ優先権の主張の基礎となる出願											
国際調査を完了した日 31.10.2016		国際調査報告の発送日 08.11.2016									
国際調査機関の名称及びあて先 日本国特許庁 (ISA/J P) 郵便番号100-8915 東京都千代田区霞が関三丁目4番3号		特許庁審査官 (権限のある職員) 宮司 卓佳	5 S 6 2 9 3								
		電話番号 03-3581-1101 内線 3546									

国際調査報告		国際出願番号 PCT/J P 2 0 1 6 / 0 7 9 6 3 7
C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
Y A	JP 2004-312083 A (KDD I 株式会社) 2004. 11. 04, 段落 [0016]-[0035], 図 1-4 (ファミリーなし)	4-5, 12 6-11
A	JP 2000-148276 A (富士通株式会社) 2000. 05. 26, 請求項 1, 7, 段落 [0017]-[0027] & EP 999490 A2, 段落[0019]-[0030]	3
A	JP 2011-138298 A (株式会社エヌ・ティ・ティ・データ) 2011. 07. 14, 段落[0018]-[0027] (ファミリーなし)	8

フロントページの続き

(81)指定国 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, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG), AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA

(注) この公表は、国際事務局(WIPO)により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願(日本語実用新案登録出願)の国際公開の効果は、特許法第184条の10第1項(実用新案法第48条の13第2項)により生ずるものであり、本掲載とは関係ありません。