(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2017-107512
(P2017-107512A)
(43)公開日　平成29年6月15日(2017.6.15)

(51)Int.Cl.		F I			テーマコード（参考）
G06Q 50/10	(2012.01)	G06Q	50/10		5L049
		G06Q	50/10	100	

審査請求 未請求　請求項の数 7　OL　（全 15 頁）

(21)出願番号　特願2015-242682 (P2015-242682)
(22)出願日　平成27年12月11日 (2015.12.11)

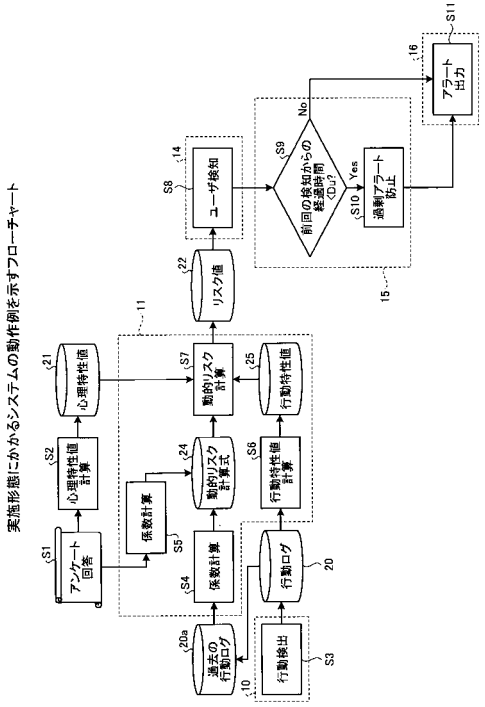
（出願人による申告）平成２７年度、総務省、「サイバー攻撃の解析・検知に関する研究開発」研究開発委託契約に基づく開発項目「利用者の行動特性に基づくサイバー攻撃検知技術の研究開発」委託研究、産業技術力強化法第１９条の適用を受ける特許出願

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　110002147
特許業務法人酒井国際特許事務所
(72)発明者　寺田　剛陽
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　津田　宏
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　鳥居　悟
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】リスク算定方法、リスク算定プログラムおよびリスク算定装置

(57)【要約】
【課題】アラートの精度を高めることを可能とする。
【解決手段】実施形態のリスク算定方法は、ユーザに特徴的な心理特性を示す心理特性情報と、ユーザの行動履歴が記録された履歴情報のうち所定期間における行動履歴から求めた所定期間においてユーザに特徴的な行動特性を示す行動特性情報とに基づいて、リスク値を計算する処理をコンピュータが実行する。また、リスク算定方法は、計算したリスク値が所定の基準値を超過したユーザについてアラートを出力する処理をコンピュータが実行する。
【選択図】図２



【特許請求の範囲】
【請求項１】
ユーザに特徴的な心理特性を示す心理特性情報と、前記ユーザの行動履歴が記録された履歴情報のうち所定期間における行動履歴から求めた該所定期間において前記ユーザに特徴的な行動特性を示す行動特性情報とに基づいて、リスク値を計算し、
計算した前記リスク値が所定の基準値を超過したユーザについてアラートを出力する
処理をコンピュータが実行することを特徴とするリスク算定方法。
【請求項２】
前記アラートを出力する処理は、計算した前記リスク値が所定の基準値を超過したユーザについて、直近にアラートを出力してからの経過時間が所定時間内である場合にはアラートの出力を抑制する
ことを特徴とする請求項１に記載のリスク算定方法。
【請求項３】
前記アラートを出力する処理は、計算した前記リスク値が前記ユーザの複数の期間について計算した前記リスク値の度数分布において上位の所定範囲に属する場合に前記アラートを出力する
ことを特徴とする請求項１または２に記載のリスク算定方法。
【請求項４】
複数のユーザごとに計算したリスク値の集計結果をもとに前記基準値を算出する処理をコンピュータが更に実行し、
前記アラートを出力する処理は、計算した前記リスク値が前記算出された基準値を超過したユーザについてアラートを出力する
ことを特徴とする請求項１乃至３のいずれか一項に記載のリスク算定方法。
【請求項５】
前記計算する処理は、前記行動履歴に含まれる前記ユーザの入力間隔、削除キーの操作回数および操作対象とするウインドウ画面の切り替え回数のうちの少なくとも１つの値をもとに前記行動特性情報を求める
ことを特徴とする請求項１乃至４のいずれか一項に記載のリスク算定方法。
【請求項６】
ユーザに特徴的な心理特性を示す心理特性情報と、前記ユーザの行動履歴が記録された履歴情報のうち所定期間における行動履歴から求めた該所定期間において前記ユーザに特徴的な行動特性を示す行動特性情報とに基づいて、リスク値を計算し、
計算した前記リスク値が所定値を超過したユーザについてアラートを出力する
処理をコンピュータに実行させることを特徴とするリスク算定プログラム。
【請求項７】
ユーザに特徴的な心理特性を示す心理特性情報と、前記ユーザの行動履歴が記録された履歴情報のうち所定期間における行動履歴から求めた該所定期間において前記ユーザに特徴的な行動特性を示す行動特性情報とに基づいて、リスク値を計算するリスク計算部と、
計算した前記リスク値が所定値を超過したユーザについてアラートを出力する出力部と
を有することを特徴とするリクス算定装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、リスク算定方法、リスク算定プログラムおよびリスク算定装置に関する。
【背景技術】
【０００２】
従来、各種サービスをユーザに提供する業務用又は商用のシステムにおいては、ユーザがクラッキングの被害を受けないように、ユーザに対してアラートを出力することで、システムのセキュリティを向上させている。ユーザに対してアラートの出力を行う技術とし

ては、ユーザの自信度（自己評価）に基づいた支援情報を提供する技術が知られている。なお、クラッキングの被害については、例えば標準型攻撃メールによるものがあり、以下の説明ではＩＴ被害と呼ぶものとする。

【先行技術文献】

【特許文献】

【０００３】

【特許文献１】特開平２－２０８７１０号公報

【特許文献２】特開２００９－１３４４９６号公報

【特許文献３】特開２０１５－１７６３７５号公報

【発明の概要】

【発明が解決しようとする課題】

【０００４】

しかしながら、上述した従来技術では、ユーザの自信度（自己評価）という時間的に変化のない静的なファクター（要因）をもとにアラートの出力を行うため、アラートの精度が低いという問題がある。

【０００５】

例えば、ＩＴ被害に対するリスクには、昼過ぎの眠くなる時間帯などの時間帯で異なる個人の行動や、午前または午後で変化する業務内容など、時間によって動的に変化する要因がある。しかしながら、時間的に変化のない静的な要因によってアラートを出力する場合には、時間帯に関係なくアラートが出続けることがあり、時間によって動的に変化するリスクに対応することが困難である。

【０００６】

１つの側面では、アラートの精度を高めることを可能とするリスク算定方法、リスク算定プログラムおよびリスク算定装置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】

【０００７】

第１の案では、リスク算定方法は、ユーザに特徴的な心理特性を示す心理特性情報と、ユーザの行動履歴が記録された履歴情報のうち所定期間における行動履歴から求めた所定期間においてユーザに特徴的な行動特性を示す行動特性情報とに基づいて、リスク値を計算する処理をコンピュータが実行する。また、リスク算定方法は、計算したリスク値が所定の基準値を超過したユーザについてアラートを出力する処理をコンピュータが実行する。

【発明の効果】

【０００８】

本発明の１実施態様によれば、アラートの精度を高めることができる。

【図面の簡単な説明】

【０００９】

【図１】図１は、実施形態にかかるシステムの構成例を示すブロック図である。

【図２】図２は、実施形態にかかるシステムの動作例を示すフローチャートである。

【図３】図３は、リスク値の時間的変化を説明する説明図である。

【図４】図４は、リスク値の時間的変化を説明する説明図である。

【図５】図５は、リスク値の度数分布を説明する説明図である。

【図６】図６は、リスク値のデータテーブルの一例を示す説明図である。

【図７】図７は、リスク値のデータテーブルの一例を示す説明図である。

【図８】図８は、リスク値のデータテーブルの一例を示す説明図である。

【図９】図９は、リスク値のデータテーブルの一例を示す説明図である。

【図１０】図１０は、変形例にかかるシステムの動作例を示すフローチャートである。

【図１１】図１１は、情報処理装置のハードウエア構成を例示するブロック図である。

【発明を実施するための形態】

【００１０】

以下、図面を参照して、実施形態にかかるリスク算定方法、リスク算定プログラムおよびリスク算定装置を説明する。実施形態において同一の機能を有する構成には同一の符号を付し、重複する説明は省略する。なお、以下の実施形態で説明するリスク算定方法、リスク算定プログラムおよびリスク算定装置は、一例を示すに過ぎず、実施形態を限定するものではない。また、以下の各実施形態は、矛盾しない範囲内で適宜組みあわせてもよい。

【００１１】

図１は、実施形態にかかるシステム１の構成例を示すブロック図である。図１に示すように、システム１は、端末装置２と、ＬＡＮ（Local Area Network）などの通信ネットワーク（図示しない）を介して端末装置２と接続されたサーバ装置３とを有する。

【００１２】

端末装置２は、例えば、ＰＣ（パーソナルコンピュータ）やスマートフォンなどのユーザが使用する情報処理装置（コンピュータ）である。サーバ装置３は、端末装置２をクライアント（Ｃ）として収容するシステム１の情報処理装置であり、いわゆるサーバ（Ｓ）である。一実施形態として、サーバ装置３には、ＰＣやＷＳ（ワークステーション）などの装置を採用できる。

【００１３】

端末装置２およびサーバ装置３の各々には、クライアント（Ｃ）またはサーバ（Ｓ）にかかるプログラムがインストールされる。かかるプログラムを端末装置２およびサーバ装置３のプロセッサ上で動作させることによって、端末装置２およびサーバ装置３の各々は、クライアント（Ｃ）またはサーバ（Ｓ）における各種機能を実現できる。

【００１４】

端末装置２は、プログラムをプロセッサ上で動作させることによって、行動検出部１０、動的リスク算出部１１、通信部１２、ユーザ検知部１４、過剰アラート防止部１５および出力部１６の機能を有する。同様に、サーバ装置３は、プログラムをプロセッサ上で動作させることによって、閾値算出部１３の機能を有する。

【００１５】

行動検出部１０は、キーボード、マウスなどの入力装置を介してユーザＵが行った行動を検出する。行動検出部１０は、検出した行動内容を検出時刻とともに行動ログ２０に記録する。具体的には、行動検出部１０は、ログイン認証などで認証されたユーザＵを示す識別情報（例えばユーザＩＤ）とともに、検出した行動内容および検出時刻を行動ログ２０に記録する。行動ログ２０は、ユーザＵごとの行動履歴、すなわちユーザＵの行動内容を時系列で記録したデータである。

【００１６】

動的リスク算出部１１は、行動ログ２０より所定期間内のユーザＵの行動履歴を抽出し、抽出した行動履歴から期間内においてユーザＵに特徴的な行動特性を示す行動特性値を求める。動的リスク算出部１１がユーザＵの行動履歴を抽出する期間は、１時間、１日といった時間単位である。例えば、動的リスク算出部１１は、直近から１時間前または１日前までのユーザＵの行動履歴を行動ログ２０より抽出する。次いで、動的リスク算出部１１は、ユーザＵへのアンケート結果などにより事前に得られた、ユーザＵに特徴的な心理特性を示す心理特性値２１と、所定期間における行動特性値とをもとに、ユーザＵがＩＴ被害にあうリスクを示すリスク値２２を算出する。

【００１７】

例えば、動的リスク算出部１１は、ＲＳ（リスク値）＝ｆ（Ｐｓ）＋ｇ（Ｂ，Ｔ）とするリスク計算式よりリスク値２２を算出する。このリスク計算式において、Ｐｓは心理特性、Ｂは行動特性、Ｔは期間（時間）を示す。また、ｆはＰｓの関数、ｇはＢ、Ｔの関数であることを示す。このリスク計算式より算出されるリスク値（ＲＳ）は、アンケートを行った時から時間的に変化のない静的な心理特性値２１だけでなく、昼過ぎの眠くなる時間帯や午前または午後で変化する業務内容など、時間帯で異なるユーザＵの行動特性値を反映する値となる。したがって、動的リスク算出部１１より算出されるリスク値（ＲＳ）

は、ユーザＵの行動特性値を求めた期間（Ｔ）ごとに変化する動的な値となる。

【００１８】

なお、動的リスク算出部１１は、ログイン認証などで認証されたユーザＵを示す識別情報（例えばユーザＩＤ）に基づくユーザＵごとに、各期間におけるリスク値２２を算出する。期間ごとに算出した各ユーザＵのリスク値２２は、データテーブルなどに格納される。

【００１９】

通信部１２は、ＬＡＮ（Local Area Network）等の通信ネットワーク（図示しない）を介して外部装置（例えばサーバ装置３）との通信を行う。具体的には、通信部１２は、動的リスク算出部１１により算出されたリスク値２２をサーバ装置３へ送信する。また、通信部１２は、ＩＴ被害についてのアラートを出力する基準のリスク値（閾値）となるアラート基準値２３をサーバ装置３より受信する。通信部１２は、サーバ装置３より受信したアラート基準値２３をユーザ検知部１４へ出力する。

【００２０】

閾値算出部１３は、１または複数の端末装置２より受信した複数名のユーザＵのリスク値（複数名）２２ａを集計してアラート基準値２３を算出する。具体的には、各ユーザＵについて算出されたリスク値２２は、通信部１２を介してサーバ装置３に送られて、リスク値（複数名）２２ａに蓄積される。閾値算出部１３は、このリスク値（複数名）２２ａを集計して平均値、度数分布などの統計データを求め、ＩＴ被害のリスクの高いユーザＵを検出するための目安となるアラート基準値２３を算出する。閾値算出部１３は、算出したアラート基準値２３を通信ネットワークを介して端末装置２へ送信する。

【００２１】

例えば、閾値算出部１３は、リスク値（複数名）２２ａを集計した平均値をアラート基準値２３とする。この場合、算出されたアラート基準値２３をもとに、ＩＴ被害についてのリスクが複数のユーザＵの平均よりも高いユーザＵを検知できる。また、閾値算出部１３は、リスク値（複数名）２２ａを集計した度数分布をもとに、上位の所定範囲（例えば上位数％）に属するリスク値の境界値をアラート基準値２３とする。この場合、算出されたアラート基準値２３をもとに、ＩＴ被害についてのリスクが上位の所定範囲に属するユーザＵを検知できる。

【００２２】

ユーザ検知部１４は、サーバ装置３より取得したアラート基準値２３と、各ユーザＵのリスク値２２とを比較し、アラート基準値２３よりもリスク値２２が超過するユーザＵを検知する。ユーザ検知部１４は、検知結果を過剰アラート防止部１５を介して出力部１６へ出力する。出力部１６は、ディスプレイへの表示や、音声出力などにより、アラート基準値２３よりもリスク値２２が超過するユーザＵについてＩＴ被害が生じうる危険があることを示すアラートを出力する。

【００２３】

過剰アラート防止部１５は、ユーザ検知部１４により検知されたアラート基準値２３よりもリスク値２２が超過するユーザＵについて、短期間のうちにアラートが連続して出力され、アラートの出力が過剰となることを防止する。具体的には、過剰アラート防止部１５は、ユーザＩＤなどの識別情報が同じユーザＵについて、直近にアラートを出力してからの経過時間が所定時間内である場合にはアラートの出力を抑制する。

【００２４】

また、過剰アラート防止部１５は、ユーザＩＤなどの識別情報が同じユーザＵについて、複数の期間にわたるリスク値２２の度数分布を求める。そして、過剰アラート防止部１５は、求めた度数分布において今回のリスク値２２が上位の所定範囲（例えば上位数％）に属する場合には、アラートの出力を抑制することなく、出力部１６よりアラートを出力させる。

【００２５】

これにより、複数の期間にわたるリスク値２２の度数分布において、今回のリスク値２

２が上位に属する場合、すなわち、ＩＴ被害を受けやすい状態である場合には、ユーザＵに対してアラートを出力することができる。また、リスク値２２が度数分布の上位２％に属する場合にアラートを出力するものとすると、ユーザＵの行動特性値を求める期間が１時間単位ならば１００時間に２回程度の頻度、１日単位ならば１００日に２日程度の頻度にアラートの出力を抑えることができる。

【００２６】

図２は、実施形態にかかるシステム１の動作例を示すフローチャートである。図２に示すように、システム１では、特徴的な心理特性を得るためのアンケートをユーザＵに対して予め行い、アンケート回答を得る（Ｓ１）。そして、得られたアンケート回答をもとに、ユーザＵの特徴的な心理特性を示す心理特性値２１を計算し（Ｓ２）、求めておく。この心理特性値２１は、例えば半年に１回などの間隔で実行されるアンケートより回答が得られる度に更新される。

【００２７】

ユーザＵに対して行うアンケートは、心理状態に関する質問項目を含むものである。質問項目の一例としては、標準型攻撃メールについての訓練メールでの開封経験（プログラムの実行経験）、ウイルスの感染経験、自信過剰度を評価する質問項目、目先の利益の優先度を評価する質問項目、クラッキングの被害に遭う可能性を問う質問項目などがある。自信過剰度を評価する質問項目、目先の利益の優先度を評価する質問項目などの心理状態に関する質問項目については、例えば、ユーザの回答を数値化した（段階別に評価した）ものなどであってよい。また、アンケートには、心理状態に関する質問項目だけでなく、訓練メールでの開封経験、ウイルスの感染経験など、セキュリティに対する意識の低い人か否かを判定するための質問項目を含めてもよい。

【００２８】

心理特性値２１は、これらの質問項目への回答をもとに、自信過剰（Ｐｓ１）、面倒くさがり（Ｐｓ２）、目先の利益を優先（Ｐｓ３）、せっかち（Ｐｓ４）…などの心理特性（Ｐｓ）を数値化したものである。

【００２９】

行動検出部１０では、ユーザＵが行った行動を検出し、検出した行動内容を時刻とともに行動ログ２０に記録する（Ｓ３）。行動ログ２０に記録される行動内容には、例えば、マウス、キーボードの操作の他、画面の切り替え操作、メールの送受信操作、各種画面（例えば警告画面）の表示時間などがある。

【００３０】

動的リスク算出部１１では、ユーザＵのリスク値（ＲＳ＿ｕ）をユーザＵの心理特性（Ｐｓ＿ｕ）および行動特性（Ｂ＿ｕ）の和または積により計算する動的リスク計算式２４の係数計算（Ｓ４、Ｓ５）を行う。

【００３１】

動的リスク計算式２４は、例えばユーザＵのリスク値（ＲＳ＿ｕ）を次の式（１）で計算する。式（１）において、αはＰｓ＿ｕの係数、βはＢ＿ｕの係数である。

【００３２】

【数１】

$$RS_u = \alpha^{*} Ps_u + \beta^{*}(B_u) \quad \cdots(1)$$

【００３３】

リスクに関係するユーザＵの心理特性（Ｐｓ＿ｕ）および行動特性（Ｂ＿ｕ）が複数存在する場合、ユーザＵのそれぞれの値はＰｓ＿｛ｕ，ｉ｝（ｉ＝１，２，…，ｎ）、Ｂ＿｛ｕ，ｊ｝（ｊ＝１，２，…，ｍ）と表現でき、式（１）は次の式（２）のように表現できる。

【００３４】

【数２】

$$RS_u = \Sigma\alpha_i^{*}Ps_\{u,i\} + \Sigma\beta_j^{*}B\{u,j\} \qquad \cdots(2)$$

【００３５】

式（２）では、和（Σ）としてるが、積（Π）としてもよい。α＿ｉ、β＿ｊは、各特性（ｉ、ｊ）における係数である。さらに、ある時刻におけるユーザＵのリスク値（ＲＳ＿ｕ）は、次の式（３）のように表現できる。

【００３６】

【数３】

$$RS_\{u,t\} = \Sigma\alpha_i^{*}Ps_\{u,i,t\} + \Sigma\beta_j^{*}B\{u,j,t\} \qquad \cdots(3)$$

【００３７】

Ｓ４、Ｓ５では、ユーザＵの１ヶ月程度の過去の行動ログ２０ａを行動特性（Ｂ）における既知の値、Ｓ１におけるアンケート回答を心理特性（Ｐｓ）における既知の値として、動的リスク計算式２４の係数（α＿ｉ、β＿ｊ）の計算を行う。この係数計算は、例えば特開２０１５－１７６３７５号公報などにおいて公知の方法であり、従来の回帰分析手法を用いて計算される。なお、動的リスク計算式２４の係数（α＿ｉ、β＿ｊ）については、上述したようにユーザＵごとに求めたものを用いてもよいし、一般的なユーザＵをモデルとして予め計算しておいた係数値を用いてもよい。

【００３８】

動的リスク算出部１１では、行動ログ２０より所定期間内のユーザＵの行動履歴を抽出し、期間（Ｔ）内においてユーザＵに特徴的な行動特性を示す行動特性値２５（Ｂ｛ｕ，ｊ，Ｔ｝）を計算する（Ｓ６）。

【００３９】

具体的には、抽出された行動履歴をもとに、例えばマウス、キーボードの操作から、キー入力の時間間隔、一定時間内のマウスのクリック操作の回数、バックスペースなどの削除キーの操作の回数などの行動特性値Ｂ｛ｕ，１，Ｔ｝を計算する。この行動特性値Ｂ｛ｕ，１，Ｔ｝は、例えばユーザＵの注意力が落ちると時間間隔は遅くなり、操作回数は多くなる値である。

【００４０】

また、画面の切り替え操作からは、複数のウインドウ画面の中から操作対象とするアクティブウインドウ画面の切り替え回数などの行動特性値Ｂ｛ｕ，２，Ｔ｝を計算する。この行動特性値Ｂ｛ｕ，２，Ｔ｝は、例えば業務が多忙である時に多くなる値である。

【００４１】

また、各種画面の表示時間からは、注意喚起画面の表示時間などの行動特性値Ｂ｛ｕ，３，Ｔ｝を計算する。行動特性値Ｂ｛ｕ，３，Ｔ｝は、例えば業務が多忙である時に短くなる値である。このように、動的リスク算出部１１は、期間（Ｔ）内におけるユーザＵの行動特性ごとの行動特性値２５（Ｂ｛ｕ，１，Ｔ｝、Ｂ｛ｕ，２，Ｔ｝…Ｂ｛ｕ，ｊ，Ｔ｝）を計算する。

【００４２】

次いで、動的リスク算出部１１は、ユーザＵの心理特性値２１と、期間（Ｔ）内におけるユーザＵの行動特性値２５とを動的リスク計算式２４に代入し、ユーザＵの期間（Ｔ）におけるリスク値２２を計算する（Ｓ７）。

【００４３】

図３は、リスク値の時間的変化を説明する説明図である。図３において、ＴＨは、アラートを出力する基準のリスク値（閾値）であるアラート基準値２３を示す。ＲＳ１は、ユーザＡについて、心理特性値２１と、時間（ｔ）ごとの行動特性値２５とを動的リスク計算式２４に代入して求めたリスク値である。このＲＳ１に対し、ＲＳ１ａは、ユーザＡについて、時間（ｔ）ごとの行動特性値２５を用いずに、心理特性値２１をもとに求めたリスク値である。同様に、ＲＳ２は、ユーザＢについて、心理特性値２１と、時間（ｔ）ご

との行動特性値２５とを動的リスク計算式２４に代入して求めたリスク値である。また、ＲＳ２ａは、ユーザＢについて、時間（ｔ）ごとの行動特性値２５を用いずに、心理特性値２１をもとに求めたリスク値である。

【００４４】

図３に示すように、時間（ｔ）ごとの行動特性値２５を用いずに、アンケートを行った時から時間的に変化のない静的な心理特性値２１をもとに求めたリスク値（ＲＳ１ａ、ＲＳ２ａ）は、時間で変化することがない。このため、例えばリスク値がＴＨを超過する場合（ＲＳ２ａの場合）は、時間（ｔ）に関係なくアラートが出力され続けることとなる。

【００４５】

これに対し、動的リスク算出部１１により算出されるリスク値２２（ＲＳ１またはＲＳ２）は、アンケートを行った時から時間的に変化のない静的な心理特性値２１だけでなく、時間（ｔ）で異なるユーザＵの行動特性値２５を反映した時間的に変化する値となる。具体的には、図３に示すように、ユーザＡのリスク値ＲＳ１またはユーザＢのリスク値ＲＳ２は、ユーザＡ、Ｂの時間ごとに変化する行動特性値２５を反映し、時間的に変化する値となる。この時間ごとに変化する行動特性値２５は、昼過ぎの眠くなる時間帯や午前または午後で変化する業務内容などを的確に反映したものである。よって、動的リスク算出部１１は、動的に変化するユーザＡ、Ｂのリスクに対応した、精度の高いリスク値（ＲＳ１、ＲＳ２）を求めることができる。

【００４６】

ユーザ検知部１４は、サーバ装置３より取得したアラート基準値２３と、各ユーザＵのリスク値２２とを比較し、アラート基準値２３よりもリスク値２２が超過するユーザＵを検知する（Ｓ８）。ユーザ検知部１４は、検知結果を過剰アラート防止部１５を介して出力部１６へ出力する。出力部１６では、ユーザ検知部１４からの検知結果をもとに、アラート基準値２３よりもリスク値２２が超過するユーザＵについてＩＴ被害が生じうる危険があることを示すアラートを出力する（Ｓ１１）。

【００４７】

過剰アラート防止部１５は、ユーザ検知部１４の検知結果をもとに、アラート基準値２３よりもリスク値２２が超過するユーザＵについて前回の検知からの経過時間が予め設定された時間（Ｄｕ）未満であるか否かを判定する（Ｓ９）。Ｄｕの値は、アラートの出力間隔を空けるように、例えば１日程度の値が適宜設定される。

【００４８】

前回の検知からの経過時間が予め設定された時間（Ｄｕ）未満である場合（Ｓ９：ＹＥＳ）、過剰アラート防止部１５は、出力部１６からのアラートの出力を抑制し、アラートの出力が過剰となることを防止する（Ｓ１０）。また、前回の検知からの経過時間が予め設定された時間（Ｄｕ）未満でない場合（Ｓ９：ＮＯ）、過剰アラート防止部１５は、出力部１６からのアラートの出力を抑制することなく、アラート基準値２３よりもリスク値２２が超過するユーザＵに対するアラートをそのまま出力部１６より出力させる。

【００４９】

また、過剰アラート防止部１５は、ユーザＩＤなどの識別情報が同じユーザＵについて、複数の期間にわたるリスク値２２の度数分布を求め、求めた度数分布と今回のリスク値２２とを比較して、アラートの抑制を行ってもよい。例えば、過剰アラート防止部１５は、求めた度数分布において今回のリスク値２２が上位の所定範囲（例えば上位数％）に属さない場合には、際立ってリスクの高い状態ではないことから、アラートの出力を抑制する。また、過剰アラート防止部１５は、今回のリスク値２２が度数分布の上位の所定範囲（例えば上位数％）に属する場合には、アラートの出力を抑制することなく、出力部１６よりアラートを出力させる。

【００５０】

図４は、リスク値の時間的変化を説明する説明図である。図４に示すように、ユーザＡ、ユーザＢにおけるリスク値（ＲＳ）は、期間（Ｔ）によって変化する。ここで、ユーザＡのリスク値は、２Ｔおよび４Ｔのところでアラート基準値２３を超過している。したが

って、例えば１Ｔが１時間単位である場合には、２時間ごとにアラートが出力され、アラートが頻繁に出力されることとなる。このように、アラートが頻繁に出力されると、ユーザＵは、アラートに対して慣れてしまい、アラートに対する対処が遅れる場合がある。

【００５１】

図５は、リスク値の度数分布を説明する説明図である。図５に示すように、過剰アラート防止部１５は、一定期間（例えば１００Ｔ程度）でのユーザＵ個人のリスク値（ＲＳ）の度数分布を作り、ユーザＵがめったに取らない上位の所定範囲を求める。例えば、過剰アラート防止部１５は、度数分布が正規分布に従うと仮定することで、平均値（μ）と標準偏差（σ）を求め、ユーザＵが１００回中２回（＝２％）取りうるリスク値（＝μ＋２σ）を求める。

【００５２】

このように、過剰アラート防止部１５は、各ユーザＵについて、リスク値（ＲＳ）の度数分布から上位の所定範囲となるリスク値を求めておき、今回のリスク値２２が上位の所定範囲に属するか否かを判定する。そして、過剰アラート防止部１５は、今回のリスク値２２が上位の所定範囲に属さない場合には、際立ってリスクの高い状態ではないことから、アラートの出力を抑制する。また、過剰アラート防止部１５は、今回のリスク値２２が上位の所定範囲に属する場合には、出力部１６よりアラートを出力させる。これにより、ユーザＵにとって煩わしくない頻度でのアラートが可能となる。

【００５３】

図６～図９は、リスク値のデータテーブルの一例を示す説明図である。図６に示すように、各ユーザＵについて算出されたリスク値２２は、ユーザＵごと（ｕ＿１，ｕ＿２，…）のテーブルデータで管理される。

【００５４】

また、このテーブルデータで管理されるユーザＵごとのリスク値は、通信部１２よりサーバ装置３へ送信される。サーバ装置３の閾値算出部１３は、ユーザＵごとのリスク値を集計してアラート基準値２３を算出し、端末装置２へ送信する。ここで、アラート基準値２３の値は、９．０と算出されたものとする。

【００５５】

ユーザ検知部１４は、ユーザＵごと（ｕ＿１，ｕ＿２，…）のテーブルデータを参照し、アラート基準値２３（９．０）を超過するユーザＵを検知する。具体的には、図７に示すように、リスク値が９．０を超過するユーザｕ＿９、ｕ＿１２、ｕ＿１４、ｕ＿２０（黒丸参照）が検知される。

【００５６】

次いで、過剰アラート防止部１５は、図８に示すように、ユーザＵにおける時間（Ｔ＿｛１，ｕ｝、Ｔ＿｛２，ｕ｝…）ごとのリスク値を格納するテーブルデータを参照し、直近にアラートを出力してからの経過時間が所定時間内である場合にはアラートの出力を抑制する。

【００５７】

例えば、図８の例において、時刻ｔの１単位が１時間である場合には、２０時間でリスク値が９．０を超過する（黒丸参照）時刻が複数あり、頻繁にアラートを受けることとなる。したがって、直近にアラートを出力してからの経過時間が所定時間内である場合にはアラートの出力を抑制することで、ユーザＵがアラート慣れを起こすことを防止する。

【００５８】

また、過剰アラート防止部１５は、図９に示すように、ユーザＵにおける時間（Ｔ＿｛１，ｕ｝、Ｔ＿｛２，ｕ｝…）ごとのリスク値を格納するテーブルデータを参照し、リスク値の度数分布を求める。

【００５９】

具体的には、過剰アラート防止部１５は、ユーザＵのリスク値（ＲＳ＿｛ｕ，ｔ｝）の分布を正規分布とみなし、所定期間（例えばＴ＿｛１，ｕ｝～Ｔ＿｛２０，ｕ｝）における平均（μ）と標準偏差（σ）を求める。そして、過剰アラート防止部１５は、ユーザＵ

がめったに取らない上位のリスク値（ＲＳ＿｛ｕ，ａｎｏｍａｌｙ｝）を求める。例えば、ユーザＵが約２％の確率で取りうるリスク値（＝μ＋２σ）を求め、過剰アラート防止部１５は、今回のリスク値２２が約２％の確率で取りうる高いリスク値である場合には、出力部１６よりアラートを出力させる。

【００６０】

図９の例では、時刻がＴ＿｛２０，ｕ｝である時に、約２％の確率で取りうる高いリスク値であることから、アラートが出力されることとなる。

【００６１】

（変形例）

図１０は、変形例にかかるシステム１ａの動作例を示すフローチャートである。図１０に示すように、変形例にかかるシステム１ａでは、端末装置２ａの行動検出部１０が検出した行動ログ２０を通信部１２を介してサーバ装置３ａに送る。そして、サーバ装置３ａにおいて、動的リスク算出部１１によるユーザＵのリスク値２２の算出、ユーザ検知部１４によるユーザＵの検知、過剰アラート防止部１５による過剰アラートの防止および出力部１６によるアラート出力を行う。このように、端末装置２ａより行動ログ２０をサーバ装置３ａが収集し、ユーザＵのリスク値２２の計算やアラートの出力などの処理については、サーバ装置３ａ側で行ってもよい。

【００６２】

以上のように、システム１では、動的リスク算出部１１がユーザＵの行動履歴が記録された行動ログ２０をもとに、所定期間（Ｔ）における行動履歴から所定期間（Ｔ）においてユーザＵに特徴的な行動特性を示す行動特性値２５を求める。また、動的リスク算出部１１は、ユーザＵに特徴的な心理特性を示す心理特性値２１と、所定期間（Ｔ）においてユーザＵに特徴的な行動特性を示す行動特性値２５とに基づいて、ユーザＵがＩＴ被害にあうリスク値２２を計算する。また、システム１では、出力部１６が計算されたリスク値２２が所定の基準値を超過したユーザＵについてアラートを出力する。したがって、システム１では、時間によって動的に変化するリスクに対応することができ、リスクをもとに出力するアラートの精度を高めることができる。

【００６３】

なお、図示した各装置の各構成要素は、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、各装置の分散・統合の具体的形態は図示のものに限られず、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。

【００６４】

例えば、本実施形態では端末装置２およびサーバ装置３を含むクライアント・サーバ（Ｃ／Ｓ）モデルのシステム１を例示したが、閾値算出部１３を自装置内で実現する端末装置２単体の装置構成であってもよい。また、Ｃ／Ｓモデルのサーバ装置３は、クラウドコンピューティングとしてもよい。

【００６５】

また、本実施形態では、動的リスク算出部１１はユーザＵごとのリスク値２２を求めているが、動的リスク算出部１１が求めるリスク値２２は、ユーザＵごとのものに限定しない。例えば、動的リスク算出部１１は、ユーザＵが属するグループ（例えば、企業における部門など）単位で集計し、グループ単位のリスク値２２を求めてもよい。このようにグループ単位のリスク値２２を求める場合には、業務内容、業務時間、昼休みの時刻、フレックス勤務の有無など、グループによって異なる行動特性をリスク計算（Ｓ７）に反映できる。

【００６６】

また、端末装置２およびサーバ装置３の情報処理装置で行われる各種処理機能は、ＣＰＵ（またはＭＰＵ、ＭＣＵ（Micro Controller Unit）等のマイクロ・コンピュータ）上で、その全部または任意の一部を実行するようにしてもよい。また、各種処理機能は、ＣＰＵ（またはＭＰＵ、ＭＣＵ等のマイクロ・コンピュータ）で解析実行されるプログラ

ム上、またはワイヤードロジックによるハードウエア上で、その全部または任意の一部を実行するようにしてもよいことは言うまでもない。

【００６７】

ところで、上記の実施形態で説明した各種の処理は、予め用意されたプログラムをコンピュータで実行することで実現できる。そこで、以下では、上記の実施例と同様の機能を有するプログラムを実行するコンピュータ（ハードウエア）の一例を説明する。図１１は、情報処理装置１００のハードウエア構成を例示するブロック図である。

【００６８】

図１１が示すように、情報処理装置１００は、各種演算処理を実行するＣＰＵ１０１と、データ入力を受け付ける入力装置１０２と、モニタ１０３と、スピーカ１０４とを有する。また、情報処理装置１００は、記憶媒体からプログラム等を読み取る媒体読取装置１０５と、各種装置と接続するためのインタフェース装置１０６と、有線または無線により外部機器と通信接続するための通信装置１０７とを有する。また、情報処理装置１００は、各種情報を一時記憶するＲＡＭ１０８と、ハードディスク装置１０９とを有する。また、情報処理装置１００内の各部（１０１～１０９）は、バス１１０に接続される。

【００６９】

ハードディスク装置１０９には、行動検出部１０、動的リスク算出部１１、通信部１２、閾値算出部１３、ユーザ検知部１４、過剰アラート防止部１５および出力部１６の各処理部と同様の機能を有するプログラムが記憶される。また、ハードディスク装置１０９には、プログラムを実現するための各種データが記憶される。入力装置１０２は、例えば情報処理装置１００の操作者から操作情報の入力を受け付ける。モニタ１０３は、例えば操作者が操作する各種画面を表示する。インタフェース装置１０６は、例えば印刷装置等が接続される。通信装置１０７は、ＬＡＮ（Local Area Network）等の通信ネットワークと接続され、通信ネットワークを介した外部機器との間で各種情報をやりとりする。

【００７０】

ＣＰＵ１０１は、ハードディスク装置１０９に記憶された各プログラムを読み出して、ＲＡＭ１０８に展開して実行することで、各種の処理を行う。また、これらのプログラムは、情報処理装置１００を行動検出部１０、動的リスク算出部１１、通信部１２、閾値算出部１３、ユーザ検知部１４、過剰アラート防止部１５および出力部１６として機能させることができる。

【００７１】

なお、上記のプログラムは、必ずしもハードディスク装置１０９に記憶されている必要はない。例えば、情報処理装置１００が読み取り可能な記憶媒体に記憶されたプログラムを、情報処理装置１００が読み出して実行するようにしてもよい。情報処理装置１００が読み取り可能な記憶媒体は、例えば、ＣＤ－ＲＯＭやＤＶＤディスク、ＵＳＢ（Universal Serial Bus）メモリ等の可搬型記録媒体、フラッシュメモリ等の半導体メモリ、ハードディスクドライブ等が対応する。また、公衆回線、インターネット、ＬＡＮ（Local Area Network）等に接続された装置にこのプログラムを記憶させておき、情報処理装置１００がこれらからプログラムを読み出して実行するようにしてもよい。

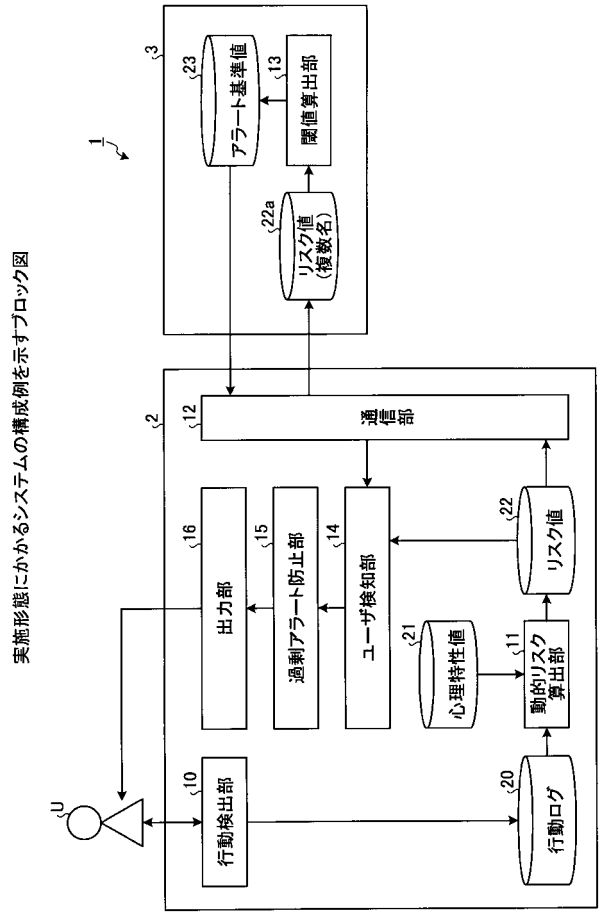
【符号の説明】

【００７２】

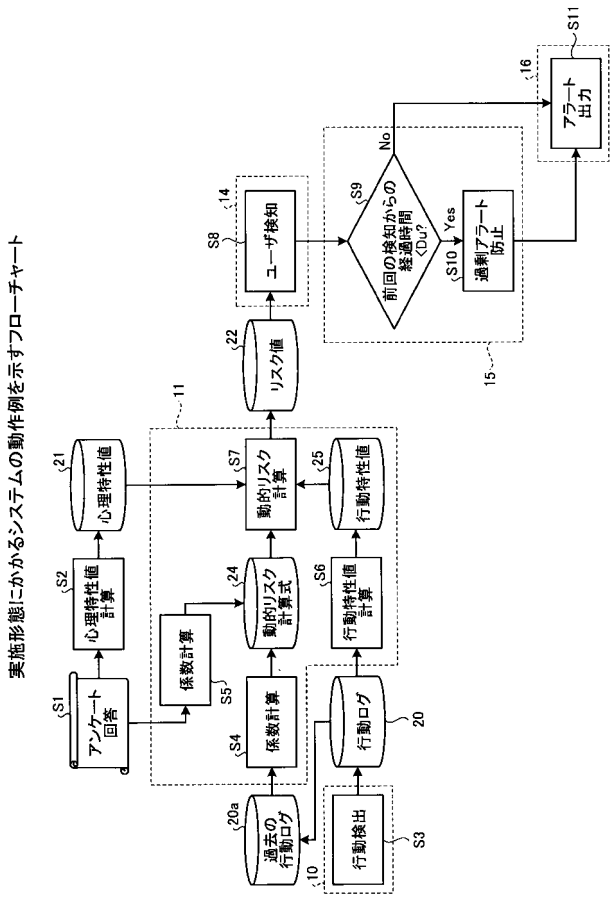
１、１ａ…システム
２、２ａ…端末装置
３、３ａ…サーバ装置
１０…行動検出部
１１…動的リスク算出部
１２…通信部
１３…閾値算出部
１４…ユーザ検知部
１５…過剰アラート防止部

１６…出力部
２０…行動ログ
２１…心理特性値
２２…リスク値
２２ａ…リスク値（複数名）
２３…アラート基準値
２４…動的リスク計算式
２５…行動特性値
１００…情報処理装置
ＲＳ、ＲＳ１、ＲＳ１ａ、ＲＳ２、ＲＳ２ａ…リスク値
ＴＨ…アラート基準値
Ｕ…ユーザ

【図１】

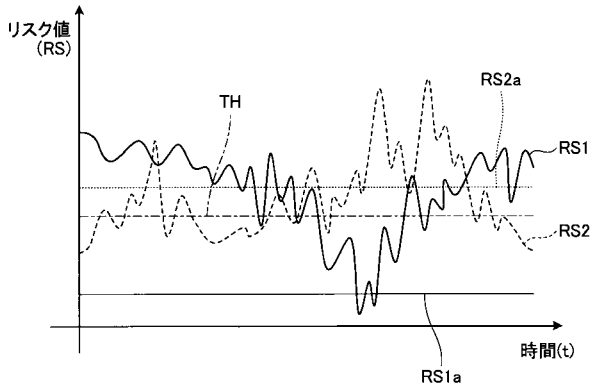


【図２】



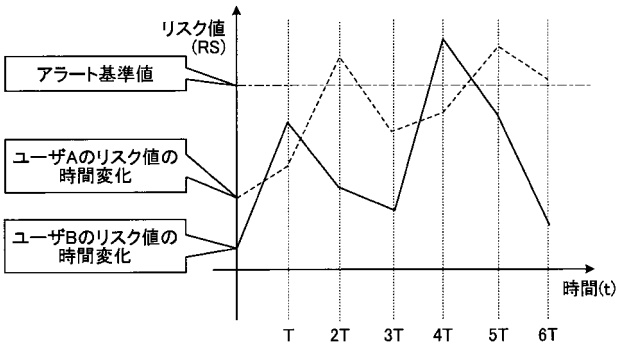
【図３】

リスク値の時間的変化を説明する説明図



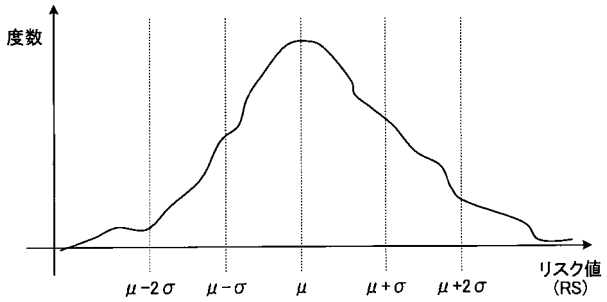
【図４】

リスク値の時間的変化を説明する説明図



【図５】

リスク値の度数分布を説明する説明図



【図６】

リスク値のデータテーブルの一例を示す説明図

ユーザID	α	β	Ps_{u,t}	B_{u,t}	RS_{u,t}
u_1	1	10	0.17	0.13	1.5
u_2	1	10	0.80	0.37	4.5
u_3	1	10	0.58	0.72	7.8
u_4	1	10	0.38	0.94	9.8
u_5	1	10	0.89	0.37	4.6
u_6	1	10	0.92	0.16	2.6
u_7	1	10	0.99	0.26	3.6
u_8	1	10	1.00	0.88	9.8
u_9	1	10	0.89	0.18	2.7
u_10	1	10	0.57	0.10	1.5
u_11	1	10	0.79	0.03	1.1
u_12	1	10	0.15	0.15	1.6
u_13	1	10	0.81	0.59	6.7
u_14	1	10	0.48	0.64	6.9
u_15	1	10	0.60	0.61	6.7
u_16	1	10	0.52	0.92	9.7
u_17	1	10	0.03	0.09	1.0
u_18	1	10	0.39	0.95	9.9
u_19	1	10	0.72	0.20	2.7
u_20	1	10	0.62	0.65	7.1
⋮	⋮	⋮	⋮	⋮	⋮

【図７】

リスク値のデータテーブルの一例を示す説明図

ユーザID	α	β	Ps_{u,t}	B_{u,t}	RS_{u,t}	RS_{u,t}>9.0
u_1	1	10	0.78	0.66	7.3	
u_2	1	10	0.13	0.70	7.1	
u_3	1	10	0.15	0.44	4.5	
u_4	1	10	0.92	0.11	2.0	
u_5	1	10	0.43	0.53	5.7	
u_6	1	10	0.01	0.89	8.9	
u_7	1	10	0.46	0.50	5.4	
u_8	1	10	0.32	0.80	8.3	
u_9	1	10	0.13	0.97	9.8	●
u_10	1	10	0.31	0.23	2.6	
u_11	1	10	0.86	0.29	3.8	
u_12	1	10	0.37	1.00	10.4	●
u_13	1	10	0.40	0.20	2.4	
u_14	1	10	0.67	0.97	10.4	●
u_15	1	10	0.89	0.14	2.2	
u_16	1	10	0.76	0.79	8.7	
u_17	1	10	0.91	0.33	4.2	
u_18	1	10	0.55	0.41	4.6	
u_19	1	10	0.50	0.42	4.7	
u_20	1	10	0.27	0.94	9.6	●
⋮	⋮	⋮	⋮	⋮	⋮	⋮

【図８】

リスク値のデータテーブルの一例を示す説明図

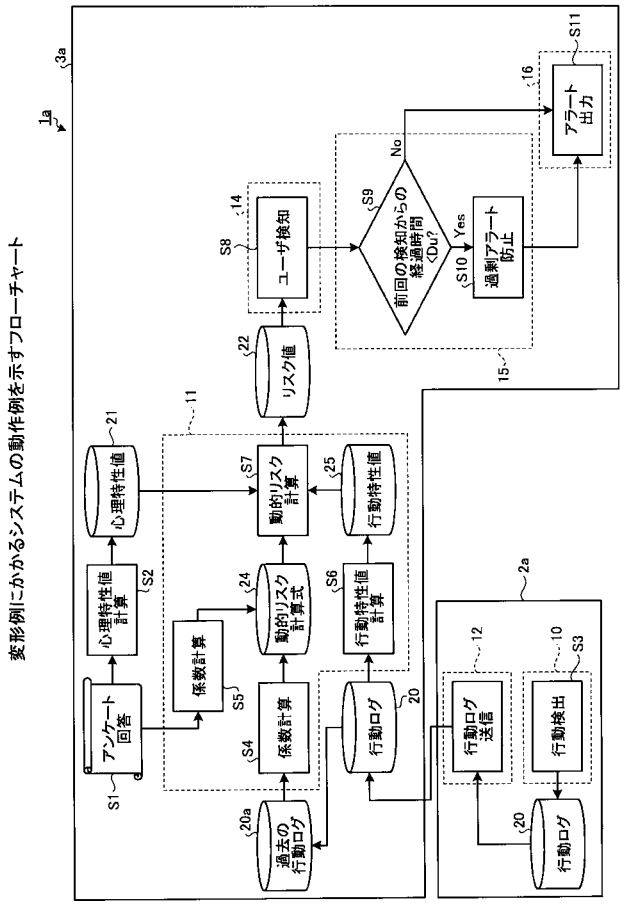
時刻t	α	β	Ps_{u,t}	B_{u,t}	RS_{u,t}	RS_{u,t}>9.0
T_{1,u}	1	10	0.70	0.87	9.4	●
T_{2,u}	1	10	0.70	0.85	9.2	●
T_{3,u}	1	10	0.70	0.28	3.5	
T_{4,u}	1	10	0.70	0.59	6.6	
T_{5,u}	1	10	0.70	0.49	5.6	
T_{6,u}	1	10	0.70	0.65	7.2	
T_{7,u}	1	10	0.70	0.46	5.3	
T_{8,u}	1	10	0.70	0.88	9.5	●
T_{9,u}	1	10	0.70	1.03	11.0	●
T_{10,u}	1	10	0.70	1.05	11.2	●
T_{11,u}	1	10	0.70	1.16	12.3	●
T_{12,u}	1	10	0.70	0.54	6.1	
T_{13,u}	1	10	0.70	0.59	6.6	
T_{14,u}	1	10	0.70	0.27	3.4	
T_{15,u}	1	10	0.70	0.60	6.7	
T_{16,u}	1	10	0.70	0.33	4.0	
T_{17,u}	1	10	0.70	0.52	5.9	
T_{18,u}	1	10	0.70	0.24	3.1	
T_{19,u}	1	10	0.70	0.47	5.4	
T_{20,u}	1	10	0.70	3.00	30.7	●
…	…	…	…	…	…	…

【図９】

リスク値のデータテーブルの一例を示す説明図

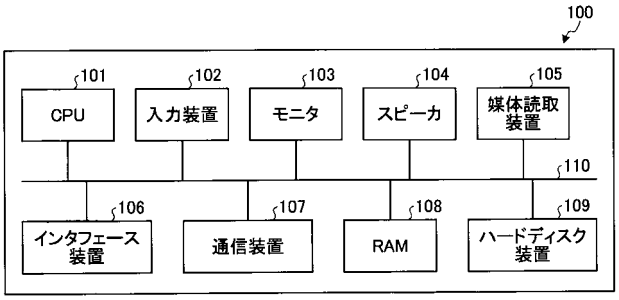
時刻t	α	β	Ps_{u,t}	B_{u,t}	RS_{u,t}	RS_{u,t}>9.0	RS_{u,t}>RS_{u,anomaly}
T_{1,u}	1	10	0.70	0.90	9.7	●	
T_{2,u}	1	10	0.70	0.59	6.6		
T_{3,u}	1	10	0.70	0.49	5.6		
T_{4,u}	1	10	0.70	1.20	12.7	●	
T_{5,u}	1	10	0.70	1.18	12.5	●	
T_{6,u}	1	10	0.70	0.75	8.2		
T_{7,u}	1	10	0.70	0.30	3.7		
T_{8,u}	1	10	0.70	0.58	6.5		
T_{9,u}	1	10	0.70	0.44	5.1		
T_{10,u}	1	10	0.70	1.13	12.0	●	
T_{11,u}	1	10	0.70	0.69	7.6		
T_{12,u}	1	10	0.70	0.35	4.2		
T_{13,u}	1	10	0.70	0.59	6.6		
T_{14,u}	1	10	0.70	0.63	7.0		
T_{15,u}	1	10	0.70	1.18	12.5	●	
T_{16,u}	1	10	0.70	0.36	4.3		
T_{17,u}	1	10	0.70	0.56	6.3		
T_{18,u}	1	10	0.70	0.55	6.2		
T_{19,u}	1	10	0.70	0.92	9.9	●	
T_{20,u}	1	10	0.70	3.00	30.7	●	●
…	…	…	…	…	…	…	…

【図１０】



【図１１】

情報処理装置のハードウエア構成を例示するブロック図



フロントページの続き

(72)発明者　片山　佳則
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Ｆターム(参考) 5L049 CC11　CC12