(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2017-503293
(P2017-503293A)
(43)公表日　平成29年1月26日(2017.1.26)

(51)Int.Cl.	F I	テーマコード（参考）
G06F 21/55 (2013.01)	G06F 21/55	

審査請求 有　予備審査請求 未請求　（全 43 頁）

(21)出願番号	特願2016-561070 (P2016-561070)
(86)(22)出願日	平成27年4月30日 (2015.4.30)
(85)翻訳文提出日	平成27年6月25日 (2015.6.25)
(86)国際出願番号	PCT/CN2015/078019
(87)国際公開番号	WO2016/082462
(87)国際公開日	平成28年6月2日 (2016.6.2)
(31)優先権主張番号	201410708281.6
(32)優先日	平成26年11月27日 (2014.11.27)
(33)優先権主張国	中国 (CN)

(71)出願人　513309030
シャオミ・インコーポレイテッド
中華人民共和国・１０００８５・ベイジン・ハイディアン・ディストリクト・キンヘ・ミドル・ストリート・ナンバー・６８・レインボー・シティ・ショッピング・モール・２・オブ・チャイナ・リソーシズ・フロア・１３
(74)代理人　100103894
弁理士　家入　健

最終頁に続く

(54)【発明の名称】ユーザ行為識別方法及びユーザ行為識別装置、プログラム、及び記録媒体

(57)【要約】
本発明は、悪意のある行為をより効果的に且つより正確に識別するためのユーザ行為識別方法及びユーザ行為識別装置、プログラム、及び記録媒体に関する。前記方法は、所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得するステップと、前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップと、その評価結 果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップとを含む。
【選択図】図１

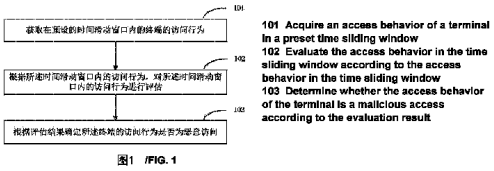


图1 /FIG. 1

【特許請求の範囲】
【請求項１】
所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得するステップと、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップと、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップと
を含むことを特徴とするユーザ行為識別方法。
【請求項２】
前記時間スライディングウィンドウは、ｍ個に等分されたタイムスライスを含み、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
タイムスライス内のアクセス回数が所定のスライス回数閾値を超えるかをタイムスライス毎に判断して、アクセス回数が所定のスライス回数閾値を超えるｎ個のタイムスライスを取得するステップと、
ｎとｍとの比例が所定の第１の比例閾値を超えるのかを判断するステップと
を含み、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップは、
ｎとｍとの比例が所定の第１の比例閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断するステップを含む
ことを特徴とする請求項１に記載のユーザ行為識別方法。
【請求項３】
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するステップと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算するステップと、
前記時間分散が所定の分散閾値を超えるのかを判断するステップと
を含み、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップは、
前記時間分散が所定の分散閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断するステップを含む
ことを特徴とする請求項１に記載のユーザ行為識別方法。
【請求項４】
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するステップと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算するステップと、
前記時間分散と時間間隔の平均値との比率を計算するステップと、
前記比率が所定の第２の比例閾値より小さいかを判断するステップと
を含み、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップは、
前記比率が所定の第２の比例閾値より小さい場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断するステップを含む
ことを特徴とする請求項１に記載のユーザ行為識別方法。

【請求項５】
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
前記時間スライディングウィンドウ内のアクセス行為の総回数を取得するステップと、
前記総回数が所定の総回数閾値を超えるのかを判断するステップと、
その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップと、を含む
ことを特徴とする請求項１に記載のユーザ行為識別方法。
【請求項６】
所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得するための取得モジュールと、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するための評価モジュールと、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するための判断モジュールと
を含むことを特徴とするユーザ行為識別装置。
【請求項７】
前記時間スライディングウィンドウは、ｍ個に等分されたタイムスライスを含み、
前記評価モジュールは、
タイムスライス内のアクセス回数が所定のスライス回数閾値を超えるかをタイムスライス毎に判断して、アクセス回数が所定のスライス回数閾値を超えるｎ個のタイムスライスを取得するためのタイムスライスサブモジュールと、
ｎとｍとの比例が所定の第１の比例閾値を超えるのかを判断するための第１比例サブモジュールと
を含み、
前記判断モジュールは、
ｎとｍとの比例が所定の第１の比例閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する
ことを特徴とする請求項６に記載のユーザ行為識別装置。
【請求項８】
前記評価モジュールは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するための間隔サブモジュールと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算するための分散サブモジュールと、
前記時間分散が所定の分散閾値を超えるのかを判断するための第１の評価サブモジュールと
を含み、
前記判断モジュールは、
前記時間分散が所定の分散閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する
ことを特徴とする請求項６に記載のユーザ行為識別装置。
【請求項９】
前記評価モジュールは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するための間隔サブモジュールと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算するための分散サブモジュールと、
前記時間分散と時間間隔の平均値との比率を計算するための比率サブモジュールと、
前記比率が所定の第２の比例閾値より小さいかを判断するための第２の比例サブモジュ

ールと
を含み、
前記判断モジュールは、
前記比率が所定の第２の比例閾値より小さい場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する
ことを特徴とする請求項６に記載のユーザ行為識別装置。
【請求項１０】
前記評価モジュールは、
前記時間スライディングウィンドウ内のアクセス行為の総回数を取得するための総回数サブモジュールと、
前記総回数が所定の総回数閾値を超えるのかを判断するための総回数判断サブモジュールと、
その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するための第２の評価サブモジュールと、を含む
ことを特徴とする請求項６に記載のユーザ行為識別装置。
【請求項１１】
プロセッサと、
プロセッサにより実行可能なインストラクションを格納するためのメモリと
を含む、ユーザ行為識別装置において、
前記プロセッサは、
所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得し、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価し、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断する、ように構成される
ことを特徴とするユーザ行為識別装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信及びコンピュータ処理の技術分野に関し、特に、ユーザ行為識別方法及びとユーザ行為識別装置に関する。
【背景技術】
【０００２】
インターネットの発展に伴い、ネットワークを介する資源共有化が進みつつある。人々は、ネットワークを介して豊富な情報を素早く便利に取得することが可能になった。しかしながら、多くのウェブサイトは、人々が情報収集している間、悪意のある攻撃に晒されている。
【０００３】
本発明の発明者は、従来技術において、悪意のある攻撃は、比較的短い時間内に、ウェブサイトにデータパケットを頻繁に送信することを発見した。このような事象は、値引き商品を争って買うために短い時間内に頻繁にアクセスするウェブサイト中でよく起こる。このような高頻度のアクセス行為は、通常、商品を争って買うために開発されたソフトウェアにより実現され、人為的操作ではこのように高い頻度が得られない。従来技術において、当該悪意のある行為を阻止する手段がないのはないが、その阻止の効果が理想的ではない。従って、ユーザの悪意のある行為を、どのようにより効果的に識別するかは、早急に解決すべき問題である。
【発明の概要】
【０００４】

本発明は、従来技術に存在する上記のような問題を解決するために、ユーザ行為識別方法及びユーザ行為識別装置を提供する。

【０００５】

本発明の実施例の第１の局面によれば、

所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得するステップと、

前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップと、

その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップと

を含むユーザ行為識別方法を提供する。

【０００６】

本発明の実施例に係る技術案は、ユーザのアクセス行為を時間スライディングウィンドウを用いてモニタリングして、アクセス行為を評価することにより、ユーザのアクセス行為に悪意があるか否かを判断する、という有益な効果を奏する。

【０００７】

一実施例において、

前記時間スライディングウィンドウは、ｍ個に等分されたタイムスライスを含み、

前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、

タイムスライス内のアクセス回数が所定のスライス回数閾値を超えるかをタイムスライス毎に判断して、アクセス回数が所定のスライス回数閾値を超えるｎ個のタイムスライスを取得するステップと、

ｎとｍとの比例が所定の第１の比例閾値を超えるのかを判断するステップと

を含み、

その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップは、

ｎとｍとの比例が所定の第１の比例閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断するステップを含む。

【０００８】

本発明の実施例に係る技術案は、各タイムスライス内のアクセス行為をモニタリングし、アクセス回数が持続して高い数値のままであるのかを検査することにより、アクセス行為に悪意があるか否かを判断するので、その評価結果がより正確になる、という有益な効果を奏する。

【０００９】

一実施例において、

前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、

前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するステップと、

取得した時間間隔に基づいて、アクセス行為の時間分散を計算するステップと、

前記時間分散が所定の分散閾値を超えるのかを判断するステップと

を含み、

その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップは、

前記時間分散が所定の分散閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断するステップを含む。

【００１０】

本発明の実施例に係る技術案は、時間間隔の分散計算を行うことにより、アクセス行為が固定頻度で発生するのかを判断し、アクセス行為が固定頻度で発生する場合、当該アク

セス行為は、ユーザによる行為ではなく、ソフトウェアによる行為であると判断することができるので、悪意のある行為をより正確に識別することができる、という有益な効果を奏する。

【００１１】

一実施例において、

前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、

前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するステップと、

取得した時間間隔に基づいて、アクセス行為の時間分散を計算するステップと、

前記時間分散と時間間隔の平均値との比率を計算するステップと、

前記比率が所定の第２の比例閾値より小さいかを判断するステップと

を含み、

その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップは、

前記比率が所定の第２の比例閾値より小さい場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断するステップを含む。

【００１２】

本発明の実施例に係る技術案は、分散と時間間隔の平均値をさらに比較することにより、悪意のある行為をより正確に識別することができる、という有益な効果を奏する。

【００１３】

一実施例において、

前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、

前記時間スライディングウィンドウ内のアクセス行為の総回数を取得するステップと、

前記総回数が所定の総回数閾値を超えるのかを判断するステップと、

その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップと、を含む。

【００１４】

本発明の実施例に係る技術案は、上記技術案を基に、アクセス行為の総回数を用いてアクセス行為をさらに評価することにより、悪意のある行為をより正確に識別することができる、という有益な効果を奏する。

【００１５】

本発明の実施例の第２の局面によれば、

所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得するための取得モジュールと、

前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するための評価モジュールと、

その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するための判断モジュールと

を含むユーザ行為識別装置を提供する。

【００１６】

一実施例において、

前記時間スライディングウィンドウは、ｍ個に等分されたタイムスライスを含み、

前記評価モジュールは、

タイムスライス内のアクセス回数が所定のスライス回数閾値を超えるかをタイムスライス毎に判断して、アクセス回数が所定のスライス回数閾値を超えるｎ個のタイムスライスを取得するためのタイムスライスサブモジュールと、

ｎとｍとの比例が所定の第１の比例閾値を超えるのかを判断するための第１比例サブモジュールと

を含み、
前記判断モジュールは、
ｎとｍとの比例が所定の第１の比例閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する。
【００１７】
一実施例において、
前記評価モジュールは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するための間隔サブモジュールと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算するための分散サブモジュールと、
前記時間分散が所定の分散閾値を超えるのかを判断するための第１の評価サブモジュールと
を含み、
前記判断モジュールは、
前記時間分散が所定の分散閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する。
【００１８】
一実施例において、
前記評価モジュールは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するための間隔サブモジュールと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算するための分散サブモジュールと、
前記時間分散と時間間隔の平均値との比率を計算するための比率サブモジュールと、
前記比率が所定の第２の比例閾値より小さいかを判断するための第２の比例サブモジュールと
を含み、
前記判断モジュールは、
前記比率が所定の第２の比例閾値より小さい場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する。
【００１９】
一実施例において、
前記評価モジュールは、
前記時間スライディングウィンドウ内のアクセス行為の総回数を取得するための総回数サブモジュールと、
前記総回数が所定の総回数閾値を超えるのかを判断するための総回数判断サブモジュールと、
その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するための第２の評価サブモジュールと、を含む。
【００２０】
本発明の実施例の第３の局面によれば、
プロセッサと、
プロセッサにより実行可能なインストラクションを格納するためのメモリと
を含むユーザ行為識別装置を提供するが、
前記プロセッサは、
所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得し、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価し、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるの

かを判断する
ように構成される。
【００２１】
以上の一般的な説明と以下のような細部的な説明は、例示的なものであって、本発明に対する限定として理解してはいけない。
【図面の簡単な説明】
【００２２】
以下の図面は、明細書に盛り込まれて明細書の一部分を構成し、本発明の実施例に対する説明に用いられるとともに、本発明の原理を解釈するために用いられる。
【図１】本発明の例示的な一実施例に係るユーザ行為識別方法のフローチャートである。
【図２】本発明の例示的な一実施例に係るユーザ行為識別方法のフローチャートである。
【図３】本発明の例示的な一実施例に係るユーザ行為識別方法のフローチャートである。
【図４】本発明の例示的な一実施例に係るユーザ行為識別装置のブロック図である。
【図５】本発明の例示的な一実施例に係る評価モジュールのブロック図である。
【図６Ａ】本発明の例示的な一実施例に係る評価モジュールのブロック図である。
【図６Ｂ】本発明の例示的な一実施例に係る評価モジュールのブロック図である。
【図７】本発明の例示的な一実施例に係る評価モジュールのブロック図である。
【図８】本発明の例示的な一実施例に係る装置のブロック図である。
【発明を実施するための形態】
【００２３】
以下、図面を参照して、例示的な実施例について詳細に説明する。以下の図面に関する説明において、別途の説明がない限り、異なる図面中の同一の符号は、同一又は類似する要素を示すこととする。以下の例示的実施例において説明する複数の実施形態は、本発明に係る全ての実施形態を代表するわけではない。逆に、それらは、添付の特許請求の範囲に記載される本発明の一部の態様を示す装置及び方法の例に過ぎない。
【００２４】
現在、ネットでのイベントが頻繁に行われ、ネット店舗は、期間限定の値引きイベントを頻繁に開催する。ユーザは、低価格商品を買うために、短い時間内に当該店舗のウェブサイトに頻繁にアクセスする。一部のユーザは、商品を争って買うために開発されたソフトウェアを利用して購入行為を行う。商品を争って買うために開発されたソフトウェアは、一般ユーザより高いアクセス頻度で店舗のウェブサイトをアクセスすることができる。しかし、商品を争って買うために開発されたソフトウェアによるアクセス行為は、一種の悪意のある行為に該当し、ウェブサイトが一時的に閲覧不能状態になりうる。一つの解決案として、所定時間内のアクセス回数が所定の閾値を超えるか否かを判断し、超える場合、悪意のあるアクセス行為が存在すると判断する。しかし、当該識別方法は、比較的単一であり、当該アクセス回数がユーザの行為によるものなのか、それとも商品を争って買うために開発されたソフトウェアによるものなのかを、正確に識別することができず、識別結果は正確でない。
【００２５】
本実施例では、当該問題を解決するために、端末によるアクセス行為を時間スライディングウィンドウにてモニタリングすることにより、端末によるアクセス行為に悪意があるか否かを正確に識別することができる。
【００２６】
本実施例における時間スライディングウィンドウは、動的な時間ウィンドウであり、長さが一定であり、例えば３６００秒間である。当該時間スライディングウィンドウは、終了位置が常に現在時間であるため、時間の経過とともに移動する。
【００２７】
従来技術における所定時間長さに基づいてアクセス回数を検出する技術案として、例えば、所定時間長さが１０００秒間であり、０～１０００秒の間に一回検出し、１００１～２０００秒の間に一回検出し、以降はこれをもって類推する。しかしながら、５００～１

５００秒の間に発生するアクセス行為は検出することができない。一方、本実施例では、時間スライディングウィンドウの移動に伴いリアルタイムに検出を行うようにする。例えば、時間スライディングウィンドウは、所定時間長さが１０００秒間であり、０～１０００秒の間に一回検出し、１～１００１秒の間に一回検出し、２～１００２秒の間に一回検出し、以降はこれをもって類推する。本実施例は、従来技術の技術案に比較し、検出結果がより正確で、悪意のある行為をより正確に識別することができる。

【００２８】

図１は、例示的な一実施例に係るユーザ行為識別方法のフローチャートである。当該方法は、サーバにより実現され、図１に示すように、以下のステップを含む。

【００２９】

ステップ１０１において、所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得する。

【００３０】

ステップ１０２において、前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価する。

【００３１】

ステップ１０３において、評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断する。

【００３２】

本実施例では、端末によるアクセス行為を時間スライディングウィンドウ内でリアルタイムにモニタリングすることができ、一定時間内のアクセス行為をモニタリングしてアクセス行為に悪意があるかを評価することができるので、識別結果がより正確になる。本実施例では、単一端末の行為に対してモニタリング及び評価を行っているが、ユーザ名、ＩＰ（インターネットプロトコル）アドレス又はＭＡＣ（媒体アクセス制御）アドレスなどにより端末を特定することができる。

【００３３】

悪意のあるアクセスの存在が識別されると、例えば、検証コードの送信を端末に要求するか、または、当該ユーザ（又は当該端末）のアクセスを一時的に遮断するか、または、当該ユーザをブラックリストに加えることにより当該ユーザのアクセスを永久に拒否するか、または、警告メッセージをユーザに送信するなど、複数種類の手段を採用することができる。

【００３４】

一実施例において、ステップ１０２はステップＡとして実現される。

【００３５】

ステップＡにおいて、前記時間スライディングウィンドウ中の各タイムスライス内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価する。

【００３６】

本実施例では、時間スライディングウィンドウをさらに同一長さ（等分）の複数のタイムスライスに細分する。例えば、時間スライディングウィンドウの所定時間長さが３６００秒間であり、１０個のタイムスライスを含む場合、各タイムスライスの時間長さは３６０秒間である。本実施例は、タイムスライスを単位にユーザのアクセス行為をモニタリングすることにより、モニタリングの粒度をさらに縮小することができ、悪意のある行為をより正確に識別することができる。しかも、本実施例では、各タイムスライス内のアクセス行為及び時間スライディングウィンドウ内の全体のアクセス行為に基づいて評価を行うため、その評価結果がより正確になる。

【００３７】

一実施例において、ステップＡは、ステップＡ１とステップＡ２とを含む。

【００３８】

ステップＡ１において、タイムスライス毎に、タイムスライス内のアクセス回数が所定

のスライス回数閾値を超えるのかを判断することにより、アクセス回数が所定のスライス回数閾値を超えるｎ個のタイムスライスを取得する。

【００３９】

ステップＡ２において、ｎとタイムスライス総数ｍの比例が所定の第１の比例閾値を超えるのかを判断する。

【００４０】

ステップ１０３は、ステップＡ３として実現される。

【００４１】

ステップＡ３において、ｎとｍとの比例が所定の第１の比例閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する。

【００４２】

即ち、アクセス回数が所定のスライス回数閾値を超えるタイムスライスを決定する。タイムスライス総数に占めるスライス回数閾値を超えるタイムスライスの数の比例が、所定の第１の比例閾値を超えるのかを判断する。その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価する。

【００４３】

本実施例において、タイムスライス総数に占めるスライス回数閾値を超えるタイムスライスの数の比例が、所定の第１の比例閾値を超える場合、アクセス回数が高すぎて、悪意のあるアクセスが存在すると判断する。そうでない場合、悪意のあるアクセスが存在しないと判断する。

【００４４】

例えば、時間スライディングウィンドウＴが３６００秒間の長さを有し、１０個のタイムスライスｔ１～ｔ１０を含む場合、各タイムスライスの長さは３６０秒間である。１０個のタイムスライスに対応するアクセス回数は、それぞれ、ｔ１＝５０、ｔ２＝６０、ｔ３＝５２、ｔ４＝５５、ｔ５＝４８、ｔ６＝５６、ｔ７＝５８、ｔ８＝５４、ｔ９＝５６、ｔ１０＝５７である。スライス回数閾値が５０であるとすれば、タイムスライスｔ５を除く他の９個のタイムスライスに対するアクセス回数は、いずれもスライス回数閾値を超えている。スライス回数閾値を超えるタイムスライスの数がタイムスライス総数に占める比例は、９／１０＝９０％として算出される。第１の比例閾値が９０％である場合、スライス回数閾値を超えるタイムスライスの数がタイムスライス総数に占める比例である９０％と第１の比例閾値である９０％を比較することにより、アクセス行為を評価して、当該時間スライディングウィンドウＴ内に悪意のあるアクセス行為が存在すると判断することができる。

【００４５】

一実施例において、ステップ１０２は、さらに、技術案Ｂにより実現される。

【００４６】

技術案Ｂのうち、

ステップＢ１において、前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得する。

【００４７】

ステップＢ２において、取得した時間間隔に基づいて、アクセス行為の時間分散を計算する。

【００４８】

ステップＢ３において、前記時間分散に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価する。ここで、前記時間分散が所定の分散閾値を超えるのかを判断する。

【００４９】

ステップ１０３において、前記時間分散が所定の分散閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する。

【００５０】

本実施例では、時間分散を所定の分散閾値と比較し、所定の分散閾値より大きい場合、分散が比較的大きいこと、即ちアクセス行為の時間間隔の変動が比較的大きいことを示しているので、当該アクセス行為は、商品を争って買うために開発されたソフトウェアによる行為ではなく、ユーザによる行為であると判断し、さらに、悪意のある行為が存在しないと判断することができる。逆に、所定の分散閾値以下である場合、悪意のある行為が存在すると判断する。

【００５１】

例えば、前記時間スライディングウィンドウ中の互い隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔ｘ１、ｘ２、ｘ３…ｘｎを取得する。この場合、以下の式により分散を算出することができる。

【００５２】

$$s^2 = \frac{1}{n}[(\mathrm{x1} - \bar{x})^2 + (\mathrm{x2} - \bar{x})^2 + \ldots (\mathrm{xn} - \bar{x})^2]$$

ここで、

$\bar{x}$

はｘ１～ｘｎの平均値であり、ｓは算出する分散である。

【００５３】

一実施例において、技術案Ｂは、ステップＡ１～Ａ３と組み合わせることができる。例えば、各タイムスライスに対応する分散を計算し、分散が分散閾値より大きいタイムスライスを特定して、分散が分散閾値より大きいタイムスライスの数とタイムスライス総数の比例を決定し、さらに、当該比例を第１の比例閾値と比較して、悪意のあるアセクスが存在するかを判断する。

【００５４】

一実施例において、技術案Ｂをさらに改良することができる。ステップＢ３は、ステップＢ３１～Ｂ３２を含むことができる。

【００５５】

前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得する。

【００５６】

取得した時間間隔に基づいて、アクセス行為の時間分散を計算する。

【００５７】

ステップＢ３１において、前記時間分散と時間間隔の平均値との比率を計算する。

【００５８】

ステップＢ３２において、前記比率が所定の第２の比例閾値より小さいか否かを判断する。その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価する。

【００５９】

ステップ１０３は、ステップＢ３３として実現される。

【００６０】

ステップＢ３３において、前記比率が所定の第２の比例閾値より小さい場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する。

【００６１】

本実施例において、時間分散と時間間隔の平均値との比率が所定の第２の比例閾値を超えると、当該時間分散を持つ時間間隔は時間間隔の平均値とは非常に近い値であるので、当該アクセス行為が、商品を争って買うために開発されたソフトウェアによる行為であり、悪意のあるアクセスが存在すると判断することができる。そうでない場合、当該アクセ

ス行為は、ユーザによる行為であり、悪意のあるアクセスが存在しないと判断することができる。

【００６２】

例えば、平均値ｘが１であり、時間分散が０．５である場合、時間分散と平均値との比例は５０％であり、所定の第２の比例閾値１００％より大きい。０．５である分散は、比較的小さいものの、平均値１からの外れ度合いが比較的大きい。

【００６３】

また、例えば、平均値ｘが１０であり、時間分散が０．５である場合、時間分散と平均値との比例は５％であり、所定の第２の比例閾値１０％より小さい。１０である平均値が比較的大きいため、０．５である時間分散を持つ時間間隔は平均値に非常に近い。

【００６４】

本実施例では、分散と平均値との接近度合い（他の面から見ると、外れ度合いとも言える）を比較することにより、アクセス行為をより正確に評価することができる。

【００６５】

一実施例において、ステップ１０２は、技術案Ｃとして実現される。

【００６６】

技術案Ｃのうち、

ステップＣ１において、前記時間スライディングウィンドウ内のアクセス行為の総回数を取得する。

【００６７】

ステップＣ２において、前記総回数が所定の総回数閾値を超えるのかを判断する。

【００６８】

ステップＣ３において、その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価する。

【００６９】

本実施例において、時間スライディングウィンドウ内のアクセス行為の総回数が総回数閾値を超えると、アクセス量が高すぎて、悪意のあるアクセスが存在すると判断する。そうでない場合、悪意のあるアクセスが存在しないと判断する。

【００７０】

一実施例において、技術案Ｃは、上記の技術案と組み合わせることができる。ステップＡ又は技術案Ｂの判断結果の基に、さらに、技術案Ｃの判断を行い、いずれも悪意のあるアクセスが存在すると判断される場合のみにおいて、悪意のあるアクセスが存在すると結論付けることができる。

【００７１】

以下、幾つかの実施例を通じて、ユーザ行為識別方法を紹介するようにする。

【００７２】

図２は、例示的な一実施例に係るユーザ行為識別方法のフローチャートである。当該方法は、サーバにより実現され、図２に示すように、以下のステップを含む。

【００７３】

ステップ２０１において、所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得する。

【００７４】

ステップ２０２において、時間スライディングウィンドウ中のタイムスライス毎に、タイムスライスに対応するアクセス回数を所定のスライス回数閾値と比較する。

【００７５】

ステップ２０３において、アクセス回数が所定のスライス回数閾値を超えるタイムスライスを決定する。

【００７６】

ステップ２０４において、スライス回数閾値を超えるタイムスライスの数がタイムスライス総数に占める比例を計算する。

【００７７】
ステップ２０５において、算出した比例が所定の第１の比例閾値を超えるのかを判断する。所定の第１の比例閾値を超える場合、ステップ２０６に移り、所定の第１の比例閾値を超えない場合、ステップ２０７に移る。
【００７８】
ステップ２０６において、悪意のあるアクセスが存在すると判断する。
【００７９】
ステップ２０７において、悪意のあるアクセスが存在しないと判断する。
【００８０】
本実施例では、タイムスライスを用いてアクセス行為をより細かくモニタリングすることができる。アクセス回数を小さい粒度にてモニタリングすることにより、悪意のあるアクセスが存在するかをより正確に識別することができる。
【００８１】
図３は、例示的な一実施例に係るユーザ行為識別方法のフローチャートである。当該方法は、サーバにより実現され、図３に示すように、以下のステップを含む。
【００８２】
ステップ３０１において、所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得する。
【００８３】
ステップ３０２において、前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得する。
【００８４】
ステップ３０３において、取得した時間間隔に基づいて、時間間隔の平均値を計算する。
【００８５】
ステップ３０４において、取得した時間間隔に基づいて、アクセス行為の時間分散を計算する。
【００８６】
ステップ３０５において、前記時間分散と時間間隔の平均値との比率を計算する。
【００８７】
ステップ３０６において、前記比率が所定の第２の比例閾値より小さいかを判断する。所定の第２の比例閾値より小さい場合、ステップ３０７に移り、所定の第２の比例閾値以上である場合、ステップ３０８に移る。
【００８８】
ステップ３０７において、悪意のあるアクセスが存在すると判断する。
【００８９】
ステップ３０８において、悪意のあるアクセスが存在しないと判断する。
【００９０】
本実施例では、分散を用いて、取得したアクセス行為が均一な時間間隔で発生したのかを判断する。そうである場合、ユーザによるアクセス行為ではなく、ソフトウェアによるアクセス行為であると判断し、悪意のあるアクセスが存在すると判断する。そうではない場合、悪意のあるアクセスが存在しないと判断する。当該方法によれば、悪意のあるアクセス行為をより正確に識別することができる。
【００９１】
以上の説明により、サーバにより実現されるユーザ行為識別方法がより一層明確になった。装置の内部構造と機能について以下に記載する。
【００９２】
図４は、例示的な一実施例に係るユーザ行為識別装置の模式図である。図４を参照して、当該装置は、取得モジュール４０１と、評価モジュール４０２と、判断モジュール４０３とを含む。

【００９３】
取得モジュール４０１は、所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得する。
【００９４】
評価モジュール４０２は、前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価する。
【００９５】
判断モジュール４０３は、その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断する。
【００９６】
一実施例において、前記時間スライディングウィンドウは、ｍ個に等分されたタイムスライスを含む。図５に示すように、前記評価モジュール４０２は、タイムスライスサブモジュール４０２１と、第１比例サブモジュール４０２８とを含む。
【００９７】
タイムスライスサブモジュール４０２１は、タイムスライス内のアクセス回数が所定のスライス回数閾値を超えるかをタイムスライス毎に判断して、アクセス回数が所定のスライス回数閾値を超えるｎ個のタイムスライスを取得する。
【００９８】
第１比例サブモジュール４０２８は、ｎとｍとの比例が所定の第１の比例閾値を超えるのかを判断する。
【００９９】
前記判断モジュール４０３は、ｎとｍとの比例が所定の第１の比例閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する。
【０１００】
一実施例において、前記評価モジュール４０２は、図６Ａに示すように、間隔サブモジュール４０２２と、分散サブモジュール４０２３と、第１の評価サブモジュール４０２４とを含む。
【０１０１】
間隔サブモジュール４０２２は、前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得する。
【０１０２】
分散サブモジュール４０２３は、取得した時間間隔に基づいて、アクセス行為の時間分散を計算する。
【０１０３】
第１の評価サブモジュール４０２４は、前記時間分散が所定の分散閾値を超えるのかを判断する。
【０１０４】
前記判断モジュール４０３は、前記時間分散が所定の分散閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する。
【０１０５】
一実施例において、タイムスライスサブモジュール４０２１は、間隔サブモジュール４０２２と、分散サブモジュール４０２３と、第１の評価サブモジュール４０２４とを含んでもよい。
【０１０６】
一実施例において、前記評価モジュール４０２は、図６Ｂに示すように、間隔サブモジュール４０２２と、分散サブモジュール４０２３と、比率サブモジュール４０２９と、第２の比例サブモジュール４０２１０とを含む。
【０１０７】
間隔サブモジュール４０２２は、前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得する。

【０１０８】
分散サブモジュール４０２３は、取得した時間間隔に基づいて、アクセス行為の時間分散を計算する。
【０１０９】
比率サブモジュール４０２９は、前記時間分散と時間間隔の平均値との比率を計算する。
【０１１０】
第２の比例サブモジュール４０２１０は、前記比率が所定の第２の比例閾値より小さいかを判断する。
【０１１１】
前記判断モジュール４０３は、前記比率が所定の第２の比例閾値より小さい場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する。
【０１１２】
一実施例において、前記評価モジュール４０２は、図７に示すように、総回数サブモジュール４０２５と、総回数判断サブモジュール４０２６と、第２の評価サブモジュール４０２７とを含む。
【０１１３】
総回数サブモジュール４０２５は、前記時間スライディングウィンドウ内のアクセス行為の総回数を取得する。
【０１１４】
総回数判断サブモジュール４０２６は、前記総回数が所定の総回数閾値を超えるのかを判断する。
【０１１５】
第２の評価サブモジュール４０２７は、その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価する。
【０１１６】
上記実施例に係る装置において、各モジュールによる操作の具体的な形態は、ユーザ行為識別方法に関する実施例において既に詳細に説明しているため、ここでは、その詳細な説明を省略するようにする。
【０１１７】
図８は、例示的な一実施例に係るユーザ行為識別に用いられる装置８００のブロック図である。例えば、装置８００は、コンピュータとして提供されてもよい。図８を参照して、装置８００は、１つ又は複数のプロセッサを含む処理アセンブリ８２２と、処理アセンブリ８２２により実行可能なインストラクション、例えばアプリケーションプログラムを格納するための、メモリ８３２をはじめとするメモリ資源を含む。メモリ８３２に格納されるアプリケーションプログラムは、それぞれ一組のインストラクションに対応する１つ又は複数のモジュールを含んでもよい。また、処理アセンブリ８２２は、インストラクションを実行することにより、上記のユーザ行為識別方法を実行するように配置される。
【０１１８】
装置８００は、装置８００の電源管理を実行するように配置される電源アセンブリ８２６と、装置８００をネットワークに接続するための１つの有線又は無線のネットワークインタフェース８５０と、１つの入出力（Ｉ／Ｏ）インタフェースス８５８とを含んでもよい。装置８００は、例えばＷｉｎｄｏｗｓ　ＳｅｒｖｅｒＴＭ、Ｍａｃ　ＯＳ　ＸＴＭ、ＵｎｉｘＴＭ、ＬｉｎｕｘＴＭ、ＦｒｅｅＢＳＤＴＭ又は類似するオペレーションシステムのような、メモリ８３２に格納されるオペレーションシステムを備えてもよい。
【０１１９】
プロセッサと、プロセッサにより実行可能なインストラクションを格納するためのメモリとを含むユーザ行為識別装置において、
前記プロセッサは、
所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得し、

前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価し、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断する、ように構成される。

【０１２０】

前記プロセッサは、さらに、
前記時間スライディングウィンドウは、ｍ個に等分されたタイムスライスを含み、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価することは、
タイムスライス内のアクセス回数が所定のスライス回数閾値を超えるかをタイムスライス毎に判断して、アクセス回数が所定のスライス回数閾値を超えるｎ個のタイムスライス取得することと、
ｎとｍとの比例が所定の第１の比例閾値を超えるのかを判断することを含み、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断することは、
ｎとｍとの比例が所定の第１の比例閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断することを含む
ように構成されてもよい。

【０１２１】

前記プロセッサは、さらに、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価することは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得することと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算することと、
前記時間分散が所定の分散閾値を超えるのかを判断することと、を含み、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断することは、
前記時間分散が所定の分散閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断することを含む
ように構成されてもよい。

【０１２２】

前記プロセッサは、さらに、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価することは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得することと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算することと、
前記時間分散と時間間隔の平均値との比率を計算することと、
前記比率が所定の第２の比例閾値より小さいか否かを判断することを含み、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断することは、
前記比率が所定の第２の比例閾値より小さい場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断することを含む
ように構成されてもよい。

【０１２３】

前記プロセッサは、さらに、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価することは、
前記時間スライディングウィンドウ内のアクセス行為の総回数を取得することと、

前記総回数が所定の総回数閾値を超えるのかを判断することと、
その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価することと、を含む
ように構成されてもよい。
【０１２４】
コンピュータ読み取り可能な非揮発性の記録媒体において、前記記録媒体中のインストラクションが移動端末のプロセッサにより実行される場合、移動端末がユーザ行為識別方法を実行することができる。
【０１２５】
前記ユーザ行為識別方法は、
所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得するステップと、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップと、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップと
を含む。
【０１２６】
前記記録媒体中のインストラクションは、さらに、
前記時間スライディングウィンドウは、ｍ個に等分されたタイムスライスを含み、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
タイムスライス内のアクセス回数が所定のスライス回数閾値を超えるかをタイムスライス毎に判断して、アクセス回数が所定のスライス回数閾値を超えるｎ個のタイムスライスを取得するステップと、
ｎとｍとの比例が所定の第１の比例閾値を超えるのかを判断するステップとを含み、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップは、
ｎとｍとの比例が所定の第１の比例閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断するステップを含む
ように構成されてもよい。
【０１２７】
前記記録媒体中のインストラクションは、さらに、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するステップと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算するステップと、
前記時間分散が所定の分散閾値を超えるのかを判断するステップと、を含み、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップは、
前記時間分散が所定の分散閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断するステップを含む
ように構成されてもよい。
【０１２８】
前記記録媒体中のインストラクションは、さらに、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するステップと、

取得した時間間隔に基づいて、アクセス行為の時間分散を計算するステップと、
前記時間分散と時間間隔の平均値との比率を計算するステップと、
前記比率が所定の第２の比例閾値より小さいかを判断するステップと、を含み、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップは、
前記比率が所定の第２の比例閾値より小さい場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断するステップを含む
ように構成されてもよい。

【０１２９】

前記記録媒体中のインストラクションは、さらに、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
前記時間スライディングウィンドウ内のアクセス行為の総回数を取得するステップと、
前記総回数が所定の総回数閾値を超えるのかを判断するステップと、
その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップと、を含む
ように構成されてもよい。

【０１３０】

当業者は、明細書を理解し、且つここで開示した発明を実施することにより、本発明の他の実施例に容易に想到することができる。本願は、本発明のあらゆる変更、用途または適応を含むことをその趣旨とする。これらの変更、用途または適応は、本発明の一般的な原理に基づき、本願において開示されていない本技術分野の公知常識又は慣用技術手段を含む。明細書と実施例は、単に例示的なものに過ぎない。本発明の範囲と精神は、添付の特許請求の範囲により示される。

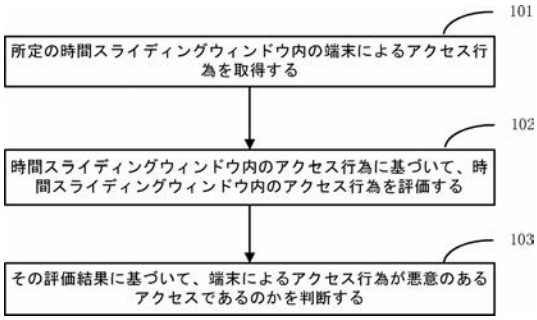
【０１３１】

本発明は、以上の記載および図面により示される正確な構造に限られることはなく、その範囲を逸脱しない限り様々な修正や変更が可能であることと、理解すべきである。本発明の範囲は、添付する特許請求の範囲のみにより限定される。

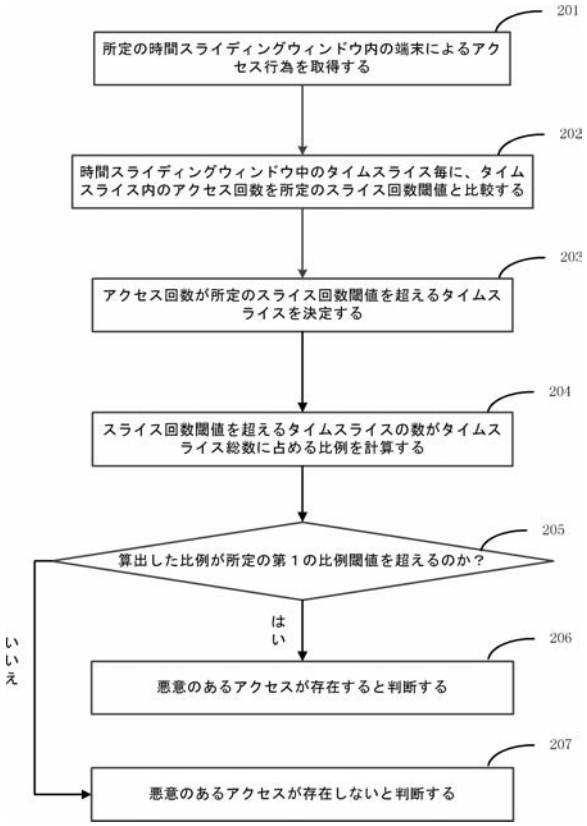
【０１３２】

本願は、出願番号がＣＮ２０１４１０７０８２８１．６であって、出願日が２０１４年１１月２７日である中国特許出願に基づき優先権を主張し、当該中国特許出願のすべての内容は本願に援用される。

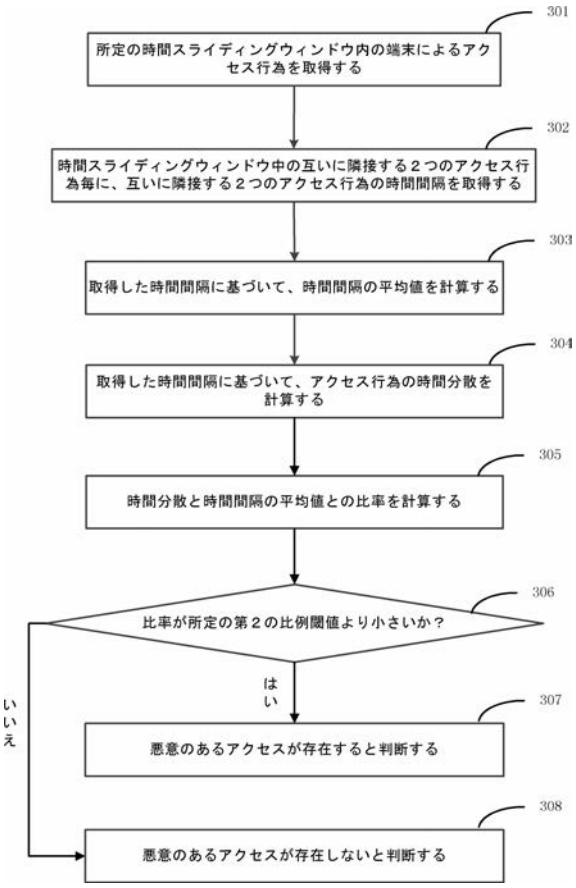
【図１】


101
所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得する
102
時間スライディングウィンドウ内のアクセス行為に基づいて、時間スライディングウィンドウ内のアクセス行為を評価する
103
その評価結果に基づいて、端末によるアクセス行為が悪意のあるアクセスであるのかを判断する

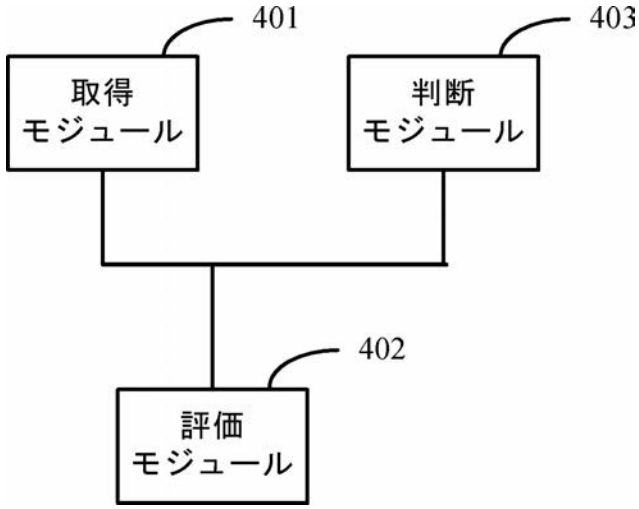
【図２】


201
所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得する
202
時間スライディングウィンドウ中のタイムスライス毎に、タイムスライス内のアクセス回数を所定のスライス回数閾値と比較する
203
アクセス回数が所定のスライス回数閾値を超えるタイムスライスを決定する
204
スライス回数閾値を超えるタイムスライスの数がタイムスライス総数に占める比例を計算する
205
算出した比例が所定の第１の比例閾値を超えるのか？
はい
いいえ
206
悪意のあるアクセスが存在すると判断する
207
悪意のあるアクセスが存在しないと判断する

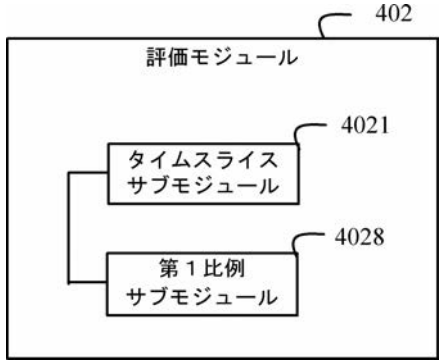
【図３】


301
所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得する
302
時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得する
303
取得した時間間隔に基づいて、時間間隔の平均値を計算する
304
取得した時間間隔に基づいて、アクセス行為の時間分散を計算する
305
時間分散と時間間隔の平均値との比率を計算する
306
比率が所定の第２の比例閾値より小さいか？
はい
いいえ
307
悪意のあるアクセスが存在すると判断する
308
悪意のあるアクセスが存在しないと判断する

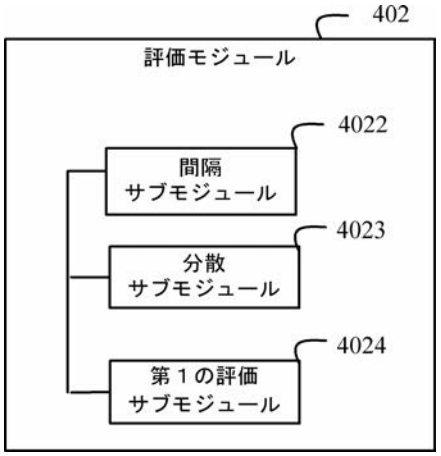
【図４】


401
取得
モジュール
403
判断
モジュール
402
評価
モジュール

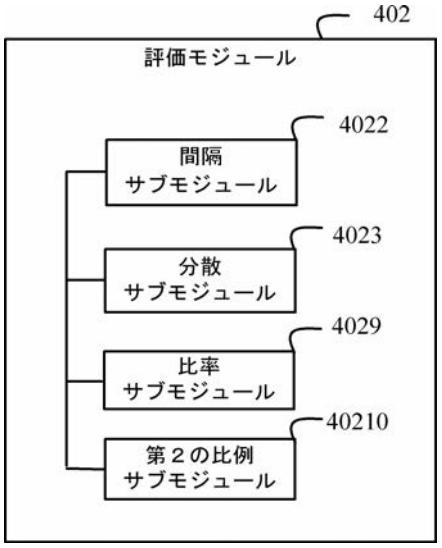
【図５】


402
評価モジュール
4021
タイムスライス
サブモジュール
4028
第１比例
サブモジュール

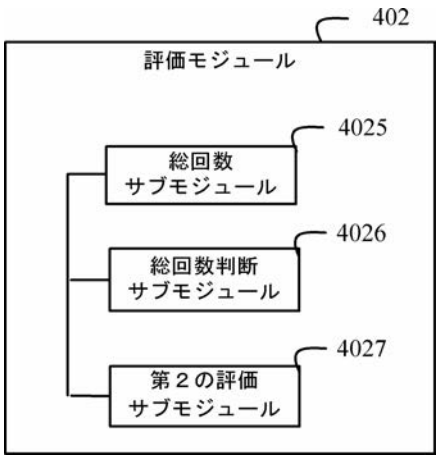
【図６Ａ】


402
評価モジュール
4022
間隔
サブモジュール
4023
分散
サブモジュール
4024
第１の評価
サブモジュール

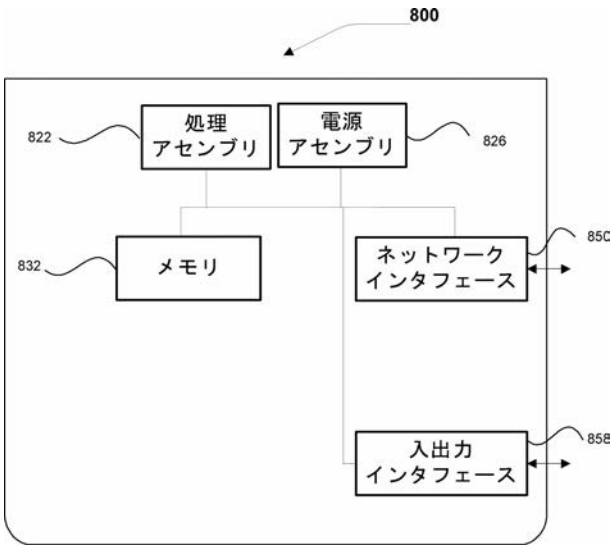
【図６Ｂ】


402
評価モジュール
4022
間隔
サブモジュール
4023
分散
サブモジュール
4029
比率
サブモジュール
40210
第２の比例
サブモジュール

【図７】


402
評価モジュール
4025
総回数
サブモジュール
4026
総回数判断
サブモジュール
4027
第２の評価
サブモジュール

【図８】


800
822
処理
アセンブリ
電源
アセンブリ
826
832
メモリ
ネットワーク
インタフェース
入出力
インタフェース

【手続補正書】
【提出日】平成27年6月25日(2015.6.25)
【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】
所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得するステップと、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップと、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップと
を含むことを特徴とするユーザ行為識別方法。
【請求項２】
前記時間スライディングウィンドウは、ｍ個に等分されたタイムスライスを含み、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
タイムスライス内のアクセス回数が所定のスライス回数閾値を超えるかをタイムスライス毎に判断して、アクセス回数が所定のスライス回数閾値を超えるｎ個のタイムスライスを取得するステップと、
ｎとｍとの比例が所定の第１の比例閾値を超えるのかを判断するステップと
を含み、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップは、
ｎとｍとの比例が所定の第１の比例閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断するステップを含む
ことを特徴とする請求項１に記載のユーザ行為識別方法。
【請求項３】
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するステップと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算するステップと、
前記時間分散が所定の分散閾値を超えるのかを判断するステップと
を含み、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップは、
前記時間分散が所定の分散閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断するステップを含む
ことを特徴とする請求項１に記載のユーザ行為識別方法。
【請求項４】
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するステップと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算するステップと、
前記時間分散と時間間隔の平均値との比率を計算するステップと、

前記比率が所定の第２の比例閾値より小さいかを判断するステップと
を含み、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップは、
前記比率が所定の第２の比例閾値より小さい場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断するステップを含む
ことを特徴とする請求項１に記載のユーザ行為識別方法。
【請求項５】
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
前記時間スライディングウィンドウ内のアクセス行為の総回数を取得するステップと、
前記総回数が所定の総回数閾値を超えるのかを判断するステップと、
その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップと、を含む
ことを特徴とする請求項１に記載のユーザ行為識別方法。
【請求項６】
所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得するための取得モジュールと、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するための評価モジュールと、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するための判断モジュールと
を含むことを特徴とするユーザ行為識別装置。
【請求項７】
前記時間スライディングウィンドウは、ｍ個に等分されたタイムスライスを含み、
前記評価モジュールは、
タイムスライス内のアクセス回数が所定のスライス回数閾値を超えるかをタイムスライス毎に判断して、アクセス回数が所定のスライス回数閾値を超えるｎ個のタイムスライスを取得するためのタイムスライスサブモジュールと、
ｎとｍとの比例が所定の第１の比例閾値を超えるのかを判断するための第１比例サブモジュールと
を含み、
前記判断モジュールは、
ｎとｍとの比例が所定の第１の比例閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する
ことを特徴とする請求項６に記載のユーザ行為識別装置。
【請求項８】
前記評価モジュールは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するための間隔サブモジュールと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算するための分散サブモジュールと、
前記時間分散が所定の分散閾値を超えるのかを判断するための第１の評価サブモジュールと
を含み、
前記判断モジュールは、
前記時間分散が所定の分散閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する
ことを特徴とする請求項６に記載のユーザ行為識別装置。
【請求項９】

前記評価モジュールは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するための間隔サブモジュールと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算するための分散サブモジュールと、
前記時間分散と時間間隔の平均値との比率を計算するための比率サブモジュールと、
前記比率が所定の第２の比例閾値より小さいかを判断するための第２の比例サブモジュールと
を含み、
前記判断モジュールは、
前記比率が所定の第２の比例閾値より小さい場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する
ことを特徴とする請求項６に記載のユーザ行為識別装置。
【請求項１０】
前記評価モジュールは、
前記時間スライディングウィンドウ内のアクセス行為の総回数を取得するための総回数サブモジュールと、
前記総回数が所定の総回数閾値を超えるのかを判断するための総回数判断サブモジュールと、
その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するための第２の評価サブモジュールと、を含む
ことを特徴とする請求項６に記載のユーザ行為識別装置。
【請求項１１】
プロセッサと、
プロセッサにより実行可能なインストラクションを格納するためのメモリと
を含む、ユーザ行為識別装置において、
前記プロセッサは、
所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得し、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価し、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断する、ように構成される
ことを特徴とするユーザ行為識別装置。
【請求項１２】
プロセッサにより実行されることにより、請求項１から請求項５のいずれか１項に記載のユーザ行為識別方法を実現することを特徴とするプログラム。
【請求項１３】
請求項１２に記載のプログラムが記録された記録媒体。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信及びコンピュータ処理の技術分野に関し、特に、ユーザ行為識別方法及びとユーザ行為識別装置、プログラム、及び記録媒体に関する。
【背景技術】
【０００２】

インターネットの発展に伴い、ネットワークを介する資源共有化が進みつつある。人々は、ネットワークを介して豊富な情報を素早く便利に取得することが可能になった。しかしながら、多くのウェブサイトは、人々が情報収集している間、悪意のある攻撃に晒されている。

【０００３】

本発明の発明者は、従来技術において、悪意のある攻撃は、比較的短い時間内に、ウェブサイトにデータパケットを頻繁に送信することを発見した。このような事象は、値引き商品を争って買うために短い時間内に頻繁にアクセスするウェブサイト中でよく起こる。このような高頻度のアクセス行為は、通常、商品を争って買うために開発されたソフトウェアにより実現され、人為的操作ではこのように高い頻度が得られない。従来技術において、当該悪意のある行為を阻止する手段がないのはないが、その阻止の効果が理想的ではない。従って、ユーザの悪意のある行為を、どのようにより効果的に識別するかは、早急に解決すべき問題である。

【発明の概要】

【０００４】

本発明は、従来技術に存在する上記のような問題を解決するために、ユーザ行為識別方法及びユーザ行為識別装置、プログラム、及び記録媒体を提供する。

【０００５】

本発明の実施例の第１の局面によれば、

所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得するステップと、

前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップと、

その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップと

を含むユーザ行為識別方法を提供する。

【０００６】

本発明の実施例に係る技術案は、ユーザのアクセス行為を時間スライディングウィンドウを用いてモニタリングして、アクセス行為を評価することにより、ユーザのアクセス行為に悪意があるか否かを判断する、という有益な効果を奏する。

【０００７】

一実施例において、

前記時間スライディングウィンドウは、ｍ個に等分されたタイムスライスを含み、

前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、

タイムスライス内のアクセス回数が所定のスライス回数閾値を超えるかをタイムスライス毎に判断して、アクセス回数が所定のスライス回数閾値を超えるｎ個のタイムスライスを取得するステップと、

ｎとｍとの比例が所定の第１の比例閾値を超えるのかを判断するステップと

を含み、

その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップは、

ｎとｍとの比例が所定の第１の比例閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断するステップを含む。

【０００８】

本発明の実施例に係る技術案は、各タイムスライス内のアクセス行為をモニタリングし、アクセス回数が持続して高い数値のままであるのかを検査することにより、アクセス行為に悪意があるか否かを判断するので、その評価結果がより正確になる、という有益な効果を奏する。

【０００９】

一実施例において、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するステップと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算するステップと、
前記時間分散が所定の分散閾値を超えるのかを判断するステップと
を含み、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップは、
前記時間分散が所定の分散閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断するステップを含む。
【００１０】
本発明の実施例に係る技術案は、時間間隔の分散計算を行うことにより、アクセス行為が固定頻度で発生するのかを判断し、アクセス行為が固定頻度で発生する場合、当該アクセス行為は、ユーザによる行為ではなく、ソフトウェアによる行為であると判断することができるので、悪意のある行為をより正確に識別することができる、という有益な効果を奏する。
【００１１】
一実施例において、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するステップと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算するステップと、
前記時間分散と時間間隔の平均値との比率を計算するステップと、
前記比率が所定の第２の比例閾値より小さいかを判断するステップと
を含み、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップは、
前記比率が所定の第２の比例閾値より小さい場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断するステップを含む。
【００１２】
本発明の実施例に係る技術案は、分散と時間間隔の平均値をさらに比較することにより、悪意のある行為をより正確に識別することができる、という有益な効果を奏する。
【００１３】
一実施例において、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
前記時間スライディングウィンドウ内のアクセス行為の総回数を取得するステップと、
前記総回数が所定の総回数閾値を超えるのかを判断するステップと、
その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップと、を含む。
【００１４】
本発明の実施例に係る技術案は、上記技術案を基に、アクセス行為の総回数を用いてアクセス行為をさらに評価することにより、悪意のある行為をより正確に識別することができる、という有益な効果を奏する。
【００１５】
本発明の実施例の第２の局面によれば、
所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得するための取

得モジュールと、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するための評価モジュールと、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するための判断モジュールと
を含むユーザ行為識別装置を提供する。
【００１６】
一実施例において、
前記時間スライディングウィンドウは、ｍ個に等分されたタイムスライスを含み、
前記評価モジュールは、
タイムスライス内のアクセス回数が所定のスライス回数閾値を超えるかをタイムスライス毎に判断して、アクセス回数が所定のスライス回数閾値を超えるｎ個のタイムスライスを取得するためのタイムスライスサブモジュールと、
ｎとｍとの比例が所定の第１の比例閾値を超えるのかを判断するための第１比例サブモジュールと
を含み、
前記判断モジュールは、
ｎとｍとの比例が所定の第１の比例閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する。
【００１７】
一実施例において、
前記評価モジュールは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するための間隔サブモジュールと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算するための分散サブモジュールと、
前記時間分散が所定の分散閾値を超えるのかを判断するための第１の評価サブモジュールと
を含み、
前記判断モジュールは、
前記時間分散が所定の分散閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する。
【００１８】
一実施例において、
前記評価モジュールは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するための間隔サブモジュールと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算するための分散サブモジュールと、
前記時間分散と時間間隔の平均値との比率を計算するための比率サブモジュールと、
前記比率が所定の第２の比例閾値より小さいかを判断するための第２の比例サブモジュールと
を含み、
前記判断モジュールは、
前記比率が所定の第２の比例閾値より小さい場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する。
【００１９】
一実施例において、
前記評価モジュールは、
前記時間スライディングウィンドウ内のアクセス行為の総回数を取得するための総回数

サブモジュールと、
前記総回数が所定の総回数閾値を超えるのかを判断するための総回数判断サブモジュールと、
その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するための第２の評価サブモジュールと、を含む。
【００２０】
本発明の実施例の第３の局面によれば、
プロセッサと、
プロセッサにより実行可能なインストラクションを格納するためのメモリと
を含むユーザ行為識別装置を提供するが、
前記プロセッサは、
所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得し、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価し、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断する
ように構成される。
本発明の実施例の第４の局面によれば、
プロセッサにより実行されることにより、本発明の実施例の第１の態様によるユーザ行為識別方法を実現するためのプログラムを提供する。
本発明の実施例の第５の局面によれば、
本発明の実施例の第４の態様によるプログラムが記録された記録媒体を提供する。
【００２１】
以上の一般的な説明と以下のような細部的な説明は、例示的なものであって、本発明に対する限定として理解してはいけない。
【図面の簡単な説明】
【００２２】
以下の図面は、明細書に盛り込まれて明細書の一部分を構成し、本発明の実施例に対する説明に用いられるとともに、本発明の原理を解釈するために用いられる。
【図１】本発明の例示的な一実施例に係るユーザ行為識別方法のフローチャートである。
【図２】本発明の例示的な一実施例に係るユーザ行為識別方法のフローチャートである。
【図３】本発明の例示的な一実施例に係るユーザ行為識別方法のフローチャートである。
【図４】本発明の例示的な一実施例に係るユーザ行為識別装置のブロック図である。
【図５】本発明の例示的な一実施例に係る評価モジュールのブロック図である。
【図６Ａ】本発明の例示的な一実施例に係る評価モジュールのブロック図である。
【図６Ｂ】本発明の例示的な一実施例に係る評価モジュールのブロック図である。
【図７】本発明の例示的な一実施例に係る評価モジュールのブロック図である。
【図８】本発明の例示的な一実施例に係る装置のブロック図である。
【発明を実施するための形態】
【００２３】
以下、図面を参照して、例示的な実施例について詳細に説明する。以下の図面に関する説明において、別途の説明がない限り、異なる図面中の同一の符号は、同一又は類似する要素を示すこととする。以下の例示的実施例において説明する複数の実施形態は、本発明に係る全ての実施形態を代表するわけではない。逆に、それらは、添付の特許請求の範囲に記載される本発明の一部の態様を示す装置及び方法の例に過ぎない。
【００２４】
現在、ネットでのイベントが頻繁に行われ、ネット店舗は、期間限定の値引きイベントを頻繁に開催する。ユーザは、低価格商品を買うために、短い時間内に当該店舗のウェブサイトに頻繁にアクセスする。一部のユーザは、商品を争って買うために開発されたソフトウェアを利用して購入行為を行う。商品を争って買うために開発されたソフトウェアは

、一般ユーザより高いアクセス頻度で店舗のウェブサイトをアクセスすることができる。しかし、商品を争って買うために開発されたソフトウェアによるアクセス行為は、一種の悪意のある行為に該当し、ウェブサイトが一時的に閲覧不能状態になりうる。一つの解決案として、所定時間内のアクセス回数が所定の閾値を超えるか否かを判断し、超える場合、悪意のあるアクセス行為が存在すると判断する。しかし、当該識別方法は、比較的単一であり、当該アクセス回数がユーザの行為によるものなのか、それとも商品を争って買うために開発されたソフトウェアによるものなのかを、正確に識別することができず、識別結果は正確でない。

【００２５】

本実施例では、当該問題を解決するために、端末によるアクセス行為を時間スライディングウィンドウにてモニタリングすることにより、端末によるアクセス行為に悪意があるか否かを正確に識別することができる。

【００２６】

本実施例における時間スライディングウィンドウは、動的な時間ウィンドウであり、長さが一定であり、例えば３６００秒間である。当該時間スライディングウィンドウは、終了位置が常に現在時間であるため、時間の経過とともに移動する。

【００２７】

従来技術における所定時間長さに基づいてアクセス回数を検出する技術案として、例えば、所定時間長さが１０００秒間であり、０～１０００秒の間に一回検出し、１００１～２０００秒の間に一回検出し、以降はこれをもって類推する。しかしながら、５００～１５００秒の間に発生するアクセス行為は検出することができない。一方、本実施例では、時間スライディングウィンドウの移動に伴いリアルタイムに検出を行うようにする。例えば、時間スライディングウィンドウは、所定時間長さが１０００秒間であり、０～１０００秒の間に一回検出し、１～１００１秒の間に一回検出し、２～１００２秒の間に一回検出し、以降はこれをもって類推する。本実施例は、従来技術の技術案に比較し、検出結果がより正確で、悪意のある行為をより正確に識別することができる。

【００２８】

図１は、例示的な一実施例に係るユーザ行為識別方法のフローチャートである。当該方法は、サーバにより実現され、図１に示すように、以下のステップを含む。

【００２９】

ステップ１０１において、所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得する。

【００３０】

ステップ１０２において、前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価する。

【００３１】

ステップ１０３において、評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断する。

【００３２】

本実施例では、端末によるアクセス行為を時間スライディングウィンドウ内でリアルタイムにモニタリングすることができ、一定時間内のアクセス行為をモニタリングしてアクセス行為に悪意があるかを評価することができるので、識別結果がより正確になる。本実施例では、単一端末の行為に対してモニタリング及び評価を行っているが、ユーザ名、ＩＰ（インターネットプロトコル）アドレス又はＭＡＣ（媒体アクセス制御）アドレスなどにより端末を特定することができる。

【００３３】

悪意のあるアクセスの存在が識別されると、例えば、検証コードの送信を端末に要求するか、または、当該ユーザ（又は当該端末）のアクセスを一時的に遮断するか、または、当該ユーザをブラックリストに加えることにより当該ユーザのアクセスを永久に拒否するか、または、警告メッセージをユーザに送信するなど、複数種類の手段を採用することが

できる。
【００３４】
一実施例において、ステップ１０２はステップＡとして実現される。
【００３５】
ステップＡにおいて、前記時間スライディングウィンドウ中の各タイムスライス内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価する。
【００３６】
本実施例では、時間スライディングウィンドウをさらに同一長さ（等分）の複数のタイムスライスに細分する。例えば、時間スライディングウィンドウの所定時間長さが３６００秒間であり、１０個のタイムスライスを含む場合、各タイムスライスの時間長さは３６０秒間である。本実施例は、タイムスライスを単位にユーザのアクセス行為をモニタリングすることにより、モニタリングの粒度をさらに縮小することができ、悪意のある行為をより正確に識別することができる。しかも、本実施例では、各タイムスライス内のアクセス行為及び時間スライディングウィンドウ内の全体のアクセス行為に基づいて評価を行うため、その評価結果がより正確になる。
【００３７】
一実施例において、ステップＡは、ステップＡ１とステップＡ２とを含む。
【００３８】
ステップＡ１において、タイムスライス毎に、タイムスライス内のアクセス回数が所定のスライス回数閾値を超えるのかを判断することにより、アクセス回数が所定のスライス回数閾値を超えるｎ個のタイムスライスを取得する。
【００３９】
ステップＡ２において、ｎとタイムスライス総数ｍの比例が所定の第１の比例閾値を超えるのかを判断する。
【００４０】
ステップ１０３は、ステップＡ３として実現される。
【００４１】
ステップＡ３において、ｎとｍとの比例が所定の第１の比例閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する。
【００４２】
即ち、アクセス回数が所定のスライス回数閾値を超えるタイムスライスを決定する。タイムスライス総数に占めるスライス回数閾値を超えるタイムスライスの数の比例が、所定の第１の比例閾値を超えるのかを判断する。その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価する。
【００４３】
本実施例において、タイムスライス総数に占めるスライス回数閾値を超えるタイムスライスの数の比例が、所定の第１の比例閾値を超える場合、アクセス回数が高すぎて、悪意のあるアクセスが存在すると判断する。そうでない場合、悪意のあるアクセスが存在しないと判断する。
【００４４】
例えば、時間スライディングウィンドウＴが３６００秒間の長さを有し、１０個のタイムスライスｔ１～ｔ１０を含む場合、各タイムスライスの長さは３６０秒間である。１０個のタイムスライスに対応するアクセス回数は、それぞれ、ｔ１＝５０、ｔ２＝６０、ｔ３＝５２、ｔ４＝５５、ｔ５＝４８、ｔ６＝５６、ｔ７＝５８、ｔ８＝５４、ｔ９＝５６、ｔ１０＝５７である。スライス回数閾値が５０であるとすれば、タイムスライスｔ５を除く他の９個のタイムスライスに対するアクセス回数は、いずれもスライス回数閾値を超えている。スライス回数閾値を超えるタイムスライスの数がタイムスライス総数に占める比例は、９／１０＝９０％として算出される。第１の比例閾値が９０％である場合、スライス回数閾値を超えるタイムスライスの数がタイムスライス総数に占める比例である９０

％と第１の比例閾値である９０％を比較することにより、アクセス行為を評価して、当該時間スライディングウィンドウＴ内に悪意のあるアクセス行為が存在すると判断することができる。

【００４５】

一実施例において、ステップ１０２は、さらに、技術案Ｂにより実現される。

【００４６】

技術案Ｂのうち、

ステップＢ１において、前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得する。

【００４７】

ステップＢ２において、取得した時間間隔に基づいて、アクセス行為の時間分散を計算する。

【００４８】

ステップＢ３において、前記時間分散に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価する。ここで、前記時間分散が所定の分散閾値を超えるのかを判断する。

【００４９】

ステップ１０３において、前記時間分散が所定の分散閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する。

【００５０】

本実施例では、時間分散を所定の分散閾値と比較し、所定の分散閾値より大きい場合、分散が比較的大きいこと、即ちアクセス行為の時間間隔の変動が比較的大きいことを示しているので、当該アクセス行為は、商品を争って買うために開発されたソフトウェアによる行為ではなく、ユーザによる行為であると判断し、さらに、悪意のある行為が存在しないと判断することができる。逆に、所定の分散閾値以下である場合、悪意のある行為が存在すると判断する。

【００５１】

例えば、前記時間スライディングウィンドウ中の互い隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔ｘ１、ｘ２、ｘ３…ｘｎを取得する。この場合、以下の式により分散を算出することができる。

【００５２】

$$s^2 = \frac{1}{n}[(\mathrm{x1} - \bar{x})^2 + (\mathrm{x2} - \bar{x})^2 + \ldots (\mathrm{xn} - \bar{x})^2]$$

ここで、

$\bar{x}$

はｘ１～ｘｎの平均値であり、ｓは算出する分散である。

【００５３】

一実施例において、技術案Ｂは、ステップＡ１～Ａ３と組み合わせることができる。例えば、各タイムスライスに対応する分散を計算し、分散が分散閾値より大きいタイムスライスを特定して、分散が分散閾値より大きいタイムスライスの数とタイムスライス総数の比例を決定し、さらに、当該比例を第１の比例閾値と比較して、悪意のあるアセクスが存在するかを判断する。

【００５４】

一実施例において、技術案Ｂをさらに改良することができる。ステップＢ３は、ステップＢ３１～Ｂ３２を含むことができる。

【００５５】

前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得する。

【００５６】

取得した時間間隔に基づいて、アクセス行為の時間分散を計算する。

【００５７】

ステップＢ３１において、前記時間分散と時間間隔の平均値との比率を計算する。

【００５８】

ステップＢ３２において、前記比率が所定の第２の比例閾値より小さいか否かを判断する。その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価する。

【００５９】

ステップ１０３は、ステップＢ３３として実現される。

【００６０】

ステップＢ３３において、前記比率が所定の第２の比例閾値より小さい場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する。

【００６１】

本実施例において、時間分散と時間間隔の平均値との比率が所定の第２の比例閾値未満である場合、当該時間分散を持つ時間間隔は時間間隔の平均値とは非常に近い値であるので、当該アクセス行為が、商品を争って買うために開発されたソフトウェアによる行為であり、悪意のあるアクセスが存在すると判断することができる。そうでない場合、当該アクセス行為は、ユーザによる行為であり、悪意のあるアクセスが存在しないと判断することができる。

【００６２】

例えば、平均値ｘが１であり、時間分散が０．５である場合、時間分散と平均値との比例は５０％であり、所定の第２の比例閾値１０％より大きい。０．５である分散は、比較的小さいものの、平均値１からの外れ度合いが比較的大きい。

【００６３】

また、例えば、平均値ｘが１０であり、時間分散が０．５である場合、時間分散と平均値との比例は５％であり、所定の第２の比例閾値１０％より小さい。１０である平均値が比較的大きいため、０．５である時間分散を持つ時間間隔は平均値に非常に近い。

【００６４】

本実施例では、分散と平均値との接近度合い（他の面から見ると、外れ度合いとも言える）を比較することにより、アクセス行為をより正確に評価することができる。

【００６５】

一実施例において、ステップ１０２は、技術案Ｃとして実現される。

【００６６】

技術案Ｃのうち、

ステップＣ１において、前記時間スライディングウィンドウ内のアクセス行為の総回数を取得する。

【００６７】

ステップＣ２において、前記総回数が所定の総回数閾値を超えるのかを判断する。

【００６８】

ステップＣ３において、その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価する。

【００６９】

本実施例において、時間スライディングウィンドウ内のアクセス行為の総回数が総回数閾値を超えると、アクセス量が高すぎて、悪意のあるアクセスが存在すると判断する。そうでない場合、悪意のあるアクセスが存在しないと判断する。

【００７０】

一実施例において、技術案Ｃは、上記の技術案と組み合わせることができる。ステップ

Ａ又は技術案Ｂの判断結果の基に、さらに、技術案Ｃの判断を行い、いずれも悪意のあるアクセスが存在すると判断される場合のみにおいて、悪意のあるアクセスが存在すると結論付けることができる。

【００７１】

以下、幾つかの実施例を通じて、ユーザ行為識別方法を紹介するようにする。

【００７２】

図２は、例示的な一実施例に係るユーザ行為識別方法のフローチャートである。当該方法は、サーバにより実現され、図２に示すように、以下のステップを含む。

【００７３】

ステップ２０１において、所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得する。

【００７４】

ステップ２０２において、時間スライディングウィンドウ中のタイムスライス毎に、タイムスライスに対応するアクセス回数を所定のスライス回数閾値と比較する。

【００７５】

ステップ２０３において、アクセス回数が所定のスライス回数閾値を超えるタイムスライスを決定する。

【００７６】

ステップ２０４において、スライス回数閾値を超えるタイムスライスの数がタイムスライス総数に占める比例を計算する。

【００７７】

ステップ２０５において、算出した比例が所定の第１の比例閾値を超えるのかを判断する。所定の第１の比例閾値を超える場合、ステップ２０６に移り、所定の第１の比例閾値を超えない場合、ステップ２０７に移る。

【００７８】

ステップ２０６において、悪意のあるアクセスが存在すると判断する。

【００７９】

ステップ２０７において、悪意のあるアクセスが存在しないと判断する。

【００８０】

本実施例では、タイムスライスを用いてアクセス行為をより細かくモニタリングすることができる。アクセス回数を小さい粒度にてモニタリングすることにより、悪意のあるアクセスが存在するかをより正確に識別することができる。

【００８１】

図３は、例示的な一実施例に係るユーザ行為識別方法のフローチャートである。当該方法は、サーバにより実現され、図３に示すように、以下のステップを含む。

【００８２】

ステップ３０１において、所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得する。

【００８３】

ステップ３０２において、前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得する。

【００８４】

ステップ３０３において、取得した時間間隔に基づいて、時間間隔の平均値を計算する。

【００８５】

ステップ３０４において、取得した時間間隔に基づいて、アクセス行為の時間分散を計算する。

【００８６】

ステップ３０５において、前記時間分散と時間間隔の平均値との比率を計算する。

【００８７】

ステップ３０６において、前記比率が所定の第２の比例閾値より小さいかを判断する。所定の第２の比例閾値より小さい場合、ステップ３０７に移り、所定の第２の比例閾値以上である場合、ステップ３０８に移る。

【００８８】

ステップ３０７において、悪意のあるアクセスが存在すると判断する。

【００８９】

ステップ３０８において、悪意のあるアクセスが存在しないと判断する。

【００９０】

本実施例では、分散を用いて、取得したアクセス行為が均一な時間間隔で発生したのかを判断する。そうである場合、ユーザによるアクセス行為ではなく、ソフトウェアによるアクセス行為であると判断し、悪意のあるアクセスが存在すると判断する。そうではない場合、悪意のあるアクセスが存在しないと判断する。当該方法によれば、悪意のあるアクセス行為をより正確に識別することができる。

【００９１】

以上の説明により、サーバにより実現されるユーザ行為識別方法がより一層明確になった。装置の内部構造と機能について以下に記載する。

【００９２】

図４は、例示的な一実施例に係るユーザ行為識別装置の模式図である。図４を参照して、当該装置は、取得モジュール４０１と、評価モジュール４０２と、判断モジュール４０３とを含む。

【００９３】

取得モジュール４０１は、所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得する。

【００９４】

評価モジュール４０２は、前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価する。

【００９５】

判断モジュール４０３は、その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断する。

【００９６】

一実施例において、前記時間スライディングウィンドウは、ｍ個に等分されたタイムスライスを含む。図５に示すように、前記評価モジュール４０２は、タイムスライスサブモジュール４０２１と、第１比例サブモジュール４０２８とを含む。

【００９７】

タイムスライスサブモジュール４０２１は、タイムスライス内のアクセス回数が所定のスライス回数閾値を超えるかをタイムスライス毎に判断して、アクセス回数が所定のスライス回数閾値を超えるｎ個のタイムスライスを取得する。

【００９８】

第１比例サブモジュール４０２８は、ｎとｍとの比例が所定の第１の比例閾値を超えるのかを判断する。

【００９９】

前記判断モジュール４０３は、ｎとｍとの比例が所定の第１の比例閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する。

【０１００】

一実施例において、前記評価モジュール４０２は、図６Ａに示すように、間隔サブモジュール４０２２と、分散サブモジュール４０２３と、第１の評価サブモジュール４０２４とを含む。

【０１０１】

間隔サブモジュール４０２２は、前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得する。

【０１０２】
分散サブモジュール４０２３は、取得した時間間隔に基づいて、アクセス行為の時間分散を計算する。
【０１０３】
第１の評価サブモジュール４０２４は、前記時間分散が所定の分散閾値を超えるのかを判断する。
【０１０４】
前記判断モジュール４０３は、前記時間分散が所定の分散閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する。
【０１０５】
一実施例において、タイムスライスサブモジュール４０２１は、間隔サブモジュール４０２２と、分散サブモジュール４０２３と、第１の評価サブモジュール４０２４とを含んでもよい。
【０１０６】
一実施例において、前記評価モジュール４０２は、図６Ｂに示すように、間隔サブモジュール４０２２と、分散サブモジュール４０２３と、比率サブモジュール４０２９と、第２の比例サブモジュール４０２１０とを含む。
【０１０７】
間隔サブモジュール４０２２は、前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得する。
【０１０８】
分散サブモジュール４０２３は、取得した時間間隔に基づいて、アクセス行為の時間分散を計算する。
【０１０９】
比率サブモジュール４０２９は、前記時間分散と時間間隔の平均値との比率を計算する。
【０１１０】
第２の比例サブモジュール４０２１０は、前記比率が所定の第２の比例閾値より小さいかを判断する。
【０１１１】
前記判断モジュール４０３は、前記比率が所定の第２の比例閾値より小さい場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断する。
【０１１２】
一実施例において、前記評価モジュール４０２は、図７に示すように、総回数サブモジュール４０２５と、総回数判断サブモジュール４０２６と、第２の評価サブモジュール４０２７とを含む。
【０１１３】
総回数サブモジュール４０２５は、前記時間スライディングウィンドウ内のアクセス行為の総回数を取得する。
【０１１４】
総回数判断サブモジュール４０２６は、前記総回数が所定の総回数閾値を超えるのかを判断する。
【０１１５】
第２の評価サブモジュール４０２７は、その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価する。
【０１１６】
上記実施例に係る装置において、各モジュールによる操作の具体的な形態は、ユーザ行為識別方法に関する実施例において既に詳細に説明しているため、ここでは、その詳細な説明を省略するようにする。
【０１１７】

図８は、例示的な一実施例に係るユーザ行為識別に用いられる装置８００のブロック図である。例えば、装置８００は、コンピュータとして提供されてもよい。図８を参照して、装置８００は、１つ又は複数のプロセッサを含む処理アセンブリ８２２と、処理アセンブリ８２２により実行可能なインストラクション、例えばアプリケーションプログラムを格納するための、メモリ８３２をはじめとするメモリ資源を含む。メモリ８３２に格納されるアプリケーションプログラムは、それぞれ一組のインストラクションに対応する１つ又は複数のモジュールを含んでもよい。また、処理アセンブリ８２２は、インストラクションを実行することにより、上記のユーザ行為識別方法を実行するように配置される。

【０１１８】

装置８００は、装置８００の電源管理を実行するように配置される電源アセンブリ８２６と、装置８００をネットワークに接続するための１つの有線又は無線のネットワークインタフェース８５０と、１つの入出力（Ｉ／Ｏ）インタフェースス８５８とを含んでもよい。装置８００は、例えばＷｉｎｄｏｗｓ　ＳｅｒｖｅｒＴＭ、Ｍａｃ　ＯＳ　ＸＴＭ、ＵｎｉｘＴＭ、ＬｉｎｕｘＴＭ、ＦｒｅｅＢＳＤＴＭ又は類似するオペレーションシステムのような、メモリ８３２に格納されるオペレーションシステムを備えてもよい。

【０１１９】

プロセッサと、プロセッサにより実行可能なインストラクションを格納するためのメモリとを含むユーザ行為識別装置において、

前記プロセッサは、

所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得し、

前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価し、

その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断する、ように構成される。

【０１２０】

前記プロセッサは、さらに、

前記時間スライディングウィンドウは、ｍ個に等分されたタイムスライスを含み、

前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価することは、

タイムスライス内のアクセス回数が所定のスライス回数閾値を超えるかをタイムスライス毎に判断して、アクセス回数が所定のスライス回数閾値を超えるｎ個のタイムスライス取得することと、

ｎとｍとの比例が所定の第１の比例閾値を超えるのかを判断することを含み、

その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断することは、

ｎとｍとの比例が所定の第１の比例閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断することを含む

ように構成されてもよい。

【０１２１】

前記プロセッサは、さらに、

前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価することは、

前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得することと、

取得した時間間隔に基づいて、アクセス行為の時間分散を計算することと、

前記時間分散が所定の分散閾値を超えるのかを判断することと、を含み、

その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断することは、

前記時間分散が所定の分散閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断することを含む

ように構成されてもよい。
【０１２２】
前記プロセッサは、さらに、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価することは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得することと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算することと、
前記時間分散と時間間隔の平均値との比率を計算することと、
前記比率が所定の第２の比例閾値より小さいか否かを判断することを含み、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断することは、
前記比率が所定の第２の比例閾値より小さい場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断することを含む
ように構成されてもよい。
【０１２３】
前記プロセッサは、さらに、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価することは、
前記時間スライディングウィンドウ内のアクセス行為の総回数を取得することと、
前記総回数が所定の総回数閾値を超えるのかを判断することと、
その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価することと、を含む
ように構成されてもよい。
【０１２４】
コンピュータ読み取り可能な非揮発性の記録媒体において、前記記録媒体中のインストラクションが移動端末のプロセッサにより実行される場合、移動端末がユーザ行為識別方法を実行することができる。
【０１２５】
前記ユーザ行為識別方法は、
所定の時間スライディングウィンドウ内の端末によるアクセス行為を取得するステップと、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップと、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップと
を含む。
【０１２６】
前記記録媒体中のインストラクションは、さらに、
前記時間スライディングウィンドウは、ｍ個に等分されたタイムスライスを含み、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
タイムスライス内のアクセス回数が所定のスライス回数閾値を超えるかをタイムスライス毎に判断して、アクセス回数が所定のスライス回数閾値を超えるｎ個のタイムスライスを取得するステップと、
ｎとｍとの比例が所定の第１の比例閾値を超えるのかを判断するステップとを含み、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップは、
ｎとｍとの比例が所定の第１の比例閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断するステップを含む

ように構成されてもよい。
【０１２７】
前記記録媒体中のインストラクションは、さらに、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するステップと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算するステップと、
前記時間分散が所定の分散閾値を超えるのかを判断するステップと、を含み、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップは、
前記時間分散が所定の分散閾値を超える場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断するステップを含む
ように構成されてもよい。
【０１２８】
前記記録媒体中のインストラクションは、さらに、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
前記時間スライディングウィンドウ中の互いに隣接する２つのアクセス行為毎に、互いに隣接する２つのアクセス行為の時間間隔を取得するステップと、
取得した時間間隔に基づいて、アクセス行為の時間分散を計算するステップと、
前記時間分散と時間間隔の平均値との比率を計算するステップと、
前記比率が所定の第２の比例閾値より小さいかを判断するステップと、を含み、
その評価結果に基づいて、前記端末によるアクセス行為が悪意のあるアクセスであるのかを判断するステップは、
前記比率が所定の第２の比例閾値より小さい場合、前記端末によるアクセス行為が悪意のあるアクセスであると判断するステップを含む
ように構成されてもよい。
【０１２９】
前記記録媒体中のインストラクションは、さらに、
前記時間スライディングウィンドウ内のアクセス行為に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップは、
前記時間スライディングウィンドウ内のアクセス行為の総回数を取得するステップと、
前記総回数が所定の総回数閾値を超えるのかを判断するステップと、
その判断結果に基づいて、前記時間スライディングウィンドウ内のアクセス行為を評価するステップと、を含む
ように構成されてもよい。
【０１３０】
当業者は、明細書を理解し、且つここで開示した発明を実施することにより、本発明の他の実施例に容易に想到することができる。本願は、本発明のあらゆる変更、用途または適応を含むことをその趣旨とする。これらの変更、用途または適応は、本発明の一般的な原理に基づき、本願において開示されていない本技術分野の公知常識又は慣用技術手段を含む。明細書と実施例は、単に例示的なものに過ぎない。本発明の範囲と精神は、添付の特許請求の範囲により示される。
【０１３１】
本発明は、以上の記載および図面により示される正確な構造に限られることはなく、その範囲を逸脱しない限り様々な修正や変更が可能であることと、理解すべきである。本発明の範囲は、添付する特許請求の範囲のみにより限定される。
【０１３２】
本願は、出願番号がＣＮ２０１４１０７０８２８１．６であって、出願日が２０１４年

１１月２７日である中国特許出願に基づき優先権を主張し、当該中国特許出願のすべての内容は本願に援用される。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/078019

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) 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)

H04L

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

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

CNPAT, WPI, EPODOC, CNKI, GOOGLE: presuppose recognition behaviour identify user action terminal time slide window malicious access evaluate

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 104486298 A (XIAOMI TECHNOLOGY CO., LTD.), 01 April 2015 (01.04.2015), claims 1-11	1-11
X	CN 102769549 A (TENCENT TECHNOLOGY (SHENZHEN) CO., LTD.), 07 November 2012 (07.11.2012), description, paragraphs 0057-0143, and figures 1-5	1-11
A	CN 101446956 A (BEIJING INSTITUTE OF TECHNOLOGY), 03 June 2009 (03.06.2009), the whole document	1-11
A	WO 2011022272 A2 (BEHAVIORAL RECOGNITION SYSTEMS, INC. et al.), 24 February 2011 (24.02.2011), the whole document	1-11

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

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
15 July 2015 (15.07.2015)	**29 July 2015 (29.07.2015)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **ZHAO, Tianqi** Telephone No.: (86-10) **61648112**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/078019

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 104486298 A	01 April 2015	None	
CN 102769549 A	07 November 2012	None	
CN 101446956 A	03 June 2009	None	
WO 2011022272 A2	24 February 2011	US 2011043625 A1	24 February 2011

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号
PCT/CN2015/078019

A. 主题的分类

H04L 29/06 (2006.01) i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT, WPI, EPODOC, CNKI, GOOGLE: 识别 用户 行为 终端 时间 滑动 窗口 恶意 访问 评估 预设 recognition behavior identify user action terminal time slide window malicious access evaluate

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 104486298 A (小米科技有限责任公司) 2015年 4月 1日 (2015-04-01) 权利要求1-11	1-11
X	CN 102769549 A (腾讯科技深圳有限公司) 2012年 11月 7日 (2012-11-07) 说明书第0057-0143段，图1-5	1-11
A	CN 101446956 A (北京理工大学) 2009年 6月 3日 (2009-06-03) 全文	1-11
A	WO 2011022272 A2 (BEHAVIORAL RECOGNITION SYSTEMS, INC.等) 2011年 2月 24日 (2011-02-24) 全文	1-11

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2015年 7月 15日	2015年 7月 29日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 北京市海淀区蓟门桥西土城路6号 100088 中国	赵天奇
传真号 (86-10)62019451	电话号码 (86-10)61648112

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/078019

检索报告引用的专利文件			公布日（年/月/日）		同族专利		公布日（年/月/日）
CN	104486298	A	2015年 4月 1日		无		
CN	102769549	A	2012年 11月 7日		无		
CN	101446956	A	2009年 6月 3日		无		
WO	2011022272	A2	2011年 2月 24日	US	2011043625	A1	2011年 2月 24日

表 PCT/ISA/210（同族专利附件）（2009年7月）

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,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,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,UG,US

(72)発明者 ジャン フア
中華人民共和国 １０００８５ ベイジン ハイディアン ディストリクト キンヘ ミドル ストリート ナンバー ６８ レインボー シティ ショッピング モール ２ オブ チャイナ リソーシズ フロア １３ シャオミ・インコーポレイテッド内
(72)発明者 シャー イー
中華人民共和国 １０００８５ ベイジン ハイディアン ディストリクト キンヘ ミドル ストリート ナンバー ６８ レインボー シティ ショッピング モール ２ オブ チャイナ リソーシズ フロア １３ シャオミ・インコーポレイテッド内
(72)発明者 ホン ディンクン
中華人民共和国 １０００８５ ベイジン ハイディアン ディストリクト キンヘ ミドル ストリート ナンバー ６８ レインボー シティ ショッピング モール ２ オブ チャイナ リソーシズ フロア １３ シャオミ・インコーポレイテッド内
(72)発明者 ワン ハイジュウ
中華人民共和国 １０００８５ ベイジン ハイディアン ディストリクト キンヘ ミドル ストリート ナンバー ６８ レインボー シティ ショッピング モール ２ オブ チャイナ リソーシズ フロア １３ シャオミ・インコーポレイテッド内