【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成18年1月5日(2006.1.5)

【公表番号】特表2004-537916(P2004-537916A)
【公表日】平成16年12月16日(2004.12.16)
【年通号数】公開・登録公報2004-049
【出願番号】特願2003-518110(P2003-518110)
【国際特許分類】
Ｈ０４Ｌ　12/66　(2006.01)
Ｇ０６Ｆ　13/00　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　12/66　Ｂ
Ｇ０６Ｆ　13/00　６１０Ｑ

【手続補正書】
【提出日】平成17年7月14日(2005.7.14)
【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】
通信網上で作動するシステムに係る振舞い形式を識別する方法であって、該システムは複数の、サーバ計算機とクライアント計算機とを含み、少くとも若干のサーバ計算機は該通信網上で１またはそれ以上のクライアント計算機との間でデータを配信し、また受信するようになっていて、該方法は、
（ａ）該システム内部で送られたデータアイテムに係る識別データを受信する段階であって、送られた各データアイテムについて、受信した識別データは、該システム内部で該データアイテムが送られた配信先か配送元かあるいはその両方の計算機を識別する段階と、
（ｂ）該受信した識別データを該システム内部で送られたデータアイテムの分布を示している提示に、識別された計算機の機能として、組織する段階と、
（ｃ）該提示を用いて分類手段を学習訓練して複数の振舞い形式を認識する段階とを備えている。
【請求項２】
請求項１記載の方法であって、段階（ｂ）は該システムにおけるサーバ及びクライアント計算機のトポロジカルな提示を作ることを含んでおり、また該方法は、各受信したデータアイテムについて、該識別された計算機と関係している活動のレベルを表わしているカウンタをインクレメントする段階と、
活動のレベルを示している識別子を該識別された計算機に対応している該トポロジカルな提示のどんな部分に対しても加え、それによって該システム内部で送られたデータの分布を表わしている提示を創る段階とを備えている方法。
【請求項３】
請求項２記載の方法において、前記トポロジカルな提示は、該網の領域をそれぞれが表わしている複数の地域と、
該網の対応している領域内部のサーバ計算機をそれぞれが表わしている複数の部分地域と、
対応しているサーバ計算機に対してクライアントとして動作しているクライアント計算機をそれぞれが表わしている複数の副次の部分地域とを含んでいて、さらに、

該識別された計算機に対応しているトポロジカルな提示のどの部分に対しても識別子を加える前記段階はどの部分地域または副次の部分地域でも対応がとれているものに対して識別子を加えることを含んでいる。
【請求項４】
請求項３記載の方法であって、前記変換する段階は、該提示を活動の頻度提示に変換することと、該頻度表示をベクトルに変換して、このベクトルが分類手段への入力に適したものとすることとを含んでいる方法。
【請求項５】
請求項１記載の方法において、該受信したデータアイテムはさらに該システム内部で送られたデータの属性を識別し、
また段階（ｂ）は、該システム内のサーバ計算機間のリンクにそれぞれが対応している複数のリストを創る段階を備え、また、
各受信したデータアイテムについて、該対応している送られたデータが通ったリンクを識別する段階と、
該識別されたリンクに対応しているリストを識別する段階と、
該データアイテムの属性を識別する段階と、
各識別された属性について、該識別されたリスト内で対応しているカウンタをインクレメントする段階とを含んでいる。
【請求項６】
請求項５記載の方法において、該方法は複数の異なるサイズの時間期間について実行され、それによって各サイズの時間期間について複数の振舞いの形式が存在するようになる。
【請求項７】
請求項１ないし請求項６のいずれか１項記載の方法において、受信されているデータが電子メールデータである方法。
【請求項８】
請求項７記載の方法において、前記受信段階（ａ）は、ファイヤウォール構成の一部となっているログファイルか、電子メールサーバ機械からアクセス可能なログファイルか、複数の電子メールサーバ機械からアクセス可能な複数のログファイルかのいずれかからデータを収集することを含んでいる。
【請求項９】
複数のサーバ計算機及びクライアント計算機を含むシステム内部で送られた未知のデータアイテムに係る異常な振舞いを識別する方法であって、
未知のデータアイテムに係るデータを受信する段階と、
請求項２もしくは請求項５のいずれかの記載により該受信したデータを提示に組織する段階と、
請求項４の記載により該提示を該分類手段への入力に適したフォーマットに変換する段階と、
該変換された提示を該学習訓練した分類手段に入力する段階と、
該未知のデータを振舞いの形式として分類するために該分類手段を作動する段階とを含む方法。
【請求項１０】
通信網内部で動作するシステムに係る異常な振舞いを識別する装置であって、該システムは複数のサーバ計算機及びクライアント計算機を備え、各サーバ計算機は該通信網上で１またはそれ以上のクライアント計算機との間で、データを送りまたデータを受けるように構成されており、また、該装置は、
該システム内部で送られたデータアイテムに係るデータを受信するように構成されてた受信手段であって、受信したデータアイテムの各々は、ある時間期間中に前記データアイテムが送られた配信先か配送元かあるいはその両方の計算機を該システム内部で識別する手段と、

該受信したデータを、送られたデータの形式の機能として、受信したデータの群とするようにし、それによって各群が振舞いの形式を表わすようにする動作可能な手段と、
各群におけるデータを組織して、該システム内部で送られたデータの分布を該時間期間中に識別された計算機の機能として示している提示にするように構成された組織用手段と、
入力として該提示を受領するように動作可能であり、かつ該群に対応している振舞いを表す出力を生成するように動作可能である分類手段とを具備する。
【請求項１１】
請求項１０記載の装置において、該受信用手段はファイヤウォール構成の一部であるログファイルか、サーバ機械からアクセス可能なログファイルか、あるいは複数のサーバ機械からアクセス可能な複数のログファイルかのいずれか１つからデータを検索するよう動作可能な手段と動作上関係している。
【請求項１２】
該組織用手段が該システムのサーバ及びクライアント計算機の活動のレベルを示す提示を創るように構成された手段を含む請求項１０記載の装置。
【請求項１３】
請求項１０記載の装置であって、少くとも若干のサーバ計算機を通るデータを解析し、かつ該解析されたデータと関係している属性を識別するように構成された手段を含み、該解析されたデータに係る受信したデータは前記サーバ計算機と識別された属性とを識別する装置。
【請求項１４】
該分類手段は、ニューラル網か、統計的分類器か、パターン認識器かのいずれか１つを備えている請求項１０ないし請求項１３のいずれか１項記載の装置。
【請求項１５】
該受信したデータが電子メールデータである請求項１０ないし請求項１４のいずれか１項記載の装置。
【請求項１６】
電子メールビールスを識別するのに使用するための電子メール活動デバイスであって、該デバイスは網の中に置かれて、該網内の他のデバイスと通信するように動作可能であり、
ファイヤウォール構成の一部であるログファイルか、電子メールサーバ機械からアクセス可能なログファイルか、あるいは複数の電子メールサーバ機械からアクセス可能な複数のログファイルのいずれか１つからある時間期間中に電子メールトラヒックを表わすデータを検索するように動作可能な検索手段と、
該検索したデータを該期間中の前記電子メールトラヒックの分布を示す提示に組織するように構成された組織手段と、
該提示を分類手段への入力として適したフォーマットに変換するように構成された変換手段と、
該変換された提示を入力として受領するように動作可能であり、かつ電子メールトラヒックの形式を表わしている出力を生成するように動作可能である分類手段とを含む電子メール活動デバイス。