(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6091436号
(P6091436)
(45)発行日　平成29年3月8日(2017.3.8)　(24)登録日　平成29年2月17日(2017.2.17)

(51)Int.Cl.　　F I
G06F 13/00 (2006.01)　　G06F 13/00 351N
H04L 12/26 (2006.01)　　H04L 12/26

請求項の数 27　(全 15 頁)

(21)出願番号　特願2013-554956(P2013-554956)
(86)(22)出願日　平成24年1月31日(2012.1.31)
(65)公表番号　特表2014-509015(P2014-509015A)
(43)公表日　平成26年4月10日(2014.4.10)
(86)国際出願番号　PCT/IB2012/050451
(87)国際公開番号　WO2012/114215
(87)国際公開日　平成24年8月30日(2012.8.30)
審査請求日　平成26年8月13日(2014.8.13)
審判番号　不服2016-5237(P2016-5237/J1)
審判請求日　平成28年4月8日(2016.4.8)
(31)優先権主張番号　11155862.3
(32)優先日　平成23年2月24日(2011.2.24)
(33)優先権主張国　欧州特許庁(EP)

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
INTERNATIONAL BUSINESS MACHINES CORPORATION
アメリカ合衆国10504　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
New Orchard Road, Armonk, New York 10504, United States of America
(74)代理人　100108501
弁理士　上野　剛史

最終頁に続く

(54)【発明の名称】ネットワーク・イベント管理のための装置、方法、およびコンピュータ・プログラム

(57)【特許請求の範囲】
【請求項１】
ネットワーク・イベント・フラッドを予測するための装置であって、
１つまたは複数のデバイスからのイベント放出レートを検出するためのイベント・レート検出器と、
複数の前記デバイスからの前記イベント放出レートの集約レートおよび集約レート・トレンドを生成するためのアグリゲータと、
複数の期間にわたる複数の前記集約レート・トレンドの最大許容イベント・レート値を含む複数のレベルを生成するためのレベル生成器と、
前記複数のレベルを記憶するための記憶構成要素と、
現在の集約レート・トレンドと前記レベルの１つ又は複数とを比較するための比較器であって、前記複数のレベルそれぞれが異なる予め定められた時点で用いられ、前記比較が当該予め定められた異なる時点で繰り返される、前記比較器と、
前記現在の集約レート・トレンドが第１の時点で前記レベルの前記１つ又は複数のうちの一つを超えることを前記比較器が検出するのに応答して、予測イベント・フラッドを示す信号を送信するための信号器と
を備えている、前記装置。
【請求項２】
前記アグリゲータは、平均イベント・レートを計算するためのアベレージャを備えている、請求項１に記載の装置。

【請求項３】
前記アグリゲータは、統計的に正規化された集約レートまたは集約レート・トレンドを計算するための統計計算器を備えている、請求項１又は２に記載の装置。
【請求項４】
前記統計的に正規化された集約レートまたは集約レート・トレンドは、正規化されたトレンドを定義する、請求項３に記載の装置。
【請求項５】
前記正規化されたトレンドは、最小二乗法によって計算される、請求項４に記載の装置。
【請求項６】
前記複数の期間は、時刻、曜日、月のうちの日、年のうちの日のうちの、１つまたは複数に従って定義される、請求項１～５のいずれか一項に記載の装置。
【請求項７】
前記信号器に応答して、前記第１の時点で最大のイベント放出レートを有するデバイスから前記第１の時点で最小のイベント放出レートを有するデバイスへと、降順で前記デバイスの識別子リストを順序付けするための、順序付け構成要素をさらに備えている、請求項１～６のいずれか一項に記載の装置。
【請求項８】
前記識別子リストから前記第１の時点で最大のイベント放出レートを有する前記デバイスを選択するため、および、前記デバイスをフラッド保護モードに配置するための候補デバイスとして識別するための、第１のセレクタをさらに備えている、請求項７に記載の装置。
【請求項９】
前記フラッド保護モードは、前記デバイスからの低減イベント放出レートを受信器に受け入れさせる、請求項８に記載の装置。
【請求項１０】
前記受信器はネットワーク・モニタを備えている、請求項９に記載の装置。
【請求項１１】
前記ネットワーク・モニタはプローブを備えている、請求項１０に記載の装置。
【請求項１２】
前記候補デバイスをフラッド保護デバイスとして前記フラッド保護モードに配置するためのフラッド保護制御構成要素をさらに備えている、請求項８～１１のいずれか一項に記載の装置。
【請求項１３】
第２の時点で最小のイベント放出レートを有するフラッド保護デバイスを選択するため、および、前記デバイスを前記フラッド保護モードから除去するための候補デバイスとして識別するための、第２のセレクタをさらに備えている、請求項１２に記載の装置。
【請求項１４】
ネットワーク・イベント・フラッドを予測するための方法であって、
イベント・レート検出器によって、１つまたは複数のデバイスからのイベント放出レートを検出するステップと、
アグリゲータによって、複数の前記デバイスからの前記イベント放出レートの集約レートおよび集約レート・トレンドを生成するステップと、
レベル生成器によって、複数の期間にわたる複数の前記集約レート・トレンドの最大許容イベント・レート値を含む複数のレベルを生成するステップと、
記憶構成要素によって、前記複数のレベルを記憶するステップと、
比較器によって、現在の集約レート・トレンドと前記レベルの１つ又は複数とを比較するステップであって、前記複数のレベルそれぞれが予め定められた異なる時点で用いられ、前記比較が当該予め定められた異なる時点で繰り返される、前記比較するステップと、
信号器によって、前記現在の集約レート・トレンドが第１の時点で前記レベルの前記１

つ又は複数のうちの一つを超えることを前記比較器が検出するのに応答して、予測イベント・フラッドを示す信号を送信するステップと
を含む、前記方法。
【請求項１５】
前記集約レートおよび集約レート・トレンドを生成するステップが、平均イベント・レートを計算するためのアベレージャを使用するステップを含む、請求項１４に記載の方法。
【請求項１６】
前記集約レートおよび集約レート・トレンドを生成するステップが、統計的に正規化された集約レートまたは集約レート・トレンドを計算するための統計計算器を使用するステップを含む、請求項１４又は１５のいずれか一項に記載の方法。
【請求項１７】
前記統計的に正規化された集約レートまたは集約レート・トレンドは、正規化されたトレンドを定義する、請求項１６に記載の方法。
【請求項１８】
前記正規化されたトレンドは、最小二乗法によって計算される、請求項１７に記載の方法。
【請求項１９】
前記複数の期間は、時刻、曜日、月のうちの日、年のうちの日のうちの、１つまたは複数に従って定義される、請求項１４～１８のいずれか一項に記載の方法。
【請求項２０】
順序付け構成要素によって、前記信号器に応答して、前記第１の時点で最大のイベント放出レートを有するデバイスから前記第１の時点で最小のイベント放出レートを有するデバイスへと、降順で前記デバイスの識別子リストを順序付けするステップをさらに含む、請求項１４～１９のいずれか一項に記載の方法。
【請求項２１】
前記識別子リストから前記第１の時点で最大のイベント放出レートを有する前記デバイスを選択し、前記デバイスをフラッド保護モードに配置するための候補デバイスとして識別するステップをさらに含む、請求項２０に記載の方法。
【請求項２２】
前記フラッド保護モードは、前記デバイスからの低減イベント放出レートを受信器に受け入れさせる、請求項２１に記載の方法。
【請求項２３】
前記受信器はネットワーク・モニタを備えている、請求項２２に記載の方法。
【請求項２４】
前記ネットワーク・モニタはプローブを備えている、請求項２３に記載の方法。
【請求項２５】
フラッド保護制御構成要素によって、前記候補デバイスをフラッド保護デバイスとして前記フラッド保護モードに配置するステップをさらに含む、請求項２１～２４のいずれか一項に記載の方法。
【請求項２６】
第２の時点で最小のイベント放出レートを有するフラッド保護デバイスを選択し、前記デバイスを前記フラッド保護モードから除去するための候補デバイスとして識別するステップをさらに含む、請求項２５に記載の方法。
【請求項２７】
コンピュータ・システムに、請求項１４～２６のいずれか一項に記載の方法の各ステップを実行させる、コンピュータ・プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、ネットワーク・イベント管理の分野に関する。具体的に言えば、本発明はネットワーク・イベント・フラッド（flood）を予測するため、およびかかる予測されるフラッドからネットワークを保護するための、装置および方法に関する。

【背景技術】

【０００２】

使用可能なネットワーク管理システムはいくつかある。これらのシステムは、異種デバイスからネットワークを介して障害情報を収集した後、オペレータがネットワークを管理し、これを効率的に修復できるような形で、この情報を相関、分類、優先順序付け、および提示する。加えて、将来の潜在的な問題を予測するために、ネットワーク・デバイスから収集された動作データに基本的な予測統計分析技法が適用されてきた。

【０００３】

ネットワーク管理は、ネットワーク内の様々なデバイスからデータを収集することを含む。知られた実装では、多くの種類のネットワーク・デバイスおよびシステムから大量のソース・データを提供できるこのタスクを実行するために、プローブまたはエージェントなどの多種多様な監視デバイスを使用する。

【０００４】

非常に大規模なネットワークを管理する際の問題の１つは、特にネットワーク・カスケード障害が発生する場合、非常に多くの障害イベントを発生させる可能性のあるネットワーク障害モードが存在することである。多数の障害イベントは、ネットワーク管理システムをフラッドさせ、システムを無反応にし、さらにオペレータが障害の原因を分離するかまたは修復作業を効率良く優先順位付けするのを困難にする可能性がある。既存のソリューションでは、（複数のデバイスからのデータの収集が可能な）監視プローブは、障害イベント・レートが所与のしきい値を超えるとシャットダウンを開始し、その後レベルがしきい値未満に戻ると再起動を開始することができる。しかしながらこの時点までに、しばしばカスケード障害の発生はすでに開始されており、多くの他のデバイスは管理システムのフラッドを開始している可能性がある。典型的には、このフラッド保護の基本形が活動化される前に、すでに多数の障害イベントがシステム内に常駐していることにもなる。不利なことに、このソリューションは結果として、ネットワークの修正に不可欠な可能性のある情報を含む大量のデータの損失も生じさせる。さらに、プローブが複数のデバイスを監視している場合、それらのうちのたった１つがイベント・フラッドを起こした場合であっても、すべてのデバイスからのすべてのデータが失われる。最終的に、プローブがどのようにデータ・フラッドを管理するかのインテリジェントな中央管理は不可能である。

【０００５】

たとえば、米国特許第７５３９７５２号は、固定しきい値を超えるイベント数の検出および許可されるイベント数の抑制を開示している。他の例として、米国特許明細書第２０１０００５２９２４号は、固定しきい値を超えるイベント数の検出およびイベント情報のバッファリングを開示している。これは、イベント・フラッドのインシデント時にはシステムを管理するために情報が使用できなくなることを意味している。

【０００６】

既存の予測分析システムは、しばしば、デバイスが障害状態に発展する前に単純な進行を表示するデバイス・メトリクスに集中する。たとえば、将来の問題を予測するために線形トレンドをディスク・スペースまたは中央処理ユニット（ＣＰＵ）の使用率に適合させるか、あるいは異常な使用率を示すためにこれらのメトリクスの履歴分析を実行する。ここでも、それぞれの場合に、予測データは異常性を特定するために固定しきい値に依拠し、このメトリクスの収集および分析はかなり困難であるため、これらのシステムはデバイス特有の障害イベント・レートに対して柔軟な手法を講じることができない。

【先行技術文献】

【特許文献】

【０００７】

【特許文献１】米国特許第７５３９７５２号

【特許文献２】米国特許明細書第２０１０００５２９２４号
【発明の概要】
【発明が解決しようとする課題】
【０００８】
したがって、現況技術に従ったネットワーク・システムにおける前述の問題に対処する必要がある。
【課題を解決するための手段】
【０００９】
したがって本発明は、第１の態様において、１つまたは複数のデバイスからのイベント放出レートを検出するためのイベント・レート検出器と、複数の当該デバイスからの当該イベント放出レートの集約レートおよび集約レート・トレンドを生成するためのアグリゲータ（aggregator）と、複数の期間にわたる複数の当該集約レート・トレンドの最大許容イベント・レート値を含む複数のレベルを生成するためのレベル生成器と、当該複数のレベルを記憶するための記憶構成要素と、現在の集約レート・トレンドと当該レベルのうちの少なくとも選択されたレベルとを比較するための比較器と、当該現在の集約レート・トレンドが第１の時点で当該レベルのうちの当該少なくとも選択されたレベルを超えることを当該比較器が検出するのに応答して、予測イベント・フラッドを信号送信するための信号器とを備える、ネットワーク・イベント・フラッドを予測するための装置を提供する。
【００１０】
好ましくは、当該アグリゲータは平均イベント・レートを計算するためのアベレージャ（averager）を備える。好ましくは、当該アグリゲータは、統計的に正規化された集約レートまたはレート・トレンドを計算するための統計計算器を備える。好ましくは、当該統計的に正規化された集約レートまたはレート・トレンドは、正規化されたトレンドを定義する。好ましくは、当該正規化されたトレンドは、最小二乗法によって計算される。好ましくは、当該複数の期間は、時刻、曜日、月のうちの日（days of month）、年のうちの日（days or year）のうちの１つまたは複数に従って定義される。
【００１１】
さらに装置は、当該信号器に応答して、当該第１の時点で最大のイベント放出レートを有するデバイスから当該第１の時点で最小のイベント放出レートを有するデバイスへと、降順で当該デバイスの識別子リストを順序付けするための、順序付け構成要素を備えることができる。さらに装置は、当該リストから当該第１の時点で最大のイベント放出レートを有する当該デバイスを選択するため、および、当該デバイスをフラッド保護モードに配置するための候補デバイスとして識別するための、第１のセレクタを備えることができる。好ましくは、当該フラッド保護モードは、当該デバイスからの低減イベント放出レートを受信器に受け入れさせる。好ましくは、当該受信器はネットワーク・モニタを備える。好ましくは、当該ネットワーク・モニタはプローブを備える。さらに装置は、請求項８から１１のいずれか一項に従い、当該候補デバイスをフラッド保護デバイスとして当該フラッド保護モードに配置するためのフラッド保護制御構成要素を備える。さらに装置は、第２の時点で最小のイベント放出レートを有するフラッド保護デバイスを選択するため、および、当該デバイスを当該フラッド保護モードから除去するための候補デバイスとして識別するための、第２のセレクタを備えることができる。
【００１２】
第２の態様では、イベント・レート検出器によって、１つまたは複数のデバイスからのイベント放出レートを検出すること、アグリゲータによって、複数の当該デバイスからの当該イベント放出レートの集約レートおよび集約レート・トレンドを生成すること、レベル生成器によって、複数の期間にわたる複数の当該集約レート・トレンドの最大許容イベント・レート値を含む複数のレベルを生成すること、記憶構成要素によって、当該複数のレベルを記憶すること、比較器によって、現在の集約レート・トレンドと当該レベルのうちの少なくとも選択されたレベルとを比較すること、および、信号器によって、当該現在の集約レート・トレンドが第１の時点で当該レベルのうちの当該少なくとも選択されたレ

ベルを超えることを当該比較器が検出するのに応答して、予測イベント・フラッドを信号送信することを含む、ネットワーク・イベント・フラッドを予測するための方法が提供される。

【００１３】

好ましくは、当該集約するステップは、平均イベント・レートを計算するためのアベレージャを使用することを含む。好ましくは、当該集約するステップは、統計的に正規化された集約レートまたはレート・トレンドを計算するための統計計算器を使用することを含む。好ましくは、当該統計的に正規化された集約レートまたはレート・トレンドは、正規化されたトレンドを定義する。好ましくは、当該正規化されたトレンドは、最小二乗法によって計算される。好ましくは、当該複数の期間は、時刻、曜日、月のうちの日、年のうちの日のうちの、１つまたは複数に従って定義される。さらに方法は、順序付け構成要素によって、当該信号器に応答して、当該第１の時点で最大のイベント放出レートを有するデバイスから当該第１の時点で最小のイベント放出レートを有するデバイスへと、降順で当該デバイスの識別子リストを順序付けするステップを含むことができる。さらに方法は、当該リストから当該第１の時点で最大のイベント放出レートを有する当該デバイスを選択し、当該デバイスをフラッド保護モードに配置するための候補デバイスとして識別するステップを含むことができる。好ましくは、当該フラッド保護モードは、当該デバイスからの低減イベント放出レートを受信器に受け入れさせる。好ましくは、当該受信器はネットワーク・モニタを備える。好ましくは、当該ネットワーク・モニタはプローブを備える。

【００１４】

さらに方法は、当該候補デバイスをフラッド保護デバイスとして当該フラッド保護モードに配置する、フラッド保護制御構成要素によって実行されるステップを含むことができる。さらに方法は、第２の時点で最小のイベント放出レートを有するフラッド保護デバイスを選択すること、および、当該デバイスを当該フラッド保護モードから除去するための候補デバイスとして識別することを、含むことができる。

【００１５】

第３の態様では、コンピュータ・システム内にロードされ、その上で実行された場合、当該コンピュータ・システムに第２の態様に従った方法のすべてのステップを実行させるために、コンピュータ読み取り可能媒体上に格納されたコンピュータ・プログラム・コードを含む、コンピュータ・プログラムが提供される。

【００１６】

次に本発明の好ましい実施形態を、単なる例として図面を参照しながら説明する。

【図面の簡単な説明】

【００１７】

【図１】本発明の好ましい実施形態の実装に好適な、例示の多層ネットワーク・イベント管理システムを示す図である。

【図２】本発明の一実施形態に従ったレベルを作成する方法を示す、簡略流れ図である。

【図３】本発明の一実施形態に従った潜在的なイベント・フラッドの問題に対処する例示の方法を図４との組み合わせで示す、簡略流れ図である。

【図４】本発明の一実施形態に従った潜在的なイベント・フラッドの問題に対処する例示の方法を図３との組み合わせで示す、簡略流れ図である。

【図５】本発明の実施形態に従った、たとえばフィールド・プログラマブル・ゲート・アレイまたは特定用途向けデバイスなどのハードウェア内で、あるいは、デバイスを制御するように配置構成されたファームウェア内で具体化可能なような、装置または論理配置構成を示す、簡略概略図である。

【発明を実施するための形態】

【００１８】

図１は、本発明の好ましい実施形態の実装に好適な、例示の多層ネットワーク・イベント管理システム１００を示す図である。

【００１９】
監視されているデバイスは１０２に示され、この例では、デバイス１０２（デバイス１、デバイス２、．．．デバイスｎ）はプローブ１によって監視されている。
【００２０】
プローブ１は、ロー障害データを監視し、これを正規化された障害イベントに変更し、オブジェクト・サーバ１０６の集合レイヤに送信する、プローブ・セット１０４（プローブ１、プローブ２、．．．プローブｍ）のうちの１つである。
【００２１】
集合レイヤは、デバイス特有のフラッド保護をオンまたはオフに変更可能なレイヤでもある。レイヤ１０６は、集合オブジェクト・サーバ（集合オブジェクト・サーバ１、集合オブジェクト・サーバ２、．．．集合オブジェクト・サーバｋ）のレイヤである。
【００２２】
集約オブジェクト・サーバ１０８は、イベント・フラッドによって最も悪影響を受けることになるネットワーク管理システムのレイヤであるため、ソケットベースの通信システムを介してプローブを制御するものである。
【００２３】
オブジェクト・サーバの表示レイヤは詳細に示されていないが、表示レイヤへのゲートウェイは１１０に存在する。表示レイヤ・オブジェクト・サーバはイベント・リストにデータを送り、オペレータが障害データと対話できるようにする。
【００２４】
単一のオブジェクト・サーバ・システムでは、プローブはオブジェクト・サーバにデータを送り、さらにオブジェクト・サーバによる制御も受ける。
【００２５】
好ましい実施形態では、本発明に従い、デバイス特有の障害イベント・レート・データが中央に集められる。このデータが要約され、デバイス・イベント・レートの履歴データベースを構築するために記憶される。この履歴データは、線形トレンド・アルゴリズムおよび前の用法のベースラインを生成するアルゴリズムの両方を使用して分析される。すべての個別のデバイス・イベント・レートを合計することによって、ネットワーク・イベント・レート全体に対しても同じ分析が実行される。このプロセスにより、１つまたは複数のレベルの確立が可能となり、これは、たとえば時刻、曜日、月のうちの日、またはイベント・トラフィック量の季節変動などのさらに広い期間変動性に従った変動を、考慮に入れることができる。
【００２６】
図２に進むと、本発明の一実施形態に従ったかかるレベルを作成する方法を示す、簡略流れ図が示される。
【００２７】
開始ステップ２００の後、２０２で、デバイス・イベント・レート・データが収集される。このアクティビティは、前述のように時間と共に変化するイベント・レートを代表する適切な大量のイベント・レート・データを抽出するために、長期間にわたって実行可能である。２０４で、デバイス・イベント・レート・データは、たとえばデータベースなどのデータ・ストア内に記憶され、データのそれぞれのサンプルは時間基準に関連付けられている。デバイス・イベント・レート・データの集約のための１つまたは複数の時間基準が、２０６で選択される。具体的な例として、デバイス・イベント・レート集約のために選択される時間基準は、前述のような時刻基準または曜日基準などであってよい。２０８で、システム全体にわたるイベント・レートを与えるために、選択された１つまたは複数の時間基準に関するデバイス・イベント・レート・データが集約され、ここから２１０で、イベント・レート・データの（ベースライン、しきい値、または履歴最高許容レベルなどの）レベルが導出され、１つまたは複数の時間基準に関連付けられる。１つまたは複数の時間基準に関連付けられたイベント・レート・データのレベルは、２１２で記憶され、システムは続行ステップ２１４で他の処理を続行する。

【００２８】
このイベント・レート・データは、イベント・レート・データをトレンドし、特定のデバイスに伴う潜在的な将来の問題を予測するイベント情報を生成するために使用される。これは、前のアクティビティの履歴ベースラインを取り、アクティビティが大幅に変化した場合に障害イベントを表示するために使用される。最終的に、イベント・レート全体がトレンドされ、障害イベント管理システムを上回る前に、イベント・ストーム（event storm）が構築される可能性が高いかどうかが判別される。その後、特定のデバイス・イベント・レート・トレンドが使用され、それらのデバイスから低減イベント・レート・フラッド保護モードへ、イベント・フィードを自動的に押し進める。予測されたイベント・フラッドが回避されると、同じ技法を逆に使用して、デバイス・イベント・フィードを通常の動作に復元することができる。

【００２９】
制御オブジェクト・サーバは、オブジェクト・サーバ内に常駐する特定のデバイスからのすべての障害イベントのタリー（tally）における変化を合計する、自動化プロセスを実行する。デバイスはノード、すなわちネットワーク上のホスト名によって識別される。これが、サンプル期間（たとえば５分毎とすることができる）にわたってデバイス当たりのイベント・レートを与える。デバイスがフラッド保護モードに配置された場合であっても、イベントの低減数はプローブでの着信イベント数を反映するタリー・カウントを増加している。これは、プローブでのフラッド保護状態がどのようであっても、イベント・レート計算がデバイスによって生成される障害イベント数について依然として正確であることを意味する。

【００３０】
デバイス当たりのイベント・レートはタイム・スタンプと共に記憶される。その後、この履歴記録は以下のように分析される。

【００３１】
第１に、最小二乗系統適合（linefit）または他の統計的適合法を使用して、デバイス・イベント・レート・トレンドを近似する。線形トレンドが、今後の所与の時間（たとえば１週間）内に許容（構成可能）しきい値を超えることが示された場合、ネットワーク管理システム内に予測障害イベントが表示されることになるため、結果としてオペレータはこのデバイスに対する修復アクションを優先順位付けすることができる。これにより、特定のデバイスから来る障害イベントの数が増大していることが識別され、これをオペレータに警告する。

【００３２】
第２に、あるデバイスに関する同じ曜日の同じ時刻からのイベント・レートが平均化され、履歴レベルが生成される。初期にこのレベルを構築するためには、週などの最小の２つの延長期間のデータが必要である。当業者であれば明らかなように、平均化される週の数のデータは構成可能である。デバイス障害イベント・レートがこのデバイスの履歴レベルと構成可能な量だけ異なる場合、障害イベントがネットワーク管理システム内に表示されるため、結果としてオペレータはこのデバイスに関する修復アクションを優先順位付けすることができる。このテストは「正規性の回廊（ｃｏｒｒｉｄｏｒ　ｏｆ　ｎｏｒｍａｌｉｔｙ）」とも呼ばれ、週、月の同じ時刻および曜日などで同様の挙動が予測可能であるという原理に基づいている。本明細書では、同じデバイスが各期間内の同じ時刻に障害を起こすかどうかを示す場合、ネットワークを改善するためにレベル自体をツールとして使用することも可能である。これは、オペレータが問題の原因を指摘するのに役立つ。これが有用な可能性のある典型的な例は、週末にわたってデバイスがシャットダウンされ月曜朝の同時刻に立ち上げられ、これが次に通常は安全に無視できるネットワークの障害イベントを発生させる場合である。機械は出現に失敗した場合、破滅的な結果を有する可能性があり、レベルの変動はこれを即時に識別する。

【００３３】
当業者であれば明らかなように、特定の一時的な状況に関連するいくつかのベースライ

ンまたは履歴最大値測度が確立可能であるという点で、現在のトレンドとベースラインまたは履歴最大値との比較は反復的であるか、あるいは、いずれかの特定のケースで、いくつかの追加の発見的問題解決を適切なレベルの選択に適用することが必要な場合がある。たとえば、休暇期間にわたるネットワークのシャットダウン後、１月１日に労働週間が始まるものとする。好ましい実施形態に従ったシステムでは、月曜日に第１のレベル、労働週間の最初の日に第２のレベル、および月の最初の日に第３のレベルが存在することができる。この環境では、本発明の好ましい実施形態の改良が、使用のために適切なレベルまたは履歴最大値を選択するための規則を適用する。この規則は、たとえばしきい値を決定するために最低レベルを選択することであってよい。当業者であれば、多くの代替の配置構成が明らかとなろう。

【００３４】

図３および図４を組み合わせて参照すると、本発明の一実施形態に従った潜在的なイベント・フラッドの問題に対処する例示の方法を示す、簡略流れ図が示される。

【００３５】

方法は開始ステップ３００で開始され、ステップ３０２で、デバイス・イベント・レート・データが集められる。３０４で、好ましくはたとえば最小二乗適合を使用して、システム全体にわたる系統適合が計算される。テスト・ステップ３０６で、合計トレンド・レートが第１の将来システム最大値と比較される。当業者であれば明らかなように、第１の将来システム最大値に関する期間は、特定のネットワーク・システムの必要性に従って構成可能である。好ましい実施形態のレベル要素の前述の説明から明らかなように、ここでの最大値は、選択に適用可能な規則に従った１つまたは複数のレベル値から選択されることになる。比較の結果が否定の場合、プロセスはステップ４１１で続行する。応答が肯定的な場合、ステップ３１０で各デバイスについて系統適合が生成され、ステップ３１２で、この値を使用して、第１の将来システム最大値全体のイベント・レートの予測時間でのデバイス当たりのイベント・レートが予測される。ステップ３１４で、ステップ３１２で各デバイスについて導出された値を使用して、第１の将来システム最大値全体のイベント・レートの予測時間でのデバイス当たりの最大イベント・レートを伴うデバイスから、第１の将来システム最大値全体のイベント・レートの予測時間でのデバイス当たりの最小イベント・レートを伴うデバイスへと、降順でデバイスのリストが生成される。ステップ３１６で、フラッド保護モードにない最高のデバイス（「ターゲット・デバイス」）がリストから識別される。ステップ３１８で、ターゲット・デバイスに関する常駐障害イベントを有するすべてのプローブの位置が特定され、ステップ３２０で、そのデバイスを監視しているこうした各プローブに関するフラッド保護リストにターゲット・デバイスが追加される。ステップ３２２で、保護リストがすべてのプローブに送信され、ステップ３２４で、デバイスに関するフラッド保護が活動化された旨をシステム・ユーザに警告するために、ユーザ・イベントがトリガされる。

【００３６】

図４では、ステップ４００でプロセスが続行する。ステップ４０２で、新しい計算を提供するために、システム全体にわたるトレンド計算からターゲット・デバイス・イベント・データが除去され、ステップ４０４で、システムに関する結果のトレンド・レートが第１の将来システム最大値と比較される。テスト・ステップ４０４での決定が否定である場合、プロセスは開始ステップ３００に戻る。テスト・ステップ４０４の結果が肯定である場合、テスト・ステップ４０８で、すべてのデバイスがすでにフラッド保護モードにあるかどうかが決定される。決定が否定である場合、プロセスはステップ３１５に戻る。決定が肯定である場合、ステップ４１２で、ステップ４０２で導出された結果のトレンド・レートが次の将来システム最大値より大きいかどうかを決定するために、他のテストが実行される。決定が肯定である場合、プロセスは開始ステップ３００に戻る。決定が否定である場合、ステップ４１６でデバイス当たりの系統適合が計算され、ステップ４１８で短期間にわたるデバイス当たりのイベント・レートが予測される。各デバイスに関して導出された値を使用して、デバイス当たりの最大イベント・レートを伴うデバイスからデバイス

当たりの最小イベント・レートを伴うデバイスへと、降順でデバイスのリストが生成され、ステップ４２２で、フラッド保護モードにあるリスト内の最低デバイスの位置が特定され、ターゲット・デバイスとなる。ステップ４２４で、監視しているすべてのプローブに関する保護リストからターゲット・デバイスが除去され、ステップ４２６ですべてのプローブに保護リストが送信される。ステップ４２８で、デバイスに対するフラッド保護がここで非アクティブであることをシステム・ユーザに通知するために、ユーザ・イベントがトリガされ、ステップ４３０でプロセスは開始ステップ３００に戻る。

【００３７】

以下の擬似コード指定は、２４時間でその短期間を、４８時間でその長期間を有する例示システム内で、インテリジェント・フラッド制御アルゴリズムがどのように働くかを、より詳細に、また当業者に良く知られた用語および構造で記述する。

【００３８】

１．構成可能数のイベント・レート・サンプル期間だけ待機する。

２．最新の２４時間（＊）にわたる全イベント・レート・データの合計の最小二乗系統適合を生成する。

３．トレンドが、オブジェクト・サーバが次の２４時間（＊）内に処理可能である、合計イベント・レートが選択されたベースラインに従って調節された最大値を超えること、ことを予測するか。

４．予測しない場合、１７に進む。

５．各デバイスに関するイベント・レート・データの最小二乗適合を生成する。

６．イベント・レート全体が、オブジェクト・サーバが処理可能な、選択されたベースラインに従って調節された最大値を超える時点で、各デバイスに関する予測イベント・レートを計算する。

７．予測イベント・レート上でソートされたデバイスのリストを生成する。第１が最高である。

８．未だフラッド保護モードにない最初のデバイスを見つける。

９．常駐イベントを使用してこのデバイスに関する常駐障害イベントを生成したすべてのプローブを見つける。

１０．デバイスを監視するすべてのプローブに関するフラッド保護リストにデバイス名を追加する。

１１．フラッド保護リストをプローブに送信する。

１２．どのシステムが自動的に実行したかがユーザにわかるように、デバイスがフラッド保護モードに入ったことを示すためのイベントを生成する。

１３．合計イベント・レート最小二乗トレンドからデバイス・イベント・レートを差し引く。

１４．新規トレンドが、オブジェクト・サーバが次の２４時間（＊）内に処理可能である、合計イベント・レートが選択されたベースラインに従って調節された最大値を超えること、ことを予測するか。

１５．予測する場合、さらにすべてのデバイスがフラッド保護モードにない場合、８に進む。

１６．１に進む。

１７．トレンドが、オブジェクト・サーバが次の４８時間（＊）内に処理可能である、合計イベント・レートが選択されたベースラインに従って調節された最大値を超えること、ことを予測するか。

１８．予測する場合、１に進む。

１９．各デバイスに関するイベント・レート・データの最小二乗適合を生成する。

２０．２４時間（＊）内の各デバイスに関する予測イベント・レートを計算する。

２１．予測イベント・レート上でソートされたデバイスのリストを生成する。第１が最高である。

２２．フラッド保護モードにあるリスト内の最後のデバイスを見つける。

２３．デバイスを監視するすべてのプローブに関するフラッド保護リストからデバイス名を除去する。ステップ９でこのデバイスに関して見つかったプローブを使用する。
２４．フラッド保護リストをプローブに送信する。
２５．どのシステムが自動的に実行したかがユーザにわかるように、デバイスがフラッド保護モードから外されたことを示すための解決イベントを生成する。
２６．１に進む。
（＊）時間数は構成可能である。

【００３９】
図５に進むと、本発明の実施形態に従った、たとえばフィールド・プログラマブル・ゲート・アレイまたは特定用途向けデバイスなどのハードウェア内で、あるいは、デバイスを制御するように配置構成されたファームウェア内で具体化可能なような、装置または論理配置構成が示される。

【００４０】
図５の装置は、アグリゲータ５０４にイベント・レート・データを提供するイベント・レート検出器５０２を有する、ネットワーク・フラッド予測器および保護器機構５００を備える。アグリゲータ５０４は、好ましくはアベレージャ５１４および統計計算器５１６を用いてデータを集約し、集約されたデータをレベル生成器５０６に提供する。レベル生成器５０６は、その生成されたレベルをストレージ５０８に記憶する。比較器５１０は、イベント・レート検出器５０２から現在のイベント・レート・データを受信するように、さらに、このデータをストレージ５０８からのレベルのうちの１つまたは複数と比較するように、適合される。予測イベント・フラッドを示す比較器５１０によって生成される比較の結果に基づいて、信号器５１２は、予測イベント・フラッドに対するそれらの相対的な予測貢献を示す基準に従って、リスト順序付け構成要素５１８でデバイスの順序付けリストを生成するためのアクションを開始することにより、機構５００のフラッド保護器部分を備える構成要素に信号を送信するように指示される。リスト順序付け構成要素５１８はその順序付けリストをセレクタ５２０に提供し、セレクタ５２０はフラッド保護モードに配置されるデバイスを選択し、フラッド保護制御構成要素５２２にネットワーク・モニタ５２４に対して適切なコマンドを発行させる。次にネットワーク・モニタ５２４は、プローブ５２６、５２８などでのイベントの受け入れを制御する。

【００４１】
したがって、システム全体に関する線形トレンドが、次の２４時間（これは異なる期間に対して構成可能である）以内にデータのフラッドがネットワーク管理システムを上回るであろうということを示す場合、各デバイスに関するトレンドが分析され、この将来のフラッドに対して最も貢献するデバイスを見つける。次に、このデバイスを監視しているプローブに、このデバイスからのデータ・レートを低減させるための命令が送信され、この変更を示すために障害イベントがネットワーク管理システム内に表示される。

【００４２】
その後、システム全体のトレンド分析は、計算中のデバイスを含まずに反復される。このデバイスをシステム全体から除去することで、所与の時間枠内にシステムを上回ることになる将来のトレンドが生じることになった場合、フラッドに対して次に高い貢献を果たすことが予測されるデバイスがイベント低減モードに入れられることになる。このプロセスは、ネットワーク管理システム全体が、予測されるカスケード障害によってフラッドされることのない状態になるまで反復される。

【００４３】
イベント・レート・データは、フラッド保護モードに入っているか否かに関わらず、すべてのネットワーク・デバイスから集められる。トレンド全体が、システム全体がより長い期間、例えば４８時間フラッドすることが無い旨を示す場合、フラッド保護モードにあるデバイスからの障害イベント・データは通常動作に復元される。デバイス障害イベントは、イベント・レート・トレンドが最低のイベントが最初に通常動作に戻るように復元される。変更を示す解決イベントが管理システムに追加される。デバイスをフラッド保護モ

ードに追加する場合よりも長い予測期間が使用される理由は、トレンド全体への変動がわずかな場合、デバイスが頻繁に保護モードへの出入りを切り換えることのないよう保証するためである。

【００４４】

本発明の好ましい実施形態は、ネットワーク管理システムがどれだけのデータを処理できるかを自動的かつインテリジェントに管理することを保証する。これにより、ネットワーク管理システムは、極度のイベント・フラッド状態下であっても、好反応、有益、かつ有用を維持することが保証される。

【００４５】

当業者であれば、本発明の好ましい実施形態の方法のすべてまたは一部が、方法のステップを実行するように配置構成された論理要素を備える論理装置または複数の論理装置内で好適かつ有用に具体化可能であること、および、かかる論理要素がハードウェア構成要素、ファームウェア構成要素、またはそれらの組み合わせを備えることが可能であることが、明らかとなろう。

【００４６】

当業者であれば、本発明の好ましい実施形態に従った論理配置構成のすべてまたは一部が、方法のステップを実行するための論理要素を備える論理装置内に好適に具体化可能であること、および、かかる論理要素が論理ゲートなどの構成要素を、たとえばプログラマブル論理アレイまたは特定用途向け集積回路内に備えることが可能であることが、明らかとなろう。さらにかかる論理配置構成は、たとえば、固定または伝送可能なキャリア媒体を使用して記憶および伝送可能な仮想ハードウェア記述子言語を使用して、かかるアレイまたは回路内に論理構造を一時的または永続的に確立するための許可要素内で、具体化可能である。

【００４７】

前述の方法および配置構成は、１つまたは複数のプロセッサ（図示せず）上で実行中のソフトウェア内で完全または部分的に好適に実施可能でもあること、および、ソフトウェアは、磁気または光ディスクなどの任意の好適なデータ・キャリア（同様に図示せず）上に担持された１つまたは複数のコンピュータ・プログラム要素の形で提供可能であることを、理解されよう。データの伝送のためのチャネルは、すべての記述の記録媒体、ならびに有線または無線の信号搬送媒体などの信号搬送媒体を、同様に含むことができる。

【００４８】

さらに本発明は、コンピュータ・システムで使用するためのコンピュータ・プログラム製品として好適に具体化可能である。こうした実装は、たとえばディスケット、ＣＤ－ＲＯＭ、ＲＯＭ、またはハード・ディスクなどのコンピュータ読み取り可能媒体などの、有形媒体上に固定されるか、あるいは、光またはアナログ通信回線を含むがこれらに限定されない有形媒体を介して、または、マイクロ波、赤外線、または他の伝送技法を含むがこれらに限定されない無線技法を使用して非有形に、モデムまたは他のインターフェース・デバイスを通じて、コンピュータ・システムに伝送可能である、一連のコンピュータ読み取り可能命令を含むことができる。一連のコンピュータ読み取り可能命令は、本明細書で前述した機能のすべてまたは一部を具体化する。

【００４９】

当業者であれば、こうしたコンピュータ読み取り可能命令が、多くのコンピュータ・アーキテクチャまたはオペレーティング・システムで使用するためのいくつかのプログラミング言語で作成可能であることを理解されよう。さらにこうした命令は、半導体、磁気、または光を含むがこれらに限定されない、現在または将来の任意のメモリ技術を使用して記憶可能であるか、あるいは、光、赤外線、またはマイクロ波を含むがこれらに限定されない、現在または将来の任意の津新技術を使用して伝送可能である。かかるコンピュータ・プログラム製品は、たとえば市販パッケージ・ソフトウェアなどの印刷または電子文書が添付される、コンピュータ・システムのたとえばシステムＲＯＭまたは固定ディスク上に事前ロードされる、あるいは、たとえばインターネットまたはワールド・ワイド・ウェ

ブなどのネットワークを介してサーバまたは電子掲示板から配布される、取り外し可能媒体として配布可能であることが企図される。

【００５０】

一代替では、本発明の好ましい実施形態は、コンピュータ・インフラストラクチャ内に配備され、その上で実行された場合、当該コンピュータ・システムに方法のすべてのステップ実行させるように動作可能なコンピュータ・プログラム・コードを配備するステップを含むサービスを配備する、コンピュータ実装方法の形で実現可能である。

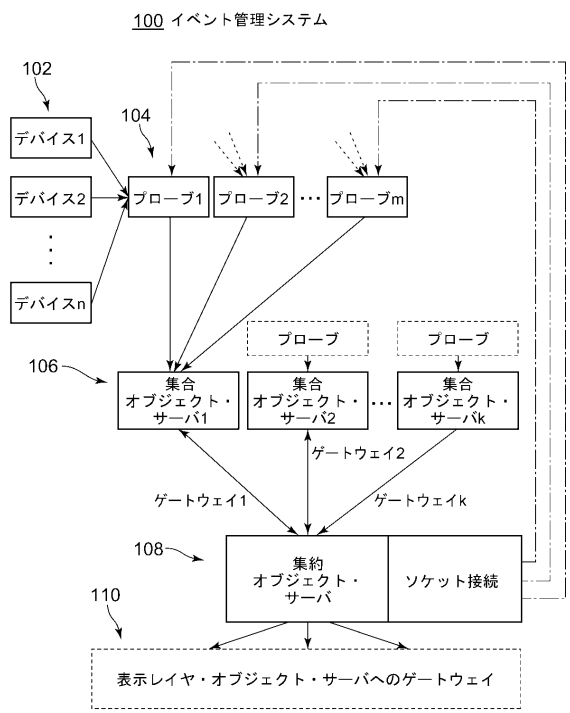
【００５１】

他の代替では、本発明の好ましい実施形態は、その上に機能データを有するデータ・キャリアの形で実現可能であり、当該機能データは、コンピュータ・システム内にロードされ、それによって動作された場合、当該コンピュータ・システムが方法のすべてのステップを実行できるようにするための機能コンピュータ・データ構造を含む。

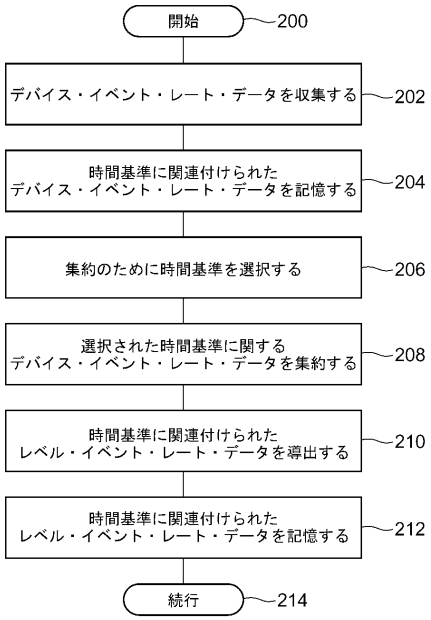
【００５２】

当業者であれば、本発明の範囲を逸脱することなく、前述の例示実施形態に対して多くの改良および修正が実行可能であることが明らかとなろう。

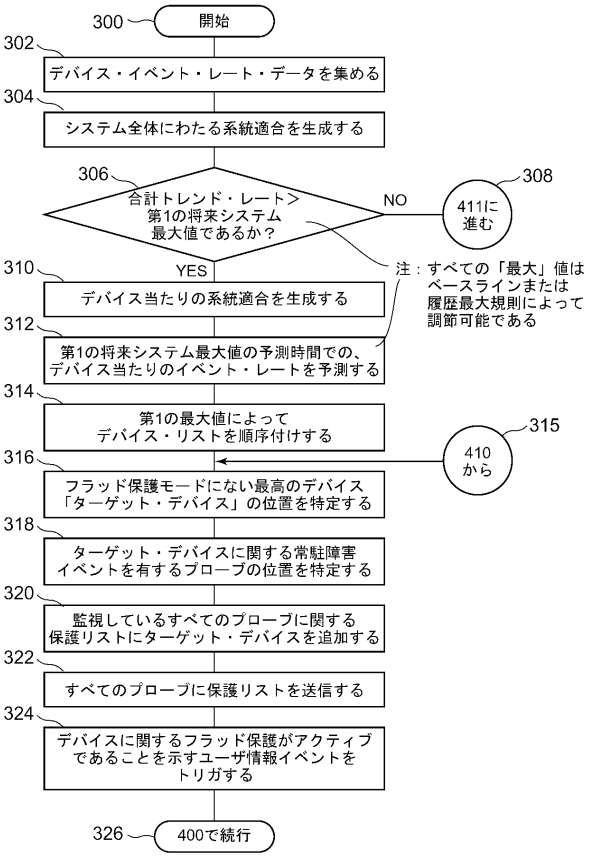
【図１】



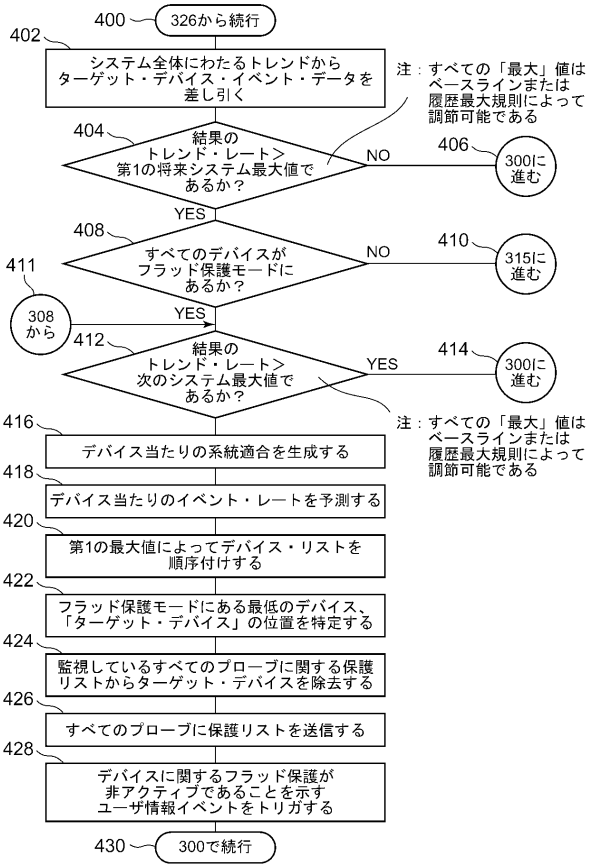
【図２】



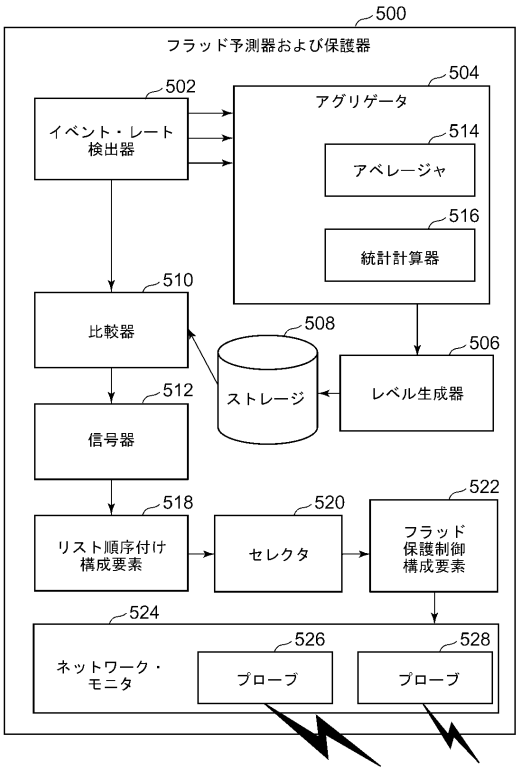
【図３】


300
開始
302
デバイス・イベント・レート・データを集める
304
システム全体にわたる系統適合を生成する
306
合計トレンド・レート＞
第1の将来システム
最大値であるか？
NO
308
411に
進む
YES
注：すべての「最大」値は
ベースラインまたは
履歴最大規則によって
調節可能である
310
デバイス当たりの系統適合を生成する
312
第1の将来システム最大値の予測時間での、
デバイス当たりのイベント・レートを予測する
314
第1の最大値によって
デバイス・リストを順序付けする
315
410
から
316
フラッド保護モードにない最高のデバイス
「ターゲット・デバイス」の位置を特定する
318
ターゲット・デバイスに関する常駐障害
イベントを有するプローブの位置を特定する
320
監視しているすべてのプローブに関する
保護リストにターゲット・デバイスを追加する
322
すべてのプローブに保護リストを送信する
324
デバイスに関するフラッド保護がアクティブ
であることを示すユーザ情報イベントを
トリガする
326
400で続行

【図４】


400
326から続行
402
システム全体にわたるトレンドから
ターゲット・デバイス・イベント・データを
差し引く
注：すべての「最大」値は
ベースラインまたは
履歴最大規則によって
調節可能である
404
結果の
トレンド・レート＞
第1の将来システム最大値で
あるか？
NO
406
300に
進む
YES
408
すべてのデバイスが
フラッド保護モードに
あるか？
NO
410
315に
進む
411
308
から
YES
412
結果の
トレンド・レート＞
次のシステム最大値で
あるか？
YES
414
300に
進む
注：すべての「最大」値は
ベースラインまたは
履歴最大規則によって
調節可能である
416
デバイス当たりの系統適合を生成する
418
デバイス当たりのイベント・レートを予測する
420
第1の最大値によってデバイス・リストを
順序付けする
422
フラッド保護モードにある最低のデバイス、
「ターゲット・デバイス」の位置を特定する
424
監視しているすべてのプローブに関する保護
リストからターゲット・デバイスを除去する
426
すべてのプローブに保護リストを送信する
428
デバイスに関するフラッド保護が
非アクティブであることを示す
ユーザ情報イベントをトリガする
430
300で続行

【図５】


500
フラッド予測器および保護器
502
イベント・レート
検出器
504
アグリゲータ
514
アベレージャ
516
統計計算器
510
比較器
508
ストレージ
506
レベル生成器
512
信号器
518
リスト順序付け
構成要素
520
セレクタ
522
フラッド
保護制御
構成要素
524
ネットワーク・
モニタ
526
プローブ
528
プローブ

フロントページの続き

(74)代理人 100112690
弁理士 太佐 種一
(72)発明者 フランクリン、デヴィッド、リチャード
イギリス国エスイー１ ９ピーゼッド グレイターロンドン ロンドン サウスバンク アッパーグラウンド７６
(72)発明者 スチュワート、クリスティアン、ジョン
イギリス国エスイー１ ９ピーゼッド グレイターロンドン ロンドン サウスバンク アッパーグラウンド７６
(72)発明者 ディンジャー、ジョン
アメリカ合衆国２７７０３－９１３５ ノースカロライナ州ダラム サウス・マイアミ・ブールヴァード３９０１
(72)発明者 レイク、ジョン、マイケル
アメリカ合衆国２７７０９ ノースカロライナ州リサーチトライアングルパーク コーンウォリス・ロード３０３９ ピーオーボックス１２１９５

合議体
審判長 和田 志郎
審判官 稲葉 和生
審判官 山澤 宏

(56)参考文献 特開２００６－２３８０４３（ＪＰ，Ａ）
特開２００５－９４３６１（ＪＰ，Ａ）
特開２００１－８４１９５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F11/28-11/34
G06F13/00
H03J9/00-9/06
H04L12/00-12/28
H04L12/44-12/955