(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6457777号
(P6457777)
(45)発行日　平成31年1月23日(2019.1.23)　(24)登録日　平成30年12月28日(2018.12.28)

(51)Int.Cl.　　F I
G06Q 50/10 (2012.01)　　G06Q 50/10
G16Z 99/00 (2019.01)　　G06F 19/00 ６００

請求項の数 11　外国語出願　(全 18 頁)

(21)出願番号　特願2014-211549(P2014-211549)
(22)出願日　平成26年10月16日(2014.10.16)
(65)公開番号　特開2015-109074(P2015-109074A)
(43)公開日　平成27年6月11日(2015.6.11)
審査請求日　平成29年7月14日(2017.7.14)
(31)優先権主張番号　3382/MUM/2013
(32)優先日　平成25年10月25日(2013.10.25)
(33)優先権主張国　インド(IN)

(73)特許権者　510337621
タタ　コンサルタンシー　サービシズ　リミテッド
ＴＡＴＡ　Ｃｏｎｓｕｌｔａｎｃｙ　Ｓｅｒｖｉｃｅｓ　Ｌｉｍｉｔｅｄ
インド国　マハーラシュトラ、ムンバイ　４０００２１、ナリマン　ポイント、ナーマル　ビルディング　９階
Ｎｉｒｍａｌ　Ｂｕｉｌｄｉｎｇ，９ｔｈ　Ｆｌｏｏｒ，Ｎａｒｉｍａｎ　Ｐｏｉｎｔ，Ｍｕｍｂａｉ　４０００２１，Ｍａｈａｒａｓｈｔｒａ，Ｉｎｄｉａ．
(74)代理人　100079108
弁理士　稲葉　良幸

最終頁に続く

(54)【発明の名称】ルールの自動化された生成および動的な更新

(57)【特許請求の範囲】
【請求項１】
ルールの自動化された生成および更新のためのコンピュータ実装方法であって、
プロセッサ（１１０）によって、事前に定められた期間の間に、少なくとも１つのデータストリームに関連する少なくとも１つのデータトレンドを入手するステップであって、前記少なくとも１つのデータトレンドは、前記事前に定められた期間中に前記少なくとも１つのデータストリームによって辿られるパターンを示すステップと、
前記プロセッサ（１１０）によって、前記少なくとも１つのデータストリームに関連する少なくとも１つのデルタ値を計算するステップであって、前記少なくとも１つのデルタ値は、特定の時間インスタンスにおける前記少なくとも１つのデータトレンドに対する前記少なくとも１つのデータストリームの逸脱を示すステップと、
前記プロセッサ（１１０）によって、前記少なくとも１つのデータトレンドと、それぞれのデータストリームに関連付けられた識別メタデータと、以前に生成されたルールとに基づいて、前記少なくとも１つのデータストリームを含む複数のデータストリームの間における少なくとも１つの関係を特定するステップであって、前記識別メタデータは、それぞれのデータストリームの一意の識別情報を示すステップと、
前記プロセッサ（１１０）によって、前記少なくとも１つのデルタ値および前記少なくとも１つの関係に基づいて少なくとも１つのルールを生成するステップであって、前記少なくとも１つのルールは、前記少なくとも１つのデータストリームの前記逸脱を追跡するためにユーザによって設定された条件を含むステップと、

前記プロセッサ（１１０）によって、前記少なくとも１つのルールが違反された場合に前記ユーザに通知を提供するステップであって、前記通知は、前記ルール違反に関連する詳細、アクション、および前記ルール違反を克服するための提案のうちの少なくとも１つを含むステップと、

前記プロセッサ（１１０）によって、前記少なくとも１つのデータストリーム内で、特定の時間インスタンスにおいて、設定された条件からの前記少なくとも１つのルールの逸脱を追跡することにより、ルール違反のパターンを特定するステップであって、ルール違反トレンドは、時間期間にわたって発生した前記ルール違反のパターンに基づいて生成されるステップと、

前記プロセッサ（１１０）によって、前記通知へのユーザ応答、前記ルール違反トレンド、前記少なくとも１つのデルタ値、および前記少なくとも１つの関係に基づいて前記少なくとも１つのルールを更新するステップと

を含み、

前記少なくとも１つのデータストリームは、タイムスタンプ、データ値、およびデータのタイプを含み、前記少なくとも１つのデータトレンドを用いて、指定された時間期間中における少なくとも１つのデータストリームの最大および最小のデータ値の判定が支援される、コンピュータ実装方法。

【請求項２】

前記入手するステップは、

前記プロセッサ（１１０）によって、検索メタデータに基づいて少なくとも１つのデータソースからデータを検索するステップであって、前記データソースが、インハウスデータベース、外部データベース、およびオンラインポータルのうちの少なくとも１つを含み、前記検索メタデータは、前記少なくとも１つのデータソースからの前記データの検索を支援する詳細を示すステップと、

前記プロセッサ（１１０）によって、前記データを前記少なくとも１つのデータストリームへと変換するステップであって、前記少なくとも１つのデータストリームは、事前に定義されたフォーマットであるステップと、

前記プロセッサ（１１０）によって、前記少なくとも１つのデータストリームに関連する前記少なくとも１つのデータトレンドを特定するステップと、

を含む、請求項１に記載のコンピュータ実装方法。

【請求項３】

前記入手するステップは、前記少なくとも１つのデータストリームへと変換するために前記データからサンプルを選択するステップをさらに含む、請求項２に記載のコンピュータ実装方法。

【請求項４】

前記ユーザが、前記通知内で提供されている「受け入れ」、「拒否」、および「無視」タブのうちの１つを選択することによって前記通知に応答する、請求項１に記載のコンピュータ実装方法。

【請求項５】

前記プロセッサ（１１０）によって、ルールの前記自動化された生成および更新に関連する詳細を提供するためのパフォーマンスレポートを生成するステップをさらに含む、請求項１に記載のコンピュータ実装方法。

【請求項６】

ルールの自動化された生成および動的な更新のためのルール生成システム（１０２）であって、

プロセッサ（１１０）と、

前記プロセッサ（１１０）により実行可能なルール生成モジュール（１２２）であって、

事前に定められた期間の間に少なくとも１つのデータストリームに関連する少なくとも１つのデータトレンドを入手するステップであって、前記少なくとも１つのデータトレ

ンドは、前記事前に定められた期間中に前記少なくとも１つのデータストリームによって辿られるパターンを示すステップ、

前記少なくとも１つのデータストリームに関連する少なくとも１つのデルタ値を計算するステップであって、前記少なくとも１つのデルタ値は、特定の時間インスタンスにおける前記少なくとも１つのデータトレンドに対する前記少なくとも１つのデータストリームの逸脱を示すステップ、

前記少なくとも１つのデータトレンドと、それぞれのデータストリームに関連付けられた識別メタデータと、以前に生成されたルールとに基づいて、複数のデータストリームの間における少なくとも１つの関係を特定するステップであって、前記識別メタデータは、それぞれのデータストリームの一意の識別情報を示すステップ、

前記少なくとも１つのデルタ値および前記少なくとも１つの関係に基づいて少なくとも１つのルールを生成するステップであって、前記少なくとも１つのルールは、前記少なくとも１つのデータストリームの前記逸脱を追跡するためにユーザによって設定された条件を含むステップ、

前記少なくとも１つのルールが違反された場合に前記ユーザに通知を提供するステップであって、前記通知は、前記ルール違反に関連する詳細、アクション、および前記ルール違反を克服するための提案のうちの少なくとも１つを含むステップ、

前記少なくとも１つのデータストリーム内で、特定の時間インスタンスにおいて、設定された条件からの前記少なくとも１つのルールの逸脱を追跡することにより、ルール違反のパターンを特定するステップであって、ルール違反トレンドは、時間期間にわたって発生した前記ルール違反のパターンに基づいて生成されるステップ、並びに、

前記プロセッサ（１１０）によって、前記通知へのユーザ応答、前記ルール違反トレンド、前記少なくとも１つのデルタ値、および前記少なくとも１つの関係に基づいて前記少なくとも１つのルールを更新するステップ

を行うルール生成モジュール（１２２）と、

を備え、

前記少なくとも１つのデータストリームは、タイムスタンプ、データ値、およびデータのタイプを含み、前記少なくとも１つのデータトレンドを用いて、指定された時間期間中における少なくとも１つのデータストリームの最大および最小のデータ値の判定が支援される、ルール生成システム（１０２）。

【請求項７】

検索メタデータに基づいて少なくとも１つのデータソースからデータを検索するステップであって、前記データソースは、インハウスデータベース、外部データベース、およびオンラインポータルのうちの少なくとも１つを含み、前記検索メタデータは、前記少なくとも１つのデータソースからの前記データの検索を支援する詳細を示すステップと、

前記データを前記少なくとも１つのデータストリームへと変換するステップであって、前記少なくとも１つのデータストリームは、事前に定義されたフォーマットであるステップと、

前記少なくとも１つのデータストリームに関連する前記少なくとも１つのデータトレンドを特定するステップと

を行うための、前記プロセッサ（１１０）に結合されているトレンド分析モジュール（１２０）をさらに含む、請求項６に記載のルール生成システム（１０２）。

【請求項８】

前記トレンド分析モジュール（１２０）は、前記少なくとも１つのデータストリームへと変換するために前記データからサンプルを選択する、請求項６に記載のルール生成システム（１０２）。

【請求項９】

前記ユーザが、前記通知内で提供されている「受け入れ」、「拒否」、および「無視」タブのうちの１つを選択することによって前記通知に応答する、請求項６に記載のルール生成システム（１０２）。

【請求項１０】
前記更新モジュール（１２４）は、ルールの前記自動化された生成および更新に関連する詳細を提供するためのパフォーマンスレポートを生成する、請求項６に記載のルール生成システム（１０２）。
【請求項１１】
方法を実行するためのコンピュータプログラムを記録したコンピュータ読取可能媒体であって、前記方法は、
プロセッサ（１１０）によって、事前に定められた期間の間に少なくとも１つのデータストリームに関連する少なくとも１つのデータトレンドを入手するステップであって、前記少なくとも１つのデータトレンドは、前記事前に定められた期間中に前記少なくとも１つのデータストリームによって辿られるパターンを示すステップと、
前記プロセッサ（１１０）によって、前記少なくとも１つのデータストリームに関連する少なくとも１つのデルタ値を計算するステップであって、前記少なくとも１つのデルタ値は、特定の時間インスタンスにおける前記少なくとも１つのデータトレンドに対する前記少なくとも１つのデータストリームの逸脱を示すステップと、
前記プロセッサ（１１０）によって、前記少なくとも１つのデータトレンドと、それぞれのデータストリームに関連付けられた識別メタデータと、以前に生成されたルールとに基づいて、複数のデータストリームの間における少なくとも１つの関係を特定するステップであって、前記識別メタデータは、それぞれのデータストリームの一意の識別情報を示すステップと、
前記プロセッサ（１１０）によって、前記少なくとも１つのデルタ値および前記少なくとも１つの関係に基づいて少なくとも１つのルールを生成するステップであって、前記少なくとも１つのルールは、前記少なくとも１つのデータストリームの前記逸脱を追跡するためにユーザによって設定された条件を含むステップと、
前記プロセッサ（１１０）によって、前記少なくとも１つのルールが違反された場合に前記ユーザに通知を提供するステップであって、前記通知は、前記ルール違反に関連する詳細、アクション、および前記ルール違反を克服するための提案のうちの少なくとも１つを含むステップと、
前記プロセッサ（１１０）によって、前記少なくとも１つのデータストリーム内で、特定の時間インスタンスにおいて、設定された条件からの前記少なくとも１つのルールの逸脱を追跡することにより、ルール違反のパターンを特定するステップであって、ルール違反トレンドは、時間期間にわたって発生した前記ルール違反のパターンに基づいて生成されるステップと、
前記プロセッサ（１１０）によって、前記通知へのユーザ応答、前記ルール違反トレンド、前記少なくとも１つのデルタ値、および前記少なくとも１つの関係に基づいて前記少なくとも１つのルールを更新するステップと
を含み、
前記少なくとも１つのデータストリームは、タイムスタンプ、データ値、およびデータのタイプを含み、前記少なくとも１つのデータトレンドを用いて、指定された時間期間中における少なくとも１つのデータストリームの最大および最小のデータ値の判定が支援される、コンピュータ読取可能媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
[0001] 本発明の主題は、一般にはトレンド分析に関し、詳細には、データトレンド分析に基づくルールの自動化された生成および動的な更新のための方法およびシステムに関する。
【背景技術】
【０００２】
[0002] 最近では、環境に関連した様々な側面のダイナミクスの洞察を得るために、組織

は、自分たちのリソースをトレンド分析の領域に投資している。一般に理解されているように、トレンド分析は、様々なトレンドを特定するために十分な期間にわたってデータを比較することに関連している。あらゆる分野におけるデータの幅広い可用性に起因して、トレンド分析に関する用途は、ほとんど無限であると思われる。例えば、トレンド分析は、市場のトレンド、売上の伸び、在庫水準、および金利など、組織の成長および発展にとって有益な情報を予測するために使用され得る。トレンド分析は、コンピューティングシステムを、その上で稼働しているいくつかのソフトウェアアプリケーションに基づいてモニタするためにも使用され得る。さらに、トレンド分析は、故障解析のために、および差し迫った問題の早期警告インジケータとしても使用され得る。

【発明の概要】

【０００３】

[0003] 添付図面を参照して、詳細な説明を説明する。それらの図においては、参照番号の最も左側の数字は、その参照番号が最初に登場する図を識別する。同様の機能およびコンポーネントを参照するために、それらの図面を通じて同じ番号を使用する。

【図面の簡単な説明】

【０００４】

【図１】[0004]本発明の主題の一実施形態によるルール生成システムを実装するネットワーク環境を示す図である。

【図２】[0005]本発明の主題の一実施形態による、データトレンド分析に基づくルールの自動化された生成および動的な更新のための方法を示す図である。

【発明を実施するための形態】

【０００５】

[0006] データトレンド分析に基づくルールの自動化された生成および更新のためのシステムおよび方法。この（１つまたは複数の）システムおよび（１つまたは複数の）方法は、ラップトップ、デスクトップ、ワークステーション、タブレットＰＣ、ノート、ポータブルコンピュータ、タブレットコンピュータ、インターネット機器、および類似のシステムなど、多様なコンピューティングデバイスにおいて実装されることが可能である。しかしながら、本発明の主題の実施形態は、新たなコンピューティングシステムおよびプラットフォームが利用可能になった場合には、それらの新たなコンピューティングシステムおよびプラットフォームに適用することが可能であるため、いかなる特定のコンピューティングシステム、アーキテクチャー、またはアプリケーションデバイスにも限定されないということを当業者であれば理解することができる。

【０００６】

[0007] この数十年間で、世界中の様々な領域において、例えば、過去のデータに基づいて未来の事象を予測する目的で環境をモニタするために、トレンド分析技法が使用されている。環境とは、モニタリングおよび予測の目的でトレンド分析が実行可能な任意のフィールドまたはプラットフォームとして理解することができる。例えば、ある組織は、自分たちの製品の売上をモニタするために、それゆえ、関連のある将来の障害を予想するために、トレンド分析を利用するかもしれない。これにより、その組織は、損失を回避するために先制措置を取ることができる。

【０００７】

[0008] 徹底的で詳細なトレンド分析を確実に行うためには、その環境に関連する大量のデータを取り扱い処理しなければならない。例えば、コンピューティングシステムのパフォーマンスを評価するために、そのコンピューティングシステム上で稼働している多くのソフトウェアアプリケーションによって使用されているデータが取得され得る。このデータに基づいて、トレンド分析を行うことが可能である。トレンド分析は、別々の時間インスタンスにおいて各ソフトウェアアプリケーションによって使用され得るデータに基づいて、コンピューティングシステムの遅いオペレーションなど、厄介な問題の原因を特定する際に役立つ。したがって、ソフトウェアアプリケーションによって使用されているデータが、過去のデータのトレンドからかなり変化していることを示す場合には、問題を解決

するために適切なアクションがしかるべく取られ、コンピューティングシステムの妨害のないスムーズなオペレーションが確実となる。

【０００８】

[0009] 一般に、過去のデータのトレンドに対するデータの逸脱または変化を検知するために、複数のルールが定義される。ルールとは、過去のデータのトレンドからのデータの任意の変化を検知するためにユーザによって設定された条件として理解することができる。例えば、ユーザは、ソフトウェアアプリケーションによって使用されているデータの量が過去のデータのトレンドから１０％超の変動を示すとすぐにアラームがトリガーされるというルールを定義することができる。同様に、公衆衛生当局による町の健康状況のモニタリングという別の例においては、その町の死亡者数が過去のデータのトレンドから５％超の変動が生じるとすぐにアラームがトリガーされるというルールを定義することができる。したがって、これらのようなルールは、環境に関連する事象の効果的な追跡を維持することを容易にする。

【０００９】

[0010] 当業者なら理解できるであろうが、それぞれの業界は、異なるダイナミクスを有しており、したがって、異なる目的でトレンド分析およびルール生成を使用することがある。しかしながら、そのようなルールは、本質的にジェネリックであり、それらのルールの適用またはモニタされている特定の環境に基づいて修正されることはできない。したがって、ルール生成中に環境の特定のニーズが考慮に入れられず、それは、いくつかの重要な面の見落としにつながり、ひいては、誤った不正確なモニタリングにつながる。

【００１０】

[0011] さらに、ルールは一般に、ユーザまたはユーザのグループによって定義される。ユーザは、対応する分野における専門家、およびソフトウェアアプリケーションが開発されている対象のクライアントなどのステークホルダを含むが、それらには限定されない。したがって、ルールの有効性および正確さは、個人のスキルセットに依存し、したがって、ルール生成におけるエラーの可能性は否定できない。

【００１１】

[0012] また、複雑なルールの生成の場合は、ユーザは、環境の正確なモニタリングを確実にするために、データと、対応するルールとの間における関係を導き出さなければならないことがある。さらに、複雑なシステムの場合は、大量のデータおよび複数のルールを定義しなければならないことがある。その上、ある期間にわたって環境のダイナミクスおよび特性が徐々に変化する可能性がある。結果として、ルールは、定期的にしかるべく更新されなければならない可能性がある。しかしながら、ルールを定義することの手作業的な性質に起因して、ルールの生成および更新の際中にユーザによって相当な量の労力が注がれなければならない。その後、そのようなアクティビティーは、毎回かなりの量の時間を必要とする可能性がある。結果として、トレンド分析に関する全体的なコストも、著しく増大する。

【００１２】

[0013] 間違ったルールをユーザが不注意で定義してしまう可能性があるシナリオについて考える。そのようなシナリオにおいては、間違ったルールに基づいてレポートが生成された場合には、ユーザは、ルール、及び、レポート内で提供されるデータの正確さを特定することができない可能性がある。したがって、間違ったルールを生成する場合は、誤りを捉えることは、ユーザにとって難題となる。さらに、これによって、環境のモニタリングがエラーの影響を受けやすくなる場合がある。またさらに、ルールの無効性が検知された場合は、ユーザは、ルールを手作業で修正することに相当な労力を注がなければならない可能性がある。さもなくば、間違ったルールを完全に無効にしなければならない可能性がある。

【００１３】

[0014] 本発明の主題によれば、例えばデータトレンド分析に基づいて環境をモニタするために使用されるルールを生成および更新するためのルール生成システム（以下、システ

ムと称する）が提供される。一実装形態においては、このシステムは、モニタされている環境に関連する少なくとも１つのデータストリームに対応する少なくとも１つのデータトレンドを入手することができる。他の実装形態においては、データストリームは、時間の順に並べられたデータとして理解することができ、データ値、タイムスタンプ、およびデータのタイプを含むことができるが、それらには限定されない。さらに、少なくとも１つのデータトレンドは、事前に定められた時間期間中に少なくとも１つのデータストリームによって辿られるパターンとして理解することができる。

【００１４】

[0015] 少なくとも１つのデータトレンドを入手すると、少なくとも１つのデータストリームに関連する少なくとも１つのデルタ値が計算することが可能となる。少なくとも１つのデルタ値は、特定の時間インスタンスにおける少なくとも１つのデータトレンドに対する少なくとも１つのデータストリーム内の逸脱を示している。さらに、少なくとも１つのデータトレンドと、それぞれのデータストリームに関連付けられている識別メタデータとに基づいて、複数のデータストリームの間における少なくとも１つの関係を特定することができる。識別メタデータは、それぞれのデータストリームに一意のＩＤを提供する情報として理解することができる。その後、少なくとも１つの関係および少なくとも１つのデルタ値に基づいて、少なくとも１つのルールが、自動化された様式で生成されることが可能である。その少なくとも１つのルールは、少なくとも１つのデータストリームの逸脱を追跡するためにユーザによって設定された条件を示している。一実装形態においては、少なくとも１つのルールが違反されている旨を示す通知がユーザに提供される。その通知は、ルール違反に関連する詳細、およびルール違反を克服するための提案を含むことができるが、それらには限定されない。

【００１５】

[0016] ある期間に渡る少なくとも１つのルールの違反に続いて、ルール違反トレンドを特定することもできる。一実装形態においては、通知へのユーザ応答、ルール違反トレンド、少なくとも１つのデルタ値、および少なくとも１つの関係に基づいて、少なくとも１つのルールを自動的に更新することができる。

【００１６】

[0017] 一実装形態においては、このシステムは、環境に関連するデータを少なくとも１つのデータソースから検索するために検索メタデータを利用することができる。検索メタデータは、そのデータが格納されている、少なくとも１つのデータソース内のロケーションを特定することを容易にする。検索メタデータの例は、データベース名、テーブル名、データベースＩＰ、データベースポート、データベースのタイプ、データベースユーザ名、データベースパスワード、データを検索するための少なくとも１つのクエリー、および検索頻度を含むことができるが、それらには限定されない。さらに、少なくとも１つのデータソースは、外部データベース、インハウスデータベース、およびオンラインポータルを含むことができるが、それらには限定されない。したがって、検索メタデータに基づいて、少なくとも１つのデータソースからデータを検索することが可能である。一実装形態においては、環境のさらなるモニタリングのためのデータを選択するためにサンプリングを実行する。知らているように、サンプリングは、データ全体の特徴を推定する目的での統計データ内からのデータのサブセットの選択を含むことができる。

【００１７】

[0018] 一実装形態においては、少なくとも１つのデータソースから検索されるデータは、異なるフォーマットかもしれない。データのフォーマットにおける不均一性に起因する誤った分析を回避するために、データは、自然言語処理（ＮＬＰ）を経るなどして、システムにとって認識可能なフォーマットへと変換されることが可能である。一実装形態においては、データは、少なくとも１つのデータストリームへ変換することが可能である。さらに、そのような変換中に、それぞれのデータストリームに識別メタデータを割り当てることが可能である。識別メタデータは、それぞれのデータストリームに一意の識別情報を提供する。一実装形態においては、識別メタデータは、環境、アプリケーション、および

サーバに関連する詳細を含むことができるが、それらには限定されない。

【００１８】

[0019] 一実装形態においては、少なくとも１つのデータストリームに関連する少なくとも１つのデータトレンドを特定することが可能である。前述のように、少なくとも１つのデータトレンドは、事前に定められた期間の間に少なくとも１つのデータストリームによって辿られるパターンを示している。さらに、このシステムは、少なくとも１つのデルタ値を計算するために少なくとも１つのデータトレンドを入手することができる。上述のように、少なくとも１つのデルタ値は、特定の時間インスタンスにおける少なくとも１つのデータトレンドに対する少なくとも１つのデータストリーム内の変化の度合いである。一実装形態においては、少なくとも１つのデルタ値は、少なくとも１つのデータストリームのうちのデータ値の割合という形式で計算されることが可能である。

【００１９】

[0020] 少なくとも１つのデルタ値の計算に続いて、このシステムは、複数のデータストリームの間における少なくとも１つの関係を特定することができる。一実装形態においては、この少なくとも１つの関係は、それぞれのデータストリームに関連付けられている識別メタデータに基づいて特定することが可能である。少なくとも１つの関係が特定されると、少なくとも１つのデータトレンドおよび少なくとも１つの関係に基づいて、少なくとも１つのルールを生成することが可能である。その少なくとも１つのルールは、少なくとも１つのデータストリームの逸脱を追跡するためにユーザによって設定された条件として理解することができる。さらに、少なくとも１つのルールの違反に際して、すなわち、条件が満たされた場合に、通知をユーザに提供するようにできる。一実装形態においては、ある期間に渡るルール違反の後、このシステムは、対応するルール違反トレンドを特定することができる。ルール違反トレンドは、その期間に渡ってルール違反が発生したパターンを示している。

【００２０】

[0021] さらに、そのような通知は、ルール違反に関連する詳細、およびルール違反を克服するための提案を含むことができるが、それらには限定されない。このシステムがコンピューティングシステムのデータ使用を評価する例を考慮すると、そのような提案は、少なくとも１つのルールが違反された１つまたは複数のソフトウェアアプリケーションの終了に関連するものにできる。さらにユーザは、その提案を受け入れること、拒否すること、または無視することによって、通知に応答することができる。提案を受け入れることは、少なくとも１つのルールの有効性および正確さを示す。しかしながら、提案の拒否は、少なくとも１つのルールの無効性および不正確さを示しており、したがって、その少なくとも１つのルールは無効とみなすことができる。

【００２１】

[0022] 一実装形態においては、ユーザ応答、少なくとも１つのデータトレンド、少なくとも１つの関係、およびルール違反トレンドに基づいて、少なくとも１つのルールを更新することが可能である。一実装形態においては、ルールの自動化された生成および更新に関連する詳細を提供するためのパフォーマンスレポートを生成する。

【００２２】

[0023] 理解されるように、ルールの自動化された生成および更新に起因して、ルールの有効性および正確さが個人のスキルセットに依存する状況を回避することが可能である。さらに、複雑なルールの生成および更新に必要とされる労力の量が最小化されることが可能である。その後、投資される時間および関連するコストも、大幅に最小化される。またルールは、データトレンドに基づいて生成および更新されるため、環境の特定のダイナミクスを考慮して生成および更新され、正確さおよび信頼性が確実なものとなる。言い換えれば、データのあらゆる変化に基づいてルールを改訂することによって、システムは、その環境における動的で継続的な変化に適合可能となる。また、別々のデータストリームの間における関係を特定することによって、ルールの正確な生成のために、ある環境に関連する様々な要因の間の相互依存が利用される。したがって、本発明の主題は、データトレ

ンド分析を使用して、環境の包括的な、正確な、時間を節約する、コスト効率の高いモニタリングを容易にする。

【００２３】

[0024] 本発明の主題のこれらおよびその他の利点について、添付の図と共にさらに詳しく説明する。データトレンド分析に基づくルールの自動化された生成および更新のための説明される（１つまたは複数の）システムおよび（１つまたは複数の）方法の態様は、任意の数の異なるコンピューティングシステム、環境、および／または構成に実装することが可能であるが、実施形態については、以降の例示的な（１つまたは複数の）システムというコンテキストにおいて説明する。

【００２４】

[0025] 図１は、本発明の主題の一実施形態によるルール生成システム１０２（システム１０２とも称する）を実装するネットワーク環境１００を示している。ネットワーク環境１００においては、システム１０２は、ネットワーク１０４に接続されている。さらに、システム１０２は、データベース１０６に接続されている。加えて、ネットワーク環境１００は、ネットワーク１０４に接続されている１つまたは複数のユーザデバイス１０８－１、１０８－２、．．．１０８－Ｎ（まとめてユーザデバイス１０８と称し、個々にもユーザデバイス１０８と称する）を含む。

【００２５】

[0026] システム１０２は、ネットワーク１０４に接続される複数のコンピューティングデバイスの任意のセットとして構成することが可能である。例えば、システム１０２は、ワークステーション、パーソナルコンピュータ、デスクトップコンピュータ、マルチプロセッサシステム、ラップトップ、ネットワークコンピュータ、ミニコンピュータ、サーバなどとして実装することが可能である。加えて、システム１０２は、ユーザのためにミラー化されたタスクを実行するための複数のサーバを含むことができる。

【００２６】

[0027] さらに、システム１０２は、ネットワーク１０４を通じてユーザデバイス１０８に接続することが可能である。ユーザデバイス１０８の例としては、パーソナルコンピュータ、デスクトップコンピュータ、スマートフォン、ＰＤＡ、およびラップトップが含まれるが、それらには限定されない。ユーザデバイス１０８とシステム１０２との間における通信リンクは、様々な形態の接続を通じて、例えば、ダイヤルアップモデム接続、ケーブルリンク、デジタルサブスクライバーライン（ＤＳＬ）、ワイヤレスもしくは衛星リンク、またはその他の任意の適切な形態の通信を介して実現される。

【００２７】

[0028] さらに、ネットワーク１０４は、ワイヤレスネットワーク、有線ネットワーク、またはそれらの組合せとすることができる。ネットワーク１０４は、個別のネットワーク、または、互いに相互接続されて単一の大きなネットワークとして機能する多くのそのような個別のネットワークの集合、例えば、インターネットまたはイントラネットとすることも可能である。ネットワーク１０４は、イントラネット、ローカルエリアネットワーク（ＬＡＮ）、ワイドエリアネットワーク（ＷＡＮ）、インターネット、およびそれらに類するものなど、様々なタイプのネットワークのうちの１つとして実装されることが可能である。ネットワーク１０４は、専用ネットワークまたは共有ネットワークのいずれかであることが可能であり、共有ネットワークとは、互いに通信するために、多様なプロトコル、例えば、ハイパーテキスト転送プロトコル（ＨＴＴＰ）、トランスミッションコントロールプロトコル／インターネットプロトコル（ＴＣＰ／ＩＰ）などを使用する異なるタイプのネットワークの連合を表す。さらに、ネットワーク１０４は、システム１０２とユーザデバイス１０８との間におけるリンクを提供するために、ネットワークスイッチ、ハブ、ルータ、ホストバスアダプタ（ＨＢＡ）などのネットワークデバイスを含むことができる。ネットワーク１０４内のネットワークデバイスは、通信リンクを通じてシステム１０２およびユーザデバイス１０８と対話することができる。

【００２８】

[0029] 上述の実施形態においては、システム１０２は、１つまたは複数のプロセッサ１１０と、（１つまたは複数の）インターフェース１１２と、プロセッサ１１０に接続されたメモリ１１４とを含む。プロセッサ１１０は、単一の処理ユニットまたは複数のユニットとすることができ、それらのすべては、複数のコンピューティングユニットを含むこともできる。プロセッサ１１０は、１つまたは複数のマイクロプロセッサ、マイクロコンピュータ、マイクロコントローラ、デジタルシグナルプロセッサ、中央処理装置、状態マシン、論理回路、および／または、オペレーション命令に基づいて信号を操作する任意のデバイスとして実装されることが可能である。数ある機能の中でも、プロセッサ１１０は、メモリ１１４内に格納されているコンピュータ読取可能命令およびデータをフェッチして実行するように構成されている。

【００２９】

[0030] インターフェース１１２は、多様なソフトウェアインターフェースおよびハードウェアインターフェース、例えば、キーボード、マウス、外部メモリ、およびプリンタなどの（１つまたは複数の）周辺デバイスのためのインターフェースを含むことができる。さらに、インターフェース１１２は、システム１０２が、ネットワーク環境１００内のその他のコンピューティングデバイス、例えばウェブサーバ、およびデータベース１０６等の外部データリポジトリなどとの通信を可能にすることができる。インターフェース１１２は、有線ネットワーク、例えばＬＡＮ、ケーブルなど、およびワイヤレスネットワーク、例えばＷＬＡＮ、セルラー、衛星などを含む、多種多様なプロトコルおよびネットワーク（ネットワーク１０４など）内の複数の通信を容易にすることができる。インターフェース１１２は、システム１０２を複数のコンピューティングデバイスに接続するための１つまたは複数のポートを含むことができる。

【００３０】

[0031] メモリ１１４は、例えば、スタティックランダムアクセスメモリ（ＳＲＡＭ）およびダイナミックランダムアクセスメモリ（ＤＲＡＭ）などの揮発性メモリ、ならびに／または、読み取り専用メモリ（ＲＯＭ）、消去可能プログラマブルＲＯＭ、フラッシュメモリ、ハードディスク、光学ディスク、および磁気テープなどの不揮発性メモリを含む、当技術分野において知られている任意の非一時的なコンピュータ読取可能媒体を含むことができる。しかしながら、非一時的なコンピュータ読取可能媒体は、一時的な伝搬信号を除外する。

【００３１】

[0032] システム１０２はまた、（１つまたは複数の）モジュール１１６およびデータ１１８を含む。（１つまたは複数の）モジュール１１６は、特定のタスクを実行するかまたは特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含む。一実装形態においては、（１つまたは複数の）モジュール１１６は、トレンド分析モジュール１２０、ルール生成モジュール１２２、更新モジュール１２４、および（１つまたは複数の）その他のモジュール１２６を含む。この他のモジュール１２６は、システム１０２のアプリケーションおよび機能を補強するプログラムまたはコード化された命令を含んでもよい。

【００３２】

[0033] その一方で、データ１１８は、とりわけ、（１つまたは複数の）モジュール１１６のうちの１つまたは複数によって処理、受信、および生成されたデータを格納するためのリポジトリとして機能する。データ１１８は、例えば、トレンド分析データ１２８、ルール生成データ１３０、およびその他のデータ１３２を含む。その他のデータ１３２は、モジュール１１６内の１つまたは複数のモジュールの実行の結果として生成されたデータを含む。

【００３３】

[0034] 一実装形態においては、システム１０２は、データトレンド分析に基づくルールの自動化された生成および動的な更新を容易にすることができる。一実装形態においては、トレンド分析モジュール１２０は、少なくとも１つのデータソースからデータを検索す

るために検索メタデータを利用することができる。検索メタデータは、データベース名、テーブル名、データベースＩＰ、データベースポート、データベースのタイプ、データベースユーザ名、データベースパスワード、データを検索するための少なくとも１つのクエリー、および検索頻度を含むことができるが、それらには限定されない。さらに、少なくとも１つのデータソースは、外部データベース、インハウスデータベース、およびオンラインポータルを含むことができるが、それらには限定されない。したがって、トレンド分析モジュール１２０は、検索メタデータに基づいてデータを検索することができる。さらなる実装形態においては、トレンド分析モジュール１２０は、環境のモニタリングのためにデータのサンプルを利用することができる。

【００３４】

[0035] 一実装形態においては、技術的な問題に起因して、ある期間に渡ってデータを検索することができない可能性が存在する。そのような状況においては、トレンド分析モジュール１２０は、見つからないデータを、そのようなデータの以前のトレンドに基づいて推定することができる。例えば、トレンド分析モジュール１２０は、データが検索されなかった期間に関連する詳細を埋めるために、技術的な問題が生じる前に受信されたデータと、技術的な問題が生じた後に受信されたデータとの平均を取ることができる。また、検索されたデータが欠陥を有しているかまたは誤っているケースにおいては、同様の技法を用いて、かかるデータを推定することが可能である。したがって、データの検索におけるいかなる不整合も、全体的な分析を妨げることはないと言える。

【００３５】

[0036] 当業者が理解するように、少なくとも１つのデータソースから検索されるデータは、異なるフォーマットである場合がある。したがって、トレンド分析モジュール１２０は、データを、システム１０２にとって認識可能なフォーマットへと変換する。一実装形態においては、トレンド分析モジュール１２０は、データを少なくとも１つのデータストリームへと変換することができる。データストリームは、時間の順に並べられたデータとして理解することができ、タイムスタンプ、データ値、およびデータのタイプを含むことができるが、それらには限定されない。タイムスタンプは、少なくとも１つのソースからのデータの検索の時刻を示すことができる。さらに、データ値は、データの数値を示すことができる。同様に、データのタイプは、データの性質を指定するために保持されることが可能である。例えば、アプリケーションモニタリングの場合は、データは、インフラストラクチャーデータ、アプリケーションデータ、および可用性データとすることができる。

【００３６】

[0037] 一実装形態においては、トレンド分析モジュール１２０は、それぞれのデータストリームに一意の識別情報を提供するために識別メタデータをそれぞれのデータストリームに割り当てることができる。識別メタデータは、環境名、アプリケーション、サーバ、およびその他の構成アイテムに関連する詳細をさらに含むことができるが、それらには限定されない。そのような詳細は、データストリームをその他のデータストリームから区別するために利用することができる。一実装形態においては、少なくとも１つのデータストリームへのデータの変換に続いて、トレンド分析モジュール１２０は、少なくとも１つのデータストリームに関連する少なくとも１つのデータトレンドを特定することができる。少なくとも１つのデータトレンドは、事前に定められた時間期間の間に少なくとも１つのデータストリームによって辿られるパターンを示している。少なくとも１つのデータトレンドは、特定の時間インスタンスにおける少なくとも１つのデータストリームのデータ値の平均を決定する際に用いられる。一例においては、少なくとも１つのデータトレンドは、指定された時間期間中における少なくとも１つのデータストリームの最大および最小のデータ値を判定する際に支援を行うことができる。少なくとも１つのデータトレンドのさらに良好な明確さおよび理解を提供するために、ソフトウェアアプリケーションによる中央処理装置（ＣＰＵ）利用割合のデータトレンドを示すテーブル１を、次のように示す。

【００３７】

【表１】

表１

時刻	日										トレンド
	1	2	3	4	5	6	7	8	9	10	
10:00	4	2	2	4	2	3	5	3	4	1	=sum(d1:d10)/10
10:03	6	3	2	2	2	4	4	2	4	2	=sum(d1:d10)/10
10:06	2	4	2	1	2	5	3	1	3	1	=sum(d1:d10)/10
10:09	1	2	1	3	1	6	2	1	2	1	=sum(d1:d10)/10

【００３８】

[0038] テーブル１において示されているように、１０日間の持続時間にわたる異なる時間インスタンスにおけるソフトウェアアプリケーションによるＣＰＵ利用度が分析される。さらに、テーブル１において示されている少なくとも１つのデータトレンドに基づいてＣＰＵ利用度の平均を計算することも可能である。このテーブルにおいては少なくとも１つのデータトレンドを特定するために平均値が利用されているが、しかしながら、その他の実装形態においては、平均または平均値以外のパラメータの点から少なくとも１つのデータトレンドを特定することが可能である。例えば、平均値からの分散または標準偏差の点から少なくとも１つのデータトレンドを特定することが可能である。また、トレンド分析モジュール１２０は、少なくとも１つのデータソースから新たなデータが検索された場合には、その少なくとも１つのデータトレンドを更新することができる。一実装形態においては、トレンド分析モジュール１２０に関連する詳細がトレンド分析データ１２８内に格納される。

【００３９】

[0039] 一実装形態においては、ルール生成モジュール１２２は、少なくとも１つのデータストリームに関連する少なくとも１つのデルタ値の計算のために、少なくとも１つのデータトレンドを入手することができる。少なくとも１つのデルタ値は、特定の時間インスタンスにおける少なくとも１つのデータトレンドに対する少なくとも１つのデータストリームの逸脱として理解される。一実装形態においては、ルール生成モジュール１２２は、少なくとも１つのデルタ値を、少なくとも１つのデータストリームのうちのデータ値の割合という形式で計算することができる。例えば、データストリームのデータ値が３０であり、データ値の逸脱を示すデータ値が６である場合には、対応するデルタ値は、２０％として計算することができる。

【００４０】

[0040] 一実装形態においては、少なくとも１つのデルタ値の計算に際して、ルール生成モジュール１２２は、複数のデータストリームの間における少なくとも１つの関係を特定する。例えば、データストリームＡは、異なる複数の時間インスタンスにおいてソフトウェアアプリケーションによって使用されるデータを示す。同様に、データストリームＢは、異なる時間インスタンスにおけるソフトウェアアプリケーションによるＣＰＵ利用割合に関連するものである。一実装形態においては、特定の時間インスタンスにおけるソフトウェアアプリケーションによるＣＰＵ利用割合は、その特定の時間インスタンスにおいてソフトウェアアプリケーションによって使用されるデータに比例して変動する。したがって、データストリームＡのいかなる変化も、データストリームＢにおける対応する変化につながる。ルール生成モジュール１２２は、少なくとも１つのデータトレンドと、それぞれのデータストリームに対応する識別メタデータとに基づいて、少なくとも１つの関係を特定することができる。各データストリームに関連する識別メタデータは、対応する識別

の詳細を示しているため、ルール生成モジュール１２２は、複数のデータストリームの間における少なくとも１つの関係を確立するために識別メタデータを比較することができる。一実装形態においては、ルール生成モジュール１２２は、少なくともデータトレンドと、以前に生成されたルールとの間における少なくとも１つの関係を特定することができる。そのような特定は、異なるデータトレンド上でのルールの違反の影響を決定する際に支援を行うことができる。

【００４１】

[0041] 一実装形態においては、少なくとも１つのデルタ値および少なくとも１つの関係の計算に続いて、ルール生成モジュール１２２は、少なくとも１つのルールを生成する。その少なくとも１つのルールは、少なくとも１つのデータストリーム内の逸脱を追跡するためにユーザによって設定された条件を示している。ユーザは、対応する分野における専門家、およびステークホルダを含むことができるが、それらには限定されない。さらに、ルール生成モジュール１２２は、特定の時間インスタンスにおけるしきい値違反をモニタするために少なくとも１つのルールを生成することができる。例えば、ルール生成モジュール１２２は、データストリームのデルタ値が１０％超の逸脱を示すべきではないというルールを生成する。そのような一例においては、データストリームのデルタ値が１０％超の変動を示すとすぐに、ルールが違反されていると判定される。一実装形態においては、ルールは、そのルールによって設定された条件が満足されたまたは満たされた場合に、違反されていると判定するように構成できる。

【００４２】

[0042] 一実装形態においては、ルール生成モジュール１２２は、事前に定められた持続時間におけるしきい値違反をモニタするために少なくとも１つのルールを生成する。例えば、ルール生成モジュール１２２は、データストリームのデルタ値が午後２時～午後４時の間に１０％超逸脱するというルールを生成する。したがって、デルタ値が午後２時と午後４時との間に１０％超の変動を示した場合には、ルールが違反されているとみなされる。別の実装形態においては、ルール生成モジュール１２２は、しきい値違反の連続した事象をモニタするために少なくとも１つのルールを生成する。例えば、ルール生成モジュール１２２は、データストリームのデルタ値が５つの連続したデータ値の間に１０％超逸脱するというルールを生成する。したがって、デルタ値が５つの連続したデータ値の間に１０％超の変動を示した場合には、ルールが違反されているとみなされる。さらに別の実装形態においては、ルール生成モジュール１２２は、上述の条件の任意の組合せを伴うルールを生成することができる。

【００４３】

[0043] 一実装形態においては、ルール生成モジュール１２２は、複数のデータストリームの間における少なくとも１つの関係を利用する複雑なルールを生成することもできる。例えば、ルール生成モジュール１２２は、データストリーム１のデルタ値Ａが１０％逸脱し、データストリーム２のデルタ値Ｂが５％逸脱するというルールを生成することができる。したがって、これらの条件が両方とも満たされた場合に、ルールが違反されているとみなされる。

【００４４】

[0044] 少なくとも１つのルールの違反に際して、ルール生成モジュール１２２は、少なくとも１つのルールの違反を示すための通知をユーザに提供することができる。一実装形態においては、その通知は、ルール違反に関連する詳細、アクション、およびルール違反を克服するための提案を含むことができるが、それらには限定されない。アクションは、通知を受け入れること、拒否すること、または無視することによってユーザが通知に応答することを可能にする「受け入れ」、「拒否」、および「無視」タブを含むことができるが、それらには限定されない。さらに、ユーザが提案を受け入れた場合には、それは、少なくとも１つのルールが正確で有効であるということを示すことができる。同様に、ユーザが提案を拒否した場合には、それは、少なくとも１つのルールが不正確で無効であるということを示すことができる。一実装形態においては、ルール生成モジュール１２２に関

連する詳細は、ルール生成データ１３０内に格納される。

【００４５】

[0045] さらに、更新モジュール１２４は、所定の時間期間にわたる少なくとも１つのルールの違反に関連するルール違反トレンドを特定することができる。ルール違反トレンドは、少なくとも１つのルールが違反されるパターンとして理解することが可能である。ユーザ応答、少なくとも１つのデータトレンド、少なくとも１つの関係、およびルール違反トレンドに基づいて、更新モジュール１２４は、少なくとも１つのルールを更新する。したがって、少なくとも１つのルールは、ルール違反トレンド、少なくとも１つの関係、少なくとも１つのデータトレンド、およびユーザ応答における変化に基づいて更新され続けることが可能である。一実装形態においては、更新モジュール１２４は、ルールの自動化された生成および更新に関連する詳細をユーザに提供するためのパフォーマンスレポートを生成する。パフォーマンスレポートは、少なくとも１つのデータトレンド、少なくとも１つのデルタ値、少なくとも１つの関係、少なくとも１つのルール、少なくとも１つのルール違反トレンド、および、少なくとも１つのルールの改訂に関連する詳細を含むことができるが、それらには限定されない。一実装形態においては、更新モジュール１２４に関連する詳細は、ルール生成データ１３０内に格納される。

【００４６】

[0046] 図２は、本発明の主題の一実施形態による、データトレンド分析に基づくルールの自動化された生成および動的な更新のための方法２００を示している。方法２００は、いくつかの異なるやり方で多様なコンピューティングシステムにおいて実現することが可能である。例えば、ここで説明する方法２００は、上述のようなルール生成システム１０２を使用して実装されることが可能である。

【００４７】

[0047] 方法２００は、完全にまたは部分的に、コンピュータ実行可能命令という一般的なコンテキストにおいて説明されることが可能である。一般に、コンピュータ実行可能命令は、特定の機能を実行するかまたは特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造、プロシージャー、モジュール、機能などを含むことができる。この方法のステップは、プログラムされたコンピュータによって実行可能ということを当業者なら容易に認識するであろう。本明細書においては、いくつかの実施形態はまた、プログラムストレージデバイス、例えば、デジタルデータストレージメディアをカバーすることを意図されており、それらは、マシンまたはコンピュータによって読み取り可能であり、命令のマシンによって実行可能なまたはコンピュータによって実行可能なプログラムをエンコードし、前記命令は、説明されている方法２００のステップのうちのいくつかまたはすべてを実行する。

【００４８】

[0048] 方法２００が説明されている順序は、限定として解釈されることを意図されておらず、この方法または代替方法を実装するために任意の数の説明されている方法ブロックが任意の順序で組み合わされることが可能である。加えて、本明細書において説明されている主題の趣旨および範囲から逸脱することなく、個々のブロックがこの方法から削除されることが可能である。さらに、これらの方法は、任意の適切なハードウェア、ソフトウェア、ファームウェア、またはそれらの組合せにおいて実装されることが可能である。方法２００は、システム１０２を参照して説明されているが、その説明は、その他のシステムにも拡張されることが可能であるということが理解されるであろう。

【００４９】

[0049] 方法２００は、データトレンド分析に基づくルールの自動化された生成および動的な更新を容易にすることができる。一実装形態においては、検索メタデータに基づいて少なくとも１つのデータソースからデータが検索される。少なくとも１つのデータソースは、外部データベース、インハウスデータベース、およびオンラインポータルを含むことができるが、それらには限定されない。さらに、検索メタデータは、データベース名、テーブル名、データベースＩＰ、データベースポート、データベースのタイプ、データベー

スユーザ名、データベースパスワード、データを検索するための少なくとも１つのクエリー、および検索頻度を含むことができるが、それらには限定されない。一実装形態においては、環境のモニタリングのためにデータのサンプルが利用される。

【００５０】

[0050] 一実装形態においては、技術的な問題に起因して、ある期間に渡ってデータを検索することができない可能性が存在する。そのような一実装形態においては、見つからないデータを、かかるデータの以前のトレンドに基づいて推定することが可能である。例えば、データが検索されなかった期間に関連する詳細を埋めるために、技術的な問題の前に受信されたデータと、技術的な問題の後に受信されたデータとの平均が計算されて考慮されることが可能である。したがって、データの検索におけるいかなる不整合も、全体的な分析を妨げることはない。

【００５１】

[0051] 別の実装形態においては、少なくとも１つのデータソースから検索されるデータは、システム１０２が認識可能なフォーマットへと変換される。一実装形態においては、データは、生のフォーマットで取得され、次いで少なくとも１つのデータストリームへと変換される。データストリームは、時間の順に並べられたデータとして理解することが可能である。それぞれのデータストリームは、タイムスタンプ、データ値、およびデータのタイプを含むことができるが、それらには限定されない。

【００５２】

[0052] 一実装形態においては、上記のような変換中に、それぞれのデータストリームに一意の識別情報を提供するために識別メタデータがそれぞれのデータストリームに割り当てられる。識別メタデータは、環境名、アプリケーション、サーバ、およびその他の構成アイテムに関連する詳細をさらに含むことができるが、それらには限定されない。少なくとも１つのデータストリームへのデータの変換に続いて、少なくとも１つのデータストリームに関連する少なくとも１つのデータトレンドが特定される。少なくとも１つのデータトレンドは、事前に定められた期間の間に少なくとも１つのデータストリームによって辿られるパターンを示している。少なくとも１つのデータソースから新たなデータが検索された場合には、少なくとも１つのデータトレンドを更新することが可能である。

【００５３】

[0053] ブロック２０２において、少なくとも１つのデータストリームに関連する少なくとも１つのデルタ値の計算のために、少なくとも１つのデータトレンドを入手する。少なくとも１つのデルタ値は、特定の時間インスタンスにおける少なくとも１つのデータトレンドに対する少なくとも１つのデータストリームの逸脱を示している。一実装形態においては、少なくとも１つのデルタ値は、少なくとも１つのデータストリームのうちのデータ値の割合という形式で計算される。一実装形態においては、システム１０２のルール生成モジュール１２２は、少なくとも１つのデータトレンドを入手することができる。

【００５４】

[0054] ブロック２０４において、少なくとも１つのデルタ値の計算に際して、複数のデータストリームの間における少なくとも１つの関係を特定する。少なくとも１つのデータトレンドと、それぞれのデータストリームに対応する識別メタデータとに基づいて、少なくとも１つの関係を特定することが可能である。一実装形態においては、複数のデータストリームの間における少なくとも１つの関係を確立するために、それぞれのデータストリームに関連する識別メタデータが比較される。一実装形態においては、別々のデータトレンド上でのルールの違反の影響を判定する際に支援を行うための、少なくとも１つのデータトレンドと、以前に生成されたルールとの間における少なくとも１つの関係を特定する。

【００５５】

[0055] 一実装形態においては、システム１０２のルール生成モジュール１２２は、少なくとも１つのデータトレンドおよび識別メタデータに基づいて複数のデータストリームの間における少なくとも１つの関係を特定することができる。

【００５６】
[0056] ブロック２０６において、少なくとも１つのデルタ値の計算、および少なくとも１つの関係の特定に基づいて、少なくとも１つのルールが生成される。その少なくとも１つのルールは、少なくとも１つのデータストリーム内の逸脱を追跡するためにユーザによって設定された条件として理解することが可能である。一実装形態においては、ユーザは、対応する分野における専門家、およびステークホルダを含むことができるが、それらには限定されない。一例においては、特定の時間インスタンスにおけるしきい値違反をモニタするために少なくとも１つのルールが生成される。例えば、データストリームのデルタ値が１５％超の逸脱を示すというルールが生成される。したがって、データストリームのデルタ値が１５％超の変動を示すとすぐに、ルールが違反されているとみなされる。なぜなら、条件が満たされたからである。同様に、事前に定められた持続時間におけるしきい値違反をモニタするために少なくとも１つのルールを生成することが可能である。さらに、しきい値違反の連続した発生をモニタするために少なくとも１つのルールが生成される。一実装形態においては、少なくとも１つのルールは、上述の条件の任意の組合せを伴って生成されることが可能である。別の実装形態においては、複数のデータストリームの間における少なくとも１つの関係を利用する複雑なルールが生成される。

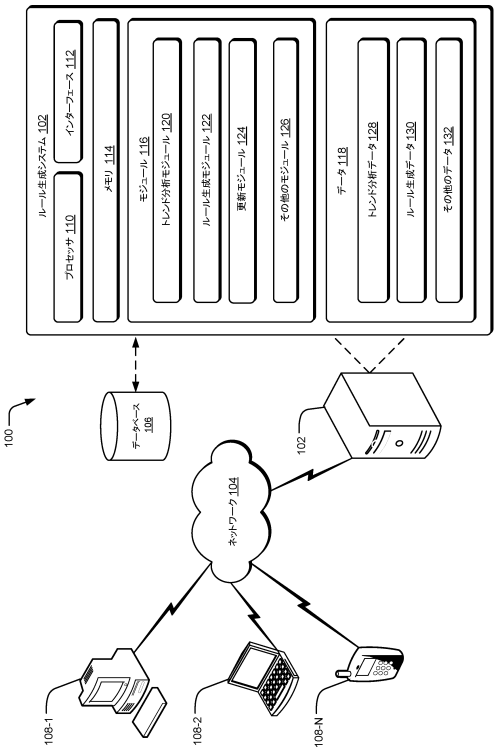
【００５７】
[0057] 少なくとも１つのルールの違反に際して、少なくとも１つのルールの違反を示すための通知がユーザに提供される。一実装形態においては、その通知は、ルール違反に関連する詳細、アクション、およびルール違反を克服するための提案を含むことができるが、それらには限定されない。アクションは、通知を受け入れること、拒否すること、または無視することによってユーザが通知に応答することを可能にする「受け入れ」、「拒否」、および「無視」タブを含むことができるが、それらには限定されない。さらに、ユーザ応答に基づいて少なくとも１つのルールの有効性および正確さが確立される。一実装形態においては、システム１０２のルール生成モジュール１２２は、少なくとも１つのデルタ値および少なくとも１つの関係に基づいて少なくとも１つのルールを生成することができる。

【００５８】
[0058] ブロック２０８において、所定の時間期間にわたる少なくとも１つのルールの違反に関連するルール違反トレンドが特定される。ルール違反トレンドは、少なくとも１つのルールが違反されるパターンとして理解される。一実装形態においては、システム１０２の更新モジュール１２４は、ルール違反トレンドを特定することができる。

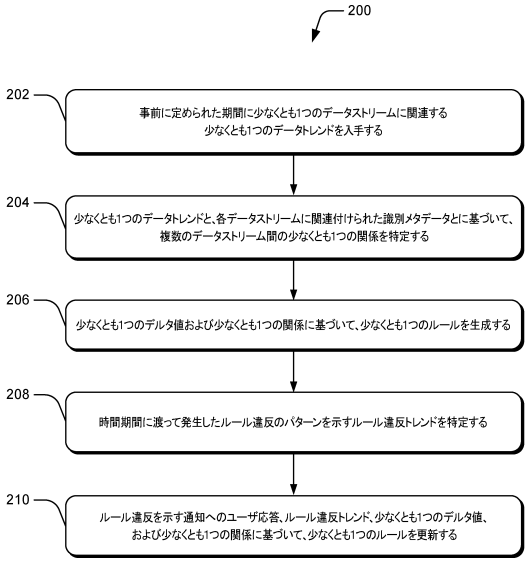
【００５９】
[0059] ブロック２１０において、ユーザ応答、少なくとも１つのデータトレンド、少なくとも１つの関係、およびルール違反トレンドに基づいて、少なくとも１つのルールが更新される。さらに、少なくとも１つのルールは、ルール違反トレンド、少なくとも１つの関係、少なくとも１つのデータトレンド、およびユーザ応答における変化に基づいて更新を続けることが可能である。一実装形態においては、ルールの自動化された生成および更新に関連する詳細をユーザに提供するためのパフォーマンスレポートが生成される。パフォーマンスレポートは、少なくとも１つのデータトレンド、少なくとも１つのデルタ値、少なくとも１つの関係、少なくとも１つのルール、少なくとも１つのルール違反トレンド、および、少なくとも１つのルールの改訂に関連する詳細を含むことができるが、それらには限定されない。

【００６０】
[0060] データトレンド分析に基づくルールの自動化された生成および更新のための方法の実装形態が、構造的な特徴および／または方法に特有の言葉で説明されているが、本発明の主題は、それらの説明されている特定の特徴または方法に必ずしも限定されるものではないことが理解される。

【図１】


ルール生成システム 102
プロセッサ 110
インターフェース 112
メモリ 114
モジュール 116
トレンド分析モジュール 120
ルール生成モジュール 122
更新モジュール 124
その他のモジュール 126
データ 118
トレンド分析データ 128
ルール生成データ 130
その他のデータ 132
100
データベース 106
ネットワーク 104
102
108-1
108-2
108-N

【図２】


200
202
事前に定められた期間に少なくとも1つのデータストリームに関連する
少なくとも1つのデータトレンドを入手する
204
少なくとも1つのデータトレンドと、各データストリームに関連付けられた識別メタデータとに基づいて、
複数のデータストリーム間の少なくとも1つの関係を特定する
206
少なくとも1つのデルタ値および少なくとも1つの関係に基づいて、少なくとも1つのルールを生成する
208
時間期間に渡って発生したルール違反のパターンを示すルール違反トレンドを特定する
210
ルール違反を示す通知へのユーザ応答、ルール違反トレンド、少なくとも1つのデルタ値、
および少なくとも1つの関係に基づいて、少なくとも1つのルールを更新する

フロントページの続き

(74)代理人 100109346
弁理士 大貫 敏史
(74)代理人 100117189
弁理士 江口 昭彦
(74)代理人 100134120
弁理士 内藤 和彦
(72)発明者 ティワリ, タンマヤ
インド国, コルカター７０００９１, ソルト レイク エレクトロニクス コンプレックス セクター ５, ブロック イーピー アンド ジーピー, プロット ビー－１, タタ コンサルタンシー サービシズ
(72)発明者 デイ, スラス クマール
インド国, コルカター７０００９１, ソルト レイク エレクトロニクス コンプレックス セクター ５, ブロック イーピー アンド ジーピー, プロット ビー－１, タタ コンサルタンシー サービシズ
(72)発明者 チャタジー, スワルプ
インド国, コルカター７０００９１, ソルト レイク エレクトロニクス コンプレックス セクター ５, ブロック イーピー アンド ジーピー, プロット ビー－１, タタ コンサルタンシー サービシズ

審査官 山内 裕史

(56)参考文献 特開２００３－２６３５８１（ＪＰ, Ａ）
特表２００９－５００７６７（ＪＰ, Ａ）
米国特許出願公開第２０１３／００８６２０３（ＵＳ, Ａ１）
国際公開第２０１２／１５３４０４（WO, Ａ１）
特開２００５－２８５０４０（ＪＰ, Ａ）

(58)調査した分野(Int.Cl., ＤＢ名)
Ｇ０６Ｑ １０／００ － ９９／００
Ｇ０６Ｆ １９／００