(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4473153号
(P4473153)

(45)発行日　平成22年6月2日(2010.6.2)　(24)登録日　平成22年3月12日(2010.3.12)

(51)Int.Cl.		F I		
G06F 13/10	(2006.01)	G06F	13/10	340A
G06F 13/14	(2006.01)	G06F	13/14	330B
H04L 12/26	(2006.01)	H04L	12/26	

請求項の数 31　(全 21 頁)

(21)出願番号　特願2005-35725(P2005-35725)
(22)出願日　平成17年2月14日(2005.2.14)
(65)公開番号　特開2005-276177(P2005-276177A)
(43)公開日　平成17年10月6日(2005.10.6)
審査請求日　平成17年2月14日(2005.2.14)
(31)優先権主張番号　10/783,435
(32)優先日　平成16年2月20日(2004.2.20)
(33)優先権主張国　米国(US)

(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　ＭＡＳＣＨＩＮＥＳ　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
(74)代理人　100108501
弁理士　上野　剛史
(74)代理人　100112690
弁理士　太佐　種一
(74)代理人　100091568
弁理士　市位　嘉宏

最終頁に続く

(54)【発明の名称】ネットワーク構成のチェックおよび修理のための方法、システムおよびプログラム

(57)【特許請求の範囲】
【請求項１】
ネットワークの構成チェックを実施するためのプログラムを含み、ハードウエア論理及びコンピュータ読取り可能媒体の組合せの一つとして実装される製品であって、前記プログラムが、
少なくとも１つのトランザクションを求めて、ネットワーク内に接続された構成に関するデータを格納するネットワーク・データ・ストア(170)を走査するステップであって、前記トランザクションは、ネットワーク内に接続される構成を含んでいて、構成の追加、更新、変更をする、前記走査するステップと、
前記トランザクションについて、イベントをトランザクションにマッピングすることで、少なくとも１つのイベントを生成するステップと、
前記イベントについて、前記トランザクションの構成に関連する構成データを取得するステップと、
前記イベントについて少なくとも１つのトリガを生成するステップであって、前記トリガは少なくとも１つの構成ポリシーに関連する、前記生成するステップと、
前記トリガに関連する前記構成ポリシーを、前記トリガが生成された前記イベントに関連する構成データと比較するステップと、
前記比較に基づいて、前記構成ポリシーが違反されたかどうか判定するステップとを含み、これらのステップをコンピュータに実施させる製品。
【請求項２】

前記構成ポリシーがローカル・ポリシー・データ・ストア(172)から取り出される、請求項１に記載の製品。

【請求項３】

前記ローカル・ポリシー・データ・ストア内の前記構成ポリシーが、リモート・ポリシー・データ・ストア(174)内の構成ポリシーで自動的に構成される、請求項２に記載の製品。

【請求項４】

さらに、

システム管理者が生成しようとする新しいネットワーク構成を表わす仮説ネットワーク・シナリオを受信するステップと、

前記仮説ネットワーク・シナリオに基づいて、少なくとも１つのトランザクションを生成するステップと、

前記ネットワーク・データ・ストアに、前記トランザクションについての構成データを取り込むステップと、

前記比較に基づいて、前記ポリシーが違反されたかどうか判定した後で、前記トランザクションをロール・バックするステップとを含む、請求項１に記載の製品。

【請求項５】

さらに、

既存のネットワーク構成に対して構成チェックを実施する要求を受信するステップを含む、請求項１に記載の製品。

【請求項６】

さらに、

前記構成ポリシーが違反された場合、その構成ポリシー内に指定されたアクションを実施するステップを含む、請求項１に記載の製品。

【請求項７】

前記アクションが、前記構成ポリシーが生成されたという表示をログすること、少なくとも１つのポリシー違反イベントを生成すること、通知を送信すること、および前記ネットワークをグラフィカルに描写するネットワーク・トポロジ・ビューアを強調表示することのうちの少なくとも１つである、請求項６に記載の製品。

【請求項８】

さらに、

前記構成ポリシーが違反された場合、

知識データ・ストア内の解決策にアクセスするステップと、

前記構成ポリシーが違反されないように、前記解決策を適用するステップとを含む、請求項１に記載の製品。

【請求項９】

さらに、

前記構成ポリシーが違反された場合、

前記ネットワーク内の構成要素が解決策を提供できることを決定するステップと、

前記構成ポリシーが違反されないように、前記構成要素に前記解決策を適用させるステップとを含む、請求項１に記載の製品。

【請求項１０】

前記ポリシーが違反されたかどうか判定する前記ステップがさらに、前記ネットワーク内の構成要素間の非互換性、パフォーマンスの問題および可用性の問題のうちの少なくとも１つを識別するステップを含み、前記非互換性は、構成要素間の競合であって、前記パフォーマンスは、所望のパフォーマンス・レベルが満たされているかどうかに関し、前記可用性は、前記ネットワーク内のどこかに、単一障害箇所があるかどうかに関するものである、請求項１に記載の製品。

【請求項１１】

ネットワークの事前対応型構成チェックを実施するためのプログラムを含み、ハードウ

エア論理及びコンピュータ読取り可能媒体の組合せの一つとして実装される製品であって、前記プログラムが、
システム管理者が生成しようとする新しいネットワーク構成を表わす仮説ネットワーク・シナリオを受信するステップと、
前記仮説ネットワーク・シナリオに基づいて、少なくとも１つのトランザクションを生成するステップであって、前記トランザクションは、仮想ネットワーク・シナリオ内に接続される構成を含んでいて、構成の追加、更新、変更をする、前記生成するステップと、
ネットワーク・データ・ストアに、前記トランザクションについての構成データであって、前記トランザクションによって記述された仮想ネットワーク・シナリオの構成についての構成データを含む前記構成データを取り込むステップと、
イベントのトランザクションへのマッピングを使用して、前記トランザクションについて、少なくとも１つのイベントを生成するステップと、
前記イベントに関連する構成データを使用して、構成ポリシーが違反されたかどうか判定するステップとを含み、これらのステップをコンピュータに実施させる製品。
【請求項１２】
さらに、
前記トランザクションについての前記構成データを、前記ネットワーク・データ・ストアから削除することによって、前記トランザクションをロール・バックするステップを含む、請求項１１に記載の製品。
【請求項１３】
ネットワークの事後対応型構成チェックを実施するためのプログラムを含み、ハードウエア論理及びコンピュータ読取り可能媒体の組合せの一つとして実装される製品であって、前記プログラムが、
既存のネットワーク構成に対して構成チェックを実施する要求を受信するステップと、
少なくとも１つのトランザクションを求めて、ネットワーク内に接続された構成に関するデータを格納するネットワーク・データ・ストア(170)を走査するステップと、
イベントのトランザクションへのマッピングを使用して、前記トランザクションについて、少なくとも１つのイベントを生成するステップと、
前記イベントに関連する構成データを使用して、前記ネットワーク内の構成要素間の非互換性、パフォーマンスの問題および可用性の問題のうちの少なくとも１つのトランザクション結果を判定することによって構成ポリシーが違反されたかどうか判定するステップであって、前記非互換性は、構成要素間の競合であって、前記パフォーマンスは、所望のパフォーマンス・レベルが満たされているかどうかに関し、前記可用性は、前記ネットワーク内のどこかに、単一障害箇所があるかどうかに関するものである、構成ポリシーが違反されたかどうか判定するステップとを含み、これらのステップをコンピュータに実施させる製品。
【請求項１４】
さらに、
前記構成ポリシーが違反された場合、前記違反を自動的に訂正するステップをさらに含む、請求項１３に記載の製品。
【請求項１５】
ネットワークの構成チェックを実施するためのシステムであって、
プロセッサと、
前記プロセッサにとってアクセス可能なコンピュータ読取り可能媒体と、
前記プロセッサに、
少なくとも１つのトランザクションを求めて、ネットワーク・データ・ストアを走査するステップであって、前記トランザクションは、ネットワーク内に接続される構成を含んでいて、構成の追加、更新、変更をする、前記走査するステップと、
前記トランザクションについて、イベントをトランザクションにマッピングすることで、少なくとも１つのイベントを生成するステップと、

前記イベントについて、前記トランザクションの構成に関連する構成データを取得するステップと、
前記イベントについて少なくとも１つのトリガを生成するステップであって、前記トリガは少なくとも１つの構成ポリシーに関連する、前記生成するステップと、
前記トリガに関連する前記構成ポリシーを、前記トリガが生成された前記イベントに関連する構成データと比較するステップと、
前記比較に基づいて、前記構成ポリシーが違反されたかどうか判定するステップとを実施させるコードを含むプログラムとを含むシステム。
【請求項１６】
前記構成ポリシーがローカル・ポリシー・データ・ストア(172)から取り出される、請求項１５に記載のシステム。
【請求項１７】
前記ローカル・ポリシー・データ・ストア内の前記構成ポリシーが、リモート・データ・ストア(174)内の構成ポリシーで自動的に更新される、請求項１６に記載のシステム。
【請求項１８】
前記コードが、前記プロセッサに、
システム管理者が生成しようとする新しいネットワーク構成を表わす仮説ネットワーク・シナリオを受信するステップと、
前記仮説ネットワーク・シナリオに基づいて、少なくとも１つのトランザクションを生成するステップと、
前記ネットワーク・データ・ストアに、前記トランザクションについての構成データを取り込むステップと、
前記比較に基づいて、構成ポリシーが違反されたかどうか判定した後で、前記トランザクションをロール・バックするステップとをさらに実施させる、請求項１５に記載のシステム。
【請求項１９】
前記コードが、前記プロセッサに、
既存のネットワーク構成に対して構成チェックを実施する要求を受信するステップをさらに実施させる、請求項１５に記載のシステム。
【請求項２０】
前記コードが、前記プロセッサに、
前記構成ポリシーが違反された場合、前記構成ポリシー内に指定されたアクションを実施するステップをさらに実施させる、請求項１５に記載のシステム。
【請求項２１】
前記アクションが、前記構成ポリシーが生成されたという表示をログすること、少なくとも１つのポリシー違反イベントを生成すること、通知を送信すること、および前記ネットワークをグラフィカルに描写するネットワーク・トポロジ・ビューアを強調表示することのうちの少なくとも１つである、請求項２０に記載のシステム。
【請求項２２】
前記コードが、前記プロセッサに、
前記構成ポリシーが違反された場合、
知識データ・ストア内の解決策にアクセスするステップと、
前記構成ポリシーが違反されないように、前記解決策を適用するステップとをさらに実施させる、請求項１５に記載のシステム。
【請求項２３】
前記コードが、前記プロセッサに、
前記構成ポリシーが違反された場合、
前記ネットワーク内の構成要素が解決策を提供できることを決定するステップと、
前記構成ポリシーが違反されないように、前記構成要素に前記解決策を適用させるステップとをさらに実施させる、請求項１５に記載のシステム。

【請求項２４】
前記ポリシーが違反されたかどうか判定するための前記コードが、前記プロセッサに、前記ネットワーク内の構成要素間の非互換性、パフォーマンスの問題および可用性の問題のうちの少なくとも１つを識別するステップをさらに実施させることができ、、前記非互換性は、構成要素間の競合であって、前記パフォーマンスは、所望のパフォーマンス・レベルが満たされているかどうかに関し、前記可用性は、前記ネットワーク内のどこかに、単一障害箇所があるかどうかに関するものである、請求項１５に記載のシステム。
【請求項２５】
ネットワークの事前対応型構成チェックを実施するためのシステムであって、
プロセッサと、
前記プロセッサにとってアクセス可能なコンピュータ読取り可能媒体と、
前記プロセッサに、
システム管理者が生成しようとする新しいネットワーク構成を表わす仮説ネットワーク・シナリオを受信するステップと、
前記仮説ネットワーク・シナリオに基づいて、少なくとも１つのトランザクションを生成するステップであって、前記トランザクションは、仮想ネットワーク・シナリオ内に接続される構成を含んでいて、構成の追加、更新、変更をする、前記生成するステップと、
ネットワーク・データ・ストアに、前記トランザクションについての構成データであって、前記トランザクションによって記述された仮想ネットワーク・シナリオの構成についての構成データを含む前記構成データを取り込むステップと、
イベントのトランザクションへのマッピングを使用して、前記トランザクションについて、少なくとも１つのイベントを生成するステップと、
前記イベントに関連する構成データを使用して、構成ポリシーが違反されたかどうか判定するステップとを実施させることができるコードを含むプログラムとを含むシステム。
【請求項２６】
前記コードが、前記プロセッサに、
前記トランザクションについての前記構成データを、前記ネットワーク・データ・ストアから削除することによって、前記トランザクションをロール・バックするステップをさらに実施させることができる、請求項２５に記載のシステム。
【請求項２７】
ネットワークの事後対応型構成チェックを実施するためのシステムであって、
プロセッサと、
前記プロセッサにとってアクセス可能なコンピュータ読取り可能媒体と、
前記プロセッサに、
既存のネットワーク構成に対して構成チェックを実施する要求を受信するステップと、
少なくとも１つのトランザクションを求めて、ネットワーク・データ・ストアを走査するステップであって、前記トランザクションは、ネットワーク内に接続される構成を含んでいて、構成の追加、更新、変更をする、前記走査するステップと、
イベントのトランザクションへのマッピングを使用して、前記トランザクションについて、少なくとも１つのイベントを生成するステップと、
前記イベントに関連する構成データを使用して、前記ネットワーク内の構成要素間の非互換性、パフォーマンスの問題および可用性の問題のうちの少なくとも１つのトランザックション結果を判定することによって構成ポリシーが違反されたかどうか判定するステップであって、前記非互換性は、構成要素間の競合であって、前記パフォーマンスは、所望のパフォーマンス・レベルが満たされているかどうかに関し、前記可用性は、前記ネットワーク内のどこかに、単一障害箇所があるかどうかに関するものである、構成ポリシーが違反されたかどうか判定するステップとを実施させることができるコードを含むプログラムとを含むシステム。
【請求項２８】
前記コードが、前記プロセッサに、

前記構成ポリシーが違反された場合、前記違反を自動的に訂正するステップをさらに実施させることができる、請求項２７に記載のシステム。

【請求項２９】

ネットワークの構成チェックを実施するための方法であって、

少なくとも１つのトランザクションを求めて、ネットワーク・データ・ストアを走査するステップであって、前記トランザクションは、ネットワーク内に接続される構成を含んでいて、構成の追加、更新、変更をする、前記走査するステップと、

前記トランザクションについて、イベントをトランザクションにマッピングすることで、少なくとも１つのイベントを生成するステップと、

前記イベントについて、前記トランザクションの構成に関連する構成データを取得するステップと、

前記イベントについて少なくとも１つのトリガを生成するステップであって、前記トリガは少なくとも１つの構成ポリシーに関連する、前記生成するステップと、

前記トリガに関連する前記構成ポリシーを、前記トリガが生成された前記イベントに関連する構成データと比較するステップと、

前記比較に基づいて、前記構成ポリシーが違反されたかどうか判定するステップとを含む方法。

【請求項３０】

ネットワークの事前対応型構成チェックを実施するための方法であって、

システム管理者が生成しようとする新しいネットワーク構成を表わす仮説ネットワーク・シナリオを受信するステップと、

前記仮説ネットワーク・シナリオに基づいて、少なくとも１つのトランザクションを生成するステップであって、前記トランザクションは、仮想ネットワーク・シナリオ内に接続される構成を含んでいて、構成の追加、更新、変更をする、前記生成するステップと、

ネットワーク・データ・ストアに、前記トランザクションについての構成データであって、前記トランザクションによって記述された仮想ネットワーク・シナリオの構成についての構成データを含む前記構成データを取り込むステップと、

イベントのトランザクションへのマッピングを使用して、前記トランザクションについて、少なくとも１つのイベントを生成するステップと、

前記イベントに関連する構成データを使用して、構成ポリシーが違反されたかどうか判定するステップとを含む方法。

【請求項３１】

ネットワークの事後対応型構成チェックを実施するための方法であって、

既存のネットワーク構成に対して構成チェックを実施する要求を受信するステップと、

少なくとも１つのトランザクションを求めて、ネットワーク・データ・ストアを走査するステップであって、前記トランザクションは、ネットワーク内に接続される構成を含んでいて、構成の追加、更新、変更をする、前記走査するステップと、

イベントのトランザクションへのマッピングを使用して、前記トランザクションについて、少なくとも１つのイベントを生成するステップと、

前記イベントに関連する構成データを使用して、前記ネットワーク内の構成要素間の非互換性、パフォーマンスの問題および可用性の問題のうちの少なくとも１つのトランザックション結果を判定することによって構成ポリシーが違反されたかどうか判定するステップであって、前記非互換性は、構成要素間の競合であって、前記パフォーマンスは、所望のパフォーマンス・レベルが満たされているかどうかに関し、前記可用性は、前記ネットワーク内のどこかに、単一障害箇所があるかどうかに関するものである、構成ポリシーが違反されたかどうか判定するステップとを含む方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、ネットワーク構成のチェックおよび修理に関する。

【背景技術】
【０００２】
ストレージ・エリア・ネットワーク（ＳＡＮ：storage area network）は、共有されるデータ記憶装置を、クライアント・コンピュータによってアクセスすることができる関連サーバ・コンピュータに相互接続する、高速ネットワークまたはサブネットワークであると説明することができる。ＳＡＮは、直接接続ストレージ・モデルと比較して、いくつかの理由で、ブロック・ストレージ・システムのための好ましいストレージ・アーキテクチャ・モデルになりつつある。たとえば、ＳＡＮによって、複数のサーバが記憶装置のブロックを直接的に共有することができ、またストレージを、サーバとは別個に管理することができる。さらに、ＳＡＮを管理するシステム管理者は、追加のデータ記憶装置を独立して追加することができるので、記憶容量を増加させるために追加のサーバを購入する必要がない。
【０００３】
ＳＡＮなどの複雑なネットワーク環境では、ネットワーク内の構成要素間で、非互換の多くのソースが存在する。たとえば、ホスト・バス・アダプタ（ＨＢＡ：Host Bus Adapter）ファームウェア・レベルは、ＨＢＡが接続されたスイッチ内のファームウェアと競合し得る。ＨＢＡは、ホスト・バスとファイバ・チャネル・ループの間に存在し、またホスト・バスとファイバ・チャネル・ループの間の情報転送を管理するＩ／Ｏアダプタであると説明することができる。スイッチは、ネットワークのセグメント間に存在するものであると説明することができ、またスイッチは、データ・パケットを受信し、データ・パケットの宛先を決定し、その宛先にデータ・パケットを転送する。ファイバ・チャネル・ループは、シリアル・データ転送アーキテクチャと説明することができる。別の例では、装置ドライバが、記憶装置の機能を十分に利用するように適切に構成されないことがある。装置ドライバは、装置を制御するプログラムと説明することができる。ＳＡＮ上のすべての可能な問題を決定することは、手作業によるものであり、たいていエラーが発生しやすい作業である。さらに、問題を緩和するために正しい変更を加えることもまた、エラーを引き起こしやすく、結果的に問題が悪化することになり得る。
【０００４】
システム管理者が認識する必要がある、それぞれ異なるベンダからの装置間の相互運用上の制約が多数あるので、ＳＡＮを構成することは、時間がかかり、難しい作業でもある。一般に、ベンダは、ＳＡＮ装置がベンダの戦略的パートナーの装置およびサービスと相互動作するように、ＳＡＮ装置を作成し、またこれは、他のベンダよりも競争上優位に立つために行われる。また相互運用上の制約は、絶えず変化しており、したがって、システム管理者が変化に遅れずについていくことは難しい。
【０００５】
したがって、ＳＡＮの利点を活用するために、システム管理者は、ＳＡＮを容易に管理することができるべきである。したがって、ＳＡＮ管理ソフトウェアは通常、あらゆるＳＡＮインストレーションと一緒に展開される。ＳＡＮ管理ソフトウェア・ツールの一特徴は、システム管理者がＳＡＮを構成するのを手助けできることである。こうした１つのＳＡＮ管理ソフトウェア・ツールは、（インターナショナル・ビジネス・マシーンズ・コーポレーション社（International Business Machines Corporation）からの）ＩＢＭ（Ｒ）Ｔｉｖｏｌｉ（Ｒ）ストレージ・エリア・ネットワーク・マネージャであり、これは、トポロジの発見、ならびにＳＡＮ全体にわたる構成要素およびディスク・リソースの表示を提供し、また監視および問題の識別を提供して、ＳＡＮの保守を容易にするのに役立つ。
【０００６】
したがって、システム管理者は、新しい記憶装置がＳＡＮ内の既存の記憶装置と確実に互換となるように、ＳＡＮ用に購入される新しい記憶装置を選択するのに助けを必要とする。また新しい記憶装置がＳＡＮ内で構成される場合、ＳＡＮ管理者は、特定のＳＡＮインストレーションに特有のＳＡＮ構成上の制約が違反されないように、新しい記憶装置を

選択するのに助けを必要とする。たとえば、ＳＡＮのインストレーションは、パフォーマンス、信頼性あるいはセキュリティ問題のいずれかまたはこれらのうちの２つ以上の組合せを満たすために、どの装置がグループ化されるべきかに関する何らかの具体的な規則を伴い得る。

【非特許文献１】「ＨＴＴＰを介したＣＩＭオペレーションの仕様（Specificationfor CIM Operations over HTTP）」、１．１版、２００２年５月２日

【発明の開示】

【発明が解決しようとする課題】

【０００７】

既存のネットワーク管理ツールは有用であるが、当技術分野では、ＳＡＮネットワークなどのネットワークのチェックおよび修理の向上が求められている。

【課題を解決するための手段】

【０００８】

ネットワークの構成チェックを実施するための方法、システムおよびプログラムが提供される。少なくとも１つのトランザクションを求めて、ネットワーク・データ・ストアが走査される。前記トランザクションについて、少なくとも１つのイベントが生成される。少なくとも１つの構成ポリシーが、前記イベントに関連付けられる。前記構成ポリシーが、前記イベントに関連する構成データと比較される。その比較に基づいて、前記構成ポリシーが違反されたかどうか判定される。

【０００９】

事前対応型の（proactive）ネットワーク構成チェックを実施するための方法、システムおよびプログラムも提供される。仮説のネットワーク・シナリオが受信される。仮説のネットワーク・シナリオに基づいて、少なくとも１つのトランザクションが生成される。ネットワーク・データ・ストアに、前記トランザクションについての構成データが取り込まれる。イベントのトランザクションへのマッピングを使用して、前記トランザクションについて、少なくとも１つのイベントが生成される。前記イベントに関連する構成データを使用して、構成ポリシーが違反されたかどうか判定される。

【００１０】

さらに、事後対応型の（reactive）ネットワーク構成チェックを実施するための方法、システムおよびプログラムが提供される。既存のネットワーク構成に対して構成チェックを実施する要求が受信される。少なくとも１つのトランザクションを求めて、ネットワーク・データ・ストアが走査される。イベントのトランザクションへのマッピングを使用して、前記トランザクションについて、少なくとも１つのイベントが生成される。前記イベントに関連する構成データを使用して、構成ポリシーが違反されたかどうか判定される。

【００１１】

さらに、構成上の問題を訂正するための方法、システムおよびプログラムが提供される。構成上の問題が検出される。知識データ・ストア内に、その構成上の問題についての少なくとも１つの解決策が存在するかどうか判定される。知識データ・ストア内に、少なくとも１つの解決策が存在することが決定された場合は、その構成上の問題を解決するための解決策を自動的に選択する。前記解決策を自動的に適用することができる場合は、前記解決策を自動的に適用する。前記解決策を自動的に適用することができない場合は、ユーザに通知する。

【００１２】

次に、図面を参照する。図面では、同じ参照番号は、全体を通して、対応する部分を表す。

【発明を実施するための最良の形態】

【００１３】

以下の説明では、その一部を形成し、また本発明の複数の実装を図示する添付の図面を参照する。本発明の範囲から逸脱せずに、他の実装を使用することができ、また構成面およびオペレーション面の変更が行われ得ることが理解されよう。

【００１４】
本発明の実装では、自律型（autonomic：オートノミック）構成システムが提供され、この自律型構成システムによって、システム管理者は、ネットワーク内（ＳＡＮなど）への新しい構成要素（ソフトウェアやハードウェア構成要素など）の潜在的な追加のために生じる、ネットワークまたはストレージあるいはその両方に関連する潜在的な構成上の問題を識別することができる。また自律型構成システムは、（たとえば新しいウイルス用のパッチがどのように配布され得るかに類似の）相互運用サイト、あるいはたとえばシステム管理分野の専門家によって維持されるデータ・ストレージから、最新の構成要件（構成ポリシーなど）を自動的にダウンロードする。構成ポリシーは、自律型構成システムによってアクセス可能なポリシー・データ・ストア内に格納される。特定の実装では、構成ポリシーは、ＣＩＭ－ＳＮＩＡ／ＳＭＩＳ仮想ストレージ・モデルに基づく。

【００１５】
自律型構成システムは、自動的にまたは明示的な呼出しによって、仮説のまたは既存の構成が指定された構成ポリシーのいずれかに違反しているかどうか判定する。自律型構成システムは、警告イベントまたは通知メッセージあるいはその両方を生成して、システム管理者に構成エラーについて通知することができる。自律型構成システムは、ネットワーク・トポロジ・ビューアを用いて、ネットワークまたはストレージあるいはその両方に関連する構成上の問題を強調表示することもできる。

【００１６】
本発明の実装によって、ネットワーク環境内の非互換性を検出するための自律型構成システムが提供され、非互換性についての正しい解決策が得られる場合、自律型構成システムは、その解決策を自動的に適用する。

【００１７】
本発明の実装によって、手動で（たとえばユーザによって）、またはツール（プランナー・ツールなど）によって呼び出される時間的な関係（１２時間毎や５分毎など）を使用して、構成チェックを起動することができる。さらに、本発明の実装によって、ポイント・イン・タイム・ネットワーク（ＳＡＮなど）のデータ、またはＳＡＮの少なくとも１つの旧バージョンを示す履歴データあるいはその両方の構成チェックが実施される。

【００１８】
図１に、本発明の特定の実装によるコンピューティング環境のブロック図を示す。管理サーバ・コンピュータ１２０は、他の構成要素（ソフトウェアやハードウェア装置など）が接続されたネットワーク１９０に接続される。ネットワーク１９０は、たとえばストレージ・エリア・ネットワーク（ＳＡＮ）、ローカル・エリア・ネットワーク（ＬＡＮ：Local Area Network）、広域エリア・ネットワーク（ＷＡＮ：Wide Area Network）、インターネット、イントラネットなど、任意のタイプのネットワークを含み得る。本明細書の例は、ＳＡＮを参照し得るが、その例は、本発明の様々な実装についての理解を高めるためのものにすぎず、また本発明の実装をＳＡＮに限定するためのものではない。

【００１９】
管理サーバ・コンピュータ１２０は、揮発性あるいは不揮発性のいずれか一方またはその両方の装置で実装することができるシステム・メモリ１２２を含む。自律型構成システム１５０は、システム・メモリ１２２内で実行される。さらに、少なくとも１つのサーバ・アプリケーション１６０が、システム・メモリ１２２内で実行される。

【００２０】
管理サーバ・コンピュータ１２０は、ネットワーク・データ・ストア１７０、ローカル・ポリシー・データ・ストア１７２、および知識データ・ストア１７６に接続される。ローカル・ポリシー・データ・ストア１７２内のデータは、ネットワーク１９２を介して、リモート・ポリシー・データ・ストア１７４内のデータで更新され得る。

【００２１】
ネットワーク・データ・ストア１７０は、既存の構成データを保持する。本発明の特定の実装では、ネットワーク内の構成要素は、ネットワーク・データ・ストア１７０内に格

納するために、ファームウェア・レベル、装置ドライバ・レベルおよび構成データなど、その特性について報告し得る。自律型構成システム１５０は、構成要素を監視するために、少なくとも１つのエージェントを配置することができ、構成要素内で特定のアクティビティが行われるときに、エージェントは、自律型構成システム１５０にデータを返送し、それは、ネットワーク・データ・ストア１７０内に格納される。

【００２２】

たとえば、ストレージ管理イニシアティブ標準（ＳＭＩＳ：StorageManagement Initiative Standard）は、ＳＡＮ内の構成要素がその特性について報告する、データ・ストレージ・ソフトウェアのための標準について記載している。ＳＭＩＳは、全員がストレージ・ネットワーキング業界団体（ＳＮＩＡ：StorageNetworking Industry Association）のメンバである、（パートナー開発プログラム（ＰＤＰ：Partner DevelopmentProgram）と自称する団体によって作成された。ＳＭＩＳでは、ファームウェア・レベルおよび構成データなど、互換性に影響を及ぼす属性を更新するための方法が、ＳＡＮの構成要素によって提供される。

【００２３】

データ・ストアは、たとえばデータベースとすることができる。分かりやすいように、別個のデータ・ストア１７０、１７２、１７４、１７６が示されているが、データ・ストア１７０、１７２、１７４、１７６内のデータは、管理サーバ・コンピュータ１２０に接続されたそれよりも少ないまたは多いデータ・ストア内に格納されることも、管理サーバ・コンピュータ１２０に接続された他のコンピュータ上のデータ・ストア内に格納されることもある。

【００２４】

それぞれのデータ・ストア１７０、１７２、１７４、１７６は、直接アクセス記憶装置（ＤＡＳＤ：Direct Access Storage Device）、単純ディスク束（ＪＢＯＤ：Just a Bunch of Disks）、独立ディスク冗長アレイ（ＲＡＩＤ：RedundantArray of Independent Disks）、仮想装置など、記憶装置アレイを含み得る。

【００２５】

図２に、本発明の特定の実装による自律型構成システム１５０のさらなる詳細を示すブロック図を示す。構成要素２１０、２１２、２１４、２１６、２１８、２２０および２２２は、自律型構成マネージャ１５０の別個の構成要素として示されているが、構成要素２１０、２１２、２１４、２１６、２１８、２２０および２２２の機能は、図示するよりも少ない構成要素でも、それとは異なる構成要素内でも実装することができる。さらに、構成要素２１０、２１２、２１４、２１６、２１８、２２０および２２２のうちの少なくとも１つの機能は、管理サーバ・コンピュータ１２０に接続された別のコンピュータで実装することができる。

【００２６】

本発明の実装によって、事前対応型と事後対応型の両方のチェックを実施することができる。事前対応型層２１２によって、システム管理者は、構成したい新しいネットワーク構成に関する仮説的なシナリオを作成しチェックすることができる。事後対応型層２１０によって、システム管理者は、既存のネットワーク構成の構成チェックのための特性を指定することができる。

【００２７】

自律型ポリシー更新層２２４は、リモート・ポリシー・データ・ストア１７４に接触して、最新の構成ポリシーの変更を取得し、自律型ポリシー更新層２２４は、ローカル・ポリシー・データ・ストア１７２内に、その構成ポリシーを格納する。スキャナ／イベント生成器層２１４は、トランザクションを求めて、ネットワーク・データ・ストア１７０を走査し、少なくとも１つのトランザクションについて、イベントを生成する。トランザクションの例には、ホストｘｙｚをスイッチ１２３に接続、ホスト１ｂ６への新しいカードの追加、スイッチ９０２のファームウェア・コードの更新、構成要素のゾーン変更などが含まれる。

【００２８】
スキャナ／イベント生成器層２１４は、少なくとも１つのトランザクションを求めて、ネットワーク・データ・ストア１７０を走査し、その少なくとも１つのトランザクションについて、少なくとも１つのイベントを生成する。特定の実装では、少なくとも１つのイベントを、有効なトランザクションに関連付けるマッピングが存在する。ホストｘｙｚをスイッチ１２３に接続のトランザクションの場合、イベントの一例は、ホストｘｙｚおよびスイッチ１２３に関する構成データを取得する検証イベントとすることができる。構成データは、ホストのオペレーティング・システム、ホストとしてのＨＢＡの数、スイッチのファームウェア・レベルなどを識別し得る。イベントおよび取得された構成データは、ポリシー実行／トリガ生成器２１６に渡される。

【００２９】
具体的には、ポリシー実行／トリガ生成器２１６は、スキャナ／イベント生成器２１４から、特定のタイプのイベントおよび対応するデータを受信した後で、そのイベントについて、少なくとも１つのタイプのトリガを生成する。ホストｘｙｚをスイッチ１２３に接続のトランザクションおよび検証イベントの場合、トリガの例には、ホスト名－スイッチ名およびホスト位置－スイッチ位置が含まれる。またトリガは、トリガが生成されたイベントおよびそのイベントの構成データに関連付けられる。

【００３０】
ポリシー実行エンジン・ディスパッチャ（「ディスパッチャ」）２１８は、少なくとも１つのトリガに関連するローカル・ポリシー・データ・ストア１７２から、少なくとも１つの構成ポリシーを取り出し、その構成ポリシーをメモリにキャッシュする。特定の実装では、トリガによっては、関連する構成ポリシーをもたないことがある。構成ポリシーの例は、ホストｘｙｚはスイッチと同じ位置にあるというポリシー、およびホストｘｙｚは別のホストに接続されたスイッチには接続され得ないというポリシーとすることができる。

【００３１】
評価器２２０は、少なくとも１つの構成ポリシーを、トリガが生成されたイベントに関連する構成データと比較して、構成ポリシーが違反されたかどうか判定する。ホスト位置－スイッチ位置のトリガの場合、評価器２２０は、ホストｘｙｚはスイッチと同じ位置にあるという構成ポリシーを、ホストｘｙｚおよびスイッチ１２３の構成データと比較し得る。ホストｘｙｚおよびスイッチ１２３が同じ位置にない場合、その構成は、構成ポリシーに一致していない。アクション・マネージャ２２２は、評価器２２０による決定に基づいて、少なくとも１つのアクションを実施する。

【００３２】
図３に、本発明の特定の実装による事前対応型の手法の論理を示す。制御は、ブロック３００で、事前対応型層２１２を使用して生成された仮説ネットワーク・シナリオを受信することから開始する。特定の実装では、ネットワーク・トポロジは、事前対応型層２１２によって提供されるユーザ・インターフェースを使用して作成され得る。特定の代替実装では、ユーザは、パフォーマンス、可用性および他の制約を、ユーザ・インターフェースを介して入力することができ、ネットワーク・トポロジが自動的に作成される。ブロック３１０で、事前対応型層２１２は、仮説ネットワーク・シナリオに基づいて、少なくとも１つのトランザクションを作成する。ブロック３２０で、事前対応型層２１２は、ネットワーク・データ・ストア１７０に、少なくとも１つのトランザクションについての構成データを取り込む。特定の実装では、事前対応型層２１２は、ホスト構成要素、スイッチなど、ネットワーク内に含まれ得る構成要素の構成データを格納する。トランザクションがホストｘｙｚをスイッチ１２３に接続である場合、事前対応型層２１２は、ホストｘｙｚおよびスイッチ１２３の構成データを、ネットワーク・データ・ストア１７０内に格納する。

【００３３】
ブロック３３０で、自律型構成システム１５０の構成要素は、少なくとも１つのトラン

ザクションによって、非互換性、パフォーマンスの問題あるいは可用性の問題のいずれかまたはこれらの２つ以上の組合せがもたらされているかどうか判定する。非互換性は、構成要素間の競合と説明することができる。パフォーマンスの問題は、所望のパフォーマンス・レベルが満たされているかどうかに関する問題であると説明することができる。可用性の問題は、ネットワーク内のどこかに、単一障害箇所（single point of failure）があるかどうかに関する問題であると説明することができる。

【００３４】

ブロック３４０で、自律型構成システム１５０の構成要素は、報告を作成し送信する。ブロック３５０で、事前対応型層２１２は、少なくとも１つのトランザクションをロール・バックして、ネットワーク・データ・ストア１７０を、たとえば追加された構成データを削除することによって、前の整合状態に戻す（すなわちネットワーク・データ・ストア１７０を、それが少なくとも１つのトランザクションを作成する前の状態に戻す）。

【００３５】

図４に、本発明の特定の実装による事後対応型の手法の論理を示す。制御は、ブロック４００で、自律型構成システム１５０が、既存のネットワーク構成のチェックを実施するように求める要求を受信することから開始する。具体的には、事後対応層２１０は、システム管理者が、既存ネットワーク構成の構成チェックのための特性を指定できるようにする。たとえば、その特性によって、構成チェックが実施されるネットワークのゾーン、構成チェックが実施されるネットワーク内の構成要素、または構成チェックが実施される時間間隔(直前の１２時間など)が指定され得る。ブロック４１０で、指定された特性について、自律型構成システム１５０の構成要素は、既存のネットワーク構成によって、非互換性、パフォーマンスの問題および／または可用性の問題がもたらされているかどうか判定する。ブロック４２０で、ブロック４１０で行われた決定に基づいて、アクション・マネージャ２２２によって、少なくとも１つのアクションが実施される。

【００３６】

図５に、本発明の特定の実装による構成チェック実施の論理を示す。制御は、ブロック５００で、スキャナ／イベント生成器層２１４のスキャナが、少なくとも１つのトランザクションを求めて、ネットワーク・データ・ストア１７０を走査することから開始する。特定の実装では、スキャナは、新しいトランザクションを求めて走査する。ブロック５１０で、スキャナ／イベント生成器２１４のイベント生成器は、少なくとも１つのトランザクションについて、少なくとも１つのイベントを生成する。少なくとも１つのイベントは、トランザクションのイベントへのマッピングを使用して生成され得る。

【００３７】

特定の実装では、構成ポリシーは、接続タイプ、ゾーン・タイプ、ノード・タイプ、ループ・タイプまたはパス・パフォーマンス・タイプに分類され得る。接続タイプ・ポリシーは、どの構成要素が互いに直接接続されることができ、どの構成要素が直接接続され得ないかを示す。ゾーン・タイプのポリシーは、どの構成要素が同じゾーンに存在することができ、どの構成要素が同じゾーンに存在し得ないかを示す。ゾーンは、データ・パケットがどのように構成要素群間のポートを通過するかを定義する。たとえば、あるゾーンで、データ・パケットは、ホスト・コンピュータＡの第１のポートから、スイッチＢの第３のポートを流れ得る。次いで、特定のホスト・コンピュータは、特定のスイッチ・ポートを使用しないようにされ得る。ノード・タイプ・ポリシーは、どのタイプのＨＢＡが特定のホスト内に存在することができ、またドライバ、ファームウェアおよびオペレーティング・システム（ＯＳ：operating system）ソフトウェアのどの組合せに互換性があるかを示す。ループ・タイプ・ポリシーは、ファイバ・チャネル・アービトレーテッド・ループの一部として、どの構成要素が存在することができ、どの構成要素が存在し得ないかを示す。パス・パフォーマンス・タイプ・ポリシーは、所与のリンクまたは１組のリンクにとって、どのパス・ロードが適切であるかを示す。

【００３８】

接続データ（ノードＡがノードＢに接続されるなど）がネットワーク・データ・ストア

１７０から取り出される場合、スキャナ／イベント生成器層２１４は、接続タイプ・イベントを生成し、ポリシー実行エンジン・トリガ生成器（「トリガ生成器」）２１６に、接続の２つの終端に関するデータを送信する。ネットワーク１９０内のノード（ホスト・コンピュータ、スイッチまたはストレージ・アレイなど）の場合、スキャナ／イベント生成器層２１４は、ノードについての関連情報（ソフトウェアおよびハードウェア属性など）を抽出し、ノード・イベントの一部として、トリガ生成器２１６にその情報を送信する。ゾーンの場合、スキャナ／イベント生成器層２１４は、そのゾーン内のすべての構成要素のリストを取得し、ゾーン・イベントの一部として、ポリシー実行／トリガ生成器２１６にその情報を送信する。ネットワーク内のループの場合、スキャナ／イベント生成器層２１４は、そのループ内のすべての構成要素のリストを取得し、ループ・イベントの一部として、ポリシー実行／トリガ生成器２１６にその情報を送信する。スイッチ間リンクの場合、スキャナ／イベント生成器層２１４は、そのリンクを通るすべてのパスのリストを取得し、パス・パフォーマンス・イベントの一部として、ポリシー実行／トリガ生成器２１６にローディング情報を送信する。

【００３９】

スキャナ／イベント生成器２１４から、少なくとも１つのイベントおよび対応する構成データを受信した後で、ブロック５２０で、ポリシー実行／トリガ生成器２１６は、その少なくとも１つのイベントについて、少なくとも１つのタイプのトリガを生成する。用語「トリガ」は、ポリシー実行エンジン評価器２２０が理解することができる形でデータを編成することによって表されるアクションであると説明することができる。たとえば、２つより多い構成要素を含むゾーンの単一ゾーン・イベントの場合、トリガ生成器２１６は、複数の異なるトリガを生成する。トリガは、考慮対象であるゾーン内の２つの構成要素の組合せを表し得る。こうした場合、「ｎ」個の構成要素からなる単一のゾーン・イベントについて、トリガ生成器２１６は、単一の組合せのそれぞれがトリガによって表される、サイズ２のそれぞれ異なる組合せを生成する。同様に、ノードおよび接続イベントの場合、トリガ生成器２１６は、ソフトウェア、ファームウェアおよびハードウェア特性のそれぞれ異なる組合せを評価するトリガを生成する。

【００４０】

ブロック５３０で、ポリシー実行エンジン・ディスパッチャ（「ディスパッチャ」）２１８は、ローカル・ポリシー・データ・ストア１７２から、少なくとも１つの構成ポリシーを取り出し、その少なくとも１つの構成ポリシーをメモリ内にキャッシュする。ブロック５４０で、少なくとも１つのタイプのトリガについて、ディスパッチャ２１８は、取り出されたポリシーのうちの０個以上のポリシーをトリガに関連付け、ポリシー実行エンジン評価器（「評価器」）２２０に、関連する構成ポリシーを送信する。

【００４１】

ブロック５４０で、評価器２２０は、少なくとも１つのトリガについて、構成ポリシーを、トリガによって供給されるデータと比較して、構成ポリシーが違反されたかどうか判定する。

【００４２】

ブロック５５０で、アクション・マネージャ２２２は、評価器２２０による決定に基づいて、少なくとも１つのアクションを実施する。特定の実装では、構成ポリシーが違反された場合には、アクション・マネージャ２２２は、違反のログ、ポリシー違反イベントの生成、通知の送信（システム管理者にｅメールを送信するなど）、またはネットワークをグラフィカルに描写するネットワーク・トポロジ・ビューアの特定の部分を強調表示するなど、構成ポリシー内に指定された適切な措置を取る。特定の実装では、アクション・マネージャ２２２は、違反を自動的に訂正する。たとえば、アクション・マネージャは、知識データ・ストア１７６からデータを取り出し、解決策を適用することができる。

【００４３】

図６に、本発明の特定の実装による自律型訂正の論理を示す。制御は、ブロック６００で、自律型構成システム１５０が、ネットワークまたはストレージあるいはその両方に関

連する構成上の問題を検出することから開始する。事前対応型の手法および事後対応型の手法に加えて、様々なやり方で、ネットワークまたはストレージあるいはその両方に関連するネットワークの構成上の問題が検出され得る。たとえば、自律型構成システム１５０は、ネットワークの各構成要素に、その属性および接続性について定期的に問い合わせることができる。次いで、自律型構成システム１５０は、各接続の動作状態チェック（health check）を実施し得る。別のネットワークまたはストレージあるいはその両方に関連する構成上の問題の検出技術は、共通情報モデル（ＣＩＭ：CommonInformation Model）指示、ネットワーク管理プロトコル（ＳＮＭＰ：Network Management Protocol）トラップとして、または他の報告の技術を使用して、Ｉ／Ｏ障害などの実際の問題を報告する構成要素を要する。ＣＩＭは、情報管理のためのオブジェクト指向モデルの標準である。ＣＩＭ標準は、分散管理タスクフォース・インク社（DistributedManagement Task Force (DMTF), Inc）によって提供される。ＣＩＭ標準に関するさらなる情報については、「ＨＴＴＰを介したＣＩＭオペレーションの仕様（Specificationfor CIM Operations over HTTP）」、１．１版、２００２年５月２日を参照されたい。ＳＮＭＰは、ネットワーク内の構成要素を監視および管理するためのプロトコルであると説明することができる。ＳＮＭＰによってサポートされる機能によって、データの要求および取出し、データの設定または書込み、およびイベントの発生を知らせるトラップが可能になる。

【００４４】

ネットワークまたはストレージあるいはその両方に関連する構成上の問題が検出される場合には、ネットワークまたはストレージあるいはその両方に関連する構成上の問題を解決するために何を行う必要があるかを決定するいくつかのやり方がある。ブロック６１０で、構成要素が解決策を識別したかどうか判定される。そうである場合、処理は、ブロック６２０に続き、そうでない場合、処理は、ブロック６３０に続く。場合によっては、ある構成要素が、別の構成要素内で何が必要とされているかを直接的に識別することができる。たとえば、特定のベンダ固有の小型コンピュータ・システム・インターフェース（ＳＣＳＩ：Small Computer System Interface）コマンドを含む記憶装置を必要とする装置ドライバの構成では、接続された記憶装置がそのコマンドを有さない場合は、その装置ドライバを、コマンドを使用しないように構成することができ、あるいは装置構成、ファームウェア、またはマイクロコードが、そのコマンドを含むように更新される。ブロック６２０で、構成要素は、解決策を提供する。

【００４５】

ブロック６３０で、ネットワークまたはストレージあるいはその両方に関連する構成上の問題についての解決策が、知識データ・ストア１７６内で得られるかどうか判定される。そうである場合、処理は、ブロック６４０に続き、そうでない場合、処理は、ブロック６６０に続く。知識データ・ストア１７６は、たとえばシステム管理分野の専門家によって集められ、またプログラムのインストール時に、またはライブ更新のプロセスとして（インターネットを介してなど）入手可能にされる。

【００４６】

ネットワークまたはストレージあるいはその両方に関連する構成上の問題についての複数の解決策が得られる場合、ブロック６４０で、様々な要因に基づいて、１つが自動的に選択される。たとえば、ネットワークまたはストレージあるいはその両方に関する一部の情報を、それぞれの解決策とともに含めることができ、既存のまたは仮説のシナリオが、ネットワークまたはストレージあるいはその両方に関する含まれている情報にどれほど近似しているかに基づいて、１つの解決策が選択され得る。また一部の要因は、たとえば、ある解決策が特定のベンダからの構成要素に、より有効であり、あるいは解決策が大規模なネットワーク構成よりも小規模なネットワーク構成により有効であることとすることができる。特定の代替実装では、複数の可能な解決策がある場合、ユーザには、複数の可能な解決策から１つを選択し、または自動選択を可能にするオプションが提供され得る。

【００４７】

知識データ・ストア内の一部の解決策は、ユーザ介入を必要とし得る。たとえば、ネッ

トワークまたはストレージあるいはその両方に関連する構成上の検出された問題が、構成要素が電流を受けていないことである場合、ユーザは、（たとえば構成要素を電源に「差し込む」などによって）その構成要素に電力を供給する必要があり得る。他の解決策が自動的に適用される。たとえば、ゾーン変更が望ましい場合は、ゾーン変更が自動的に実施され得る。ブロック６５０で、選択された解決策を自動的に適用することができるかどうか判定される。解決策を自動的に適用することができる場合、処理は、ブロック６６０に続き、そうでない場合、処理は、ブロック６７０に続く。

【００４８】

ブロック６６０で、知識データ・ストア１７６から選択された解決策が自動的に適用される。したがって、特定の実装では、ネットワークまたはストレージあるいはその両方に関連する構成上の問題を解決するために、所与の１組の条件について、知識データ・ストア１７６からの最も適合する解決策が自動的に適用される。

【００４９】

ブロック６７０で、ネットワークまたはストレージあるいはその両方に関連する構成上の問題についての解決策が知識データ・ストア内に存在しない、またはそれが自動的に解決され得ない場合は、ユーザに通知される。特定の実装では、ユーザが解決策を提供する場合、その解決策が知識データ・ストア１７６に追加され得る。

【００５０】

したがって、本発明の実装によって、制約が自律型構成システム１５０内にハード・コードされないことが可能になり、新しい構成上の制約を、制約のデータ・ストアからダウンロードすることが可能になり、事前対応型および事後対応型のネットワーク構成チェックが可能になり、またネットワークまたはストレージあるいはその両方に関連する構成上の問題の自動訂正が可能になる。

【００５１】

ＩＢＭおよびＴｉｖｏｌｉは、米国または他国あるいはその両方のインターナショナル・ビジネス・マシーンズ・コーポレーション社の登録商標またはコモンロー商標である。

【００５２】

追加の実装の詳細

ネットワーク構成のチェックおよび修理のための上述の技術は、ソフトウェア、ファームウェア、ハードウェアまたはその任意の組合せを製造するための標準のプログラミングまたは工学技術あるいはその両方を使用した、方法、装置または製品として実装することができる。本明細書では、用語「製品（article of manufacture）」は、ハードウェア論理（集積回路チップ、プログラマブル・ゲート・アレイ（ＰＧＡ：ProgrammableGate Array）、特定用途向け集積回路（ＡＳＩＣ：Application Specific Integrated Circuit）など）、または磁気記憶装置（ハード・ディスク・ドライブ、フロッピー（Ｒ）ディスク、テープなど）、光ストレージ（ＣＤ－ＲＯＭ、光ディスクなど）、揮発性および不揮発性のメモリ装置（ＥＥＰＲＯＭ、ＲＯＭ、ＰＲＯＭ、ＲＡＭ、ＤＲＡＭ、ＳＲＡＭ、ファームウェア、プログラマブル論理など）などのコンピュータ読取り可能媒体内で実装されたコードまたは論理を指す。コンピュータ読取り可能媒体内のコードは、プロセッサによってアクセスされ実行される。様々な実装が実装されるコードはさらに、伝送媒体を介して、またはファイル・サーバからネットワークを介してアクセス可能とすることができる。こうした場合、コードが実装された製品は、ネットワーク伝送回線などの伝送媒体、無線伝送媒体、空間を伝播する信号、無線波、赤外線信号などを含み得る。したがって、「製品」は、コードが実装された媒体を含み得る。さらに、「製品」は、コードが実装され、処理され、実行される、ハードウェアとソフトウェア構成要素の組合せを含み得る。もちろん、本発明の範囲から逸脱せずに、この構成に対して多くの修正を行うことができ、また製品が当技術分野で周知の任意の信号搬送媒体を含み得ることが当業者には理解されよう。

【００５３】

図３～６の論理は、特定の順序で発生する具体的なオペレーションについて説明してい

る。代替の実装では、一部の論理オペレーションは、別の順序で実施され、修正され、または削除され得る。さらに、オペレーションが上述の論理に追加され、またそれは、上述の実装に依然として合致し得る。さらに、本明細書で述べたオペレーションは、順次行われることができ、または一部のオペレーションは、平行に処理されることができ、あるいは単一のプロセスによって実施されるものとして述べたオペレーションは、分散されたプロセスによって実施することもできる。

【００５４】

図３～６に図示した論理は、ソフトウェア、ハードウェア、プログラマブルおよび非プログラマブルなゲート・アレイ論理で、あるいはハードウェア、ソフトウェアまたはゲート・アレイ論理の何らかの組合せで実装することができる。

【００５５】

図７に、本発明の特定の実装に従って使用され得るコンピュータ・システムのアーキテクチャを示す。管理サーバ・コンピュータ１２０は、アーキテクチャ７００を実装し得る。コンピュータ・アーキテクチャ７００は、プロセッサ７０２（マイクロプロセッサなど）、メモリ７０４（揮発性メモリ装置など）、およびストレージ７１０（磁気ディスク・ドライブ、光ディスク・ドライブ、テープ・ドライブなどの不揮発性記憶域）を実装し得る。オペレーティング・システム７０５は、メモリ７０４内で実行され得る。ストレージ７１０は、内部記憶装置、あるいは接続されたまたはネットワーク・アクセス可能ストレージを含み得る。ストレージ７１０内のコンピュータ・プログラム７０６は、当技術分野で周知のやり方で、メモリ７０４内にロードされ、プロセッサ７０２によって実行され得る。アーキテクチャはさらに、ネットワークとの通信を可能にするネットワーク・カード７０８を含む。入力装置７１２は、プロセッサ７０２にユーザ入力を提供するために使用され、またキーボード、マウス、ペン・スタイラス、マイク、タッチ・スクリーン、あるいは当技術分野で周知の他の任意のアクティブ化または入力の機構を含み得る。出力装置７１４は、プロセッサ７０２、または表示モニタ、プリンタ、ストレージなどの他の構成要素からの情報をレンダリングすることができる。コンピュータ・システムのコンピュータ・アーキテクチャ７００は、図示したよりも少ない構成要素を含むことも、本明細書に図示していない追加の構成要素を含むことも、図示した構成要素と追加の構成要素の何らかの組合せを含むこともある。

【００５６】

コンピュータ・アーキテクチャ７００は、メインフレーム、サーバ、パーソナル・コンピュータ、ワークステーション、ラップトップ、ハンドヘルド・コンピュータ、電話装置、ネットワーク装置、仮想化装置、ストレージ・コントローラなど、当技術分野で周知の任意のコンピューティング装置を含み得る。当技術分野で周知の任意のプロセッサ７０２およびオペレーティング・システム７０５が使用され得る。

【００５７】

本発明の実装の上記内容は、例示および説明のために提示されている。網羅的とすることも、本発明を、開示されている厳密な形に限定することも意図されていない。上記の教示に鑑みて、多くの修正および変更が可能である。本発明の範囲は、この詳細な説明ではなく、それに添付された特許請求の範囲によって限定されるものとする。上記の明細、例およびデータは、本発明の構成の製造および使用についての完全な説明を提供している。本発明の精神および範囲から逸脱せずに、本発明の多くの実装が行われ得るので、本発明は、添付の特許請求の範囲に属する。

【図面の簡単な説明】

【００５８】

【図１】本発明の特定の実装によるコンピューティング環境のブロック図である。

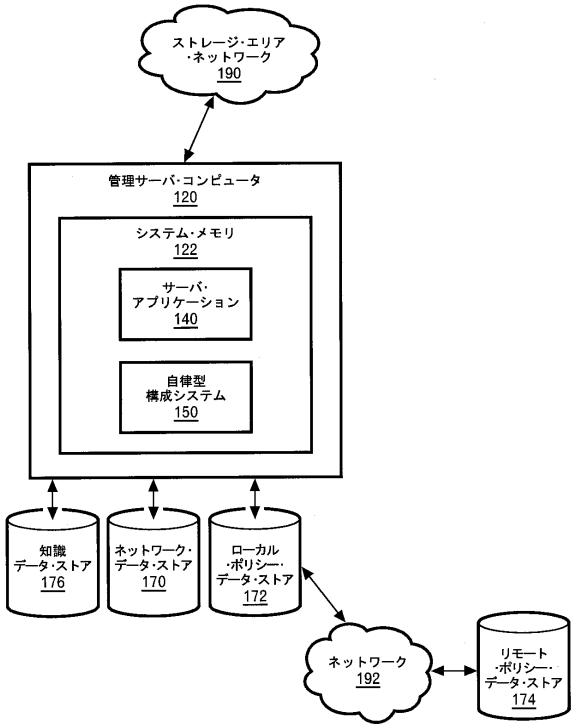
【図２】本発明の特定の実装による自律型構成システムをより詳細に示すブロック図である。

【図３】本発明の特定の実装による事前対応型の手法の論理を示す図である。

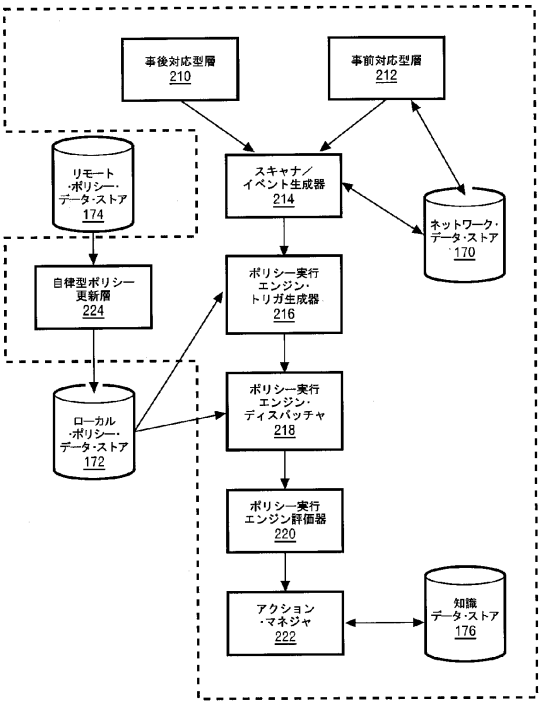
【図４】本発明の特定の実装による事後対応型の手法の論理を示す図である。

【図５】本発明の特定の実装による構成チェック実施の論理を示す図である。
【図６】本発明の特定の実装による自律型の訂正の論理を示す図である。
【図７】本発明の特定の実装に従って使用され得るコンピュータ・システムのアーキテクチャを示す図である。
【符号の説明】
【００５９】
１２０　管理サーバ・コンピュータ
１２２　システム・メモリ
１４０　サーバ・アプリケーション
１５０　自律型構成システム
１７０　ネットワーク・データ・ストア
１７２　ローカル・ポリシー・データ・ストア
１７４　リモート・ポリシー・データ・ストア
１７６　知識データ・ストア
１９０　ストレージ・エリア・ネットワーク
１９２　ネットワーク
２１０　事後対応型（reactive）層
２１２　事前対応型（proactive）層
２１４　スキャナ／イベント生成器
２１６　ポリシー実行エンジン・トリガ生成器
２１８　ポリシー実行エンジン・ディスパッチャ
２２０　ポリシー実行エンジン評価器
２２２　アクション・マネージャ
２２４　自律型ポリシー更新層
７００　コンピュータ・アーキテクチャ
７０２　プロセッサ
７０４　メモリ
７０５　オペレーティング・システム
７０６　コンピュータ・プログラム
７０８　ネットワーク・カード
７１０　ストレージ
７１２　入力装置
７１４　出力装置

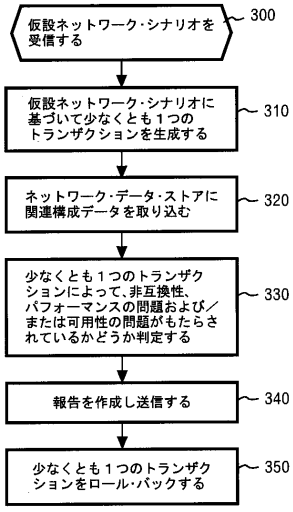
【図１】


ストレージ・エリア
・ネットワーク
190
管理サーバ・コンピュータ
120
システム・メモリ
122
サーバ・
アプリケーション
140
自律型
構成システム
150
知識
データ・ストア
176
ネットワーク・
データ・ストア
170
ローカル
・ポリシー・
データ・ストア
172
ネットワーク
192
リモート
・ポリシー・
データ・ストア
174

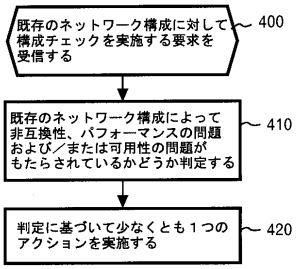
【図２】


事後対応型層
210
事前対応型層
212
リモート
・ポリシー・
データ・ストア
174
スキャナ／
イベント生成器
214
ネットワーク・
データ・ストア
170
自律型ポリシー
更新層
224
ポリシー実行
エンジン・
トリガ生成器
216
ローカル
・ポリシー・
データ・ストア
172
ポリシー実行
エンジン・
ディスパッチャ
218
ポリシー実行
エンジン評価器
220
アクション
・マネジャ
222
知識
データ・ストア
176

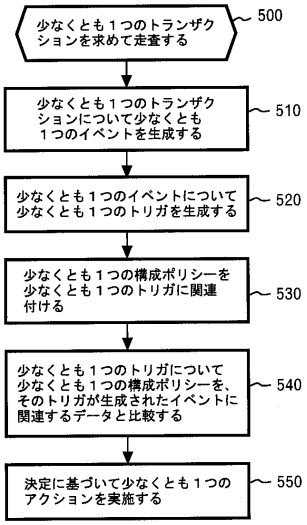
【図３】


仮設ネットワーク・シナリオを
受信する
300
仮設ネットワーク・シナリオに
基づいて少なくとも１つの
トランザクションを生成する
310
ネットワーク・データ・ストアに
関連構成データを取り込む
320
少なくとも１つのトランザク
ションによって、非互換性、
パフォーマンスの問題および／
または可用性の問題がもたらさ
れているかどうか判定する
330
報告を作成し送信する
340
少なくとも１つのトランザク
ションをロール・バックする
350

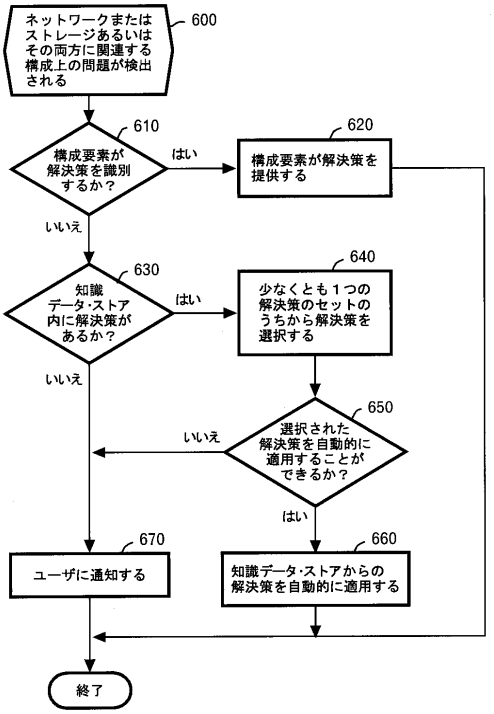
【図４】


既存のネットワーク構成に対して
構成チェックを実施する要求を
受信する
400
既存のネットワーク構成によって
非互換性、パフォーマンスの問題
および／または可用性の問題が
もたらされているかどうか判定する
410
判定に基づいて少なくとも１つの
アクションを実施する
420

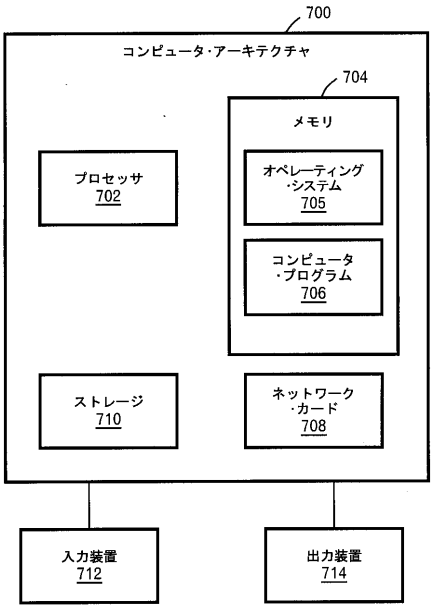
【図５】


少なくとも１つのトランザクションを求めて走査する
500
少なくとも１つのトランザクションについて少なくとも１つのイベントを生成する
510
少なくとも１つのイベントについて少なくとも１つのトリガを生成する
520
少なくとも１つの構成ポリシーを少なくとも１つのトリガに関連付ける
530
少なくとも１つのトリガについて少なくとも１つの構成ポリシーを、そのトリガが生成されたイベントに関連するデータと比較する
540
決定に基づいて少なくとも１つのアクションを実施する
550

【図６】


ネットワークまたはストレージあるいはその両方に関連する構成上の問題が検出される
600
構成要素が解決策を識別するか？
610
はい
構成要素が解決策を提供する
620
いいえ
知識データ・ストア内に解決策があるか？
630
はい
少なくとも１つの解決策のセットのうちから解決策を選択する
640
いいえ
選択された解決策を自動的に適用することができるか？
650
はい
ユーザに通知する
670
知識データ・ストアからの解決策を自動的に適用する
660
終了

【図７】


700
コンピュータ・アーキテクチャ
704
メモリ
プロセッサ
702
オペレーティング・システム
705
コンピュータ・プログラム
706
ストレージ
710
ネットワーク・カード
708
入力装置
712
出力装置
714

フロントページの続き

(74)代理人 100086243
弁理士 坂口 博
(72)発明者 クーオン・ミン・レ
アメリカ合衆国８５７４８ アリゾナ州ツーソン イースト・モニュメント・エステイツ・サークル １０９５１
(72)発明者 デービッド・マイケル・シャッケルフォード
アメリカ合衆国８５７４３ アリゾナ州ツーソン ノース・ミル・クロッシング・ウェイ １０１０２
(72)発明者 グレゴリー・エドワード・マクブライド
アメリカ合衆国８５７１０ アリゾナ州ツーソン ノース・サーノフ・ドライブ ３５６
(72)発明者 ジェームズ・ミッチェル・ラットリフ
アメリカ合衆国８５６０２ アリゾナ州ベンソン ウェスト・ヤヴァパイ・プレイス ３２４２
(72)発明者 カラドハー・ヴォルガンティ
アメリカ合衆国９５１３６ カリフォルニア州サンホセ ミル・クリーク・レーン ５２４０
(72)発明者 サンディープ・ゴピセッティ
アメリカ合衆国９５０３７－２７００ カリフォルニア州モーガン・ヒル クレイトン・アヴェニュー １９０４１
(72)発明者 ロバート・ベヴァリー・バシャム
アメリカ合衆国９７００７ オレゴン州アロホ トレモント・ウェイ・サウス・ウェスト ２０２０１
(72)発明者 ディネッシュ・シー・ヴェルマ
アメリカ合衆国１０５４９ ニューヨーク州ニュー・キャッスル キスコ・パーク・ドライブ ５６
(72)発明者 カンウォン・リー
アメリカ合衆国１０９５４ ニューヨーク州ナヌエット アヴァロン・ガーデンズ・ドライブ ２５１
(72)発明者 ダクシ・アグラワル
アメリカ合衆国１０５９８ ニューヨーク州ヨークタウン・ハイツ ボールドウィン・ロード １８７０ ユニット・ナンバー２９
(72)発明者 ブレント・ウィリアム・ヤードレー
アメリカ合衆国９７００６ オレゴン州ビーバートン サウス・ウェスト・ワン・ハンドレッド・シックスティ・サード・アヴェニュー ９２０ ナンバー２１１５
(72)発明者 ハリド・フィラリ・アディブ
アメリカ合衆国７８７２７ テキサス州オースチン デスティニーズ・ゲート・ドライブ ４４１３

審査官 横山 佳弘

(56)参考文献 特開２００３－２６３３４９（ＪＰ，Ａ）
特開２０００－２１６７８０（ＪＰ，Ａ）
特開平０３－１４５８４６（ＪＰ，Ａ）
特開２０００－２０９２０２（ＪＰ，Ａ）
特開２００２－０４２２１８（ＪＰ，Ａ）
特開平０９－１６０８４９（ＪＰ，Ａ）
特開２０００－２０７２３７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ １３／１０

G06F　13/14
H04L　12/26
G06F　13/00