(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7648564号
(P7648564)

(45)発行日　令和7年3月18日(2025.3.18)

(24)登録日　令和7年3月10日(2025.3.10)

(51)国際特許分類

Ｈ０４Ｌ　43/20　(2022.01)		Ｈ０４Ｌ	43/20
Ｈ０４Ｌ　43/04　(2022.01)		Ｈ０４Ｌ	43/04

ＦＩ

請求項の数　5　（全15頁）

(21)出願番号　特願2022-60589(P2022-60589)
(22)出願日　令和4年3月31日(2022.3.31)
(65)公開番号　特開2023-151142(P2023-151142A)
(43)公開日　令和5年10月16日(2023.10.16)
審査請求日　令和6年1月23日(2024.1.23)
（出願人による申告）令和三年度、総務省「先進的仮想化ネットワークの基盤技術の研究開発」委託事業、産業技術力強化法第１７条の適用を受ける特許出願

(73)特許権者　000208891
ＫＤＤＩ株式会社
東京都新宿区西新宿二丁目３番２号
(74)代理人　100165179
弁理士　田▲崎▼ 聡
(74)代理人　100175824
弁理士　小林 淳一
(74)代理人　100114937
弁理士　松本 裕幸
(72)発明者　河崎 純一
埼玉県ふじみ野市大原二丁目１番１５号
株式会社ＫＤＤＩ総合研究所内
審査官　安井 雅史

最終頁に続く

(54)【発明の名称】　データ収集装置、データ収集方法及びコンピュータプログラム

(57)【特許請求の範囲】

【請求項１】

クラウドネイティブネットワーク機能（ＣＮＦ）が用いられた監視対象の仮想ネットワークに関するマッピング情報及び前記監視対象の仮想ネットワークの構成情報に基づいて生成されたテーブルであって、監視単位毎に設けられたタグ情報と、前記監視対象の仮想ネットワークの仮想ネットワークインスタンス及び前記仮想ネットワークインスタンスが実行される仮想化基盤の情報処理装置から収集されるネットワーク情報を識別するための識別情報と、前記タグ情報を付加するためのタグ付加条件とが対応付けて格納されるマッピングテーブルと、

前記仮想ネットワークインスタンス及び前記仮想化基盤の情報処理装置から収集されたネットワーク情報を受信するコレクタ部と、

前記コレクタ部が受信したネットワーク情報に対して、前記マッピングテーブルに基づいて前記タグ情報を付加するマッピング部と、

を備え、

前記マッピング情報は、監視単位毎に、前記タグ情報、前記識別情報、前記タグ付加条件、及び前記タグ付加条件として前記監視対象の仮想ネットワークの構成情報の動的な情報が用いられる場合に前記動的な情報を取得するための付加情報を有し、

前記付加情報は、前記動的な情報と前記動的な情報の取得先とを示す情報であり、

前記マッピングテーブルは、各監視単位のタグ情報毎に、前記識別情報、前記タグ付加条件、及び前記タグ付加条件に合致した場合に付加されるタグ情報を格納し、

前記動的な情報が用いられる前記タグ付加条件は、前記付加情報に基づいて取得された前記動的な情報が前記マッピングテーブルに格納される、
データ収集装置。
【請求項２】
前記付加情報に示される取得先から、前記付加情報に示される前記動的な情報を取得し、取得した前記動的な情報を使用して前記マッピングテーブルを生成するマッピングテーブル生成部、
をさらに備える請求項１に記載のデータ収集装置。
【請求項３】
前記マッピングテーブル生成部は、前記マッピング情報と前記監視対象の仮想ネットワークの構成とのうち少なくとも一方が変更された場合に、前記マッピング情報に基づいて、前記監視対象の仮想ネットワークの構成情報を再取得し、再取得した前記監視対象の仮想ネットワークの構成情報を使用して前記マッピングテーブルを更新する、
請求項２に記載のデータ収集装置。
【請求項４】
データ収集装置が、クラウドネイティブネットワーク機能（ＣＮＦ）が用いられた監視対象の仮想ネットワークに関するマッピング情報及び前記監視対象の仮想ネットワークの構成情報に基づいて生成されたテーブルであって、監視単位毎に設けられたタグ情報と、前記監視対象の仮想ネットワークの仮想ネットワークインスタンス及び前記仮想ネットワークインスタンスが実行される仮想化基盤の情報処理装置から収集されるネットワーク情報を識別するための識別情報と、前記タグ情報を付加するためのタグ付加条件とが対応付けて格納されるマッピングテーブルを備え、
前記データ収集装置が、前記仮想ネットワークインスタンス及び前記仮想化基盤の情報処理装置から収集されたネットワーク情報を受信するネットワーク情報受信ステップと、
前記データ収集装置が、前記ネットワーク情報受信ステップで受信したネットワーク情報に対して、前記マッピングテーブルに基づいて前記タグ情報を付加するタグ付加ステップと、を含み、
前記マッピング情報は、監視単位毎に、前記タグ情報、前記識別情報、前記タグ付加条件、及び前記タグ付加条件として前記監視対象の仮想ネットワークの構成情報の動的な情報が用いられる場合に前記動的な情報を取得するための付加情報を有し、
前記付加情報は、前記動的な情報と前記動的な情報の取得先とを示す情報であり、
前記マッピングテーブルは、各監視単位のタグ情報毎に、前記識別情報、前記タグ付加条件、及び前記タグ付加条件に合致した場合に付加されるタグ情報を格納し、
前記動的な情報が用いられる前記タグ付加条件は、前記付加情報に基づいて取得された前記動的な情報が前記マッピングテーブルに格納される、
データ収集方法。
【請求項５】
コンピュータに、
クラウドネイティブネットワーク機能（ＣＮＦ）が用いられた監視対象の仮想ネットワークに関するマッピング情報及び前記監視対象の仮想ネットワークの構成情報に基づいて生成されたテーブルであって、監視単位毎に設けられたタグ情報と、前記監視対象の仮想ネットワークの仮想ネットワークインスタンス及び前記仮想ネットワークインスタンスが実行される仮想化基盤の情報処理装置から収集されるネットワーク情報を識別するための識別情報と、前記タグ情報を付加するためのタグ付加条件とが対応付けて格納されるマッピングテーブルを記憶するステップと、
前記仮想ネットワークインスタンス及び前記仮想化基盤の情報処理装置から収集されたネットワーク情報を受信するネットワーク情報受信ステップと、
前記ネットワーク情報受信ステップで受信したネットワーク情報に対して、前記マッピングテーブルに基づいて前記タグ情報を付加するタグ付加ステップと、
を実行させるためのコンピュータプログラムであり、

前記マッピング情報は、監視単位毎に、前記タグ情報、前記識別情報、前記タグ付加条件、及び前記タグ付加条件として前記監視対象の仮想ネットワークの構成情報の動的な情報が用いられる場合に前記動的な情報を取得するための付加情報を有し、
前記付加情報は、前記動的な情報と前記動的な情報の取得先とを示す情報であり、
前記マッピングテーブルは、各監視単位のタグ情報毎に、前記識別情報、前記タグ付加条件、及び前記タグ付加条件に合致した場合に付加されるタグ情報を格納し、
前記動的な情報が用いられる前記タグ付加条件は、前記付加情報に基づいて取得された前記動的な情報が前記マッピングテーブルに格納される、
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、データ収集装置、データ収集方法及びコンピュータプログラムに関する。

【背景技術】

【０００２】

近年、仮想化技術の進展により、通信ネットワークの分野においても仮想化された通信ネットワーク（仮想ネットワーク）が普及しつつある。仮想ネットワークは、利用者の状況に応じて必要な時に必要な分だけネットワーク機能を拡充することができるという利点を持つ。一方で、仮想ネットワークは、ネットワーク構成要素が増え且つネットワーク構成が動的に変化するために、ネットワークの保守や運用面において安定的にネットワークを稼働させるためのネットワーク監視が課題である。仮想ネットワークは、仮想化基盤である物理サーバ上に仮想ネットワークインスタンスとしてネットワーク機能が構築されるため、物理サーバと仮想ネットワークインスタンスの両面から稼働状況を監視することが求められる。

【０００３】

特許文献１には、仮想ネットワークを監視するために、ＶＮＦ（Virtual Network Function、仮想化ネットワーク機能）と当該ＶＮＦをサポートする基盤であるネットワーク機能仮想化インフラストラクチャ（ＮＦＶＩ）とから得られるデータに基づいて、オートスケール等のライフサイクル管理動作の必要性を判断する、仮想ネットワーク監視技術が記載されている。

【先行技術文献】

【特許文献】

【０００４】

【文献】特表２０１８－５０４８０９号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

しかし、上述した特許文献１に記載された仮想ネットワーク監視技術は、仮想マシン（ＶＭ）ベースの仮想化ネットワーク機能であるＶＮＦが対象であるために、ＣＮＦ（Cloud-native Network Function、クラウドネイティブネットワーク機能）を対象にすることが難しい。ＣＮＦは、ＶＭベースのＶＮＦとは異なるアーキテクチャであるコンテナベースの仮想化ネットワーク機能である。コンテナはクラウドコンピューティングサービスで広く利用されている技術であるため、ＣＮＦは今後特に普及が見込まれる。

【０００６】

本発明は、このような事情を考慮してなされたものであり、その目的は、ＣＮＦが用いられた仮想ネットワークを対象にしたネットワーク監視に寄与することにある。

【課題を解決するための手段】

【０００７】

（１）本発明の一態様は、クラウドネイティブネットワーク機能（ＣＮＦ）が用いられた監視対象の仮想ネットワークに関するマッピング情報及び前記監視対象の仮想ネットワー

クの構成情報に基づいて生成されたテーブルであって、監視単位毎に設けられたタグ情報と、前記監視対象の仮想ネットワークの仮想ネットワークインスタンス及び前記仮想ネットワークインスタンスが実行される仮想化基盤の情報処理装置から収集されるネットワーク情報を識別するための識別情報と、前記タグ情報を付加するためのタグ付加条件とが対応付けて格納されるマッピングテーブルと、前記仮想ネットワークインスタンス及び前記仮想化基盤の情報処理装置から収集されたネットワーク情報を受信するコレクタ部と、前記コレクタ部が受信したネットワーク情報に対して、前記マッピングテーブルに基づいて前記タグ情報を付加するマッピング部と、を備え、前記マッピング情報は、監視単位毎に、前記タグ情報、前記識別情報、前記タグ付加条件、及び前記タグ付加条件として前記監視対象の仮想ネットワークの構成情報の動的な情報が用いられる場合に前記動的な情報を取得するための付加情報を有し、前記付加情報は、前記動的な情報と前記動的な情報の取得先とを示す情報であり、前記マッピングテーブルは、各監視単位のタグ情報毎に、前記識別情報、前記タグ付加条件、及び前記タグ付加条件に合致した場合に付加されるタグ情報を格納し、前記動的な情報が用いられる前記タグ付加条件は、前記付加情報に基づいて取得された前記動的な情報が前記マッピングテーブルに格納される、データ収集装置である。

（２）本発明の一態様は、前記付加情報に示される取得先から、前記付加情報に示される前記動的な情報を取得し、取得した前記動的な情報を使用して前記マッピングテーブルを生成するマッピングテーブル生成部、をさらに備える上記（１）のデータ収集装置である。

（３）本発明の一態様は、前記マッピングテーブル生成部は、前記マッピング情報と前記監視対象の仮想ネットワークの構成とのうち少なくとも一方が変更された場合に、前記マッピング情報に基づいて、前記監視対象の仮想ネットワークの構成情報を再取得し、再取得した前記監視対象の仮想ネットワークの構成情報を使用して前記マッピングテーブルを更新する、上記（２）のデータ収集装置である。

【０００８】

（４）本発明の一態様は、データ収集装置が、クラウドネイティブネットワーク機能（ＣＮＦ）が用いられた監視対象の仮想ネットワークに関するマッピング情報及び前記監視対象の仮想ネットワークの構成情報に基づいて生成されたテーブルであって、監視単位毎に設けられたタグ情報と、前記監視対象の仮想ネットワークの仮想ネットワークインスタンス及び前記仮想ネットワークインスタンスが実行される仮想化基盤の情報処理装置から収集されるネットワーク情報を識別するための識別情報と、前記タグ情報を付加するためのタグ付加条件とが対応付けて格納されるマッピングテーブルを備え、前記データ収集装置が、前記仮想ネットワークインスタンス及び前記仮想化基盤の情報処理装置から収集されたネットワーク情報を受信するネットワーク情報受信ステップと、前記データ収集装置が、前記ネットワーク情報受信ステップで受信したネットワーク情報に対して、前記マッピングテーブルに基づいて前記タグ情報を付加するタグ付加ステップと、を含み、前記マッピング情報は、監視単位毎に、前記タグ情報、前記識別情報、前記タグ付加条件、及び前記タグ付加条件として前記監視対象の仮想ネットワークの構成情報の動的な情報が用いられる場合に前記動的な情報を取得するための付加情報を有し、前記付加情報は、前記動的な情報と前記動的な情報の取得先とを示す情報であり、前記マッピングテーブルは、各監視単位のタグ情報毎に、前記識別情報、前記タグ付加条件、及び前記タグ付加条件に合致した場合に付加されるタグ情報を格納し、前記動的な情報が用いられる前記タグ付加条件は、前記付加情報に基づいて取得された前記動的な情報が前記マッピングテーブルに格納される、データ収集方法である。

【０００９】

（５）本発明の一態様は、コンピュータに、クラウドネイティブネットワーク機能（ＣＮＦ）が用いられた監視対象の仮想ネットワークに関するマッピング情報及び前記監視対象の仮想ネットワークの構成情報に基づいて生成されたテーブルであって、監視単位毎に設けられたタグ情報と、前記監視対象の仮想ネットワークの仮想ネットワークインスタンス及び前記仮想ネットワークインスタンスが実行される仮想化基盤の情報処理装置から収集

されるネットワーク情報を識別するための識別情報と、前記タグ情報を付加するためのタグ付加条件とが対応付けて格納されるマッピングテーブルを記憶するステップと、前記仮想ネットワークインスタンス及び前記仮想化基盤の情報処理装置から収集されたネットワーク情報を受信するネットワーク情報受信ステップと、前記ネットワーク情報受信ステップで受信したネットワーク情報に対して、前記マッピングテーブルに基づいて前記タグ情報を付加するタグ付加ステップと、を実行させるためのコンピュータプログラムであり、前記マッピング情報は、監視単位毎に、前記タグ情報、前記識別情報、前記タグ付加条件、及び前記タグ付加条件として前記監視対象の仮想ネットワークの構成情報の動的な情報が用いられる場合に前記動的な情報を取得するための付加情報を有し、前記付加情報は、前記動的な情報と前記動的な情報の取得先とを示す情報であり、前記マッピングテーブルは、各監視単位のタグ情報毎に、前記識別情報、前記タグ付加条件、及び前記タグ付加条件に合致した場合に付加されるタグ情報を格納し、前記動的な情報が用いられる前記タグ付加条件は、前記付加情報に基づいて取得された前記動的な情報が前記マッピングテーブルに格納される、コンピュータプログラムである。

【発明の効果】

【００１０】

本発明によれば、ＣＮＦが用いられた仮想ネットワークを対象にしたネットワーク監視に寄与することができるという効果が得られる。

【図面の簡単な説明】

【００１１】

【図１】一実施形態に係るネットワーク監視システムの構成例を示すブロック図である。

【図２】一実施形態に係るデータ収集方法及び仮想ネットワーク監視方法の手順の例を示すシーケンス図である。

【図３】一実施形態に係るマッピングテーブル更新方法の手順の例を示すシーケンス図である。

【図４】一実施形態に係るマッピング情報の具体的な構成例である。

【図５】一実施形態に係るマッピングテーブルの具体的な構成例である。

【図６】一実施形態に係るタグ付け方法の手順の例を示すフローチャートである。

【発明を実施するための形態】

【００１２】

以下、図面を参照し、本発明の実施形態について説明する。

図１は、一実施形態に係るネットワーク監視システム１の構成例を示すブロック図である。図１において、ネットワーク監視システム１は、監視対象の仮想ネットワークからネットワーク情報を収集し、収集したネットワーク情報に基づいて監視対象の仮想ネットワークの状態を分析し、監視対象の仮想ネットワークの状態の分析結果を出力する。

【００１３】

監視対象の仮想ネットワークは、ＣＮＦ（クラウドネイティブネットワーク機能）が用いられた仮想ネットワークであって、複数のＣＮＦ＿４０とＣＮＦオーケストレータ６０とを備える。ＣＮＦ＿４０は、仮想化基盤の情報処理装置である物理サーバ３０上で実行される仮想ネットワークインスタンスとして構築される。ＣＮＦオーケストレータ６０は、監視対象の仮想ネットワークに用いられるＣＮＦ＿４０のオーケストレーションを行う。

【００１４】

ＣＮＦ＿４０及び物理サーバ３０には、監視エージェント５０がインストールされている。監視エージェント５０は、自己がインストールされたＣＮＦ＿４０又は物理サーバ３０に関するネットワーク情報を収集するためのエージェントである。ネットワーク情報は、監視対象の仮想ネットワークの状態の分析に使用される情報であって、例えばネットワークリソースや計算リソース等の仮想ネットワーク性能状態を示す情報である。

【００１５】

ネットワーク監視システム１は、マッピングテーブル生成部１１と、データ収集蓄積部１２と、データ解析部１３とを備える。本実施形態においては、マッピングテーブル生成

部１１とデータ収集蓄積部１２とがデータ収集装置に対応する。
【００１６】
ネットワーク監視システム１の各機能は、ネットワーク監視システム１がＣＰＵ（Central Processing Unit：中央演算処理装置）及びメモリ等のコンピュータハードウェアを備え、ＣＰＵがメモリに格納されたコンピュータプログラムを実行することにより実現される。なお、ネットワーク監視システム１として、汎用のコンピュータ装置を使用して構成してもよく、又は、専用のハードウェア装置として構成してもよい。例えば、ネットワーク監視システム１は、インターネット等の通信ネットワークに接続されるサーバコンピュータを使用して構成されてもよい。また、ネットワーク監視システム１の各機能はクラウドコンピューティングにより実現されてもよい。また、ネットワーク監視システム１は、単独のコンピュータにより実現するものであってもよく、又はネットワーク監視システム１の機能を複数のコンピュータに分散させて実現するものであってもよい。また、ネットワーク監視システム１として、例えばWWWシステム等を利用してウェブサイトを開設するように構成してもよい。
【００１７】
マッピングテーブル生成部１１は、ネットワーク管理者等のユーザが使用するユーザ端末３からマッピング情報を受信する。マッピング情報は、監視対象の仮想ネットワークに対する監視ポリシーを含む情報である。
【００１８】
マッピングテーブル生成部１１は、マッピング情報に含まれる監視ポリシーに基づいて監視対象の仮想ネットワークの構成情報を取得する。監視対象の仮想ネットワークの構成情報は、ＣＮＦオーケストレータ６０や物理サーバ３０から取得される。
【００１９】
マッピングテーブル生成部１１は、マッピング情報に含まれる監視ポリシーとＣＮＦオーケストレータ６０や物理サーバ３０から取得された監視対象の仮想ネットワークの構成情報とに基づいて、マッピングテーブル１１０を生成する。マッピングテーブル１１０は、監視単位毎に設けられたタグ情報と、監視対象の仮想ネットワークのＣＮＦ＿４０及び物理サーバ３０から収集されるネットワーク情報を識別するための識別情報と、タグ情報をネットワーク情報に付加するためのタグ付加条件とが対応付けて格納されたテーブルである。
【００２０】
マッピングテーブル生成部１１は、生成したマッピングテーブル１１０をデータ収集蓄積部１２へ送信する。
【００２１】
またマッピングテーブル生成部１１は、監視対象の仮想ネットワークに対する監視ポリシーと監視対象の仮想ネットワークの構成とのうち少なくとも一方が変更された場合に、最新の監視ポリシーに基づいて、監視対象の仮想ネットワークの構成情報を再取得し、再取得した監視対象の仮想ネットワークの構成情報を使用してマッピングテーブル１１０を更新する。マッピングテーブル生成部１１は、更新したマッピングテーブル１１０をデータ収集蓄積部１２へ送信する。
【００２２】
データ収集蓄積部１２は、コレクタモジュール（コレクタ部）１２１と、マッピングモジュール（マッピング部）１２２と、データストア（データ記憶部）１２３とを備える。
【００２３】
コレクタモジュール１２１は、監視対象の仮想ネットワークのＣＮＦ＿４０及び物理サーバ３０から各監視エージェント５０により収集されたネットワーク情報を、各監視エージェント５０から受信する。
【００２４】
マッピングモジュール１２２は、コレクタモジュール１２１が受信したネットワーク情報に対して、マッピングテーブル１１０に基づいて該当するタグ情報を付加する。

【００２５】
　データストア１２３は、マッピングモジュール１２２によってタグ情報が付加されたネットワーク情報を格納する。データストア１２３に格納されたネットワーク情報は、タグ情報によって監視単位毎に分類される。データ収集蓄積部１２は、データ解析部１３からのデータ要求に応じて、データストア１２３内のタグ付ネットワーク情報をデータ解析部１３へ返信する。
【００２６】
　データ解析部１３は、データ収集蓄積部１２からタグ付ネットワーク情報を取得し、取得したタグ付ネットワーク情報のタグ情報で識別される監視単位毎のネットワーク情報に基づいて、監視単位毎に、監視対象の仮想ネットワークの性能解析を行う。この性能解析は、例えば、所定のアルゴリズムを用いて構築された機械学習モデルである各ＣＮＦ＿４０に対応するＣＮＦモデル１３０が用いられる。また、ＣＮＦモデル１３０に対しては、性能解析のための所定のデータ前処理が施されたネットワーク情報が使用される。
　なお、データ解析部１３が解析に用いる手法は機械学習に限定されず、その他のアルゴリズム等による解析手法が適用されてもよい。
【００２７】
　データ解析部１３は、監視対象の仮想ネットワークの監視単位毎の性能解析結果をユーザ端末３へ送信する。これにより、ネットワーク管理者等のユーザは、ユーザ端末３が受信した性能解析結果によって、監視対象の仮想ネットワークについて監視単位毎に性能状態を認識することができる。
【００２８】
　次に図２を参照して本実施形態に係るデータ収集方法及び仮想ネットワーク監視方法を説明する。図２は、本実施形態に係るデータ収集方法及び仮想ネットワーク監視方法の手順の例を示すシーケンス図である。
【００２９】
（ステップＳ１）　ネットワーク管理者は、ユーザ端末３を使用して、マッピングテーブル生成部１１へマッピング情報を入力する。当該入力されたマッピング情報（入力マッピング情報）には、監視単位毎にネットワーク情報を分類して監視単位毎のタグ情報を付加するための情報（監視ポリシー）が含められる。
【００３０】
（ステップＳ２）　マッピングテーブル生成部１１は、入力マッピング情報に基づいて、ＣＮＦオーケストレータ６０に対して、監視対象の仮想ネットワークの構成情報（監視対象仮想ネットワーク構成情報）のうち必要な監視対象仮想ネットワーク構成情報を要求する。
【００３１】
（ステップＳ３）　ＣＮＦオーケストレータ６０は、マッピングテーブル生成部１１からの要求に応じて、要求された監視対象仮想ネットワーク構成情報をマッピングテーブル生成部１１へ返信する。
【００３２】
（ステップＳ４）　マッピングテーブル生成部１１は、入力マッピング情報に基づいて、物理サーバ３０に対して、必要な監視対象仮想ネットワーク構成情報を要求する。
【００３３】
（ステップＳ５）　物理サーバ３０は、マッピングテーブル生成部１１からの要求に応じて、要求された監視対象仮想ネットワーク構成情報をマッピングテーブル生成部１１へ返信する。
【００３４】
（ステップＳ６）　マッピングテーブル生成部１１は、入力マッピング情報とＣＮＦオーケストレータ６０や物理サーバ３０から取得された監視対象仮想ネットワーク構成情報とに基づいて、マッピングテーブル１１０を生成する。
【００３５】

（ステップＳ７）　マッピングテーブル生成部１１は、生成したマッピングテーブル１１０（テーブル情報）をマッピングモジュール１２２へ送信する。

【００３６】

（ステップＳ８）　マッピングモジュール１２２は、マッピングテーブル生成部１１から受信したマッピングテーブル１１０（テーブル情報）をメモリに読み込み保持する。

【００３７】

上記のステップＳ１からステップＳ８によって、マッピングテーブル１１０が生成されマッピングモジュール１２２に設定される。次いで、データ収集段階として以降のステップが実行される。

【００３８】

（ステップＳ９）　物理サーバ３０に事前にインストールされた監視エージェント５０は、定期的に物理サーバ３０からネットワーク情報を収集し、収集したネットワーク情報をコレクタモジュール１２１へ送信する。

【００３９】

（ステップＳ１０）　監視対象の仮想ネットワークのＣＮＦ＿４０に事前にインストールされた監視エージェント５０は、定期的にＣＮＦ＿４０からネットワーク情報を収集し、収集したネットワーク情報をコレクタモジュール１２１へ送信する。

【００４０】

（ステップＳ１１）　コレクタモジュール１２１は、監視対象の仮想ネットワークのＣＮＦ＿４０及び物理サーバ３０の各監視エージェント５０から受信したネットワーク情報を、マッピングモジュール１２２へ転送する。

【００４１】

（ステップＳ１２）　マッピングモジュール１２２は、コレクタモジュール１２１から受信したネットワーク情報に対して、マッピングテーブル１１０に基づいて該当するタグ情報を付加する。

【００４２】

（ステップＳ１３）　データストア１２３は、マッピングモジュール１２２によってタグ情報が付加されたタグ付ネットワーク情報を格納する。

【００４３】

上記のステップＳ９からステップＳ１３によって、タグ情報によって監視単位毎に分類されるネットワーク情報（タグ付ネットワーク情報）がデータストア１２３に蓄積される。次いで、データ解析段階として以降のステップが実行される。

【００４４】

（ステップＳ１４）　データ解析部１３は、データストア１２３に対して、データ解析の対象のタグ付ネットワーク情報を要求する。例えば、データ解析部１３は、データ解析の対象の監視単位に対応するタグ付ネットワーク情報をデータストア１２３に要求する。例えば、データ解析部１３は、データ解析の対象の監視日時に収集されたタグ付ネットワーク情報をデータストア１２３に要求する。ネットワーク情報は、収集された日時を含んでいる。

【００４５】

（ステップＳ１５）　データストア１２３は、データ解析部１３からの要求に応じて、要求されたタグ付ネットワーク情報をデータ解析部１３へ返信する。

【００４６】

（ステップＳ１６）　データ解析部１３は、事前に構築された機械学習モデルであるＣＮＦモデル１３０を用いて、データストア１２３から取得したタグ付ネットワーク情報を解析する。

【００４７】

（ステップＳ１７）　データ解析部１３は、解析結果をネットワーク管理者のユーザ端末３へ送信する。

【００４８】

次に図３を参照して本実施形態に係るマッピングテーブル更新方法を説明する。図３は、本実施形態に係るマッピングテーブル更新方法の手順の例を示すシーケンス図である。

【００４９】

（ステップＳ３１）　ネットワーク管理者は、監視対象の仮想ネットワークに対する監視ポリシーを変更する場合、ユーザ端末３を使用して、マッピングテーブル生成部１１へ、変更後のマッピング情報を入力する。当該入力された変更後のマッピング情報（入力マッピング情報＿変更後）には、変更後の監視ポリシーが含められる。

【００５０】

（ステップＳ３２）　ＣＮＦオーケストレータ６０は、オートスケール等により監視対象の仮想ネットワークの構成が変わった場合、マッピングテーブル生成部１１に対して、監視対象の仮想ネットワークの構成の変更を通知する。

【００５１】

（ステップＳ３３）　マッピングテーブル生成部１１は、入力マッピング情報の変更ありの場合、入力マッピング情報＿変更後に基づいて、ＣＮＦオーケストレータ６０に対して、必要な監視対象仮想ネットワーク構成情報を要求する。

【００５２】

マッピングテーブル生成部１１は、入力マッピング情報の変更なし且つ監視対象の仮想ネットワークの構成の変更ありの場合、入力マッピング情報に基づいて、ＣＮＦオーケストレータ６０に対して、必要な監視対象仮想ネットワーク構成情報を要求する。

【００５３】

マッピングテーブル生成部１１は、入力マッピング情報の変更あり且つ監視対象の仮想ネットワークの構成の変更ありの場合、入力マッピング情報＿変更後に基づいて、ＣＮＦオーケストレータ６０に対して、必要な監視対象仮想ネットワーク構成情報を要求する。

【００５４】

（ステップＳ３４）　ＣＮＦオーケストレータ６０は、マッピングテーブル生成部１１からの要求に応じて、要求された監視対象仮想ネットワーク構成情報をマッピングテーブル生成部１１へ返信する。

【００５５】

（ステップＳ３５）　マッピングテーブル生成部１１は、入力マッピング情報の変更ありの場合、入力マッピング情報＿変更後に基づいて、物理サーバ３０に対して、必要な監視対象仮想ネットワーク構成情報を要求する。

【００５６】

マッピングテーブル生成部１１は、入力マッピング情報の変更なし且つ監視対象の仮想ネットワークの構成の変更ありの場合、入力マッピング情報に基づいて、物理サーバ３０に対して、必要な監視対象仮想ネットワーク構成情報を要求する。

【００５７】

マッピングテーブル生成部１１は、入力マッピング情報の変更あり且つ監視対象の仮想ネットワークの構成の変更ありの場合、入力マッピング情報＿変更後に基づいて、物理サーバ３０に対して、必要な監視対象仮想ネットワーク構成情報を要求する。

【００５８】

（ステップＳ３６）　物理サーバ３０は、マッピングテーブル生成部１１からの要求に応じて、要求された監視対象仮想ネットワーク構成情報をマッピングテーブル生成部１１へ返信する。

【００５９】

（ステップＳ３７）　マッピングテーブル生成部１１は、入力マッピング情報の変更ありの場合、入力マッピング情報＿変更後とＣＮＦオーケストレータ６０や物理サーバ３０から取得された監視対象仮想ネットワーク構成情報とに基づいて、マッピングテーブル１１０を更新する。

【００６０】

（ステップＳ３８）　マッピングテーブル生成部１１は、更新後のマッピングテーブル１

１０（テーブル情報）をマッピングモジュール１２２へ送信する。
【００６１】
（ステップＳ３９）　マッピングモジュール１２２は、マッピングテーブル生成部１１から受信した更新後のマッピングテーブル１１０（テーブル情報）をメモリに再読み込みし元のマッピングテーブル１１０に上書きし保持する。これにより、マッピングテーブル１１０が更新されマッピングモジュール１２２に設定される。
【００６２】
図４は、本実施形態に係るマッピング情報の具体的な構成例である。図４の例では、監視単位毎に、監視単位名、識別情報、条件及び付加情報が関連付けてマッピング情報に格納される。識別情報は、ネットワーク情報を識別するための識別情報である。条件は、タグ情報を付加するためのタグ付加条件である。付加情報は、条件として動的な情報が用いられる場合に、当該動的な情報（監視対象仮想ネットワーク構成情報）を取得するための情報である。マッピングテーブル生成部１１は、条件として動的な情報が用いられる場合に、付加情報に示される監視対象仮想ネットワーク構成情報を、付加情報に示される取得先（物理サーバ３０又はＣＮＦオーケストレータ６０）から取得する。
【００６３】
図４の例では、pidns（ＰＩＤ名前空間）と「TCP source IP address（ＴＣＰ送信元ＩＰアドレス）」とが識別情報に使用されている。pidnsについては、付加情報に基づいて物理サーバ３０から取得される動的な情報（監視対象仮想ネットワーク構成情報）が条件（タグ付加条件）として使用される。「TCP source IP address」については、ネットワーク管理者がマッピング情報として入力した値（静的情報）が条件（タグ付加条件）として使用される。
【００６４】
図５は、本実施形態に係るマッピングテーブル１１０の具体的な構成例である。図５の例は、図４のマッピング情報の例に基づいて生成されたものである。図５の例では、各監視単位のタグ情報毎に、識別情報、条件（タグ付加条件）及び条件（タグ付加条件）に合致した場合に付加されるタグ情報が対応付けてマッピングテーブル１１０に格納される。
【００６５】
pidnsに関連付けられる条件（タグ付加条件）は、マッピング情報の付加情報に基づいて物理サーバ３０から取得された動的な情報（監視対象仮想ネットワーク構成情報）がマッピングテーブル１１０に格納される。「TCP source IP address」に関連付けられる条件（タグ付加条件）は、ネットワーク管理者がマッピング情報として入力した値（静的情報）がマッピングテーブル１１０に格納される。
【００６６】
マッピングモジュール１２２は、図５のマッピングテーブル１１０を使用し、コレクタモジュール１２１が受信したネットワーク情報において、例えば、識別情報「pidns」が条件（タグ付加条件）「4026533925」に合致した場合に、当該ネットワーク情報に対してタグ情報「amf」を付加する。また、マッピングモジュール１２２は、図５のマッピングテーブル１１０を使用し、コレクタモジュール１２１が受信したネットワーク情報において、例えば、識別情報「TCP source IP address」が条件（タグ付加条件）「192.168.13.81」に合致した場合に、当該ネットワーク情報に対してタグ情報「smf」を付加する。
【００６７】
図６は、本実施形態に係るタグ付け方法の手順の例を示すフローチャートである。図６のフローチャートは、図５のマッピングテーブル１１０に対応する。
【００６８】
（ステップＳ１０１）　マッピングモジュール１２２は、コレクタモジュール１２１からネットワーク情報（収集データ）を受信する。
【００６９】
（ステップＳ１０２）　マッピングモジュール１２２は、マッピングテーブル１１０に基

づいて、コレクタモジュール１２１から受信したネットワーク情報に識別情報「pidns」が含まれているか否かを判断する。識別情報「pidns」が含まれている場合にはステップＳ１０３に進み、そうではない場合にはステップＳ１０５に進む。

【００７０】

（ステップＳ１０３）　マッピングモジュール１２２は、ネットワーク情報に含まれている識別情報「pidns」が、マッピングテーブル１１０内の識別情報「pidns」の条件に合致するか否かを判断する。条件に合致する場合にはステップＳ１０４に進み、そうではない場合にはステップＳ１０５に進む。

【００７１】

（ステップＳ１０４）　マッピングモジュール１２２は、ネットワーク情報に対して、合致した識別情報「pidns」の条件に該当するマッピングテーブル１１０内のタグ情報を付加する。

【００７２】

（ステップＳ１０５）　マッピングモジュール１２２は、マッピングテーブル１１０に基づいて、コレクタモジュール１２１から受信したネットワーク情報に識別情報「TCP source IP address」が含まれているか否かを判断する。識別情報「TCP source IP address」が含まれている場合にはステップＳ１０６に進み、そうではない場合には図６の処理を終了する。

【００７３】

（ステップＳ１０６）　マッピングモジュール１２２は、ネットワーク情報に含まれている識別情報「TCP source IP address」が、マッピングテーブル１１０内の識別情報「TCP source IP address」の条件に合致するか否かを判断する。条件に合致する場合にはステップＳ１０７に進み、そうではない場合には図６の処理を終了する。

【００７４】

（ステップＳ１０７）　マッピングモジュール１２２は、ネットワーク情報に対して、合致した識別情報「TCP source IP address」の条件に該当するマッピングテーブル１１０内のタグ情報を付加する。

【００７５】

本実施形態によれば、ＣＮＦが用いられた仮想ネットワークを対象にしたネットワーク監視に寄与することができるという効果が得られる。

【００７６】

また、仮想ネットワークの監視において、ＣＮＦ等の仮想ネットワークインスタンス及びその仮想化基盤から収集されるネットワーク情報に対してマッピングテーブルを用いて監視単位毎のタグ情報を付加し、タグ付ネットワーク情報を蓄積することによって、任意の監視単位毎に監視対象の仮想ネットワークの性能情報を集約して解析することができる。

【００７７】

また、監視対象の仮想ネットワークに対する監視ポリシーや監視対象の仮想ネットワークの構成が変わった場合に、その変更の通知に応じてマッピングテーブルを更新することによって、監視対象の仮想ネットワークに関する環境の変化に追従しながら、任意の監視単位毎での監視対象の仮想ネットワークの監視を継続することができる。

【００７８】

なお、これにより、例えばネットワーク監視システムにおける総合的なサービス品質の向上を実現することができることから、国連が主導する持続可能な開発目標（SDGs）の目標９「レジリエントなインフラを整備し、持続可能な産業化を推進するとともに、イノベーションの拡大を図る」に貢献することが可能となる。

【００７９】

以上、本発明の実施形態について図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、本発明の要旨を逸脱しない範囲の設計変更等も含まれる。

【００８０】

また、上述した各装置の機能を実現するためのコンピュータプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行するようにしてもよい。なお、ここでいう「コンピュータシステム」とは、ＯＳや周辺機器等のハードウェアを含むものであってもよい。また、「コンピュータシステム」は、WWWシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。

また、「コンピュータ読み取り可能な記録媒体」とは、フレキシブルディスク、光磁気ディスク、ＲＯＭ、フラッシュメモリ等の書き込み可能な不揮発性メモリ、ＤＶＤ（Digital Versatile Disc）等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。

【００８１】

さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通信回線を介してプログラムが送信された場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリ（例えばＤＲＡＭ（Dynamic Random Access Memory））のように、一定時間プログラムを保持しているものも含むものとする。

また、上記プログラムは、このプログラムを記憶装置等に格納したコンピュータシステムから、伝送媒体を介して、あるいは、伝送媒体中の伝送波により他のコンピュータシステムに伝送されてもよい。ここで、プログラムを伝送する「伝送媒体」は、インターネット等のネットワーク（通信網）や電話回線等の通信回線（通信線）のように情報を伝送する機能を有する媒体のことをいう。

また、上記プログラムは、前述した機能の一部を実現するためのものであってもよい。さらに、前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であってもよい。

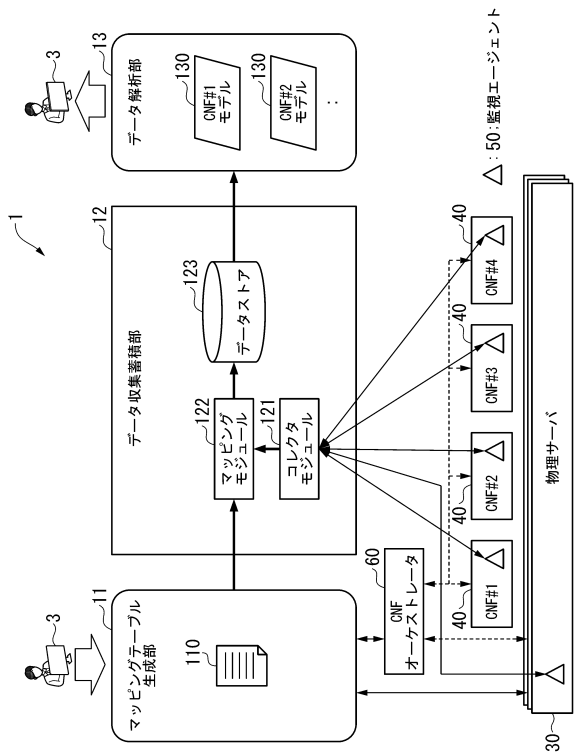
【符号の説明】

【００８２】

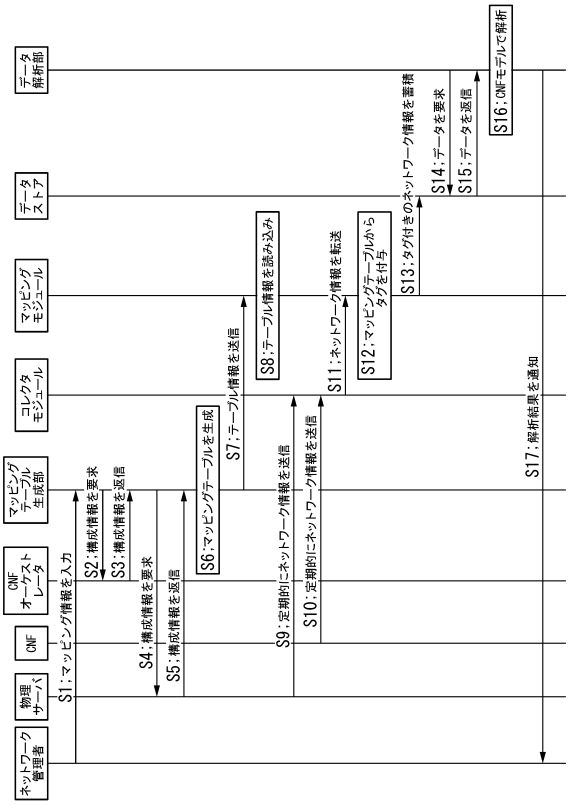
１…ネットワーク監視システム、３…ユーザ端末、１１…マッピングテーブル生成部、１２…データ収集蓄積部、１３…データ解析部、３０…物理サーバ、４０…ＣＮＦ、５０…監視エージェント、６０…ＣＮＦオーケストレータ、１１０…マッピングテーブル、１２１…コレクタモジュール、１２２…マッピングモジュール、１２３…データストア、１３０…ＣＮＦモデル

【図面】

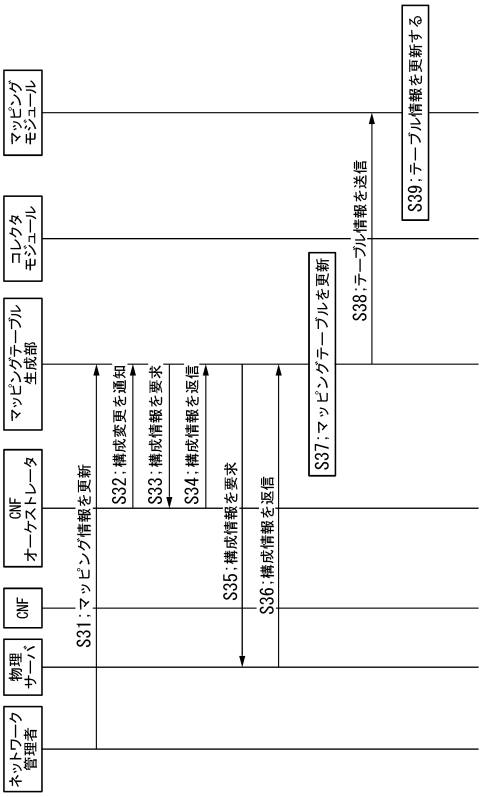
【図１】



【図２】



【図３】



【図４】

マッピング情報の構成例

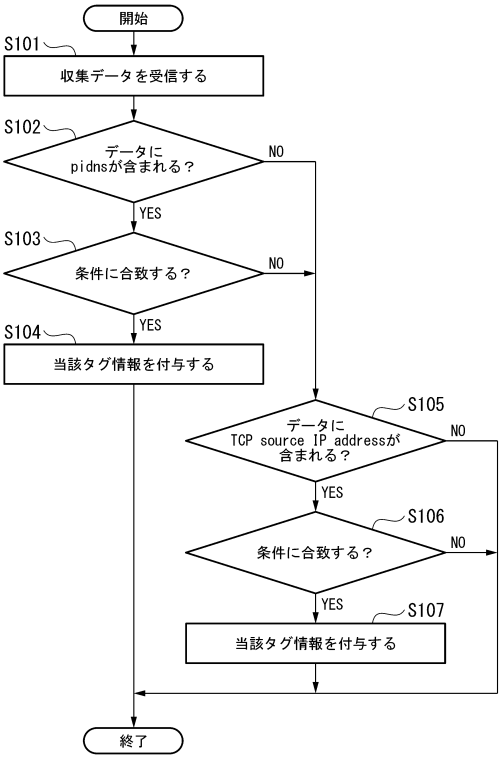
監視単位	識別情報	条件	付加情報
AMF	pidns	== pidns_a	pid=`sudo docker ps -q | xargs sudo docker inspect --format '{{.State.Pid}} {{.Name}}' | grep amf' pidns_a=' sudo ls -l /proc/$pid/ns/pid_for_children'
AMF	TCP source IP address	=="192.168.13.80"	
SMF	pidns	== pidns_s	pid=`sudo docker ps -q | xargs sudo docker inspect --format '{{.State.Pid}} {{.Name}}' | grep smf' pidns_s=' sudo ls -l /proc/$pid/ns/pid_for_children'
SMF	TCP source IP address	=="192.168.13.81"	
UPF	pidns	== pidns_u	pid=`sudo docker ps -q | xargs sudo docker inspect --format '{{.State.Pid}} {{.Name}}' | grep upf' pidns_u=' sudo ls -l /proc/$pid/ns/pid_for_children'

【図５】

マッピングテーブルの構成例

識別情報	条件	タグ
pidns	==4026533925	amf
pidns	==4026534744	smf
pidns	==4026534002	upf
TCP source IP address	= “192.168.13.80”	amf
TCP source IP address	= “192.168.13.81”	smf

【図６】



フロントページの続き

(56)参考文献 特開２０２１－１４１４８１（ＪＰ，Ａ）
特開２００２－０４４１２５（ＪＰ，Ａ）
米国特許出願公開第２０２１／０３２０８７８（ＵＳ，Ａ１）
国際公開第２０１６／１１７６９７（WO，Ａ１）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ １２／００－１２／６６
Ｈ０４Ｌ ４１／００－６９／４０