(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7310885号
(P7310885)

(45)発行日　令和5年7月19日(2023.7.19)

(24)登録日　令和5年7月10日(2023.7.10)

(51)国際特許分類
Ｇ０６Ｆ　9/455(2018.01)

ＦＩ
Ｇ０６Ｆ　9/455　１５０

請求項の数　9　（全17頁）

(21)出願番号　特願2021-521575(P2021-521575)
(86)(22)出願日　令和1年5月27日(2019.5.27)
(86)国際出願番号　PCT/JP2019/020820
(87)国際公開番号　WO2020/240642
(87)国際公開日　令和2年12月3日(2020.12.3)
審査請求日　令和3年11月11日(2021.11.11)

(73)特許権者　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100103894
弁理士　家入 健
(72)発明者　羽角 太地
東京都港区芝五丁目７番１号 日本電気株式会社内
(72)発明者　池田 聡
東京都港区芝五丁目７番１号 日本電気株式会社内
審査官　坂東 博司

最終頁に続く

(54)【発明の名称】　仮想マシン制御システム、仮想マシン制御方法、及び、制御プログラム

(57)【特許請求の範囲】
【請求項１】
複数の仮想マシンホストと、
前記複数の仮想マシンホストとネットワークを介して接続された仮想マシン制御装置と、
前記複数の仮想マシンホストに分散して配置された属性情報の類似する仮想マシン間の通信ログをインシデント調査に必要な情報として収集する通信履歴記録装置と、
を備え、
前記仮想マシン制御装置は、
複数の仮想マシンの属性情報を受信する通信端末情報受信手段と、
前記通信端末情報受信手段によって受信された前記複数の仮想マシンの属性情報の類似度を判定する類似度判定手段と、
前記類似度判定手段により属性情報が類似していると判定された複数の前記仮想マシンを少なくとも２つ以上の仮想マシンホストに分散して配置する端末配置手段と、
を備えた、仮想マシン制御システム。
【請求項２】
前記類似度判定手段は、
前記通信端末情報受信手段によって受信された前記複数の仮想マシンの属性情報を、距離を表すデータ構造の特徴ベクトルに変換するデータ変換手段と、
前記データ変換手段から出力された複数の前記特徴ベクトルに基づいて、前記複数の仮想マシンを一又は複数のクラスタに分類するクラスタ計算手段と、

を有し、
前記端末配置手段は、前記クラスタ毎に、そのクラスタに含まれる前記仮想マシンを前記仮想マシンホストに配置するとともに、そのクラスタに２つ以上の前記仮想マシンが含まれる場合、当該クラスタに含まれる前記２つ以上の仮想マシンを少なくとも２つ以上の前記仮想マシンホストに分散して配置するように構成されている、
請求項１に記載の仮想マシン制御システム。
【請求項３】
前記端末配置手段は、同一の前記クラスタに２つ以上の前記仮想マシンが含まれる場合、当該クラスタに含まれる前記２つ以上の仮想マシンを、前記２つ以上の仮想マシンホストの各々に配置される仮想マシンの数が最小となるように、当該２つ以上の仮想マシンホストに分散して配置するように構成されている、
請求項２に記載の仮想マシン制御システム。
【請求項４】
前記端末配置手段は、同一の前記クラスタに２つ以上の前記仮想マシンが含まれる場合、当該クラスタに含まれる前記２つ以上の仮想マシンを、前記２つ以上の仮想マシンホストのそれぞれに均等に振り分けて配置するように構成されている、
請求項２に記載の仮想マシン制御システム。
【請求項５】
前記端末配置手段は、同一の前記クラスタに２つ以上の前記仮想マシンが含まれる場合、さらに、当該クラスタに含まれる前記２つ以上の仮想マシンのそれぞれについて、仮想マシンホストに要求する配置要件及びネットワーク要件を満たすように、前記２つ以上の仮想マシンホストに分散して配置するように構成されている、
請求項２～４の何れか一項に記載の仮想マシン制御システム。
【請求項６】
複数の仮想マシンホストと、
前記複数の仮想マシンホストとネットワークを介して接続された仮想マシン制御装置と、
前記複数の仮想マシンホストに分散して配置された属性情報の類似する仮想マシン間の通信ログをインシデント調査に必要な情報として収集する通信履歴記録装置と、
を備えた仮想マシン制御システムにおける前記仮想マシン制御装置による仮想マシン制御方法であって、
複数の仮想マシンの属性情報を受信するステップと、
受信した前記複数の仮想マシンの属性情報の類似度を判定するステップと、
属性情報が類似していると判定された複数の前記仮想マシンを少なくとも２つ以上の仮想マシンホストに分散して配置するステップと、
を備えた、仮想マシン制御方法。
【請求項７】
受信した前記複数の仮想マシンの属性情報の類似度を判定するステップは、
受信した前記複数の仮想マシンの属性情報を、距離を表すデータ構造の特徴ベクトルに変換するステップと、
複数の前記特徴ベクトルに基づいて、前記複数の仮想マシンを一又は複数のクラスタに分類するステップと、
を有し、
属性情報が類似していると判定された複数の前記仮想マシンを少なくとも２つ以上の仮想マシンホストに分散して配置するステップでは、
前記クラスタ毎に、そのクラスタに含まれる前記仮想マシンを前記仮想マシンホストに配置するとともに、そのクラスタに２つ以上の前記仮想マシンが含まれる場合、当該クラスタに含まれる前記２つ以上の仮想マシンを少なくとも２つ以上の前記仮想マシンホストに分散して配置する、
請求項６に記載の仮想マシン制御方法。
【請求項８】

複数の仮想マシンホストと、
前記複数の仮想マシンホストとネットワークを介して接続された仮想マシン制御装置と、
前記複数の仮想マシンホストに分散して配置された属性情報の類似する仮想マシン間の通信ログをインシデント調査に必要な情報として収集する通信履歴記録装置と、
を備えた仮想マシン制御システムにおける前記仮想マシン制御装置の制御処理をコンピュータに実行させる制御プログラムであって、
複数の仮想マシンの属性情報を受信する処理と、
受信した前記複数の仮想マシンの属性情報の類似度を判定する処理と、
属性情報が類似していると判定された複数の前記仮想マシンを少なくとも２つ以上の仮想マシンホストに分散して配置する処理と、
をコンピュータに実行させる制御プログラム。
【請求項９】
受信した前記複数の仮想マシンの属性情報の類似度を判定する処理は、
受信した前記複数の仮想マシンの属性情報を、距離を表すデータ構造の特徴ベクトルに変換する処理と、
複数の前記特徴ベクトルに基づいて、前記複数の仮想マシンを一又は複数のクラスタに分類する処理と、
を有し、
属性情報が類似していると判定された複数の前記仮想マシンを少なくとも２つ以上の仮想マシンホストに分散して配置する処理では、
前記クラスタ毎に、そのクラスタに含まれる前記仮想マシンを前記仮想マシンホストに配置するとともに、そのクラスタに２つ以上の前記仮想マシンが含まれる場合、当該クラスタに含まれる前記２つ以上の仮想マシンを少なくとも２つ以上の前記仮想マシンホストに分散して配置する、
請求項８に記載の制御プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、仮想マシン制御装置、仮想マシン制御システム、仮想マシン制御方法、及び、プログラムが格納された非一時的なコンピュータ可読媒体に関する。
【背景技術】
【０００２】
近年のサイバー攻撃の増加に伴い、組織における情報セキュリティ対策が増々重要になってきている。情報セキュリティ上、脅威となる可能性がある事象をインシデントと言い、インシデントの発生に備えるインシデントマネジメントについての検討が進められている（非特許文献１参照）。特にインシデントの発生後の対策（インシデント対応）が重要である（例えば、非特許文献２及び非特許文献３参照）。
【０００３】
インシデント発生後のオペレーションとしては、ネットワークシステムを構成する情報機器等に記録された情報ログや通信ネットワークのログを根拠とした、事実解明調査（インシデント調査）を行うことが必須である。そのため、基幹システムを始めとした各種システムにおける、情報ログの収集指針、情報ログを収集する仕組みなど、情報ログの管理などについての重要性が再認識されている。
【０００４】
特に被害の大きいサイバー攻撃の一種である標的型攻撃は、標的のネットワーク内部において攻撃者が端末間を移動し、被害を拡大させてゆくことから、内部ネットワークの端末間通信ログを収集することが肝要である。一般的に、端末間通信ログは端末間のネットワークに流れるパケットをキャプチャするか、端末内にインストールされたソフトウェアより収集される。
【０００５】

さらにクラウド関連技術の発展や、機動性・耐障害性・価格面などのメリットから、クラウドに配置したシンクライアント等の仮想端末型サービスなどを導入する組織が増加している（例えば非特許文献４参照）。そのため、クラウド環境下における、インシデント調査を目的としたログの収集も重要となってきている。

【０００６】

しかしながら、クラウド環境下に存在する端末の利用者が、サイバー攻撃に起因するインシデント調査を目的として、クラウド内端末間通信ログを収集しようとする場合、上記に示した端末間通信ログ収集方法では困難が生じる。

【０００７】

即ち、同一の仮想マシンホストに配置された複数の仮想マシン間の内部通信の収集に関し、同仮想マシンホスト内から継続的に収集したり、仮想マシン内部において継続的に収集したりすることは、メモリ入出力（ＩＯ）やディスクＩＯに負荷をかける。これは、仮想マシンホストに格納された全ての仮想マシンのパフォーマンスの劣化を引き起こしてしまう。なお、仮想マシンホストとは、所謂、物理マシンのことである。

【０００８】

一方、クラウド内端末間通信ログを収集するため、仮想マシンホスト外部に通信ログを収集する装置を設置する方法（通常監視方法）も考えられる。この方法では、仮想マシンホスト内の仮想マシンと、当該仮想マシンホスト外部（外部のネットワーク、他の仮想マシンホスト、又は、その他の通信装置）と、の間の通信ログの収集は可能である。しかしながら、この方法では、同一仮想マシンホストに配置された複数の仮想マシン間の通信ログを収集することができないという問題がある。

【０００９】

特に標的型攻撃では、例えば同じ部署に属する複数のマシンが攻撃を受けることが考えられる。つまり、標的型攻撃では、例えば最初に攻撃を受けたマシンの属性情報に類似する属性情報を持つ他のマシンが続けて攻撃を受けることが考えられる。なお、属性情報とは、例えば、マシンのスペック、又は、マシンを使用する単一又は複数の使用者（ユーザ）の、区別可能な任意の性質を指す。属性情報は、例えば、マシン上で稼働するＯＳ（Ｏｐｅｒａｔｉｏｎ　Ｓｙｓｔｅｍ）、アプリケーションの種類又は名称、又は、そのマシンを使用するユーザの所属する部署や職位などを含む。

【００１０】

そのため、仮に、同一仮想マシンホストに格納された複数の仮想マシン間においてインシデントに関連する通信が発生した場合、上記した通常監視方法では、端末間通信ログをネットワークログとして収集できない可能性がある。これは、インシデント調査において証拠となる端末間通信ログに抜けが生じることを意味する。

【００１１】

ここで、仮想マシンホスト外部からインシデント調査に必要な端末間通信ログを収集できるかどうかは、各仮想マシンをどの仮想マシンホストに配置するかという、仮想マシンの管理方法に依存している。

【００１２】

クラウド環境下における、仮想マシンの管理に関連する技術として、例えば、特許文献１及び特許文献２が知られている。特許文献１には、複数の仮想マシンが格納された物理マシン間の通信の許可情報及びネットワーク距離を用いて、ある物理マシンで新たに仮想マシンを稼働させた場合のネットワークコストを計算することが開示されている。この計算結果により、ネットワークシステム全体のコストを最小化させることができる。また、特許文献２には、利用者の要求する仮想マシンの水準と、物理マシンの属性と、に基づいて仮想マシンを配置する方法が開示されている。

【先行技術文献】

【特許文献】

【００１３】

【文献】特許５３７７７７５号公報

特開２０１３－３９４６号公報
【非特許文献】
【００１４】
【文献】一般社団法人ＪＰＣＥＲＴコーディネーションセンター、“ＣＳＩＲＴガイド”、インターネット〈URL:https://www.jpcert.or.jp/csirt_material/files/guide_ver1.0_20151126.pdf〉
Ponemon Institute、“Ponemon Institute's 2017 Cost of Data Breach Study: Global Overview”、インターネット〈URL:https://www-01.ibm.com/marketing/iwm/dre/signup?source=urx-15763〉
独立行政法人情報処理推進機構、“サイバーレスキュー隊（Ｊ－ＣＲＡＴ）分析レポート２０１５、特定業界を執拗に狙う攻撃キャンペーンの分析”、インターネット〈URL:https://www.ipa.go.jp/files/000053445.pdf〉
ＩＤＣ　Ｊａｐａｎ、“国内クライアント仮想化関連市場予測を発表”、インターネット〈URL:https://www.idcjapan.co.jp/Press/Current/201806251Apr.html〉
Ward, J. H., Jr.、“ハイラキカルグルーピングトゥオプティマイズアンオブジェクティブファンクション（Hierarchical Grouping to Optimize an Objective Function）”、Journal of the American Statistical Association, 58, p.236-244.
【発明の概要】
【発明が解決しようとする課題】
【００１５】
しかしながら、関連技術には、クラウドシステム全体のネットワーク負荷削減、又は、利用者の要求する仮想マシンの要件を満足する仮想マシンの最適配置について開示されているに過ぎない。つまり、関連技術には、クラウド環境下において、インシデント調査に必要な属性情報の類似する仮想マシン間の通信ログをいかにして容易に収集するのかについては開示されていない。そのため、関連技術では、セキュリティ性能を十分に向上させることができないという課題があった。
【００１６】
例えば、特許文献１に開示された方式では、システム全体のネットワーク負荷を軽減するため、ある仮想マシンと、当該ある仮想マシンと通信を行う別の仮想マシンとは、同じ仮想マシンホスト上に配置される。そのため、ある仮想マシンと通信が行われる他の複数の仮想マシンは、何れも当該ある仮想マシンと同じ仮想マシンホストに固まって配置されることになる。ここで、同一仮想マシンホストに固まって配置された複数の仮想マシンの属性情報は、類似している可能性が高い。例えば、あるサーバに接続を行う端末（仮想マシン）群は、同じ職務や部署に属していることなどが考えられる。そのため、特許文献１に開示された方式では、クラウド環境下において、インシデント調査に必要な属性情報の類似する仮想マシン間の通信ログを収集することが困難であり、その結果、セキュリティ性能を十分に向上させることができない。
【００１７】
また、特許文献２に開示された方式では、各仮想マシンが、その仮想マシンの要求水準を満たす仮想マシンホストに配置される。そのため、同様の要求水準を要求する複数の仮想マシンは、同じ仮想マシンホストに固まって配置されることになる。ここで、同様の要求水準を要求する仮想マシンの属性情報は、使用者の職務、職位、部署等において類似している可能性が高い。そのため、特許文献２に開示された方式では、クラウド環境下において、インシデント調査に必要な属性情報の類似する仮想マシン間の通信ログを収集することが困難であり、その結果、セキュリティ性能を十分に向上させることができない。
【００１８】
本開示の目的は、このような課題を解決するためになされたものである。即ち、本開示の目的は、セキュリティ性能を向上させることが可能な仮想マシン制御装置、仮想マシン制御システム、仮想マシン制御方法、及び、プログラムが格納された非一時的なコンピュータ可読媒体を提供することである。

【課題を解決するための手段】
【００１９】
本開示にかかる仮想マシン装置は、複数の仮想マシンの属性情報を受信する通信端末情報受信手段と、前記通信端末情報受信手段によって受信された前記複数の仮想マシンの属性情報の類似度を判定する類似度判定手段と、前記類似度判定手段により属性情報が類似していると判定された複数の前記仮想マシンを少なくとも２つ以上の仮想マシンホストに分散して配置する端末配置手段と、を備える。
【００２０】
また、本開示にかかる仮想マシン制御方法は、複数の仮想マシンの属性情報を受信するステップと、受信した前記複数の仮想マシンの属性情報の類似度を判定するステップと、属性情報が類似していると判定された複数の前記仮想マシンを少なくとも２つ以上の仮想マシンホストに分散して配置するステップと、を備える。
【００２１】
さらに、本開示にかかる非一時的なコンピュータ可読媒体は、複数の仮想マシンの属性情報を受信する処理と、受信した前記複数の仮想マシンの属性情報の類似度を判定する処理と、属性情報が類似していると判定された複数の前記仮想マシンを少なくとも２つ以上の仮想マシンホストに分散して配置する処理と、をコンピュータに実行させるプログラムが格納される。
【発明の効果】
【００２２】
本開示によれば、セキュリティ性能を向上させることが可能な仮想マシン制御装置、仮想マシン制御システム、仮想マシン制御方法、及び、プログラムが格納された非一時的なコンピュータ可読媒体を提供することができる。
【図面の簡単な説明】
【００２３】
【図１】実施の形態１にかかる仮想マシン制御システムの構成例を示すブロック図である。
【図２】図１に示す仮想マシン制御システムに設けられた仮想マシン制御装置の概要を示すブロック図である。
【図３】図１に示す仮想マシン制御システムに設けられた仮想マシン制御装置の具体的な構成例を示すブロック図である。
【図４】図３に示す仮想マシン制御装置に設けられた通信端末情報受信部によって受信された各仮想マシンの属性情報の具体例を示す図である。
【図５】図３に示す仮想マシン制御装置に設けられたホスト要件記憶部に記憶されている各仮想マシンホストの属性情報の具体例を示す図である。
【図６】図３に示す仮想マシン制御装置に設けられたデータ変換部において算出された各仮想マシンの特徴ベクトルの具体例を示す図である。
【図７】各仮想マシンと、各仮想マシンが配置される仮想マシンホストと、の関係を示す図である。
【図８】図３に示す仮想マシン制御装置の動作を示すフローチャートである。
【図９】図３に示す仮想マシン制御装置に設けられたクラスタ計算部によるクラスタリングの経過を可視化したデンドログラムである。
【図１０】図３に示す仮想マシン制御装置による各仮想マシンの配置先の決定方法の詳細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】
【００２４】
以下、図面を参照して、本開示の実施の形態について説明する。各図面において、同一又は対応する要素には同一の符号が付されており、説明の明確化のため、必要に応じて重複する説明を省略する。
【００２５】
＜実施の形態１＞

最初に、図１を用いて、本実施の形態における仮想マシン制御システムの構成について説明する。図１は、仮想マシン制御システム１の構成例を示すブロック図である。

【００２６】

図１に示す仮想マシン制御システム１は、仮想マシンの通信ログを仮想マシンホスト外部から容易に収集できるように、当該仮想マシンの仮想マシンホストへの配置を行うシステムである。

【００２７】

具体的には、仮想マシン制御システム１は、仮想マシン制御装置１００と、ネットワーク２と、複数の仮想マシンホスト２００と、通信履歴記録装置３００と、によって構成されている。仮想マシン制御装置１００と、複数の仮想マシンホスト２００と、通信履歴記録装置３００とは、ネットワーク２を介して接続されている。

【００２８】

なお、ネットワーク２は、有線ネットワークでもよいし、無線ネットワークでもよい。また、ネットワーク２は、例えば、複数の仮想マシンホスト２００が接続されたデータセンタ内のネットワークであってもよいし、ＶＰＮ等を利用して論理的に構成されたネットワークであってもよいし、その他の任意のネットワークであってもよい。なお、ＶＰＮは、Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋの略である。以下、ネットワーク２は通常のＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）ネットワークであるものとして説明する。

【００２９】

仮想マシン制御装置１００は、取得した各仮想マシンの属性情報と、予め保持している各仮想マシンホスト２００の属性情報と、に基づいて、各仮想マシンの配置先となる仮想マシンホスト２００を決定する。このとき、仮想マシン制御装置１００は、各仮想マシン間の通信ログが通信履歴記録装置３００によって収集されやすくなるように、各仮想マシンの配置先となる仮想マシンホスト２００を決定する。なお、仮想マシン制御装置１００は、専用の分析装置でもよいし、パーソナルコンピュータ等の汎用的な装置によって実現されてもよい。

【００３０】

各仮想マシンホスト２００は、所謂物理マシンであって、複数の仮想マシンを格納したホストコンピュータである。各仮想マシンホスト２００に格納された仮想マシンは、同じ仮想マシンホストに格納された他の仮想マシンと通信することができるとともに、別の仮想マシンホストに格納された他の仮想マシン及びその他の通信機器とネットワーク２を介して通信することができる。

【００３１】

通信履歴記録装置３００は、ネットワーク２において収集可能な通信情報を、無線または有線などの通信を用いて受信し、収集した通信情報を記録する装置である。

【００３２】

≪仮想マシン制御装置１００の概要≫

続いて、図２を用いて、本実施の形態にかかる仮想マシン制御装置１００の概要について説明する。図２は、仮想マシン制御装置１００の概要を示すブロック図である。

【００３３】

図２に示すように、仮想マシン制御装置１００は、通信端末情報受信部（通信端末情報受信手段）１０１、類似度判定部（類似度判定手段）１１０、及び、通信端末配置部（端末配置手段）１０５を備える。

【００３４】

通信端末情報受信部１０１は、複数の仮想マシンホスト２００の何れかに配置予定の仮想マシンの属性情報を、無線又は有線などの通信を用いて受信する。

【００３５】

類似度判定部１１０は、通信端末情報受信部１０１によって受信された一又は複数の仮想マシンの属性情報の類似度を判定する。

【００３６】
通信端末配置部１０５は、類似度判定部１１０によって属性情報が類似していると判定された複数の仮想マシンを、同一の仮想マシンホスト２００に集中して配置するのではなく、少なくとも２つ以上の仮想マシンホスト２００に分散して配置する。換言すると、通信端末配置部１０５は、類似度判定部１１０によって属性情報が類似していると判定された複数の仮想マシンを、できるだけ互いに異なる仮想マシンホスト２００に配置する。
【００３７】
それにより、仮想マシン制御装置１００は、クラウド環境下において、インシデント調査に必要な属性情報の類似する仮想マシン間の通信ログを、複数の仮想マシンホスト２００の外部に設置された通信履歴記録装置３００を用いて容易に収集することができる。つまり、仮想マシン制御装置１００は、セキュリティ性能を十分に向上させることができる。
【００３８】
≪仮想マシン制御装置１００の具体的な構成例≫
続いて、図３を用いて、本実施の形態にかかる仮想マシン制御装置１００の詳細について説明する。図３は、仮想マシン制御装置１００の具体的な構成例を示すブロック図である。
【００３９】
図３に示すように、仮想マシン制御装置１００は、通信端末情報受信部１０１、ホスト要件記憶部１０２、類似度判定部１１０、通信端末配置部１０５、及び、配置情報記憶部１０６を備える。類似度判定部１１０は、データ変換部（データ変換手段）１０３、及び、クラスタ計算部（クラスタ計算手段）１０４によって構成されている。なお、仮想マシン制御装置１００は、図３に示す構成に限られず、図３に示す構成と同等の機能を実現可能な他の構成に適宜変更可能である。
【００４０】
通信端末情報受信部１０１は、複数の仮想マシンホスト２００の何れかに配置予定の仮想マシンの属性情報を、無線又は有線などの通信を用いて受信する。
【００４１】
図４は、通信端末情報受信部１０１によって受信された各仮想マシンの属性情報の具体例を示す図である。図４の例では、各仮想マシンの端末ＩＰ（ＩＰアドレス）と、当該端末ＩＰを持つ仮想マシンの属性情報である“所属部署”、“用途”、“セキュリティ要件”、“ネットワーク要件”、及び、“通信先”と、を組み合わせたテーブルが示されている。なお、通信端末情報受信部１０１によって受信される各仮想マシンの属性情報には、上記内容に限られず、例えば、各仮想マシンに必要とされる計算資源（ＣＰＵ、ＧＰＵなど）、或いは、各仮想マシンに必要とされるメモリ容量など、が含まれても良い。
【００４２】
ホスト要件記憶部１０２は、各仮想マシンの配置先（格納先）となる複数の仮想マシンホスト２００のそれぞれの属性情報を保持する。
【００４３】
図５は、ホスト要件記憶部１０２によって保持される各仮想マシンホスト２００の属性情報の具体例を示す図である。図５に示すように、例えば、テーブル４１には、各仮想マシンホスト２００のＩＰと、それに対応する仮想マシンホスト識別子と、の組み合わせが示されている。また、テーブル４２には、各仮想マシンホスト識別子と、それに対応する“セキュリティ要件”と、の組み合わせが示されている。さらに、テーブル４３には“所属部署”の一覧が示され、テーブル４４には“端末用途”の一覧が示され、テーブル４５には“セキュリティ要件”の一覧が示されている。
【００４４】
データ変換部１０３は、各仮想マシンの属性情報と各仮想マシンホスト２００の属性情報とを参照して、通信端末情報受信部１０１によって受信された各仮想マシンの属性情報を、距離を表すデータ構造の特徴ベクトルに変換する。
【００４５】

図６は、データ変換部１０３において算出された各仮想マシンの特徴ベクトルの具体例を示す図である。図６の例では、各仮想マシンの識別子である端末識別子と、当該端末識別子を持つ仮想マシンの特徴ベクトルと、を組み合わせたテーブルが示されている。ここで、各仮想マシンの特徴ベクトルは、各属性（例えば“所属部署”）の全種類の要素（例えば“営業部”、“開発部”）の組み合わせによって構成され、各属性の全種類の要素のうち該当する要素が１、該当しない要素が０で表されている。なお、図６の例では、各属性の要素（種類）の個数は、ホスト要件記憶部１０２によって保持されているテーブル４３，４４に依存している。また、図６の例では、各仮想マシンの端末識別子及びそれに対応する特徴ベクトルに加えて、その端末識別子を持つ仮想マシンの端末ＩＰが示されている。

【００４６】

クラスタ計算部１０４は、データ変換部１０３から出力された複数の特徴ベクトルのそれぞれを、それらの類似度に基づいて任意の個数のクラスタに分類する。分類されたクラスタとそれらに含まれる仮想マシン識別子は、通信端末配置部１０５に供給される。

【００４７】

通信端末配置部１０５は、クラスタ計算部１０４から出力されたクラスタ毎に、そのクラスタに含まれる複数の仮想マシンを、同一の仮想マシンホスト２００に集中して配置するのではなく、少なくとも２つ以上の仮想マシンホスト２００に分散して配置する。なお、このとき、配置要件及びネットワーク要件も考慮される。配置要件及びネットワーク要件の詳細については後述する。

【００４８】

配置情報記憶部１０６は、通信端末配置部１０５によって何れかの仮想マシンホスト２００に配置された各仮想マシンの配置情報を保持する。

【００４９】

図７は、各仮想マシンと、各仮想マシンが配置される仮想マシンホストと、の関係を示す図である。図７の例では、各仮想マシンに割り当てられた端末識別子と、その仮想マシンの端末ＩＰと、配置先の仮想マシンホスト識別子と、を組み合わせたテーブルが示されている。

【００５０】

≪本実施の形態にかかる仮想マシン制御動作≫

続いて、図８を用いて、本実施の形態にかかる仮想マシン制御動作を説明する。

図８は、仮想マシン制御装置１００の動作を示すフローチャートである。

【００５１】

図８に示すように、仮想マシン制御装置１００による計算処理では、まず、通信端末情報受信部１０１において、一つ又は複数の仮想マシンの属性情報を含んだ通信端末情報を受信する（Ｓ００１）。

【００５２】

その後、データ変換部１０３において、通信端末情報受信部１０１によって受信された各通信端末情報に基づいて、当該通信端末情報に対応する特徴ベクトルの生成を行う（Ｓ００２）。

【００５３】

特徴ベクトルの生成処理では、まず、通信端末情報受信部１０１によって受信された通信端末情報に基づいて、その通信端末情報に記されている任意の属性の属性ベクトルを作成する（Ｓ００３）。

【００５４】

具体的には、まず、ホスト要件記憶部１０２に保持された各属性（例えば“所属部署”）の全種類分の要素（例えば“営業部”、“開発部”）からなるベクトルを用意して、このベクトルを構成する要素の全てを０に初期化する。その後、初期化されたベクトルを構成する複数の要素のうち、通信端末情報に含まれる仮想マシンの属性に該当する要素を０から１に書き換える。それにより、各属性の属性ベクトルが形成される（Ｓ００３）。

【００５５】

その後、一又は複数の属性ベクトルを結合することにより、仮想マシンに対応する一つの特徴ベクトルを形成する。なお、結合される複数の属性ベクトルの順番は、例えば通信端末情報に記載された属性の順番でもよいし、属性名を昇順ソートすることにより得られる順番でもよいし、属性名を任意の指標を用いてソートすることにより得られる順番でもよい。本実施の形態では、通信端末情報に記載された属性の順に複数の属性ベクトルを結合することにより、１つの特徴ベクトルを形成している（Ｓ００４）。

【００５６】

以下、一例として、通信端末情報受信部１０１によって図４に示す通信端末情報が受信され、かつ、属性情報には、２つの属性“所属部署”及び“用途”が含まれている場合の動作について説明する。この場合において、通信端末情報受信部１０１によって受信された通信端末情報の端末ＩＰの各々に対して、特徴ベクトルを算出するとともに、ネットワーク内で重複しない任意の端末識別子を付与する。それにより、図６に示すような特徴ベクトル群が得られる。

【００５７】

例えば、端末ＩＰが“１９２．１６８．０．１１”を示す仮想マシンは、属性“所属部署”の種類（要素）が“営業部”を示し、かつ、属性“用途”の種類が“クライアント”を示している。そのため、“所属部署”の属性ベクトルは“１００”となり、“営業部”の属性ベクトルは“１０００”となる。そして、“所属部署”及び“用途”の順番でこれらの属性ベクトルを結合することにより、特徴ベクトルは“１００１０００”と表される。

【００５８】

その後、クラスタ計算部１０４において、データ変換部１０３から出力された各仮想マシンの特徴ベクトルをクラスタリングする（Ｓ００５）。

【００５９】

具体的には、凝集型クラスタリングアルゴリズムなどの任意のアルゴリズムを用いることにより、特徴ベクトル群を任意の個数のクラスタに分類する。本実施の形態では、クラスタリング方法としてウォード法（非特許文献５参照）が採用され、距離がユークリッド距離で表され、分離クラスタ数を２個にするため閾値が３．０に設定された場合を例に説明する。上記のクラスタリング方法（ウォード法）を用いて図６に示す特徴ベクトルを２個のクラスタに分類した結果を、図９に示す。

【００６０】

図９は、ウォード法によるクラスタリングの経過を可視化したデンドログラムである。図９の点線は、閾値（本実施の形態では３．０）を表している。本実施の形態のクラスタリング設定を用いることにより、図６に示す特徴ベクトルは２つのクラスタであるクラスタ１及びクラスタ２に分類されている。具体的には、端末識別子“Ｍ０００１”、“Ｍ０００２”、“Ｍ０００３”、“Ｍ０００４”は、クラスタ１に分類され、端末識別子“Ｍ００２１”、“Ｍ００２２”、“Ｍ００３１”は、クラスタ２に分類されている。

【００６１】

その後、通信端末配置部１０５において、配置要件及びネットワーク要件を考慮しつつ、クラスタ計算部１０４により算出されたクラスタ毎に、そのクラスタに含まれる一つ又は複数の仮想マシンの仮想マシンホストへの振り分けを行う（Ｓ００６）。

【００６２】

具体的には、クラスタ計算部１０４により算出されたクラスタ毎に、そのクラスタに分類された端末識別子を持つ全ての仮想マシンのそれぞれについて、配置要件を満たす複数の仮想マシンホスト（配置候補群）の中から何れかを選択する処理を行う。

【００６３】

なお、配置要件とは、通信端末情報に含まれる属性情報の中から選択された任意の一つ又は複数の属性情報である。また、ネットワーク要件とは、予め高頻度の通信を行うことが見込まれた仮想マシンらについて、同じ仮想マシンホストに配置することを要求する属性情報である。そのため、“ネットワーク要件”が“あり”の属性情報を持つ仮想マシンは、“通信先”の属性情報において指定された端末ＩＰを持つ仮想マシンと同じ仮想マシンホスト

２００に配置される。図４の例では、端末ＩＰが“１９２．１６８．０．２１”を示す仮想マシンは、“ネットワーク要件”が“あり”であるため、“通信先”において指定された端末ＩＰ“１９２．１６８．０．２２”を示す仮想マシンと同じ仮想マシンホスト２００に配置される。

【００６４】

仮想マシンの配置要件を満たす仮想マシンホストとは、例えば、仮想マシンの“ネットワーク要件”が“あり”以外の場合において、当該仮想マシンの全ての配置要件について同位又は上位の属性情報を有する一つ又は複数の仮想マシンホストのことである。或いは、仮想マシンの配置要件を満たす仮想マシンホストとは、例えば、仮想マシンの“ネットワーク要件”が“あり”以外の場合において、当該仮想マシンの属性が仮想マシンホストの属性の部分集合である一つ又は複数の仮想マシンホストのことである。

【００６５】

例えば、配置要件に“セキュリティ要件”の属性情報が含まれる場合、“セキュリティ要件”の属性情報が“高い”を示す仮想マシンホストは、“ネットワーク要件”が“なし”、かつ、“セキュリティ要件”が“標準”を示す仮想マシンの配置要件を満たす。

【００６６】

通信端末配置部１０５は、クラスタ毎に、そのクラスタに分類された全ての仮想マシンに対する配置候補群を特定する。そして、通信端末配置部１０５は、そのクラスタに分類された全ての仮想マシンを、配置候補群の仮想マシンホストのそれぞれに均等に振り分ける。或いは、通信端末配置部１０５は、そのクラスタに分類された全ての仮想マシンを、配置候補群の仮想マシンホストの各々に配置される仮想マシンの数が最小となるように、配置候補群の仮想マシンホストのそれぞれに振り分ける。

【００６７】

本実施の形態では、図１０に示すフローチャートと、以下の数式（１）のアルゴリズムと、を用いることにより、クラスタ毎に、そのクラスタに分類された全ての仮想マシンのそれぞれについて配置先の仮想マシンホストを選択する。なお、数式（１）において、ｍは仮想マシンを表し、Ｃは仮想マシンｍの属するクラスタを表し、Ｈは仮想マシンホストを表している。

【００６８】

【数１】

$$\text{m に対する H の配置スコア} = 1 - \left(\frac{\text{C から H に配置した仮想マシン数}}{\text{C から配置された総仮想マシン数}} \right)$$

・・・（１）

【００６９】

また、“ネットワーク要件”が“あり”を示す仮想マシンは、通信先属性に記載された端末ＩＰを持つ仮想マシンが最も多く配置されている仮想マシンホストに配置される。なお、通信先属性に記載された端末ＩＰが最も多く配置されている仮想マシンホストが複数存在する場合には、その中でランダムに選択された仮想マシンホストに配置される。

【００７０】

その後、配置情報記憶部１０６において、各仮想マシンにおける、端末識別子、それに対応する端末ＩＰ、及び、通信端末配置部１０５によって算出された、当該仮想マシンが配置される仮想マシンホスト識別子を、纏めて格納する（Ｓ００７）。

【００７１】

図７には、図５に示す仮想マシンホスト（識別子Ｈ１，Ｈ２）が設けられている場合の、配置情報記憶部１０６に格納される情報の一例が示されている。図７の例では、識別子Ｈ１の仮想マシンホストには、端末識別子“Ｍ０００１”、“Ｍ０００３”、“Ｍ００３１”の仮想マシンが配置されている。また、識別子Ｈ２の仮想マシンホストには、端末識別子“Ｍ０００２”、“Ｍ０００４”、“Ｍ００２１”、“Ｍ００２２”の仮想マシンが配置されている。

【００７２】
以上のように、本実施の形態にかかる仮想マシン制御装置１００は、仮想マシンの要求する配置要件及びネットワーク要件を考慮しつつ、属性情報の類似する複数の仮想マシンを少なくとも２つ以上の仮想マシンホストに分散して配置する。換言すると、仮想マシン制御装置１００は、仮想マシンの要求する配置要件及びネットワーク要件を考慮しつつ、属性情報の類似する複数の仮想マシンをできるだけ互いに異なる仮想マシンホストに配置する。それにより、仮想マシン制御装置１００は、クラウド環境下において、インシデント調査に必要な属性情報の類似する仮想マシン間の通信ログを、複数の仮想マシンホスト外部に設置された通信履歴記録装置によって容易に収集することができる。つまり、仮想マシン制御装置１００は、セキュリティ性能を十分に向上させることができる。
【００７３】
なお、関連技術では、クラウド環境下において、各仮想マシンが、計算資源効率化の観点から、空きストレージ容量に最も余裕のある仮想マシンホストに配置されている。つまり、関連技術では、クラウド環境下において、サイバー攻撃を受けた際のインシデント調査のために通信ログを収集することについては考慮されていない。それに対し、本実施の形態にかかる仮想マシン制御装置１００は、各仮想マシンの属性情報の類似度を計算して、類似する属性情報を持つ複数の仮想マシンを少なくとも２つ以上の仮想マシンホストに分散して配置している。それにより、仮想マシン制御装置１００は、クラウド環境下において、インシデント調査に必要な属性情報の類似する仮想マシン間の通信ログを、複数の仮想マシンホスト外部に設置された通信履歴記録装置を用いて容易に収集することができる。つまり、仮想マシン制御装置１００は、セキュリティ性能を十分に向上させることができる。
【００７４】
上記実施の形態における各構成は、ハードウェア又はソフトウェア、もしくはその両方によって構成され、１つのハードウェア又はソフトウェアから構成してもよいし、複数のハードウェア又はソフトウェアから構成してもよい。実施の形態における各機能（各処理）を、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）やメモリ等を有するコンピュータにより実現してもよい。例えば、記憶装置（記憶媒体）に実施の形態における方法（処理）を行うためのプログラムを格納し、各機能を、記憶装置に格納されたプログラムをＣＰＵで実行することにより実現してもよい。
【００７５】
このようなプログラムは、様々なタイプの非一時的なコンピュータ可読媒体（ｎｏｎ－ｔｒａｎｓｉｔｏｒｙ　ｃｏｍｐｕｔｅｒ　ｒｅａｄａｂｌｅ　ｍｅｄｉｕｍ）を用いて格納され、コンピュータに供給することができる。非一時的なコンピュータ可読媒体は、様々なタイプの実体のある記録媒体（ｔａｎｇｉｂｌｅ　ｓｔｏｒａｇｅ　ｍｅｄｉｕｍ）を含む。非一時的なコンピュータ可読媒体は、例えば、磁気記録媒体、光磁気記録媒体、ＣＤ－ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）、ＣＤ－Ｒ、ＣＤ－Ｒ／Ｗ、半導体メモリを含む。磁気記録媒体は、例えば、フレキシブルディスク、磁気テープ、ハードディスクドライブなどである。光磁気記録媒体は、例えば光磁気ディスクなどである。半導体メモリは、例えば、マスクＲＯＭ、ＰＲＯＭ（Ｐｒｏｇｒａｍｍａｂｌｅ　ＲＯＭ）、ＥＰＲＯＭ（Ｅｒａｓａｂｌｅ　ＰＲＯＭ）、フラッシュＲＯＭ、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）を含む。また、プログラムは、様々なタイプの一時的なコンピュータ可読媒体（ｔｒａｎｓｉｔｏｒｙ　ｃｏｍｐｕｔｅｒ　ｒｅａｄａｂｌｅ　ｍｅｄｉｕｍ）によってコンピュータに供給されてもよい。一時的なコンピュータ可読媒体の例は、電気信号、光信号、及び電磁波を含む。一時的なコンピュータ可読媒体は、電線及び光ファイバ等の有線通信路、又は無線通信路を介して、プログラムをコンピュータに供給できる。
【００７６】
以上、図面を参照して、本開示の実施の形態について詳しく説明してきたが、具体的な構成は上述のものに限られることはなく、本開示の要旨を逸脱しない範囲内において様々

な設計変更等が可能である。

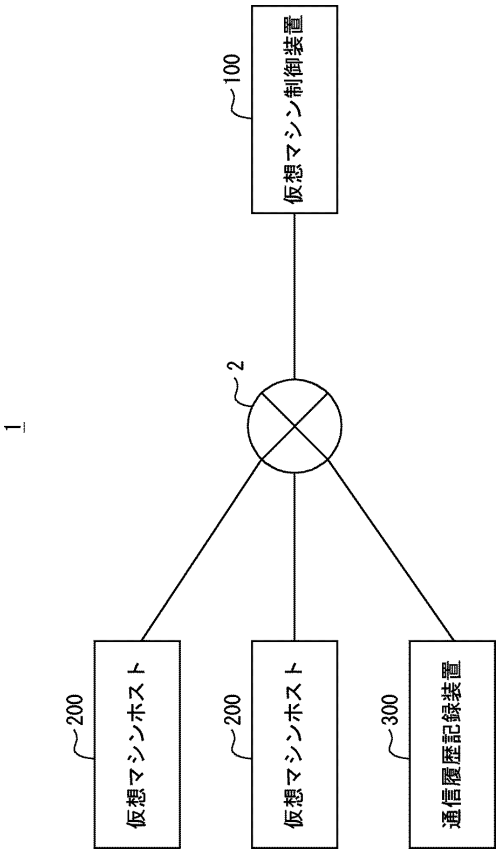
【符号の説明】

【００７７】

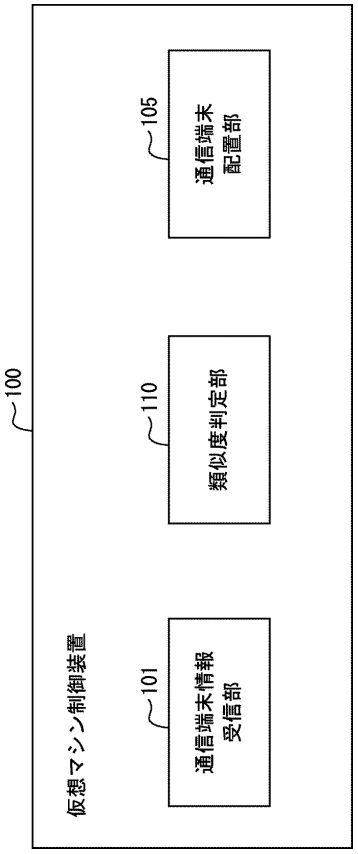
１　仮想マシン制御システム
２　ネットワーク
４１～４５　テーブル
１００　仮想マシン制御装置
１０１　通信端末情報受信部
１０２　ホスト要件記憶部
１０３　データ変換部
１０４　クラスタ計算部
１０５　通信端末配置部
１０６　配置情報記憶部
１１０　類似度判定部
２００　仮想マシンホスト
３００　通信履歴記録装置

【図面】

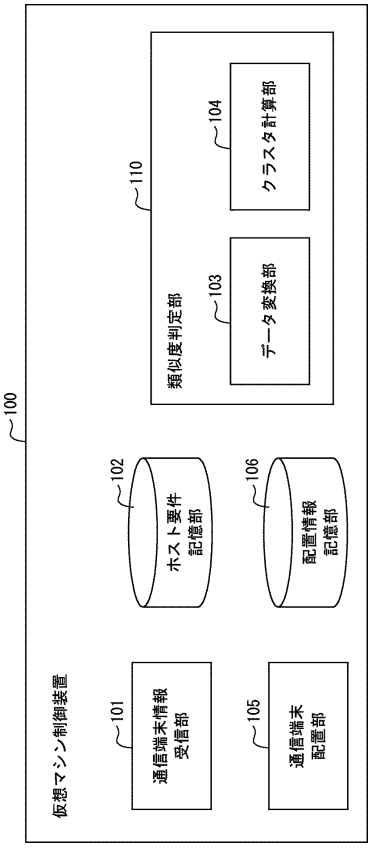
【図１】



【図２】



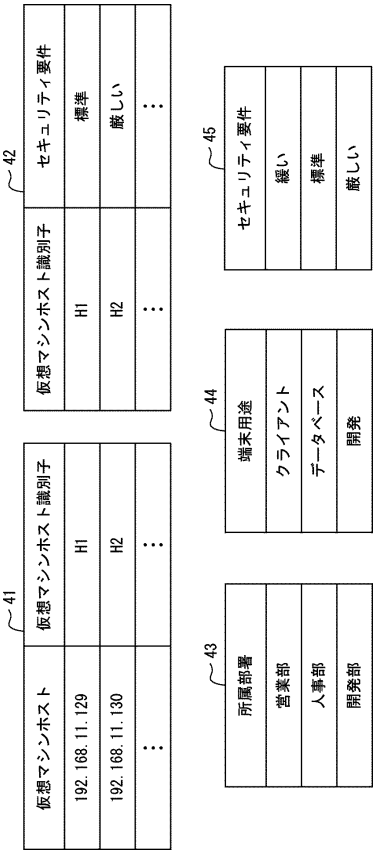
【図３】



【図４】

端末ＩＰ	所属部署	用途	セキュリティ要件	ネットワーク要件	通信先
192.168.0.11	営業部	クライアント	標準	なし	－
192.168.0.12	営業部	クライアント	標準	なし	－
192.168.0.13	営業部	クライアント	標準	なし	－
192.168.0.14	営業部	クライアント	標準	なし	－
192.168.0.21	人事部	サーバ	標準	あり	192.168.0.22
192.168.0.22	人事部	データベース	厳しい	なし	－
：	：	：	：	：	：
192.168.0.31	開発部	開発	標準	なし	－
：	：	：	：	：	：

【図５】



【図６】

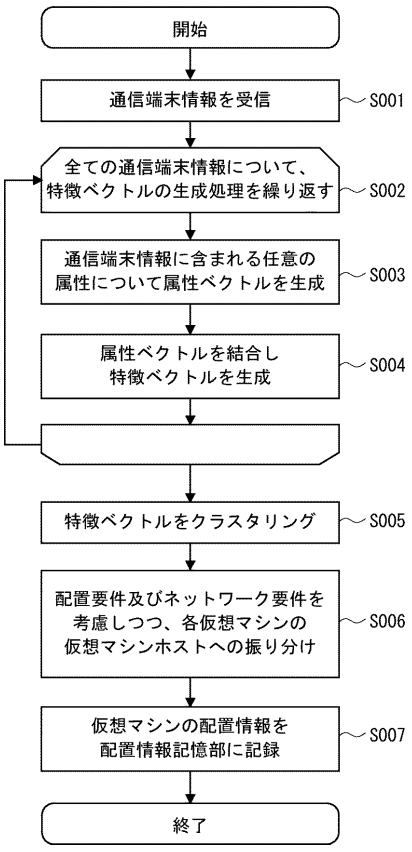
特徴ベクトル

端末識別子	営業部	人事部	開発部	クライアント	サーバ	データベース	開発	端末ＩＰ
M0001	1	0	0	1	0	0	0	192.168.0.11
M0002	1	0	0	1	0	0	0	192.168.0.12
M0003	1	0	0	1	0	0	0	192.168.0.13
M0004	1	0	0	1	0	0	0	192.168.0.14
M0021	0	1	0	0	1	0	0	192.168.0.21
M0022	0	1	0	0	0	1	0	192.168.0.22
M0031	0	0	1	0	0	0	1	192.168.0.31

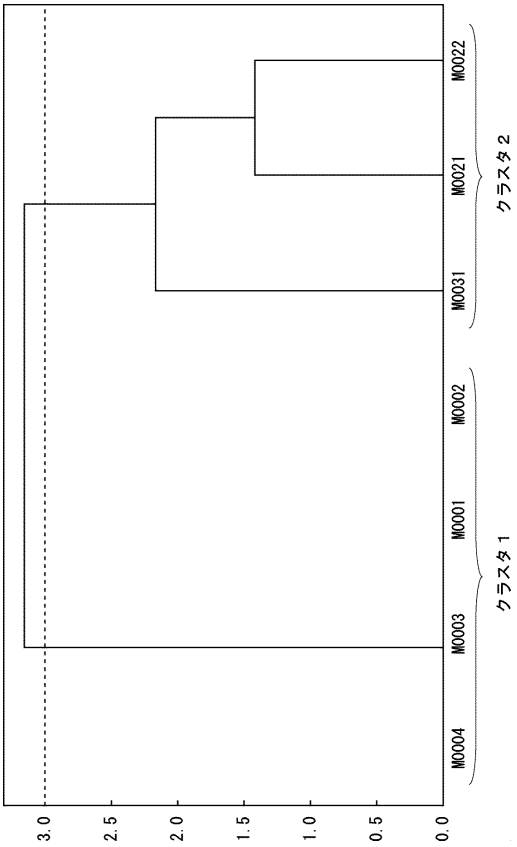
【図７】

端末識別子	端末ＩＰ	仮想マシンホスト識別子
M0001	192.168.0.11	H1
M0002	192.168.0.12	H2
M0003	192.168.0.13	H1
M0004	192.168.0.14	H2
M0021	192.168.0.21	H2
M0022	192.168.0.22	H2
…	…	…
M0031	192.168.0.31	H1
…	…	…

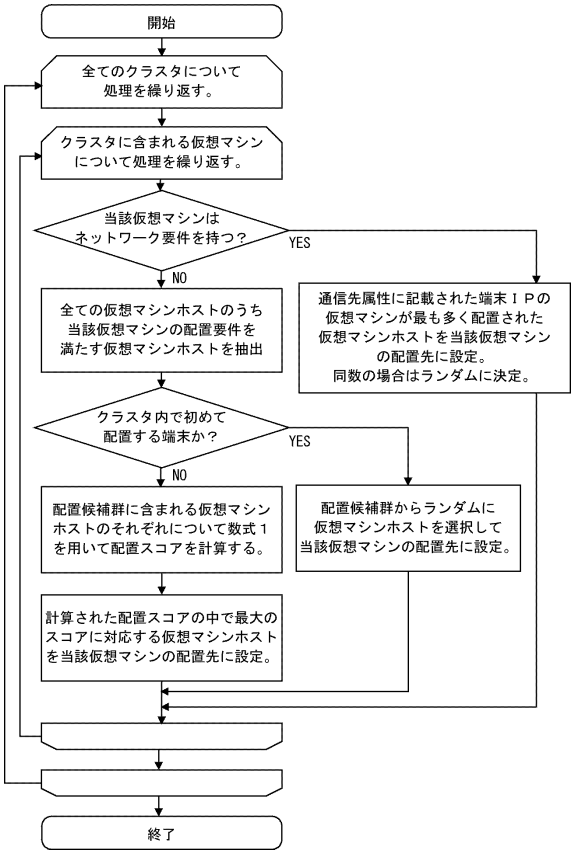
【図８】



【図９】


M0022
M0021
M0031
M0002
M0001
M0003
M0004
クラスタ２
クラスタ１
3.0
2.5
2.0
1.5
1.0
0.5
0.0

【図１０】


開始
全てのクラスタについて
処理を繰り返す。
クラスタに含まれる仮想マシン
について処理を繰り返す。
当該仮想マシンは
ネットワーク要件を持つ？
YES
NO
全ての仮想マシンホストのうち
当該仮想マシンの配置要件を
満たす仮想マシンホストを抽出
通信先属性に記載された端末ＩＰの
仮想マシンが最も多く配置された
仮想マシンホストを当該仮想マシン
の配置先に設定。
同数の場合はランダムに決定。
クラスタ内で初めて
配置する端末か？
YES
NO
配置候補群に含まれる仮想マシン
ホストのそれぞれについて数式１
を用いて配置スコアを計算する。
配置候補群からランダムに
仮想マシンホストを選択して
当該仮想マシンの配置先に設定。
計算された配置スコアの中で最大の
スコアに対応する仮想マシンホスト
を当該仮想マシンの配置先に設定。
終了

フロントページの続き

(56)参考文献 国際公開第２０１２／１４４６４７（WO，Ａ１）
特開２０１５－１６２１０９（ＪＰ，Ａ）
国際公開第２０１４／１４２２１７（WO，Ａ１）
米国特許出願公開第２０１６／０１０５８０１（ＵＳ，Ａ１）
西嶋 崇 TAKASHI NISHIJIMA，仮想Ｌｉｎｕｘ環境を活用したネットワーク構築演習システムと実ネットワークとの通信を可能とするゲートウェイ機能の開発 Development of the Gateway Function which Communicates with Real Networks and the Computer Network Construction Training System using a Virtual Linux，マルチメディア，分散，協調とモバイル（ＤＩＣＯＭＯ２０１０）シンポジウム論文集 情報処理学会シンポジウムシリーズ Ｖｏｌ．２０１０ Ｎｏ．１ ［ＣＤ－ＲＯＭ］ IPSJ Symposium Series，日本，社団法人情報処理学会，2010年07月07日，第2010巻，1875～1882，【ISSN】1882-0840

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ９／４５５