

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6010672号
(P6010672)

(45) 発行日 平成28年10月19日 (2016. 10. 19)

(24) 登録日 平成28年9月23日 (2016. 9. 23)

(51) Int. Cl.	F I
G 0 6 F 21/56 (2013.01)	G 0 6 F 21/56 3 4 0
G 0 6 F 21/53 (2013.01)	G 0 6 F 21/53

請求項の数 4 (全 12 頁)

(21) 出願番号	特願2015-183559 (P2015-183559)	(73) 特許権者	000102728
(22) 出願日	平成27年9月17日 (2015. 9. 17)		株式会社エヌ・ティ・ティ・データ
(62) 分割の表示	特願2012-9490 (P2012-9490)		東京都江東区豊洲三丁目3番3号
原出願日	平成24年1月19日 (2012. 1. 19)	(74) 代理人	100095407
(65) 公開番号	特開2015-228264 (P2015-228264A)		弁理士 木村 満
(43) 公開日	平成27年12月17日 (2015. 12. 17)	(72) 発明者	花館 蔵之
審査請求日	平成27年9月17日 (2015. 9. 17)		東京都江東区豊洲三丁目3番3号 株式会
			社エヌ・ティ・ティ・データ内
		(72) 発明者	石津 健佑
			東京都江東区豊洲三丁目3番3号 株式会
			社エヌ・ティ・ティ・データ内
		(72) 発明者	柿沼 基樹
			東京都江東区豊洲三丁目3番3号 株式会
			社エヌ・ティ・ティ・データ内

最終頁に続く

(54) 【発明の名称】 セキュリティ設定システム、セキュリティ設定方法およびプログラム

(57) 【特許請求の範囲】

【請求項1】

起動対象の仮想マシンを定義する仮想マシンイメージの識別情報を取得する仮想マシンイメージ識別情報取得手段と、

前記起動対象の仮想マシンを識別する仮想マシン識別情報を取得する仮想マシン識別情報取得手段と、

前記仮想マシンイメージに基づいて起動される仮想マシンに対して検出すべき通信データを含むシグネチャファイルを識別するシグネチャ識別情報を、前記仮想マシンイメージの識別情報に対応づけて記憶するシグネチャ識別情報記憶手段と、

前記仮想マシンイメージ識別情報取得手段で取得した仮想マシンイメージの識別情報に対応する前記シグネチャ識別情報を、前記シグネチャ識別情報記憶手段に記憶したシグネチャ識別情報に基づいて特定するシグネチャ識別情報特定手段と、

前記仮想マシン識別情報取得手段で取得した仮想マシン識別情報を前記シグネチャ識別情報特定手段で特定したシグネチャ識別情報により示されるシグネチャファイルに対応づけて記憶するシグネチャファイル記憶手段と、

前記シグネチャファイル記憶手段に記憶された対応するシグネチャファイルに基づいて前記起動対象の仮想マシンを起動する仮想マシン起動手段と、

を備えることを特徴とするセキュリティ設定システム。

【請求項2】

前記シグネチャファイル記憶手段に記憶された対応するシグネチャファイルからシグネ

10

20

チャデータを設定するシグネチャデータ設定手段をさらに備え、

前記仮想マシン起動手段は、前記シグネチャデータに基づいて前記起動対象の仮想マシンを起動する、

ことを特徴とする請求項 1 に記載のセキュリティ設定システム。

【請求項 3】

仮想マシンイメージ識別情報取得手段と仮想マシン識別情報取得手段とシグネチャ識別情報記憶手段とシグネチャ識別情報特定手段とシグネチャファイル記憶手段と仮想マシン起動手段を備えるセキュリティ設定システムによるセキュリティ設定方法であって、

前記仮想マシンイメージ識別情報取得手段が起動対象の仮想マシンを定義する仮想マシンイメージの識別情報を取得する仮想マシンイメージ識別情報取得ステップと、

前記仮想マシン識別情報取得手段が前記起動対象の仮想マシンを識別する仮想マシン識別情報を取得する仮想マシン識別情報取得ステップと、

前記シグネチャ識別情報記憶手段が前記仮想マシンイメージに基づいて起動される仮想マシンに対して検出すべき通信データを含むシグネチャファイルを識別するシグネチャ識別情報を、前記仮想マシンイメージの識別情報に対応づけて記憶するシグネチャ識別情報記憶ステップと、

前記シグネチャ識別情報特定手段が前記仮想マシンイメージ識別情報取得ステップで取得した仮想マシンイメージの識別情報に対応する前記シグネチャ識別情報を、前記シグネチャ識別情報記憶ステップで記憶したシグネチャ識別情報に基づいて特定するシグネチャ識別情報特定ステップと、

前記シグネチャファイル記憶手段が前記仮想マシン識別情報取得ステップで取得した仮想マシン識別情報を前記シグネチャ識別情報特定ステップで特定したシグネチャ識別情報により示されるシグネチャファイルに対応づけて記憶するシグネチャファイル記憶ステップと、

前記仮想マシン起動手段が前記シグネチャファイル記憶ステップで記憶された対応するシグネチャファイルに基づいて前記起動対象の仮想マシンを起動する仮想マシン起動ステップと、

を備えることを特徴とするセキュリティ設定方法。

【請求項 4】

コンピュータを、

起動対象の仮想マシンを定義する仮想マシンイメージの識別情報を取得する仮想マシンイメージ識別情報取得手段、

前記起動対象の仮想マシンを識別する仮想マシン識別情報を取得する仮想マシン識別情報取得手段、

前記仮想マシンイメージに基づいて起動される仮想マシンに対して検出すべき通信データを含むシグネチャファイルを識別するシグネチャ識別情報を、前記仮想マシンイメージの識別情報に対応づけて記憶するシグネチャ識別情報記憶手段、

前記仮想マシンイメージ識別情報取得手段で取得した仮想マシンイメージの識別情報に対応する前記シグネチャ識別情報を、前記シグネチャ識別情報記憶手段に記憶したシグネチャ識別情報に基づいて特定するシグネチャ識別情報特定手段、

前記仮想マシン識別情報取得手段で取得した仮想マシン識別情報を前記シグネチャ識別情報特定手段で特定したシグネチャ識別情報により示されるシグネチャファイルに対応づけて記憶するシグネチャファイル記憶手段、

前記シグネチャファイル記憶手段に記憶された対応するシグネチャファイルに基づいて前記起動対象の仮想マシンを起動する仮想マシン起動手段、

として機能させることを特徴とするプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、セキュリティ設定システム、セキュリティ設定方法およびプログラムに関す

10

20

30

40

50

る。

【背景技術】

【0002】

近年、ADSL網や光ファイバ網の整備や、各種ネットワークサービスの充実を背景にして、ネットワークに接続される機器の数が飛躍的に増加しており、ネットワークセキュリティの問題が顕著になってきている。

【0003】

ネットワークセキュリティの問題として挙げられるものとして、ネットワーク機器の脆弱性を突いて機器に感染・増殖するコンピュータウイルスや、機器の脆弱性とユーザの設定ミスなどにつけこんでネットワーク機器の制御を奪ったり、機器内に記録されているデータの窃盗や破壊を行ったりする不正アクセスがある。

10

【0004】

このような外部ネットワークからの攻撃を防止するため、IDS (Intrusion Detection System) やIPS (Intrusion Protection System) といった不正を検知する技術が一般的に用いられている。IDS およびIPSは、不正アクセスやウイルス等を不正な攻撃として検知するシステムであり、IDSは不正な攻撃を管理者へ通知するのに対し、IPSは管理者へ通知するとともに自動的に通信を遮断する。

【0005】

このようなIDSおよびIPSとして、不正アクセスやコンピュータウイルスを特徴付けるシグネチャデータを、ネットワークを介して配布して監視を行う技術が提案されている (例えば特許文献1)。

20

【先行技術文献】

【特許文献】

【0006】

【特許文献1】特開2007-11628号公報

【発明の概要】

【発明が解決しようとする課題】

【0007】

しかし、仮想マシンを動作させる仮想化基盤上に特許文献1の技術を適用する場合、多くの仮想マシンの起動が想定され、これら一つ一つの仮想マシンのOSやセキュリティ要件に適合したシグネチャデータを設定することが困難となる。また、各仮想マシンのOSやセキュリティ要件に適合したシグネチャデータを設定する場合、管理者は各仮想マシンに対応したシグネチャデータを手動で設定し、仮想マシン毎に配信する必要がある。したがって各仮想マシンに適合したシグネチャデータを効率よく設定するという観点からみると未だ十分とは言えない。

30

【0008】

本発明は、上述のような事情に鑑みてなされたものであり、各仮想マシンに適合したシグネチャデータを効率よく設定することのできるセキュリティ設定システム、セキュリティ設定方法およびプログラムを提供することを目的としている。

40

【課題を解決するための手段】

【0009】

上記目的を達成するため、本発明の第1の観点に係るセキュリティ設定システムは、起動対象の仮想マシンを定義する仮想マシンイメージの識別情報を取得する仮想マシンイメージ識別情報取得手段と、

前記起動対象の仮想マシンを識別する仮想マシン識別情報を取得する仮想マシン識別情報取得手段と、

前記仮想マシンイメージに基づいて起動される仮想マシンに対して検出すべき通信データを含むシグネチャファイルを識別するシグネチャ識別情報を、前記仮想マシンイメージの識別情報に対応づけて記憶するシグネチャ識別情報記憶手段と、

50

前記仮想マシンイメージ識別情報取得手段で取得した仮想マシンイメージの識別情報に対応する前記シグネチャ識別情報を、前記シグネチャ識別情報記憶手段に記憶したシグネチャ識別情報に基づいて特定するシグネチャ識別情報特定手段と、

前記仮想マシン識別情報取得手段で取得した仮想マシン識別情報を前記シグネチャ識別情報特定手段で特定したシグネチャ識別情報により示されるシグネチャファイルに対応づけて記憶するシグネチャファイル記憶手段と、

前記シグネチャファイル記憶手段に記憶された対応するシグネチャファイルに基づいて前記起動対象の仮想マシンを起動する仮想マシン起動手段と、

を備えることを特徴とする。

【0010】

前記シグネチャファイル記憶手段に記憶された対応するシグネチャファイルからシグネチャデータを設定するシグネチャデータ設定手段をさらに備え、

前記仮想マシン起動手段は、前記シグネチャデータに基づいて前記起動対象の仮想マシンを起動する、

ようにしてもよい。

【0011】

上記目的を達成するため、本発明の第2の観点に係るセキュリティ設定方法は、

仮想マシンイメージ識別情報取得手段と仮想マシン識別情報取得手段とシグネチャ識別情報記憶手段とシグネチャ識別情報特定手段とシグネチャファイル記憶手段と仮想マシン起動手段を備えるセキュリティ設定システムによるセキュリティ設定方法であって、

前記仮想マシンイメージ識別情報取得手段が起動対象の仮想マシンを定義する仮想マシンイメージの識別情報を取得する仮想マシンイメージ識別情報取得ステップと、

前記仮想マシン識別情報取得手段が前記起動対象の仮想マシンを識別する仮想マシン識別情報を取得する仮想マシン識別情報取得ステップと、

前記シグネチャ識別情報記憶手段が前記仮想マシンイメージに基づいて起動される仮想マシンに対して検出すべき通信データを含むシグネチャファイルを識別するシグネチャ識別情報を、前記仮想マシンイメージの識別情報に対応づけて記憶するシグネチャ識別情報記憶ステップと、

前記シグネチャ識別情報特定手段が前記仮想マシンイメージ識別情報取得ステップで取得した仮想マシンイメージの識別情報に対応する前記シグネチャ識別情報を、前記シグネチャ識別情報記憶ステップで記憶したシグネチャ識別情報に基づいて特定するシグネチャ識別情報特定ステップと、

前記シグネチャファイル記憶手段が前記仮想マシン識別情報取得ステップで取得した仮想マシン識別情報を前記シグネチャ識別情報特定ステップで特定したシグネチャ識別情報により示されるシグネチャファイルに対応づけて記憶するシグネチャファイル記憶ステップと、

前記仮想マシン起動手段が前記シグネチャファイル記憶ステップで記憶された対応するシグネチャファイルに基づいて前記起動対象の仮想マシンを起動する仮想マシン起動ステップと、

を備えることを特徴とする。

【0012】

上記目的を達成するため、本発明の第3の観点に係るプログラムは、

コンピュータを、

起動対象の仮想マシンを定義する仮想マシンイメージの識別情報を取得する仮想マシンイメージ識別情報取得手段、

前記起動対象の仮想マシンを識別する仮想マシン識別情報を取得する仮想マシン識別情報取得手段、

前記仮想マシンイメージに基づいて起動される仮想マシンに対して検出すべき通信データを含むシグネチャファイルを識別するシグネチャ識別情報を、前記仮想マシンイメージの識別情報に対応づけて記憶するシグネチャ識別情報記憶手段、

前記仮想マシンイメージ識別情報取得手段で取得した仮想マシンイメージの識別情報に対応する前記シグネチャ識別情報を、前記シグネチャ識別情報記憶手段に記憶したシグネチャ識別情報に基づいて特定するシグネチャ識別情報特定手段、

前記仮想マシン識別情報取得手段で取得した仮想マシン識別情報を前記シグネチャ識別情報特定手段で特定したシグネチャ識別情報により示されるシグネチャファイルに対応づけて記憶するシグネチャファイル記憶手段、

前記シグネチャファイル記憶手段に記憶された対応するシグネチャファイルに基づいて前記起動対象の仮想マシンを起動する仮想マシン起動手段、

として機能させることを特徴とする。

【発明の効果】

10

【0013】

本発明によれば、各仮想マシンに適合したシグネチャデータを効率よく設定することのできるセキュリティ設定システム、セキュリティ設定方法およびプログラムを提供することができる。

【図面の簡単な説明】

【0014】

【図1】本発明の実施形態に係るセキュリティ設定システムの一例を示すブロック図である。

【図2】シグネチャ管理DBの構成例を示す図である。

【図3】仮想マシンイメージ管理DBの構成例を示す図である。

20

【図4】設定処理の一例を示すフローチャートである。

【図5】仮想シグネチャ管理DBの一例を示す図である。

【図6】照合処理の一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】

【0015】

以下、本発明の実施形態に係るセキュリティ設定システムを、図面を参照して説明する。

【0016】

本実施形態に係るセキュリティ設定システム100は、仮想マシン管理装置200と、DBサーバ300とから構成される。セキュリティ設定システム100は、仮想化基盤上で動作する複数の仮想マシンのOSや機能に適合するシグネチャであって予め作成されたものを、DBサーバ300上で管理し、仮想マシンの起動と同時に、各仮想マシンに対応するシグネチャをデータベース上から検索し、配信、設定する、プログラム制御により動作するコンピュータシステムである。

30

【0017】

仮想マシン管理装置200は、主に、仮想マシンの管理者からの入力操作に応じて、起動が要求される仮想マシンに対するシグネチャデータの設定を行うコンピュータであり、図1に示すように、記憶部210と、制御部220と、通信部230と、上記各部を相互に接続するシステムバス240を備えている。

【0018】

40

記憶部210は、フラッシュメモリ、ハードディスク等の不揮発性メモリから構成され、制御部220の各機能部を実現させるためのプログラムと仮想マシン識別情報一覧が記憶されている。また、記憶部210には、後述する処理により、一の仮想マシン識別情報と複数のシグネチャファイルとを対応付ける仮想シグネチャ管理テーブルが格納される。

【0019】

制御部220は、CPU等から構成される。制御部220は、プログラムに従って動作し、起動を要求された仮想マシンに適合するシグネチャデータを設定する設定処理や、仮想マシンの利用者からの仮想マシン利用要求にしたがってパケットの照合を行う照合処理に必要な機能を提供する。制御部220は、プログラムにより提供される主要な機能部として、仮想マシン管理部221と、シグネチャ管理部222と、パケット監視部223を

50

備えている。

【0020】

仮想マシン管理部221は、詳しくは後述するが、記憶部210に格納されている仮想マシン識別情報一覧に従って起動を要求された仮想マシンに一意に対応する仮想マシン識別情報を作成する機能と、シグネチャ管理部222に、対応するシグネチャデータの取得を要求する機能と、起動を要求された仮想マシンを起動する機能を有している。

【0021】

シグネチャ管理部222は、詳しくは後述するが、仮想マシン管理部221からの要求に応じてDBサーバ300に、対応するシグネチャデータの検索と取得を要求する機能と、取得したシグネチャデータをシグネチャ管理テーブルとして記憶部210へ格納する機能を有している。

10

【0022】

パケット監視部223は、詳しくは後述するが、仮想マシンの利用者からの利用要求に応じて、記憶部210に格納されているシグネチャID管理テーブルを参照してパケットパターンの照合を行い、仮想マシンへのアクセス許可を判定する機能を有している。

【0023】

通信部230は、シリアルインタフェース、或いはアナログ信号を受信するためのアナログインタフェースを有している。通信部230は、制御部220による制御により、DBサーバ300と通信を行う。

【0024】

20

DBサーバ300は、仮想マシン管理装置200からの指示にしたがって、対応するシグネチャデータを検索し、仮想マシン管理装置200へシグネチャデータを提供するコンピュータである。DBサーバ300には、図2に示すようなシグネチャ管理DBと図3に示すような仮想マシンイメージ管理DBとが格納される。図2に示すシグネチャ管理DBは、シグネチャファイル管理テーブルとシグネチャID管理テーブルとから構成され、シグネチャファイル管理テーブルは、不正アクセスやウイルスの情報を定義したシグネチャファイルを、シグネチャを識別するシグネチャ識別情報ごとに対応づけたテーブルである。なお、シグネチャファイルには、不正アクセスやウイルスを検出した際に行われる処理等も含まれている。シグネチャID管理テーブルは、シグネチャ識別情報を、仮想マシンイメージを識別する仮想マシン識別情報ごとに対応づけたテーブルである。図3に示す仮想マシンイメージ管理DBは、仮想マシンイメージ管理テーブルから構成される。仮想マシンイメージ管理テーブルは、仮想マシンイメージファイルを特定する仮想マシンイメージファイル名を、仮想マシンイメージを識別する仮想マシン識別情報と対応づけたテーブルである。

30

【0025】

DBサーバ300は、仮想マシン管理装置200からの要求にしたがって仮想マシンイメージファイルやシグネチャファイルを、格納された各種テーブルから検索し、仮想マシン管理装置200へ提供する。

【0026】

以上が、セキュリティ設定システム100の構成である。続いて、セキュリティ設定システム100の動作について、図4～図6を参照して説明する。

40

【0027】

まず、設定処理におけるセキュリティ設定システム100の動作について、図4を参照して説明する。設定処理は、仮想マシンの管理者によるコンピュータの入力操作により、仮想マシンの起動要求を、通信部230を介して受信することにより開始される。

【0028】

制御部220は、仮想マシン管理部221の機能により仮想マシンの起動要求を取得する(ステップS101)。仮想マシンの起動要求には、起動が要求される仮想マシンの仮想マシンイメージ識別情報が含まれている。

【0029】

50

そして、仮想マシン管理部 221 は、記憶部 210 に格納されている仮想マシン識別情報一覧に含まれる複数の仮想マシン識別情報から任意の識別情報を選択するなどして、仮想マシン識別情報を生成する（ステップ S102）。なお、一度選択された仮想マシン識別情報は、仮想マシンの起動が終了するまでは再度選択されることのないように仮想マシン管理部 221 により制御される。また、起動を要求する仮想マシンが複数ある場合には、それぞれの要求に対して仮想マシン識別情報が生成される。

【0030】

続いて仮想マシン管理部 221 は、仮想マシンイメージ識別情報を、通信部 230 を介して DBサーバ 300 へ送信し、仮想マシンイメージファイルの送信を要求する（ステップ S103）。仮想マシンイメージファイルは、起動する仮想マシンの構成を定義する構成情報定義ファイルなどであり、仮想マシンを起動する際に参照される。

10

【0031】

DBサーバ 300 は、仮想マシン管理装置 200 から仮想マシンイメージ識別情報を受信すると、仮想マシン管理装置 200 からの要求に応じたデータを検索して提供する検索処理を開始する。まず、DBサーバ 300 は、仮想マシンイメージ管理 DB を参照することにより、当該仮想マシンイメージ識別情報に対応する仮想マシンイメージファイルを検索して特定する（ステップ S201）。そして DBサーバ 300 は、検索結果として、特定した仮想マシンイメージファイルを仮想マシン管理装置 200 へ送信する（ステップ S202）。

【0032】

20

仮想マシン管理装置 200 の制御部 220 は、仮想マシン管理部 221 の機能により通信部 230 を介して仮想マシンイメージファイルを取得すると、仮想マシン識別情報と仮想マシンイメージ識別情報とをシグネチャ管理部 222 へ渡す。シグネチャ管理部 222 は、仮想マシン識別情報と仮想マシンイメージ識別情報とを取得すると、取得した仮想マシンイメージ識別情報を、通信部 230 を介して DBサーバ 300 へ送信してシグネチャファイルの送信を要求する（ステップ S104）。

【0033】

DBサーバ 300 は、仮想マシン管理装置 200 から仮想マシンイメージ識別情報を受信すると、当該仮想マシンイメージ識別情報に対応するシグネチャ識別情報を、シグネチャ ID 管理テーブルを参照して特定する（ステップ S203）。続いて DBサーバ 300 は、ステップ S203 の処理で特定したシグネチャ識別情報に対応するシグネチャファイルを、シグネチャファイル管理テーブルを参照して特定する（ステップ S204）。ステップ S204 の処理の後、DBサーバ 300 は、特定してシグネチャファイルを仮想マシン管理装置 200 に送信して（ステップ S205）、処理を終了する。

30

【0034】

仮想マシン管理装置 200 の制御部 220 は、シグネチャ管理部 222 の機能により通信部 230 を介してシグネチャファイルを取得すると、図 5 に示すように、取得したシグネチャファイルをステップ S104 の処理で取得した仮想マシン識別情報と対応付けて、記憶部 210 の仮想シグネチャ管理 DB のシグネチャ管理テーブルへ格納する（ステップ S105）。ステップ S106 の処理の後、シグネチャ管理部 222 は、シグネチャ ID 管理テーブルへの格納が正常に行われたことを示す格納完了通知を仮想マシン管理部 221 へ渡す。

40

【0035】

図 4 に戻り、仮想マシン管理部 221 は、格納完了通知を取得すると、ステップ S202 の処理により DBサーバ 300 から送信された仮想マシンイメージファイルに基づいて、仮想マシンの管理者により起動の要求された仮想マシンを起動する（ステップ S106）。

【0036】

ステップ S106 の処理の後、仮想マシン管理部 221 は、仮想マシンの起動が完了したことを示す起動完了通知を、通信部 230 を介して仮想マシンの管理者に送信し（ステ

50

ップS107)、設定処理を終了する。

【0037】

次に、照合処理におけるセキュリティ設定システム100の動作について、図6を参照して説明する。照合処理は、対象となる仮想マシンの通信を監視する処理であり、仮想マシンが起動されることにより開始される。ここでは、仮想マシンの利用者により仮想マシンに対する利用要求が送信された場合における通信の監視を例に説明する。

【0038】

制御部220は、パケット監視部223の機能により、仮想マシンの利用要求を取得する(ステップS301)。仮想マシンの利用要求には、利用が要求される仮想マシンの仮想マシン識別情報と、当該仮想マシン上での処理の内容や通信データの内容を示す操作情報とが含まれている。なお、当該セキュリティ設定システム100は、仮想マシンに対する通信を全て監視するため、利用要求に限らず、例えば、通信の宛先やポート番号、プロトコルやパケットのデータ部を取得する機能も有している。

【0039】

続いてパケット監視部223は、取得した仮想マシン識別情報に基づいて、当該仮想マシン識別情報に対応するシグネチャファイルを、記憶部210に格納されている仮想シグネチャ管理テーブルから検索して特定する(ステップS302)。パケット監視部223は、ステップS302の処理で特定したシグネチャファイルを参照することで、当該シグネチャファイルの内容と、ステップS301の処理で取得した仮想マシンの利用要求に含まれる操作情報とを照合し、不正パケットであるか否かを判定する(ステップS303)。

【0040】

ステップS303の処理では、例えば、当該操作情報により示される通信データパケットのパケットパターンが、ステップS302の処理で特定したシグネチャファイルに含まれているか否かを、当該シグネチャファイルの内容(シグネチャデータ)を参照して判定する。パケット監視部223は、シグネチャファイルに当該パケットパターンが含まれている場合に不正パケットであると判定し、含まれていない場合には、不正パケットではないと判定する。

【0041】

ステップS303の処理において、不正パケットではないと判定した場合(ステップS303; No)、パケット監視部223は、ステップS301で取得した仮想マシンの利用要求により特定される仮想マシンに対してのアクセスを許可し、操作情報により特定される操作を開始させ(ステップS304)、処理を終了する。

【0042】

一方、ステップS303の処理において、不正パケットであると判定した場合(ステップS303; Yes)、パケット監視部223は、当該セキュリティ設定システム100がIDSを採用しているかIPSを採用しているかに応じた処理を行い(ステップS306)、処理を終了する。

【0043】

例えば、当該セキュリティ設定システム100がIDSを採用している場合には、不正パケットを検知したことを示す不正検知情報を、仮想マシンの管理者へ送信し、IPSを採用している場合には、不正パケットを検知した場合に、当該パケットを破棄して、仮想マシンの管理者と利用者に通知する。なお、この例では当該セキュリティ設定システム100における照合処理にて、仮想マシンに対する通信の監視を行う処理について説明したが、当該セキュリティ設定システム100は、監視対象の仮想マシンから利用者端末等への通信についても同様にして監視を行うことができる。

【0044】

以上が、セキュリティ設定システム100の動作である。このような構成によれば、仮想マシンイメージを識別する仮想マシンイメージ識別情報に対応するシグネチャ識別情報が特定され、特定されたシグネチャ識別情報により識別されるシグネチャファイルが動的

に設定されることとなる。したがって、各仮想マシンに適合したシグネチャデータを効率よく設定することができる。また、各仮想マシンの起動と同時に動的にシグネチャデータが設定されるため、仮想マシンの起動からシグネチャデータを設定するまでのタイムラグが解消され、その間における不正アクセス等の攻撃を防止することができる。

【0045】

(変形例)

この発明は、上記の実施形態に限定されず、種々の変形及び応用が可能である。図4に示す設定処理において、ステップS102の処理の後に、ステップS103の処理とステップS201～S202の処理を実行する例を示したが、これは一例である。当該ステップS103の処理とステップS201～S202の処理は、ステップS105の処理の後でステップS106における仮想マシンの起動前に実行してもよい。

10

【0046】

また、上記実施形態では、セキュリティ設定システム100が仮想マシン管理装置200と、DBサーバ300とから構成される例を示したが、仮想マシン管理装置200が、DBサーバ300が備えるシグネチャ管理DBと仮想マシンイメージ管理DBとを備えていれば、セキュリティ設定システム100は、仮想マシン管理装置200から構成されてもよい。

【0047】

また、上記実施形態では、物理的構成を有する仮想マシン管理装置200により上記各処理を実行する例を示したが、これは一例である。例えば、図示しないサーバ上で予め格納されている仮想化ソフトウェアを起動し、当該仮想マシン管理装置200における各構成を仮想化環境で使用してもよい。すなわち、仮想マシン管理装置200自体を仮想サーバとしてもよい。

20

【0048】

上記実施形態では、ステップS105の処理において、シグネチャファイルを仮想マシン識別情報と対応付けて仮想シグネチャ管理DBのシグネチャ管理テーブルに格納する例を示したが、当該仮想シグネチャ管理テーブルは仮想マシン毎に、仮想マシンの管理者により編集可能であってもよい。この場合には、編集後のシグネチャファイルのファイル名を変更することが望ましい。

【0049】

また、上述の機能を、OS (Operating System) とアプリケーションとの分担、またはOSとアプリケーションとの協同により実現する場合等には、OS以外の部分のみを媒体に格納してもよい。

30

【0050】

また、搬送波にプログラムを重畳し、通信ネットワークを介して配信することも可能である。例えば、通信ネットワーク上の掲示板 (BBS、Bulletin Board System) に当該プログラムを掲示し、ネットワークを介して当該プログラムを配信してもよい。そして、これらのプログラムを起動し、オペレーティングシステムの制御下で、他のアプリケーションプログラムと同様に実行することにより、上述の処理を実行できるように構成してもよい。

40

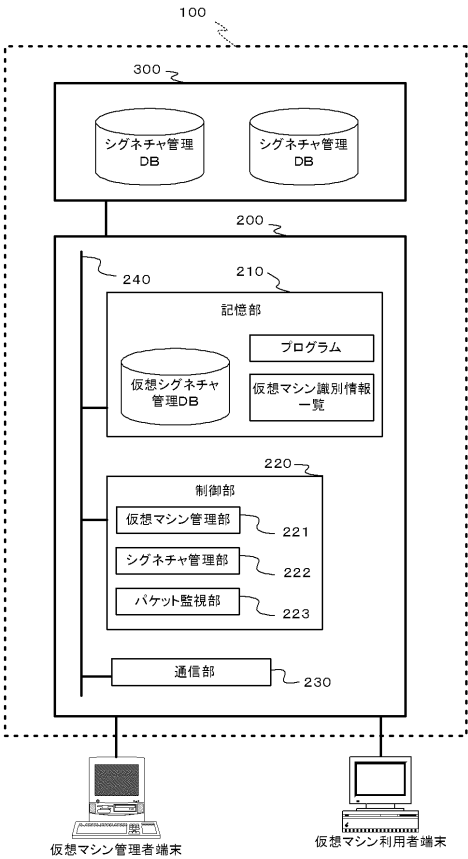
【符号の説明】**【0051】**

- 100 セキュリティ設定システム
- 200 仮想マシン管理装置
- 210 記憶部
- 220 制御部
- 221 仮想マシン管理部
- 222 シグネチャ管理部
- 223 パケット監視部
- 230 通信部

50

240 システムバス
300 DBサーバ

【図 1】



【図 2】

シグネチャ管理DB

シグネチャファイル管理テーブル

シグネチャ識別情報	シグネチャファイル
SIG1	Sig1. rules
SIG2	Sig2. rules
SIG3	Sig3. rules
SIG4	Sig4. rules
⋮	⋮
SIGN	SigN. rules

シグネチャID管理テーブル

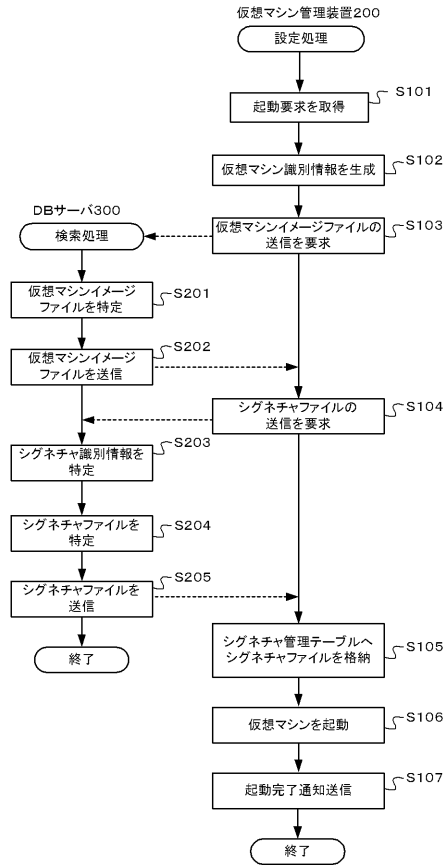
仮想マシンイメージ識別情報	シグネチャ識別情報
1	SIG1 SIG2 SIG4
2	SIG2 SIG3 ...
3	SigN
⋮	⋮
M	SIG2 SIG4

【図 3】

仮想マシンイメージ管理DB

仮想マシンイメージ管理テーブル	
仮想マシンイメージ 識別情報	仮想マシンイメージ ファイル
1	Img1. tty
2	Img2. tty
3	Img3. tty
4	Img4. tty
⋮	⋮
M	ImgM. tty

【図 4】

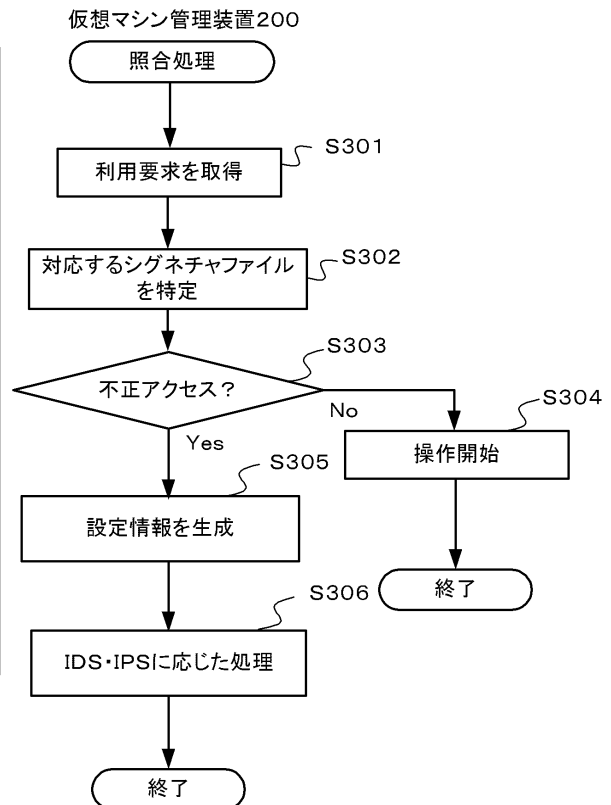


【図 5】

仮想シグネチャ管理DB

シグネチャ管理テーブル	
仮想マシン識別情報	シグネチャ ファイル
VM1	Sig1. rules Sig4. rules ...
VM2	Sig2. rules Sig3. rules
VM3	Sig1. rules
⋮	⋮
VMO	Sig1. rules Sig3. rules SigN. rules

【図 6】



フロントページの続き

審査官 岸野 徹

- (56)参考文献 特開2009-223778 (JP, A)
特開2007-011628 (JP, A)
特開2009-129332 (JP, A)
特開2011-160301 (JP, A)
特表2012-533104 (JP, A)
米国特許出願公開第2009/0158432 (US, A1)

- (58)調査した分野(Int.Cl., DB名)
G06F 21/56
G06F 21/53