

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2010年9月10日(10.09.2010)

(10) 国際公開番号
WO 2010/100769 A1

PCT

(51) 国際特許分類:
G06F 21/22 (2006.01)

(21) 国際出願番号: PCT/JP2009/054827

(22) 国際出願日: 2009年3月6日(06.03.2009)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人(米国を除く全ての指定国について): 株式会社日立製作所 (Hitachi, Ltd.) [JP/JP]; 〒1008280 東京都千代田区丸の内一丁目6-6 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人(米国についてのみ): 山口明彦 (YAMAGUCHI, Akihiko) [JP/JP]; 〒2448555 神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア事業部内 Kanagawa (JP). 紅山伸夫 (BENIYAMA, Nobuo) [JP/JP]; 〒2448555 神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア事業部内 Kanagawa (JP). 畠山敦 (HATAKEYAMA, Atsushi) [JP/JP]; 〒2448555 神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフト

ウェア事業部内 Kanagawa (JP). 齊藤恒太 (SAITO, Kota) [JP/JP]; 〒2448555 神奈川県横浜市戸塚区戸塚町5030番地 株式会社日立製作所ソフトウェア事業部内 Kanagawa (JP).

(74) 代理人: 大賀真司, 外 (OHGA, Shinji et al.); 〒1050022 東京都港区海岸1-2-20 汐留ビルディング3階サンネクスト国際特許事務所 Tokyo (JP).

(81) 指定国(表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

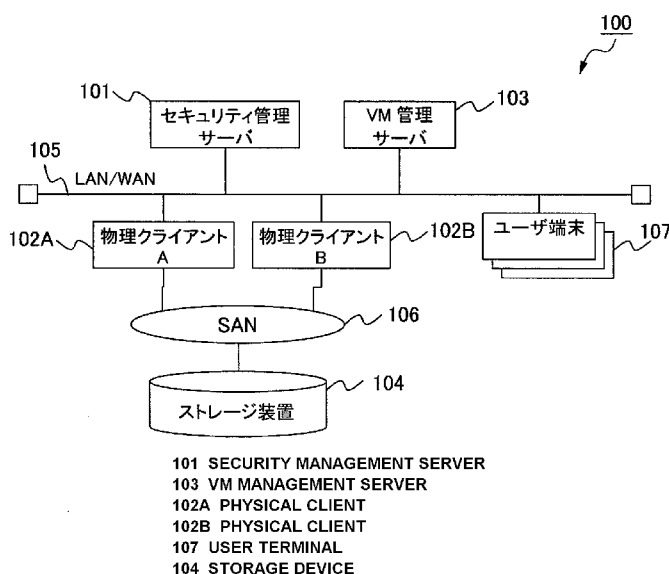
(84) 指定国(表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ

[続葉有]

(54) Title: SECURITY MANAGEMENT DEVICE AND METHOD

(54) 発明の名称: セキュリティ管理装置及び方法

図1



(57) Abstract: In case that as types of virtual machines provided to a user terminal by a physical client, there are a master virtual machine which is built according to master information constituting a part or overall of a virtual machine, and an individual virtual machine which is built according to individual information a part or overall of which is constituted by the master information, the security checks of a plurality of the virtual machines are executed selectively for the types of virtual machines corresponding to the contents of check items on the basis of every items.

(57) 要約: 物理クライアントがユーザ端末に提供する仮想マシンの種別として、仮想マシンの一部又は全部を構成するマスタ情報に基づき構築されるマスタ仮想マシンと、マスタ情報により一部又は全部が構成される個別情報に基づき構築される個別仮想マシンとが存在する場合に、複数の仮想マシンのセキュリティチェックを、チェック項目ごとに、当該チェック項目の内容に応じた種別の仮想マシンに対して選択的に実行するようにした。



(AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB,
GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL,
NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF,
CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD,
TG).

添付公開書類:

— 国際調査報告 (条約第 21 条(3))

明細書

セキュリティ管理装置及び方法

技術分野

- 5 本発明は、セキュリティ管理装置及び方法に関し、特に、複数の仮想クライアントが共通の構成をもつネットワークシステムにおいて当該複数の仮想クライアントに対するセキュリティ検査を実行するセキュリティ管理サーバに適用して好適なものである。

10 背景技術

- S O X法の施行などを背景に、企業によるコンプライアンス対応や、情報セキュリティ対策の強化が求められている。企業内の各個人が利用するクライアント端末においてもセキュリティ管理が重要となっており、ネットワークに接続されたクライアント端末（以下、これを単にクライアントと呼ぶ）
15 について常に最新のセキュリティ状態を把握及び監視したいというニーズが高まってきている。

- 従来、このようなニーズに答える技術として、ネットワークに接続されたクライアントのセキュリティ状態を監査する方法が、例えば特開2002-247033号公報（以下、これを特許文献1と呼ぶ）に開示されている。
20 また、ネットワークに接続された各クライアントの資産（インストールされたソフトウェアやパッチなど）がセキュアであるか否かを検査し、検査結果を集計して管理者に報告するソフトウェアが様々なベンダからリリースされている。

- 一方、T C O削減や運用管理容易化などの観点から、ソフトウェアで計算
25 機をエミュレーションし、仮想的な計算機環境、すなわち仮想マシンを提供する仮想化技術が普及している。仮想化技術を用いることにより、複数の仮

想マシン間で仮想マシンのマシンイメージを共有することが可能となる。この場合、共有するマシンイメージとの差分情報のみを仮想マシンごとに管理すればよい。

このような仮想化技術は、例えば、特許文献1や特開2006-221649号公報（以下、これを特許文献2と呼ぶ）などに開示されており、さらに、VMware（登録商標）社のLinked Clone技術（VMware（登録商標）View3パンフレット、http://www.vmware.com/files/pdf/view_brochure.pdf（以下、これを非特許文献1と呼ぶ）参照）や、NetApp（登録商標）社のFlexClone（登録商標）技術（NetApp（登録商標）社FlexClone（登録商標）データシート、<http://media.netapp.com/documents/ds-2837-0808-flexclone.pdf>（以下、これを非特許文献2と呼ぶ））など、様々なベンダよりかかる仮想化技術を用いた製品がリリースされている。また、仮想マシンをある物理マシンから別の物理マシンへマイグレーションさせる技術も、例えば特開2007-66265号公報において開示されている。

15

発明の開示

大規模なネットワーク環境ではセキュリティ検査対象のクライアント数が多いため、すべてのクライアントのセキュリティチェックを行うためには長時間を要し、各クライアントの最新のセキュリティ状態を把握することが困難である。

20

また近年の仮想化技術の普及に伴う仮想マシン数の増加により、管理対象のクライアント数が大幅に増加することが予想され、今後、ますます大規模なネットワーク環境における各仮想マシンの最新のセキュリティ状態を把握することが困難となる可能性がある。そのため、このようなネットワーク環境では、セキュリティチェックを高速に行うことが要求されている。

25

本発明は以上の点を考慮してなされたもので、セキュリティチェックを高

速かつ効率的に行い得るセキュリティ管理装置及び方法を提案しようとするものである。

- かかる課題を解決するため本発明においては、物理クライアントがユーザ端末に提供するそれぞれ仮想的な計算機環境である複数の仮想マシンのセキュリティを管理するセキュリティ管理装置において、前記複数の仮想マシン
- 5 に対するセキュリティチェックに関する 1 又は複数のチェック項目を規定したチェックポリシーと、セキュリティチェックプログラムとを記憶する記憶装置と、前記セキュリティチェックプログラムに基づき、前記チェックポリシーに従って、前記複数の仮想マシンに対するセキュリティチェックを実行する
- 10 CPU (Central Processing Unit) とを備え、前記仮想マシンの種別として、仮想マシンの一部又は全部を構成するマスタ情報に基づき構築されるマスタ仮想マシンと、前記マスタ情報により一部又は全部が構成される個別情報に基づき構築される個別仮想マシンとが存在し、前記 CPU は、前記セキュリティチェックを、前記チェック項目ごとに、当該チェック項目の内容に応じた種別の前記仮想マシンに対して選択的に実行することを特徴とする。
- 15

- また本発明においては、物理クライアントがユーザ端末に提供するそれぞれ仮想的な計算機環境である複数の仮想マシンのセキュリティを管理するセキュリティ管理方法において、前記複数の仮想マシンに対するセキュリティ
- 20 セキュリティ管理方法において、前記複数の仮想マシンに対するセキュリティチェックに関する 1 又は複数のチェック項目を規定したチェックポリシーと、セキュリティチェックプログラムとを記憶する第 1 のステップと、前記セキュリティチェックプログラムに基づき、前記チェックポリシーに従って、前記
- 25 複数の仮想マシンに対するセキュリティチェックを実行する第 2 のステップとを備え、前記仮想マシンの種別として、仮想マシンの一部又は全部を構成するマスタ情報に基づき構築されるマスタ仮想マシンと、前記マスタ情報により一部又は全部が構成される個別情報に基づき構築される個別仮想マシンとが存在し、前記第 2 のステップでは、前記セキュリティチェックを、前記

チェック項目ごとに、当該チェック項目の内容に応じた種別の前記仮想マシンに対して選択的に実行することを特徴とする。

本発明によれば、セキュリティチェックを、チェック項目ごとに、必要な種別の仮想マシンに対して選択的に実行することができるため、不要な種別
5 に対するセキュリティチェックを省略させることができる。かくするにつきセキュリティチェックを高速かつ効率的に行い得るセキュリティ管理システム及び方法を実現できる。

図面の簡単な説明

10 図1は、第1の実施の形態によるネットワークシステムの全体構成を示すブロック図である。

図2は、第1の実施の形態によるセキュリティ管理サーバの概略構成を示すブロック図である。

15 図3は、第1の実施の形態によるチェックポリシー管理テーブルの構成を示す図表である。

図4は、個別VM／マスタVM対応管理テーブルの構成を示す図表である。

図5は、チェック結果管理テーブルの構成を示す図表である。

図6は、クライアント管理テーブルの構成を示す図表である。

20 図7は、第1の実施の形態による物理クライアントの概略構成を示すブロック図である。

図8は、第1の実施の形態によるVM管理サーバの概略構成を示すブロック図である。

図9は、仮想マシン管理テーブルの構成を示す図表である。

図10は、物理マシン管理テーブルの構成を示す図表である。

25 図11は、第1の実施の形態によるネットワークシステムの論理構成を示すブロック図である。

図 1 2 は、第 1 の実施の形態によるセキュリティ管理制御処理の処理手順を示す P A D 図である。

図 1 3 は、第 1 の実施の形態の設定処理の処理手順を示す P A D 図である。

図 1 4 は、第 1 の実施の形態のチェックポリシー設定画面の構成例を示す概略図である。

図 1 5 は、第 1 の実施の形態の個別 V M / マスタ V M 対応設定画面の構成例を示す概略図である。

図 1 6 は、第 1 の実施の形態のセキュリティチェック処理の処理手順を示す P A D 図である。

10 図 1 7 は、V M 情報収集処理の処理手順を示す P A D 図である。

図 1 8 は、第 1 の実施の形態の動作例を示す図である。

図 1 9 は、第 2 の実施の形態によるネットワークシステムの全体構成を示すブロック図である。

図 2 0 は、第 2 の実施の形態による物理クライアントの構成を示すブロック図である。

図 2 1 は、第 2 の実施の形態によるネットワークシステムの論理構成を示す図である。

図 2 2 は、第 2 の実施の形態によるチェックポリシー管理テーブルの構成を示す図表である。

20 図 2 3 は、第 2 の実施の形態のセキュリティチェック処理の処理手順を示す P A D 図である。

図 2 4 は、第 3 の実施の形態によるネットワークシステムの全体構成を示すブロック図である。

図 2 5 は、第 3 の実施の形態によるセキュリティ管理サーバの構成を示す
25 ブロック図である。

図 2 6 は、第 3 の実施の形態による V M 管理サーバの構成を示すブロック

図である。

図 27 は、第 3 の実施の形態によるチェックポリシー設定画面の構成例を示す概略図である。

図 28 は、第 3 の実施の形態によるセキュリティ管理制御処理の処理手順を示す PAD 図である。

図 29 は、第 3 の実施の形態によるチェック対象設定処理の処理手順を示す PAD 図である。

図 30 は、第 4 の実施の形態によるネットワークシステムの全体構成を示すブロック図である。

10 図 31 は、第 4 の実施の形態によるセキュリティ管理サーバの構成を示すブロック図である。

図 32 は、チェック対象管理テーブルの構成を示す図表である。

図 33 は、第 4 の実施の形態のチェック対象設定処理の処理手順を示す PAD 図である。

15

発明を実施するための最良の形態

本発明の一実施の形態について図面について詳述する。

なお、以後の説明では「x x x テーブル」、「x x x リスト」、「x x x DB」、「x x x キュー」等の表現にて本発明の情報を説明するが、これら
20 情報は必ずしもテーブル、リスト、DB、キュー、等のデータ構造以外で表現されていてもよい。そのため、データ構造に依存しないことを示すために「x x x テーブル」、「x x x リスト」、「x x x DB」、「x x x キュー」等について「x x x 情報」と呼ぶことがある。

以後の説明では「プログラム」を主語として説明を行う場合があるが、
25 プログラムはプロセッサによって実行されることで定められた処理をメモリ及び通信ポート（通信制御装置）を用いながら行うため、プロセッサ（CPU）

を主語とした説明としてもよい。また、プログラムを主語として開示された処理は管理サーバ等の計算機、情報処理装置が行う処理としてもよい。また、プログラムの一部または全ては専用ハードウェアによって実現されてもよい。

また、各種プログラムはプログラム配布サーバや記憶メディアによって各
5 計算機にインストールされてもよい。

(1) 第1の実施の形態

(1-1) 本実施の形態によるネットワークシステムの構成

図1において、100は全体として本実施の形態によるネットワークシステムを示す。このネットワークシステム100では、セキュリティ管理サーバ101と、第1及び第2の物理クライアント102A、102Bからなる
10 物理クライアント群と、VM (Virtual Machine: 仮想マシン) 管理サーバ103と、ユーザ端末107とが例えばLAN (Local Area Network) 又はWAN (Wide Area Network) などから構成されるネットワーク105を介して相互に接続されている。また第1及び第2の物理クライアント102A、1
15 02Bには、SAN (Storage Area Network) 106を介してストレージ装置104に接続されている。なお本実施の形態では、簡単のために、物理クライアント群を第1及び第2の物理クライアント102A、102Bの2台のみから構成している場合について説明するが、物理クライアント群を構成する物理クライアントの台数が3台以上であっても本発明は適用可能である。

20 セキュリティ管理サーバ101は、例えばパーソナルコンピュータ、ワークステーション又はメインフレームなどから構成され、後述のように第1及び第2の物理クライアント102A、102B上で動作する各仮想マシンのセキュリティ状態を管理する。

第1及び第2の物理クライアント102A、102Bは、クライアントマシンとして利用される仮想マシン (以下、適宜、これを仮想クライアントと呼ぶ) をユーザ端末107に提供する。またVM管理サーバ103は、第1
25

及び第2の物理クライアント102A, 102A上で動作する仮想クライアントを管理する。

ストレージ装置104は、第1及び第2の物理クライアント102A, 102B上で動作する各仮想クライアントの構成情報（CPU（Central Processing Unit）、メモリ、通信装置及び記憶装置に格納されたデータなどの各情報）である複数又は単数のマシンイメージ情報320や、仮想クライアントが使用する各種データなどが格納される。

ユーザ端末107は、一般的なパーソナルコンピュータやシンクライアントなどから構成される端末装置であり、一般利用者が第1及び第2の物理クライアント102A, 102B上で動作する仮想クライアントを利用するために利用する。ユーザ端末107は、本実施の形態のセキュリティ管理方法によるセキュリティ管理の対象外である。

なお、セキュリティ管理サーバ101とVM管理サーバ103は1つの計算機から構成されていてもよく、また第1又は第2の物理クライアント102A, 102Bと同じ計算機であってもよい。またセキュリティ管理サーバ101に保持される各種プログラムや各種情報の一部又は全部を、1つ以上の（複数の）計算機に配置し、複数の計算機でセキュリティ管理サーバ101を実現する構成をとってもよい。同様に、1つ以上の（複数の）計算機でVM管理サーバ103を構築したり、1つ以上の（複数の）計算機で第1及び第2の物理クライアント102A, 102Bを構築するようにしてもよい。

また第1及び第2の物理クライアント102A, 102B上で動作する仮想マシンに対する命令や情報の入出力方法としては以下の（a）及び（b）の方法が考えられるが、これら以外であってもよい。

（a）第1及び第2の物理クライアント102A, 102Bが有するディスプレイやキーボード及び又はマウス等の入出力装置を対象として、当該入出力装置からの入力を仮想マシンに提供し、仮想マシンの出力（例えば表示及

び音声)をその入出力装置へ出力する。

(b) 第1及び第2の物理クライアント102A, 102Bとは別の計算機が有するディスプレイやキーボード及び又はマウス等の入出力装置を対象として、当該入出力装置からの入力を仮想マシンに提供し、仮想マシンの出力

5 (例えば表示及び音声)をその入出力装置へ出力する。

(1-2) セキュリティ管理サーバの構成

図2は、本実施の形態におけるセキュリティ管理サーバ101の具体的な構成を示す。セキュリティ管理サーバ101は、CPU201、主メモリ202、指示入力装置203、ディスプレイ204、外部記憶装置205及び
10 通信制御装置206を備え、これらがシステムバス207を介して相互に接続されることにより構成されている。

CPU201は、セキュリティ管理サーバ101全体の動作制御を司るプロセッサである。このCPU201が主メモリ202に格納された各種プログラムを実行することにより、セキュリティ管理サーバ101により後述の
15 ような処理が行われる。また主メモリ202は、各種プログラムや各種情報を保持するために用いられるほか、CPU201のワークメモリとしても用いられる。

指示入力装置203は、セキュリティ管理サーバ101に対する各種指示を入力するための装置であり、キーボード及び又はマウスなどから構成され
20 る。ディスプレイ204は、例えば液晶パネルやCRT (Cathode-Ray Tube) などから構成され、CPU201の制御のもとに、セキュリティ管理サーバ101による処理の実行状況や実行結果等を表示する。

外部記憶装置205は、例えばハードディスク装置から構成される大容量の記憶媒体であり、各種のプログラムやデータを保存するために用いられる。
25 外部記憶装置205に保存されたプログラムは、指示入力装置203からのプログラム起動命令などに応じて主メモリ202にロードされ、CPU20

1により実行される。通信制御装置206は、ネットワーク105を介して当該ネットワーク105に接続された他の装置と各種データやコマンドを交換するために用いられる。

5 なお、セキュリティ管理サーバ101は、指示入力装置203及びディスプレイ204以外の入出力装置を有してもよく、さらにこの入出力装置をセキュリティ管理サーバ101とは別の計算機が有してもよい。この場合、その計算機が有する入出力装置からの入力をセキュリティ管理サーバ101が受信したり、仮想クライアントVMの出力（例えば表示及び又は音声等）を当該計算機へ送信することによって、この計算機が有する入出力装置への出力
10 力を実現することが考えられる。

ここで本実施の形態によるセキュリティ管理サーバ101の外部記憶装置205に格納される主要なプログラムについて説明する。

本実施の形態の場合、上述のようにセキュリティ管理サーバ101は、第1及び第2の物理クライアント102A、102B上で動作する各仮想クライアントのセキュリティを管理する。そのための手段として、外部記憶装置
15 205には、図2に示すように、セキュリティ管理制御プログラム210、設定プログラム211、VM情報収集プログラム212、セキュリティチェックプログラム213及びOS214などのプログラムが格納される。

このうちセキュリティ管理制御プログラム210は、セキュリティ管理サーバ101の各種プログラムを制御するためのプログラムであり、設定プログラム211は、ユーザからの指示に従って各種設定を行うためのプログラムである。
20

またVM情報収集プログラム212は、VM管理サーバ103から仮想クライアントの管理情報を収集し、後述のクライアント管理テーブル223を作成又は更新するためのプログラムである。
25

さらにセキュリティチェックプログラム213は、クライアント管理テー

ブル 2 2 3 に登録された各クライアントに対するセキュリティチェックを行うためのプログラムである。OS 2 1 4 は、周辺装置との間のデータの入出力など、コンピュータ上で各プログラムを実行するための基本機能を提供する。

- 5 次に、外部記憶装置 2 0 5 に格納される主要な情報について説明する。これに際して、まず「マスタ情報」、「マスタ VM」、「個別カスタマイズ情報」及び「個別 VM」という用語について定義する。

以下において、「マスタ情報」とは、個別の仮想マシン（仮想クライアント）や、個別の利用者の環境で、個別にカスタマイズした部分を除く、仮想
10 マシンを構成する情報のことをいうものとする。仮想マシンを構成する情報とは、マシンイメージの一部又は全部を指す。またマシンイメージとは、仮想マシンの CPU、メモリ及び通信制御装置などのハードウェアの仕様や個数や量、BIOS の設定、及び、仮想マシンのディスクをエミュレーション
15 するディスクイメージなどを含んで構成される、仮想マシンを起動するために必要な各種情報を指す。なお、同じマスタ情報を持つ複数の仮想マシンにとって、マスタ情報は、仮想マシンを構成する情報の共通部分となる。

また「マスタ VM」とは、マスタ情報に対するセキュリティチェックを行う対象となる仮想マシンのことをいう。

さらに「個別カスタマイズ情報」とは、マスタ情報をベースとして個別に
20 仮想マシンをカスタマイズした場合において、個別にカスタマイズした部分の情報をいう。例えば、利用者毎にカスタマイズしたデスクトップ環境や利用者のプロファイルに関する情報、及び、特別な用途の仮想マシン（仮想クライアント）に個別にインストールしたソフトウェアの情報などがこれに該当する。

25 さらに「個別 VM」とは、個別カスタマイズ情報に対するセキュリティチェックを行う対象となる仮想マシンのことをいう。

「マスタ情報」及び「個別カスタマイズ情報」の具体例について説明する。

例えば、あるソフトウェアAをインストール済みの仮想マシンAのマシンイメージをコピーし、当該仮想マシンAと同じ構成の仮想マシンBを生成した後、当該仮想マシンBにソフトウェアBをインストールした場合、ソフトウェアAを含む仮想マシンAのマシンイメージがマスタ情報、ソフトウェアBを含む仮想マシンBで個別にカスタマイズした部分、すなわち仮想マシンBのマシンイメージにおける仮想マシンAのマシンイメージとの差分が個別カスタマイズ情報である。

また、他の例として、複数の仮想マシンで共通に利用する、仮想マシンを構成する情報に基づいて複数の仮想マシンを起動し、仮想マシンごとの差分情報を個別管理する仮想化技術(例えば特開2006-221649号公報)において、「複数の仮想マシンで共通に利用する仮想マシンを構成する情報」が「マスタ情報」に該当し、「仮想マシンごとの差分情報」が個別カスタマイズ情報に該当する。

セキュリティ管理サーバ101の外部記憶装置205に格納される主要な情報の説明に戻る。本実施の形態の場合、セキュリティ管理サーバ101が第1及び第2の物理クライアント102A、102B上で動作する各仮想クライアントのセキュリティを管理する手段として、外部記憶装置205には、図2に示すように、チェックポリシー管理テーブル220、個別VM/マスタVM対応管理テーブル221、チェック結果管理テーブル222及びクライアント管理テーブル223などが格納される。

チェックポリシー管理テーブル220は、第1及び第2の物理クライアント102A、102B上で動作する仮想クライアントに対して実行すべきセキュリティチェックのポリシーを管理するためのテーブルであり、図13及び図14について後述するように図14に示すチェックポリシー設定画面500を用いた管理者の設定操作に応じて設定プログラム211により作成される。

このチェックポリシ管理テーブル 220 は、図 3 に示すように、チェック事項欄 220 A、ID 欄 220 B、詳細欄 220 C、チェック対象欄 220 D、重要度欄 220 E 及びチェック期限欄 220 F から構成される。

そしてチェック事項欄 220 A には、予め固定的に規定されているセキュリティチェックを実行すべき事項（以下、これをチェック事項と呼ぶ）の名称が格納される。

本実施の形態の場合、かかるチェック事項としては、所定の更新プログラムを適用しているか否かを判定する「更新プログラムの判定」、ウィルス対策製品をインストールしているか否かを判定する「ウィルス対策製品の判定」、インストール禁止の不正ソフトウェアをインストールしていないか否かを判定する「不正ソフトウェアの判定」、必ずインストールすべきソフトウェアをインストールしているか否かを判定する「必須ソフトウェアの判定」、及び、適切なセキュリティ設定を行っているか否かを判定する「セキュリティ設定の判定」の 5 つがある。ただし、チェック事項の数及び内容はこれに限られない。

また詳細欄 220 C には、対応するチェック事項内の詳細項目が格納される。例えば図 3 の場合、「更新プログラム」に関しては、チェック対象の仮想マシンが「パッチ A」、「パッチ B」、……を適用しているか否かをそれぞれチェックすべきことが規定され、「ウィルス対策製品」に関しては、「2008/1/1」にウィルス定義された「ウィルスチェッカー A」のバージョン「1.0」、「2008/1/1」にウィルス定義された「ウィルスチェッカー B」のバージョン「1.0」、……のいずれかがインストールされているか否かをチェックすべきことが規定されている。

以下においては、チェック事項内のセキュリティチェックすべき各詳細項目をそれぞれチェック項目と呼ぶものとする。例えば、「更新プログラム」というチェック事項に関しては、「パッチ A」、「パッチ B」、……を適用

しているか否かのチェックがそれぞれチェック項目に該当する。また「不正ソフトウェア」というチェック事項に関しては、「ソフトウェアX」のバージョン「2.0」、「ソフトウェアY」の全バージョン、……がそれぞれインストールされているか否かのチェックがそれぞれチェック項目に該当する。な

- 5 お、「ウィルス対策製品」というチェック事項に関しては、詳細欄 2 2 0 C に挙げられたウィルス対策製品のうちのいずれかがインストールされているか否かというチェックが1つのチェック項目となる。

- I D 欄 2 2 0 B には、対応するチェック項目に対して付与された I D が格納される。図 3 の場合、例えば「更新プログラム」というチェック事項の「パッチ A」というチェック項目については「C1-01」という I D が付与され、「更新プログラム」というチェック事項の「パッチ B」というチェック項目については「C1-02」という I D が付与されている。
- 10

- さらにチェック対象欄 2 2 0 D には、対応するチェック項目についてセキュリティチェックを実行すべき対象が格納される。具体的に、チェック対象
- 15 欄 2 2 0 D には、「マスタ」、「個別」、「マスタ or 個別」及び「マスタ and 個別」のいずれかが格納される。「マスタ」はマスタ VM のみがチェックに合格すればよいことを表し、「個別」は個別 VM のみがチェックに合格すればよいことを表す。また「マスタ or 個別」は、マスタ VM 及び個別 VM のいずれか一方がチェックに合格すればよいことを表し、「マスタ and 個別」
- 20 は、マスタ VM 及び個別 VM の双方がチェックに合格する必要があることを表す。

- 例えば、あるソフトウェアをマスタ VM にインストールして配布する場合、マスタ VM にインストールされていれば、そのソフトウェアは個別 VM にもインストールされているため、該当ソフトウェアのインストール状況を判定
- 25 するチェック項目についてはチェック対象として「マスタ」が指定される。

「マスタ」が指定された場合、そのチェック項目については、マスタ VM に

対してのみセキュリティチェックが行われ、そのチェック結果が該当マスタVMだけでなく、該当マスタVMと関連するすべての個別VMのチェック結果として採用される。

またセキュリティ設定を個人で不正に変更していないか、というようなチェック項目については、チェック対象として「個別」が設定される。「個別」が設定された場合、そのチェック項目については、個別VMに対してのみセキュリティチェックが行われ、そのチェック結果がその個別VMのチェック結果として採用される。なお、このチェック項目について、マスタVMはチェック対象外となる。

- 10 重要度欄 220Eには、対応するチェック項目について設定された重要度が格納される。本実施の形態の場合、かかる重要度としては、「高」、「中」又は「低」のいずれかが設定される。なお、重要度として設定される値は、チェック項目の重要度を表す値であれば、他の値でも構わない。

- 15 このうち「高」は、システムの空きリソース不足などの問題がない限り、できる限り迅速にチェックを行うべきことを表す。また「中」は、チェック期限内であれば、チェック対象の仮想クライアントの利用者の邪魔をしないよう、仮想クライアントが未使用時に、空きリソース上で該当仮想クライアントを起動してチェックを行うべきことを表す。

- 20 さらに「低」は、「中」と同様に、チェック期限内であれば、仮想クライアントが未使用時に空きリソース上で該当仮想クライアントを起動してチェックを行うが、システムの空きリソース量が残り少ないなど、該当仮想クライアントを起動することにより、他の仮想クライアントへの悪影響が懸念される場合には、チェックを抑制してもよい。本実施の形態では、システムの空きリソース量が、該当仮想クライアントを起動すると、それ以上の仮想ク
25 ライアントを起動できない場合には、空きリソース量が十分になるまで、チェックを行わないことを表す。

なお、重要度が「中」又は「低」に設定されたいずれのチェック項目についても、後述するチェック期限を経過した場合には、できる限り迅速にセキュリティチェックを行う。

5 なお、本実施の形態の場合、「高」、「中」、「低」は、上記の意味を示すものとしたが、システムの状況と、チェック項目ごとの重要度の値に応じて、該当チェック項目のチェック処理をすぐに行うか、後で行うかを判断するための材料であれば、他の意味でもよい。

10 さらにチェック期限欄 220F には、対応するチェック項目について設定されたセキュリティチェックを実行すべき期限（以下、これをチェック期限と呼ぶ）が格納される。

このチェックポリシー管理テーブル 220 は、セキュリティチェックプログラム 213 が各仮想クライアントに対するセキュリティチェックを実行する際に参照される。

15 一方、個別 VM / マスタ VM 対応管理テーブル 221 は、各仮想クライアント（個別 VM）と、当該仮想クライアントのマスタ情報をチェックするための仮想クライアント（マスタ VM）との対応関係を管理するためのテーブルであり、図 13 及び図 15 について後述するように、図 15 に示す個別 VM / マスタ VM 対応設定画面 600 を用いた管理者の設定操作に応じて設定プログラム 211 により各エントリが登録される。ただし、個別 VM とマスタ VM との対応関係は VM 管理サーバ 103 においても管理しているため、
20 この情報を設定プログラム 211 が VM 管理サーバ 103 から定期的に取得し、個別 VM / マスタ VM 対応管理テーブル 221 を自動更新するようにしてもよい。

25 この個別 VM / マスタ VM 対応管理テーブル 221 は、図 4 に示すように、クローン VM 欄 221A 及びマスタ VM 欄 221B から構成される。そしてクローン VM 欄 221A には対応する仮想クライアントに対して付与された

I D（以下、これをマシン I Dと呼ぶ）が格納され、マスタ V M欄 2 2 1 B には対応するマスタ V Mのマシン I Dが格納される。

他方、チェック結果管理テーブル 2 2 2 は、個別 V M及びマスタ V Mに対するセキュリティチェックのチェック結果を管理するためのテーブルであり、

5 図 5 に示すように、C I D欄 2 2 2 A、マシン I D欄 2 2 2 B 及び複数の I D欄 2 2 2 C から構成される。

そして C I D欄 2 2 2 A には、そのチェック期限のセキュリティチェックに対して付与された識別情報（C I D）が格納される。またマシン I D欄 2 2 2 B には、セキュリティチェックを行った対応する仮想クライアントのマシン I Dが格納される。

10

さらに各 I D欄 2 2 2 C は、それぞれ図 3 について上述した各チェック項目に対して付与された I D（I D欄 2 2 0 B 参照）にそれぞれ対応付けられており、これら I D欄 2 2 2 C には、それぞれ対応するセキュリティチェックの際に対応する仮想クライアントについて実行したセキュリティチェック

15 のチェック結果が格納される。

例えば図 5 において、「○」はそのチェック期限のその仮想マシンのそのチェック項目に関するセキュリティチェックに合格したことを表し、「×」は、かかるセキュリティチェックに不合格であったことを表し、「—」は、かかるセキュリティチェックの対象外であることを表している。また「未」は、かかるセキュリティチェックが未だ行われていない（未チェック）であることを表す。また図 5 において、破線 2 2 2 D で囲まれた行は、マスタ V Mに対するセキュリティチェックのチェック結果の例を表し、破線 2 2 2 E、2 2 2 F 及び 2 2 2 G でそれぞれ囲まれたエリアは、マスタ V Mに対するセキュリティチェックのチェック結果を個別 V Mにも反映した結果を表している。

25

なお仮想クライアントに対するセキュリティチェックのチェック方法とし

ては、WMI (Windows (登録商標) Management Instrumentation) やSSH (Secure SHell) を用いて採取した情報をもとにセキュリティの対策状況をチェックするエージェントレス方式や、仮想クライアント上で稼動するエージェントから情報を取得してセキュリティの対策状況をチェックする方式
5 など様々な方法があるが、本実施の形態においては、いずれの方法でも採用可能である。

他方、クライアント管理テーブル223は、セキュリティ管理サーバ101において第1及び第2の物理クライアント102A、102B上で動作するセキュリティチェック対象の仮想クライアントを管理するためのテーブル
10 であり、VM管理サーバ103の仮想マシン管理テーブル420から読み出した各仮想マシンの管理情報がそれぞれ格納される。

實際上、このクライアント管理テーブル223は、図6に示すように、マシンID欄223A、IPアドレス欄223B、対応物理マシンID欄223C及びリソース情報欄223Dから構成される。

15 そしてマシンID欄223Aには、システム上に存在する仮想クライアント及び物理クライアントに対してそれぞれ付与されたマシンIDが格納され、IPアドレス欄223Bには、その仮想クライアント又は物理クライアントにアクセスするためのIPアドレスが格納される。

また対応物理マシンID欄223Cには、対応する仮想マシンが仮想クライアントである場合にその仮想クライアントが動作している物理クライアント(第1又は第2の物理クライアント102A、102B)に対して付与された識別情報(物理マシンID)が格納される。
20

リソース情報欄223Dは、CPU欄223DA、メモリ欄223DB及びディスク欄223DCなどから構成されており、これらCPU欄223DA、メモリ欄223DB及びディスク欄223DCには、それぞれ対応する
25 仮想クライアント又は物理クライアントに割り当てられているCPU、メモ

リ及びディスクなどのリソースのリソース量が格納される。ただし、このリソース情報欄 223D は省略してもよい。

なお、以上のチェックポリシー管理テーブル 220、個別VM/マスタVM 対応管理テーブル 221、チェック結果管理テーブル 222 及びクライアント管理テーブル 223 は、プログラムが動的に生成や更新を行うため、プログラムの起動前から外部記憶装置 205 内に存在している必要はない。またこれらのテーブルを、外部記憶装置 205 ではなく、初期時より主メモリ 202 において保持するようにしてもよい。

(1-3) 物理クライアントの構成

10 続いて、第1及び第2の物理クライアント 102A、102B の構成について説明する。なお、第2の物理クライアント 102B は、第1の物理クライアント 102A と同じ構成を有するため、ここでは第1の物理クライアント 102A の構成のみを説明することとし、第2の物理クライアント 102B の構成については説明を省略する。

15 図7は、第1の物理クライアント 102A の概略構成を示す。この図7に示すように、第1の物理クライアント 102A は、CPU 301、主メモリ 302、外部記憶装置 303、通信制御装置 304 及びホストバスアダプタ (HBA) 305 がシステムバス 306 を介して相互に接続されることにより構成されている。

20 CPU 301 は、第1の物理クライアント 102A 全体の動作制御を司るプロセッサである。このCPU 301 が主メモリ 302 に格納された各種プログラムを実行することにより、第1の物理クライアント 102A によって、ユーザ端末 107 への仮想クライアントの提供を含む各種処理が行われる。また主メモリ 302 は、かかる各種プログラムや各種情報を保持するために
25 用いられるほか、CPU 301 のワークメモリとしても用いられる。

通信制御装置 304 は、ネットワーク 105 に接続された他の装置と当該

ネットワーク 105 を介して各種データやコマンドを交換するための通信制御機能を備える。またホストバスアダプタ 305 は、SAN 106 を介してストレージ装置 104 に対するデータの読み書きを行うための通信制御機能を備える。

- 5 外部記憶装置 303 は、例えばハードディスク装置から構成される大容量の記憶媒体であり、ハイパバイザプログラム 310 を含む各種プログラムを保持するために用いられる。

ハイパバイザプログラム 310 は、ストレージ装置 104 に格納されているマシンイメージ情報 320 に基づき、CPU 301、主メモリ 302、外部記憶装置 303 及び通信制御装置 304 を含む第 1 の物理クライアント 102A のハードウェア資源を用いて仮想クライアントを動作させるためのプログラムである。なお「マシンイメージ情報」とは、仮想クライアントの CPU、メモリ及び通信制御装置などのハードウェアの仕様や個数や量、BIOS の設定、及び、仮想マシンのディスクをエミュレーションするディスクイメージなどを含んで構成される、各ユーザ端末 107 にそれぞれ提供する仮想クライアントを起動するために必要な各種情報のことをいう。

またハイパバイザプログラム 310 は、性能情報取得機能 311 を備える。性能情報取得機能 311 は、ネットワーク 105 経由で第 1 の物理クライアント 102A の CPU 利用率やメモリ使用量を取得できる機能である。この性能情報取得機能 311 による情報の取得方法としては、例えば、SNMP (Simple Network Management Protocol) エージェントによる MIB (Management Information Base) 情報を提供する方法や、WMI などの管理用のインタフェースを備える方法、又は SSH を利用してリモートで性能情報取得コマンドを実行する方法などがある。

- 25 ストレージ装置 104 には、ハイパバイザプログラム 310 が使用する、仮想マシン（仮想クライアント）のマシンイメージ情報 320 が格納されて

いる。ストレージ装置 104 は、SAN 106 を介して第 1 及び第 2 の物理クライアント 102A、102B と接続されており、マシンイメージ情報 320 は、第 1 又は第 2 の物理クライアント 102A、102B 上で稼動するいずれのハイパバイザプログラム 310 から参照可能である。本実施の形態の場合、マシンイメージ情報 320 は、複製可能な単数又は複数のファイルから構成される。

ハイパバイザプログラム 310 は、マシンイメージ情報 320 を読み込み、仮想マシンに割り当てるリソース量（CPU 処理時間、メモリ容量、ディスク容量など）や、エミュレーションするハードウェア（CPU や通信制御装置など）を決定し、仮想マシンに割り当てるリソース量の制御や、エミュレーションするハードウェアに対する命令を、第 1 及び第 2 の物理クライアント 102A、102B の各種ハードウェア資源に対する命令に変換することにより、仮想マシン（仮想クライアント）をエミュレーションする。またハイパバイザプログラム 310 は、マシンイメージ情報 320 内のディスクイメージに格納された OS 及びアプリケーションなどのプログラムや、各種設定情報及び又はユーザデータなどを読み込み、仮想マシン上で稼動する各種ソフトウェアを実行する。さらにハイパバイザプログラム 310 は、一般的な OS と同様に、ネットワーク 105 経由で、外部記憶装置 303 又はストレージ装置 104 に格納された各種ファイルをコピーする機能を備える。

（1-4）VM 管理サーバの構成

図 8 は、本実施の形態における VM 管理サーバ 103 の概略構成を示す。VM 管理サーバ 103 は、CPU 401、主メモリ 402、指示入力装置 403、ディスプレイ 404、外部記憶装置 405 及び通信制御装置 406 を備え、これらがシステムバス 407 を介して相互に接続されることにより構成されている。

CPU 401 は、VM 管理サーバ 103 全体の動作制御を司るプロセッサ

である。このCPU 401が主メモリ402に格納された各種プログラムを実行することにより、VM管理サーバ103により後述のような処理が行われる。また主メモリ402は、各種プログラや各種データを保持するために用いられるほか、CPU 401のワークメモリとしても用いられる。

5 指示入力装置403は、セキュリティ管理サーバ101に対する各種指示を入力するための装置であり、キーボード及び又はマウスなどから構成される。ディスプレイ404は、例えば液晶パネルやCRTなどから構成され、CPU 401の制御のもとに、VM管理サーバ103による処理の実行状況や実行結果等を表示する。

10 外部記憶装置405は、例えばハードディスク装置から構成される大容量の記憶媒体であり、各種のプログラムやデータを保存するために用いられる。外部記憶装置405に保存されたプログラムは、指示入力装置403からのプログラム起動命令などに応じて主メモリ402にロードされ、CPU 401により実行される。通信制御装置406は、ネットワーク105を介して
15 当該ネットワーク105に接続された他の装置と各種データやコマンドを交換するために使用する。

ここで、本実施の形態によるVM管理サーバ103の外部記憶装置405に格納される主要なプログラムについて説明する。

本実施の形態の場合、上述のようにVM管理サーバ103は、第1及び第
20 2の物理クライアント102A、102A上で動作する仮想クライアントを管理する。そのための手段として、外部記憶装置405には、図8に示すように、VM管理プログラム410、VM移動プログラム411及び管理情報参照プログラム412などのプログラム群と、仮想マシン管理テーブル420及び物理マシン管理テーブル421が格納される。

25 このうちVM管理プログラム410は、指示入力装置403を用いた利用者からの指示やネットワーク105経由での他のプログラムからの指示に従

って仮想マシンの生成、削除、起動又は停止などを行い、その結果に基づき、仮想マシン管理テーブル420に各仮想マシンの管理情報や状態を登録するプログラムである。またVM管理プログラム410は、既存の仮想マシンのマシンイメージの一部又は全部の複製や、それに準ずる技術により、既存の

5 仮想マシンと同様の構成の仮想マシンを作成する機能を持つプログラムである。かかる仮想マシンの作成は、例えば指示入力装置403を用いたマシンイメージの複製命令に応じて、ネットワーク105経由でハイパバイザプログラム310に対してマシンイメージを構成するファイルのコピーを指示することにより実現される。

- 10 VM移動プログラム411は、指示入力装置403を用いた利用者からの指示や、ネットワーク105経由での他のプログラムからの指示に従って、ある物理マシン上の仮想マシンを別の物理マシンに移動させるプログラムである。

- 管理情報参照プログラム412は、指示入力装置403を用いた利用者からの指示や、ネットワーク105経由での他のプログラムからの指示に従い、
- 15 仮想マシン管理テーブル420及び物理マシン管理テーブル421の情報を返すプログラムである。

- 仮想マシン管理テーブル420は、VM管理サーバ103の管理対象の各仮想マシンについて、当該仮想マシンの識別情報、IPアドレス、当該仮想
- 20 マシンが稼働させる物理クライアント（第1又は第2の物理クライアント102A、102B）の識別情報、必要リソース量（当該仮想マシンに割り当てるCPUやメモリなどのリソース量）、及び、状態（「起動中」や「停止中」など）を含む各種管理情報を管理するために用いられる。

- 實際上、この仮想マシン管理テーブル420は、図9に示すように、マシンID欄420A、IPアドレス欄420B、対応物理マシンID欄420
- 25 C、状態欄420D及びリソース情報欄420Eなどから構成される。そし

てこれらマシンID欄420A、IPアドレス欄420B及び対応物理マシンID欄420Cには、図6について上述したクライアント管理テーブル223のエントリのうち、仮想クライアントに対応するエントリの実マシンID欄223A、IPアドレス欄223B又は対応物理マシンID欄223Cと同じ情報が格納される。また状態欄420Dには、対応する仮想マシンのそのときの状態（起動又は停止）を表す値が格納される。

さらにリソース情報欄420Eは、CPU欄420EA、メモリ欄420EB及びディスク欄420ECなどから構成されており、これらCPU欄420EA、メモリ欄420EB及びディスク欄420ECなどには、それぞれ図6のクライアント管理テーブル223の対応するCPU欄223DA、メモリ欄223DB又はディスク欄223DCなどに格納されている情報と同じ情報が格納される。

また物理マシン管理テーブル421は、ネットワーク105に接続された物理マシン（本実施の形態においては第1及び第2の物理クライアント102A、102B）を管理するためのテーブルであり、図10に示すように、マシンID欄421A、IPアドレス欄421B及びリソース情報欄421Cから構成される。

そしてマシンID欄421Aには、対応する物理マシンに付与された識別情報が格納され、IPアドレス欄421Bには、その物理マシンのIPアドレスが格納される。またリソース情報欄421Cは、CPU情報欄421CA、メモリ情報欄421CB及びディスク情報欄421CCなどから構成され、これらCPU情報欄421CA、メモリ情報欄421CB及びディスク情報欄421CC等には、対応する物理マシンに搭載されたCPU、メモリ及びディスク等のスペックが格納される。

（1－5）論理構成及び設定内容

続いて、本実施の形態によるネットワークシステム100の論理構成につ

いて説明する。図 1 1 は、本実施の形態におけるネットワークシステム 1 0 0 の論理構成例を示す。

第 1 の物理クライアント 1 0 2 A のハイパバイザプログラム 3 1 0 A 上には、第 1 ～第 4 の仮想クライアント VM 1 ～VM 4 が存在し、これら第 1 ～
5 第 4 の仮想クライアント VM 1 ～VM 4 の状態は、第 1 ～第 3 の仮想クライアント VM 1 ～VM 3 が起動中、第 4 の仮想クライアント VM 4 が停止中となっている。また第 2 の物理クライアント 1 0 2 B のハイパバイザプログラム 3 1 0 B 上には、一つの仮想クライアントも存在しない。

一方、ストレージ装置 1 0 4 には、第 1 ～第 4 の仮想クライアント VM 1
10 ～VM 4 のマシンイメージが格納されている。第 2 ～第 4 の仮想クライアント VM 2 ～VM 4 のマシンイメージは、第 1 の仮想クライアント VM 1 のマシンイメージの複製により生成したものである。マシンイメージの複製は、例えば、管理者が VM 管理サーバ 1 0 3 を用いて、ネットワーク 1 0 5 経由でハイパバイザプログラム 3 1 0 A に対して、マシンイメージを構成するフ
15 ァイルのコピーを指示することにより実現される。

なお、第 1 の仮想クライアント VM 1 は、管理者が、一般利用者へ提供する仮想クライアントを生成する際に、スクラッチから仮想マシンを構築せずに済むよう、マシンイメージ情報 3 2 0 を複製して新規の仮想クライアントを生成するために使用する。

20 第 2 ～第 4 の仮想クライアント VM 2 ～VM 4 は、一般利用者が使用する仮想マシンであり、これら第 2 ～第 4 の仮想クライアント VM 2 ～VM 4 は、一般利用者の手によって、カスタマイズされている。ただし、本実施の形態では、第 1 の仮想クライアント VM 1 のディレクトリやファイルに対するユーザ権限の設定や OS の設定（レジストリの設定など）などにより、一般利
25 用者が可能なカスタマイズ可能な項目は、以下の（A）～（C）に制限されているものとする。

(A) 個人のデスクトップ環境の設定 (壁紙やスクリーンセーバの設定など)

(B) 個人のプロフィール情報 (個人のパスワードなど)

(C) ユーザ権限でアクセス可能な特定のディレクトリへのユーザファイルの作成、変更、削除又は外部から取り込んだファイルの配置 (過半媒体やネットワーク 1 0 5 経由でのマシン外部から取り込んだファイルの配置)

VM管理サーバ 1 0 3 の仮想マシン管理テーブル 4 2 0 (図 9) には、第 1 ~ 第 4 の仮想クライアント VM 1 ~ VM 4 に関する情報が登録されている。また物理マシン管理テーブル 4 2 1 (図 1 0) には、第 1 及び第 2 の物理クライアント 1 0 2 A, 1 0 2 B に関する情報が登録されている。

10 さらにセキュリティ管理サーバ 1 0 1 の個別 VM / マスタ VM 対応管理テーブル 2 2 1 (図 8) には、第 2 ~ 第 4 の仮想クライアント VM 2 ~ VM 4 のマスタ VM が第 1 の仮想クライアント VM 1 であるという情報がそれぞれ登録されている。

(1 - 6) 処理手順

15 続いて、本実施の形態による仮想クライアントのセキュリティ管理方法に関する各プログラムの処理の手順について説明する。なお、以下においては、各種処理の主体を「プログラム」として説明するが、実際には対応する CPU 2 0 1, 3 0 1, 4 0 1 がその「プログラム」に基づいてその処理を実行することは言うまでもない。

20 (1 - 6 - 1) セキュリティ管理制御プログラムの処理

まず、セキュリティ管理サーバ 1 0 1 (図 2) のセキュリティ管理制御プログラム 2 1 0 (図 2) の処理について説明する。図 1 2 は、本実施の形態におけるセキュリティ管理制御プログラム 2 1 0 により実行されるセキュリティ管理制御処理の処理手順を示す。

25 セキュリティ管理制御プログラム 2 1 0 は、指示入力装置 2 0 3 からのセキュリティチェックの開始指示コマンド等により起動されると、まず VM 管

理サーバ 103 の管理情報参照プログラム 412 から第 1 及び第 2 の物理クライアント 102 A, 102 B 上で動作する各仮想クライアントに関する情報を取得し、取得した各仮想クライアントに関する情報をクライアント管理テーブル 223 に格納する (SP100)。

5 続いてセキュリティ管理制御プログラム 210 は、チェックポリシー管理テーブル 220 にチェックポリシーが登録済みであるか否かを判定する (SP101)。そしてセキュリティ管理制御プログラム 210 は、この判定において否定結果を得ると、チェックポリシーの設定を促すメッセージをディスプレイ 204 に出力してこのセキュリティ管理制御処理を終了する (SP109)。

10 これに対してセキュリティ管理制御プログラム 210 は、ステップ SP101 の判定において肯定結果を得ると、一連のセキュリティチェック処理 (SP104 の繰り返し処理によって、全チェック項目のチェックが完了するまでの一連の処理) ごとの一意的識別情報であるチェック ID (図 5 の CID) を生成する (SP102)。このチェック ID は、チェック結果管理テーブル 222 内に格納されたチェック結果が、今回のセキュリティチェックの
15 チェック結果であるか否かを判断するために用いる。チェック ID は、一意であればよく、GUID (Global Unique Identifier) などの一意であることが保障される文字列データであっても、連番の数値データであっても、他の形式のデータであっても構わない。続いてセキュリティ管理制御プログラム
20 210 は、現在の日時を OS 214 から取得し、メモリ 202 に保存する (SP103)。

この後、セキュリティ管理制御プログラム 210 は、チェックポリシーに設定されたすべてのチェック項目のチェックが完了するまで、以下に説明するステップ SP105 〜 ステップ SP108 の処理を繰り返し実行する (SP
25 104)。

すなわちセキュリティ管理制御プログラム 210 は、セキュリティチェッ

クプログラム 2 1 3 を実行し、各仮想クライアントに対するセキュリティチェックを行う (S P 1 0 5)。なお、セキュリティチェックプログラム 2 1 3 を実行する際、プログラムの引数などにより、ステップ S P 1 0 2 で作成したチェック I D と、ステップ S P 1 0 3 で取得した日時データと、ステップ S P 1 0 4 の繰り返し処理におけるインターバル時間 (= T とする) を渡す。本実施の形態では、インターバル時間の値は、システムで定めた固定値 T とするが、チェックポリシーの一項目として管理者が指定する構成としてもよい。

続いて、セキュリティ管理制御プログラム 2 1 0 は、チェック結果管理テーブル 2 2 2 を確認し、まだチェックが完了していないチェック項目が残っているか否かを判定する (S P 1 0 6)。

セキュリティ管理制御プログラム 2 1 0 は、この判定において肯定結果を得ると、一定時間 (= T) の間待った (S P 1 0 7) 後にステップ S P 1 0 4 に戻り、この後ステップ S P 1 0 6 において否定結果を得るまで、ステップ S P 1 0 4 〜ステップ S P 1 0 7 の処理を繰り返す。

そしてセキュリティ管理制御プログラム 2 1 0 は、やがてすべてのチェック項目のセキュリティチェックが完了することによりステップ S P 1 0 6 において否定結果を得ると、このセキュリティ管理制御処理を終了する (S P 1 0 8)。

20 (1-6-2) 設定プログラムの処理

一方、図 1 3 は、セキュリティ管理サーバ 1 0 1 (図 2) の設定プログラム 2 1 1 により実行される設定処理の処理手順を示す。設定プログラム 2 1 1 は、指示入力装置 2 0 3 からの設定プログラムの開始指示コマンド等により起動されると、そのとき何らかの設定をしようとする項目 (以下、これを設定対象項目と呼ぶ) の指定を促すメッセージをディスプレイ 2 0 4 上に表示し、管理者により設定対象項目が指定されるのを待ち受ける (S P 2 0 0)。

そして設定プログラム 211 は、やがて設定対象項目が指定されると、そのとき指定された設定対象項目が「チェックポリシーの設定」及び「個別 VM とマスタ VM との対応関係の設定」のいずれであるかを判定する（S P 2 0 1）。

- 5 そして設定プログラム 211 は、ステップ S P 2 0 1 の判定において、そのとき指定された設定対象項目が「チェックポリシーの設定」であると判定した場合には、チェックポリシーを設定するための所定の G U I 画面（以下、これをチェックポリシー設定画面と呼ぶ）をディスプレイ 204 に表示する。かくして管理者は、このチェックポリシー設定画面を用いて所望のチェックポリ
10 シを設定することができる。そして設定プログラム 211 は、このとき管理者により設定されたチェックポリシーをチェックポリシー管理テーブル 220 に格納し（S P 2 0 2）、この後この設定処理を終了する。

- また設定プログラム 211 は、ステップ S P 2 0 1 の判定において、そのとき指定された設定対象項目が「個別 VM とマスタ VM との対応関係の設定」
15 であると判定した場合には、個別 VM とマスタ VM との対応関係を設定するための所定の G U I 画面（以下、これを個別 VM / マスタ VM 対応設定画面と呼ぶ）をディスプレイ 204 に表示する。かくして管理者は、この個別 V
M / マスタ VM 対応設定画面を用いて個別 VM とマスタ VM との対応関係を
設定することができる。そして設定プログラム 211 は、このとき管理者に
20 より設定された個別 VM とマスタ VM との対応関係を個別 VM / マスタ VM
対応管理テーブル 221 に格納し（S P 2 0 3）、この後この設定処理を終了する。

- さらに設定プログラム 211 は、ステップ S P 2 0 1 の判定において、そのとき指定された設定対象項目が「チェックポリシーの設定」及び「個別 VM
25 とマスタ VM との対応関係の設定」のいずれでもないと判定したときには、エラーをディスプレイ 204 に表示し（S P 2 0 4）、この後この設定処理

を終了する。

なおチェックポリシー設定画面の構成例を図14に示す。この図14のチェックポリシー設定画面500では、セキュリティチェックのチェック項目として予め定められた各項目にそれぞれ対応させてチェックポリシー詳細設定部501～505が設けられている。本実施の形態の場合、上述のようにかかるチェック項目として、「更新プログラムの判定」、「ウイルス対策製品の判定」、「不正ソフトウェアの判定」、「必須ソフトウェアの判定」及び「セキュリティ設定の判定」の5つが予め定められている。

そして例えば「更新プログラムの判定」というチェック項目に対応するチェックポリシー詳細設定部501では、更新が適用されたか否かをチェックすべき更新プログラムを指定でき、指定した更新プログラムごとにチェック対象、重要度及びチェック期限を指定できる。

また「ウイルス対策製品の判定」というチェック項目に対応するチェックポリシー詳細設定部502では、許可するウイルス対策製品、該当ウイルス対策製品のウイルス定義ファイルのバージョン及び定義日と、チェック対象、重要度及びチェック期限とを指定できる。

さらに「不正ソフトウェアの判定」というチェック項目に対応するチェックポリシー詳細設定部503では、インストールを禁止するソフトウェア及び当該ソフトウェアのバージョンを指定でき、指定したソフトウェアごとにチェック対象、重要度及びチェック期限を指定できる。

また「必須ソフトウェアの判定」というチェック項目に対応するチェックポリシー詳細設定部504では、必ずインストールすべきソフトウェアを指定でき、指定したソフトウェアごとにチェック対象、重要度及びチェック期限を指定できる。

さらに「セキュリティ設定の判定」というチェック項目に対応するチェックポリシー詳細設定部505では、予め用意されたセキュリティ設定に関する

チェック項目ごとにチェックの要否、チェック対象、重要度及びチェック期限を指定できる。

また「セキュリティ設定の判定」というチェック項目に対応するチェックポリシー詳細設定部 505 以外のチェックポリシー詳細設定部 501～504 には、それぞれ対応するチェック項目をチェック対象とするか否かを指定するためのラジオスイッチ 501A～504A が設けられている。

そしてチェックポリシー設定画面 500 では、所望するチェックポリシー詳細設定部 501 内に必要事項を入力後、OK ボタン 506 又はキャンセルボタン 507 をクリックすることによって、このチェックポリシー設定画面 500 を閉じることができる。

この際、設定プログラム 211 は、OK ボタン 506 がクリックされた場合には、チェックポリシー設定画面 500 において指定された情報をチェックポリシー管理テーブル 220 に新規登録し、又はチェックポリシー設定画面 500 において指定された情報に基づいてチェックポリシー管理テーブル 220 を更新し、キャンセルボタン 507 がクリックされた場合は、何もせずに処理を終了する。

また個別 VM / マスタ VM 対応設定画面の構成例を図 15 に示す。この図 15 に示す個別 VM / マスタ VM 対応設定画面 600 は、クライアント管理テーブル 223 から取得した、管理対象の仮想クライアントを表示する管理対象 VM 一覧表示部 601 と、個別 VM / マスタ VM 対応管理テーブルに登録済みの個別 VM とマスタ VM との関係を提示する登録済み情報表示部 602 と、追加的に対応付けようとする個別 VM 及びマスタ VM を指定する対応情報追加設定部 604 とからなる。

そして設定プログラム 211 は、登録済み情報表示部 602 に表示された個別 VM 及びマスタ VM の対応関係のうち、いずれかの対応関係と対応付けられたチェックボックス 607 がチェックされた状態で削除ボタン 603 が

クリックされると、その個別VM及びマスタVMの対応関係に関する情報を個別VM／マスタVM対応管理テーブル221から削除する。

また設定プログラム211は、対応情報追加設定部604において個別VM及びマスタVMのペアが指定された後、追加ボタン605がクリックされると、指定された情報を個別VM／マスタVM対応管理テーブル221に追加する。

さらに設定プログラム211は、個別VM／マスタVM対応設定画面500の右下に表示された終了ボタン606がクリックされると、この個別VM／マスタVM対応設定画面500を閉じて処理を終了する。

10 (1-6-3) セキュリティチェックプログラムの処理

次に、図12のステップSP105におけるセキュリティチェックプログラム213の処理内容について説明する。なお、上述のようにセキュリティチェックプログラム213は、セキュリティ管理制御プログラム210から、ステップSP102で作成したチェックIDと、ステップSP103で取得した日時データと、ステップSP105～ステップSP108における繰り返し処理のインターバル時間(=T)とを受け取る。

図16は、セキュリティ管理サーバ101のセキュリティチェックプログラム213が実行するセキュリティチェック処理の処理手順を示す。セキュリティチェックプログラム213は、まず、クライアント管理テーブル223を参照することにより各仮想クライアントの管理情報を取得し、さらに個別VM／マスタVM対応管理テーブル221を参照して、取得した各仮想クライアントの管理情報を、個別VMの管理情報とマスタVMの管理情報に分類する(SP300)。

続いてセキュリティチェックプログラム213は、ステップSP300において分類した管理情報のうち、マスタVMの管理情報を取得し、全マスタVMに対して、後述するステップSP302～ステップSP315の処理を

繰り返し実行する（S P 3 0 1）。

具体的に、セキュリティチェックプログラム 2 1 3 は、チェックポリシー管理テーブル 2 2 0 からマスタ VM のチェック項目に関する情報を取得し、さらにチェック結果管理テーブル 2 2 2 からそのとき対象としているマスタ VM のチェック結果のうち、今回のセキュリティチェックの結果（つまりチェック ID が一致するエントリの情報）を取得する。

次いで、セキュリティチェックプログラム 2 1 3 は、ステップ S P 3 0 2 で取得したマスタ VM に対するチェック項目と、そのとき対象としているマスタ VM に対するセキュリティチェックのチェック結果とを参照し、未チェックのチェック項目が存在するかを判定する（S P 3 0 3）。

セキュリティチェックプログラム 2 1 3 は、この判定において否定結果を得ると、ステップ S P 3 0 1 に戻って、この後ステップ S P 3 0 3 において肯定結果を得るまで同様の処理を繰り返す。

そしてセキュリティチェックプログラム 2 1 3 は、やがて対象とするマスタ VM に対するすべてのチェック項目のセキュリティチェックが終了することによりステップ S P 3 0 3 において肯定結果を得ると、チェックポリシー管理テーブル 2 2 0 に設定された重要度に基づいて、対象としているマスタ VM に対して未チェックのチェック項目を、重要度が「高」のチェック項目と、重要度が「中」のチェック項目と、重要度が「低」のチェック項目とに分類する。またセキュリティチェックプログラム 2 1 3 は、セキュリティ管理制御プログラム 2 1 0 から受け取った日時情報と、現在の日時と、チェックポリシー管理テーブル 2 2 0 に設定されたチェック期限との情報に基づいて、チェック期限切れのチェック項目をリストアップする（S P 3 0 4）。なお、期限切れの判断は、S P 1 0 3 にて採取してメモリ 2 0 2 に格納した時刻（すなわち、一連のチェック処理の開始時刻）に、チェック期限に記載の時間を加えた時刻が、現在時刻よりも古い場合は期限切れと判断する。なお、本実施

の形態では、チェック期限として、一連のチェック処理の開始時刻からの経過時間を記載するものとしたが、UNIX時間(1970年1月1日0時0分0秒からの秒数)や、特定の日時などを記載し、チェック期限に記載された時刻が、現在時刻よりも古い場合に期限切れと判断してもよい。なお、この場合は、一度、該当チェック項目のセキュリティチェックに合格した仮想クライアントは、再度、同じ項目のセキュリティチェックは実行しないようにしてもよい。

さらにセキュリティチェックプログラム213は、VM管理サーバ103の管理情報参照プログラム412から仮想マシン管理テーブル420に格納された情報と、物理マシン管理テーブル421に格納された情報とを取得し、これらの情報と仮想マシン管理テーブル420とに基づいて、対象としているマスタVMが現在起動中であるか否かを判定する(SP305)。なお、所定のVMが停止中とは、ハイパバイザプログラム310が所定のVM上で動作するアプリケーションプログラムやOS等のソフトウェア実行を終了し、所定のVMの提供に用いていた物理クライアント102の主メモリ302の領域を開放する、いわゆる所定のVMが終了した状態(かつ所定のVMの初期化前の状態)を指す。しかし、本実施の形態では所定のVMの停止中とした場合に、ハイパバイザプログラム310が所定のVMが提供するレジスタ及びメモリ空間の内容をマシンイメージに書き戻し、所定のVM上で動作するアプリケーションプログラムやOS等のソフトウェア実行を終了する一次停止状態を含めてもよい。なお、ハイパバイザプログラム310は一時停止状態のVMの処理を再開して再び起動中にするために、当該VMのマシンイメージから、メモリ空間の内容やレジスタの内容を含む各種情報を読み込み、これらの内容に基づいて所定のVMのレジスタ内容とメモリ空間の内容を復旧し、VMとしてのソフトウェア実行を再開させることができる。したがって、ハイパバイザプログラム310の説明で述べた、仮想マシン(仮

想クライアント)をエミュレーションする処理を、一時停止中のVMに適用する場合は上記復旧を行うものと読み替えてもよい。

そしてセキュリティチェックプログラム213は、この判定において否定結果を得ると、ステップSP305において取得した仮想マシン管理テーブル420の情報に基づいて、そのマスタVMの必要リソース量を取得する。

5 またセキュリティチェックプログラム213は、これに加えて物理マシン管理テーブル421から各物理クライアント(第1及び第2の物理クライアント102A, 102B)に必要な各リソース(CPU、メモリ及びディスク等)の量(以下、これを必要リソース量と呼ぶ)を取得する。さらにセキュ

10 リティチェックプログラム213は、同じく物理マシン管理テーブル421から取得したIPアドレスを用いて、各物理クライアント(第1及び第2の物理クライアント102A, 102B)にリモートアクセスし、これら物理クライアントの性能情報取得機能311から現在の性能情報(CPU利用率及びメモリ使用量)を取得し、現在のシステムの空きリソース量を算出する

15 (SP306)。

続いてセキュリティチェックプログラム213は、ステップSP306において取得した、対象とするマスタVMの必要リソース量と、現在のシステムの空きリソース量とを比較し、当該マスタVMを起動できるか否かを判定する(SP307)。

20 セキュリティチェックプログラム213は、この判定によりかかるマスタVMの起動ができないと判断した場合は、ステップSP304で作成した、当該マスタVMの未チェックのチェック項目の分類結果を参照し(SP308)、重要度が「高」のチェック項目又はチェック期限を過ぎたチェック項目があれば、管理者に対するアラートを発行する(SP309)。なお、管

25 理者に対するアラートの発行方法としては、管理者にリソース不足の旨を通知する方法であれば、ディスプレイ204にメッセージを表示する方法や、

管理者宛てに電子メールを送信する方法などのほか、他の種々の方法を広く適用することができる。そしてセキュリティチェックプログラム 2 1 3 は、ステップ S P 3 0 1 に戻って、この後同様の処理を繰り返す。

またセキュリティチェックプログラム 2 1 3 は、ステップ S P 3 0 7 において、そのマスタ VM の 2 台分の空きリソースがないと判断した場合（対象とするマスタ VM を起動すると、それ以上の VM を起動できないと判断した場合）は、ステップ S P 3 0 4 において作成したそのマスタ VM に対して未チェックのチェック項目の分類結果を参照し、重要度が「高」、重要度が「中」又はチェック期限を過ぎたチェック項目があるか否かを判定する（ステップ S P 3 1 0）。

そしてセキュリティチェックプログラム 2 1 3 は、この判定において肯定結果を得ると、VM 管理サーバ 1 0 3 の VM 管理プログラム 4 1 0 を利用してそのマスタ VM を起動する（S P 3 1 1）。具体的に、セキュリティチェックプログラム 2 1 3 は、第 1 又は第 2 の物理クライアント 1 0 2 A, 1 0 2 B を制御することにより、そのハイパバイザプログラム 3 1 0 に、ストレージ装置 1 0 4 から対応するマシンイメージ情報 3 2 0 を読み込ませ、これを主メモリ 3 0 2 上で展開させる。ただし、このマスタ VM を稼働させる物理クライアント（第 1 又は第 2 の物理クライアント 1 0 2 A, 1 0 2 B）の空きリソースが不足している場合には、VM 管理サーバ 1 0 3 の VM 移動プログラム 4 1 1 を利用して、最も空きリソースが多い物理クライアントにそのマスタ VM を移動させた後、当該マスタ VM を起動する。

続いてセキュリティチェックプログラム 2 1 3 は、対象とするマスタ VM に対し、重要度が「高」のチェック項目、重要度が「中」のチェック項目及びチェック期限を過ぎたチェック項目に対してそれぞれセキュリティチェックを行い、そのチェック結果をチェック結果管理テーブル 2 2 2 に格納する。またセキュリティチェックプログラム 2 1 3 は、チェック対象が「マスタ」

であるチェック項目については、そのマスタVMと関連する個別VMに対するセキュリティチェックのチェック結果として、当該マスタVMのチェック結果をチェック結果管理テーブル222に格納する。さらに、セキュリティチェックプログラム213は、チェック対象が「マスタ or 個別」であるチェック項目については、そのマスタVMに対するセキュリティチェックのチェック結果が合格であった場合にのみ、当該マスタVMと関連する個別VMのチェック結果として、チェック結果管理テーブル222に当該マスタVMに対するセキュリティチェックのチェック結果を格納する（ステップSP312）。そしてセキュリティチェックプログラム213は、ステップSP301に戻って、この後同様の処理を繰り返す。

さらにセキュリティチェックプログラム213は、ステップSP307において、対応する物理クライアント（第1又は第2の物理クライアント102A, 102B）内にそのマスタVMの2台分以上の空きリソースが存在すると判断した場合には、VM管理サーバ103のVM管理プログラム410を利用してそのマスタVMを起動する（ステップSP313）。この際、セキュリティチェックプログラム213は、ステップSP311と同様に、そのマスタVMを稼働させる物理クライアント（第1又は第2の物理クライアント102A, 102B）の空きリソースが不足している場合には、VM管理サーバ103のVM移動プログラム411を利用して、最も空きリソースが多い物理クライアントにそのマスタVMを移動させた後、当該マスタVMを起動する。

続いて、セキュリティチェックプログラム213は、対象とするマスタVMに対してセキュリティチェックを行い、そのチェック結果をチェック結果管理テーブル222に格納する。またセキュリティチェックプログラム213は、ステップSP312と同様に、チェック対象の設定に応じて、そのマスタVMと関連する個別VMに対するセキュリティチェックのチェック結果

として、当該マスタVMのチェック結果をチェック結果管理テーブル222に格納する（SP314）。そしてセキュリティチェックプログラム213は、ステップSP301に戻って、この後同様の処理を繰り返す。

なお、ステップSP307～ステップSP314の処理は一例であって、
5 例えば、ステップSP307においてそのマスタVMの2台分の空きリソースがないと判断した場合にもステップSP308及びステップSP309の処理を行うようにしてもよい。

これに対してセキュリティチェックプログラム213は、ステップSP305の判定において肯定結果を得ると、対象とするマスタVMに対して、重要度が「高」のチェック項目及びチェック期限を過ぎたチェック項目についてのみセキュリティチェックを行い、そのチェック結果をチェック結果管理
10 テーブル222に格納する。このようにマスタVMが起動されている場合には、重要度が「高」のチェック項目及びチェック期限を過ぎたチェック項目についてのみセキュリティチェックを行うのは、そのマスタVMが起動されている場合、そのマスタVMによって何らかの処理が行われている可能性
15 あるため、その処理を邪魔しないようにするためである。またセキュリティチェックプログラム213は、ステップSP312と同様に、チェック対象の設定に応じて、そのマスタVMと関連する個別VMに対するセキュリティチェックのチェック結果として、当該マスタVMのチェック結果をチェック
20 結果管理テーブル222に格納する（SP315）。そしてセキュリティチェックプログラム213は、ステップSP301に戻って、この後同様の処理を繰り返す。

続いて、セキュリティチェックプログラム213は、ステップSP300において分類した管理情報のうち、個別VMの管理情報を取得し、全個別V
25 Mに対して、後述するステップSP317～ステップSP330の処理を繰り返し実行する（SP316）。

具体的に、セキュリティチェックプログラム 2 1 3 は、チェックポリシー管理テーブル 2 2 0 から個別 VM のチェック項目に関する情報を取得し、さらにチェック結果管理テーブル 2 2 2 からそのとき対象としている個別 VM のチェック結果のうち、今回のセキュリティチェックのチェック処理の結果（つまりチェック ID が一致するエントリの情報）を取得する（S P 3 1 7）。

次いで、セキュリティチェックプログラム 1 2 3 は、ステップ S P 3 1 7 で取得した個別 VM に対するセキュリティチェックのチェック項目と、そのとき対象としている個別 VM に対するセキュリティチェックのチェック結果とを参照し、未チェックのチェック項目が残っているかを判定する（S P 3 1 8）。

セキュリティチェックプログラム 2 1 3 は、この判定において否定結果を得るとステップ S P 3 1 6 に戻り、この後ステップ S P 3 1 8 において肯定結果を得るまで同様の処理を繰り返す。

そしてセキュリティチェックプログラム 2 1 3 は、やがてすべてのチェック項目に対するセキュリティチェックが終了することによりステップ S P 3 1 8 において肯定結果を得ると、ステップ S P 3 0 4 と同様にして、対象とする個別 VM に対して未チェックのチェック項目をリストアップする（S P 3 1 9）。

続いてセキュリティチェックプログラム 2 1 3 は、ステップ S P 3 0 5 と同様にして、対象とする個別 VM が起動中であるか否かを判断し（S P 3 2 0）、当該個別 VM が停止中のときには、ステップ S P 3 0 6 と同様にして、その個別 VM の必要リソース量と、各物理クライアントの現在の性能情報とをそれぞれ取得し、現在のシステムの空きリソース量を算出する（S P 3 2 1）。

次いでセキュリティチェックプログラム 2 1 3 は、ステップ S P 3 0 7 と同様にして、その個別 VM を起動できるか否かを判定する（S P 3 2 2）。

そしてセキュリティチェックプログラム 2 1 3 は、その個別 VM の起動ができないと判断した場合は、ステップ S P 3 0 8 同様に、その個別 VM の未チェックのチェック項目に、重要度が「高」のチェック項目又はチェック期限を過ぎたチェック項目があれば、管理者へアラートを発行する（S P 3 2 3, S P 3 2 4）。そしてセキュリティチェックプログラム 2 1 3 は、ステップ S P 3 1 6 に戻って、この後同様の処理を繰り返す。

またセキュリティチェックプログラム 2 1 3 は、ステップ S P 3 2 2 において、そのマスタ VM の 2 台分の空きリソースがないと判断した場合（対象とするマスタ VM を起動すると、それ以上の VM を起動できないと判断した場合）は、ステップ S P 3 1 9 において作成したその個別 VM の未チェックのチェック項目の分類結果を参照し、重要度が「高」、重要度が「中」又はチェック期限を過ぎたチェック項目があるか否かを判定する（S P 3 2 5）。

そしてセキュリティチェックプログラム 2 1 3 は、この判定において肯定結果を得ると、ステップ S P 3 1 1 と同様に、その個別 VM を起動する（S P 3 2 6）。

またセキュリティチェックプログラム 2 1 3 は、ステップ S P 3 1 2 と同様に、その個別 VM に対して、重要度が「高」のチェック項目、重要度が「中」のチェック項目及びチェック期限を過ぎたチェック項目についてのみセキュリティチェックを行い、そのチェック結果をチェック結果管理テーブル 2 2 2 に格納する（S P 3 2 7）。そしてセキュリティチェックプログラム 2 1 3 は、ステップ S P 3 1 6 に戻って、この後同様の処理を繰り返す。

さらにセキュリティチェックプログラム 2 1 3 は、ステップ S P 3 2 2 において、対応する物理クライアント（第 1 又は第 2 の物理クライアント 1 0 2 A, 1 0 2 B）内にそのマスタ VM の 2 台分以上の空きリソースが存在すると判断した場合には、ステップ S P 3 1 3 と同様の手順で、その個別 VM を起動し（S P 3 2 8）、この後ステップ S P 3 1 4 と同様の手順によりそ

の個別VMに対するチェックを行い、チェック結果をチェック結果管理テーブル222に格納する（SP329）。そしてセキュリティチェックプログラム213は、ステップSP316に戻って、この後同様の処理を繰り返す。

- これに対してセキュリティチェックプログラム213は、ステップSP320の判定において肯定結果を得ると、ステップSP315と同様にして、その個別VMに対して重要度が「高」のチェック項目及びチェック期限を過ぎたチェック項目についてのみセキュリティチェックを行い、そのチェック結果をチェック結果管理テーブル222に格納する（SP330）。そしてセキュリティチェックプログラム213は、ステップSP316に戻って、
- 10 この後同様の処理を繰り返し、やがてすべての個別VMに対するステップSP317～ステップSP330の処理が完了すると、このセキュリティチェック処理を終了する。

（1-6-4）VM情報収集プログラムの処理

- 続いて、セキュリティ管理サーバ101（図2）のVM情報収集プログラム212（図2）の処理内容について説明する。
- 15

- 図17は、本実施の形態によるVM情報収集プログラム212により実行されるVM情報収集処理の処理手順を示す。VM情報収集プログラム212は、まずVM管理サーバ103の管理情報参照プログラム412を呼び出し、仮想マシン管理テーブル420から各仮想マシンの管理情報（以下、これを
- 20 仮想マシン管理情報と呼ぶ）を取得する（SP400）。

続いてVM情報収集プログラム212は、取得した仮想マシン管理情報の一部又は全部をクライアント管理テーブル223に格納し（SP401）、この後このVM情報収集処理を終了する。

（1-7）本実施の形態の動作及び効果

- 25 本実施の形態における動作例を、図18に示す。例えばチェックポリシー管理テーブル220における「C1-01」というチェック項目を仮想マシンVM1に

対して実施し、チェックに合格した場合は（図 18 の「C1-01-（1）」）、個別 VM（VM 2 ～ VM 4）に対するチェックを行わずに、各個別のチェック結果を「○」にすることができる（図 18 の「C1-01-（2）」）。これにより、セキュリティチェック処理の処理量を減らすことができ、仮想クライアント
5 の利用者への影響を抑えつつ、セキュリティチェック処理の高速化ができるようになる。

また、チェックポリシー管理テーブル 220 における「C5-01」というチェック項目を仮想マシン VM 2 に対して実施しようとした場合に、仮想マシン VM 2 が利用中であれば、この「C5-01」というチェック項目の重要度が「低」な
10 のでチェックをスキップし、後に仮想マシン VM 2 が未使用のときにチェック処理を行う（図 18 の「C5-01」）。これにより、セキュリティチェック処理が仮想マシン VM 2 の利用者を与える影響をおさえることができるようになる。

また、チェックポリシー管理テーブル 220 における「C3-02」というチェック
15 項目を仮想マシン VM 3 に対して実施しようとした場合、この「C3-02」というチェック項目は重要度が「高」なので、仮想マシン VM 3 が利用中にも関わらず、当該チェック項目のチェック処理を実施する（図 18 の「C3-02-（1）」）。同じく、「C3-02」というチェック項目を仮想マシン VM 4 に対して実施しようとした際、第 1 の物理クライアント 102A がリソース不足であった場合
20 （図 18 の「C3-02-（2）」）、仮想マシン VM 4 は第 2 の物理クライアント 102B 上で起動しチェック処理を実施する（図 18 の「C3-02-（3）」）。これにより、重要度が高いチェック項目については迅速にチェックを行うことができるようになる。

以上のように本実施の形態によるセキュリティ管理方法によれば、セキュ
25 リティチェックを、チェック項目ごとに、必要な種別の仮想マシンに対して選択的に実行することができるため、不要な種別に対するセキュリティチェ

ックを省略させることができる。かくするにつき仮想クライアントのセキュリティチェックを高速かつ効率的に行うことができる。

また従来技術によると、各仮想クライアントに対するセキュリティチェックの実行により、チェック処理を行う管理サーバ側だけでなく、チェック対象のクライアント側にも少なからずの負荷を与えるという問題もあるが、本実施の形態によるセキュリティ管理方法によれば、複数台の管理サーバでの並列実行などによって高速化を行う方法ではなく、セキュリティチェックの処理量を減らす方法での高速化を実現できる。

(2) 第2の実施の形態

10 (2-1) 本実施の形態によるネットワークシステムの構成

次に、第2の実施の形態について説明する。本実施の形態では、管理対象の複数の仮想クライアントがマシンの構成情報（あるマシンイメージの全部又は一部など）を共有し、共有するマシンの構成情報に変更を加えると、当該マシンの構成情報を共有しているすべての仮想クライアントにその変更が反映される仮想化技術、特に、共有するマシンの構成情報に変更を加えると、既に起動中の仮想クライアントには変更が反映されず、仮想クライアントのOSを再起動した際に、その変更が反映される仮想化技術をベースとする（例えば特許文献2や、非特許文献1の技術）。なお、OSの再起動とは仮想クライアントを起動した状態で、当該仮想クライアントのOSの処理を終了し、再度起動を行う場合のみならず、当該仮想クライアントのOSの終了後に仮想クライアントが停止状態となり、その後仮想クライアントを起動してOSを起動する場合も含む。なお、このような変更反映を行う仮想化技術の一例としては以下の処理によって実現する方法が考えられる。しかし、これ以外の方法を採用してもよい。

25 (ステップ1) マスタVMに対する変更箇所を記録する。なお、変更箇所の記録方法としては変更された個々のファイル名や、変更箇所のファイルシス

テム上のアドレスなどにより特定した変更箇所を記録する。変更箇所を特定する方法は、他の方法でもよい。また、更新データや更新前データも含めて記録してもよい。また、当該記録はハイパバイザプログラムまたはマスタVMまたは別なコンピュータが行うことが考えられる。

- 5 (ステップ2) 個別VM上のOSの再起動を検知し、記録された変更箇所のデータをマスタVMのディスクイメージから個別VMのディスクイメージにコピーする。当該検知及びコピーはハイパバイザプログラムまたはマスタVMまたは別なコンピュータが行うことが考えられる。なお、個別VMにのみ存在するファイルまたは設定と矛盾する上記コピーについては矛盾を発生させるファイル（またはデータ）についてのコピーを抑止してもよい。

(ステップ3) コピー後に個別VM上にてOSの起動を行わせる。これによってコピーされたファイル（データ）を反映したソフトウェア実行環境が個別VM上にて実現される。

- ただし、共通の情報の変更を反映させるために、仮想クライアントの再起動を必要としない仮想化技術については、第1の実施の形態の範囲では本発明を適用可能である。

- なお、本実施の形態では、以上のような仮想化技術の実装には依存しないため、仮想化技術の詳細な説明は省略し、一例として簡単に説明するにとどめる。また、以上のような仮想化技術には、共有するマシンの構成情報があるマシンイメージそのものであり、共有するマシンの構成情報だけで仮想マシンが構成できる技術（以下、これを仮想化技術1と呼ぶ）と、共有するマシンの構成情報だけでは仮想マシンが構成できず、共有するマシンの構成情報と、個別の仮想クライアントごとに持つ、個別のマシンの構成情報を合わせて個別の仮想クライアントが構成できる技術（以下、これを仮想化技術2と呼ぶ）がある。本実施の形態では、かかる仮想化技術1及び仮想化技術2のいずれにも対応できる方式について説明する。

図 1 との対応部分に同一符号を付して示す図 19 において、700 は全体として第 2 の実施の形態によるネットワークシステムを示す。このネットワークシステム 700 は、第 1 及び第 2 の物理クライアント 702 A, 702 B の外部記憶装置 303 (図 20) 並びにストレージ装置 703 において保持されるプログラム及び各種情報と、セキュリティ管理サーバ 701 により実行されるセキュリティチェックのチェック項目及び当該セキュリティチェックの処理手順とが異なる点を除いて第 1 の実施の形態によるネットワークシステム 100 と同様に構成されている。

まず本実施の形態による第 1 及び第 2 の物理クライアント 702 A, 702 B の構成について説明する。図 7 との対応部分に同一符号を付して示す図 20 は、第 2 の実施の形態による第 1 の物理クライアント 702 A の構成を示す。なお第 2 の物理クライアント 702 B も、第 1 の物理クライアント 702 A と同様の構成である。

第 1 の物理クライアント 702 A の外部記憶装置 303 には、ハイパバイザプログラム 310 に加え、VM イメージ管理プログラム 800 が保持される。また、ストレージ装置 703 には、複数又は単数の VM 共通構成情報 801、複数又は単数の個別 VM 構成情報 802、並びに共通／個別対応情報 803 が格納される。

VM 共通構成情報 801 は、複数又は単数の仮想クライアントを構成する情報の一部又は全部であり、典型的には、複数の仮想クライアントから共有される。上記仮想化技術 1 においては、ある仮想クライアントのマシンイメージであり、上記仮想化技術 2 においては、ある仮想クライアントを構成する情報の一部である。

個別 VM 構成情報 802 は、個別の仮想クライアントごとにカスタマイズした情報を含む、仮想クライアントを構成する情報の一部である。上記仮想化技術 1 においては、VM 共通構成情報 802 のみから構成される仮想クラ

クライアントとの差分情報であり、上記仮想化技術 2 においては、VM 共通構成情報 801 とあわせて、ある仮想クライアントを構成する情報である。

共通／個別対応情報 803 は、個別 VM 構成情報 802 のそれぞれについて、どの VM 共通構成情報 801 と関連するかを示す情報である。

- 5 VM イメージ管理プログラム 800 は、VM 共通構成情報 801 と、個別 VM 構成情報 802 を管理するプログラムであり、ハイパバイザプログラム 310 に対して仮想的なマシンイメージを提供する。すなわち、本実施の形態におけるハイパバイザプログラム 310 は、VM イメージ管理プログラム 800 を介してマシンイメージにアクセスする。
- 10 例えば VM イメージ管理プログラム 800 は、共通／個別対応情報 802 に基づいて、VM 共通構成情報 801 と、個別 VM 構成情報 802 とを合わせたマシンイメージを仮想的に構築する。また VM イメージ管理プログラム 800 は、ある VM 共通構成情報 801 に変更があった場合は、すべての仮想クライアントに変更後の情報が反映されたことを確認するまで（つまり変更前の情報が不要になるまで）、変更前の情報と、変更後の情報の両方を管理し、ハイパバイザプログラム 310 の要求に応じて、変更前か変更後のいずれかの情報を提供する。
- 15

（2-2）論理構成

- 続いて、本実施の形態によるネットワークシステム 700 の論理構成について、上述した第 1 の実施の形態によるネットワークシステム 100 の論理構成（図 11 参照）と異なる部分を説明する。なお、本実施の形態では、上記仮想化技術 1 のように、VM 共通構成情報 801 が、当該情報のみで仮想マシンを起動するに十分な情報を有するマシンイメージであるものとする。
- 20

- 図 21 は、第 2 の実施の形態によるネットワークシステム 700 の論理構成を示す。ストレージ装置 703 には、VM 共通構成情報 801 と、第 1 の仮想クライアント VM1 以外の各仮想クライアント（第 2～第 4 の仮想クラ
- 25

イアントVM2～VM4)用の個別VM構成情報802 (VM共通構成情報801との差分情報)とが格納されている。

なお、上述のようにVM共通構成情報801は、当該情報のみで、第1の仮想クライアントVM1を起動するに十分な情報を有するマシンイメージとするが、ストレージ装置703に第1の仮想クライアントVM1用の個別VM構成情報802を格納し、第1の仮想クライアントVM1がVM共通構成情報801と、当該第1の仮想クライアントVM1用の個別VM構成情報802とを合わせて仮想マシンを起動するに十分な情報を有する構成をとってもよい。

10 第2～第4の仮想クライアントVM2～VM4は、第1の仮想クライアントVM1をベースに生成した仮想マシンであり、これら第2～第4の仮想クライアントVM2～VM4のマシンイメージは、VMイメージ管理プログラム800により、VM共通構成情報801と、各仮想クライアント用の個別VM構成情報802とを合わせて仮想的に構成される。

15 本実施の形態では、マスタVMにインストールしたソフトウェアのアンインストールを除く、あらゆる操作を個別VMの利用者に許すこととする。なお、ソフトウェアのアンインストールを抑止する方法としては、レジストリへのアンインストールの禁止設定、個別VMの利用者のユーザ権限による保護、アンインストールパスワードの設定などがあるが、他の方法でも構わない。

20 また第1の実施の形態と同様に、セキュリティ管理サーバ701が保持する別VM/マスタVM対応管理テーブル221 (図2及び図4)には、第2～第4の仮想クライアントVM2～VM4のマスタVMがいずれも第1の仮想クライアントVM1であることが登録される。

25 なお、上述のように本実施の形態では、VM共通構成情報801は、当該情報のみで、第1の仮想クライアントVM1を起動するに十分な情報を有す

るマシンイメージとしたが、第1の仮想クライアントVM1がVM共通構成情報801と、当該第1の仮想クライアントVM1用の個別VM構成情報802とを合わせて仮想クライアントを起動するに十分な情報を有する構成をとった場合、いずれかの個別VM、すなわち第2～第4の仮想クライアント

5 VM2～VM4をマスタVMとしても定義する。具体的には、例えば第2の仮想クライアントVM2をマスタVMかつ個別VMとし、個別VM／マスタVM対応管理テーブル221には、第2～第4の仮想クライアントVM2～VM4のマスタVMがそれぞれ第2の仮想クライアントVM2であることを登録する。

10 (2-3) 処理手順

続いて、本実施の形態におけるチェックポリシーについて説明する。図22は、本実施の形態によるセキュリティ管理サーバ701により保持されるチェックポリシー管理テーブル705の構成例を示す。

マスタVMに対するセキュリティチェックが合格した場合、個別VMに対

15 するセキュリティチェックを行わないチェック項目（すなわちチェック対象が「マスタ」又は「マスタ or 個別」であるチェック項目）については、マスタVMの変更が個別VMにも反映されていることを確認する必要がある。すなわち起動中の個別VMには、マスタVMの変更が反映されないため、個別VMのOSの再起動が必要となる。

20 そこで、本実施の形態におけるチェックポリシーは、第1の実施の形態におけるチェックポリシーの内容に加え、「マスタの変更の反映」というチェック項目を持つ。このチェック項目は、マスタVMの変更が個別VMに反映されたか否かを確認するチェック項目である。なお、このチェック項目は、「チェック対象」が「個別」、「重要度」が「高」にそれぞれ固定されており、

25 これら「チェック対象」及び「重要度」の変更はできないものとする。またこのチェック項目の「チェック期限」は、他のチェック項目と異なり、セキ

セキュリティチェックを実行する期限を表すものではなく、「対策期限」を表す。

本実施の形態における、セキュリティチェックプログラム 2 1 3 の処理手順について説明する。本実施の形態におけるセキュリティチェック処理は、

図 1 6 との対応部分に同一符号を付した図 2 3 に示すように、第 1 の実施の

- 5 形態によるセキュリティチェック処理のステップ S P 3 1 2 の後にステップ S P 4 0 0 を、ステップ S P 3 1 4 の後にステップ S P 4 0 1 を、ステップ S P 3 1 5 の後にステップ S P 4 0 2 をそれぞれ加えた内容となっている。

また本実施の形態のセキュリティチェック処理では、ステップ S P 3 2 6 の後のステップ S P 4 0 3、ステップ S P 3 2 8 の後のステップ S P 4 0 4

- 10 及びステップ S P 3 2 0 の後のステップ S P 4 0 5 において、第 1 の実施の形態によるセキュリティチェック処理の対応するステップ S P 3 2 7、ステップ S P 3 2 9 又はステップ S P 3 3 0 と同じ処理を実行した後に、上述のようにチェックポリシーに追加した「マスタの変更の反映」というチェック項目に関するセキュリティチェックを実施する。

- 15 まず、追加したステップ S P 4 0 0、ステップ S P 4 0 1 及びステップ S P 4 0 2 におけるセキュリティ管理サーバ 7 0 1 のセキュリティチェックプログラム 7 0 4（図 2 1）の処理内容について説明する。

本実施の形態のセキュリティチェックプログラム 7 0 4 は、ステップ S P 3 1 2 の処理後、ステップ S P 3 1 2 で実施したチェック項目について、前

- 20 回のセキュリティチェックのチェック結果と、今回のセキュリティチェックのチェック結果とを比較する。そしてセキュリティチェックプログラム 7 0 4 は、前回のセキュリティチェックでは不合格で、今回のセキュリティチェックでは合格したチェック項目がある場合には、マスタ VM の変更の反映が必要と判断し、マスタ VM の変更日時として、OS 2 1 4 から、現在の日時
25 を取得する（S P 4 0 0）。またセキュリティチェックプログラム 7 0 4 は、これと同様の処理を、ステップ S P 4 0 1 ではステップ S P 3 1 4 で実施し

たチェック項目について、ステップSP402ではステップSP315で実施したチェック項目について実行する。

次に、ステップSP403、ステップSP404及びステップSP405におけるセキュリティチェックプログラム704の処理内容について説明する。

セキュリティチェックプログラム704は、ステップSP403において、図16のステップSP327同様に、処理対象の個別VMに対し、重要度が「高」のチェック項目、重要度が「中」のチェック項目及びチェック期限を過ぎたチェック項目についてのみ、チェックを行う。

10 ただし、「マスタの変更の反映」というチェック項目については、かかるステップSP400、ステップSP401又はステップSP402において行ったマスタVMの変更反映の要否判定の結果、マスタVMの変更の反映が必要と判断した場合に限り、セキュリティチェックを実行する。

15 このセキュリティチェックの方法は、例えば、チェック対象の個別VMのイベントログやsyslogなどのログ情報を参照し、最終リブート日時を取得し、上記ステップSP400、ステップSP401又はステップSP402で取得した、マスタVMの変更日時以降にリブートが行われているかどうかで判定する。

20 このセキュリティチェックのチェック結果が不合格であった場合、セキュリティチェックプログラム704は、マスタVMの変更日時と、現在時刻とを比較し、指定された期限を過ぎていればアラートを発行する。

25 ステップSP404及びステップSP405は、それぞれ第1の実施の形態におけるステップSP329及びステップSP330と同様の処理を行った後に、ステップSP403で説明した「マスタの変更の反映」のチェック項目についてのチェック処理を実行する。

以上、本実施の形態のセキュリティ管理方法におけるチェックポリシー管理

テーブルのチェック期限の項目は、第 1 の実施の形態に記載のように、当該期限を経過する前はマスタ VM 及び個別 VM に対する強制的なチェック開始を抑制するための設定値とすることに加え、本実施の形態に記載のように、OS の再起動の有無を繰り返し確認し、対策期限経過後にも未再起動であれば再起動を促す所定の処理（上記ではアラート発行）を開始するための設定値とするものである。

なお、本実施の形態では、セキュリティチェックプログラム 213 がマスタ VM の変更を検知した時刻を、マスタ VM の変更時刻とみなし、その時刻を基点とし、対策期限内に個別 VM が再起動されたかどうか判断する例について説明したが、実際のマスタ VM に変更が生じた日時を基点として、期限切れを判断してもよい。例えば、セキュリティ管理サーバは、マスタ VM が起動している物理クライアント 702 のハイパバイザプログラム 310、または VM イメージ管理プログラム 800、または VM 管理サーバからマスタ VM に対する変更日時を取得し、この変更日時に対策期限を加えた日時を現在日時と比較してもよい。

（2－4）本実施の形態の効果

以上のように本実施の形態のセキュリティ管理方法によれば、マスタ VM の構成情報に変更を加えても、既に起動中の仮想クライアントには変更が反映されず、仮想クライアントを再起動した際に、その変更が反映される仮想化技術を適用したネットワークシステム 700 に対しても、第 1 の実施の形態と同様のセキュリティ管理を行うことができる。

（3）第 3 の実施の形態

次に、第 3 の実施の形態について説明する。図 1 との対応部分に同一符号を付して示す図 24 は、第 3 の実施の形態によるネットワークシステム 900 を示す。このネットワークシステム 900 は、チェックポリシーに設定するチェック対象を、システムの環境の情報から当該システムが自動的に判断す

る点を除いて第1の実施の形態によるネットワークシステム1と同様に構成されている。

図2との対応部分に同一符号を付した図25は、本実施の形態におけるセキュリティ管理サーバ901の構成を示す。このセキュリティ管理サーバ901は、外部記憶装置205に、図2について上述した各種プログラム及び各種情報に加えて、チェック対象設定プログラム1000が格納されている点と、チェックポリシーに設定するチェック対象を、システムの環境の情報から自動的に判断する機能がセキュリティ管理制御プログラム1001に搭載された点とを除いて第1の実施の形態によるセキュリティ管理サーバ901と同様に構成されている。

チェック対象設定プログラム1000は、システムの環境の情報から個別VMにおいてカスタマイズ可能な項目と、カスタマイズ不可能な項目とを調査し、個別VMにおいてカスタマイズ不可能な項目についてはマスタVMをチェック対象とし、カスタマイズ可能な項目については個別VMをチェック対象として、チェックポリシー管理テーブル220に設定するプログラムである。

カスタマイズの可否を判断するための環境情報を取得する方法としては、マスタVMのレジストリの情報から取得したり、個別VMを利用する利用者の権限を調査する方法などが考えられるが、本実施の形態においては、VM管理サーバ902への問い合わせによって、カスタマイズの可否を判断する。

一方、図8との対応部分に同一符号を付した図26は、本実施の形態におけるVM管理サーバ902の構成を示す。このVM管理サーバ902は、外部記憶装置405に、図8について上述した各種プログラム及び各種情報に加え、セキュリティ管理プログラム1002が格納されている点を除いて第1の実施の形態によるVM管理サーバ103と同様に構成されている。

セキュリティ管理プログラム1002は、当該VM管理サーバ902で生成する仮想クライアントに対してセキュリティに関する利用制限を設定でき、

さらに指示入力装置 4 0 3 を用いた利用者からの指示や、ネットワーク 1 0 5 経由での他のプログラムからの指示に従い、上記利用制限の情報を返すプログラムである。

図 2 7 は、本実施の形態によるセキュリティ管理サーバ 9 0 1 により表示
5 されるチェックポリシー設定画面 1 1 0 0 を示す。本実施の形態のチェックポリシー設定画面 1 1 0 0 は、チェック対象として「マスタ」、「個別」、「マスタ or 個別」及び「マスタ and 個別」に加えて「自動」も指定できる点が第 1 の実施の形態によるチェックポリシー設定画面 5 0 0 と異なる。チェック対象として「自動」を指定した場合、そのチェック項目については、個別 VM
10 でカスタマイズが可能か否かを、セキュリティ管理サーバ 9 0 1 のセキュリティ管理制御プログラム 1 0 0 1 がシステムの環境の情報から自動的に判断し、チェック対象を特定する。

次に、以上のようにチェックポリシーに設定するチェック対象を、システム
の環境の情報から自動的に判断する処理に関するセキュリティ管理制御プロ
15 グラム 1 0 0 1 の処理手順について説明する。

図 1 2 との対応部分に同一符号を付して示す図 2 8 は、本実施の形態によるセキュリティ管理制御処理の処理手順を示す。本実施の形態によるセキュリティ管理制御処理は、ステップ S P 1 0 2 の処理実行の前に、ステップ S P 5 0 0 及びステップ S P 5 0 1 の処理を実行する点が第 1 の実施の形態に
20 によるセキュリティ管理制御処理と異なる。

この場合、セキュリティ管理制御プログラム 1 0 0 1 は、ステップ S P 5 0 0 に進むと、チェックポリシーのチェック対象として「自動」が選択されているかを確認し、「自動」が選択されている場合には、ステップ S P 5 0 1 に進む。またセキュリティ管理制御プログラム 1 0 0 1 は、ステップ S P 5
25 0 1 では、チェック対象設定プログラム 1 0 0 0 を実行することによりチェック対象を自動判定し、チェックポリシーに設定された「自動」の部分に「マ

スタ」や「個別」などの値を設定する。

図29は、図28のステップSP501において起動されたチェック対象設定プログラム1000により実行されるチェック対象設定処理の処理手順を示す。

- 5 本実施の形態におけるチェック対象設定プログラム1000は、まず、チェックポリシーを参照し、チェック対象が「自動」の項目をリストアップし（SP600）、この後セキュリティ管理プログラム1002を呼び出し、仮想クライアントの利用制限の情報を取得する（SP601）。

- 10 続いてチェック対象設定プログラム1000は、ステップSP602において、ステップSP600においてリストアップしたチェック対象が「自動」の各項目について、ステップSP603～ステップSP605の処理を繰り返す（SP602）。

- 15 具体的に、チェック対象設定プログラム1000は、ステップSP601で取得した利用制限の情報を参照し、処理対象のチェック項目がカスタマイズ可能か否かを判定する（SP603）。

- 20 そしてチェック対象設定プログラム1000は、この判定において肯定結果を得ると、そのチェック項目のチェック対象として「個別」を設定し（SP604）、否定結果を得ると、そのチェック項目のチェック対象として「マスタ」を設定する（SP605）。例えばチェック対象設定プログラム1000は、パスワード付きスクリーンセーバが設定されているか、というチェック項目のチェック対象は、個別VMでのスクリーンセーバの設定が、禁止されていなければ「個別」を、禁止されていれば「マスタ」を設定する。

- 25 そしてチェック対象設定プログラム1000は、ステップSP604又はステップSP605の処理を完了すると、この図29に示すチェック対象設定処理を終了する。

以上のように本実施の形態によるネットワークシステム900では、チェ

ックポリシーに設定するチェック対象を、システムの環境の情報から自動的に判断して設定するため、第1の実施の形態により得られる効果に加えて、チェックポリシーの設定作業を容易化することができるという効果をも得ることができる。

5 (4) 第4の実施の形態

次に、第4の実施の形態について説明する。本実施の形態では、第3の実施の形態同様、チェックポリシーに設定するチェック対象について、システムの環境の情報から自動的に判断する例について説明する。第3の実施の形態では、1つのチェック項目に対してすべてのマスタVMに共通する1つのチェック対象しか設定できなかったが、本実施の形態では、1つのチェック項目に対してマスタVM別に異なるチェック対象を指定できる。

図24との対応部分に同一符号を付して示す図30は、第4の実施の形態によるネットワークシステム1200を示す。このネットワークシステム1200は、セキュリティ管理サーバ1201の構成が異なる点を除いて第3の実施の形態によるネットワークシステム900と同様に構成されている。

この場合は、セキュリティ管理サーバ1201は、図26との対応部分に同一符号を付した図31に示すように、外部記憶装置205に格納されたセキュリティ管理制御プログラム1300、セキュリティチェックプログラム1301及びチェック対象設定プログラム1302の構成が異なる点と、当該外部記憶装置205に、図2について上述した各種プログラム及び各種情報に加えて、チェック対象管理テーブル1303が格納されている点とを除いて第3の実施の形態によるセキュリティ管理サーバ901と同様に構成されている。

なお、以下においては、カスタマイズ可否を判断するための環境情報の例として、マスタVMのレジストリの情報を参照する例を示す。また本実施の形態におけるセキュリティチェックプログラム1301は、チェックポリシー

においてチェック対象が「自動」に設定された項目については、チェック対象管理テーブル 1 3 0 3 を参照してチェック対象の情報を取得する、という違いのみであるため、処理手順の説明は省略する。

5 チェック対象管理テーブル 1 3 0 3 は、マスタ VM ごとにそれぞれ設定された、チェック項目ごとのチェック対象を管理するためのテーブルであり、図 2 9 に示すように、マシン ID 欄 1 3 0 3 A 及び複数の ID 欄 1 3 0 2 B から構成される。

10 そしてマシン ID 欄 1 3 0 3 A には、チェックポリシーにおいてチェック対象が「自動」に設定された各マスタ VM のマシン ID が格納される。また ID 欄 1 3 0 2 B は、チェックポリシーにおいて設定された各チェック項目にそれぞれ対応させて設けられており、これら ID 欄 1 3 0 2 B には、それぞれ対応するチェック項目についてそのマスタ VM に関して設定されたチェック対象（「マスタ」又は「個別」）が格納される。

15 図 3 3 は、図 2 8 のステップ S P 5 0 1 において起動されたチェック対象設定プログラム 1 3 0 2 により実行されるチェック対象設定処理の処理手順を示す。

本実施の形態におけるチェック対象設定プログラム 1 3 0 2 は、まず、チェックポリシーを参照し、チェック対象が「自動」の項目をリストアップする（S P 7 0 0）。

20 続いてチェック対象設定プログラム 1 3 0 2 は、個別 VM / マスタ VM 対応管理テーブル 2 2 1 と、クライアント管理テーブル 2 2 3 を参照し、すべてのマスタ VM の管理情報を取得する（S P 7 0 1）。

この後、チェック対象設定プログラム 1 3 0 2 は、すべてのマスタ VM に対して、以下に説明するステップ S P 7 0 3 ~ ステップ S P 7 0 6 の処理を
25 繰り返す（S P 7 0 2）。

具体的に、チェック対象設定プログラム 1 3 0 2 は、ステップ S P 7 0 0

においてリストアップした、チェック対象が「自動」の各項目について、ステップSP704～ステップSP706の処理を繰り返す（SP703）。

すなわち、チェック対象設定プログラム1302は、処理対象のマスタVMのレジストリの情報を参照して、処理対象の項目がカスタマイズ可能か判定する（SP704）。

そしてチェック対象設定プログラム1302は、この判定において肯定結果を得ると、チェック対象管理テーブル1303における該当マスタVMの該当チェック項目の欄に「個別」を設定し（SP705）、否定結果を得ると、当該チェック項目の欄に「マスタ」を設定する（ステップ706）。

10 そしてチェック対象設定プログラム1302は、ステップSP705又はステップSP706の処理を完了すると、この図33に示すチェック対象設定処理を終了する。

15 以上のように本実施の形態によるセキュリティ管理方法によれば、1つのチェック項目に対してマスタVM別に異なるチェック対象を指定できるため、第3の実施の形態により得られる効果に加えて、より詳細なセキュリティ管理を行うことができる。

産業上の利用可能性

本発明は、ネットワーク上の仮想クライアントに対してセキュリティ検査を行う種々の構成のセキュリティ管理装置に広く適用することができる。

請求の範囲

1. 物理クライアントがユーザ端末に提供するそれぞれ仮想的な計算機環境である複数の仮想マシンのセキュリティを管理するセキュリティ管理装置
5 において、

前記複数の仮想マシンに対するセキュリティチェックに関する1又は複数のチェック項目を規定したチェックポリシーと、セキュリティチェックプログラムとを記憶する記憶装置と、

前記セキュリティチェックプログラムに基づき、前記チェックポリシーに従
10 って、前記複数の仮想マシンに対するセキュリティチェックを実行するCPU (Central Processing Unit) と

を備え、

前記CPUは、前記仮想マシンの種別として、仮想マシンの一部又は全部を構成するマスタ情報に基づき構築されるマスタ仮想マシンと、前記マスタ
15 情報により一部又は全部が構成される個別情報に基づき構築される個別仮想マシンとを管理し、

前記CPUは、前記セキュリティチェックを、前記チェック項目ごとに、当該チェック項目の内容に応じた種別の前記仮想マシンに対して選択的に実行する

20 ことを特徴とするセキュリティ管理装置。

2. 前記個別仮想マシンは、再起動後に前記マスタ情報の変更が反映され、
前記CPUは、

前記マスタ情報の変更後に、前記個別仮想マシンが再起動されているか否かを確認する

25 ことを特徴とする請求項1に記載のセキュリティ管理装置。

3. 前記チェックポリシーにおいて、前記チェック項目ごとに重要度が予め設

定され、

前記CPUは、

前記チェック項目に設定された重要度に応じて当該チェック項目のセキュリティチェックを実行するか否かを判定する

5 ことを特徴とする請求項1に記載のセキュリティ管理装置。

4. 前記チェックポリシーにおいて、前記チェック項目ごとにセキュリティチェックを実行すべきチェック期限が予め設定され、

前記CPUは、

10 先行するチェック期限内にセキュリティチェックを実行していない前記チェック項目のセキュリティチェックを優先的に実行する

ことを特徴とする請求項1に記載のセキュリティ管理装置。

5. 前記チェックポリシーにおいて、前記セキュリティチェックのチェック対象となる前記仮想マシンの種別が、前記チェック項目ごとにユーザにより予め定められた

15 ことを特徴とする請求項1に記載のセキュリティ管理装置。

6. 前記CPUは、

前記チェックポリシーにおいて、前記セキュリティチェックのチェック対象を自動選択すべき設定がなされている前記チェック項目については、当該チェック項目に関して前記個別仮想マシンごとにカスタマイズが可能か否かに

20 基づいて、チェック対象とする前記仮想マシンの種別を選択する

ことを特徴とする請求項1に記載のセキュリティ管理装置。

7. 前記CPUは、

チェック対象の前記仮想マシンが動作を停止中であるときには、前記物理クライアントにおける空きリソース量に応じて、当該仮想マシンに対して実行するセキュリティチェックのチェック項目を決定する

25 行するセキュリティチェックのチェック項目を決定する

ことを特徴とする請求項1に記載のセキュリティ管理装置。

8. 物理クライアントがユーザ端末に提供するそれぞれ仮想的な計算機環境である複数の仮想マシンのセキュリティを管理するセキュリティ管理方法において、

前記複数の仮想マシンに対するセキュリティチェックに関する 1 又は複数の
5 のチェック項目を規定したチェックポリシーと、セキュリティチェックプログラムとを記憶する第 1 のステップと、

前記セキュリティチェックプログラムに基づき、前記チェックポリシーに従って、前記複数の仮想マシンに対するセキュリティチェックを実行する第 2
のステップと

10 を備え、

前記仮想マシンの種別として、仮想マシンの一部又は全部を構成するマスタ情報に基づき構築されるマスタ仮想マシンと、前記マスタ情報により一部又は全部が構成される個別情報に基づき構築される個別仮想マシンとが存在し、

15 前記第 2 のステップでは、

前記セキュリティチェックを、前記チェック項目ごとに、当該チェック項目の内容に応じた種別の前記仮想マシンに対して選択的に実行することを特徴とするセキュリティ管理方法。

9. 前記個別仮想マシンは、再起動後に前記マスタ情報の変更が反映され、

20 前記第 2 のステップでは、

前記マスタ情報の変更後に、前記個別仮想マシンが再起動されているか否かを確認する

ことを特徴とする請求項 8 に記載のセキュリティ管理方法。

10. 前記チェックポリシーにおいて、前記チェック項目ごとに重要度が予め
25 設定され、

前記第 2 のステップでは、

前記チェック項目に設定された重要度に応じて当該チェック項目のセキュリティチェックを実行するか否かを判定する

ことを特徴とする請求項 8 に記載のセキュリティ管理方法。

- 1 1. 前記チェックポリシーにおいて、前記チェック項目ごとにセキュリティ
5 チェックを実行すべきチェック期限が予め設定され、

前記第 2 のステップでは、

先行するチェック期限内にセキュリティチェックを実行していない前記チェック項目のセキュリティチェックを優先的に実行する

ことを特徴とする請求項 8 に記載のセキュリティ管理方法。

- 10 1 2. 前記チェックポリシーにおいて、前記セキュリティチェックのチェック対象となる前記仮想マシンの種別が、前記チェック項目ごとにユーザにより予め定められた

ことを特徴とする請求項 8 に記載のセキュリティ管理方法。

- 1 3. 前記第 2 のステップでは、

- 15 前記チェックポリシーにおいて、前記セキュリティチェックのチェック対象を自動選択すべき設定がなされている前記チェック項目については、当該チェック項目に関して前記個別仮想マシンごとにカスタマイズが可能か否かに基づいて、チェック対象とする前記仮想マシンの種別を選択する

ことを特徴とする請求項 8 に記載のセキュリティ管理方法。

- 20 1 4. 前記第 2 のステップでは、

チェック対象の前記仮想マシンが動作を停止中であるときには、前記物理クライアントにおける空きリソース量に応じて、当該仮想マシンに対して実行するセキュリティチェックのチェック項目を決定する

ことを特徴とする請求項 8 に記載のセキュリティ管理方法。

- 25 1 5. 前記セキュリティチェックは、前記物理クライアント以外のリソースに空きのあるその他の物理クライアントを用いて複数の仮想マシンの一部

の起動を伴うことを特徴とする請求項 1 に記載のセキュリティ管理装置。

図1

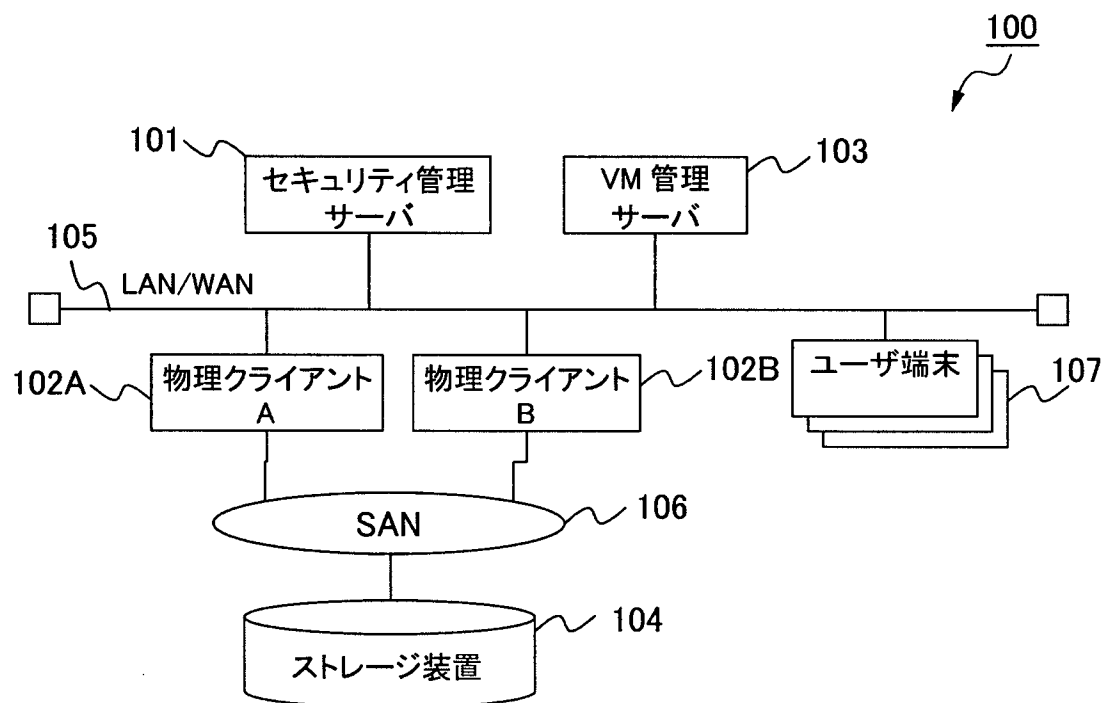


図2

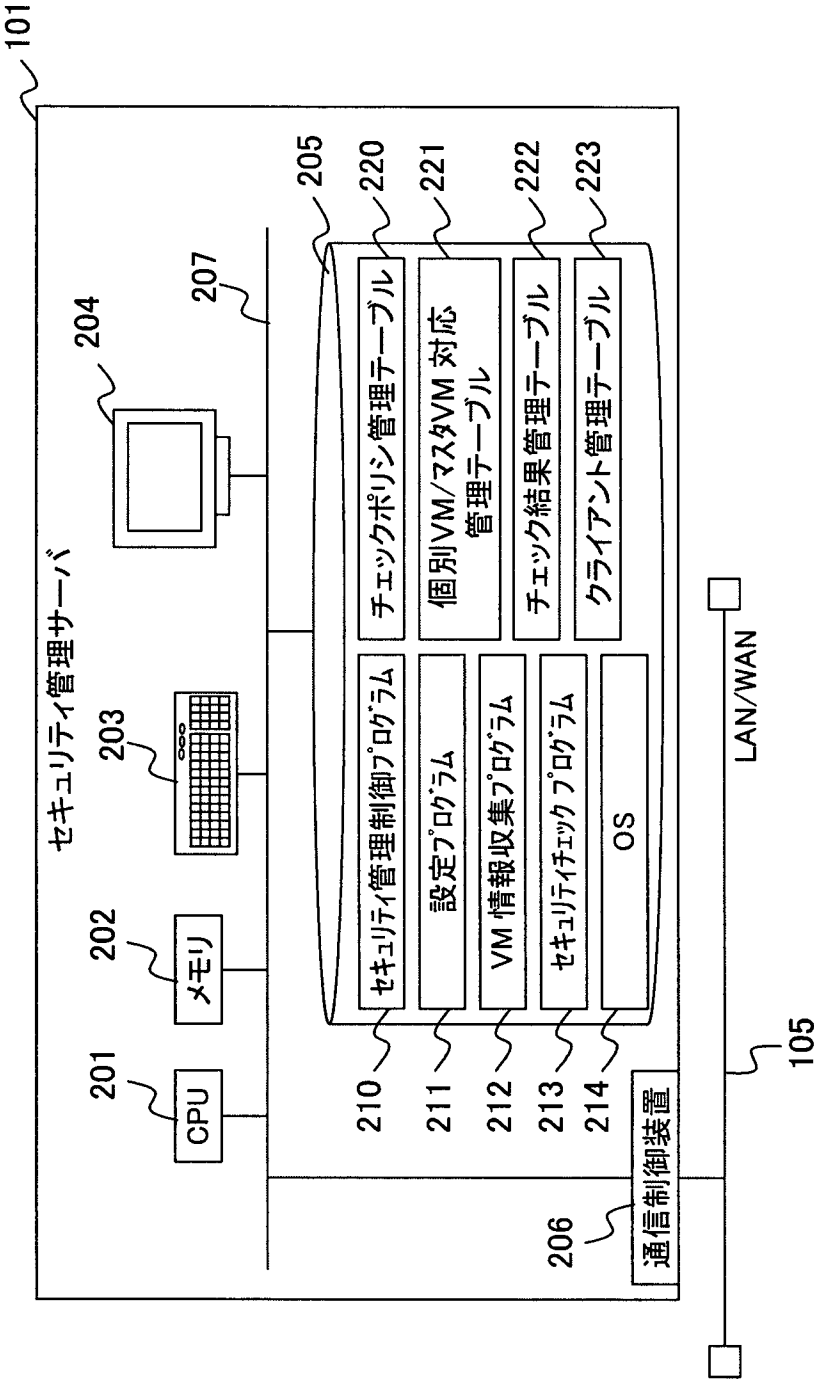


図3

チェック事項	ID	詳細	チェック対象	重要度	チェック期限
更新プログラム	C1-01	パッチA	マスタ	高	1日
	C1-02	パッチB	マスタ	中	7日
	...	...	...	...	...
ウイルス対策製品	C2	ウィルスチェッカーA, 1.0, 2008/1/1, ...	マスタ or 個別	高	1日
		ウィルスチェッカーB, 1.0, 2008/1/1, ...			
		...			
不正ソフトウェア	C3-01	ソフトウェアX, 2.0	個別	中	1日
	C3-02	ソフトウェアY, 全バージョン	マスタ and 個別	高	1日
	...	...	...	...	...
必須ソフトウェア	C4-01	ソフトウェアA, 6.0	マスタ	低	14日
	C4-02	ソフトウェアB, 5.0	マスタ	高	1日
	...	...	...	...	...
セキュリティ設定	C5-01	パスワード付きスクリーンセーバ設定の有無	個別	低	30日
	C5-02	ログインパスワードの脆弱性	個別	中	7日
	...	...	...	...	...

220A
220B
220C
220D
220E
220F
220

図4

クローンVM	マスタVM
VM2	VM1
VM3	VM1
VM4	VM1

221A

221B

221

図5

222A 222B 222C 222C				222C 222C				222C 222C				222C 222C				222C 222C			
CID	マシンID	C1-01	C1-02	...	C2	...	C3-01	C3-02	...	C4-01	C4-02	...	C5-01	C5-02	...	222D			
001	VM1	○	○		○		○	○		○	—		—	—		222D			
001	VM2	○	○		○		○	○		○	○		○	○					
001	VM3	○	○		○		○	○		○	○		○	○					
001	VM4	○	○		○		○	○		○	○		×	○					
002	VM1	○	○		○		—	○		未	○		—	—		222E			
002	VM2	○	○		○		未	未		未	○		未	未					
002	VM3	○	○		○		未	未		未	○		未	未					
002	VM4	○	○		○		未	未		未	○		未	未					
																222F			
																222G			
																222			

図6

223A		223B	223C	223D		
マシンID	IPアドレス	対応物理マシンID	リソース情報			...
VM1	10.1.1.1	PM1	CPU	メモリ	ディスク	...
VM2	10.1.1.2	PM1	2GHz	1GB	20GB	...
VM3	10.1.1.3	PM1	2GHz	1GB	20GB	...
VM4	10.1.1.4	PM1	2GHz	1GB	20GB	...

223DA

223DB

223DC

223

図7

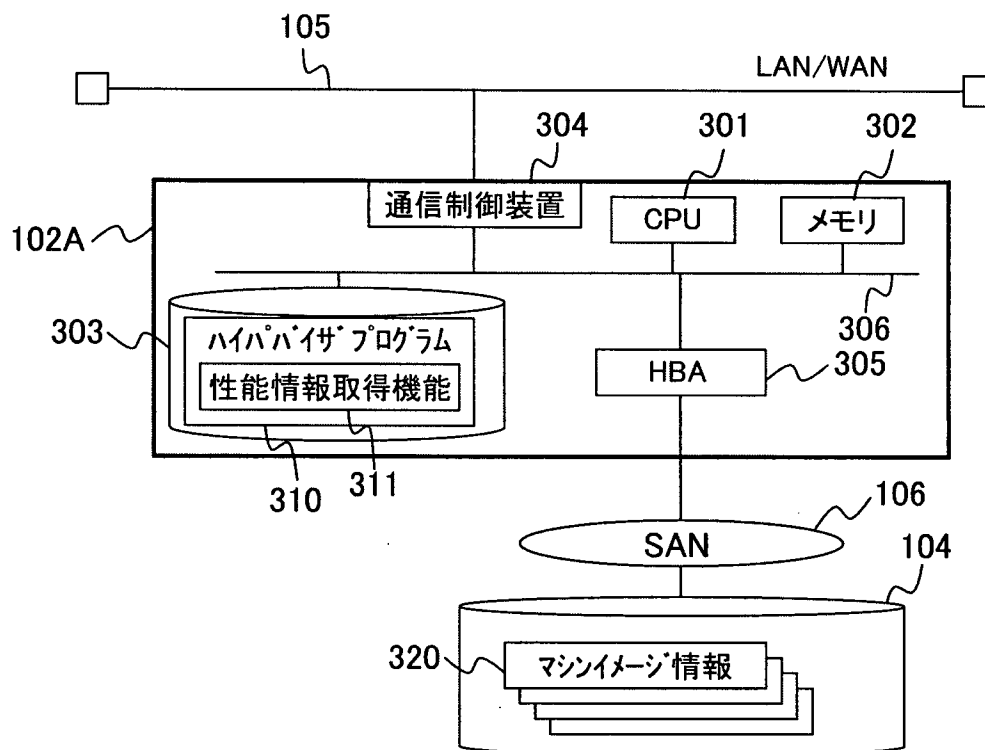


図8

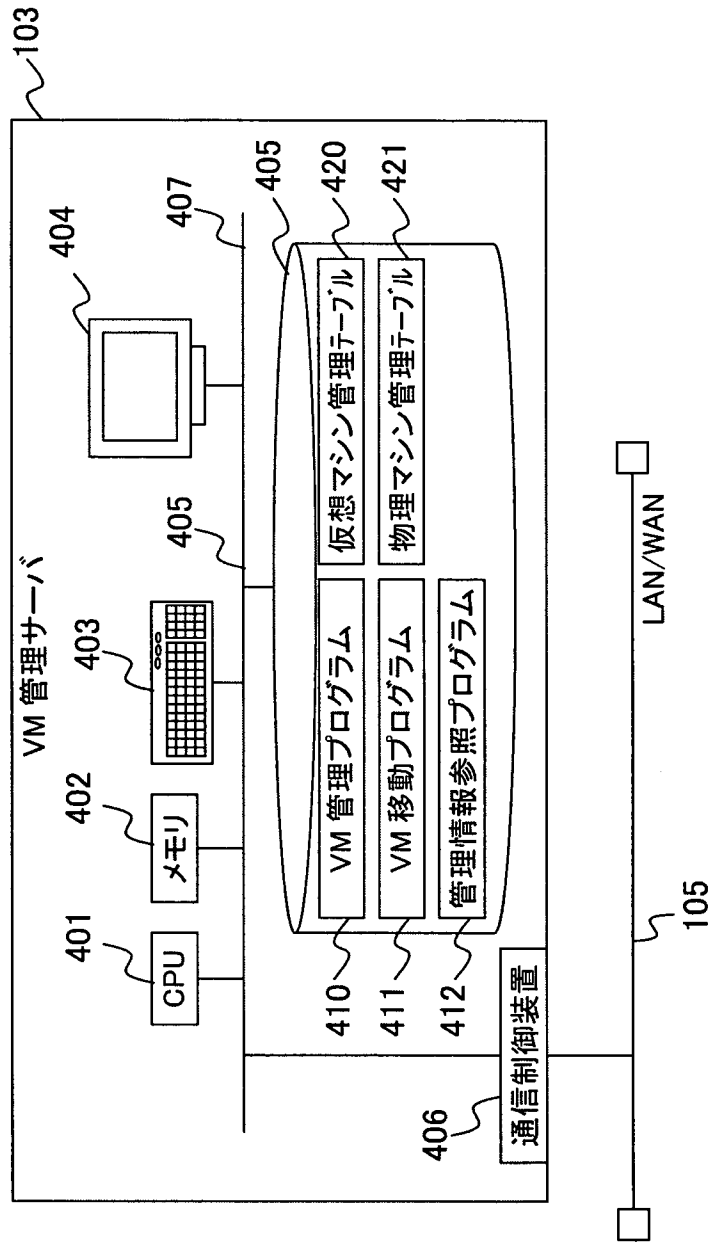


図9

420A		420B		420C		420D		420E		
マシンID	IPアドレス	対応物理 マシンID	状態	リソース情報			...			
				CPU	メモリ	ディスク				
VM1	10.1.1.1	PM1	起動	2GHz	1GB	20GB	...			
VM2	10.1.1.2	PM1	起動	2GHz	1GB	20GB	...			
VM3	10.1.1.3	PM1	起動	2GHz	1GB	20GB	...			
VM4	10.1.1.4	PM1	停止	2GHz	1GB	20GB	...			

420EA

420EB

420EC

420

図10

421A		421B		421C		
マシンID	IPアドレス	リソース情報				
		CPU情報	メモリ情報	ディスク情報	...	
PM1	10.1.1.101	12GHz(3GHz × 4)	8GB	100GB	...	
PM2	10.1.1.102	12GHz(3GHz × 4)	8GB	100GB	...	
		421CA	421CB	421CC	<u>421</u>	

図11

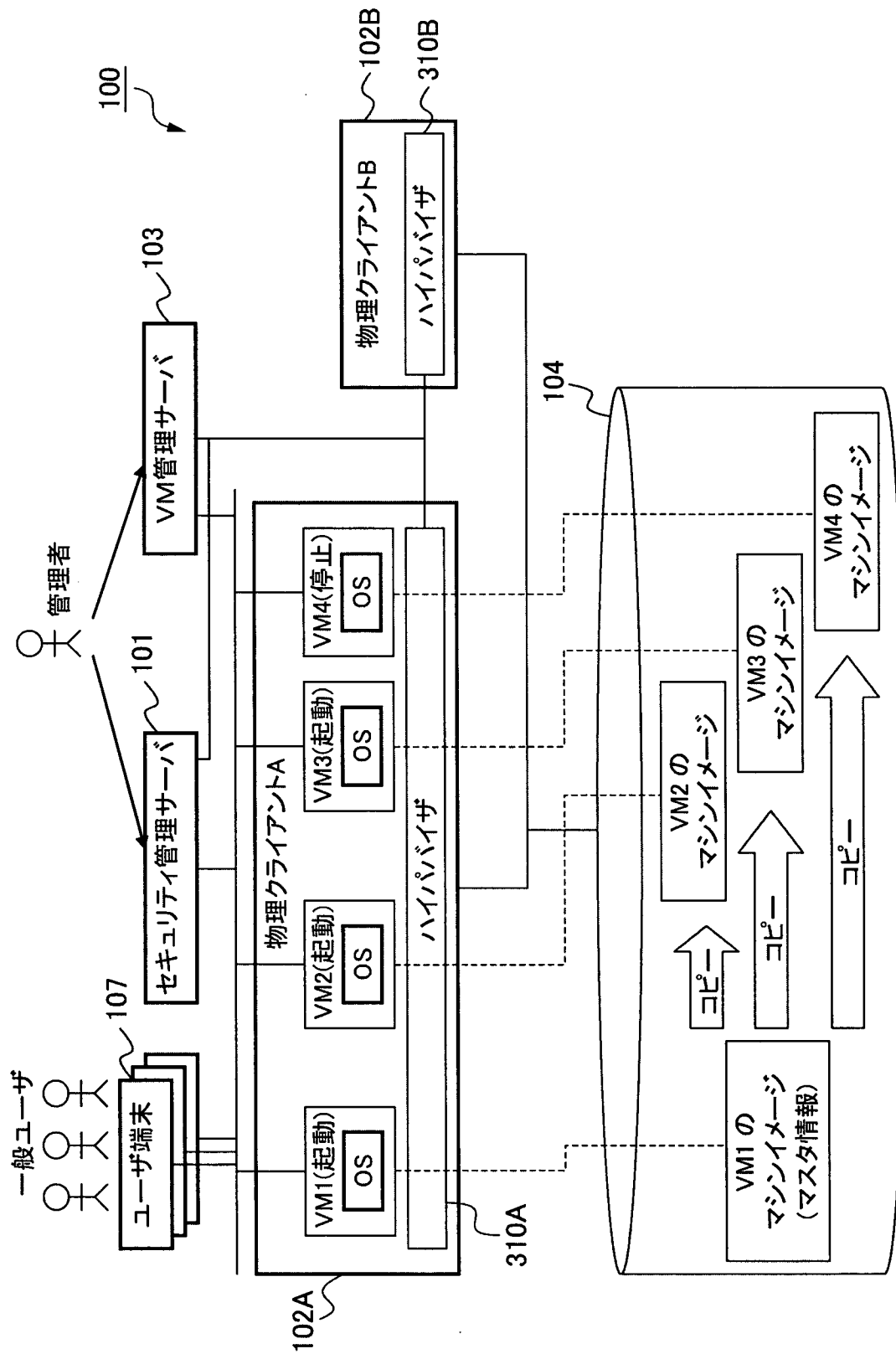


図12

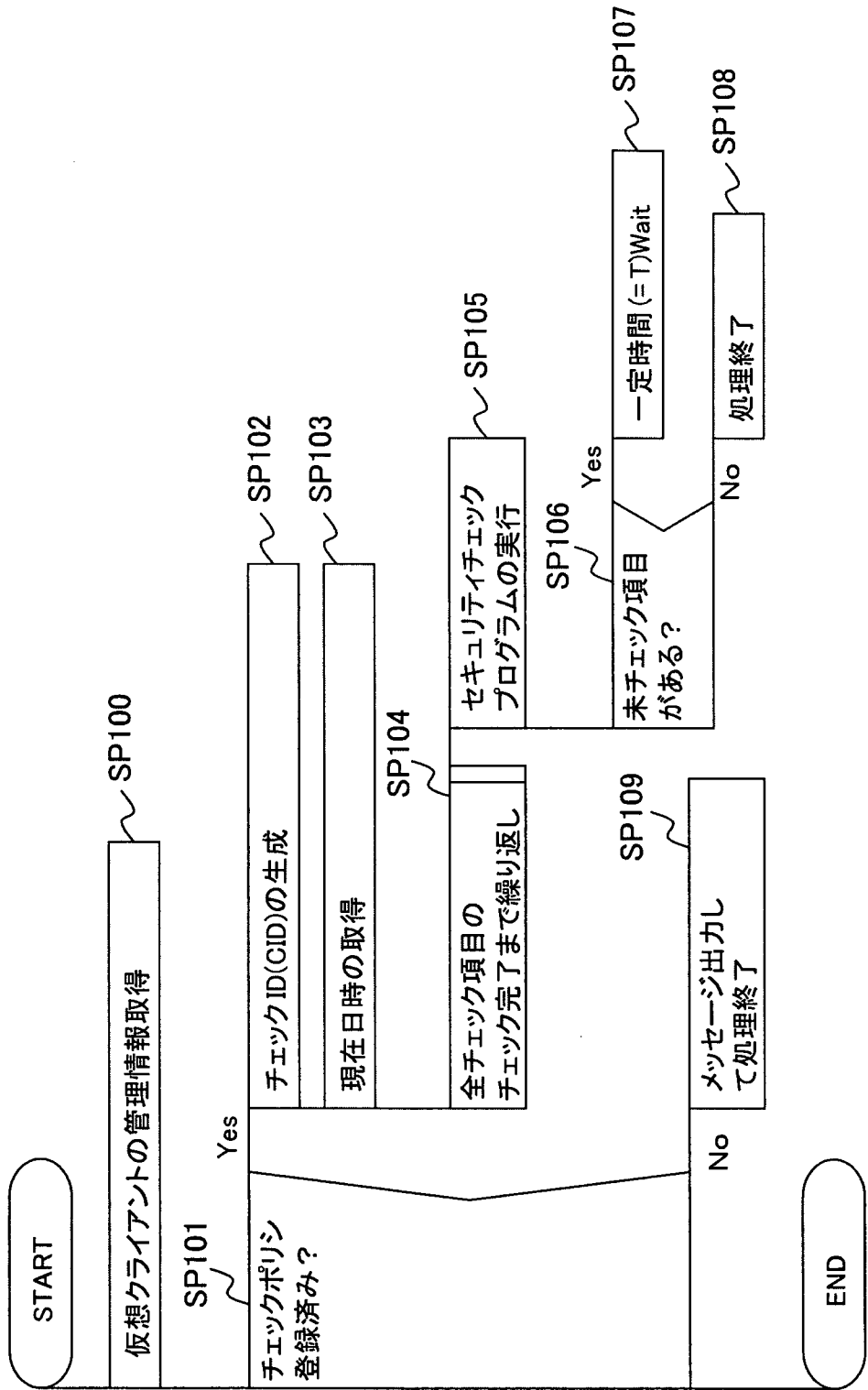


図13

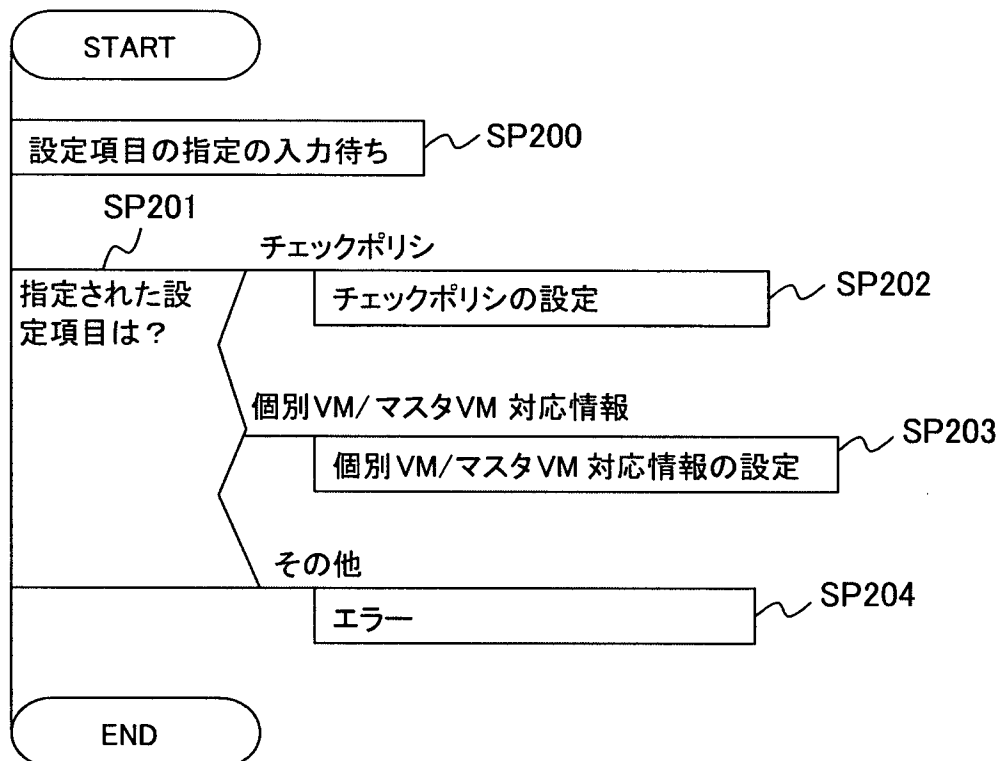


図14

チェックポリシー設定 - ☐ ☒

■ **更新プログラムの判定** ● ON ○ OFF 501A

更新プログラム	チェック対象	重要度	チェック期限
パッチA	マスタ	高	1日
パッチB	マスタ	中	7日

■ **ウイルス対策製品の判定** ● ON ○ OFF 502A

・許可する製品

ウイルス対策製品	バージョン	ウイルス定義	...
ウイルスチェッカーA	1.0	2008/1/1	
ウイルスチェッカーB	1.0	2008/1/1	

・チェックポリシー

チェック対象	重要度	チェック期限
マスタ or 個別	高	1日

■ **不正ソフトウェアの判定** ● ON ○ OFF 503A

不正ソフトウェア	バージョン	チェック対象	重要度	チェック期限
ソフトウェアX	2.0	個別	中	1日
ソフトウェアY		マスタ and 個別	高	1日

■ **必須ソフトウェアの判定** ● ON ○ OFF 504A

必須ソフトウェア	バージョン	チェック対象	重要度	チェック期限
ソフトウェアA	6.0	マスタ	低	14日
ソフトウェアB	5.0	マスタ	高	1日

■ **セキュリティ設定の判定**

チェック項目	チェック要非	チェック対象	重要度	チェック期限
パスワード付きスクリーンセーバの設定	要	個別	低	30日
ログインパスワードの脆弱性	要	個別	中	7日
無期限パスワード設定禁止	非	—	—	—

506
 507

図15

600

—☐ ☒

個別VM/ マスタVM 対応情報設定

601

■ 管理対象 VM 一覧

仮想マシンID	IPアドレス	CPU	メモリ	ディスク	...
VM1	10.1.1.1	...	...	...	...
VM2	10.1.1.2	...	...	...	...
VM3	10.1.1.3	...	...	...	...
VM4	10.1.1.4	...	...	...	...

602

■ 登録済み情報

選択	個別 VM	マスタVM
☒	VM2	VM1
☐	VM3	VM1

607

603

削除

604

■ 追加

・個別 VM : VM4

・マスタ VM : VM1

605

追加

606

終了

図16

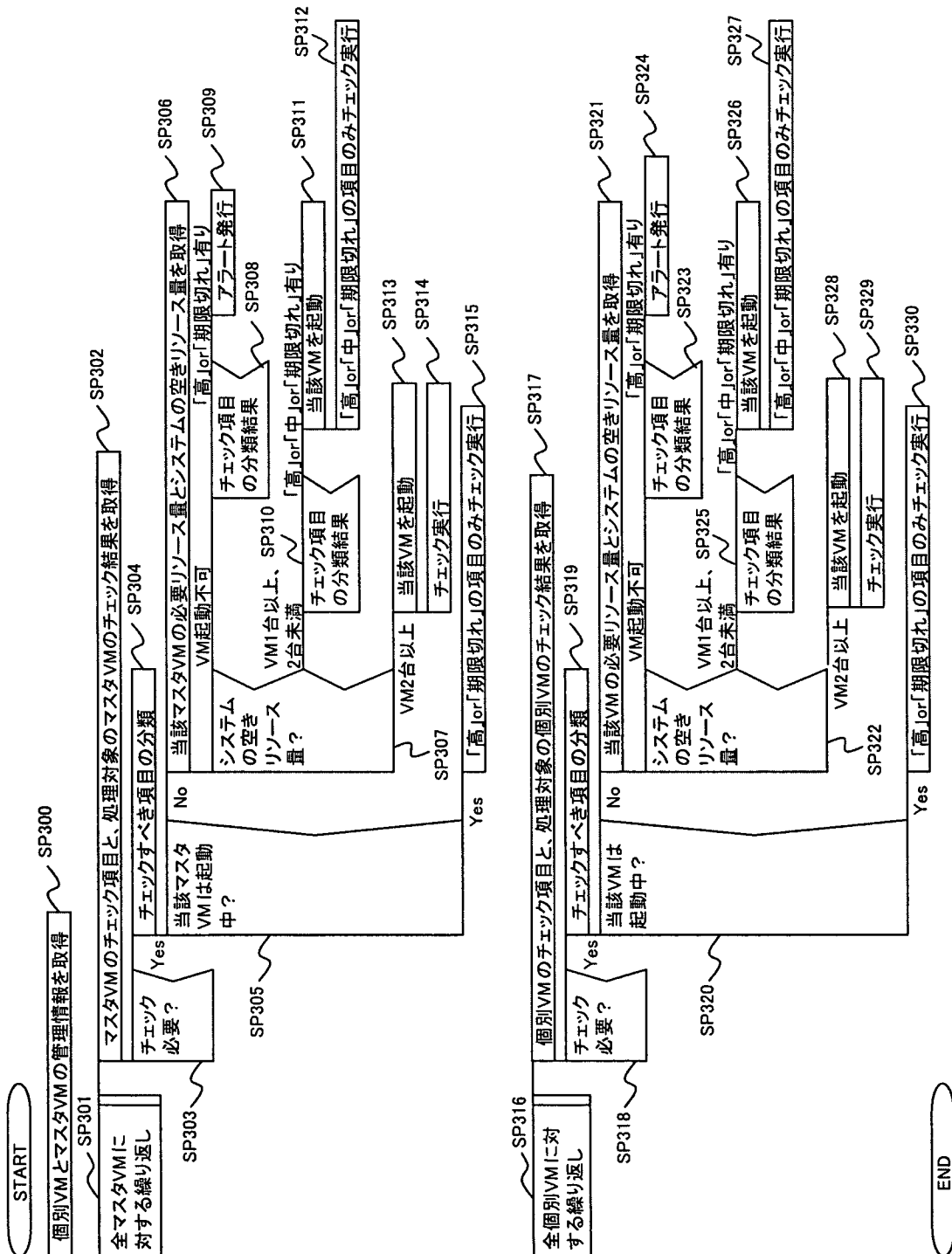


図17

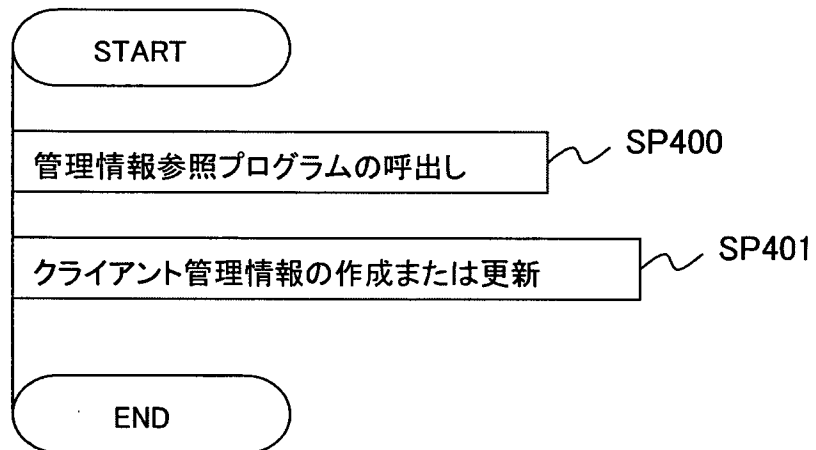


图 18

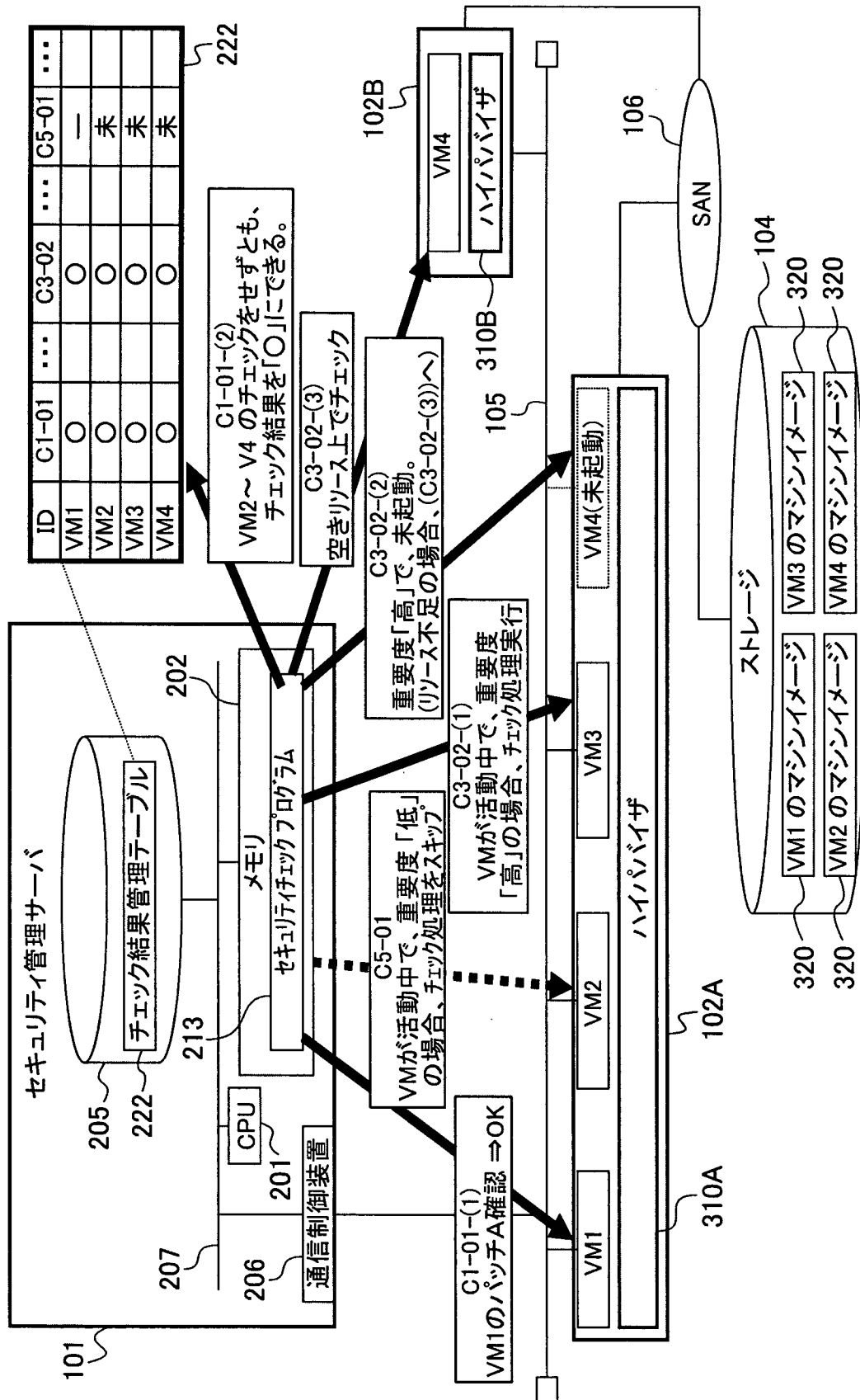


図19

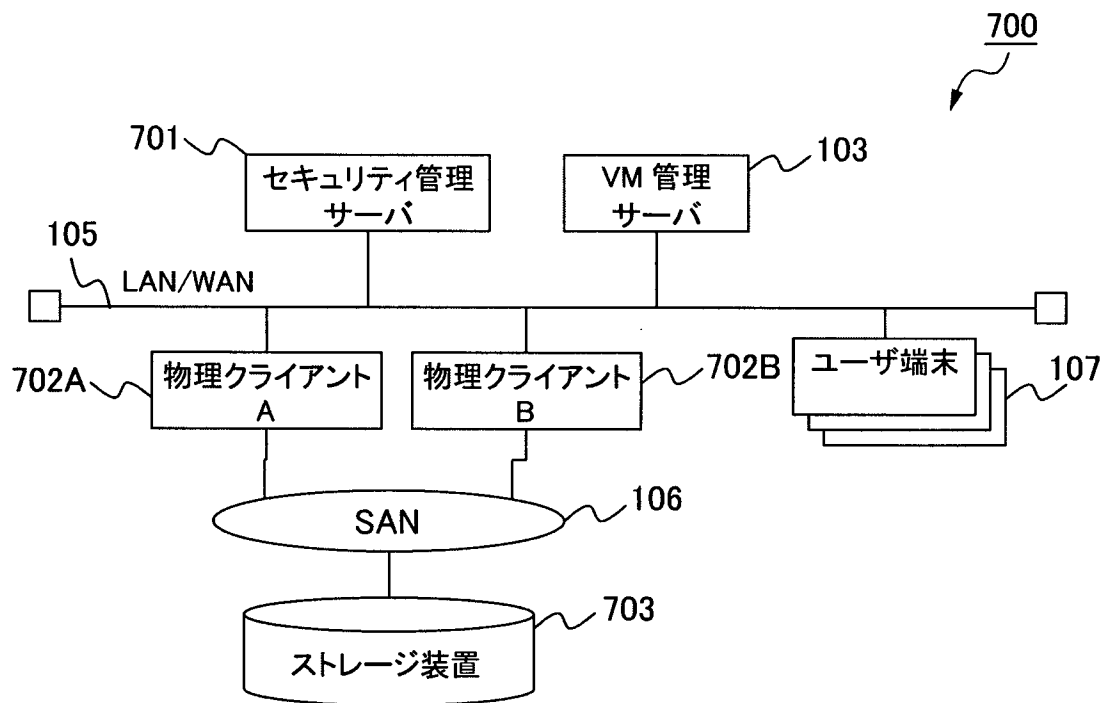


図20

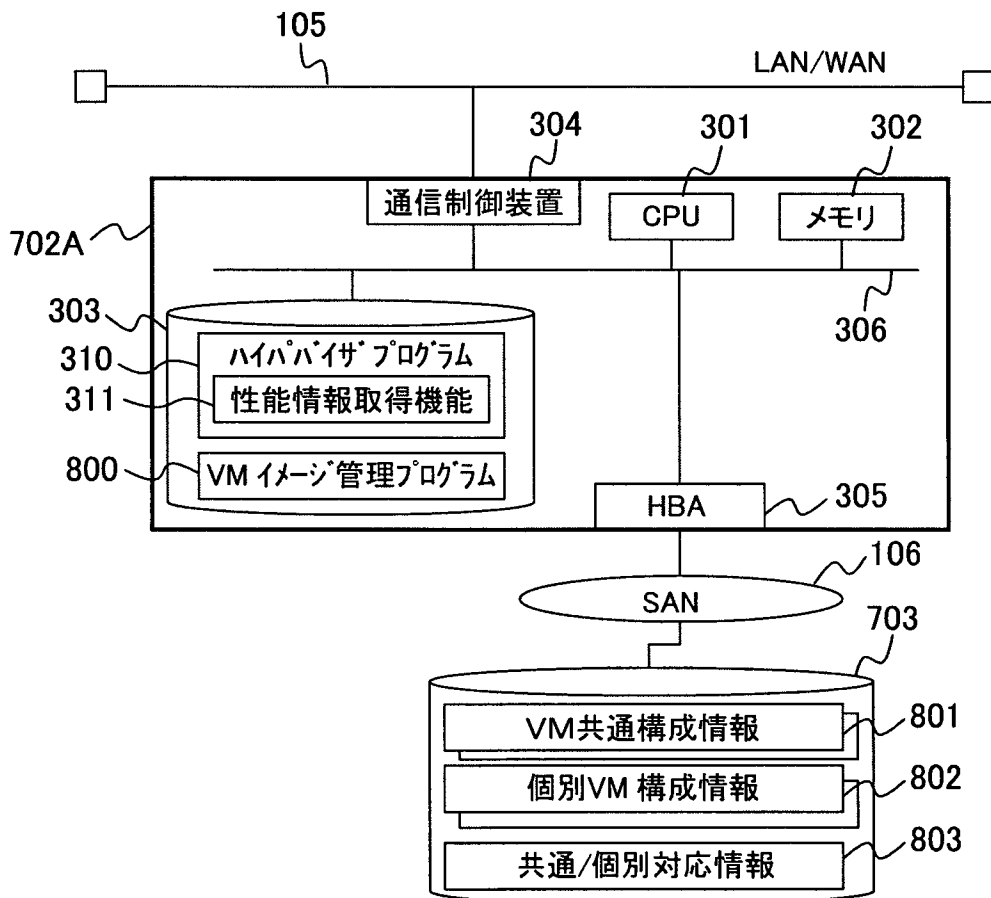


图21

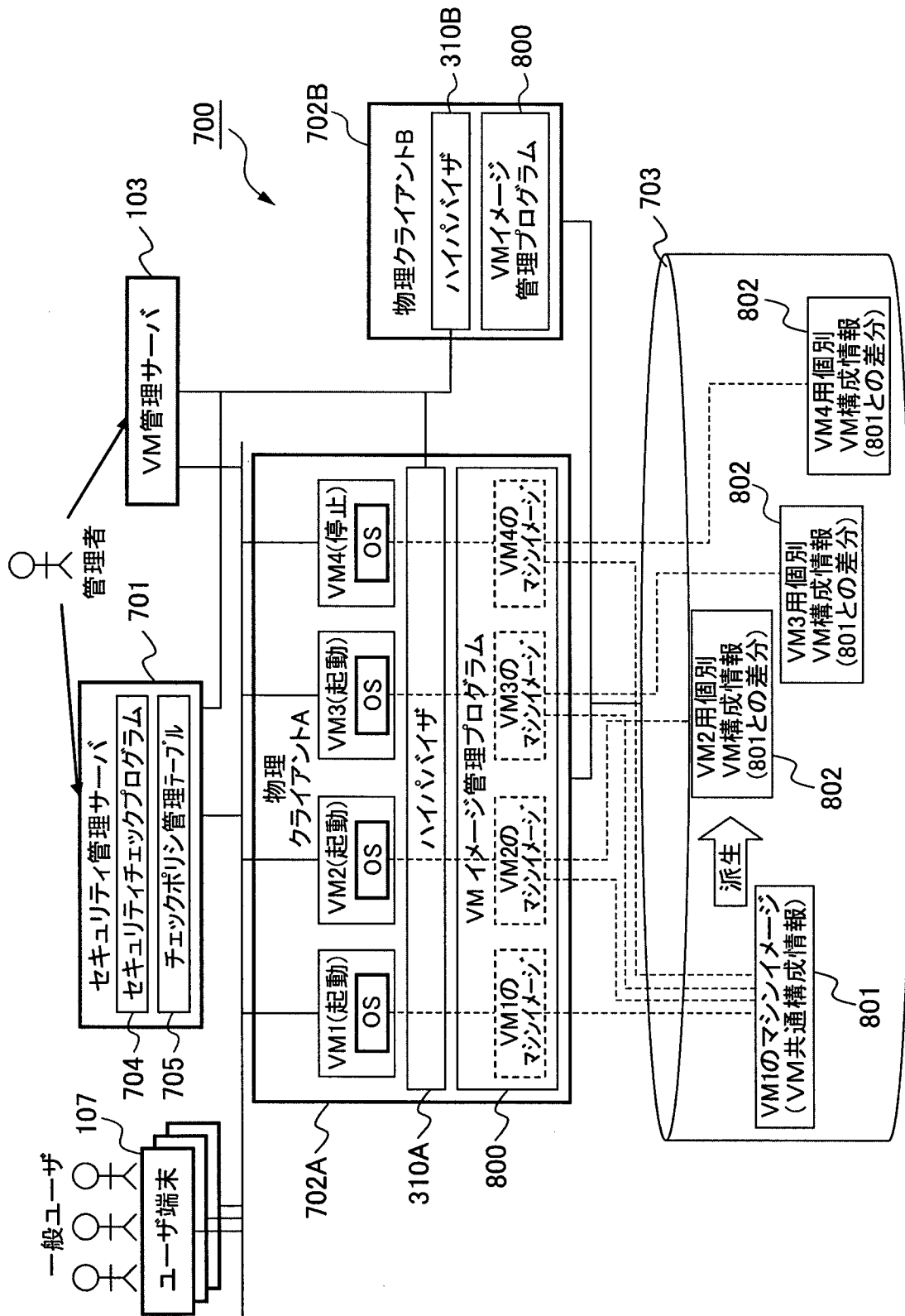


図22

チェック事項	ID	詳細	チェック対象	重要度	チェック期限
更新プログラム	C1-01	パッチA	マスタ	高	1日
	C1-02	パッチB	マスタ	中	7日
	...	...	...	...	...
ウイルス対策製品	C2	ウイルスチェッカー-A, 1.0, 2008/1/1, ...	マスタ or 個別	高	1日
		ウイルスチェッカー-B, 1.0, 2008/1/1, ...			
		...			
不正ソフトウェア	C3-01	ソフトウェアX, 2.0	個別	中	1日
	C3-02	ソフトウェアY, 全バージョン	マスタ and 個別	高	1日
	...	...	...	...	...
必須ソフトウェア	C4-01	ソフトウェアA, 6.0	マスタ	低	14日
	C4-02	ソフトウェアB, 5.0	マスタ	高	1日
	...	...	...	...	...
セキュリティ設定	C5-01	パスワード付きスクリーンセーバ設定の有無	個別	低	30日
	C5-02	ログインパスワードの脆弱性	個別	中	7日
	...	...	...	...	...
マスタの変更の反映	C6		個別	高	1日

図23

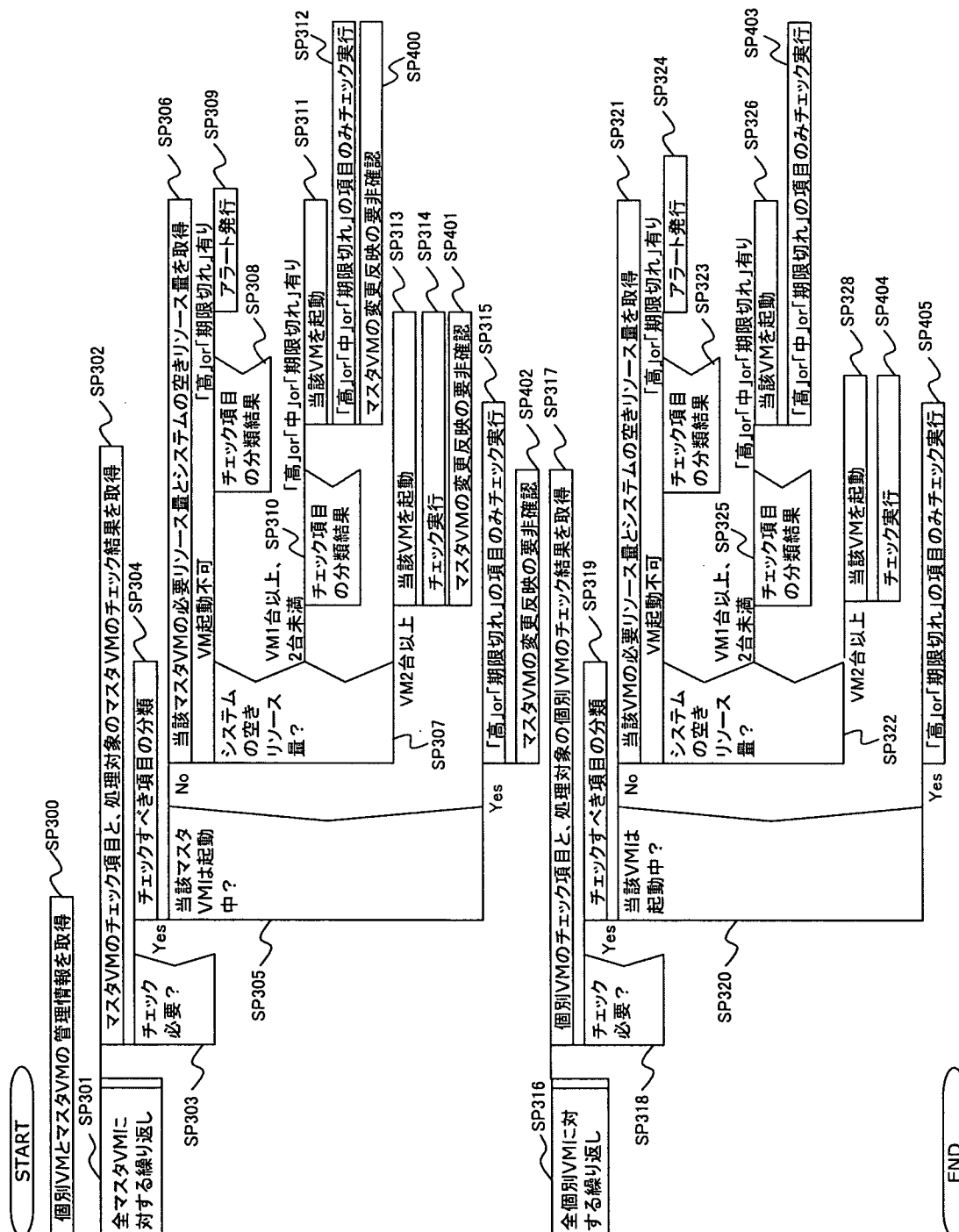


図24

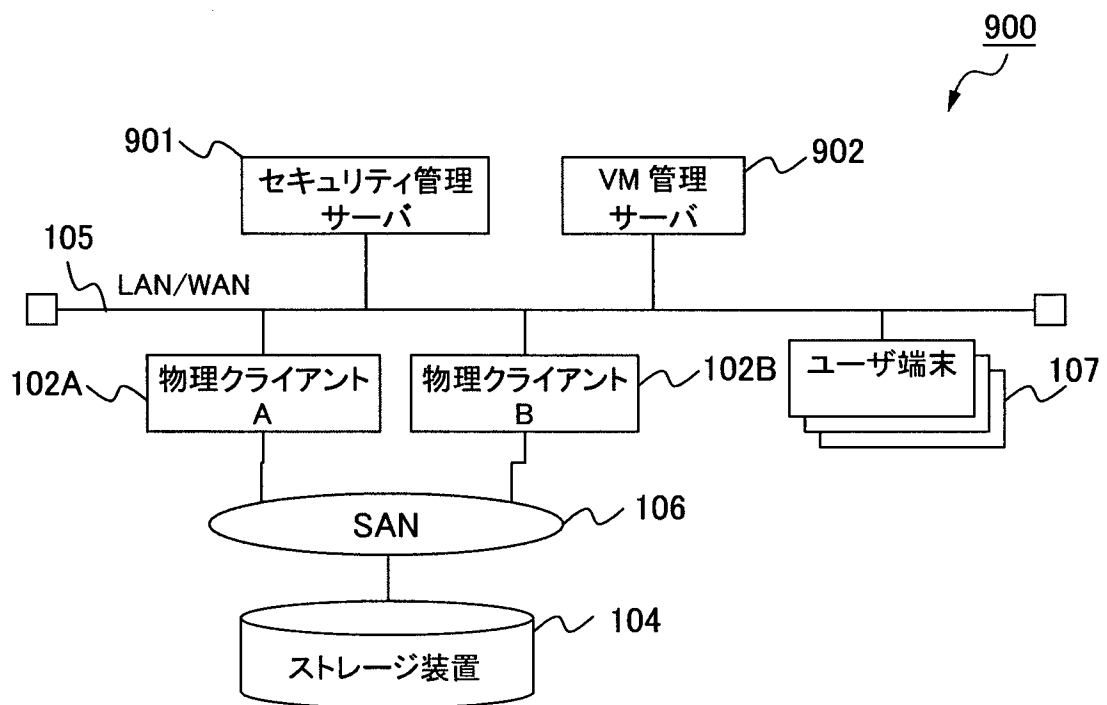


図25

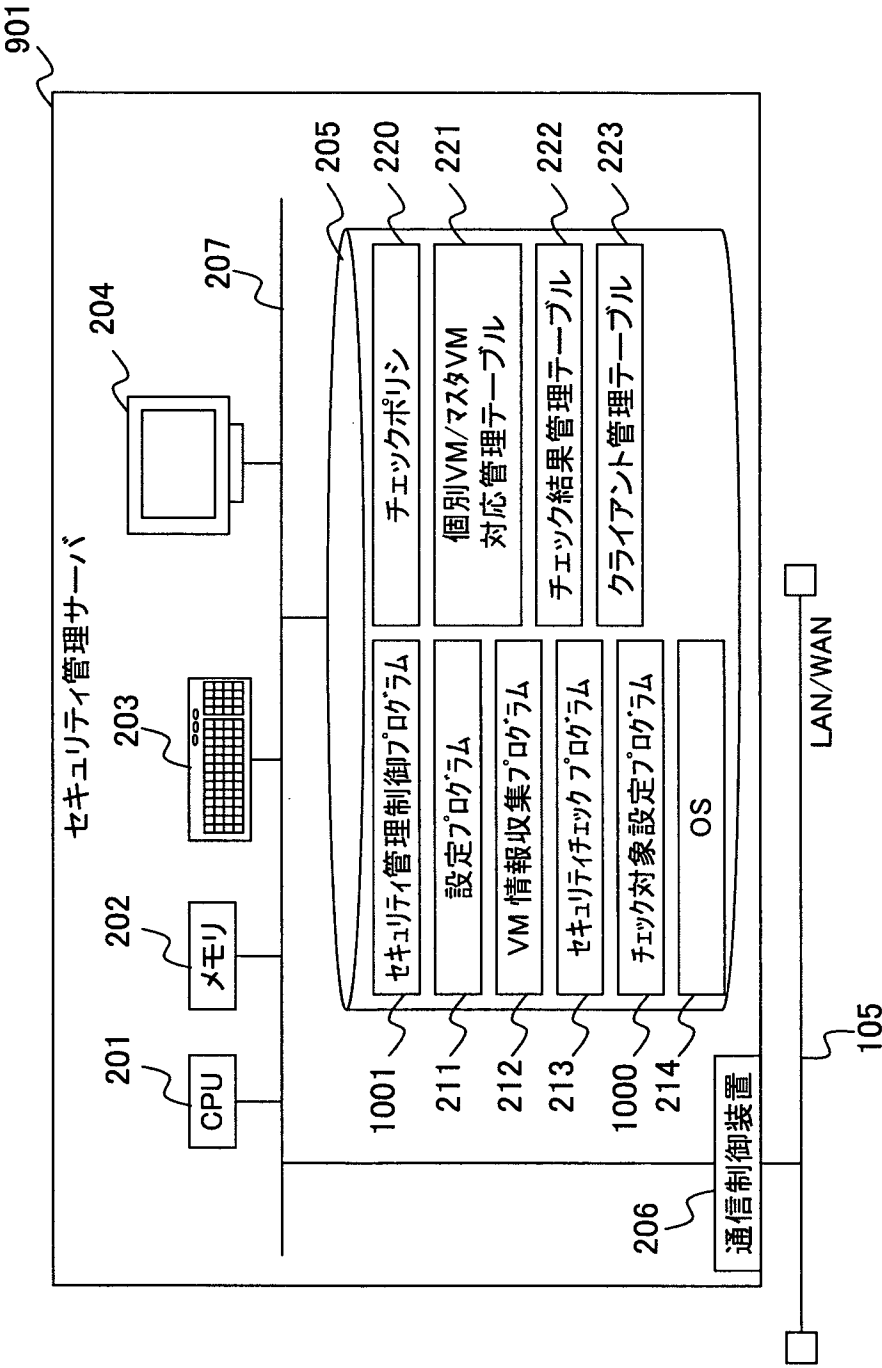


図26

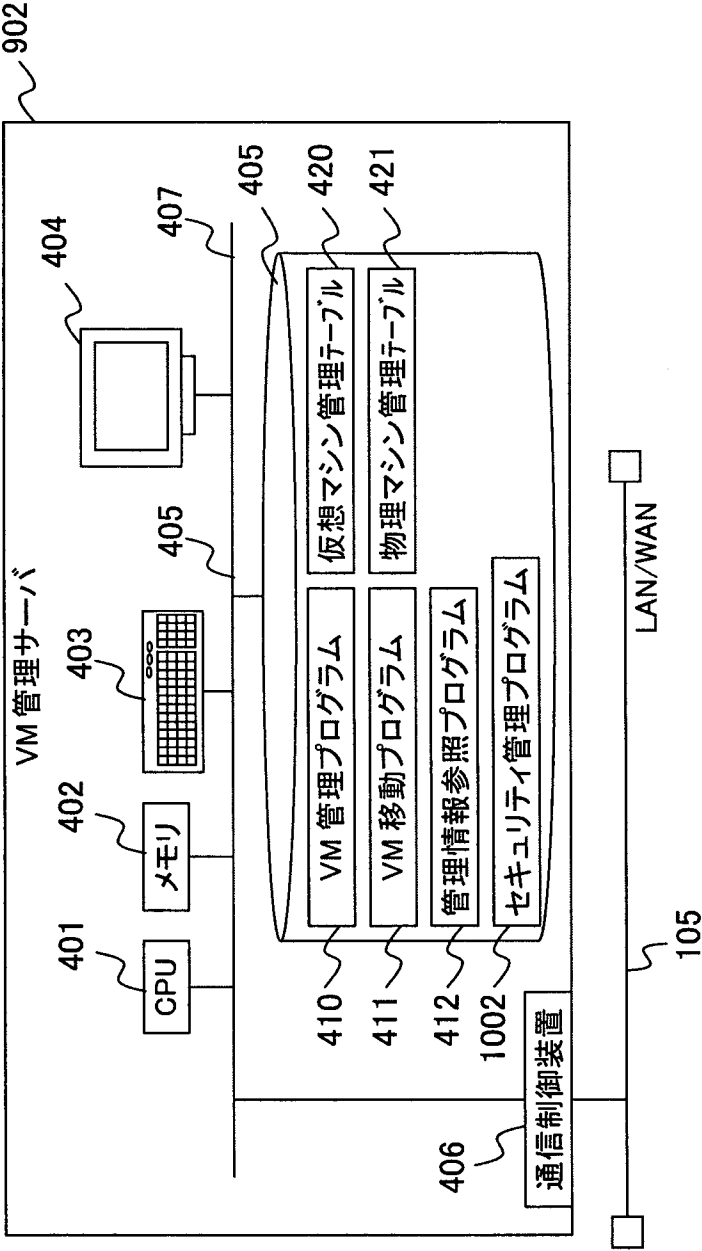


図27

チェックポリシー設定 - ☐ ☒

■更新プログラムの判定 ●ON ○OFF 501A

更新プログラム	チェック対象	重要度	チェック期限
パッチA	自動	高	1日
パッチB	自動	中	7日

■ウイルス対策製品の判定 ●ON ○OFF 502A

許可する製品

ウイルス対策製品	バージョン	ウイルス定義	...
ウイルスチェッカーA	1.0	2008/1/1	
ウイルスチェッカーB	1.0	2008/1/1	

・チェックポリシー

チェック対象	重要度	チェック期限
自動	高	1日

■不正ソフトウェアの判定 ●ON ○OFF 503A

不正ソフトウェア	バージョン	チェック対象	重要度	チェック期限
ソフトウェアX	2.0	自動	高	1日
ソフトウェアY		自動	中	1日

■必須ソフトウェアの判定 ●ON ○OFF 504A

必須ソフトウェア	バージョン	チェック対象	重要度	チェック期限
ソフトウェアA	6.0	自動	低	14日
ソフトウェアB	5.0	自動	高	1日

■セキュリティ設定の判定 505

チェック項目	チェック要非	チェック対象	重要度	チェック期限
パスワード付きスクリーンセーバの設定	要	自動	低	30日
ログインパスワードの脆弱性	要	自動	中	7日
無期限パスワード設定禁止	非	—	—	—

OK 506
キャンセル 507

図28

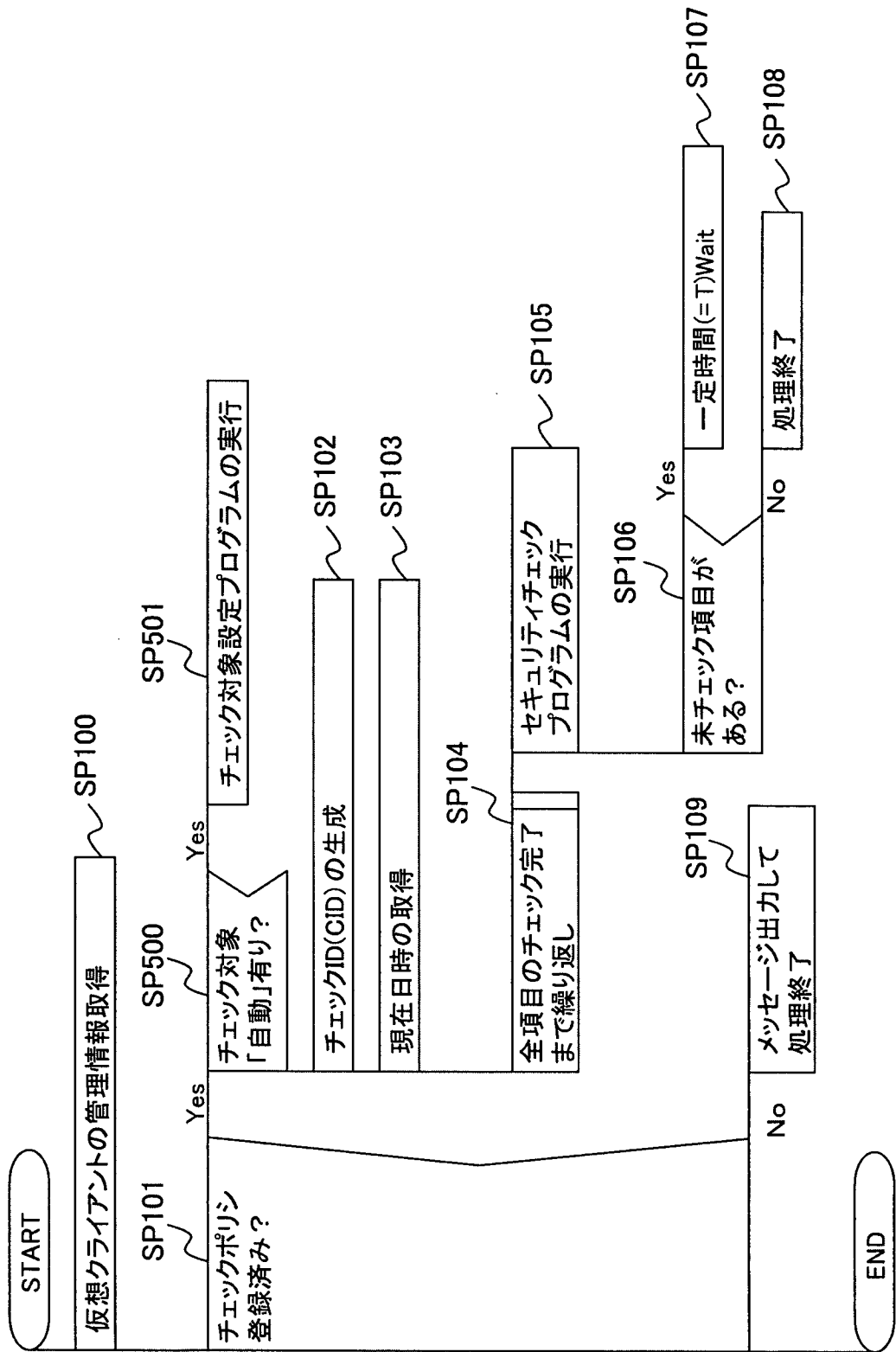


図29

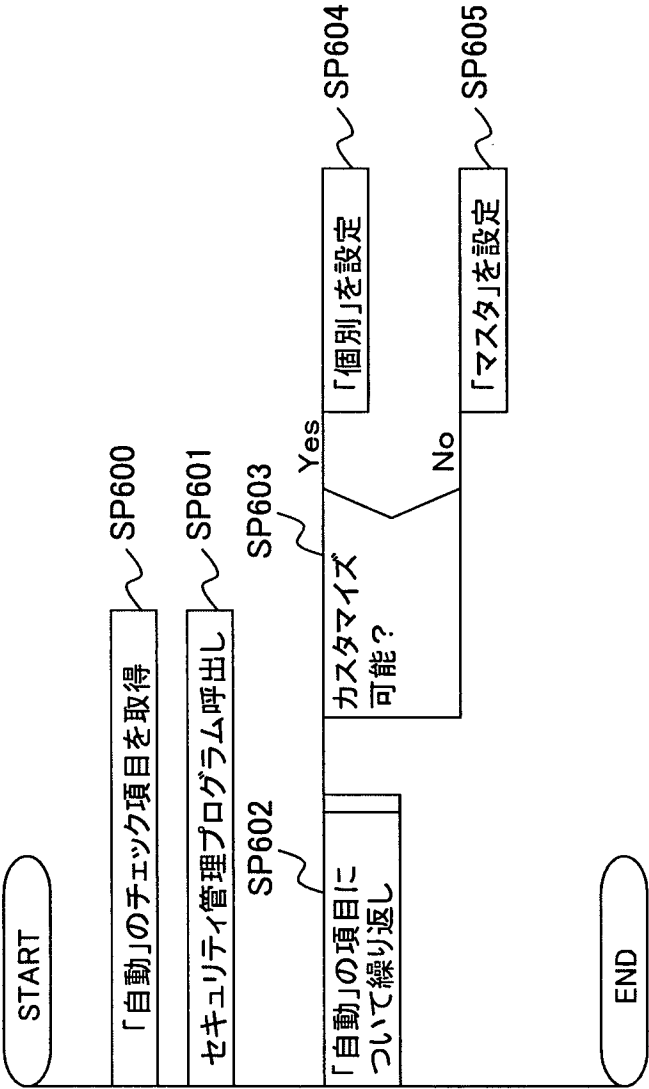


図30

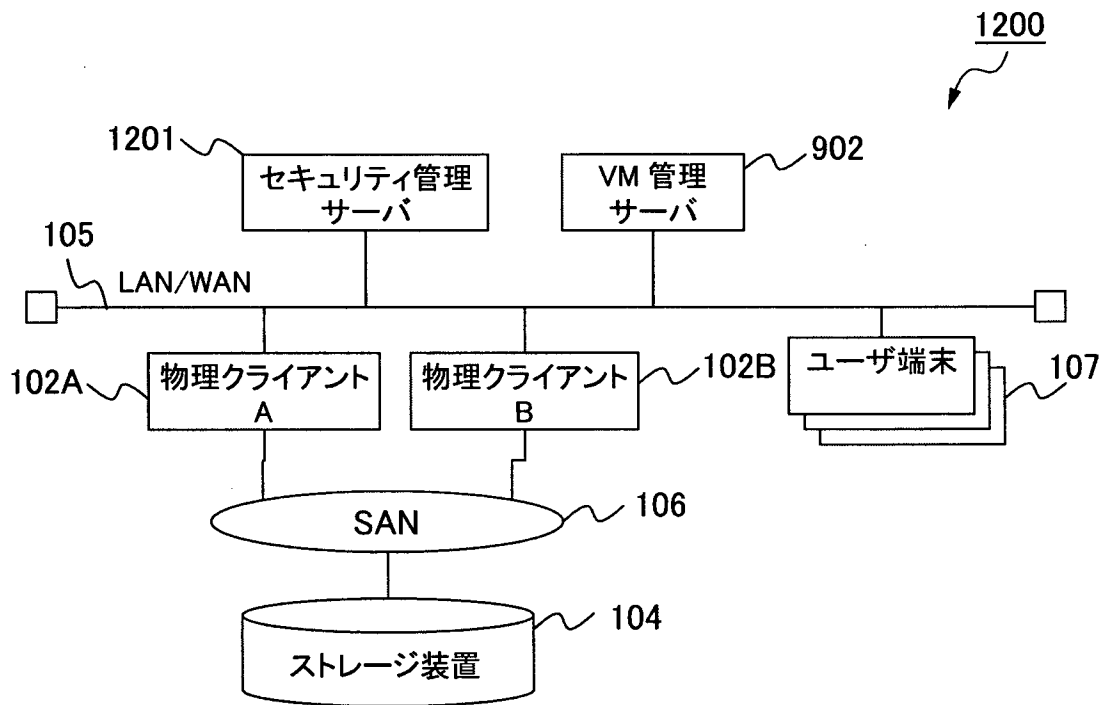


図31

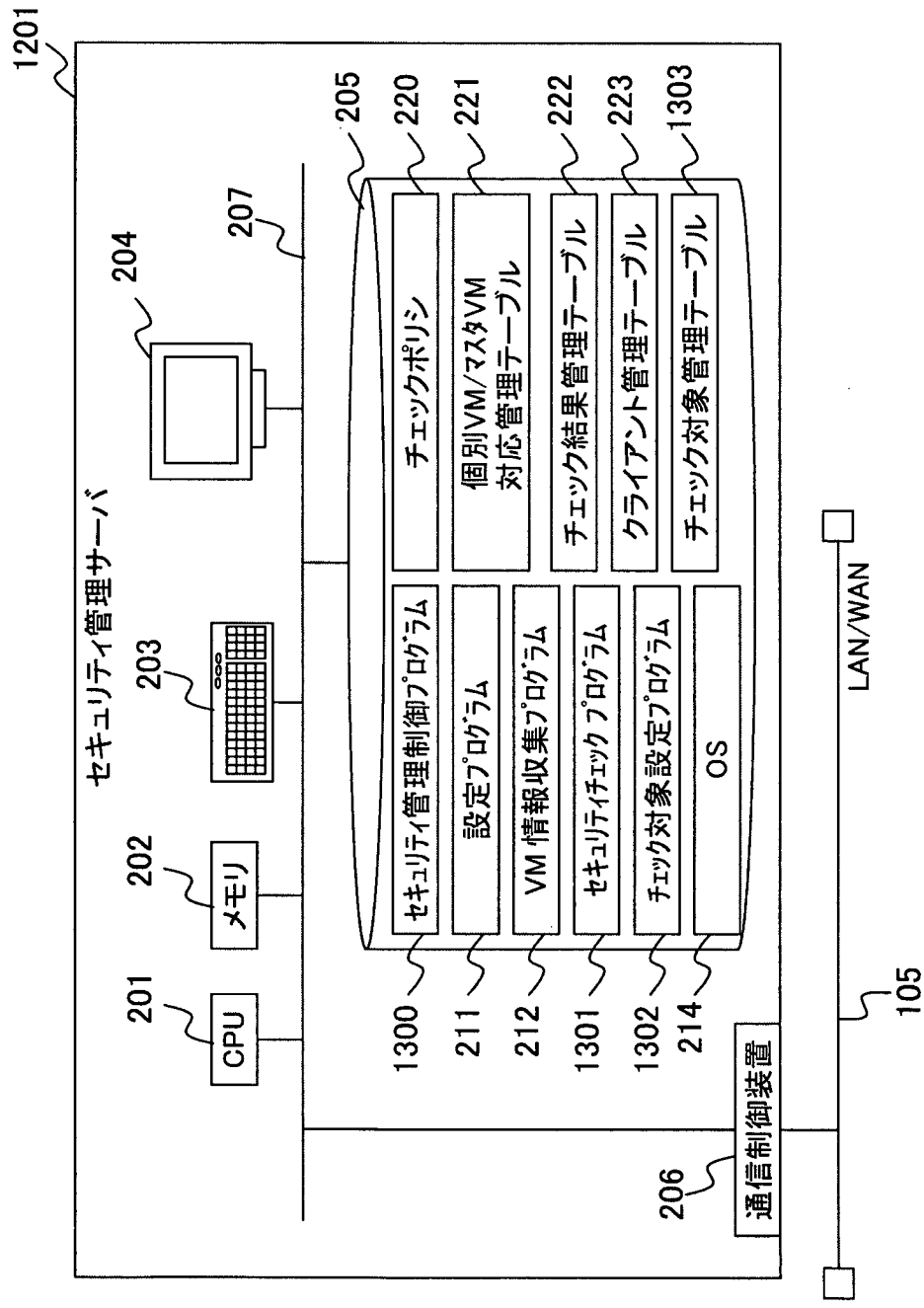
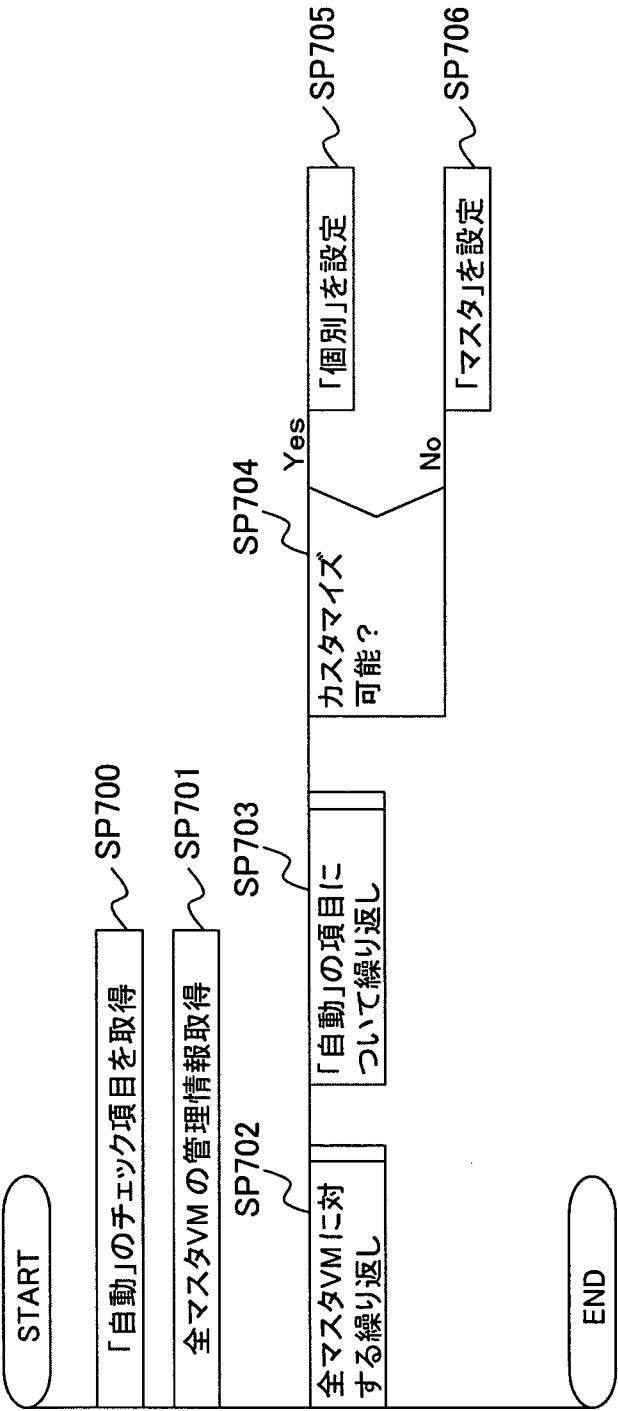


図33



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/054827

A. CLASSIFICATION OF SUBJECT MATTER

G06F21/22 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F21/22

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2009

Kokai Jitsuyo Shinan Koho 1971-2009 Toroku Jitsuyo Shinan Koho 1994-2009

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-296132 A (Mitsubishi Electric Corp.), 17 October, 2003 (17.10.03), Abstract; Par. Nos. [0009] to [0010]; Fig. 6 (Family: none)	1-15
A	JP 6-230957 A (Toshiba Corp.), 19 August, 1994 (19.08.94), Par. Nos. [0009] to [0013]; Fig. 1 (Family: none)	1-15
A	JP 2008-027322 A (Hitachi, Ltd.), 07 February, 2008 (07.02.08), Abstract; Claim 12; Par. No. [0050]; Fig. 29 (Family: none)	1-15

☒ Further documents are listed in the continuation of Box C.☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
08 April, 2009 (08.04.09)Date of mailing of the international search report
21 April, 2009 (21.04.09)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2009/054827

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2006-221649 A (Dell Products L.P.), 24 August, 2006 (24.08.06), Abstract; Par. Nos. [0009] to [0014]; Fig. 1 & US 2006/0184937 A1 & GB 602673 D0	1-15
A	JP 2006-235692 A (Hitachi, Ltd.), 07 September, 2006 (07.09.06), Abstract; Par. Nos. [0002] to [0012] (Family: none)	1-15
A	JP 2006-244373 A (Kabushiki Kaisha IT Sabisu), 14 September, 2006 (14.09.06), Abstract; Par. Nos. [0011] to [0014], [0053] to [0064]; Fig. 2 (Family: none)	1-15

A. 発明の属する分野の分類（国際特許分類（I P C））

Int.Cl. G06F21/22 (2006.01)i

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（I P C））

Int.Cl. G06F21/22

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 0 9 年
日本国実用新案登録公報	1 9 9 6 - 2 0 0 9 年
日本国登録実用新案公報	1 9 9 4 - 2 0 0 9 年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2003-296132 A（三菱電機株式会社）2003. 10. 17, 要約, 段落【0009】 - 【0010】, 図 6（ファミリーなし）	1-15
A	JP 6-230957 A（株式会社東芝）1994. 08. 19, 段落【0009】 - 【0013】, 図 1（ファミリーなし）	1-15
A	JP 2008-027322 A（株式会社日立製作所）2008. 02. 07, 要約, 請求項 12, 段落【0050】, 図 29（ファミリーなし）	1-15

☒ C 欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の 1 以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日

0 8 . 0 4 . 2 0 0 9

国際調査報告の発送日

2 1 . 0 4 . 2 0 0 9

国際調査機関の名称及びあて先

日本国特許庁（I S A / J P）

郵便番号 1 0 0 - 8 9 1 5

東京都千代田区霞が関三丁目 4 番 3 号

特許庁審査官（権限のある職員）

赤穂 州一郎

5 S

3 1 4 5

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 4 6

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求項の番号
A	JP 2006-221649 A (デル・プロダクツ・エル・ピー) 2006.08.24, 要約, 【0009】 - 【0014】, 図 1 & US 2006/0184937 A1 & GB 602673 D0	1-15
A	JP 2006-235692 A (株式会社日立製作所) 2006.09.07, 要約, 段落 【0002】 - 【0012】 (ファミリーなし)	1-15
A	JP 2006-244373 A (株式会社 I T サービス) 2006.09.14, 要約, 段落 【0011】 - 【0014】, 【0053】 - 【0064】, 図 2 (ファミリーなし)	1-15