(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4826077号
(P4826077)
(45)発行日　平成23年11月30日(2011.11.30)　(24)登録日　平成23年9月22日(2011.9.22)

(51)Int.Cl.　　F I
G06F 9/445 (2006.01)　　G06F 9/06 610K
G06F 3/06 (2006.01)　　G06F 3/06 301Z

請求項の数 4　(全 23 頁)

(21)出願番号　特願2004-251215(P2004-251215)
(22)出願日　平成16年8月31日(2004.8.31)
(65)公開番号　特開2006-72405(P2006-72405A)
(43)公開日　平成18年3月16日(2006.3.16)
審査請求日　平成19年7月24日(2007.7.24)

(73)特許権者　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　100100310
弁理士　井上　学
(72)発明者　高本　良史
東京都国分寺市東恋ケ窪一丁目２８０番地
株式会社日立製作所中央研究所内
(72)発明者　黒川　洋
神奈川県秦野市堀山下１番地　株式会社日立製作所エンタープライズサーバ事業部内
(72)発明者　畑▲崎▼　恵介
東京都国分寺市東恋ケ窪一丁目２８０番地
株式会社日立製作所中央研究所内

最終頁に続く

(54)【発明の名称】ブートディスク管理方法

(57)【特許請求の範囲】
【請求項１】
外部ディスク装置に接続された複数のサーバと、該複数のサーバを管理する管理サーバを有し、該複数のサーバと該管理サーバはネットワークスイッチを介して接続され、前記複数のサーバは前記外部ディスク装置からオペレーティングシステムをブートする計算機システムにおけるブートディスク管理方法であって、
前記管理サーバは、前記サーバと前記サーバが接続された前記ネットワークスイッチのポート番号と、該ポート番号に設定された仮想ネットワーク識別子を対応させた情報を記憶し、
前記対応情報に基づいて前記複数のサーバのうちの第１のサーバが接続された前記ネットワークスイッチのポート番号と前記管理サーバが接続された前記ネットワークスイッチのポート番号を取得し、前記第１のサーバと前記管理サーバとの間に構築する仮想ネットワークの識別子を設定し、
前記管理サーバから前記第１のサーバに対しエージェントプログラムを送信し、
該エージェントプログラムが前記第１のサーバのディスクインターフェースが有する固有情報を取得して前記管理サーバに転送し、前記管理サーバは転送された固有情報をもとに前記第１のサーバからアクセス可能な外部ディスクを設定することを特徴とするブートディスク管理方法。
【請求項２】
前記管理サーバは、前記仮想ネットワーク識別子を設定した後に、前記第１のサーバをリ

セットすることを特徴とする請求項１におけるブートディスク管理方法。
【請求項３】
前記エージェントプログラムは、前記管理サーバに備えられた前記複数のサーバとそれぞれの固有情報との対応表を元に前記第１サーバの固有情報を設定することを特徴とする請求項１に記載のブートディスク管理方法。
【請求項４】
前記対応情報は、前記サーバの識別子と前記仮想ネットワークの識別子とを対応させたサーバ管理テーブルに記憶していることを特徴とする請求項１に記載のブートディスク管理方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、外部ディスクからオペレーティングシステムを起動するサーバにおけるディスクの管理方法に関する。
【背景技術】
【０００２】
一般にディスク装置を備えたサーバシステムでは、サーバのオペレーティングシステムをディスク装置内のブートディスクにインストールしておき、サーバ起動時にブートディスクを発見しオペレーティングシステムをブートする構成とするのが一般的である。
従来技術の一つとして、サーバに内蔵された固定ディスクから起動するブート方法がある。サーバ内にあらかじめオペレーティングシステムをインストールするためのディスク装置を用意しておき、そのディスクにオペレーティングシステムをインストールすることでサーバをブートすることができる。この場合、サーバに対して１つのブートディスクしか存在せず、またブートディスクは他のサーバから共有される事はない。
【０００３】
従って、ブートディスクに対する他サーバから参照あるいは更新される可能性は少なくセキュリティは高い方法である。一方、ブート方法として、外部のディスクアレイ装置などからブートする形態がある。ディスクアレイ装置は、大規模な容量を有し、ファイバチャネルやファイバチャネルスイッチを介して複数のサーバと接続することができる。ディスクアレイ装置のように外部ディスクからＯＳをブートする場合は、セキュリティにおける課題がある。ディスクアレイ装置は、基本的にはネットワークと同じく、接続された全てのサーバからディスクアレイ装置内のディスクを参照あるいは更新することができる。従って、他のサーバからブートディスクを改ざんされたり、内容を参照される可能性がある。
【０００４】
この課題に対し、ディスクアレイ装置は、ファイバチャネルの装置が有するユニークな装置識別子であるＷＷＮ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｎａｍｅ）を用いて、ある特定のサーバが有するＷＷＮとディスクアレイ装置内のディスクとの対応付けを行う機能を有している。例えば、ＷＷＮ１を有するサーバ１からディスクアレイ装置に対するアクセスはディスク１しか見せないといったアクセス範囲を限定する機能である。この機能を用いる事で、サーバ間のディスクに対するセキュリティを維持することができるようになっている。しかし、ＷＷＮはサーバ内のファイバチャネルアダプタ内に記録された識別子であることから、オペレーティングシステムが起動し、ＷＷＮを取得するプログラム（エージェント）を動作させなければＷＷＮを取得することができない。従って、オペレーティングシステムのインストール時にはＷＷＮが未解決であるため、オペレーティングシステムをインストールし、その後エージェントが起動してＷＷＮを取得するまではディスクアレイ装置のセキュリティ機能を使用することができない。そのため、セキュリティが低くなる期間が存在してしまう。
【０００５】
【特許文献１】特開2004-118250

【発明の開示】
【発明が解決しようとする課題】
【０００６】
本発明で解決しようとする課題は、ディスクアレイ装置などの外部ディスク装置にオペレーティングシステムをインストールする場合に、事前にディスクアレイのセキュリティ機能を適用し、外部ディスク装置を用いたブート形態においても高いセキュリティを保ち、かつサーバの運用管理の手間を少なくすることである。
【０００７】
上記課題を解決する方法の一つとして、オペレーティングシステムをインストールする前にサーバが有するＷＷＮを調査しておき、ディスクアレイ装置のセキュリティ機能を設定する方法が考えられる。しかし、この方法では、人手で作業するため間違いが生じてしまう可能性があることや、多数のサーバに対して設定しなければならない場合に多くの時間を有してしまう。一方、ＷＷＮをエージェントを使用することなく取得する技術が特許文献１に記載される。これは、ディスクアレイ装置が保持するアクセスされた機器のＷＷＮを取得することでファイバチャネルの接続関係を知る方法でいる。しかし、この方法は、サーバとＷＷＮとの関係が不明であり、サーバに対するオペレーティングシステムのインストール時には適用することができない。
【課題を解決するための手段】
【０００８】
複数のサーバが外部ディスク装置に接続され、サーバは外部ディスク装置からオペレーティングシステムをブートする形態におけるブートディスクの管理方法であって、
サーバが接続されたネットワークスイッチのポートを検索し、サーバと管理サーバだけが属する仮想ネットワークを構築し、ネットワークブートにより管理サーバからサーバに対しサーバ情報取得プログラムを送信し、サーバ情報取得プログラムはサーバのストレージインターフェースが有する固有情報を取得し管理サーバに転送し、管理サーバは固有情報をもとにサーバからアクセス可能な外部ディスク装置内のディスクを設定することを特徴とする。
【発明の効果】
【０００９】
本発明のブートディスク管理方法は、オペレーティングシステムのインストール前に外部ディスク装置のセキュリティを設定することができ、またセキュリティの設定に必要な情報を自動的に取得することができるという利点がある。
【実施例１】
【００１０】
図１は、本発明における実施例の全体図を示している。
複数のサーバ１０７は、それぞれのネットワークインターフェースカード（ＮＩＣ）１１２を介してネットワークスイッチ（ＮＷ　ＳＷ）１０８に接続され、ファイバチャネルアダプタ（ＦＣＡ）１１１を介してファイバチャネルスイッチ１０６に接続されている。また、ファイバチャネルスイッチ１０６はディスクアレイ装置１０９にも接続され、サーバ１０７からアクセスできる。ネットワークスイッチ１０８は、システムを管理する管理サーバ１０１にも接続されている。また、サーバ１０７の各々にはＢＭＣ（Baseboard Management Controller）１１３が内蔵されており、ネットワークを介して、サーバ１０７のハードウェアの状態監視や、電源制御、サーバ１０７のリセットを行うことができる。一般に、ＢＭＣ１１３は、サーバ１０７とは別の電源が供給されており、サーバ１０７が停止していても、ネットワークを介してＢＭＣ１１３を遠隔操作することができる。管理サーバ１０１は、サーバ１０７，ネットワークスイッチ１０８，ファイバチャネルスイッチ１０６，ディスクアレイ装置１０９に対し、ネットワークを経由して状態の監視や必要に応じて制御を行う。
【００１１】
管理サーバ１０１は、サーバ管理機構１０２とブートディスク管理機構１０３から構成

されている。サーバ管理機構１０２は、サーバや、サーバに接続されているデバイスを管理する。ブートディスク管理機構１０３は、サーバの起動に必要なディスクの管理を行う機構であり、本発明の特徴の一つである。ブートディスク管理機構１０３は、セキュリティ設定機構１０４とサーバ情報取得機構１０５から構成されている。セキュリティ機構１０４は、ディスクアレイ装置１０９内のディスクアレイ管理機構１１５を制御する機構であり、より具体的にはセキュリティ機能１１６を制御する事でサーバとディスクアレイ内のディスク１１０との関係づけを行う。サーバ情報取得機構は、サーバの情報を取得するための機構であり、ネットワークスイッチ１０８内のネットワークスイッチ管理機能１１４等を制御し、サーバ１０７の情報を取得する機能を有する。

【００１２】

本実施例では、サーバ１０７はディスクアレイ装置１０９内にオペレーティングシステムが格納されるケースにおいて、オペレーティングシステムをインストールする前に、サーバ１０７とディスクアレイ装置１０９内のディスク１１０との対応付けを行う。

図２は、本実施例におけるサーバ１０７の詳細な構成を示している。サーバ１０７にはプログラムやデータを格納するメモリ２０１と、メモリ内のプログラムを実行するプロセッサ２０２と、ファイバチャネルアダプタ１１１と、ネットワークインターフェースカード１１２と、ＢＭＣ１１３から構成されている。ファイバチャネルアダプタ１１１は通信機構２０３によりファイバチャネル通信を行うが、ファイバチャネル通信にはＷＷＮ（Ｗｏｒｌｄ　Ｗｉｄｅ　Ｎａｍｅ）と呼ばれるユニークなデバイス識別子が必要とされる。ＷＷＮによってファイバチャネルの通信相手を特定することができる。ファイバチャネルアダプタ１１１内には、このＷＷＮを格納しておくＷＷＮ格納メモリ２０４が用意されており、通信機構２０３はＷＷＮ格納メモリ２０４を参照しながら通信を行う。

【００１３】

ネットワークインターフェースカード１１２は、ネットワーク通信をおこなう通信機構２０５とネットワークブート機構２０６から構成される。ネットワークブート機構２０６は、サーバ１０７の起動時に動作させることができ、ネットワークを介してサーバ１０７の起動に必要なプログラムを取得する機能を有している。ＢＭＣ１１３は、主にサーバ１０７のハードウェアの監視や制御を行う。サーバのハードウェアの情報転送や制御コマンドの受付・転送は通信機構２０７を介して行う。通信機構２０７は、一般的なネットワークと同じで構わない。サーバ１０７のハードウェアに異常が発生した場合はサーバ監視機構２０８が検知し、通信機構２０７から異常を通知する。また、遠隔から通信機構２０７を介して、サーバ１０７の電源をＯＮ／ＯＦＦやハードウェアリセットを行うことができる。そのため、ＢＭＣは一般には、サーバ１０７の電源とは別系統の電源が供給されており、サーバの電源がＯＦＦの状態でもＢＭＣ１１３は通信機構２０７を介して遠隔制御を行う事ができる。

【００１４】

図３は、図１における管理サーバ１０１の構成を示している。管理サーバ１０１は、サーバ管理機構１０２と、ブートディスク管理機構１０３から構成されている。サーバ管理機構１０２は、サーバの状態監視や制御を行う。例えば、現在稼働しているサーバが正常に稼働しているかといったイベントや、あるいは新たに追加されたサーバのイベントを監視などである。この際、重要になる情報は管理対象となるサーバの把握である。そのために、サーバ管理テーブル３０１を有している。サーバ管理テーブル３０１は、現在監視や制御の対象となっているサーバの構成情報や設定情報が格納されている。サーバ管理テーブル３０１の詳細は後で述べる。ブートディスク管理機構１０３は、サーバ情報取得機構１０５とセキュリティ設定機構１０４から構成される。サーバ情報取得機構１０５は仮想ネットワーク設定機構３０６，ネットワークブート管理機構３０２から構成される。仮想ネットワーク設定機構は、図１におけるネットワークスイッチ１０８の仮想ネットワーク（ＶＬＡＮ）を設定する機能を有している。

【００１５】

仮想ネットワークとは、物理的に同一のネットワークスイッチに接続された機器を、論

理的に複数のネットワークに分離する機能である。本実施例における仮想ネットワーク設定機構３０６は、制御対象となるサーバと、管理サーバとの間でプライベートなネットワークを構築する動作を行う。ネットワークブート管理機構３０２は、図２におけるネットワークブート機構２０６に対応する処理を行う。ネットワークブート機構２０６は、ネットワークブート機構２０６からの要求に対応して、ネットワークブートイメージデータ３０３の転送や、ネットワークブートに必要な情報を転送する。本実施例におけるネットワークブートイメージには、オペレーティングシステム（ＯＳ）３０５とＯＳ上で稼働するサーバ情報取得エージェント３０４が格納されている。サーバ情報取得エージェント３０４は、ＯＳ３０５が起動すると自動的に動作するように設定されている。セキュリティ設定機構１０４は、ディスクアレイ装置１０９のセキュリティ機能１１６を制御し、サーバとディスクとの対応付けを行う。

【００１６】

図４は、図３におけるサーバ管理テーブル３０１の詳細を示している。サーバ管理テーブル３０１は、管理サーバ１０１に管理されるテーブルであり、管理サーバ１０１が管理対象としているサーバの一覧と、各サーバの管理情報が格納されている。テーブルのカラム４０１は、サーバの識別子が格納されている。サーバ識別子４０１は、サーバが特定できる情報であれば良い。サーバのシリアル番号や、ブレードサーバであれば、ブレード番号などである。カラム４０２は、ネットワーク接続ポート番号を示している。これは、サーバ１０７とネットワークスイッチ１０８の接続対応を示している。この情報は、独立したサーバであれば、システム管理者が設定しても良いし、ブレードサーバのように接続状態があらかじめ決まっている場合は、あらかじめ固定情報として設定される場合もある。

【００１７】

本実施例では、どちらの方法を使っても構わない。カラム４０３はサーバのプロセッサ種別を示している。カラム４０４はサーバが搭載しているメモリ容量を示している。カラム４０５はブートディスクの場所を示している。サーバに内蔵されたディスクからＯＳを起動する場合は内蔵ディスクと記述され、外部のディスクアレイ装置から起動する場合は、そのディスク番号が記述される。ディスクアレイ装置が複数存在する場合は装置番号を含んでも構わない。カラム４０６は仮想ネットワークの識別子が格納される。仮想ネットワークの識別子が同じサーバは、同じネットワークに属していることを意味し、異なる場合は論理的に通信が切り離されていることを意味する。

【００１８】

図５は、本実施例のディスクアレイ装置１０６におけるセキュリティ機能１１６の詳細を示している。セキュリティ機能は、サーバとディスクとの対応付けを行う機能を有する。ディスクアレイ装置のように、大規模なディスクを有するケースでは、多数のサーバが同一のディスクアレイ装置に接続される。こういったケースにおいて、ディスクに格納されたデータのセキュリティを保護する意味で、サーバが参照・更新できるディスクを制限する機能である。具体的には、セキュリティ機構１０４はディスクマッピング機構５０１とディスクマッピング機構５０１とディスクマッピングテーブル（５０２，５０３，５０４）から構成される。ディスクマッピング機構は、サーバからのアクセス時に、ディスクマッピングテーブル（５０２，５０３，５０４）に従って、サーバがアクセスできるディスクを制限する。カラム５０２は、サーバの識別子であり、前述のＷＷＮが使用される。

【００１９】

カラム５０３は仮想ディスク番号であり、カラム５０４は物理ディスク番号が格納されている。ディスクマッピング機構は、例えばＷＷＮ１を有するファイバチャネルアダプタからのアクセスであれば、仮想ディスク番号（ＬＵ０，ＬＵ１，ＬＵ３）へのアクセスを許す制御を行う。仮想ディスク番号（ＬＵ０，ＬＵ１，ＬＵ３）は、実際には物理ディスク（ＬＵ１０，ＬＵ１１，ＬＵ１７）に対応している。このように、セキュリティ機能は、ある特定のサーバに対して特定のディスクを仮想化してアクセスする機能を有している。ディスクマッピングテーブル５０２に格納されていないＷＷＮからのアクセスに対しては、ディスクへのアクセスはできない制御を行う。

【００２０】
図６は、図５におけるセキュリティ機能１１６の動作を図示している。サーバ１（６０１）はファイバチャネルアダプタ６０５を有し、ファイバチャネルアダプタ６０５はＷＷＮ１（６０５）が記録されている。サーバ２（６０２）はファイバチャネルアダプタ６０４を有し、ファイバチャネルアダプタ６０４はＷＷＮ２（６０６）が記録されている。サーバ１（６０１）とサーバ２（６０２）はファイバチャネルスイッチ６０７に接続され、ファイバチャネルスイッチ６０７からはディスクアレイ装置６０８に接続されている。セキュリティ機能６０９によりサーバ１（６０１）には、物理ディスクＬＵ１０（６１７），ＬＵ１１（６１８），ＬＵ１７（６１９）に対応した仮想ディスクＬＵ０（６１２），ＬＵ１（６１３），ＬＵ２（６１４）へアクセスすることができる。一方、サーバ２（６０２）には、物理ディスクＬＵ２１（６２０），ＬＵ２２（６２１）に対応した仮想ディスクＬＵ０（６１５），ＬＵ１（６１６）へアクセスすることができる。サーバ１（６０１）から、物理ディスクＬＵ２１（６２０）やＬＵ２２（６２１）にアクセスすることはできない。

【００２１】
図７は、本発明における実施例の動作シーケンスを示している。図示するシーケンスは、サーバ７０１，ブートディスク管理機構７０２，ディスクアレイセキュリティ機能７０３である。７０４は、新規サーバの導入イベント示している。例えば、ブレードサーバ等では、新たにサーバが導入されると自動的に発行される。また、単体サーバの場合は、サーバをネットワークスイッチに接続した後、システム管理者が手動でイベントを発行しても構わない。また、新規サーバ導入ではなく、既に導入されている未設定サーバを使用するといったケースにおけるイベントでも構わない。ここでのイベントは、未だＯＳをインストールするディスクが決定していないサーバを新たに使用する際に発生するイベントである。このイベントにより、ブートディスク管理機構７０２のサーバ管理機構７０５が動作する。サーバ管理機構７０５は、イベントを解析した後、サーバの新規導入であることを解析し、仮想ネットワーク設定機構７０６を呼び出す。仮想ネットワーク設定機構７０６は、新規に導入されたサーバと管理サーバ間でプライベートなネットワークを構築する。

【００２２】
その後、リセット７０７指示をサーバに対して転送する。リセット指示によりサーバがリセットされると、サーバは前述のネットワークブート機構７０８が動作する。これにより、イメージデータがブートディスク管理機構７０２から転送される７０９。サーバ７０１は、転送されたイメージデータを使用してＯＳのブートが開始される７１０。ＯＳの起動に連動して、自動的にサーバ情報取得エージェント７１１が起動し、サーバのさまざまな情報を取得した後、取得した情報をブートディスク管理機構７０２に対して転送する（７１２）。この情報の中には、サーバが有しているファイバチャネルアダプタのＷＷＮが含まれる。サーバ情報の転送を確認すると、ブートディスク管理機構７０２は、仮想ネットワーク設定機構により７０６で設定された仮想ネットワークを解除し、ブートディスク管理機構７０２が起動する前のネットワーク状態に戻す。その後、セキュリティ機構１０４は、取得したサーバ情報内に含まれるＷＷＮを使用して、ディスクアレイ装置のセキュリティ機能７０３に対して、サーバとディスクとの対応付けを指示する。上記一連の処理により、新規に導入されたサーバに対し、ＯＳをインストールするためのディスクを自動的に準備することができる。これにより、ＯＳインストール７１６を開始することができる。

【００２３】
以下では、図７におけるシーケンスをより詳細に説明する。図８は、サーバ管理機構１０２の動作フローを示している。ステップ８０１はサーバイベント検知を行う。ステップ８０２では、イベントを解析し、ブートディスクの割当てが必要なイベントかどうかを判定する。ブートディスクの割当てが必要なイベントの場合は、ステップ８０３でイベント発生サーバのネットワークの接続ポートを検索する。これは、図４のサーバ管理テーブル

を検索することで実現できる。ステップ８０４は、ブートディスク管理機構を呼び出す。この際、ステップ８０３で取得した接続ポート番号をパラメタとして転送する。ステップ８０２において、ブートディスクの割当てが必要でないイベントの場合は、そのイベントに対応した処理を行いフローを終了する。

【００２４】

図９は、ブートディスク管理機構１０３の処理フローを示している。ステップ９０１は、仮想ネットワーク設定機構の呼出を行う。仮想ネットワーク設定機構には、新規に仮想ネットワークを設定する機能と、既に設定している仮想ネットワークを解除する機能を有するが、ステップ９０１では仮想ネットワークの設定を行う。ステップ９０１の処理により、イベントを発生したサーバと、管理サーバ１０１との間で１対１のプライベートな仮想ネットワークが構築される。ステップ９０２では、イベントを発生したサーバに対し、リセット指示を行う。リセットは、ＢＭＣ１１３に対して発行され、この指示を受けたサーバのＢＭＣは該当サーバをリセットする。サーバはリセットによりブートディスクの検索を開始するが、本実施例では未だＯＳディスクは決定していないため、ネットワークブート機構２０６が優先して動作する。ネットワークブート機構２０６の動作に連動して、ネットワークブート管理機構３０２が動作する。この動作については、後で詳細に説明する。ネットワークブート管理機構３０２は、イベントを発生したサーバが有するＷＷＮを取得する。ステップ９０４では、ステップ９０１で設定したプライベートなネットワークを元の状態に戻す処理を行う。ステップ９０５では、ステップ９０３により取得したＷＷＮをパラメタとして、セキュリティ設定機構１０４を呼び出す。

【００２５】

図１０では、仮想ネットワーク設定機構３０６の動作フローを示している。ステップ１００１では、要求された指示が仮想ネットワークの設定なのか解除なのかを判断する。仮想ネットワークの設定の場合はステップ１００２に移り、解除の場合はステップ１００２に移る。ステップ１００２では、イベント発生サーバの現状の接続ポート番号を保存する。ステップ１００３は、管理サーバの接続ポート番号を検索する。ステップ１００４は、イベント発生サーバの現状の仮想ネットワーク（ＶＬＡＮ）番号を保存する。これは、仮想ネットワークを解除する場合に使用される。現状のＶＬＡＮ番号は図４におけるサーバ管理テーブルを参照することで実現できる。

【００２６】

ステップ１００５は、現状の管理サーバのＶＬＡＮ番号を保存する。ステップ１００６では、イベント発生サーバと管理サーバとを他とは独立したＶＬＡＮを設定する。この際使用される情報は、サーバと管理サーバの接続ポート番号である。ネットワークスイッチ１０８の管理機能１１４に対して、指定したポート番号に接続された機器を指定されたＶＬＡＮに属するように指示する。独立したＶＬＡＮ番号は、例えば、図４におけるサーバ管理テーブルの仮想ネットワークカラム４０６をサーチし、設定されていないＶＬＡＮ番号を検索するといった処理により実現することができる。あるいは、あらかじめ所定のＶＬＡＮ番号を決定し、そのＶＬＡＮ番号は他では使用しないことでも実現できる。

【００２７】

仮想ネットワークを解除するケースでは、ステップ１００７においてイベント発生サーバの接続番号を取り出す。ステップ１００８では管理サーバの接続ポート番号を取り出す。ステップ１００９ではステップ１００４で保存されたＶＬＡＮ番号を取り出す。ステップ１０１０では、ステップ１００５で保存されたＶＬＡＮ番号を取り出す。上記ステップで取り出した情報を基に、ステップ１０１１ではイベント発生サーバと管理サーバのＶＬＡＮ番号を元の状態に戻す。仮想ネットワークを設定することで、管理サーバ１０１以外のサーバがネットワークブート機構２０６に反応する誤動作を防ぐ事ができ、また他サーバのネットワークへの影響を無くすことができる。

【００２８】

図１１は、図１０における仮想ネットワーク設定機構３０６によって設定された仮想ネットワークの設定例を示している。サーバ（１１０１、１１０２、１１０３）はそれぞれ

、ネットワークスイッチ１１０５に接続されている。ここで、サーバ１１０４が新たに導入された場合に、管理サーバ１１０７と導入されたサーバ１１０４とを独立した仮想ネットワーク１１０６が自動的に構成される。本実施例では、仮想ネットワークの設定にＶＬＡＮを用いたが、目的は他サーバとのネットワークの影響をなくすことであり、ＶＬＡＮを使用する以外にもネットワークスイッチ１０８の制御ハードウェアを直接制御し、ハードウェアレベルで仮想ネットワークを構築しても構わない。これによりサーバ１１０４と管理サーバ間で完全に独立したネットワークを構築できるため、サーバ１１０４から発行されるネットワークを経由したリクエストが、他のサーバに影響を与えることなく処理を行うことができるようになる。

【００２９】

図１２はネットワークブート機構２０６の処理フローを示している。ステップ１２０１は、接続されているネットワークに対してブロードキャストパケットを発行する。これは、ＩＰアドレスを取得するためである。サーバの電源がＯＮされた直後は、まだＩＰアドレス（ネットワークアドレス）を持っておらず、他の機器とＩＰを使ったネットワーク通信を行う事ができない。本実施例においては、仮想ネットワークを構築しているため、ブロードキャストを発行しても管理サーバにしかパケットは届かない。これにより、他のサーバに影響を与えることなく新規導入サーバを管理することができるようになる。ＩＰアドレスを管理しているサーバは、ブロードキャストに応答してＩＰアドレスを与える。ステップ１２０２は、ＩＰアドレスの受け取りを行い、ネットワークインターフェースカードにＩＰアドレスを設定する。ステップ１２０３は、ブートに必要なデータを保持しているサーバを受け取る。ステップ１２０４は、ステップ１２０３で取得したサーバからイメージデータを取得する。ステップ１２０５は、取得したイメージデータを起動する。この一連の処理により、ネットワークを介してシステムを起動することができる。

【００３０】

図１３は、図１２のネットワークブート機構に対応するサーバ側となるネットワークブート管理機構の処理フローを示している。ステップ１３０１は、ブロードキャストに対応してＩＰアドレスを付与する。ステップ１３０２は、イメージデータを保持するサーバを送信するが、本実施例では管理サーバ１０１がイメージデータの保持サーバとなる。ステップ１３０３は、ネットワークブートイメージを送信する。上記処理により、ネットワークを介したブートが可能となる。

【００３１】

図１４は、サーバ情報取得エージェント３０４の処理フローを示している。この処理は、図１２および図１３において示したネットワークブートにより自動的に起動される。ステップ１４０１はプロセッサ種別を取得する。ステップ１４０２はメモリ容量を取得する。ステップ１４０３はファイバチャネルアダプタのＷＷＮを取得する。ステップ１４０４は取得した情報を管理サーバ１０１に転送する。一連の処理は、ネットワークブートによりＯＳ３０５が起動した後、自動的にサーバ情報取得エージェント３０４が起動し処理されるように設定しておく。

【００３２】

図１５はセキュリティ設定機構の処理フローを示している。ステップ１５０１は、イベントを発生したサーバのＷＷＮを取得する。図１４においてステップ１４０３にて取得したＷＷＮを受け取ることで実現できる。ステップ１５０２は、ステップ１５０１、サーバに対して新たに割り当てるブートディスクを生成する。このステップは、ディスクアレイに新規ディスクの生成を要求しても構わないし、別な手段としては、あらかじめ複数のブートディスクをプールしておき、必要に応じてプールから取り出す方法などが考えられる。ステップ１５０３はステップ１５０１で取得したＷＷＮをパラメタとして、イベント発生サーバとステップ１５０２で割り当てたブートディスクとを対応づけの要求を行う。要求は、セキュリティ機能１１６が処理する。上記処理により、サーバに新なディスクが対応付けされ、ＯＳをインストールするディスクを用意することができる。また、本実施例では、ブートディスクの割り当てに本発明を用いたが、必ずしもブートディスクの割り当

てだけでなく、例えばデータディスクの割り当ても同じ手順で行うことができる。

【実施例２】

【００３３】

図１６は、本発明における実施例２の管理サーバの構成を示している。実施例２では、ファイバチャネルアダプタ１１１に格納されているＷＷＮ２０４を書き換えることができる場合の実施例を示す。実施例１と異なるのは、サーバ管理テーブル１６０１、ブートディスク管理機構１６０２、セキュリティ設定機構１６０５である。ブートディスク管理機構１６０２はネットワークブートイメージデータの構造が大きく異なる。１６０２は、ＯＳ３０５上で稼働するエージェントプログラムであるが、実施例１とは異なり、情報を書き込む機能を有する。

【００３４】

図１７は、サーバ管理テーブル１６０１を示している。実施例１のサーバ管理テーブル３０１に、カラム１７０１が追加される。カラム１７０１は、各サーバに割り当てるＷＷＮが格納されている。サーバが新たに追加された場合に、ファイバチャネルアダプタ１１１のＷＷＮに書き込むＷＷＮデータが格納されている。

【００３５】

図１８は、サーバ情報取得・設定エージェント１６０２の処理フローを示している。この処理は、図１２および図１３において示したネットワークブートにより自動的に起動される。ステップ１８０１はプロセッサ種別を取得する。ステップ１８０２はメモリ容量を取得する。ステップ１８０３はファイバチャネルアダプタに対しＷＷＮを設定する。ここで設定されるＷＷＮデータは、サーバ管理テーブル１６０１のサーバに対応するＷＷＮである。ステップ１８０４は取得した情報を管理サーバ１０１に転送する。一連の処理は、ネットワークブートによりＯＳ３０５が起動した後、自動的にサーバ情報取得エージェント１６０２が起動し処理されるように設定しておく。

【００３６】

図１９は、セキュリティ設定機構１６０５の処理フローを示している。ステップ１９０１は、イベントを発生したサーバの識別子を取得する。ステップ１９０２は、ステップ１９０１で取得したサーバに対応するＷＷＮ情報を取得する。ステップ１９０３は、ブートディスクの割当てを行う。このステップは、ディスクアレイに新規ディスクの生成を要求しても構わないし、別な手段としては、あらかじめ複数のブートディスクをプールしておき、必要に応じてプールから取り出す方法などが考えられる。ステップ１９０４はステップ１９０２で取得したＷＷＮをパラメタとして、イベント発生サーバとステップ１９０３で割り当てたブートディスクとを対応づけの要求を行う。要求は、セキュリティ機能１１６が処理する。上記処理により、ＷＷＮを変更可能なファイバチャネルアダプタの場合において、サーバに新なディスクが対応付けされ、ＯＳをインストールするディスクを用意することができる。

【００３７】

図２０は、実施例２におけるシーケンスを示している。図示するシーケンスは、サーバ２００１，ブートディスク管理機構２００２，ディスクアレイセキュリティ機能２００３である。２００４は、新規サーバの導入イベント示している。例えば、ブレードサーバ等では、新たにサーバが導入されると自動的に発行される。また、単体サーバの場合は、サーバをネットワークスイッチに接続した後、システム管理者が手動でイベントを発行しても構わない。また、新規サーバ導入ではなく、既に導入されている未設定サーバを使用するといったケースにおけるイベントでも構わない。ここでのイベントは、未だＯＳをインストールするディスクが決定していないサーバを新たに使用する際に発生するイベントである。このイベントにより、ブートディスク管理機構２００５のサーバ管理機構２００５が動作する。サーバ管理機構２００５は、イベントを解析した後、サーバの新規導入であることを解析し、仮想ネットワーク設定機構２００６を呼び出す。仮想ネットワーク設定機構２００６は、新規に導入されたサーバと管理サーバ間でプライベートなネットワークを構築する。その後、リセット２００７指示をサーバに対して転送する。リセット指示に

よりサーバがリセットされると、サーバは前述のネットワークブート機構２００８が動作する。これにより、イメージデータがブートディスク管理機構２００２から転送される（２００９）。

【００３８】

サーバ２００１は、転送されたイメージデータを使用してＯＳのブートが開始される２０１０。ＯＳの起動に連動して、自動的にサーバ情報取得。設定エージェント２０１１が起動し、サーバのさまざまな情報を取得およびＷＷＮの設定（２０１２）をした後、取得した情報をブートディスク管理機構２００２に対して転送する。サーバ情報の転送を確認すると、ブートディスク管理機構２００２は、仮想ネットワーク設定機構により２０１３で設定された仮想ネットワークを解除し、ブートディスク管理機構２００２が起動する前のネットワーク状態に戻す。その後、セキュリティ機構２０１４は、サーバに設定したＷＷＮを使用して、ディスクアレイ装置のセキュリティ機能２００３に対して、サーバとディスクとの対応付けを指示する。上記一連の処理により、新規に導入されたサーバに対し、ＯＳをインストールするためのディスクを自動的に準備することができる。

【実施例３】

【００３９】

実施例３では、セキュリティ制御をファイバチャネルスイッチで行うことに特徴がある。まず、図２１を参照して構成を説明する。

ファイバチャネルスイッチ１０６は、接続されたポートやＷＷＮ毎にゾーニングと呼ばれる接続制限を設ける機能を有している。例えば、ファイバチャネルスイッチ１０６のポート１に接続された機器とポート１０に接続された機器とを対応付け、他の機器からは見せなくする機能である。この機能を本発明におけるディスク割当に使用することができる。

【００４０】

複数のサーバ１０７は、ネットワークインターフェースカード（ＮＩＣ）１１２を介してネットワークスイッチ（ＮＷ　ＳＷ）１０８に接続され、ファイバチャネルアダプタ（ＦＣＡ）１１１を介してファイバチャネルスイッチ１０６に接続されている。また、ファイバチャネルスイッチ１０６はディスク装置２１０７にも接続され、サーバ１０７からアクセスできる。ネットワークスイッチ１０８は、システムを管理する管理サーバ２１０１にも接続されている。ファイバチャネルスイッチ１０６には、ファイバチャネルスイッチ管理機能２１０６が内蔵され、ネットワークを介して遠隔からファイバチャネルスイッチ１０６を制御することができる。サーバ１０７にはＢＭＣ（Baseboard Management Controller）１１３が内蔵されており、ネットワークを介して、サーバ１０７のハードウェアの状態を監視したり、電源を制御したり、リセットすることができる。

【００４１】

一般に、ＢＭＣ１１３は、サーバ１０７とは別の電源が供給されており、サーバ１０７が停止していても、ネットワークを介してＢＭＣ１１３を遠隔操作することができる。管理サーバ２１０１は、サーバ１０７，ネットワークスイッチ１０８，ファイバチャネルスイッチ１０６，ディスク装置２１０７に対し、ネットワークを経由して状態の監視や必要に応じて制御を行う。管理サーバ２１０１は、サーバ管理機構２１０２とブートディスク管理機構２１０３から構成されている。サーバ管理機構２１０２は、サーバや、サーバに接続されているデバイスを管理する。ブートディスク管理機構２１０３は、サーバの起動に必要なディスクの管理を行う機構であり、本発明の特徴の一つである。ブートディスク管理機構２１０３は、セキュリティ設定機構２１０４とサーバ情報取得機構２１０５から構成されている。セキュリティ機構２１０４は、ファイバチャネルスイッチ１０６内のファイバチャネルスイッチ管理機構２１０６を制御する機構である。サーバ情報取得機構は、サーバの情報を取得するための機構であり、ネットワークスイッチ１０８内のネットワークスイッチ管理機能１１４等を制御し、サーバ１０７の情報を取得する機能を有する。本発明の実施例３では、サーバ１０７はディスク装置２１０７内にオペレーティングシステムが格納されるケースにおいて、オペレーティングシステムをインストールする前に、サーバ１０７とディスク装置２１０７との対応付けを行う。

【００４２】
図２２は、管理サーバ２１０１の構成図を示している。管理サーバ２１０１は、サーバ管理機構２２０１と、ブートディスク管理機構１０３から構成されている。サーバ管理機構２２０１は、サーバの状態監視や制御を行う。例えば、現在稼働しているサーバが正常に稼働しているかといったイベントや、あるいは新たに追加されたサーバのイベントを監視などである。この際、重要になる情報は管理対象となるサーバの把握である。そのために、サーバ管理テーブル３０１とストレージ管理テーブル２２０２を有している。サーバ管理テーブル３０１は、現在監視や制御の対象となっているサーバの構成情報や設定情報が格納されている。ストレージ管理テーブル２２０２は、各サーバに接続されているストレージの接続関係を示すテーブルである。ブートディスク管理機構１０３は、サーバ情報取得機構１０５とセキュリティ設定機構１０４から構成される。
【００４３】
サーバ情報取得機構１０５は仮想ネットワーク設定機構３０６，ネットワークブート管理機構３０２から構成される。仮想ネットワーク設定機構は、図２１におけるネットワークスイッチ１０８の仮想ネットワークを設定する機能を有している。仮想ネットワークとは、物理的に同一のネットワークスイッチに接続された機器を、論理的に複数のネットワークに分離する機能である。本実施例における仮想ネットワーク設定機構３０６は、制御対象となるサーバと、管理サーバとの間でプライベートなネットワークを構築する動作を行う。ネットワークブート管理機構３０２は、図２におけるネットワークブート機構２０６に対応する処理を行う。
【００４４】
ネットワークブート機構２０６は、ネットワークブート機構２０６からの要求に対応して、ネットワークブートイメージデータ３０３の転送や、ネットワークブートに必要な情報を転送する。本実施例におけるネットワークブートイメージには、オペレーティングシステム（ＯＳ）３０５とＯＳ上で稼働するサーバ情報取得エージェント３０４が格納されている。サーバ情報取得エージェント３０４は、ＯＳ３０５が起動すると自動的に動作するように設定されている。セキュリティ設定機構１０４は、ファイバチャネルスイッチ１０６のファイバチャネル管理機能２１０６を制御し、サーバとディスクとの対応付けを行う。
【００４５】
図２３はストレージ管理テーブル２２０２の構成を示している。カラム２３０１は接続装置の識別子であり、サーバの識別子やディスク装置の識別子が格納される。カラム２３０２はファイバチャネルスイッチの接続ポート番号を示している。カラム２３０３は接続装置の種別を示している。このテーブルにより、ファイバチャネルスイッチ１０６の接続構成を把握することができる。
【００４６】
図２４は、セキュリティ設定機構２２０３の処理フローを示している。ステップ２４０１は、イベントが発生したサーバの識別子を取得する。サーバ識別子を取得することで、図２３のストレージ管理テーブルを検索することで、イベントが発生したサーバが接続されているファイバチャネルスイッチ１０６のポート番号を知ることができるようになる。ステップ２４０２では、ブートディスクの割り当てを行う。ステップ２４０３では、ファイバチャネルスイッチ１０６のファイバチャネルスイッチ管理機能２１０６を制御し、ファイバチャネルスイッチ１０６のポートに接続されたサーバあるいはエージェントが取得したＷＷＮを用いて、同じくファイバチャネルスイッチ１０６に接続されたディスク装置２１０７との対応付けを行う。
【００４７】
図２５は、実施例３の動作シーケンスを示している。図示するシーケンスは、サーバ２５０１，ブートディスク管理機構２５０２，ファイバチャネルスイッチ管理機能２５０３である。２５０４は、新規サーバの導入イベント示している。例えば、ブレードサーバ等では、新たにサーバが導入されると自動的に発行される。また、単体サーバの場合は、サ

ーバをネットワークスイッチに接続した後、システム管理者が手動でイベントを発行しても構わない。また、新規サーバ導入ではなく、既に導入されている未設定サーバを使用するといったケースにおけるイベントでも構わない。ここでのイベントは、未だＯＳをインストールするディスクが決定していないサーバを新たに使用する際に発生するイベントである。このイベントにより、ブートディスク管理機構２５０２のサーバ管理機構２５０５が動作する。サーバ管理機構２５０５は、イベントを解析した後、サーバの新規導入であることを解析し、仮想ネットワーク設定機構２５０６を呼び出す。仮想ネットワーク設定機構２５０６は、新規に導入されたサーバと管理サーバ間でプライベートなネットワークを構築する。その後、リセット２５０７指示をサーバに対して転送する。リセット指示によりサーバがリセットされると、サーバは前述のネットワークブート機構２５０８が動作する。

【００４８】

これにより、イメージデータがブートディスク管理機構２５０２から転送される（２５０９）。サーバ２５０１は、転送されたイメージデータを使用してＯＳのブートが開始される２５１０。ＯＳの起動に連動して、自動的にサーバ情報取得エージェント２５１１が起動し、サーバのさまざまな情報を取得した後、取得した情報をブートディスク管理機構２５０２に対して転送する（２５１２）。この情報の中には、サーバが有しているファイバチャネルアダプタのＷＷＮが含まれる。サーバ情報の転送を確認すると、ブートディスク管理機構２５０２は、仮想ネットワーク設定機構により２５０６で設定された仮想ネットワークを解除し、ブートディスク管理機構２５０２が起動する前のネットワーク状態に戻す。その後、ファイバチャネルスイッチ管理機構２５０３は、取得したサーバ情報内に含まれるＷＷＮやストレージ管理テーブル２２０２を使用して、ファイバチャネルスイッチ１０６のファイバチャネルスイッチ管理機能２１０６に対して、サーバとディスクとの対応付けを指示する。上記一連の処理により、ファイバチャネルスイッチ１０６を使用して、新規に導入されたサーバに対し、ＯＳをインストールするためのディスクを自動的に準備することができる。

【実施例４】

【００４９】

実施例４では、ディスクアレイ装置に新規に接続されたサーバのディスクを自動的に割り当てる機能を有している点に特徴がある。

図２６は、実施例４の全体図を示している。複数のサーバ１０７は、ネットワークインターフェースカード（ＮＩＣ）１１２を介してネットワークスイッチ（ＮＷ　ＳＷ）１０８に接続され、ファイバチャネルアダプタ（ＦＣＡ）１１１を介してファイバチャネルスイッチ１０６に接続されている。また、ファイバチャネルスイッチ１０６はディスクアレイ装置１０９にも接続され、サーバ１０７からアクセスできる。ネットワークスイッチ１０８は、システムを管理する管理サーバ２６０１にも接続されている。また、サーバ１０７にはＢＭＣ（Baseboard Management Controller）１１３が内蔵されており、ネットワークを介して、サーバ１０７のハードウェアの状態を監視したり、電源を制御したり、リセットすることができる。一般に、ＢＭＣ１１３は、サーバ１０７とは別の電源が供給されており、サーバ１０７が停止していても、ネットワークを介してＢＭＣ１１３を遠隔操作することができる。

【００５０】

管理サーバ１０１は、サーバ１０７，ネットワークスイッチ１０８，ファイバチャネルスイッチ１０６，ディスクアレイ装置１０９に対し、ネットワークを経由して状態の監視や必要に応じて制御を行う。管理サーバ２６０１は、サーバ管理機構２６０２とブートディスク管理機構２６０３から構成されている。サーバ管理機構２６０２は、サーバや、サーバに接続されているデバイスを管理する。ブートディスク管理機構２６０３は、サーバの起動に必要なディスクの管理を行う機構であり、本発明の特徴の一つである。ブートディスク管理機構２６０３は、セキュリティ設定機構２６１０から構成されている。セキュリティ機構２６０６は、ディスクアレイ装置２６０５内のディスクアレイ管理機構２６１

１を制御する機構であり、より具体的にはセキュリティ機能２６０６を制御する事でサーバとディスクアレイ装置内のディスク１１０との関係づけを行う。

【００５１】

また、動的ディスク割当機能２６０７は、本発明の特徴の一つである。動的ディスク割当機能２６０７は、サーバ１０７からのディスクアクセス時に、新たなＷＷＮを有するサーバからのアクセスの場合、動的にディスク１１０を割り当てる機能を有する。本発明の実施例４では、サーバ１０７はディスクアレイ装置１０９内にオペレーティングシステムが格納されるケースにおいて、オペレーティングシステムをインストールする前に、サーバ１０７とディスクアレイ装置１０９内のディスク１１０との対応付けを動的に行う。

【００５２】

図２７は、図２６における管理サーバ２６０１の構成を示している。管理サーバ２６０１は、サーバ管理機構２６０２と、ブートディスク管理機構２６０３から構成されている。サーバ管理機構２６０２は、サーバの状態監視や制御を行う。例えば、現在稼働しているサーバが正常に稼働しているかといったイベントや、あるいは新たに追加されたサーバのイベントを監視などである。この際、重要になる情報は管理対象となるサーバの把握である。そのために、サーバ管理テーブル３０１を有している。サーバ管理テーブル３０１は、現在監視や制御の対象となっているサーバの構成情報や設定情報が格納されている。ブートディスク管理機構２６０３は、セキュリティ設定機構２６１０から構成される。セキュリティ設定機構２６１０は、ディスクアレイ装置２６０５のセキュリティ機能２６０７を制御し、サーバとディスクとの対応付けを行う。

【００５３】

図２８は、ブートディスク管理機構２６０３の処理フローを示している。ステップ２８０１は、イベント発生サーバのサーバ番号を取得する。ステップ２８０２は、ディスク割当確認を行う。これは、ディスクアレイ装置２６０５の動的ディスク割当機能２６０７がサーバに対して割り当てたディスクが、正しい対応かどうかを判断する処理である。これは、不当なサーバに対してディスクを割り当てていないか確認する処理である。ステップ２８０３は、サーバから転送されたＷＷＮとディスクアレイ装置２６０５が対応づけたディスクと一致しているかどうか検査する。もし、ＷＷＮが一致しない場合は、ステップ２８０４にて割当を即座に解除する。この処理により、動的ディスク割当機能２６０７を介して、不当なサーバにディスクを割り当てる事を防ぐことができる。

【００５４】

図２９は、動的ディスク割当機能２６０７の処理フローを示している。ステップ２９０１は、アクセスしたサーバが有するＷＷＮがセキュリティ機能２６０６に登録されたＷＷＮかどうかを判断する。もし、登録されていないＷＷＮを有するサーバからのアクセスであればステップ２９０２に移行し規程内のＷＷＮかどうかを判断する。あるメーカが発行するＷＷＮには一定の決まりがあるため、これを利用して特定のメーカの機器からのアクセスであれば動的ディスク割当を許す判断を行う。規程内のＷＷＮであればステップ２９０３により新規ディスクを割り当てる。ステップ２９０４にて、当該ＷＷＮと新規に割り当てたディスクとの対応付けを行う。上記処理により、不当なサーバからのアクセス時に、ディスク割当を行う事を防ぐことができる。

【００５５】

図３０は、実施例４の動作シーケンスを示している。図示するシーケンスは、サーバ３００１，ブートディスク管理機構３００２，ディスクアレイのセキュリティ機構３００３である。３００４は、新規サーバのディスクアレイ装置へのアクセスを示している。このアクセスにより、ディスクアレイ装置内のセキュリティ機構３００３は、動的にディスクを割り当てる。これにより、他の実施例にくらべ、少ない処理でディスクを割り当てることができる。しかし、複数のサーバから構成される場合、正しいサーバにディスクを割り当てたかどうか確認する必要がある。そのため、インストールされたＯＳ上で稼働するサーバ情報取得エージェントから受け取ったＷＷＮを用いて、新規サーバに対して正しくディスクを割り当てたかどうかを確認する必要がある（３００８）。これらの処理により、

少ない処理で正しくディスクを対応づけることができるようになる。

【産業上の利用可能性】

【００５６】

本発明によれば、複数のサーバに対して共通の外部ディスク装置備えて、そこから各サーバのオペレーティングシステムをブートする形態の計算機システムにて、ディスクアレイ装置に備えるセキュリティ機能を使用して他サーバからの更新、改ざん等を防止して安全にオペレーティングシステムのブートをすることができ、またそのための設定に必要な情報を自動的に取得することができる。したがって本発明は共通ディスク装置を用いる計算機システムに採用する効果が大きく、この分野で利用可能性が高い。

【図面の簡単な説明】

【００５７】

【図１】本発明の実施例１の全体構成図を示す。
【図２】上記実施例のサーバの構成図を示す。
【図３】上記実施例の管理サーバの構成図を示す。
【図４】上記実施例のサーバ管理テーブルを示す。
【図５】上記実施例のセキュリティ機能の構成図を示す。
【図６】上記実施例のセキュリティ機能の設定例を示す。
【図７】上記実施例の本発明の動作シーケンスを示す。
【図８】上記実施例のサーバ管理機構の処理フローを示す。
【図９】上記実施例のブートディスク管理機構の処理フローを示す。
【図１０】上記実施例の仮想ネットワーク設定機構の処理フローを示す。
【図１１】上記実施例の仮想ネットワークの設定例を示す。
【図１２】上記実施例のネットワークブート機構の処理フローを示す
【図１３】上記実施例のネットワークブート管理機構の処理フローを示す。
【図１４】上記実施例のサーバ情報取得エージェントの処理フローを示す。
【図１５】上記実施例のセキュリティ設定機構の処理フローを示す。
【図１６】本発明の実施例２の管理サーバの構成図を示す。
【図１７】上記実施例のサーバ管理テーブルを示す。
【図１８】サーバ情報取得エージェントの処理フローを示す。
【図１９】上記実施例のセキュリティ設定機構の処理フローを示す。
【図２０】上記実施例の動作シーケンスを示す。
【図２１】本発明の実施例３の全体構成図を示す。
【図２２】上記実施例の管理サーバの構成図を示す。
【図２３】上記実施例のストレージ管理テーブルを示す。
【図２４】上記実施例のセキュリティ設定機構の処理フローを示す。
【図２５】上記実施例の本発明の動作シーケンスを示す。
【図２６】本発明の実施例４の全体構成図を示す。
【図２７】上記実施例の管理サーバの構成図を示す。
【図２８】上記実施例のブートディスク管理機構の処理フローを示す。
【図２９】上記実施例の動的ディスク割当て機構の処理フローを示す。
【図３０】上記実施例の本発明の動作シーケンスを示す。

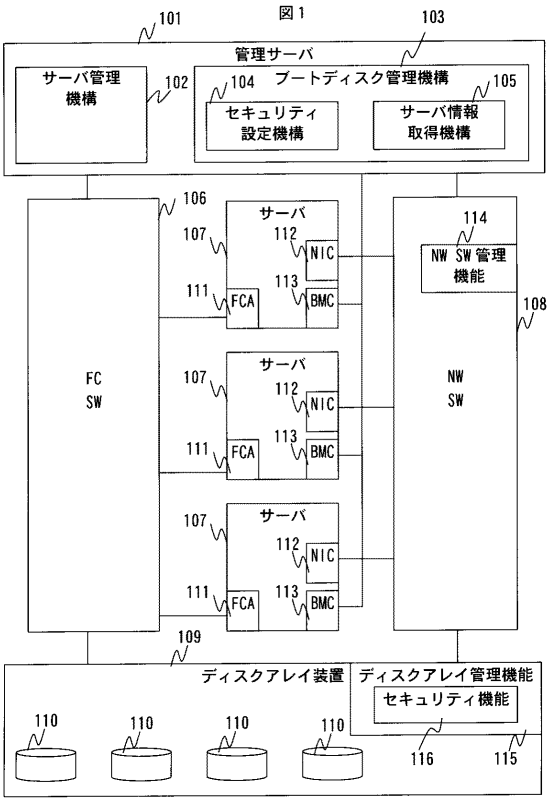
【符号の説明】

【００５８】

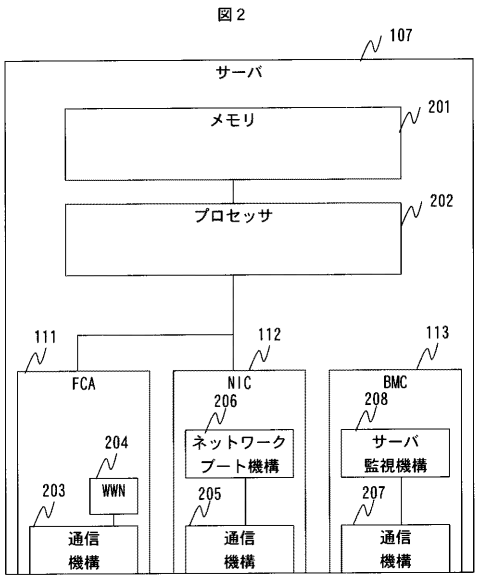
１０１　管理サーバ
１０２　サーバ管理機構
１０３　ブートディスク管理機構
１０４　セキュリティ設定機構
１０５　サーバ情報取得機構
１０６　ファイバチャネルスイッチ
１０７　サーバ

１０８　ネットワークスイッチ
１０９　ディスクアレイ装置
１１０　ディスク
１１１　ファイバチャネルアダプタ
１１２　ネットワークインターフェースカード
１１３　ＢＭＣ
１１５　ディスクアレイ管理機能
１１６　セキュリティ機能。

【図１】

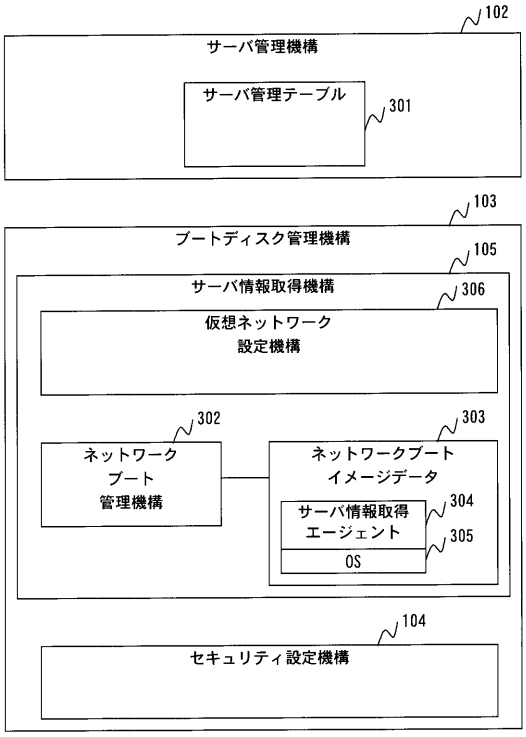


【図２】



【図３】

図３



【図４】

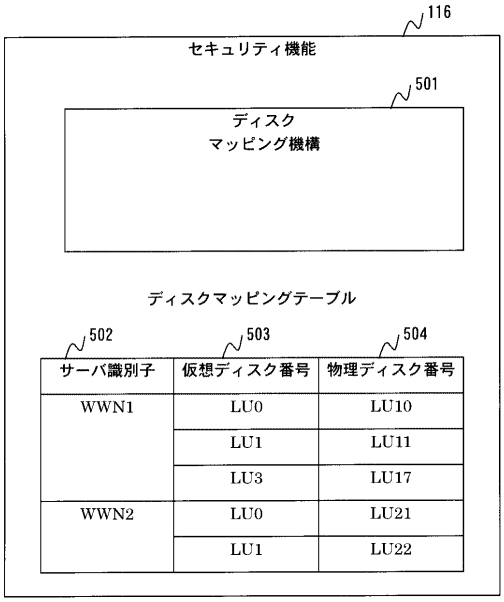
図４

サーバ管理テーブル

401 サーバ識別子	402 ネットワーク接続ポート	403 プロセッサ種別	404 メモリ容量	405 ブートディスク	406 仮想ネットワーク
サーバ１	1	CPU1	1GB	LU1	VLAN1
サーバ２	2	CPU1	1GB	LU0	VLAN1
サーバ３	3	CPU2	2GB	LU0	VLAN2
サーバ４	4	CPU1	2GB	LU2	VLAN3
サーバ５	5	CPU2	1GB	－	－
サーバ６	6	CPU1	4GB	－	－
サーバ７	7	CPU2	1GB	－	－
サーバ８	8	CPU1	4GB	－	－
管理サーバ	10	CPU1	4GB	内蔵ディスク	－

【図５】

図５

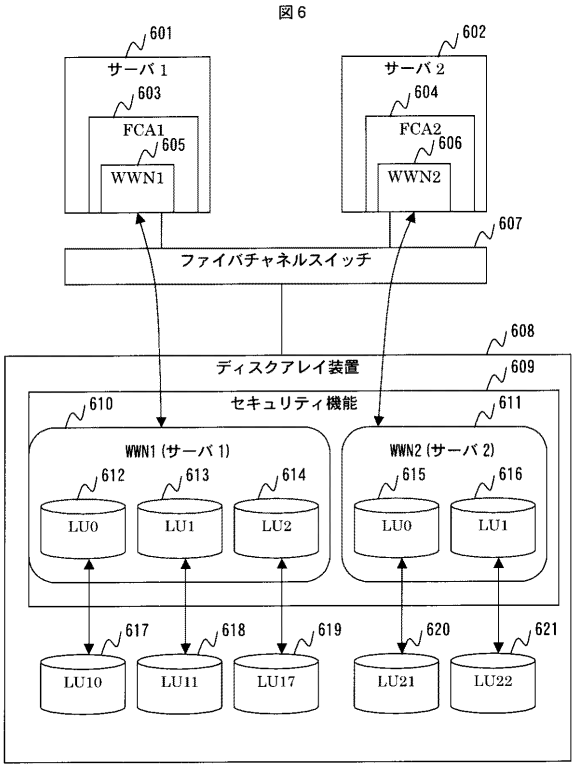


ディスクマッピングテーブル

502 サーバ識別子	503 仮想ディスク番号	504 物理ディスク番号
WWN1	LU0	LU10
	LU1	LU11
	LU3	LU17
WWN2	LU0	LU21
	LU1	LU22

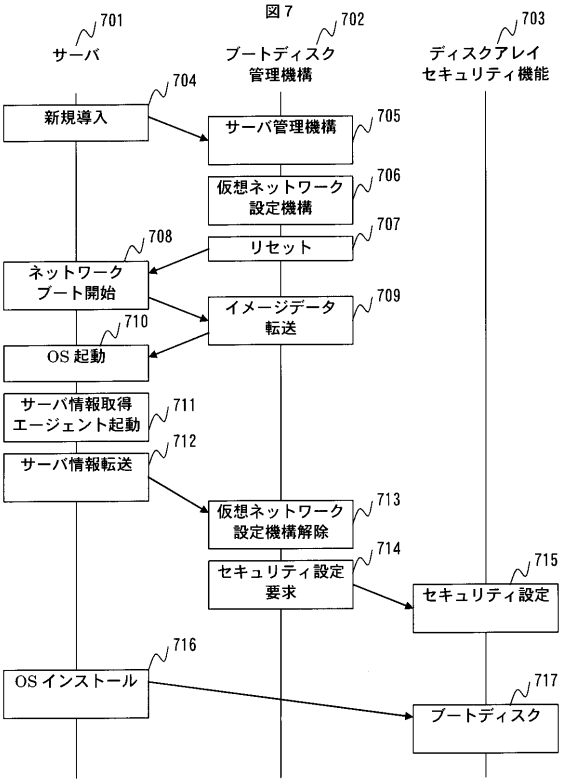
【図６】

図６



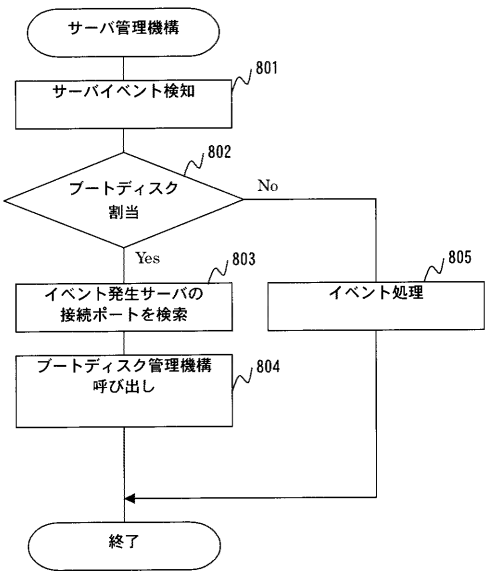
【図７】

図７



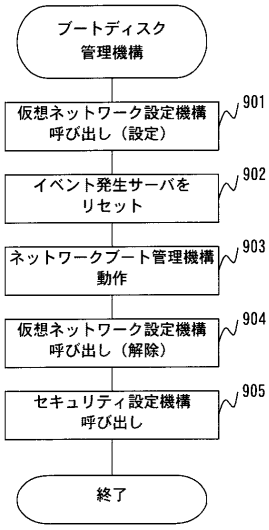
【図８】

図８



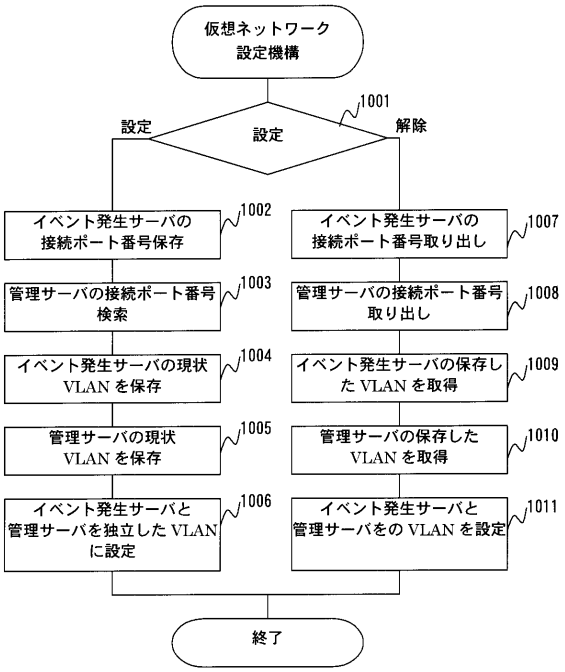
【図９】

図９



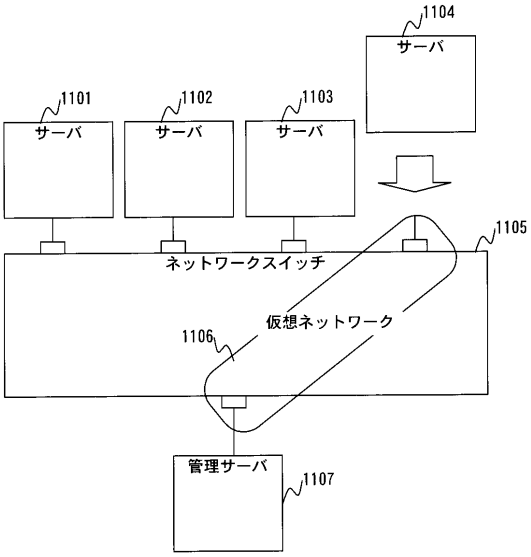
【図１０】

図１０



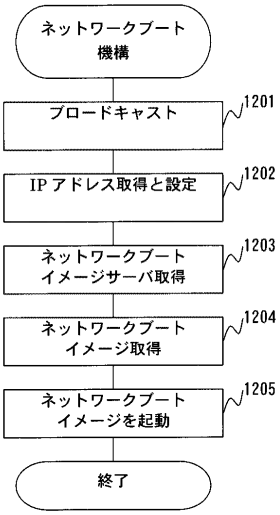
【図１１】

図１１



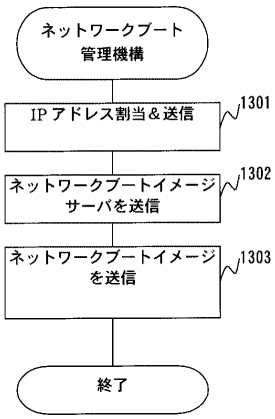
【図１２】

図１２



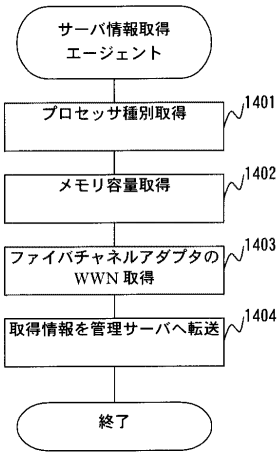
【図１３】

図１３



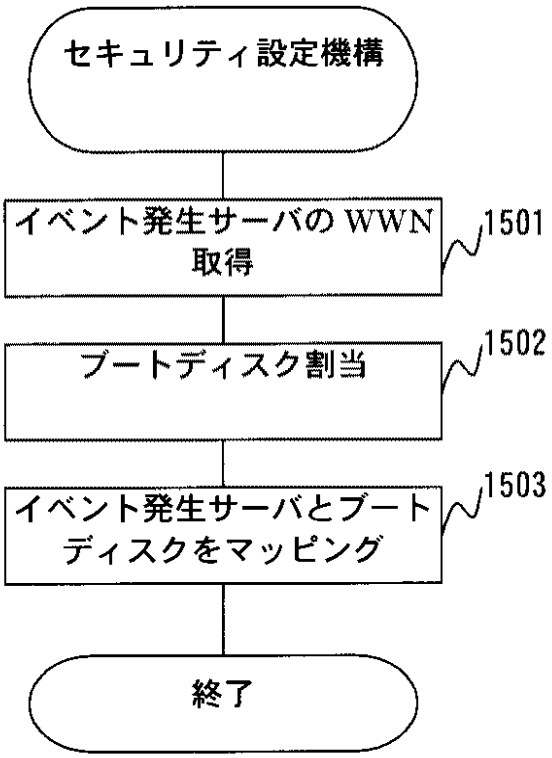
【図１４】

図１４



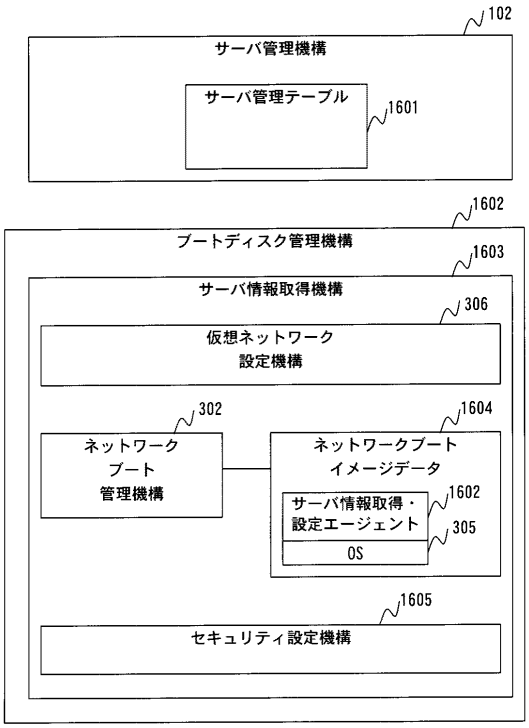
【図１５】

図１５



【図１６】

図１６



【図１７】

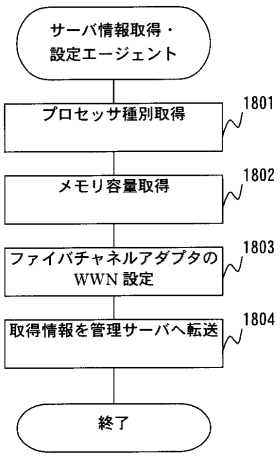
図１７

サーバ管理テーブル

401 サーバ識別子	402 ネットワーク接続ポート	403 プロセッサ種別	404 メモリ容量	405 ブートディスク	406 仮想ネットワーク	1701 設定 WWN
サーバ 1	1	CPU1	1GB	LU1	VLAN1	WWN1
サーバ 2	2	CPU1	1GB	LU0	VLAN1	WWN2
サーバ 3	3	CPU2	2GB	LU0	VLAN2	WWN3
サーバ 4	4	CPU1	2GB	LU2	VLAN3	WWN4
サーバ 5	5	CPU2	1GB	−	−	WWN5
サーバ 6	6	CPU1	4GB	−	−	WWN5
サーバ 7	7	CPU2	1GB	−	−	WWN6
サーバ 8	8	CPU1	4GB	−	−	WWN7
管理サーバ	10	CPU1	4GB	内蔵ディスク	−	−

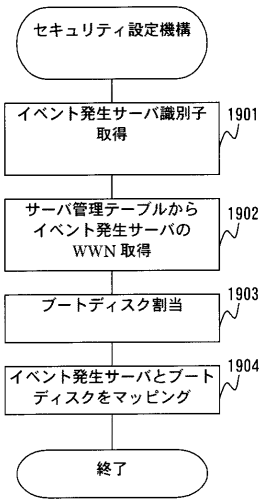
【図１８】

図１８



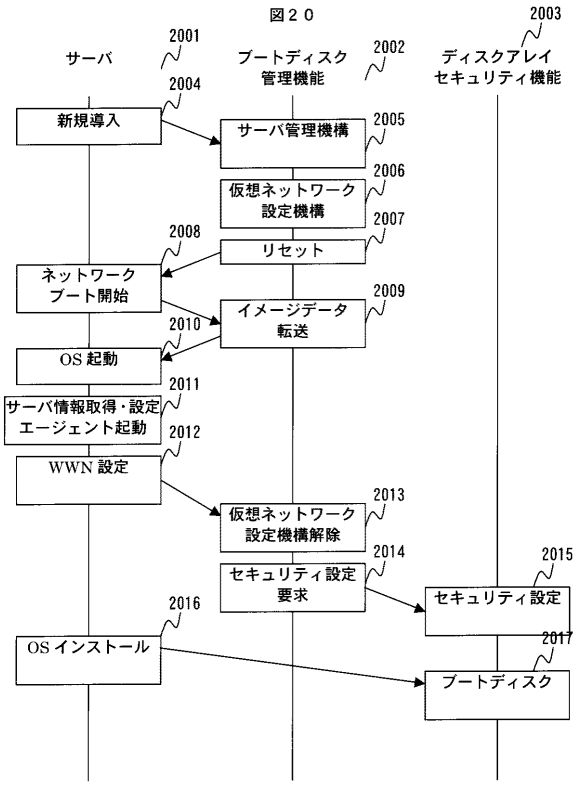
【図１９】

図１９



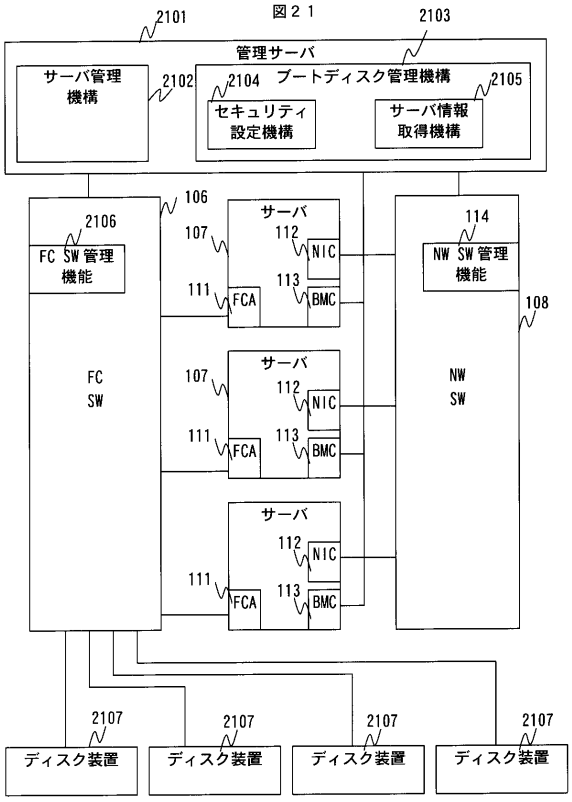
【図２０】

図２０



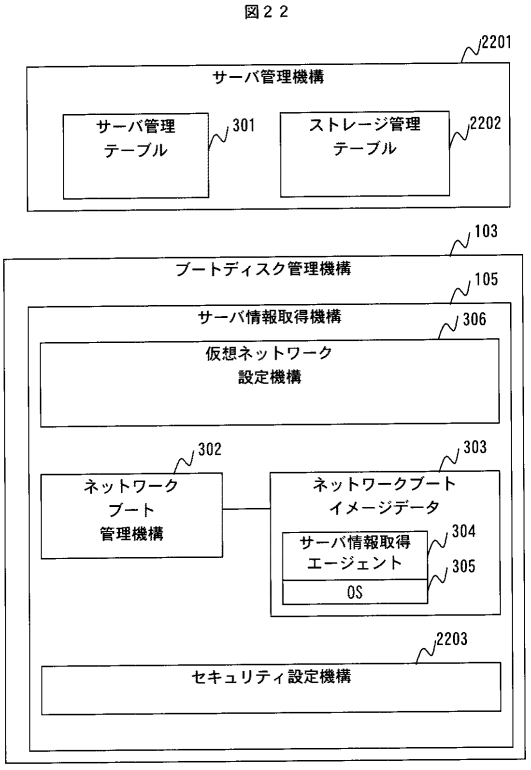
【図２１】

図２１



【図２２】

図２２



【図２３】

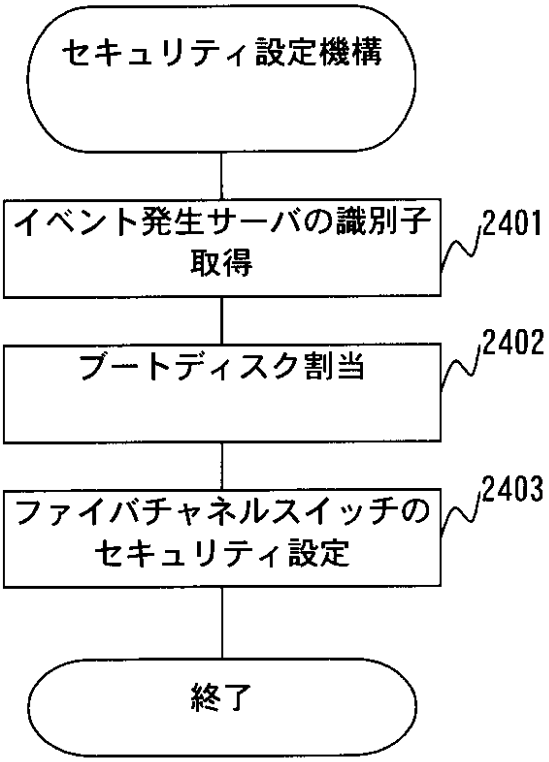
図２３

ストレージ管理テーブル

2301 接続装置識別子	2302 FCスイッチ接続ポート	2303 装置種別
サーバ１	1	サーバ
サーバ２	2	サーバ
サーバ３	3	サーバ
サーバ４	4	サーバ
ディスク１	5	ディスク
ディスク２	6	ディスク
ディスク３	7	ディスク
ディスク４	8	ディスク

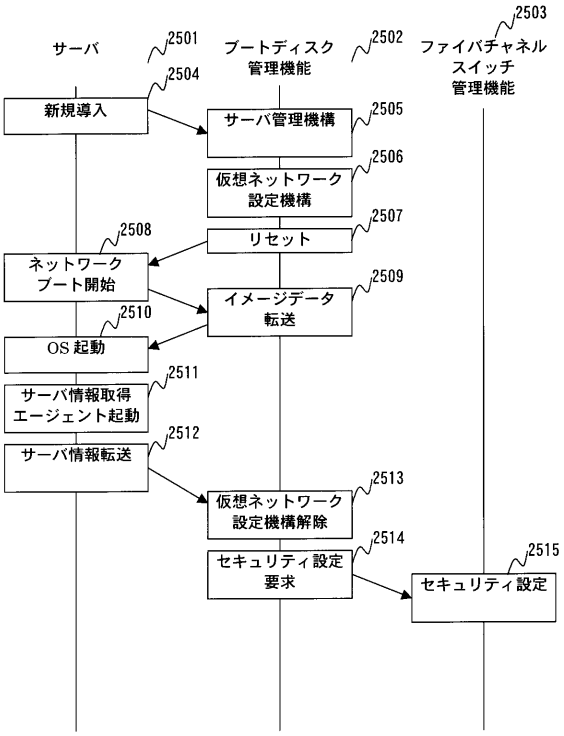
【図２４】

図２４



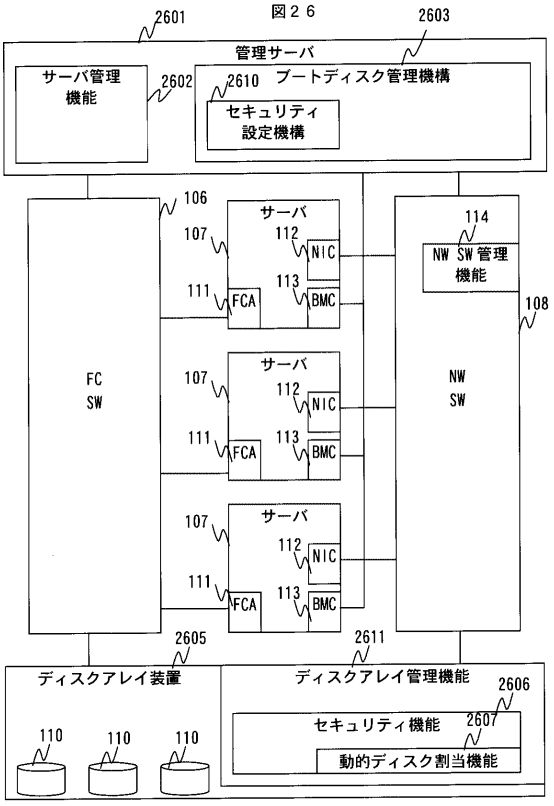
【図２５】

図２５



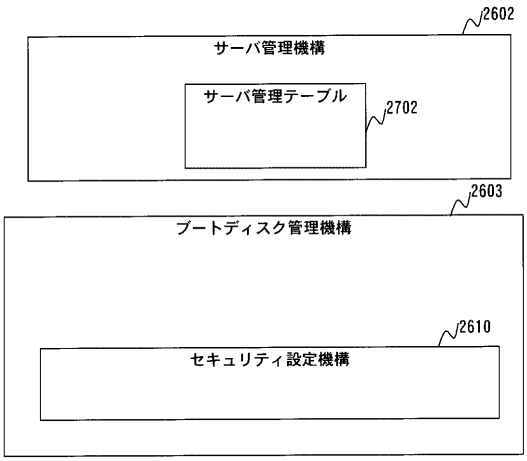
【図２６】

図２６



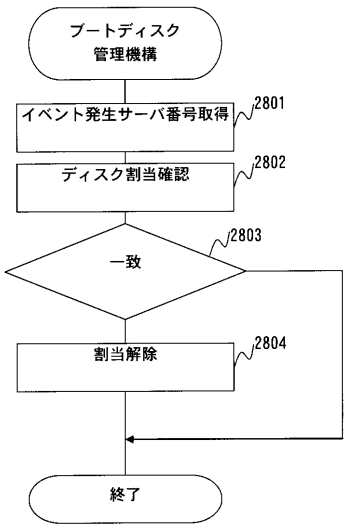
【図２７】

図２７



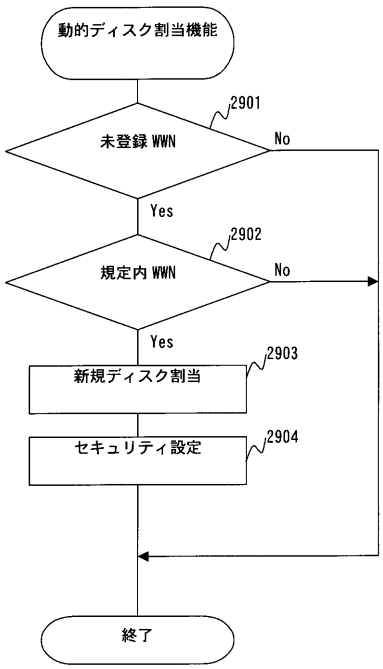
【図２８】

図２８



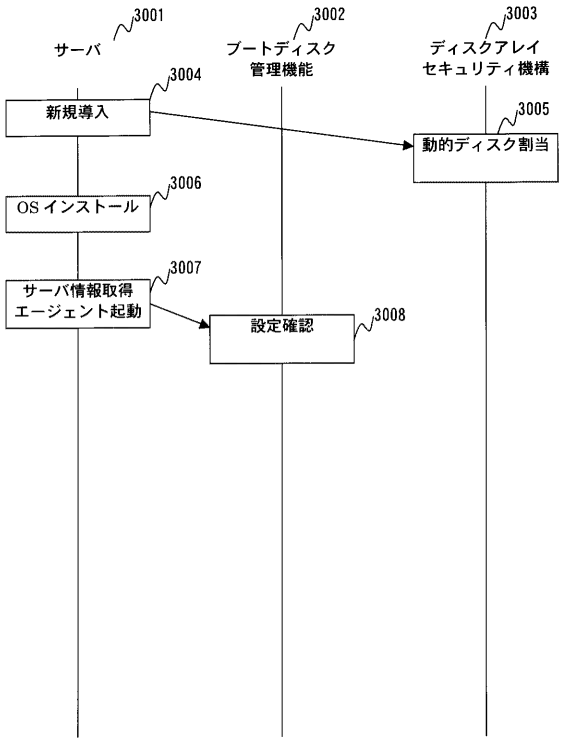
【図２９】

図２９



【図３０】

図３０



フロントページの続き

審査官　稲垣　良一

(56)参考文献　特開２００１－７５８５３（ＪＰ，Ａ）
特開２００４－１３７７８（ＪＰ，Ａ）
特開２００２－１４９５９９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　　９／４４５
Ｇ０６Ｆ　　３／０６
Ｇ０６Ｆ　１２／００
Ｇ０６Ｆ　２１／２２　　－　　２１／２４