(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-79251
(P2006-79251A)
(43)公開日　平成18年3月23日(2006.3.23)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/22	(2006.01)	G06F	9/06	660E	5B076
G06F 1/00	(2006.01)	G06F	1/00	370E	5B276

審査請求 有　請求項の数 3　OL　（全 8 頁）

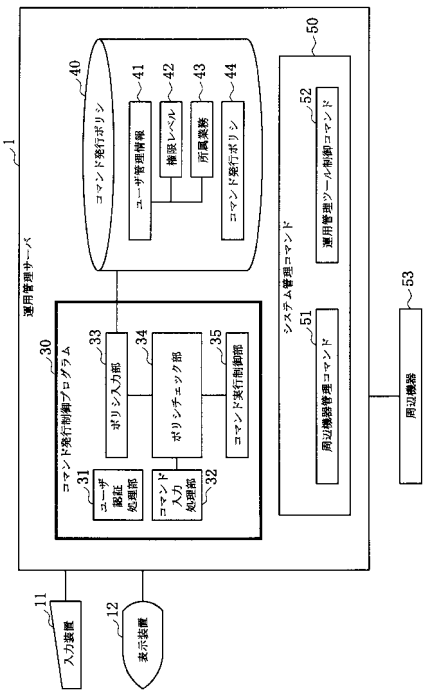
(21)出願番号　特願2004-260888 (P2004-260888)
(22)出願日　平成16年9月8日 (2004.9.8)

(71)出願人　000152985
株式会社日立情報システムズ
東京都品川区大崎１－２－１
(74)代理人　100102587
弁理士　渡邊　昌幸
(74)代理人　100077274
弁理士　磯村　雅俊
(72)発明者　京林　弘晃
東京都渋谷区道玄坂一丁目１６番５号　株式会社日立情報システムズ内

Ｆターム(参考)　5B076 FB05
5B276 FB05

(54)【発明の名称】コマンド実行制御システムおよび制御方法、ならびにそのプログラム

(57)【要約】
【課題】複数の業務処理システムおよび周辺機器を運用管理する運用管理サーバにおいて、オペレーションミスの防止によるデータ破壊等の事故を低減する。
【解決手段】操作者の操作権限と担当業務システムを定義したユーザ管理情報４１と、各コマンド毎にコマンド発行条件を操作権限と対応付けて定義したコマンド実行ルール定義情報（権限レベル）４２と、各業務システム毎に、管理対象の周辺機器を含む当該業務システムで実行可能なコマンドとそのオペランド指定値を定義した業務ルール定義情報（所属業務）４３とからなるコマンド発行ポリシ情報４４を管理サーバ１の記憶部４０に格納し、コマンド発行制御プログラム３０により、入力されたコマンドに対してポリシチェック部３４においてコマンド発行ポリシ情報４４と照合してコマンド実行の可否を制御する。
【選択図】図１



【特許請求の範囲】
【請求項１】
運用管理サーバ内に、操作者の操作権限と担当業務システムを定義したユーザ管理情報と、各コマンド毎にコマンド発行条件を該操作権限と対応付けて定義したコマンド実行ルール定義情報と、各業務システム毎に、管理対象の周辺機器を含む当該業務システムで実行可能なコマンドとそのオペランド指定値を定義した業務ルール定義情報とからなるコマンド発行ポリシ情報を記憶した記憶部、および、入力されたコマンドに対して前記記憶部に記憶されているコマンド発行ポリシ情報と照合し、コマンド実行の可否を制御するコマンド発行制御手段を有することを特徴とするコマンド実行制御システム。
【請求項２】
運用管理サーバ内に入力されたシステム管理用コマンドを、作業者の権限に応じて実行範囲を制御するコマンド発行制御方法において、
コマンド発行制御手段は、運用管理サーバのデータベースに保存される権限レベルおよび所属業務を含むユーザ管理情報と、コマンド発行ポリシ情報とを基に、作業者の認証、権限レベルをチェックし、
担当業務に応じて、入力されたシステム管理コマンドに対し、発行禁止コマンドまたはオペランドをチェックし、
チェック結果が実行ルールに違反した場合は、該システム管理コマンドの実行を中止し、
業務ルールに定義されたコマンドおよびオペランドと、更に指定値を検索して、業務ルールのチェックを実施し、
ルール違反がない場合には、注意喚起対象のコマンドまたはオペランドであるかをチェックし、
注意喚起対象のコマンドまたはオペランドであれば、実行可否を管理者装置に問合せ、該管理者装置からコマンド発行の指定があった場合のみ、コマンド発行を行い、
該システム管理コマンドを実行することを特徴とするコマンド実行制御方法。
【請求項３】
運用管理サーバのコンピュータに、運用管理サーバのデータベースに保存される権限レベルおよび所属業務を含むユーザ管理情報と、コマンド発行ポリシ情報とを基に、作業者の認証、権限レベルをチェックする手順、担当業務に応じて、入力されたシステム管理コマンドに対し、発行禁止コマンドまたはオペランドをチェックする手順、チェック結果が実行ルールに違反した場合は、該システム管理コマンドの実行を中止する手順、業務ルールに定義されたコマンドおよびオペランドと、更に指定値を検索して、業務ルールのチェックを実施する手順、ルール違反がない場合には、注意喚起対象のコマンドまたはオペランドであるかをチェックする手順、注意喚起対象のコマンドまたはオペランドであれば、実行可否を管理者装置に問合せる手順、該管理者装置からコマンド発行の指定があった場合のみ、コマンド発行を行う手順、該システム管理用コマンドを実行する手順を、それぞれ実行させるためのコマンド実行制御用プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、業務処理コンピュータシステムの運用業務に関し、特に、複数の顧客に各種業務処理サービスを提供するサーバまたはストレージシステムなどを運用・管理するデータセンタなどにおいて、作業者がシステム条件の設定変更やシステム障害対策を実施する際に、オペレーションミスによるシステム障害の発生を防止するために好適なコマンド実行制御システム、およびコマンド実行制御方法、ならびにそのプログラムに関する。
【背景技術】
【０００２】
近年、業務処理コンピュータシステムのオープン化、複雑化に伴って、システムを運用・管理するツールの増加や運用手順の複雑化を招いている。これにより、運用担当者やシ

ステム保守担当者が、システムをオペレーションする時間も長くなり、運用コマンドのオペランドの指定ミスや欠落などに起因するシステム障害の発生件数も増加傾向にある。

また、運用担当者の作業は、通常、操作対象システムに対して管理者権限を必要とするため、ＯＳ（オペレーティング・システム）へのログイン操作は、管理者権限を与えられたユーザが行う場合が多い。なお、個別に権限管理を行っていない運用管理ツールを利用した操作の場合、作業者の担当範囲を超えた操作も可能となるため、オペレーションミスによって、他の顧客システムのデータを破壊してしまうケースも懸念される。

【０００３】

このような技術背景において、システム運用時のオペレーションミスを防ぐ手法として、例えば、特開平６－１２３４７号公報に記載の『遠隔操作コマンド実行制御方式』（特許文献１参照）がある。

上記公報に記載の発明では、１つの情報処理システムから他の情報処理システムを操作、監視するために、操作コンピュータからどのコマンドがどのオペレータにより実行を許されているかの情報を定義する機構を備えており、操作コンピュータから遠隔操作時に遠隔地にある操作対象コンピュータに対して、実行すべきコマンドとオペレータを特定する情報を転送し、被操作対象コンピュータ上で当該コマンドが操作コンピュータからの遠隔操作が許されているかを判断した後、当該操作コマンドを実行可能にする。

さらに、被操作対象コンピュータ上でコマンド毎に実行してもよいシステムの動作状態および条件を予め定義しておく機構と、システムの動作状態を常に把握している情報管理機構を備えており、定義情報とシステム状態を確認することにより、当該コマンドを実行する前に当該コマンドの実行可否を被操作対象コンピュータの状態に応じて決定している。

【０００４】

【特許文献１】特開平６－１２３４７号公報

【発明の開示】

【発明が解決しようとする課題】

【０００５】

従来の技術においても、運用コマンド操作時のオペレーションミスを防止する方法の１つとして、ＯＳに登録されたユーザアカウントに対応した作業者にコマンドの実行権限を与えて、危険なコマンドの実行を制限させることが可能である。しかし、この方法は、作業者が個別の業務処理システム毎に個別のシステム管理コマンドを利用する場合には有効であるが、複数の業務処理システムに対し、同一のシステム管理コマンドを利用する場合などは、コマンドのオペランドに個別業務処理システム毎に割り当てられたＩＤ等を指定する必要があるため、アクセス権による実行制限ができず、オペレーションミスによって、担当業務処理システム以外の設定を変更してしまう可能性がある。

【０００６】

また、前記特開平６－１２３４７号公報記載の技術においては、操作者と操作対象コンピュータ、および実行可能コマンドとの対応付けの制御と、コマンド実行時の被操作対象コンピュータの状態に応じたコマンド実行可否を制御しているため、複数の異なる業務処理システム単位のコマンド実行制御が実現されていない。また、同じコマンドであっても被制御対象の業務処理システムの違いによってそのコマンドのオペランド設定値を変更する必要がある場合に、入力コマンドのオペランド設定値の誤りをチェックすることが行われていない。

【０００７】

また、前記公報記載の技術では、コマンド実行可否の判断処理を被操作対象コンピュータ側で行っているため、例えば、運用管理サーバに入力されたコマンドが、直接、前記運用管理サーバに接続されたストレージ装置に対するコマンドの場合には、被操作対象装置がストレージ装置であるため被操作対象装置側でコマンド実行可否を判断することが出来ないという問題がある。

【０００８】

（目的）
そこで、本発明の目的は、複数の業務処理システムおよび周辺機器を運用管理する運用管理サーバにおいて、オペレーションミスの防止によるデータ破壊等の事故を低減することが可能なコマンド実行制御システムおよび制御方法、ならびにそのプログラムを提供することにある。
【課題を解決するための手段】
【０００９】
上記目的を達成するため、作業者毎に実行可能なコマンドやオペランドの組合せおよびルールをポリシに定義し、これに基づいてコマンドの実行可否を制限するシステムを設ける。すなわち、運用管理サーバに、作業者とコマンド発行ルールを決定するための権限レベルおよび担当業務を保存するためのユーザ管理情報と、管理ツールで提供されるコマンドやオペランドを、どの権限または業務担当者に実行を許可（または拒否）するかを定義したコマンド発行ポリシを管理させる。
また、運用管理サーバ内には、作業者からのコマンドを受付けて、前記のコマンド発行ポリシとの照合を行ってコマンドの実行可否を決定し、コマンドを実行制御するためのコマンド発行制御プログラムを設ける。
【００１０】
このコマンド発行制御プログラムは、コマンドの受付けに先立ち、ユーザ認証を実施して作業者の権限レベルと業務有効範囲を決定する。そして、コマンド発行ポリシ内の定義情報から、作業者毎に適用すべきルールを作成する。このルールを利用して、作業者の作業範囲や担当顧客をコマンドの発行前にチェックすることで、オペランド指定ミスや欠落および要注意コマンドの発行を防止することが可能となる。
なお、システム管理コマンドは、作業者が利用するＯＳのユーザアカウントでは、実行できないように、ファイルのアクセス権を設定しておくことで、コマンド発行制御プログラムを介さないコマンドの発行を防止することが可能になる。
【発明の効果】
【００１１】
本発明によれば、複数の顧客に業務処理サービスを提供しているサーバやストレージ機器等の運用・保守業務において、担当者毎の作業範囲および担当システムをルール化してデータベースに保存し、専用のコマンド入力インタフェースを提供してこれをチェックすることで、オペレーションミスの防止によるデータ破壊等の事故を低減することが可能となる。
さらに、ユーザ管理機能を持たないシステム管理ツールが多くかつ複数顧客のシステムを、運用・保守するデータセンタなどにおいては、作業者の担当範囲を超えた操作を抑止できるため、アウトソーシングサービスの信頼性向上に繋がる。
【発明を実施するための最良の形態】
【００１２】
以下、本発明の実施の形態を、図面を用いて詳細に説明する。
図１は、本発明のコマンド発行制御システムでコマンドの発行制限を行う方式の一実施例を説明するためのシステム構成図である。
図１において、運用管理サーバ１は、作業者からのコマンドを受付けるための入力装置１１と入力内容を表示するための表示装置１２および、作業者からのコマンドを受付けて周辺機器５３を制御するための周辺機器管理コマンド５１や運用管理ツールの設定変更を行うための運用管理ツール制御コマンド５２などのシステム管理コマンド５０を有する。さらに、作業者からのコマンドを実行制御するためのプログラム３０とコマンド発行時のルールを作成するためのコマンド発行ポリシ４０を有する。
【００１３】
コマンド発行制御プログラム３０は、コマンド発行ポリシ４０内に存在するユーザ管理情報４１とコマンド発行ポリシ４４をポリシ入力部３３により入力し、ユーザ認証処理部３１によって、作業者を認証する。認証OKとなった場合は、作業者に作業可能範囲を決定す

るための権限レベル４２と担当業務４３を割り当てる。そして、コマンド入力処理部３２によって、作業者からのコマンドを受付け、ポリシチェック部３４で権限チェックを実施し、権限を保有している場合は、コマンド実行制御部３５によって作業者からのコマンドを実行する。

【００１４】

図２は、本発明のコマンド発行制御システムにおいて、コマンドの発行制限を実施する場合に、作業者を認証するために必要なユーザ管理情報の登録例を示す図である。

図２において、ユーザ名とパスワードは、本システムを利用する作業者を認証するための管理情報であり、ＯＳの管理ユーザとは異なる。また、権限レベルは、システム管理ツールを利用する際に、コマンドの実行可否を決定するためのレベルであり、所属業務は、担当する顧客を識別するための情報である。

【００１５】

図３は、本発明のコマンド発行制御システムにおいて、コマンドの発行制限を実施する場合に、コマンドの実行ルールを決定するためのコマンド発行ポリシ（実行ルール）の登録例を示す図である。

図３において、ポリシ種別は、禁止、必須、注意喚起などのルールの種類を表す。適用は先に説明したユーザ管理情報の権限レベルに対応し（(1)により図２との関連を示す）、当該ルールをどの権限保有者に適用すべきかを決定するための情報である。コマンドとオペランドは、作業者が投入したコマンドまたはオペランドに対し、当該ルールの対象となるか否かを決定するために必要な情報である。

【００１６】

図４は、本発明のコマンド発行制御システムにおいて、コマンドの発行制限を実施する場合に、担当業務を決定するためのコマンド発行ポリシ（業務ルール）の登録例を示す図である。

図４において、適用業務は、先に説明したユーザ管理情報の所属業務に対応し、顧客毎にチェックすべき情報（ルール）であることを示す。コマンドおよびオペランドと指定値は、作業者からの投入されたコマンドに対し、必ず指定されなければならないオペランドと指定値を定義したものである。なお、適用業務は、先に説明したユーザ管理情報の所属業務に対応し（(2)により図２との関連を示す）、当該ルールをどの所属業務に適用すべきかを決定するための情報である。

【００１７】

図５は、本発明の一実施形態に係るコマンドを実行する際の処理手順を示すフローチャートである。

コマンド発行制御プログラム３０のポリシ入力部３３は、作業者のユーザ認証結果から権限レベルと所属業務を決定し、作業者に有効なポリシを保持する。そして、コマンド入

【００１８】

力処理部３２でコマンドを入力し（５０１）、ポリシチェック部３４で、発行禁止コマンドまたはオペランドをチェックする（５０２）。チェック結果がルール（実行ルール）に違反した場合は、コマンドの実行を中止する（５０３）。違反していなければ、次に進む。次は、業務ルールに定義されたコマンドおよびオペランドと、更に指定値を検索して、業務ルールのチェックを実施する（５０４）。指定値が設定されていない場合などは、ルール違反とみなし、コマンドの実行を中止する（５０５）。ルール違反がない場合には次に進む。次は、注意喚起対象のコマンドまたはオペランドであるかをチェックし（５０６）、注意喚起対象であれば、実行可否を管理者装置に問合せ（５０７）、該管理者装置からコマンド発行の指定があった場合のみ（５０８）、コマンド発行を行う（５０９）。コマンド発行の指定がない場合には、コマンド発行を行わない。なお、管理者装置は、問合わせに対して予め定めてあるものだけに承認を与える、例えばパソコン等の装置を配置する。

【００１９】

図６は、本発明の一実施形態に係るコマンド実行制御プログラムによるコマンド発行の一例図である。

コマンド実行制御プログラムでユーザ認証がＯＫとなった場合、コマンド入力用のプロンプトが表示される。作業者は、このプロンプトからコマンドを入力し、Enterキーを押下する。Enterキーの押下後、作業者に割り当てられた禁止ルールに違反した場合は、６０１に示すとおり、コマンドが実行できない旨のメッセージが表示される。また、必須ルールに違反した場合は、６０２に示すとおり、オペランド未指定によりコマンドが実行できない旨のメッセージが表示される。更に、注意喚起ルールに合致した場合は、６０３に示すとおり、続行可否確認メッセージが表示され、作業者の指示によりコマンドの実行を制御することが可能となる。

また、特定のオペランドで指定した文字列が、担当顧客以外であった場合など、業務ルールに違反した場合は、６０４に示すとおり、メッセージが表示され、コマンドを実行することはできない。

【００２０】

図７は、本発明の一実施形態に係るコマンドの実行制御を行った場合の動作結果例を示す説明図である。

運用管理サーバ７０１には、ストレージ装置９００が接続され、ストレージ管理コマンド群８００によって、Ａ社用ディスク９０１やＢ社用ディスク９０２を操作する。ここで、作業者ＡＢＣ（７０２）はＡ社用の操作コマンドxyz t AAA（８０１）を利用する。また、作業者ＤＥＦ（７０３）はＢ社用の操作コマンドxyz t BBB（８０３）を利用する。なお、aaaコマンド（８０２）は、双方とも利用できない要注意コマンドである。

これらの発行ルールは、運用管理サーバ７０１内のコマンド発行ポリシ７０５に予め格納される。この時は、コマンド発行制御プログラム７０４経由で作業した場合に、aaaコマンドの実行や作業者ＡＢＣが、Ｂ社用のディスクを操作することはできない。逆に、作業者ＤＥＦは、Ａ社用のディスクを操作することは不可能となる。

【００２１】

図５に示すコマンド実行処理フローをプログラムコード化し、完成したプログラムをＣＤ－ＲＯＭなどの記録媒体に格納しておけば、本実施形態の運用管理サーバのコンピュータに記録媒体を装着し、プログラムをインストールして実行させることにより、本発明を容易に実現できる。また、記録媒体をインターネットを介してダウンロードしたり、直接に貸与または販売することで、コマンド実行制御プログラムを広く汎用化することも可能である。

【産業上の利用可能性】

【００２２】

本実施形態における顧客の業務処理システムを、運用・保守するための管理サーバやストレージ装置を備えたデータセンタ等における情報処理のアウトソーシングサービスに利用できる。

【図面の簡単な説明】

【００２３】

【図１】本発明の一実施形態に係るコマンド実行制御システムの構成図である。

【図２】本発明の一実施形態に係る運用管理サーバ内で管理されるユーザ管理情報の登録例を示す図である。

【図３】同じく運用管理サーバ内で管理されるコマンド発行ポリシ（実行ルール）の登録例を示す図である。

【図４】同じく運用管理サーバ内で管理されるコマンド発行ポリシ（業務ルール）の登録例を示す図である。

【図５】本発明の一実施形態に係るコマンド実行処理手順を示すフローチャートである。

【図６】本発明の一実施形態に係るコマンド実行制御プログラムによるコマンド発行の図である。

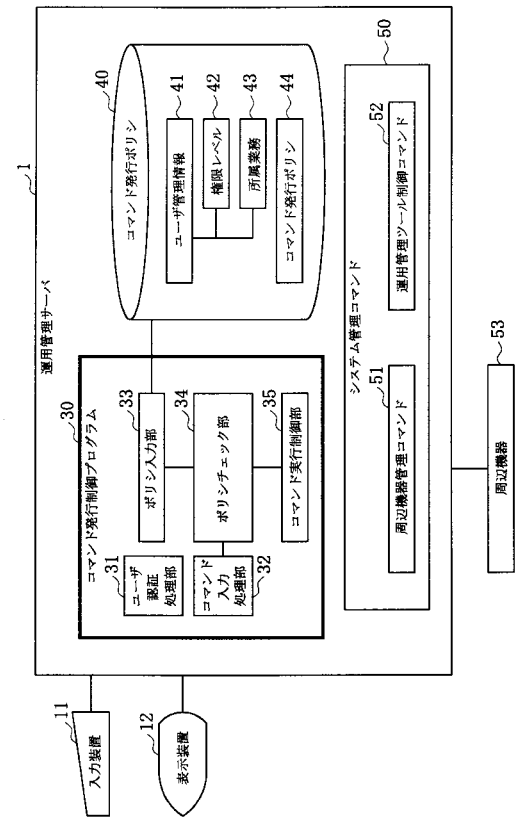
【図７】本発明の一実施形態に係る動作結果例を示す説明図である。

【符号の説明】

【００２４】

１・・・・・・・・運用管理サーバ
１１・・・・・・・・入力装置
１２・・・・・・・・表示装置
３０・・・・・・・・コマンド発行制御プログラム
３１・・・・・・・・ユーザ認証処理部
３２・・・・・・・・コマンド入力処理部
３３・・・・・・・・ポリシ入力部
３４・・・・・・・・ポリシチェック部
３５・・・・・・・・コマンド実行制御部
４０・・・・・・・・コマンド発行ポリシ
４１・・・・・・・・ユーザ管理情報
４２・・・・・・・・権限レベル
４３・・・・・・・・所属業務
４４・・・・・・・・コマンド発行ポリシ
５０・・・・・・・・システム管理コマンド
５１・・・・・・・・周辺機器管理コマンド
５２・・・・・・・・運用管理ツール制御コマンド
５３・・・・・・・・周辺機器

【図１】



【図２】

ユーザ管理情報

ユーザ名	パスワード	権限レベル	所属業務	…
ＡＢＣ	*****	operator	A社	…
ＤＥＦ	*****	operator	B社	…
ＧＨＩ	*****	admin	ＡＬＬ	…
…	…	…	…	…

①　②

【図３】

①

コマンド発行ポリシ（実行ルール）

ポリシ種別	適用	コマンド	オペランド	…
禁止	operator	aaa		…
必須	operator	bbb	-a	…
注意喚起	ＡＬＬ	xyz	-b	…
…	…	…	…	…

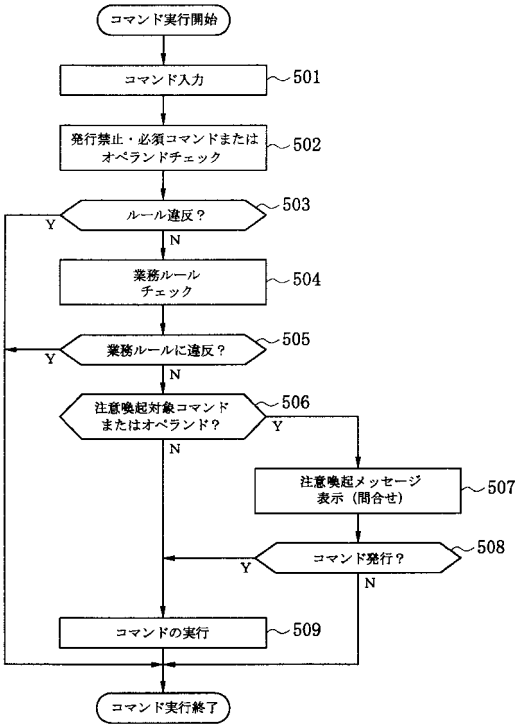
【図４】

コマンド発行ポリシ（業務ルール）

適用業務	コマンド	オペランド	指定値	…
A社	setdata	-t	ADATA	…
B社	setdata	-t	BDATA	…
C社		-r	CDATA	…
…	…	…	…	…

②

【図５】



【図６】

(ABC)>aaa -t ADATA ～601
aaaコマンドは実行できません
(ABC)>bbb -b ～602
bbbコマンドに-aオペランドが指定されていないため実行できません。
(ABC)>xyz -b -t ADATA ～603
-bが指定されました。続行しますか(y/n)y
xyz -bを実行しました
(ABC)>xyz -b -t BDATA ～604
BDATAの操作はできません

【図７】