

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5425912号
(P5425912)

(45) 発行日 平成26年2月26日 (2014. 2. 26)

(24) 登録日 平成25年12月6日 (2013. 12. 6)

(51) Int. Cl.

F I

G 0 6 F 21/44 (2013. 01)

G 0 6 F 21/20 1 4 4 B

G 0 6 F 21/12 (2013. 01)

G 0 6 F 21/22 1 1 2 F

請求項の数 12 (全 10 頁)

(21) 出願番号	特願2011-529000 (P2011-529000)	(73) 特許権者	511076424
(86) (22) 出願日	平成20年9月30日 (2008. 9. 30)		ヒューレット・パカード デベロップメント カンパニー エル. ビー.
(65) 公表番号	特表2012-504271 (P2012-504271A)		Hewlett-Packard Development Company, L. P.
(43) 公表日	平成24年2月16日 (2012. 2. 16)		アメリカ合衆国 テキサス州 77070
(86) 国際出願番号	PCT/US2008/078210		ヒューストン コンパック センタ ド
(87) 国際公開番号	W02010/039118		ライブ ウェスト 11445
(87) 国際公開日	平成22年4月8日 (2010. 4. 8)	(74) 代理人	100099623
審査請求日	平成23年5月23日 (2011. 5. 23)		弁理士 奥山 尚一
		(74) 代理人	100096769
			弁理士 有原 幸一
		(74) 代理人	100107319
			弁理士 松島 鉄男

最終頁に続く

(54) 【発明の名称】 パーティション上のサービスの認証

(57) 【特許請求の範囲】

【請求項 1】

システム内で複数のオペレーティングシステムを動作可能にするように当該システムを個別のセクションに分割し、サービスを実行するよう構成したパーティションと、

前記パーティションと関連付けた認証サービスのリストと、

前記パーティションと通信状態にあり、前記システムを制御する管理プロセッサであって、前記サービスが前記認証サービスのリストにリストされている場合に、前記サービスに対するクレデンシャルを生成するように構成された管理プロセッサとを備えてなり、

前記パーティションは、前記サービスから前記管理プロセッサに管理プロセッサのリソースを求める要求を送信し、前記要求は前記サービスに対する前記クレデンシャルを含むものであり、

前記管理プロセッサは、前記要求が前記サービスに対して認証されていることを検証した後に、前記要求を実行することを特徴とするサービスを認証するシステム。

【請求項 2】

前記サービスから前記管理プロセッサに、クレデンシャルを求める要求を送信するメッセージキューを更に備える請求項 1 に記載のシステム。

【請求項 3】

前記サービスが前記認証サービスのリストにリストされていることを検証した後に、ク

10

20

レデンシャルを求める前記要求を前記管理プロセッサに送信するように、前記メッセージキューを構成する請求項2に記載のシステム。

【請求項4】

前記サービスから前記管理プロセッサに管理プロセッサのリソースを求める要求を送信する帯域内通信デーモンを更に備え、前記要求は前記サービスに対する前記クレデンシャルを含む請求項1に記載のシステム。

【請求項5】

システム内で複数のオペレーティングシステムを動作可能にするように当該システムを個別のセクションに分割するパーティション上で稼働するサービスを認証する方法であって、

クレデンシャルを求める要求を前記サービスによって開始することと、

前記パーティションと関連付けた認証サービス群に前記サービスがリストされているかを前記パーティションによって検証することと、

前記サービスが前記認証サービス群にリストされていた場合、前記パーティションが、前記パーティションと通信状態にある前記システムを制御するために、クレデンシャルを求める前記要求を管理プロセッサに送信することと、

前記サービスに対して前記要求が認証されたことを前記管理プロセッサにより検証した後に、前記要求を実行することと
を含んでなる方法。

【請求項6】

前記管理プロセッサに、前記サービス用の演算リソースを求める要求を前記サービスにより送信することを更に含んでなり、

前記要求は、前記要求に応じて前記管理プロセッサから受信した前記サービスに対するクレデンシャルを含む請求項5に記載の方法。

【請求項7】

前記クレデンシャルは、前記管理プロセッサが生成したランダムなパスワードを含む請求項6に記載の方法。

【請求項8】

前記クレデンシャルは、指定期間後に期限切れする請求項6に記載の方法。

【請求項9】

前記クレデンシャルが期限切れした場合、クレデンシャルを求める新たな要求を前記管理プロセッサに自動的に送信することを更に含んでなる請求項8に記載の方法。

【請求項10】

システム内で複数のオペレーティングシステムを動作可能にするように当該システムを個別のセクションに分割するパーティション上で稼働するサービスを認証するコンピュータプログラムであって、

前記プログラムをコンピュータプロセッサが実行すると、前記コンピュータプロセッサに、

前記サービスに対応する一意なサービス識別子を含み、クレデンシャルを求める要求を前記サービスによって開始する、ステップと、

前記サービスが認証サービス群にリストされているかを前記パーティションにより検証するステップと、

前記サービスが前記認証サービス群にリストされていた場合に、前記クレデンシャルを求める要求を前記パーティションが管理プロセッサに送信するステップと

前記サービスに対して前記要求が認証されたことを前記管理プロセッサにより検証した後に、前記要求を実行するステップと
を実行させるコンピュータプログラム。

【請求項11】

前記プログラムが、前記コンピュータプロセッサに、前記要求に応じて、前記サービスに対するクレデンシャルを前記管理プロセッサから受信するステップを更に実行させる請

10

20

30

40

50

求項 10 に記載のコンピュータプログラム。

【請求項 12】

前記プログラムが、前記コンピュータプロセッサに、前記管理プロセッサに前記サービス用の演算リソースを求める要求を送信するステップを更に実行させ、前記演算リソースを求める要求は、前記一意なサービス識別子及び前記クレデンシャルを含む請求項 11 に記載のコンピュータプログラム。

【発明の詳細な説明】

【背景技術】

【0001】

多くのシステム（例えば、ブレードサーバ又はセルラサービス）は、システムを個別のセクションに分割するパーティションを利用して、システム内で複数のオペレーティングシステムを動作可能にしている。パーティションは 2 つの主なカテゴリである、ソフトパーティションとハードパーティションとを含む。ハードパーティションは、システムを物理的に独立したパーティションに分割することによってボードレベルで実装され、該パーティションにより、論理的且つ電氣的に複数のオペレーティングシステムを隔離する。ソフトパーティションは、サーバリソース（例えば、CPU 及びメモリ使用量）を各パーティションに割り当てることによって処理コアレベルで実装され、該パーティションは複数のオペレーティングシステムを機能的に離隔するが、電氣的には隔離しない。

10

【0002】

パーティションは、該パーティション内で稼働する様々なサービスを有してもよい。サービスをパーティション内で動作させるには、システムの他のパーティションから情報及び／又は構成変更を要求する必要があるかも知れない。これまで、そうした要求は、セキュリティドメインへのアクセスを制御せずに、又は要求をロギングせずに、実行されてきた。しかしながら、システムのセキュリティに関する認識が高まり、要求の実行を認可する及び／又は証跡エントリをロギングする前に、サービスの認証が必要となった。

20

【発明の概要】

【0003】

本開示の実施形態は、パーティション上で動作するサービスを認証するシステム及び方法に関する。

【0004】

30

簡単に説明すると、一実施形態では、特に、サービスを認証するシステムを備える。このシステムは、サービスを実行するよう構成したパーティションと、該パーティションに関連付けた認証サービスのリストと、該パーティションと通信状態の管理プロセッサとを備えており、管理プロセッサを、サービスが認証サービスのリストにリストされている場合、当該サービスに対してクレデンシャルを生成するように構成する。

【0005】

別の実施形態では、特に、パーティション上で稼働するサービスを認証する方法を備える。この方法は、サービスによってクレデンシャルを求める要求を開始すること、そのサービスが、パーティションと関連付けた認証サービス群にリストされているかを検証すること、サービスが認証サービス群にリストされている場合、クレデンシャルを求める要求を管理プロセッサに送信することを備える。

40

【0006】

別の実施形態では、特に、サービスを認証するプログラムを備えるコンピュータ可読記憶媒体を備える。プログラムをコンピュータプロセッサが実行すると、該プログラムがプロセッサに、サービスによってクレデンシャルを求める要求を開始し、該要求はサービスに対応する一意なサービス識別子を含むステップと、サービスが認証サービス群にリストされているかを検証するステップと、サービスが認証サービス群にリストされている場合に、クレデンシャルを求める要求を管理プロセッサに送信するステップとを実行させる。

【0007】

本開示に関する他のシステム、方法、特徴、効果については、以下の図面及び詳細な説

50

明を検討すると、当業者には明らかになるであろう。そうした更なるシステム、方法、特徴、効果の全ては、本明細書に含まれ、本発明の範囲内とし、添付のクレームで保護されるものとする。

【図面の簡単な説明】

【0008】

以下の図面を参照することで、本発明の多くの態様について、一層理解できるであろう。図面の構成要素は必ずしも正確な縮尺ではなく、本発明の原理を明確に説明する際に強調されている。また、図面中、同一参照番号により複数の図を通して対応する部品を指している。

【図1】本開示の一実施形態によるパーティション分割したシステムの図である。

10

【図2】本開示の一実施形態による例示的な認証システムに含まれる管理ツールをインストールした後の、図1のパーティション分割したシステムの図である。

【図3】本開示の一実施形態によるサービス開始時の図2の認証システムの図である。

【図4】本開示の一実施形態による管理プロセッサのリソースに要求を行うサービスを含む、図2の認証システムの図である。

【図5】本開示の一実施形態によるパーティション上で稼働するサービスを認証する例示的な方法について説明するフローチャートである。

【発明を実施するための形態】

【0009】

本明細書で開示するのは、パーティション上で稼働するサービスの認証に関する方法及びシステムの様々な実施形態である。次に、図面で示した実施形態の説明について詳細に言及するが、同一参照番号は、複数の図を通して同一部品を指す。

20

【0010】

パーティションをシステム内に作成する際、システムの管理プロセッサ(MP)は、プロセッサ依存ハードウェアコントローラ(PDHC)に、構成するパーティションと関連付けた1つ又は複数のインタフェースを起動するよう命令する。図1は、本開示の1実施形態によるパーティション分割したシステム100の図である。パーティション分割したシステムは、所望する数のパーティションを含んでもよい。図1の非限定的な実施形態では、単一のパーティション101を説明目的のみで示す。パーティション101は、インタフェース109を介してPDHC106と通信する。PDHC106は、パーティション101と関連付けた帯域内通信チャネル107とブロック転送(BT)インタフェース108を含み、其々、共通情報モデルオブジェクトマネージャ(CIMOM)111とベースボード管理コントローラ(BMC)112と通信する。CIMOM111とBMC112をMP110に含む。パーティション101を管理するパーティション管理アカウント113も、CIMOM111と通信状態にする。

30

【0011】

図2は、例示的な認証システム200に含まれる管理ツールをインストールした後の、図1のパーティション分割したシステムの図である。パーティション101上での管理ツールのインストールは、パーティション101の作成と同時、又は後で行ってもよい。例えば、HPUX環境では、認証システム200用ソフトウェアをオペレーティングシステム(OS)と共にインストールしてもよい。Windows(登録商標)、OpenVNS、Linux又は他の環境では、認証システム200の適切な実施形態のインストールを、OSをパーティション上にインストールするのとは別に行ってもよい。任意のOSで、更新及び追加サービスのインストールをサポートしてもよい。如何なる環境でもインストール及び更新には、パーティションへの管理又はルートアクセスを伴う。パーティション101上にインストールする特定のOSは、インタフェース109へのアクセスを制御するために、そのOS特有のファイルシステム許可を使用してもよい。

40

【0012】

図2の実施形態では、パーティション101にインストールした管理ツールは、帯域内通信デーモン202、帯域内通信に対する認証デーモン203、メッセージキュー204

50

、及び認証サービス（AuthServ）群205を含む。帯域内通信デーモン202は、インタフェース109を介して帯域内通信チャンネル107と通信する。帯域内通信用認証デーモン203は、メッセージキュー204を介してAuthServ群205と通信し、インタフェース109を介してブロック転送インタフェース108と通信する。AuthServ群205は、サービス識別子（SID）のリストを含む。一意のSIDを、パーティション上で稼働するサービスと関連付ける。図2の非限定的な実施形態では、SID1とSID2を説明目的のみで示している。AuthServ群205と関連付けるSIDの数は、他の実施形態では異なるかも知れない。AuthServ群205にあるSIDのリストを、パーティション管理アカウント113によって追加投入し、リストされたSIDは、パーティション101上で稼働するよう認可するサービスに対応する。かかるサービスは、例えば、給与アプリケーション、グローバルな作業負荷マネージャ、又は付加価値のあるアプリケーション等のソフトウェアアプリケーションを含むが、これらに限定するものではない。

10

【0013】

帯域内通信デーモン202の実施形態は、MPリソース用演算リソースを求める要求を、パーティション101上で稼働するサービスからMP110へ送信してもよい。実施形態によっては、帯域内通信デーモン202がパーティション101とMP110間の要求を開始するのを禁止する。例えば、デーモン202はパーティション101上のサービスとMP110との間で要求を転送だけしてもよい。従って、かかる実施形態では、帯域内通信デーモン202は、MP110にアクセスするためにそれ自体のアクセスクレデンシャルを有する必要はない。

20

【0014】

帯域内通信203用認証デーモンの実施形態を使用して、インタフェース109及びBTインタフェース108を介してMP110からサービスに対するクレデンシャルを要求してもよい。インタフェース109の実施形態は、インテリジェントプラットフォーム管理インタフェース（IPMI）を含んでもよく、IPMIに接続するためには管理ユーザレベルのアクセスが求められる。かかる実施形態では、認証デーモン203は、MP110にデータを伝送するために、特別に定義したIPMI要求を使用してもよい。また、認証デーモン203は、サービスと通信するためにメッセージキュー204を使用してもよい。

30

【0015】

AuthServ群205の実施形態を使用して、メッセージキュー204へのアクセスを制御してもよい。メッセージキュー204を、帯域内通信203用認証デーモンが使用して、MP110からのクレデンシャルを要求する。AuthServ群205からSIDを作成、追加、修正、又は削除するには、パーティション101への管理者レベルのアクセスを必要としてもよい。また、AuthServ群205で、MP110のリソースへのアクセスのレベルを、特定のサービスが認証されるレベルで指定してもよい。

【0016】

図3は、本開示の1実施形態によるサービス開始時の図2の認証システムの図である。単一のサービス314を図3に示しているが、任意の適切な数のサービスもパーティション101上で稼働してもよい。サービス314は、パーティション101上の一意なサービス認証（SID）の下で稼働する。パーティション管理アカウント113によって認証されたサービスは、AuthServ群205にリストされたSIDを有する。開始時には、サービス314は、MP110にアクセスするクレデンシャルを有さなくてもよい。従って、サービス314は、クレデンシャルを求める要求を、メッセージキュー204を介して、帯域内通信203用認証デーモンへ送信する。メッセージキュー204は、要求の妥当性をAuthServ群205にリストされているSIDに基づいて決定する。AuthServ群205にリストされているSIDを有するサービスのみがMP110にアクセスして、クレデンシャルを求める要求をすることができる。また、メッセージキュー204は、AuthServ群205で定義されたファイルシステムの許可を実施でき

40

50

る。

【0017】

クレデンシャルを求める要求を受信すると、MP110は、パーティション101上のサービス314に対するクレデンシャルが存在するかを確認するよう検査する。クレデンシャルが存在する場合、MP110は、インタフェース109を介して帯域内通信用認証デーモン203にクレデンシャルを返す。次に、帯域内通信用認証デーモン203は、サービス314にクレデンシャルを戻す。クレデンシャルがその時点で存在しない場合、MP110は、要求を発するサービス314に対して特別に定義した役割を有するクレデンシャルを作成する。その特別な役割を、パーティション管理アカウント113によってAuthServ群205において定義し、MP110へのアクセス権を特にサービス314に合せて調整してもよい。従って管理者は、サービス314によるアクセスを、適宜必要な特権だけに限定してもよい。

10

【0018】

例示的な1実施形態では、特に、クレデンシャルはサービス314に対してMP110が発行するランダムで一意的なパスワードを含んでもよい。実施形態によっては、パスワードを例えば、サービスのSID、又はサービス314に対してMP110が作成した一意なアカウントと関連付けてもよい。MP110が、要求するサービスに対するアカウントを作成する場合、アカウント名をパスワードと共にサービスに戻す、或いはまた、サービス314はそのアカウント名としてSIDを使用してもよい。他の実施形態では、管理者が所望すれば、パスワードを、構成するパスワード長の要件に適合させてもよく、大文字及び小文字と数字の両方から構成してもよい。更に、実施形態によっては、特に、パスワード長の最小値（例えば、8文字以上）があってもよい。

20

【0019】

複数のパーティションを含む図3の別の実施形態では、サービスの個別のインスタンスを異なるパーティション上で稼働させてもよい。サービスの各個別のインスタンスは、サービスのホームパーティションに対して一意な個別のクレデンシャルを必要とするかも知れない。要求のソースパーティションを、認証及び認証プロセスの一部として、MP110に対して識別して、要求するサービスが認証されることを確実にして、要求発生元のパーティション上で稼働するようにしてもよい。SIDが要求するサービスに対して存在しない場合、一意なクレデンシャルを要求するサービスに対してMP110によって生成し、該クレデンシャルを使用して、要求するサービスからのMP110リソースを求める要求を認証してもよい。

30

【0020】

図4は、本開示の1実施形態によるMPリソースを求める要求をするサービス414を含む、図2の認証システムの図である。図4を参照すると、サービス414がMP110から帯域内通信用認証デーモン203を介してクレデンシャルを取得したなら、サービス414は帯域内通信チャンネル107で帯域内通信デーモン202及びインタフェース109を介してMP110と通信できる状態になる。帯域内通信チャンネル107又はデーモン202の実施形態では、基本的なHTTP認証をサポートしてもよい。サービス414がMP110への要求を開始すると、サービス414は、例えば、MP110からのSID及び／又は他のクレデンシャルを含む、認証情報を、HTTP基本認証の規定に沿った当該要求のHTTPヘッダの認証フィールドにセットしてもよい。認証フィールドの認証情報を使用して、サービス414を認証し、パーティション管理アカウント113においてサービスの役割に対して定義した許可を検査した後に、要求をMP110によって実行してもよい。認証システムの実施形態では、MP110から演算リソースを要求するサービス414のクレデンシャルを通過させ、認証する任意の適切な方法を使用してもよい。

40

【0021】

図5は、本開示の1実施形態によるパーティション上で稼働するサービスを認証する例示的な方法500について説明するフローチャートである。ブロック510では、サービスをパーティションにインストールする。その時点で、サービスを一意のSIDに割り当

50

てる。実施形態によっては、一意なサービスIDを管理者によって割り当ててもよい。ブロック520では、サービスの一意なSIDを、パーティションへのルートアクセスを有するエンティティによってパーティション上のAuthServ群に追加する。他の実施形態では、管理者によってSIDを加えてもよい。ブロック530では、サービスを開始する。ブロック540では、サービスは認証デーモンに接続してMPにクレデンシャルを求める要求をし、該要求を、メッセージキューを介して送信する。ブロック550では、メッセージキューにより、要求するサービスがリストされているかを確認するようにAuthServ群でリストされたSIDを検査する。ブロック560で、サービスがAuthServ群にリストされている場合に、メッセージキューはクレデンシャルを求める要求を、インタフェースを介して管理プロセッサに送信し、ブロック570で、管理プロセッサは、当該パーティション上の当該サービスに特定のクレデンシャルを作成する。その後、管理プロセッサは、ブロック580で、これらのクレデンシャルをインタフェースを介してサービスに返す。ブロック590でサービスは引き続き実行し、サービスはブロック570で発行したクレデンシャルを使用して、全要求を管理プロセッサに対して行う。管理プロセッサは、特定のパーティション上のサービスを一意に識別、認証し、また実施形態によっては、サービスのリソース要求をロギングしてもよい。

【0022】

実施形態によっては、特に、クレデンシャルの有効期限を認めてもよい。かかる実施形態では、指定した最長クレデンシャル存続期間より長期間に亘りサービスが再開しない場合、そのサービスのクレデンシャルは期限切れとなる。1実施形態では、特に、最長クレデンシャル存続期間を、管理者が指定してもよい。他の実施形態では、最長クレデンシャル存続期間を所定の値としてもよい。クレデンシャルの期限切れが発生した場合、サービスが行った管理プロセッサへの要求は失敗となる。失敗が期限切れクレデンシャルによるものである場合、サービスを再度認証デーモンに接続し、更新したクレデンシャルを要求する。サービスがAuthServ群にリストされている限り、新たなクレデンシャル要求は成功し、サービスは、更にユーザや管理者が介入せずに、新たに更新したクレデンシャルを自動的に受信する。

【0023】

本開示の実施形態を、ハードウェア、ソフトウェア、ファームウェア、又はそれらの組み合わせで実装できる。様々な実施形態では、システムの構成要素を、メモリに保存された適当な命令実行システムによって実行されるソフトウェア又はファームウェアに、実装する。実施形態によっては、ハードウェアで実装する場合、システムの構成要素を、当該技術分野で全て周知の以下の技術の何れか又は組合せで、実装でき、それらはデータ信号で論理機能を実装する論理ゲートを有する個々の論理回路、適切な組み合わせの論理ゲートを有する特定用途向け集積回路(ASIC)、プログラマブルゲートアレイ(PGA)、フィールドプログラマブルゲートアレイ(FPGA)等である。

【0024】

ソフトウェアコンポーネントは、論理関数を実装するための順序付けた実行可能命令のリストを含んでもよく、コンピュータベースのシステム、プロセッサ含有システム等の命令実行システム、装置又はデバイス、或いは命令実行システム、装置又はデバイスから命令をフェッチし、実行できる他のシステムによって、或いはそうしたシステムと接続して使用する任意のコンピュータ可読媒体でも具現化できる。更に、本開示の範囲には、ハードウェア又はソフトウェアで構成した媒体で具現化する論理で1つ又は複数の実施形態の機能を具現化することを含む。

【0025】

フローチャート中の処理に関する記述又はブロックについては、当該処理における特定の論理関数又はステップを実装する1つ又は複数の実行可能命令を含むコードのモジュール、セグメント又は部分を表すものとして理解すべきであり、本開示の当該技術分野にある程度熟達した者が理解するように、図示又は説明した機能の順序とは異なる、関連する機能に応じて略同時に又は逆順も含む順序で該実施形態の機能を実行してもよい別の実装

10

20

30

40

50

も、本開示の好適な実施形態の範囲に含む。

【 0 0 2 6 】

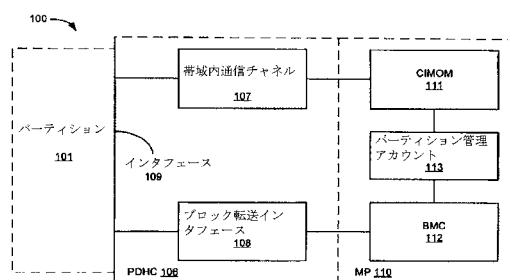
条件付き言語、特に「できる」、「する可能性がある」、「する場合がある」、又は「してもよい」等は、特に明記しない限り、或いは使用する文脈の中で別の意味に理解されない限り、特定の実施形態が、特定の特徴、要素及び／又はステップを含む可能性があるが、必須ではないこと、を一般的に伝えるものである。よって、こうした条件付き言語は、特徴、要素及び／又はステップが多少なりとも1つ又は複数の実施形態に必要であること、或いは1つ又は複数の実施形態は、ユーザの入力又はプロンプティングの有無にかかわらず、これらの特徴、要素及び／又はステップを含むか否か、或いは特定の実施形態において実施するか否かを決定する論理を必然的に含むことを、一般的に意味するものではない。

10

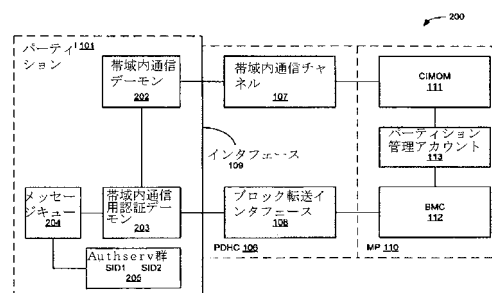
【 0 0 2 7 】

以上説明した本発明の実施形態は、単なる可能な実施例であり、本発明の原理を明確に理解するためだけに記載されたものであることを、強調すべきである。多くの変形例や変更例を、本発明の精神及び原理から実質的に逸脱せずに、本発明の上述した実施形態（複数可）に対して作成してもよい。かかる変更例及び変形例の全てを、本明細書では、本開示及び本発明の範囲内に含み、以下のクレームによって保護するものとする。

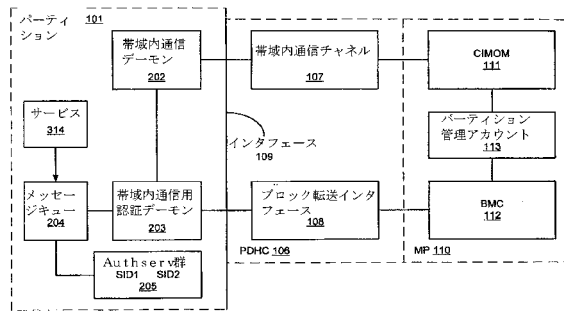
【图 1】



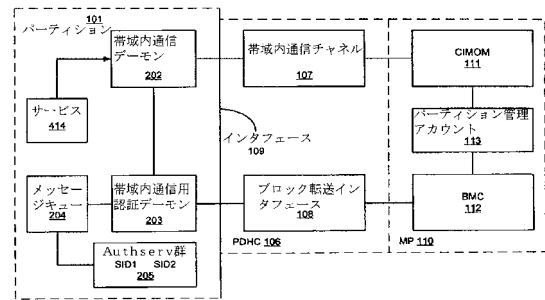
【图 2】



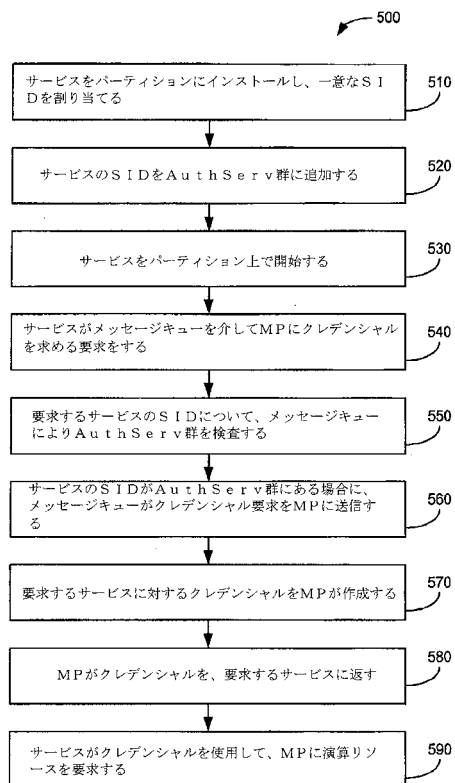
【図 3】



【図 4】



【図 5】



フロントページの続き

(74)代理人 100114591

弁理士 河村 英文

(72)発明者 オイラー, キース エス.

アメリカ合衆国 テキサス州 75080-1400, リチャードソン, ウォータービュー
パークウェイ 3000

(72)発明者 クレイグ, ラッセル オー.

アメリカ合衆国 コロラド州 80528-9544, フォート コリンズ, メイルストップ
42, 5L E8, イースト ハーモニー ロード 3404

審査官 木村 励

(56)参考文献 特開2005-056405 (JP, A)

特開2007-026442 (JP, A)

特表2008-500651 (JP, A)

米国特許出願公開第2005/0108395 (US, A1)

米国特許出願公開第2006/0149906 (US, A1)

米国特許出願公開第2008/0101276 (US, A1)

米国特許出願公開第2008/0250486 (US, A1)

(58)調査した分野(Int.Cl., DB名)

G06F 21/30 - 21/46

G06F 21/10 - 21/14