(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4550145号
(P4550145)

(45)発行日　平成22年9月22日(2010.9.22)　(24)登録日　平成22年7月16日(2010.7.16)

(51)Int.Cl.		F I		
H04L 12/66	(2006.01)	H04L	12/66	B
G06F 13/00	(2006.01)	G06F	13/00	351Z
G06F 21/20	(2006.01)	G06F	15/00	330A

請求項の数 19　(全 13 頁)

(21)出願番号	特願2008-541662 (P2008-541662)
(86)(22)出願日	平成18年7月17日 (2006.7.17)
(65)公表番号	特表2009-517900 (P2009-517900A)
(43)公表日	平成21年4月30日 (2009.4.30)
(86)国際出願番号	PCT/EP2006/064332
(87)国際公開番号	WO2007/060030
(87)国際公開日	平成19年5月31日 (2007.5.31)
審査請求日	平成21年3月25日 (2009.3.25)
(31)優先権主張番号	0524111.2
(32)優先日	平成17年11月26日 (2005.11.26)
(33)優先権主張国	英国 (GB)

早期審査対象出願

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(74)代理人　100108501
弁理士　上野　剛史
(74)代理人　100112690
弁理士　太佐　種一
(74)代理人　100091568
弁理士　市位　嘉宏

最終頁に続く

(54)【発明の名称】アクセス制御のための方法、装置、およびコンピュータ・プログラム

(57)【特許請求の範囲】

【請求項１】

公開／承認メッセージ・ブローカへのアクセスを制御するための方法であって、

前記メッセージ・ブローカにより提供される公開／承認機能を機能セットに分割するステップと、

各機能セットを通信経路と関連付けるステップと、

複数の通信経路の１つを介して前記メッセージ・ブローカに到来し、かつ前記メッセージ・ブローカにより提供される公開機能または承認機能へのアクセスを要求する要求を、前記メッセージ・ブローカで受信するステップと、

どの通信経路が使用されるかを判定するステップと、

前記要求される機能が、どの機能セットの一部分であるか識別するステップと、

前記識別された機能セットが、使用される前記通信経路と関連付けられているかどうかを判定するステップと、

前記識別された機能セットが、使用される前記通信経路と関連付けられていると判定されたのに応じて、前記要求される公開機能または承認機能へのアクセスを提供するステップと

を含む方法。

【請求項２】

どの通信経路が使用されるかを判定する前記ステップが、

前記メッセージ・ブローカにアクセスするために、どのポートが使用されるかを判定す

るステップを含み、また
前記識別された機能セットが、使用される前記通信経路と関連付けられているかどうか判定する前記ステップが、
前記識別された機能セットが、前記ブローカにアクセスするために使用される前記ポートと関連付けられているかどうか判定するステップを含む、請求項１に記載の方法。
【請求項３】
どの通信経路が使用されるかを判定する前記ステップが、
前記要求が生成された通信ネットワークを決定するステップを含み、また
前記識別された機能セットが、使用される前記通信経路と関連付けられているかどうかを判定する前記ステップが、
前記識別された機能セットが、前記要求が生成された前記通信ネットワークと関連付けられているかどうか判定するステップを含む、請求項１または２に記載の方法。
【請求項４】
前記要求が生成された前記通信ネットワークが、ネットワーク部分およびホスト部分を含むアドレスにより識別可能であり、また前記識別された機能セットが関連付けられている前記通信ネットワークがまた、少なくともネットワーク部分によって識別可能であり、さらに、前記識別された機能セットが、前記要求が生成された前記通信ネットワークと関連付けられているかどうか判定する前記ステップが、
前記要求が生成された前記通信ネットワークの前記ネットワーク部分を、前記識別された機能セットが関連付けられている前記通信ネットワークの前記ネットワーク部分と比較するステップを含む、請求項３に記載の方法。
【請求項５】
前記比較するステップが、
両方の通信ネットワークの前記ネットワーク部分が同じかどうか判定するために、サブネット・マスクを使用するステップを含む、請求項４に記載の方法。
【請求項６】
前記ブローカに接続するための要求が受信され、前記方法が、
前記接続要求に対する接続オブジェクトを作成するステップと、
前記接続オブジェクト内に含まれる情報を用いて、同じリクエスタからの任意の将来の要求がそれを介して到来する前記通信ネットワークを決定するステップとを含む、請求項１ないし５のいずれかに記載の方法。
【請求項７】
前記識別された機能セットが、使用される前記通信経路と関連付けられていないと判定されたことに応じて、前記要求を廃棄するステップを含む、請求項１ないし６のいずれかに記載の方法。
【請求項８】
前記要求が許容されなかったことを前記リクエスタに通知するステップを含む、請求項７に記載の方法。
【請求項９】
データベース機能を求める要求がそれを介して到来する前記通信経路に基づいて、データベースにより提供される機能へのアクセスを提供するステップを含む、請求項１ないし８のいずれかに記載の方法。
【請求項１０】
公開／承認メッセージ・ブローカへのアクセスを制御するための装置であって、
前記メッセージ・ブローカにより提供される公開／承認機能を機能セットに分割する手段と、
各機能セットを、通信経路と関連付ける手段と、
複数の通信経路の１つを介して前記メッセージ・ブローカに到来し、かつ前記メッセージ・ブローカにより提供される公開機能または承認機能へのアクセスを要求する要求を、前記メッセージ・ブローカで受信する手段と、

どの通信経路が使用されるかを判定する手段と、
前記要求される機能が、どの機能セットの一部分であるか識別する手段と、
前記識別された機能セットが、使用される前記通信経路と関連付けられているかどうかを判定する手段と、
前記識別された機能セットが、使用される前記通信経路と関連付けられていると判定されたのに応じて、前記要求される公開機能または承認機能へのアクセスを提供する手段とを備える装置。
【請求項１１】
どの通信経路が使用されるかを判定する前記手段が、
前記メッセージ・ブローカにアクセスするために、どのポートが使用されるかを判定する手段を備え、また
前記識別された機能セットが、使用される前記通信経路と関連付けられているかどうかを判定する前記手段が、
前記識別された機能セットが、前記ブローカにアクセスするために使用される前記ポートと関連付けられているかどうか判定する手段を備える、請求項１０に記載の装置。
【請求項１２】
どの通信経路が使用されるかを判定する前記手段が、
前記要求が生成された通信ネットワークを決定する手段を備え、また
前記識別された機能セットが、使用される前記通信経路と関連付けられているかどうかを判定する前記手段が、
前記識別された機能セットが、前記要求が生成された前記通信ネットワークと関連付けられているかどうか判定する手段を備える、請求項１０または１１に記載の装置。
【請求項１３】
前記要求が生成された前記通信ネットワークが、ネットワーク部分およびホスト部分を含むアドレスにより識別可能であり、また前記識別された機能セットが関連付けられている前記通信ネットワークがまた、少なくともネットワーク部分によって識別可能であり、さらに、前記識別された機能セットが、前記要求が生成された前記通信ネットワークと関連付けられているかどうか判定する手段が、
前記要求が生成された前記通信ネットワークの前記ネットワーク部分を、前記識別された機能セットが関連付けられている前記通信ネットワークの前記ネットワーク部分と比較する手段を備える、請求項１２に記載の装置。
【請求項１４】
前記比較する手段が、
両方の通信ネットワークの前記ネットワーク部分が同じかどうか判定するために、サブネット・マスクを使用する手段を備える、請求項１３に記載の装置。
【請求項１５】
前記ブローカに接続するための要求が受信され、前記装置が、
前記接続要求に対する接続オブジェクトを作成する手段と、
前記接続オブジェクト内に含まれる情報を用いて、同じリクエスタからの任意の将来の要求がそれを介して到来する前記通信ネットワークを決定する手段とを備える、請求項１０ないし１４のいずれかに記載の装置。
【請求項１６】
前記識別された機能セットが、使用される前記通信経路と関連付けられていないと判定されたことに応じて、前記要求を廃棄する手段を備える、請求項１０ないし１５のいずれかに記載の装置。
【請求項１７】
前記要求が許容されなかったことを前記リクエスタに通知する手段を備える、請求項１６に記載の装置。
【請求項１８】
データベース機能を求める要求がそれを介して到来する前記通信経路に基づいて、デー

タベースにより提供される機能へのアクセスを提供する手段を備える、請求項１０ないし１７のいずれかに記載の装置。

【請求項１９】

コンピュータ上で動作するとき、請求項１ないし９のいずれかの方法を実施するように適合されたプログラム・コード手段を備えるコンピュータ・プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明はアクセス制御に関する。

【背景技術】

【０００２】

サーバは、各ネットワークが特定タイプのデバイスをそのサーバに接続する２つ以上のネットワークに接続されることが多い。図１は、ＳＣＡＤＡ（監視制御データ収集）システム１０の一例を示す。デバイス３０、４０、および５０は、石油パイプライン２０に接続される。それらは、例えば、石油の流量および温度などの情報を監視する感知デバイスとすることができる。それらは、ネットワーク６０を介してメッセージ・ブローカ７０に情報を公開(publish)する。メッセージ・ブローカ７０は、第１のネットワーク・アダプタ・カードを介してこのネットワークに接続され、また第２のネットワーク・アダプタ・カードを介して、デバイス８０、８５、および９０を含む企業イントラネット９５にも接続される（アダプタ・カードはいずれも図に示されていない）。このようなデバイスは、公開するデバイスから情報を受信するように承認(subscribe)し、またこのような情報を使用して石油パイプラインのオペレーションを監視する。

【０００３】

図２に示すように、メッセージ・ブローカ７０は、いわゆる「非武装地帯」（ＤＭＺ）ネットワーク１００中に位置することができる。このゾーンは、外部ネットワーク（例えば、インターネット）と内部ネットワーク（例えば、企業イントラネット）の間の緩衝域として働く。外部および内部ネットワーク上のマシンは共に、ＤＭＺ内のサーバに接続されるが、ファイアウォール１１０、１２０により制御された特定のポートでのみ接続され得る。ＳＣＡＤＡアプリケーションに対して使用される公開／承認メッセージ・ブローカの場合では、インターネットから接続されるマシンは、例として、データを公開し、また企業イントラネットから接続されるマシンは、例として、その到来するデータを承認することができる。ブローカは、ブローカとそのサブスクライバの間で、事前に確立された接続を介してこのような情報を送信することになる。ＤＭＺは、インターネット接続されたマシンが、ＤＭＺ内のどのＩＰアドレスおよびポートに接続できるかを判定するパケット・フィルタ（ファイアウォール）１１０を入口に有することができる。メッセージ・ブローカと企業ネットワークの間にもまた、同様の設定１２０がある。

【０００４】

したがって、マシンとのトラフィックを規制するファイアウォールが既知であることを理解されたい。ファイアウォールは、数多くのタイプのものとすることができる。例えば、ネットワーク・レイヤのファイアウォールは、ソースもしくは宛先ＩＰアドレス、およびソースもしくは宛先ポート、ならびにプロトコル・タイプに基づいて、トラフィックをフィルタするように構成することができる。アプリケーション・レイヤのファイアウォールも知られており、これらは、特定のアプリケーションとのトラフィックをフィルタするために使用することができる。それらは、例えば、不適切なコンテンツがウェブ・ページで表示されるのを阻止するために使用することができる。

【０００５】

しかし、ファイアウォールは、完全なセキュリティ・ソリューションの一部に過ぎない。他のアクセス制御機構もまた、当技術分野でよく知られている。例えば、ＶＰＮ（仮想私設網）は、信頼されるユーザに一般のユーザには利用できない資源へのアクセスを提供する。公開／承認領域のＡＣＬ（アクセス制御リスト）は、特定のトピックに関してどの

ユーザが公開できるか、また特定のトピックをどのユーザが承認できるかを判定するために使用することができる。同様に、特定のマシンまたはアプリケーションへのアクセスは、特定のアクセス・ポートを介してのみ可能となり得る。

【０００６】

サーバが１つのネットワークだけを介してアクセスされる場合も、セキュリティがやはり問題になる。

【発明の開示】

【発明が解決しようとする課題】

【０００７】

１つのサーバが、異なるデバイスによってアクセスされる状況に対処する、改善されたセキュリティ機構が業界で求められている。サーバは、１つのネットワークだけに、あるいは複数のネットワークに接続され得るが、各ネットワーク上のデバイスは、そのサーバにアクセスしようと試みる。

【課題を解決するための手段】

【０００８】

第１の態様によると、公開／承認メッセージ・ブローカへのアクセスを制御するための方法が提供され、本方法は、

メッセージ・ブローカにより提供される公開／承認機能を機能セットに分割するステップと、

各機能セットを通信経路と関連付けるステップと、

複数の通信経路の１つを介してメッセージ・ブローカに到来し、かつメッセージ・ブローカにより提供される公開機能または承認機能へのアクセスを要求する要求を、メッセージ・ブローカで受信するステップと、

どの通信経路が使用されるかを判定するステップと、

要求された機能が、どの機能セットの一部分であるか識別するステップと、

識別された機能セットが、使用される通信経路と関連付けられているかどうかを判定するステップと、

識別された機能セットが、使用される通信経路と関連付けられていると判定されたのに応じて、要求される公開機能または承認機能へのアクセスを提供するステップと

を含む。

【０００９】

一実施形態では、メッセージ・ブローカにアクセスするために、どのポートが使用されるかが判定され、次いで、識別された機能セットが、ブローカにアクセスするために使用されるポートと関連付けられているかどうかが判定される。

【００１０】

一実施形態では、どの通信ネットワークから要求が生成されたかが判定され、次いで、識別された機能セットが、要求が生成された通信ネットワークと関連付けられているかどうかが判定される。

【００１１】

一実施形態では、要求が生成された通信ネットワークが、ネットワーク部分およびホスト部分を含むアドレスにより識別可能である。この実施形態では、識別された機能セットが関連付けられている通信ネットワークはまた、少なくともネットワーク部分によって識別可能である。識別された機能セットが、要求が生成された通信ネットワークと関連付けられているかどうか判定するために、要求が生成された通信ネットワークのネットワーク部分が、識別された機能セットが関連付けられている通信ネットワークのネットワーク部分と比較される。

【００１２】

一実施形態では、両方の通信ネットワークのネットワーク部分が同じかどうか判定するために、サブネット・マスクが使用される。

【００１３】

一実施形態では、ブローカに接続するための要求が受信される。これは、接続要求に対して接続オブジェクトが作成される結果となる。接続オブジェクト内に含まれる情報が次いで使用されて、同じリクエスタからの任意の将来の要求がそれを介して到来する通信ネットワークを決定する。

【００１４】

一実施形態では、識別された機能セットが、使用される通信経路と関連付けられていないと判定された場合、要求は廃棄される。リクエスタは、要求が許容されなかったことをリクエスタに通知することができる。

【００１５】

一実施形態では、データベース機能を求める要求がそれを介して到来する通信経路に基づいて、データベースにより提供される機能へのアクセスが提供される。

【００１６】

他の態様によると、公開／承認メッセージ・ブローカへのアクセスを制御するための装置が提供され、その装置は、

メッセージ・ブローカにより提供される公開／承認機能を機能セットへと分割する手段と、

各機能セットを、通信経路と関連付ける手段と、

複数の通信経路の１つを介してメッセージ・ブローカに到来し、かつメッセージ・ブローカにより提供される公開機能または承認機能へのアクセスを要求する要求を、メッセージ・ブローカで受信する手段と、

どの通信経路が使用されるかを判定する手段と、

要求される機能が、どの機能セットの一部分であるか識別する手段と、

識別された機能セットが、使用される通信経路と関連付けられているかどうかを判定する手段と、

識別された機能セットが、使用される通信経路と関連付けられていると判定されたのに応じて、要求された公開機能または承認機能へのアクセスを提供する手段と

を備える。

【００１７】

本発明は、コンピュータ・ソフトウェアで実施することができる。

【００１８】

本発明の好ましい実施形態を、例示のためだけであるが、添付の図面を参照して次に説明する。

【発明を実施するための最良の形態】

【００１９】

デバイスのネットワーク位置に基づいて、サーバにより提供される機能へのデバイス・アクセスを制御するための機構が開示される。

【００２０】

本発明は、図３から図１１を参照し、好ましい実施形態に従って説明する。図は、互いに関連させて読むべきである。

【００２１】

メッセージ・ブローカ７０により提供される何らかの機能を実施するための要求は、ステップ４００（図１０）で受信される。要求は、ブローカの接続ポート（例えば、ネットワーク９．２．ｘ．ｘ上のＩＰアドレス９．２．３．４を有するポート１８８３）で受信される。このような要求のフォーマットが図５に示されている。要求は、そのフォーマットに対して２つの部分を有する。すなわち、ネットワーク情報部分３００、および要求情報部分３１０である。部分３１０は、

ｉ）ユーザＩＤ

ｉｉ）メッセージ・ブローカで、ブローカ提供機能にマップする機能コード。このような機能は、コンポーネント２３０により提供される。

ｉｉｉ）メッセージ長さ

ｉｖ）ＱｏＳ（サービス品質）およびメッセージ優先順位などの情報に関係し得るフラグ
ｖ）メッセージ・トピック
ｖｉ）メッセージの主ペイロード
などの情報を含む。

【００２２】
ネットワーク情報部分３００は、
ｉ）ソースＩＰアドレス
ｉｉ）ソース・ポート
ｉｉｉ）宛先アドレス
ｉｖ）宛先ポート
ｖ）使用されるプロトコルの識別子（例えば、ＴＣＰまたはＵＤＰ）
などのより低いレベルの情報を含む。

【００２３】
これらのエレメントは、プロトコル・ヘッダの一部である。要求デバイスは、必ずしも、ブローカが接続されているネットワークと同じネットワーク上にある必要がなく、したがって、ＩＰソース・アドレスは、完全に異なるものであり得ることに留意されたい。

【００２４】
ステップ４１０で、新しく受信された要求が接続要求であると判定された場合、図６で示す接続オブジェクト３２０（本質的に、状態情報）を作成する（ステップ４２０で）ためには、ユーザＩＤと共にネットワーク情報が使用される。この接続オブジェクトは、受信接続ポートに記憶される。各接続オブジェクトはまた、それと関連付けられたソケットＩＤを有する。

【００２５】
いずれにしても、処理はステップ４３０に達し、接続ポートは、その要求をブローカ・インターフェース２２０への経路で（on its way to）送る。ブローカ・インターフェースは、ブローカ７０により提供される機能２３０に対するコールを行うために使用される。ステップ４４０で、要求は、インターセプタ２００により、具体的には、インターセプト・コンポーネント２７０により、ブローカ・インターフェースへの経路上でインターセプトされる。接続情報コンポーネント２４０は、ステップ４５０で、インターセプトされた要求に対する接続情報がローカルで利用できるかどうかを判定する。これが、現在の接続セッションに対して、この特定のクライアントから受ける最初の要求である場合、ローカルに利用可能な接続情報は何もないことになる。その場合、その要求が生成された接続ポートに、その要求に関連する接続オブジェクトを要求する（ステップ４６０）。受信された接続オブジェクトは、次いで、将来の要求で使用するために、インターセプタ・コンポーネントでローカルに記憶される（図示せず）。他の実施形態では、単に、接続情報を、要求ごとに接続ポートに要求することもできる。

【００２６】
ステップ４７０で、要求されたオペレーションが、特定の要求デバイスに対して許可されるかどうか判定するために、（図７および図８で示された）ユーザ・プロファイルおよび機能テーブル情報３３０、３４０が（照会コンポーネント２５０を用いて）照会される。

【００２７】
機能テーブル３３０は、コンポーネント２３０（図３）によって提供されるブローカ機能を一覧表示する。したがって、デバイスは、例示のためだけであるが、以下のオペレーションを要求することができる。
ｉ）接続する
ｉｉ）切断する
ｉｉｉ）公開する
ｉｖ）ａｃｋを公開する（Ｐｕｂｌｉｓｈ＿ａｃｋ）（サブスクライバがメッセージの

受領を確認応答することができる）
ｖ）リリースを公開する（Ｐｕｂｌｉｓｈ＿ｒｅｌｅａｓｅ）（パブリッシャは、一度限りのメッセージをリリースすることができる）
ｖｉ）完了を公開する（Ｐｕｂｌｉｓｈ＿ｃｏｍｐｌｅｔｅ）（サブスクライバは、一度限りのメッセージの完了を確認することができる）
ｖｉｉ）承認する
【００２８】
要求メッセージの機能コードはそれぞれ、上記オペレーションの１つに対して、テーブルによりマップされる。
【００２９】
デバイスは、任意の機能を要求することができるが、好ましい実施形態によれば、デバイスのネットワーク位置が、要求されたオペレーションをブローカが実際に実行するかどうかに対して影響を与える。機能テーブル３３０の第３列は、各オペレーションに対して許可されたユーザのユーザ・プロファイルを示す。したがって、タイプ２のユーザだけがメッセージを公開することができるが、一方、タイプ１のユーザだけが承認オペレーションを要求することができる。したがって、事実上、メッセージ・ブローカのアプリケーション機能は、特定タイプのユーザだけが各機能セットへのアクセス権を有する機能セットに分割される。これは、図９でベン図により示される。この図から、以下の機能が、機能セット１の一部であることが分かるはずである。
ｉ）ａｃｋを公開する（Ｐｕｂｌｉｓｈ＿ａｃｋ）
ｉｉ）完了を公開する（Ｐｕｂｌｉｓｈ＿ｃｏｍｐｌｅｔｅ）
ｉｉｉ）承認する
ｉｖ）接続する
ｖ）切断する
【００３０】
機能セット２には以下のものがある。
ｉ）公開する
ｉｉ）リリースを公開する（Ｐｕｂｌｉｓｈ＿ｒｅｌｅａｓｅ）
ｉｉｉ）接続する
ｉｖ）切断する
【００３１】
２つの機能セットだけが示されており、また各セットには複数の機能があるが、これはそうである必要はない。２を超える機能セットとすることができる。さらに、機能セットは１つの機能を有するだけでもよい。
【００３２】
ユーザ・プロファイル・テーブル３４０は、タイプ２のユーザと比較したとき、タイプ１のユーザが何を意味するかを定義する。図のテーブルは、要求デバイスがブローカにより提供される機能にアクセスできるかどうかを判定する場合、関連する情報が、指定されたＮｅｔ　ＩＤ（ネットワークＩＤ）／サブネット・マスクの対と、ブローカがそれを介してアクセスされる宛先ポートと、要求ユーザ名とであることを定義している。ユーザ・プロファイル中のいくつかのエントリは、ワイルドカード化され得ることが、図から理解できる。言い換えると、プロファイル１のユーザが誰であるかは問題ではない。
【００３３】
図１１の処理に戻って参照すると、照会コンポーネント２５０は、インターセプトされたメッセージの要求情報部分から機能コードを抽出する。これは、ユーザから要求されるオペレーション、およびこのようなオペレーションを実施することが許可されるユーザ・タイプを、機能テーブル３３０から決定するために使用される。例として、機能７が要求される。これは、機能テーブル中で、タイプ１のユーザだけに許可される公開オペレーションにマップされている。次いで、プロファイル・テーブル３４０がアクセスされて、タイプ１のユーザに必要な特性が決定される。論理的なＡＮＤ演算が、要求のソースＩＰア

ドレス（例えば、１０．０．５６．７７）とサブネット・マスク（例えば、２５５．２５５．０．０）の間で行われる。ＩＰアドレスは、通常、Ｎｅｔ　ＩＤ（すなわち、ネットワーク部分）およびノードＩＤ（すなわち、ホスト／マシン部分）から構成される。ＡＮＤ演算が実施されて、ソースＩＰアドレスからＮｅｔ　ＩＤ部分（この場合１０．０）が抽出される。次いで、それを、プロファイル中で指定されたＮｅｔ　ＩＤと比較することができる。（フル・アドレスである１０．０．０．０をプロファイル中で指定することもできるが、この実施形態での関連する（Ｎｅｔ　ＩＤ）部分は１０．０であり、代替の実施形態では、ネットワーク部分だけがプロファイル中で指定されることに留意されたい。）ソースＩＰアドレスから抽出されたＮｅｔ　ＩＤが、プロファイル中で指定されたＮｅｔ　ＩＤ部分に一致する場合、プロファイルのこの部分はマッチされる。言い換えると、要求は、適切なサブネットから来ている。この例ではマッチがあり、その結果、適切なＩＰアドレス範囲から要求が来ていることになる。しかし、特定のポートを介してブローカにアクセスすることが必要になる可能性もあるが、その場合もやはり、これが検査される。ステップ４６０で要求された接続オブジェクトは（すでに、よりローカルに利用可能でなければ）、要求ソースＩＰアドレス、宛先ポートなどを決定するのに使用できることに留意されたい。したがって、テーブル中の各列に対して、関連する接続オブジェクトから値を取得することができる。いくつかの自動化されたルールを適用することができる。例えば、ユーザ名フィールドは、その中にワイルドカードを有する。その結果、接続オブジェクトからこの値を取得する必要がなくなる。同様に、ソースＩＰアドレスが取得され、デバイスがこの特性を満たしていないと判定された場合、他の列に対して値を取得する必要はなくなる。

【００３４】

ユーザ・プロファイル・テーブルの列は、例示のためだけに過ぎないことに留意されたい。重要な点は、アプリケーション機能へのユーザのアクセスが、ユーザのネットワーク位置に関連する１つまたは複数の特性に基づいて制御されていることである。

【００３５】

要求メッセージ、したがって、要求メッセージから作成される接続オブジェクトは、ソースＩＰアドレスが、ユーザ・プロファイル中で指定されるＮｅｔ　ＩＤとサブネット・マスクの組合せにより定義される範囲内に含まれるかどうかを指定しないことが図５および図６から理解されよう。しかし、その要求のソースＩＰアドレスと、指定されたＮｅｔ　ＩＤ／サブネットの組合せの比較は、それがその範囲に存在するかどうかを判定することになる（上記を参照）。サブネットおよびサブネット・マスクは、当技術分野ですでによく知られたトピックであり、したがって、本明細書で詳細をさらに述べないものとする。

【００３６】

照会ステップ４７０から得られた情報は、ゲート・キーパ２６０に渡される。言い換えると、要求が必要な基準を満たしているかどうかにかかわらず渡される。ゲート・キーパ２６０は、次いで、このような情報を用いて、要求が許容可能であるかどうか判定する（ステップ４８０）。要求が必要な基準を満たしていなかった場合（例えば、要求が、関連するプロファイル情報中で指定されたものとは異なるサブネットから生成されている場合）、ステップ４９０で要求は廃棄される。これは、要求が単に実行されないことを意味することもできるが、より一般的に、要求が許容されていないことを要求デバイスに通知することを含むこともできる。

【００３７】

他方で、ステップ４８０で、要求が許容可能であると見なされた場合、ゲート・キーパ２６０は、要求をブローカ・インターフェース２２０に渡し、それを介して、適切なオペレーション（この例では、公開）を要求することができる。これ以降、メッセージ・ブローカの機能は、当技術分野でよく知られた方法で動作する。

【００３８】

要約すると、サーバのアプリケーション・レベルのプロトコルは、機能によりセットへ

とセグメント化される。これらのセットのそれぞれは、次いで、この機能セットにアクセスするための要件を記述するプロファイルと関連付けられる。図１の例に戻って参照すると、このような発明は、ＳＣＡＤＡタイプの環境で非常に効果的に使用することができる。繰り返すと、このような環境では、センサは外部ネットワークを介してメッセージ・ブローカにアクセスできるが、一方、モニタは内部ネットワークを介してメッセージ・ブローカにアクセスすることができる。このような設定では、モニタに公開させること、および情報を受信するようにセンサに承認させることは望ましくない可能性がある。すべてのデバイスのユーザＩＤおよびそのアクセス許可を一覧表示にする必要があるのではなく、要求デバイスのネットワーク位置に基づくことにより、アクセス制御を実施することが可能になる。

【００３９】

上記で示したように、アクセス制御の実施において、ソースＩＰアドレス、サブネット、宛先ポート、およびユーザＩＤ情報の使用は、例示的なものに過ぎない。例えば、それ自体の宛先ポートを使用することができる。その場合、本発明の機能は、ファイアウォール技術（例えば、図２のパケット・フィルタ１１０、１２０）中に構築され得る。現在のファイアウォールを使用してポート・アクセスを制限することはすでに知られている。しかし、このようなファイアウォール技術は、特定のポートを介して要求できるオペレーション・タイプを指定するように拡張され得る。

【００４０】

最後に、上述の実施形態は、２つ以上のネットワークに接続されたサーバに関して参照を行っているが、本発明はそのように限定されることはない。例えば、デバイスは、単一のネットワークを介してサーバにアクセスすることができる。サーバは、単一のネットワーク上の複数のポートで待ち受ける（listen）ことができる。ファイアウォールを、どのソースＩＰアドレス範囲が、サーバ上のどのポートにアクセスすることが許容されているかを制御するために使用することができ、その場合、照会コンポーネントは、その意志決定において、ポート番号を検討する必要があるだけである。代替的には、ソースＩＰアドレス範囲およびポートをプロファイル中で指定することもでき、また照会コンポーネントは、妥当性検証を行うこともできる。

【図面の簡単な説明】

【００４１】

【図１】従来技術による、外部と内部ネットワークの両方に接続されたサーバを示す図である。

【図２】従来技術による、非武装地帯（ＤＭＺ）ネットワーク中に位置する図１のサーバを示す図である。

【図３】好ましい実施形態による、本発明の構成部品を示す図である。

【図４】好ましい実施形態による、本発明の構成部品を示す図である。

【図５】本発明の好ましい実施形態による、図１のサーバで受信されるメッセージのフォーマットを示す図である。

【図６】本発明の好ましい実施形態による、デバイスが図１のサーバに接続されたときに作成される接続オブジェクトのフォーマットを示す図である。

【図７】本発明の好ましい実施形態による、ユーザ・プロファイルに、サーバのアプリケーション機能をマッピングした表形式の情報を示す図である。

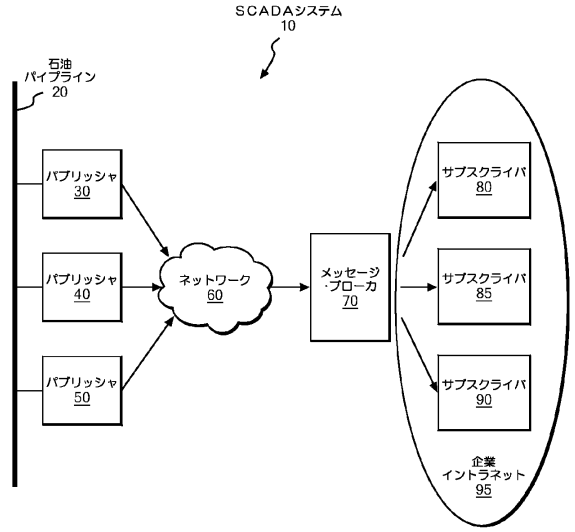
【図８】本発明の好ましい実施形態による、ユーザ・プロファイルに、サーバのアプリケーション機能をマッピングした表形式の情報を示す図である。

【図９】例示的な実施形態で提供される機能セットのベン図である。

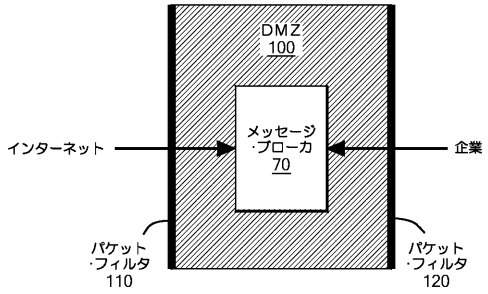
【図１０】好ましい実施形態による本発明の処理を示す図である。

【図１１】好ましい実施形態による本発明の処理を示す図である。

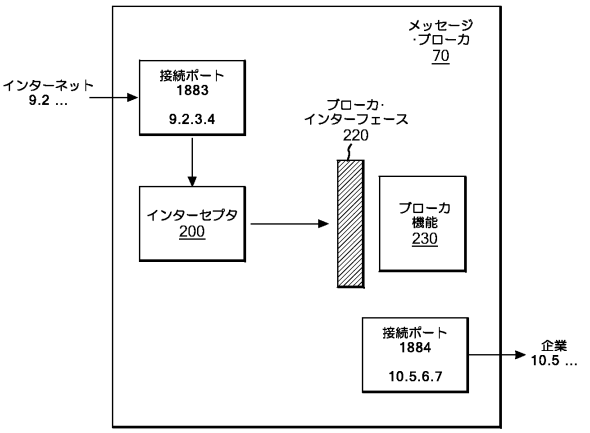
【図１】



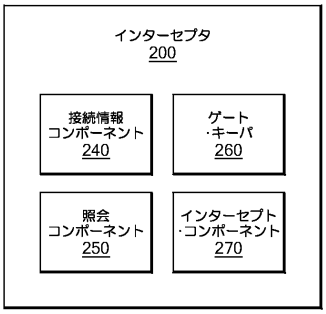
【図２】



【図３】

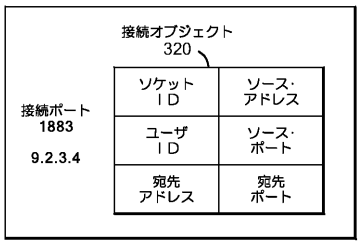


【図４】



【図５】

【図６】



【図７】

機能テーブル 330

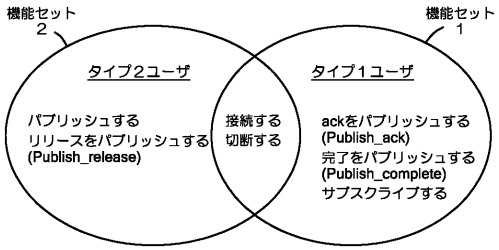
機能コード	機能	ユーザ・タイプ
1	接続する	1, 2
2	切断する	1, 2
3	パブリッシュする	2
4	ackをパブリッシュする (Puback)	1
5	リリースをパブリッシュする (Pubrel)	2
6	完了をパブリッシュする (Pubcomp)	1
7	サブスクライブする	1

【図８】

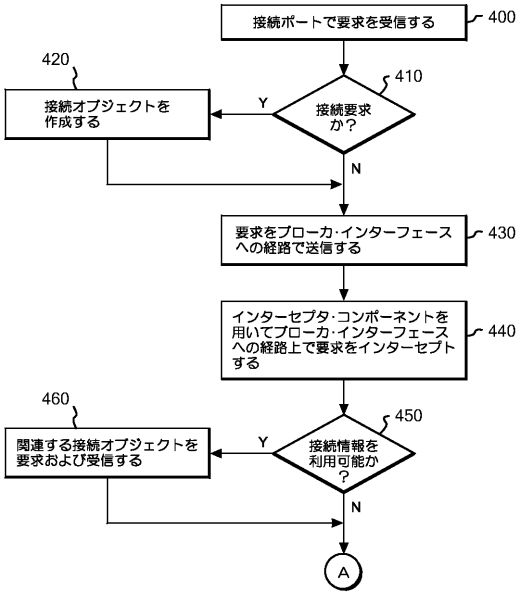
ユーザ・プロファイル・テーブル 340

プロファイル	ネット ＩＤ	サブネット ・マスク	宛先 ポート	ユーザ名
1	1.0.0.0.0	255.255.0.0	1884	*
2	*	*	1883	*

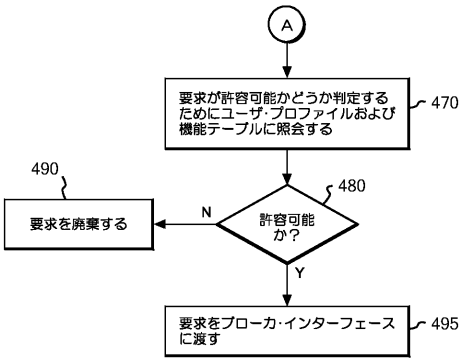
【図９】



【図１０】



【図１１】



フロントページの続き

(74)代理人 100086243
弁理士 坂口 博
(72)発明者 アップルビー リチャード マーク
イギリス国 ＳＯ３１ ９ＪＥ ウォーサッシ・ハンプシャー ウォーサッシ・ロード ハイフィールドズ
(72)発明者 スタンフォードクラーク アンドリュー ジェームズ
イギリス国 ＰＯ３８ ２ＬＪ ワイト島 チャール サウスダウン・レーン ダウンエンド・コテッジ

審査官 安藤 一道

(56)参考文献 英国特許出願公開第２３６３２９７（ＧＢ，Ａ）
J.Rosenberg,H.Schulzrinne, SIP For Presence, draft-rosenberg-sip-pip-00.txt, IETF INTERNET DRAFT, １９９８年１１月１３日

(58)調査した分野(Int.Cl., ＤＢ名)
H04L 12/66
G06F 13/00
G06F 21/20