(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2007-287148
(P2007-287148A)
(43)公開日　平成19年11月1日(2007.11.1)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330A	5B017
G06F 15/00	(2006.01)	G06F	15/00	ZEC	5B285
G06F 21/24	(2006.01)	G06F	12/14	520C	5J104
H04L 9/32	(2006.01)	H04L	9/00	673A	

審査請求 未請求　請求項の数 20　ＯＬ　（全 25 頁）

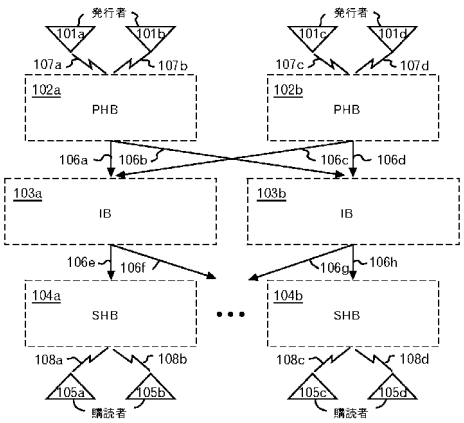
(21)出願番号　特願2007-103883 (P2007-103883)
(22)出願日　平成19年4月11日 (2007.4.11)
(31)優先権主張番号　11/402685
(32)優先日　平成18年4月12日 (2006.4.12)
(33)優先権主張国　米国 (US)

(71)出願人　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】配送保証されるコンテンツベースのパブリッシュ／サブスクライブ・システムの動的アクセス制御

(57)【要約】
【課題】コンテンツベースのパブリッシュ／サブスクライブ・システムなどの分散メッセージング・システムの改良されたアクセス制御技術を開示する。
【解決手段】例えば、メッセージを発行側クライアントから購読側クライアントに複数のブローカーを介して配送するコンテンツベースのパブリッシュ／サブスクライブ・システムのアクセス制御を提供する方法は、次のステップ／操作を含む。アクセス制御ポリシーのひとつまたは複数の変更を指定する。ひとつまたは複数の変更にアクセス制御バージョン識別子を対応付ける。ひとつまたは複数の変更を、ひとつまたは複数の変更により影響を受ける発行側クライアントまたは購読側クライアントと対応する複数のブローカーのうちのひとつまたは複数のブローカーに送る。ひとつまたは複数の変更と対応付けられたアクセス制御バージョン識別子を複数のブローカーの各々に送る。
【選択図】図１



【特許請求の範囲】
【請求項１】
メッセージを発行側クライアントから購読側クライアントに複数のブローカを介して配送するコンテンツベースのパブリッシュ・システムまたはサブスクライブ・システムのいずれかにおいてアクセス制御を提供する方法であって、
アクセス制御ポリシーのひとつまたは複数の変更を指定するステップと、
前記ひとつまたは複数の変更にアクセス制御バージョン識別子を対応付けるステップと、
前記ひとつまたは複数の変更を、前記ひとつまたは複数の変更により影響を受ける発行側クライアントまたは購読側クライアントに対応する前記複数のブローカのうちひとつまたは複数のブローカに送るステップと、
前記複数のブローカの各々に、前記ひとつまたは複数の変更に対応する前記アクセス制御バージョン識別子を送るステップと、を有する方法。
【請求項２】
既存のアクセス制御ポリシーの前記ひとつまたは複数の変更の各々を、前記アクセス制御バージョン識別子に対応付けて、バッチとしてシステムに格納および実装することによって、前記ひとつまたは複数の変更をシステムの前記既存のアクセス制御ポリシーのひとつまたは複数の過去の変更とは一意的に識別する、請求項１の方法。
【請求項３】
前記複数のブローカの各々が発行者ホスティング・ブローカ（ＰＨＢ）、購読者ホスティング・ブローカ（ＳＨＢ）、および中間ブローカ（ＩＢ）のうちの少なくとも１つであり、前記指定するステップ、前記対応付けるステップ、および前記送るステップをセキュリティ・アドミニストレータに従って行う、請求項１の方法。
【請求項４】
前記セキュリティ・アドミニストレータが前記ひとつまたは複数の変更および前記対応するアクセス制御バージョン識別子を、前記ひとつまたは複数の変更により影響を受ける発行側クライアントまたは購読側クライアントに対応するＰＨＢおよびＳＨＢに送る、請求項３の方法。
【請求項５】
ＳＨＢが、前記ひとつまたは複数の変更を受け取った際、その影響を受けるクライアントの制限付きのサブスクリプションを計算する、請求項３の方法。
【請求項６】
前記ＳＨＢが制限付きのサブスクリプションを前記アクセス制御番号とともにひとつまたは複数の他のブローカに送る、請求項５の方法。
【請求項７】
ＰＨＢが、前記ひとつまたは複数の変更を受け取った際、前記ひとつまたは複数の変更を前記アクセス制御ポリシーに適用して、最新の発行権および前記アクセス制御バージョン識別子を取得するステップと、
発行されるデータ・メッセージを受け取った際、前記最新の発行権を前記メッセージに適用するステップのうち、少なくとも１つのステップを行う、請求項３の方法。
【請求項８】
前記ＰＨＢが前記データ・メッセージを前記アクセス制御番号とともにひとつまたは複数の他のブローカに送る、請求項７の方法。
【請求項９】
ＩＢが制御バージョン・ベクトルを維持する、請求項３の方法。
【請求項１０】
メッセージを発行側クライアントから購読側クライアントに複数のブローカを介して配送するコンテンツベースのパブリッシュ・システムまたはサブスクライブ・システムのいずれかにおいてアクセス制御を提供する装置であって、
メモリと、

メモリに連結されて、（ｉ）アクセス制御ポリシーのひとつまたは複数の変更を指定する、（ｉｉ）前記ひとつまたは複数の変更にアクセス制御バージョン識別子を対応付ける、（ｉｉｉ）前記ひとつまたは複数の変更を、前記ひとつまたは複数の変更により影響を受ける発行側クライアントまたは購読側クライアントに対応する前記複数のブローカのうちのひとつまたは複数のブローカに送る、および（ｉｖ）前記ひとつまたは複数の変更に対応付けられる前記アクセス制御バージョン識別子を前記複数のブローカの各々に送る、ように作動する少なくとも１つのプロセッサと、を有する装置。

【請求項１１】

発行側クライアントから購読側クライアントにメッセージ配送を提供するコンテンツベースのパブリッシュ／サブスクライブ・システムであって、

ネットワークを介して互いに作動的に連結される複数のブローカで、前記ブローカの各々が発行者ホスティング・ブローカ（ＰＨＢ）、購読者ホスティング・ブローカ（ＳＨＢ）、および中間ブローカ（ＩＢ）のうち少なくとも１つとして構成される、前記複数のブローカと、

前記複数のブローカの少なくとも一部に作動的に連結され、システム内の少なくとも１つのアクセス制御ポリシーを格納および更新するように構成される少なくとも１つのアドミニストレータとを有し、

前記複数のブローカの少なくとも一部、および少なくとも１つのアドミニストレータが、間にひとつまたは複数のメッセージを挟んで送るアクセス制御バージョン識別子を含むことによってシステム内に前記アクセス制御ポリシーの変更を実装するように構成され、前記アクセス制御識別子が有効な前記アクセス制御ポリシーを一意的に識別して、前記アクセス制御ポリシーの前記変更を、前記アクセス制御ポリシーの前記変更により影響を受けるひとつまたは複数のプリンシパルに対応する発行側クライアントおよび購読側クライアントに確定的かつ統一的に適用する、コンテンツベースのパブリッシュ／サブスクライブ・システム。

【請求項１２】

前記複数のブローカが、前記ＰＨＢ以外のブローカでアクセス制御状態の永続ストレージの必要性をなくすように構成される、請求項１１のシステム。

【請求項１３】

少なくとも１つのＰＨＢが、最新のアクセス制御ポリシーに対応付ける前記制御バージョン識別子を永続的に格納するように構成される、請求項１１のシステム。

【請求項１４】

少なくとも１つのＰＨＢが、メッセージが発行された時点で有効であったアクセス制御ポリシーに対応付けるアクセス制御バージョン識別子を永続的に格納するように構成される、請求項１３のシステム。

【請求項１５】

ＰＨＢとＳＨＢの間に多重パスが存在し、別のパスにあるＩＢが同一のアクセス制御状態を維持する必要がない、請求項１１のシステム。

【請求項１６】

前記ＩＢの少なくとも一部が、アクセス制御ルールを維持するのではなく、１つのＳＨＢにつき１バージョンで、アクセス制御バージョン・ベクトルを維持する、請求項１１のシステム。

【請求項１７】

各ＳＨＢがそれに接続されるプリンシパルの最新のアクセス制御ルールを維持する、請求項１１のシステム。

【請求項１８】

（ｉ）ＳＨＢがそれに接続されるプリンシパルのアクセス制御ルールの変更を購読依頼し、（ｉｉ）ＩＢがプリンシパルごとにアクセス制御ルールの変更をフィルタリングし、（ｉｉｉ）高信頼性配送を使用して、アクセス制御ルールの変更がそれを必要とする前記ＳＨＢで確実に受け取れるようにし、（ｉｖ）新しいプリンシパルからの接続を受け入れる

ＳＨＢが要求応答プロトコルを使用して、当該プリンシパルの前記アクセス制御ルールを初期化する、請求項１１のシステム。
【請求項１９】
（ｉ）ＳＨＢがサブスクリプションと前記最新のアクセス制御ルールとの論理積を求めて、前記論理積を求めたサブスクリプションの前記制御バージョンを前記制御ルールの前記バージョンを使用して割り当て、維持し、（ｉｉ）前記ＳＨＢが前記アクセス制御バージョン識別子をもつ求めたサブスクリプションを上流のＩＢに伝搬し、および（ｉｉｉ）ＩＢがサブスクリプション状態をアクセス制御バージョン識別子で維持する、請求項１８のシステム。
【請求項２０】
（ｉ）ＰＨＢがデータ・メッセージに前記アクセス制御バージョン識別子を含め、（ｉｉ）ＩＢがサブスクリプション状態を使用して、前記データ・メッセージに含めた前記アクセス制御バージョン識別子が前記サブスクリプション状態の前記アクセス制御バージョン番号以下である場合に前記メッセージをフィルタリングし、そうでなければ前記メッセージを下流に送り、（ｉｉｉ）ＳＨＢがメッセージと一致する論理積を求めたサブスクリプションの制御バージョン識別子とメッセージの制御バージョンが等しいかを点検して、購読アクセス制御ルールを施行する、請求項１９のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本出願は、一般的に分散メッセージング・システムに関係し、さらに具体的には当該システムのアクセス制御技術に関係する。
【背景技術】
【０００２】
非同期分散アプリケーションと併用する分散メッセージング・システムで採用される一般に普及したアプローチは、コンテンツベースのパブリッシュ／サブスクライブ（ｐｕｂ／ｓｕｂ）メッセージング・アプローチである。コンテンツベースのｐｕｂ／ｓｕｂシステムは、メッセージを発行する発行側クライアント・デバイスまたはマシン（「発行者」）と、そのサブスクリプションで指定される述語／ブール型フィルタと一致するメッセージへの関心を登録する購読側クライアント・デバイスまたはマシン（「購読者」）を含む。このシステムは発行されるメッセージを関心を寄せる購読者全員に確実にタイムリーに配送し、典型的にはこのためのルーティング・ブローカ・デバイスまたはマシン（「ブローカ」）を含む。こうして、コンテンツベースのｐｕｂ／ｓｕｂパラダイムにおいては、発行者がそのメッセージを受け取る購読者を知る必要がなく、また購読者も受け取るメッセージの発信者を知る必要がないため、情報提供者（すなわち、発行者）と消費者（すなわち、購読者）が切り離される。
【０００３】
多くのアプリケーションでは、コンテンツベースのｐｕｂ／ｓｕｂシステムはしっかりしたサービス保証（高信頼性、順序のある、ギャップレス配送など）、多数のクライアントをサポートする高いスケーラビリティ、高いサービス可用性、高い性能／処理能力を提供することが求められる。以上の目標を達成するために、典型的なシステムは、（１）サブスクリプション情報を発行者に向けて伝搬、統合する、（２）サブスクリプション情報を使って、コンテンツのフィルタリングを行い、ネットワーク帯域幅の有効利用と良好なスケーラビリティを達成する、（３）サービス可用性を高めるために冗長ネットワーク・パスを利用する。
【０００４】
ｐｕｂ／ｓｕｂシステムの商業的な採用の妨げとなりうる重要な割に軽視されることの多い問題が、アプリケーションに提供されるセキュリティ保証である。特に、アプリケーションは配布されるときにイベントの機密性、完全性、真正性を確保したいと考える。信頼できる発信元だけにイベントの発行を認め、許可された購読者もしくは料金を支払う購

読者だけに情報／イベントを配信することを求められることが多い。利用に基づいた購読者への請求決済を可能にする会計および監査についての問題が密接に関係している。
【特許文献１】米国特許出願番号第１０／１７７，４７４号「Ｇａｐｌｅｓｓ Ｄｅｌｉｖｅｒｙ ａｎｄ Ｄｕｒａｂｌｅ Ｓｕｂｓｃｒｉｐｔｉｏｎｓ ｉｎ ａ Ｃｏｎｔｅｎｔ－Ｂａｓｅｄ Ｐｕｂｌｉｓｈ／Ｓｕｂｓｃｒｉｂｅ Ｓｙｓｔｅｍ」２００２年６月２１日出願
【非特許文献１】Ｙ．Ｚｈａｏ（Ｙ．チャオ）ら、Ａ Ｇｅｎｅｒａｌ Ａｌｇｏｒｉｔｈｍｉｃ Ｍｏｄｅｌ ｆｏｒ Ｓｕｂｓｃｒｉｐｔｉｏｎ Ｐｒｏｐａｇａｔｉｏｎ ａｎｄ Ｃｏｎｔｅｎｔ－ｂａｓｅｄ Ｒｏｕｔｉｎｇ ｗｉｔｈ Ｄｅｌｉｖｅｒｙ Ｇｕａｒａｎｔｅｅｓ、ＲＣ２３６６９、ＩＢＭ Ｒｅｓｅａｒｃｈ ２００５年
【非特許文献２】Ｙ．Ｚｈａｏ（Ｙ．チャオ）ら、Ｓｕｂｓｃｒｉｐｔｉｏｎ Ｐｒｏｐａｇａｔｉｏｎ ｉｎ Ｈｉｇｈｌｙ－ａｖａｉｌａｂｌｅ Ｐｕｂｌｉｓｈ／Ｓｕｂｓｃｒｉｂｅ Ｍｉｄｄｌｅｗａｒｅ、 ＡＣＭ／ＩＦＩＰ／ＵＳＥＮＩＸ、第５回国際ミドルウェア会議２００５年
【発明の開示】
【発明が解決しようとする課題】
【０００５】
ｐｕｂ／ｓｕｂシステムにおけるこのアクセス制御の問題は、アクセス制御ポリシーの変更という問題でさらに複雑になる。アクセス制御ポリシーの変更に伴うひとつの問題が、変更を行ったときに発生するｐｕｂ／ｓｕｂサービスの中断である。
【０００６】
従って、アクセス制御ポリシーの変更に効率的かつ効果的に役割を担うことのできる分散メッセージング・システムのアクセス制御技術の改良が必要である。
【課題を解決するための手段】
【０００７】
本発明の原理は、コンテンツベースのパブリッシュ／サブスクライブ・システムなどの分散メッセージング・システムに改良されたアクセス制御技術を提供する。
【０００８】
例えば、本発明のある側面では、メッセージを複数のブローカを介して発行側クライアントから購読側クライアントに配送するコンテンツベースのパブリッシュ／サブスクライブ・システムにおけるアクセス制御を提供する方法は、次のステップ／操作を含む。アクセス制御ポリシーのひとつまたは複数の変更を指定する。アクセス制御バージョン識別子をひとつまたは複数の変更に対応付ける。ひとつまたは複数の変更を該ひとつまたは複数の変更により影響を受ける発行側クライアントもしくは購読側クライアントに対応する複数のブローカのうちひとつまたは複数のブローカに送る。ひとつまたは複数の変更に対応するアクセス制御バージョン識別子を複数のブローカの各々に送る。ある実施例では、アクセス制御バージョン識別子は数字である。
【０００９】
既存のアクセス制御ポリシーのひとつまたは複数の変更の各々は、それにアクセス制御バージョン識別子を対応付けるとともに、バッチとしてシステムに格納および実装され、ひとつまたは複数の変更を、システムの既存のアクセス制御ポリシーのひとつまたは複数の過去の変更とは一意的に識別できるようにしてもよい。
【００１０】
複数のブローカの各々は、発行者ホスティング・ブローカ（ＰＨＢ）、購読者ホスティング・ブローカ（ＳＨＢ）、および中間ブローカ（ＩＢ）のうちの少なくとも１つでよく、上記指定する、対応付ける、および送る各ステップをセキュリティ・アドミニストレータに従って行う。
【００１１】
セキュリティ・アドミニストレータはひとつまたは複数の変更および対応のアクセス制御バージョン識別子を、ひとつまたは複数の変更により影響を受ける発行側クライアント

もしくは購読側クライアントに対応付けられたＰＨＢおよびＳＨＢに送ることができる。
【００１２】
ＳＨＢは、ひとつまたは複数の変更を受け取った際、その対象となるクライアントに関し制限付きのサブスクリプションを計算できる。それからＳＨＢは制限付きのサブスクリプションをアクセス制御番号とともにひとつまたは複数の他のブローカに送ることができる。
【００１３】
ＰＨＢは、ひとつまたは複数の変更を受け取った際、ひとつまたは複数の変更をアクセス制御ポリシーに適用して、最新の発行権およびアクセス制御バージョン識別子を取得できる。また、ＰＨＢは、発行されるデータ・メッセージを受け取った際、最新の発行権をそのメッセージに適用できる。それからＰＨＢはデータ・メッセージをアクセス制御番号とともにひとつまたは複数の他のブローカに送ることができる。
【００１４】
ＩＢは制御バージョン・ベクトルを維持できる。
【００１５】
本発明の別の側面において、発行側クライアントから購読側クライアントにメッセージ配送を提供するコンテンツベースのパブリッシュ／サブスクライブ・システムは、ネットワークを介して互いに作動的に連結される複数のブローカを含み、ブローカの各々は発行者ホスティング・ブローカ（ＰＨＢ）、購読者ホスティング・ブローカ（ＳＨＢ）、および中間ブローカ（ＩＢ）のうちの少なくとも１つとして構成される。システムはまた、複数のブローカの少なくとも一部に作動的に連結され、システム内の少なくとも１つのアクセス制御ポリシーを格納および更新するように構成される少なくとも１つのアドミニストレータを含む。複数のブローカの少なくとも一部および少なくとも１つのアドミニストレータは、ひとつまたは複数のメッセージを挟んで送るアクセス制御バージョン識別子を含むことによって、システム内のアクセス制御ポリシーの変更を実施するように構成し、そこではアクセス制御識別子は有効なアクセス制御ポリシーを一意的に識別して、アクセス制御ポリシーの変更をアクセス制御ポリシーの変更により影響を受けるひとつまたは複数のプリンシパルに対応付けられる発行側クライアントおよび購読側クライアントに確定的かつ統一的に適用する。
【００１６】
有利なことに、システムはそれによって、少なくとも１つのブローカのクラッシュおよび再始動がその少なくとも１つのブローカの非永続状態を失ったときでも、またネットワーク内の少なくとも１つのリンクが途切れ、その接続を再確立し、少なくとも１つのリンクで送信される少なくとも１つのメッセージを脱落、重複、または順序を間違って配送させてしまうときでも、システムの同じプリンシパルの代わりに確定的かつ統一的なアクセス制御のセマンティクス（ｓｅｍａｎｔｉｃｓ）を購読者全員に保証できる。すなわち、システム内の別のサブネットワークで接続されているときでも、またそのサブネットワークが別の通信遅延およびネットワークもしくはルーティング・ブローカの障害を受けるときでも、同じプリンシパルの代わりに別の購読者がまったく同じシーケンスのメッセージを受け取ることになる（サブスクリプション・フィルタ差分を法として）。
【００１７】
複数のブローカは、ＰＨＢ以外のブローカでアクセス制御状態の永続ストレージの必要をなくすように構成できる。ＰＨＢは最新のアクセス制御ポリシーに対応する制御バージョン識別子を永続的に格納するように構成できる。ＰＨＢは、メッセージが発行された時点で有効であったアクセス制御ポリシーに対応するアクセス制御バージョン識別子を永続的に格納するように構成できる。ＰＨＢとＳＨＢの間には多重パスが存在してもよく、別のパス上のＩＢは同一のアクセス制御状態を維持する必要はない。ＩＢの少なくとも一部は、アクセス制御ルールを維持するのではなく、１つのＳＨＢごとに１つのバージョンとして、アクセス制御バージョン・ベクトルを維持できる。各ＳＨＢはそれに接続されるプリンシパルに関して最新のアクセス制御ルールを維持できる。

【００１８】
ＳＨＢはそれに接続されるプリンシパルに関するアクセス制御ルールの変更を購読依頼できる。ＩＢはプリンシパルによってアクセス制御ルールの変更をフィルタリングしてもよい。高信頼性配送を使用して、アクセス制御ルールの変更をそれを必要とするＳＨＢが確実に受け取るようにする。新たなプリンシパルからの接続を受け入れるＳＨＢは要求応答プロトコルを使用して、そのプリンシパルのアクセス制御ルールを初期化できる。
【００１９】
ＳＨＢはサブスクリプションと最新のアクセス制御ルールとの論理積を求め、論理積を求めたサブスクリプションの制御バージョンをそのバージョンの制御ルールを使って割り当ておよび維持する。ＳＨＢはそれで残ったサブスクリプションをそのアクセス制御バージョン識別子とともに上流のＩＢに伝搬できる。ＩＢはアクセス制御バージョン識別子とともにサブスクリプション状態を維持できる。
【００２０】
ＰＨＢはデータ・メッセージにアクセス制御バージョン識別子を含むことができる。ＩＢはサブスクリプション状態を使って、データ・メッセージのアクセス制御バージョン識別子がサブスクリプション状態のアクセス制御バージョン番号以下の場合メッセージをフィルタリングし、そうでなければメッセージを下流に送る。ＳＨＢはメッセージがメッセージの制御バージョンと一致する論理積を求めたサブスクリプションの制御バージョン識別子が等しいかを点検して、購読アクセス制御ルールを施行する。
【００２１】
本発明の上記並びにその他の目的、特徴、および利点は、添付の図面と関連して以下のその例示的な実施例の詳細な説明を読むと明らかになるであろう。
【発明を実施するための最良の形態】
【００２２】
本発明で代替接続構成も考えられるが、本発明の例示的な実施例を、好ましくはまとめて接続し、１つのオーバーレイ・ネットワークを形成する複数のブローカデバイスもしくはブローカを含む例示的なコンテンツベースのパブリッシュ／サブスクライブ・システムと合わせて以下説明していく。複数のブローカは発行者から購読者に送られるひとつまたは複数のメッセージを、少なくとも部分的に、これらメッセージのコンテンツおよび購読者が要求するフィルタリング述語、もしくはこれらメッセージのコンテンツまたは購読者が要求するフィルタリング述語に基づいて、配送する役割を担う。
【００２３】
ブローカは一定の機能に従いグループ分けできる。例えば、ひとつまたは複数のブローカは発行者のホスティング専用とするのが好ましいであろう。これらブローカを本明細書では発行者ホスティング・ブローカまたはＰＨＢと呼ぶ。また、ひとつまたは複数のブローカを購読者のホスティング専用とするのが好ましいであろう。これらブローカを本明細書では購読者ホスティング・ブローカまたはＳＨＢと呼ぶ。ＰＨＢとＳＨＢの間には、ルーティングおよびフィルタリング、もしくはルーティングまたはフィリタリングを含む任意の数の中間ホップが存在してもよい。当該ホップのブローカを本明細書では中間ブローカまたはＩＢと呼ぶ。説明しやすくするために、異なるブローカの各々が個々別々のエンティティであると仮定する。ただし、実際の実施においては、どのブローカもひとつまたは複数のＰＨＢ、ＳＨＢ、およびＩＢの機能を行うことができる。
【００２４】
本発明のアクセス制御サービス・モデルおよびアクセス制御ポリシー配布およびメッセージ配送プロトコルの例示的な実施例を説明する前に、図１、図２、および図３の状況で当該モデルおよびプロトコルを実装できる例示的なコンテンツベースのｐｕｂ／ｓｕｂシステムを説明する。当該コンテンツベースのｐｕｂ／ｓｕｂシステムは、特許文献１に詳細に述べられている。本発明のアクセス制御技術はこの例示的なシステムに限定されるものではないことは理解されるべきである。
【００２５】

図１は、本発明のある側面に従って形成した代表的なブローカのネットワークを含むコンテンツベースのｐｕｂ／ｓｕｂシステムの少なくとも一部を図示する。発行者１０１ａ、１０１ｂ、１０１ｃ、および１０１ｄは、それぞれ対応するクライアント接続１０７ａ、１０７ｂ、１０７ｃおよび１０７ｄを通して、特定のＰＨＢ１０２ａおよび１０２ｂとの接続を確立することが好ましい。クライアント接続は一般的に、例えば赤外線、無線周波数、衛星、マイクロ波等などのワイヤレス通信リンク、および例えば電話、ケーブル、光ファイバー等などの専用通信接続を含め、伝送される情報を伝えるあらゆる種類の通信媒体でよい。好ましくは、クライアント接続の各々は、転送制御プロトコル／インターネット・プロトコル（ＴＣＰ／ＩＰ）ソケット接続など信頼性の高い先入れ先出し（ＦＩＦＯ）方式の接続であるが、それだけに限定されない。

【００２６】

購読者１０５ａ、１０５ｂ、１０５ｃ、および１０５ｄは、それぞれ対応するクライアント接続１０８ａ、１０８ｂ、１０８ｃ、および１０８ｄを通して、ＳＨＢ１０４ａおよび１０４ｂとの接続を独立して確立するのが好ましい。クライアント接続１０８ａ、１０８ｂ、１０８ｃ、および１０８ｄは前述したクライアント接続１０７ａ、１０７ｂ、１０７ｃおよび１０７ｄと両立するのが好ましい。ＰＨＢ１０２ａ、１０２ｂおよびＳＨＢ１０４ａ、１０４ｂは、ブローカ間接続１０６ａ、１０６ｂ、１０６ｃ、１０６ｄ、１０６ｅ、１０６ｆ、１０６ｇ、１０６ｈを介して、ＩＢ１０３ａおよび１０３ｂに接続してもよい。ネットワークがギャップレス配送プロトコルを採用し、接続障害とメッセージ並べ替えを許容できるとすると、ブローカ間接続にＴＣＰ／ＩＰなどの高信頼性ＦＩＦＯプロトコルを使う必要はなく、信頼性は劣るがより高速のプロトコルを使うことによってシステムの処理能力を高めると有利であろう。

【００２７】

図２に図示するように、各発行者、購読者、およびブローカ（１５０として示す）は、プロセッサ１５２、メモリ１５４、およびひとつまたは複数の入出力（Ｉ／Ｏ）デバイス１５６に従い実装できる。本明細書で使用する「プロセッサ」という用語は、例えば、中央処理装置（ＣＰＵ）および他の処理回路（例、マイクロプロセッサ）、もしくは中央処理装置（ＣＰＵ）または他の処理回路（例、マイクロプロセッサ）を含むもののようなあらゆる処理デバイスを含むことを意図していることを了解するべきである。加えて、「プロセッサ」という用語は１台の処理デバイスより多くの処理デバイスをいうこともあり、また１台の処理デバイスに関連する様々なエレメントを他の処理デバイスと共有することもあることは理解されるべきである。本明細書で使用する「メモリ」という用語は、例えば、ランダム・アクセス・メモリ（ＲＡＭ）、読取専用メモリ（ＲＯＭ）、固定ストレージ媒体（例、ハードドライブ）、取り外し可能なストレージ媒体（例、ディスケット）、フラッシュメモリ等など、プロセッサもしくはＣＰＵに関連するメモリおよびその他のコンピュータ読み取り可能媒体を含むことを意図している。また、本明細書で使用する「入出力デバイス」または「Ｉ／Ｏデバイス」という用語は、例えば、データをプロセッサに入力するひとつまたは複数の入力デバイス（例、キーボード、マウス、ネットワーク・インターフェース・カード等）およびプロセッサに関連する結果を提示するひとつまたは複数の出力デバイス（例、プリンタ、モニタ、ネットワーク・インターフェース・カード等）もしくはデータをプロセッサに入力するひとつまたは複数の入力デバイス（例、キーボード、マウス、ネットワーク・インターフェース・カード等）またはプロセッサに関連する結果を提示するひとつまたは複数の出力デバイス（例、プリンタ、モニタ、ネットワーク・インターフェース・カード等）を含めることを意図している。

【００２８】

従って、本明細書で詳しく説明するアプリケーション・プログラム、またはそのソフトウェア・コンポーネントは、本発明の方法論を実行する命令もしくはコードを含めて、ひとつまたは複数の関連するストレージ媒体（例、ＲＯＭ、固定または取り外し可能なストレージ）に格納することができ、利用する準備ができたとき、プロセッサ１５２によって全体もしくは一部がロードされて（例、ＲＡＭに）実行される。このように、各発行者、

購読者、およびブローカは、例えば、独立型コンピュータ、コンピュータ上でランするプロセスまたはアプリケーション、もしくはシステム故障による遅延を最小限にするために、複数のコンピュータ内で分散方式でランする冗長プロセスのクラスターのいずれでもよい。

【００２９】

ここで図３を参照すると、本発明のある側面に従い、ブローカ・ネットワークの実施を図示する代表的な情報フロー図が示されている。図から明らかなように、ブローカ・ネットワークの例示的な情報フロー図は、本明細書で情報ストリームと呼ぶ複数のノード（楕円形で示す）と、本明細書で変換と呼ぶエッジもしくはパス（発信元楕円形と宛先楕円形の間の矢印で示す）とを有する。情報フロー図はシステム・アドミニストレータが、静的にまたはサブスクリプション要求に応答するいずれかで構成できる。情報フロー図は、中間情報ストリーム２１２ａ、２１２ｂ、２１２ｃ、２１２ｄ、２１２ｅ、２１２ｆ、２１２ｇ、２１２ｈ、２１２ｉ、２１２ｊ、２１２ｋ、２１２ｌ、２１２ｍ、２１２ｎ、２１２ｏ、２１２ｐ、２１２ｑ、２１２ｒ、２１２ｓ、２１２ｔ、２１２ｕ、２１２ｖ、２１２ｗ、２１２ｘ、２１２ｙ、２１２ｚ、２１２ａａ、２１２ｂｂ、２１２ｃｃ、２１２ｄｄ（集合的に、２１２）を介して、本明細書でパブエンドと呼ぶ発信元情報ストリーム２１１ａおよび２１１ｂと、本明細書でサブエンドと呼ぶ宛先情報ストリーム２１６ａ、２１６ｂ、２１６ｃ、２１６ｄ、２１６ｅ、２１６ｆ、２１６ｇ、２１６ｈ、２１６ｉ、２１６ｊ、２１６ｋ、２１６ｌ（集合的に、２１６）との間のパスを定義する。

【００３０】

好ましくは、各発行者はメッセージを１つだけのパブエンドに配送するが、各購読者は１つのＳＨＢ内でひとつまたは複数のサブエンドからメッセージを受け取る。各変換は、フィルタ変換２１４ａ、２１４ｂ、２１４ｃ、２１４ｄ、２１４ｅ、２１４ｆ、２１４ｇ、２１４ｈ、２１４ｉ、２１４ｊ、２１４ｋ、２１４ｌ、２１４ｍ、２１４ｎ、２１４ｏ、２１４ｐ、２１４ｑ、２１４ｒ、２１４ｓ、２１４ｔ、２１４ｕ、２１４ｖ、２１４ｗ、２１４ｘ、２１４ｙ、２１４ｚ（集合的に、２１４）、リンク変換２１３ａ、２１３ｂ、２１３ｃ、２１３ｄ、２１３ｅ、２１３ｆ、２１３ｇ、２１３ｈ、２１３ｉ、２１３ｊ、２１３ｋ、２１３ｌ、２１３ｍ、２１３ｎ、２１３ｏ、２１３ｐ、２１３ｑ、２１３ｒ、２１３ｓ（集合的に、２１３）、またはマージ結合変換２１５ａ、２１５ｂのいずれかである。所定の変換を通過しながら情報を遅延、消失、または並べ替えできるが、実際にはこれはリンク上でしか起こらないのが一般的である。

【００３１】

フィルタはコンテンツ・フィルタを表す述語を含むのが好ましい。例えば、フィルタ２１４ｅは「場所＝ＮＹ」と一致するコンテンツをもつメッセージしか通過しないと指定する。対応する述語をもたないフィルタ（例、２１４ｉおよび２１４ｊ）はすべてのコンテンツを通過するが、これは本質的にはリンクに匹敵する。

【００３２】

各ブローカ２０２ａ、２０２ｂ、２０３ａ、２０３ｂ、２０４ａ、２０４ｂは、それぞれ対応するタイマまたはクロック２２２ａ、２２２ｂ、２２２ｃ、２２２ｄ、２２２ｅ、２２２ｆをもつことが好ましい。本発明の方法論ではこれらクロックが実時間と同期する必要はないが、これらクロックが互いに少なくともほぼ正確、または同期していれば、性能は高まるであろう。クロックをあるブローカに対応付けることに加えて、ＰＨＢ２０２ａおよび２０２ｂはそれぞれ対応する安定したストレージ媒体２２１ａおよび２２１ｂを必要とする。安定したストレージとは、例えば、ＲＡＭ、固定ストレージ、取り外し可能なストレージ等など、不揮発性メモリを含むことを意図している。残りのブローカ（例、ＳＨＢおよびＩＢ）２０３ａ、２０３ｂ、２０４ａ、２０４ｂは安定したストレージである必要はなく、代わりに「ソフト」状態を使える。ＰＨＢにだけ安定したストレージがあればいいということと、ＳＨＢおよびＩＢがソフト状態を利用できるということにより、本ブローカ・ネットワークは、ストア・アンド・フォワード技術を採用する他のプロトコルと有利に区別される。これら従来のプロトコルは安定したストレージを一般的にネット

ワーク内の各ブローカに対応付ける必要がある。

【００３３】

パブエンドから所定のクライアントのサブエンドまでのパスは、クライアントが受け取るのを保証されるのはどのメッセージかを決定する。具体的には、各パスはパスに沿った各フィルタに対応する述語の論理積（すなわち、論理ＡＮＤ）を満たすメッセージを伝搬する。所定のノードに対応するパスが複数ある場合、そのノードはパスフィルタの論理和（すなわち、論理ＯＲ）を満たすメッセージを受け取る。

【００３４】

単なる例として、サブエンド２１６ａおよび２１６ｂに対応するクライアントＣ１を考えてみる。サブエンド２１６ａとパブエンドの間のパス、すなわち２１４ｏ、２１３ｉ、２１４ｅ、２１３ａ、および２１４ａに基づき、Ｃ１はパブエンド２１１ａに発行され、フィルタ「トピック＝１」＆「場所＝ＮＹ」＆「ｐ＞３」を満たすメッセージを受け取り、ここで「＆」の記号は論理ＡＮＤ演算を表す。同様に、サブエンド２１６ｂとパブエンドの間のパス、すなわち２１４ｑ、２１３ｍ、２１４ｇ、２１３ｆ、および２１４ｄに基づき、Ｃ１はパブエンド２１１ｂに発行され、フィルタ「トピック＝１」＆「場所＝ＮＹ」＆「ｐ＞３」を満たすメッセージを受け取る。

【００３５】

各サブエンドは順序のあるストリームであることが好ましい。そのため、クライアントＣ１はパブエンド２１１ａからの関係あるメッセージのすべて（すなわち、所定のパスに対応するフィルタを満たすコンテンツをもつメッセージ）を発行された順番で受け取り、パブエンド２１１ｂからの関係あるメッセージのすべてを発行された順番で受け取る。ただし、パブエンド２１１ａに発行されたメッセージとパブエンド２１１ｂに発行される別のメッセージとの間に、順序は必要ない。すなわち、発行時とは無関係で、パブエンド２１１ａからの所定のメッセージがパブエンド２１１ｂからの所定のメッセージの前に到着するか、または後に到着するかは一般的に予測できないことを意味する。これは、コンテンツ選択（例、トピック＝１＆場所＝ＮＹ＆ｐ＞３）および発行者順序のあるクライアント・サブスクリプションの例である。

【００３６】

対して、１つのサブエンド２１６ｅに対応するクライアントＣ２を考えてみる。図３に示すように、サブエンド２１６ｅとパブエンドの間のパス、すなわち２１４ｓ、２１３ｋ、２１４ｉ、２１５ａ、２１３ｂ、２１４ｂ、２１３ｅ、および２１４ｃは、パブエンド２１１ａからのフィルタ「トピック＝２」とパブエンド２１１ｂからのフィルタ「トピック＝２」のマージ結合であり、さらに「ｉ＝１」によってフィルタリングされる。クライアントＣ２は対応するサブエンドが１つであるため、１つの順序のあるストリームを受け取る。これは、コンテンツ選択（例、トピック＝２＆ｉ＝１）と総合順序のあるクライアント・サブスクリプションの例である。クライアントＣ３は同じコンテンツ選択（例、トピック＝２＆ｉ＝１）と総合順序のあるサブスクリプションであるため、クライアントＣ２と同じ順序で同じメッセージを受け取ることに留意する。本ブローカ・ネットワークのこの統一的な総合順序特性は、マージ結合変換が確定的であり、同一の入力情報ストリームを受け取る２つのマージ結合変換は同じマージ結合出力情報ストリームを生むことの結果である。

【００３７】

図３の例示的な情報フロー図は、本ｐｕｂ／ｓｕｂシステムのギャップレスな配送方法論を指す。要約すると、好ましくは各情報ストリームは各特定の時間間隔またはチックの間に発生したトラックを維持する。このため、各情報ストリームはデータ・メッセージ（または沈黙）とそのチックについてどの程度熱心に知りたいのかを表す関心度を有することが好ましい。知識は下流（すなわち、矢印の方向）に流れる一方、関心度は上流（すなわち、矢印の方向とは逆の方向）に流れる。従って、サブエンドは、知識チックのギャップレス・シーケンスが延長していることを検出したときにメッセージを配送する。他方でパブエンドはメッセージを安定したストレージにログする。安定したストレージに維持さ

れるこれらログはその後、他のブローカが所定のチック中に何が起こったかの知識をもたない場合に、関心度のアービタ（ａｒｂｉｔｅｒ）として利用できる。

【００３８】

例示的なコンテンツベースのｐｕｂ／ｓｕｂシステムを上記説明してきたところで、ここで本発明のアクセス制御の原理を例示的に説明していく。

【００３９】

本発明の原理は、金融市場における電子取引などのミッション・クリティカルなアプリケーションでしばしば求められるように、パブリッシュ／サブスクライブ・システムが新しいアクセス制御ポリシーを成立させるためにシャットダウンをする必要なく機能し続けることを実現する。

【００４０】

従って、本発明の例示的な実施例は、コンテンツベースのフィルタリングおよびルーティング、高信頼性配送並びに冗長ルートを備えるｐｕｂ／ｓｕｂシステムの動的アクセス制御を提供する。この目的のために、コンテンツベースのｐｕｂ／ｓｕｂシステムにおける動的アクセス制御の確定的サービス・モデルを提供する。このようなサービス・モデルの確定的な保証により、イベントの機密性に正確な制御が可能となり、クライアントの場所、ネットワーク遅延、および障害などの問題とは独立する。アドミニストレータは、発行されたメッセージ・ストリームでアクセス制御の変更が起こった正確な時点を知る。このモデルによる高信頼性配送のセマンティクスが明確に定義され、すなわち同じプリンシパルの２以上の購読者は、購読者がどこに接続されていても、プリンシパルのアクセス制御ポリシーが変更されたときに同じメッセージのセットを受け取る。

【００４１】

本明細書で使用する「プリンシパル」とは一般的にあるエンティティをいうことは理解される。当該エンティティは認証技術によって能動的に特定され、検証できる。プリンシパルにはシステムのリソースまたはサービスを使用する一定の権利が与えられる。システムの実際のクライアントはプリンシパルの代理として行為して、システムのリソース／サービスを使用できる。システムがクライアントにサービスを提供しようとする場合、システムはクライアントが接続するプリンシパルに与えられる権利に従ってサービスを提供する。プリンシパルの種類の例は以下説明する。

【００４２】

本発明の例示的な実施例は、この確定的なサービス・モデルをサポートするアルゴリズムも提供する。このアルゴリズムを使って、アクセス制御の変更を、その影響を受けるプリンシパルが接続している全ブローカに統一的に実施する。システムは、システムの効率と変更を成立させる時宜性を犠牲にしうるこれらブローカからのコンセンサスを得る必要はない。このアルゴリズムは、（１）アクセス制御の施行をネットワーク全体に配信でき、イベント発信元に密接に行える点で効率的であり、かつ（２）パス間のコンセンサスを得る必要なく、ルーティングがどの冗長パスでも選べることによって可用性が高い。

【００４３】

Ａ．サービス・モデル

【００４４】

本セクションでは、動的アクセス制御の確定的なサービス・モデルを例示的に説明する。より具体的には、動的アクセス制御に関わる様々なエンティティとその役割、アクセス制御ルールを指定するためのコンテンツベース形態、およびアクセス制御変更の明確な開始点を説明する。

【００４５】

例示的なサービス・モデルでは、アクセス制御に関わるエンティティは以下の２種類がある。

【００４６】

（１）セキュリティ・アドミニストレータ。セキュリティ・アドミニストレータとは、システム内のアクセス制御の最終認証者である。セキュリティ・アドミニストレータはク

ライアント・プリンシパル（以下に定義する）のアクセス権およびその現在のアクセス権に何らかの変更をすべきかどうか、もしくはクライアント・プリンシパルのアクセス権またはその現在のアクセス権に何らかの変更をすべきかどうかを決める（クライアント・サービス契約などの外部要因に基づき）。セキュリティ・アドミニストレータはその決定を管理インターフェースからシステムに命令する。

【００４７】

大型のシステムでは、セキュリティ・アドミニストレータが複数いる場合もある。各アドミニストレータが行う変更が重複したクライアントの組に影響することがあるため、システムはトランザクションごとに直列化可能に変更を受け入れる。このように例示的に説明し、解説を簡潔にするために、セキュリティ・アドミニストレータを１シーケンスのポリシーの変更を開始する１つのエンティティとして考える。別のアドミニストレータからのポリシーの変更が順序付けられ、変更の矛盾は解決されたと想定する。

【００４８】

（２）クライアント・プリンシパル。例示的なｐｕｂ／ｓｕｂシステムのクライアントは、クライアントが接続したときに認証によりシステムが決定／検証するプリンシパルに対応付けられている。本明細書で例示的に使用する「クライアント」という用語は、発行者（すなわち、発行側クライアント）または購読者（すなわち、購読側クライアント）のいずれかをいうことは理解されるべきである。実際には、クライアントは発行者および購読者の両者として行為できる。すなわち、クライアントはシステムに接続し、メッセージを発行する、またはメッセージを購読依頼して受け取ることができる。クライアントが接続し、メッセージを発行および購読依頼／受け取ることのできる能力は、そのプリンシパルのアクセス権によって規制される。例えば、クライアントが株価情報、金融ニュース、およびＩＢＭコーポレーションのレポートを受け取ることに関心をもっているが、そのプリンシパルが株価情報へのアクセス権しかもたない場合、クライアントは要求してもニュースおよびレポートは一切受け取れない。

【００４９】

例示的なシステムのアクセス制御ルールはプリンシパルに対応付けられる。同じプリンシパルの複数のクライアントはシステム内の別の場所で接続できる。

【００５０】

例示的なシステムのプリンシパルには、（１）グループ、および（２）個人の２種類がある。グループ・プリンシパルとは個人または再帰的に他のグループ・プリンシパルの集合体である。グループ・プリンシパルに与えられるアクセス権は自動的にそのグループの全メンバー、および再帰的にメンバー・グループのメンバーに与えられる。

【００５１】

プリンシパルのアクセス権は、接続する権利、メッセージを発行する権利、およびメッセージを購読依頼して受け取る権利を含む。これら３つの権利のアクセス制御ルールを指定するためにコンテンツベースの形態を採用する。アクセス制御ルールは以下の３要素１組の形をとる。

【００５２】

［プリンシパル、アクセス形態、コンテンツ・フィルタ］

【００５３】

当該形態のルールは、プリンシパルがシステムに接続し、コンテンツ・フィルタと一致するメッセージを発行または購読依頼する権利をもつことを指定する。発行および購読依頼ルールは３要素１組ではないフィルタを採用することができるが、接続ルールは真または偽で指定して、接続する権利があるかどうかを示す。例えば、プリンシパル「Ｊｏｈｎ　Ｄｏｅ」に接続および株価情報を購読依頼することを認めるルールは以下のように指定される。

【００５４】

［Ｊｏｈｎ　Ｄｏｅ、接続、真］

［Ｊｏｈｎ　Ｄｏｅ、購読依頼、タイプ＝'株価'］

【００５５】
アクセス制御ルールは、すべてのルールがプリンシパルになにをすることを認めるかを指定する肯定形で内部で維持される。プリンシパルにすることを認めないことを指定する否定形はセキュリティ・アドミニストレータへの便宜として提供され、コンテンツ・フィルタの否定をとることによって内部で肯定形に変換される。
【００５６】
アクセス制御ルールの統制の下、クライアントはそのプリンシパルの発行ルールと一致するメッセージの発行を認められ、そのサブスクリプション・フィルタおよびそのプリンシパルの購読ルールの両方と一致するメッセージの受け取りを認められる。このことから、システムは、（１）許可された発信元だけにしかメッセージの発行を認めないことにより情報の真正性、（２）許可された購読者だけにメッセージを配信することにより情報の機密性、（３）ただ廃棄するつもりで大量のメッセージを要求する悪意の購読者により開始されるサービス妨害（ＤｏＳ：ｄｅｎｉａｌ　ｏｆ　ｓｅｒｖｉｃｅ）攻撃に対する保護の提供を可能にする。このような大量のメッセージはネットワークの渋滞を招いて、システムが他のクライアントにサービスを提供する能力を減じることになりかねない。
【００５７】
グループ・プリンシパルおよび個人プリンシパルは同じ形態の接続、発行、および購読依頼アクセス権を共有する。加えて、グループ・プリンシパルにはメンバーリストと呼ぶ新しいタイプのルールが存在する。例えば、Ｊａｎｅ　ＳｍｉｔｈとＪａｍｅｓ　Ｂｒｏｗｎを含み、株価情報、ニュース、およびレポート全部を購読する権利をもつプレミアム購読者グループは、以下のアクセス制御ルールをもつ。
【００５８】
［プレミアム・グループ、メンバー・リスト、｛Ｊａｎｅ　Ｓｍｉｔｈ、Ｊａｍｅｓ　Ｂｒｏｗｎ｝］
［プレミアム・グループ、購読依頼、タイプ＝'株価'またはタイプ＝'ニュース'またはタイプ＝'レポート'］
【００５９】
グループ内の全メンバーには自動的にそのグループのアクセス権が与えられる。このため、個人プリンシパルのアクセス権は個人の権利と個人が所属する全部のグループ・プリンシパルの権利の論理和となる。そのため、Ｊａｎｅ　ＳｍｉｔｈとＪａｍｅｓ　Ｂｒｏｗｎは二人に与えられる他のアクセス権に加えて、株価情報、ニュースおよびレポートのすべてにアクセス権をもつことになる。
【００６０】
図４は例示的なサービス・モデルの例を図示する。
【００６１】
例示的な確定的サービス・モデルはアクセス制御の変更の明確な開始点を提供する。このモデルでは、アクセス制御ルール／変更３０１はセキュリティ・アドミニストレータ３０２が管理コンソールで開始し、ＡＣＬ　ＤＢ（アクセス制御データベース）と呼ばれる永続ストレージ３０３に格納される。セキュリティ・アドミニストレータはいつでも、ひとつまたは複数のプリンシパルに関係する多数の変更を指定できる。これら変更は原子的に施行しなければならないバッチと考えられる。セキュリティ・アドミニストレータが変更の各バッチを確認した後、変更はブローカ・ネットワーク３０４に伝搬する。
【００６２】
発行者（図示せず）が接続するブローカはひとつまたは複数のメッセージ・ストリームをホストする。各ストリームはひとつまたは複数の発行者が発行したメッセージを順番に有する。例えば、図４に示すように、ブローカ３０５はメッセージ・ストリーム３０６をホストする。
【００６３】
これらストリームの各々について、ブローカはセキュリティ・アドミニストレータが指定した新たなアクセス制御ルールを成立させる開始点を選ぶ。開始点は、（１）連続する

変更のバッチが後の開始点を求める、および（２）開始点以降のメッセージが旧ルールに従って配送されることのないよう開始点が十分遅くなるように選ぶ。これはストリームで新たに発行されたメッセージを開始点とすることによって達成できる。開始点情報は将来の問い合わせおよび参照のためにセキュリティ・アドミニストレータに送り戻される。新しいルールは、プリンシパルのクライアントがどこに接続していようとも、開始点以降のすべてのメッセージにシステム全体で統一的に施行される。

【００６４】

図４には、購読者が購読依頼したひとつまたは複数のメッセージ３０８を受け取る購読者３０７も図示され、その例を以下詳しく説明する。

【００６５】

アクセス制御ポリシーの変更の効果を、プリンシパルＪｏｈｎ　Ｄｏｅの購読権が３段階で変更された例を使って説明する。（１）Ｊｏｈｎ　Ｄｏｅは株価情報だけに購読アクセスをもつ販促グループのメンバーとなった。（２）Ｊｏｈｎ　Ｄｏｅはプレミアム購読者となり、その後３種類の金融情報すべて（株価情報、金融ニュース、レポート）への購読アクセスが与えられた。（３）Ｊｏｈｎ　Ｄｏｅのプレミアム・サブスクリプションが終了し、その結果金融ニュースとレポートの購読権を失った。

【００６６】

図４に関連し、プリンシパルＪｏｈｎ　Ｄｏｅの購読者はシステムに接続して、記事＝「ｉｂｍ」のサブスクリプションを要求したと仮定する。このサービス・モデルでは、Ｊｏｈｎ　Ｄｏｅのアクセス権が変更するたびに、システムは各メッセージ・ストリームの明確な開始点を提供して、（１）開始点以前のメッセージは、そのメッセージが変更前にサブスクリプション・フィルタとアクセス権フィルタを満たす場合かつその場合に限ってクライアントに配送される、および（２）開始点以降のメッセージは、そのメッセージが変更以降のサブスクリプション・フィルタとアクセス権フィルタの両方を満たす場合かつその場合に限ってクライアントに配送される。図４の例のストリームでは、選ばれた開始点が第１アクセス変更についてはメッセージ１００、第２アクセス変更についてはメッセージ１０３および第３変更についてはメッセージ１０６である場合、クライアントに配送されるメッセージは１００、１０３、１０４、１０７、１０９となる。範囲１０３・・・１０５では株価情報以外だけが配送されることに留意する。メッセージ・ストリームが１より多いシステムの場合、この活動がすべてのストリームに起こり、それぞれその個々の開始点をもつ。

【００６７】

ブローカのネットワークが採用するルーティング・トポロジーは、各ノードが冗長で互いに交換可能に動作できる複数の仮想ブローカを含むノードの全域ツリーの抽象的なトポロジーモデルである。ツリーはループなしルーティングのタスクを単純にする非周期構造である。冗長ブローカを備えるツリーのノードは可用性が高い。

【００６８】

図１の状況で上記説明した例示的なｐｕｂ／ｓｕｂシステム（本発明の例示的なサービス・モデルを実装できる）から、発行者が接続するブローカを発行者ホスティング・ブローカ（ＰＨＢ）と呼び、購読者が接続するブローカを購読者ホスティング・ブローカ（ＳＨＢ）と呼んだことを思い出していただきたい。単純にするために、１つのＰＨＢの観点からルーティングを論じる。抽象的なネットワークは、クライアントをホストするあらゆる物理的なブローカが葉ノードで仮想ブローカを実装するように構成できる。そのため、このモデルでは、ＳＨＢはツリーの葉ノードにしか存在しない。また、ＰＨＢは１つだけあり、ツリーの根に存在する。上流／下流の方向は根に向かう／根から離れる。１クライアントは１ブローカに接続するため、各葉ノードは１つのブローカを含む。ブローカをツリーのノードにグループ分けし、ブローカ間のリンクをツリーのエッジにグループ分けすることによって、冗長パスのグラフをこのモデルのトポロジーに変換できるため、このトポロジー・モデルは大きな範囲の実際のトポロジーを表すことができる。

【００６９】

アクセス制御のある例示的な実施とは、ＰＨＢおよび中間ブローカがクライアントのサブスクリプションと一致する発行されたすべてのメッセージをＳＨＢに送り、ＳＨＢがクライアントのサブスクリプションだけでなくそのアクセス権にも一致するメッセージを配送することによってアクセス制御を施行する。このようなソリューションは完璧に正しい実施となるが、後で廃棄するメッセージを送る帯域幅がかなりの無駄となりうる。

【００７０】

サブスクリプション伝搬とは、ＰＨＢおよび中間ブローカにサブスクリプション述語に関する知識を取得してフィルタリングを行うことを要求する代わりに、ＳＨＢに送る無駄なメッセージを少なくすることになりうる最適化である。クライアントのアクセス権をそのサブスクリプションとともに伝搬することによって、通信コストの更なる節約が達成できる。

【００７１】

前述した確定的サービス保証を提供することは、冗長パスをもつネットワークで展開されるコンテンツベースのシステムでは大変なことである。コンテンツベースのルーティングのために、発行者割り当てシーケンス番号などの従来の方法ではギャップを検出することはできない。各購読者が完全に一意的なシーケンスのメッセージを配送することを求めるかもしれないからである。そのため、コンテンツベースのシステムの信頼性はルーティングパス上のブローカにギャップ検出を支援することが必要である。

【００７２】

代替ルートの冗長ブローカが互いに異なるサブスクリプションおよびアクセス制御情報をもちうるため、複数のパス、通信非同期、および障害がサブスクリプションおよびアクセス制御情報の伝搬を複雑にする。同じ発行ストリームからのメッセージがそれらのブローカを経由している場合、異なるサブスクリプション・フィルタとアクセス制御フィルタのセットに一致する。その結果、購読者に配送されるメッセージ・シーケンスにギャップが現れる可能性がある。

【００７３】

サブスクリプション伝搬の例示的なプロトコルが、非特許文献１および非特許文献２に開示されており、その開示を参照により本明細書に組み込む。これらプロトコルは高信頼性配送を保全し、システムの可用性と負荷分散のために冗長パスのどこでも自由なルーティングの選択を可能にする。さらに、当該プロトコルにより、メッセージが占有する永続ストレージをシステムが取り戻せるように、開始点以降のメッセージがまったく確認応答されていなければ、発行されたメッセージ・ストリーム上のサブスクリプションの高信頼性配送の開始点をストリームのどの時点としても選べることとなる。

【００７４】

以下、当該高信頼性配送およびサブスクリプション伝搬プロトコルを、ｐｕｂ／ｓｕｂクライアントに動的アクセス制御の確定的なセマンティクスを施行する効率的かつ可用性の高い分散プロトコルを構築する基本要素として使用する。ドメインベースの信頼モデルを採用する。同じドメイン内のすべてのブローカは互いに信頼する。互いに信頼しないブローカは別のドメインに入れることとし、ドメイン間の通信はその信頼レベルに応じてアクセス制御ルールを割り当てることによって統制する。単純にするために、１つの信頼されたドメインにおけるプロトコルを論じる。多くの商業ケースでは、ｐｕｂ／ｓｕｂシステムをアドミニストレータの完全な管理の下にある管理された環境で展開するため、これは実用的である。１ドメインを１発行側／購読側クライアントとして扱い、プリンシパルをそのドメインに割り当てることによって、この概念を複数の信頼されたドメインに敷衍することができる。信頼されていないドメインを通してシステムに接続されるクライアントは、ドメインの権利とそれ自身のアクセス権の両方を満たすメッセージにしかアクセスできない。

【００７５】

Ｂ．アクセス制御ポリシー配布およびメッセージ配送プロトコル

【００７６】

図５は、メッセージ配送の確定的サービス保証を提供するアクセス制御ポリシー配布およびメッセージ配送プロトコルを図示する。概説したように、プロトコルは、アクセス制御情報を関係あるプリンシパルをホストするブローカに配信するステップ（４０１）、発行者の発行権を満たすメッセージだけを受け入れることによって発行活動を制限するステップ（４０２）、その購読権を使ってクライアントのサブスクリプションを制限するステップ（４０３）、制限付きのサブスクリプションを伝搬し、そのためクライアントのサブスクリプションとアクセス権の両方でコンテンツのフィルタリングを行うことによって、ルーティング・ブローカでアクセス制御を施行するステップ（４０４）、ＳＨＢで最終的なアクセス制御の施行をするステップ（４０５）を備える。これらプロトコルの各側面を図１から図４に図示したコンポーネントを再び参照しながら以下説明する。

【００７７】

前述したように、アクセス制御ポリシーはＡＣＬ　ＤＢと呼ばれる永続ストレージで維持する。セキュリティ・アドミニストレータはトランザクション・バッチでＡＣＬ　ＤＢのポリシー変更を行う。アクセス制御ポリシーは制御バージョンに対応付けられ、制御バージョンは整数カウンタである。各トランザクション・バッチはＡＣＬ　ＤＢを新しい制御バージョンにする。この新しいアクセス制御ルールに新バージョン番号を割り当てる。旧アクセス制御ルールがいくつかのメッセージでまだ有効なこともあるため、ＡＣＬ　ＤＢはバージョンの異なるアクセス制御ルールが入り混じった状態で含まれる。全体を送らないように、ＡＣＬ　ＤＢはアクセス制御の新バージョンを増分変更として発行することにより配信する。

【００７８】

各ＰＨＢ／ＳＨＢは現在接続されているクライアントの最新の制御ルールのキャッシュを維持する。新しいプリンシパルのクライアントが接続する場合、ブローカはそのプリンシパルの初期バージョンのアクセス制御ルールを、ＡＣＬ　ＤＢに要求／応答プロトコルを使用して検索する。ブローカは接続されるプリンシパルの将来のアクセス制御の変更を受け取るためのサブスクリプションも確立する。サブスクリプション伝搬および高信頼性配送サービスは、ブローカが接続されるプリンシパルの初期バージョンのアクセスルールを取得した後のすべてのアクセス制御変更を確実に受け取るようにする。

【００７９】

ＰＨＢが新バージョンのアクセス制御ルールを受け取った場合、ＰＨＢはそのキャッシュを更新する。ＰＨＢは新バージョンの開始点を発行されることになる次のメッセージとして選ぶ。新たに発行されるメッセージは、有効な現在の発行権と一致する場合に限り受け入れる。加えて、新たに発行されるメッセージは、有効なアクセス制御バージョンを保持しながらシステムに送信される。ここで、購読権をどのように施行するかを説明する。

【００８０】

コンテンツベースのルーティングが純粋にクライアントのサブスクリプションだけに基づき、アクセス制御がクライアントが接続するブローカでのみ施行されるシステムにおいては、ルーティング・ブローカはそのアクセス権ではなくクライアントのサブスクリプションだけに一致するメッセージを送ることができる。これらメッセージは後で単に廃棄されるだけで、システムの帯域幅の無駄になる。

【００８１】

アクセス制御情報を、クライアントのサブスクリプションに加えてメッセージのルーティングに影響を与えることのできる別の種類の情報として扱うことができる。このため、当初のクライアント・サブスクリプション・フィルタをネットワークの残りに伝搬する代わりに、ＳＨＢはクライアント・サブスクリプション・フィルタとＳＨＢキャッシュにある最新バージョンのコンテンツベースのアクセスルールとの論理積である制限付き形態のフィルタを伝搬する。アクセス制御ルールが変更されると、ＳＨＢは影響を受ける全クライアント／プリンシパルの制限付きのサブスクリプションを新バージョンのルールで再計算する。その結果得られるサブスクリプションを制御バージョンと一緒に原子的に上流に伝搬する。上流のルーティング・ブローカはサブスクリプションが制限されているかどう

かを知る必要なくサブスクリプションを操作する。上流のルーティング・ブローカはその下流で各ＳＨＢの制御バージョンのベクトルを維持するだけでよい。

【００８２】

制限付きフィルタを伝搬するとき、コンテンツベースのルーティングはクライアント・サブスクリプション・フィルタとアクセス制御ルールの論理積に基づく。このことから、ルーティング・ブローカはアクセス制御およびＳＨＢに参加できる。

【００８３】

前述したように、システム内のメッセージはメッセージに有効な制御バージョンを保持する。下流のメッセージをルーティングする場合、ルーティング・ブローカはこのバージョンのメッセージとその下流に位置するＳＨＢのその制御バージョン・ベクトルの部分ベクトルとを比較する。メッセージは、下流からの制限付きのサブスクリプションと一致せず、かつブローカの制御バージョン・ベクトルの部分ベクトルのすべてのエレメントがメッセージのもの以上の場合に限って除外される。ブローカが十分な大きさの制御バージョン・ベクトルをもたない場合、ブローカは一応メッセージを下流に送る。例えば、ブローカｂは、メッセージがたとえ無駄になっても、すなわちサブスクリプション・フィルタと下流のブローカを根とするサブネットワークで接続されるクライアントの購読権が一致しなくても、とにかく下流のブローカにメッセージを送る。ブローカｂが十分な大きさの制御バージョン・ベクトルをもつ場合、ブローカｂは、メッセージがブローカｂが下流のブローカｂ’を根とするサブネットワークのために維持するサブスクリプション・フィルタと一致しない場合、メッセージを除外して、下流のブローカｂ’にメッセージを送るのを差し控えることができる。

【００８４】

アクセス制御の最終的な施行者は、中間ルーティング・ブローカがクライアントのアクセス権と一致しないメッセージを一応送ることがあるため、ＳＨＢである。

【００８５】

ＳＨＢはまず、メッセージが要求するバージョンのアクセス制御ルールを受け取ったかどうかを調べる。受け取っていない場合、ＳＨＢはそのアクセス制御ルールのバージョンが到着するまでメッセージの処理を遅らせる。ＳＨＢが制御バージョンのルールを受け取ったら、ＳＨＢはそのメッセージと一致する各制限付きのサブスクリプションを調べる。制限付きのサブスクリプションがメッセージと同じ制御バージョンの場合、メッセージは購読側クライアントに配送される。そうでなければ、メッセージはクライアントに配送されない。

【００８６】

制御バージョンを使うことで、メッセージ配送アルゴリズムがサービス・モデルの明確な開始点の特徴を実施できるだけでなく、システムがより非同期し耐故障性をもつことにもなる。制御バージョン番号を付けてアクセス制御の変更を配信することで、システム内の各ブローカは、全ブローカに一斉配信するトランザクション・セッションを利用する場合に、遅いまたはクラッシュしたブローカを待たずに、非同期して進めることができる。ルーティング・ツリー・ノードの大半のブローカに障害が起こった場合でも、新しいアクセス制御ルールを成立させることができ、残りのブローカはその冗長ピアから同意を取得する必要なくアクセス制御の施行に参加できる。ブローカが復旧したら、その制御バージョンが最新のものでなくても、それでもブローカはアイドル状態に留まっていたはずのネットワーク容量のその部分を利用して、メッセージのルーティングに参加できる。

【００８７】

唯一接続されるプリンシパルの制御ルール・キャッシュを利用することで、プリンシパルの数が多い大規模な環境でもシステムを基準化させられる。ＳＨＢはローカルに接続されるプリンシパルのアクセス制御ルールだけを知ればよい。

【００８８】

ここで図６および図７を参照すると、本発明のある実施例に従い、アクセス制御ポリシー配布およびメッセージ配送プロトコルを実装するコンテンツベースのパブリッシュ／サ

ブスクライブ・システムの一部が示されている。図示する例では、単純にするために１つのセキュリティ・アドミニストレータ、１つのＰＨＢ、１つのＩＢ、１つのＳＨＢのみが示されていることは理解されるべきである。このため、実際のシステムでは複数の当該コンポーネントを含む。また、ＰＨＢは直接、すなわちＩＢを介さなくてもＳＨＢに連結できる。さらに、セキュリティ・アドミニストレータ、ＰＨＢ、ＳＨＢ、およびＩＢは説明するステップを行うコンピューティング・デバイスをいうことは理解されるべきである。当該コンピューティング・デバイスは図２に図示するように構成して、説明するステップ／操作をプロセッサおよびメモリの構成により実行できるようにする。

【００８９】

図示するように、この例では、セキュリティ・アドミニストレータ５０２は上記説明したようにアクセス制御ポリシー変更（すなわち、アクセス制御ポリシー変更のバッチ）を含むメッセージを、割り当てられた制御バージョン番号とともに適切なブローカに送る。適切なブローカとは、ポリシーの変更により影響を受けるプリンシパルの代わりにクライアントをホストするあらゆるブローカとなろう。この例では、適切なブローカはＰＨＢ（５０４）およびＳＨＢ１（５０８）として示される。

【００９０】

上記説明したように、また図６に図示するように、アクセス制御ルールが変更されると、ＳＨＢは影響を受ける全クライアント／プリンシパルの制限付きのサブスクリプションを新バージョンのルールで再計算する。その結果得られるサブスクリプションは制御バージョンと一緒に原子的に上流に伝搬される。上流のルーティング・ブローカ（この例ではＩＢ５０６）はサブスクリプションが制限されているかどうかを知る必要なくサブスクリプションを操作する。上流のルーティング・ブローカはその下流で各ＳＨＢの制御バージョンのベクトルを維持するだけでよい。

【００９１】

また、上記説明したように、また図７に図示するように、ＰＨＢが新バージョンのアクセス制御ルールを受け取った際、ＰＨＢはそのキャッシュを更新する。ＰＨＢは新バージョンの開始点を発行されることになる新たなメッセージとして選ぶ。新たに発行されるメッセージは有効なアクセス制御バージョンを保持しながらシステムにＰＨＢ（５０４）によって送信される。

【００９２】

ここで図８から図１２を参照すると、フローチャートはアクセス制御ポリシー配布およびメッセージ配送プロトコルで、ＳＨＢ（図８および図９）、ＰＨＢ（ステップ６Ｃおよび６Ｄ）、およびＩＢ（図１２）がとるステップを表す。これらフローチャートは上記説明したアクセス制御ポリシー配布およびメッセージ配送プロトコルの様々な側面の例を表す。

【００９３】

図８は、新バージョンのアクセス制御に関する情報を受け取った際にＳＨＢが行う処理を表す。

【００９４】

ステップ６０２で、ＳＨＢはアクセス制御ルールとバージョン番号を受け取る。

【００９５】

ステップ６０４で、ＳＨＢはそのアクセス制御ポリシーのキャッシュを更新する。

【００９６】

ステップ６０６で、ＳＨＢはクライアント・サブスクリプション・フィルタとアクセス制御ポリシー・フィルタの論理積を計算する。

【００９７】

ステップ６０８で、ＳＨＢは上流のブローカに論理積を求めたサブスクリプションと使用する制御ルールのバージョン番号を伝搬する。

【００９８】

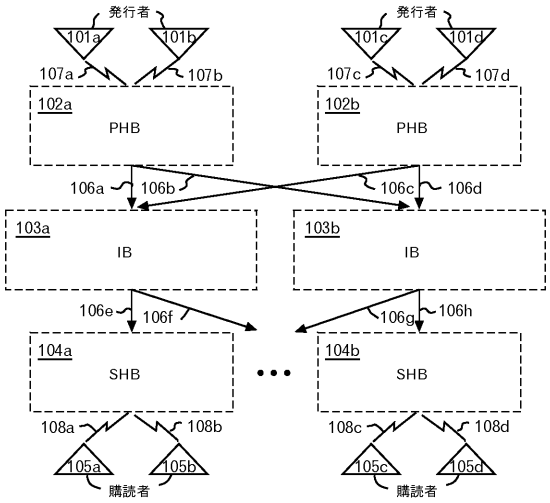
ステップ６１０で、ＳＨＢはこの最新のＡＣＬの変更と同じ制御バージョン番号をもつ

バッファに入れられたメッセージがあるかどうかを点検する。
【００９９】
ステップ６１０で「いいえ」の場合、ＳＨＢはそれに対してそれ以上なにも行わない（ブロック６１２）。
【０１００】
ステップ６１０で「はい」の場合、ＳＨＢは、これらメッセージの各々について、論理積を求めたサブスクリプションのどれかと一致するかどうかを点検する（ステップ６１４）。
【０１０１】
ステップ６１４で「いいえ」の場合、ＳＨＢはメッセージを廃棄する（ステップ６１６）。
【０１０２】
ステップ６１４で「はい」の場合、ＳＨＢは、このような論理積を求めたサブスクリプションについて、その制御バージョン番号がメッセージのものと同じかどうかを点検する（ステップ６１８）。
【０１０３】
ステップ６１８で「いいえ」の場合、ＳＨＢはメッセージを廃棄する（ステップ６１６）。
【０１０４】
ステップ６１８で「はい」の場合、ＳＨＢはメッセージを論理積を求めたサブスクリプションの購読者に送る（ステップ６２０）。
【０１０５】
図９は、新たなクライアントのサブスクリプションを受け取った際にＳＨＢが行う処理を表す。
【０１０６】
ステップ６２２で、ＳＨＢはクライアント・サブスクリプション・フィルタを受け取る。
【０１０７】
ステップ６２４で、ＳＨＢはアクセス制御ポリシーのキャッシュからクライアントのプリンシパルの最新のアクセス購読ルールを検索する。
【０１０８】
ステップ６２６で、ＳＨＢはクライアント・サブスクリプション・フィルタとアクセス制御ポリシー・フィルタの論理積を計算する。
【０１０９】
ステップ６２８で、ＳＨＢは上流のブローカに論理積を求めたサブスクリプションと使用する制御ルールのバージョン番号を伝搬する。
【０１１０】
図１０は、新バージョンのアクセス制御に関する情報を受け取った際ＰＨＢが行う処理を表す。
【０１１１】
ステップ６３０で、ＰＨＢはアクセス制御ルールとバージョン番号を受け取る。
【０１１２】
ステップ６３２で、ＰＨＢはそのアクセス制御ポリシーのキャッシュを更新する。
【０１１３】
図１１は、新たなデータ・メッセージを受け取った際ＰＨＢが行う処理を表す。
【０１１４】
ステップ６３４で、ＰＨＢはデータ・メッセージを受け取る。
【０１１５】
ステップ６３６で、ＰＨＢはメッセージが発行者のプリンシパルの最新の発行権と一致するかどうかを点検する。

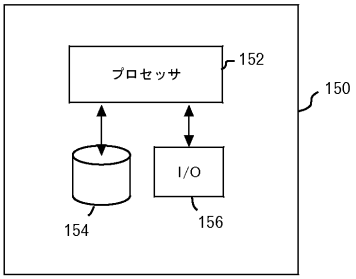
【０１１６】
ステップ６３６で「いいえ」の場合、ＰＨＢはメッセージを廃棄する（ステップ６３８）。
【０１１７】
ステップ６３６で「はい」の場合、ＰＨＢはメッセージの最新バージョン番号を使って制御バージョン番号を設定し、メッセージを送る（ステップ６４０）。
【０１１８】
図１２は、データ・メッセージを受け取った際にＩＢが行う処理を表す。
【０１１９】
ステップ６４２で、ＩＢはデータ・メッセージを受け取る。
【０１２０】
ステップ６４４で、ＩＢはメッセージの制御バージョンがＩＢの制御バージョン・ベクトルのエレメント以下であるかどうかを点検する。
【０１２１】
ステップ６４４で「はい」の場合、ＩＢはメッセージが下流からのサブスクリプションと一致するかどうかを点検する（ステップ６４６）。
【０１２２】
ステップ６４６で「いいえ」の場合、ＩＢはメッセージを廃棄する（ステップ６４８）。
【０１２３】
ステップ６４４で「いいえ」の場合もしくはステップ６４６で「はい」の場合、ＩＢはメッセージを下流に送る（ステップ６５０）。
【０１２４】
上記の処理ステップは例示的な性質のものであることを意図しており、そのため本発明のアクセス制御ポリシー配布およびメッセージ配送プロトコルはこれより少ないもしくは多い処理ステップ、他の処理ステップ、および上記処理ステップを別の順番で行うことができ、もしくはこれより少ないもしくは多い処理ステップ、他の処理ステップ、または上記処理ステップを別の順番で行うことができることは理解されるべきである。
【０１２５】
有利なことに、本明細書で説明したように、本発明の例示的な実施例によるサービス・モデルはシステム内の同じプリンシパルの代わりに全購読者に対して確定的かつ統一的なアクセス制御のセマンティクスを実質的に保証できる。このことは、ひとつまたは複数のブローカのクラッシュおよび再始動のためにひとつまたは複数のブローカに有効なアクセス制御ポリシーの非永続状態を失わせることになった場合でも当てはまる。また、ネットワーク内の少なくとも１つのリンクが途切れ、その接続が再確立されたことにより、そのリンクを通して送信される少なくとも１つのメッセージが脱落、重複、または順序を間違って配送されてしまう場合でさえも当てはまる。すなわち、同じプリンシパルの代わりに様々な購読者は、システム内の別のサブネットワークで接続されている場合でも、またそのサブネットワークが別の通信遅延およびネットワークもしくはルーティング・ブローカの障害を受ける場合であっても、まったく同じシーケンスのメッセージを受け取る（サブスクリプション・フィルタ差分を法として）。
【０１２６】
また、このようなサービス・モデルで、コンテンツベースのパブリッシュ／サブスクライブ・システムに適用できるコンテンツベース形態を使って発行と購読両方のアクセス制御を施行できること、および単にＳＨＮ以外の全ブローカがアクセス制御ルールを維持する必要なく購読者のアクセス制御に参加できることを可能にする。
【０１２７】
本明細書において、本発明の例示的な実施例を添付の図面を参照しながら説明してきたが、本発明はこのまったく同じ実施例に限定されるものではなく、本発明の範囲または精神を逸脱することなく当業者には他の様々な変更および修正が行えることは理解されるべ

きである。
【図面の簡単な説明】
【０１２８】
【図１】本発明のある実施例による、代表的なブローカのネットワークを含むコンテンツベースのパブリッシュ／サブスクライブ・システムの少なくとも一部を図示するブロック図である。
【図２】本発明のある実施例による、コンテンツベースのパブリッシュ／サブスクライブ・システムのひとつまたは複数のコンポーネントのコンピューティング・アーキテクチャを図示するブロック図である。
【図３】本発明のある実施例による、ブローカ・ネットワークの実施を図示する情報フロー図である。
【図４】本発明のある実施例による、サービス・モデルの代表的な実施を図示するブロック図である。
【図５】本発明のある実施例による、アクセス制御ポリシー配布およびメッセージ配送プロトコルの概要を図示するフロー図である。
【図６】本発明のある実施例による、アクセス制御ポリシー配布およびメッセージ配送プロトコルを実施するコンテンツベースのパブリッシュ／サブスクライブ・システムの一部を図示するブロック図である。
【図７】本発明のある実施例による、アクセス制御ポリシー配布およびメッセージ配送プロトコルを実施するコンテンツベースのパブリッシュ／サブスクライブ・システムの一部を図示するブロック図である。
【図８】本発明のある実施例によるアクセス制御ポリシー配布およびメッセージ配送プロトコルを図示するフロー図である。
【図９】本発明のある実施例によるアクセス制御ポリシー配布およびメッセージ配送プロトコルを図示するフロー図である。
【図１０】本発明のある実施例によるアクセス制御ポリシー配布およびメッセージ配送プロトコルを図示するフロー図である。
【図１１】本発明のある実施例によるアクセス制御ポリシー配布およびメッセージ配送プロトコルを図示するフロー図である。
【図１２】本発明のある実施例によるアクセス制御ポリシー配布およびメッセージ配送プロトコルを図示するフロー図である。

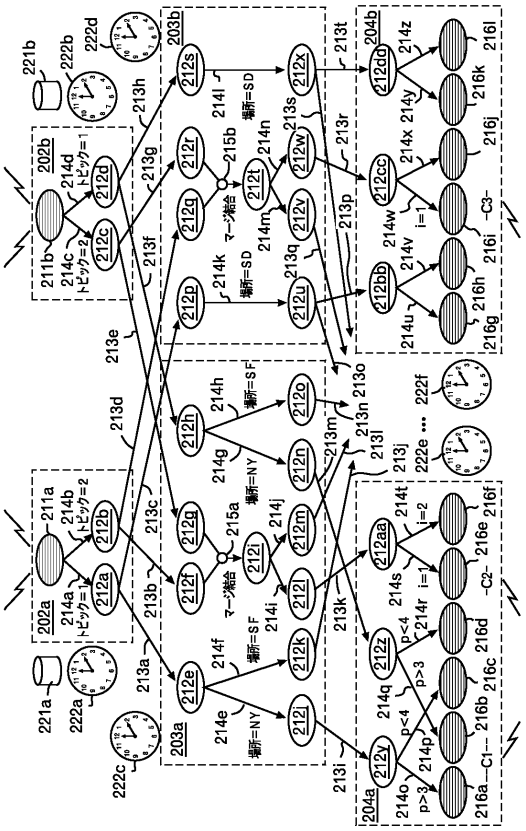
【図１】


発行者
101a
101b
101c
101d
107a
107b
107c
107d
102a
PHB
102b
PHB
106a
106b
106c
106d
103a
IB
103b
IB
106e
106f
106g
106h
104a
SHB
104b
SHB
108a
108b
108c
108d
105a
105b
105c
105d
購読者
購読者

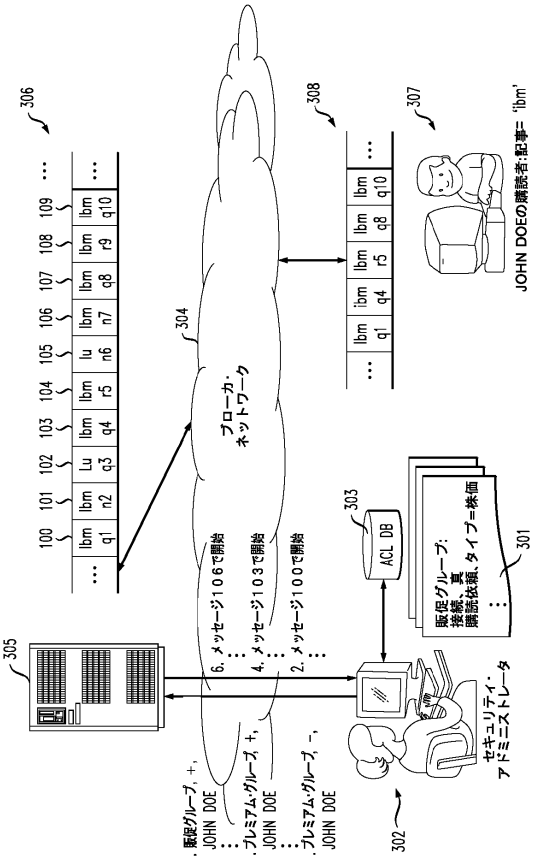
【図２】


プロセッサ
152
150
I/O
154
156

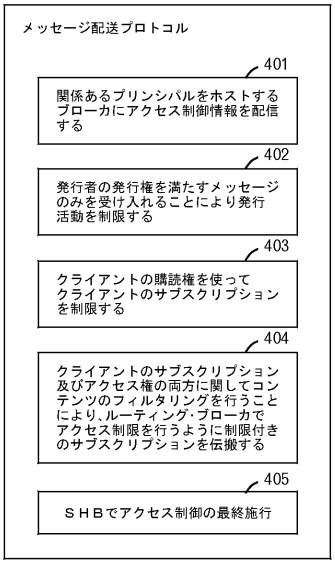
【図３】



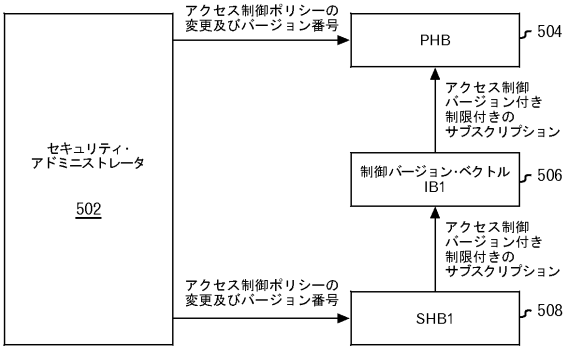
【図４】


306
308
307
304
ブローカ・ネットワーク
303
ACL DB
301
305
302
JOHN DOEの購読者:記事= 'ibm'
セキュリティ・アドミニストレータ
1. 販促グループ, +, JOHN DOE
3. プレミアム・グループ, +, JOHN DOE
5. プレミアム・グループ, -, JOHN DOE
6. メッセージ106で開始
4. メッセージ103で開始
2. メッセージ100で開始

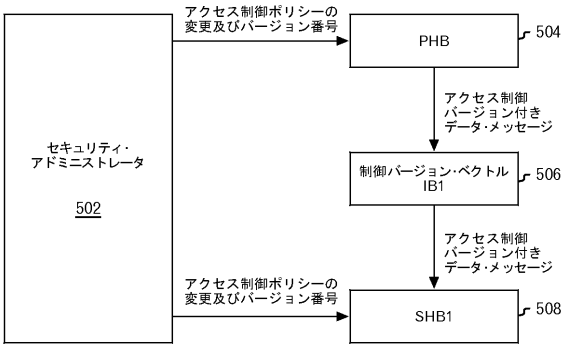
【図５】



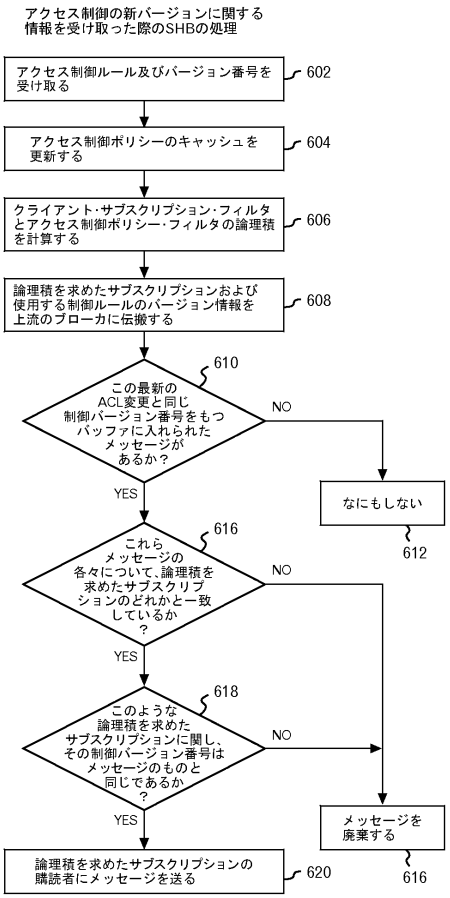
【図６】



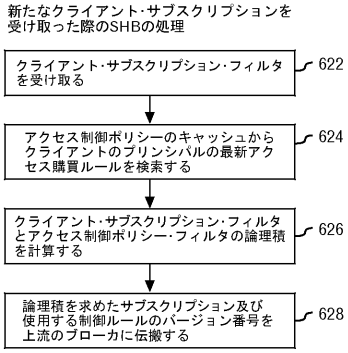
【図７】



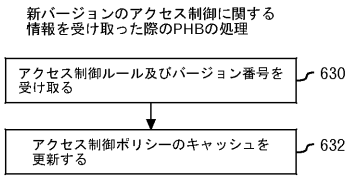
【図８】



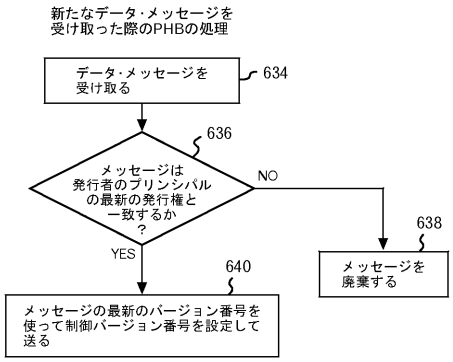
【図９】



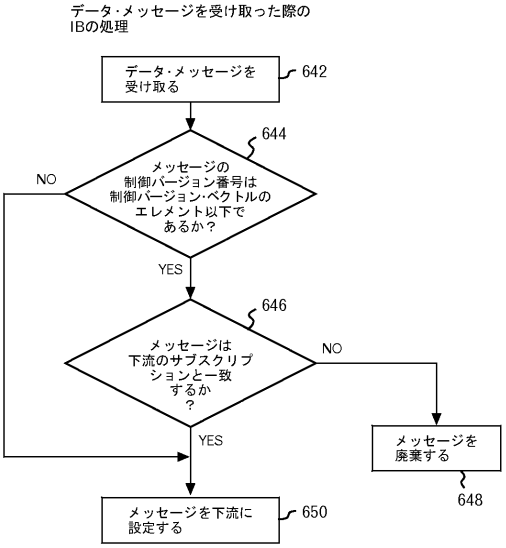
【図１０】



【図１１】


新たなデータ･メッセージを
受け取った際のPHBの処理
データ･メッセージを
受け取る
634
636
メッセージは
発行者のプリンシパル
の最新の発行権と
一致するか
？
NO
638
メッセージを
廃棄する
YES
640
メッセージの最新のバージョン番号を
使って制御バージョン番号を設定して
送る

【図１２】


データ･メッセージを受け取った際の
IBの処理
データ･メッセージを
受け取る
642
644
メッセージの
制御バージョン番号は
制御バージョン･ベクトルの
エレメント以下で
あるか？
NO
YES
646
メッセージは
下流のサブスクリプ
ションと一致
するか
？
NO
YES
メッセージを
廃棄する
648
メッセージを下流に
設定する
650

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 ユアンユアン、チャオ
アメリカ合衆国 １０５９１ ニューヨーク州 タリータウン ブロードウェイ・ストリート ２１９ アパートメント ３
(72)発明者 ダニエル、チャールズ、スターマン
アメリカ合衆国 ９４０２４ カリフォルニア州 ロスアルトス ダミアン・ウェイ ９６０
(72)発明者 スメール、クメール、ボーラ
アメリカ合衆国 １００２７ ニューヨーク州 ニューヨーク ブロードウェイ ３１１７ アパートメント ４７

Ｆターム(参考) 5B017 AA03 BA06 BB06 CA16
5B285 AA01 AA05 BA07 CA02 CA03 CA06 CA12 DA05
5J104 AA07 AA16 EA03 KA01 KA04 NA05 NA27 NA38 PA14