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

特許第5860204号
(P5860204)

(45)発行日　平成28年2月16日(2016.2.16)　(24)登録日　平成27年12月25日(2015.12.25)

(51)Int.Cl.		F I		
G06F 13/00	(2006.01)	G06F	13/00	520B
G06F 21/33	(2013.01)	G06F	21/33	
G06Q 30/06	(2012.01)	G06Q	30/06	122
H04L 9/32	(2006.01)	H04L	9/00	675B

請求項の数 12　(全 35 頁)

(21)出願番号　特願2010-176024(P2010-176024)
(22)出願日　平成22年8月5日(2010.8.5)
(62)分割の表示　特願2004-523114(P2004-523114)の分割
原出願日　平成15年7月10日(2003.7.10)
(65)公開番号　特開2011-8803(P2011-8803A)
(43)公開日　平成23年1月13日(2011.1.13)
審査請求日　平成22年9月3日(2010.9.3)
審判番号　不服2014-21410(P2014-21410/J1)
審判請求日　平成26年10月23日(2014.10.23)
(31)優先権主張番号　10/199,967
(32)優先日　平成14年7月19日(2002.7.19)
(33)優先権主張国　米国(US)

(73)特許権者　508041080
オープン　インヴェンション　ネットワーク　リミテッド　ライアビリティ　カンパニー
アメリカ合衆国　ニューヨーク州　１０５７６　ポンド　リッジ　ピーオーボックス　３５７
(74)代理人　100092093
弁理士　辻居　幸一
(74)代理人　100082005
弁理士　熊倉　禎男
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100086771
弁理士　西島　孝喜

最終頁に続く

(54)【発明の名称】電子商取引コミュニティネットワーク及びコミュニティ間／コミュニティ内の安全な経路指定の実施

(57)【特許請求の範囲】
【請求項１】
少なくとも１つのネットワークによって結合されたサーバ群の送信元コミュニティ及び宛先コミュニティにそれぞれ属する送信元サーバ及び宛先サーバに関し、前記送信元サーバから前記宛先サーバまでの電子商取引文書の配信のためにセキュリティ・チェーンを確立するための方法であって、
前記送信元サーバ又は当該送信元サーバの委任サーバのリクエストにより、前記送信元コミュニティ及び宛先コミュニティに対して相互に受け入れられる電子文書交換のセキュリティ信任を定める処理であって、前記セキュリティ信任には、少なくとも、ＳＡＭＬ（Security Assertion Markup Language）認証に基づくＳＡＭＬアサーション(assertion)の生成を含み、
ＳＡＭＬ認証手段が、前記送信元サーバのエンベロープ・プロトコルから抽出したパスワードと、登録されているパスワードとを比較して認証を行い、認証が成功した場合には前記ＳＡＭＬアサーションを生成して署名する処理と、
前記送信元サーバが、前記ＳＡＭＬアサーションの電子証明を前記ＳＡＭＬ認証手段から受け取る処理と、
前記送信元サーバが、電子メッセージのエンベロープ・プロトコルに従って、電子エンベロープにおいて前記ＳＡＭＬアサーションの電子証明及び電子商取引文書をパッケージする処理と、
前記ＳＡＭＬアサーションの電子証明における電子署名がレジストリに登録されている

かにより、前記電子文書交換のセキュリティ信任と整合する１以上の信頼できるコネクタデバイスを決定し、当該信頼できるコネクタデバイスを通って前記宛先サーバまで前記電子エンベロープをネットワークを介して到達させるための経路を指定する処理と、
前記経路を介したネットワーク上で前記電子エンベロープを前記宛先サーバまで送信する処理と、
を含むことを特徴とする方法。
【請求項２】
前記電子エンベロープを前記送信元サーバから受け取る処理と、
前記ＳＡＭＬアサーションの電子証明における電子署名と、サーバ群の前記宛先コミュニティに登録され保存された前記送信元コミュニティに対する電子署名とを比較する処理と、
前記ＳＡＭＬアサーションの電子証明を転送した送信元サーバを含む前記送信元コミュニティが電子商取引文書を送るのに信頼できるものであるかどうかを宛先コミュニティのレジストリサーバから判断する処理と、
をさらに含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記ＳＡＭＬアサーションの電子証明における電子署名が、前記レジストリに登録されているかにより信頼できると判断した、サーバ群の少なくとも１つの媒介コミュニティにおける１以上のコネクタデバイスを通して、前記電子エンベロープの経路を指定する処理と、
前記電子エンベロープを前記媒介コミュニティのための認証ゲートウェイで受け取り、そして前記ＳＡＭＬアサーションの電子証明における電子署名と、前記媒介コミュニティに登録され保存された送信元コミュニティに対する電子署名とを比較する処理と、
前記媒介コミュニティに対応する媒介ＳＡＭＬアサーションの電子証明を、ＳＡＭＬ認証手段から取得する処理と、
前記媒介ＳＡＭＬアサーションの電子証明を前記電子エンベロープと併せて電子エンベロープ内にパッケージする処理と、
前記注釈付き電子エンベロープを、前記ネットワークを介して前記宛先サーバに転送する処理と、
をさらに含むことを特徴とする請求項１に記載の方法。
【請求項４】
前記電子エンベロープを前記宛先サーバで受け取る処理と、
前記媒介コミュニティの前記媒介ＳＡＭＬアサーションの電子証明における電子署名と、前記宛先コミュニティによって登録され保存された媒介コミュニティに対する電子署名とを比較する処理と、
前記送信元コミュニティの前記ＳＡＭＬアサーションの電子証明における電子署名と、前記宛先コミュニティによって登録され保存された送信元コミュニティに対する電子署名とを比較する処理と、
前記ＳＡＭＬアサーションの電子証明を転送した送信元サーバを含む前記送信元コミュニティが、電子商取引文書を送るのに信頼できるものであるかどうかを宛先コミュニティのレジストリサーバから判断するステップと、
を含むことを特徴とする請求項３に記載の方法。
【請求項５】
送信元サーバから電子商取引文書を宛先サーバにおいて安全に受け取るために経路指定する方法であって、前記送信元サーバ及び前記宛先サーバのそれぞれはネットワークによって結合されたサーバ群の送信元コミュニティ及び宛先コミュニティに属し、
前記宛先サーバ又は当該宛先サーバの委任サーバのリクエストにより、前記送信元サーバ又は前記送信元コミュニティが使用するトランスポート／エンベロープ・プロトコルを用いて１以上の電子文書の経路を定める処理であって、前記トランスポート／エンベロープ・プロトコルは、少なくともトランスポート及びエンベロープの対を含み、指向グラフ

として表される経路指定法則に従い、送信元及び宛先コミュニティに共通のトランスポート・プロトコル及びエンベロープ・プロトコルがない場合には、送信元コミュニティ及び宛先コミュニティ間の経路上に１以上の媒介コミュニティを加え、トランスポート・プロトコル又はエンベロープ・プロトコルの少なくとも何れか１つを共通してもつ前記媒介コミュニティへ前記電子商取引文書が伝搬される当該処理と、

電子商取引文書及びＳＡＭＬアサーションの電子証明を含む電子エンベロープを前記送信元サーバから受け取る処理と、

前記送信元サーバを認証するため、前記ＳＡＭＬアサーションの電子証明における電子署名と、前記宛先コミュニティに登録され保存された前記送信元コミュニティに対する電子署名とを比較する処理と、

前記ＳＡＭＬアサーションの電子証明を転送した認証済み送信元サーバを含む前記送信元コミュニティが、電子商取引文書を送るのに信頼できるものであるかどうかを宛先コミュニティのレジストリサーバから判断する処理と、

を含むことを特徴とする方法。

【請求項６】

少なくとも媒介コミュニティを介して、前記送信元サーバから、前記媒介コミュニティに対応する媒介ＳＡＭＬアサーションの電子認証をさらに含む電子エンベロープを受け取る処理と、

前記媒介コミュニティのＳＡＭＬアサーションの電子証明における電子署名と、前記宛先コミュニティによって登録され保存された媒介コミュニティに対する電子署名とを比較する処理と、

をさらに含むことを特徴とする請求項５記載の方法。

【請求項７】

少なくとも１つのネットワークによってエンベロープ変換ゲートウェイ装置を介して結合されたサーバ群の送信元コミュニティ及び宛先コミュニティにそれぞれ属する送信元サーバ及び宛先サーバに関し、前記送信元サーバから前記宛先サーバまで電子商取引文書を安全にルーティング（経路指定）するための方法であって、

前記送信元サーバ又は当該送信元サーバの委任サーバのリクエストにより、サーバ群の前記送信元コミュニティ及び前記宛先コミュニティに対して相互に受け入れられる、電子文書交換のセキュリティ信任を定める処理であって、前記セキュリティ信任には、少なくとも、ＳＡＭＬ（Security Assertion Markup Language）認証に基づくＳＡＭＬアサーション(assertion)の生成を含み、

第１のセキュリティ手段が、前記送信元サーバのエンベロープ・プロトコルから抽出したパスワードと、登録されているパスワードとを比較して認証を行い、認証が成功した場合には前記ＳＡＭＬアサーションを生成して署名する処理と、

第１のセキュリティ認証情報（security credential)を前記第１のセキュリティ手段から受け取る処理と、

前記ＳＡＭＬアサーションの電子証明における電子署名が、レジストリに登録されているかにより、相互に受け入れられる前記電子文書交換のセキュリティ信任と整合する認証コネクタデバイスを決定し、前記宛先サーバまでの認証ゲートウェイ装置を通るルーティングが決定する処理と、ここで、前記認証ゲートウェイ装置は、前記第１のセキュリティ認証情報を有効にする手段、前記電子商取引文書を解読してこれを再び暗号化する手段、第１の電子エンベロープ・プロトコルを第２の電子エンベロープ・プロトコルに変換する手段、及び前記第２の電子エンベロープ・プロトコルに従って、第２のセキュリティ認証情報を前記電子商取引文書と併せて転送する手段を含み、

前記第１の電子エンベロープ・プロトコルに従って、前記宛先サーバまでの認証ゲートウェイ装置を通る前記ルーティングを用いて、前記第１のセキュリティ認証情報及び前記電子商取引文書をネットワークを介して転送する処理と、

を含むことを特徴とする方法。

【請求項８】

前記ネットワークを介した認証ゲートウェイ装置からの電子エンベロープを、前記宛先コミュニティで受け取る処理と、
前記第２のセキュリティ認証情報と、前記宛先コミュニティによって登録され保存された認証ゲートウェイ装置に対する電子署名とを比較する処理と、
前記認証ゲートウェイ装置及び前記送信元コミュニティが電子商取引文書を送るのに信頼できるものであるかどうかを宛先コミュニティのレジストリサーバから判断する処理と、
を含むことを特徴とする請求項７に記載の方法。
【請求項９】
第１のセキュリティ手段が前記送信元サーバを認証する処理は、
レジストリサーバと媒介コネクタデバイスとの間で通信可能であり、第１のセキュリティ手段が前記送信元サーバを認証するために前記レジストリサーバへのアクセスが可能であること、及び、
前記送信元サーバは、第１のセキュリティ手段によって前記送信元サーバを認証するために前記媒介コネクタデバイスを呼び出し、そして前記第１のセキュリティ認証情報を、前記第１のセキュリティ手段から前記送信元サーバへ返送すること、
を含むことを特徴とする請求項７又は８のいずれか１項に記載の方法。
【請求項１０】
エンベロープ変換ゲートウェイ装置を介して送信元サーバから電子商取引文書を宛先サーバにおいて安全に受け取るために経路指定する方法であって、前記送信元サーバ及び前記宛先サーバのそれぞれはネットワークによって結合されたサーバ群の送信元コミュニティ及び宛先コミュニティに属し、
前記宛先サーバ又は当該宛先サーバの委任サーバのリクエストにより、前記送信元サーバ又は前記送信元コミュニティが使用するトランスポート／エンベロープ・プロトコルを用いて１以上の電子文書交換の経路を定める処理であって、前記トランスポート／エンベロープ・プロトコルは、少なくともトランスポート及びエンベロープの対を含み、指向グラフとして表される経路指定法則に従い、送信元及び宛先コミュニティに共通のトランスポート・プロトコル及びエンベロープ・プロトコルがない場合には、送信元コミュニティ及び宛先コミュニティ間の経路上に１以上の媒介コミュニティを加え、トランスポート・プロトコル又はエンベロープ・プロトコルの少なくとも何れか１つを共通してもつ前記媒介コミュニティへ前記電子商取引文書が伝搬される当該処理と、
前記ＳＡＭＬアサーションの電子証明における電子署名がレジストリに登録されているかに基づき、前記電子文書交換のセキュリティ信任と整合する認証コネクタデバイスを決定し、当該認証コネクタデバイスを介して、前記送信元コミュニティからの電子商取引文書及び第２のセキュリティ認証情報を含む電子エンベロープを認証ゲートウェイ装置から受け取る処理と、ここで、前記認証ゲートウェイ装置は、前記送信元コミュニティからの第１のセキュリティ認証情報（security credential)を有効にする手段、前記電子商取引文書を解読してこれを再び暗号化する手段、第１の電子エンベロープ・プロトコルを第２の電子エンベロープ・プロトコルに変換する手段、前記第２の電子エンベロープ・プロトコルに従って第２のセキュリティ認証情報を前記電子商取引文書と併せて転送する手段の一つ以上を備え、
前記送信元サーバを認証するため、前記第２のセキュリティ認証情報の電子署名と、前記宛先コミュニティに登録され保存された前記認証ゲートウェイ装置に対する電子署名とを比較する処理と、
前記認証ゲートウェイ装置及び認証済み送信元サーバを含む前記送信元コミュニティが、電子商取引文書を送るのに信頼できるものであるかどうかを宛先コミュニティのレジストリサーバから判断する処理と、
を含むことを特徴とする方法。
【請求項１１】
サーバ群の商取引コミュニティのネットワークを確立する方法であって、各商取引コミ

ュニティは、ローカルレジストリサーバと、他の商取引コミュニティに存在するサーバに利用可能な少なくとも１つのサービス手段とを有し、
第１の商取引コミュニティ内の少なくとも１つのグローバル・イエローページ・サーバに登録して保存する処理であって、少なくとも２つの商取引コミュニティ間でのオペレーティング取り決めと、外部ゲートウェイ装置のポート構成及び他の商取引コミュニティによって使用可能なアドレスと、前記第１の商取引コミュニティの電子セキュリティ認証情報とを登録して保存する前記処理と、
前記外部ゲートウェイ装置を介して前記他の商取引コミュニティにアクセスできる、前記第１の商取引コミュニティでの複数のサービス手段を、グローバル・イエローページと併せて登録する処理と、
前記サーバ群の前記第１の商取引コミュニティが前記他の商取引コミュニティからの要求に応じるために、１以上の前記サービス手段の詳細と、前記外部ゲートウェイ装置のポート構成及びアドレスとを、少なくとも１つのグローバル・ホワイトページ・サーバに登録する処理と、
前記グローバル・イエローページ・サーバ及び前記グローバル・ホワイトページ・サーバが前記他の商取引コミュニティに属するサーバからの要求に応答する処理と、
を含むことを特徴とする方法。
【請求項１２】
前記商取引コミュニティのネットワークにおけるホストコミュニティが前記グローバル・イエローページを管理し、
新しいコミュニティが、前記商取引コミュニティのネットワークに接続し、前記グローバル・イエローページ・サーバからのサービス手段に対する参照(reference)を見つけるために認証され、さらに前記ホストコミュニティのオペレーティング取り決めと、外部ゲートウェイ装置のポート構成及びアドレスと、電子セキュリティ認証情報とを交換することにより、前記グローバル・ホワイトページ・サーバから前記サービス手段の詳細にアクセスできるようになることを特徴とする請求項１１に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
（著作権情報）
本特許文献の開示の一部は、著作権の保護を受ける題材を含んでいる。著作権者は、本特許文献が米国特許商標庁の特許ファイル又は記録において公開されたときに、誰もが特許文献又は特許の開示を複写することに異議はないが、他の場合には、如何なる場合にも全ての著作権を留保する。
【０００２】
本発明は、コミュニティ内の参加者間、及び、コミュニティのネットワークに入っているコミュニティ内の参加者間で、電子商取引文書の通信をサポートするシステム及びプロトコルに関する。より具体的には、本発明は、電子商取引文書を参加者間において経路指定し、経路に沿った送信を保護するためのシステム及びプロトコルに関する。
【背景技術】
【０００３】
企業間（Ｂ２Ｂ）及びアプリケーション間（Ａ２Ａ）の電子商取引は、電子データ交換（ＥＤＩ）のためのこれまでのプロトコルを切り替えつつある。企業がＢ２Ｂ及びＡ２Ａシステムを用いてその効率性を改善しようと努力するにつれて、多数の互換性のないプラットフォーム及び競合する規格が登場した。互換性のある規格においては、満たされるべき溝が残っている。例えば、業界は、何が単純なウェブサービスであるかを定義した。単純なウェブサービスに関する規格は、ＵＤＤＩ、ＷＳＤＬ、ＸＳＤＬ、及びＳＯＡＰを含む。しかし、これらの規格は、実用的なＢ２Ｂ及びＡ２Ａの電子商取引に対するセキュリティ、信頼性、管理可能性、及び構成の要求を完全に意味するものではない。プロセスの流れに基づく会話及び共同ウェブサービスの構成は、共同する複雑なウェブサービスの構

成要素であり、包括的な又は統合された規格を目的とするものではない。
【０００４】
Ｂ２Ｂ及びＡ２Ａの電子商取引に適用可能な規格を拡張する多数の業界提案がある。構成の成果には、ＯＡＳＩＳによるｅｂＸＭＬ／ＢＰＳＳ、ＩＢＭによるＷＳＦＬ、マイクロソフトからのＸＬＡＮＧを含む。やり取りの成果にはは、ＯＡＳＩＳによるｅｂＸＭＬ／ＴＲＰ及びマイクロソフトのＷＳ－ｒｏｕｔｉｎｇを含む。有力なセキュリティの成果には、ＩＢＭ及びマイクロソフトによるＷＳ－ｓｅｃｕｒｉｔｙであり、さらに、ＯＡＳＩＳにおいてはＳＡＭＬと呼ばれる補完的なセキュリティの成果がある。信頼性に対しては、マイクロソフトからの提案、ＯＡＳＩＳによるｅｂＸＭＬ／ＴＲＰ、及びＩＢＭによるＨＴＴＰＲがある。Ｗ３Ｃは、これらの領域すべてにおける規格化に対処するものである。主要な業界当事者は、ＷＳＩと呼ばれる対抗するコンソーシウムを形成した。プロセスの流れに対しては現実的な規格は全く存在しないが、プロセスの流れに固有の実施が多数行われている。管理可能性に対しては、電子商取引に含まれるエンティティのポリシー及び能力を特定することにより、ウェブサービスの相互運用性を推進する情報を手中的に定義することが有益になる。集中的な定義に対する１つの業界標準は、ＯＡＳＩＳにより普及されているｅｂＸＭＬ　ＣＰＰ／ＣＰＡ契約の定義である。
【０００５】
したがって、ＳＯＡＰ、ＵＤＤＩ、ｅｂＸＭＬ、ＷＳＤＬ、ＷＳ－ｓｅｃｕｒｉｔｙ、ＳＡＭＬ、及びＸＳＤＬを含む多数の関連のあるウェブサービス規格に存在する溝を受け入れ、且つ統合して満たす方法及び構造を考案する機会が生じる。全体的にみれば、終端間のサービス、及びビジネスをすることを望むエンティティ間での安全な電子商取引文書を供給できるようにすることが役に立つ。
【発明の概要】
【課題を解決するための手段】
【０００６】
本発明は、コミュニティのネットワークを確立し、異なるインターフェースを有するコミュニティ間で文書の経路指定をし、このことを信頼できる信用性のある方法により行う装置及び方法を含む。本発明の特定の態様は、特許請求の範囲、明細書、及び図面に述べられる。
【図面の簡単な説明】
【０００７】
【図１】幾つかのコミュニティに属する幾つかのエンティティを示す。
【図２】代替的な通信チャネルを有するエンティティ又はコネクタを示す。
【図３】同様な通信チャネルを用いて、２つのコネクタ間でハブとして作用するコネクタを示す。
【図４】コミュニティネットワークにおけるコミュニティ間のコミュニティ境界にわたる通信を示す。
【図５】コミュニティネットワークにおけるコミュニティ間のコミュニティ境界にわたる通信を示す。
【図６】媒介コミュニティ、一連の通信を示す。
【図７】変換サービスのための媒介コミュニティの用途を示す。
【図８】コミュニティ内の経路指定をサポートする電子レジストリデータのブロック図である。
【図９】より詳細な電子レジストリ図である。
【図１０】コミュニティ間の経路指定をサポートする電子レジストリデータのブロック図である。
【図１１】経路をコンパイルすることができるＸＭＬフォーマットを示す。
【図１２】経路をコンパイルすることができるＸＭＬフォーマットを示す。
【図１３】コミュニティ内及びコミュニティ間における経路指定の高レベルの図である。
【図１４】コミュニティ内及びコミュニティ間における経路指定の高レベルの図である。

【図１５】コミュニティ内におけるセキュリティの実施を示す。
【図１６】コミュニティ間におけるセキュリティの実施を示す。
【図１７】代行セキュリティサービスを示す。
【図１８Ａ】ゲートウェイに対する認証代行を示す。
【図１８Ｂ】ゲートウェイに対する認証代行を示す。
【図１９Ａ】ＭＭＬ安全プロトコルとＳＡＭＬ安全プロトコルと間の変換が、コミュニティ間の通信まで拡張された状態を示す。
【図１９Ｂ】ＭＭＬ安全プロトコルとＳＡＭＬ安全プロトコルと間の変換が、コミュニティ間の通信まで拡張された状態を示す。
【図２０】付加的なセキュリティ用途例のブロック図である。
【図２１】付加的なセキュリティ用途例であり、図２０の設計を用いたレジストリサービスのローカル認証を示す。
【図２２】レジストリサービスのリモート認証のための付加的なセキュリティ用途例の変形態様である。
【図２３】付加的なセキュリティ用途例であり、ローカル及びリモート認証を示す。
【図２４】付加的なセキュリティ用途例であり、ローカル及びリモート認証を示す。
【図２５】付加的なセキュリティ用途例であり、文書サービスのサブスクリプションに対する属性アサーションの取得を示す。
【図２６】通信ネットワークの確立を示す。
【図２７】通信ネットワークの確立を示す。
【発明を実施するための形態】
【０００８】
以下の詳細な説明は、図面を参照して行われる。好ましい実施形態は、特許請求の範囲によって定められる本発明を説明するために記載されるものであって、本発明の範囲を限定するものではない。当業者であれば、以下の説明に関して種々の等価な変形物を認識するであろう。
【０００９】
図１は、コミュニティ及びコミュニティのネットワークを示す。これらのコミュニティにおいては、コミュニティは、コミュニティの部分であるユーザ、会社、サービス、及びコネクタのような情報を含むローカルレジストリを維持する。コミュニティは、市場、エンタープライズ、又はサブエンタープライズとすることができる。コミュニティは、１つ又はそれ以上のネットワークに属することができる。典型的には、コミュニティ及びネットワークは、幾つかの共通の企業利益を有する。相互運用性は、１つ又はそれ以上のコミュニティのネットワークにおけるメンバコミュニティ間にある。ネットワークは、金市場ネットワーク１、貴金属市場ネットワーク２、プライベート・ネットワーク３、及びグローバル取引ウェブネットワーク４を含む。この図においては、金市場ネットワーク１及び貴金属市場ネットワーク２は、グローバル取引ウェブネットワーク４の中に含まれている。貴金属市場ネットワーク２は、金市場１４及び銀市場１３を含む。金市場の顧客は、銀市場１３で銀を取引することができ、銀市場の顧客は、金市場１４で取引することができる。一方のコミュニティ、ＰＱＲエンタープライズ１７は、金市場ネットワーク１、プライベート・ネットワーク３、及びグローバル取引ウェブネットワーク４に属し、他方のコミュニティ、ＡＢＣ大サプライヤ１８は、プライベート・ネットワーク３に属する。この図においては、ＸＹＺ金市場１４は、金取引のための市場又はコミュニティである。エンタープライズは、このコミュニティに属する。ＰＱＲエンタープライズ１７のようにこれ自体でコミュニティを形成したエンタープライズは、金市場ネットワーク１に属する。これらのコミュニティは、金市場ネットワーク１の部分でもあり、グローバル取引ウェブネットワーク４の部分でもある。小サプライヤ１５は、金市場コミュニティの部分である。他のエンタープライズ１６は、金市場ネットワーク１の部分のコミュニティである。ＸＹＺ金市場１４と、その他の金市場エンティティ１５ないし１７との接続は、金市場がエンタープライズ（コミュニティその他の）間のすべてのトラフィックを要求することを表し

ている。例えば、請求書及びビジネス・インテリジェンス情報の収集といった、ＸＹＺ金市場１４を通って経路指定されるべき金取引処理する。ＰＱＲエンタープライズ１７は、金市場の一部であり、さらに、サプライヤ１８と共に、ローカルプライベート・ネットワークの一部である。小サプライヤ１５は、これ自体ではコミュニティを形成することを望まないが、代わりに、金属市場のレジストリにおいて、ユーザ、組織、サービス、及び変換のようなメタデータを登録する個々の小サプライヤとすることができる。一方、ＡＢＣ大サプライヤ１８は、それ自体のプライベート・ネットワークを形成した。というのは、例えば、そのメタデータ、内部バックオフィスシステム、及び一般的な公衆のアクセスから隠れた変換を維持することを望み、それらが相当な費用で作られたからである。ＰＲＱ１７は、ＡＢＣのクライアントであるため、プライベート・ネットワーク３に参加している。金融サービスプロバイダのＤＥＦ金融１２は、グローバル取引ウェブネットワーク１４内のすべての人に金融サービスを与えることを望み、したがって、これ自体のコミュニティを形成し、グローバル取引ウェブルート１１に登録する。コミュニティのネットワークは、コミュニティのグローバル・レジストリを利用可能にする。グローバル・レジストリは、コミュニティの検索を可能にし、及び該コミュニティに対する又は外部コネクタに対する１つ又はそれ以上の経路の判断を可能にし、これを通して、該コミュニティに向けられた電子商取引文書の経路指定をすることができる。一方のコミュニティから別のコミュニティに経路指定される文書は、２つのコミュニティのための外部コネクタ間で直接経路指定することもできるし、又は、１つ又はそれ以上の媒介コミュニティを通して間接的に経路指定することもできる。さらに、コミュニティを含むトランザクションのための企業及びセキュリティ法則を定義して、コミュニティのレジストリ内に維持することができる。一般には、図１は、電子商取引フラットフォームにおける相互運用性のための弾みをつけるエンティティ及びコミュニティの混合された忠実性を示している。

【００１０】

コネクタとは、他のアプリケーションと通信するアプリケーションの一般的な用語である。コネクタは、ハブ、ゲートウェイ、外部ポート、集中コネクタなどとして機能する他のコネクタにより、ピアツーピア（Ｐ２Ｐ）ベースであるか又は指向ベースで通信することができる。Ｐ２Ｐ通信するコネクタは、同じトランスポート／エンベロープ・プロトコルを用いる他のコネクタと通信することができる。Ｐ２Ｐ通信するコネクタは、任意的に、同じトランスポート／エンベロープ・プロトコルを用いないコネクタと通信しようとする場合に、変換サービスを行う他のハブコネクタの援助を得ることができる。指向ベースで通信するコネクタは、経路指定法則によりハブコネクタを通して通信する。コネクタにおける経路指定法則は、１つ又はそれ以上のトランスポート／エンベロープ・プロトコルの１つ又はそれ以上のハブ及びスポーク・トポロジを支持する指向グラフにマップすることができる。ハブ及びスポーク・トポロジは、１つ又はそれ以上の層において、通信をスポークに沿って、ハブまで向けられる。このことは、請求書作成発行、ビジネス・インテリジェンス収集、トラッキング、監査、会計その他のような集中サービスを可能にする。多数のハブ及びスポーク組織は、図２に示されるように、同じコネクタをオーバレイして、異なるトランスポート／エンベロープ・プロトコル及び技術をサポートすることができる。例えば、ＨＴＴＰ又はＨＴＴＰＳを用いるのではなく、Ｓｏｎｉｃをトランスポート技術として用いるためには、より強いハブ及びスポーク構成が必要になることがある。任意的に、通信経路は、送信元及び宛先が同じコミュニティの一部であるかどうかによって決まる。（コミュニティ全体を含むことができる）サブコミュニティ内では、集中機能は不要であり、コネクタ間においてはＰ２Ｐ通信が可能にされ、これは、或いは、他のサブコミュニティの宛先と通信する場合には、親コネクタと通信するようにされる。

【００１１】

コネクタは、単純コネクタ（時には、単純にコネクタと呼ばれる）、ハブ（時にはゲートウェイ又はルータと呼ばれる）、又は集中コネクタと表示が付される。或いは、これらは、機能により述べることができる。単純コネクタは、同じサブコミュニティのコネクタ間でＰ２Ｐ通信可能であるとき以外は、ハブコネクタにより通信するように指示される。

いわゆるハブは、明確にこれらに導かれたか又はリンクされたコネクタにより用いられる。ハブは、１つより多い機能で作用することができ、したがって、送信元から宛先までの経路において、１度以上現れることになる。ハブは、電子商取引文書又はメッセージを転送する。ハブは、さらに、通常のエンベロープ・プロトコルをサポートするトランスポート・プロトコルにおいて変換することができる。例えば、ハブは、エンベロープ・プロトコルを変換し、さらに、受信によってではなく、送信によって、異なるトランスポート・プロトコルを実施することができる。集中コネクタは、これらに対して明確に導かれていないか又はリンクされていないコネクタにより用いることができるハブの特別な例である。例えば、経路指定法則に従って、コネクタを送信元からトラバースすることが、宛先によって用いられるトランスポート／エンベロープ・プロトコルをサポートするいずれのハブにも導かない場合に、集中コネクタが変換機能を行うことは有益である。

【００１２】

図２は、３つのコネクタ、すなわち、単純なコネクタ２０１、及び一対のハブ２０２ないし２０３を示し、一方はゲートウェイ２０３と呼ばれる。コネクタ２０１は、トランスポート／エンベロープ・プロトコルがＳＯＡＰ／ＨＴＴＰ２０４である場合には、通信をハブ２０２に対して向け、ＭＭＬ／Ｓｏｎｉｃ２０５を用いる場合には、ハブ２０３に向ける経路指定法則により拘束される。事実上、子２０１は、親２０２ないし２０３を有する。関連のある親は、用いられる通信プロトコル２０４ないし２０５によって決まる。通信プロトコルのための指向経路のオーバレイは、トランスポート・セキュリティ・プロトコルによって、さらにオーバレイされるため、親を通る経路は、トランスポート／エンベロープ／トランスポート・セキュリティ・プロトコルのトリプレットによって決まる。或いは、ここで用いられるトランスポート／エンベロープ・プロトコルは、カプセル化及びトランスポートの両方をサポートする単一の統一プロトコルのことを指すことができる。現在、トランスポート・プロトコル及びエンベロープ・プロトコルは区別できるものであるが、トランスポート／エンベロープ・プロトコルという用語は、どのような近い将来にも統一されたプロトコルを含むことが意図される。

【００１３】

図３ないし図７は、送信元Ａ及び宛先Ｂの異なる関係を示す。図３においては、送信元３０１及び宛先Ｂは、同じコミュニティにある。これら両方は、通信をＭＭＬＳｏｎｉｃ３０４、３０５によりハブ３０３に向ける経路指定法則によって、ハブ３０３に導く。図４においては、送信元４０１及び宛先４０２は、コミュニティ境界４０３により分けられた異なるコミュニティにある。送信元及び宛先は、ＳＯＡＰ／ＨＴＴＰＳプロトコル４０６、４０７が用いられる場合には、それぞれ、ハブ４０４及び４０５により通信するように指示される。コミュニティ間の通信は、外部コネクタを介するものであるため、この例におけるハブは、さらに、他のコミュニティにアクセス可能なものとして登録された外部コネクタである。図５においては、送信元５０１及び宛先５０２は、ここでも、コミュニティ境界５０３により分けられている。送信元５０１は、ｅｂＸＭＬ／ＨＴＴＰＳプロトコル５０７により通信するように指示されている。ハブ５０５、５０６は、中央コネクタとして考えることができ、ハブ５０４及びコネクタ５０２は、これに対して明確に方向付けられ又はリンクされているわけではない。宛先５０２は、ＭＭＬ／ＨＴＴＰＳプロトコルを用いると仮定する。ハブ５０４は、変換能力をもたないが、ハブ５０５及び５０６はこの能力をもつ。ハブの共通プロトコルは、ＳＯＡＰ／ｓｏｍｅトランスポートである。それぞれのハブは、ｅｂＸＭＬ／ＨＴＴＰＳをＳＯＡＰ／ｓｏｍｅトランスポート５０５に変換し、ＭＭＬ／ＨＴＴＰＳも同じようにＳＯＡＰ／ｓｏｍｅトランスポート５０６に変換する。ハブが、２つの変換機能を行う場合には、これらは、送信元から宛先までのこの経路において、２度現れることになる。図示されるように、ハブ５０５、５０６は、コミュニティ境界５０３にわたり通信するため、外部コネクタでもある。通信境界５０３がない場合には、ハブは外部コネクタにはならない。

【００１４】

図６ないし図７においては、媒介コミュニティが導入されて、サービスを与える。これ

らのサービスは、ゲートウェイ及びビジネス・インテリジェンス・データの収集である。媒介コミュニティは、典型的には、種々のプロトコルを用いてゲートウェイを通してエンタープライズに接続性を与える市場である。これらは、さらに、信頼できる媒介手段として働き、エンタープライズが互いに作用し合うようにすることができる。これらは、さらに、ビジネス・インテリジェンス・データをその顧客に与えることができる。図６においては、サービスは、ネットワークにおける２つのコミュニティを橋渡ししている。多数のネットワークに属し、これを可能にする両方のネットワークのメンバのネットワーク間の橋渡しとして働く媒介物をサポートするようにする実施が可能である。例えば、図６においては、送信元コミュニティ６０１及び宛先コミュニティ６０２は、同じコミュニティネットワークには属していない。コミュニティ６０３は、送信元６０１と共通の一方のコミュニティネットワーク、及び、宛先６０２と共通の別のコミュニティネットワークに属すると仮定する場合には、該コミュニティ６０３は、送信元と宛先との間の通信における信頼できる媒介物として働くことができる。この場合の図におけるコミュニティ境界６０８もまたコミュニティネットワーク境界である。送信元６０１及び宛先６０２により用いられるプロトコル６０６、６０７は同じであるため、これは、単純な例である。ハブ６０３ないし６０５のいずれにおいても変換は必要ではない。図７においては、コネクタ７０１はｅｂＸＭＬ／ＨＴＴＰＳ７０６プロトコルを用い、コネクタ７０２はＭＭＬ／ｓｏｎｉｃプロトコル７０７を用いるため、変換が必要になる。この図においては、ハブ７１１、７１２、７１３は、コミュニティ境界７０８によって送信元コミュニティ及び宛先コミュニティから分けられた媒介コミュニティに属する。３つのハブすべては、送信元から宛先までのトランスポートに関係している。ハブ７１１は、電子商取引文書をハブ７０４から受け取る外部コネクタである。ハブ７１２によって、ｅｂＸＭＬ／ＨＴＴＰＳからｓｏａｐ／ＨＴＴＰＳへの第１の変換が行われる。このことは、依然として、宛先において要求されるプロトコルの組み合わせではないため、文書はハブ７１３に転送される。ハブ７１３は、ｓｏａｐ／ＨＴＴＰＳからＭＭＬ／ｓｏｎｉｃへのさらに別の変換を行い、これが宛先におけるプロトコルの組み合わせである。文書は、ハブ７０５に転送される。

【００１５】

図３ないし図７に示されるように、メッセージを運ぶのに要求される経路指定は、経路指定情報及び経路指定アルゴリズムを含むレジストリによりサポートされる。図８は、経路指定情報を含むレジストリの部分の単純化された図である。コネクタ８０１は、このデータ構造の中心特徴である。コネクタは、エンベロープ変換、トランスポート変換、外部可視性、ピアツーピア経路指定、サブコミュニティにおけるメンバシップ、及び同じサブコミュニティにおける他のコネクタに対するピアツーピア経路指定のような能力８０２を有する。したがって、コネクタ８０１と能力８０２との間の関係８１１は、ゼロ又はそれ以上の能力をサポートする。１つ又はそれ以上のリンク８０３が、コネクタ８０１をプロトコル８０４その他のコネクタに接続する。コネクタ８０１と特定のトランスポート／エンベロープ・プロトコル８０４との間の関係８１６は、１つ又はそれ以上のプロトコルをサポートする。コネクタ８０１から８１２を通り、リンク８０３から８１５を通り、プロトコル８０４までは、関係は１対１である。すなわち、上述の場合を除く、図８には示されていないトランスポート・プロトコルが、さらに、セキュリティ考慮事項により差別化される場合を除いては、コネクタ８０１から特定のトランスポート／エンベロープ・プロトコル８０４までに１つより多くの発信リンク８１３が存在しない。アウトバウンド・リンク８１３及びインバウンド・リンク８１４は、経路指定法則に対応する。さらに、アウトバウンド・リンク８１３は、特定のトランスポート／エンベロープ・プロトコル８１５、８０４により通信されるべきメッセージが別のコネクタに転送される必要があるという経路指定法則を表わす。リンク８０３は、子及び親コネクタ８０１の両方に関連する。インバウンド・リンク８１４は、子コネクタに適用される経路指定法則により表わされる特定のトランスポート／エンベロープ・プロトコルに従って、コネクタ８０１を該子コネクタによる通信の宛先として指定する。トランスポート／エンベロープ・プロトコル８０４においては、トランスポート情報８０６及びエンベロープ・フォーマット情報８０５の両

方がある。このトランスポート及びエンベロープ情報８０６、８０５は、オブジェクト構造を標準化するために、同じオブジェクトの部分になる代わりに、プロトコル対８０４にリンクされることができる（８１８、８１７）。さらに、いわゆるチャネルオブジェクトを、コネクタ８０１とプロトコル８０４との間に導入して、経路指定がトランスポート／エンベロープ／セキュリティの三つ組みによって決まる場合には、上述の例において、データ構造をさらに標準化することができる。

【００１６】

図９は、コネクタを説明するレジストリの部分の代替的な図を示す。コネクタ９０１は、種々の属性を有する。これは、コミュニティの名前及び個々のコネクタの名前との連結とすることができる名前を有する。これは、記述及びユニバーサル・リソース・インジケータ（ＵＲＩ）を有する。フラグは、コネクタが集中コネクタであるか又は外部コネクタであるかを示す。外部コネクタは、ユーザ定義コネクタである。コミュニティ内では、サブコミュニティにおけるメンバシップが属性ｐｅｅｒＴｏＰｅｅｒＧｒｏｕｐ（ピアツーピアグループ）に反映される。この属性は、管理ドメイン又はサブコミュニティの名前を含むストリングとすることができる。コネクタ９０１の能力は、トランスポート変換９２２、エンベロープ変換９２３、及びルータ作用９２４を含む。コネクタ９０１は、１つより多いトランスポート変換能力９２２を有することができる。現在の実施においては、トランスポートは、特定のエンベロープ・プロトコルと関連している。変換は、ｔｒａｎｓｐｏｒｔ１からｔｒａｎｓｐｏｒｔ２までの双方向であると仮定される。フラグは、２つのトランスポート・プロトコルがソフトウェアの実施に固有のものであるかどうかを示す。一方のソフトウェア実施は、ＨＴＴＰ、ＨＴＴＰＳ、及びｓｏｎｉｃ変換プロトコルに固有のトランスポート・サポートを与える。ＦＴＰのような他のトランスポート・プロトコルは、ユーザにより実施することができる。コネクタ９０１は、また、１つより多いエンベロープ変換能力９２３を有することができる。変換は、ここでも、双方向であると仮定される。コネクタは、さらに、ルータ能力９２４を有することができる。ルータ能力は、ハブコネクタが、他のコネクタから受け取ったメッセージを転送する能力のことを指す。この実施においては、経路指定は、特定のエンベロープ・プロトコルと関連する。コネクタ９０１は、さらに、トランスポート／エンベロープ・プロトコル９０４と関連する。トランスポート仕様は、特定のエンベロープ・プロトコル及びプロトコル形態に対してサポートされる。種々のトランスポート形式は、特定のエンベロープ・プロトコルと併せて用いることができる。物理アドレスは、特定のトランスポート形式と関連する。任意的に、トランスポートのセキュリティは、特定のトランスポートと関連することがある。トランスポート仕様９０４は、トランスポート／エンベロープの対であるか、又はトランスポート／エンベロープ／セキュリティの三つ組みを反映することができる。フラグは、トランスポート仕様に従って、経路指定法則が無視できるかどうか、及び、コネクタと同じサブコミュニティのメンバである他のコネクタとの間での通信がピアツーピアベースで指示されたかどうかを示す。経路指定法則は、可能となった経路９２５に対応する。図９に示されるレジストリ組織は、チャネルオブジェクトをコネクタ９０１とトランスポート仕様９０４との間に導入することによりさらに標準化して、該トランスポート仕様を、エンベロープ・プロトコル又はトランスポート／エンベロープ・プロトコルによって、グループ分けすることができる。

【００１７】

図１０は、コミュニティ間での経路指定をサポートするレジストリの部分の高レベルの図を与える。ターゲット１００１は、送信元が到達しようとしている宛先である。ターゲットは、最終的な宛先であってもよいし、又は宛先に転送されることになっている宛先に近い点である。ターゲットは、ＵＲＬのようなアドレスを与えるコミュニティと関連しており、ここでコミュニティレジストリにアクセスすることができる。本実施は、１つの媒介コミュニティ１００３の宛先をサポートし、これにより、メッセージがターゲット１００１に転送される。ターゲットは、宛先コネクタ１００４、及び１つ又はそれ以上のトランスポート／エンベロープ・プロトコル１００５と関連している。図８におけるように、

トランスポート／エンベロープ・プロトコルは、エンベロープ・フォーマット１００６及びトランスポート１００７に関連している。

【００１８】

以下は、単純なハブ及びスポークのトポロジにおける２つのアプリケーションをもつこのスキーマを用いたサンプルＸＭＬファイルである。

```
<?xml version="1.0" encoding="UTF-8"?>
<Registry xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespac
eSchemaLocation="D:¥design¥routing¥registry.xsd">
 <Connector uuid="A">
  <TransportSpec uuid="A01">
   <Parent>Hub01</Parent>
   <EnvelopeProtocol version="C1">SOAP</EnvelopeProtocol>
   <TransportType>Sonic</TransportType>
   <PhysicalAddress>String</PhysicalAddress>
  </TransportSpec>
 </Connector>
 <Connector uuid="Hub">
  <TransportSpec uuid="Hub01">
   <Parent>None</Parent>
   <Child>A01</Child>
   <Child>B01</Child>
   <EnvelopeProtocol version="C1">SOAP</EnvelopeProtocol>
   <TransportType>Sonic</TransportType>
   <PhysicalAddress>String</PhysicalAddress>
  </TransportSpec>
  <Capability>
   <Hub>
    <EnvelopeProtocol version="C1">SOAP</EnvelopeProtocol>
   </Hub>
  </Capability>
 </Connector>
 <Connector uuid="B">
  <TransportSpec uuid="B01">
   <Parent>Hub01</Parent>
   <EnvelopeProtocol version="C1">SOAP</EnvelopeProtocol>
   <TransportType>Sonic</TransportType>
    <PhysicalAddress>String</PhysicalAddress>
  </TransportSpec>
  </Connector>
</Registry>
```

【００１９】

このレジストリデータは、送信元及び宛先コネクタ３０１、３０２がＳＯＡＰ／Ｓｏｎｉｃプロトコル３０４、３０５を利用する図３の変形態様に対応する。このサンプルエントリにおいては、ハブ３０３は、「Ｈｕｂ　０１」と名づけられる。データは、一般には、図９の組織と適合する。

【００２０】

経路指定ブロックの単一フォーマットは、コミュニティ内、及びコミュニティ間における経路指定の両方に用いることができる。図１１及び図１２は、経路をＸＭＬを用いて示すことができるフォーマットを示し、サンプルは以下の通りである。図１１及び図１２においては、経路１１１は、２つ又はそれ以上のコネクタ１１０３／１２０３と関連してい

る（１１０２）。コネクタ１２０３は、名前１２０５、エンベロープ形式１２０６、固有の又は外部のトランスポート１２０７のフラグ、コネクタ機能宛先１２０８、及びトランスポート・プロトコル１２０９を含む複雑なデータ形式１２０４と関連している。トランスポート・プロトコル１２０９は、さらに、図には示されていないトランスポート・アドレスと関連している。経路１１０１は、送信元から宛先までトラバースされるべきコネクタのリストを定義する。コネクタ１１０３／１２０３は、経路に沿って単一の機能を与える。名前１２０５は、発行側権限接頭語／コネクタ形式／コミュニティの名前／ローカルの名前の連結のような独特な名前とすることができる。エンベロープ形式１２０６は、このコネクタにおける到着時のエンベロープ形式であり、これは例えば、ＳＯＡＰ、ｅｂＸＭＬ、又はＭＭＬである。「Ｉｓ　Ｎａｔｉｖｅ」フラグ１２０７は、トランスポート形式が、ソフトウェアシステムに固有のものであるが、又はユーザにより実施される拡張機能としてサポートされるものであるかを示す。コネクタ機能１２０８は、このノードで行われるべき機能を識別する。トランスポート１２０９は、このノードに到達するのに用いられるトランスポートを識別する。このノードに対するトランスポート／エンベロープ・プロトコルは、トランスポート１２０９及びエンベロープ形式１２０６の組み合わせに対応する。このデータ組織に一般に適合するＸＭＬコードのサンプルは、以下の通りである。

```
<?xml version="1.0" encoding"UTF-8"?>
<Route xmlns="http://commerceone.com/wse/routing" xmlns:xsi="http://www.w3.or
g/2001/XMLSchema-instance" xsi:schemaLocation="http://commerceone.com/wse/rou
ting D:¥design¥routing¥route-block.xsd">
 <Connector>
  <Name>
    BUY:C:buySpice:nutmeg
  </Name>
  <EnvelopeType>ebXML</EnvelopeType>
  <isNative>true</isNative>
  <ConnectorFunction>se- rvice-send</ConnectorFunction>
  <Transport type="HTTPS" mode="sync" reliable="false">
   <Address>http://buyer.com/- buy/nutmeg</Address>
  </Transport>
 </Connector>
 <Connector>
  <Name>
    BUY:C:buySpice:gw1
  </Name>
  <EnvelopeType>ebXM- L</EnvelopeType>
  <isNative>true</isNative>
 <ConnectorFunction>envelope-gateway</ConnectorFunction>
  <Transport type="HTTPS" mode="sync" reliable="false">
   <Address>http://gateway.seller.com/external/Address>
  </Transport>
 </Connector>
 <Connector>
  <Name>
    BUY:C:buySpice:exotic
  </Name>
  <EnvelopeType>SOAP-C1</EnvelopeType>
  <isNative>true</isNative>
  <ConnectorFunction>se- rvice-receive</ConnectorFunction>
  <Transport type="Sonic" mode="async" reliable="true">
   <Address>SonicCluster1:Sel- lApp</Address>
  </Transport>
 </Connector>
</Route>
```

【００２１】

これは、送信元３０１が、ｅｂＸＭＬ／ＨＴＴＰＳプロトコル３０４を用いて、ハブ３０３と通信する図３の変形態様に対応する経路を示す。送信元コネクタ３０１は、ｎｕｔｍｅｇと名づけられた固有のコネクタである。ハブコネクタ３０３もまた、ＧＷ１と名づけられた固有のコネクタであり、エンベロープ・ゲートウェイ機能を行う。宛先３０２は、ＳＯＡＰ／Ｓｏｎｉｃプロトコル３０５を用いて、ハブ３０３と通信する。宛先３０２は、ｅｘｏｔｉｃと名づけられた固有のコネクタである。３つのコネクタすべては、コミュニティＢＵＹ：Ｃ：ｂｕｙＳｐｉｃｅに属する。送信元及び宛先により用いられるトランスポート・プロトコルは、ソフトウェアの実施に固有のものであるため、ハブ３０３は、エンベロープ及びトランスポート・プロトコルの変換を単一の機能として行う。したがって、サンプル経路コールにおいては一度だけ現れる。

【００２２】

図１３及び図１４は、コミュニティ内及びコミュニティ間での経路指定の高レベル図である。経路は、送信元、宛先、及びこれらの間に一連のコネクタを含む。安全な経路指定のためには、経路は、さらに、１つ又はそれ以上のセキュリティゾーンを含み、通信が常に安全であるようにする。図１３においては、サービスとすることができる送信元及び宛先は、コネクタ１３０１にマップされる。ローカルレジストリ１３０２は、コネクタについての情報を含み、ここから送信元及び宛先コネクタで始まる部分的な通路のリストを構成することができる（１３０３）。電子商取引文書が通るコネクタの部分的な通路リストを構築することは、幾つかのサブステップを含む。レジストリの情報は、コネクタにおける通信に対する経路指定法則を含み、これは、指向グラフとして表わすことができる。部分的な通路リストを作成することは、子コネクタから親コネクタにトラバースすることを含む。トラバースにおける各々のコネクタでは、次の上部に利用可能な代替的なトランスポート／エンベロープ・プロトコルが、別々の部分的な通路として扱われる。送信元又は宛先からの部分的な通路のトラバースを完了させることは、トラバーサルの特定のトランスポート／エンベロープ・プロトコルを用いた利用可能な親コネクタがないコネクタに到達することに対応する。或いは、部分的な通路のトラバースを完了させることは、トラバーサルの特定のトランスポート／エンベロープ・プロトコルを用いたピアツーピア通信するコネクタに到達することに対応させることができる。コネクタがピアツーピア通信であるかどうかを判断する際、フラグが、コネクタに対して、同じサブコミュニティの他のコネクタに対する経路指定を無視することを可能にするように設定されている場合には、該コネクタが属するサブコミュニティを考慮する必要がある。子コネクタから親コネクタまでトラバースさせることにより、部分的な通路リストが、送信元及び宛先コネクタに対して作成され、１つ又はそれ以上の部分的な通路が各々のリストに含まれる。送信元及び宛先の部分的な通路リストは、リンクされる（１３０４）。それぞれの送信元及び宛先の部分的な通路リストは、両方の部分的な通路リストがコネクタを共有しており、該共有コネクタに対するトランスポート／エンベロープ・プロトコルが両方のリストにおいて同じであるか、又は該共有コネクタがそれぞれのリストにおけるそれぞれのトランスポート／エンベロープ・プロトコル間で変換する変換能力がある場合には、該共有コネクタによりリンクすることができる。それぞれのリストは、さらに、それぞれのリストにおいて同様なコネクタ間でリンクすることができ、該同様なコネクタは、同じトランスポート／エンベロープ・プロトコルをサポートするコネクタである。上述のように、この経路指定方法に対する拡張機能は、トランスポート／エンベロープ／セキュリティの三つ組みを、部分的な通路リストを構築するための基礎として用いることである。それぞれのリストをリンクさせるための別の代替的な手法は、それぞれの部分的な通路リストに現れるトランスポート／エンベロープ・プロトコル間で変換する能力を有する１つ又はそれ以上の集中コネクタによりリンクさせることである。集中コネクタを用いるためには、部分的な通路リストを、コネクタから、該親コネクタに明確にリンクされていない集中コネクタに延ばすことができる。

【００２３】

図１４は、コミュニティにわたる経路指定に適用される。コミュニティにわたる経路は、コミュニティ間にホップ（hop:通信間のノードの意）を含み、コミュニティ内には内側のコネクタ間ホップを含む。サービスとすることができる送信元及び宛先は、コネクタ１４０１にマップされる。それぞれの送信元及び宛先コネクタは、コミュニティに属する。送信元及び宛先コミュニティは、次いで、コミュニティネットワークに属する。１つ又はそれ以上のネットワークは、送信元及び宛先コミュニティをリンクするものとして、レジストリ１４０３から識別される１４０２。送信元及び宛先コミュニティが、コミュニティネットワークにおいてメンバシップを共有する場合には、それぞれのコミュニティの外部コネクタは、共通のトランスポート／エンベロープ・プロトコルを用いて直接リンクさせることができる。送信元及び宛先コミュニティに、共通のトランスポート／エンベロープ・プロトコルがない場合には、１つ又はそれ以上の媒介コミュニティを経路に加えて、変換サービスを行うことができる。送信元及び宛先の外部コネクタは、１つ又はそれ以上の

媒介コミュニティの同様なコミュニティにリンクされる。幾つかの実施においては、媒介コミュニティの数は、経路指定を単純にするために、１、２、３、又は、５又は１０より少ない他の小さい数に制限される。場合によっては媒介コミュニティを通る送信元及び宛先コミュニティの外部コネクタ間の経路が求められた場合には、参加コミュニティの各々の中のコミュニティ間の経路が計算される。送信元及び宛先コミュニティにおいては、１つ又はそれ以上のレジストリ１４０５のデータを利用して、それぞれの外部コネクタに対する送信元及び宛先コネクタからの経路が計算される（１４０４）。媒介コミュニティにおいては、受信及び発信外部コネクタからの経路が計算される。完全な経路は、コミュニティ間及びコミュニティ内の経路を組み合わせて（１４０６）、送信元から宛先までへのコネクタ間の経路を生成することにより特定される。コミュニティにわたる経路指定は、ローカル又はグローバル・レジストリに格納され予め計算された経路を利用することができる。予め計算された経路は、媒介コミュニティを指定することができ、これにより、メッセージが経路指定される。媒介コミュニティは、変換、会計、ビジネス・インテリジェンスその他のサービスを与えることができる。メッセージを送信元から宛先まで送るために、経路が計算される場合には、経路を後の使用のために保存することが有効である。或いは、アイドル（空き）ＣＰＵサイクルを有効に利用して、コミュニティネットワーク内の他のコミュニティに対する経路、又は、媒介コミュニティネットワーク内のコミュニティを通して到達することができるあらゆる媒介コミュニティネットワークを超えたコミュニティに対する経路を予め計算することができる。

【００２４】

電子商取引文書の経路指定は、遭遇する可能性がある多くの脅威のために、安全で信頼できる経路を辿ることが好ましい。有線上の文書は、暗号化されなければ危険にさらされる。送信元又は宛先が脅かされて、機密として維持されるべき情報が公開される。送信元と宛先との間のコネクタは、不当に作用することがあり、文書を欠落させたり、遅延させたり、又は再送信したり、これらが受信した文書を記録して機密情報を公開したり、又は文書を修正することがある。変換責任をもつコネクタは、変換中に不当に作用することがあり、すなわち文書の意味（セマンティックス）をあっさり変更することがある。これらの周知の問題は、電子商取引文書の安全で信頼できる通信方法及び装置を与える機会を生成する。

【００２５】

図１５から図１９までは、安全で信頼できる通信の幾つかの用途例を示す。送信元と宛先との間の信頼関係は、前の合意により確立される。例えば、取引パートナーである会社が合意し、その合意を共同合意形態で登録することができる。この共同合意は、用いる文書形式及び相互に合意可能なセキュリティメジャー、例えば署名及び暗号化を含むことができる。セキュリティ合意は、取引パートナー間で達するか、又はそれぞれの取引パートナーが属するコミュニティから採用することができる。合意に達するやり方は重要でなく、信頼できる通信において保障される。

【００２６】

送信元から宛先までの経路に沿ったコネクタは、これらが信頼できるものとしてレジストリにリスト表示された場合に信頼できるものとなる。ハブは、経路指定に従って、経路における次のホップに沿って文書を送ること、及びこれが有するコンテンツのあらゆる知識を保護すること、又は該経路に沿った文書の送信さえも保護することに対して信頼される。ハブの機能が文書を転送するものだけである場合には、該ハブは、文書が暗号化されているか又は署名されているかどうかについて懸念する必要はない。仮想プライベート・ネットワーク通信又はＨＴＴＰＳ通信のような暗号化通信をサポートするためには、ハブは、ＰＫＩその他のセキュリティモデルを実施するものとしてキー及び証明を有することができる。

【００２７】

エンベロープ変換サービスを与える、いわゆるゲートウェイと呼ばれるコネクタは、より複雑な信頼問題を呈する。文書を一方のフォーマットから別のフォーマットに変換する

ことは、ハブ又はコネクタが受け取るものを暗号解除し、署名を検証できるものであることを要求する。変換後、ゲートウェイは、これが変換したものを再署名して暗号化する。これらすべてを達成するためには、ゲートウェイにより受け取られたメッセージは、宛先のためのキーではなく、ゲートウェイのキーを用いて暗号化されるべきである。ゲートウェイは、好ましくは検証署名をサポートするレジストリを参照することにより、受け取ったメッセージの署名を検証できるものではなくてはならない。ゲートウェイが文書を変換した後、受け取ったメッセージが署名されていた場合には、文書に再署名する。さらに別の変換が要求されていない場合には、経路に沿った又は宛先に対する次のゲートウェイに対応するキーを用いて、メッセージを暗号化する。ゲートウェイは、多数のキーの対又は証明を有することができ、異なるキーの対は、暗号化、署名、及び安全な仮想プライベート・ネットワーク接続のために用いることができる。

【００２８】

ゲートウェイを通る送信元から宛先までへの認証は、逐次的なものである。第１のゲートウェイは、送信元の署名を検証し、文書に再署名する。後続するゲートウェイはメッセージを受け取ったゲートウェイを信頼しなければならないため、ゲートウェイは、送信元を信頼しなければならない。鎖（チェーン）状の各々のゲートウェイは、前にあるゲートウェイを信頼し、これが受け取る署名を認証して、これ自体の署名を適用する。このセキュリティ・チェーンを確立する際、例えば、ＳＡＭＬアサーション（assertion）を受け入れて、ゲートウェイにより適用することができる。生じるあらゆる争いを解決するために、ゲートウェイが変換された文書の広範なアーカイブを維持することが望ましい。文書は、好ましくは、存在する場合には、受け取った署名を含む原文書として暗号化解除後に１度、及び変換後で暗号化前に１度というように、好ましくはゲートウェイの署名を示して、２度アーカイブされるべきである。

【００２９】

全体的に、経路における信頼関係は、送信元及び宛先が互いに信頼関係にあるとき、送信元及び宛先が変換を行うゲートウェイと信頼関係にあるとき、及び経路における各々のコネクタが該経路における前の及び後続のコネクタと信頼関係にあるときに確立することができる。送信元と宛先との間の信頼関係は、上述されている。電子商取引においては、集団が電子文書を交換する前に、互いに信頼するのは妥当なことである。ゲートウェイは変換機能を行うため、送信元及び宛先は、ゲートウェイを信頼するべきである。信頼できるゲートウェイのリストは、レジストリに維持することができる。送信元又は宛先のいずれかに、変換サービスを行うゲートウェイコネクタとの信頼関係がない場合には、そのゲートウェイは用いるべきではない。すべての取引パートナーが特にこれに敏感であるわけではないが、防衛産業参加者のようなセキュリティ意識の強い取引パートナーは、文書のコンテンツを読み取ることができる１つ１つのコネクタを知ることが有利であることを見出す。文書の暗号解除又はこれらの変換なしで、文書を転送するだけのコネクタのために信頼関係の必要条件を緩和することができる。

【００３０】

例えば、送信元がＭＭＬエンベロープを用い、宛先がｅｂＸＭＬを用いる特定の送信元及び宛先を考える。可能性のある１つの経路としては、ＭＭＬを用いる送信元から第１のゲートウェイまで、ＭＭＬからＳＯＡＰへのエンベロープ変換、第１のゲートウェイから第２のゲートウェイまでの転送、ＳＯＡＰからｅｂＸＭＬへの変換、及び第２のゲートウェイから宛先への転送である。この場合には、送信元は、ゲートウェイ及び宛先の両方を信頼しなければならない。宛先は、送信元及びゲートウェイを信頼しなければならない。送信元又は宛先のいずれかが変換を行う媒介ゲートウェイと信頼関係にない場合には、経路は受け入れ不可能である。

【００３１】

ゲートウェイは、さらに、ゲートウェイ直前の送信元と、直後のゲートウェイ又は宛先を信頼するべきである。これは、推移的な信頼関係と呼ぶことができる。変換を行う信頼チェーンにおける各々の要素は、信頼できる要素と確実に相互作用していることを望む。

上述の例に続いて、経路がゲートウェイ１からゲートウェイ２、さらにゲートウェイ３を通り、次いで宛先までトラバースすると仮定する。経路と併せて、第１のゲートウェイは、送信元及び第２のゲートウェイを信頼しなければならない。第２のゲートウェイは第１及び第３のゲートウェイを信頼しなければならない。第３のゲートウェイは第２のゲートウェイ及び宛先を信頼しなければならない。実際、ゲートウェイ３は、ゲートウェイ２を信頼し、これは逆に、ゲートウェイ１を信頼するため、該ゲートウェイ３は、該ゲートウェイ１を信頼する。推移的な信頼関係は、これが送信元と宛先との間の明確な信頼関係と組み合わされている場合には、この種の経路に沿っては、十分なものと考えられる。代替的手法として、媒介コミュニティが変換ゲートウェイを与える場合には、単純化された信頼関係モデルを適用することができる。この場合には、変換サービスを行う媒介コミュニティにより用いられる１つ１つのゲートウェイの信頼関係を要求することなく、変換サービスを与える媒介コミュニティを信頼するので十分になる。この信頼関係の単純化は、媒介コミュニティが含まれる場合においてのみ適用可能であると考えられる。例えば、送信元及び宛先が同じコミュニティにある場合には、送信元及び宛先は互いに信頼関係にあるが、文書の変換を行うゲートウェイとは信頼関係にない。コミュニティ内においては、ゲートウェイは、明確に信頼できるものであるべきである。コミュニティのネットワーク内においては、媒介コミュニティの変換機構の１つ１つのコンポーネントを信頼する必要なく、該媒介コミュニティは、特定の変換サービスを行うのに信頼できるである。

【００３２】

認証及び信頼関係に対する多くの異なるモデルを用いることができる。認証のために現在用いられている３つのセキュリティモデルは、ユーザ名及びパスワード、ＳＡＭＬ認証アサーション、及びＸ．５０９証明である。これらその他のセキュリティモデルの作動は、あわせてセキュリティ信任の作成と呼ぶことができる。セキュリティ信任は、別々のプロセスとして実行されるか又はコードのルーチン又はセクションとして実行されるサーバにより与えることができる。ユーザ名及びパスワードの認証においては、受け取り側がユーザ名及びパスワードを検証する。ユーザ名及びパスワードの通信は、暗号化されたチャネルを介したものであるべきである。

【００３３】

ＳＡＭＬアサーションは、より複雑である。送信元と宛先との間の信頼関係の部分は、該宛先がＳＡＭＬアサーションを生成する権限を信頼することである。この信頼関係は、コミュニティの広さのレベルであってもよいし又は特定の送信元により用いられる特定の権限に対するものであってもよい。一般に、信頼できるＳＡＭＬアサーション認証の権限その他の信頼できる権限の証明は、該アサーションを検証するのに必要なパーティによるアクセスのためにレジストリ内に維持される。

【００３４】

動作においては、ＳＡＭＬサービスは、ＳＡＭＬクライアントからアクセス可能とすることができる。ＳＡＭＬサービスは、リクエストをＳＡＭＬクライアントからを受け取り、該クライアントに応答し戻す。例えば、ＳＯＡＰエンベロープをこの通信に用いることができる。ＳＡＭＬサービスは、認証及び属性リクエストの両方をサポートすることができる。認証リクエストに応答して、これは、セキュリティ信任を生成することができる。属性リクエストに応答して、これは、属性アサーションを生成することができる。ＳＡＭＬサービスにより生成されたアサーションは、典型的には、ＳＡＭＬサービスの署名キーを用いて署名される。基本的な認証においては、ＳＡＭＬサービスは、取引パートナー又はユーザＩＤ及びパスワードをＳＯＡＰエンベロープのアプリケーション信任ヘッダブロックから抽出することができる。このサービスは、レジストリアクセス・アプリケーションプログラム・インターフェースを呼び出して、取引パートナー又はユーザＩＤに対応するパスワードを取得する。これは、受け取ったパスワードをレジストリのパスワードと比較する。これらが適合する場合には、アサーションを生成してこれに署名する。これらが適合しない場合には、エラーを報告する。代替的な実施形態においては、パスワードがレジストリに格納される前に、これをハッシュすることができる。その場合には、ハッシュ

が比較される。

【００３５】

Ｘ．５０９認証においては、信頼関係は証明を発行した証明権限に基づくべきである。信頼できる証明権限のリスト表示は、証明権限のアイデンティティ又は証明権限アイデンティティ及び対応するアイデンティティの組み合わせに基づくことができる。ＶｅｒｉＳｉｇｎクラスの３つの証明のような信頼できる証明権限のリストは、どのコミュニティから来たかに関係なく信頼される証明を含むことができる。或いは、信頼できる証明権限のリストは、リモートコミュニティ特有のものとすることができる。したがって、Ｂｏｅｉｎｇの証明は、これらがＢｏｅｉｎｇコミュニティから来る場合においてのみ信頼される。ＶｅｒｉＳｉｇｎの証明は、多数のコミュニティに対して信頼されることができる。

【００３６】

ＳＡＭＬサービスは、Ｘ．５０９認証証明に応答することができる。Ｘ．５０９証明の受け取りにより、これは、証明を、ＳＯＡＰエンベロープのアプリケーション信任ヘッダブロックから抽出することができる。これは、添付物に格納されたプロセス情報を取得することができる。添付物が空である場合には、認証の失敗を報告する。添付物のプロセス情報フィールドから抽出されたクライアント証明を信任ヘッダブロックからのものと比較する。証明が適合しない場合には、認証の失敗を報告する。これらが適合する場合には、レジストリアクセス・アプリケーション・インターフェースを呼び出して、取引パートナー又はユーザＩＤをレジストリから得る。プロセス情報をレジストリ証明と比較する。これらが適合しない場合には、認証の失敗を報告する。これらが適合する場合には、アサーションを生成し、これに署名することができる。アサーションはクライアントに戻される。

【００３７】

信頼関係機構は、さらに、電子商取引文書の異なるレベルの分類を実施するのに用いることができる。例えば、重要な軍事コンポーネントは、特別な最高機密セキュリティ信任を要求するが、売店の品物はルーチンのアサーションを用いて扱うことができる。特別な経路指定法則は、特別なアサーションに適用することができる。例えば、最高機密文書は、最高機密文書を変換するように認証された特別に信頼できるゲートウェイを通してしか経路指定できない。特に信頼できるゲートウェイは、高められた監視、特に強い暗号化、専用トランスポート媒体などのような付加的なセキュリティ措置を受けることになる。

【００３８】

送信元と宛先との間の信頼関係が与えられると、保護された信頼できる通信の機構は、送信元及び宛先が同じコミュニティにあるかどうか、これらがセキュリティサーバにより直接相互作用するのか又はプロキシによりって相互作用するのか、及びこれら両方が同じセキュリティ機構を用いるかどうかのような要因によって決まることになる。図１５は、コミュニティ内の１つのセキュリティの実施を示す。このコミュニティにおいては、送信元１５１１及び宛先１５１２を含むすべてのコネクタが、互いに信頼関係にある。この場合においては、セキュリティサーバ１５０１は、コミュニティに対してローカルなＳＡＭＬサーバである。送信元１５１１は、認証のためのセキュリティ信任をＳＡＭＬサーバ１５０１から取得し、さらに、権限のための属性アサーションも取得することができる。少なくともセキュリティ信任及び電子商取引文書がエンベロープに包まれて、コミュニティ内の経路に沿って、送信元から宛先まで送られる。この経路は、図示されないコネクタを含むことができる。

【００３９】

図１６は、第１のコミュニティ１６０５における送信元１６１１と、第２のコミュニティ１６０６における宛先１６１２とを示す。ネットワーク概念は、送信元及び宛先が、これらが文書を交換する他のコミュニティについての情報を有することを要求する。ＳＡＭＬがセキュリティ機構として用いられる場合には、他のコミュニティについてのこの情報は、セキュリティサービスを与えることに対して信頼された他のコミュニティにおけるＳＡＭＬサーバのアイデンティティを含む。他のコミュニティにおけるＳＡＭＬサービスは

、ローカルなコミュニティにより信頼されるものとして明確にリスト表示される。図１５においては、コミュニティ１６０６、１６０６の各々は、ＳＡＭＬサービス１６０１、１６０２、及び送信元１６１１又は宛先１６１２のいずれかを含む。送信元が文書を宛先に送る場合には、送信元は、そのＳＡＭＬサーバ１６０１に対して、ＳＡＭＬアサーションを与えるように要求する。この送信元は、さらに、宛先のＳＡＭＬサーバ１６０２を照会して認証情報を取得する。両方のＳＡＭＬサーバからのアサーションは、電子商取引文書と併せて宛先に送られる。性能を高めるものとして、送信元が属するコミュニティ又は送信元のセキュリティサービスは、第２のコミュニティ１６０６から取得されたＳＡＭＬアサーション、又はローカル及び外部のＳＡＭＬアサーションの両方を後の使用のために保存して、システム性能を改善することができる。ＳＡＭＬ機構に対する代替的技術として、ＰＫＩ機構が用いられる場合には、送信元に対する証明を発行した信頼できる証明権限の証明は、宛先コミュニティ（１６０６）に登録されなければならない。ユーザ名及びパスワードのセキュリティに対しては、有効なユーザ名及びパスワードの組み合わせが、宛先コミュニティ及びゲートウェイに登録される。

【００４０】

図１７は、セキュリティサービスの代行を示す。この図においては、コネクタ１７１１がセキュリティサービスをホストし、送信元１７２１及び１７２２のためのプロキシとして作用する。送信元１７２１、１７２２は、セキュリティサービスが、プロキシ１７１１により行われるように登録することができる。プロキシ１７１１がＳＡＭＬサービス１７０１と通信する場合には、これ自体及び送信元を識別し、これに代わってセキュリティのアサーションをリクエストする。ＳＡＭＬサーバは、次いで、送信元の代わりにセキュリティアサーションをホストに対して発行し、さらに、属性アサーションを発行することができる。ホストは、少なくともセキュリティアサーション及び電子商取引文書を宛先に転送する。セキュリティアサーションには、セキュリティプロセスにおけるホストの関与を開示するアドバイス・ステートメントが伴うことがある。

【００４１】

図１８Ａ及び図１８Ｂは、ゲートウェイ１８１２に対する認証代行を示す。図１８Ａにおいては、コネクタ１８２１、１８２２は、大きなコミュニティ１８０５のサブコミュイティ１８０６にある。これらのコネクタ１８２１、１８２２は、ＭＭＬプロトコルを使用して、ゲートウェイ１８１２と通信する。これらは、ＭＰＩＤ、ユーザＩＤ、及びパスワードをゲートウェイに渡す。プロセス情報は、同じ情報を含む。ゲートウェイは、これが受け取るＭＰＩＤ、ユーザＩＤ、及びパスワードのレジストリ検索を行う。この三つ組みが、レジストリに見出される場合には、ゲートウェイは、ＭＭＬエンベロープの添付物として、信任オブジェクトを生成する。ゲートウェイは、代行認証リクエストをＳＡＭＬサービスに送る。ＳＡＭＬサービスは、ゲートウェイの信任を用いて認証する。ＳＡＭＬサービスは、アドバイスセクションを含むことができる認証アサーションを戻す。認証アサーションは、ゲートウェイ１８１２が宛先１８１１に転送するものの部分である。

【００４２】

図１８Ｂにおいては、ゲートウェイ１８１２を通る通信が逆になる。送信元１８１１は、ＭＭＬプロトコルを用いるサブコミュニティ１８０６におけるコネクタ１８２１、１８２２と通信する。送信元１８１１は、ＳＡＭＬセキュリティ信任をＳＡＭＬサーバ１８０１から取得し、これを電子商取引文書と併せてゲートウェイ１８１２に転送する。ゲートウェイは、ＳＯＡＰエンベロープをＭＭＬエンベロープに変換する。ゲートウェイは、これ自体のＭＰＩＤ、ユーザＩＤ、及びパスワードを用いて、セキュリティ信任を生成し、これをＭＭＬエンベロープに添付する。ＭＭＬエンベロープは、ＭＭＬ１８０６を用いるサブコミュニティに送られる。

【００４３】

図１９Ａ及び図１９Ｂにおいては、ＭＭＬ及びＳＡＭＬのセキュリティプロトコル間の変換が、コミュニティ１９０５、１９０６間の通信まで拡張されている。送信元１９２２は、ＭＭＬを用いるコミュニティ内にあり、宛先１９１１は、ＳＯＡＰを用いるコミュニ

ティ内にある。送信元の取引パートナー１９２２は、ポータルルータ１９２１により、セキュリティ信任及び電子商取引文書の、エンベロープ及びセキュリティ変換を扱うゲートウェイ１９１２への転送を行う。ルータ１９２１は、セキュリティ信任をゲートウェイ１９１２に渡す。セキュリティ信任は、ＭＭＬエンベロープの中にある。ゲートウェイは、ＣＰＩＤをＭＭＬエンベロープにおけるセキュリティ信任から抽出して、代行認証リクエストをＳＡＭＬサービスに送る。認証は、ゲートウェイの信任を用いて行われる。ＳＡＭＬサービスは、上記で詳述したように、認証アサーションを戻す。認証アサーション及び変換された電子商取引文書は、宛先１９１１に転送される。図１９Ｂにおいては、ゲートウェイ１９１２を通る通信が逆になる。送信元１９１１は、ＭＭＬプロトコルを用いるサブコミュニティ１９０６における宛先１９２２と通信する。送信元１９１１は、ＳＡＭＬセキュリティ信任をＳＡＭＬサーバ１９０１から取得し、これを電子商取引文書と併せてゲートウェイ１９１２に送る。ゲートウェイは、ＳＯＡＰエンベロープをＭＭＬエンベロープに変換する。ゲートウェイは、これ自体のＭＰＩＤ、ユーザＩＤ、及びパスワードを用いて、セキュリティ信任を生成し、これをＭＭＬエンベロープに添付する。ＭＭＬエンベロープは、ＭＭＬを用いるサブコミュニティ１９０６に送られる。

【００４４】

上述された代行シナリオを可能にするために、ＳＡＭＬプロトコルスキーマを、以下のように拡張することができる。

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema targetNamespace="http://schemas.commerceone.com/wse/securi- ty/del
egation" xmlns:samlp="http://www.oasis-open.org/committees/se- curity/docs/dra
ft-sstc-schema- protocol-27.xsd"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:c1del="http://schemas.comme
rceone.com/wse/security/delegation"
elementFormDefault="qualified" attributeFormDefault="unqualified" version="0.1
">
      <xsd:import namespace="http://www.w3.org/200- 0/09/xmldsig#" schemaLoca
tion="xmldsig-core-schema.xsd"/>
      <xsd:import namespace="http://www.oasis-open.org/committees/security/-
docs/draft- sstc-schema-protocol-27.xsd" schemaLocation="draft-sstc- -schema-p
rotocol-27.xsd"/>
      <!-- //DelegateFor - the ID of the TP or service for which the delegate
 is making the authentication request
           //CommunityID - the community ID where the TP or service is define
d
           //CommunityType - the community type (e.g. MOE4x)
          //Description - info only -->
      <xsd:complexType name="DelegationType">
            <xsd:complexContent>
                  <xsd:extension base="samlp:AuthenticationQueryType">
                      <xsd:attribute name="DelegateFor" type="xsd:string"/>
                      <xsd:attribute name="CommunityID" type="xsd:string"/>
                      <xsd:attribute name="CommunityType" type="xsd:string"
/>
                      <xsd:attribute name="Description" type="xsd:string"/>
                  </xsd:extension>
            </xsd:complexContent>
      </xsd:complexType>
</xsd:schema>
```

【００４５】

スキーマに適合する代行認証リクエストは以下のように表わされる。

```
<?xml version="1.0" encoding="UTF-8"?>
<Request xmlns="http://www.oasis-open.org/committees/security/do- cs/draft-sst
c-schema-protocol-27.xsd" xmlns:ds="http://www.w3.org/2000/09/- xmldsig#"
xmlns:saml="http://www.oasis-open.org/committees/security/docs/d- raft-sstc-sc
hema-assertion-27.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSc- hema-instance"
xmlns:c1del="http://schemas.commerceone.com/wse/security/de- legation"
xsi:schemaLocation="http://www.oasis-open.org/committees/securit- y/docs/draft
-sstc-schema-protocol-27.xsd
C:.backslash.XMLSPY.about.2.3.bac- kslash.draft-sstc-schema-protocol-27.xsd"
xsi:schemaLocation="http://schem- as.commerceone.com/wse/security/delegation
C:.backslash.XMLSPY.about.2.3.b- ackslash.sec-delegation-ext.xsd" RequestID="1
fgtTGzMXSqpN++/LcFpBmZWrQg=" MajorVersion="1" MinorVersion="0" IssueInstant="2
001-09-11T09:30:47-05:00- ">
      <RespondWith>AuthenticationStatement</Respond- With>
      <!-- The SAML service will treat the signature block as a blob -->
      <ds:Signature Id="ID01">
           <!-- digital signature -->
      </ds:Signature>
      <AuthenticationQuery xsi:type="c1del:DelegationType" DelegateFor="TPxxx
">
           <saml:Subject>
             <saml:NameIdentifier Name="unique-string-that-identifies-the-TP"
/>
             <saml:SubjectConfirmation>
                  <!-- For basic authentication -->
                  <saml:ConfirmationMethod>http//www.oa- sis- open.org/comm
itties/security/docs/draft-sstc-core-27/password
            <!-- For X509 certificate based authentication
                <saml:ConfirmationMethod>http://www.oasis- open.org/committi
es/security/docs/draft-sstc-core-27/X509 -->
                </saml:ConfirmationMethod>
             </saml:SubjectConfirm- ation>
           </saml:Subject>
      </AuthenticationQuery>
</Request>
```

【００４６】

上のＤｅｌｅｇｔｅＦｏｒ及びＮａｍｅＩｄｅｎｔｉｆｉｅｒは、同じエンティティ、すなわち、代行認証が行われる集団を指す。代行を含むこのリクエストに対するサンプル応答は、以下のように表わされる。

<?xml version="1.0" encoding="UTF-8"?>
<!--Sample XML file generated by XML Spy v4.2 U (http://www.xmlspy.com)-->
<Response xmlns="http://www.oasis-open.org/committees/security/d- ocs/draft-sstc-schema-protocol-27.xsd" xmlns:ds="http://www.w3.org/2000/09- /xmldsig#" xmlns:saml="http://www.oasis-open.org/committees/security/docs/- draft-sstc-schema-assertion-27.xsd" xmlns:xsi="http://www.w3.org/2001/XMLS- chema-instance" xsi:schemaLocation="http://www.oasis-open.org/committees/s- ecurity/docs/draft-sstc-schema-protocol-27.xsd
C:.backslash.XMLSPY.about.2- .3.backslash.draft-sstc-schema-protocol-27.xsd" ResponseID="String"
InResponseTo="1fgtTGzMXSqpN++/LcFpBmZWrQg=" MajorVersion="1" MinorVersion="0" IssueInstant="2001-09-11T09:30:47-05:00">

```
    <Status>
            <StatusCode Value="samlp:Success">
                  <SubStatusCode Value="q:name"/>
            </StatusCode>
            <StatusMessage>String</StatusM- essage>
            <StatusDetail/>
    </Status>
    <saml:Assertion MajorVersion="1" MinorVersion="0"
AssertionID="+1UyxJDBUza+ao+LqMrE98wmhAl=" Issuer="String" IssueInstant="2001-0
9- 11T09:30:47-05:00">
            <saml:Conditions NotBefore="2001-09-11T09:30:47-05:00" NotOnOrAfte
r="2001-09-11T09:30:47-05:00"/>
            <saml:Advice>
                  <saml:Subject>
                        <saml:NameIdentifier Name="ID-of-the-delegate"/>
                  </saml:Subject>
                  <saml:AdviceElement xsi:type="xsd:string" value="some descr
iption"/>
            </saml:Advice>
            <saml:AuthenticationStatement>
                  <saml:Subject>
                        <saml:NameIdentifier Name="unique-string-that-identi
fies- the-TP"/>
                        <saml:SubjectConfirmation>
                              <!-- For basic authentication -->
                              <saml:ConfirmationMethod>http:/- /www.oasis-
open.org/committies/security/docs/draft-sstc-core-27/pa- ssword
                              <!-- For X509 certificate based authenticatio
n
                              <saml:ConfirmationMethod>http://www.oasis- op
en.org/committies/security/docs/draft-sstc-core-27/X509 -->
                              </saml:ConfirmationMethod>
                        </saml:SubjectConfirm- ation>
                   </saml:Subject>
            </saml:AuthenticationSt- atement>
            <ds:Signature Id="ID11">

            </ds:Signature>
     </saml:Assertion>
</Response>
```

ＳＡＭＬサービスが代行によりアサーションを生成した場合には、これは、上の＜Ａｄｖｉｃｅ＞ブロックを用いて、代行を公表する。代行なしでは、応答は同様なものになるが、＜Ａｄｖｉｃｅ＞ブロックがない。

【００４７】

１つの実施においては、アサーションスキーマは、単一のリクエストメッセージが認証及び属性リクエストの両方を含むことを可能にしない。この実施においては、ＳＡＭＬクライアントは、まず認証リクエストに、次いで、属性リクエストにサブミットする。属性リクエストは、認証に続く。サンプル属性リクエストは、以下の通りである。

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Sample XML file generated by XML Spy v4.2 U (http://www.xmlspy.com)-->
<!--Attribute Request-->
<Request xmlns="http://www.oasis-open.org/committees/security/do- cs/draft-sst
c-schema-protocol-27.xsd" xmlns:ds="http://www.w3.org/2000/09/- xmldsig#"
xmlns:saml="http://www.oasis-open.org/committees/security/docs/d- raft-sstc-sc
hema-assertion-27.xsd" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.oasis-open.org/committees/se- curity/docs/draft
-sstc-schema-protocol-27.xsd
C:.backslash.XMLSPY.about.2.- 3.backslash.draft-sstc-schema-protocol-27.xsd"
RequestID="1 fgtTGzMXSqpN++/LcFpBmZWrQg=" MajorVersion="1" MinorVersion="0" Is
sueInstant="2001-09-11T09:30:47-05:00">
    <RespondWith>AttributeStatement</RespondWith>
    <AttributeQuery>
            <saml:Subject>
                <saml:NameIdentifier Name="unique-string-that-identifies-t
his-TP"/>
            </saml:Subject>
            <saml:AttributeDesignator AttributeName="attribute-name-string" A
ttributeNamespace="attribut- e-name-space-string"/>
    </AttributeQuery>
</Request>
```

【００４８】

属性アサーションの応答はこのリクエストに続く。

【００４９】

付加的なセキュリティ用途例の詳細は図２０から図２５までに示される。図２０は、サンプルクライアント・サービス設計のブロック図である。この設計においては、レジストリサービス認証及び費用承認は、ＣＰレベルのアイデンティティに基づく。レジストリマネージャ認証及び承認は、ユーザレベルのアイデンティティに基づく。レジストリサービスは、認証のためにＳＡＭＬを用いる。これは、プロバイダのアプリケーションインターフェースが、直接、特権を判断するように要求し、すなわち認証されたＣＰアイデンティティに基づいて、これ自体の承認を行うことを要求する。ＳＡＭＬクライアント２０１２は、格納されたＳＡＭＬクライアントデータ２０１１にアクセスする。ＳＡＭＬクライアント２０１２は、ローカル及びリモートの場合の間で切り換えられるＳＡＭＬクライアントスイッチ２０１３と通信する。ローカルの場合においては、通信は、直接ＳＡＭＬサービス２０１６により行われる。リモートの場合においては、コンポーネント２０１４、２０１５は、スイッチとリモートＳＡＭＬサービスとの間で通信を扱う。信任及びＳＡＭＬアサーションは、ＨＴＴＰＳ又は別の保護プロトコルを介してコンポーネント間で交換することができる。ＳＡＭＬサービス２０１６は、サービス及びユーザ管理プロバイダ２０１７と通信し、これは、証明ベースのユーザ識別、ユーザＩＤ及びパスワードベースの認証、又は別の認証スキームに適応させることができる。サービス及びユーザ管理プロバイダ２０１７は、共通のオブジェクトフレームワーク（ＣＯＦ）２０１８をサポートするモジュールと通信し、これは、次いで、レジストリ２０１９にアクセスする。

【００５０】

図２１は、図２０に示される設計を用いるレジストリサービスのローカル認証を示す。この図における番号付けは、図２０と一致しているが、レジストリクライアント２１０１、レジストリサービス２１０５、ＣＯＦ２１０６及びレジストリ２１０７が加えられている。この応用例においては、レジストリクライアント２１０２が最初に呼び出される。レジストリクライアント２１０１は、ＳＡＭＬクライアント２１１２を呼び出して、認証を取得する。上述されたどの認証スキームを用いてもよい。ＳＡＭＬクライアントは、格納

されたＳＡＭＬクライアントデータ２１１１に対するアクセスを有することができる。これは、格納されたデータからの認証リクエストを有効にして、有効なアサーションを戻すことができる。そうでない場合には、これは、リモート認証により進む。ＳＡＭＬクライアントは、コンポーネント２１１４、２１１５を通して、ＳＡＭＬサービス２１１６と通信する。ＳＡＭＬサービスは、認証を行い、セキュリティ信任を生成し、これに署名することができ、該セキュリティ信任をＳＡＭＬクライアント２１１２に戻す。この応用例の変形態様は、レジストリサービスのリモート認証に対する図２２に示される。ここでも、レジストリクライアント２１０２が最初に呼び出される。レジストリクライアントは、行われる必要があるリモート呼び出しを判断する。これは、コンポーネント２２０２を起動させて、ｈｔｔｐｓ接続２２０３のような通信チャネルを通して、対応するコンポーネント２２０４と通信するようにし、さらに、ＳＡＭＬクライアント２２１２と通信するようにする。処理は、上述のように継続する。

【００５１】

図２３及び図２４は、ローカル及びリモートの承認をそれぞれ示す。図２３においては、レジストリクライアント２３０１は、直接レジストリサービス２３０５を呼び出し、例えば、図２１に示されたように取得されたセキュリティ信任を渡す。レジストリサービスは、セキュリティ信任をもつＳＡＭＬクライアント２３１２を呼び出して、セキュリティ信任を有効にし、認証ＣＰＩＤを得る。認証されたＣＰＩＤにおいては、レジストリサービス２３０５は、ユーザマネージャプロバイダの数表示を呼び出して、認証されたＣＰの特権を取得する。ＣＯＦ２３１８により、ＣＰの特権がレジストリ２３１９から取得される。レジストリサービスの数表示２３０５は、特権を施行する。図２４においては、ローカル認証プロセスは、リモート認証まで拡張される。認証として、レジストリクライアント２４０１は、コンポーネント２４０２、２４０３を通して通信し、この場合には、該コンポーネントを通してレジストリサービス２４０５に到達する。

【００５２】

図２５は、文書サービス・サブスクリプションの属性アサーションの取得を示す。コンポーネント２５０２及び２５０３は、ＩＣＤクライアント２５１１、２５２１、及び承認モジュール２５１２、２５２２を含むものとしてさらに詳細に示される。ＩＣＤクライアント２５１１は、送り側レジストリ２５４１と関連する送り側ＩＣＤサービス２５３１を呼び出す。分割ライン２５００の左側の送り側から、ＩＣＤサービス２５３１が受け取り側ＩＣＤサービス２５３２を呼び出す。セキュリティ計算器がＳＡＭＬクライアント２５３３を呼び出して、属性アサーションを得る。ＳＡＭＬクライアントは、受け取り側ではローカルであるＳＡＭＬサービス２５３４を呼び出す。ＳＡＭＬサービスは、サービスプロバイダアプリケーションインターフェース２５３５を呼び出して、送り手のための情報を取得し、属性アサーションを生成する。サービスプロバイダは、レジストリ２５４２にアクセスすることができる。属性アサーションは、送り側ＩＣＤサービス２５３１に渡し戻され、ＩＣＤセキュリティブロック２５１１の中に包まれる。権限モジュール２５１２は、属性アサーションをＳＯＡＰエンベロープヘッダのようなエンベロープヘッダの中に入れる。エンベロープは、コンポーネントに送信され、ここでは、受け取り側の承認モジュール２５２２が属性アサーションを読み取り、サブスクリプションを施行する。

【００５３】

図２６及び図２７は、コミュニティネットワークの確立を示す。図２６においては、２つのコミュニティ２６０１、２６０５がコミュニティネットワークに参加している。コミュニティのオペレータは、外部ポート２６０２、２６０６、及びローカルレジストリ２６０３、２６０７を含むコミュニティを設定する。ローカルレジストリが外部ポートを識別する。コミュニティのオペレータは、従来の契約であってもよいし、又は電子契約であってもよい作動構成２６１１を作成する。作動構成は、コミュニティがネットワークを形成するか又はこれに入るようにする。コミュニティは、ネットワークにおいて他者に曝される１つ又はそれ以上のサービスを有する。発見サービス及びプッシュサービスは、重複登録なしで、ネットワークにおけるコミュニティが、他のコミュニティのサービスを用いる

ことを可能にする。コミュニティのオペレータは、さらに、時には、グローバル・イエローページ・ディレクトリ２６１４と呼ばれるネットワーク検索レジストリを確立する。ネットワークが作動すると、コミュニティは、サービス情報をそのローカルレジストリからグローバル・イエローページまで押し、又はグローバル・イエローページが情報を参加コミュニティから引き出すことができる。グローバル・イエローページは、参加コミュニティをポーリングするか又は情報を引き出すことができるコミュニティからの通知を待つことができる。コミュニティのオペレータは、ローカルコミュニティで可視の、特定のネットワークで可視の、すべてのネットワークで可視の、又は特定の他のコミュニティに対して可視の特定のサービスをマークすることができる。グローバル・イエローページのサービス情報のリスト表示は、可視性によりマークしたサービスに対応するべきである。これらのグローバル・イエローページは、ＵＤＤＩベースのレジストリとして実施することができる。これは、コミュニティの外であってもよいし、又はネットワークにおけるコミュニティの１つによりホストされるものであってもよい。コミュニティのネットワークには、１つ又はそれ以上のグローバル・イエローページがあってよい。コミュニティのオペレータは、互いの外部ポートの詳細及びＵＲＬ２６１２についての情報を交換する。この情報は、外部ポート２６０２、２６０２間の通信を可能にする。コミュニティのオペレータは、さらに、セキュリティ信任又はＳＡＭＬ証明２６１３のようなセキュリティ関連情報を交換する。手元にある交換された情報により、それぞれのコミュニティのオペレータは、これらのレジストリを外部コミュニティに接続するのに必要な情報でロードする。例えば、外部コミュニティの外部ポート及びセキュリティ情報を登録することができる。さらに、外部コミュニティポートに対応するこれら自体の外部ポートを登録することができる。さらに、コミュニティのオペレータは、時には、ホワイトページ２６１５と呼ばれるグローバル検索レジストリを確立する。これは、コミュニティの外にあってもよいし、又はネットワークのコミュニティの１つによりホストされるものであってもよい。グローバル検索レジストリがコミュニティの１つによりホストされている場合には、これは、コミュニティアドレスサーバとして作用する。コミュニティアドレスサーバが機能するコミュニティのネットワークの一部となる個々のコミュニティは、コミュニティアヂレスサーバと交換することにより、設定された情報２６１１、２６１２、２６１３をネットワークに入れることができる。特に、ネットワーク内の１つ１つのコミュニティに対してレジストリのエントリを設定するのではなく、そのローカルレジストリにコミュニティアドレスサーバのポートを登録することにより、ポート、セキュリティ信任などのような他の外部コミュニティに対する設定を該コミュニティアドレスサーバから取得することができる。相互運用性は、コミュニティネットワークの法則及び慣習に従って、及び場合によっては、互いにビジネスを行っているコミュニティにおける双方向合意２６１１を適用することにより、コミュニティアドレスサーバを通して確立することができる。

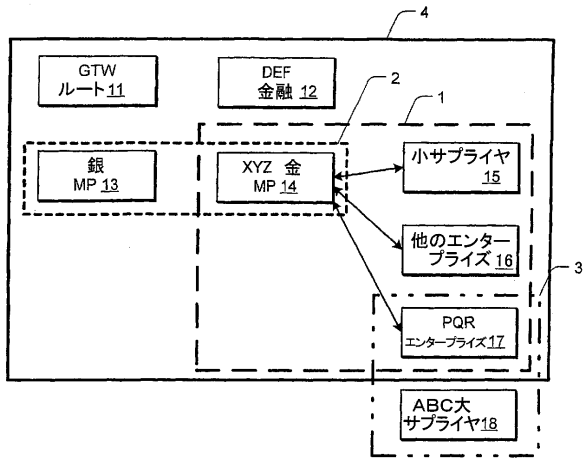
【００５４】

図２７は、１つのコミュニティがコミュニティアドレスサーバをホストする２つより多いコミュニティのネットワークを示す。コミュニティ２７０２は、コミュニティアドレスサーバ２７０４を保持する。コミュニティ２７０１及び２７０３は、ホストコミュニティと情報交換し、これらの各々が提供するサービス、及び互いに通信を可能にするプロトコルを発見できるようになる。これらの通信は、直接のものであってもよいし、媒介コミュニティにより仲介されてもよいし、又は、ネットワークの法則に従って、媒介コミュニティを通過するように義務づけられていてもよい。２つより多いコミュニティのネットワークにおいては、直接のプライベートリンクが参加コミュニティ間で確立され、それぞれのコミュニティのレジストリ内に記録されてもよいし、又はコミュニティアドレスサーバを用いて、接続及び信頼関係を確立してもよい。可能性の少ない用途例は、コミュニティアドレスサーバなしで確立された２つより多いコミュニティのネットワークであり、ここでは、すべてのメンバが２地点間ベースで互いに登録する。この用途例は、ネットワークに対して、新しいメンバが合理的に加えられることによるどのような利益も得ることはない。

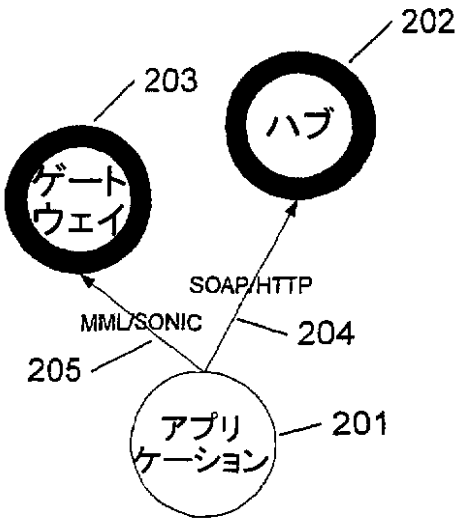
【００５５】

本発明は、上述の好ましい実施形態及び例を参照して開示されるが、これらの例は、限定的な意味ではなく、例示的なものであることを意図していることが理解されるだろう。記載された実施形態には、コンピュータ支援処理がかかわっている。したがって、本発明は、コンピュータ支援処理のための方法、変換処理を行う論理を含むシステム、変換処理を行う論理を与えた媒体、変換処理を行う論理を与えたデータ・ストリーム、又は、コンピュータがアクセス可能な変換処理サービスで具体化することができる。当業者であれば、本発明の精神及び添付の特許請求の範囲内の改良及び組み合わせを容易に発想するであろうと考えられる。

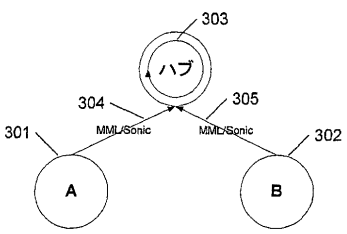
【図１】



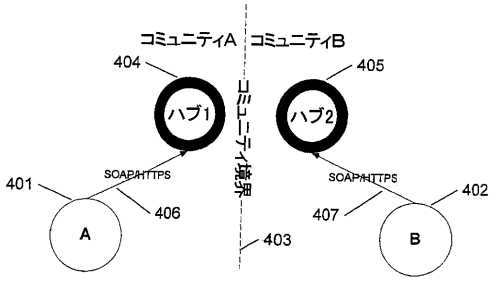
【図２】



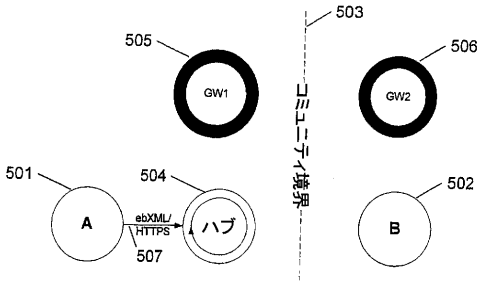
【図３】



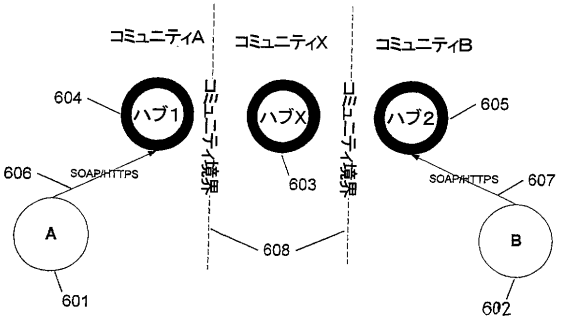
【図４】



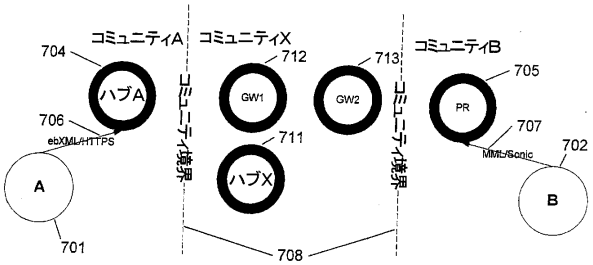
【図５】



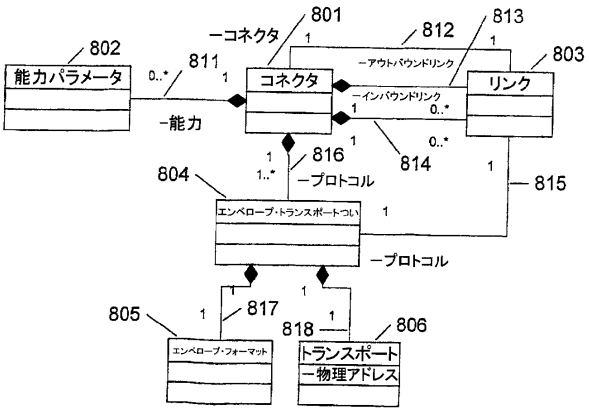
【図６】



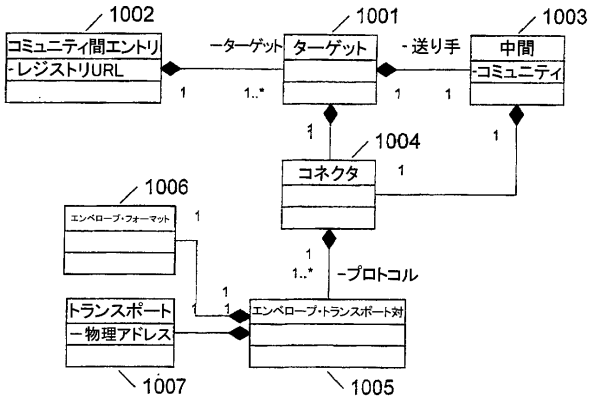
【図７】



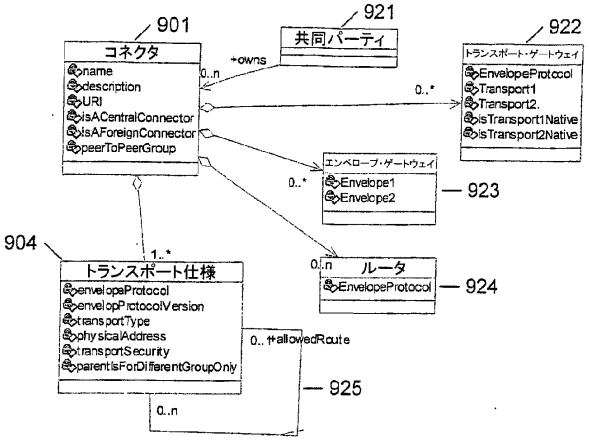
【図８】



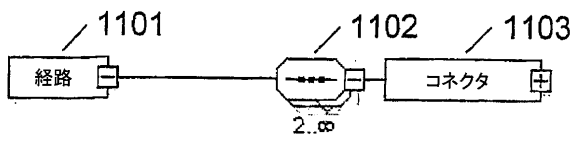
【図１０】



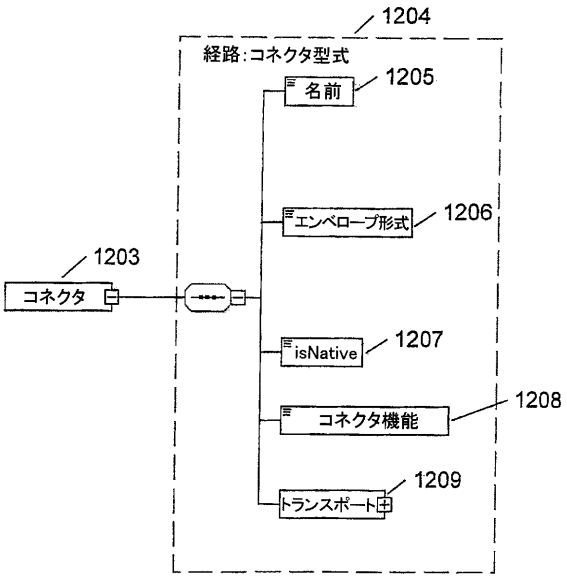
【図９】



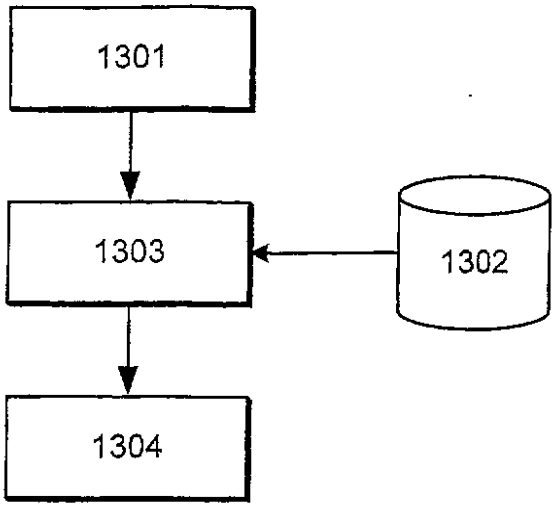
【図１１】



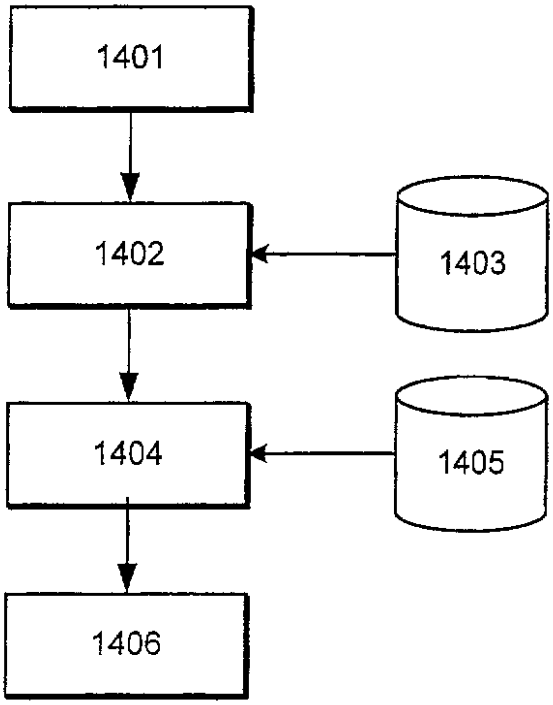
【図１２】



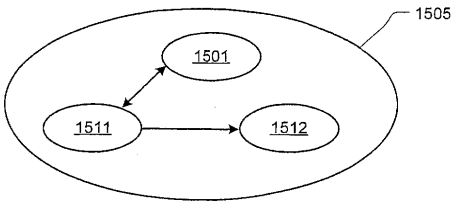
【図１３】



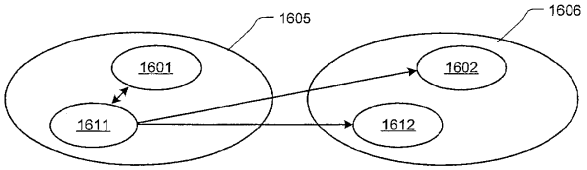
【図１４】



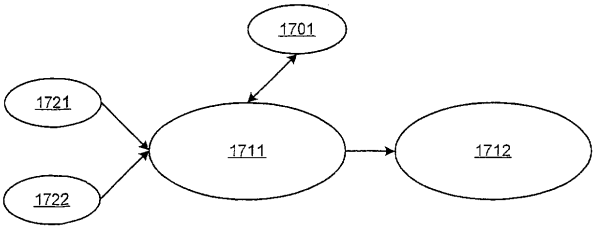
【図１５】



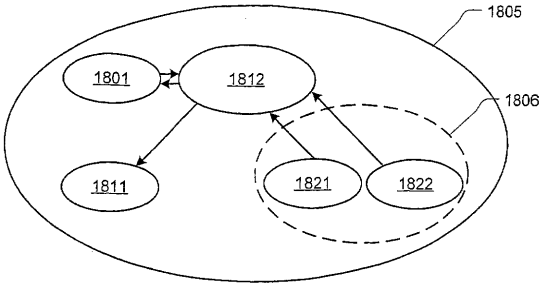
【図１６】



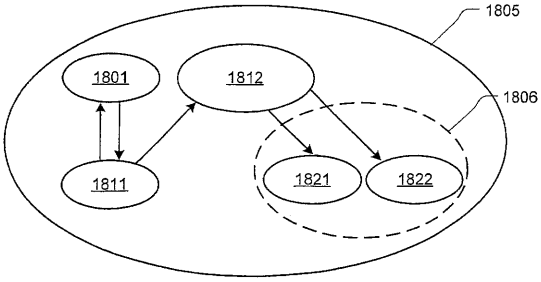
【図１７】



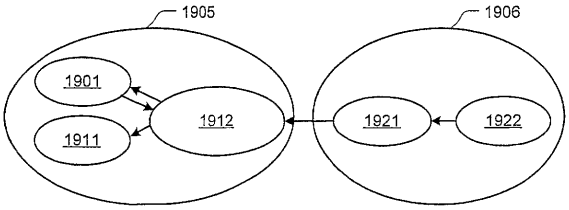
【図１８Ａ】



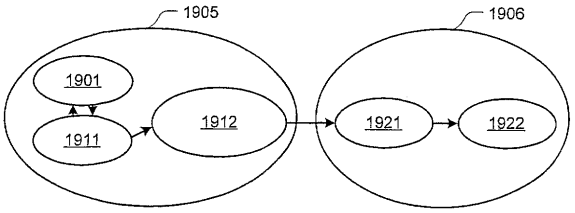
【図１８Ｂ】



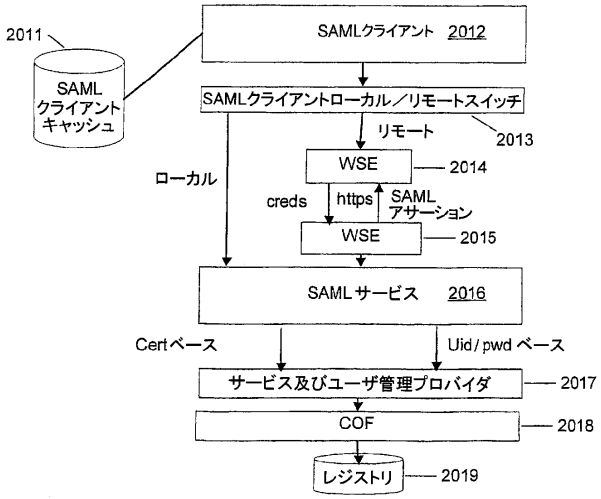
【図１９Ａ】



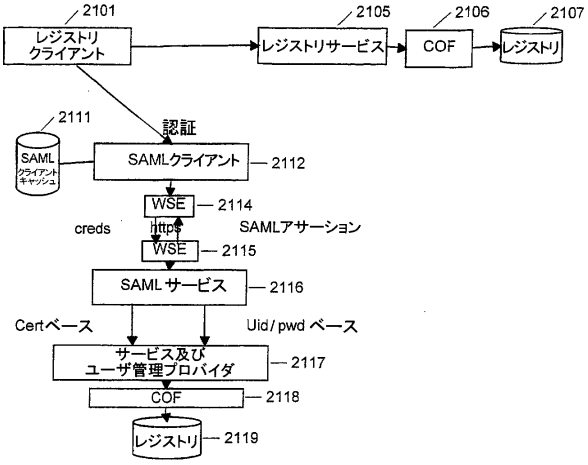
【図１９Ｂ】



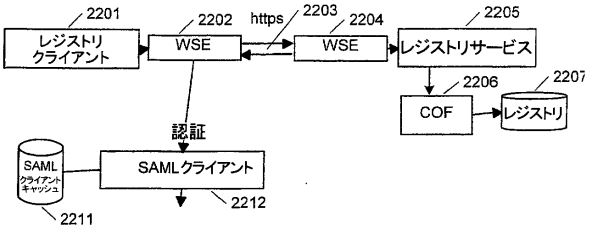
【図２０】



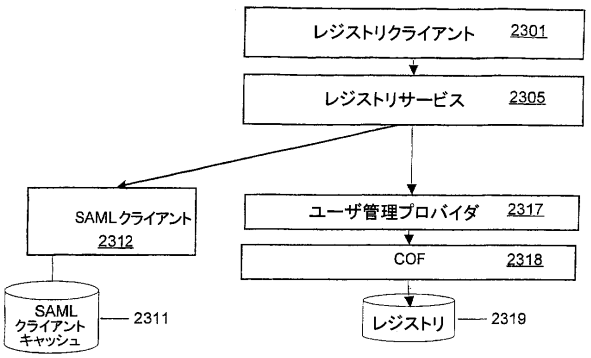
【図２１】



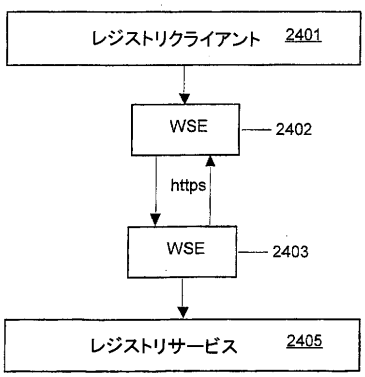
【図２２】



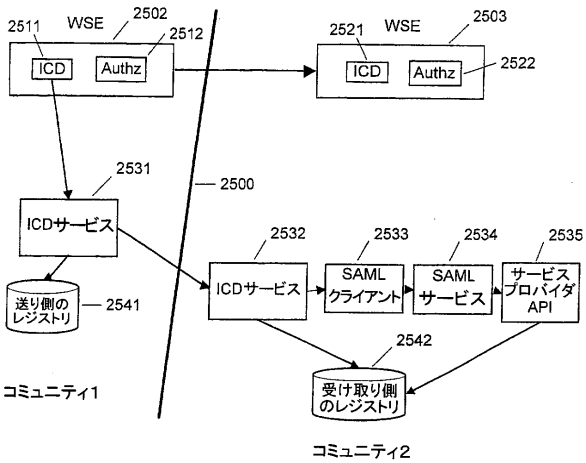
【図２３】



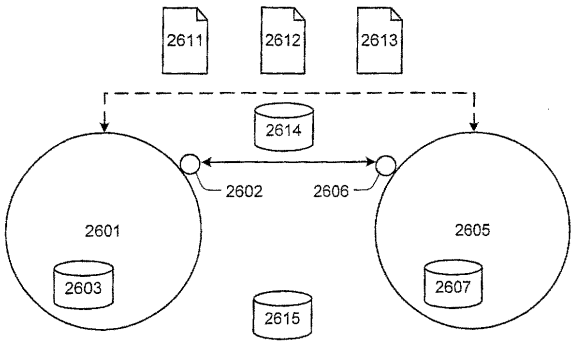
【図２４】



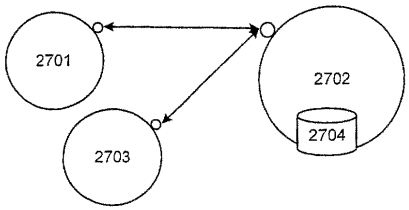
【図２５】


2511
WSE
2502
2512
ICD
Authz
2521
WSE
2503
ICD
Authz
2522
2531
2500
ICDサービス
2532
2533
2534
2535
ICDサービス
SAML
クライアント
SAML
サービス
サービス
プロバイダ
API
送り側の
レジストリ
2541
2542
受け取り側
のレジストリ
コミュニティ1
コミュニティ2

【図２６】


2611
2612
2613
2614
2602
2606
2601
2605
2603
2607
2615

【図２７】


2701
2702
2704
2703

フロントページの続き

(74)代理人 100109070
弁理士 須田 洋之
(74)代理人 100109335
弁理士 上杉 浩
(74)代理人 100120525
弁理士 近藤 直樹
(74)代理人 100122563
弁理士 越柴 絵里
(72)発明者 サプラム ラグナス
アメリカ合衆国 テキサス州 ７８６１３ シダー パーク ワイド アントラー コーヴ １３０２
(72)発明者 カシー ジャヤラム ラジャン
アメリカ合衆国 カリフォルニア州 ９５１１１ サン ホセ センチュリー メドー コート ５４４５
(72)発明者 クラウス トッド クリストファー
アメリカ合衆国 カリフォルニア州 ９５１３９ サン ホセ レオミンスター コート ３７
(72)発明者 クラル クリストファー
アメリカ合衆国 ワシントン州 ９８１９９ シアトル ローズモント プレイス ウェスト ２４１６
(72)発明者 サンフィリッポ ジョセフ
アメリカ合衆国 カリフォルニア州 ９５１２４ サン ホセ クランフォード サークル ４０２０

合議体
審判長 和田 志郎
審判官 稲葉 和生
審判官 千葉 輝久

(56)参考文献 米国特許出願公開第２００２／３２７９０（ＵＳ，Ａ１）
小柳津育郎，やさしい情報セキュリティ：第４回 証明書とディジタル封筒，ビジネスコミュニケーション，株式会社ビジネスコミュニケーション社，１９９６年１１月１日，３３巻，１１号，ｐ．６７－７１
実森仁志，Ｗｅｂでのシングル・サインオン標準，ＯＡＳＩＳがXMLベースで４月に草案，日経インターネットテクノロジー，日経ＢＰ社，２００２年５月２２日，５９号，ｐ．１８
中尾康二ほか，情報セキュリティマネジメントの国際、国内規格化動向，信学技報，電子情報通信学会，２００１年１１月１４日，１０１巻，４４１号，ｐ．３１－３６，（ＮＳ２００１－１４６）
安井晴海，企業ネット最前線：ＪＣＢ ＩＣカード移行にらむ戦略ネット マルチ機能をＩＰで高速処理，日経コミュニケーション，日経ＢＰ社，２００２年６月３日，３６７号，ｐ．１０８－１１３
【保険会社共同ゲートウェイ】保険会社と代理店を結ぶ共同ゲートウェイを構築，ビジネスコミュニケーション，株式会社ビジネスコミュニケーション社，２００１年１２月１日，３８巻，１２号，ｐ．３９－４０
松下嘉哉ほか，XMLを基盤とするビジネスプロトコルの動向，ＦＵＪＩＴＳＵ，富士通株式会社，２００２年５月１０日，５３巻，３号，ｐ．１９５－１９９

(58)調査した分野(Int.Cl.，ＤＢ名)
G06Q10/00-50/00

G06F13/00-15/00