(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4819328号
(P4819328)
(45)発行日　平成23年11月24日(2011.11.24)　(24)登録日　平成23年9月9日(2011.9.9)

(51)Int.Cl.　　F I
*G06F 21/20 (2006.01)*　　G06F 15/00 330A
*H04L 9/32 (2006.01)*　　H04L 9/00 675D

請求項の数 44　(全 13 頁)

(21)出願番号　特願2004-187041(P2004-187041)
(22)出願日　平成16年6月24日(2004.6.24)
(65)公開番号　特開2005-25739(P2005-25739A)
(43)公開日　平成17年1月27日(2005.1.27)
審査請求日　平成19年6月21日(2007.6.21)
(31)優先権主張番号　10/608,334
(32)優先日　平成15年6月30日(2003.6.30)
(33)優先権主張国　米国(US)

前置審査

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(74)復代理人　100115624
弁理士　濱中　淳宏
(74)復代理人　100129171
弁理士　柿沼　健一
(72)発明者　ダリオ　バザン　ベジャラノ
アメリカ合衆国　９８０７４　ワシントン州　サマミッシュ　２４０　アベニュー　サウスイースト　５５８

最終頁に続く

(54)【発明の名称】セキュリティプロトコルの自動ネゴシエーションのためのシステムおよび方法

(57)【特許請求の範囲】
【請求項１】
セキュリティプロトコルを自動的にネゴシエートする方法において、
内部ノード又は外部ノードのいずれかである、受信側ノードが、第１のプロトコルセットを有する内部ノードと、第２のプロトコルセットを有する外部ノードとの間に安全な接続を確立するためのセキュリティ認証要求を受信することであって、
（１）前記内部ノードは、複数のノードのための安全な情報を維持する分散型ディレクトリを備えるセキュリティ使用可能ドメイン内に存在し、
（２）前記外部ノードは、前記ノードの分散型ディレクトリ内に存在せず、
前記受信側ノードが、前記内部ノードに関連付けられた第１のプロトコルセットと前記外部ノードに関連付けられた第２のプロトコルセットとを比較すること、
前記受信側ノードが、前記内部ノード及び前記外部ノードが共通の２以上の安全なプロトコルを含むことを判定すること、
前記受信側ノードが、２以上の安全なプロトコルに関連づけられた転送速度、及び１以上の暗号キーのビット深度からなるグループの少なくとも１つのメンバーに基づいて、前記２以上の安全なプロトコルから推奨のプロトコルを選択することであって、前記転送速度は、２以上の安全なプロトコルを使用して、前記ネットワークデータが転送されるスピードを示し、前記１以上の暗号キーのビット深度は前記１以上の暗号キーを構成するビットの数である選択すること、及び、
前記受信側ノードが、前記推奨のプロトコルに基づいて、前記外部ノードと前記内部ノ

ードとの間に安全な接続を自動的に確立すること
を含むことを特徴とする方法。
【請求項２】
前記外部ノードには、少なくとも１つのコンピュータまたはネットワーク使用可能無線デバイスが含まれることを特徴とする請求項１に記載の方法。
【請求項３】
前記内部ノードには、少なくとも１つのクライアントコンピュータまたはサーバが含まれることを特徴とする請求項１に記載の方法。
【請求項４】
前記セキュリティ使用可能ドメインは、分散型ディレクトリドメインを含むことを特徴とする請求項１に記載の方法。
【請求項５】
前記セキュリティ使用可能ドメインは、証明書ベースのドメインを含むことを特徴とする請求項１に記載の方法。
【請求項６】
前記証明書ベースのドメインは、Ｋｅｒｂｅｒｏｓ使用可能ドメインを含むことを特徴とする請求項５に記載の方法。
【請求項７】
前記一致するプロトコルはＸ．５０９証明書を含むことを特徴とする請求項６に記載の方法。
【請求項８】
前記セキュリティ認証要求が前記外部ノードによって生成されることを特徴とする請求項１に記載の方法。
【請求項９】
前記セキュリティ認証要求を受信することが前記内部ノードによって実行されることを特徴とする請求項８に記載の方法。
【請求項１０】
前記セキュリティ認証要求が前記内部ノードによって生成されることを特徴とする請求項１に記載の方法。
【請求項１１】
前記セキュリティ認証要求を受信することが前記外部ノードによって実行されることを特徴とする請求項１０に記載の方法。
【請求項１２】
前記外部ノードと前記内部ノードとの間のセッションが完了した場合に前記安全な接続を終了するこ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１３】
複数の一致するプロトコルが見つかった場合に前記安全な接続を確立する際に使用するためにプロトコルを選択するこ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１４】
前記内部ノードと前記外部ノードとの少なくとも１つを認証するこ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１５】
前記認証することは証明書を認証局に伝達することを含むことを特徴とする請求項１４に記載の方法。
【請求項１６】
セキュリティプロトコルを自動的にネゴシエートするシステムにおいて、
内部ノードであって、前記内部ノードが、複数のノードのための安全な情報を維持する分散型ディレクトリを備えるセキュリティ使用可能ドメイン内に存在し、前記内部ノードは、前記内部ノードによりサポートされる１以上の安全プロトコルを備える第１のプロトコルセットを記録するように構成され、

ネゴシエーションエンジンであって、前記ネゴシエーションエンジンは、
（１）前記第１のプロトコルセットを有する前記内部ノードと、前記ノードの分散型ディレクトリ内に含まれない外部ノードと、の間に安全な接続を確立するためのセキュリティ認証要求を受信し、前記外部ノードは、前記外部ノードによりサポートされる安全プロトコルを備える第２のプロトコルセットを記録するように構成されること、
（２）前記内部ノードに関連付けられた前記第１のプロトコルセットと前記外部ノードに関連付けられた前記第２のプロトコルセットとを比較すること、
（３）前記第１のプロトコルセットと前記第２のプロトコルセットは、共通の２以上の安全なプロトコルを含むことを判定すること、
（４）前記２以上の安全なプロトコルに関連づけられた転送速度、及び１以上の暗号キーのビット深度からなるグループの少なくとも１つのメンバーに基づいて、前記２以上の安全なプロトコルから推奨のプロトコルを選択することであって、
ａ）前記転送速度は、２以上の安全なプロトコルを使用して、前記ネットワークデータが転送されるスピードを示し、
ｂ）前記１以上の暗号キーのビット深度は、前記１以上の暗号キーを構成するビットの数である、選択すること、及び
（５）前記推奨のプロトコルに基づいて、前記外部ノードと前記内部ノードとの間に安全な接続を自動的に確立すること
を実行するように構成されるネゴシエーションエンジンと
を含むことを特徴とするシステム。

【請求項１７】
前記外部ノードには、少なくとも１つのコンピュータ、または、ネットワーク使用可能無線デバイスが含まれることを特徴とする請求項１６に記載のシステム。

【請求項１８】
前記内部ノードには、少なくとも１つのクライアントコンピュータ、または、サーバが含まれることを特徴とする請求項１６に記載のシステム。

【請求項１９】
前記セキュリティ使用可能ドメインは、分散型ディレクトリドメインを含むことを特徴とする請求項１６に記載のシステム。

【請求項２０】
前記セキュリティ使用可能ドメインは、証明書ベースのドメインを含むことを特徴とする請求項１６に記載のシステム。

【請求項２１】
前記証明書ベースのドメインは、Ｋｅｒｂｅｒｏｓ使用可能ドメインを含むことを特徴とする請求項２０に記載のシステム。

【請求項２２】
前記一致するプロトコルはＸ．５０９証明書を含むことを特徴とする請求項２１に記載のシステム。

【請求項２３】
前記セキュリティ認証要求が前記外部ノードによって生成されることを特徴とする請求項１６に記載のシステム。

【請求項２４】
前記セキュリティ認証要求が前記内部ノードによって受信されることを特徴とする請求項２３に記載のシステム。

【請求項２５】
前記セキュリティ認証要求は、前記内部ノードによって生成されることを特徴とする請求項１６に記載のシステム。

【請求項２６】
前記セキュリティ認証要求が前記外部ノードによって受信されることを特徴とする請求項２５に記載のシステム。

【請求項２７】
前記外部ノードと前記内部ノードとの間のセッションが完了した場合に前記ネゴシエーションエンジンが前記安全な接続を終了することを特徴とする請求項１６に記載のシステム。
【請求項２８】
前記第１のプロトコルセットと前記第２のプロトコルセットとの間に一致が見つからない場合に前記ネゴシエーションエンジンが接続処理を終了することを特徴とする請求項１６に記載のシステム。
【請求項２９】
複数の一致するプロトコルが見つかった場合に、前記ネゴシエーションエンジンが前記安全な接続を確立する際に使用するためにプロトコルを選択することを特徴とする請求項１６に記載のシステム。
【請求項３０】
前記内部ノードと前記外部ノードとの少なくとも１つが他方を認証することを特徴とする請求項１６に記載のシステム。
【請求項３１】
前記認証することは、証明書を認証局に伝達することを特徴とする請求項３０に記載のシステム。
【請求項３２】
セキュリティプロトコルを自動的にネゴシエートする方法を実行するために構成されるコンピュータ実行可能命令を記憶する１以上のコンピュータ記録可読媒体において、前記方法が、
内部ノード又は外部ノードのいずれかである、受信側ノードが、内部ノードと外部ノードとの間に安全な接続を確立するためのセキュリティ認証要求を受信すること、
（１）前記内部ノードは、前記内部ノードによりサポートされる１以上の安全プロトコルを識別する第１のプロトコルセットを記録し、前記内部ノードが、複数のノードのための安全な情報を維持する中央集中型の分散型ディレクトリを備えるセキュリティ使用可能ドメイン内に存在し、
（２）前記外部ノードは、前記外部ノードによりサポートされる安全プロトコルを識別する第２のプロトコルセットを記録し、前記外部ノードは、前記ノードのソフトウェアベースディレクトリ内に存在せず、
前記受信側ノードが、前記内部ノードに関連付けられた第１のプロトコルセットと前記外部ノードに関連付けられた第２のプロトコルセットとを比較すること、
前記受信側ノードが、前記内部ノード及び前記外部ノードが共通の２以上の安全なプロトコルを含むことを判定すること、
前記受信側ノードが、２以上の安全なプロトコルに関連づけられた転送速度、及び１以上の暗号キーのビット深度からなるグループの少なくとも１つのメンバーに基づいて、前記２以上の安全なプロトコルから推奨のプロトコルを選択することであって、前記転送速度は、２以上の安全なプロトコルを使用して、前記ネットワークデータが転送されるスピードを示し、前記１以上の暗号キーのビット深度は前記１以上の暗号キーを構成するビットの数である、選択すること、及び、
前記受信側ノードが、前記推奨のプロトコルに基づいて、前記外部ノードと前記内部ノードとの間に安全な接続を自動的に確立すること
を含むことを特徴とするコンピュータ記録可読媒体。
【請求項３３】
前記外部ノードには、少なくとも１つのコンピュータ、または、ネットワーク使用可能無線デバイスが含まれることを特徴とする請求項３２に記載のコンピュータ記録可読媒体。
【請求項３４】
前記内部ノードには、少なくとも１つのクライアントコンピュータ、または、サーバが

含まれることを特徴とする請求項３２に記載のコンピュータ記録可読媒体。
【請求項３５】
前記セキュリティ使用可能ドメインは、分散型ディレクトリドメインを含むことを特徴とする請求項３２に記載のコンピュータ記録可読媒体。
【請求項３６】
前記セキュリティ使用可能ドメインは、証明書ベースのドメインを含むことを特徴とする請求項３２に記載のコンピュータ記録可読媒体。
【請求項３７】
前記証明書ベースのドメインは、Ｋｅｒｂｅｒｏｓ使用可能ドメインを含むことを特徴とする請求項３６に記載のコンピュータ記録可読媒体。
【請求項３８】
前記一致するプロトコルはＸ．５０９証明書を含むことを特徴とする請求項３７に記載のコンピュータ記録可読媒体。
【請求項３９】
前記セキュリティ認証要求が前記外部ノードによって生成されることを特徴とする請求項３２に記載のコンピュータ記録可読媒体。
【請求項４０】
前記セキュリティ認証要求を受信することは前記内部ノードによって実行されることを特徴とする請求項３９に記載のコンピュータ記録可読媒体。
【請求項４１】
前記セキュリティ認証要求が前記内部ノードによって生成されることを特徴とする請求項３２に記載のコンピュータ記録可読媒体。
【請求項４２】
前記セキュリティ認証要求を受信することが前記外部ノードによって実行されることを特徴とする請求項４１に記載のコンピュータ記録可読媒体。
【請求項４３】
前記方法は、前記外部ノードと前記内部ノードとの間のセッションが完了した場合に前記安全な接続を終了することをさらに含むことを特徴とする請求項３２に記載のコンピュータ記録可読媒体。
【請求項４４】
前記方法は、複数の一致するプロトコルが見つかった場合に前記安全な接続を確立する際に使用するためにプロトコルを選択することをさらに含むことを特徴とする請求項３２に記載のコンピュータ記録可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワーク接続されたコンピューティングの分野に関し、より詳細には、セキュリティ使用可能ドメインと１つまたは複数の外部ノードとの間のセキュリティプロトコルの自動ネゴシエーションに関する。
【背景技術】
【０００２】
ネットワーク接続技術の発達により、ネットワーク管理者およびその他の者が彼らのネットワークおよび他のインストールに対するより優秀かつより高度なセキュリティ制御を維持することが可能になった。Ｍｉｃｒｏｓｏｆｔ Ｗｉｎｄｏｗｓ（登録商標）ＮＴ、２０００および関連製品により、例えば管理者は、Ａｃｔｉｖｅ Ｄｉｒｅｃｔｏｒｙ（登録商標）（ＡＤ）構成を使用したセキュリティ使用可能（ｓｅｃｕｒｉｔｙ－ｅｎａｂｌｅｄ）ネットワークドメインを配置することが可能になる。公知のＫｅｂｅｒｏｓネットワーク規格も同様に、ネットワーク内のノードがキー／認証プラットフォームを使用して相互に認証することを可能にする。これらの動作技術により、ネットワーク管理者は、例えばネットワークサーバから個々のワークステーションまたは他のクライアントに均一

にインストールするためにルール、アプリケーション、パッチ、ドライブ、および他の資源を安全にプッシュすることができる場合がある。セキュリティ使用可能ドメイン内のすべてのマシンは、これらおよび他のタイプのデータの伝送を透過的に識別し、認証することができる場合がある。

【発明の開示】

【発明が解決しようとする課題】

【０００３】

しかし、セキュリティ使用可能ドメイン外にノードがある場合、ルール、アプリケーション、または他の資源をワークステーションとやり取りする機能はより困難になる。例えば、企業は、ローカルエリアネットワーク（ＬＡＮ）上に配置されたコンピュータの集合を有する場合があるが、Ａｃｔｉｖｅ　Ｄｉｒｅｃｔｏｒｙ（登録商標）または他のセキュリティ使用可能ドメインの一部ではない遠隔位置にあるコンピュータとも対話する。安全なドメインの境界を越えた通信は、一部には当該ドメイン内のマシンと当該ドメイン外のマシンとの間に接続を確立することが相互にサポートされたセキュリティプロトコルに関して合意することを要求するので、より複雑化する。

【０００４】

システム管理者および他の者は、したがって、セッションが行われる前に内部マシンと外部マシンの間の互換性のあるプロトコルを特定することにより、セキュリティ使用可能ドメインに外部エージェントまたはノードが入るための構成を試みなければならない。例えば、外部ノードは、トランスポート層セキュリティ（ＴＬＳ）プロトコル、Ｋｅｒｂｅｒｏｓベースのプロトコル、セキュアソケットレイヤ（ＳＳＬ）または他のプロトコルを介してセキュリティ使用可能ドメイン内の管理サーバと通信するよう構成することができる。このマシンは、そのプロトコル、すなわちそのデフォルトプロトコルで、プロトコルの障害を指摘し、そのプロトコルを切り替えるよう要求し、または外部ノードまたはエージェントに対して他の応答を行う。したがって、セキュリティ、トランスポート、または他のプロトコルの手動設定または調整が要求される場合があるが、これは時間が掛かりエラーが頻発する可能性のあるプロセスである。問題は他にもある。

【課題を解決するための手段】

【０００５】

当技術分野のこれらおよび他の問題を克服する本発明は、ある点で、管理者の介入を必要とせずに自動で外部エージェントまたはノードとの安全な通信を確立し身元を確認することのできるセキュリティプロトコルの自動ネゴシエーションのためのシステムおよび方法に関する。本発明によれば、ある点で、セキュリティ使用可能ドメイン内のネットワークマネージャもしくは他のエージェントまたはノードは、外部エージェントまたはノードとの安全な接続を確立するための試みを開始することができる。この要求は、マネージャが使用するために使用可能な一組のセキュリティプロトコルを示すデータフィールドを含んでいる。外部エージェントは、その要求を受信することができ、内部エージェントまたはマネージャに使用可能なプロトコルを外部エージェントがサポートする一組のプロトコルと比較することができる。使用可能なプロトコルの間の一致が見つかった場合、通信はその選択されたプロトコルに基づいて進めることができる。実施形態では、外部エージェントと内部エージェントのそれぞれはキー、証明書、または他の認証機構を介して相互に確認することができる。

【発明を実施するための最良の形態】

【０００６】

図１は、本発明の一実施形態による、プロトコルネゴシエーションプラットフォームおよび方法が動作することのできるアーキテクチャを示す図である。図から分かるように、この実施形態では、一組のクライアント、サーバ、エージェントまたは他のノード、もしくはマシンは、セキュリティ使用可能ドメイン１０２で動作することができる。セキュリティ使用可能ドメインは、実施形態では、例えばＭｉｃｒｏｓｏｆｔ　Ｗｉｎｄｏｗｓ（登録商標）Ａｃｔｉｖｅ　Ｄｉｒｅｃｔｏｒｙ（登録商標）、Ｋｅｒｂｅｒｏｓまたは他

の証明書ベースまたはキーベースのドメイン、もしくは他の閉じた、すなわち安全な分散型ディレクトリまたは他の環境であるか、またはこれらを含むことができる。セキュリティ使用可能ドメイン内には、実施形態ではサーバまたは他のノードであるかまたはこれらを含むことのできる内部マネージャ１０４と、一組の内部エージェント１０６（Ｎを任意の数としてＡ１、Ａ２．．．ＡＮで示す）を説明のために示している。

【０００７】

実施形態では、当該一組の内部エージェント１０６は、追加サーバ、ワークステーションまたは他のクライアント、もしくはセキュリティ使用可能ドメイン１０２内で動作し、内部マネージャ１０４と通信する他の内部エージェントまたはノードから構成されるか、もしくはこれらを含むことができる。実施形態では、内部マネージャ１０４は、記憶に関する動作ガイドライン（例えば、ＲＡＩＤポリシー、フェイルオーバー基準、メモリ制限）、帯域幅使用率もしくは他のルールまたはデータなど、ネットワークルールまたは他のデータを当該一組の内部エージェント１０６に送信または「プッシュ」するようなネットワーク管理機能をスケジュール設定し、または実行することができる。これらまたは他のタイプのデータを伝達する際、当該内部マネージャ１０４および当該一組の内部エージェント１０６は、ルールおよび他のデータのネットワークおよび分散の保全性を保証するためにセキュリティ使用可能ドメインのセキュリティ資源を利用することができる。

【０００８】

図に示すように、実施形態では、セキュリティ使用可能ドメイン１０２は、例えば実施形態ではＸ．５０９または他の規格またはフォーマットに従って構成された証明書であるか、またはこれを含むことのできる証明書１０８のような証明書を使用して認証サービスを提供することができる。実施形態では、キーまたは他の機構も同様に使用することができる。図に示すように、証明書１０８を内部マネージャ１０４に対する認証データと関連付け、これを提供することができる。当該一組の内部エージェント１０６のどの１つでも、検証のために証明書１０８を認証局（ｃｅｒｔｉｆｉｃａｔｅ　ａｕｔｈｏｒｉｔｙ）１１０に伝達することにより、内部マネージャ１０４から受け取ったルール、命令、または他のデータを認証することができる。認証局１１０自体を、セキュリティ使用可能ドメイン１０２内に配置してもよく、または図のようにセキュリティ使用可能ドメイン１０２外に配置してもよい。

【０００９】

実施形態では、認証局１１０は、証明書１０８または他の認証機構を読み取り、復号し、結果を当該一組の内部エージェント１０６または他のノードに戻すよう構成されたサーバまたは他のノードであるか、またはこれを含むことができる。当該一組の内部エージェント１０６のノードのそれぞれは、同様にそれらに証明書、キー、またはセキュリティ使用可能ドメイン１０２に適合する他の認証データを関連付けることができる。当該一組の内部エージェント１０６のノードは、同様に証明書または他の機構を使用して通信し、相互に互いを認証することができる。

【００１０】

図１に示した実施形態では、外部エージェント１１４は、同様に通信ネットワーク１１２を介して内部マネージャ１０４と通信するよう構成されている。外部エージェント１１４もまた、サーバ、ワークステーション、もしくは他のノードまたは資源であるか、またはこれを含むことができる。外部エージェント１１４は同様に、認証のために外部エージェント１１４を特定する証明書１１６をそれ自体に関連付けることができる。実施形態では外部エージェント１１４がそれを介して内部マネージャ１０４または他の内部ノードと通信することのできる通信ネットワーク１１２は、例えばインターネット、イントラネット、ローカルエリアネットワーク（ＬＡＮ）、ワイドエリアネットワーク（ＷＡＮ）、メトロポリタンエリアネットワーク（ＭＡＮ）、ストレージエリアネットワーク（ＳＡＮ）、フレームリレー接続、Ａｄｖａｎｃｅｄ　Ｉｎｔｅｌｌｉｇｅｎｔ　Ｎｅｔｗｏｒｋ（ＡＩＮ）接続、同期光伝送網（ＳＯＮＥＴ）接続、デジタルＴ１、Ｔ３、Ｅ１、またはＥ３回線、Ｄｉｇｉｔａｌ　Ｄａｔａ　Ｓｅｒｖｉｃｅ（ＤＤＳ）接続、ＡＴＭ（非同期転

送モード）接続、ＦＤＤＩ（ファイバー分散データインターフェース）、Ｃｏｐｐｅｒ Ｄｉｓｔｒｉｂｕｔｅｄ Ｄａｔａ Ｉｎｔｅｒｆａｃｅ（ＣＤＤＩ）、または他の有線、無線、または光接続のどれか１つまたは複数であるか、またはこれを含むことができるか、もしくはこれとインターフェースすることができる。外部エージェント１１４は、実施形態では、ワークステーション、サーバ、無線ネットワーク使用可能デバイス、またはネットワーク接続された通信用に構成された他のノード、エージェントまたはプラットフォームであるか、もしくはこれを含むことができる。

【００１１】

ドメイン横断通信（ｃｒｏｓｓ－ｄｏｍａｉｎ ｃｏｍｍｕｎｉｃａｔｉｏｎ）の従来の実施態様とは異なり、本発明の実施形態によれば、外部エージェント１１４は、自動的かつ透過的な方法で互換性のあるプロトコルを相互に選択して相互に互換性のあるプロトコルに基づいて安全な接続を確立するために、内部マネージャ１０４との連絡を開始することができる。例えば図２に示すように、外部エージェント１１４で実行中の外部アプリケーション１３０は、外部ネゴシエーションエンジン１２６を介して内部マネージャ１０４との連絡を開始することができる。外部アプリケーション１３０は、例えばデータバックアップスケジューラ、ファイアーウォール、ウイルス保護または他のアプリケーションのようなシステムユーティリティ、プロダクティビティ、または他のアプリケーションであるか、またはこれを含むことができる。外部アプリケーション１３０は、様々なタスクを実行するために、例えばユーザプロファイル、更新、または他のデータを要求し、したがって内部マネージャ１０４とのそのような通信を開始することができる。

【００１２】

外部ネゴシエーションエンジン１２６は、セキュリティ使用可能ドメイン１０２で内部マネージャ１０４と相互に互換性のある通信リンクを確立するために外部アプリケーション１３０が要求した通信を処理し管理することができる。図に示すように、実施形態では、外部ネゴシエーションエンジン１２６は、公知のＳｉｍｐｌｅ ａｎｄ Ｐｒｏｔｅｃｔｅｄ ＧＳＳ－ＡＰＩネゴシエーション（ＳＰＮＥＧＯ）プロトコルの実施態様として示されているネゴシエーションモジュール１１８を開始し管理することができる。他のプロトコルを使用することもできる。実施形態では、ネゴシエーションモジュール１１８は、例えばアプリケーションプログラミングインターフェース（ＡＰＩ）または他の機構を介して外部エージェント１１４のオペレーティングシステムによりアクセスし、開始し、または生成することができる。

【００１３】

外部ネゴシエーションエンジン１２６は同様に、外部エージェント１１４がプロトコルネゴシエーションプロセスを実行するために利用することのできるメッセージベースの、または他のチャネルを示す外部トランスポート指定子１２０を含むか、または生成することができる。例えば、実施形態では、外部アプリケーション１３０もしくは他のソフトウェアまたはモジュールが、例えば動的リンクライブラリ（ｄｌｌ）または標準の暗号化または他の符号化方式をサポートする他の資源にアクセスすることを可能にして、外部トランスポート指定子１２０はＳｅｃｕｒｉｔｙ Ｓｕｐｐｏｒｔ Ｐｒｏｖｉｄｅｒ Ｉｎｔｅｒｆａｃｅ（ＳＳＰＩ）プロトコルをＭｉｃｒｏｓｏｆｔ．ＮＥＴアーキテクチャの一部として指定することができる。他のプロトコルを外部トランスポート指定子１２０内に使用または指定することができる。外部ネゴシエーションエンジン１２６はしたがって、そのデータまたは他のデータを示すデータグラムを、図２に示すように内部マネージャ１０４に関連付けられた内部ネゴシエーションエンジン１２８に伝達することができる。

【００１４】

内部ネゴシエーションエンジン１２８は同様に、ネゴシエーションモジュール１２２と内部トランスポート指定子１２４を含むか、またはこれとインターフェースすることができる。内部ネゴシエーションエンジン１２８は、内部マネージャ１０４によって実行され、またはアクセスされる内部アプリケーション１３２と通信することができる。内部アプリケーション１３２は、例えば、システム管理、プロダクティビティ、または他のアプリ

ケーションであるか、またはこれを含むことができる。内部マネージャ１０４との通信の確立を求める要求を受信した際、内部ネゴシエーションエンジン１２８は、内部トランスポート指定子１２４による外部エージェント１１４とのメッセージベースの、または他のチャネルを、例えばＳＳＰＩプロトコルを使用してチャネル通信を確認して、確立することができる。

【００１５】

外部エージェント１１４と内部マネージャ１０４との間に確立された予備チャネルにより、外部ネゴシエーションエンジン１２６と内部ネゴシエーションエンジン１２８はプロトコルネゴシエーションと低減（ｒｅｄｕｃｔｉｏｎ）を開始することができる。実施形態では、外部エージェント１１４は、図３に示すような外部プロトコルテーブル１３４を内部マネージャ１０４に送信することができる。外部プロトコルテーブル１３４は、どのプロトコルを使用して外部エージェント１１４を構成できるかを指定することができる。内部マネージャ１０４が受信した際、外部プロトコルテーブル１３４を、内部マネージャ１０４が使用するために使用可能な一組のセキュリティプロトコルを示す内部プロトコルテーブル１３６と比較することができる。外部プロトコルテーブル１３４と内部プロトコルテーブル１３６のどちらか一方は、例えばトランスポート層セキュリティ（ＴＬＳ）、セキュアソケットレイヤ（ＳＳＬ）、Ｋｅｒｂｅｒｏｓ、セキュアＩＰ（ＩＰＳｅｃ）、または他の使用可能なプロトコルまたは規格を示すフィールドを含むことができる。内部マネージャ１０４に関連付けられた内部ネゴシエーションエンジン１２８は、図３に示すように外部エージェント１１４と内部マネージャ１０４によって相互にサポートされた１つまたは複数のプロトコルを示すことができる。

【００１６】

内部ネゴシエーションエンジン１２８は、実施形態では、同様に、類似のプロトコル比較のために内部プロトコルテーブル１３６を外部エージェント１１４に関連付けられた外部ネゴシエーションエンジン１２６に伝達することができる。この結果、ネゴシエーションエンジン１２６およびネゴシエーションエンジン１２８は、セキュリティ使用可能ドメインを横断して安全な通信を確立するために相互に使用可能なプロトコルの選択をネゴシエートすることができる。例えば、外部エージェント１１４と内部マネージャ１０４との両方に対して共通プロトコルが１つしか使用可能でない場合、外部エージェント１１４と内部マネージャ１０４は、ＴＬＳまたは他のプロトコルなどのプロトコルを使用してセッションをセットアップすることに同意することができる。外部ネゴシエーションエンジン１２６と内部ネゴシエーションエンジン１２８とが共通のプロトコルを見つけられないということで一致した場合、ドメイン横断通信を確立するための試みを終了することができる。反対に、外部ネゴシエーションエンジン１２６と内部ネゴシエーションエンジン１２８とが共通した複数のプロトコルを特定した場合、転送速度、キーのビット深度または他のセキュリティ機構のようなネットワーク基準、もしくは他の要因に基づいて１つのプロトコルを選択することができる。

【００１７】

相互に互換性のあるプロトコルが整備されている場合、外部エージェント１１４と内部マネージャ１０４の間に安全なセッションを確立することができる。実施形態では、追加されたセキュリティのために、外部エージェント１１４と内部マネージャ１０４のそれぞれが同様に、相手ノードの識別、特権レベル、または他のセキュリティ詳細を検証するために認証ステップを実行することができる。図１に示すように、これは証明書または他のセキュリティ機構を使用して実行することができる。外部エージェント１１４は、証明書１０８を認証局１１０に伝達することによって内部マネージャ１０４を認証することができる。内部マネージャ１０４は、反対に、証明書１１６を認証局１１０に伝達することによって外部エージェント１１４を認証することができる。他のセキュリティ機構を使用することもできる。

【００１８】

外部エージェント１１４と内部マネージャ１０４との間で交換されるデータのタイプま

たはコンテンツは、実施形態では、これら２つのノード間の相互認証に基づくことができる。例えば、ネットワーク管理ルールまたはパラメータに対するアクセスを、所与のレベルのアクセス特権だけを示す内部または外部ノードに対して確保することができる。他の認証ルールまたは基準も使用することができる。操作セキュリティプロトコルを確立しており、認証処理が１つでも完了した後では、外部エージェント１１４と内部マネージャ１０４とは、データ、アプリケーション、ルール、または他の情報を交換することができる。トラフィックが完了した場合、外部ネゴシエーションエンジン１２６と内部ネゴシエーションエンジン１２８とは通信リンクを解放または終了することができる。

【００１９】

本発明の一実施形態によるネットワークネゴシエーション処理全体を図４に示す。ステップ４０２で、処理を開始することができる。ステップ４０４で、セキュリティ使用可能ドメイン１０２を横断して安全な接続を確立することを求める要求は、外部エージェント１１４、内部マネージャ１０４、もしくは他のクライアント、エージェント、またはノードのどれかで生成することができる。ステップ４０６で、安全な接続を確立することを求める、送信側ノードと互換性のある第１のプロトコルセットを組み込んだ要求を、内部マネージャ１０４、外部エージェント１１４、もしくは他のクライアント、エージェントまたはノードのどれかである受信側ノードに送信することができる。ステップ４０８で、この要求は受信側ノードによって受信することができる。ステップ４１０で、内部マネージャ１０４、外部エージェント１１４、もしくは他のクライアント、エージェントまたはノードのどれかである受信側ノードは、使用可能なプロトコル間で一致を見つけることができるか否かを判定するために第１のプロトコルセットを受信側ノードの第２のプロトコルセットと比較する。

【００２０】

第１のプロトコルセットと第２のプロトコルセットの間に一致が見つかった場合、処理はステップ４１２に進むことができ、そこで複数の一致するプロトコルが見つかったか否かに関して判定することができる。複数の一致するプロトコルセットが見つかった場合、処理はステップ４１４に進むことができ、そこで一致する複数のプロトコルの１つを、転送速度、キーのビット深度、または他のセキュリティ機構のようなプロトコル基準、もしくは他の要因に基づいて使用するために選択することができる。次いで処理はステップ４１６に進むことができ、そこで安全な接続またはセッションを、選択されたプロトコルに基づいて外部エージェント１１４と内部マネージャ１０４との間で開始することができる。同様に、ステップ４１２で一致するプロトコルが１つしか見つからなかった場合、処理はステップ４１６に進むことができ、そこで安全な接続またはセッションを開始することができる。例えば、実施形態では、指定されたポートをＴＣＰ／ＩＰまたは他の通信または他のプロトコルの下で開くことができる。

【００２１】

ステップ４１８で、利用される一致するプロトコルに従ってハンドシェーキングおよび他のステップを進めて、プロトコル特定交換を外部エージェント１１４と内部マネージャ１０４との間で開始することができる。ステップ４２０で、外部エージェント１１４と内部マネージャ１０４のどちらかまたは両方を、適宜、対応する（外部エージェント１１４の）証明書１１６または（内部マネージャの）証明書１０８を認証局１０８に送ることによって、対応する他のノードを認証することができる。実施形態では、証明書１１６または証明書１０８もしくは他のセキュリティデータは、Ｘ．５０９規格または他の規格またはフォーマットに準拠する証明オブジェクトであるか、またはこれを含むことができる。適切な認証が完了すると、処理はステップ４２２に進むことができ、そこで外部エージェント１１４と内部マネージャ１０４との間で安全な接続またはセッションを実行することができる。例えば、ネットワークまたは他のルールを、システム管理または他の目的のためにこれら２つのノード間で伝達することができる。

【００２２】

安全なセッションが完了すると、処理はステップ４２４に進み、そこで外部エージェン

ト１１４と内部マネージャ１０４との間の安全な接続を終了するかまたは解放することができる。ステップ４２６では、処理を終了するか、反復するか、前の処理点に戻るか、または他の行動を取ることができる。同様に、ステップ４１０の判定で一致するプロトコルが特定されなかった場合、処理は、終了するか、反復するか、前の処理点に戻るか、または他の行動を取るためにステップ４２６に進むことができる。

【００２３】

本発明の上記の記述は説明を目的としたものであり、当業者には構成および実施態様に対する修正が想起されよう。例えば、本発明は全般に単一の外部エージェント１１４に関して説明したが、実施形態では、セキュリティ使用可能ドメイン１０２内の内部マネージャ１０４もしくは他のクライアントまたはノードと一致するプロトコルを自動的にネゴシエートするよう複数の外部エージェントまたはノードを構成することができる。同様に、認証機構を全般にＸ．５０９または他の規格を使用して単一の認証エンティティである認証局１１０がサポートしているように記載したが、実施形態では、複数の認証エンティティもしくは他の認証または認可プラットフォームを使用することもできる。他のハードウェア、ソフトウェア、または１つのものとして記載した他の資源を実施形態では分散させることができ、同様に実施形態では分散されたものとして記載された資源を結合することができる。

【００２４】

さらに、セキュリティ使用可能ドメイン１０２外部のノードまたはエージェントと当該ドメイン内部のノードまたはエージェントの一方または他方の例を、安全なプロトコルのネゴシエーションを開始するように度々記載したが、本発明に従い構成された、ドメイン外部または内部のいかなるノードまたはエージェントでもプロトコル処理を開始することができるということが理解されよう。同様に、内部および外部エージェントのどちらか一方または両方は他方のエージェントまたはノードの認証を開始することができる。したがって、本発明の範囲は添付の特許請求の範囲によってのみ限定されるものである。

【図面の簡単な説明】

【００２５】

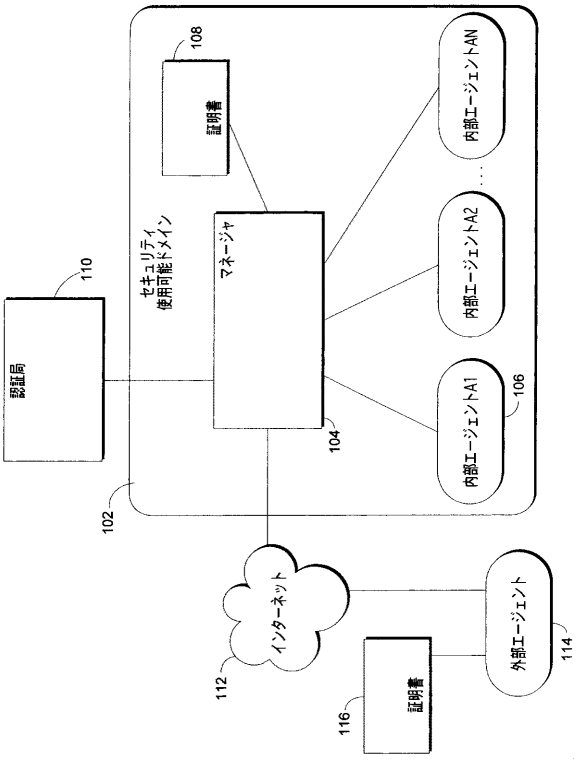
【図１】本発明の一実施形態が動作することのできるネットワークアーキテクチャを示す図である。

【図２】本発明の一実施形態による内部ノードと外部ノードの間のネゴシエーションプロセスを示す図である。

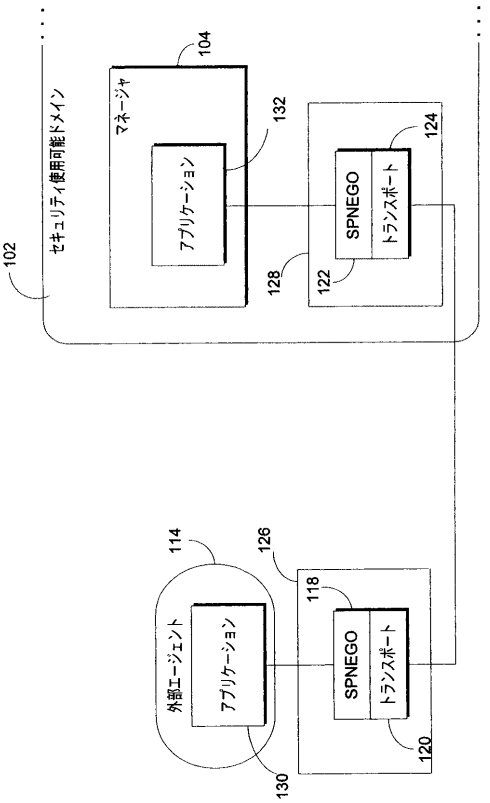
【図３】本発明の一実施形態によるプロトコルテーブル間の比較を示す図である。

【図４】本発明の一実施形態によるプロトコルネゴシエーション処理全体を示す図である。

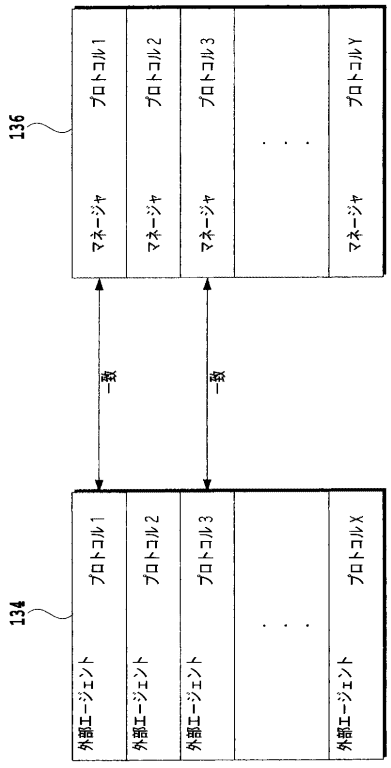
【図１】


108
証明書
内部エージェントAN
セキュリティ使用可能ドメイン
マネージャ
内部エージェントA2
110
認証局
内部エージェントA1
106
104
102
インターネット
外部エージェント
114
112
証明書
116

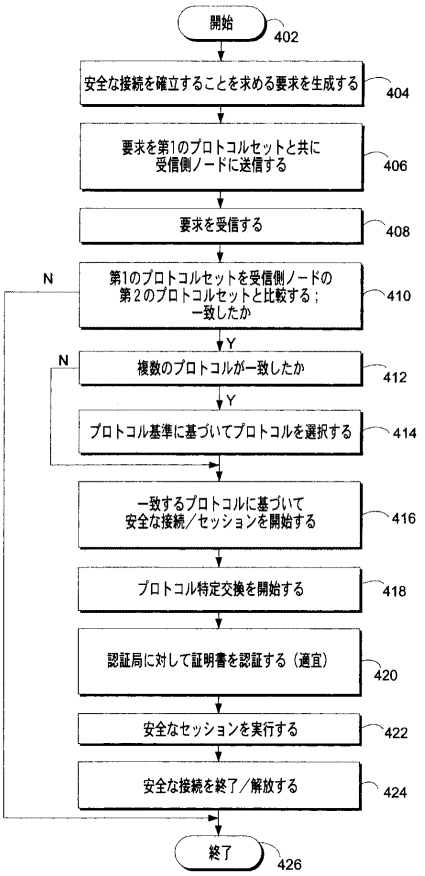
【図２】


104
セキュリティ使用可能ドメイン
マネージャ
132
アプリケーション
124
SPNEGO
トランスポート
102
128
122
114
126
外部エージェント
アプリケーション
118
SPNEGO
トランスポート
130
120

【図３】


136
プロトコル1
プロトコル2
プロトコル3
プロトコルY
マネージャ
一致
一致
134
プロトコル1
プロトコル2
プロトコル3
プロトコルX
外部エージェント

【図４】


開始
402
安全な接続を確立することを求める要求を生成する
404
要求を第1のプロトコルセットと共に
受信側ノードに送信する
406
要求を受信する
408
第1のプロトコルセットを受信側ノードの
第2のプロトコルセットと比較する；
一致したか
410
N
Y
複数のプロトコルが一致したか
412
N
Y
プロトコル基準に基づいてプロトコルを選択する
414
一致するプロトコルに基づいて
安全な接続／セッションを開始する
416
プロトコル特定交換を開始する
418
認証局に対して証明書を認証する（適宜）
420
安全なセッションを実行する
422
安全な接続を終了／解放する
424
終了
426

フロントページの続き

審査官　間野　裕一

(56)参考文献　特開２０００－３１５９９７（ＪＰ，Ａ）
米国特許第５０１０５７２（ＵＳ，Ａ）
国際公開第９９／３８０８１（WO，Ａ１）
米国特許第５８２８８９３（ＵＳ，Ａ）
米国特許出願公開第２００２／００７８３７１（ＵＳ，Ａ１）
米国特許出願公開第２００２／０１５７０１９（ＵＳ，Ａ１）
及川晴生，実践！インターネットＶＰＮ　第４回　ＩＰｓｅｃのオプション設定，ＮＥＴＷＯＲＫ　ＭＡＧＡＺＩＮＥ，株式会社アスキー，２００３年　２月　１日，第８巻，第２号，第１９４－１９７頁

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０
Ｈ０４Ｌ　９／３２
Ｈ０４Ｌ　２９／０６