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

特許第5714596号
(P5714596)

(45)発行日　平成27年5月7日(2015.5.7)　(24)登録日　平成27年3月20日(2015.3.20)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675D
G09C 1/00	(2006.01)	H04L	9/00	675A
G06F 21/33	(2013.01)	G09C	1/00	640E
		H04L	9/00	675B
		G06F	21/33	

請求項の数 13　(全 15 頁)

(21)出願番号	特願2012-538846(P2012-538846)
(86)(22)出願日	平成22年10月28日(2010.10.28)
(65)公表番号	特表2013-511209(P2013-511209A)
(43)公表日	平成25年3月28日(2013.3.28)
(86)国際出願番号	PCT/US2010/054573
(87)国際公開番号	WO2011/059774
(87)国際公開日	平成23年5月19日(2011.5.19)
審査請求日	平成25年10月10日(2013.10.10)
(31)優先権主張番号	12/616,789
(32)優先日	平成21年11月12日(2009.11.12)
(33)優先権主張国	米国(US)

(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　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(74)代理人　100091214
弁理士　大貫　進介

最終頁に続く

(54)【発明の名称】証明書属性に基づくＩＰセキュリティ証明書交換

(57)【特許請求の範囲】

【請求項１】

リモートエンドポイントからデジタル証明書を受信する、ローカルエンドポイントの通信コンポーネントであって、前記受信されるデジタル証明書は前記ローカルエンドポイントのデジタル証明書を発行したのと同じ認証機関によって発行されたものであり、受信されるデジタル証明書は該デジタル証明書のセキュリティコンテキストを定義する証明書属性をもつ、通信コンポーネントと、

受信されたデジタル証明書の証明書属性の１つまたは複数を参照することによって、前記リモートエンドポイントとのＩＰｓｅｃ（インターネットプロトコルセキュリティ）通信を検証し、ルート証明書を使用して前記ＩＰｓｅｃ通信をさらに検証する、前記ローカルエンドポイントのセキュリティコンポーネントと

を備えた、コンピュータ実装されるセキュリティシステムであって、

証明書属性は少なくともサービス品質（ＱｏＳ）データを含む、

システム。

【請求項２】

証明書属性はさらに、セキュリティコンテキストの一意のＩＤ、ＩＰｓｅｃセッションを確立する相手となれる少なくとも一つのエンドポイントの一つまたは複数のＩＰアドレスまたはプロキシシステムのＩＰアドレスのうちの少なくとも一つを含むことを特徴とする請求項１に記載のシステム。

【請求項３】

前記デジタル証明書は、ある特定の証明書属性にロックされることを特徴とする請求項１に記載のシステム。
【請求項４】
前記デジタル証明書は、ある特定のアドレスまたはアドレスグループにロックされることを特徴とする請求項１に記載のシステム。
【請求項５】
前記認証機関が複数ゾーンに渡るＩＰｓｅｃ通信のための前記デジタル証明書および他のデジタル証明書を発行することを特徴とする請求項１に記載のシステム。
【請求項６】
前記セキュリティコンポーネントは、属性優先度に従って証明書属性を処理することを特徴とする請求項１に記載のシステム。
【請求項７】
前記１つまたは複数の証明書属性は、プロキシシステムのＩＰアドレスおよびゾーンを含むことを特徴とする請求項１に記載のシステム。
【請求項８】
第一のエンドポイントにおいて、ピアエンドポイントからデジタル証明書を受信するステップであって、受信されるデジタル証明書は前記第一のエンドポイントのデジタル証明書を発行したのと同じ認証機関によって発行されたものであり、受信されるデジタル証明書は該デジタル証明書のセキュリティコンテキストを定義する１つまたは複数の証明書属性をもつ、ステップと、
前記第一のエンドポイントによって、前記１つまたは複数の証明書属性およびルート証明書に基づいて、前記ピアエンドポイントのセキュリティコンテキストを検証するステップと、
前記セキュリティコンテキストの検証に基づいて、前記第一のエンドポイントと前記ピアエンドポイントとの間にＩＰｓｅｃセッションを確立することを前記第一のエンドポイントが許可するステップと
を含む、コンピュータが実施するセキュリティ方法であって、
証明書属性は少なくともサービス品質（ＱｏＳ）データを含む、
方法。
【請求項９】
前記認証機関が複数ゾーンを管理することを特徴とする請求項８に記載の方法。
【請求項１０】
前記証明書を、ある特定の属性にロックダウンするステップをさらに備えたことを特徴とする請求項８に記載の方法。
【請求項１１】
前記セキュリティコンテキストがＩＰｓｅｃセッションを確立する相手となれる特定のエンドポイントのＩＰアドレスを含むことを特徴とする請求項８に記載の方法。
【請求項１２】
前記セキュリティコンテキストがＩＰｓｅｃセッションを確立する相手となれるエンドポイントのグループのＩＰアドレスの範囲を含むことを特徴とする請求項８に記載の方法。
【請求項１３】
受信されたデジタル証明書の属性を、前記第一のエンドポイントのセキュリティデータと比較して、前記ピアエンドポイントを前記第一のエンドポイントに対して検証するステップをさらに備えたことを特徴とする請求項８に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、証明書属性に基づくＩＰセキュリティ証明書交換に関する。
【背景技術】

【０００２】
ＩＰｓｅｃ（インターネットプロトコルセキュリティ）は、ＩＰパケットに対する認証および暗号化サービス、ならびに通信ピアの相互認証を提供する。２つのピアエンドポイントの間のＩＰｓｅｃ通信は通常、２つのフェーズ、すなわちトラフィック保護パラメータの相互認証および交渉と、ピア間のトラフィックへの保護パラメータの適用（たとえば、暗号化および／または認証）とを伴う。第１のフェーズでは、ピアが互いを認証するための一技法は、証明書を使用することによる。接続の各ピアエンドポイントは、対応するエンドポイントが他のエンドポイントとのＩＰｓｅｃセッションに参加することを承認する証明書を与えられる。２つのエンドポイントが、証明書に基づくＩＰｓｅｃセッションを確立するために、両方のマシンは、信頼される共通の認証機関からの証明書をもっている必要がある。
【０００３】
一部のデータセンタでは、複数の分離コンテキストを確立することが望ましい場合がある。たとえば、ＩＳＰ（インターネットサービスプロバイダ）は、複数の顧客をもつ場合があり、各顧客に安全な分離したゾーンを提供する必要がある。この分離を現在のインフラストラクチャで遂行するために、ＩＳＰは、各ゾーンごとに認証機関を展開する。複数の認証機関の展開および維持は、時間を消費し、労働集約的なプロセスである。
【発明の概要】
【０００４】
以下は、本明細書に記載するある新規実施形態を基本的に理解させるために、簡略化した要約を提示している。この要約は、広範な概要ではなく、主要／重大な要素を明らかにすることも、その範囲を定めることも意図していない。その唯一の目的は、後で提示する、より詳細な説明の前置きとして、ある概念を簡略化した形で提示することである。
【０００５】
開示するアーキテクチャは、証明書属性に基づくＩＰｓｅｃ（インターネットプロトコルセキュリティ）証明書交換を提供する。これにより、あるＩＰｓｅｃエンドポイントは、別のＩＰｓｅｃエンドポイントの証明書のセキュリティコンテキストを、証明書ルートに加えて証明書属性を参照することによって検証することが可能になる。証明書ルートだけではなく証明書属性を使ってＩＰｓｅｃ証明書交換を容易にすることによって、ゾーンごとに１つの認証機関を必要とするのではなく、単一の認証機関を使う複数の分離したネットワークゾーンを構築することが可能になっている。
【０００６】
さらに、ＩＰｓｅｃ証明書交換中に証明書属性が使用可能であることを、より集中型の通信に活用することができる。たとえば、ＱｏＳ（サービス品質）フィールドを使って、あるエンドポイントに、別のエンドポイントよりも高い優先度を与えることができる。
【０００７】
さらに、証明書属性をＩＰｓｅｃ証明書交換プロセス中に使用して、エンドポイントのセキュリティコンテキストを識別することができる。たとえば、証明書は、セキュリティコンテキストの一意のＩＤ（識別子）である属性を含み得る。受信側ＩＰｓｅｃエンドポイントが別のエンドポイントから要求を受信すると、受信側エンドポイントは、現在のマシンにインストールされた証明書のセキュリティコンテキストが、要求元の証明書のセキュリティコンテキストと同じであることを検証することができる。
【０００８】
さらに、ＩＰｓｅｃ証明書の使用を、単一ＩＰまたはＩＰグループのためにロックダウンすることができる。ＩＰｓｅｃ証明書中の属性の１つは、証明書と一緒に使うことができるＩＰアドレス（複数可）とすることができる。これにより、異なるＩＰアドレスをもつ別のマシン上で証明書がコピーされ、再利用されることを防止する。
【０００９】
上記および関連する目的の遂行のために、本明細書では、特定の例示的態様を、以下の説明および添付の図面に関連して説明する。こうした態様は、本明細書に開示する原理が

実施され得る様々なやり方を示し、その態様および等価物はすべて、本特許請求対象の範囲内であることを意図している。他の利点および新規特徴が、以下の詳細な説明を図面と併せて検討すると明らかになるであろう。

【図面の簡単な説明】

【００１０】

【図１】本開示アーキテクチャによるコンピュータ実施セキュリティシステムを示す図である。

【図２】複数ゾーンに渡る証明書生成および管理のための認証機関含むセキュリティシステムを示す図である。

【図３】単一ゾーンのサブゾーン内での証明書生成および管理のための認証機関を含むセキュリティシステムを示す図である。

【図４】ＩＰｓｅｃ通信のためのデジタル証明書中で利用することができる例示的な証明書属性を示す図である。

【図５】コンピュータ実施セキュリティ方法を示す図である。

【図６】図５の方法の追加態様を示す図である。

【図７】あるＩＰアドレスに対するＩＰｓｅｃ証明書を処理する方法を示す図である。

【図８】開示するアーキテクチャによる、ＩＰｓｅｃ通信のための属性処理を実行するように動作可能なコンピューティングシステムを示すブロック図である。

【図９】ＩＰｓｅｃ通信のための証明書属性を処理するコンピューティング環境を示す概略的なブロック図である。

【発明を実施するための形態】

【００１１】

開示するアーキテクチャは、証明書属性に基づくＩＰｓｅｃ（インターネットプロトコルセキュリティ）証明書交換をもたらす。この交換により、それぞれが証明書を有する２つのＩＰｓｅｃエンドポイントが、証明書ルートに加えて証明書属性を参照することによって、他方のセキュリティコンテキストを検証することが可能になる。複数の分離したネットワークゾーンのこのような作成が、今では、ゾーンごとに１つの認証機関を必要とするのではなく、単一の認証機関を使って可能である。

【００１２】

ここで図面を参照するが、同じ参照番号が、全体を通して同じ要素を指すのに使われている。以下の記述では、説明目的で、多数の具体的詳細を、その完全な理解のために記載する。ただし、新規実施形態は、こうした具体的詳細なしで実施され得ることが明らかであろう。他の事例では、公知の構造およびデバイスを、その説明を容易にするためにブロック図の形で示す。意図するところは、本特許請求対象の精神および範囲内であるすべての修正形態、等価物、および代替形態をカバーすることである。

【００１３】

図１は、開示するアーキテクチャによるコンピュータ実施セキュリティシステム１００を示す。システム１００は、リモートエンドポイント１０８からデジタル証明書１０６を受信する、ローカルエンドポイント１０４の通信コンポーネント１０２を含む。通信コンポーネント１０２は、データパケットを送信し、受信するハードウェアおよび／またはソフトウェアを少なくとも含み得る。デジタル証明書１０６は、証明書属性を含む。システム１００は、証明書属性の１つまたは複数を処理して、リモートエンドポイント１０８とのＩＰｓｅｃ通信を検証する、ローカルエンドポイント１０４のセキュリティコンポーネント１１０も含み得る。

【００１４】

言い換えると、システム１００は、ルート証明書のみに基づく場合よりも、証明書属性を使うＩＰｓｅｃ中のピア証明書の検証を容易にする。各ピア証明書は、証明書のセキュリティコンテキストを記述する属性を含む。たとえば、ＩＰｓｅｃ証明書中の属性の１つは、顧客ＩＤとすることができる。

【００１５】

エンドポイント間でのＩＰｓｅｃ証明書交換（ローカルエンドポイント１０４が、その証明書１１２をリモートエンドポイント１０８に送信する）の間、各エンドポイントは、ピアによって提示される証明書の属性を調べ、ＩＰｓｅｃセッションのセットアップに関する決定を行うことができる。上記例において、ピアによって提示された証明書が同じ顧客ＩＤを含む場合、ＩＰｓｅｃセッションが許可される。ただし、両方の証明書（リモート証明書１０６およびローカル証明書１１２）は依然として、単一の認証機関によって発行される必要がある。このソリューションは、展開されている分離コンテキストの数に関わらず、ただ１つの認証機関を使用する。

【００１６】

別の態様は、ＩＰｓｅｃ証明書を、ある特定のＩＰアドレスまたはアドレス群にロックすることによってセキュリティを高めることができることである。たとえば、証明書は、証明書がその上で使われることが意図される物理ネットワークのＩＰアドレス（またはアドレスグループ）を含み得る。ＩＰｓｅｃ接続をオープンするとき、各エンドポイントは、他方のエンドポイントが使っている実際のＩＰアドレスを、提示された証明書中のＩＰアドレスのリストと比較する。他方のエンドポイントのＩＰアドレスがリストにある場合、接続は継続する。アドレスがリストにない場合は、たとえば、攻撃者が正当なマシンから異なる（無許可）マシンに証明書を何とかしてコピーした乗っ取りの試みを示し得るので、接続は失敗することになる。開示するアーキテクチャは、このような攻撃を検出する機能を提供し、そうすることによって、ソリューションの全体的セキュリティを高める。

【００１７】

上で示したように、セキュリティコンポーネント１１０は、ルート証明書を使ってＩＰｓｅｃ通信を検証することもできる。デジタル証明書１０６（および証明書１１２）は、デジタル証明書のセキュリティコンテキストを定義する１つまたは複数の証明書属性を含む。さらに、デジタル証明書は、ある特定のアドレスやアドレスグループなど、ある特定の証明書属性のためにロックすることができる。セキュリティコンポーネント１１０は、属性優先度に従って証明書属性を処理することができる。

【００１８】

言い換えると、ある属性に、別の属性または属性セットを上回る重みを与えることができる。たとえば、ＱｏＳ（サービス品質）属性を使用して、あるエンドポイントに、別のエンドポイントより高い優先度を与えることができる。属性分析プロセスは、証明書属性（複数可）を所定の属性セットと比較することも含むことができ、全属性が一致する場合、ＩＰｓｅｃセッションを確立することができる。ただし、３つのうち２つしか一致しない場合、セッションは失敗し、または通信レベルを低下させて行われる。

【００１９】

１つまたは複数の証明書属性は、それを通してエンドポイントが通信し、かつ／またはゾーンが置かれているプロキシシステムのＩＰアドレスを含み得る。ピアリモートエンドポイント１０８は、ローカルデジタル証明書１１２またはリモートエンドポイント１０８が他のピアエンドポイントから受信し得る他の証明書を受信し処理するローカルエンドポイント１０４として、同様のコンポーネント（たとえば、通信コンポーネントおよびセキュリティコンポーネント）も含み得ることに留意されたい。

【００２０】

図２は、複数ゾーンに対する証明書生成および管理のための認証機関２０２を含むセキュリティシステム２００を示す。認証機関２０２はここでは、複数ゾーンに渡るＩＰｓｅｃ通信のためのデジタル証明書を生成し管理する（発行する）ために展開される単一（ただ１つ）の機関とすることができる。ここで、システム２００は、２つのゾーン、すなわち第１のゾーン（Ｚｏｎｅ１）、および第２のゾーン（Ｚｏｎｅ２）を含む（ただし、より多くのゾーンを利用することができる）。第１のゾーンは、第１のゾーンの証明書２０８（Ｄｉｇ　Ｃｅｒｔ$_{11}$）を受信し使用する第１のゾーンのエンドポイント２０６など、複数のエンドポイント２０４（Ｅｎｄｐｏｉｎｔ$_{11}$、．．．、Ｅｎｄｐｏｉｎｔ$_{1S}$）（エンドポイント２０４のそれぞれは、デジタル証明書が発行される）を含む。同様に

、第２のゾーンは、第２のゾーンの証明書２１４（Ｄｉｇ　Ｃｅｒｔ$_{21}$）を受信し使用する第２のゾーンのエンドポイント２１２など、複数のエンドポイント２１０（Ｅｎｄｐｏｉｎｔ$_{21}$、．．．、Ｅｎｄｐｏｉｎｔ$_{2T}$）（エンドポイント２１０のそれぞれは、デジタル証明書が発行される）を含む。

【００２１】

認証機関２０２は、ネットワーク２１６を介して第１および第２のゾーン両方、および関連づけられたエンドポイントに対して、ならびに場合によってはネットワーク２１６の外のエンドポイントおよびゾーンに対して、証明書管理を行う唯一の認証機関とすることができる。

【００２２】

動作中、第１のゾーンのエンドポイント２０６が、第２のゾーンのエンドポイント２１２とのＩＰｓｅｃセッションを要求する場合、エンドポイント（２０６、２１２）は、対応するデジタル証明書（２０８、２１４）を、ＩＰｓｅｃ接続を介して交換する。第１のゾーンのエンドポイント２０６は、第２のゾーンのエンドポイント２１２が第１のゾーンの証明書２０８に対してそうするように、１つまたは複数のセキュリティコンテキスト属性、および可能性としては他の属性に関して第２のゾーンの証明書２１４を分析する。さらに、第１および第２のゾーンのエンドポイント（２０６、２１２）のルート証明書を渡したり、検証することができる。両方のエンドポイントからの検証が成功した場合、エンドポイント（２０６、２１２）間にＩＰｓｅｃセッションを確立することができる。

【００２３】

図３は、単一ゾーンのサブゾーン内での証明書生成および管理のための認証機関２０２を含むセキュリティシステム３００を示す。認証機関２０２はやはり、複数のサブゾーン（またはセグメント）に渡るＩＰｓｅｃ通信およびセッションのためのデジタル証明書を生成し管理する（発行する）ために展開される単一（ただ１つ）の機関とすることができる。ここで、システム３００は、あるゾーンの２つのサブゾーン、すなわち第１のサブゾーン（Ｓｕｂｚｏｎｅ１）、および第２のサブゾーン（Ｓｕｂｚｏｎｅ２）を含む（ただし、より多くのサブゾーンを利用することができる）。第１のサブゾーンは、第１のサブゾーンの証明書３０４（Ｄｉｇ　Ｃｅｒｔ$_{11}$）を受信し使用する第１のサブゾーンのエンドポイント３０２など、複数のエンドポイント２０４（Ｅｎｄｐｏｉｎｔ$_{11}$、．．．、Ｅｎｄｐｏｉｎｔ$_{1S}$）（各エンドポイントは、デジタル証明書が発行される）を含む。同様に、第２のサブゾーンは、第２のサブゾーンの証明書３０８（Ｄｉｇ　Ｃｅｒｔ$_{21}$）を受信し使用する第２のサブゾーンのエンドポイント３０６など、複数のエンドポイント２１０（Ｅｎｄｐｏｉｎｔ$_{21}$、．．．、Ｅｎｄｐｏｉｎｔ$_{2T}$）（各エンドポイントは、デジタル証明書が発行される）を含む。

【００２４】

認証機関２０２は、ネットワーク２１６を介して第１および第２のサブゾーンの両方、および関連づけられたエンドポイントに対して、ならびに場合によってはネットワーク２１６の外のエンドポイントおよびゾーン／サブゾーンに対して証明書管理を行う、ゾーンおよびサブゾーン用の唯一の認証機関とすることができる。

【００２５】

動作中、第１のサブゾーンのエンドポイント３０２が、第２のサブゾーンのエンドポイント３０６とのＩＰｓｅｃセッションを要求する場合、エンドポイント（３０２、３０６）は、対応するデジタル証明書（３０４、３０８）を、ＩＰｓｅｃ接続を介して交換する。第１のサブゾーンのエンドポイント３０２は、第２のサブゾーンのエンドポイント３０６が第１のサブゾーンの証明書３０４に対してそうするように、１つまたは複数のセキュリティコンテキスト属性、および可能性としては他の属性に関して第２のサブゾーンの証明書３０８を分析する。さらに、第１および第２のサブゾーンのエンドポイント（３０２、３０６）のルート証明書を渡したり、検証することができる。両方のエンドポイントからの検証が成功した場合、エンドポイント（３０２、３０６）の間にＩＰｓｅｃセッションを確立することができる。

【００２６】
図４は、ＩＰｓｅｃ通信のためのデジタル証明書４０２中で利用することができる例示的な証明書属性４００を示す。上で示したように、属性４００は、ＱｏＳデータ、セキュリティコンテキストの一意のＩＤ、ＩＰｓｅｃセッションがそれに対して取得され得るエンドポイント（物理マシンまたは仮想マシン）のＩＰアドレス、ＩＰｓｅｃセッション（複数可）がそれに対して取得され得るエンドポイントからなる１つのグループ（または複数のグループ）のＩＰアドレス、（たとえば、会社に対する）顧客ＩＤ、ゾーンＩＤ、サークルＩＤ、プロキシシステムのＩＰアドレスなどを含み得る。開示するアーキテクチャは、あらゆるクラス（たとえば、識別、組織、サーバ、オンライン商取引、民間組織または政府組織などの証明を必要とする個人）のデジタル証明書にも該当する。
【００２７】
ＩＰｓｅｃの属性処理は、単一の属性（会社ＩＤ）のみを処理しても、複数の属性（たとえば、会社ＩＤおよびｚｏｎｅ１）を処理してもよい。さらに、たとえば、第１の属性が第３の属性より重みを与えられるように、重みづけシステムを利用することができる。代替的に、または組み合わせて、ゾーン属性が最優先として順位づけされ、顧客ＩＤがより低い優先度として続くなどのような、所定の基準に従って属性を順位づけしてもよい。
【００２８】
エンドポイントは、属性に従って異なるゾーンおよびエンドポイントへのアクセスをそれぞれが定義する複数の証明書を含み得ることに留意されたい。
【００２９】
本開示アーキテクチャの新規態様を実施する例示的な手順を表す１組のフローチャートが、本明細書に含まれる。説明を簡単にするために、たとえば、フローチャートまたはフロー図の形で本明細書に示す１つまたは複数の手順は、一連の作用として示し説明するが、手順は作用の順序によって限定されないことを理解されたい。というのは、ある作用は、手順によって異なる順序で起きてもよく、かつ／または本明細書において示し説明する他の作用と同時に起きてもよいからである。たとえば、手順は、状態図でのように、相関する一連の状態またはイベントとしても表され得ることが当業者には理解されよう。さらに、手順に例示するすべての作用が、新規実装形態に必要となり得るわけではない。
【００３０】
図５は、コンピュータ実施セキュリティ方法を示す。５００で、エンドポイントにおいて、１つまたは複数の証明書属性を有するデジタル証明書をピアエンドポイントから受信する。５０２で、ピアエンドポイントのセキュリティコンテキストを、エンドポイントにおいて、１つまたは複数の証明書属性に基づいて検証する。５０４で、ＩＰｓｅｃセッションを、セキュリティコンテキストの検証に基づいて、エンドポイントとピアエンドポイントとの間で確立する。
【００３１】
図６は、図５の方法の追加態様を示す。６００で、デジタル証明書を、複数ゾーンを管理する認証機関から、エンドポイントおよびピアエンドポイントに対して発行する。６０２で、証明書を、ある特定の属性に対してロックダウンする。６０４で、ある属性を、ある特定のエンドポイントのＩＰアドレスとして定義する。６０６で、ある属性を、あるグループのＩＰアドレスの範囲として定義する。６０８で、セキュリティコンテキストを、属性の１つまたは複数として定義する。６１０で、エンドポイントのデジタル証明書のある属性を、エンドポイントのセキュリティデータと比較し、ピアエンドポイントをエンドポイントと突き合わせて検証する。
【００３２】
図７は、あるＩＰアドレスへのＩＰｓｅｃ証明書を処理する方法を示す。７００で、ＩＰｓｅｃ通信を、ある特定のＩＰアドレスへのロックダウンを有するエンドポイントの間で開始する。７０２で、各エンドポイントは、他方のエンドポイントのＩＰアドレスを、提示された証明書中のＩＰアドレスのリストと比較する。７０４でＩＰアドレスがリストにある場合、フローは７０６に進み、エンドポイント間でＩＰｓｅｃセッションを確立す

る。あるいは、７０４でＩＰアドレスがリストにない場合、フローは７０８に進み、ＩＰｓｅｃセッションの開始に失敗する。

【００３３】

本出願において使われている限り、「コンポーネント」および「システム」などの用語は、コンピュータ関連のエンティティ、すなわちハードウェア、ハードウェアおよびソフトウェアの組合せ、ソフトウェア、または実行中のソフトウェアのいずれかを指すことを意図している。たとえば、コンポーネントは、プロセッサ上で稼動するプロセス、プロセッサ、ハードディスクドライブ、（光学、固体状態および／もしくは磁気記憶媒体の）複数の記憶ドライブ、オブジェクト、実行可能ファイル、実行スレッド、プログラム、ならびに／またはコンピュータとすることができるが、これらに限定されない。例として、サーバ上で稼動するアプリケーションおよびそのサーバ両方がコンポーネントとなり得る。１つまたは複数のコンポーネントが実行プロセスおよび／または実行スレッド中に常駐することができ、コンポーネントを、１台のコンピュータに配置し、および／または２台以上のコンピュータの間に分散することができる。「例示的」という言葉は、本明細書において、一例、事例、または例示となることを意味するために使われ得る。「例示的」として本明細書に記載するどの態様も設計も、必ずしも他の態様または設計よりも好まれ、または有利であることを解釈されるべきではない。

【００３４】

ここで図８を参照すると、本開示アーキテクチャによる、ＩＰｓｅｃ通信のための属性処理を実行するように動作可能なコンピューティングシステム８００のブロック図が示されている。様々な態様のための追加コンテキストを提供するために、図８および以下の説明は、様々な態様が実装され得る適切なコンピューティングシステム８００を簡潔に、概略的に説明することを意図している。上記説明は、１つまたは複数のコンピュータ上で稼働し得るコンピュータ実行可能命令の一般的コンテキストにおけるものであるが、新規実施形態も、他のプログラムモジュールと組み合わせて、および／またはハードウェアとソフトウェアの組合せとして実装され得ることが当業者には理解されよう。

【００３５】

様々な態様を実装するコンピューティングシステム８００は、処理ユニット（複数可）８０４と、システムメモリ８０６などのコンピュータ可読ストレージと、システムバス８０８とを有するコンピュータ８０２を含む。処理ユニット（複数可）８０４は、シングルプロセッサ、マルチプロセッサ、シングルコアユニットおよびマルチコアユニットなど、市販されている様々なプロセッサのいずれでもよい。さらに、新規方法は、１つまたは複数の関連デバイスにそれぞれが動作可能に結合され得る、ミニコンピュータ、メインフレームコンピュータ、ならびにパーソナルコンピュータ（たとえば、デスクトップ、ラップトップなど）、ハンドヘルドコンピューティングデバイス、マイクロプロセッサベースまたはプログラム可能家電製品などを含む他のコンピュータシステム構成で実施され得ることが当業者には理解されよう。

【００３６】

システムメモリ８０６は、揮発性（ＶＯＬ）メモリ８１０（たとえば、ＲＡＭ（ランダムアクセスメモリ））および不揮発性メモリ（ＮＯＮ－ＶＯＬ）８１２（たとえば、ＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭなど）などのコンピュータ可読ストレージを含み得る。ＢＩＯＳ（基本入出力システム）は、不揮発性メモリ８１２に格納することができ、起動中などに、コンピュータ８０２内部のコンポーネントの間でのデータおよび信号の通信を容易にする基本ルーチンを含む。揮発性メモリ８１０は、データをキャッシュするスタティックＲＡＭなどの高速ＲＡＭも含み得る。

【００３７】

システムバス８０８は、メモリサブシステム８０６を含むがそれに限定されないシステムコンポーネントと処理ユニット（複数可）８０４とのインターフェイスを提供する。システムバス８０８は、市販されている様々なバスアーキテクチャのいずれかを用いる、（メモリコントローラを用いてまたは用いずに）メモリバスにさらに相互接続し得るいくつ

かのタイプのバス構造、および周辺バス（たとえば、ＰＣＩ、ＰＣＩｅ、ＡＧＰ、ＬＰＣなど）のいずれでもよい。

【００３８】

コンピュータ８０２は、マシン可読な記憶サブシステム（複数可）８１４と、記憶サブシステム（複数可）８１４をシステムバス８０８および他の所望のコンピュータコンポーネントとインターフェイスをとらせる記憶インターフェイス（複数可）８１６とをさらに含む。記憶サブシステム（複数可）８１４は、たとえば、ＨＤＤ（ハードディスクドライブ）、磁気ＦＤＤ（フロッピー（登録商標）ディスクドライブ）、および／または光ディスク記憶ドライブ（たとえば、ＣＤ－ＲＯＭドライブ、ＤＶＤドライブ）の１つまたは複数を含み得る。記憶インターフェイス（複数可）８１６は、たとえば、ＥＩＤＥ、ＡＴＡ、ＳＡＴＡ、およびＩＥＥＥ１３９４などのインターフェイス技術を含み得る。

【００３９】

オペレーティングシステム８２０、１つまたは複数のアプリケーションプログラム８２２、他のプログラムモジュール８２４、およびプログラムデータ８２６を含む、１つまたは複数のプログラムおよびデータが、メモリサブシステム８０６、取外し可能メモリサブシステム８１８（たとえば、フラッシュドライブフォームファクター技術）、ならびに／または記憶サブシステム（複数可）８１４（たとえば、光学、磁気、固体状態）に格納され得る。

【００４０】

１つまたは複数のアプリケーションプログラム８２２、他のプログラムモジュール８２４、およびプログラムデータ８２６は、たとえば、図１のシステム１００のエンティティおよびコンポーネント、図２のシステム２００のエンティティおよびコンポーネント、図３のシステム３００のエンティティおよびコンポーネント、図４の証明書および属性、ならびに図５～７のフローチャートによって表される方法を含み得る。

【００４１】

概して、プログラムは、特定のタスクを実施し、または特定の抽象データタイプを実装するルーチン、方法、データ構造、他のソフトウェアコンポーネントなどを含む。オペレーティングシステム８２０、アプリケーション８２２、モジュール８２４、および／またはデータ８２６の全部または一部は、たとえば、揮発性メモリ８１０などのメモリにもキャッシュされ得る。本開示アーキテクチャは、市販されている様々なオペレーティングシステム、またはオペレーティングシステム（たとえば、仮想マシンとして）の組合せで実装され得ることを理解されたい。

【００４２】

記憶サブシステム（複数可）８１４およびメモリサブシステム（８０６、８１８）は、データ、データ構造、コンピュータ実行可能命令などの揮発性および不揮発性記憶のためのコンピュータ可読媒体として働く。コンピュータ可読媒体は、コンピュータ８０２によってアクセスされ得る利用可能などの媒体でもよく、取外し可能または固定型である揮発性および不揮発性の内部および／または外部媒体を含む。コンピュータ８０２にとって、媒体は、適切などのデジタル形式のデータの格納にも適合する。本開示アーキテクチャの新規方法を実施するコンピュータ実行可能命令を格納する、たとえばジップドライブ、磁気テープ、フラッシュメモリカード、フラッシュドライブ、カートリッジなど、他のタイプのコンピュータ可読媒体が利用され得ることが当業者には理解されよう。

【００４３】

ユーザは、キーボードおよびマウスなどの外部ユーザ入力デバイス８２８を使ってコンピュータ８０２、プログラム、およびデータと対話することができる。他の外部ユーザ入力デバイス８２８は、マイクロホン、ＩＲ（赤外線）リモコン、ジョイスティック、ゲームパッド、カメラ認識システム、スタイラスペン、タッチスクリーン、および／またはジェスチャーシステム（たとえば、目の動き、頭の動きなど）などを含み得る。ユーザは、たとえばタッチパッド、マイクロホン、キーボードなどの搭載ユーザ入力デバイス８３０を使ってコンピュータ８０２、プログラム、およびデータと対話することができ、ここで

コンピュータ８０２は、たとえば可搬型コンピュータである。こうしたおよび他の入力デバイスは、システムバス８０８を介して入出力（Ｉ／Ｏ）デバイスインターフェイス（複数可）８３２により処理ユニット（複数可）８０４に接続されるが、たとえばパラレルポート、ＩＥＥＥ１３９４シリアルポート、ゲームポート、ＵＳＢポート、ＩＲインターフェイスなど、他のインターフェイスによっても接続することができる。Ｉ／Ｏデバイスインターフェイス（複数可）８３２は、たとえばプリンタ、オーディオデバイス、カメラデバイス、ならびにそれ以外、たとえばサウンドカードおよび／またはオンボードオーディオ処理能力などの出力周辺装置８３４の使用も容易にする。

【００４４】

１つまたは複数のグラフィックスインターフェイス（複数可）８３６（一般にはグラフィックス処理ユニット（ＧＰＵ）とも呼ばれる）は、コンピュータ８０２、外部ディスプレイ（複数可）８３８（たとえば、ＬＣＤ、プラズマ）および／または搭載ディスプレイ８４０（たとえば、可搬型コンピュータ用）の間でグラフィックスおよびビデオ信号を提供する。グラフィックスインターフェイス（複数可）８３６は、コンピュータシステムボードの一部として製造することもできる。

【００４５】

コンピュータ８０２は、１つまたは複数のネットワークおよび／または他のコンピュータへのワイヤード／ワイヤレス通信サブシステム８４２による論理接続を使って、ネットワーク接続された環境（たとえば、ＩＰベース）内で動作し得る。他のコンピュータは、ワークステーション、サーバ、ルータ、パーソナルコンピュータ、マイクロプロセッサベースの娯楽機器、ピアデバイスまたは他の共通ネットワークノードを含み、コンピュータ８０２に関連して記載した要素の多くまたはすべてを通常は含み得る。論理接続は、ＬＡＮ（ローカルエリアネットワーク）、ＷＡＮ（ワイドエリアネットワーク）、ホットスポットなどとのワイヤード／ワイヤレス接続性を含み得る。ＬＡＮおよびＷＡＮネットワーク接続環境は、職場および企業においてよく見られ、イントラネットなど、企業規模のコンピュータネットワークを容易にし、これらはすべて、インターネットなどのグローバル通信ネットワークに接続し得る。

【００４６】

ネットワーク接続環境内で使われる場合、コンピュータ８０２は、ワイヤード／ワイヤレス通信サブシステム８４２（たとえば、ネットワークインターフェイスアダプタ、搭載トランシーバサブシステムなど）を介してネットワークに接続して、ワイヤード／ワイヤレスネットワーク、ワイヤード／ワイヤレスプリンタ、ワイヤード／ワイヤレス入力デバイス８４４などと通信する。コンピュータ８０２は、モデムまたはネットワーク経由の通信を確立する他の手段を含み得る。ネットワーク接続された環境では、コンピュータ８０２に対するプログラムおよびデータは、分散型システムに関連づけられたリモートメモリ／記憶デバイスに格納することができる。図示したネットワーク接続は例示であり、コンピュータの間で通信リンクを確立する他の手段も用いられ得ることが理解されよう。

【００４７】

コンピュータ８０２は、ＩＥＥＥ８０２．ｘｘ系の標準などの無線技術を用いて、たとえば、プリンタ、スキャナ、デスクトップおよび／または可搬型コンピュータ、ＰＤＡ（携帯情報端末）、通信衛星、ワイヤレスに検出可能なタグ、および電話に関連づけられたどの機器または場所（たとえば、キオスク、ニューススタンド、洗面所）ともワイヤレス通信（たとえば、ＩＥＥＥ８０２．１１無線経由の変調技法）するように動作可能に配置されたワイヤレスデバイスなどのワイヤード／ワイヤレスデバイスまたはエンティティと通信するように動作可能である。これは、少なくとも、ホットスポット用のＷｉ－Ｆｉ（すなわち、ワイヤレスフィデリティ）、ＷｉＭａｘ（登録商標）、およびＢｌｕｅｔｏｏｔｈ（登録商標）ワイヤレス技術を含む。したがって、通信は、従来のネットワークでのように、予め定義された構造でも、単に少なくとも２つのデバイスの間のアドホック通信でもよい。Ｗｉ－Ｆｉネットワークは、安全で安心な高速ワイヤレス接続性を提供するための、ＩＥＥＥ８０２．１１ｘ（ａ、ｂ、ｇなど）と呼ばれる無線技術を用いる。Ｗｉ－

Ｆｉネットワークは、コンピュータを互いと、インターネットと、およびワイヤーネットワーク（ＩＥＥＥ８０２．３に関係した媒体および機能を用いる）と接続するのに使うことができる。

【００４８】

例示した態様は、通信ネットワークを介してリンクされるリモート処理デバイスによって一定のタスクが実施される分散型コンピューティング環境において実施することもできる。分散型コンピューティング環境において、プログラムモジュールは、ローカルおよび／またはリモートシステムおよび／または記憶システム内に配置され得る。

【００４９】

ここで図９を参照すると、ＩＰｓｅｃ通信のための証明書属性を処理するコンピューティング環境９００の概略的なブロック図を例示してある。環境９００は、１つまたは複数のクライアント９０２を含む。クライアント（複数可）９０２は、ハードウェアおよび／またはソフトウェア（たとえば、スレッド、プロセス、コンピューティングデバイス）とすることができる。クライアント（複数可）９０２は、たとえば、クッキー（複数可）および／または関連づけられたコンテキスト情報を収容することができる。

【００５０】

環境９００は、１つまたは複数のサーバ９０４も含む。サーバ（複数可）９０４も、ハードウェアおよび／またはソフトウェア（たとえば、スレッド、プロセス、コンピューティングデバイス）とすることができる。サーバ９０４は、たとえば、アーキテクチャを利用することによって変換を実施するためのスレッドを収容することができる。クライアント９０２とサーバ９０４との間の可能な１つの通信物は、２つ以上のコンピュータプロセスの間で送信されるように適合されたデータパケットの形とすることができる。データパケットは、たとえば、クッキーおよび／または関連づけられたコンテキスト情報を含み得る。環境９００は、クライアント（複数可）９０２とサーバ（複数可）９０４との間の通信を容易にするのに利用され得る通信フレームワーク９０６（たとえば、インターネットなどのグローバル通信ネットワーク）を含む。

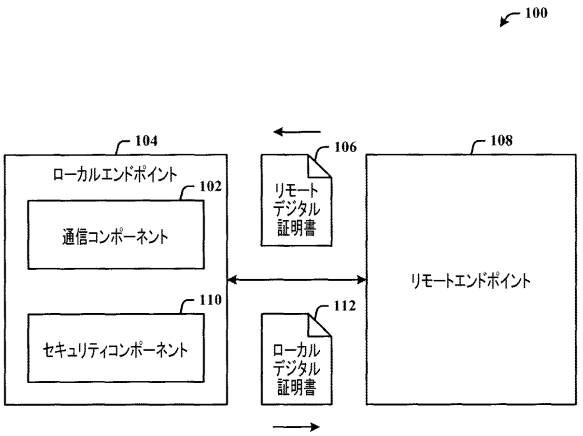
【００５１】

通信は、ワイヤー（光ファイバーを含む）および／またはワイヤレス技術により容易にされ得る。クライアント（複数可）９０２は、クライアント（複数可）９０２にとってローカルな情報（たとえば、クッキー（複数可）および／または関連づけられたコンテキスト情報）を格納するのに利用され得る１つまたは複数のクライアントデータストア９０８に動作可能に接続される。同様に、サーバ（複数可）９０４は、サーバ９０４にとってローカルな情報を格納するのに利用され得る１つまたは複数のサーバデータストア９１０に動作可能に接続される。

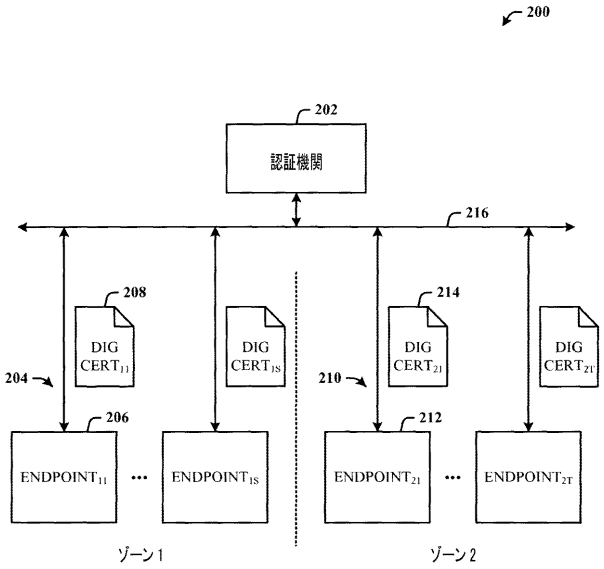
【００５２】

上記の説明内容は、開示したアーキテクチャのいくつかの例を含む。当然ながら、コンポーネントおよび／または手順の考えうるあらゆる組合せを説明することはできないが、さらに多くの組合せおよび置換が可能であることが、当業者には理解できよう。したがって、新規アーキテクチャは、添付の請求項の精神および範囲内であるこのようなすべての変更形態、修正形態、および変形形態を包含することを意図したものである。さらに、詳細な説明または請求項で「含む」という用語が使われている限りでは、請求項で移行語として解釈されるときに「備える」がそう解釈されるように、「備える」という用語と同様に包括的であることを意図している。

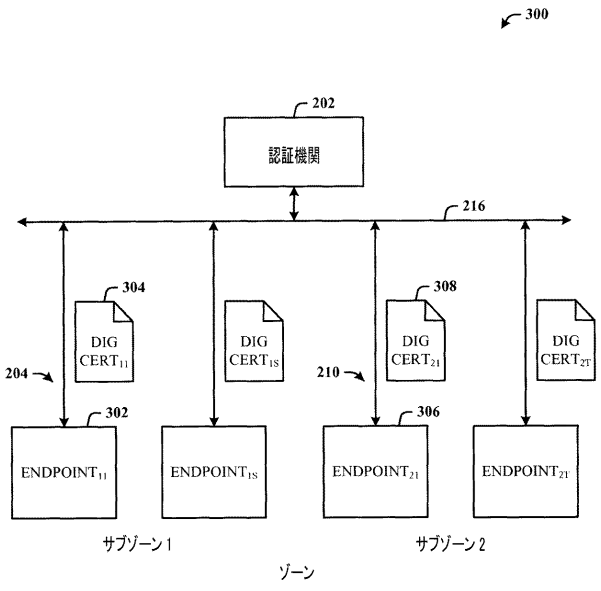
【図１】


100
104
ローカルエンドポイント
102
通信コンポーネント
110
セキュリティコンポーネント
106
リモート
デジタル
証明書
112
ローカル
デジタル
証明書
108
リモートエンドポイント

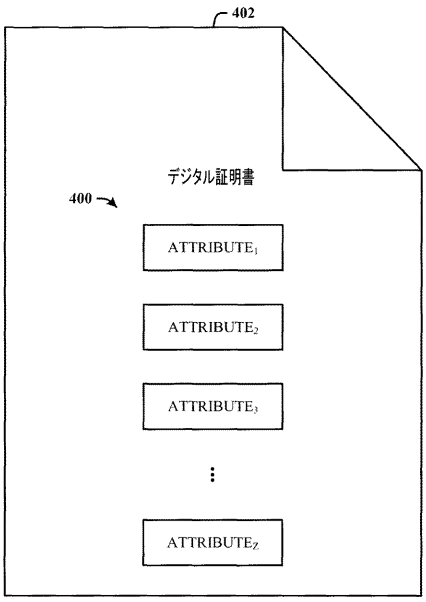
【図２】


200
202
認証機関
216
208
DIG
CERT11
DIG
CERT1S
214
DIG
CERT21
DIG
CERT2T
204
210
206
212
ENDPOINT11
ENDPOINT1S
ENDPOINT21
ENDPOINT2T
ゾーン1
ゾーン2

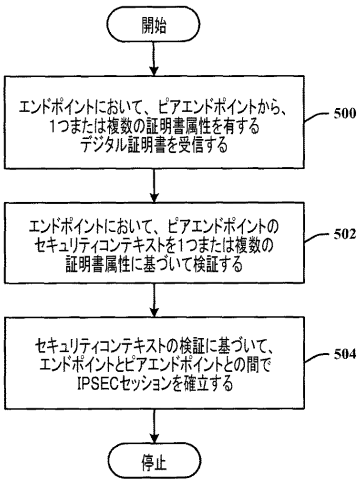
【図３】


300
202
認証機関
216
304
DIG
CERT11
DIG
CERT1S
308
DIG
CERT21
DIG
CERT2T
204
210
302
306
ENDPOINT11
ENDPOINT1S
ENDPOINT21
ENDPOINT2T
サブゾーン1
サブゾーン2
ゾーン

【図４】


402
デジタル証明書
400
ATTRIBUTE1
ATTRIBUTE2
ATTRIBUTE3
ATTRIBUTEZ

【図５】


開始
エンドポイントにおいて、ピアエンドポイントから、1つまたは複数の証明書属性を有するデジタル証明書を受信する
500
エンドポイントにおいて、ピアエンドポイントのセキュリティコンテキストを1つまたは複数の証明書属性に基づいて検証する
502
セキュリティコンテキストの検証に基づいて、エンドポイントとピアエンドポイントとの間でIPSECセッションを確立する
504
停止

【図６】

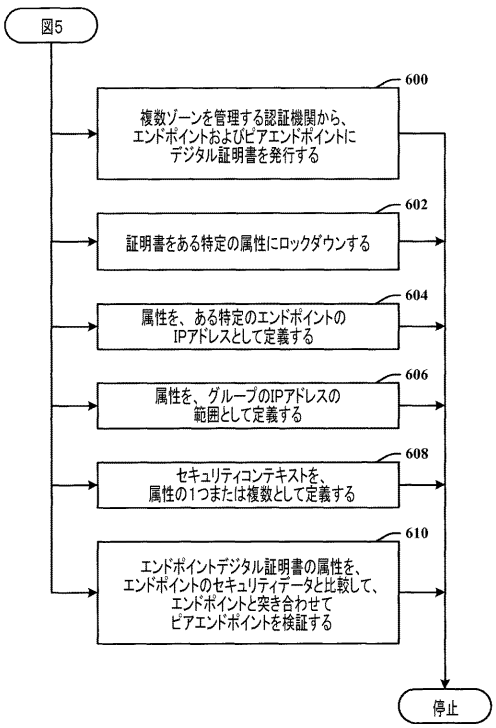
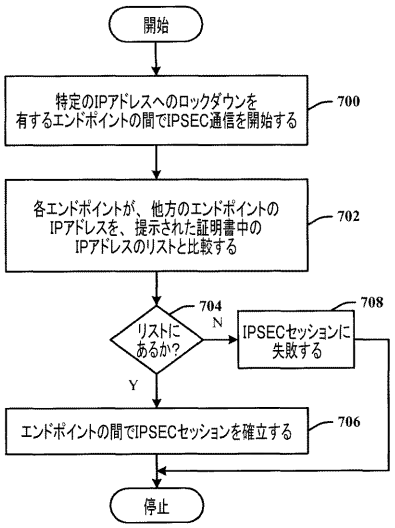
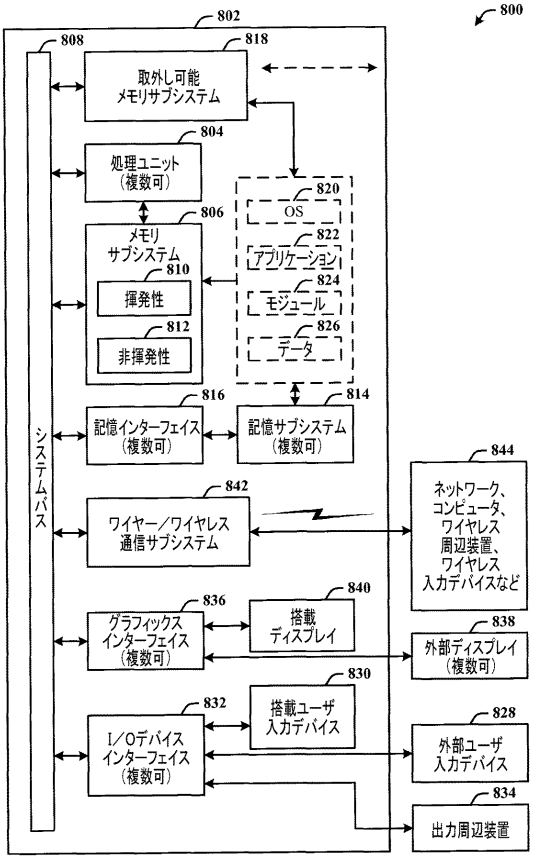


図5
600
複数ゾーンを管理する認証機関から、エンドポイントおよびピアエンドポイントにデジタル証明書を発行する
602
証明書をある特定の属性にロックダウンする
604
属性を、ある特定のエンドポイントのIPアドレスとして定義する
606
属性を、グループのIPアドレスの範囲として定義する
608
セキュリティコンテキストを、属性の1つまたは複数として定義する
610
エンドポイントデジタル証明書の属性を、エンドポイントのセキュリティデータと比較して、エンドポイントと突き合わせてピアエンドポイントを検証する
停止

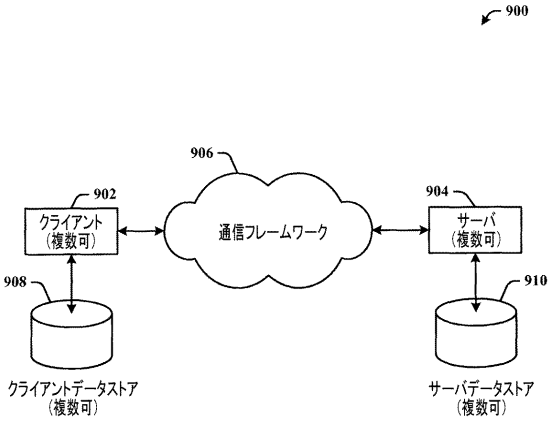
【図７】


開始
特定のIPアドレスへのロックダウンを有するエンドポイントの間でIPSEC通信を開始する
700
各エンドポイントが、他方のエンドポイントのIPアドレスを、提示された証明書中のIPアドレスのリストと比較する
702
リストにあるか?
704
N
IPSECセッションに失敗する
708
Y
エンドポイントの間でIPSECセッションを確立する
706
停止

【図８】


800
802
808
システムバス
818
取外し可能メモリサブシステム
804
処理ユニット（複数可）
806
メモリサブシステム
810
揮発性
812
非揮発性
820
OS
822
アプリケーション
824
モジュール
826
データ
816
記憶インターフェイス（複数可）
814
記憶サブシステム（複数可）
842
ワイヤー／ワイヤレス通信サブシステム
844
ネットワーク、コンピュータ、ワイヤレス周辺装置、ワイヤレス入力デバイスなど
836
グラフィックスインターフェイス（複数可）
840
搭載ディスプレイ
838
外部ディスプレイ（複数可）
830
搭載ユーザ入力デバイス
832
I／Oデバイスインターフェイス（複数可）
828
外部ユーザ入力デバイス
834
出力周辺装置

【図９】


900
906
902
クライアント
（複数可）
通信フレームワーク
904
サーバ
（複数可）
908
910
クライアントデータストア
（複数可）
サーバデータストア
（複数可）

フロントページの続き

(72)発明者 アナトリー パナシュク
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ内
(72)発明者 ダルシャン レンジゴウダ
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ内
(72)発明者 アビシェク シュクラ
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション エルシーエー－インターナショナル パテンツ内

審査官 青木 重徳

(56)参考文献 特開２００４－２７４５２１（ＪＰ，Ａ）
特開２００６－１３４３１２（ＪＰ，Ａ）
特開２００４－３６４３１５（ＪＰ，Ａ）
大山 実、千田 昇一、戸部 美春、窪田 光裕、田中 博巳、空 一弘，“Ｘ．５００ ディレクトリ入門 第２版”，日本，東京電機大学出版局 学校法人東京電機大学 丸山 孝一郎，２００１年 3月２０日，第２版第１刷，ｐ．１６１－１６６
C. Lynn, S. Kent, K. Seo, “X.509 Extensions for IP Addresses and AS Identifiers”, Request for Comments: 3779, [online], ２００４年 6月, [retrieved on 2014-10-10]. Retrieved from the Internet, ＵＲＬ, <http://tools.ietf.org/pdf/rfc3779.pdf>
辻元 孝博、唐澤 圭、藤崎 智宏、三上 博英，“ＩＰｖ６ ＩＰＳｅｃによるＥｎｄ－ｔｏ－Ｅｎｄ ＶＰＮ構築方式に関する考察”，電子情報通信学会技術研究報告，日本，社団法人電子情報通信学会，２００１年 7月１８日，Ｖｏｌ．１０１、Ｎｏ．２１４，ｐ．２０５－２１０
磯原 隆将、石田 千枝、北田 夕子、竹森 敬祐、笹瀬 巌，“検疫結果を保証するセキュリティ保証基盤”，情報処理学会論文誌，日本，社団法人情報処理学会，２００６年 2月１５日，第４７巻、第２号，ｐ．４３４－４４５

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／３３
Ｇ０９Ｃ １／００