(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2013-531834
(P2013-531834A)
(43)公表日　平成25年8月8日(2013.8.8)

(51)Int.Cl.	F I	テーマコード（参考）
G06F 21/33 (2013.01)	G06F 21/20 133	

審査請求 未請求　予備審査請求 未請求　（全 21 頁）

(21)出願番号	特願2013-510122 (P2013-510122)
(86)(22)出願日	平成23年4月27日 (2011.4.27)
(85)翻訳文提出日	平成25年1月11日 (2013.1.11)
(86)国際出願番号	PCT/US2011/034188
(87)国際公開番号	WO2011/142971
(87)国際公開日	平成23年11月17日 (2011.11.17)
(31)優先権主張番号	12/779,457
(32)優先日	平成22年5月13日 (2010.5.13)
(33)優先権主張国	米国 (US)

(71)出願人　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
(72)発明者　アナット　エヤル
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

最終頁に続く

(54)【発明の名称】ＩＰｓｅｃとＩＫＥバージョン１の認証を伴うワンタイム・パスワード

(57)【要約】
ネットワーク・アクセス制御がワンタイム・パスワードをサポートしないＩＫＥｖ１を使用していても、正しいワンタイム・パスワードを提供したクライアントにＩＰｓｅｃセッションを通じてネットワークへのアクセスを許可するように適合されたシステムである。認証サービスは、ワンタイム・パスワードを含むアクセス要求をクライアントから受け取り、ワンタイム・パスワードをチェックするサービスにワンタイム・パスワードを提供する。このワンタイム・パスワード・サービスは、パスワードの正当性検証が成功し、クライアントが正しく認証された場合にクッキーを返す。クッキーはクライアント・コンピュータに渡され、証明書要求の一部として使用される。証明機関は、認証されたクライアントから証明書要求を受け取った場合には証明書を生成し、証明書を用いてネットワークへアクセスするためのＩＰｓｅｃセッションを生成することができる。

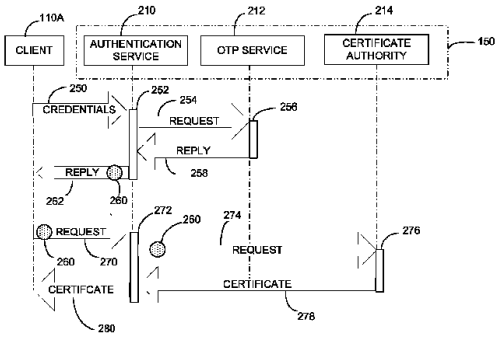


FIG. 2

【特許請求の範囲】
【請求項１】
ＩＰｓｅｃセッションを確立するようにコンピューティング装置を動作させる方法であって、
ワンタイム・パスワードを含む第１の通信を送信するステップと、
前記第１の通信に応答して、前記ワンタイム・パスワードの正当性検証に成功したことを示すインジケーションを含む応答を受け取るステップと、
前記インジケーションを含む第２の通信を送信するステップと、
前記第２の通信に応答して、前記ワンタイム・パスワードの正当性検証が成功したことを示すインジケーションを含む証明書を受け取るステップと、
前記証明書を用いて前記ＩＰｓｅｃセッションを確立するステップと
を含むことを特徴とする方法。
【請求項２】
前記ＩＰｓｅｃセッションを確立するステップが、企業ネットワークへのリモート・アクセス向けのＩＰｓｅｃセッションを確立するステップを含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記ワンタイム・パスワードの正当性検証が成功したことを示す前記インジケーションが、前記応答内のクッキーを含むことを特徴とする請求項１に記載の方法。
【請求項４】
前記第２の通信を送信するステップが、前記コンピューティング装置の秘密鍵で暗号化されたパラメータを送信すること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】
前記第２の通信において前記コンピューティング装置の秘密鍵を用いて値を生成するステップ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６】
前記第１の通信を送信するステップが、認証サービス宛ての前記第１の通信を送信するステップを含み、前記第２の通信を送信するステップが、前記認証サービス宛ての第２の通信を送信するステップを含むことを特徴とする請求項１に記載の方法。
【請求項７】
前記応答を受け取るステップが、ワンタイム・パスワード・サービスにより生成されたクッキーを含むメッセージを受け取るステップを含み、前記証明書を受け取るステップが、証明機関により生成された証明書を受け取るステップ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】
前記第１の通信を送信するステップが、認証ゲートウェイ宛ての前記第１の通信を送信するステップを含み、前記第２の通信を送信するステップが、前記認証ゲートウェイ宛ての第２の通信を送信するステップを含むことを特徴とする請求項１に記載の方法。
【請求項９】
ネットワークに接続された少なくとも１つのプロセッサであって、
認証サービスと、
ワンタイム・パスワード・サービスと、
証明機関と、
を実装する少なくとも１つのプロセッサを備え、
前記認証サービスが、前記ネットワーク上で第１の通信をクライアントから受信するように適合され、前記第１の通信が前記クライアントに関連付けられた認証情報とワンタイム・パスワードを含み、
前記認証サービスが、前記クライアントに関連付けられた前記認証情報の正当性を検証し、前記ワンタイム・パスワードを前記ワンタイム・パスワード・サービスに運搬し、
前記ワンタイム・パスワード・サービスが、前記ワンタイム・パスワードの正当性を検

証し、前記認証サービスに前記ワンタイム・パスワードの正当性検証の結果のインジケーションを返すように適合され、
前記認証機関が、前記ワンタイム・パスワードの正当性検証の結果の前記インジケーションを受け取るように適合され、前記ワンタイム・パスワードの正当性検証が成功したことを前記結果が示す場合に選択的に証明書を発行するように適合されたことを特徴とするシステム。
【請求項１０】
前記認証サービス、前記ワンタイム・パスワード・サービス、および前記証明機関が認証ゲートウェイを備えることを特徴とする請求項９に記載のシステム。
【請求項１１】
前記クライアントに関連付けられた前記認証情報が、前記クライアントのユーザの認証情報を備え、前記認証サービスが、前記ユーザの前記認証情報を認証するように適合されたことを特徴とする請求項９に記載のシステム。
【請求項１２】
前記システムがさらに、アクセス制御ゲートウェイを含む企業ネットワークを備え、前記アクセス制御ゲートウェイが、前記企業ネットワークへのアクセスを、前記証明機関が発行した証明書を有するクライアント・コンピュータに許可するＩＰｓｅｃセッションを選択的に生成するよう適合されたことを特徴とする請求項９に記載のシステム。
【請求項１３】
前記企業ネットワークが、ワンタイム・パスワード認証に基づいてリモート・アクセス制御をサポートしないことを特徴とする請求項１２に記載のシステム。
【請求項１４】
前記企業ネットワークがＩＫＥｖｌアクセス制御を使用することを特徴とする請求項１３に記載のシステム。
【請求項１５】
前記証明機関が、前記クライアントの認証に基づいて公開鍵暗号化を実施するよう適合され、前記証明機関が、前記クライアントが前記公開鍵暗号化ベースの認証を用いて認証に成功し、かつ、前記ワンタイム・パスワードの正当性検証が成功したことを前記結果が示す場合に、選択的に前記証明書を発行することを特徴とする請求項９に記載のシステム。
【発明の詳細な説明】
【背景技術】
【０００１】
大部分のプライベート・ネットワークでは、クライアント・コンピュータがネットワーク上のリソースにアクセスできる前に何らかの形の認証が必要である。クライアント・コンピュータを、当該コンピュータ、または当該コンピュータのユーザが認証情報を提供したときに認証することができる。当該認証情報は、１つまたは複数の「ファクタ」に基づくことがある。ファクタは、スマート・カードのようなユーザが所有するもの、またはパスワードのようなユーザが知っているもの、または指紋もしくは眼瞼読取（ｅｙｅｌｉｄ　ｒｅａｄｉｎｇ）のようなユーザの何らかの属性であるかもしれない。認証に必要なこれらのファクタの数および性質は、不適切にアクセスが許可されるリスク、または、クライアント・コンピュータがネットワークにアクセスすることが認められない可能性に依存するかもしれない。
【０００２】
認証情報はこれらのファクタのうち１つまたは複数に直接基づくこともある。他の事例では、認証情報がこれらのファクタのうち１つまたは複数から間接的に導出されることもある。クライアント・コンピュータは、これらのファクタのうち１つまたは複数を、ネットワーク管理者が信頼するソースに提供することができる。次いで当該ソースが証明書を発行し、装置を正当なクライアントとして確認することができる。当該証明書により、単体でまたは他のファクタとともに、クライアント・コンピュータを認証することができる

。当該情報がどのように取得されるかに関わらず、当該情報をクライアント・コンピュータとアクセス制御機構の間の交換の一部として使用して、クライアントを認証できる場合にアクセス制御機構がアクセスを許可するだけであるようにすることができる。

【０００３】

様々な機構を使用して、クライアントへのアクセスを許可するかまたは拒否するかの決定を行うことができる。一般的に、認証プロセスに続いて、認証情報を追加のパラメータとともに用いて権限付与プロセスを実施し、特定のクライアントのアクセス権限を決定する。クライアントのアクセス権限に基づいてアクセスが制限される具体的な機構は、ネットワークのトランスポート層の実装に依存しうる。一般に、クライアントが認証されると、トランスポート層は、当該クライアントのアクセス権限と一致するメッセージを、当該クライアントに対して送受信する。認証されない装置に対しては、ネットワークに物理的に接続されていても、当該トランスポート層は当該装置とメッセージをやり取りしない。

【０００４】

アクセス判定を行うための１つの機構は、ＩＰｓｅｃと呼ばれるプロトコルの使用を含む。クライアントが認証されなければ、ネットワーク・トランスポート層は、クライアントがネットワーク通信を送受信するためのＩＰｓｅｃセッションを生成しない。

【０００５】

認証の１つのタイプにワンタイム・パスワードがあり、高い安全性をもたらすと考えられている。新たなパスワードを一定間隔で生成するかまたは予め準備されたパスワードのリストを生成するクロックに結び付けられた電子装置のような、ワンタイム・パスワードを生成できる複数の技術がある。パスワードを生成する形態に関わらず、パスワードを使用して限られた期間だけネットワークへアクセスすることができるので、パスワードにより安全性が高められる。当該限られた期間は、相対的に短い時間間隔によりまたはパスワードを使用することにより、定義することができる。したがって、悪意のある第三者がパスワードへのアクセスを取得した場合であっても、当該第三者は当該パスワードを使用してネットワークにアクセスできる可能性は低い。

【０００６】

残念ながら、ＩＰｓｅｃはアクセス制御向けに広く使用されているが、多くの実装形態ではワンタイム・パスワードをサポートしない。ＩＰｓｅｃセッションを生成するには、ＩＫＥ（Ｉｎｔｅｒｎｅｔ　Ｋｅｙ　Ｅｘｃｈａｎｇｅ）プロトコルを使用する必要がある。広く使用されているＩＫＥのバージョン１（ＩＫＥｖ１）ではワンタイム・パスワードがサポートされていない。ＩＫＥのバージョン２（ＩＫＥｖ２）ではワンタイム・パスワードがサポートされているが、ＩＫＥｖ２は、特に企業ネットワーク向けのリモート・アクセス制御に対して、広くは使用されていない。

【発明の概要】

【０００７】

発明者らは、ネットワークへのアクセスを正当なワンタイム・パスワードを提示するクライアントにのみ制限するようにネットワーク・アクセス制御システムを適合させることで、ネットワーク・セキュリティを改善できることを認識し理解した。当該ネットワーク・アクセス制御システムは、本質的にワンタイム・パスワードをサポートするものである。当該アクセス・システムは、ワンタイム・パスワードを含む認証要求をクライアントから受け取ると、当該パスワードをワンタイム・パスワード・サービスに提供する認証サービスを備える。当該ワンタイム・パスワード・サービスはパスワードの正当性をチェックし、正当性が検証されると、当該ワンタイム・パスワードの正当性が検証されたというインジケータを返す。当該インジケータはクライアントに返すことができ、当該クライアントは次いで当該インジケーションを証明書要求と関連して送信することができる。証明機関は、当該インジケータを受け取ると正当な証明書を発行する。クライアントは次いで当該証明書を使用して接続を生成する。

【０００８】

ワンタイム・パスワードの正当性が検証されたというインジケータをクライアントが送

信したことに基づいて証明機関が選択的に証明書を発行するので、正当なワンタイム・パスワードを有するクライアントにアクセスが制限される。このように、正当な証明書を利用するアクセス制御機構は、ワンタイム・パスワード認証をサポートするプロトコルをアクセス制御機構自体が使用しない場合であっても、正当なワンタイム・パスワードを有するクライアントにアクセスを許可し、正当なワンタイム・パスワードを有さないクライアントへのアクセスを拒否する。具体的な例として、アクセス制御機構が、ＩＫＥｖ１を用いて生成されたＩＰｓｅｃセキュリティ・アソシエーションを使用してアクセス制御の判定を行うことができる。

【０００９】

以上は、本発明の非限定的な要約であり、添付の特許請求の範囲により定義される。

【図面の簡単な説明】

【００１０】

添付図面は正しい縮尺で描くことを意図したものではない。図面においては、様々な図において示されている夫々の同一またはほぼ同一の構成要素は同じ番号で表される。明確にするため、各図面において全ての構成要素にはラベルが付されていないこともある。

【図１】本発明の幾つかの実施形態に従ってクライアント装置を認証できる例示的なネットワーク環境の略図である。

【図２】本発明の幾つかの実施形態に従って、ワンタイム・パスワードに基づいて証明書を取得するプロセスの概略図である。

【図３】図２のプロセスで発行される証明書に基づいてネットワーク・アクセスを取得するプロセスの概略図である。

【発明を実施するための形態】

【００１１】

ワンタイム・パスワードをサポートしないアクセス制御を使用するネットワークを、かかるパスワードを使用するように適合させることができる。１つまたは複数のサービスを提供することにより当該適合を実装することができる。当該１つまたは複数のサービスは、ワンタイム・パスワードの正当性を検証でき、クライアントに対するワンタイム・パスワードが認証されたというインジケーションを発行することができる。証明機関は、ネットワーク・アクセスを取得するために用いられる証明書を付与するために、かかる証明書を要求するクライアントが、そのワンタイム・パスワードの正当性が検証されたというインジケーションを受け取ったことを条件としてもよい。

【００１２】

幾つかの実施形態では、本技法を企業ネットワークで使用して、クライアントが正当なワンタイム・パスワードを有しているかどうかに基づいてクライアントのアクセスを許可または拒否することができる。このように、ワンタイム・パスワード認証をサポートしないリモート・アクセス制御システムを有する企業ネットワークを、ワンタイム・パスワードに基づくアクセス制御ポリシを実装するように適合させてもよい。幾つかの実施形態では、本技法を旧式のネットワーク・アクセス制御システムと併用してもよい。１例として、ＩＫＥｖ１を用いてＩＰｓｅｃセキュリティ・アソシエーションを介してアクセス制御を行うシステムを、ネットワーク・アクセスに対する正当なワンタイム・パスワードを要求するように適合させてもよい。

【００１３】

本明細書で説明した技法を任意の適切なネットワーク環境で使用することができる。本発明の諸実施形態を実施できるネットワーク環境の例示的な実施形態を図１に示す。

【００１４】

図１は、コンピュータ・システム１００の略図を示す。コンピュータ・システム１００を、従来型のコンピュータ・システムで使用される装置から構成してもよい。しかし、コンピュータ・システム１００は、コンピュータ・システム１００内部の装置が、ネットワークへのアクセスを許可するためのワンタイム・パスワードを要求するようにプログラムされているという点で従来型のコンピュータ・システムとは異なる。

【００１５】
コンピュータ・システム１００はプライベート・ネットワークを含み、ここでは、サーバ１２４のようなネットワークに接続された複数のリソースを有するマネージド・ネットワーク１２０として示してある。クライアント装置をネットワークに接続して、ネットワーク・リソースにアクセスすることができる。しかし、ネットワークへのアクセスが、許可されたクライアント装置にのみ制限されているので、当該ネットワークはプライベートである。
【００１６】
本例では、マネージド・ネットワーク１２０が、会社または企業の内部のネットワークであってもよい。あるいは、マネージド・ネットワーク１２０が大規模ネットワークのドメインまたは他の部分であってもよい。マネージド・ネットワーク１２０を、ネットワークに関するアクセス基準を提供する個人またはエンティティによって管理してもよい。本明細書に記載の例示的なシステムでは、当該アクセス基準には、ワンタイム・パスワードと、許可されたクライアント装置を特定できる他の情報が含まれる。
【００１７】
許可されたクライアント装置を特定できる情報に関して、任意の適切な情報を使用してもよい。幾つかの実施形態では、装置のユーザがネットワークにアクセスする権限を有しており当該権限の証明の役割を果たすクライアント情報を入力したことを理由として、当該装置を認証してもよい。これらの実施形態では、認証情報が、装置のユーザに関連してもよく、ユーザ名または他のコードであってもよい。他の実施形態では、当該認証情報が、コンピュータ上の複数のユーザ・セッションに関連付けられた複数のユーザのうち１名のみに関連してもよい。例えば、コンピュータが複数のユーザ・セッションをサポートする場合、ユーザ・セッションの一部のみにネットワークへのアクセスを許可してもよい。これらの実施形態では、認証情報が１つまたは複数の特定のユーザ・セッションに関連してもよい。したがって、本発明は、認証されるエンティティの種類によっては限定されない。
【００１８】
図１に示すように、マネージド・ネットワーク１２０は、サーバ１２４ならびにクライアント１１０Ｂおよび１１０Ｃのようなネットワーク装置を備える。ここで、ＷＡＮ（ｗｉｄｅ　ａｒｅａ　ｎｅｔｗｏｒｋ）１２２がネットワーク装置を相互接続すると示されている。本構成は説明を簡単にするために示されているが、アクセスが制御されるネットワークが複数の相互接続ネットワークを含んでもよく、または、異種もしくは追加の相互接続アーキテクチャを含んでもよい。同様に簡単にするため、少数のネットワーク装置が示されているが、マネージド・ネットワークが多数の装置を含んでもよい。
【００１９】
装置を、アクセス制御を提供するゲートウェイを介してマネージド・ネットワーク１２０に接続させてもよい。簡単にするため、単一のアクセス制御ゲートウェイ１１６が示されている。アクセス制御ゲートウェイ１１６は、既知であるか将来開発されるかに関わらず、無線アクセス・ポイント、ハードワイヤードのアクセス・ポイントまたは他の任意の種類のアクセス・ポイントの一部であってもよい。しかし、示した例では、アクセス制御ゲートウェイ１１６はインターネットのようなパブリック・ネットワーク１３０に接続される。パブリック・ネットワークへのかかる接続により、遠隔地にあるクライアント装置が、アクセス制御ゲートウェイ１１６が実施するアクセス制御ポリシに従うことができるならば、マネージド・ネットワーク１２０にアクセスすることができる。
【００２０】
図１の例では、アクセス制御ゲートウェイ１１６は切替装置１１８とアクセス制御サーバ１１２を備える。アクセス制御サーバ１１２を、ユーザ・インタフェース１１３を介して、または、他の任意の適切な方法で構成してもよい。切替装置１１８は、ネットワーク内に含め得る数種の切替装置のうち何れかを表す。ここで、切替装置１１８はネットワークのトランスポート層のコンポーネントを示す。切替装置１１８は、ルータ、スイッチ、

ハブ、ゲートウェイ、または他の任意の適切な切替装置であってもよい。商用の実装においては、必要に応じてネットワークを介してパケットをルーティングすることに関与する複数の切替装置が存在してもよいが、簡単にするため、かかる装置のうち１つのみを示す。

【００２１】

図１の例は、クライアント１１０Ｂと１１０Ｃに対して既にマネージド・ネットワーク１２０へのアクセスが与えられていることを示している。見方を変えると、図１は、クライアント１１０Ａがアクセス制御ゲートウェイ１１６を介してマネージド・ネットワーク１２０に接続することを求めることを示し、したがってクライアント１１０Ａはマネージド・ネットワーク１２０の外部に示されている。動作においては、クライアント１１０Ａのようなクライアントがマネージド・ネットワーク１２０へのアクセスを求めると、アクセス制御装置は、クライアント１１０Ａにマネージド・ネットワーク１２０へのアクセスを与えるべきかどうか判定する。示した実施形態では、当該アクセス制御装置がアクセス制御サーバ１１２内で実行されている。しかし、当然ことながら、アクセスされているネットワーク装置がアクセス制御装置の役割を果たす実施形態を含めて、他の諸実施形態が可能である。アクセス判定がアクセス制御サーバ１１２で行われる実施形態では、クライアントが適切なワンタイム・パスワードを提供するかどうかに少なくとも部分的に基づいてネットワーク・アクセスを許可するか拒否するかを判定するように、アクセス制御サーバ１１２をプログラムしてもよい。

【００２２】

さらに、他のファクタに基づいてアクセスに条件を与えるようにアクセス制御サーバ１１２を構成してもよい。例えば、アクセス制御ゲートウェイ１１２は、クライアントを認証し、ネットワークの「健全な」ポリシに従うハードウェア構成またはソフトウェア構成をクライアントが報告したことを検証してもよい。認証されたクライアントの諸態様の数および種類に関わらず、アクセス制御サーバ１１２は、全ての要求された態様の正当性が検証されない場合には、クライアントにネットワーク・アクセスを許可すべきとは示さない。

【００２３】

アクセス制御サーバ１１２は、ネットワーク・アクセスの判定結果を実施機構（enforcement mechanism）に伝達する。当該実施機構をネットワーク１２０のトランスポート層内部に含めてもよく、これは切り替え装置１１８により表されているが、当該実施機構が多数の異種または追加の装置を含んでもよい。示した諸実施形態では、クライアントにネットワーク・アクセスを許可すべきという判定を、クライアント１１０Ａのようなマネージド・ネットワーク１２０へのアクセスを求めるリモート・クライアントにセキュリティ・アソシエーションを生成するように要求することによって行ってもよい。

【００２４】

セキュリティ・アソシエーションは、当業界で公知であり、セキュリティ・アソシエーションで結び付けられた或るネットワーク装置により使用して、ネットワーク通信が当該セキュリティ・アソシエーションの一部である別の装置から生じたと判定してもよい。セキュリティ・アソシエーションを使用して、当該セキュリティ・アソシエーションの一部である別の装置からの通信が、それらが送信された後に変更されていないことをネットワーク装置が保証することを可能にしてもよい。さらに、セキュリティ・アソシエーションを使用して、セキュリティ・アソシエーションを介して接続された装置の間の通信を暗号化してもよい。このようなセキュリティ・アソシエーションを使用することは、場合によっては信頼性、完全性、および機密性と呼ばれる。

【００２５】

本明細書で説明した諸実施形態では、アクセス制御ゲートウェイがセキュリティ・アソシエーションを使用して信頼性、完全性、および機密性を提供してもよい。ゲートウェイを通過する、許可された装置へのメッセージをゲートウェイにより暗号化して、当該メッセージが変更されていない場合には当該メッセージをセキュリティ・アソシエーションの

一部である権限のあるクライアントのみによって復号化できるようにしてもよい。同様に、ゲートウェイで受信したメッセージを、当該メッセージを復号化し認証できる場合にのみ、マネージド・ネットワーク１２０へ転送してもよい。しかし、他の実施形態では、信頼性を保証するためにのみセキュリティ・アソシエーションを使用してもよく、ゲートウェイはメッセージを、当該メッセージが認証された場合に渡してもよい。

【００２６】

セキュリティ・アソシエーションがゲートウェイで使用される具体的な方法に関わらず、装置とゲートウェイが秘密情報を共有することとなるプロトコルでメッセージを交換することにより、セキュリティ・アソシエーションを生成してもよい。続いて当該秘密情報を、情報を他方に送信するときに、クライアントまたはゲートウェイにより適用して、公知の暗号機能を用いて当該情報を署名または暗号化してもよい。受信者も、セキュリティ・アソシエーションの一部である秘密情報へアクセスして、当該情報を復号化し、および／または、当該情報が当該セキュリティ・アソシエーションを共有する別の装置により署名されたことの正当性を検証することができる。

【００２７】

図１の例では、アクセス制御サーバ１１２は、ネットワーク１３０上でネットワーク・アクセスを求めるクライアント１１０Ａと対話してもよい。この対話の結果、アクセス制御サーバ１１２とリモート・クライアント１１０Ａはセキュリティ・アソシエーションを生成することができる。クライアント１１０Ａからの通信がマネージド・ネットワーク１２０では直接には許可されないように、切替装置１１８を構成してもよい。寧ろ、これらの通信を最初にアクセス制御サーバ１１２で処理してもよい。アクセス制御サーバ１１２が、確立されたセキュリティ・アソシエーションを用いて通信が送信されたと判定する場合は、これらの通信をマネージド・ネットワーク１２０に送ってもよい。通信が暗号化されている場合は、アクセス制御サーバ１１２がセキュリティ・アソシエーションを使用して通信を復号化し、ネットワーク・サーバ１２４のような他のネットワーク装置がクライアント装置１１０Ａからの通信にアクセスできるようにしてもよい。

【００２８】

逆に、ネットワーク１２０上の装置から送信された通信に対して、アクセス制御サーバ１１２によって生成された、認証されたクライアントとのセキュリティ・アソシエーションに従ってかかる通信がエンコードされている場合に、切替装置１１８はかかる通信をネットワーク１３０に渡すことができるにすぎない。ネットワーク通信がセキュリティ・アソシエーションに従って暗号化されているので、他の装置は、パブリック・ネットワーク１３０上の通信にアクセスできたとしても、その内容を引き出すことはできない。このように、リモート・クライアントがアクセス制御サーバ１１２との正当なセキュリティ・アソシエーションを生成できる場合にのみ、当該リモート・クライアントはマネージド・ネットワーク１２０上の装置に対してメッセージを送受信することができる。

【００２９】

したがって、セキュリティ・アソシエーションは、権限のあるクライアントのみが当該セキュリティ・アソシエーションを生成できるように生成される。セキュリティ・アソシエーションを生成する前に、アクセス制御サーバ１１２は、クライアント１１０Ａのようなクライアントに関する認証情報を受信してもよい。認証情報を任意の適切な方法で取得してもよい。当該認証情報が、クライアント装置１１０Ａのユーザ・インタフェースを介してクライアント装置１１０Ａに入力された情報に全体としてまたは部分的に基づいてもよい。代替または追加として、当該認証情報が、クライアントと外部装置との間の対話に全体としてまたは部分的に基づいてもよい。これらのシナリオでは、認証情報が、外部装置により実施された認証が成功したことの証拠であってもよい。かかる証拠は証明書の形であってもよく、アクセス制御サーバ１１２が当該証明書を使用してアクセスを許可するかどうかを判定してもよい。外部装置による認証の証明を実証するための証明書は当業界で公知であり、アクセス制御サーバ１１２は、証明書を公知の形式で受け入れてもよいが、外部装置による認証を実証する、任意の適切な形式での情報を使用してもよい。

【００３０】
図１に示す実施形態では、認証サーバ１５０は外部装置の１例である。認証サーバ１５０は、任意の適切な方法で装置を認証することができる。示したように、認証サーバ１５０は、装置が許可されるかどうかを特定するために使用できる、許可された装置に関する情報のデータ記憶１５２を維持することができる。例えば、データ記憶１５２が、許可された装置と、装置が正当なパスワードを提供したかどうかを判定するために認証サーバが使用できる情報のようなセキュリティ情報とから成るリストを含んでもよい。しかし、他の任意の適切なアプローチを使用してもよく、データ記憶１５２が異種または追加の種類の情報を含んでもよい。当該情報には、許可された装置に対する予め記憶された鍵または許可された装置の確認を行う際に使用される他のセキュリティ情報が含まれる。

【００３１】
示した実施形態では、クライアント１１０Ａが、インターネットのようなパブリック・ネットワーク１３０上の認証サーバ１５０にアクセスするとして示されている。本実施形態では、クライアント１１０Ａと認証サーバ１５０の間の通信を、公開鍵／秘密鍵暗号化を用いて暗号化または保護してもよい。しかし、クライアント１１０Ａと認証サーバ１５０の間の通信に対して任意の適切な機構を使用してもよい。

【００３２】
また、示した実施形態では、認証サーバ１５０はネットワーク１２０の外部に示されている。認証サーバ１５０をネットワーク１２０上に設けることを含めて、他の実施形態も可能である。かかる実施形態では、切替装置１１８が、認証サーバへの制限された接続を認証されていない装置に提供してもよい。

【００３３】
認証サーバ１５０の位置に関わらず、認証サーバ１５０とアクセス制御サーバ１１２の間の通信のための機構を提供してもよい。示した実施形態では、当該機構が証明書を介したものであってもよい。認証サーバ１５０は、クライアント１１０Ａの認証が成功した場合に証明書をクライアント１１０Ａに発行してもよい。アクセス制御サーバ１１２が正当性を検証できる、認証サーバ１５０が保持するセキュリティ情報を用いて、当該証明書を署名してもよい。１例として、証明書を、公開鍵／秘密鍵の対の秘密鍵で署名または暗号化してもよい。アクセス制御サーバ１１２が当該鍵の対の公開鍵を有する場合、アクセス制御サーバ１１２は、証明書が認証サーバ１５０により発行されたことの正当性を検証してもよい。証明書は、クライアント１１０Ａを特定する情報を含んでもよい。当該情報は、当該情報の完全性を保証するために認証サーバ１５０により署名され、それにより、アクセス制御サーバ１１２は、当該証明書がクライアント１１０Ａに発行されたと判定することができる。したがって、アクセス制御サーバ１１２は当該証明書を利用して、クライアント１１０Ａとのセキュリティ・アソシエーションを生成するためにクライアント１１０Ａが認証されることを判定してもよい。

【００３４】
図１のコンピュータ・システムのコンポーネントを、当業界で公知な種類のネットワーク・コンポーネントを用いて実装してもよい。しかし、認証サーバ１５０を、正当なワンタイム・パスワードを提示する証明書を装置に発行するにすぎないように適合させてもよい。このように、アクセス制御ゲートウェイ１１６がワンタイム・パスワードを認識しなくても、それでも、マネージド・ネットワーク１２０へのアクセスは正当なワンタイム・パスワードを有するクライアントに限定される。したがって、システム１００と同様のアクセス制御技法を、ワンタイム・パスワードを要求する機能抜きでアクセス制御ゲートウェイが実装されている既存のネットワークとともに使用してもよい。

【００３５】
本発明者は、かかるネットワークが多数存在することを認識し理解している。具体的には、多数のネットワークでは、ネットワークへのアクセスを求めるクライアントが、アクセス制御コンポーネントとのセキュリティ・アソシエーションを、ＩＰｓｅｃプロトコルをＩＫＥｖ１（ｉｎｔｅｒｎｅｔ　ｋｅｙ　ｅｘｃｈａｎｇｅ　ｐｒｏｔｏｃｏｌ、ｖｅ

ｒｓｉｏｎ　１）とともに用いて生成することを要求することによって、アクセス判定が実施される。ＩＰｓｅｃをＩＫＥｖ１とともに使用するアクセス制御ゲートウェイは企業ネットワークで普及している。したがって、かかるネットワークにおいて、認証サーバ１５０を追加するかまたは既存の認証サーバを修正することで、ワンタイム・パスワードを要求するアクセス制御ポリシを実装するように当該ネットワークを適合させてもよい。

【００３６】

図２を参照すると、クライアント１１０Ａのようなネットワークへのアクセスを求めるクライアントが証明書を取得できるプロセスが示されている。図２に示すように、クライアント１１０Ａが認証サーバ１５０と通信してもよい。クライアント１１０Ａと認証サーバ１５０の間の通信を任意の適切な方法で伝送してもよい。図１の例では、これらの通信を、インターネットのようなパブリック・ネットワーク１３０上で伝送する。しかし、インターネットを使用することは本発明を限定するものではない。

【００３７】

示した実施形態では、認証サーバ１５０は複数のサービスを提供する。これらのサービスには、認証サービス２１０、ワンタイム・パスワード・サービス２１２、および証明機関２１４が含まれる。かかるサービスを、当業界で公知であるプログラミング技法を用いて実装して、ネットワーク上で他の装置と対話し特定の機能をサービスとして提供するように適合させてもよい。かかる通信向けのプロトコルは公知であり、クライアント１１０Ａと認証サービス２１０、ワンタイム・パスワード・サービス２１２、および証明機関２１４の間の通信に使用してもよい。しかし、任意の適切な技法を用いて、任意の適切な形式のサービスを実装してもよい。

【００３８】

通信の具体的な形式に関わらず、クライアント１１０Ａが証明書を認証サーバ１５０から取得するプロセスを、クライアント１１０Ａが通信２５０を認証サービス２１０に送信することから始めることができる。通信２５０を、例えば、パブリック・ネットワーク１３０上で運搬される１つまたは複数のパケットとして送信してもよい。通信２５０の具体的な形式に関わらず、通信２５０はクライアント１１０Ａの認証情報をクライアント１１０Ａから認証サービス２１０へ運搬することができる。通信２５０内に含まれる認証情報は、当業界で公知な種類の任意数の認証情報を含むことができる。これらの認証情報は、例えば、クライアント装置１１０Ａのユーザに関する情報またはクライアント装置自体に関する情報を含んでもよい。ユーザ情報は、例えば、ユーザ名およびパスワード、または、当該ユーザ名とパスワードの入力に基づいて生成した何らかの情報を含んでもよい。

【００３９】

当業界で公知な認証情報に加えて、通信２５０はワンタイム・パスワードを含んでもよい。通信２５０内部のワンタイム・パスワードを、クライアント１１０Ａに取り付けたハードウェア・コンポーネントにより生成してもよい。しかし、かかるワンタイム・パスワードを、ユーザが入力するか、または、別の方法でクライアント１１０Ａに利用可能としてもよい。

【００４０】

図２では通信２５０を１つの矢印で示したが、当然のことながら、通信２５０はクライアント１１０から認証サーバ１５０への複数の送信を含んでもよい。さらに、これらの送信のうち１つまたは複数を、認証サービス２１０からの通信に応答して送信してもよい。具体的な例として、認証サービス２１０がチャレンジ・メッセージを送信してもよい。クライアント１１０Ａは、当該チャレンジ・メッセージに対して、通信２５０の一部として適切な応答を生成しなければならない。

【００４１】

また、通信２５０が認証情報を含むと述べたが、「含む」という用語を認証情報または他のセキュリティ情報と関連して本明細書において使用する際は、当該用語は、送信者が認証情報または他のセキュリティ情報にアクセスしたことを受信者が検証できる情報を通信２５０が実際に含む可能性を包含する。当該検証では、セキュリティ情報の送信は必要

ではない。

【００４２】

通信２５０の形式に関わらず、認証サービス２１０は受信した情報を処理２５２の一部として処理してもよい。処理２５２では、認証サービス２１０が、通信２５０に含まれる認証情報がネットワーク１２０へアクセスする権限を有するクライアントに対応することの正当性を検証することを必要としてもよい。かかる正当性検証を、当業界で公知な技法を用いて実施してもよい。

【００４３】

さらに、処理２５２では、認証情報が権限のあるクライアントに対応するかどうかに応じて、ワンタイム・パスワード・サービス２１２への通信２５４を選択的に生成することを必要としてもよい。認証サービス２１０は、通信２５０に含まれるクライアント１１０から受信したワンタイム・パスワードに基づいて、通信２５４を生成してもよい。

【００４４】

ワンタイム・パスワード・サービス２１２は、プロセス２５６で通信２５４を処理してもよい。プロセス２５６では、ワンタイム・パスワード・サービス２１２が、通信２５４が正当なワンタイム・パスワードを含むかどうかを判定してもよい。

【００４５】

任意の適切な技法を処理２５６で使用して、ワンタイム・パスワードの正当性を検証してもよい。当該技法には、ワンタイム・パスワードの正当性を検証するための当業界で公知な技法が含まれる。正当性検証には、パスワードが正当なパスワードに対応することと当該パスワードが正当な時点に提示されることとの両方を判定することが含まれる。パスワードは、例えば、その有効期限が切れたかまたは過去に使用されたことがあることを理由として、不正であるかもしれない。しかし、ワンタイム・パスワードの正当性を検証するために使用される具体的な技法は本発明にとって重要ではない。

【００４６】

通信２５０に関して、通信２５４は１つの矢印として示されている。しかし、通信２５４が、ワンタイム・パスワード・サービス２１２と認証サービス２１０の間で１つまたは複数のメッセージが渡されることを必要としてもよいことは理解されよう。さらに、図２では簡単にするため示していないが、通信２５４内の情報を、ワンタイム・パスワード・サービス２１２により発行された情報に基づいて生成してもよい。具体的な例として、ワンタイム・パスワード・サービス２１２が、認証サービス２１０が提供するチャレンジをクライアント１１０Ａに発行してもよい。クライアント１１０Ａが送信したパスワード情報が、ワンタイム・パスワード・サービス２１２により発行され、クライアント１１０Ａにより当該パスワードでエンコードされた、チャレンジを含んでもよい。したがって、通信２５４がパスワードを含むと言及しているが、当該パスワードをエンコードされた形式でまたは他の任意の適切な方法で表現してもよい。

【００４７】

ワンタイム・パスワード・サービス２１２がワンタイム・パスワードをクライアント１１０Ａから受け取る形式に関わらず、ワンタイム・パスワード・サービス２１２は、当該ワンタイム・パスワードの正当性を検証する試みの結果を示す通信２５８を発行してもよい。通信２５８が、ワンタイム・パスワードの正当性検証が成功したことを示してもよく、または、当該パスワードの正当性検証が成功しなかったことを示してもよい。認証サービス２１０での処理２５２に、通信２５８の内容に基づいて条件を付してもよい。

【００４８】

通信２５８がワンタイム・パスワードの認証成功を示す場合は、認証サービス２１０が、クライアント１１０Ａに通信２６２の一部として送信されるクッキー２６０を発行してもよい。本例では、クッキー２６０は、認証サービス２１０がクライアント２５０の認証情報の正当性を検証したこととワンタイム・パスワード・サービス２１２がクライアント１１０Ａにより提供されたワンタイム・パスワードの正当性を検証したこととの両方を示す。しかし、クライアント１１０Ａの認証とワンタイム・パスワードの正当性検証を別々

に示してもよいことは理解されよう。

【００４９】

認証サービス２１０は、これらの条件の何れかが満たされない場合は通信２６２にクッキー２６０を発行しない。より一般的には、認証サービス２１０は、ネットワーク・アクセスに対する全ての要件が満たされていない場合はクッキー２６０を発行しない。幾つかの実施形態では、クッキー２６０が提供されない場合は、通信２６２を完全に省略してもよい。しかし、他の実施形態では、アクセスに対する全ての要件がクライアント１１０Ａによって満たされない場合は、通信２６２をクッキー２６０なしで提供してもよい。

【００５０】

クッキー２６０は任意の適切な形態であってもよい。当該形態には、当業界で公知な形式が含まれる。例えば、クッキー２６０は、クッキー２６０が認証サービスによって特にクライアント１１０Ａに発行されたことの正当性を続いてクッキー２６０の受信者が検証できるように、認証サービス２１０によって署名または暗号化された情報を含んでもよい。

【００５１】

クッキー２６０の形式に関わらず、通信２６２は、クッキー２６０を含み、認証サービス２１０とワンタイム・パスワード・サービス２１２が正当性を検証した認証情報をクライアント１１０Ａが正しく提示したことを認証機関２１４に対して実証し、クライアント１１０Ａがネットワークにアクセスする権利があるとみなせるようにすることを可能にする。したがって、クライアント１１０Ａはクッキー２６０を通信２７０に取り込むことができる。本実施形態では、通信２７０は認証サービス２１０に送信される。処理２７２では、認証サービス２１０は、要求を通信２７０内部に含まれるクッキーとともに通信２７４内の証明機関２１４に転送する。通信２７４を、当業界で公知のプロトコルを用いて証明機関２１４への登録要求としてフォーマットしてもよい。

【００５２】

処理２７６では、証明機関２１４は当業界で公知な技法を用いて登録要求２７４を処理してもよい。しかし、当該処理が、クッキー２６０を含む登録要求に付随するものであってもよい。処理２７６において証明機関２１４が、クッキー２６０がクライアント１１０Ａに対して生成され、かつ、通信２７０における元の証明書要求がクライアント１１０Ａによって開始されたと判定した場合、証明機関２１４は証明書をクライアント１１０Ａに発行する。

【００５３】

処理２７６では、当業界で公知な技法を用いて、証明書が要求される特定のクライアントによって証明書要求が生成されたことの正当性を検証してもよい。また、公知な技法を用いて、クッキー２６０がクライアント１１０Ａに発行され、かつ、クライアント１１０Ａにより転送されたことの正当性を検証してもよい。クッキー２６０内に含まれる情報に基づいて、クライアント１１０Ａに利用可能な秘密情報を用いて当該情報をエンコードすることと組み合わせて、当該正当性検証を行ってもよい。クライアント１１０Ａに利用可能な当該秘密情報は、例えば、証明機関２１４がそれに対応する鍵を保持する、鍵を含んでもよい。具体的な例として、当該秘密情報は、証明機関２１４がそれに対する公開鍵を保持する、公開鍵／秘密鍵の対の秘密鍵であってもよい。しかし、証明機関２１４がクッキー２６０の正当性を検証し証明書を要求するソースの正当性を検証するための、任意の適切な機構を使用してもよい。

【００５４】

この正当性検証がどのように実施されるかに関わらず、証明機関２１４が情報の正当性を検証すると、証明機関２１４は通信２７８で運搬される証明書を発行する。認証サービス２１０は通信２８０で当該証明書をクライアント１１０Ａに転送してもよい。このシナリオでは、通信２８０における当該証明書は、ワンタイム・パスワード・サービス２１２によって発行された情報を直接含まない。しかし、クライアント１１０Ａは、ワンタイム・パスワード・サービス２１２によって受け入れられる正当なワンタイム・パスワードの

提示に成功しなかった場合は、証明機関２１４から証明書を受け取らない。したがって、証明機関２１４が発行した証明書はセキュリティ・アソシエーションの生成で従来から使用されている形式であってもよいが、それでも、当該証明書は正当なワンタイム・パスワードを要求するポリシを実施する機構であってもよい。

【００５５】

図３を参照すると、クライアント１１０Ａが当該証明書を使用してネットワークへのアクセスを取得できるプロセスが示されている。図３のプロセスでは、先ず、クライアント１１０Ａがアクセス制御サーバ１１２とのネットワーク対話３１０を開始してセキュリティ・アソシエーションを生成する。ネットワーク対話３１０では、当業界で公知である、セキュリティ・アソシエーションを確立するためのネットワーク装置間の通信を必要としてもよい。示した実施形態では、ネットワーク対話３１０の結果、クライアント１１０Ａとアクセス制御サーバ１１２が正しく互いを認証したならば、ＩＰｓｅｃセキュリティ・アソシエーションが生成される。

【００５６】

示した実施形態では、ネットワーク対話３１０は、ＩＫＥｖｌを用いてクライアント１１０とアクセス制御サーバ１１２の間で共有された秘密を確立する段階を含む。さらに、ネットワーク対話３１０では、クライアント１１０Ａが証明書３１２をアクセス制御サーバ１１２に送信することを含んでもよい。証明書３１２は、証明機関２１４（図２）が発行した証明書であってもよい。図２に関連して上述したように、クライアント１１０Ａがワンタイム・パスワード・サーバ２１２への正当なワンタイム・パスワードの提示に成功したことをクライアント１１０Ａが証明機関２１４に実証した場合にのみ、証明書３１２が発行される。したがって、アクセス制御サーバ１１２はクライアント１１０Ａがワンタイム・パスワードを提示したことの正当性を明示的には検証しないが、それでも、クライアント１１０Ａが正当なワンタイム・パスワードを提示しない場合は、アクセス制御サーバ１１２はクライアント１１０Ａとのセキュリティ・アソシエーションを生成しない。したがって、アクセス制御サーバ１１２が実施する処理３１４は、ＩＫＥｖｌを用いてセキュリティ・アソシエーションを生成するための当業界で公知の従来型の処理であってもよいが、それでも、クライアント１１０Ａがワンタイム・パスワードを提示しなかった場合はセキュリティ・アソシエーションが生成されず、それにより、マネージド・ネットワーク１２０へのアクセスを、正当なワンタイム・パスワードを他の任意の必要な認証情報に加えて提示できるクライアントにのみ制限する。

【００５７】

クライアント１１０Ａがワンタイム・パスワードを提示したため、正当な証明書３１２を提示できる場合は、処理３１４の結果、ＩＰｓｅｃセキュリティ・アソシエーション３２０が生成される。当該セキュリティ・アソシエーションに基づいて、ネットワーク１２０のトランスポート層３１８内部のアクセス実施コンポーネントは、クライアント１１０Ａとネットワーク装置１２４のようなネットワーク装置との間の通信を可能としてもよい。トランスポート層３１８内部の具体的なコンポーネントは本発明には重要ではなく、任意の適切なコンポーネントまたはコンポーネントの組合せを使用してアクセス制御判定を行ってもよい。しかし、幾つかの実施形態では、アクセス制御判定を、図１の例にある切替装置１１８または他の同様なコンポーネントにより行ってもよい。

【００５８】

アクセス制御判定を実施する具体的なコンポーネントに関わらず、ＩＰｓｅｃセキュリティ・アソシエーション３２０を用いてクライアント１１０Ａにより送信されたネットワーク対話３２２は、トランスポート層内部の処理３２４に基づいて、ネットワーク装置１２４とのネットワーク対話３２６としてマネージド・ネットワーク１２０へと伝わってもよい。ネットワーク装置１２４がネットワーク対話３２６を受け取り、内向きの対話に処理３２８を行い、外向きのネットワーク対話３２６を生成してもよい。かかる外向きのネットワーク対話３２６が、セキュリティ・アソシエーション３２０内部の対話３２２としてトランスポート層３１８を通過してもよい。

【００５９】
しかし、ＩＰｓｅｃセキュリティ・アソシエーション３２０が生成されない場合、トランスポート層３１８は通信をクライアント１１０Ａからネットワーク１２０に渡さず、かかる通信はネットワーク装置１２４により受信されない。反対に、装置１２４が送信したネットワーク通信は、クライアント１１０Ａ向けであっても、トランスポート層３１８によりネットワーク１２０の外には渡されない。このように、クライアント１１０Ａは、正当なセキュリティ・アソシエーション３２０を生成しない場合は、ネットワーク装置１２４との通信がブロックされ、証明書が要求される。クライアント１１０Ａは、正当なワンタイム・パスワードを提示した場合にのみ当該証明書を取得する。
【００６０】
このように本発明の少なくとも１つの実施形態の幾つかの態様を説明したので、様々な変形、修正、および改良が当業者には容易に想到されるであろうことは理解されよう。
【００６１】
１例として、クライアント・コンピューティング装置がマネージド・ネットワークへのアクセスを取得してサーバ１２４のようなネットワーク・リソースにアクセスする実施形態を説明する。「クライアント」が任意のネットワーク・リソースに関していかなる特定の機能を実施する必要もないことは理解されるべきであろう。クライアントを、ＩＰｓｅｃセキュリティ・アソシエーション３２０を生成するためにサービスとの対話を求める任意のコンピューティング装置とみなしてもよく、これは、当該サービスの性質または当該サービスが実装される装置の具体的な構成とは無関係である。
【００６２】
例えば、図２は、認証サービス２１０、ワンタイム・パスワード・サービス２１２および証明機関２１４が単一の装置、即ち、認証サーバ１５０内に含まれることを示す。これらのコンポーネントが同一の物理装置に含まれる必要はなく、これらのコンポーネントの機能を任意数の適切な装置に分散させてもよい。
【００６３】
さらに、アクセス制御サーバ１１２と認証サーバ１５０についても、これらのコンポーネントを別々の装置に実装する必要はない。
【００６４】
さらに別の可能な変形の例として、図２は、認証サービス２１０を介したワンタイム・パスワード・サービス２１２と証明機関２１４との通信を示すが、これは本発明の要件ではない。例えば、クライアント１１０Ａが認証機関２１４と直接通信してもよい。
【００６５】
また、認証サービスが、クライアント１１０Ａを認証した後に通信要求２５６を送信すると説明しているが、この順序は重要ではない。例えば、認証サービスが、応答通信２５８を受け取った後にクライアント１１０Ａの認証を試みてもよい。
【００６６】
さらに、図３は、ＩＰｓｅｃがＩＰｓｅｃトンネル・モードで使用される実施形態を示す。本実施形態では、ＩＰｓｅｃトンネルがクライアント１１０Ａとゲートウェイ１１６の間で生成され、次いでゲートウェイがトラフィックをサーバ１２４のようなエンド・リソースに送信する。ＩＰｓｅｃトンネルはゲートウェイで終了し、そこからは通信をそのまま（ｃｌｅａｒ）またはＩＰｓｅｃを介して送信することができる。
【００６７】
代替的な実施形態では、ＩＰｓｅｃをＩＰｓｅｃ転送モードで使用してもよい。本実施形態では、エンド・ツー・エンドのＩＰｓｅｃ接続をクライアント１１０Ａとサーバ１２４のようなエンド・リソースの間で生成してもよい。この場合、アクセス制御装置は、サーバ１１２のような別々のアクセス制御装置においてではなく、エンド・リソースの一部であってもよい。
【００６８】
かかる変形、修正、および改善は本開示の一部であることが意図され、本発明の趣旨お

よび範囲内にあると意図されている。したがって以上の説明および図面は例にすぎない。

【００６９】

上述の本発明の諸実施形態は、多数の方法のうち何れかで実装することができる。例えば、当該諸実施形態を、ハードウェア、ソフトウェア、またはそれらの組合せを用いて実装してもよい。ソフトウェアで実装すると、ソフトウェア・コードを、単一のコンピュータで提供されるかまたは複数のコンピュータ間で分散されるかに関わらず、任意の適切なプロセッサまたはプロセッサ集合で実行することができる。かかるプロセッサを、１つまたは複数のプロセッサが１つの集積回路コンポーネント内にある、集積回路で実装してもよい。しかし、任意の適切な形式の回路を用いてプロセッサを実装してもよい。

【００７０】

さらに、コンピュータを、ラックマウント・コンピュータ、デスクトップ・コンピュータ、ラップトップ・コンピュータ、またはタブレット・コンピュータのような、幾つかの形態のうち何れかで具体化してもよい。さらに、コンピュータを、一般にはコンピュータとはみなされないが適切な処理機能を有する装置に組み込んでもよい。当該装置には、ＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉａｌ　Ａｓｓｉｓｔａｎｔ）、スマートフォンまたは他の任意の適切なポータブル装置もしくは固定電子装置が含まれる。

【００７１】

また、コンピュータが１つまたは複数の入出力装置を備えてもよい。これらの装置を、とりわけ、ユーザ・インタフェースを提示するために使用することができる。ユーザ・インタフェースの提供に使用できる出力装置の例には、出力を視覚的に提示するためのプリンタまたはディスプレイ・スクリーン、出力を可聴的に提示するためのスピーカまたは他の音声生成装置が含まれる。ユーザ・インタフェース向けに使用できる入力装置の例には、キーボード、マウス、タッチ・パッド、およびデジタイジング・タブレットのようなポインティング・デバイスが含まれる。別の例として、コンピュータが音声認識を通じてまたは他の可聴形式で入力情報を受け取ってもよい。

【００７２】

かかるコンピュータを、任意の適切な形式の１つまたは複数のネットワークで相互接続してもよい。当該ネットワークには、企業ネットワークまたはインターネットのような、ローカル・エリア・ネットワークまたは広域ネットワークが含まれる。かかるネットワークは、任意の適切な技術に基づいてもよく、任意の適切なプロトコルに従って動作してもよく、無線ネットワーク、有線ネットワークまたは光ファイバ・ネットワークを含んでもよい。

【００７３】

また、本明細書で概観した様々な方法またはプロセスを、様々なオペレーティング・システムまたはプラットフォームのうち任意の１つを使用する１つまたは複数のプロセッサ上で実行可能なソフトウェアとしてコーディングしてもよい。さらに、かかるソフトウェアを、幾つかの適切なプログラミング言語および／またはプログラミング・ツールもしくはスクリプティング・ツールのうち何れかを用いて書いてもよく、フレームワークまたは仮想マシン上で実行される実行可能な機械語コードまたは中間コードとしてコンパイルしてもよい。

【００７４】

この点において、本発明を、１つまたは複数のコンピュータまたは他のプロセッサ上で実行されたときに、上述の本発明の様々な実施形態を実装する方法を実施する１つまたは複数のプログラムでエンコードした、コンピュータ読取可能媒体（または複数のコンピュータ読取可能媒体）（例えば、コンピュータ・メモリ、１つまたは複数のフロッピ・ディスク、ＣＤ（Ｃｏｍｐａｃｔ　ｄｉｓｋ）、光ディスク、ＤＶＤ（ｄｉｇｉｔａｌ　ｖｉｄｅｏ　ｄｉｓｋ）、磁気テープ、フラッシュ・メモリ、フィールド・プログラマブル・ゲート・アレイもしくは他の半導体装置における回路構成、または他の非一時的な有形のコンピュータ記憶媒体）として具体化してもよい。１つまたは複数のコンピュータ読取可能媒体は、そこに格納した１つまたは複数のプログラムを１つまたは複数の様々なコンピ

ュータまたは他のプロセッサにロードして上述の本発明の様々な態様を実装できるように、可搬であることができる。本明細書で使用する際、「非一時的なコンピュータ読取可能記憶媒体」という用語は、製造物（即ち、製品）または機械であると考えうるコンピュータ読取可能媒体のみを包含する。

【００７５】

「プログラム」または「ソフトウェア」という用語は、本明細書では上述の本発明の様々な態様を実装するようにコンピュータまたは他のプロセッサをプログラムするために使用できる任意の種類のコンピュータ・コードまたは１組のコンピュータ実行可能命令を指すように一般的な意味で使用される。さらに、本実施形態の１態様によれば、実行時に本発明の方法を実施する１つまたは複数のコンピュータ・プログラムは、単一のコンピュータまたはプロセッサ上に存在する必要はないが、幾つかの様々なコンピュータまたはプロセッサの間でモジュール形式で分散させて本発明の様々な態様を実装してもよいことは理解されるべきであろう。

【００７６】

コンピュータ実行可能命令は、プログラム・モジュールのような、１つまたは複数のコンピュータまたは他の装置によって実行される多数の形態であってもよい。一般に、プログラム・モジュールは、特定のタスクを実施するかまたは特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造、等を含む。一般に、プログラム・モジュールの機能を様々な実施形態において必要に応じて組み合わせるかまたは分散させてもよい。

【００７７】

また、データ構造をコンピュータ読取可能媒体に任意の適切な形態で格納してもよい。説明を簡単にするため、データ構造は、データ構造内の場所を通じて関連するフィールドを有すると示してもよい。かかる関係を、フィールド間の関係を伝達する当該フィールド向けの記憶域に、コンピュータ読取可能媒体内の場所を割り当てることによって同様に実現してもよい。しかし、任意の適切な機構を使用して、データ構造のフィールド内の情報の関係を確立してもよい。当該機構には、ポインタの使用によるもの、データ要素間の関係を確立するタグまたは他の機構が含まれる。

【００７８】

本発明の様々な態様を単体で、組合せで、または上述した諸実施形態で具体的には論じなかった様々な配置構成で使用してもよく、したがって、その適用においては、以上の記載で説明したまたは図面で示したコンポーネントの細部と配置構成には限定されない。例えば、１実施形態で説明した諸態様を、他の実施形態で説明した諸態様と任意に組み合わせてもよい。

【００７９】

また、その例は提供していないが、本発明を方法として具体化してもよい。方法の一部として実施される動作は、任意の適切な方法で順序付けてもよい。したがって、動作が示したものと異なる順序で実施される実施形態を構成してもよい。当該実施形態では幾つかの動作を同時に実施してもよいが、示した実施形態ではこれらは逐次的な動作として示してある。

【００８０】

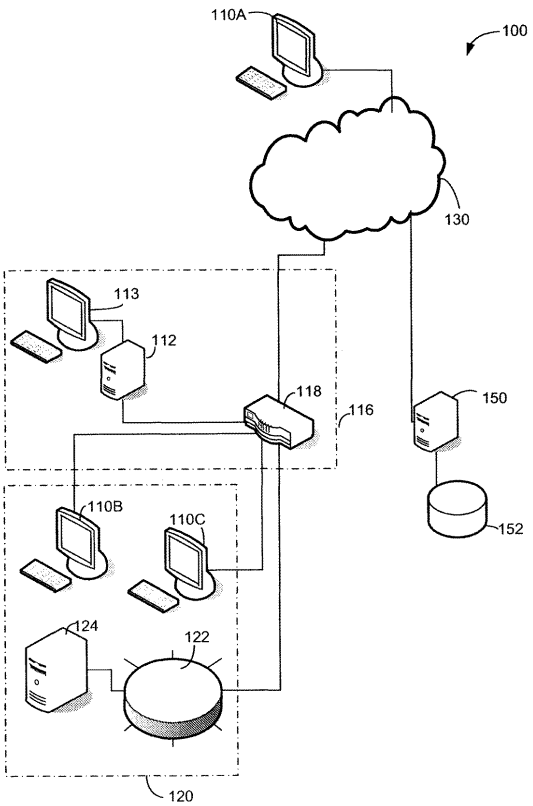
特許請求の範囲で「第１」、「第２」、「第３」、等のような順序語を用いてクレーム要素を修正することは、それ自体、或るクレーム要素の別のクレーム要素に対するいかなる優先度、先行性、または順序も暗示せず、方法の動作を実施する時間的順序も暗示せず、単に、特定の名前を有する或るクレーム要素を、（順序項の使用を除いて）同じ名前を有する別の要素から区別してクレーム要素を区別するためのラベルとして用いられる。

【００８１】

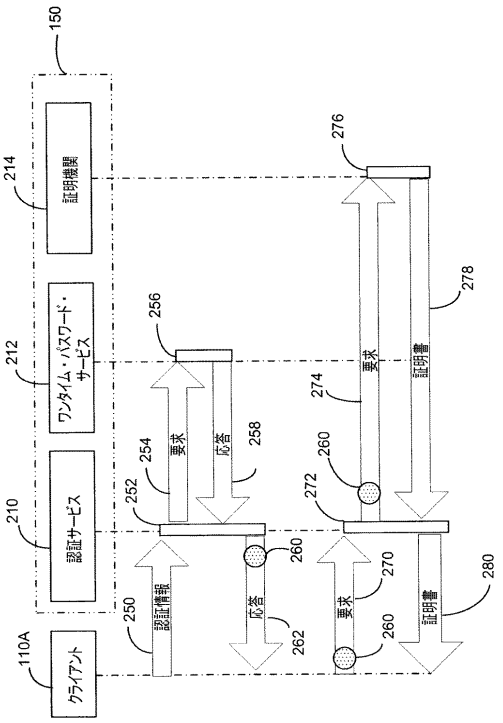
また、本明細書で使用する言回しおよび用語は説明のためであって限定として捉えるべきではない。本明細書での「含まれる」、「備える」、「有する」、「含む」、または「関与する」およびそれらの変形の使用は、それ以降に列挙した項目とその均等物、ならび

に追加の項目を包含することを意味する。

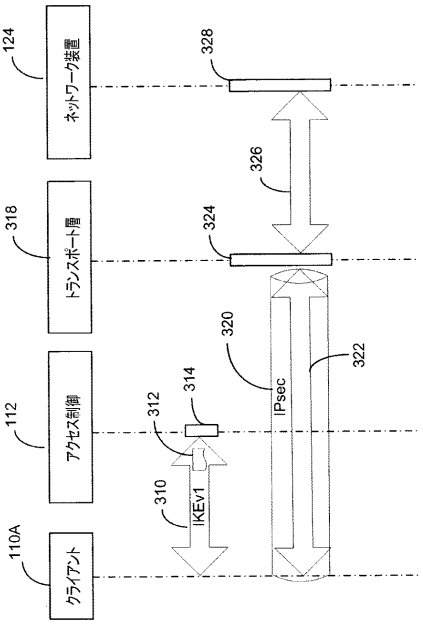
【図１】



【図２】



【図３】


124
ネットワーク装置
328
326
318
トランスポート層
324
320
322
IPsec
314
312
112
アクセス制御
310
IKEv1
110A
クライアント

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/034188

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i, H04L 29/06(2006.01)i, G06F 21/20(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L 9/32; G06F 21/24; G06F 15/16; G06F 15/00; G06F 17/30; G06F 21/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility models

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: one time password, credential, certificate and IPsec.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2007-0072463 A (LEE, SANG GON) 04 July 2007 See abstract, figures 1-4 and claims 1-3.	1-15
A	KR 10-2009-0120047 A (SK TELECOM CO., LTD.) 24 November 2009 See abstract, figure 2 and claims 1-7,13-17,22-24,28-29.	1-15
A	US 2007-0067828 A1 (EYAL BYCHKOV) 22 March 2007 See abstract, figure 3B and claims 1-20.	1-15

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 DECEMBER 2011 (12.12.2011)	**12 DECEMBER 2011 (12.12.2011)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 189 Cheongsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Yang, Jong Phil Telephone No. 82-42-481-8595

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2011/034188

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 10-2007-0072463 A	04.07.2007	None	
KR 10-2009-0120047 A	24.11.2009	None	
US 2007-0067828 A1	22.03.2007	None	

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PE,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

(72)発明者 ベン バーンスタイン
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 アナット バー－アナン
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 ニムロド ベレッド
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