

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第5827680号
(P5827680)

(45) 発行日 平成27年12月2日(2015.12.2)

(24) 登録日 平成27年10月23日(2015.10.23)

(51) Int.Cl. F I
G O 6 F 21/33 (2013.01) G O 6 F 21/33

請求項の数 15 (全 18 頁)

(21) 出願番号	特願2013-510122 (P2013-510122)	(73) 特許権者	314015767
(86) (22) 出願日	平成23年4月27日 (2011.4.27)		マイクロソフト テクノロジー ライセンシング, エルエルシー
(65) 公表番号	特表2013-531834 (P2013-531834A)		アメリカ合衆国 ワシントン州 98052 レッドモンド ワン マイクロソフト ウェイ
(43) 公表日	平成25年8月8日 (2013.8.8)		
(86) 国際出願番号	PCT/US2011/034188	(74) 代理人	100140109
(87) 国際公開番号	W02011/142971		弁理士 小野 新次郎
(87) 国際公開日	平成23年11月17日 (2011.11.17)	(74) 代理人	100075270
審査請求日	平成26年4月28日 (2014.4.28)		弁理士 小林 泰
(31) 優先権主張番号	12/779,457	(74) 代理人	100101373
(32) 優先日	平成22年5月13日 (2010.5.13)		弁理士 竹内 茂雄
(33) 優先権主張国	米国 (US)	(74) 代理人	100118902
			弁理士 山本 修

最終頁に続く

(54) 【発明の名称】 I P s e c と I K E バージョン 1 の認証を伴うワンタイム・パスワード

(57) 【特許請求の範囲】

【請求項 1】

I P s e c 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 の通信を認証サービスに送信するステップと、

前記第 1 の通信に回答してワンタイム・パスワード・サービスから、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、

第 2 の通信を証明機関に送信するステップであって、前記第 2 の通信が、前記第 1 の通信に回答して前記ワンタイム・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検証に成功したことを示す前記インジケーションを含む、ステップと、

前記第 2 の通信に回答して前記証明機関から、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を含む証明書を受け取るステップと、

前記証明機関が提供する前記証明書を用いて前記 I P s e c セッションを確立するステップと

を含む方法。

【請求項 2】

前記 I P s e c 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 I P s e c セッションを確立するステップを含む、請求項 1 に記載の方法。

【請求項 3】

10

20

前記ワнта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、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、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、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、請求項 1 に記載の方法。

10

【請求項 7】

前記応答を受け取るステップが、ワнта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、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、請求項 1 に記載の方法。

20

【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нта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 つのプロセッサを含み、

前記認証サービスが、前記ネットワークを介して第 1 の通信をクライアントから受信するように構成され、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нта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нтаイム・パスワードを前記ワнтаイム・パスワード・サービスに伝えるように構成され、

30

前記ワнтаイム・パスワード・サービスが、前記ワнта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нта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構成され、

前記証明機関が、前記クライアントからの前記ワнта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含む第 2 の通信を前記ネットワークを介して前記クライアントから受け取るように構成され、前記クライアントから受け取った前記結果が前記ワнтаイム・パスワードの前記ワнтаイム・パスワード・サービスによる正当性検証が成功したことを示す場合に選択的に証明書を発行するように構成され、前記証明書が前記ワнтаイム・パスワードの正当性検証が成功したことのインジケーションを含む、

40

システム。

【請求項 10】

前記認証サービス、前記ワнта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含む、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含み、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構成された、請求項 9 に記載のシステム。

【請求項 12】

50

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含み、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 I P s e c セッションを選択的に形成するよう構成された、請求項 9 に記載のシステム。

【請求項 1 3】

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、請求項 1 2 に記載のシステム。

【請求項 1 4】

前記企業ネットワークが I K E v 1 アクセス制御を使用する、請求項 1 3 に記載のシステム。

【請求項 1 5】

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構成され、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、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 (e y e l i d r e a d i n g) 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、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、I P s e c 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

10

20

30

40

50

トがネットワーク通信を送受信するための I P s e c セッションを生成しない。

【 0 0 0 5 】

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。

10

【 0 0 0 6 】

残念ながら、I P s e c 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。I P s e c セッションを生成するには、I K E (I n t e r n e t K e y E x c h a n g e) プロトコルを使用する必要がある。広く使用されている I K E のバージョン 1 (I K E v 1) ではワンタイム・パスワードがサポートされていない。I K E のバージョン 2 (I K E v 2) ではワンタイム・パスワードがサポートされているが、I K E v 2 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 】

20

【 0 0 0 7 】

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。

30

【 0 0 0 8 】

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、I K E v 1 を用いて生成された I P s e c 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。

40

【 0 0 0 9 】

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 】

【 0 0 1 0 】

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。

50

【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 10
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 20
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ー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】

10

20

30

40

50

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。

10

【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(w
i
d
e
a
r
e
a
n
e
t
w
o
r
k)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】

20

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12
0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ー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】

30

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】

40

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

50

可能である。アクセス判定がアクセス制御サーバ 1 1 2 で行われる実施形態では、クライアントが適切なワントタイム・パスワードを提供するかどうか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 1 1 2 をプログラムしてもよい。

【 0 0 2 2 】

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 1 1 2 を構成してもよい。例えば、アクセス制御ゲートウェイ 1 1 2 は、クライアントを認証し、ネットワークの「健全な」ポリシー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 1 1 2 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。

10

【 0 0 2 3 】

アクセス制御サーバ 1 1 2 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 1 2 0 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 1 1 8 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 1 1 0 A のようなマネージド・ネットワーク 1 2 0 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。

20

【 0 0 2 4 】

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。

30

【 0 0 2 5 】

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のみ、マネージド・ネットワーク 1 2 0 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。

40

【 0 0 2 6 】

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。

【 0 0 2 7 】

50

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。

10

【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。

20

【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。

30

【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。

40

【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15

50

0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。

10

20

【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。

30

【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, version 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ー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。

40

【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

50

関 2 1 4 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 1 1 0 A と認証サービス 2 1 0、ワнтаイム・パスワード・サービス 2 1 2、および証明機関 2 1 4 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。

【 0 0 3 8 】

通信の具体的な形式に関わらず、クライアント 1 1 0 A が証明書を認証サーバ 1 5 0 から取得するプロセスを、クライアント 1 1 0 A が通信 2 5 0 を認証サービス 2 1 0 に送信することから始めることができる。通信 2 5 0 を、例えば、パブリック・ネットワーク 1 3 0 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 2 5 0 の具体的な形式に関わらず、通信 2 5 0 はクライアント 1 1 0 A の認証情報をクライアント 1 1 0 A から認証サービス 2 1 0 へ運搬することができる。通信 2 5 0 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 1 1 0 A 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。

10

【 0 0 3 9 】

当業界で公知な認証情報に加えて、通信 2 5 0 はワнтаイム・パスワードを含んでもよい。通信 2 5 0 内部のワнтаイム・パスワードを、クライアント 1 1 0 A 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нта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 1 1 0 A に利用可能としてもよい。

20

【 0 0 4 0 】

図 2 では通信 2 5 0 を 1 つの矢印で示したが、当然のことながら、通信 2 5 0 はクライアント 1 1 0 から認証サーバ 1 5 0 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、認証サービス 2 1 0 からの通信に回答して送信してもよい。具体的な例として、認証サービス 2 1 0 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 1 1 0 A は、当該チャレンジ・メッセージに対して、通信 2 5 0 の一部として適切な応答を生成しなければならない。

30

【 0 0 4 1 】

また、通信 2 5 0 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 2 5 0 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。

【 0 0 4 2 】

通信 2 5 0 の形式に関わらず、認証サービス 2 1 0 は受信した情報を処理 2 5 2 の一部として処理してもよい。処理 2 5 2 では、認証サービス 2 1 0 が、通信 2 5 0 に含まれる認証情報がネットワーク 1 2 0 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。

40

【 0 0 4 3 】

さらに、処理 2 5 2 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нтаイム・パスワード・サービス 2 1 2 への通信 2 5 4 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 2 1 0 は、通信 2 5 0 に含まれるクライアント 1 1 0 から受信したワнтаイム・パスワードに基づいて、通信 2 5 4 を生成してもよい。

【 0 0 4 4 】

ワнтаイム・パスワード・サービス 2 1 2 は、プロセス 2 5 6 で通信 2 5 4 を処理してもよい。プロセス 2 5 6 では、ワнтаイム・パスワード・サービス 2 1 2 が、通信 2 5 4

50

が正当なワнтаイム・パスワードを含むかどうかを判定してもよい。

【 0 0 4 5 】

任意の適切な技法を処理 2 5 6 で使用して、ワнта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нта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で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нта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。

【 0 0 4 6 】

通信 2 5 0 に関して、通信 2 5 4 は 1 つの矢印として示されている。しかし、通信 2 5 4 が、ワнтаイム・パスワード・サービス 2 1 2 と認証サービス 2 1 0 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 2 5 4 内の情報を、ワнтаイム・パスワード・サービス 2 1 2 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нтаイム・パスワード・サービス 2 1 2 が、認証サービス 2 1 0 が提供するチャレンジをクライアント 1 1 0 A に発行してもよい。クライアント 1 1 0 A が送信したパスワード情報が、ワнтаイム・パスワード・サービス 2 1 2 により発行され、クライアント 1 1 0 A 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 2 5 4 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。

【 0 0 4 7 】

ワнтаイム・パスワード・サービス 2 1 2 がワнтаイム・パスワードをクライアント 1 1 0 A から受け取る形式に関わらず、ワнтаイム・パスワード・サービス 2 1 2 は、当該ワнта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 2 5 8 を発行してもよい。通信 2 5 8 が、ワнта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 2 1 0 での処理 2 5 2 に、通信 2 5 8 の内容に基づいて条件を付してもよい。

【 0 0 4 8 】

通信 2 5 8 がワнтаイム・パスワードの認証成功を示す場合は、認証サービス 2 1 0 が、クライアント 1 1 0 A に通信 2 6 2 の一部として送信されるクッキー 2 6 0 を発行してもよい。本例では、クッキー 2 6 0 は、認証サービス 2 1 0 がクライアント 2 5 0 の認証情報の正当性を検証したこととワнтаイム・パスワード・サービス 2 1 2 がクライアント 1 1 0 A により提供されたワнта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 1 1 0 A の認証とワнта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。

【 0 0 4 9 】

認証サービス 2 1 0 は、これらの条件の何れかが満たされない場合は通信 2 6 2 にクッキー 2 6 0 を発行しない。より一般的には、認証サービス 2 1 0 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 2 6 0 を発行しない。幾つかの実施形態では、クッキー 2 6 0 が提供されない場合は、通信 2 6 2 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 1 1 0 A によって満たされない場合は、通信 2 6 2 をクッキー 2 6 0 なしで提供してもよい。

【 0 0 5 0 】

クッキー 2 6 0 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 2 6 0 は、クッキー 2 6 0 が認証サービスによって特にクライアント 1 1 0 A に発行されたことの正当性を続いてクッキー 2 6 0 の受信者が検証できるように、認証サービス 2 1 0 によって署名または暗号化された情報を含んでもよい。

【 0 0 5 1 】

10

20

30

40

50

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ー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、まず、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、IKEv1 を用いてクライアント 1

10

20

30

40

50

10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нтаム・パスワード・サーバ212への正当なワнта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нта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нта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、I K E v l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нта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нта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нта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、I P s e c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、I P s e c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、I P s e c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нта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

10

20

30

40

50

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。

10

【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。

20

【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。

30

【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。

40

【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よい。当該装置には、PDA(Personal Digital Assistant)、スマートフォンまたは

50

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、およびデジタル化・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。

10

【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。

20

【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。

30

【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ピーまたは1組のコピー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。

40

【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

50

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。

【 0 0 7 7 】

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。

10

【 0 0 7 8 】

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。

【 0 0 7 9 】

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。

20

【 0 0 8 0 】

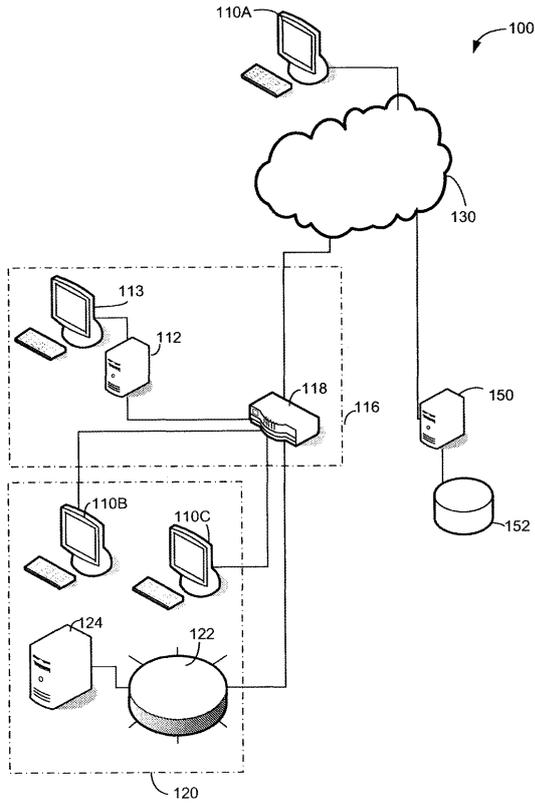
特許請求の範囲で「第1」、「第2」、「第3」、等のような順序語を用いてクレーム要素を修正することは、それ自体、或るクレーム要素の別のクレーム要素に対するいかなる優先度、先行性、または順序も暗示せず、方法の動作を実施する時間的順序も暗示せず、単に、特定の名前を有する或るクレーム要素を、（順序項の使用を除いて）同じ名前を有する別の要素から区別してクレーム要素を区別するためのラベルとして用いられる。

30

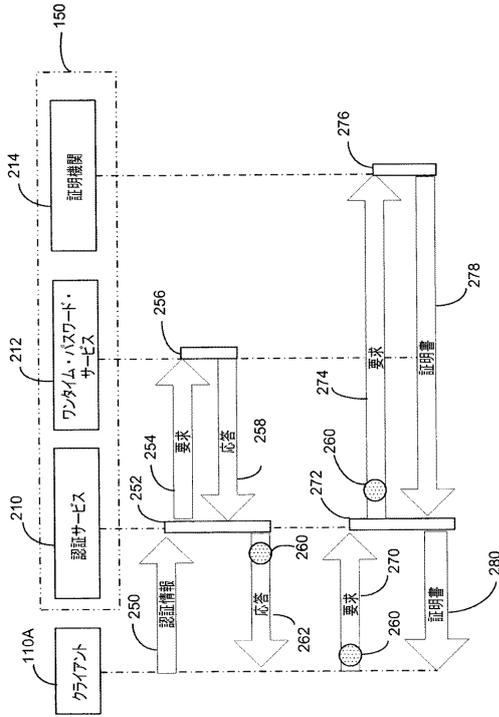
【 0 0 8 1 】

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。

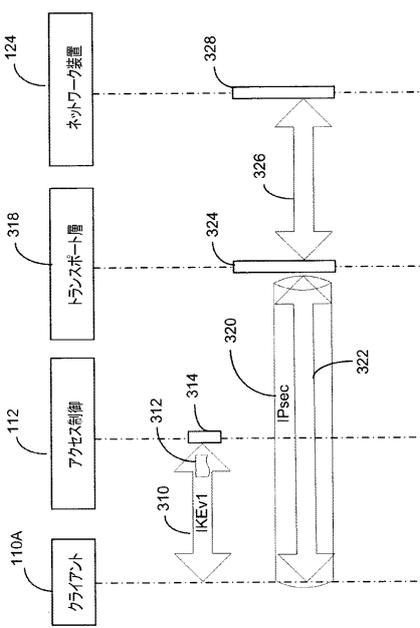
【図1】



【図2】



【図3】



フロントページの続き

- (74)代理人 100153028
弁理士 上田 忠
- (74)代理人 100120112
弁理士 中西 基晴
- (74)代理人 100196508
弁理士 松尾 淳一
- (74)代理人 100147991
弁理士 鳥居 健一
- (74)代理人 100119781
弁理士 中村 彰吾
- (74)代理人 100162846
弁理士 大牧 綾子
- (74)代理人 100173565
弁理士 末松 亮太
- (74)代理人 100138759
弁理士 大房 直樹
- (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 エルシーイー - インターナショナル パテント内
- (72)発明者 ベン パーンスタイン
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 エルシーイー - インターナショナル パテント内
- (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 エルシーイー - インターナショナル パテント内
- (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 エルシーイー - インターナショナル パテント内

審査官 岸野 徹

- (56)参考文献 特開2006-120148(JP,A)
特開平11-282804(JP,A)
特開2008-129673(JP,A)
特表2007-518349(JP,A)
馬場 達也 TATSUYA BABA, 12.3.5 PIC, マスタリングIPsec 初版, 日本, 株式会
社オライリー・ジャパン, 2001年10月25日, pp.288~295, Security Mechanisms for I
nternet Protocol

- (58)調査した分野(Int.Cl., DB名)
G06F 21/33