(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7109909号
(P7109909)

(45)発行日　令和4年8月1日(2022.8.1)

(24)登録日　令和4年7月22日(2022.7.22)

(51)国際特許分類		FI		
H04L 9/32 (2006.01)		H04L	9/32	200B
H04L 9/08 (2006.01)		H04L	9/08	B
G09C 1/00 (2006.01)		H04L	9/08	F
G06F 21/33 (2013.01)		H04L	9/32	200D
		G09C	1/00	640E

請求項の数　22　外国語出願　（全24頁）　最終頁に続く

(21)出願番号　特願2017-224431(P2017-224431)
(22)出願日　平成29年11月22日(2017.11.22)
(65)公開番号　特開2018-117340(P2018-117340A)
(43)公開日　平成30年7月26日(2018.7.26)
審査請求日　令和2年11月17日(2020.11.17)
(31)優先権主張番号　15/361,672
(32)優先日　平成28年11月28日(2016.11.28)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　517409103
エスエスホー コミュニケーションズ セキュリティ オサケユイチアユルキネン
フィンランド国，００３８０ ヘルシンキ，コルネティンティエ ３
(74)代理人　100099759
弁理士　青木 篤
(74)代理人　100123582
弁理士　三橋 真二
(74)代理人　100114018
弁理士　南山 知広
(74)代理人　100180806
弁理士　三浦 剛
(74)代理人　100205969
弁理士　氷室 詩乃

最終頁に続く

(54)【発明の名称】　コンピュータネットワーク内のユーザの認証

(57)【特許請求の範囲】

【請求項１】

ネットワーク装置であって、

少なくとも１つのプロセッサと、実行されたとき、ホストに対してユーザ装置を認証する認証エージェントエンティティとして前記ネットワーク装置を動作させる命令を格納するメモリとを含むネットワーク装置であって、

ネットワークを介して、前記ユーザ装置からのホストへの接続要求を受信し、

前記接続要求を受信したことに応答して、前記ユーザ装置の少なくとも一つのユーザ役割を決定し、

一時的認証子を、決定した前記少なくとも一つのユーザ役割に基づいて認証装置から取得し、

前記接続要求に基づいて、前記ユーザ役割に基づいて取得した前記一時的認証子を使用して前記ホストの認証を実行する、ように構成されたネットワーク装置。

【請求項２】

認証局を設けるように構成された装置から前記一時的認証子を取得するように構成された、請求項１に記載のネットワーク装置。

【請求項３】

前記一時的認証子を前記メモリに格納し、前記接続要求の受信に応答して、決定した前記少なくとも一つのユーザ役割に基づいて、前記メモリから前記一時的認証子を取り出すように構成された、請求項１に記載のネットワーク装置。

【請求項４】
前記メモリは、揮発性メモリを含む、請求項３に記載のネットワーク装置。
【請求項５】
前記一時的認証子は、証明書を含む、請求項１に記載のネットワーク装置。
【請求項６】
前記証明書は、他の一時的認証子の公開鍵部分の少なくとも一部を含む、請求項５に記載のネットワーク装置。
【請求項７】
前記一時的認証子は、他の制限を有し、前記他の制限は、前記一時的認証子を使用することができる回数の制限及び／又は前記一時的認証子の使用の制限を含む、請求項１に記載のネットワーク装置。
【請求項８】
取得した前記一時的認証子を使用して第２認証子を取得するように更に構成され、前記第２認証子は、前記一時的認証子の少なくとも一部に基づいている、請求項１に記載のネットワーク装置。
【請求項９】
前記第２認証子は、一時的なキーペア及び少なくとも１以上の永続的認証子の使用に基づいている、請求項８に記載のネットワーク装置。
【請求項１０】
前記認証エージェントエンティティは、前記認証装置と異なる、請求項１に記載のネットワーク装置。
【請求項１１】
取得した前記一時的認証子は、有効期間に関連する、請求項１に記載のネットワーク装置。
【請求項１２】
ネットワーク装置に設けられた認証エージェントエンティティによってホストに対してユーザ装置を認証する方法であって、
ネットワークを介して、前記認証エージェントエンティティによって前記ユーザ装置からの前記ホストへの接続要求を受信するステップと、
受信した前記接続要求に応答して、前記認証エージェントエンティティによって前記ユーザ装置の少なくとも一つのユーザ役割を決定するステップと、
前記認証エージェントエンティティによって、一時的認証子を、決定した前記少なくとも一つのユーザ役割に基づいて認証装置から取得するステップと、
前記認証エージェントエンティティによって、前記接続要求に基づいて、前記ユーザ役割に基づいて取得した前記一時的認証子を使用して前記ホストに対して前記ユーザ装置を認証するステップと、を含み、
前記認証エージェントエンティティは、前記認証装置と異なる、方法。
【請求項１３】
前記一時的認証子を取得するステップは、前記一時的認証子を生成することを含む、請求項１２に記載の方法。
【請求項１４】
前記一時的認証子をメモリに格納することを含む、請求項１２に記載の方法であって、前記取得するステップは、前記メモリから前記一時的認証子を取り出すことを含む、方法。
【請求項１５】
前記一時的認証子は、証明書を含む、請求項１２に記載の方法。
【請求項１６】
前記証明書は、他の一時的認証子の公開鍵部分の少なくとも一部を含む、請求項１５に記載の方法。
【請求項１７】
前記一時的認証子は、他の制限を有し、前記他の制限は、前記一時的認証子を使用する

ことができる回数の制限及び／又は前記一時的認証子の使用の制限を含む、請求項１２に記載の方法。
【請求項１８】
前記一時的認証子は、一時的なキーペア及び少なくとも１以上の永続的認証子の使用に基づいている、請求項１２に記載の方法。
【請求項１９】
実行されたとき、ホストに対してユーザ装置を認証する認証エージェントエンティティとしてネットワーク装置を動作させる命令を、前記ネットワーク装置のプロセッサに実行させるためのプログラムコードを含む非一時的なコンピュータ可読媒体であって、前記命令は、
ネットワークを介して、前記プロセッサによって、前記ユーザ装置からの前記ホストへの接続要求を受信するステップと、
受信した前記接続要求に応答して、前記プロセッサによって、前記ユーザ装置の少なくとも一つのユーザ役割を決定するステップと、
前記プロセッサによって、一時的認証子を、決定した前記少なくとも一つのユーザ役割に基づいて認証装置から取得するステップと、
前記プロセッサによって、前記接続要求に基づいて、前記ユーザ役割に基づいて取得した前記一時的認証子を使用して前記ホストに対して前記ユーザ装置を認証するステップと、
を含む、非一時的なコンピュータ可読媒体。
【請求項２０】
前記命令は、前記一時的認証子を前記ネットワーク装置のメモリに格納することを含み、前記取得するステップは、前記メモリから前記一時的認証子を取り出すことを含む、請求項１９に記載の非一時的なコンピュータ可読媒体。
【請求項２１】
前記メモリは、揮発性メモリを含む、請求項２０に記載の非一時的なコンピュータ可読媒体。
【請求項２２】
前記一時的認証子は、証明書を含む、請求項１９に記載の非一時的なコンピュータ可読媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、コンピュータ化されたネットワーク内のホストへのアクセスに関する。特に、アクセス及び通信に認証子を使用することに関する。
【背景技術】
【０００２】
コンピュータ化されたネットワークシステムは、典型的には、様々なコンピューティング装置及び装置間のデータ通信を可能にする他の機器を含む。物理コンピューティング装置は、しばしばホストと呼ばれる。ホストは、物理コンピューティング装置内の、仮想コンピューティング装置又はＬｉｎｕｘコンテナなどのコンテナ又は等価物であってもよい。各ホストは、１つ又は複数のユーザカウント、プロセス、及び／又はファイルを含むか、又はそれらと関連付けることができる。
【０００３】
ユーザは、コンピュータ化されたネットワークシステムにおける通信のために構成されたユーザ装置を用いてホストにアクセスできる。アクセスされるホストは、ターゲットホストと呼ばれることもある。ユーザは、様々な理由により、コンピュータ化されたネットワーク内のホストにアクセスしたい場合がある。例えば、ホストは、様々なサービスを提供することができ、及び／又はユーザが使用したいファイル又は他のコンテンツを格納できる。コンピュータ化されたネットワークシステム内のホスト及び他のエンティティにアクセスするための様々な構成がなされる。これらの非限定的な例には、ウェブベースのア

クセス、セキュリティプロトコル（例えば、セキュアシェルプロトコル、　ＳＳＨ）ベースのアクセス、ファイル転送アクセス、リモートプロシージャコールアクセス、及び／又はソフトウェアアップグレードアクセスが含まれる。そのようなアクセスは、例えば、エンドユーザ、自動化、及び／又はシステム管理者によって使用されてもよい。

【０００４】

データ通信、ホストへのアクセス、ユーザ装置及びホスト自体は、権限のない者による攻撃に対して脆弱である場合がある。したがって、セキュリティ（安全性）への配慮が重要である。例えば、企業、政府機関又は地方自治体組織又は非営利団体ならびに個人ユーザは、通常、コンピュータシステム及びそこに格納されたデータがどのようにアクセスされ使用されるのかを管理することを望む。

【０００５】

データの安全性を強化するための様々なソリューションが提案されている。これらの一部は、キー（鍵）の使用に基づいている。鍵は、例えば、装置間で通信されるデータの暗号化及び／又は格納されたデータの暗号化に使用できる。暗号化に加えて、鍵は、認証、承認機能、電子署名などにも使用される。公開鍵と秘密鍵が使用される。公開鍵暗号方式又は非対称暗号方式では、公開鍵と秘密鍵のペアが使用される。公開鍵は広く配布されてもよいが、秘密鍵は所有者にしか知られない。これは、認証（公開鍵はペアの秘密鍵の所有者がメッセージを送信したことを検証するために使用される）と暗号化（ペアの秘密鍵の所有者のみが公開鍵で暗号化されたメッセージを復号化できる）を達成する。別のセキュリティ機能は、鍵の検証や署名に使用される証明書の使用に基づいている。公開鍵証明書を使用して公開鍵の所有権を証明できる。公開鍵証明書は、電子証明書又はＩＤ証明書としても知られる電子文書であって、鍵に関する情報、鍵の所有者の身元（Ｉｄｅｎｔｉｔｙ、ＩＤ）に関する情報、及び証明書の内容が正しいことを検証したエンティティの電子署名を含む。原理は、署名が有効で証明書を調査する人が署名者を信頼している場合、その鍵を使用してその所有者と安全に通信できるということである。証明書は、攻撃者が安全なＷｅｂサイトや他のサーバに偽装するのを防ぐための優れた防御を提供すると考えられている。証明書は、認証局（ＣＡ：　Ｃｅｒｔｉｆｉｃａｔｅ　Ａｕｔｈｏｒｉｔｙ）によって署名される。ＣＡは、信頼できる者又は組織、例えば、自己証明書を発行するように顧客に請求する会社、であってもよい。ウェブの信頼スキームでは、鍵（自己署名証明書）の所有者又は証明書を調べる人が知っており、かつ信用しうる他のユーザ（「裏書」）を署名者とすることができる。

【０００６】

鍵と証明書は、セキュリティを強化するためにコンピュータ化されたネットワークシステムにおいて広く使用されている。そのような広範な使用は問題を引き起こす場合がある。例えば、任意の組織及び／又はコンピュータ化されたシステムでは、多数の証明書が使用されることがある。これらの証明書の一部は、誰も気づかない、又は把握しないシステムで使用されうる。特定の問題は、有効期間の設定がない証明書又は長期間の経過後に期限切れになる証明書によって生じる場合がある。また、アクセス権が失効したユーザ、例えば、元従業員又は下請け業者に証明書が発行されている場合がある。証明書が存在し無効にならない限り、証明書はホストへのアクセスに使用できる。さらに、ホストへのアクセス要求に応じて接続が確立されると、それは長期間にわたって、さらには無期限であっても、オープン状態のままになる場合がある。

【０００７】

システムをスキャンして、任意の古い及び／又は未使用の証明書及び／又はさもなければ疑わしい証明書及び鍵とオープン状態の古い接続を取り除くことができる。しかし、スキャンにはかなりの時間がかかり、及び／又は使用してはならないものを見逃すことがある。

【０００８】

多数の物理エンティティがユーザにホストへのアクセスを提供する仮想化環境やクラウドコンピューティングでは、証明書、その他の認証子、セキュリティ機能、古い接続の管

理がさらに問題になる。例えば、クラウド内の異なる物理エンティティ又はホストによって異なるセッションで１つのサービスにアクセスする１人のユーザにそのサービスを提供すると、証明書及び／又は鍵が多数の場所で使用されることになる。さらに、異なるタイプのホストは、アクセスに異なる認証子の使用を必要とすることがある。ユーザは、例えば、レガシータイプ又はクラウドタイプのホストのどちらに彼／彼女がアクセスしようとしているかを認識していない場合がある。これは、鍵と証明書の使用、及び一般的なホストへのアクセスを管理する上で、多くの課題を設定することになる。

【０００９】

上記問題は、特定の通信プロトコル及びデータ処理装置に限定されず、証明書などの認証子がデータの安全性を強化するために使用される任意のコンピュータ化されたシステムで生じる場合があることに留意されたい。

【発明の概要】

【発明が解決しようとする課題】

【００１０】

本発明の実施形態は、上記問題の１つ又は複数に対処することを目的とする。

【課題を解決するための手段】

【００１１】

ある態様によれば、少なくとも１つのプロセッサと、実行されたとき、装置をエージェントとして動作させる命令を格納するメモリとを含む装置であって、接続要求を受信したことに応答して、一時的認証子を決定し、一時的認証子を使用して第２認証子を取得し、第２認証子は、一時的認証子の少なくとも一部の使用に基づいており、第２認証子を使用してホストの認証を実行する、ように構成された装置が提供される。

【００１２】

別の態様によれば、エージェントエンティティによってホストに対してユーザを認証する方法が提供される。本方法は、エージェントエンティティによってユーザからのホストへの接続要求を受信するステップと、受信した接続要求に応答して、エージェントエンティティによって一時的認証子を決定するステップと、エージェントエンティティによって一時的認証子を使用して第２認証子を取得するステップであって、第２認証子は、一時的認証子の少なくとも一部の使用に基づいている、ステップと、エージェントによって、第２認証子を使用してホストに対してユーザを認証するステップと、を含む。

【００１３】

さらに別の態様によれば、コンピュータ化されたネットワーク内のホストとホストへのアクセスを要求する装置との間のセキュリティ方法のための命令を、プロセッサに実行させるためのプログラムコードを含む非一時的なコンピュータ可読媒体が提供される。実行される本セキュリティ方法は、ユーザから受信したホストへの接続要求を処理するステップと、受信した接続要求に応答して、一時的認証子を決定するステップと、一時的認証子を使用して第２認証子を取得するステップであって、第２認証子は、一時的認証子の少なくとも一部の使用に基づいている、ステップと、第２認証子を使用してホストに対してユーザを認証するステップと、を含む。

【００１４】

より詳細な態様によれば、本装置は、ユーザ装置を含む。別の態様によれば、本装置は、ユーザ装置が接続要求を送信する接続先であるネットワーク装置を含む。本装置は、一時的認証子を生成するように構成できる。本装置はまた、一時的認証子をメモリに格納し、接続要求の受信に応答してメモリから一時的認証子を取り出すように構成されてもよい。このメモリは、揮発性メモリを含む。

【００１５】

第２認証子は、証明書を含めてもよい。一時的認証子は、公開鍵を含めてもよい。証明書は、一時的認証子の公開鍵部分の少なくとも一部を含めてもよい。

【００１６】

第２認証子は、制限された存続期間を有することができる。

【００１７】
第２認証子は、一時的なキーペア及び少なくとも１以上の永続的認証子の使用に基づくことができる。
【００１８】
より詳細な特定の態様は、本明細書から明らかになる。
【００１９】
本発明の様々な例示的な実施形態は、添付の図面によって例示される。ステップ及び要素は、並べ替えられ、省略され、結合されて新しい実施形態を形成してもよく、実行されるものとして示される任意のステップは、別の装置又はモジュールによって実行されるようにしてもよい。
【図面の簡単な説明】
【００２０】
【図１】本発明の一態様が具体化され取得するネットワークの例を示す。
【図２】一実施形態によるフローチャートを示す。
【図３】別の態様を示す。
【図４】一実施形態によるフローチャートを示す。
【図５ａ】エージェントの使用例を示す。
【図５ｂ】エージェントの使用例を示す。
【図５ｃ】エージェントの使用例を示す。
【図６】プリンシパルの概念に関する一例を示す。
【図７】さらに別の態様を示す。
【図８】さらに別の態様を示す。
【図９】さらに別の態様を示す。
【図１０】さらに別の態様を示す。
【図１１】さらに別の態様によるフローチャートを示す。
【図１２】データ処理装置を示す。
【発明を実施するための形態】
【００２１】
図１は、本明細書に記載のいくつかの態様が具現化されているコンピュータ化されたネットワークシステム１の例を示す。より詳細には、図１は、中間装置２０が、ホストとホストにアクセス可能な装置との間にセキュリティ機能を提供する態様の特定の例を示す。この特定の例では、ユーザ１０は、ユーザ装置１１を使用してホスト３０にアクセスする。ネットワークを介したアクセスパスは、ユーザ装置１１からホスト３０への矢印１００及び１０６によって示される。
【００２２】
ネットワークは、例えば、企業又は他の組織のイントラネット、又はインターネットなどのより広範なネットワークを含むことができる。ネットワークは、例えば、ＩＰｖ４（インターネットプロトコルバージョン４）又はＩＰｖ６（インターネットプロトコルバージョン６）ベースのネットワークである。ネットワークシステムは、１以上のデータネットワークを含むことができる。
【００２３】
この態様の中間装置は、中間装置がホストと装置との間に中間ノードを提供するために、ホストとホストへのアクセスを要求する装置と通信するように構成されたインターフェース装置２２、２３を含む。中間装置は、インターフェース装置に接続され、少なくとも１つのプロセッサと、実行されたときに、制御装置に本明細書で説明するタスクを実行させる命令を格納するメモリとを含む制御装置２８をさらに備える。プロセッサは、ホスト３０へのアクセスのために装置１１からの要求１００を処理するように構成できる。要求を受信した後、プロセッサは、要求されたアクセスで使用する認証子４０を取得できる。これは、要求１０２を外部セキュリティ装置２５に送信し、そこから認証子４０をメッセージ１０４で受信することによって提供できる。あるいは、統合セキュリティ装置に中間

装置を設けることができ、そこから認証子を要求できる。中間装置２０はさらに、取得された認証子を使用する通信を監視するように構成される。中間装置２０は、セキュリティ装置からの認証子に基づいて確立された通信を制御するように構成することもできる。

【００２４】

認証子は、証明書を含むことができ、制御装置は、認証局（ＣＡ）を備えるセキュリティ装置から証明書を要求するように構成される。ＣＡは、外部エンティティであってもよく、あるいは中間装置と統合されてもよい。

【００２５】

この説明では、「ホスト」又は「ターゲットホスト」という用語は、装置１１によってアクセス可能なエンティティを指す。アクセスされたホスト３０は、ネットワークを介してユーザにサービスを提供できる。ホストは、例えば、サーバ又は他の物理的なデータ処理エンティティによって提供されてもよい。ホストは、クラウドコンピューティングベースの仮想環境内に提供されてもよい。

【００２６】

ホストには論理的役割が与えられる。すなわち、ホストは必ずしも特定の名前とＩＤで識別される必要はないが、論理的役割を割り当てられる。例えば、ウェブサーバ、データベースサーバ（例えば、Ｏｒａｃｌｅデータベースサーバ）などの論理的役割をホストに割り当てることができる。ターゲットホストは、静的役割ベース（ｓｔａｔｉｃ　ｒｏｌｅ－ｂａｓｅｄ）のテンプレートで構成できる。ホスト構成とアプリケーションソフトウェアは、自動システム構成ツールを使用してプロビジョニングできる。これらの例には、ＣＨＥＦ、ＰＵＰＰＥＴ、ＡＮＳＩＢＬＥなどの商品名で提供されるものが含まれる。

【００２７】

論理的役割は、設定ツールテンプレートを使用してプロビジョニングできる。論理的役割に基づいてユーザプリンシパルなどの特徴が、システムレベルのアカウントにマッピングできる。プリンシパルは、システム内の論理的特権として理解される。ユーザは、自分自身を認証する場合にプリンシパルのセットが与えられる。次に、これらのプリンシパルがターゲットホストで使用され、ユーザをターゲットシステムアカウントにマッピングできる。例えば、ｘｘｘデータベースサーバでは、「ｘｘｘ－ａｄｍｉｎｓ」プリンシパルが「ｘｘｘ」システムアカウントへのアクセスを提供する。

【００２８】

ユーザ装置１１は、無線インターフェースを介してネットワークに接続されたモバイル装置を備えることができる。したがって、接続の少なくとも一部は、無線インターフェースを介して提供されることができる。例えば、ユーザ装置は、通信ネットワークへの無線アクセスを提供されてもよい。ネットワークへの無線接続は、例えば、無線ローカルエリアネットワーク（ＷＬＡＮ）、ＧＳＭ／ＥＤＧＥ／ＨＳＰＡ、３Ｇ、４Ｇ、５Ｇ、又はＷｉＭＡＸ規格、及び／又は光ネットワーク及び近距離無線ネットワーク、又は任意の将来のワイヤレス標準の開発に基づいて、基地局を介して提供されることができる。ユーザ装置はまた、固定回線接続を介してネットワークに接続されたコンピュータ装置を備えてもよい。

【００２９】

通信ネットワークへのアクセスは、適切なセキュリティプロトコルに基づいて保護することができる。制御装置２０は、認証子に対する要求をセキュリティ装置に送信する前に、ホスト３０へのアクセス要求１００を認証するように構成された認証コンポーネント（要素）を備えることができる。例えば、セキュアシェル（ＳＳＨ）プロトコル、セキュアソケットレイヤ（ＳＳＬ）プロトコル、トランスポートレイヤセキュリティ（ＴＬＳ）プロトコルなどを使用できる。図１の例では、ユーザ装置１１がネットワーク要素内に設けられた別のＳＳＨエンティティ２１との通信に適合したＳＳＨクライアント１２を備えるように示されている。

【００３０】

ネットワークシステム及びその中の通信は、悪意のあるユーザによる攻撃及びデータ漏

洩及び他の不正なデータ通信からシステムを保護し、及び／又はデータ損失を防止するために、絶えず監視できる。中間装置は、装置とホスト間の通信を監視するための中間監視機能をネットワークに提供するために使用されてもよい。監視は、暗号化された通信にも適用できる。中間装置はまた、通信を仲介するように構成されてもよい。仲介は様々な理由で提供される場合がある。例えば、防御、分析、監査の目的のため、及び／又はデータの損失を防止するために仲介を用いてデータを作成できる。例えば、企業、政府機関又は地方自治体組織、非営利団体などの組織は、内部コンピュータシステムの使用及びアクセスを監査及び／又は監視することを望む場合がある。これを提供する方法は、適切な中間ノードによって二者間で通信されるデータを取得し、分析することである。

【００３１】

中間装置を流れるデータの少なくとも一部は、暗号化される場合がある。そのような場合、中間データ処理装置は、そこを流れる暗号化されたデータにＭＩＴＭ（Ｍａｎ－Ｉｎ－Ｔｈｅ－Ｍｉｄｄｌｅ）型の操作を提供して、データの平文を取得するように構成できる。ＭＩＴＭ操作は、暗号化されたデータの復号化を含む。これは、秘密鍵又は暗号化に使用される他の暗号化クレデンシャルの知識に基づくことができる。データキャプチャ中間ノードは、信頼できる者、典型的にはネットワークの所有者によって操作され維持され、したがって、復号化に必要な鍵及び／又は他のセキュリティ情報を提供できる。これは一例に過ぎず、示されたアーキテクチャ及び／又はＭＩＴＭ型の操作がすべての状況で必要というわけではないことに留意されたい。例えば、監視される通過データフローは、平文であってもよく、例えば、平文転送制御プロトコル（ＴＣＰ）又はユーザデータグラムプロトコル（ＵＤＰ）通信であってもよい。示された構成の代わりに、他のネットワーク構成及びモードも可能である。例えば、インターフェースは、バスチオンモードにすることができる。

【００３２】

暗号監査部（ａｕｄｉｔｏｒ）のようなデータキャプチャ装置は、スタンドアローンのハードウェア要素として提供されてもよいし、別の要素、例えば、ファイアウォール又は同様の要素に埋め込まれてもよい。データキャプチャ装置は、クラウドコンピューティング環境に設定された仮想マシンとして提供することもできる。ファイアウォールは、一つ又は複数のプロトコル、例えば、セキュアシェル（ＳＳＨ）プロキシ、リモートデスクトッププロトコル（ＲＤＰ）プロキシ、仮想ネットワークコンピューティング（ＶＮＣ）プロキシ、ファイル転送プロトコル／セキュア（ＦＴＰ／Ｓ、ＦＴＰ ｏｖｅｒ ｓｅｃｕｒｅソケット（ＳＳＬ）、トランスポート層セキュリティ（ＴＬＳ）プロトコル）プロキシ、又はＨＴＴＰ／Ｓ（ＨＴＴＰ／ＳＳＬ ｏｖｅｒ ＳＳＬ／ＴＬＳ）プロキシ、を含むことができる。プロキシは、複数のプロトコルを実装することもできる。各プロキシは、セッションの平文へのアクセスを取得するために、ＭＩＴＭ操作、又はキーエスクロー又は他の適切な方法を実行するＭＩＴＭ要素を含むことができる。

【００３３】

図１では、ユーザ装置１１とターゲットホスト３０との間の通信セッションが中間データキャプチャ装置２０を通って流れる。中間ノード２０は、そこを通るトラフィックを監視し、例えば、データ監査目的のためにデータを取得するよう構成されたデータキャプチャエンティティをホストする。キャプチャされたデータは、中間ノードで処理及び／又は格納されてもよい。可能性として、キャプチャされたデータの少なくとも一部は、格納及び／又は処理のために別のエンティティに転送される。これは、図１に監査ログエンティティ３５によって示されている。監査ログエンティティは、インターフェース３４を介して中間装置に連絡できる。したがって、装置は、暗号グラフィック監査部又はショート暗号監査部と呼ぶことができる。様々な理由により、システム内のデータトラフィックを監査することが望まれている。例えば、企業ポリシーでは、すべてのデータトラフィック、又は特定のホストからのトラフィックを強制的に監査することがある。ネットワーク・トポロジー上の理由により、監査ノードを処理するためにキーマネージャを設定する必要さえあるかもしれない。監査ノードは、パスワードとキーボードの双方向認証だけを透過的

にサポートできる。すべての課題と応答は、暗号化されていないチャネルを通じて平文で送信されるため、監査ノードを介して透過的にリレーできる。コンテンツの暗号化が使用される場合、監査ノードは平文のパスワードを提供される必要があるだろう。監査システムのキャプチャ要素を高いセキュリティレベルの装置であると分類することができるので、ポリシーを介してこの操作を許可できる。

【００３４】

監査目的のためにキャプチャされたデータが、どのような方法で処理、例えば復号化され分析されるのかは、本明細書に開示される原理の理解にはあまり関連がないことに留意されたい。関連するのは、ユーザ装置１１が中間データキャプチャ装置２０を介してホスト３０にアクセスし、アクセス要求とアクセスの許可後に装置間で通信された通信を含むデータが中間装置を介してルーティングされるということである。

【００３５】

図２のフローチャートは、一態様による動作を示している。２００において、中間装置は、装置からホストへのアクセス要求を受信する。次いで、中間装置は、２０２で、ホストへの要求されたアクセスで使用する認証子を取得する。２０４において、中間装置は、認証子を使用する通信を監視する。

【００３６】

認証子は、外部セキュリティ装置又は統合セキュリティ装置から取得できる。認証子を取得することは、認証子の要求を中間装置からセキュリティ装置、例えば認証局（ＣＡ）に送信することを含めてもよい。監視は、証明書又は他の認証子を使用する通信を監視することを含めてもよい。使用は、アクセスに証明書を使用すること、アプリケーションに応じて、確立された通信セッション（複数可）中に認証子を他の目的のために使用することを意味すると理解されるものとする。

【００３７】

ホストへのアクセス要求は、認証子の要求を送信する前に、要求装置と中間装置との間の通信に使用される少なくとも１つの第２認証子に基づいて認証されてもよい。

【００３８】

監視は、認証子の使用に関する少なくとも１つの条件に基づくことができる。認証子の使用に関する少なくとも１つの条件は、セキュリティ装置とは独立して中間装置によって設定されてもよい。中間装置において、セキュリティ装置からの認証子の使用に関する少なくとも１つの条件の情報を受信することも可能である。特定の態様によれば、認証子は、装置から受信したアクセス要求の認証に使用される第２認証子の有効期間よりも短い有効期間を有する。認証子の有効期間は、セキュリティ装置から受信した認証子の有効期間よりも短くなるように設定されてもよい。また、認証子の有効期間は、ホストに関連して規定された最大セッション長及び／又は装置に関連して規定された最大セッション長よりも短くなるように規定されてもよい。

【００３９】

監視は、認証子の使用を監視することを含むことができる。例えば、認証子がどこで使用されるか、どの位の量のデータが誰によって転送されるか及び／又は認証子がいつ使用されるか、を監視できる。認証子のユーザ（装置及び／又はユーザ）の身元を監視して、悪者がそれを入手しないことを保証できる。ホスト及びホストにおける如何なる変更を監視してもよい。装置の挙動もまた監視できる。例えば、確立された通信に中断があることが検出される。次いで、中断は許容範囲か、又は認証子を無効にするか、及び／又は通信セッションを終了するかを決定できる。認証子に基づいて確立された１つ又は複数の通信セッションに関連する様々なイベントも監視できる。例えば、セキュリティ装置からの認証子に基づいて確立された通信セッションを有するユーザが、他の通信セッションを多数有する場合、許容範囲の数以上の通信セッションを開始しようとする場合、又はそのような通信セッションを仲介しようとする場合、適切な制御動作を行ってもよい。

【００４０】

適切な制御動作を、制御動作の必要性を引き起こすイベントを検出する監視動作に応答

してとることができる。制御動作は、装置のための新しい認証子の要求を含めてもよい。これは、確立された通信セッション及び／又はホストに変更があった場合、又は通信が中断した後に継続される場合に、必要とされることがある。監視によってアラートが引き起こされることもある。アラートは、システムの管理者、ホスト及び／又はホストにアクセスするユーザのためのものであってもよい。中間装置はまた、装置によるホストへのアクセスを防止し、及び／又は、怪しい挙動あるいは予め規定された別のイベント、例えば、長すぎる中断、ユーザの身元又は装置の変更、及び／又は、多数のホストへのアクセスの試みの検出に応答し、装置による少なくとも１つの他のホストへのアクセスを防止できる。ホストへのアクセス又は少なくとも１つの他のホストへのアクセスは、中間装置によって、例えば、ホスト（複数可）へのアクセス用の認証子の使用を一時的に又は永続的に防止することによって、一時的又は永続的に制限されることもある。認証子に基づいて確立された通信セッションの長さも制御されてもよい。

【００４１】

図１は、別個のセキュリティ装置、より詳細には認証サーバ２５を示す。認証サーバは、ネットワークシステムの証明書を発行する機能を提供する認証局（ＣＡ）を含むことができる。ＣＡなどのセキュリティ装置は、記録システム２９と通信して、ユーザを認証し、追加情報、例えばグループ情報を取得できる。セキュリティ装置は、ポリシーの決定をさらに実施できる。ポリシーの決定には、とりわけ、ユーザの認証方法、ユーザグループのプリンシパルへのマッピング方法、及び証明書に含まれるオプションと拡張機能が含まれる。

【００４２】

記録システム２９は、信頼できるユーザ情報レジストリを提供できる。記録システムは、信頼できるユーザ情報源とシステムポリシー規定を提供するように構成できる。顧客側の環境では、これは、例えば、ユーザとグループ（プリンシパル）を保持する、アクティブディレクトリ、ＬＤＡＰ（Ｌｉｇｈｔｗｅｉｇｈｔ Ｄｉｒｅｃｔｏｒｙ Ａｃｃｅｓｓ Ｐｒｏｔｏｃｏｌ）ディレクトリ／ＯｐｅｎＬＤＡＰディレクトリであってもよい。ユーザは、記録システムによって一意に識別できる。一意の識別子（ＩＤ）は、例えば、ＬＤＡＰ ＤＮ（ｃｎ＝Ｍａｒｋｋｕ Ｒｏｓｓｉ、ｃｎ＝ｕｓｅｒｓ、ｄｃ＝ｓｓｈ、ｄｃ＝ｃｏｍ）であってもよい。他のユーザ属性を認証フロー中に使用することでユーザを識別することもできる。ＩＤの他の例には、例えば、ｕｉｄ「ｍｒｏｓｓｉ」、電子メールアドレス、その他のアドレス情報、例えば電話番号、ユーザカウント名を含む。

【００４３】

ユーザ及びユーザグループは、記録システムに構成できる。構成は、例えば、３つのレベルを持つことができる。この場合、第１のレベルは、アクティブなユーザをログイン情報（ユーザ名、パスワード、電子メールアドレス、システムアカウント名など）で規定し、ユーザを論理グループにマッピングするためのもの、第２のレベルは、ユーザ認証情報をユーザアカウントにマッピングする規則を規定するためのもの、第３のレベルは、ユーザとユーザグループをプリンシパルにマッピングするポリシー規則を規定するためのものである。

【００４４】

中間監視装置２０は、様々な他のエンティティと通信するための適切なインターフェース装置を備える。図１において、インターフェース２２の例は、ユーザ装置１１との通信のためのものである。ユーザ１０は、自分のユーザ端末装置１１を用いてホスト３０へのアクセスを開始すると、ターゲットホストに直接アクセスするのではなく、ユーザはまず中間装置にアクセスする。装置２０へのアクセスは、ユーザ装置１１に設けられ、中間装置２０に設けられたクライアント／サーバ２１と通信するように構成されたクライアント１２によって処理されることができる。図の例において、中間装置２０は、ユーザ装置１１、特にユーザ装置に設けられたＳＳＨクライアント１２との安全な通信のためのＳＳＨクライアント２１を備える。このために、変更されていないセキュアシェル（ＳＳＨ）クライアントをユーザ装置１１及び／又は中間装置２０で使用できる。

【００４５】
中間装置２０は、データ処理装置２８に接続されたインターフェースを介して装置からアクセス１００の要求を受信できる。アクセス要求は、アクセス要求の装置によって、認証に使用する少なくとも１つの第２認証子を含むことができる。中間装置２０とホスト間の通信１０６は、インターフェース２３を介して処理できる。通信は、セキュリティ装置２５から取得された認証子に基づくことができる。インターフェース２４は、セキュリティ装置２５との通信のために提供できる。中間装置２０は、要求１０２を送信し、セキュリティ装置からインターフェース２４を介して認証子４０を応答１０４で受信できる。
【００４６】
明瞭化のために別個のインターフェースが示され、論理インターフェースを示すことを理解されたい。インターフェース装置は、示されているものとは異なる数の物理的接続、又はただ１つの物理的接続を含むことができる。さらに、セキュリティ装置は、中間ノード内又は内部の統合要素として提供されてもよく、したがって、中間装置２０とセキュリティ装置との間のインターフェースは、装置２０内の内部インターフェースであってもよい。
【００４７】
認証子の要求は、少なくとも１つの第２認証子に基づいて中間装置によってアクセス要求が認証された後にセキュリティ装置に送信されてもよい。ユーザは、任意の適切な認証子に基づいて中間装置によって認証されることができる。認証子は、例えば、ＰＫＩ構成に従い、公開鍵及び秘密鍵のペアなどの鍵を含むことができる。鍵の集中管理のために鍵管理装置を設けることができる。例えば、ユニバーサル・キーマネージャ・サーバが提供されてもよい。キーマネージャは、データネットワークシステムの装置及びアプリケーション用の鍵を生成し、配布し、管理する。例えば、キーマネージャは、鍵を作成し、システム内の各ホストに非対称鍵のセットを提供できる。
【００４８】
いくつかの例において、セキュリティ装置２５に向けて通信するためのＳＳＨエージェント２７もまた提供されてもよい。ＳＳＨエージェント２７は、ＳＳＨエージェントプロトコルを実装し、例えばＣＡと通信し、ユーザ認証情報を取得し、例えばキーペアなどのユーザ認証の複数の認証子に対処するように構成できる。
【００４９】
中間装置２０は、ユーザのＳＳＨセッションを終了させ、監査ポリシーに基づいてユーザを認証してもよい。中間装置は、ＣＡクライアント機能を埋め込み、ＣＡクライアントを使用して、ユーザの公開鍵にＣＡの署名をすることができる。ＣＡは、記録システムでユーザ認証情報を検証できる。ＣＡは、記録システムでユーザプリンシパルを解決することもできる。ＣＡは、ユーザの公開鍵、及び他の属性、例えばプリンシパルを含む証明書を作成し、その結果物の証明書にその秘密鍵で署名する。暗号監査装置は、対応する秘密鍵と一緒にＳＳＨ認証で証明書を使用する。
【００５０】
次に、ターゲットサーバは、ユーザの証明書を検証する。ターゲットサーバは、ユーザプリンシパルを使用して要求されたシステムアカウントにログインできることを検証する。
【００５１】
この態様は、認証子、例えば、認証子の使用に関する追加の条件を設定できる証明書、を使用して確立された接続に対する監視及び制御を提供する。例えば、この態様は、セッション長の制御を可能にし、乗っ取られた上に不正目的で使用される有効な証明書を使用して作成されたセッションの可能性を防止／低減する。また、この態様は、必要とされる鍵の数を減らすことができる。
【００５２】
以下では、ハイブリッドコンピュータネットワーク環境においてホストにアクセスするための別の態様について、図３及び４を参照して説明する。図３において、いくつかの要素は、図１の要素と同様であるため、ここに詳細な説明は省略する。

【００５３】
ハイブリッド環境は、第１タイプのホスト３２と第２タイプのホスト３４とを少なくとも含むことができる。この異なるログイン資格（クレデンシャル）は、ターゲットホストにアクセスできるようにするため、ユーザ１０に必要とされることがある。ユーザにとって透過的な操作は、ユーザがアクセスしたいターゲットホストのタイプと、ターゲットホストへのアクセスに必要な認証子（複数可）とを決定するように構成された中間装置３８によって提供できる。中間装置は、必要に応じて、セキュリティ装置３６から認証子を取得できる。中間装置３８に含まれるエージェント３９によって、応答及び／又は決定を提供できる。
【００５４】
中間装置は、少なくとも１つのプロセッサと、実行されたとき、装置に適切な動作を実行させる命令を格納するメモリとを備える。これには、ユーザからのホストへのアクセス要求の受信、ホストへのアクセス用の認証子の取得、ホストのタイプの決定、及びアクセス要求の処理が含まれる。処理は、第１タイプのホストへのアクセス用の第１タイプの認証子と、第２タイプのホストへのアクセス用の第２タイプの認証子とを使用する中間装置をもたらす決定を含む。
【００５５】
中間装置は、決定したホストのタイプに応じて、セキュリティ装置から認証子を選択的に要求してもよい。この場合、タイプの決定は、認証子を要求する前に実行される。あるいは、中間装置は、異なるタイプの認証子を含む認証子バスケットをホストに送信してもよい。次に、ホストは、使用するように適合された１以上の認証子を選択できる。
【００５６】
可能性として、中間装置が異なるタイプのホストの認証子を取得し、決定したホストのタイプに応じてセキュリティ装置からすでに受信した認証子を使用するかを決定する。
【００５７】
第１タイプのホストはレガシーホストを含むことができ、第２タイプのホストはクラウドホストを含むことができる。装置は、ターゲットホストがレガシーホスト又はクラウドホストであるかを決定するように構成されてもよい。レガシー・ターゲットホストは、証明書ベースの認証を必ずしもサポートしない、あるいはレガシーホストは、証明書を使用するように構成されていない。代わりに、レガシーホストは、例えば、プリンシパルキーのペアに基づいて操作できる。例えば、対象アカウントの「ａｕｔｈｏｒｉｚｅｄ＿ｋｅｙｓ」ファイルは、対応する「プリンシパルキーのペア」の公開鍵を追加／投入（ｐｏｐｕｌａｔｉｏｎ）できる。追加／投入は、例えば、ホストのプロビジョニング段階で実行される。ＳＳＨユニバーサル・キーマネージャ（ＵＫＭ（登録商標））のような鍵管理システムを使用して、追加／投入を動的に実行する可能性がある。中間装置は、証明書又はプリンシパルキーベースのアクセスが使用されるかを決定するように構成できる。一態様によれば、装置は、ホストへのアクセス要求に応答してホストのタイプを決定し、ホストがクラウドホストであると決定したことに応答して証明書を要求し、ホストがレガシーホストであると決定したことに応答してプリンシパルキーペアを使用するように構成される。
【００５８】
図４は、第１タイプのホスト及び第２タイプのホストを含むハイブリッドコンピュータネットワーク環境のための方法のフローチャートを示す。この方法では、４００でホストへのアクセス要求が受信される。４０２でホストのタイプが決定される。次に、４０４で、アクセス要求は、第１タイプのホストへのアクセス用の第１タイプの認証子と、第２タイプのホストへのアクセス用の第２タイプの認証子とを使用して処理される。
【００５９】
適切な認証子は、ホストのタイプの決定の前、同時に、又はその後に取得できる。
【００６０】
図５ａ、図５ｂ、及び図５ｃは、ハイブリッドコンピュータネットワーク内のホストにアクセスするための方法を実施する異なる可能性を示す。図５ａによれば、５０で、エー

ジェントは、クライアントからアクセス要求を受信した後、クライアントがアクセスを要求するホストによって使用される認証子のタイプを決定する。認証子のタイプを決定すると、エージェントは、決定したタイプの認証子の要求としてメッセージ５１をＣＡに送信する。ＣＡは、決定したタイプの認証子を用いて５２で応答する。エージェントは、メッセージ５３で、この認証子を使用してクライアントにホストへのアクセスを提供する。このタイプの操作は、ホストへの変更が必要でないという利点がある。また、ＣＡでの処理を最適に保つことができる。

【００６１】

図５ｂに示す可能性において、エージェントは、メッセージ５４で、異なるタイプの複数の認証子の送信要求をＣＡに送信する。これらは、好ましくは、クライアント又はエージェント用にＣＡがサポートするあらゆるタイプのものであってもよい。ＣＡは、メッセージ５５でエージェントに異なるタイプの認証子のリストを返す。次に、エージェントは、５６で特定のホストにアクセスするために使用される認証子のタイプを選択し、５７で選択した認証子を使用してホストにアクセスする。この操作方法は、１つの要求で異なるタイプの複数のホストへのアクセスを可能にしながら、ホストでは何らの変更を必要としないという利点がある。

【００６２】

図５ｃは、５８でエージェントが異なるタイプの複数の認証子の送信要求をＣＡに送信する動作を示す。この要求は、好ましくは、クライアント又はエージェント用にＣＡがサポートするあらゆるタイプの認証子に対してできる。ＣＡは、メッセージ５９でエージェントに異なるタイプの認証子のリストを返す。エージェントは、ＣＡから受信した複数の認証子を使用して、アクセス要求６０をホストに送信する。エージェントは、ＣＡから受信したすべての認証子をホストに提供できる。ホストは、複数の認証子を含むアクセス要求６０を受信し、６１でその要求の処理に使用される適切な認証子を選択する。ホストは、選択した認証子を使用して認証プロセスを完了できる。

【００６３】

より具体的な態様によれば、証明書ベースの認証フローは、図１及び２を参照して上述したものと同様に動作する。この例と図１との間の相違点は、セキュリティ装置又はＣＡ３６が構成される方法である。レガシー・ターゲットホストが証明書ベースの認証をサポートしていない、あるいはそれを使用するように構成されていないので、ＣＡはレガシー・ターゲットホストを含むすべてのプリンシパルに対して「プリンシパルキーペア」を持つ可能性がある。ユーザがターゲットホスト（レガシーホスト又はクラウドホストでもよい）へのアクセス要求を送信するとき、この要求は、ＣＡがユーザ装置の公開鍵に署名して証明書を返すという指示を含むことができる。ＣＡは、ユーザ認証を確認し、その結果物の証明書にユーザのプリンシパルを追加できる。

【００６４】

ＣＡは、証明書応答においてすべての適用可能なプリンシパルキーの公開鍵を返す。次に、ＳＳＨハンドシェイクは、｛Ｃｅｒｔｉｆｉｃａｔｅ（ｐｒｉｎｃｉｐａｌ１、ｐｒｉｎｃｉｐａｌ２　．．．）、ＰｒｉｎｃｉｐａｌＫｅｙ１、ＰｒｉｎｃｉｐａｌＫｅｙ２．．．｝というＩＤを用いて続行される。ターゲットホストの構成に基づいて、ターゲットホストは秘密鍵（証明書又はプリンシパルキー）のいずれかを使用して署名動作を要求する。ターゲットホストがクラウドホストである場合、中間装置３８のエージェント３９は、証明書の公開鍵と一致する秘密鍵を有する。ターゲットホストがレガシーホストの場合、エージェントは署名要求をＣＡに委任する。ＣＡは、記録システムでユーザ認証を検証し、ユーザ承認が依然として有効な場合にその動作に署名する。証明書は、例えば、Ｘ．５０９規格に準拠する証明書、又は他の証明書の規格であってもよい。

【００６５】

ターゲットホストの設定は、「使用」と「プリンシパル」で行うことができる。クラウドホストは、「認証されたプリンシパル」マッピングを用いて設定できる。これは、証明書のプリンシパルをホスト上のローカルアカウントにマッピングする。レガシーホストの

ローカルアカウントは、アカウントの「ａｕｔｈｏｒｉｚｅｄ＿ｋｅｙｓ」ファイル内のプリンシパルキーの公開鍵を許可するように設定できる。使用とプリンシパルの役割の例を図６に示す。

【００６６】

この例では、ユーザＵ１～Ｕｎを、ユーザ役割を規定するプリンシパルにマップしている。この例において、ユーザ役割は、管理者、ウェブマスター、及びデータベース管理者である。各ホストに対して、これらのプリンシパルをアカウントにマップして、そのホスト上での様々な管理アクション、ディレクトリ、及びファイルに対するアクセス権限を精緻化する。これにより、各ユーザが比較的少数のプリンシパルにしかマッピングされず、異なるアカウントに対して比較的少数のプリンシパルのマッピングだけがホストで必要となるため、異なるホストを有するユーザの権限のマッピングが簡略化される。さらに、ユーザのプリンシパルへのマッピングは、主として人事情報ベースのマッピングとなり得る。また、プリンシパルのアカウントへのマッピングは、主にＩＴ部門が保有する情報に基づいたマッピングとなり得る。これにより、利用可能な特定のマッピングに関する最良の情報セットを持つ組織によって各マッピングを行うことが可能になる。

【００６７】

記録システムとＣＡの論理ポリシー構成は、「ユーザ」と「プリンシパル」だけを基準に動作できる。

【００６８】

ユーザ視点では、ログインフローは、レガシーホストとクラウドホストの両方で同じである。エージェントは、レガシーホストの場合にプロキシキー操作を実行して、ユーザ認証を提供する。

【００６９】

監査が必要な場合、両方のホストタイプは、ユーザからＣＡへの同様の監査証跡をターゲットホストに提供する。

【００７０】

この構成は、保持する必要がある鍵の量を大幅に減らせるという利点がある。クラウド型ホストの認証子は、比較的短い有効期間を持つように設定できる。したがって、アクセスに使用された直後に、スキャンによって発見される前に有効期間が切れる。これは、特に、新しい仮想ホスト又はサーバが絶えず作成され削除されるクラウド環境において利点がある。

【００７１】

次に、図７～１０を参照して安全なアクセスを提供するエージェントに関連する態様を説明する。エージェント機能７０は、中間装置に実装できる。エージェントは、受信に応答して、ユーザ装置１１から接続要求１００をホスト７２に送信し、一時的なキーペア又は別の認証子を作成するように構成される。エージェントはまた、そのメモリ、例えば揮発性メモリから一時的認証子を取り出すことができる。接続要求は、上述したように、ユーザ装置と装置のＳＳＨエンティティ間で通信されてもよい。ＳＳＨクライアント７１は、システム構成に応じて、ネットワーク側のいずれか、例えば、上述したような中間装置、又はユーザ装置１１に提供できる。

【００７２】

エージェント７０は、作成された一時的なキーペアを使用して証明書を取得する。証明書は、一時的なキーペアの少なくとも一部を使用して制限された存続期間を有する。証明書は、より永続的認証子に基づいてもよい。次いで、取得された証明書７４は、ホスト７２への認証に使用される。より永続的認証子は、認証子の権威によって提供される任意の認証子とすることができる。

【００７３】

一時的なキーペア又は別の一時的認証子は、一度しか使用できないように、又は比較的短い有効期間を持つように作成できる。別の条件は、関連付けられた証明書の存続期間中にのみ使用できることである。また、一時的なキーペアを不揮発性メモリに格納できない

と規定もできる。したがって、エージェントは、１回の認証動作のため、又は限られた時間（例えば、５分間のウィンドウ中のあらゆる認証動作）のため、又はＳＳＨエージェントの存続期間のために、１回だけ使用される一時的なキーをメモリ内に作成できる。

【００７４】

ＳＳＨクライアントがユーザ装置上に実装されている場合、エージェントは、任意によりユーザのホームディレクトリからユーザのレガシーキーを読み取ることができる。

【００７５】

図８は、１つのタイプの認証子のみが必要な場面において、クライアント、エージェント、ＣＡ、及びＣＡに関連する要素間のシグナリングフローを示す。クライアント、この例ではＳＳＨクライアントは、エージェントにＩＤを要求する。エージェントは、一時的なキーペアを、予め作成しておくか、この段階で作成できる。

【００７６】

エージェントは、公開鍵署名要求のためにＣＡに要求を送信する。ＣＡは、適切なメッセージをアクティブディレクトリと交換することによって、ユーザを認証する。

【００７７】

ユーザが認証されると、ＣＡは証明書を作成できる。証明書は、ボールト（Ｖａｕｌｔ）で署名されている。次に、署名された証明書は、ＣＡからエージェントに転送できる。次に、エージェントは、証明書をＳＳＨクライアントに転送できる。これにより証明書を使用できるようになる。

【００７８】

クライアントは、証明書に対応する秘密鍵の所有を確認するためにチャレンジの署名を要求できる。チャレンジの署名要求を受信すると、エージェントは証明書に対応する一時的なキーでチャレンジに署名し、その署名応答によって要求に応答できる。

【００７９】

図９は、ハイブリッドモードのシグナリングを示す。この場合、鍵はＣＡのＨＳＭ／Ｖａｕｌｔに格納され、秘密鍵がユーザに見られることはない。

【００８０】

上記のように、クライアントは、まずエージェントからＩＤを要求する。エージェントは、公開鍵の署名要求のためにＣＡに要求を送信する。ＣＡは、適切なメッセージをアクティブディレクトリと交換することによって、ユーザを認証する。ユーザを認証すると、ＣＡは証明書を作成できる。証明書は、ボールトで署名される。

【００８１】

この段階で、ＣＡは、署名された証明書とプリンシパルキーをエージェントに返すことができる。エージェントは、証明書とプリンシパルキーをクライアントに転送できる。

【００８２】

クライアントは、プリンシパルキーの署名を要求できる。要求を受け取ると、ＣＡは、アクティブディレクトリでユーザを認証し、その後、ボールトからプリンシパルキーの署名を要求できる。署名要求に対する応答は、ＣＡからエージェントへ、さらにはクライアントへ転送される。

【００８３】

クライアントは、証明書又はプリンシパルキーのいずれかを選択して使用できる。あるいは、クライアントは、ホストに対して認証するときに証明書とプリンシパルキーの両方を使用でき、ホストは適切な認証メカニズムとキーを選択する。

【００８４】

図１０は、一実施形態による様々なエンティティ間のシグナリングロジックを示す。ホストサーバ８４への接続要求は、メッセージ１でクライアント８０によって受信される。クライアントは、ステージ２で一時的なキーペアを作成する。キーペアは、例えば、｛Ｃ１－ＰＵＢ、Ｃ１－ＰＲＩＶ｝とすることができる。次に、ユーザ名、パスワード、及びＣｌ－ＰＵＢを含むアクセス要求３を、認証局（ＣＡ）８２に送信する。次に、ＣＡは、メッセージ４によって、Ｃｌ－Ｐｕｂ、ＣＡ－Ｐｕｂｌ、及び署名を含む証明書を返す。

次に、クライアント８０は、メッセージ５をホストサーバ８４に送信するときに証明書を使用する。ステージ６で、ホストサーバは、証明書がＣＡ　ｐｕｂを使用してＣＡによって発行されたことを検証する。肯定的検証の後、サーバは、証明書が信頼できるＣＡ８２によって認可されたものであると信頼できる。その代わり、チャレンジ７がクライアント８０に送信される。クライアントは、チャレンジにＣｌ－ＰＲＩＶで署名することでそれに応答する。ステージ９で、ホストサーバ８４はクライアントの身元を確認できる。

【００８５】

図１１は、ホストに対してユーザを認証するためのエージェントエンティティの動作を示すフローチャートである。この方法では、エージェントエンティティは、５００でユーザからホストへの接続要求を受信し、それに応答して、５０２で一時的認証子を決定する。決定は、一時的認証子を生成するエージェントエンティティを含むことができる。可能性として、エージェントは一時的認証子をそのメモリ内、例えば揮発性メモリ内、に格納し、決定するステップは、メモリから一時的認証子を取り出すステップを含む。次いで、エージェントエンティティは、５０４で一時的認証子を使用して第２認証子を取得できる。第２認証子は、その使用が一時的認証子に少なくとも部分的に基づいているように、外部認証権限によって生成できる。第２認証子は、例えば、一時的なキーペア及び少なくともう一つの永続的認証子の使用に基づいてもよい。次に、エージェントは、５０６で第２認証子を使用してホストに対してユーザを認証できる。

【００８６】

受信した第２認証子は、証明書を含むことができる。一時的認証子は、公開鍵を含むことができる。次に、受信した証明書は、一時的認証子の公開鍵部分の少なくとも一部を含むことができる。

【００８７】

第２認証子の存続期間は、例えば上述したように、制限される。

【００８８】

この態様では、ホストサーバとのアクセス及び通信を安全にするためにキーを使用する必要性を低減するか、又は一切回避することさえ可能である。キーの数を減らすことで、キーの管理が容易になる。これは、特にクラウド環境の場合に当てはまる。ユーザが使用するキーは証明書に変換できる。証明書には、その使用を制限する様々な条件を設定できる。例えば、証明書は、制限された存続期間、例えば、制限された使用回数及び制限された使用、を有することができる。

【００８９】

図１２は、上記実施形態を実現するために必要なデータ処理機能を提供するための制御装置の一例を示す。制御装置９０は、例えば、図１の中間データセキュリティ装置２０を制御し、あるいは図３の３８又は図１、３、５及び７～１０の任意のエージェントを実装するために、例えば、統合され、連結され、及び／又はさもなければ配置されることができる。制御装置９０は、さらに通信セッション、認証子及び任意の追加情報の制御を提供するように構成できる。監視機能に加えて、制御装置は、要求装置、セキュリティ装置、及びホストによる認証、データの復号化、シグナリング及びデータ通信動作などの動作に関連した制御機能を提供するように構成できる。制御装置は、アクセス及び他の制御動作のために中間装置が必要とする鍵又は他の認証子を決定できる。これらの目的のために、制御装置は、少なくとも１つのメモリ９１、少なくとも１つのデータ処理ユニット９２、９３、及び少なくとも１つの入力／出力インターフェース９４を含む。インターフェースを介して、制御装置は、それぞれの装置の他のエンティティに結合できる。制御装置は、適切なソフトウェアコードを実行して制御機能を提供するように構成できる。制御装置は、他の制御エンティティと相互接続することもできる。コンピュータ化されたネットワークにおいてホストとホストにアクセスできる装置との間の中間セキュリティ機能を提供するための手段は、適切なデータ処理及びインターフェース構成を含むことができる。

【００９０】

一態様によれば、中間装置は、中間装置がホストと装置間に中間セキュリティ機能を提

供するように、ホストとホストへのアクセスを要求する装置との通信用に構成されたインターフェース手段と、装置からホストへのアクセス要求を処理し、セキュリティ装置から、要求されたアクセスで使用するための少なくとも１つの認証子を取得し、少なくとも１つの認証子を使用する通信を監視するように構成された制御手段とを含むことができる。

【００９１】

別の態様によれば、ハイブリッドコンピュータネットワーク環境のための制御手段が提供され、環境は第１タイプのホストと第２タイプのホストとを含み、この場合、手段は、装置に、受信したホストへのアクセス要求を処理させ、ホストにアクセスするための認証子を取得させ、ホストのタイプを決定させ、第１タイプのホストへのアクセス用の第１タイプの認証子と、第２タイプのホストへのアクセス用の第２タイプの認証子とを使用して、アクセス要求を処理させる。

【００９２】

一態様によれば、接続要求の受信に応答して、一時的認証子を決定し、一時的認証子を使用して第２認証子を取得し、第２認証子は、一時的認証子の少なくとも一部の使用に基づいており、第２認証子を使用してホストで認証を実行するように構成されたエージェント機能を提供する。この態様における第２認証子は、ＣＡなどの外部セキュリティ装置から要求されてもよい。制御手段は、ネットワーク要素又はユーザ装置に設けられてもよい。

【００９３】

制御手段は、認証子に対する要求をセキュリティ装置に送信する前に、ホストへのアクセス要求を認証するように構成された認証要素をさらに備えることができる。

【００９４】

さらに、制御手段は、アクセス要求装置からのアクセス要求を受信し認証するように構成されてもよく、アクセス要求はアクセス要求の認証に使用するための少なくとも１つの第２認証子を含み、アクセス要求がセキュリティ装置からの少なくとも１つの第２認証子に基づいて認証された後に、セキュリティ装置からの少なくとも１つの認証子を要求し受信し、セキュリティ装置からの少なくとも１つの認証子に基づいて装置とホスト間の通信を処理すること、を含む。

【００９５】

制御手段は、少なくとも１つの認証子の使用に関して少なくとも１つの条件に基づいて通信を監視するように構成することもできる。制御手段は、セキュリティ装置とは独立して少なくとも１つの認証子の使用に関して少なくとも１つの条件を設定できる。制御手段は、セキュリティ装置からの少なくとも１つの認証子の使用に関して少なくとも１つの条件の情報を受信できる。条件は、認証子の有効期間を含むことができる。有効期間は、装置から受信したアクセス要求の認証用の第２認証子の有効期間よりも短く設定できる。制御手段は、セキュリティ装置から受信した認証子の有効期間、装置から受信したアクセスの要求の認証に使用される第２認証子の有効期間、ホストに関連して規定された最大セッション長、及び／又は装置に関連して規定された最大セッション長よりも短い認証子の有効期間の満了を監視してもよい。

【００９６】

制御手段は、少なくとも１つの認証子の使用、少なくとも１つの認証子のユーザ、装置の動作、ホストに関連するイベント、少なくとも１つの認証子、及び／又は少なくとも１つの認証子がどのように及び／又はいつ使用されるかに基づいて確立された１以上の通信セッションに関連するイベントを監視するように構成されてもよい。

【００９７】

制御手段は、監視に基づいて制御動作をとるようにさらに構成できる。例えば、制御手段は、装置に対する新しい認証子を要求し、警告を出し、装置によるホストへのアクセスを防止し、装置による少なくとも１つの他のホストへのアクセスを防止し、装置によるホストへのアクセス又は少なくとも１つの他のホストへのアクセスを制限し、及び／又は少なくとも１つの認証子に基づいて確立された通信セッションの長さを制御する。

【００９８】

制御手段は、装置とホスト間の暗号化された通信を傍受するように構成された中間装置に含めることができる。中間装置は、データ監査システムの少なくともいくつかの機能を提供してもよい。

【００９９】

制御手段は、決定したホストのタイプに応じてセキュリティ装置から認証子を選択的に要求するように構成できる。制御手段は、決定したホストのタイプに応じて、セキュリティ装置から受信した少なくとも１つの認証子を使用するかを決定できる。制御手段は、複数の認証子から１つの認証子を選択してもよいし、セキュリティ装置から受信した複数又は全ての認証子を１以上のホストに送信してもよい。制御手段は、ホストへのアクセス要求に応答して、ホストのタイプを判定し、ホストがクラウドホストであると判定したことに応答して証明書を使用し、ホストがレガシーホストであると判定したことに応答してプリンシパルキーペアを使用してもよい。

【０１００】

中間装置は、セキュリティ装置を用いて、ホストとホストへのアクセスを要求する装置との通信を可能にするためのインターフェース手段を備えることができる。装置は、ユーザ装置と通信するための第１のインターフェース手段と、アクセス要求の認証用の第２認証子を用いるアクセス要求は、第１のインターフェース手段を介してユーザ装置から受信することができ、セキュリティ装置から認証子を要求する第２のインターフェース手段と、ホストと通信するための第３のインターフェース手段とを含む。

【０１０１】

制御手段は、一時的認証子を作成及び／又は取り出すことができる。一時的認証子を格納するためのメモリ手段を設けることもできる。制御手段は、アクセス要求の受信に応答して、メモリ手段から一時的認証子を取り出すことができる。

【０１０２】

一時的認証子は、公開鍵を含むことができる。一時的認証子に応答して作成された証明書又は別の認証子は、一時的認証子の公開鍵部分の少なくとも一部を含むことができる。認証子は、一時的なキーペア及び少なくとも１つのより永続的な認証子の使用に基づくことができる。

【０１０３】

様々な実施形態及びそれらの組み合わせ又は下位区分は、方法、装置、又はコンピュータプログラム製品として実装されてもよい。一態様によれば、少なくともいくつかの機能は、仮想化された環境において提供される。同様に実行するためのコンピュータプログラムコードをダウンロードする方法も提供されてもよい。コンピュータプログラム製品は、非一時的なコンピュータ可読媒体に格納できる。例えば、メモリチップ、プロセッサ内に実装されたメモリブロック、ハードディスク又はフロッピーディスクなどの磁気媒体、及び例えばＤＶＤなどの光学媒体、及びそのデータの変形例であるＣＤ、磁気ディスク、又は半導体メモリなどに格納できる。方法ステップは、プロセッサ及びメモリを使用してコンピュータに方法ステップを実行させるように動作可能な命令を使用して実装できる。命令は、メモリ又は不揮発性記憶装置などの任意のコンピュータ可読媒体に格納されてもよい。

【０１０４】

必要なデータ処理装置は、１つ又は複数のデータプロセッサによって提供されてもよい。上述した各機能は、別々のプロセッサ又は統合プロセッサによって提供されてもよい。データプロセッサは、ローカル技術環境に適した任意のタイプであってもよく、非限定的な例として、汎用コンピュータ、専用コンピュータ、マイクロプロセッサ、デジタル信号プロセッサ（ＤＳＰ）、特定用途向け集積回路（ＡＳＩＣ）、ゲートレベル回路及び、マルチコアプロセッサアーキテクチャベースのプロセッサを含む。データ処理は、いくつかのデータ処理モジュールに分散させることができる。処理及び／又はホストの少なくとも一部は、仮想化された環境に提供できる。

【０１０５】

データプロセッサは、例えば、少なくとも１つのチップによって提供されてもよい。メモリ（複数可）は、ローカル技術環境に適した任意のタイプであってもよく、半導体ベースのメモリ装置、磁気メモリ装置及びシステム、光メモリ装置及びシステム、固定メモリ及びリムーバブルメモリなどの任意の適切なデータ記憶技術を用いて実装されてもよい。

【０１０６】

一般に、様々な実施形態は、ハードウェア又は専用回路、ソフトウェア、ロジック、又はそれらの任意の組み合わせで実装されてもよい。本発明のいくつかの態様は、ハードウェアで実装されてもよく、他の態様は、コントローラ、マイクロプロセッサ又は他のコンピューティング装置によって実行されるファームウェア又はソフトウェアで実装されてもよいが、本発明はそれらに限定されない。本発明の様々な態様は、ブロック図、フローチャート、又はその他の図的表現を使用して例示及び説明されているが、本明細書に記載されたこれらのブロック、装置、システム、技法又は方法は、以下において様々な組み合わせを含み、例として、ハードウェア、ソフトウェア、ファームウェア、専用回路又はロジック、汎用ハードウェア又はコントローラ又は他のコンピューティング装置、又はそれらのいくつかの組み合わせを含むが、それらに限定されない。

【０１０７】

融通が利くクラウド環境向けに、集中化されたスケーラブルなアクセス管理ソリューションを提供できる。アクセス権の更新は即時に行うことができる。ホスト単位の変更は不要である。特定の態様は、対話型及び非対話型（マシン間）の両方の接続をサポートする。

【０１０８】

特定のアプリケーションでは、プロキシ又はＣＡプロキシサービスを提供することもできる。ＣＡプロキシは、ターゲットホストで実行される。プロキシは、「オンデマンドサーバベースの認証」の事例で使用して、ユーザの公開鍵をキャッシュし、ＣＡ通信を管理できる。ＣＡ通信を管理するための「オンデマンドユーザプロビジョニング」の事例で使用される。

【０１０９】

ＮＳＳ（Ｎａｍｅ　Ｓｅｒｖｉｃｅ　Ｓｗｉｔｃｈ）サービスは、特定の実施形態において、ターゲットホストに対するネットワークユーザ情報を提供する。ＮＳＳサービスは、標準の「ｐａｍ＿ｍｋｈｏｍｅｄｉｒ」ＰＡＭモジュールとともに「オンデマンドユーザプロビジョニング」を実装している。Ｏｒｄａｉｎ　ＮＳＳサービス及びＰＡＭモジュールは、ターゲットホストにオンデマンドのユーザプロビジョニングを提供する。

【０１１０】

状況によっては、ＳＳＯエージェントも提供される場合がある。ＳＳＯエージェントを使用して、非対話型シングルサインオン機能を実装し、非ユーザ特権で実行し、例えばユーザ認証情報を提供するための共有された秘密に基づいて認証局（ＣＡ）との信頼関係を確立できる。

【０１１１】

可能性として、傍受監査装置の異なる構成を使用することができる。これらには、要塞モード、ルータモード、ブリッジモードなどがある。監視装置は、ＣＡクライアント（ＳＳＨエージェント）機能を組み込んでいるので、発行されたユーザ証明書を確認できる。ユーザ証明書には、ＳＳＨ固有の拡張機能を使用して注釈を付けることができるため、ＣＡとＣｒｙｐｔｏ　Ａｕｄｉｔｏｒはより細かいポリシーを適用できる。例えば、Ｃｒｙｐｔｏ　Ａｕｄｉｔｏｒは、認証証明書の期限が切れた後にユーザのＳＳＨセッションを終了する。また、証明書は、ＳＳＨポート転送オプションが許可されているプロトコルとポート番号レベルを記述できる。証明書は、Ｃｒｙｐｔｏ　Ａｕｄｉｔｏｒパケット処理エンジンによって実装される詳細なセッション監査パラメータを記述できる。

【０１１２】

上述の様々な態様及び特徴は、図面によって及び／又は上記には具体的に示されていない方法で組み合わせることができる。

【０１１３】

前述の説明は、例示的かつ非限定的な例として、本発明の例示的な実施形態及び態様の完全かつ情報提供の説明を提供する。しかしながら、添付の図面及び添付の特許請求の範囲と併せて読めば、上記説明を考慮して、当業者には、本開示の精神及び範囲内に入る様々な変更及び適応が明らかになるであろう。

【図面】

【図１】

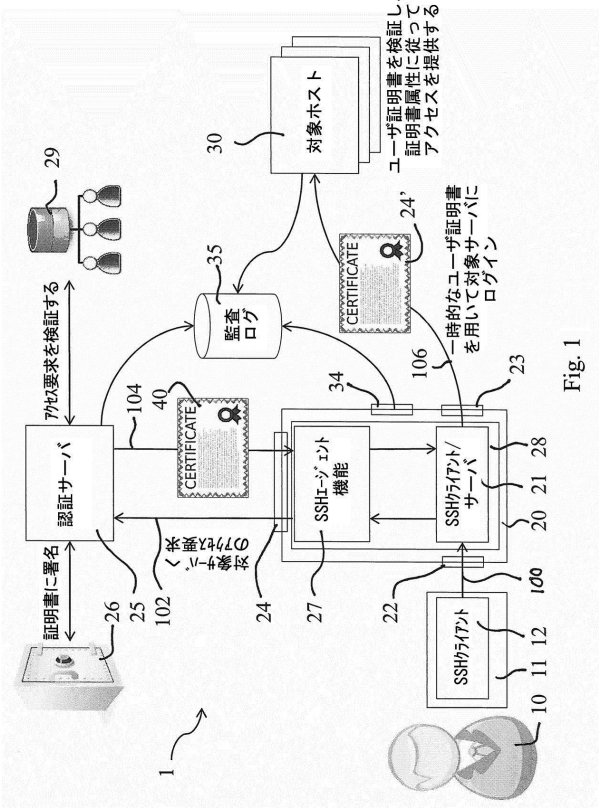

Fig. 1

【図２】

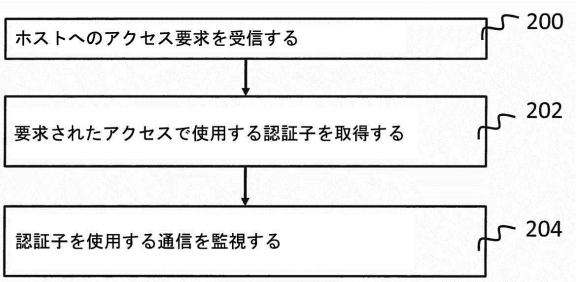

Fig. 2

【図３】

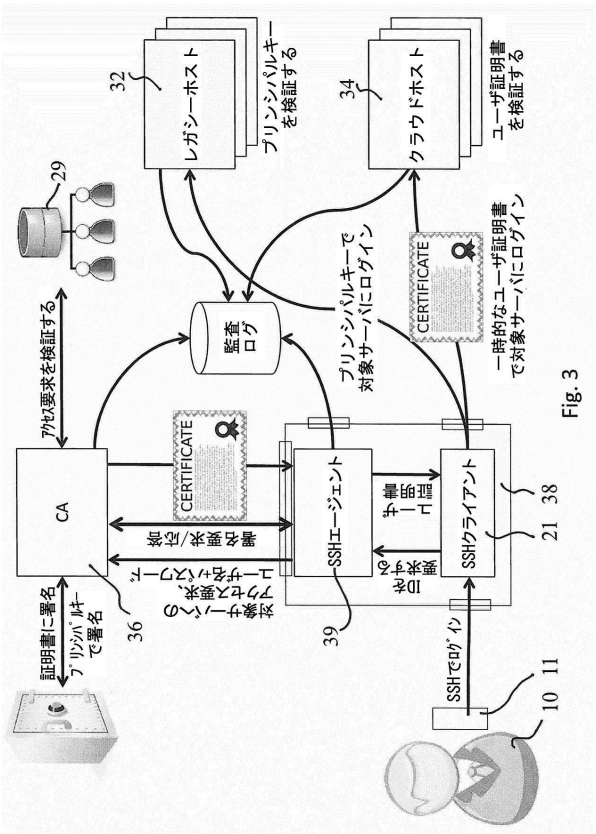

Fig. 3

【図４】

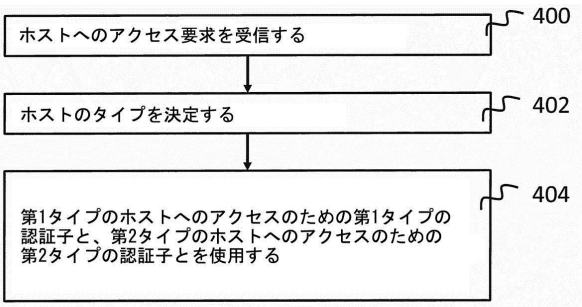

Fig. 4

【図５ａ】

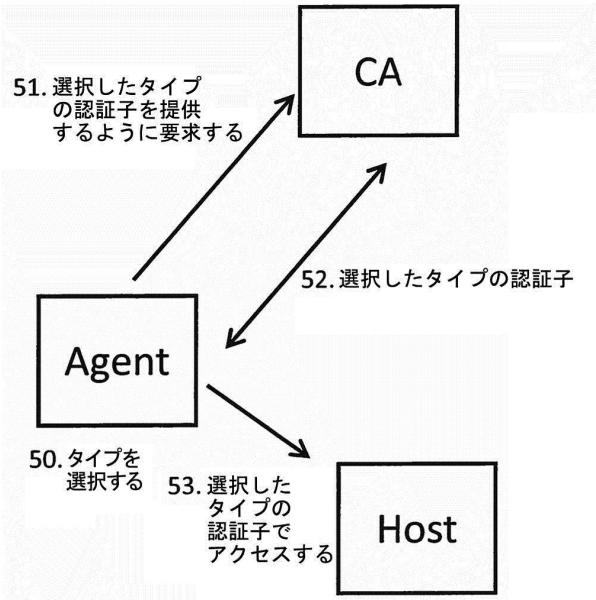

Fig. 5a

【図５ｂ】

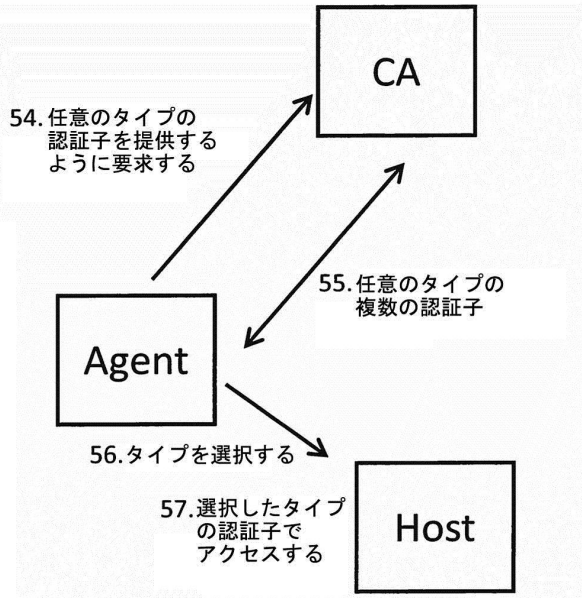

Fig. 5b

【図５ｃ】

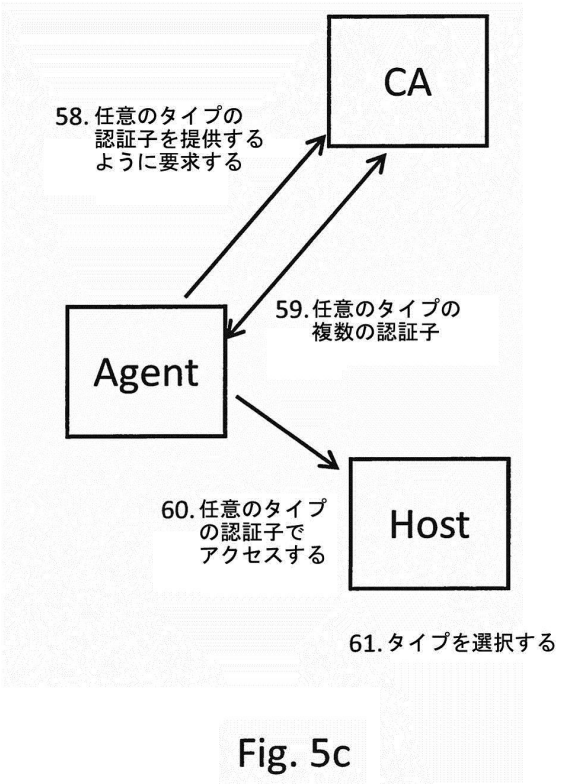

Fig. 5c

【図６】

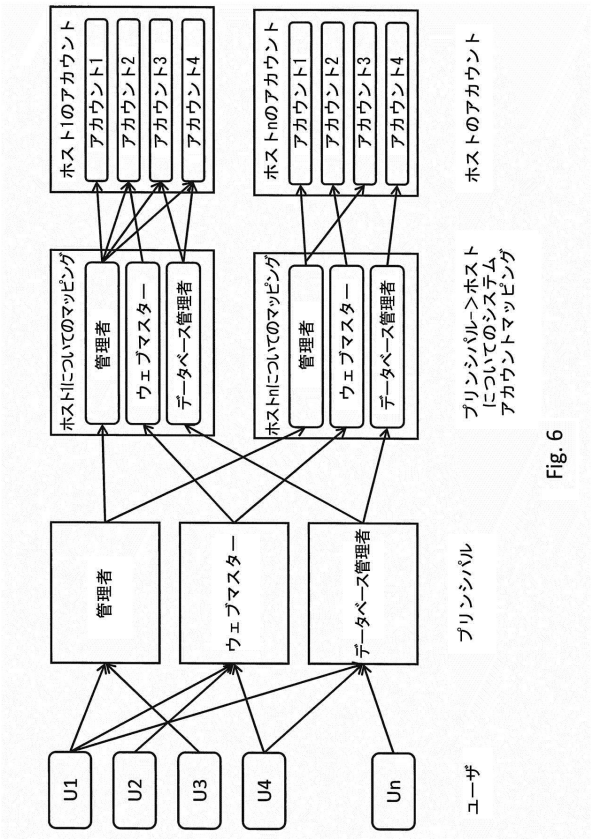

Fig. 6

【図７】

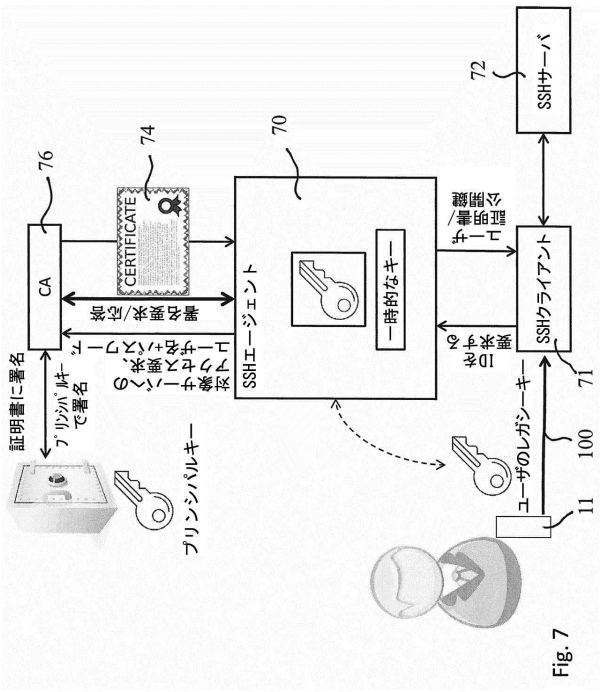

Fig. 7

【図８】

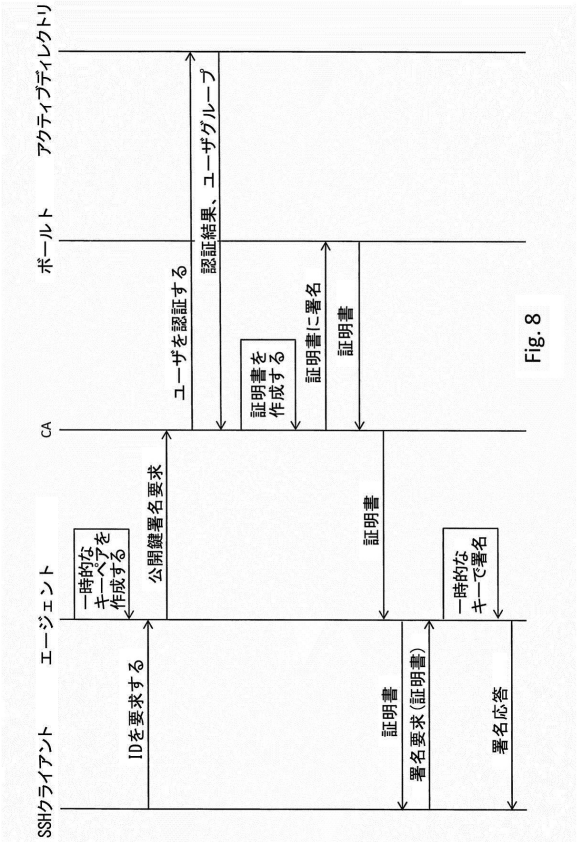

Fig. 8

【図９】

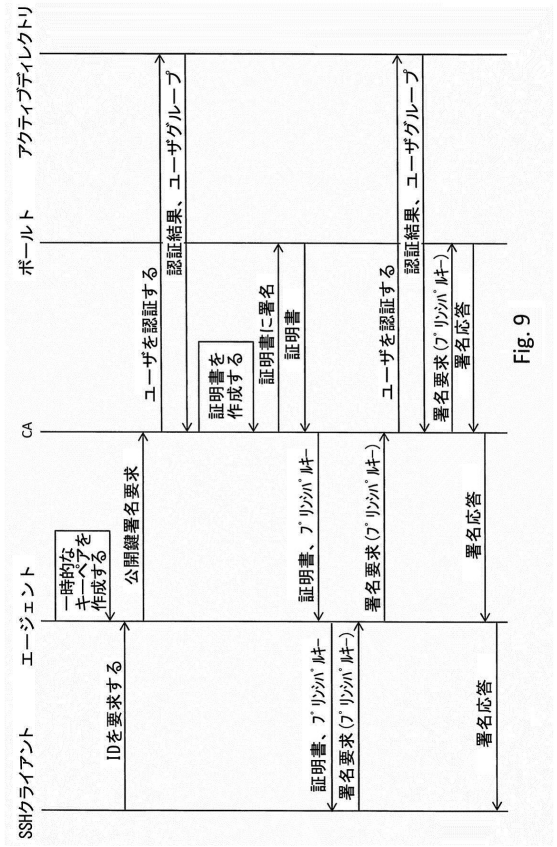

Fig. 9

【図１０】

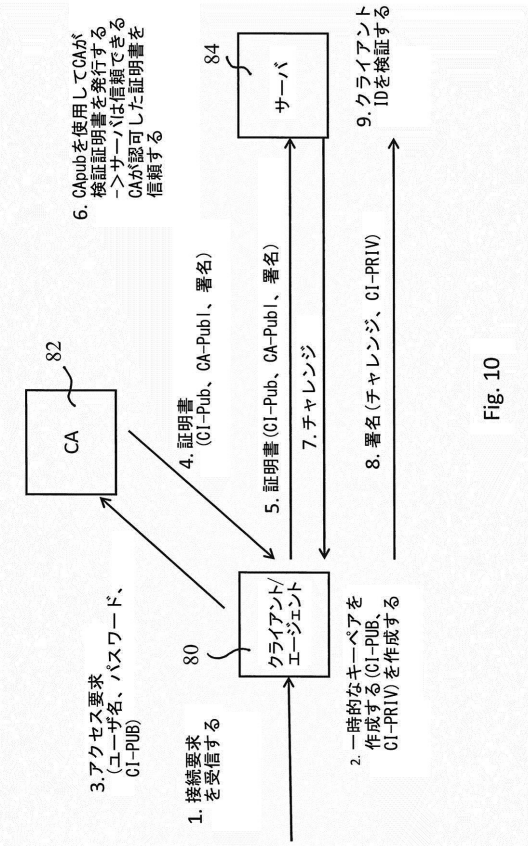

Fig. 10

【図１１】

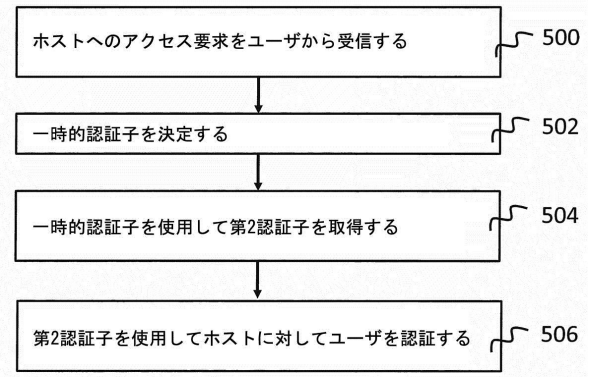

Fig. 11

【図１２】

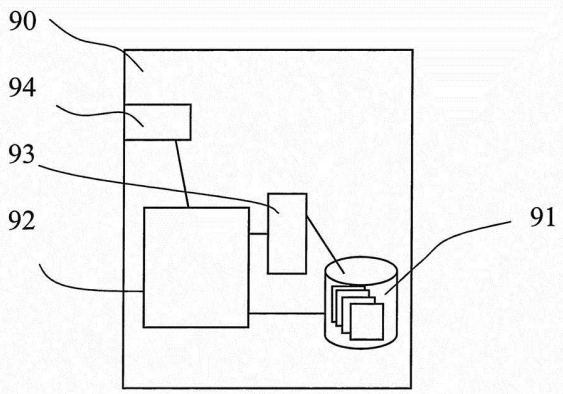

Fig. 12

フロントページの続き

(51)国際特許分類　　FI
　　G06F　21/33

(72)発明者　マルック ロッシ
　　フィンランド国，０４４３０ ヤルベンパー，キビオヤンティエ ３ ベー ２

審査官　青木 重徳

(56)参考文献　特表２００９－５３３９４５（ＪＰ，Ａ）
　　特開２００５－０８５１０２（ＪＰ，Ａ）
　　特開２０１０－１９２９４７（ＪＰ，Ａ）
　　特開２００８－００５４３４（ＪＰ，Ａ）
　　米国特許第０６３６７００９（ＵＳ，Ｂ１）
　　米国特許出願公開第２０１３／００８１１３２（ＵＳ，Ａ１）

(58)調査した分野　(Int.Cl.，ＤＢ名)
　　Ｈ０４Ｌ　９／３２
　　Ｈ０４Ｌ　９／０８
　　Ｇ０９Ｃ　１／００
　　Ｇ０６Ｆ　２１／３３