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

特許第4434319号
(P4434319)

(45)発行日　平成22年3月17日(2010.3.17)　(24)登録日　平成22年1月8日(2010.1.8)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675A
G06F 13/00	(2006.01)	G06F	13/00	354Z
G06F 21/20	(2006.01)	G06F	15/00	330A
H04L 9/08	(2006.01)	H04L	9/00	601A
		H04L	9/00	601E

請求項の数 27　(全 21 頁)

(21)出願番号	特願平10-535814
(86)(22)出願日	平成10年2月11日(1998.2.11)
(65)公表番号	特表2001-511982(P2001-511982A)
(43)公表日	平成13年8月14日(2001.8.14)
(86)国際出願番号	PCT/US1998/002211
(87)国際公開番号	WO1998/036522
(87)国際公開日	平成10年8月20日(1998.8.20)
審査請求日	平成17年2月14日(2005.2.14)
(31)優先権主張番号	08/799,402
(32)優先日	平成9年2月12日(1997.2.12)
(33)優先権主張国	米国(US)

(73)特許権者
ベリゾン　ラボラトリーズ　インコーポレイテッド
アメリカ合衆国　１９８０１　デラウェア，ウィルミントン，オレンジ　ストリート　１２０９
(74)復代理人
アクシス国際特許業務法人
(74)代理人
弁理士　倉内　基弘
(72)発明者　シャムブルーム，ダブリュー．デイビッド
アメリカ合衆国　０２１７４－１４１１
マサチューセッツ，アーリントン，オーバールック　ロード　９６

最終頁に続く

(54)【発明の名称】秘密保持性の遠隔命令を実行するための方法

(57)【特許請求の範囲】

【請求項１】

ネットワークサーバを介してクライアントコンピュータからデスティネーションサーバに送られるメッセージのセキュリティを向上する方法であって、

（ａ）ネットワークサーバが前記クライアントコンピュータから少なくとも一つの認証要求を受信するステップと、

（ｂ）ネットワークサーバが前記クライアントコンピュータからデータを受信するための秘密保持性接続を設定するステップと、

（ｃ）ネットワークサーバが確認センタからのクライアント認証情報を含むクレデンシャルキャッシュを発生させるステップと、

（ｄ）ネットワークサーバが前記クレデンシャルキャッシュをクライアントコンピュータに伝送し、かつネットワークサーバから前記クライアント認証情報を消去するステップと、

（ｅ）ネットワークサーバが前記クラインアントコンピュータから前記クライアント認証情報を含む新規なクレデンシャルキャッシュおよび前記デスティネーションサーバに対する対応するメッセージを受信するステップと、

（ｆ）ネットワークサーバが前記クライアント認証情報および秘密保持性認証プロトコルを使用して、前記確認センタから前記デスティネーションサーバにアクセスするための許可データを獲得するステップと、

（ｇ）ネットワークサーバが前記許可データおよび前記メッセージを前記デスティネーシ

ョンサーバに伝送するステップとを含むことを特徴とするセキュリティ向上方法。
【請求項２】
前記クライアントコンピュータからの前記認証要求に応答して、前記ネットワークサーバが実行する諸ステップであって、
前記クライアントコンピュータに、パブリック－プライベートキー対と関連するネットワークサーバキーおよび既知の暗号化アルゴリズムを伝送するステップと、
前記クライアントコンピュータから、前記暗号化アルゴリズムおよび前記ネットワークサーバキーを使用して暗号化されたセッションキーを受信するステップと、
前記既知の暗号化アルゴリズムおよび前記セッションキーを使用して暗号化されたクライアント情報を送出して前記クライアントコンピュータに対してネットワークサーバを認証するステップとを含む請求項１記載の方法。
【請求項３】
前記ネットワークサーバが秘密保持性ソケット層（ＳＳＬ）を使用して秘密保持性接続を設定する請求項１記載の方法。
【請求項４】
前記クレデンシャルキャッシュを発生させるステップが、
（ａ）前記クライアントコンピュータの代わりに許可指示の要求を前記確認センタに送るステップと、
（ｂ）前記確認センタから前記許可指示を受信するステップと、
（ｃ）前記許可指示を前記クレデンシャルキャッシュに記憶するステップとを含む請求項１記載の方法。
【請求項５】
前記許可指示を受信するステップが、ＤＥＳシンメトリックシークレットキーベースの認証プロトコルを使用して遂行される請求項４記載の方法。
【請求項６】
前記クレデンシャルキャッシュを発生させるステップは、ケルベロス（Kerberos）プロトコルを使用して獲得されるクライアント認証情報を用いる請求項１記載の方法。
【請求項７】
前記クレデンシャルキャッシュを発生させるステップが、次の諸ステップ、すなわち
（ａ）既知の暗号化アルゴリズムとユーザキーを使用して暗号化されたセキュリティセッションキーを受信するステップと、
（ｂ）前記クライアント認証情報から前記ユーザキーを生成するステップと、
（ｃ）前記ネットワークサーバにて前記既知のアルゴリズムを使用して前記セキュリティセッションキーを解読して、前記セキュリティセッションキーおよび前記許可指示を獲得するステップとを含む請求項４記載の方法。
【請求項８】
前記クライアント認証情報からユーザキーを生成するステップがさらに、クライアントパスワードに適用されるワンウェイハッシュアルゴリズムにより遂行される請求項７記載の方法。
【請求項９】
前記クライアントコンピュータに前記クレデンシャルキャッシュを伝送するステップがさらに、該クレデンシャルキャッシュをコード化するステップを含み、該クレデンシャルキャッシュが前記セキュリティセッションキーおよび前記許可指示を含む請求項７記載の方法。
【請求項１０】
前記クレデンシャルキャッシュをコード化するステップが、ＡＳＣＩＩコード化により遂行される請求項９記載の方法。
【請求項１１】
前記クレデンシャルキャッシュをコード化するステップがさらに、ＵＲＬ－コード化の使用を含む請求項１０記載の方法。

【請求項１２】
前記デスティネーションサーバにアクセスするために許可データを獲得するステップがさらに、前記ネットワークサーバが実行する諸ステップであって、
（ａ）前記確認センタに前記許可指示を伝送するステップと、
（ｂ）許可指示が、確認センタから先に受信されたのと同じ許可指示であることを前記確認センタにより認証された場合、アクセス指示を受信するステップとを含む請求項１１記載の方法。
【請求項１３】
前記許可データを使用してデスティネーションサーバにアクセスするため、前記クライアントコンピュータの授権を確認するステップを含む請求項１記載の方法。
【請求項１４】
前記デスティネーションサーバにアクセスするために前記クライアントコンピュータの授権を確認するデスティネーションサーバのステップがさらに、
（ａ）前記メッセージを前記デスティネーションサーバに伝送する加入者が、前記アクセス指示を受信するためにキー分配センタにより認証プロトコルを使用して認証された者と同じ加入者であることを認証するステップと、
（ｂ）前記クライアントコンピュータがデスティネーションサーバにアクセスすることを授権されたか否かをアクセス制御規準に基づいて判断するステップとを含む請求項１３記載の方法。
【請求項１５】
（ａ）ネットワーク接続を介してコマンドを発行する第１コンピュータサーバと、
（ｂ）秘密保持性接続によって前記第１コンピュータサーバに接続される第２コンピュータサーバにして、前記第１コンピュータサーバに関する認証要求を発生させるとともに、該認証要求に応答して受信したクライアント認証情報を含むクレジデンシャルキャッシュを発生させる認証デバイスをさらに有し、かつ、前記クレジデンシャルキャッシュを第１コンピュータサーバに伝送するとともに、前記クライアント認証情報を消去する第２コンピュータサーバと、
（ｃ）前記ネットワークを介して前記第２コンピュータサーバに応答しかつ前記認証要求を受信できる第３コンピュータサーバにして、前記認証要求に応答して、前記第１コンピュータサーバのアイデンティティを認証し、そして前記第１コンピュータサーバに関する認証指示情報を前記第２コンピュータサーバに送る第３コンピュータサーバと、
（ｄ）前記ネットワークに操作可能に接続される第４コンピュータサーバにして、前記第２コンピュータサーバが該第４コンピュータサーバに認証指示情報を伝送して前記第１コンピュータサーバを認証する場合、前記コマンドを受信して実行し得る第４コンピュータサーバと
を備えることを特徴とするコンピュータシステム。
【請求項１６】
非秘密保持性ネットワークを介して、クライアントコンピュータからネットワークサーバを経てデスティネーションサーバに送られるメッセージに対するセキュリティを改善したコンピュータシステムであって、
（ａ）前記クライアントコンピュータと前記ネットワークサーバ間に秘密保持性のネットワーク接続を設定するための手段と、
（ｂ）ネットワークサーバにて、秘密保持性の態様で確認センタからクライアント認証情報を獲得するとともに、クレデンシャルキャッシュを生成するための手段と、
（ｃ）前記クライアント認証情報を含む前記クレジデンシャルキャッシュを前記ネットワークサーバから前記クライアントコンピュータに伝送するとともに、該ネットワークサーバから前記クライアント認証情報を消去するための手段と、
（ｄ）前記メッセージおよび前記クライアント認証情報を前記クライアントコンピュータから前記ネットワークサーバに伝送するための手段と、
（ｅ）秘密保持性認証プロトコルを使用して前記非秘密保持性ネットワークを介して前記

確認センタから前記デスティネーションサーバにアクセスするための許可を獲得するための手段と
を備えることを特徴とするコンピュータシステム。
【請求項１７】
前記デスティネーションサーバにて、前記メッセージを使用して前記デスティネーションサーバにアクセスするために前記クライアントコンピュータの授権を確認するための手段と、
前記クライアントコンピュータの授権が確認された場合、前記メッセージで前記デスティネーションサーバにアクセスするための手段と
を備える請求項１６記載のコンピュータシステム。
【請求項１８】
前記秘密保持性のネットワーク接続を設定するための手段がＳＳＬプロトコルを含む請求項１６記載のコンピュータシステム。
【請求項１９】
前記クライアント認証情報を獲得するための手段が、ケルベロスプロトコルを含む請求項１６記載のコンピュータシステム。
【請求項２０】
（ａ）秘密保持性ネットワーク接続を介してクライアントコンピュータからクライアント識別情報を受信するためのクライアントネットワークインターフェースと、
（ｂ）ネットワーク接続を介する確認センタおよびクレデンシャルキャッシュを生成するための手段とクライアント認証情報および許可付与データを交換するための許可付与ネットワークインターフェースと、
（ｃ）前記確認センタから受信される前記クライアント認証情報を含む前記クレデンシャルキャッシュを、該クライアント認証情報を保持することなく、前記クライアントコンピュータに伝送するための手段と、
（ｄ）デスティネーションコンピュータと操作可能に通信するためのデスティネーションコンピュータネットワークインターフェースであって、前記クライアントコンピュータから受信するクライアント認証情報および前記確認センタから受信する許可付与データをネットワーク接続を介して前記デスティネーションコンピュータに伝送するためのデスティネーションコンピュータネットワークインターフェースと
を備えることを特徴とするネットワークコンピュータサーバ。
【請求項２１】
前記クライアントネットワークインターフェースがさらに、
（ａ）前記クライアントコンピュータから認証要求を受信するためのウェブサーバと、
（ｂ）既知の暗号化アルゴリズムのパブリック－プライベートキー対と関連するキーを含むネットワークサーバキーデータベースと、
（ｃ）前記クライアントコンピュータにより生成され、前記パブリック－プライベートキー対のパブリックキーと前記既知の暗号化アルゴリズムを使用して暗号化されるクライアント生成セッションキーを解読するためのデクリプタと、
（ｄ）前記クライアント生成セッションキーと前記暗号化アルゴリズムを使用して認証メッセージを暗号化できるエンクリプタと
を含む請求項２０のネットワークコンピュータサーバ。
【請求項２２】
前記クライアント認証情報を前記クライアントコンピュータから受信するために通されるネットワーク接続が、秘密保持性ソケット層（ＳＳＬ）プロトコルを使用することにより秘密保持される請求項２０記載のネットワークコンピュータサーバ。
【請求項２３】
前記許可付与ネットワークインターフェースが、ケルベロス認証プロトコルを使用することによって秘密保持される請求項２０記載のネットワークコンピュータサーバ。
【請求項２４】

ネットワークサーバを介してクライアントコンピュータからデスティネーションサーバに送られるメッセージのセキュリティを向上する方法であって、
（ａ）ネットワークサーバがクライアント識別情報および秘密保持性認証プロトコルを使用して、確認センタからクライアント認証情報を獲得するステップと、
（ｂ）ネットワークサーバが前記クライアント認証情報を含むクレデンシャルキャッシュを前記クライアントコンピュータに伝送するステップと、
（ｃ）ネットワークサーバが前記クライアント認証情報を消去するステップと、
（ｄ）ネットワークサーバが前記クライアントコンピュータから前記クレデンシャルキャッシュおよび前記デスティネーションサーバに対するメッセージを受信するステップと、
（ｅ）ネットワークサーバが前記クレデンシャルキャッシュおよび秘密保持性認証プロトコルを使用して、前記確認センタから前記デスティネーションサーバにアクセスのための許可データを獲得するステップと、
（ｆ）ネットワークサーバが前記許可データおよび前記メッセージを前記デスティネーションサーバに伝送するステップと
を含むことを特徴とするセキュリティ向上方法。
【請求項２５】
ネットワークを介してクライアント、確認センタおよびに応答するコンピュータサーバであって、
クライアント識別情報および秘密保持性認証プロトコルを用いて前記クライアントの代わりに前記確認センタからクライアント認証情報を獲得するための手段と、
前記クライアント認証情報を含むクレデンシャルキャッシュを前記クライアントに伝送する手段と、
前記ネットワークサーバから前記クライアント認証情報を消去するための手段と、
前記クライアントから前記クレデンシャルキャッシュおよび前記デスティネーションサーバに対するメッセージを受信するための手段と、
前記クレデンシャルキャッシュおよび秘密保持性認証プロトコルを用いて、前記確認センタから、前記クライアントの代わりに前記デスティネーションサーバにアクセスするための許可データを獲得するための手段とを備えたコンピュータサーバ。
【請求項２６】
ネットワークトランザクションのセキュリティを改善する方法であって、
（ａ）サーバがクライアントからデータを受信するための秘密保持性接続を確立するステップと、
（ｂ）サーバが該サーバの外部の源からのクライアント認証情報を含むクレデンシャルキャッシュを生成するステップと、
（ｃ）サーバが前記クレデンシャルキャッシュを前記クライアントに伝送するステップと、
（ｄ）サーバが前記クライアント認証情報を該サーバから消去するステップとを含む方法。
【請求項２７】
（ｅ）サーバが前記クレデンシャルキャッシュを前記クライアントから受信するステップと、
（ｆ）サーバが前記クライアント認証情報を用いて、前記クライアントの代わりにデスティネーションサーバにアクセスするための許可データを獲得するステップと、
（ｇ）サーバが前記許可データ及びメッセージを前記デスティネーションサーバに伝送するステップとをさらに含む請求項２６記載の方法。
【発明の詳細な説明】
［発明の分野］
本発明は、非秘密保持性ネットワークを使用するコンピュータ間におけるデータ伝送のセキュリティを改良する技術に関し、特定すると、クライアントからネットワークサーバへ、ついでデスティネーションサーバへ、あるいはデスティネーションサーバからネットワ

ークサーバへ、ついで分散コンピュータシステムの一部としてのクライアントへ伝送されるメッセージの完全性およびセキュリティを改善するための方法およびシステムに関する。

［発明の背景］

分散コンピュータシステムは、相互接続された複数の別個のコンピュータを含む。汎用の分散システムの一つの簡単な例は、ネットワークを介して相互接続される数個のワークステーションおよびサーバを含むネットワークドシステムである。ネットワークは、複数の組織が情報およびリソースを共有することを可能にするから普及している。さらに、ネットワークドシステムにおいては、もしも一つのコンピュータが破損、ないしクラッシュしても、他のコンピュータが動作し続ける。

相互接続の態様の形式、コストおよび信頼性は、ネットワークドシステムにおける重要な考慮事項である。比較的短い距離を介しての大型のネットワークは、普通イーサネットまたはトークンリンクのようなローカルエーリヤネットワーク（ＬＡＮ）を使用するが、これは１または複数のワイヤ上の多数の異なるコンピュータ間の通信を可能にする。モデムの使用は、広い領域にわたるコンピュータネットワークを創成せしめる。何故ならば、接続は電話ラインのようなデータリンクを介してなされ得るからである。広域エーリヤネットワーク（ＷＡＮ）は、普通、マイクロウェーブリンクのようなオプチカルファイバおよび導線電話ラインやサテライトの組合せを使用して、数個の小型のＬＡＮを接続する。ネットワークのネットワークは、インターネットワークとして言及されることが多い。

コンピュータネットワーク特にインターネットワークは、セキュリティ違反に犯されやすい。ネットワーク内の各要素のセキュリティの程度は異なる。これは、一部には、各エンティティが、種々の層の物理的および動作上のセキュリティにより保護され得るからである。さらに、インターネットワーク内の各要素またはネットワークは、そのセキュリティの実施が大幅に異なる異なる組織により所有ないし制御されることがあり得る。コンピュータ間の相互接続も、同様に非秘密保持性であることがある。ネットワークのある部分は電話線またはマイクロウェーブリンクのような物理的に非秘密保持性のリンクを使用することがあるから、ハッカーや無免許者が、電話ラインを介しての通信を盗聴ないし傍受し、彼らの希望に従ってそれらを変更したり後での使用のためそれらを複写したりすることがある。ログインやコマンド情報を複写した無免許者は、その情報を利用して、ネットワーク上の他のコンピュータにアクセスする潜在性を有する。

ネットワークセキュリティは、普通、３つの一般的概念に基づく。診断ルーチンを実行したり遠隔的ログインを遂行したりするような動作をなせという各要求に対して、ネットワークは、（１）要求を認証し、（２）アクセス制御規準によりアクセスを制御し、そして（３）非授権者の使用を検出するために各要求を検査する。

認証は、授権者のユーザが要求を指示したこと、および要求がデスティネーションへの行程上で無免許者により不正に変更されなかったことを決定するプロセスである。認証の一つの一般的な例は、ログイン時におけるパスワードの使用である。ユーザからユーザ名およびパスワードを受け取ると、ホストコンピュータは、そのパスワードをアクセス制御ファイル内の授権ユーザ名のリストと比較し、もしもパスワードがユーザ名と関連するパスワードと一致すれば、ホストコンピュータはアクセスを許容する。しかしながら、上述の状況においては、ユーザとホストが秘密保持接続を介して通信していることが仮定される。そうでないと、無免許者がユーザからホストへの通信を傍受し、ユーザ名とパスワード情報を盗むことがあり得る。無免許者は、盗まれたユーザ名およびパスワード情報を使用することによって後刻ホストに不法にアクセスすることができよう。

複数の相互接続コンピュータを含むネットワークドシステムにおいては、第１のコンピュータが、中間のサーバを介して第２のサーバすなわちデスティネーションサーバからサービスを要求することがあり得る。第１コンピュータは、普通クライアントと称される。デスティネーションサーバからサービスを受けるために、クライアントは、デスティネーションサーバに対して自らを認証することによって開始しなければならない。しかしながら、クライアントは、非秘密保持性のラインを介してデスティネーションサーバと通信して

いようから、単純に明文でパスワードを送ることができない。その代わり、クライアントとデスティネーションサーバは、複数の質問と応答の交換で接触して、認証プロセスを構成し、これで、要求中のクライアントが授権ユーザであることをデスティネーションサーバに納得させることとなろう。
従来技術は、クライアントをこのようなサーバに対してそのように認証するために使用できる暗号ベースの認証プロセスの諸例を含んでいる。このような認証プロセスは、パブリックキーまたはシークレットキー暗号化システムのいずれかに基づくことができる。代表的な、シークレットキー認証方式においては、各授権加入者が、その加入者のみが知っており、信頼された第３の加入者または認証サーバに登録されたシークレットキーを所持している。認証サーバは、登録されたユーザおよびシークレットキーのリストを維持しており、それゆえ、物理的に秘密保持性でなければならない。これに対して、パブリック認証方式においては、各ユーザはパブリックキーとプライベートキーを有している。パブリックキーは提示され、プライベートキーはそのユーザにのみ既知である。パブリックキー認証システムを使用しての認証は、秘密保持認証サーバを必要としないから魅力的である。
シークレットキーベースのネットワーク認証方式の１例は、Kerberos（ケルベロス）と称される信頼された第３加入者認証サービスである。認証を必要とするネットワークサービスおよびクライアントは、Kerberosに登録し、シークレットキーを受け取る。ここで、キー（またはキーが誘導されるパスフレーズ）は、ユーザおよびKerberosホストサーバにのみ知られている。Kerberosはまた、一時的なセッションキーを発生するが、このキーは二つの登録されたKerberos主体（ユーザまたはホスト）間においてメッセージを暗号化するのに使用できる。代表的なKerberosソフトウェアパッケージは、Massachusetts Institute of Technorogy（ＭＩＴ）のProject Athenaから出ているKerberos Version 5である。Kerberos認証方式はまた、J.KohlおよびC.Neumanの「The Network Authentication Service（V5）,Request for Comments: 1510」（1993年9月）に論述されている。Kerberosと第３の信頼加入者の個人認証方式は、２主体間によりスピーディーな秘密保持性のアクセスを許容し得る。
他の従来の方式は、ネットワークセキュリティの問題を取り扱うために開発された。例えば、２種の認証プロトコル、Secure Sockets Layer（SSL）およびSecure Hyper Text Transfer Protocol（S-HTTP）が、特に、暗号化を使用することによってインターネットを横切って伝送される情報を保護するように設計された。クライアントとデスティネーションサーバーは両者とも，ＳＳＬをサポートしなければならない。ＳＳＬはアプリケーションに無関係であり、トランスポート層で動作し、それがHTTP，ftg，telnet，gopher，Network News Transport Protocol（NNTP）およびSimple Mail Transport Protocol（SMTP）で動作することを意味する。ＳＳＬは、クライアントとサーバー間の認証および暗号化ルーチンを処理するために数種の暗号化アルゴリズムをサポートする。
Ｓ－ＨＴＴＰは、ＨＴＴＰの秘密保持に関する拡張部であり、World Wide Webの通信プロトコルである。Ｓ－ＨＴＴＰは、Enterprise Integration Technologiesにより開発された公的に利用可能なプロトコルである。ＳＳＬと異なり、Ｓ－ＨＴＴＰは、ＨＴＴＰプロトコルに、より密接に関係づけられる。また、ＳＳＬは、普通クライアントおよびサーバー間の通信リンクを暗号化するが、Ｓ－ＨＴＴＰは、各メッセージを個々に暗号化できる。Ｓ－ＨＴＴＰ下におけるクライアント／サーバートランザクションにおいて、クライアントはパブリックキーを所持することを要しない。秘密保持性のトランザクションは、任意の時点に行うことができる。何故ならば、Ｓ－ＨＴＴＰメッセージの送信者は、その優先暗号をメッセージとともに送るからである。
分散システムの開発における現在の傾向は、管理されたホストの技術思想である。被管理ホストシステムにおいては、クライアントはネットワークサーバにアクセスし、ネットワークサーバを介して、第２のサーバにアクセスを要求する。このサーバは遠隔ホストまたは被管理ホストと称され得る。より大型のネットワークにおいては、ネットワークサーバは、多数のクライアントが多数のデスティネーションサーバにアクセスするための出入り口兼代理人として動作している。クライアントからデスティネーションサーバへのトラン

ザクションが秘密保持性であるようにするためには、クライアントとネットワークサーバ間のトランザクションおよびネットワークサーバとデスティネーションサーバ間のトランザクションが、ネットワーク認証プロセスにより保護されるべきことである。
証明書ベースの認証方式においては、相互に通信することを希望する全エンティティは、証明局と称される第３の加入者に登録されねばならない。証明局は、登録する加入者のアイデンティティを確認し、証明書を発行する。加入者は、それを使用して他の登録された加入者に対して自己を認証する。例えば、IBM’s World RegistryおよびSun Microsystem’s SunCAを含め、適当な認証証明書を提供する多くの証明局が存在する。
クライアントとネットワークサーバ間のトランザクションおよびネットワークサーバとデスティネーションサーバ間のトランザクションを保護するために、単に１形式の認証プロセスを使用することと関連して多くの問題が存在する。このシステムの使用は、例えば、ネットワークサーバ、全クライアントおよび全デスティネーションサーバが、究極的に同じトップレベルの証明局に対して追跡可能な証明書を所持することを要する。さらに、クライアントシステムの各個々のユーザに、クライアント証明書が発行されねばならない。もしもクライアントの証明書が、個々のワークステーションに蓄積されているとしたら、クライアントは、特定のワークステーションのみを使用することに限定されるであろう。もしもクライアント証明書が、ディスケットのような携帯用媒体上に蓄積されていたとすると、それらは損出や盗難を受け、全ネットワークシステムのセキュリティを減ずるであろう。さらに、クライアントワークステーションは、ＵＮＩＸまたはＤＯＳのような種々の異なるオペレーティングシステムをランする、ＰＣまたはＭａｃｌｎｔｏｓｈのような多数の異なるハードウェアデバイスを任意のものとし得、種々の全クライアントにより支持される単一の媒体はない。要約すると、クライアントとネットワークサーバ間の証明書認証システムの使用は、支持するのが管理的に難しい。
全トランザクションに対してKerberos認証方式が使用されると、各クライアントワークステーションは、キー分配センタと通信するのに必要なソフトウェアを所持することが要求される。この手法は、多くの種々のクライアントを支持するために多くの異なるバージョンのソフトウェアを提供するという問題を含む問題に遭遇する。
一つの認証方式がクライアントとネットワークサーバ間のトランザクションを保護するのに使用され、ネットワークサーバとデスティネーションサーバ間のトランザクションを保護するのに他の認証方式が使用されると、クライアントとデスティネーションサーバとの間のトランザクションにおいては、ネットワークサーバはクライアントに対する代理人として作用しなければならず、クライアントの認証を遂行するためにネットワークサーバを必要とすることが望ましくないことがしばしばあり得る。二つの異なる認証方式を使用することによって、クライアントは、デスティネーションサーバに対して自分自身を直接に認証することはしないであろうから、ネットワークサーバはクライアントサーバのアイデンティティおよびメモリを有するがごとくに作用することを要する。サーバーサーバトランザクションにおいては、ユーザは、普通、シェルプログラムを使用してネットワークサーバにログオンされる。シェルプログラムは、ネットワークサーバ上にレコードを作り、そしてネットワークサーバはユーザのアイデンティティおよび使用（すなわち日時）のレコードを維持する。ユーザがログオンされている限り、シェルログオンプログラムが存在する。これに対して、クライアント－被管理ホストトランザクションにおいては、シェルログオンプログラムはクライアントコンピュータ上においては生きているが、サーバ上には存在しない。代わりに、ネットワークサーバが、クライアントに代わってキー分配センタまたは認証サーバとインターフェースする。これをなすために、World Wide Webサーバとして構成されたネットワークサーバが、トランジェントプロセス（HTTP Common Gateway Interface（CGI）要求が実行された場合のように）を創成、実行し、キー分配センタに質問する。これらの一時的プロセスは、ある意味において、トランザクションの期間中ユーザのアイデンティティを仮定しなければならない。しかしながら、それらの機能が完了すると、これらのトランザクションプロセスは終了、消滅し、収集したかもしれないアイデンティティまたはセッション状態データを失うこととなる。

ネットワークサーバがクライアントによる処理を完了したときにクライアント上に何らの情報を維持しないと、サーバはステートレスとして記述される。ステートレスファイルサーバは、ファイルおよびファイル内における位置に関する情報を要求それ自体から誘導することによってクライアント情報を保持することを回避する。ステートフルサーバ（例えば、揮発性メモリにファイル情報を記録するもの）は、サーバが破損するとき情報を失う。加えて、クライアントがなくなるとき、サーバは、クライアントがトランザクションに必要とされる情報を維持するために割り当てられたスペースをもはや維持していないことおよびスペースを再要求できないかもしれないことに気ずかないかもしれない。これに対して、ステートレスサーバは、クライアントまたはサーバの破損に続いて、動作を続行するためには、クライアントからの最後の完全に自立の要求に応答すれば足りる。ＵＮＩＸ動作環境においては、ＵＮＩＸプロセス（例えばデーモン）はステートフルであることが時々ある。しかしながら、個々のトランジェントプロセスは永続的でなく、それゆえ状態情報を内部に維持できない。

それゆえ、複数のネットワークドコンピュータを含むトランザクションのセキュリティを増大し、インターネットのような非秘密保持性の接続を介して中間のサーバを経て被管理ホストにコマンドを送るクライアントを含むトランザクションのセキュリティを増大するための方法およびシステムの必要性が存在する。

また、クライアント、ネットワークサーバおよび被管理ホストを包含するトランザクションのセキュリティを増大する方法およびシステムであって、クライアントが共通操作性および行政管理上限定されたサブセットのデバイスまたはオペレーティングシステムの一つに限定されないクライアントを包含するトランザクションのセキュリティを増大する方法およびシステムの必要性が存在する。

さらに、クライアント、ネットワークサーバおよび被管理ホストを包含するトランザクションのセキュリティを増大する方法およびシステムであって、セキュリティの増大がクライアントとネットワークサーバ間の通信のためのＳＳＬプロトコルを使用することによって達成され、被管理ホストに対するクライアントのアイデンティティおよびクライアントに対する被管理ホストのアイデンティティを認証するのにKerberos認証システムが使用され、クライアントが、インターネットのような非秘密保持性のネットワーク接続を介して被管理ホストと通信するトランザクションのセキュリティを増大する方法およびシステムの必要性が存在する。

また、多くの種々のクライアントをして、認証プロトコルを使用して非秘密保持性のネットワーク接続を介してネットワークサーバを経てデスティネーションサーバと通信せしめ、データまたはコマンドを非秘密保持性のコンピュータネットワークを介してクライアントからネットワークサーバを経てデスティネーションサーバに伝送せしめる必要性も存在する。

他の要望は、ネットワークサーバがクライアントに代わってデスティネーションサーバにアクセスできるように、必要なクライアント情報を各トランザクションでネットワークサーバにパスせしめるシステムおよび方法にある。

本発明の他の目的は、好ましい具体例についての以下の図面および説明から明らかとなろう。

［発明の開示］

本発明に従うシステムおよび方法は、インターネットのような非秘密保持性のネットワークを使用してクライアント、ネットワークサーバおよび被管理ホスト間のデータ伝送のセキュリティを増すことである。クライアントとネットワークサーバ間に秘密保持性のネットワーク接続を設定後、ネットワークサーバにてキー分配センタからクライアント認証情報を得るために秘密保持性認証プロトコルが使用される。クライアント認証情報は、ネットワークサーバからクライアントに伝送される。クライアント識別情報が、クライアントから、デスティネーションサーバに対するメッセージとともにネットワークサーバに伝送される。許可は、秘密保持性認証プロトコルを使用して非秘密保持性ネットワークを介してキー分配センタからデスティネーションサーバにアクセスするように得られる。

デスティネーションサーバにて、前記クライアントがデスティネーションサーバにアクセスする権限は、メッセージを使用して確認される。デスティネーションサーバは、もしもクライアントの権限が適正に確認されれば、メッセージでアクセスされる。
クライアントとネットワークサーバ間の秘密保持性のネットワーク接続の設定は、Secure Socket Layer（SSL）プロトコルを使用できる。クライアント認証情報を獲得して、ネットワークサーバとデスティネーションサーバ間のネットワーク接続を確立するのは、Kerberos認証プロトコルを使用できる。認証されたユーザによるデスティネーションサーバに対するアクセスは、デスティネーションサーバ上におけるアクセス制御リストにより制御できる。
本発明に従うコンピュータシステムは、ネットワーク接続を介してコマンドを発行するクライアントのような第１のコンピュータサーバと、第１サーバに応答して、クライアントに代わって第４のサーバにアクセスするための、ネットワークサーバのような第２のコンピュータサーバを含む。第１および第２のサーバは、両者間の同じネットワークの操作可能な接続を介して通信できる。第２サーバはまた、第１サーバに代わって認証要求を生成できる認証デバイスを有する。キー分配コンピュータのような第３のコンピュータサーバが、認証要求を受信し、要求に応答して第１サーバのアイデンティティを認証し、第１サーバに関する認証指示情報をネットワークを介して前記第２サーバに送り返す。被管理ホストのような第４のコンピュータサーバもネットワークに相互接続され、もしもネットワークサーバが認証指示情報を被管理ホストに伝送しそして前記第１サーバが第４サーバにアクセスするように授権された場合、第１サーバからのコマンドを受信し、実行する。
【図面の簡単な説明】
図１は本発明を実施するのに使用できる一つのシステムのブロック図である。
図２は図１のクライアントおよびネットワークサーバのより詳細なブロック図である。
図３は図１のクライアント、ネットワークサーバ、キー分配センタおよびデスティネーションサーバのより詳細なブロック図である。
図４は本発明を実施するのに使用できる他のシステムのブロック図である。
図５～５ａは本発明に従う図４のシステムの動作を示すフローチャートである。
図６は図４のシステムの他の側面を示すブロック図である。
図７～７ａは本発明に従う図６のシステムの動作を示すフローチャートである。
［発明を実施するための好ましいモード］
以下図面を参照して、本発明を好ましい実施例について説明する。
Ａ．第１具体例
まず、本発明を実施するのに有用な方法および装置を、図１、２および３を参照して一般的に説明する。
図１に示されるように、本発明は、クライアントワークステーション（クライアント２００として総括的に指示される）を使用する。このクライアントワークステーションは、一例として、Microsoft Windows,Windows 95またはWindowsNT,MacIntoshまたはUNIXワークステーションをランするパーソナルコンピュータとし得る。クライアント２００は、データリンク２０２を介して非秘密保持性ネットワーク２５０（インターネットのような）に接続される。非秘密保持性ネットワーク接続２５０に沿ってクライアント２００と通信するネットワークサーバ３００は、単に例示としてＵＮＩＸとし得る。ネットワークサーバ３００は、データリンク２０４を介して非秘密保持性ネットワーク接続２５０に接続され、また、適当なデータリンク３０２を介して第２の非秘密保持性ネットワーク接続３５０と、そして適当なデータリンク３０４を介して第３の非秘密保持性ネットワーク接続４５０と接続される。デスティネーションサーバ５００は、これまたデータリンク３６０を介し非秘密保持性ネットワーク接続を経てネットワークサーバ３００と通信する。デスティネーションサーバ５００は、単に例示としてＵＮＩＸサーバとし得る。キー分配センタ（ＫＤＣ）４００は、適正なアイデンティティ設定要求を確認するもので、同様にデータリンク３７０および非秘密保持性ネットワーク接続３５０を介してネットワークサーバ３００と通信する。

図１は、ハードウェア要素の各々が従来形式の商業的に入手し得るコンピュータシステムにより実施できる。データリンク２０２，２０４，３０２，３６０および３７０は、例えばモデムを使用するデータリンクのような適当な通信媒体とし得る。また単に例示として、各コンピュータまたはサーバは、ＵＮＩＸのようなオペレーティングシステムを使用して動作し得る。

さらに、ネットワークサーバ３００およびＫＤＣ４００は、システムのセキュリティと妥協するのに使用できる情報を含んでよく、それゆえ、ネットワークサーバ３００およびＫＤＣ４００への物理的アクセスは、適切に制御できる。

１．クライアントとネットワークサーバ間の秘密保持性ネットワーク接続の設定。図１の具体例において、クライアント２００およびネットワークサーバ３００は、非秘密保持性ネットワーク２５０を介して通信する。クライアント２００は、データリンク２０２を介して非秘密保持性ネットワーク２５０に接続されるが、このリンクは、単に例示的にＴＣＰ／ＩＰネットワーク接続とし得る。ネットワークサーバ３００は、データリンク２０４を介して非秘密保持性のネットワーク２５０に接続されるが、このリンクもＴＣＰ／ＩＰネットワーク接続とし得る。メッセージのプライバシと完全性を高めるために、クライアント２００およびネットワーク３００は、好ましくは、秘密保持性の認証および／または暗号化プロトコルを使用して通信し、クライアント２００とネットワークサーバ３００間に秘密保持性ネットワーク接続を設定するのがよい。適当に信頼性のある公的に利用可能な認証プロトコルを使用できるが、かかるプロトコルはクライアント２００に対してネットワークサーバ３００のアイデンティティをうまく立証できることを条件とする。それにより、クライアント２００の側に、将来の通信がネットワークサーバ３００とのものであり、ある扮装のエンティティとのものでないとの信頼をもたらす。認証プロトコルはまた、クライアント２００とネットワークサーバ３００に対してのみ既知でありかつクライアント２００とネットワークサーバ３００間の後続のトランザクションを暗号化するのに使用できるセッションキーを生ずる。ＴＣＰ／ＩＰに使用するために特に開発されたこの種の認証プロトコルの１例は、Netscape Communication Corporationにより開発された公的に利用可能なSecure Sockets Layer（SSL）プロトコルである。

図２は、クライアント２００とネットワークサーバ３００間で通信が実施される態様の１具体例をより詳細に示している。図２に示されるように、ウェブブラウザ２０５を含んでよいクライアント２００は、矢印２０６で指示されるように、ネットワークサーバ３００のウェブサーバ３０５への認証された秘密保持性のアクセス要求を開始する。クライアント２００は、例えば、Netscape Navigatorのような任意の公的に利用可能なウェブブラウザソフトウェアパッケージを動作させてよい。要求は非秘密保持性通信リンクを横切って明示的に伝送され得るから、２０６における要求は、ログインまたはパスワード情報を含むべきではない。

ネットワークサーバ３００のウェブサーバ３０５は、情報をウェブブラウザ２０５に伝送することによって２０６の要求に応答する。しかして、この情報は、クライアント２００に対してネットワークサーバ３００のアイデンティティを認証し、かつクライアント２００とネットワークサーバ３００間の将来の伝送を暗号化するのに使用されるであろう追加の情報の生成を指示するのに使用される。もしも例えば、図２のシステムにおいてＳＳＬトランザクションが採用されるならば、ウェブサーバ３０５は、矢印２０８で示されるように、ウェブブラウザ２０５に、サーバ３００のパブリックキーおよびネットワークサーバ３００により指示される暗号化アルゴリズムを指示するアイデンティファイヤを含む証明書を送る。接続を適正に設定するためには、ネットワーク３００およびクライアント２００は、矢印２１０で指示されるハンドシェイクプロセスを遂行するが、これは、もしうまく完了すれば、クライアント２００とネットワークサーバ３００にクライアント２００とネットワークサーバ３００にのみ既知のセッションキーが提供される。このセッションキーは、ネットワークサーバ３００とクライアント２００間の将来のトランザクションを暗号化するのに使用できる。例えば、ＳＳＬのハンドシェイクプロセスにおいては、クライアント２００はセッションキーを作り、証明書においてネットワークサーバ３００によ

り指示される暗号化アルゴリズムの一つおよびネットワークサーバ３００により送られるパブリックキーを使用することによってセッションキーを暗号化し、そして暗号化されたセッションキーをネットワークサーバ３００に送る。暗号化されたセッションキーを受信した後、ネットワークサーバ３００は、このセッションキーを解読し、潜在するセッションキーで暗号化されたメッセージをクライアント２００に戻すことによってクライアント２００に対してそれ自体を認証する。

矢印２１０により指示されるハンドシェイクがうまく完了すると、クライアント２００とサーバ３００とは、将来のトランザクションを暗号化するためにセッションキーを使用し続ける。図１に総括的に指示されるように、クライアント２００とサーバ３００間の接続２０２および２０４は、それゆえ、暗号化アルゴリズムにより達成されるセキュリティの程度で保護される。

一度クライアント２００とネットワークサーバ３００間に適当に秘密保持性のネットワーク接続が設定されると、サーバ３０５は、ログインフォームをクライアント２００に送り、クライアント２００は、２１２で指示されるように、Kerberos主体の名前とパスワードより成るログインデータをウェブサーバ３０５に戻す。

２．キー分配センタに対してクライアントを認証し、キー分配センタからクライアント認証情報を獲得。

図３は、単に例示として、インターネットのような非秘密保持性ＴＣＰ／ＩＰネットワーク３５０を介してＫＤＣ４００からクライアント認証情報を得るプロセスを図示している。これは、ネットワークサーバ３００がKerberosユーザ主体に代わって動作することを確立するために、後で使用されることになる。他の公的に利用可能な非秘密保持性認証プロトコルも使用できる。しかしながら、システムのセキュリティは、タイムスタンプの使用を合体した認証プロトコルを実施することによってさらに増大せしめることができる。タイムスタンプは、リプレイの攻撃、すなわち認証プロトコルシーケンスのある部分を記録し、後日認証プロトコルを汚すために古いメッセージを使用するのに使用できる。

タイムスタンプを使用する公的に利用可能な認証プロトコルの一つの例は、MITのProject Athenaにより開発されたKerberos Version 5である。以下に記述される好ましい具体例は、Kerberos Version 5の使用を仮定する。認証手続きの詳細は以下のごとくである。

ウェブサーバ３０５が、矢印３５６により指示されるようにウェブブラウザ２０５から暗号化ログイン情報を受け取ると、ネットワークサーバ３００は、クライアント２００のKerberosユーザの主名と許可指示要求を、矢印３５２により指示されるように非秘密保持性ネットワーク３５０を介してＫＤＣ４００に通す。ＫＤＣ４００は、許可指示要求を受け取ると、ネットワークサーバ３００とＫＤＣ４００間のトランザクションを保護するためのＫＤＣセッションキーを生成する。ＫＤＣ４００は、３５２にてクライアント２００のKerberosユーザ主名を受け取ると、キーデータベース４０５からクライアント２００のシークレットキーを抽出する。このデータベースは、ＫＤＣ４００とその他の適正に登録されたクライアントにより使用されるシークレットキーを記憶している。ＫＤＣ４００は、ついでクライアント２００のシークレットキーを使用して、ＫＤＣセッションキーの一つのコピーを暗号化し、許可指示を作成する。これは、普通、単に例示として、タイムスタンプ、クライアント２００のユーザ名およびネットワークアドレス、さらにはＫＤＣセッションキーの他のコピーを含むものである。この許可指示は、クライアント２００により、ＫＤＣ４００に対してそれ自体を認証するため後日使用される。許可指示は、ＫＤＣ４００にのみ既知であるＫＤＣ４００のプライベートキーで暗号化される。ＫＤＣ４００は、それゆえ、その認証を確認するために後で許可指示を解読できる。

ＫＤＣ４００は、ついで、矢印３５４で指示されるように暗号化セッションキーおよび許可指示の両者をネットワークサーバ３００に戻す。ネットワークサーバ３００は、ＫＤＣ４００から暗号化情報を受信し、クライアント２００のユーザキーを使用してＫＤＣセッションキーを解読する。１具体例において、クライアントユーザキーはクライアント２００のパスワードおよびその他の情報のワンウェイハッシュであり、したがってネットワークサーバは、クライアント２００のパスワードを吟味することによってユーザキーを誘導

することもできる。許可指示およびＫＤＣセッションキーの両者は、クレデンシャルキャッシュ３２０に記憶される。ウェブサーバ３０５は、クレデンシャルキャッシュ３２０の内容をコード化し、そして矢印３５７で指示されるように、クレデンシャルキャッシュ３２０の内容をウェブブラウザ２０５に送る。ネットワークサーバ３００に存在したかもしれない認証情報は、ついで消去その他の方法で抹消される。その後、クライアントがトランザクションを継続するためには、クライアントはサーバ３００のメモリをリフレッシュしなければならない。情報がクレデンシャルキャッシュ３２０に記憶されている内にハッカーまたは無免許者が、ネットワークサーバ３００にアクセスしようとやりくりした場合、許可指示とセッションキーしか得られない。何故ならば、Kerberosパスワードは、使用された後に破壊されるからである。しかしながら、この情報は限定された値よりなるものである。何故ならば、許可指示は、好ましい具体例においては、日／時スタンプを含み無価値であり、普通比較的短い特定の期間の後消えてしまうからである。

３．コマンドをデスティネーションサーバへの送出。

クライアント２００は、いまやキャッシュ３２０からコード化されたクレデンシャルキャッシュをもったから、このキャッシュ情報を、究極的にデスティネーションサーバ５００に向けられたコマンドのようなメッセージとともに、矢印３５８にて指示されるようにネットワークサーバ３００に送ることができる。ネットワークサーバ３００は、コード化クレデンシャルキャッシュ情報を解読し、許可指示およびＫＤＣセッションキーをクレデンシャルキャッシュ３３０に記憶する。クレデンシャルキャッシュ３３０は上述のクレデンシャルキャッシュ３２０と同じではないが、その中のデータは同じである。実際に、情報は、同じ物理的記憶デバイス上の同じ位置に記憶されよう。けれども、実際問題としては、これはそうでない可能性が高い。

矢印３６０で指示されるように、ネットワークサーバ３００は、セッションキーにより暗号化された許可指示を、認証書およびデスティネーションサーバ５００のアクセス要求とともにＫＤＣ４００に送る。この認証書は、ＫＤＣセッションキーを使用して暗号化された、Kerberosユーザの主名およびタイムスタンプを含む。ＫＤＣ４００は、ＫＤＣシークレットキーを使用して許可指示を解読し、ＫＤＣセッションキーおよび有効期間を得る。ＫＤＣ４００がうまく解読すると、ＫＤＣは、許可指示がそれが先に発行したものと同じであることを保証される。ついで、ＫＤＣ４００は、ＫＤＣセッションキーを使用して認証書を解読し、Kerberosユーザの主名およびタイムスタンプを得る。タイムスタンプが有効期間内にあれば、ＫＤＣ４００はアクセス指示を発生する。アクセス指示は、普通、Kerberosユーザ名、有効期間およびネットワークサーバ３００とデスティネーションサーバ５００間で使用するためのサーバセッションキーを含むものであるが、これらはすべて、デスティネーションサーバ５００のプライベートキーで暗号化されている。ＫＤＣは、ついで、矢印３６２で指示されるように、暗号化アクセス指示と、ＫＤＣセッションキーを使用して暗号化されたサーバセッションキーのコピーをネットワークサーバ３００に送る。

その後、ネットワークサーバ３００は、ＫＤＣセッションキーを使用して暗号化されたサーバセッションキーのコピーを解読する。ネットワークサーバ３００は、ついで、サーバセッションキーを使用してメッセージまたはコマンドを暗号化し、矢印３６４で指示されるように、暗号化メッセージをアクセス指示および新認証書とともに、非秘密保持性ネットワーク４５０を介してデスティネーションサーバ５００に送る。デスティネーション５００は、そのプライベートキーを使用して、サーバセッションキーを解読、獲得する。

デスティネーション５００およびネットワークサーバ３００のみに既知のサーバセッションキーを使用することによって、クライアント２００のアイデンティティの認証が、デスティネーションサーバ５００で確認できる。デスティネーションサーバは５００は、ついでクライアント２００からのコマンドのようなメッセージの完全性を信用することができ、それによりもしも確認が正しければサーバ５００へのアクセスを許容する。デスティネーションサーバ５００は、クライアント２００のアイデンティティを、デスティネーションサーバ５００内のＡＣＬファイル５０５に記憶できるアクセス制御基準（ＡＣＬ）リス

トと比較できる。
Ｂ．第２の具体例
本発明のより詳しい具体例、特にKerberos認証プロセスを使用する具体例が図４～図７に示してある。図４は、図５Ａ～５ａのフローチャートとともにログインプロセスの詳細を記述している。ログインが達成されたら、図６が、図７～７ａとともに、コマンドがクライアントから被管理ホストのようなデスティネーションサーバに発行される方法の詳細を示している。
１．ログインプロセス
図４を参照すると、点線６１０により総括的に指示されるクライアント６００が、ウェブブラウザ６２０を備えている。ウェブブラウザ６２０は、点線７１０により総括的に指示されるネットワークサーバ７００と通信する。以下にさらに詳述されるように、矢印６３０，６３５，６３７および６４０は、ウェブブラウザ６２０とネットワークサーバ７００のウェブサーバ７２０間の交換を指示している。ウェブサーバ７２０は、矢印７５０および７６０で指示されるように第１のＣＧＩサービスインターフェースと情報を交換する。ＣＧＩサービスインターフェース７４０は、ウェブサーバ７２０により分岐されるプロセスとし得る。矢印８００，８１０および８２０により指示されるように、ＣＧＩサービスインターフェース７４０は、Kerberosイニシャライズクライアント７８０と情報を交換する。しかして、後者は、ＣＧＩサービスインターフェース７４０により分岐されるプロセスとし得る。ネットワークサーバ７００はさらにクレデンシャルキャッシュ８３０を含んでいるが、このクレデンシャルキャッシュは、矢印８１０により指示されるようにKerberosイニシャライズクライアントから情報を受け取り、矢印８２０により示されるようにＣＧＩサービスインターフェース７４０に情報を送る。
矢印８８０および８９０により示されるように、ネットワークサーバ７００、特にKerberosイニシャライズクライアント７８０は、点線８６０により総括的に指示されるKerberosサーバ８４０と通信する。この具体例において、Keroberosサーバ８４０は、矢印９２０により指示されるようにKerberosデータベース９１０にアクセスできるキー分配センタ（ＫＤＣ）９００を含む。Kerberosサーバ８４０は、ネットワークサーバ７００と同じコンピュータまたは異なるコンピュータ上でランする１群のプロセスとし得る。
図５～５ａのフローチャートはさらに、図４のシステムがログイン手続を遂行する方法を記述している。フローチャートのボックス内に使用される「矢印」なる用語は、図４内の対応する数値を言及するものである。ウェブブラウザ６２０は、ＨＴＴＰＳ要求をウェブサーバ７２０に送る［ボックス６０１］。ウェブサーバ７２０はウェブブラウザ６２０に対する証明書で応答する。この証明書は、ネットワークサーバのパブリックキーと、ネットワークサーバが指示する１または複数の暗号化アルゴリズムのリストを含む。しかして、後者は、ITU X.509に似てよい。ウェブ７２０はまた、ウェブブラウザ６２０との秘密保持ソケット層（ＳＳＬ）暗号化接続を設定し、ログインフォームをブラウザ６２０に送る［ボックス６０２］。
これに応答して、ウェブブラウザ６２０はウェブサーバ７２０にログインデータを戻すが、これは、この例においては、Kerberos主名のユーザ名およびパスワードを含んでいる［ボックス６０３］。
ウェブサーバ７２０は、共通ゲートウェイインターフェース（ＣＧＩ）サービスインターフェースを実行する。ログインデータは、ウェブサーバ７２０から標準入力点を経てＣＧＩサービスインターフェース７４０に通される［ボックス６０４］。ＣＧＩサービスインターフェース７４０のプロセスは、トランジェントプロセスであり、ログイン情報をKerberosイニシャライズクライアント７８０に通す。詳述すると、ＣＧＩサービスインターフェース７４０は、Kerberosイニシャライズクライアント７８０を実行する。ログインデータは、入力パラメータとして、ＣＧＩサービスインターフェース７４０から８００を経て標準入力を介してKerberosイニシャライズクライアント７８０に通される［ボックス６０５］。Kerberosイニシャライズクライアント７８０は、チケット賦与チケット（ＴＧＴ）要求をKerberosサーバ８４０のキー分配センタ（ＫＤＣ）に送る［ボックス６０６］。

換言すると、Kerberosイニシャライズクライアント７８０は、ＫＤＣ９００に対して許可指示についての要求、ここでは例えばＴＧＴを開始する。上述したように、許可指示は、適正な認証のためＫＤＣ９００との将来のトランザクション中に使用される情報を含む。ＫＤＣは、Kerberosデータベース９１０からKerberos主体に対するユーザキーを抽出する［ボックス６０７］。Kerberosのアプリケーションにおいて、クライアント６００のシークレットキーは、好ましくはクライアント６００のパスワードの秘密保持性のワンウェイハッシュがよい。ついで、ＫＤＣ９００は、ＴＧＴを、ユーザキーで暗号化されたＫＤＣセッションキーとともにKeroberosイニシャライズクライアントに送る［ボックス６０８］。

Kerberosイニシャライズクライアント７８０は、クライアント６００のパスワードを使用して、ユーザキーを発生してＫＤＣセッションキーをユーザキーで解読し、ＴＧＴおよびＫＤＣセッションキーをクレデンシャルキャッシュ８３０に記憶し、そして抜け出る［６０９］。クレデンシャルキャッシュ８３０は、トランザクションの処理において使用されるデータ記憶デバイスであり、このデータをＣＧＩサービスインターフェース７４０に利用可能にする。

ＣＧＩサービスインターフェース７４０は、クレデンシャルキャッシュをＡＳＣＩＩ－およびＵＲＬ－コード化する［ボックス６１１］。ＣＧＩサービスインターフェース７４０は、ついで、コード化クレデンシャルキャッシュおよびコマンドフォームをウェブサーバ７２０に送り、クレデンシャルキャッシュを破壊し、ついで抜け出る［ボックス６１２］。ウェブ７２０は、コード化クレデンシャルキャッシュおよびコマンドフォームをウェブブラウザ６２０に送る［ボックス６１３］。

換言すると、イニシャライズクライアント７８０は、一度情報をクレデンシャルキャッシュ８３０に記憶すると、イニシャライズクライアント７８０は抜け出る。イニシャライズクライアント７８０はトランジェントプロセスを包含するから、含まれる全データは通常消去される。しかしながら、許可指示およびＫＤＣセッションキーは一時的にクレデンシャルキャッシュ８３０に記憶されている。ＣＧＴインターフェース７４０はクレデンシャルキャッシュ８３０の内容を抽出し、その内容をASCII-およびURL-コード化する。ＣＧＩインターフェース７４０もトランジェントプロセスであり、それゆえ、抜け出る前に情報を抽出してウェブサーバ７２０にパスすることが必要である。

ウェブサーバ７２０はコード化クレデンシャルキャッシュを符号化し、データをコマンドフォームと同様にウェブブラウザ６２０に送る。一度ネットワークサーバ７００がデータをクライアント６００に送ると、データを取り扱った全トランジェントプロセスは、抜け出て終了し、したがって、クライアント６００についての全認証情報は消去され除去される。クライアント６００がトランザクションを継続するためには、クライアントは、サーバ７２０のメモリをリフレッシュし、認証プロセスの第２のフェーズを続ける。トランザクション間における期間中ネットワークサーバ７００上にはトランザクションに関する情報は存在しないから、もしも非授権者がネットワークサーバ７００に不適正にアクセスしようとやりくりすれば、上述のように、得られる情報は、限定された値より成り、システムの完全性は保持されることとなる。

２．コマンドの発行。

図４および図５～５ａに記述されるように適正なログインが遂行されると、図６および図７～７ｂに記載されるように、コマンドがクライアント６００から被管理ホスト１２００に発行され得る。図６および図７～７ｂ内の数字は、図４および図５～５ａの同様な構造およびステップに対応している。

図６を参照すると、クライアント６００のウェブブラウザ６２０は、矢印６３８および６３９で指示されるように、ネットワークサーバ７００のウェブサーバ７２０と通信する。ウェブサーバ７２０は、矢印１０１０および１０２０２より指示されるようにデータをＣＧＩサービスインターフェース１０００とデータを交換する。ＣＧＩインターフェース１００は、矢印１０６０で指示されるようにコマンドデータを秘密保持性遠隔実行クライアント１０４０にパスする。秘密保持性遠隔実行クライアント１０４０は、ＣＧＩサービス

インターフェース１０００２より分岐されるプロセスである。ＣＧＩサービスインターフェース１０００はまた、矢印１０９０により示されるようにデータをクレデンシャルキャッシュ１０８０に通し、クレデンシャルキャッシュ１０８０の方は、矢印１１００により示されるようにＴＧＴを含むデータを秘密保持性遠隔実行クライアント１０４０にパスする。秘密保持性遠隔実行クライアント１０４０は、矢印１１１０および１１２０により示されるように、Kerberosサーバ８４０のＫＤＣ９００と通信する。

秘密保持性遠隔実行クライアント１０４０は、矢印１２４０，１２６０および１２６４で示されるように、点線１２２０により総括的に指示される被管理ホスト１２００にデータを送ることができる。詳述すると、秘密保持性遠隔実行クライアント１０４０は、矢印１２４０により示されるようにインターネットスパーデーモン１２８０にデータを送り、また矢印１２６０および１２６４により指示されるように秘密保持性遠隔実行デーモン１２９０にもデータを送る。インターネットスーパーデーモン１２８０は、永続性のデーモンプロセスである。秘密保持性遠隔実行デーモン１２９０は、インターネットスーパーデーモン１２８０により分岐されるプロセスである。秘密保持性遠隔実行デーモン１２９０はまた、矢印１２６２および１３００により示されるように秘密保持性遠隔実行クライアント１０４０と通信する。秘密保持性遠隔実行デーモン１２９０は、矢印１３２０により示されるようにキーテーブル１３１０にアクセスでき、また矢印１３４０で示されるようにＡＣＬファイル１３３０にアクセスできる。キーテーブル１３１０は、好ましくは被管理ホスト上のルートユーザによってのみ読み出すことができるファイルであるのがよい。秘密保持性遠隔実行デーモン１２９０はさらに、サービスプロセス１３５００と情報を交換するが、このプロセスは、矢印１３６０および１３７０により指示されるように、秘密保持性遠隔実行デーモン１２９０により分岐されるプロセスである。秘密保持性遠隔実行デーモン１２９０は、矢印１３８０により指示されるように、永続性デーモンプロセスであるシステムロギングデーモン１３９０にデータを送ることができる。システムロギングデーモン１３９０はさらに、矢印１４１０により指示されるように、サーバ７００のシステムロギングデーモン１４００と通信する。システムロギングデーモン１４００は、永続性デーモンプロセスであり、全秘密保持性遠隔実行アクティビティの非揮発的記録をなす目的で、矢印１４２０により指示されるようにログファイル１４１０にアクセスできる。

ここで図７～７ｂのフローチャートを参照すると、図６のシステムは次の態様で動作する。フローチャートのボックスに使用される「矢印」なる用語は、図６の対応する数に言及する。ウェブブラウザ６２０は、コマンドデータおよびコード化クレデンシャルキャッシュの内容をウェブサーバ７２０に提供する［ボックス１５０１］。ウェブサーバ７２０はＣＧＩサービスインターフェース１０００を実行し、環境におけるコード化クレデンシャルキャッシュデータおよびコマンドデータを標準入力を経てウェブサーバ７２からＣＧＩインターフェース１０００にパスする［ボックス１５０２］。

ＣＧＩサービスインターフェース１０００は、コード化クレデンシャルキャッシュを解読し、それをクレデンシャルキャッシュ１０８０に再記憶する［ボックス１５０３］。ＣＧＩサービスインターフェース１０００は秘密保持性遠隔実行クライアント１０４０を実行し、命令データを入力パラメータとしてＣＧＩサービスインターフェース１０００から秘密保持性遠隔実行クライアント１０４０にパスする［ボックス１５０４］。秘密保持性遠隔実行クライアント１０４０は、クレデンシャルキャッシュ１０８０からＴＧＴおよびＫＤＣセッションキーを抽出する［ボックス１５０５］。

ついで、秘密保持性遠隔実行クライアント１０４０は、ＴＧＴおよび認証書＃１をＫＤＣ９００に送る［ボックス１０５０］。ＫＤＣ９００はＴＧＴを解読し、認証書＃２を秘密保持性遠隔実行クライアント１０４０に送る［１５０７］。秘密保持性遠隔実行クライアント１０４０は、ついで、被管理ホスト１２００に対するサービスチケット要求をＫＤＣ９００に送る［ボックス１５０８］。ＫＤＣ９００は、サーバセッションキーを作成し、Kerberosデータベース９１０から被管理ホスト１２００に対するKerberosサーバ主体キーを抽出する［ボックス１５０９］。ＫＤＣ９００は、被管理ホスト１２００に対するKerberos ＳＴを作成し、それを、ＫＤＣセッションキーで暗号化されたサーバセッションキー

と一緒に秘密保持性遠隔実行クライアント１０４０に戻し、そして秘密保持性遠隔実行クライアント１０４０は、サーバセッションをＫＤＣセッションキーで解読する［ボックス１５１０］。ついで、秘密保持性遠隔実行クライアント１０４０は、接続要求を被管理ホスト１２００のインターネットスパーデーモン１２８０に送る［ボックス１５１１］。インターネットスーパーデーモン１２８０は、秘密保持性遠隔実行デーモン１２９０を分岐、実行し暗号化要件を特定するコマンドラインパラメータをパスする［ボックス１５１２］。秘密保持性遠隔実行クライアント１０４０は、被管理ホスト１２００に対するＳＴおよび認証書＃３を秘密保持性遠隔実行デーモン１２９０に送る［１５１３］。秘密保持性遠隔実行デーモン１２９０は、キーテーブル１３１０から被管理ホスト１２００に対するサーバキーを抽出し、サーバチケットを解読し、そして認証書＃４を秘密保持性遠隔実行クライアント１０４０に送り、暗号化された接続を確立する［ボックス１５１４］。秘密保持性遠隔実行クライアント１０４０は、ついで、コマンドデータを秘密保持性遠隔実行デーモン１２９０に送る［ボックス１５１５］。秘密保持性遠隔実行デーモン１２９０はまた、ＡＣＬファイル１３３０からアクセス制御リスト（ＡＣＬ）を抽出し、Kerberos主体が被管理ホスト１２００上の特定ユーザとしてコマンドを実行するように授権される［ボックス１５１６］。

秘密保持性遠隔実行デーモン１２９０はまた、監査追跡データ（例えばKerberos主体名、遠隔ユーザおよびホスト名、ローカルユーザ名およびコマンドデータのような）を被管理ホスト１２００上のシステムロギングデーモン１３９０に送る［ボックス１５１７］。これは、全秘密保持性遠隔実行アクティビティ記録を提供することである。システムロギングデーモン１３９０の方は、監査追跡データをサーバ７００上のシステムロギングデーモン１４００に送る［ボックス１５１８］。システムロギングデーモン１４００は、監査追跡データをログファイル１４１０に記録する［ボックス１５１９］。

秘密保持性遠隔実行デーモン１２９０は、サービスプロセス１３５０を実行して、コマンドを実行し、コマンドデータを入力パラメータとしてパスする［１５２０］。秘密保持性遠隔実行デーモン１２９０により分岐されるサービスプロセス１３５０は、出力を秘密保持性遠隔実行デーモン１２９０に戻し、ついで抜け出す［ボックス１５２１］。秘密保持性遠隔実行デーモン１２９０は、出力を秘密保持性遠隔実行クライアント１０４０に送り、そして抜け出る［ボックス１５２２］。秘密保持性遠隔実行クライアント１０４０は出力をＣＧＩサービスインターフェース１００に送り、そして抜け出る［ボックス１５２３］。ＣＧＩサービスインターフェース１０００は、出力をウェブサーバ７２０に送り、クレデンシャルキャッシュ１０８０を破壊し、ついで抜け出る［ボックス１５２４］。ウェブサーバ７２０は、ついで出力をウェブブラウザ６２０に送る［ボックス１５２５］。これにより、ユーザはクライアントシステムのユーザは、実行された命令の結果を見ることが可能となる。

１より多いサーバおよびクライアントを使用することもでき、また本発明は複数のクライアントおよび複数のデスティネーションサーバに等しく適用し得ることを理解されたい。ここで使用されるところの、ネットワークサーバ３００，デスティネーションサーバ５００およびＫＤＣ４００に適用されるところの「秘密保持性」なる用語は、サーバに記憶される情報が、通常の予測される動作条件下で適当に授権された個人によってのみアクセスできることを意味することを理解されたい。

以上本発明を本発明の好ましい具体例について説明したが、当業者であれば、請求の範囲に示される本発明の技術思想から逸脱することなく種々の変化変更をなし得ることが認められよう。

【図１】

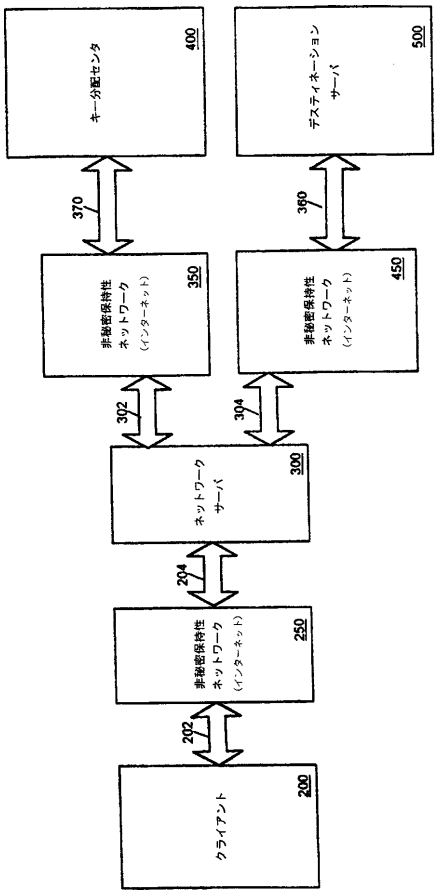

Figure 1

【図２】

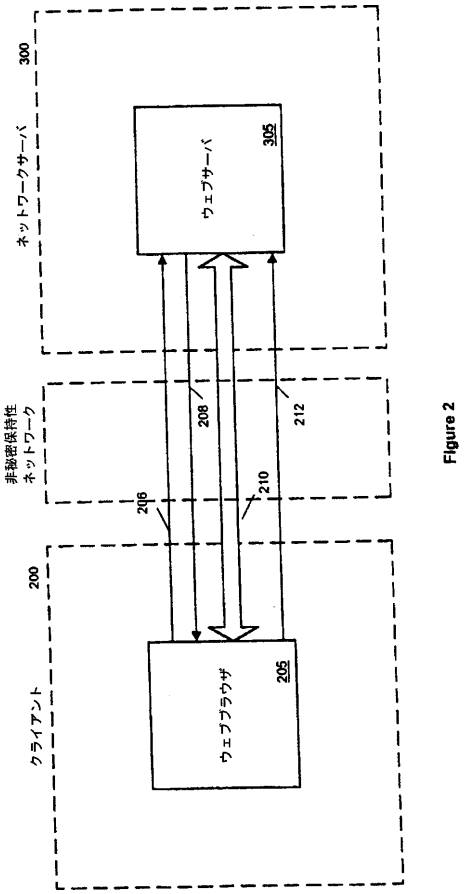

Figure 2

【図３】

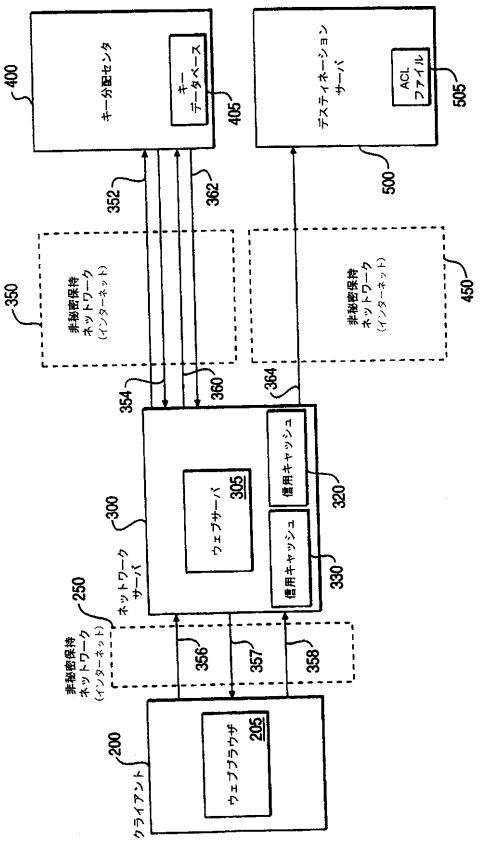

FIG. 3

【図４】

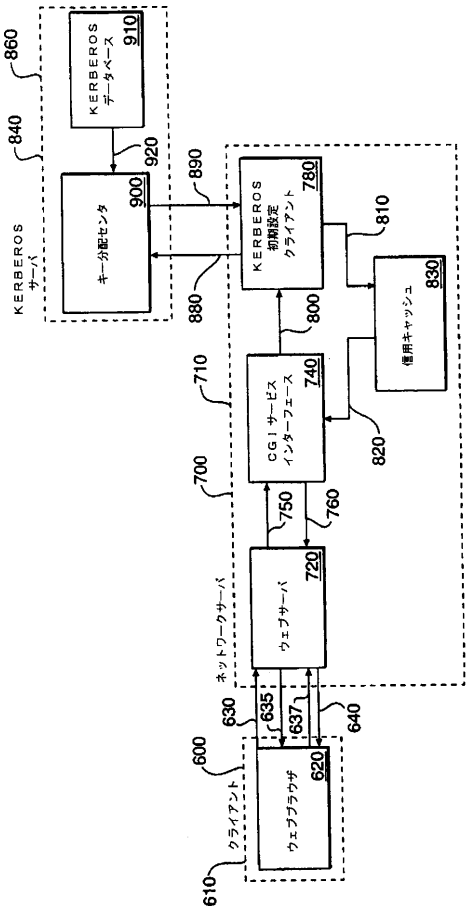

FIG. 4

【図５】

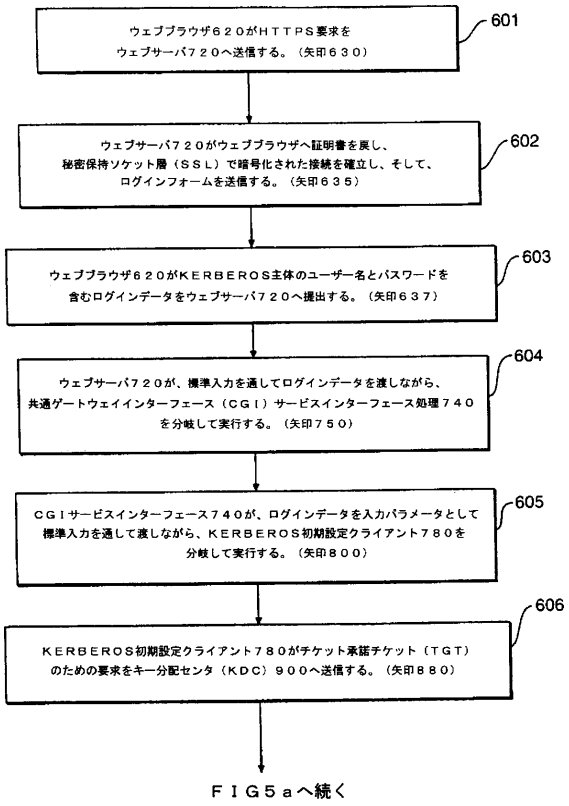

FIG. 5

【図５ａ】

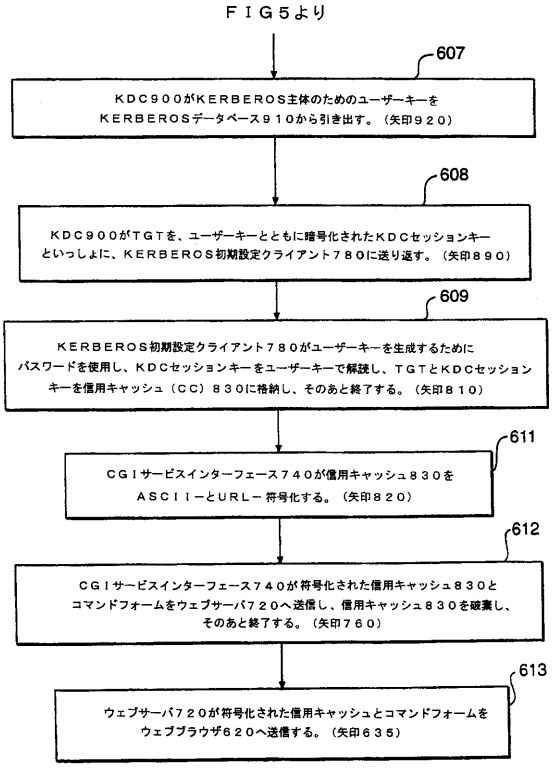

FIG. 5a

【図６】

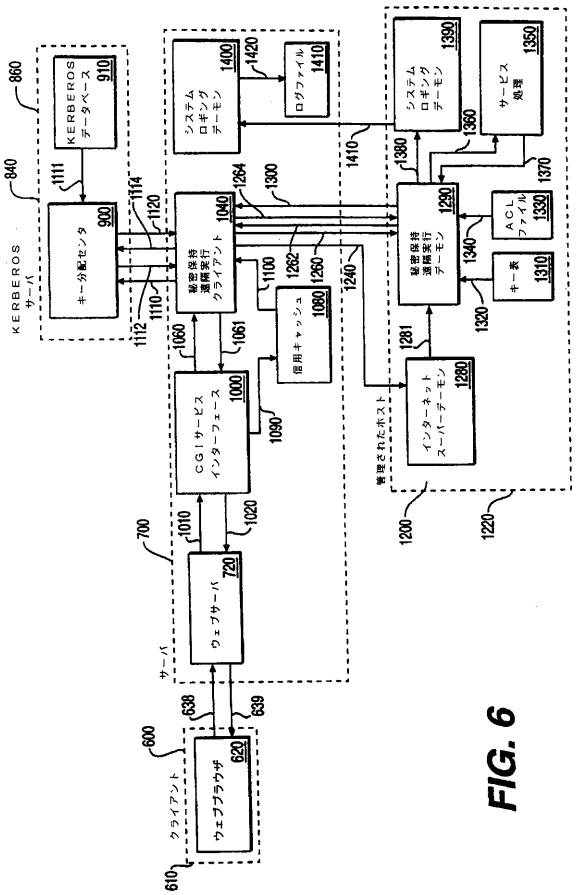

FIG. 6

【図７】

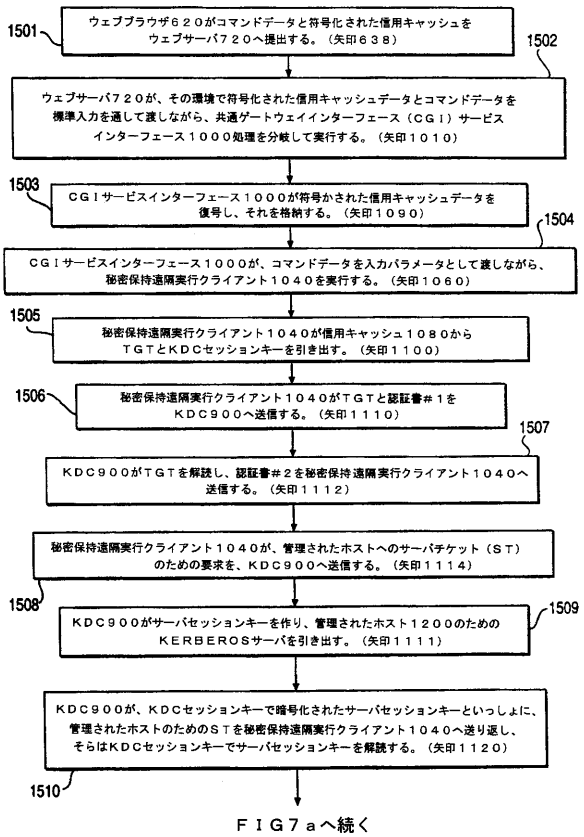

FIG. 7

【図７ａ】

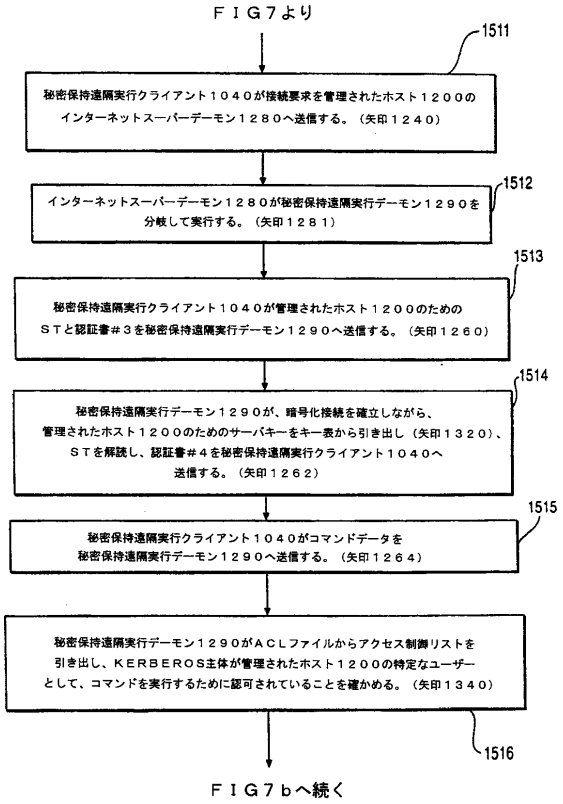

FIG. 7a

【図７ｂ】

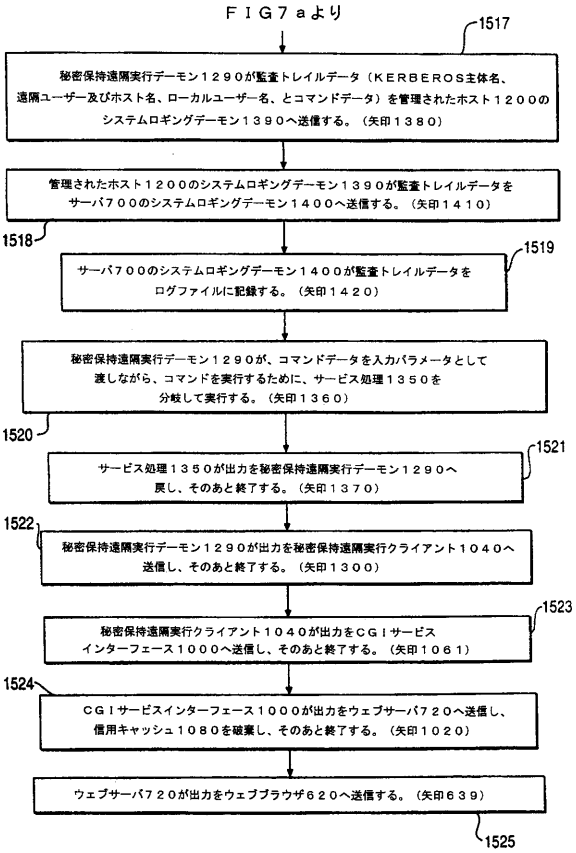

FIG. 7b

フロントページの続き

審査官　鳥居　稔

(56)参考文献　特開平０５－３２７６９１（ＪＰ，Ａ）
特開平０７－０４９８３９（ＪＰ，Ａ）
特開平０８－１０６４３７（ＪＰ，Ａ）
佐藤　豊　YUTAKA SATOU，マルチメディア時代のインターネット技術，インターフェース　第２１巻　第９号　Interface，日本，ＣＱ出版株式会社，１９９５年　９月　１日，第21巻，頁１３０－頁１４６

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/32