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

特許第4601706号
(P4601706)

(45)発行日　平成22年12月22日(2010.12.22)　(24)登録日　平成22年10月8日(2010.10.8)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330C
G06F 21/24	(2006.01)	G06F	15/00	330B
H04L 9/32	(2006.01)	G06F	12/14	540A
G09C 1/00	(2006.01)	H04L	9/00	673A
		G09C	1/00	640E

請求項の数 53　(全 24 頁)

(21)出願番号　特願2008-518283 (P2008-518283)
(86)(22)出願日　平成18年6月19日 (2006.6.19)
(65)公表番号　特表2008-544405 (P2008-544405A)
(43)公表日　平成20年12月4日 (2008.12.4)
(86)国際出願番号　PCT/US2006/023838
(87)国際公開番号　WO2007/001998
(87)国際公開日　平成19年1月4日 (2007.1.4)
審査請求日　平成21年6月16日 (2009.6.16)
(31)優先権主張番号　11/166,524
(32)優先日　平成17年6月23日 (2005.6.23)
(33)優先権主張国　米国(US)

早期審査対象出願

(73)特許権者　507421049
吉岡　昌美
アメリカ合衆国　カリフォルニア州　サン　ホセ　１０９　アルバニー　サークル　４６７１
(74)代理人　100116872
弁理士　藤田　和子
(74)代理人　100140866
弁理士　佐藤　武史
(74)代理人　100114775
弁理士　高岡　亮一
(72)発明者　吉岡　昌美
アメリカ合衆国　カリフォルニア州　サン　ホセ　１０９　アルバニー　サークル　４６７１

最終頁に続く

(54)【発明の名称】通信ネットワーク上でのクライアントとサーバ間の安全なデータ通信

(57)【特許請求の範囲】

【請求項１】

通信ネットワーク上でクライアントとサーバとの間で安全にデータを送受信するために前記クライアントに実装された装置であって、

前記装置は、メモリに接続されたマイクロプロセッサを備えており、

前記メモリに接続されたマイクロプロセッサは、

クライアント証明書を前記サーバに送るための証明書送信器と、

少なくとも前記クライアント及び前記サーバ間でデータが送受信されている間、前記サーバから送られる一連のサーバ接続メッセージを受け取って監視するための接続メッセージ受信器であって、前記一連のサーバ接続メッセージは、送受信中の前記データから独立しており、送受信中の前記データと並行して受信される、接続メッセージ受信器と、

前記接続メッセージ受信器に接続されており、受信される前記一連のサーバ接続メッセージに攪乱が発見された場合にデータ送信を停止させるためのデータ送信制御器と、

を備えるデータ交換モジュールを形成するようにプログラムされており、

前記証明書送信器は、もしデータ送信が完了する前にデータ送信が停止された場合に、前記クライアント証明書を前記サーバに再送信し、

前記マイクロプロセッサは、更に、

データ及びサーバ証明書を暗号化して送信用の暗号化データを生成するためのデータ暗号化器であって、前記サーバ証明書は前記サーバから受けとる、データ暗号化器と、

少なくとも前記暗号化データが送信されている間、一連のクライアント接続メッセー

ジを前記サーバに送信するための接続メッセージ送信器であって、前記一連のクライアント接続メッセージは、送信される前記暗号化データから独立しており、送信される前記暗号化データと並行して送信される、接続メッセージ送信器と、
を形成するようにプログラムされている、装置。
【請求項２】
前記一連のクライアント接続メッセージは、前記クライアントに特有のシーケンスあるいはパターンを有している、請求項１に記載の装置。
【請求項３】
前記マイクロプロセッサは、ユーザ識別情報に基づいて、ユーザがデータ送信のために前記クライアントを使用することを許可するセキュリティモジュールを更に形成するようにプログラムされている、請求項１に記載の装置。
【請求項４】
前記セキュリティモジュールは、ユーザ名、パスワード、ユーザ個人情報、ハードウェア向きセキュリティ鍵、及びユーザのバイオメトリック情報のうちの少なくとも１つを用いて、前記ユーザを認証する、請求項３に記載の装置。
【請求項５】
ユーザ名、パスワード、ユーザ個人情報、及びユーザのバイオメトリック情報のうちの少なくとも１つを記録するに適したデータベースを更に備えている、請求項４に記載の装置。
【請求項６】
前記マイクロプロセッサは、所定の特定プロトコルからの逸脱がないかどうか、前記データ交換モジュールの動作シーケンスを監視するためのプロトコル監視器であって、前記特定プロトコルからの逸脱が発見された場合に前記データ送信を停止させる、プロトコル監視器を更に形成するようにプログラムされている、請求項１に記載の装置。
【請求項７】
通信ネットワーク上でクライアント間を行き来するデータを安全に送信するためのサーバであって、
前記サーバは、
クライアントから送信されたデータを格納するためのメモリであって、各々が特定のクライアントに関係付けられたデータベースを有する、メモリと、
クライアントから送られたクライアント証明書を受け取り、前記クライアント証明書に基づいて前記クライアントを認証するための認証器と、
前記クライアント証明書に基づいてサーバ証明書を生成し、前記サーバ証明書を前記クライアントに送るための証明書送信器であって、前記サーバ証明書は前記クライアント証明書の情報を含んでいる、証明書送信器と、
前記サーバ及び前記クライアントの間でデータが送受信されている間、一連のサーバ接続メッセージを前記クライアントに連続的に送るための接続メッセージ送信器であって、前記一連のサーバ接続メッセージは、送受信中の前記データから独立しており、送受信中の前記データと並行して送信される、接続メッセージ送信器と、
前記クライアントからの一連のクライアント接続メッセージを受け取って監視するための接続メッセージ受信器であって、前記一連のクライアント接続メッセージは、送受信中の前記データから独立しており、送受信中の前記データと並行して受信される、接続メッセージ受信器と、
受信される前記一連のクライアント接続メッセージに攪乱が発見された場合にデータ送信を停止させるための制御器と、
を備えており、
前記制御器は、前記認証器及び前記メモリに接続されたメモリアクセスコントローラを有しており、
前記メモリアクセスコントローラは、送信クライアントから受け取った暗号化データを、前記送信クライアントから送られたデータ送信リクエストによって特定された受信クラ

イアントに関係付けられたデータベースに格納させ、前記受信クライアントが認証され且つデータ読み出しをリクエストしている場合に、格納された前記暗号化データを前記受信クライアントに送信することを許す、
サーバ。
【請求項８】
前記認証器は、前記クライアント証明書が登録されたクライアント証明書に一致するかどうかを決定する、請求項７に記載のサーバ。
【請求項９】
前記メモリアクセスコントローラは、前記データ送信リクエストが限定された期間を特定する場合に、前記格納されたデータを前記限定された期間保持する、請求項７に記載のサーバ。
【請求項１０】
通信ネットワーク上のクライアント間でデータを安全に送信するためのシステムであって、
前記システムは、
前記通信ネットワークに接続されたサーバと、
各クライアントに実装された装置であって、前記サーバと通信可能なデータ交換モジュールを備える、装置と、
を備えており、
前記データ交換モジュールは、
クライアント証明書を前記サーバに送るための証明書送信器であって、前記クライアント証明書は前記クライアントに一意的に割り振られる、証明書送信器と、
データ及びサーバ証明書を暗号化して送信用の暗号化データを生成するための暗号化器であって、前記サーバ証明書は前記サーバから受信される、暗号化器と、
前記暗号化データが送信されている間、前記サーバに一連のクライアント接続メッセージを連続的に送るための接続メッセージ送信器であって、前記一連のクライアント接続メッセージは、送信中の前記暗号化データから独立しており、送信中の前記暗号化データと並行して送信される、接続メッセージ送信器と、
前記サーバから送られる一連のサーバ接続メッセージを受け取って監視するための接続メッセージ受信器であって、前記一連のサーバ接続メッセージは、前記サーバと前記クライアントとの間で送受信されるデータから独立しており、送受信される前記データと並行して受信される、接続メッセージ受信器と、
前記接続メッセージ受信器に接続されており、受信される前記一連のサーバ接続メッセージに攪乱が発見された場合にデータ送信を停止させる、データ送信制御器と、
を備えており、
前記証明書送信器は、データ送信が完了する前にデータ送信が停止された場合には、前記クライアント証明書を前記サーバに再送信し、
前記サーバは、
前記クライアントから送信されたデータを格納するためのメモリであって、各々が特定のクライアントに関係付けられたデータベースを有する、メモリと、
前記クライアントから送られたクライアント証明書を受け取り、前記クライアント証明書に基づいて前記クライアントを認証するための認証器と、
前記クライアント証明書に基づいてサーバ証明書を生成し、前記サーバ証明書を前記クライアントに送るための証明書送信器であって、前記サーバ証明書は前記クライアント証明書の情報を含んでいる、証明書送信器と、
少なくとも前記サーバ及び前記クライアントの間でデータが送受信されている間、一連のサーバ接続メッセージを前記クライアントに連続的に送るための接続メッセージ送信器であって、前記一連のサーバ接続メッセージは、送受信中の前記データから独立しており、送受信中の前記データと並行して送信される、接続メッセージ送信器と、
前記クライアントからの前記一連のクライアント接続メッセージを受け取って監視する

ための接続メッセージ受信器であって、前記一連のクライアント接続メッセージは、送受信中の前記データから独立しており、送受信中の前記データと並行して受信される、接続メッセージ受信器と、
受信される前記一連のクライアント接続メッセージに攪乱が発見された場合にデータ送信を停止させるための制御器と、
を備えている、システム。
【請求項１１】
前記装置は、ユーザ識別情報に基づいて、ユーザがデータ送信のために前記クライアントを使用することを許可するセキュリティモジュールを更に備えた、請求項１０に記載のシステム。
【請求項１２】
前記サーバが、更に、前記認証器及び前記メモリに接続されたメモリアクセスコントローラであって、送信クライアントから受け取った暗号化データを、前記送信クライアントから送られたデータ送信リクエストによって特定された受信クライアントに関係付けられたデータベースに格納させ、前記受信クライアントが認証され且つデータ読み出しをリクエストしている場合に、格納された前記暗号化データを前記受信クライアントに送信することを許す、メモリアクセスコントローラを備えた、請求項１０に記載のシステム。
【請求項１３】
通信ネットワーク上でクライアントとサーバとの間でデータを安全に送受信するための方法であって、前記方法は前記クライアントによって実行され、前記クライアントはメモリに接続されたマイクロプロセッサを備え、
前記方法は、
ユーザからのリクエストに応じて、データ送信リクエスト及びクライアント証明書を前記サーバに前記マイクロプロセッサを用いて送るステップであって、前記クライアント証明書は前記クライアントに特有に割り当てられ、前記データ送信リクエストは少なくとも１つの受信クライアントを特定する、ステップと、
前記サーバからサーバ証明書を受け取るステップと、
前記マイクロプロセッサを用いて送信データを前記サーバ証明書と共に暗号化するステップと、
前記暗号化データを前記サーバに送信するステップと、
前記クライアントが認証された後、少なくとも前記クライアントと前記サーバとの間でデータが送受信されている間、一連のクライアント接続メッセージを前記クライアントから前記サーバに前記マイクロプロセッサを用いて送信するステップであって、前記一連のクライアント接続メッセージは、送信される前記暗号化データから独立しており、送信される前記暗号化データと並行して送信される、ステップと、
前記クライアントが認証された後、少なくとも前記クライアントと前記サーバとの間で前記データが送受信されている間、前記サーバから連続的に送られる一連のサーバ接続メッセージを受け取るステップであって、前記一連のサーバ接続メッセージは、送受信中の前記データから独立しており、送受信中の前記データと並行して受信される、ステップと、
受信される前記一連のサーバ接続メッセージに何らかの攪乱が発見されたかどうかを決定するために、前記一連のサーバ接続メッセージを、前記マイクロプロセッサを用いて監視するステップと、
前記一連のサーバ接続メッセージに攪乱が発見された場合に、前記クライアントと前記サーバとの間のデータ送信を、前記マイクロプロセッサを用いて停止させるステップと、
前記暗号化データの送信が完了する前にデータ送信が停止された場合、前記クライアントを再認証した後に、前記暗号化データを前記クライアントから前記サーバに前記マイクロプロセッサを用いて再送信するステップと、
を含む、方法。
【請求項１４】

前記一連のサーバ接続メッセージは、特定のシーケンスあるいはパターンを有している、請求項１３に記載の方法。

【請求項１５】

前記クライアントは、前記クライアントが前記サーバにログオンした時から前記クライアント接続メッセージを送信し始め、前記クライアントが前記サーバからログオフした時に前記クライアント接続メッセージの送信を停止する、請求項１３に記載の方法。

【請求項１６】

前記一連のクライアント接続メッセージは、クライアントに特有のシーケンスあるいはパターンを有している、請求項１３に記載の方法。

【請求項１７】

ユーザ識別情報に基づいて、ユーザがデータ送信するために前記クライアントを使用することを許可するステップを更に備えた、請求項１３に記載の方法。

【請求項１８】

前記許可するステップは、前記ユーザを、ユーザ名、パスワード、前記ユーザの個人情報、ハードウェア向きセキュリティ鍵、及び前記ユーザのバイオメトリック情報のうちの少なくとも１つを用いて、前記ユーザを認証するステップを含む、請求項１７に記載の方法。

【請求項１９】

特定のプロトコルからの何らかの逸脱があるかどうかを決定するために、前記クライアントと前記サーバとの間のプロセスの動作シーケンスを、前記マイクロプロセッサを用いて監視するステップと、

前記動作シーケンスにおいて前記特定のプロトコルからの逸脱が発見された場合に前記プロセスを停止させるステップと、

前記プロセスが前記逸脱の故に停止された場合に、前記クライアントを再認証した後に、前記データを再送信するステップと、

を更に含む、請求項１３に記載の方法。

【請求項２０】

通信ネットワーク上でクライアントとサーバとの間でデータを安全に送受信するための方法であって、前記方法は前記サーバによって実行され、前記サーバはメモリに接続されたマイクロプロセッサを備え、

前記方法は、

前記クライアントが認証された後、前記サーバと前記クライアントとの間でデータが送受信されている間、前記クライアントから連続的に送られる一連のクライアント接続メッセージを受け取るステップであって、前記一連のクライアント接続メッセージは、送受信中の前記データから独立しており、送受信中の前記データと並行して受信される、ステップと、

前記クライアントが認証された後、少なくとも前記データが送受信されている間、一連のサーバ接続メッセージを前記サーバから前記クライアントに前記マイクロプロセッサを用いて送信するステップであって、前記一連のサーバ接続メッセージは、送受信中の前記データから独立しており、送受信中の前記データと並行して送信されるステップと、

受信される前記一連のクライアント接続メッセージに何らかの攪乱が発見されたかどうかを決定するために、前記一連のクライアント接続メッセージを、前記マイクロプロセッサを用いて監視するステップと、

前記一連のクライアント接続メッセージに攪乱が発見された場合に、前記クライアントと前記サーバとの間のデータ送信を停止させ、前記クライアントを再認証し、前記データを前記サーバから前記クライアントに前記マイクロプロセッサを用いて再送信するステップと、

を含む、方法。

【請求項２１】

前記サーバは、前記クライアントが前記サーバにログオンした時から前記クライアント

接続メッセージを受信し始め、前記クライアントが前記サーバからログオフした時に前記クライアント接続メッセージの受信を停止する、請求項２０に記載の方法。
【請求項２２】
前記一連のクライアント接続メッセージは、クライアントに特有のシーケンスあるいはパターンを有している、請求項２０に記載の方法。
【請求項２３】
前記サーバは、前記クライアントが前記サーバにログオンした時から前記サーバ接続メッセージを送信し始め、前記クライアントが前記サーバからログオフした時に前記サーバ接続メッセージの送信を停止する、請求項２０に記載の方法。
【請求項２４】
前記一連のサーバ接続メッセージは、特有のシーケンスあるいはパターンを有している、請求項２０に記載の方法。
【請求項２５】
データ送信リクエスト及びクライアント証明書を前記クライアントから受け取るステップであって、前記クライアント証明書は、前記クライアントに特別に割り当てられており、前記データ送信リクエストは、少なくとも１つの受信クライアントを特定している、受け取るステップと、
前記クライアント証明書を用いて前記クライアントを、前記マイクロプロセッサを用いて認証するステップと、
前記クライアント証明書に基づいて、前記クライアント証明書の情報を含んだサーバ証明書を、前記マイクロプロセッサを用いて生成するステップと、
前記サーバ証明書を前記クライアントに送信するステップと、
を更に含む、請求項２０に記載の方法。
【請求項２６】
前記クライアントから暗号化データを受け取るステップと、
前記暗号化データを、特定された前記受信クライアントに関係付けられたメモリ内のデータベースに前記マイクロプロセッサを用いて格納するステップと、
を更に含む、請求項２５に記載の方法。
【請求項２７】
前記認証するステップは、前記クライアント証明書が、登録されたクライアント証明書の一つに一致するかどうかを決定するステップを含む、請求項２５に記載の方法。
【請求項２８】
クライアント識別情報を用いて前記クライアントを、前記マイクロプロセッサを用いて認証するステップを更に含む、請求項２０に記載の方法。
【請求項２９】
前記クライアントと前記サーバとの間のプロセスの動作シーケンスを、前記マイクロプロセッサを用いて監視して、特定のプロトコルからの何らかの逸脱があるかどうかを決定するステップと、
前記動作シーケンスにおいて前記特定のプロトコルからの逸脱が発見された場合に前記プロセスを停止させるステップと、
前記プロセスが前記逸脱の故に停止された場合に、前記クライアントを再認証して前記データを、前記マイクロプロセッサを用いて再送信するステップと、
を更に含む、請求項２０に記載の方法。
【請求項３０】
データ取り出しリクエスト及びクライアント証明書を第２のクライアントから受け取るステップと、
前記第２のクライアントから受け取った前記クライアント証明書を用いて前記第２のクライアントを、前記マイクロプロセッサを用いて認証するステップと、
前記第２のクライアントが認証された場合に、前記第２のクライアントが前記第２のクライアントに関係付けられたデータベースからデータを取り出すことを許可するステップ

と、
を更に含む、請求項２０に記載の方法。
【請求項３１】
前記第２のクライアントを認証するステップは、前記クライアント証明書が、登録されたクライアント証明書の一つに一致するかどうかを決定するステップを含む、請求項３０に記載の方法。
【請求項３２】
通信ネットワークに接続された仲介サーバを介してクライアント間でデータを安全に送信する方法であって、
前記方法は、
ユーザリクエストに応じて、データ送信リクエスト及びクライアント証明書を前記クライアントから前記サーバに前記マイクロプロセッサを用いて送信するステップであって、前記クライアント証明書は前記クライアントに特有に割り当てられており、前記データ送信リクエストは、少なくとも１つの受信クライアントを特定する、ステップと、
前記サーバ内で前記マイクロプロセッサを用いて、前記クライアント証明書を用いて前記クライアントを認証するステップと、
前記サーバ内で前記マイクロプロセッサを用いて、前記クライアント証明書に基づいてサーバ証明書を生成するステップであって、前記サーバ証明書は前記クライアント証明書の情報を含む、ステップと、
前記サーバ内で前記マイクロプロセッサを用いて、前記サーバ証明書を前記サーバから前記クライアントに送信するステップと、
前記クライアントにおいて、前記クライアント内で前記マイクロプロセッサを用いて、送信データを前記サーバ証明書と共に暗号化するステップと、
暗号化データを前記サーバに送信するステップと、
前記クライアント内で前記マイクロプロセッサを用いて前記クライアントが認証された後、前記暗号化データが送信されている間、一連のクライアント接続メッセージを前記クライアントから前記サーバに連続的に送信するステップであって、前記一連のクライアント接続メッセージは、前記暗号化データから独立しており、前記暗号化データと並行して送信される、ステップと、
前記サーバ内で前記マイクロプロセッサを用いて前記クライアントが認証された後、少なくとも前記クライアントと前記サーバとの間でデータが送受信されている間、一連のサーバ接続メッセージを前記サーバから前記クライアントに送るステップであって、前記一連のサーバ接続メッセージは、送受信中の前記データから独立しており、送受信中の前記データと並行して送信されるステップと、
受信される前記一連のクライアント接続メッセージに何らかの攪乱が発見されたかどうかを決定するために、前記サーバ内で前記マイクロプロセッサを用いて、前記クライアント接続メッセージを前記サーバにおいて監視するステップと、
受信される前記一連のサーバ接続メッセージに何らかの攪乱が発見されたかどうかを決定するために、前記クライアント内で前記マイクロプロセッサを用いて、接続メッセージを前記クライアントにおいて監視するステップと、
前記一連のクライアント接続メッセージあるいは前記一連のサーバ接続メッセージの何れかに攪乱が発見された場合に、前記サーバ内または前記クライアント内の前記マイクロプロセッサを用いて、前記クライアントと前記サーバとの間のデータ送信を停止させ、前記クライアントを再認証し、送信停止された前記データを再送信するステップと、
前記暗号化データの前記サーバへの送信が完了した場合に、前記暗号化データを、前記受信クライアントに関係付けられたメモリ内のデータベースに格納するステップと、
を含む、方法。
【請求項３３】
データ取り出しリクエスト及びクライアント証明書を、第２のクライアント内で前記マイクロプロセッサを用いて前記第２のクライアントから送信するステップと、

前記第２のクライアントから受け取った前記クライアント証明書を用いて、前記サーバ内で前記マイクロプロセッサを用いて前記第２のクライアントを認証するステップと、
前記第２のクライアントが認証された場合に、前記第２のクライアントが前記第２のクライアントに関係付けられたデータベースからデータを取り出すことを、前記サーバ内で前記マイクロプロセッサを用いて許可するステップと、
を更に含む、請求項３２に記載の方法。
【請求項３４】
前記第２のクライアントを認証するステップは、前記クライアント証明書が、登録されたクライアント証明書の一つに一致するかどうかを決定するステップを含む、請求項３３に記載の方法。
【請求項３５】
コンピュータによって読み取り可能なプログラム格納装置であって、前記コンピュータによって実行可能な、通信ネットワーク上でクライアントからサーバにデータを安全に送信する方法を実行する命令のプログラムを具現化し、
前記方法は、
ユーザからのリクエストに応じて、データ送信リクエスト及びクライアント証明書を前記サーバに送るステップであって、前記クライアント証明書は前記クライアントに特有に割り当てられており、前記データ送信リクエストは少なくとも１つの受信クライアントを特定する、ステップと、
前記サーバからサーバ証明書を受け取るステップと、
送信データを前記サーバ証明書と共に暗号化するステップと、
暗号化データを前記サーバに送信するステップと、
前記クライアントが認証された後、少なくとも前記暗号化データが送信されている間、一連のクライアント接続メッセージを前記クライアントから前記サーバに連続的に送信するステップであって、前記一連のクライアント接続メッセージは、前記暗号化データから独立しており、前記暗号化データと並行して送信されるステップと、
前記クライアントが認証された後、前記クライアントと前記サーバの間でデータが送受信されている間、前記サーバから連続的に送られる一連のサーバ接続メッセージを前記クライアントにおいて受け取るステップであって、前記一連のサーバ接続メッセージは、送信受中の前記データから独立しており、送受信中の前記データと並行して受信されるステップと、
受信される前記一連のサーバ接続メッセージに何らかの攪乱が発見されたかどうかを決定するために、前記一連のサーバ接続メッセージを監視するステップと、
前記一連のサーバ接続メッセージに攪乱が発見された場合に、前記クライアントと前記サーバの間のデータ送信を停止させるステップと、
前記暗号化データの送信が完了する前にデータ送信が停止された場合、前記クライアントを再認証した後に、前記暗号化データを前記クライアントから前記サーバに再送信するステップと、
を含む、プログラム格納装置。
【請求項３６】
コンピュータによって読み取り可能なプログラム格納装置であって、前記コンピュータによって実行可能な、通信ネットワーク上でクライアントからサーバにデータを安全に送信する方法を実行する命令のプログラムを具現化し、
前記方法は、
前記クライアントが認証された後、前記クライアントと前記サーバとの間でデータが送受信されている間、前記クライアントから連続的に送られる一連のクライアント接続メッセージを前記サーバにおいて受け取るステップであって、前記一連のクライアント接続メッセージは、送受信中の前記データから独立しており、送信中の前記データと並行して受信される、ステップと、
前記クライアントが認証された後、少なくとも前記データが送受信されている間、一連の

サーバ接続メッセージを前記サーバから前記クライアントに送信するステップであって、前記一連のサーバ接続メッセージは、送受信中の前記データから独立しており、送受信中の前記データと並行して送信される、ステップと、
受信される前記一連のクライアント接続メッセージに何らかの攪乱が発見されたかどうかを決定するために、前記一連のクライアント接続メッセージを監視するステップと、
前記一連のクライアント接続メッセージに攪乱が発見された場合に、前記クライアントと前記サーバとの間のデータ送信を停止させ、データ送信が完了する前にデータ送信が停止された場合、前記クライアントを再認証し、前記データを再送信するステップと、
を含む、プログラム格納装置。
【請求項３７】
前記方法は、
データ送信リクエスト及びクライアント証明書を送信クライアントである前記クライアントから受け取るステップであって、前記クライアント証明書は前記クライアントに特有に割り当てられており、前記データ送信リクエストは少なくとも１つの受信クライアントを特定している、ステップと、
前記クライアント証明書が登録されたクライアント証明書の１つに一致する場合に前記クライアントを認証するステップと、
前記クライアント証明書に基づいて、前記クライアント証明書の情報を含んだサーバ証明書を生成するステップと、
前記サーバ証明書を前記クライアントに送信するステップと、
を更に含む、請求項３６に記載のプログラム格納装置。
【請求項３８】
前記方法は、
前記クライアントから暗号化データを受け取るステップと、
特定された前記受信クライアントに関係付けられたデータベース内に前記暗号化データを格納するステップと、
を更に含む、請求項３７に記載のプログラム格納装置。
【請求項３９】
データ取り出しリクエスト及びクライアント証明書を受信クライアントである第２のクライアントから受け取るステップと、
前記第２のクライアントから受け取った前記クライアント証明書を用いて前記第２のクライアントを認証するステップと、
前記第２のクライアントが認証された場合に、前記第２のクライアントが前記第２のクライアントに関係付けられたデータベースからデータを取り出すことを許可にするステップと、
を更に含む、請求項３６に記載のプログラム格納装置。
【請求項４０】
前記一連のサーバ接続メッセージは、特定のシーケンスあるいはパターンを有している、請求項３５に記載のプログラム格納装置。
【請求項４１】
前記クライアント接続メッセージの送信は、前記クライアントが前記サーバにログオンした時から始められ、前記クライアントが前記サーバからログオフした時に停止される、請求項３５に記載のプログラム格納装置。
【請求項４２】
前記一連のクライアント接続メッセージは、クライアントに特有のシーケンスあるいはパターンを有している、請求項３５に記載のプログラム格納装置。
【請求項４３】
前記方法は、
ユーザ識別情報に基づいて、ユーザがデータ送信のために前記クライアントを使用することを許可するステップを更に含む、

請求項３５に記載のプログラム格納装置。
【請求項４４】
前記許可するステップは、
ユーザ名、パスワード、ユーザ個人情報、ハードウェア向きセキュリティ鍵、及びユーザのバイオメトリック情報のうちの少なくとも１つを用いて、前記ユーザを認証するステップを含む、請求項４３に記載のプログラム格納装置。
【請求項４５】
前記方法は、
前記クライアントと前記サーバとの間のプロセスの動作シーケンスを監視するステップと、
前記動作シーケンスにおいて特定のプロトコルからの逸脱が発見された場合に前記プロセスを停止させるステップと、
前記プロセスが前記逸脱の故に停止された場合に、前記クライアントを再認証して前記データを再送信するステップと、
を更に含む、請求項３５に記載のプログラム格納装置。
【請求項４６】
前記クライアント接続メッセージの受信は、前記クライアントが前記サーバにログオンした時から始められ、前記クライアントが前記サーバからログオフした時に停止される、請求項３６に記載のプログラム格納装置。
【請求項４７】
前記一連のクライアント接続メッセージは、クライアントに特有のシーケンスあるいはパターンを有している、請求項３６に記載のプログラム格納装置。
【請求項４８】
前記サーバ接続メッセージの送信は、前記クライアントが前記サーバにログオンした時から始められ、前記クライアントが前記サーバからログオフした時に停止される、請求項３６に記載のプログラム格納装置。
【請求項４９】
前記一連のサーバ接続メッセージは、特定のシーケンスあるいはパターンを有している、請求項３６に記載のプログラム格納装置。
【請求項５０】
前記認証するステップは、前記クライアント証明書が、登録されたクライアント証明書の１つに一致するかどうかを決定するステップを含む、請求項３７に記載のプログラム格納装置。
【請求項５１】
前記方法は、クライアント識別情報を用いて前記クライアントを認証するステップを更に含む、請求項３６に記載のプログラム格納装置。
【請求項５２】
前記方法は、
前記クライアントと前記サーバとの間のプロセスの動作シーケンスを監視するステップと、
前記動作シーケンスにおいて特定のプロトコルからの逸脱が発見された場合に前記プロセスを停止させるステップと、
前記プロセスが前記逸脱の故に停止された場合に、前記クライアントを再認証して前記データを再送信するステップと、
を更に含む、請求項３６に記載のプログラム格納装置。
【請求項５３】
前記認証するステップは、前記クライアント証明書が、登録されたクライアント証明書の１つに一致するかどうかを決定するステップを含む、請求項３９に記載のプログラム格納装置。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信ネットワーク上におけるクライアントコンピューター（クライアント）間の安全なデータ通信に関し、特に、中間サーバを介してクライアント間で安全にデータ通信及び交換を行う方法及び装置に関する。
【背景技術】
【０００２】
通信ネットワーク上での安全なデータの交換は、多くの事業及び産業分野において最も重要な問題の一つである。電子データを安全に送信するために、様々な暗号化方法及び暗号化鍵スキーム（公開及び秘密）が使われてきた。例えば、通常、電子メール交換システムはユーザ名とパスワードによって守られており、発信メッセージの内容と添付ファイルのための暗号化機能を有している。通常、データ交換システムにおける暗号化された通信にはセキュア・ソケット・レイヤー（ＳＳＬ）プロトコルが用いられる。トランスポート・レイヤー・セキュリティ（ＴＬＳ）プロトコルを用いることもできる。電子取引においては、ユーザを識別するために電子証明書（デジタルＩＤ）も用いられる。送信データは暗号化され、データ交換サーバへのアクセスはパスワードと証明書の使用によって制限されてはいるが、このような従来のデータ交換システムは送信中の“通信経路”を守ることはしない。例えば、暗号化されたデータが発信元／送信者から送り出された後、宛先／受信者に届く前に、データパケットとしての暗号化データがハッキングされたり、変更されたりするかもしれない。ユーザがデータ交換サーバへのアクセスを許可され、データをダウンロードあるいはアップロードし始めた後に、データが傍受、漏洩されたり、あるいはフィルタにかけられることによりデータ内の情報がハッキングされるかもしれない。更に、インターネット上の買い物やインターネット銀行業務（オンラインバンキング）のような電子取引においては、ユーザは、最初に安全なサイトにログオンするときにだけ（通常ユーザ名とパスワードを用いて）認証・許可される。そのような電子取引の間には、偽装したユーザがログオンして安全なサイトにアクセスしようとしたり、あるいはユーザが意図しないサイトに誘導されユーザの個人情報が奪われるかもしれない。しかしながら、従来のシステムは、ユーザが最初に認証されたユーザと同じユーザであり、サーバがそのままの同じサーバであるかどうかを確認する手段を有していない。
【発明の開示】
【発明が解決しようとする課題】
【０００３】
本発明は、通信ネットワーク上でクライアントとサーバの間でデータを安全に送信するための方法及び装置を提供することを目的とする。
【課題を解決するための手段】
【０００４】
安全なデータ送信は、クライアントが最初に認証された後、（ａ）少なくともデータが送信されている間、一連のクライアント接続メッセージをクライアントからサーバに送信すること、（ｂ）少なくとも前記データが送信されている間、一連のサーバ接続メッセージをサーバからクライアントに送信すること、（ｃ）クライアント接続メッセージをサーバにおいて監視すること、（ｄ）サーバ接続メッセージをクライアントにおいて監視すること、（ｅ）クライアント接続メッセージあるいはサーバ接続メッセージのいずれかに攪乱が発見された場合に、クライアントとサーバの間のデータ送信を停止させ、クライアントを再認証してデータを再送信すること、及び（ｆ）暗号化データがサーバに無事に送信された場合に、受信者に関係付けられたデータベースに暗号化データを格納すること、を含む。
【発明を実施するための最良の形態】
【０００５】
本明細書に組み込まれ、その一部を構成する添付の図面は、本発明の１つあるいはそれ

以上の実施例を提示しており、発明の詳細な記述と共に本発明の原理と実施の形態とを説明する。

【０００６】

本発明の実施の形態は、通信ネットワーク上でクライアントからサーバにデータを安全に送信するための方法と装置として記載される。当業者には、以下の本発明の詳細な記載が例示的なものであり、決して限定的に解釈されるこを意図したものでないことが理解できるであろう。本開示内容から本発明の他の実施例が容易に示唆されることが当業者にはわかるであろう。添付の図面に示されるように、実施形態を参照して本発明が詳細に説明される。図面及び以下の詳細な説明を通して、同様の要素には同様の参照番号が用いられる。

【０００７】

ここに記載される実施の形態においてよく知られた慣例的な特徴は、記載を明瞭にするため、その全てが説明されるわけではない。もちろん、具体的な実施の形態の開発に当たっては、開発者の特定の目的を達するため、その用途や事業に応じた制約など、実施形態に特有の数多くの決定がなされなければならないであろう。また、そのような特定の目的は、実施の形態によって、また開発者によって異なるであろう。さらに、そのような開発の努力は複雑であり時間がかかるかもしれない。しかし、それにもかかわらず、本開示を得た当業者にとっては、それらは技術開発における通常の事業活動であることが理解される。

【０００８】

本発明による１つの実施例においては、要素、プロセスステップ、及び／又はデータ構成は、様々なタイプのオペレーティングシステム（ＯＳ）、コンピューティングプラットフォーム、ファームウェア、コンピュータープログラム、コンピューター言語、及び／又は汎用マシーンを用いて実施され得る。本発明による方法は、処理回路上で実行されるプログラムされたプロセスとして実施され得る。そのような処理回路は、プロセッサ及びオペレーティングシステムの様々な組み合わせ、あるいは独立した装置としての形態をとることができる。プロセスは、そのようなハードウェアによって実行される命令として、ハードウェアのみで、あるいはそれらの組み合わせとして実施され得る。ソフトウェアは、機械によって読み取り可能なプログラム記録装置に記録されてもよい。

【０００９】

本発明の１つの実施例によれば、本発明の方法は、パーソナルコンピューター、ワークステーションコンピューター、メインフレームコンピューター、あるいは高性能サーバなどのデータ処理コンピューター上に実施されてもよい。高性能サーバは、カリフォルニア州、パロアルトのサン・マイクロシステムズのソラリス、ワシントン州、レッドモンドのマイクロソフトコーポレイションのマイクロソフトウインドウズＸＰ及びウインドウズ２０００、あるいは、数多く市販されているリナックスのようなユニックスオペレーティングシステムの様々なバージョンなどのＯＳを実行してもよい。また、本発明による方法は、多プロセッサシステムや、入力デバイス、出力デバイス、ディスプレイ、ポインティングデバイス、メモリ、記録装置、プロセッサとのデータのやり取りのためのメディアインターフェースなど、様々な周辺機器を有するコンピューティング環境に実施されてもよい。また、そのようなコンピューターシステムやコンピューティング環境は、ローカルにあるいはインターネットを介してネットワーク化されていてもよい。

【００１０】

図１は、本発明による形態を実施するのに適したコンピューターシステム１００を示すブロック図である。図１に示されるように、コンピューターシステム１００は、バス１０２を備えており、バス１０２は、中央処理装置１０４、システムメモリ１０６（典型的にはＲＡＭ）、入力／出力（Ｉ／Ｏ）制御装置１０８、ディスプレイアダプタ１１２を介して接続されたディスプレイスクリーン１１０のような外部装置、シリアルポート１１４及び１１６、キーボード１１８、固定ディスクドライブ１２０、フロッピーディスク（登録商標）１２４を受け入れるように構成されたフロッピーディスク（登録商標）ドライブ１

２２、ＣＤ－ＲＯＭ１２８を受け入れるように構成されたＣＤ－ＲＯＭドライブ１２６などの主要なサブシステムを相互接続している。多くの他の装置、例えば、シリアルポート１１４を介して接続されたポインティングデバイス１３０（例えば、コンピューターマウス）、シリアルポート１１６を介して接続されたモデム１３２などが接続されてもよい。モデム１３２によって、電話線網を介して遠隔のサーバに直接接続したり、ＰＯＰ（Ｐｏｉｎｔ　ｏｆ　Ｐｒｅｓｅｎｃｅ）を介してインターネットに直接接続することができる。あるいは、ネットワークインターフェースアダプタ１３４を介し、当業者によく知られたネットワークインターフェースシステム（例えば、イーサネット（登録商標）、ｘＤＳＬ，アップルトークなど）を用いて、ローカルエリアネットワークやワイドエリアネットワークに接続してもよい。

【００１１】

他の多くの装置やサブシステム（図示せず）が同様の方法で接続されてもよい。また、以下に説明される本発明を実施するために、図１に示される全ての装置が必要とは限らない。さらに、装置やサブシステムは、図１に示されるのとは異なる方法で相互接続されてもよい。図１に示されるようなコンピューターシステムの動作は当業者にはよく知られており、本発明の記載を不必要に複雑化しないため、本明細書においては詳細に議論されない。本発明を実施するコンピューターコードは、システムメモリ１０６や、固定ディスク１２０、フロッピーディスク（登録商標）１２４、あるいはＣＤ－ＲＯＭやＤＶＤ－ＲＯＭのような光学記録媒体１２８などの記録媒体に記録されてもよい。

【００１２】

前述したように、従来のデータ交換システム及び電子取引システムは、ＩＤ／パスワードによる保護及びデータ暗号化を提供するが、通信中のデータトラフィック及びデータ通信経路は情報傍受、盗聴、フィルタリングなどに対して脆弱なままである。本発明は、クライアント（クライアントコンピューター）とクライアントとの間に中間サーバを設け、クライアントコンピューターと中間サーバとの間で接続メッセージを交換することによって通信経路を保護し、更なる安全性を提供する。本発明は、クライアントとサーバ間の電子取引にも適用可能である。本発明の実施例によれば、データ送信の間、特定のシーケンス、順序、あるいはパターンを有する一連の接続メッセージが、「背景（バックグラウンド）」通信として交換される。もし、クライアント側あるいはサーバ側の何れかにおいて、特定のシーケンス、順序、あるいはパターンに攪乱が観察された場合、進行中のデータ送信は中断され、データ送信プロセスは、最初のクライアント・サーバ証明書及び認証プロセスからやり直しされる。更に、クライアント・サーバ間で接続メッセージの送受信を行うことにより、お互いに正しい相手と通信していることを両者が継続的に確認することができる。本発明は、更に、クライアント及びサーバがクライアント証明書及びサーバ証明書を交換する証明書プロセスを提供する。

【００１３】

図２は、本発明の１つの実施例による、通信ネットワーク上でクライアント１０及び１２の間でデータを安全に送信するシステム２００を模式的に示す。システムは、通信ネットワーク１４に接続された中間サーバ１６を備えている。図２には２つのクライアントしか示されていないが、システム２００には２つより多くのクライアントが含まれていてもよい。このシステムは閉鎖的であり、全てのユーザ（及びクライアント）はシステムに加入する前に登録されなければならない。サーバ１６は、全ての登録されたユーザ／クライアントを知っており、クライアント間のデータ交換を仲介する。データ送信は、暗号化体系、例えばＳＳＬプロトコルを採用することによって保護される。ＳＳＬプロトコルに加えて、又はその代わりに、他の暗号化体系を用いてもよい。ユーザは、送信されるデータの受信者として、一人のユーザ、あるいはユーザグループを選択することができる。

【００１４】

各クライアントは、サーバ１６と通信可能なデータ交換モジュールを有する。図３は、本発明の１つの実施例によるデータ交換モジュール２０を備えたクライアント１０を模式的に示す。例えば、データ交換モジュール２０は、クライアントコンピューターに搭載（

インストール）されたアプリケーションプログラムでもよい。本発明の１つの実施例によれば、アプリケーションプログラムは、インストールされたクライアントと１対１の対応関係にあり、モジュールに固有の識別情報、例えばシリアル番号によって識別される。クライアント１０の電子証明書（クライアント証明書）は、たとえば、アプリケーションプログラムがその製造者によってクライアント１０にインストールされるときに付与される。電子証明書は、更新・変更されてもよく、例えば毎年、あるいは２年毎に更新されてもよい。クライアント証明書はそのクライアントを識別するために特別に割り当てられる。

【００１５】

図３に示すように、データ交換モジュール２０は、証明書送信器２２、暗号化器２４、接続メッセージ送信器２６、接続メッセージ受信器２８、データ送信制御器３０、及びインターフェース３２を備える。データ交換モジュール２０は、更に、サーバ１６から受け取ったデータを復号する復号化器３８を備えている。クライアント１０は、また、データを処理するためのデータ処理モジュール（図示せず）のような他の要素をも備えている。

【００１６】

証明書送信器２２は、クライアント証明書をインターフェース３２を介してサーバ１６に送信する。クライアント１０が認証された場合、サーバ証明書がサーバ１６からクライアント１０に返送される。クライアント１０は、送信すべきデータにサーバ証明書を添付し、暗号化器２４が送信データ及びサーバ証明書を一緒に暗号化することにより暗号化データを生成する。例えば、セキュアソケットレイヤー（ＳＳＬ）プロトコルが暗号化に用いられる。

【００１７】

接続メッセージ送信器２６は、少なくとも暗号化データが送信されている間、一連のクライアント接続メッセージをサーバ１６に送信し続ける。本発明の１つの実施例によれば、クライアント１０は、クライアント１０がサーバ１６にログオンした時からクライアント接続メッセージを送信し始め、クライアント１０がサーバ１６からログオフした時にクライアント接続メッセージの送信を停止する。一連のクライアント接続メッセージは、クライアント１０に特有のシーケンス、順序、あるいはパターンを有する。例えば、クライアント接続メッセージの１つ１つに番号を付したり、時刻印（タイムスタンプ）したり、あるいはそれ以外の方法によって接続メッセージの各々が互いに識別・分別可能であるようにして、一連の接続メッセージが観察者によって特定可能な特別なシーケンスを形成するようにする。あるいは、クライアント接続メッセージにはいくつかのタイプがあり、その異なるタイプのシーケンスがパターンを形成する。たとえば、もし接続メッセージが４つのタイプ、Ａ、Ｂ、Ｃ、Ｄを有する場合、ＡＢＣＤＡＢＣＤＡＢＣＤというシーケンスは特定の周期的なパターンを構成する。クライアント接続メッセージはそのクライアントに特有であるか、あるいはクライアント識別子を含んでおり、従って、どのクライアントがその特有なクライアント接続メッセージを送っているのかをサーバが区別することができる。また、クライアント接続メッセージのパターンはクライアント毎に異なっている。更に、特有のシーケンス、順序、あるいはパターンは、所望の期間ごとに更新・変更されてもよい。

【００１８】

接続メッセージ受信器２８は、サーバ１６から送られたサーバ接続メッセージを受信し監視する。クライアント接続メッセージと同様に、一連のサーバ接続メッセージは特定のシーケンス、順序、あるいはパターンを有する。データ送信の間、接続メッセージ受信器２８は、受信したサーバ接続メッセージのシーケンスを監視し検査する。もし、順序（あるいは特有のパターン）が攪乱された場合、例えば、サーバ接続メッセージ（のいくつか）が欠損していたり、順序が入れ違っている場合、データのハッキング、誘導、傍受、その他、データ送信への何らかの攻撃があったことを意味する。

【００１９】

データ送信制御器３０は、証明書送信器２２、暗号化器２４、接続メッセージ送信器２６、及び接続メッセージ受信器２８を制御する。もし接続メッセージ受信器２８が受信し

たサーバ接続メッセージの攪乱を検出した場合、データ送信制御器３０が現在進行中のデータ送信を中止させる。もしデータ送信が完了する前にデータ送信が停止された場合、データ送信制御器３０は、クライアント認証プロセスをやり直させ、証明書送信器２２がクライアント証明書をサーバ１６に再送するようにする。

【００２０】

本発明による１つの実施例によれば、クライアント１０は、セキュリティモジュール４０及びメモリあるいはデータベース４２を更に備えている。ユーザ名、パスワード、生体情報などのユーザ識別情報及び生年月日、出生地などのその他の個人情報がメモリ４２に保存されてもよい。また、アプリケーションプログラムが搭載される時に、たとえば、米国イリノイ州、アーリントンハイツのアラジンナレッジシステムズが提供するＨＡＳＰ（Ｈａｒｄｗａｒｅ　Ａｇａｉｎｓｔ　Ｓｏｆｔｗａｒｅ　Ｐｉｒａｃｙ）鍵のようなハードウェア用セキュリティ鍵４４がインストールされてもよい。ＨＡＳＰ鍵は、個別のコンピューターで実行されるソフトウェアを保護し、ライセンスするために用いられる。他のタイプのハードウェア用鍵、パスワード、あるいはパスコードなどが用いられてもよい。

【００２１】

セキュリティモジュール４０は、ユーザ識別情報に基づいて、ユーザがクライアント１０を使うのを許可する。セキュリティモジュール４０は、上述の識別・個人情報の様々な組み合わせを用いてユーザを識別し、認証する。ユーザが１つあるいはそれ以上のタイプの個人情報をユーザインターフェース３４から入力するように促してもよい。ユーザがクライアントを使ってデータを送信する前に、正しいハードウェア用セキュリティ鍵を挿入するように要求してもよい。あるいは、クライアント１０が使われる状況に応じ、１つのハードウェア用セキュリティ鍵を共有することにより、複数のユーザがクライアント１０を使えるようにしてもよい。ユーザの生体情報を用いる場合、たとえば、指紋センサーや撮像装置など、使おうとするユーザからの生体情報を受け取る生体情報センサー４６をクライアント１０に備えてもよい。その場合、当業者にはよく理解できるように、セキュリティモジュール４０は生体識別処理を行うソフトウェア及び／又は回路（図示せず）を備えている。データ交換モジュールが搭載され、特定のクライアントとユーザのために初期化される時に、上述した識別・個人情報の全てを記録してもよい。なお、図３において、セキュリティモジュール４０はデータ交換モジュール２０とは別のモジュールとして示されているが、セキュリティモジュール４０はデータ交換モジュールと一体化されていたり、その一部であってもよい。

【００２２】

無事にユーザの識別及び認証が済むと、ユーザはクライアント１０を使ってデータ送信することを許可される。ユーザのリクエストやコマンドに応じて、クライアント１０は、まず、アクセスリクエストにクライアント証明書を添付してサーバ１６に送る。サーバ１６は、リクエストしているクライアント１０が正しいクライアント証明書を持っていることを確認してから、クライアント１０にサーバ１６のサーバ証明書を返送する。あるいは、サーバ１６は、まず、承認（肯定的な認証結果）のみをクライアント１０に送り、処理を続けて（クライアント１０がシステムにログオンするのを許可し）、クライアント１０が更にデータ送信リクエストを行ってからサーバ証明書を返送してもよい。クライアント１０のデータ取り出しリクエストに対しては、サーバ１６はサーバ証明書を返送しなくてもよい。また、データ交換モジュール及び／又はクライアントマシンの識別情報（例えばシリアル番号）を用いて、クライアント１０の認証プロセスを更に行ってもよい。どの情報をいかなる順序で用いるかは、クライアント１０とサーバ１６間のプロトコルの選択によって決められてもよい。そのようなプロセスの特定のシーケンス（順序）自体を更なる安全措置として用いてもよい。

【００２３】

従って、データ交換モジュール２０は、データ送信制御器３０に制御されるプロトコル監視器（モニター）３６を更に備えてもよい。プロトコル監視器３６は、所定の特定プロトコルからの逸脱がないかどうか、データ交換モジュール２０の動作のシーケンスを監視

する。もし、タイミングや、動作のシーケンスが特定のプロトコルから逸脱した場合、プロセスが攻撃されていたり、ハッキングされたり、偽装したクライアント・ユーザがサーバ１６にアクセスしようと試みているのかもしれない。そのような場合、証明書プロセス及び／又はそれに引き続くデータ送信は、データ送信制御器によって停止され、プロセス全体が最初からやり直しされる。このことにより、更なるセキュリティのレイヤが提供される。

【００２４】

本発明による１つの実施例によれば、サーバ１６は中間サーバに限らず、オンラインショッピング、オンライン銀行取引や他の電子取引を提供する商業用のサーバであってもよい。そのような場合、クライアント１０は顧客クライアントでもよい。そのような顧客クライアントは、データ交換モジュールのためのアプリケーションプログラムを商業用サーバからダウンロードしたり、あるいはオフラインでインストールするために、アプリケーションプログラムを記録した光ディスク（ＣＤ）のような記録媒体を購入してもよい。電子取引が行われている間、あるいは顧客クライアントがサーバにログオンしている間、クライアント接続メッセージ及びサーバ接続メッセージが顧客クライアントと商業用サーバとの間で交換されてもよい。クライアント／サーバ接続メッセージは、電子取引の間、顧客／サーバが正しい実体であることを確認し続けることを可能にし、さらに、通信経路を不正な干渉から保護する。電子証明書が別途に顧客クライアントに送られてもよい。前述した証明書の交換は、顧客クライアントの最初の認証プロセスで行われてもよく、あるいは顧客クライアントが支払や資金振替を行うときや、重要な情報や秘密にすべき情報が顧客クライアントからサーバに送信されるときにサーバ証明書を添付してもよい。

【００２５】

図４は、本発明の１つの実施例によるサーバを模式的に示している。サーバ１６は、制御器５０、認証器５２、証明書送信器５４、接続メッセージ送信器５６、接続メッセージ受信器５８、メモリ６０、及びインターフェース７０を備えている。認証器５２は、クライアント１０から送られたクライアント証明書を受け取り、そのクライアント証明書に基づいてクライアントを認証する。例えば、認証器５２は、クライアント１０からのクライアント証明書が登録されたクライアント証明書の１つに一致するかどうかを決定する。メモリ６０は、登録されたクライアントの情報や、認証器５２が用いる登録されたクライアントの証明書を保持するデータベース６８を備えていてもよい。クライアント証明書に加え、ユーザ名やパスワードがクライアント１０の認証に用いられてもよい。

【００２６】

クライアント１０が認証された場合は、証明書送信器５４がクライアント証明書に基づいて、あるいはクライアント証明書の関数として、サーバ証明書を生成し、そのサーバ証明書をクライアントに送信する。サーバ証明書はクライアント証明書の情報を含んでいる。例えば、クライアント証明書をサーバ証明書に添付して送り返してもよい。

【００２７】

クライアントの接続メッセージ送信器２６と同様、サーバの接続メッセージ送信器５６は、一連のサーバ接続メッセージをクライアント１０に送る。少なくともサーバ１６及びクライアント１０の間でデータが送信されている間、サーバ接続メッセージが送信される。本発明による１つの実施例によれば、サーバ１６は、クライアント１０がサーバ１６にログオンした時からサーバ接続メッセージを送り始め、クライアント１０がサーバ１６からログオフした時にサーバ接続メッセージの送信を止める。サーバ接続メッセージはブロードキャスト（同放通信）されるのではなく、現在サーバ１６にログオンしている特定のクライアント１０にだけ送信される。クライアント接続メッセージと同様、サーバ接続メッセージは、クライアント１０によってモニターできる特定のシーケンス、順序、あるいはパターンを有している。

【００２８】

接続メッセージ受信器５８は、クライアント１０から送られるクライアント接続メッセージを受け取って監視する。制御器５０は、接続メッセージ受信器５８がクライアント接

続メッセージのシーケンス、順序、あるいはパターンに攪乱を発見した場合、データ送信を停止させる。もし、データ送信が完了する前に、受け取ったクライアント接続メッセージが攪乱されているが故にデータ送信が停止、あるいは中断された場合、制御器５０はクライアント１０にインターフェース７０を介してエラーメッセージを送ってもよい。そのようなエラーメッセージに応答して、クライアント１０は、データを再送信するため、クライアント証明書を送信することにより再認証プロセスを開始する。もし、データ送信が無事完了した場合、送信されたデータ（アップロードされたデータ）は、サーバ１６のメモリ６０に格納され、通常は特定の期間保持される。

【００２９】

メモリ６０は、各々が特定のクライアントに関連付けられたデータベース６２、６４、６６、・・・を備えている。本発明による１つの実施例によれば、クライアント１０のユーザは、どのユーザ（すなわち、単数又は複数の受信者クライアント）にデータを送信し、また格納されたデータをどれくらいの期間サーバ１６に保存しておくべきかを指定できる。このような指定情報は、データ送信リクエストにおいて特定することができる。もし、特定の保存期間が指定されない場合、制御器５０がデフォルトの保存期間を設定してもよい。このようにして、サーバ１６にアップロードされたデータが受信者クライアントに対応するデータベースに指定された期間だけ保存され、その期間の間、受信者クライアントはそのデータにアクセスしてデータの取り出し（ダウンロード）を行うことができる。

【００３０】

例えば、クライアント１０（送信者クライアントＡ）がデータをサーバ１６に送信する場合、データ送信リクエストは少なくとも一人の受信者クライアント、例えばクライアント１２（受信者クライアントＢ）を含んでいる。そして、クライアント１０から送信されたデータは、クライアント１２（受信者クライアントＢ）に関連付けられているデータベース６４に保存される。保存されたデータは、暗号化されたまま保持され、またクライアント証明書の情報を含んだサーバ証明書を含んでいる。従って、クライアント１２がデータを受け取って復号化する時、クライアント１２はクライアント１０が送信者クライアントＡであることを確認できる。

【００３１】

制御器５０は、認証器５２とメモリ６０に結合され、上述のメモリ動作を実行するメモリアクセス制御器７２を備えていてもよい。すなわち、メモリアクセス制御器７２は、クライアント１０（送信者クライアントＡ）からのデータ送信リクエストを受け取り、クライアント１０からの暗号化されたデータを、データ送信リクエストで特定されているクライアント１２（受信者クライアントＢ）に関連付けられたデータベース６４に格納する。クライアント１２が自身に関連付けられているデータベース６４へのアクセス及びデータ取り出しをリクエストすると、メモリアクセス制御器７２は、クライアント１２が認証器５２によって認証された後、格納されたデータがクライアント１２に送信されることを許す。認証器５２は、クライアント１０を認証するのと同様の方法でクライアント１２を認証する。

【００３２】

更に、サーバ１６は、制御器５０によって制御されるプロトコル監視器７４を備えていてもよい。プロトコル監視器７４は、所定のプロトコルからの逸脱がないかどうか、サーバ１６の動作シーケンスを監視する。もし、タイミングや動作シーケンスが特定のプロトコルから逸脱している場合、サーバプロセスがアタックあるいはハッキングされていたり、また偽装したクライアント／ユーザがサーバ１６にアクセスしようとしているのを示唆しているかもしれない。そのような場合、制御器５０によって証明書プロセス及び／又はその後のデータ送信が停止され、プロセス全体が初めからやり直しされる。このことにより、更なる安全性が提供される。

【００３３】

本発明による一実施例においては、サーバ１６は、上述のような中間サーバではなく商業用サーバであってもよい。そのような場合、各データベース６２、６４、等は、各々の

クライアントの金融情報、購買情報や、関連した個人情報などを保持するクライアントのアカウントの記録であってもよい。制御器５０あるいはメモリアクセス制御器７２は、データを特定期間だけ保持するというより、各クライアントが自分のアカウント記録にアクセスするのを制御する。認証器５２、証明書送信機５４、接続メッセージ送信器５６、接続メッセージ受信器５８、及びプロトコル監視器７４は、中間サーバと同じような方法で商業用サーバ上に搭載・実装されてよい。

【００３４】

上述のように、少なくともデータがサーバとクライアントの間で送信されている間、図５に示されるように、サーバとクライアント間のバックグラウンド（背景）通信として、一連のクライアント接続メッセージ（ｍ１、ｍ２、ｍ３、・・・）がサーバに送られ、一連のサーバ接続メッセージ（Ｍ１、Ｍ２、Ｍ３、・・・）がクライアントに送られる。更に安全性を増すために、２種類、あるいは３種類以上の一連の接続メッセージがいずれの方向の通信に用いられてもよい。接続メッセージの各々は、送り主（ソース）、宛先、及び前述のシーケンス情報を含む小さなデータパケットであってもよい。従って、図５に示すように、通信経路に沿って２方向に流れるクライアント接続メッセージ及びサーバ接続メッセージによって、暗号化された送信データが保護される。クライアント接続メッセージ及びサーバ接続メッセージはデータ通信経路の「護衛」あるいは「番犬」として働き、接続メッセージの流れに生じた攪乱は、データ通信経路への不法な干渉を示唆する。攪乱はどちらの側（即ちクライアント及びサーバ側）でも検出できる。クライアント接続メッセージ及びサーバ接続メッセージにより、クライアント及びサーバの自己同一性（身元）を継続的に確認することができる。即ち、データ通信あるいは電子取引を行っている間中、クライアントは正しいクライアントであり、サーバも正しいサーバであることを確認できる。

【００３５】

図６は、本発明の１つの実施例による、通信ネットワーク上でクライアントとサーバの間でデータを安全に送信するための方法を模式的に示す。クライアントはサーバと通信可能なデータ交換モジュールを備えている。データ交換モジュールは、ユーザの識別情報を有するように設定された特定のクライアントにあわせ、特定のユーザ用に設定されている。例えば、データ交換モジュールは、アプリケーションプログラムをクライアントにインストールすることによって設定され、その設定は、クライアント証明書を付与し、クライアント／サーバ接続メッセージ機能やその他の特定のプロトコルの設定を行うことを含む。クライアント及びサーバは、上述の実施例で説明したクライアント１１及びサーバ１６であってもよい。

【００３６】

本発明の１つの実施例によれば、許可されたユーザのみがデータ交換・通信システムにアクセスすることができる。クライアントを使ってデータを送信しようとするユーザは、まず、ユーザ識別（ＩＤ）情報を入力するように促される。入力されたＩＤ情報は、保存された、既に許可されているユーザのＩＤ情報と比較される（ステップ２０２）。例えば、ユーザ名、パスワード、個人情報、ハードウェア用セキュリティ鍵、ユーザの生体情報などの組み合わせを用いて、ユーザの認証を行う。要求されたユーザＩＤ情報がお互いに合致すれば、ユーザは、データ交換・通信システムを使うことが許可される（ステップ２０４）。

【００３７】

たとえば、ユーザがデータ送信リクエストを行うと、ユーザのリクエストに従い、クライアント証明書とデータ送信リクエスト（アップロードリクエスト）がサーバに送られる（ステップ２０６）。データ送信リクエストは少なくとも一人の受信者クライアント／ユーザを特定する。サーバはクライアント証明書を受け取り（ステップ２０８）、そのクライアント証明書が登録されたクライアント証明書の１つと一致するかどうかを決定する（ステップ２１０）。もしクライアント証明書が一致すれば、サーバはクライアントを認証し（ステップ２１２）、クライアント証明書に基づいてサーバ証明書を生成する（ステッ

プ２１４）。サーバはサーバ証明書をクライアントに送信する（ステップ２１６）。サーバ証明書はクライアント証明書の情報を含んでいる。クライアントを認証する際、更なる安全性のため、パスワードやシリアル番号などのクライアントＩＤを併せて用いてもよい。クライアントはサーバ証明書を受け取る（ステップ２１８）。クライアントとサーバの間で各々の証明書を交換することによってクライアントが認証され、更にクライアントはサーバ証明書からサーバの身元を確認できる。

【００３８】

クライアントの認証が済むと、通常クライアントはサーバにログオンする。その後、クライアントとサーバは各々の接続メッセージを送信し始めてもよい（ステップ２２０、２２２）。少なくともデータが送信されている間、一連のクライアント接続メッセージがクライアントからサーバに送られ、一連のサーバ接続メッセージがサーバからクライアントに送られる。

【００３９】

データを送信する時、クライアントは、受け取ったサーバ証明書を送信データに添付し、それらを一緒に暗号化する（ステップ２２４）。例えばＳＳＬプロトコルが暗号化に用いられてもよい。暗号化されたデータ（サーバ証明書を含む）はサーバに送られる（ステップ２２６）。サーバは暗号化されたデータを受け取り、受信者に関連付けられたデータベースに保存する（ステップ２２８）。もし、クライアントからのデータ送信リクエストが２人以上の受信者を特定している場合、送信されたデータは各々の受信者に対応する各データベースに保存される。

【００４０】

図７は、本発明の１つの実施例による、接続メッセージを用いてデータ送信経路を保護するメカニズムを模式的に示している。クライアントがサーバにログオンした後、クライアント及びサーバは各々の接続メッセージを送り始め（図６のステップ２２０、２２２）、クライアントがサーバからログオフするまで送り続ける。接続メッセージの送信は、クライアントとサーバの間の「主」データ送信と平行して行われ、接続メッセージは少なくともデータ送信の開始からその終了までの時間を保護するようにクライアントとサーバの間で交換される。上述のように、一連のクライアント接続メッセージはクライアントに特定のシーケンスあるいはパターンを有し、サーバ接続メッセージも特定のシーケンスあるいはパターンを有している。

【００４１】

図７に示されるように、クライアント接続メッセージはサーバで受け取られ、監視される（ステップ２３０）。もし、クライアント接続メッセージに攪乱が発見された場合（ステップ２３２）、サーバは現在進行中のデータ送信を中止する（ステップ２３４）。接続メッセージの攪乱としては、例えば、接続メッセージの欠損、順序の入れ替わり、予想外の遅れ、等である。攪乱が観察されたり、データ通信が完了する前に中止された場合、サーバは、エラーメッセージをクライアントに送ってもよい（ステップ２３６）。エラーメッセージに応答し、クライアント（のデータ交換モジュール）はデータ送信を停止し、クライアント認証手続きをやり直す。

【００４２】

同様に、クライアントはサーバ接続メッセージを受け取って監視する（ステップ２４０）。もし、サーバ接続メッセージに攪乱が発見された場合（ステップ２４２）、クライアントは現在進行中のデータ送信を中止する（ステップ２４４）。もしデータ送信が中断された場合、クライアントのプロセスはクライアント認証手続きに戻り（図６のステップ２０６）、クライアント証明書がサーバに再送信される。クライアント／サーバ証明書が無事に交換された後、クライアントはデータをサーバに再送信する。

【００４３】

データ送信の停止（中断）、クライアントの再認証、及びデータの再送信は、ユーザが介入することなく、クライアントのデータ送信モジュールとサーバによって自動的に行われてもよい。従って、ユーザがこの再試行プロセスに気づかなかったとしても、システム

は安全無事なデータ送信を確実にする。もし、クライアント／サーバ証明書が繰り返して攪乱され、再試行を所定回数行ってもデータ送信が完了できない場合、データ交換モジュールはユーザに警告メッセージを出してもよい。

【００４４】

上述の例においては、クライアントの認証は証明書交換手続きによって行われている。しかし、本発明の１つの実施例によれば、クライアント証明書及びサーバ証明書を交換する前に、最初のクライアント認証が行われてもよい。例えば、クライアントがユーザ名とパスワードを送ってサーバにログオンし、データ送信を行う前に証明書を互いに交換する。クライアント／サーバ接続メッセージは、証明書交換の前、あるいは証明書交換の後データ送信の前に送り始めてもよい。認証手続き、証明書交換、及び接続メッセージ送信の特定の手順やタイミングは、クライアントに特定のプロトコルとして設定されてもよく、そのようなプロセスの動作シーケンスを監視することにより、クライアント・サーバ通信への外的干渉を検出することができる。もし、動作シーケンスに特定プロトコルからの逸脱が発見された場合、クライアント及び／又はサーバはそのプロセスを停止し、クライアントを再認証し、そして、暗号化されたデータをクライアントからサーバに再送信してもよい。

【００４５】

図８は、本発明の１つの実施例による、受信者（他のクライアント）によるデータの取り出しを模式的に示す。受信者クライアントのユーザがサーバからデータを取り出そうとするとき、その受信者ユーザは、上記と同様の方法（図６のステップ２０２、２０４）によって認証されてもよい（ステップ２５２、２５４）。

【００４６】

受信者ユーザはデータの取り出しをリクエストし、それに応じてデータ取り出し（ダウンロード）リクエストとクライアント証明書がサーバに送られる（ステップ２５６）。サーバはクライアント証明書を受け取り（ステップ２５８）、クライアント証明書が登録されたクライアントの証明書の一つに一致するかどうかを決定する（ステップ２６０）。サーバは、もしクライアント証明書が一致すればクライアントを認証して、クライアントがサーバにログオンすることを許す。サーバは、クライアント証明書に基づいてサーバ証明書を生成してもよく、そのサーバ証明書をクライアントに送信する（図８には示されず）。データ取出しにおいては受信者クライアントはデータをサーバに送信しないため、サーバ証明書をクライアントに送る必要はない。しかし、サーバ証明書は、クライアントにおいてサーバの身元を確認するために用いられてもよい。

【００４７】

更に、保存されていたデータを取り出した後、ログオフする前に、同じセッションで受信者クライアントが更にデータ送信を行いたい場合、その受信者クライアントはサーバにデータ送信のための別のリクエストを送ってもよい。そのような場合、データ送信リクエストと共にクライアント証明書がサーバに再送信され、それを受け取ったサーバは、前述と同様の方法でサーバ証明書を生成してクライアントに送り返してもよい。あるいは、サーバは、そのセッションでクライアントから最初に受け取ったクライアント証明書を保存しておいてもよい。しかし、本発明の１つの実施例によれば、クライアント（の中のデータ交換モジュール）は、同じセッションの中でクライアントがサーバに新しいリクエストを送る度にクライアント証明書を自動的に（ユーザの介入なく）添付する。このことにより、サーバは、（クライアント接続メッセージを受け取ることに加え）クライアントの身元を確認する更なる機会が与えられる。

【００４８】

クライアントが認証されるか、あるいはクライアントがサーバにログオンすると、クライアントとサーバは各々の接続メッセージを送信し始める（ステップ２６４、２６６）。クライアントは、自分自身に関連付けらたデータベースにアクセスすることを許され（ステップ２６８）、その中に保存されている（サーバ証明書を含んだ）暗号化データがサーバからクライアントに送信される（ステップ２７０）。受信者クライアントは受け取った

データを復号する。受信者は、送信者クライアントの情報を含んだサーバ証明書から送信者を確認してもよい。クライアント／サーバ接続メッセージの監視、必要な場合の再認証及び再送信は、図７に記載されたのと同様にして行われる。

【００４９】

本発明による実施例及び応用例が上記よって示され説明されたが、これらの記載から、当業者には、本発明の概念から離脱することなく、上述したよりも更に多くの変更が可能であることが理解される。従って、請求項の記載を除き、本発明を限定すべきではない。

【図面の簡単な説明】

【００５０】

【図１】本発明の態様を実施するのに適したコンピューターシステムを模式的に示す図である。

【図２】本発明の１つの実施例による、通信ネットワーク上のクライアント間でデータを安全に送信するシステムを模式的に示す図である。

【図３】本発明の１つの実施例による、データ交換モジュールを備えたクライアントを模式的に示すブロック図である。

【図４】本発明の１つの実施例によるサーバを模式的に示すブロック図である。

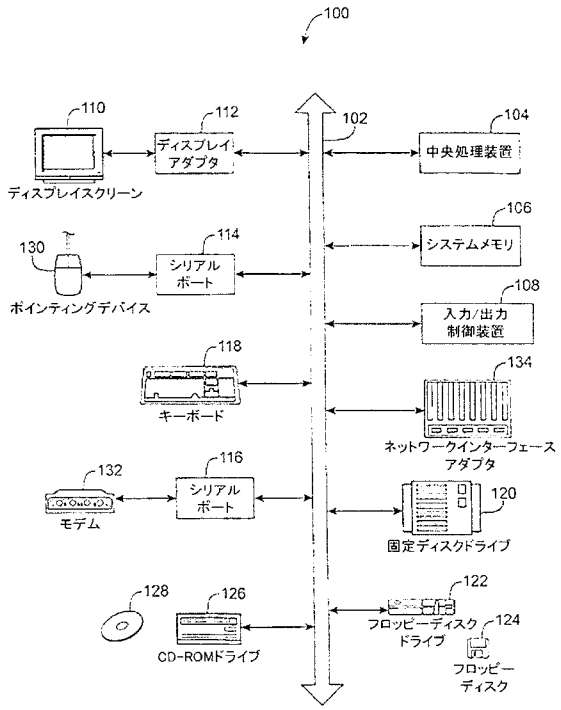
【図５】本発明の１つの実施例による、双方向接続メッセージの流れによる通信経路保護を概念的に示す図である。

【図６】本発明の１つの実施例による、通信ネットワーク上のクライアントとサーバ間でデータを安全に送信する方法を模式的に示すプロセスフローチャートである。

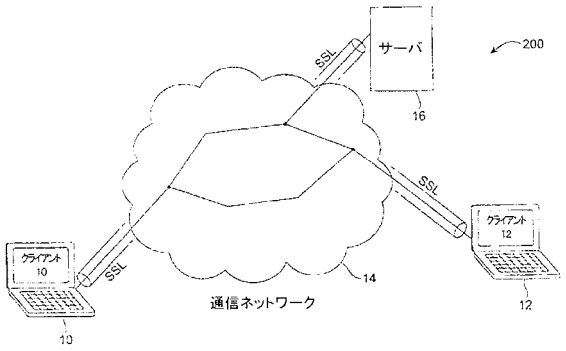
【図７】本発明の１つの実施例による、接続メッセージを用いてデータ通信経路を保護する機構を模式的に示すプロセスフローチャートである。

【図８】本発明の１つの実施例による、受信者クライアントによるサーバからのデータの取り出しを模式的に示すプロセスフローチャートである。

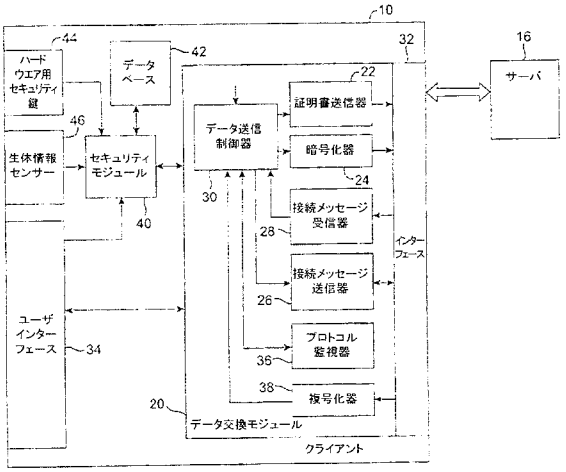
【図１】



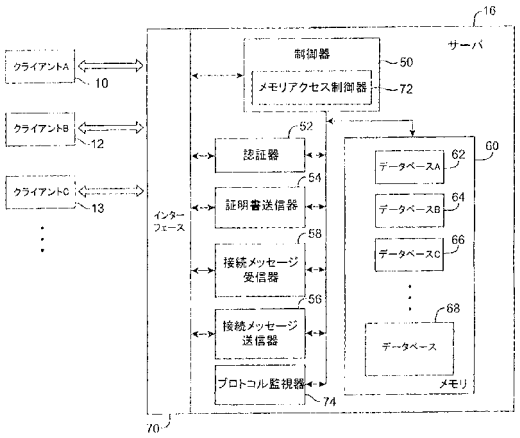
【図２】



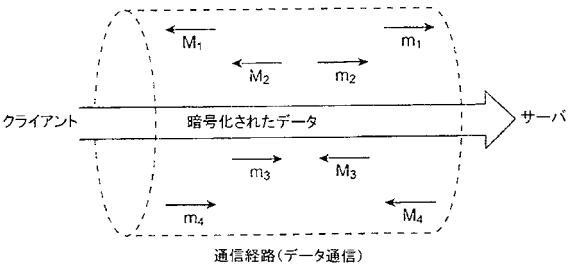
【図３】


10
44
ハードウエア用セキュリティ鍵
データベース
42
32
16
サーバ
22
証明書送信器
データ送信制御器
暗号化器
24
46
生体情報センサー
セキュリティモジュール
40
30
接続メッセージ受信器
28
インターフェース
接続メッセージ送信器
26
ユーザインターフェース
34
プロトコル監視器
36
38
複号化器
20
データ交換モジュール
クライアント

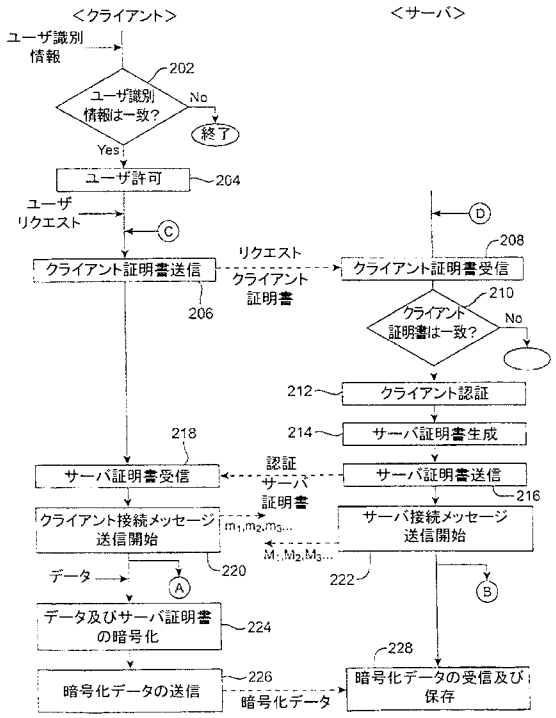
【図４】


16
サーバ
クライアントA
10
クライアントB
12
クライアントC
13
制御器
50
メモリアクセス制御器
72
認証器
52
証明書送信器
54
接続メッセージ受信器
58
接続メッセージ送信器
56
プロトコル監視器
74
インターフェース
60
データベースA
62
データベースB
64
データベースC
66
68
データベース
メモリ
70

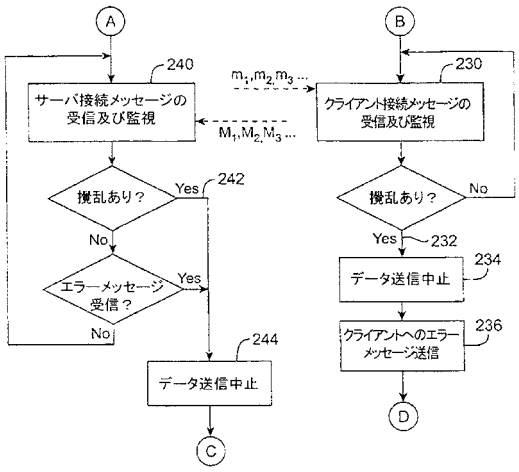
【図５】


M1
m1
M2
m2
クライアント
暗号化されたデータ
サーバ
m3
M3
m4
M4
通信経路(データ通信)

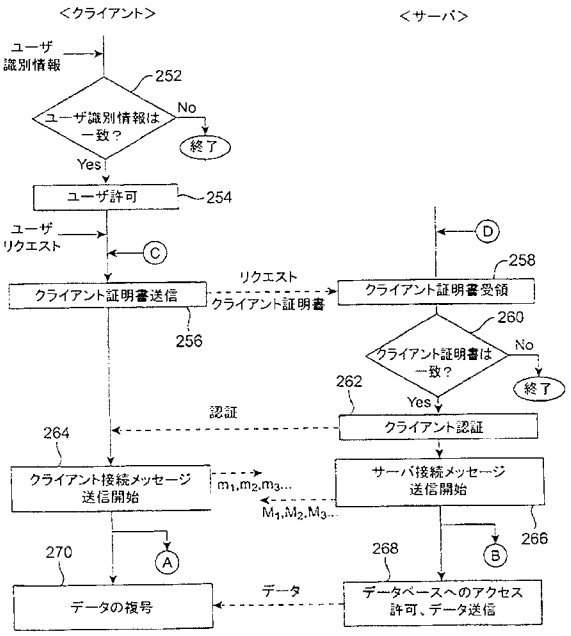
【図６】


<クライアント>
<サーバ>
ユーザ識別情報
202
ユーザ識別情報は一致?
No
終了
Yes
ユーザ許可
204
ユーザリクエスト
C
D
208
リクエスト
クライアント証明書
クライアント証明書送信
クライアント証明書受信
206
210
クライアント証明書は一致?
No
212
クライアント認証
214
サーバ証明書生成
218
認証サーバ証明書
サーバ証明書受信
サーバ証明書送信
216
クライアント接続メッセージ送信開始
m1,m2,m3...
M1,M2,M3...
サーバ接続メッセージ送信開始
データ
220
222
A
B
データ及びサーバ証明書の暗号化
224
228
暗号化データの送信
226
暗号化データ
暗号化データの受信及び保存

【図７】


A
B
240
サーバ接続メッセージの受信及び監視
m1,m2,m3...
M1,M2,M3...
230
クライアント接続メッセージの受信及び監視
攪乱あり?
Yes
242
No
攪乱あり?
No
Yes
232
エラーメッセージ受信?
Yes
No
データ送信中止
234
クライアントへのエラーメッセージ送信
236
244
データ送信中止
C
D

【図８】


<クライアント>
<サーバ>
ユーザ識別情報
252
ユーザ識別情報は一致？
No
終了
Yes
ユーザ許可
254
ユーザリクエスト
C
D
258
クライアント証明書送信
リクエスト
クライアント証明書
クライアント証明書受領
256
260
クライアント証明書は一致？
No
終了
262
Yes
認証
クライアント認証
264
クライアント接続メッセージ送信開始
m1,m2,m3...
M1,M2,M3...
サーバ接続メッセージ送信開始
266
270
A
B
268
データの複号
データ
データベースへのアクセス許可、データ送信

フロントページの続き

審査官　市川　武宜

(56)参考文献　米国特許出願公開第２００４／００５９９０９（ＵＳ，Ａ１）
特開２００４－３６３７３９（ＪＰ，Ａ）
特開２００４－１９４１９６（ＪＰ，Ａ）
特開平０９－２００１９８（ＪＰ，Ａ）
特開平０７－１３１４４９（ＪＰ，Ａ）
特開平１１－０３９２１９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/20
G06F 21/24
G09C 1/00
H04L 9/32