(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4386926号
(P4386926)
(45)発行日　平成21年12月16日(2009.12.16)　(24)登録日　平成21年10月9日(2009.10.9)

(51)Int.Cl.		F I		
H04L 12/56	(2006.01)	H04L	12/56	Z
H04L 12/22	(2006.01)	H04L	12/22	
G06F 13/00	(2006.01)	G06F	13/00	540S
		G06F	13/00	353C

請求項の数 8　(全 21 頁)

(21)出願番号　特願2007-36895(P2007-36895)
(22)出願日　平成19年2月16日(2007.2.16)
(65)公開番号　特開2008-205632(P2008-205632A)
(43)公開日　平成20年9月4日(2008.9.4)
審査請求日　平成20年12月5日(2008.12.5)

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100092152
弁理士　服部　毅巖
(72)発明者　縄手　芳郎
神奈川県川崎市幸区堀川町６６番地２　富士通エルエスアイソリューション株式会社内
(72)発明者　矢嶋　純
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】暗号通信プログラム、暗号通信方法および暗号通信装置

(57)【特許請求の範囲】
【請求項１】
マルチタスク機能を用いてＴＬＳ／ＳＳＬ通信を行う暗号通信プログラムにおいて、
コンピュータを、
１つまたは複数の通信対象装置に複数のユーザのコンテンツデータを送信する場合、コンテンツデータを送信するデータ転送フェーズにおいて、送信する複数の前記コンテンツデータのうち、前記通信対象装置に送信する際に１つの前記コンテンツデータを格納する複数のユーザで共用の送信用通信領域、
前記データ転送フェーズにおいて複数の前記コンテンツデータのうち前記送信用通信領域を独占する排他制御により、前記送信用通信領域に格納された前記コンテンツデータを前記通信対象装置に送信する制御を行う排他制御手段、
前記送信用通信領域より大きく、ユーザ毎に設けられた複数の送受信兼用通信領域、
前記コンテンツデータの送信方法に関する取り決めと対向ユーザの認証を行うハンドシェイクフェーズにおいて前記通信対象装置に送信するユーザ毎のメッセージを生成し、生成した前記メッセージを前記各送受信兼用通信領域に格納するメッセージ生成手段、
前記各送受信兼用通信領域に格納された前記メッセージをそれぞれ送信する送信手段、
として機能させることを特徴とする暗号通信プログラム。
【請求項２】
前記送受信兼用通信領域はシステムメモリ内に設けられていることを特徴とする請求項１記載の暗号通信プログラム。

【請求項３】
前記送受信兼用通信領域は、ネットワーク接続用インタフェース内に設けられていることを特徴とする請求項１記載の暗号通信プログラム。
【請求項４】
コンピュータのマルチタスク機能を用いてＴＬＳ／ＳＳＬ通信を行う暗号通信方法において、
排他制御手段が、１つまたは複数の通信対象装置に複数のユーザのコンテンツデータを送信する場合、データ転送フェーズにおいて複数の前記コンテンツデータのうち、前記通信対象装置に送信する際に１つの前記コンテンツデータを格納する複数のユーザで共用の送信用通信領域を独占する排他制御により、前記送信用通信領域に格納された前記コンテンツデータを前記通信対象装置に送信する制御を行い、
メッセージ生成手段が、ハンドシェイクフェーズにおいて前記通信対象装置に送信するユーザ毎のメッセージを生成し、生成した前記メッセージを前記送信用通信領域より大きく、ユーザ毎に設けられた複数の送受信兼用通信領域に格納し、
送信手段が、前記各送受信兼用通信領域に格納された前記メッセージをそれぞれ送信する、
ことを特徴とする暗号通信方法。
【請求項５】
マルチタスク機能を用いてＴＬＳ／ＳＳＬ通信を行う暗号通信装置において、
１つまたは複数の通信対象装置に複数のユーザのコンテンツデータを送信する場合、データ転送フェーズにおいて、送信する複数の前記コンテンツデータのうち、前記通信対象装置に送信する際に１つの前記コンテンツデータを格納する複数のユーザで共用の送信用通信領域と、
前記データ転送フェーズにおいて複数の前記コンテンツデータのうち前記送信用通信領域を独占する排他制御により、前記送信用通信領域に格納された前記コンテンツデータを前記通信対象装置に送信する制御を行う排他制御手段と、
前記送信用通信領域より大きく、ユーザ毎に設けられた複数の送受信兼用通信領域と、
ハンドシェイクフェーズにおいて前記通信対象装置に送信するユーザ毎のメッセージを生成し、生成した前記メッセージを前記各送受信兼用通信領域に格納するメッセージ生成手段と、
前記各送受信兼用通信領域に格納された前記メッセージをそれぞれ送信する送信手段と、
を有することを特徴とする暗号通信装置。
【請求項６】
マルチタスク機能を用いてＴＬＳ／ＳＳＬ通信を行う暗号通信プログラムにおいて、
コンピュータを、
１つまたは複数の通信対象装置に複数のユーザのコンテンツデータを送信するデータ転送フェーズにおいて、送信する複数の前記コンテンツデータのうち、前記通信対象装置に送信する際に１つの前記コンテンツデータを格納する複数のユーザで共用の送信用通信領域、
前記コンテンツデータを送信するフェーズにおいて複数の前記コンテンツデータのうち前記送信用通信領域を独占する排他制御により、前記送信用通信領域に格納された前記コンテンツデータを前記通信対象装置に送信する制御を行う排他制御手段、
前記送信用通信領域より大きく、ユーザ毎に設けられた複数の送受信兼用通信領域、
前記コンテンツデータの送信方法に関する取り決めを行うフェーズにおいて前記通信対象装置に送信するユーザ毎のメッセージを生成し、生成した前記メッセージを前記各送受信兼用通信領域に格納するメッセージ生成手段、
前記各送受信兼用通信領域に格納された前記メッセージをそれぞれ送信する送信手段、
として機能させることを特徴とする暗号通信プログラム。
【請求項７】

前記送受信兼用通信領域は、システムメモリ内に設けられていることを特徴とする請求項６記載の暗号通信プログラム。

【請求項８】

前記送受信兼用通信領域は、ネットワーク接続用インタフェース内に設けられていることを特徴とする請求項６記載の暗号通信プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は暗号および認証などのセキュリティ技術を利用した暗号通信プログラム、暗号通信方法および暗号通信装置に関し、特に、安全な情報通信の規格であるＴＬＳ（Transport Layer Security）やＳＳＬ（Secure Socket Layer）をマルチタスク向けに実現する暗号通信プログラム、暗号通信方法および暗号通信装置に関する。

【背景技術】

【０００２】

ネットワーク上で第三者による「盗聴」「改竄」「なりすまし」といったトラブルを回避するための暗号化通信方法の１つとして、ＴＬＳ／ＳＳＬ通信が知られている。ＴＬＳ／ＳＳＬ通信は、ハンドシェイクフェーズとデータ転送フェーズとを有し、ハンドシェイクフェーズでは対向サーバ／クライアント間で、認証並びに暗号化方式とその鍵とのネゴシエーションを行い、データ転送フェーズでは認証済みの対向サーバ／クライアントとその合意された暗号化方式と鍵とを使用して情報を暗号化してやりとりする。この通信の特徴としては、ハンドシェイクフェーズでは、公開鍵暗号方式の使用、対向サーバ／クライアントの認証および対向サーバ／クライアントからの応答待ちの動作のため処理が遅く、逆にデータ転送フェーズでは、ユーザが転送するコンテンツを共通鍵暗号方式で一方的に送りつけるだけなので処理が速い。

【０００３】

マルチタスクとは、１台のコンピュータで同時に複数の処理を並行して行う機能である。ユーザが対向サーバ／クライアントとマルチタスク向けＴＬＳ／ＳＳＬ通信を実施する場合、受信にはユーザ毎に設けられた受信専用バッファ領域を使用し、送信にはユーザ毎に設けられた送信専用バッファ領域を使用するのが一般的である。実用的にユーザ毎の送信用バッファ領域は、１ＫＢ～２ＫＢ程度に削減することができる。一方、ユーザ毎の受信用バッファ領域は、ＴＬＳ／ＳＳＬ通信における下記の規約上の制限により、そのサイズが１６ＫＢ強に保持されているのが一般的である。

【０００４】

＜規約上の制限＞

ＴＬＳ／ＳＳＬ通信では、データ転送フェーズにおいて対向サーバ／クライアントから送信されるコンテンツデータを、ＭＡＣ値検証可能である暗号化されたレコードという単位のデータに変換する。

【０００５】

図１３は、暗号化されたレコードを示す図である。

レコード９０は、ヘッダ９１と、コンテンツデータ９２と、ＭＡＣ値９３と、パディング部９４とを有している。

【０００６】

ＭＡＣ値検証とは、メッセージが改竄されていないオリジナルそのものか否かを、ハッシュ関数をもとに処理した値で検証するものである。ところが、ＴＬＳ／ＳＳＬ通信の規約により、レコードの全部を受信しなければ、そのレコードに対するＭＡＣ値検証は実行できない。このことにより、受信用バッファ領域は、レコード単位の最大サイズである１６ＫＢ強に保持する必要がある。

【０００７】

また、以下の仕組み上の制限も存在する。

＜仕組み上の制限＞
ユーザの要求データ量と対向サーバ／クライアントが送信するデータ量との関係が独立しているため、マルチユーザで受信用バッファ領域を共用するとマルチユーザ同士で対向ユーザからのデータを消し合う（他のユーザのデータを上書きしてしまう）事態が起こる。このため、受信用バッファ領域は必ずユーザ毎に設けなければならない。
【０００８】
ところで、メモリサイズが制限されている組み込み機器でＴＬＳ／ＳＳＬ通信を実装する場合、メモリサイズをできるだけ小さくしたいという要求が存在する（例えば、特許文献１参照）。特に受信用バッファ領域と送信用バッファ領域とをそれぞれ小さくすることによるメモリサイズの削減要求に対応する効果は大きい。このため、前述したＴＬＳ／ＳＳＬ通信の規約上の制限と仕組み上の制限に準拠し、パフォーマンス面での大きな低下を阻止して、より小さなメモリサイズでマルチタスク向けＴＬＳ／ＳＳＬ通信を実装することが要求されている。
【０００９】
ここで、前述したように、受信用バッファ領域は、ＴＬＳ／ＳＳＬ通信の規約上の制限と仕組み上の制限に準拠するため、必ずユーザ毎に１６ＫＢ強を保持しなければならない。
【特許文献１】特開２００２－３５１８３５号公報
【発明の開示】
【発明が解決しようとする課題】
【００１０】
ところで、送信用バッファ領域は、データ送信がユーザ主体であることを考慮すれば、同時に２ユーザが使用しないように排他制御を用いることにより、全ユーザで共用することができる。この場合、データ転送フェーズは、ユーザが転送したいコンテンツを一方的に送りつけるだけであり、処理も高速である。したがって、排他制御を用いて複数のユーザで共用した送信用バッファ領域を使用して、各ユーザのデータ転送フェーズを実行しても、全体として大きなパフォーマンスの低下は許容できる範囲である。
【００１１】
しかしながら、ハンドシェイクフェーズは、その処理が遅いため、あるユーザがメッセージ送信中のとき、共用送信用バッファ領域を独占してしまい、そのユーザ以外のユーザが送信できないという事態が生じ、全体としての大きなパフォーマンスが低下するという問題がある。本発明はこのような点に鑑みてなされたものであり、パフォーマンスの低下を防止しつつ、使用メモリ領域の低減を図ることができる暗号通信プログラム、暗号通信方法および暗号通信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】
【００１２】
本発明では上記問題を解決するために、図１に示すような処理をコンピュータ１に実行させるための暗号通信プログラムが提供される。
本発明に係る暗号通信プログラムは、マルチタスク機能を用いてＴＬＳ／ＳＳＬ通信を行うプログラムである。
【００１３】
この暗号通信プログラムを実行するコンピュータ１は以下の機能を有する。
送信用通信領域２は、コンピュータ１内に複数のユーザ共用で設けられており、通信対象装置３に複数のユーザのデータ転送フェーズにおいて、転送する複数のコンテンツデータのうち、通信対象装置３に転送する際に１つのコンテンツデータを格納する。
【００１４】
排他制御手段４は、データ転送フェーズにおいて複数のコンテンツデータのうち送信用通信領域２に格納されたコンテンツデータのみを通信対象装置３に転送する制御を行う。
送受信兼用通信領域５ａ、５ｂは、ユーザ毎に設けられており、送信用通信領域２より大きく設定されている。

【００１５】
メッセージ生成手段６は、ハンドシェイクフェーズにおいて通信対象装置３に送信するユーザ毎のメッセージを生成し、生成したメッセージを送受信兼用通信領域５ａ、５ｂに格納する。
【００１６】
送信手段７は、送受信兼用通信領域５ａ、５ｂに格納されたメッセージの送信をそれぞれ行う。
このような暗号通信プログラムによれば、ハンドシェイクフェーズにおいてメッセージ生成手段６により、通信対象装置３に送信するユーザ毎のメッセージが生成され、生成されたメッセージが送受信兼用通信領域５ａ、５ｂに格納される。送信手段７により、送受信兼用通信領域５ａ、５ｂに格納されたメッセージの送信が行われる。
【００１７】
また、通信対象装置３に複数のユーザのコンテンツデータを転送する場合、データ転送フェーズにおいて、送信用通信領域２により、１つのコンテンツデータが格納され、排他制御手段４により、送信用通信領域２に格納されたコンテンツデータのみが通信対象装置３に転送される制御が行われる。
【発明の効果】
【００１８】
本発明によれば、データ転送フェーズにおいては、処理速度が速いため、排他制御を利用して複数のユーザ共用の送信用通信領域を用いてデータ通信を行ってもパフォーマンスの低下を防止することができる。また、ハンドシェイクフェーズにおいては、ユーザ毎に設けられた送受信兼用通信領域を用いてメッセージの送信を行うようにしたので、あるユーザがメッセージ送信中のときに、通信領域が独占されることがない。これにより、パフォーマンスの低下を防止しつつ、全体として通信領域の低減を図ることができる。
【発明を実施するための最良の形態】
【００１９】
以下、本発明の実施の形態を、図面を参照して詳細に説明する。
まず、本発明の概要について説明し、その後、実施の形態を説明する。
図１は、本発明の概要を示す図である。
【００２０】
本発明の暗号通信プログラムは、暗号通信プログラムを実行するコンピュータ１を、送信用通信領域２、排他制御手段４、送受信兼用通信領域５ａ、５ｂ、メッセージ生成手段６および送信手段７として機能させることができる。
【００２１】
送信用通信領域２は、コンピュータ１内に複数のユーザ共用で設けられており、通信対象装置３に複数のユーザのデータ転送フェーズにおいて、転送する複数のコンテンツデータのうち、通信対象装置３に転送する際に１つのコンテンツデータを格納する。
【００２２】
排他制御手段４は、データ転送フェーズにおいて複数のコンテンツデータのうち送信用通信領域２に格納されたコンテンツデータのみを通信対象装置３に転送する制御を行う。
送受信兼用通信領域５ａ、５ｂは、ユーザ毎に設けられており、各容量が送信用通信領域２より大きく設定されている。
【００２３】
メッセージ生成手段６は、ハンドシェイクフェーズにおいて通信対象装置３に送信するユーザ毎のメッセージを生成し、生成したメッセージを送受信兼用通信領域５ａ、５ｂに格納する。
【００２４】
送信手段７は、送受信兼用通信領域５ａ、５ｂに格納されたメッセージの送信をそれぞれ行う。
このような暗号通信プログラムによれば、ハンドシェイクフェーズにおいてメッセージ

生成手段６により、通信対象装置３に送信するユーザ毎のメッセージが生成され、生成されたメッセージが送受信兼用通信領域５ａ、５ｂに格納される。送信手段７により、送受信兼用通信領域５ａ、５ｂに格納されたメッセージの送信が行われる。

【００２５】

また、通信対象装置３に複数のユーザのデータ転送フェーズにおいて、送信用通信領域２により、１つのコンテンツデータが格納され、排他制御手段４により、送信用通信領域２に格納されたコンテンツデータのみが通信対象装置３に転送される制御が行われる。

【００２６】

以下、本発明の実施の形態を説明する。

図２は、実施の形態のシステムを示すブロック図である。

本実施の形態のシステムは、クライアント装置（コンピュータ）１００と、サーバ装置（通信対象装置）２００とがネットワーク１０を介して接続されている。

【００２７】

クライアント装置１００とサーバ装置２００とはデータの送受信を行う際に以下の要領でＴＬＳ／ＳＳＬ通信を行う。

（１）クライアント装置１００は、通信データの暗号化に使用可能な暗号の種類をサーバ装置２００に通知し、クライアント装置１００およびサーバ装置２００が使用する共通鍵暗号を選択する。

【００２８】

（２）サーバ装置２００が、署名付き公開鍵証明書を送信する。

（３）クライアント装置１００は、インポートされているルート証明書で署名を確認し、サーバ装置２００を認証する。

【００２９】

（４）クライアント装置１００は、暗号用の共通鍵を生成し、サーバ装置２００の公開鍵で暗号化して送る。

（５）サーバ装置２００は、自らの秘密鍵で復号化して、共通鍵を取り出す。

【００３０】

（６）クライアント装置１００およびサーバ装置２００は、それぞれ共通鍵を用いて、暗号化通信を開始する。

以上のクライアント装置１００およびサーバ装置２００の認証や暗号化方式とその鍵のネゴシエーションは、ハンドシェイクフェーズで行い、ハンドシェイクフェーズで取り決めた暗号化方式と鍵を用いてデータ転送フェーズを行う。

【００３１】

図３は、ハンドシェイクフェーズを説明する図である。

＜ハンドシェイクフェーズ＞

ハンドシェイクフェーズにおいて、クライアント装置１００は、Ｃｌｉｅｎｔ Ｈｅｌｌｏメッセージをサーバ装置２００に送信する（ステップＳ１）。

【００３２】

サーバ装置２００は、Ｃｌｉｅｎｔ Ｈｅｌｌｏメッセージを受信して、Ｓｅｒｖｅｒ Ｈｅｌｌｏメッセージ、Ｓｅｒｖｅｒ Ｃｅｒｔｉｆｉｃａｔｅメッセージ、Ｓｅｒｖｅｒ Ｋｅｙ Ｅｘｃｈａｎｇｅメッセージ、Ｃｅｒｔｉｆｉｃａｔｅ ＲｅｑｕｅｓｔメッセージおよびＳｅｒｖｅｒ Ｈｅｌｌｏ Ｄｏｎｅメッセージをクライアント装置１００に送信する（ステップＳ２）。

【００３３】

クライアント装置１００は、これらのメッセージを受信して、Ｃｌｉｅｎｔ Ｃｅｒｔｉｆｉｃａｔｅメッセージ、Ｃｌｉｅｎｔ Ｋｅｙ Ｅｘｃｈａｎｇｅメッセージ、Ｃｅｒｔｉｆｉｃａｔｅ Ｖｅｒｉｆｙメッセージ、Ｃｈａｎｇｅ Ｃｉｐｈｅｒ ＳｐｅｃメッセージおよびＦｉｎｉｓｈｅｄメッセージをサーバ装置２００に送信する（ステップＳ３）。

【００３４】

サーバ装置２００は、これらのメッセージを受信して、Ｃｈａｎｇｅ Ｃｉｐｈｅｒ Ｓｐｅｃメッセージおよび Ｆｉｎｉｓｈｅｄメッセージをクライアント装置１００に送信する（ステップＳ４）。

【００３５】

クライアント装置１００は、これらのメッセージを受信すると、ハンドシェイクフェーズを終了する（ステップＳ５）。なお、図３中メッセージの語尾にアスタリスク（＊）を付したメッセージは、オプショナルメッセージであり、常に送信される訳ではない。

【００３６】

以下、図中のメッセージについて説明する。

Ｃｌｉｅｎｔ Ｈｅｌｌｏメッセージは、クライアント装置１００が、最初にサーバ装置２００に接続するときや、Ｈｅｌｌｏ Ｒｅｑｕｅｓｔをサーバ装置２００から受け取ったときや、既存のコネクションにおいて暗号化パラメータ等を変更するときにサーバ装置２００へ送信するメッセージである。内容は使用される暗号化方式やデータの圧縮方式に関する候補のリストなどである。このＣｌｉｅｎｔ Ｈｅｌｌｏメッセージは、リプレイ攻撃（以前に正規ユーザ間で交わされた通信内容を再利用することで通信相手を欺く、という攻撃方法）を防ぐための一回限りの乱数データを含む。

【００３７】

Ｓｅｒｖｅｒ Ｈｅｌｌｏメッセージは、Ｃｌｉｅｎｔ Ｈｅｌｌｏメッセージに対するサーバ装置２００の応答メッセージであり、サーバ装置２００が独自に生成したＣｌｉｅｎｔ Ｈｅｌｌｏメッセージとは異なる一回限りの乱数データを含む。クライアント装置１００がサポートする暗号化処理／圧縮アルゴリズムのリストの中から選んだアルゴリズムが用いられる。

【００３８】

Ｓｅｒｖｅｒ Ｃｅｒｔｉｆｉｃａｔｅメッセージは、サーバ装置２００からクライアント装置１００に送られるメッセージである。サーバ装置２００は自分の証明書をこのメッセージを使用してクライアント装置１００に送付する。また、ここにはその証明書を発行した認証局の証明書や、さらに上位の認証局があればその証明書といった形で、ルート認証局までの証明書チェーンを含んだリスト形式で送信されることがある。

【００３９】

Ｓｅｒｖｅｒ Ｋｅｙ Ｅｘｃｈａｎｇｅメッセージは、サーバ装置２００が証明書を持っていない場合、または持っていても署名にしか使用できない場合に、サーバ装置２００からクライアント装置１００に送信されるメッセージである。

【００４０】

Ｃｅｒｔｉｆｉｃａｔｅ Ｒｅｑｕｅｓｔメッセージは、クライアント認証を行う際に、サーバ装置２００からクライアントの証明書の提示を要求するためのメッセージである。このメッセージに、サーバ装置２００が信頼する認証局のリストが付加されている。

【００４１】

Ｓｅｒｖｅｒ Ｈｅｌｌｏ Ｄｏｎｅメッセージは、サーバ装置２００からクライアント装置１００に向けた鍵交換をサポートする一連のメッセージが送信されたことをクライアント装置１００に通知するためのメッセージである。

【００４２】

Ｃｌｉｅｎｔ Ｃｅｒｔｉｆｉｃａｔｅメッセージは、クライアント認証を行う場合にクライアント装置１００が自分の証明書をサーバ装置２００に送信するためのメッセージである。データの形式はＳｅｒｖｅｒ Ｃｅｒｔｉｆｉｃａｔｅメッセージと同様である。

【００４３】

Ｃｌｉｅｎｔ Ｋｅｙ Ｅｘｃｈａｎｇｅメッセージは、セッションで暗号化のために使用される鍵（セッションキー）などのセキュリティパラメターを生成するときに使用されるマスタシークレットを生成する元になるプリマスタシークレットデータをクライアント装置１００から送信するためのメッセージである。例えばＲＳＡの場合、プリマスタシ

ークレットデータはサーバの公開鍵で暗号化される。

【００４４】

Ｃｅｒｔｉｆｉｃａｔｅ　Ｖｅｒｉｆｙメッセージは、サーバ装置２００がクライアントの認証を行うために必要なデータを送信するメッセージである。具体的には双方が既知のこれまでやり取りしたハンドシェイクフェーズにおけるメッセージのハッシュ値をとり、クライアントの秘密鍵で暗号化したものである。サーバ装置２００でこれをクライアントの公開鍵で復号し、同じように取得したハッシュ値と比較することで検証を行う。

【００４５】

Ｃｈａｎｇｅ　Ｃｉｐｈｅｒ　Ｓｐｅｃメッセージは、ハンドシェイクフェーズで決定した暗号化仕様やセキュリティパラメターの利用開始を相手に知らせるメッセージである。

【００４６】

Ｆｉｎｉｓｈｅｄメッセージは、これまでにネゴシエーションされた暗号仕様、鍵およびシークレットで保護される最初のメッセージであり、クライアント装置１００、サーバ装置２００双方とも、ネゴシエーションが正常に行われたことを相手に知らせるためのメッセージである。

【００４７】

ハンドシェイクフェーズでは、公開鍵暗号方式の使用、認証、応答待ちの動作のため、処理が遅い。以下、ハンドシェイクフェーズで使用されるこれらのメッセージを「ハンドシェイクメッセージ」という。

【００４８】

図４は、データ転送フェーズを説明する図である。

データ転送フェーズにおいて、クライアント装置１００からサーバ装置２００にデータを送信する場合は、クライアント装置１００は、送信するデータを暗号化して暗号化データ（レコード）を生成し、生成した暗号化データを送信する。サーバ装置２００は、暗号化データを受信し、復号してデータを得る。

【００４９】

サーバ装置２００からクライアント装置１００にデータを送信する場合は、サーバ装置２００は、送信するデータを暗号化し、暗号化データを送信する。クライアント装置１００は、暗号化データを受信し、復号してデータを得る。

【００５０】

データ転送フェーズでは、共通鍵暗号方式を使用し、送信したいデータを暗号化して一方的に送りつけるだけなので、ハンドシェイクフェーズに比べ処理速度は速い。

以下、このようなデータの送受信に使用するデータ格納領域について詳しく説明する。

【００５１】

図５は、クライアント装置のハードウェア構成例を示す図である。

クライアント装置１００は、ＣＰＵ（Central Processing Unit）１０１によって装置全体が制御されている。ＣＰＵ１０１には、バス１０７を介してシステムメモリ（System Memory）１０２、ハードディスクドライブ（ＨＤＤ:Hard Disk Drive）１０３、グラフィック処理装置１０４、およびイーサネット（登録商標）接続用ＬＳＩ（Ｅｔｈｅ　Ｃｏｎｎｅｃｔ　ＬＳＩ）１０６が接続されている。

【００５２】

システムメモリ１０２には、ＣＰＵ１０１に実行させるマルチタスク向けＯＳ（Operating System）のプログラムやアプリケーションプログラムの少なくとも一部が一時的に格納される。また、システムメモリ１０２には、ＣＰＵ１０１による処理に必要な各種データ等が格納される。ＨＤＤ１０３には、ＯＳやアプリケーションプログラムが格納される。また、ＨＤＤ１０３内には、プログラムファイルが格納される。

【００５３】

グラフィック処理装置１０４には、モニタ１１が接続されている。グラフィック処理装置１０４は、ＣＰＵ１０１からの命令に従って、画像をモニタ１１の画面に表示させる。

イーサネット接続用ＬＳＩ１０６は、ネットワーク１０に接続されている。イーサネット接続用ＬＳＩ１０６は、ネットワーク１０を介して、サーバ装置２００との間でデータの送受信を行う。

【００５４】

以上のようなハードウェア構成によって、本実施の形態の処理機能を実現することができる。なお、図５にはクライアント装置１００のハードウェア構成を示したがサーバ装置２００についても同様のハードウェア構成で実現することができる。このようなハードウェア構成のシステムにおいて暗号化データ通信を行うために、クライアント装置１００内には、以下のような機能が設けられる。

【００５５】

図６は、クライアント装置の機能を示すブロック図である。

以下、一例としてユーザＡ（マルチユーザＡ）、ユーザＢ（マルチユーザＢ）が、クライアント装置１００を介してサーバ装置２００との間でＴＬＳ／ＳＳＬ通信を行う場合について説明する。

【００５６】

クライアント装置１００のシステムメモリ１０２は、ユーザＡ用送受信バッファ領域１０２ａと、ユーザＢ用送受信バッファ領域１０２ｂと、兼用送信バッファ領域１０２ｃとを有している。

【００５７】

ユーザＡ用送受信バッファ領域１０２ａは、ユーザＡに割り当てられる受信兼ハンドシェイク送信用のバッファ領域を有している。

ユーザＢ用送受信バッファ領域１０２ｂは、ユーザＢに割り当てられる受信兼ハンドシェイク送信用のバッファ領域を有している。

【００５８】

兼用送信バッファ領域１０２ｃは、ユーザＡおよびユーザＢ共用の送信用バッファ領域を有している。これら各バッファ領域は、後述するシステムの動作によってシステムメモリ１０２内に確保される。

【００５９】

なお、兼用送信バッファ領域１０２ｃは、例えば１ＫＢ～２ＫＢ程度に設定される。また、受信兼ハンドシェイク送信用バッファ領域は１６ＫＢ強に設定される。

また、イーサネット接続用ＬＳＩ１０６は、それぞれ少なくとも１つの送信部（送信専用通信ブロック）１０６ａと受信部（受信専用通信ブロック）１０６ｂとを有している。

【００６０】

図７は、ＣＰＵの機能を示すブロック図である。

ＣＰＵ１０１は、ユーザアプリケーション層１０１ａと、ＴＬＳ／ＳＳＬ層１０１ｂと、ＴＣＰ／ＩＰ層１０１ｃとを有している。

【００６１】

ユーザアプリケーション層１０１ａは、ＴＣＰ／ＩＰの最上位に位置し、各種サービス毎に、異なるプロトコルのやり取りを実現する。

ＴＬＳ／ＳＳＬ層１０１ｂは、ユーザアプリケーション層１０１ａ直下の層であり、データの暗号化を実行する。また、ＴＬＳ／ＳＳＬ層１０１ｂは、認証機関の発行するディジタル証明書に基づいて、サーバ装置２００やクライアント装置１００の正当性を保証する。

【００６２】

ＴＣＰ／ＩＰ層１０１ｃは、サーバ装置２００に渡すべきデータを示す情報や、パケットの状態を管理する。

次に、ハンドシェイクフェーズおよびデータ転送フェーズにおけるシステムの動作を説明する。

【００６３】

図８は、ハンドシェイクフェーズの動作を示すシーケンス図である。

まず、ユーザアプリケーション層１０１ａが、兼用送信バッファ領域１０２ｃ（２ＫＢ）とマルチユーザ数分の受信兼ハンドシェイク送信用バッファ領域（各１６ＫＢ）をシステムメモリ１０２に確保し、各ユーザに割り当てる（ステップＳ１１）。本実施の形態では、ユーザＡ用送受信バッファ領域１０２ａと、ユーザＢ用送受信バッファ領域１０２ｂとを割り当てるため、その容量は１６×２＝３２ＫＢとなる。

【００６４】

次に、ユーザアプリケーション層１０１ａが、ＴＬＳ／ＳＳＬ層１０１ｂにハンドシェイク開始指示を送る（ステップＳ１２）。

ハンドシェイク開始指示を受け取ったＴＬＳ／ＳＳＬ層１０１ｂは、ステップＳ１１で各ユーザに割り当てられた受信兼ハンドシェイク送信用バッファ領域を指定する（ステップＳ１３）。具体的には、ユーザＡが送受信するデータの格納領域：ユーザＡ用送受信バッファ領域１０２ａ、ユーザＢが送受信するデータの格納領域：ユーザＢ用送受信バッファ領域１０２ｂとする。なお、図８で、ブロックがＴＬＳ／ＳＳＬ層１０１ｂとＴＣＰ／ＩＰ層１０１ｃに跨っているのは、ＴＬＳ／ＳＳＬ層１０１ｂでの決定事項がＴＣＰ／ＩＰ層１０１ｃにも反映されることを示している。（以下も同様）。

【００６５】

次に、ＴＬＳ／ＳＳＬ層１０１ｂは、サーバ装置２００に送信するハンドシェイクメッセージ等のハンドシェイク用データを作成し、ユーザＡ用送受信バッファ領域１０２ａおよびユーザＢ用送受信バッファ領域１０２ｂに格納する（ステップＳ１４）。

【００６６】

次に、ＴＬＳ／ＳＳＬ層１０１ｂは、送信部１０６ａの制御権を獲得する（排他制御）（ステップＳ１５）。

次に、ＴＬＳ／ＳＳＬ層１０１ｂは、ＴＣＰ／ＩＰ層１０１ｃにユーザＡ用送受信バッファ領域１０２ａおよびユーザＢ用送受信バッファ領域１０２ｂのいずれか一方に格納されたハンドシェイク用データ（以下、一例としてユーザＡ用送受信バッファ領域１０２ａに格納されたハンドシェイク用データ）の送受信指示を送る（ステップＳ１６）。

【００６７】

ＴＣＰ／ＩＰ層１０１ｃは、ＴＬＳ／ＳＳＬ層１０１ｂからの送受信指示を受け取ると、イーサネット接続用ＬＳＩ１０６に送受信指示を送る（ステップＳ１７）。

イーサネット接続用ＬＳＩ１０６は、送受信指示を受け取ると、サーバ装置２００との間でハンドシェイクメッセージの交換を行う（ステップＳ１８）。

【００６８】

イーサネット接続用ＬＳＩ１０６は、ハンドシェイクメッセージの交換が終了すると、受信通知をＴＣＰ／ＩＰ層１０１ｃに送る（ステップＳ１９）。

ＴＣＰ／ＩＰ層１０１ｃは、受信通知を受け取ると、ＴＬＳ／ＳＳＬ層１０１ｂに受け取った受信通知を送る（ステップＳ２０）。

【００６９】

ＴＬＳ／ＳＳＬ層１０１ｂは、ＴＣＰ／ＩＰ層１０１ｃからの受信通知を受け取ると、送信専用通信ブロックの制御権を開放する（排他制御）（ステップＳ２１）。

次に、ＴＬＳ／ＳＳＬ層１０１ｂは、受信したハンドシェイク用データをユーザＡ用送受信バッファ領域１０２ａに格納する（ステップＳ２２）。

【００７０】

次に、ＴＬＳ／ＳＳＬ層１０１ｂは、認証並びに暗号化方式とその鍵とのネゴシエーション（データ処理）を行う（ステップＳ２３）。

ハンドシェイクフェーズでは、ステップＳ１３～Ｓ２３の動作をユーザ毎に繰り返し行う（図８中点線内）。

【００７１】

ハンドシェイクフェーズの終了時にＴＬＳ／ＳＳＬ層１０１ｂは、ハンドシェイク終了指示をユーザアプリケーション層１０１ａに送る（ステップＳ２４）。

ハンドシェイクフェーズの終了後、ＣＰＵ１０１は、データ転送フェーズを開始する。

【００７２】
図９は、データ転送フェーズの動作を示すシーケンス図である。
まず、送信対象のコンテンツデータを受け取ると、ユーザアプリケーション層１０１ａは、ＴＬＳ／ＳＳＬ層１０１ｂに暗号通信指示を送る（ステップＳ３１）。
【００７３】
ＴＬＳ／ＳＳＬ層１０１ｂは、送信する暗号化レコードの格納領域を兼用送信バッファ領域１０２ｃに指定し、ユーザＡの暗号化レコードを受信する格納領域をユーザＡ用送受信バッファ領域１０２ａに指定し、ユーザＢの暗号化レコードを受信する格納領域をユーザＢ用送受信バッファ領域１０２ｂに指定する（ステップＳ３２）。
【００７４】
次に、ＴＬＳ／ＳＳＬ層１０１ｂは、兼用送信バッファ領域１０２ｃの制御権を獲得する（排他制御）（ステップＳ３３）。なお、ＴＬＳ／ＳＳＬ層１０１ｂが、ユーザアプリケーション層１０１ａに排他制御指示を送り、ユーザアプリケーション層１０１ａが、排他制御を行うようにしてもよい。
【００７５】
このとき、プロセス間で交換される信号(セマフォ)から使用を制限する割り込み処理制御機能の排他制御を用いて、兼用送信バッファ領域１０２ｃで転送フェーズでのコンテンツデータの送信を行う（ステップＳ３４～Ｓ４０）。なお、送受信時の各バッファ領域の指定には、ＴＣＰ／ＩＰ層１０１ｃの送信用のソケットおよび受信用のソケットを扱う関数の引数にバッファ指定をすることで行う。
【００７６】
以上述べたように、本実施の形態のシステムでは、ハンドシェイクフェーズでは、送信時の処理速度が遅く、受信バッファ領域は空であるというＴＬＳの特徴を利用して、ユーザＡ用送受信バッファ領域１０２ａおよびユーザＢ用送受信バッファ領域１０２ｂを用いてハンドシェイクメッセージの交換を行うようにしたので、あるユーザがメッセージ送信中のときに、送信用バッファ領域を独占することがない。よって、パフォーマンスの低下を防止しつつ、通信を行うことができる。
【００７７】
また、データ転送フェーズでは、ユーザが転送したいコンテンツデータを一方的に送る処理であり、処理速度が速いという特徴を利用して、兼用送信バッファ領域１０２ｃを使用し、かつ、同時に２ユーザが使用しないように排他制御を行うようにしたので、パフォーマンス面での低下を阻止し、従来と比較してメモリサイズを削減することができる。
【００７８】
また、従来に比べ構成や制御を複雑化することなく、簡易な構成で実現することができる。
ここで、マルチユーザ数を１０とすると、従来の通信バッファ領域サイズ（送受信に必要なバッファ領域サイズ）は、１０（マルチユーザ数）×｛１６ＫＢ（受信用バッファ領域）＋２ＫＢ（送信用バッファ領域）｝＝１８０ＫＢとなるが、本実施の形態のシステムにおける通信バッファ領域サイズは、通信バッファ領域サイズ＝１０×１６ＫＢ（受信用兼ハンドシェイクフェーズ送信用バッファ領域）＋２ＫＢ（送信用バッファ領域）＝１６２ＫＢとなり、比較すると同様なパフォーマンスで１８ＫＢのメモリが削減されたことがわかる。
【００７９】
次に、第２の実施の形態のシステムについて説明する。
以下、第２の実施の形態のシステムについて、前述した第１の実施の形態との相違点を中心に説明し、同様の事項については、その説明を省略する。
【００８０】
第２の実施の形態のシステムは、クライアント装置の構成が異なり、それ以外は第１の実施の形態と同様である。
図１０は、第２の実施の形態のクライアント装置の機能を示すブロック図である。

【００８１】
クライアント装置１００ａは、ＣＰＵ１０１と、システムメモリ１１２とイーサネット接続用ＬＳＩ１１６とを有している。
イーサネット接続用ＬＳＩ１１６は、ユーザＡ用送受信バッファ領域１０２ａと同様の機能を有するユーザＡ用送受信部１０６ｃと、ユーザＢ用送受信バッファ領域１０２ｂと同様の機能を有するユーザＢ用送受信部１０６ｄと、兼用送信バッファ領域１０２ｃと同様の機能を有する兼用送信部１０６ｅとを有している。
【００８２】
システムメモリ１１２は、システムメモリ１０２からイーサネット接続用ＬＳＩ１１６に移行した機能を除いた機能を有している。
次に、第２の実施の形態のシステムの動作について説明する。
【００８３】
図１１は、第２の実施の形態のハンドシェイクフェーズの動作を示すシーケンス図である。
まず、ユーザアプリケーション層１０１ａが、兼用送信バッファ領域１０２ｃ（２ＫＢ）とマルチユーザ数分の送受信用の通信ブロック領域（各１６ＫＢ）をイーサネット接続用ＬＳＩ１１６に確保し、各ユーザに割り当てる（ステップＳ１１ａ）。
【００８４】
次に、ユーザアプリケーション層１０１ａが、ＴＬＳ／ＳＳＬ層１０１ｂにハンドシェイク開始指示を送る（ステップＳ１２ａ）。
ＴＬＳ／ＳＳＬ層１０１ｂは、ステップＳ１１ａで各ユーザに割り当てられた送受信用の通信ブロック領域（格納領域）を指定する（ステップＳ１３ａ）。具体的には、ユーザＡが送受信するデータの通信ブロック領域：ユーザＡ用送受信部１０６ｃ、ユーザＢが送受信するデータの通信ブロック領域：ユーザＢ用送受信部１０６ｄとする。
【００８５】
次に、ＴＬＳ／ＳＳＬ層１０１ｂは、サーバ装置２００に送信するハンドシェイク用データを作成し、ユーザＡ用送受信部１０６ｃおよびユーザＢ用送受信部１０６ｄに格納する（ステップＳ１４ａ）。
【００８６】
ステップＳ１５ａ～Ｓ１９ａ：ステップＳ１６～Ｓ２０と同様。ここで、送信部１０６ａの代わりに、ユーザＡ用送受信部１０６ｃおよびユーザＢ用送受信部１０６ｄを設けたことにより、排他制御を行うことなくユーザ毎のハンドシェイクフェーズを並行して行うことができる。
【００８７】
ＴＬＳ／ＳＳＬ層１０１ｂは、ＴＣＰ／ＩＰ層１０１ｃからの受信通知を受け取ると、受信したハンドシェイク用データを、ユーザＡ用送受信部１０６ｃ、ユーザＢ用送受信部１０６ｄに格納する（ステップＳ２０ａ）。
【００８８】
ステップＳ２１ａ、Ｓ２２ａ：ステップＳ２３、Ｓ２４と同様。
ハンドシェイクフェーズでは、ステップＳ１３ａ～Ｓ２１ａの動作をユーザ毎に繰り返し行う（図１１中点線内）。
【００８９】
図１２は、第２の実施の形態のデータ転送フェーズの動作を示すシーケンス図である。
ステップＳ３１ａ：ステップＳ３１と同様。
次に、ＴＬＳ／ＳＳＬ層１０１ｂは、送信するデータの格納領域を、兼用送信部１０６ｅに指定し、ユーザＡの暗号化データを受信する格納領域をユーザＡ用送受信部１０６ｃに指定し、ユーザＢの暗号化データを受信する格納領域をユーザＢ用送受信部１０６ｄに指定する（ステップＳ３２ａ）。
【００９０】
次に、ＴＬＳ／ＳＳＬ層１０１ｂは、兼用送信部１０６ｅの制御権を獲得する（排他制

御）（ステップＳ３３ａ）。
ステップＳ３４ａ～Ｓ４０ａ：ステップＳ３４～Ｓ４０と同様。
【００９１】
この第２の実施形態のシステムによれば、第１の実施の形態のシステムと同様の効果が得られる。
そして、第２の実施形態のシステムによれば、ハンドシェイクフェーズにおいて排他制御を行うことなくハンドシェイク用データの送受信を行うことができるため、処理の効率化を図ることができる。
【００９２】
以上、本発明の暗号および認証のセキュリティ技術を用いた通信プログラム、通信方法および通信装置を、図示の実施の形態に基づいて説明したが、本発明はこれに限定されるものではなく、各部の構成は、同様の機能を有する暗号および認証のセキュリティ技術を用いた任意の構成のものに置換することができる。また、本発明に、他の任意の構成物や工程が付加されていてもよい。
【００９３】
また、本発明は、前述した各実施の形態のうちの、任意の２以上の構成（特徴）を組み合わせたものであってもよい。
なお、前述した各実施の形態においては、本発明をＴＬＳ／ＳＳＬ通信に適用した場合について説明したが、本発明はこれに限らず、下記（１）～（４）の条件を有する通信プロトコルに適用することができる。
【００９４】
（１）「コンテンツデータを転送するフェーズ」（ＴＬＳ／ＳＳＬ通信の場合、データ転送フェーズ）の前に、「コンテンツデータの転送方法に関する取り決めと対向ユーザの認証を行うフェーズ」(ＴＬＳ／ＳＳＬ通信の場合、ハンドシェイクフェーズ）を持つ。
【００９５】
（２）「コンテンツデータの転送方法に関する取り決めと対向ユーザの認証を行うフェーズ」では、通信装置とサーバ装置間のデータの送受信は交互に行われる。
（３）「コンテンツデータを転送するフェーズ」では、通信装置とサーバ装置間のデータの送受信は交互に行わなくてもよく、受信用バッファ領域はユーザ毎に保持しなければならない。
【００９６】
（４）データを受信するために最小限必要な受信用バッファ領域サイズは、送信するために最小限必要な送信用バッファ領域サイズと同等かそれ以上である。
また、本発明では、サーバ装置が実施の形態のクライアント装置１００、１００ａが備える機能を有していてもよい。
【００９７】
なお、本発明は、特に携帯端末機器に好適に適用することができる。
なお、上記の処理機能は、コンピュータによって実現することができる。その場合、クライアント装置１００、１００ａが有すべき機能の処理内容を記述したプログラムが提供される。そのプログラムをコンピュータで実行することにより、上記処理機能がコンピュータ上で実現される。処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体としては、例えば、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリ等が挙げられる。磁気記録装置としては、例えば、ハードディスク装置（ＨＤＤ）、フレキシブルディスク（ＦＤ）、磁気テープ等が挙げられる。光ディスクとしては、例えば、ＤＶＤ（Digital Versatile Disc）、ＤＶＤ－ＲＡＭ（Random Access Memory）、ＣＤ－ＲＯＭ（Compact Disc Read Only Memory）、ＣＤ－Ｒ（Recordable）／ＲＷ（ReWritable）等が挙げられる。光磁気記録媒体としては、例えば、ＭＯ（Magneto-Optical disk）等が挙げられる。
【００９８】
プログラムを流通させる場合には、例えば、そのプログラムが記録されたＤＶＤ、ＣＤ

－ＲＯＭ等の可搬型記録媒体が販売される。また、プログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することもできる。

【００９９】

通信プログラムを実行するコンピュータは、例えば、可搬型記録媒体に記録されたプログラムもしくはサーバコンピュータから転送されたプログラムを、自己の記憶装置に格納する。そして、コンピュータは、自己の記憶装置からプログラムを読み取り、プログラムに従った処理を実行する。なお、コンピュータは、可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することもできる。また、コンピュータは、サーバコンピュータからプログラムが転送される毎に、逐次、受け取ったプログラムに従った処理を実行することもできる。

【０１００】

（付記１）　マルチタスク機能を用いてＴＬＳ／ＳＳＬ通信を行う暗号通信プログラムにおいて、

コンピュータを、

１つまたは複数の通信対象装置に複数のユーザのコンテンツデータを転送する場合、コンテンツデータを転送するデータ転送フェーズにおいて、転送する複数の前記コンテンツデータのうち、前記通信対象装置に転送する際に１つの前記コンテンツデータを格納する複数のユーザで共用の送信用通信領域、

前記データ転送フェーズにおいて複数の前記コンテンツデータのうち前記送信用通信領域に格納された前記コンテンツデータのみを前記通信対象装置に転送する制御を行う排他制御手段、

前記送信用通信領域より大きく、ユーザ毎に設けられた複数の送受信兼用通信領域、

前記コンテンツデータの転送方法に関する取り決めと対向ユーザの認証を行うハンドシェイクフェーズにおいて前記通信対象装置に送信するユーザ毎のメッセージを生成し、生成した前記メッセージを前記各送受信兼用通信領域に格納するメッセージ生成手段、

前記各送受信兼用通信領域に格納された前記メッセージの送信をそれぞれ行う送信手段、

として機能させることを特徴とする暗号通信プログラム。

【０１０１】

（付記２）　前記送受信兼用通信領域はシステムメモリ内に設けられていることを特徴とする付記１記載の暗号通信プログラム。

（付記３）　前記排他制御手段は、前記ハンドシェイクフェーズにおいて前記送受信兼用通信領域に格納された前記コンテンツデータのみを前記通信対象装置に転送する制御を行うことを特徴とする付記２記載の暗号通信プログラム。

【０１０２】

（付記４）　前記送受信兼用通信領域は、ネットワーク接続用インタフェース内に設けられていることを特徴とする付記１記載の暗号通信プログラム。

（付記５）　コンピュータのマルチタスク機能を用いてＴＬＳ／ＳＳＬ通信を行う暗号通信方法において、

排他制御手段が、１つまたは複数の通信対象装置に複数のユーザのコンテンツデータを転送する場合、データ転送フェーズにおいて複数の前記コンテンツデータのうち、前記通信対象装置に転送する際に１つの前記コンテンツデータを格納する複数のユーザで共用の送信用通信領域に格納された前記コンテンツデータのみを前記通信対象装置に転送する制御を行い、

メッセージ生成手段が、ハンドシェイクフェーズにおいて前記通信対象装置に転送するユーザ毎のメッセージを生成し、生成した前記メッセージを前記送信用通信領域より大きく、ユーザ毎に設けられた複数の送受信兼用通信領域に格納し、

送信手段が、前記各送受信兼用通信領域に格納された前記メッセージの送信をそれぞれ行う、

ことを特徴とする暗号通信方法。

【０１０３】

（付記６） マルチタスク機能を用いてＴＬＳ／ＳＳＬ通信を行う暗号通信装置において、

１つまたは複数の通信対象装置に複数のユーザのコンテンツデータを転送する場合、データ転送フェーズにおいて、転送する複数の前記コンテンツデータのうち、前記通信対象装置に転送する際に１つの前記コンテンツデータを格納する複数のユーザで共用の送信用通信領域と、

前記データ転送フェーズにおいて複数の前記コンテンツデータのうち前記送信用通信領域に格納された前記コンテンツデータのみを前記通信対象装置に転送する制御を行う排他制御手段と、

前記送信用通信領域より大きく、ユーザ毎に設けられた複数の送受信兼用通信領域と、

ハンドシェイクフェーズにおいて前記通信対象装置に送信するユーザ毎のメッセージを生成し、生成した前記メッセージを前記各送受信兼用通信領域に格納するメッセージ生成手段と、

前記各送受信兼用通信領域に格納された前記メッセージの送信をそれぞれ行う送信手段と、

を有することを特徴とする暗号通信装置。

【０１０４】

（付記７） マルチタスク機能を用いて暗号および認証などのセキュリティ技術を利用した通信を行う暗号通信プログラムにおいて、

コンピュータを、

１つまたは複数の通信対象装置に複数のユーザのコンテンツデータを転送するデータ転送フェーズにおいて、転送する複数の前記コンテンツデータのうち、前記通信対象装置に転送する際に１つの前記コンテンツデータを格納する複数のユーザで共用の送信用通信領域、

前記コンテンツデータを転送するフェーズにおいて複数の前記コンテンツデータのうち前記送信用通信領域に格納された前記コンテンツデータのみを前記通信対象装置に転送する制御を行う排他制御手段、

前記送信用通信領域より大きく、ユーザ毎に設けられた複数の送受信兼用通信領域、

前記コンテンツデータの転送方法に関する取り決めを行うフェーズにおいて前記通信対象装置に送信するユーザ毎のメッセージを生成し、生成した前記メッセージを前記各送受信兼用通信領域に格納するメッセージ生成手段、

前記各送受信兼用通信領域に格納された前記メッセージの送信をそれぞれ行う送信手段、

として機能させることを特徴とする暗号通信プログラム。

【０１０５】

（付記８） 前記送受信兼用通信領域は、システムメモリ内に設けられていることを特徴とする付記７記載の暗号通信プログラム。

（付記９） 前記排他制御手段は、前記ハンドシェイクフェーズにおいて前記送受信兼用通信領域に格納された前記コンテンツデータのみを前記通信対象装置に転送する制御を行うことを特徴とする付記８記載の暗号通信プログラム。

【０１０６】

（付記１０） 前記送受信兼用通信領域は、ネットワーク接続用インタフェース内に設けられていることを特徴とする付記７記載の暗号通信プログラム。

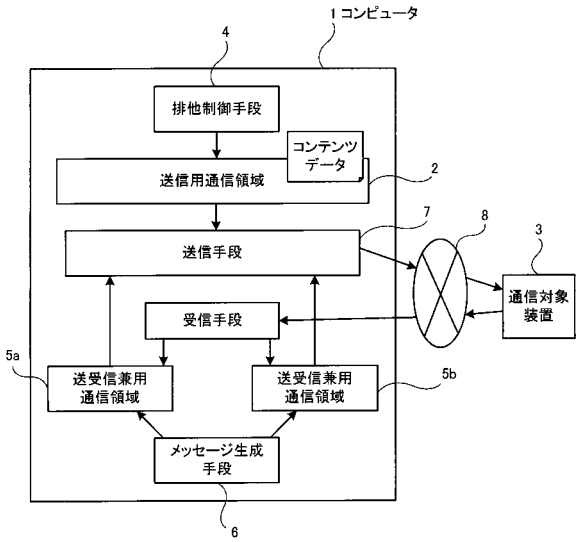
（付記１１） コンピュータのマルチタスク機能を用いて暗号および認証などのセキュリティ技術を利用した通信を行う暗号通信方法において、

排他制御手段が、１つまたは複数の通信対象装置に複数のユーザのコンテンツデータを転送するフェーズにおいて、コンテンツデータを転送するフェーズにおいて複数の前記コンテンツデータのうち、前記通信対象装置に転送する際に１つの前記コンテンツデータを

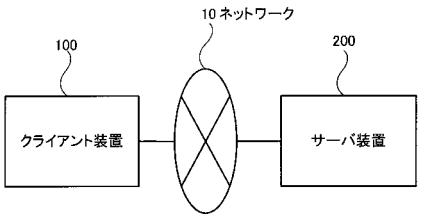
格納する複数のユーザで共用の送信用通信領域に格納された前記コンテンツデータのみを前記通信対象装置に転送する制御を行い、
メッセージ生成手段が、前記コンテンツデータの転送方法に関する取り決めを行うフェーズにおいて前記通信対象装置に転送するユーザ毎のメッセージを生成し、生成した前記メッセージを前記送信用通信領域より大きく、ユーザ毎に設けられた複数の送受信兼用通信領域に格納し、
送信手段が、前記各送受信兼用通信領域に格納された前記メッセージの送信をそれぞれ行う、
ことを特徴とする暗号通信方法。
【０１０７】
（付記１２）　マルチタスク機能を用いて暗号および認証などのセキュリティ技術を利用した通信を行う暗号通信装置において、
１つまたは複数の通信対象装置に複数のユーザのコンテンツデータを転送するフェーズにおいて、転送する複数の前記コンテンツデータのうち、前記通信対象装置に転送する際に１つの前記コンテンツデータを格納する複数のユーザで共用の送信用通信領域と、
前記コンテンツデータを転送するフェーズにおいて複数の前記コンテンツデータのうち前記送信用通信領域に格納された前記コンテンツデータのみを前記通信対象装置に転送する制御を行う排他制御手段と、
前記送信用通信領域より大きく、ユーザ毎に設けられた複数の送受信兼用通信領域と、
前記コンテンツデータの転送方法に関する取り決めを行うフェーズにおいて前記通信対象装置に送信するユーザ毎のメッセージを生成し、生成した前記メッセージを前記各送受信兼用通信領域に格納するメッセージ生成手段と、
前記各送受信兼用通信領域に格納された前記メッセージの送信をそれぞれ行う送信手段と、
を有することを特徴とする暗号通信装置。
【図面の簡単な説明】
【０１０８】
【図１】本発明の概要を示す図である。
【図２】実施の形態のシステムを示すブロック図である。
【図３】ハンドシェイクフェーズを説明する図である。
【図４】データ転送フェーズを説明する図である。
【図５】クライアント装置のハードウェア構成例を示す図である。
【図６】クライアント装置の機能を示すブロック図である。
【図７】ＣＰＵの機能を示すブロック図である。
【図８】ハンドシェイクフェーズの動作を示すシーケンス図である。
【図９】データ転送フェーズの動作を示すシーケンス図である。
【図１０】第２の実施の形態のクライアント装置の機能を示すブロック図である。
【図１１】第２の実施の形態のハンドシェイクフェーズの動作を示すシーケンス図である。
【図１２】第２の実施の形態のデータ転送フェーズの動作を示すシーケンス図である。
【図１３】暗号化されたレコードを示す図である。
【符号の説明】
【０１０９】
１　コンピュータ
２　送信用通信領域
３　通信対象装置
４　排他制御手段
５ａ、５ｂ　送受信兼用通信領域
６　メッセージ生成手段
７　送信手段

８、１０　ネットワーク
１００、１００ａ　クライアント装置
１０１ａ　ユーザアプリケーション層
１０１ｂ　ＴＬＳ／ＳＳＬ層
１０１ｃ　ＴＣＰ／ＩＰ層
１０２、１１２　システムメモリ
１０２ａ　ユーザＡ用送受信バッファ領域
１０２ｂ　ユーザＢ用送受信バッファ領域
１０２ｃ　兼用送信バッファ領域
１０６、１１６　イーサネット接続用ＬＳＩ
１０６ａ　送信部
１０６ｂ　受信部
１０６ｃ　ユーザＡ用送受信部
１０６ｄ　ユーザＢ用送受信部
１０６ｅ　兼用送信部
２００　サーバ装置

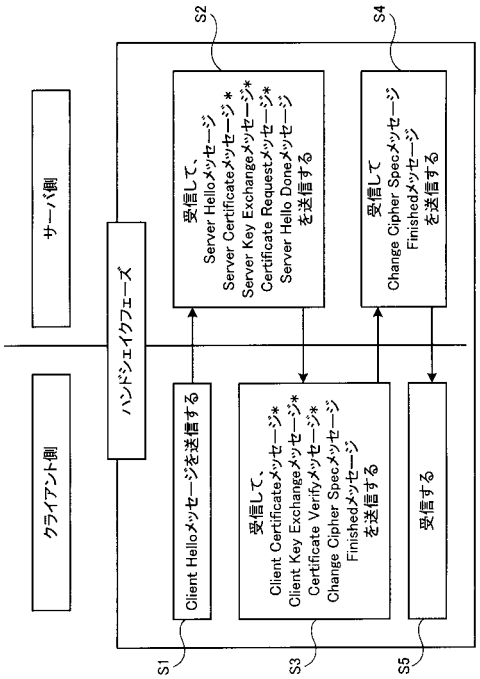
【図１】



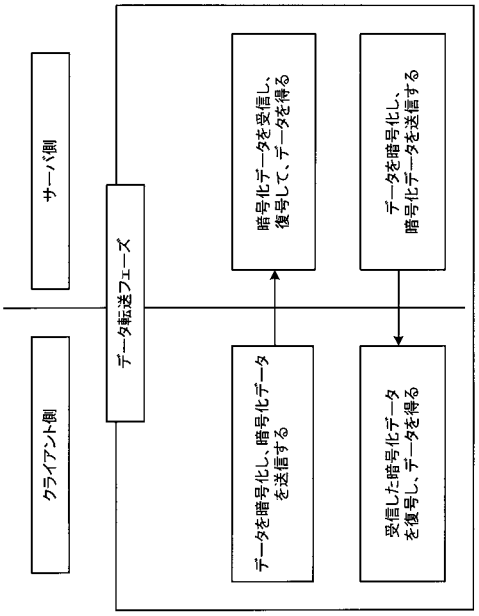
【図２】



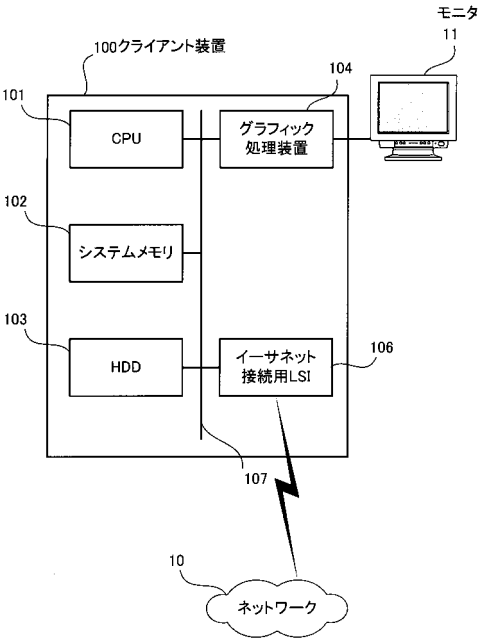
【図３】



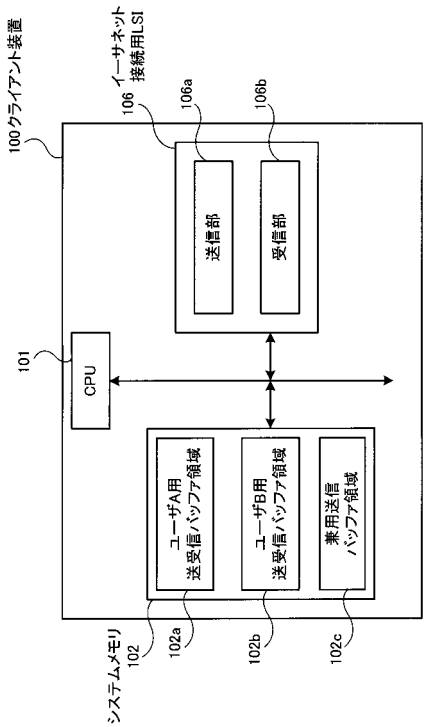
【図４】


サーバ側
クライアント側
データ転送フェーズ
暗号化データを受信し、復号して、データを得る
データを暗号化し、暗号化データを送信する
データを暗号化し、暗号化データを送信する
受信した暗号化データを復号し、データを得る

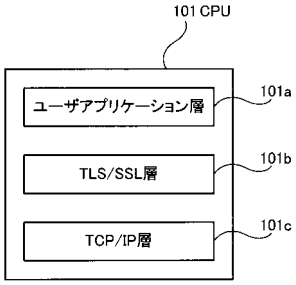
【図５】


モニタ
11
100クライアント装置
104
101
CPU
グラフィック処理装置
102
システムメモリ
103
HDD
イーサネット接続用LSI
106
107
10
ネットワーク

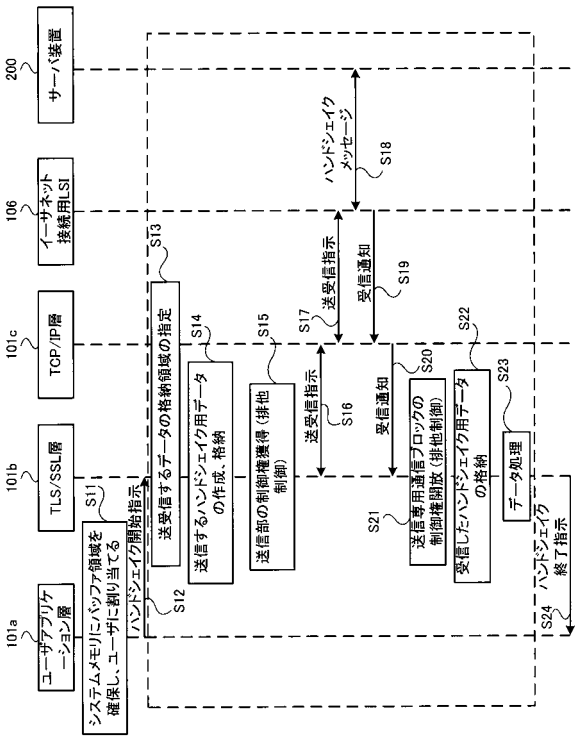
【図６】


100クライアント装置
イーサネット接続用LSI
106
106a
106b
送信部
受信部
101
CPU
ユーザA用送受信バッファ領域
ユーザB用送受信バッファ領域
兼用送信バッファ領域
システムメモリ
102
102a
102b
102c

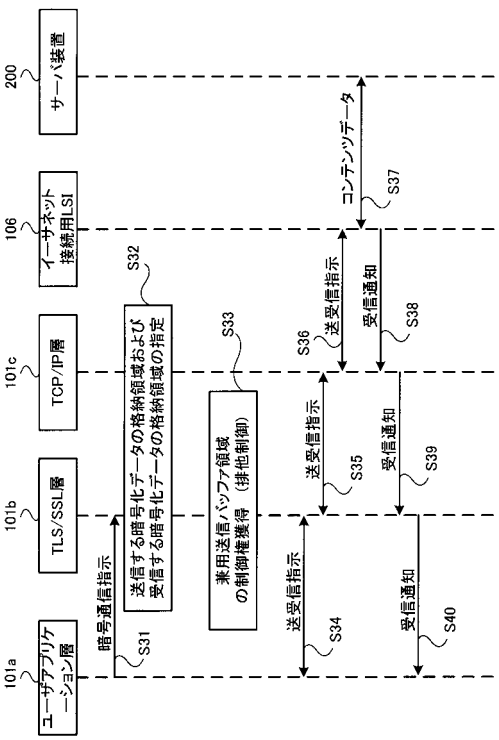
【図７】


101 CPU
ユーザアプリケーション層
101a
TLS/SSL層
101b
TCP/IP層
101c

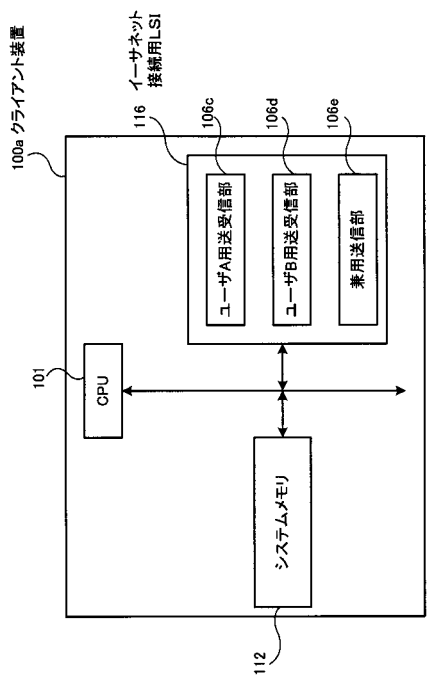
【図８】


200
サーバ装置
106
イーサネット接続用LSI
101c
TCP/IP層
101b
TLS/SSL層
101a
ユーザアプリケーション層
システムメモリにバッファ領域を確保し、ユーザに割り当てる
S11
ハンドシェイク開始指示
S12
送受信するデータの格納領域の指定
S13
送信するハンドシェイク用データの作成、格納
S14
送信部の制御権獲得（排他制御）
S15
送受信指示
S16
受信通知
S17
ハンドシェイクメッセージ
S18
送受信指示
受信通知
S19
送信専用通信ブロックの制御権開放（排他制御）
S20
S21
受信したハンドシェイク用データの格納
S22
データ処理
S23
ハンドシェイク終了指示
S24

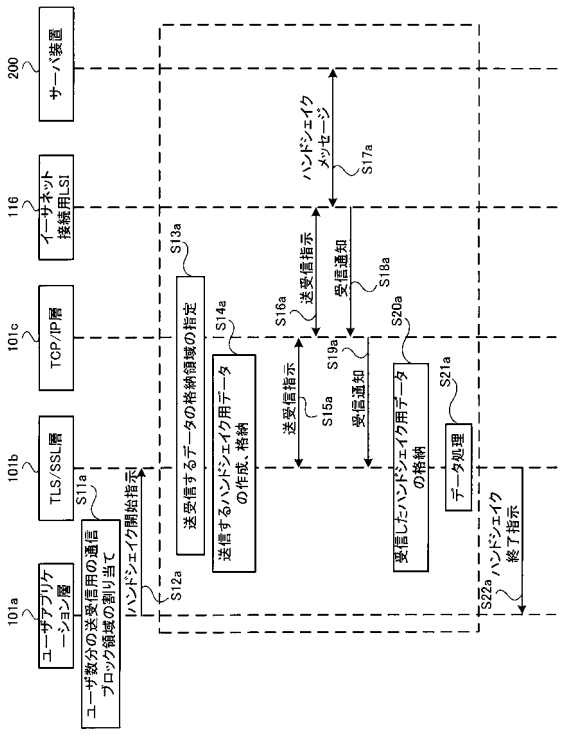
【図９】


200
サーバ装置
106
イーサネット接続用LSI
101c
TCP/IP層
101b
TLS/SSL層
101a
ユーザアプリケーション層
暗号通信指示
S31
送信する暗号化データの格納領域および受信する暗号化データの格納領域の指定
S32
兼用送信バッファ領域の制御権獲得（排他制御）
S33
送受信指示
S34
送受信指示
S35
受信通知
S36
受信通知
S37
コンテンツデータ
送受信指示
S38
受信通知
S39
受信通知
S40

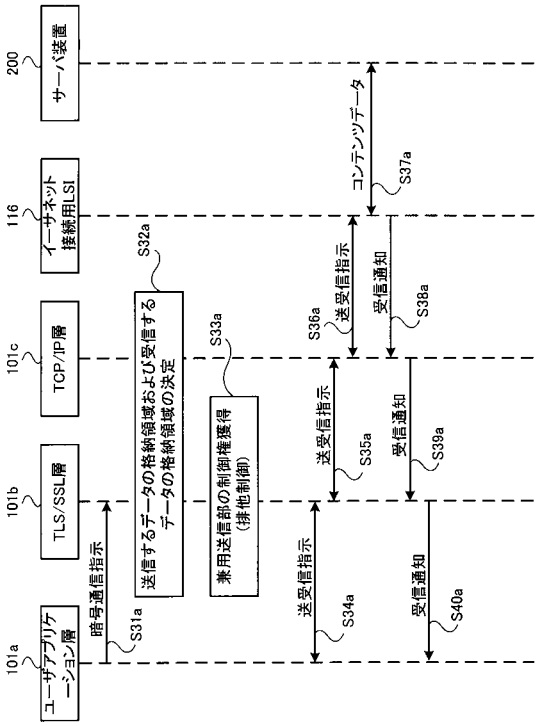
【図１０】


100a クライアント装置
116 イーサネット接続用LSI
106c
106d
106e
ユーザA用送受信部
ユーザB用送受信部
兼用送信部
101
CPU
システムメモリ
112

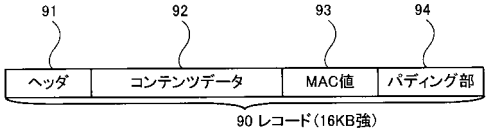
【図１１】


200
サーバ装置
116
イーサネット接続用LSI
101c
TCP/IP層
101b
TLS/SSL層
101a
ユーザアプリケーション層
ユーザ数分の送受信用の通信ブロック領域の割り当て
S11a
ハンドシェイク開始指示
S12a
送受信するデータの格納領域の指定
S13a
送信するハンドシェイク用データの作成、格納
S14a
送受信指示
S15a
S16a
送受信指示
受信通知
S18a
S19a
ハンドシェイクメッセージ
S17a
受信したハンドシェイク用データの格納
S20a
データ処理
S21a
ハンドシェイク終了指示
S22a

【図１２】


200
サーバ装置
116
イーサネット接続用LSI
101c
TCP/IP層
101b
TLS/SSL層
101a
ユーザアプリケーション層
暗号通信指示
S31a
送信するデータの格納領域および受信するデータの格納領域の決定
S32a
兼用送信部の制御権獲得（排他制御）
S33a
送受信指示
S34a
送受信指示
S35a
送受信指示
S36a
コンテンツデータ
S37a
受信通知
S38a
受信通知
S39a
受信通知
S40a

【図１３】


91
92
93
94
ヘッダ
コンテンツデータ
MAC値
パディング部
90 レコード（16KB強）

フロントページの続き

(72)発明者　小森　裕之
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　野口　新
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

審査官　衣鳩　文彦

(56)参考文献　特開平０６－０４４１９６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／００
Ｇ０６Ｆ　１３／００