(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2006-333095
(P2006-333095A)
(43)公開日　平成18年12月7日(2006.12.7)

(51)Int.Cl.	F I			テーマコード（参考）
H04L 9/08 (2006.01)	H04L	9/00	601C	5J104
	H04L	9/00	601E	

審査請求 未請求　請求項の数 20　ＯＬ　（全 17 頁）

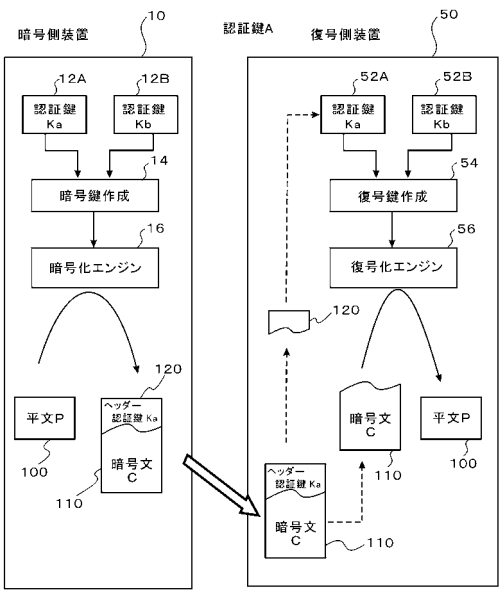
(21)出願番号　特願2005-154098 (P2005-154098)
(22)出願日　平成17年5月26日 (2005.5.26)

(71)出願人　504369959
深谷　博美
埼玉県上尾市大字上１１１４番地の５
(74)代理人　100082223
弁理士　山田　文雄
(74)代理人　100094282
弁理士　山田　洋資
(72)発明者　深谷　博美
埼玉県上尾市大字上１１１４番地の５

Ｆターム(参考)　5J104 AA01　AA16　EA04　EA15　EA16
EA18　JA03　NA02　NA37

(54)【発明の名称】暗号通信方法、暗号通信システム、暗号通信装置及び暗号通信プログラム

(57)【要約】
【課題】　特定の相手側機器のみで復号可能な暗号文により暗号通信を行うことができ、暗号文を受信する度に相手側の認証を行って交互認証を可能にし、送・受信データの暗号化・復号化処理を高速で行うことができる暗号通信方法を提供する。
【解決手段】　相手側機器認証鍵（Ｋｂ）と自己の機器認証鍵（Ｋａ）を用いて作成した暗号・復号鍵を用いて秘密鍵暗号アルゴリズムにより送・受信データの暗号・復号化を行う。互いに、送信するデータを暗号鍵を用いて暗号化した暗号文Ｃ（110）とし、この暗号文Ｃと共に送信側の機器認証鍵Ｋａのみを相手側に送信する。相手側電子機器（５０）では、受信した暗号文Ｃ（110）に添付されていた相手側機器認証鍵（Ｋａ）と自己の機器認証鍵（Ｋｂ）を用いて復号鍵を作成し、この復号鍵を用いて暗号文を復号する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
それぞれ機器固有の機器認証鍵を有する電子機器の間で、秘密鍵暗号アルゴリズムにより送信データの暗号・復号化を行う暗号通信方法において、以下のステップを備えることを特徴とする暗号通信方法：
a) 第１の電子機器において：
a-1) 送信側の第１の電子機器の機器認証鍵Ｋａと受信側の第２の電子機器の機器認証鍵Ｋｂとを組み合わせた暗号鍵Ｋａｂを作成し；
a-2) この暗号鍵を用いて送信データＰを暗号文Ｃとし；
a-3) この暗号文Ｃと送信側電子機器の機器認証鍵Ｋａとを、第２の電子機器に送信し；
b) 暗号文を受信した第２の電子機器では、
b-1) 受信側電子機器の機器認証鍵Ｋｂと暗号文Ｃに添付されていた送信側電子機器の機器認証鍵Ｋａとを用いて復号鍵Ｋａｂを作成し；
b-2) この復号鍵を用いて前記暗号文Ｃを復号する。
【請求項２】
ステップa-1)で用いる第２の電子機器の機器認証鍵Ｋｂは、第２の電子機器から第１の電子機器に予め送信されたものを使用することを特徴とする請求項１の暗号通信方法。
【請求項３】
前記機器認証鍵Ｋｂは、第２の電子機器から第１の電子機器に予め送信された暗号文に添付されていたものであることを特徴とする請求項２の暗号通信方法。
【請求項４】
第２の電子機器から第１の電子機器に送信する場合には、ステップb-1)で作成された復号鍵を暗号鍵として用いて送信データを暗号化し、得られた暗号文を第２の電子機器の機器認証鍵Ｋｂを添付して第１の電子機器に送信することを特徴とする請求項１～３の暗号通信方法。
【請求項５】
ステップb-1)の後に行われる第１の電子機器と第２の電子機器との間のデータ送受信は、互いに、送信データを前記暗号鍵を用いて暗号化した暗号文とし、この暗号文と共に送信側の機器認証鍵のみを相手側に送信し；
相手側電子機器では、受信した暗号文に添付されていた相手側機器認証鍵と自己の機器認証鍵を用いて復号鍵を作成し、この復号鍵を用いて暗号文を復号することを特徴とする請求項１～４の何れかの暗号通信方法。
【請求項６】
前記機器認証鍵Ｋａ，Ｋｂは、それぞれの電子機器の識別情報、製造番号、製造日付を含む機器情報から選ばれた固有ＩＤであることを特徴とする請求項１～５の暗号通信方法。
【請求項７】
前記機器認証鍵Ｋａ，Ｋｂは、それぞれの電子機器に予め付与されたユニーク値であることを特徴とする請求項１～５の暗号通信方法。
【請求項８】
前記暗号鍵Ｋａｂは、機器認証鍵Ｋａ，Ｋｂをパスフレーズとしてこれを連結したものであることを特徴とする請求項１～７の暗号通信方法。
【請求項９】
前記ステップa-1)において、前記暗号鍵Ｋａｂは機器認証鍵Ｋａ，Ｋｂの他に暗号側利用者が入力したパスワードを組み合わせて作成され、前記ステップb-1)では、復号側利用者が入力したパスワードを組み合わせて前記復号鍵を作成することを特徴とする請求項１の暗号通信方法。
【請求項１０】
前記ステップa-1)において、暗号側利用者が入力したパスワードをさらに組み合わせて

前記暗号鍵Ｋａｂを作成し、前記ステップa-3）ではこのパスワードも含めて相手側第２の電子機器に送信し、前記ステップb-1)では復号側利用者が入力したパスワードと第１の電子機器から送信されたパスワードとが一致することを条件として、前記機器認証鍵Ｋａ、Ｋｂとパスワードとを用いて前記復号鍵を作成することを特徴とする請求項１の暗号通信方法。

【請求項１１】

前記ステップa-1)において、復号側利用者と共有する共有キーと乱数とをさらに組み合わせて前記暗号鍵を作成し、前記ステップa－3)ではこの前記乱数も含めて相手側第２の電子機器に送信し、

前記ステップb-1)において、提供された前記乱数と、復号側第２の電子機器が所持する共有キーとを組み合わせて前記復号鍵を作成することを特徴とする請求項１の暗号通信方法。

【請求項１２】

それぞれ機器固有の機器認証鍵を有する第１の電子機器と第２の電子機器との間で秘密鍵暗号アルゴリズムにより送信データの暗号・復号化を行う暗号通信システムにおいて：

前記第１の電子機器は、

第１の電子機器の固有ＩＤ又は予め付与されたユニーク値を用いて作成された第１機器認証鍵Ｋａを記憶する第１機器認証鍵記憶手段と；

第２の電子機器から提供された第２の電子機器固有の第２機器認証鍵Ｋｂを読取る第２機器認証鍵読取手段と；

第１機器認証鍵Ｋａと第２機器認証鍵Ｋｂとを用いて暗号鍵を作成する暗号鍵作成手段と；

得られた暗号鍵を用いて、送信データＰを暗号文Ｃに暗号化する暗号化手段と；

得られた暗号文Ｃを第１機器認証鍵Ｋａを含む属性情報と共に第２の電子機器に送信する送信手段とを備え；

前記第２の電子機器は、

第２の電子機器の固有ＩＤ又は予め付与されたユニーク値を用いて作成された前記第２機器認証鍵Ｋｂを記憶する第２機器認証鍵記憶手段と；

第１の電子機器から送信された暗号文Ｃに添付された属性情報から第１機器認証鍵Ｋａを読取る第１機器認証鍵読取手段と；

読取られた第１機器認証鍵Ｋａと自己の第２機器認証鍵Ｋｂとを用いて復号鍵を作成する復号鍵作成手段と；

得られた復号鍵を用いて、第１の電子機器から提供された暗号文Ｃを復号化して平文の送信データＰを得る復号化手段と；

を備えることを特徴とする暗号通信システム。

【請求項１３】

相手側電子機器に送る送信データを秘密鍵暗号アルゴリズムにより暗号化して送信し、また相手側電子機器から受信した暗号文を復号化する暗号通信装置において：

電子機器の固有ＩＤ又は予め付与されたユニーク値を用いて作成された第１機器認証鍵Ｋａを記憶する機器認証鍵記憶手段と；

相手側電子機器から提供された相手側電子機器固有の第２機器認証鍵Ｋｂを読取る機器認証鍵読取手段と；

第１機器認証鍵Ｋａと第２機器認証鍵Ｋｂとを用いて暗号鍵を作成する暗号鍵作成手段と；

得られた暗号鍵を用いて、送信データＰを暗号文Ｃに暗号化する暗号化手段と；

得られた暗号文Ｃを第１機器認証鍵Ｋａを含む属性情報と共に相手側電子機器に送信し、また相手側電子機器から送信された暗号文と相手側機器認証鍵を含む属性情報を受信する送・受信手段と；

第１機器認証鍵Ｋａと第２機器認証鍵Ｋｂとを用いて復号鍵を作成する復号鍵作成手段と；

得られた復号鍵を用いて、相手側電子機器から提供された暗号文Ｃ’を平文の送信データＰ’に復号化する復号化手段；
を備えることを特徴とする暗号通信装置。
【請求項１４】
前記暗号通信装置が、利用者の端末装置に着脱可能な外部暗号通信装置として構成されていることを特徴とする請求項１３の暗号通信装置。
【請求項１５】
利用者の電子機器に着脱可能な外部暗号通信装置であって、相手側電子機器に送る送信データを秘密鍵暗号アルゴリズムにより暗号化して送信し、また相手側電子機器から受信した暗号文を復号化する外部暗号通信装置において：
外部暗号化通信装置の固有ＩＤ又は予め付与されたユニーク値を用いて作成された第１機器認証鍵Ｋａを記憶する機器認証鍵記憶手段と；
相手側電子機器から提供された相手側電子機器固有の第２機器認証鍵Ｋｂを読取る機器認証鍵読取手段と；
第１機器認証鍵Ｋａと第２機器認証鍵Ｋｂとを用いて暗号鍵を作成する暗号鍵作成手段と；
得られた暗号鍵を用いて、送信データＰを暗号文Ｃに暗号化する暗号化手段と；
得られた暗号文Ｃを第１機器認証鍵Ｋａを含む属性情報と共に相手側電子機器に送信すること、また相手側電子機器から送信された暗号文Ｃ’と相手側機器認証鍵を含む属性情報を受信することを、当該外部暗号化通信装置を接続した電子機器に指示する送・受信指示手段と；
第１機器認証鍵Ｋａと第２機器認証鍵Ｋｂとを用いて復号鍵を作成する復号鍵作成手段と；
得られた復号鍵を用いて、相手側電子機器から提供された暗号文Ｃ’を平文Ｐ’に復号化する復号化手段；
とを備えることを特徴とする外部暗号通信装置。
【請求項１６】
利用者の電子機器に着脱可能な外部暗号通信装置であって、相手側電子機器に送る送信データを秘密鍵暗号アルゴリズムにより暗号化して送信し、また相手側電子機器から受信した暗号文を復号化する外部暗号通信装置において：
電子機器の固有ＩＤ又は予め付与されたユニーク値を用いて作成された第１機器認証鍵Ｋａを記憶する機器認証鍵記憶手段と；
相手側電子機器から提供された相手側電子機器固有の第２機器認証鍵Ｋｂを読取る機器認証鍵読取手段と；
第１機器認証鍵Ｋａと第２機器認証鍵Ｋｂとを用いて暗号鍵を作成する暗号鍵作成手段と；
得られた暗号鍵を用いて、送信データＰを暗号文Ｃに暗号化する暗号化手段と；
得られた暗号文Ｃを第１機器認証鍵Ｋａを含む属性情報と共に相手側電子機器に送信すること、また相手側電子機器から送信された暗号文Ｃ’と相手側機器認証鍵Ｋｂを含む属性情報を受信することを、当該外部暗号化通信装置を接続した電子機器に指示する送・受信指示手段と；
第１機器認証鍵Ｋａと第２機器認証鍵Ｋｂとを用いて復号鍵を作成する復号鍵作成手段と；
得られた復号鍵を用いて、相手側電子機器から提供された暗号文Ｃ’を平文Ｐ’に復号化する復号化手段；
とを備えることを特徴とする外部暗号通信装置。
【請求項１７】
それぞれ機器固有の機器認証鍵を有する電子機器の間で、秘密鍵暗号アルゴリズムにより送・受信データの暗号・復号化を行う暗号通信プログラムにおいて；
送信側電子機器の機器認証鍵と受信側電子機器の機器認証鍵とを用いて暗号鍵を作成し

；
この暗号鍵で送信データを暗号化して暗号文を作成し；
この暗号文と送信側電子機器の機器認証鍵とを相手側電子機器に送信することを特徴とする暗号通信プログラム。
【請求項１８】
それぞれ機器固有の機器認証鍵を有する電子機器の間で、秘密鍵暗号アルゴリズムにより送・受信データの暗号・復号化を行う暗号通信プログラムにおいて；
受信した暗号文に添付された送信側電子機器の機器認証鍵と受信側電子機器の機器認証鍵とを用いて復号鍵を作成し；
この復号鍵を用いて暗号文を復号することを特徴とする暗号通信プログラム。
【請求項１９】
それぞれ機器固有の機器認証鍵を有する電子機器の間で、秘密鍵暗号アルゴリズムにより送・受信データの暗号・復号化を行う暗号通信プログラムにおいて；
送信時には：
送信側電子機器の機器認証鍵Ｋａと受信側電子機器の機器認証鍵Ｋｂとを用いて暗号鍵Ｋａｂを作成するステップと；
この暗号鍵Ｋａｂで送信データＰを暗号化して暗号文Ｃを作成し；
この暗号文Ｃと送信側電子機器の機器認証鍵Ｋａとを相手側電子機器に送信し；
受信時には、
相手側電子機器から受信した暗号文Ｃ’に添付された相手側電子機器の機器認証鍵Ｋｂと受信側電子機器の機器認証鍵Ｋａとを用いて復号鍵Ｋａｂを作成し；
この復号鍵Ｋａｂを用いて暗号文Ｃ’を復号することを特徴とする暗号通信プログラム。
【請求項２０】
それぞれ機器固有の機器認証鍵を有する電子機器の間で、秘密鍵暗号アルゴリズムにより送信データの暗号・復号化を行う暗号通信プログラムであって、以下の各ステップを備えることを特徴とする暗号通信プログラム：
a) 送信側の第１の電子機器の機器認証鍵Ｋａと受信側の第２の電子機器の機器認証鍵Ｋｂとを組み合わせた暗号鍵Ｋａｂを作成し；
b) この暗号鍵Ｋａｂを用いて送信データＰを暗号文Ｃとし；
c) この暗号文Ｃと送信側電子機器の機器認証鍵Ｋａとを、第２の電子機器に送信し；
d) 相手側の第２の電子機器から暗号文Ｃ’と相手側の機器認証鍵Ｋｂとを受信し；
e) 受信側電子機器の機器認証鍵Ｋａと送信側電子機器の機器認証鍵Ｋｂとを用いて復号鍵Ｋｂａを作成し；
f) この復号鍵Ｋｂａを用いて前記暗号文Ｃ’を復号する。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、暗号通信方法及びシステムに関する。さらに詳しくは、機器固有の機器認証鍵を持つ電子機器の間で秘密鍵暗号アルゴリズムにより送・受信データの暗号・復号化を行う暗号通信方法及びシステムに関するものである。さらに、この暗号通信方法に用いる暗号通信装置、外部暗号通信装置、暗号通信プログラムに関するものである。
【背景技術】
【０００２】
インターネットに代表される情報伝達手段の発展に伴い、通信ネットワークを介したデータの送受信が広く行われている。これに伴い、情報の漏洩、改竄、成りすましを防止するための種々のデータ暗号通信方式が提案されている。この暗号通信では通信されるデータが暗号化する際には、必ず暗号鍵を指定する。共通鍵暗号方式は、平文を暗号化する暗号鍵と暗号文を平文に復号化する復号鍵とを同じ共通鍵とするもので、暗号化アルゴリズムと復号化アルゴリズムは対称性を有するため、暗号化、復号化の処理速度に優れる。し

かし、事前に何らかの方法を用いて「鍵」を受信者側に手渡しておく必要があり、万一、その時点で第三者に「鍵」が漏れてしまえば、その後の暗号を全て解読されてしまう危険性が高くなる。又、多数の相手に対して同様の暗号化通信を行う場合、相手の数だけ鍵を用意する必要がある。

【０００３】

近年では、公開鍵と秘密鍵という異なった２種類に鍵のペアによって暗号化、復号化を行う公開鍵暗号方式による暗号通信も行われている。これは、相手側の公開鍵を用いて暗号化したデータを相手に送り、相手は送られた暗号文を自分の秘密の秘密鍵で復号化するもので、この秘密鍵を持っていない他人には、この暗号文を解読できない。１つの鍵を公開しておけば、誰にでもその鍵を使ってもらうことが出来、多数の相手とのやり取りを行う場合でも、自分の秘密鍵だけを管理しておけば良く、鍵の管理が煩雑になることはない点で優れている。しかし暗号化アルゴリズムと復号化アルゴリズムが非対称であり、数学的に難しい処理が多くなるため、高速処理が難しくなる。このため、ネット上で暗号化したコンテンツなどを受信者に送りリアルタイムに復号化することが要求される交互通信の場合や、データ量が非常に大きい場合には向いていないという問題があった。特にメモリ量が制限される携帯型端末では、十分な処理速度を得るのが難しいという問題があった。

【０００４】

また、安全な通信のためには通信相手の認証が必要となる。通常は、通信開始の前に通信相手の認証を、ユーザーＩＤ、パスワードによる認証手続で行ったり、電子署名によって行ったりする。しかし、このようなＩＤ，パスワード、電子署名なども一度漏洩すれば、成りすましを防止することはできない。通信開始時の認証だけではなく、暗号化データを交互に送受信する度に、相手側を認証することが望ましい。

【発明の開示】

【発明が解決しようとする課題】

【０００５】

本発明は、このような状況に鑑みなされたものであり、特定の相手側機器のみで復号可能な暗号文により暗号通信を行うことができ、暗号文を受信する度に相手側の認証を行って交互認証を可能にし、送・受信データの暗号化・復号化処理を高速で行うことができる暗号通信方法を提供することを第１の目的とする。

【０００６】

又、この暗号通信方法に用いる暗号通信システムを提供することを第２の目的とし、この暗号通信方法に用いる暗号通信装置を提供することを第３の目的とする。さらに本発明は、この暗号通信方法に用いる暗号通信プログラムを提供することを第４の目的とする。

【課題を解決するための手段】

【０００７】

本発明の第１の目的は、それぞれ機器固有の機器認証鍵を有する電子機器の間で、秘密鍵暗号アルゴリズムにより送信データの暗号・復号化を行う暗号通信方法において、以下のステップを備えることを特徴とする暗号通信方法：

a) 第１の電子機器において：

a-1) 送信側の第１の電子機器の機器認証鍵Ｋａと受信側の第２の電子機器の機器認証鍵Ｋｂとを組み合わせた暗号鍵Ｋａｂを作成し；

a-2) この暗号鍵を用いて送信データＰを暗号文Ｃとし；

a-3) この暗号文Ｃと送信側電子機器の機器認証鍵Ｋａとを、第２の電子機器に送信し；

b) 暗号文を受信した第２の電子機器では、

b-1) 受信側電子機器の機器認証鍵Ｋｂと暗号文Ｃに添付されていた送信側電子機器の機器認証鍵Ｋａとを用いて復号鍵Ｋａｂを作成し；

b-2) この復号鍵を用いて前記暗号文Ｃを復号する、

により達成される。

【０００８】

すなわち、本発明の暗号通信方法は、送信データ（平文Ｐ）を暗号化する暗号鍵と、暗号文Ｃを平文Ｐに復号する復号鍵とを同じ共通のものとするものであり、暗号化エンジン、復号化エンジンは対称的なものとなり、高速処理を行うことができる。但し、暗号鍵Ｋａｂは、送信側の第１の電子機器の機器認証鍵Ｋａと、相手の受信側の第２の電子機器の機器認証鍵Ｋｂとを組み合わせて作成される。受信側の第２の電子機器では、暗号文Ｃに添付された送信側電子機器の機器認証鍵Ｋａと、受信側電子機器の機器認証鍵Ｋｂとを用いて復号鍵Ｋａｂを作成する。この復号鍵Ｋａｂにより受信した暗号文Ｃを復号する。暗号文Ｃが復号できれば、暗号化したデータを送信した相手側は受信側機器認証鍵Ｋｂを用いて暗号鍵Ｋａｂを作成したことが分かり、相手側を認証することができる。これにより送信データの暗号通信と送信側電子機器の認証とを同時におこなうことができるようにしたものである。

【０００９】

送信側の第１の電子機器が暗号鍵作成に使用する受信側電子機器の機器認証鍵Ｋｂは、暗号通信開始時は、受信側の第２の電子機器から予め送信側第１の電子機器に送信・配付されたものを使用する（請求項２）。この機器認証鍵Ｋｂは第２の電子機器から第１の電子機器に送信された暗号文に添付されたものでもよい（請求項３）。

【００１０】

暗号通信が開始された後の返信は、受信側電子機器（第２の電子機器）で暗号文復号化に使用した復号鍵Ｋａｂを用いて返信データを暗号化し、この暗号文に第２の電子機器の機器認証鍵Ｋｂを添付して第１の電子機器に送信する（請求項４）。返信暗号文を受信した第１の電子機器は、自己の機器認証鍵Ｋａを返信暗号文に添付されていた相手側機器認証鍵Ｋｂと組み合わせて再度復号鍵Ｋａｂを作成し、この復号鍵で返信暗号文を復号化する。暗号文を復号できれば、この返信暗号文を作成した電子機器は、前回暗号文を送信した相手側電子機器であることを認証することができる。

【００１１】

このように一度暗号通信が開始された後に行われる第１の電子機器と第２の電子機器との間のデータ送受信は、互いに、送信データを前記暗号鍵を用いて暗号化した暗号文とし、この暗号文と共に送信側の機器認証鍵のみを相手側に送信する。相手側電子機器では、受信した暗号文に添付されていた相手側機器認証鍵と自己の機器認証鍵を用いて復号鍵を作成し、この復号鍵を用いて暗号文を復号する（請求項５）。これにより、暗号文を送信してきた相手側が、直前にこちらから送信した相手側であると認証することができる。すなわち、交互通信ごとに交互認証を行いながら暗号通信を行うことができる。

【００１２】

機器認証鍵は、暗号通信を行う当該電子機器の機器固有のＩＤ又は識別情報を用いて作成されたものであり、例えば、ＣＰＵそれ自体に書き込まれている識別番号、製造番号、製造日付などの固有の機器情報を固有ＩＤとして使用することができる（請求項６）。ＣＰＵ等の集積回路やネットワーク機器は、互いを認識するための機器識別ＩＤが有り、これらをユニークＩＤとして、これから、機器認証鍵を作成することができる。また、電子機器のフラッシュメモリーなどに付与したユニーク値を機器認証鍵としてもよい（請求項７）。

【００１３】

暗号鍵Ｋａｂは、機器認証鍵Ｋａ，Ｋｂを、例えばパスフレーズとしてこれを連結したものとすることができる（請求項８）。

【００１４】

暗号鍵Ｋａｂは、機器認証鍵Ｋａ，Ｋｂの他に暗号側利用者が入力したパスワードを組み合わせて作成してもよく、この場合には、復号側利用者がパスワードを入力して復号鍵Ｋａｂを作成することになる（請求項９，１０）。

【００１５】

暗号側利用者（装置）と復号側利用者（装置）とで共有する共有キー用いる場合には、この共有キーとさらに乱数とを組み合わせて暗号鍵を作成してもよい。この場合には、乱

数を含めて復号側電子機器に送信し、復号側電子機器では、提供された乱数と、復号側電子機器が所持する共有キーとを組み合わせて復号鍵を作成する（請求項１１）。

【００１６】

交互暗号通信を行う電子機器は、互いに通信ネットワークを介して送受信可能な端末とすることができ、又何れか一方、或いは両方ともネットワークサーバとすることができる。暗号文と機器認証鍵は通信ネットワークを介して暗号側通信装置（例えばサーバ）から復号側通信装置（例えばクライアント端末）へ配布される。これにより、コンテンツを暗号化した暗号文を特定のクライアント端末のみで復号可能な暗号化データとして配信することができる。

【００１７】

本発明の第２の目的は、それぞれ機器固有の機器認証鍵を有する第１の電子機器と第２の電子機器との間で秘密鍵暗号アルゴリズムにより送信データの暗号・復号化を行う暗号通信システムにおいて：

前記第１の電子機器は、

第１の電子機器の固有ＩＤ又は予め付与されたユニーク値を用いて作成された第１機器認証鍵Ｋａを記憶する第１機器認証鍵記憶手段と；

第２の電子機器から提供された第２の電子機器固有の第２機器認証鍵Ｋｂを読取る第２機器認証鍵読取手段と；

第１機器認証鍵Ｋａと第２機器認証鍵Ｋｂとを用いて暗号鍵を作成する暗号鍵作成手段と；

得られた暗号鍵を用いて、送信データＰを暗号文Ｃに暗号化する暗号化手段と；

得られた暗号文Ｃを第１機器認証鍵Ｋａを含む属性情報と共に第２の電子機器に送信する送信手段とを備え；

前記第２の電子機器は、

第２の電子機器の固有ＩＤ又は予め付与されたユニーク値を用いて作成された前記第２機器認証鍵Ｋｂを記憶する第２機器認証鍵記憶手段と；

第１の電子機器から送信された暗号文Ｃに添付された属性情報から第１機器認証鍵Ｋａを読取る第１機器認証鍵読取手段と；

読取られた第１機器認証鍵Ｋａと自己の第２機器認証鍵Ｋｂとを用いて復号鍵を作成する復号鍵作成手段と；

得られた復号鍵を用いて、第１の電子機器から提供された暗号文Ｃを復号化して平文の送信データＰを得る復号化手段と；

を備えることを特徴とする暗号通信システム、

により達成される（請求項１２）。

【００１８】

さらに本発明の第３の目的は、相手側電子機器に送る送信データを秘密鍵暗号アルゴリズムにより暗号化して送信し、また相手側電子機器から受信した暗号文を復号化する暗号通信装置において：電子機器の固有ＩＤ又は予め付与されたユニーク値を用いて作成された第１機器認証鍵Ｋａを記憶する機器認証鍵記憶手段と；相手側電子機器から提供された相手側電子機器固有の第２機器認証鍵Ｋｂを読取る機器認証鍵読取手段と；第１機器認証鍵Ｋａと第２機器認証鍵Ｋｂとを用いて暗号鍵を作成する暗号鍵作成手段と；得られた暗号鍵を用いて、送信データＰを暗号文Ｃに暗号化する暗号化手段と；得られた暗号文Ｃを第１機器認証鍵Ｋａを含む属性情報と共に相手側電子機器に送信し、また相手側電子機器から送信された暗号文と相手側機器認証鍵を含む属性情報を受信する送・受信手段と；第１機器認証鍵Ｋａと第２機器認証鍵Ｋｂとを用いて復号鍵を作成する復号鍵作成手段と；得られた復号鍵を用いて、相手側電子機器から提供された暗号文Ｃ’を平文の送信データＰ’に復号化する復号化手段を備えることを特徴とする暗号通信装置により達成される。

【００１９】

暗号化装置認証鍵（第１機器認証鍵Ｋａ）を含む属性情報を暗号文に付加する属性情報付加手段を設けるのが好ましい態様である。また、暗号鍵作成手段に、暗号化装置認証鍵

（第１機器認証鍵Ｋａ）と復号化装置認証鍵（第２機器認証鍵Ｋｂ）とを組み合わせて逆変換不能の疑似乱数を作成する疑似乱数作成エンジンを備えさせ、作成された疑似乱数を用いて暗号鍵を作成するものとすれば、より複雑安全な暗号鍵Ｋａｂを作成することができる。

【００２０】

この暗号通信装置は、利用者の端末装置に着脱可能な外部暗号化装置として構成してもよく、例えばＵＳＢメモリー、ＳＤメモリやＩＣカードなどの記憶媒体に各構成手段をプログラムで構成した態様とすることができる（請求項１４）。これにより、利用者が外部暗号通信装置装置を自分の端末装置から外しておくことにより、他人が当該利用者の端末を利用して当該利用者に成りすましたデータ送受信を行うことを防止できる。又、出先の端末装置に自分の外部暗号化装置を装着することにより、データの暗号通信を行うことができる。

【００２１】

送・受信手段を持たない外部暗号通信装置とした場合には、送・受信手段に代えて、暗号文Ｃを第１機器認証鍵Ｋａを含む属性情報と共に相手側電子機器に送信すること、また相手側電子機器から送信された暗号文Ｃ’と相手側機器認証鍵を含む属性情報を受信することを、当該外部暗号化通信装置を接続した電子機器に指示する送・受信指示手段を設けることができる。これにより外部暗号通信装置を装着した電子機器（例えばパソコン）の送受信端末を介して暗号通信を行うことが可能となる（請求項１５）。

【００２２】

また、外部暗号通信装置で使用する第１機器認証鍵Ｋａは、この外部暗号通信装置を装着する電子機器の固有ＩＤ又はこの電子機器に予め付与されたユニーク値を用いて作成されたものであってもよい（請求項１６）。

【００２３】

また、暗号通信装置の各手段（暗号鍵・復号鍵作成手段と暗号化・復号化手段）を論理回路として構成した集積回路（ＬＳＩ等）とし、機器認証鍵作成に使用する固有ＩＤはこの集積回路の製造番号または当該集積回路固有の識別情報としてもよい。又、これら各手段をプログラムとして構成してもよい。

【００２４】

本発明の第４の目的は、それぞれ機器固有の機器認証鍵を有する電子機器の間で、秘密鍵暗号アルゴリズムにより送・受信データの暗号・復号化を行う暗号通信プログラムにおいて；

送信側電子機器の機器認証鍵と受信側電子機器の機器認証鍵とを用いて暗号鍵を作成し；

この暗号鍵で送信データを暗号化して暗号文を作成し；

この暗号文と送信側電子機器の機器認証鍵とを相手側電子機器に送信することを特徴とする暗号通信プログラム、

により達成される（請求項１７）。

【００２５】

また本発明の第４の目的は、それぞれ機器固有の機器認証鍵を有する電子機器の間で、秘密鍵暗号アルゴリズムにより送・受信データの暗号・復号化を行う暗号通信プログラムにおいて；

受信した暗号文に添付された送信側電子機器の機器認証鍵と受信側電子機器の機器認証鍵とを用いて復号鍵を作成し；

この復号鍵を用いて暗号文を復号することを特徴とする暗号通信プログラム、

により達成される（請求項１８）。

さらに本発明の第４の目的は、それぞれ機器固有の機器認証鍵を有する電子機器の間で、秘密鍵暗号アルゴリズムにより送・受信データの暗号・復号化を行う暗号通信プログラムにおいて；

送信時には：

送信側電子機器の機器認証鍵Ｋａと受信側電子機器の機器認証鍵Ｋｂとを用いて暗号鍵Ｋａｂを作成するステップと；
この暗号鍵Ｋａｂで送信データＰを暗号化して暗号文Ｃを作成し；
この暗号文Ｃと送信側電子機器の機器認証鍵Ｋａとを相手側電子機器に送信し；
受信時には、
相手側電子機器から受信した暗号文Ｃ’に添付された相手側電子機器の機器認証鍵Ｋｂと受信側電子機器の機器認証鍵Ｋａとを用いて復号鍵Ｋｂａを作成し；
この復号鍵Ｋａｂを用いて暗号文Ｃ’を復号することを特徴とする暗号通信プログラム、によっても達成される（請求項１９）。

【００２６】

また本発明の第４の目的は、それぞれ機器固有の機器認証鍵を有する電子機器の間で、秘密鍵暗号アルゴリズムにより送信データの暗号・復号化を行う暗号通信プログラムであって、以下の各ステップを備えることを特徴とする暗号通信プログラム：
a) 送信側の第１の電子機器の機器認証鍵Ｋａと受信側の第２の電子機器の機器認証鍵Ｋｂとを組み合わせた暗号鍵Ｋａｂを作成し；
b) この暗号鍵Ｋａｂを用いて送信データＰを暗号文Ｃとし；
c) この暗号文Ｃと送信側電子機器の機器認証鍵Ｋａとを、第２の電子機器に送信し；
d) 相手側の第２の電子機器から暗号文Ｃ’と相手側の機器認証鍵Ｋｂとを受信し；
e) 受信側電子機器の機器認証鍵Ｋａと送信側電子機器の機器認証鍵Ｋｂとを用いて復号鍵Ｋａｂ作成し；
f) この復号鍵Ｋａｂを用いて前記暗号文Ｃ’を復号する、
により達成される（請求項２０）。

【発明を実施するための最良の形態】

【００２７】

以下、本発明の実施形態について図面を参照して説明する。図１は本発明の暗号通信方法の概念図、図２は暗号側通信装置（第１の電子機器）の実施形態を示す概念図、図３は復号側通信装置（第２の電子機器）の実施形態を示す概念図である。

【００２８】

これらの図において、符号１０は暗号側通信装置（第１の電子機器）であり、５０は復号側通信装置（第２の電子機器）である。暗号側通信装置１０は、暗号側装置認証鍵（第１機器認証鍵）Ｋａを記憶する機器認証鍵記憶手段１２Ａと、復号側装置認証鍵（第２機器認証鍵）Ｋｂを読取る機器認証鍵読取手段１２Ｂと、暗号鍵作成手段１４と暗号化手段１６とを備える。復号側通信装置５０は、相手側通信装置から受信した暗号文１１０に添付された相手側の第１機器認証鍵Ｋａを読取る機器認証鍵読取手段５２Ａと、復号側装置の機器認証鍵（第２機器認証鍵）Ｋｂを記憶する機器認証鍵記憶手段５２Ｂと、復号鍵作成手段５４と復号化手段５６とを備える。

【００２９】

暗号側装置１０の機器認証鍵記憶手段１２Ａは、暗号側装置１０の固有ＩＤを用いて作成された暗号側装置固有の機器認証鍵Ｋａを記憶する。この固有ＩＤとは、当該機器固有のＩＤ又は識別情報であり、例えば、ＣＰＵそれ自体に書き込まれている製造番号（シリアルナンバー）やネットワーク機器に互いを認識するための付されている機器識別ＩＤなどの固有の識別コード（ユニークＩＤ）を使用する。この固有ＩＤを例えば暗号化したものを機器認証鍵として用いる。或いは、電子機器のフラッシュメモリーなどに予め付与されたユニーク値を機器認証鍵としてもよい。このようなユニーク値として、製品番号や製造日付、電子機器を始動した日付、時間など、さらに任意の英数字を組み合わせたものを用いることができる。このようなユニーク値は、例えばＵＳＢメモリ、フラッシュメモリのコントローラ領域（一回だけ書き込み可能）に書き込むことにより付与する。復号化装置５０の機器認証鍵Ｋｂも、同様にして復号化装置５０の固有ＩＤを用いて作成されたものが第２の機器認証鍵記憶手段５２Ｂに記憶される。

【００３０】

暗号文作成の際には、暗号側通信装置１０は暗号鍵作成手段１４を用いて、自らの認証鍵Ｋａと相手側の復号側通信装置５０の機器認証鍵Ｋｂとを用いて暗号鍵Ｋａｂを作成する。作成された暗号鍵を用いて平文Ｐ（１００）を暗号化して暗号文Ｃ（１１０）を作成し、これに属性情報１２０を例えばヘッダーとして添付する。属性情報には暗号鍵作成に使用した機器認証鍵Ｋａを含めておく。暗号文Ｃを受信した相手の復号側通信装置５０は属性情報１２０から、暗号化装置１０が暗号鍵作成に使用した認証鍵Ｋａを読取り、自己の機器認証鍵Ｋｂと組み合わせて復号鍵作成手段５４により復号鍵Ｋａｂを作成する。作成された復号鍵Ｋａｂは暗号化に用いられた暗号鍵Ｋａｂと同じものとなる。この復号鍵を用いて復号化エンジン５６により暗号文Ｃを復号して平文Ｐとする。

【００３１】

図２により、暗号側電子機器１０内での暗号化処理の流れをより具体的に説明する。暗号鍵作成手段１４は、疑似乱数作成手段１８，キー作成手段２０，暗号鍵作成エンジン２２、秘密鍵記憶手段２４，乱数発生エンジン２６とを備えている。疑似乱数作成手段１８は、暗号化装置の機器認証鍵Ｋａと復号化装置の機器認証鍵Ｋｂとを組み合わせて逆変換不能の疑似乱数を作成するものであり、Hash関数を用いることができる。例えば、認証鍵Ｋａが「Ａ１０１」であり、認証鍵Ｋｂが「Ｂ２０２」で表せる場合には、これらをパスフレーズとしてタンデムに連結した「Ａ１０１Ｂ２０２」をhash関数で処理して疑似乱数を求める。求められた疑似乱数を、キーボードなど外部入力手段２８で入力されたパスワードと秘密鍵記憶手段２４に記憶された秘密鍵と組み合わせ、キー作成手段２０によりキー（Ｘ）を作成する。このキー（Ｘ）は、疑似乱数、パスワード、秘密鍵を単に連結したものでもよいし、加減乗除したものでもよい。秘密鍵は、暗号化装置利用者と復号化装置利用者を企業内や、特定のグループに属するものに限定する場合に使用するグループ情報であり、同一グループに属する相手側通信装置５０にも秘密鍵記憶手段６２に同じ秘密鍵を記憶しておく（図３参照）。

【００３２】

作成されたキー（Ｘ）は、暗号鍵作成エンジン２２により、共有キー（Ｙ）と乱数（Ｚ）と組み合わせられ、暗号鍵（Ｘ・Ｙ・Ｚ）が作成される。共有キー（Ｙ）は、復号化装置５０にも同じものが記憶されている。但し、乱数は暗号文作成の度に異なる数字となるように、乱数発生エンジン２６により作成されたものを使用する。暗号鍵（Ｘ・Ｙ・Ｚ）は、Ｘ，Ｙ，Ｚを連結しただけのものでもよいし、或いは適当なアルゴリズムにより数学的処理を行ったものでもよい。

【００３３】

作成された暗号鍵（Ｘ・Ｙ・Ｚ）をＫａｂとして用いて、暗号化エンジン１６により平文Ｐ（１００）を暗号化し暗号文Ｃ（１１０）が作成される。さらに、属性情報付加手段３０が、暗号化装置の機器認証鍵Ｋａ，パスワード、乱数（Ｚ）を属性情報１２０として暗号文Ｃ（１１０）に添付する。こうして作成された暗号文と属性情報とが復号化装置５０に送信される。なお、属性情報１２０は、暗号文１１０のヘッダーとしてもよいが、暗号文内部に潜在させ、その存在箇所、或いは存在自体が復号化装置以外からは分からないようにすることもできる。

【００３４】

次に、暗号文を受信した復号側電子機器５０内での復号化処理の流れを図３により説明する。復号鍵作成手段５４は、疑似乱数作成手段５８，キー作成手段６０，復号鍵作成エンジン６２、秘密鍵記憶手段６４とを備えている。これらは、暗号化装置１０の疑似乱数作成手段１８，キー作成手段２０，暗号鍵作成エンジン２２、秘密鍵記憶手段２４と同じものである。乱数発生エンジンを使用しない点のみが暗号鍵作成手段１４と異なる。復号化エンジン５６は暗号化エンジン１６と対称アルゴリズムのものである。復号化装置５０が暗号化装置１０と異なるその他の点は、属性情報読取り手段６６を備えている点である。

【００３５】

暗号化装置１０で作成された暗号文Ｃ（１１０）とその属性情報１２０を受け取った復

号化装置５０は、その属性情報読取手段６６、機器認証鍵読取手段５２Ａにより、属性情報内に格納された暗号化装置の機器認証鍵Ｋａを読取る。

【００３６】

この機器認証鍵Ｋａと機器認証鍵記憶手段５２Ｂに記憶されれていた暗号化装置の機器認証鍵Ｋａとを組み合わせて、疑似乱数を作成する。使用する疑似乱数作成手段５８は暗号化装置１０の疑似乱数作成手段１８と同じものであるから、作成される疑似乱数は暗号装置１０で作成されていた疑似乱数と同じものとなる。以下、パスワード入力手段（キーボードなど）７０から入力されたパスワード、秘密鍵記憶手段６４に記憶されている秘密鍵を用いてキー作成手段６０によってキー（Ｘ）を作成する。属性情報読取り手段６６で属性情報１２０に格納されていた乱数（Ｚ）を読取り、復号鍵作成エンジン６２は、キー（Ｘ），共有キー（Ｙ）、乱数（Ｚ）を組み合わせて復号鍵（Ｘ・Ｙ・Ｚ）を作成する。入力されたパスワードが正しければ、そして秘密鍵が暗号化装置のものと同じであれば、最終的に作成される復号鍵は、暗号鍵と同じものとなり、暗号化エンジン５８により暗号文１１０を平文に復号することができる。

【００３７】

以上の暗号化装置（第１の電子機器）、復号化装置（第２の電子機器）の構成手段は、プログラムとして構成してもよく、又論理回路として構成したＬＳＩなどの集積回路とすることもできる。又、暗号化装置、復号化装置は、利用者の端末に着脱可能とした外部装置としてもよい。外部装置としてＵＳＢメモリー，ＳＤカード、ＩＣカードなどの記憶媒体を用い、各構成手段をプログラムで構成することができる。暗号化エンジン、復号化エンジンが複雑な処理を要求されない対称アルゴリズムであるので、メモリ量が少ない外部装置でも高速処理が可能となる。

【００３８】

暗号化装置と復号化装置の各構成要素をまとめて暗号化・復号化装置としてもよい。暗号化する平文は発信者と送信者間で通信されるデータであればよく、例えば、コンテンツを配信する場合に、特定の復号化装置を持つ受信者のみが復号できる暗号文として配信することができる。

【００３９】

次に、電子機器（通信装置）間で交互に暗号通信を行う工程について、第４～７図により詳細に説明する。第４図は暗号側通信装置（第１の電子機器）としてのクライアント端末と復号側通信装置（第２の電子機器）としてのサーバとの間で行われる１回目の認証工程を示す概念図であり、クライアント端末における送信データ暗号化工程と、暗号文を受信したサーバにおけるデータ復号化工程を示す。第５図は、サーバからの再認証工程を示す概念図であり、サーバーにおける送信データ暗号化工程と、暗号文を受信したクライアント端末におけるデータ復号化工程を示す。第６図は、暗号通信開始時に電子機器間で行われる認証工程のシーケンスを示す図である。第７図は、認証後にも送受信ごとに交互に機器認証を行いながらの暗号通信を行うシーケンスを示す図である。

【００４０】

まず第１の電子機器（クライアント端末）１０から第２の電子機器（サーバ）５０に接続要求の通信を行う（図６、ステップ１０２）。第４図に示すように、サーバ５０は平文作成手段により任意の平文Ｐを作成し、第２機器認証鍵記憶手段１２Ｂ’から読み出したサーバ機器認証鍵Ｋｂと共に、送受信手段８０’から、クライアント１０の送受信手段８０に送信する（第６図、ステップＳ１０４）。この段階では、平文Ｐは暗号化されていない。

【００４１】

クライアント端末１０の第２機器認証鍵読取手段１２Ｂは受信したサーバ機器認証鍵Ｋｂを読取り、得られたサーバ機器認証鍵Ｋｂと第１機器認証鍵記憶手段１２Ａに記憶されていたクライアント１０の機器認証鍵Ｋａとを組み合わせて暗号鍵Ｋａｂを作成する（ステップＳ１０６）。暗号化手段１６はこの暗号鍵Ｋａｂによりサーバ５０から受信した平文Ｐを暗号化し暗号文Ｃを得る（ステップＳ１０８）。この暗号文Ｃとクライアント端末

１０の機器認証鍵Ｋａとを送受信手段８０を介してサーバ５０に送信する（ステップＳ１１０）。

【００４２】

サーバ５０の第１機器認証鍵読取手段１２Ａ’は受信暗号文Ｃに添付されたクライアント機器認証鍵Ｋａを読取る。復号鍵作成手段５４’は読取られた機器認証鍵Ｋａと第２機器認証鍵記憶手段に記憶されているサーバ５０の機器認証鍵Ｋｂを組み合わせて復号鍵Ｋａｂを作成し（ステップＳ１１２）、復号化手段５６’は、得られた復号鍵Ｋａｂを用いてクライアント端末から送られた暗号文Ｃを復号して平文Ｐ’を得る（ステップＳ１１４）。得られた平文Ｐ’が、先にクライアント端末に送信した平文Ｐと一致するか平文比較手段（認証手段）７２により比較する（ステップＳ１１６）。平文Ｐ，Ｐ’が一致しない場合は、暗号文Ｃを送信した相手側は、サーバーが前回送信で平文Ｐを送信したクライアント端末ではないとして、以降の通信を停止する。

【００４３】

平文Ｐ，Ｐ’が一致していれば、暗号文Ｃを送信した相手側はサーバの機器認証鍵Ｋｂを入手したクライアント１０であると認証出来たことになり、以降の通信を続ける。サーバはクライアントに再度の認証手続を行う（図５）。サーバ５０の平文作成手段７０は、前回送信した平文Ｐとは異なる平文Ｐ２を作成する。クライアント１０から送られてきたクライアント機器認証鍵Ｋａとサーバの機器認証鍵Ｋｂとを用いて、この平文Ｐ２を暗号化し暗号文Ｃ２を作成し（ステップＳ１１８）、暗号文Ｃ２とサーバ機器認証鍵Ｋｂをクライアント１０に送信する（ステップＳ１２０）。

【００４４】

クライアント１０は受信した暗号文に添付された相手側機器認証鍵Ｋｂと自己の機器認証鍵Ｋａとを用いて、改めて復号鍵Ｋａｂを作成し（ステップＳ１２２）、得られた復号鍵Ｋａｂで暗号文Ｃ２を復号する（ステップＳ１２４）。復号できれば暗号文Ｃ２を送信してきた相手側は、前回クライアントから送信した相手側（すなわちサーバ５０）であることが認証できる。復号できなければ前回クライアントから送信した相手側（すなわちサーバ５０）からの通信ではないものと判定できる。なお、暗号文Ｃ２の復号に成功したかどうかは、復号鍵で復号したものが判読可能な意味のある内容であるかどうかで判断が出来る。平文Ｐ２をテキスト文とした場合には、その暗号文Ｃ２を正規に復号できなければ、意味のある文章が得られないばかりでなく、全て文字化けのテキストとして文章を構成しないことになる。このことから復号成功の判別が可能である。

【００４５】

クライアント１０は復号して得られた平文Ｐ２’をサーバ５０に送信する（ステップＳ１２６）。サーバ５０は受信した平文Ｐ２’を直前の通信でクライアントに送った平文Ｐ２と比較し、一致していれば、通信相手は通信開始時のクライアント１０であることを認証できる（ステップＳ１２８）。

【００４６】

この後、初めてサーバ５０よりクライアント１０に通信データが送信される。サーバ５０は送信すべきデータを暗号鍵Ｋａｂで暗号化し（図７，ステップＳ１３０）、得られたデータ暗号文Ｃ３をサーバ機器認証鍵Ｋｂと共にクライアント１０に送信する（ステップＳ１３２）。クライアント１０では、送られてきた機器認証鍵Ｋｂと自己の機器認証鍵Ｋａとを用いて改めて復号鍵を作成し（ステップＳ１３４）、データ暗号文Ｃ３を復号する（ステップＳ１３６）。復号できれば相手側はサーバ５０であると認証できる。

【００４７】

クライアント１０は返信データを作成し、又は既に作成済みの返信データを用意し（ステップＳ１３８）、暗号文Ｃ３に添付されてた相手側機器認証鍵Ｋｂと自己の機器認証鍵Ｋａとを組み合わせて、再度暗号文を作成し、送信データを暗号化し（ステップＳ１４０）、得られた暗号文Ｃ４を自己の機器認証鍵Ｋａと共にサーバ５０に送信する（ステップＳ１４２）。

【００４８】

サーバ５０は送られてきたクライアント認証鍵Ｋａと自己の機器認証鍵Ｋｂとで新たに復号鍵Ｋａｂを作成し、データ暗号文Ｃ４を復号する。復号したものが判読可能であれば復号成功であり、同時に相手側が通信相手のクライアント１０であることを認証出来たことになる（ステップＳ１４６）。これまでと同様、相手側からの直前の暗号通信で送られてきた相手側機器認証鍵Ｋａを用いて暗号鍵Ｋａｂを作成してクライアントから要求されたデータを暗号化し（ステップＳ１４８）、得られたデータ暗号文Ｃ６をサーバ機器認証鍵Ｋｂと一緒にクライアントに送信する（ステップＳ１５０）。クライアント１０は、これまでと同様にして復号鍵作成（ステップＳ１５２）、データ暗号文Ｃ５の復号とこれに付随する相手側機器の認証を行う（ステップＳ１５４）。暗号文Ｃ５の復号と認証に成功したならば、前回同様の手順でデータ作成（ステップＳ１５６）、データ暗号化（ステップＳ１５８）を行い、得られたデータ暗号文Ｃ６を自己の機器認証鍵Ｋａと共にサーバ５０に送信する（ステップＳ１６０）。

【００４９】

この後も、これまでと同様、相手側からの直前の通信で送られてきた相手側機器認証鍵を用いて、送信の度ごとに暗号鍵の作成、受信の度ごとに復号鍵の作成を行いながら、暗号通信を行う（ステップＳ１６２，１６４）。これにより暗号通信を行いながら、常に相手側が直前の通信を行った相手側電子機器であったかどうかの確認、認証が出来る。すなわち暗号通信の送受信ごとに相手側電子機器の機器認証を交互に行うことが出来る。暗号通信を傍受して、添付されていた機器認証鍵を入手しても暗号文の復号、データの暗号化を行うことが出来ない。これにより暗号通信の機密性を極めて高くすることが出来る。暗号通信に用いる暗号方式は共通鍵を用いたものであるから、高速な暗号化処理、復号化処理を行うことが出来、データを交互に高速に送受信することが可能である。

【産業上の利用可能性】

【００５０】

以上のように本発明の暗号通信方法・システムでは、それぞれ機器固有の機器認証鍵を有する電子機器の間で、相手側機器認証鍵と自己の機器認証鍵を用いて作成した暗号・復号鍵を用いて秘密鍵暗号アルゴリズムにより送・受信データの暗号・復号化を行う。互いに、送信するデータを暗号鍵を用いて暗号化した暗号化データとし、この暗号化データと共に送信側の機器認証鍵のみを相手側に送信する。相手側電子機器では、受信した暗号化データに添付されていた相手側機器認証鍵と自己の機器認証鍵を用いて復号鍵を作成し、この復号鍵を用いて暗号化データを復号する。これにより、特定の相手側電子機器のみで復号可能な暗号文で暗号通信を行うことが出来る。また、暗号通信の送受信ごとに相手側電子機器の機器認証を交互に行うことが出来るので、通信の安全性が極めて高いものとなる。復号処理で使用する復号鍵は暗号鍵と同じ鍵となるので、復号化エンジンのアルゴリズムに複雑なものが必要なく、高速な復号処理が可能となり、高速通信における暗号通信が可能となる。

【図面の簡単な説明】

【００５１】

【図１】本発明の暗号通信方法の概念図

【図２】暗号側通信装置（第１の電子機器）の実施形態を示す概念図

【図３】復号側通信装置（第２の電子機器）の実施形態を示す概念図

【図４】暗号側通信装置（第１の電子機器）としてのクライアント端末と復号側通信装置（第２の電子機器）としてのサーバとの間で行われる１回目の認証工程を示す概念図であり、クライアント端末における送信データ暗号化工程と、暗号文を受信したサーバにおけるデータ復号化工程を示す図

【図５】サーバからの再認証工程を示す概念図

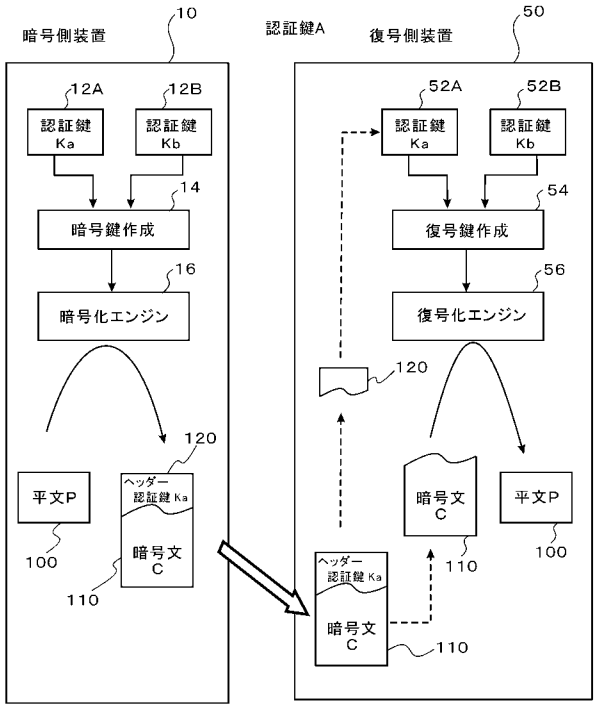
【図６】暗号通信開始時に電子機器間で行われる認証工程のシーケンスを示す図

【図７】認証後にも送受信ごとに交互に機器認証を行いながらの暗号通信を行うシーケンスを示す図

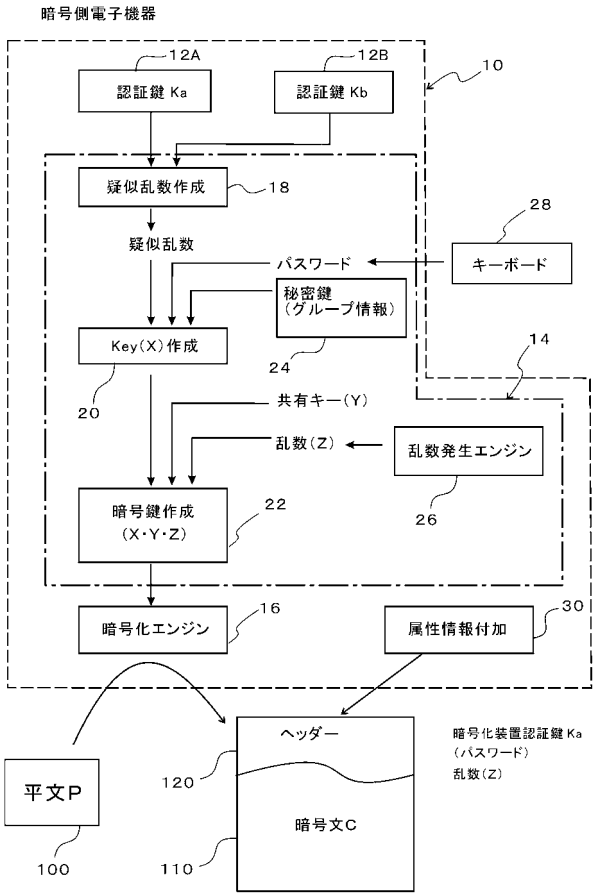
【符号の説明】

【００５２】
１０　暗号側通信装置（第１の電子機器）
１２Ａ　機器認証鍵記憶手段
１２Ｂ　機器認証鍵読取手段
１４、１４’暗号鍵作成手段
１６、１６’　暗号化手段（暗号化エンジン）
１８、５８　疑似乱数作成エンジン
２０、６０　キー作成手段
２２　暗号鍵作成エンジン
２４、６４　秘密鍵記憶手段
２６　乱数発生エンジン
２８、７０　パスワード入力手段
３０　属性情報付加手段
５０　復号側通信装置（第２の電子機器）
５２Ａ　機器認証鍵読取手段
５２Ｂ　機器認証鍵記憶手段
５４　５４’　復号鍵作成手段
５６　５６’　復号化手段（復号エンジン）
６２　復号鍵作成エンジン
６６　属性情報読取り手段
７０　平文作成手段
７２　平文比較（認証）手段
８０，８０’　送受信（指示）手段
１００　平文
１１０　暗号文
１２０　属性情報

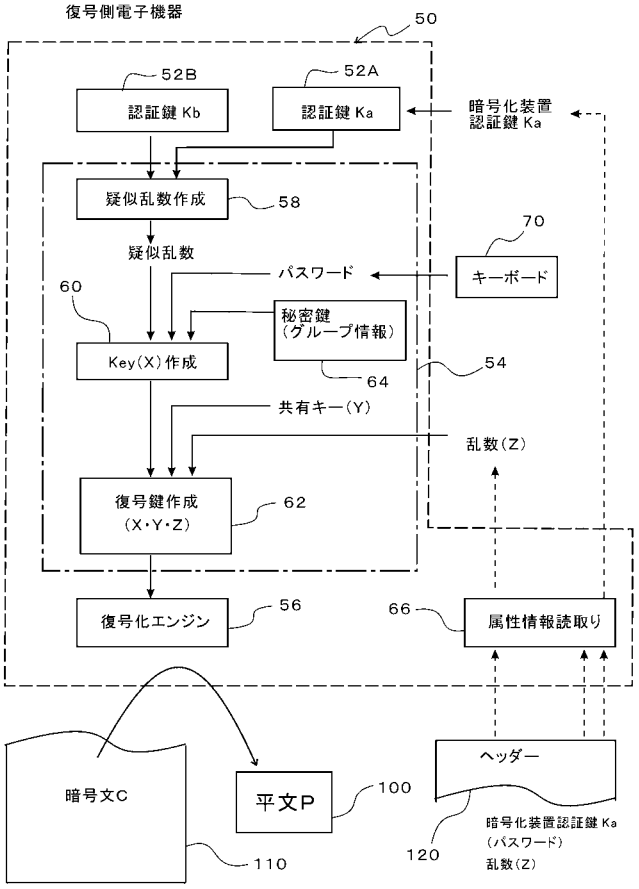
【図１】


暗号側装置
10
認証鍵A
復号側装置
50
12A
認証鍵 Ka
12B
認証鍵 Kb
52A
認証鍵 Ka
52B
認証鍵 Kb
14
暗号鍵作成
54
復号鍵作成
16
暗号化エンジン
56
復号化エンジン
120
平文P
100
ヘッダー
認証鍵 Ka
暗号文 C
110
暗号文 C
110
ヘッダー
認証鍵 Ka
暗号文 C
110
暗号文 C
110
平文P
100

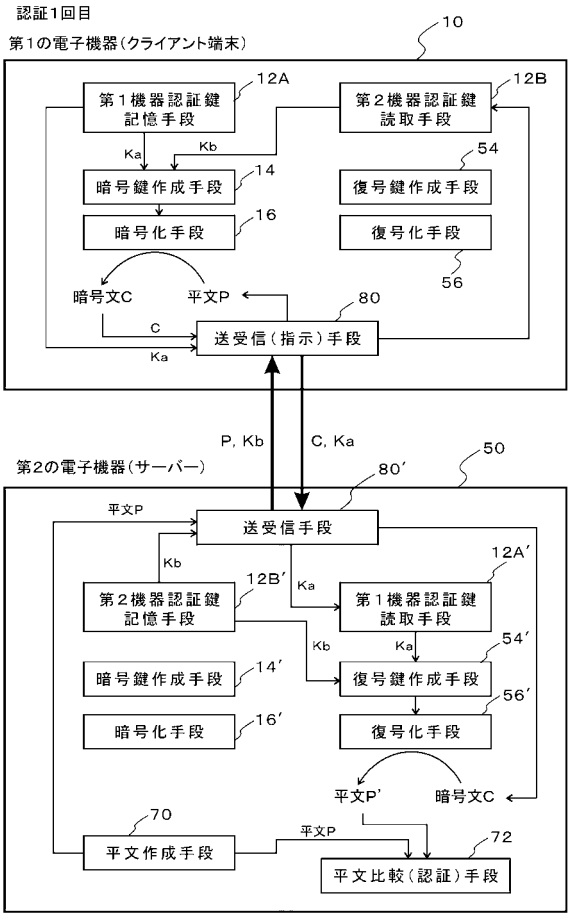
【図２】


暗号側電子機器
12A
認証鍵 Ka
12B
認証鍵 Kb
10
疑似乱数作成
18
疑似乱数
パスワード
28
キーボード
秘密鍵
（グループ情報）
24
Key(X)作成
20
14
共有キー(Y)
乱数(Z)
乱数発生エンジン
26
暗号鍵作成
(X・Y・Z)
22
暗号化エンジン
16
属性情報付加
30
ヘッダー
120
暗号文C
110
平文P
100
暗号化装置認証鍵 Ka
（パスワード）
乱数(Z)

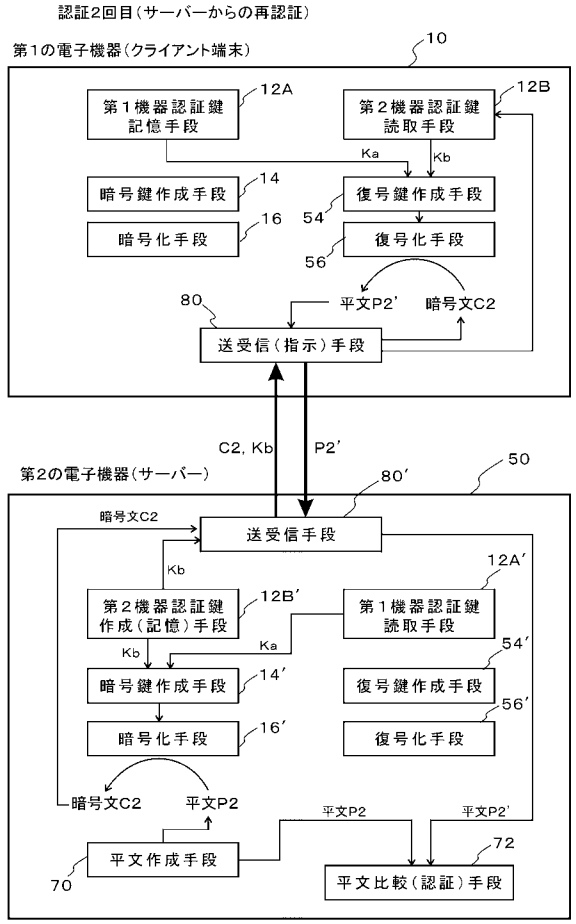
【図３】


復号側電子機器
50
52B
認証鍵 Kb
52A
認証鍵 Ka
暗号化装置
認証鍵 Ka
疑似乱数作成
58
70
疑似乱数
パスワード
キーボード
60
秘密鍵
（グループ情報）
Key(X)作成
64
54
共有キー(Y)
乱数(Z)
復号鍵作成
(X・Y・Z)
62
復号化エンジン
56
66
属性情報読取り
暗号文C
110
平文P
100
ヘッダー
120
暗号化装置認証鍵 Ka
（パスワード）
乱数(Z)

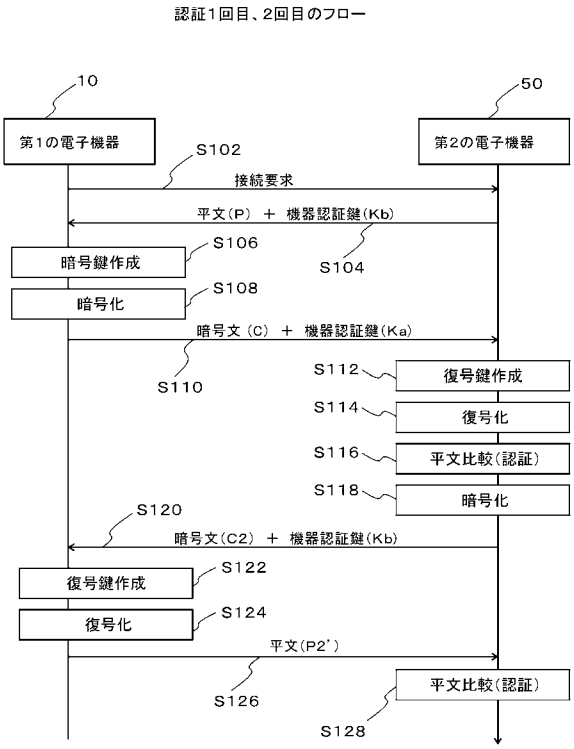
【図４】


認証1回目
第1の電子機器（クライアント端末）
10
第1機器認証鍵
記憶手段
12A
第2機器認証鍵
読取手段
12B
Ka
Kb
暗号鍵作成手段
14
復号鍵作成手段
54
暗号化手段
16
復号化手段
56
暗号文C
平文P
80
C
Ka
送受信（指示）手段
P, Kb
C, Ka
第2の電子機器（サーバー）
50
80′
平文P
送受信手段
Kb
12B′
Ka
12A′
第2機器認証鍵
記憶手段
第1機器認証鍵
読取手段
Kb
Ka
暗号鍵作成手段
14′
復号鍵作成手段
54′
暗号化手段
16′
復号化手段
56′
平文P′
暗号文C
70
平文作成手段
平文P
72
平文比較（認証）手段

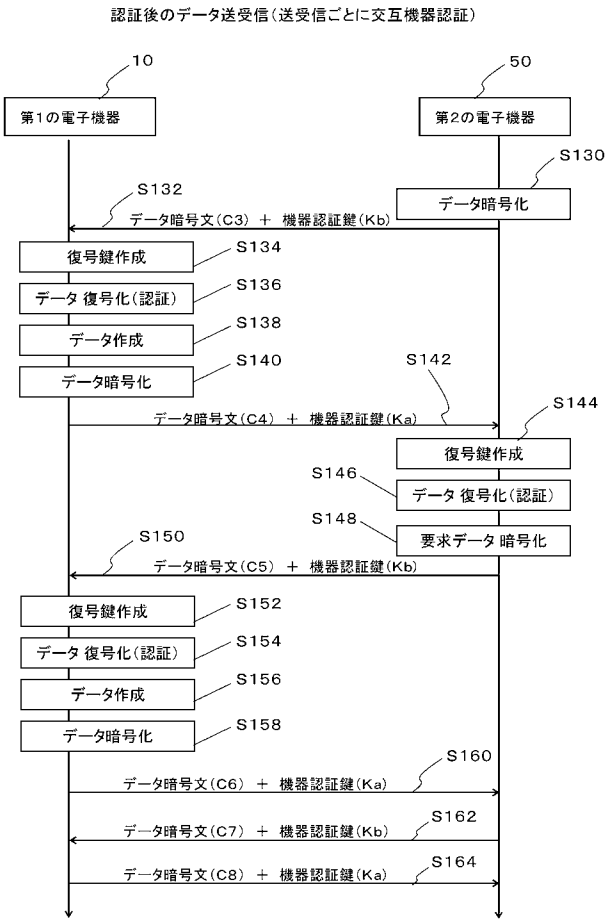
【図５】


認証2回目（サーバーからの再認証）
第1の電子機器（クライアント端末）
10
第１機器認証鍵記憶手段
12A
第２機器認証鍵読取手段
12B
Ka
Kb
暗号鍵作成手段
14
復号鍵作成手段
54
暗号化手段
16
復号化手段
56
80
平文P2'
暗号文C2
送受信（指示）手段
C2, Kb
P2'
第2の電子機器（サーバー）
50
80'
暗号文C2
送受信手段
Kb
12A'
第２機器認証鍵作成（記憶）手段
12B'
第１機器認証鍵読取手段
Ka
Kb
54'
暗号鍵作成手段
14'
復号鍵作成手段
56'
暗号化手段
16'
復号化手段
暗号文C2
平文P2
平文P2
平文P2'
72
平文作成手段
70
平文比較（認証）手段

【図６】


認証1回目、2回目のフロー
10
第1の電子機器
50
第2の電子機器
S102
接続要求
平文（P）＋機器認証鍵（Kb）
S104
暗号鍵作成
S106
暗号化
S108
暗号文（C）＋機器認証鍵（Ka）
S110
S112
復号鍵作成
S114
復号化
S116
平文比較（認証）
S118
暗号化
S120
暗号文（C2）＋機器認証鍵（Kb）
復号鍵作成
S122
復号化
S124
平文（P2'）
S126
平文比較（認証）
S128

【図７】


認証後のデータ送受信（送受信ごとに交互機器認証）
10
第1の電子機器
50
第2の電子機器
S130
S132
データ暗号化
データ暗号文（C3）＋機器認証鍵（Kb）
復号鍵作成
S134
データ 復号化（認証）
S136
データ作成
S138
データ暗号化
S140
S142
データ暗号文（C4）＋機器認証鍵（Ka）
S144
復号鍵作成
S146
データ 復号化（認証）
S148
要求データ 暗号化
S150
データ暗号文（C5）＋機器認証鍵（Kb）
復号鍵作成
S152
データ 復号化（認証）
S154
データ作成
S156
データ暗号化
S158
S160
データ暗号文（C6）＋機器認証鍵（Ka）
S162
データ暗号文（C7）＋機器認証鍵（Kb）
S164
データ暗号文（C8）＋機器認証鍵（Ka）