(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2010 年 6 月 10 日(10.06.2010)

PCT

(10) 国際公開番号
WO 2010/064666 A1

(51) 国際特許分類:
H04L 9/08 (2006.01)

(21) 国際出願番号: PCT/JP2009/070284

(22) 国際出願日: 2009 年 12 月 3 日(03.12.2009)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2008-311360 2008 年 12 月 5 日(05.12.2008) JP

(71) 出願人 (米国を除く全ての指定国について): パナソニック電工株式会社 (PANASONIC ELECTRIC WORKS CO., LTD.) [JP/JP]; 〒5718686 大阪府門真市大字門真１０４８番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 福田 尚弘 (FUKUDA, Naohiro) [JP/JP]; 〒5718686 大阪府門真市大字門真１０４８番地 パナソニック電工株式会社内 Osaka (JP).

(74) 代理人: 西川 惠清, 外 (NISHIKAWA, Yoshikiyo et al.); 〒5300001 大阪府大阪市北区梅田１丁目１２番１７号 梅田スクエアビル９階 北斗特許事務所 Osaka (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

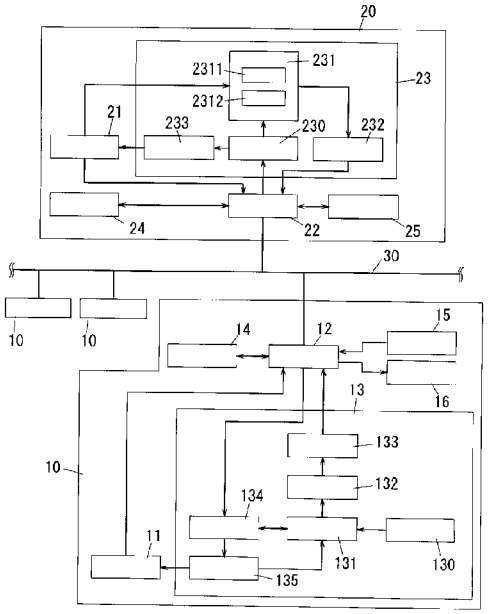
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告（条約第 21 条(3)）

(54) **Title**: KEY DISTRIBUTION SYSTEM

(54) 発明の名称 : 鍵配布システム

[図1]



(57) **Abstract**: The key distribution system is equipped with terminals (10), which engage in encrypted communications with one another using a secret communication key (K10) as a common key, and a server (20). When requesting that a new secret communication key (K11) be issued, a terminal (10) generates a secret value (R10), encrypts it using a public key, and sends it to the server (20). The server (20) encrypts the encrypted secret value (R10) using a private key that is paired with the public key. The server (20) issues a new secret communication key (K11), encrypts it using the secret value (R10) as a common key, and transmits it to the terminal (10). The terminal (10) decodes the encrypted new secret communication key (K11) using the secret value (R10) in order to obtain the new secret communication key (K11). The terminal (10) and the server (20) subsequently engage in encrypted communication with each other using the new secret communication key (K11) as a common key.

(57) 要約: 鍵配布システムは、通信用秘密鍵（Ｋ１０）を共通鍵として用いて互いに暗号化通信を行う端末（１０）とサーバ（２０）とを備える。上記端末（１０）は、新たな通信用秘密鍵（Ｋ１１）の発行の要求時には、秘密値（Ｒ１０）を生成し、公開鍵で暗号化して上記サーバ（２０）に送信する。上記サーバ（２０）は、上記暗号化された秘密値（Ｒ１０）を上記公開鍵とペアとなる私有鍵で復号化する。上記サーバ（２０）は、新たな通信用秘密鍵（Ｋ１１）を発行し、秘密値（Ｒ１０）を共通鍵として用いて暗号化して上記端末（１０）に送信する。上記端末（１０）は、暗号化された上記新たな通信用秘密鍵（Ｋ１１）を上記秘密値（Ｒ１０）を用いて復号化して上記新たな通信用秘密鍵（Ｋ１１）を取得する。その後、上記端末（１０）と上記サーバ（２０）とは、上記新たな通信用秘密鍵（Ｋ１１）を共通鍵として用いて互いに暗号化通信を行う。

WO 2010/064666 A1

明　細　書

発明の名称 ： 鍵配布システム

技術分野

[0001] 本発明は、鍵配布システムに関し、特にサーバと端末との間の暗号化通信に用いられる共通鍵である通信用秘密鍵をサーバが端末に配布する鍵配布システムに関する。

背景技術

[0002] 従来から、有効期限を定めたセッション鍵を用いて暗号化通信を行う通信システムがある。この通信システムでは、セッション鍵を暗号化して配布する。セッション鍵の暗号化には、クリプトナイトプロトコルと称する共通鍵暗号が用いられる。

[0003] 共有鍵暗号では、サーバ（住宅用サーバ）と端末（設備機器）とには同じ共通鍵（以下では、「通信用秘密鍵」という）があらかじめ設定される。通信用秘密鍵は端末毎に決まっているから、端末の利用者が変わったとしても端末の通信用秘密鍵は変わらない。したがって、端末を前に利用していた利用者は、端末から通信用秘密鍵を取得しておけば、端末とサーバとの間の通信を傍受できる。そのため、同じ端末の新たな利用者による利用状況（たとえば生活習慣）などが前の利用者に監視されたり、前の利用者によって端末が不正に利用されたり（勝手に操作されたり）するおそれがある。

[0004] 文献１（特開２０００－３４９７４８号公報）は、共有鍵暗号よりも通信の秘匿性が高い公開鍵暗号を開示する。公開鍵暗号であっても、公開鍵と私有鍵とを変更しない限り、前の利用者が通信を傍受することを完全には防止できない。

[0005] そこで、利用者が変わった際には、公開鍵と私有鍵とを変更することが考えられる。しかしながら、文献１に開示された公開鍵暗号は、送信者と受信者とが情報を共有するために送信者と受信者とがそれぞれ相手の公開鍵とペアになる秘密鍵（私有鍵）を保有していなければならない。そのため、文献

１に開示された公開鍵暗号では、秘密鍵そのものの交換は行えない。

発明の開示

[0006] 本発明は上記事由に鑑みて為された。本発明の目的は、サーバが新たに発行した、端末との暗号化通信に用いる通信用秘密鍵を他者に知られないように安全にサーバから端末に配布できる鍵配布システムを提供することである。

[0007] 本発明に係る鍵配布システムは、端末と、通信ネットワークを介して上記端末に接続されるサーバとを備える。上記端末は、通信用秘密鍵と公開鍵とを記憶する書換可能な第１鍵記憶ユニットを有する。上記端末は、上記第１鍵記憶ユニットに記憶された上記通信用秘密鍵を共通鍵として用いた暗号化通信を上記サーバと行うための第１通信ユニットを有する。上記端末は、鍵要求ユニットを有する。上記鍵要求ユニットは、上記サーバに新たな通信用秘密鍵の発行を要求するときに、数値よりなる秘密値を新たに生成するように構成される。上記鍵要求ユニットは、さらに、上記第１記憶ユニットに記憶された上記公開鍵を用いて上記秘密値を暗号化して第１の暗号を生成し、上記第１の暗号を上記サーバに送信するように構成される。上記サーバは、上記通信用秘密鍵に加えて、上記公開鍵とペアになる私有鍵である復号用秘密鍵を記憶する書換可能な第２鍵記憶ユニットを有する。上記サーバは、上記第２鍵記憶ユニットに記憶された上記通信用秘密鍵を共通鍵として用いた暗号化通信を上記端末と行うための第２通信ユニットを有する。上記サーバは、鍵発行ユニットを有する。上記鍵発行ユニットは、上記端末から新たな通信用秘密鍵の発行が要求されると、新たな通信用秘密鍵を発行して上記第２鍵記憶ユニットに記憶させるように構成される。上記鍵発行ユニットは、さらに、上記復号用秘密鍵を用いて上記第１の暗号を復号化することによって上記秘密値を取得するように構成される。上記鍵発行ユニットは、さらに、当該秘密値を利用して上記新たな通信用秘密鍵を暗号化して第２の暗号を生成し、新たな通信用秘密鍵の発行を要求した上記端末に上記第２の暗号を送信するように構成される。上記鍵要求ユニットは、上記秘密値を利用して

上記第２の暗号を復号化することによって上記新たな通信用秘密鍵を取得して、上記第１鍵記憶ユニットに記憶させるように構成される。上記第１通信ユニットは、上記第１鍵記憶ユニットに上記新たな通信用秘密鍵が記憶された後は、上記新たな通信用秘密鍵を共通鍵として用いた暗号化通信を上記サーバと行うように構成される。上記第２通信ユニットは、上記第２鍵記憶ユニットに上記新たな通信用秘密鍵が記憶された後は、上記新たな通信用秘密鍵を共通鍵として用いた暗号化通信を上記端末と行うように構成される。

[0008] この鍵配布システムでは、端末がサーバに新たな通信用秘密鍵の発行を要求する際に、公開鍵を用いて秘密値を暗号化してサーバに送信する。サーバは、暗号化された秘密値を公開鍵とペアになる私有鍵を用いて復号化する。サーバは、新たな通信用秘密鍵を、秘密値で復号化できるように暗号化して、端末に送信する。端末は、暗号化された通信用秘密鍵を、秘密値を利用して復号化して、新たな通信用秘密鍵を取得する。したがって、この鍵配布システムによれば、新たな通信用秘密鍵をサーバから端末に安全に届けることができる。

[0009] 好ましくは、上記鍵要求ユニットは、上記サーバに新たな通信用秘密鍵の発行を要求するときに、上記第１鍵記憶ユニットに記憶された上記通信用秘密鍵を上記公開鍵として用いて上記新たに生成された秘密値を暗号化するように構成される。上記鍵発行ユニットは、上記端末から新たな通信用秘密鍵の発行が要求されると、上記新たな通信用秘密鍵を発行するとともに、上記新たな通信用秘密鍵とペアになる私有鍵である新たな復号用秘密鍵を発行して上記第２鍵記憶ユニットに記憶させ、上記第２記憶ユニットに上記新たな復号用秘密鍵が記憶された後は、上記新たな復号用秘密鍵を用いて上記第１の暗号を復号化するように構成される。

[0010] この鍵配布システムによれば、通信用秘密鍵を公開鍵として用いるから、サーバだけが暗号化された秘密値を復号化できる。したがって、第三者は、通信用秘密鍵を用いても、暗号化された秘密鍵を復号化できない。よって、新たな通信用秘密鍵をサーバから端末により安全に届けることができる。

[0011] 好ましくは、上記鍵要求ユニットは、上記秘密値として使用する第１乱数と、第２乱数とを生成し、上記サーバに新たな通信用秘密鍵の発行を要求する前に上記第２乱数を上記サーバに送信し、上記第１乱数と上記第２乱数との単純演算により通信数値を生成し、上記公開鍵を用いて上記通信数値を暗号化して上記サーバに送信するように構成される。

[0012] この鍵配布システムによれば、第三者に秘密値が知られてしまうことを防止でき、通信用秘密鍵が第三者に知られる可能性を低減できる。しかも、秘密値より桁数が多い通信数値は、端末からサーバに秘密値を送信するときだけ使用される。そのため、秘密値より桁数が大きい通信数値を用いて通信用秘密鍵の暗号化や復号化を行わなくて済み、端末やサーバの処理負荷を低減できる。

[0013] 好ましくは、上記鍵発行ユニットは、上記端末から新たな通信用秘密鍵の発行が要求されると、上記端末から受信した上記秘密値を含むメッセージコードを生成し、上記メッセージコードを用いて上記新たな通信用秘密鍵を暗号化して上記端末に送信するように構成される。

[0014] この鍵配布システムによれば、メッセージ認証を行うことによって、サーバと端末とは、第三者による通信用秘密鍵の改竄を検出できる。よって、通信用秘密鍵を用いた暗号化通信の安全性を保証できる。

[0015] 本発明に係る別の鍵配布システムは、端末と、通信ネットワークを介して上記端末に接続されるサーバとを備える。上記端末は、通信用秘密鍵を記憶する書換可能な第１鍵記憶ユニットと、所定の原始元を記憶する第１原始元記憶ユニットと、を有する。上記端末は、上記第１記憶ユニットに記憶された上記通信用秘密鍵を共通鍵として用いた暗号化通信を上記サーバと行うための第１通信ユニットと、鍵要求ユニットと、を有する。上記鍵要求ユニットは、上記サーバに新たな通信用秘密鍵の発行を要求するときに、数値よりなる第１秘密値を新たに生成するように構成される。上記鍵要求ユニットは、さらに、上記第１原始元記憶ユニットに記憶された上記原始元に上記第１秘密値を適用することによりディフィー・ヘルマン鍵共有方式の第１公開鍵

を生成して上記サーバに送信するように構成される。上記サーバは、上記通信用秘密鍵を記憶する第２鍵記憶ユニットと、上記所定の原始元を記憶する第２原始元記憶ユニットと、を有する。上記サーバは、上記第２記憶ユニットに記憶された上記通信用秘密鍵を共通鍵として用いた暗号化通信を上記端末と行うための第２通信ユニットと、鍵発行ユニットと、を有する。上記鍵発行ユニットは、上記端末から新たな通信用秘密鍵の発行が要求されると、数値よりなる第２秘密値を生成し、上記端末から受信した第１公開鍵と上記第２秘密値とを用いて上記ディフィー・ヘルマン鍵共有方式の共通鍵を生成するように構成される。上記鍵発行ユニットは、さらに、上記第２原始元記憶ユニットに記憶された上記原始元に上記第２秘密値を適用することにより上記ディフィー・ヘルマン鍵共有方式の第２公開鍵を生成するように構成される。上記鍵発行ユニットは、さらに、上記共通鍵を用いて上記新たな通信用秘密鍵を暗号化して上記第２公開鍵とともに新たな通信用秘密鍵の発行を要求した上記端末に送信するように構成される。上記鍵要求ユニットは、上記サーバから暗号化された上記新たな通信用秘密鍵と上記第２公開鍵とを受信すると、上記新たに生成された秘密値と上記サーバから受信した上記第２公開鍵とを用いて上記共通鍵を生成するように構成される。上記鍵要求ユニットは、さらに、暗号化された上記新たな通信用秘密鍵を生成された上記共通鍵を用いて復号化して上記新たな通信用秘密鍵を取得して、上記第１鍵記憶ユニットに記憶させるように構成される。上記第１通信ユニットは、上記第１記憶ユニットに上記新たな通信用秘密鍵が記憶された後は、上記新たな通信用秘密鍵を共通鍵として用いた暗号化通信を上記サーバと行うように構成される。上記第２通信ユニットは、上記第２記憶ユニットに上記新たな通信用秘密鍵が記憶された後は、上記新たな通信用秘密鍵を共通鍵として用いた暗号化通信を上記端末と行うように構成される。

[0016] この鍵配布システムによれば、ディフィー・ヘルマン鍵共有方式の共通鍵を利用して、新たな通信用秘密鍵を暗号化して端末に送信する。そのため、元の通信用秘密鍵を知っている第三者であっても暗号化された新たな通信用

秘密鍵を復号化できない。よって、新たな通信用秘密鍵を端末に安全に届けることができる。

図面の簡単な説明

[0017] [図1]実施形態１の鍵配布システムのブロック図である。

[図2]同上の動作説明図である。

[図3]同上の動作を示すフローチャートである。

[図4]実施形態２の鍵配布システムのブロック図である。

[図5]同上の動作説明図である。

[図6]同上の変形例の鍵配布システムの動作説明図である。

[図7]実施形態３の鍵配布システムのブロック図である。

[図8]同上の動作説明図である。

[図9]実施形態４の鍵配布システムのブロック図である。

[図10]同上の動作説明図である。

発明を実施するための最良の形態

[0018] （実施形態１）

図１に示すように、本実施形態の鍵配布システムは、複数の端末１０と、各端末１０に通信ネットワーク３０を介して接続されるサーバ２０とを備える。通信ネットワーク３０は、広域網と構内網とのいずれであってもよい。端末１０およびサーバ２０は、通信ネットワーク３０に接続するための通信インターフェイスと、所定のデータを記憶するためのメモリと、所定の機能を実現するためのマイクロコンピュータとを利用して構成されている。

[0019] 端末１０は、通信ネットワーク３０を介してサーバ２０に接続される。端末１０は、第１鍵記憶ユニット１１と、第１通信ユニット１２と、鍵要求ユニット１３と、第１識別情報記憶ユニット１４と、セッション鍵要求ユニット１５と、セッション鍵受取ユニット１６と、を有する。

[0020] 第１鍵記憶ユニット１１は、書換可能な記録媒体である。第１鍵記憶ユニット１１は、通信用秘密鍵と、セッション鍵とを記憶するように構成される。なお、本実施形態では、通信用秘密鍵が公開鍵としても用いられる。よっ

て、第１鍵記憶ユニット１１は、通信用秘密鍵と公開鍵とを記憶しているといえる。

[0021] 第１識別情報記憶ユニット１４は、たとえば、書換可能な記録媒体である。第１識別情報記憶ユニット１４は、鍵配布システムにおいて端末１０とサーバ２０とを特定するための識別情報（識別子）を記憶する。なお、上記の識別情報は、鍵配布システムにおいて固有の（ユニークな）情報である。識別情報は、たとえば、ＭＡＣアドレスや、ＩＰｖ６におけるＩＰアドレス、構内網において設定されたアドレスである。

[0022] 第１通信ユニット１２は、サーバ２０と暗号化通信をするために設けられる。第１通信ユニット１２は、第１記憶ユニット１１に記憶された通信用秘密鍵を共通鍵として用いた暗号化通信をサーバ２０と行うように構成される。また、第１通信ユニット１２は、第１記憶ユニット１１に記憶されたセッション鍵を共通鍵として用いた暗号化通信をサーバ２０と行うように構成される。第１通信ユニット１２は、送信元の識別情報（端末１０の識別情報）と送信先の識別情報（サーバ２０の識別情報）と所定の電文とを含むパケットを送信する。このパケットの電文は通信用秘密鍵またはセッション鍵を用いて暗号化される。

[0023] 鍵要求ユニット１３は、サーバ２０に対して通信用秘密鍵の発行を要求する処理（発行要求処理）と、通信用秘密鍵の受取の処理を行うように構成される。

[0024] 鍵要求ユニット１３は、たとえば、端末１０の利用者が変わったときに通信用秘密鍵を変更するために設けられている。発行要求処理は、利用者が特定の操作、たとえば発行要求処理を開始するためのスイッチの操作によって開始される。端末１０は、通信ネットワーク３０に接続されたときに（通信ネットワーク３０に参加したことを通知するためのパケットを送信するときに）、自動的に発行要求処理を実行するように構成されていてもよい。端末１０が通信ネットワーク３０に接続された後は、定期的あるいは不定期的に発行要求処理が実行されるようにしてもよい。この場合、発行要求処理を実

行する第１時間間隔は、セッション鍵の発行を要求する処理を実行する第２時間間隔に比べて十分に長く設定することが好ましい。たとえば、第２時間間隔を１日程度とする場合には、第１時間間隔は１ヶ月以上とすることが好ましい。

[0025] セッション鍵要求ユニット１５は、サーバ２０に対してセッション鍵の発行を要求する処理を行うように構成される。

[0026] セッション鍵受取ユニット１６は、サーバ２０からのセッション鍵の受取の処理を行うように構成される。

[0027] サーバ２０は、第２鍵記憶ユニット２１と、第２通信ユニット２２と、鍵発行ユニット２３と、第２識別情報記憶ユニット２４と、セッション鍵発行ユニット２５と、を有する。

[0028] 第２鍵記憶ユニット２１は、書換可能な記録媒体である。第２鍵記憶ユニット２１は、通信用秘密鍵と、セッション鍵とを記憶するように構成される。第２記憶ユニット２１は、さらに、通信用秘密鍵とペアになる私有鍵である復号用秘密鍵を記憶するように構成される。

[0029] このように通信用秘密鍵と復号用秘密鍵とはペアとなる暗号鍵である。つまり、通信用秘密鍵と復号用秘密鍵との間の関係は、公開鍵暗号における公開鍵と秘密鍵（私有鍵）との間の関係と同等である。つまり、復号用秘密鍵は、通信用秘密鍵を公開鍵として暗号化された電文を復号化するための私有鍵である。よって、通信用秘密鍵（公開鍵暗号における公開鍵に相当）を用いて暗号化された電文（暗号文）を復号化するためには、通信用秘密鍵ではなく復号用秘密鍵（公開暗号鍵における私有鍵に相当）が必要である。また、復号用秘密鍵を用いて暗号化された電文（暗号文）を復号化するためには、通信用秘密鍵が必要である。

[0030] したがって、本実施形態の鍵配布システムでは、端末１０とサーバ２０とは、公開鍵暗号方式によって暗号化通信を行える。

[0031] 第２鍵記憶ユニット２１は、通信用秘密鍵と、復号用秘密鍵と、セッション鍵とからなる鍵束を、サーバ２０に接続された各端末１０と関連付けて記

憶するように構成される。つまり、端末１０の識別情報が、通信用秘密鍵と復号用秘密鍵とセッション鍵とのそれぞれと対応付けられている。

[0032] 第２識別情報記憶ユニット２４は、たとえば、書換可能な記録媒体である。第２識別情報記憶ユニット２４は、上記識別情報を記憶する。

[0033] 第２通信ユニット２２は、端末１０と暗号化通信をするために設けられる。第２通信ユニット２２は、第２記憶ユニット２１に記憶された通信用秘密鍵を共通鍵として用いた暗号化通信を端末１０と行うように構成される。また、第２通信ユニット２２は、第２記憶ユニット２１に記憶されたセッション鍵を共通鍵として用いた暗号化通信を端末１０と行うように構成される。第２通信ユニット２２は、送信元の識別情報（サーバ２０の識別情報）と送信先の識別情報（端末１０の識別情報）と所定の電文とを含むパケットを送信する。このパケットの電文は通信用秘密鍵またはセッション鍵を用いて暗号化される。

[0034] 鍵発行ユニット２３は、端末１０から通信用秘密鍵の発行が要求されたときに、通信用秘密鍵の発行の処理を行うように構成される。

[0035] セッション鍵発行ユニット２５は、端末１０からセッション鍵の発行が要求されたときに、セッション鍵の発行の処理を行うように構成される。つまり、サーバ２０は、端末１０からの要求に応答してセッション鍵を発行する。

[0036] 本実施形態では、サーバ２０は、サーバ２０と端末１０との間で送受信される電文の暗号化に用いられるセッション鍵を端末１０に配布するように構成されている。

[0037] 端末１０は、たとえば住宅内に設けた通信機能を有する設備機器である。サーバ２０は、たとえば認証サーバであり、住宅内の各設備機器（端末１０）と通信可能な住宅用サーバを利用して構成される。サーバ２０を利用して宅内の各設備機器（端末１０）の制御や監視が行える。

[0038] セッション鍵要求ユニット１５は、サーバ２０にセッション鍵の配布を要求する際には、ノンス（第１ノンス）を生成する。第１ノンスは、１回だけ

使用される数値である。第１ノンスは、通常は乱数である。セッション鍵要求ユニット１５は、第１ノンスとセッション鍵要求メッセージ（セッション鍵要求コマンド）と端末１０の識別情報とを含む電文を第１通信ユニット１２がサーバ２０に送信するように第１通信ユニット１２を制御する。セッション鍵要求メッセージは、セッション鍵の発行を要求するためのコマンドである。

[0039] なお、第１通信ユニット１２は、送信元アドレス（送信元の識別情報）と送信先アドレス（送信先の識別情報）とを含むパケットを送信するから、サーバ２０は、送信元アドレスによって端末１０の識別情報を取得できる。よって、上記の電文では端末１０の識別情報を省略できる。

[0040] セッション鍵発行ユニット２５は、端末１０からセッション鍵要求メッセージを受け取ると、セッション鍵を生成し、第２鍵記憶ユニット２１に記憶させる。また、セッション鍵発行ユニット２５は、第２鍵記憶ユニット２１に記憶された通信用秘密鍵を用いてセッション鍵を暗号化する。セッション鍵発行ユニット２５は、セッション鍵を暗号化するために、通信用秘密鍵を用いて第２メッセージ認証コード（第２メッセージコード）を生成する。セッション鍵発行ユニット２５は、第２メッセージ認証コードとセッション鍵との排他論理和を暗号化されたセッション鍵として用いる。すなわち、セッション鍵発行ユニット２５は、第２メッセージ認証コードを共通鍵として用いてセッション鍵を暗号化する。第２メッセージ認証コードを生成するための情報は、端末１０から受信した端末１０の識別情報および第１ノンスと、セッション鍵発行ユニット２５が生成したノンス（第２ノンス）と、サーバ２０の識別情報とを含む。セッション鍵発行ユニット２５は、暗号化されたセッション鍵と第２ノンスとを第２通信ユニット２２が端末１０に送信するように第２通信ユニット２２を制御する。

[0041] セッション鍵受取ユニット１６は、サーバ２０から暗号化されたセッション鍵と、第２ノンスとを受け取ると、暗号化されたセッション鍵を復号化する。セッション鍵受取ユニット１６は、暗号化されたセッション鍵を復号化

するために、第２メッセージ認証コードと値が等しい第１メッセージ認証コード（第１メッセージコード）を生成する。端末１０は、端末１０の識別情報と第１ノンスとサーバ２０の識別情報と通信用秘密鍵とを有しているから、サーバ２０から第２ノンスを受信することで、第１メッセージ認証コードを生成できる。

[0042] 暗号化されたセッション鍵は、第２メッセージ認証コードとセッション鍵との排他的論理和である。よって、暗号化されたセッション鍵と第１メッセージ認証コードとの排他的論理和を求めることにより、セッション鍵を取得できる。

[0043] セッション鍵受取ユニット１６は、取得したセッション鍵を第１鍵記憶ユニット１１に記憶させる。このとき、セッション鍵受取ユニット１６は、第１鍵記憶ユニット１１に記憶されたセッション鍵を新たに取得したセッション鍵に更新するように構成されていてもよい。

[0044] 鍵要求ユニット１３は、秘密値生成モジュール１３０と、秘密値記憶モジュール１３１と、秘密値暗号化モジュール１３２と、秘密値送信モジュール１３３と、を有する。

[0045] 秘密値生成モジュール１３０は、新たな通信用秘密鍵の発行を要求する際に数値よりなる秘密値を生成するように構成される。秘密値は乱数である。つまり、秘密値生成モジュール１３０は、通信用秘密鍵の発行を要求する処理毎にランダムな数値を持つ秘密値を生成する。そのため、秘密値は、通信用秘密鍵の発行を要求する処理毎に異なる数値を持つ。同じ秘密値は新たな通信用秘密鍵を端末１０が受け取るまで用いられる。

[0046] 秘密値記憶モジュール１３１は、秘密値生成モジュール１３０で生成された秘密値を記憶するように構成される。なお、秘密値記憶モジュール１３１は、既に秘密値を記憶している場合には、記憶している秘密値を秘密値生成モジュール１３０で生成された秘密値に更新するように構成されていてもよい。

[0047] 秘密値暗号化モジュール１３２は、秘密値記憶モジュール１３１に記憶さ

れた秘密値を暗号化して第１の暗号を生成するように構成される。秘密値暗号化モジュール１３２は、第１鍵記憶ユニット１１に記憶された通信用秘密鍵を公開鍵として用いて秘密値を暗号化する。たとえば、秘密値暗号化モジュール１３２は、新たな通信用秘密鍵を要求する処理の開始時に第１鍵記憶ユニット１１に記憶されている通信用秘密鍵を用いて公開鍵方式（たとえば、ＲＳＡ）で秘密値を暗号化して第１の暗号を生成する。

[0048] 秘密値送信モジュール１３３は、新たな通信用秘密鍵の発行を要求する要求メッセージ（要求コマンド）とともに秘密値暗号化モジュール１３２で生成された第１暗号がサーバ２０に送信されるように第１通信ユニット１２を制御するように構成される。秘密値送信モジュール１３３は、第１の暗号と一緒に端末１０の識別情報も第１通信ユニット１２に送信させる。

[0049] 鍵発行ユニット２３は、鍵生成モジュール２３０と、通信用秘密鍵暗号化モジュール２３１と、通信用秘密鍵送信モジュール２３２と、第２保管モジュール２３３と、を有する。

[0050] 鍵生成モジュール２３０は、第２通信ユニット２２が端末１０から要求メッセージを受け取ると、新たな通信用秘密鍵を生成するように構成される。また、鍵生成モジュール２３０は、第２通信ユニット２２が要求メッセージを受け取ると、新たな通信用秘密鍵とペアとなる新たな復号用秘密鍵を生成するように構成される。

[0051] 通信用秘密鍵暗号化モジュール２３１は、秘密値取得部２３１１と、暗号化部２３１２と、を有する。

[0052] 秘密値取得部２３１１は、第２通信ユニット２２が要求メッセージを受け取ると、第２通信ユニット２２が受け取った第１の暗号を復号化して秘密値を取得するように構成される。秘密値取得部２３１１は、通信用秘密鍵とペアとなる復号用秘密鍵を用いて第１の暗号を復号化する。なお、秘密値取得部２３１１は、端末１０の通信用秘密鍵とペアになる復号用秘密鍵を抽出する際に、端末１０の識別情報を検索キーに用いる。

[0053] 暗号化部２３１２は、秘密値取得部２３１１より得た秘密値を共通鍵とし

て用いて新たな通信用秘密鍵を暗号化して第２の暗号を生成するように構成される。暗号化部２３１２は、たとえば、新たな通信用秘密鍵と秘密値との排他的論理和を第２の暗号（暗号化された新たな通信用秘密鍵）として用いる。

[0054] 通信用秘密鍵送信モジュール２３２は、新たな通信用秘密鍵の発行を要求した端末１０に第２通信ユニット２２が第２の暗号を送信するように第２通信ユニット２２を制御するように構成される。

[0055] 第２保管モジュール２３３は、鍵生成モジュール２３０で生成された新たな通信用秘密鍵と新たな復号用秘密鍵とを第２鍵記憶ユニット２１に記憶させるように構成される。なお、第２保管モジュール２３３は、第２鍵記憶ユニット２１に記憶された通信用秘密鍵を、鍵生成モジュール２３０で生成された新たな通信用秘密鍵に更新するように構成されていてもよい。また、第２保管モジュール２３３は、第２鍵記憶ユニット２１に記憶された復号用秘密鍵を、鍵生成モジュール２３０で生成された新たな復号用秘密鍵に更新するように構成されていてもよい。

[0056] このように鍵発行ユニット２３は、端末１０から新たな通信用秘密鍵の発行が要求されると、新たな通信用秘密鍵を発行して第２鍵記憶ユニット２１に記憶させる。鍵発行ユニット２３は、復号用秘密鍵を用いて第１の暗号を復号化することによって秘密値を取得する。鍵発行ユニット２３は、秘密値を利用して新たな通信用秘密鍵を暗号化して第２の暗号を生成する。鍵発行ユニット２３は、新たな通信用秘密鍵の発行を要求した端末１０に第２の暗号を送信する。

[0057] また、鍵発行ユニット２３は、端末１０から新たな通信用秘密鍵の発行が要求されると、新たな通信用秘密鍵を発行するとともに、新たな通信用秘密鍵とペアになる私有鍵である新たな復号用秘密鍵を発行して第２鍵記憶ユニット２１に記憶させる。鍵発行ユニット２３は、第２鍵記憶ユニット２１に新たな復号用秘密鍵が記憶された後は、新たな復号用秘密鍵を用いて第１の暗号を復号化する。

[0058] このようにして第２鍵記憶ユニット２１には新たな通信用秘密鍵が記憶されるから、第２通信ユニット２２は、通信用秘密鍵を共通鍵として用いた暗号化通信を端末１０と行う場合には、新たな通信用秘密鍵を使用する。

[0059] 鍵要求ユニット１３は、さらに、通信用秘密鍵復号化モジュール１３４と、第１保管モジュール１３５と、を有する。

[0060] 通信用秘密鍵復号化モジュール１３４は、上記第１通信ユニット１２が第２の暗号を受け取ると、秘密値記憶モジュール１３１に記憶された秘密値を用いて第１通信ユニット１２が受け取った第２の暗号を復号化し、これによって新たな通信用秘密鍵を得るように構成される。第２の暗号は秘密値と新たな通信用秘密鍵との排他的論理和である。第２の暗号と秘密値との排他的論理和を求めることにより新たな通信用秘密鍵が得られる。なお、通信用秘密鍵復号化モジュール１３４は、新たな通信用秘密鍵を得た後に、秘密値記憶モジュール１３１に記憶された秘密値を消去するように構成されていてもよい。

[0061] 第１保管モジュール１３５は、通信用秘密鍵復号化モジュール１３４によって得られた新たな通信用秘密鍵を第１鍵記憶ユニット１１に記憶させるように構成される。なお、第１保管モジュール１３５は、第１鍵記憶ユニット１１に記憶された通信用秘密鍵を、新たな通信用秘密鍵に更新するように構成されていてもよい。

[0062] このように鍵要求ユニット１３は、サーバ２０に新たな通信用秘密鍵の発行を要求するときに、数値よりなる秘密値を新たに生成する。鍵要求ユニット１３は、第１鍵記憶ユニット１１に記憶された通信用秘密鍵を公開鍵として用いて秘密値を暗号化して第１の暗号を生成してサーバ２０に送信する。鍵要求ユニットは、秘密値を利用して第２の暗号を復号化することによって新たな通信用秘密鍵を取得して、第１鍵記憶ユニット１１に記憶させる。

[0063] このようにして第１鍵記憶ユニット１１には新たな通信用秘密鍵が記憶されるから、第１通信ユニット１２は、通信用秘密鍵を共通鍵として用いた暗号化通信をサーバ２０と行う場合には、新たな通信用秘密鍵を使用する。

[0064] 次に、図２及び図３を参照して本実施形態の鍵配布システムの動作について説明する。

[0065] なお、端末１０の出荷時には、端末１０に通信用秘密鍵を登録する作業と、管理装置２０に通信用秘密鍵と復号用秘密鍵とを登録する作業とが行われる。通信用秘密鍵と復号用秘密鍵との登録には、管理装置（製品管理装置）４０が用いられる。管理装置４０は、通信用秘密鍵と復号用秘密鍵との登録の際には、インターネットのような通信路を用いてサーバ２０および端末１０に接続される。

[0066] 図２に示すように、管理装置４０は、通信用秘密鍵Ｋ１０と復号用秘密鍵Ｋ２０とをサーバ２０に送信する（図２のプロセスＰ１０）。サーバ２０は、管理装置４０から受け取った通信用秘密鍵Ｋ１０と復号用秘密鍵Ｋ２０とを第２鍵記憶ユニット２１に登録する（図３のステップＳ１１）。管理装置４０は、通信用秘密鍵Ｋ１０と復号用秘密鍵Ｋ２０との漏洩を防止するために、ＳＳＬ（Secure Socket Layer）やＴＬＳ（Transport Layer Security）のような技術を用いてサーバ２０と通信する。

[0067] また、管理装置４０は、端末１０を識別するための識別情報（端末識別情報）ＩＤ１０をサーバ２０に送信する。サーバ２０は、管理装置４０から受け取った識別情報ＩＤ１０を第２識別情報記憶ユニット２４に登録する。なお、機器を通信ネットワークＮＴに接続するためのミドルウェアとしてのＥＭＩＴ（Embedded Micro Internetworking Technology）が端末１０に搭載されている場合，ＥＭＩＴのオブジェクトＩＤを端末識別情報ＩＤ１０に用いることができる。

[0068] 管理装置４０は、端末１０の識別情報ＩＤ１０と、サーバ２０に登録された通信用秘密鍵Ｋ１０とを端末１０に送信する（図２のプロセスＰ２０）。端末１０は、管理装置４０から受け取った識別情報ＩＤ１０を第１識別情報記憶ユニット１４に登録する。また、端末１０は、管理装置４０から受け取った通信用秘密鍵Ｋ１０を第１鍵記憶ユニット１１に登録する（図３のステップＳ１２）。

[0069] すなわち、サーバ２０の第２鍵記憶ユニット２１と端末１０の第１鍵ユニット１１とには、それぞれ事前秘密鍵として通信用秘密鍵Ｋ１０が登録される。また、サーバ２０の第２鍵記憶ユニット２１には、通信用秘密鍵Ｋ１０とペアになる事前秘密鍵として復号用秘密鍵Ｋ２０が登録される。

[0070] 本実施形態の鍵配布システムでは、以下の手順でサーバ２０が端末１０にセッション鍵を配布する。

[0071] 端末１０がサーバ２０にセッション鍵の発行を要求する際、セッション鍵要求ユニット１５は、第１ノンスＮ１０を生成する。セッション鍵要求ユニット１５は、第１通信ユニット１２を制御して、第１ノンスＮ１０とセッション鍵要求メッセージとを端末１０の識別情報ＩＤ１０とともにサーバ２０に送信する（図２のプロセスＰ３０）。

[0072] 第２通信ユニット２２がセッション鍵要求メッセージを受け取ると、セッション鍵発行ユニット２５は、セッション鍵Ｋ３０を生成する。セッション鍵発行ユニット２５は、第２鍵記憶ユニット２１に記憶された通信用秘密鍵Ｋ１０と情報Ｉ２０とを用いて、第２メッセージ認証コードMAC_{K10}（Ｉ２０）を生成する。情報Ｉ２０は、端末１０から受信した端末１０の識別情報ＩＤ１０および第１ノンスＮ１０と、第２ノンスＮ２０と、サーバ２０の識別情報（サーバ識別情報）ＩＤ２０とである。すなわち、Ｉ２０＝（ＩＤ１０，Ｎ１０，Ｎ２０，ＩＤ２０）である。

[0073] セッション鍵発行ユニット２５は、第２メッセージ認証コード（＝MAC_{K10}（ＩＤ１０，Ｎ１０，Ｎ２０，ＩＤ２０））とセッション鍵Ｋ３０との排他的論理和を演算して暗号化されたセッション鍵（＝［MAC_{K10}（ＩＤ１０，Ｎ１０，Ｎ２０，ＩＤ２０）　ＸＯＲ　Ｋ３０］）を生成する。セッション鍵発行ユニット２５は、第２通信ユニット２２を制御して、暗号化されたセッション鍵を第２ノンスＮ２０とともに端末１０に送信する（図２のプロセスＰ４０）。

[0074] なお、プロセスＰ３０において端末１０から識別情報ＩＤ１０を受け取っていなければ、情報Ｉ２０から識別情報ＩＤ１０を省略してもよい。

[0075] 以上の動作をまとめると、端末１０は、サーバ２０にセッション鍵の発行を要求する際に、第１ノンスＮ１０と識別情報ＩＤ１０とを送信する（図２のプロセスＰ３０）。サーバ２０は、端末１０の要求に応答して、暗号化されたセッション鍵（＝［MAC_{K10}（ＩＤ１０，Ｎ１０，Ｎ２０，ＩＤ２０）ＸＯＲ　Ｋ３０］）を第２ノンスＮ２０とともに送信する（図２のプロセスＰ４０）。

[0076] 暗号化されたセッション鍵と第２ノンスＮ２０とを第１通信ユニット１２が受け取ると、セッション鍵受取ユニット１６は、第１メッセージ認証コードを生成する。

[0077] セッション鍵受取ユニット１６は、第１メッセージ認証コード（＝MAC_{K10}（ＩＤ１０，Ｎ１０，Ｎ２０，ＩＤ２０）と暗号化されたセッション鍵（＝［MAC_{K10}（ＩＤ１０，Ｎ１０，Ｎ２０，ＩＤ２０）　ＸＯＲ　Ｋ３０］）との排他的論理和を演算することで、セッション鍵Ｋ３０を取得する。セッション鍵受取ユニット１６は、受け取ったセッション鍵Ｋ３０を第１鍵記憶ユニット１１に記憶させる。

[0078] このようにして端末１０は、サーバ２０からセッション鍵Ｋ３０を受け取る。端末１０は、サーバ２０から受け取ったセッション鍵Ｋ３０を、当該セッション鍵Ｋ３０の有効期間中、サーバ２０との間の通信に使用する。

[0079] 本実施形態の鍵配布システムでは、以下の手順でサーバ２０が端末１０に通信用秘密鍵を配布する。

[0080] 発行要求処理が開始されると、秘密値生成モジュール１３０は、乱数である秘密値Ｒ１０を生成する（図３のステップＳ１３）。秘密値Ｒ１０は秘密値記憶モジュール１３１に記憶される。秘密値暗号化モジュール１３２は、第１鍵記憶ユニット１１に記憶された通信用秘密鍵Ｋ１０を公開鍵として用いて秘密値Ｒ１０を暗号化して第１の暗号PEN_{K10}（Ｒ１０）を生成する（図３のステップＳ１４）。秘密値送信モジュール１３３は、第１通信ユニット１２を制御して、第１の暗号PEN_{K10}（Ｒ１０）を、端末１０の識別情報ＩＤ１０および要求メッセージとともにサーバ２０に送信する（図３のステップ

Ｓ１５、図２のプロセスＰ５０）。このように、端末１０、通信用秘密鍵の発行をサーバ２０に要求する際に、端末１０の識別情報ＩＤ１０と第１の暗号$ＰＥＮ_{K10}$（Ｒ１０）とを送信する。

[0081] 第１の暗号$ＰＥＮ_{K10}$（Ｒ１０）は、電文が価値を持っている時間内（次の通信用秘密鍵Ｋ１１が端末１０に配布されるまでの時間内）は、復号用秘密鍵Ｋ２０でなければ復号化できない。そのため、他者が通信用秘密鍵Ｋ１０を知っていても秘密値Ｒ１０を知ることができない。

[0082] 第２通信ユニット２２が要求メッセージを受け取ると（図３のステップＳ１６）、秘密値取得部２３１１は、第２鍵記憶ユニット２１に記憶された復号用秘密鍵Ｋ２０を用いて第１の暗号$ＰＥＮ_{K10}$（Ｒ１０）を復号化して、秘密値Ｒ１０を取得する（図３のステップＳ１７）。

[0083] また、鍵生成モジュール２３０は、新たな通信用秘密鍵Ｋ１１と、新たな通信用秘密鍵Ｋ１１とペアとなる新たな復号用秘密鍵Ｋ２１とを生成する（図３のステップＳ１８）。

[0084] 暗号化部２３１２は、秘密値取得部２３１１より得た秘密値Ｒ１０を共通鍵として用いて新たな通信用秘密鍵Ｋ１１を暗号化して第２の暗号を生成する（図３のステップＳ１９）。本実施形態では、暗号化部２３１２は、新たな通信用秘密鍵Ｋ１１と秘密値Ｒ１０との排他的論理和（＝［Ｒ１０　ＸＯＲ　Ｋ１１］）を第２の暗号として用いる。

[0085] 第２保管モジュール２３３は、鍵生成モジュール２３０で生成された新たな通信用秘密鍵Ｋ１１と新たな復号用秘密鍵Ｋ２１とを第２鍵記憶ユニット２１に記憶させる。

[0086] 通信用秘密鍵送信モジュール２３２は、第２通信ユニット２２を制御して、新たな通信用秘密鍵Ｋ１１の発行を要求した端末１０に第２の暗号を送信する（図３のステップＳ２０、図２のプロセスＰ６０）。このように、サーバ２０は、端末１０に第２の暗号（＝［Ｒ１０　ＸＯＲ　Ｋ１１］）を送信する。

[0087] 通信用秘密鍵復号化モジュール１３４は、上記第１通信ユニット１２が第

２の暗号を受け取ると（図３のステップＳ２１）、第２の暗号（＝［Ｒ１０　ＸＯＲ　Ｋ１１］）と秘密値Ｒ１０との排他的論理和を求めることにより新たな通信用秘密鍵Ｋ１１を得る（図３のステップＳ２２）。

[0088] 第１保管モジュール１３５は、通信用秘密鍵復号化モジュール１３４によって得られた新たな通信用秘密鍵Ｋ１１を第１鍵記憶ユニット１１に記憶させる。

[0089] そして、第１通信ユニット１２は、第１鍵記憶ユニット１１に新たな通信用秘密鍵Ｋ１１が記憶された後は、新たな通信用秘密鍵Ｋ１１を共通鍵として用いた暗号化通信をサーバ２０と行う。第２通信ユニット２２は、第２鍵記憶ユニット２１に新たな通信用秘密鍵Ｋ１１が記憶された後は、新たな通信用秘密鍵Ｋ１１を共通鍵として用いた暗号化通信を端末１０と行う。

[0090] そのため、新たな通信用秘密鍵Ｋ１１が発行された後は、他者が前の通信用秘密鍵Ｋ１０を知っていても、端末１０とサーバ２０との間の通信を盗聴できなくなる。

[0091] 端末１０がサーバ２０から新たな通信用秘密鍵Ｋ１１を取得した後は、以下の手順でサーバ２０が端末１０にセッション鍵を配布する。

[0092] 端末１０がサーバ２０にセッション鍵の発行を要求する際、セッション鍵要求ユニット１５は、第１ノンスＮ１０とは別の新たな第１ノンスＮ１１を生成する。セッション鍵要求ユニット１５は、第１通信ユニット１２を制御して、第１ノンスＮ１１とセッション鍵要求メッセージとを端末１０の識別情報ＩＤ１０とともにサーバ２０に送信する（図２のプロセスＰ７０）。

[0093] 第２通信ユニット２２がセッション鍵要求メッセージを受け取ると、セッション鍵発行ユニット２５は、セッション鍵Ｋ３０とは別の新たなセッション鍵Ｋ３１を生成し、第２鍵記憶ユニット２１に記憶させる。セッション鍵発行ユニット２５は、第２鍵記憶ユニット２１に記憶された通信用秘密鍵Ｋ１１と情報Ｉ２１とを用いて、第２メッセージ認証コードMAC_{K11}（Ｉ２１）を生成する。情報Ｉ２１は、端末１０から受信した端末１０の識別情報ＩＤ１０および第１ノンスＮ１１と、第２ノンスＮ２０とは別の新たな第２ノン

スＮ２１と、サーバ２０の識別情報（サーバ識別情報）ＩＤ２０とである。すなわち、Ｉ２１＝（ＩＤ１０，Ｎ１１，Ｎ２１，ＩＤ２０）である。

[0094] セッション鍵発行ユニット２５は、暗号化されたセッション鍵（＝［MAC_{K11}（ＩＤ１０，Ｎ１１，Ｎ２１，ＩＤ２０）　ＸＯＲ　Ｋ３１］）を生成して、第２ノンスＮ２１とともに端末１０に送信する（図２のプロセスＰ８０）。

[0095] 第２ノンスＮ２１と暗号化されたセッション鍵とを第１通信ユニット１２が受け取ると、セッション鍵受取ユニット１６は第１メッセージ認証コードを生成する。

[0096] セッション鍵受取ユニット１６は、第１メッセージ認証コード（＝MAC_{K11}（ＩＤ１０，Ｎ１１，Ｎ２１，ＩＤ２０）と暗号化されたセッション鍵（＝［MAC_{K11}（ＩＤ１０，Ｎ１１，Ｎ２１，ＩＤ２０）　ＸＯＲ　Ｋ３１］）との排他的論理和を演算することで、セッション鍵Ｋ３１を取得する。セッション鍵受取ユニット１６は、受け取ったセッション鍵Ｋ３１を第１鍵記憶ユニット１１に記憶させる。

[0097] このようにして端末１０は、サーバ２０から新たなセッション鍵Ｋ３１を受け取る。

[0098] 本実施形態の鍵配布システムでは、端末１０がサーバ２０に新たな通信用秘密鍵の発行を要求する際に、公開鍵を用いて秘密値を暗号化してサーバ２０に送信する。サーバ２０は、暗号化された秘密値を公開鍵とペアになる私有鍵を用いて復号化する。サーバ２０は、新たな通信用秘密鍵を、秘密値で復号化できるように暗号化して、端末１０に送信する。端末１０は、暗号化された通信用秘密鍵を、秘密値を利用して復号化して、新たな通信用秘密鍵を取得する。

[0099] 仮に端末１０の利用者が変わった場合に、前の利用者が通信用秘密鍵を知っていたとしても、公開鍵とペアとなる私有鍵までは知りえない。そのため、前の利用者は、秘密値を知ることはできない。よって、秘密値を安全に利用できる。また、秘密値は新たな通信用秘密鍵をサーバ２０に要求してから

取得するまでしか使用されない。そのため、秘密値が有効である時間内に、他人が秘密値を知る可能性はきわめて低い。よって、秘密値を用いて新たな通信用秘密鍵を暗号化することで、新たな通信用秘密鍵をサーバ２０から端末１０に安全に届けることができる。

[0100] このように、本実施形態の鍵配布システムによれば、新たな通信用秘密鍵をサーバ２０から端末１０に安全に届けることができる。

[0101] また、通信用秘密鍵を公開鍵として用いるから、サーバ２０だけが暗号化された秘密値を復号化できる。したがって、第三者は、通信用秘密鍵を用いても、暗号化された秘密鍵を復号化できない。よって、新たな通信用秘密鍵をサーバ２０から端末１０により安全に届けることができる。

[0102] なお、サーバ２０は、通信用秘密鍵と復号用秘密鍵とを用いることで、特定の端末１０しか利用できないセッション鍵を他人に知られることなく配布できる。サーバ２０が端末１０に新たなセッション鍵を配布する処理（セッション鍵の更新処理）は、端末１０の利用者が変わったときに行われる。

[0103] セッション鍵は、適宜のタイミングで定期的または不定期的に更新してもよい。つまり、同じ利用者が継続して端末１０を利用している間にセッション鍵の更新処理が行われるようにしてもよい。一般に、セッション鍵は使い捨ての暗号鍵である。そのため、たとえば、端末１０は、同じセッション鍵を所定の有効期間（たとえば１日）だけ保持するように構成されていてもよい。この場合、当該有効期間においてセッション鍵の更新処理が実行されれば、端末１０は当該有効期間よりも短い期間でセッション鍵を廃棄する。

[0104] 端末１０がセッション鍵を共通鍵として用いてサーバ２０と通信可能である場合、この端末１０はサーバ２０の管理下にあるといえる。同じサーバ２０の管理下にある端末１０同士は、互いに異なるセッション鍵を有していても、同じグループに属するといえる。なお、複数の端末１０に同じセッション鍵を配布することは想定していない。

[0105] たとえば、サーバ２０が住宅用サーバであり、第１端末１０がスイッチであり、第２端末１０が照明器具であるとする。また、サーバ２０が、第１端

末１０と第２端末１０とにそれぞれ異なるセッション鍵を配布したとする。この場合、各端末１０に配布されたセッション鍵はサーバ２０により保存・管理されている。よって、第１端末１０と第２端末１０とを同じ住宅内に存在する住宅設備としてグループ化できる。鍵配布システムは、同じグループに属する端末１０を互いに通信可能となるようにバインディングできる。バインディングされた端末１０同士は、サーバ２０を通して通信可能である。たとえば、上記の例では、スイッチである第１端末１０の操作を照明器具である第２端末１０の動作に反映させることができる。

[0106] なお、新たな通信用秘密鍵Ｋ１１が第三者により読み取られる確率を低減するために、第２の暗号（＝［Ｒ１０　ＸＯＲ　Ｋ１１］）をさらに暗号化することが好ましい。たとえば、サーバ２０の暗号化部２３１２は、第２の暗号をさらに元の通信用秘密鍵Ｋ１０を共通鍵として用いた共通鍵方式（たとえば、ＤＥＳ、３－ＤＥＳ、ＡＥＳ）で暗号化してもよい。この場合、端末１０の通信用秘密鍵復号化モジュール１３４は、暗号化された第２の暗号を元の通信用秘密鍵Ｋ１０で復号化した後に、第２の暗号と秘密値Ｒ１０との排他的論理和を求めることにより新たな通信用秘密鍵Ｋ１１を取得するように構成される。このようにすれば、前の利用者は、通信用秘密鍵Ｋ１０を知っていたとしても、端末１０での復号化のアルゴリズムに何を用いるかを容易に知ることはできない。また、前の利用者は、秘密値Ｒ１０を知る必要もある。よって、新たな通信用秘密鍵Ｋ１０が第三者に知られる可能性を大幅に低減できる。

[0107] （実施形態２）

図４に示すように、本実施形態の鍵配布システムは、端末１０Ａとサーバ２０Ａとが実施形態１と異なる。本実施形態の鍵配布システムと実施形態１の鍵配布システムとで共通する構成には同一の符号を付して説明を省略する。

[0108] サーバ２０Ａは、鍵発行ユニット２３Ａの通信用秘密鍵暗号化モジュール２３１Ａが実施形態１のサーバ２０と異なる。

[0109] 通信用秘密鍵暗号化モジュール２３１Ａは、秘密値取得部２３１１と、暗号化部２３１２Ａと、暗号化鍵生成部２３１３と、を有する。

[0110] 暗号化鍵生成部２３１３は、第２鍵記憶ユニット２１に記憶された通信用秘密鍵（新たな通信用秘密鍵ではなく端末１０Ａが所有している通信用秘密鍵）を共通鍵として用いることで、秘密値を含むメッセージ認証コード（メッセージコード）よりなる暗号化鍵を生成するように構成される。

[0111] 暗号化部２３１２Ａは、暗号化鍵生成部２３１３より得た暗号化鍵を共通鍵として用いて新たな通信用秘密鍵を暗号化して第２の暗号を生成するように構成される。暗号化部２３１２Ａは、たとえば、暗号化鍵生成部２３１３より得た暗号化鍵と新たな通信用秘密鍵との排他的論理和を第２の暗号（暗号化された新たな通信用秘密鍵）として用いる。

[0112] このように本実施形態の鍵発行ユニット２３Ａは、端末１０Ａから新たな通信用秘密鍵の発行が要求されると、端末１０Ａから受信した秘密値を含むメッセージ認証コードを生成する。そして、鍵発行ユニット２３Ａは、メッセージ認証コードを用いて新たな通信用秘密鍵を暗号化して端末１０Ａに送信する。

[0113] 端末１０Ａは、鍵要求ユニット１３Ａの通信用秘密鍵復号化モジュール１３４Ａで実施形態１の端末１０と異なる。

[0114] 通信用秘密鍵復号化モジュール１３４は、復号化鍵生成部１３４１と、復号部１３４２と、を有する。

[0115] 復号化鍵生成部１３４１は、第１通信ユニット１２が第２の暗号を受け取ると、第１鍵記憶ユニット１１に記憶された通信用秘密鍵と秘密値記憶モジュール１３１に記憶された秘密値とを用いて復号化鍵を生成する。復号化鍵は、暗号化鍵生成部２３１３で生成された暗号化鍵と同じ値を持つメッセージ認証コードである。つまり、復号化鍵生成部１３４１は、第１鍵記憶ユニット１１に記憶された通信用秘密鍵を共通鍵として用いることで、秘密値記憶モジュール１３１に記憶された秘密値を含むメッセージ認証コードを生成する。

[0116] 復号部１３４２は、復号化鍵生成部１３４１より得た復号化鍵を共通鍵として用いて第２の暗号を復号化し、これによって新たな通信用秘密鍵を取得するように構成される。復号化部１３４２は、たとえば、復号化鍵生成部１３４１より得た復号化鍵と第２の暗号との排他的論理和を演算することで、新たな通信用秘密鍵を取得する。

[0117] 次に図５を参照して本実施形態の鍵配布システムの動作について説明する。なお、プロセスＰ１０、Ｐ２０、Ｐ３０，Ｐ４０，Ｐ５０，Ｐ７０，Ｐ８０については実施形態１で述べたから説明を省略する。

[0118] 発行要求処理が開始されると、端末１０Ａは、端末１０Ａの識別情報ＩＤ１０と、第１の暗号$ＰＥＮ_{K10}$（Ｒ１０）とをサーバ２０Ａに送信する（プロセスＰ５０）。

[0119] 第２通信ユニット２２が要求メッセージを受け取ると、秘密値取得部２３１１は第２鍵記憶ユニット２１に記憶された復号用秘密鍵Ｋ２０を用いて第１の暗号$ＰＥＮ_{K10}$（Ｒ１０）を復号化して、秘密値Ｒ１０を取得する。

[0120] また、鍵生成モジュール２３０は、新たな通信用秘密鍵Ｋ１１と、新たな通信用秘密鍵Ｋ１１とペアとなる新たな復号用秘密鍵Ｋ２１とを生成する。

[0121] 暗号化鍵生成部２３１３は、第２鍵記憶ユニット２１に記憶された元の通信用秘密鍵Ｋ１０を共通鍵として用いることで、秘密値Ｒ１０を含むメッセージ認証コードよりなる暗号化鍵を生成する。具体的には、暗号化鍵生成部２３１３は、通信用秘密鍵Ｋ１０と情報Ｉ３０とを用いて、暗号化鍵（＝$ＭＡＣ_{K10}$（Ｉ３０））を生成する。情報Ｉ３０は、端末１０Ａから受信した秘密値Ｒ１０と、ノンス（第３ノンス）Ｎ３０と、サーバ２０Ａの識別情報ＩＤ２０とである。すなわち、Ｉ３０＝（Ｒ１０，Ｎ３０，ＩＤ２０）である。このように暗号化鍵生成部２３１３は、暗号化鍵を生成するために、第３ノンスＮ３０を生成する。第３ノンスＮ３０の値は、セッション鍵の発行時に生成された第２ノンスＮ２０とは異なる。なお、第３ノンスＮ３０の代わりに第２ノンスＮ２０を用いても良い。しかしながら、第２ノンス２０とは別の第３ノンスＮ３０を用いたほうが通信の安全性が高い。

[0122] 暗号化部２３１２Ａは、暗号化鍵生成部２３１３より得た暗号化鍵（＝ＭＡＣ$_{K10}$（Ｒ１０，Ｎ３０，ＩＤ２０））を共通鍵として用いて新たな通信用秘密鍵Ｋ１１を暗号化して第２の暗号を生成する。本実施形態では、暗号化部２３１２Ａは、新たな通信用秘密鍵Ｋ１１と暗号化鍵（＝ＭＡＣ$_{K10}$（Ｒ１０，Ｎ３０，ＩＤ２０））との排他的論理和（＝［ＭＡＣ$_{K10}$（Ｒ１０，Ｎ３０，ＩＤ２０）　ＸＯＲ　Ｋ１１］）を第２の暗号として用いる。

[0123] 第２保管モジュール２３３は、鍵生成モジュール２３０で生成された新たな通信用秘密鍵Ｋ１１と新たな復号用秘密鍵Ｋ２１とを第２鍵記憶ユニット２１に記憶させる。

[0124] 通信用秘密鍵送信モジュール２３２は、第２通信ユニット２２を制御して、新たな通信用秘密鍵Ｋ１１の発行を要求した端末１０Ａに、第２の暗号を第３ノンスＮ３０とともに送信する（図５のプロセスＰ６０Ａ）。このように、サーバ２０Ａは、端末１０Ａに第２の暗号（＝［ＭＡＣ$_{K10}$（Ｒ１０，Ｎ３０，ＩＤ２０）　ＸＯＲ　Ｋ１１］）と、第３ノンスＮ３０とを送信する。

[0125] なお、暗号化鍵の情報Ｉ３０には、端末１０Ａの識別情報ＩＤ１０を含めるようにしてもよい。すなわち、暗号化鍵の値は、ＭＡＣ$_{K10}$（ＩＤ１０，Ｒ１０，Ｎ３０，ＩＤ２０）であってもよい。

[0126] 通信用秘密鍵復号化モジュール１３４Ａでは、第１通信ユニット１２が第２の暗号と第３ノンスＮ３０とを受け取ると、秘密値記憶モジュール１３１に記憶された秘密値Ｒ１０、サーバ２０Ａの識別情報ＩＤ２０と、サーバ２０Ａから受信した第３ノンスＮ３０と元の通信用秘密鍵Ｋ１０とを用いて暗号化鍵に相当する値（＝ＭＡＣ$_{K10}$（Ｒ１０，Ｎ３０，ＩＤ２０））を算出し、復号化鍵を生成する。

[0127] 復号化部１３４２は、復号化鍵生成部１３４１より得た復号化鍵（＝ＭＡＣ$_{K10}$（Ｒ１０，Ｎ３０，ＩＤ２０））と第２の暗号（＝［ＭＡＣ$_{K10}$（Ｒ１０，Ｎ３０，ＩＤ２０）　ＸＯＲ　Ｋ１１］）との排他的論理和を演算することで、新たな通信用秘密鍵Ｋ１１を取得する。なお、情報Ｉ３０が端末１０Ａの識別情報ＩＤ１０を含む場合には、復号化鍵の生成にも識別情報ＩＤ１０

を用いる。

[0128] 第１保管モジュール１３５は、通信用秘密鍵復号化モジュール１３４Ａによって得られた新たな通信用秘密鍵Ｋ１１を第１鍵記憶ユニット１１に記憶させる。

[0129] 上述のようにメッセージ認証コードを暗号化鍵として用いれば、新たな通信用秘密鍵Ｋ１１が漏洩する可能性をさらに低減できる。また、メッセージ認証を行うことによって、サーバ２０Ａと端末１０Ａとは、第三者による通信用秘密鍵の改竄を検出できる。よって、通信用秘密鍵を用いた暗号化通信の安全性を保証できる。

[0130] なお、端末１０Ａがサーバ２０Ａに接続されると、サーバ２０Ａが端末１０Ａにチャレンジコードを送信するようにしてもよい。この場合、端末１０Ａは、サーバ２０Ａからチャレンジコードを受け取らなければ、発行要求処理を開始できないように構成される。このようにすれば、サーバ２０Ａへのトラフィックを増大させてサービスの提供を不能にするＤｏＳ（Denial of Service attack）という攻撃を防止できる。

[0131] なお、サーバ２０Ａは、新たな通信用秘密鍵とともにセッション鍵を端末１０Ａに送信するように構成されていてもよい。

[0132] この場合、セッション鍵発行ユニット２５は、端末１０から新たな通信用秘密鍵の発行が要求されたときに、セッション鍵の発行の処理を行うように構成される。

[0133] セッション鍵発行ユニット２５は、端末１０から要求メッセージを受け取ると、セッション鍵を生成する。また、セッション鍵発行ユニット２５は、第２鍵記憶ユニット２１に記憶された通信用秘密鍵を用いてセッション鍵を暗号化する。セッション鍵発行ユニット２５は、セッション鍵を暗号化するために、通信用秘密鍵を用いて第２メッセージ認証コード（第２メッセージコード）を生成する。セッション鍵発行ユニット２５は、第２メッセージ認証コードとセッション鍵との排他論理和を暗号化されたセッション鍵として用いる。第２メッセージ認証コードを生成するための情報は、端末１０から

受信した端末１０の識別情報および秘密値と、第２ノンスと、サーバ２０の識別情報とを含む。セッション鍵発行ユニット２５は、暗号化されたセッション鍵を通信用秘密鍵送信ユニット２３２に与える。また、セッション鍵発行ユニット２５は、第２ノンスを通信用秘密鍵暗号化モジュール２３１Ａの暗号化鍵生成部２３１３に与える。

[0134] 次に図６を参照して本実施形態の変形例の鍵配布システムの動作について説明する。なお、プロセスＰ１０、Ｐ２０、Ｐ３０，Ｐ４０，Ｐ５０については実施形態１で述べたから説明を省略する。

[0135] 発行要求処理が開始されると、端末１０Ａは、端末１０Ａの識別情報ＩＤ１０と、第１の暗号$ＰＥＮ_{K10}$（Ｒ１０）とをサーバ２０Ａに送信する（プロセスＰ５０）。

[0136] 第２通信ユニット２２が要求メッセージを受け取ると、セッション鍵発行ユニット２５はセッション鍵Ｋ３０とは別の新たなセッション鍵Ｋ３１を生成する。セッション鍵発行ユニット２５は、第２鍵記憶ユニット２１に記憶された通信用秘密鍵Ｋ１１と情報Ｉ２２とを用いて、第２メッセージ認証コードと$ＭＡＣ_{K11}$（Ｉ２２）を生成する。情報Ｉ２２は、端末１０から受信した端末１０Ａの識別情報ＩＤ１０および秘密値Ｒ１０と、第２ノンスＮ２１と、サーバ２０の識別情報ＩＤ２０とである。すなわち、Ｉ２２＝（ＩＤ１０，Ｒ１０，Ｎ２１，ＩＤ２０）である。

[0137] セッション鍵発行ユニット２５は、暗号化されたセッション鍵（＝［$ＭＡＣ_{K11}$（ＩＤ１０，Ｒ１０，Ｎ２１，ＩＤ２０）　ＸＯＲ　Ｋ３１］）を通信用秘密鍵送信ユニット２３２に与える。また、セッション鍵発行ユニット２５は、第２ノンスＮ２１を暗号化鍵生成部２３１３に与える。

[0138] 鍵発行ユニット２３Ａでは、秘密値取得部２３１１が第１の暗号$ＰＥＮ_{K10}$（Ｒ１０）を復号化して、秘密値Ｒ１０を取得する。

[0139] 暗号化鍵生成部２３１３は、通信用秘密鍵Ｋ１０と情報Ｉ３１とを用いて、暗号化鍵（＝$ＭＡＣ_{K10}$（Ｉ３１））を生成する。情報Ｉ３１は、端末１０Ａから受信した秘密値Ｒ１０と、セッション鍵発行ユニット２５より得た第２

ノンスＮ２１と、サーバ２０Ａの識別情報ＩＤ２０とである。すなわち、Ｉ３１＝（Ｒ１０，Ｎ２１，ＩＤ２０）である。

[0140] 暗号化部２３１２Ａは、新たな通信用秘密鍵Ｋ１１と暗号化鍵（＝MAC_{K10}（Ｒ１０，Ｎ２１，ＩＤ２０））との排他的論理和（＝［MAC_{K10}（Ｒ１０，Ｎ２１，ＩＤ２０）　ＸＯＲ　Ｋ１１］）を第２の暗号として用いる。

[0141] 通信用秘密鍵送信モジュール２３２は、第２通信ユニット２２を制御して、新たな通信用秘密鍵Ｋ１１の発行を要求した端末１０Ａに、第２の暗号とともに暗号化されたセッション鍵と第２ノンスＮ２１とを送信する（図６のプロセスＰ６１）。このように、変形例では、サーバ２０Ａは、第２の暗号（＝［MAC_{K10}（Ｒ１０，Ｎ２１，ＩＤ２０）　ＸＯＲ　Ｋ１１］）と、暗号化されたセッション鍵（＝［MAC_{K11}（ＩＤ１０，Ｒ１０，Ｎ２１，ＩＤ２０）　ＸＯＲ　Ｋ３１］）と、第２ノンスＮ２１とを端末１０Ａに送信する。

[0142] 端末１０Ａは、サーバ２０Ａから第２の暗号（＝［MAC_{K10}（Ｒ１０，Ｎ２１，ＩＤ２０）　ＸＯＲ　Ｋ１１］）と、暗号化されたセッション鍵（＝［MAC_{K11}（ＩＤ１０，Ｒ１０，Ｎ２１，ＩＤ２０）　ＸＯＲ　Ｋ３１］）と、第２ノンスＮ２１とを受け取ると、上述した処理を行うことで、新たな通信用秘密鍵Ｋ１１と新たなセッション鍵Ｋ３１とを取得する。

[0143] 上述の変形例では、新たな通信用秘密鍵Ｋ１１と新たなセッション鍵Ｋ３１とを同時に端末１０Ａに配布できる。そのため、図５に示す例に比べればサーバ２０Ａと端末１０Ａとの間のトラフィックを低減できる。よって、サーバ２０Ａと端末１０Ａとの間の通信に要する電力を低減でき、省エネルギ化を達成できる。

[0144] なお、この変形例では、セッション鍵発行ユニット２５が生成した第２ノンスを鍵発行ユニット２３Ａで使用しているが、鍵発行ユニット２３Ａが生成した第３ノンスをセッション鍵発行ユニット２５で使用してもよい。

[0145] なお、本実施形態では、メッセージ認証の手続には、クリプトナイトを採用している。しかしながら、メッセージ認証の手続には、ケルベロスを採用してもよい。ケルベロスではノンスに代えて時間が用いられる。したがって

、ケルベロスでは、ノンス性ないし乱数性の管理が時間管理に置き換えられる。

[0146] （実施形態３）

図７に示すように、本実施形態の鍵配布システムは、端末１０Ｂとサーバ２０Ｂとが実施形態２と異なる。本実施形態の鍵配布システムと実施形態２の鍵配布システムとで共通する構成には同一の符号を付して説明を省略する。

[0147] 端末１０Ｂは、鍵要求ユニット１３Ｂで実施形態２の端末１０Ａと異なる。

[0148] 鍵要求ユニット１３Ｂは、秘密値生成モジュール１３０と、秘密値記憶モジュール１３１と、秘密値暗号化モジュール１３２Ｂと、秘密値送信モジュール１３３と、通信用秘密鍵復号化モジュール１３４Ａと、第１保管モジュール１３５と、乱数生成モジュール１３６と、乱数送信モジュール１３７と、を有する。

[0149] 乱数生成モジュール１３６は、秘密値として用いられる第１乱数とは別の第２乱数を生成するように構成される。乱数生成モジュール１３６は、第２乱数を秘密値暗号化モジュール１３２Ｂと乱数送信モジュール１３７とに与える。第２乱数は、秘密値よりも桁数が多い数値であることが好ましい。第２乱数の桁数を多くすればするほど、秘密値が漏洩する可能性を低くできる。

[0150] 乱数送信モジュール１３７は、乱数生成モジュール１３６より受け取った第２乱数がサーバ２０Ｂに送信されるように第１通信ユニット１２を制御するように構成される。ここで、第２乱数は発行要求処理の実行前にサーバ２０Ｂに送信されることが好ましい。たとえば、乱数送信モジュール１３７は、端末１０Ｂが通信ネットワーク３０に接続された際に、サーバ２０Ｂに第２乱数を送信するように構成される。

[0151] 秘密値暗号化モジュール１３２Ｂは、通信数値生成部１３２１と、通信数値暗号化部１３２２と、を有する。

[0152] 通信数値生成部１３２１は、秘密値記憶モジュール１３１に記憶された秘密値より桁数が通信数値を生成するように構成される。通信数値生成部１３２１は、乱数生成モジュール１３６より得た第２乱数と秘密値記憶モジュール１３１に記憶された秘密値との単純演算により通信数値を生成する。本実施形態では、通信数値生成部１３２１は、演算に用いる秘密値に桁数を大きくするための第２乱数を結合することで通信数値を生成する。ここで、秘密値をＲ１０、第２乱数をＲ２０としたとき、通信数値は「Ｒ１０‖Ｒ２０」で表される。ｘ‖ｙは、左側の数値ｘに右側の数値ｙを単純に連結することを意味する。このような単純演算をコンカチネーションと呼ぶ。たとえば、「１２３‖１２３」は、「１２３１２３」になる。よって、通信数値では、上位の数値が秘密値であり、下位の数値が第２乱数である。このように通信数値生成部１３２１は、秘密値と第２乱数とを単純に連結するコンカチネーションにより通信数値を生成する。たとえば、秘密値が三桁の数値「１２３」であり、第２乱数が三桁の数値「４５６」である場合、通信数値は「１２３‖４５６」で表され、その値は「１２３４５６」である。なお、通信数値生成部１３２１は、秘密値と第２乱数との和を通信数値として用いても良いし、秘密値と第２乱数との積を通信数値として用いても良い。要は、通信数値の乱雑性が秘密値の乱雑性よりも高くなればよい。

[0153] 通信数値暗号化部１３２２は、通信数値生成部１３２１で生成された通信数値を暗号化して第１の暗号を生成するように構成される。通信数値暗号化部１３２２は、第１鍵記憶ユニット１１に記憶された通信用秘密鍵を公開鍵として用いて通信数値を暗号化する。たとえば、通信数値暗号化部１３２２は、新たな通信用秘密鍵を要求する処理の開始時に第１鍵記憶ユニット１１に記憶されている通信用秘密鍵を用いて公開鍵方式（たとえば、ＲＳＡ）で通信数値を暗号化して第１の暗号を生成する。

[0154] このように本実施形態の鍵要求ユニット２３Ｂは、秘密値として使用する第１乱数と、第２乱数とを生成する。鍵要求ユニット２３Ｂは、サーバ２０Ｂに新たな通信用秘密鍵の発行を要求する前に第２乱数をサーバ２０Ｂに送

信する。鍵要求ユニット２３Ｂは、第１乱数と第２乱数との単純演算により通信数値を生成する。鍵要求ユニット２３Ｂは、第１鍵記憶ユニット１１に記憶された公開鍵（本実施形態では通信用秘密鍵）を用いて通信数値を暗号化してサーバ２０Ｂに送信する。

[0155] サーバ２０Ｂは、鍵発行ユニット２３Ｂで実施形態２のサーバ２０Ａと異なる。

[0156] 鍵発行ユニット２３Ｂは、鍵生成モジュール２３０と、通信用秘密鍵暗号化モジュール２３１Ｂと、通信用秘密鍵送信モジュール２３２と、第２保管モジュール２３３と、乱数記憶モジュール２３４と、を有する。

[0157] 乱数記憶モジュール２３４は、たとえば、第２通信ユニット２２が端末１０Ｂから受け取った第２乱数を記憶するように構成される。

[0158] 通信用秘密鍵暗号化モジュール２３１Ｂは、秘密値取得部２３１１Ｂと、暗号化部２３１２Ａと、暗号化鍵生成部２３１３と、を有する。

[0159] 秘密値取得部２３１１Ｂは、第２通信ユニット２２が要求メッセージを受け取ると、第２通信ユニット２２が受け取った第１の暗号を復号化して通信数値を得るように構成される。秘密値取得部２３１１Ｂは、通信用秘密鍵とペアとなる復号用秘密鍵を用いて第１の暗号を復号化する。また、秘密値取得部２３１１Ｂは、取得した通信数値と乱数記憶モジュール２３４に記憶された第２乱数との単純演算により秘密値を取得するように構成される。

[0160] 次に図８を参照して本実施形態の鍵配布システムの動作について説明する。なお、プロセスＰ１０、Ｐ２０、Ｐ３０，Ｐ４０，Ｐ７０，Ｐ８０については実施形態１で述べたから説明を省略する。また、プロセスＰ５０Ｂとプロセスプロセス５０とで重複する説明を省略し、プロセスＰ６０Ｂとプロセスプロセス６０Ａとで重複する説明も省略する。

[0161] 発行要求処理が開始されると、通信数値生成部１３２１は、乱数生成モジュール１３６より得た第２乱数Ｒ２０と秘密値記憶モジュール１３１に記憶された秘密値Ｒ１０との単純演算により通信数値Ｒ１０‖Ｒ２０を生成する。

[0162] 通信数値暗号化部１３２２は、第１鍵記憶ユニット１１に記憶された通信用秘密鍵Ｋ１０を公開鍵として用いて通信数値Ｒ１０‖Ｒ２０を暗号化して第１の暗号$ＰＥＮ_{K10}$（Ｒ１０‖Ｒ２０）を生成する。

[0163] 秘密値送信モジュール１３３は、第１通信ユニット１２を制御して、第１の暗号$ＰＥＮ_{K10}$（Ｒ１０‖Ｒ２０）を、端末１０Ｂの識別情報ＩＤ１０および要求メッセージとともにサーバ２０Ｂに送信する（図８のプロセスＰ５０Ｂ）。

[0164] このように、端末１０Ｂは、通信用秘密鍵の発行をサーバ２０Ｂに要求する際に、端末１０Ｂの識別情報ＩＤ１０と第１の暗号$ＰＥＮ_{K10}$（Ｒ１０‖Ｒ２０）とを送信する。

[0165] 第２通信ユニット２２が要求メッセージを受け取ると、秘密値取得部２３１１Ｂは、第２鍵記憶ユニット２１に記憶された復号用秘密鍵Ｋ２０を用いて第１の暗号$ＰＥＮ_{K10}$（Ｒ１０‖Ｒ２０）を復号化して、通信数値Ｒ１０‖Ｒ２０を取得する。さらに、秘密値取得部２３１１Ｂは、乱数記憶モジュール１３７に記憶された第２乱数Ｒ２０と通信数値Ｒ１０‖Ｒ２０との単純演算によって、秘密値Ｒ１０を取得する。つまり、秘密値取得部２３１１Ｂは、通信数値Ｒ１０‖Ｒ２０から第２乱数Ｒ２０を取り除く。

[0166] 暗号化部２３１２Ａは、暗号化鍵生成部２３１３より得た暗号化鍵（＝$ＭＡＣ_{K10}$（Ｒ１０，Ｎ３０，ＩＤ２０））を共通鍵として用いて新たな通信用秘密鍵Ｋ１１を暗号化して第２の暗号（＝［$ＭＡＣ_{K10}$（Ｒ１０，Ｎ３０，ＩＤ２０）　ＸＯＲ　Ｋ１１］）を生成する。

[0167] 通信用秘密鍵送信モジュール２３２は、第２通信ユニット２２を制御して、新たな通信用秘密鍵Ｋ１１の発行を要求した端末１０Ｂに第２の暗号と第３ノンスＮ３０とを送信する（図８のプロセスＰ６０Ｂ）。

[0168] このように、サーバ２０Ｂは、端末１０Ｂに第２の暗号（＝［$ＭＡＣ_{K10}$（Ｒ１０，Ｎ３０，ＩＤ２０）　ＸＯＲ　Ｋ１１］）を送信する。

[0169] 上述のように、端末１０Ｂは、発行要求処理において、秘密値Ｒ１０より桁数が多い通信数値Ｒ１０‖Ｒ２０を生成して、サーバ２０Ｂに送信する。

ここで、通信数値Ｒ１０‖Ｒ２０は第三者に知られる可能性がある。しかしながら、通信数値Ｒ１０‖Ｒ２０は桁数が多く、しかも第三者は秘密値Ｒ１０と第２乱数Ｒ２０とからどのように通信数値Ｒ１０‖Ｒ２０が生成されているかを知ることはできない。よって、通信数値Ｒ１０‖Ｒ２０から総当たり法などで秘密値Ｒ１０を得ることは、秘密値Ｒ１０が価値を持つ時間内ではほぼ不可能である。

[0170] 本実施形態の鍵配布システムでは、秘密値を用いて生成された通信数値を端末１０Ｂがサーバ２０Ｂに送信する。通信数値は秘密値より桁数が多いから、秘密値そのものを送信する場合に比べて秘密値が第三者に知られる可能性が大幅に低減される。

[0171] ここで、単純に秘密値の桁数を多くすることによっても、秘密値が第三者に知られる可能性を大幅に低減できる。しかしながら、この場合には、サーバ２０Ｂや端末１０Ｂでの処理負荷が増大してしまう。

[0172] これに対して、本実施形態の鍵配布システムでは、秘密値より桁数が多い通信数値は、端末１０Ｂからサーバ２０Ｂに秘密値を送信するときだけ使用される。そのため、秘密値より桁数が大きい通信数値を用いて通信用秘密鍵の暗号化や復号化を行わなくて済む。つまり、本実施形態の鍵配布システムは、サーバ２０Ｂに秘密値を送信するときだけ擬似的に秘密値の桁数を多くするから、処理負荷が増大することがない。

[0173] このように本実施形態の鍵配布システムは、秘密値が第三者に知られる可能性を低減でき、しかもサーバ２０Ｂおよび端末１０Ｂの処理負荷の増加を抑制できる。

[0174] （実施形態４）

図９に示すように、本実施形態の鍵配布システムは、端末１０Ｃとサーバ２０Ｃとが実施形態２と異なる。本実施形態の鍵配布システムと実施形態２の鍵配布システムとで共通する構成には同一の符号を付して説明を省略する。

[0175] 端末１０Ｃは、第１鍵記憶ユニット１１と、第１通信ユニット１２と、鍵

要求ユニット１３Ｃと、第１識別情報記憶ユニット１４と、セッション鍵要求ユニット１５と、セッション鍵受取ユニット１６と、第１原始元記憶ユニット１７と、を有する。端末１０Ｃと端末１０Ａとで共通する構成の説明は省略する。

[0176] 第１原始元記憶ユニット１７は、大きい値の素数ｐと適宜値の原始元ｇとを記憶するように構成される。通信の安全性を考慮すれば、素数ｐと原始元ｇとを非公開とすることが好ましい。素数ｐと原始元ｇとを非公開とする場合には、素数ｐと原始元ｇとは管理装置４０によって端末１０Ｃに与えられる。

[0177] 鍵要求ユニット１３Ｃは、秘密値生成モジュール（第１秘密値生成モジュール）１３０Ｃと、秘密値記憶モジュール（第１秘密値記憶モジュール）１３１Ｃと、第１公開鍵生成モジュール１３８と、第１公開鍵送信モジュール１３９と、を有する。

[0178] 秘密値生成モジュール１３０Ｃは、新たな通信用秘密鍵の発行を要求する際に数値よりなる秘密値（第１秘密値）を生成するように構成される。第１秘密値は乱数である。

[0179] 秘密値記憶モジュール１３１Ｃは、秘密値生成モジュール１３０Ｃで生成された第１秘密値を記憶するように構成される。

[0180] 第１公開鍵生成モジュール１３８は、第１原始元記憶モジュール１７に記憶された原始元に秘密値記憶モジュール１３１Ｃに記憶された第１秘密値を適用することによって、ディフィー・ヘルマン鍵共有方式の第１公開鍵Ｋ４１を第１の暗号として生成するように構成される。第１秘密値をｘとすると、第１公開鍵Ｋ４１は、g^xのｐを法とした剰余R^x（＝g^x　ｍｏｄ　ｐ）で表される。

[0181] 第１公開鍵送信モジュール１３９は、新たな通信用秘密鍵の発行を要求する要求メッセージ（要求コマンド）とともに第１公開鍵生成モジュール１３８で生成された第１公開鍵Ｋ４１がサーバ２０に送信されるように第１通信ユニット１２を制御するように構成される。第１公開鍵送信モジュール１３

９は、第１公開鍵Ｋ４１とともに端末１０Ｃの識別情報も第１通信ユニット１２に送信させる。

[0182] このように、鍵要求ユニット１３Ｃは、サーバ２０Ｃに新たな通信用秘密鍵の発行を要求するときに、数値よりなる第１秘密値を新たに生成する。また、鍵要求ユニット１３Ｃは、第１原始元記憶ユニット１７に記憶された原始元に第１秘密値を適用することによりディフィー・ヘルマン鍵共有方式の第１公開鍵Ｋ４１を生成する。鍵要求ユニット１３Ｃは、第１公開鍵Ｋ４１をサーバ２０Ｃに送信する。

[0183] サーバ２０Ｃは、第２鍵記憶ユニット２１と、第２通信ユニット２２と、鍵発行ユニット２３Ｃと、第２識別情報記憶ユニット２４と、セッション鍵発行ユニット２５と、第２原始元記憶ユニット２６と、を有する。サーバ２０Ｃとサーバ２０Ａとで共通する構成の説明は省略する。

[0184] 第２原始元記憶ユニット２６は、第１原始元記憶ユニット１７と同様に、大きい値の素数ｐと適宜値の原始元ｇとを記憶するように構成される。素数ｐと原始元ｇとを非公開とする場合には、素数ｐと原始元ｇとは管理装置４０によってサーバ２０Ｃに与えられる。

[0185] 鍵発行ユニット２３Ｃは、鍵生成モジュール２３０Ｃと、通信用秘密鍵暗号化モジュール２３１Ｃと、通信用秘密鍵送信モジュール２３２Ｃと、第２保管モジュール２３３Ｃと、第２秘密値生成モジュール２３５と、第２公開鍵生成モジュール２３６と、を有する。

[0186] 鍵生成モジュール２３０Ｃは、第２通信ユニット２２が端末１０Ｃから要求メッセージを受け取ると、新たな通信用秘密鍵を生成するように構成される。

[0187] 第２秘密値生成モジュール２３５は、第２通信ユニット２２が要求メッセージを受け取ると、数値よりなる第２秘密値を生成するように構成される。第２秘密値は乱数である。つまり、第２秘密値生成モジュール２３５は、要求メッセージの受信毎にランダムな数値を持つ第２秘密値を生成する。つまり、通信用秘密鍵を発行する毎に第２秘密値は異なる数値を持つ。第２秘密

値は新たな通信用秘密鍵を端末１０Ｃに送信するまで用いられる。

[0188] 通信用秘密鍵暗号化モジュール２３１Ｃは、第２共通鍵生成モジュール２３１４と、暗号化部２３１２Ｃと、を有する。

[0189] 第２共通鍵生成モジュール２３１４は、第２通信ユニット２２が要求メッセージを受け取ると、第２通信ユニット２２が受け取った第１公開鍵Ｋ４１と第２秘密値生成モジュール２３５で生成された第２秘密値とを用いて、ディフィー・ヘルマン鍵共有方式の共通鍵Ｋ４０を生成するように構成される。第２秘密値をｙとすると、共通鍵Ｋ４０は、$(R^x)^y$のｐを法とした剰余R^{x^y}（$＝g^{xy}$　ｍｏｄ　ｐ）で表される。このような共通鍵Ｋ４０（＝Ｒｘｙ）は素数ｐを法としてg^{xy}と合同である。すなわち、$R^{xy}＝g^{xy}$　ｍｏｄ　ｐである。

[0190] 暗号化部２３１２Ｃは、第２共通鍵生成モジュール２３１４より得られた共通鍵Ｋ４０を用いて新たな通信用秘密鍵を暗号化して、第２の暗号を生成するように構成される。本実施形態では、暗号化部２３１２Ｃは、共通鍵Ｋ４０を用いて、メッセージ認証コードよりなる暗号化鍵を生成する。暗号化部２３１２Ｃは、この暗号化鍵を共通鍵として用いて新たな通信用秘密鍵を暗号化して第２の暗号を生成する。暗号化部２３１２Ｃは、たとえば、暗号化鍵と新たな通信用秘密鍵との排他的論理和を第２の暗号（暗号化された新たな通信用秘密鍵）として用いる。

[0191] 第２公開鍵生成モジュール２３６は、第２原始元記憶モジュール２６に記憶された原始元に第２秘密値生成モジュール２３５で生成された第２秘密値を適用することによって、ディフィー・ヘルマン鍵共有方式の第２公開鍵Ｋ４２を生成するように構成される。第２秘密値をｙとすると、第２公開鍵Ｋ４２は、g^yのｐを法とした剰余R^y（$＝g^y$　ｍｏｄ　ｐ）で表される。

[0192] 通信用秘密鍵送信モジュール２３２Ｃは、第２通信ユニット２２を制御して、通信用秘密鍵暗号化モジュール２３１Ｃで生成された第２の暗号と、第２公開鍵生成モジュール２３６で生成された第２公開鍵Ｋ４２とを端末１０Ｃに送信するように構成される。

[0193] 第２保管モジュール２３３Ｃは、鍵生成モジュール２３０Ｃで生成された新たな通信用秘密鍵を第２鍵記憶ユニット２１に記憶させるように構成される。なお、第２保管モジュール２３３は、第２鍵記憶ユニット２１に記憶された通信用秘密鍵を、鍵生成モジュール２３０Ｃで生成された新たな通信用秘密鍵に更新するように構成されていてもよい。

[0194] このように、鍵発行ユニット２３Ｃは、端末１０Ｃから新たな通信用秘密鍵の発行が要求されると、数値よりなる第２秘密値を生成する。鍵発行ユニット２３Ｃは、端末１０Ｃから受信した第１公開鍵と第２秘密値とを用いてディフィー・ヘルマン鍵共有方式の共通鍵Ｋ４０を生成する。鍵発行ユニット２３Ｃは、第２原始元記憶ユニット２６に記憶された原始元に第２秘密値を適用することによりディフィー・ヘルマン鍵共有方式の第２公開鍵Ｋ４２を生成する。鍵発行ユニット２３Ｃは、共通鍵Ｋ４０を用いて新たな通信用秘密鍵を暗号化して第２公開鍵Ｋ４２とともに端末１０Ｃに送信する。

[0195] また、鍵発行ユニット２３Ｃは、端末１０Ｃから新たな通信用秘密鍵の発行が要求されると、新たな通信用秘密鍵を発行して第２鍵記憶ユニット２１に記憶させる。そのため、第２通信ユニット２２は、通信用秘密鍵を共通鍵として用いた暗号化通信を端末１０Ｃと行う場合には、新たな通信用秘密鍵を使用する。

[0196] 鍵要求ユニット１３Ｃは、さらに、通信用秘密鍵復号化モジュール１３４Ｃと、第１保管モジュール１３５と、を有する。

[0197] 通信用秘密鍵復号化モジュール１３４Ｃは、第１共通鍵生成モジュール１３４３と、復号化部１３４２Ｃと、を有する。

[0198] 第１共通鍵生成モジュール１３４３は、第１通信ユニット１２が第２の暗号と第２公開鍵Ｋ４２とを受け取ると、秘密値記憶モジュール１３１Ｃに記憶された第１秘密値ｘと第２公開鍵Ｋ４２とを用いてディフィー・ヘルマン鍵共有方式の共通鍵Ｋ４０を生成するように構成される。上述したように、共通鍵Ｋ４０は剰余R^{xy}（＝g^{xy}　ｍｏｄ　ｐ）で表され、第２公開鍵Ｋ４２は剰余R^{y}（＝g^{y}　ｍｏｄ　ｐ）で表される。よって、第１秘密値ｘと第２公

開鍵Ｋ４２とから共通鍵Ｋ４０を生成できる。

[0199] 復号化部１３４２Ｃは、第１共通鍵生成モジュール１３４３で生成された共通鍵Ｋ４０を用いて第１通信ユニット１２が受け取った第２の暗号を復号化し、これによって新たな通信用秘密鍵を得るように構成される。本実施形態では、復号化部１３４２Ｃは、共通鍵Ｋ４０を用いて、暗号化部２３１２Ｃで生成された暗号化鍵と等しいメッセージ認証コードよりなる復号化鍵を生成する。復号化部１３４２Ｃは、この復号化鍵を共通鍵として用いて新たな通信用秘密鍵を復号化して第２の暗号を取得する。復号化部１３４２Ｃは、たとえば、復号化鍵と第２の暗号との排他論理和を求めることにより新たな通信用秘密鍵を取得する。

[0200] このように鍵要求ユニット１３Ｃは、サーバ２０Ｃから暗号化された新たな通信用秘密鍵（第２の暗号）と第２公開鍵Ｋ４２とを受信すると、第１秘密値とサーバ２０Ｃから受信した第２公開鍵とを用いて共通鍵Ｋ４０を生成する。鍵要求ユニット１３Ｃは、共通鍵Ｋ４０を用いて第２の暗号を復号化して新たな通信用秘密鍵を取得して、第１鍵記憶ユニット１１に記憶させる。そのため、第１通信ユニット１２は、通信用秘密鍵を共通鍵として用いた暗号化通信をサーバ２０Ｃと行う場合には、新たな通信用秘密鍵を使用する。

[0201] 次に、図１０を参照して本実施形態の鍵配布システムの動作について説明する。なお、プロセスＰ３０，Ｐ４０，Ｐ７０，Ｐ８０については実施形態１で述べたから説明を省略する。

[0202] なお、端末１０Ｃの出荷時には、端末１０Ｃに通信用秘密鍵を登録する作業と、管理装置２０に通信用秘密鍵Ｃを登録する作業とが行われる。通信用秘密鍵の登録には、管理装置４０が用いられる。管理装置４０は、通信用秘密鍵の登録の際には、インターネットのような通信路を用いてサーバ２０Ｃおよび端末１０Ｃに接続される。

[0203] 図１０に示すように、管理装置４０は、通信用秘密鍵Ｋ１０をサーバ２０Ｃに送信する（図１０のプロセスＰ１０Ｃ）。サーバ２０Ｃは、管理装置４

０から受け取った通信用秘密鍵Ｋ１０を第２鍵記憶ユニット２１に登録する。

[0204] 管理装置４０は、端末１０Ｃを識別するための識別情報（端末識別情報）ＩＤ１０をサーバ２０Ｃに送信する。サーバ２０Ｃは、管理装置４０から受け取った識別情報ＩＤ１０を第２識別情報記憶ユニット２４に登録する。

[0205] 管理装置４０は、端末１０Ｃの識別情報ＩＤ１０と、サーバ２０Ｃに登録された通信用秘密鍵Ｋ１０とを端末１０Ｃに送信する（図１０のプロセスＰ２０Ｃ）。端末１０Ｃは、管理装置４０から受け取った識別情報ＩＤ１０を第１識別情報記憶ユニット１４に登録する。また、端末１０Ｃは、管理装置４０から受け取った通信用秘密鍵Ｋ１０を第１鍵記憶ユニット１１に登録する。

[0206] すなわち、サーバ２０Ｃの第２鍵記憶ユニット２１と端末１０Ｃの第１鍵ユニット１１とには、それぞれ事前秘密鍵として通信用秘密鍵Ｋ１０が登録される。本実施形態では、実施形態２とは異なり、サーバ２０の第２鍵記憶ユニット２１には、通信用秘密鍵Ｋ１０とペアになる事前秘密鍵として復号用秘密鍵Ｋ２０が登録されない。

[0207] 発行要求処理が開始されると、秘密値生成モジュール１３０Ｃは、第１秘密値ｘを生成する。第１秘密値ｘは秘密値記憶モジュール１３１Ｃに記憶される。第１公開鍵生成モジュール１３８は、秘密値記憶モジュール１３１Ｃに記憶された第１秘密値ｘと第１原始元記憶ユニット１７に記憶された原始元ｇおよび素数ｐとを利用して、第１公開鍵Ｋ４１を生成する。第１公開鍵送信モジュール１３９は、第１通信ユニット１２を制御して、第１公開鍵Ｋ４１を、端末１０Ｃの識別情報ＩＤ１０および要求メッセージとともにサーバ２０Ｃに送信する（図１０のプロセスＰ５０Ｃ）。このように、端末１０Ｃは、通信用秘密鍵の発行をサーバ２０Ｃに要求する際に、端末１０Ｃの識別情報ＩＤ１０と第１の公開鍵Ｋ４１（＝R^x）とを送信する。

[0208] 第２通信ユニット２２が要求メッセージを受信すると、第２秘密値生成モジュール２３５は、第２秘密値ｙを生成する。

[0209] 第２公開鍵生成モジュール２３６は、第２原始元記憶モジュール２６に記憶された原始元ｇに第２秘密値生成モジュール２３５で生成された第２秘密値ｙを適用することによって、第２公開鍵Ｋ４２（＝R^y）を生成する。

[0210] 第２共通鍵生成モジュール２３１４は、第２通信ユニット２２が受け取った第１公開鍵Ｋ４１と第２秘密値生成モジュール２３５で生成された第２秘密値ｙとを用いて、共通鍵Ｋ４０を生成する。

[0211] 暗号化部２３１２Ｃは、共通鍵Ｋ４０と情報Ｉ４０とを用いて、暗号化鍵（＝MAC_{K40}（Ｉ４０））を生成する。情報Ｉ４０は、共通鍵Ｋ４０と、第２公開鍵Ｋ４２（＝R^y）と、サーバ２０Ｃの識別情報ＩＤ２０とである。すなわち、Ｉ４０＝（Ｋ４０，R^y，ＩＤ２０）である。剰余Ｒｙは乱数である第２秘密値ｙにより生成されているから、実質的にノンスとして使用できる。

[0212] 暗号化部２３１２Ｃは、暗号化鍵（＝MAC_{K40}（Ｋ４０，R^y，ＩＤ２０））と新たな通信用秘密鍵Ｋ１１との排他的論理和（＝［MAC_{K40}（Ｋ４０，R^y，ＩＤ２０）　ＸＯＲ　Ｋ１１］）を第２の暗号（暗号化された新たな通信用秘密鍵）として用いる。共通鍵Ｋ４０は第１秘密値ｘを用いて生成されるため、通信用秘密鍵暗号化モジュール２３１Ｃは第１秘密値ｘを用いて新たな通信用秘密鍵Ｋ１１を暗号化しているといえる。

[0213] 通信用秘密鍵送信モジュール２３２Ｃは、第２通信ユニット２２を制御して、第２の暗号（＝［MAC_{K40}（Ｋ４０，R^y，ＩＤ２０）　ＸＯＲ　Ｋ１１］）と、第２公開鍵Ｋ４２（＝R^y）とを端末１０Ｃに送信する（図１０のプロセスＰ６０Ｃ）。

[0214] 第２保管モジュール２３３Ｃは、鍵生成モジュール２３０Ｃで生成された新たな通信用秘密鍵Ｋ１１を第２鍵記憶ユニット２１に記憶させる。

[0215] このように、サーバ２０Ｃは端末１０Ｃに第２の暗号と第２公開鍵Ｋ４２とを送信する。

[0216] 第１通信ユニット１２が第２の暗号と第２公開鍵Ｋ４２とを受け取ると、第１共通鍵生成モジュール１３４３は、秘密値記憶モジュール１３１Ｃに記憶された第１秘密値ｘと第２公開鍵Ｋ４２とを用いてディフィー・ヘルマン

鍵共有方式の共通鍵Ｋ４０を生成する。

[0217] このように、第１共通鍵生成モジュール１３４３は第１秘密値ｘと剰余R^yとを用いて、$(R^y)^x$の値を求める。ここで、$R^{yx}=(R^y)^x \mod p$とすると、R^{yx}は素数ｐを法としてg^{xy}と合同である。よって、$R^{xy}=R^{yx}$である。そのため、第１共通鍵生成モジュール１３４３は、共通鍵Ｋ４０を生成できる。

[0218] 復号化部１３４２Ｃは、第１共通鍵生成モジュール１３４３で生成された共通鍵Ｋ４０と、サーバ２０Ｃの識別情報ＩＤ２０と、サーバ２０Ｃから受信した第２公開鍵Ｋ４２とを用いて復号化鍵（$=MAC_{K40}$（Ｋ４０，R^y，ＩＤ２０））を生成する。復号化部１３４２Ｃは、生成された復号化鍵（$=MAC_{K40}$（Ｋ４０，R^y，ＩＤ２０））と第２の暗号（＝［MAC_{K40}（Ｋ４０，R^y，ＩＤ２０）　ＸＯＲ　Ｋ１１］）との排他的論理和を演算することで、新たな通信用秘密鍵Ｋ１１を取得する。

[0219] 第１保管モジュール１３５は、通信用秘密鍵復号化モジュール１３４Ｃによって得られた新たな通信用秘密鍵Ｋ１１を第１鍵記憶ユニット１１に記憶させる。

[0220] そして、第１通信ユニット１２は、第１鍵記憶ユニット１１に新たな通信用秘密鍵Ｋ１１が記憶された後は、新たな通信用秘密鍵Ｋ１１を共通鍵として用いた暗号化通信をサーバ２０Ｃと行う。第２通信ユニット２２は、第２鍵記憶ユニット２１に新たな通信用秘密鍵Ｋ１１が記憶された後は、新たな通信用秘密鍵Ｋ１１を共通鍵として用いた暗号化通信を端末１０Ｃと行う。

[0221] そのため、新たな通信用秘密鍵Ｋ１１が発行された後は、他者が前の通信用秘密鍵Ｋ１０を知っていても、端末１０Ｃとサーバ２０Ｃとの間の通信を盗聴できなくなる。

[0222] 以上述べた本実施形態の鍵配布システムは、ディフィー・ヘルマン鍵共有方式の共通鍵Ｋ４０を利用して、新たな通信用秘密鍵Ｋ１１を暗号化して端末１０Ｃに送信する。そのため、元の通信用秘密鍵Ｋ１０を知っている第三者であっても暗号化された新たな通信用秘密鍵Ｋ１１を復号化できない。よ

って、新たな通信用秘密鍵Ｋ１１を端末１０Ｃに安全に届けることができる。

請求の範囲

[請求項1] 端末と、通信ネットワークを介して上記端末に接続されるサーバとを備え、

上記端末は、

通信用秘密鍵と公開鍵とを記憶する書換可能な第１鍵記憶ユニットと、

上記第１鍵記憶ユニットに記憶された上記通信用秘密鍵を共通鍵として用いた暗号化通信を上記サーバと行うための第１通信ユニットと、

上記サーバに新たな通信用秘密鍵の発行を要求するときに、数値よりなる秘密値を新たに生成するとともに、上記第１記憶ユニットに記憶された上記公開鍵を用いて上記秘密値を暗号化して第１の暗号を生成し、上記第１の暗号を上記サーバに送信する鍵要求ユニットと、を有し、

上記サーバは、

上記通信用秘密鍵に加えて、上記公開鍵とペアになる私有鍵である復号用秘密鍵を記憶する書換可能な第２鍵記憶ユニットと、

上記第２鍵記憶ユニットに記憶された上記通信用秘密鍵を共通鍵として用いた暗号化通信を上記端末と行うための第２通信ユニットと、

上記端末から新たな通信用秘密鍵の発行が要求されると、新たな通信用秘密鍵を発行して上記第２鍵記憶ユニットに記憶させ、上記復号用秘密鍵を用いて上記第１の暗号を復号化することによって上記秘密値を取得し、当該秘密値を利用して上記新たな通信用秘密鍵を暗号化して第２の暗号を生成し、新たな通信用秘密鍵の発行を要求した上記端末に上記第２の暗号を送信する鍵発行ユニットと、を有し、

上記鍵要求ユニットは、上記秘密値を利用して上記第２の暗号を復号化することによって上記新たな通信用秘密鍵を取得して、上記第１

鍵記憶ユニットに記憶させるように構成され、

上記第１通信ユニットは、上記第１鍵記憶ユニットに上記新たな通信用秘密鍵が記憶された後は、上記新たな通信用秘密鍵を共通鍵として用いた暗号化通信を上記サーバと行うように構成され、

上記第２通信ユニットは、上記第２鍵記憶ユニットに上記新たな通信用秘密鍵が記憶された後は、上記新たな通信用秘密鍵を共通鍵として用いた暗号化通信を上記端末と行うように構成されることを特徴とする鍵配布システム。

[請求項2] 上記鍵要求ユニットは、上記サーバに新たな通信用秘密鍵の発行を要求するときに、上記第１鍵記憶ユニットに記憶された上記通信用秘密鍵を上記公開鍵として用いて上記新たに生成された秘密値を暗号化するように構成され、

上記鍵発行ユニットは、上記端末から新たな通信用秘密鍵の発行が要求されると、上記新たな通信用秘密鍵を発行するとともに、上記新たな通信用秘密鍵とペアになる私有鍵である新たな復号用秘密鍵を発行して上記第２鍵記憶ユニットに記憶させ、上記第２記憶ユニットに上記新たな復号用秘密鍵が記憶された後は、上記新たな復号用秘密鍵を用いて上記第１の暗号を復号化するように構成されることを特徴とする請求項１記載の鍵配布システム。

[請求項3] 上記鍵要求ユニットは、上記秘密値として使用する第１乱数と、第２乱数とを生成し、上記サーバに新たな通信用秘密鍵の発行を要求する前に上記第２乱数を上記サーバに送信し、上記第１乱数と上記第２乱数との単純演算により通信数値を生成し、上記公開鍵を用いて上記通信数値を暗号化して上記サーバに送信するように構成されることを特徴とする請求項１記載の鍵配布システム。

[請求項4] 上記鍵発行ユニットは、上記端末から新たな通信用秘密鍵の発行が要求されると、上記端末から受信した上記秘密値を含むメッセージコードを生成し、上記メッセージコードを用いて上記新たな通信用秘密

鍵を暗号化して上記端末に送信するように構成されることを特徴とする請求項１記載の鍵配布システム。

[請求項5] 端末と、通信ネットワークを介して上記端末に接続されるサーバとを備え、

上記端末は、

通信用秘密鍵を記憶する書換可能な第１鍵記憶ユニットと、

所定の原始元を記憶する第１原始元記憶ユニットと、

上記第１記憶ユニットに記憶された上記通信用秘密鍵を共通鍵として用いた暗号化通信を上記サーバと行うための第１通信ユニットと、

上記サーバに新たな通信用秘密鍵の発行を要求するときに、数値よりなる第１秘密値を新たに生成するとともに、上記第１原始元記憶ユニットに記憶された上記原始元に上記第１秘密値を適用することによりディフィー・ヘルマン鍵共有方式の第１公開鍵を生成して上記サーバに送信する鍵要求ユニットと、を有し、

上記サーバは、

上記通信用秘密鍵を記憶する第２鍵記憶ユニットと、

上記所定の原始元を記憶する第２原始元記憶ユニットと、

上記第２記憶ユニットに記憶された上記通信用秘密鍵を共通鍵として用いた暗号化通信を上記端末と行うための第２通信ユニットと、

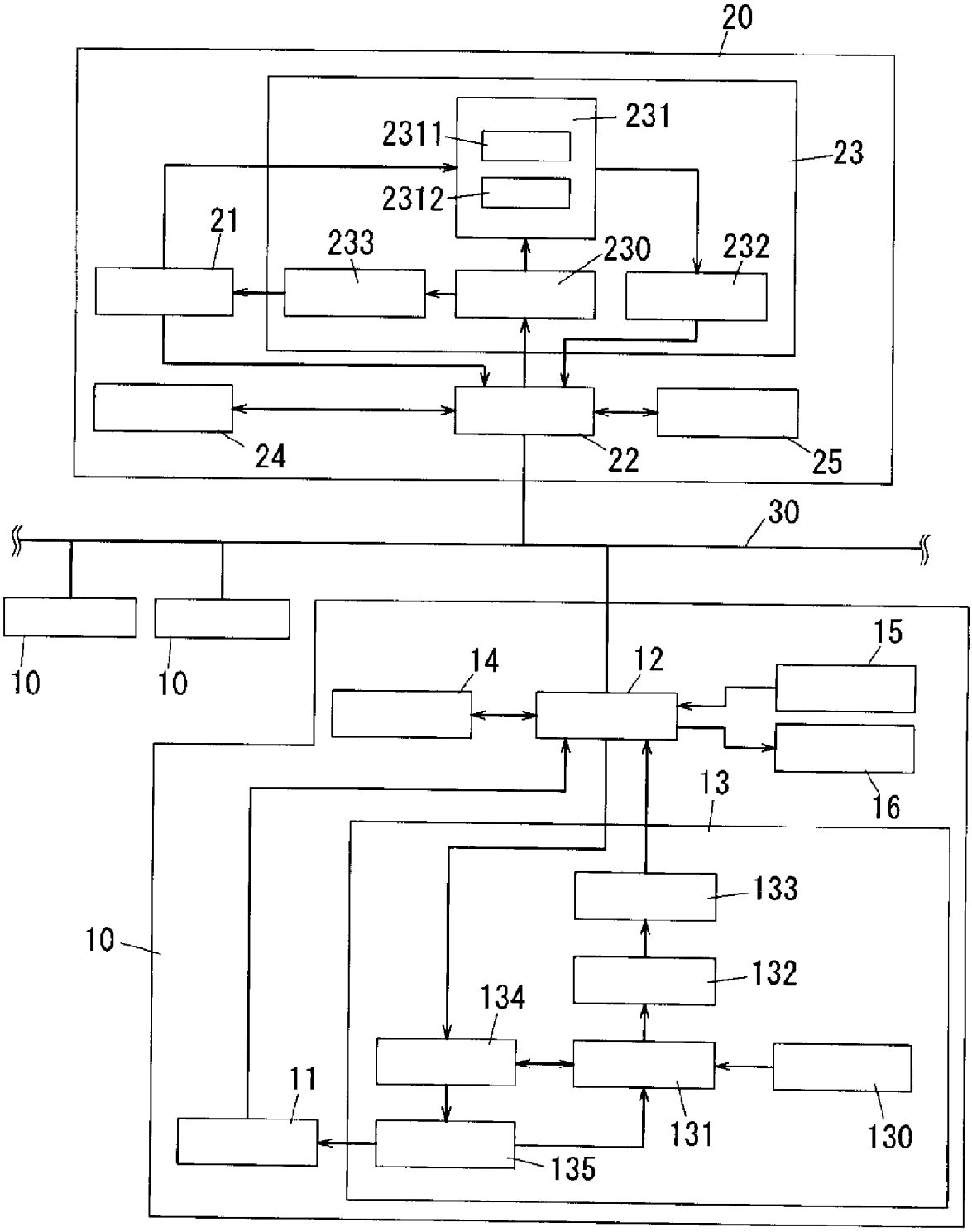
上記端末から新たな通信用秘密鍵の発行が要求されると、数値よりなる第２秘密値を生成し、上記端末から受信した第１公開鍵と上記第２秘密値とを用いて上記ディフィー・ヘルマン鍵共有方式の共通鍵を生成し、上記第２原始元記憶ユニットに記憶された上記原始元に上記第２秘密値を適用することにより上記ディフィー・ヘルマン鍵共有方式の第２公開鍵を生成し、上記共通鍵を用いて上記新たな通信用秘密鍵を暗号化して上記第２公開鍵とともに新たな通信用秘密鍵の発行を要求した上記端末に送信する鍵発行ユニットと、を有し、

上記鍵要求ユニットは、上記サーバから暗号化された上記新たな通信用秘密鍵と上記第２公開鍵とを受信すると、上記新たに生成された秘密値と上記サーバから受信した上記第２公開鍵とを用いて上記共通鍵を生成し、暗号化された上記新たな通信用秘密鍵を生成された上記共通鍵を用いて復号化して上記新たな通信用秘密鍵を取得して、上記第１鍵記憶ユニットに記憶させるように構成され、

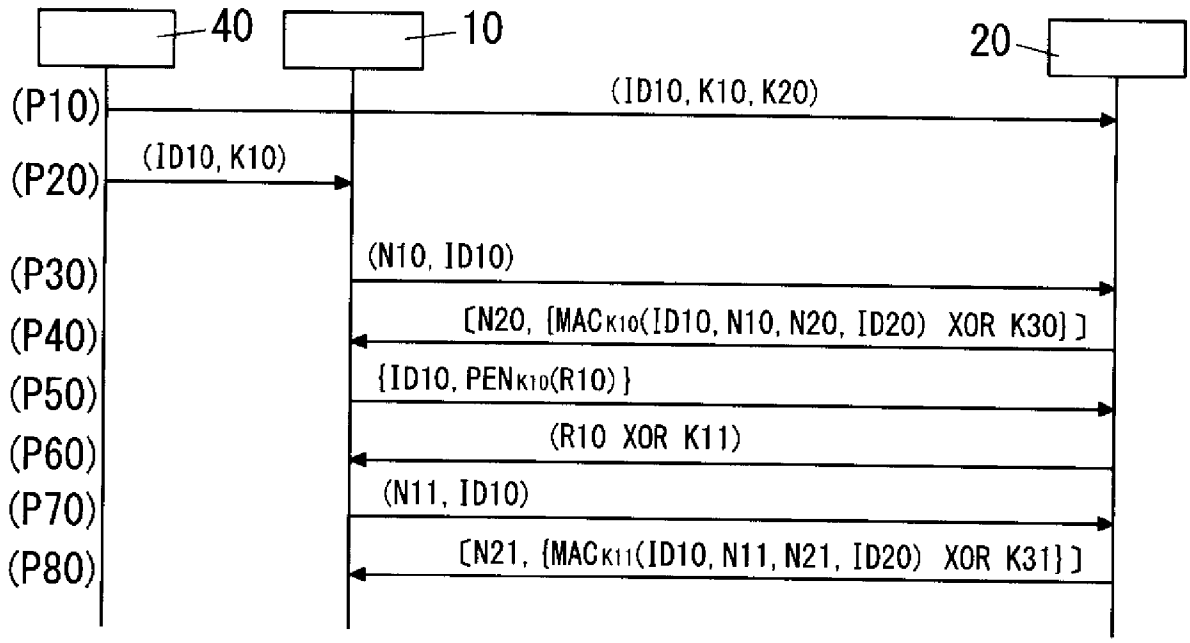
上記第１通信ユニットは、上記第１記憶ユニットに上記新たな通信用秘密鍵が記憶された後は、上記新たな通信用秘密鍵を共通鍵として用いた暗号化通信を上記サーバと行うように構成され、

上記第２通信ユニットは、上記第２記憶ユニットに上記新たな通信用秘密鍵が記憶された後は、上記新たな通信用秘密鍵を共通鍵として用いた暗号化通信を上記端末と行うように構成されることを特徴とする鍵配布システム。

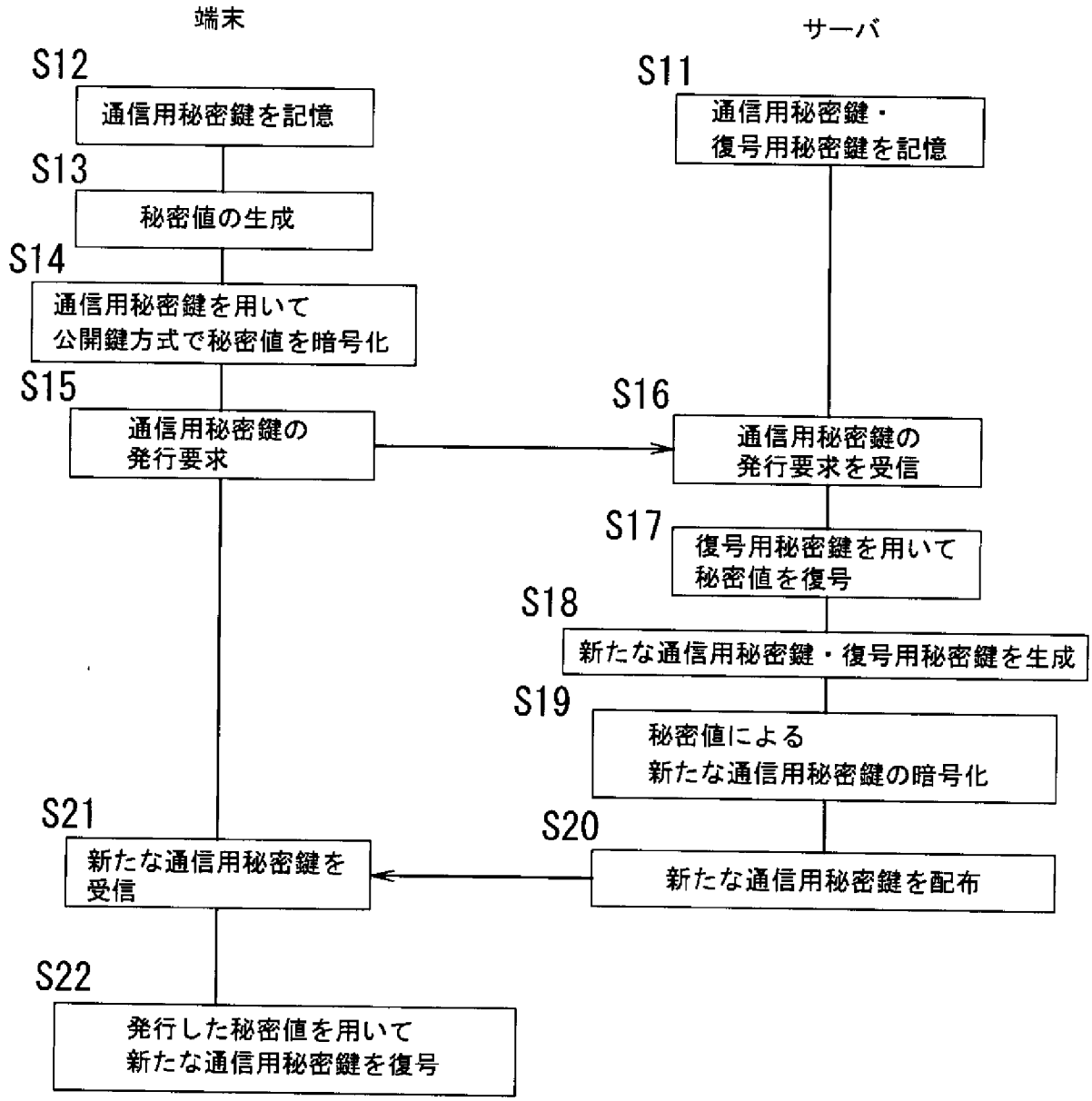
[図1]


20
231
2311
2312
23
21
233
230
232
24
22
25
30
10
10
15
14
12
16
13
133
10
132
134
11
131
130
135

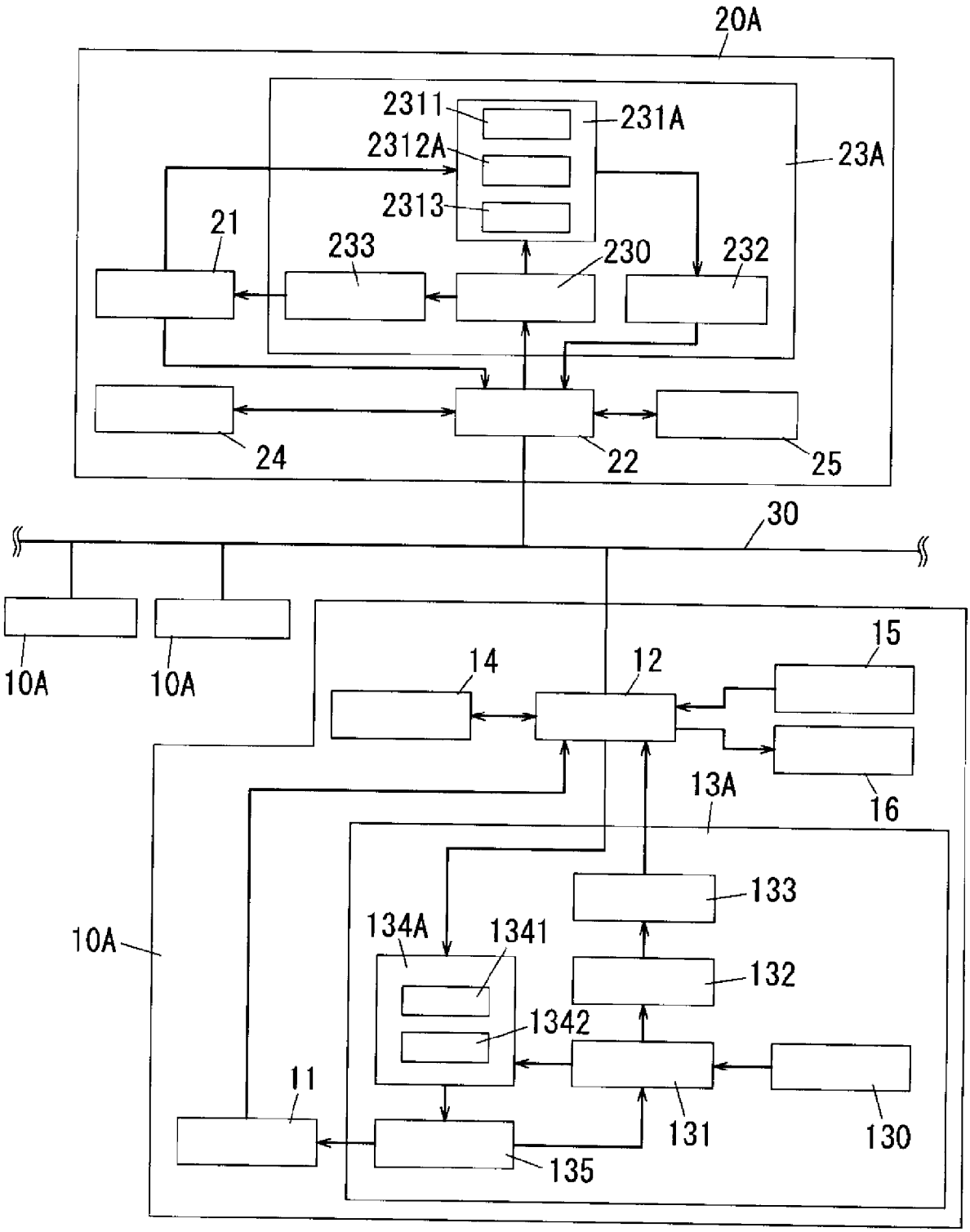
[図2]


40
10
20
(P10)
(ID10, K10, K20)
(P20)
(ID10, K10)
(P30)
(N10, ID10)
(P40)
[N20, {MACK10(ID10, N10, N20, ID20) XOR K30}]
(P50)
{ID10, PENK10(R10)}
(P60)
(R10 XOR K11)
(P70)
(N11, ID10)
(P80)
[N21, {MACK11(ID10, N11, N21, ID20) XOR K31}]

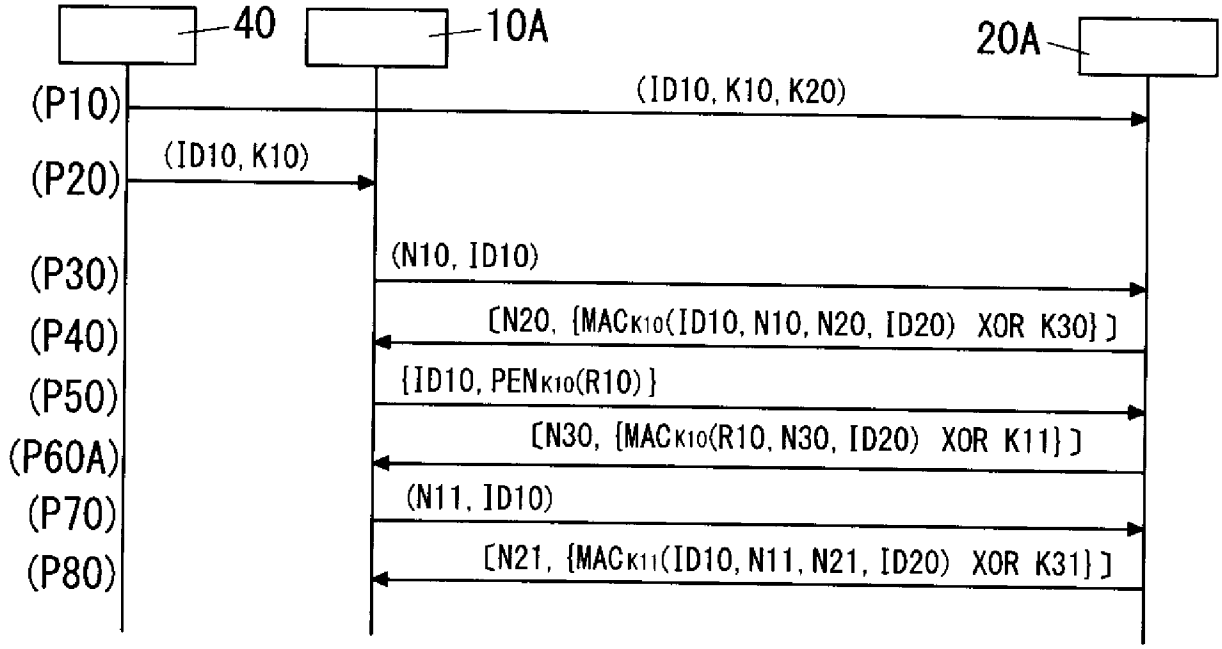
[図3]


端末
サーバ
S12
通信用秘密鍵を記憶
S13
秘密値の生成
S14
通信用秘密鍵を用いて
公開鍵方式で秘密値を暗号化
S15
通信用秘密鍵の
発行要求
S11
通信用秘密鍵・
復号用秘密鍵を記憶
S16
通信用秘密鍵の
発行要求を受信
S17
復号用秘密鍵を用いて
秘密値を復号
S18
新たな通信用秘密鍵・復号用秘密鍵を生成
S19
秘密値による
新たな通信用秘密鍵の暗号化
S20
新たな通信用秘密鍵を配布
S21
新たな通信用秘密鍵を
受信
S22
発行した秘密値を用いて
新たな通信用秘密鍵を復号

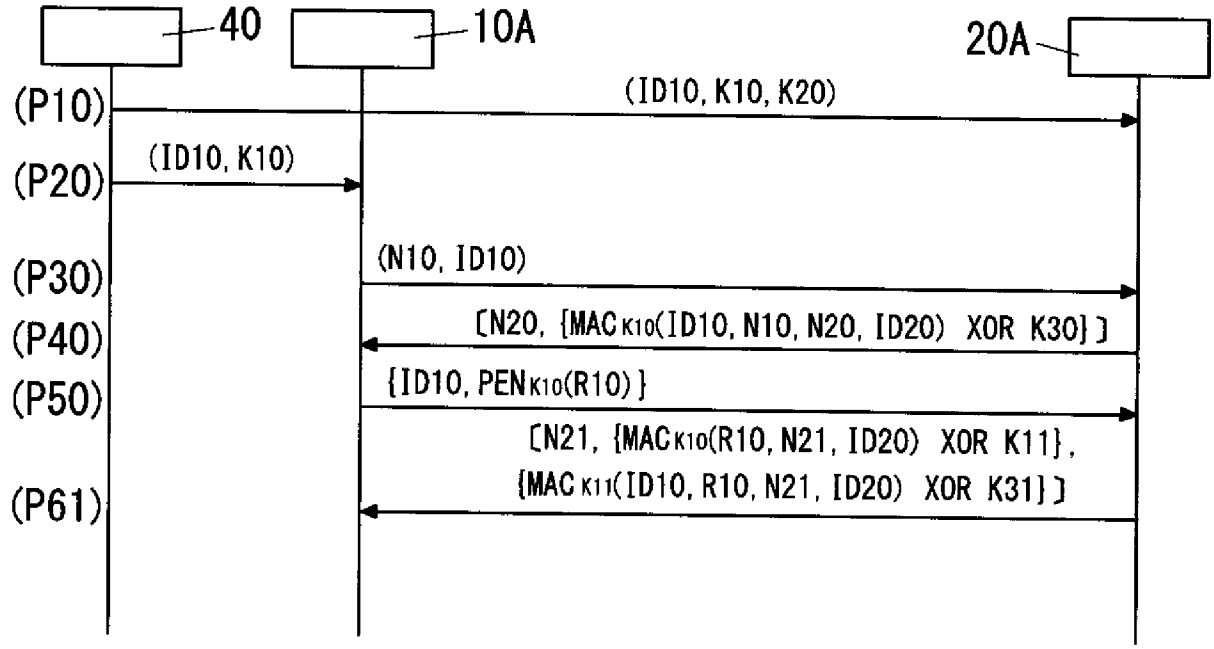
[図4]


20A
2311
231A
2312A
23A
2313
21
233
230
232
24
22
25
30
10A
10A
14
12
15
16
13A
133
134A
1341
132
1342
10A
11
131
130
135

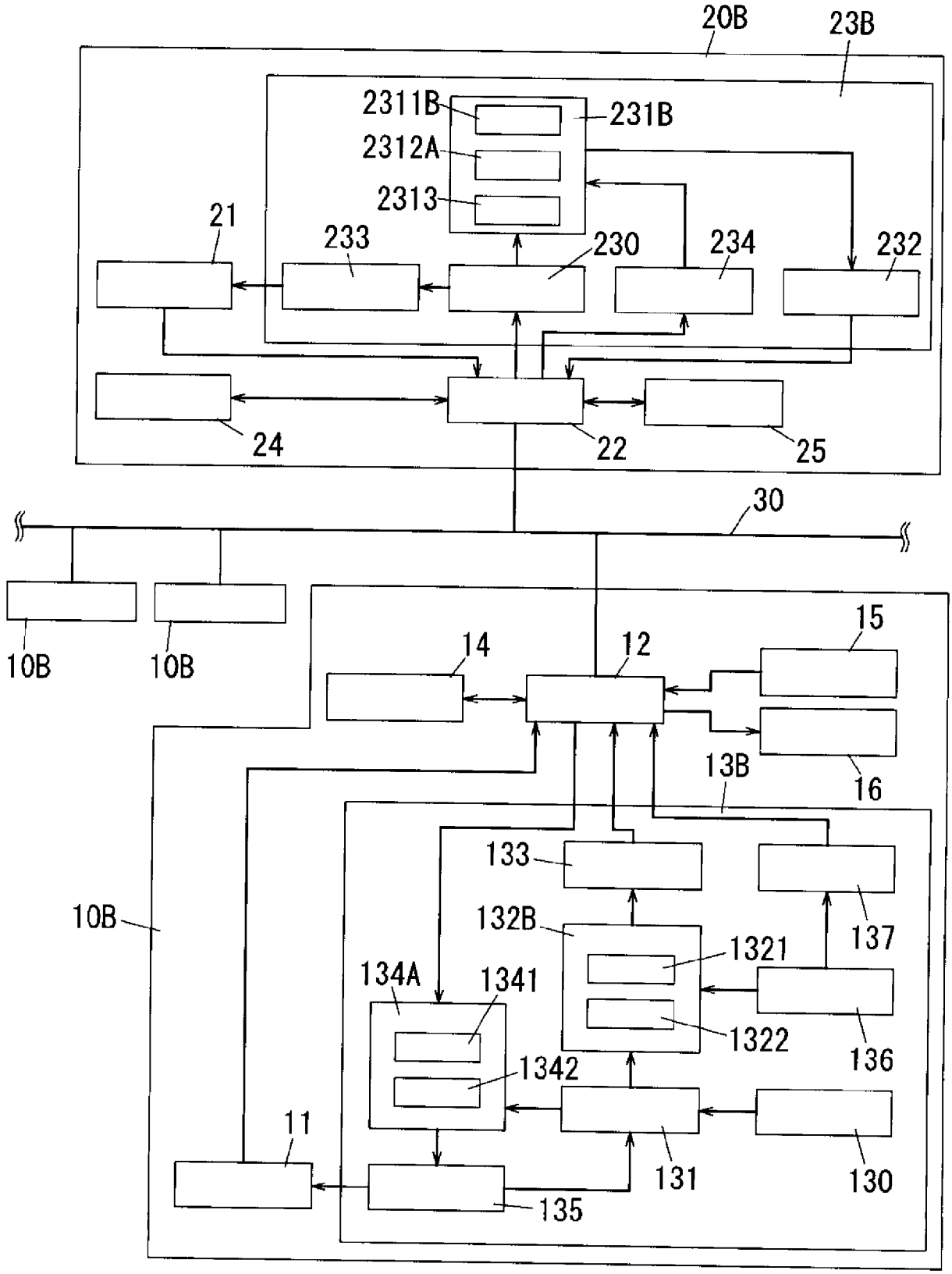
[図5]


40
10A
20A
(P10)
(ID10, K10, K20)
(P20)
(ID10, K10)
(P30)
(N10, ID10)
(P40)
〔N20, {MACK10(ID10, N10, N20, ID20) XOR K30}〕
(P50)
{ID10, PENK10(R10)}
(P60A)
〔N30, {MACK10(R10, N30, ID20) XOR K11}〕
(P70)
(N11, ID10)
(P80)
〔N21, {MACK11(ID10, N11, N21, ID20) XOR K31}〕

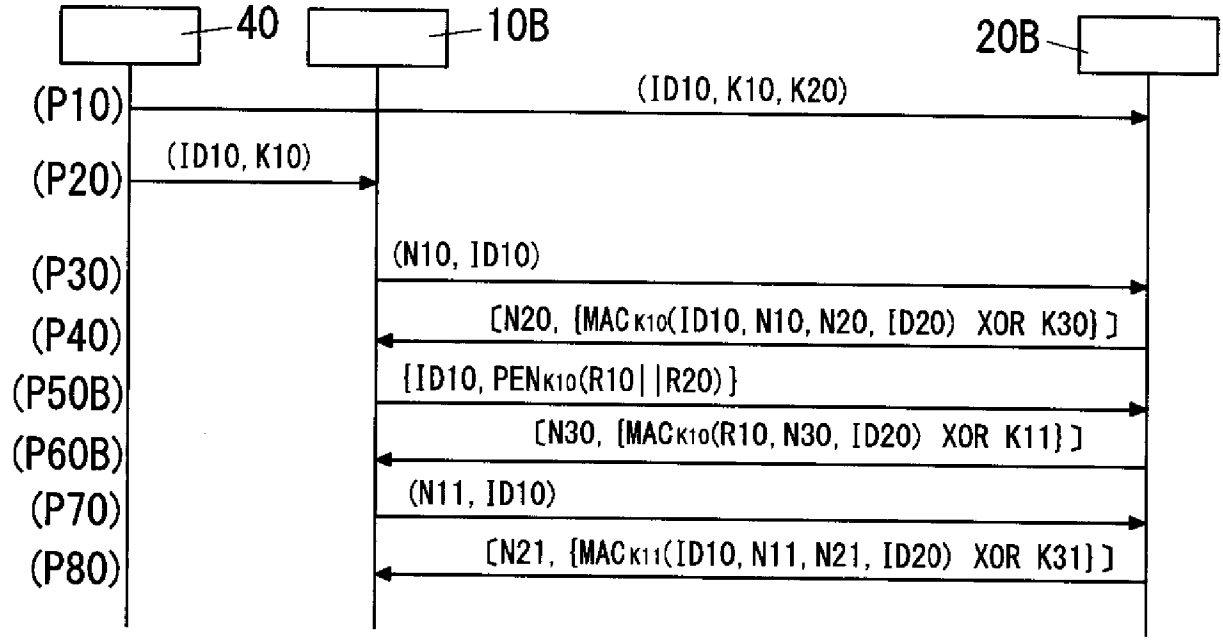
[図6]


40
10A
20A
(P10)
(ID10, K10, K20)
(P20)
(ID10, K10)
(P30)
(N10, ID10)
(P40)
〔N20, {MACK10(ID10, N10, N20, ID20) XOR K30}〕
(P50)
{ID10, PENK10(R10)}
〔N21, {MACK10(R10, N21, ID20) XOR K11},
{MACK11(ID10, R10, N21, ID20) XOR K31}〕
(P61)

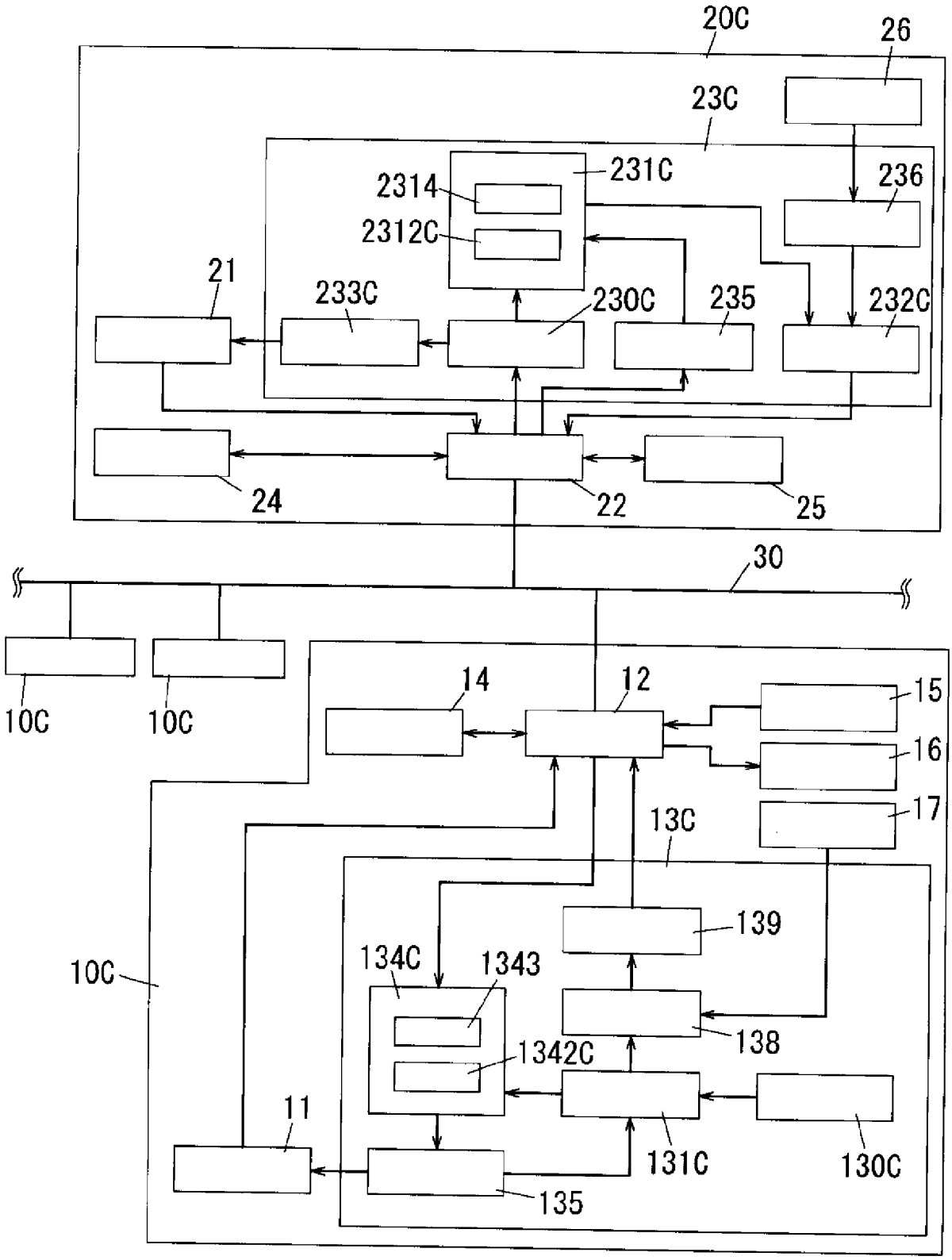
[図7]


20B
23B
2311B
231B
2312A
2313
21
233
230
234
232
24
22
25
30
10B
10B
14
12
15
16
13B
133
132B
1321
137
134A
1341
1322
136
1342
11
131
130
135
10B

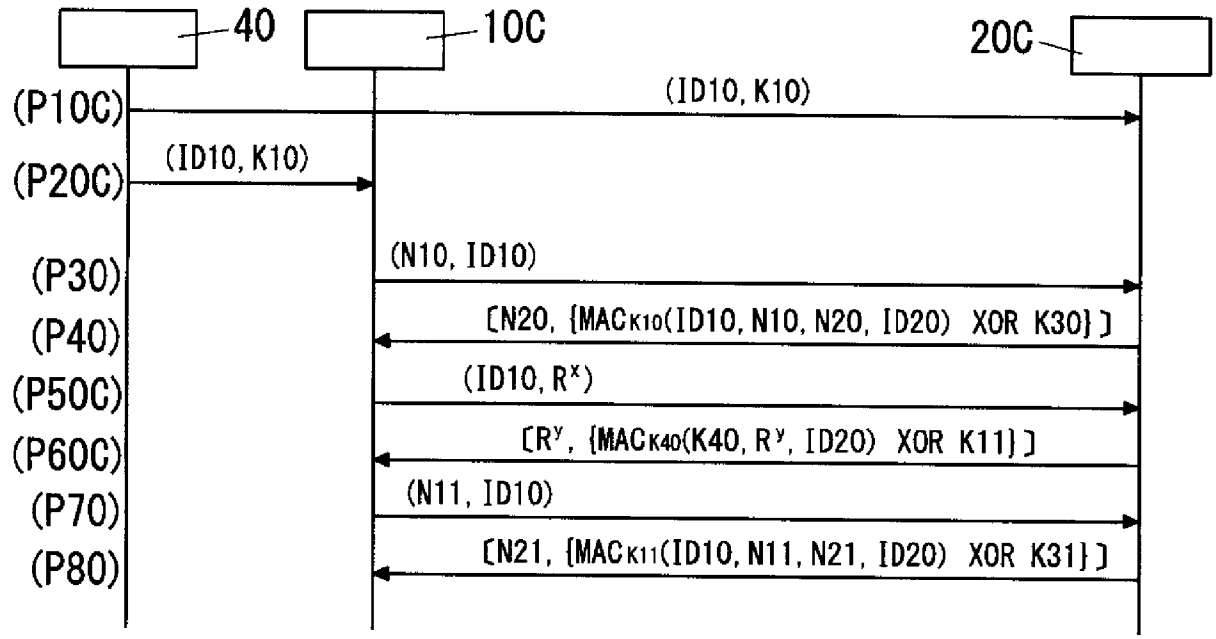
[図8]


40
10B
20B
(P10)
(ID10, K10, K20)
(P20)
(ID10, K10)
(P30)
(N10, ID10)
(P40)
〔N20, {MACK10(ID10, N10, N20, 〔D20) XOR K30}〕
(P50B)
{ID10, PENK10(R10||R20)}
(P60B)
〔N30, {MACK10(R10, N30, ID20) XOR K11}〕
(P70)
(N11, ID10)
(P80)
〔N21, {MACK11(ID10, N11, N21, ID20) XOR K31}〕

[図9]


20C
26
23C
231C
2314
2312C
236
21
233C
230C
235
232C
24
22
25
30
10C
10C
14
12
15
16
17
13C
139
10C
134C
1343
138
1342C
11
131C
130C
135

[図10]


40
10C
20C
(P10C)
(ID10, K10)
(P20C)
(ID10, K10)
(P30)
(N10, ID10)
(P40)
[N20, {MACK10(ID10, N10, N20, ID20) XOR K30}]
(P50C)
(ID10, Rx)
(P60C)
[Ry, {MACK40(K40, Ry, ID20) XOR K11}]
(P70)
(N11, ID10)
(P80)
[N21, {MACK11(ID10, N11, N21, ID20) XOR K31}]

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/070284

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/08(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2010
Kokai Jitsuyo Shinan Koho	1971-2010	Toroku Jitsuyo Shinan Koho	1994-2010

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2003-69547 A (Fujitsu Ltd.), 07 March 2003 (07.03.2003), paragraphs [0022] to [0076] & US 2003/0046539 A1	1,2,4 3
Y A	JP 11-196081 A (Advanced Mobile Telecommunications Security Technology Research Laboratories Co., Ltd.), 21 July 1999 (21.07.1999), paragraphs [0002] to [0011] (Family: none)	1,2,4,5 3
Y	JP 2002-198957 A (Sony Corp.), 12 July 2002 (12.07.2002), paragraphs [0257] to [0266] & US 2002/0073229 A1	5

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 February, 2010 (12.02.10)	23 February, 2010 (23.02.10)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2009/070284

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-138674 A (Matsushita Electric Industrial Co., Ltd.), 16 May 2000 (16.05.2000), paragraph [0044] & EP 998073 A2	3
A	WO 2005/048008 A2 (M-SYSTEMS FLASH DISK PIONEERS LTD.), 26 May 2005 (26.05.2005), page 6, line 1 to page 6, line 3; page 8, line 20 to page 17, line 15 & EP 1692800 A	3

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００９／０７０２８４

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１０年
日本国実用新案登録公報	１９９６－２０１０年
日本国登録実用新案公報	１９９４－２０１０年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	JP 2003-69547 A (富士通株式会社) 2003.03.07, 段落【0022】～【0076】 & US 2003/0046539 A1	1,2,4
A		3
Y	JP 11-196081 A (株式会社高度移動通信セキュリティ技術研究所) 1999.07.21, 段落【0002】～【0011】（ファミリーなし）	1,2,4,5
A		3

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日 １２．０２．２０１０	国際調査報告の発送日 ２３．０２．２０１０
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｓ　３８５７ 鳥居　稔 電話番号　０３－３５８１－１１０１　内線　３５４６

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	JP 2002-198957 A (ソニー株式会社) 2002.07.12, 段落【0257】～【0266】 & US 2002/0073229 A1	5
A	JP 2000-138674 A (松下電器産業株式会社) 2000.05.16, 段落【0044】 & EP 998073 A2	3
A	WO 2005/048008 A2 (M-SYSTEMS FLASH DISK PIONEERS LTD.) 2005.05.26, 第6頁第1行目～第6頁第3行目, 第8頁第20行目～第17頁第15行目 & EP 1692800 A	3