(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
2012 年 3 月 1 日(01.03.2012)

PCT

(10) 国際公開番号
WO 2012/025988 A1

(51) 国際特許分類:
H04L 9/14 (2006.01)

(21) 国際出願番号: PCT/JP2010/064238

(22) 国際出願日: 2010 年 8 月 24 日(24.08.2010)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (Mitsubishi Electric Corporation) [JP/JP]; 〒1008310 東京都千代田区丸の内二丁目７番３号 Tokyo (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 柴田 陽一 (SHIBATA, Yoichi) [—/JP]; 〒1008310 東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内 Tokyo (JP). 辻 宏郷 (TSUJI, Hirosato) [—/JP]; 〒1008310 東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内 Tokyo (JP). 松井 充 (MATSUI, Mitsuru) [—/JP]; 〒1008310 東京都千代田区丸の内二丁目７番３号 三菱電機株式会社内 Tokyo (JP).

(74) 代理人: 溝井 章司, 外 (MIZOI, Shoji et al.); 〒2470056 神奈川県鎌倉市大船二丁目１７番１０号 ＮＴＡ大船ビル３階 溝井国際特許事務所 Kanagawa (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, JP, 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, TH, 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, LR, 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 (AL, 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**: ENCRYPTION DEVICE, ENCRYPTION SYSTEM, ENCRYPTION METHOD AND ENCRYPTION PROGRAM

(54) 発明の名称 : 暗号化装置、暗号化システム、暗号化方法及び暗号化プログラム

[図4]

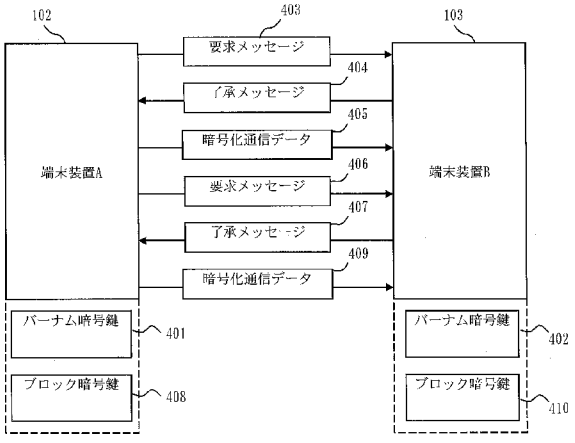


FIG. 4:
102, 103 TERMINAL DEVICE
401, 402 VERNAM ENCRYPTION KEY
403, 406 REQUEST MESSAGE
404, 407 ACKNOWLEDGEMENT MESSAGE
405, 409 ENCRYPTED COMMUNICATION DATA
408, 410 BLOCK ENCRYPTION KEY

(57) **Abstract**: The objective of the present invention is to make encrypted communication possible even if encryption keys for a one-time pad cipher (Vernam cipher) are insufficient. A one-time pad encryption unit encrypts communication data by way of a one-time pad cipher to generate encrypted data, using portions of a one-time pad encryption key stored in a one-time pad encryption key storage unit in order. A block encryption unit encrypts the communication data by way of a block cipher to generate encrypted data using a block encryption key stored in a block encryption key storage unit. An encryption control unit controls whether to encrypt the communication data with the one-time pad encryption unit or to encrypt with the block encryption unit depending upon the remaining number of bits of the one-time pad encryption key stored in the one-time pad encryption key storage unit.

(57) 要約: ワンタイムパッド暗号（バーナム暗号）の暗号鍵が不足した場合であっても、暗号通信を可能とすることを目的とする。ワンタイムパッド暗号化部は、ワンタイムパッド暗号鍵記憶部に記憶されたワンタイムパッド暗号鍵の一部を順に用いて、通信データをワンタイムパッド暗号により暗号化して暗号化データを生成する。ブロック暗号化部は、ブロック暗号鍵記憶部に記憶されたブロック暗号鍵を用いて、通信データをブロック暗号により暗号化して暗号化データを生成する。暗号化制御部は、ワンタイムパッド暗号鍵記憶部に記憶されたワンタイムパッド暗号鍵の残りビット数に応じて、通信データをワンタイムパッド暗号化部に暗号化させるか、ブロック暗号化部に暗号化させるかを制御する。

WO 2012/025988 A1

明　細　書

発明の名称 ：

暗号化装置、暗号化システム、暗号化方法及び暗号化プログラム

技術分野

[0001] この発明は、ワンタイムパッド暗号とブロック暗号とのどちらの暗号化方式で通信データを暗号化するかを制御する技術に関する。

背景技術

[0002] ワンタイムパッド暗号は、送信側と受信側とで鍵を共有する共通鍵暗号の一方式である。ワンタイムパッド暗号は、通信データと同量（同一ビット数）の暗号鍵を用いて暗号化を行う。また、ワンタイムパッド暗号は、一度暗号化に使用した暗号鍵を再利用せず、暗号鍵を使い捨てにする。

ワンタイムパッド暗号の典型的な例としては、通信データと暗号鍵とについて１ビットづつ排他的論理和等を計算して、計算した結果を暗号化通信データとするバーナム暗号がある。

[0003] ブロック暗号は、ワンタイムパッド暗号と同様に共通鍵暗号の一方式である。ブロック暗号は、データをブロックと呼ばれる単位（通常は固定長）に分割して、ブロック毎に暗号鍵を用いて暗号化を行う。通常、ブロック暗号では、複数のブロックを同じ暗号鍵で暗号化する。

ブロック暗号の例としては、Ｃａｍｅｌｌｉａ（登録商標）、ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）等がある。

[0004] ワンタイムパッド暗号による暗号通信においては、通信データと同量の暗号鍵を消費するため、多くの暗号鍵が必要となる。そして、ワンタイムパッド暗号では、暗号鍵が枯渇した場合に暗号通信を行うことができなくなる。

しかし、ワンタイムパッド暗号は、解読不可能であり、ブロック暗号よりも安全性が高いと言える。

[0005] 特許文献１には、暗号対象となる通信データの重要性によって、適用する暗号方式をワンタイムパッド暗号とブロック暗号とを使い分けることについ

ての記載がある。これにより、ワンタイムパッド暗号の暗号鍵の消費を軽減している。

[0006] 特許文献２には、端末装置毎の暗号鍵の蓄積量を監視し、蓄積量が少ない端末装置に対して優先的に暗号鍵を生成させることについての記載がある。これにより、特定の端末装置の暗号鍵が枯渇することの防止を図っている。

先行技術文献

特許文献

[0007] 特許文献1：特開２００７－２５８８５０号公報

特許文献2：特開２００８－３０６６３３号公報

発明の概要

発明が解決しようとする課題

[0008] 特許文献１に記載された方法は、通信データの重要性で適用する暗号方式を使い分け、ワンタイムパッド暗号の暗号鍵の消費を抑えている。しかし、特許文献１に記載された方法を適用したとしても、ワンタイムパッド暗号の暗号鍵が不足する場合が発生し、暗号通信を行うことができない場合が発生する虞がある。

また、通信データの重要性は主観的な基準であり、暗号化の対象となっている通信データの重要性は通信開始時、もしくは、事前に利用者又は管理者が判断しなければならない。そのため、通信データの入力が行われた時点から通信データが暗号化されるまでの間に利用者による重要性の判断が必要となり、暗号通信に関する処理のすべてを自動化することができない。

さらに、音声による通話中に重要な会話内容が含まれる場合などのように、通信データの種類によっては、重要性が事前に判断できないものもある。そのため、暗号対象の通信データの重要性を基準として暗号方式を切り替えることは、汎用的に有効な手段ではない。

[0009] 特許文献２に記載された方法では、端末装置が携帯端末といった、常時通信ができるものではない場合、不足した暗号鍵を補うことができない場合が

ある。したがって、暗号通信を行うことができない場合が発生する虞がある。

[0010] この発明は、ワンタイムパッド暗号の暗号鍵が不足した場合であっても、暗号通信を可能とすることを目的とする。

課題を解決するための手段

[0011] この発明に係る暗号化装置は、

ワンタイムパッド暗号で使用するワンタイムパッド暗号鍵を記憶するワンタイムパッド暗号鍵記憶部と、

前記ワンタイムパッド暗号鍵記憶部が記憶したワンタイムパッド暗号鍵の一部を順に用いて、通信データをワンタイムパッド暗号により暗号化して暗号化データを生成するワンタイムパッド暗号化部と、

ブロック暗号で使用するブロック暗号鍵を記憶するブロック暗号鍵記憶部と、

前記ブロック暗号鍵記憶部が記憶したブロック暗号鍵を用いて、通信データをブロック暗号により暗号化して暗号化データを生成するブロック暗号化部と、

前記ワンタイムパッド暗号鍵記憶部が記憶したワンタイムパッド暗号鍵の残りビット数に応じて、通信データを前記ワンタイムパッド暗号化部に暗号化させるか、前記ブロック暗号化部に暗号化させるかを制御する暗号化制御部と

を備えることを特徴とする。

発明の効果

[0012] この発明に係る暗号化装置は、ワンタイムパッド暗号鍵の残量に応じて、ワンタイムパッド暗号を使用するか、ブロック暗号を使用するかを制御する。そのため、ワンタイムパッド暗号鍵が不足した場合には、ブロック暗号で暗号通信を行うように制御することができ、ワンタイムパッド暗号の暗号鍵が不足した場合であっても、暗号通信が可能である。

図面の簡単な説明

[0013] [図1]実施の形態１に係る通信方式を適用可能な暗号化システム１の概略図。

[図2]鍵共有装置Ｃ１０４と鍵共有装置Ｄ１０５とが、ネットワーク１０１、もしくは、ネットワーク１０１とは物理的もしくは論理的に接続されていないネットワーク１０６を介して、バーナム暗号鍵の共有を行う場合の動作概要を示す図。

[図3]端末装置Ａ１０２が、通信ケーブル１０７を介して鍵共有装置Ｃ１０４からバーナム暗号鍵３０１を取得する場合の動作概要を示す図。

[図4]端末装置Ａ１０２と端末装置Ｂ１０３とがバーナム暗号による暗号通信を開始し、バーナム暗号用の暗号鍵が不足した時点からブロック暗号による暗号通信に方式の切り替えを行う場合の動作概要を示す図。

[図5]図４の通信処理の流れを示すフローチャート。

[図6]端末装置Ａ１０２と端末装置Ｂ１０３とが暗号通信を開始する時点で、バーナム暗号鍵が不足しているため、ブロック暗号による暗号通信を開始する場合の動作概要を示す図。

[図7]図６の通信処理の流れを示すフローチャート。

[図8]実施の形態１における端末装置Ａ１０２及び端末装置Ｂ１０３の機能構成を示す機能ブロック図。

[図9]端末装置８０１の送信制御部８０３の処理の流れを示すフローチャート。

[図10]端末装置８０１の受信制御部８０４の処理の流れを示すフローチャート。

[図11]実施の形態１における鍵共有装置Ｃ１０４及び鍵共有装置Ｄ１０５の機能構成を示す機能ブロック図。

[図12]鍵共有装置Ｃ１０４と鍵共有装置Ｄ１０５とがネットワーク１０１もしくはネットワーク１０６を介して、バーナム暗号鍵１２０１及びブロック暗号鍵１２０２の共有を行う場合の動作概要を示す図。

[図13]鍵共有装置Ｃ１０４から端末装置Ａ１０２が通信ケーブル１０７を介して、バーナム暗号鍵１３０１及びブロック暗号鍵１３０２を取得する場合

の動作概要を示す図。

[図14]実施の形態２における端末装置Ａ１０２及び端末装置Ｂ１０３の機能構成を示す機能ブロック図。

[図15]実施の形態２における鍵共有装置Ｃ１０４及び鍵共有装置Ｄ１０５の機能構成を説明する機能ブロック図。

[図16]端末装置Ａ１０２と端末装置Ｂ１０３とがバーナム暗号による暗号通信を開始し、バーナム暗号用の暗号鍵が不足した時点からブロック暗号による暗号通信に方式の切り替えを行う場合の動作概要を示す図。

[図17]図１６の通信処理の流れを示すフローチャート。

[図18]図１６の通信処理の流れを示すフローチャート。

[図19]端末装置Ａ１０２と端末装置Ｂ１０３が暗号通信を開始する時点で、バーナム暗号鍵が不足しているため、ブロック暗号による暗号通信を開始する場合の動作概要を示す図。

[図20]図１９の通信処理の流れを示すフローチャート。

[図21]実施の形態３における端末装置Ａ１０２及び端末装置Ｂ１０３の機能構成を示す機能ブロック図。

[図22]端末装置Ａ１０２と端末装置Ｂ１０３とがバーナム暗号による暗号通信を開始し、バーナム暗号用の暗号鍵が枯渇した時点からブロック暗号による暗号通信に方式の切り替えを行う場合の動作概要を示す図。

[図23]図２２の通信処理の流れを示すフローチャート。

[図24]図２２の通信処理の流れを示すフローチャート。

[図25]端末装置Ａ１０２と端末装置Ｂ１０３が暗号通信を開始する時点で、バーナム暗号鍵が枯渇しているため、ブロック暗号による暗号通信を開始する場合の動作概要を示す図。

[図26]図２５の通信処理の流れを示すフローチャート。

[図27]実施の形態４における端末装置Ａ１０２及び端末装置Ｂ１０３の機能構成を示す機能ブロック。

[図28]端末装置Ａ１０２と端末装置Ｂ１０３とが暗号通信を開始する時点で

、バーナム暗号鍵が不足しており、かつ、ブロック暗号鍵の残りが１つしかない場合の動作概要を示す図。

[図29]図２８の通信処理の流れを示すフローチャート。

[図30]実施の形態５における端末装置Ａ１０２及び端末装置Ｂ１０３の機能構成を説明する機能ブロック図。

[図31]端末装置Ａ１０２と端末装置Ｂ１０３とがバーナム暗号による暗号通信を開始し、バーナム暗号鍵の残量が事前に決められた量よりも少なくなった時点で、バーナム暗号鍵に増大処理を施す場合の動作概要を示す図。

[図32]図３１の通信処理の流れを示すフローチャート。

[図33]図３１の通信処理の流れを示すフローチャート。

[図34]図３１の通信処理の流れを示すフローチャート。

[図35]実施の形態６における端末装置Ａ１０２及び端末装置Ｂ１０３の機能構成を示す機能ブロック図。

[図36]実施の形態７におけるバーナム暗号鍵増大部８１９の処理を説明する図。

[図37]実施の形態８におけるバーナム暗号鍵増大部８１９の処理を説明する図。

[図38]実施の形態９における図４の通信処理の流れを示すフローチャート。

[図39]実施の形態９における図４の通信処理の流れを示すフローチャート。

[図40]実施の形態９において、端末装置Ａ１０２と端末装置Ｂ１０３が暗号通信を開始する時点で、端末装置Ｂ１０３のバーナム暗号鍵が不足しているため、ブロック暗号による暗号通信を開始する場合の動作概要を示す図。

[図41]図４０の通信処理の流れを示すフローチャート。

[図42]実施の形態９における端末装置８０１の送信制御部８０３の処理の流れを示すフローチャート。

[図43]実施の形態９における端末装置８０１の受信制御部８０４の処理の流れを示すフローチャート。

[図44]実施の形態１０における図２２の通信処理の流れを示すフローチャー

ト。

[図45]実施の形態１０における図２２の通信処理の流れを示すフローチャート。

[図46]実施の形態１０における図２５の通信処理の流れを示すフローチャート。

[図47]実施の形態１０における端末装置８０１の送信制御部８０３の処理の流れを示すフローチャート。

[図48]実施の形態１０における端末装置８０１の受信制御部８０４の処理の流れを示すフローチャート。

[図49]実施の形態１１における図２８の通信処理の流れを示すフローチャート。

[図50]実施の形態１１における端末装置８０１の送信制御部８０３の処理の流れを示すフローチャート。

[図51]実施の形態１１における端末装置８０１の受信制御部８０４の処理の流れを示すフローチャート。

[図52]実施の形態１２における端末装置の動作の説明図。

[図53]実施の形態１３における端末装置Ａ１０２及び端末装置Ｂ１０３の機能構成を説明する機能ブロック図。

[図54]端末装置８０１のハードウェア構成の一例を示す図。

発明を実施するための形態

[0014] 以下、図に基づき、発明の実施の形態を説明する。

以下の説明において、処理装置は後述するＣＰＵ９１１等である。記憶装置は後述するＲＯＭ９１３、ＲＡＭ９１４、磁気ディスク９２０等の記憶装置である。つまり、処理装置、記憶装置はハードウェアである。

[0015] 以下の説明では、ワンタイムパッド暗号の例として、バーナム暗号を用いて説明する。もちろん、他のワンタイムパッド暗号を用いても構わない。この場合、以下の説明におけるバーナム暗号をワンタイムパッド暗号と読み替えればよい。

[0016] 実施の形態１.

実施の形態１では、バーナム暗号用の暗号鍵（以下、バーナム暗号鍵）が枯渇した場合に、暗号方式をバーナム暗号からＣａｍｅｌｌｉａ（登録商標）、ＡＥＳといったブロック暗号に切り替える技術について説明する。これにより、バーナム暗号鍵が不足することによる暗号通信の中断を引き起こすことなく、バーナム暗号鍵が補充されるまでの期間においても、暗号通信の継続を可能にする。

[0017] 実施の形態１では、バーナム暗号鍵の残量（残りビット数）に応じて暗号方式を使い分ける。バーナム暗号鍵の残量は装置が容易に把握できる情報である。そのため、バーナム暗号鍵の残量を基準に暗号方式を切り替えることにより、装置を使用するユーザに暗号方式の切り替えに関する操作を求めることなく、自動で暗号方式を切り替える仕組みを実現することができる。

[0018] 図１は、実施の形態１に係る通信方式を適用可能な暗号化システム１の概略図である。

インターネットなどのネットワーク１０１には、端末装置Ａ１０２と端末装置Ｂ１０３とが接続される。また、鍵共有装置Ｃ１０４と鍵共有装置Ｄ１０５がネットワーク１０１、もしくは、ネットワーク１０１とは物理的もしくは論理的に接続されていないネットワーク１０６と接続される。さらに、端末装置Ａ１０２と鍵共有装置Ｃ１０４とは、ＵＳＢ（Ｕｎｉｖｅｒｓａｌ Ｓｅｒｉａｌ Ｂｕｓ）などの通信ケーブル１０７で接続されている。同様に、端末装置Ｂ１０３と鍵共有装置Ｄ１０５とは、通信ケーブル１０８で接続されている。

[0019] 以下では、鍵共有装置Ｃ１０４と鍵共有装置Ｄ１０５との間で共有されたバーナム暗号鍵を用いて、端末装置Ａ１０２と端末装置Ｂ１０３との間で暗号通信を行う例を説明する。

なお、端末装置Ａ１０２と端末装置Ｂ１０３とは、それぞれ、暗号化データを送信する送信側通信装置（暗号化装置）でもあり、暗号化データを受信する受信側通信装置（復号装置）でもある。以下では、端末装置Ａ１０２を

送信側通信装置の例とし、端末装置Ｂ１０３を受信側通信装置の例とする。

また、端末装置Ａ１０２は鍵共有装置Ｃ１０４からバーナム暗号鍵を取得し、端末装置Ｂ１０３は鍵共有装置Ｄ１０５からバーナム暗号鍵を取得するものとする。

[0020] まず、鍵共有装置同士によるバーナム暗号鍵の共有方法について説明する。

図２は、鍵共有装置Ｃ１０４と鍵共有装置Ｄ１０５とが、ネットワーク１０１、もしくは、ネットワーク１０１とは物理的もしくは論理的に接続されていないネットワーク１０６を介して、バーナム暗号鍵の共有を行う場合の動作概要を示す図である。

鍵共有装置Ｃ１０４と鍵共有装置Ｄ１０５とは、ネットワーク１０１もしくはネットワーク１０６を介して、所定の方法（鍵共有アルゴリズム）によりバーナム暗号鍵２０１を共有する。なお、バーナム暗号鍵２０１を共有する方法は、どのような方法であっても構わない。例えば、鍵共有装置Ｃ１０４と鍵共有装置Ｄ１０５とが、物理的もしくは論理的に安全な通信路で接続された上でバーナム暗号鍵２０１を共有すればよい。実施の形態１では、一例として、量子暗号通信による鍵共有が行われるものとする。

[0021] 次に、鍵共有装置から端末装置がバーナム暗号鍵を取得する場合の動作概要について説明する。

図３は、端末装置Ａ１０２が、通信ケーブル１０７を介して鍵共有装置Ｃ１０４からバーナム暗号鍵３０１を取得する場合の動作概要を示す図である。

まず、端末装置Ａ１０２は、バーナム暗号鍵要求メッセージ３０２を鍵共有装置Ｃ１０４へ送信する。鍵共有装置Ｃ１０４は、バーナム暗号鍵要求メッセージ３０２を受信した後、保有しているバーナム暗号鍵３０１を端末装置Ａ１０２へ送信する。バーナム暗号鍵３０１を受信した端末装置Ａ１０２は、バーナム暗号鍵３０１を記憶装置に記憶する。

なお、端末装置Ｂ１０３が、通信ケーブル１０８を介して鍵共有装置Ｄ１

０５からバーナム暗号鍵を取得する方法も同様である。

[0022] 次に、端末装置Ａ１０２と端末装置Ｂ１０３とがバーナム暗号による暗号通信を開始し、バーナム暗号用の暗号鍵が不足した時点からブロック暗号による暗号通信に方式の切り替えを行う場合の動作概要について説明する。

図４は、端末装置Ａ１０２と端末装置Ｂ１０３とがバーナム暗号による暗号通信を開始し、バーナム暗号用の暗号鍵が不足した時点からブロック暗号による暗号通信に方式の切り替えを行う場合の動作概要を示す図である。

なお、暗号通信の事前準備として、端末装置Ａ１０２はバーナム暗号用の暗号鍵４０１を保有している。また、端末装置Ｂ１０３もバーナム暗号鍵４０２を保有している。端末装置Ａ１０２が保有するバーナム暗号鍵４０１と、端末装置Ｂ１０３が保有するバーナム暗号鍵４０２とは、前述の方法により、それぞれ鍵共有装置Ｃ１０４と鍵共有装置Ｄ１０５から取得したものである。実施の形態１においては、バーナム暗号鍵４０１とバーナム暗号鍵４０２は、同一のものであるとする。

また、端末装置Ａ１０２はブロック暗号用のブロック暗号鍵４０８を保有している。また、端末装置Ｂ１０３もブロック暗号鍵４１０を保有している。端末装置Ａ１０２が保有するブロック暗号鍵４０８と、端末装置Ｂ１０３が保有するブロック暗号鍵４１０とは同一のものであるとする。端末装置Ａ１０２と端末装置Ｂ１０３との間におけるブロック暗号鍵の共有方法については、後の実施の形態で説明する。

[0023] まず、端末装置Ａ１０２は、保有しているバーナム暗号鍵４０１の残量を確認する。ここでは、バーナム暗号鍵４０１には残量があるものとする。そこで、端末装置Ａ１０２は、バーナム暗号鍵４０１の残量に基づき、バーナム暗号を行うことができるデータ通信量を算出する。そして、端末装置Ａ１０２は、バーナム暗号通信要求メッセージ４０３を端末装置Ｂ１０３へ送信する。

バーナム暗号通信要求メッセージ４０３を受信した端末装置Ｂ１０３は、保有しているバーナム暗号鍵４０２の残量を確認する。ここでは、バーナム

暗号鍵４０２には、バーナム暗号鍵４０１と同じ残量があるものとする。そこで、端末装置Ｂ１０３は、バーナム暗号鍵４０２の残量に基づき、バーナム暗号を行うことができるデータ通信量を算出する。そして、端末装置Ｂ１０３は、バーナム暗号通信了承メッセージ４０４を端末装置Ａ１０２へ送信する。

バーナム暗号通信了承メッセージ４０４を受信した端末装置Ａ１０２は、バーナム暗号鍵４０１を用いて、通信データにバーナム暗号による暗号化を施し、暗号化通信データ４０５を生成する。そして、端末装置Ａ１０２は、生成した暗号化通信データ４０５を端末装置Ｂ１０３へ送信する。

暗号化通信データ４０５を受信した端末装置Ｂ１０３は、バーナム暗号鍵４０２で暗号化通信データ４０５を復号し、通信データを得る。なお、バーナム暗号鍵４０１とバーナム暗号鍵４０２とは、同一であるため、バーナム暗号鍵４０１で暗号化された暗号化通信データ４０５は、バーナム暗号鍵４０２で復号可能である。

[0024] もし、端末装置Ａ１０２における暗号化通信データ４０５の生成時にバーナム暗号を行うことができるデータ通信量を超えて、暗号化を行う必要がある場合、端末装置Ａ１０２はブロック暗号切替要求メッセージ４０６を端末装置Ｂ１０３へ送信する。

ブロック暗号切替要求メッセージ４０６を受信した端末装置Ｂ１０３は、ブロック暗号切替了承メッセージ４０７を端末装置Ａ１０２へ送信する。

ブロック暗号切替了承メッセージ４０７を受信した端末装置Ａ１０２は、通信データをブロック暗号鍵４０８で暗号化し、暗号化通信データ４０９を生成する。そして、端末装置Ａ１０２は、生成した暗号化通信データ４０９を端末装置Ｂ１０３へ送信する。

暗号化通信データ４０９を受信した端末装置Ｂ１０３は、ブロック暗号鍵４１０で暗号化通信データ４０９を復号し、通信データを得る。なお、ブロック暗号鍵４０８とブロック暗号鍵４１０とは、同一であるため、ブロック暗号鍵４０８で暗号化された暗号化通信データ４０９は、ブロック暗号鍵４

１０で復号可能である。

[0025] 次に、図４の通信処理について詳しく説明する。図５は、図４の通信処理の流れを示すフローチャートである。

[0026] 端末装置Ａ１０２は、保有しているバーナム暗号鍵４０１の量（ビット数）を確認し、バーナム暗号で暗号通信を行うことができるデータ量を算出する（Ｓ１０１）。そして、端末装置Ａ１０２は、バーナム暗号通信要求メッセージ４０３を端末装置Ｂ１０３へ送信する（Ｓ１０２）。

端末装置Ｂ１０３は、端末装置Ａ１０２からバーナム暗号通信要求メッセージ４０３を受信する（Ｓ１０３）。すると、端末装置Ｂ１０３は、保有しているバーナム暗号鍵４０２の量を確認し、バーナム暗号で暗号通信を行うことができるデータ量を算出する（Ｓ１０４）。そして、端末装置Ｂ１０３は、バーナム暗号通信了承メッセージ４０４を端末装置Ａ１０２へ送信する（Ｓ１０５）。

端末装置Ａ１０２は、端末装置Ｂ１０３からバーナム暗号通信了承メッセージ４０４を受信する（Ｓ１０６）。すると、端末装置Ａ１０２は、通信データのうち単位データ量分のデータをバーナム暗号鍵４０１で暗号化して、暗号化通信データ４０５を生成する。（Ｓ１０７）。なお、単位データ量分のデータとは、予め決められたビット数のデータである。あるいは、予め決められた単位のデータ、例えば、１ファイルのデータ等である。また、例えば、携帯電話における音声通話データの場合であれば、１０～２０ミリ秒程度の短い時間毎の音声通話データである。そして、端末装置Ａ１０２は、暗号化通信データ４０５を端末装置Ｂ１０３へ送信する（Ｓ１０８）。

端末装置Ｂ１０３は、端末装置Ａ１０２から暗号化通信データ４０５を受信する（Ｓ１０９）。すると、端末装置Ｂ１０３は、バーナム暗号鍵４０２で暗号化通信データ４０５を復号し、通信データを得る（Ｓ１１０）。

[0027] 続いて、端末装置Ａ１０２は、未送信の通信データの有無を確認する（Ｓ１１１）。未送信の通信データがなければ（Ｓ１１１でＮＯ）、端末装置Ａ１０２は処理を終了する（Ｓ１１２）。一方、未送信の通信データがあれば

（Ｓ１１１でＹＥＳ）、端末装置Ａ１０２はＳ１１３へ処理を進める。

[0028] 端末装置Ａ１０２は、バーナム暗号で暗号通信を行うことができるデータ量が、１度に暗号化する単位データ量以上かを確認する（Ｓ１１３）。この際、端末装置Ａ１０２は、Ｓ１０１で算出した、バーナム暗号で暗号通信を行うことができるデータ量から、これまでに端末装置Ｂ１０３へ暗号化通信データを送信した通信データのデータ量を減算して、現時点でバーナム暗号で暗号通信を行うことができるデータ量を算出する。

バーナム暗号で暗号通信を行うことができるデータ量が単位データ量以上であれば（Ｓ１１３でＹＥＳ）、端末装置Ａ１０２はＳ１０７へ処理を戻す。一方、バーナム暗号で暗号通信を行うことができるデータ量が単位データ量未満であれば（Ｓ１１３でＮＯ）、端末装置Ａ１０２はブロック暗号切替要求メッセージ４０６を端末装置Ｂ１０３へ送信する（Ｓ１１４）。

[0029] 端末装置Ｂ１０３は、ブロック暗号切替要求メッセージ４０６を受信する。（Ｓ１１５）。すると、端末装置Ｂ１０３は、ブロック暗号切替了承メッセージ４０７を端末装置Ａ１０２へ送信する（Ｓ１１６）。

端末装置Ａ１０２は、ブロック暗号切替了承メッセージ４０７を受信する（Ｓ１１７）。すると、端末装置Ａ１０２は、通信データのうち単位データ量分のデータをブロック暗号鍵４０８で暗号化して、暗号化通信データ４０９を生成する（Ｓ１１８）。そして、端末装置Ａ１０２は、暗号化通信データ４０９を端末装置Ｂ１０３へ送信する（Ｓ１１９）。

端末装置Ｂ１０３は、暗号化通信データ４０９を受信する（Ｓ１２０）。すると、端末装置Ｂ１０３は、ブロック暗号鍵４１０で暗号化通信データ４０９を復号し、通信データを得る（Ｓ１２１）。

[0030] 続いて、端末装置Ａ１０２は、未送信の通信データの有無を確認する（Ｓ１２２）。未送信の通信データがなければ（Ｓ１２２でＮＯ）、端末装置Ａ１０２は処理を終了する（Ｓ１２３）。一方、未送信の通信データがあれば（Ｓ１２２でＹＥＳ）、端末装置Ａ１０２はＳ１１８へ処理を戻す。

[0031] 次に、通信開始時点でバーナム暗号鍵が不足しており、バーナム暗号によ

る暗号通信が開始できない時に、ブロック暗号による暗号通信を開始する場合の動作概要について説明する。

図６は、端末装置Ａ１０２と端末装置Ｂ１０３とが暗号通信を開始する時点で、バーナム暗号鍵が不足しているため、ブロック暗号による暗号通信を開始する場合の動作概要を示す図である。

なお、端末装置Ａ１０２はブロック暗号用のブロック暗号鍵６０３を保有している。また、端末装置Ｂ１０３もブロック暗号鍵６０５を保有している。端末装置Ａ１０２が保有するブロック暗号鍵６０３と、端末装置Ｂ１０３が保有するブロック暗号鍵６０５とは同一のものであるとする。端末装置Ａ１０２と端末装置Ｂ１０３との間におけるブロック暗号鍵の共有方法については、後の実施の形態で説明する。

[0032] まず、端末装置Ａ１０２は、保有しているバーナム暗号鍵の量を確認する。ここでは、バーナム暗号鍵が枯渇している（０ビットである）とする。そこで、端末装置Ａ１０２は、ブロック暗号通信要求メッセージ６０１を端末装置Ｂ１０３へ送信する。

ブロック暗号通信要求メッセージ６０１を受信した端末装置Ｂ１０３は、ブロック暗号通信了承メッセージ６０２を端末装置Ａ１０２へ送信する。

ブロック暗号通信了承メッセージ６０２を受信した端末装置Ａ１０２は、ブロック暗号鍵６０３を用いて、通信データにブロック暗号による暗号化を施し、暗号化通信データ６０４を生成する。そして、端末装置Ａ１０２は、生成した暗号化通信データ６０４を端末装置Ｂ１０３へ送信する。

暗号化通信データ６０４を受信した端末装置Ｂ１０３は、ブロック暗号鍵６０５で暗号化通信データ６０４を復号し、通信データを得る。なお、ブロック暗号鍵６０３とブロック暗号鍵６０５とは、同一であるため、ブロック暗号鍵６０３で暗号化された暗号化通信データ６０４は、ブロック暗号鍵６０５で復号可能である。

[0033] 次に、図６の通信処理について詳しく説明する。図７は、図６の通信処理の流れを示すフローチャートである。

[0034] 端末装置Ａ１０２は、保有しているバーナム暗号鍵の量を確認し、バーナム暗号鍵が不足していることを把握する（Ｓ２０１）。なお、バーナム暗号で暗号通信を行うことができるデータ量が、１度に暗号化する単位データ量未満である場合に、バーナム暗号鍵が不足していると判定する。そして、端末装置Ａ１０２は、ブロック暗号通信要求メッセージ６０１を端末装置Ｂ１０３へ送信する（Ｓ２０２）。

端末装置Ｂ１０３は、端末装置Ａ１０２からブロック暗号通信要求メッセージ６０１を受信する（Ｓ２０３）。そして、端末装置Ｂ１０３は、ブロック暗号通信了承メッセージ６０２を端末装置Ａ１０２へ送信する（Ｓ２０４）。

端末装置Ａ１０２は、端末装置Ｂ１０３からブロック暗号通信了承メッセージ６０２を受信する（Ｓ２０５）。すると、端末装置Ａ１０２は、通信データのうち単位データ量分のデータをブロック暗号鍵６０３で暗号化して、暗号化通信データ６０４を生成する（Ｓ２０６）。そして、端末装置Ａ１０２は、暗号化通信データ６０４を端末装置Ｂ１０３へ送信する（Ｓ２０７）。

端末装置Ｂ１０３は、暗号化通信データ６０４を受信する（Ｓ２０８）。すると、端末装置Ｂ１０３は、ブロック暗号鍵６０５で暗号化通信データ６０４を復号し、通信データを得る（Ｓ２０９）。

[0035] 続いて、端末装置Ａ１０２は、未送信の通信データの有無を確認する（Ｓ２１０）。未送信の通信データがなければ（Ｓ２１０でＮＯ）、端末装置Ａ１０２は処理を終了する（Ｓ２１１）。一方、未送信の通信データがあれば（Ｓ２１０でＹＥＳ）、端末装置Ａ１０２はＳ２０６へ処理を戻す。

[0036] 次に、実施の形態１における端末装置Ａ１０２及び端末装置Ｂ１０３の機能について説明する。

図８は、実施の形態１における端末装置Ａ１０２及び端末装置Ｂ１０３の機能構成を示す機能ブロック図である。ここで、端末装置Ａ１０２と端末装置Ｂ１０３とは、同一の機能構成である。そこで、ここでは、端末装置Ａ１

０２と端末装置Ｂ１０３とを端末装置８０１として説明する。

端末装置８０１は、通信インターフェイス８０２、送信制御部８０３（暗号化制御部）、受信制御部８０４（復号制御部）、バーナム暗号鍵管理部８０５、バーナム暗号化部８０６、バーナム復号部８０７、ブロック暗号化部８０８、ブロック復号部８０９、バーナム暗号鍵取得部８１０、送信データ記憶部８１１、受信データ記憶部８１２、バーナム暗号鍵記憶部８１３（バーナム復号鍵記憶部）及びブロック暗号鍵記憶部８１４（ブロック復号鍵記憶部）を備える。

[0037] 通信インターフェイス８０２は、外部装置と通信を行う通信装置である。

より具体的には、通信インターフェイス８０２は、鍵共有装置Ｃ１０４や鍵共有装置Ｄ１０５からバーナム暗号鍵を受信するための装置である。

また、通信インターフェイス８０２は、端末装置８０１が暗号通信の送信側である場合は受信側となる端末装置に暗号化通信データを送信し、通信インターフェイス８０２暗号通信の受信側である場合は送信側となる端末装置から暗号化通信データを受信するための装置である。

[0038] 送信制御部８０３は、バーナム暗号鍵管理部８０５から得られるバーナム暗号鍵の残量情報を参照し、バーナム暗号化部８０６とブロック暗号化部８０８とのどちらに通信データの暗号化をさせるかを処理装置により制御する。また、送信制御部８０３は、バーナム暗号化部８０６又はブロック暗号化部８０８に暗号化させ、得られた暗号化通信データを送信する。

[0039] 受信制御部８０４は、暗号化通信データを受信する。そして、受信制御部８０４は、バーナム暗号鍵管理部８０５から得られるバーナム鍵の残量情報を参照して、受信した暗号化通信データに対する復号をバーナム復号部８０７とブロック復号部８０９とのどちらに復号させるかを処理装置により制御する。

[0040] バーナム暗号鍵管理部８０５は、バーナム暗号鍵記憶部８１３が記憶するバーナム暗号鍵の残量に関する情報を送信制御部８０３や受信制御部８０４に提供する。より具体的には、バーナム暗号鍵管理部８０５は、バーナム暗

号鍵の残量が不足しているか否かを示す情報を提供する。

なお、バーナム暗号鍵管理部８０５は、バーナム暗号で暗号通信を行うことができるデータ量が、１度に暗号化する単位データ量未満である場合に、バーナム暗号鍵が不足していると判定する。

[0041] バーナム暗号化部８０６は、送信データ記憶部８１１から通信データを取得し、バーナム暗号鍵記憶部８１３からバーナム暗号鍵を取得する。そして、バーナム暗号化部８０６は、処理装置によりバーナム暗号鍵を用いたバーナム暗号を通信データに施し、暗号化通信データを生成する。得られた暗号化通信データは送信制御部８０３に渡される。

[0042] バーナム復号部８０７は、バーナム暗号鍵記憶部８１３からバーナム暗号鍵を取得し、受信制御部８０４から暗号化通信データを取得する。そして、バーナム復号部８０７は、処理装置によりバーナム暗号鍵を用いて暗号化通信データを復号し、通信データを生成する。得られた通信データは受信データ記憶部８１２に記憶される。

[0043] ブロック暗号化部８０８は、送信データ記憶部８１１から通信データを取得し、ブロック暗号鍵記憶部８１４からブロック暗号鍵を取得する。そして、ブロック暗号化部８０８は、処理装置によりブロック暗号鍵を用いたブロック暗号を通信データに施し、暗号化通信データを生成する。得られた暗号化通信データは送信制御部８０３に渡される。

[0044] ブロック復号部８０９は、ブロック暗号鍵記憶部８１４からブロック暗号鍵を取得し、受信制御部８０４から暗号化通信データを取得する。そして、ブロック復号部８０９は、処理装置によりブロック暗号鍵を用いて暗号化通信データを復号し、通信データを生成する。得られた通信データは受信データ記憶部８１２に記憶される。

[0045] バーナム暗号鍵取得部８１０は、鍵共有装置Ｃ１０４や鍵共有装置Ｄ１０５等の鍵共有装置からバーナム暗号鍵を取得し、得られたバーナム暗号鍵をバーナム暗号鍵記憶部８１３に記憶する。

[0046] 送信データ記憶部８１１は、受信側となる端末装置へ送信する通信データ

を記憶する記憶装置である。

[0047] 受信データ記憶部８１２は、送信側となる端末装置から取得した通信データを記憶する記憶装置である。

[0048] バーナム暗号鍵記憶部８１３は、バーナム暗号鍵を記憶する記憶装置である。

[0049] ブロック暗号鍵記憶部８１４は、ブロック暗号鍵を記憶する記憶装置である。

[0050] 次に、送信側の端末装置である端末装置Ａ１０２の処理について詳しく説明する。

図９は、端末装置８０１の送信制御部８０３の処理の流れを示すフローチャートである。

[0051] 送信制御部８０３は、バーナム暗号鍵管理部８０５からバーナム暗号鍵の残量が不足しているか否かを示す残量情報を取得する（Ｓ３０１）。そして、送信制御部８０３は、バーナム暗号鍵の残量が不足していなければ（Ｓ３０２でＮＯ）、Ｓ３０３に処理を進め、残量が不足していれば（Ｓ３０２でＹＥＳ）、Ｓ３１１に処理を進める（Ｓ３０２）。

[0052] Ｓ３０３～Ｓ３１０の処理について説明する。

送信制御部８０３は、通信インターフェイス８０２を介して、バーナム暗号通信要求メッセージを端末装置Ｂ１０３へ送信し（Ｓ３０３）、端末装置Ｂ１０３からバーナム暗号通信了承メッセージを受信する（Ｓ３０４）。そして、送信制御部８０３は、バーナム暗号化部８０６に通信データのうち単位データ量分のデータを暗号化させ、暗号化通信データを取得する（Ｓ３０５）。送信制御部８０３は、取得した暗号化通信データを通信インターフェイス８０２を解して端末装置Ｂ１０３へ送信する（Ｓ３０６）。

[0053] 続いて、送信制御部８０３は、未送信の通信データの有無を確認する（Ｓ３０７）。未送信の通信データがなければ（Ｓ３０７でＮＯ）、送信制御部８０３は処理を終了する。一方、未送信の通信データがあれば（Ｓ３０７でＹＥＳ）、送信制御部８０３はＳ３０８へ処理を進める。

[0054] 送信制御部８０３は、バーナム暗号鍵管理部８０５からバーナム暗号鍵の残量が不足しているか否かを示す残量情報を取得して、バーナム暗号による暗号通信が継続可能であるか否かを判定する（Ｓ３０８）。継続可能であれば（Ｓ３０８でＹＥＳ）、送信制御部８０３はＳ３０５へ処理を戻す。一方、継続不可能であれば（Ｓ３０８でＮＯ）、送信制御部８０３はＳ３０９へ処理を進める。

[0055] 送信制御部８０３は、通信インターフェイス８０２を介して、ブロック暗号切替要求メッセージを端末装置Ｂ１０３に送信し（Ｓ３０９）、端末装置Ｂ１０３からブロック暗号切替了承メッセージを受信し（Ｓ３１０）、Ｓ３１３に処理を進める。

[0056] Ｓ３１１～３１２の処理について説明する。

送信制御部８０３は、ブロック暗号通信要求メッセージを端末装置Ｂ１０３に送信し（Ｓ３１１）、端末装置Ｂ１０３からブロック暗号通信了承メッセージを受信し（Ｓ３１２）、Ｓ３１３に処理を進める。

[0057] Ｓ３１３以降の処理について説明する。

送信制御部８０３は、ブロック暗号化部８０８に通信データのうち単位データ量分のデータを暗号化させ、暗号化通信データを取得する（Ｓ３１３）。そして、送信制御部８０３は、暗号化通信データを端末装置Ｂ１０３へ送信する（Ｓ３１４）。

続いて、送信制御部８０３は、未送信の通信データの有無を確認する（Ｓ３１５）。未送信の通信データがなければ（Ｓ３１５でＮＯ）、送信制御部８０３は処理を終了する。一方、未送信の通信データがあれば（Ｓ３１５でＹＥＳ）、送信制御部８０３はＳ３１３へ処理を戻す。

[0058] 次に、受信側の端末装置である端末装置Ｂ１０３の処理について詳しく説明する。

図１０は、端末装置８０１の受信制御部８０４の処理の流れを示すフローチャートである。

[0059] 受信制御部８０４は、バーナム暗号通信要求メッセージ、又は、ブロック

暗号通信要求メッセージを端末装置Ａ１０２から通信インターフェイス８０２を介して受信する（Ｓ４０１）。受信制御部８０４は、バーナム暗号要求メッセージを受信した場合はＳ４０３に処理を進め、ブロック暗号要求メッセージを受信した場合はＳ４１０に処理を進める（Ｓ４０２）。

[0060] Ｓ４０３～４０９の処理について説明する。

受信制御部８０４は、通信インターフェイス８０２を介して、バーナム暗号了承メッセージを端末装置Ａ１０２へ送信し（Ｓ４０３）、端末装置Ａ１０２から暗号化通信データを受信する（Ｓ４０４）。受信制御部８０４は、受信した暗号化通信データをバーナム復号部８０７に送信して、復号させ通信データを生成させる（Ｓ４０５）。生成された通信データは、受信データ記憶部８１２に記憶される。

[0061] 続いて、受信制御部８０４は、未受信の通信データの有無を確認する（Ｓ４０６）。未受信の通信データがなければ（Ｓ４０６でＮＯ）、受信制御部８０４は処理を終了する。一方、未受信の通信データがあれば（Ｓ４０６でＹＥＳ）、受信制御部８０４はＳ４０７へ処理を進める。

なお、未受信の通信データがあるか否かは、例えば、所定の時間内に次の暗号化データ、又は、ブロック暗号切替要求メッセージが送信されているかによって判定される。

[0062] 受信制御部８０４は、バーナム暗号鍵管理部８０５からバーナム暗号鍵の残量が不足しているか否かを示す残量情報を取得して、バーナム暗号による暗号通信が継続可能であるか否かを判定する（Ｓ４０７）。継続可能であれば（Ｓ４０７でＹＥＳ）、受信制御部８０４はＳ４０４へ処理を戻す。一方、継続不可能であれば（Ｓ４０７でＮＯ）、受信制御部８０４はＳ４０８へ処理を進める。

[0063] 受信制御部８０４は、端末装置Ａ１０２からブロック暗号切替要求メッセージを受信し（Ｓ４０８）、ブロック暗号切替了承メッセージを端末装置Ａ１０２に送信し（Ｓ４０９）、Ｓ４１１に処理を進める。

[0064] Ｓ４１０の処理について説明する。

受信制御部８０４は、ブロック暗号通信了承メッセージを端末装置Ａ１０２に送信し（Ｓ４１０）、Ｓ４１１に処理を進める。

[0065] Ｓ４１１以降の処理について説明する。

受信制御部８０４は、端末装置Ａ１０２から暗号化通信データを受信する（Ｓ４１１）。受信制御部８０４は、受信した暗号化通信データをブロック復号部８０９に送信して、復号させ通信データを生成させる（Ｓ４１２）。生成された通信データは、受信データ記憶部８１２に記憶される。

続いて、受信制御部８０４は、未送信の通信データの有無を確認する（Ｓ４１３）。未送信の通信データがなければ（Ｓ４１３でＮＯ）、受信制御部８０４は処理を終了する。一方、未送信の通信データがあれば（Ｓ４１３でＹＥＳ）、受信制御部８０４はＳ４１１へ処理を戻す。

[0066] なお、上記説明では、Ｓ４０７で受信制御部８０４がバーナム暗号による暗号通信が継続可能であるか否かを判定し、バーナム暗号による暗号通信を継続するか、ブロック暗号による暗号通信に切り替えるかを決定した。しかし、受信制御部８０４は、バーナム暗号による暗号通信が継続可能であるか否かを判定せず、端末装置Ａ１０２からブロック暗号切替要求メッセージを受信したか否かにより、バーナム暗号による暗号通信を継続するか、ブロック暗号による暗号通信に切り替えるかを決定してもよい。

[0067] 次に、実施の形態１における鍵共有装置Ｃ１０４及び鍵共有装置Ｄ１０５の機能について説明する。

図１１は、実施の形態１における鍵共有装置Ｃ１０４及び鍵共有装置Ｄ１０５の機能構成を示す機能ブロック図である。ここで、鍵共有装置Ｃ１０４と鍵共有装置Ｄ１０５とは、同一の機能構成である。そこで、ここでは、鍵共有装置Ｃ１０４と鍵共有装置Ｄ１０５とを鍵共有装置１１０１として説明する。

鍵共有装置１１０１は、通信インターフェイス１１０２、バーナム暗号鍵共有部１１０３、バーナム暗号鍵転送部１１０４及びバーナム暗号鍵記憶部１１０５を備える。

[0068] 通信インターフェイス１１０２は、外部装置と通信を行う通信装置である。

より具体的には、通信インターフェイス１１０２は、他の鍵共有装置とバーナム暗号鍵を共有するための通信を行うための装置である。

また、通信ケーブル等で接続されている端末装置に、バーナム暗号鍵を送信するための装置である。

[0069] バーナム暗号鍵共有部１１０３は、他の鍵共有装置と通信を行い、バーナム暗号鍵を共有し、共有したバーナム暗号鍵をバーナム暗号鍵記憶部１１０５に記憶する。

[0070] バーナム暗号鍵転送部１１０４は、バーナム暗号鍵記憶部１１０５からバーナム暗号鍵を取得し、端末装置へ送信する。

[0071] バーナム暗号鍵記憶部１１０５は、他の鍵共有装置との通信により得られたバーナム暗号鍵を記憶する記憶装置である。

[0072] 以上のように、実施の形態１に係る暗号化システム１では、２者間で行われているバーナム暗号による暗号通信において、バーナム暗号鍵の不足を検知する。これにより、暗号通信中もしくは暗号通信開始時にバーナム暗号鍵が不足した場合であっても、バーナム暗号による暗号通信からブロック暗号による暗号通信に切り替え、暗号通信を継続することができる。

[0073] また、実施の形態１では、バーナム暗号による暗号通信からブロック暗号による暗号通信への切り替えをバーナム暗号鍵の不足時に行っている。バーナム暗号鍵の不足は装置内で検知できるものであるため、端末装置Ａ１０２、端末装置Ｂ１０３の利用者の判断や処理を必要としないで、暗号通信の切り替えを実現することが可能である。

[0074] なお、ブロック暗号による暗号通信を行っている場合に、端末装置Ａ１０２や端末装置Ｂ１０３が鍵共有装置Ｃ１０４や鍵共有装置Ｄ１０５からバーナム暗号鍵を取得して、再びバーナム暗号鍵の残りビット数が所定のビット数以上になることが考えられる。この場合、端末装置Ａ１０２と端末装置Ｂ１０３とは、ブロック暗号による暗号通信からバーナム暗号による暗号通信

へ切り替えてもよい。

[0075] 実施の形態２.

実施の形態２では、ブロック暗号鍵の共有方法について説明する。実施の形態２では、実施の形態１において、端末装置Ａ１０２及び端末装置Ｂ１０３が鍵共有装置Ｃ１０４及び鍵共有装置Ｄ１０５からバーナム暗号鍵を取得する際に、併せてブロック暗号鍵も同時に取得する。これにより、ブロック暗号鍵についても端末装置間で安全に共有する。

[0076] まず、鍵共有装置同士によるバーナム暗号鍵及びブロック暗号鍵の共有方法について説明する。

図１２は、鍵共有装置Ｃ１０４と鍵共有装置Ｄ１０５とがネットワーク１０１もしくはネットワーク１０６を介して、バーナム暗号鍵１２０１及びブロック暗号鍵１２０２の共有を行う場合の動作概要を示す図である。

鍵共有装置Ｃ１０４と鍵共有装置Ｄ１０５とは、ネットワーク１０１もしくはネットワーク１０６を介して、所定の方法（鍵共有アルゴリズム）によりバーナム暗号鍵１２０１及びブロック暗号鍵１２０２を共有する。なお、バーナム暗号鍵１２０１及びブロック暗号鍵１２０２を共有する方法は、どのような方法であっても構わない。例えば、鍵共有装置Ｃ１０４と鍵共有装置Ｄ１０５とが、物理的もしくは論理的に安全な通信路で接続された上でバーナム暗号鍵１２０１及びブロック暗号鍵１２０２を共有すればよい。実施の形態２では、一例として、量子暗号通信による鍵共有が行われるものとする。

[0077] 次に、鍵共有装置から端末装置がバーナム暗号鍵及びブロック暗号鍵を取得する場合の動作概要について説明する。

図１３は、鍵共有装置Ｃ１０４から端末装置Ａ１０２が通信ケーブル１０７を介して、バーナム暗号鍵１３０１及びブロック暗号鍵１３０２を取得する場合の動作概要を示す図である。

まず、端末装置Ａ１０２は、暗号鍵要求メッセージ１３０３を鍵共有装置Ｃ１０４へ送信する。鍵共有装置Ｃ１０４は、暗号鍵要求メッセージ１３０

３を受信した後、保有しているバーナム暗号鍵１３０１及びブロック暗号鍵１３０２を端末装置Ａ１０２へ送信する。バーナム暗号鍵１３０１及びブロック暗号鍵１３０２を受信した端末装置Ａ１０２は、バーナム暗号鍵１３０１及びブロック暗号鍵１３０２を記憶する。

なお、端末装置Ｂ１０３が、通信ケーブル１０８を介して鍵共有装置Ｄ１０５からバーナム暗号鍵及びブロック暗号鍵を取得する方法も同様である。

[0078] 次に、実施の形態２における端末装置Ａ１０２及び端末装置Ｂ１０３の機能について説明する。

図１４は、実施の形態２における端末装置Ａ１０２及び端末装置Ｂ１０３の機能構成を示す機能ブロック図である。図１４に示す端末装置は、図８に示す端末装置が備える機能に加え、ブロック暗号鍵取得部８１５を備える。

[0079] ブロック暗号鍵取得部８１５は、鍵共有装置Ｃ１０４や鍵共有装置Ｄ１０５等の鍵共有装置からブロック暗号鍵を取得し、得られたブロック暗号鍵をブロック暗号鍵記憶部８１４に記憶する。

[0080] 次に、実施の形態２における鍵共有装置Ｃ１０４及び鍵共有装置Ｄ１０５の機能について説明する。

図１５は、実施の形態２における鍵共有装置Ｃ１０４及び鍵共有装置Ｄ１０５の機能構成を説明する機能ブロック図である。図１５に示す鍵共有装置は、図１１に示す鍵共有装置が備える機能に加え、ブロック暗号鍵共有部１１０６、ブロック暗号鍵転送部１１０７及びブロック暗号鍵記憶部１１０８を備える。

[0081] ブロック暗号鍵共有部１１０６は、他の鍵共有装置と通信を行い、ブロック暗号鍵を共有し、共有したブロック暗号鍵をブロック暗号鍵記憶部１１０８に記憶する。

[0082] ブロック暗号鍵転送部１１０７はブロック暗号鍵記憶部１１０８からブロック暗号鍵を取得し、端末装置へ送信する。

[0083] ブロック暗号鍵記憶部１１０８は他の鍵共有装置との通信により得られたブロック暗号鍵を記憶する記憶装置である。

[0084] 以上のように、実施の形態２に係る暗号化システム１では、鍵共有装置Ｃ１０４と鍵共有装置Ｄ１０５とで、バーナム暗号鍵とともにブロック暗号鍵も共有する。そして、端末装置Ａ１０２と端末装置Ｂ１０３とが、鍵共有装置Ｃ１０４と鍵共有装置Ｄ１０５とのそれぞれからバーナム暗号鍵とともにブロック暗号鍵も取得する。これにより、ブロック暗号鍵についても端末装置間で安全に共有する。

[0085] 実施の形態３.

実施の形態３では、バーナム暗号鍵の残量が所定の量よりも少なくなった時点で、残存するバーナム暗号鍵からブロック暗号鍵を生成することについて説明する。これにより、事前にブロック暗号鍵を端末装置間で共有していなくても、バーナム暗号鍵の不足時にブロック暗号による暗号通信に切り替えることを可能とする。

そこで、実施の形態３においては、端末装置Ａ１０２と端末装置Ｂ１０３とは、暗号通信開始時、バーナム暗号鍵のみを共有しており、ブロック暗号鍵は保持していないものとする。

なお、ここでは、バーナム暗号鍵が不足した時点において、バーナム暗号鍵はブロック暗号鍵の生成に必要となる量が残っているものとして説明する。

[0086] まず、実施の形態３において、端末装置同士がバーナム暗号による暗号通信を開始し、バーナム暗号用の暗号鍵が不足した時点からブロック暗号による暗号通信に方式の切り替えを行う場合の動作概要について説明する。

図１６は、端末装置Ａ１０２と端末装置Ｂ１０３とがバーナム暗号による暗号通信を開始し、バーナム暗号用の暗号鍵が不足した時点からブロック暗号による暗号通信に方式の切り替えを行う場合の動作概要を示す図である。図１６に示す処理では、実施の形態１における図４の処理に加えて、バーナム暗号鍵からブロック暗号鍵を生成する処理が行われる。

なお、暗号通信の事前準備として、端末装置Ａ１０２はバーナム暗号用のバーナム暗号鍵１６０１を保有している。また、端末装置Ｂ１０３もバーナ

ム暗号鍵１６０２を保有している。端末装置Ａ１０２が保有するバーナム暗号鍵１６０１と端末装置Ｂ１０３が保有するバーナム暗号鍵１６０２は、前述の方法により、それぞれ鍵共有装置Ｃ１０４と鍵共有装置Ｄ１０５から取得したものである。実施の形態３においては、バーナム暗号鍵１６０１とバーナム暗号鍵１６０２とは、同一のものであるとする。

また、暗号通信前の時点で、端末装置Ａ１０２と端末装置Ｂ１０３とは、それぞれブロック暗号鍵１６０８とブロック暗号鍵１６１０とを保有していない。

[0087] 処理の開始から、端末装置Ｂ１０３がブロック暗号切替了承メッセージ１６０７を端末装置Ａ１０２へ送信するまでの処理は、図４に示す処理と同様であるため、説明を省略する。

ブロック暗号切替了承メッセージ１６０７を受信した端末装置Ａ１０２は、残存しているバーナム暗号鍵１６０１からブロック暗号鍵１６０８を生成する。端末装置Ａ１０２は、通信データをブロック暗号鍵１６０８で暗号化し、暗号化通信データ１６０９を生成する。そして、端末装置Ａ１０２は、生成した暗号化通信データ１６０９を端末装置Ｂ１０３へ送信する。

暗号化通信データ１６０９を受信した端末装置Ｂ１０３は、残存しているバーナム暗号鍵１６０２からブロック暗号鍵１６１０を生成する。端末装置Ｂ１０３は、ブロック暗号鍵１６１０で暗号化通信データ１６０９を復号し、通信データを得る。

[0088] なお、端末装置Ａ１０２と端末装置Ｂ１０３とは、予め共有された同一の方法により、バーナム暗号鍵からブロック暗号鍵を生成するものとする。

例えば、端末装置Ａ１０２と端末装置Ｂ１０３とは、残存するバーナム暗号鍵の一部を、そのままブロック暗号鍵とする。つまり、ブロック暗号鍵が２５６ビットである場合、残存するバーナム暗号鍵のうち所定の２５６ビットを切り出してブロック暗号鍵とする。

[0089] 次に、図１６の通信処理について詳しく説明する。図１７及び図１８は、図１６の通信処理の流れを示すフローチャートである。図１７及び図１８に

示す処理では、実施の形態１における図５に示す処理に加えて、バーナム暗号鍵からブロック暗号鍵を生成する処理が行われる。

[0090] ＳＳ０１からＳＳ１７までの処理は、図５に示すＳ１０１からＳ１１７までの処理と同様であるため、説明を省略する。

[0091] 端末装置Ａ１０２は、ブロック暗号切替了承メッセージ４０７を受信すると、残存しているバーナム暗号鍵１６０１からブロック暗号鍵１６０８を生成する（Ｓ５１８）。端末装置Ａ１０２は、通信データのうち単位データ量分のデータをブロック暗号鍵１６０８で暗号化して、暗号化通信データ１６０９を生成する（Ｓ５１９）。そして、端末装置Ａ１０２は、暗号化通信データ１６０９を端末装置Ｂ１０３へ送信する（Ｓ５２０）。

端末装置Ｂ１０３は、暗号化通信データ１６０９を受信する（Ｓ５２１）。すると、端末装置Ｂ１０３は、残存しているバーナム暗号鍵１６０２からブロック暗号鍵１６１０を生成する（Ｓ５２２）。そして、端末装置Ｂ１０３は、ブロック暗号鍵１６１０で暗号化通信データ１６０９を復号し、通信データを得る（Ｓ５２３）。

[0092] Ｓ５２４からＳ５２５までの処理は、図５に示すＳ１２２からＳ１２３までの処理と同様であるため、説明を省略する。

[0093] 次に、実施の形態３において、通信開始時点でバーナム暗号鍵が残りわずかとなっており、バーナム暗号による暗号通信が開始できない時に、ブロック暗号による暗号通信を開始する場合の動作概要について説明する。

図１９は、端末装置Ａ１０２と端末装置Ｂ１０３が暗号通信を開始する時点で、バーナム暗号鍵が不足しているため、ブロック暗号による暗号通信を開始する場合の動作概要を示す図である。図１９に示す処理では、実施の形態１における図６の処理に加えて、バーナム暗号鍵からブロック暗号鍵を生成する処理が行われる。

なお、ここでは、通信開始時点でバーナム暗号鍵は枯渇しておらず、ブロック暗号鍵の生成に必要な量以上残っているものとする。

[0094] 処理の開始から、端末装置Ｂ１０３がブロック暗号切替了承メッセージ１

９０３を端末装置Ａ１０２へ送信するまでの処理は、図６に示す処理と同様であるため、説明を省略する。

ブロック暗号通信了承メッセージ１９０３を受信した端末装置Ａ１０２は、残存しているバーナム暗号鍵１９０１からブロック暗号鍵１９０４を生成する。端末装置Ａ１０２は、通信データをブロック暗号鍵１９０４で暗号化し、暗号化通信データ１９０５を生成する。そして、端末装置Ａ１０２は、生成した暗号化通信データ１９０５を端末装置Ｂ１０３へ送信する。

暗号化通信データ１９０５を受信した端末装置Ｂ１０３は、残存しているバーナム暗号鍵１９０６からブロック暗号鍵１９０７を生成する。端末装置Ｂ１０３は、ブロック暗号鍵１９０７で暗号化通信データ１９０５を復号し、通信データを得る。

[0095] 次に、図１９の通信処理について詳しく説明する。図２０は、図１９の通信処理の流れを示すフローチャートである。図１９に示す処理では、実施の形態１における図７に示す処理に加えて、バーナム暗号鍵からブロック暗号鍵を生成する処理が行われる。

[0096] Ｓ６０１からＳ６０５までの処理は、図７に示すＳ２０１からＳ２０５までの処理と同様であるため、説明を省略する。

[0097] 端末装置Ａ１０２は、ブロック暗号通信了承メッセージ１９０３を受信すると、残存するバーナム暗号鍵１９０１からブロック暗号鍵１９０４を生成する（Ｓ６０６）。端末装置Ａ１０２は、通信データのうち単位データ量分のデータをブロック暗号鍵１９０４で暗号化して、暗号化通信データ１９０５を生成する（Ｓ６０７）。そして、端末装置Ａ１０２は、暗号化通信データ１９０５を端末装置Ｂ１０３へ送信する（Ｓ６０８）。

端末装置Ｂ１０３は、暗号化通信データ１９０５を受信する（Ｓ６０９）。すると、端末装置Ｂ１０３は、残存しているバーナム暗号鍵１９０６からブロック暗号鍵１９０７を生成する（Ｓ６１０）。そして、端末装置Ｂ１０３は、ブロック暗号鍵１９０７で暗号化通信データ１９０５を復号し、通信データを得る（Ｓ６１１）。

[0098] Ｓ６１２からＳ６１３までの処理は、図７に示すＳ２１０からＳ２１１までの処理と同様であるため、説明を省略する。

[0099] 次に、実施の形態３における端末装置Ａ１０２及び端末装置Ｂ１０３の機能について説明する。

図２１は、実施の形態３における端末装置Ａ１０２及び端末装置Ｂ１０３の機能構成を示す機能ブロック図である。図２１に示す端末装置は、図８に示す端末装置が備える機能に加え、暗号鍵変換部８１６を備える。

[0100] 暗号鍵変換部８１６は、バーナム暗号鍵記憶部８１３からバーナム暗号鍵を取得し、取得したバーナム暗号鍵から処理装置によりブロック暗号鍵を生成してブロック暗号鍵記憶部８１４に記憶する。

[0101] 以上のように、実施の形態３に係る暗号化システム１では、残存しているバーナム暗号鍵からブロック暗号鍵を生成する。これにより、実施の形態２のように、事前にブロック暗号鍵を共有することなく、バーナム暗号鍵による暗号通信からブロック暗号による暗号通信へ切り替えることができる。

[0102] なお、上記説明では、バーナム暗号鍵が不足した場合に、残存するバーナム暗号鍵からブロック暗号鍵を生成した。この場合、バーナム暗号鍵が不足した時点において、ブロック暗号鍵を生成するために必要な量以上、バーナム暗号鍵が残存することが前提となる。

そこで、バーナム暗号鍵が不足する前に、残存するバーナム暗号鍵からブロック暗号鍵を生成してもよい。例えば、端末装置が鍵共有装置からバーナム暗号鍵を取得した時点で、残存するバーナム暗号鍵からブロック暗号鍵を生成してもよい。この場合、ブロック暗号鍵を生成するために必要な量以上、バーナム暗号鍵が残存しており、残存するバーナム暗号鍵からブロック暗号鍵を生成できないということがない。

[0103] 実施の形態４.

実施の形態４では、ブロック暗号鍵を複数保持しておき、暗号通信に利用しているブロック暗号鍵を定期的に破棄し、新しいブロック暗号鍵を使って暗号通信を行うことについて説明する。これにより、ブロック暗号による暗

号通信をより安全な通信として実現する。

以下の説明では、一例として実施の形態１に上記の機能を追加したものを示す。

[0104] まず、実施の形態４において、端末装置同士がバーナム暗号による暗号通信を開始し、バーナム暗号用の暗号鍵が不足した時点からブロック暗号による暗号通信に方式の切り替えを行う場合の動作概要について説明する。

図２２は、端末装置Ａ１０２と端末装置Ｂ１０３とがバーナム暗号による暗号通信を開始し、バーナム暗号用の暗号鍵が不足した時点からブロック暗号による暗号通信に方式の切り替えを行う場合の動作概要を示す図である。図２２に示す処理では、実施の形態１における図４の処理に加えて、利用したブロック暗号鍵を破棄し、次のブロック暗号鍵を設定する処理が行われる。

なお、暗号通信の事前準備として、端末装置Ａ１０２はバーナム暗号用のバーナム暗号鍵２２０１と複数のブロック暗号鍵２２０２～２２０４（ブロック暗号鍵１～ｎ）を保有している。また、端末装置Ｂ１０３もバーナム暗号鍵２２０５と複数のブロック暗号鍵２２０６～２２０８（ブロック暗号鍵１～ｎ）を保有している。実施の形態４においては、バーナム暗号鍵２２０１とバーナム暗号鍵２２０５とは同一のものであり、ブロック暗号鍵２２０２～２２０４とブロック暗号鍵２２０６～２２０８とも、それぞれ同一のものである。

なお、ブロック暗号鍵の１～ｎの値は、ブロック暗号鍵を識別する識別番号（識別情報）である。

[0105] 処理の開始から、端末装置Ｂ１０３がブロック暗号切替了承メッセージ２２１３を端末装置Ａ１０２へ送信するまでの処理は、図４に示す処理と同様であるため、説明を省略する。

ブロック暗号切替了承メッセージ２２１３を受信した端末装置Ａ１０２は、通信データをブロック暗号鍵２２０２で暗号化し、暗号化通信データ２２１４を生成し、端末装置Ｂ１０３へ送信する。

暗号化通信データ２２１４を受信した端末装置Ｂ１０３は、ブロック暗号鍵２２０６で暗号化通信データ２２１４を復号し、通信データを得る。

端末装置Ａ１０２と端末装置Ｂ１０３とは、それぞれ、ブロック暗号鍵２２０２、ブロック暗号鍵２２０６を破棄する。そして、端末装置Ａ１０２と端末装置Ｂ１０３とは、それぞれ、次にブロック暗号鍵による暗号化を行う場合には、それぞれブロック暗号鍵２２０３、ブロック暗号鍵２２０７を用いるように設定する。

[0106] 次に、図２２の通信処理について詳しく説明する。図２３及び図２４は、図２２の通信処理の流れを示すフローチャートである。図２３及び図２４に示す処理では、実施の形態１における図５に示す処理に加えて、利用したブロック暗号鍵を破棄し、次のブロック暗号鍵を設定する処理が行われる。

[0107] Ｓ７０１からＳ７１７までの処理は、図５に示すＳ１０１からＳ１１７までの処理と同様であるため、説明を省略する。

[0108] 端末装置Ａ１０２は、ブロック暗号切替了承メッセージ２２１３を受信すると、通信データのうち単位データ量分のデータをブロック暗号鍵２２０２で暗号化して暗号化通信データ２２１４を生成する（Ｓ７１８）。そして、端末装置Ａ１０２は、暗号化通信データ２２１４を端末装置Ｂ１０３へ送信する（Ｓ７１９）。

端末装置Ｂ１０３は、暗号化通信データ２２１４を受信する（Ｓ７２０）。すると、端末装置Ｂ１０３は、ブロック暗号鍵２２０６で暗号化通信データ２２１４を復号し、通信データを得る（Ｓ７２１）。

[0109] 続いて、端末装置Ａ１０２は、未送信の通信データの有無を確認する（Ｓ７２２）。未送信の通信データがなければ（Ｓ７２２でＮＯ）、端末装置Ａ１０２はブロック暗号鍵２２０２を破棄し、次にブロック暗号鍵による暗号化を行う場合には、ブロック暗号鍵２２０３を用いるように設定する（Ｓ７２３）。そして、端末装置Ａ１０２は、処理を終了する（Ｓ７２４）。一方、未送信の通信データがあれば（Ｓ７２２でＹＥＳ）、端末装置Ａ１０２はＳ７１８へ処理を戻す。

同様に、端末装置Ｂ１０３は、未受信の通信データの有無を確認する（Ｓ７２５）。なお、例えば、端末装置Ｂ１０３は、端末装置Ａ１０２から所定の時間内に次の通信データを受信しない場合、未受信の通信データがないと判定する。未受信の通信データがなければ（Ｓ７２５でＮＯ）、端末装置Ａ１０２はブロック暗号鍵２２０６を破棄し、次にブロック暗号鍵による暗号化を行う場合には、ブロック暗号鍵２２０７を用いるように設定する（Ｓ７２６）。そして、端末装置Ｂ１０３は、処理を終了する（Ｓ７２７）。一方、未受信の通信データがあれば（Ｓ７２５でＹＥＳ）、端末装置Ｂ１０３はＳ７２０へ処理を戻す。

[0110] 次に、実施の形態４において、通信開始時点でバーナム暗号鍵が不足しており、バーナム暗号による暗号通信が開始できない時に、ブロック暗号による暗号通信を開始する場合の動作概要について説明する。

図２５は、端末装置Ａ１０２と端末装置Ｂ１０３が暗号通信を開始する時点で、バーナム暗号鍵が不足しているため、ブロック暗号による暗号通信を開始する場合の動作概要を示す図である。図２５に示す処理では、実施の形態１における図６の処理に加えて、利用したブロック暗号鍵を破棄し、次のブロック暗号鍵を設定する処理が行われる。

なお、暗号通信の事前準備として、端末装置Ａ１０２は複数のブロック暗号鍵２５０１～２５０３（ブロック暗号鍵１～ｎ）を保有している。また、端末装置Ｂ１０３も複数のブロック暗号鍵２５０４～２５０６（ブロック暗号鍵１～ｎ）を保有している。端末装置Ａ１０２が保有するブロック暗号鍵２５０１～２５０３と、端末装置Ｂ１０３が保有するブロック暗号鍵２５０４～２５０６とは、それぞれ同一のものであるとする。

[0111] 処理の開始から、端末装置Ｂ１０３がブロック暗号切替了承メッセージ２５０８を端末装置Ａ１０２へ送信するまでの処理は、図６に示す処理と同様であるため、説明を省略する。

ブロック暗号通信了承メッセージ２５０８を受信した端末装置Ａ１０２は、ブロック暗号鍵２５０１を用いて、通信データにブロック暗号による暗号

化を施し、暗号化通信データ２５０９を生成する。そして、端末装置Ａ１０２は、生成した暗号化通信データ２５０９を端末装置Ｂ１０３へ送信する。

暗号化通信データ２５０９を受信した端末装置Ｂ１０３は、ブロック暗号鍵２５０４で暗号化通信データ２５０９を復号し、通信データを得る。

暗号通信の終了後、端末装置Ａ１０２と端末装置Ｂ１０３とは、それぞれブロック暗号鍵２５０１、ブロック暗号鍵２５０４を破棄し、次にブロック暗号鍵による暗号化を行う場合には、それぞれブロック暗号鍵２５０２、ブロック暗号鍵２５０５を用いるように設定する。

端末装置Ａ１０２と端末装置Ｂ１０３とは、それぞれ、ブロック暗号鍵２５０１、ブロック暗号鍵２５０４を破棄する。そして、端末装置Ａ１０２と端末装置Ｂ１０３とは、それぞれ、次にブロック暗号鍵による暗号化を行う場合には、それぞれブロック暗号鍵２５０２、ブロック暗号鍵２５０５を用いるように設定する。

[0112] 次に、図２５の通信処理について詳しく説明する。図２６は、図２５の通信処理の流れを示すフローチャートである。図２６に示す処理では、実施の形態１における図７に示す処理に加えて、利用したブロック暗号鍵を破棄し、次のブロック暗号鍵を設定する処理が行われる。

[0113] ＳＳ８０１からＳ８０５までの処理は、図７に示すＳ２０１からＳ２０５までの処理と同様であるため、説明を省略する。

[0114] 端末装置Ａ１０２は、端末装置Ｂ１０３からブロック暗号通信了承メッセージ２５０８を受信すると、通信データのうち単位データ量分のデータをブロック暗号鍵２５０１で暗号化して、暗号化通信データ２５０９を生成する（Ｓ８０６）。そして、端末装置Ａ１０２は、暗号化通信データ２５０９を端末装置Ｂ１０３へ送信する（Ｓ８０７）。

端末装置Ｂ１０３は、暗号化通信データ２５０９を受信する（Ｓ８０８）。すると、端末装置Ｂ１０３は、ブロック暗号鍵２５０４で暗号化通信データ２５０９を復号し、通信データを得る（Ｓ８０９）。

[0115] 続いて、端末装置Ａ１０２は、未送信の通信データの有無を確認する（Ｓ

８１０）。未送信の通信データがなければ（Ｓ８１０でＮＯ）、端末装置Ａ１０２はブロック暗号鍵２５０１を破棄し、次にブロック暗号鍵による暗号化を行う場合には、ブロック暗号鍵２５０２を用いるように設定する（Ｓ８１１）。そして、端末装置Ａ１０２は、処理を終了する（Ｓ８１２）。一方、未送信の通信データがあれば（Ｓ８１０でＹＥＳ）、端末装置Ａ１０２はＳ８０６へ処理を戻す。

同様に、端末装置Ｂ１０３は、未受信の通信データの有無を確認する（Ｓ８１３）。なお、例えば、端末装置Ｂ１０３は、端末装置Ａ１０２から所定の時間内に次の通信データを受信しない場合、未受信の通信データがないと判定する。未受信の通信データがなければ（Ｓ８１３でＮＯ）、端末装置Ｂ１０３はブロック暗号鍵２５０４を破棄し、次にブロック暗号鍵による暗号化を行う場合には、ブロック暗号鍵２５０５を用いるように設定する（Ｓ８１４）。そして、端末装置Ｂ１０３は、処理を終了する（Ｓ８１５）。一方、未受信の通信データがあれば（Ｓ８１３でＹＥＳ）、端末装置Ａ１０２はＳ８０８へ処理を戻す。

[0116] 次に、実施の形態４における端末装置Ａ１０２及び端末装置Ｂ１０３の機能について説明する。

図２７は、実施の形態４における端末装置Ａ１０２及び端末装置Ｂ１０３の機能構成を示す機能ブロック図である。図２７に示す端末装置は、図８に示す端末装置が備える機能に加え、ブロック暗号鍵更新部８１７を備える。

[0117] ブロック暗号鍵更新部８１７は、ブロック暗号鍵記憶部８１４から現在使われているブロック暗号鍵を削除し、次のブロック暗号鍵を設定する。

[0118] 以上のように、実施の形態４に係る暗号化システム１では、ブロック暗号鍵を複数保持しておき、暗号通信に利用しているブロック暗号鍵を定期的に破棄し、新しいブロック暗号鍵を使って暗号通信を行う。これにより、ブロック暗号による暗号通信の安全性を高めることができる。

[0119] なお、ここでは、ブロック暗号鍵を定期的に破棄し、新しいブロック暗号鍵を使って暗号通信を行う機能を実施の形態１に係る暗号化システム１に追

加した場合について説明した。しかし、ブロック暗号鍵を定期的に破棄し、新しいブロック暗号鍵を使って暗号通信を行う機能を実施の形態３に係る暗号化システム１に追加してもよい。この場合、暗号鍵変換部８１６（図２１参照）は、バーナム暗号鍵から複数のブロック暗号鍵を生成する。例えば、残存するバーナム暗号鍵を、所定のビット毎に分割して複数のブロック暗号鍵とする。つまり、ブロック暗号鍵が２５６ビットである場合、残存するバーナム暗号鍵（の一部）を、２５６ビット毎に分割して複数のブロック暗号鍵とする。

[0120] 実施の形態５.

実施の形態５では、実施の形態４において、ブロック暗号鍵が残り１つとなった時点でブロック暗号による暗号化を行う場合には、現在のブロック暗号鍵をハッシュ関数などのランダム化によって更新することについて説明する。これにより、同じブロック暗号鍵を繰り返し用いることによる安全性の低下を防ぐ技術について説明する。

[0121] バーナム暗号鍵が不足しており、ブロック暗号鍵の残りが１つしかない時に端末装置間でブロック暗号による暗号通信を行うと、次回以降のブロック暗号による暗号通信においても同じブロック暗号鍵を用いることになる。そのため、暗号通信を行うほど、暗号通信の安全性が低下していくことになる。

そこで、実施の形態５では、ブロック暗号鍵の残りが１つしかない時にブロック暗号による暗号通信を行った場合、そのブロック暗号鍵をハッシュ関数などを用いたランダム化によって更新する。

[0122] まず、通信開始時点でバーナム暗号鍵が不足しており、かつ、ブロック暗号鍵の残りが１つである時に、ブロック暗号による暗号通信を開始する場合の動作概要について説明する。

図２８は、端末装置Ａ１０２と端末装置Ｂ１０３とが暗号通信を開始する時点で、バーナム暗号鍵が不足しており、かつ、ブロック暗号鍵の残りが１つしかない場合の動作概要を示す図である。

なお、端末装置Ａ１０２はブロック暗号用のブロック暗号鍵２８０３を保有している。また、端末装置Ｂ１０３もブロック暗号鍵２８０５を保有している。端末装置Ａ１０２が保有するブロック暗号鍵２８０３と、端末装置Ｂ１０３が保有するブロック暗号鍵２８０５とは、それぞれ同一のものであるとする。

[0123] 処理の開始から、端末装置Ｂ１０３がブロック暗号切替了承メッセージ２８０２を端末装置Ａ１０２へ送信するまでの処理は、図６に示す処理と同様であるため、説明を省略する。

ブロック暗号通信了承メッセージ２８０２を受信した端末装置Ａ１０２は、ブロック暗号鍵２８０３を用いて、通信データにブロック暗号による暗号化を施し、暗号化通信データ２８０４を生成する。そして、端末装置Ａ１０２は、生成した暗号化通信データ２８０４を端末装置Ｂ１０３へ送信する。

暗号化通信データ２８０４を受信した端末装置Ｂ１０３は、ブロック暗号鍵２８０５で暗号化通信データ２８０４を復号し、通信データを得る。

暗号通信の終了時、端末装置Ａ１０２と端末装置Ｂ１０３とは、それぞれ、ブロック暗号鍵２８０３、ブロック暗号鍵２８０５にハッシュ関数などによるランダム化を施し、ブロック暗号鍵２８０６、ブロック暗号鍵２８０７を生成する。そして、端末装置Ａ１０２と端末装置Ｂ１０３とは、次にブロック暗号鍵による暗号化を行う場合には、それぞれブロック暗号鍵２８０６、ブロック暗号鍵２８０７を用いるように設定する。このとき、端末装置Ａ１０２と端末装置Ｂ１０３とは、それぞれ、ブロック暗号鍵２８０３、２８０５を削除する。

[0124] 次に、図２８の通信処理について詳しく説明する。図２９は、図２８の通信処理の流れを示すフローチャートである。図２９に示す処理では、実施の形態１における図７に示す処理に加えて、利用したブロック暗号鍵を更新する処理が行われる。

[0125] Ｓ９０１からＳ９０５までの処理は、図７に示すＳ２０１からＳ２０５までの処理と同様であるため、説明を省略する。

[0126] 端末装置Ａ１０２は、端末装置Ｂ１０３からブロック暗号通信了承メッセージ２８０２を受信すると、通信データのうち単位データ量分のデータをブロック暗号鍵２８０３で暗号化して、暗号化通信データ２８０４を生成する（Ｓ９０６）。そして、端末装置Ａ１０２は、暗号化通信データ２８０４を端末装置Ｂ１０３へ送信する（Ｓ９０７）。

端末装置Ｂ１０３は、暗号化通信データ２８０４を受信する（Ｓ９０８）。すると、端末装置Ｂ１０３は、ブロック暗号鍵２８０５で暗号化通信データ２８０４を復号し、通信データを得る（Ｓ９０９）。

[0127] 続いて、端末装置Ａ１０２は、未送信の通信データの有無を確認する（Ｓ９１０）。未送信の通信データがなければ（Ｓ９１０でＮＯ）、端末装置Ａ１０２はブロック暗号鍵２８０３にハッシュ関数などによるランダム化を施し、ブロック暗号鍵２８０６を生成する（Ｓ９１１）。そして、端末装置Ａ１０２は、次回の暗号通信にブロック暗号鍵２８０６を設定し、ブロック暗号鍵２８０３を破棄して（Ｓ９１２）、処理を終了する（Ｓ９１３）。一方、未送信の通信データがあれば（Ｓ９１０でＹＥＳ）、端末装置Ａ１０２はＳ９０６へ処理を戻す。

同様に、端末装置Ｂ１０３は、未受信の通信データの有無を確認する（Ｓ９１４）。なお、例えば、端末装置Ｂ１０３は、端末装置Ａ１０２から所定の時間内に次の通信データを受信しない場合、未受信の通信データがないと判定する。未受信の通信データがなければ（Ｓ９１４でＮＯ）、端末装置Ａ１０２はブロック暗号鍵２８０５にハッシュ関数などによるランダム化を施し、ブロック暗号鍵２８０７を生成する（Ｓ９１５）。なお、端末装置Ｂ１０３がランダム化に用いるハッシュ関数などは、Ｓ９１１で端末装置Ａ１０２が用いたものと同じものである。したがって、ここで、生成されるブロック暗号鍵２８０７と、Ｓ９１１で生成されるブロック暗号鍵２８０６とは同じである。そして、端末装置Ｂ１０３は、処理を終了する（Ｓ８１５）。一方、未受信の通信データがあれば（Ｓ９１４でＹＥＳ）、端末装置Ｂ１０３は処理をＳ９０８へ戻す。

[0128] 次に、実施の形態５における端末装置Ａ１０２及び端末装置Ｂ１０３の機能について説明する。

図３０は、実施の形態５における端末装置Ａ１０２及び端末装置Ｂ１０３の機能構成を説明する機能ブロック図である。図３０に示す端末装置は、図２７に示す端末装置が備える機能に加え、ハッシュ関数処理部８１８（ブロック暗号鍵生成部）を備える。また、ブロック暗号鍵更新部８１７の処理が異なる。

[0129] ブロック暗号鍵更新部８１７は、ブロック暗号鍵記憶部８１４から現在使われているブロック暗号鍵を削除し、次のブロック暗号鍵を設定する。

但し、ブロック暗号鍵の残りが１つしかなく、次のブロック暗号鍵が存在しない場合は、ブロック暗号鍵更新部８１７は、現在使われているブロック暗号鍵をハッシュ関数処理部に渡す。そして、ブロック暗号鍵更新部８１７は、ハッシュ関数処理部８１８から新しいブロック暗号鍵を受け取り、ブロック暗号鍵記憶部８１４に記憶する。

[0130] ハッシュ関数処理部８１８は、ブロック暗号鍵更新部８１７からブロック暗号鍵を受け取る。ハッシュ関数処理部８１８は、受け取ったブロック暗号鍵にハッシュ関数などによるランダム化を施し、新しいブロック暗号鍵を生成する。そして、生成したブロック暗号鍵をブロック暗号鍵更新部８１７に渡す。

[0131] 以上のように、実施の形態５に係る暗号化システム１では、ブロック暗号鍵の残りが１つである場合、現在使われているブロック暗号鍵から新しいブロック暗号鍵を生成する。これにより、ブロック暗号による暗号通信の安全性を高めることができる。

[0132] なお、上記に示したような、現在使われているブロック暗号鍵から新しいブロック暗号鍵を生成する処理は、ブロック暗号鍵の残りが１つである状態が継続している限り、暗号通信を行うたびに行われる。

[0133] 実施の形態６.

実施の形態６では、実施の形態１～５において、バーナム暗号鍵の残量が

一定量よりも少なくなった時点で、残存するバーナム暗号鍵を増大することについて説明する。これにより、バーナム暗号鍵が不足することを防止する。

以下の説明では、一例として、実施の形態１に上記の機能を追加したものを示す。

[0134] バーナム暗号を行うためには、暗号化の対象となるデータと同量の暗号鍵が必要である。そのため、暗号化対象のデータが膨大である場合、暗号鍵の消費もそれに比例して膨大となる。そこで、実施の形態６においては、バーナム暗号鍵の残量が事前に決められた量よりも少なくなった場合に、残存しているバーナム暗号鍵に増大処理を施し、バーナム暗号鍵の分量を増大させる。

例えば、バーナム暗号鍵が半分になった時点で、残っているバーナム暗号鍵に増大処理を施し、２倍の長さにすれば、元の長さと同じだけのバーナム暗号鍵が確保できる。

[0135] しかし、鍵共有装置から取得したバーナム暗号鍵に対して、何度も増大処理を行うと、バーナム暗号鍵の安全性が低下する虞がある。例えば、鍵共有装置から取得したバーナム暗号鍵が真性乱数である場合に、後の実施の形態で説明するように、擬似乱数を用いてバーナム暗号鍵を増大させると、バーナム暗号鍵の安全性が低下する虞がある。

そこで、実施の形態６においては、鍵共有装置から取得したバーナム暗号鍵に対して増大処理を実行する回数を制限する。

[0136] まず、実施の形態６において、端末装置同士がバーナム暗号による暗号通信を開始し、バーナム暗号鍵の残量が事前に決められた量よりも少なくなった時点で、バーナム暗号鍵に増大処理を施す場合の動作概要について説明する。

図３１は、端末装置Ａ１０２と端末装置Ｂ１０３とがバーナム暗号による暗号通信を開始し、バーナム暗号鍵の残量が事前に決められた量よりも少なくなった時点で、バーナム暗号鍵に増大処理を施す場合の動作概要を示す図

である。

暗号通信の事前準備として、端末装置Ａ１０２はバーナム暗号用のバーナム暗号鍵３１０１を保有している。また、端末装置Ｂ１０３もバーナム暗号鍵３１０２を保有している。バーナム暗号鍵３１０１とバーナム暗号鍵３１０２とは同一のものであるとする。

また、端末装置Ａ１０２はブロック暗号用のブロック暗号鍵３１１３を保有している。また、端末装置Ｂ１０３もブロック暗号鍵３１１５を保有している。端末装置Ａ１０２が保有するブロック暗号鍵３１１３と、端末装置Ｂ１０３が保有するブロック暗号鍵３１１５とは同一のものであるとする。

[0137] 処理の開始から、端末装置Ｂ１０３がバーナム暗号により生成した暗号化通信データ３１０５から通信データを得るまでの処理は、図４に示す処理と同様であるため、説明を省略する。

もし、暗号化通信データ３１０５を生成することでバーナム暗号鍵の残量が事前に決められた量より少なくなった場合、端末装置Ａ１０２はバーナム暗号鍵増大要求メッセージ３１０６を端末装置Ｂ１０３へ送信する。

バーナム暗号鍵増大要求メッセージ３１０６を受信した端末装置Ｂ１０３は、バーナム暗号鍵増大了承メッセージ３１０７を端末装置Ａ１０２へ送信する。

バーナム暗号鍵増大了承メッセージ３１０７を受信した端末装置Ａ１０２は、バーナム暗号鍵３１０１に増大処理を施し、新たなバーナム暗号鍵３１０８を生成する。端末装置Ａ１０２は、生成したバーナム暗号鍵３１０８で通信データを暗号化し、暗号化通信データ３１０９を生成する。そして、端末装置Ａ１０２は、生成した暗号化通信データ３１０９を端末装置Ｂ１０３へ送信する。

暗号化通信データ３１０９を受信した端末装置Ｂ１０３は、バーナム暗号鍵３１０２に増大処理を施し、新たなバーナム暗号鍵３１１０を生成する。端末装置Ｂ１０３は、生成したバーナム暗号鍵３１１０で暗号化通信データ３１０９を復号し、通信データを得る。

なお、端末装置Ａ１０２と端末装置Ｂ１０３とは、予め共有された同一の方法により、バーナム暗号鍵を増大させるものとする。

[0138] 端末装置Ａ１０２と端末装置Ｂ１０３とは、事前に決められた回数までは、現在のバーナム暗号鍵の残量が事前に決められた量より少なくなる度に、同様の増大処理を行う。一方、事前に決められた回数だけ増大処理を行った場合、バーナム暗号鍵が事前に決められた量より少なくなっても増大処理は行わず、以降に示す処理を実行する。

[0139] もし、端末装置Ａ１０２における暗号化通信データ３１０９の生成時にバーナム暗号を行うことができるデータ通信量を超えて、暗号化を行う必要がある場合、端末装置Ａ１０２はブロック暗号切替要求メッセージ３１１１を端末装置Ｂ１０３へ送信する。

ブロック暗号切替要求メッセージ３１１１を受信した端末装置Ｂ１０３は、ブロック暗号切替了承メッセージ３１１２を端末装置Ａ１０２へ送信する。

ブロック暗号切替了承メッセージ３１１２を受信した端末装置Ａ１０２は、通信データをブロック暗号鍵３１１３で暗号化し、暗号化通信データ３１１４を生成する。そして、端末装置Ａ１０２は、生成した暗号化通信データ３１１４を端末装置Ｂ１０３へ送信する。

暗号化通信データ３１１４を受信した端末装置Ｂ１０３は、ブロック暗号鍵３１１５で暗号化通信データ３１１４を復号し、通信データを得る。

[0140] 次に、図３１の通信処理について詳しく説明する。図３２から図３４は、図３１の通信処理の流れを示すフローチャートである。図３２から図３４に示す処理では、実施の形態１における図５の処理に加えて、バーナム暗号鍵を増大するための処理が行われる。

[0141] Ｓ１００１からＳ１０１２までの処理は、図５に示すＳ１０１からＳ１１２までの処理と同様であるため、説明を省略する。

[0142] 未送信の通信データがあった場合（Ｓ１０１１でＹＥＳ）、端末装置Ａ１０２は、バーナム暗号鍵の残量が事前に決められた量より少ないかを確認す

る（Ｓ１０１３）。残量が事前に決められた量以上の場合（Ｓ１０１３でＮＯ）、Ｓ１００７へ処理を戻す。一方、残量が事前に決められた量より少ない場合（Ｓ１０１３でＹＥＳ）、Ｓ１０１４へ処理を進める。

そして、端末装置Ａ１０２は、今までにバーナム暗号鍵の増大処理を行った回数が事前に決められた制限回数より少ないかを確認する（Ｓ１０１４）。増大処理を行った回数が事前に定められた回数以上の場合（Ｓ１０１４でＮＯ）、Ｓ１０２５へ処理を進める。一方、増大処理を行った回数が事前に定められた回数より少ない場合（Ｓ１０１４でＹＥＳ）、端末装置Ａ１０２は、バーナム暗号鍵増大要求メッセージ３１０６を端末装置Ｂ１０３へ送信する（Ｓ１０１５）。

[0143] 端末装置Ｂ１０３は、バーナム暗号鍵増大要求メッセージ３１０６を受信する（Ｓ１０１６）。すると、端末装置Ｂ１０３は、バーナム暗号鍵増大了承メッセージ３１０７を端末装置Ａ１０２へ送信する（Ｓ１０１７）。

端末装置Ａ１０２は、バーナム暗号鍵増大了承メッセージ３１０７を受信する（Ｓ１０１８）。すると、バーナム暗号鍵３１０１に増大処理を施し、新たなバーナム暗号鍵３１０８を生成する（Ｓ１０１９）。端末装置Ａ１０２は、生成したバーナム暗号鍵３１０８で通信データのうち単位データ量分のデータを暗号化し、暗号化通信データ３１０９を生成する（Ｓ１０２０）。そして、端末装置Ａ１０２は、暗号化通信データ３１０９を端末装置Ｂ１０３へ送信する（Ｓ１０２１）。

端末装置Ｂ１０３は、暗号化通信データ３１０９を受信する（Ｓ１０２２）。すると、端末装置Ｂ１０３は、バーナム暗号鍵３１０２に増大処理を施し、新たなバーナム暗号鍵３１１０を生成する（Ｓ１０２３）。端末装置Ｂ１０３は、生成したバーナム暗号鍵３１１０で暗号化通信データ３１０９を復号し、通信データを得る（Ｓ１０２４）。

Ｓ１０２１で暗号化通信データ３１０９を端末装置Ｂ１０３へ送信した後、端末装置Ａ１０２はＳ１０１１へ処理を戻す。

[0144] 増大処理を行った回数が事前に定められた回数以上の場合（Ｓ１０１４で

ＮＯ）、端末装置Ａ１０２は、引き続き通信データをバーナム暗号で暗号化する（Ｓ１０２５）。

Ｓ１０２６からＳ１０４１までの処理は、図５に示すＳ１０８からＳ１２３までの処理と同様であるため、説明を省略する。

[0145] 次に、実施の形態６における端末装置Ａ１０２及び端末装置Ｂ１０３の機能について説明する。

図３５は、実施の形態６における端末装置Ａ１０２及び端末装置Ｂ１０３の機能構成を示す機能ブロック図である。図３５に示す端末装置は、図８に示す端末装置が備える機能に加え、バーナム暗号鍵増大部８１９を備える。

[0146] バーナム暗号鍵増大部８１９は、バーナム暗号鍵記憶部８１３から残存しているバーナム暗号鍵を取得し、増大処理を行う。増大処理を行った結果として得られたバーナム暗号鍵をバーナム暗号鍵記憶部８１３に渡す。

[0147] 以上のように、実施の形態６に係る暗号化システムでは、バーナム暗号鍵の残量が所定量より少なくなると、残りのバーナム暗号鍵に対して増大処理を実行して、バーナム暗号鍵の残量を増大させる。これにより、バーナム暗号鍵が不足することを防止する。

また、鍵共有装置から取得したバーナム暗号鍵に対して、増大処理を実行する回数を制限することにより、バーナム暗号鍵の安全性が所定以上に低下することを防止している。

[0148] 実施の形態７.

実施の形態７では、実施の形態６で説明したバーナム暗号鍵の増大方法の一例について説明する。

実施の形態７では、残存するバーナム暗号鍵に一定の割合で擬似乱数を混ぜることによりバーナム暗号鍵を増大させる。これにより、バーナム暗号鍵の乱数性を維持しつつ、バーナム暗号鍵の不足を防止する。

[0149] 図３６は、実施の形態７におけるバーナム暗号鍵増大部８１９の処理を説明する図である。

バーナム暗号鍵増大部８１９は、内部に擬似乱数生成器３６０１を有する

。バーナム暗号鍵増大部８１９は、バーナム暗号鍵３６０２が入力されると、小さな単位、例えば１ビットごとに分解する。そして、バーナム暗号鍵増大部８１９は、擬似乱数生成器３６０１から受け取った擬似乱数３６０３を分解したバーナム暗号鍵３６０２の間に挿入する。

この処理により、バーナム暗号鍵増大部８１９は、入力されたバーナム暗号鍵３６０２から新しいバーナム暗号鍵３６０４を生成し、出力する。この例では、新しいバーナム暗号鍵３６０４の長さは、入力されたバーナム暗号鍵３６０２長さの２倍となる。

[0150] 実施の形態８.

実施の形態８では、実施の形態６で説明したバーナム暗号鍵の増大方法の、実施の形態７とは異なる例について説明する。

実施の形態８では、残存するバーナム暗号鍵を種として、ハッシュ関数や暗号方式による擬似乱数生成を行い、得られた擬似乱数を新しいバーナム暗号鍵とする。これにより、バーナム暗号鍵の乱数性を維持しつつ、バーナム暗号鍵の枯渇を防止する。

[0151] 図３７は、実施の形態８におけるバーナム暗号鍵増大部８１９の処理を説明する図である。

バーナム暗号鍵増大部８１９は、内部に擬似乱数生成器３７０１とハッシュ関数３７０２を有する。バーナム暗号鍵増大部８１９は、バーナム暗号鍵３７０３が入力されると、擬似乱数生成器３７０１から受け取った擬似乱数３７０４とバーナム暗号鍵３７０３とを組み合わせ、ハッシュ関数３７０２に入力する。擬似乱数３７０４とバーナム暗号鍵３７０３とを組み合わせるとは、例えば、バーナム暗号鍵３７０３の前又は後に擬似乱数３７０４を付加することである。そして、ハッシュ関数３７０２でランダム化されたものを新しいバーナム暗号鍵３７０５として出力する。

この処理により、バーナム暗号鍵増大部８１９は、入力されたバーナム暗号鍵３７０３から新しいバーナム暗号鍵３７０５を生成し、出力する。この例では、新しいバーナム暗号鍵３７０５の長さは、ハッシュ関数３７０２に

よって元のバーナム暗号鍵の長さと同じになる。

[0152] 実施の形態９.

実施の形態１～８においては、端末装置が鍵共有装置と接続されていることを前提として説明した。しかし、例えば、端末装置が携帯電話等の携帯端末である場合には、端末装置と鍵共有装置が接続されていない状況も起こりうる。この場合、鍵共有装置から端末装置へのバーナム暗号鍵又はブロック暗号鍵の転送処理を行う時期が、端末装置間で一致していないことにより、端末装置間で保有している暗号鍵の量が異なっている場合が起こりえる。

例えば、ある時点で端末装置Ａ１０２が鍵共有装置Ｃ１０４からバーナム暗号鍵を取得したとする。その後、鍵共有装置Ｃ１０４と鍵共有装置Ｄ１０５との間で新たなバーナム暗号鍵が共有されたとする。そして、端末装置Ｂ１０３が鍵共有装置Ｄ１０５からバーナム暗号鍵を取得したとする。すると、端末装置Ｂ１０３は端末装置Ａ１０２が保有していないバーナム暗号鍵を保有していることになる。この場合、端末装置Ａ１０２と端末装置Ｂ１０３との間で暗号通信を行う場合、端末装置Ａ１０２のバーナム暗号鍵が先に不足することになる。

そこで、実施の形態９では、暗号通信を行う前に端末装置間で互いの保有しているバーナム暗号鍵の情報を共有し、互いの保有しているバーナム暗号鍵の状況に応じて暗号通信を切り替えることを説明する。

[0153] まず、実施の形態９において、端末装置Ａ１０２と端末装置Ｂ１０３とがバーナム暗号による暗号通信を開始し、バーナム暗号鍵が不足した時点からブロック暗号による暗号通信に方式の切り替えを行う場合の処理について説明する。

図３８及び図３９は、実施の形態９における図４の通信処理の流れを示すフローチャートである。図３８及び図３９に示す処理では、実施の形態１における図５の処理に加えて、事前にバーナム暗号鍵の残量を端末装置間で共有する処理が行われる。

[0154] 端末装置Ａ１０２は、保有しているバーナム暗号鍵４０１の量を確認し（

Ｓ１１０１）、バーナム暗号通信要求メッセージ４０３をバーナム暗号鍵４０１の残量値と共に端末装置Ｂ１０３へ送信する（Ｓ１１０２）。

端末装置Ｂ１０３は、端末装置Ａ１０２からバーナム暗号通信要求メッセージ４０３を受信する（Ｓ１１０３）。すると、端末装置Ｂ１０３は、保有しているバーナム暗号鍵４０２の量を確認し（Ｓ１１０４）、バーナム暗号で暗号通信を行うことができるデータ量を算出する（Ｓ１１０５）。そして、端末装置Ｂ１０３は、バーナム暗号通信了承メッセージ４０４をバーナム暗号鍵４０２の残量値と共に端末装置Ａ１０２へ送信する（Ｓ１１０６）。

端末装置Ａ１０２は、端末装置Ｂ１０３からバーナム暗号通信了承メッセージ４０４を受信する（Ｓ１１０７）。すると、端末装置Ａ１０２は、バーナム暗号で暗号通信を行うことができるデータ量を算出する（Ｓ１１０８）。また、端末装置Ａ１０２は、通信データのうち単位データ量分のデータにバーナム暗号鍵４０１を用いた暗号化を施して、暗号化通信データ４０５を生成する（Ｓ１１０９）。そして、端末装置Ａ１０２は、暗号化通信データ４０５を端末装置Ｂ１０３へ送信する（Ｓ１１１０）。

端末装置Ｂ１０３は、端末装置Ａ１０２から暗号化通信データ４０５を受信する（Ｓ１１１１）。すると、端末装置Ｂ１０３は、バーナム暗号鍵４０２を用いて暗号化通信データ４０５を復号して通信データを得る（Ｓ１１１２）。

[0155] 続いて、端末装置Ａ１０２は、未送信の通信データの有無を確認する（Ｓ１１１３）。未送信の通信データがなければ（Ｓ１１１３でＮＯ）、端末装置Ａ１０２は処理を終了する（Ｓ１１１４）。一方、未送信の通信データがあれば（Ｓ１１１３でＹＥＳ）、端末装置Ａ１０２はＳ１１１５へ処理を進める。

[0156] 端末装置Ａ１０２は、バーナム暗号で暗号化通信を行うことができるデータ量が、１度に暗号化する単位データ量以上かを確認する（Ｓ１１１５）。この際、端末装置Ａ１０２は、（Ｓ１１０８）で算出したデータ量から、現時点で端末装置Ａ１０２がバーナム暗号で暗号通信を行うことができるデー

タ量を算出する。また、端末装置Ａ１０２は、バーナム暗号通信了承メッセージ４０４とともに受信した端末装置Ｂ１０３が保有するバーナム暗号鍵の残量から、現時点で端末装置Ｂ１０３がバーナム暗号で暗号通信を行うことができるデータ量を算出する。そして、端末装置Ａ１０２と端末装置Ｂ１０３とがバーナム暗号で暗号通信を行うことができるデータ量のうち、少ない方のデータ量が、１度に暗号化する単位データ量を超えているかを確認する。

少ない方のデータ量が単位データ量以上であれば（Ｓ１１１５でＹＥＳ）、端末装置Ａ１０２はＳ１１０９へ処理を戻す。一方、少ない方のデータ量が単位データ量未満であれば（Ｓ１１１５でＮＯ）、端末装置Ａ１０２はブロック暗号切替要求メッセージ４０６を端末装置Ｂ１０３へ送信する（Ｓ１１１６）。

[0157] Ｓ１１１７からＳ１１２５までの処理は、図５に示すＳ１１５からＳ１２３までの処理と同様であるため、説明を省略する。

[0158] 次に、通信開始時点で受信側端末装置のバーナム暗号鍵が不足しており、バーナム暗号による暗号通信が開始できない時に、ブロック暗号による暗号通信を開始する場合の動作概要について説明する。

図４０は、実施の形態９において、端末装置Ａ１０２と端末装置Ｂ１０３が暗号通信を開始する時点で、端末装置Ｂ１０３のバーナム暗号鍵が不足しているため、ブロック暗号による暗号通信を開始する場合の動作概要を示す図である。

なお、端末装置Ａ１０２はバーナム暗号鍵４００１とブロック暗号鍵４００２とを保有しており、端末装置Ｂ１０３はバーナム暗号鍵を保有せず、ブロック暗号鍵４００３を保有しているとする。つまり、端末装置Ｂ１０３はバーナム暗号鍵が枯渇している状態であるとする。

[0159] まず、端末装置Ａ１０２は、保有しているバーナム暗号鍵４００１の量を確認し、端末装置Ｂ１０３にバーナム暗号通信要求メッセージ４００４を送信する。

バーナム暗号通信要求メッセージ４００４を受信した端末装置Ｂ１０３は、バーナム暗号鍵が枯渇していることを確認し、バーナム暗号通信拒否メッセージ４００５を送信する。

バーナム暗号通信拒否メッセージ４００５を受信した端末装置Ａ１０２は、端末装置Ｂ１０３にブロック暗号通信要求メッセージ４００６を送信する。

ブロック暗号通信要求メッセージ４００６を受信した端末装置Ｂ１０３は、端末装置Ａ１０２にブロック暗号通信了承メッセージ４００７を送信する。

以降の処理は、図６に示す処理と同様であるため、説明を省略する。

[0160] 次に、図４０の通信処理について詳しく説明する。図４１は、図４０の通信処理の流れを示すフローチャートである。

[0161] まず、端末装置Ａ１０２は、保有しているバーナム暗号鍵４００１の量を確認し（Ｓ１２０１）、端末装置Ｂ１０３にバーナム暗号通信要求メッセージ４００４を送信する（Ｓ１２０２）。

端末装置Ｂ１０３は、バーナム暗号通信要求メッセージ４００４を受信する（Ｓ１２０３）。すると、端末装置Ｂ１０３は、保有しているバーナム暗号鍵の量を確認し（Ｓ１２０４）、バーナム暗号による暗号通信が可能なデータ量が不足していることを算出する（Ｓ１２０５）。そして、端末装置Ｂ１０３は、バーナム暗号通信拒否メッセージ４００５を端末装置Ａ１０２へ送信する（Ｓ１２０６）。

端末装置Ａ１０２は、バーナム暗号通信拒否メッセージ４００５を受信する（Ｓ１２０７）。すると、端末装置Ａ１０２は、ブロック暗号通信要求メッセージ４００６を端末装置Ｂ１０３へ送信する（Ｓ１２０８）。

[0162] Ｓ１２０９からＳ１２１７までの処理は、図７に示すＳ２０３からＳ２１１までの処理と同様であるため、説明を省略する。

[0163] 次に、送信側の端末装置である端末装置Ａ１０２の処理について詳しく説明する。

図４２は、実施の形態９における端末装置８０１の送信制御部８０３の処理の流れを示すフローチャートである。

[0164] 送信制御部８０３は、バーナム暗号鍵管理部８０５からバーナム暗号鍵の残量が不足しているか否かを示す残量情報を取得する（Ｓ１３０１）。そして、送信制御部８０３は、バーナム暗号鍵の残量が不足していなければ（Ｓ１３０２でＮＯ）、Ｓ１３０３に処理を進め、残量が不足していれば（Ｓ１３０２でＹＥＳ）、Ｓ１３１２に処理を進める（Ｓ１３０２）。

[0165] 送信制御部８０３は、通信インターフェイス８０２を介して、バーナム暗号通信要求メッセージを端末装置Ｂ１０３へ送信し（Ｓ１３０３）、端末装置Ｂ１０３からメッセージを受信する（Ｓ１３０４）。そして、送信制御部８０３は、受信したメッセージがバーナム暗号通信了承メッセージであれば、処理をＳ１３０６へ進め、バーナム暗号通信拒否メッセージであれば、処理をＳ１３１２へ進める。

[0166] Ｓ１３０６からＳ１３１６までの処理は、図９に示すＳ３０５からＳ３１５までの処理と同様であるため、説明を省略する。

[0167] 次に、受信側の端末装置である端末装置Ｂ１０３の処理について詳しく説明する。

図４３は、実施の形態９における端末装置８０１の受信制御部８０４の処理の流れを示すフローチャートである。

[0168] 受信制御部８０４は、バーナム暗号通信要求メッセージ、又は、ブロック暗号通信要求メッセージを端末装置Ａ１０２から通信インターフェイス８０２を介して受信する（Ｓ１４０１）。受信制御部８０４は、バーナム暗号要求メッセージを受信した場合はＳ１４０３に処理を進め、ブロック暗号要求メッセージを受信した場合はＳ１４１２に処理を進める（Ｓ１４０２）。

[0169] 受信制御部８０４は、バーナム暗号鍵管理部８０５からバーナム暗号鍵の残量が不足しているか否かを示す残量情報を取得する（Ｓ１４０３）。受信制御部８０４は、バーナム暗号鍵の残量が不足していれば（Ｓ１４０３でＹＥＳ）、処理をＳ１４０４へ進め、バーナム暗号鍵の残量が不足していなけ

れば（Ｓ１４０３でＮＯ）、処理をＳ１４０５へ進める。

バーナム暗号鍵の残量が不足していた場合、受信制御部８０４は、バーナム暗号通信拒否メッセージを端末装置Ａ１０２へ送信し（Ｓ１４０４）、処理をＳ１４１３へ進める。

[0170] Ｓ１４０５からＳ１４１５までの処理は、図１０に示すＳ４０３からＳ４１３までの処理と同様であるため、説明を省略する。

[0171] 以上のように、実施の形態９に係る暗号化システム１では、端末装置間で互いの保有しているバーナム暗号鍵の残量を共有することで、保有するバーナム暗号鍵に差異がある場合であっても、暗号方式の切り替えを行うことができる。

[0172] なお、上記説明では、単に、端末装置Ａ１０２と端末装置Ｂ１０３とのうち、バーナム暗号鍵の残量の少ない方に合わせて、暗号方式の切り替えを行った。

しかし、端末装置Ａ１０２と端末装置Ｂ１０３とで保有するバーナム暗号鍵にずれがある場合も考えられる。つまり、端末装置Ａ１０２が保有しているバーナム暗号鍵のうち、一部を端末装置Ｂ１０３が保有しておらず、端末装置Ｂ１０３が保有しているバーナム暗号鍵のうち、一部を端末装置Ａ１０２が保有していない場合が考えられる。この場合、端末装置Ａ１０２と端末装置Ｂ１０３とが共通して保有しているバーナム暗号鍵の残量に応じて、暗号方式を切り替える必要がある。

[0173] この場合、例えば、端末装置は、鍵共有装置からバーナム暗号鍵を取得する場合、バーナム暗号鍵のビット数をカウントしておく。例えば、初めに、端末装置が鍵共有装置から１０００ビットのバーナム暗号鍵を取得した場合、端末装置は１ビット目から１０００ビット目までのバーナム暗号鍵を取得したとカウントする。次に、端末装置が鍵共有装置から５００ビットのバーナム暗号鍵を取得した場合、端末装置は１００１ビット目から１５００ビット目までのバーナム暗号鍵を取得したとカウントする。

また、端末装置は、使用したバーナム暗号鍵のビット数もカウントしてお

く。例えば、初めに１００ビットのバーナム暗号鍵を使用したのであれば、１ビット目から１００ビット目までのバーナム暗号鍵を使用したとカウントする。

したがって、端末装置は、現在何ビット目から何ビット目までのバーナム暗号鍵が使用できる状態で残っているかを知ることができる。

[0174] この場合、端末装置Ａ１０２は、バーナム暗号鍵の残量を確認する代わりに、何ビット目から何ビット目までのバーナム暗号鍵が使用できる状態で残っているか確認する。そして、バーナム暗号通信要求メッセージとともに、何ビット目から何ビット目までのバーナム暗号鍵が使用できる状態で残っているかを示す情報を端末装置Ｂ１０３へ送信する。

端末装置Ｂ１０３は、何ビット目から何ビット目までのバーナム暗号鍵が使用できる状態で残っているか確認する。そして、端末装置Ａ１０２が保有するバーナム暗号鍵と端末装置Ｂ１０３が保有するバーナム暗号鍵との共通部分を特定する。共通部分で暗号通信できるデータ量が１度に暗号化する単位データ量を超えていれば、端末装置Ｂ１０３は、バーナム暗号通信了承メッセージとともに、何ビット目から何ビット目までのバーナム暗号鍵が使用できる状態で残っているかを示す情報を端末装置Ａ１０２へ送信する。一方、共通部分が１度に暗号化する単位データ量を超えていなければ、端末装置Ｂ１０３は、バーナム暗号通信拒否メッセージを返す。

端末装置Ａ１０２は、バーナム暗号通信了承メッセージを受信した場合、端末装置Ａ１０２が保有するバーナム暗号鍵と端末装置Ｂ１０３が保有するバーナム暗号鍵との共通部分を特定する。そして、特定した共通部分のバーナム暗号鍵で通信データのうち単位データ量分のデータを暗号化して、暗号化データを生成し、端末装置Ｂ１０３へ送信する。

また、端末装置Ａ１０２は、未送信の通信データがある場合、共通部分のバーナム暗号鍵の残りで暗号通信を行うことができるデータ量が、１度に暗号化する単位データ量を超えているかを確認する。超えていれば、バーナム暗号による暗号通信を行い、超えていなければ、ブロック暗号による暗号通

信に切り替える。

[0175] 実施の形態１０.

実施の形態４では、ブロック暗号鍵を複数保持しておき、暗号通信に利用しているブロック暗号鍵を定期的に破棄し、新しいブロック暗号鍵を使って暗号通信を行うことについて説明した。実施の形態４においては、端末装置が鍵共有装置と接続されていることを前提として説明した。

しかし、実施の形態９で説明したように、例えば、端末装置が携帯端末である場合では、端末装置と鍵共有装置が接続されていない状況も起こりうる。この場合、鍵共有装置から端末装置へのバーナム暗号鍵又はブロック暗号鍵の転送処理を行う時期や頻度が、端末装置間で一致していないことにより、端末装置間で保有している暗号鍵が異なっている場合があり得る。また、端末装置間での通信エラーなどにより、バーナム暗号鍵及びブロック暗号鍵の消費にずれが生じる可能性もある。そのため、通信開始時に暗号通信に用いる暗号鍵を確定させておく必要がある。

そこで、実施の形態１０では、暗号通信を行う前に端末装置間で互いの保有しているブロック暗号鍵の個数を共有し、互いの保有しているブロック暗号鍵の状況に応じて暗号通信の切り替えを行うことについて説明する。

[0176] まず、実施の形態１０において、端末装置Ａ１０２と端末装置Ｂ１０３とがバーナム暗号による暗号通信を開始し、バーナム暗号鍵が不足した時点からブロック暗号による暗号通信に方式の切り替えを行う場合の処理について説明する。

図４４及び図４５は、実施の形態１０における図２２の通信処理の流れを示すフローチャートである。図４４及び図４５に示す処理では、実施の形態４における図２３及び図２４の処理に加えて、事前にブロック暗号鍵の情報を端末装置間で共有する処理が行われる。

なお、実施の形態１０では、実施の形態４と同様、図２２に示すように、各ブロック暗号鍵は識別番号により識別されるものとする。

[0177] Ｓ１５０１からＳ１５１３までの処理は、図２３に示すＳ７０１からＳ７

１３までの処理（図５に示すＳ１０１からＳ１１３までの処理）と同様であるため、説明を省略する。

[0178] バーナム暗号で暗号通信を行うことができるデータ量が、１度に暗号化する単位データ量を超えている場合（Ｓ１５１３でＹＥＳ）、端末装置Ａ１０２は識別番号何番から何番までのブロック暗号鍵を保有しているかを確認する（Ｓ１５１４）。そして、端末装置Ａ１０２は、ブロック暗号切替要求メッセージ２２１２と共に、保有しているブロック暗号鍵の識別番号を端末装置Ｂ１０３へ送信する（Ｓ１５１５）。

端末装置Ｂ１０３は、ブロック暗号切替要求メッセージ２２１２とブロック暗号鍵の識別番号とを受信する（Ｓ１５１６）。すると、端末装置Ｂ１０３は、保有しているブロック暗号鍵の識別番号を確認し（Ｓ１５１７）、暗号通信で利用するブロック暗号鍵を確定する（Ｓ１５１８）。例えば、端末装置Ｂ１０３は、端末装置Ａ１０２と端末装置Ｂ１０３との両方が保有しているブロック暗号鍵のうち、最も識別番号の小さいブロック暗号鍵を暗号通信で利用するブロック暗号鍵として確定する。そして、端末装置Ｂ１０３は、ブロック暗号切替了承メッセージ２２１３とともに、確定したブロック暗号鍵の識別番号を端末装置Ａ１０２へ送信する（Ｓ１５１９）。

[0179] 端末装置Ａ１０２は、ブロック暗号切替了承メッセージ２２１３と、確定したブロック暗号鍵の識別番号とを受信する（Ｓ１５２０）。すると、端末装置Ａ１０２は、受信した識別番号が示すブロック暗号鍵で通信データを暗号化して、暗号化通信データ２２１４を生成する（Ｓ１５２１）。そして、端末装置Ａ１０２は、暗号化通信データ２２１４を端末装置Ｂ１０３へ送信する（Ｓ１５２２）。

端末装置Ｂ１０３は、暗号化通信データ２２１４を受信する（Ｓ１５２３）。すると、端末装置Ｂ１０３は、（Ｓ１５１８）で確定した識別番号のブロック暗号鍵で暗号化通信データ２２１４を復号し、通信データを得る（Ｓ１５２４）。

[0180] Ｓ１５２５からＳ１５３０までの処理は、Ｓ７２２からＳ７２７までの処

理と同様であるため、説明を省略する。

[0181] 次に、通信開始時点で受信側端末装置のバーナム暗号鍵が不足しており、バーナム暗号による暗号通信が開始できない時に、ブロック暗号による暗号通信を開始する場合の動作概要について説明する。

図４６は、実施の形態１０における図２５の通信処理の流れを示すフローチャートである。図４６に示す処理では、実施の形態４における図２６の処理に加えて、事前にブロック暗号鍵の情報を端末装置間で共有する処理が行われる。

[0182] 端末装置Ａ１０２は、保有しているバーナム暗号鍵の量を確認し、バーナム暗号鍵が不足していることを把握する（Ｓ１６０１）。なお、バーナム暗号で暗号通信を行うことができるデータ量が、１度に暗号化する単位データ量未満である場合に、バーナム暗号鍵が不足していると判定する。すると、端末装置Ａ１０２は、端末装置Ａ１０２は識別番号何番から何番までのブロック暗号鍵を保有しているかを確認する（Ｓ１６０２）。そして、端末装置Ａ１０２は、ブロック暗号切替要求メッセージ２５０７と共に、保有しているブロック暗号鍵の識別番号を端末装置Ｂ１０３へ送信する（Ｓ１６０３）。

端末装置Ｂ１０３は、ブロック暗号切替要求メッセージ２５０７とブロック暗号鍵の識別番号とを受信する（Ｓ１６０４）。すると、端末装置Ｂ１０３は、保有しているブロック暗号鍵の識別番号を確認し（Ｓ１６０５）、暗号通信で利用するブロック暗号鍵を確定する（Ｓ１６０６）。例えば、端末装置Ｂ１０３は、端末装置Ａ１０２と端末装置Ｂ１０３との両方が保有しているブロック暗号鍵のうち、最も識別番号の小さいブロック暗号鍵を暗号通信で利用するブロック暗号鍵として確定する。そして、端末装置Ｂ１０３は、ブロック暗号切替了承メッセージ２５０８とともに、確定したブロック暗号鍵の識別番号を端末装置Ａ１０２へ送信する（Ｓ１６０７）。

[0183] 端末装置Ａ１０２は、ブロック暗号切替了承メッセージ２５０８と、確定したブロック暗号鍵の識別番号とを受信する（Ｓ１６０８）。すると、端末

装置Ａ１０２は、受信した識別番号が示すブロック暗号鍵で通信データを暗号化して、暗号化通信データ２５０９を生成する（Ｓ１６０９）。そして、端末装置Ａ１０２は、暗号化通信データ２５０９を端末装置Ｂ１０３へ送信する（Ｓ１６１０）。

端末装置Ｂ１０３は、暗号化通信データ２５０９を受信する（Ｓ１６１１）。すると、端末装置Ｂ１０３は、（Ｓ１６０６）で確定した識別番号のブロック暗号鍵で暗号化通信データ２５０９を復号し、通信データを得る（Ｓ１６１２）。

[0184] Ｓ１６１３からＳ１６１８までの処理は、図２６のＳ８１０からＳ８１５までの処理と同様であるため、説明を省略する。

[0185] 次に、送信側の端末装置である端末装置Ａ１０２の処理について詳しく説明する。

図４７は、実施の形態１０における端末装置８０１の送信制御部８０３の処理の流れを示すフローチャートである。

[0186] Ｓ１７０１からＳ１７０８までの処理は、図９に示すＳ３０１からＳ３０８までの処理と同様であるため、説明を省略する。

[0187] Ｓ１７０９～１７１１の処理について説明する。

送信制御部８０３は、ブロック暗号鍵記憶部８１４が記憶したブロック暗号鍵の識別番号を確認する（Ｓ１７０９）。送信制御部８０３は、通信インターフェイス８０２を介して、ブロック暗号切替要求メッセージとともに、ブロック暗号鍵記憶部８１４が記憶したブロック暗号鍵の識別番号を端末装置Ｂ１０３へ送信する（Ｓ１７１０）。そして、送信制御部８０３は、端末装置Ｂ１０３から、ブロック暗号切替了承メッセージとともに、暗号通信で利用するブロック暗号鍵の識別番号を受信し（Ｓ１７１１）、Ｓ１７１５に処理を進める。

[0188] Ｓ１７１２からＳ１７１４の処理について説明する。

送信制御部８０３は、ブロック暗号鍵記憶部８１４が記憶したブロック暗号鍵の識別番号を確認する（Ｓ１７１２）。送信制御部８０３は、通信イン

ターフェイス８０２を介して、ブロック暗号通信要求メッセージとともに、ブロック暗号鍵記憶部８１４が記憶したブロック暗号鍵の識別番号を端末装置Ｂ１０３へ送信する（Ｓ１７１３）。そして、送信制御部８０３は、端末装置Ｂ１０３から、ブロック暗号通信了承メッセージとともに、暗号通信で利用するブロック暗号鍵の識別番号を受信し（Ｓ１７１４）、Ｓ１７１５に処理を進める。

[0189] Ｓ１７１５以降の処理について説明する。

送信制御部８０３は、Ｓ１７１１やＳ１７１４で受信した識別番号のブロック暗号鍵で、ブロック暗号化部８０８に通信データのうち単位データ量分のデータを暗号化させ、暗号化通信データを取得する（Ｓ１７１５）。そして、送信制御部８０３は、暗号化通信データを端末装置Ｂ１０３へ送信する（Ｓ１７１６）。

続いて、送信制御部８０３は、未送信の通信データの有無を確認する（Ｓ１７１７）。未送信の通信データがなければ（Ｓ１７１７でＮＯ）、送信制御部８０３は処理を終了する。一方、未送信の通信データがあれば（Ｓ１７１７でＹＥＳ）、送信制御部８０３はＳ１７１５へ処理を戻す。

[0190] 次に、受信側の端末装置である端末装置Ｂ１０３の処理について詳しく説明する。

図４８は、実施の形態１０における端末装置８０１の受信制御部８０４の処理の流れを示すフローチャートである。

[0191] Ｓ１８０１からＳ１８０７までの処理は、図１０に示すＳ４０１からＳ４０７までの処理と同様であるため、説明を省略する。

[0192] Ｓ１８０８～１８１１の処理について説明する。

受信制御部８０４は、端末装置Ａ１０２からブロック暗号切替要求メッセージと、端末装置Ａ１０２が保有するブロック暗号鍵の識別番号とを受信する（Ｓ１８０８）。受信制御部８０４は、ブロック暗号鍵記憶部８１４が記憶したブロック暗号鍵の識別番号を確認する（Ｓ１８０９）。受信制御部８０４は、（Ｓ１８０８）で受信した端末装置Ａ１０２が保有するブロック暗

号鍵の識別番号と、（Ｓ１８０９）で確認した端末装置Ｂ１０３が保有するブロック暗号鍵の識別番号とから暗号通信で用いるブロック暗号鍵を確定する（Ｓ１８１０）。そして、受信制御部８０４は、通信インターフェイス８０２を介して、ブロック暗号切替了承メッセージとともに、確定したブロック暗号鍵の識別番号を端末装置Ａ１０２へ送信し（Ｓ１８１１）、Ｓ１８１５に処理を進める。

[0193] Ｓ１８１２からＳ１８１４の処理について説明する。

受信制御部８０４は、ブロック暗号鍵記憶部８１４が記憶したブロック暗号鍵の識別番号を確認する（Ｓ１８１２）。受信制御部８０４は、（Ｓ１８０２）で受信した端末装置Ａ１０２が保有するブロック暗号鍵の識別番号と、（Ｓ１８１２）で確認した端末装置Ｂ１０３が保有するブロック暗号鍵の識別番号とから暗号通信で用いるブロック暗号鍵を確定する（Ｓ１８１３）。そして、受信制御部８０４は、通信インターフェイス８０２を介して、ブロック暗号通信了承メッセージとともに、確定したブロック暗号鍵の識別番号を端末装置Ａ１０２へ送信し（Ｓ１８１４）、Ｓ１８１５に処理を進める。

[0194] Ｓ１８１５以降の処理について説明する。

受信制御部８０４は、端末装置Ａ１０２から暗号化通信データを受信する（Ｓ１８１５）。受信制御部８０４は、受信した暗号化通信データをブロック復号部８０９に送信して、Ｓ１８１０やＳ１８１３で確定した識別番号のブロック暗号鍵で復号させ通信データを生成させる（Ｓ１８１６）。生成された通信データは、受信データ記憶部８１２に記憶される。

続いて、受信制御部８０４は、未受信の通信データの有無を確認する（Ｓ１８１７）。未受信の通信データがなければ（Ｓ１８１７でＮＯ）、受信制御部８０４は処理を終了する。一方、未受信の通信データがあれば（Ｓ１８１７でＹＥＳ）、受信制御部８０４はＳ１８１５へ処理を戻す。

[0195] 以上のように、実施の形態１０に係る暗号化システム１では、端末装置間で互いの保有しているブロック暗号鍵の分量を共有することで、保有するブ

ロック暗号鍵に差異がある場合であっても、暗号方式の切り替えを行うことができる。

[0196] 実施の形態１１.

実施の形態５では、ブロック暗号鍵が残り１つとなった時点でブロック暗号による暗号化を行う場合には、現在のブロック暗号鍵をハッシュ関数などのランダム化によって更新することについて説明した。実施の形態５においては、通信エラーなどにより、ブロック暗号鍵の更新回数が同期しなくなった場合に暗号通信が行えなくなる。

そこで、実施の形態１１では、暗号通信を行う前に端末装置間で互いの保有しているブロック暗号鍵の更新回数を共有し、互いの保有しているブロック暗号鍵の更新回数を同期することについて説明する。

[0197] まず、通信開始時点で受信側端末装置のバーナム暗号鍵が不足しており、バーナム暗号による暗号通信が開始できない時に、ブロック暗号による暗号通信を開始する場合の動作概要について説明する。

図４９は、実施の形態１１における図２８の通信処理の流れを示すフローチャートである。図４９に示す処理では、実施の形態５における図２９の処理に加えて、事前にブロック暗号鍵の更新回数を端末装置間で共有する処理が行われる。

[0198] 端末装置Ａ１０２は、保有しているバーナム暗号鍵の量を確認し、バーナム暗号鍵が不足していることを把握する（Ｓ１９０１）。なお、バーナム暗号で暗号通信を行うことができるデータ量が、１度に暗号化する単位データ量未満である場合に、バーナム暗号鍵が不足していると判定する。すると、端末装置Ａ１０２は、保有しているブロック暗号鍵の更新回数を確認する（Ｓ１９０２）。そして、端末装置Ａ１０２は、ブロック暗号通信要求メッセージ２８０１とともに、ブロック暗号鍵の更新回数を端末装置Ｂ１０３へ送信する（Ｓ１９０３）。

端末装置Ｂ１０３は、端末装置Ａ１０２からブロック暗号通信要求メッセージ２８０１と、ブロック暗号鍵の更新回数とを受信する（Ｓ１９０４）。

すると、端末装置Ｂ１０３は、保有しているブロック暗号鍵の更新回数を確認する（Ｓ１９０５）。端末装置Ｂ１０３は、暗号通信で用いるブロック暗号鍵の更新回数を確定する（Ｓ１９０６）。例えば、端末装置Ｂ１０３は、ブロック暗号鍵について、端末装置Ａ１０２における更新回数と端末装置Ｂ１０３における更新回数とのうち、多いほうの更新回数を、暗号通信で利用するブロック暗号鍵の更新回数として確定する。そして、端末装置Ｂ１０３は、ブロック暗号通信了承メッセージ２８０４とともに、確定したブロック暗号鍵の更新回数を端末装置Ａ１０２へ送信する（Ｓ１９０７）。

また、端末装置Ｂ１０３は、（Ｓ１９０６）で確定したブロック暗号鍵について、確定した更新回数になっていない場合、確定した更新回数になるまで更新処理を繰り返し実行する（Ｓ１９０８）。これにより、ブロック暗号鍵が暗号通信で使用する状態になる。なお、確定した更新回数になっていない場合とは、確定した更新回数よりも、更新回数が少ない場合という意味である。

[0199] 端末装置Ａ１０２は、ブロック暗号切替了承メッセージ２８０４と、確定したブロック暗号鍵の更新回数とを受信する（Ｓ１９０９）。端末装置Ａ１０２は、ブロック暗号鍵が受信した更新回数になっていない場合、受信した更新回数になるまで更新処理を繰り返し実行する（Ｓ１９１０）。これにより、ブロック暗号鍵が暗号通信で使用する状態になる。なお、受信した更新回数になっていない場合とは、受信した更新回数よりも、更新回数が少ない場合という意味である。端末装置Ａ１０２は、暗号通信で使用する状態のブロック暗号鍵で通信データを暗号化して、暗号化通信データ２８０４を生成する（Ｓ１９１１）。そして、端末装置Ａ１０２は、暗号化通信データ２８０４を端末装置Ｂ１０３へ送信する（Ｓ１９１２）。

端末装置Ｂ１０３は、暗号化通信データ２８０４を受信する（Ｓ１９１３）。すると、端末装置Ｂ１０３は、暗号通信で使用する状態のブロック暗号鍵で暗号化通信データ２８０４を復号し、通信データを得る（Ｓ１９１４）。

[0200] Ｓ１９１５からＳ１９２２までの処理は、図２９に示すＳ９１０からＳ９１７までの処理と同様であるため、説明を省略する。

[0201] 次に、送信側の端末装置である端末装置Ａ１０２の処理について詳しく説明する。

図５０は、実施の形態１１における端末装置８０１の送信制御部８０３の処理の流れを示すフローチャートである。

[0202] Ｓ２００１からＳ２００８までの処理は、図９に示すＳ３０１からＳ３０８までの処理と同様であるため、説明を省略する。

[0203] 送信制御部８０３は、ブロック暗号鍵記憶部８１４が記憶したブロック暗号鍵の更新回数とを確認する（Ｓ２００９）。送信制御部８０３は、通信インターフェイス８０２を介して、ブロック暗号切替要求メッセージとともに、ブロック暗号鍵記憶部８１４が記憶したブロック暗号鍵の更新回数を端末装置Ｂ１０３へ送信する（Ｓ２０１０）。そして、送信制御部８０３は、端末装置Ｂ１０３から、ブロック暗号切替了承メッセージとともに、暗号通信で利用するブロック暗号鍵の更新回数を受信し（Ｓ２０１１）、Ｓ２０１５に処理を進める。

[0204] Ｓ２０１２からＳ２０１４の処理について説明する。

送信制御部８０３は、ブロック暗号鍵記憶部８１４が記憶したブロック暗号鍵の更新回数とを確認する（Ｓ２０１２）。送信制御部８０３は、通信インターフェイス８０２を介して、ブロック暗号通信要求メッセージとともに、ブロック暗号鍵記憶部８１４が記憶したブロック暗号鍵の更新回数を端末装置Ｂ１０３へ送信する（Ｓ２０１３）。そして、送信制御部８０３は、端末装置Ｂ１０３から、ブロック暗号通信了承メッセージとともに、暗号通信で利用するブロック暗号鍵の更新回数を受信し（Ｓ２０１４）、Ｓ２０１５に処理を進める。

[0205] Ｓ２０１５以降の処理について説明する。

送信制御部８０３は、ブロック暗号鍵について、Ｓ２０１１やＳ２０１４で受信した更新回数になっていない場合、受信した更新回数になるまで更新

処理を繰り返し実行する（Ｓ２０１５）。これにより、ブロック暗号鍵が暗号通信で使用する状態になる。送信制御部８０３は、暗号通信で使用する状態のブロック暗号鍵で、ブロック暗号化部８０８に通信データのうち単位データ量分のデータを暗号化させ、暗号化通信データを取得する（Ｓ２０１６）。そして、送信制御部８０３は、暗号化通信データを端末装置Ｂ１０３へ送信する（Ｓ２０１７）。

続いて、送信制御部８０３は、未送信の通信データの有無を確認する（Ｓ２０１８）。未送信の通信データがなければ（Ｓ２０１８でＮＯ）、送信制御部８０３は処理を終了する。一方、未送信の通信データがあれば（Ｓ２０１８でＹＥＳ）、送信制御部８０３はＳ２０１６へ処理を戻す。

[0206] 次に、受信側の端末装置である端末装置Ｂ１０３の処理について詳しく説明する。

図５１は、実施の形態１１における端末装置８０１の受信制御部８０４の処理の流れを示すフローチャートである。

[0207] Ｓ２１０１からＳ２１０７までの処理は、図１０に示すＳ４０１からＳ４０７までの処理と同様であるため、説明を省略する。

[0208] Ｓ２１０８～２１１１の処理について説明する。

受信制御部８０４は、端末装置Ａ１０２からブロック暗号切替要求メッセージと、端末装置Ａ１０２が保有するブロック暗号鍵の更新回数とを受信する（Ｓ２１０８）。受信制御部８０４は、ブロック暗号鍵記憶部８１４が記憶したブロック暗号鍵の更新回数を確認する（Ｓ２１０９）。受信制御部８０４は、（Ｓ２１０８）で受信した端末装置Ａ１０２が保有するブロック暗号鍵の更新回数と、（Ｓ２１０９）で確認した端末装置Ｂ１０３が保有するブロック暗号鍵の更新回数とから暗号通信で用いるブロック暗号鍵及びその更新回数を確定する（Ｓ２１１０）。そして、受信制御部８０４は、通信インターフェイス８０２を介して、ブロック暗号切替了承メッセージとともに、確定したブロック暗号鍵の更新回数を端末装置Ａ１０２へ送信し（Ｓ２１１１）、Ｓ２１１５に処理を進める。

[0209] Ｓ２１１２からＳ２１１４の処理について説明する。

受信制御部８０４は、ブロック暗号鍵記憶部８１４が記憶したブロック暗号鍵の更新回数を確認する（Ｓ２１１２）。受信制御部８０４は、（Ｓ２１０２）で受信した端末装置Ａ１０２が保有するブロック暗号鍵の更新回数と、（Ｓ２１１２）で確認した端末装置Ｂ１０３が保有するブロック暗号鍵の更新回数とから暗号通信で用いるブロック暗号鍵及びその更新回数を確定する（Ｓ２１１３）。そして、受信制御部８０４は、通信インターフェイス８０２を介して、ブロック暗号通信了承メッセージとともに、確定したブロック暗号鍵の更新回数を端末装置Ａ１０２へ送信し（Ｓ２１１４）、Ｓ２１１５に処理を進める。

[0210] Ｓ２１１５以降の処理について説明する。

受信制御部８０４は、ブロック暗号鍵について、Ｓ２１１０やＳ２１１３で確定した更新回数になっていない場合、確定した更新回数になるまで更新処理を繰り返し実行する（Ｓ２１１５）。これにより、ブロック暗号鍵が暗号通信で使用する状態になる。受信制御部８０４は、端末装置Ａ１０２から暗号化通信データを受信する（Ｓ２１１６）。受信制御部８０４は、受信した暗号化通信データをブロック復号部８０９に送信して、暗号通信で使用する状態のブロック暗号鍵で復号させ通信データを生成させる（Ｓ２１１７）。生成された通信データは、受信データ記憶部８１２に記憶される。

続いて、受信制御部８０４は、未受信の通信データの有無を確認する（Ｓ２１１８）。未受信の通信データがなければ（Ｓ２１１８でＮＯ）、受信制御部８０４は処理を終了する。一方、未受信の通信データがあれば（Ｓ２１１８でＹＥＳ）、受信制御部８０４はＳ２１１６へ処理を戻す。

[0211] 以上のように、実施の形態１１に係る暗号化システム１では、端末装置間で互いの保有しているブロック暗号鍵の更新回数を共有することで、保有するブロック暗号鍵の更新回数に差異がある場合であっても、暗号方式の切り替えを行うことができる。

[0212] 実施の形態１２.

通常、バーナム暗号鍵及びブロック暗号鍵は未使用時には不揮発性メモリなどに保存されている。実施の形態１２では、バーナム暗号鍵及びブロック暗号鍵を、使用する直前にＲＡＭなどの揮発性メモリにロードし、不揮発性メモリからは消去する。これにより、不正な電源遮断などによって、すでに使用したバーナム暗号鍵及びブロック暗号鍵を取り出されることを防止する。

[0213] 通常、バーナム暗号鍵及びブロック暗号鍵（以下、この実施の形態においては暗号鍵と呼ぶ）は、装置の電源が遮断された場合でも、装置内で保持されている必要がある。そのため、未使用の暗号鍵はＨＤＤ等の不揮発性の記憶装置に保存されることになる。

[0214] 実施の形態１２においては、暗号化通信データを不正者により復号されることを防ぐため、暗号鍵による暗号化もしくは復号が完了した後、暗号化や復号に使用した暗号鍵を消去し、再度同じ装置内で同じ暗号鍵を用いないこととする。

ところが、暗号化もしくは復号処理が開始されてから完了する前に、装置の電源を遮断すると、暗号鍵の消去処理が正常に行われない場合がある。特に、この場合、暗号化通信データが通信路を流れており、かつ、装置内に暗号鍵が残る状態が発生し得る。この状態では、装置から暗号鍵を不正に抜き取られ、暗号化通信データを復号されてしまう危険性がある。

[0215] 図５２は、実施の形態１２における端末装置の動作の説明図である。

図５２に示すように、端末装置は、未使用時にはＨＤＤ等の不揮発性の記憶装置に保存している暗号鍵を、使用する直前に揮発性メモリにロードし、ＨＤＤや不揮発性メモリにある暗号鍵を消去する。これにより、装置の電源を遮断されたとしても装置内には暗号鍵が残留することがないため、不正な抜き取りによって暗号鍵が露見することがなく、暗号化通信データを復号される危険性がない。

[0216] 例えば、バーナム暗号鍵記憶部８１３やブロック暗号鍵記憶部８１４は、ＨＤＤ等の不揮発性の記憶装置である。

送信制御部８０３や受信制御部８０４から暗号化や復号の指示を受けたバーナム暗号化部８０６、バーナム復号部８０７、ブロック暗号化部８０８、ブロック復号部８０９は、バーナム暗号鍵記憶部８１３やブロック暗号鍵記憶部８１４から暗号鍵を取得する。すると、バーナム暗号化部８０６、バーナム復号部８０７、ブロック暗号化部８０８、ブロック復号部８０９は、取得した暗号鍵をＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）等の揮発性の記憶装置に記憶するとともに、取得した暗号鍵をバーナム暗号鍵記憶部８１３やブロック暗号鍵記憶部８１４から削除する。そして、バーナム暗号化部８０６、バーナム復号部８０７、ブロック暗号化部８０８、ブロック復号部８０９は、揮発性の記憶装置に記憶した暗号鍵で暗号化や復号を行う。

[0217] 実施の形態１３.

実施の形態１３では、バーナム暗号鍵及びブロック暗号鍵の残量や、現在の暗号通信に使われている暗号方式や、暗号方式が切り替わる時を通知することについて説明する。これにより、端末装置の利用者が現在の暗号通信及び暗号鍵の状況を直感的に把握することを可能にする。

[0218] 通常、バーナム暗号鍵及びブロック暗号鍵（以下、この実施の形態においては暗号鍵と呼ぶ）は、端末装置内で保有されているため、その情報を利用者が把握することは容易ではない。また、暗号通信における暗号化処理、復号処理についても端末装置内で行われるものである。そのため、例えば、バーナム暗号鍵の不足によって、バーナム暗号による暗号通信からブロック暗号による暗号通信に切り替わった時に、暗号方式の切り替えを利用者が把握することは容易ではない。

暗号方式の切り替えは、暗号通信の安全性が変化することを意味している。また、暗号鍵の残量は暗号方式の切り替えが起こるまでの期間を示す指標となるものである。そのため、これらの情報を利用者が把握できることは重要である。そこで、実施の形態１３では、暗号通信中に、現在の暗号鍵の残量と暗号方式とを画面表示、音及び端末の振動によって、利用者に通知する

。

[0219] まず、実施の形態１３における端末装置Ａ１０２及び端末装置Ｂ１０３の機能について説明する。

図５３は、実施の形態１３における端末装置Ａ１０２及び端末装置Ｂ１０３の機能構成を説明する機能ブロック図である。図５３に示す端末装置は、図８に示す端末装置が備える機能に加え、暗号鍵残量通知制御部８２０（残量通知部）、暗号方式通知制御部８２１（残量通知部）、画面表示制御部８２２、音声出力制御部８２３、振動制御部８２４、ディスプレイ８２５、スピーカー８２６及び振動装置８２７を備える。

[0220] 暗号鍵残量通知制御部８２０は、バーナム暗号鍵記憶部８１３からバーナム暗号鍵の残量情報を取得し、ブロック暗号鍵記憶部８１４からブロック暗号鍵の残量情報を取得する。そして、暗号鍵残量通知制御部８２０は、取得したバーナム暗号鍵の残量情報とブロック暗号鍵の残量情報とを、利用者に暗号鍵の残量を通知するための通知情報に処理装置により変換して、画面表示制御部８２２、音声出力制御部８２３、振動制御部８２４に送る。

[0221] 暗号方式通知制御部８２１は、送信制御部８０３、受信制御部８０４から、現在使用している暗号方式を示す情報を取得する。そして、暗号方式通知制御部８２１は、取得した暗号方式を示す情報を、利用者に暗号方式を通知するための情報に変換して、画面表示制御部８２２、音声出力制御部８２３、振動制御部８２４に送る。また、暗号方式通知制御部８２１は、暗号方式が切り替わった場合には、暗号方式が切り替わったことを示す情報を画面表示制御部８２２、音声出力制御部８２３、振動制御部８２４に送る。

[0222] 画面表示制御部８２２は、暗号鍵残量通知制御部８２０及び暗号方式通知制御部８２１から受け取った情報より、ディスプレイ８２５に対して、画面表示を指示する。

音声出力制御部８２３は、暗号鍵残量通知制御部８２０及び暗号方式通知制御部８２１から受け取った情報より、スピーカー８２６に対して、音声出力を指示する。

振動制御部８２４は、暗号鍵残量通知制御部８２０及び暗号方式通知制御部８２１から受け取った情報より、振動装置８２７に対して、端末を振動させるように指示する。

ディスプレイ８２５は、液晶ディスプレイなどの画面に絵や文字を表示することができる機器である。

スピーカー８２６は、音声出力が可能な機器である。

振動装置８２７は、端末を振動させることができる装置である。

[0223] 例えば、暗号鍵残量通知制御部８２０は、バーナム暗号鍵の残量やブロック暗号鍵の残量を、常時、数値等によりディスプレイ８２５に表示させておく。そして、暗号鍵残量通知制御部８２０は、バーナム暗号鍵が事前に決められた所定の量より少なくなり、実施の形態６で説明した増大処理が実行された場合、そのことを示す情報をディスプレイ８２５に表示するとともに、スピーカー８２６から音を出力させ、振動装置８２７を振動させる。また、暗号方式通知制御部８２１は、バーナム暗号からブロック暗号に暗号方式が切り替えられた場合、そのことを示す情報をディスプレイ８２５に表示するとともに、スピーカー８２６から音を出力させ、振動装置８２７を振動させる。さらに、暗号鍵残量通知制御部８２０は、最後の１つのブロック暗号鍵が使用され、実施の形態５で説明したブロック暗号鍵のランダム化が行われた場合、そのことを示す情報をディスプレイ８２５に表示するとともに、スピーカー８２６から音を出力させ、振動装置８２７を振動させる。

つまり、暗号鍵残量通知制御部８２０と暗号方式通知制御部８２１とは、暗号鍵の変換や暗号方式の切り替えが行われ、暗号通信の安全性が低下する度に、そのことを利用者へ通知する。

例えば、暗号鍵の変換や暗号方式の切り替えが行われる度に、使用される暗号鍵や暗号方式に応じて、ディスプレイ８２５に表示させる情報の色や表示させる文字、記号、図形や、音の種類、音の長さや、振動の種類、振動の間隔を変化させてもよい。

[0224] なお、暗号鍵残量通知制御部８２０と暗号方式通知制御部８２１とは、暗

号鍵の変換や暗号方式の切り替えが行われ、暗号通信の安全性が低下する前に、もうすぐ暗号鍵の変換や暗号方式の切り替えが行われることを利用者へ通知してもよい。これにより、例えば、利用者にバーナム暗号鍵を鍵共有装置から取得するように促すことができる。

[0225] 実施の形態１４.

実施の形態１４では、上述した実施の形態における暗号通信の実現方法について説明する。

[0226] 実装の形態１～１３における、暗号通信を行う前までの通信処理は、ＳＩＰ（Ｓｅｓｓｉｏｎ Ｉｎｉｔｉａｔｉｏｎ Ｐｒｏｔｏｃｏｌ）で実現できる。

具体的には、ＳＩＰのシーケンスに従い、バーナム暗号通信要求メッセージ、ブロック暗号通信要求メッセージをＩＮＶＩＴＥメッセージで行い、暗号鍵の情報などはＳＤＰ（Ｓｅｓｓｉｏｎ Ｄｅｓｃｒｉｐｔｉｏｎ Ｐｒｏｔｏｃｏｌ）で記述する。バーナム暗号通信了承メッセージ、ブロック暗号通信了承メッセージは２００ ＯＫを示す応答メッセージで行い、ＩＮＶＩＴＥメッセージと同様に暗号鍵の情報などはＳＤＰで記述する。一方、バーナム暗号通信拒否メッセージは、４８８ Ｎｏｔ Ａｃｃｅｐｔａｂｌｅを示す応答メッセージで行う。

また、暗号通信及び暗号通信中の暗号方式の切り替えなどはＳＲＴＰ（Ｓｅｃｕｒｅ Ｒｅａｌ－Ｔｉｍｅ Ｐｒｏｔｏｃｏｌ）で実現できる。

つまり、ＳＩＰに従ったネゴシエーションにより、開始する暗号方式と暗号鍵を決定し、ＳＲＴＰに従った通信により、暗号通信と暗号方式の切り替えを実現することができる。

[0227] 以上の実施の形態における端末装置８０１のハードウェア構成について説明する。

図５４は、端末装置８０１のハードウェア構成の一例を示す図である。

図５４に示すように、端末装置８０１は、プログラムを実行するＣＰＵ９１１（Ｃｅｎｔｒａｌ・Ｐｒｏｃｅｓｓｉｎｇ・Ｕｎｉｔ、中央処理装置、

処理装置、演算装置、マイクロプロセッサ、マイクロコンピュータ、プロセッサともいう）を備えている。ＣＰＵ９１１は、バス９１２を介してＲＯＭ９１３、ＲＡＭ９１４、ディスプレイ８２５、キーボード９０２（Ｋ／Ｂ）、スピーカー８２６、振動装置８２７、通信ボード９１５（通信インターフェイス８０２の一例）、磁気ディスク装置９２０（ＨＤＤ，固定ディスク装置）と接続され、これらのハードウェアデバイスを制御する。磁気ディスク装置９２０の代わりに、光ディスク装置、メモリカード読み書き装置などの記憶装置でもよい。磁気ディスク装置９２０は、所定の固定ディスクインタフェースを介して接続される。

[0228] 磁気ディスク装置９２０又はＲＯＭ９１３などには、オペレーティングシステム９２１（ＯＳ）、ウィンドウシステム９２２、プログラム群９２３、ファイル群９２４が記憶されている。プログラム群９２３のプログラムは、ＣＰＵ９１１、オペレーティングシステム９２１、ウィンドウシステム９２２により実行される。

[0229] プログラム群９２３には、上記の説明において「送信制御部８０３」、「受信制御部８０４」、「バーナム暗号鍵管理部８０５」、「バーナム暗号化部８０６」、「バーナム復号部８０７」、「ブロック暗号化部８０８」、「ブロック復号部８０９」、「バーナム暗号鍵取得部８１０」、「ブロック暗号鍵取得部８１５」、「暗号鍵変換部８１６」、「ブロック暗号鍵更新部８１７」、「ハッシュ関数処理部８１８」、「バーナム暗号鍵増大部８１９」、「暗号鍵残量通知制御部８２０」、「暗号方式通知制御部８２１」、「画面表示制御部８２２」、「音声出力制御部８２３」等として説明した機能を実行するソフトウェアやプログラムやその他のプログラムが記憶されている。プログラムは、ＣＰＵ９１１により読み出され実行される。

ファイル群９２４には、上記の説明において「送信データ記憶部８１１」、「受信データ記憶部８１２」、「バーナム暗号鍵記憶部８１３」、「ブロック暗号鍵記憶部８１４」に格納される情報やデータや信号値や変数値やパラメータが、「データベース」の各項目として記憶される。「データベース

」は、ディスクやメモリなどの記録媒体に記憶される。ディスクやメモリなどの記憶媒体に記憶された情報やデータや信号値や変数値やパラメータは、読み書き回路を介してＣＰＵ９１１によりメインメモリやキャッシュメモリに読み出され、抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示などのＣＰＵ９１１の動作に用いられる。抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示のＣＰＵ９１１の動作の間、情報やデータや信号値や変数値やパラメータは、メインメモリやキャッシュメモリやバッファメモリに一時的に記憶される。

[0230] なお、鍵共有装置１１０１も、端末装置８０１と同様に、プログラムを実行するＣＰＵ９１１を備えている。ＣＰＵ９１１は、バス９１２を介してＲＯＭ９１３、ＲＡＭ９１４、キーボード９０２（Ｋ／Ｂ）、通信ボード９１５（通信インターフェイス１１０２の一例）、磁気ディスク装置９２０と接続され、これらのハードウェアデバイスを制御する。

[0231] 磁気ディスク装置９２０又はＲＯＭ９１３などには、オペレーティングシステム９２１（ＯＳ）、ウィンドウシステム９２２、プログラム群９２３、ファイル群９２４が記憶されている。プログラム群９２３のプログラムは、ＣＰＵ９１１、オペレーティングシステム９２１、ウィンドウシステム９２２により実行される。

[0232] プログラム群９２３には、上記の説明において「バーナム暗号鍵共有部１１０３」、「バーナム暗号鍵転送部１１０４」、「ブロック暗号鍵共有部１１０６」、「ブロック暗号鍵転送部１１０７」等として説明した機能を実行するソフトウェアやプログラムやその他のプログラムが記憶されている。

ファイル群９２４には、上記の説明において「バーナム暗号鍵記憶部１１０５」、「ブロック暗号鍵記憶部１１０８」に格納される情報やデータや信号値や変数値やパラメータが、「データベース」の各項目として記憶される。

[0233] また、上記の説明におけるフローチャートの矢印の部分は主としてデータや信号の入出力を示し、データや信号値は、ＲＡＭ９１４のメモリ、その他

光ディスク等の記録媒体やＩＣチップに記録される。また、データや信号は、バス９１２や信号線やケーブルその他の伝送媒体や電波によりオンライン伝送される。

また、上記の説明において「～部」として説明するものは、「～回路」、「～装置」、「～機器」、「～手段」、「～機能」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。また、「～装置」として説明するものは、「～回路」、「～機器」、「～手段」、「～機能」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。すなわち、「～部」として説明するものは、ＲＯＭ９１３に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェアのみ、或いは、素子・デバイス・基板・配線などのハードウェアのみ、或いは、ソフトウェアとハードウェアとの組合せ、さらには、ファームウェアとの組合せで実施されても構わない。ファームウェアとソフトウェアは、プログラムとして、ＲＯＭ９１３等の記録媒体に記憶される。プログラムはＣＰＵ９１１により読み出され、ＣＰＵ９１１により実行される。すなわち、プログラムは、上記で述べた「～部」としてコンピュータ等を機能させるものである。あるいは、上記で述べた「～部」の手順や方法をコンピュータ等に実行させるものである。

符号の説明

[0234] １０１，１０６　ネットワーク、１０２　端末装置Ａ、１０３　端末装置Ｂ、１０４　鍵共有装置Ｃ、１０５　鍵共有装置Ｄ、１０７，１０８　通信ケーブル、６０４　暗号化通信データ、８０１　端末装置、８０２　通信インターフェイス、８０３　送信制御部、８０４　受信制御部、８０５　バーナム暗号鍵管理部、８０６　バーナム暗号化部、８０７　バーナム復号部、８０８　ブロック暗号化部、８０９　ブロック復号部、８１０　バーナム暗号鍵取得部、８１１　送信データ記憶部、８１２　受信データ記憶部、８１３　バーナム暗号鍵記憶部、８１４　ブロック暗号鍵記憶部、８１５　ブロック暗号鍵取得部、８１６　暗号鍵変換部、８１７　ブロック暗号鍵更新部

、８１８　ハッシュ関数処理部、８１９　バーナム暗号鍵増大部、８２０　暗号鍵残量通知制御部、８２１　暗号方式通知制御部、８２２　画面表示制御部、８２３　音声出力制御部、８２４　振動制御部、８２５　ディスプレイ、８２６　スピーカー、８２７　振動装置、１１０１　鍵共有装置、１１０２　通信インターフェイス、１１０３　バーナム暗号鍵共有部、１１０４　バーナム暗号鍵転送部、１１０５　バーナム暗号鍵記憶部、１１０６　ブロック暗号鍵共有部、１１０７　ブロック暗号鍵転送部、１１０８　ブロック暗号鍵記憶部。

請求の範囲

[請求項1] ワンタイムパッド暗号で使用する、複数ビットからなるワンタイムパッド暗号鍵を記憶するワンタイムパッド暗号鍵記憶部と、

前記ワンタイムパッド暗号鍵記憶部が記憶したワンタイムパッド暗号鍵の一部を順に用いて、通信データをワンタイムパッド暗号により暗号化して暗号化データを生成するワンタイムパッド暗号化部と、

ブロック暗号で使用するブロック暗号鍵を記憶するブロック暗号鍵記憶部と、

前記ブロック暗号鍵記憶部が記憶したブロック暗号鍵を用いて、通信データをブロック暗号により暗号化して暗号化データを生成するブロック暗号化部と、

前記ワンタイムパッド暗号鍵記憶部が記憶したワンタイムパッド暗号鍵の残りビット数に応じて、通信データを前記ワンタイムパッド暗号化部に暗号化させるか、前記ブロック暗号化部に暗号化させるかを制御する暗号化制御部と

を備えることを特徴とする暗号化装置。

[請求項2] 前記暗号化制御部は、通信データを所定の単位データ毎に順次前記ワンタイムパッド暗号化部に暗号化させている場合に、前記ワンタイムパッド暗号鍵記憶部が記憶したワンタイムパッド暗号鍵のビット数が次に暗号化させる単位データのビット数より少なくなると、通信データを前記ブロック暗号化部に暗号化させるように切り替える

ことを特徴とする請求項１に記載の暗号化装置。

[請求項3] 前記暗号化制御部は、通信データを前記ブロック暗号化部に暗号化させている場合に、前記ワンタイムパッド暗号鍵記憶部が記憶したワンタイムパッド暗号鍵が前記単位データのビット数よりも多い所定の第１ビット数以上になると、通信データを前記ワンタイムパッド暗号化部に暗号化させるように切り替える

ことを特徴とする請求項２に記載の暗号化装置。

[請求項4] 前記暗号化制御部は、前記ワンタイムパッド暗号鍵記憶部が記憶したワンタイムパッド暗号鍵が通信開始時に前記単位データ量以上である場合、通信データを前記ワンタイムパッド暗号化部に暗号化させ、通信開始時に前記ワンタイムパッド暗号鍵記憶部が記憶したワンタイムパッド暗号鍵が前記単位データ量よりも少ない場合、通信データを前記ブロック暗号化部に暗号化させる

ことを特徴とする請求項２又は３に記載の暗号化装置。

[請求項5] 前記暗号化制御部は、さらに、通信データの送信先の端末が記憶したワンタイムパッド暗号鍵の残りビット数に応じて、通信データを前記ワンタイムパッド暗号化部に暗号化させるか、前記ブロック暗号化部に暗号化させるかを制御する

ことを特徴とする請求項１から４までのいずれかに記載の暗号化装置。

[請求項6] 前記暗号化装置は、さらに、

前記ワンタイムパッド暗号鍵記憶部が記憶したワンタイムパッド暗号鍵が予め定められた第２ビット数よりも少なくなった場合に、通信データの送信先の端末と予め共有した方法により、前記ワンタイムパッド暗号鍵記憶部が記憶したワンタイムパッド暗号鍵のビット数を増大させるワンタイムパッド暗号鍵増大部

を備えることを特徴とする請求項１から５までのいずれかに記載の暗号化装置。

[請求項7] 前記ワンタイムパッド暗号鍵増大部は、ワンタイムパッド暗号鍵のビット数を増大させる処理を所定の回数以上実行した場合には、ワンタイムパッド暗号鍵を増大させることを止める

ことを特徴とする請求項６に記載の暗号化装置。

[請求項8] 前記ワンタイムパッド暗号鍵増大部は、前記ワンタイムパッド暗号鍵記憶部が記憶したワンタイムパッド暗号鍵に対して、所定のビット毎に乱数値を挿入する方法により、ワンタイムパッド暗号鍵のビット

数を増大させる

ことを特徴とする請求項６又は７に記載の暗号化装置。

[請求項9] 前記ワンタイムパッド暗号鍵増大部は、前記ワンタイムパッド暗号鍵記憶部が記憶したワンタイムパッド暗号鍵を入力として、所定の乱数発生関数を計算する方法により発生した乱数値を新たなワンタイムパッド暗号鍵とする

ことを特徴とする請求項６又は７に記載の暗号化装置。

[請求項10] 前記暗号化装置は、さらに、

通信データの送信先の端末と予め共有した方法により、前記ワンタイムパッド暗号鍵記憶部が記憶したワンタイムパッド暗号鍵からブロック暗号鍵を生成する暗号鍵変換部

を備え、

前記ブロック暗号鍵記憶部は、前記暗号鍵変換部が生成したブロック暗号鍵を記憶する

ことを特徴とする請求項１から９までのいずれかに記載の暗号化装置。

[請求項11] 前記ブロック暗号鍵記憶部は、複数のブロック暗号鍵を記憶し、

前記暗号化装置は、さらに、

前記ブロック暗号化部が暗号化に用いた使用済のブロック暗号鍵を前記ブロック暗号鍵記憶部から削除するブロック暗号鍵更新部

を備えることを特徴とする請求項１から１０までのいずれかに記載の暗号化装置。

[請求項12] 前記暗号化装置は、さらに、

通信データの送信先の端末と予め共有した方法により、前記ブロック暗号鍵記憶部が記憶したブロック暗号鍵から新たなブロック暗号鍵を生成するブロック暗号鍵生成部

を備えることを特徴とする請求項１から１１までのいずれかに記載の暗号化装置。

[請求項13] 前記暗号化制御部は、前記ブロック暗号化部に暗号化させる場合に、通信データの送信先端末との間で、どのブロック暗号鍵を使用するかを確定し、確定したブロック暗号鍵を用いて前記ブロック暗号化部に暗号化させる

ことを特徴とする請求項１１又は１２に記載の暗号化装置。

[請求項14] 前記ワンタイムパッド暗号鍵記憶部は、ワンタイムパッド暗号鍵を記憶する不揮発性の記憶装置であり、

前記ワンタイムパッド暗号化部は、ワンタイムパッド暗号鍵を前記ワンタイムパッド暗号鍵記憶部から揮発性の記憶装置へコピーするとともに、コピー元のワンタイムパッド暗号鍵を前記ワンタイムパッド暗号鍵記憶部から削除した上で、前記揮発性の記憶装置にコピーしたワンタイムパッド暗号鍵を用いて通信データを暗号化する

ことを特徴とする請求項１から１３までのいずれかに記載の暗号化装置。

[請求項15] 前記暗号化装置は、さらに、

前記暗号化制御部が用いる暗号化方式を切り替えた場合に、ユーザへ通知する通知部

を備えることを特徴とする１から１４までのいずれかに記載の暗号化装置。

[請求項16] 暗号化装置と復号装置とを備える暗号化システムであり、

前記暗号化装置は、

ワンタイムパッド暗号で使用する、複数ビットからなるワンタイムパッド暗号鍵を記憶するワンタイムパッド暗号鍵記憶部と、

前記ワンタイムパッド暗号鍵記憶部が記憶したワンタイムパッド暗号鍵の一部を順に用いて、通信データをワンタイムパッド暗号により暗号化して暗号化データを生成するワンタイムパッド暗号化部と、

ブロック暗号で使用するブロック暗号鍵を記憶するブロック暗号鍵記憶部と、

前記ブロック暗号鍵記憶部が記憶したブロック暗号鍵を用いて、通信データをブロック暗号により暗号化して暗号化データを生成するブロック暗号化部と、

前記ワンタイムパッド暗号鍵記憶部が記憶したワンタイムパッド暗号鍵の残りビット数に応じて、通信データを前記ワンタイムパッド暗号化部に暗号化させるか、前記ブロック暗号化部に暗号化させるかを制御するとともに、前記ワンタイムパッド暗号化部と前記ブロック暗号化部とのどちらに暗号化させるかを示すメッセージを前記復号装置へ通知する暗号化制御部と、

を備え、

前記復号装置は、

ワンタイムパッド暗号で使用する、複数ビットからなるワンタイムパッド復号鍵を記憶するワンタイムパッド復号鍵記憶部と、

前記ワンタイムパッド復号鍵記憶部が記憶したワンタイムパッド復号鍵の一部を順に用いて、暗号化データをワンタイムパッド暗号により復号して通信データを生成するワンタイムパッド復号部と、

ブロック暗号で使用するブロック復号鍵を記憶するブロック復号鍵記憶部と、

前記ブロック復号鍵記憶部が記憶したブロック復号鍵を用いて、暗号化データをブロック暗号により復号して通信データを生成するブロック復号部と、

前記暗号化制御部から通知されたメッセージに応じて、暗号化データを前記ワンタイムパッド復号部に復号させるか、前記ブロック復号部に復号させるかを制御する復号制御部と

を備えることを特徴とする暗号化システム。

[請求項17] 処理装置が、記憶装置に記憶された複数ビットからなるワンタイムパッド暗号鍵の一部を順に用いて、通信データをワンタイムパッド暗号により暗号化して暗号化データを生成するワンタイムパッド暗号化

工程と、

処理装置が、記憶装置に記憶されたブロック暗号鍵を用いて、通信データをブロック暗号により暗号化して暗号化データを生成するブロック暗号化工程と、

処理装置が、記憶装置に記憶されたワンタイムパッド暗号鍵の残りビット数に応じて、通信データを前記ワンタイムパッド暗号化工程でワンタイムパッド暗号により暗号化させるか、前記ブロック暗号化工程でブロック暗号により暗号化させるかを制御する暗号化制御工程とを備えることを特徴とする暗号化方法。

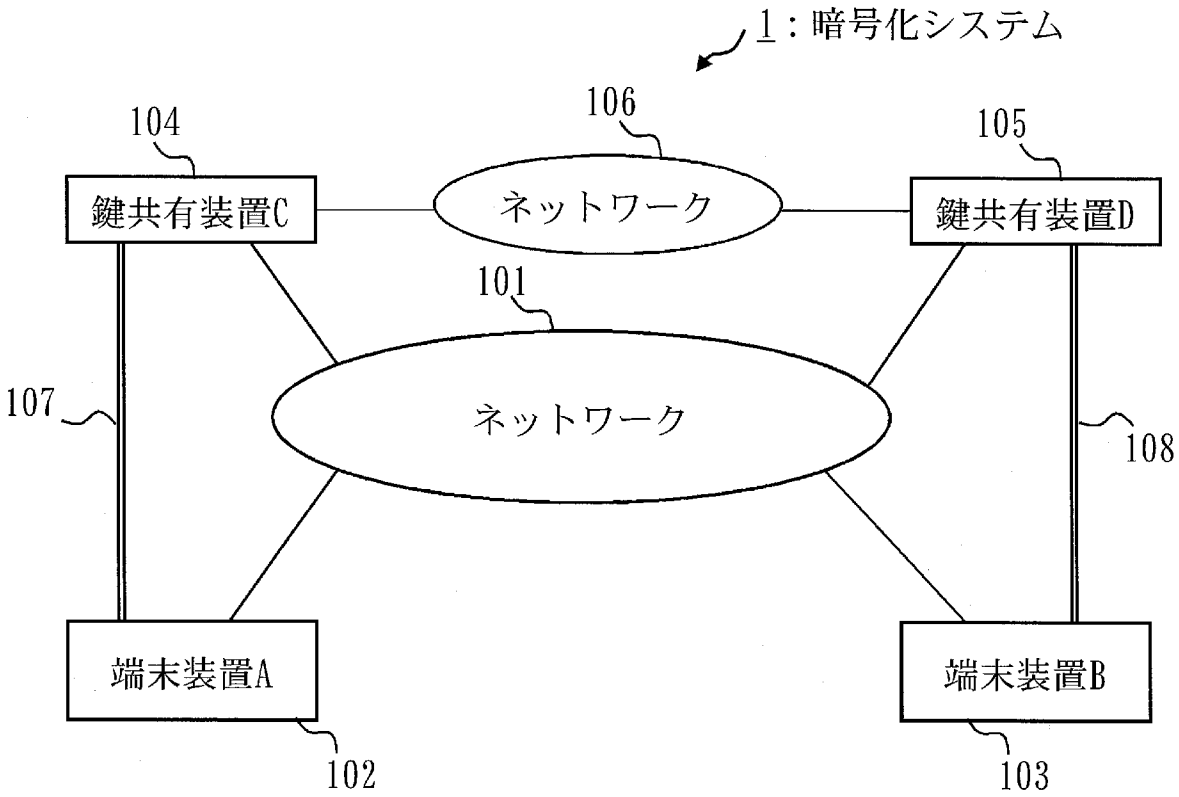
[請求項18] 記憶装置に記憶された複数ビットからなるワンタイムパッド暗号鍵の一部を順に用いて、通信データをワンタイムパッド暗号により暗号化して暗号化データを生成するワンタイムパッド暗号化処理と、

記憶装置に記憶されたブロック暗号鍵を用いて、通信データをブロック暗号により暗号化して暗号化データを生成するブロック暗号化処理と、

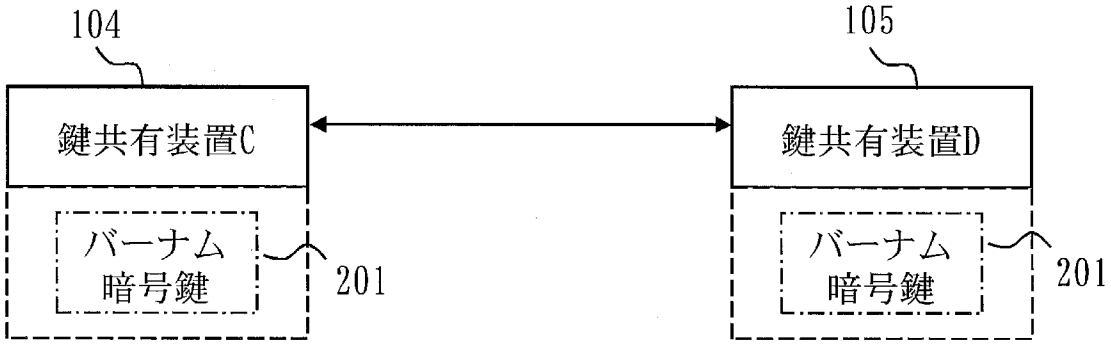
記憶装置に記憶されたワンタイムパッド暗号鍵の残りビット数に応じて、通信データを前記ワンタイムパッド暗号化処理でワンタイムパッド暗号により暗号化させるか、前記ブロック暗号化処理でブロック暗号により暗号化させるかを制御する暗号化制御処理と

をコンピュータに実行させることを特徴とする暗号化プログラム。

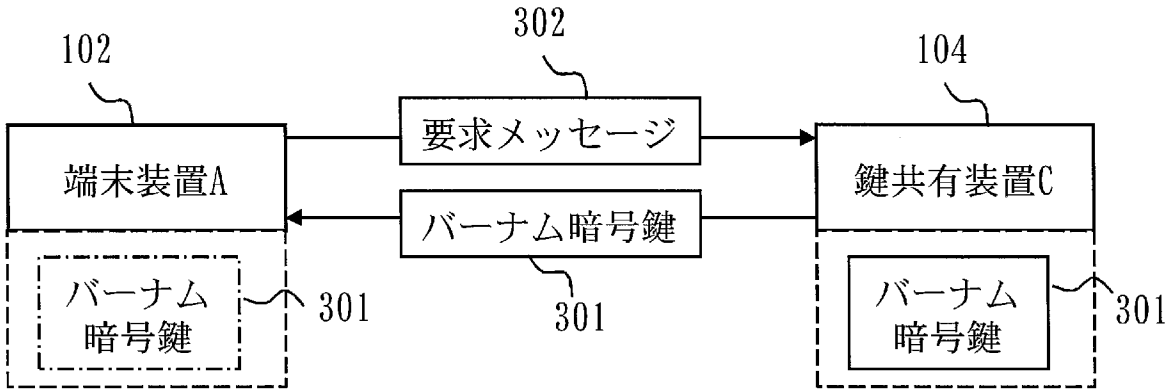
[図1]


1：暗号化システム
104
106
105
鍵共有装置C
ネットワーク
鍵共有装置D
101
107
ネットワーク
108
端末装置A
端末装置B
102
103

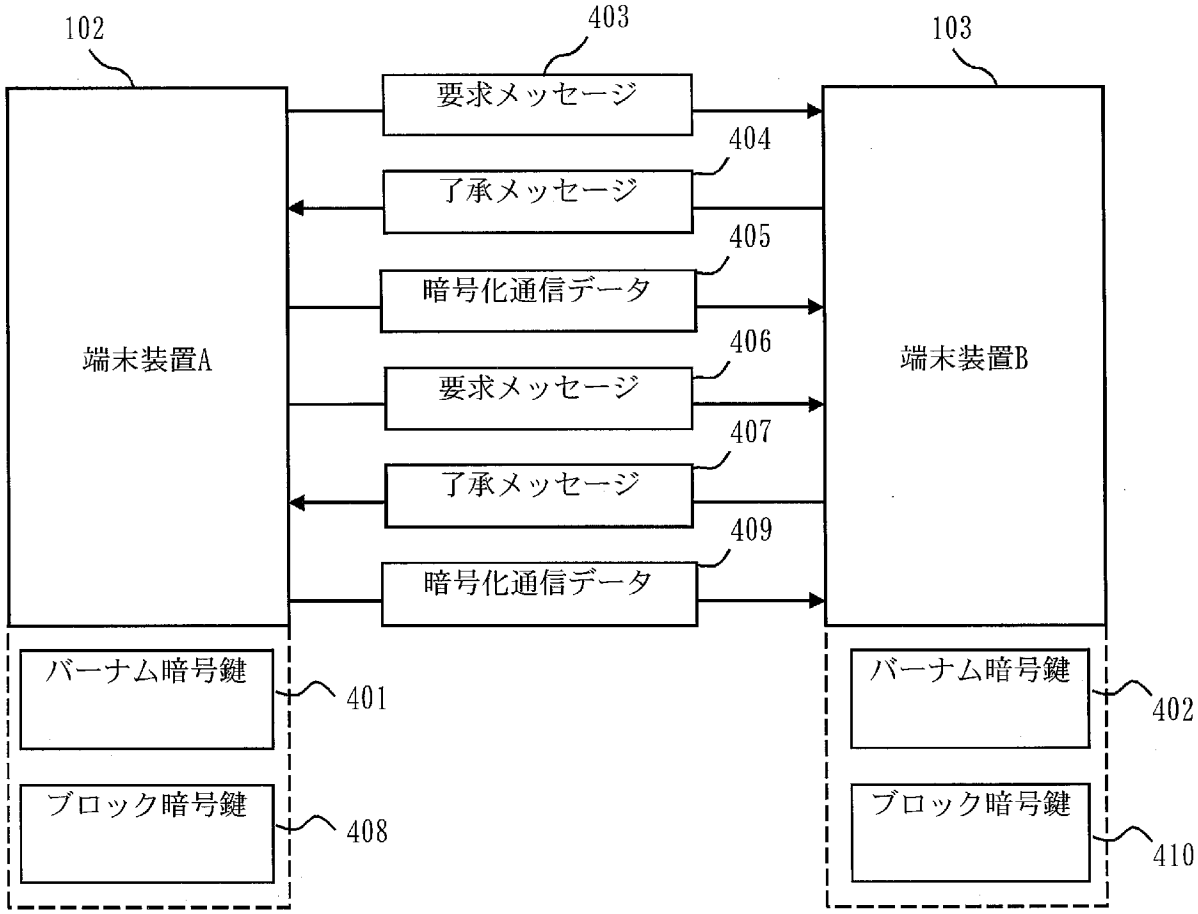
[図2]


104
105
鍵共有装置C
鍵共有装置D
バーナム
暗号鍵
201
バーナム
暗号鍵
201

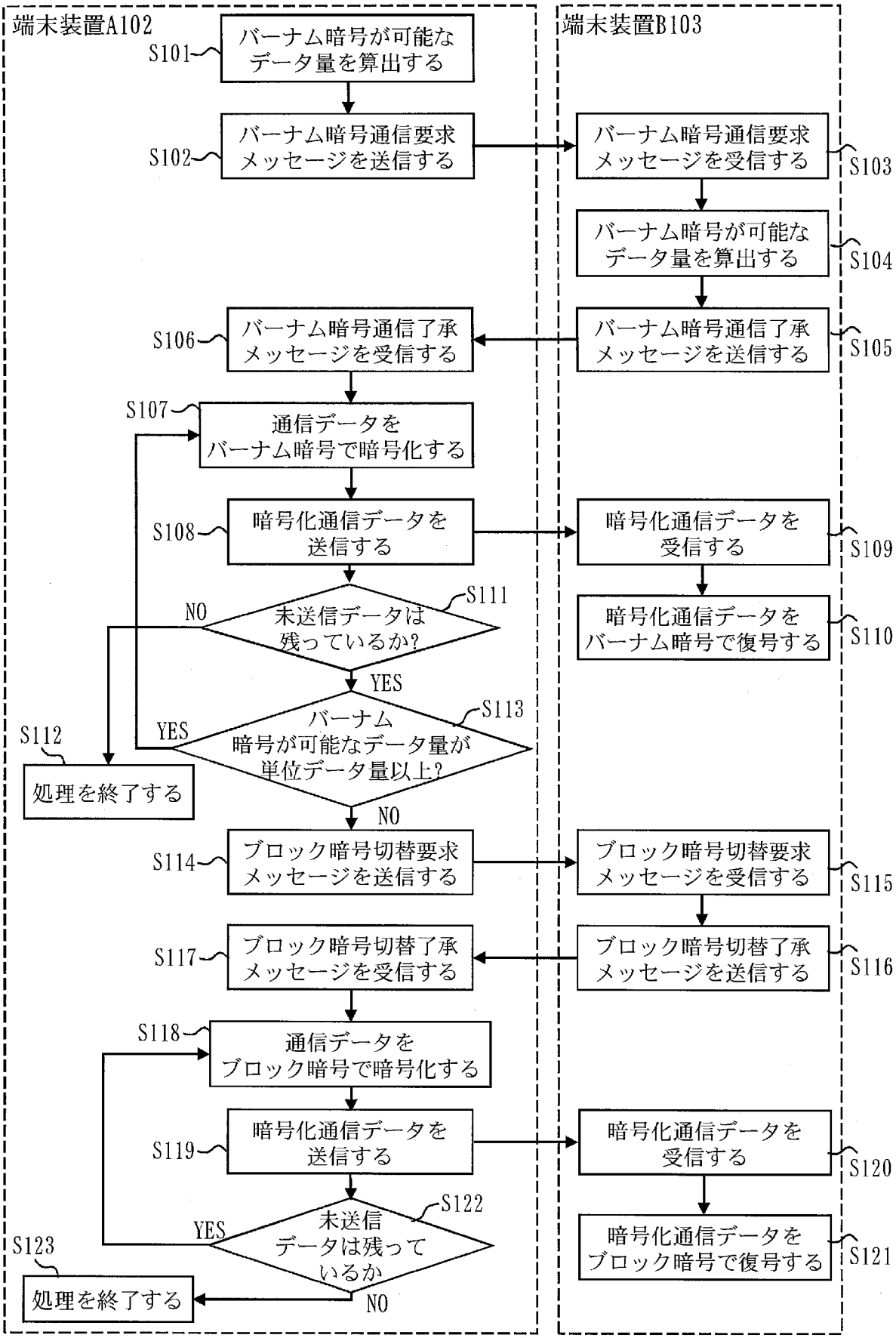
[図3]


102
302
104
端末装置A
要求メッセージ
鍵共有装置C
バーナム暗号鍵
バーナム
暗号鍵
301
301
バーナム
暗号鍵
301

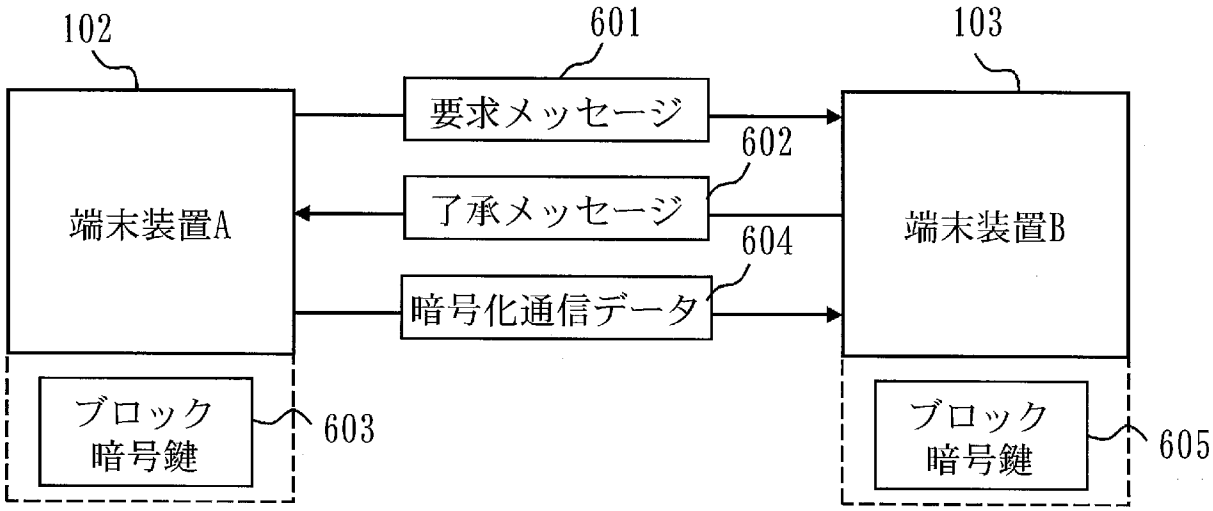
[図4]


102
403
103
要求メッセージ
404
了承メッセージ
405
暗号化通信データ
端末装置A
406
要求メッセージ
端末装置B
407
了承メッセージ
409
暗号化通信データ
バーナム暗号鍵
401
バーナム暗号鍵
402
ブロック暗号鍵
408
ブロック暗号鍵
410

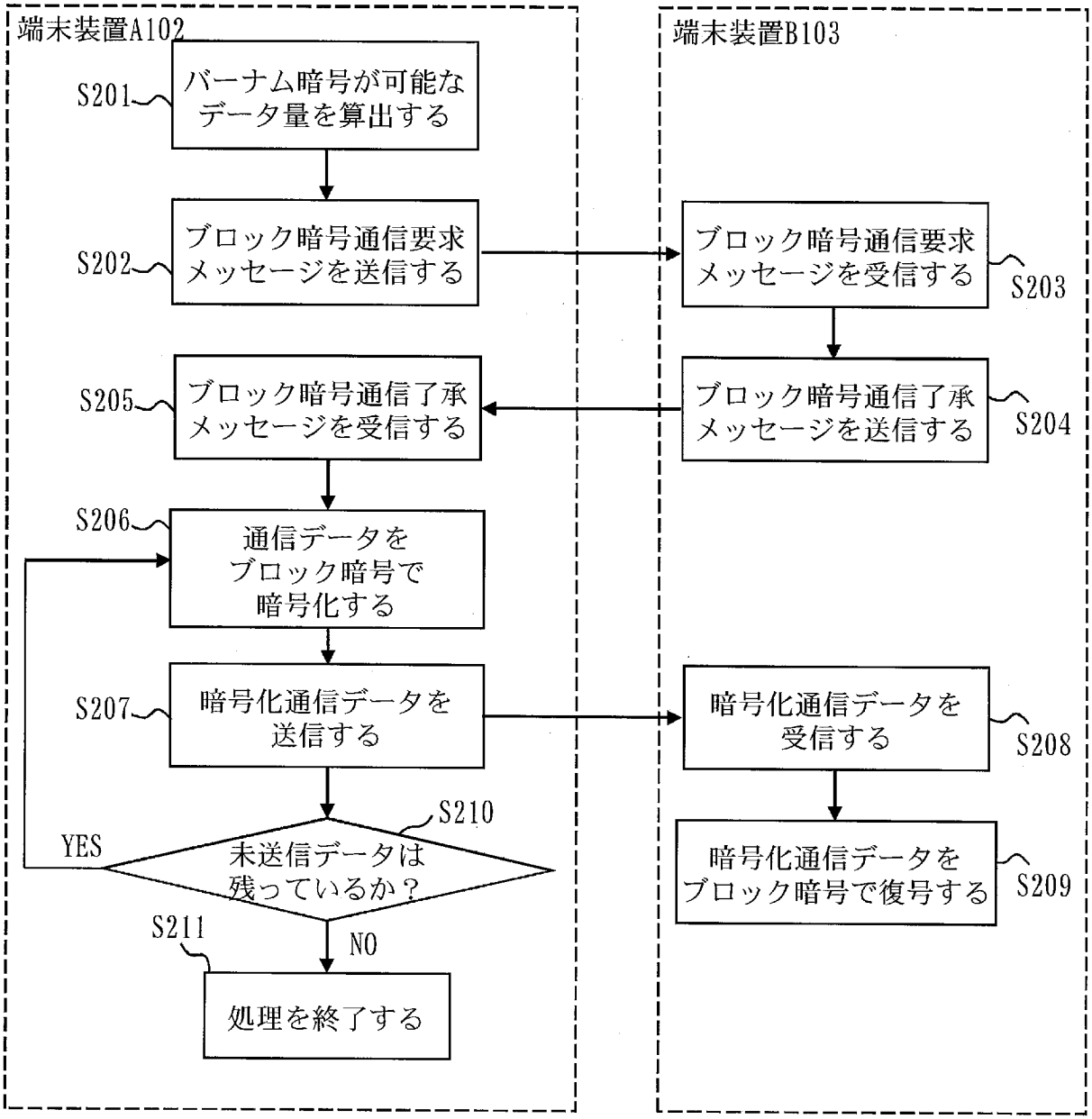
[図5]


端末装置A102
端末装置B103
S101
バーナム暗号が可能なデータ量を算出する
S102
バーナム暗号通信要求メッセージを送信する
S103
バーナム暗号通信要求メッセージを受信する
S104
バーナム暗号が可能なデータ量を算出する
S105
バーナム暗号通信了承メッセージを送信する
S106
バーナム暗号通信了承メッセージを受信する
S107
通信データをバーナム暗号で暗号化する
S108
暗号化通信データを送信する
S109
暗号化通信データを受信する
S110
暗号化通信データをバーナム暗号で復号する
S111
未送信データは残っているか?
NO
YES
S112
処理を終了する
S113
バーナム暗号が可能なデータ量が単位データ量以上?
YES
NO
S114
ブロック暗号切替要求メッセージを送信する
S115
ブロック暗号切替要求メッセージを受信する
S116
ブロック暗号切替了承メッセージを送信する
S117
ブロック暗号切替了承メッセージを受信する
S118
通信データをブロック暗号で暗号化する
S119
暗号化通信データを送信する
S120
暗号化通信データを受信する
S121
暗号化通信データをブロック暗号で復号する
S122
未送信データは残っているか
YES
NO
S123
処理を終了する

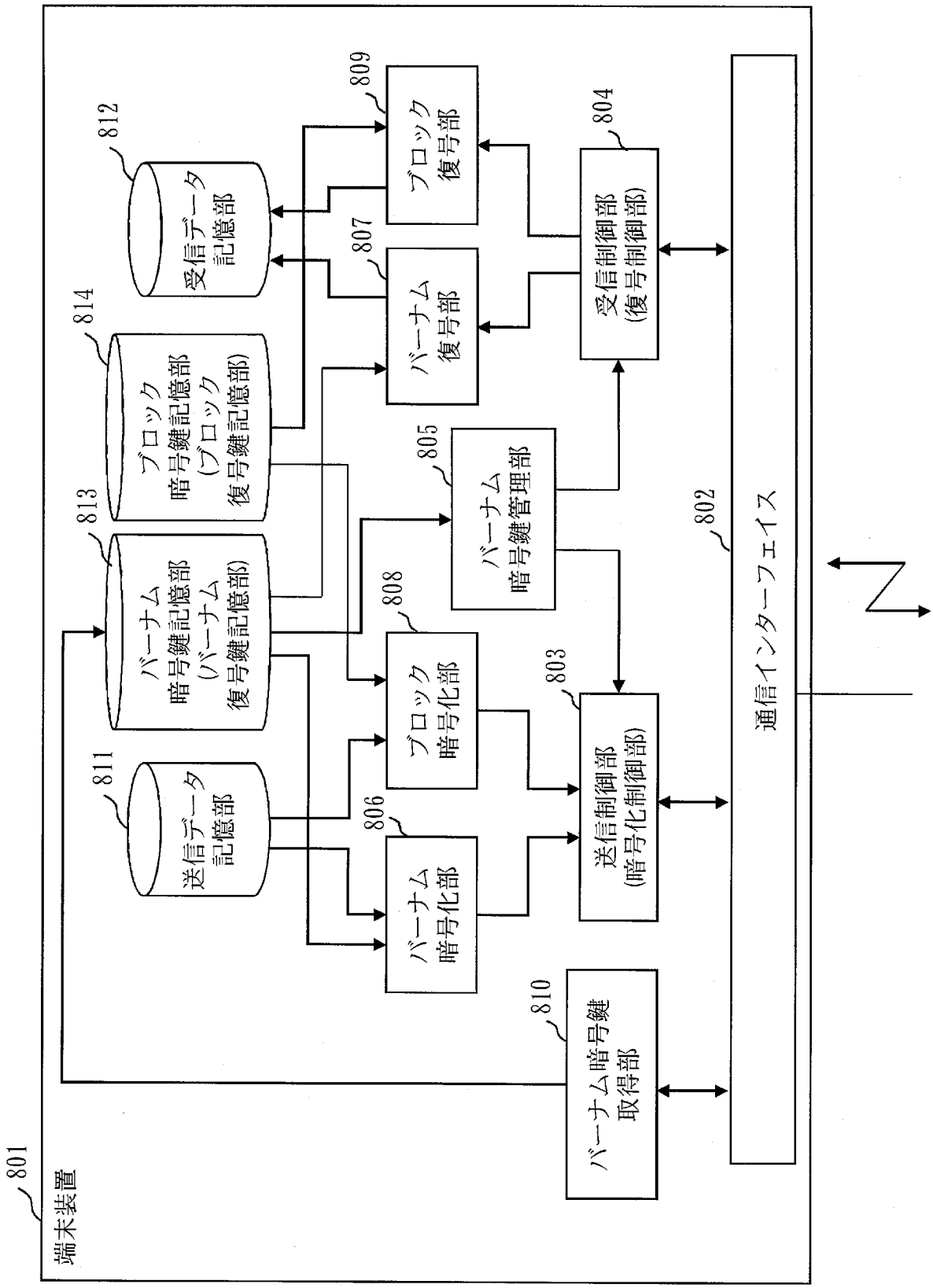
[図6]


102
601
103
要求メッセージ
602
了承メッセージ
604
暗号化通信データ
端末装置A
端末装置B
ブロック
暗号鍵
603
ブロック
暗号鍵
605

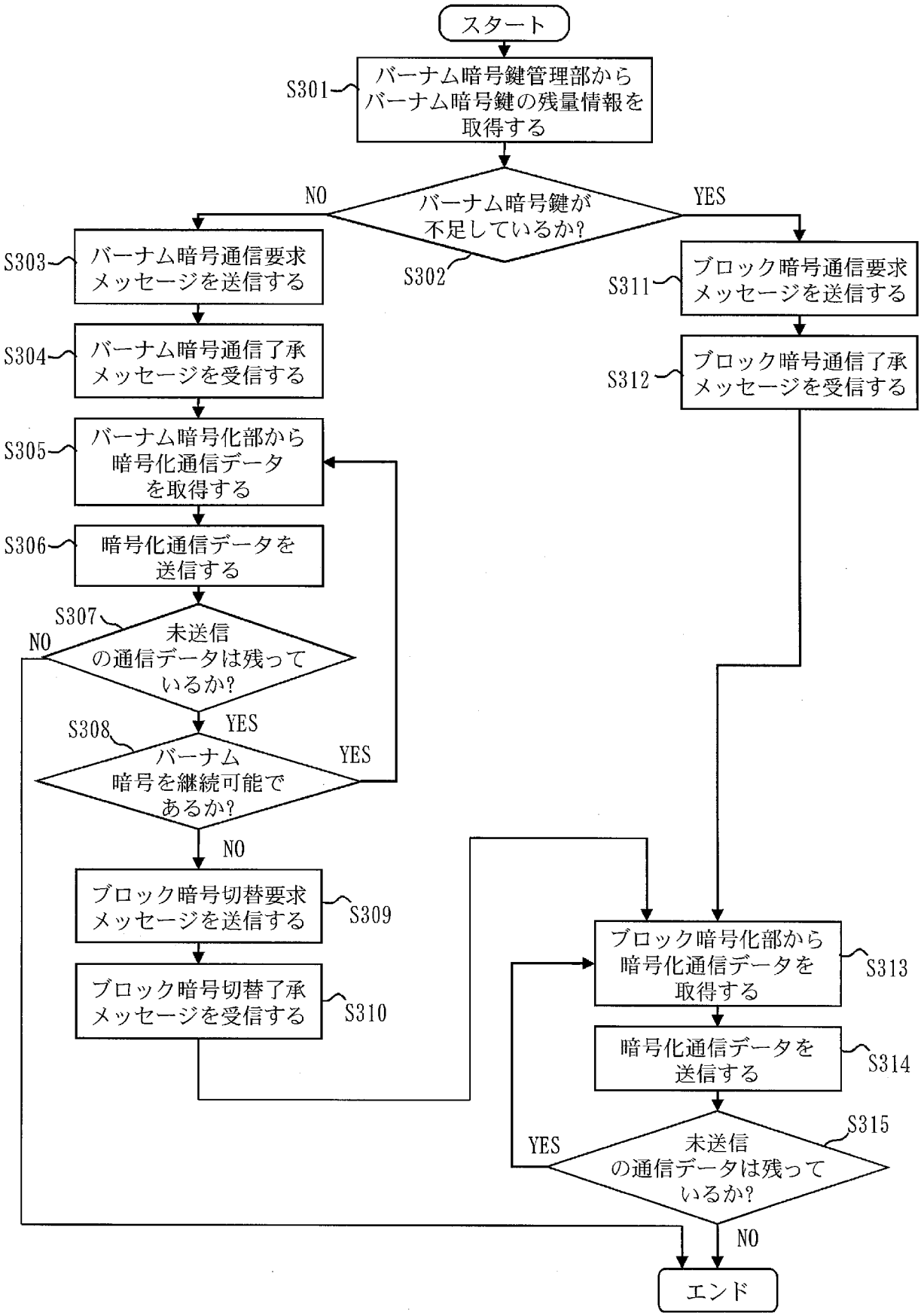
[図7]


端末装置A102
端末装置B103
S201
バーナム暗号が可能な
データ量を算出する
S202
ブロック暗号通信要求
メッセージを送信する
ブロック暗号通信要求
メッセージを受信する
S203
S205
ブロック暗号通信了承
メッセージを受信する
ブロック暗号通信了承
メッセージを送信する
S204
S206
通信データを
ブロック暗号で
暗号化する
S207
暗号化通信データを
送信する
暗号化通信データを
受信する
S208
S210
YES
未送信データは
残っているか？
暗号化通信データを
ブロック暗号で復号する
S209
S211
NO
処理を終了する

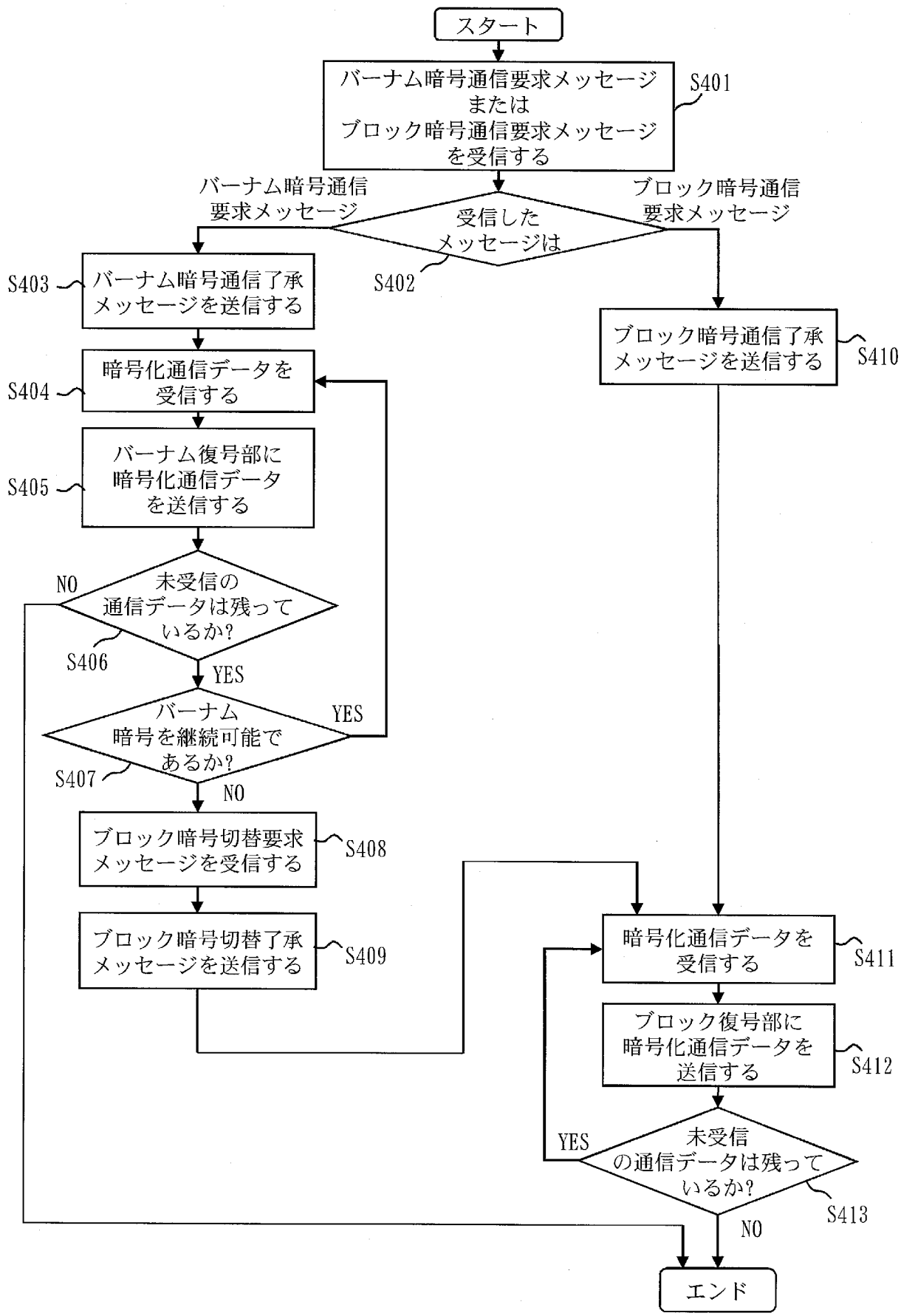
[図8]


801
端末装置
802
通信インターフェイス
803
送信制御部
(暗号化制御部)
804
受信制御部
(復号制御部)
805
バーナム
暗号鍵管理部
806
バーナム
暗号化部
807
バーナム
復号部
808
ブロック
暗号化部
809
ブロック
復号部
810
バーナム暗号鍵
取得部
811
送信データ
記憶部
812
受信データ
記憶部
813
バーナム
暗号鍵記憶部
(バーナム
復号鍵記憶部)
814
ブロック
暗号鍵記憶部
(ブロック
復号鍵記憶部)

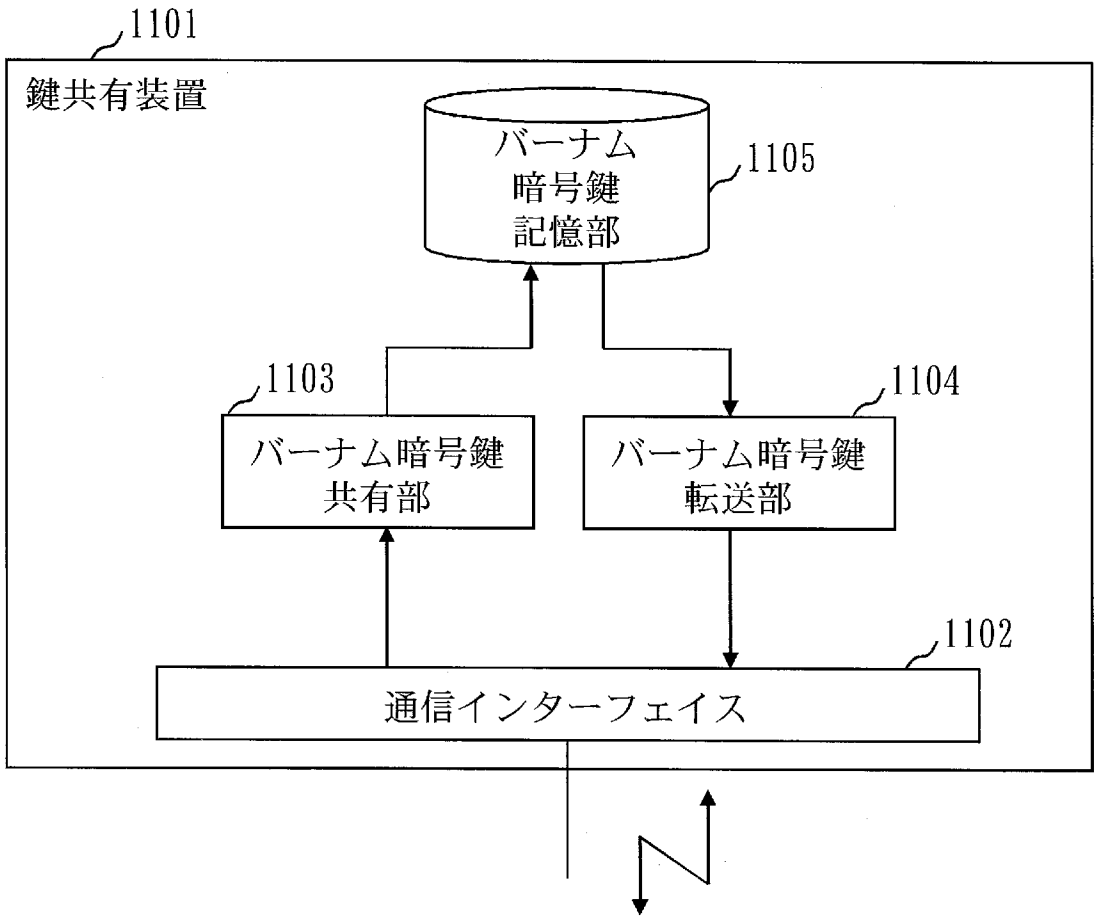
[図9]


スタート
S301
バーナム暗号鍵管理部から
バーナム暗号鍵の残量情報を
取得する
バーナム暗号鍵が
不足しているか?
S302
NO
YES
S303
バーナム暗号通信要求
メッセージを送信する
S304
バーナム暗号通信了承
メッセージを受信する
S305
バーナム暗号化部から
暗号化通信データ
を取得する
S306
暗号化通信データを
送信する
S307
未送信
の通信データは残って
いるか?
NO
YES
S308
バーナム
暗号を継続可能で
あるか?
YES
NO
S309
ブロック暗号切替要求
メッセージを送信する
S310
ブロック暗号切替了承
メッセージを受信する
S311
ブロック暗号通信要求
メッセージを送信する
S312
ブロック暗号通信了承
メッセージを受信する
S313
ブロック暗号化部から
暗号化通信データを
取得する
S314
暗号化通信データを
送信する
S315
未送信
の通信データは残って
いるか?
YES
NO
エンド

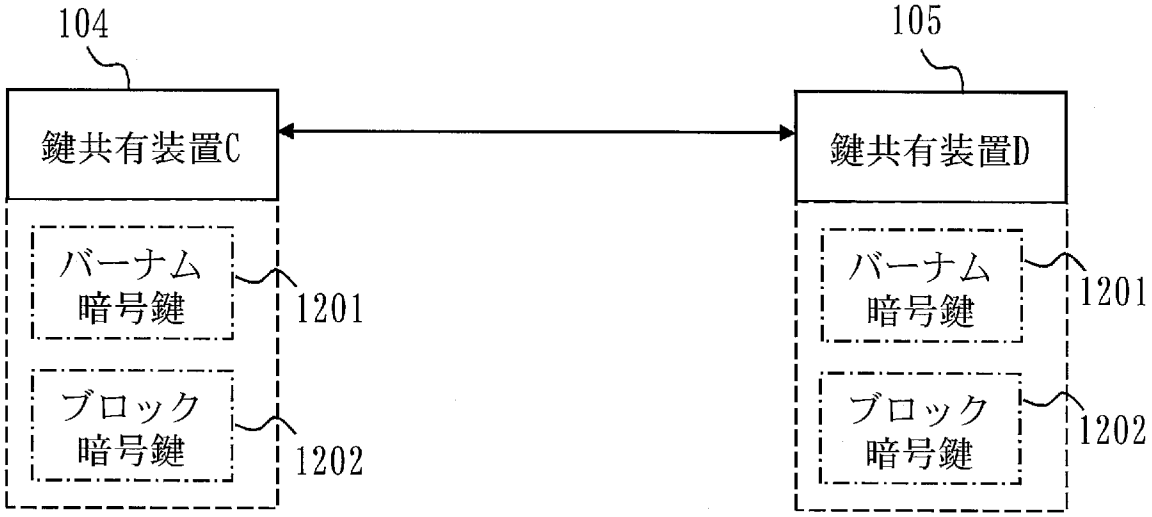
[図10]


スタート
バーナム暗号通信要求メッセージ
または
ブロック暗号通信要求メッセージ
を受信する
S401
受信した
メッセージは
S402
バーナム暗号通信
要求メッセージ
ブロック暗号通信
要求メッセージ
S403
バーナム暗号通信了承
メッセージを送信する
S404
暗号化通信データを
受信する
S405
バーナム復号部に
暗号化通信データ
を送信する
S406
未受信の
通信データは残って
いるか?
NO
YES
S407
バーナム
暗号を継続可能で
あるか?
YES
NO
S408
ブロック暗号切替要求
メッセージを受信する
S409
ブロック暗号切替了承
メッセージを送信する
S410
ブロック暗号通信了承
メッセージを送信する
S411
暗号化通信データを
受信する
S412
ブロック復号部に
暗号化通信データを
送信する
S413
未受信
の通信データは残って
いるか?
YES
NO
エンド

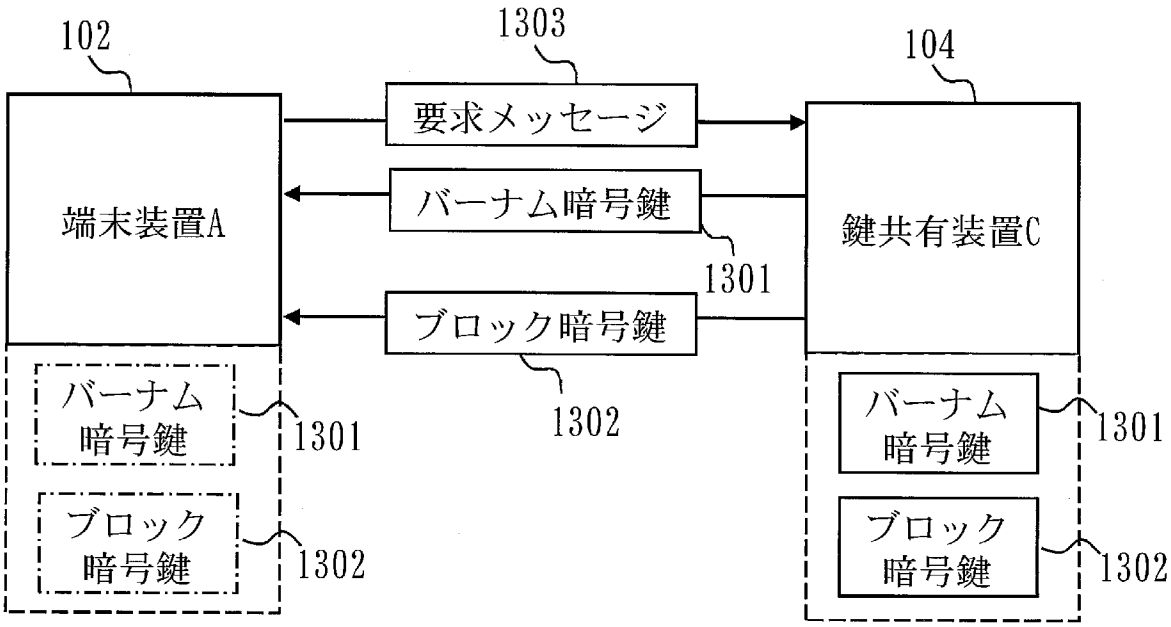
[図11]


1101
鍵共有装置
バーナム
暗号鍵
記憶部
1105
1103
バーナム暗号鍵
共有部
1104
バーナム暗号鍵
転送部
1102
通信インターフェイス

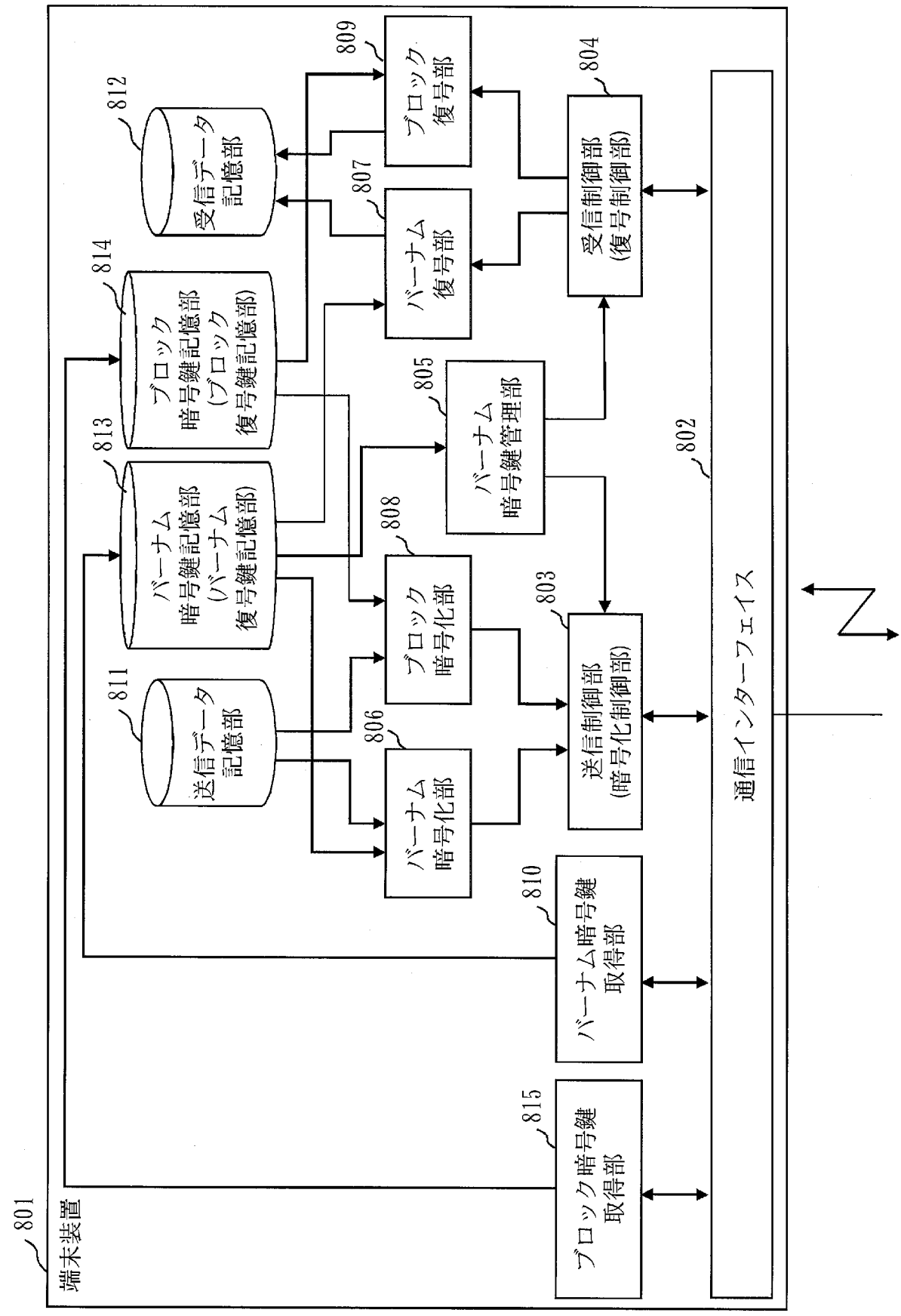
[図12]


104
鍵共有装置C
バーナム
暗号鍵
1201
ブロック
暗号鍵
1202
105
鍵共有装置D
バーナム
暗号鍵
1201
ブロック
暗号鍵
1202

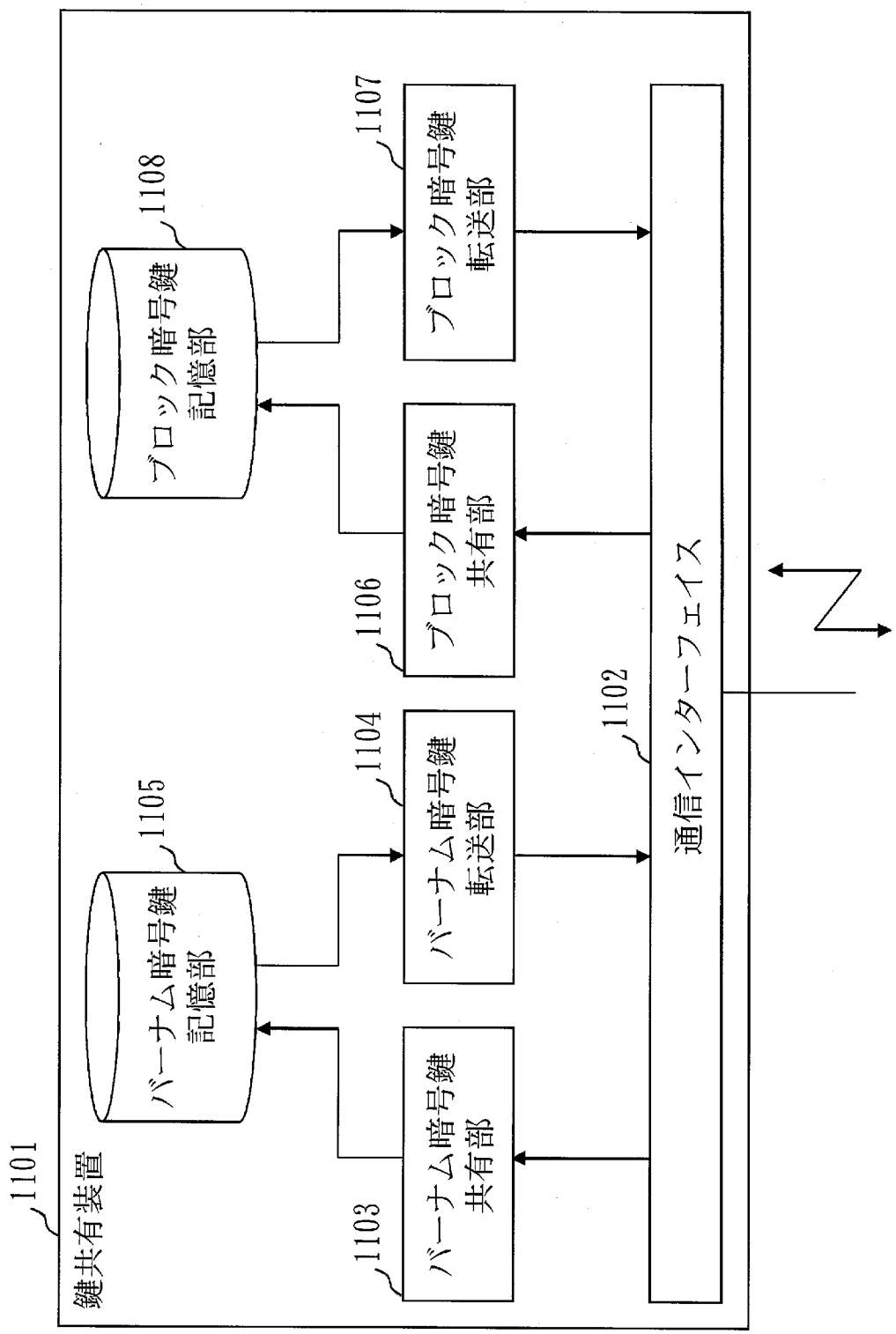
[図13]


102
1303
104
要求メッセージ
端末装置A
バーナム暗号鍵
鍵共有装置C
1301
ブロック暗号鍵
バーナム
暗号鍵
1301
1302
ブロック
暗号鍵
1302
バーナム
暗号鍵
1301
ブロック
暗号鍵
1302

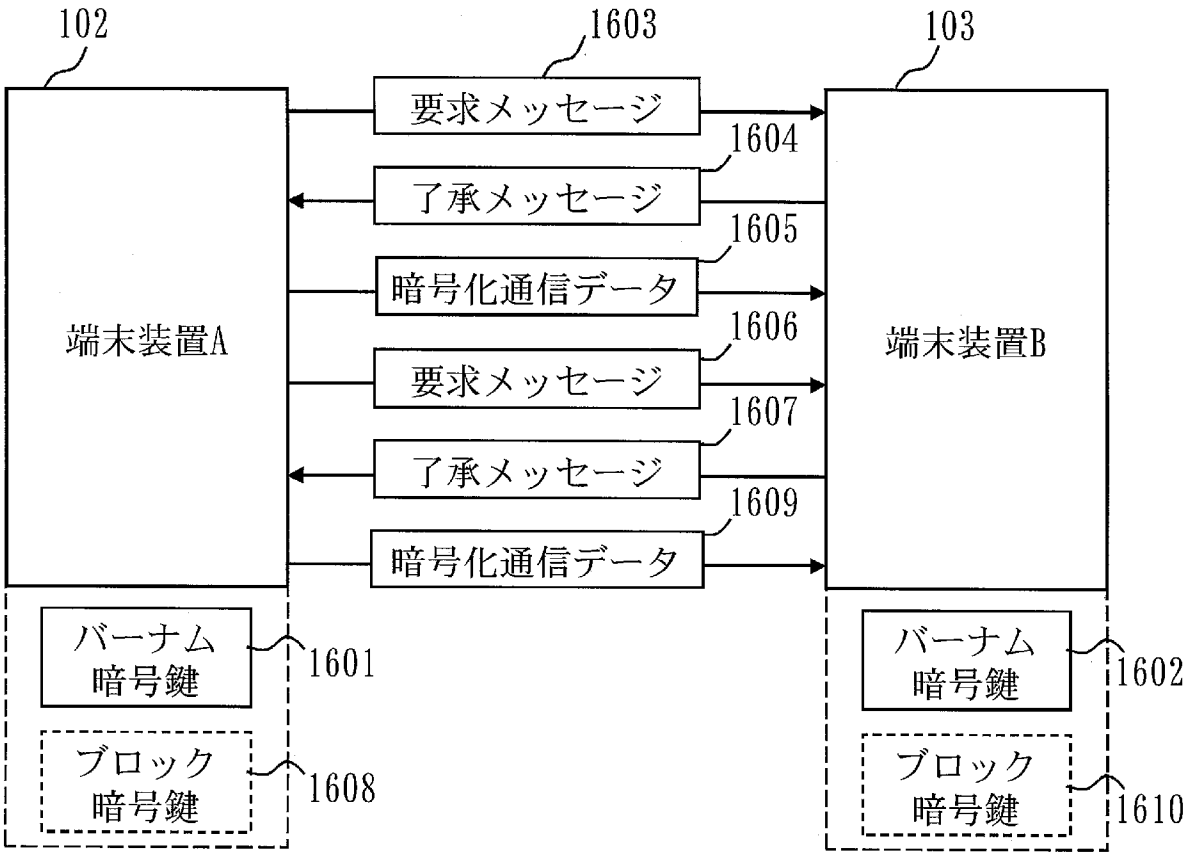
[図14]


801
端末装置
802
通信インターフェイス
803
送信制御部
(暗号化制御部)
804
受信制御部
(復号制御部)
805
バーナム
暗号鍵管理部
806
バーナム
暗号化部
807
バーナム
復号部
808
ブロック
暗号化部
809
ブロック
復号部
810
バーナム暗号鍵
取得部
811
送信データ
記憶部
812
受信データ
記憶部
813
バーナム
暗号鍵記憶部
(バーナム
復号鍵記憶部)
814
ブロック
暗号鍵記憶部
(ブロック
復号鍵記憶部)
815
ブロック暗号鍵
取得部

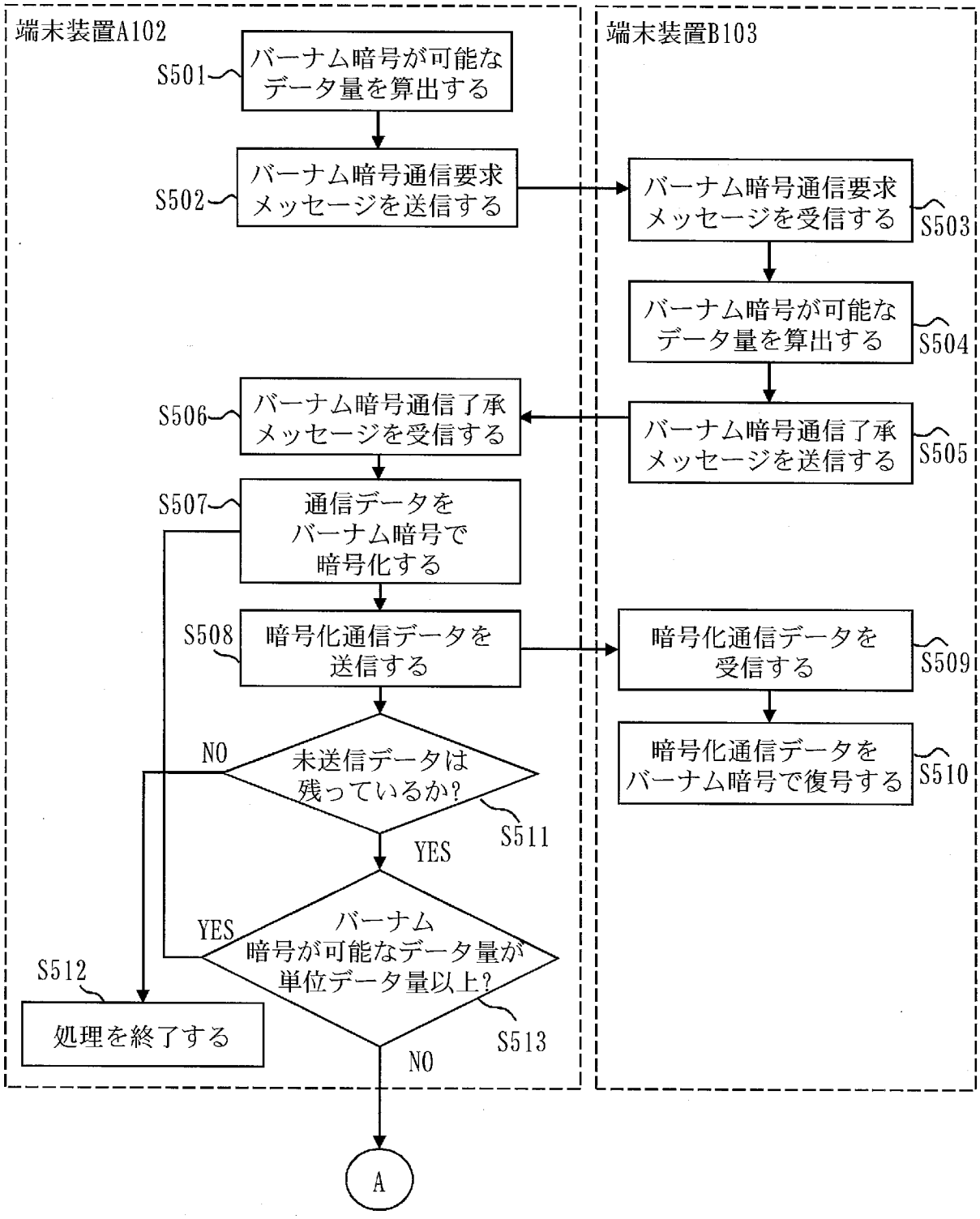
[図15]


鍵共有装置
1101
バーナム暗号鍵
記憶部
1105
ブロック暗号鍵
記憶部
1108
バーナム暗号鍵
共有部
1103
バーナム暗号鍵
転送部
1104
ブロック暗号鍵
共有部
1106
ブロック暗号鍵
転送部
1107
通信インターフェイス
1102

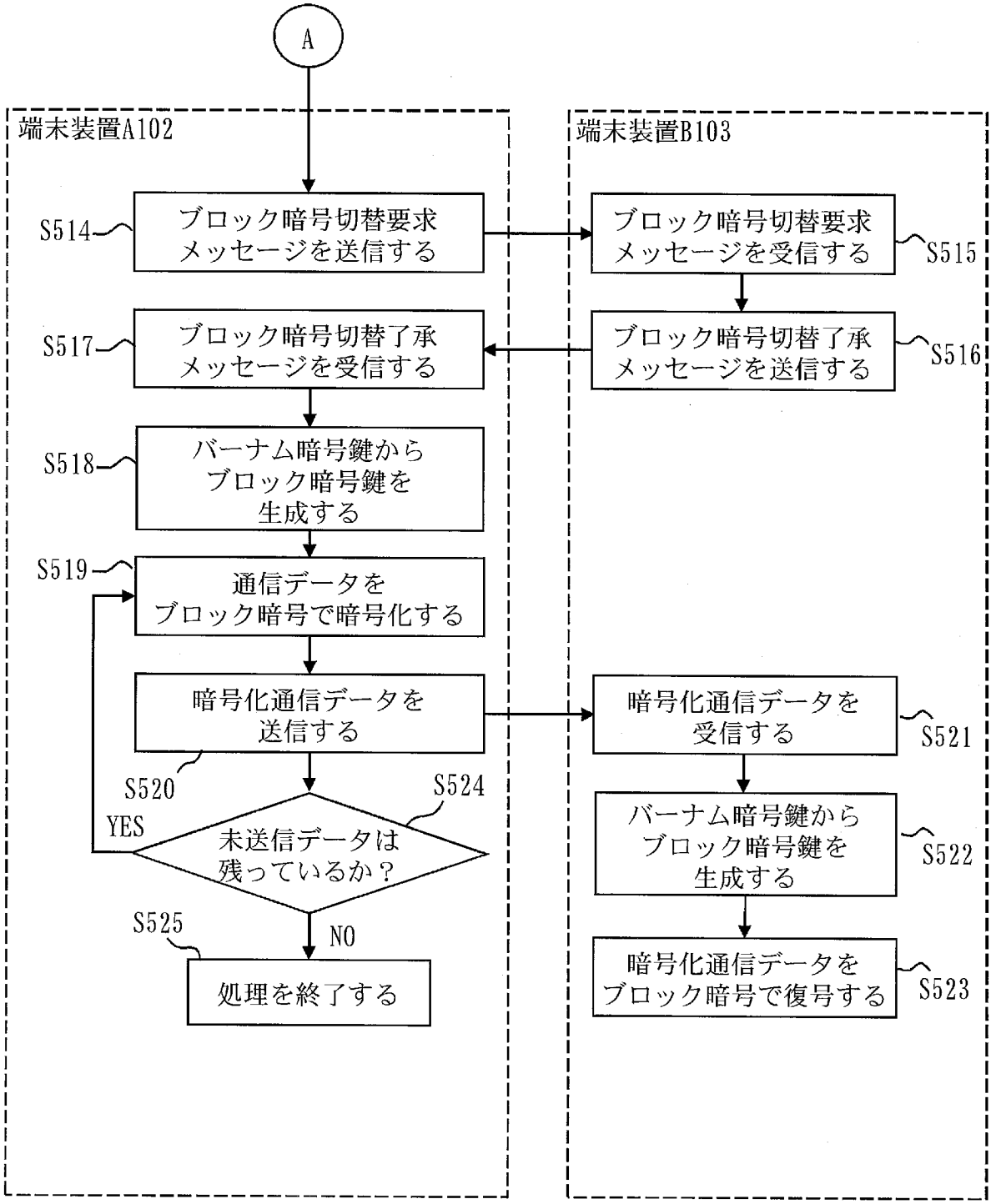
[図16]


102
1603
103
要求メッセージ
1604
了承メッセージ
1605
暗号化通信データ
端末装置A
1606
要求メッセージ
端末装置B
1607
了承メッセージ
1609
暗号化通信データ
バーナム
暗号鍵
1601
バーナム
暗号鍵
1602
ブロック
暗号鍵
1608
ブロック
暗号鍵
1610

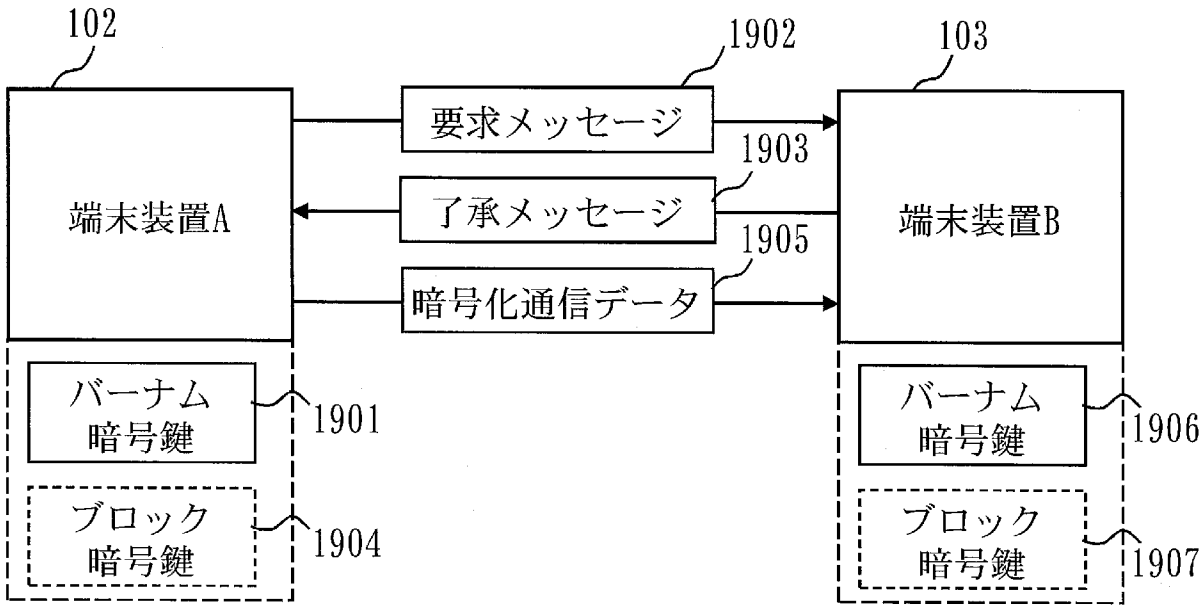
[図17]


端末装置A102
端末装置B103
S501
バーナム暗号が可能なデータ量を算出する
S502
バーナム暗号通信要求メッセージを送信する
バーナム暗号通信要求メッセージを受信する
S503
バーナム暗号が可能なデータ量を算出する
S504
バーナム暗号通信了承メッセージを送信する
S505
S506
バーナム暗号通信了承メッセージを受信する
S507
通信データをバーナム暗号で暗号化する
S508
暗号化通信データを送信する
暗号化通信データを受信する
S509
暗号化通信データをバーナム暗号で復号する
S510
NO
未送信データは残っているか?
S511
YES
YES
バーナム暗号が可能なデータ量が単位データ量以上?
S513
S512
処理を終了する
NO
A

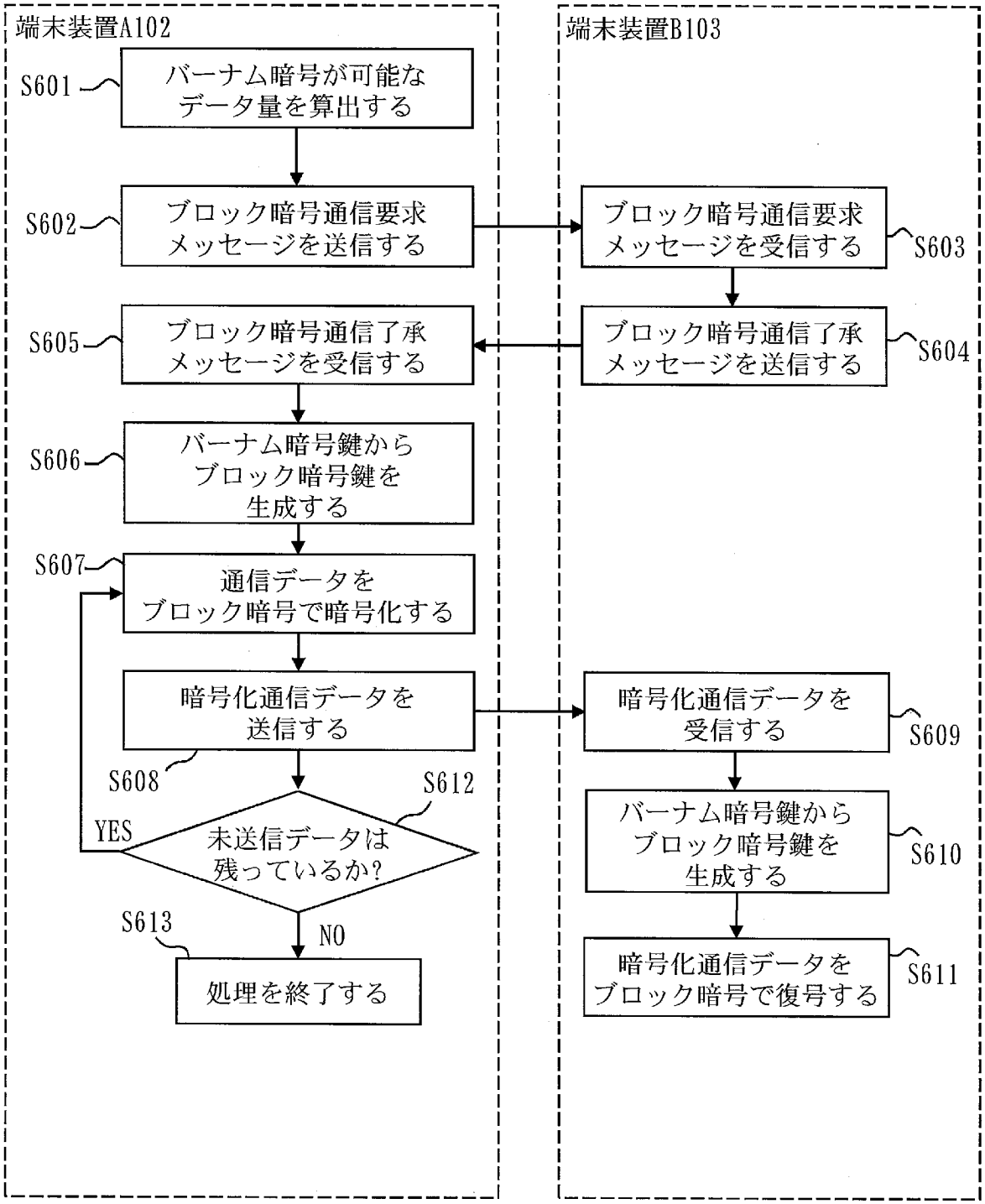
[図18]


A
端末装置A102
端末装置B103
S514
ブロック暗号切替要求メッセージを送信する
ブロック暗号切替要求メッセージを受信する
S515
S517
ブロック暗号切替了承メッセージを受信する
ブロック暗号切替了承メッセージを送信する
S516
S518
バーナム暗号鍵からブロック暗号鍵を生成する
S519
通信データをブロック暗号で暗号化する
暗号化通信データを送信する
暗号化通信データを受信する
S521
S520
S524
YES
未送信データは残っているか？
バーナム暗号鍵からブロック暗号鍵を生成する
S522
S525
NO
暗号化通信データをブロック暗号で復号する
S523
処理を終了する

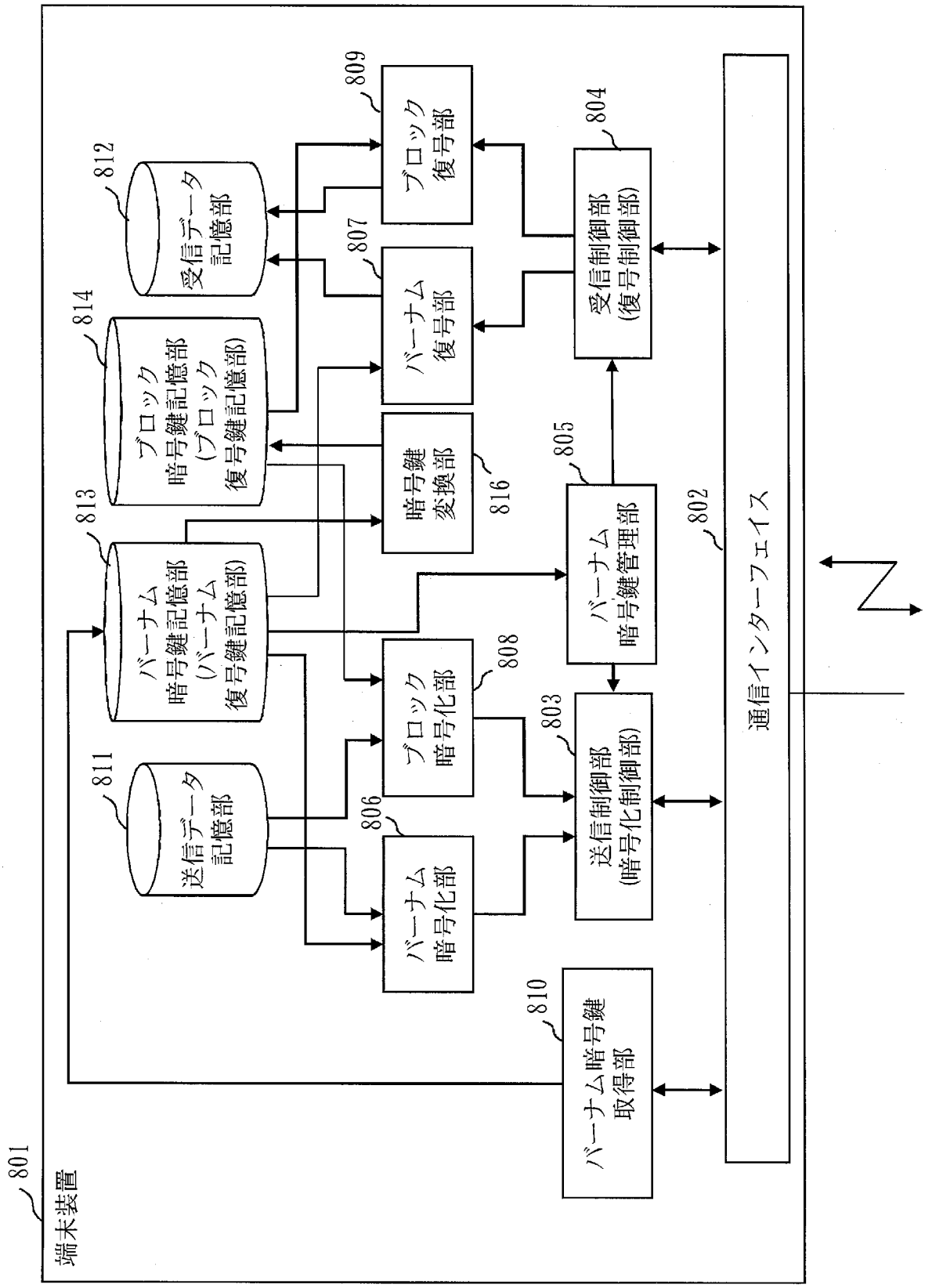
[図19]


102
1902
103
要求メッセージ
1903
端末装置A
了承メッセージ
端末装置B
1905
暗号化通信データ
バーナム
暗号鍵
1901
バーナム
暗号鍵
1906
ブロック
暗号鍵
1904
ブロック
暗号鍵
1907

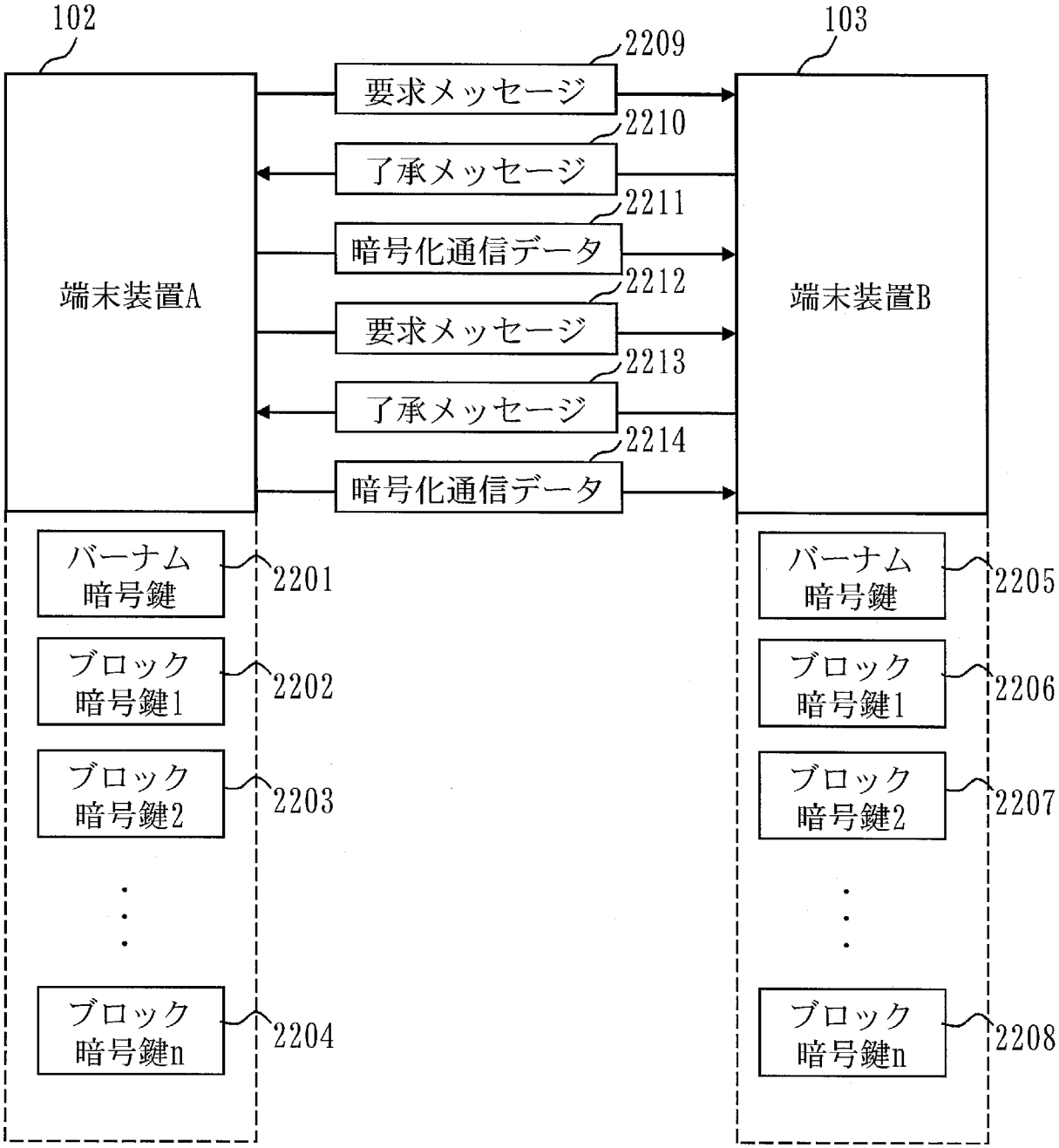
[図20]


端末装置A102
端末装置B103
S601
バーナム暗号が可能なデータ量を算出する
S602
ブロック暗号通信要求メッセージを送信する
ブロック暗号通信要求メッセージを受信する
S603
S605
ブロック暗号通信了承メッセージを受信する
ブロック暗号通信了承メッセージを送信する
S604
S606
バーナム暗号鍵からブロック暗号鍵を生成する
S607
通信データをブロック暗号で暗号化する
暗号化通信データを送信する
暗号化通信データを受信する
S609
S608
S612
YES
未送信データは残っているか?
バーナム暗号鍵からブロック暗号鍵を生成する
S610
S613
NO
暗号化通信データをブロック暗号で復号する
S611
処理を終了する

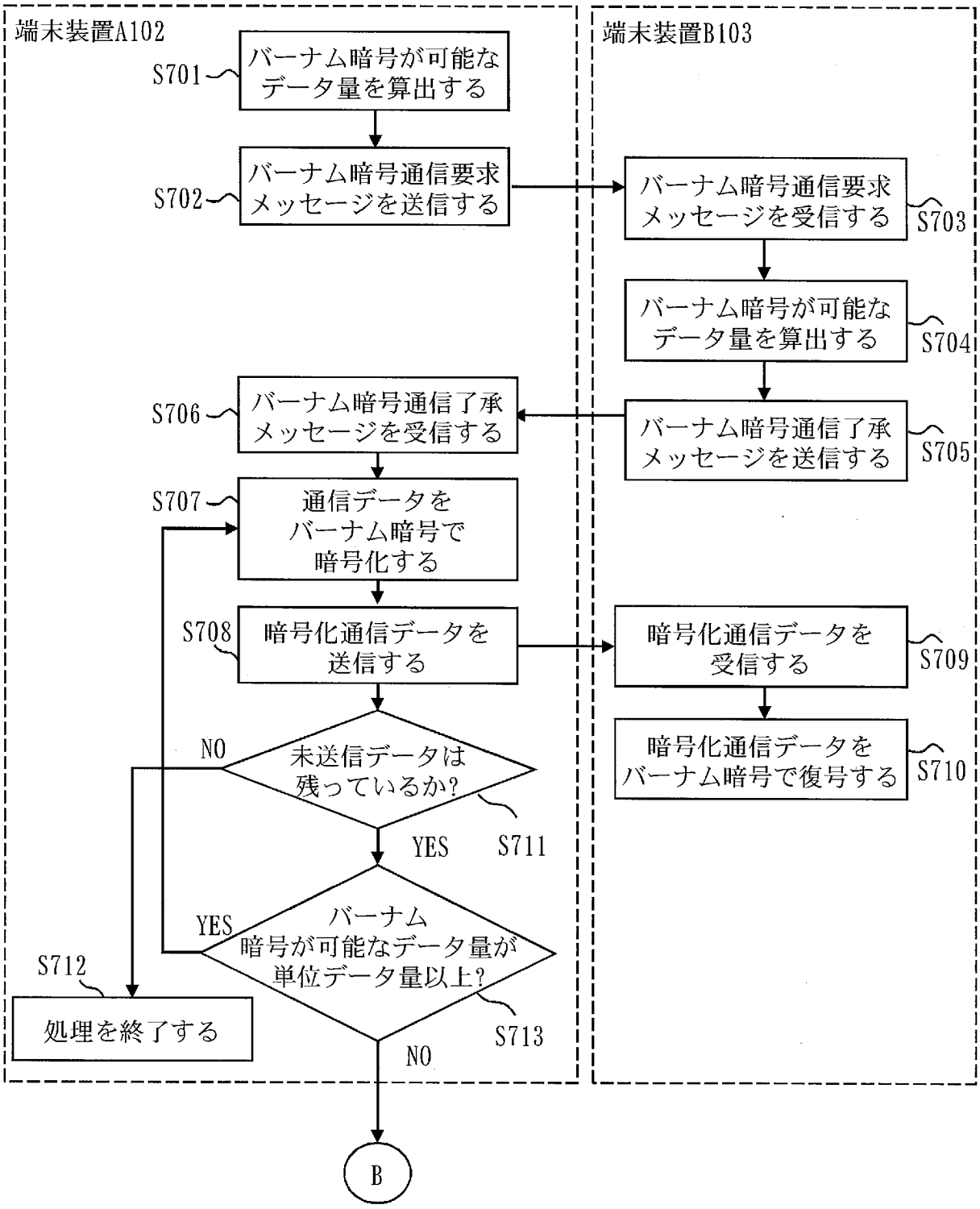
[図21]


801
端末装置
802
通信インターフェイス
803
送信制御部
(暗号化制御部)
804
受信制御部
(復号制御部)
805
バーナム
暗号鍵管理部
806
バーナム
暗号化部
807
バーナム
復号部
808
ブロック
暗号化部
809
ブロック
復号部
810
バーナム暗号鍵
取得部
811
送信データ
記憶部
812
受信データ
記憶部
813
バーナム
暗号鍵記憶部
(バーナム
復号鍵記憶部)
814
ブロック
暗号鍵記憶部
(ブロック
復号鍵記憶部)
816
暗号鍵
変換部
N

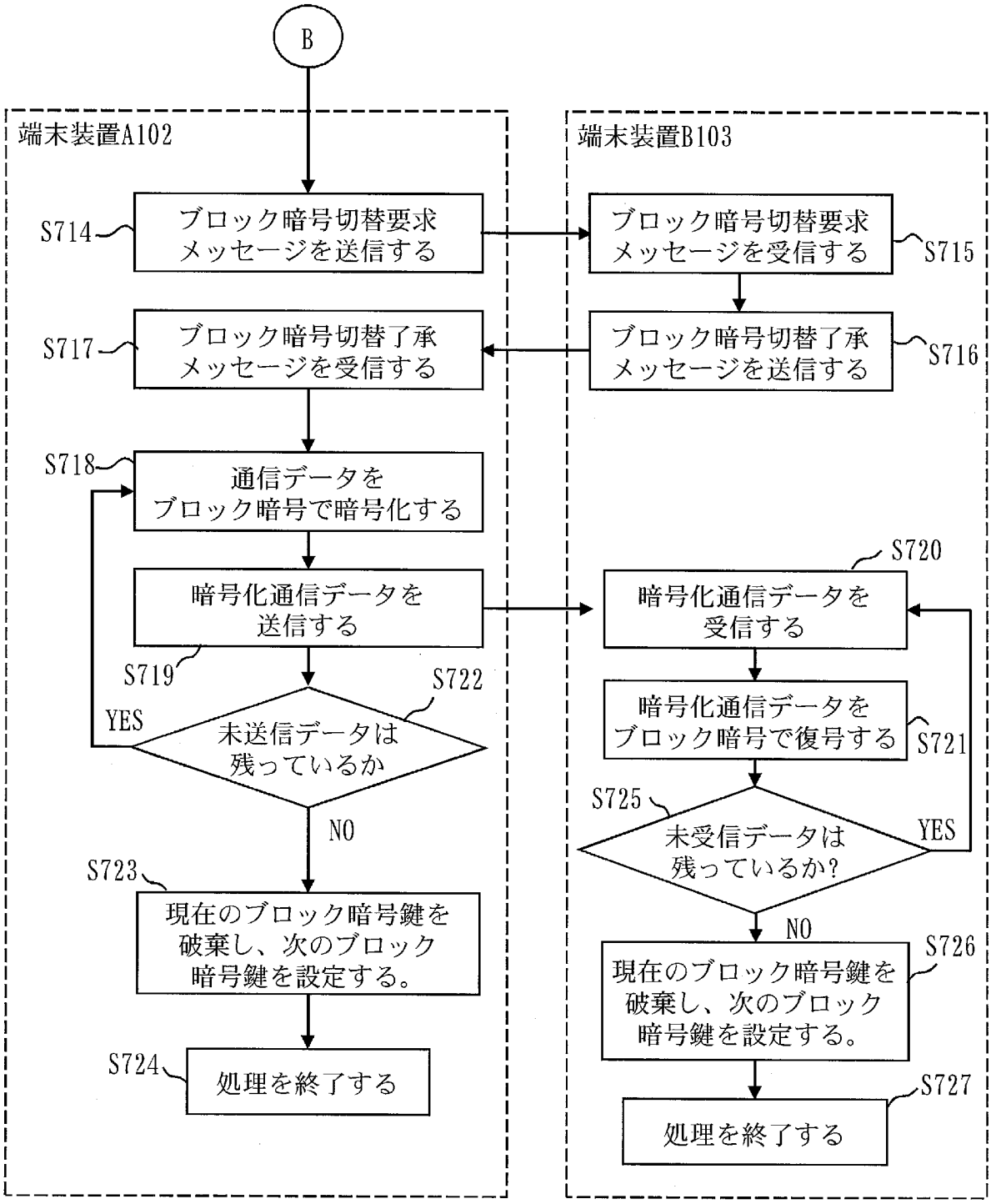
[図22]


102
103
2209
要求メッセージ
2210
了承メッセージ
2211
暗号化通信データ
2212
要求メッセージ
2213
了承メッセージ
2214
暗号化通信データ
端末装置A
端末装置B
バーナム暗号鍵
2201
ブロック暗号鍵1
2202
ブロック暗号鍵2
2203
ブロック暗号鍵n
2204
バーナム暗号鍵
2205
ブロック暗号鍵1
2206
ブロック暗号鍵2
2207
ブロック暗号鍵n
2208

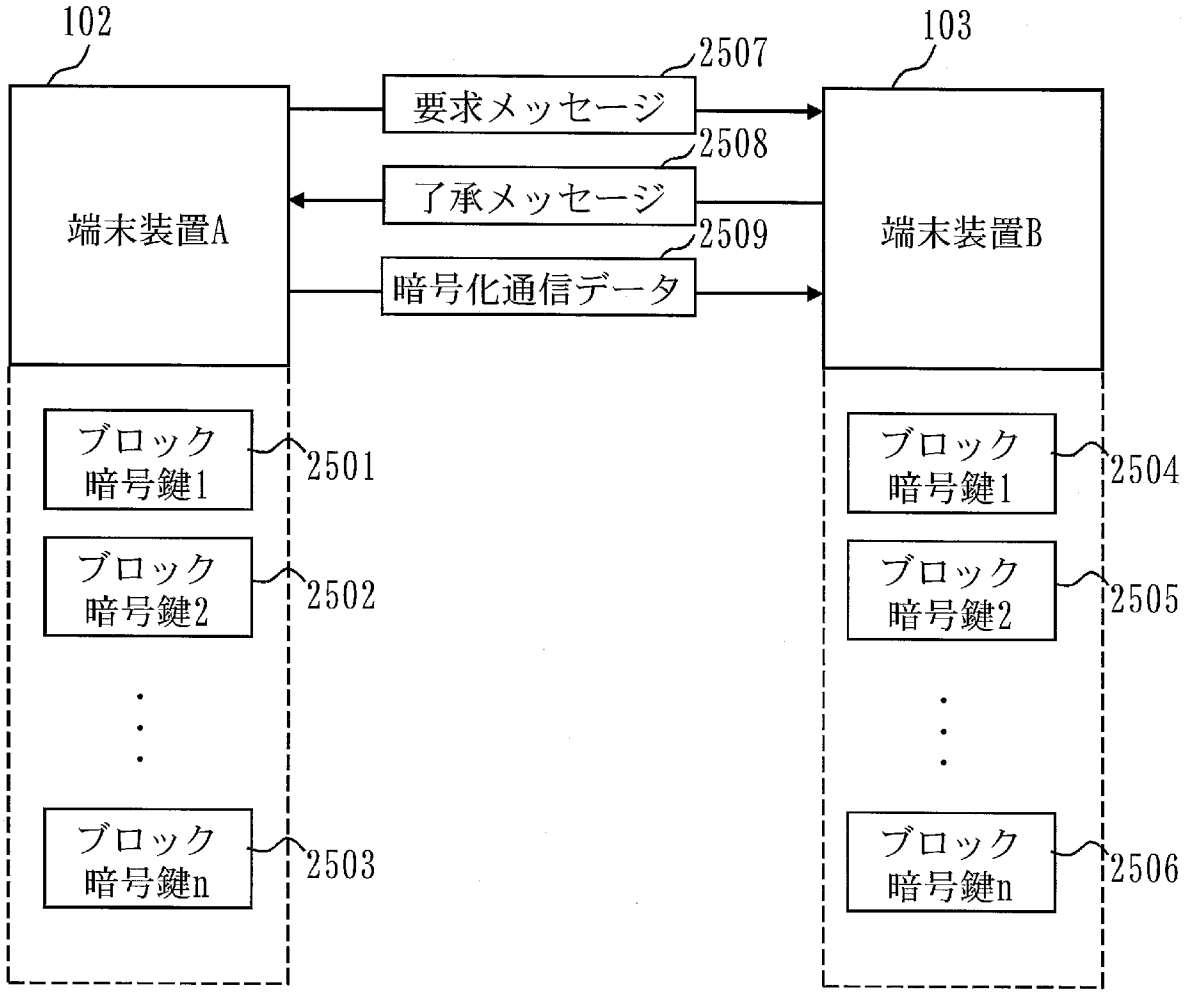
[図23]


端末装置A102
端末装置B103
S701
バーナム暗号が可能なデータ量を算出する
S702
バーナム暗号通信要求メッセージを送信する
バーナム暗号通信要求メッセージを受信する
S703
バーナム暗号が可能なデータ量を算出する
S704
バーナム暗号通信了承メッセージを送信する
S705
S706
バーナム暗号通信了承メッセージを受信する
S707
通信データをバーナム暗号で暗号化する
S708
暗号化通信データを送信する
暗号化通信データを受信する
S709
暗号化通信データをバーナム暗号で復号する
S710
NO
未送信データは残っているか?
S711
YES
YES
バーナム暗号が可能なデータ量が単位データ量以上?
S713
NO
S712
処理を終了する
B

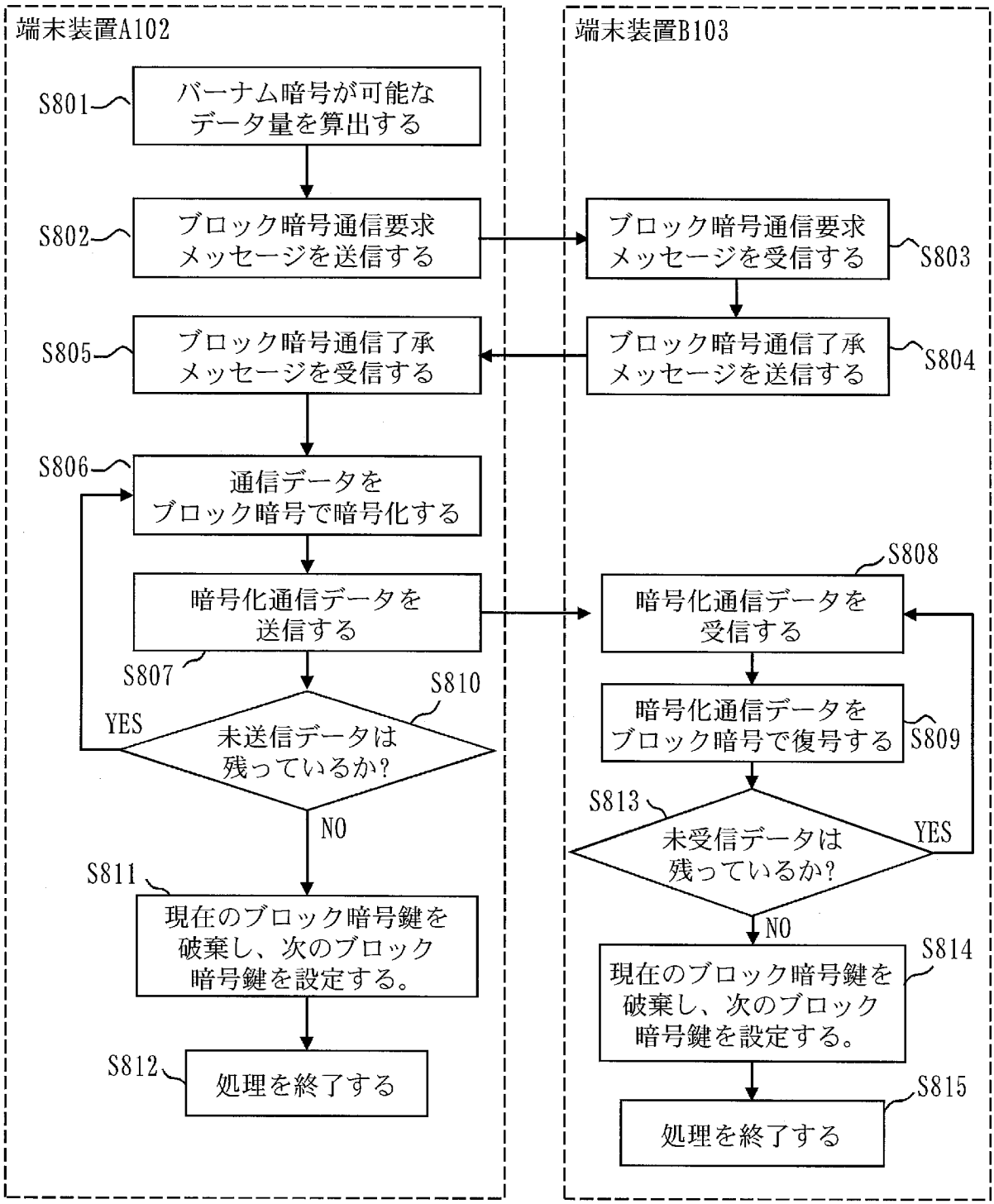
[図24]


B
端末装置A102
端末装置B103
S714
ブロック暗号切替要求メッセージを送信する
ブロック暗号切替要求メッセージを受信する
S715
S717
ブロック暗号切替了承メッセージを受信する
ブロック暗号切替了承メッセージを送信する
S716
S718
通信データをブロック暗号で暗号化する
S720
暗号化通信データを送信する
暗号化通信データを受信する
S719
S722
YES
未送信データは残っているか
暗号化通信データをブロック暗号で復号する
S721
S725
未受信データは残っているか?
YES
NO
NO
S723
現在のブロック暗号鍵を破棄し、次のブロック暗号鍵を設定する。
S726
現在のブロック暗号鍵を破棄し、次のブロック暗号鍵を設定する。
S724
処理を終了する
S727
処理を終了する

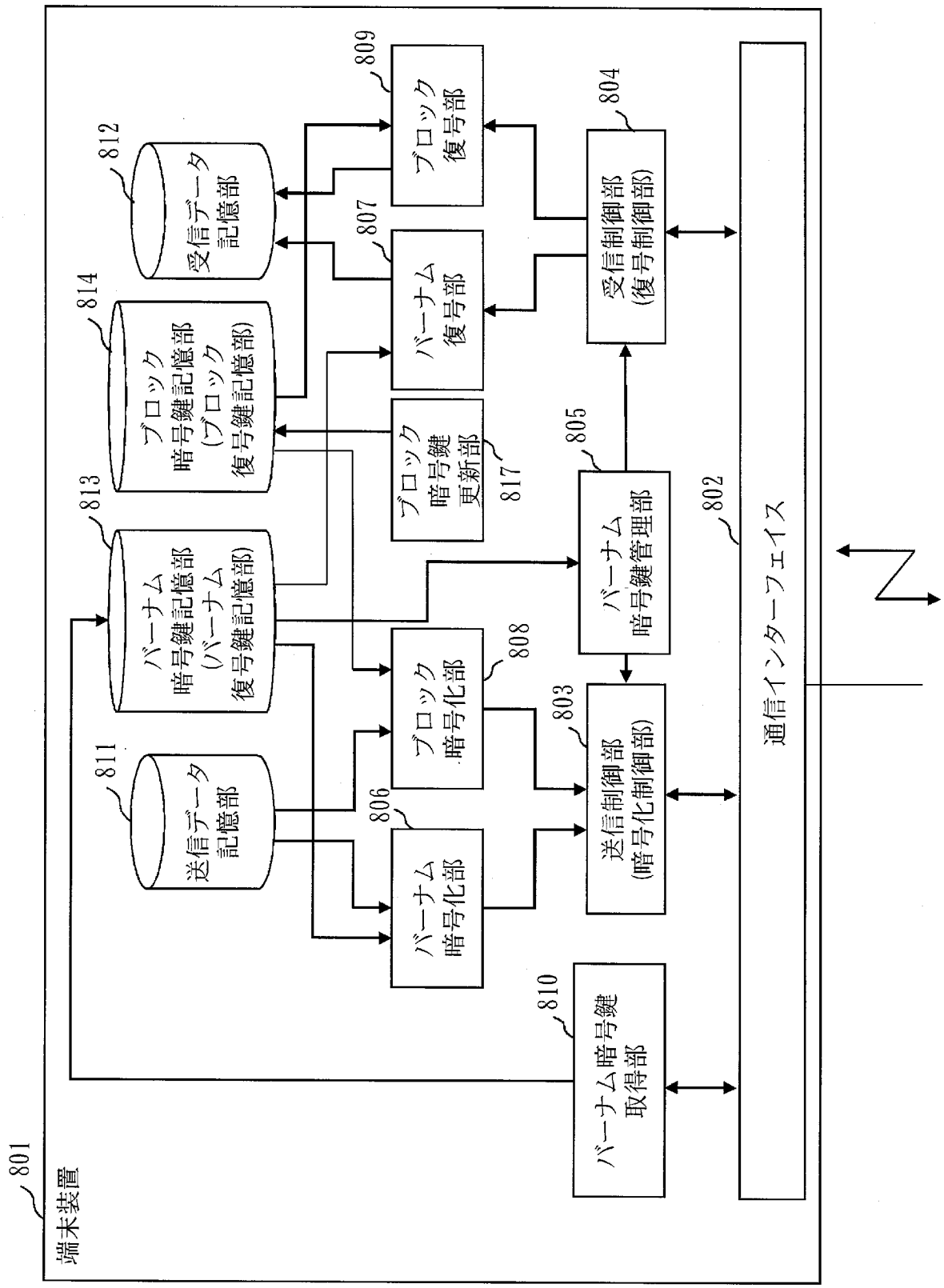
[図25]


102
103
2507
要求メッセージ
2508
了承メッセージ
2509
暗号化通信データ
端末装置A
端末装置B
ブロック
暗号鍵1
2501
ブロック
暗号鍵2
2502
ブロック
暗号鍵n
2503
ブロック
暗号鍵1
2504
ブロック
暗号鍵2
2505
ブロック
暗号鍵n
2506

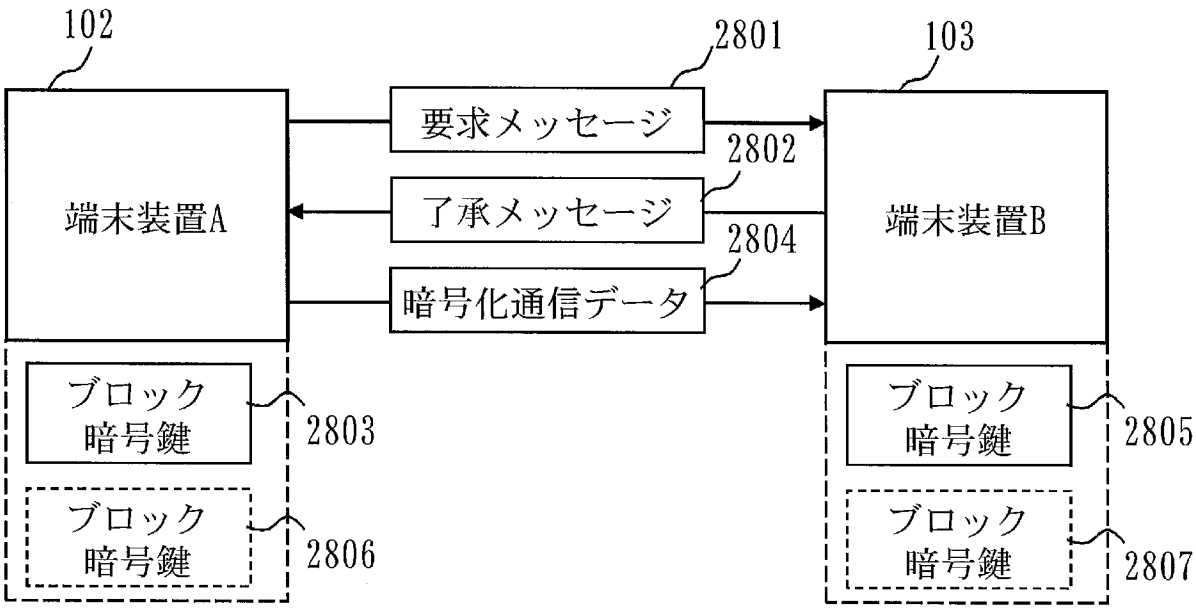
[図26]


端末装置A102
S801
バーナム暗号が可能なデータ量を算出する
S802
ブロック暗号通信要求メッセージを送信する
S805
ブロック暗号通信了承メッセージを受信する
S806
通信データをブロック暗号で暗号化する
暗号化通信データを送信する
S807
S810
YES
未送信データは残っているか?
NO
S811
現在のブロック暗号鍵を破棄し、次のブロック暗号鍵を設定する。
S812
処理を終了する
端末装置B103
ブロック暗号通信要求メッセージを受信する
S803
ブロック暗号通信了承メッセージを送信する
S804
S808
暗号化通信データを受信する
暗号化通信データをブロック暗号で復号する
S809
S813
未受信データは残っているか?
YES
NO
S814
現在のブロック暗号鍵を破棄し、次のブロック暗号鍵を設定する。
S815
処理を終了する

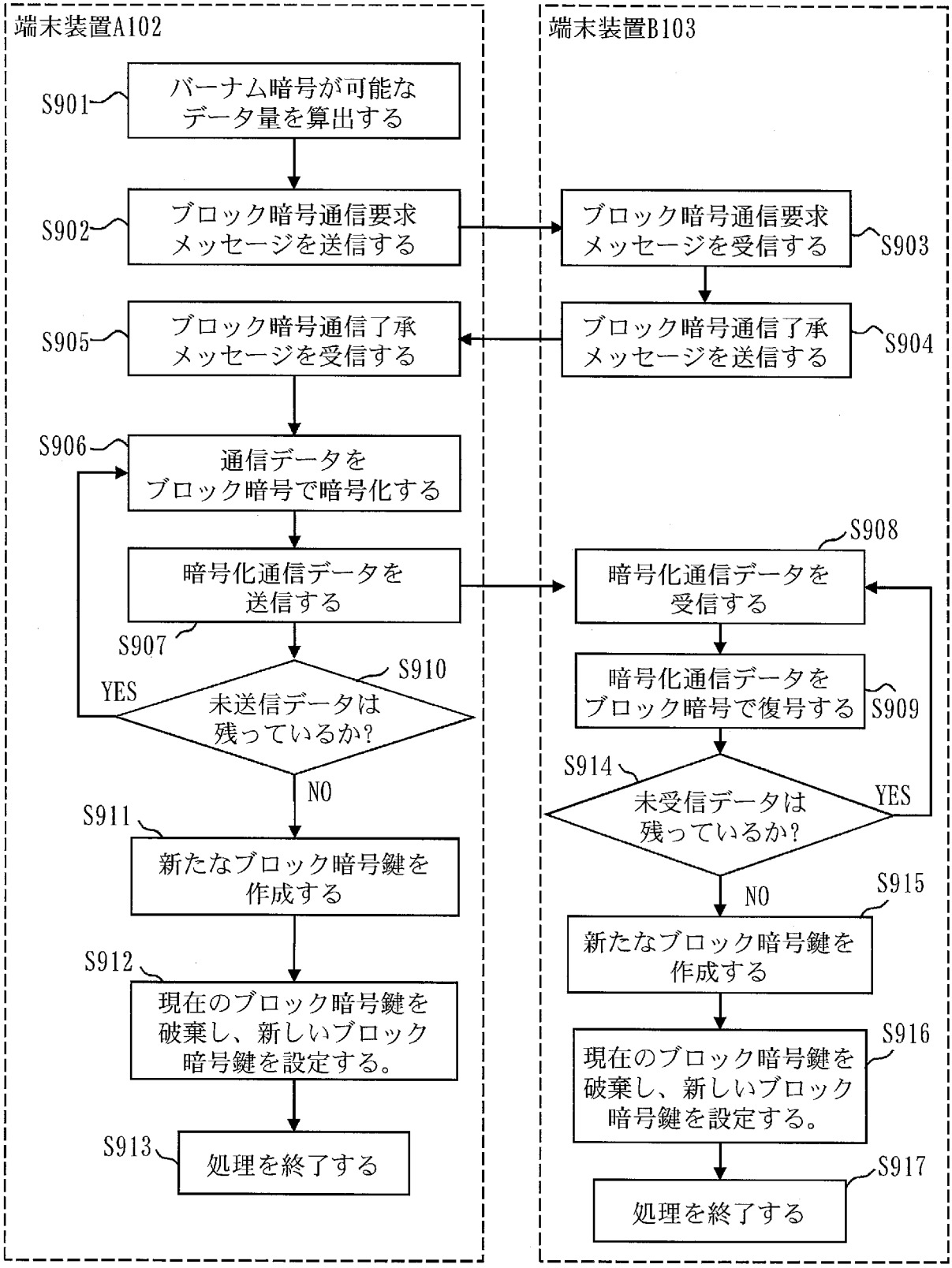
[図27]


801
端末装置
802
通信インターフェイス
803
送信制御部
(暗号化制御部)
804
受信制御部
(復号制御部)
805
バーナム
暗号鍵管理部
806
バーナム
暗号化部
807
バーナム
復号部
808
ブロック
暗号化部
809
ブロック
復号部
810
バーナム暗号鍵
取得部
811
送信データ
記憶部
812
受信データ
記憶部
813
バーナム
暗号鍵記憶部
(バーナム
復号鍵記憶部)
814
ブロック
暗号鍵記憶部
(ブロック
復号鍵記憶部)
817
ブロック
暗号鍵
更新部

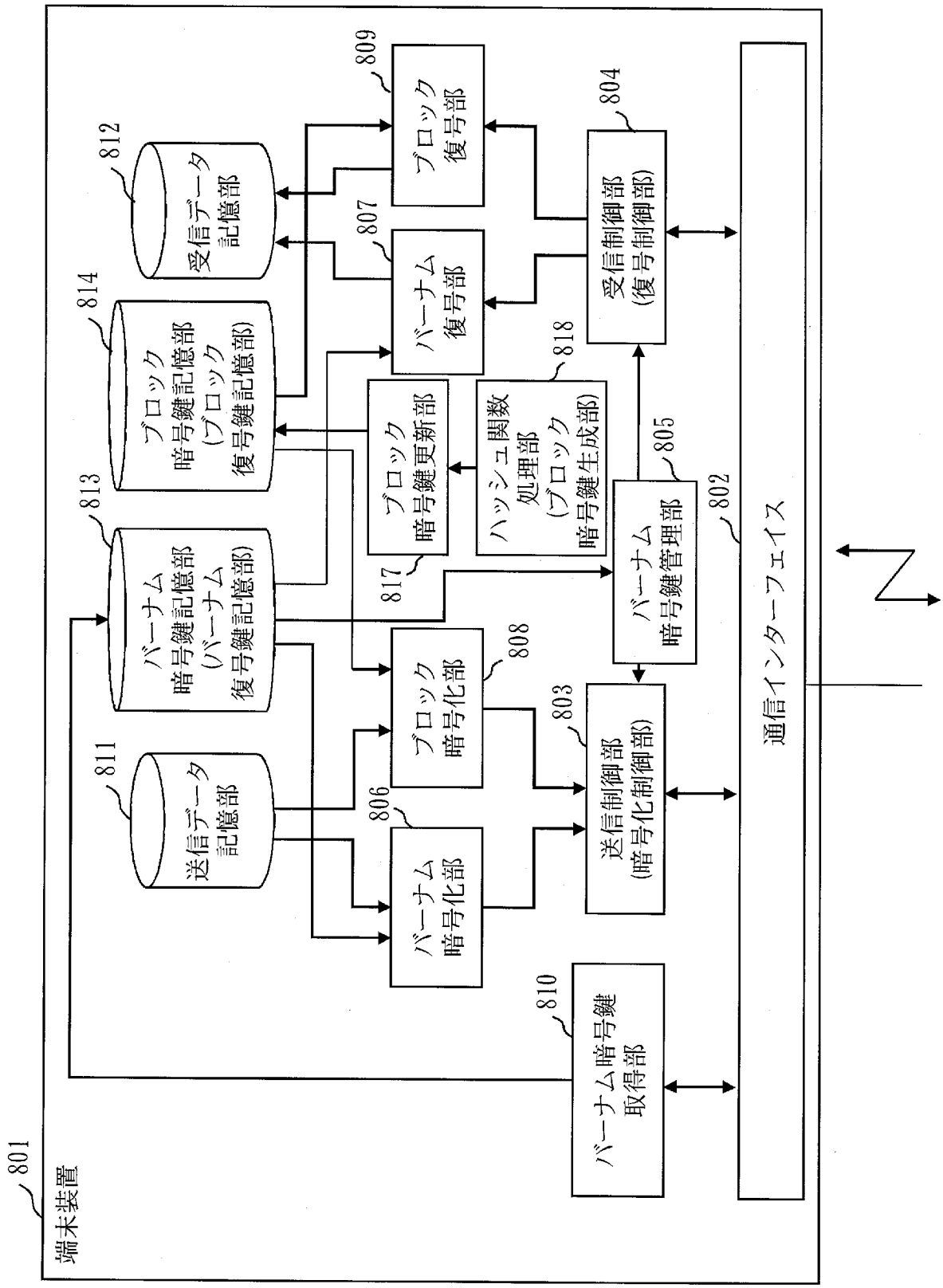
[図28]


102
2801
103
要求メッセージ
2802
了承メッセージ
端末装置A
2804
暗号化通信データ
端末装置B
ブロック
暗号鍵
2803
ブロック
暗号鍵
2805
ブロック
暗号鍵
2806
ブロック
暗号鍵
2807

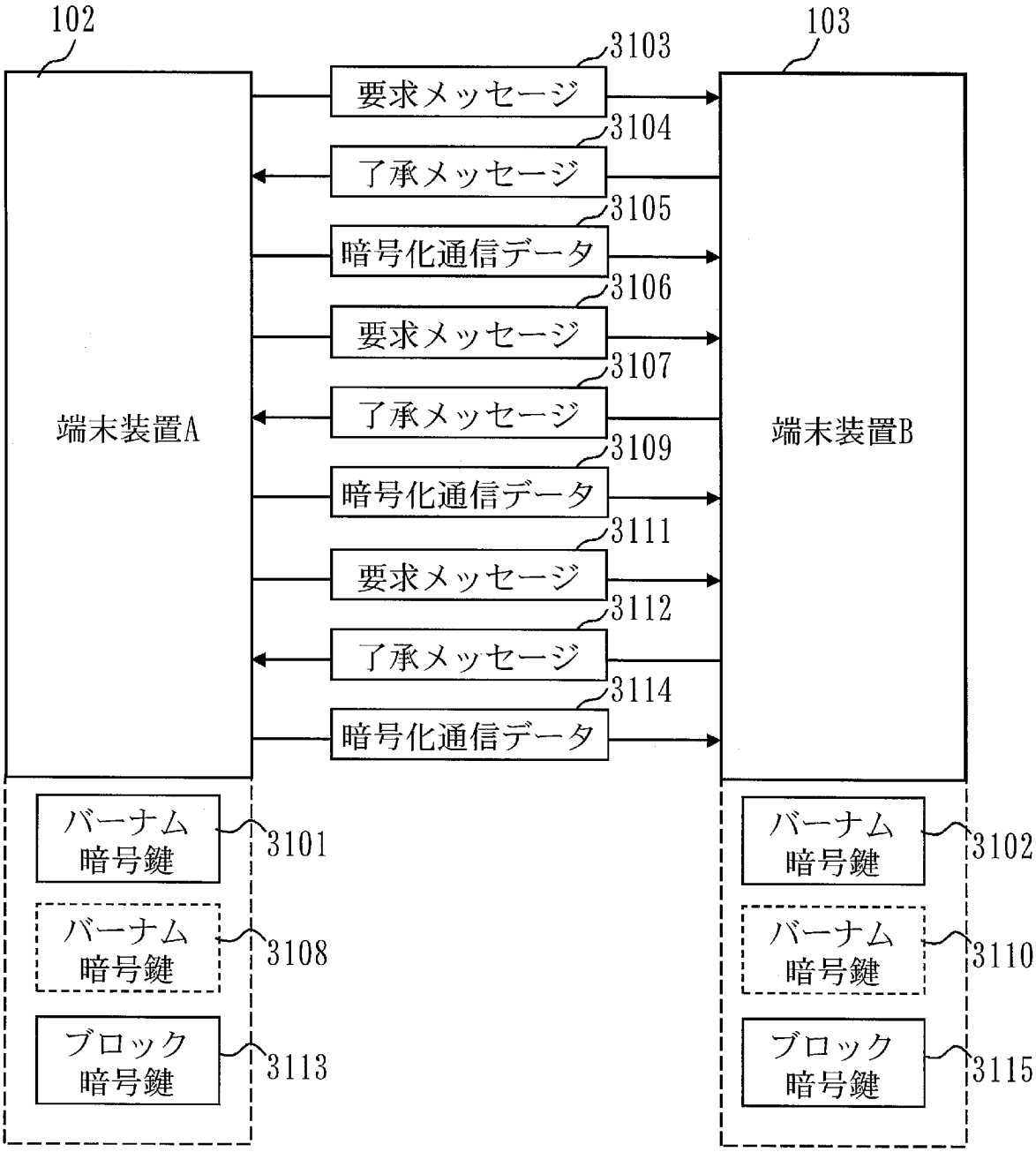
[図29]


端末装置A102
端末装置B103
S901
バーナム暗号が可能なデータ量を算出する
S902
ブロック暗号通信要求メッセージを送信する
S903
ブロック暗号通信要求メッセージを受信する
S904
ブロック暗号通信了承メッセージを送信する
S905
ブロック暗号通信了承メッセージを受信する
S906
通信データをブロック暗号で暗号化する
S907
暗号化通信データを送信する
S908
暗号化通信データを受信する
S909
暗号化通信データをブロック暗号で復号する
S910
未送信データは残っているか?
YES
NO
S911
新たなブロック暗号鍵を作成する
S912
現在のブロック暗号鍵を破棄し、新しいブロック暗号鍵を設定する。
S913
処理を終了する
S914
未受信データは残っているか?
YES
NO
S915
新たなブロック暗号鍵を作成する
S916
現在のブロック暗号鍵を破棄し、新しいブロック暗号鍵を設定する。
S917
処理を終了する

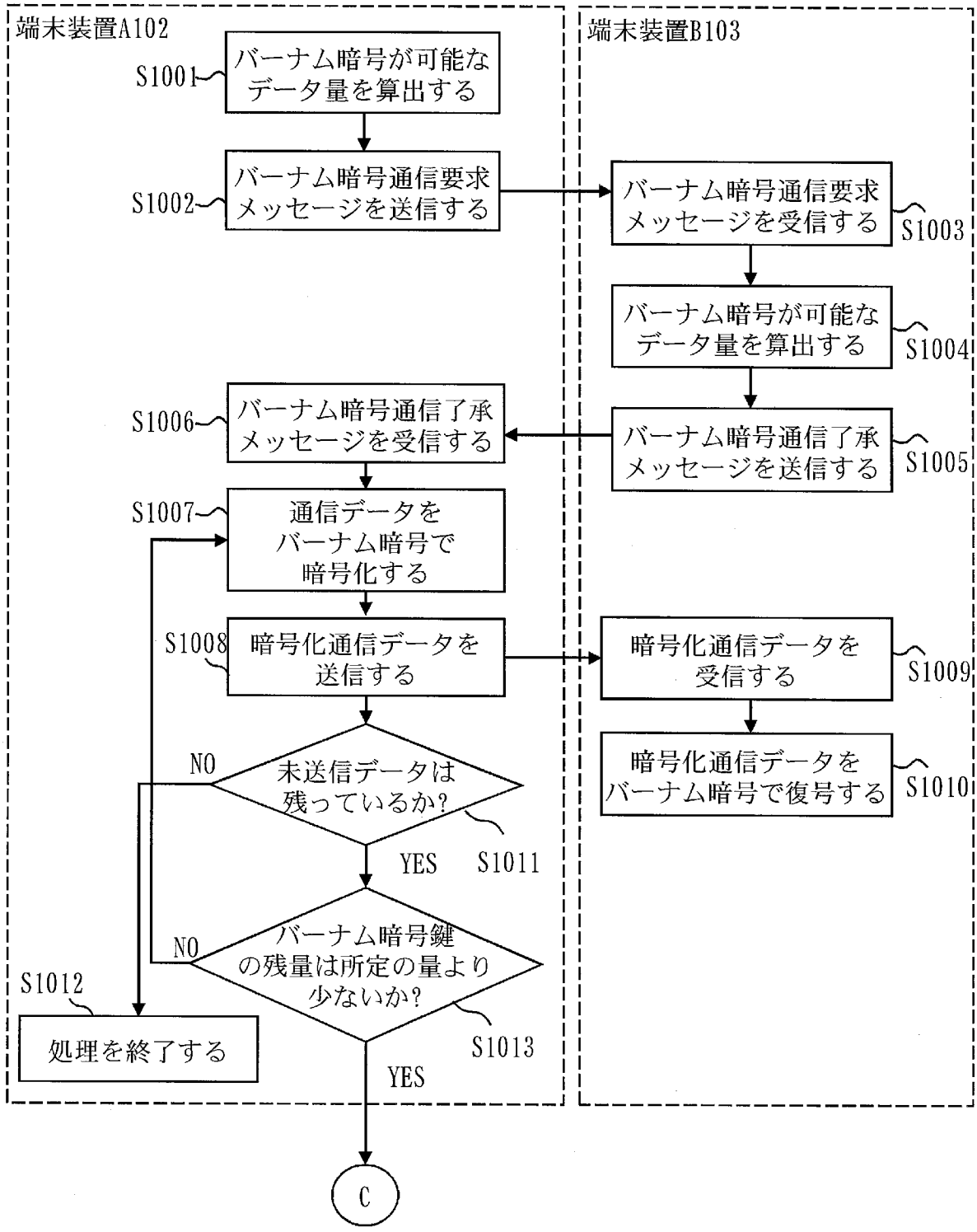
[図30]


801
端末装置
802
通信インターフェイス
803
送信制御部
(暗号化制御部)
804
受信制御部
(復号制御部)
805
バーナム
暗号鍵管理部
806
バーナム
暗号化部
807
バーナム
復号部
808
ブロック
暗号化部
809
ブロック
復号部
810
バーナム暗号鍵
取得部
811
送信データ
記憶部
812
受信データ
記憶部
813
バーナム
暗号鍵記憶部
(バーナム
復号鍵記憶部)
814
ブロック
暗号鍵記憶部
(ブロック
復号鍵記憶部)
817
ブロック
暗号鍵更新部
818
ハッシュ関数
処理部
(ブロック
暗号鍵生成部)

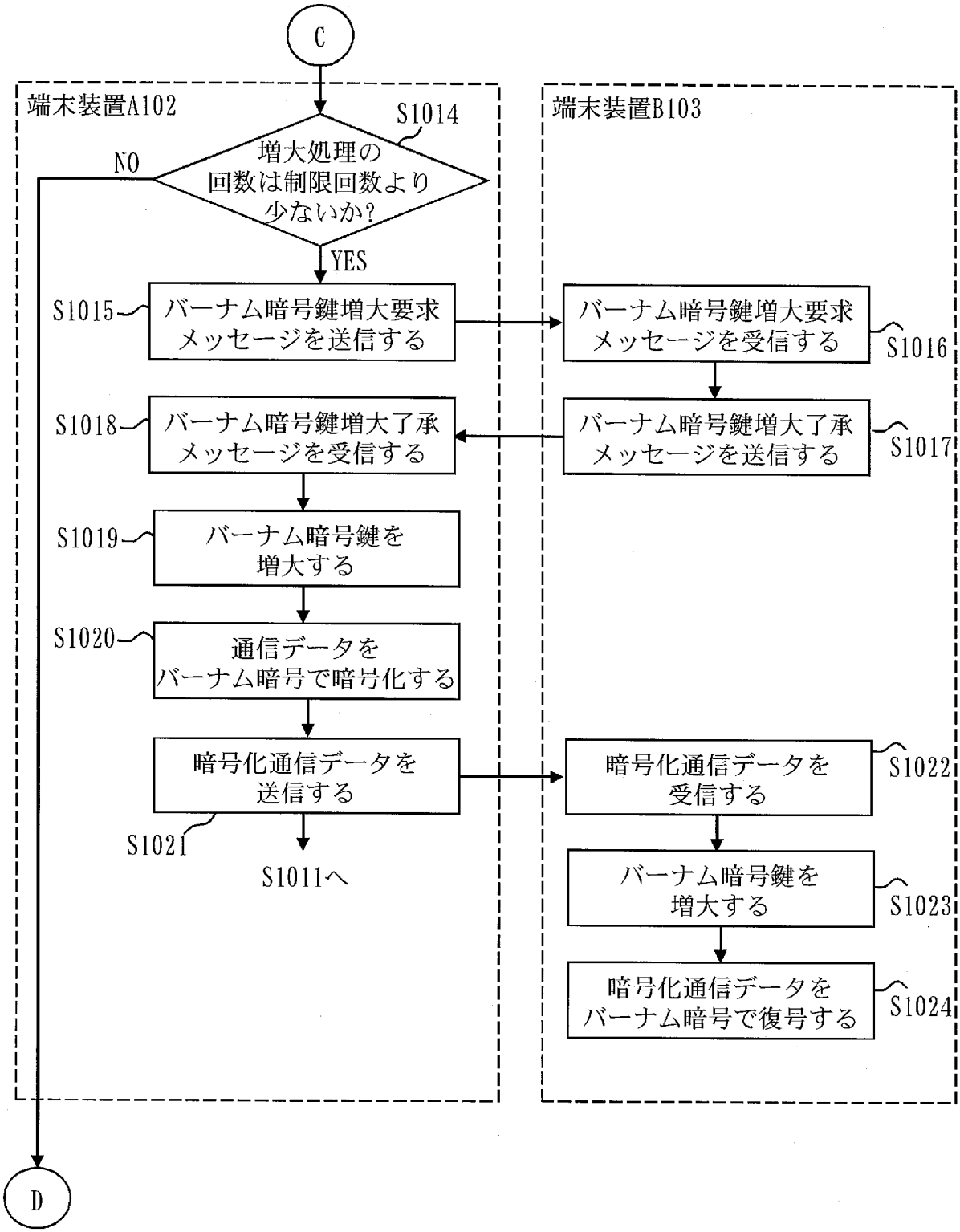
[図31]


102
103
3103
要求メッセージ
3104
了承メッセージ
3105
暗号化通信データ
3106
要求メッセージ
3107
了承メッセージ
3109
暗号化通信データ
3111
要求メッセージ
3112
了承メッセージ
3114
暗号化通信データ
端末装置A
端末装置B
バーナム暗号鍵
3101
バーナム暗号鍵
3108
ブロック暗号鍵
3113
バーナム暗号鍵
3102
バーナム暗号鍵
3110
ブロック暗号鍵
3115

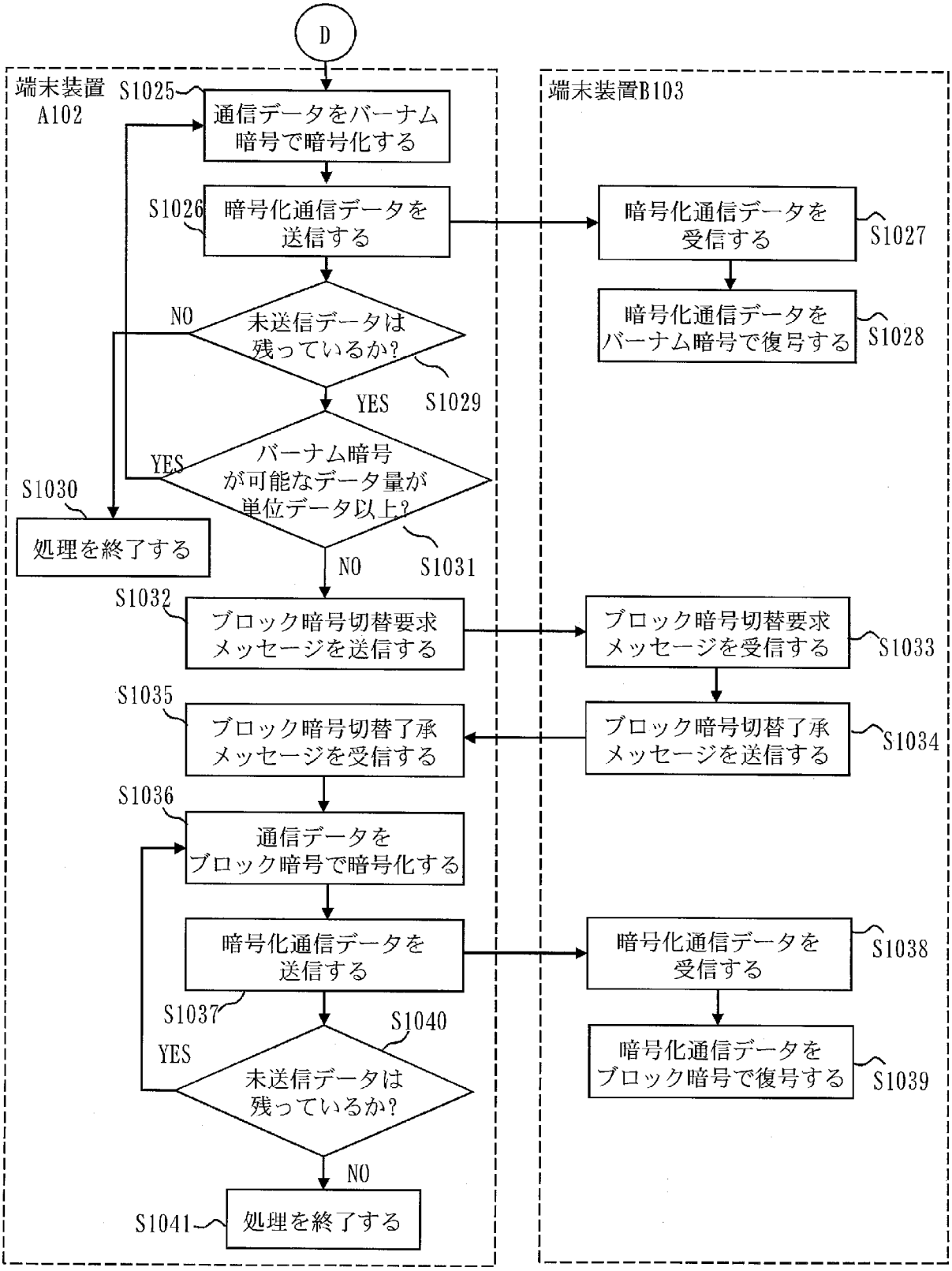
[図32]


端末装置A102
端末装置B103
S1001
バーナム暗号が可能なデータ量を算出する
S1002
バーナム暗号通信要求メッセージを送信する
バーナム暗号通信要求メッセージを受信する
S1003
バーナム暗号が可能なデータ量を算出する
S1004
バーナム暗号通信了承メッセージを送信する
S1005
S1006
バーナム暗号通信了承メッセージを受信する
S1007
通信データをバーナム暗号で暗号化する
S1008
暗号化通信データを送信する
暗号化通信データを受信する
S1009
暗号化通信データをバーナム暗号で復号する
S1010
NO
未送信データは残っているか?
S1011
YES
NO
バーナム暗号鍵の残量は所定の量より少ないか?
S1013
YES
S1012
処理を終了する
C

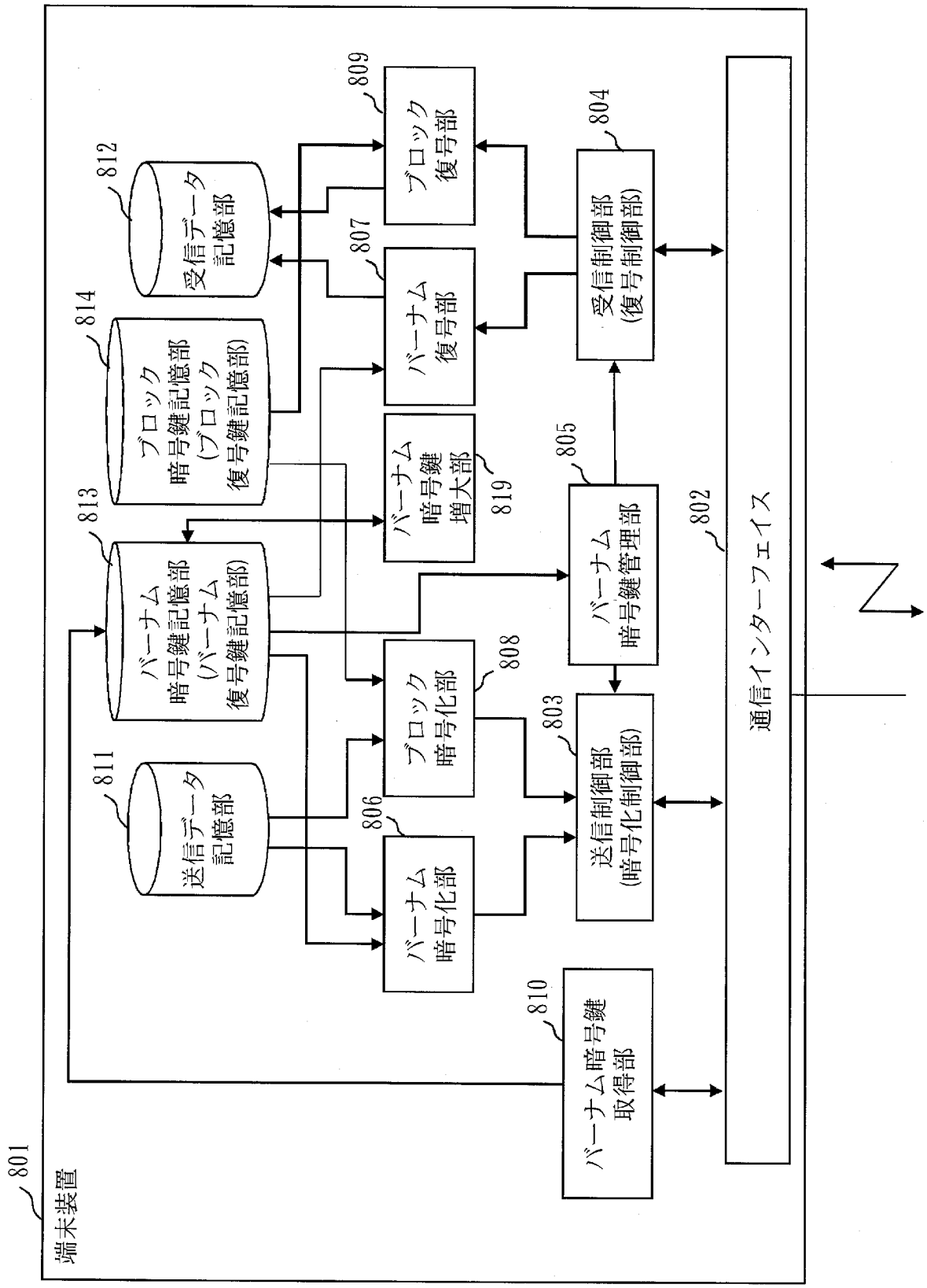
[図33]


C
端末装置A102
端末装置B103
S1014
増大処理の回数は制限回数より少ないか?
NO
YES
S1015
バーナム暗号鍵増大要求メッセージを送信する
バーナム暗号鍵増大要求メッセージを受信する
S1016
S1018
バーナム暗号鍵増大了承メッセージを受信する
バーナム暗号鍵増大了承メッセージを送信する
S1017
S1019
バーナム暗号鍵を増大する
S1020
通信データをバーナム暗号で暗号化する
暗号化通信データを送信する
暗号化通信データを受信する
S1022
S1021
S1011へ
バーナム暗号鍵を増大する
S1023
暗号化通信データをバーナム暗号で復号する
S1024
D

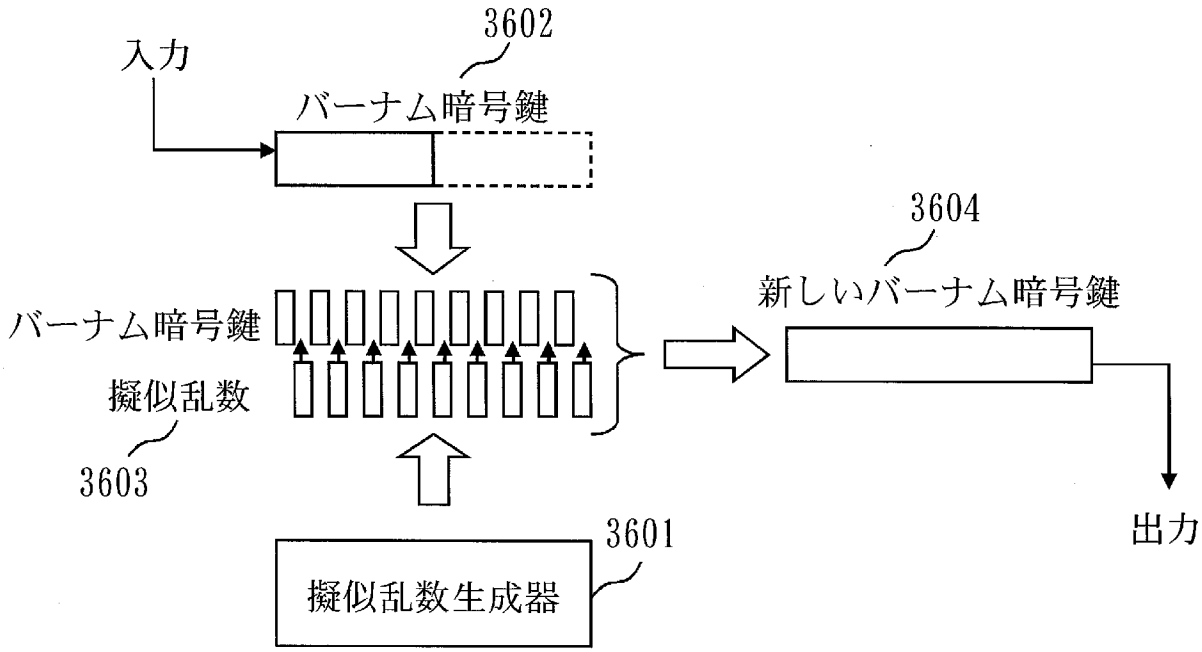
[図34]


D
端末装置 A102
端末装置B103
S1025
通信データをバーナム暗号で暗号化する
S1026
暗号化通信データを送信する
暗号化通信データを受信する
S1027
暗号化通信データをバーナム暗号で復号する
S1028
NO
未送信データは残っているか?
S1029
YES
YES
バーナム暗号が可能なデータ量が単位データ以上?
S1030
処理を終了する
NO
S1031
S1032
ブロック暗号切替要求メッセージを送信する
ブロック暗号切替要求メッセージを受信する
S1033
S1035
ブロック暗号切替了承メッセージを受信する
ブロック暗号切替了承メッセージを送信する
S1034
S1036
通信データをブロック暗号で暗号化する
暗号化通信データを送信する
暗号化通信データを受信する
S1038
S1037
S1040
YES
未送信データは残っているか?
暗号化通信データをブロック暗号で復号する
S1039
NO
S1041
処理を終了する

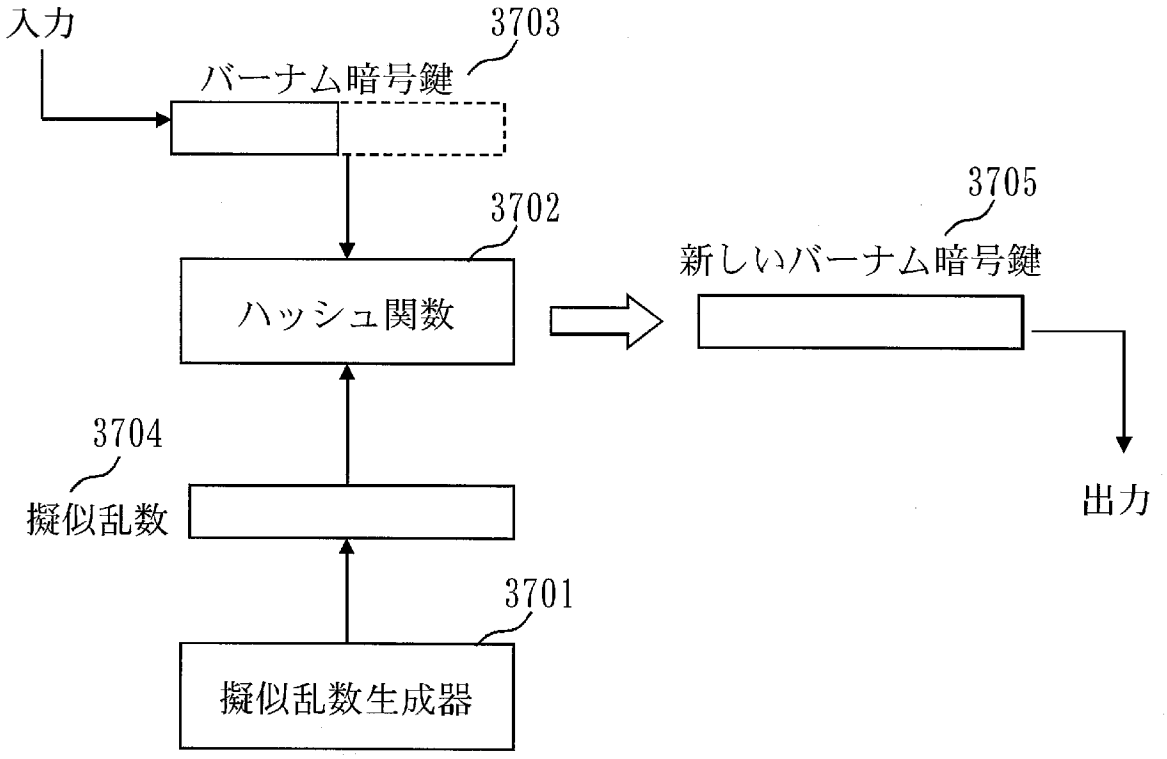
[図35]


801
端末装置
802
通信インターフェイス
803
送信制御部
(暗号化制御部)
804
受信制御部
(復号制御部)
805
バーナム
暗号鍵管理部
806
バーナム
暗号化部
807
バーナム
復号部
808
ブロック
暗号化部
809
ブロック
復号部
810
バーナム暗号鍵
取得部
811
送信データ
記憶部
812
受信データ
記憶部
813
バーナム
暗号鍵記憶部
(バーナム
復号鍵記憶部)
814
ブロック
暗号鍵記憶部
(ブロック
復号鍵記憶部)
819
バーナム
暗号鍵
増大部

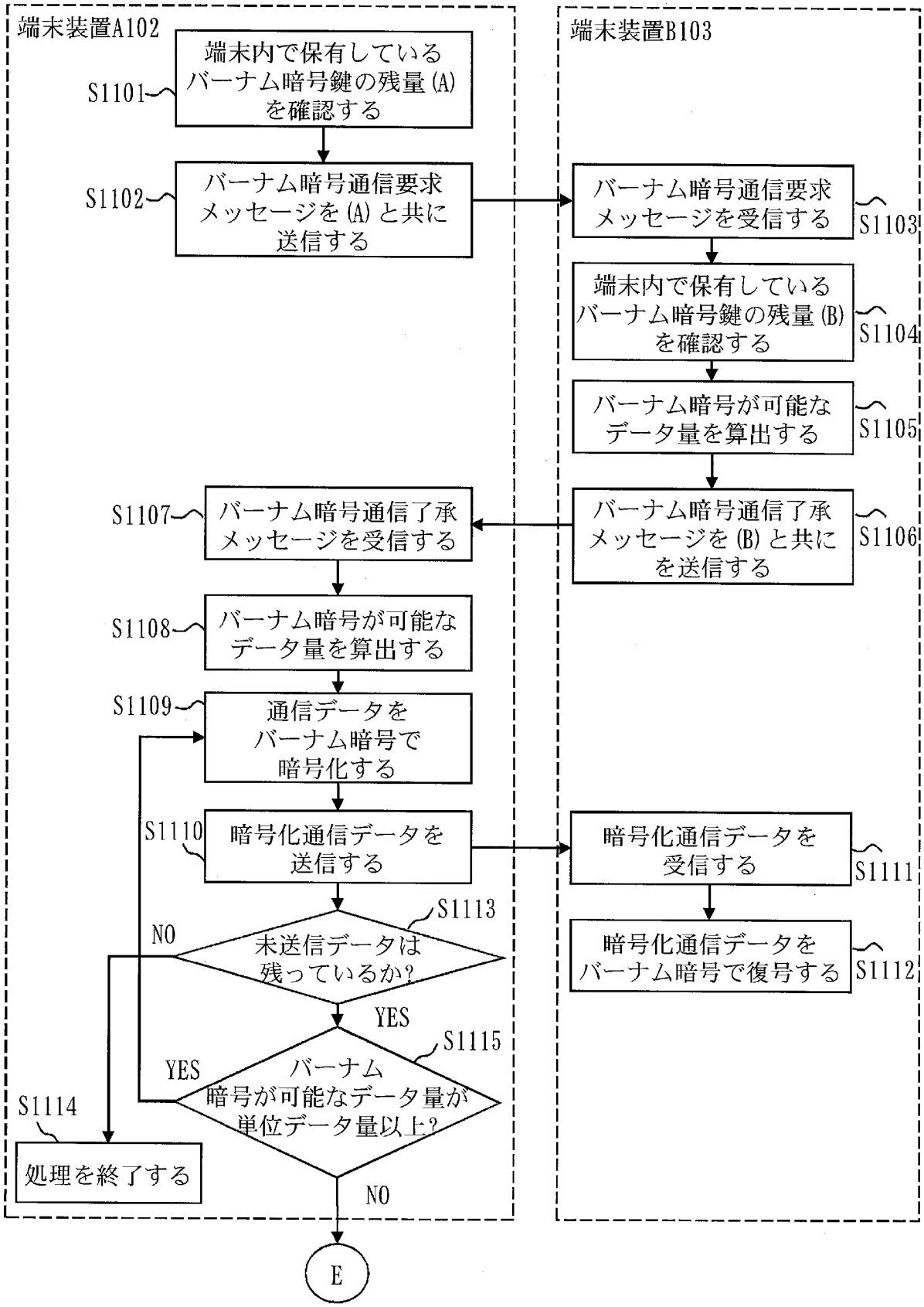
[図36]


入力
3602
バーナム暗号鍵
3604
新しいバーナム暗号鍵
バーナム暗号鍵
擬似乱数
3603
出力
3601
擬似乱数生成器

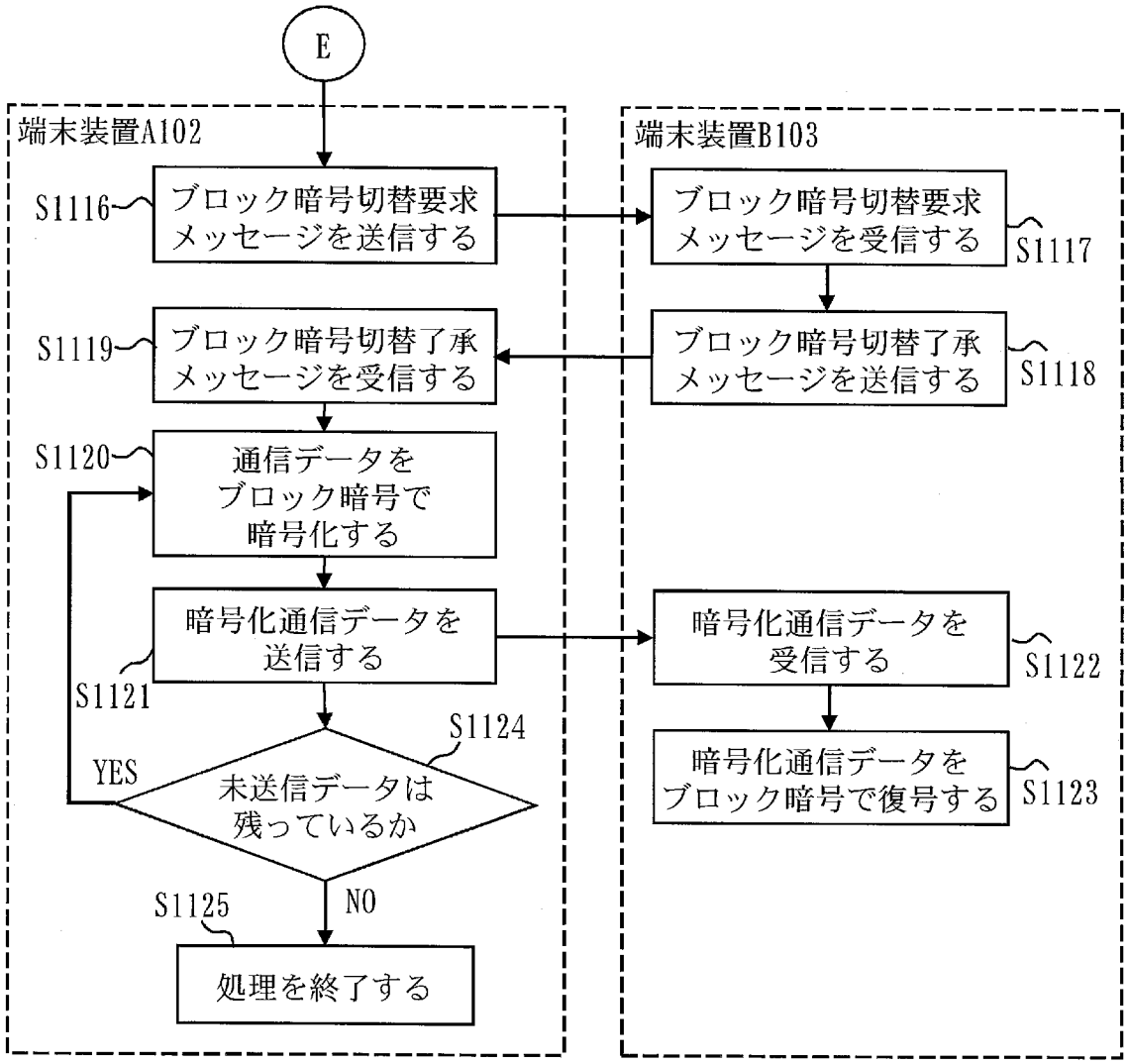
[図37]


入力
3703
バーナム暗号鍵
3705
3702
新しいバーナム暗号鍵
ハッシュ関数
出力
3704
擬似乱数
3701
擬似乱数生成器

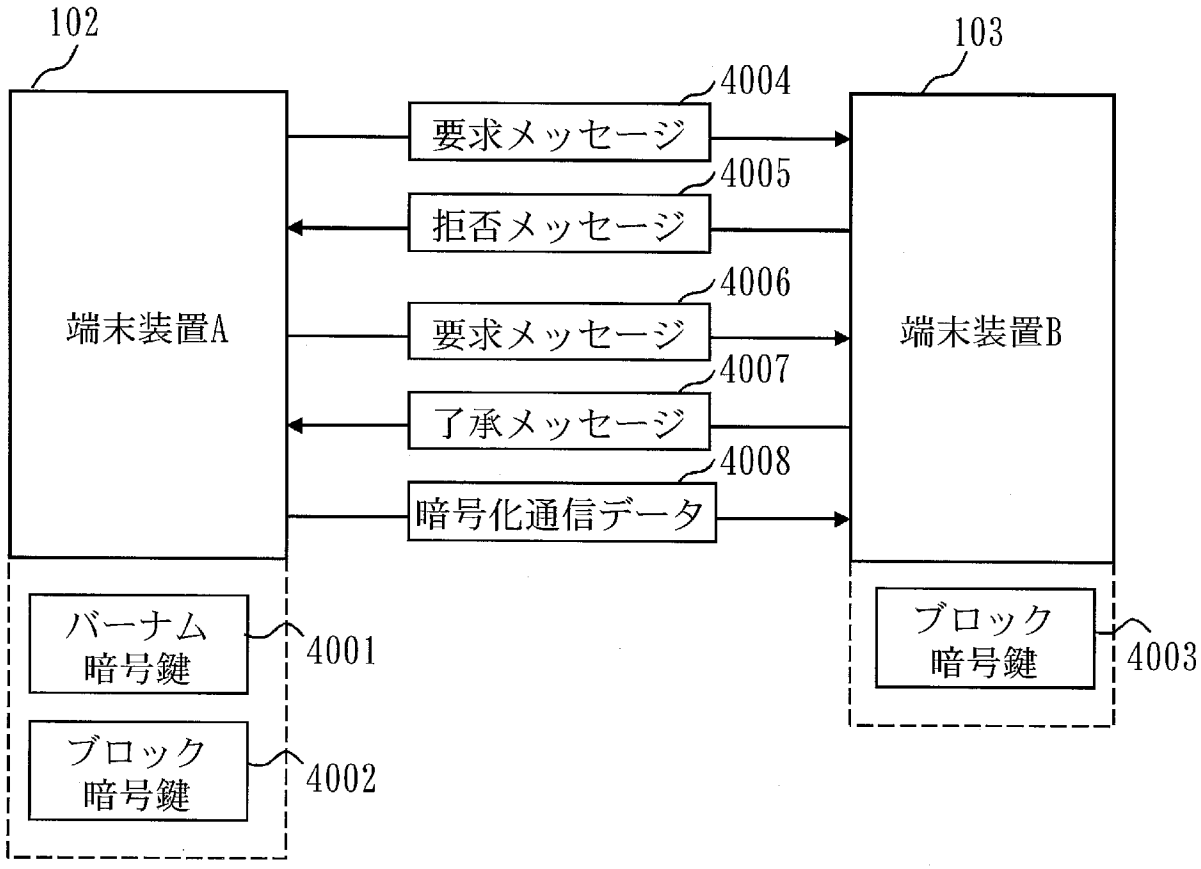
[図38]


端末装置A102
端末装置B103
端末内で保有しているバーナム暗号鍵の残量(A)を確認する
S1101
バーナム暗号通信要求メッセージを(A)と共に送信する
S1102
バーナム暗号通信要求メッセージを受信する
S1103
端末内で保有しているバーナム暗号鍵の残量(B)を確認する
S1104
バーナム暗号が可能なデータ量を算出する
S1105
バーナム暗号通信了承メッセージを(B)と共にを送信する
S1106
バーナム暗号通信了承メッセージを受信する
S1107
バーナム暗号が可能なデータ量を算出する
S1108
通信データをバーナム暗号で暗号化する
S1109
暗号化通信データを送信する
S1110
暗号化通信データを受信する
S1111
暗号化通信データをバーナム暗号で復号する
S1112
未送信データは残っているか?
S1113
NO
YES
バーナム暗号が可能なデータ量が単位データ量以上?
S1115
YES
NO
処理を終了する
S1114
E

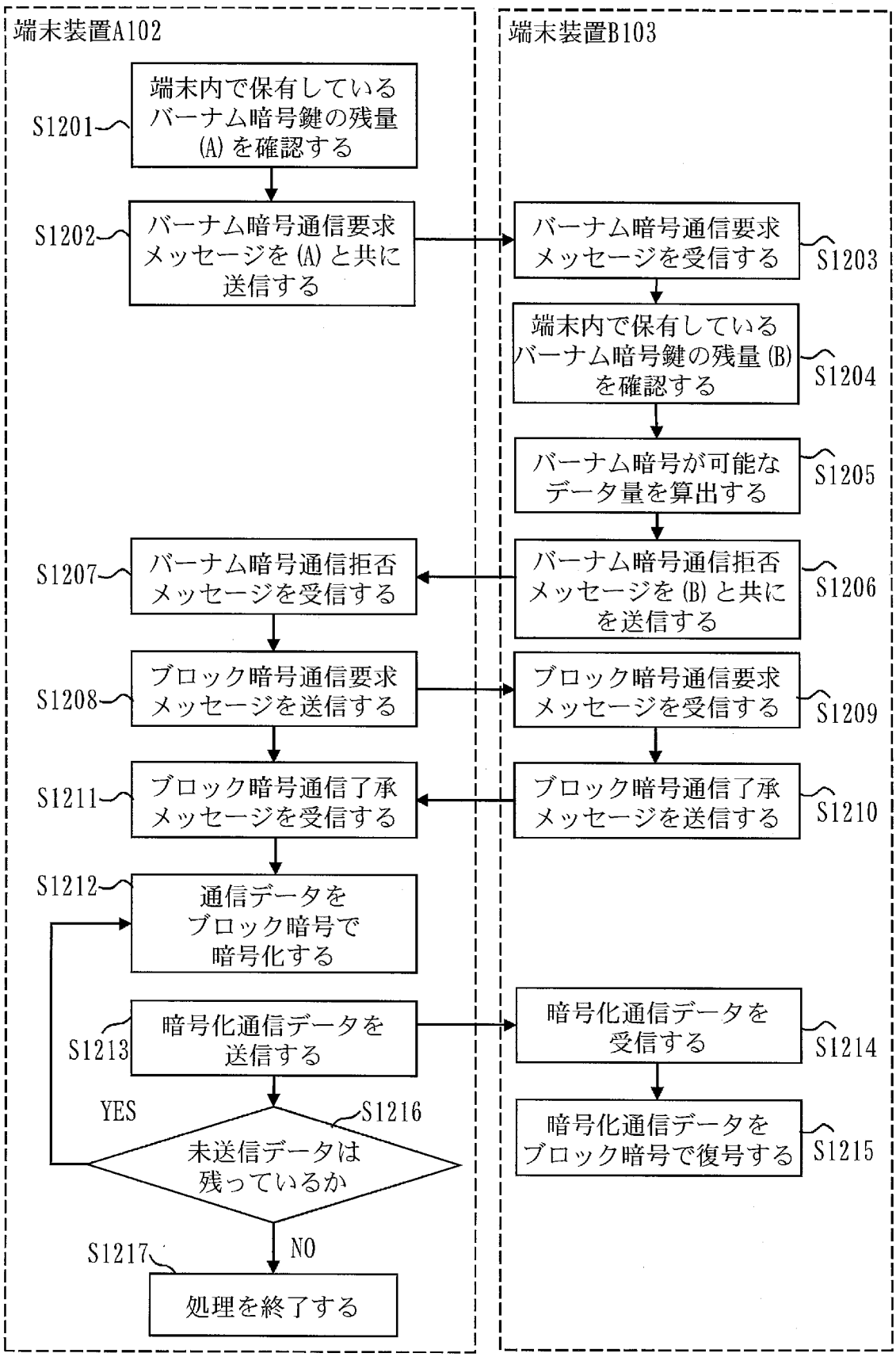
[図39]


E
端末装置A102
端末装置B103
S1116
ブロック暗号切替要求メッセージを送信する
ブロック暗号切替要求メッセージを受信する
S1117
S1119
ブロック暗号切替了承メッセージを受信する
ブロック暗号切替了承メッセージを送信する
S1118
S1120
通信データをブロック暗号で暗号化する
暗号化通信データを送信する
S1121
暗号化通信データを受信する
S1122
S1124
YES
未送信データは残っているか
暗号化通信データをブロック暗号で復号する
S1123
S1125
NO
処理を終了する

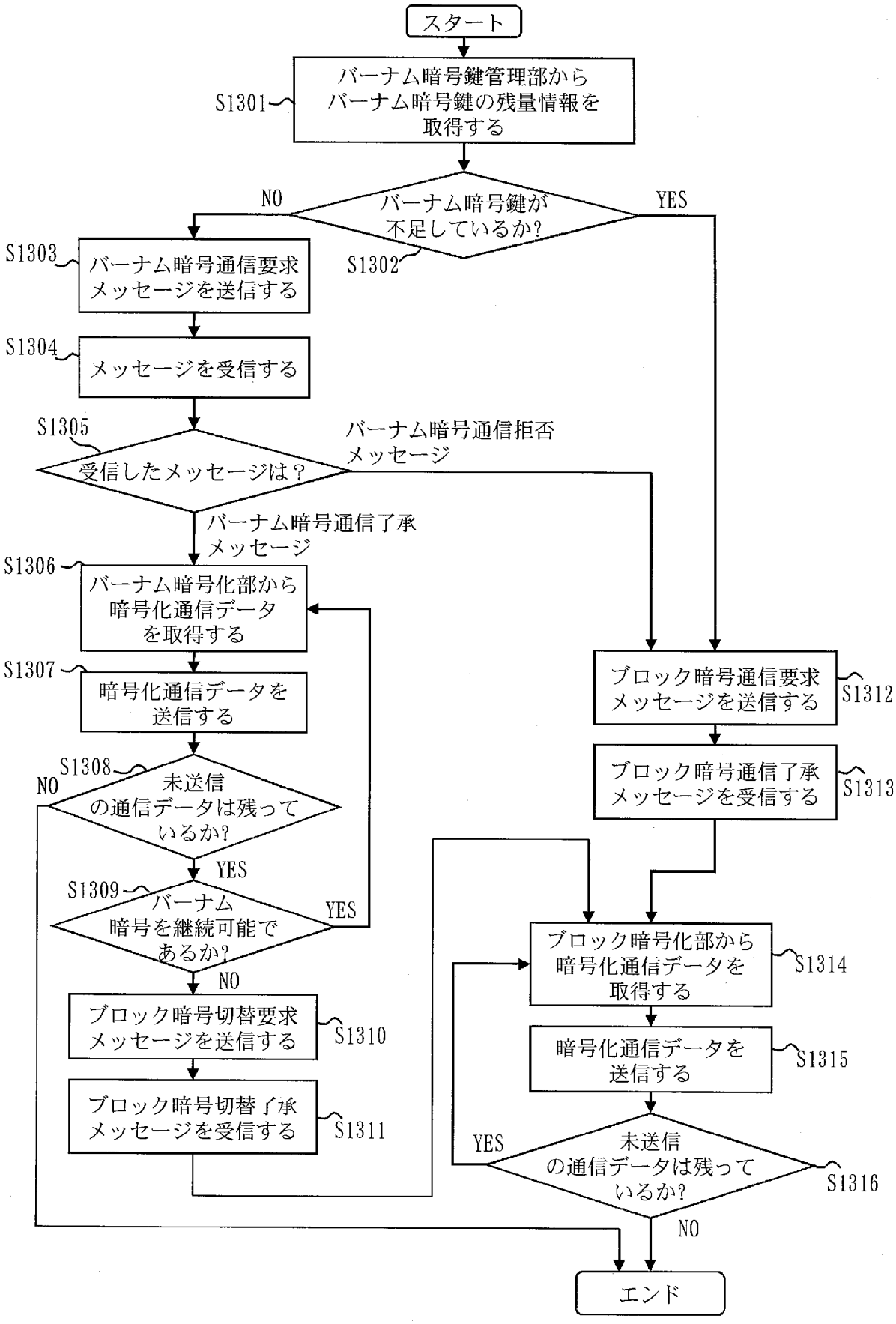
[図40]


102
103
4004
要求メッセージ
4005
拒否メッセージ
4006
要求メッセージ
4007
了承メッセージ
4008
暗号化通信データ
端末装置A
端末装置B
バーナム
暗号鍵
4001
ブロック
暗号鍵
4002
ブロック
暗号鍵
4003

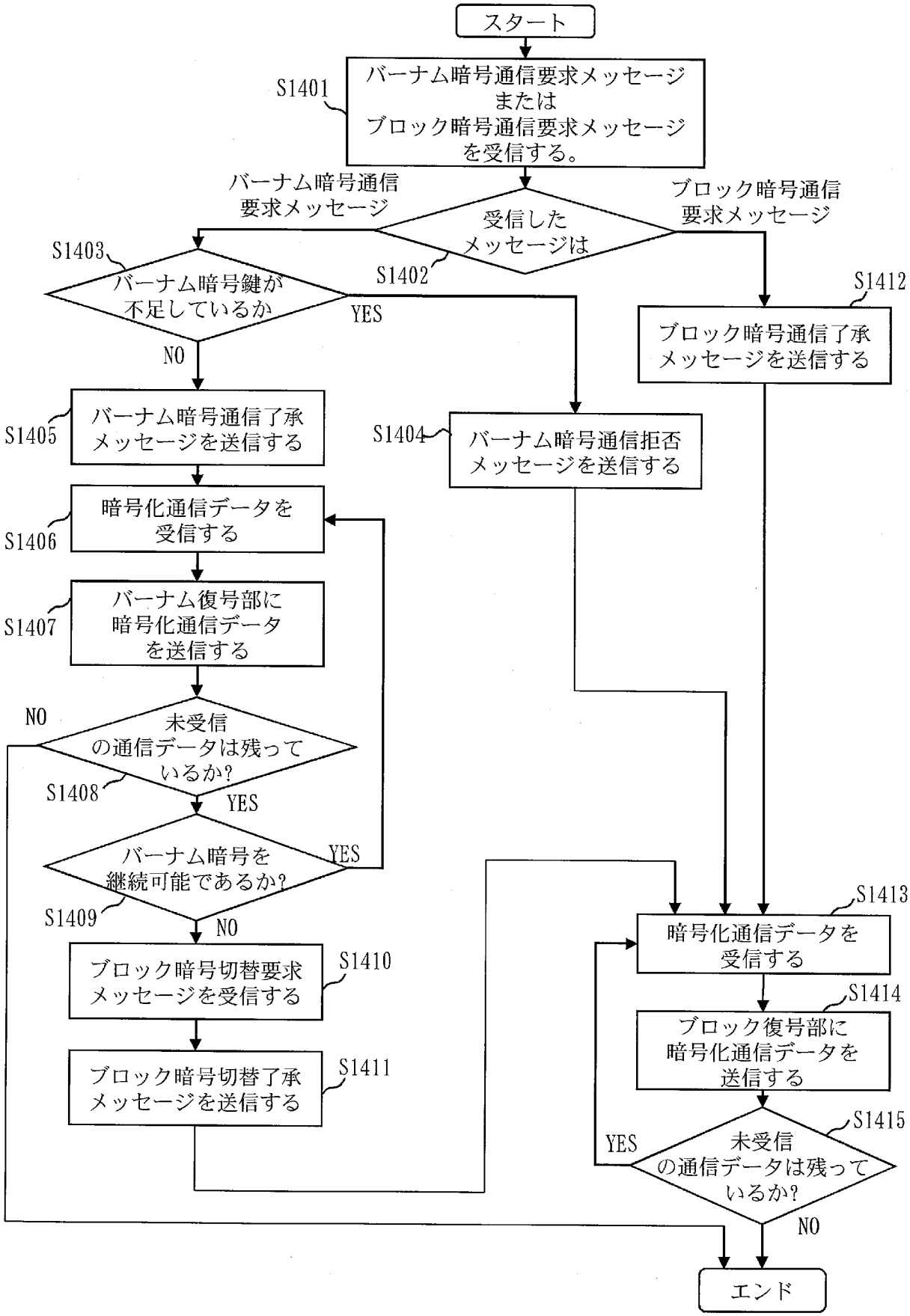
[図41]


端末装置A102
端末装置B103
端末内で保有しているバーナム暗号鍵の残量(A)を確認する
S1201
バーナム暗号通信要求メッセージを(A)と共に送信する
S1202
バーナム暗号通信要求メッセージを受信する
S1203
端末内で保有しているバーナム暗号鍵の残量(B)を確認する
S1204
バーナム暗号が可能なデータ量を算出する
S1205
バーナム暗号通信拒否メッセージを(B)と共にを送信する
S1206
バーナム暗号通信拒否メッセージを受信する
S1207
ブロック暗号通信要求メッセージを送信する
S1208
ブロック暗号通信要求メッセージを受信する
S1209
ブロック暗号通信了承メッセージを送信する
S1210
ブロック暗号通信了承メッセージを受信する
S1211
通信データをブロック暗号で暗号化する
S1212
暗号化通信データを送信する
S1213
暗号化通信データを受信する
S1214
暗号化通信データをブロック暗号で復号する
S1215
未送信データは残っているか
S1216
YES
NO
処理を終了する
S1217

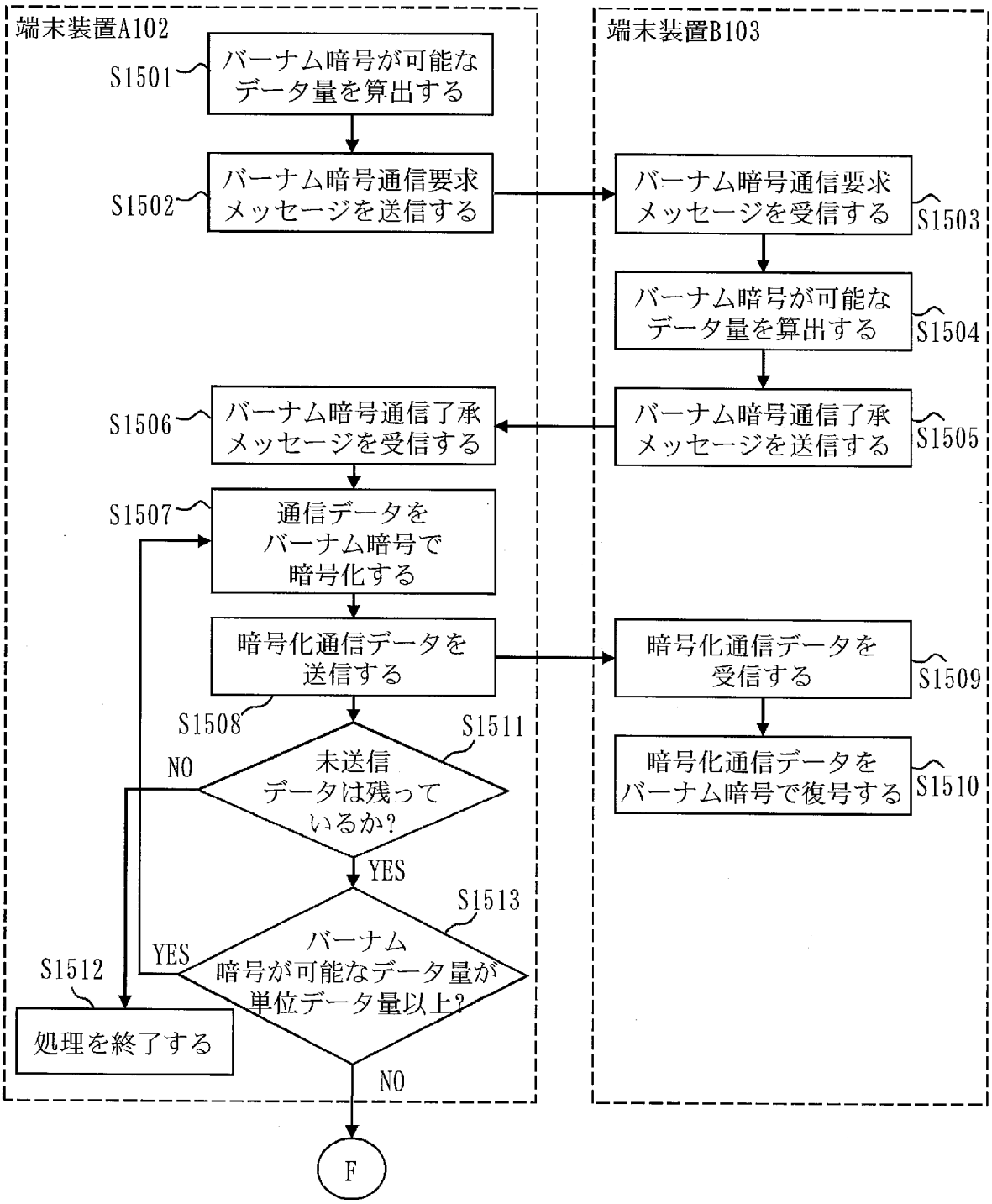
[図42]


スタート
S1301
バーナム暗号鍵管理部から
バーナム暗号鍵の残量情報を
取得する
バーナム暗号鍵が
不足しているか?
S1302
NO
YES
S1303
バーナム暗号通信要求
メッセージを送信する
S1304
メッセージを受信する
S1305
受信したメッセージは?
バーナム暗号通信拒否
メッセージ
バーナム暗号通信了承
メッセージ
S1306
バーナム暗号化部から
暗号化通信データ
を取得する
S1307
暗号化通信データを
送信する
S1308
未送信
の通信データは残って
いるか?
NO
YES
S1309
バーナム
暗号を継続可能で
あるか?
YES
NO
S1310
ブロック暗号切替要求
メッセージを送信する
S1311
ブロック暗号切替了承
メッセージを受信する
S1312
ブロック暗号通信要求
メッセージを送信する
S1313
ブロック暗号通信了承
メッセージを受信する
S1314
ブロック暗号化部から
暗号化通信データを
取得する
S1315
暗号化通信データを
送信する
S1316
未送信
の通信データは残って
いるか?
YES
NO
エンド

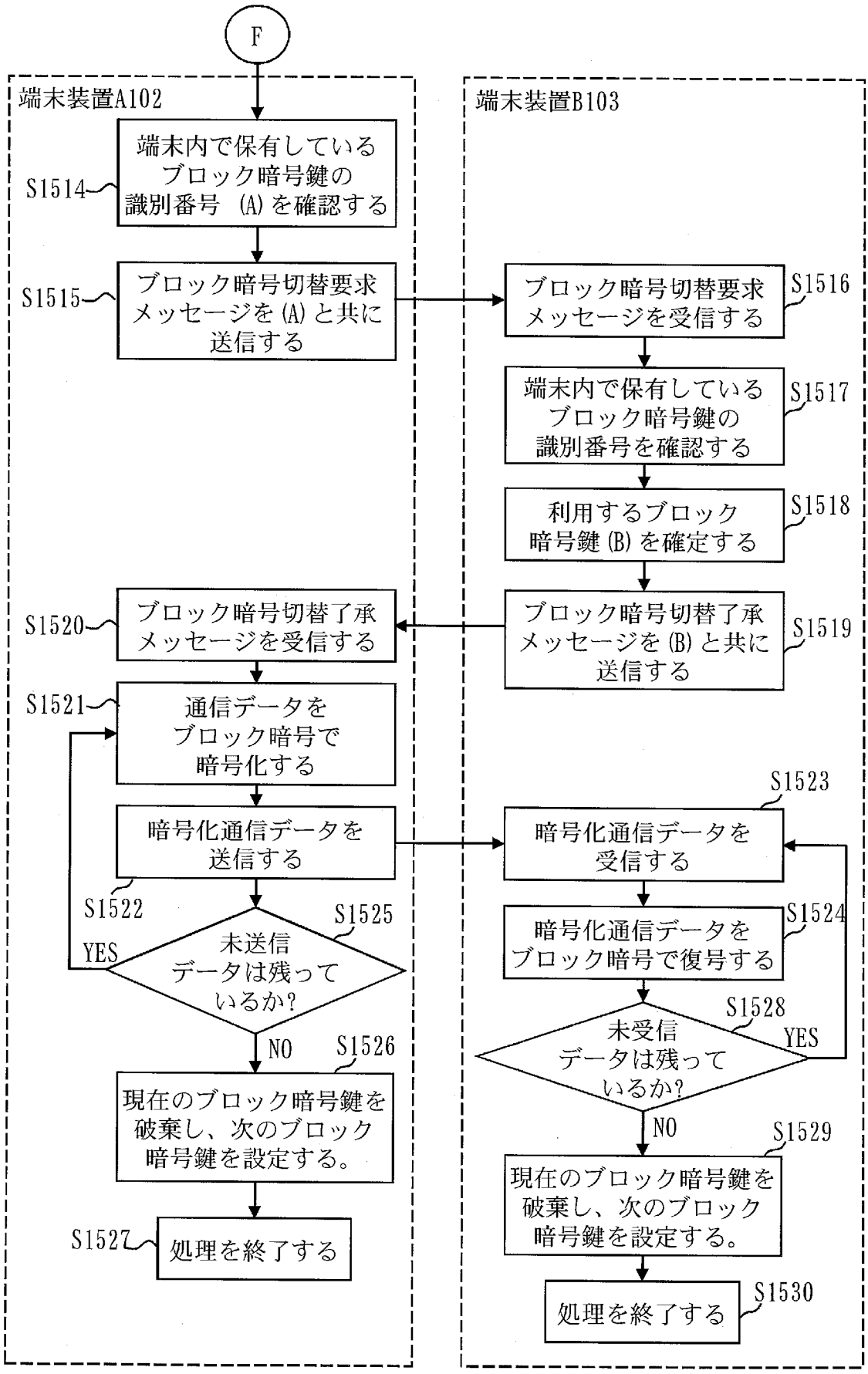
[図43]


スタート
S1401
バーナム暗号通信要求メッセージ
または
ブロック暗号通信要求メッセージ
を受信する。
バーナム暗号通信
要求メッセージ
受信した
メッセージは
S1402
ブロック暗号通信
要求メッセージ
S1403
バーナム暗号鍵が
不足しているか
YES
NO
S1412
ブロック暗号通信了承
メッセージを送信する
S1405
バーナム暗号通信了承
メッセージを送信する
S1404
バーナム暗号通信拒否
メッセージを送信する
S1406
暗号化通信データを
受信する
S1407
バーナム復号部に
暗号化通信データ
を送信する
NO
未受信
の通信データは残って
いるか?
S1408
YES
バーナム暗号を
継続可能であるか?
YES
S1409
NO
S1410
ブロック暗号切替要求
メッセージを受信する
S1411
ブロック暗号切替了承
メッセージを送信する
S1413
暗号化通信データを
受信する
S1414
ブロック復号部に
暗号化通信データを
送信する
S1415
YES
未受信
の通信データは残って
いるか?
NO
エンド

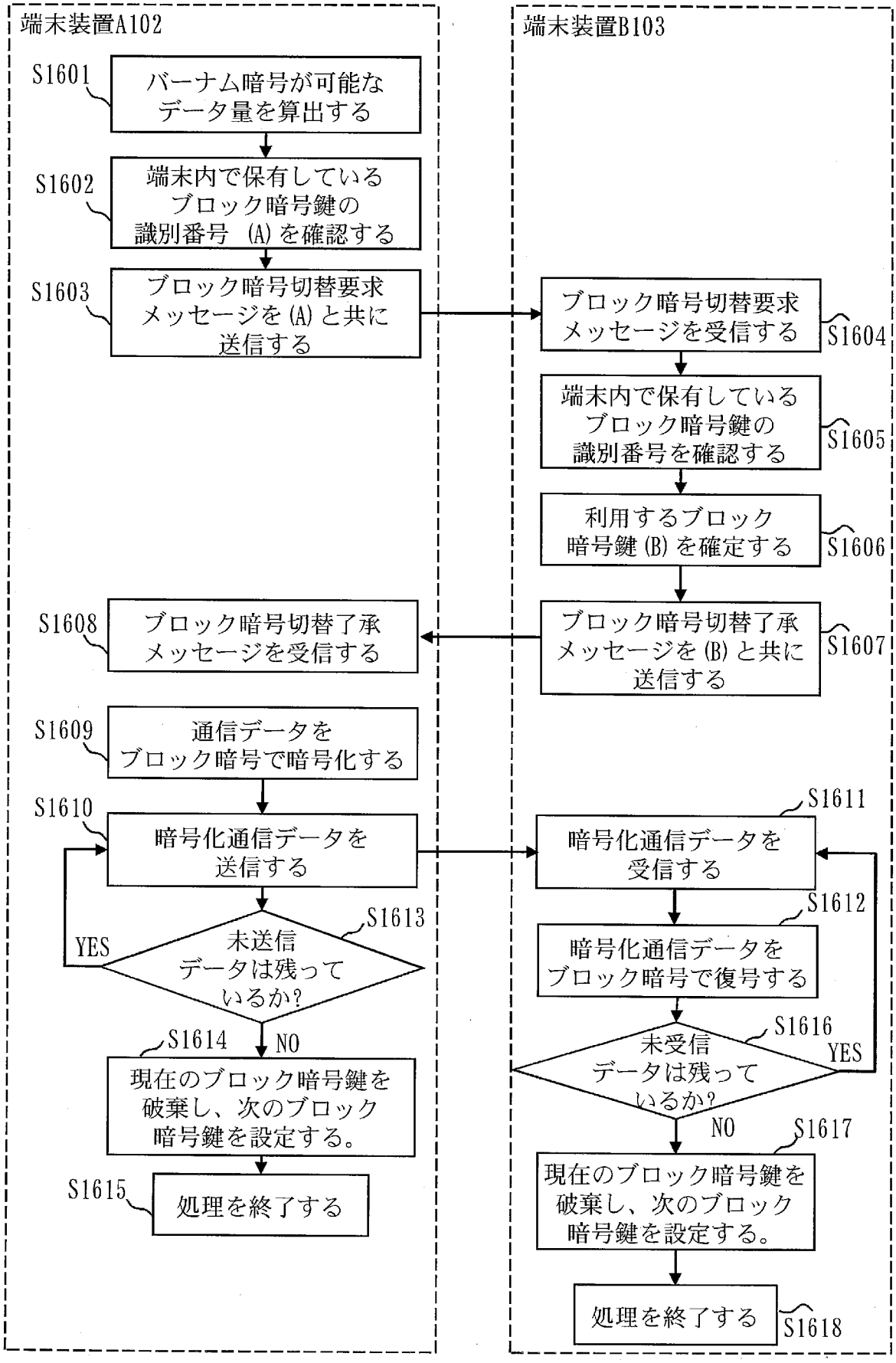
[図44]


端末装置A102
S1501
バーナム暗号が可能なデータ量を算出する
S1502
バーナム暗号通信要求メッセージを送信する
端末装置B103
バーナム暗号通信要求メッセージを受信する
S1503
バーナム暗号が可能なデータ量を算出する
S1504
バーナム暗号通信了承メッセージを送信する
S1505
S1506
バーナム暗号通信了承メッセージを受信する
S1507
通信データをバーナム暗号で暗号化する
暗号化通信データを送信する
暗号化通信データを受信する
S1509
暗号化通信データを復号する
S1510
S1508
S1511
未送信データは残っているか?
NO
YES
S1513
バーナム暗号が可能なデータ量が単位データ量以上?
YES
S1512
処理を終了する
NO
F

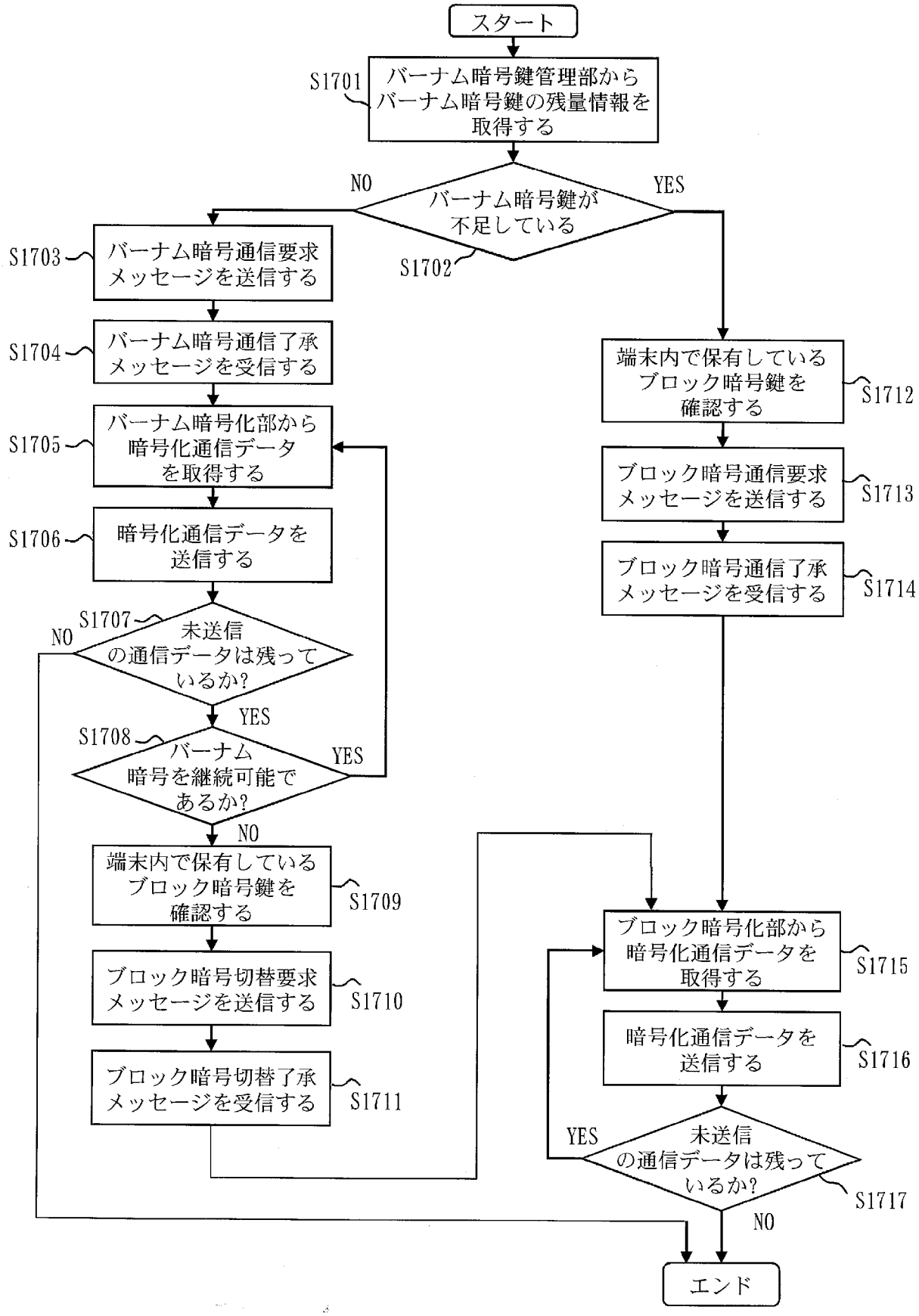
[図45]


F
端末装置A102
端末装置B103
端末内で保有している
ブロック暗号鍵の
識別番号 (A) を確認する
S1514
ブロック暗号切替要求
メッセージを (A) と共に
送信する
S1515
ブロック暗号切替要求
メッセージを受信する
S1516
端末内で保有している
ブロック暗号鍵の
識別番号を確認する
S1517
利用するブロック
暗号鍵 (B) を確定する
S1518
ブロック暗号切替了承
メッセージを (B) と共に
送信する
S1519
ブロック暗号切替了承
メッセージを受信する
S1520
通信データを
ブロック暗号で
暗号化する
S1521
暗号化通信データを
送信する
暗号化通信データを
受信する
S1523
S1522
未送信
データは残って
いるか?
S1525
YES
NO
暗号化通信データを
ブロック暗号で復号する
S1524
未受信
データは残って
いるか?
S1528
YES
NO
現在のブロック暗号鍵を
破棄し、次のブロック
暗号鍵を設定する。
S1526
現在のブロック暗号鍵を
破棄し、次のブロック
暗号鍵を設定する。
S1529
処理を終了する
S1527
処理を終了する
S1530

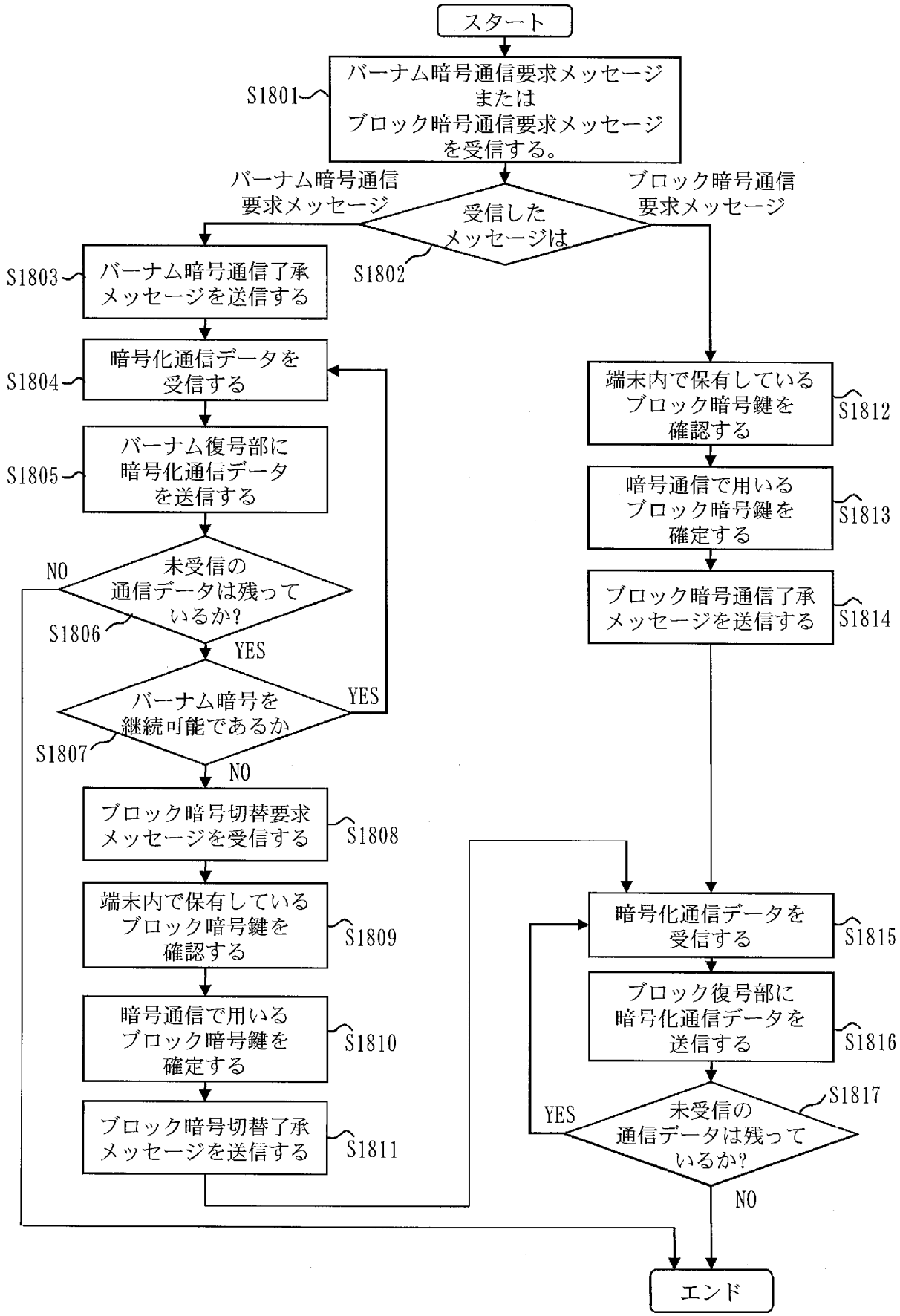
[図46]


端末装置A102
S1601
バーナム暗号が可能なデータ量を算出する
S1602
端末内で保有しているブロック暗号鍵の識別番号 (A) を確認する
S1603
ブロック暗号切替要求メッセージを (A) と共に送信する
S1608
ブロック暗号切替了承メッセージを受信する
S1609
通信データをブロック暗号で暗号化する
S1610
暗号化通信データを送信する
S1613
未送信データは残っているか?
YES
NO
S1614
現在のブロック暗号鍵を破棄し、次のブロック暗号鍵を設定する。
S1615
処理を終了する
端末装置B103
ブロック暗号切替要求メッセージを受信する
S1604
端末内で保有しているブロック暗号鍵の識別番号を確認する
S1605
利用するブロック暗号鍵 (B) を確定する
S1606
ブロック暗号切替了承メッセージを (B) と共に送信する
S1607
S1611
暗号化通信データを受信する
S1612
暗号化通信データをブロック暗号で復号する
S1616
未受信データは残っているか?
YES
NO
S1617
現在のブロック暗号鍵を破棄し、次のブロック暗号鍵を設定する。
処理を終了する
S1618

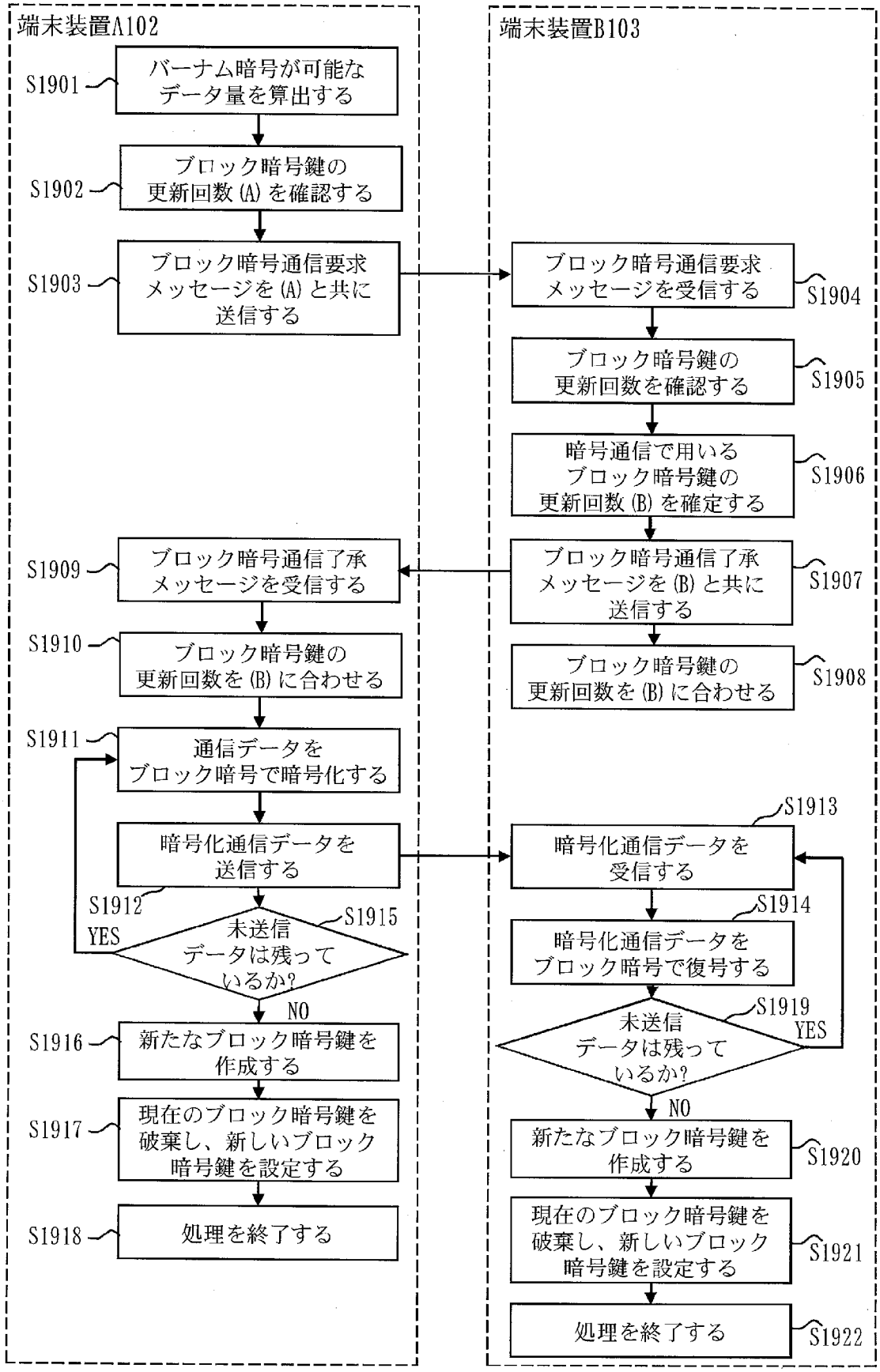
[図47]


スタート
S1701
バーナム暗号鍵管理部から
バーナム暗号鍵の残量情報を
取得する
S1702
バーナム暗号鍵が
不足している
NO
YES
S1703
バーナム暗号通信要求
メッセージを送信する
S1704
バーナム暗号通信了承
メッセージを受信する
S1705
バーナム暗号化部から
暗号化通信データ
を取得する
S1706
暗号化通信データを
送信する
S1707
未送信
の通信データは残って
いるか?
NO
YES
S1708
バーナム
暗号を継続可能で
あるか?
YES
NO
端末内で保有している
ブロック暗号鍵を
確認する
S1709
ブロック暗号切替要求
メッセージを送信する
S1710
ブロック暗号切替了承
メッセージを受信する
S1711
端末内で保有している
ブロック暗号鍵を
確認する
S1712
ブロック暗号通信要求
メッセージを送信する
S1713
ブロック暗号通信了承
メッセージを受信する
S1714
ブロック暗号化部から
暗号化通信データを
取得する
S1715
暗号化通信データを
送信する
S1716
未送信
の通信データは残って
いるか?
S1717
YES
NO
エンド

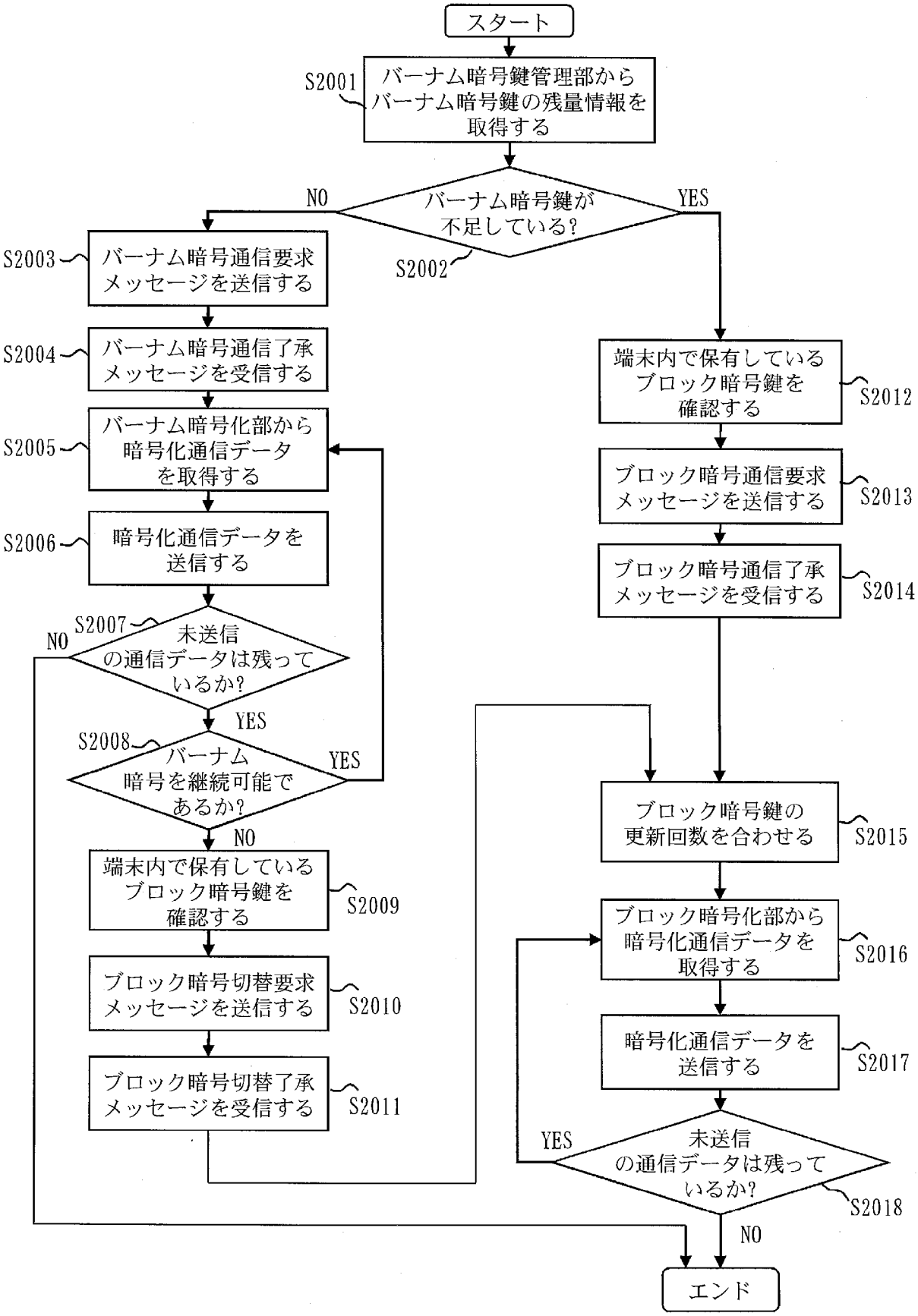
[図48]


スタート
バーナム暗号通信要求メッセージ
または
ブロック暗号通信要求メッセージ
を受信する。
S1801
受信した
メッセージは
S1802
バーナム暗号通信
要求メッセージ
ブロック暗号通信
要求メッセージ
バーナム暗号通信了承
メッセージを送信する
S1803
暗号化通信データを
受信する
S1804
バーナム復号部に
暗号化通信データ
を送信する
S1805
未受信の
通信データは残って
いるか?
S1806
NO
YES
バーナム暗号を
継続可能であるか
S1807
YES
NO
ブロック暗号切替要求
メッセージを受信する
S1808
端末内で保有している
ブロック暗号鍵を
確認する
S1809
暗号通信で用いる
ブロック暗号鍵を
確定する
S1810
ブロック暗号切替了承
メッセージを送信する
S1811
端末内で保有している
ブロック暗号鍵を
確認する
S1812
暗号通信で用いる
ブロック暗号鍵を
確定する
S1813
ブロック暗号通信了承
メッセージを送信する
S1814
暗号化通信データを
受信する
S1815
ブロック復号部に
暗号化通信データを
送信する
S1816
未受信の
通信データは残って
いるか?
S1817
YES
NO
エンド

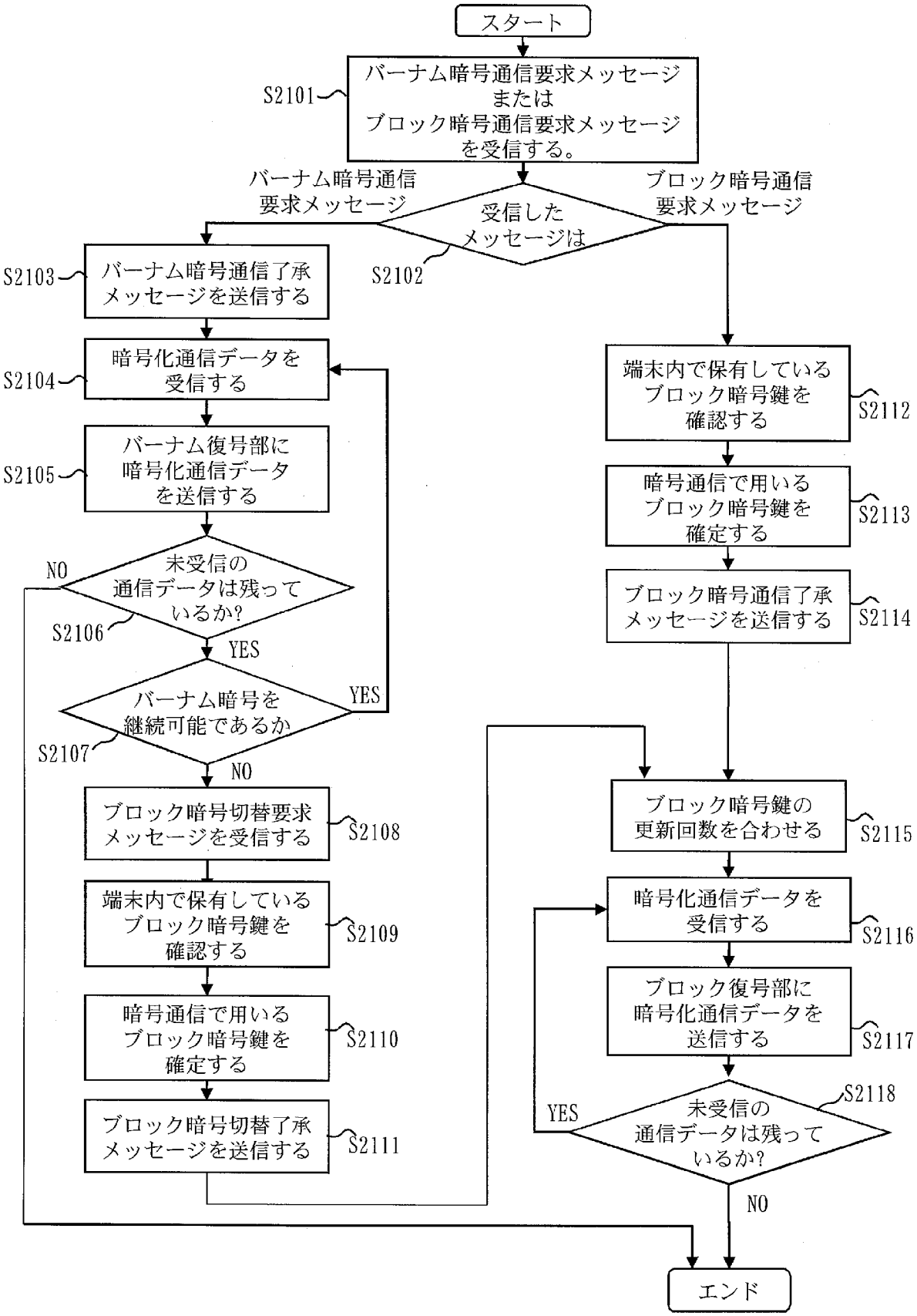
[図49]


端末装置A102
S1901
バーナム暗号が可能なデータ量を算出する
S1902
ブロック暗号鍵の更新回数(A)を確認する
S1903
ブロック暗号通信要求メッセージを(A)と共に送信する
S1909
ブロック暗号通信了承メッセージを受信する
S1910
ブロック暗号鍵の更新回数を(B)に合わせる
S1911
通信データをブロック暗号で暗号化する
暗号化通信データを送信する
S1912
YES
S1915
未送信データは残っているか?
NO
S1916
新たなブロック暗号鍵を作成する
S1917
現在のブロック暗号鍵を破棄し、新しいブロック暗号鍵を設定する
S1918
処理を終了する
端末装置B103
ブロック暗号通信要求メッセージを受信する
S1904
ブロック暗号鍵の更新回数を確認する
S1905
暗号通信で用いるブロック暗号鍵の更新回数(B)を確定する
S1906
ブロック暗号通信了承メッセージを(B)と共に送信する
S1907
ブロック暗号鍵の更新回数を(B)に合わせる
S1908
S1913
暗号化通信データを受信する
S1914
暗号化通信データをブロック暗号で復号する
S1919
YES
未送信データは残っているか?
NO
新たなブロック暗号鍵を作成する
S1920
現在のブロック暗号鍵を破棄し、新しいブロック暗号鍵を設定する
S1921
処理を終了する
S1922

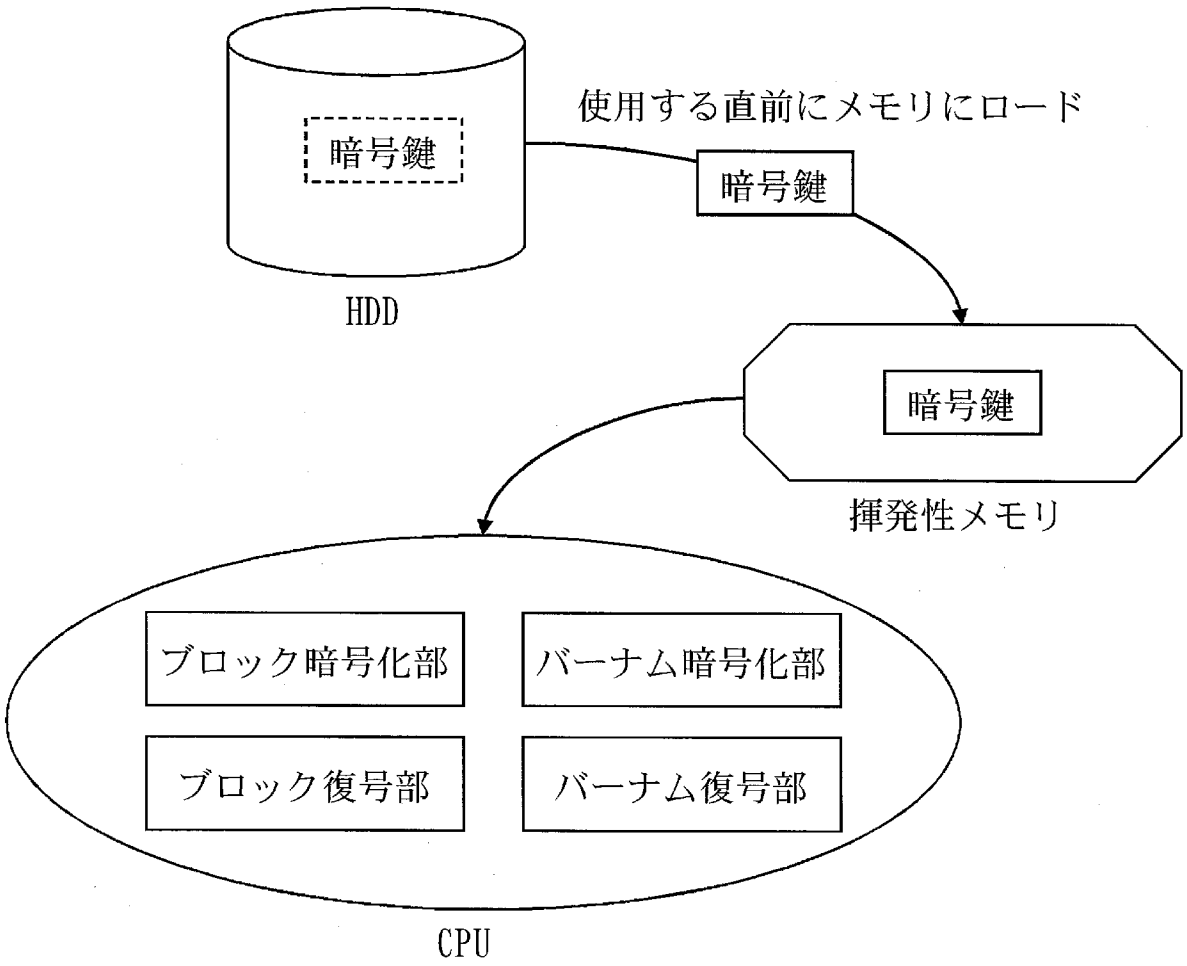
[図50]


スタート
S2001
バーナム暗号鍵管理部から
バーナム暗号鍵の残量情報を
取得する
バーナム暗号鍵が
不足している?
S2002
NO
YES
S2003
バーナム暗号通信要求
メッセージを送信する
S2004
バーナム暗号通信了承
メッセージを受信する
S2005
バーナム暗号化部から
暗号化通信データ
を取得する
S2006
暗号化通信データを
送信する
S2007
未送信
の通信データは残って
いるか?
NO
YES
S2008
バーナム
暗号を継続可能で
あるか?
YES
NO
S2009
端末内で保有している
ブロック暗号鍵を
確認する
S2010
ブロック暗号切替要求
メッセージを送信する
S2011
ブロック暗号切替了承
メッセージを受信する
端末内で保有している
ブロック暗号鍵を
確認する
S2012
ブロック暗号通信要求
メッセージを送信する
S2013
ブロック暗号通信了承
メッセージを受信する
S2014
ブロック暗号鍵の
更新回数を合わせる
S2015
ブロック暗号化部から
暗号化通信データを
取得する
S2016
暗号化通信データを
送信する
S2017
YES
未送信
の通信データは残って
いるか?
S2018
NO
エンド

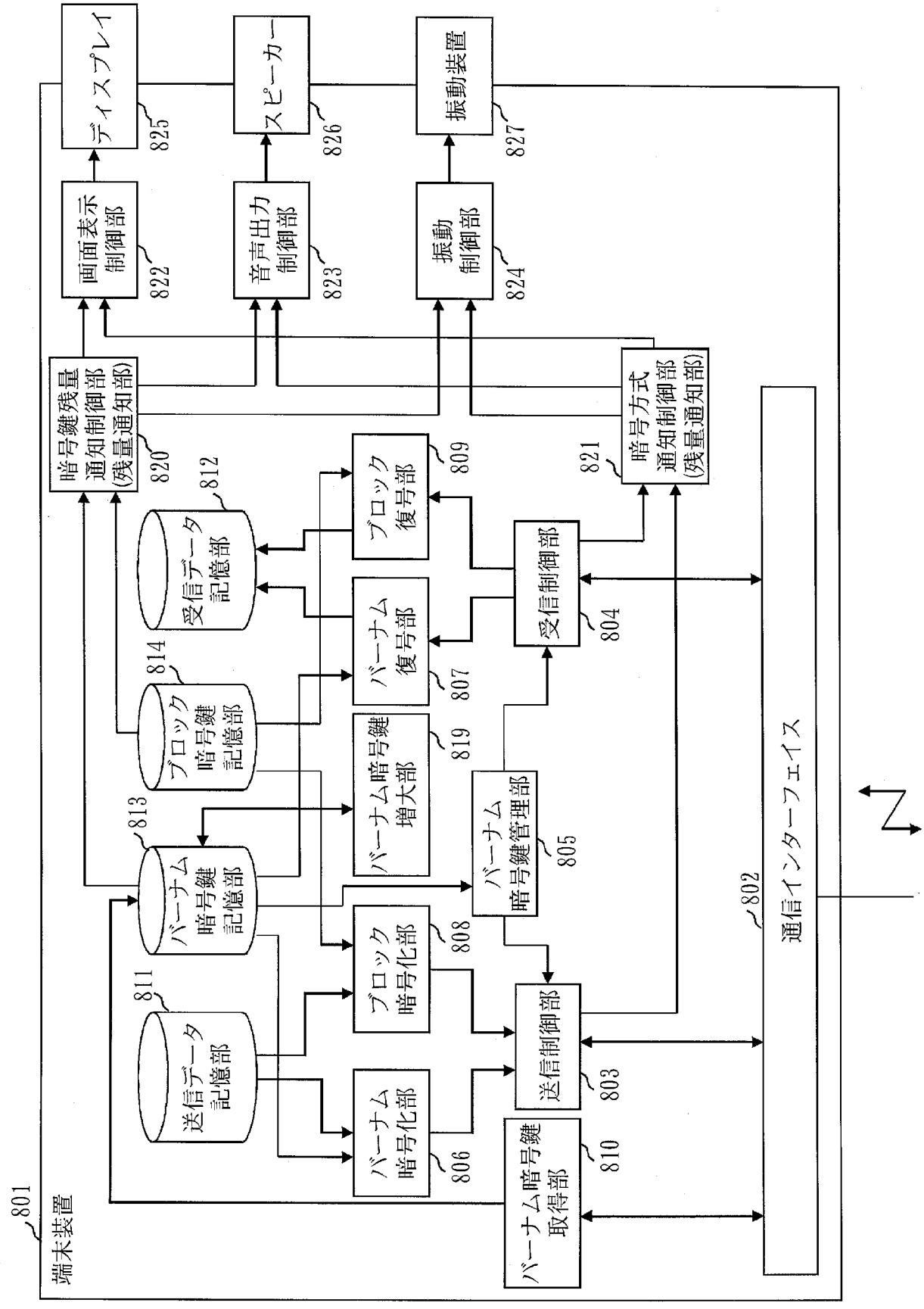
[図51]


スタート
S2101
バーナム暗号通信要求メッセージ
または
ブロック暗号通信要求メッセージ
を受信する。
バーナム暗号通信
要求メッセージ
受信した
メッセージは
S2102
ブロック暗号通信
要求メッセージ
S2103
バーナム暗号通信了承
メッセージを送信する
S2104
暗号化通信データを
受信する
S2105
バーナム復号部に
暗号化通信データ
を送信する
NO
未受信の
通信データは残って
いるか?
S2106
YES
YES
バーナム暗号を
継続可能であるか
S2107
NO
S2108
ブロック暗号切替要求
メッセージを受信する
S2109
端末内で保有している
ブロック暗号鍵を
確認する
S2110
暗号通信で用いる
ブロック暗号鍵を
確定する
S2111
ブロック暗号切替了承
メッセージを送信する
S2112
端末内で保有している
ブロック暗号鍵を
確認する
S2113
暗号通信で用いる
ブロック暗号鍵を
確定する
S2114
ブロック暗号通信了承
メッセージを送信する
S2115
ブロック暗号鍵の
更新回数を合わせる
S2116
暗号化通信データを
受信する
S2117
ブロック復号部に
暗号化通信データを
送信する
S2118
YES
未受信の
通信データは残って
いるか?
NO
エンド

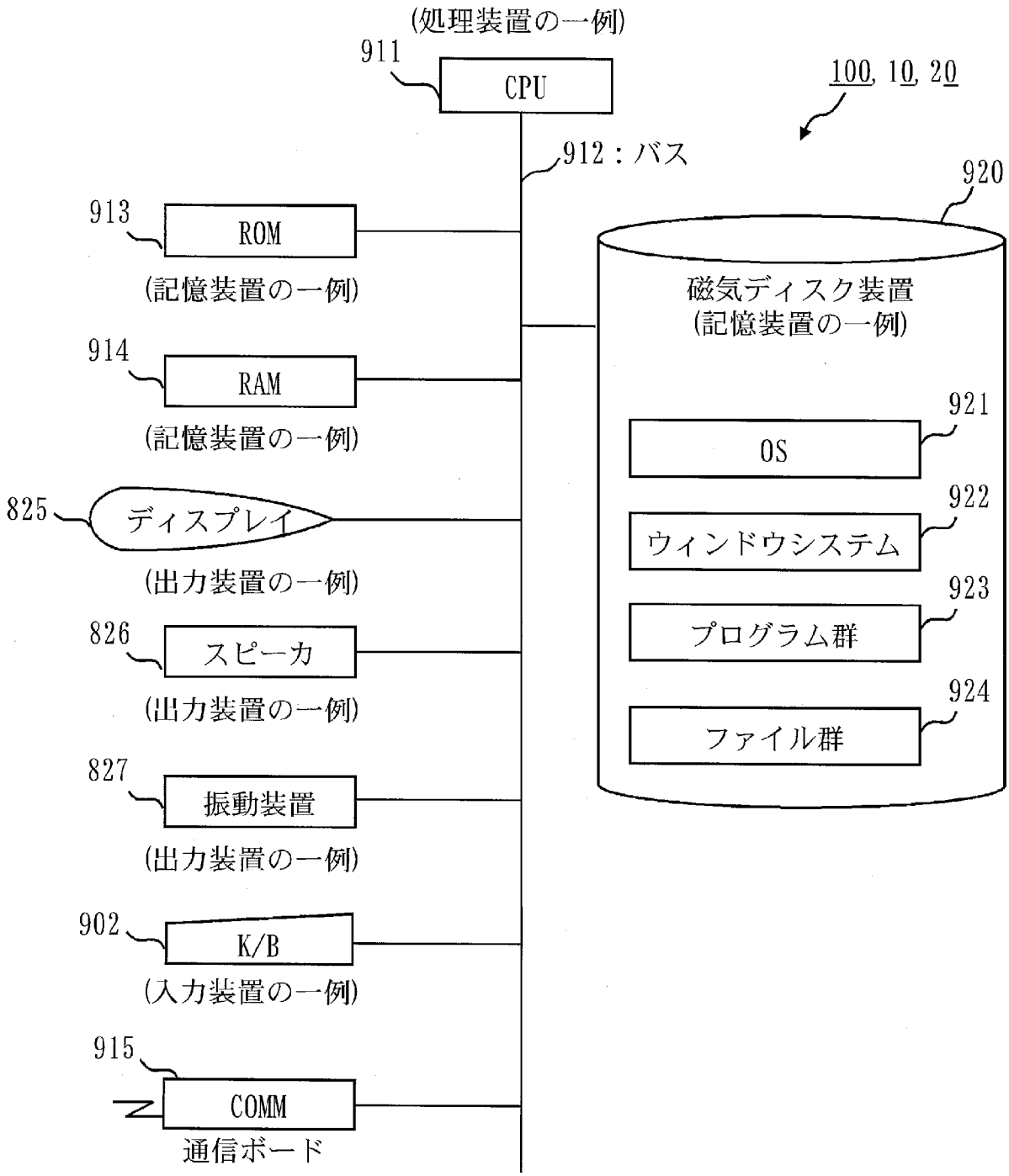
[図52]


暗号鍵
HDD
使用する直前にメモリにロード
暗号鍵
暗号鍵
揮発性メモリ
ブロック暗号化部
バーナム暗号化部
ブロック復号部
バーナム復号部
CPU

[図53]


801
端末装置
ディスプレイ
825
スピーカー
826
振動装置
827
画面表示制御部
822
音声出力制御部
823
振動制御部
824
暗号鍵残量通知制御部(残量通知部)
820
暗号方式通知制御部(残量通知部)
821
受信データ記憶部
812
ブロック復号部
809
ブロック暗号鍵記憶部
814
バーナム復号部
807
受信制御部
804
バーナム暗号鍵増大部
819
バーナム暗号鍵記憶部
813
バーナム暗号鍵管理部
805
送信データ記憶部
811
ブロック暗号化部
808
送信制御部
803
802
通信インターフェイス
バーナム暗号化部
806
バーナム暗号鍵取得部
810

[図54]


(処理装置の一例)
911
CPU
100, 10, 20
912：バス
920
913
ROM
(記憶装置の一例)
磁気ディスク装置
(記憶装置の一例)
914
RAM
(記憶装置の一例)
921
OS
825
ディスプレイ
(出力装置の一例)
922
ウィンドウシステム
923
プログラム群
826
スピーカ
(出力装置の一例)
924
ファイル群
827
振動装置
(出力装置の一例)
902
K/B
(入力装置の一例)
915
COMM
通信ボード

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2010/064238

A. CLASSIFICATION OF SUBJECT MATTER
H04L9/14(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)
H04L9/14

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.
A	JP 2000-278260 A (Hitachi Information Systems, Inc.), 06 October 2000 (06.10.2000), paragraph [0008] (Family: none)	1-18
A	JP 7-250057 A (Mita Kogyo Kabushiki Kaisha), 26 September 1995 (26.09.1995), paragraphs [0013], [0014] & US 5652662 A	1-18
A	JP 11-17673 A (Canon Inc.), 22 January 1999 (22.01.1999), paragraph [0023] & US 6307940 B1	12

☐ 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
22 September, 2010 (22.09.10)	05 October, 2010 (05.10.10)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１０／０６４２３８

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04L9/14(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.　H04L9/14

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
A	JP 2000-278260 A (株式会社日立情報システムズ) 2000.10.06, 段落【0008】 (ファミリーなし)	1-18
A	JP 7-250057 A (三田工業株式会社) 1995.09.26, 段落【0013】,【0014】 & US 5652662 A	1-18
A	JP 11-17673 A (キャノン株式会社) 1999.01.22, 段落【0023】 & US 6307940 B1	12

☐　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 ２２．０９．２０１０	国際調査報告の発送日 ０５．１０．２０１０
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　４１８０ 西田　聡子 電話番号　０３－３５８１－１１０１　内線　３５４６