(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
2005 年12 月29 日 (29.12.2005)

PCT

(10) 国際公開番号
WO 2005/125082 A1

(51) 国際特許分類[7]: H04L 9/08

(21) 国際出願番号: PCT/JP2005/010262

(22) 国際出願日: 2005 年6 月3 日 (03.06.2005)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2004-184165 2004 年6 月22 日 (22.06.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒5718501 大阪府門真市大字門真１００６番地 Osaka (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 金子 友晴 (KANEKO, Tomoharu). 稲垣 達也 (INAGAKI, Tatsuya).

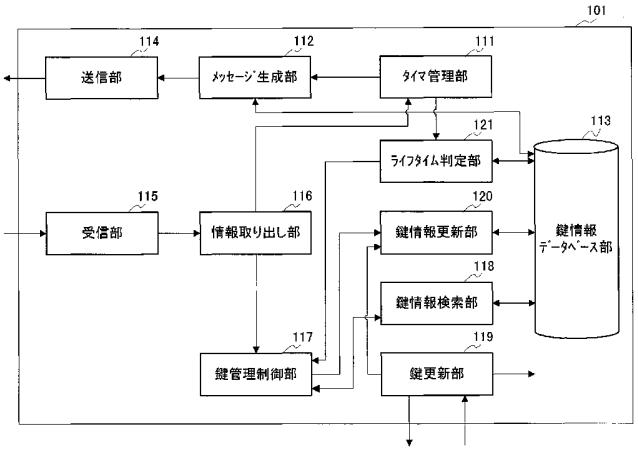
(74) 代理人: 鷲田 公一 (WASHIDA, Kimihito); 〒2060034 東京都多摩市鶴牧１丁目２４－１新都市センタービル５階 Tokyo (JP).

(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, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[続葉有]

(54) Title: COMMUNICATION SYSTEM AND COMMUNICATION APPARATUS

(54) 発明の名称: 通信システムおよび通信装置



114...TRANSMITTING PART
112...MESSAGE GENERATING PART
111...TIMER MANAGING PART
121...LIFE TIME DETERMINING PART
115...RECEIVING PART
116...INFORMATION EXTRACTING PART
117...KEY MANAGEMENT CONTROL PART
120...KEY INFORMATION UPDATING PART
118...KEY INFORMATION RETRIEVING PART
119...KEY UPDATING PART
113...KEY INFORMATION DATABASE PART

(57) Abstract: A communication system and communication apparatus that can improve the stability and security of communication. In this communication system, a communication apparatus (101) generates, at predetermined intervals, a keep-alive message based on key information stored in a key information database part (113) and transmits the keep-alive message to a communication apparatus (102). The communication apparatus (102) receives the keep-alive message from the communication apparatus (101), and a key information updating part (157) updates (for example, corrects), based on this keep-alive message, the data stored in a key information database part (154). In this way, the information stored in the communication apparatus (101) and the information stored in the communication apparatus (102) can be made common, and problems, such as a communication interruption, caused by disagreement between the information stored in the communication apparatus (101) and the information stored in the communication apparatus (102) can be solved, resulting in improvement of the stability and security of communication between the two communication apparatuses.

[続葉有]

WO 2005/125082 A1

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書
— 補正書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: 通信の安定性および安全性を向上することができる通信システムおよび通信装置。この通信システムでは、通信装置（１０１）が、所定間隔ごとに鍵情報データベース部（１１３）に記憶されている鍵情報を基にしてキープアライブメッセージを生成し、通信装置（１０２）に対して送信する。通信装置（１０２）は、通信装置（１０１）からキープアライブメッセージを受信して、このキープアライブメッセージを基に鍵情報更新部（１５７）が鍵情報データベース部（１５４）に記憶されているデータの更新（補正など）を行う。これにより通信装置（１０１）にて記憶されている情報と通信装置（１０２）にて記憶されている情報とを共通化でき、通信装置（１０１）および通信装置（１０２）が記憶している情報の不一致から生じる通信断絶などの不都合を解消することができるため、両装置間で行われる通信の安定性および安全性を向上することができる。

明 細 書

通信システムおよび通信装置

技術分野

[0001] 本発明は、通信システムおよび通信装置に関し、特に通信の安定性および安全性を向上する通信システムおよび通信装置に関する。

背景技術

[0002] インターネットにおけるセキュリティ技術として、IPSec(IP Security)が知られている。IPSecでは、安全な鍵交換を実現するためにIKE(Internet Key Exchange)プロトコルを実装する必要がある。しかし、IKEは、通信を行う各通信装置に個別に設定情報を保持させる必要があるなど運用が煩雑になる。そこで、特定の装置に鍵を配布させることによって運用しやすくするなど簡易的な鍵交換を行う従来方式が提案されている(特許文献1参照)。

[0003] この従来の鍵交換方式が適用される通信システムにおいては、通信のセキュリティを確保するため、鍵には有効期限が定義される。そして、その有効期限が近づくと、通信中の通信装置は、鍵を配布する装置に新しい鍵の配布を要求することにより取得して、鍵の更新を行う。

特許文献1:特開2001－292135号公報

発明の開示

発明が解決しようとする課題

[0004] しかしながら、各通信装置に搭載されている時計がまったく同じ時刻を刻むことは少なく、わずかながら誤差を生じるのが普通である。したがって、鍵の有効期限がある程度長く定義されると、通信中の二つの通信装置の間で、各々管理している時刻のずれが大きくなり有効期限についてもずれが生じてしまう。そうすると、一方の通信装置でだけ鍵が無効になるという事態が生じ、上記二つの通信装置間で通信を継続できなくなることがある問題がある。

[0005] また、鍵を更新する場合に、通信を行っている通信装置間で、一方の通信装置だけが鍵の更新を完了しているタイミングでは、もう一方の通信装置は、新しい鍵を持

っていないため、この新しい鍵を用いて送信されたデータを受信することができず、通信を継続できない問題がある。

[0006] 本発明の目的は、一方の通信装置でだけ鍵が無効になるという事態を防ぐことができ、通信の安定性および安全性を向上する通信システムおよび通信装置を提供することである。

課題を解決するための手段

[0007] 本発明の通信システムは、第1の通信装置と第2の通信装置との間で鍵を用いて通信を行う通信システムであって、前記第1の通信装置は、前記鍵の有効期限を含む鍵情報を記憶する記憶手段と、前記鍵情報を所定間隔ごとに送信する送信手段と、を具備し、前記第2の通信装置は、前記鍵の有効期限を含む他の鍵情報を記憶する他の記憶手段と、前記第1の通信装置からの前記鍵情報を受信する受信手段と、前記他の記憶手段に記憶している前記他の鍵情報を前記受信手段で受信した前記鍵情報で補正する補正手段と、を具備する構成を採る。

発明の効果

[0008] 本発明によれば、通信装置にて記憶されている情報と他の通信装置にて記憶されている情報との共通化を図り、通信装置および他の通信装置が記憶している情報の不一致から生じる通信断絶などを解消することにより、通信の安定性および安全性を向上する通信システムおよび通信装置を提供することができる。

図面の簡単な説明

[0009] [図1]本実施の形態に係る通信システムの全体構成図

[図2]メッセージの構成の一例を示す図

[図3]図1の通信装置の構成を示すブロック図

[図4]鍵情報データベース部の構成の一例を示す図

[図5]図1の他の通信装置の構成を示すブロック図

発明を実施するための最良の形態

[0010] 以下、本発明の一実施の形態について図面を参照して詳細に説明する。

[0011] まず、本実施の形態に係る通信システム100の構成について、図1を参照して説明

する。

[0012] 図1に示すように、通信システム100は、通信装置101と、通信装置102と、インターネットシステム103と、鍵配布サーバ装置104とを備える。

[0013] この通信システム100には、IPSec(IP Security)が適用されている。また、通信システム100では、通信装置101と通信装置102との間で行われる通信における暗号や認証などに用いられる有効期限付きの鍵が、通信装置101および通信装置102の各々により鍵配布サーバ装置104から取得される。これにより、通信装置101および通信装置102は、両者間の通信で利用する鍵を共有する。

[0014] 通信装置101および通信装置102は、各々において鍵の有効期限を管理している。具体的には、通信装置101は、所定間隔ごとに鍵の有効期限が切れているか否かを判定する。判定の結果、有効期限が切れていると判定した場合には、通信装置101は、その有効期限が切れていると判定した鍵の代わりの新しい鍵を鍵配布サーバ装置104から取得する。なお、通信装置102においても同様の動作が行われる。

[0015] 次いで、通信装置101と通信装置102との間で行われる鍵の有効期限にかかる同期処理について説明する。なお、ここでは、通信装置101が手順を開始する側のイニシエータとして動作し、また、通信装置102がイニシエータに応答するレスポンダとして動作するものとして説明する。

[0016] 通信装置101は、所定間隔ごとにキープアライブメッセージを生成し、このキープアライブメッセージを通信装置102に対しインターネットシステム103を介して送信する。なお、このキープアライブメッセージは、鍵識別情報、その鍵の有効期限、および使用状態などの情報を含むものである。

[0017] 通信装置102は、通信装置101からのキープアライブメッセージを受信して、このキープアライブメッセージに含まれる鍵識別情報と対応する鍵情報を自装置が保持しているか否かを検索する。検索の結果、キープアライブメッセージに含まれる鍵識別情報と対応する鍵情報を自装置が保持していない場合には、通信装置102は、その鍵情報の鍵を鍵配布サーバ装置104から取得する手順を実行する。

[0018] 一方、検索の結果、キープアライブメッセージに含まれる鍵識別情報と対応する鍵情報を自装置が保持している場合には、通信装置102は、そのキープアライブメッセ

ージに含まれる情報により、自装置が保持している鍵情報に関する各種情報の更新を行う。これにより、例えば、通信装置101の鍵の有効期限と通信装置102の鍵の有効期限の同期が図られる。

[0019] 次に、通信装置102は、キープアライブリプライメッセージを生成し、このキープアライブリプライメッセージを通信装置101に対しインターネットシステム103を介して送信する。なお、このキープアライブリプライメッセージは、鍵識別情報、その鍵の有効期限、および使用状態などの情報を含むものである。

[0020] 通信装置101は、通信装置102からのキープアライブリプライメッセージを受信して、このキープアライブリプライメッセージに含まれる鍵識別情報と対応する鍵情報を自装置が保持しているか否かを検索する。検索の結果、キープアライブリプライメッセージに含まれる鍵識別情報と対応する鍵情報を自装置が保持していない場合には、通信装置101は、その鍵情報の鍵を鍵配布サーバ装置104から取得する手順を実行する。

[0021] 一方、検索の結果、キープアライブリプライメッセージに含まれる鍵識別情報と対応する鍵情報を自装置が保持している場合には、通信装置101は、特別の動作を行わない。

[0022] 図2は、上記キープアライブメッセージおよびキープアライブリプライメッセージの構成の一例を示した図である。図2に示すように、上記メッセージは、メッセージタイプ(キープアライブメッセージ又はキープアライブリプライメッセージであることを示す)、メッセージ長、鍵識別情報、有効期限、およびステータス(使用状態)を含んでいる。なお、括弧内の数字は、それぞれの情報のビット数を示している。

[0023] 図3は、通信装置101の構成を示すブロック図である。

[0024] 図3に示すように、通信装置101は、タイマ管理部111と、メッセージ生成部112と、鍵情報データベース部113と、送信部114と、受信部115と、情報取り出し部116と、鍵管理制御部117と、鍵情報検索部118と、鍵更新部119と、鍵情報更新部120と、ライフタイム判定部121とを備える。

[0025] 通信装置101においては、タイマ管理部111は、鍵情報の有効期限を管理するために、定期的に満了する鍵管理タイマを設定している。この鍵管理タイマが満了する

ごとに、タイマ管理部111は、鍵管理タイマが満了した旨を示すタイマ満了情報をメッセージ生成部112に出力する。

[0026] メッセージ生成部112は、鍵情報データベース部113に記憶されている鍵情報に関する各種情報を基にして、キープアライブメッセージを生成し、このキープアライブメッセージを送信部114に出力する。なお、鍵情報データベース部113は、図4に示すように、鍵識別情報、通信先の機器の識別情報、有効期限(期限が切れるまでの残り時間)、および鍵の使用状態を対応づけて記憶している。

[0027] 送信部114は、メッセージ生成部112からのキープアライブメッセージを通信装置102に送信する。

[0028] また、通信装置101においては、受信部115は、通信装置102からキープアライブリプライメッセージを受け取り、情報取り出し部116に出力する。

[0029] 情報取り出し部116は、受信部115からのキープアライブリプライメッセージを受け取り、そのキープアライブリプライメッセージに含まれる各種情報を取り出して鍵管理制御部117に出力する。

[0030] 鍵管理制御部117は、情報取り出し部116から受け取る鍵識別情報と、この鍵識別情報が鍵情報データベース部113に記憶されているか否か検索することを命じる検索命令信号とを鍵情報検索部118に出力する。

[0031] 鍵情報検索部118は、鍵管理制御部117からの鍵識別情報および検索命令信号を受け取り、この鍵識別情報をキーとして鍵情報データベース部113を検索する。そして、鍵情報検索部118は、検索が終了すると検索結果情報を鍵管理制御部117に出力する。

[0032] 鍵管理制御部117は、鍵情報検索部118からの検索結果情報を受け取り、この検索結果情報が鍵情報データベース部113に鍵識別情報がないことを示しているときには、鍵更新部119に対して鍵識別情報と、その鍵識別情報により特定される鍵を鍵配布サーバ装置104から取得することを命じる取得命令信号とを出力する。

[0033] 鍵更新部119は、鍵管理制御部117からの鍵識別情報および取得命令信号を受け取り、鍵配布サーバ装置104からその鍵識別情報で特定される鍵を取得する。そして、鍵更新部119は、取得した鍵を鍵記憶部(図示せず)に出力するとともに、その

鍵に関する各種情報を鍵情報更新部120に出力する。

[0034] 鍵情報更新部120は、鍵更新部119からの各種情報を鍵情報データベース部113に記憶する処理を行う。

[0035] 一方、鍵情報検索部118からの検索結果情報が鍵情報データベース部113に鍵識別情報があることを示しているときには、鍵管理制御部117は、特別の動作を行わない。

[0036] また、通信装置101においては、タイマ管理部111は、鍵の有効期限を確認する所定の間隔ごとに有効期限を確認することを命じる有効期限確認命令信号をライフタイム判定部121に出力する。

[0037] ライフタイム判定部121は、鍵情報データベース部113に記憶されている鍵情報の有効期限が切れているか否かを鍵識別情報ごとに判定する。そして、ライフタイム判定部121は、有効期限が切れていると判定した鍵の鍵識別情報を取得し、鍵管理制御部117に出力する。

[0038] 鍵管理制御部117は、ライフタイム判定部121から鍵識別情報を受け取ると、鍵更新部119に対して鍵識別情報と、その鍵識別情報により特定される鍵を鍵配布サーバ装置104から取得することを命じる取得命令信号とを出力する。

[0039] 鍵更新部119は、鍵管理制御部117からの鍵識別情報および取得命令信号を受け取り、鍵配布サーバ装置104からその鍵識別情報で特定される鍵を取得する。そして、鍵更新部119は、取得した鍵を鍵記憶部(図示せず)に出力するとともに、その鍵に関する各種情報を鍵情報更新部120に出力する。

[0040] 図5は、通信装置102の構成を示すブロック図である。

[0041] 図5に示すように、通信装置102は、受信部151と、情報取り出し部152と、鍵管理制御部153と、鍵情報データベース部154と、鍵情報検索部155と、鍵更新部156と、鍵情報更新部157と、タイマ管理部158と、ライフタイム判定部159と、メッセージ生成部160と、送信部161とを備える。

[0042] 通信装置102においては、受信部151は、通信装置101からキープアライブメッセージを受け取り、情報取り出し部152に出力する。

[0043] 情報取り出し部152は、受信部151からのキープアライブメッセージを受け取り、そ

のキープアライブメッセージに含まれる各種情報を取り出して鍵管理制御部153に出力する。

[0044] 鍵管理制御部153は、情報取り出し部152から受け取る鍵識別情報と、この鍵識別情報が鍵情報データベース部154に記憶されているか否か検索することを命じる検索命令信号とを鍵情報検索部155に出力する。

[0045] 鍵情報検索部155は、鍵管理制御部153からの鍵識別情報および検索命令信号を受け取り、この鍵識別情報をキーとして鍵情報データベース部154を検索する。そして、鍵情報検索部155は、検索が終了すると検索結果情報を鍵管理制御部153に出力する。

[0046] 鍵管理制御部153は、鍵情報検索部155からの検索結果情報を受け取り、この検索結果情報が鍵情報データベース部154に鍵識別情報がないことを示しているときには、鍵更新部156に対して鍵識別情報と、その鍵識別情報により特定される鍵を鍵配布サーバ装置104から取得することを命じる取得命令信号とを出力する。

[0047] 鍵更新部156は、鍵管理制御部153からの鍵識別情報および取得命令信号を受け取り、鍵配布サーバ装置104からその鍵識別情報で特定される鍵を取得する。そして、鍵更新部156は、取得した鍵を鍵記憶部(図示せず)に出力するとともに、その鍵に関する各種情報を鍵情報更新部157に出力する。

[0048] 鍵情報更新部157は、鍵更新部156からの各種情報を鍵情報データベース部154に記憶する処理を行う。

[0049] 一方、鍵情報検索部155からの検索結果情報が鍵情報データベース部154に鍵識別情報があることを示しているときには、鍵管理制御部153は、情報取り出し部152からの各種情報と鍵情報の更新を命じる更新命令信号を鍵情報更新部157に出力する。

[0050] 鍵情報更新部157は、鍵管理制御部153からの鍵識別情報に対応づけて記憶されている各種情報を、鍵管理制御部153からの各種情報で上書きして更新する処理を行う。

[0051] そして、鍵管理制御部153は、鍵情報更新部157が鍵情報データベース部154に記憶する処理又は上書きして更新する処理を完了すると、メッセージ生成部160に

対してメッセージの生成を命令する信号を出力する。

[0052] メッセージ生成部160は、鍵管理制御部153からの命令信号を受け取ると、鍵情報データベース部154に記憶されている鍵情報に関する各種情報を基にして、キープアライブリプライメッセージを生成し、このキープアライブリプライメッセージを送信部161に出力する。なお、鍵情報データベース部154は、図4に示すように、鍵識別情報、通信先の機器の識別情報、有効期限(期限が切れるまでの残り時間)、および鍵の状態を対応づけて記憶している。

[0053] また、通信装置102においては、タイマ管理部158は、鍵の有効期限を確認する所定の間隔ごとに有効期限を確認することを命じる有効期限確認命令信号をライフタイム判定部159に出力する。

[0054] ライフタイム判定部159は、鍵情報データベース部154に記憶されている鍵情報の有効期限が切れているか否かを鍵識別情報ごとに判定する。そして、ライフタイム判定部159は、有効期限が切れていると判定した鍵の鍵識別情報を取得し、鍵管理制御部153に出力する。

[0055] 鍵管理制御部153は、ライフタイム判定部159から鍵識別情報を受け取ると、鍵更新部156に対して鍵識別情報と、その鍵識別情報により特定される鍵を鍵配布サーバ装置104から取得することを命じる取得命令信号とを出力する。

[0056] 鍵更新部156は、鍵管理制御部153からの鍵識別情報および取得命令信号を受け取り、鍵配布サーバ装置104からその鍵識別情報で特定される鍵を取得する。そして、鍵更新部156は、取得した鍵を鍵記憶部(図示せず)に出力するとともに、その鍵に関する各種情報を鍵情報更新部157に出力する。

[0057] なお、上記キープアライブメッセージおよびキープアライブリプライメッセージには、タイマ管理部111およびタイマ管理部158において管理している現在時刻を含めることもできる。これにより、通信装置101および通信装置102との間でタイマ管理部にて管理する現在時刻のずれを調整することができる。

[0058] この場合には、通信装置101のメッセージ生成部112は、キープアライブメッセージを生成する際に、タイマ管理部111から現在時刻を取得し、この現在時刻情報を含めてキープアライブメッセージを生成して、送信部114に出力する。

[0059] 通信装置102の情報取り出し部152は、通信装置101からのキープアライブメッセージから現在時刻情報を取り出してタイマ管理部158に出力する。タイマ管理部158は、管理している現在時刻を情報取り出し部152からの現在時刻情報で調整する。

[0060] そして、メッセージ生成部160は、キープアライブリプライメッセージを生成する際に、タイマ管理部158から現在時刻取得し、この現在時刻情報を含めてキープアライブリプライメッセージを生成して、送信部161に出力する。

[0061] またなお、上記説明においては、メッセージ生成部112は、鍵情報データベース部113に記憶されている情報をそのまま利用してキープアライブメッセージを生成していたが、有効期限がしきい値より少ないときには、その有効期限をゼロとしてキープアライブメッセージを生成することとしてもよい。

[0062] これにより、通信装置102は、このキープアライブメッセージを受け取って、これに含まれる各種情報で鍵情報データベース部154の情報を上書きすることになり、つぎにライフタイム判定部159が有効期限を確認するときには、有効期限をゼロとされた鍵は、必ず鍵更新部156による鍵配布サーバ装置104からの取得(鍵の更新)の対象となる。また、通信装置101では、上記しきい値を適当に設定することで、通信装置102における鍵配布サーバ装置104からの鍵取得と略同時期に鍵の取得(鍵の更新)が行われる。そのため、通信装置101の鍵の有効期限と通信装置102の鍵の有効期限の同期が図られる。

[0063] なお、その有効期限をゼロとしてキープアライブメッセージを生成する代わりに、通信装置101のメッセージ生成部112が、通信装置102における鍵の更新を促す命令信号をキープアライブメッセージとともに生成し、送信部114に出力する構成としてもよい。これによっても、通信装置101の鍵の有効期限と通信装置102の鍵の有効期限の同期が図られる。

[0064] なお、通信システム100の構成要素である各装置間の通信は、無線により行われても、また、有線により行われてもよい。

[0065] このように、本実施の形態によれば、通信装置101は、所定間隔ごとに鍵情報データベース部113に記憶されている鍵情報を基にしてキープアライブメッセージを生成し、通信装置102に対して送信する。通信装置102は、通信装置101からキープアラ

イブメッセージを受信して、このキープアライブメッセージを基にして鍵情報更新部157が鍵情報データベース部154に記憶されているデータの更新（補正など）を行う。

[0066] こうすることで、通信装置にて記憶されている情報と他の通信装置にて記憶されている情報とを共通化することにより、通信装置および他の通信装置が記憶している情報の不一致から生じる通信断絶などの不都合を解消することができるため、両装置間で行われる通信の安定性および安全性を向上することができる。

[0067] 本明細書は、2004年6月22日出願の特願2004－184165に基づく。この内容はすべてここに含めておく。

産業上の利用可能性

[0068] 本発明は、通信の安定性および安全性を向上する通信システムおよび通信装置として有用である。

請求の範囲

[1] 第1の通信装置と第2の通信装置との間で鍵を用いて通信を行う通信システムであって、

前記第1の通信装置は、

前記鍵の有効期限を含む鍵情報を記憶する記憶手段と、

前記鍵情報を所定間隔ごとに送信する送信手段と、

を具備し、

前記第2の通信装置は、

前記鍵の有効期限を含む他の鍵情報を記憶する他の記憶手段と、

前記第1の通信装置からの前記鍵情報を受信する受信手段と、

前記他の記憶手段に記憶している前記他の鍵情報を前記受信手段で受信した前記鍵情報で補正する補正手段と、

を具備する通信システム。

[2] 前記第1の通信装置は、

自装置における現在時刻を管理する現在時刻管理部を具備し、

前記送信手段は前記現在時刻を所定間隔ごとに送信し、

前記第2の通信装置は、

自装置における他の現在時刻を管理する他の現在時刻管理部を具備し、

前記受信手段は前記第1の通信装置からの前記現在時刻を受信し、

前記補正手段は前記他の現在時刻管理部が管理する前記他の現在時刻を前記受信手段が受信した前記現在時刻で補正する請求項1に記載の通信システム。

[3] 前記第1の通信装置および前記第2の通信装置が通信に用いる前記鍵を管理する鍵管理装置をさらに備え、

前記第2の通信装置は、

前記第1の通信装置から送信される前記鍵情報で特定される前記鍵を前記他の記憶手段に記憶しているか否かを判定する判定手段と、

前記判定手段による判定結果が前記他の記憶手段に前記第1の通信装置から送信される前記鍵情報で特定される前記鍵を記憶していないことを示すときに、前記他

の記憶手段に記憶していない前記鍵を前記鍵管理装置から取得する鍵取得手段と、

を具備する請求項1に記載の通信システム。

[4] 前記第1の通信装置は、

前記有効期限がしきい値より少ない前記鍵の取得の制御情報を生成する制御情報生成手段を具備し、

前記送信手段は、前記制御情報を前記第2の通信装置に送信し、

前記第2の通信装置は、

前記鍵取得手段にて前記制御情報に基づき前記鍵管理装置から前記鍵を取得する請求項3に記載の通信システム。

[5] 他の通信装置と鍵を用いて通信を行う通信装置であって、

前記鍵の有効期限を含む鍵情報を記憶する記憶手段と、

前記他の通信装置からの前記鍵の有効期限を含む他の鍵情報を受信する受信手段と、

前記記憶手段に記憶している前記鍵情報を前記受信手段で受信した前記他の鍵情報で補正する補正手段と、

を具備する通信装置。

[6] 自装置における現在時刻を管理する現在時刻管理部をさらに具備し、

前記受信手段は前記他の通信装置からの前記現在時刻を受信し、

前記補正手段は前記現在時刻管理部が管理する前記現在時刻を前記受信手段が受信した前記現在時刻で補正する請求項5に記載の通信装置。

[7] 前記他の通信装置から送信される前記鍵情報で特定される前記鍵を前記記憶手段に記憶しているか否かを判定する判定手段と、

前記判定手段による判定結果が前記記憶手段に前記他の通信装置から送信される前記鍵情報で特定される前記鍵を記憶していないことを示すときに前記記憶手段に記憶していない前記鍵を取得する鍵取得手段と、

をさらに具備する請求項5に記載の通信装置。

[8] 前記鍵取得手段は前記他の通信装置からの制御情報に基づき前記鍵を取得する

ことを特徴とする請求項7に記載の通信装置。

[9] 請求項5記載の通信装置と鍵を用いて通信を行う通信装置であって、

前記鍵の有効期限を含む鍵情報を記憶する記憶手段と、

前記鍵情報を所定間隔ごとに送信する送信手段と、

を具備する通信装置。

[10] 自装置における現在時刻を管理する現在時刻管理部を具備し、

前記送信手段は前記現在時刻を所定間隔ごとに送信する請求項9に記載の通信装置。

[11] 前記有効期限がしきい値より少ない前記鍵の取得の制御情報を生成する制御情報生成手段を具備し、

前記送信手段は前記制御情報を送信する請求項9に記載の通信装置。

補正書の請求の範囲

[2005年10月27日 (27.10.05) 国際事務局受理：出願当初の請求の範囲 1-8 は補正された；出願当初の請求の範囲 9-11 は取り下げられた。]

[1] (補正後) 第1の通信装置と第2の通信装置との間で鍵を用いて通信を行う通信システムであって、

前記第1の通信装置は、前記鍵の識別情報と前記鍵の有効期限とを対応づけて記憶する記憶手段と、前記鍵の有効期限を含むメッセージを所定間隔ごとに送信する送信手段と、前記メッセージに対する応答メッセージを受信する受信手段と、前記応答メッセージに含まれる前記第2の通信装置における前記鍵の有効期限に基づいて、前記記憶手段に記憶する鍵の有効期限を補正する補正手段と、を具備し、

前記第2の通信装置は、前記メッセージを受信する受信手段と、自装置における前記鍵の有効期限を含めた、前記メッセージに対する前記応答メッセージを送信する送信手段と、を具備する通信システム。

[2] (補正後) 前記第1の通信装置および前記第2の通信装置が通信に用いる前記鍵を管理する鍵管理装置をさらに備え、

前記第2の通信装置は、

前記鍵の識別情報と当該鍵の有効期限とを記憶する記憶手段と、

前記メッセージに含まれる鍵の識別情報に対応する鍵の識別情報を前記記憶手段に記憶しているか否かを判定する判定手段と、

前記判定手段による判定結果が前記記憶手段に前記メッセージに含まれる鍵の識別情報に対応する鍵の識別情報を記憶していないことを示すときに、前記鍵を前記鍵管理装置から取得する鍵取得手段と、

を具備し、

前記第2の通信装置の前記送信手段は、前記応答メッセージに前記取得した鍵の有効期限を含めて送信する請求項1に記載の通信システム。

[3] (補正後) 前記第1の通信装置の前記送信手段は、自装置における前記鍵の有効期限がしきい値より少ないときに前記鍵の更新を促す命令信号を前記メッセージに含めて送信し、

前記第2の通信装置は、前記鍵取得手段にて前記命令信号に基づき前記鍵管理装置から前記鍵を取得し、前記送信手段にて前記応答メッセージに前記取得した鍵

の有効期限を含めて送信する請求項2に記載の通信システム。

[4] （補正後） 他の通信装置と鍵を用いて通信を行う通信装置であって、

前記鍵の識別情報と当該鍵の有効期限とを対応づけて記憶する記憶手段と、

前記鍵の有効期限を含むメッセージを所定間隔ごとに送信する送信手段と、

前記メッセージに対する応答メッセージに含まれる前記他の通信装置における前記鍵の有効期限に基づいて、前記記憶手段に記憶する鍵の有効期限を補正する補正手段と、

を具備する通信装置。

[5] （補正後） 前記送信手段は、自装置における前記鍵の有効期限がしきい値より少ないときに鍵の更新を促す命令信号を前記メッセージに含めて送信する請求項4記載の通信装置。

[6] （補正後） 他の通信装置と鍵を用いて通信を行う通信装置であって、

前記他の通信装置における前記鍵の有効期限を含むメッセージを受信する受信手段と、

受信した前記メッセージに応答して、自装置における前記鍵の有効期限を含めた、前記メッセージに対する前記応答メッセージを送信する送信手段と、

を具備する通信装置。

[7] （補正後） 前記鍵の識別情報と前記鍵の有効期限とを記憶する記憶手段と、

前記メッセージに含まれる鍵の識別情報に対応する鍵の識別情報を前記記憶手段に記憶しているか否かを判定する判定手段と、

前記判定手段による判定結果が前記記憶手段に前記メッセージに含まれる鍵の識別情報に対応する鍵の識別情報を記憶していないことを示すときに、前記鍵を鍵管理装置から取得する鍵取得手段と、

を具備し、

前記送信手段は、前記応答メッセージに前記取得した鍵の有効期限を含めて送信する請求項6記載の通信装置。

[8] （補正後） 前記受信手段は、前記他の通信装置における前記鍵の有効期限がしきい値より小さいときに前記メッセージに含めて送信される鍵の更新を促す命令信号を

受信し、

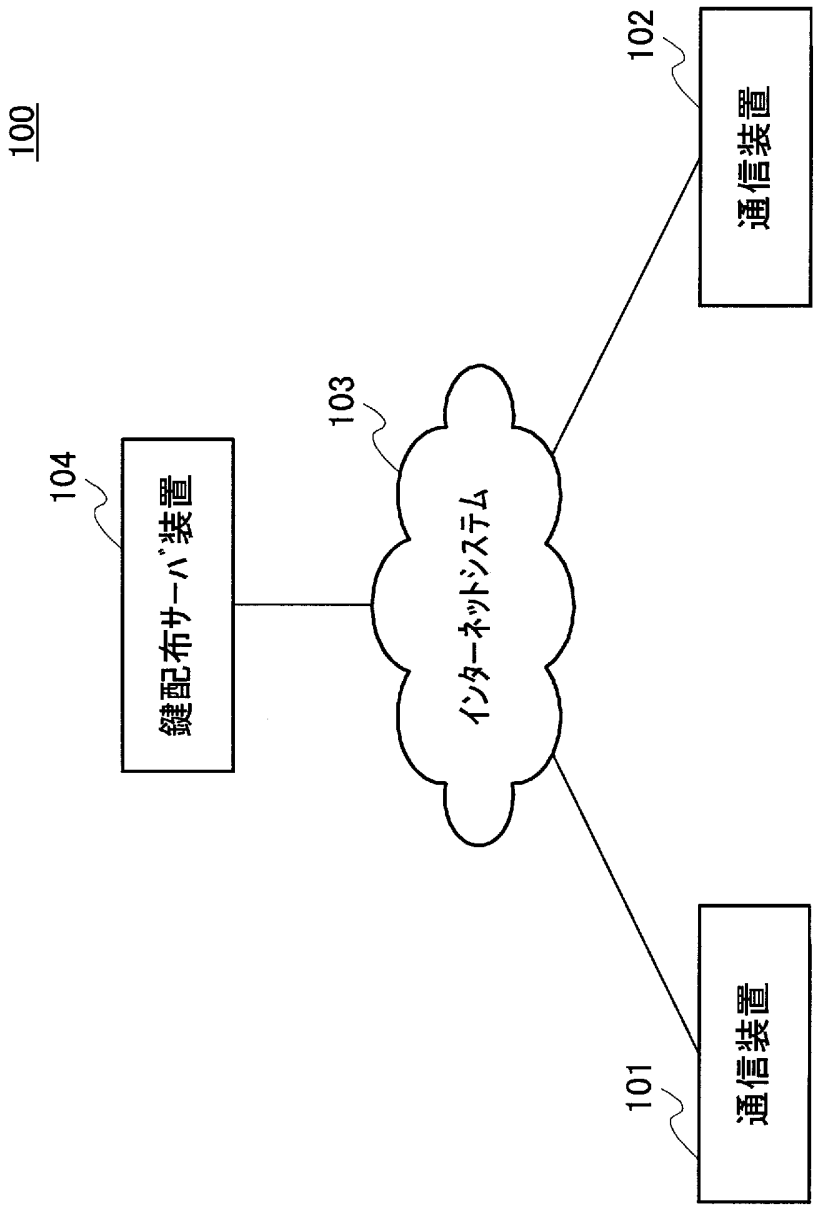
前記鍵取得手段は、前記命令信号に基づき前記鍵管理装置から前記鍵を取得し、前記送信手段は、前記応答メッセージに前記取得した鍵の有効期限を含めて送信する請求項7記載の通信装置。

[9] (削除)

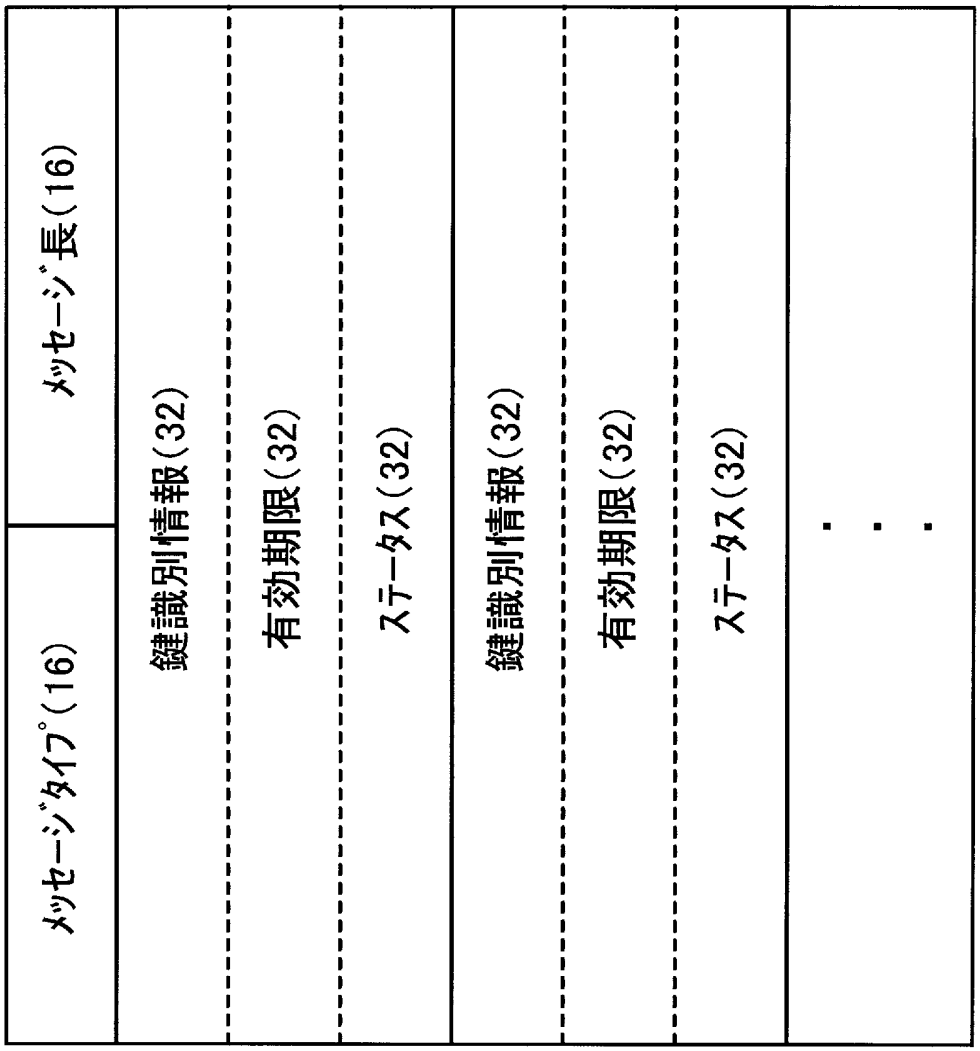
[10] (削除)

[11] (削除)

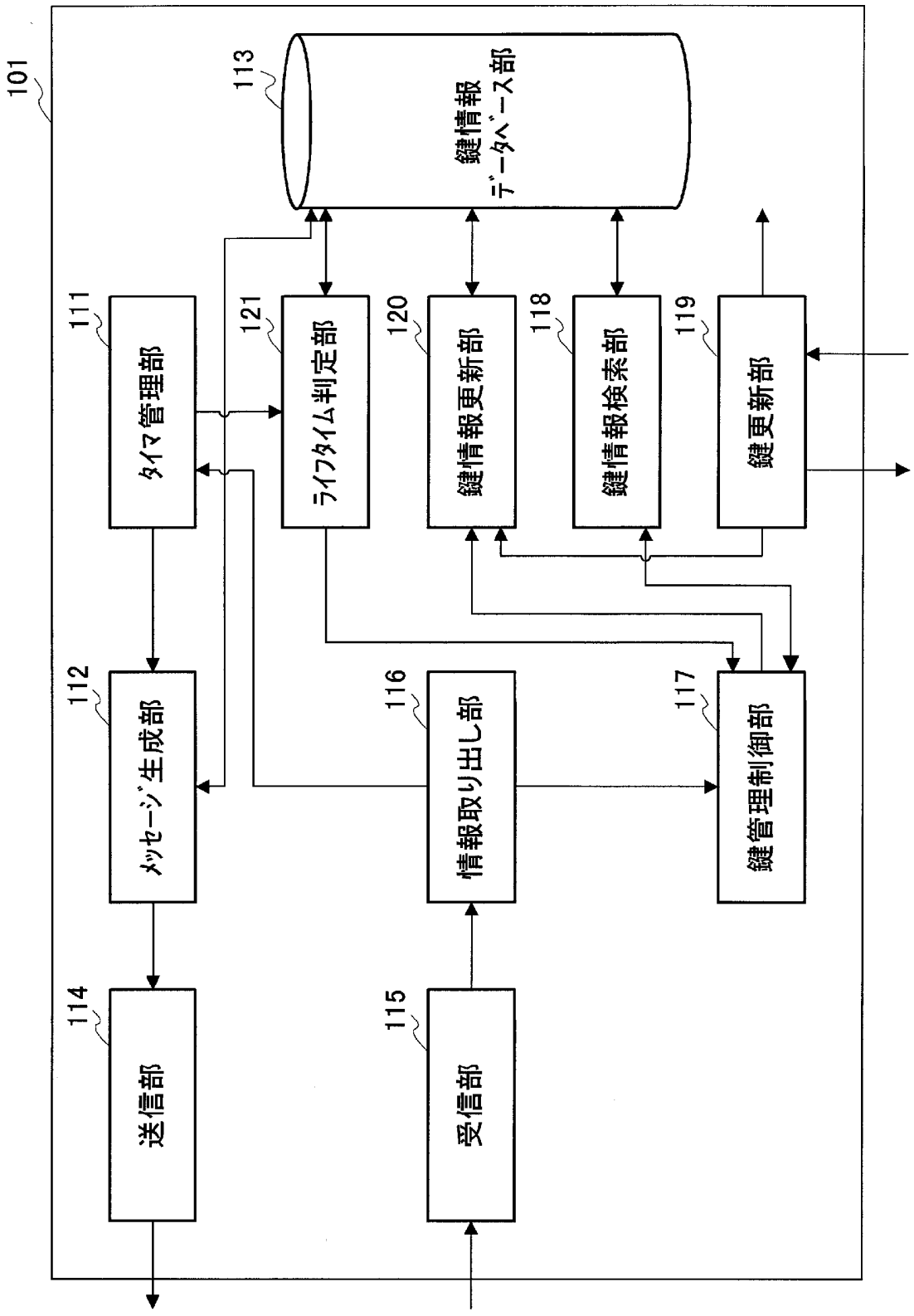
[図1]



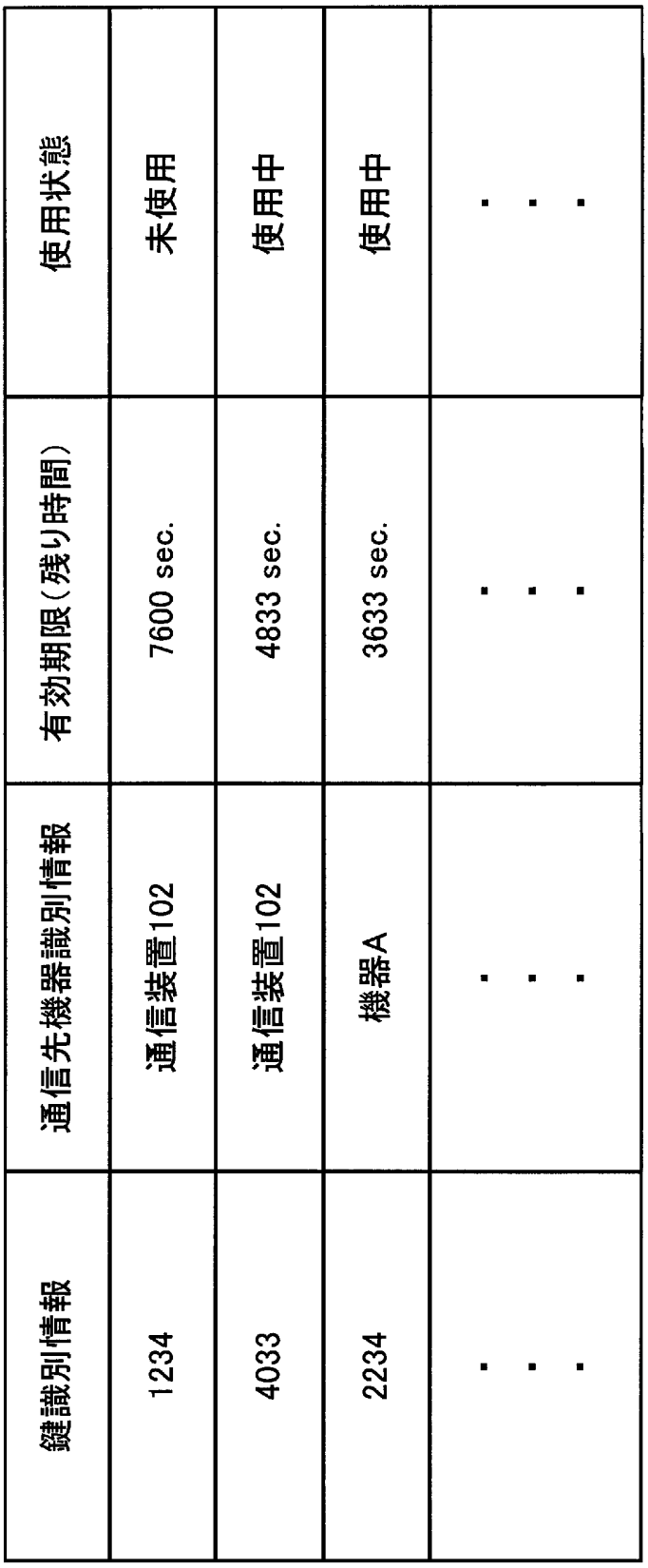
[図2]


メッセージタイプ(16)
メッセージ長(16)
鍵識別情報(32)
有効期限(32)
ステータス(32)
鍵識別情報(32)
有効期限(32)
ステータス(32)

[図3]

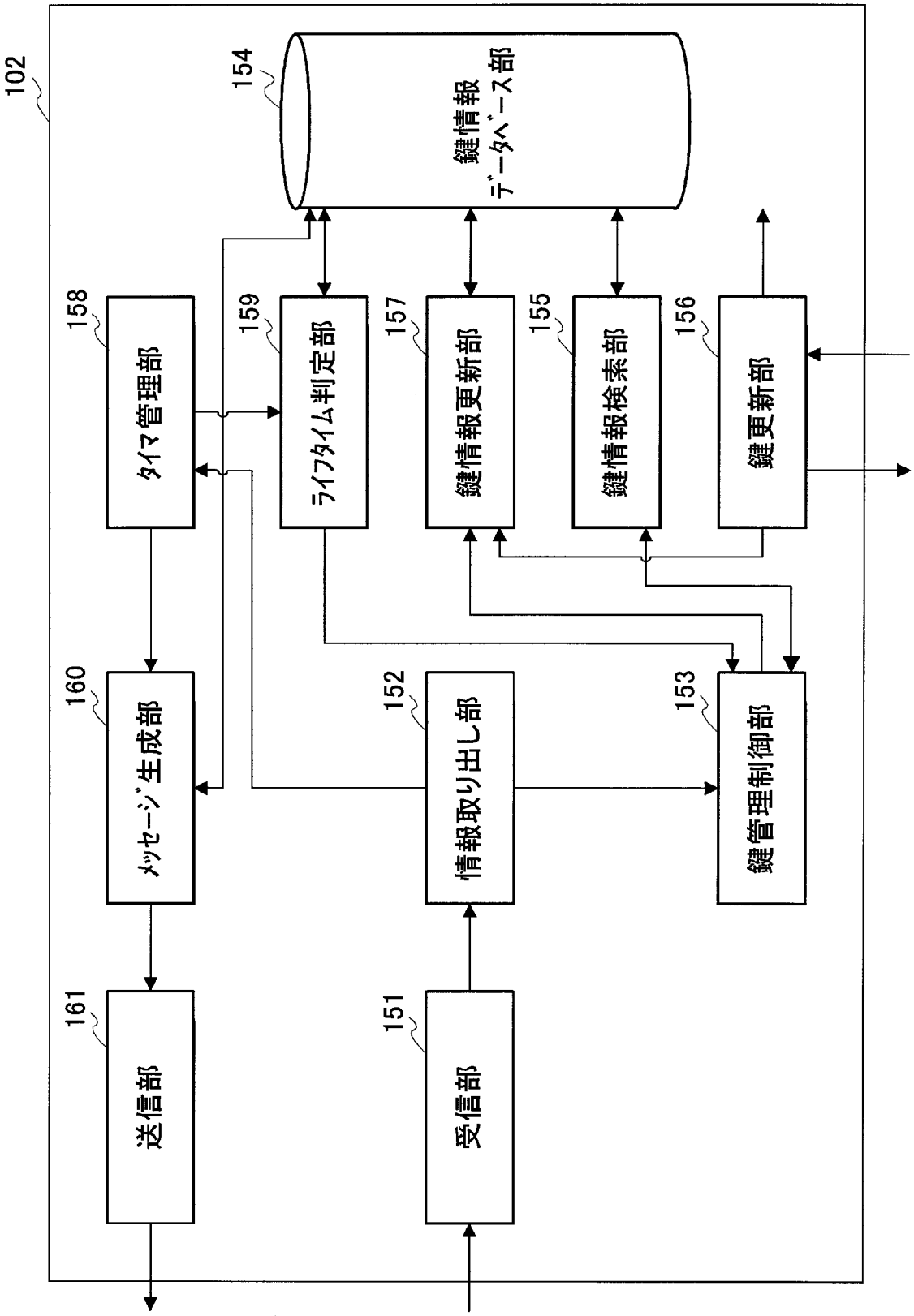

101
113
鍵情報
ﾃﾞｰﾀﾍﾞｰｽ部
111
タイマ管理部
121
ライフタイム判定部
120
鍵情報更新部
118
鍵情報検索部
119
鍵更新部
112
ﾒｯｾｰｼﾞ生成部
116
情報取り出し部
117
鍵管理制御部
114
送信部
115
受信部

[図4]



鍵識別情報	通信先機器識別情報	有効期限（残り時間）	使用状態
1234	通信装置102	7600 sec.	未使用
4033	通信装置102	4833 sec.	使用中
2234	機器A	3633 sec.	使用中
・ ・ ・	・ ・ ・	・ ・ ・	・ ・ ・

[図5]


102
154
鍵情報
データベース部
158
タイマ管理部
159
ライフタイム判定部
157
鍵情報更新部
155
鍵情報検索部
156
鍵更新部
160
メッセージ生成部
152
情報取り出し部
153
鍵管理制御部
161
送信部
151
受信部

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2005/010262

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/08

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)
Int.Cl[7] H04L9/08

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2005
Kokai Jitsuyo Shinan Koho 1971-2005 Toroku Jitsuyo Shinan Koho 1994-2005

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.
X Y	JP 2004-166153 A (NEC Corp., NEC Tsushin System Kabushiki Kaisha), 10 June, 2004 (10.06.04), & US 2004/0105549 A1 Particularly, Par. Nos. [0021] to [0084]	1,3,4,5,7-9, 11 2,6,10
Y	JP 11-212926 A (NEC Tsushin System Kabushiki Kaisha), 06 August, 1999 (06.08.99), Particularly, Par. Nos. [0034] to [0036] (Family: none)	2,6,10
A	JP 2003-101533 A (Toshiba Corp.), 04 April, 2003 (04.04.03), & US 2003/0061518 A1 All pages	1-11

☐ 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
30 August, 2005 (30.08.05)	13 September, 2005 (13.09.05)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

国際調査報告

国際出願番号 PCT／JP2005／010262

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl.[7] H04L9/08

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.[7] H04L9/08

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2005年
日本国実用新案登録公報	1996－2005年
日本国登録実用新案公報	1994－2005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	関連する請求の範囲の番号
X	JP 2004-166153 A （日本電気株式会社，日本電気通信システム株式会社） 2004.06.10 & US 2004/0105549 A1 特に第21-84段落を参照	1, 3, 4, 5, 7-9, 11
Y		2, 6, 10
Y	JP 11-212926 A （日本電気通信システム株式会社） 1999.08.06 （ファミリなし） 特に第34-36段落を参照	2, 6, 10
A	JP 2003-101533 A （株式会社東芝） 2003.04.04 & US 2003/0061518 A1 全頁を参照	1-11

☐ 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 30. 08. 2005	国際調査報告の発送日 13.9.2005
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 9364 中里 裕正 電話番号 03－3581－1101 内線 3546