(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4365733号
(P4365733)
(45)発行日　平成21年11月18日(2009.11.18)　(24)登録日　平成21年8月28日(2009.8.28)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601C
H04L 9/00 601E

請求項の数 8　(全 12 頁)

(21)出願番号　特願2004-184165(P2004-184165)
(22)出願日　平成16年6月22日(2004.6.22)
(65)公開番号　特開2006-13628(P2006-13628A)
(43)公開日　平成18年1月12日(2006.1.12)
審査請求日　平成17年3月14日(2005.3.14)

(73)特許権者　000005821
パナソニック株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100105050
弁理士　鷲田　公一
(72)発明者　金子　友晴
神奈川県横浜市港北区綱島東四丁目３番１号　パナソニックモバイルコミュニケーションズ株式会社内
(72)発明者　稲垣　達也
大阪府門真市大字門真１００６番地　松下電器産業株式会社内

審査官　青木　重徳

最終頁に続く

(54)【発明の名称】通信システムおよび通信装置

(57)【特許請求の範囲】
【請求項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インターネットを介した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通信装置を介して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。
【請求項２】
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。
【請求項３】
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。
【請求項４】
他の通信装置と鍵を用いてインターネットを介した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通信装置を介して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。
【請求項５】
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。
【請求項６】
他の通信装置と鍵を用いてインターネットを介した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通信装置を介して送信する送信手段と、
を具備する通信装置。
【請求項７】
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。
【請求項８】
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。
【発明の詳細な説明】
【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】
本発明は、かかる点に鑑みてなされたものであり、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を目的とする。
【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インターネットを介した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通信装置を介して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。
【発明を実施するための最良の形態】
【０００９】
本発明の骨子は、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を解消し、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である。

【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。

【産業上の利用可能性】

【００６７】

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。

【図面の簡単な説明】

【００６８】

【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

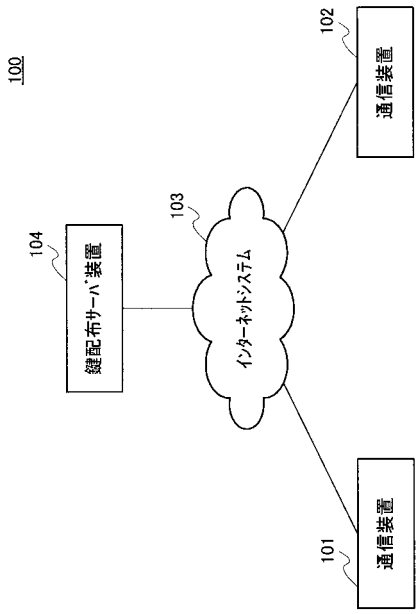
【図５】図１の他の通信装置の構成を示すブロック図

【符号の説明】

【００６９】

１００　通信システム
１０１、１０２　通信装置
１０３　インターネットシステム
１０４　鍵配布サーバ装置
１１１、１５８　タイマ管理部
１１２、１６０　メッセージ生成部
１１３、１５４　鍵情報データベース部
１１４、１６１　送信部
１１５、１５１　受信部
１１６、１５２　情報取り出し部
１１７、１５３　鍵管理制御部
１１８、１５５　鍵情報検索部
１１９、１５６　鍵更新部
１２０、１５７　鍵情報更新部
１２１、１５９　ライフタイム判定部

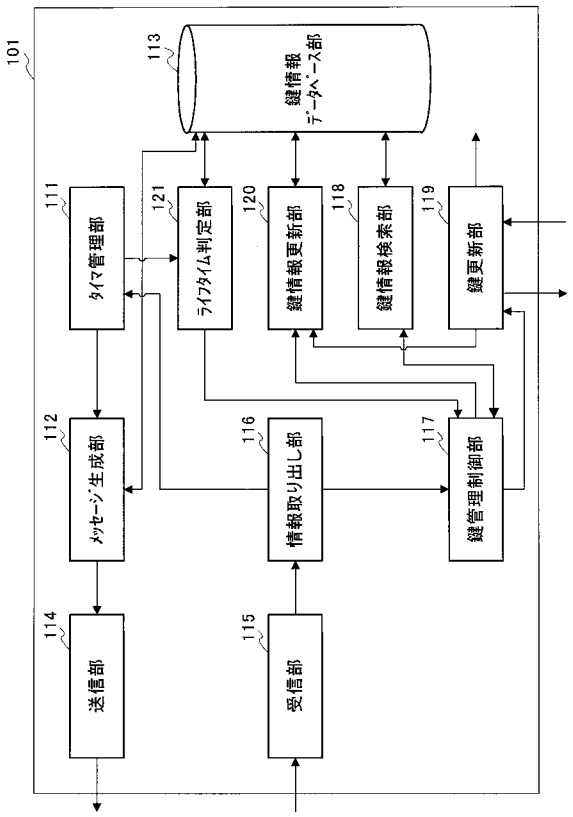
【図１】



【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)	
・ ・ ・	

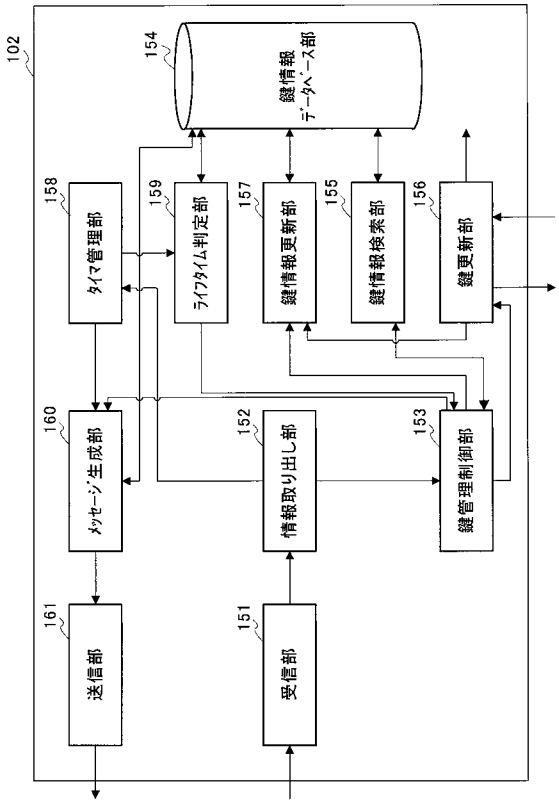
【図３】



【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

フロントページの続き

(56)参考文献 特開２００４－０９６５８３（ＪＰ，Ａ）
特開昭６１－２９６８３５（ＪＰ，Ａ）
特開２００３－２４４１２０（ＪＰ，Ａ）
特開平１０－２７６１８６（ＪＰ，Ａ）
特開平０４－０７００２９（ＪＰ，Ａ）
特開２００１－２３７８２０（ＪＰ，Ａ）
特開２００１－１５６７７０（ＪＰ，Ａ）
特開２００４－０２３２２４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８