(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2014-50069
(P2014-50069A)
(43)公開日　平成26年3月17日(2014.3.17)

(51)Int.Cl.		F I		テーマコード（参考）
H04L 9/14	(2006.01)	H04L 9/00	641	5J104

審査請求 未請求　請求項の数 16　OL　（全 12 頁）

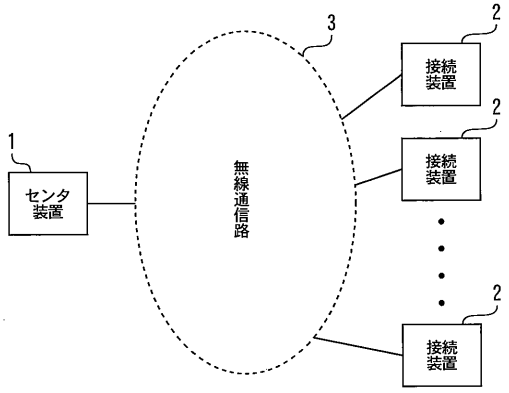
(21)出願番号　特願2012-193962 (P2012-193962)
(22)出願日　平成24年9月4日 (2012.9.4)

(71)出願人　591230295
ＮＴＴエレクトロニクス株式会社
神奈川県横浜市神奈川区新浦島町一丁目１番地３２
(71)出願人　000196587
西日本旅客鉄道株式会社
大阪府大阪市北区芝田２丁目４番２４号
(71)出願人　399041158
西日本電信電話株式会社
大阪府大阪市中央区馬場町３番１５号
(74)代理人　100082175
弁理士　高田　守
(74)代理人　100106150
弁理士　高橋　英樹

最終頁に続く

(54)【発明の名称】暗号通信システム及び暗号通信方法

(57)【要約】
【課題】通信速度が遅い場合でも通信路の輻輳を防ぐことができる暗号通信システム及び暗号通信方法を得る。
【解決手段】センタ装置１に無線通信路３を介して複数の接続装置２が接続されている。センタ装置１は、第１の現行鍵で平文を暗号化して接続装置２に送信し、接続装置２から受信した暗号文を第１の現行鍵又は旧鍵で復号する。センタ装置１は、暗号鍵が生成されると、保持していた旧鍵を削除し、暗号鍵を第１の未来鍵に更新し、保持していた第１の未来鍵を第１の現行鍵に更新し、保持していた第１の現行鍵を旧鍵に更新する。接続装置２は、第２の現行鍵で平文を暗号化してセンタ装置１に送信し、センタ装置１から受信した暗号文を第２の現行鍵又は第２の未来鍵で復号する。接続装置２は、センタ装置１から受信した第１の現行鍵と第１の未来鍵をそれぞれ第２の現行鍵と第２の未来鍵として置き換える。
【選択図】図１



【特許請求の範囲】
【請求項１】
センタ装置と、
前記センタ装置に通信路を介して接続された複数の接続装置とを備え、
前記センタ装置は、
暗号鍵を定期的に生成する暗号鍵生成部と、
現在使用している第１の現行鍵と、前記第１の現行鍵の更新後に使用する第１の未来鍵と、前記第１の現行鍵の前に使用していた旧鍵とを保持し、前記暗号鍵生成部が前記暗号鍵を生成すると、保持していた前記旧鍵を削除し、前記暗号鍵を前記第１の未来鍵に更新し、保持していた前記第１の未来鍵を前記第１の現行鍵に更新し、保持していた前記第１の現行鍵を前記旧鍵に更新する第１の暗号鍵管理部と、
前記第１の現行鍵で平文を暗号化して暗号文を得る第１の暗号化部と、
前記第１の暗号化部から出力された前記暗号文を前記複数の接続装置の１つに送信する第１の暗号文送信部と、
前記複数の接続装置の１つから送信された暗号文を受信する第１の暗号文受信部と、
前記第１の暗号文受信部が受信した前記暗号文を前記第１の現行鍵で復号し、前記第１の現行鍵で復号できない場合は前記旧鍵で復号して平文を得る第１の復号部と、
前記第１の現行鍵と前記第１の未来鍵を鍵配送用鍵で暗号化して前記複数の接続装置の１つに送信する暗号鍵送信部とを有し、
前記接続装置は、
前記暗号鍵送信部から送信された前記第１の現行鍵と前記第１の未来鍵を受信して前記鍵配送用鍵で復号する暗号鍵受信部と、
現在使用している第２の現行鍵と、前記第２の現行鍵の更新後に使用する第２の未来鍵とを保持し、前記暗号鍵受信部から出力された前記第１の現行鍵と前記第１の未来鍵をそれぞれ前記第２の現行鍵と前記第２の未来鍵として置き換える第２の暗号鍵管理部と、
前記第２の現行鍵で平文を暗号化する第２の暗号化部と、
前記第２の暗号化部から出力された前記暗号文を前記センタ装置に送信する第２の暗号文送信部と、
前記第１の暗号文送信部から送信された前記暗号文を受信する第２の暗号文受信部と、
前記第２の暗号文受信部で受信された前記暗号文を前記第２の現行鍵で復号し、前記第２の現行鍵で復号できない場合は前記第２の未来鍵で復号して平文を得る第２の復号部とを有することを特徴とする暗号通信システム。
【請求項２】
前記接続装置は、前記センタ装置が次に鍵更新する時刻である次回鍵更新時刻からその次に鍵更新する時刻である次々回鍵更新時刻までに鍵配送要求パケットを生成し、前記鍵配送要求パケットと接続装置番号を前記センタ装置に送信する暗号鍵配送要求部を更に有し、
前記センタ装置は、前記複数の接続装置の１つから前記鍵配送要求パケットと前記接続装置番号を受信する暗号鍵要求受信部を更に有し、
前記鍵配送要求パケットと前記接続装置番号を受信すると、前記暗号鍵送信部は、前記第１の現行鍵と前記第１の未来鍵を前記鍵配送用鍵で暗号化して、前記接続装置番号に対応する前記接続装置に送信することを特徴とする請求項１に記載の暗号通信システム。
【請求項３】
前記複数の接続装置の前記暗号鍵配送要求部は、前記次回鍵更新時刻から前記次々回鍵更新時刻までのランダムな時刻に前記鍵配送要求パケットを生成し、前記センタ装置に送信することを特徴とする請求項２に記載の暗号通信システム。
【請求項４】
前記センタ装置の前記暗号鍵送信部は、前記次回鍵更新時刻、前記次々回鍵更新時刻、及び鍵更新間隔の少なくとも２つを前記接続装置の前記暗号鍵受信部に送信することを特徴とする請求項２又は３に記載の暗号通信システム。

【請求項５】
前記第２の暗号鍵配送要求部は鍵更新間隔を保持し、
前記センタ装置の前記暗号鍵送信部は、前記次回鍵更新時刻と前記次々回鍵更新時刻の少なくとも１つを前記接続装置の前記暗号鍵受信部に送信することを特徴とする請求項２又は３に記載の暗号通信システム。
【請求項６】
前記暗号鍵配送要求部は、前記接続装置の電源がＯＦＦになっていて、前記次回鍵更新時刻から前記次々回鍵更新時刻までに前記鍵配送要求パケットを前記センタ装置に送信できなかった場合、前記次々回線更新時刻以降に前記接続装置の電源がＯＮした時点で前記鍵配送要求パケットを前記センタ装置に送信することを特徴とする請求項２～５の何れか１項に記載の暗号通信システム。
【請求項７】
前記第２の復号部において前記第２の未来鍵で復号ができた場合は、それ以降は前記第２の復号部及び前記第２の暗号化部は前記第２の未来鍵でそれぞれ復号及び暗号化をすることを特徴とする請求項１～６の何れか１項に記載の暗号通信システム。
【請求項８】
前記暗号鍵送信部は、前記第１の現行鍵と前記第１の未来鍵の代わりに、前記第１の現行鍵と前記第１の未来鍵を生成するためのデータを送信することを特徴とする請求項１～７の何れか１項に記載の暗号通信システム。
【請求項９】
通信路を介して接続されたセンタ装置と複数の接続装置との間で暗号通信を行う方法であって、
前記センタ装置が暗号鍵を定期的に生成するステップと、
前記センタ装置が、現在使用している第１の現行鍵と、前記第１の現行鍵の更新後に使用する第１の未来鍵と、前記第１の現行鍵の前に使用していた旧鍵とを保持し、前記暗号鍵が生成されると、保持していた前記旧鍵を削除し、前記暗号鍵を前記第１の未来鍵に更新し、保持していた前記第１の未来鍵を前記第１の現行鍵に更新し、保持していた前記第１の現行鍵を前記旧鍵に更新するステップと、
前記センタ装置が第１の現行鍵で平文を暗号化して前記複数の接続装置の１つに送信するステップと、
前記センタ装置が前記複数の接続装置の１つから送信された暗号文を受信し、前記第１の現行鍵で復号し、前記第１の現行鍵で復号できない場合は前記旧鍵で復号するステップと、
前記センタ装置が前記第１の現行鍵と前記第１の未来鍵を鍵配送用鍵で暗号化して前記複数の接続装置の１つに送信するステップと、
前記接続装置が、前記センタ装置から送信された前記第１の現行鍵と前記第１の未来鍵を受信して前記鍵配送用鍵で復号するステップと、
前記接続装置が、現在使用している第２の現行鍵と、前記第２の現行鍵の更新後に使用する第２の未来鍵とを保持し、受信した前記第１の現行鍵と前記第１の未来鍵をそれぞれ前記第２の現行鍵と前記第２の未来鍵に更新するステップと、
前記接続装置が、前記第２の現行鍵で平文を暗号化して前記センタ装置に送信するステップと、
前記接続装置が、前記センタ装置から送信された前記暗号文を受信し、前記第２の現行鍵で復号し、前記第２の現行鍵で復号できない場合は前記第２の未来鍵で復号するステップとを備えることを特徴とする暗号通信方法。
【請求項１０】
前記接続装置が、前記センタ装置が次に鍵更新する時刻である次回鍵更新時刻からその次に鍵更新する時刻である次々回鍵更新時刻までに鍵配送要求パケットを生成し、前記鍵配送要求パケットと接続装置番号を前記センタ装置に送信するステップと、
前記センタ装置が、前記複数の接続装置の１つから前記鍵配送要求パケットと前記接続

装置番号を受信するステップと、
前記センタ装置が、前記鍵配送要求パケットと前記接続装置番号を受信すると、前記第１の現行鍵と前記第１の未来鍵を前記鍵配送用鍵で暗号化して、前記接続装置番号に対応する前記接続装置に送信するステップとを更に備えることを特徴とする請求項９に記載の暗号通信方法。
【請求項１１】
前記複数の接続装置は、前記次回鍵更新時刻から前記次々回鍵更新時刻までの間のランダムな時刻に前記鍵配送要求パケットを生成し、前記センタ装置に送信することを特徴とする請求項１０に記載の暗号通信方法。
【請求項１２】
前記センタ装置は、前記次回鍵更新時刻、前記次々回鍵更新時刻、及び鍵更新間隔の少なくとも２つを前記接続装置に送信することを特徴とする請求項１０又は１１に記載の暗号通信方法。
【請求項１３】
前記複数の接続装置は鍵更新間隔を保持し、
前記センタ装置は、前記次回鍵更新時刻と前記次々回鍵更新時刻の少なくとも１つを前記接続装置に送信することを特徴とする請求項１０又は１１に記載の暗号通信方法。
【請求項１４】
前記接続装置は、前記接続装置の電源がＯＦＦになっていて、前記次回鍵更新時刻から前記次々回鍵更新時刻までに前記鍵配送要求パケットを前記センタ装置に送信できなかった場合、前記次々回線更新時刻以降に前記接続装置の電源がＯＮした時点で前記鍵配送要求パケットを前記センタ装置に送信することを特徴とする請求項１０～１３の何れか１項に記載の暗号通信方法。
【請求項１５】
前記接続装置は、前記第２の未来鍵で復号ができた場合は、それ以降は前記第２の未来鍵で暗号化及び復号をすることを特徴とする請求項９～１４の何れか１項に記載の暗号通信方法。
【請求項１６】
前記センタ装置は、前記第１の現行鍵と前記第１の未来鍵の代わりに、前記第１の現行鍵と前記第１の未来鍵を生成するためのデータを送信することを特徴とする請求項９～１５の何れか１項に記載の暗号通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信路を介して接続されたセンタ装置と複数の接続装置との間で暗号通信を行う際に、通信速度が遅い場合でも通信路の輻輳を防ぐことができる暗号通信システム及び暗号通信方法に関する。
【背景技術】
【０００２】
従来、通信路を介して接続されたセンタ装置と複数の接続装置との間で暗号通信を行う場合には、接続装置の接続開始時に接続装置がセンタ装置に鍵配送を要求して暗号鍵を取得していた。
【０００３】
図６は鍵配送処理を示す図である。接続装置が暗号鍵を取得するには、鍵配送要求、鍵配送、鍵配送応答の３ｗａｙの通信が最低限必要である。例えば、サーバ（センタ装置に対応）とクライアント（接続装置に対応）との間の暗号通信に広く用いられるＳＳＬ（Secure Socket Layer）においては、client helloが鍵配送要求に、premaster secret messageが鍵配送に、finishedが鍵配送応答に対応する（例えば、非特許文献１参照）。このＳＳＬでは更に証明書の交換・認証等の処理のための通信が必要となる。
【０００４】

センタ装置から接続装置に暗号鍵そのものを配送することは危険であるため、暗号鍵を生成するためのデータを送付し、双方で決められたアルゴリズムにより同じ鍵を共有する方法がしばしば用いられる（例えば、非特許文献２参照）。また、ＳＳＬでは乱数（premaster secret）を送付し、その値から決められたアルゴリズムにより計算する等により双方で同じ暗号鍵を生成する。

【先行技術文献】

【非特許文献】

【０００５】

【非特許文献１】The SSL Protocol Version 3.0、インターネット＜ URL ： http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt＞

【非特許文献２】W. Diffie and M. E. Hellman, ”New Directions in Cryptography”, IEEE transactions on Information Theory, vol.IT-22, No.6, pp.644-654, Nov, 1976

【発明の概要】

【発明が解決しようとする課題】

【０００６】

従来は、センタ装置で鍵が更新されていない場合でも、接続装置での通信の開始時や装置の立ち上げ時に鍵配送が行われていた。接続装置への鍵配送を減らすには、センタ装置で鍵が更新された場合のみ、鍵配送を行うことが望ましい。これを実現するには、センタ装置での鍵更新に同期して全ての接続装置への鍵配送を行う必要がある。しかし、複数の接続装置への鍵配送の衝突によって通信路の輻輳が発生する。これを避けるには鍵配送を順次行う必要があるが、一部の接続装置で新しい暗号鍵の配送が間に合わず通信ができない場合がある。この問題は、通信速度が例えば１０Ｍｂｐｓ以下の遅い場合に顕著となる。

【０００７】

本発明は、上述のような課題を解決するためになされたもので、その目的は通信速度が遅い場合でも通信路の輻輳を防ぐことができる暗号通信システム及び暗号通信方法を得るものである。

【課題を解決するための手段】

【０００８】

本発明に係る暗号通信システムは、センタ装置と、前記センタ装置に通信路を介して接続された複数の接続装置とを備え、前記センタ装置は、暗号鍵を定期的に生成する暗号鍵生成部と、現在使用している第１の現行鍵と、前記第１の現行鍵の更新後に使用する第１の未来鍵と、前記第１の現行鍵の前に使用していた旧鍵とを保持し、前記暗号鍵生成部が前記暗号鍵を生成すると、保持していた前記旧鍵を削除し、前記暗号鍵を前記第１の未来鍵に更新し、保持していた前記第１の未来鍵を前記第１の現行鍵に更新し、保持していた前記第１の現行鍵を前記旧鍵に更新する第１の暗号鍵管理部と、前記第１の現行鍵で平文を暗号化して暗号文を得る第１の暗号化部と、前記第１の暗号化部から出力された前記暗号文を前記複数の接続装置の１つに送信する第１の暗号文送信部と、前記複数の接続装置の１つから送信された暗号文を受信する第１の暗号文受信部と、前記第１の暗号文受信部が受信した前記暗号文を前記第１の現行鍵で復号し、前記第１の現行鍵で復号できない場合は前記旧鍵で復号して平文を得る第１の復号部と、前記第１の現行鍵と前記第１の未来鍵を鍵配送用鍵で暗号化して前記複数の接続装置の１つに送信する暗号鍵送信部とを有し、前記接続装置は、前記暗号鍵送信部から送信された前記第１の現行鍵と前記第１の未来鍵を受信して前記鍵配送用鍵で復号する暗号鍵受信部と、現在使用している第２の現行鍵と、前記第２の現行鍵の更新後に使用する第２の未来鍵とを保持し、前記暗号鍵受信部から出力された前記第１の現行鍵と前記第１の未来鍵をそれぞれ前記第２の現行鍵と前記第２の未来鍵として置き換える第２の暗号鍵管理部と、前記第２の現行鍵で平文を暗号化する第２の暗号化部と、前記第２の暗号化部から出力された前記暗号文を前記センタ装置に送信する第２の暗号文送信部と、前記第１の暗号文送信部から送信された前記暗号文を受信する第２の暗号文受信部と、前記第２の暗号文受信部で受信された前記暗号文を前記第

２の現行鍵で復号し、前記第２の現行鍵で復号できない場合は前記第２の未来鍵で復号して平文を得る第２の復号部とを有することを特徴とする。

【発明の効果】

【０００９】

本発明により、通信速度が遅い場合でも通信路の輻輳を防ぐことができる。

【図面の簡単な説明】

【００１０】

【図１】本発明の実施の形態に係る暗号通信システムを示す全体図である。

【図２】本発明の実施の形態に係るセンタ装置を示すブロック図である。

【図３】本発明の実施の形態に係る接続装置を示すブロック図である。

【図４】本発明の実施の形態に係る鍵配送処理フローを示す図である。

【図５】本発明の実施の形態における暗号鍵管理及び暗号通信の状況を示す図である。

【図６】鍵配送処理を示す図である。

【発明を実施するための形態】

【００１１】

本発明の実施の形態に係る暗号通信システム及び暗号通信方法について図面を参照して説明する。同じ又は対応する構成要素には同じ符号を付し、説明の繰り返しを省略する場合がある。

【００１２】

図１は、本発明の実施の形態に係る暗号通信システムを示す全体図である。１台のセンタ装置１に対して複数の接続装置２（最大で数千台）が１０Ｍｂｐｓ以下の低速の無線通信路３を介して接続されている。センタ装置１と接続装置２との間で双方向の暗号通信が行われ、接続装置２間の通信は無い。

【００１３】

図２は、本発明の実施の形態に係るセンタ装置を示すブロック図である。暗号鍵管理部４は、現在使用している第１の現行鍵と、第１の現行鍵の更新後に使用する第１の未来鍵と、第１の現行鍵の前に使用していた旧鍵とを保持している。

【００１４】

平文入力部５は、平文を外部装置から入力する。暗号化部６は、平文入力部５から出力された平文を第１の現行鍵で暗号化して暗号文を得る。暗号文送信部７は、暗号化部６から出力された暗号文を複数の接続装置２の１つに送信する。

【００１５】

暗号文受信部８は、複数の接続装置２の１つから送信された暗号文を受信する。復号部９は、暗号文受信部８が受信した暗号文を第１の現行鍵で復号し、第１の現行鍵で復号できない場合は旧鍵で復号して平文を得る。平文出力部１０は、復号部９から出力された平文を外部装置に出力する。

【００１６】

暗号鍵生成部１１は、暗号鍵を定期的に生成する。暗号鍵生成部１１が暗号鍵を生成すると、暗号鍵管理部４は、保持していた旧鍵を削除し、暗号鍵を第１の未来鍵に更新し、保持していた第１の未来鍵を第１の現行鍵に更新し、保持していた第１の現行鍵を旧鍵に更新する。

【００１７】

暗号鍵要求受信部１２は、複数の接続装置２の１つから鍵配送要求パケットと接続装置番号を受信して暗号鍵管理部４に供給する。これに応じて暗号鍵管理部４は、暗号鍵送信部１３に第１の現行鍵、第１の未来鍵、鍵生成時刻等を供給する。暗号鍵送信部１３は、第１の現行鍵と第１の未来鍵を鍵配送用鍵で暗号化して、接続装置番号に対応する接続装置２に送信する。具体的には、暗号鍵送信部１３は、第１の現行鍵、第１の未来鍵、次回鍵更新時刻、センタ装置１の時計における鍵配送時の時刻、及び鍵更新間隔のハッシュ値を算出し、ハッシュ前のデータとハッシュ値を暗号化して送信する。ハッシュ値は鍵配送時に通信エラーや改竄が発生していないことを検証するために用いる。暗号鍵配送応答受

信部１４は、鍵配送を行った接続装置２から鍵配送応答パケットを受信し、鍵配送完了を暗号鍵管理部４に伝える。

【００１８】

図３は、本発明の実施の形態に係る接続装置を示すブロック図である。暗号鍵管理部１５は、現在使用している第２の現行鍵と、第２の現行鍵の更新後に使用する第２の未来鍵とを保持している。

【００１９】

平文入力部１６は、平文を外部装置から入力する。暗号化部１７は、平文入力部１６から出力された平文を第２の現行鍵で暗号化する。暗号文送信部１８は、暗号化部１７から出力された暗号文をセンタ装置１に送信する。

【００２０】

暗号文受信部１９は、暗号文送信部７から送信された暗号文を受信する。復号部２０は、暗号文受信部１９で受信された暗号文を第２の現行鍵で復号し、第２の現行鍵で復号できない場合は第２の未来鍵で復号して平文を得る。平文出力部２１は、復号部２０から出力された平文を外部装置に出力する。

【００２１】

ここで、復号部２０において第２の現行鍵で復号できた場合には、その後も復号部２０及び暗号化部１７は第２の現行鍵でそれぞれ復号及び暗号化をする。一方、復号部２０において第２の未来鍵で復号できた場合は、それ以降は復号部２０及び暗号化部１７は第２の未来鍵でそれぞれ復号及び暗号化をする。ただし、接続装置２での暗号化には常に第２の現行鍵を用い、第２の現行鍵で復号できない場合にのみ第２の未来鍵で復号することとしてもよい。

【００２２】

第２の現行鍵でも第２の未来鍵でも復号できない場合には通信エラーと判定し、鍵の切り替えは実行しない。なお、復号できたか否かは暗号化するデータにＣＲＣ（Cyclic Redundancy Check)を含めておき、ＣＲＣ検証ができるか否かで判定する。このように第２の現行鍵を使用していて復号できなくなった時点で、第２の未来鍵に切り替えることにより、鍵配送を受けることなく暗号通信を継続することができる。

【００２３】

暗号鍵受信部２２は、暗号鍵送信部１３から送信された第１の現行鍵と第１の未来鍵を受信して鍵配送用鍵で復号し、ハッシュ検証する。ハッシュ検証が成功した場合には受信した暗号鍵を暗号鍵管理部１５に供給し、暗号鍵配送応答部２４に暗号鍵受領を通知し、暗号鍵配送要求部２３に次回鍵更新時刻と鍵更新間隔を供給し、接続装置２の時計を受信したセンタ装置１の時刻に合わせる。ハッシュ検証が失敗した場合には受信したパケットを破棄する。

【００２４】

暗号鍵管理部１５は、暗号鍵受信部２２から出力された第１の現行鍵と第１の未来鍵をそれぞれ第２の現行鍵と第２の未来鍵に更新する。暗号鍵受領を通知された暗号鍵配送応答部２４は、鍵配送応答パケットを生成し、鍵配送用鍵で暗号化してセンタ装置１の暗号鍵配送応答受信部１４に送信する。

【００２５】

暗号鍵配送要求部２３は、鍵配送時に受領した次回鍵更新時刻と鍵更新間隔から次々回鍵更新時刻を計算する。そして、鍵配達受領後、センタ装置１が次に鍵更新する時刻である次回鍵更新時刻からその次に鍵更新する時刻である次々回鍵更新時刻までの間のランダムな時刻に、鍵配送要求パケットを生成し、鍵配送要求パケットと接続装置番号をセンタ装置１に送信する。このように鍵配達受領後、次々回鍵更新時刻までに鍵配送要求を行うことで、途切れることなく暗号通信を継続することができる。なお、ランダムな時刻は乱数等を用いて決められる。

【００２６】

また、接続装置２の電源がＯＦＦになっていると、暗号鍵配送要求部２３が、次回鍵更

新時刻から次々回鍵更新時刻までに鍵配送要求パケットをセンタ装置１に送信できない場合がある。その場合には、次々回線更新時刻以降に接続装置２の電源がＯＮした時点で鍵配送要求パケットをセンタ装置１の暗号鍵配送応答受信部１４に送信する。

【００２７】

続いて、図４は、本発明の実施の形態に係る鍵配送処理フローを示す図である。接続装置２の初期化時に、センタ装置１が鍵配送用鍵を生成する（ステップＳ１）。接続装置２が鍵配送用鍵を受領して暗号鍵管理部１５に書き込む（ステップＳ２）。鍵配送用鍵は配送する鍵を秘匿するために必要なものであり、接続装置２ごとに異なる鍵配送用鍵が予め生成され、センタ装置１の暗号鍵管理部４と接続装置２の暗号鍵管理部１５に書き込まれている。

【００２８】

センタ装置１では定期的に（一定の鍵更新間隔で）通信用の暗号鍵の鍵更新が行われる（ステップＳ３）。鍵更新間隔は通信システムで決められる。センタ装置１は、第１の現行鍵と第１の未来鍵と旧鍵とを保持し、鍵更新が行われると、保持していた旧鍵を削除し、暗号鍵を第１の未来鍵に更新し、保持していた第１の未来鍵を第１の現行鍵に更新し、保持していた第１の現行鍵を旧鍵に更新する。

【００２９】

接続装置２は、センタ装置１から受領した次回鍵更新時刻と鍵更新間隔から、次回鍵更新時刻から次々回鍵更新時刻までのランダムな時刻に決定される鍵配送用要求タイミングをチェックする（ステップＳ４）。鍵配送用要求タイミングを過ぎている場合には直ちに鍵配送要求パケットを生成し、鍵配送要求パケットと接続装置番号をセンタ装置１に送信する（ステップＳ５）。なお、鍵配送用要求のタイミングを超過した時点で接続装置の電源がＯＦＦになっている場合には、その後初めて接続装置２の電源がＯＮした時点で直ちに鍵配送要求を行う。

【００３０】

センタ装置１は接続装置２からの鍵配送要求を待ち（ステップＳ６）、鍵配送要求を受信すると第１の現行鍵、第１の未来鍵、センタ時刻、次回鍵更新時刻、鍵更新間隔のハッシュ値を算出する（ステップＳ７）。ハッシュ前のデータとハッシュ値を鍵配送用鍵で暗号化して接続装置２に送信する（ステップＳ８）。

【００３１】

接続装置２は鍵等を受領する（ステップＳ９）。これらを鍵配送用鍵で復号し、ハッシュ検証及び時刻合わせを行う。センタ装置１から受信した第１の現行鍵と第１の未来鍵が、それぞれ暗号鍵管理部１５に保持されていた元の第２の現行鍵と第２の未来鍵に置き換わる。接続装置２は鍵配送応答パケットを生成する（ステップＳ１０）。この鍵配送応答パケットを鍵配送用鍵で暗号化し、センタ装置１へ鍵配送応答を行う（ステップＳ１１）。その後、鍵配送用要求タイミングのチェックＳ４に戻る。センタ装置１は鍵配送応答を受領した後、鍵配送完了を確認する（ステップＳ１２）。その後、鍵配送要求受領待ちＳ６に戻る。

【００３２】

なお、鍵配送用鍵やハッシュ値を用いることは鍵配送における一般的な方法であり、実用上の種々のバリエーションが考えられる。本実施の形態では鍵配送用鍵として共通鍵を用いるが、公開鍵でもよい。センタ装置１と接続装置２との間で時刻ずれが生じると接続装置２における鍵配送用要求タイミングにずれが生ずるため、鍵配送のたびに時刻合わせを行う。

【００３３】

鍵配送の一連の処理が済むと通信可能状態となる。通信可能状態では鍵配送用要求タイミングのチェックＳ４を常時行っており、鍵配送用要求タイミングを超過した場合には鍵配送要求が出される。

【００３４】

続いて、図５は、本発明の実施の形態における暗号鍵管理及び暗号通信の状況を示す図

である。図中でＫｎは暗号鍵であり、ｎは鍵の区別を示し、ｎが同じものは同じ鍵を示す。各装置が保持する鍵をカッコ内に示し、センタ装置１では（旧鍵、第１の現行鍵、第１の未来鍵）、接続装置２では（第２の現行鍵、第２の未来鍵）を示す。ｔＫｎは暗号鍵Ｋｎが第１の現行鍵から旧鍵になる鍵更新時刻を示し、ｔＩは鍵更新間隔を示す。ｔｎは暗号鍵Ｋｎが第１の現行鍵、Ｋｎ＋１が第１の未来鍵として鍵配送される時刻を示す。

【００３５】

（１）接続装置２がセンタ装置１に鍵配送要求をする（図４のステップＳ５）。（２）センタ装置１は鍵配送要求を受けて、センタ装置１の現行鍵Ｋ１と未来鍵Ｋ２を接続装置２に送信する（図４のステップＳ８）。この際に次回鍵更新時刻ｔＫ１（Ｋ１が現行鍵から旧鍵となる時刻）と鍵更新間隔ｔＩも送信する。（３）接続装置２は第１の現行鍵Ｋ１と第１の未来鍵Ｋ２を受信して確認した後、接続装置２の第２の現行鍵と第２の未来鍵をＫ１とＫ２にそれぞれ置き換え、センタ装置１に鍵配送応答を送信する（図４のステップＳ１１）。（４）（５）センタ装置１と接続装置２は両者とも現行鍵Ｋ１で暗号化する。

【００３６】

（６）時刻ｔＫ１においてセンタ装置１で鍵更新が行われる。新規に生成された暗号鍵Ｋ３が未来鍵に、未来鍵Ｋ２が現行鍵に、現行鍵Ｋ１が旧鍵になり、元の旧鍵Ｋ０は削除される。

【００３７】

センタ装置１で鍵更新が行われた後も、接続装置２はセンタ装置１からの通信を受信するまではセンタ装置１での鍵更新を認識できない。このため、（７）接続装置２からセンタ装置１に通信する場合、接続装置２が古い鍵（センタ装置１の鍵更新前の第１の現行鍵）である接続装置２の第２の現行鍵Ｋ１で暗号化してしまう。この場合、センタ装置１は鍵更新後の第１の現行鍵Ｋ２で復号を試みるが、鍵不一致のため復号できないので、センタ装置１は旧鍵Ｋ１で復号する。これにより、途切れることなく暗号通信を継続することができる。

【００３８】

（８）センタ装置１から通信する場合、センタ装置１の現行鍵Ｋ２で暗号化し、接続装置２は現行鍵Ｋ１で復号を試みるが、鍵不一致のため復号できないので、接続装置２は未来鍵Ｋ２で復号する。（９）未来鍵Ｋ２で復号に成功した後は、接続装置２は未来鍵Ｋ２で暗号化を行うようになる。なお、鍵更新の後に接続装置からの通信（７）が無く、センタ装置１からの通信（８）が最初に行われる場合も有る。

【００３９】

（１０）次回鍵更新時刻ｔＫ１から次々回鍵更新時刻（ｔＫ１＋ｔＩ）までの間のランダムな時刻ｔ２に、接続装置２がセンタ装置１に鍵配送要求をする（図４のステップＳ５）。（１１）センタ装置１は鍵配送要求を受けて、センタ装置１の現行鍵Ｋ２と未来鍵Ｋ３を接続装置２に送信する（図４のステップＳ８）。（１２）接続装置２は現行鍵Ｋ２と未来鍵Ｋ３を受信して確認した後、接続装置２の第２の現行鍵と第２の未来鍵をＫ２とＫ３にそれぞれ置き換え、センタ装置１に鍵配送応答を送信する（図４のステップＳ１１）。（１３）（１４）センタ装置１と接続装置２は両者とも現行鍵Ｋ２で暗号化する。以降、同様のステップが繰り返される。

【００４０】

以上のように本実施の形態では、センタ装置１が第１の現行鍵と第１の未来鍵と旧鍵を保持し、接続装置２が第２の現行鍵と第２の未来鍵を保持する構成により、鍵配送の回数を最小限（鍵更新の回数×接続装置数）に抑えて、途切れることなく暗号通信を継続することができる。そして、各接続装置２は保持している鍵で復号ができなくなる時刻までに更新された鍵を受け取ればよいため、センタ装置１は鍵更新ごとに全ての接続装置２への鍵配送を同時に行う必要が無い。このため、通信速度が遅い場合でも他の接続装置への鍵配送との衝突による通信路の輻輳を防ぐことができる。具体的には、複数の接続装置２が次回鍵更新時刻から次々回鍵更新時刻までのランダムな時刻に鍵配送要求を行えば、複数の接続装置２への鍵配送のタイミングがずれるため、通信路の輻輳を防ぐことができる。

【００４１】

なお、本実施の形態では、鍵配送要求タイミングを決定するため、センタ装置１の暗号鍵送信部１３が次回鍵更新時刻と鍵更新間隔を接続装置２の暗号鍵受信部２２に送信している。これに限らず、センタ装置１の暗号鍵送信部１３が、次回鍵更新時刻、次々回鍵更新時刻、及び鍵更新間隔の少なくとも２つを接続装置２の暗号鍵受信部２２に送信すればよい。また、接続装置２の第２の暗号鍵配送要求部２３に鍵更新間隔を予め書き込んでおき、センタ装置１の暗号鍵送信部１３が次回鍵更新時刻と次々回鍵更新時刻の少なくとも１つを接続装置２の暗号鍵受信部２２に送信することでもよい。

【００４２】

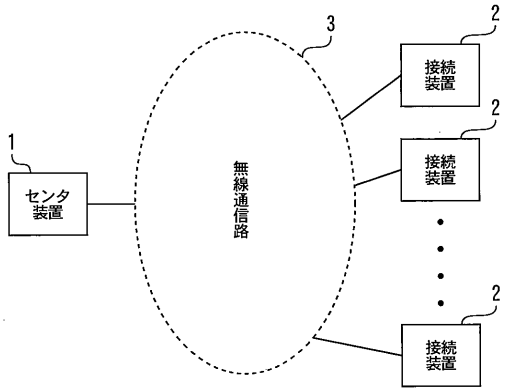
また、センタ装置１の暗号鍵送信部１３が、第１の現行鍵と第１の未来鍵の代わりに、第１の現行鍵と第１の未来鍵を生成するためのデータを送信するようにしてもよい。この場合には、接続装置２は、受信したデータに基づいて第１の現行鍵と第１の未来鍵を生成する。

【符号の説明】

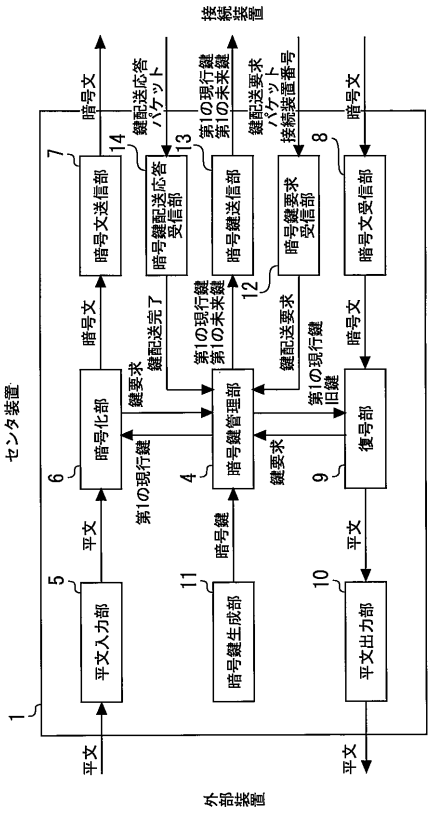
【００４３】

１　センタ装置、２　接続装置、３　無線通信路（通信路）、４　暗号鍵管理部（第１の暗号鍵管理部）、５，１６　平文入力部、６　暗号化部（第１の暗号化部）、７　暗号文送信部（第１の暗号文送信部）、８　暗号文受信部（第１の暗号文受信部）、９　復号部（第１の復号部）、１０，２１　平文出力部、１１　暗号鍵生成部、１２　暗号鍵要求受信部、１３　暗号鍵送信部、１４　暗号鍵配送応答受信部、１５　暗号鍵管理部（第２の暗号鍵管理部）、１７　暗号化部（第２の暗号化部）、１８　暗号文送信部（第２の暗号文送信部）、１９　暗号文受信部（第２の暗号文受信部）、２０　復号部（第２の復号部）、２２　暗号鍵受信部、２３　暗号鍵配送要求部、２４　暗号鍵配送応答部

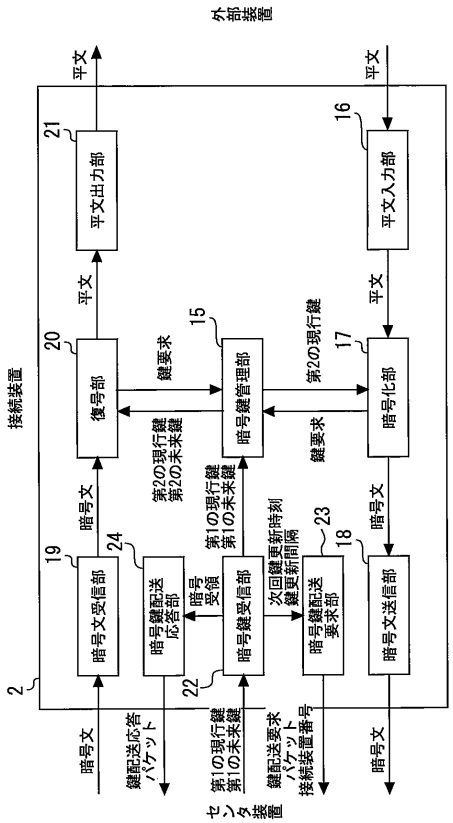
【図１】



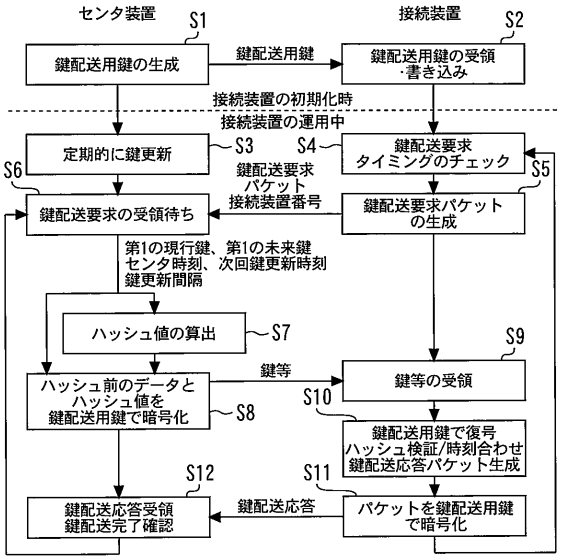
【図２】



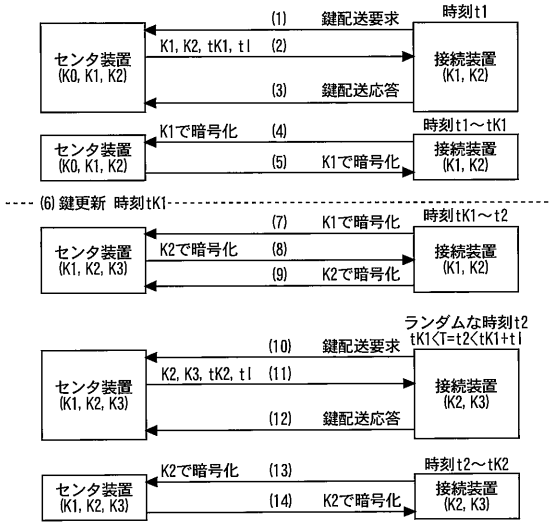
【図３】


外部装置
平文
平文
平文
平文
暗号文
暗号文
暗号文
暗号文
鍵要求
鍵要求
第2の現行鍵
第2の未来鍵
第1の現行鍵
第1の未来鍵
次回鍵更新時刻
鍵更新間隔
暗号
受領
鍵配送応答パケット
第1の現行鍵
第1の未来鍵
鍵配送要求パケット
接続装置番号
センタ装置
接続装置
平文出力部
平文入力部
復号部
暗号鍵管理部
暗号化部
暗号文受信部
暗号鍵配送応答部
暗号鍵受信部
暗号鍵配送要求部
暗号文送信部
21
16
20
15
17
19
24
23
18
22
2

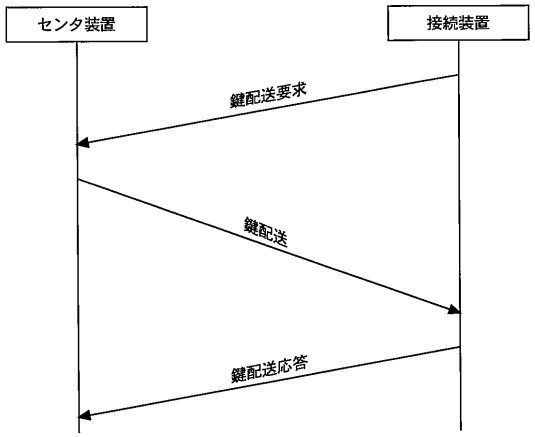
【図４】


センタ装置
S1
接続装置
S2
鍵配送用鍵の生成
鍵配送用鍵
鍵配送用鍵の受領
・書き込み
接続装置の初期化時
接続装置の運用中
定期的に鍵更新
S3
S4
鍵配送要求
タイミングのチェック
S6
S5
鍵配送要求
パケット
接続装置番号
鍵配送要求の受領待ち
鍵配送要求パケット
の生成
第1の現行鍵、第1の未来鍵
センタ時刻、次回鍵更新時刻
鍵更新間隔
ハッシュ値の算出
S7
S9
鍵等
ハッシュ前のデータと
ハッシュ値を
鍵配送用鍵で暗号化
S8
鍵等の受領
S10
鍵配送用鍵で復号
ハッシュ検証/時刻合わせ
鍵配送応答パケット生成
S12
S11
鍵配送応答受領
鍵配送完了確認
鍵配送応答
パケットを鍵配送用鍵
で暗号化

【図５】


センタ装置
(K0, K1, K2)
(1) 鍵配送要求
時刻t1
K1, K2, tK1, tI
(2)
接続装置
(K1, K2)
(3) 鍵配送応答
K1で暗号化
(4)
時刻t1～tK1
センタ装置
(K0, K1, K2)
(5) K1で暗号化
接続装置
(K1, K2)
(6) 鍵更新 時刻tK1
(7) K1で暗号化
時刻tK1～t2
センタ装置
(K1, K2, K3)
K2で暗号化
(8)
接続装置
(K1, K2)
(9) K2で暗号化
ランダムな時刻t2
tK1<T=t2<tK1+tI
(10) 鍵配送要求
センタ装置
(K1, K2, K3)
K2, K3, tK2, tI
(11)
接続装置
(K2, K3)
(12) 鍵配送応答
K2で暗号化
(13)
時刻t2～tK2
センタ装置
(K1, K2, K3)
(14) K2で暗号化
接続装置
(K2, K3)

【図６】


センタ装置
接続装置
鍵配送要求
鍵配送
鍵配送応答

フロントページの続き

(74)代理人　100148057
弁理士　久野　淑己
(72)発明者　岡本　章雄
神奈川県横浜市神奈川区新浦島町一丁目１番地３２　ＮＴＴエレクトロニクス株式会社内
(72)発明者　音川　真徳
神奈川県横浜市神奈川区新浦島町一丁目１番地３２　ＮＴＴエレクトロニクス株式会社内
(72)発明者　野尻　昌伸
神奈川県横浜市神奈川区新浦島町一丁目１番地３２　ＮＴＴエレクトロニクス株式会社内
(72)発明者　延原　隆良
大阪府大阪市北区芝田二丁目４番２４号　西日本旅客鉄道株式会社内
(72)発明者　森　崇
大阪府大阪市北区芝田二丁目４番２４号　西日本旅客鉄道株式会社内
(72)発明者　大木　啓司
大阪府大阪市北区芝田二丁目４番２４号　西日本旅客鉄道株式会社内
(72)発明者　柿元　勇樹
大阪府大阪市北区芝田二丁目４番２４号　西日本旅客鉄道株式会社内
(72)発明者　町田　雄治
大阪府大阪市中央区馬場町３番１５号　西日本電信電話株式会社内

Ｆターム(参考) 5J104 AA16　AA32　EA04　EA15　JA03　NA02　NA37