(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4688426号
(P4688426)
(45)発行日　平成23年5月25日(2011.5.25)　(24)登録日　平成23年2月25日(2011.2.25)

(51)Int.Cl.　　F I
H04L 9/16 (2006.01)　　H04L 9/00 643
H04W 84/12 (2009.01)　　H04L 12/28 310
H04W 88/08 (2009.01)　　H04Q 7/00 182
H04W 12/04 (2009.01)

請求項の数 7　(全 21 頁)

(21)出願番号　特願2004-64922(P2004-64922)
(22)出願日　平成16年3月9日(2004.3.9)
(65)公開番号　特開2005-260286(P2005-260286A)
(43)公開日　平成17年9月22日(2005.9.22)
審査請求日　平成19年2月8日(2007.2.8)

前置審査

(73)特許権者　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100092152
弁理士　服部　毅巖
(72)発明者　茅島　直史
神奈川県横浜市港北区新横浜三丁目９番１８号　富士通ネットワークテクノロジーズ株式会社内
(72)発明者　永野　裕二
神奈川県横浜市港北区新横浜三丁目９番１８号　富士通ネットワークテクノロジーズ株式会社内

最終頁に続く

(54)【発明の名称】無線通信システム

(57)【特許請求の範囲】
【請求項１】
通信データを暗号鍵で暗号化および復号化し、無線通信する無線通信システムにおいて、
複数の異なる前記暗号鍵を有する暗号鍵リストが記憶された暗号鍵記憶手段と、前記通信データを暗号化する前記暗号鍵を変更することのみを示す変更情報を定期的に無線送信する変更情報送信手段と、前記変更情報が無線送信されたとき、予め規定されている規則に従って前記暗号鍵リストから前記暗号鍵を選択する暗号鍵選択手段と、を有するアクセスポイントと、
前記暗号鍵リストと同じ端末側暗号鍵リストが記憶された端末側暗号鍵記憶手段と、前記変更情報を受信する変更情報受信手段と、前記変更情報が受信されたとき、予め規定されている前記規則と同じ規則に従って前記端末側暗号鍵リストから前記暗号鍵を選択する端末側暗号鍵選択手段と、を有する端末と、
を有することを特徴とする無線通信システム。
【請求項２】
前記アクセスポイントは、前記暗号鍵リストを更新するリスト更新手段と、更新された前記暗号鍵リストを送信するリスト送信手段と、をさらに有し、
前記端末は、更新された前記暗号鍵リストを受信するリスト受信手段と、受信された前記暗号鍵リストを前記端末側暗号鍵記憶手段に記憶するリスト記憶手段と、をさらに有することを特徴とする請求項１記載の無線通信システム。

【請求項３】
前記暗号鍵記憶手段は、２つの記憶領域を有し、
前記リスト更新手段は、現在使用されている前記暗号鍵リストが記憶されていない方の前記記憶領域に、更新した前記暗号鍵リストを記憶することを特徴とする請求項２記載の無線通信システム。
【請求項４】
前記端末側暗号鍵記憶手段は、２つの記憶領域を有し、
前記リスト記憶手段は、現在使用されている前記端末側暗号鍵リストが記憶されていない方の前記記憶領域に、受信された前記暗号鍵リストを記憶することを特徴とする請求項２記載の無線通信システム。
【請求項５】
前記アクセスポイントは、前記変更情報が送信された後、送信する前記通信データを一時的に保持する通信データ保持手段と、をさらに有し、
前記端末は、前記変更情報が受信された後、送信する前記通信データを一時的に保持する端末側通信データ保持手段と、をさらに有することを特徴とする請求項１記載の無線通信システム。
【請求項６】
前記アクセスポイントは、前記端末から前記暗号鍵の変更が終了したことを示す変更終了情報を受信した後、保持していた前記通信データを送信する通信データ保持解除手段と、をさらに有し、
前記端末は、前記変更終了情報を送信する終了情報送信手段と、前記変更終了情報が送信された後、保持していた前記通信データを送信する端末側通信データ保持解除手段と、をさらに有することを特徴とする請求項５記載の無線通信システム。
【請求項７】
前記端末は、前記変更情報を受信したことを示す応答信号を、ＭＡＣフレームのフレーム制御のタイプおよびサブタイプに格納して前記アクセスポイントに送信する応答信号送信手段と、をさらに有することを特徴とする請求項１記載の無線通信システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は無線通信システムに関し、特に通信データを暗号鍵で暗号化および復号化し、無線通信する無線通信システムに関する。
【背景技術】
【０００２】
近年、電子機器間のデータ通信は、無線ＬＡＮ（Local Area Network）によって盛んに行われるようになってきた。この無線ＬＡＮの通信システムには、無線通信機能を備えたパーソナルコンピュータなどのクライアント端末と、クライアント端末と無線通信をして、クライアント端末を有線ＬＡＮに接続するアクセスポイントとを備えたものがある。クライアント端末は、他のクライアント端末と通信をする場合には、無線によって他のクライアント端末と通信をし、有線ＬＡＮと通信する場合には、無線によってアクセスポイントを経由して有線ＬＡＮと通信をする。なお、アクセスポイント同士の接続形態は、有線ＬＡＮを介するインフラストラクチャ方式や、無線ＬＡＮを介する無線ディストリビューションシステムがある。
【０００３】
無線通信では、第三者が無線を傍受する恐れがあるため、暗号化通信を行って、データを秘匿する必要がある。無線ＬＡＮでは、暗号鍵を利用してデータを暗号化している。暗号鍵は、通信を行う者の間で共有されていなければならない。そのため、暗号鍵は、無線通信システムを構成するクライアント端末とアクセスポイントの各々の初期設定処理段階で設定され、共有される。
【０００４】

しかし、暗号化データが連続して傍受されると、傍受した暗号化データから、無線ＬＡＮの通信エリアで使用されている暗号鍵が推定される恐れがある。そこで、アクセスポイントとＬＡＮ接続された鍵管理サーバを有し、鍵管理サーバにて暗号鍵を更新すると、各アクセスポイントおよび無線端末に配送するようにした暗号鍵更新システムがある（例えば、特許文献１参照）。この暗号鍵更新システムでは、暗号鍵を更新し、セキュリティの向上を図っている。

【０００５】

また、端末とアクセスポイントに索引可能に暗号鍵を記憶し、アクセスポイントにおいて使用決定した暗号鍵の索引情報を端末に送信し、端末において索引情報に基づいた暗号鍵を使用する無線通信システムがある（例えば、特許文献２参照）。この無線通信システムでは、鍵を変更することによってセキュリティの向上を図っている。

【０００６】

また、無線通信を行う当事者間のみで秘匿性を保持した暗号用の鍵配送と認証手順とを同時に行う無線ＬＡＮシステムの認証方法がある（例えば、特許文献３参照）。この無線ＬＡＮシステムの認証方法では、認証解消後の同一アクセスポイントに対する２回目以降の認証手順を簡略化することができるようになっている。

【特許文献１】特開２００１－１１１５４３号公報（段落番号〔００３５〕～〔００４１〕、図１）

【特許文献２】特開２００３－２５８７９０号公報（段落番号〔００２２〕～〔００２４〕、図１）

【特許文献３】特開２００３－５６４１号公報（段落番号〔００３３〕～〔００３７〕、図１）

【発明の開示】

【発明が解決しようとする課題】

【０００７】

しかし、特許文献１の暗号鍵更新システムでは、有線ＬＡＮ上に鍵サーバを設置して暗号鍵を更新するため、鍵サーバを必要とする分、システム構成が大きくなるという問題点があった。

【０００８】

また、特許文献２の無線通信システムでは、使用する暗号鍵を索引するための索引情報をアクセスポイントから端末に送信するため、索引情報が傍受されると、どの暗号鍵が使用されているか第三者に知られる恐れがあるという問題点があった。

【０００９】

また、特許文献３の無線ＬＡＮシステムの認証方法では、１度認証した後は、暗号鍵を固定するため、第三者に知られる恐れがあるという問題点があった。

本発明はこのような点に鑑みてなされたものであり、システム構成を大きくすることなく、セキュリティ強度を向上した無線通信システム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】

【００１０】

本発明では上記問題を解決するために、通信データを暗号鍵で暗号化および復号化し、無線通信する無線通信システムにおいて、複数の異なる暗号鍵を有する暗号鍵リスト１ｄが記憶された暗号鍵記憶手段１ｃと、通信データを暗号化する暗号鍵を変更することのみを示す変更情報を定期的に無線送信する変更情報送信手段１ａと、変更情報が無線送信されたとき、予め規定されている規則に従って暗号鍵リスト１ｄから暗号鍵を選択する暗号鍵選択手段１ｂと、を有するアクセスポイント１と、暗号鍵リスト１ｄと同じ端末側暗号鍵リスト２ｄが記憶された端末側暗号鍵記憶手段２ｃと、変更情報を受信する変更情報受信手段２ａと、変更情報が受信されたとき、予め規定されている規則と同じ規則に従って端末側暗号鍵リスト２ｄから暗号鍵を選択する端末側暗号鍵選択手段２ｂと、を有する端末２と、を有することを特徴とする無線通信システムが提供される。

【００１１】

このような無線通信システムによれば、アクセスポイント１は、暗号鍵を変更することのみを示す変更情報を定期的に端末２に送信し、複数の暗号鍵を有する暗号鍵リスト１ｄから予め規定されている規則に従って、暗号鍵を選択する。端末２は、アクセスポイント１から変更情報を受信すると、暗号鍵リスト１ｄと同じ暗号鍵を有する端末側暗号鍵リスト２ｄから、予め規定されている暗号鍵選択手段１ｂが暗号鍵を選択する規則と同じ規則に従って、暗号鍵を選択する。

【００１２】

これにより、アクセスポイント１と端末２は、暗号鍵を変更することのみを示す変更情報によって、複数ある暗号鍵から同じ暗号鍵を選択する。また、暗号鍵リスト１ｄをアクセスポイント１に、端末側暗号鍵リスト２ｄを端末２に記憶することにより、暗号鍵を管理するためのサーバなどが不要である。

【発明の効果】

【００１３】

本発明の無線通信システムでは、アクセスポイントと端末は、暗号鍵を変更することのみを示す変更情報によって、複数ある暗号鍵から同じ暗号鍵を選択するようにした。従って、変更情報が第三者に傍受されても、変更情報は暗号鍵を変更することを示しているだけなので、どの暗号鍵が選択されるのかを知られることがなく、セキュリティを向上することができる。また、暗号鍵リストをアクセスポイントに、端末側暗号鍵リストを端末に記憶することにより、システム構成の規模を抑制することができる。

【発明を実施するための最良の形態】

【００１４】

以下、本発明の原理を図面を参照して詳細に説明する。

図１は、本発明の原理を説明する原理図である。

図に示すように無線通信システムは、アクセスポイント１と端末２から構成され、通信データを暗号鍵で暗号化および復号化し、無線通信する。アクセスポイント１は、変更情報送信手段１ａ、暗号鍵選択手段１ｂ、暗号鍵記憶手段１ｃ、および暗号鍵リスト１ｄを有している。端末２は、変更情報受信手段２ａ、端末側暗号鍵選択手段２ｂ、端末側暗号鍵記憶手段２ｃ、および端末側暗号鍵リスト２ｄを有している。

【００１５】

アクセスポイント１の変更情報送信手段１ａは、通信データを暗号化する暗号鍵を変更することを示す変更情報を、定期的に端末２に無線送信する。

暗号鍵選択手段１ｂは、変更情報送信手段１ａが変更情報を端末２に無線送信したとき、規則に従って暗号鍵リスト１ｄから暗号鍵を選択する。例えば、暗号鍵選択手段１ｂは、暗号鍵リスト１ｄの先頭から順に暗号鍵を選択する。

【００１６】

暗号鍵記憶手段１ｃは、暗号鍵リスト１ｄを記憶する。暗号鍵リスト１ｄは、複数の異なる暗号鍵を有するリストである。

端末２の変更情報受信手段２ａは、アクセスポイント１から変更情報を受信する。

【００１７】

端末側暗号鍵選択手段２ｂは、変更情報受信手段２ａにより変更情報が受信されたとき、アクセスポイント１の暗号鍵選択手段１ｂが暗号鍵を選択する規則と同じ規則に従って、端末側暗号鍵リスト２ｄから暗号鍵を選択する。上記の暗号鍵選択手段１ｂの例に従えば、端末側暗号鍵選択手段２ｂは、端末側暗号鍵リスト２ｄの先頭から順に暗号鍵を選択する。

【００１８】

端末側暗号鍵記憶手段２ｃは、端末側暗号鍵リスト２ｄを記憶する。端末側暗号鍵リスト２ｄは、アクセスポイント１の暗号鍵リスト１ｄと同じ暗号鍵を同じ配列で有するリストである。

【００１９】

以下、原理図の動作について説明する。
アクセスポイント１の変更情報送信手段１ａは、通信データを暗号化する暗号鍵を変更するとき、暗号鍵を変更することを示す変更情報を端末２に無線送信する。
【００２０】
暗号鍵選択手段１ｂは、変更情報送信手段１ａにより変更情報が送信されると、規則に従って暗号鍵を暗号鍵リスト１ｄから選択する。
一方、端末２の端末側暗号鍵選択手段２ｂは、変更情報受信手段２ａにより変更情報が受信されると、暗号鍵選択手段１ｂと同じ規則に従って端末側暗号鍵リスト２ｄから暗号鍵を選択する。端末側暗号鍵リスト２ｄは、暗号鍵リスト１ｄと同じ暗号鍵を有しているので、アクセスポイント１と同じ暗号鍵が複数の異なる暗号鍵から選択される。
【００２１】
このように、アクセスポイント１と端末２は、暗号鍵を変更することを示す変更情報によって、複数ある暗号鍵から同じ暗号鍵を選択するようにした。従って、変更情報が第三者に傍受されても、変更情報は暗号鍵を変更することを示しているだけなので、どの暗号鍵が選択されるのか知られることがなく、セキュリティを向上することができる。また、暗号鍵リスト１ｄをアクセスポイント１に、端末側暗号鍵リスト２ｄを端末２に記憶することにより、暗号鍵を管理するためのサーバなどが不要で、システム構成の規模を抑制することができる。
【００２２】
次に、本発明の実施の形態を図面を参照して詳細に説明する。
図２は、本発明の無線通信システムのシステム構成例を示す説明図である。
図に示す無線通信システムは、インフラストラクチャ方式で構成されている。アクセスポイント（以下、ＡＰ）１０とＡＰ２０は、ＬＡＮケーブル３０で接続されている。端末４０～６０は、例えば、パーソナルコンピュータであり、無線機能を有している。端末４０，５０は、ＡＰ１０と無線通信をすることができる。端末６０は、ＡＰ２０と無線通信することができる。端末４０，５０と端末６０は、ＡＰ１０，２０を介して通信することができる。
【００２３】
ＡＰ１０と端末４０，５０、ＡＰ２０と端末６０は、通信データを第三者によって解読されないよう、暗号鍵によって暗号化して無線通信する。暗号鍵は、例えば、標準仕様ＩＥＥＥ８０２．１１で定められた暗号化機能のＷＥＰ（Wired Equivalent Privacy）鍵である。
【００２４】
ＡＰ１０と端末４０，５０は、複数の異なる暗号鍵を有する暗号鍵リストを共有している。ＡＰ２０と端末６０も同様に、暗号鍵リストを共有している。ＡＰ１０，２０は、端末４０～６０に対し、使用する暗号鍵を変更する変更指示を出し、自らも使用する暗号鍵を変更する。ＡＰ１０と端末４０，５０は、暗号鍵リストの暗号鍵を変更する規則が決まっており、変更後は同一の暗号鍵を使用していることになっている。ＡＰ２０と端末６０も同様に、暗号鍵リストの暗号鍵を変更する規則が決まっており、変更後は同一の暗号鍵を使用していることになっている。
【００２５】
また、ＡＰ１０，２０は、定期的に暗号鍵リストを更新し、端末４０～６０に送信する。
図３は、暗号鍵リストの更新を説明する図である。
【００２６】
ＡＰ１０は、複数の異なる暗号鍵を有する暗号鍵リストを作成する。そして、図に示すように、作成した暗号鍵リスト７１を無線通信によって端末４０に送信する。
暗号鍵リスト７１は、ＡＰ１０と端末４０との間で公開鍵認証を行う際に送信される。また、暗号鍵リスト７１は、定期的に更新され、端末４０に送信される。
【００２７】

なお、図３では、ＡＰ１０と端末４０しか示してないが、端末５０にも同様に暗号鍵リスト７１を送信する。また、ＡＰ２０も端末６０に対して、同様に暗号鍵リストを送信する。

【００２８】

このように、複数の異なる暗号鍵を有する暗号鍵リストをＡＰと端末で共有し、ＡＰから使用する暗号鍵を変更する変更指示を出す。端末は、ＡＰから変更指示を受けて、ＡＰが暗号鍵を変更する規則と同じ規則によって暗号鍵を変更する。従って、第三者が無線通信を傍受しても、暗号鍵の変更指示があったことしか知ることができず、どの暗号鍵が使用されているか解読されるおそれがない。また、暗号鍵リストは、ＡＰによって定期的に更新される。従って、暗号鍵は、恒久的に変更されることになり、第三者は暗号鍵を推定することが困難となる。

【００２９】

次に、ＡＰ１０のハードウェアの一例について説明する。

図４は、ＡＰのハードウェア構成例を示した図である。

図に示すようにＡＰ１０は、ＣＰＵ(Central Processing Unit)１０ａによって装置全体が制御されている。ＣＰＵ１０ａには、バス１０ｉを介して、ＲＯＭ（Read Only Memory）１０ｂ、フラッシュＲＯＭ１０ｃ、ＲＡＭ（Random Access Memory）１０ｄ、回線制御デバイス１０ｅ、無線ＬＡＮ制御デバイス１０ｆ、回線Ｉ／Ｆ（Ｉ／Ｆ：インターフェース）１０ｇおよび無線Ｉ／Ｆ１０ｈが接続されている。

【００３０】

ＲＯＭ１０ｂには、ＣＰＵ１０ａに実行させるＯＳ（Operating System）のプログラムが格納されている。フラッシュＲＯＭ１０ｃには、ＡＰ２０および端末４０，５０と通信するためのアプリケーションプログラムが格納されている。

【００３１】

ＲＡＭ１０ｄには、ＯＳのプログラムおよびアプリケーションプログラムが展開される。また、ＲＡＭ１０ｄには、ＣＰＵ１０ａのＯＳのプログラムおよびアプリケーションプログラムの処理に必要な各種データが格納される。

【００３２】

回線制御デバイス１０ｅは、ＣＰＵ１０ａからの命令に従って、ＡＰ２０とのデータの送受信を制御する。無線ＬＡＮ制御デバイス１０ｆは、ＣＰＵ１０ａからの命令に従って、端末４０，５０との無線によるデータの送受信を制御する。

【００３３】

回線Ｉ／Ｆ１０ｇは、ＬＡＮケーブル３０と接続される回線インターフェースである。無線Ｉ／Ｆ１０ｈは、無線信号を送受信する無線インターフェースである。

以上のようなハードウェア構成によって、ＡＰ１０は、ＡＰ２０とＬＡＮケーブル３０を介して通信し、端末４０，５０と無線通信することができる。なお、ＡＰ２０も図４と同様のハードウェア構成を有し、その説明を省略する。

【００３４】

次に、端末４０のハードウェアの一例について説明する。

図５は、端末のハードウェア構成例を示した図である。

図に示すように端末４０は、ＣＰＵ４０ａによって装置全体が制御されている。ＣＰＵ４０ａには、バス４０ｇを介してＲＡＭ４０ｂ、ハードディスクドライブ(ＨＤＤ:Hard Disk Drive)４０ｃ、グラフィック処理装置４０ｄ、入力Ｉ／Ｆ４０ｅ、および無線通信Ｉ／Ｆ４０ｆが接続されている。

【００３５】

ＲＡＭ４０ｂには、ＣＰＵ４０ａに実行させるＯＳのプログラム、ＡＰ１０と無線通信するためのアプリケーションプログラムの少なくとも一部が一時的に格納される。また、ＲＡＭ４０ｂには、ＣＰＵ４０ａによる処理に必要な各種データが保存される。ＨＤＤ４０ｃには、ＯＳやアプリケーションプログラムなどが格納される。

【００３６】

グラフィック処理装置４０ｄには、モニタ４０ｈが接続されている。グラフィック処理装置４０ｄは、ＣＰＵ４０ａからの命令に従って、画像をモニタ４０ｈの表示画面に表示させる。

【００３７】

入力Ｉ／Ｆ４０ｅには、キーボード４０ｉが接続されている。入力Ｉ／Ｆ４０ｅは、キーボード４０ｉから送られてくる信号を、バス４０ｇを介してＣＰＵ４０ａに送信する。

無線通信Ｉ／Ｆ４０ｆは、ＣＰＵ４０ａからの命令に従って、ＡＰ１０と無線通信する無線インターフェースである。

【００３８】

以上のようなハードウェア構成によって、端末４０は、ＡＰ１０と無線通信することができる。なお、端末５０，６０も図５と同様のハードウェア構成を有し、その説明を省略する。

【００３９】

次に、ＡＰ１０の機能について説明する。なお、ＡＰ２０は、ＡＰ１０と同じ機能を有し、その説明を省略する。

図６は、ＡＰの機能ブロック図である。

【００４０】

図に示すようにＡＰ１０は、暗号鍵記憶部１１、暗号鍵リスト１２ａ，１２ｂ、タイマ部１３ａ，１３ｂ、変更情報送信部１４、暗号鍵選択部１５、リスト更新部１６、リスト送信部１７、およびデータ送受信部１８を有している。

【００４１】

暗号鍵記憶部１１は、２つの暗号鍵リスト１２ａ，１２ｂを記憶するための２つの記憶領域１１ａ，１１ｂを有している。暗号鍵記憶部１１は、例えば、図４に示したＲＡＭ１０ｄの記憶装置である。

【００４２】

暗号鍵リスト１２ａ，１２ｂは、複数の異なる暗号鍵を有するリストである。暗号鍵リスト１２ａ，１２ｂの一方は、現在、通信データの暗号化に使用されている暗号鍵を有するリストであり、他方は、現在使用されていないリストである。

【００４３】

ここで、暗号鍵リスト１２ａ，１２ｂのデータ構成例について図を用いて説明する。

図７は、暗号鍵リストのデータ構成例を示した図である。

図に示すように暗号鍵リスト１２ａは、複数の異なる暗号鍵Ａ１～Ａ６，…を有している。暗号鍵Ａ１は、リストの先頭（記憶装置のアドレスの先頭方向）に配置され、暗号鍵Ａ２～Ａ６，…は、順次リストの後方に向かって配置されている。なお、暗号鍵リスト１２ｂも図７と同様に、複数の異なる暗号鍵を有している。

【００４４】

図６の説明に戻る。

タイマ部１３ａは、設定されたタイマ時間毎に、タイマ信号を変更情報送信部１４に出力する。タイマ部１３ｂは、設定されたタイマ時間毎に、タイマ信号をリスト更新部１６に出力する。タイマ部１３ａ，１３ｂには、別々のタイマ時間が設定される。

【００４５】

変更情報送信部１４は、タイマ部１３ａからのタイマ信号を受けて、通信データを暗号化する暗号鍵を変更することを示す変更情報を端末４０，５０に無線送信する。

暗号鍵選択部１５は、変更情報送信部１４が端末４０，５０に変更情報を無線送信すると、新たな暗号鍵を、現在使用している暗号鍵リスト１２ａ，１２ｂから規則に従って選択する。暗号鍵を選択する規則は、例えば、現在使用している暗号鍵リストの先頭から暗号鍵を順次選択し、末尾の暗号鍵を選択した場合には、再び、現在使用している暗号鍵リストの先頭の暗号鍵を選択する。また、記憶領域１１ａ，１１ｂの一方に、新たな暗号鍵リストが記憶された場合は、現在使用している暗号鍵リストの末尾の暗号鍵を選択すると、次は、新たな暗号鍵リストの先頭から暗号鍵を選択する。そして、順次暗号鍵を選択し

、末尾の暗号鍵を選択した場合には、新たな暗号鍵リストの先頭の暗号鍵を選択する。

【００４６】

リスト更新部１６は、タイマ部１３ｂからのタイマ信号を受けて、現在使用されている暗号鍵リスト１２ａ，１２ｂが記憶されていない方の記憶領域１１ａ，１１ｂに、新たな暗号鍵リストを作成する。例えば、記憶領域１１ａに、現在使用されている暗号鍵リストが記憶されているとする。この場合、リスト更新部１６は、記憶領域１１ｂに、新たな暗号鍵リストを作成する。次回は、記憶領域１１ａに新たな暗号鍵リストを作成する。なお、新たに作成する暗号鍵リストの暗号鍵は、無作為に生成され、配列される。

【００４７】

リスト送信部１７は、リスト更新部１６によって作成された新たな暗号鍵リストを、無線通信によって、端末４０，５０に送信する。

データ送受信部１８は、暗号鍵選択部１５で選択された暗号鍵により、通信データを暗号化し、端末４０，５０に無線送信する。また、データ送受信部１８は、暗号鍵選択部１５で選択された暗号鍵により、端末４０，５０から受信した通信データを復号化する。

【００４８】

次に、端末４０の機能について説明する。なお、端末５０，６０は、端末４０と同じ機能を有し、その説明を省略する。

図８は、端末の機能ブロック図である。

【００４９】

図に示すように端末４０は、暗号鍵記憶部４１、暗号鍵リスト４２ａ，４２ｂ、変更情報受信部４３、暗号鍵選択部４４、リスト受信部４５、リスト記憶部４６、およびデータ送受信部４７を有している。

【００５０】

暗号鍵記憶部４１は、２つの暗号鍵リスト４２ａ，４２ｂを記憶するための２つの記憶領域４１ａ，４１ｂを有している。暗号鍵記憶部４１は、例えば、図５に示したＲＡＭ４０ｂの記憶装置である。

【００５１】

暗号鍵リスト４２ａ，４２ｂは、ＡＰ１０の記憶領域１１ａ，１１ｂに記憶されている暗号鍵リスト１２ａ，１２ｂと同じ内容を有している。すなわち、暗号鍵リスト４２ａ，４２ｂは、暗号鍵リスト１２ａ，１２ｂと同じ暗号鍵を同じ配列で有している。なお、ＡＰ１０で現在使用されている暗号鍵リスト１２ａ，１２ｂに対応する暗号鍵リスト４２ａ，４２ｂが、現在端末４０で使用されているリストとなる。

【００５２】

変更情報受信部４３は、ＡＰ１０から暗号鍵を変更することを示す変更情報を受信する。

暗号鍵選択部４４は、変更情報受信部４３がＡＰ１０から変更情報を受信すると、ＡＰ１０の暗号鍵選択部１５と同じ規則に従って、現在使用している暗号鍵リスト４２ａ，４２ｂから暗号鍵を選択する。すなわち、ＡＰ１０から変更情報が送信されると、暗号鍵選択部４４は、ＡＰ１０の暗号鍵リスト１２ａ，１２ｂと同じ内容の暗号鍵リスト４２ａ，４２ｂから、ＡＰ１０の暗号鍵選択部１５と同じ規則に従って、新たな暗号鍵を選択する。よって、ＡＰ１０で選択された暗号鍵と同じ暗号鍵が選択される。

【００５３】

リスト受信部４５は、ＡＰ１０から新たに作成された暗号鍵リストを受信する。

リスト記憶部４６は、リスト受信部４５がＡＰ１０から受信した新たな暗号鍵リストを、現在使用されている暗号鍵リストが記憶されていない方の記憶領域４１ａ，４１ｂに記憶する。これによって、記憶領域４１ａ，４１ｂには、ＡＰ１０の記憶領域１１ａ，１１ｂに格納されている暗号鍵リスト１２ａ，１２ｂと同じ内容の暗号鍵リスト４２ａ，４２ｂが記憶されることになる。

【００５４】

データ送受信部４７は、暗号鍵選択部４４で選択された暗号鍵により、通信データを暗

号化し、ＡＰ１０に無線送信する。また、データ送受信部４７は、暗号鍵選択部４４で選択された暗号鍵により、ＡＰ１０から受信した通信データを復号化する。暗号鍵選択部４４で選択された暗号鍵は、ＡＰ１０のデータ送受信部１８が使用している暗号鍵と同じになっている。これによって、ＡＰ１０と端末４０は、互いに通信データを送受信することができる。

【００５５】

ところで、端末４０は、ＡＰ１０から変更情報が送信されると、新たな暗号鍵を選択する処理に入る。このとき、ＡＰ１０が通信データを端末４０に無線送信すると、端末４０は、その通信データを受信することができない。同様に、ＡＰ１０が新たな暗号鍵を選択する処理に入ったとき、端末４０が通信データをＡＰ１０に無線送信すると、ＡＰ１０は、その通信データを受信することができない。そこで、ＡＰ１０のデータ送受信部１８と端末４０のデータ送受信部４７は、送信する通信データを、暗号鍵を選択する処理の間保持する機能を有している。

【００５６】

以下、データ送受信部１８の通信データの保持機能について説明する。

図９は、データ送受信部の詳細な機能ブロック図である。

図に示すバッファ８１は、変更情報送信部１４が端末４０，５０に暗号鍵を変更することを示す変更情報を送信し、端末４０，５０からＡＣＫ（ACKnowledgement）フレームを受信すると、端末４０，５０に送信する通信データを保持する。ＡＰ１０が端末４０，５０から暗号鍵の変更が終了したことを示す情報を受信し、端末４０，５０にＡＣＫフレームを返すと、バッファ８１は、保持していた通信データをセレクタ８２に出力する。

【００５７】

セレクタ８２は、２つの入力を有している。一方の入力には、通信データが直接入力され、他方の入力には、バッファ８１を介して通信データが入力される。セレクタ８２は、通常、直接入力される通信データを出力する。セレクタ８２は、変更情報送信部１４が暗号鍵を変更することを示す変更情報を端末４０，５０に送信し、端末４０，５０からＡＣＫフレームを受信すると、通信データの出力を停止する。ＡＰ１０が端末４０，５０から暗号鍵の変更が終了したことを示す情報を受信し、端末４０，５０にＡＣＫフレームを返すと、セレクタ８２は、バッファ８１が保持していた通信データを出力する。その後、セレクタ８２は、直接入力される通信データを出力する。

【００５８】

ＷＥＰ暗号部８３は、セレクタ８２から出力される通信データを、暗号鍵選択部１５で選択された暗号鍵で暗号化する。暗号化された通信データは、端末４０，５０に無線送信される。

【００５９】

このように、データ送受信部１８は、暗号鍵の変更処理が行われる間、通信データをバッファ８１に保持する。そして、暗号鍵の変更処理が終了した後、バッファ８１に保持していた通信データを端末４０，５０に無線送信するようにした。これにより、ＡＰ１０と端末４０，５０は、確実に通信データを送受信することができる。

【００６０】

なお、データ送受信部４７も図９と同様の機能ブロックを有し、暗号鍵の変更処理が行われる間、ＡＰ１０に送信する通信データを保持する。

次に、暗号鍵を選択する暗号鍵リストの切り替え方法（規則）について図を用いて説明する。

【００６１】

図１０は、暗号鍵リストの切り替え方法について説明する図である。

図には、暗号鍵リストＬ０，Ｌ１が示してある。暗号鍵リストＬ０は、ｎ個の異なる暗号鍵Ａ１～Ａｎを有している。暗号鍵リストＬ１は、ｎ個のことなる暗号鍵Ｂ１～Ｂｎを有している。暗号鍵リストＬ０は、現在使用されている暗号鍵リストとする。暗号鍵リストＬ１は、新たに作成された暗号鍵リストとする。

【００６２】
前述したように、新たな暗号鍵リストＬ１が作成されると、現在使用されている暗号鍵リストＬ０の末尾の暗号鍵Ａｎが選択された後は、暗号鍵リストＬ１の先頭の暗号鍵Ｂ１が選択される。
【００６３】
次に、通信データのＭＡＣフレームフォーマットについて説明する。
図１１は、通信データのＭＡＣフレームフォーマットを示した図である。
図には、通信データのＭＡＣフレームフォーマット９１と、ＭＡＣフレームフォーマット９１のフレーム制御の詳細を示したフレーム制御フォーマット９２が示してある。
【００６４】
ＭＡＣフレームフォーマット９１は、フレーム制御、デュレーション／ＩＤ、アドレス１、アドレス２、アドレス３、シーケンス制御、アドレス４、フレーム本体（ボディ）およびＦＣＳ（Frame Check Sequence）から構成されている。
【００６５】
デュレーション／ＩＤには、無線回線を使用する予定時間（μＳ）が格納される。アドレス１～アドレス４には、送信先、送信元のＭＡＣアドレスが格納される。フレーム本体には、ＭＡＣフレームのデータが格納される。シーケンス制御には、ＭＡＣフレームの順番制御をするデータが格納される。ＦＣＳには、データのエラーチェックをするためのデータが格納される。
【００６６】
フレーム制御フォーマット９２は、プロトコル・バージョン、タイプ、サブタイプ、Ｔｏ＿ＤＳ（To Distribution System）、Ｆｒｏｍ＿ＤＳ（From Distribution System）、ＭｏｒｅＦｒａｇ（More Fragment）、Ｒｅｔｅｙ、パワー管理、ＭｏｒｅＤａｔａ、ＷＥＰおよびＯｒｄｅｒから構成されている。
【００６７】
プロトコル・バージョンには、ＭＡＣフレームのプロトコルのバージョンが格納される。タイプ、サブタイプには、送受信された情報に対する応答の情報（ＡＣＫ）が格納される。Ｔｏ＿ＤＳには、受信局が基地局であるか端末であるかを示す情報が格納される。例えば、Ｔｏ＿ＤＳに１が格納されているとき、受信局が基地局であることを示す。Ｔｏ＿ＤＳに０が格納されているとき、受信局が端末であることを示す。Ｆｒｏｍ＿ＤＳには、送信局が基地局であるか端末であるかを示す情報が格納される。例えば、Ｆｒｏｍ＿ＤＳに１が格納されているとき、送信局が基地局であることを示す。Ｆｒｏｍ＿ＤＳに０が格納されているとき、送信局が端末であることを示す。ＭｏｒｅＦｒａｇには、上位レイヤのパケットを分割して送信するか否かを示す情報が格納される。Ｒｅｔｒｙには、ＭＡＣフレームが再送フレームか否かを示す情報が格納される。パワー管理には、端末の電力管理をするか否かの情報が格納される。ＭｏｒｅＤａｔａには、後続する送信待ちパケットの有無を示す情報が格納される。ＷＥＰには、ＷＥＰによる暗号化の有無を示す情報が格納される。Ｏｒｄｅｒには、ストリクトリオーダード（Strictry-Ordered）サービスクラス（順を入れ替えてはならないサービスクラス）であるか否かを示す情報が格納される。
【００６８】
ＡＰ１０と端末４０，５０との間で情報の送受信を行い、その応答としてＡＣＫを返す場合には、フレーム制御フォーマット９２のタイプのビットを０１（Ｂ２＝０、Ｂ３＝１）にし、サブタイプのビットを１１０１（Ｂ７＝１、Ｂ６＝１、Ｂ５＝０、Ｂ４＝１）にする。そして、フレーム制御フォーマット９２のタイプ、サブタイプを確認することにより、ＡＣＫが帰ってきたか否かを判断する。例えばＡＰ１０が、変更情報を端末４０，５０に送信したとする。端末４０，５０は、ＡＣＫフレームとして、フレーム制御フォーマット９２のタイプに０１、サブタイプに１１０１を格納し、ＡＰ１０に送信する。ＡＰ１０は、フレーム制御フォーマット９２のタイプ、サブタイプを確認して、変更情報の送信に対するＡＣＫフレームが帰ってきたか否かを判断する。
【００６９】

従来では、ＩＰ（Internet Protocol）フレームやＵＤＰ（User Datagram Protocol）フレームのデータにＡＣＫを示す情報を格納していた。そのため、ＡＣＫが帰ってきたか否かを判断するには、ＩＰフレームやＵＤＰフレームのデータ自体を調べなければならなかった。上記では、ＭＡＣフレームフォーマット９１のフレーム制御フォーマット９２のタイプ、サブタイプにＡＣＫを示す情報を格納することにより、ＡＣＫが帰ってきたか否かの判断が容易となる。また、ＡＣＫの判断時間を短くすることができる。

【００７０】

次に、暗号鍵リストの作成処理の流れについてシーケンス図を用いて説明する。

図１２は、暗号鍵リストの作成処理の流れを示したシーケンス図である。

ＡＰ１０と端末４０は、以下のステップに従って、暗号鍵リストの作成処理を行う。

【００７１】

ステップＳ１において、ＡＰ１０のタイマ部１３ｂは、初期化し、タイマを始動する。

ステップＳ２において、リスト更新部１６は、暗号鍵の作成時間か否かを判断する。すなわち、リスト更新部１６は、タイマ部１３ｂからタイマ信号が出力されたか否かを判断する。リスト更新部１６は、タイマ部１３ｂからタイマ信号が出力されない場合，ステップＳ２を繰り返す。タイマ部１３ｂからタイマ信号が出力された場合、ステップＳ３へ進む。

【００７２】

ステップＳ３において、リスト更新部１６は、新たな暗号鍵リストを作成する。

ステップＳ４において、ＡＰ１０は、公開鍵により、作成した新たな暗号鍵リストを暗号化する。

【００７３】

ステップＳ５において、ＡＰ１０は、暗号化した暗号鍵リストを端末４０に送信する。

ステップＳ６において、ＡＰ１０は、端末４０からＡＣＫフレームが返ってくるのを待つ。

【００７４】

ステップＳ７において、端末４０のリスト記憶部４６は、ステップＳ５でＡＰ１０から暗号鍵リストを受信したことにより、ＡＰ１０にＡＣＫフレームを送信する。

ステップＳ８において、リスト記憶部４６は、受信された暗号鍵リストを秘密鍵によって復号する。

【００７５】

ステップＳ９において、リスト記憶部４６は、受信した暗号鍵リストを、現在使用されている暗号鍵リストが記憶されていない方の記憶領域４１ａ，４１ｂに記憶する。

ステップＳ１０において、ＡＰ１０のリスト更新部１６は、ステップＳ７でのＡＣＫフレームの受信を受けて、作成した暗号鍵リストを、現在使用されている暗号鍵リストが記憶されていない方の記憶領域１１ａ，１１ｂに記憶する。

【００７６】

以上のステップを繰り返し、ＡＰ１０と端末４０は暗号鍵リストを定期的に作成し、更新していく。

次に、暗号鍵の変更処理の流れについてシーケンス図を用いて説明する。

【００７７】

図１３は、暗号鍵の変更処理の流れを示したシーケンス図である。

ＡＰ１０と端末４０は、以下のステップに従って、暗号鍵の変更処理を行う。

ステップＳ２１において、ＡＰ１０のタイマ部１３ａは、初期化し、タイマを始動する。

【００７８】

ステップＳ２２において、変更情報送信部１４は、暗号鍵の変更時間か否かを判断する。すなわち、変更情報送信部１４は、タイマ部１３ａからタイマ信号が出力されたか否かを判断する。変更情報送信部１４は、タイマ部１３ａからタイマ信号が出力されない場合、ステップＳ２２を繰り返す。タイマ部１３ａからタイマ信号が出力された場合、ステッ

プＳ２３へ進む。
【００７９】
ステップＳ２３において、変更情報送信部１４は、暗号鍵を変更することを示す変更情報を端末４０に出力する。
ステップＳ２４において、端末４０は、変更情報を受信したことを示すＡＣＫフレームをＡＰ１０に送信する。
【００８０】
ステップＳ２５において、データ送受信部１８は、通信を停止し、図９で説明したように、送信する通信データをバッファ８１に保持する。
ステップＳ２６において、暗号鍵選択部１５は、現在使用している暗号鍵が、暗号鍵リスト１２ａ，１２ｂの末尾に存在しているものか否かを判断する。暗号鍵選択部１５は、現在使用している暗号鍵が、暗号鍵リスト１２ａ，１２ｂの末尾にない暗号鍵である場合、ステップＳ２７へ進む。暗号鍵リスト１２ａ，１２ｂの末尾にある暗号鍵である場合、ステップＳ２８へ進む。
【００８１】
ステップＳ２７において、暗号鍵選択部１５は、現在使用されている暗号鍵リスト１２ａ，１２ｂの次の暗号鍵を選択する。
ステップＳ２８において、暗号鍵選択部１５は、現在使用されている暗号鍵リスト１２ａ，１２ｂが記憶されていない方の記憶領域１１ａ，１１ｂに新たな暗号鍵リストが記憶されているか否か判断する。新たな暗号鍵リストが記憶領域１１ａ，１１ｂに記憶されている場合、ステップＳ２９へ進む。新たな暗号鍵リストが記憶領域１１ａ，１１ｂに記憶されていない場合、ステップＳ３０へ進む。
【００８２】
ステップＳ２９において、暗号鍵選択部１５は、新たに作成された暗号鍵リストの先頭の暗号鍵を選択する。
ステップＳ３０において、暗号鍵選択部１５は、現在使用されている暗号鍵リストの先頭から次の暗号鍵を選択する。
【００８３】
ステップＳ３１において、データ送受信部１８は、通信データを暗号化する暗号鍵を、暗号鍵選択部１５によって選択された暗号鍵に変更する。
ステップＳ３２において、端末４０のデータ送受信部４７は、ステップＳ２４でのＡＣＫフレームの送信により、通信を停止し、図９で説明したのと同様に、送信する通信データをバッファに保持する。
【００８４】
ステップＳ３３において、暗号鍵選択部４４は、現在使用している暗号鍵が、暗号鍵リスト４２ａ，４２ｂの末尾に存在しているものか否かを判断する。暗号鍵選択部４４は、現在使用している暗号鍵が、暗号鍵リスト４２ａ，４２ｂの末尾にない暗号鍵である場合、ステップＳ３４へ進む。暗号鍵リスト４２ａ，４２ｂの末尾にある暗号鍵である場合、ステップＳ３５へ進む。
【００８５】
ステップＳ３４において、暗号鍵選択部４４は、現在使用されている暗号鍵リスト４２ａ，４２ｂの次の暗号鍵を選択する。
ステップＳ３５において、暗号鍵選択部４４は、現在使用されている暗号鍵リスト４２ａ，４２ｂが記憶されていない方の記憶領域４１ａ，４１ｂに、ＡＰ１０から受信した暗号鍵リストが記憶されているか否か判断する。ＡＰ１０から受信した暗号鍵リストが記憶領域４１ａ，４１ｂに記憶されている場合、ステップＳ３６へ進む。ＡＰ１０から受信した暗号鍵リストが記憶領域４１ａ，４１ｂに記憶されていない場合、ステップＳ３７へ進む。
【００８６】
ステップＳ３６において、暗号鍵選択部４４は、ＡＰ１０から受信された暗号鍵リスト

の先頭の暗号鍵を選択する。
ステップＳ３７において、暗号鍵選択部４４は、現在使用されている暗号鍵リストの先頭から次の暗号鍵を選択する。
【００８７】
ステップＳ３８において、データ送受信部４７は、通信データを暗号化する暗号鍵を、暗号鍵選択部４４によって選択された暗号鍵に変更する。
ステップＳ３９において、端末４０は、暗号鍵の変更処理が終了し、通信データの送受信が行えることを示す通信再開情報をＡＰ１０に送信する。
【００８８】
ステップＳ４０において、端末４０は、ＡＰ１０からＡＣＫフレームを待つ。
ステップＳ４１において、ＡＰ１０は、ステップＳ３９での端末４０からの通信再開情報を受けて、ＡＣＫフレームを端末４０に送信する。
【００８９】
ステップＳ４２において、ＡＰ１０のデータ送受信部１８は、バッファ８１に保持していた通信データを端末４０に送信し、通信を再開する。
ステップＳ４３において、端末４０のデータ送受信部４７は、ステップＳ４１でのＡＣＫフレームを受けて、バッファに保持していた通信データをＡＰ１０に送信する。
【００９０】
以上のステップを繰り返し、ＡＰ１０と端末４０は暗号鍵を変更する。
なお、図１２、図１３で示したＡＣＫフレームは、図１１で説明したように、ＭＡＣフレームフォーマット９１のフレーム制御フォーマット９２のタイプ、サブタイプに格納され、送受信される。
【００９１】
次に、ＡＰ１０の状態遷移について説明する。
図１４は、ＡＰの状態遷移を示した図である。
図に示す通信中１０１は、ＡＰ１０が端末４０と通信データを送受信している状態を示している。暗号鍵変更中１０２は、ＡＰ１０が暗号鍵の変更処理を行っている状態を示している。暗号鍵変更完了１０３は、ＡＰ１０が暗号鍵の変更処理を終了するときの状態を示している。
【００９２】
図に示すようにＡＰ１０は、通信中１０１の状態において、設定された時間毎に、新たな暗号鍵リストを作成し、端末４０，５０へ送信する。また、暗号鍵リストの作成とは別の設定された時間毎に、暗号鍵を変更することを示す変更情報を端末４０，５０に送信する。
【００９３】
ＡＰ１０は、通信中１０１の状態において、新たな暗号鍵リストを端末４０，５０に送信したことに対するＡＣＫフレームを端末４０，５０から受信すると、作成した暗号鍵リストを記憶装置に記憶する。また、ＡＰ１０は、通信中１０１の状態において、変更情報を端末４０，５０に送信したことに対するＡＣＫフレームを端末４０，５０から受信すると、暗号鍵変更中１０２の状態に遷移する。
【００９４】
ＡＰ１０は、暗号鍵変更中１０２の状態において、端末４０，５０に送信する通信データをバッファに保持する処理を行う。ＡＰ１０は、暗号鍵変更中１０２の状態において、暗号鍵の変更を完了すると、暗号鍵変更完了１０３の状態に遷移する。
【００９５】
ＡＰ１０は、暗号鍵変更完了１０３の状態において、端末４０，５０から通信再開情報を受信すると、端末４０，５０に対し、通信再開情報を受信したことを示すＡＣＫフレームを送信する。そして、ＡＰ１０は、通信中１０１の状態に遷移する。なお、ＡＰ１０は、暗号鍵変更完了１０３の状態においても、端末４０，５０に送信する通信データをバッファに保持する処理を行う。

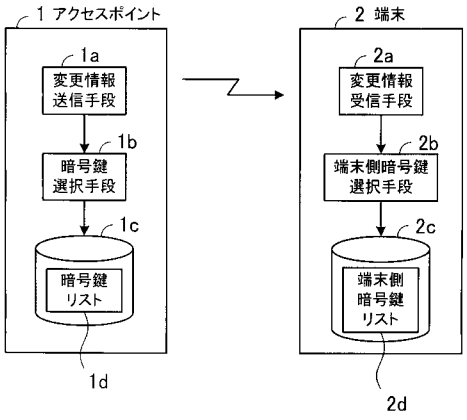
【００９６】
次に、端末４０の状態遷移について説明する。
図１５は、端末の状態遷移を示した図である。
図に示す通信中１１１は、端末４０がＡＰ１０と通信データを送受信している状態を示している。暗号鍵変更中１１２は、端末４０が暗号鍵の変更処理を行っている状態を示している。暗号鍵変更完了１１３は、端末４０が暗号鍵の変更処理を終了するときの状態を示している。
【００９７】
端末４０は、通信中１１１の状態において、新たな暗号鍵リストをＡＰ１０から受信すると、受信した暗号鍵リストを記憶装置に記憶する。また、端末４０は、通信中１１１の状態において、ＡＰ１０から変更情報を受信すると、ＡＰ１０に変更情報を受信したことを示すＡＣＫフレームを送信し、暗号鍵変更中１１２の状態に遷移する。
【００９８】
端末４０は、暗号鍵変更中１１２の状態において、ＡＰ１０に送信する通信データをバッファに保持する処理を行う。端末４０は、暗号鍵変更中１１２の状態において、暗号鍵の変更を完了すると、暗号鍵変更完了１１３の状態に遷移する。
【００９９】
端末４０は、暗号鍵変更完了１１３の状態において、ＡＰ１０に通信再開情報を送信する。そして、ＡＰ１０からＡＣＫフレームが返ってくると、端末４０は、通信中１１１の状態に遷移する。なお、端末４０は、暗号鍵変更完了１１３の状態においても、ＡＰ１０に送信する通信データをバッファに保持する処理を行う。
【０１００】
このように、アクセスポイントと端末は、暗号鍵を変更することを示す変更情報によって、複数ある暗号鍵から同じ暗号鍵を選択するようにした。変更情報は、暗号鍵を指定するためのインデックス情報とは異なり、暗号鍵を変更することを示しているだけなので、変更情報が第三者に傍受されても、どの暗号鍵が選択されるのか解読されることがなく、セキュリティを向上することができる。
【０１０１】
また、新たな暗号鍵リストを作成して更新し、暗号鍵の種類を恒久的に変更するようにした。よって、暗号鍵の解読が困難となり、セキュリティを向上することができる。特に、処理機能が向上した現在のパーソナルコンピュータ等の情報処理機器を用いても、暗号鍵を解読することは困難である。
【０１０２】
また、アクセスポイントの内部で暗号鍵リストを更新し、記憶するようにした。よって、暗号鍵を管理するサーバなどが不要で、システム構成を小規模にでき、コスト低減を図ることができる。
【０１０３】
また、暗号鍵リストを記憶するための記憶領域を２つ設け、現在使用されている暗号鍵リストの暗号鍵の変更とは非同期に、現在使用されていない記憶領域に、新たに作成した暗号鍵リストを記憶できるようにした。よって、シームレスな暗号鍵変更が可能となる。
【０１０４】
また、暗号鍵の変更中、通信データをバッファで一時的に保持し、変更終了後、バッファに一時的に保持していた通信データを送信するようにした。よって、通信データを欠損することなく確実に通信することが可能となる。
【０１０５】
さらに、変更信号の受信、暗号鍵リストの受信、および通信再開情報の受信に対する応答としてのＡＣＫフレームを、ＭＡＣフレームのフレーム制御のタイプおよびサブタイプに格納するようにした。よって、ＩＰフレームやＵＤＰフレームのデータ自体の内容を調べる必要がなく、ＡＣＫフレームの有無を容易に判断することができる。
【０１０６】

（付記１）　通信データを暗号鍵で暗号化および復号化し、無線通信する無線通信システムにおいて、
複数の異なる前記暗号鍵を有する暗号鍵リストが記憶された暗号鍵記憶手段と、前記通信データを暗号化する前記暗号鍵を変更することを示す変更情報を定期的に無線送信する変更情報送信手段と、前記変更情報が無線送信されたとき、規則に従って前記暗号鍵リストから前記暗号鍵を選択する暗号鍵選択手段と、を有するアクセスポイントと、
前記暗号鍵リストと同じ端末側暗号鍵リストが記憶された端末側暗号鍵記憶手段と、前記変更情報を受信する変更情報受信手段と、前記変更情報が受信されたとき、前記規則と同じ規則に従って前記端末側暗号鍵リストから前記暗号鍵を選択する端末側暗号鍵選択手段と、を有する端末と、
を有することを特徴とする無線通信システム。
【０１０７】
（付記２）　前記アクセスポイントは、前記暗号鍵リストを更新するリスト更新手段と、更新された前記暗号鍵リストを送信するリスト送信手段と、をさらに有し、
前記端末は、更新された前記暗号鍵リストを受信するリスト受信手段と、受信された前記暗号鍵リストを前記端末側暗号鍵記憶手段に記憶するリスト記憶手段と、をさらに有することを特徴とする付記１記載の無線通信システム。
【０１０８】
（付記３）　前記暗号鍵記憶手段は、２つの記憶領域を有し、
前記リスト更新手段は、現在使用されている前記暗号鍵リストが記憶されていない方の前記記憶領域に、更新した前記暗号鍵リストを記憶することを特徴とする付記２記載の無線通信システム。
【０１０９】
（付記４）　前記端末側暗号鍵記憶手段は、２つの記憶領域を有し、
前記リスト記憶手段は、現在使用されている前記端末側暗号鍵リストが記憶されていない方の前記記憶領域に、受信された前記暗号鍵リストを記憶することを特徴とする付記２記載の無線通信システム。
【０１１０】
（付記５）　前記アクセスポイントは、前記変更情報が送信された後、送信する前記通信データを一時的に保持する通信データ保持手段と、をさらに有し、
前記端末は、前記変更情報が受信された後、送信する前記通信データを一時的に保持する端末側通信データ保持手段と、をさらに有することを特徴とする付記１記載の無線通信システム。
【０１１１】
（付記６）　前記アクセスポイントは、前記端末から前記暗号鍵の変更が終了したことを示す変更終了情報を受信した後、保持していた前記通信データを送信する通信データ保持解除手段と、をさらに有し、
前記端末は、前記変更終了情報を送信する終了情報送信手段と、前記変更終了情報が送信された後、保持していた前記通信データを送信する端末側通信データ保持解除手段と、をさらに有することを特徴とする付記５記載の無線通信システム。
【０１１２】
（付記７）　前記端末は、前記変更情報を受信したことを示す応答信号を、ＭＡＣフレームのフレーム制御のタイプおよびサブタイプに格納して前記アクセスポイントに送信する応答信号送信手段と、をさらに有することを特徴とする付記１記載の無線通信システム。
【０１１３】
（付記８）　通信データを暗号鍵で暗号化および復号化し、無線通信するアクセスポイントにおいて、
複数の異なる前記暗号鍵を有する暗号鍵リストが記憶された暗号鍵記憶手段と、
前記通信データを暗号化する前記暗号鍵を変更することを示す変更情報を端末に定期的

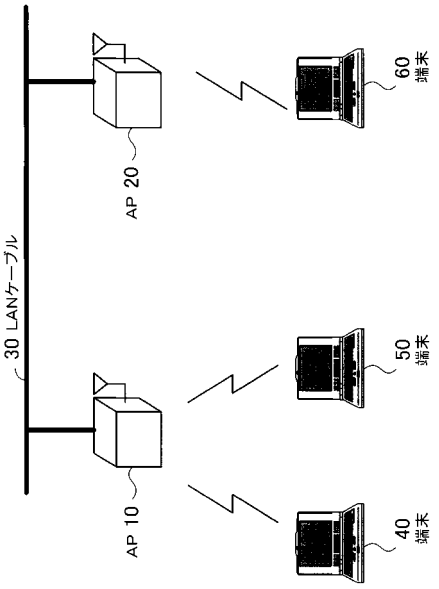
に無線送信する変更情報送信手段と、
前記変更情報が無線送信されたとき、規則に従って前記暗号鍵リストから前記暗号鍵を選択する暗号鍵選択手段と、
を有することを特徴とするアクセスポイント。
【０１１４】
（付記９）　通信データを暗号鍵で暗号化および復号化し、無線通信する端末において、
アクセスポイントが有する複数の異なる前記暗号鍵を有する暗号鍵リストと同じ端末側暗号鍵リストが記憶された端末側暗号鍵記憶手段と、
前記アクセスポイントから、前記通信データを暗号化する前記暗号鍵を変更することを示す変更情報を定期的に受信する変更情報受信手段と、
前記変更情報が受信されたとき、前記アクセスポイントが前記暗号鍵を前記暗号鍵リストから選択する規則と同じ規則に従って前記端末側暗号鍵リストから前記暗号鍵を選択する端末側暗号鍵選択手段と、
を有することを特徴とする端末。
【図面の簡単な説明】
【０１１５】
【図１】本発明の原理を説明する原理図である。
【図２】本発明の無線通信システムのシステム構成例を示す説明図である。
【図３】暗号鍵リストの更新を説明する図である。
【図４】ＡＰのハードウェア構成例を示した図である。
【図５】端末のハードウェア構成例を示した図である。
【図６】ＡＰの機能ブロック図である。
【図７】暗号鍵リストのデータ構成例を示した図である。
【図８】端末の機能ブロック図である。
【図９】データ送受信部の詳細な機能ブロック図である。
【図１０】暗号鍵リストの切り替え方法を説明する図である。
【図１１】通信データのＭＡＣフレームフォーマットを示した図である。
【図１２】暗号鍵リストの作成処理の流れを示したシーケンス図である。
【図１３】暗号鍵の変更処理の流れを示したシーケンス図である。
【図１４】ＡＰの状態遷移を示した図である。
【図１５】端末の状態遷移を示した図である。
【符号の説明】
【０１１６】
１　アクセスポイント
１ａ　変更情報送信手段
１ｂ　暗号鍵選択手段
１ｃ　暗号鍵記憶手段
１ｄ，１２ａ，１２ｂ，４２ａ，４２ｂ　暗号鍵リスト
２，４０，５０，６０　端末
２ａ　変更情報受信手段
２ｂ　端末側暗号鍵選択手段
２ｃ　端末側暗号鍵記憶手段
２ｄ　端末側暗号鍵リスト
１０，２０　ＡＰ
１１，４１　暗号鍵記憶部
１１ａ，１１ｂ，４１ａ，４１ｂ　記憶領域
１３ａ，１３ｂ　タイマ部
１４　変更情報送信部
１５，４４　暗号鍵選択部

１６　リスト更新部
１７　リスト送信部
１８，４７　データ送受信部
４３　変更情報受信部
４５　リスト受信部
４６　リスト記憶部

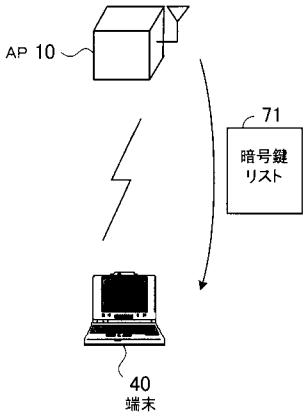
【図１】



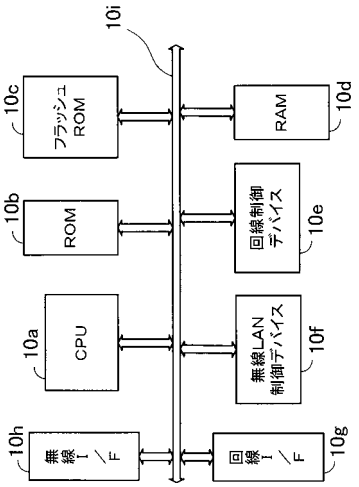
【図２】



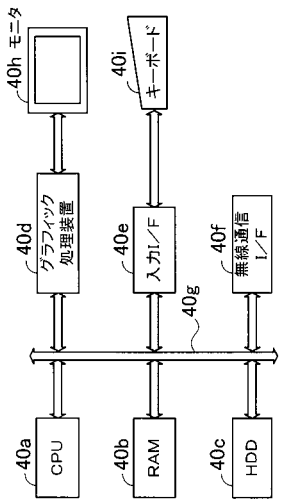
【図３】


AP 10
71
暗号鍵
リスト
40
端末

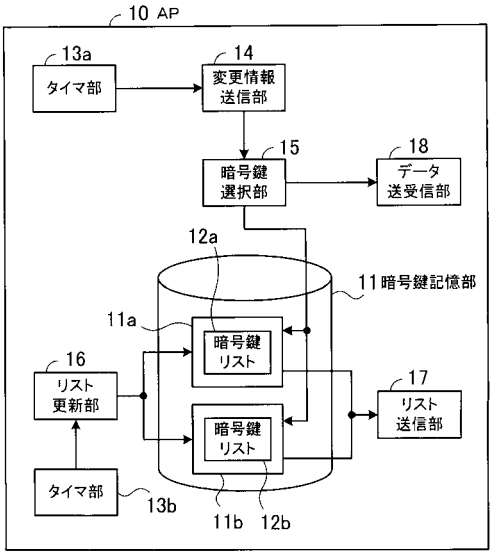
【図４】


10i
10c
フラッシュ
ROM
RAM
10d
10b
ROM
回線制御
デバイス
10e
10a
CPU
無線LAN
制御デバイス
10f
10h
無線
I/F
回線
I/F
10g

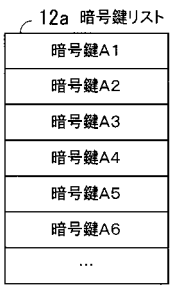
【図５】


40h モニタ
40i
キーボード
40d
グラフィック
処理装置
40e
入力I/F
40f
無線通信
I/F
40g
40a
CPU
40b
RAM
40c
HDD

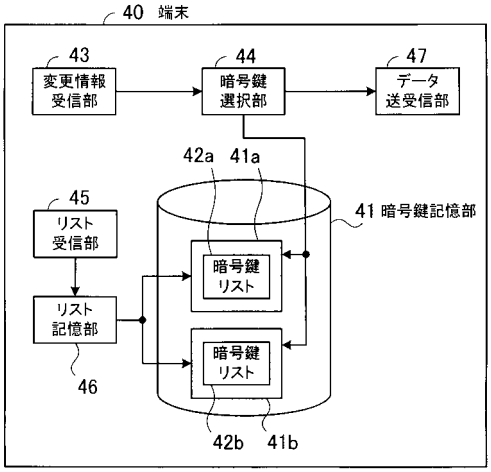
【図６】


10 AP
13a
タイマ部
14
変更情報
送信部
15
暗号鍵
選択部
18
データ
送受信部
12a
11 暗号鍵記憶部
11a
暗号鍵
リスト
16
リスト
更新部
暗号鍵
リスト
17
リスト
送信部
タイマ部
13b
11b
12b

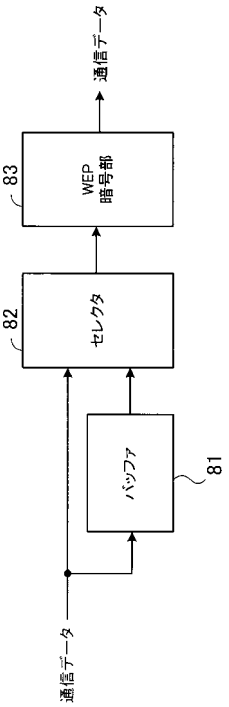
【図７】


12a 暗号鍵リスト
暗号鍵A1
暗号鍵A2
暗号鍵A3
暗号鍵A4
暗号鍵A5
暗号鍵A6
…

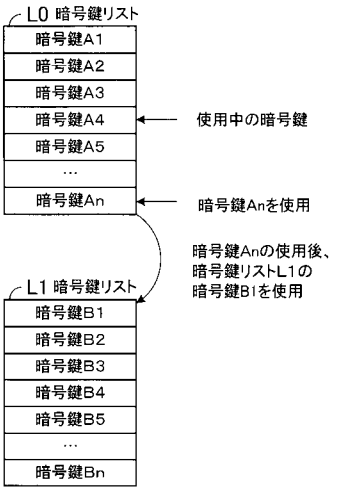
【図８】


40 端末
43
変更情報
受信部
44
暗号鍵
選択部
47
データ
送受信部
42a 41a
41 暗号鍵記憶部
45
リスト
受信部
リスト
記憶部
46
暗号鍵
リスト
暗号鍵
リスト
42b 41b

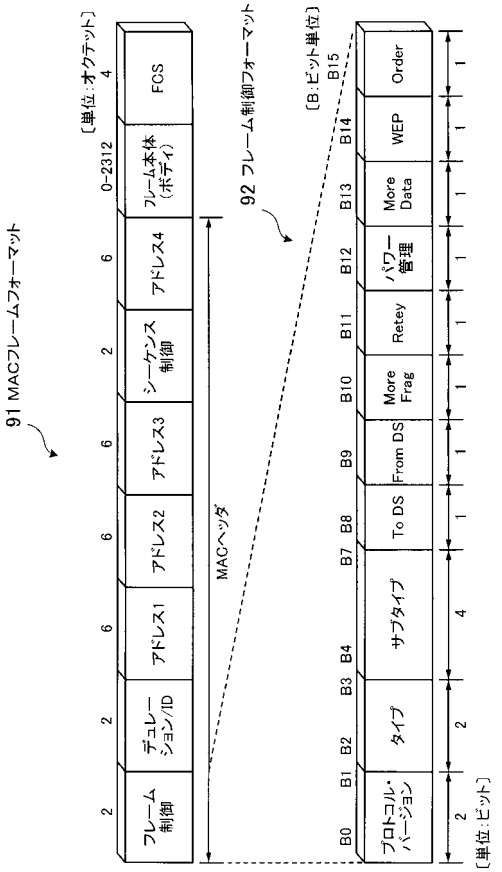
【図９】


通信データ
83
WEP
暗号部
82
セレクタ
バッファ
81
通信データ

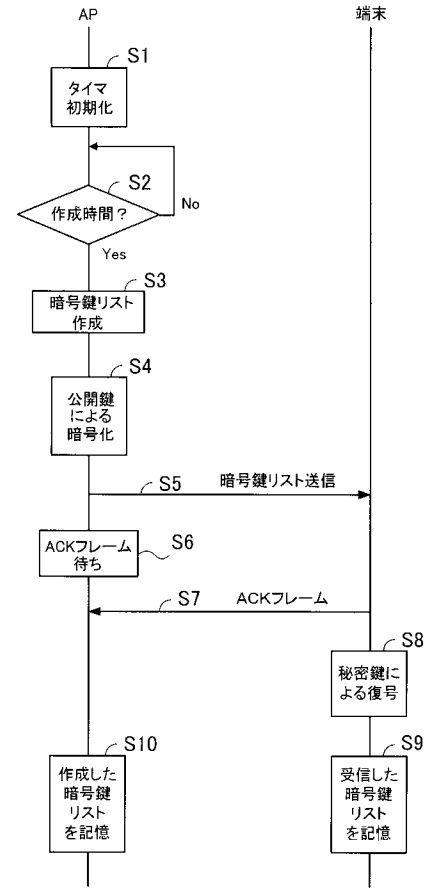
【図１０】


L0 暗号鍵リスト
暗号鍵A1
暗号鍵A2
暗号鍵A3
暗号鍵A4
暗号鍵A5
…
暗号鍵An
使用中の暗号鍵
暗号鍵Anを使用
暗号鍵Anの使用後、
暗号鍵リストL1の
暗号鍵B1を使用
L1 暗号鍵リスト
暗号鍵B1
暗号鍵B2
暗号鍵B3
暗号鍵B4
暗号鍵B5
…
暗号鍵Bn

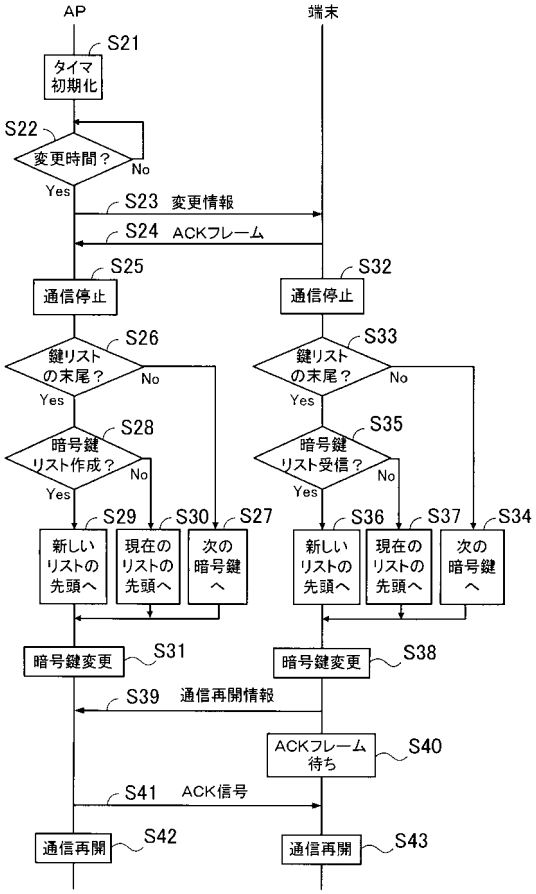
【図１１】


91 MACフレームフォーマット
92 フレーム制御フォーマット
〔単位：オクテット〕
〔B：ビット単位〕
フレーム制御
デュレーション/ID
アドレス1
アドレス2
アドレス3
シーケンス制御
アドレス4
フレーム本体（ボディ）
FCS
0-2312
MACヘッダ
プロトコル・バージョン
タイプ
サブタイプ
To DS
From DS
More Frag
Retey
パワー管理
More Data
WEP
Order
B0 B1 B2 B3 B4 B7 B8 B9 B10 B11 B12 B13 B14 B15
〔単位：ビット〕

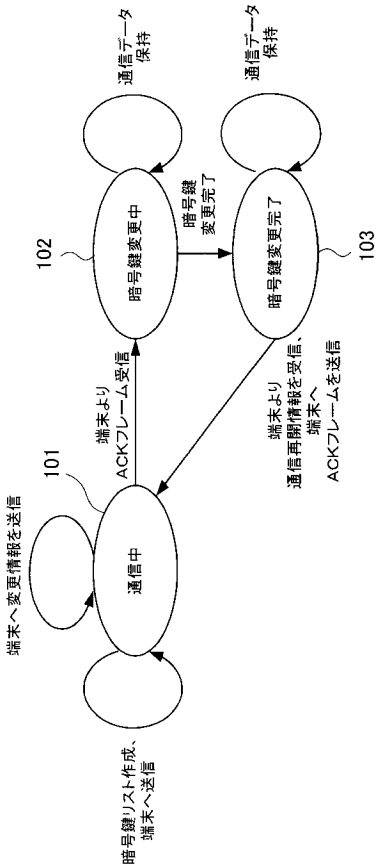
【図１２】



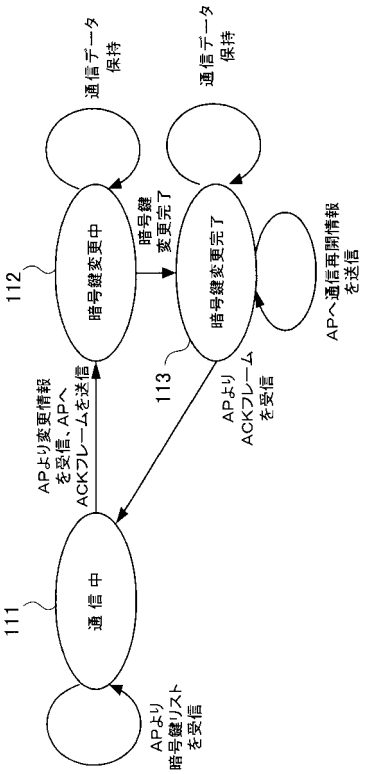
【図１３】



【図１４】



【図１５】



フロントページの続き

(72)発明者　野村　祐司
神奈川県横浜市港北区新横浜三丁目９番１８号　富士通ネットワークテクノロジーズ株式会社内

審査官　新田　亮

(56)参考文献　特開平０９－０８３５０６（ＪＰ，Ａ）
特開平１１－３３１１５１（ＪＰ，Ａ）
特開２００１－１１１５４３（ＪＰ，Ａ）
特開２００２－１１２１３３（ＪＰ，Ａ）
特開２００２－２９０３９６（ＪＰ，Ａ）
特開２００３－１０１５２８（ＪＰ，Ａ）
特開２００３－２５８７８８（ＪＰ，Ａ）
特開２００３－２５８７９０（ＪＰ，Ａ）
特開２００３－３３３０３１（ＪＰ，Ａ）
特開２００４－００７５６７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／１６
Ｈ０４Ｗ　１２／０４
Ｈ０４Ｗ　８４／１２
Ｈ０４Ｗ　８８／０８