(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4253657号
(P4253657)
(45)発行日　平成21年4月15日(2009.4.15)　(24)登録日　平成21年1月30日(2009.1.30)

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

請求項の数 12　(全 25 頁)

(21)出願番号　特願2005-513582(P2005-513582)
(86)(22)出願日　平成16年2月25日(2004.2.25)
(86)国際出願番号　PCT/JP2004/002228
(87)国際公開番号　WO2005/025126
(87)国際公開日　平成17年3月17日(2005.3.17)
審査請求日　平成17年9月14日(2005.9.14)
(31)優先権主張番号　特願2003-312156(P2003-312156)
(32)優先日　平成15年9月4日(2003.9.4)
(33)優先権主張国　日本国(JP)
(31)優先権主張番号　特願2004-533(P2004-533)
(32)優先日　平成16年1月5日(2004.1.5)
(33)優先権主張国　日本国(JP)

(73)特許権者　503027931
学校法人同志社
京都府京都市上京区今出川通烏丸東入玄武町６０１
(73)特許権者　393031586
株式会社国際電気通信基礎技術研究所
京都府相楽郡精華町光台二丁目２番地２
(74)代理人　100112715
弁理士　松山　隆夫
(72)発明者　笹岡　秀一
京都府京田辺市多々羅都谷１－３　同志社大学内
(72)発明者　青野　智之
京都府相楽郡精華町光台二丁目２番地２
株式会社国際電気通信基礎技術研究所内
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】
指向性を電気的に切換え可能な第１のアンテナ（２０）と、
第２のアンテナ（１１）と、
前記第１及び第２のアンテナ（２０，１１）を介して無線伝送路により電波を相互に送受信する第１及び第２の無線装置（３０，１０）とを備え、
前記第１の無線装置（３０）は、前記第２の無線装置における受信信号強度を複数の強度に変化させるために前記第１のアンテナ（２０）の指向性を複数個の指向性に切換えることにより前記第２の無線装置（１０）との間で伝搬する電波の成分に変化を生じさせたときに前記第２の無線装置（１０）から受信した複数の電波に基づいて前記複数の電波の強度プロファイルを示す第１の受信信号プロファイルを生成し、その生成した第１の受信信号プロファイルに基づいて第１の秘密鍵（Ｋｓ２）を生成し、
前記第２の無線装置（１０）は、前記第１の無線装置における受信信号強度を複数の強度に変化させるために前記第１のアンテナ（２０）の指向性を複数個の指向性に切換えることにより前記第１の無線装置（３０）との間で伝搬する電波の成分に変化を生じさせたときに前記第１の無線装置（３０）から受信した複数の電波に基づいて前記複数の電波の強度プロファイルを示す第２の受信信号プロファイルを生成し、その生成した第２の受信信号プロファイルに基づいて前記第１の秘密鍵（Ｋｓ２）と同じ第２の秘密鍵（Ｋｓ１）を生成する、無線通信システム。
【請求項２】

前記第１及び第２の受信信号プロファイルの各々は、前記複数個の指向性に対応した複数の強度からなり、

前記第１及び第２の無線装置（３０，１０）は、前記複数の強度を多値化してそれぞれ前記第１及び第２の秘密鍵（Ｋｓ２，Ｋｓ１）を生成する、請求の範囲第１項に記載の無線通信システム。

【請求項３】

前記第１及び第２の無線装置（３０，１０）は、時分割復信方式により前記複数の電波を送受信する、請求の範囲第１項に記載の無線通信システム。

【請求項４】

前記第１の無線装置（３０）は、前記生成した第１の秘密鍵（Ｋｓ２）が前記第２の秘密鍵（Ｋｓ１）に一致することを確認する、請求の範囲第１項に記載の無線通信システム。

【請求項５】

指向性を電気的に切換え可能な第１のアンテナ（２０）と、

第２のアンテナ（１１）と、

前記第１及び第２のアンテナ（２０，１１）を介して無線伝送路により電波を相互に送受信する第１及び第２の無線装置（３０Ａ，１０Ａ）とを備え、

前記第１の無線装置（３０Ａ）は、前記第２の無線装置における受信信号強度を複数の強度に変化させるために前記第１のアンテナ（２０）の指向性を複数個の指向性に切換えることにより前記第２の無線装置（１０Ａ）との間で伝搬する電波の成分に変化を生じさせたときに前記第２の無線装置（１０Ａ）が所定の通信プロトコルに従って送信した複数のデータに対応する複数の電波を受信し、その受信した複数の電波に基づいて前記複数の電波の強度プロファイルを示す第１の受信信号プロファイルを生成し、その生成した第１の受信信号プロファイルに基づいて第１の秘密鍵（Ｋｓ２）を生成し、

前記第２の無線装置（１０Ａ）は、前記第１の無線装置における受信信号強度を複数の強度に変化させるために前記第１のアンテナ（２０）の指向性を複数個の指向性に切換えることにより前記第１の無線装置（３０Ａ）との間で伝搬する電波の成分に変化を生じさせたときに前記第１の無線装置（３０Ａ）が前記所定の通信プロトコルに従って送信した複数のデータに対応する複数の電波を受信し、その受信した複数の電波に基づいて前記複数の電波の強度プロファイルを示す第２の受信信号プロファイルを生成し、その生成した第２の受信信号プロファイルに基づいて前記第１の秘密鍵（Ｋｓ２）と同じ第２の秘密鍵（Ｋｓ１）を生成する、無線通信システム。

【請求項６】

前記第１の無線装置（３０Ａ）は、前記第１のアンテナ（２０）が無指向性に制御されたときに前記第２の無線装置（１０Ａ）との間で前記無線伝送路を確立し、前記無線伝送路が確立した後、前記第１のアンテナ（２０）の指向性を前記複数個に変えながら前記第２の無線装置（１０Ａ）との間で前記複数のデータを送受信する、請求の範囲第５項に記載の無線通信システム。

【請求項７】

前記第１の無線装置（３０Ａ）は、前記第２の無線装置（１０Ａ）との間における前記各データの送受信において、前記第１のアンテナ（２０）の指向性を更新して前記第２の無線装置（１０Ａ）から前記データを受信し、前記更新した前記第１のアンテナ（２０）の指向性を維持して前記受信したデータを前記第２の無線装置（１０Ａ）へ送信する、請求の範囲第６項に記載の無線通信システム。

【請求項８】

前記所定の通信プロトコルは、複数の階層からなり、

前記複数のデータは、前記複数の階層のうち、前記データを前記電気信号に変換する階層におけるデータフォーマットに含まれ、

前記データを前記電気信号に変換する階層は、複数の通信プロトコルに共通な階層である、請求の範囲第６項に記載の無線通信システム。

【請求項９】
前記複数のデータの各々は、前記第１および第２の無線装置（３０Ａ，１０Ａ）により受信された電波の強度を検出する区間と、前記第１のアンテナ（２０）の指向性を変更する区間とからなる、請求の範囲第５項に記載の無線通信システム。
【請求項１０】
前記第１の無線装置（３０，３０Ａ）は、前記生成した第１の秘密鍵（Ｋｓ２）が前記第２の秘密鍵（Ｋｓ１）に不一致であるとき、前記第１の秘密鍵（Ｋｓ２）を前記第２の秘密鍵（Ｋｓ１）に一致させる、請求の範囲第１項から請求の範囲第９項のいずれか１項に記載の無線通信システム。
【請求項１１】
前記第１のアンテナ（２０）は、盗聴者の端末（５０）に近接して配置された第１の無線装置（３０，３０Ａ）に設置される、請求の範囲第１項から請求の範囲第９項のいずれか１項に記載の無線通信システム。
【請求項１２】
前記第１及び第２の無線装置（３０，３０Ａ，１０，１０Ａ）は、前記第１及び第２の秘密鍵（Ｋｓ２，Ｋｓ１）を用いてデータを暗号及び復号して相互に通信する、請求の範囲第１項から請求の範囲第９項のいずれか１項に記載の無線通信システム。
【発明の詳細な説明】
【技術分野】
この発明は、無線通信システムに関し、特に、暗号化した情報を無線により通信する無線通信システムに関するものである。
【背景技術】
最近、情報化社会の発展に伴い情報通信が益々重要になるとともに、情報の盗聴または不正利用がより深刻な問題となっている。このような情報の盗聴を防止するために従来から情報を暗号化して送信することが行なわれている。
情報を暗号化して端末間で通信を行なう方式として公開鍵暗号方式と秘密鍵暗号方式とがある。公開鍵暗号方式は、安全性が高いが、大容量のデータの暗号化には向かない。
一方、秘密鍵暗号方式は、処理が比較的簡単であり、大容量のデータの高速暗号化も可能であるが、秘密鍵を通信の相手方に送信する必要がある。また、秘密鍵暗号方式は、同一の秘密鍵を使用し続けると、暗号解読の攻撃を受けやすく、安全性が損なわれる可能性がある。
そこで、秘密鍵を相手方に送信せずに秘密鍵を共有する方法として、２つの端末間の伝送路の特性を測定し、その測定した特性に基づいて各端末で秘密鍵を生成する方法が提案されている（堀池　元樹、笹岡　秀一，「陸上移動通信路の不規則変動に基づく秘密鍵共有方式」，信学技報，社団法人　電子情報通信学会，２００２年１０月，ＴＥＣＨＮＩＣＡＬ　ＲＥＰＯＲＴ　ＯＦ　ＩＥＩＣＥ　ＲＣＳ２００２－１７３，ｐ．７－１２）。
この方法は、２つの端末間でデータを送受信したときの遅延プロファイルを各端末で測定し、その測定した遅延プロファイルをアナログ信号からデジタル信号に変換して各端末で秘密鍵を生成する方法である。即ち、伝送路を伝搬する電波は可逆性を示すために、一方の端末から他方の端末へデータを送信したときの遅延プロファイルは、他方の端末から一方の端末へ同じデータを送信したときの遅延プロファイルと同じになる。従って、一方の端末で測定した遅延プロファイルに基づいて生成された秘密鍵は、他方の端末で測定した遅延プロファイルに基づいて作成された秘密鍵と同じになる。
このように、伝送路特性を用いて秘密鍵を生成する方法は、同じデータを２つの端末間で相互に送信するだけで同じ秘密鍵を共有することができる。
しかし、２つの端末間で送信されるデータを盗聴者が各端末の近傍で傍受して遅延プロファイルを測定すれば、盗聴者は、各端末で測定した遅延プロファイルに近い遅延プロファイルを取得することができる。その結果、秘密鍵が解読される可能性がある。
それゆえに、この発明の目的は、秘密鍵の盗聴を抑制可能な無線通信システムを提供することである。

【発明の開示】

この発明によれば、無線通信システムは、第１及び第２のアンテナと、第１及び第２の無線装置とを備える。第１のアンテナは、指向性を電気的に切換え可能である。第１及び第２の無線装置は、第１及び第２のアンテナを介して無線伝送路により電波を相互に送受信する。そして、第１の無線装置は、第１のアンテナの指向性が所定のパターンにより複数個に変えられたときに第２の無線装置から受信した複数の電波に基づいて複数の電波の強度プロファイルを示す第１の受信信号プロファイルを生成し、その生成した第１の受信信号プロファイルに基づいて第１の秘密鍵を生成する。また、第２の無線装置は、第１のアンテナの指向性が所定のパターンにより複数個に変えられたときに第１の無線装置から受信した複数の電波に基づいて複数の電波の強度プロファイルを示す第２の受信信号プロファイルを生成し、その生成した第２の受信信号プロファイルに基づいて第１の秘密鍵と同じ第２の秘密鍵を生成する。

好ましくは、第１及び第２の受信信号プロファイルの各々は、複数個の指向性に対応した複数の強度からなる。第１及び第２の無線装置は、複数の強度を多値化してそれぞれ第１及び第２の秘密鍵を生成する。

好ましくは、第１及び第２の無線装置は、時分割復信方式により複数の電波を送受信する。

好ましくは、第１の無線装置は、生成した第１の秘密鍵が第２の秘密鍵に一致することを確認する。

また、この発明によれば、無線通信システムは、第１および第２のアンテナと、第１および第２の無線装置とを備える。第１のアンテナは、指向性を電気的に切換え可能なアンテナである。第１および第２の無線装置は、第１及び第２のアンテナを介して無線伝送路により電波を相互に送受信する。そして、第１の無線装置は、第１のアンテナの指向性が所定のパターンにより複数個に変えられたときに第２の無線装置が所定の通信プロトコルに従って送信した複数のデータに対応する複数の電波を受信し、その受信した複数の電波に基づいて複数の電波の強度プロファイルを示す第１の受信信号プロファイルを生成し、その生成した第１の受信信号プロファイルに基づいて第１の秘密鍵を生成する。また、第２の無線装置は、第１のアンテナの指向性が所定のパターンにより複数個に変えられたときに第１の無線装置が所定の通信プロトコルに従って送信した複数のデータに対応する複数の電波を受信し、その受信した複数の電波に基づいて複数の電波の強度プロファイルを示す第２の受信信号プロファイルを生成し、その生成した第２の受信信号プロファイルに基づいて第１の秘密鍵と同じ第２の秘密鍵を生成する。

好ましくは、第１の無線装置は、第１のアンテナが無指向性に制御されたときに第２の無線装置との間で無線伝送路を確立し、無線伝送路が確立した後、第１のアンテナの指向性を複数個に変えながら第２の無線装置との間で複数のデータを送受信する。

好ましくは、第１の無線装置は、第２の無線装置との間における各データの送受信において、第１のアンテナの指向性を更新して第２の無線装置からデータを受信し、更新した第１のアンテナの指向性を維持して受信したデータを第２の無線装置へ送信する。

好ましくは、所定の通信プロトコルは、複数の階層からなる。複数のデータは、複数の階層のうち、データを電気信号に変換する階層におけるデータフォーマットに含まれる。そして、データを電気信号に変換する階層は、複数の通信プロトコルに共通な階層である。

好ましくは、複数のデータの各々は、第１および第２の無線装置により受信された電波の強度を検出する区間と、第１のアンテナの指向性を変更する区間とからなる。

好ましくは、第１の無線装置は、生成した第１の秘密鍵が第２の秘密鍵に不一致であるとき、第１の秘密鍵を第２の秘密鍵に一致させる。

好ましくは、第１のアンテナは、盗聴者の端末に近接して配置された第１の無線装置に設置される。

好ましくは、第１及び第２の無線装置は、第１及び第２の秘密鍵を用いてデータを暗号及び復号して相互に通信する。

この発明による無線通信システムにおいては、指向性を電気的に切換え可能な第１のアンテナを介して２つの無線装置間で所定のデータが送受信される。そして、第１のアンテナの指向性を複数個に変えたときに検出される複数の電波の強度プロファイルを示す受信信号プロファイルが２つの無線装置において生成され、その生成された各受信信号プロファイルに基づいて２つの無線装置において秘密鍵が作成される。この場合、各無線装置において生成される受信信号プロファイルは、２つの無線装置間に形成される伝送路に固有である。即ち、２つの無線装置間で送受信される複数の電波を傍受して受信信号プロファイルを生成しても、その生成した受信信号プロファイルは、２つの端末装置で生成される受信信号プロファイルと異なる。

従って、この発明によれば、２つの無線装置において作成される秘密鍵の盗聴を抑制できる。

また、この発明による無線通信システムにおいては、指向性を電気的に切換え可能なアンテナを介して２つの無線装置間で所定のデータが所定の通信プロトコルに従って送受信される。そして、このアンテナの指向性を複数個に変えたときに検出される複数の電波の強度プロファイルを示す受信信号プロファイルが２つの無線装置において生成され、その生成された各受信信号プロファイルに基づいて２つの無線装置において秘密鍵が作成される。この場合、各無線装置において生成される受信信号プロファイルは、２つの無線装置間に形成される伝送路に固有である。即ち、２つの無線装置間で送受信される複数の電波を傍受して受信信号プロファイルを生成しても、その生成した受信信号プロファイルは、２つの端末装置で生成される受信信号プロファイルと異なる。

従って、この発明によれば、２つの無線装置において作成される秘密鍵の盗聴を抑制できる。また、２つの無線装置において作成される秘密鍵を生成するためのデータを所定の通信プロトコルに従って送受信できる。

【図面の簡単な説明】

図１は、この発明の実施の形態１による無線通信システムの概略図である。

図２は、図１に示す一方の無線装置の概略ブロック図である。

図３は、図１に示す他方の無線装置の概略ブロック図である。

図４は、図３に示す指向性設定部の概略ブロック図である。

図５は、図２及び図３に示す鍵一致確認部の概略ブロック図である。

図６は、図２及び図３に示す鍵一致化部の概略ブロック図である。

図７は、受信信号プロファイルＲＳＳＩの概念図である。

図８は、図１に示す２つの無線装置間で通信を行なう動作を説明するためのフローチャートである。

図９は、実施の形態２による無線通信システムの概略図である。

図１０は、図９に示す一方の無線装置の内部構成を示す概略ブロック図である。

図１１は、図９に示す他方の無線装置の内部構成を示す概略ブロック図である。

図１２は、図１１に示す指向性設定部の機能ブロック図である。

図１３は、所定の通信プロトコルであるＩＥＥＥ８０２．１１ｂ（またはＩＥＥＥ８０２．１１ｇ）の物理層およびＭＡＣ層のフォーマットを示す図である。

図１４は、２つの無線装置間でデータを送受信する通常の方法の概念図である。

図１５は、２つの無線装置間におけるデータの再送の概念図である。

図１６は、実施の形態２において、２つの無線装置間でデータを送受信する方法の概念図である。

図１７は、図９に示す２つの無線装置間で通信を行なう動作を説明するためのフローチャートである。

【発明を実施するための最良の形態】

本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

［実施の形態１］

図１は、この発明の実施の形態１による無線通信システムの概略図である。無線通信シ

ステム１００は、無線装置１０，３０と、アンテナ１１と、アレーアンテナ２０とを備える。無線装置１０は、例えば、ユーザの移動体通信端末である。また、無線装置３０は、例えば、無線アクセスポイントである。

アンテナ１１は、無線装置１０に装着される。そして、アンテナ１１は、全方位性のアンテナである。アレーアンテナ２０は、アンテナ素子２１～２７を備える。アンテナ素子２４は、給電素子であり、アンテナ素子２１～２３，２５～２７は、無給電素子である。そして、アンテナ素子２４は、アンテナ素子２１～２３，２５～２７によって取り囲まれている。無給電素子であるアンテナ素子２１～２３，２５～２７に装荷された可変容量素子であるバラクタダイオードに印加する直流電圧を制御することにより、アレーアンテナ２０は、適応ビーム形成が可能である。

即ち、アレーアンテナ２０は、無線装置３０に含まれるバラクタダイオード（図示せず）に印加する直流電圧を変えることによって指向性が変えられる。従って、アレーアンテナ２０は、電気的に指向性を切換え可能なアンテナである。そして、アレーアンテナ２０は、無線装置３０に装着される。

無線装置１０と無線装置３０との間で通信が行われる場合、電波は、無線装置１０のアンテナ１１と無線装置３０のアレーアンテナ２０との間を直接伝搬したり、中間物４０による影響を受けて伝搬する。中間物４０としては、反射物及び障害物が想定される。中間物４０が反射物である場合、無線装置１０のアンテナ１１または無線装置３０のアレーアンテナ２０から出射した電波は、中間物４０によって反射されて無線装置３０のアレーアンテナ２０または無線装置１０のアンテナ１１へ伝搬する。また、中間物４０が障害物である場合、無線装置１０のアンテナ１１または無線装置３０のアレーアンテナ２０から出射した電波は、中間物４０によって回折されて無線装置３０のアレーアンテナ２０または無線装置１０のアンテナ１１へ伝搬する。

このように、電波は、無線装置１０のアンテナ１１と無線装置３０のアレーアンテナ２０との間を直接伝搬したり、中間物４０による反射を受けて反射波として伝搬したり、中間物４０による回折を受けて回折波として伝搬したりする。そして、電波は、無線装置１０のアンテナ１１または無線装置３０のアレーアンテナ２０から無線装置３０のアレーアンテナ２０または無線装置１０のアンテナ１１へ伝搬する場合、直接伝搬成分、反射波成分及び回折波成分が混在しており、無線装置１０のアンテナ１１または無線装置３０のアレーアンテナ２０から無線装置３０のアレーアンテナ２０または無線装置１０のアンテナ１１へ伝搬した電波がどのような成分により構成されるかによって無線装置１０と無線装置３０との間の伝送路の特性が決定される。

この発明においては、無線装置１０と無線装置３０との間で通信が行なわれる場合、アレーアンテナ２０の指向性を複数個に変えて時分割復信（ＴＤＤ：Ｔｉｍｅ　Ｄｉｖｉｓｉｏｎ　Ｄｕｐｌｅｘ）等の同一周波数で送受信する方式で所定のデータが無線装置１０，３０間で送受信される。そして、無線装置１０，３０は、アレーアンテナ２０の指向性を複数個に変えたときの複数の電波の強度を示す受信信号プロファイルＲＳＳＩを生成し、その生成した受信信号プロファイルＲＳＳＩに基づいて秘密鍵を作成する。

秘密鍵が無線装置１０，３０において生成されると、無線装置１０，３０は、生成した秘密鍵により情報を暗号化して相手方へ送信し、相手方から受信した暗号化情報を復号して情報を取得する。

図２は、図１に示す一方の無線装置１０の概略ブロック図である。無線装置１０は、信号発生部１１０と、送信処理部１２０と、アンテナ部１３０と、受信処理部１４０と、プロファイル生成部１５０と、鍵作成部１６０と、鍵一致確認部１７０と、鍵記憶部１８０と、鍵一致化部１９０と、暗号部２００と、復号部２１０とを含む。

信号発生部１１０は、秘密鍵を生成するときに無線装置３０へ送信するための所定の信号を生成し、その生成した所定の信号を送信処理部１２０へ出力する。送信処理部１２０は、変調、周波数変換、多元接続及び送信信号の増幅等の送信系の処理を行なう。アンテナ部１３０は、図１に示すアンテナ１１からなり、送信処理部１２０からの信号を無線装置３０へ送信し、無線装置３０からの信号を受信して受信処理部１４０またはプロファイ

ル生成部１５０へ供給する。
受信処理部１４０は、受信信号の増幅、多元接続、周波数変換及び復調等の受信系の処理を行なう。そして、受信処理部１４０は、受信処理を行なった信号を必要に応じて鍵一致確認部１７０、鍵一致化部１９０及び復号部２１０へ出力する。
プロファイル生成部１５０は、アレーアンテナ２０の指向性を複数個に変えたときの複数の電波をアンテナ部１３０から順次受け、その受けた複数の電波の強度を検出する。そして、プロファイル生成部１５０は、検出した複数の強度からなる受信信号プロファイルＲＳＳＩを生成して鍵作成部１６０へ出力する。
鍵作成部１６０は、プロファイル生成部１５０からの受信信号プロファイルＲＳＳＩに基づいて秘密鍵Ｋｓ１を作成する。そして、鍵作成部１６０は、作成した秘密鍵Ｋｓ１を鍵一致確認部１７０及び鍵一致化部１９０へ出力する。
鍵一致確認部１７０は、所定の信号を送信処理部１２０、アンテナ部１３０及び受信処理部１４０を介して無線装置３０と送受信し、鍵作成部１６０によって作成された秘密鍵Ｋｓ１が無線装置３０において作成された秘密鍵Ｋｓ２に一致するか否かを後述する方法によって確認する。そして、鍵一致確認部１７０は、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に一致すると確認したとき、秘密鍵Ｋｓ１を鍵記憶部１８０に記憶する。また、鍵一致確認部１７０は、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に不一致であることを確認したとき、不一致信号ＮＭＴＨを生成して鍵一致化部１９０へ出力する。
鍵記憶部１８０は、鍵一致確認部１７０及び鍵一致化部１９０からの秘密鍵Ｋｓ１を記憶する。また、鍵記憶部１８０は、記憶した秘密鍵Ｋｓ１を暗号部２００及び復号部２１０へ出力する。なお、鍵記憶部１８０は、秘密鍵Ｋｓ１を一時的、例えば、無線装置３０との通信の間だけ記憶するようにしてもよい。
鍵一致化部１９０は、鍵一致確認部１７０から不一致信号ＮＭＴＨを受けると、後述する方法によって秘密鍵Ｋｓ１を秘密鍵Ｋｓ２に一致させる。そして、鍵一致化部１９０は、一致させた秘密鍵が秘密鍵Ｋｓ２に一致することを鍵一致確認部１７０における方法と同じ方法によって確認する。
暗号部２００は、送信データを鍵記憶部１８０に記憶された秘密鍵Ｋｓ１によって暗号して送信処理部１２０へ出力する。復号部２１０は、受信処理部１４０からの信号を鍵記憶部１８０からの秘密Ｋｓ１によって復号して受信データを生成する。
図３は、図１に示す他方の無線装置３０の概略ブロック図である。無線装置３０は、無線装置１０のアンテナ部１３０をアンテナ部２２０に代え、指向性設定部２３０を追加したものであり、その他は、無線装置１０と同じである。
アンテナ部２２０は、図１に示すアレーアンテナ２０からなる。そして、アンテナ部２２０は、送信処理部１２０からの信号を指向性設定部２３０によって設定された指向性で無線装置１０へ送信し、無線装置１０からの信号を指向性設定部２３０によって設定された指向性で受信して受信処理部１４０またはプロファイル生成部１５０へ出力する。
指向性設定部２３０は、アンテナ部２２０の指向性を設定する。また、指向性設定部２３０は、無線装置１０，３０において秘密鍵Ｋｓ１，Ｋｓ２を生成するとき、後述する方法により所定の順序に従ってアンテナ部２２０の指向性を順次切換える。
なお、無線装置３０のプロファイル生成部１５０は、アレーアンテナ２０の指向性を複数個に変えたときの複数の電波をアンテナ部２２０から順次受け、その受けた複数の電波の強度を検出する。そして、プロファイル生成部１５０は、検出した複数の強度からなる受信信号プロファイルＲＳＳＩを生成して鍵作成部１６０へ出力する。
図４は、図３に示す指向性設定部２３０の概略ブロック図である。指向性設定部２３０は、制御電圧発生回路２３１と、バラクタダイオード２３２とを含む。制御電圧発生回路２３１は、制御電圧セットＣＬＶ１～ＣＬＶｎ（ｎは自然数）を順次発生し、その発生した制御電圧セットＣＬＶ１～ＣＬＶｎをバラクタダイオード２３２へ順次出力する。バラクタダイオード２３２は、制御電圧セットＣＬＶ１～ＣＬＶｎに応じて無給電素子であるアンテナ素子２１～２３，２５～２７に装荷される容量を変え、アレーアンテナ２０の指向性を複数個に順次変える。

図５は、図２及び図３に示す鍵一致確認部１７０の概略ブロック図である。鍵一致確認部１７０は、データ発生部１７１と、データ比較部１７２と、結果処理部１７３とを含む。なお、無線装置１０，３０の鍵一致確認部１７０は、同じ構成からなるが、図５においては、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に一致することを確認する動作を説明するために、無線装置３０においてはデータ発生部１７１のみを示す。

データ発生部１７１は、鍵作成部１６０から秘密鍵Ｋｓ１を受けると、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に一致することを確認するための鍵確認用データＤＣＦＭ１を発生し、その発生した鍵確認用データＤＣＦＭ１を送信処理部１２０及びデータ比較部１７２へ出力する。

この場合、データ発生部１７１は、秘密鍵Ｋｓ１から非可逆的な演算及び一方向的な演算等により、鍵確認用データＤＣＦＭ１を発生する。より具体的には、データ発生部１７１は、秘密鍵Ｋｓ１またはＫｓ２のハッシュ値を演算することにより、鍵確認用データＤＣＦＭ１を発生する。

データ比較部１７２は、データ発生部１７１から鍵確認用データＤＣＦＭ１を受け、無線装置３０のデータ発生部１７１で発生された鍵確認用データＤＣＦＭ２を受信処理部１４０から受ける。そして、データ比較部１７２は、鍵確認用データＤＣＦＭ１を鍵確認用データＤＣＦＭ２と比較する。データ比較部１７２は、鍵確認用データＤＣＦＭ１が鍵確認用データＤＣＦＭ２に一致するとき、一致信号ＭＴＨを生成して結果処理部１７３へ出力する。

また、データ比較部１７２は、鍵確認用データＤＣＦＭ１が鍵確認用データＤＣＦＭ２に不一致であるとき、不一致信号ＮＭＴＨを生成する。そして、データ比較部１７２は、不一致信号ＮＭＴＨを鍵一致化部１９０へ出力し、不一致信号ＮＭＴＨを送信処理部１２０及びアンテナ部１３０を介して無線装置３０へ送信する。

結果処理部１７３は、データ比較部１７２から一致信号ＭＴＨを受けると、鍵作成部１６０から受けた秘密鍵Ｋｓ１を鍵記憶部１８０へ記憶する。

図６は、図２及び図３に示す鍵一致化部１９０の概略ブロック図である。鍵一致化部１９０は、擬似シンドローム作成部１９１と、不一致ビット検出部１９２と、鍵不一致訂正部１９３と、データ発生部１９４と、データ比較部１９５と、結果処理部１９６とを含む。

なお、無線装置１０，３０の鍵一致化部１９０は、同じ構成からなるが、図６においては、秘密鍵Ｋｓ１を秘密鍵Ｋｓ２に一致させる動作を説明するために、無線装置３０においては擬似シンドローム作成部１９１のみを示す。

擬似シンドローム作成部１９１は、鍵一致確認部１７０のデータ比較部１７２から不一致信号ＮＭＴＨを受けると、鍵作成部１６０から受けた秘密鍵Ｋｓ１のシンドロームx_1を演算する。より具体的には、擬似シンドローム作成部１９１は、秘密鍵Ｋｓ１のビットパターンx_1を検出し、ビットパターンx_1に対して検査行列Ｈを乗算してシンドローム$s1 = x_1 H^T$を演算する。そして、擬似シンドローム作成部１９１は、ビットパターンx_1を鍵不一致訂正部１９３へ出力し、演算したシンドローム$s1 = x_1 H^T$を不一致ビット検出部１９２へ出力する。

なお、これらの演算は、ｍｏｄ２の演算であり、H^Tは、検査行列Ｈの転置行列である。

不一致ビット検出部１９２は、擬似シンドローム作成部１９１からシンドロームｓ１を受け、無線装置３０の擬似シンドローム作成部１９１によって演算されたシンドローム$s2 = x_2 H^T$を受信処理部１４０から受ける。そして、不一致ビット検出部１９２は、シンドロームｓ１とシンドロームｓ２との差分ｓ＝ｓ１－ｓ２を演算する。

なお、秘密鍵Ｋｓ１，Ｋｓ２のビットパターンの差分（鍵不一致のビットパターン）を$e = x_1 - x_2$とすると、$s = eH^T$の関係が成立する。ｓ＝０の場合、ｅ＝０となり、秘密鍵Ｋｓ１のビットパターンは、秘密鍵Ｋｓ２のビットパターンに一致する。

不一致ビット検出部１９２は、演算した差分ｓが０でないとき（即ち、$e \neq 0$のとき）、鍵不一致のビットパターンｅを鍵不一致訂正部１９３へ出力する。

鍵不一致訂正部１９３は、擬似シンドローム作成部１９１からビットパターンx_1を受け、不一致ビット検出部１９２から鍵不一致のビットパターンｅを受ける。そして、鍵不一致訂正部１９３は、ビットパターンx_1から鍵不一致のビットパターンｅを減算することにより相手方の秘密鍵のビットパターン$x_2 = x_1 - e$を演算する。

このように、鍵一致化部１９０は、秘密鍵Ｋｓ１，Ｋｓ２の不一致を誤りと見なして誤り訂正の応用により秘密鍵Ｋｓ１，Ｋｓ２の不一致を解消する。

この秘密鍵を一致させる方法は、鍵不一致のビット数が誤り訂正能力以上である場合に鍵の一致化に失敗する可能性があるので、鍵一致化の動作を行なった後に鍵一致の確認を行なう必要がある。

データ発生部１９４は、一致化後の鍵$x_2 = x_1 - e$を鍵不一致訂正部１９３から受けると、鍵x_2に基づいて鍵確認用データＤＣＦＭ３を発生させ、その発生させた鍵確認用データＤＣＦＭ３をデータ比較部１９５へ出力する。また、データ発生部１９４は、発生させた鍵確認用データＤＣＦＭ３を送信処理部１２０及びアンテナ部１３０を介して無線装置３０へ送信する。

なお、データ発生部１９４は、鍵一致確認部１７０のデータ発生部１７１による鍵確認用データＤＣＦＭ１の発生方法と同じ方法により鍵確認用データＤＣＦＭ３を発生する。

データ比較部１９５は、データ発生部１９４から鍵確認用データＤＣＦＭ３を受け、無線装置３０で発生された鍵確認用データＤＣＦＭ４を受信処理部１４０から受ける。そして、データ比較部１９５は、鍵確認用データＤＣＦＭ３を鍵確認用データＤＣＦＭ４と比較する。

データ比較部１９５は、鍵確認用データＤＣＦＭ３が鍵確認用データＤＣＦＭ４に一致するとき、一致信号ＭＴＨを生成して結果処理部１９６へ出力する。

また、データ比較部１９５は、鍵確認用データＤＣＦＭ３が鍵確認用データＤＣＦＭ４に不一致であるとき、不一致信号ＮＭＴＨを生成する。そして、データ比較部１９５は、不一致信号ＮＭＴＨを送信処理部１２０及びアンテナ部１３０を介して無線装置３０へ送信する。

結果処理部１９６は、データ比較部１９５から一致信号ＭＴＨを受けると、鍵不一致訂正部１９３から受けた鍵$x_2 = x_1 - e$を鍵記憶部１８０へ記憶する。

このように、データ発生部１９４、データ比較部１９５及び結果処理部１９６は、鍵一致確認部１７０における確認方法と同じ方法によって一致化が施された鍵の一致を確認する。

図７は、受信信号プロファイルＲＳＳＩの概念図である。指向性設定部２３０の制御電圧発生回路２３１は、各々が電圧Ｖ１～Ｖ６からなる制御電圧セットＣＬＶ１～ＣＬＶｎを順次発生してバラクタダイオード２３２へ出力する。この場合、電圧Ｖ１～Ｖ６は、それぞれ、アンテナ素子２１～２３，２５～２７に装荷される容量を変えるための電圧であり、０～２０Ｖの範囲で変えられる。

バラクタダイオード２３２は、パターンＰ１からなる制御電圧セットＣＬＶ１に応じてアレーアンテナ２０の指向性をある１つの指向性に設定する。そして、アレーアンテナ２０は、設定された指向性で無線装置１０からの電波を受信してプロファイル生成部１５０へ供給する。プロファイル生成部１５０は、アレーアンテナ２０（アンテナ部２２０）から受けた電波の強度ＷＩ１を検出する。

次に、バラクタダイオード２３２は、パターンＰ２からなる制御電圧セットＣＬＶ２に応じてアレーアンテナ２０の指向性を別の指向性に設定する。そして、アレーアンテナ２０は、設定された指向性で無線装置１０からの電波を受信してプロファイル生成部１５０へ供給する。プロファイル生成部１５０は、アレーアンテナ２０（アンテナ部２２０）から受けた電波の強度ＷＩ２を検出する。

以後、同様にして、バラクタダイオード２３２は、それぞれ、パターンＰ３～Ｐｎからなる制御電圧セットＣＬＶ３～ＣＬＶｎに応じてアレーアンテナ２０の指向性を順次変える。そして、アレーアンテナ２０は、各々設定された指向性で無線装置１０からの電波を受信してプロファイル生成部１５０へ供給する。プロファイル生成部１５０は、アレーア

ンテナ２０（アンテナ部２２０）から受けた電波の強度ＷＩ３～ＷＩｎを順次検出する。
そして、プロファイル生成部１５０は、強度ＷＩ１～ＷＩｎからなる強度プロファイルを示す受信信号プロファイルＲＳＳＩを生成して鍵作成部１６０へ出力する。
パターンＰ１～Ｐｎによってアレーアンテナ２０の指向性を複数個に順次切換えて無線装置３０から無線装置１０へデータを送信したとき、無線装置１０のプロファイル生成部１５０が受信信号プロファイルＲＳＳＩを生成する。
鍵作成部１６０は、プロファイル生成部１５０から受信信号プロファイルＲＳＳＩを受け、受信信号プロファイルＲＳＳＩから最大強度ＷＩｍａｘ（＝ＷＩ６）を検出する。そして、鍵作成部１６０は、最大強度ＷＩｍａｘ（＝ＷＩ６）によって受信信号プロファイルＲＳＳＩを規格化し、各強度ＷＩ１～ＷＩｎを多値化する。鍵作成部１６０は、多値化した各値を検出し、その検出した各値をビットパターンとする秘密鍵Ｋｓ１またはＫｓ２を作成する。
図８は、図１に示す２つの無線装置１０，３０間で通信を行なう動作を説明するためのフローチャートである。一連の動作が開始されると、無線装置３０の送信処理部１２０は、ｋ＝１を設定する（ステップＳ１）。そして、指向性設定部２３０は、パターンＰ１によりアレーアンテナ２０の指向性を１つの指向性に設定する（ステップＳ２）。
その後、無線装置１０の信号発生部１１０は、所定の信号を発生して送信処理部１２０へ出力する。送信処理部１２０は、所定の信号に変調等の処理を施し、アンテナ１１を介して無線装置３０へ所定の信号を構成する電波を送信する（ステップＳ３）。
無線装置３０において、アレーアンテナ２０は、無線装置１０からの電波を受信し、その受信した電波をプロファイル生成部１５０へ出力する。プロファイル生成部１５０は、アレーアンテナ２０から受けた電波の強度Ｉ１ｋを検出する（ステップＳ４）。
その後、無線装置３０の信号発生部１１０は、所定の信号を発生して送信処理部１２０へ出力する。送信処理部１２０は、所定の信号に変調等の処理を施し、アレーアンテナ２０を介して無線装置１０へ所定の信号を構成する電波を送信する（ステップＳ５）。
無線装置１０において、アンテナ１１は、無線装置３０からの電波を受信し、その受信した電波をプロファイル生成部１５０へ出力する。プロファイル生成部１５０は、アンテナ１１から受けた電波の強度Ｉ２ｋを検出する（ステップＳ６）。
その後、無線装置３０の送信処理部１２０は、ｋ＝ｋ＋１を設定し（ステップＳ７）、ｋ＝ｎであるか否かを判定する（ステップＳ８）。そして、ｋ＝ｎでないとき、ステップＳ２～Ｓ８が繰返し実行される。即ち、アレーアンテナ２０の指向性がパターンＰ１～Ｐｎによってｎ個に変えられて、無線装置１０のアンテナ１１と無線装置３０のアレーアンテナ２０との間で所定の信号を構成する電波が送受信され、強度Ｉ１１～Ｉ１ｎ及びＩ２１～Ｉ２ｎが検出されるまで、ステップＳ２～Ｓ８が繰返し実行される。
ステップＳ８において、ｋ＝ｎであると判定されると、無線装置３０において、プロファイル生成部１５０は、強度Ｉ１１～Ｉ１ｎから受信信号プロファイルＲＳＳＩ１を作成して鍵作成部１６０へ出力する。
鍵作成部１６０は、受信信号プロファイルＲＳＳＩ１から最大強度ＷＩｍａｘ１を検出し、その検出した最大強度ＷＩｍａｘ１によって受信信号プロファイルＲＳＳＩ１を規格化し、強度Ｉ１１～Ｉ１ｎを多値化する。そして、鍵作成部１６０は、多値化した各値をビットパターンとする秘密鍵Ｋｓ２を生成する（ステップＳ９）。
また、無線装置１０のプロファイル生成部１５０は、強度Ｉ２１～Ｉ２ｎから受信信号プロファイルＲＳＳＩ２を作成して鍵作成部１６０へ出力する。鍵作成部１６０は、受信信号プロファイルＲＳＳＩ２から最大強度ＷＩｍａｘ２を検出し、その検出した最大強度ＷＩｍａｘ２によって受信信号プロファイルＲＳＳＩ２を規格化し、強度Ｉ２１～Ｉ２ｎを多値化する。そして、鍵作成部１６０は、多値化した各値をビットパターンとする秘密鍵Ｋｓ１を生成する（ステップＳ１０）。
その後、無線装置１０において、鍵作成部１６０は、秘密鍵Ｋｓ１を鍵一致確認部１７０へ出力する。鍵一致確認部１７０のデータ発生部１７１は、上述した方法によって鍵確認用データＤＣＦＭ１を発生して送信処理部１２０及びデータ比較部１７２へ出力する。

送信処理部１２０は、鍵確認用データＤＣＦＭ１に変調等の処理を施し、アンテナ部１３０を介して無線装置３０へ鍵確認用データＤＣＦＭ１を送信する。

そして、アンテナ部１３０は、無線装置３０において発生された鍵確認用データＤＣＦＭ２を無線装置３０から受信し、その受信した鍵確認用データＤＣＦＭ２を受信処理部１４０へ出力する。受信処理部１４０は、鍵確認用データＤＣＦＭ２に所定の処理を施し、鍵一致確認部１７０のデータ比較部１７２へ鍵確認用データＤＣＦＭ２を出力する。

データ比較部１７２は、データ発生部１７１からの鍵確認用データＤＣＦＭ１を受信処理部１４０からの鍵確認用データＤＣＦＭ２と比較する。そして、データ比較部１７２は、鍵確認用データＤＣＦＭ１が鍵確認用データＤＣＦＭ２に一致しているとき、一致信号ＭＴＨを生成して結果処理部１７３へ出力する。結果処理部１７３は、一致信号ＭＴＨに応じて、鍵作成部１６０からの秘密鍵Ｋｓ１を鍵記憶部１８０に記憶する。

一方、鍵確認用データＤＣＦＭ１が鍵確認用データＤＣＦＭ２に不一致であるとき、データ比較部１７２は、不一致信号ＮＭＴＨを生成して送信処理部１２０及び鍵一致化部１９０へ出力する。送信処理部１２０は、不一致信号ＮＭＴＨをアンテナ部１３０を介して無線装置３０へ送信する。そして、無線装置３０は、無線装置１０において秘密鍵Ｋｓ１，Ｋｓ２の不一致が確認されたことを検知する。

これにより、無線装置１０における鍵一致の確認が終了する（ステップＳ１１）。

なお、無線装置１０における鍵一致確認に代えて、無線装置３０において鍵一致確認をしてもよい（ステップＳ１２）。

ステップＳ１１において、秘密鍵Ｋｓ１，Ｋｓ２の不一致が確認されたとき、無線装置１０において、鍵一致化部１９０の擬似シンドローム作成部１９１は、鍵一致確認部１７０から不一致信号ＮＭＴＨを受ける。そして、擬似シンドローム作成部１９１は、不一致信号ＮＭＴＨに応じて、鍵作成部１６０から受けた秘密鍵Ｋｓ１のビットパターンx_1を検出し、その検出したビットパターンx_1のシンドローム$s1 = x_1 H^T$を演算する。

擬似シンドローム作成部１９１は、演算したシンドローム$s1 = x_1 H^T$を不一致ビット検出部１９２へ出力し、ビットパターンx_1を鍵不一致訂正部１９３へ出力する。

一方、無線装置３０は、ステップＳ１１において無線装置１０から不一致信号ＮＭＴＨを受信し、その受信した不一致信号ＮＭＴＨに応じて、シンドローム$s2 = x_2 H^T$を演算して無線装置１０へ送信する。

無線装置１０のアンテナ部１３０は、無線装置３０からシンドローム$s2 = x_2 H^T$を受信して受信処理部１４０へ出力する。受信処理部１４０は、シンドローム$s2 = x_2 H^T$に対して所定の処理を施し、シンドローム$s2 = x_2 H^T$を鍵一致化部１９０へ出力する。

鍵一致化部１９０の不一致ビット検出部１９２は、受信処理部１４０から無線装置３０において作成されたシンドローム$s2 = x_2 H^T$を受ける。そして、不一致ビット検出部１９２は、無線装置１０で作成されたシンドローム$s1 = x_1 H^T$と無線装置３０において作成されたシンドローム$s2 = x_2 H^T$との差分$s = s1 - s2$を演算する。

その後、不一致ビット検出部１９２は、$s \neq 0$であることを確認し、鍵不一致のビットパターン$e = x_1 - x_2$を$s = e H^T$に基づいて演算し、その演算した鍵不一致のビットパターンｅを鍵不一致訂正部１９３へ出力する。

鍵不一致訂正部１９３は、擬似シンドローム作成部１９１からのビットパターンx_1と、不一致ビット検出部１９２からの鍵不一致のビットパターンｅとに基づいて、無線装置３０において作成された秘密鍵Ｋｓ２のビットパターン$x_2 = x_1 - e$を演算する。

そして、データ発生部１９４、データ比較部１９５及び結果処理部１９６は、鍵一致確認部１７０における鍵一致確認の動作と同じ動作によって、一致化された鍵$x_2 = x_1 - e$の一致を確認する。

これにより、鍵不一致対策が終了する（ステップＳ１３）。

なお、無線装置１０における鍵不一致対策に代えて、無線装置３０において鍵不一致対策をしてもよい（ステップＳ１４）。

ステップＳ１１において、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に一致することが確認されたと

き、またはステップＳ１３において鍵不一致対策がなされたとき、暗号部２００は、鍵記憶部１８０から秘密鍵Ｋｓ１を読出して送信データを暗号化し、暗号化した送信データを送信処理部１２０へ出力する。そして、送信処理部１２０は、暗号化された送信データに変調等を施し、アンテナ部１３０を介して暗号化された送信データを無線装置３０へ送信する。

また、アンテナ部１３０は、暗号化された送信データを無線装置３０から受信し、その受信した暗号化された送信データを受信処理部１４０へ出力する。受信処理部１４０は、暗号化された送信データに所定の処理を施し、暗号化された送信データを復号部２１０へ出力する。

復号部２１０は、受信処理部１４０からの暗号化された送信データを復号して受信データを取得する。

これにより、秘密鍵Ｋｓ１による暗号・復号が終了する（ステップＳ１５）。

無線装置３０においても、無線装置１０と同じ動作によって秘密鍵Ｋｓ２による暗号・復号が行なわれる（ステップＳ１６）。そして、一連の動作が終了する。

上述したステップＳ３，Ｓ４に示す動作は、無線装置３０において受信信号プロファイルＲＳＳＩ１を生成するための電波を無線装置１０のアンテナ１１から無線装置３０のアレーアンテナ２０へ送信し、かつ、無線装置３０において電波の強度Ｉ１ｋを検出する動作であり、ステップＳ５，Ｓ６に示す動作は、無線装置１０において受信信号プロファイルＲＳＳＩ２を生成するための電波を無線装置３０アレーアンテナ２０から無線装置１０のアンテナ１１へ送信し、かつ、無線装置１０において電波の強度Ｉ２ｋを検出する動作である。そして、所定の信号を構成する電波の無線装置１０のアンテナ１１から無線装置３０のアレーアンテナ２０への送信及び所定の信号を構成する電波の無線装置３０のアレーアンテナ２０から無線装置１０のアンテナ１１への送信は、アレーアンテナ２０の指向性を１つの指向性に設定して交互に行なわれる。つまり、所定の信号を構成する電波は、無線装置１０のアンテナ１１と無線装置３０のアレーアンテナ２０との間で時分割復信（ＴＤＤ）等の同一周波数で送受信する方式により送受信される。

従って、アレーアンテナ２０の指向性を１つの指向性に設定して無線装置１０のアンテナ１１から無線装置３０のアレーアンテナ２０へ所定の信号を構成する電波を送信し、無線装置３０において電波の強度Ｉ１ｋを検出した直後に、同じ所定の信号を構成する電波を無線装置３０のアレーアンテナ２０から無線装置１０のアンテナ１１へ送信し、無線装置１０において電波の強度Ｉ２ｋを検出することができる。その結果、無線装置１０，３０間において同じ伝送路特性を確保して所定の信号を構成する電波を無線装置１０，３０間で送受信でき、電波の可逆性により電波の強度Ｉ１１～Ｉ１ｎをそれぞれ電波の強度Ｉ２１～Ｉ２ｎに一致させることができる。そして、無線装置１０において作成される秘密鍵Ｋｓ１を無線装置３０において作成される秘密鍵Ｋｓ２に容易に一致させることができる。

また、所定の信号を構成する電波は、無線装置１０，３０間で時分割復信（ＴＤＤ）等の同一周波数で送受信する方式により送受信されるので、電波の干渉を抑制して１つのアレーアンテナ２０を介して所定の信号を構成する電波を無線装置１０，３０間で送受信できる。

更に、アレーアンテナ２０の指向性を１つの指向性に設定して無線装置１０，３０間で所定の信号を構成する電波を送受信し、秘密鍵Ｋｓ１，Ｋｓ２を作成するための受信信号プロファイルＲＳＳＩ１，ＲＳＳＩ２を生成するので、図１に示すようにアレーアンテナ２０を装着した無線装置３０の近傍に盗聴装置５０が配置されていても、盗聴装置５０による秘密鍵Ｋｓ１，Ｋｓ２の盗聴を抑制できる。

即ち、盗聴装置５０は、アンテナ１１及びアレーアンテナ２０から送信された電波をアンテナ５１を介して受信するが、アレーアンテナ２０は指向性を各指向性に設定して電波を送受信するので、アンテナ１１とアレーアンテナ２０との間で送受信される電波は、アンテナ１１またはアレーアンテナ２０とアンテナ５１との間で送受信される電波と異なり、盗聴装置５０は、無線装置３０が送受信する電波と同じ電波を送受信できず、電波の強

度Ｉ１ｋと同じ強度を得ることができない。その結果、盗聴装置５０は、秘密鍵Ｋｓ１，Ｋｓ２を盗聴することができない。

従って、この発明においては、電気的に指向性を切換え可能なアレーアンテナ２０を盗聴装置５０の近傍に配置された無線装置３０に装着することを特徴とする。

更に、鍵確認用データＤＣＦＭ１～４は、秘密鍵Ｋｓ１，Ｋｓ２に非可逆的な演算、または一方向的な演算を施して発生されるので、鍵確認用データＤＣＦＭ１～４が盗聴されても秘密鍵Ｋｓ１，Ｋｓ２が解読される危険性を極めて低くできる。

更に、シンドロームｓ１，ｓ２は、秘密鍵Ｋｓ１，Ｋｓ２のビットパターンを示す鍵x_1，x_2に検査行列Ｈの転置行列H^Tを乗算して得られるので、シンドロームｓ１，ｓ２が盗聴されても直ちに情報のビットパターンが推測されることは特殊な符号化を想定しない限り起こらない。従って、盗聴を抑制して秘密鍵を一致させることができる。

なお、無線装置１０，３０間で通信を行なう動作は、実際には、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）によって行なわれ、無線装置１０に搭載されたＣＰＵは、図８に示す各ステップＳ３，Ｓ６，Ｓ１０，Ｓ１１，Ｓ１３，Ｓ１５を備えるプログラムをＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）から読出し、無線装置３０に搭載されたＣＰＵは、図８に示す各ステップＳ１，Ｓ２，Ｓ４，Ｓ５，Ｓ７，Ｓ８，Ｓ９，Ｓ１２，Ｓ１４，Ｓ１６を備えるプログラムをＲＯＭから読出し、無線装置１０，３０に搭載された２つのＣＰＵは、その読出したプログラムを実行して図８に示すフローチャートに従って無線装置１０，３０間で通信を行なう。

従って、ＲＯＭは、無線装置１０，３０間で通信を行なう動作をコンピュータ（ＣＰＵ）に実行させるためのプログラムを記録したコンピュータ（ＣＰＵ）読取り可能な記録媒体に相当する。

そして、図８に示す各ステップを備えるプログラムは、アレーアンテナ２０の指向性を複数個に順次変えて受信した複数の電波に基づいて、無線装置１０，３０間における通信をコンピュータ（ＣＰＵ）に実行させるプログラムである。

上記においては、電気的に指向性を切換え可能なアレーアンテナ２０を無線装置３０のみに装着すると説明したが、この発明においては、アレーアンテナ２０は、無線装置１０及び３０の両方に装着されてもよい。

即ち、この発明においては、アレーアンテナ２０は、２つの無線装置１０，３０のうち、少なくとも一方の無線装置に装着されていればよい。そして、アレーアンテナ２０を装着した無線装置は、好ましくは、盗聴装置５０の近傍に配置される。

また、この発明においては、秘密鍵Ｋｓ１，Ｋｓ２の鍵長は、無線装置１０，３０間の通信環境に応じて決定されてもよい。即ち、無線装置１０，３０間の通信環境が盗聴し易い環境であるとき、秘密鍵Ｋｓ１，Ｋｓ２の鍵長を相対的に長くし、無線装置１０，３０間の通信環境が盗聴しにくい環境であるとき、秘密鍵Ｋｓ１，Ｋｓ２の鍵長を相対的に短くする。

更に、定期的に秘密鍵Ｋｓ１，Ｋｓ２の鍵長を変えるようにしてもよい。

更に、無線装置１０，３０間で送受信する情報の機密性に応じて秘密鍵Ｋｓ１、Ｋｓ２の鍵長を変えるようにしてもよい。即ち、情報の機密性が高いとき秘密鍵Ｋｓ１，Ｋｓ２の鍵長を相対的に長くし、情報の機密性が低いとき秘密鍵Ｋｓ１，Ｋｓ２の鍵長を相対的に短くする。

そして、この鍵長は、アレーアンテナ２０の指向性を変化させる個数、即ち、制御電圧セットＣＬＶ１～ＣＬＶｎの個数により制御される。秘密鍵Ｋｓ１，Ｋｓ２は、検出された電波の強度Ｉ１１～Ｉ１ｎ，Ｉ２１～Ｉ２ｎの個数からなるビットパターンを有し、電波の強度Ｉ１１～Ｉ１ｎ，Ｉ２１～Ｉ２ｎの個数は、アレーアンテナ２０の指向性を変化させる個数に等しいからである。つまり、制御電圧セットＣＬＶ１～ＣＬＶｎの個数により秘密鍵Ｋｓ１，Ｋｓ２の鍵長を制御できる。

このように、この発明においては、秘密鍵Ｋｓ１，Ｋｓ２の鍵長は、電気的に指向性を切換え可能なアレーアンテナ２０の指向性を変化させる個数によって決定される。

更に、上記においては、２つの無線装置間において秘密鍵を生成する場合、即ち、１つ

の無線装置が１つの無線装置と通信する場合について説明したが、この発明は、これに限らず、１つの無線装置が複数の無線装置と通信する場合についても適用される。この場合、１つの無線装置は、通信の相手毎にアレーアンテナ２０の指向性の切換パターンを変えて秘密鍵を生成する。１つの無線装置は、アレーアンテナ２０の指向性の切換パターンを１つに固定して複数の無線装置との間で秘密鍵を生成することも可能であるが（複数の無線装置の設置場所によって１つの無線装置との伝送路が異なるので、通信の相手毎に異なる秘密鍵を生成できる）、盗聴を効果的に抑制するには、通信の相手毎にアレーアンテナ２０の指向性の切換パターンを変えて秘密鍵を生成するのが好ましい。

［実施の形態２］

図９は、実施の形態２による無線通信システムの概略図である。無線通信システム２００は、図１に示す無線通信システム１００の無線装置１０，３０をそれぞれ無線装置１０Ａ，３０Ａに代えたものであり、その他は、無線通信システム１００と同じである。

無線装置１０Ａには、アンテナ１１が装着され、無線装置３０Ａには、アレーアンテナ２０が装着される。無線装置１０Ａは、無線ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）のプロトコルであるＩＥＥＥ８０２．１１ｂまたはＩＥＥＥ８０２．１１ｇに従って無線装置３０Ａとの間で通信を行なう。

図１０は、図９に示す一方の無線装置１０Ａの内部構成を示す概略ブロック図である。無線装置１０Ａは、無線装置１０の信号発生部１０を信号発生部１１０Ａに代えたものであり、その他は、無線装置１０と同じである。

信号発生部１１０Ａは、秘密鍵を生成するときに無線装置３０Ａへ送信するための所定の信号を生成し、その生成した所定の信号を送信処理部１２０へ出力する。送信処理部１２０は、暗号部２００から暗号化データを受けると、その受けた暗号化データに対して変調、周波数変換および増幅等を施してアンテナ部１３０から送信する。

なお、実施の形態２においては、送信処理部１２０は、信号発生部１１０Ａから所定の信号を受けると、所定の信号を所定の通信プロトコルであるＩＥＥＥ８０２．１１ｂ（またはＩＥＥＥ８０２．１１ｇ）の物理層を構成するデータフォーマットに含め、変調、周波数変換および増幅等を施してアンテナ部１３０から送信する。

図１１は、図９に示す他方の無線装置３０Ａの内部構成を示す概略ブロック図である。無線装置３０Ａは、無線装置３０の信号発生部１１０を信号発生部１１０Ａに代え、指向性設定部２３０を指向性設定部２３０Ａに代えたものであり、その他は、無線装置３０と同じである。信号発生部１１０Ａについては、上述したとおりである。

実施の形態２においては、アンテナ部２２０は、送信処理部１２０からの信号を指向性設定部２３０Ａによって設定された無指向性または指向性で無線装置１０Ａへ送信する。すなわち、アンテナ部２２０は、オムニアンテナまたは指向性アンテナとして機能し、送信処理部１２０からの信号を無線装置１０Ａへ送信する。また、アンテナ部２２０は、無線装置１０Ａからの信号を指向性設定部２３０Ａによって設定された指向性で受信して受信処理部１４０またはプロファイル生成部１５０へ出力する。

指向性設定部２３０Ａは、アンテナ部２２０の指向性を設定する機能を持ち、無線装置１０Ａ，３０Ａにおいて秘密鍵Ｋｓ１，Ｋｓ２を生成するとき、後述する方法により、所定の順序に従ってアンテナ部２２０の指向性を順次切換え、またはアンテナ部２２０を無指向性に設定する。

図１２は、図１１に示す指向性設定部２３０Ａの機能ブロック図である。指向性設定部２３０Ａは、指向性設定部２３０の制御電圧発生回路２３１を制御電圧発生回路２３１Ａに代えたものであり、その他は、指向性設定部２３０と同じである。

指向性設定部２３０Ａは、制御電圧セットＣＬＶ１～ＣＬＶｎ（ｎは自然数）を順次発生し、その発生した制御電圧セットＣＬＶ１～ＣＬＶｎをバラクタダイオード２３２へ順次出力する。バラクタダイオード２３２は、制御電圧セットＣＬＶ１～ＣＬＶｎに応じて無給電素子であるアンテナ素子２１～２３，２５～２７に装荷される容量を変え、アレーアンテナ２０をオムニアンテナまたは指向性アンテナとして機能させる。すなわち、バラクタダイオード２３２は、制御電圧セットＣＬＶ１～ＣＬＶｎに応じて無給電素子２１～

２３，２５～２７のリアクタンス値を変えることによってアレーアンテナ２０をオムニアンテナまたは指向性アンテナとして機能させる。この場合、制御電圧セットＣＬＶ１～ＣＬＶｎの全てが０Ｖからなるとき、アレーアンテナ２０は、オムニアンテナとして機能する。そして、バラクタダイオード２３２は、制御電圧セットＣＬＶ１～ＣＬＶｎの複数の異なるセットに応じて、無給電素子２１～２３，２５～２７のリアクタンス値を順次変え、アレーアンテナ２０の指向性を複数個に順次変える。

図１３は、所定の通信プロトコルであるＩＥＥＥ８０２．１１ｂ（またはＩＥＥＥ８０２．１１ｇ）の物理層およびＭＡＣ（Ｍｅｄｉａ Ａｃｃｅｓｓ Ｃｏｎｔｒｏｌ）層のフォーマットを示す図である。物理層は、データを電気信号に変換し、実際の伝送を行なう階層である。そして、物理層は、ＩＥＥＥ８０２．１１ｂおよびＩＥＥＥ８０２．１１ｇの両方に共通なデータフォーマットからなる。また、ＭＡＣ層は、各無線装置間で信頼性の高いデータ伝送を行なう階層である。物理層は、ＰＬＣＰ（Ｐｈｙｓｉｃａｌ Ｌａｙｅｒ Ｃｏｎｖｅｒｇｅｎｃｅ Ｐｒｏｔｏｃｌ）プリアンブルと、ＰＬＣＰヘッダとからなる。

ＰＬＣＰプリアンブルは、ＳＹＮＣ（ＳＹＮＣｈｒｏｎｉｚａｔｉｏｎ ｆｉｅｌｄ）信号と、ＳＦＤ（Ｓｔａｒｔ Ｆｒａｍｅ Ｄｅｌｉｍｅｔｅｒ）信号とからなる。また、ＰＬＣＰヘッダは、ＳＩＧＮＡＬ（ＳＩＧＮＡＬ ｏｒ ｄａｔａ ｒａｔｅ）信号と、ＳＥＲＶＩＣＥ信号と、ＬＥＮＧＴＨ信号と、ＣＲＣ（Ｃｙｃｌｉｃ Ｒｅｄｕｎｄａｎｃｙ Ｃｏｄｅ）信号とからなる。

ＳＹＮＣ信号は、１２８ビットのデータ長を有する信号であり、同期の確立に使用される。ＳＦＤ信号は、１６ビットのデータ長を有する信号であり、ＰＬＣＰプリアンブルの終了を示す。

ＳＩＧＮＡＬ信号は、８ビットのデータ長を有する信号であり、ＭＡＣ層のデータ速度を示す。ＳＥＲＶＩＣＥ信号は、８ビットのデータ長を有する信号であり、機能拡張用として予約されている。ＬＥＮＧＴＨ信号は、１６ビットのデータ長を有する信号であり、ＭＡＣ層のデータ長を示す。ＣＲＣ信号は、１６ビットのデータ長を有する信号であり、誤り検出に用いられる。

また、ＭＡＣ層は、ＰＳＤＵ（ＰＬＣＰ Ｓｅｒｖｉｃｅ Ｄａｔａ Ｕｎｉｔ）からなる。そして、ＰＳＤＵは、４８ビット以上のデータ長を有するＭＡＣ層のデータである。

実施の形態２においては、秘密鍵Ｋｓ１，Ｋｓ２を生成する場合、無線装置１０Ａ，３０Ａは、所定のデータを物理層に含め、アレーアンテナ２０の指向性を変化させながら送信する。より具体的には、ＳＹＮＣ信号、ＳＦＤ信号、ＳＩＧＮＡＬ信号、ＳＥＲＶＩＣＥ信号、ＬＥＮＧＴＨ信号およびＣＲＣ信号のうち、ＳＹＮＣ信号、ＳＦＤ信号、ＳＩＧＮＡＬ信号およびＳＥＲＶＩＣＥ信号を複数のデータＤ０～Ｄ１１から構成する。そして、複数のデータＤ１～Ｄ１１は、所定のデータを分割したデータである。

データＤ０は、３６ビットのデータ長を有する。また、複数のデータＤ１～Ｄ１１の各々は、１１ビットのデータ長を有する。１１ビットのデータ長に相当する時間長を期間Ｔ０とすると、複数のデータＤ１～Ｄ１１の各々は、３ビットのデータ長に相当する期間Ｔ１と、８ビットのデータ長に相当する期間Ｔ２とに分割される。

秘密鍵Ｋｓ１，Ｋｓ２を生成する場合、データＤ０のデータ長に相当する期間Ｔ３、アレーアンテナ２０をオムニアンテナとして機能させ、データＤ１～Ｄ１１全体のデータ長に相当する期間Ｔ４、アレーアンテナ２０を指向性アンテナとして機能させ、ＬＥＮＧＴＨ信号およびＣＲＣ信号のデータ長に相当する期間Ｔ５、アレーアンテナ２０をオムニアンテナとして機能させて所定のデータを送信する。

そして、期間Ｔ４においてアレーアンテナ２０を指向性アンテナとして機能させる場合、アレーアンテナ２０の指向性が順次切換えられる。より具体的には、複数のデータＤ１～Ｄ１１の各々の期間Ｔ１においてアレーアンテナ２０の指向性が変化され、期間Ｔ２において、その変化された指向性でデータが送信される。従って、図１３に示す例においては、アレーアンテナ２０の指向性が１１回変更されて所定のデータが送信される。

所定のデータを受信する場合、所定のデータの送信時と同じように、期間Ｔ３，Ｔ５においてアレーアンテナ２０をオムニアンテナとして機能させ、期間Ｔ４においてアレーアンテナ２０を指向性アンテナとして機能させる。そして、所定のデータの受信時においては、複数のデータＤ１～Ｄ１１の各々の期間Ｔ１においてアレーアンテナ２０の指向性が変化され、その変化された指向性で受信した電波の強度が期間Ｔ２において検出される。従って、図１３に示す例においては、所定のデータの受信時においても、アレーアンテナ２０の指向性は、１１回変更される。

なお、期間Ｔ３においてアレーアンテナ２０をオムニアンテナとして機能させるのは、通信の初期においては、ＡＧＣ（Ａｕｔｏ　Ｇａｉｎ　Ｃｏｎｔｒｏｌ）機能を働かせ、データの受信レベルを最適値に調整する必要があるからである。また、期間Ｔ５においてアレーアンテナ２０をオムニアンテナとして機能させるのは、次の理由による。物理層およびＭＡＣ層のデータ受信に誤りが生じると、確認応答（＝ＡＣＫ信号）が返らず、再送状態が続いてしまう。したがって、これを防止するためにＭＡＣ層のデータに関連するＬＥＮＧＴＨ信号および物理層のデータ受信の成否を判定するＣＲＣ信号をオムニアンテナで送受信することにしたものである。

図１４は、２つの無線装置１０Ａ，３０Ａ間でデータを送受信する通常の方法の概念図である。また、図１５は、２つの無線装置１０Ａ，３０Ａ間におけるデータの再送の概念図である。更に、図１６は、この発明の実施の形態において、２つの無線装置１０Ａ，３０Ａ間でデータを送受信する方法の概念図である。

通常の方法においては、無線装置３０Ａは、アレーアンテナ２０の指向性を指向性パターン（１）に従って順次切換えて所定のデータＤＡを無線装置１０Ａへ送信する。そして、無線装置１０Ａは、所定のデータＤＡの受信を確認すると、確認応答ＡＣＫを無線装置３０Ａへ送信し、無線装置３０Ａは、アレーアンテナ２０の指向性を指向性パターン（１）に従って順次切換えて確認応答ＡＣＫを受信する。その後、無線装置３０Ａは、アレーアンテナ２０の指向性を指向性パターン（２）に従って順次切換えて所定のデータＤＡを無線装置１０Ａへ送信する。そして、無線装置１０Ａは、無線装置３０Ａから所定のデータＤＡを受信する（図１４参照）。

しかし、このような通常の方法においては、アレーアンテナ２０の指向性の変更によって図１３に示すＳＹＮＣ信号以降のデータを誤って受信した場合、物理層の同期は成立しているが、ＭＡＣ層より上位の層の同期が成立しないため、確認応答ＡＣＫが返送されず、図１５に示すように、アレーアンテナ２０の指向性を指向性パターン（１）に従って順次切換えて所定のデータＤＡを再送する動作が継続する。その結果、無線装置１０Ａ，３０Ａ間において双方向の通信ができなくなる。

そこで、この発明においては、図１６に示す方法で所定のデータＤＡを送受信する。すなわち、無線装置３０Ａは、アレーアンテナ２０にオムニパターンを設定して所定のデータＤＡを無線装置１０Ａへ送信する。つまり、無線装置３０Ａは、アレーアンテナ２０をオムニアンテナとして機能させて所定のデータＤＡを無線装置１０Ａへ送信する。

そして、無線装置１０Ａは、無線装置３０Ａからの所定のデータＤＡの受信を確認すると、確認応答ＡＣＫを無線装置３０Ａへ送信する。無線装置３０Ａは、アレーアンテナ２０の指向性を指向性パターン（１）に従って順次切換えて確認応答ＡＣＫを受信する。その後、無線装置３０Ａは、アレーアンテナ２０の指向性を指向性パターン（１）に従って順次切換えて所定のデータＤＡを無線装置１０Ａへ送信する。そして、無線装置１０Ａは、無線装置３０Ａから所定のデータＤＡを受信する（図１６参照）。

図１６に示す方法においては、無線装置３０Ａは、最初の送信において、通信が確立しているオムニパターンを使用するため、無線装置１０Ａから確認応答ＡＣＫを必ず受信できる。その結果、無線装置１０Ａ，３０Ａ間における双方向の通信を確保できる。

そして、確認応答ＡＣＫは、図１３に示す物理層のフォーマットからなるので、無線装置３０Ａは、アレーアンテナ２０の指向性を指向性パターン（１）に従って順次切換えて確認応答ＡＣＫを受信するとき、受信した確認応答ＡＣＫに含まれる複数のデータＤ１～Ｄ１１に対応する複数の電波強度を検出できる。また、無線装置３０Ａは、確認応答ＡＣ

Ｋの受信時における指向性パターン（１）を使用してアレーアンテナ２０の指向性を順次切換えて所定のデータＤＡを無線装置１０Ａへ送信するので、無線装置１０Ａは、無線装置３０Ａにおいて検出された複数の電波強度と同じ複数の電波強度を検出できる。

図１６に示す方法によって所定のデータを無線装置１０Ａ，３０Ａ間で１回送受信した場合、無線装置１０Ａ，３０Ａは、１１個の電波強度からなる強度プロファイルＰＩ１１，ＰＩ２１をそれぞれ検出する。そして、無線装置１０Ａ，３０Ａ間における所定のデータの送受信をｍ（ｍは自然数）回繰返すことによって、無線装置１０Ａ，３０Ａは、ｍ個の強度プロファイルＰＩ１１～ＰＩ１ｍ，ＰＩ２１～ＰＩ２ｍをそれぞれ検出する。

そして、強度プロファイルＰＩ１１～ＰＩ１ｍの全体に含まれる電波強度は、図７に示すｎ個の電波強度ＷＩ１～ＷＩｎに等しい。従って、無線装置１０Ａ，３０Ａ間における所定のデータの１回の送受信によって、ｎ個の電波強度ＷＩ１～ＷＩｎのうちの１１個の電波強度ＷＩ（ｉ）～ＷＩ（ｉ＋１０）（ｉ＝１～ｎ－１０）が検出される。

つまり、この発明においては、所定の通信プロトコルであるＩＥＥＥ８０２．１１ｂ（またはＩＥＥＥ８０２．１１ｇ）の物理層に所定のデータＤＡを含めて無線装置１０Ａ，３０Ａ間で送受信することをｍ回繰り返すことによってｎ個の電波強度ＷＩ１～ＷＩｎが検出され、その検出されたｎ個の電波強度ＷＩ１～ＷＩｎに基づいて秘密鍵Ｋｓ１，Ｋｓ２が生成される。

図１７は、図９に示す２つの無線装置１０Ａ，３０Ａ間で通信を行なう動作を説明するためのフローチャートである。一連の動作が開始されると、無線装置３０Ａの送信処理部１２０は、ｋ＝１を設定する（ステップＳ２１）。そして、指向性設定部２３０Ａは、アレーアンテナ２０をオムニアンテナとして機能させ、所定のデータＤＡを無線装置１０Ａへ送信する（ステップＳ２２）。

続いて、無線装置１０Ａのアンテナ部１３０は、所定のデータＤＡを受信し（ステップＳ２３）、その受信した所定のデータＤＡを受信処理部１４０へ出力する。そして、受信処理部１４０は、所定のデータＤＡの受信を確認すると、送信処理部１２０は、確認応答（ＡＣＫ信号）をアンテナ部１３０から無線装置３０Ａへ送信する（ステップＳ２４）。

無線装置３０Ａの指向性設定部２３０Ａは、アンテナ部２２０をオムニアンテナ、指向性アンテナおよびオムニアンテナとして順次機能させ、アンテナ部２２０は、確認応答（ＡＣＫ信号）を受信する（ステップＳ２５）。すなわち、アレーアンテナ２０は、図１３に示すデータＤ０をオムニアンテナとして受信し、指向性をパターンＰｋにより１１個に変化させながらデータＤ１～Ｄ１１を受信し、更に、ＬＥＮＧＴＨ信号およびＣＲＣ信号をオムニアンテナとして受信する。

そして、アンテナ部２２０は、受信した複数のデータＤ１～Ｄ１１に対応する複数の電波をプロファイル生成部１５０へ出力する。プロファイル生成部１５０は、アンテナ部２２０からの複数の電波の強度プロファイルＰＩ１ｋを検出する（ステップＳ２６）。

次に、無線装置３０Ａの信号発生部１１０Ａは、所定のデータを発生して送信処理部１２０へ出力し、送信処理部１２０は、所定のデータを物理層のデータＤ１～Ｄ１１に割り当て、オムニアンテナ、指向性アンテナおよびオムニアンテナとして順次機能させたアンテナ部２２０を介して無線装置１０Ａへ所定のデータを送信する（ステップＳ２７）。すなわち、アンテナ部２２０は、図１３に示すデータＤ０をオムニアンテナとして送信し、指向性をパターンＰｋにより１１個に変化させながらデータＤ１～Ｄ１１を送信し、更に、ＬＥＮＧＴＨ信号およびＣＲＣ信号をオムニアンテナとして送信する。

無線装置１０Ａにおいて、アンテナ部１３０は、無線装置３０Ａから所定のデータを受信する。（ステップＳ２８）。そして、アンテナ部１３０は、受信した複数のデータＤ１～Ｄ１１に対応する複数の電波をプロファイル生成部１５０へ出力する。プロファイル生成部１５０は、アンテナ部部１３０からの複数の電波の強度プロファイルＰＩ２ｋを検出する（ステップＳ２９）。

その後、無線装置３０Ａの送信処理部１２０は、ｋ＝ｋ＋１を設定し（ステップＳ３０）、ｋ＝ｍであるか否かを判定する（ステップＳ３１）。そして、ｋ＝ｍでないとき、ステップＳ２２～Ｓ３１が繰返し実行される。即ち、アレーアンテナ２０の指向性パターン

がパターンＰ１～Ｐｍによってｍ個に変えられて、無線装置１０Ａのアンテナ部１３０と無線装置３０Ａのアンテナ部２２０との間で所定のデータを構成する電波が送受信され、強度プロファイルＩ１１～Ｉ１ｍ及びＩ２１～Ｉ２ｍが検出されるまで、ステップＳ２～Ｓ１１が繰返し実行される。

ステップＳ１１において、ｋ＝ｍであると判定されると、無線装置３０Ａにおいて、プロファイル生成部１５０は、強度プロファイルＩ１１～Ｉ１ｍに含まれる強度Ｉ１１～Ｉ１ｎから受信信号プロファイルＲＳＳＩ１を作成して鍵作成部１６０へ出力する。

鍵作成部１６０は、受信信号プロファイルＲＳＳＩ１から最大強度ＷＩｍａｘ１を検出し、その検出した最大強度ＷＩｍａｘ１によって受信信号プロファイルＲＳＳＩ１を規格化し、強度Ｉ１１～Ｉ１ｎを多値化する。そして、鍵作成部１６０は、多値化した各値をビットパターンとする秘密鍵Ｋｓ２を生成する（ステップＳ３２）

また、無線装置１０Ａのプロファイル生成部１５０は、強度プロファイルＩ２１～Ｉ２ｍに含まれる強度Ｉ２１～Ｉ２ｎから受信信号プロファイルＲＳＳＩ２を作成して鍵作成部１６０へ出力する。鍵作成部１６０は、受信信号プロファイルＲＳＳＩ２から最大強度ＷＩｍａｘ２を検出し、その検出した最大強度ＷＩｍａｘ２によって受信信号プロファイルＲＳＳＩ２を規格化し、強度Ｉ２１～Ｉ２ｎを多値化する。そして、鍵作成部１６０は、多値化した各値をビットパターンとする秘密鍵Ｋｓ１を生成する（ステップＳ３３）。

ステップＳ３４～ステップＳ３９は、図８に示すフローチャートのステップＳ１４～ステップＳ１９と同じである。

上述したステップＳ２２～Ｓ２４に示す動作は、アレーアンテナ２０をオムニアンテナとして機能させて無線装置１０Ａと無線装置３０Ａとの間で通信を確立する動作である。また、ステップＳ２４～Ｓ２６に示す動作は、無線装置３０Ａにおいて受信信号プロファイルＲＳＳＩ１を生成するための電波を無線装置１０Ａのアンテナ１１から無線装置３０Ａのアレーアンテナ２０へ送信し、かつ、無線装置３０Ａにおいて電波の強度プロファイルＰＩ１ｋを検出する動作であり、ステップＳ２７～Ｓ２９に示す動作は、無線装置１０Ａにおいて受信信号プロファイルＲＳＳＩ２を生成するための電波を無線装置３０Ａのアレーアンテナ２０から無線装置１０Ａのアンテナ１１へ送信し、かつ、無線装置１０Ａにおいて電波の強度プロファイルＰＩ２ｋを検出する動作である。そして、所定のデータを構成する電波の無線装置１０Ａのアンテナ１１から無線装置３０Ａのアレーアンテナ２０への送信及び所定のデータを構成する電波の無線装置３０Ａのアレーアンテナ２０から無線装置１０Ａのアンテナ１１への送信は、アレーアンテナ２０の指向性をパターンＰｋに従って変えながら交互に行なわれる。つまり、所定のデータを構成する電波は、無線装置１０Ａのアンテナ１１と無線装置３０Ａのアレーアンテナ２０との間で時分割通信により送受信される。

従って、アレーアンテナ２０の指向性をパターンＰｋに従って変えながら無線装置１０Ａのアンテナ１１から無線装置３０Ａのアレーアンテナ２０へ所定のデータを構成する電波を送信し、無線装置３０Ａにおいて電波の強度プロファイルＰＩ１ｋを検出した直後に、同じ所定のデータを構成する電波を無線装置３０Ａのアレーアンテナ２０から無線装置１０Ａのアンテナ１１へ送信し、無線装置１０Ａにおいて電波の強度プロファイルＰＩ２ｋを検出することができる。その結果、無線装置１０Ａ，３０Ａ間において同じ伝送路特性を確保して所定のデータを構成する電波を無線装置１０Ａ，３０Ａ間で送受信でき、電波の可逆性により電波の強度Ｉ１１～Ｉ１ｎをそれぞれ電波の強度Ｉ２１～Ｉ２ｎに一致させることができる。そして、無線装置１０Ａにおいて作成される秘密鍵Ｋｓ１を無線装置３０において作成される秘密鍵Ｋｓ２に容易に一致させることができる。

また、所定のデータを構成する電波は、無線装置１０Ａ，３０Ａ間で時分割通信により送受信されるので、電波の干渉を抑制して１つのアレーアンテナ２０を介して所定のデータを構成する電波を無線装置１０Ａ，３０Ａ間で送受信できる。

更に、所定のデータは、所定の通信プロトコルであるＩＥＥＥ８０２．１１ｂおよびＩＥＥＥ８０２．１１ｇに共通な物理層に含めて無線装置１０Ａ，３０Ａ間で送受信されるので、通信プロトコルがＩＥＥＥ８０２．１１ｂからＩＥＥＥ８０２．１１ｇへ変化して

もデータフォーマットを変えずに秘密鍵Ｋｓ１，Ｋｓ２を生成できる。

更に、無線装置３０Ａは、無線装置１０Ａからの確認応答（ＡＣＫ信号）の受信時および所定のデータの無線装置１０Ａへの送信時、同じパターンＰｋによってアレーアンテナ２０の指向性を順次変更する（ステップＳ２５，Ｓ２７参照）。そして、同じパターンＰｋによってアレーアンテナ２０の指向性を順次変更して無線装置１０Ａから確認応答（ＡＣＫ信号）を受信する動作（ステップＳ２５）および所定のデータを無線装置１０Ａへ送信する動作（ステップＳ２７）は、ｋ＝ｍになるまで繰返し実行されるので、ステップＳ２５，Ｓ２７において、パターンＰｋに従ってアレーアンテナ２０の指向性を順次変更することは、アレーアンテナ２０の指向性を更新して無線装置１０Ａから確認応答（ＡＣＫ信号）を受信し、その更新した指向性を維持して所定のデータを無線装置１０Ａへ送信することに相当する。

このように、図１６に示す方法によって所定のデータを無線装置１０Ａ，３０Ａ間で送受信することによって所定のデータの再送が繰返されるのを防止し、無線装置１０Ａ，３０Ａ間における双方向の通信を確保できる。すなわち、無線装置１０Ａ，３０Ａにおいて同じ秘密鍵Ｋｓ１，Ｋｓ２を安定して作成できる。

更に、アレーアンテナ２０の指向性をパターンＰｋに従って変えながら無線装置１０Ａ，３０Ａ間で所定のデータを構成する電波を送受信し、秘密鍵Ｋｓ１，Ｋｓ２を作成するための受信信号プロファイルＲＳＳＩ１，ＲＳＳＩ２を生成するので、図９に示すようにアレーアンテナ２０を装着した無線装置３０Ａの近傍に盗聴装置５０が配置されていても、盗聴装置５０による秘密鍵Ｋｓ１，Ｋｓ２の盗聴を抑制できる。

即ち、盗聴装置５０は、アンテナ１１及びアレーアンテナ２０から送信された電波をアンテナ５１を介して受信するが、アレーアンテナ２０は指向性をパターンＰｋに従って変えながら電波を送受信するので、アンテナ１１とアレーアンテナ２０との間で送受信される電波は、アンテナ１１またはアレーアンテナ２０とアンテナ５１との間で送受信される電波と異なり、盗聴装置５０は、無線装置３０Ａが送受信する電波と同じ電波を送受信できず、電波の強度プロファイルＰＩ１ｋと同じ強度プロファイルを得ることができない。その結果、盗聴装置５０は、秘密鍵Ｋｓ１，Ｋｓ２を盗聴することができない。

従って、この発明においては、電気的に指向性を切換え可能なアレーアンテナ２０を盗聴装置５０の近傍に配置された無線装置３０Ａに装着することを特徴とする。

更に、鍵確認用データＤＣＦＭ１～４は、秘密鍵Ｋｓ１，Ｋｓ２に非可逆的な演算、または一方向的な演算を施して発生されるので、鍵確認用データＤＣＦＭ１～４が盗聴されても秘密鍵Ｋｓ１，Ｋｓ２が解読される危険性を極めて低くできる。

更に、シンドロームｓ１，ｓ２は、秘密鍵Ｋｓ１，Ｋｓ２のビットパターンを示す鍵x_1，x_2に検査行列Ｈの転置行列H^Tを乗算して得られるので、シンドロームｓ１，ｓ２が盗聴されても直ちに情報のビットパターンが推測されることは特殊な符号化を想定しない限り起こらない。従って、盗聴を抑制して秘密鍵を一致させることができる。

なお、無線装置１０Ａ，３０Ａ間で通信を行なう動作は、実際には、ＣＰＵによって行なわれ、無線装置１０Ａに搭載されたＣＰＵは、図１７に示す各ステップＳ２３，Ｓ２４，Ｓ２８，Ｓ２９，Ｓ３３，Ｓ３４，Ｓ３６，Ｓ３８を備えるプログラムをＲＯＭから読出し、無線装置３０Ａに搭載されたＣＰＵは、図１７に示す各ステップＳ２１，Ｓ２２，Ｓ２５，Ｓ２６，Ｓ２７，Ｓ３０，Ｓ３１，Ｓ３２，Ｓ３５，Ｓ３７，Ｓ３９を備えるプログラムをＲＯＭから読出し、無線装置１０Ａ，３０Ａに搭載された２つのＣＰＵは、その読出したプログラムを実行して図１７に示すフローチャートに従って無線装置１０Ａ，３０Ａ間で通信を行なう。

従って、ＲＯＭは、無線装置１０Ａ，３０Ａ間で通信を行なう動作をコンピュータ（ＣＰＵ）に実行させるためのプログラムを記録したコンピュータ（ＣＰＵ）読取り可能な記録媒体に相当する。

そして、図１７に示す各ステップを備えるプログラムは、アレーアンテナ２０の指向性を複数個に順次変えて受信した複数の電波に基づいて、無線装置１０Ａ，３０Ａ間における通信をコンピュータ（ＣＰＵ）に実行させるプログラムである。

その他は、実施の形態１と同じである。

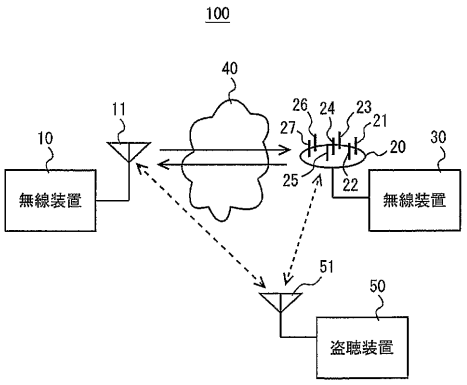
今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【産業上の利用可能性】

この発明は、秘密鍵の盗聴を抑制可能な無線通信システムに適用される。

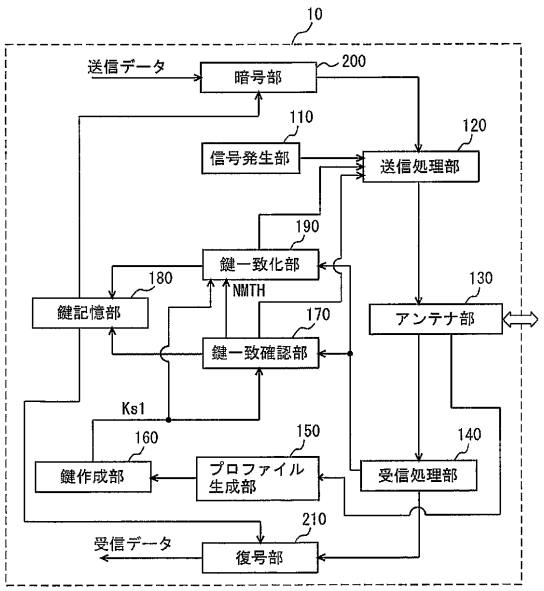
【図１】

ＦＩＧ．１

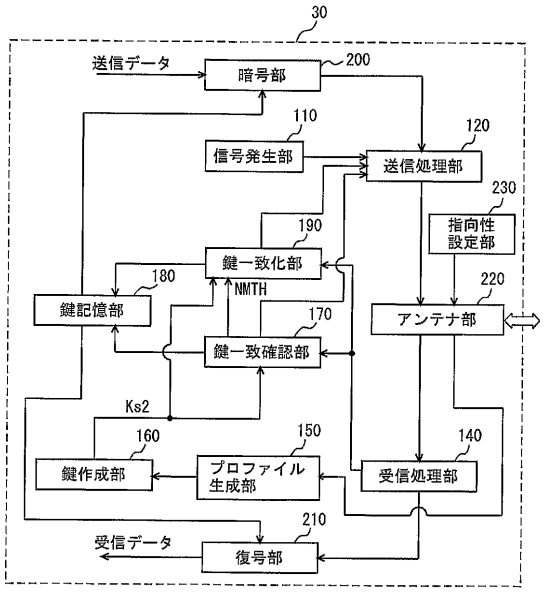


【図２】

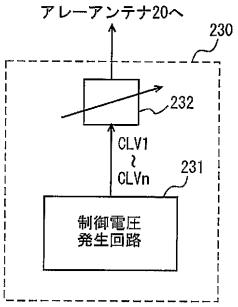
ＦＩＧ．２



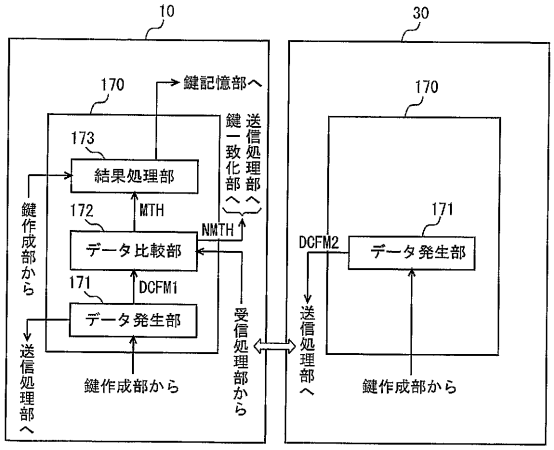
【図３】
ＦＩＧ．３



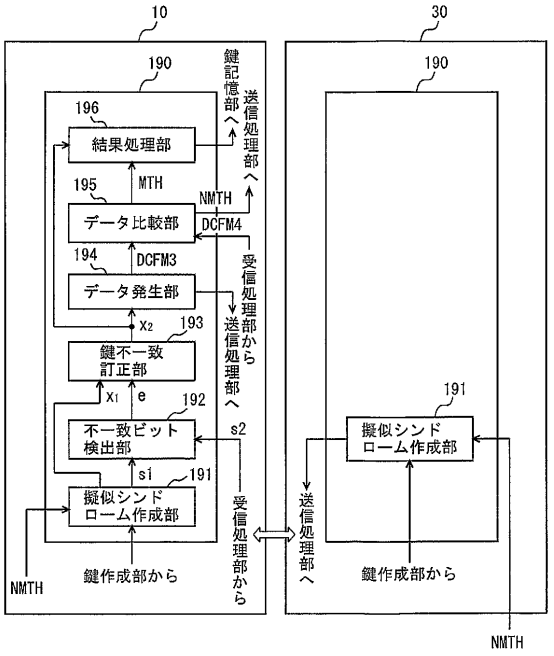
【図４】
ＦＩＧ．４



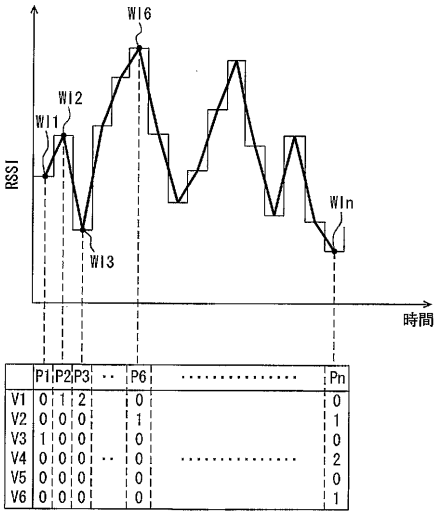
【図５】
ＦＩＧ．５



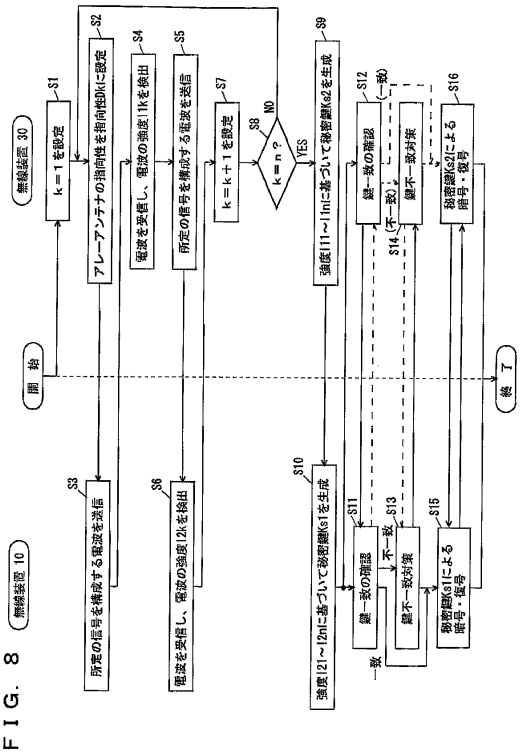
【図６】
ＦＩＧ．６



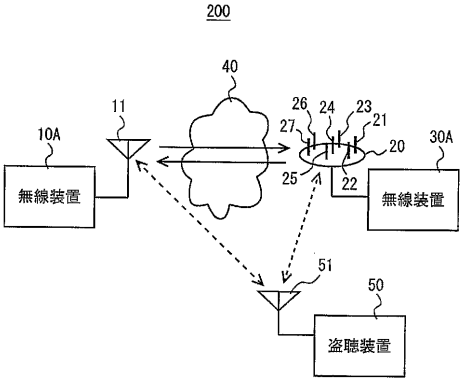
【図７】
ＦＩＧ．７



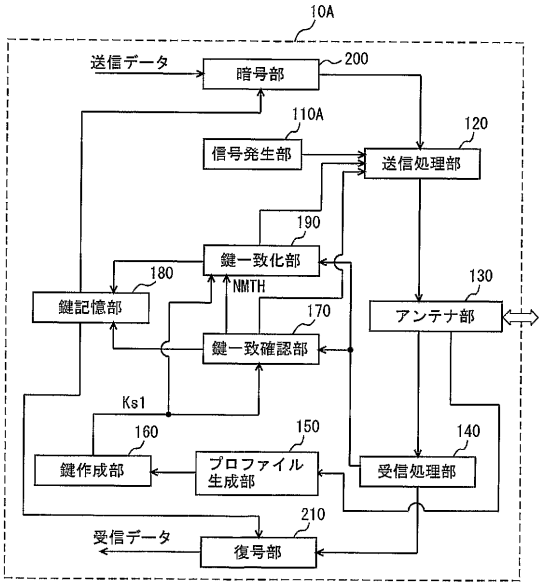
【図８】



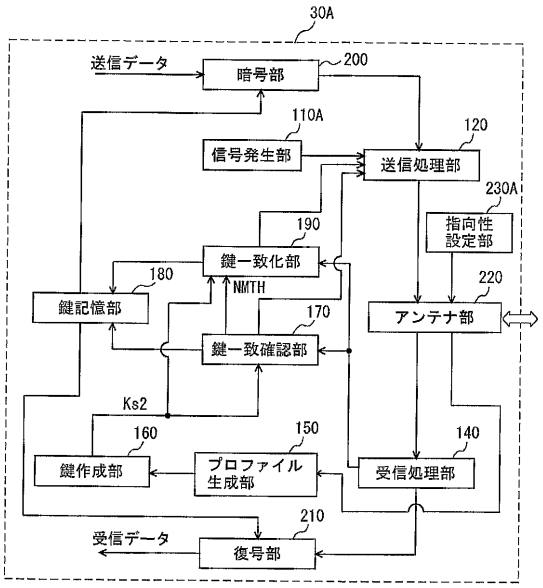
【図９】
ＦＩＧ．９



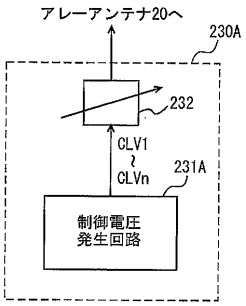
【図１０】
ＦＩＧ．１０



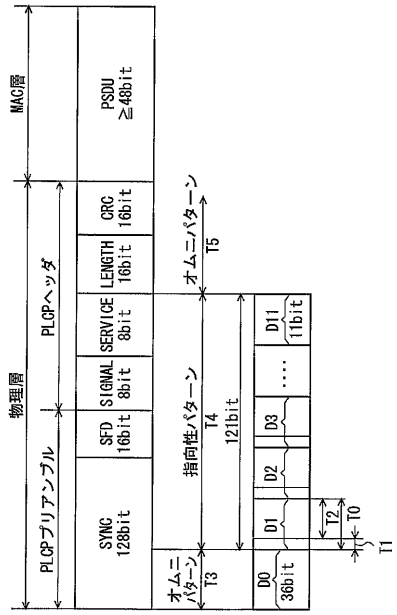
【図１１】
ＦＩＧ．１１



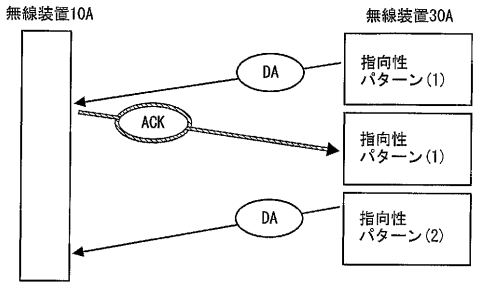
【図１２】
ＦＩＧ．１２



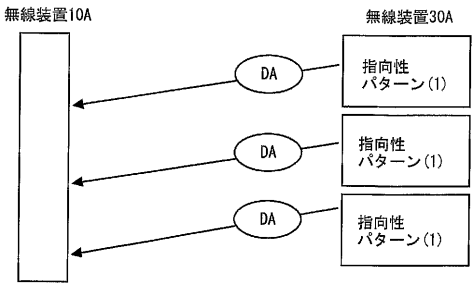
【図１３】
ＦＩＧ．１３



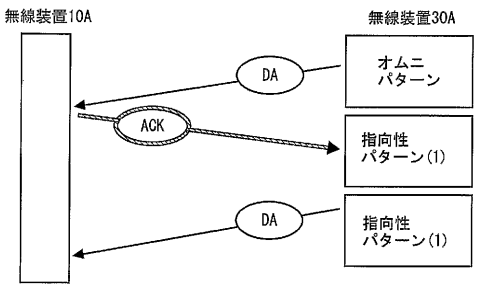
【図１４】
ＦＩＧ．１４



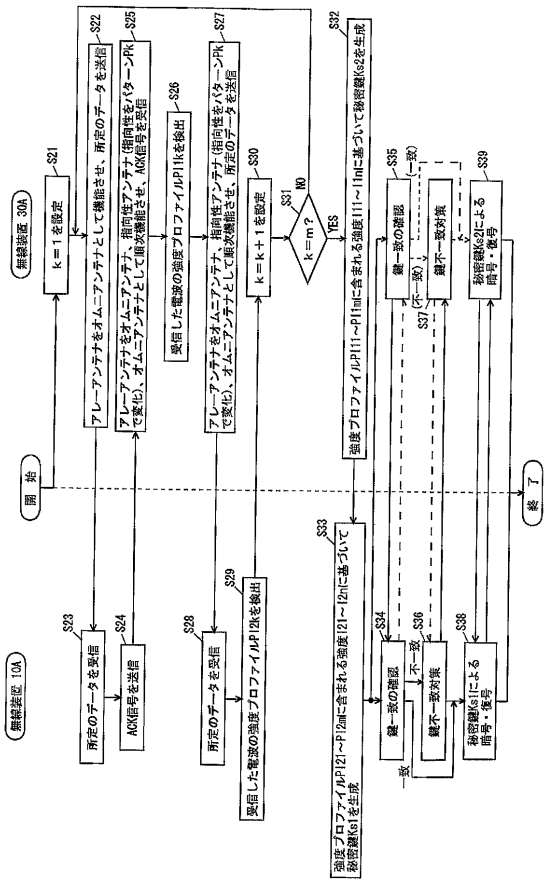
【図１５】
ＦＩＧ．１５



【図１６】
ＦＩＧ．１６



【図１７】



ＦＩＧ．１７

フロントページの続き

（出願人による申告）平成１６年度独立行政法人情報通信研究機構、研究テーマ「自律分散型無線ネットワークの研究開発」に関する委託研究、産業活力再生特別措置法第３０条の適用を受ける特許出願

(72)発明者　大平　孝
京都府相楽郡精華町光台二丁目２番地２　株式会社国際電気通信基礎技術研究所内

審査官　青木　重徳

(56)参考文献　特開２００３－０１８０９１（ＪＰ，Ａ）
国際公開第０３／０７３６８９（WO，Ａ１）
特開２００２－１５２１９１（ＪＰ，Ａ）
特開２００２－１８９５４３（ＪＰ，Ａ）
特開２００１－３２６６３０（ＪＰ，Ａ）
北浦明人，笹岡秀一，“陸上移動通信におけるＯＦＤＭの伝送路特性に基づく秘密鍵共有方式”，電子情報通信学会技術研究報告（ＲＣＳ２００３－１１７～１３０），日本，社団法人電子情報通信学会，２００３年　8月１５日，Ｖｏｌ．１０３，Ｎｏ．２５４，ｐ．２３－２８
森浩樹，笹岡秀一，大平孝，“受信信号強度の空間相関に基づく秘密鍵生成に適したアンテナパターンの検討”，電子情報通信学会技術研究報告（ＲＣＳ２００３－１８６～２１４），日本，社団法人電子情報通信学会，２００３年１１月１４日，Ｖｏｌ．１０３，Ｎｏ．４６０，ｐ．４７－５２
中山清喬，笹岡秀一，“移動通信における通信路雑音を用いたセキュリティ通信方式の検討”，２００２年電子情報通信学会総合大会講演論文集，日本，社団法人電子情報通信学会，２００２年　3月　7日，通信１，Ｂ－５－７３，ｐ．５２３

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L　9/08
JSTPlus(JDreamII)
JMEDPlus(JDreamII)
JST7580(JDreamII)