(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5126651号
(P5126651)

(45)発行日　平成25年1月23日(2013.1.23)　(24)登録日　平成24年11月9日(2012.11.9)

(51)Int.Cl.　F I
*H04L 9/08 (2006.01)*　H04L 9/00 601C
*H04B 1/40 (2006.01)*　H04L 9/00 601E
H04B 1/40

請求項の数 6　(全 44 頁)

(21)出願番号　特願2007-84381(P2007-84381)
(22)出願日　平成19年3月28日(2007.3.28)
(65)公開番号　特開2008-245010(P2008-245010A)
(43)公開日　平成20年10月9日(2008.10.9)
審査請求日　平成22年3月3日(2010.3.3)

（出願人による申告）平成１８年度独立行政法人情報通信研究機構、研究テーマ「超高速ギガビット無線ＬＡＮ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

(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　伊藤　隆
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
(72)発明者　橋本　徹
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
(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

最終頁に続く

(54)【発明の名称】通信システムおよびそれに用いる無線装置

(57)【特許請求の範囲】
【請求項１】
第１の通信装置と、
相互に異なるｍ（ｍは２以上の整数）個の無線伝送路を介して前記第１の通信装置と電波を送受信する第２の通信装置とを備え、
前記第１の通信装置は、１つの無線伝送路を介して前記第２の通信装置から受信した複数の電波の強度に基づいてｋ（ｋは２以上の整数）個のビットからなる第１の部分秘密鍵を生成する第１の部分鍵生成処理を前記ｍ個の無線伝送路について実行してｍ個の第１の部分秘密鍵を生成し、その生成したｍ個の第１の部分秘密鍵を組合わせて第１の秘密鍵を生成し、
前記第２の通信装置は、１つの無線伝送路を介して前記第１の通信装置から受信した複数の電波の強度に基づいて前記ｋ個のビットからなる第２の部分秘密鍵を生成する第２の部分鍵生成処理を前記ｍ個の無線伝送路について実行してｍ個の第２の部分秘密鍵を生成し、その生成したｍ個の第２の部分秘密鍵を組合わせて前記第１の秘密鍵と同じビット列からなる第２の秘密鍵を生成し、
前記第１の通信装置は、
第１のアンテナと、
前記第１のアンテナを介して前記第２の通信装置と電波を送受信する第１の無線装置とを含み、
前記第２の通信装置は、

ｍ個の第２のアンテナと、
前記ｍ個の第２のアンテナに対応して設けられ、各々が前記第２のアンテナを介して前記第１の無線装置と電波を送受信するｍ個の第２の無線装置と、
前記ｍ個の第２の無線装置が前記第１の無線装置から受信した電波の電波強度に基づいて秘密鍵を生成する鍵生成装置とを含み、
前記第１の部分鍵生成処理は、前記第１の無線装置が前記第１のアンテナを介して１つの第２の無線装置から受信した複数の電波の強度に基づいて前記第１の部分秘密鍵を生成する処理からなり、
前記第２の部分鍵生成処理は、１つの前記第２の無線装置が前記第２のアンテナを介して前記第１の無線装置から受信した複数の電波の強度に基づいて前記第２の部分秘密鍵を生成する処理からなり、
前記第１の無線装置は、前記第１のアンテナを介して前記ｍ個の無線装置から受信した複数の電波に基づいて前記第１の部分鍵生成処理をｍ回実行して前記ｍ個の第１の部分秘密鍵を生成し、その生成したｍ個の第１の部分秘密鍵を組合わせて前記第１の秘密鍵を生成し、
前記ｍ個の第２の無線装置の各々は、前記第２のアンテナを介して前記第１の無線装置から受信した複数の電波の強度に基づいて前記第２の部分鍵生成処理を実行して前記第２の部分秘密鍵を生成し、
前記鍵生成装置は、前記ｍ個の第２の無線装置からｍ個の第２の部分秘密鍵を受信し、その受信したｍ個の第２の部分秘密鍵を組合わせて前記第２の秘密鍵を生成する、通信システム。

【請求項２】
前記ｍ個の第２のアンテナの各々は、電気的に指向性を切換え可能な指向性アンテナからなり、
前記第１の部分鍵生成処理は、前記指向性アンテナの指向性が複数の指向性に切換えられたときに前記第１の無線装置が前記第１のアンテナを介して１つの第２の無線装置から受信した複数の電波の強度に基づいて前記第１の部分秘密鍵を生成する処理からなり、
前記第２の部分鍵生成処理は、前記指向性アンテナの指向性が前記複数の指向性に切換えられたときに１つの前記第２の無線装置が前記第２のアンテナを介して前記第１の無線装置から受信した複数の電波の強度に基づいて前記第２の部分秘密鍵を生成する処理からなる、請求項１に記載の通信システム。

【請求項３】
第１の無線装置と、
各々が指向性を電気的に切換え可能な指向性アンテナを介して前記第１の無線装置と電波を送受信するｍ（ｍは２以上の整数）個の第２の無線装置と、
前記ｍ個の第２の無線装置が前記第１の無線装置から受信した電波の電波強度に基づいて、秘密鍵を生成する鍵生成装置とを備え、
前記第１の無線装置は、前記指向性アンテナの指向性が複数の指向性に変えられたときに前記ｍ個の第２の無線装置から受信したｍ×ｎ（ｎは２以上の整数）個の第１の電波の強度であるｍ×ｎ個の第１の電波強度を組合わせて第１の秘密鍵を生成し、
前記ｍ個の第２の無線装置の各々は、前記指向性アンテナの指向性が前記複数の指向性に変えられたときに前記第１の無線装置から受信したｎ個の第２の電波の強度であるｎ個の第２の電波強度に基づいて部分秘密鍵を生成し、
前記鍵生成装置は、前記ｍ個の第２の無線装置から受信したｍ個の部分秘密鍵を組合わせて前記第１の秘密鍵と同じビット列からなる第２の秘密鍵を生成する、通信システム。

【請求項４】
前記ｍ個の第２の無線装置の各々は、前記指向性アンテナの指向性が複数の指向性に変えられたときに前記第１の無線装置からｋ（ｋは２以上の整数）個の電波を受信するごとに前記ｋ個の電波に対応するｋ個の電波強度を検出し、その検出したｋ個の電波強度に基づいて前記部分秘密鍵を生成し、

前記鍵生成装置は、前記ｍ個の第２の無線装置からｍ個の部分秘密鍵を任意の順序で受信して前記第２の秘密鍵を生成する、請求項３に記載の通信システム。
【請求項５】
前記第１の無線装置は、前記第１の秘密鍵を用いて前記ｍ個の第２の無線装置と無線通信を行ない、
前記ｍ個の第２の無線装置の各々は、前記第２の秘密鍵を用いて前記第１の無線装置と無線通信を行なう、請求項１から請求項４のいずれか１項に記載の通信システム。
【請求項６】
無線伝送路を用いて秘密鍵を生成する通信システムに用いられる無線装置であって、
請求項１から請求項５のいずれか１項に記載の第１の無線装置または第２の無線装置からなる無線装置。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、通信システムおよびそれに用いる無線装置に関し、特に、暗号化した情報を無線により通信する通信システムおよびそれに用いる無線装置に関するものである。
【背景技術】
【０００２】
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。
【０００３】
情報を暗号化して端末装置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。
【０００４】
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。
【０００５】
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つの端末装置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装置で秘密鍵を生成する方法が提案されている（非特許文献１）。
【０００６】
この方法は、２つの端末装置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装置で測定し、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装置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、一方の端末装置から他方の端末装置へデータを送信したときの遅延プロファイルは、他方の端末装置から一方の端末装置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、一方の端末装置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、他方の端末装置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。
【０００７】
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つの端末装置間で相互に送受信するだけで同じ秘密鍵を共有することができる。
【非特許文献１】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．
【発明の開示】

【発明が解決しようとする課題】
【０００８】
しかし、２つの端末間で送信される複数の電波を盗聴者が各端末の近傍で傍受して強度プロファイルを測定すれば、盗聴者は、各端末で測定した強度プロファイルに近い強度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。
【０００９】
そこで、この発明は、かかる問題を解決するためになされたものであり、その目的は、秘密鍵の盗聴を抑制可能な通信システムを提供することである。
【００１０】
また、この発明の別の目的は、秘密鍵の盗聴を抑制可能な通信システムに用いる無線装置を提供することである。
【課題を解決するための手段】
【００１１】
この発明によれば、通信システムは、第１および第２の通信装置を備える。第２の通信装置は、相互に異なるｍ（ｍは２以上の整数）個の無線伝送路を介して第１の通信装置と電波を送受信する。そして、第１の通信装置は、１つの無線伝送路を介して第２の通信装置から受信した複数の電波の強度に基づいてｋ（ｋは２以上の整数）個のビットからなる第１の部分秘密鍵を生成する第１の部分鍵生成処理をｍ個の無線伝送路について実行してｍ個の第１の部分秘密鍵を生成し、その生成したｍ個の第１の部分秘密鍵を組合わせて第１の秘密鍵を生成する。また、第２の通信装置は、１つの無線伝送路を介して第１の通信装置から受信した複数の電波の強度に基づいてｋ個のビットからなる第２の部分秘密鍵を生成する第２の部分鍵生成処理をｍ個の無線伝送路について実行してｍ個の第２の部分秘密鍵を生成し、その生成したｍ個の第２の部分秘密鍵を組合わせて第１の秘密鍵と同じビット列からなる第２の秘密鍵を生成する。
【００１２】
好ましくは、第１の通信装置は、第１のアンテナと、第１の無線装置とを含む。第１の無線装置は、第１のアンテナを介して第２の通信装置と電波を送受信する。第２の通信装置は、ｍ個の第２のアンテナと、ｍ個の第２の無線装置と、鍵生成装置とを含む。ｍ個の第２の無線装置は、ｍ個の第２のアンテナに対応して設けられ、各々が第２のアンテナを介して第１の無線装置と電波を送受信する。鍵生成装置は、ｍ個の第２の無線装置が第１の無線装置から受信した電波の電波強度に基づいて秘密鍵を生成する。第１の部分鍵生成処理は、第１の無線装置が第１のアンテナを介して１つの第２の無線装置から受信した複数の電波の強度に基づいて第１の部分秘密鍵を生成する処理からなる。第２の部分鍵生成処理は、１つの第２の無線装置が第２のアンテナを介して第１の無線装置から受信した複数の電波の強度に基づいて第２の部分秘密鍵を生成する処理からなる。第１の無線装置は、第１のアンテナを介してｍ個の無線装置から受信した複数の電波に基づいて第１の部分鍵生成処理をｍ回実行してｍ個の第１の部分秘密鍵を生成し、その生成したｍ個の第１の部分秘密鍵を組合わせて第１の秘密鍵を生成する。ｍ個の第２の無線装置の各々は、第２のアンテナを介して第１の無線装置から受信した複数の電波の強度に基づいて第２の部分鍵生成処理を実行して第２の部分秘密鍵を生成する。鍵生成装置は、ｍ個の第２の無線装置からｍ個の第２の部分秘密鍵を受信し、その受信したｍ個の第２の部分秘密鍵を組合わせて第２の秘密鍵を生成する。
【００１３】
好ましくは、ｍ個の第２のアンテナの各々は、電気的に指向性を切換え可能な指向性アンテナからなる。第１の部分鍵生成処理は、指向性アンテナの指向性が複数の指向性に切換えられたときに第１の無線装置が第１のアンテナを介して１つの第２の無線装置から受信した複数の電波の強度に基づいて第１の部分秘密鍵を生成する処理からなる。第２の部分鍵生成処理は、指向性アンテナの指向性が複数の指向性に切換えられたときに１つの第２の無線装置が前記第２のアンテナを介して第１の無線装置から受信した複数の電波の強度に基づいて第２の部分秘密鍵を生成する処理からなる。

【００１４】
また、この発明によれば、通信システムは、第１の無線装置と、ｍ（ｍは２以上の整数）個の第２の無線装置と、鍵生成装置とを備える。ｍ個の第２の無線装置は、各々が指向性を電気的に切換え可能な指向性アンテナを介して第１の無線装置と電波を送受信する。鍵生成装置は、ｍ個の第２の無線装置が第１の無線装置から受信した電波の電波強度に基づいて、秘密鍵を生成する。第１の無線装置は、指向性アンテナの指向性が複数の指向性に変えられたときにｍ個の第２の無線装置から受信したｍ×ｎ（ｎは２以上の整数）個の第１の電波の強度であるｍ×ｎ個の第１の電波強度を組合わせて第１の秘密鍵を生成する。ｍ個の第２の無線装置の各々は、指向性アンテナの指向性が前記複数の指向性に変えられたときに第１の無線装置から受信したｎ個の第２の電波の強度であるｎ個の第２の電波強度に基づいて部分秘密鍵を生成する。そして、鍵生成装置は、ｍ個の第２の無線装置から受信したｍ個の部分秘密鍵を組合わせて第１の秘密鍵と同じビット列からなる第２の秘密鍵を生成する。
【００１５】
好ましくは、ｍ個の第２の無線装置の各々は、指向性アンテナの指向性が複数の指向性に変えられたときに第１の無線装置からｋ（ｋは２以上の整数）個の電波を受信するごとにｋ個の電波に対応するｋ個の電波強度を検出し、その検出したｋ個の電波強度に基づいて部分秘密鍵を生成する。鍵生成装置は、ｍ個の第２の無線装置からｍ個の部分秘密鍵を任意の順序で受信して第２の秘密鍵を生成する。
【００１６】
好ましくは、ｍ個の第２の無線装置は、相互に異なる周波数を用いて第１の無線装置との間で電波を送受信する。
【００１７】
好ましくは、ｍ個の第２の無線装置の各々は、無線通信空間における無線通信に用いられていない周波数を用いて第１の無線装置との間で電波を送受信する。
【００１８】
好ましくは、第１の無線装置は、ｍ個の第２の無線装置のうちのｊ（ｊは２≦ｊ＜ｍを満たす整数）個の第２の無線装置との間で指向性アンテナの指向性を変えながら電波を送受信して第１の秘密鍵を生成する。鍵生成装置は、ｊ個の第２の無線装置から受信したｊ個の部分秘密鍵を組合わせて第２の秘密鍵を生成する。
【００１９】
好ましくは、ｊ個の第２の無線装置は、無線通信空間における無線通信に用いられている周波数を用いて無線通信を行なう第２の無線装置をｍ個の第２の無線装置から除いた第２の無線装置からなる。
【００２０】
好ましくは、第１の無線装置は、第１の秘密鍵を用いてｍ個の第２の無線装置と無線通信を行なう。ｍ個の第２の無線装置の各々は、第２の秘密鍵を用いて第１の無線装置と無線通信を行なう。
【００２１】
更に、この発明によれば、無線装置は、無線伝送路を用いて秘密鍵を生成する通信システムに用いられる無線装置であって、請求項２から請求項６のいずれか１項に記載の第１の無線装置または第２の無線装置からなる。
【発明の効果】
【００２２】
この発明においては、第１および第２の通信装置の各々は、指向性を複数の指向性に切換えながら送受信された複数の電波に基づいて生成されたｍ個の部分秘密鍵を組合せて秘密鍵を生成する。その結果、秘密鍵を生成するときのｍ個の部分秘密鍵の組合せ方法を秘匿した状態で秘密鍵が生成される。
【００２３】
従って、この発明によれば、秘密鍵の盗聴を抑制できる。

【発明を実施するための最良の形態】
【００２４】
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。
【００２５】
図１は、この発明の実施の形態による通信システム１００の概略図である。通信システム１００は、無線装置１０，２０，３０，４０と、鍵生成装置５０と、有線ケーブル５１～５３とを備える。
【００２６】
無線装置１０，２０，３０は、それぞれ、指向性が可変のアレーアンテナ１１，２１，３１を備える。アレーアンテナ１１，２１，３１の各々は、電気的に指向性を切換え可能なアンテナである。そして、無線装置１０，２０，３０は、それぞれ、有線ケーブル５１～５３によって鍵生成装置５０に接続される。無線装置４０は、全方位性のアンテナ４１を備える。
【００２７】
無線装置１０は、アレーアンテナ１１の指向性が複数の指向性に切換えられたときにアレーアンテナ１１を介して無線装置４０と周波数ｆ１で電波を送受信し、無線装置４０から受信した複数の電波の強度に基づいて、後述する方法によって部分秘密鍵Ｋｓ１＿ｐａｒｔ１を生成する。そして、無線装置１０は、その生成した部分秘密鍵Ｋｓ１＿ｐａｒｔ１を有線ケーブル５１を介して鍵生成装置５０へ送信する。また、無線装置１０は、鍵生成装置５０によって生成された秘密鍵Ｋｓ１を有線ケーブル５１を介して受信し、その受信した秘密鍵Ｋｓ１を用いて無線装置４０と無線通信を行なう。
【００２８】
無線装置２０は、アレーアンテナ２１の指向性が複数の指向性に切換えられたときにアレーアンテナ２１を介して無線装置４０と周波数ｆ２（≠ｆ１）で電波を送受信し、無線装置４０から受信した複数の電波の強度に基づいて、後述する方法によって部分秘密鍵Ｋｓ１＿ｐａｒｔ２を生成する。そして、無線装置２０は、その生成した部分秘密鍵Ｋｓ１＿ｐａｒｔ２を有線ケーブル５２を介して鍵生成装置５０へ送信する。また、無線装置２０は、鍵生成装置５０によって生成された秘密鍵Ｋｓ１を有線ケーブル５２を介して受信し、その受信した秘密鍵Ｋｓ１を用いて無線装置４０と無線通信を行なう。
【００２９】
無線装置３０は、アレーアンテナ３１の指向性が複数の指向性に切換えられたときにアレーアンテナ３１を介して無線装置４０と周波数ｆ３（≠ｆ２≠ｆ１）で電波を送受信し、無線装置４０から受信した複数の電波の強度に基づいて、後述する方法によって部分秘密鍵Ｋｓ１＿ｐａｒｔ３を生成する。そして、無線装置３０は、その生成した部分秘密鍵Ｋｓ１＿ｐａｒｔ３を有線ケーブル５３を介して鍵生成装置５０へ送信する。また、無線装置３０は、鍵生成装置５０によって生成された秘密鍵Ｋｓ１を有線ケーブル５３を介して受信し、その受信した秘密鍵Ｋｓ１を用いて無線装置４０と無線通信を行なう。
【００３０】
無線装置４０は、アンテナ４１を介して無線装置１０，２０，３０との間で電波を順次送受信する。この場合、無線装置４０は、それぞれ、周波数ｆ１，ｆ２，ｆ３を用いて無線装置１０，２０，３０との間で電波を送受信する。そして、無線装置４０は、無線装置１０，２０，３０から順次受信した複数の電波の強度に基づいて、後述する方法によって３個の部分秘密鍵Ｋｓ２＿ｐａｒｔ１～Ｋｓ２＿ｐａｒｔ３を生成し、その生成した３個の部分秘密鍵Ｋｓ２＿ｐａｒｔ１～Ｋｓ２＿ｐａｒｔ３を組合わせて秘密鍵Ｋｓ２を生成する。また、無線装置４０は、生成した秘密鍵Ｋｓ２を用いて無線装置１０，２０，３０と無線通信を行なう。
【００３１】
鍵生成装置５０は、無線装置１０，２０，３０から３個の部分秘密鍵Ｋｓ１＿ｐａｒｔ１～Ｋｓ１＿ｐａｒｔ３を受信し、その受信した３個の部分秘密鍵Ｋｓ１＿ｐａｒｔ１～

Ｋｓ１＿ｐａｒｔ３を組合わせて秘密鍵Ｋｓ１を生成する。そして、鍵生成装置５０は、その生成した秘密鍵Ｋｓ１をそれぞれ有線ケーブル５１～５３を介して無線装置１０，２０，３０へ送信する。

【００３２】

無線装置１０と無線装置４０との間で無線通信が行われる場合、電波は、無線装置１０のアレーアンテナ１１と無線装置４０のアンテナ４１との間を直接伝搬したり、中間物（図示せず）による影響を受けて伝搬する。中間物としては、反射物及び障害物が想定される。中間物が反射物である場合、無線装置１０のアレーアンテナ１１または無線装置４０のアンテナ４１から出射した電波は、中間物によって反射されて無線装置４０のアンテナ４１または無線装置１０のアレーアンテナ１１へ伝搬する。また、中間物が障害物である場合、無線装置１０のアレーアンテナ１１または無線装置４０のアンテナ４１から出射した電波は、中間物によって回折されて無線装置４０のアンテナ４１または無線装置１０のアレーアンテナ１１へ伝搬する。

【００３３】

また、無線装置２０，３０と無線装置４０との間で無線通信が行なわれる場合も、電波は、無線装置１０と無線装置４０との間で通信が行なわれる場合と同様にアレーアンテナ２１，３１とアンテナ４１との間を直接伝搬したり、中間物による影響を受けて伝搬する。

【００３４】

このように、電波は、無線装置１０，２０，３０のアレーアンテナ１１，２１，３１と無線装置４０のアンテナ４１との間を直接伝搬したり、中間物による反射を受けて反射波として伝搬したり、中間物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１０，２０，３０のアレーアンテナ１１，２１，３１から無線装置４０のアンテナ４１（または無線装置４０のアンテナ４１から無線装置１０，２０，３０のアレーアンテナ１１，２１，３１）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のアレーアンテナ１１，２１，３１から無線装置４０のアンテナ４１（または無線装置４０のアンテナ４１から無線装置１０，２０，３０のアレーアンテナ１１，２１，３１）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１０，２０，３０と無線装置４０との間の伝送路の特性が決定される。

【００３５】

この発明においては、無線装置１０，２０，３０と無線装置４０との間で通信が行なわれる場合、アレーアンテナ１１，２１，３１の指向性を複数の指向性に変えて時分割復信（ＴＤＤ：Ｔｉｍｅ　Ｄｉｖｉｓｉｏｎ　Ｄｕｐｌｅｘ）等により所定のデータが無線装置１０，２０，３０と無線装置４０との間で送受信される。そして、無線装置１０，２０，３０は、アレーアンテナ１１，２１，３１の指向性を複数の指向性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を後述する方法によって生成し、その生成した受信信号プロファイルＲＳＳＩに基づいて後述する方法によって部分秘密鍵を生成し、その生成した部分秘密鍵をそれぞれ有線ケーブル５１～５３を介して鍵生成装置５０へ送信する。鍵生成装置５０は、無線装置１０，２０，３０から受信した部分秘密鍵を組合わせて秘密鍵を生成する。

【００３６】

また、無線装置４０は、アレーアンテナ１１，２１，３１の指向性が複数の指向性に変えられ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を後述する方法によって生成し、その生成した受信信号プロファイルＲＳＳＩに基づいて後述する方法によって秘密鍵を生成する。

【００３７】

秘密鍵が無線装置４０および鍵生成装置５０において生成されると、無線装置１０，２０，３０は、鍵生成装置５０によって生成され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秘密鍵によって復号して情報を取得する。また、無線装置４０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秘密鍵によって復号して情報を取得する。この場合、盗聴装置（図示せず）は、無線装置１０，２０，３０，４０の近傍で無線通信を傍受するが、無線装置４０および鍵生成装置５０における部分秘密鍵の組合せ方法を検知できないので、無線装置４０および鍵生成装置５０において生成された秘密鍵を盗聴することができない。

【００３８】

図２は、図１に示すアレーアンテナ１１の斜視図である。アレーアンテナ１１は、アンテナ素子１１１～１１７を備える。アンテナ素子１１１～１１６は、無給電素子であり、アンテナ素子１１７は、給電素子である。アンテナ素子１１１～１１６は、アンテナ素子１１７の周りに略円形に等間隔に配置される。そして、アレーアンテナ１１が送受信する電波の波長をλとした場合、無給電素子であるアンテナ素子１１１～１１６と給電素子であるアンテナ素子１１７との間隔は、例えば、λ／４に設定される。

【００３９】

無給電素子であるアンテナ素子１１１～１１６には、可変容量素子であるバラクタダイオード（図示省略）が個々に装荷され、その装荷された各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１１は、適応ビーム形成が可能である。

【００４０】

即ち、アレーアンテナ１１は、各バラクタダイオードに印加される直流電圧を変えることによってその指向性が変えられる。従って、アレーアンテナ１１は、電気的に指向性を切換え可能なアンテナである。

【００４１】

なお、図１に示すアレーアンテナ２１，３１の各々も、図２に示すアレーアンテナ１１と同じ構造からなり、指向性が変えられる。

【００４２】

図３は、指向性を切換え可能なアレーアンテナ１１を搭載した無線装置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、指向性設定部２２０とを含む。

【００４３】

信号発生部１１０は、秘密鍵を生成するときに無線装置４０へ送信するための所定のデータからなるパケットを発生し、その発生したパケットを送信処理部１２０へ出力する。

【００４４】

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。そして、送信処理部１２０は、アンテナ部１３０を介して周波数ｆ１，ｆ２，ｆ３の各々でキャリアセンスを行ない、無線装置１０以外の無線装置２０，３０，４０が無線通信を行なっていないことを確認すると、信号発生部１１０からのパケットを周波数ｆ１で変調し、その変調したパケットをアンテナ部１３０を介して送信する。

【００４５】

アンテナ部１３０は、図１に示すアレーアンテナ１１を主構成要素とし、送信処理部１２０からのパケットを無線装置４０へ送信し、無線装置４０からのパケット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。

【００４６】

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データまたは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。

【００４７】

プロファイル生成部１５０は、アンテナ部１３０を構成しているアレーアンテナ１１の指向性が複数の指向性に切換えられ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後述する方法によって検出する。そして、プロファイル生成部１５０は、検出した複数の電波強度からなる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を鍵作成部１６０へ出力する。
【００４８】
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、後述する方法によって、ビット列からなる部分秘密鍵Ｋｓ１＿ｐａｒｔ１を作成する。そして、鍵作成部１６０は、作成した部分秘密鍵Ｋｓ１＿ｐａｒｔ１を有線ケーブル５１を介して鍵生成装置５０へ送信する。
【００４９】
鍵一致確認部１７０は、鍵生成装置５０において後述する方法によって生成された秘密鍵Ｋｓ１を有線ケーブル５１を介して受信する。そして、鍵一致確認部１７０は、所定のデータからなるパケットを送信処理部１２０、アンテナ部１３０及び受信処理部１４０を介して無線装置４０と送受信し、鍵生成装置５０によって作成された秘密鍵Ｋｓ１が無線装置４０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に一致することを確認したとき、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を生成して送信処理部１２０および鍵一致化部１９０へ出力する。
【００５０】
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４０との通信の間だけ記憶するようにしてもよい。
【００５１】
鍵一致化部１９０は、鍵生成装置５０において後述する方法によって生成された秘密鍵Ｋｓ１を有線ケーブル５１を介して受信する。そして、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。鍵一致化部１９０は、秘密鍵Ｋｓ１が秘密鍵Ｋｓ２に一致することを確認すると、秘密鍵Ｋｓ１を鍵記憶部１８０に記憶する。
【００５２】
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によって暗号化して送信処理部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からの秘密鍵Ｋｓ１によって復号して受信データを生成する。
【００５３】
指向性設定部２２０は、アンテナ部１３０の指向性を設定する。また、指向性設定部２２０は、無線装置４０および鍵生成装置５０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１３０の指向性を順次切換える。
【００５４】
なお、図１に示す無線装置２０，３０の各々は、図３に示す無線装置１０と同じ構成からなる。
【００５５】
図４は、全方位性のアンテナ４１を搭載した無線装置４０の概略ブロック図である。無線装置４０は、図３で説明した無線装置１０の指向性設定部２２０を削除し、アンテナ部１３０をアンテナ部２３０に代え、鍵作成部１６０、鍵一致確認部１７０及び鍵一致化部１９０をそれぞれ鍵作成部１６０Ａ、鍵一致確認部１７０Ａ及び鍵一致化部１９０Ａに代えたものであり、その他は、無線装置１０と同じ構成からなる。
【００５６】
鍵作成部１６０Ａは、プロファイル生成部１５０から受信信号プロファイルＲＳＳＩを受けると、その受けた受信信号プロファイルＲＳＳＩに基づいて、後述する方法によって秘密鍵Ｋｓ２を作成する。そして、鍵作成部１６０Ａは、その作成した秘密鍵Ｋｓ２を鍵

一致確認部１７０Ａ及び鍵一致化部１９０Ａへ出力する。

【００５７】

鍵一致確認部１７０Ａは、鍵作成部１６０Ａから秘密鍵Ｋｓ２を受ける。そして、鍵一致確認部１７０Ａは、所定のデータからなるパケットを送信処理部１２０、アンテナ部２３０及び受信処理部１４０を介して無線装置１０，２０，３０と送受信し、無線装置４０において作成された秘密鍵Ｋｓ２が鍵生成装置５０において作成された秘密鍵Ｋｓ１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１７０Ａは、秘密鍵Ｋｓ２が秘密鍵Ｋｓ１に一致することを確認したとき、秘密鍵Ｋｓ２を鍵記憶部１８０に記憶する。また、鍵一致確認部１７０Ａは、秘密鍵Ｋｓ２が秘密鍵Ｋｓ１に不一致であることを確認したとき、不一致信号ＮＭＴＨを生成して送信処理部１２０及び鍵一致化部１９０Ａへ出力する。

【００５８】

鍵一致化部１９０Ａは、鍵一致確認部１７０Ａ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Ｋｓ２を秘密鍵Ｋｓ１に一致させる。そして、鍵一致化部１９０Ａは、一致させた秘密鍵が秘密鍵Ｋｓ１に一致することを鍵一致確認部１７０Ａにおける方法と同じ方法によって確認する。鍵一致化部１９０Ａは、秘密鍵Ｋｓ２が秘密鍵Ｋｓ１に一致することを確認すると、秘密鍵Ｋｓ２を鍵記憶部１８０に記憶する。

【００５９】

なお、無線装置４０においては、鍵記憶部１８０は、鍵一致確認部１７０Ａ及び鍵一致化部１９０Ａからの秘密鍵Ｋｓ２を記憶する。

【００６０】

アンテナ部２３０は、図１に示すアンテナ４１からなる。そして、アンテナ部２３０は、送信処理部１２０からのデータを無線装置１０，２０，３０へ送信し、無線装置１０，２０，３０からのデータを受信して受信処理部１４０またはプロファイル生成部１５０へ出力する。

【００６１】

図５は、図３に示す指向性設定部２２０の概略ブロック図である。指向性設定部２２０は、バラクタダイオード２２１～２２６と、制御電圧発生回路２２７とを含む。バラクタダイオード２２１～２２６は、それぞれ、図１に示すアンテナ素子１１１～１１６に装荷される。

【００６２】

制御電圧発生回路２２７は、制御電圧セットＣＬＶ１～ＣＬＶｎ（ｎは２以上の整数）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２２１～２２６へ順次出力する。

【００６３】

制御電圧セットＣＬＶ１～ＣＬＶｎの各々は、６個のバラクタダイオード２２１～２２６に対応して６個の電圧値Ｖ１～Ｖ６からなる。そして、バラクタダイオード２２１～２２６は、制御電圧セットＣＬＶ１を受けると、その受けた制御電圧セットＣＬＶ１に応じて、無給電素子であるアンテナ素子１１１～１１６に装荷される容量を所定の容量に設定し、アレーアンテナ１１，２１，３１の指向性を１つの指向性に設定する。また、バラクタダイオード２２１～２２６は、制御電圧セットＣＬＶ２を受けると、その受けた制御電圧セットＣＬＶ２に応じて、無給電素子であるアンテナ素子１１１～１１６に装荷される容量を所定の容量に設定し、アレーアンテナ１１，２１，３１の指向性を別の指向性に設定する。従って、バラクタダイオード１１１～１１６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１１１～１１６に装荷される容量を順次変え、アレーアンテナ１１，２１，３１の指向性をｎ個の指向性に順次変える。

【００６４】

図６は、図３に示す鍵一致確認部１７０および図４に示す鍵一致確認部１７０Ａ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の鍵一致確認部１７０及び無線装置

４０の鍵一致確認部１７０Ａは、同じ構成からなるが、図６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４０においてはデータ発生部１７１のみを示す。

【００６５】

無線装置１０のデータ発生部１７１は、鍵生成装置５０から秘密鍵Ｋｓ１を受信すると、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。

【００６６】

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。

【００６７】

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４０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。

【００６８】

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へ出力するとともに、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４０へ送信する。

【００６９】

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、鍵生成装置５０から受けた秘密鍵Ｋｓ１を鍵記憶部１８０へ出力し、記憶する。

【００７０】

なお、無線装置４０の鍵一致確認部１７０Ａは、無線装置１０の鍵一致確認部１７０と同じ構成からなり、データ発生部１７１及びデータ比較部１７２は、無線装置１０の鍵一致確認部１７０のデータ発生部１７１及びデータ比較部１７２と同じ機能を果たす。そして、鍵一致確認部１７０Ａの結果処理部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１６０Ａから受けた秘密鍵Ｋｓ２を鍵記憶部１８０へ出力し、記憶する。

【００７１】

図７は、図３に示す鍵一致化部１９０および図４に示す鍵一致化部１９０Ａ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。

【００７２】

なお、無線装置１０の鍵一致化部１９０及び無線装置４０の鍵一致化部１９０Ａは、同じ構成からなるが、図７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４０においては擬似シンドローム作成部１９１のみを示す。

【００７３】

無線装置１０の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、鍵生成装置５０から受けた秘密鍵Ｋｓ１のシンドロームｓ１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ｘ１を検出し、ビットパターンｘ１に対して検査行列Ｈを乗算してシンドロームｓ１＝ｘ１$H^T$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ｘ１を鍵不一致訂正部１９３へ出力し、演算したシンドロームｓ１＝ｘ１Ｈ$^{T}$を不一致ビット検出部１９２へ出力する。

【００７４】

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。

【００７５】

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４０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＝ｘ２Ｈ$^{T}$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。

【００７６】

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＝ｘ１－ｘ２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。

【００７７】

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≠０のとき）、鍵不一致のビットパターンｅをｓ＝ｅＨ$^{T}$から導出し、その導出したビットパターンｅを鍵不一致訂正部１９３へ出力する。

【００７８】

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ｘ１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ｘ１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ｘ２＝ｘ１－ｅを演算する。

【００７９】

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。

【００８０】

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。

【００８１】

データ発生部１９４は、一致化後のビットパターン（鍵）ｘ２＝ｘ１－ｅを鍵不一致訂正部１９３から受けると、ビットパターン（鍵）ｘ２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４０へ送信する。

【００８２】

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。

【００８３】

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４０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。

【００８４】

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。

【００８５】

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４０へ送信する。

【００８６】

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から受けたビットパターン（鍵）ｘ２＝ｘ１－ｅを鍵記憶部１８０へ出力し、記憶する。

【００８７】

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。

【００８８】

図８は、受信信号強度の概念図である。指向性設定部２２０の制御電圧発生回路２２７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２２１～２２６へ出力する。この場合、電圧Ｖ１～Ｖ６は、それぞれ、アンテナ素子１１１～１１６に装荷される容量を変えるための電圧であり、例えば、－２０～０Ｖの範囲の直流電圧からなる。そして、制御電圧発生回路２２７は、電圧Ｖ１～Ｖ６の各々の電圧値を８ビットのデータにより変えることによって各制御電圧セットＣＬＶ１～ＣＬＶｎを決定し、その決定した各制御電圧セットＣＬＶ１～ＣＬＶｎをバラクタダイオード２２１～２２６へ出力する。

【００８９】

バラクタダイオード２２１～２２６は、電圧［Ｖ１１，Ｖ１２，Ｖ１３，Ｖ１４，Ｖ１５，Ｖ１６］からなる制御電圧セットＣＬＶ１に応じてアレーアンテナ１１，２１，３１の指向性をある１つの指向性に設定する。また、バラクタダイオード２２１～２２６は、電圧［Ｖ２１，Ｖ２２，Ｖ２３，Ｖ２４，Ｖ２５，Ｖ２６］からなる制御電圧セットＣＬＶ２に応じてアレーアンテナ１１，２１，３１の指向性を別の指向性に設定する。以下、同様にして、バラクタダイオード２２１～２２６は、それぞれ、電圧［Ｖ３１，Ｖ３２，Ｖ３３，Ｖ３４，Ｖ３５，Ｖ３６］～［Ｖｎ１，Ｖｎ２，Ｖｎ３，Ｖｎ４，Ｖｎ５，Ｖｎ６］からなる制御電圧セットＣＬＶ３～ＣＬＶｎに応じてアレーアンテナ１１，２１，３１の指向性を順次切換える。

【００９０】

このように、バラクタダイオード２２１～２２６は、制御電圧セットＣＬＶ１～ＣＬＶｎに応じてアレーアンテナ１１，２１，３１の指向性をｎ個の指向性に順次切換える。この場合、制御電圧発生回路２２７は、各パケットＰＫＴｎごとにアレーアンテナ１１，２１，３１の指向性が切換えられるように制御電圧セットＣＬＶ１～ＣＬＶｎをバラクタダイオード２２１～２２６へ順次出力し、バラクタダイオード２２１～２２６は、各パケットＰＫＴｎごとにアレーアンテナ１１，２１，３１の指向性を切換える。

【００９１】

そして、アレーアンテナ１１，２１，３１は、指向性をｎ個の指向性に順次切換えながら各指向性において１個のパケットを送信する。

【００９２】

その結果、無線装置１０，２０，３０のプロファイル生成部１５０は、アレーアンテナ１１，２１，３１の指向性がｎ個の指向性に切換えられたときのｎ個の電波をアンテナ部１３０から受ける。

【００９３】

そして、無線装置１０，２０，３０のプロファイル生成部１５０は、アレーアンテナ１１，２１，３１の指向性がｎ個の指向性に切換えられたときのｎ個の電波に対応するｎ個の電波強度ＷＩ１～ＷＩｎを検出する。

【００９４】

以下、秘密鍵の作成方法について説明する。図９は、受信信号プロファイルの概念図である。秘密鍵Ｋｓ１，Ｋｓ２が生成される場合、無線装置４０は、例えば、１６個のパケ

ットＰＫＴ１～ＰＫＴ１６を無線装置１０，２０，３０との間で、順次、相互に送受信する。この場合、例えば、無線装置４０は、無線装置１０、無線装置２０、無線装置３０、無線装置１０、無線装置２０、・・・の順に１６個のパケットＰＫＴ１～ＰＫＴ１６を相互に送受信する。また、アレーアンテナ１１，２１，３１の指向性は、一定時間ごとに１６個の指向性に順次切換えられる。

【００９５】

そして、無線装置１０のプロファイル生成部１５０は、一定時間ごとにアンテナ部１３０からｎ（＝１６）個の電波を受け、その受けたｎ（＝１６）個の電波に対応するｎ（＝１６）個の電波強度ＷＩ１＿１０～ＷＩｎ＿１０（＝ＲＳＳＩ１～ＲＳＳＩ１６またはＲＳＳＩ４９～ＲＳＳＩ６４または・・・）を検出する。その後、無線装置１０のプロファイル生成部１５０は、一定時間ごとにｎ（＝１６）個の電波強度ＷＩ１＿１０～ＷＩｎ＿１０（＝ＲＳＳＩ１～ＲＳＳＩ１６またはＲＳＳＩ４９～ＲＳＳＩ６４または・・・）を順次配列した受信信号プロファイルＲＳＳＩ＿１０を生成し、その生成した受信信号プロファイルＲＳＳＩ＿１０を鍵作成部１６０へ出力する。無線装置１０のプロファイル生成部１５０は、一定時間ごとに受信信号プロファイルＲＳＳＩ＿１０の生成を繰り返し行なう。

【００９６】

また、無線装置２０のプロファイル生成部１５０は、一定時間ごとにアンテナ部１３０からｎ（＝１６）個の電波を受け、その受けたｎ（＝１６）個の電波に対応するｎ（＝１６）個の電波強度ＷＩ１＿２０～ＷＩｎ＿２０（＝ＲＳＳＩ１７～ＲＳＳＩ３２；・・・）を検出する。その後、無線装置２０のプロファイル生成部１５０は、一定時間ごとにｎ（＝１６）個の電波強度ＷＩ１＿２０～ＷＩｎ＿２０（＝ＲＳＳＩ１７～ＲＳＳＩ３２；・・・）を順次配列した受信信号プロファイルＲＳＳＩ＿２０を生成し、その生成した受信信号プロファイルＲＳＳＩ＿２０を鍵作成部１６０へ出力する。無線装置２０のプロファイル生成部１５０は、一定時間ごとに受信信号プロファイルＲＳＳＩ＿２０の生成を繰り返し行なう。

【００９７】

更に、無線装置３０のプロファイル生成部１５０は、一定時間ごとにアンテナ部１３０からｎ（＝１６）個の電波を受け、その受けたｎ（＝１６）個の電波に対応するｎ（＝１６）個の電波強度ＷＩ１＿３０～ＷＩｎ＿３０（＝ＲＳＳＩ３３～ＲＳＳＩ４８；・・・）を検出する。その後、無線装置３０のプロファイル生成部１５０は、一定時間ごとにｎ（＝１６）個の電波強度ＷＩ１＿３０～ＷＩｎ＿３０（＝ＲＳＳＩ３３～ＲＳＳＩ４８；・・・）を順次配列した受信信号プロファイルＲＳＳＩ＿３０を生成し、その生成した受信信号プロファイルＲＳＳＩ＿３０を鍵作成部１６０へ出力する。無線装置３０のプロファイル生成部１５０は、一定時間ごとに受信信号プロファイルＲＳＳＩ＿３０の生成を繰り返し行なう。

【００９８】

更に、無線装置４０のプロファイル生成部１５０は、アンテナ部２３０からｎ（＝３８４）個の電波を受け、その受けたｎ（＝３８４）個の電波に対応するｎ（＝３８４）個の電波強度ＷＩ１＿４０～ＷＩｎ＿４０（＝ＲＳＳＩ１～ＲＳＳＩ３８４）を検出する。そして、無線装置４０のプロファイル生成部１５０は、ｎ（＝３８４）個の電波強度ＷＩ１＿４０～ＷＩｎ＿４０（＝ＲＳＳＩ１～ＲＳＳＩ３８４）を順次配列した受信信号プロファイルＲＳＳＩ＿４０を生成し、その生成した受信信号プロファイルＲＳＳＩ＿４０を鍵作成部１６０Ａへ出力する。

【００９９】

無線装置１０，２０，３０の鍵作成部１６０は、それぞれ、受信信号プロファイルＲＳＳＩ＿１０，ＲＳＳＩ＿２０，ＲＳＳＩ＿３０を一定時間ごとにプロファイル生成部１５０から受け、その受けた受信信号プロファイルＲＳＳＩ＿１０，ＲＳＳＩ＿２０，ＲＳＳＩ＿３０に基づいて、以下に説明する方法によって、それぞれ、部分秘密鍵Ｋｓ１＿ｐａｒ１，Ｋｓ１＿ｐａｒｔ２，Ｋｓ１＿ｐａｒｔ３を生成する。

【０１００】
また、無線装置４０の鍵作成部１６０Ａは、受信信号プロファイルＲＳＳＩ＿４０をプロファイル生成部１５０から受け、その受けた受信信号プロファイルＲＳＳＩ＿４０に基づいて、以下に説明する方法によって秘密鍵Ｋｓ２を生成する。
【０１０１】
更に、鍵生成装置５０は、一定時間ごとに無線装置１０，２０，３０からそれぞれ部分秘密鍵Ｋｓ１＿ｐａｒｔ１，Ｋｓ１＿ｐａｒｔ２，Ｋｓ１＿ｐａｒｔ３を受け、その受けた部分秘密鍵Ｋｓ１＿ｐａｒｔ１，Ｋｓ１＿ｐａｒｔ２，Ｋｓ１＿ｐａｒｔ３に基づいて、以下に説明する方法によって秘密鍵Ｋｓ１を生成する。
【０１０２】
［秘密鍵の作成方法１］
図１０は、鍵生成装置５０における秘密鍵の作成方法を示す図である。無線装置１０の鍵作成部１６０は、受信信号強度ＲＳＳＩ１～ＲＳＳＩ１６からなる受信信号プロファイルＲＳＳＩ＿１０をプロファイル生成部１５０から受け、その受けた受信信号プロファイルＲＳＳＩ＿１０を構成する１６個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ１６の平均値ＲＳＳＩ＿ａｖｅ１を演算する。そして、無線装置１０の鍵作成部１６０は、１６個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ１６のうち、平均値ＲＳＳＩ＿ａｖｅ１に近い値を有する８個の受信信号強度を破棄し、残りの８個の受信信号強度を平均値ＲＳＳＩ＿ａｖｅ１で２値化してビット列［Ｂｉｔ１，・・・，Ｂｉｔ８］からなる部分秘密鍵Ｋｓ１＿ｐａｒｔ１－１を作成する。この場合、無線装置１０の鍵作成部１６０は、残りの８個の受信信号強度の各々を平均値ＲＳＳＩ＿ａｖｅ１と比較し、受信信号強度が平均値ＲＳＳＩ＿ａｖｅ１よりも大きいとき、その受信信号強度を“１”に変換し、受信信号強度が平均値ＲＳＳＩ＿ａｖｅ１よりも小さいとき、その受信信号強度を“０”に変換してビット列［Ｂｉｔ１，・・・，Ｂｉｔ８］からなる部分秘密鍵Ｋｓ１＿ｐａｒｔ１－１を作成する。
【０１０３】
無線装置１０の鍵作成部１６０は、部分秘密鍵Ｋｓ１＿ｐａｒｔ１－１を作成すると、その作成した部分秘密鍵Ｋｓ１＿ｐａｒｔ１－１を有線ケーブル５１を介して鍵生成装置５０へ送信する。
【０１０４】
また、無線装置２０の鍵作成部１６０は、受信信号強度ＲＳＳＩ１７～ＲＳＳＩ３２からなる受信信号プロファイルＲＳＳＩ＿２０をプロファイル生成部１５０から受け、その受けた受信信号プロファイルＲＳＳＩ＿２０を構成する１６個の受信信号強度ＲＳＳＩ１７～ＲＳＳＩ３２の平均値ＲＳＳＩ＿ａｖｅ２を演算する。そして、無線装置２０の鍵作成部１６０は、１６個の受信信号強度ＲＳＳＩ１７～ＲＳＳＩ３２のうち、平均値ＲＳＳＩ＿ａｖｅ２に近い値を有する８個の受信信号強度を破棄し、残りの８個の受信信号強度を平均値ＲＳＳＩ＿ａｖｅ２と比較して上述した方法によってビット列［Ｂｉｔ９，・・・，Ｂｉｔ１６］からなる部分秘密鍵Ｋｓ１＿ｐａｒｔ２－１を作成する。無線装置２０の鍵作成部１６０は、部分秘密鍵Ｋｓ１＿ｐａｒｔ２－１を作成すると、その作成した部分秘密鍵Ｋｓ１＿ｐａｒｔ２－１を有線ケーブル５２を介して鍵生成装置５０へ送信する。
【０１０５】
更に、無線装置３０の鍵作成部１６０は、受信信号強度ＲＳＳＩ３３～ＲＳＳＩ４８からなる受信信号プロファイルＲＳＳＩ＿３０をプロファイル生成部１５０から受け、その受けた受信信号プロファイルＲＳＳＩ＿３０を構成する１６個の受信信号強度ＲＳＳＩ３３～ＲＳＳＩ４８の平均値ＲＳＳＩ＿ａｖｅ３を演算する。そして、無線装置３０の鍵作成部１６０は、１６個の受信信号強度ＲＳＳＩ３３～ＲＳＳＩ４８のうち、平均値ＲＳＳＩ＿ａｖｅ３に近い値を有する８個の受信信号強度を破棄し、残りの８個の受信信号強度を平均値ＲＳＳＩ＿ａｖｅ３と比較して上述した方法によってビット列［Ｂｉｔ１７，・・・，Ｂｉｔ２４］からなる部分秘密鍵Ｋｓ１＿ｐａｒｔ３－１を作成する。無線装置３０の鍵作成部１６０は、部分秘密鍵Ｋｓ１＿ｐａｒｔ３－１を作成すると、その作成した

部分秘密鍵Ｋｓ１＿ｐａｒｔ３－１を有線ケーブル５３を介して鍵生成装置５０へ送信する。

【０１０６】

その後、無線装置１０の鍵作成部１６０は、受信信号強度ＲＳＳＩ４９～ＲＳＳＩ６４からなる受信信号プロファイルＲＳＳＩ＿１０をプロファイル生成部１５０から受け、その受けた受信信号プロファイルＲＳＳＩ＿１０を構成する１６個の受信信号強度ＲＳＳＩ４９～ＲＳＳＩ６４に基づいて、上述した方法によって部分秘密鍵Ｋｓ１＿ｐａｒｔ１－２を作成し、その作成した部分秘密鍵Ｋｓ１＿ｐａｒｔ１－２を有線ケーブル５１を介して鍵生成装置５０へ送信する。

【０１０７】

以下、同様にして、無線装置１０，２０，３０は、それぞれ、部分秘密鍵Ｋｓ１＿ｐａｒｔ１，Ｋｓ１＿ｐａｒｔ２，Ｋｓ１＿ｐａｒｔ３を作成し、その作成した部分秘密鍵Ｋｓ１＿ｐａｒｔ１，Ｋｓ１＿ｐａｒｔ２，Ｋｓ１＿ｐａｒｔ３をそれぞれ有線ケーブル５１～５３を介して鍵生成装置５０へ送信する。

【０１０８】

鍵生成装置５０は、無線装置１０，２０，３０から部分秘密鍵Ｋｓ１＿ｐａｒｔ１－１，Ｋｓ１＿ｐａｒｔ２－１，Ｋｓ１＿ｐａｒｔ３－１，Ｋｓ１＿ｐａｒｔ１－２，・・・を順次受け、その受けた部分秘密鍵Ｋｓ１＿ｐａｒｔ１－１，Ｋｓ１＿ｐａｒｔ２－１，Ｋｓ１＿ｐａｒｔ３－１，Ｋｓ１＿ｐａｒｔ１－２，・・・を順に配列して１２８ビットのビット列［Ｂｉｔ１～Ｂｉｔ１２８］からなる秘密鍵Ｋｓ１を作成する。

【０１０９】

図１１は、全方位性のアンテナ４１を搭載した無線装置４０における秘密鍵の作成方法を示す図である。無線装置４０の鍵作成部１６０Ａは、アレーアンテナ１１の指向性が１６個の指向性に切換えられたときに無線装置１０から受信した電波の受信信号強度である１６個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ１６をプロファイル生成部１５０から受け、その受けた１６個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ１６の平均値ＲＳＳＩ＿ａｖｅ１を演算し、１６個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ１６のうち、平均値ＲＳＳＩ＿ａｖｅ１に近い順に８個の受信信号強度を破棄し、残りの８個の受信信号強度を平均値ＲＳＳＩ＿ａｖｅ１と比較して上述した方法によってビット列［Ｂｉｔ１，・・・，Ｂｉｔ８］からなる部分秘密鍵Ｋｓ２＿ｐａｒｔ１を作成する。

【０１１０】

次に、無線装置４０の鍵作成部１６０Ａは、アレーアンテナ２１の指向性が１６個の指向性に切換えられたときに無線装置２０から受信した電波の受信信号強度である１６個の受信信号強度ＲＳＳＩ１７～ＲＳＳＩ３２をプロファイル生成部１５０から受け、その受けた１６個の受信信号強度ＲＳＳＩ１７～ＲＳＳＩ３２の平均値ＲＳＳＩ＿ａｖｅ２を演算し、１６個の受信信号強度ＲＳＳＩ１７～ＲＳＳＩ３２のうち、平均値ＲＳＳＩ＿ａｖｅ２に近い順に８個の受信信号強度を破棄し、残りの８個の受信信号強度を平均値ＲＳＳＩ＿ａｖｅ２と比較して上述した方法によってビット列［Ｂｉｔ９，・・・，Ｂｉｔ１６］からなる部分秘密鍵Ｋｓ２＿ｐａｒｔ２を作成する。

【０１１１】

その後、無線装置４０の鍵作成部１６０Ａは、アレーアンテナ３１の指向性が１６個の指向性に切換えられたときに無線装置３０から受信した電波の受信信号強度である１６個の受信信号強度ＲＳＳＩ３３～ＲＳＳＩ４８をプロファイル生成部１５０から受け、その受けた１６個の受信信号強度ＲＳＳＩ３３～ＲＳＳＩ４８の平均値ＲＳＳＩ＿ａｖｅ３を演算し、１６個の受信信号強度ＲＳＳＩ３３～ＲＳＳＩ４８のうち、平均値ＲＳＳＩ＿ａｖｅ３に近い順に８個の受信信号強度を破棄し、残りの８個の受信信号強度を平均値ＲＳＳＩ＿ａｖｅ３と比較して上述した方法によってビット列［Ｂｉｔ１７，・・・，Ｂｉｔ２４］からなる部分秘密鍵Ｋｓ２＿ｐａｒｔ３を作成する。

【０１１２】

引き続いて、無線装置４０の鍵作成部１６０Ａは、アレーアンテナ１１の指向性が１６

個の指向性に切換えられたときに無線装置１０から受信した電波の受信信号強度である１６個の受信信号強度ＲＳＳＩ４９～ＲＳＳＩ６４をプロファイル生成部１５０から受け、その受けた１６個の受信信号強度ＲＳＳＩ４９～ＲＳＳＩ６４の平均値ＲＳＳＩ＿ａｖｅ４を演算し、１６個の受信信号強度ＲＳＳＩ４９～ＲＳＳＩ６４のうち、平均値ＲＳＳＩ＿ａｖｅ４に近い順に８個の受信信号強度を破棄し、残りの８個の受信信号強度を平均値ＲＳＳＩ＿ａｖｅ４と比較して上述した方法によってビット列［Ｂｉｔ２５，・・・，Ｂｉｔ３２］からなる部分秘密鍵Ｋｓ２＿ｐａｒｔ４を作成する。

【０１１３】

以下、同様にして、無線装置４０の鍵作成部１６０Ａは、無線装置１０，２０，３０から、順次、１６個の電波を受信するごとに上述した方法によって部分秘密鍵Ｋｓ２＿ｐａｒｔ５，Ｋｓ２＿ｐａｒｔ６，・・・，Ｋｓ２＿ｐａｒｔ１６を作成する。

【０１１４】

そうすると、無線装置４０の鍵作成部１６０Ａは、作成した部分秘密鍵Ｋｓ２＿ｐａｒｔ１，Ｋｓ２＿ｐａｒｔ２，・・・，Ｋｓ２＿ｐａｒｔ１６を順に配列して秘密鍵Ｋｓ２を作成する。

【０１１５】

上述したように、無線装置１０，２０，３０は、それぞれ、アレーアンテナ１１，２１，３１の指向性が１６個の指向性に順次切換えられたときに無線装置４０から受信した１６個の電波に対応する１６個の受信信号強度に基づいて８ヒットのビット列からなる部分秘密鍵Ｋｓ１＿ｐａｒｔ１－１，Ｋｓ１＿ｐａｒｔ２－１，Ｋｓ１＿ｐａｒｔ３－１，Ｋｓ１＿ｐａｒｔ１－２，・・・を作成し、その作成した部分秘密鍵Ｋｓ１＿ｐａｒｔ１－１，Ｋｓ１＿ｐａｒｔ２－１，Ｋｓ１＿ｐａｒｔ３－１，Ｋｓ１＿ｐａｒｔ１－２，・・・をそれぞれ有線ケーブル５１～５３を介して鍵生成装置５０へ送信する。そして、鍵生成装置５０は、それぞれ、無線装置１０，２０，３０から受信した部分秘密鍵Ｋｓ１＿ｐａｒｔ１－１，Ｋｓ１＿ｐａｒｔ２－１，Ｋｓ１＿ｐａｒｔ３－１，Ｋｓ１＿ｐａｒｔ１－２，・・・を順に配列した秘密鍵Ｋｓ１を作成する。

【０１１６】

また、無線装置４０は、それぞれ、アレーアンテナ１１，２１，３１の指向性が１６個の指向性に順次切換えられたときに無線装置１０，２０，３０から受信した１６個の電波に対応する１６個の受信信号強度に基づいて８ビットのビット列からなる部分秘密鍵Ｋｓ２＿ｐａｒｔ１，Ｋｓ２＿ｐａｒｔ２，・・・，Ｋｓ２＿ｐａｒｔ１６を作成し、その作成した部分秘密鍵Ｋｓ２＿ｐａｒｔ１，Ｋｓ２＿ｐａｒｔ２，・・・，Ｋｓ２＿ｐａｒｔ１６を順に配列した秘密鍵Ｋｓ２を作成する。

【０１１７】

このように、無線装置１０，２０，３０および無線装置４０は、同じ複数の受信信号強度に基づいて、同じ方法によって同じ複数の部分秘密鍵を作成し、無線装置４０および鍵生成装置５０は、同じ複数の部分秘密鍵を同じ方法によって配列した秘密鍵Ｋｓ１，Ｋｓ２を作成する。

【０１１８】

従って、秘密鍵Ｋｓ１を秘密鍵Ｋｓ２に一致させることができる。つまり、無線装置４０および鍵生成装置５０は、同じ秘密鍵を共有できる。

【０１１９】

また、以上に説明した秘密鍵の作成方法１においては、無線装置１０および無線装置４０は、無線装置１０と無線装置４０との間の無線伝送路ＲＴ１を介して受信した１６個の電波に対応する１６個の受信信号強度ごとに平均値ＲＳＳＩ＿ａｖｅを演算し、その演算した平均値ＲＳＳＩ＿ａｖｅを用いてそれぞれ部分秘密鍵Ｋｓ１＿ｐａｒｔ１，Ｋｓ２＿ｐａｒｔ１を作成し、無線装置２０および無線装置４０は、無線装置２０と無線装置４０との間の無線伝送路ＲＴ２を介して受信した１６個の電波に対応する１６個の受信信号強度ごとに平均値ＲＳＳＩ＿ａｖｅを演算し、その演算した平均値ＲＳＳＩ＿ａｖｅを用いてそれぞれ部分秘密鍵Ｋｓ１＿ｐａｒｔ２，Ｋｓ２＿ｐａｒｔ２を作成し、無線装置３０

および無線装置４０は、無線装置３０と無線装置４０との間の無線伝送路ＲＴ３を介して受信した１６個の電波に対応する１６個の受信信号強度ごとに平均値ＲＳＳＩ＿ａｖｅを演算し、その演算した平均値ＲＳＳＩ＿ａｖｅを用いてそれぞれ部分秘密鍵Ｋｓ１＿ｐａｒｔ３，Ｋｓ２＿ｐａｒｔ３を作成する。

【０１２０】

従って、無線伝送路ＲＴ１～ＲＴ３の異なる無線通信特性を反映した部分秘密鍵Ｋｓ１＿ｐａｒｔ１～Ｋｓ１＿ｐａｒｔ３，Ｋｓ２＿ｐａｒｔ１～Ｋｓ２＿ｐａｒｔ３を作成できる。

【０１２１】

更に、秘密鍵Ｋｓ１は、異なる無線通信特性を反映した部分秘密鍵Ｋｓ１＿ｐａｒｔ１～Ｋｓ１＿ｐａｒｔ３を組合わせて作成され、秘密鍵Ｋｓ２は、異なる無線通信特性を反映した部分秘密鍵Ｋｓ２＿ｐａｒｔ１～Ｋｓ２＿ｐａｒｔ３を組合わせて作成される。従って、秘密鍵Ｋｓ１，Ｋｓ２における“１”または“０”の配列状態をダイナミックに変えることができる。その結果、秘密鍵Ｋｓ１，Ｋｓ２の盗聴を抑制できる。

【０１２２】

［秘密鍵の作成方法２］

図１２は、鍵生成装置５０における秘密鍵の他の作成方法を示す図である。無線装置１０は、アレーアンテナ１１の指向性が１６個の指向性に切換えられたときに無線装置４０から１６個の電波を受信し、その受信した１６個の電波の強度である１６個の受信信号強度ＲＳＳ１～ＲＳＳＩ１６を検出して鍵生成装置５０へ送信する。

【０１２３】

また、無線装置２０は、アレーアンテナ２１の指向性が１６個の指向性に切換えられたときに無線装置４０から１６個の電波を受信し、その受信した１６個の電波の強度である１６個の受信信号強度ＲＳＳＩ１７～ＲＳＳＩ３２を検出して鍵生成装置５０へ送信する。

【０１２４】

更に、無線装置３０は、アレーアンテナ３１の指向性が１６個の指向性に切換えられたときに無線装置４０から１６個の電波を受信し、その受信した１６個の電波の強度である１６個の受信信号強度ＲＳＳＩ３３～ＲＳＳＩ４８を検出して鍵生成装置５０へ送信する。

【０１２５】

更に、無線装置１０は、アレーアンテナ１１の指向性が１６個の指向性に切換えられたときに無線装置４０から１６個の電波を受信し、その受信した１６個の電波の強度である１６個の受信信号強度ＲＳＳＩ４９～ＲＳＳＩ６４を検出して鍵生成装置５０へ送信する。

【０１２６】

以下、無線装置１０，２０，３０は、順次、アレーアンテナ１１，２１，３１の指向性が１６個の指向性に切換えられたときに無線装置４０から１６個の電波を受信し、その受信した１６個の電波の強度である１６個の受信信号強度を検出して鍵生成装置５０へ送信する。そして、無線装置３０が無線装置４０から受信した１６個の電波の強度が１６個の受信信号強度ＲＳＳＩ３６９～ＲＳＳＩ３８４になると、無線装置１０，２０，３０と無線装置４０との間の無線通信は、終了する。

【０１２７】

鍵生成装置５０は、無線装置１０からの１６個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ１６、無線装置２０からの１６個の受信信号強度ＲＳＳＩ１７～ＲＳＳＩ３２、無線装置３０からの１６個の受信信号強度ＲＳＳＩ３３～ＲＳＳＩ４８、無線装置１０からの１６個の受信信号強度ＲＳＳＩ４９～ＲＳＳＩ６４、・・・、無線装置３０からの１６個の受信信号強度ＲＳＳＩ３６９～ＲＳＳＩ３８４を順次受信する。そして、鍵生成装置５０は、その受信した３８４個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ１６，ＲＳＳＩ１７～ＲＳＳＩ３２，ＲＳＳＩ３３～ＲＳＳＩ４８，・・・，ＲＳＳＩ３６９～ＲＳＳＩ３８４を直列

に配列し、その直列に配列した３８４個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ３８４の平均値ＲＳＳＩ＿ａｖｅを演算する。その後、鍵生成装置５０は、３８４個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ３８４のうち、平均値ＲＳＳＩ＿ａｖｅに近い順に２５６個の受信信号強度を削除し、残りの１２８個の受信信号強度ＲＳＳＩ１’～ＲＳＳＩ１２８’を平均値ＲＳＳＩ＿ａｖｅで多値化して１２８個のビットＢｉｔ１～Ｂｉｔ１２８からなる秘密鍵Ｋｓ１を生成する。

【０１２８】

なお、上述した方法によって秘密鍵Ｋｓ１を作成する場合、無線装置１０，２０，３０のプロファイル生成部１５０は、それぞれ、有線ケーブル５１～５３に接続されている。

【０１２９】

図１３は、全方位性のアンテナ４１を搭載した無線装置４０における秘密鍵の他の作成方法を示す図である。無線装置４０は、アレーアンテナ１１の指向性が１６個の指向性に切換えられたときに無線装置１０から１６個の電波を受信し、その受信した１６個の電波の強度である１６個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ１６を検出する。

【０１３０】

また、無線装置４０は、アレーアンテナ２１の指向性が１６個の指向性に切換えられたときに無線装置２０から１６個の電波を受信し、その受信した１６個の電波の強度である１６個の受信信号強度ＲＳＳＩ１７～ＲＳＳＩ３２を検出する。

【０１３１】

更に、無線装置４０は、アレーアンテナ３１の指向性が１６個の指向性に切換えられたときに無線装置３０から１６個の電波を受信し、その受信した１６個の電波の強度である１６個の受信信号強度ＲＳＳＩ３３～ＲＳＳＩ４８を検出する。

【０１３２】

以下、無線装置４０は、無線装置１０，２０，３０から、順次、１６個の電波を受信し、その受信した１６個の電波の強度を検出する。そして、無線装置４０において検出した受信信号強度の個数が３８４個に達すると、無線装置４０は、無線装置１０，２０，３０との無線通信を停止する。

【０１３３】

その後、無線装置４０は、受信信号強度ＲＳＳＩ１～ＲＳＳＩ１６、受信信号強度ＲＳＳＩ１７～ＲＳＳＩ３２、受信信号強度ＲＳＳＩ３３～ＲＳＳＩ４８、・・・、受信信号強度ＲＳＳＩ３６９～ＲＳＳＩ３８４を直列に配列し、その直列に配列した３８４個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ３８４の平均値ＲＳＳＩ＿ａｖｅを演算する。そして、無線装置４０は、３８４個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ３８４のうち、平均値ＲＳＳＩ＿ａｖｅに近い順に２５６個の受信信号強度を削除し、残りの１２８個の受信信号強度ＲＳＳＩ１’～ＲＳＳＩ１２８’を平均値ＲＳＳＩ＿ａｖｅで多値化して１２８個のビットＢｉｔ１～Ｂｉｔ１２８からなる秘密鍵Ｋｓ２を生成する。

【０１３４】

このように、秘密鍵の作成方法２においても、無線装置４０および鍵生成装置５０は、同じ複数の受信信号強度に基づいて、同じ方法によって秘密鍵Ｋｓ１，Ｋｓ２を作成する。

【０１３５】

従って、秘密鍵Ｋｓ１を秘密鍵Ｋｓ２に一致させることができる。つまり、無線装置４０および鍵生成装置５０は、同じ秘密鍵を共有できる。

【０１３６】

また、秘密鍵の作成方法２においては、無線装置４０および鍵生成装置５０は、異なる無線伝送路ＲＴ１～ＲＴ３を介して送受信された１６個ごとの電波の強度である受信信号強度ＲＳＳＩ１～ＲＳＳＩ１６，ＲＳＳＩ１７～ＲＳＳＩ３２，・・・，ＲＳＳＩ３６９～ＲＳＳＩ３８４をまとめて３８４個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ３８４とし、その３８４個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ３８４の平均値ＲＳＳＩ＿ａｖｅを演算する。そして、無線装置４０および鍵生成装置５０は、その演算した平均値ＲＳＳＩ＿

ａｖｅを用いて２５６個の受信信号強度を削除し、残りの１２８個の受信信号強度を平均値ＲＳＳＩ＿ａｖｅによって多値化して秘密鍵Ｋｓ１，Ｋｓ２を作成する。

【０１３７】

この場合、平均値ＲＳＳＩ＿ａｖｅは、３個の無線伝送路ＲＴ１～ＲＴ３の平均的な無線通信特性が反映された受信信号強度になり、秘密鍵Ｋｓ１，Ｋｓ２は、３８４個の受信信号強度のうち、平均値ＲＳＳＩ＿ａｖｅに近い２５６個の受信信号強度が削除され、残りの１２８個の受信信号強度を平均値ＲＳＳＩ＿ａｖｅによって多値化したビット列からなる。

【０１３８】

従って、３個の無線伝送路ＲＴ１～ＲＴ３の平均的な無線通信特性を反映して秘密鍵Ｋｓ１，Ｋｓ２を作成できる。

【０１３９】

また、３８４個の受信信号強度のうち、平均値ＲＳＳＩ＿ａｖｅに近い２５６個の受信信号強度が削除されるので、無線伝送路ＲＴ１を介して受信された電波の受信信号強度、無線伝送路ＲＴ２を介して受信された電波の受信信号強度および無線伝送路ＲＴ３を介して受信された電波の受信信号強度は、秘密鍵Ｋｓ１，Ｋｓ２の作成に反映される度合が異なる。例えば、無線伝送路ＲＴ１を介して受信された電波の受信信号強度は、秘密鍵Ｋｓ１，Ｋｓ２の作成に殆ど反映されず、無線伝送路ＲＴ２を介して受信された電波の受信信号強度は、相対的に少ない数の受信信号強度が秘密鍵Ｋｓ１，Ｋｓ２の作成に反映され、無線伝送路ＲＴ３を介して受信された電波の受信信号強度は、相対的に多数の受信信号強度が秘密鍵Ｋｓ１，Ｋｓ２の作成に反映される。その結果、盗聴装置は、各無線伝送路ＲＴ１～ＲＴ３を介して受信された電波の受信信号強度が秘密鍵Ｋｓ１，Ｋｓ２の作成に反映される度合を検知できない。従って、秘密鍵Ｋｓ１，Ｋｓ２の盗聴を抑制できる。

【０１４０】

図１４および図１５は、それぞれ、図１に示す通信システム１００において秘密鍵を作成して暗号通信を行なう動作を説明するための第１および第２のフローチャートである。

【０１４１】

一連の動作が開始されると、無線装置１０および無線装置４０は、アレーアンテナ１１の指向性が複数の指向性に切換えられたときに相互に複数の電波を送受信し、ビット列Ａからなる部分秘密鍵Ｋｓ１＿ｐａｒｔ１，Ｋｓ２＿ｐａｒｔ１を生成する（ステップＳ１）。

【０１４２】

そして、無線装置１０は、その生成した部分秘密鍵Ｋｓ１＿ｐａｒｔ１を有線ケーブル５１を介して鍵生成装置５０へ送信し（ステップＳ２）、鍵生成装置５０は、部分秘密鍵Ｋｓ１＿ｐａｒｔ１を受信する（ステップＳ３）。

【０１４３】

その後、無線装置２０および無線装置４０は、アレーアンテナ２１の指向性が複数の指向性に切換えられたときに相互に複数の電波を送受信し、ビット列Ｂからなる部分秘密鍵Ｋｓ１＿ｐａｒｔ２，Ｋｓ２＿ｐａｒｔ２を生成する（ステップＳ４）。

【０１４４】

そして、無線装置２０は、その生成した部分秘密鍵Ｋｓ１＿ｐａｒｔ２を有線ケーブル５２を介して鍵生成装置５０へ送信し（ステップＳ５）、鍵生成装置５０は、部分秘密鍵Ｋｓ１＿ｐａｒｔ２を受信する（ステップＳ６）。

【０１４５】

引き続いて、無線装置３０および無線装置４０は、アレーアンテナ３１の指向性が複数の指向性に切換えられたときに相互に複数の電波を送受信し、ビット列Ｃからなる部分秘密鍵Ｋｓ１＿ｐａｒｔ３，Ｋｓ２＿ｐａｒｔ３を生成する（ステップＳ７）。

【０１４６】

そして、無線装置３０は、その生成した部分秘密鍵Ｋｓ１＿ｐａｒ３を有線ケーブル５３を介して鍵生成装置５０へ送信し（ステップＳ８）、鍵生成装置５０は、部分秘密鍵Ｋ

ｓ１＿ｐａｒｔ３を受信する（ステップＳ９）。

【０１４７】

その後、無線装置４０は、部分秘密鍵Ｋｓ２＿ｐａｒｔ１～Ｋｓ２＿ｐａｒｔ３を構成するビット列Ａ，Ｂ，Ｃのトータルビット数Ｎを演算し（ステップＳ１０）、トータルビット数Ｎが所定数に達したか否かを判定する（ステップＳ１１）。

【０１４８】

ステップＳ１１において、トータルビット数Ｎが所定数に達していないと判定されたとき、ステップＳ１１においてトータルビット数Ｎが所定数に達したと判定されるまで上述したステップＳ１～ステップＳ１１が繰り返し実行される。

【０１４９】

そして、ステップＳ１１において、トータルビット数Ｎが所定数に達したと判定されると、無線装置４０は、複数の部分秘密鍵Ｋｓ２＿ｐａｒｔ１，Ｋｓ２＿ｐａｒｔ２，・・・を順に配列して秘密鍵Ｋｓ２を生成する。即ち、無線装置４０は、複数の部分秘密鍵Ｋｓ２＿ｐａｒｔ１，Ｋｓ２＿ｐａｒｔ２，・・・を組合わせて秘密鍵Ｋｓ２を生成する（ステップＳ１２）。また、鍵生成装置５０は、複数の部分秘密鍵Ｋｓ１＿ｐａｒｔ１，Ｋｓ１＿ｐａｒｔ２，・・・を組合わせて秘密鍵Ｋｓ１を生成する（ステップＳ１３）。

【０１５０】

その後、鍵生成装置５０は、その生成した秘密鍵Ｋｓ１をそれぞれ有線ケーブル５１～５３を介して無線装置１０，２０，３０へ送信し（ステップＳ１４）、無線装置１０，２０，３０は、秘密鍵Ｋｓ１を受信する（ステップＳ１５）。

【０１５１】

そして、無線装置３０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４０へ鍵確認用データＤＣＦＭ１を送信する。

【０１５２】

そして、アンテナ部１３０は、無線装置４０において発生された鍵確認用データＤＣＦＭ２を無線装置４０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。

【０１５３】

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。

【０１５４】

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４０へ送信する。そして、無線装置４０は、無線装置３０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。

【０１５５】

これにより、無線装置３０における鍵一致の確認が終了する（ステップＳ１６）。

【０１５６】

なお、無線装置３０における鍵一致確認に代えて、無線装置４０において鍵一致確認をしてもよい（ステップＳ１７）。

【０１５７】

ステップＳ１６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

３０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ｘ１を検出し、その検出したビットパターンｘ１のシンドロームｓ１＝ｘ１Ｈ$^{T}$を演算する。

【０１５８】

擬似シンドローム作成部１９１は、演算したシンドロームｓ１＝ｘ１Ｈ$^{T}$を不一致ビット検出部１９２へ出力し、ビットパターンｘ１を鍵不一致訂正部１９３へ出力する。

【０１５９】

一方、無線装置４０は、ステップＳ１６において無線装置３０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＝ｘ２Ｈ$^{T}$を演算して無線装置３０へ送信する。

【０１６０】

無線装置３０のアンテナ部１３０は、無線装置４０からシンドロームｓ２＝ｘ２Ｈ$^{T}$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＝ｘ２Ｈ$^{T}$に対して所定の処理を施し、シンドロームｓ２＝ｘ２Ｈ$^{T}$を鍵一致化部１９０へ出力する。

【０１６１】

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４０において作成されたシンドロームｓ２＝ｘ２Ｈ$^{T}$を受ける。そして、不一致ビット検出部１９２は、無線装置３０で作成されたシンドロームｓ１＝ｘ１Ｈ$^{T}$と無線装置４０において作成されたシンドロームｓ２＝ｘ２Ｈ$^{T}$との差分ｓ＝ｓ１－ｓ２を演算する。

【０１６２】

その後、不一致ビット検出部１９２は、ｓ≠０であることを確認し、鍵不一致のビットパターンｅ＝ｘ１－ｘ２をｓ＝ｅＨ$^{T}$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。

【０１６３】

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ｘ１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４０において作成された秘密鍵Ｋｓ２のビットパターンｘ２＝ｘ１－ｅを演算する。

【０１６４】

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ｘ２＝ｘ１－ｅの一致を確認する。

【０１６５】

これにより、鍵不一致対策が終了する（ステップＳ１８）。

【０１６６】

なお、上述した無線装置３０における鍵不一致対策（ステップＳ１８）に代えて、無線装置４０においてステップＳ１８と同じ動作からなる鍵不一致対策をしてもよい（ステップＳ１９）。

【０１６７】

ステップＳ１６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Ｓ１８において鍵不一致対策がなされたとき、無線装置３０の暗号部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、その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、暗号化された送信データをアンテナ部１３０を介して無線装置４０へ送信する。

【０１６８】

また、無線装置３０のアンテナ部１３０は、暗号化された送信データを無線装置４０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。

【０１６９】

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秘密鍵Ｋｓ１によって復号して受信データを取得する。

【０１７０】

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Ｓ２０）。

【０１７１】

無線装置４０においても、上述した無線装置１３０における秘密鍵Ｋｓ１による暗号・復号動作（ステップＳ２０）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Ｓ２１）。そして、一連の動作が終了する。

【０１７２】

なお、図１５においては、無線装置３０と無線装置４０との間で秘密鍵Ｋｓ１と秘密鍵Ｋｓ２との鍵不一致確認および鍵不一致対策を行ない、無線装置３０，４０間で秘密鍵Ｋｓ１，Ｋｓ２を用いた無線通信が行なわれると説明したが、実際には、無線装置１０と無線装置４０との間および無線装置２０と無線装置４０との間においても、秘密鍵Ｋｓ１と秘密鍵Ｋｓ２との鍵不一致確認および鍵不一致対策が行なわれ、無線装置１０，２０と無線装置４０との間で秘密鍵Ｋｓ１，Ｋｓ２を用いた無線通信が行なわれる。この場合、無線装置１０，２０の各々は、図１５に示すステップＳ１６，Ｓ１８，Ｓ２０を実行する。

【０１７３】

図１６は、図１４に示すステップＳ１の詳細な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１０の送信処理部１２０は、ｐ＝１を設定する（ステップＳ３１）。そして、無線装置１０の指向性設定部２２０は、制御電圧セットＣＬＶ１によってアレーアンテナ１１の指向性を１つの指向性Ｄｐに設定する（ステップＳ３２）。

【０１７４】

その後、無線装置４０の信号発生部１１０は、所定のデータからなるパケットＰＫＴ１を発生して送信処理部１２０へ出力する。無線装置３０の送信処理部１２０は、パケットＰＫＴ１を周波数ｆ１で変調し、アンテナ４１（アンテナ部２３０）を介して無線装置１０へ所定のデータを構成する電波を送信する（ステップＳ３３）。

【０１７５】

無線装置１０において、アレーアンテナ１１（アンテナ部１３０）は、無線装置４０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。無線装置１０のプロファイル生成部１５０は、アレーアンテナ１１から受けた電波の強度ＷＩ１ｐを検出する（ステップＳ３４）。

【０１７６】

その後、無線装置１０の信号発生部１１０は、所定のデータからなるパケットＰＫＴ１を発生して送信処理部１２０へ出力する。無線装置１０の送信処理部１２０は、パケットＰＫＴ１を周波数ｆ１で変調し、アレーアンテナ１１を介して無線装置４０へ所定のデータを構成する電波を送信する（ステップＳ３５）。

【０１７７】

無線装置４０において、アンテナ４１（アンテナ部２３０）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。無線装置４０のプロファイル生成部１５０は、アンテナ４１から受けた電波の強度ＷＩ２ｐを検出する（ステップＳ３６）。

【０１７８】

その後、無線装置１０の送信処理部１２０は、ｐ＝Ｐ（＝１６）であるか否かを判定する（ステップＳ３７）。そして、ｐ＝Ｐでないとき、無線装置１０の送信処理部１２０は、ｐ＝ｐ＋１を設定し（ステップＳ３８）、ステップＳ３７においてｐ＝Ｐであると判定されるまで、上述したステップＳ３２～Ｓ３８が繰返し実行される。即ち、アレーアンテナ１１の指向性が制御電圧セットＣＬＶ１～ＣＬＶＰによってＰ個の指向性に変えられて

、無線装置４０のアンテナ４１と無線装置１０のアレーアンテナ１１との間で所定のデータを構成する電波が送受信され、電波強度ＷＩ１１～ＷＩ１Ｐ及びＷＩ２１～ＷＩ２Ｐが検出されるまで、ステップＳ３２～Ｓ３８が繰返し実行される。

【０１７９】

ステップＳ３７において、ｐ＝Ｐであると判定されると、無線装置１０において、プロファイル生成部１５０は、Ｐ個の電波強度ＷＩ１１～ＷＩ１Ｐからなる受信信号プロファイルＲＳＳＩ＿１０を作成して鍵作成部１６０へ出力する。

【０１８０】

無線装置１０の鍵作成部１６０は、受信信号プロファイルＲＳＳＩ＿１０を構成するＰ個の受信信号強度ＷＩ１１～ＷＩ１Ｐの平均値を演算し、その演算した平均値に近い強度を有する所定数（＝８個）の受信信号強度を削除し、Ｐ個の電波強度ＷＩ１１～ＷＩ１Ｐからｋ個（８個）の受信信号強度ＷＩ１１～ＷＩ１ｋを選択する。そして、無線装置１０の鍵作成部１６０は、ｋ個の受信信号強度ＷＩ１１～ＷＩ１ｋを平均値によって多値化し、その多値化した各値をビットパターンとするビット列Ａ（＝部分秘密鍵Ｋｓ１＿ｐａｒｔ１）を作成する（ステップＳ３９）。

【０１８１】

また、無線装置４０のプロファイル生成部１５０は、Ｐ個の受信信号強度ＷＩ２１～ＷＩ２Ｐからなる受信信号プロファイルＲＳＳＩ＿４０を作成して鍵作成部１６０Ａへ出力する。

【０１８２】

無線装置４０の鍵作成部１６０Ａは、受信信号プロファイルＲＳＳＩ＿４０を構成するＰ個の受信信号強度ＷＩ２１～ＷＩ２Ｐの平均値を演算し、その演算した平均値に近い強度を有する所定数（＝８個）の受信信号強度を削除し、Ｐ個の受信信号強度ＷＩ２１～ＷＩ２Ｐからｋ個（８個）の受信信号強度ＷＩ２１～ＷＩ２ｋを選択する。そして、無線装置４０の鍵作成部１６０Ａは、ｋ個の受信信号強度ＷＩ２１～ＷＩ２ｋを平均値によって多値化し、その多値化した各値をビットパターンとするビット列Ａ（＝部分秘密鍵Ｋｓ２＿ｐａｒｔ１）を作成する（ステップＳ４０）。そして、一連の動作は、終了する。

【０１８３】

なお、図１４に示すステップＳ４，Ｓ７における詳細な動作も、図１６に示すフローチャートに従って実行される。

【０１８４】

図１６に示すステップＳ３３，Ｓ３４の動作は、無線装置１０，２０，３０において受信信号プロファイルＲＳＳＩ＿１０，ＲＳＳＩ＿２０，ＲＳＳＩ＿３０を生成するための電波を無線装置４０のアンテナ４１から無線装置１０，２０，３０のアレーアンテナ１１，２１，３１へ送信し、かつ、無線装置１０，２０，３０において電波の受信信号強度ＷＩ１ｐを検出する動作であり、ステップＳ３５，Ｓ３６に示す動作は、無線装置４０において受信信号プロファイルＲＳＳＩ＿４０を生成するための電波を無線装置１０，２０，３０のアレーアンテナ１１，２１，３１から無線装置４０のアンテナ４１へ送信し、かつ、無線装置４０において電波の強度ＷＩ２ｐ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４０のアンテナ４１から無線装置１０，２０，３０のアレーアンテナ１１，２１，３１への送信及び所定のデータを構成する電波の無線装置１０，２０，３０のアレーアンテナ１１，２１，３１から無線装置４０のアンテナ４１への送信は、アレーアンテナ１１，２１，３１の指向性を１つの指向性Ｄｐに設定して交互に行なわれる。つまり、所定のデータを構成する電波は、無線装置４０のアンテナ４１と無線装置１０，２０，３０のアレーアンテナ１１，２１，３１との間で時分割復信（ＴＤＤ）等により送受信される。

【０１８５】

従って、アレーアンテナ１１，２１，３１の指向性を１つの指向性に設定して無線装置４０のアンテナ４１から無線装置１０，２０，３０のアレーアンテナ１１，２１，３１へ所定のデータを構成する電波を送信し、無線装置１０，２０，３０において電波強度ＷＩ

１ｐ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１０，２０，３０のアレーアンテナ１１，２１，３１から無線装置４０のアンテナ４１へ送信し、無線装置４０において電波強度ＷＩ２ｐを検出することができる。その結果、無線装置１０，２０，３０と無線装置４０との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１０，２０，３０と無線装置４０との間で送受信でき、電波の可逆性によりＰ個の電波強度ＷＩ１１～ＷＩ１Ｐをそれぞれ Ｐ個の電波強度ＷＩ２１～ＷＩ２Ｐに一致させることができる。その結果、ｋ個の電波強度ＷＩ１１～ＷＩ１ｋをそれぞれｋ個の電波強度ＷＩ２１～ＷＩ２ｋに一致させることができる。そして、鍵生成装置５０において作成される秘密鍵Ｋｓ１を無線装置４０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。

【０１８６】

また、所定のデータを構成する電波は、無線装置１０，２０，３０と無線装置４０との間で時分割復信（ＴＤＤ）等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１１，２１，３１を介して所定のデータを構成する電波を無線装置１０，２０，３０と無線装置４０との間で送受信できる。

【０１８７】

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。

【０１８８】

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ｘ１，ｘ２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。

【０１８９】

更に、秘密鍵Ｋｓ１は、無線装置１０，２０，３０においてそれぞれ生成された部分秘密鍵Ｋｓ１＿ｐａｒｔ１，Ｋｓ１＿ｐａｒｔ２，Ｋｓ１＿ｐａｒｔ３を組合わせて生成され、秘密鍵Ｋｓ２は、無線装置４０がそれぞれ無線装置１０，２０，３０から受信した電波の受信信号強度に基づいて生成された部分秘密鍵Ｋｓ２＿ｐａｒｔ１，Ｋｓ２＿ｐａｒｔ２，Ｋｓ２＿ｐａｒｔ３を組合わせて生成されるので、盗聴装置は、無線装置４０および鍵生成装置５０において、どのように部分秘密鍵を組合わせているのかを検知できず、更に、Ｐ個の電波強度ＷＩ１１～ＷＩ１Ｐ，ＷＩ２１～ＷＩ２Ｐのうち、Ｐ－ｋ個の受信信号強度が削除されてｋ個の電波強度ＷＩ１１～ＷＩ１ｋ，ＷＩ２１～ＷＩ２ｋが選択され、ｋビットの部分秘密鍵Ｋｓ１＿ｐａｒｔ１～Ｋｓ１＿ｐａｒｔ３；Ｋｓ２＿ｐａｒｔ１～Ｋｓ２＿ｐａｒｔ３が生成されていることを検知できない。そうすると、秘密鍵Ｋｓ１，Ｋｓ２の鍵長が解っている場合でも、総当り方式で秘密鍵の解読を行なうと、実用的な期間内で秘密鍵の解読をできないので、秘密鍵Ｋｓ１，Ｋｓ２の鍵長が解らない状態では、秘密鍵Ｋｓ１，Ｋｓ２の解読を行なうことは殆どできない。従って、盗聴装置による秘密鍵Ｋｓ１，Ｋｓ２の盗聴を抑制できる。

【０１９０】

更に、無線装置１０と無線装置４０との間の無線通信、無線装置２０と無線装置４０との間の無線通信および無線装置３０と無線装置４０との間の無線通信は、それぞれ、異なる周波数ｆ１，ｆ２，ｆ３を用いて行なわれるので、盗聴装置は、どのような周波数を用いて無線通信を行なっているかを検知できず、無線装置１０，２０，３０と無線装置４０との間の無線通信を傍受することが困難である。その結果、秘密鍵Ｋｓ１，Ｋｓ２の盗聴を抑制できる。

【０１９１】

図１７は、図１に示す通信システム１００において秘密鍵を作成して暗号通信を行なう他の動作を説明するためのフローチャートである。

【０１９２】

一連の動作が開始されると、無線装置１０および無線装置４０は、アレーアンテナ１１の指向性が複数の指向性に切換えられたときに相互に複数の電波を送受信し、それぞれ、所定数の受信信号強度ＲＳＳＩ１＿１０～ＲＳＳＩＰ＿１０；ＲＳＳＩ１＿４０（１）～ＲＳＳＩＰ＿４０（１）を検出する（ステップＳ１Ａ）。この場合、受信信号強度ＲＳＳＩ１＿１０～ＲＳＳＩＰ＿１０は、それぞれ、受信信号強度ＲＳＳＩ１＿４０（１）～ＲＳＳＩＰ＿４０（１）に等しい。

【０１９３】

そして、無線装置１０は、その検出した受信信号強度ＲＳＳＩ１＿１０～ＲＳＳＩＰ＿１０を有線ケーブル５１を介して鍵生成装置５０へ送信し（ステップＳ２Ａ）、鍵生成装置５０は、受信信号強度ＲＳＳＩ１＿１０～ＲＳＳＩＰ＿１０を受信する（ステップＳ３Ａ）。

【０１９４】

その後、無線装置２０および無線装置４０は、アレーアンテナ２１の指向性が複数の指向性に切換えられたときに相互に複数の電波を送受信し、それぞれ、所定数の受信信号強度ＲＳＳＩ１＿２０～ＲＳＳＩＰ＿２０；ＲＳＳＩ１＿４０（２）～ＲＳＳＩＰ＿４０（２）を検出する（ステップＳ４Ａ）。この場合、受信信号強度ＲＳＳＩ１＿２０～ＲＳＳＩＰ＿２０は、それぞれ、受信信号強度ＲＳＳＩ１＿４０（２）～ＲＳＳＩＰ＿４０（２）に等しい。

【０１９５】

そして、無線装置２０は、その検出した受信信号強度ＲＳＳＩ１＿２０～ＲＳＳＩＰ＿２０を有線ケーブル５２を介して鍵生成装置５０へ送信し（ステップＳ５Ａ）、鍵生成装置５０は、受信信号強度ＲＳＳＩ１＿２０～ＲＳＳＩＰ＿２０を受信する（ステップＳ６Ａ）。

【０１９６】

引き続いて、無線装置３０および無線装置４０は、アレーアンテナ３１の指向性が複数の指向性に切換えられたときに相互に複数の電波を送受信し、それぞれ、所定数の受信信号強度ＲＳＳＩ１＿３０～ＲＳＳＩＰ＿３０；ＲＳＳＩ１＿４０（３）～ＲＳＳＩＰ＿４０（３）を検出する（ステップＳ７Ａ）。この場合、受信信号強度ＲＳＳＩ１＿３０～ＲＳＳＩＰ＿３０は、それぞれ、ＲＳＳＩ１＿４０（３）～ＲＳＳＩＰ＿４０（３）に等しい。

【０１９７】

そして、無線装置３０は、その検出した受信信号強度ＲＳＳＩ１＿３０～ＲＳＳＩＰ＿３０を有線ケーブル５３を介して鍵生成装置５０へ送信し（ステップＳ８Ａ）、鍵生成装置５０は、受信信号強度ＲＳＳＩ１＿３０～ＲＳＳＩＰ＿３０を受信する（ステップＳ９Ａ）。

【０１９８】

その後、無線装置４０は、受信信号強度ＲＳＳＩ１＿１０～ＲＳＳＩＰ＿１０，ＲＳＳＩ１＿２０～ＲＳＳＩＰ＿２０，ＲＳＳＩ１＿３０～ＲＳＳＩＰ＿３０を構成する受信信号強度のトータル個数Ｍを演算し（ステップＳ１０Ａ）、トータル個数Ｍが所定数ｎに達したか否かを判定する（ステップＳ１１Ａ）。

【０１９９】

ステップＳ１１Ａにおいて、トータル個数Ｍが所定数ｎに達していないと判定されたとき、ステップＳ１１Ａにおいてトータル個数Ｍが所定数ｎに達したと判定されるまで上述したステップＳ１Ａ～ステップＳ１１Ａが繰り返し実行される。

【０２００】

そして、ステップＳ１１Ａにおいて、トータル個数Ｍが所定数ｎに達したと判定されると、無線装置４０は、ｎ個（３８４個）の受信信号強度ＲＳＳＩ１～ＲＳＳＩｎ（ＲＳＳＩ１＿４０（１）～ＲＳＳＩＰ＿４０（１），ＲＳＳＩ１＿４０（２）～ＲＳＳＩＰ＿４０（２），ＲＳＳＩ１＿４０（３）～ＲＳＳＩＰ＿４０（３）を順に配列した受信信号強度からなる）の平均値ＲＳＳＩ＿ａｖｅを演算するとともに、ｎ個の受信信号強度ＲＳＳ

Ｉ１～ＲＳＳＩｎのうち、平均値ＲＳＳＩ＿ａｖｅに近い順に所定数（＝２５６個）の受信信号強度を削除し、ｊ個の受信信号強度ＲＳＳＩ１～ＲＳＳＩｊを平均値ＲＳＳＩ＿ａｖｅによって多値化して秘密鍵Ｋｓ２を生成する（ステップＳ１２Ａ）。

【０２０１】

また、鍵生成装置５０は、ｎ個（３８４個）の受信信号強度ＲＳＳＩ１～ＲＳＳＩｎ（ＲＳＳＩ１＿１０～ＲＳＳＩＰ＿１０，ＲＳＳＩ１＿２０～ＲＳＳＩＰ＿２０，ＲＳＳＩ１＿３０～ＲＳＳＩＰ＿３０を順に配列した受信信号強度からなる）の平均値ＲＳＳＩ＿ａｖｅを演算するとともに、ｎ個の受信信号強度ＲＳＳＩ１～ＲＳＳＩｎのうち、平均値ＲＳＳＩ＿ａｖｅに近い順に所定数（＝２５６個）の受信信号強度を削除し、ｊ個の受信信号強度ＲＳＳＩ１～ＲＳＳＩｊを平均値ＲＳＳＩ＿ａｖｅによって多値化して秘密鍵Ｋｓ１を生成する（ステップＳ１３Ａ）。

【０２０２】

その後、鍵生成装置５０は、その生成した秘密鍵Ｋｓ１をそれぞれ有線ケーブル５１～５３を介して無線装置１０，２０，３０へ送信し（ステップＳ１４Ａ）、無線装置１０，２０，３０は、秘密鍵Ｋｓ１を受信する（ステップＳ１５Ａ）。

【０２０３】

そして、一連の動作は、図１５に示すステップＳ１６へ移行し、上述したステップＳ１６，Ｓ１８（またはステップＳ１７，Ｓ１９）およびステップＳ２０，Ｓ２１が順次実行される。

【０２０４】

図１８は、図１７に示すステップＳ１Ａの詳細な動作を説明するためのフローチャートである。図１８に示すフローチャートは、図１６に示すフローチャートのステップＳ３９，Ｓ４０をそれぞれステップＳ３９Ａ，Ｓ４０Ａに代えたものであり、その他は、図１６に示すフローチャートと同じである。

【０２０５】

図１７のステップＳ１Ａの詳細な動作が開始されると、上述したステップＳ３１～ステップＳ３８が順次実行され、ステップＳ３７において、ｐ＝Ｐであると判定されると、無線装置１０において、プロファイル生成部１５０は、Ｐ個の電波強度ＷＩ１１～ＷＩ１Ｐを順に配列したＰ個の受信信号強度ＲＳＳＩ１＿１０～ＲＳＳＩＰ＿１０を検出する（ステップＳ３９Ａ）。

【０２０６】

その後、無線装置４０において、プロファイル生成部１５０は、Ｐ個の電波強度ＷＩ２１～ＷＩ２Ｐを順に配列したＰ個の受信信号強度ＲＳＳＩ１＿４０（１）～ＲＳＳＩＰ＿４０（１）を検出する（ステップＳ４０Ａ）。そして、一連の動作は終了する。

【０２０７】

なお、図１７に示すステップＳ４Ａ，Ｓ７Ａの詳細な動作も、図１８に示すフローチャートに従って実行される。この場合、無線装置２０のプロファイル生成部１５０は、ステップＳ３９ＡにおいてＰ個の受信信号強度ＲＳＳＩ１＿２０～ＲＳＳＩＰ＿２０を検出し、無線装置４０のプロファイル生成部１５０は、ステップＳ４０ＡにおいてＰ個の受信信号強度ＲＳＳＩ１＿４０（２）～ＲＳＳＩＰ＿４０（２）を検出する。そして、無線装置３０のプロファイル生成部１５０は、ステップＳ３９ＡにおいてＰ個の受信信号強度ＲＳＳＩ１＿３０～ＲＳＳＩＰ＿３０を検出し、無線装置４０のプロファイル生成部１５０は、ステップＳ４０ＡにおいてＰ個の受信信号強度ＲＳＳＩ１＿４０（３）～ＲＳＳＩＰ＿４０（３）を検出する。

【０２０８】

また、図１７、図１５および図１８に示すフローチャートに従って秘密鍵Ｋｓ１，Ｋｓ２が作成され、通信システム１００において暗号通信が行なわれる場合、無線装置１０，２０，３０は、図３において鍵作成部１６０が削除され、プロファイル生成部１５０がそれぞれ有線ケーブル５１～５３に接続された構成からなる。

【０２０９】

従って、無線装置１０のプロファイル生成部１５０は、図１７に示すステップＳ２Ａにおいて、Ｐ個の受信信号強度ＲＳＳＩ１＿１０～ＲＳＳＩＰ＿１０を有線ケーブル５１を介して鍵生成装置５０へ送信し、無線装置２０のプロファイル生成部１５０は、図１７に示すステップＳ４Ａにおいて、Ｐ個の受信信号強度ＲＳＳＩ１＿２０～ＲＳＳＩＰ＿２０を有線ケーブル５２を介して鍵生成装置５０へ送信し、無線装置３０のプロファイル生成部１５０は、図１７に示すステップＳ７Ａにおいて、Ｐ個の受信信号強度ＲＳＳＩ１＿３０～ＲＳＳＩＰ＿３０を有線ケーブル５３を介して鍵生成装置５０へ送信する。

【０２１０】

図１８に示すステップＳ３３，Ｓ３４の動作は、無線装置１０，２０，３０においてＰ個の受信信号強度ＲＳＳＩ１＿１０～ＲＳＳＩＰ＿１０；ＲＳＳＩ１＿２０～ＲＳＳＩＰ＿２０；ＲＳＳＩ１＿３０～ＲＳＳＩＰ＿３０を生成するための電波を無線装置４０のアンテナ４１から無線装置１０，２０，３０のアレーアンテナ１１，２１，３１へ送信し、かつ、無線装置１０，２０，３０においてＰ個の受信信号強度ＲＳＳＩ１＿１０～ＲＳＳＩＰ＿１０；ＲＳＳＩ１＿２０～ＲＳＳＩＰ＿２０；ＲＳＳＩ１＿３０～ＲＳＳＩＰ＿３０を検出する動作であり、ステップＳ３５，Ｓ３６に示す動作は、無線装置４０においてＰ個の受信信号強度ＲＳＳＩ１＿４０（１）～ＲＳＳＩＰ＿４０（１），ＲＳＳＩ１＿４０（２）～ＲＳＳＩＰ＿４０（２），ＲＳＳＩ１＿４０（３）～ＲＳＳＩＰ＿４０（３）を生成するための電波を無線装置１０，２０，３０のアレーアンテナ１１，２１，３１から無線装置４０のアンテナ４１へ送信し、かつ、無線装置４０においてＰ個の受信信号強度ＲＳＳＩ１＿４０（１）～ＲＳＳＩＰ＿４０（１），ＲＳＳＩ１＿４０（２）～ＲＳＳＩＰ＿４０（２），ＲＳＳＩ１＿４０（３）～ＲＳＳＩＰ＿４０（３）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４０のアンテナ４１から無線装置１０，２０，３０のアレーアンテナ１１，２１，３１への送信及び所定のデータを構成する電波の無線装置１０，２０，３０のアレーアンテナ１１，２１，３１から無線装置４０のアンテナ４１への送信は、アレーアンテナ１１，２１，３１の指向性を１つの指向性Ｄｐに設定して交互に行なわれる。つまり、所定のデータを構成する電波は、無線装置４０のアンテナ４１と無線装置１０，２０，３０のアレーアンテナ１１，２１，３１との間で時分割復信（ＴＤＤ）等により送受信される。

【０２１１】

従って、アレーアンテナ１１，２１，３１の指向性を１つの指向性に設定して無線装置４０のアンテナ４１から無線装置１０，２０，３０のアレーアンテナ１１，２１，３１へ所定のデータを構成する電波を送信し、無線装置１０，２０，３０において電波強度ＷＩ１ｐ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１０，２０，３０のアレーアンテナ１１，２１，３１から無線装置４０のアンテナ４１へ送信し、無線装置４０において電波強度ＷＩ２ｐを検出することができる。その結果、無線装置１０，２０，３０と無線装置４０との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１０，２０，３０と無線装置４０との間で送受信でき、電波の可逆性によりＰ個の電波強度ＷＩ１１～ＷＩ１Ｐをそれぞれ Ｐ個の電波強度ＷＩ２１～ＷＩ２Ｐに一致させることができる。その結果、Ｐ個の受信信号強度ＲＳＳＩ１＿１０～ＲＳＳＩＰ＿１０；ＲＳＳＩ１＿２０～ＲＳＳＩＰ＿２０；ＲＳＳＩ１＿３０～ＲＳＳＩＰ＿３０をそれぞれＰ個の受信信号強度ＲＳＳＩ１＿４０（１）～ＲＳＳＩＰ＿４０（１）；ＲＳＳＩ１＿４０（２）～ＲＳＳＩＰ＿４０（２）；ＲＳＳＩ１＿４０（３）～ＲＳＳＩＰ＿４０（３）に一致させることができる。そして、鍵生成装置５０において作成される秘密鍵Ｋｓ１を無線装置４０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。

【０２１２】

また、無線装置４０および鍵生成装置５０は、異なる無線伝送路ＲＴ１～ＲＴ３（無線装置１０，４０間の無線伝送路、無線装置２０，４０間の無線伝送路および無線装置３０，４０間の無線伝送路）を介して送受信されたＰ個（＝１６個）ごとの電波の強度である受信信号強度ＲＳＳＩ１～ＲＳＳＩＰ，ＲＳＳＩＰ＋１～ＲＳＳＩ２Ｐ，・・・，ＲＳＳＩｎ－１５～ＲＳＳＩｎをまとめてｎ個（＝３８４個）の受信信号強度ＲＳＳＩ１～ＲＳ

ＳＩｎとし、そのｎ個の受信信号強度ＲＳＳＩ１～ＲＳＳＩｎの平均値ＲＳＳＩ＿ａｖｅを演算する。そして、無線装置４０および鍵生成装置５０は、その演算した平均値ＲＳＳＩ＿ａｖｅを用いてｉ個（＝２５６個）の受信信号強度を削除し、残りのｊ個（＝１２８個）の受信信号強度を平均値ＲＳＳＩ＿ａｖｅによって多値化して秘密鍵Ｋｓ１，Ｋｓ２を作成する。

【０２１３】

この場合、平均値ＲＳＳＩ＿ａｖｅは、３個の無線伝送路ＲＴ１～ＲＴ３の平均的な無線通信特性が反映された受信信号強度になり、秘密鍵Ｋｓ１，Ｋｓ２は、ｎ個の受信信号強度のうち、平均値ＲＳＳＩ＿ａｖｅに近いｉ個の受信信号強度が削除され、残りのｊ個の受信信号強度を平均値ＲＳＳＩ＿ａｖｅによって多値化したビット列からなる。

【０２１４】

従って、３個の無線伝送路ＲＴ１～ＲＴ３の平均的な無線通信特性を反映して秘密鍵Ｋｓ１，Ｋｓ２を作成できる。また、ｎ個の受信信号強度のうち、平均値ＲＳＳＩ＿ａｖｅに近いｉ個の受信信号強度が削除されるので、無線伝送路ＲＴ１を介して受信された電波の受信信号強度、無線伝送路ＲＴ２を介して受信された電波の受信信号強度および無線伝送路ＲＴ３を介して受信された電波の受信信号強度は、秘密鍵Ｋｓ１，Ｋｓ２の作成に反映される度合が異なる。その結果、盗聴装置は、各無線伝送路ＲＴ１～ＲＴ３を介して受信された電波の受信信号強度が秘密鍵Ｋｓ１，Ｋｓ２の作成に反映される度合を検知できない。従って、秘密鍵Ｋｓ１，Ｋｓ２の盗聴を抑制できる。

【０２１５】

図１７、図１５および図１８に示すフローチャートに従って秘密鍵Ｋｓ１，Ｋｓ２が作成される場合、その他、図１４、図１５および図１６に示すフローチャートに従って秘密鍵Ｋｓ１，Ｋｓ２が作成される場合と同様の効果を享受できる。

【０２１６】

なお、図１４、図１５および図１６に示すフローチャートに従って無線装置１０，２０，３０と無線装置４０との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１４および図１５に示すステップＳ１，Ｓ２，Ｓ１５，Ｓ１６，Ｓ１８，Ｓ２０および図１６に示すステップＳ３１，Ｓ３２，Ｓ３４，Ｓ３５，Ｓ３７，Ｓ３８，Ｓ３９を備えるプログラムをＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）から読出し、無線装置２０に搭載されたＣＰＵは、図１４および図１５に示すステップＳ４，Ｓ５，Ｓ１５，Ｓ１６，Ｓ１８，Ｓ２０および図１６に示すステップＳ３１，Ｓ３２，Ｓ３４，Ｓ３５，Ｓ３７，Ｓ３８，Ｓ３９を備えるプログラムをＲＯＭから読出し、無線装置３０に搭載されたＣＰＵは、図１４および図１５に示すステップＳ７，Ｓ８，Ｓ１５，Ｓ１６，Ｓ１８，Ｓ２０および図１６に示すステップＳ３１，Ｓ３２，Ｓ３４，Ｓ３５，Ｓ３７，Ｓ３８，Ｓ３９を備えるプログラムをＲＯＭから読出し、無線装置４０に搭載されたＣＰＵは、図１４および図１５に示すステップＳ１，Ｓ４，Ｓ７，Ｓ１０，Ｓ１１，Ｓ１２，Ｓ１７，Ｓ１９，Ｓ２１および図１６に示すステップＳ３３，Ｓ３６，Ｓ４０を備えるプログラムをＲＯＭから読出し、無線装置１０，２０，３０，４０に搭載された４つのＣＰＵは、その読出したプログラムを実行して図１４、図１５および図１６に示すフローチャートに従って無線装置１０，２０，３０と無線装置４０との間で通信を行なう。

【０２１７】

また、図１７、図１５および図１８に示すフローチャートに従って無線装置１０，２０，３０と無線装置４０との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１０に搭載されたＣＰＵは、図１７および図１５に示すステップＳ１Ａ，Ｓ２Ａ，Ｓ１５Ａ，Ｓ１６，Ｓ１８，Ｓ２０および図１８に示すステップＳ３１，Ｓ３２，Ｓ３４，Ｓ３５，Ｓ３７，Ｓ３８，Ｓ３９Ａを備えるプログラムをＲＯＭから読出し、無線装置２０に搭載されたＣＰＵは、図１７および図１５に示すステップＳ４Ａ，Ｓ５Ａ，Ｓ１５Ａ，Ｓ１６，Ｓ１８，Ｓ２０および図１８に示すステップＳ３１，Ｓ３２，Ｓ３４，Ｓ３５，Ｓ３７，Ｓ３８，Ｓ３９Ａを備えるプログラムをＲＯＭから読出し、無線装置３

０に搭載されたＣＰＵは、図１７および図１５に示すステップＳ７Ａ，Ｓ８Ａ，Ｓ１５Ａ，Ｓ１６，Ｓ１８，Ｓ２０および図１８に示すステップＳ３１，Ｓ３２，Ｓ３４，Ｓ３５，Ｓ３７，Ｓ３８，Ｓ３９Ａを備えるプログラムをＲＯＭから読出し、無線装置４０に搭載されたＣＰＵは、図１７および図１５に示すステップＳ１Ａ，Ｓ４Ａ，Ｓ７Ａ，Ｓ１０Ａ，Ｓ１１Ａ，Ｓ１２Ａ，Ｓ１７，Ｓ１９，Ｓ２１および図１８に示すステップＳ３３，Ｓ３６，Ｓ４０Ａを備えるプログラムをＲＯＭから読出し、無線装置１０，２０，３０，４０に搭載された４つのＣＰＵは、その読出したプログラムを実行して図１７、図１５および図１８に示すフローチャートに従って無線装置１０，２０，３０と無線装置４０との間で通信を行なう。

【０２１８】

従って、ＲＯＭは、無線装置１０，２０，３０と無線装置４０との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。

【０２１９】

図１９は、この発明の実施の形態による他の通信システムの概略図である。この発明の実施の形態による通信システムは、図１９に示す通信システム３００であってもよい。

【０２２０】

通信システム３００は、パーソナルコンピュータ３１０と、アンテナ３１１と、鍵生成装置３２０と、アレーアンテナ３２１～３２４と、有線ケーブル３１２，３２５～３２９，３４１，３４２と、ネットワーク３３０と、暗号化装置３４０と、アクセスポイント３５０とを備える。

【０２２１】

パーソナルコンピュータ３１０は、有線ケーブル３１２によってアンテナ３１１に接続される。アンテナ３１１は、全方位性のアンテナである。鍵生成装置３２０は、それぞれ、有線ケーブル３２５～３２８によってアレーアンテナ３２１～３２４に接続され、有線ケーブル３２９によってネットワーク３３０に接続される。

【０２２２】

アレーアンテナ３２１～３２４の各々は、図１および図２に示すアレーアンテナ１１と同じ構成からなり、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３２１～３２４は、相互に異なる位置に配置される。

【０２２３】

暗号化装置３４０は、有線ケーブル３４１によってネットワーク３３０に接続され、有線ケーブル３４２によってアクセスポイント３５０に接続される。

【０２２４】

パーソナルコンピュータ３１０は、アンテナ３１１を介してアレーアンテナ３２１～３２４と、順次、無線通信を行ない、上述した作成方法２によって秘密鍵Ｋｓ２を作成する。そして、パーソナルコンピュータ３１０は、その作成した秘密鍵Ｋｓ２を用いて暗号化装置３４０との間で暗号通信を行なう。より具体的には、パーソナルコンピュータ３１０は、送信データを秘密鍵Ｋｓ２によって暗号化し、その暗号化した送信データをアンテナ３１１を介してアクセスポイント３５０へ送信する。また、パーソナルコンピュータ３１０は、暗号化された送信データをアクセスポイント３５０から受信し、その受信した暗号かされた送信データを秘密鍵Ｋｓ２によって復号し、送信データを受信する。

【０２２５】

鍵生成装置３２０は、順次、アレーアンテナ３２１～３２４を用いてパーソナルコンピュータ３１０と無線通信を行ない、上述した作成方法２によって秘密鍵Ｋｓ１を作成する。そして、鍵生成装置３２０は、その作成した秘密鍵Ｋｓ１を有線ケーブル３２９、ネットワーク３３０および有線ケーブル３４１を介して暗号化装置３４０へ送信する。

【０２２６】

暗号化装置３４０は、鍵生成装置３２０から秘密鍵Ｋｓ１を受信し、その受信した秘密鍵Ｋｓ１を用いてパーソナルコンピュータ３１０との間で暗号通信を行なう。より具体的

には、暗号化装置３４０は、送信データを秘密鍵Ｋｓ１によって暗号化し、その暗号化した送信データを有線ケーブル３４２およびアクセスポイント３５０を介してパーソナルコンピュータ３１０へ送信する。また、暗号化装置３４０は、アクセスポイント３５０および有線ケーブル３４２を介してパーソナルコンピュータ３１０から暗号化された送信データを受信し、その受信した暗号化された送信データを秘密鍵Ｋｓ１によって復号して送信データを受信する。

【０２２７】

アクセスポイント３５０は、暗号化された送信データを有線ケーブル３４２を介して受信し、その受信した暗号化された送信データをパーソナルコンピュータ３５０へ送信する。また、アクセスポイント３５０は、暗号化された送信データをパーソナルコンピュータ３１０から受信し、その受信した暗号化された送信データを有線ケーブル３４２を介して暗号化装置３４０へ送信する。

【０２２８】

パーソナルコンピュータ３１０は、図４に示す無線装置４０と同じ構成からなる。この場合、図４に示すアンテナ部２３０は、アンテナ３１１からなる。

【０２２９】

図２０は、図１９に示す鍵生成装置３２０の構成を示す概略図である。鍵生成装置３２０は、図３に示す無線装置１０のアンテナ部１３０をアンテナ部２４０に代え、プロファイル生成部１５０をプロファイル生成部１５０Ａに代え、鍵作成部１６０を鍵作成部１６０Ｂに代えたものであり、その他は、無線装置１０と同じである。

【０２３０】

プロファイル生成部１５０Ａは、アンテナ部２４０を構成するアレーアンテナ３２１から９６個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ９６を受け、その後、アンテナ部２４０を構成するアレーアンテナ３２２から９６個の受信信号強度ＲＳＳＩ９７～ＲＳＳＩ１９２を受け、引き続いて、アンテナ部２４０を構成するアレーアンテナ３２３から９６個の受信信号強度ＲＳＳＩ１９３～ＲＳＳＩ２８８を受け、その後、アンテナ部２４０を構成するアレーアンテナ３２４から９６個の受信信号強度ＲＳＳＩ２８９～ＲＳＳＩ３８４を受ける。そして、プロファイル生成部１５０Ａは、順次、アンテナ部２４０から受けた９６個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ９６；ＲＳＳＩ９７～ＲＳＳＩ１９２；ＲＳＳＩ１９３～ＲＳＳＩ２８８；ＲＳＳＩ２８９～ＲＳＳＩ３８４を順に配列した３８４個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ３８４を作成して鍵作成部１６０Ｂへ出力する。

【０２３１】

鍵作成部１６０Ｂは、３８４個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ３８４をプロファイル生成部１５０Ａから受け、その受けた３８４個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ３８４の平均値ＲＳＳＩ＿ａｖｅを演算する。そして、鍵作成部１６０Ｂは、３８４個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ３８４のうち、平均値ＲＳＳＩ＿ａｖｅに近い順に２５６個の受信信号強度を削除し、残りの１２８個の受信信号強度を平均値ＲＳＳＩ＿ａｖｅによって多値化して秘密鍵Ｋｓ１を作成する。

【０２３２】

鍵作成部１６０Ｂは、秘密鍵Ｋｓ１を作成すると、その作成した秘密鍵Ｋｓ１を鍵一致確認部１７０および鍵一致化部１９０へ出力する。

【０２３３】

アンテナ部２４０は、図１９に示すアレーアンテナ３２１～３２４からなる。そして、アンテナ部２４０は、送信処理部１２０からのパケットをパーソナルコンピュータ３１０へ送信し、パーソナルコンピュータ３１０からのパケットを受信して受信処理部１４０またはプロファイル生成部１５０Ａへ供給する。

【０２３４】

なお、指向性設定部２２０は、アンテナ部２４０を構成する４個のアレーアンテナ３２１～３２４へそれぞれ制御電圧セットＣＬＶ１～ＣＬＶ９６，ＣＬＶ９７～ＣＬＶ１９２，ＣＬＶ１９３～ＣＬＶ２８８，ＣＬＶ２８９～ＣＬＶ３８４を順次供給する。この場合

、アレーアンテナ３２１は、制御電圧セットＣＬＶ１～ＣＬＶ９６に応じて、指向性が９６個の指向性に順次切換えられ、アレーアンテナ３２２は、制御電圧セットＣＬＶ９７～ＣＬＶ１９２に応じて、指向性が９６個の指向性に順次切換えられ、アレーアンテナ３２３は、制御電圧セットＣＬＶ１９３～ＣＬＶ２８８に応じて、指向性が９６個の指向性に順次切換えられ、アレーアンテナ３２４は、制御電圧セットＣＬＶ２８９～ＣＬＶ３８４に応じて、指向性が９６個の指向性に順次切換えられる。

【０２３５】

パーソナルコンピュータ３１０および鍵生成装置３２０間で秘密鍵Ｋｓ１，Ｋｓ２が生成される場合、例えば、鍵生成装置３２０は、制御電圧セットＣＬＶ１～ＣＬＶ９６をアレーアンテナ３２１へ順次供給してアレーアンテナ３２１の指向性を９６個の指向性に順次切換えながらパーソナルコンピュータ３１０との間で９６個の電波を送受信し、その次に、制御電圧セットＣＬＶ９７～ＣＬＶ１９２をアレーアンテナ３２２へ順次供給してアレーアンテナ３２２の指向性を９６個の指向性に順次切換えながらパーソナルコンピュータ３１０との間で９６個の電波を送受信し、その後、制御電圧セットＣＬＶ１９３～ＣＬＶ２８８をアレーアンテナ３２３へ順次供給してアレーアンテナ３２３の指向性を９６個の指向性に順次切換えながらパーソナルコンピュータ３１０との間で９６個の電波を送受信し、最後に、制御電圧セットＣＬＶ２８９～ＣＬＶ３８４をアレーアンテナ３２４へ順次供給してアレーアンテナ３２４の指向性を９６個の指向性に順次切換えながらパーソナルコンピュータ３１０との間で９６個の電波を送受信する。

【０２３６】

アレーアンテナ３２１は、指向性が９６個の指向性に順次切換えられたときの９６個の電波をパーソナルコンピュータ３１０から受信し、その受信した９６個の電波を有線ケーブル３２５を介して鍵生成装置３２０のプロファイル生成部１５０Ａへ送信する。また、アレーアンテナ３２２は、指向性が９６個の指向性に順次切換えられたときの９６個の電波をパーソナルコンピュータ３１０から受信し、その受信した９６個の電波を有線ケーブル３２６を介して鍵生成装置３２０のプロファイル生成部１５０Ａへ送信する。更に、アレーアンテナ３２３は、指向性が９６個の指向性に順次切換えられたときの９６個の電波をパーソナルコンピュータ３１０から受信し、その受信した９６個の電波を有線ケーブル３２７を介して鍵生成装置３２０のプロファイル生成部１５０Ａへ送信する。更に、アレーアンテナ３２４は、指向性が９６個の指向性に順次切換えられたときの９６個の電波をパーソナルコンピュータ３１０から受信し、その受信した９６個の電波を有線ケーブル３２８を介して鍵生成装置３２０のプロファイル生成部１５０Ａへ送信する。

【０２３７】

鍵生成装置３２０のプロファイル生成部１５０Ａは、アレーアンテナ３２１から９６個の電波を受信すると、その受信した９６個の電波の受信信号強度ＲＳＳＩ１～ＲＳＳＩ９６を検出する。その後、鍵生成装置３２０のプロファイル生成部１５０Ａは、アレーアンテナ３２２から９６個の電波を受信すると、その受信した９６個の電波の受信信号強度ＲＳＳＩ９７～ＲＳＳＩ１９２を検出する。引き続いて、鍵生成装置３２０のプロファイル生成部１５０Ａは、アレーアンテナ３２３から９６個の電波を受信すると、その受信した９６個の電波の受信信号強度ＲＳＳＩ１９３～ＲＳＳＩ２８８を検出する。最後に、鍵生成装置３２０のプロファイル生成部１５０Ａは、アレーアンテナ３２４から９６個の電波を受信すると、その受信した９６個の電波の受信信号強度ＲＳＳＩ２８９～ＲＳＳＩ３８４を検出する。そして、鍵生成装置３２０のプロファイル生成部１５０Ａは、検出した受信信号強度ＲＳＳＩ１～ＲＳＳＩ９６；ＲＳＳＩ９７～ＲＳＳＩ１９２；ＲＳＳＩ１９３～ＲＳＳＩ２８８；ＲＳＳＩ２８９～ＲＳＳＩ３８４を順に配列した３８４個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ３８４を生成して鍵作成部１６０Ｂへ出力する。

【０２３８】

そうすると、鍵生成装置３２０の鍵作成部１６０Ｂは、３８４個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ３８４をプロファイル生成部１５０Ａから受信し、その受信した３８４個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ３８４に基づいて、上述した方法によって秘密鍵Ｋ

ｓ１を作成する。
【０２３９】
一方、パーソナルコンピュータ３１０のプロファイル生成部１５０は、アレーアンテナ３２１の指向性が９６個の指向性に順次切換えられたときに鍵生成装置３２０のアレーアンテナ３２１から送信された９６個の電波をアンテナ３１１を介して受信し、その受信した９６個の電波の受信信号強度ＲＳＳＩ１～ＲＳＳＩ９６を検出する。その後、パーソナルコンピュータ３１０のプロファイル生成部１５０は、アレーアンテナ３２２の指向性が９６個の指向性に順次切換えられたときに鍵生成装置３２０のアレーアンテナ３２２から送信された９６個の電波をアンテナ３１１を介して受信し、その受信した９６個の電波の受信信号強度ＲＳＳＩ９７～ＲＳＳＩ１９２を検出する。引き続いて、パーソナルコンピュータ３１０のプロファイル生成部１５０は、アレーアンテナ３２３の指向性が９６個の指向性に順次切換えられたときに鍵生成装置３２０のアレーアンテナ３２３から送信された９６個の電波をアンテナ３１１を介して受信し、その受信した９６個の電波の受信信号強度ＲＳＳＩ１９３～ＲＳＳＩ２８８を検出する。最後に、パーソナルコンピュータ３１０のプロファイル生成部１５０は、アレーアンテナ３２４の指向性が９６個の指向性に順次切換えられたときに鍵生成装置３２０のアレーアンテナ３２４から送信された９６個の電波をアンテナ３１１を介して受信し、その受信した９６個の電波の受信信号強度ＲＳＳＩ２８９～ＲＳＳＩ３８４を検出する。
【０２４０】
そして、パーソナルコンピュータ３１０のプロファイル生成部１５０は、検出した受信信号強度ＲＳＳＩ１～ＲＳＳＩ９６；ＲＳＳＩ９７～ＲＳＳＩ１９２；ＲＳＳＩ１９３～ＲＳＳＩ２８８；ＲＳＳＩ２８９～ＲＳＳＩ３８４を順に配列した３８４個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ３８４を生成して鍵作成部１６０へ出力する。
【０２４１】
そうすると、パーソナルコンピュータ３１０の鍵作成部１６０Ａは、３８４個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ３８４をプロファイル生成部１５０から受信し、その受信した３８４個の受信信号強度ＲＳＳＩ１～ＲＳＳＩ３８４に基づいて、上述した方法によって秘密鍵Ｋｓ２を作成する。
【０２４２】
鍵生成装置３２０は、秘密鍵Ｋｓ１を生成すると、その生成した秘密鍵Ｋｓ１を有線ケーブル３２９、ネットワーク３３０および有線ケーブル３４１を介して暗号化装置３４０へ送信する。暗号化装置３４０は、鍵生成装置３２０から秘密鍵Ｋｓ１を受信し、その受信した秘密鍵Ｋｓ１を用いて送信データを暗号化する。そして、暗号化装置３４０は、秘密鍵Ｋｓ１によって暗号化した送信データを有線ケーブル３４２を介してアクセスポイント３５０へ送信する。
【０２４３】
アクセスポイント３５０は、暗号化装置３４０から受信した暗号化された送信データを無線通信によってパーソナルコンピュータ３１０へ送信する。
【０２４４】
また、パーソナルコンピュータ３１０は、秘密鍵Ｋｓ２を作成すると、その作成した秘密鍵Ｋｓ２を用いて送信データを暗号化し、その暗号化した送信データを無線通信によってアクセスポイント３５０へ送信する。
【０２４５】
これによって、パーソナルコンピュータ３１０とｃとの間で暗号通信が行なわれる。
【０２４６】
なお、パーソナルコンピュータ３１０と暗号化装置３４０との間の暗号通信は、上述した図１７、図１５および図１８に示すフローチャートに従って実行される。
【０２４７】
図１９に示す通信システム３００において秘密鍵Ｋｓ１，Ｋｓ２を作成した場合の盗聴装置による秘密鍵Ｋｓ１，Ｋｓ２の盗聴実験について説明する。盗聴実験は、図１９に示

すレイアウトで行なわれた。

【０２４８】

盗聴実験においては、盗聴装置（図示せず）をパーソナルコンピュータ３１０の近傍に配置して各種の作成方法によって秘密鍵Ｋｓ１，Ｋｓ２を作成した場合に、盗聴装置がパーソナルコンピュータ３１０と鍵生成装置３２０との間で送受信される電波を傍受して作成した秘密鍵ＫｓＴと秘密鍵Ｋｓ１，Ｋｓ２との相違ビット数が評価された。なお、作成された秘密鍵Ｋｓ１，Ｋｓ２，ＫｓＴの鍵長は、１２８ビットである。

【０２４９】

図２１は、アンテナ３１１と４個のアレーアンテナ３２１～３２４の各々との間で秘密鍵を作成した場合の盗聴実験の結果を示す図である。また、図２２は、この発明による作成方法２によって秘密鍵を作成した場合の盗聴実験の結果を示す図である。

【０２５０】

図２１および図２２において、縦軸は、出現確率を表し、横軸は、鍵誤り個数を表す。また、図２１の（ａ）～（ｄ）は、それぞれ、アレーアンテナ３２１～３２４とアンテナ３１１との間で電波を送受信して秘密鍵Ｋｓ１，Ｋｓ２を作成した場合に盗聴装置において作成された秘密鍵ＫｓＴが秘密鍵Ｋｓ１，Ｋｓ２に対して誤っているビットの個数分布を示し、図２２は、この発明による作成方法２によって秘密鍵Ｋｓ１，Ｋｓ２を作成した場合に盗聴装置において作成された秘密鍵ＫｓＴが秘密鍵Ｋｓ１，Ｋｓ２に対して誤っているビットの個数分布を示す。

【０２５１】

アンテナ３１１およびアレーアンテナ３２１間で電波を送受信して秘密鍵Ｋｓ１，Ｋｓ２を作成する場合、アレーアンテナ３２１の指向性は、３８４個の指向性に順次切換えられ、パーソナルコンピュータ３１０および鍵生成装置３２０の各々は、３８４個の電波に対応する３８４個の受信信号強度を検出する。そして、パーソナルコンピュータ３１０および鍵生成装置３２０は、３８４個の受信信号強度の平均値を演算し、その演算した平均値に近い順に２５６個の受信信号強度を削除し、残りの１２８個の受信信号強度を平均値によって多値化してそれぞれ、秘密鍵Ｋｓ２，Ｋｓ１を作成する。アンテナ３１１およびアレーアンテナ３２２～３２４間で電波を送受信して秘密鍵Ｋｓ１，Ｋｓ２を作成する場合も、同様である。

【０２５２】

アンテナ３１１およびアレーアンテナ３２１間で電波を送受信して秘密鍵Ｋｓ１，Ｋｓ２を作成した場合、ビットの不一致数（＝誤り個数）の平均は、１２８個のうちの６７．７個であり、分散幅は、４５．５個である（図２１の（ａ）参照）。また、アンテナ３１１およびアレーアンテナ３２２間で電波を送受信して秘密鍵Ｋｓ１，Ｋｓ２を作成した場合、ビットの不一致数（＝誤り個数）の平均は、１２８個のうちの３３．４個であり、分散幅は、３８．８個である（図２１の（ｂ）参照）。更に、アンテナ３１１およびアレーアンテナ３２３間で電波を送受信して秘密鍵Ｋｓ１，Ｋｓ２を作成した場合、ビットの不一致数（＝誤り個数）の平均は、１２８個のうちの６４．９個であり、分散幅は、６５．１個である（図２１の（ｃ）参照）。更に、アンテナ３１１およびアレーアンテナ３２４間で電波を送受信して秘密鍵Ｋｓ１，Ｋｓ２を作成した場合、ビットの不一致数（＝誤り個数）の平均は、１２８個のうちの４９．０個であり、分散幅は、３７．５個である（図２１の（ｄ）参照）。

【０２５３】

このように、アンテナ３１１とアレーアンテナ３２１～３２４との間で個別に秘密鍵Ｋｓ１，Ｋｓ２を作成した場合、秘密鍵ＫｓＴと秘密鍵Ｋｓ１，Ｋｓ２とのビットの不一致数の平均は、３３．４個～６７．７個の範囲で分散し、盗聴装置によって盗聴され易い場合もあれば、盗聴され難い場合もある。

【０２５４】

一方、この発明による作成方法２によって秘密鍵Ｋｓ１，Ｋｓ２を作成した場合、ビットの不一致数（＝誤り個数）の平均は、１２８個のうちの４３．６個であり、分散幅は、

３４．５個である（図２２参照）。
【０２５５】
従って、この発明による作成方法２を用いて秘密鍵Ｋｓ１，Ｋｓ２を作成することによってビットの不一致数が３３．４個～６７．７個の範囲で分散していたのをほぼ一定値（＝４３．６個）に抑制できる。また、不一致数の分散幅を３４．５個～６５．１個から３７．５まで抑制できる。
【０２５６】
その結果、この発明による作製方法２によって秘密鍵Ｋｓ１，Ｋｓ２を作成することによって盗聴装置による秘密鍵Ｋｓ１，Ｋｓ２の盗聴を抑制できる。
【０２５７】
図２３は、この発明による通信システム１００の応用例を示す図である。通信システム４００は、通信システム１００と、パーソナルコンピュータ４１０と、インターネットデータセンター４２０と、ネットワーク４３０とを備える。
【０２５８】
パーソナルコンピュータ４１０は、有線ケーブル４１１によって通信システム１００の無線装置４０に接続され、有線ケーブル４１２によってネットワーク４３０に接続される。
【０２５９】
インターネットデータセンター４２０は、キーセンター４２１と、ウェブサイト４２２とを含む。キーセンター４２１は、有線ケーブル４１３によってネットワーク４３０に接続される。ウェブサイト４２２は、有線ケーブル４１４によってネットワークに接続される。
【０２６０】
パーソナルコンピュータ４１０は、キーセンター４２１との公開鍵Ｋｏｐを共有する。また、パーソナルコンピュータ４１０は、通信システム１００の無線装置４０が上述した方法によって作成した秘密鍵Ｋｓ２を有線ケーブル４１１を介して受信する。
【０２６１】
そうすると、パーソナルコンピュータ４１０は、秘密鍵Ｋｓ２を公開鍵Ｋｏｐで暗号化し、その暗号化した暗号化秘密鍵｛Ｋｏｐ／Ｋｓ２｝を有線ケーブル４１２およびネットワーク４３０を介してキーセンター４２１へ送信する。
【０２６２】
キーセンター４２１は、ネットワーク４３０および有線ケーブル４１３を介して暗号化秘密鍵｛Ｋｏｐ／Ｋｓ２｝を受信し、その受信した暗号化秘密鍵｛Ｋｏｐ／Ｋｓ２｝を公開鍵Ｋｏｐで復号して秘密鍵Ｋｓ２を取得する。
【０２６３】
そして、キーセンター４２１は、秘密鍵Ｋｓ２をパーソナルコンピュータ４１０に対応付けて管理するとともに、秘密鍵Ｋｓ２をウェイサイト４２２へ出力する。
【０２６４】
ウェブサイト４２２は、キーセンター４２１から秘密鍵Ｋｓ２を受け、その受けた秘密鍵Ｋｓ２を保持する。
【０２６５】
パーソナルコンピュータ４１０は、秘密鍵Ｋｓ２を公開鍵Ｋｏｐで暗号化してキーセンター４２１へ送信した後、秘密鍵Ｋｓ２を用いてウェブサイト４２２との間で暗号化通信を行ない、ウェブサイト４２２から各種の情報を取得する。
【０２６６】
より具体的には、パーソナルコンピュータ４１０は、取得したい情報を秘密鍵Ｋｓ２で暗号化し、その暗号化した情報を有線ケーブル４１２、ネットワーク４３０および有線ケーブル４１４を介してウェブサイト４２２へ送信する。
【０２６７】
ウェブサイト４２２は、有線ケーブル４１４を介してパーソナルコンピュータ４１０か

ら送信された暗号化情報を受信し、その受信した暗号化情報を秘密鍵Ｋｓ２によって復号する。そして、ウェブサイト４２２は、その復号した情報に基づいて、パーソナルコンピュータ４１０が取得したい情報を特定し、その特定した情報を秘密鍵Ｋｓ２で暗号化してパーソナルコンピュータ４１０へ送信する。

【０２６８】

パーソナルコンピュータ４１０は、ウェブサイト４２２からの暗号化情報を受信し、その受信した暗号化情報を秘密鍵Ｋｓ２で復号する。そして、パーソナルコンピュータ４１０は、所望の情報を取得する。

【０２６９】

このように、通信システム４００によれば、パーソナルコンピュータ４１０は、通信システム１００でローカルに生成された秘密鍵Ｋｓ２をネットワーク４３０を介して離れた位置に存在するキーセンター４２１およびウェブサイト４２２と共有できる。

【０２７０】

なお、パーソナルコンピュータ４１０は、秘密鍵Ｋｓ２をインターネットデータセンター４２０へ送信する場合、パーソナルコンピュータ４１０のＩＰアドレス等のパーソナルコンピュータ４１０に固有の情報で暗号化してインターネットデータセンター４２０へ送信してもよい。

【０２７１】

上記においては、アレーアンテナ１１の指向性が複数の指向性に切換えられたときに無線装置１０と無線装置４０との間で送受信された複数の電波の強度に基づいて生成された部分秘密鍵と、アレーアンテナ２１の指向性が複数の指向性に切換えられたときに無線装置２０と無線装置４０との間で送受信された複数の電波の強度に基づいて生成された部分秘密鍵と、アレーアンテナ３１の指向性が複数の指向性に切換えられたときに無線装置３０と無線装置４０との間で送受信された複数の電波の強度に基づいて生成された部分秘密鍵とを組合わせて秘密鍵Ｋｓ１，Ｋｓ２を作成すると説明した。

【０２７２】

この場合、アレーアンテナ１１，２１，３１の指向性が複数の指向性に切換えられたときに無線装置１０，２０，３０と無線装置４０との間で送受信された複数の電波の強度に基づいて３個の部分秘密鍵を生成し、その生成した３個の部分秘密鍵を組合わせて秘密鍵Ｋｓ１，Ｋｓ２を作成することは、異なる３つの無線伝送路を用いて３個の部分秘密鍵を生成し、その生成した３個の部分秘密鍵を組合わせて秘密鍵Ｋｓ１，Ｋｓ２を作成することに相当する。

【０２７３】

従って、この発明による通信システムは、一般に、全方位性のアンテナを搭載する第１の無線装置と、電気的に指向性を切換え可能なアレーアンテナを搭載するｍ（ｍは２以上の整数）個の第２の無線装置と、鍵生成装置とを備え、第１の無線装置とｍ個の第２の無線装置との間でアレーアンテナの指向性を複数の指向性に順次切換えながらｍ個の部分秘密鍵を生成し、その生成したｍ個の部分秘密鍵を鍵生成装置によって組合わせて秘密鍵Ｋｓ１，Ｋｓ２を作成するものであればよい。

【０２７４】

この場合、ｍ個の第２の無線装置の各々は、全方位性のアンテナを搭載していてもよい。

【０２７５】

この発明においては、無線装置４０およびアンテナ４１は、「第１の通信装置」を構成し、無線装置４０は、「第１の無線装置」を構成し、アンテナ４１は、「第１のアンテナ」を構成する。

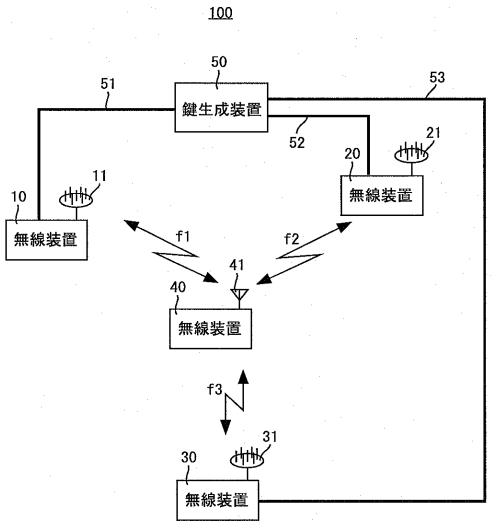
【０２７６】

また、無線装置１０，２０，３０およびアレーアンテナ１１，２１，３１は、「第２の通信装置」を構成し、無線装置１０，２０，３０は、「ｍ個の第２の無線装置」を構成し、アレーアンテナ１１，２１，３１は、「ｍ個の第２のアンテナ」を構成する。

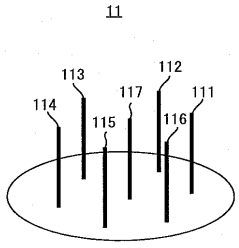
【０２７７】
今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。
【産業上の利用可能性】
【０２７８】
この発明は、秘密鍵の盗聴を抑制可能な通信システムに適用される。また、この発明は、秘密鍵の盗聴を抑制可能な通信システムに用いる無線装置に適用される。
【図面の簡単な説明】
【０２７９】
【図１】この発明の実施の形態による通信システムの概略図である。
【図２】図１に示すアレーアンテナの斜視図である。
【図３】指向性を切換え可能なアレーアンテナを搭載した無線装置の概略ブロック図である。
【図４】全方位性のアンテナを搭載した無線装置の概略ブロック図である。
【図５】図３に示す指向性設定部の概略ブロック図である。
【図６】図３に示す鍵一致確認部および図４に示す鍵一致確認部の概略ブロック図である。
【図７】図３に示す鍵一致化部および図４に示す鍵一致化部の概略ブロック図である。
【図８】受信信号強度の概念図である。
【図９】受信信号プロファイルの概念図である。
【図１０】鍵生成装置における秘密鍵の作成方法を示す図である。
【図１１】全方位性のアンテナを搭載した無線装置における秘密鍵の作成方法を示す図である。
【図１２】鍵生成装置における秘密鍵の他の作成方法を示す図である。
【図１３】全方位性のアンテナを搭載した無線装置における秘密鍵の他の作成方法を示す図である。
【図１４】図１に示す通信システムにおいて秘密鍵を作成して暗号通信を行なう動作を説明するための第１のフローチャートである。
【図１５】図１に示す通信システムにおいて秘密鍵を作成して暗号通信を行なう動作を説明するための第２のフローチャートである。
【図１６】図１４に示すステップＳ１の詳細な動作を説明するためのフローチャートである。
【図１７】図１に示す通信システムにおいて秘密鍵を作成して暗号通信を行なう他の動作を説明するためのフローチャートである。
【図１８】図１７に示すステップＳ１Ａの詳細な動作を説明するためのフローチャートである。
【図１９】秘密鍵の盗聴実験に用いたレイアウトを示す図である。
【図２０】図１９に示す鍵生成装置の構成を示す概略図である。
【図２１】アンテナと４個のアレーアンテナの各々との間で秘密鍵を作成した場合の盗聴実験の結果を示す図である。
【図２２】この発明による作製方法２によって秘密鍵を作成した場合の盗聴実験の結果を示す図である。
【図２３】この発明による通信システムの応用例を示す図である。
【符号の説明】
【０２８０】
１０，２０，３０，４０　無線装置、１１，２１，３１，３２１～３２４　アレーアンテナ、４１，３１１　アンテナ、５０，３２０　鍵生成装置、５１～５３，３１２，３２５～３２９，３４１，３４２，４１１～４１４　有線ケーブル、１００，３００，４００

通信システム、１１０　信号発生部、１１１～１１７　アンテナ素子、１２０　送信処理部、１３０，２３０　アンテナ部、１４０　受信処理部、１５０　プロファイル生成部、１６０，１６０Ａ　鍵作成部、１７０，１７０Ａ　鍵一致確認部、１７１，１９４　データ発生部、１７２，１９５　データ比較部、１７３，１９６　結果処理部、１８０　鍵記憶部、１９０，１９０Ａ　鍵一致化部、１９１　擬似シンドローム作成部、１９２　不一致ビット検出部、１９３　鍵不一致訂正部、２００　暗号部、２１０　復号部、２２０　指向性設定部、２２１～２２６　バラクタダイオード、２２７　制御電圧発生回路、３１０　パーソナルコンピュータ、３３０，４３０　ネットワーク、３４０　暗号化装置、３５０　アクセスポイント、４２０　インターネットデータセンター、４２１　キーセンター、４２２　ウェブサイト。

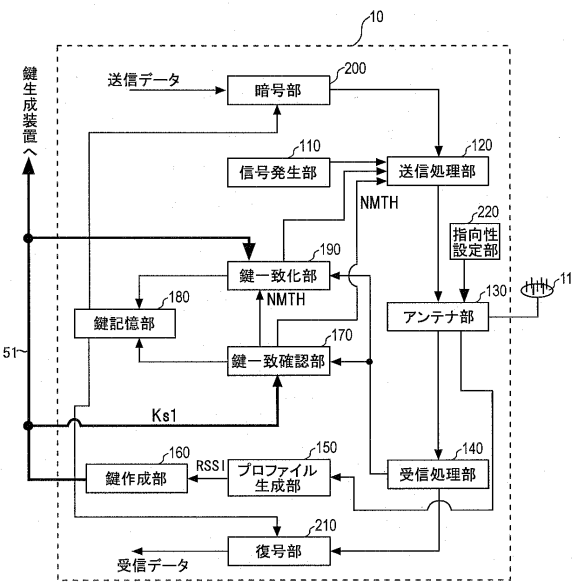
【図１】



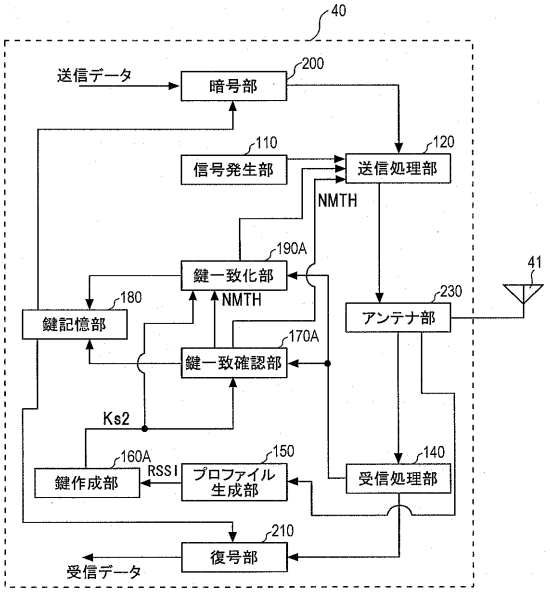

【図２】



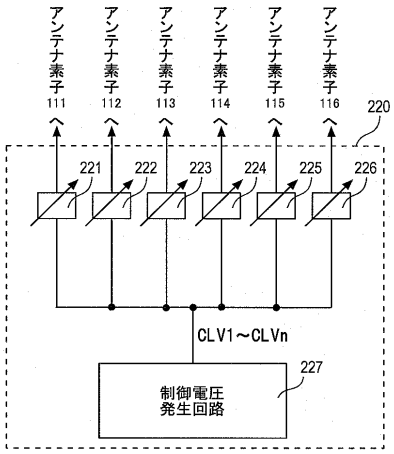

【図３】



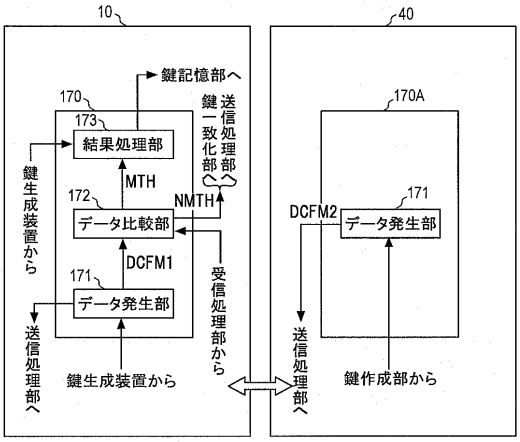
【図４】


40
送信データ
暗号部
200
信号発生部
110
送信処理部
120
NMTH
190A
鍵一致化部
41
NMTH
180
鍵記憶部
230
アンテナ部
170A
鍵一致確認部
Ks2
160A
RSSI
150
プロファイル生成部
鍵作成部
140
受信処理部
210
復号部
受信データ

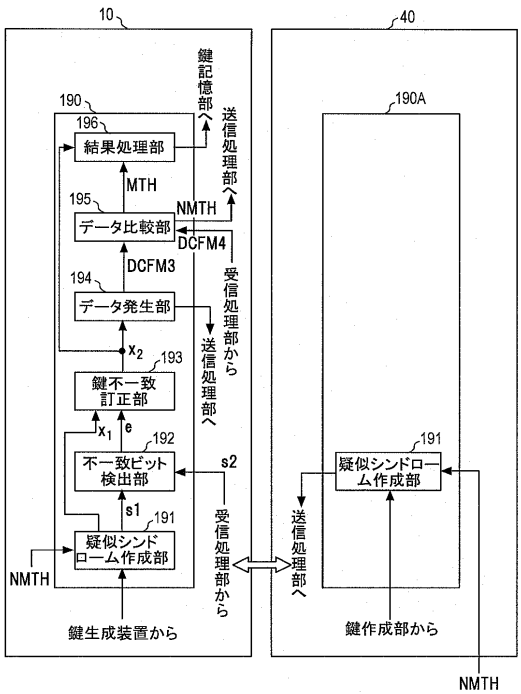
【図５】


アンテナ素子111へ
アンテナ素子112へ
アンテナ素子113へ
アンテナ素子114へ
アンテナ素子115へ
アンテナ素子116へ
220
221
222
223
224
225
226
CLV1～CLVn
制御電圧発生回路
227

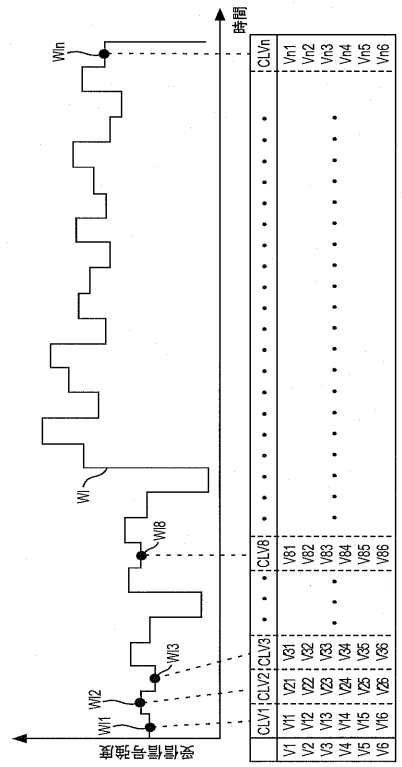
【図６】


10
40
鍵記憶部へ
170
173
結果処理部
鍵一致化部へ
送信処理部へ
MTH
NMTH
172
データ比較部
DCFM1
171
データ発生部
鍵生成装置から
送信処理部へ
受信処理部から
170A
DCFM2
171
データ発生部
送信処理部へ
鍵作成部から

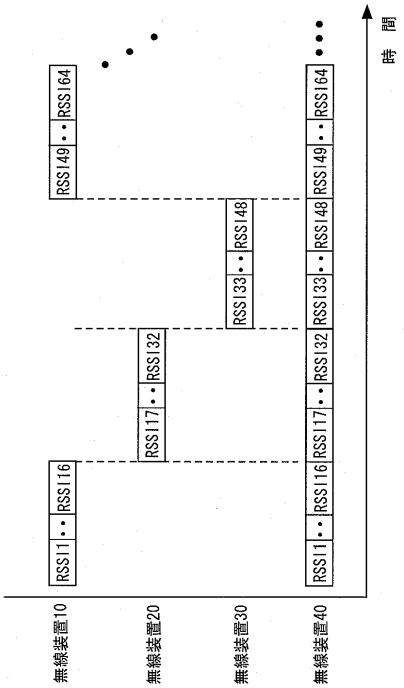
【図７】


10
40
鍵記憶部へ
送信処理部へ
190
196
結果処理部
MTH
195
NMTH
データ比較部
DCFM4
DCFM3
194
データ発生部
受信処理部から
送信処理部へ
x2
193
鍵不一致訂正部
x1
e
192
不一致ビット検出部
s2
s1
191
疑似シンドローム作成部
NMTH
鍵生成装置から
受信処理部から
送信処理部へ
190A
191
疑似シンドローム作成部
鍵作成部から
NMTH

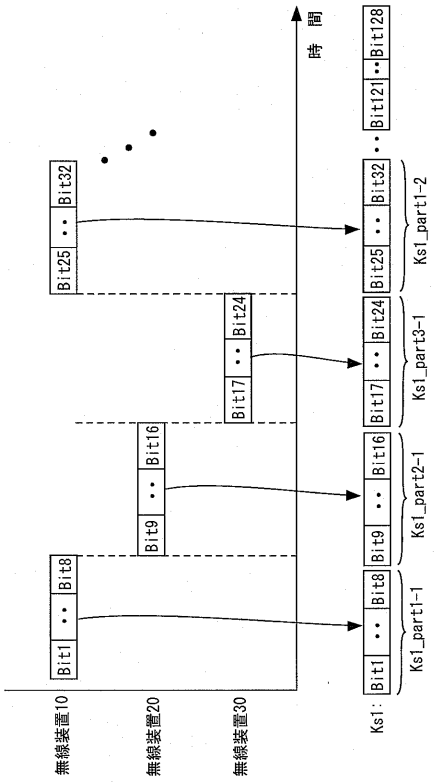
【図８】


時間
Win
Wi1
Wi2
Wi3
Wi8
Wi
CLV1
CLV2
CLV3
CLV8
CLVn
Vn1
Vn2
Vn3
Vn4
Vn5
Vn6
V11
V21
V31
V81
V12
V22
V32
V82
V13
V23
V33
V83
V14
V24
V34
V84
V15
V25
V35
V85
V16
V26
V36
V86

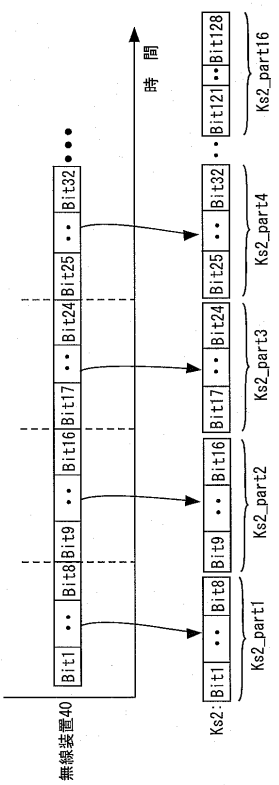
【図９】


時間
無線装置10
無線装置20
無線装置30
無線装置40
RSSI1
RSSI16
RSSI17
RSSI32
RSSI33
RSSI48
RSSI49
RSSI64

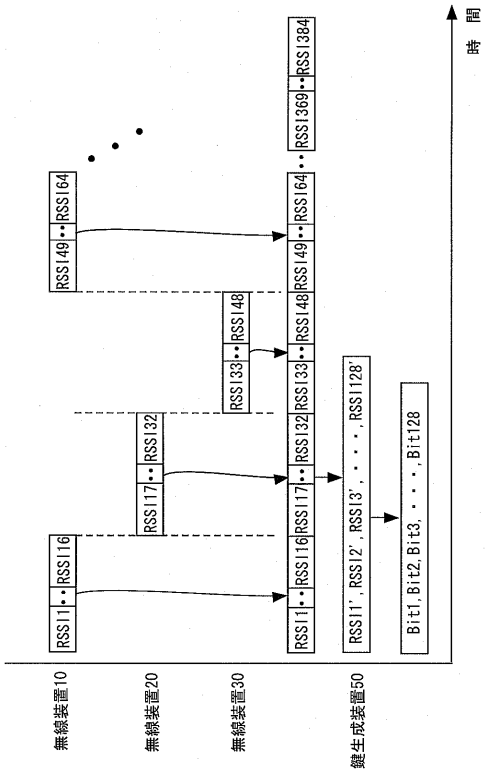
【図１０】


時間
無線装置10
無線装置20
無線装置30
Bit1
Bit8
Bit9
Bit16
Bit17
Bit24
Bit25
Bit32
Bit121
Bit128
Ks1:
Ks1_part1-1
Ks1_part2-1
Ks1_part3-1
Ks1_part1-2

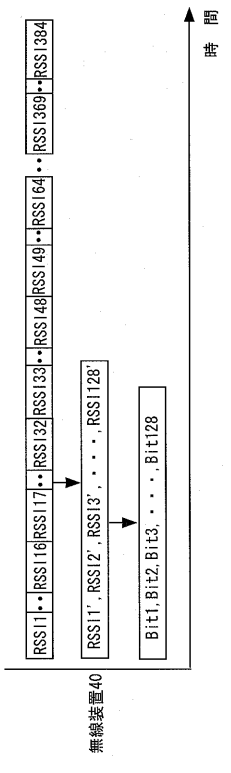
【図１１】


時間
無線装置40
Bit1
Bit8
Bit9
Bit16
Bit17
Bit24
Bit25
Bit32
Bit121
Bit128
Ks2:
Ks2_part1
Ks2_part2
Ks2_part3
Ks2_part4
Ks2_part16

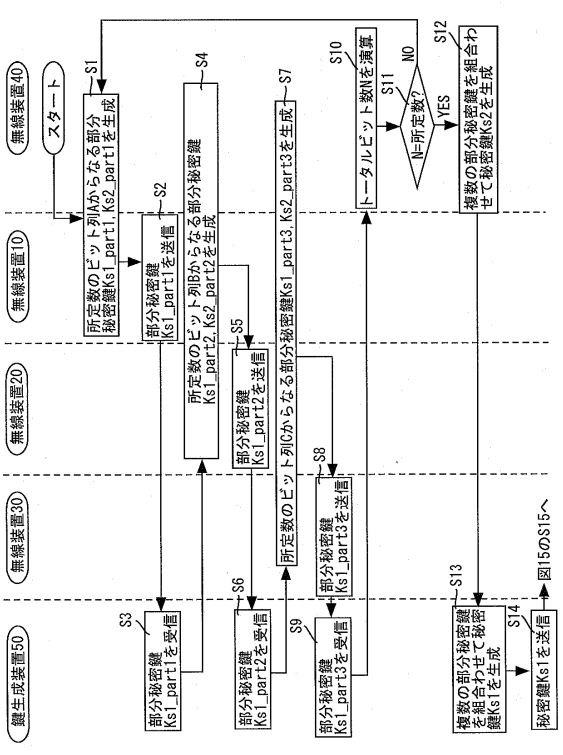
【図１２】



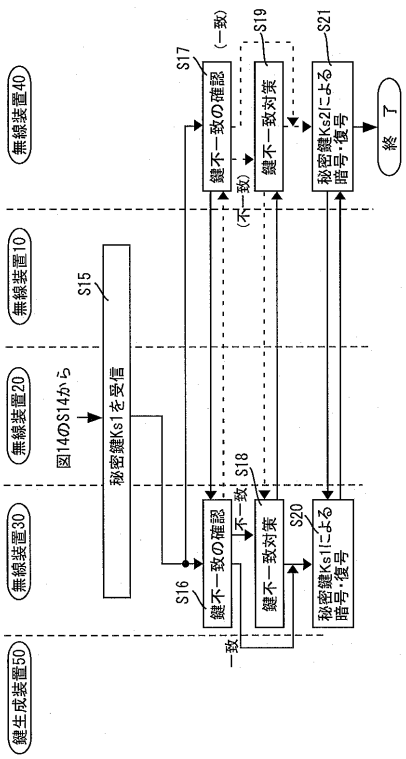

【図１３】



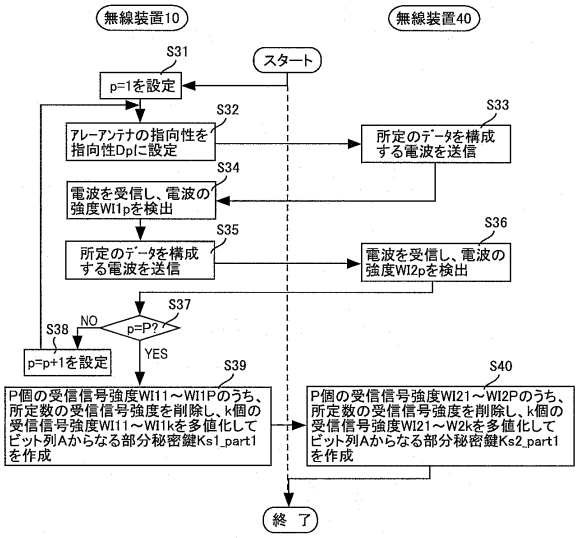

【図１４】



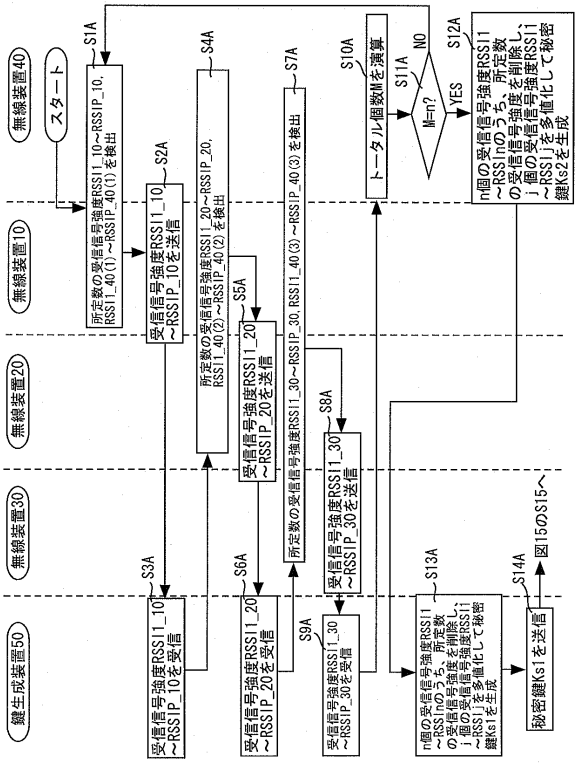

【図１５】



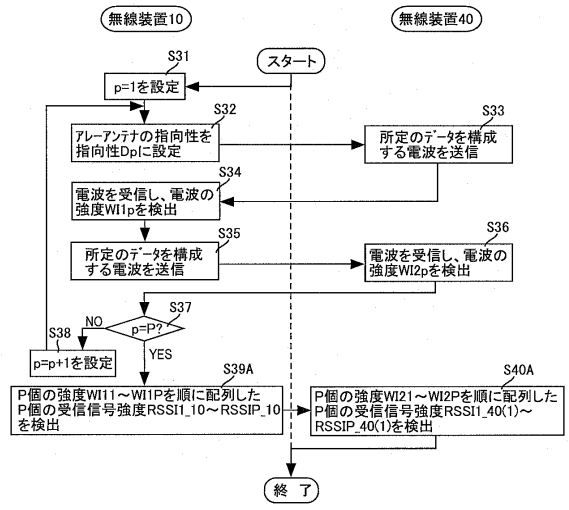
【図１６】



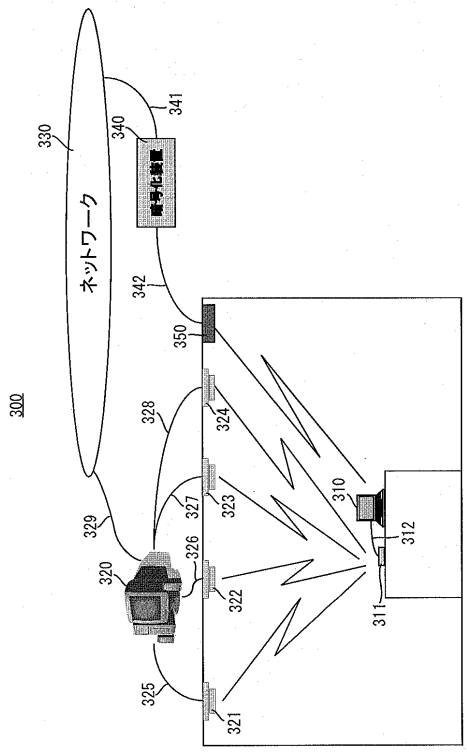

【図１７】



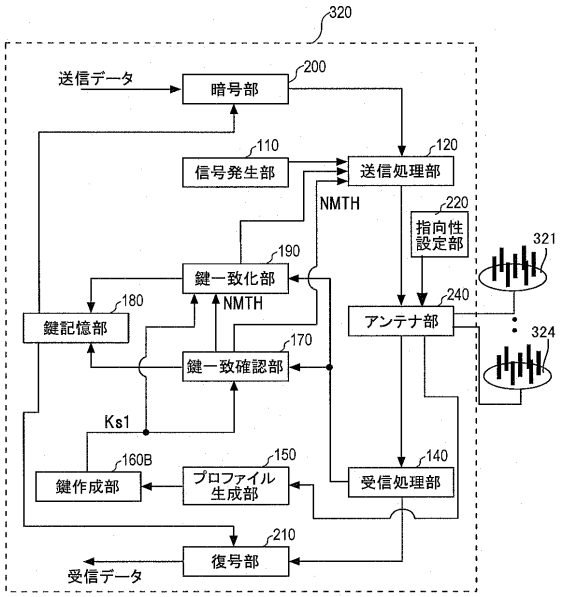

【図１８】



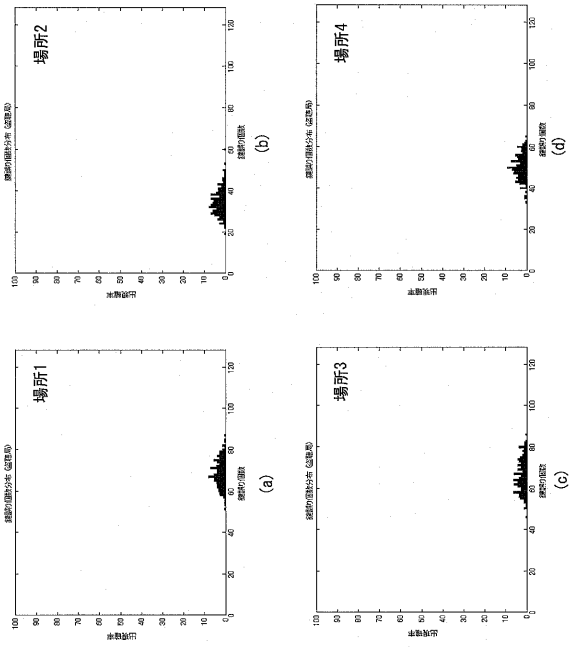

【図１９】



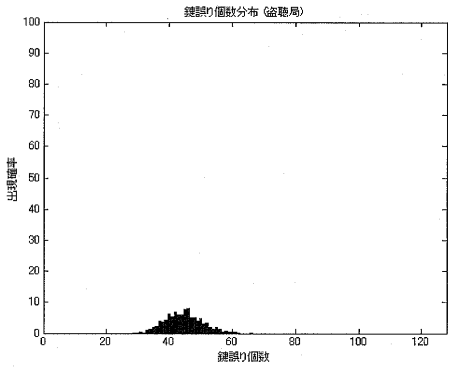
【図２０】



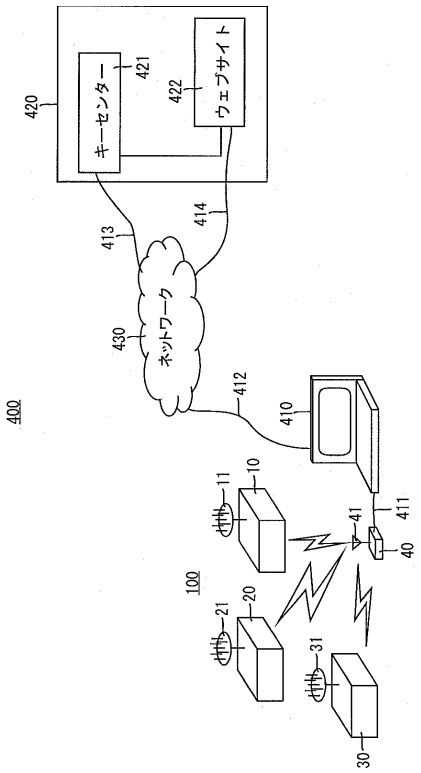

【図２１】




【図２２】




【図２３】



フロントページの続き

(72)発明者　木崎　一廣
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　石田　信行

(56)参考文献　特開２００２－３４４４３８（ＪＰ，Ａ）
特開２００４－３２６７９（ＪＰ，Ａ）
特開２００４－２９７５２７（ＪＰ，Ａ）
特開２００６－５８２２（ＪＰ，Ａ）
特開２００６－２１７３０１（ＪＰ，Ａ）
特開２００６－２２２８１７（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｂ　　１／４０