(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2012 年 1 月 26 日(26.01.2012)

PCT

(10) 国際公開番号
WO 2012/011264 A1

(51) 国際特許分類:
H04W 12/08 (2009.01) *H04W 84/12* (2009.01)

(21) 国際出願番号: PCT/JP2011/004057

(22) 国際出願日: 2011 年 7 月 15 日(15.07.2011)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2010-163597 2010 年 7 月 21 日(21.07.2010) JP

(71) 出願人 (米国を除く全ての指定国について): 日本電気株式会社 (NEC Corporation) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 大森 陽子 (OMORI, Youko) [JP/JP]; 〒1088001 東京都港区芝五丁目７番１号日本電気株式会社内 Tokyo (JP).

(74) 代理人: 桂木 雄二 (KATSURAGI, Yuji); 〒1700013 東京都豊島区東池袋３丁目２１－１８第一笠原ビル６０３号室 Tokyo (JP).

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

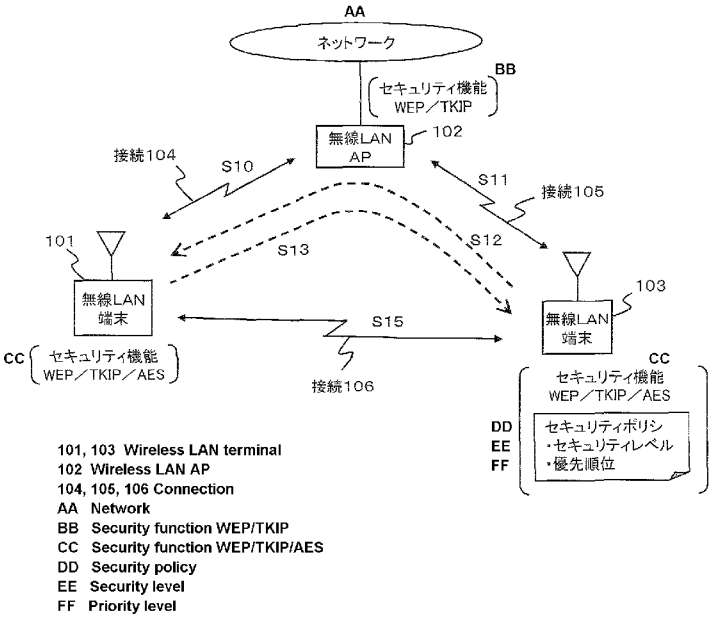
(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告（条約第 21 条(3)）

(54) **Title**: WIRELESS LAN COMMUNICATION TERMINAL IN WIRELESS LAN SYSTEM, AND COMMUNICATION CONTROL METHOD FOR WIRELESS LAN COMMUNICATION TERMINAL

(54) 発明の名称 : 無線ＬＡＮシステムにおける無線ＬＡＮ通信端末およびその通信制御方法

[図1]



(57) **Abstract**: Provided is a wireless LAN communication terminal such that it is possible to set a desired security level with another terminal without increasing the power consumption of the terminal. Also provided is a communication control method for said wireless LAN communication terminal. A wireless LAN communication terminal (103) in a wireless LAN system having an access point (102) acquires, from another terminal (101), information pertaining to the current connection with the access point and the security function information that the other terminal has when the other terminal is connected to the access point (102). Then, the wireless LAN communication terminal (103) compares the connection information and the security function information of the other terminal with the security policy of the wireless LAN communication terminal (103) itself. Subsequently, the wireless LAN communication terminal (103) selects whether to directly connect (106) with the other terminal or to relay-connect (105, 104) with the other terminal via an access point in a manner such that the aforementioned security policy is satisfied and on the basis of the comparison result, and communicates with the other terminal using the selected connection.

(57) 要約:

[続葉有]

WO 2012/011264 A1

端末の消費電力を増加させることなく、相手端末との間で所望のセキュリティ設定を可能にする無線ＬＡＮ通信端末およびその通信制御方法を提供する。アクセスポイント（１０２）を有する無線ＬＡＮシステムにおける無線ＬＡＮ通信端末（１０３）が、相手端末（１０１）がアクセスポイント１０２と接続されている場合、相手端末が有するセキュリティ機能情報とアクセスポイントとの現在の接続情報とを相手端末から取得し、相手端末のセキュリティ機能情報および接続情報と、自端末のセキュリティポリシとを比較し、比較結果に基づいて当該セキュリティポリシを満たすように相手端末との直接接続（１０６）あるいはアクセスポイントを介した中継接続（１０５，１０４）のいずれかを選択しと、選択された接続を用いて相手端末との通信を行う。

明　細　書

発明の名称 ：

無線ＬＡＮシステムにおける無線ＬＡＮ通信端末およびその通信制御方法

技術分野

[0001] 本発明は無線ＬＡＮ（ローカルエリアネットワーク）システムに係り、特に無線ＬＡＮ通信端末およびその通信制御方法に関する。

背景技術

[0002] 無線ＬＡＮでは、電波によりデータの送受信を行うことからセキュリティ強化が常に課題となっており、いくつかのセキュリティ規格が実際に採用されている。たとえばＴＫＩＰ(Temporal Key Integrity Protocol)は、それまで使用されてきたＷＥＰ(Wired Equivalent Privacy)の脆弱性を克服する暗号化方式であり、ＡＥＳ(Advanced Encryption Standard)はさらに強固な暗号化アルゴリズムを採用した標準規格である。一般に、無線ＬＡＮのアクセスポイント経由で通信を行う場合、無線通信端末はアクセスポイントとの間のセキュリティを自局でサポートされているセキュリティ機能を用いて設定することができる。

[0003] しかしながら、このようなセキュリティ機能を備えた無線ＬＡＮ端末であっても、常に同じセキュリティレベルが要求されるわけではない。たとえば、社外の無線ＬＡＮ環境で使用する場合には高いセキュリティレベルの設定が必要であり、社内の無線ＬＡＮでは低いセキュリティレベルでもよい。そこで、使用場所や環境に応じてセキュリティ設定を変更できる無線ＬＡＮシステムが提案されている。

[0004] たとえば特許文献１に開示された無線ＬＡＮ通信装置では、サーバにアクセスポイントごとに対応づけたセキュリティ設定情報を記憶しておき、無線ＬＡＮ通信端末が１つのアクセスポイントに無線接続すると、当該アクセスポイントに対応したセキュリティレベルが無線ＬＡＮ通信端末に設定される。

先行技術文献

特許文献

[0005] 特許文献1：特開２００８－２１９７５０号公報

発明の概要

発明が解決しようとする課題

[0006] 上述したように、アクセスポイント経由で通信を行う場合、無線ＬＡＮ通信端末は、自端末とアクセスポイントとの間のセキュリティを設定することが可能である。しかしながら、アクセスポイントから相手端末までの間のセキュリティレベルを自端末で設定することはできない。そのため、相手端末が自端末と同等レベルのセキュリティを設定できる場合であっても、そのようなセキュリティレベルが相手側で設定されていなければ、希望する強度のセキュリティで当該相手端末と通信を行うことはできない。

[0007] さらに、相手端末とアクセスポイントとの間のセキュリティの設定は当該相手端末がアクセスポイントへ帰属した時に決定される。したがって、この帰属が完了した後で当該相手端末と通信を開始する場合、自端末は相手端末のセキュリティ設定内容を知ることができない。

[0008] これに対して、自端末が相手端末と直接接続すれば、セキュリティを直接設定することは可能である。しかしながら、この場合、自端末がアクセスポイントとして動作することになり、単に端末として既存のアクセスポイントに接続した場合よりもネットワーク制御が複雑となり、消費電力が増加するという新たな課題が生じる。

[0009] そこで、本発明の目的は、端末の消費電力を増加させることなく、相手端末との間で所望のセキュリティ設定を可能にする無線ＬＡＮ通信端末およびその通信制御方法を提供することにある。

課題を解決するための手段

[0010] 本発明による無線ＬＡＮ通信端末は、少なくとも１つのアクセスポイントを有する無線ＬＡＮ（ローカルエリアネットワーク）システムにおける無線

ＬＡＮ通信端末であって、通信相手となる無線ＬＡＮ通信端末（以下、相手端末という。）がアクセスポイントと接続されている場合、前記相手端末が有するセキュリティ機能情報と前記アクセスポイントとの現在の接続情報とを前記相手端末から取得する取得手段と、前記相手端末の前記セキュリティ機能情報および前記接続情報と、自端末のセキュリティポリシとを比較し、前記比較結果に基づいて当該セキュリティポリシを満たすように前記相手端末との直接接続あるいは前記アクセスポイントを介した中継接続のいずれかを選択する選択手段と、前記選択された接続を用いて前記相手端末との通信を行う通信手段と、を有することを特徴とする。

[0011] 本発明による通信制御方法は、少なくとも１つのアクセスポイントを有する無線ＬＡＮ（ローカルエリアネットワーク）システムにおける無線ＬＡＮ通信端末の通信制御方法であって、取得手段が、通信相手となる無線ＬＡＮ通信端末（以下、相手端末という。）がアクセスポイントと接続されている場合、前記相手端末が有するセキュリティ機能情報と前記アクセスポイントとの現在の接続情報とを前記相手端末から取得し、選択手段が、前記相手端末の前記セキュリティ機能情報および前記接続情報と、自端末のセキュリティポリシとを比較し、前記比較結果に基づいて当該セキュリティポリシを満たすように前記相手端末との直接接続あるいは前記アクセスポイントを介した中継接続のいずれかを選択し、通信手段が前記選択された接続を用いて前記相手端末との通信を行う、ことを特徴とする。

発明の効果

[0012] 本発明によれば、端末の消費電力を増加させることなく、相手端末との間で所望のセキュリティ設定が可能となる。

図面の簡単な説明

[0013] [図1]本発明の第１実施形態による無線ＬＡＮシステムの概略的構成および通信制御手順を示す模式的システム構成図である。

[図2]図１に示すシステムにおける通信制御手順の一例を示すシーケンス図である。

[図3]本発明の第１実施例による無線ＬＡＮ通信端末の通信制御方法を示すフローチャートである。

[図4]本発明の第２実施例による無線ＬＡＮ通信端末の通信制御方法を示すフローチャートである。

[図5]本発明の第２実施形態による無線ＬＡＮシステムの概略的構成および通信制御手順を示す模式的システム構成図である。

[図6]図２および図５に示すシステムで使用可能な無線ＬＡＮ通信端末の概略的構成を示すブロック図である。

発明を実施するための形態

[0014] 以下、説明の複雑化を避けるために、簡略化した無線ＬＡＮシステムを例示する。具体的には、ある無線ＬＡＮ端末が、１つのアクセスポイント（ＡＰ）に既に帰属している別の無線ＬＡＮ端末に対して通信を開始する場合を一例として説明する。ただし、これに限定されるものではなく、複数のアクセスポイントがネットワークを通して通信可能なシステムであっても、端末間の直接通信が可能である限り、本発明は適用可能である。また、強度が異なるセキュリティ機能としては、既に述べたＷＥＰ、ＴＫＩＰおよびＡＥＳを一例として使用するが、これらに限定されるものではない。

[0015] １．第１実施形態

１．１）システム

図１に示すように、本発明の第１実施形態による無線ＬＡＮシステムは、無線ＬＡＮ端末１０１が無線ＬＡＮアクセスポイント１０２と接続されており、この無線ＬＡＮ端末１０１に対して無線ＬＡＮ端末１０３が通信を開始するものとする。

[0016] 無線ＬＡＮ端末１０１にはセキュリティレベルが異なるセキュリティ機能ＷＥＰ／ＴＫＩＰ／ＡＥＳが搭載され、アクセスポイント１０２にはセキュリティ機能ＷＥＰ／ＴＫＩＰが搭載され、無線ＬＡＮ端末１０３にはセキュリティ機能ＷＥＰ／ＴＫＩＰ／ＡＥＳが搭載されているものとする。セキュリティレベルはＷＥＰ＜ＴＫＩＰ＜ＡＥＳの順で高くなり、無線ＬＡＮ端末

１０１とアクセスポイント１０２との接続１０４はセキュリティ機能ＷＥＰで設定されているものとする。

[0017] さらに、無線ＬＡＮ端末１０３には、セキュリティポリシとして、所定セキュリティレベル（たとえばＴＫＩＰ以上）および使用セキュリティの優先順位が予め設定されている。所定セキュリティとしては、ＴＫＩＰあるいはＡＥＳを用いた通信が設定され、その際の優先順位は、たとえばＴＫＩＰとＡＥＳの両方が利用可能であれば、より高い（あるいはより低い）セキュリティ機能を利用するというように設定される。ここでは、より高い方のセキュリティレベルを選択するように設定され、ＴＫＩＰではなくＡＥＳが優先的に利用されるものとする。

[0018] １．２）動作

次に、図１および図２を参照しながら、本実施形態の通信制御手順を説明する。

[0019] まず、上述したように、無線ＬＡＮ端末１０１とアクセスポイント１０２との接続１０４はＷＥＰで設定されている（ステップＳ１０）。無線ＬＡＮ端末１０３は、無線ＬＡＮ端末１０１との通信を開始しようとする際、まずアクセスポイント１０２に帰属する（ステップＳ１１）。続いて、無線ＬＡＮ端末１０３はアクセスポイント１０２経由で無線ＬＡＮ端末１０１に対してセキュリティ機能および現在の接続設定を含む接続情報を要求する（ステップＳ１２）。

[0020] 無線ＬＡＮ端末１０１は、この接続情報要求に応じて、要求された接続情報をアクセスポイント１０２経由で無線ＬＡＮ端末１０３へ返信する（ステップＳ１３）。接続情報は、自端末が搭載するセキュリティ機能情報（ここではＷＥＰ／ＴＫＩＰ／ＡＥＳ）と、アクセスポイント１０２との現在の接続設定情報（ここではＷＥＰ使用）とを含む。

[0021] 無線ＬＡＮ端末１０３は、無線ＬＡＮ端末１０１から受信したセキュリティ機能情報および現在の接続設定情報と自端末のセキュリティポリシとを比較し、無線ＬＡＮ端末１０１と直接接続する場合とアクセスポイント１０２

を介して中継接続する場合のどちらが必要なセキュリティレベルを満たすかを判定し、セキュリティポリシに合致した接続を選択する（ステップＳ１４）。ここでは、セキュリティポリシがＴＫＩＰあるいはＡＥＳのうちセキュリティレベルが高いＡＥＳを優先的に選択するように設定され、無線ＬＡＮ端末１０１のセキュリティ機能情報がＷＥＰ／ＴＫＩＰ／ＡＥＳ、アクセスポイント１０２との現在の接続設定がＷＥＰであるから、セキュリティポリシを満たすためには直接接続を選択して、無線ＬＡＮ端末１０１との間の接続１０６にＡＥＳを利用する（ステップＳ１５）。

[0022] もしステップＳ１０において無線ＬＡＮ端末１０１とアクセスポイント１０２との接続１０４がたとえばＴＫＩＰで設定されていれば、現在の接続１０４はセキュリティポリシを満たしているので、無線ＬＡＮ端末１０３は接続１０５および１０４を通した、すなわちアクセスポイント１０２を通した中継接続を選択する。

[0023] １．３）効果

上述したように、本実施形態によれば、ある無線ＬＡＮ端末がアクセスポイントに接続された別の無線ＬＡＮ端末に対して接続しようとする際、アクセスポイントとの既存の接続情報を参照して接続方法を選択する。具体的には、相手端末とアクセスポイント間のセキュリティ情報および相手端末のセキュリティ機能を取得し、アクセスポイント経由（ＡＰ中継接続）でのセキュリティレベルと、自らアクセスポイントとして動作した場合（直接接続）のセキュリティレベルと、自端末のセキュリティポリシとを比較する。この比較結果から、ＡＰ中継接続と直接接続のいずれかを選択することで、設定可能なセキュリティレベルの中から必要なレベルでの接続設定が可能となる。これにより、必要なセキュリティレベルを確保しつつ、省電力という観点から最適な接続方法を選択することができる。

[0024] ２．第１実施例

２．１）通信制御

次に、本発明の第１実施例による無線ＬＡＮ端末の通信制御方法を図３を

参照しながら詳細に説明する。なお、本実施例による無線ＬＡＮ端末は図１における無線ＬＡＮ端末１０３に対応するものであり、アクセスポイント１０２あるいは通信相手となる無線ＬＡＮ端末１０１と直接無線通信を行うための無線通信部と、次に述べる通信制御を実行する制御部あるいはプログラム制御プロセッサとが設けられているものとする（詳細は、図６を参照しながら後で説明する。）。

[0025] 図３において、無線ＬＡＮ端末１０３の制御部は、通信相手となる無線ＬＡＮ端末１０１（以下相手端末という。）との通信を開始しようとする際、まずアクセスポイント１０２に帰属する（ステップ２０１）。続いて、制御部は相手端末１０１に対してセキュリティ機能情報および現在の接続設定情報を含む接続情報の要求を無線通信部を通して送信し（ステップ２０２）、その応答として相手端末１０１からセキュリティ機能情報と現在の接続設定情報とを取得する（ステップ２０３）。

[0026] 続いて、制御部は、相手端末１０１の現在の接続設定情報から接続１０４のセキュリティレベルが自端末のセキュリティポリシを満たすか否かを判定する（ステップ２０４）。相手端末１０１の現在の接続１０４が自端末のセキュリティポリシを満たすセキュリティレベルを有するならば（ステップ２０４：ＹＥＳ）、アクセスポイント１０２を介した現在の接続１０４はセキュリティポリシを満たしているので、制御部はアクセスポイント１０２を介した中継接続を選択し、アクセスポイント１０２との間に接続１０６を確立し相手端末との通信を開始する（ステップ２０５）。

[0027] これに対して、相手端末１０１の現在の接続１０４が自端末のセキュリティポリシを満たさないならば（ステップ２０４：ＮＯ）、制御部は相手端末１０１のセキュリティ機能情報から相手端末１０１と直接接続した場合にセキュリティポリシを満たす通信が可能かどうかを判定する（ステップ２０６）。言い換えれば、相手端末１０１に搭載されたセキュリティ機能情報から、相手端末１０１との間のセキュリティをセキュリティポリシを満たすレベルまで直接上げることが可能かどうかを判断する。具体的には、相手端末１

０１は、接続１０４を介してＷＥＰでアクセスポイント１０２に接続されているが、セキュリティ機能としてはＷＥＰ／ＴＫＩＰ／ＡＥＳに対応している。したがって、無線ＬＡＮ端末１０３が自らアクセスポイントとなって相手端末１０１と直接接続することで、ＡＥＳを用いた接続を確立することが可能である。よって、無線ＬＡＮ端末１０３は接続１０６を確立し相手端末１０１とＡＥＳを用いて直接通信を開始する（ステップ２０７）。あるいは、相手端末１０１がアクセスポイントとして動作する機能を有している場合には、無線ＬＡＮ端末１０３は、相手端末１０１へアクセスポイントとして動作するように要求し、必要なセキュリティレベルであるＡＥＳを用いた接続を確立することも可能である。

[0028] ２．２）効果

以上説明したように、本実施例によれば、相手端末１０１とアクセスポイント１０２との間のセキュリティレベルが自端末１０３の要求するレベルを満たす場合には、アクセスポイント１０２を介して相手端末１０１と通信を行うことで、自端末がアクセスポイントとして動作する必要がなくなる。また、相手端末１０１とアクセスポイント１０２との間のセキュリティレベルが自端末１０３の要求するレベルに満たない場合には、相手端末１０１と直接通信することでセキュリティのレベルを確保することができる。

[0029] このように相手端末１０１とアクセスポイント１０２との間の既存の接続の状況を確認することで、直接通信の必要性の有無を確認することができ、必要なセキュリティレベルの通信を省電力で行うことが可能となる。

[0030] ３．第２実施例

３．１）通信制御

次に、本発明の第２実施例による無線ＬＡＮ端末の通信制御方法を図４を参照しながら詳細に説明する。なお、本実施例による無線ＬＡＮ端末は図１における無線ＬＡＮ端末１０３に対応するものであり、アクセスポイント１０２あるいは通信相手となる無線ＬＡＮ端末１０１と直接無線通信を行うための無線通信部と、次に述べる通信制御を実行する制御部あるいはプログラ

ム制御プロセッサとが設けられているものとする（詳細は、図６を参照しながら後で説明する。）。また、本実施例においては、無線ＬＡＮ端末１０３のセキュリティポリシでセキュリティの優先順位は特に定めず、ＡＥＳかＴＫＩＰのいずれかで通信できればよいものとする。

[0031] 図４において、無線ＬＡＮ端末１０３の制御部は、相手端末１０１との通信を開始しようとする際、まずアクセスポイント１０２に帰属し、その時にアクセスポイント１０２のセキュリティ機能（ここではＷＥＰ／ＴＫＩＰ）を取得する（ステップ３０１）。続いて、制御部は相手端末１０１に対してセキュリティ機能情報および現在の接続設定情報を含む接続情報の要求を無線通信部を通して送信し（ステップ３０２）、その応答として相手端末からセキュリティ機能情報と現在の接続設定情報とを取得する（ステップ３０３）。

[0032] 続いて、制御部は、相手端末１０１の現在の接続設定情報から接続１０４のセキュリティレベルが自端末のセキュリティポリシを満たすか否かを判定する（ステップ３０４）。相手端末１０１の現在の接続１０４が自端末のセキュリティポリシを満たすセキュリティレベルを有するならば（ステップ３０４：ＹＥＳ）、アクセスポイント１０２を介した現在の接続１０４はセキュリティポリシを満たしているので、制御部はアクセスポイント１０２を介した中継接続を選択し、アクセスポイント１０２との間に接続１０６を確立し相手端末１０１との通信を開始する（ステップ３０５）。

[0033] これに対して、相手端末１０１の現在の接続１０４が自端末のセキュリティポリシを満たさないならば（ステップ３０４：ＮＯ）、制御部は接続１０４および１０５のセキュリティレベルを上げることでセキュリティポリシを満たすことが可能かどうか判断する（ステップ３０６）。可能であれば（ステップ３０６：ＹＥＳ）、制御部は相手端末１０１に対して高いセキュリティでアクセスポイント１０２と接続するよう要求し（ステップ３０７）、現在の接続１０４をセキュリティポリシを満たす状態にしてアクセスポイント１０２を介した中継接続を選択し、アクセスポイント１０２との間に接続１

０６を確立し相手端末１０１との通信を開始する（ステップ３０８）。

[0034] 接続１０４および１０５のセキュリティレベルを上げることができない場合には（ステップ３０６：ＮＯ）、相手端末１０１のセキュリティ機能情報から相手端末１０１と直接接続した場合にセキュリティポリシを満たす通信が可能かどうかを判定する（ステップ３０９）。言い換えれば、相手端末１０１に搭載されたセキュリティ機能情報から、相手端末１０１との間でセキュリティをセキュリティポリシを満たすレベルまで直接上げることが可能かどうかを判断する。具体的には、相手端末１０１は、接続１０４を介してＷＥＰでアクセスポイント１０２に接続されているが、セキュリティ機能としてはＷＥＰ／ＴＫＩＰ／ＡＥＳに対応している。したがって、無線ＬＡＮ端末１０３が自らアクセスポイントとなって相手端末１０１と直接接続することで、ＡＥＳを用いた接続を確立することが可能である。よって、無線ＬＡＮ端末１０３の制御部は、ＡＥＳを利用した接続１０６を確立し相手端末１０１と直接通信を開始する（ステップ３１０）。あるいは、相手端末１０１がアクセスポイントとして動作する機能を持っていれば、無線ＬＡＮ端末１０３は、相手端末１０１へアクセスポイントとして動作するように要求し、必要なセキュリティレベルであるＡＥＳを用いた接続を確立することも可能である。

[0035] ３．２）効果

以上説明したように、本実施例によれば、相手端末１０１とアクセスポイント１０２との間のセキュリティレベルが自端末１０３の要求するレベルに満たない場合、相手端末１０１と直接通信する前に、相手端末１０１とアクセスポイント１０２との間のセキュリティレベルの増加が可能かどうかを判定する。このセキュリティ増加が可能であれば、自端末１０３あるいは相手端末１０１がアクセスポイントとして動作する必要がなくなり、セキュリティポリシを満たす中継接続で端末間の通信が可能となる。これによって端末の消費電力がさらに抑制されうる。

[0036] ４．第２実施形態

上記第１実施形態では、相手端末１０１のセキュリティに関する情報の入手をアクセスポイント経由で行ったが、これに限定されるものではなく、本発明の第２実施形態によれば、無線ＬＡＮ以外の通信手段により同様の接続情報を入手することも可能である。

[0037] 図５に示す本発明の第２実施形態による無線ＬＡＮシステムにおいて、図１に示すシステムと同様の機能を有するブロックには同一の参照番号が付されている。無線ＬＡＮ端末４０１および４０２は、無線ＬＡＮの通信機能とは別の通信機能４０３を有し、相互に通信可能であるものとする。別の通信機能４０３としては、たとえば短距離無線通信機能ＮＦＣ(Near Field Communication)などが利用できる。あるいは、相手端末４０１の画面に二次元バーコード等を表示し、自端末４０２のカメラでそれを撮影することで情報を入手するといった方法も考えられる。

[0038] 上述したように、相手端末４０１とアクセスポイント１０２との接続１０４ではＷＥＰが使用されている（ステップＳ１０）。自端末４０２は、相手端末４０１との通信を開始しようとする際、ＮＦＣ等を利用して接続情報の要求を送信し（ステップ２１）、それに応答して相手端末４０１が接続情報を返信する（ステップＳ２２）。こうして自端末４０２は、相手端末４０１のセキュリティ機能情報および現在の接続設定情報を取得することができる。

[0039] 自端末４０２は、相手端末４０１から受信したセキュリティ機能情報および現在の接続設定情報と自端末のセキュリティポリシとを比較し、相手端末４０１と直接接続する場合とアクセスポイント１０２を介して中継接続する場合のどちらが必要なセキュリティレベルを満たすかを判定し、セキュリティポリシに合致した接続を選択する（ステップＳ２３ａあるいはＳ２３ｂ）。

[0040] 以上説明したように、本実施形態によれば、無線ＬＡＮ以外の情報取得手段を利用して相手端末４０１から必要な情報を取得する。相手端末４０１とアクセスポイント１０２との間のセキュリティレベルが自端末４０２の要求

するレベルに満たない場合には、既に述べたように、相手端末４０１と直接通信することでセキュリティのレベルを確保することができる。このように相手端末４０１とアクセスポイント１０２との間の既存の接続の状況を確認することで直接通信の必要性の有無を確認することができ、必要なセキュリティレベルの通信を省電力で行うことが可能となる。

[0041] ５．無線ＬＡＮ端末

以下、図６を参照しながら、上述した実施例を実装可能な無線ＬＡＮ端末の構成例を説明する。

[0042] 図６に示すように、無線ＬＡＮ端末には、無線ＬＡＮ通信のための無線通信部５０１および通信制御部５０２が設けられ、さらに、上述した相手端末１０１からのセキュリティ機能情報および現在の接続設定情報を取得する機能を実装した接続情報取得部５０３が設けられている。ＣＰＵ(Central Processing Unit)等のプログラム制御プロセッサ５０４は、通信制御部５０２、接続情報取得部５０３およびセキュリティ情報格納部５０５を図３あるいは図４に示すように制御する。

[0043] セキュリティ情報格納部５０５には、上述したセキュリティポリシを予め登録しておき、接続情報取得部５０３により取得された相手端末１０１のセキュリティ機能情報および現在の接続設定情報と比較することで、その比較結果に応じて図３あるいは図４に示すようにＡＰ中継接続あるいは直接接続のいずれかを選択することができる。このような通信制御機能は、プログラム格納部５０６に記憶されたプログラムをプログラム制御プロセッサ５０４上で実行することにより実現することができる。なお、セキュリティ情報格納部５０５およびプログラム格納部５０６は単体の記憶媒体であってもよく、無線ＬＡＮ端末に着脱可能に取り付けられてもよい。

[0044] なお、第２実施形態で説明したように、短距離無線通信機能ＮＦＣを利用した無線ＬＡＮ端末であれば、接続情報取得部５０３に短距離無線通信部５０７が接続され、相手端末１０１からセキュリティ機能情報および現在の接続設定情報が取得される。

[0045] 上述したように、相手端末側のセキュリティレベルがセキュリティポリシが要求するレベルを満たせば、プログラム制御プロセッサ５０４は通信制御部５０２を制御してアクセスポイント１０２を介した中継接続を選択し、したがって通信制御部５０２はアクセスポイントとして動作する必要がなくなる。また、相手側のセキュリティレベルがセキュリティポリシが要求するレベルを満たさない場合には、自端末あるいは相手端末がアクセスポイントとして動作して相手と直接通信することでセキュリティのレベルを確保することができる。このように相手側の既存の接続状況を確認することで、直接通信の必要性の有無を確認することができ、必要なセキュリティレベルの通信を省電力で行うことが可能となる。

[0046] ６．付記

上述した実施形態の一部あるいは全部は、以下の付記のようにも記載されうるが、これらに限定されるものではない。

[0047] （付記１）

少なくとも１つのアクセスポイントを有する無線ＬＡＮ（ローカルエリアネットワーク）システムにおける無線ＬＡＮ通信端末であって、

通信相手となる無線ＬＡＮ通信端末（以下、相手端末という。）がアクセスポイントと接続されている場合、前記相手端末が有するセキュリティ機能情報と前記アクセスポイントとの現在の接続情報とを前記相手端末から取得する取得手段と、

前記相手端末の前記セキュリティ機能情報および前記接続情報と、自端末のセキュリティポリシとを比較し、前記比較結果に基づいて当該セキュリティポリシを満たすように前記相手端末との直接接続あるいは前記アクセスポイントを介した中継接続のいずれかを選択する選択手段と、

前記選択された接続を用いて前記相手端末との通信を行う通信手段と、

を有することを特徴とする無線ＬＡＮ通信端末。

[0048] （付記２）

前記選択手段は、前記現在の接続情報が前記セキュリティポリシを満たす

場合には前記中継接続を選択し、前記接続情報が前記セキュリティポリシを満たさない場合には前記相手端末のセキュリティ機能のうち前記セキュリティポリシを満たすものを利用して前記直接接続あるいは前記中継接続を選択することを特徴とする付記１に記載の無線ＬＡＮ通信端末。

[0049]（付記３）

前記接続情報が前記セキュリティポリシを満たさない場合には、前記アクセスポイントのセキュリティ機能および前記相手端末のセキュリティ機能のうち前記セキュリティポリシを満たすものを利用して前記中継接続を選択することを特徴とする付記２に記載の無線ＬＡＮ通信端末。

[0050]（付記４）

前記通信手段は、前記直接接続の場合には、自端末を無線ＬＡＮのアクセスポイントとして機能させるか、あるいは前記相手端末を無線ＬＡＮのアクセスポイントとして機能させるように要求する、ことを特徴とする付記１－３のいずれか１項に記載の無線ＬＡＮ通信端末。

[0051]（付記５）

前記取得手段は、前記アクセスポイントを通して、あるいは前記無線ＬＡＮシステムとは別の通信手段を通して、前記相手端末の前記セキュリティ機能情報および前記接続情報を取得することを特徴とする付記１－４のいずれか１項に記載の無線ＬＡＮ通信端末。

[0052]（付記６）

少なくとも１つのアクセスポイントを有する無線ＬＡＮ（ローカルエリアネットワーク）システムにおける無線ＬＡＮ通信端末の通信制御方法であって、

取得手段が、通信相手となる無線ＬＡＮ通信端末（以下、相手端末という。）がアクセスポイントと接続されている場合、前記相手端末が有するセキュリティ機能情報と前記アクセスポイントとの現在の接続情報とを前記相手端末から取得し、

選択手段が、前記相手端末の前記セキュリティ機能情報および前記接続情

報と、自端末のセキュリティポリシとを比較し、前記比較結果に基づいて当該セキュリティポリシを満たすように前記相手端末との直接接続あるいは前記アクセスポイントを介した中継接続のいずれかを選択し、

通信手段が前記選択された接続を用いて前記相手端末との通信を行う、

ことを特徴とする通信制御方法。

[0053] （付記７）

前記選択手段は、前記現在の接続情報が前記セキュリティポリシを満たす場合には前記中継接続を選択し、前記接続情報が前記セキュリティポリシを満たさない場合には前記相手端末のセキュリティ機能のうち前記セキュリティポリシを満たすものを利用して前記直接接続あるいは前記中継接続を選択することを特徴とする付記６に記載の通信制御方法。

[0054] （付記８）

前記接続情報が前記セキュリティポリシを満たさない場合には、前記アクセスポイントのセキュリティ機能および前記相手端末のセキュリティ機能のうち前記セキュリティポリシを満たすものを利用して前記中継接続を選択することを特徴とする付記７に記載の通信制御方法。

[0055] （付記９）

前記通信手段は、前記直接接続の場合には、自端末を無線ＬＡＮのアクセスポイントとして機能させるか、あるいは前記相手端末を無線ＬＡＮのアクセスポイントとして機能させるように要求する、ことを特徴とする付記６－８のいずれか１項に記載の通信制御方法。

[0056] （付記１０）

前記取得手段は、前記アクセスポイントを通して、あるいは前記無線ＬＡＮシステムとは別の通信手段を通して、前記相手端末の前記セキュリティ機能情報および前記接続情報を取得することを特徴とする付記６－９のいずれか１項に記載の通信制御方法。

[0057] （付記１１）

少なくとも１つのアクセスポイントと複数の無線ＬＡＮ通信端末とを有す

る無線ＬＡＮ（ローカルエリアネットワーク）システムにおいて、

無線ＬＡＮ通信端末が、

通信相手となる無線ＬＡＮ通信端末（以下、相手端末という。）がアクセスポイントと接続されている場合、前記相手端末が有するセキュリティ機能情報と前記アクセスポイントとの現在の接続情報とを前記相手端末から取得する取得手段と、

前記相手端末の前記セキュリティ機能情報および前記接続情報と、自端末のセキュリティポリシとを比較し、前記比較結果に基づいて当該セキュリティポリシを満たすように前記相手端末との直接接続あるいは前記アクセスポイントを介した中継接続のいずれかを選択する選択手段と、

前記選択された接続を用いて前記相手端末との通信を行う通信手段と、

を有することを特徴とする無線ＬＡＮシステム。

[0058]（付記１２）

前記選択手段は、前記現在の接続情報が前記セキュリティポリシを満たす場合には前記中継接続を選択し、前記接続情報が前記セキュリティポリシを満たさない場合には前記相手端末のセキュリティ機能のうち前記セキュリティポリシを満たすものを利用して前記直接接続あるいは前記中継接続を選択することを特徴とする付記１１に記載の無線ＬＡＮシステム。

[0059]（付記１３）

前記接続情報が前記セキュリティポリシを満たさない場合には、前記アクセスポイントのセキュリティ機能および前記相手端末のセキュリティ機能のうち前記セキュリティポリシを満たすものを利用して前記中継接続を選択することを特徴とする付記１２に記載の無線ＬＡＮシステム。

[0060]（付記１４）

前記通信手段は、前記直接接続の場合には、自端末を無線ＬＡＮのアクセスポイントとして機能させるか、あるいは前記相手端末を無線ＬＡＮのアクセスポイントとして機能させるように要求する、ことを特徴とする付記１１－１３のいずれか１項に記載の無線ＬＡＮシステム。

[0061] （付記１５）

前記取得手段は、前記アクセスポイントを通して、あるいは前記無線ＬＡＮシステムとは別の通信手段を通して、前記相手端末の前記セキュリティ機能情報および前記接続情報を取得することを特徴とする付記１１－１４のいずれか１項に記載の無線ＬＡＮシステム。

[0062] （付記１６）

少なくとも１つのアクセスポイントを有する無線ＬＡＮ（ローカルエリアネットワーク）システムにおける無線ＬＡＮ通信端末のプログラム制御プロセッサを機能させるプログラムであって、

通信相手となる無線ＬＡＮ通信端末（以下、相手端末という。）がアクセスポイントと接続されている場合、前記相手端末が有するセキュリティ機能情報と前記アクセスポイントとの現在の接続情報とを前記相手端末から取得する取得機能と、

前記相手端末の前記セキュリティ機能情報および前記接続情報と、自端末のセキュリティポリシとを比較し、前記比較結果に基づいて当該セキュリティポリシを満たすように前記相手端末との直接接続あるいは前記アクセスポイントを介した中継接続のいずれかを選択する選択機能と、

前記選択された接続を用いて前記相手端末との通信を行う通信機能と、

を有する無線ＬＡＮ通信端末として前記プログラム制御プロセッサを機能させるプログラム。

[0063] （付記１７）

前記選択機能は、前記現在の接続情報が前記セキュリティポリシを満たす場合には前記中継接続を選択し、前記接続情報が前記セキュリティポリシを満たさない場合には前記相手端末のセキュリティ機能のうち前記セキュリティポリシを満たすものを利用して前記直接接続あるいは前記中継接続を選択することを特徴とする付記１６に記載のプログラム。

[0064] （付記１８）

前記接続情報が前記セキュリティポリシを満たさない場合には、前記アク

セスポイントのセキュリティ機能および前記相手端末のセキュリティ機能のうち前記セキュリティポリシを満たすものを利用して前記中継接続を選択することを特徴とする付記１７に記載のプログラム。

[0065] （付記１９）

前記通信手段は、前記直接接続の場合には、自端末を無線ＬＡＮのアクセスポイントとして機能させるか、あるいは前記相手端末を無線ＬＡＮのアクセスポイントとして機能させるように要求する、ことを特徴とする付記１６－１８のいずれか１項に記載のプログラム。

[0066] （付記２０）

前記取得手段は、前記アクセスポイントを通して、あるいは前記無線ＬＡＮシステムとは別の通信手段を通して、前記相手端末の前記セキュリティ機能情報および前記接続情報を取得することを特徴とする付記１６－１９のいずれか１項に記載のプログラム。

産業上の利用可能性

[0067] 本発明は、無線ＬＡＮ端末、特に無線ＬＡＮを近距離通信方式として利用するシステムに提供可能である。

符号の説明

[0068] １０１、１０３、４０１、４０２　無線ＬＡＮ端末

１０２　アクセスポイント

１０４，１０５，１０６　接続

５０１　無線通信部

５０２　通信制御部

５０３　接続情報取得部

５０４　プログラム制御プロセッサ

５０５　セキュリティ情報格納部

５０６　プログラム格納部

請求の範囲

[請求項1] 少なくとも１つのアクセスポイントを有する無線ＬＡＮ（ローカルエリアネットワーク）システムにおける無線ＬＡＮ通信端末であって、

通信相手となる無線ＬＡＮ通信端末（以下、相手端末という。）がアクセスポイントと接続されている場合、前記相手端末が有するセキュリティ機能情報と前記アクセスポイントとの現在の接続情報とを前記相手端末から取得する取得手段と、

前記相手端末の前記セキュリティ機能情報および前記接続情報と、自端末のセキュリティポリシとを比較し、前記比較結果に基づいて当該セキュリティポリシを満たすように前記相手端末との直接接続あるいは前記アクセスポイントを介した中継接続のいずれかを選択する選択手段と、

前記選択された接続を用いて前記相手端末との通信を行う通信手段と、

を有することを特徴とする無線ＬＡＮ通信端末。

[請求項2] 前記選択手段は、前記現在の接続情報が前記セキュリティポリシを満たす場合には前記中継接続を選択し、前記現在の接続情報が前記セキュリティポリシを満たさない場合には前記相手端末のセキュリティ機能のうち前記セキュリティポリシを満たすものを利用して前記直接接続あるいは前記中継接続を選択することを特徴とする請求項１に記載の無線ＬＡＮ通信端末。

[請求項3] 前記現在の接続情報が前記セキュリティポリシを満たさない場合には、前記アクセスポイントのセキュリティ機能および前記相手端末のセキュリティ機能のうち前記セキュリティポリシを満たすものを利用して前記中継接続を選択することを特徴とする請求項２に記載の無線ＬＡＮ通信端末。

[請求項4] 前記通信手段は、前記直接接続の場合には、自端末を無線ＬＡＮの

アクセスポイントとして機能させるか、あるいは前記相手端末を無線ＬＡＮのアクセスポイントとして機能させるように要求する、ことを特徴とする請求項１－３のいずれか１項に記載の無線ＬＡＮ通信端末。

［請求項5］ 少なくとも１つのアクセスポイントを有する無線ＬＡＮ（ローカルエリアネットワーク）システムにおける無線ＬＡＮ通信端末の通信制御方法であって、

取得手段が、通信相手となる無線ＬＡＮ通信端末（以下、相手端末という。）がアクセスポイントと接続されている場合、前記相手端末が有するセキュリティ機能情報と前記アクセスポイントとの現在の接続情報とを前記相手端末から取得し、

選択手段が、前記相手端末の前記セキュリティ機能情報および前記接続情報と、自端末のセキュリティポリシとを比較し、前記比較結果に基づいて当該セキュリティポリシを満たすように前記相手端末との直接接続あるいは前記アクセスポイントを介した中継接続のいずれかを選択し、

通信手段が前記選択された接続を用いて前記相手端末との通信を行う、

ことを特徴とする通信制御方法。

［請求項6］ 前記選択手段は、前記現在の接続情報が前記セキュリティポリシを満たす場合には前記中継接続を選択し、前記現在の接続情報が前記セキュリティポリシを満たさない場合には前記相手端末のセキュリティ機能のうち前記セキュリティポリシを満たすものを利用して前記直接接続あるいは前記中継接続を選択することを特徴とする請求項５に記載の通信制御方法。

［請求項7］ 前記現在の接続情報が前記セキュリティポリシを満たさない場合には、前記アクセスポイントのセキュリティ機能および前記相手端末のセキュリティ機能のうち前記セキュリティポリシを満たすものを利用

して前記中継接続を選択することを特徴とする請求項６に記載の通信制御方法。

[請求項8] 前記通信手段は、前記直接接続の場合には、自端末を無線ＬＡＮのアクセスポイントとして機能させるか、あるいは前記相手端末を無線ＬＡＮのアクセスポイントとして機能させるように要求する、ことを特徴とする請求項５－７のいずれか１項に記載の通信制御方法。

[請求項9] 少なくとも１つのアクセスポイントと複数の無線ＬＡＮ通信端末とを有する無線ＬＡＮ（ローカルエリアネットワーク）システムにおいて、

無線ＬＡＮ通信端末が、

通信相手となる無線ＬＡＮ通信端末（以下、相手端末という。）がアクセスポイントと接続されている場合、前記相手端末が有するセキュリティ機能情報と前記アクセスポイントとの現在の接続情報とを前記相手端末から取得する取得手段と、

前記相手端末の前記セキュリティ機能情報および前記接続情報と、自端末のセキュリティポリシとを比較し、前記比較結果に基づいて当該セキュリティポリシを満たすように前記相手端末との直接接続あるいは前記アクセスポイントを介した中継接続のいずれかを選択する選択手段と、

前記選択された接続を用いて前記相手端末との通信を行う通信手段と、

を有することを特徴とする無線ＬＡＮシステム。

[請求項10] 少なくとも１つのアクセスポイントを有する無線ＬＡＮ（ローカルエリアネットワーク）システムにおける無線ＬＡＮ通信端末のプログラム制御プロセッサを機能させるプログラムであって、

通信相手となる無線ＬＡＮ通信端末（以下、相手端末という。）がアクセスポイントと接続されている場合、前記相手端末が有するセキュリティ機能情報と前記アクセスポイントとの現在の接続情報とを前

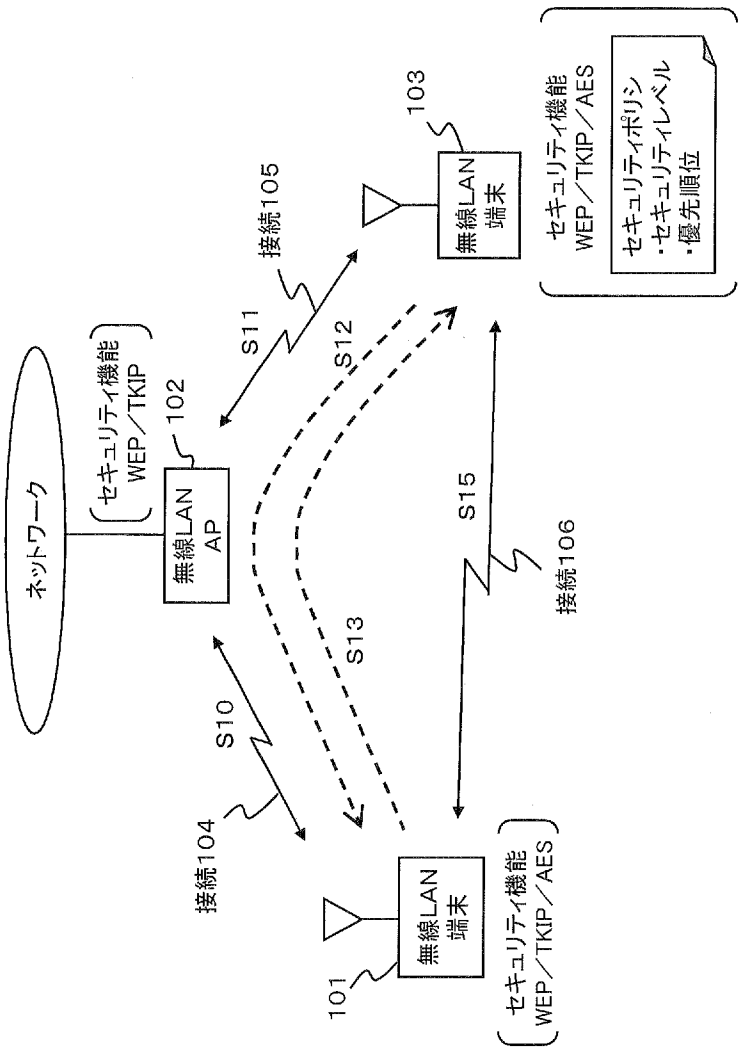
記相手端末から取得する取得機能と、

前記相手端末の前記セキュリティ機能情報および前記接続情報と、自端末のセキュリティポリシとを比較し、前記比較結果に基づいて当該セキュリティポリシを満たすように前記相手端末との直接接続あるいは前記アクセスポイントを介した中継接続のいずれかを選択する選択機能と、

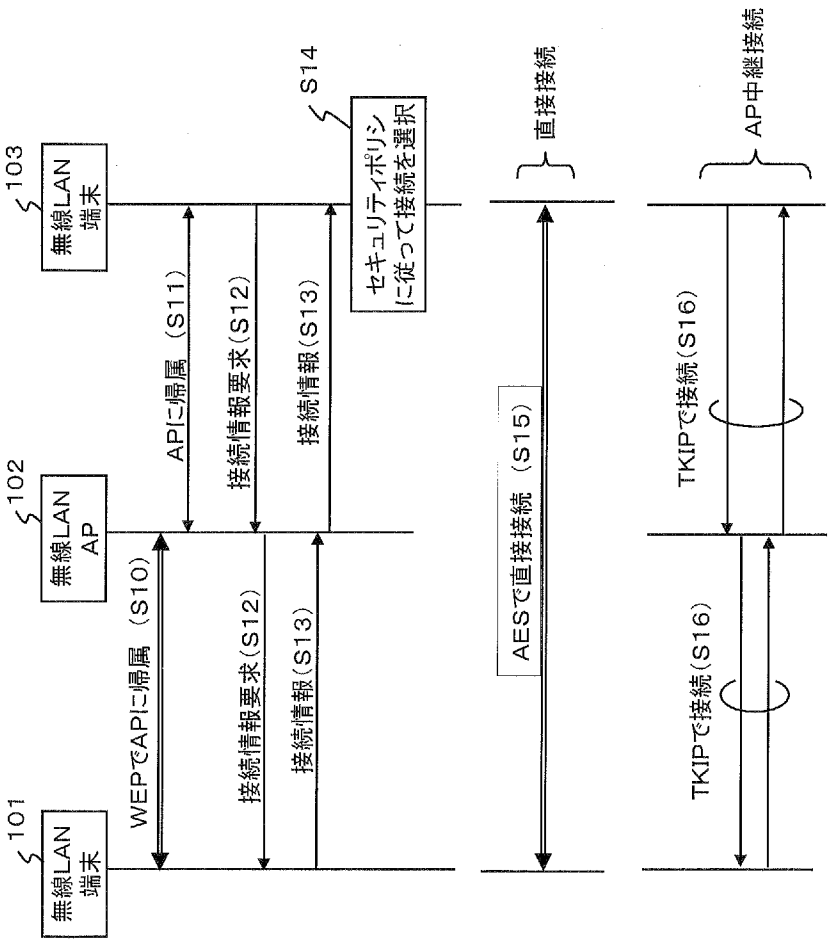
前記選択された接続を用いて前記相手端末との通信を行う通信機能と、

を有する無線ＬＡＮ通信端末として前記プログラム制御プロセッサを機能させるプログラム。

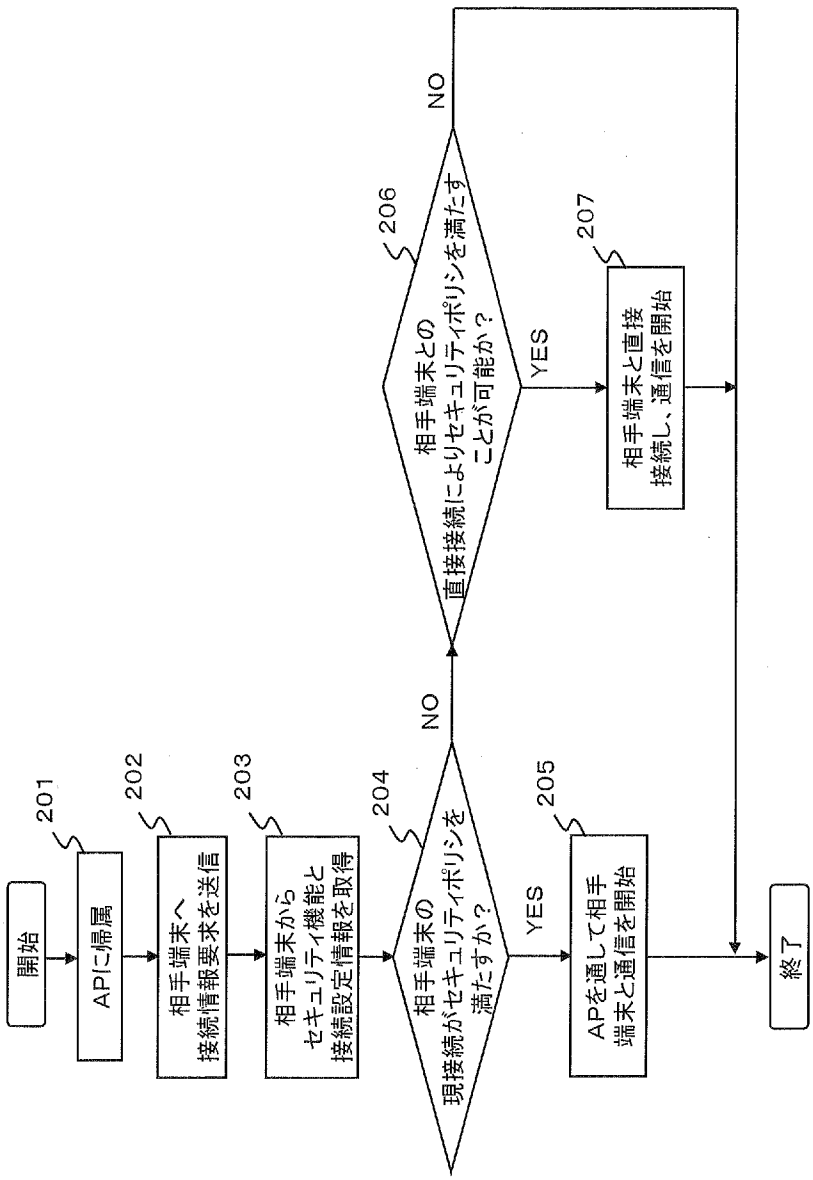
[図1]


ネットワーク
セキュリティ機能
WEP／TKIP
102
無線LAN
AP
S11
接続105
S12
S13
S15
接続106
S10
接続104
103
無線LAN
端末
セキュリティ機能
WEP／TKIP／AES
セキュリティポリシ
・セキュリティレベル
・優先順位
101
無線LAN
端末
セキュリティ機能
WEP／TKIP／AES

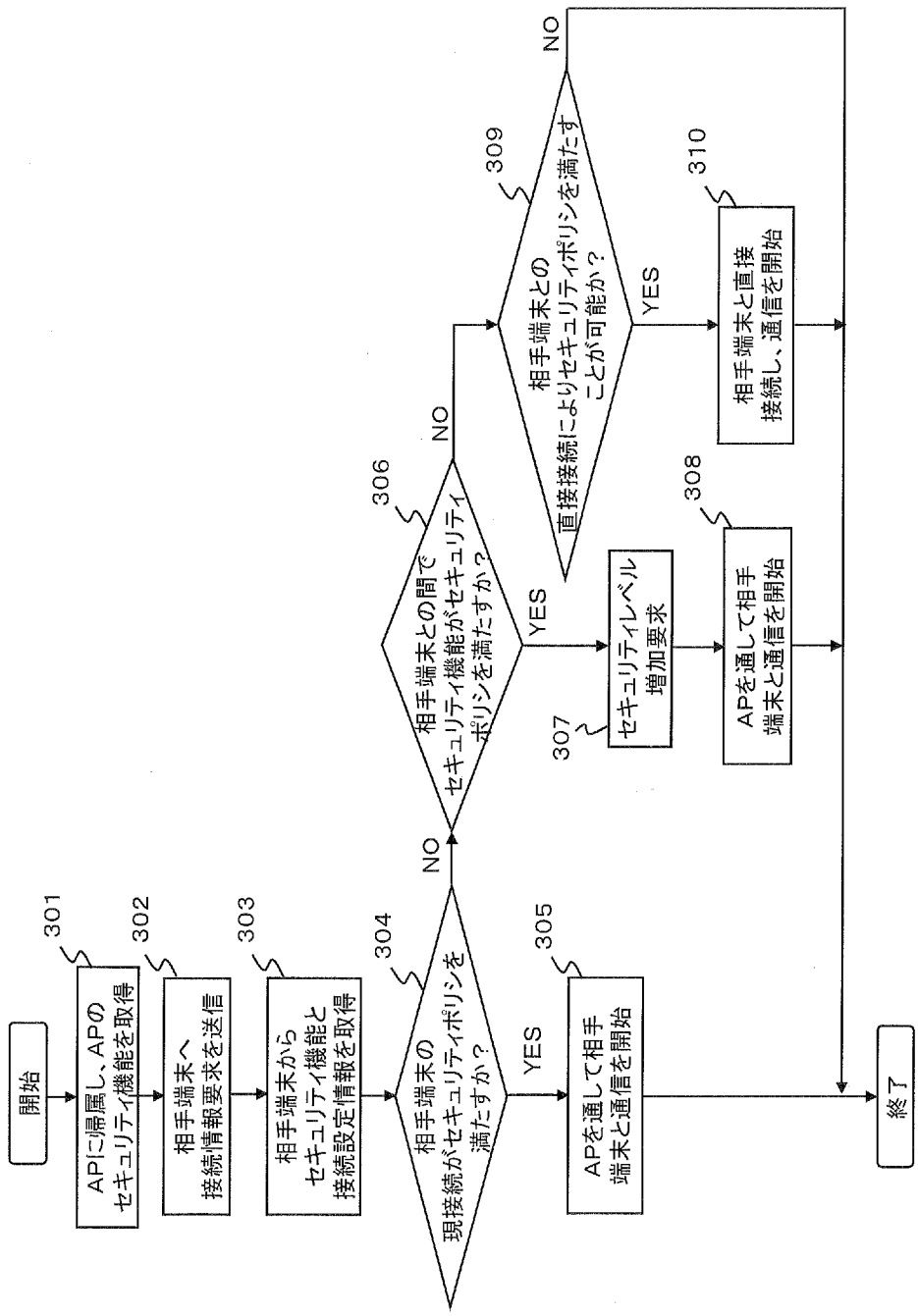
[図2]


101
無線LAN端末
102
無線LAN AP
103
無線LAN端末
WEPでAPに帰属（S10）
APに帰属（S11）
接続情報要求（S12）
接続情報（S13）
S14
セキュリティポリシに従って接続を選択
接続情報要求（S12）
接続情報（S13）
AESで直接接続（S15）
直接接続
TKIPで接続（S16）
TKIPで接続（S16）
AP中継接続

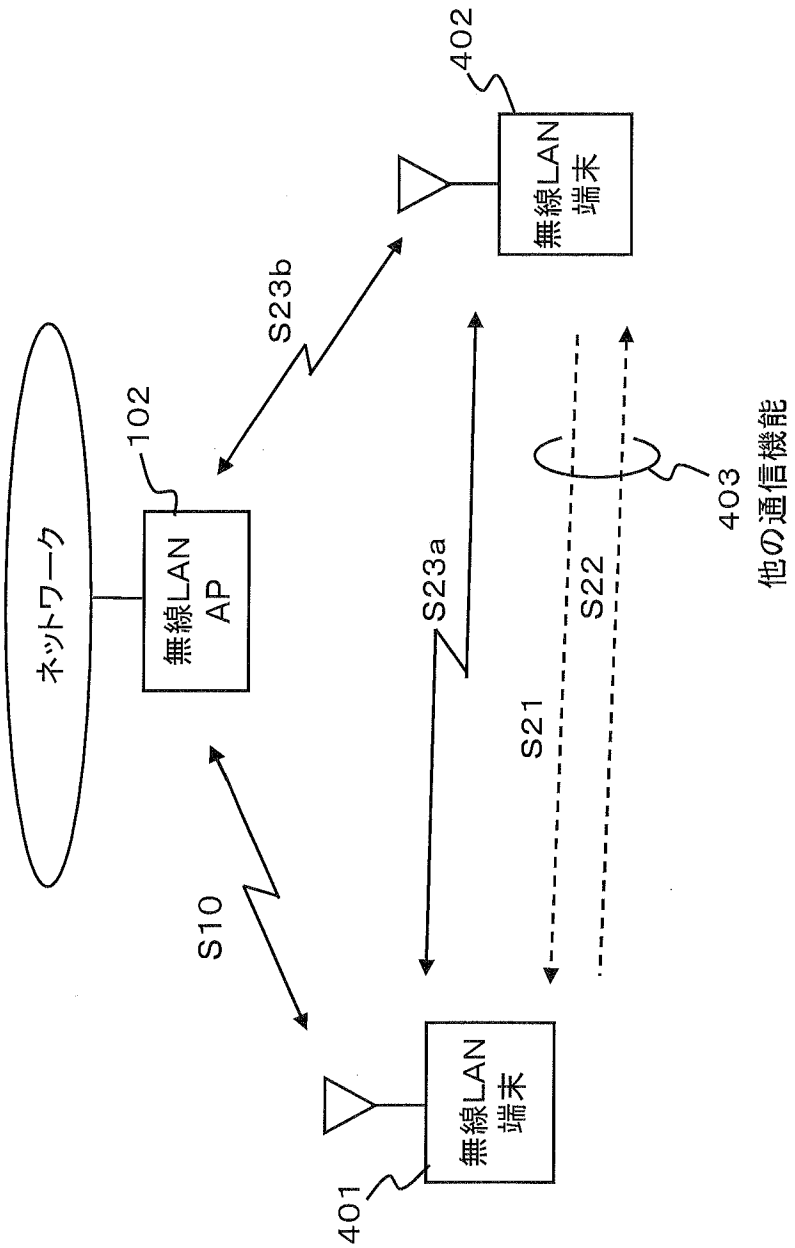
[図3]


開始
201
APに帰属
202
相手端末へ
接続情報要求を送信
203
相手端末から
セキュリティ機能と
接続設定情報を取得
204
相手端末の
現接続がセキュリティポリシを
満たすか？
NO
YES
205
APを通して相手
端末と通信を開始
206
相手端末との
直接接続によりセキュリティポリシを満たす
ことが可能か？
NO
YES
207
相手端末と直接
接続し、通信を開始
終了

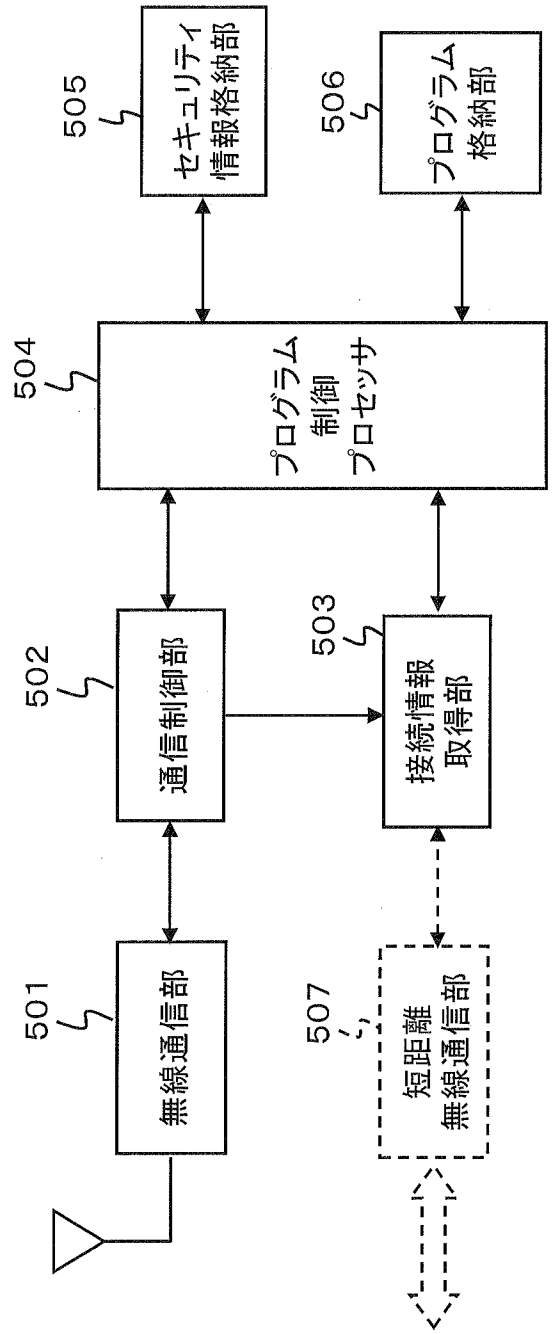
[図4]


開始
APに帰属し、APの
セキュリティ機能を取得
301
相手端末へ
接続情報要求を送信
302
相手端末から
セキュリティ機能と
接続設定情報を取得
303
相手端末の
現接続がセキュリティポリシを
満たすか？
304
YES
APを通して相手
端末と通信を開始
305
NO
相手端末との間で
セキュリティ機能がセキュリティ
ポリシを満たすか？
306
YES
セキュリティレベル
増加要求
307
APを通して相手
端末と通信を開始
308
NO
相手端末との
直接接続によりセキュリティポリシを満たす
ことが可能か？
309
YES
相手端末と直接
接続し、通信を開始
310
NO
終了

[図5]


ネットワーク
無線LAN AP
102
S23b
S23a
S10
S21
S22
403
他の通信機能
無線LAN 端末
401
無線LAN 端末
402

[図6]


505
セキュリティ情報格納部
506
プログラム格納部
504
プログラム制御プロセッサ
502
通信制御部
503
接続情報取得部
501
無線通信部
507
短距離無線通信部

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/004057

A. CLASSIFICATION OF SUBJECT MATTER
H04W12/08(2009.01)i, *H04W84/12*(2009.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W12/08, H04W84/12

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2011
Kokai Jitsuyo Shinan Koho	1971-2011	Toroku Jitsuyo Shinan Koho	1994-2011

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	JP 2009-212732 A (Sony Corp.), 17 September 2009 (17.09.2009), paragraphs [0094] to [0097], [0117], [0125] to [0130] & US 2009/0222659 A1 & CN 101527911 A	1,5,9,10 2-4,6-8
Y	JP 2009-219051 A (Canon Inc.), 24 September 2009 (24.09.2009), paragraphs [0085], [0086] & US 2010/0281525 A1 & WO 2009/113557 A1	2,3,6,7
Y	JP 2008-035371 A (Canon Inc.), 14 February 2008 (14.02.2008), paragraphs [0134] to [0160] & US 2008/0025512 A1	4,8

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 September, 2011 (09.09.11)	20 September, 2011 (20.09.11)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2011/004057

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2009-500969 A (Microsoft Corp.), 08 January 2009 (08.01.2009), paragraphs [0005] to [0008] & US 2007/0008922 A1 & US 2009/0303934 A1 & EP 1902590 A & WO 2007/008857 A2 & KR 10-2008-0032078 A & CN 101218835 A	1-10
A	JP 2008-219358 A (Sony Corp.), 18 September 2008 (18.09.2008), paragraphs [0037] to [0070] (Family: none)	1-10

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１１／００４０５７

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04W12/08(2009.01)i, H04W84/12(2009.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　H04W12/08, H04W84/12

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１１年
日本国実用新案登録公報	１９９６－２０１１年
日本国登録実用新案公報	１９９４－２０１１年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
X Y	JP 2009-212732 A (ソニー株式会社) 2009.09.17, 【0094】-【0097】, 【0117】, 【0125】-【0130】 & US 2009/0222659 A1 & CN 101527911 A	1,5,9,10 2-4,6-8
Y	JP 2009-219051 A (キヤノン株式会社) 2009.09.24, 【0085】,【0086】 & US 2010/0281525 A1 & WO 2009/113557 A1	2,3,6,7
Y	JP 2008-035371 A (キヤノン株式会社) 2008.02.14, 【0134】-【0160】 & US 2008/0025512 A1	4,8

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
０９．０９．２０１１	２０．０９．２０１１

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｊ　３７９４
齋藤　浩兵
電話番号　０３－３５８１－１１０１　内線　３５３４

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2009-500969 A (マイクロソフト コーポレーション) 2009.01.08, 【0005】-【0008】 & US 2007/0008922 A1 & US 2009/0303934 A1 & EP 1902590 A & WO 2007/008857 A2 & KR 10-2008-0032078 A & CN 101218835 A	1-10
A	JP 2008-219358 A (ソニー株式会社) 2008.09.18, 【0037】-【0070】 (ファミリーなし)	1-10