(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
2014 年 9 月 25 日(25.09.2014)

WIPO | PCT

(10) 国際公開番号
WO 2014/148448 A1

(51) 国際特許分類:
H04W 4/00 (2009.01) *H04W 88/06* (2009.01)
H04W 12/08 (2009.01)

(21) 国際出願番号: PCT/JP2014/057206

(22) 国際出願日: 2014 年 3 月 17 日(17.03.2014)

(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 2013-059464 2013 年 3 月 22 日(22.03.2013) JP

(71) 出願人: ヤマハ株式会社(YAMAHA CORPORATION) [JP/JP]; 〒4308650 静岡県浜松市中区中沢町１０番１号 Shizuoka (JP).

(72) 発明者: 浅野 貴裕(ASANO Takahiro); 〒4308650 静岡県浜松市中区中沢町１０番１号 ヤマハ株式会社内 Shizuoka (JP). 木村 俊洋(KIMURA Toshihiro); 〒4308650 静岡県浜松市中区中沢町１０番１号 ヤマハ株式会社内 Shizuoka (JP).

(74) 代理人: 本多 弘徳(HONDA Hironori); 〒1050003 東京都港区西新橋一丁目７番１３号 虎ノ門イーストビルディング１０階 栄光特許事務所 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, BN, 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, IR, IS, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, 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, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, 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, KM, 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 NETWORK SYSTEM, TERMINAL MANAGEMENT DEVICE, WIRELESS RELAY DEVICE, AND COMMUNICATIONS METHOD

(54) 発明の名称 : 無線ネットワークシステム、端末管理装置、無線中継装置、および通信方法

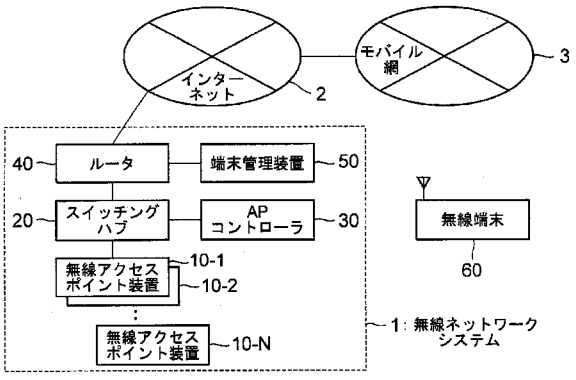


Fig. 1
1 Wireless network system
2 Internet
3 Mobile network
10-1, 10-N Wireless access point device
20 Switching hub
30 AP controller
40 Router
50 Terminal management device
60 Wireless terminal

(57) **Abstract**: Provided is a technology whereby only wireless terminals that meet a security policy are connected to a company internal network, without resulting in large cost increases. A wireless network system configuring a company internal network and including wireless access point devices that connect wireless terminals to which prescribed connection information is set, and having provided therein a terminal management device having: a determination means that communicates with wireless terminals via a communications network different from the wireless network system, and determines whether or not the wireless terminals meet a predetermined security policy; and a connection information transmission means that sends the connection information to wireless terminals determined by the determination means to have met the security policy.

(57) 要約: コストの大幅な増加を招くことなく、セキュリティポリシを満たす無線端末のみが社内ネットワークに接続されるようにする技術を提供する。社内ネットワークを構成し、所定の接続情報を設定された無線端末を接続する無線アクセスポイント装置を含む無線ネットワークシステムに、当該無線ネットワークシステムとは異なる通信網を介して無線端末と通信して予め定められたセキュリティポリシを満たすか否かを判定する判定手段と、セキュリティポリシを満たすと判定手段により判定された無線端末へ上記接続情報を送信する接続情報送信手段とを有する端末管理装置を設ける。

WO 2014/148448 A1

明　細　書

発明の名称 ：

無線ネットワークシステム、端末管理装置、無線中継装置、および通信方法

技術分野

[0001] この発明は、セキュリティホールを有していないこと等の予め定められたセキュリティポリシを満たす端末のみが無線ネットワークシステムに接続されるようにする技術に関する。

背景技術

[0002] スマートフォンやタブレット端末などのスマートデバイスが急速に普及している。この種のスマートデバイスは、従来のＰＤＡ（Personal Digital Assistant）やノート型パソコンとは異なり、アプリケーションプログラムの実行機能や通信機能、撮像機能などの多様な機能を有している。このため、この種のスマートデバイスは、個人的な用途だけでなく、ユーザの業務遂行にも利用されることが多く、スマートデバイスの普及に伴ってＢＹＯＤ(Bring Your Own Device)の導入が広がりつつある。具体的には、ユーザの勤務先の社屋内に敷設された社内ネットワークが無線ＬＡＮ（Local Area Network）を含んでいる場合には、当該ユーザの所有するスマートデバイスを無線ＬＡＮを介して社内ネットワークに接続し、当該ユーザの業務遂行に利用する、といった具合である。

[0003] ＢＹＯＤでは、社内ネットワークへのウィルスの侵入や機密漏えいを防ぐために、予め定められたセキュリティポリシを満たす端末装置に対してのみ社内ネットワークへの接続を許可することが一般的である。スマートデバイスの場合、社内ネットワークに含まれる無線ＬＡＮを介してその社内ネットワークに接続することが一般的である。このため、スマートデバイスを対象とするＢＹＯＤを実現するには、無線ＬＡＮなどの無線ネットワークシステムに対応した検疫システムが必要となる。検疫システムとは、社内ネットワ

ークに接続しようとする端末装置が予め定められたセキュリティポリシを満たしているかをチェックするためのシステムである。この種の検疫システムに関する先行技術としては特許文献１や非特許文献１に開示の技術が挙げられる。

[0004] 特許文献１には、社内ネットワークをVLAN（Virtual Local Area Network）を用いて論理的に分割し、そのうちの１つに「検疫用VLAN」の役割を担わせることが記載されている。特許文献１に開示の技術によれば、社内ネットワークに端末装置を接続する際には、まず、検疫用VLANに接続してセキュリティポリシを満たすか否かをチェックし、セキュリティポリシを満たす場合には業務遂行用のVLANに接続することで私物端末の検疫が実現される。一方、非特許文献１には、接続先をリアルタイム監視する専用のソフトウェアを端末にインストールし、そして接続先が社内ネットワークであるか一般公衆回線などの他のネットワークであるかを識別し、その識別結果に応じて端末の通信設定等を切り替える（例えば、社内ネットワークに接続されている間は社外へのｗｅｂアクセスを禁止する等）ことで機密情報の漏えいを防止する技術が開示されている。

先行技術文献

特許文献

[0005] 特許文献1：日本国特開２００６－３３１１２８号公報

非特許文献

[0006] 非特許文献1：日川佳三、“接続先ネットに応じ仕事と私用モードを切り替えるＭＤＭ、ベーシックが発表”、[ｏｎｌｉｎｅ]、平成２４年９月１０日、株式会社　日経ＢＰ、平成２５年３月２１日検索、インターネット<URL http://itpro.nikkeibp.co.jp/article/NEWS/20120910/421722/>

発明の概要

発明が解決しようとする課題

[0007] 特許文献１に開示の技術には、社内ネットワークを複数のVLANに分割する

必要があるため、システムが複雑化するといった問題や、初期設定や運用のためのコストが増加するといった問題がある。一方、非特許文献１に開示の技術には、社内ネットワークに接続するまで端末の設定が切り替えられないため、不正な設定のままで社内ネットワークへの接続が為される虞があるといった問題がある。

[0008] 本発明は上記課題に鑑みて為されたものであり、コストの大幅な増加を招くことなく、セキュリティポリシを満たす無線端末のみが社内ネットワークに接続されるようにする技術を提供することを目的とする。

課題を解決するための手段

[0009] 上記課題を解決するために本発明は、無線中継装置と端末管理装置とを含む無線ネットワークシステムにおいて、前記端末管理装置は、当該無線ネットワークシステムとは異なる通信網を介して無線端末と通信し、当該無線端末が予め定められたセキュリティポリシを満たしているか否かを判定する判定手段と、前記セキュリティポリシを満たしていると前記判定手段により判定された無線端末へ前記無線中継装置に接続するための接続情報を送信する接続情報送信手段と、を有することを特徴とする無線ネットワークシステム、を提供する。

[0010] 本発明によれば、無線端末がセキュリティポリシを満たしているか否かが端末管理装置によって判定され、満たしている場合にのみ端末管理装置から無線端末へ接続情報が送信される。この際、接続情報は当該無線ネットワークシステムとは異なる通信網経由で送信するようにしてもよい。ここで接続情報が無ければ無線端末は無線中継装置（具体的には、無線アクセスポイント装置）に接続することはできないのであるから、セキュリティポリシを満たさない無線端末の接続を確実に回避することができる。また、本発明によれば、無線端末がセキュリティポリシを満たすか否かを判定するための検疫用ＶＬＡＮを設ける必要もないため、コスト増加を招かない。したがって、無線端末を収容するための無線ネットワークシステムとして本発明の無線ネットワークシステムを用いて社内ネットワークを構築すれば、コストの大幅

な増加を招くことなく、セキュリティポリシを満たす無線端末のみが当該社内ネットワークに接続されるようにすることを実現することができる。

[0011] 別の態様としては、無線ネットワークシステムのサービスエリア内に無線端末が入ったことを検知する検知装置をさらに設け、端末管理装置には、当該検知装置により検知された無線端末を対象として判定手段によるセキュリティポリシの判定を行わせる態様が考えられる。このような態様によれば、無線ネットワークシステムのサービスエリアに無線端末が入り、当該無線ネットワークシステムへの接続が試みられる直前に当該無線端末の検疫を行うことができ、無線端末の検疫を周期的に行う場合に比較して無線端末のバッテリ消費を抑えることができる。

[0012] また、さらに別の態様としては、無線中継装置に上記検知装置の役割を果たさせる態様が考えられる。例えば、上記無線中継装置が無線アクセスポイント装置である場合には、無線端末から発せられるプローブリクエストの受信を契機として自装置のサービスエリアに無線端末が入ったことを当該無線中継装置（無線アクセスポイント装置）に検知させるのである。このような態様によれば、無線中継装置とは別個に設けたセンサに上記検知装置の役割を担わせる態様に比較して当該センサを設けない分だけコストを低く抑えることができる。

[0013] 別の態様としては、無線中継装置に接続している無線端末と当該無線中継装置を介して通信して前記判定手段による判定を行う処理を端末管理装置に定期的に実行させ、セキュリティポリシを満たさなくなったと前記判定手段により判定されたことを契機として前記無線端末から前記接続情報を削除する処理を端末管理装置に実行させる態様も考えられる。このような態様によれば、無線中継装置に接続された後に無線端末の設定等が変更されるなどしてセキュリティホールが発生することを防止することができるからである。

[0014] また、上記課題を解決するために本発明は、無線中継装置を含む無線ネットワークシステムとは異なる通信網を介して無線端末と通信し、当該無線端末が予め定められたセキュリティポリシを満たしているか否かを判定する判

定手段と、前記セキュリティポリシを満たしていると前記判定手段により判定された無線端末へ前記無線中継装置に接続するための接続情報を送信する接続情報送信手段とを有することを特徴とする端末管理装置、を提供する。

[0015] また、上記課題を解決するために本発明は、無線ネットワークシステムに含まれる無線中継装置において、無線端末から受信したリクエストメッセージの電波強度が所定の閾値を上回っており、かつ前記無線端末の端末識別子が予め登録されたものである場合に、前記端末識別子を上位装置へ通知する端末通知手段と、通信相手の無線端末を制限するためのフィルタを前記上位装置から指示に応じて更新する更新手段と、を有することを特徴とする無線中継装置を提供する。

[0016] また、上記課題を解決するために本発明は、無線中継装置を含む無線ネットワークシステムとは異なる通信網を介して無線端末と通信し、当該無線端末が予め定められたセキュリティポリシを満たしているか否かを判定し、前記セキュリティポリシを満たしていると判定された無線端末へ、前記無線中継装置に接続するための接続情報を送信することを特徴とする通信方法を提供する。

[0017] また、上記課題を解決するために本発明は、無線ネットワークシステムに含まれる無線中継装置における通信方法において、無線端末から受信したリクエストメッセージの電波強度が所定の閾値を上回っており、かつ前記無線端末の端末識別子が予め登録されたものである場合に、前記端末識別子を上位装置へ通知し、前記無線中継装置を介して通信する無線端末を制限するためのフィルタを前記上位装置から指示に応じて更新することを特徴とする通信方法を提供する。

[0018] なお、上記無線中継装置が無線アクセスポイント装置である場合には、上記端末識別子の具体例としてＭＡＣアドレスを挙げることができ、また、上記フィルタの具体例としてＭＡＣアドレスフィルタを挙げることができる。

[0019] また、上記無線中継装置は、前記無線ネットワークシステムとは異なる通信網を介して当該無線中継装置に接続するための接続情報を得た無線端末と

接続し、当該無線端末と前記無線ネットワークシステムによる通信を行う通信手段をさらに有してもよい。

[0020] 例えば、社内ネットワークに含まれる無線ネットワークシステムに、上記無線中継装置として機能する無線アクセスポイント装置と上記端末管理装置とを含めておくことでコストの大幅な増加を招くことなく、セキュリティポリシを満たす無線端末のみが当該無線ネットワークシステムを介して社内ネットワークに接続されるようにすることを実現することができる。

図面の簡単な説明

[0021] [図1]本発明の一実施形態の無線ネットワークシステム１の構成例を示すブロック図である。

[図2]同無線ネットワークシステム１に含まれる無線アクセスポイント装置１０の構成例を示すブロック図である。

[図3]同無線ネットワークシステム１に含まれる端末管理装置５０の構成例を示すブロック図である。

[図4]同実施形態における通信シーケンスを示す図である。

[図5]同実施形態における通信シーケンスを示す図である。

発明を実施するための形態

[0022] 以下、図面を参照しつつ、本発明の実施形態について説明する。

（Ａ：構成）

図１は、本発明の一実施形態の無線ネットワークシステム１を含む通信システムの構成例を示すブロック図である。無線ネットワークシステム１は、例えば企業の社屋内に敷設された無線ＬＡＮであり、当該社屋内に敷設された有線ＬＡＮ（図１では図示略）とともに上記企業における社内ネットワークを形成する。図１に示すように、無線ネットワークシステム１は、無線アクセスポイント装置１０－ｎ（ｎ＝１～Ｎ：Ｎは２以上の整数）、スイッチングハブ２０、ＡＰコントローラ３０、ルータ４０、および端末管理装置５０を含んでいる。なお、以下では、無線アクセスポイント装置１０－ｎ（ｎ＝１～Ｎ）の各々を区別する必要がない場合には「無線アクセスポイント装

置１０」と表記する。

[0023] 無線アクセスポイント装置１０とＡＰコントローラ３０は各々ＬＡＮケーブルなどの信号線によりスイッチングハブ２０に接続されている。無線アクセスポイント装置１０－ｎ（ｎ＝１～Ｎ）の各々は、ＩＥＥＥ８０２．１１等に規定されたプロトコルにしたがってスマートデバイスなどの無線端末を接続する装置である。本実施形態では、各無線アクセスポイント装置１０－ｎは、各々の発する通信電波を充分な強度で受信可能な領域（以下、無線アクセスポイント装置のサービスエリア）によって無線ネットワークシステム１の敷設されている社屋内を被覆できるように当該社屋内の各所に配置されている。

[0024] 図２は、無線アクセスポイント装置１０の構成例を示す図である。図２に示すように無線アクセスポイント装置１０は、制御部１１０、無線通信Ｉ／Ｆ部１２０、記憶部１３０、およびこれら構成要素間のデータ授受を仲介するバス１４０を含んでいる。制御部１１０はＣＰＵ（Central Processing Unit）である。制御部１１０は記憶部１３０（より正確には不揮発性記憶部１３４）に記憶されているプログラムを実行することで無線アクセスポイント装置１０の制御中枢として機能する。無線通信Ｉ／Ｆ部１２０は、アンテナや変調回路・復調回路等を含んでおり（何れも図示略）、制御部１１０から受信したデータを変調して搬送波に重畳し、無線区間へ送出する一方、無線区間から受信した搬送波に重畳されているデータを復調して制御部１１０に与える。

[0025] 記憶部１３０は、揮発性記憶部１３２と不揮発性記憶部１３４を含んでいる。揮発性記憶部１３２は例えばＲＡＭ（Random Access Memory）である。揮発性記憶部１３２は各種プログラムを実行する際のワークエリアとして制御部１１０によって利用される。不揮発性記憶部１３４は例えばＥＥＰＲＯＭ（Electrically Erasable Programmable Read-Only Memory）である。不揮発性記憶部１３４には本実施形態の特徴を顕著に示す処理を制御部１１０に実行させるデータおよびプログラムが記憶されている。

[0026] 不揮発性記憶部１３４に記憶されているデータの一例としては、上記企業の従業者の所有する私物の無線端末のうち、業務遂行にも使用する旨の申請の為された全ての無線端末のＭＡＣアドレスを表すデータの配列であるＭＡＣアドレスリストが挙げられる。また、不揮発性記憶部１３４に格納されているプログラムの一例としては、無線端末の発するプローブリクエストの受信を契機としてその送信元が自装置のサービスエリアに入ったことを検知し、当該無線端末が予め使用申請の為されたものである場合に当該無線端末のＭＡＣアドレスを上位装置（本実施形態では、ＡＰコントローラ３０）へ通知する端末通知処理を制御部１１０に実行させる無線通信プログラムが挙げられる。また、無線通信プログラムにしたがって作動している制御部１１０は、一般的な無線アクセスポイント装置における場合と同様に、ＡＰコントローラ３０から与えられる指示に応じてＭＡＣアドレスフィルタを更新する処理も実行する。

[0027] プローブリクエストとは、最寄の無線アクセスポイント装置に対してネットワーク識別子（例えば、ＥＳＳＩＤ）等のブロードキャストを促すために無線端末が送信する通信メッセージのことを言う。本実施形態の無線アクセスポイント装置１０は、定期的なネットワーク識別子のブロードキャストを行わないことは勿論、上記プローブリクエストを受信してもネットワーク識別子等のブロードキャストを行わないように設定されている。これは、ネットワーク識別子が第三者等に漏えいすることに起因する不正アクセスを防止するためである。

[0028] ＡＰコントローラ３０は、無線アクセスポイント装置１０－ｎ（ｎ＝１～Ｎ）に割り当てるネットワーク識別子や各無線アクセスポイント装置１０－ｎの使用周波数（チャネル）、各無線アクセスポイント装置１０－ｎにおけるＭＡＣアドレスフィルタの設定を一元管理するための装置である。ＡＰコントローラ３０は、無線アクセスポイント装置１０－ｎ毎に当該無線アクセスポイント装置１０－ｎに接続している無線端末の端末識別子（当該無線端末を識別するための情報、本実施形態では、ＭＡＣアドレス）を記憶し、無

線アクセスポイント装置間の無線端末の移動（所謂ハンドオーバ）を検知する機能を有している。

[0029] スイッチングハブ２０はルータ４０に接続されており、このルータ４０には端末管理装置５０が接続されている。なお、無線ネットワークシステム１とともに社内ネットワークを形成する有線ＬＡＮはスイッチングハブ２０に接続されていても良く、また、ルータ４０に接続されていても良い。図１に示すようにルータ４０はインターネット２に接続されている。つまり、無線ネットワークシステム１はルータ４０を介してインターネット２に接続されている。そして、インターネット２には例えば３ＧやＬＴＥ（Long Term Evolution）などの通信規格に準拠したモバイル網３が接続されている。

[0030] 無線端末６０は、上記企業の従業者の所有するスマートデバイスである。無線端末６０は、モバイル網３の基地局（図示略）との間に無線通信リンクを確立してデータ通信する機能（以下、第１の無線通信機能）と、無線アクセスポイント装置１０－ｎ（ｎ＝１～Ｎ）に接続してデータ通信する機能（以下、第２の無線通信機能）とを有している。これら２つの無線通信機能のうち、第２の無線通信機能についてはユーザの指示に応じたオン／オフの切り換えが可能であり、当該第２の無線通信機能をオンにすることをユーザにより指示されると、無線端末６０は、前述したプローブリクエストを送信する。また、無線端末６０には、端末管理装置５０に付与されているホスト名を示す情報が予め記憶されており、当該ホスト名に基づいて端末管理装置５０の通信アドレス（ＩＰアドレス）を特定し、前述した第１の無線通信機能によりモバイル網３およびインターネット２経由で端末管理装置５０とデータ通信する。

[0031] 端末管理装置５０は所謂ＭＤＭ（Mobile Device Management）サーバである。図３は端末管理装置５０の構成例を示す図である。図３に示すように端末管理装置５０は、制御部５１０、通信Ｉ／Ｆ部５２０、記憶部５３０、およびこれら構成要素間のデータ授受を仲介するバス５４０を含んでいる。なお、端末管理装置５０は上記各構成要素の他にも、運用管理者に各種操作を

行わせるためのユーザＩ／Ｆ部や他の機器を接続するために外部機器Ｉ／Ｆ部等を有しているが、本実施形態の特徴との関連が薄いため図示および説明を省略する。

[0032] 制御部５１０は、無線アクセスポイント装置１０における制御部１１０と同様にＣＰＵであり、記憶部５３０（より正確には不揮発性記憶部５３４）に記憶されているプログラムを実行することで端末管理装置５０の制御中枢として機能する。通信Ｉ／Ｆ部５２０は例えばＮＩＣであり、ＬＡＮケーブルなどの信号線を介してルータ４０に接続されている。通信Ｉ／Ｆ部５２０は上記信号線を介してルータ４０から受信したデータを制御部５１０に与える一方、制御部５１０から受け取ったデータを上記信号線を介して送出する。

[0033] 記憶部５３０は、揮発性記憶部５３２と不揮発性記憶部５３４を含んでいる。揮発性記憶部５３２は例えばＲＡＭである。揮発性記憶部５３２は各種プログラムを実行する際のワークエリアとして制御部５１０によって利用される。不揮発性記憶部５３４は例えばハードディスクである。不揮発性記憶部５３４には本実施形態の特徴を顕著に示す処理を制御部５１０に実行させるデータおよびプログラムが記憶されている。

[0034] 不揮発性記憶部５３４に記憶されているデータの一例としては、上記企業におけるセキュリティポリシを表すデータ（以下、セキュリティポリシデータ）が挙げられる。セキュリティポリシデータの具体例としては、無線ネットワークシステム１に接続される端末装置にインストールされているべきＯＳ（Operating System）およびアプリケーションソフトウェアの種類やバージョンを示すデータ、同端末装置にインストールされているべきではないアプリケーションソフトウェアを示すデータが挙げられる。詳細については後述するが、セキュリティポリシデータは、プローブリクエストの送信元の無線端末が上記セキュリティポリシを満たすか否かを判定する（すなわち、当該無線端末の検疫を行う）際に利用される。また、不揮発性記憶部５３４には、無線端末を無線アクセスポイント装置１０へ接続する際に必要となる接

続情報（無線ネットワークシステム１のネットワーク識別子、無線アクセスポイント装置１０との無線通信にて使用する暗号化方法を示す情報およびその暗号化におけるセキュリティキーを示す情報等）も予め記憶されている（図３では図示略）。

[0035] 不揮発性記憶部５３４に格納されているプログラムの一例としては、本実施形態の特徴を顕著に示す検疫処理を制御部５１０に実行させる検疫プログラムが挙げられる。詳細については重複を避けるために動作例において明らかにするが、当該検疫プログラムにしたがって作動している制御部５１０は、ＡＰコントローラ３０からのＭＡＣアドレスの通知を契機として当該ＭＡＣアドレスの示す無線端末とインターネット２およびモバイル網３を介して通信し、当該端末の状態を示す状態情報（インストールされているＯＳおよびアプリケーションソフトウェアの種類やバージョンを示すデータ）を取得し、セキュリティポリシデータの示すセキュリティポリシを満たすか否かを判定する判定手段として機能する。また、検疫プログラムにしたがって作動している制御部５１０は、セキュリティポリシを満たすと判定した無線端末に対して上記接続情報をインターネット２およびモバイル網３経由で送信し記憶させる接続情報送信手段としても機能する。

以上が無線ネットワークシステム１の構成である。

[0036] （Ｂ： 動作）

次いで、無線端末６０のユーザが出社して業務に従事し、退社するまでの流れに沿って本実施形態の動作を説明する。

[0037] 無線端末６０は、ユーザにより無線通信機能をオンにする操作が行われると、前述したプローブリクエストを送信する（図４参照）。無線アクセスポイント装置１０の制御部１１０は、無線端末６０から送信されたプローブリクエストの受信を契機として自装置のサービスエリア内に無線端末６０が入ったことを検知し、端末通知処理の実行を開始する。図４に示すように、制御部１１０は、まず、当該プローブリクエストが所定の条件Ａ（すなわち、電波強度が所定の閾値を上回っていること、および送信元が事前に利用申請

の為された無線端末であること）を満たすか否かを判定する（ステップＳＡ１１０）。具体的には、プローブリクエストの送信元ＭＡＣアドレスがＭＡＣアドレスリストに登録されている場合に制御部１１０は、事前に利用申請の為された無線端末であると判定する。そして、ステップＳＡ１１０の判定結果が“Ｙｅｓ”である場合に、制御部１１０は、当該プローブリクエストの送信元ＭＡＣアドレスをペイロード部に書き込んだフレーム（以下、ＭＡＣアドレス通知フレーム）をＡＰコントローラ３０へ送信する（ステップＳＡ１２０）。

[0038] このようにして無線アクセスポイント装置１０から送信されたＭＡＣアドレス通知フレームはスイッチングハブ２０による中継を経てＡＰコントローラ３０によって受信される。ＡＰコントローラ３０は、受信したＭＡＣアドレス通知フレームに書き込まれているＭＡＣアドレスをスイッチングハブ２０およびルータ４０を介して端末管理装置５０へ通知する（図４参照）。端末管理装置５０の制御部５１０は、当該ＭＡＣアドレスの通知を契機として検疫処理（ステップＳＡ２００）の実行を開始する。

[0039] 図５は、検疫処理における通信の流れを示すシーケンスフローチャートである。図５に示すように、端末管理装置５０の制御部５１０は、ＡＰコントローラ３０から通知されたＭＡＣアドレスの示す装置（本動作例では、無線端末６０）を相手装置としてインターネット２およびモバイル網３経由で通信コネクションを確立し、状態情報を取得する。次いで、制御部５１０は、無線端末６０から取得した状態情報の示す状態が予め定められたセキュリティポリシ（すなわち、セキュリティポリシデータの示すセキュリティポリシ）を満たしているか否かを判定する（ステップＳＡ２１０）。

[0040] そして、制御部５１０は、無線端末６０の状態がセキュリティポリシを満たしている場合（ステップＳＡ２１０の判定結果が“Ｙｅｓ”である場合）のみ、無線アクセスポイント装置１０との間に無線通信コネクションを確立する際に必要となる接続情報をインターネット２およびモバイル網３経由で無線端末６０へ宛てて送信し、記憶させる（ステップＳＡ２２０）。加えて

、制御部５１０は、ＡＰコントローラ３０に対して無線端末６０のＭＡＣアドレスを通知する（図５では図示略）。ＡＰコントローラ３０は、端末管理装置５０からＭＡＣアドレスを受け取ると、当該ＭＡＣアドレスにより識別される端末の無線ネットワークシステム１への接続を許可するようにＭＡＣアドレスフィルタの更新することを指示する更新指示を無線アクセスポイント装置１０－ｎ（ｎ＝１～Ｎ）の各々に与え、無線アクセスポイント装置１０－ｎ（ｎ＝１～Ｎ）の各々は当該更新指示にしたがってＭＡＣアドレスフィルタを更新する。

[0041] 無線端末６０は、端末管理装置５０から受信した接続情報を用いて最寄の無線アクセスポイント装置１０に接続する。前述したように、無線アクセスポイント装置１０においては無線端末６０の接続を許可する旨のＭＡＣアドレスフィルタの設定が為されている。このため、無線端末６０は、最寄の無線アクセスポイント装置１０を介して無線ネットワークシステム１に接続される。これに対して、無線端末６０の状態がセキュリティポリシを満たしていない場合には、端末管理装置５０から無線端末６０へ接続情報が送信されることはない。また、端末管理装置５０からＡＰコントローラ３０へ無線端末６０のＭＡＣアドレスが通知されることはなく、無線端末６０の接続が許可されるように無線アクセスポイント装置１０のＭＡＣアドレスフィルタの更新が行われることはない。このため、無線端末６０が無線ネットワークシステム１に接続されることはない。したがって、無線端末６０が予め定められたセキュリティポリシを満たす場合にのみ無線ネットワークシステム１に接続され、セキュリティポリシを満たさない端末が無線ネットワークシステム１を介して社内ネットワークに接続されることを確実に防止することができる。なお、セキュリティポリシを満たさないために無線端末６０が無線ネットワークシステム１に接続されない場合であっても、無線ネットワークシステム１とは異なる他の無線通信網（例えば、ＷＩ－ＦＩなど）に接続することは勿論可能であり、このような他の無線通信網経由或いはモバイル網３経由でインターネット２にアクセスすることも勿論可能である。

[0042] 上記の要領で無線端末６０が無線ネットワークシステム１に接続されると、端末管理装置５０の制御部５１０は、ルータ４０、スイッチングハブ２０および無線アクセスポイント装置１０を介して無線端末６０から状態情報を定期的に取得し、セキュリティポリシを満たしていることを確認する。そして、無線端末６０の状態がセキュリティポリシを満たさなくなった場合には、制御部５１０は無線ネットワークシステム１の接続情報を無線端末６０から削除し、さらに当該無線端末６０のＭＡＣアドレスをＡＰコントローラ３０へ通知し、当該無線端末６０を接続対象から除外するように各無線アクセスポイント装置１０のＭＡＣアドレスフィルタを再更新させる。セキュリティポリシを満たさなくなった無線端末が接続され続けることはセキュリティ確保の観点から好ましくなく、また、無線アクセスポイント装置への接続完了後に無線端末６０の設定を変更するといった不正を防止するためである。

[0043] 無線端末６０のユーザが退社するなどして無線端末６０が無線アクセスポイント装置１０のサービスエリア外に移動し、接続が切断されると無線アクセスポイント装置１０は当該無線端末６０のＭＡＣアドレスをＡＰコントローラ３０へ通知してハンドオーバの有無を問い合わせる。ＡＰコントローラ３０は、当該無線端末６０が他の無線アクセスポイント装置１０にハンドオーバしているか否かを確認し、ハンドオーバしていない場合には当該無線端末６０のＭＡＣアドレスを端末管理装置５０に通知する。端末管理装置５０の制御部５１０は、当該ＭＡＣアドレスの示す無線端末とインターネット２およびモバイル網３経由で通信し、当該無線端末に記憶されている接続情報を削除する。これは、セキュリティポリシを満たすことを条件に配布した接続情報が不正利用されることを回避するためである。

[0044] ここで注目すべき点は、無線端末６０が予め定められたセキュリティポリシを満たすか否かを判定するための検疫用ＶＬＡＮを別途設ける必要はなく、初期設定や運用のためのコストの増加が発生しないという点である。このように、本実施形態によれば、コストの大幅な増加を招くことなく、セキュリティポリシを満たす端末のみが社内ネットワークに接続されるようにする

ことを実現することができる。なお、上記実施形態では、セキュリティポリシによる保護の対象の社内ネットワークが無線ネットワークシステム１と有線ＬＡＮとにより構成されている場合について説明したが、社内ネットワークが無線ネットワークシステム１のみで構成されていても勿論良い。

[0045] （Ｃ：変形）

以上本発明の実施形態について説明したが、この実施形態を以下のように変形しても勿論良い。

（１）上記実施形態では、無線ネットワークシステム１が敷設された社屋に無線端末６０が入ったことを契機として当該無線端末６０がセキュリティポリシを満たすか否かを判定し、セキュリティポリシを満たす場合に無線アクセスポイント装置１０に接続する際に必要となる接続情報をインターネット２およびモバイル網３経由で端末管理装置５０から無線端末６０に与えた。しかし、無線端末６０が上記社屋内に入る前に（換言すれば、無線アクセスポイント装置１０により無線端末６０が検知される前に）、無線端末６０に接続情報を与えても良い。ただし、この場合は、無線端末６０が予め定められたセキュリティポリシを満たすこと、およびその状態が継続していることを確認するために、インターネット２およびモバイル網３経由で無線端末６０と端末管理装置５０の通信を頻繁に行う必要があり、無線端末６０のバッテリの消費が大きくなるという欠点がある。したがって、上記実施形態のように無線ネットワークシステム１が敷設された社屋に無線端末６０が入ったことを契機として当該無線端末６０がセキュリティポリシを満たすか否かを判定するようにすることが好ましい。

[0046] （２）上記実施形態では、無線ネットワークシステム１が敷設された社屋に無線端末６０が入ったことを検知するセンサの役割を、無線ネットワークシステム１に無線端末を収容するための無線アクセスポイント装置１０に兼ねさせた。しかし、上記実施形態に比較して余分な設備投資が必要となるという欠点はあるものの、無線ネットワークシステム１の敷設された社屋に無線端末６０が入ったことを検知するセンサを無線アクセスポイント装置１０と

は別個に設けても勿論良い。

[0047] （３）上記実施形態では、ＡＰコントローラ３０と端末管理装置５０とを各々別個の装置として無線ネットワークシステム１を構成したが、両者を一体の装置として通信システムを構成しても勿論良い。この場合、ＡＰコントローラ３０と端末管理装置５０の両者の機能を兼ね備えた装置が無線アクセスポイント装置１０に対する上位装置となる。また、上記実施形態では、事前に利用申請の為された無線端末であるか否かの判定を無線アクセスポイント装置に実行させたが、ＡＰコントローラ３０に当該判定を行わせ、無線アクセスポイント装置には受信したプローブリクエストの電波強度が所定の閾値を上回っているか否かの判定のみを行わせるようにしても良い。

[0048] また、上記実施形態では、無線アクセスポイント装置１０に、無線端末から受信したプローブリクエストの電波強度が所定の閾値を上回っており、かつ当該無線端末のＭＡＣアドレス（すなわち、当該無線端末の端末識別子が予め登録されたものである場合に当該ＭＡＣアドレスを上位装置へ通知する端末通知処理と、ＭＡＣアドレスフィルタを上記装置からの指示に応じて更新する処理を実行させた。しかし、これら各処理をスイッチングハブ２０やルータ４０に実行させても良い。例えば、ルータ４０にこれら各処理を実行させる場合には、無線端末から送信されたリクエストメッセージ（例えば、相手装置に対して通信コネクションの確立を要求するＳＹＮメッセージ）を受信したことを契機としてそのリクエストメッセージの電波強度を無線アクセスポイント装置から取得し、その電波強度が所定の閾値を上回っており、かつ前記無線端末の端末識別子（例えば、リクエストメッセージの送信元のＩＰアドレス）が予め登録されたものである場合に当該端末識別子を上位装置（端末管理装置５０）へ通知する処理を実行する端末通知手段と、自装置を介して通信する無線端末を制限するためのフィルタ（例えば、ＩＰアドレスに関するフィルタ）を当該上位装置から指示に応じて更新する処理を実行する更新手段とをルータ４０に設ければ良い。また、ルータ４０は無線アクセスポイント装置の機能を兼ね備えた無線ルータであっても良く、スイッチ

ングハブ２０についても無線アクセスポイント装置の機能を兼ね備えた無線スイッチングハブであっても良い。要は、無線端末とその通信相手との間の通信を中継する無線中継装置（無線アクセスポイント装置、無線スイッチングハブ、無線ルータなど）に、無線端末から受信したリクエストメッセージの電波強度が所定の閾値を上回っており、かつ前記無線端末の端末識別子が予め登録されたものである場合に当該端末識別子を上位装置へ通知する端末通知手段と、自装置を介して通信する無線端末を制限するためのフィルタを前記上位装置から指示に応じて更新する更新手段とを設ける態様であれば良い。

[0049] （４）上記実施形態では、無線アクセスポイント装置１０と端末管理装置５０とを各々別個の装置として無線ネットワークシステム１を構成したが、両者を一体の装置として通信システムを構成しても良い。すなわち、端末管理装置５０を端末管理のために別途ハードウェアとして用意する必要はなく、任意の装置に、例えばソフトウェアとして設定可能である。

[0050] （５）上記実施形態では、本発明の端末管理装置特有の機能を端末管理装置５０に実現させるプログラムが端末管理装置５０の不揮発性記憶部５３４に予め記憶されていた。しかし、ＣＤ－ＲＯＭなどのコンピュータ読み取り可能な記録媒体に当該プログラムを書き込んで配布しても良く、また、インターネットなどの電気通信回線経由のダウンロードにより当該プログラムを配布しても良い。このようにして配布されるプログラムにしたがって一般的なコンピュータを作動させることで当該コンピュータを上記実施形態の端末管理装置として機能させることが可能になるからである。無線アクセスポイント装置１０の不揮発性記憶部１３４に記憶されている無線通信プログラムについても同様である。

[0051] （６）上記実施形態では、無線端末６０が無線ネットワークシステム１に接続（無線アクセスポイント装置１０と通信）できるようにするために、インターネット２およびモバイル網３経由で端末管理装置５０が無線端末６０のセキュリティポリシの判定を行った上で、セキュリティポリシを満たす場合

に無線アクセスポイント装置１０に接続する際に必要となる接続情報をインターネット２およびモバイル網３経由で端末管理装置５０から無線端末６０に与えた。しかしながら、セキュリティポリシの判定を行うための通信や無線アクセスポイント装置１０に接続する際に必要となる接続情報の送信は、インターネット２およびモバイル網３経由に限られず、他の通信手段を経由してもよい。例えば、赤外線やBluetooth（登録商標）、NFC（Near Field Communication）を使用してもよい。

[0052] 本出願は、２０１３年３月２２日に出願された日本特許出願（特願２０１３－０５９４６４）に基づくものであり、その内容はここに参照として取り込まれる。

産業上の利用可能性

[0053] 本発明によれば、コストの大幅な増加を招くことなく、セキュリティポリシを満たす無線端末のみが社内ネットワークに接続されるようにすることが可能である。

符号の説明

[0054] １…無線ネットワークシステム、２…インターネット、３…モバイル網、１０－ｎ（ｎ＝１～Ｎ），１０…無線アクセスポイント装置、２０…スイッチングハブ、３０…ＡＰコントローラ、４０…ルータ、５０…端末管理装置、６０…無線端末、１１０，５１０…制御部、１２０…無線通信Ｉ／Ｆ部、５２０…通信Ｉ／Ｆ部、１３０，５３０…記憶部、１３２，５３２…揮発性記憶部、１３４，５３４…不揮発性記憶部、５４０…バス。

請求の範囲

[請求項1] 無線中継装置と端末管理装置とを含む無線ネットワークシステムにおいて、

前記端末管理装置は、

当該無線ネットワークシステムとは異なる通信網を介して無線端末と通信し、当該無線端末が予め定められたセキュリティポリシを満たしているか否かを判定する判定手段と、

前記セキュリティポリシを満たしていると前記判定手段により判定された無線端末へ、前記無線中継装置に接続するための接続情報を送信する接続情報送信手段と、を有する

ことを特徴とする無線ネットワークシステム。

[請求項2] 前記接続情報送信手段は、当該無線ネットワークシステムとは異なる前記通信網経由で前記接続情報を送信する

ことを特徴とする請求項１に記載の無線ネットワークシステム。

[請求項3] 前記無線ネットワークシステムのサービスエリア内に無線端末が入ったことを検知する検知装置をさらに有し、

前記端末管理装置は、

前記無線ネットワークシステムのサービスエリア内に入ったことが前記検知装置により検知された無線端末を対象として前記判定手段によるセキュリティポリシの判定を行う

ことを特徴とする請求項１に記載の無線ネットワークシステム。

[請求項4] 前記無線中継装置が前記検知装置として機能する

ことを特徴とする請求項３に記載の無線ネットワークシステム。

[請求項5] 無線中継装置を含む無線ネットワークシステムとは異なる通信網を介して無線端末と通信し、当該無線端末が予め定められたセキュリティポリシを満たしているか否かを判定する判定手段と、

前記セキュリティポリシを満たしていると前記判定手段により判定された無線端末へ、前記無線中継装置に接続するための接続情報を送

信する接続情報送信手段と

を有することを特徴とする端末管理装置。

[請求項6] 無線ネットワークシステムに含まれる無線中継装置において、

無線端末から受信したリクエストメッセージの電波強度が所定の閾値を上回っており、かつ前記無線端末の端末識別子が予め登録されたものである場合に、前記端末識別子を上位装置へ通知する端末通知手段と、

自装置を介して通信する無線端末を制限するためのフィルタを前記上位装置から指示に応じて更新する更新手段と、

を有することを特徴とする無線中継装置。

[請求項7] 前記リクエストメッセージはプローブリクエストであり、前記端末識別子はＭＡＣアドレスであり、前記フィルタはＭＡＣアドレスフィルタである

ことを特徴とする請求項６に記載の無線中継装置。

[請求項8] 前記無線ネットワークシステムとは異なる通信網を介して当該無線中継装置に接続するための接続情報を得た無線端末と接続し、当該無線端末と前記無線ネットワークシステムによる通信を行う通信手段

をさらに有することを特徴とする請求項６に記載の無線中継装置。

[請求項9] 無線中継装置を含む無線ネットワークシステムとは異なる通信網を介して無線端末と通信し、当該無線端末が予め定められたセキュリティポリシを満たしているか否かを判定し、

前記セキュリティポリシを満たしていると判定された無線端末へ、前記無線中継装置に接続するための接続情報を送信する

ことを特徴とする通信方法。

[請求項10] 無線ネットワークシステムに含まれる無線中継装置における通信方法において、

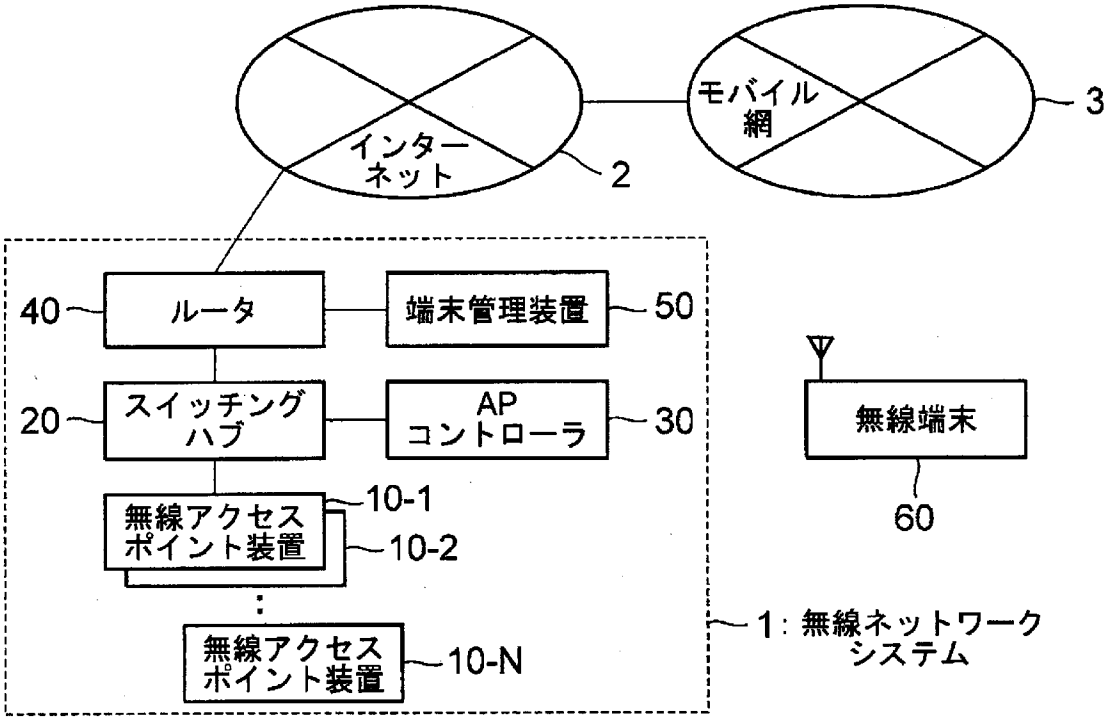
無線端末から受信したリクエストメッセージの電波強度が所定の閾値を上回っており、かつ前記無線端末の端末識別子が予め登録された

ものである場合に、前記端末識別子を上位装置へ通知し、

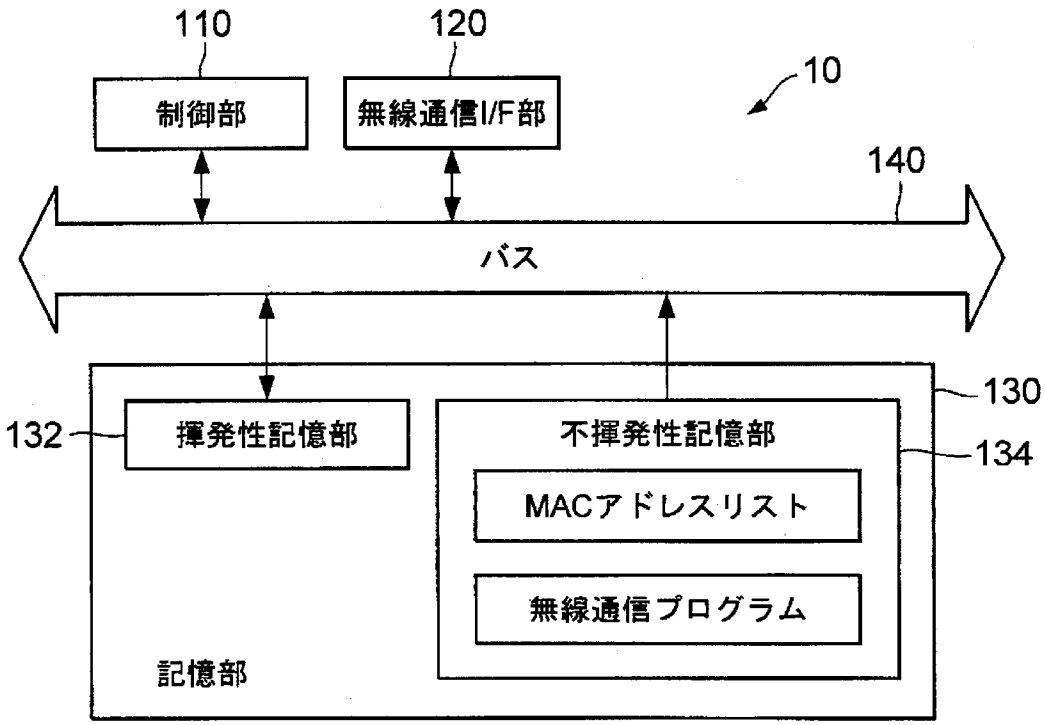
前記無線中継装置を介して通信する無線端末を制限するためのフィルタを前記上位装置から指示に応じて更新する

ことを特徴とする通信方法。

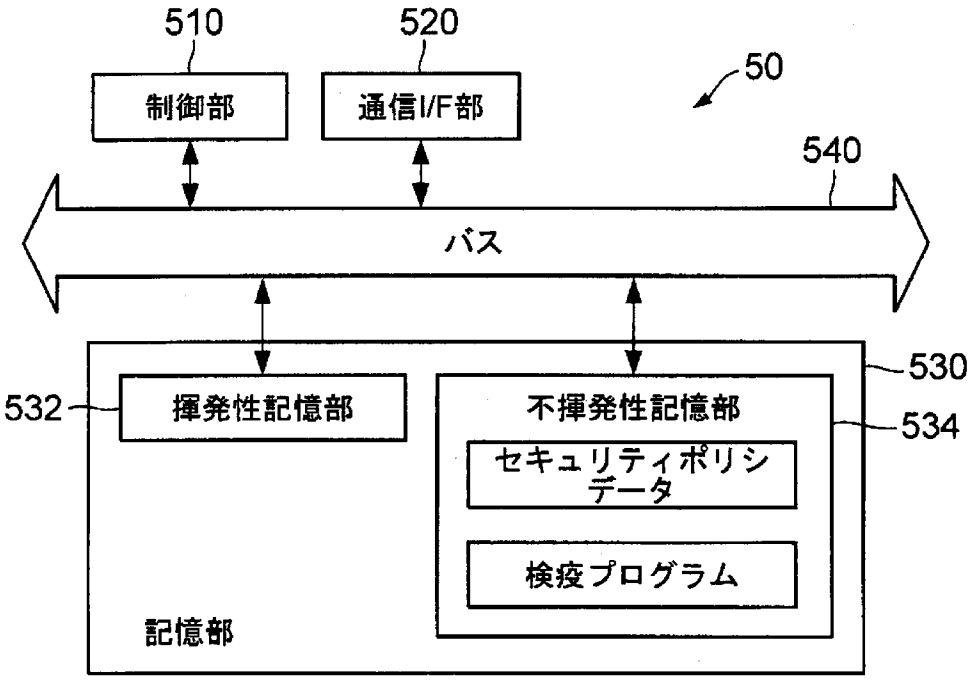
[図1]


インターネット
2
モバイル網
3
40
ルータ
端末管理装置
50
20
スイッチングハブ
AP コントローラ
30
無線端末
60
無線アクセスポイント装置
10-1
10-2
無線アクセスポイント装置
10-N
1：無線ネットワークシステム

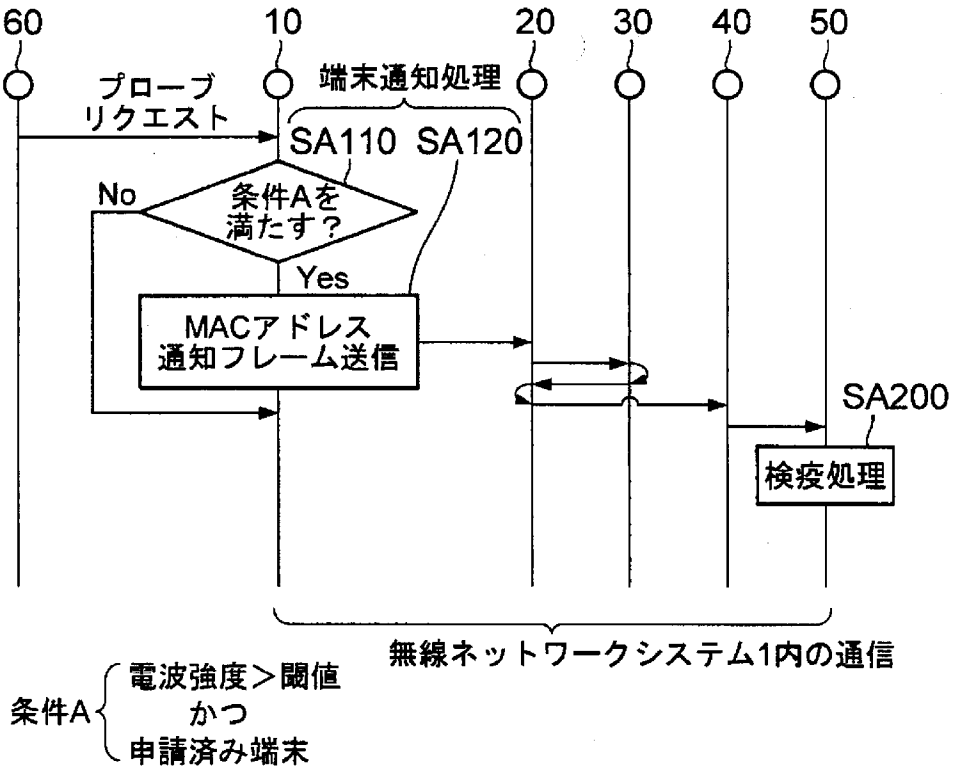
[図2]


110
制御部
120
無線通信I/F部
10
140
バス
130
132
揮発性記憶部
不揮発性記憶部
134
MACアドレスリスト
無線通信プログラム
記憶部

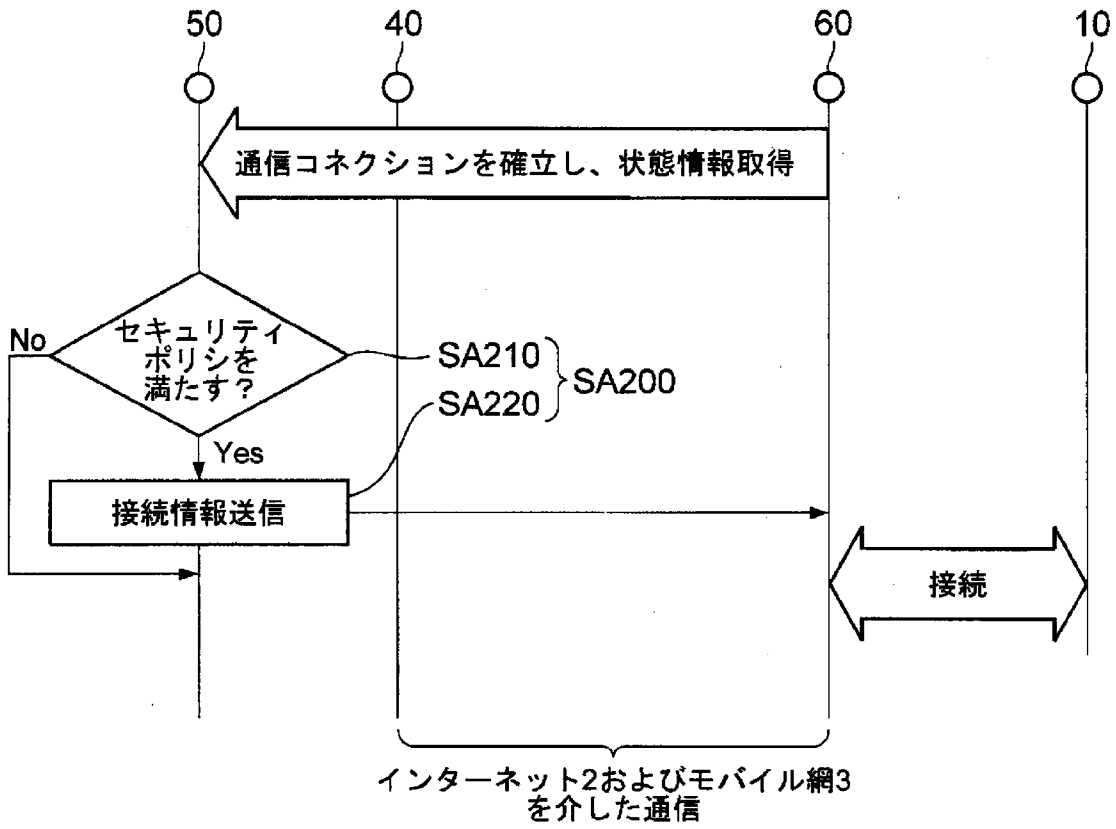
[図3]


510
520
50
制御部
通信I/F部
540
バス
530
532
揮発性記憶部
不揮発性記憶部
534
セキュリティポリシデータ
検疫プログラム
記憶部

[図4]


60
10
20
30
40
50
プローブリクエスト
端末通知処理
SA110
SA120
No
条件Aを満たす？
Yes
MACアドレス通知フレーム送信
SA200
検疫処理
無線ネットワークシステム1内の通信
条件A
電波強度＞閾値
かつ
申請済み端末

[図5]


50
40
60
10
通信コネクションを確立し、状態情報取得
No
セキュリティポリシを満たす？
SA210
SA220
SA200
Yes
接続情報送信
接続
インターネット2およびモバイル網3を介した通信

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2014/057206

A. CLASSIFICATION OF SUBJECT MATTER
H04W4/00(2009.01)i, *H04W12/08*(2009.01)i, *H04W88/06*(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)
H04W4/00-99/00, H04B7/24-7/26

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	1996-2014
Kokai Jitsuyo Shinan Koho	1971-2014	Toroku Jitsuyo Shinan Koho	1994-2014

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.
Y	JP 2005-86471 A (Japan Telecom Co., Ltd.), 31 March 2005 (31.03.2005), paragraphs [0016] to [0033]; fig. 1 to 5 (Family: none)	1-5,9
Y	JP 2008-263445 A (DoCoMo Technology, Inc.), 30 October 2008 (30.10.2008), paragraphs [0002], [0020], [0033] to [0034]; fig. 2 (Family: none)	1-5,9
Y	Akira KUBOTA et al., "Development of iNetSec Inspection Center V7.0 -Achieving Smart Device Inspections-", PFU Tech. Rev., 2012.11, vol.23, no.2, no.44, pages 1 to 7	1-5,9

☒ 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
21 May, 2014 (21.05.14)	03 June, 2014 (03.06.14)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2014/057206

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2013-507077 A (Mosaid Technorogies Inc.), 28 February 2013 (28.02.2013), paragraphs [0105] to [0112], [0121] to [0131]; fig. 6, 13 & US 2011/0081890 A1 & WO 2011/041888 A1 & CN 102257855 A & KR 10-2012-0085648 A	3,4
A	JP 2004-336538 A (Ricoh Co., Ltd.), 25 November 2004 (25.11.2004), paragraphs [0210] to [0285]; fig. 13 to 18 (Family: none)	1-5,9
A	JP 2005-167884 A (NEC Corp.), 23 June 2005 (23.06.2005), paragraphs [0095] to [0104]; fig. 13 (Family: none)	1-5,9
A	JP 2004-310581 A (NEC Corp.), 04 November 2004 (04.11.2004), entire text; all drawings (Family: none)	1-5,9
A	JP 2007-6320 A (Nakayo Telecommunications Inc.), 11 January 2007 (11.01.2007), paragraphs [0066] to [0076]; fig. 8, 9 (Family: none)	6-8,10
A	JP 2012-134703 A (KDDI Corp.), 12 July 2012 (12.07.2012), entire text; all drawings (Family: none)	6-8,10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2014/057206

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:
See extra sheet.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☒ No protest accompanied the payment of additional search fees.

Continuation of Box No.III of continuation of first sheet(2)

Claims 1, 6-8 and 10 have a common technical feature of having both a radio network system, which includes a radio relay apparatus, and radio terminals.

However, the above-said technical feature cannot be considered to be a special technical feature, since the technical feature does not make a contribution over the prior art in the light of the contents disclosed in each of the documents 1 and 2.

Further, there is no other same or corresponding special technical feature between these inventions.

Accordingly, claims are classified into two inventions each of which has a special technical feature indicated below.

(Invention 1) claims 1-5 and 9

An invention characterized in that a terminal management apparatus: communicates with the radio terminals via a communication network that is different from the radio network system including the radio relay apparatus; determines whether the radio terminals satisfy a predetermined security policy; and transmits connection information, which is used to connect to the radio relay apparatus, to radio terminals for which it has been determined that the security policy is satisfied.

(Invention 2) claims 6-8 and 10

An invention characterized in that when the radio wave intensity of a request message the radio relay apparatus has received from a radio terminal exceeds a predetermined threshold value and further the terminal identifier of the radio terminal has already been registered, the terminal identifier is informed to a host apparatus, and a filter for restricting radio terminals communicating via the radio relay apparatus is updated in response to an instruction from the host apparatus.

Claims 6-8 and 10 are not relevant to inventions which involve all of the matters to define the invention in claim 1 and which have a same category.

Further, as a result of the search which has been carried out with respect to claims classified into Invention 1, claims 6-8 and 10 are not relevant to inventions on which it is substantially possible to carry out a search without an additional prior-art search and judgment, and there is no other reason for that it can be considered that it is efficient to carry out a search on claims 6-8 and 10 together with claims 1-5 and 9, and consequently, it is impossible to classify claims 6-8 and 10 into Invention 1.

Document 1: JP 2005-86471 A (Japan Telecom Co., Ltd.), 31 March 2005 (31.03.2005), paragraphs [0016] to [0033]; fig. 1 to 5

Document 2: JP 2008-263445 A (DoCoMo Technology, Inc.), 30 October 2008 (30.10.2008), paragraphs [0002], [0020], [0033] to [0034]; fig. 2

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１４／０５７２０６

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　H04W4/00(2009.01)i, H04W12/08(2009.01)i, H04W88/06(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.　H04W4/00-99/00, H04B7/24-7/26

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	１９７１－２０１４年
日本国実用新案登録公報	１９９６－２０１４年
日本国登録実用新案公報	１９９４－２０１４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
Y	JP 2005-86471 A（日本テレコム株式会社）2005.03.31, 段落【００１６】－【００３３】,【図１】－【図５】 （ファミリーなし）	1-5,9
Y	JP 2008-263445 A（ドコモ・テクノロジ株式会社）2008.10.30, 段落【０００２】,【００２０】,【００３３】－【００３４】, 【図２】（ファミリーなし）	1-5,9

☑　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
２１．０５．２０１４	０３．０６．２０１４

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　３１３９
東　昌秋
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
Y	久保田　旭，外２名， 『ｉＮｅｔＳｅｃ　Ｉｎｓｐｅｃｔｉｏｎ　Ｃｅｎｔｅｒ　Ｖ７．０開発　～スマートデバイス検疫の実現～』， ＰＦＵ・テクニカルレビュー，2012.11，ｖｏｌ．２３，ｎｏ．２，第４４号，第１ページ－第７ページ	1-5,9
Y	JP 2013-507077 A （モサイド・テクノロジーズ・インコーポレーテッド）2013.02.28, 段落【０１０５】－【０１１２】,【０１２１】－【０１３１】, 【図６】,【図１３】 & US 2011/0081890 A1 & WO 2011/041888 A1 & CN 102257855 A & KR 10-2012-0085648 A	3,4
A	JP 2004-336538 A（株式会社リコー）2004.11.25, 段落【０２１０】－【０２８５】,【図１３】－【図１８】 （ファミリーなし）	1-5,9
A	JP 2005-167884 A（日本電気株式会社）2005.06.23, 段落【００９５】－【０１０４】,【図１３】（ファミリーなし）	1-5,9
A	JP 2004-310581 A（日本電気株式会社）2004.11.04，全文，全図 （ファミリーなし）	1-5,9
A	JP 2007-6320 A（株式会社ナカヨ通信機）2007.01.11, 段落【００６６】－【００７６】,【図８】,【図９】 （ファミリーなし）	6-8,10
A	JP 2012-134703 A（ＫＤＤＩ株式会社）2012.07.12，全文，全図 （ファミリーなし）	6-8,10

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１４／０５７２０６

第Ⅱ欄　請求の範囲の一部の調査ができないときの意見（第１ページの２の続き）

法第8条第3項（ＰＣＴ17条(2)(a)）の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

１．☐ 請求項 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、

２．☐ 請求項 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、

３．☐ 請求項 _____ は、従属請求の範囲であってＰＣＴ規則6.4(a)の第２文及び第3文の規定に従って記載されていない。

第Ⅲ欄　発明の単一性が欠如しているときの意見（第１ページの３の続き）

次に述べるようにこの国際出願に二以上の発明があるとこの国際調査機関は認めた。

特別ページを参照

１．☑ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求項について作成した。

２．☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求項について調査することができたので、追加調査手数料の納付を求めなかった。

３．☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったので、この国際調査報告は、手数料の納付のあった次の請求項のみについて作成した。

４．☐ 出願人が必要な追加調査手数料を期間内に納付しなかったので、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求項について作成した。

追加調査手数料の異議の申立てに関する注意

☐ 追加調査手数料及び、該当する場合には、異議申立手数料の納付と共に、出願人から異議申立てがあった。

☐ 追加調査手数料の納付と共に出願人から異議申立てがあったが、異議申立手数料が納付命令書に示した期間内に支払われなかった。

☑ 追加調査手数料の納付はあったが、異議申立てはなかった。

請求項１、請求項６－８，１０は、無線中継装置を含む無線ネットワークシステムと無線端末とを有するという共通の技術的特徴を有している。しかしながら、当該技術的特徴は、文献１及び文献２のそれぞれの開示内容に照らして、先行技術に対する貢献をもたらすものではないから、当該技術的特徴は、特別な技術的特徴であるとはいえない。また、これらの発明の間には、他に同一の又は対応する特別な技術的特徴は存在しない。そして、請求の範囲は、各々下記の特別な技術的特徴を有する２の発明に区分される。

（発明１）請求項１－５，９
端末管理装置が、無線中継装置を含む無線ネットワークシステムとは異なる通信網を介して無線端末と通信し、無線端末が予め定められたセキュリティポリシを満たしているか否かを判定し、セキュリティポリシを満たしていると判定された無線端末へ、無線中継装置に接続するための接続情報を送信することを特徴とする発明。

（発明２）請求項６－８，１０
無線中継装置が、無線端末から受信したリクエストメッセージの電波強度が所定の閾値を上回っており、かつ無線端末の端末識別子が予め登録されたものである場合に、端末識別子を上位装置へ通知し、無線中継装置を介して通信する無線端末を制限するためのフィルタを上位装置から指示に応じて更新することを特徴とする発明。

請求項６－８，１０は、請求項１の発明特定事項を全て含む同一カテゴリーの発明ではない。そして、請求項６－８，１０は、発明１に区分された請求項について調査した結果、実質的に追加的な先行技術調査や判断を必要とすることなく調査を行うことが可能である発明ではなく、請求項１－５，９とまとめて調査を行うことが効率的であるといえる他の事情もないから、請求項６－８，１０を発明１に区分することはできない。

文献１：JP 2005-86471 A（日本テレコム株式会社）2005.03.31,
段落【００１６】－【００３３】,【図１】－【図５】
文献２：JP 2008-263445 A（ドコモ・テクノロジ株式会社）2008.10.30,
段落【０００２】,【００２０】,【００３３】－【００３４】,【図２】