

(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 10 月 4 日(04.10.2012)



(10) 国際公開番号

WO 2012/132174 A1

- (51) 国際特許分類:
H04W 12/08 (2009.01) H04W 52/28 (2009.01)
H04M 1/00 (2006.01) H04W 64/00 (2009.01)
H04M 11/00 (2006.01)
- (21) 国際出願番号: PCT/JP2012/000451
- (22) 国際出願日: 2012 年 1 月 25 日(25.01.2012)
- (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 2011-068856 2011 年 3 月 25 日(25.03.2011) JP
- (71) 出願人 (米国を除く全ての指定国について): パナソニック株式会社(PANASONIC CORPORATION)
[JP/JP]; 〒5718501 大阪府門真市大字門真 1 0 0 6 Osaka (JP).
- (72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 稲見 聡(IN-AMI, Satoshi).
- (74) 代理人: 特許業務法人 小笠原特許事務所
(OGASAWARA PATENT OFFICE); 〒5640063 大阪

府吹田市江坂町 1 丁目 2 3 番 1 0 1 号 大同生命江坂ビル 1 3 階 Osaka (JP).

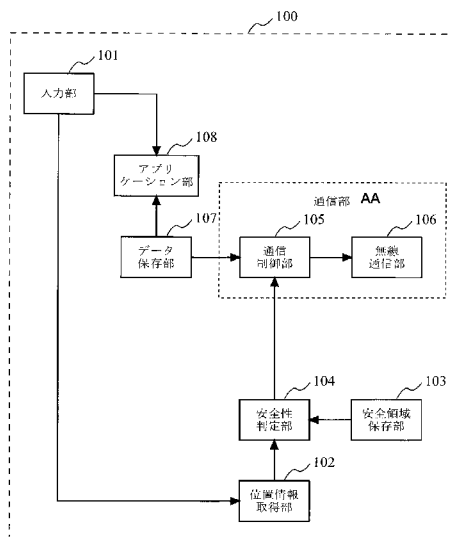
- (81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, 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, 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).

[続葉有]

(54) Title: INFORMATION COMMUNICATION TERMINAL WITH SECURITY CONTROL FUNCTION, COMMUNICATION SYSTEM, AND METHOD OF COMMUNICATION PERFORMED BY SAID TERMINAL

(54) 発明の名称: セキュリティ制御機能を備えた情報通信端末、通信システム、及び当該端末が行う通信方法

【図3】



- 101 Input unit
102 Position information acquiring unit
103 Safety region storing unit
104 Safety determination unit
105 Communication control unit
106 Wireless communication unit
107 Data storing unit
108 Application unit
AA Communication unit

(57) Abstract: According to the present invention, a position information acquiring unit (102) acquires position information indicating the position where an information communication terminal (100) is currently located. A safety region storing unit (103) preliminarily stores a safety region having little security risk of information leak and so forth, thus being determined safe. A safety determination unit (104) determines the security risk of wireless communication at the present position by the information communication terminal (100) on the basis of the position information and the safety region. A communication control unit (105) controls a wireless communication unit (106) so that the wireless communication unit (106) transmits a wireless signal with a large radio field strength if the safety determination unit (104) determines that the risk is low and transmits a wireless signal with a small radio field strength if the safety determination unit (104) determines that the risk is high.

(57) 要約: 位置情報取得部 102 は、情報通信端末 100 が現在居る位置を示す位置情報を取得する。安全領域保存部 103 は、情報漏洩等のセキュリティリスクが低く安全であると考えられる安全領域を予め保存している。安全性判定部 104 は、位置情報と安全領域とに基づいて、現在位置における情報通信端末 100 による無線通信のセキュリティリスクを判定する。通信制御部 105 は、安全性判定部 104 でリスクが低いと判定されれば、大きい電波強度で無線信号を送信するように、また安全性判定部 104 でリスクが高いと判定されれば、小さい電波強度で無線信号を送信するように、無線通信部 106 を制御する。



添付公開書類:

— 国際調査報告 (条約第 21 条(3))

明 細 書

発明の名称：

セキュリティ制御機能を備えた情報通信端末、通信システム、及び当該端末が行う通信方法

技術分野

[0001] 本発明は、セキュリティ制御機能を備えた情報通信端末に関し、より特定のには、情報通信端末間で行われる通信のセキュリティを向上させるために位置情報を用いて電波強度を制御する情報通信端末、この情報通信端末を複数含む通信システム、及び情報通信端末が実行する通信方法に関する。

背景技術

[0002] 近年では、より多くの人々がデスクトップパーソナルコンピュータ（以下、PCと記す）、ノートPC、タブレットPC、PDA（personal digital assistant）、携帯電話、及びスマートフォン等、アプリケーションを実行可能な情報通信端末を複数所有しており、状況に応じて複数の情報通信端末の使い分けがなされている。また、これらの情報通信端末に搭載されるハードウェアの進歩は著しい。例えば、情報通信端末は、ギガヘルツ級のクロック周波数を持つCPU（central processing unit）を搭載し、公衆回線、無線LAN（Local Area Network）、Bluetooth（登録商標）等、複数の通信手段を持つ。そこで、PCだけではなく、スマートフォンでも、PC用に作られたサイトをいろいろな場所でブラウジングすることが増えている。従って、複数の情報通信端末間で利用を切り替える際に、切り替え元の情報通信端末で使用しているアプリケーション、例えばブラウザを切り替え先の情報通信端末で継続使用可能とする、シームレスな端末移行が必要になっている。

[0003] 一方で、スマートフォン等で扱うデータは個人情報であることも多い。例えば、ブラウザでショッピングサイトを利用し、住所やクレジットカード番号等の個人情報を入力する人も多い。また、ブラウザによるアクセス履歴や

ブックマーク情報は、プライバシーにかかわるデータで、他人には見せたくないこともある。つまり、これらの情報を情報通信端末間で引き継ぐ時には、情報が漏洩して悪用されないように細心の注意を払う必要がある。

[0004] また、スマートフォンは、持ち運びが容易で、いろいろな場所で利用される。従って、GPS (Global Positioning System) を搭載すれば、利用された位置を正確に特定することができる。この位置情報を用いると、利便性と共に、プライバシーにかかわるデータの通信時のセキュリティを向上させることもできる。

[0005] この情報通信端末における位置情報を利用して通信時のセキュリティを向上させる従来の技術としては、例えば特許文献1に開示された技術がある。この特許文献1に記載された技術では、電子商取引を行う予定をしている場所や時刻の情報をサーバに予め登録しておく。そして、サーバにアクセスして電子商取引を行う場合には、情報通信端末が現在の場所及び時刻を取得してサーバに認証情報として送信する。サーバでは、予め登録してある情報と送信されてきた情報とが一致している場合にのみ、電子商取引を許可する。これにより、特許文献1に記載された技術では、通信時のセキュリティを高めている。

先行技術文献

特許文献

[0006] 特許文献1：特開2006-244381号公報

発明の概要

発明が解決しようとする課題

[0007] 上記従来の技術では、サーバと通信を行う時の情報通信端末の位置情報をサーバに登録しておくことで、情報通信端末の認証処理の精度が向上し、情報通信端末とサーバとの間での通信のセキュリティを高めることができる。しかし、情報通信端末は持ち運び可能な携帯機器であるが、サーバは持ち運べる機器ではなく、ある場所に固定されているのが常識である。つまり、上

記従来の技術は、どちらも持ち運びができる情報通信端末間の通信時に特有のセキュリティ問題を解決することを考慮した技術ではない。

[0008] 例えば、比較的広い家では、情報を含んだ電波は家の外には漏れない。しかし、狭い家では、情報を含んだ電波が外まで漏れて、他人による情報盗取の可能性が高まる。また、電車等の公共の場所では、多数の端末を持った人がごく近くにいて、盗取による情報漏洩のリスクがより高まる。つまり、場所によって、情報通信端末間で通信を行う場合の情報漏洩リスクが変化すると考えられるが、従来はこの情報漏洩リスクの変化に対応して通信方法を変化させ、セキュリティを向上させることはできなかった。

[0009] それ故に、本発明の目的は、情報通信端末間で通信を行う場合に、端末の位置情報に基づいてセキュリティリスクを判断し、この判断に応じて通信方法を変化させることで、セキュリティを確保しつつ、情報通信端末間の通信効率及び利便性を向上させることができるセキュリティ制御装置、通信システム、及び当該端末が行う通信方法を提供することである。

課題を解決するための手段

[0010] 本発明は、近距離通信で無線通信を行う情報通信端末に向けられている。そして、上記目的を達成するために、本発明の情報通信端末は、情報通信端末の位置情報を取得する位置情報取得部と、他の端末と通信する時に安全であると登録されている安全領域を保存する安全領域保存部と、情報通信端末の位置情報及び安全領域に基づいて、情報通信端末が他の端末と通信を行う場合のセキュリティリスクを判定する安全性判定部と、安全性判定部において、通信時のセキュリティリスクが高いと判定された場合、予め定めた小さい電波強度で他の端末とのデータ通信を行い、通信時のセキュリティリスクが低いと判定された場合、予め定めた大きい電波強度で他の端末とのデータ通信を行う通信部とを備えている。

[0011] 典型的には、安全領域は、ユーザが指示を入力する入力部を通じてユーザによって入力される。又は、位置情報取得部によって、これまでに取得した複数の位置情報の履歴に基づいて安全領域が決定されてもよい。

[0012] 好ましくは、安全性判定部は、位置情報取得部において情報通信端末の位置情報を取得できなかった場合は、通信時のセキュリティリスクが高いと判定する。また、安全性判定部は、位置情報から得られる情報通信端末の現在位置が安全領域内にあるか否かで、通信時のセキュリティリスクを判定する。このとき、安全性判定部は、位置情報から得られる情報取得時刻をさらに判断して、通信時のセキュリティリスクを判定してもよい。

[0013] なお、通信部が他の端末の位置情報を取得できる場合には、安全性判定部は、他の端末の位置情報をさらに考慮して、情報通信端末が他の端末と通信を行う場合のセキュリティリスクを判定することが望ましい。また、この場合には、通信部は、情報通信端末と他の端末との距離が、安全性判定部の判定に基づいて決定した電波強度で通信可能な距離になったタイミングで、データ通信を開始することができる。

発明の効果

[0014] 上記本発明によれば、端末の位置情報から判断したリスクが高い場合は、通信能力を下げてもセキュリティを高め、端末の位置情報から判断したリスクが低い場合には、セキュリティを確保しつつ通信能力も上げることができる。従って、通信能力とセキュリティを最適に制御することができる。

図面の簡単な説明

[0015] [図1]図1は、本発明が提供する情報通信端末を含めた通信システムの構成例を示す図である。

[図2]図2は、タブレットPC10の表示画面11及び携帯電話20の表示画面21の一例を示す図である。

[図3]図3は、本発明の第1の実施形態に係る情報通信端末100の構成の一例を示す図である。

[図4]図4は、位置情報取得部102で取得された位置情報の一例を示す図である。

[図5]図5は、安全領域保存部103に保存されている安全領域の一例を示す図である。

[図6]図6は、本発明の第1の実施形態に係る情報通信端末100が行う電波強度制御の処理手順を示すフローチャートである。

[図7]図7は、本発明の第2の実施形態に係る情報通信端末200の構成の一例を示す図である。

[図8]図8は、移行先端末位置情報保存部209に保存されている移行先端末の位置情報の一例を示す図である。

[図9]図9は、本発明の第2の実施形態に係る情報通信端末200が行う電波強度制御の処理手順を示すフローチャートである。

[図10]図10は、本発明の具体的な適用例を説明する図である。

発明を実施するための形態

[0016] 以下、本発明の実施形態について、図面を参照しながら説明する。

本発明では、ユーザが、使用する情報通信端末をある端末（以下、移行元端末と記す）から他の端末（以下、移行先端末と記す）に切り替える場合において、移行元端末で利用していたアプリケーションを移行先端末でも継続して利用する場面を想定している。このような場面では、移行元端末におけるアプリケーションの作業内容等の情報が、移行先端末に送信される。これにより、切り替え前に移行元端末においてユーザが利用していたアプリケーションの作業内容等が、移行先端末の画面で再現表示される。

[0017] 図1は、本発明が提供する情報通信端末を含めた通信システムの構成例を示す図である。この図1の例では、1人のユーザが、タブレットPC10、携帯電話20、及びノートPC30の、ネットワーク40に接続可能な複数の情報通信端末を所有している。そして、ユーザは、状況に応じてこれらの情報通信端末を使い分けている。例えば、自宅ではノートPC30を使用し、外出時にはタブレットPC10や携帯電話20を利用する。このような通信システムでは、例えば、自宅のノートPC30でWebサイトのインターネットニュースを視聴していたが、外出時間となったためニュースの続きを携帯電話20で視聴するという利用が想定される。また、例えば、外出先の電車の中で立ちながら携帯電話20を用いてWebサイトのインターネット

ニュースを視聴していたが、席が空いて座れたので大画面のタブレットPC 10に切り替えてニュースの続きを視聴するという利用が想定される。

[0018] インターネットニュースを視聴する場合における、タブレットPC 10及び携帯電話20における表示画面の例を、図2に示す。図2は、タブレットPC 10の表示画面11及び携帯電話20の表示画面21の一例を示す図である。

本実施形態のタブレットPC 10及び携帯電話20は、ネットワークに接続するための通信機能をそれぞれ備えており、表示画面11及び21にはこの通信機能で得たWebサイトの一部分が表示されている。なお、携帯電話20からタブレットPC 10への切り替えは、移行元端末である携帯電話20に備えられる物理的なボタンやソフトウェアキーを介した指示に従って行われてもよいし、所定の状態変化を検出して自動的に行われてもよい。

[0019] 上述した利用方法は、もちろん切り替え方向が逆の場合もあり得る。つまり、タブレットPC 10、携帯電話20、及びノートPC 30等の情報通信端末は、移行元端末及び移行先端末のいずれにもなり得るということである。

本発明の各実施形態では、少なくとも移行元端末となり得る情報通信端末の構成、及びその情報通信端末が行う処理を詳細に説明する。

[0020] <第1の実施形態>

図3は、本発明の第1の実施形態に係る情報通信端末100の構成の一例を示す図である。図3に示す第1の実施形態に係る情報通信端末100は、入力部101と、位置情報取得部102と、安全領域保存部103と、安全性判定部104と、通信制御部105と、無線通信部106と、データ保存部107と、アプリケーション部108とを備えている。

[0021] 入力部101は、キーパッドやタッチパネル等の、ユーザが情報通信端末100への指示（通信開始の要求や情報の登録等）を入力するためのインターフェースである。入力部101に入力されたユーザ指示は、位置情報取得部102及びアプリケーション部108に出力される。

[0022] 位置情報取得部 102 は、情報通信端末 100 が現在居る位置を示す位置情報を取得する。この位置情報取得部 102 は、典型的には GPS 情報を受信して位置情報を取得する。又は、位置情報取得部 102 は、Wi-Fi (Wireless Fidelity) のアクセスポイントから受信する MAC (Media Access Control) アドレスや電波強度に基づいて現在位置を推定し、この推定した現在位置を位置情報として取得してもよい。又は、位置情報取得部 102 は、携帯電話の基地局から受信する電波から現在位置を推定し、この推定した現在位置を位置情報として取得してもよい。あるいは、位置情報取得部 102 は、ネットワーク上で指定された IP (Internet Protocol) アドレス等から現在位置を推定し、この推定した現在位置を位置情報として取得してもよい。

[0023] 図 4 は、位置情報取得部 102 で取得された位置情報の一例を示す図である。図 4 の例では、GPS 情報を受信した取得時刻 (2011 年 2 月 10 日 14 時)、及び情報通信端末 100 の現在位置の緯度 (北緯 34 度 44 分 36.02 秒) 及び経度 (東経 135 度 26 分 44.35 秒) を位置情報としている。

[0024] 安全領域保存部 103 は、使用する情報通信端末 100 を切り替える場合に、必要な情報を移行元端末から移行先端末へ無線通信を介して送信しても、情報漏洩等のセキュリティリスクが低く安全であると登録されている安全領域を、予め保存しておくメモリである。この安全領域保存部 103 としては、不揮発性のフラッシュメモリが望ましいが、情報通信端末 100 を起動させるたびに毎回安全領域を設定するのであれば揮発性のメモリでもよい。安全領域は、ユーザが手動で設定してもよいし、情報通信端末 100 が自動的に設定してもよい。後者の場合、情報通信端末 100 が、移動履歴から比較的良好に居る場所を抽出し、この抽出した場所又はその近傍を安全領域として設定すること等が考えられる。あるいは、安全領域保存部 103 は、「GPS 情報が検出できる位置」等のように安全領域を満たすべきルールを設定しておいてもよい。

[0025] 図 5 は、安全領域保存部 103 に保存されている安全領域の一例を示す図

である。図5（a）の例では、北緯34度39分55.16秒及び東経135度30分18.98秒を中心として半径30メートルの範囲を、安全領域としている。図5（b）の例では、北緯N1及び東経E1の位置と、北緯N2及び東経E2の位置を対角頂点とする矩形の範囲を、安全領域としている。なお、図5で例示した安全領域は、円や矩形等の単純な形状であるが、これらの形状以外の複雑な領域を安全領域としても構わない。

[0026] 安全性判定部104は、位置情報取得部102で取得された位置情報と、安全領域保存部103に保存されている安全領域とを入力し、情報通信端末100による無線通信のセキュリティリスクを判定する。具体的には、安全性判定部104は、情報通信端末100（移行元端末）が安全領域内に居る場合は、現在位置において情報通信端末100が近くに存在する他の情報通信端末（移行先端末）と無線通信を行ってもセキュリティリスクが低く安全であるとの判定を行う。一方、安全性判定部104は、情報通信端末100が安全領域内に居ない場合は、現在位置において情報通信端末100が近くに存在する他の情報通信端末と無線通信を行った場合にセキュリティリスクが高く危険であるとの判定を行う。

[0027] 通信制御部105は、安全性判定部104で判定された結果に基づいて、無線通信部106が送信する無線信号の電波強度を制御する。具体的には、通信制御部105は、安全性判定部104における判定結果が「安全である」場合は、無線信号の電波強度を大きくするように無線通信部106に指示し、安全性判定部104における判定結果が「危険である」場合は、無線信号の電波強度を小さくするように無線通信部106に指示する。

[0028] 無線通信部106は、他の情報通信端末との間で無線通信を行うためのインタフェースである。この無線通信部106は、近距離に居る他の情報通信端末との間で無線信号を送受信できるインタフェースであればよく、例えばWi-FiやBluetooth等が利用可能である。この無線通信部106は、上述した通信制御部105と共に、情報通信端末100の通信部を構成する。

[0029] データ保存部 107 は、情報通信端末 100 が近距離に居る他の情報通信端末との間で無線通信を行う時に送信するデータを保存するためのメモリである。本発明では、データ保存部 107 に保存されるデータに、セキュリティを必要とする個人情報等が含まれているものと仮定している。このデータ保存部 107 には、フラッシュメモリや D R A M (Dynamic Random Access Memory) 等が用いられる。

[0030] アプリケーション部 108 は、データ保存部 107 に保存されているデータを利用するアプリケーションであり、例えば W e b ブラウザである。一般的には、このアプリケーション部 108 は、情報通信端末 100 が備える R O M (Read Only Memory) に保存されており、必要な時に R O M から読み出されて C P U 及び R A M (Random Access Memory) を用いて実行される。なお、図 3 に示す情報通信端末 100 の構成では、C P U、R A M、及び R O M を省略している。

[0031] 次に、上記構成による第 1 の実施形態に係る情報通信端末 100 が近距離に居る他の情報通信端末との間で無線通信を行う時の手順を、図 6 をさらに参照して説明する。

図 6 は、本発明の第 1 の実施形態に係る情報通信端末 100 が行う電波強度制御の処理手順を示すフローチャートである。なお、上述したとおり、安全領域保存部 103 には、予め安全領域が保存されているものとする。

[0032] 図 6 に示す処理は、入力部 101 が、ユーザから通信開始の指示を受けることで開始される。ユーザから通信開始が指示された入力部 101 は、位置情報取得部 102 に対して位置情報取得要求を通知する。この通知を受けた位置情報取得部 102 は、情報通信端末 100 が現在居る位置を示す位置情報を取得する (ステップ S 50)。取得された位置情報は、安全性判定部 104 に出力される。

[0033] 安全性判定部 104 は、位置情報取得部 102 から位置情報を、安全領域保存部 103 から安全領域をそれぞれ取得し、情報通信端末 100 が安全領域内に居るか否かに基づいてセキュリティリスクが低いか高いかを判断する

(ステップS 5 1)。そして、安全性判定部 1 0 4 は、情報通信端末 1 0 0 が安全領域内に居ると判断した場合(ステップS 5 1、Y e s)、今居る位置において情報通信端末 1 0 0 が他の情報通信端末と無線通信を行ってもセキュリティリスクが低く安全であるとの判定を通信制御部 1 0 5 に通知する。一方、安全性判定部 1 0 4 は、情報通信端末 1 0 0 が安全領域内に居ないと判断した場合(ステップS 5 1、N o)、今居る位置において情報通信端末 1 0 0 が他の情報通信端末と無線通信を行うとセキュリティリスクが高く危険であるとの判定を通信制御部 1 0 5 に通知する。

[0034] 安全性判定部 1 0 4 で行われる情報通信端末 1 0 0 の位置が安全領域内にあるか否かの判断は、例えば次のようにして行われる。

図 5 (a) のように、安全領域が円形領域として保存されていた場合、安全領域の中心と情報通信端末 1 0 0 の現在位置との距離 D が求められ、その距離 D と安全領域の半径 r とを比較する。そして、距離 $D \leq$ 半径 r を満足すれば、情報通信端末 1 0 0 が安全領域内に居ると判定される。なお、この距離 D は、地球は球体だけれども 2 点が近いごく狭い範囲では経線を平行線とみなすことができるので、簡単な三角関数を用いて近似計算することが可能となる。

また、図 5 (b) のように、安全領域が矩形領域として保存されていた場合、情報通信端末 1 0 0 の緯度 N を北緯 $N 1$ 及び $N 2$ の値と、経度 E を東経 $E 1$ 及び $E 2$ の値とそれぞれ比較する。そして、北緯 $N 1 \leq$ 緯度 $N \leq$ 北緯 $N 2$ かつ東経 $E 1 \leq$ 経度 $E \leq$ 東経 $E 2$ を満足すれば、情報通信端末 1 0 0 が安全領域内に居ると判定される。

[0035] 通信制御部 1 0 5 は、安全性判定部 1 0 4 からセキュリティリスクが低く安全であるとの通知を受けた場合、無線信号を送信する時の電波強度を予め定めた大きい値に設定するよう無線通信部 1 0 6 に指示を与える(ステップS 5 2)。一方、通信制御部 1 0 5 は、安全性判定部 1 0 4 からセキュリティリスクが高く危険であるとの通知を受けた場合、無線信号を送信する時の電波強度を予め定めた小さい値に設定するよう無線通信部 1 0 6 に指示を与

える（ステップＳ５３）。そして、通信制御部１０５は、データ保存部１０７から無線通信で送信するデータを取得し、無線通信部１０６を通じて、取得したデータをステップＳ５２又はＳ５３で設定した電波強度の無線信号で他の情報通信端末に送信する（ステップＳ５４）。

[0036] 以上のように、本発明の第１の実施形態に係る情報通信端末１００によれば、予め定めた安全領域内に自己端末（移行元端末）が存在する場合には、電波強度が大きい無線信号を用いて他の情報通信端末（移行先端末）と無線通信を行い、予め定めた安全領域内に自己端末が存在しない場合には、電波強度が小さい無線信号を用いて他の情報通信端末と無線通信を行う。これにより、情報通信端末の位置情報から判断したセキュリティリスクが高い場合は、通信能力を下げても安全性を優先して高くし、情報通信端末の位置情報から判断したセキュリティリスクが低い場合には、ある程度の安全性を確保しつつ通信能力も上げて離れた端末でも通信可能なように制御することができる。従って、セキュリティを確保しつつ、情報通信端末間の通信効率及び利便性を向上させることができる。

[0037] <第２の実施形態>

図７は、本発明の第２の実施形態に係る情報通信端末２００の構成の一例を示す図である。図７に示す第２の実施形態に係る情報通信端末２００は、入力部１０１と、位置情報取得部１０２と、安全領域保存部１０３と、安全性判定部２０４と、通信制御部２０５と、無線通信部２０６と、データ保存部１０７と、アプリケーション部１０８と、移行先端末位置情報保存部２０９とを備えている。図７に示すように、第２の実施形態に係る情報通信端末２００は、上記第１の実施形態に係る情報通信端末１００（図３）と比べて、安全性判定部２０４、通信制御部２０５、無線通信部２０６、及び移行先端末位置情報保存部２０９の構成が異なる。

[0038] 移行先端末位置情報保存部２０９は、データ保存部１０７に保存しているデータを送信する他の情報通信端末となる移行先端末２２０が現在居る位置を示す位置情報を保存するためのメモリである。図８は、移行先端末位置情

報保存部 209 に保存されている移行先端末の位置情報の一例を示す図である。図 8 の例では、受信した時刻（2011 年 2 月 14 日 14 時）、及び移行先端末の現在位置の緯度（北緯 34 度 44 分 36.00 秒）及び経度（東経 135 度 26 分 44.30 秒）が位置情報として保存されている。なお、保存される位置情報は、移行先端末 220 の位置を特定できる情報であればよく、絶対座標以外にも情報通信端末 200 との相対座標等で示されていてもよい。

[0039] そして、本第 2 の実施形態の安全性判定部 204、通信制御部 205、及び無線通信部 206 は、この移行先端末の位置情報を保存するための処理、及び移行先端末の位置情報を利用した安全性判定の処理をさらに実施する内容が、上記第 1 の実施形態の安全性判定部 104、通信制御部 105、及び無線通信部 106 と異なる。なお、通信制御部 205 及び無線通信部 206 は、情報通信端末 200 の通信部を構成する。

[0040] 以下、上記異なる内容を中心に第 2 の実施形態に係る情報通信端末 200 を説明し、上記第 1 の実施形態に係る情報通信端末 100 と同じ構成要素については同一の参照符号を付してその説明を省略する。

図 9 は、本発明の第 2 の実施形態に係る情報通信端末 200 が行う電波強度制御の処理手順を示すフローチャートである。なお、上述したとおり、安全領域保存部 103 には、予め安全領域が保存されているものとする。

[0041] 図 9 に示す処理は、入力部 101 が、ユーザから通信開始の指示を受けることで開始される。ユーザから通信開始が指示された入力部 101 は、位置情報取得部 102 に対して位置情報取得要求を通知する。この通知を受けた位置情報取得部 102 は、情報通信端末 100 が現在居る位置を示す位置情報を取得する（ステップ S50）。取得された位置情報は、安全性判定部 104 に出力される。これと同時に、入力部 101 は、通信制御部 205 に対して移行先端末の位置情報取得要求を通知する。この通知を受けた通信制御部 205 は、無線通信部 206 を通じて移行先端末 220 を探索し、探索できた移行先端末 220 に対して位置情報を通知するように要求する（ステッ

プ S 6 1)。

[0042] この要求に対する応答を無線通信部 2 0 6 を通じて移行先端末 2 2 0 から受信して、移行先端末の位置情報を取得できた場合には（ステップ S 6 2、Y e s）、通信制御部 2 0 5 は、この移行先端末の位置情報を移行先端末位置情報保存部 2 0 9 に保存する（ステップ S 6 3）。一方、一定時間を待っても移行先端末の位置情報を取得できなかった場合には（ステップ S 6 2、N o）、通信制御部 2 0 5 は、通信できない状態にあると判断して処理を終了する。

[0043] 移行先端末の位置情報が保存されると、安全性判定部 2 0 4 は、位置情報取得部 1 0 2 から位置情報を、安全領域保存部 1 0 3 から安全領域を、移行先端末位置情報保存部 2 0 9 から移行先端末の位置情報をそれぞれ取得し、これらの情報及び領域に基づいてセキュリティリスクが低いか高いかを判断する（ステップ S 5 1）。例えば、安全性判定部 2 0 4 は、情報通信端末 2 0 0 の現在位置も移行先端末 2 2 0 の現在位置も共に安全領域内に居れば、両端末間で無線通信を行ってもセキュリティリスクが低く安全であるとの判定を通信制御部 2 0 5 に通知する（ステップ S 5 1、Y e s）。一方、安全性判定部 2 0 4 は、情報通信端末 2 0 0 の現在位置も移行先端末 2 2 0 の現在位置も共に安全領域内に居なければ、両端末間で無線通信を行うとセキュリティリスクが高く危険であるとの判定を通信制御部 2 0 5 に通知する（ステップ S 5 1、N o）。なお、いずれか一方の端末だけが安全領域内にいる場合に、セキュリティリスクは中程度であると判断し、電波強度を中程度に設定する処理を行ってもよい。

[0044] そして、通信制御部 2 0 5 は、安全性判定部 2 0 4 からセキュリティリスクが低く安全であるとの通知を受けた場合、無線信号を送信する時の電波強度を予め定めた大きい値に設定するよう無線通信部 2 0 6 に指示を与える（ステップ S 5 2）。一方、通信制御部 2 0 5 は、安全性判定部 2 0 4 からセキュリティリスクが高く危険であるとの通知を受けた場合、無線信号を送信する時の電波強度を予め定めた小さい値に設定するよう無線通信部 2 0 6 に

指示を与える（ステップS 5 3）。そして、通信制御部 2 0 5 は、データ保存部 1 0 7 から無線通信で送信するデータを取得し、無線通信部 2 0 6 を通じて、取得したデータをステップS 5 2 又はS 5 3 で設定した電波強度の無線信号で移行先端末 2 2 0 に送信する（ステップS 5 4）。

[0045] 以上のように、本発明の第 2 の実施形態に係る情報通信端末 2 0 0 によれば、自己端末（移行元端末）に加えて相手端末（移行先端末）の現在位置をも判断して、無線信号の電波強度を設定する。これにより、上述した第 1 の実施形態による効果に加え、セキュリティをさらに向上させることが可能となる。

[0046] なお、上記実施形態では、安全領域が予め安全領域保存部 1 0 3 に保存されている場合を説明したが、安全領域は情報通信端末 1 0 0 及び 2 0 0 に予め保存されていなくてもよく、逐次保存されていくようにしてもよい。例えば、情報通信端末 1 0 0 及び 2 0 0 が、GPS 情報を常時受信していて、これまでに受信した複数の位置情報の履歴に基づいて特定の領域、例えば特に頻繁に通る領域を判定し、この判定した特定の領域を安全領域として安全領域保存部 1 0 3 に登録してもよい。このように処理することで、ユーザは、安全領域を明示的に登録する必要がなくなる。

[0047] また、上記実施形態では、情報通信端末 1 0 0 及び 2 0 0 の現在位置を、GPS 情報やWi-Fi のアクセスポイントから受信するMAC アドレス及び電波強度で検出し、この検出した現在位置と安全領域とを比較する場合を説明したが、情報通信端末 1 0 0 及び 2 0 0 の現在位置を検出できない場合もあり得る。そこで、このような安全領域と比較する情報がない場合には、セキュリティリスクが高く危険であると判断してもよい。

[0048] また、上記実施形態では、情報通信端末 1 0 0 及び 2 0 0 の現在位置と安全領域とでセキュリティリスク判定を行う場合を説明したが、現在位置に加えて現在時刻も加味してセキュリティリスク判定を行ってもよい。例えば、昼間は人混みがひどい場所でセキュリティリスクが高いと思われる場所でも、早朝は人も少なく見晴らしがよい場所であれば、比較的セキュリティリス

クは低いと判断できる場合がある。従って、このような場合、情報通信端末 100 及び 200 が安全領域内に居ない場合でも、現在時刻が早朝であればセキュリティリスクが低いと判定を行うことができる。

[0049] また、上記実施形態では、電波強度が大きいか又は小さいかの 2 パターンで制御される場合を説明したが、セキュリティリスクのレベルに合わせて複数の電波強度を用いてもよい。この場合、安全領域保存部 103 では、複数の安全領域のそれぞれに適用するセキュリティリスクレベルを関連付けて保存しておくことで、対応可能である。

[0050] さらに、上記実施形態では、情報通信端末間の通信は、ユーザの操作を契機として開始する場合を説明したが、切り替えを行う 2 つの情報通信端末の一方又は双方が移動している場合には、2 つの情報通信端末の距離が所定値よりも近接すれば自動的に通信を開始するようにしてもよい。この所定値とは、例えば、通信制御部 105 及び 205 が定めたリスク回避に適切な電波強度によってデータが移行先端末に届く距離である。

[0051] <本発明の具体的な適用例>

冒頭で説明したように、1 人のユーザが複数の情報通信端末を所有しているような場合には、外出先でタブレット PC 10 を用いて閲覧していた Web サイトを、帰宅した時に自宅のノート PC 30 を用いてシームレスに引き続き閲覧したい場面等が考えられる。この場面では、ブラウザアプリの起動や、閲覧中の Web サイトを表示するための HTML 文書の取得や、アクセス履歴等に関する移行データを、移行先端末へ送信する必要がある。このような移行データの送信にはある程度の時間がかかるため、シームレスな引き継ぎを実現するためには、前倒しで移行データの通信（ここでは「プリフェッチ通信」という）を開始しておくことが望ましい。本発明が提供する技術は、このプリフェッチ通信に適用可能である。

[0052] 例えば、自宅の半径 50 m を安全領域として定義しておき、移行元端末であるタブレット PC 10 がこの安全領域内に入れば 1 自宅のノート PC 30 と自動的にプリフェッチ通信を開始するようにする（図 10）。また、

安全領域を段階的に設けて、自宅から遠い間（半径100m）は小さい電波強度でプリフェッチ通信を行い、自宅に近付けば（半径20m）大きい電波強度でプリフェッチ通信を行うようにしてもよい。この処理により、ユーザが自宅に着く頃には移行のための通信の全て又は大半が完了し、ユーザはWebサイトの継続閲覧を素早く始めることができる。なお、このプリフェッチ通信を開始する距離は、移行するデータ量、通信速度、及び端末の移動速度などを考慮して、プリフェッチを完了するために必要十分な距離となる所定値を定めるとよい。

[0053] なお、本発明の各実施形態における情報通信端末を構成する一部又は全部の機能ブロックは、中央処理装置（CPU）、記憶装置（メモリ（ROM、RAM等）、ハードディスク等）、及び入出力装置などのハードウェア資源を用いることで実現され、典型的には集積回路であるIC（LSI、システムLSI、スーパーLSI、ウルトラLSI等とも称される）として具現化される。これらの機能ブロックは、個別に1チップ化されてもよいし、一部又は全部を含むように1チップ化されてもよい。

また、集積回路化の手法は、ICに限るものではなく、専用回路又は汎用プロセッサで実現してもよい。また、IC製造後にプログラムすることが可能なFPGA（Field Programmable Gate Array）や、IC内部の回路セルの接続や設定を再構成可能なリコンフィギュラブル・プロセッサを利用してもよい。

さらには、半導体技術の進歩又は派生する別の技術により、ICに置き換わる集積回路化の技術（バイオ技術など）が登場すれば、当然その技術を用いて機能ブロックの集積化を行ってもよい。

[0054] また、上述した本発明の各実施形態における情報通信端末が実行する通信方法は、記憶装置に格納された通信方法の手順を実行可能な所定のプログラムデータが、CPUによって解釈実行されることで実現されてもよい。この場合、プログラムデータは、CD-ROMやフレキシブルディスク等の記録媒体を介して記憶装置内に導入されてもよいし、記録媒体上から直接実行さ

れてもよい。なお、記録媒体は、ROMやRAMやフラッシュメモリ等の半導体メモリ、フレキシブルディスクやハードディスク等の磁気ディスクメモリ、CD-ROMやDVDやBD等の光ディスクメモリ、及びメモリカードなどをいう。また、記録媒体は、電話回線や搬送路などの通信媒体も含む概念である。

産業上の利用可能性

[0055] 本発明は、アプリケーションを実行可能な情報通信端末及び当該端末を構成に含んだシステム等に利用可能であり、特にセキュリティを確保しつつ、情報通信端末間の通信効率及び利便性を向上させたい場合等に有用である。

符号の説明

[0056] 10 タブレットPC
11、21 表示画面
20 携帯電話
30 ノートPC
40 ネットワーク
100、200 情報通信端末
101 入力部
102 位置情報取得部
103 安全領域保存部
104、204 安全性判定部
105、205 通信制御部
106、206 無線通信部
107 データ保存部
108 アプリケーション
209 移行先端末位置情報保存部
220 移行先端末

請求の範囲

- [請求項1] 近距離通信で無線通信を行う情報通信端末であって、
前記情報通信端末の位置情報を取得する位置情報取得部と、
他の端末と通信する時に安全であると登録されている安全領域を保存する安全領域保存部と、
前記情報通信端末の位置情報及び前記安全領域に基づいて、前記情報通信端末が前記他の端末と通信を行う場合のセキュリティリスクを判定する安全性判定部と、
前記安全性判定部において、通信時のセキュリティリスクが高いと判定された場合、予め定めた小さい電波強度で前記他の端末とのデータ通信を行い、通信時のセキュリティリスクが低いと判定された場合、予め定めた大きい電波強度で前記他の端末とのデータ通信を行う通信部とを備える、情報通信端末。
- [請求項2] ユーザが指示を入力する入力部をさらに備え、
前記安全領域は、前記入力部を通じてユーザによって入力されることを特徴とする、請求項1に記載の情報通信端末。
- [請求項3] 前記位置情報取得部は、これまでに取得した複数の位置情報の履歴に基づいて前記安全領域を決定することを特徴とする、請求項1に記載の情報通信端末。
- [請求項4] 前記安全性判定部は、前記位置情報取得部において前記情報通信端末の位置情報を取得できなかった場合は、通信時のセキュリティリスクが高いと判定することを特徴とする、請求項1に記載の情報通信端末。
- [請求項5] 前記安全性判定部は、前記位置情報から得られる前記情報通信端末の現在位置が前記安全領域内にあるか否かで、通信時のセキュリティリスクを判定することを特徴とする、請求項1に記載の情報通信端末。
- [請求項6] 前記安全性判定部は、前記位置情報から得られる情報取得時刻をさ

らに判断して、通信時のセキュリティリスクを判定することを特徴とする、請求項 5 に記載の情報通信端末。

[請求項7] 前記通信部は、前記他の端末の位置情報を取得し、
前記安全性判定部は、前記他の端末の位置情報をさらに考慮して、前記情報通信端末が前記他の端末と通信を行う場合のセキュリティリスクを判定することを特徴とする、請求項 1 に記載の情報通信端末。

[請求項8] 前記通信部は、前記情報通信端末と前記他の端末との距離が、前記安全性判定部の判定に基づいて決定した電波強度で通信可能な距離になったタイミングで、データ通信を開始することを特徴とする、請求項 7 に記載の情報通信端末。

[請求項9] 近距離通信で無線通信を行う第 1 及び第 2 の情報通信端末を含む通信システムであって、

前記第 1 の情報通信端末は、

前記第 1 の情報通信端末の位置情報を取得する位置情報取得部と、

前記第 2 の情報通信端末と通信する時に安全であると登録されている安全領域を保存する安全領域保存部と、

前記位置情報及び前記安全領域に基づいて、前記第 1 の情報通信端末が前記第 2 の情報通信端末と通信を行う場合のセキュリティリスクを判定する安全性判定部と、

前記安全性判定部において、通信時のセキュリティリスクが高いと判定された場合、予め定めた小さい電波強度で前記第 2 の情報通信端末とのデータ通信を行い、通信時のセキュリティリスクが低いと判定された場合、予め定めた大きい電波強度で前記第 2 の情報通信端末とのデータ通信を行う通信部とを備える、通信システム。

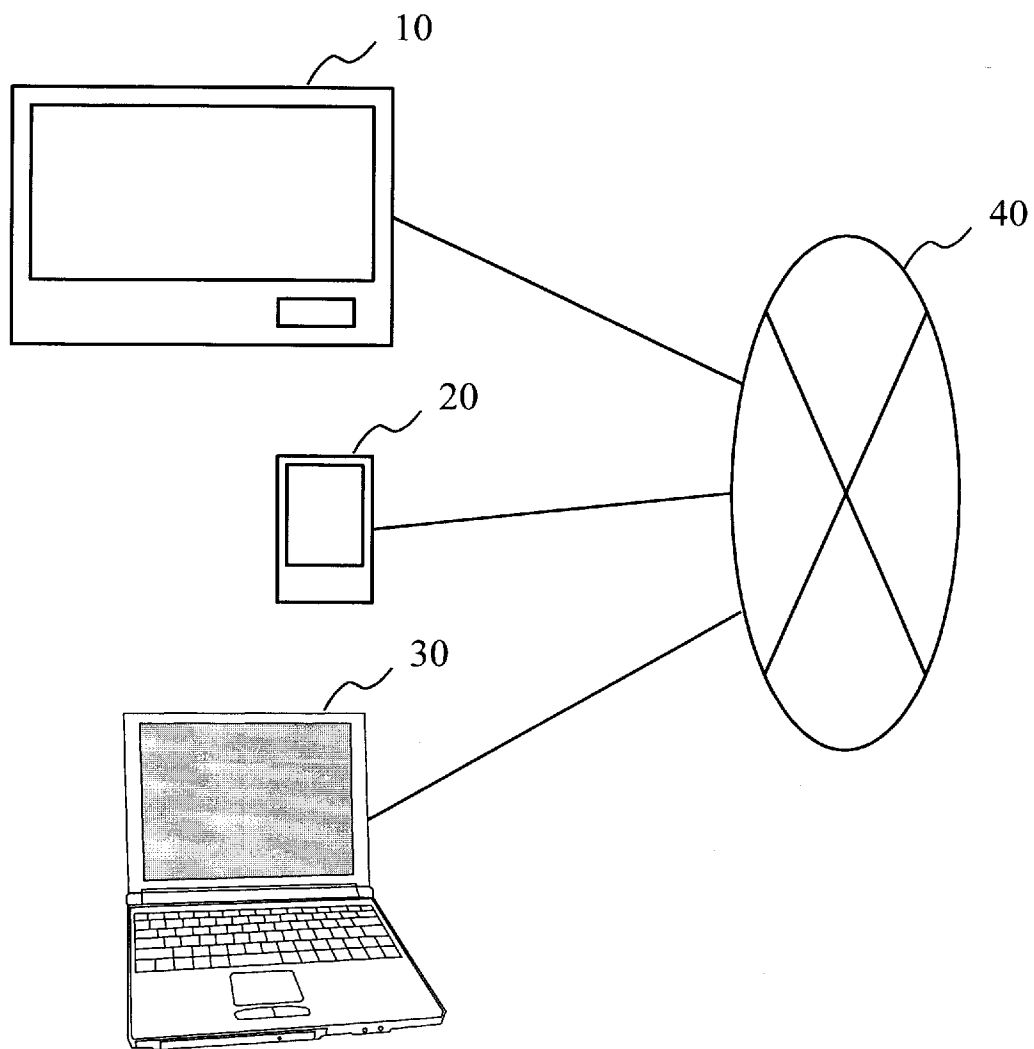
[請求項10] 近距離通信で無線通信を行う情報通信端末が行う通信方法であって、

前記情報通信端末の位置情報を取得するステップと、

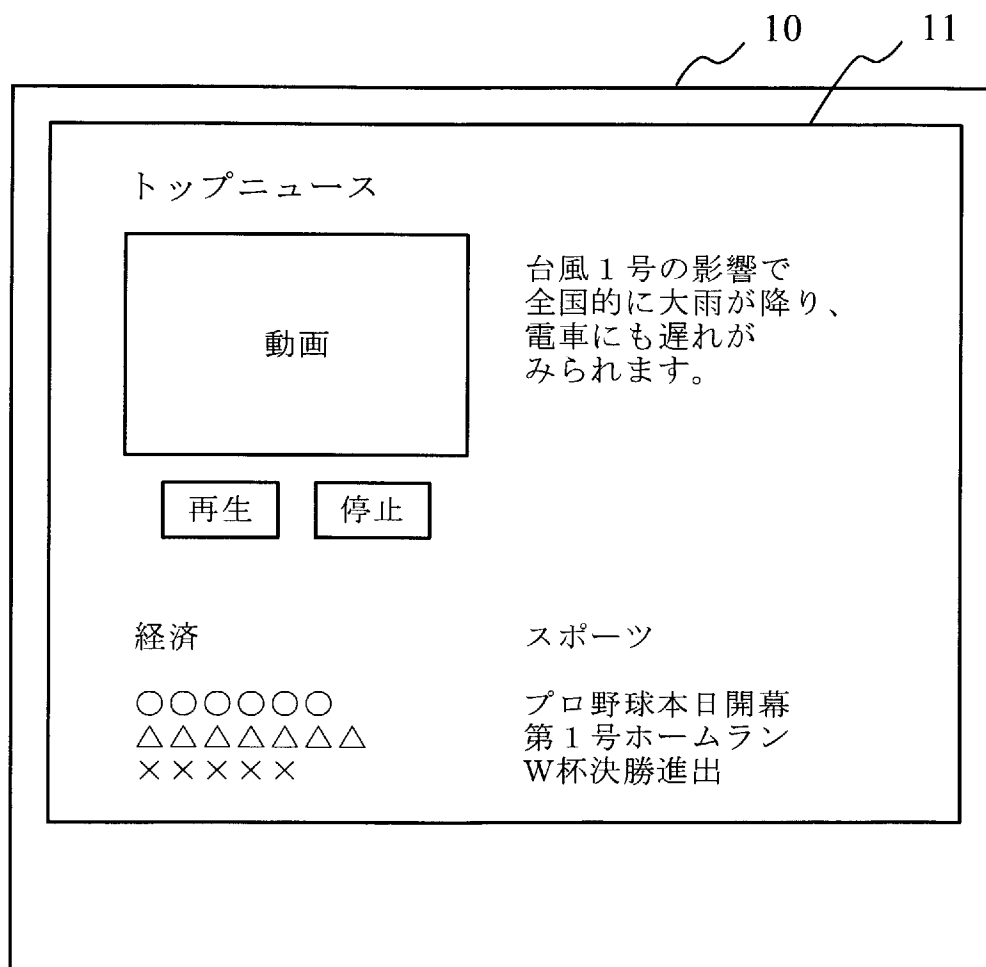
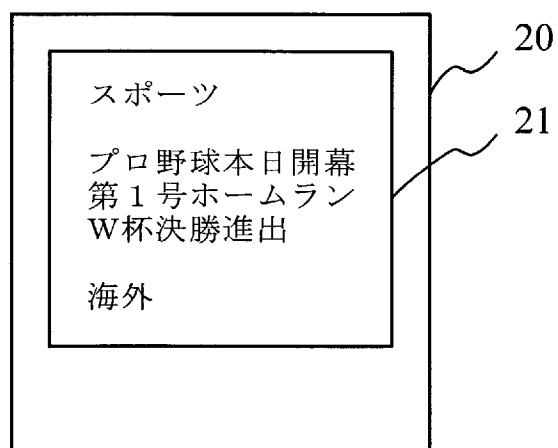
前記位置情報及び予め保存する他の端末と通信する時に安全であると登録されている安全領域に基づいて、前記情報通信端末が前記他の端末と通信を行う場合のセキュリティリスクを判定するステップと、

前記判定ステップにおいて、通信時のセキュリティリスクが高いと判定された場合、予め定めた小さい電波強度で前記他の端末とのデータ通信を行い、通信時のセキュリティリスクが低いと判定された場合、予め定めた大きい電波強度で前記他の端末とのデータ通信を行うステップとを含む、通信方法。

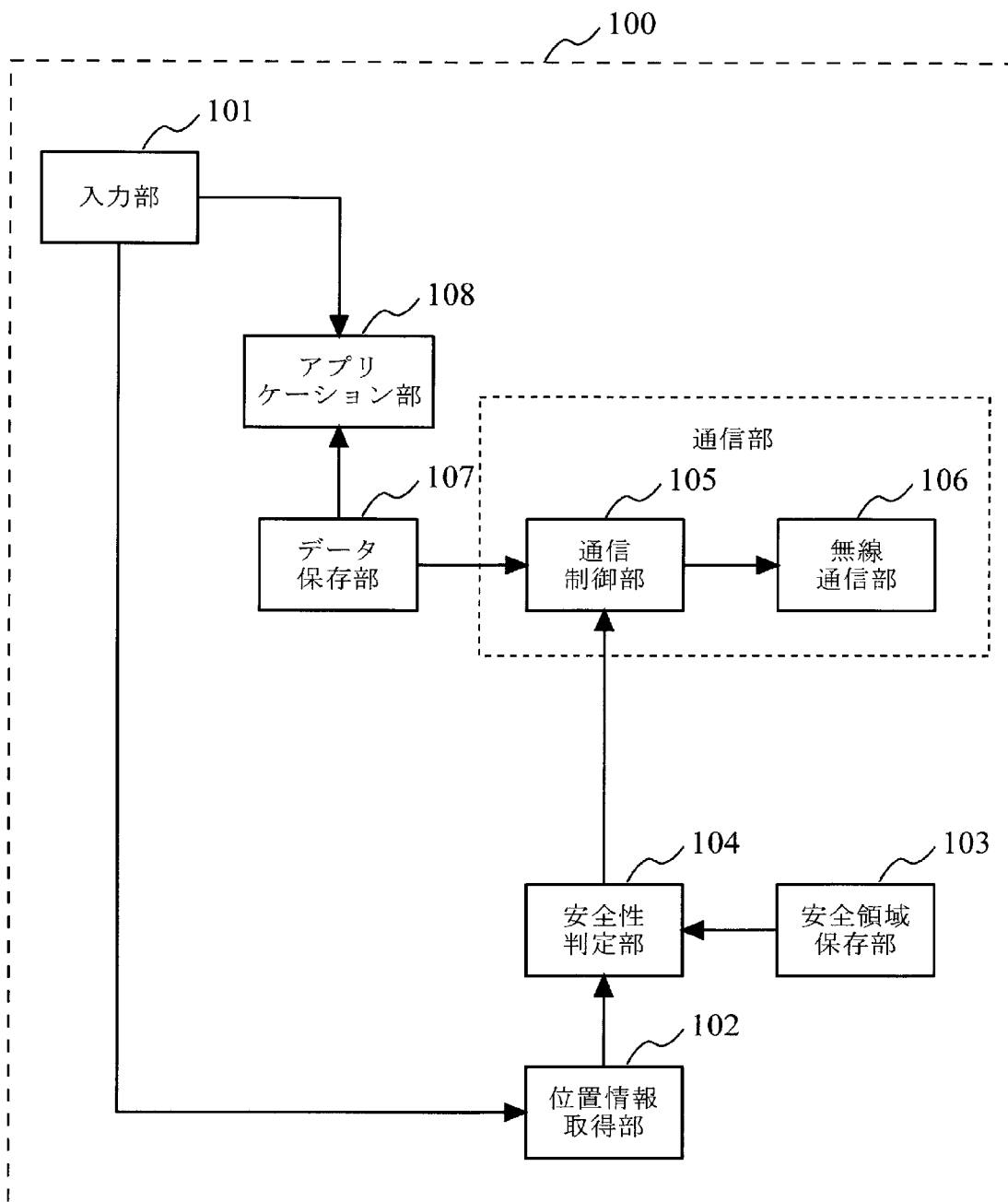
[図1]



[図2]



[図3]



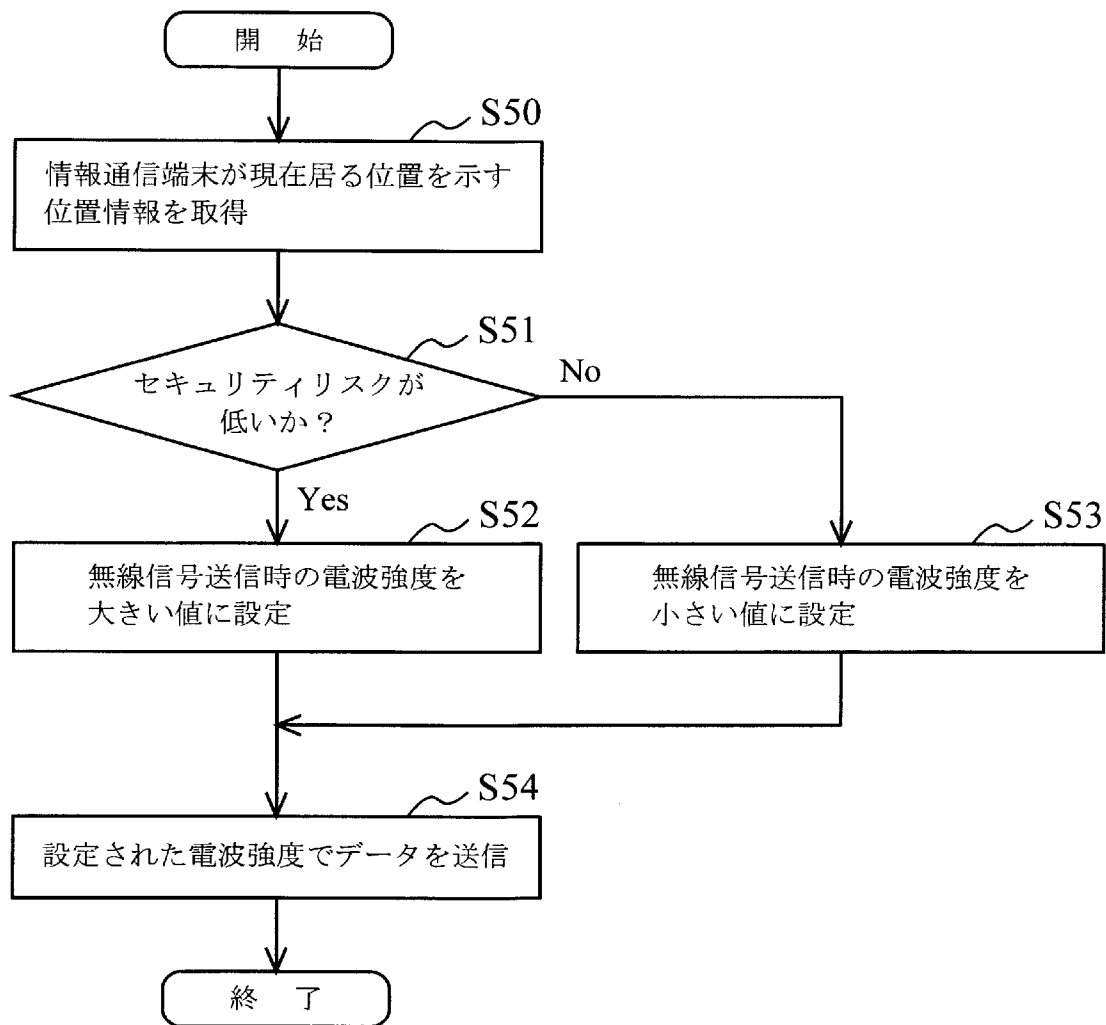
[図4]

取得時刻	現在位置（緯度，経度）
2011/2/10 14:00	(+34.44.36.02, +135.26.44.35)

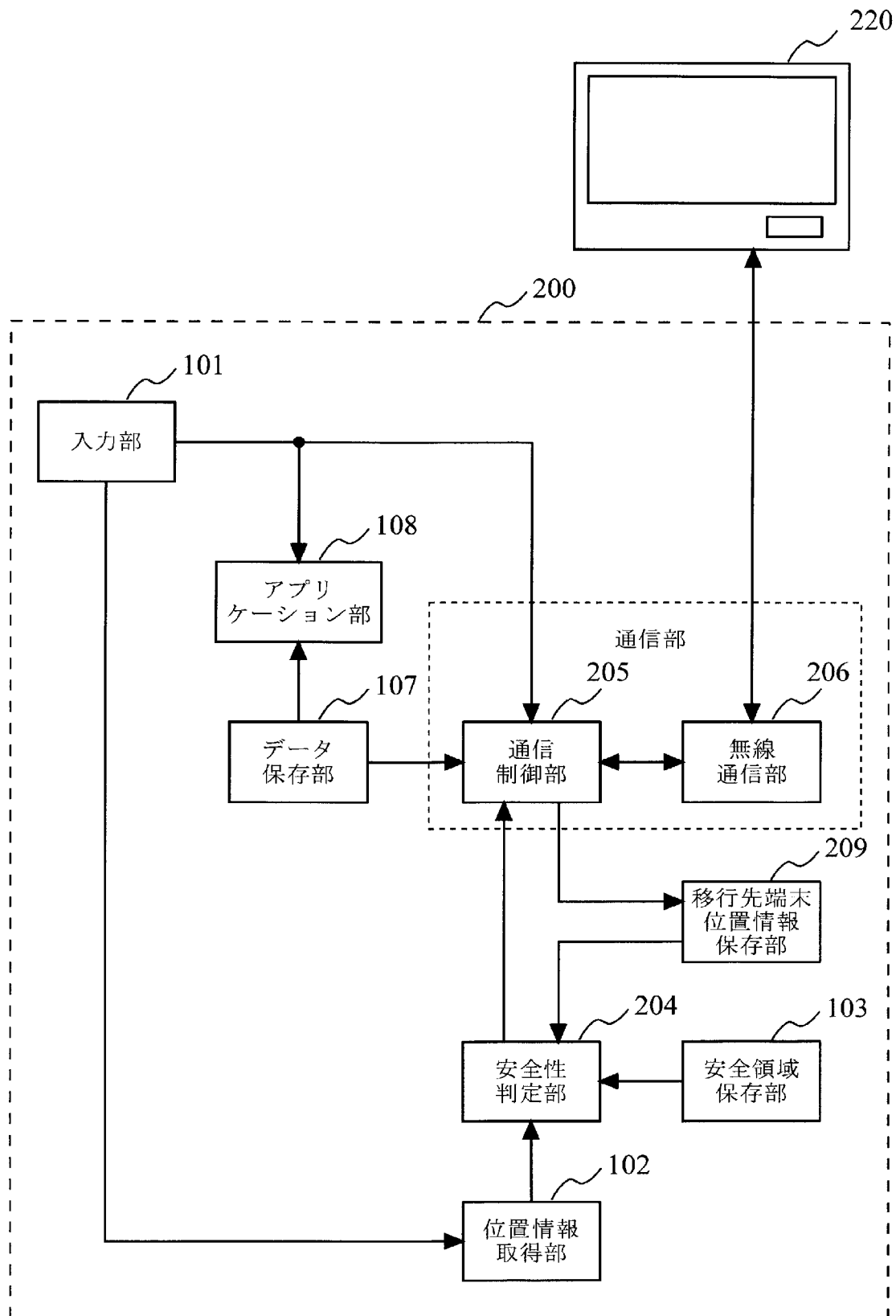
[図5]

(a)	安全領域の中心（緯度，経度）	半径距離
	(+34.39.55.16, +135.30.18.98)	30 m
(b)	矩形対角頂点	座標（緯度，経度）
	(N1, E1)	(+34.39.55.16, +135.30.28.98)
	(N2, E2)	(+34.39.55.20, +135.30.18.98)

[図6]



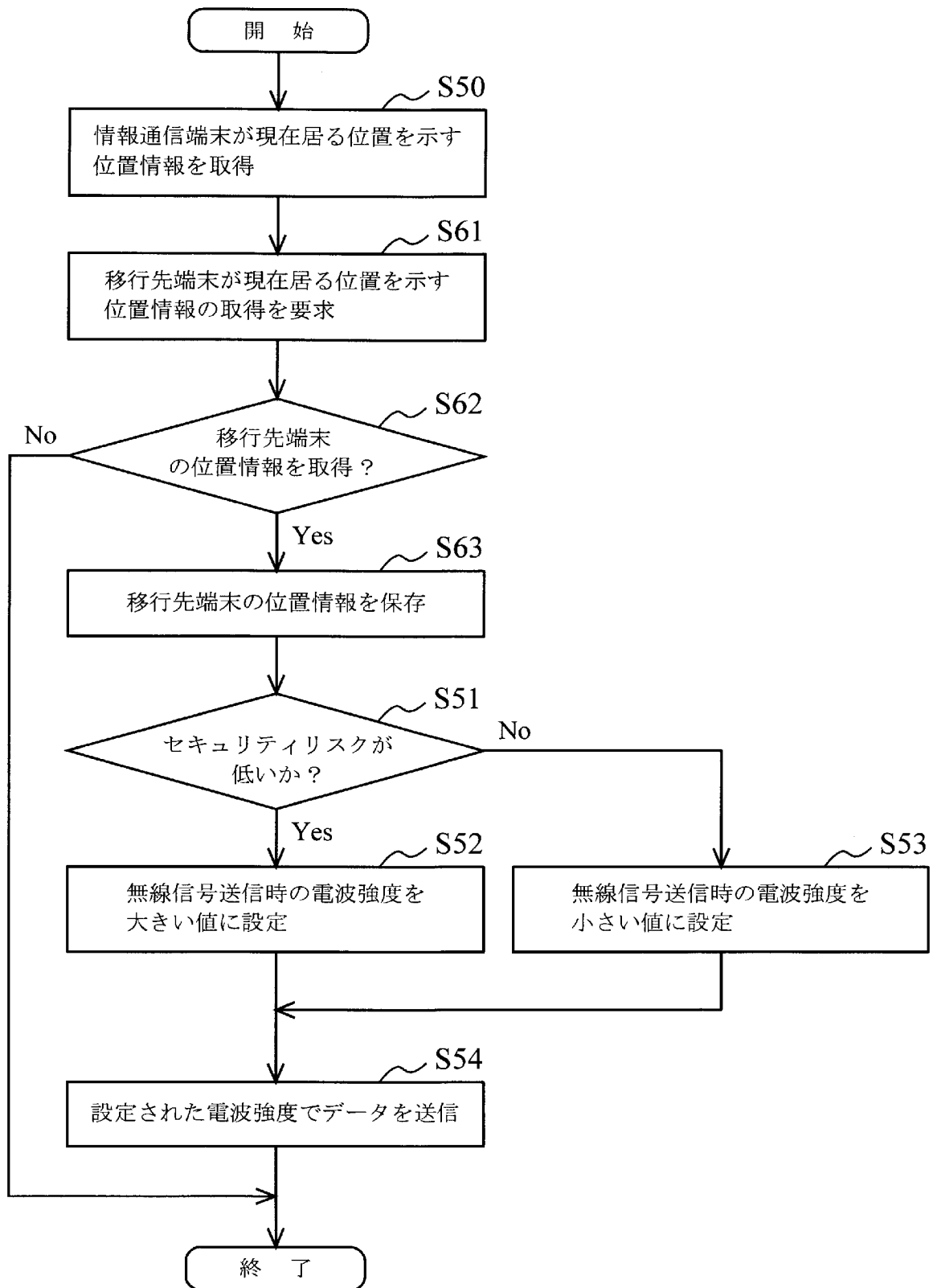
[図7]



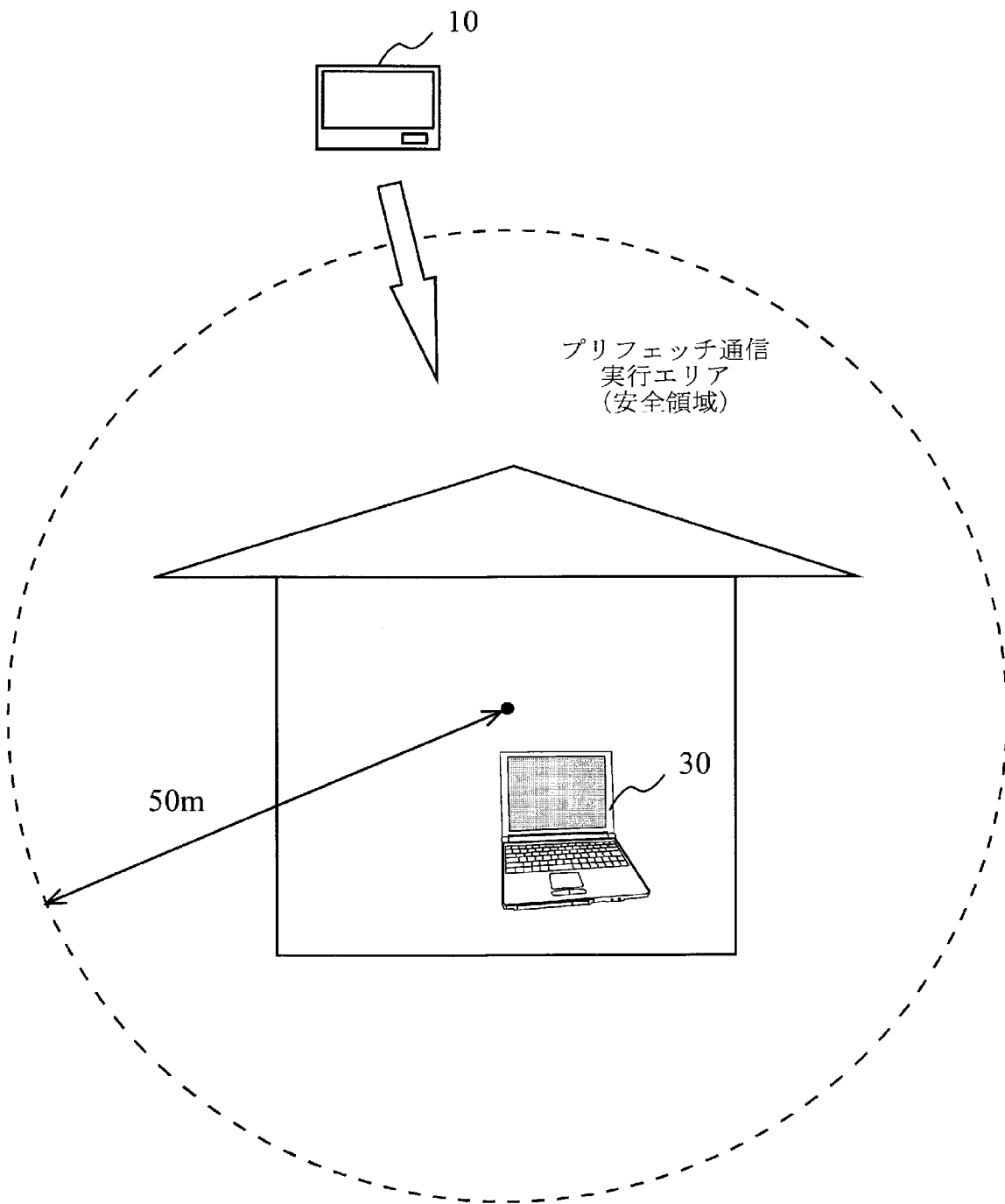
[図8]

受信時刻	現在位置（緯度，経度）
2011/2/14 14:00	(+34.44.36.00, +135.26.44.30)

[図9]



[図10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2012/000451

A. CLASSIFICATION OF SUBJECT MATTER

H04W12/08 (2009.01) i, H04M1/00 (2006.01) i, H04M11/00 (2006.01) i, H04W52/28 (2009.01) i, H04W64/00 (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, H04M1/00, H04M11/00, H04W52/28, H04W64/00

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	1996-2012
Kokai Jitsuyo Shinan Koho	1971-2012	Toroku Jitsuyo Shinan Koho	1994-2012

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.
A	JP 2003-099400 A (Fujitsu Ltd.), 04 April 2003 (04.04.2003), claims & US 2003/0061166 A1	1-10
A	JP 2004-247819 A (Matsushita Electric Industrial Co., Ltd.), 02 September 2004 (02.09.2004), claims 1, 13 (Family: none)	1-10
A	JP 2008-017302 A (NTT Docomo Inc.), 24 January 2008 (24.01.2008), paragraphs [0045] to [0066] (Family: none)	1-10



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
27 March, 2012 (27.03.12)

Date of mailing of the international search report
03 April, 2012 (03.04.12)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2012/000451

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 2008-538684 A (Microsoft Corp.), 30 October 2008 (30.10.2008), claim 1 & US 2006/0239217 A1 & US 2007/0081508 A1 & EP 1872349 A & WO 2006/113884 A2 & KR 10-2008-0002849 A & CN 101223450 A	1-10
A	JP 2005-057773 A (Toshiba Corp.), 03 March 2005 (03.03.2005), claim 1 & US 2005/0059388 A1 & GB 2404820 A & GB 318430 D0	1-10
A	JP 2006-020259 A (Sony Ericsson Mobile Communications Japan, Inc.), 19 January 2006 (19.01.2006), claim 4 & US 2006/0003815 A1 & EP 1613037 A2 & AU 2005202864 A	1-10

A. 発明の属する分野の分類 (国際特許分類 (I P C))

Int.Cl. H04W12/08 (2009.01)i, H04M1/00 (2006.01)i, H04M11/00 (2006.01)i, H04W52/28 (2009.01)i,
H04W64/00 (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 (I P C))

Int.Cl. H04W12/08, H04M1/00, H04M11/00, H04W52/28, H04W64/00

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	1 9 2 2 - 1 9 9 6 年
日本国公開実用新案公報	1 9 7 1 - 2 0 1 2 年
日本国実用新案登録公報	1 9 9 6 - 2 0 1 2 年
日本国登録実用新案公報	1 9 9 4 - 2 0 1 2 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
A	JP 2003-099400 A (富士通株式会社) 2003. 04. 04, 【特許請求の範囲】 & US 2003/0061166 A1	1-10
A	JP 2004-247819 A (松下電器産業株式会社) 2004. 09. 02, 【請求項 1】, 【請求項 1 3】 (ファミリーなし)	1-10
A	JP 2008-017302 A (株式会社エヌ・ティ・ティ・ドコモ) 2008. 01. 24, 【0045】 - 【0066】 (ファミリーなし)	1-10

☒ 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

2 7 . 0 3 . 2 0 1 2

国際調査報告の発送日

0 3 . 0 4 . 2 0 1 2

国際調査機関の名称及びあて先

日本国特許庁 (I S A / J P)
郵便番号 1 0 0 - 8 9 1 5
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)

齋藤 浩兵

電話番号 0 3 - 3 5 8 1 - 1 1 0 1 内線 3 5 3 4

5 J

3 7 9 4

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 2008-538684 A (マイクロソフト コーポレーション) 2008. 10. 30, 【請求項 1】 & US 2006/0239217 A1 & US 2007/0081508 A1 & EP 1872349 A & WO 2006/113884 A2 & KR 10-2008-0002849 A & CN 101223450 A	1-10
A	JP 2005-057773 A (株式会社東芝) 2005. 03. 03, 【請求項 1】 & US 2005/0059388 A1 & GB 2404820 A & GB 318430 D0	1-10
A	JP 2006-020259 A (ソニー・エリクソン・モバイルコミュニケーションズ株式会社) 2006. 01. 19, 【請求項 4】 & US 2006/0003815 A1 & EP 1613037 A2 & AU 2005202864 A	1-10