

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2005-286534
(P2005-286534A)

(43) 公開日 平成17年10月13日(2005. 10. 13)

(51) Int. Cl. ⁷	F I	テーマコード (参考)
H04L 12/28	H04L 12/28 300Z	5K033
H04Q 3/58	H04Q 3/58 101	5K049
H04Q 7/38	H04B 7/26 109S	5K067

審査請求 有 請求項の数 5 O L (全 7 頁)

(21) 出願番号	特願2004-95260 (P2004-95260)	(71) 出願人	000004237 日本電気株式会社 東京都港区芝五丁目7番1号
(22) 出願日	平成16年3月29日 (2004. 3. 29)	(74) 代理人	100096231 弁理士 稲垣 清
		(72) 発明者	安達 眞幸 東京都港区芝五丁目7番1号 日本電気株式会社内
		Fターム(参考)	5K033 CB01 DA06 DA19 5K049 AA07 BB16 FF01 FF32 5K067 AA32 BB04 BB08 BB21 BB34 DD17 FF07 HH05 HH22 HH23

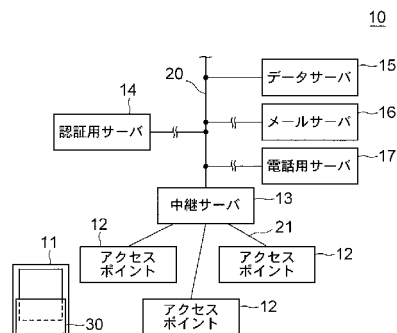
(54) 【発明の名称】 構内通信システム

(57) 【要約】

【課題】 ユーザとの間での連絡困難を解消し、且つ、無資格者によるアクセスを防止する構内通信システムを提供する。

【解決手段】 構内通信システムは、ICカード30が装着可能な携帯無線端末11と、携帯無線端末11のための複数の構内アクセスポイント12と、構内アクセスポイントをインターネット20に接続する中継サーバ13と、インターネット20に接続された認証用サーバ14、及び、複数のサーバ15、16、17を含むサーバ群とから成る。認証用サーバ14は、携帯無線端末11から受信した電子メールから読み取った個人認証ID、及び、電子メールを中継した中継サーバ13のIDに基づいて、ユーザのアクセス資格を判定し、携帯無線端末11からサーバ群へのアクセスに許可を与える。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

個人認証データを含む所定のデータを記憶する記憶媒体と、
前記記憶媒体から前記所定のデータを読み取るデータ読取り手段、及び、外部との間で
データを送受信する無線通信手段とを少なくとも有する端末装置と、

前記端末装置の無線通信手段と通信回線との間でデータを双方向に中継するデータ中継
手段と、

前記通信回線に接続され、前記端末装置から前記データ中継手段を経由して受信した個人
認証データ及び前記通信回線の経路の正否を判定し、該判定に基づいて、前記端末装置
によるアクセス資格を承認/否認する認証用サーバと、

10

前記通信回線に接続され、前記認証用サーバによってアクセス資格が承認された端末装
置によるアクセスを許可する、少なくとも1つのサーバを含むサーバ群とを備えることを
特徴とする構内通信システム。

【請求項 2】

前記認証用サーバは、受信したデータに前記データ中継手段を経由した旨の情報が含ま
れるか否かによって前記通信回線の経路の正否を判定する、請求項 1 に記載の構内通信シ
ステム。

【請求項 3】

前記通信回線がインターネットであり、前記記憶媒体は更に個人 IP アドレスを記憶し
、前記サーバ群が、前記認証用サーバによってアクセス資格が承認された端末装置に、前
記個人 IP アドレスを用いてアクセスすることを許可するデータサーバを含む、請求項 1
又は 2 に記載の構内通信システム。

20

【請求項 4】

前記記憶媒体が更に個人メールアドレスを記憶し、前記サーバ群が、前記認証用サーバ
によってアクセス資格が承認された端末装置に、前記個人メールアドレスを用いてインタ
ーネットにアクセスすることを許可するメールサーバを含む、請求項 3 に記載の構内通信
システム。

【請求項 5】

前記端末装置が、音声データを収集する音声データ収集手段を有し、前記サーバ群が、
前記認証用サーバによってアクセス資格が承認された端末装置に、特定の電話番号を用い
て IP 電話としての機能を付加する電話用サーバを含む、請求項 3 又は 4 に記載の構内通
信システム。

30

【発明の詳細な説明】**【技術分野】****【0001】**

本発明は、構内通信システムに関し、特に、外部からの不正アクセスを防止可能な構内
通信システムに関する。

【背景技術】**【0002】**

大規模な病院や、大学、工場等の構内では、構内通信専用の通信システムが用いられて
いる。図 5 に示すように、従来の構内通信システムでは、外部の通信回線 4 1 は、1 つ以
上の交換機 4 2 及び構内通信回線 4 3 を経由して、内線電話機やコンピュータ等の端末装
置 4 4 に接続される。構内で業務を行う、組織に属する各ユーザは、自身専用の端末装置
4 4、又は、任意の端末装置 4 4 を使用して、構外の通信回線 4 1 に接続された外部の端
末装置 4 5 と交信し (M 4)、又は、構内の通信回線 4 3 に接続された別の端末装置 4 4
との間で交信することが出来る (M 5)。

40

【0003】

構内通信システムでは、一般に、内線電話機やデスクトップ型コンピュータ等の端末装
置 4 4 は、固定式で用いられる。組織に属する各ユーザは、自身が例えば会議室等におり
、自席に居ない場合であっても、そのユーザの現在位置に最も近い内線電話機等の端末装

50

置 4 4 が使用可能である。しかし、別のユーザがそのユーザに連絡を取りたい場合に、その現在位置が不明の場合には、連絡を取ることが困難である。

【 0 0 0 4 】

固定式の内線電話機に代えて、組織に属する各ユーザに無線通信端末を貸与すると、電話での会話の他にデータの送受信等が可能になり、業務の効率が向上する。例えば、特許文献 1 には、病院内の患者管理システムにおいて、無線 LAN と有線のネットワークとをアクセスポイントで接続して、携帯無線端末から病院内のサーバに接続する構成が記載されている。この方式によると、組織に属する各ユーザは、構内の何れの場所においても、ネットワークにアクセスでき、上記従来の構内通信システムにおける連絡困難の問題を解消している。ここで、携帯無線端末の保持者は、アクセスの度に認証用サーバによって、アクセスの権限を有するか否かについて個人認証を受ける。

10

【 0 0 0 5 】

また、特許文献 2 には、インターネットと無線 LAN とを、無線 LAN 基地局で接続し、この無線 LAN 基地局にアクセスできる端末装置を備える構成が記載されている。無線 LAN には、P P P o E サーバを接続制御手段として、また、認証用サーバを認証手段として接続する。無線 LAN 基地局と接続した端末装置は、P P P o E サーバにアクセスしてアクセス認証とネットワークコンフィグレーションとを行うことで、無線 LAN 上の P P P o E を使用してインターネットにアクセスする。これによって、屋外や移動先などでも、端末装置を高速な無線 LAN によってインターネットにアクセス可能としている。

【特許文献 1】特開 2 0 0 3 - 3 1 8 9 1 3 号公報

20

【特許文献 2】特開 2 0 0 3 - 6 0 6 5 1 号公報

【発明の開示】

【発明が解決しようとする課題】

【 0 0 0 6 】

特許文献 1 及び特許文献 2 に記載のシステムによると、個人認証のために認証用サーバが用いられ、無資格者によるアクセスの排除を可能にしている。しかし、近年では、個人 ID 等が頻繁に盗まれ、無資格者が、認証用サーバによる資格判定をすり抜けて、業務用サーバに侵入する事例が増大している。この場合、企業秘密の業務情報が無資格者に盗用され、或いは、必要な業務情報が改ざんされて、業務に支障をきたす事例が度々発生している。

30

【 0 0 0 7 】

本発明は、上記に鑑み、構内通信システムにおける担当者の連絡困難等の問題を解消し、且つ、無資格者が業務用サーバにアクセスし、或いは、業務用サーバのデータを改ざんすることを防止できる構内通信システム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】

【 0 0 0 8 】

上記目的を達成するために、本発明の構内通信システムは、個人認証データを含む所定のデータを記憶する記憶媒体と、前記記憶媒体から前記所定のデータを読み取るデータ読取り手段、及び、外部との間でデータを送受信する無線通信手段とを少なくとも有する端末装置と、前記端末装置の無線通信手段と通信回線との間でデータを双方向に中継するデータ中継手段と、前記通信回線に接続され、前記端末装置から前記データ中継手段を経由して受信した個人認証データ及び前記通信回線の経路の正否を判定し、該判定に基づいて、前記端末装置によるアクセス資格を承認 / 否認する認証用サーバと、前記通信回線に接続され、前記認証用サーバによってアクセス資格が承認された端末装置によるアクセスを許可する、少なくとも 1 つのサーバを含むサーバ群とを備えることを特徴とする。

40

【発明の効果】

【 0 0 0 9 】

本発明の構内通信システムによると、携帯無線端末の所持によってユーザ間の連絡困難の問題が解消でき、また、認証用サーバが、個人認証データ及び通信経路の正否に基づいて、サーバ群へのアクセス資格の有無を判定するので、構内における特定の通信経路が利

50

用できない無資格者がサーバ群にアクセスする事態が防止できる。

【0010】

ここで、本発明の好ましい構内通信システムでは、前記認証用サーバは、受信したデータに前記データ中継手段を経由した旨の情報が含まれるか否かによって前記通信回線の経路の正否を判定する。この場合、無資格者によるアクセスがより効果的に防止できる。

【0011】

前記通信回線がインターネットであり、前記記憶媒体が更に個人IPアドレスを記憶し、前記サーバ群が、前記認証用サーバによってアクセス資格が承認された端末装置に、前記個人IPアドレスを用いてアクセスすることを許可するデータサーバを含むことも本発明の好ましい態様である。インターネットを利用することにより、無線端末装置の汎用性が高まる。

10

【0012】

前記記憶媒体が更に個人メールアドレスを記憶し、前記サーバ群が、前記認証用サーバによってアクセス資格が承認された端末装置に、前記個人メールアドレスを用いてインターネットにアクセスすることを許可するメールサーバを含むことも本発明の好ましい態様である。この場合、更に無線端末装置の汎用性が向上する。

【0013】

前記端末装置が、音声データを収集する音声データ収集手段を有し、前記サーバ群が、前記認証用サーバによってアクセス資格が承認された端末装置に、特定の電話番号を用いてIP電話の機能を付加する電話用サーバを含むことも本発明の好ましい態様である。この場合、端末装置の汎用性が更に向上する。

20

【発明を実施するための最良の形態】

【0014】

以下、図面を参照し、本発明の好適な実施形態例に基づいて本発明を更に詳細に説明する。図1に、本発明の一実施形態例に係る構内通信システムの構成を示す。本システムでは、組織に属する各ユーザは、ICカード（記憶媒体）30を装着可能な携帯無線端末11を所持している。携帯無線端末11は、構内の複数の場所に配置されたアクセスポイント12を経由して中継サーバ13に接続され、中継サーバ13を経由してインターネット20に接続される。インターネット20には、構内通信システム10に属する認証用サーバ14と、データサーバ15、メールサーバ16、電話用サーバ17等を含むサーバ群とが接続されている。

30

【0015】

携帯無線端末11は、図2に示すように、ICカードスロット31を有しており、そのICカードスロット31には、個人認証に必要な個人認証用IDを記憶するICカード30が挿入可能である。ICカード30は、組織に属する各個人に貸与され、ICカード30には、各個人の個人認証用IDと、個人IPアドレスと、個人メールアドレスとが記憶されている。携帯無線端末11は、音声による入出力手段（図示せず）と、データを画面上に表示するLCD装置32と、キー入力手段33と、ICカードスロットに挿入されたICカードから情報を読み取る読取り手段（図示せず）と、無線通信手段（図示せず）とを有している。

40

【0016】

図3に示すように、アクセスポイント12は、携帯無線端末11と無線の通信回線22で接続され、且つ、中継サーバ13とは構内の有線通信回線21を介して接続される。中継サーバ13は、本構内通信システムにおける中継局としての機能を持つ。また、アクセスポイント12、中継サーバ13、及び、有線通信回線21は、携帯無線端末11をインターネット20に接続するためのデータ中継手段を構成する。中継サーバ13は、インターネット上で特定のID（アドレス）を有しており、携帯無線端末11から受信した電子メールに自身のIDを付加して、認証用サーバ14に転送する機能を有する。

【0017】

認証用サーバ14は、中継サーバ13及びインターネット20を経由して、携帯無線端

50

末 1 1 との間で交信が可能である。認証用サーバ 1 4 は、携帯無線端末 1 1 から受信した電子メール (M 1) に中継サーバ 1 4 の I D が付加されていると、その携帯無線端末 1 1 が、予め設定された正規の経路を使ってアクセスした携帯無線端末であると認識し、その携帯無線端末 1 1 に対してサーバ群の各サーバへのアクセス許可を通知する機能を有する。同時に、その携帯無線端末 1 1 の I P アドレス及び中継サーバ 1 4 の I D を、データサーバ 1 5、メールサーバ 1 6、及び、電話用サーバ 1 7 を含むサーバ群に送信する機能を有する。これによって、その中継サーバ 1 4 を経由する、特定の I P アドレスの携帯無線端末からのアクセスを許可するように通知する。

【 0 0 1 8 】

ユーザは、無線携帯無線端末 1 1 を使用して本システムにアクセスするときには、まず、個人認証に必要な情報を記憶した I C カード 3 0 を携帯無線端末 1 1 に装着する。携帯無線端末 1 1 はモバイル I P v 6 などの技術を使い、携帯無線端末 1 1 をインターネットに接続する。携帯無線端末 1 1 は、インターネットに接続した後に、認証用サーバ 1 4 に対して電子メールを送信する (M 1)。なお、電子メールに限らず、受信側で通信経路が判定できる通信方法であればよい。

10

【 0 0 1 9 】

次いで、認証用サーバ 1 4 は、携帯無線端末 1 1 から送付された電子メールに含まれる個人の認証用 I D 情報と、電子メールに付加された電子メールの伝達経路の情報とに基づいて、データサーバ 1 5、メールサーバ 1 6、電話用サーバ 1 7 を含むサーバ群にアクセスする資格を有する個人が、許可された場所からアクセスしているかを判定する。この判定では、認証用サーバ 1 4 は、携帯無線端末 1 1 がインターネットに接続した際に通過したサーバを調べて、このインターネット 2 0 上で携帯無線端末 1 1 に一番近い位置にあるサーバの I D (又はアドレス) と、携帯無線端末 1 1 に取り付けられた I C カード 3 0 中の個人認証用 I D 情報とに基づいて判定する。なお、この判定では、更に、携帯無線端末の機器情報を含めてもよい。

20

【 0 0 2 0 】

認証用サーバ 1 4 は、アクセス資格を有する個人が、許可された場所からアクセスしていることが確認できたら、データサーバ 1 5、メールサーバ 1 6、及び、電話用サーバを含むサーバ群に通知し (M 2)、データサーバ 1 5、メールサーバ 1 6 内のデータに携帯無線端末 1 1 がアクセスできるようにデータサーバ 1 5、及び、メールサーバ 1 6 に設定を要求し、また、電話用サーバ 1 7 には、携帯無線端末 1 1 が I P 電話として使用できるように設定を要求する。

30

【 0 0 2 1 】

データサーバ 1 5、メールサーバ 1 6、電話用サーバ 1 7 は、認証用サーバからの通知に基づいて、指定された個人認証用 I D を有し且つ特定の I D を有するサーバ (中継サーバ) を経由する携帯無線端末 1 1 からのアクセス要求を受け入れる。データサーバ 1 5、メールサーバ 1 6、電話用サーバ 1 7 は、図 4 に示すように、アクセスが許可された携帯無線端末 1 1 に対して、各サーバへのアクセスが許可された旨を通知する (M 3)。携帯無線端末 1 1 は、データサーバ 1 5、メールサーバ 1 6、及び、電話用サーバ 1 7 などからこのアクセス許可通知を受け取り、ブラウザの起動や、電話としての機能を起動する。

40

【 0 0 2 2 】

本実施形態例に係る構内通信システムでは、上記構成を採用し、 I P v 6 などのインターネット技術と無線通信技術とを組み合わせることにより、携帯無線端末 1 1 を所持したユーザ相互間で、その携帯無線端末 1 1 が動作している限り、交信が可能である。また、構内通信システムから、携帯無線端末を所持するユーザと連絡を取ることが出来る。更に、認証用サーバ 1 4 が、中継サーバ 1 3 を経由して交信をする携帯無線端末 1 1 以外には、サーバ群へのアクセスを許可しないので、外部の無資格者による構内通信システムへの侵入を困難にする。

【 0 0 2 3 】

50

以上、本発明をその好適な実施形態例に基づいて説明したが、本発明の構内通信システムは、上記実施形態例の構成にのみ限定されるものではなく、上記実施形態例の構成から種々の修正及び変更を施したものも、本発明の範囲に含まれる。例えば、通信回線は、インターネットに限らない。

【0024】

また、アクセスポイントから中継サーバまでは、構内通信回線であるとした例を示したが、これに限らず、インターネット等でもよい。この場合、中継サーバには外部からのアクセスも可能であるが、認証用サーバが、アクセスポイントの通過で経路を判定してもよい。或いは、アクセスポイントから最も近いサーバIDに基づいて経路を判定することにより、無資格者のアクセス可能性を大幅に制限することでもよい。また、IPアドレスやメールアドレスは、ICカードに記憶するのに代えて、認証用サーバやメールサーバ等から与えてもよい。

10

【図面の簡単な説明】

【0025】

【図1】本発明の一実施形態例に係る構内通信システムのブロック図。

【図2】図1の携帯無線端末の構成を示す斜視図。

【図3】図1の通信システムにおけるデータの流れを示すブロック図。

【図4】図1の通信システムにおけるデータの流れを示すブロック図。

【図5】従来の構内通信システムを示すブロック図。

【符号の説明】

20

【0026】

10：構内通信システム

11：携帯無線端末

12：アクセスポイント

13：中継サーバ

14：認証用サーバ

15：データサーバ

16：メールサーバ

17：電話用サーバ

20：インターネット

30

21：構内通信回線

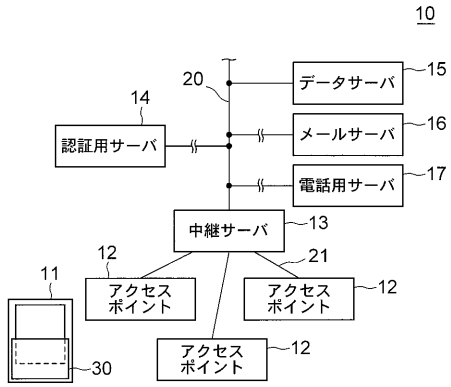
30：ICカード

31：ICカードスロット

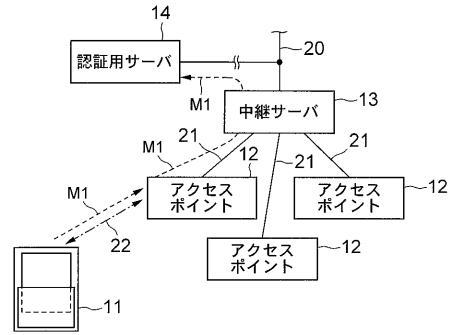
32：LCD

33：キー入力装置

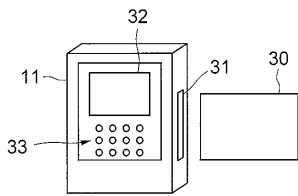
【 図 1 】



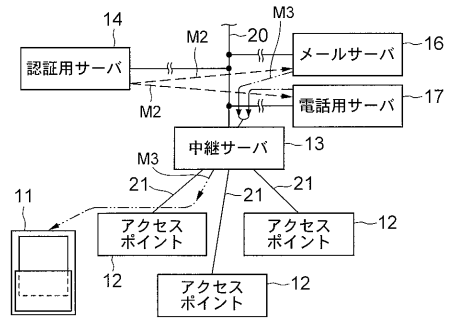
【 図 3 】



【 図 2 】



【 図 4 】



【 図 5 】

