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

特許第4659864号
(P4659864)

(45)発行日　平成23年3月30日(2011.3.30)　(24)登録日　平成23年1月7日(2011.1.7)

(51)Int.Cl.		F I		
H04W 48/18	(2009.01)	H04Q	7/00	413
H04W 36/14	(2009.01)	H04Q	7/00	309
H04W 12/06	(2009.01)	H04Q	7/00	183
H04W 12/04	(2009.01)	H04Q	7/00	182

請求項の数 9　(全 18 頁)

(21)出願番号　特願2008-196109(P2008-196109)
(22)出願日　平成20年7月30日(2008.7.30)
(65)公開番号　特開2010-34945(P2010-34945A)
(43)公開日　平成22年2月12日(2010.2.12)
審査請求日　平成22年3月11日(2010.3.11)

(73)特許権者　000006633
京セラ株式会社
京都府京都市伏見区竹田鳥羽殿町６番地
(74)代理人　110001106
キュリーズ特許業務法人
(72)発明者　立川　仁也
神奈川県横浜市都筑区加賀原２丁目１番１号　京セラ株式会社　横浜事業所内

審査官　望月　章俊

(56)参考文献　特開２００８－０１５６９６（ＪＰ，Ａ）

最終頁に続く

(54)【発明の名称】通信システム、認証サーバおよび通信方法

(57)【特許請求の範囲】
【請求項１】
第１無線基地局から第２無線基地局へのハンドオーバを実行する無線端末と、前記第１無線基地局を介した通信ネットワークへの第１アクセスの認証を行う第１認証サーバと、前記第２無線基地局を介した前記通信ネットワークへの第２アクセスの認証を行う第２認証サーバとを有する通信システムであって、
前記無線端末は、前記第１アクセスを実行中に前記第２無線基地局を識別する基地局識別子を含む無線信号を検知した場合、前記基地局識別子を前記第１認証サーバに通知し、
前記第１認証サーバは、
前記無線端末が前記通信ネットワークへのアクセスに利用できる無線基地局である利用可能基地局を識別する利用可能基地局識別子を前記第２認証サーバから取得して予め記憶する記憶部と、
前記無線端末から通知された前記基地局識別子と前記記憶部が記憶する前記利用可能基地局識別子とが合致する場合に前記第２認証サーバを特定し、前記無線端末による前記第２アクセスの認証を要求する認証要求を前記第２認証サーバに送信する要求送信部と、
前記第２認証サーバが前記認証要求に応じて前記無線端末による前記第２アクセスを許可した場合、前記第２アクセスが許可された旨の許可通知を前記第１無線基地局を介して前記無線端末に送信する通知送信部と
を備え、
前記無線端末は、前記許可通知を受信した場合、前記第２無線基地局への前記ハンドオ

ーバを実行するとともに前記第２アクセスを開始する通信システム。
【請求項２】
前記第２認証サーバは、前記認証要求を前記第１認証サーバから受信し、かつ前記無線端末による前記第２アクセスを許可する場合に、前記無線端末と前記第２無線基地局との無線通信における暗号化および復号化に用いられる鍵情報を前記第１認証サーバおよび前記第２無線基地局に送信し、
前記第１認証サーバは、前記鍵情報を前記第２認証サーバから受信した場合、前記許可通知および前記鍵情報を前記第１無線基地局を介して前記無線端末に送信し、
前記無線端末および前記第２無線基地局は、前記鍵情報を用いて前記暗号化および前記復号化を行う請求項１に記載の通信システム。
【請求項３】
前記無線端末は、前記無線端末と前記第１無線基地局との無線通信における通信品質が所定の閾値よりも劣化し、かつ前記基地局識別子を含む前記無線信号を検知した場合に、前記基地局識別子を前記第１認証サーバに通知する請求項１または２に記載の通信システム。
【請求項４】
前記記憶部は、前記利用可能基地局が追加または削除された場合、追加または削除後の前記利用可能基地局を識別する前記利用可能基地局識別子を改めて記憶する請求項１～３のいずれか一項に記載の通信システム。
【請求項５】
前記第１無線基地局は、所定の通信事業者によって提供される第１無線通信システムに含まれ、
前記第２無線基地局は、前記所定の通信事業者と異なる通信事業者によって提供される第２無線通信システムに含まれる請求項１～４のいずれか一項に記載の通信システム。
【請求項６】
前記第１無線通信システムは、所定の無線通信方式に準拠して構成され、
前記第２無線通信システムは、前記所定の無線通信方式と異なる無線通信方式に準拠して構成される請求項５に記載の通信システム。
【請求項７】
前記第２認証サーバは、前記認証要求に応じて前記無線端末の通信相手装置と通信ができるか否かを確認する請求項１に記載の通信システム。
【請求項８】
第１無線基地局を介した通信ネットワークへの第１アクセスの認証を行う認証サーバであって、
前記第１無線基地局からのハンドオーバを実行する無線端末が前記通信ネットワークへのアクセスに利用できる無線基地局である利用可能基地局を識別する利用可能基地局識別子を前記第２認証サーバから取得して予め記憶する記憶部と、
前記無線端末からハンドオーバ先の候補として通知された第２無線基地局を識別する基地局識別子と、前記記憶部が記憶する前記利用可能基地局識別子とが合致する場合に前記第２認証サーバを特定し、前記第２無線基地局を介した前記通信ネットワークへの第２アクセスの認証を要求する認証要求を、前記第２無線基地局を管理する他の認証サーバに送信する要求送信部と、
前記他の認証サーバが前記認証要求に応じて前記無線端末による前記第２アクセスを許可した場合、前記第２アクセスが許可された旨の許可通知を前記第１無線基地局を介して前記無線端末に送信する通知送信部と
を備える認証サーバ。
【請求項９】
第１無線基地局から第２無線基地局へのハンドオーバを実行する無線端末と、前記第１無線基地局を介した通信ネットワークへの第１アクセスの認証を行う第１認証サーバと、前記第２無線基地局を介した前記通信ネットワークへの第２アクセスの認証を行う第２認

証サーバとを用いた通信方法であって、
前記無線端末が前記通信ネットワークへのアクセスに利用できる無線基地局である利用可能基地局を識別する利用可能基地局識別子を前記第２認証サーバから取得して前記第１認証サーバが予め記憶するステップと、
前記無線端末が、前記第１アクセスを実行中に前記第２無線基地局を識別する基地局識別子を含む無線信号を検知した場合、前記基地局識別子を前記第１認証サーバに通知するステップと、
前記通知するステップにおいて通知された前記基地局識別子と、前記記憶するステップにおいて記憶した前記利用可能基地局識別子とが合致する場合に前記第２認証サーバを特定し、前記無線端末による前記第２アクセスの認証を要求する認証要求を、前記第１認証サーバから前記第２認証サーバに送信するステップと、
前記第２認証サーバが前記認証要求に応じて前記無線端末による前記第２アクセスを許可した場合、前記第２アクセスが許可された旨の許可通知を前記第１認証サーバから前記第１無線基地局を介して前記無線端末に送信するステップと、
前記無線端末が、前記許可通知を受信した場合、前記第２無線基地局への前記ハンドオーバを実行するとともに前記第２アクセスを開始するステップと
を備える通信方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、無線基地局を介した通信ネットワークへのアクセスの認証を行う通信システム、認証サーバおよび通信方法に関する。
【背景技術】
【０００２】
一般的に、無線端末が無線基地局を介してインターネットなどの通信ネットワークへアクセスする通信システムにおいては、当該無線端末による通信ネットワークへのアクセスの認証を行う認証サーバが設けられる。認証サーバによって通信ネットワークへのアクセスが許可されると、無線端末は、当該通信ネットワークへのアクセスが可能となる。
【０００３】
このような通信システムでは、認証サーバは、無線基地局、または無線基地局を含む無線通信システム全体について認証を管理しており、以下においては、１つの認証サーバによって認証が管理される対象（無線基地局または無線通信システム）を適宜「管理ドメイン」と称する。
【０００４】
無線端末は、通信ネットワークへのアクセスを実行中において、より条件の良い無線基地局へ接続先を切り替えるハンドオーバを実行する。ハンドオーバは、同一管理ドメイン内で実行される場合に限らず、異なる管理ドメイン間で実行されることがある。
【０００５】
異なる管理ドメイン間で無線端末がハンドオーバを実行する場合、ハンドオーバ先の管理ドメインにおいて当該管理ドメインに対応する認証サーバとの認証処理が必要になる。具体的には、無線端末は、ハンドオーバ先の管理ドメインに接続した後、当該管理ドメインに対応する認証サーバと認証処理を行い、当該認証サーバによって通信ネットワークへのアクセスが許可されると、当該通信ネットワークへのアクセスを開始することができる（例えば、特許文献１参照）。
【特許文献１】特許第４０００９３３号明細書（第１図、[００１３]-[００１４]段落）
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかしながら、異なる管理ドメイン間で実行されるハンドオーバには、次のような問題がある。具体的には、ある管理ドメインから別の管理ドメインへのハンドオーバを実行す

る無線端末は、必ずしもハンドオーバ先の管理ドメインにおいて通信ネットワークへのアクセスが許可されるとは限らない。すなわち、ハンドオーバ先の管理ドメインが無線端末による通信ネットワークへのアクセスに利用できないものである場合、無線端末は、ハンドオーバ先の管理ドメインにおいて通信ネットワークへのアクセスが拒否され、通信ネットワークへアクセスできない問題があった。

【０００７】

また、異なる管理ドメイン間でハンドオーバを実行する無線端末は、ハンドオーバ先の管理ドメインに接続した後、当該管理ドメインに対応する認証サーバによって通信ネットワークへのアクセスが許可されるまでの間においては、通信ネットワークへのアクセスを開始できない。このため、異なる管理ドメイン間で実行されるハンドオーバにおいては、無線端末がハンドオーバ先の管理ドメインに接続してから通信ネットワークへのアクセスを開始可能となるまでに長時間を要する問題があった。

【０００８】

そこで、本発明は、異なる管理ドメイン間で無線端末がハンドオーバを実行する場合であっても、ハンドオーバ先の管理ドメインにおいて通信ネットワークへのアクセスが継続されることを保証でき、かつ、無線端末が通信ネットワークへのアクセスを即座に開始できる通信システム、認証サーバおよび通信方法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】

上述した課題を解決するために、本発明は以下のような特徴を有している。まず、本発明に係る通信システムの第１の特徴は、第１無線基地局（EV-DO基地局１Ａ）から第２無線基地局（W-LAN基地局２Ａ）へのハンドオーバを実行する無線端末（無線端末１００）と、前記第１無線基地局を介した通信ネットワーク（インターネット３）への第１アクセスの認証を行う第１認証サーバ（EV-DO認証サーバ２００）と、前記第２無線基地局を介した前記通信ネットワークへの第２アクセスの認証を行う第２認証サーバ（W-LAN認証サーバ３００）とを有する通信システム（通信システム１０）であって、前記無線端末は、前記第１アクセスを実行中に前記第２無線基地局を識別する基地局識別子を含む無線信号を検知した場合、前記基地局識別子を前記第１認証サーバに通知し、前記第１認証サーバは、前記無線端末が前記通信ネットワークへのアクセスに利用できる無線基地局である利用可能基地局を識別する利用可能基地局識別子を予め記憶する記憶部（信頼ドメイン情報記憶部２２２）と、前記無線端末から通知された前記基地局識別子と前記記憶部が記憶する前記利用可能基地局識別子とが合致する場合、前記無線端末による前記第２アクセスの認証を要求する認証要求を前記第２認証サーバに送信する要求送信部（有線通信部２１１）と、前記第２認証サーバが前記認証要求に応じて前記無線端末による前記第２アクセスを許可した場合、前記第２アクセスが許可された旨の許可通知を前記第１無線基地局を介して前記無線端末に送信する通知送信部（有線通信部２１１）とを備え、前記無線端末は、前記許可通知を受信した場合、前記第２無線基地局への前記ハンドオーバを実行するとともに前記第２アクセスを開始することを要旨とする。

【００１０】

このような通信システムによれば、第１認証サーバは、無線端末が第１無線基地局を介して第１アクセスを実行中において、認証要求を事前（無線端末がハンドオーバを実行する前）に第２認証サーバに送信し、認証要求が許可された場合、第２認証サーバから第２アクセスが許可された旨の許可通知を無線端末に送信する。

【００１１】

そして、無線端末は、許可通知を受信した場合、第２無線基地局へのハンドオーバを実行するとともに第２アクセスを開始する。つまり、無線端末がハンドオーバを実行する時点で第２認証サーバから既に第２アクセスの許可が得られているため、無線端末は、第２アクセスを即座に開始できる。

【００１２】

また、第１認証サーバは、第２無線基地局が通信ネットワークへの第２アクセスに利用

できることを確認した上で認証要求を第２認証サーバに送信するため、ハンドオーバ先（第２無線基地局）において通信ネットワークへの第２アクセスが継続されることを保証できる。

【００１３】

したがって、上記の特徴に係る通信システムによれば、異なる認証サーバによって管理される無線基地局間、すなわち異なる管理ドメイン間で無線端末がハンドオーバを実行する場合でも、ハンドオーバ先の管理ドメイン（第２無線基地局）において通信ネットワークへの第２アクセスが継続されることを保証でき、かつ、無線端末が通信ネットワークへの第２アクセスを即座に開始できる。

【００１４】

本発明に係る通信システムの第２の特徴は、本発明に係る通信システムの第１の特徴に係り、前記第２認証サーバは、前記認証要求を前記第１認証サーバから受信し、かつ前記無線端末による前記第２アクセスを許可する場合に、前記無線端末と前記第２無線基地局との無線通信における暗号化および復号化に用いられる鍵情報を前記第１認証サーバおよび前記第２無線基地局に送信し、前記第１認証サーバは、前記鍵情報を前記第２認証サーバから受信した場合、前記許可通知および前記鍵情報を前記第１無線基地局を介して前記無線端末に送信し、前記無線端末および前記第２無線基地局は、前記鍵情報を用いて前記暗号化および前記復号化を行うことを要旨とする。

【００１５】

本発明に係る通信システムの第３の特徴は、本発明に係る通信システムの第１または第２の特徴に係り、前記無線端末は、前記無線端末と前記第１無線基地局との無線通信における通信品質が所定の閾値よりも劣化し、かつ前記基地局識別子を含む前記無線信号を検知した場合に、前記基地局識別子を前記第１認証サーバに通知することを要旨とする。

【００１６】

本発明に係る通信システムの第４の特徴は、本発明に係る通信システムの第１～第３のいずれか一つの特徴に係り、前記記憶部は、前記利用可能基地局が追加または削除された場合、追加または削除後の前記利用可能基地局を識別する前記利用可能基地局識別子を改めて記憶することを要旨とする。

【００１７】

本発明に係る通信システムの第５の特徴は、本発明に係る通信システムの第１～第４のいずれか一つの特徴に係り、前記第１無線基地局は、所定の通信事業者によって提供される第１無線通信システム（EV-DOシステム１）に含まれ、前記第２無線基地局は、前記所定の通信事業者と異なる通信事業者によって提供される第２無線通信システム（W-LAN認証サーバ３００）に含まれることを要旨とする。

【００１８】

本発明に係る通信システムの第６の特徴は、本発明に係る通信システムの第５の特徴に係り、前記第１無線通信システムは、所定の無線通信方式に準拠して構成され、前記第２無線通信システムは、前記所定の無線通信方式と異なる無線通信方式に準拠して構成されることを要旨とする。

【００１９】

本発明に係る認証サーバの特徴は、第１無線基地局（EV-DO基地局１Ａ）を介した通信ネットワーク（インターネット３）への第１アクセスの認証を行う認証サーバ（EV-DO認証サーバ２００）であって、前記第１無線基地局からのハンドオーバを実行する無線端末（無線端末１００）が前記通信ネットワークへのアクセスに利用できる無線基地局である利用可能基地局を識別する利用可能基地局識別子を予め記憶する記憶部（信頼ドメイン情報記憶部２２２）と、前記無線端末からハンドオーバ先の候補として通知された第２無線基地局（W-LAN基地局２Ａ）を識別する基地局識別子と、前記記憶部が記憶する前記利用可能基地局識別子とが合致する場合、前記第２無線基地局を介した前記通信ネットワークへの第２アクセスの認証を要求する認証要求を、前記第２無線基地局を管理する他の認証サーバ（W-LAN認証サーバ３００）に送信する要求送信部（有線通信部２１１）と、前記

他の認証サーバが前記認証要求に応じて前記無線端末による前記第２アクセスを許可した場合、前記第２アクセスが許可された旨の許可通知を前記第１無線基地局を介して前記無線端末に送信する通知送信部（有線通信部２１１）とを備えることを要旨とする。

【００２０】

本発明に係る通信方法の特徴は、第１無線基地局から第２無線基地局へのハンドオーバを実行する無線端末と、前記第１無線基地局を介した通信ネットワークへの第１アクセスの認証を行う第１認証サーバと、前記第２無線基地局を介した前記通信ネットワークへの第２アクセスの認証を行う第２認証サーバとを用いた通信方法であって、前記無線端末が前記通信ネットワークへのアクセスに利用できる無線基地局である利用可能基地局を識別する利用可能基地局識別子を前記第１認証サーバが予め記憶するステップ（ステップＳ１０２ａ）と、前記無線端末が、前記第１アクセスを実行中に前記第２無線基地局を識別する基地局識別子を含む無線信号を検知した場合、前記基地局識別子を前記第１認証サーバに通知するステップ（ステップＳ１０９）と、前記通知するステップにおいて通知された前記基地局識別子と、前記記憶するステップにおいて記憶した前記利用可能基地局識別子とが合致する場合、前記無線端末による前記第２アクセスの認証を要求する認証要求を、前記第１認証サーバから前記第２認証サーバに送信するステップ（ステップＳ１１３）と、前記第２認証サーバが前記認証要求に応じて前記無線端末による前記第２アクセスを許可した場合、前記第２アクセスが許可された旨の許可通知を前記第１認証サーバから前記第１無線基地局を介して前記無線端末に送信するステップ（ステップＳ１１９，Ｓ１２０）と、前記無線端末が、前記許可通知を受信した場合、前記第２無線基地局への前記ハンドオーバを実行するとともに前記第２アクセスを開始するステップ（ステップＳ１２４，Ｓ１２５）とを備えることを要旨とする。

【発明の効果】

【００２１】

本発明によれば、異なる管理ドメイン間で無線端末がハンドオーバを実行する場合であっても、ハンドオーバ先の管理ドメインにおいて通信ネットワークへのアクセスが継続されることを保証でき、かつ、無線端末が通信ネットワークへのアクセスを即座に開始できる通信システム、認証サーバおよび通信方法を提供できる。

【発明を実施するための最良の形態】

【００２２】

次に、図面を参照して、本発明の実施形態に係る通信システムについて説明する。具体的には、（１）通信システムの概略構成、（２）通信システムの詳細構成、（３）通信システムの動作、（４）作用・効果、（５）その他の実施形態について説明する。以下の実施形態における図面の記載において、同一又は類似の部分には同一又は類似の符号を付している。

【００２３】

（１）通信システムの概略構成

図１は、本実施形態に係る通信システム１０の全体構成図である。

【００２４】

本実施形態において無線端末１００は、無線通信方式（物理層およびリンク層の構成）が異なる複数の無線通信システムに接続可能な構成を有する。無線端末１００は、無線端末１００のユーザの移動に伴い、cdma2000 1x-EVDO（以下、「EV-DO」）に準拠したEV-DOシステム１から、IEEE802.11などの無線ローカルエリアネットワーク（以下、「W-LAN」）方式に準拠したW-LANシステム２へのハンドオーバを実行する。

【００２５】

EV-DOシステム１は、CDMA方式を採用した第３世代携帯電話システムであり、ＩＰパケット通信を実行可能である。EV-DOシステム１は、EV-DO基地局１Ａ（第１無線基地局）と、バックボーンネットワーク１Ｂとを有する。

【００２６】

EV-DO基地局１Ａは、EV-DOに準拠して構成され、無線端末１００と無線通信を実行する

。図１ではEV-DO基地局１Ａを１つのみ図示しているが、実際には多数のEV-DO基地局１Ａが設けられている。EV-DO基地局１Ａは、EV-DO基地局１Ａを識別する基地局識別子（具体的には、ＢＳＩＤ）を含む報知信号（無線信号）を所定周期で送信する。

【００２７】

バックボーンネットワーク１Ｂは、ＩＰルータなどによって構成される有線通信網であり、インターネット３（通信ネットワーク）に有線接続される。バックボーンネットワーク１Ｂには、EV-DO基地局１Ａを介したインターネット３へのアクセス（以下、適宜「第１アクセス」と称する）の認証を行うEV-DO認証サーバ２００（第１認証サーバ）が接続される。EV-DO認証サーバ２００は、例えばRADIUSサーバとして構成される。

【００２８】

W-LANシステム２は、EV-DOシステム１と同様にＩＰパケット通信を実行可能であり、EV-DOよりも高速な無線通信を無線端末１００と実行可能である。W-LANシステム２は、W-LAN基地局２Ａ（第２無線基地局）と、バックボーンネットワーク２Ｂとを有する。図１ではW-LAN基地局２Ａを１つのみ図示しているが、実際には多数のW-LAN基地局２Ａが設けられている。W-LAN基地局２Ａは、W-LAN基地局２Ａを識別する基地局識別子（具体的には、ＭＡＣアドレス）を含むビーコン信号（無線信号）を所定周期で送信する。

【００２９】

バックボーンネットワーク２Ｂは、ＩＰルータなどによって構成される有線通信網であり、インターネット３に有線接続される。バックボーンネットワーク２Ｂには、W-LAN基地局２Ａを介したインターネット３へのアクセス（以下、適宜「第２アクセス」と称する）の認証を行うW-LAN認証サーバ３００（第２認証サーバ）が接続される。W-LAN認証サーバ３００は、例えば、EV-DO認証サーバ２００と同様にRADIUSサーバとして構成される。

【００３０】

インターネット３には、無線端末１００の通信相手(Corresponding Node)である通信相手装置４００が接続されている。通信相手装置４００は、インターネット３を介して、ＩＰパケットを無線端末１００と送受信する。

【００３１】

EV-DOシステム１およびW-LANシステム２は、異なる通信事業者によって提供される。具体的には、当該通信事業者は、無線端末１００によるインターネット３へのアクセスを可能とするインターネット接続サービスを提供するＩＳＰ（Internet Service Provider）である。

【００３２】

本実施形態では、EV-DOシステム１およびW-LANシステム２は、相互に利用可能である。すなわち、EV-DOシステム１を提供する通信事業者と契約した無線端末（ユーザ）はW-LANシステム２を利用してインターネット３へアクセス可能である。W-LANシステム２を提供する通信事業者と契約した無線端末（ユーザ）はEV-DOシステム１を利用してインターネット３へアクセス可能である。

【００３３】

また、無線端末１００とEV-DO認証サーバ２００との通信や、EV-DO認証サーバ２００とW-LAN認証サーバ３００との通信は、IPSecによるセキュリティの高いＩＰ通信であるものとする。

【００３４】

本実施形態では、無線端末１００が、EV-DOシステム１を用いて通信相手装置４００とＩＰパケットを送受信しており、EV-DO基地局１Ａについて所望の通信品質（ＲＳＳＩまたはＳＮＲなど）を確保できず、EV-DO基地局１AからW-LAN基地局２Ａへのハンドオーバを実行する一例について説明している。

【００３５】

無線端末１００は、EV-DO基地局１AからW-LAN基地局２Ａへのハンドオーバの際、W-LAN基地局２Ａに接続する。具体的には、無線端末１００は、W-LAN基地局２Ａと無線リンクを確立し、EV-DO基地局１Ａとの無線リンクを切断することによって、リンク層（レイヤ

２）レベルのハンドオーバ（以下、リンク層ハンドオーバ）を実行する。リンク層ハンドオーバが完了すると、無線端末１００は、W-LANシステム２から新たなＩＰアドレスを取得することによって、ＩＰ層（レイヤ３）レベルのハンドオーバ（以下、ＩＰ層ハンドオーバ）を実行する。なお、EV-DOシステム１からW-LANシステム２へのハンドオーバをＩＰパケット通信が切断されることなく継続可能とするために、通信システム１０には、モバイルＩＰなどのＩＰモビリティプロトコルが採用されていてもよい。

【００３６】

（２）通信システムの詳細構成

次に、通信システム１０の詳細構成について、（２．１）無線端末の構成、（２．２）EV-DO認証サーバの構成、（２．３）W-LAN認証サーバの構成の順に説明する。

【００３７】

（２．１）無線端末の構成

図２は、無線端末１００の構成を示すブロック図である。

【００３８】

図２に示すように、無線端末１００は、少なくとも物理層の方式が異なるEV-DOシステム１およびW-LANシステム２に接続して無線通信を実行するために、異なる２つの無線通信部、具体的には、EV-DO無線通信部１１１およびW-LAN無線通信部１１２を備える。EV-DO無線通信部１１１およびW-LAN無線通信部１１２のそれぞれは、ＬＮＡ(Low Noise Amplifier)、パワーアンプ、アップコンバータおよびダウンコンバータなどを含み、無線信号の送受信を行う。

【００３９】

無線端末１００は、制御部１１０、記憶部１６０、スピーカ１７１、マイクロフォン１７２、表示部１７３、および操作部１７４をさらに含む。

【００４０】

制御部１１０は、例えばＣＰＵによって構成され、無線端末１００が具備する各種機能を制御する。例えば制御部１１０は、W-LANシステム２およびEV-DOシステム１の物理層の構成に依存しないメディア非依存ハンドオーバを実現するプロトコル、すなわちIEEE802.21に準拠したプロトコルスタックを有し、EV-DO基地局１ＡとW-LAN基地局２Ａとの間で実行するハンドオーバを制御する。

【００４１】

制御部１１０は、EV-DO無線通信部１１１およびW-LAN無線通信部１１２がEV-DO基地局１ＡおよびW-LAN基地局２Ａから受信する無線信号の品質（ＲＳＳＩやＳＮＲなど）を監視する。制御部１１０は、通常、EV-DO無線通信部１１１がEV-DO基地局１Ａと無線通信を実行中において、消費電力削減のためにW-LAN無線通信部１１２の動作を停止させている。そして、制御部１１０は、EV-DO無線通信部１１１がEV-DO基地局１Ａから受信する無線信号の品質が所定の閾値よりも劣化した場合、制御部１１０は、W-LAN無線通信部１１２の動作を開始させ、W-LAN基地局２Ａからのビーコン信号を捕捉させる。さらに制御部１１０は、W-LAN無線通信部１１２がW-LAN基地局２Ａからのビーコン信号を検知すると、当該ビーコン信号に含まれるＭＡＣアドレスを抽出し、EV-DO無線通信部１１１を用いて当該ＭＡＣアドレスをEV-DO認証サーバ２００に通知する。

【００４２】

記憶部１６０は、例えばメモリによって構成され、無線端末１００における制御などに用いられる各種情報を記憶する。マイクロフォン１７２は、音声を集音し、集音された音声に基づく音声データを音声コーデック（不図示）経由で制御部１１０に入力する。スピーカ１７１は、音声コーデック（不図示）経由で制御部１１０から取得した音声データに基づいて音声を出力する。表示部１７３は、制御部１１０を介して受信した画像を表示したり、操作内容（入力電話番号やアドレスなど）を表示したりする。操作部１７４は、テンキーやファンクションキーなどによって構成され、ユーザの操作内容を入力するために用いられる。

【００４３】

（２．２）EV-DO認証サーバの構成

図３は、EV-DO認証サーバ２００の構成を示すブロック図である。

【００４４】

図３に示すように、EV-DO認証サーバ２００は、有線通信部２１１、制御部２１０、管理ドメイン情報記憶部２２１、信頼ドメイン情報記憶部２２２、およびユーザ情報記憶部２２３を有する。

【００４５】

有線通信部２１１は、EV-DOシステム１を構成するバックボーンネットワーク１Ｂに接続され、バックボーンネットワーク１Ｂを介してEV-DO基地局１Ａと有線通信を実行する。また、有線通信部２１１は、バックボーンネットワーク１Ｂおよびインターネット３を介して、W-LAN認証サーバ３００および通信相手装置４００と有線通信を実行可能である。

【００４６】

管理ドメイン情報記憶部２２１は、EV-DO基地局１ＡのＢＳＩＤとＩＰアドレスとを対応付けた管理ドメイン情報を記憶する。信頼ドメイン情報記憶部２２２は、信頼できるドメインの情報として、W-LANシステム２に関する情報を記憶する。具体例としては、信頼ドメイン情報記憶部２２２は、W-LAN基地局２ＡのＭＡＣアドレスと、W-LANシステム２を提供する通信事業者の情報と、W-LAN認証サーバ３００のＩＰアドレスとを対応付けた信頼ドメイン情報を記憶する。すなわち、本実施形態において信頼ドメイン情報記憶部２２２は、無線端末１００がインターネット３への第２アクセスに利用できる無線基地局である利用可能基地局（W-LAN基地局２Ａ）を識別する利用可能基地局識別子（ＭＡＣアドレス）を予め記憶する記憶部を構成する。ユーザ情報記憶部２２３は、EV-DOシステム１を利用可能なユーザを識別するユーザ識別子を含むユーザ情報を記憶する。

【００４７】

制御部２１０は、例えばＣＰＵによって構成され、EV-DO認証サーバ２００が具備する各種機能を制御する。例えば、制御部２１０は、無線端末１００から有線通信部２１１を介して通知されたW-LAN基地局２Ａの基地局識別子（ＭＡＣアドレス）と、信頼ドメイン情報記憶部２２２が記憶する利用可能基地局識別子とが合致するか否かを判定する。合致すると判定された場合、有線通信部２１１は、無線端末１００による第２アクセスの認証を要求する認証要求をW-LAN認証サーバ３００に送信する。W-LAN認証サーバ３００が認証要求に応じて第２アクセスを許可した場合、第２アクセスが許可された旨の許可通知をEV-DO基地局１Ａを介して無線端末１００に送信する。すなわち有線通信部２１１は、認証要求を送信する要求送信部、および許可通知を送信する通知送信部として機能する。

【００４８】

（２．３）W-LAN認証サーバの構成

図４は、W-LAN認証サーバ３００の構成を示すブロック図である。W-LAN認証サーバ３００はEV-DO認証サーバ２００と同様の構成であるため、EV-DO認証サーバ２００と異なる点についてのみ説明する。

【００４９】

図４に示すように、W-LAN認証サーバ３００は、有線通信部３１１、制御部３１０、管理ドメイン情報記憶部３２１、信頼ドメイン情報記憶部３２２、およびユーザ情報記憶部３２３を有する。

【００５０】

有線通信部３１１は、W-LANシステム２を構成するバックボーンネットワーク２Ｂに接続され、バックボーンネットワーク２Ｂを介してW-LAN基地局２Ａと有線通信を実行する。また、有線通信部３１１は、バックボーンネットワーク２Ｂおよびインターネット３を介して、EV-DO認証サーバ２００と有線通信を実行する。

【００５１】

管理ドメイン情報記憶部３２１は、W-LAN基地局２ＡのＭＡＣアドレスとＩＰアドレスとを対応付けた管理ドメイン情報を記憶する。信頼ドメイン情報記憶部３２２は、信頼で

きるドメインの情報として、EV-DOシステム１に関する情報を記憶する。具体的には、信頼ドメイン情報記憶部３２２は、EV-DO基地局１ＡのＢＳＩＤと、EV-DOシステム１を提供する通信事業者の情報と、EV-DO認証サーバ２００のＩＰアドレスとを対応付けた信頼ドメイン情報を記憶する。ユーザ情報記憶部３２３は、W-LANシステム２を利用可能なユーザを識別するユーザ識別子を含むユーザ情報を記憶する。

【００５２】

制御部３１０は、例えばＣＰＵによって構成され、W-LAN認証サーバ３００が具備する各種機能を制御する。制御部３１０は、有線通信部３１１が無線端末１００による認証要求をEV-DO認証サーバ２００から受信した場合、ユーザ情報記憶部３２３を参照して、無線端末１００による第２アクセスを許可するか否かを判定する。制御部３１０は、無線端末１００による第２アクセスを許可すると判定した場合、有線通信部３１１を用いて、無線端末１００とW-LAN基地局２Ａとの無線通信における暗号化および復号化に用いられる鍵情報（具体的には、ＷＥＰ鍵）をEV-DO認証サーバ２００およびW-LAN基地局２Ａに送信する。ここでＷＥＰ鍵は、無線端末１００とW-LAN基地局２Ａとの無線通信に用いられる共有鍵である。

【００５３】

（３）通信システムの動作

次に、通信システム１０の動作について、（３．１）基地局識別子の登録動作、（３．２）基地局識別子の交換動作、（３．３）ハンドオーバ動作の順に説明する。

【００５４】

（３．１）基地局識別子の登録動作

図５は、EV-DO基地局１ＡおよびW-LAN基地局２Ａのそれぞれの基地局識別子を登録する登録動作を示すシーケンス図である。

【００５５】

ステップＳ１１ａにおいて、EV-DO基地局１Ａは、EV-DO基地局１Ａの設置時やサービス開始時などにおいて、EV-DO基地局１Ａの基地局識別子（ＢＳＩＤ）をEV-DO認証サーバ２００に通知する。

【００５６】

通知先となるEV-DO認証サーバ２００のＩＰアドレスは、通信事業者がEV-DO基地局１Ａを設置するときに予めEV-DO基地局１Ａに設定しておく。あるいは、EV-DO認証サーバ２００がブロードキャストメッセージでEV-DO認証サーバ２００のＩＰアドレスを定期的に報知することで、EV-DO基地局１AがEV-DO認証サーバ２００のＩＰアドレスを把握することができる。

【００５７】

ステップＳ１１ｂにおいて、W-LAN基地局２Ａは、W-LAN基地局２Ａの設置時やサービス開始時などにおいて、W-LAN基地局２Ａの基地局識別子（ＭＡＣアドレス）をW-LAN認証サーバ３００に通知する。通知先となるW-LAN認証サーバ３００のＩＰアドレスは、通信事業者がW-LAN基地局２Ａを設置するときに予めW-LAN基地局２Ａに設定しておく。あるいは、W-LAN認証サーバ３００がブロードキャストメッセージでW-LAN認証サーバ３００のＩＰアドレスを定期的に報知することで、W-LAN基地局２AがW-LAN認証サーバ３００のＩＰアドレスを把握することができる。

【００５８】

ステップＳ１２ａにおいて、EV-DO認証サーバ２００の制御部２１０は、有線通信部２１１を介して通知されたEV-DO基地局１Ａの基地局識別子（ＢＳＩＤ）を管理ドメイン情報記憶部２２１に格納することにより管理ドメイン情報を更新する。ステップＳ１２ｂにおいて、W-LAN認証サーバ３００の制御部３１０は、有線通信部３１１を介して通知されたW-LAN基地局２Ａの基地局識別子（ＭＡＣアドレス）を管理ドメイン情報記憶部３２１に格納することにより管理ドメイン情報を更新する。このようにして、EV-DO認証サーバ２００の制御部２１０は管理ドメイン情報記憶部２２１におけるEV-DO基地局１Ａの基地局識別子（ＢＳＩＤ）を管理し、W-LAN認証サーバ３００の制御部３１０は管理ドメイン

情報記憶部３２１におけるW-LAN基地局２Ａの基地局識別子（ＭＡＣアドレス）を管理する。

【００５９】

（３．２）基地局識別子の交換動作

図６は、EV-DO認証サーバ２００およびW-LAN認証サーバ３００によって実行される基地局識別子交換動作を示すシーケンス図である。

【００６０】

ステップＳ１０１において、EV-DO認証サーバ２００およびW-LAN認証サーバ３００は、基地局識別子を交換する。具体的には、EV-DO認証サーバ２００の制御部２１０は、管理ドメイン情報記憶部２２１が記憶しているEV-DO基地局１Ａの基地局識別子（ＢＳＩＤ）を有線通信部２１１からW-LAN認証サーバ３００に通知する。W-LAN認証サーバ３００の制御部３１０は、管理ドメイン情報記憶部３２１が記憶しているW-LAN基地局２Ａの基地局識別子（ＭＡＣアドレス）を有線通信部３１１からEV-DO認証サーバ２００に通知する。

【００６１】

ステップＳ１０２ａにおいて、EV-DO認証サーバ２００の制御部２１０は、有線通信部２１１を介してW-LAN認証サーバ３００から通知された基地局識別子を信頼ドメイン情報（利用可能基地局識別子）として信頼ドメイン情報記憶部２２２に記憶させる。ステップＳ１０２ｂにおいて、W-LAN認証サーバ３００の制御部３１０は、有線通信部３１１を介してEV-DO認証サーバ２００から通知された基地局識別子を信頼ドメイン情報（利用可能基地局識別子）として信頼ドメイン情報記憶部３２２に記憶させる。

【００６２】

なお、EV-DO認証サーバ２００の管理ドメイン情報記憶部２２１が記憶するEV-DO基地局１Ａの基地局識別子（ＢＳＩＤ）が追加または削除された場合、EV-DO認証サーバ２００の制御部２１０は、追加または削除後のEV-DO基地局１Ａの基地局識別子（ＢＳＩＤ）を有線通信部２１１からW-LAN認証サーバ３００に通知する。W-LAN認証サーバ３００は、EV-DO認証サーバ２００から有線通信部３１１を介して通知された基地局識別子（ＢＳＩＤ）に応じて、信頼ドメイン情報記憶部３２２における信頼ドメイン情報を更新する。

【００６３】

同様に、W-LAN認証サーバ３００の管理ドメイン情報記憶部３２１が記憶するW-LAN基地局２Ａの基地局識別子（ＭＡＣアドレス）が追加または削除された場合、W-LAN認証サーバ３００の制御部３１０は、追加または削除後のW-LAN基地局２Ａの基地局識別子（ＭＡＣアドレス）を有線通信部３１１からEV-DO認証サーバ２００に通知する。EV-DO認証サーバ２００の制御部２１０は、W-LAN認証サーバ３００から有線通信部２１１を介して通知された基地局識別子（ＭＡＣアドレス）に応じて、信頼ドメイン情報記憶部２２２における信頼ドメイン情報を更新する。

【００６４】

このように、EV-DO認証サーバ２００およびW-LAN認証サーバ３００のそれぞれは、他のドメインを信頼する(ハンドオーバ先と設定しておく)ならば、管理する基地局識別子を交換して記憶する。また、EV-DO認証サーバ２００およびW-LAN認証サーバ３００のそれぞれは、管理する基地局識別子に変化が生じたときは、他方の認証サーバに通知して現状のシステム構成に合うようにする。

【００６５】

（３．３）ハンドオーバ動作

図７は、無線端末１００がハンドオーバを実行する場合における通信システム１０の動作を示すシーケンス図である。

【００６６】

ステップＳ１０３～Ｓ１０６において、無線端末１００の制御部１１０は、EV-DO無線通信部１１１を用いて、EV-DOシステム１に接続するとともに、EV-DOシステム１を介したインターネット３への第１アクセスを開始する。

【００６７】

ステップＳ１０３において、無線端末１００の制御部１１０、およびEV-DO基地局１Ａは、リンク層（Ｌ２）およびＩＰ層（Ｌ３）における認証処理を行う。ステップＳ１０４において、無線端末１００の制御部１１０は、ＤＨＣＰ（Dynamic Host Configuration Protocol）などを用いて、第１アクセスに用いられるＩＰアドレスをEV-DO無線通信部１１１を介して取得する。

【００６８】

ステップＳ１０５において、無線端末１００の制御部１１０およびEV-DO認証サーバ２００の制御部２１０は、無線端末１００のユーザの認証処理を行う。具体的には、無線端末１００の制御部１１０は、無線端末１００がサービスを受けているＩＳＰ名(または管理ドメイン名)と、無線端末１００のユーザ識別子をEV-DO無線通信部１１１からEV-DO認証サーバ２００に通知する。無線端末１００へのEV-DO認証サーバ２００のＩＰアドレスの通知方法は、予めEV-DO認証サーバ２００のＩＰアドレスを無線端末１００の記憶部１６０に設定しておくか、ＩＰアドレスを設定するときのDHCPACKメッセージ中のオプションなどで通知する方法が考えられる。ステップＳ１０６において、無線端末１００の制御部１１０は第１アクセスを開始する。

【００６９】

ステップＳ１０７において、無線端末１００の制御部１１０は、EV-DO無線通信部１１１が接続中のEV-DO基地局１Ａとの通信品質が低下したために、別の基地局にハンドオーバすると判断し、W-LAN基地局２Ａが送信するビーコン信号をW-LAN無線通信部１１２において検知したとする。ステップＳ１０８において、無線端末１００の制御部１１０およびW-LAN無線通信部１１２は、W-LAN基地局２Ａが送信するビーコン信号から、W-LAN基地局２Ａの基地局識別子（ＭＡＣアドレス）を抽出する。

【００７０】

ステップＳ１０９およびステップＳ１１０において、無線端末１００の制御部１１０は、ステップＳ１０８で得られたW-LAN基地局２Ａの基地局識別子（ＭＡＣアドレス）を、EV-DO無線通信部１１１からEV-DO基地局１Ａを介してEV-DO認証サーバ２００に通知する。その際、無線端末１００の制御部１１０は、W-LAN基地局２Ａの基地局識別子（ＭＡＣアドレス）とともに、通信相手装置４００のＩＰアドレスを通知してもよい。

【００７１】

ステップＳ１１１において、EV-DO認証サーバ２００の制御部２１０は、有線通信部２１１を介して通知されたW-LAN基地局２Ａの基地局識別子（ＭＡＣアドレス）と、信頼ドメイン情報記憶部２２２において保持している信頼ドメイン情報とを比較する。基地局識別子（ＭＡＣアドレス）が信頼ドメイン情報記憶部２２２において保持している信頼ドメイン情報の中にあった場合、ステップＳ１１２において制御部２１０は、その信頼ドメイン情報から、当該基地局識別子（ＭＡＣアドレス）に対応するW-LAN認証サーバ３００を特定する。

【００７２】

なお、EV-DO認証サーバ２００の制御部２１０は、基地局識別子（ＭＡＣアドレス）が信頼ドメイン情報の中にあった場合に、「信頼済み」である旨を有線通信部２１１から無線端末１００に通知し、信頼ドメイン情報の中に無い場合に、「信頼していない」旨を有線通信部２１１から無線端末１００に通知してもよい。無線端末１００の制御部１１０は、その返事を元にして、事前認証によるハンドオーバができるかを判断することができる。

【００７３】

ステップＳ１１３において、EV-DO認証サーバ２００の制御部２１０は、無線端末１００の事前認証を要求する認証要求（以下、適宜「事前認証要求」と称する）を有線通信部２１１からW-LAN認証サーバ３００に通知する。当該事前認証要求には、無線端末１００がサービスを受けているＩＳＰ名(または管理ドメイン名)と、無線端末１００のユーザのユーザ識別子と、W-LAN基地局２Ａの基地局識別子（ＭＡＣアドレス）とが含まれる。例えば、無線端末１００がサービスを受けているＩＳＰ名(または管理ドメイン名)と、無線

端末１００のユーザのユーザ識別子とは、「ユーザ識別子@ＩＳＰ」といった形式とすることができ、以下ではこの形式を例に説明する。これらの情報に加え、通信相手装置４００のＩＰアドレスが事前認証要求に含まれていてもよい。

【００７４】

ステップＳ１１４において、W-LAN認証サーバ３００の制御部３１０は、事前認証要求に含まれるユーザ識別子に基づいて、ユーザ登録がされているか否かをユーザ情報記憶部３２３を参照して確認する。ユーザとして登録している場合、ステップＳ１１５においてW-LAN認証サーバ３００の制御部３１０は、事前認証要求に含まれる基地局識別子（ＭＡＣアドレス）から管理ドメイン情報記憶部３２１を参照してW-LAN基地局２Ａを特定する。

【００７５】

なお、通信相手装置４００のＩＰアドレスが通知された場合、ステップＳ１１６においてW-LAN認証サーバ３００の制御部３１０は、pingなどを用いて、通信相手装置４００との通信ができるかを確かめる。通信できない場合、W-LAN認証サーバ３００の制御部３１０は、通信できないことを有線通信部３１１からEV-DO認証サーバ２００を介して無線端末１００に通知する。このような処理により、無線端末１００の制御部１１０は、ハンドオーバした後も通信相手装置４００との通信ができるか否かを確認可能となる。

【００７６】

ステップＳ１１７において、W-LAN認証サーバ３００の制御部３１０は、管理ドメイン情報記憶部３２１を参照し、W-LAN基地局２Ａの基地局識別子（ＭＡＣアドレス）に対応するＩＰアドレスに宛てて有線通信部３１１からＷＥＰ鍵を送信する。その際、W-LAN認証サーバ３００の制御部３１０は、ＷＥＰ鍵とともに、ユーザ識別子@ＩＳＰを有線通信部３１１から送信する。W-LAN基地局２Ａは、W-LAN認証サーバ３００からＷＥＰ鍵およびユーザ識別子@ＩＳＰを受信すると、受信したＷＥＰ鍵およびユーザ識別子@ＩＳＰを保持する。

【００７７】

ステップＳ１１８において、W-LAN認証サーバ３００は、ＷＥＰ鍵をEV-DO認証サーバ２００に送信する。ステップＳ１１９およびＳ１２０において、EV-DO認証サーバ２００は、当該ＷＥＰ鍵をEV-DO基地局１Ａを介して無線端末１００に送信する。その際、EV-DO認証サーバ２００は、事前認証に成功した旨の許可通知を無線端末１００に送信する。無線端末１００は、許可通知を受信すると、W-LAN基地局２Ａへのハンドオーバ手順を開始する。

【００７８】

ステップＳ１２１において、無線端末１００の制御部１１０は、W-LAN無線通信部１１２を用いてW-LAN基地局２Ａに接続し、ユーザ識別子@ＩＳＰをW-LAN無線通信部１１２からW-LAN基地局２Ａに通知する。W-LAN基地局２Ａは、ユーザ識別子@ＩＳＰに対応するＷＥＰ鍵を用いて、以後の無線端末１００との無線通信における暗号化および復号化を行う。同様に、無線端末１００の制御部１１０は、EV-DO認証サーバ２００からEV-DO無線通信部１１１を介して受信したＷＥＰ鍵を用いて、以後のW-LAN基地局２AとW-LAN無線通信部１１２との無線通信における暗号化および復号化を行う。

【００７９】

ステップＳ１２２において、無線端末１００の制御部１１０、およびW-LAN基地局２Ａは、リンク層（Ｌ２）およびＩＰ層（Ｌ３）における認証処理を行う。ステップＳ１２３において、無線端末１００の制御部１１０は、ＤＨＣＰまたはモバイルＩＰなどに従って、第２アクセスに用いられるＩＰアドレスをW-LAN無線通信部１１２を介して取得する。この結果、無線端末１００の制御部１１０は、ステップＳ１２４においてＩＰ層ハンドオーバを実行し、W-LAN基地局２Ａを介したインターネット３への第２アクセスを開始する。

【００８０】

（４）作用・効果

以上説明したように、EV-DO認証サーバ２００は、認証要求を事前（無線端末１００がリンク層ハンドオーバを実行する前）にW-LAN認証サーバ３００に送信し、事前の認証要求が許可された場合、W-LAN認証サーバ３００から第２アクセスが許可された旨の許可通知を無線端末１００に通知する。そして、無線端末１００は、許可通知を受信した場合、W-LAN基地局２Ａへのハンドオーバを実行するとともに、W-LAN基地局２Ａを介したインターネット３への第２アクセスを開始する。

【００８１】

つまり、無線端末１００がリンク層ハンドオーバを実行する時点（W-LANシステム２への接続前）において、W-LAN認証サーバ３００から既に第２アクセスの許可が得られているため、無線端末１００は、インターネット３への第２アクセスを即座に開始できる。

【００８２】

また、EV-DO認証サーバ２００は、W-LAN基地局２Ａがインターネット３への第２アクセスに利用できることを確認した上で事前認証要求をW-LAN認証サーバ３００に送信するため、ハンドオーバ先（W-LAN基地局２Ａ）においてインターネット３への第２アクセスが継続されることを保証できる。

【００８３】

本実施形態では、W-LAN認証サーバ３００は、事前認証要求をEV-DO認証サーバ２００から受信し、かつ無線端末１００によるインターネット３へのアクセスを許可する場合に、無線端末１００とW-LAN基地局２Ａとの無線通信における暗号化および復号化に用いられるＷＥＰ鍵をEV-DO認証サーバ２００およびW-LAN基地局２Ａに送信する。EV-DO認証サーバ２００は、ＷＥＰ鍵をW-LAN認証サーバ３００から受信した場合、許可通知およびＷＥＰ鍵をEV-DO基地局１Ａを介して無線端末１００に送信する。無線端末１００およびW-LAN基地局２Ａは、ＷＥＰ鍵を用いて暗号化および復号化を行う。

【００８４】

したがって、無線端末１００およびW-LAN基地局２Ａとの間の無線区間において暗号化を行う場合であっても、無線端末１００がリンク層ハンドオーバを実行する時点（W-LANシステム２への接続前）において、無線端末１００およびW-LAN基地局２Ａは、W-LAN認証サーバ３００から既にＷＥＰが得られているため、ハンドオーバの際に直ぐに暗号化されたパケット通信を実行可能となる。

【００８５】

本実施形態では、無線端末１００は、無線端末１００とEV-DO基地局１Ａとの無線通信における通信品質が所定の閾値よりも劣化し、かつ基地局識別子（ＭＡＣアドレス）を含むビーコン信号を検知した場合に、基地局識別子（ＭＡＣアドレス）をEV-DO認証サーバ２００に通知する。このため、無線端末１００がハンドオーバを行う必要が生じた際に事前認証手順を適切に開始することができる。

【００８６】

本実施形態では、EV-DO認証サーバ２００の信頼ドメイン情報記憶部２２２は、利用可能基地局が追加または削除された場合、追加または削除後の利用可能基地局を識別する利用可能基地局識別子（ＭＡＣアドレス）を改めて記憶する。すなわち、EV-DOシステム１を提供する通信事業者が許可したW-LAN基地局２Ａを迅速に登録することができる。

【００８７】

（５）その他の実施形態

上記のように、本発明は実施形態によって記載したが、この開示の一部をなす論述及び図面はこの発明を限定するものであると理解すべきではない。この開示から当業者には様々な代替実施形態、実施例及び運用技術が明らかとなる。

【００８８】

例えば、上述した実施形態では、無線端末１００がEV-DOシステム１からW-LANシステム２へのハンドオーバを実行する場合について説明したが、無線端末１００がW-LANシステム２からEV-DOシステム１へのハンドオーバを実行する場合であっても本発明を適用可能である。さらに、EV-DOシステム１とW-LANシステム２との間で実行されるハンドオーバに

限らず、異なる認証サーバによって管理される管理ドメイン間のハンドオーバであれば、同一無線通信方式の管理ドメイン間あるいは同一通信事業者の管理ドメイン間のハンドオーバでもよい。

【００８９】

このように本発明は、ここでは記載していない様々な実施形態等を包含するということを理解すべきである。したがって、本発明はこの開示から妥当な特許請求の範囲の発明特定事項によってのみ限定されるものである。

【図面の簡単な説明】

【００９０】

【図１】本発明の実施形態に係る通信システムの全体構成図である。

【図２】本発明の実施形態に係る無線端末の構成を示すブロック図である。

【図３】本発明の実施形態に係るEV-DO認証サーバの構成を示すブロック図である。

【図４】本発明の実施形態に係るW-LAN認証サーバの構成を示すブロック図である。

【図５】本発明の実施形態に係る基地局識別子登録動作を示すシーケンス図である。

【図６】本発明の実施形態に係る基地局識別子交換動作を示すシーケンス図である。

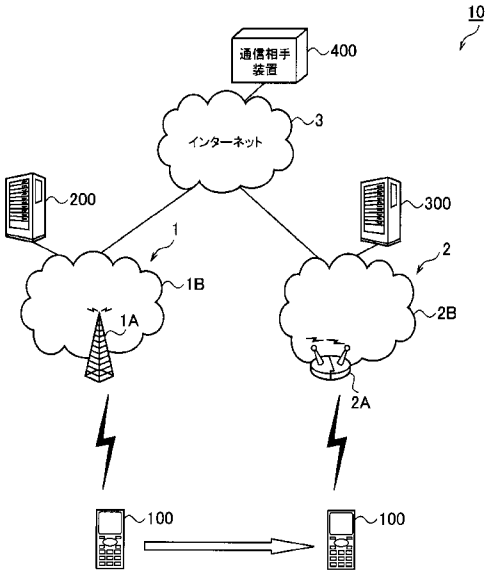
【図７】本発明の実施形態に係るハンドオーバ動作を示すシーケンス図である。

【符号の説明】

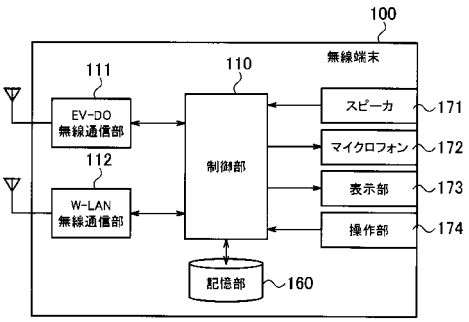
【００９１】

１…EV-DOシステム、１Ａ…EV-DO基地局、１Ｂ…バックボーンネットワーク、２…W-LANシステム、２Ａ…W-LAN基地局、２Ｂ…バックボーンネットワーク、３…インターネット、１０…通信システム、１００…無線端末、１１０…制御部、１１１…EV-DO無線通信部、１１２…W-LAN無線通信部、１６０…記憶部、１７１…スピーカ、１７２…マイクロフォン、１７３…表示部、１７４…操作部、２００…EV-DO認証サーバ、２１０…制御部、２１１…有線通信部、２２１…管理ドメイン情報記憶部、２２２…信頼ドメイン情報記憶部、２２３…ユーザ情報記憶部、３００…W-LAN認証サーバ、３１０…制御部、３１１…有線通信部、３２１…管理ドメイン情報記憶部、３２２…信頼ドメイン情報記憶部、３２３…ユーザ情報記憶部、４００…通信相手装置

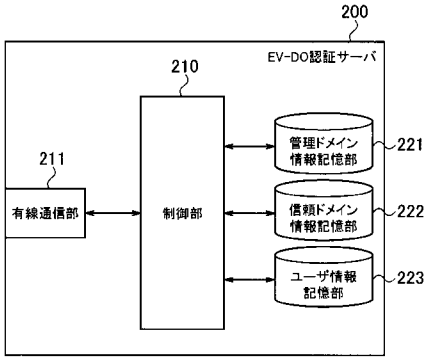
【図１】



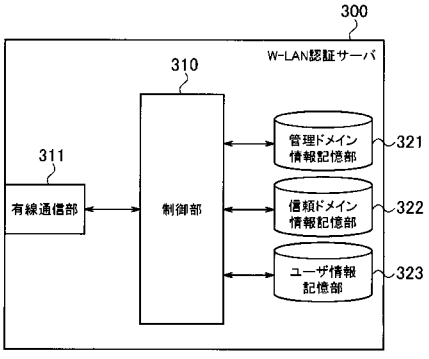
【図２】



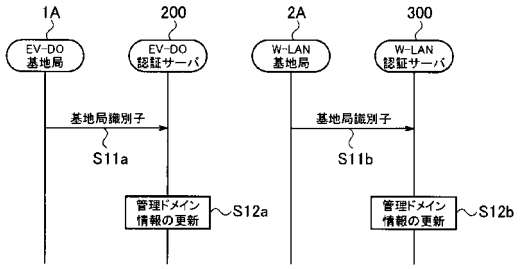
【図３】



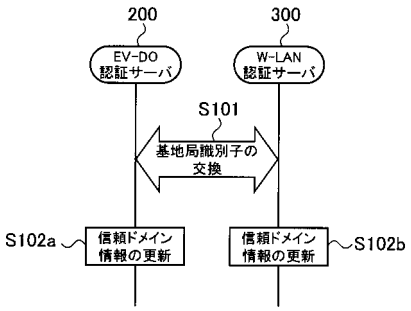
【図４】



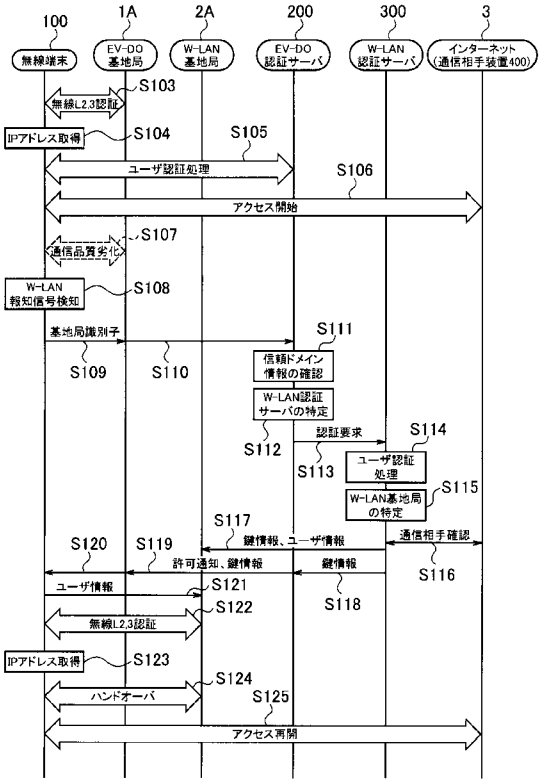
【図５】



【図６】



【図７】


100
1A
2A
200
300
3
無線端末
EV-DO 基地局
W-LAN 基地局
EV-DO 認証サーバ
W-LAN 認証サーバ
インターネット (通信相手装置400)
S103
無線L2,3認証
IPアドレス取得
S104
S105
ユーザ認証処理
S106
アクセス開始
S107
通信品質劣化
W-LAN 報知信号検知
S108
基地局識別子
S109
S110
S111
信頼ドメイン 情報の確認
W-LAN認証 サーバの特定
S112
認証要求
S113
S114
ユーザ認証 処理
S115
W-LAN基地局 の特定
S117
鍵情報、ユーザ情報
通信相手確認
S116
S120
S119
許可通知、鍵情報
鍵情報
S118
ユーザ情報
S121
S122
無線L2,3認証
IPアドレス取得
S123
S124
ハンドオーバ
S125
アクセス再開

フロントページの続き

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｗ４／００－Ｈ０４Ｗ９９／００
Ｈ０４Ｂ７／２４－Ｈ０４Ｂ７／２６