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

特許第5498140号
(P5498140)

(45)発行日　平成26年5月21日(2014.5.21)　(24)登録日　平成26年3月14日(2014.3.14)

(51)Int.Cl.		F I		
G06F 21/45	(2013.01)	G06F	21/20	145
G06F 21/44	(2013.01)	G06F	21/20	144C
H04W 12/06	(2009.01)	H04W	12/06	
H04W 84/12	(2009.01)	H04W	84/12	
G06F 13/00	(2006.01)	G06F	13/00	510A

請求項の数 9　(全 15 頁)

(21)出願番号　特願2009-274931 (P2009-274931)
(22)出願日　平成21年12月2日 (2009.12.2)
(65)公開番号　特開2011-118634 (P2011-118634A)
(43)公開日　平成23年6月16日 (2011.6.16)
審査請求日　平成24年11月30日 (2012.11.30)

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治
(74)代理人　100134175
弁理士　永川　行光

最終頁に続く

(54)【発明の名称】端末管理装置およびその制御方法

(57)【特許請求の範囲】

【請求項１】

通信端末が認証サーバにログインすることにより前記通信端末とネットワークとの通信が開始される通信システムにおける端末管理装置であって、

通信端末が前記認証サーバにログインした際の認証情報を記憶する認証情報記憶手段と、

前記通信端末が前記認証サーバへのログインを要求した場合に、当該通信端末が当該認証サーバに既にログインしている状態であるか否かを判定する判定手段と、

前記判定手段により既にログインしている状態であると判定された場合に、前記認証情報記憶手段に記憶してある前記認証情報を用いて、前記認証サーバに対して前記通信端末のログアウトを実行するログアウト実行手段とを備えることを特徴とする端末管理装置。

【請求項２】

通信端末より前記認証サーバへのログイン要求を受信した場合に、当該認証サーバへの当該ログイン要求の送信を行わずに、保留する保留手段と、

前記ログイン要求を行った前記通信端末が前記認証サーバにおいてログアウトされた状態にあるか否かを問い合わせるログアウト判定要求を他の端末管理装置へ送信する送信手段と、

前記送信手段によって送信された前記ログアウト判定要求に応じて前記他の端末管理装置からログアウト終了の通知を受信することにより、前記保留手段による保留状態を解除し、前記ログイン要求を前記認証サーバに送信してログインを実行するログイン実行手段

とを更に備えることを特徴とする請求項１に記載の端末管理装置。
【請求項３】
前記送信手段により前記ログアウト判定要求を送信する先の他の端末管理装置は、自身の位置より所定範囲に存在する端末管理装置に限られることを特徴とする請求項２に記載の端末管理装置。
【請求項４】
前記判定手段は、前記通信端末が前記認証サーバにおいてログアウトされた状態にあるか否かを他の端末管理装置に問い合わせることによって、当該通信端末が当該認証サーバに既にログインしている状態であるか否かを判定することを特徴とする請求項１乃至３のいずれか１項に記載の端末管理装置。
【請求項５】
前記端末管理装置は、無線ＬＡＮの基地局の一部を構成することを特徴とする請求項１乃至４のいずれか１項に記載の端末管理装置。
【請求項６】
前記端末管理装置は、前記通信端末の一部を構成することを特徴とする請求項１乃至４のいずれか１項に記載の端末管理装置。
【請求項７】
前記端末管理装置は、公衆無線ＬＡＮの通信システムにおける端末管理装置であることを特徴とする請求項１乃至６のいずれか１項に記載の端末管理装置。
【請求項８】
通信端末が認証サーバにログインすることにより前記通信端末とネットワークとの通信が開始される通信システムにおける端末管理装置の制御方法であって、
認証情報記憶手段が、通信端末が前記認証サーバにログインした際の認証情報を記憶する認証情報記憶工程と、
前記通信端末が前記認証サーバへのログインを要求した場合に、判定手段が、当該通信端末が当該認証サーバに既にログインしている状態であるか否かを判定する判定工程と、
前記判定工程で既にログインしている状態であると判定された場合に、ログアウト実行手段が前記認証情報記憶工程で記憶した前記認証情報を用いて、前記認証サーバに対して前記通信端末のログアウトを実行するログアウト実行工程とを有することを特徴とする端末管理装置の制御方法。
【請求項９】
コンピュータを、請求項１乃至７のいずれか１項に記載の端末管理装置の各手段として機能させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、通信端末が認証装置に対して認証処理を行い、その後、ネットワークとの通信を行う通信システムに好適な端末管理装置及びその制御方法に関する。
【背景技術】
【０００２】
通信端末が認証装置に対して認証処理を行い、その後、ネットワークとの通信を行う通信システムの１つに公衆無線ＬＡＮがある。このような公衆無線ＬＡＮにおいて、認証処理は、例えば、通信端末のユーザがログイン画面においてＩＤやパスワードを入力することで実行される。また、通信端末が行う認証処理を基地局が代行する技術も提案されている（特許文献１）。
【０００３】
一般に、公衆無線ＬＡＮは、複数の基地局の各々により形成される複数の無線スポットと、認証サーバ、ネットワークで構成される。通信端末は、予め記憶している暗号鍵を使用して基地局に接続する。つづいて、通信端末は、認証サーバに対して、これも予め記憶しているＩＤおよびパスワードを含む認証情報を基地局を介して送信し、ログイン要求を

行う。認証サーバは、上記ログイン要求に含まれるＩＤおよびパスワードをチェックする。そして、認証サーバが記憶している認証情報と一致すれば、認証サーバは通信端末のセッションを管理するセッション管理部に当該通信端末のセッションを追加し、当該通信端末に対してログイン応答（＝成功）を送信する。通信端末は、認証サーバからログイン応答（＝成功）を受信すると、基地局を介してネットワークとデータ通信を行う。

【０００４】

一般に、認証サーバは、通信端末による上記データ通信の終了を検出するとセッションタイマをスタートさせる。セッションタイマの役目は、一定時間通信を行わない通信端末のセッションをセッション管理部から削除することである（セッションが削除された以後は、通信端末はネットワークとの通信ができない）。セッションタイマのタイムアウト時間は、公衆無線ＬＡＮを運営する通信事業者の実装によるが、数十分程度と言われている。

【先行技術文献】

【特許文献】

【０００５】

【特許文献１】特開２００４－１６４５７６号公報

【発明の概要】

【発明が解決しようとする課題】

【０００６】

しかしながら、上記公衆無線ＬＡＮにおけるセッションタイマを用いた通信端末のセッション管理では、以下のような課題がある。たとえば、ユーザが認証サーバにログイン中の通信端末（セッション中の通信端末）の電源をＯＦＦし、認証サーバに対するログアウト処理を行わずに、データ通信を行った無線スポットから別の無線スポットに移動したとする。ここで通信端末の電源がＯＮされると、通信端末は予め記憶している暗号鍵を使用して移動後の無線スポットを形成する基地局に接続する。つづいて、通信端末は、認証サーバに対して、これも予め記憶しているＩＤおよびパスワードを送信し、ログイン要求を行う。

【０００７】

ここで、認証サーバにおいて、移動前の無線スポットにおいて通信端末に対して追加されたセッションのセッションタイマがタイムアウトしていないと、当該通信端末のセッションはセッション管理部に残されたままである。よって、認証サーバは、すでに管理しているセッションと重複すると判断し、移動後の基地局を介して送信されたログイン要求に対して、ログイン応答（＝失敗）を送信してしまう。つまり、通信端末は、正当なＩＤとパスワードを認証サーバに送信しているにも関わらず、移動前の無線スポットにおける通信端末に関連してスタートしたセッションタイマがタイムアウトするまで、移動後の無線スポットからログインすることができない。認証サーバは、セッションタイマがタイムアウトすると管理情報から当該通信端末に対するセッションを削除する。その後、通信端末はようやく認証サーバへのログインに成功する。

【０００８】

このような現象が発生するのは、通信端末側が認識している通信端末の状態と認証サーバが認識している当該通信端末の状態とが一致していないからである。即ち、通信端末が認証サーバにログイン要求をする時、通信端末は「現在、通信端末（自身）はログインしていない」という状態である（電源ＯＦＦにより、内部状態がいったんリセットされている為）。しかしながら、認証サーバは、通信端末のログイン要求を既に受け入れており、セッションタイマがタイムアップするまでは管理情報として当該通信端末のセッションを記憶している（つまり、「通信端末はログインしている」）。この時点で、通信端末側が認識している自分自身の状態と認証サーバが認識している当該通信端末の状態とは一致していない。

【０００９】

本発明は、上記課題に鑑みてなされたものであり、通信端末と認証サーバにより把握さ

れているログイン状態のずれを解消し、使い勝手の良い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】

【００１０】

上記の目的を達成するための本発明の一態様による端末管理装置は以下の構成を備える。すなわち、

通信端末が認証サーバにログインすることにより前記通信端末とネットワークとの通信が開始される通信システムにおける端末管理装置であって、

通信端末が前記認証サーバにログインした際の認証情報を記憶する認証情報記憶手段と、

前記通信端末が前記認証サーバへのログインを要求した場合に、当該通信端末が当該認証サーバに既にログインしている状態であるか否かを判定する判定手段と、

前記判定手段により既にログインしている状態であると判定された場合に、前記認証情報記憶手段に記憶してある前記認証情報を用いて、前記認証サーバに対して前記通信端末のログアウトを実行するログアウト実行手段とを備える。

【発明の効果】

【００１１】

本発明によれば、通信端末と認証サーバにより把握されているログイン状態のずれを解消し、使い勝手の良い通信システムを提供することが可能となる。

【図面の簡単な説明】

【００１２】

【図１】第１実施形態の通信システムの構成例を示す図。

【図２】第１実施形態の端末管理装置の構成例を示すブロック図。

【図３】（ａ）認証情報記憶テーブルのデータ構成例を示す図、（ｂ）リンク監視テーブルのデータ構成例を示す図、（ｃ）ログアウト管理テーブルのデータ構成例を示す図。

【図４】第１実施形態による端末管理装置の内部シーケンス図。

【図５】第１実施形態による通信システムのシーケンス図。

【図６】ログアウト実行判定部の処理を示すフローチャート。

【図７】通信端末の構成例を示すブロック図。

【図８】第２実施形態による端末管理装置のブロック図。

【図９】第２実施形態による通信システムのシーケンス図。

【図１０】第２実施形態による端末管理装置のフローチャート。

【発明を実施するための形態】

【００１３】

以下、添付の図面を参照して、本発明の好適な実施形態を説明する。

〈第１実施形態〉

第１実施形態のシステム構成例を図１に示す。本実施形態では所謂公衆無線ＬＡＮを例に挙げて説明するが、本発明は、通信端末が認証サーバに対して基地局を介して認証情報を送信して当該認証サーバにログインすることにより、通信端末とネットワークとの通信が開始される通信システムに適用できる。

【００１４】

図１において、公衆無線ＬＡＮでは、基地局１０３（以下、ＡＰ１０３）により無線スポット１０１が形成され、基地局１０４（以下、ＡＰ１０４）により無線スポット１０２が形成されている。ＡＰ１０３、ＡＰ１０４、認証サーバ１０５は有線ネットワークで接続されている。例えば無線スポット１０１にある通信端末１００（以下、ＳＴＡ１００）は、予め記憶している暗号鍵を使用してＡＰ１０３に接続する。つづいて、ＳＴＡ１００は、認証サーバ１０５に対して、これも予め記憶しているＩＤおよびパスワードを含む認証情報を送信し、ログイン要求を行う。認証サーバ１０５では、ログイン要求で送信された認証情報（ＩＤおよびパスワード）と、自身に記憶されている認証情報とが一致するかを判断する。一致すると判断されると、認証サーバ１０５は、通信端末のセッションを管

理するセッション管理部（不図示）にＳＴＡ１００のセッションを追加し、ＳＴＡ１００に対してログイン応答（＝成功）を送信する。認証サーバ１０５による認証に成功すると、ＳＴＡ１００は、ＡＰ１０３を介してネットワーク１０６（例えば、インターネット）との通信を開始することができる。

【００１５】

端末管理装置１０７および１０８は、ＡＰ１０３およびＡＰ１０４に接続している通信端末を管理する。端末管理装置１０７，１０８は、通信端末がＡＰ１０３，１０４に接続しているかどうかや、認証サーバ１０５にログインおよびログアウト処理を行ったか、またログイン／ログアウトに使用したＩＤおよびパスワードといった認証情報を管理する。端末管理装置１０７はＡＰ１０３を、端末管理装置１０８はＡＰ１０４をそれぞれ管理するものとする。なお、以下では、公衆無線ＬＡＮを使用する通信端末（ＳＴＡ１００）として、デジタルスチルカメラを例にしているが、もちろんこれに限られるものではない。無線通信によりＬＡＮに接続する機能を備えた情報処理装置（一般には携帯端末）であれば、いかなるものでも適用可能である。

【００１６】

図２は端末管理装置１０７、１０８のブロック図である。以下、端末管理装置１０７について説明するが、端末管理装置１０８も同様の構成を備えるものである。リンク監視部２００は、無線スポット内の通信端末が基地局に接続しているかどうか監視し、リンク監視テーブル４００（図３の（ｂ））を更新する。ログアウト実行判定部２０１は、端末管理装置１０７が、通信端末のＩＤおよびパスワードを使用して、ログアウト処理を実行するかどうかの判定を行う。ログアウト管理部２０２は、無線スポット内の通信端末のログイン状態およびログアウト状態を管理し、ログアウト管理テーブル５００（図３の（ｃ））を更新する。ログアウト実行部２０３は、ログアウト実行判定部２０１の指示によって、通信端末のログアウト処理を代行する。認証情報記憶部２０４は、通信端末のＩＤおよびパスワードを認証情報記憶テーブル３００（図３の（ａ））に記憶する。リンク確認タイマ２０５は、リンク監視部２００が上述した監視を行うタイミングを規定する。有線インターフェース（以下、有線Ｉ／Ｆ）２０６は、基地局（ＡＰ１０３，１０４）およびネットワーク１０６と通信を行うための有線接続を行うためのインターフェースである。制御部２０７は、端末管理装置１０７，１０８の全体の制御を行う。

【００１７】

図３の（ａ）は、認証情報記憶テーブル３００のデータ構成例を示す。認証情報記憶テーブル３００には、例えば、認証サーバ１０５の認証に成功した基地局のＭＡＣアドレス３０１、ＩＤ３０２およびパスワード３０３が記憶される。ここでは、ＳＴＡ１００について、ＭＡＣアドレス、ＩＤおよびパスワードが記憶されている。図３の（ｂ）はリンク監視テーブル４００のデータ構成例を示す。リンク監視テーブル４００には、管理している基地局に接続している通信端末のＭＡＣアドレス４０１が記憶される。ここでは、ＳＴＡ１００のＭＡＣアドレスを記憶している。図３の（ｃ）はログアウト管理テーブル５００のデータ構成例を示す。ログアウト管理テーブル５００には、通信端末のＭＡＣアドレス５０１と、ログインしたかどうかを示すログイン情報５０２と、ログアウトしたかどうかを示すログアウト情報５０３とが記憶される。図３の（ｃ）によれば、ＭＡＣアドレス５０１が、aa:aa:aa:aa:aa:aaであるＳＴＡ１００は、ログイン情報５０２がＹＥＳであり、ログアウト情報５０３がＮＯである。これは、ＳＴＡ１００は、認証サーバ１０５においてログインしており、かつログアウトしていない事を示す。

【００１８】

以上のような構成を備えた本実施形態の通信システム及び端末管理装置の動作について図４～図６を参照して、詳細に説明する。図４は、図２に示した端末管理装置１０７の動作を説明するシーケンス図である。図５は、図１に示した通信システムの動作を説明するシーケンス図である。図６は、端末管理装置１０７のログアウト実行判定部２０１による処理を示すフローチャートである。

【００１９】

ＳＴＡ１００は予め記憶している暗号鍵を使用してＡＰ１０３に接続する（７００、７０１）。つづいて、認証サーバに対して、これも予め記憶しているＩＤおよびパスワードを送信し、ログイン要求を行う（７０２）。認証サーバ１０５は、ＩＤおよびパスワードをチェックし、当該認証サーバ１０５が記憶している認証情報と一致すれば、通信端末を管理する管理情報にＳＴＡ１００のセッションを追加する（７０３）。そして、認証サーバ１０５は、ＡＰ１０３を介して、ＳＴＡ１００に対してログイン応答（＝成功）を送信する（７０４）。ＡＰ１０３は、ログイン応答（＝成功）を受信すると、端末管理装置１０７に対して、ＳＴＡ１００の認証情報通知を送信する（７０６）。

【００２０】

端末管理装置１０７の制御部２０７は、認証情報通知を受信すると、リンク監視部２００、ログアウト管理部２０２、認証情報記憶部２０４に以下の通知を行う（６００）。すなわち、

・リンク監視部２００にＳＴＡ１００のＭＡＣアドレスを通知し（２２０）、
・ログアウト管理部２０２にＳＴＡ１００のＭＡＣアドレスとＳＴＡ１００がログインした旨を通知し（２１１）、
・認証情報記憶部２０４にＳＴＡ１００のＭＡＣアドレスと、認証サーバ１０５への認証に用いたＩＤおよびパスワードを通知する（２１０）。

【００２１】

リンク監視部２００では、認証情報通知を受信すると、リンク監視テーブル４００に、ＳＴＡ１００のＭＡＣアドレス（図の例ではaa:aa:aa:aa:aa:aa）を記憶する。ログアウト管理部２０２では、認証情報通知を受信すると、ログアウト管理テーブル５００のＭＡＣアドレス５０１にＳＴＡ１００のＭＡＣアドレスを、ログイン情報５０２に「ＹＥＳ」を記憶する。現時点ではＳＴＡ１００はログアウトしていないので、ログアウト情報５０３は「ＮＯ」である。認証情報記憶部２０４では、認証情報通知を受信すると、認証情報記憶テーブル３００のＭＡＣアドレス３０１にＳＴＡ１００のＭＡＣアドレスを、ＩＤ３０２とパスワード３０３にはそれぞれ認証に用いられたＩＤ（図では「123」）とパスワード（図では「aaa」）を記憶する。

【００２２】

ログインの成功を示すログイン応答（７０４）を受信すると、ＳＴＡ１００はＡＰ１０３を介してネットワーク１０６とデータ通信を行う（７０７）。ＳＴＡ１００のデータ通信が終了すると、ＡＰ１０３は端末管理装置１０７および認証サーバ１０５にＳＴＡ１００のＭＡＣアドレスと共にデータ通信終了通知を行う（７０８）。

【００２３】

認証サーバ１０５はデータ通信終了通知を受信すると、ＳＴＡ１００に関してセッションタイマをスタートさせる（７１０）。端末管理装置１０７の制御部２０７は、データ通信終了通知を受信すると、リンク監視部２００にＳＴＡ１００のＭＡＣアドレスとともに、データ通信終了を通知する（６０１）。リンク監視部２００は、データ通信終了通知を受信すると（６０１）、リンク確認タイマ２０５をスタートする（６０２、７０９、２０９）。リンク確認タイマ２０５がタイムアウトすると（７１２、６０３、２１２）、リンク監視部２００は、制御部２０７にリンク確認要求を行う（６０４、２１３）。

【００２４】

端末管理装置１０７の制御部２０７は、リンク確認要求（６０４）に応答して、ＡＰ１０３に対して、ＳＴＡ１００のリンク確認要求を行う（７１３）。このリンク確認要求（７１３）に応答して、ＡＰ１０３は、ＳＴＡ１００に対して、応答を期待するパケットを送信する。図５では、ＡＰ１０３はＳＴＡ１００に対してＲＴＳ（Request To Send）パケットを送信する（７１４）。ＳＴＡ１００においては電源が切られているため（７１１）、ＲＴＳに対してＣＴＳ（ClearTo Send）は送信されない。よって、ＡＰ１０３は、端末管理装置１０７に対して、リンク確認応答（＝切断）を送信する（７１５）。

【００２５】

端末管理装置１０７の制御部２０７は、リンク確認応答（７１５）を受信すると、リン

ク監視部２００にそれを通知する（６０５、２０８）。すると、リンク監視部２００は、ログアウト実行判定部２０１に対して、ＳＴＡ１００のＭＡＣアドレスと共にログアウト判定要求（２１４）を行う（６０６）。ログアウト実行判定部２０１は、ログアウト判定要求を受信すると（Ｓ８００）、ログアウト管理テーブルのログアウト情報５０３を参照する（６０７，６０８，２１５，２１６，７２９）。図３の（ｃ）のログアウト管理テーブル５００によれば、ＳＴＡ１００はログインしており（Ｓ８０１でＹＥＳ）、ＳＴＡ１００のログアウト情報５０３は「ＮＯ」である為、ＳＴＡ１００はログアウトしていない（Ｓ８０２でＮＯ）。そして、ログアウト実行判定部２０１は、リンク監視部２００に対して、ログアウト判定応答（未ログアウト）を送信する（６０９，２２３）。

【００２６】

続いて、ログアウト実行判定部２０１は、制御部２０７に対して、セッション確認要求を行い（６１０、Ｓ８０３、２２１）、認証サーバ１０５に対して、セッション管理部にＳＴＡ１００のセッションが残っているかどうかを確認する。端末管理装置１０７は、認証サーバ１０５に対してＳＴＡ１００のＭＡＣアドレスもしくはＩＤおよびパスワードとともにセッション確認を行う（７１６）。認証サーバ１０５は、このセッション確認に応答して、セッション確認応答（ここでは、セッションあり）を送信する（７１７）。セッション確認応答を受信すると、端末管理装置１０７の制御部２０７は、ログアウト実行判定部２０１に、ＳＴＡ１００のセッションが残っている旨を通知する（６１１、２２２）。

【００２７】

ログアウト実行判定部２０１は、セッション確認応答（６１１）を受信すると（Ｓ８０４）、ＳＴＡ１００のセッションが認証サーバ１０５に残っているかを判定する。セッション確認応答（７１７）は、「セッションあり」である（Ｓ８０５でＹＥＳ）。よって、ログアウト実行判定部２０１は、ログアウトを実行すると判定する（７１８）。そして、ログアウト実行部２０３に、ＳＴＡ１００のＭＡＣアドレスと共にログアウト実行指示を送信する（６１２、２１７、Ｓ８０６）。

【００２８】

ログアウト実行部２０３は、認証情報記憶部２０４に対してＳＴＡ１００の認証情報を要求する（６１３，２２４）。認証情報記憶部２０４は認証情報の要求に応答し、認証情報記憶テーブル３００から、ＳＴＡ１００のＭＡＣアドレスおよび認証情報（ＩＤとパスワード）を選択し（７１９）、ログアウト実行部２０３に送信する（６１４、２１８）。ログアウト実行部２０３は、制御部２０７に、認証情報記憶部２０４から受信したＭＡＣアドレスおよび認証情報（ＩＤとパスワード）とともに、ログアウト要求を送信する（６１５，２１９）。

【００２９】

端末管理装置１０７は、上記のようにして選択されたＳＴＡ１００の認証情報を使用して、認証サーバ１０５にログアウト要求を行い（７２０）、認証サーバからログアウト応答（＝成功）を受信する（７２１）。認証サーバ１０５は、ログアウト応答を送信後、セッション管理部を更新し、ＳＴＡ１００のセッションを削除する（７２３）。

【００３０】

ここで、ＳＴＡ１００が無線スポット１０１から無線スポット１０２に移動したとする。ＳＴＡ１００は予め記憶している暗号鍵を使用して、無線スポット１０２の基地局であるＡＰ１０４に接続する（７２４、７２５）。つづいてＳＴＡ１００は、認証サーバ１０５に対して、これも予め記憶しているＩＤおよびパスワードを送信し、ログイン要求を行う（７２６）。ここで、認証サーバ１０５は既にＳＴＡのセッションを一旦削除している（７２３）。つまり、認証サーバ１０５のセッション管理部にＳＴＡ１００のセッションは残っていない。よって、認証サーバ１０５は、セッション管理部にＳＴＡ１００のセッションを追加することができ（７２７）、ＳＴＡに対してログイン応答（＝成功）を送信する（７２８）。それ以後、ＳＴＡ１００はＡＰ１０４を介してネットワーク１０６との通信が可能となる。

【００３１】
図６において、ＳＴＡ１００が認証サーバ１０５にログインしていない場合（Ｓ８０１でＮＯ）とは、例えば、ＳＴＡ１００が一旦ＡＰ１０３に接続したが認証サーバ１０５にログインせずにＡＰ１０３との接続が切断した場合が考えられる。この場合は、認証サーバ１０５のセッション管理部にＳＴＡ１００のセッションは残っていない。よって、端末管理装置１０７は、ＳＴＡ１００に代わってログアウトを実行する必要がなく、ログアウト実行判定部２０１は処理を終了する。また、ＳＴＡ１００がログアウトしている場合（Ｓ８０２でＹＥＳ）は、ＳＴＡ１００により正規の手順でログアウトが行われたことを示す。よって、この場合も認証サーバ１０５のセッション管理部にＳＴＡ１００のセッションは残っていない。よって、ログアウト実行判定部２０１はログアウトを代行することなく処理を終了する。また、Ｓ８０５において、ＳＴＡ１００のセッションが残っていない場合（Ｓ８０５でＮＯ）も、ログアウト実行判定部２０１はログアウトを代行することなく処理を終了する。なお、Ｓ８０５において、ＳＴＡ１００のセッションが残っていない場合とは、認証サーバ１０５においてセッションタイマがタイムアップした場合が考えられる。

【００３２】
以上の処理により、新たにＳＴＡ１００からログイン要求が発行される際には、ＳＴＡ１００が認識しているログイン／ログアウトの状態と、認証サーバ１０５が認識しているＳＴＡ１００のログイン／ログアウトの状態を一致させることが可能となる。

【００３３】
なお、本実施形態では、端末管理装置１０７，１０８は基地局（ＡＰ１０３、ＡＰ１０４）と別体であったが、端末管理装置は基地局と同一筐体内にあっても同様の効果がえらえることはいうまでもない。即ち、端末管理装置１０７，１０８が基地局の一部を構成するようにしてもよい。また、上記実施形態では、端末管理装置と基地局をそれぞれ２基保有するシステムを例に説明してきたが、それらは１基もしくは３基以上の複数であってもよく、２機以上のＳＴＡが通信システム内に存在してもよいことは言うまでもない。

【００３４】
また、上記実施形態では、通信端末と基地局との間におけるリンクを監視し、リンクの切断を検出することでログアウト実行判定部２０１による判定を開始させているが、これに限られるものではない。例えば、通信端末と基地局との間のリンクに切断が発生することを推定させる事象の発生を検出することで、ログアウト実行判定部２０１による判定を開始させるようにしてもよい。リンクに切断が発生することを推定させる事象としては、
（１）通信端末において電源オフ操作が実行されたこと（この場合、通信端末には基地局に電源オフ操作が実行されたことを通知する機能が必要となる）、
（２）通信端末においてバッテリ残量が所定値を下回ったこと（この場合、通信端末には基地局にバッテリ残量不足を通知する機能が必要となる）、
（３）通信端末と基地局との間の無線通信強度が所定値を下回ったこと（この場合、端末管理装置１０７，１０８には、通信端末との無線通信の信号強度を検出する機能が必要となる）、
などが挙げられる。

【００３５】
また、ＳＴＡ１００の構成として、電源オフ時に認証サーバに対して、従来はＳＴＡ１００のユーザが手動で行っていたログアウト処理をＳＴＡ１００が自律的に行うようにすることも可能である。例えば、上述した、「通信端末と基地局との間のリンクに切断が発生することを推定させる事象」の発生を検出した場合に、ＳＴＡ１００がログアウト処理を自律的に行うようにすることができる。このようにすれば、ＳＴＡ１００の電波をＡＰ１０３が十分受信できる状態であれば、端末管理装置１０７が行っていたログアウト処理（７２０）をＳＴＡ１００が行えるので、端末管理装置１０７の処理負荷を軽減することができる。

【００３６】

この場合、端末管理装置１０７，１０８は、ＳＴＡ１００の一部を構成することになり、ＳＴＡ１００を、例えば図７に示すような構成とすればよい。図７において図２と同じ構成に関しては、同一の符号を付与してある。電源ボタン操作検出部９００は、ＳＴＡ１００における電源ボタンの押下を検出する。バッテリ残量監視部９０１は、ＳＴＡ１００におけるバッテリ残量を監視する。電源ボタン操作検出部９００は電源ボタン押下（電源オフ操作）を検出すると、また、バッテリ残量監視部９０１はバッテリ残量の低下を検出すると、ログアウト実行判定部９０２にログアウト判定要求（２１４）を送信する。ログアウト判定要求を受信したログアウト実行判定部９０２は、ログアウト管理テーブル５００を参照し、ＳＴＡ１００がログアウトしているかどうかを判定する。そして、ログアウトしていない（ログアウト情報５０３がＮＯ）場合に、無線部９０３を介して認証サーバ１０５にログアウト要求を行う。

【００３７】

本実施形態によれば、通信端末が認識している通信端末自身の状態と、認証装置が認識している通信端末の状態を一致させることができる。それにより、認証装置にセッションが残った状態で通信装置が認証装置に対してログイン要求を行うことによりログインに失敗してしまうことを回避できる。なお、「通信端末と基地局との間のリンクに切断が発生することを推定させる事象」として、上述したような、無線通信における信号強度の低下を用いることも可能である。

【００３８】

〈第２実施形態〉

第１実施形態では、端末管理装置１０７，１０８のログアウト実行判定部２０１は、同じ端末管理装置内のリンク監視部２００からログアウト判定要求２１４を受信した。第２実施形態では、端末管理装置１０７，１０８のログアウト実行判定部２０１は、他の端末管理装置からログアウト判定要求を受信可能な構成としている。

【００３９】

第２実施形態の端末管理装置のブロック図を図８に示す。なお、図２と同一の構成に関しては、同一の符号を付与してある。有線Ｉ／Ｆ１０００は無線スポット１０１（または無線スポット１０２）を形成するＡＰ１０３（またはＡＰ１０４）と通信する為のインターフェースである。有線Ｉ／Ｆ１００１は、ネットワーク１０６と通信する為のＩ／Ｆである。端末管理装置記憶部１００３は、図１の通信システムにおける端末管理装置１０７（１０８）の識別情報（例えば、ＩＰアドレス）を記憶する。第２実施形態では、端末管理装置記憶部１００３には、図１で示した通信システム内における端末管理装置１０７，１０８の識別情報が予め記憶されているとする。なお、端末管理装置記憶部１００３には自身の識別情報を記憶しておく必要は無く、従って、例えば、端末管理装置１０７の端末管理装置記憶部１００３には端末管理装置１０８の識別情報が記憶されていればよい。

【００４０】

通信ブロック部１００９は、ログアウト管理部１００２から、ＭＡＣアドレスによる通信端末の指定を受け、通信端末が送信するデータを、有線Ｉ／Ｆ１０００と有線Ｉ／Ｆ１００１の間でブロックする。通信ブロック部１００９は、ＳＴＡ１００よりＡＰ１０３を介して認証サーバ１０５へのログイン要求がなされた場合に、制御部２０７からの指示により認証サーバ１０５への当該ログイン要求の送信を行わずに、保留するように機能する。また、ログアウト管理部１００２の指示により、保留状態を解除し、保留していたログイン要求を認証サーバ１０５に送信する。

【００４１】

図９に示すシーケンス図および図１０に示す端末管理装置１０７，１０８のフローチャートを参照して、第２実施形態の動作を詳細に説明する。なお、以下では端末管理装置１０８にログイン要求が送信された場合を説明するが、端末管理装置１０７においてログイン要求が行われた場合も同様である。

【００４２】

ＳＴＡ１００は、無線スポット１０１で認証サーバ１０５にログインし、データ通信を

行った後、ログアウト要求を行わずに、無線スポット１０２の基地局であるＡＰ１０４に接続したとする。ＳＴＡ１００は、予め記憶している暗号鍵を使用してＡＰ１０４に接続した後（図示しない）、認証サーバにログイン要求を行う（１１００）。端末管理装置１０７は、ログイン要求を受信したことを（Ｓ１２００でＹＥＳ）ログアウト管理部１００２に通知する。そして、ログアウト管理部１００２は、ログイン要求が認証サーバに届かないようにする為に、通信ブロック部１００９に対してＳＴＡ１００のＭＡＣアドレスと共に通信ブロック機能を有効にする旨を通知する（１００８、Ｓ１２０１）。通信ブロックを有効にする理由は、ＳＴＡ１００がログイン要求を送信した時点（１１００）で、認証サーバ１０５のセッション管理部（不図示）にＳＴＡ１００のセッションが残っている可能性があるからである。そのような場合に、ログイン要求を認証サーバに行うと、ログインに失敗してしまう。

【００４３】

続いて、端末管理装置１０８のログアウト管理部１００２は、端末管理装置記憶部１００３を参照し、通信システム内における他の端末管理装置（図１の場合、端末管理装置１０７）のＩＰアドレスを選択する（１１０１、Ｓ１２０２、１００５）。そして、端末管理装置１０８のログアウト管理部１００２は、端末管理装置１０７に対して、ＳＴＡ１００のＭＡＣアドレスと共にログアウト判定要求を送信する（１１０２、Ｓ１２０３、１００６）。

【００４４】

端末管理装置１０７の制御部２０７は、端末管理装置１０８よりログアウト判定要求を受信すると（Ｓ１２００でＮＯ、Ｓ１２０８でＹＥＳ）、当該ログアウト判定要求を自身のログアウト実行判定部２０１に転送する（１００７）。ログアウト判定要求が転送されたログアウト実行判定部２０１は、ログアウト管理テーブル５００のログアウト情報５０３を参照する（１１０３、Ｓ１２０９）。図３の（ｃ）によれば、ＳＴＡ１００のログアウト情報５０３は「ＮＯ」であり、ＳＴＡ１００はログアウトしていない（１１０４、Ｓ１２１０でＹＥＳ）。よって、端末管理装置１０７のログアウト実行判定部２０１は、端末管理装置１０８に対して、ログアウト判定応答（未ログアウト）を送信する（Ｓ１２１１、１１０５）。

【００４５】

続いて、端末管理装置１０７のログアウト実行判定部２０１は同じく端末管理装置１０７のログアウト実行部２０３に対して、ログアウト実行指示を行う（１１０６）。こうしてログアウト実行指示を受け取ったログアウト実行部２０３は、ログアウト処理を行い（１１０７、Ｓ１２１２）、端末管理装置１０８のログアウト管理部１００２に対して、ログアウト終了通知をする（１１０８、Ｓ１２１３）。

【００４６】

端末管理装置１０８のログアウト管理部１００２は、端末管理装置１０７から未ログアウトを受信すると、端末管理装置１０７からログアウト終了を受信するまで待機する（Ｓ１２０４でＹＥＳ、Ｓ１２０５）。そして、ログアウト管理部１００２は、ログアウト終了通知を受信する（Ｓ１２０５でＹＥＳ）と、通信ブロック部１００９に対してＳＴＡ１００のＭＡＣアドレスと共に通信ブロック機能を無効にする旨を通知する（Ｓ１２０６，１００８）。端末管理装置１０８は、通信ブロック機能が無効になると、Ｓ１２０１でブロックしていたログイン要求を認証サーバ１０５へ送信することによりログインを実行する（Ｓ１２０７）。

【００４７】

以上の動作によれば、端末管理装置１０７によるログアウト処理（１１０７）が実行されたことで、認証サーバ１０５のセッション管理部におけるＳＴＡ１００のセッションは、端末管理装置１０８を介したログイン要求に先立って削除される。よって、Ｓ１２０１で実行されたログイン要求（１１０９）は成功する（１１１０）。なお、Ｓ１２１０において未ログアウトの状態ではない（即ち、ログアウト済みである）と判定された場合には、直ちにログアウト終了通知が送信される（Ｓ１２１０でＮＯ、Ｓ１２１３）。そして、

ログアウト判定要求を行ったログアウト管理部１００２は、直ちに通信ブロック部１００９にＳＴＡ１００に関するブロック状態の解除を指示する（Ｓ１２０４でＮＯ，Ｓ１２０６）。

【００４８】

なお、以上説明した第２実施形態では、端末管理装置記憶部１００３に予め他の端末管理装置の識別情報が記憶されているとした。しかしながら、端末管理装置記憶部１００３に記憶される端末管理装置の識別情報は、ＵＰｎＰ等の機器探索プロトコルを用いて更新される構成としてもよい。そのような構成とすることで、無線スポットの増減に対して柔軟に対応することができる。また、機器探索の探索範囲を、端末管理装置の位置情報を元に所定範囲に制限する構成としてもよい。そのような構成とすることで、機器探索に要する時間を削減することが可能となる。また、遠隔地にある無線スポットの端末管理装置の識別情報が端末管理装置記憶部１００３に記憶されないようになるので、無駄なログイン判定要求の送信が防止される。

【００４９】

また、上記第２実施形態において、ＳＴＡ１００は認証サーバ１０５にログアウト要求を行わずに無線スポット１０１から移動し、無線スポット１０２の基地局であるＡＰ１０４に接続した場合を例にして説明してきた。即ち、ログイン要求を受信した基地局の端末管理装置が他の端末管理装置に対してログアウト判定要求を送信する場合を説明した。しかしながら、本発明はこれに限られるものではなく、ログイン要求を受信した基地局の端末管理装置が自身のログアウト実行判定部２０１に対してログアウト判定要求を行うようにしても良い。このようにすれば、例えば、ＳＴＡ１００の電源を切断するなどして認証サーバ１０５にログアウト要求を行わずに無線スポット１０１から移動し、その後、他の無線スポットには移動せず再び無線スポット１０１に戻りログインしようとした場合に対応することができる。また、上記実施形態では、端末管理装置と基地局をそれぞれ２基保有するシステムを例に説明してきたが、それらは１基もしくは３基以上の複数であってもよく、２機以上のＳＴＡが通信システム内に存在してもよいことは言うまでもない。

【００５０】

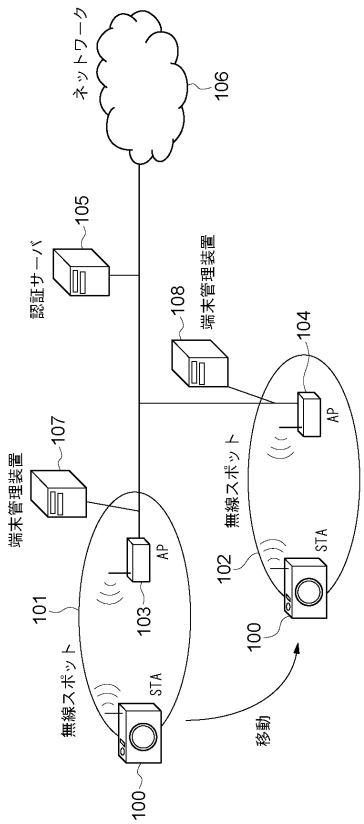
なお、上記各実施形態において、ログアウト管理部２０２，１００２に、認証サーバ１０５のセッションタイマと同じタイムアップ時間を有するタイマを設けて、該タイマのタイムアップによりログアウト管理テーブル５００を更新してもよい。これにより、ログアウト管理部２０２，１００２は、認証サーバ１０５のセッションタイマのタイムアウトとほぼ同期してログアウト情報５０３を「ＹＥＳ」に更新することができ、Ｓ８０５において無駄なセッション確認が発生することを防止できる。また、認証サーバ１０５へのセッション確認を省略し、ログアウト管理テーブル５００で未ログアウトの場合には直ちにログアウトを実行するようにしてもよい。更に、ログアウト管理テーブル５００による確認も省略可能である。これらの構成によれば、端末管理装置の構成をより簡素化できるが、認証サーバ１０５に対して無駄なログアウト要求が発生することになる。

【００５１】

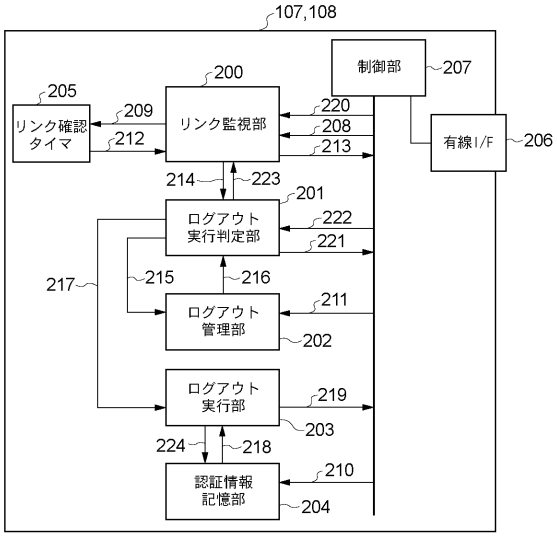
［他の実施形態］

また、本発明は、以下の処理を実行することによっても実現される。即ち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ等）がプログラムを読み出して実行する処理である。

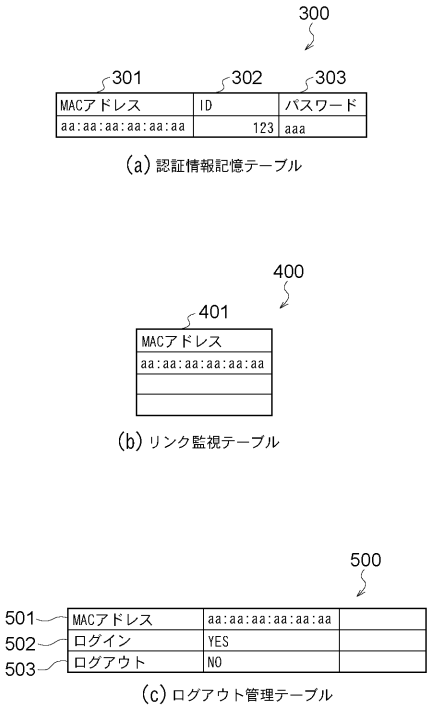
【図１】


ネットワーク
106
認証サーバ
105
端末管理装置
108
端末管理装置
107
AP
104
AP
103
無線スポット
102
STA
101
無線スポット
STA
100
100
移動

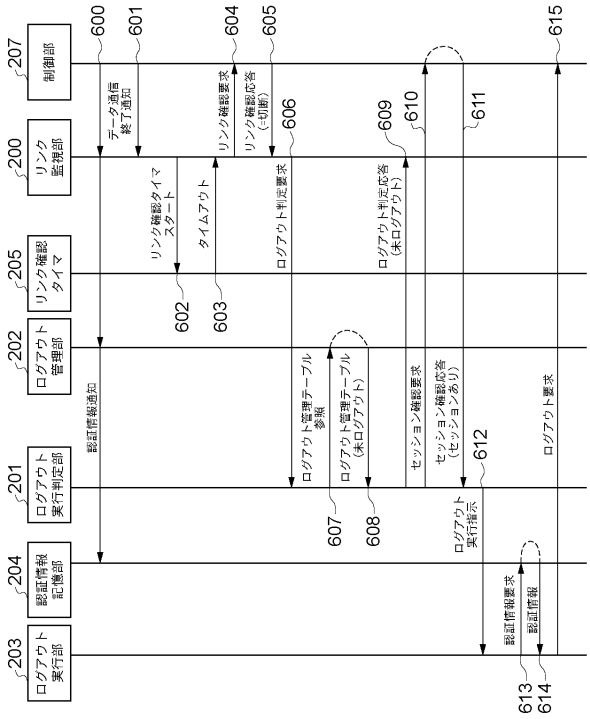
【図２】


107,108
制御部
207
200
205
リンク確認タイマ
209
212
リンク監視部
220
208
213
有線I/F
206
214
223
201
ログアウト実行判定部
222
221
217
215
216
ログアウト管理部
211
202
ログアウト実行部
219
203
224
218
認証情報記憶部
210
204

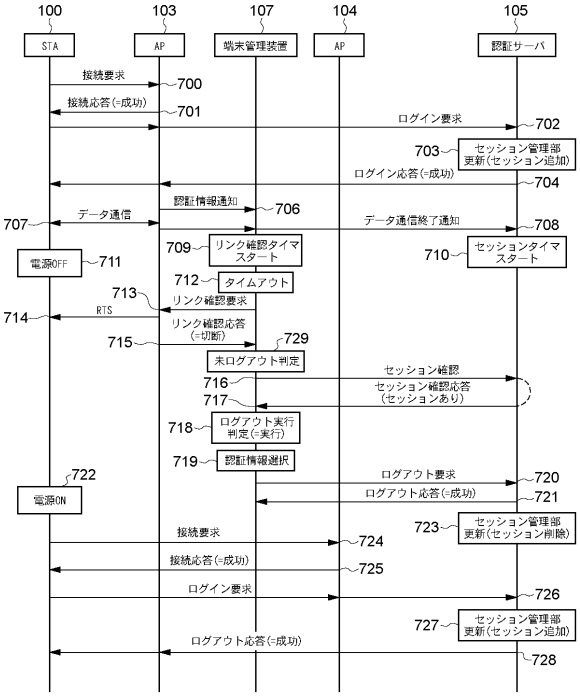
【図３】


300
301
302
303
MACアドレス
ID
パスワード
aa:aa:aa:aa:aa:aa
123
aaa
(a) 認証情報記憶テーブル
400
401
MACアドレス
aa:aa:aa:aa:aa:aa
(b) リンク監視テーブル
500
501
502
503
MACアドレス
ログイン
ログアウト
aa:aa:aa:aa:aa:aa
YES
NO
(c) ログアウト管理テーブル

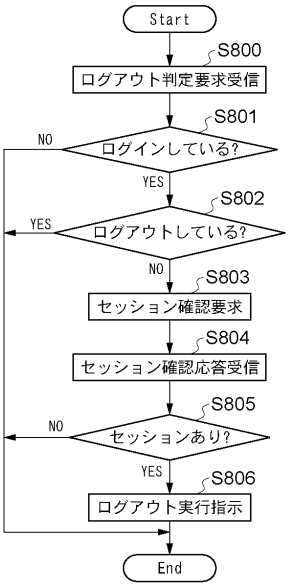
【図４】


207
制御部
200
リンク監視部
205
リンク確認タイマ
202
ログアウト管理部
201
ログアウト実行判定部
204
認証情報記憶部
203
ログアウト実行部
600
601
604
605
615
606
609
610
611
612
602
603
607
608
613
614
データ通信終了通知
リンク確認要求
リンク確認応答(切断)
リンク確認タイマスタート
タイムアウト
ログアウト判定要求
ログアウト判定応答(未ログアウト)
認証情報通知
ログアウト管理テーブル参照
ログアウト管理テーブル(未ログアウト)
セッション確認要求
セッション確認応答(セッションあり)
ログアウト要求
ログアウト実行指示
認証情報要求
認証情報

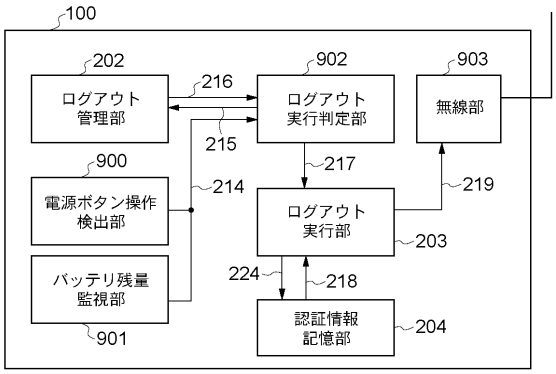
【図５】


100
STA
103
AP
107
端末管理装置
104
AP
105
認証サーバ
接続要求
700
接続応答(=成功)
701
ログイン要求
702
703
セッション管理部
更新(セッション追加)
ログイン応答(=成功)
704
認証情報通知
706
データ通信
707
データ通信終了通知
708
709
リンク確認タイマ
スタート
710
セッションタイマ
スタート
電源OFF
711
712
タイムアウト
713
リンク確認要求
RTS
714
リンク確認応答
(=切断)
715
729
未ログアウト判定
セッション確認
716
セッション確認応答
(セッションあり)
717
718
ログアウト実行
判定(=実行)
719
認証情報選択
ログアウト要求
720
ログアウト応答(=成功)
721
722
電源ON
723
セッション管理部
更新(セッション削除)
接続要求
724
接続応答(=成功)
725
ログイン要求
726
727
セッション管理部
更新(セッション追加)
ログアウト応答(=成功)
728

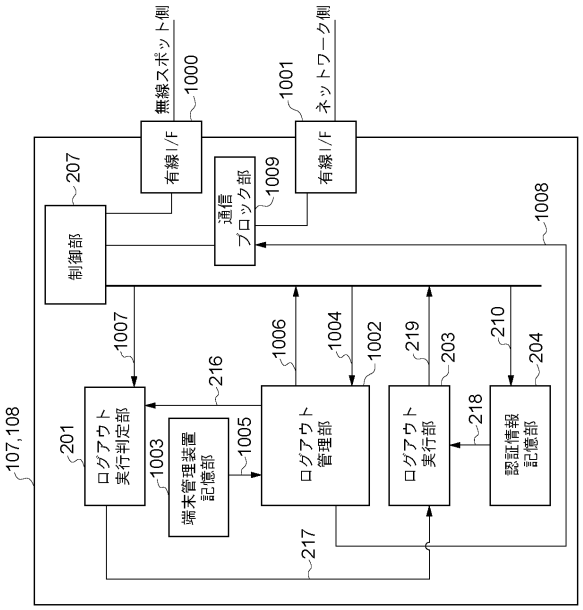
【図６】


Start
S800
ログアウト判定要求受信
S801
ログインしている?
NO
YES
S802
ログアウトしている?
YES
NO
S803
セッション確認要求
S804
セッション確認応答受信
S805
セッションあり?
NO
YES
S806
ログアウト実行指示
End

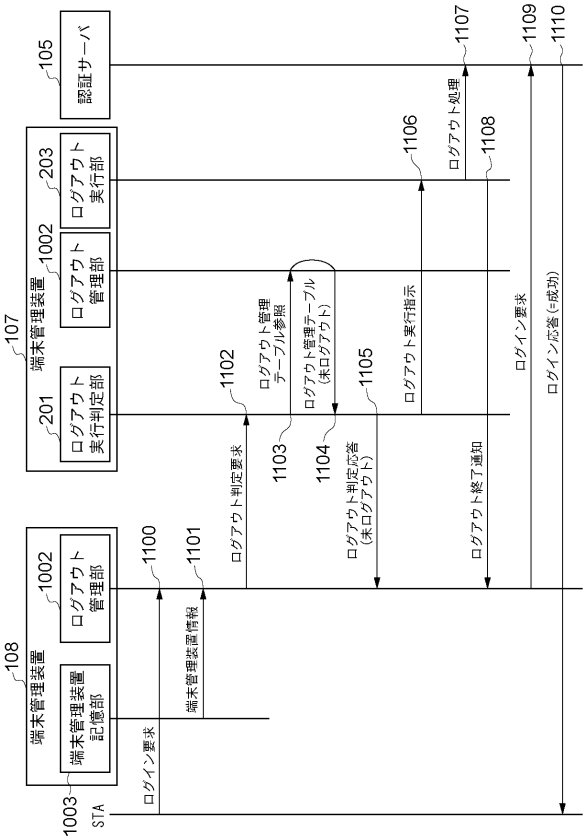
【図７】


100
202
ログアウト
管理部
216
902
ログアウト
実行判定部
903
無線部
215
900
電源ボタン操作
検出部
214
217
ログアウト
実行部
219
203
バッテリ残量
監視部
224
218
901
認証情報
記憶部
204

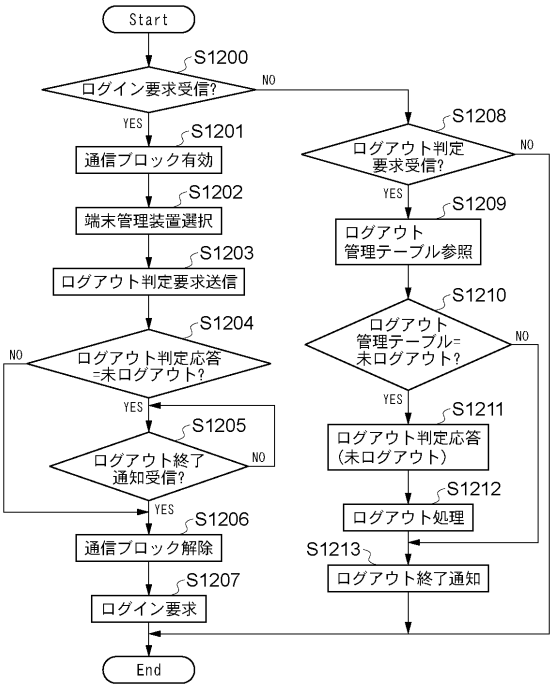
【図８】


無線スポット側
1000
1001
ネットワーク側
有線I/F
有線I/F
207
通信
ブロック部
1009
1008
制御部
1007
1006
1004
1002
219
203
210
204
216
218
107,108
201
ログアウト
実行判定部
1003
端末管理装置
記憶部
1005
ログアウト
管理部
ログアウト
実行部
認証情報
記憶部
217

【図９】


105
認証サーバ
107
端末管理装置
203
ログアウト実行部
1002
ログアウト管理部
201
ログアウト実行判定部
108
端末管理装置
1002
ログアウト管理部
端末管理装置記憶部
1003
STA
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
ログイン要求
端末管理装置情報
ログアウト判定要求
ログアウト管理テーブル参照
ログアウト管理テーブル(未ログアウト)
ログアウト判定応答(未ログアウト)
ログアウト実行指示
ログアウト終了通知
ログアウト処理
ログイン要求
ログイン応答(=成功)

【図１０】


Start
S1200
ログイン要求受信?
NO
YES
S1201
通信ブロック有効
S1202
端末管理装置選択
S1203
ログアウト判定要求送信
S1204
ログアウト判定応答=未ログアウト?
NO
YES
S1205
ログアウト終了通知受信?
NO
YES
S1206
通信ブロック解除
S1207
ログイン要求
S1208
ログアウト判定要求受信?
NO
YES
S1209
ログアウト管理テーブル参照
S1210
ログアウト管理テーブル=未ログアウト?
NO
YES
S1211
ログアウト判定応答(未ログアウト)
S1212
ログアウト処理
S1213
ログアウト終了通知
End

フロントページの続き

(72)発明者　七野　隆広
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　金木　陽一

(56)参考文献　特開２００４－１６４５７６（ＪＰ，Ａ）
特開２００６－２６８６７１（ＪＰ，Ａ）
特開２００７－０８００８６（ＪＰ，Ａ）
こうしてトラブルに打ち勝つ！　実践事例編，Windows Server World，２００４年　６月，Vol. 9，No. 6，pp. 72-84

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４５
Ｇ０６Ｆ　１３／００
Ｈ０４Ｗ　１２／０６
Ｈ０４Ｗ　８４／１２
Ｇ０６Ｆ　２１／４４