

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5573113号
(P5573113)

(45) 発行日 平成26年8月20日 (2014. 8. 20)

(24) 登録日 平成26年7月11日 (2014. 7. 11)

(51) Int. Cl.

F 1

G 0 6 F 21/31 (2013.01)

G 0 6 F 21/20 1 3 1 A

請求項の数 4 (全 15 頁)

(21) 出願番号	特願2009-256377 (P2009-256377)	(73) 特許権者	000004237
(22) 出願日	平成21年11月9日 (2009. 11. 9)		日本電気株式会社
(65) 公開番号	特開2011-100411 (P2011-100411A)		東京都港区芝五丁目7番1号
(43) 公開日	平成23年5月19日 (2011. 5. 19)	(74) 代理人	100106909
審査請求日	平成24年10月5日 (2012. 10. 5)		弁理士 棚井 澄雄
		(74) 代理人	100134544
			弁理士 森 隆一郎
		(74) 代理人	100150197
			弁理士 松尾 直樹
		(72) 発明者	朴 松蘭
			東京都港区芝五丁目7番1号 日本電気株式会社内
		審査官	脇岡 剛

最終頁に続く

(54) 【発明の名称】 認証代行サーバ装置、認証代行方法及びプログラム

(57) 【特許請求の範囲】

【請求項 1】

認証処理を行う認証サーバ装置による認証処理を代行する認証代行サーバ装置であって、

クライアント装置から、当該クライアント装置のユーザを識別する識別情報を含む認証情報を受信する認証情報受信部と、

接続を許可するユーザの認証情報と当該ユーザの権限を示す権限情報とを関連付けて記憶する記憶部が記憶している認証情報と、前記認証情報受信部が受信した認証情報とが一致するか否かを判定する判定部と、

前記記憶部から前記認証情報受信部が受信した認証情報に含まれる前記識別情報に関連付けられた権限情報を読み出す権限情報読出部と、

前記判定部によって認証情報が一致すると判定され、かつ前記権限情報読出部によって読み出された権限情報が所定の権限を示す場合に、前記ユーザの認証に成功したと判定する認証部と、

前記認証情報受信部が受信した認証情報に含まれる識別情報が、前記記憶部が記憶する認証情報に含まれていない場合、前記認証情報受信部が受信した認証情報を前記認証サーバ装置に転送する認証情報転送部と、

前記認証情報転送部が転送した認証情報が前記認証サーバ装置によって認証されたか否かを示す認証結果情報を前記認証サーバ装置から受信する認証結果情報受信部と、

前記認証サーバ装置が前記認証情報に含まれる識別情報に関連付けて記憶する権限情報

10

20

を、前記認証サーバ装置から受信する権限情報受信部と、

前記認証結果情報受信部が受信した認証結果情報が認証成功を示す場合に、前記認証情報受信部が受信した認証情報と前記権限情報受信部が受信した権限情報とを関連付けて前記記憶部に書き込む書込部と

を備えることを特徴とする認証代行サーバ装置。

【請求項 2】

前記認証サーバ装置に応答要求を送信する応答要求送信部と、

前記認証部は、前記応答要求送信部が送信した応答要求に対する応答が無い場合において、前記判定部によって認証情報が一致すると判定され、かつ前記権限情報読出部によって読み出された権限情報が所定の権限を示すときに、前記ユーザの認証に成功したと判定する

10

ことを特徴とする請求項 1 に記載の認証代行サーバ装置。

【請求項 3】

認証処理を行う認証サーバ装置による認証処理を代行する認証代行サーバ装置を用いた認証代行方法であって、

認証情報受信部は、クライアント装置から、当該クライアント装置のユーザを識別する識別情報を含む認証情報を受信し、

判定部は、接続を許可するユーザの認証情報と当該ユーザの権限を示す権限情報とを関連付けて記憶する記憶部が記憶している認証情報と、前記認証情報受信部が受信した認証情報とが一致するか否かを判定し、

20

権限情報読出部は、前記記憶部から前記認証情報受信部が受信した認証情報に含まれる前記識別情報に関連付けられた権限情報を読み出し、

認証部は、前記判定部によって認証情報が一致すると判定され、かつ前記権限情報読出部によって読み出された権限情報が所定の権限を示す場合に、前記ユーザの認証に成功したと判定し、

認証情報転送部は、前記認証情報受信部が受信した認証情報に含まれる識別情報が、前記記憶部が記憶する認証情報に含まれていない場合、前記認証情報受信部が受信した認証情報を前記認証サーバ装置に転送し、

認証結果情報受信部は、前記認証情報転送部が転送した認証情報が前記認証サーバ装置によって認証されたか否かを示す認証結果情報を前記認証サーバ装置から受信し、

30

権限情報受信部は、前記認証サーバ装置が前記認証情報に含まれる識別情報に関連付けて記憶する権限情報を、前記認証サーバ装置から受信し、

書込部は、前記認証結果情報受信部が受信した認証結果情報が認証成功を示す場合に、前記認証情報受信部が受信した認証情報と前記権限情報受信部が受信した権限情報とを関連付けて前記記憶部に書き込む

ことを特徴とする認証代行方法。

【請求項 4】

認証処理を行う認証サーバ装置による認証処理を代行する認証代行サーバ装置を、

クライアント装置から、当該クライアント装置のユーザを識別する識別情報を含む認証情報を受信する認証情報受信部、

40

接続を許可するユーザの認証情報と当該ユーザの権限を示す権限情報とを関連付けて記憶する記憶部が記憶している認証情報と、前記認証情報受信部が受信した認証情報とが一致するか否かを判定する判定部、

前記記憶部から前記認証情報受信部が受信した認証情報に含まれる前記識別情報に関連付けられた権限情報を読み出す権限情報読出部、

前記判定部によって認証情報が一致すると判定され、かつ前記権限情報読出部によって読み出された権限情報が所定の権限を示す場合に、前記ユーザの認証に成功したと判定する認証部、

前記認証情報受信部が受信した認証情報に含まれる識別情報が、前記記憶部が記憶する認証情報に含まれていない場合、前記認証情報受信部が受信した認証情報を前記認証サー

50

バ装置に転送する認証情報転送部、

前記認証情報転送部が転送した認証情報が前記認証サーバ装置によって認証されたか否かを示す認証結果情報を前記認証サーバ装置から受信する認証結果情報受信部、

前記認証サーバ装置が前記認証情報に含まれる識別情報に関連付けて記憶する権限情報を、前記認証サーバ装置から受信する権限情報受信部、

前記認証結果情報受信部が受信した認証結果情報が認証成功を示す場合に、前記認証情報受信部が受信した認証情報と前記権限情報受信部が受信した権限情報とを関連付けて前記記憶部に書き込む書込部

として機能させるためのプログラム。

【発明の詳細な説明】

10

【技術分野】

【0001】

本発明は、認証処理を行う認証サーバ装置による認証処理を代行する認証代行サーバ装置、認証代行方法及びプログラムに関する。

【背景技術】

【0002】

従来、PC (Personal Computer) 等のクライアント装置をネットワークに接続する場合、当該クライアント装置は、ISP (Internet Services Provider) 等のネットワークサービスプロバイダの認証システムにより、ネットワークへの接続を許可するか否かを判定する認証処理を受ける。この認証処理は、一般的にRADIUS (Remote Authentication Dial In User Service) プロトコルによるものが用いられている。

20

【0003】

RADIUSを用いた無線LAN (Local Area Network) への接続の認証処理は、以下のように行われる。

まず、クライアント装置は、アクセスポイント装置を介して、ユーザ名とパスワードとの組み合わせなどで示される認証情報を含むアクセス要求を認証サーバ装置に送信する。次に、認証サーバ装置は、受信したアクセス要求に含まれる認証情報と予め記憶する認証情報とが一致するか否かを検証し、クライアント装置の認証処理を行う。そして、認証サーバ装置は、クライアント装置が接続するアクセスポイント装置に認証処理の結果を示す認証結果情報を含む応答パケットを送信する。応答パケットを受信したアクセスポイント装置は、当該認証結果情報が「接続許可」を示す場合、クライアント装置にネットワークへの接続を許可する。

30

【0004】

しかし、上述した認証方法を用いた場合、アクセスポイント装置は、クライアント装置による認証要求毎に、認証サーバ装置に対してアクセス要求を送信することとなる。そのため、無線通信の劣化などによりパケットの損失が生じる可能性があり、認証処理に時間が掛かってしまうという問題があった。

そこで、アクセスポイント装置と認証サーバ装置との間に設けたプロキシサーバ装置に、一時的にサーバ装置が記憶する認証情報を蓄積させ、プロキシサーバ装置にて認証を代行するという方法が特許文献1に開示されている。当該認証方法は、以下のように行われる。ここでは、アクセスポイント装置にプロキシサーバ装置を実装した例を用いて説明を行う。

40

【0005】

まず、クライアント装置がアクセスポイント装置にアクセス要求を送信すると、アクセスポイント装置は、受信したアクセス要求に含まれるユーザ名を含む認証情報を、自装置の記憶部に記憶しているか否かをチェックする。

クライアント装置による初回の認証時には、アクセスポイント装置の記憶部は認証情報を記憶していないため、当該アクセス要求を認証サーバ装置に転送し、認証サーバ装置から認証結果情報を受信する。そして、受信した認証結果情報が「認証成功」を示す場合、

50

アクセスポイント装置は、クライアント装置から受信したアクセス要求に含まれる認証情報を記憶部に書き込み、クライアント装置にネットワークへの接続を許可する。

【0006】

他方、同一のクライアント装置による2回目以降の認証時には、アクセスポイント装置は、初回の認証時の処理により、当該クライアント装置の認証情報を記憶している。この場合、アクセスポイント装置は、受信したアクセス要求に含まれる認証情報と記憶部が記憶する認証情報とが一致するか否かを検証することで、クライアント装置の認証処理を行う。そして、認証情報が一致すると判定した場合、アクセスポイント装置は、クライアント装置にネットワークへの接続を許可する。

これにより、アクセスポイント装置は、同一のアクセスポイント装置に接続したことがあるユーザに対する認証を行う際に、認証サーバ装置へのアクセスを行わないため、認証処理にかかる時間を短縮することができる。

10

【0007】

なお、このような認証システムでは、認証サーバ装置が認証情報の変更または削除を行った場合に、その変更または削除に係る認証情報を用いたネットワーク接続が、アクセスポイント装置で保存されている認証情報により許可されることを防ぐため、認証サーバ装置は、アクセスポイント装置が記憶する認証情報の削除を定期的に行う必要がある。

【先行技術文献】

【特許文献】

【0008】

20

【特許文献1】国際公開第2004/112312号パンフレット

【発明の概要】

【発明が解決しようとする課題】

【0009】

しかしながら、上述した認証システムでは、認証サーバ装置によってアクセスポイント装置（プロキシサーバ装置）が記憶する認証情報の削除を行うため、認証サーバ装置が動作停止状態に陥った場合、アクセスポイント装置が記憶する認証情報の削除がなされず、認証サーバ装置で変更または削除を行った認証情報を用いたネットワーク接続が許可されてしまう恐れがある。この問題は、認証サーバ装置が動作停止状態に陥った場合にアクセスポイント装置またはプロキシサーバ装置による認証を行わないことで回避することができるが、一般のユーザだけでなく、ネットワーク管理者などのユーザもネットワークに接続できなくなってしまうという問題があった。

30

【0010】

本発明は、上記の問題に鑑みてなされたものであり、認証サーバ装置が動作停止状態に陥った場合に、認証サーバ装置で変更または削除を行った認証情報を用いたネットワーク接続を許可せず、特定のユーザによるネットワーク接続を許可する認証代行サーバ装置、認証代行方法及びプログラムを提供することを課題とする。

【課題を解決するための手段】

【0011】

本発明は上記の課題を解決するためになされたものであり、認証処理を行う認証サーバ装置による認証処理を代行する認証代行サーバ装置であって、クライアント装置から、当該クライアント装置のユーザを識別する識別情報を含む認証情報を受信する認証情報受信部と、接続を許可するユーザの認証情報と当該ユーザの権限を示す権限情報とを関連付けて記憶する記憶部が記憶している認証情報と、前記認証情報受信部が受信した認証情報とが一致するか否かを判定する判定部と、前記記憶部から前記認証情報受信部が受信した認証情報に含まれる前記識別情報に関連付けられた権限情報を読み出す権限情報読出部と、前記判定部によって認証情報が一致すると判定され、かつ前記権限情報読出部によって読み出された権限情報が所定の権限を示す場合に、前記ユーザの認証に成功したと判定する認証部と、前記認証情報受信部が受信した認証情報に含まれる識別情報が、前記記憶部が記憶する認証情報に含まれていない場合、前記認証情報受信部が受信した認証情報を前記

40

50

認証サーバ装置に転送する認証情報転送部と、前記認証情報転送部が転送した認証情報が前記認証サーバ装置によって認証されたか否かを示す認証結果情報を前記認証サーバ装置から受信する認証結果情報受信部と、前記認証サーバ装置が前記認証情報に含まれる識別情報に関連付けて記憶する権限情報を、前記認証サーバ装置から受信する権限情報受信部と、前記認証結果情報受信部が受信した認証結果情報が認証成功を示す場合に、前記認証情報受信部が受信した認証情報と前記権限情報受信部が受信した権限情報とを関連付けて前記記憶部書き込む書込部とを備えることを特徴とする。

【0012】

また、本発明は、認証処理を行う認証サーバ装置による認証処理を代行する認証代行サーバ装置を用いた認証代行方法であって、認証情報受信部は、クライアント装置から、当該クライアント装置のユーザを識別する識別情報を含む認証情報を受信し、判定部は、接続を許可するユーザの認証情報と当該ユーザの権限を示す権限情報とを関連付けて記憶する記憶部が記憶している認証情報と、前記認証情報受信部が受信した認証情報とが一致するか否かを判定し、権限情報読出部は、前記記憶部から前記認証情報受信部が受信した認証情報に含まれる前記識別情報に関連付けられた権限情報を読み出し、認証部は、前記判定部によって認証情報が一致すると判定され、かつ前記権限情報読出部によって読み出された権限情報が所定の権限を示す場合に、前記ユーザの認証に成功したと判定し、認証情報転送部は、前記認証情報受信部が受信した認証情報に含まれる識別情報が、前記記憶部が記憶する認証情報に含まれていない場合、前記認証情報受信部が受信した認証情報を前記認証サーバ装置に転送し、認証結果情報受信部は、前記認証情報転送部が転送した認証情報が前記認証サーバ装置によって認証されたか否かを示す認証結果情報を前記認証サーバ装置から受信し、権限情報受信部は、前記認証サーバ装置が前記認証情報に含まれる識別情報に関連付けて記憶する権限情報を、前記認証サーバ装置から受信し、書込部は、前記認証結果情報受信部が受信した認証結果情報が認証成功を示す場合に、前記認証情報受信部が受信した認証情報と前記権限情報受信部が受信した権限情報とを関連付けて前記記憶部書き込むことを特徴とする。

【0013】

また、本発明は、認証処理を行う認証サーバ装置による認証処理を代行する認証代行サーバ装置を、クライアント装置から、当該クライアント装置のユーザを識別する識別情報を含む認証情報を受信する認証情報受信部、接続を許可するユーザの認証情報と当該ユーザの権限を示す権限情報とを関連付けて記憶する記憶部が記憶している認証情報と、前記認証情報受信部が受信した認証情報とが一致するか否かを判定する判定部、前記記憶部から前記認証情報受信部が受信した認証情報に含まれる前記識別情報に関連付けられた権限情報を読み出す権限情報読出部、前記判定部によって認証情報が一致すると判定され、かつ前記権限情報読出部によって読み出された権限情報が所定の権限を示す場合に、前記ユーザの認証に成功したと判定する認証部、前記認証情報受信部が受信した認証情報に含まれる識別情報が、前記記憶部が記憶する認証情報に含まれていない場合、前記認証情報受信部が受信した認証情報を前記認証サーバ装置に転送する認証情報転送部、前記認証情報転送部が転送した認証情報が前記認証サーバ装置によって認証されたか否かを示す認証結果情報を前記認証サーバ装置から受信する認証結果情報受信部、前記認証サーバ装置が前記認証情報に含まれる識別情報に関連付けて記憶する権限情報を、前記認証サーバ装置から受信する権限情報受信部、前記認証結果情報受信部が受信した認証結果情報が認証成功を示す場合に、前記認証情報受信部が受信した認証情報と前記権限情報受信部が受信した権限情報とを関連付けて前記記憶部書き込む書込部として機能させるためのプログラムである。

【発明の効果】

【0014】

本発明によれば、認証代行サーバ装置は、ユーザの権限が所定の権限を示し、かつ記憶部が記憶している認証情報とクライアント装置から受信した認証情報とが一致する場合に、ユーザの認証に成功したと判定する。これにより、認証代行サーバ装置によって、認証

10

20

30

40

50

装置で変更または削除を行った認証情報を用いたネットワーク接続を許可することを防ぐことができ、かつ、所定の権限を有するユーザによるネットワークへの接続を確保することができる。

【図面の簡単な説明】

【0015】

【図1】本発明の一実施形態による認証システムの構成を示す概略ブロック図である。

【図2】本発明の一実施形態によるアクセスポイント装置の構成を示す概略ブロック図である。

【図3】アクセスポイント装置による定期動作を示すフローチャートである。

【図4】アクセスポイント装置による認証動作を示すフローチャートである。

【図5】ネットワークへの初回の接続時における認証システムの動作を示すシーケンス図である。

【図6】ネットワークへの2回目以降の接続時における認証システムの動作を示すシーケンス図である。

【図7】認証サーバ装置の動作停止時における認証システムの動作を示すシーケンス図である。

【発明を実施するための形態】

【0016】

以下、図面を参照しながら本発明の実施形態について詳しく説明する。

図1は、本発明の一実施形態による認証システムの構成を示す概略ブロック図である。

図1に示す認証システムは、アクセスポイント装置2（認証代行サーバ装置）、プロキシサーバ装置3、認証サーバ装置4を備える。アクセスポイント装置2とプロキシサーバ装置3とは無線で接続され、プロキシサーバ装置3と認証サーバ装置4とは有線で接続されている。また、クライアント装置1は、アクセスポイント装置2に無線で接続されている。

クライアント装置1は、ユーザが操作する端末装置であり、ユーザを特定するユーザ名（識別情報）とパスワードの組を示す認証情報を含むパケットを送信し、ネットワークへの接続を要求する。

アクセスポイント装置2は、認証情報を含むパケットをプロキシサーバ装置3に転送し、その応答パケットに基づいてクライアント装置1を無線LANに接続するか否かを判定する。また、同一のクライアント装置1による2回目以降の接続時は、認証サーバ装置4に代わって認証処理を行う。

プロキシサーバ装置3は、アクセスポイント装置2から受信したパケットを認証サーバ装置4に転送し、認証サーバ装置4から受信した応答パケットをアクセスポイント装置2に転送する。

認証サーバ装置4は、プロキシサーバ装置3から認証情報を含むパケットを受信し、ユーザの認証処理を行い、その結果を示す応答パケットをプロキシサーバ装置3に送信する。

【0017】

図2は、本発明の一実施形態によるアクセスポイント装置の構成を示す概略ブロック図である。

アクセスポイント装置2は、クライアント側通信部21（認証情報受信部）、転送判定部22、サーバ側通信部23（応答要求送信部、認証情報転送部、認証結果情報受信部、権限情報受信部）、書込部24、記憶部25、認証部26（判定部、権限情報読出部）を備える。

クライアント側通信部21は、クライアント装置1からアクセス要求パケットを受信し、また、クライアント装置1にネットワークへの接続の可否を示す応答パケットを送信する。

転送判定部22は、クライアント装置1から受信した情報を認証サーバ装置4に転送するか否かを判定する。

サーバ側通信部 23 は、クライアント側通信部 21 が受信したアクセス要求パケットを、プロキシサーバ装置 3 を介して認証サーバ装置 4 に送信し、その認証結果を示す応答パケットを受信する。また、サーバ側通信部 23 は、認証サーバ装置 4 が動作しているか否かを判定するために認証サーバ装置 4 へアクセス要求パケット（応答要求）を送信し、応答の有無を判定する。

書込部 24 は、記憶部 25 にクライアント装置 1 のユーザを特定する認証情報、及び認証サーバ装置 4 の状態を示す状態情報を書き込む。

認証部 26 は、クライアント側通信部 21 が受信したアクセス要求パケットに含まれる認証情報と記憶部 25 が記憶する認証情報とに基づいてクライアント装置 1 のユーザの認証を行う。

10

【0018】

そして、アクセスポイント装置 2 のクライアント側通信部 21 は、クライアント装置 1 から、クライアント装置 1 のユーザを識別するユーザ名を含む認証情報を受信する。次に、認証部 26 は、接続を許可するユーザの認証情報と当該ユーザの権限を示す権限情報とを関連付けて記憶する記憶部 25 が記憶している認証情報と、クライアント側通信部 21 が受信した認証情報とが一致するか否かを判定する。また、認証部 26 は、記憶部 25 からクライアント側通信部 21 が受信した認証情報に含まれるユーザ名に関連付けられた権限情報を読み出す。そして、認証部 26 は、認証情報が一致すると判定し、かつ読み出した権限情報が所定の権限を示す場合に、ユーザの認証に成功したと判定する。

これにより、アクセスポイント装置 2 は、認証サーバ装置が動作停止状態に陥った場合に、認証サーバ装置で変更または削除を行った認証情報を用いたネットワーク接続を許可せず、特定のユーザによるネットワーク接続を許可する。

20

【0019】

次に、アクセスポイント装置 2 の動作を説明する。

本実施形態によるアクセスポイント装置 2 は、認証サーバ装置 4 が動作しているか否かによって異なる処理を行うため、定期的に認証サーバ装置 4 の動作状態を確認する。そのため、まずアクセスポイント装置 2 が定期的に認証サーバ装置 4 の動作状態を確認する動作について説明する。

【0020】

図 3 は、アクセスポイント装置による定期動作を示すフローチャートである。

30

アクセスポイント装置 2 のサーバ側通信部 23 は、プロキシサーバ装置 3 を介して定期的に（例えば、12 時間毎に）アクセス要求を認証サーバ装置 4 に送信する（ステップ S1）。次に、アクセスポイント装置 2 は、当該アクセス要求に対する認証サーバ装置 4 からの応答を所定の時間の間待機する（ステップ S2）。

【0021】

所定の時間の待機を終了すると、サーバ側通信部 23 は、待機している間に認証サーバ装置 4 からの応答を受信したか否かを判定する（ステップ S3）。サーバ側通信部 23 が応答を受信したと判定した場合（ステップ S3：YES）、書込部 24 は、記憶部 25 が記憶する認証サーバ装置 4 の状態情報を、「稼動状態」に書き換える（ステップ S4）。他方、サーバ側通信部 23 が応答を受信していないと判定した場合（ステップ S3：NO）、書込部 24 は、記憶部 25 が記憶する認証サーバ装置 4 の状態情報を、「動作停止状態」に書き換える（ステップ S5）。

40

この処理を定期的に実行することにより、アクセスポイント装置 2 は、記憶部 25 が記憶する認証サーバ装置 4 の動作状態を示す状態情報を更新する。

【0022】

次に、クライアント装置 1 が認証情報を送信したときのアクセスポイント装置 2 の動作を説明する。

図 4 は、アクセスポイント装置による認証動作を示すフローチャートである。

まず、クライアント装置 1 が、ネットワークに接続するためにアクセスポイント装置に認証情報を示すパケットを送信すると、アクセスポイント装置 2 のクライアント側通信部

50

21は、当該認証情報を示すパケットを受信する（ステップS11）。次に、アクセスポイント装置2の転送判定部22は、記憶部25が記憶する状態情報が「動作停止状態」であるか否かを判定する（ステップS12）。

【0023】

転送判定部22は、状態情報が「稼動状態」とであると判定した場合（ステップS12：NO）、クライアント側通信部21が受信した認証情報に含まれるユーザ名が、記憶部25に登録されている認証情報の中に含まれるか否かを判定する（ステップS13）。

転送判定部22が、クライアント側通信部21が受信した認証情報に含まれるユーザ名が、認証情報の中に含まれないと判定した場合（ステップS13：NO）、サーバ側通信部23は、プロキシサーバ装置3を介して認証サーバ装置4にアクセス要求を示すRADIUSパケットを送信する（ステップS14）。 10

【0024】

アクセスポイント装置2がアクセス要求を示すRADIUSパケットを送信すると、認証サーバ装置4は、当該パケットを受信する。そして、認証サーバ装置4は、アクセス要求に対する応答として、認証情報の要求を示すRADIUSパケットをアクセスポイント装置2に送信する。

次に、アクセスポイント装置2のサーバ側通信部23は、認証情報の要求を示すRADIUSパケットを受信する（ステップS15）。そして、サーバ側通信部23は、認証情報の要求に対する応答として、クライアント側通信部21が受信した認証情報を示すRADIUSパケットを、プロキシサーバ装置3を介して認証サーバ装置4に送信する（ステップS16）。 20

【0025】

そして、認証サーバ装置4は、当該パケットを受信し、自装置の記憶部（図示せず）が記憶する認証情報と受信したパケットに含まれる認証情報とを比較して認証処理を行う。そして、認証サーバ装置4は、認証結果情報（「認証成功」または「認証失敗」）を示すRADIUSパケットをアクセスポイント装置2に送信する。

次に、アクセスポイント装置2のサーバ側通信部23は、認証結果情報を示すRADIUSパケットを受信する（ステップS17）。そして、認証部26は、受信したパケットが示す認証結果情報が「認証成功」を示すか否かを判定する（ステップS18）。 30

【0026】

認証部26が、認証結果情報が「認証失敗」を示すと判定した場合（ステップS18：NO）、クライアント側通信部21は、ネットワークへの接続の拒否を示す応答パケットをクライアント装置1に送信する（ステップS19）。

他方、認証部26が、認証結果情報が「認証成功」を示すと判定した場合（ステップS18：YES）、サーバ側通信部23は、クライアント側通信部21が受信した認証情報のユーザ名に関連付けられた権限情報（例えば、管理者ユーザ、デバッグユーザ、一般ユーザ、制限付きユーザなど）の送信要求を示すパケットを認証サーバ装置4に送信する（ステップS20）。ここで、権限情報とは、無線装置に対する操作を行う際の権限を示す情報であり、例えば、管理者ユーザとは、無線装置のMIB（管理情報ベース：Management Information Base）情報の書き換えを行うことのできるユーザのことである。 40

次に、認証サーバ装置4は、アクセスポイント装置2からの送信要求を受信し、受信した送信要求に含まれるユーザ名に関連付けられた権限情報を、自装置の記憶部（図示せず）から読み出し、当該権限情報を示すパケットをアクセスポイント装置2に送信する。

【0027】

次に、アクセスポイント装置2のサーバ側通信部23は、認証サーバ装置4から当該パケットを受信する（ステップS21）。サーバ側通信部23が権限情報を示すパケットを受信すると、書込部24は、クライアント側通信部21が受信した認証情報に関連付けて、サーバ側通信部23が受信した権限情報を記憶部25に書き込む（ステップS22）。そして、クライアント側通信部21は、ネットワークへの接続の許可を示す応答パケット 50

を送信する（ステップS 2 3）。

【0028】

他方、ステップS 1 3で、転送判定部2 2が、クライアント側通信部2 1が受信した認証情報に含まれるユーザ名が、認証情報の中に含まれると判定した場合（ステップS 1 3：YES）、認証部2 6は、記憶部2 5が記憶する認証情報の中にクライアント側通信部2 1が受信した認証情報と一致するものが存在するか否かを判定する（ステップS 2 4）。

認証部2 6が、記憶部2 5が記憶する認証情報の中にクライアント側通信部2 1が受信した認証情報と一致するものが存在すると判定した場合（ステップS 2 4：YES）、クライアント側通信部2 1は、ネットワークへの接続の許可を示す応答パケットをクライアント装置1に送信する（ステップS 2 5）。

10

他方、認証部2 6が、記憶部2 5が記憶する認証情報の中にクライアント側通信部2 1が受信した認証情報と一致するものが存在しないと判定した場合（ステップS 2 4：NO）、クライアント側通信部2 1は、ネットワークへの接続の拒否を示す応答パケットをクライアント装置1に送信する（ステップS 2 6）。

【0029】

また、ステップS 1 2で、転送判定部2 2が、状態情報が「動作停止状態」として判定した場合（ステップS 1 2：YES）、認証部2 6は、クライアント側通信部2 1が受信した認証情報に含まれるユーザ名に関連付けられた権限情報を記憶部2 5から読み出す（ステップS 2 7）。次に、認証部2 6は、読み出した権限情報が管理者権限を示すか否かを判定する（ステップS 2 8）。なお、クライアント装置1が初回の認証時である場合や、前回の認証に失敗している場合には、受信した認証情報に含まれるユーザ名が記憶部2 5に記憶されていないこととなる。この場合、ステップS 2 8で、認証部2 6は、権限情報が管理者権限を示さないと判定して処理を続行する。

20

【0030】

認証部2 6は、読み出した権限情報が管理者権限を示すと判定した場合（ステップS 2 8：YES）、ステップS 2 4を実行し、認証処理を行う。これにより、アクセスポイント装置2は、管理者権限を有するユーザに対して、認証サーバ装置4が動作停止状態に陥った場合にも、認証に成功したときに、ネットワークへの接続を許可することができる。なお、管理者権限を有するユーザは、認証サーバ装置4の操作を行う場合に最低限必要なユーザであり、認証サーバ装置4において変更または削除がなされないものとする。

30

他方、認証部2 6が、読み出した権限情報が管理者権限を示さないと判定した場合（ステップS 2 8：NO）、クライアント側通信部2 1は、ネットワークへの接続の拒否を示す応答パケットを送信する（ステップS 2 6）。

【0031】

なお、認証サーバ装置4は、定期的にアクセスポイント装置2の記憶部2 5が記憶する認証情報の削除を要求するパケットを送信する。そして、アクセスポイント装置2のサーバ側通信部2 3が当該パケットを受信すると、書込部2 4は記憶部2 5が記憶する認証情報を全て削除する。これは、認証サーバ装置4が認証情報の変更または削除を行った場合に、その変更または削除に係る認証情報を用いたネットワーク接続が、アクセスポイント装置2の記憶部2 5が記憶している認証情報により許可されることを防ぐために行う処理である。

40

【0032】

次に、クライアント装置1による、ネットワークへの初回の接続時、2回目以降の接続時、及び認証サーバ装置4が動作停止状態時の認証システムの動作をそれぞれ説明する。

図5は、ネットワークへの初回の接続時における認証システムの動作を示すシーケンス図である。

まず、クライアント装置1は、認証情報を示すパケットをアクセスポイント装置2に送信する（ステップS 1 0 1）。アクセスポイント装置2は、認証情報を示すパケットを受信すると、上述したステップS 1 2により、認証サーバ装置4が動作停止状態であるか否

50

かを判定する動作状態チェック処理を行う（ステップS102）。ここでは、認証サーバ装置4は正常に動作しているため、アクセスポイント装置2の記憶部25が記憶する状態情報は「稼動状態」を示している。

【0033】

次に、アクセスポイント装置2は、上述したステップS13により、記憶部25が、受信した認証情報に含まれるユーザ名を記憶しているか否かを判定するユーザチェック処理を行う（ステップS103）。ここでは、初回の接続時であるため、記憶部25には該当するユーザ名は登録されていない。そのため、アクセスポイント装置2は、上述したステップS14により、プロキシサーバ装置3にアクセス要求を示すRADIUSパケットを送信する（ステップS104）。プロキシサーバ装置3は、受信したパケットを認証サーバ装置4に転送する（ステップS105）。 10

【0034】

認証サーバ装置4は、アクセス要求を示すRADIUSパケットを受信すると、認証情報の送信を要求するRADIUSパケットをプロキシサーバ装置3に送信する（ステップS106）。プロキシサーバ装置3は、受信したパケットをアクセスポイント装置2に転送する（ステップS107）。

アクセスポイント装置2は、認証情報の送信を要求するRADIUSパケットを受信すると、上述したステップS16により、クライアント装置1から受信した認証情報を示すRADIUSパケットをプロキシサーバ装置3に送信する（ステップS108）。プロキシサーバ装置3は、受信したパケットを認証サーバ装置4に転送する（ステップS109） 20

【0035】

認証サーバ装置4は、認証情報を示すRADIUSパケットを受信すると、受信した認証情報と記憶部に記憶されている認証情報とを比較して認証処理を行う（ステップS110）。そして、認証結果情報を示すRADIUSパケットをプロキシサーバ装置3に送信する（ステップS111）。プロキシサーバ装置3は、受信したパケットをアクセスポイント装置2に転送する（ステップS112）。

【0036】

アクセスポイント装置2は、認証結果情報を示すRADIUSパケットを受信すると、上述したステップS18により、当該認証結果情報が「認証成功」を示すか否かを判定する認証正否チェック処理を行う（ステップS113）。ここでは、認証結果情報が「認証成功」を示すものとする。 30

認証結果情報が「認証成功」を示す場合、アクセスポイント装置2は、上述したステップS20により、当該認証に成功したユーザの権限情報の送信を要求するパケットをプロキシサーバ装置3に送信する（ステップS114）。プロキシサーバ装置3は、受信したパケットを認証サーバ装置4に転送する（ステップS115）。

【0037】

認証サーバ装置4は、プロキシサーバ装置3から権限情報の送信を要求するパケットを受信すると、当該パケットに含まれるユーザ名に関連付けられた権限情報を記憶部から読み出し、当該権限情報を示すパケットをプロキシサーバ装置3に送信する（ステップS116）。プロキシサーバ装置3は、受信したパケットをアクセスポイント装置2に転送する（ステップS117）。 40

アクセスポイント装置2は、権限情報を示すパケットを受信すると、上述したステップS22により、ステップS101で受信した認証情報とステップS117で受信した権限情報とを関連付けて記憶部25に書き込む（ステップS118）。そして、アクセスポイント装置2は、上述したステップS23により、クライアント装置1にネットワークへの接続の可否を示す応答パケットを送信する（ステップS119）。

これにより、認証サーバ装置4で認証に成功したユーザの認証情報と権限情報とをアクセスポイント装置2の記憶部25に記憶させることができる。

【0038】

図6は、ネットワークへの2回目以降の接続時における認証システムの動作を示すシーケンス図である。

まず、クライアント装置1は、認証情報を示すパケットをアクセスポイント装置2に送信する(ステップS201)。アクセスポイント装置2は、認証情報を示すパケットを受信すると、上述したステップS12により、認証サーバ装置4が動作停止状態であるか否かを判定する動作状態チェック処理を行う(ステップS202)。ここでは、認証サーバ装置4は正常に動作しているため、アクセスポイント装置2の記憶部25が記憶する状態情報は「稼動状態」を示している。

【0039】

次に、アクセスポイント装置2は、上述したステップS13により、記憶部25が、受信した認証情報に含まれるユーザ名を記憶しているか否かを判定するユーザチェック処理を行う(ステップS203)。ここでは、同一のクライアント装置1による2回目以降の接続時であるため、記憶部25には該当するユーザ名は登録されている。そのため、アクセスポイント装置2は、上述したステップS24により、受信した認証情報と記憶部25に記憶されている認証情報とを比較して認証処理を行う(ステップS204)。

そして、アクセスポイント装置2は、認証結果に基づいて、ステップS25、またはステップS26により、クライアント装置1にネットワークへの接続の可否を示す応答パケットを送信する(ステップS205)。

これにより、アクセスポイント装置2は、クライアント装置1による2回目以降の認証時に、認証サーバ装置4に対してアクセス要求を送信しない。そのため、認証処理に要する時間を短縮することができる。

【0040】

図7は、認証サーバ装置の動作停止時における認証システムの動作を示すシーケンス図である。

まず、クライアント装置1は、認証情報を示すパケットをアクセスポイント装置2に送信する(ステップS301)。アクセスポイント装置2は、認証情報を示すパケットを受信すると、上述したステップS12により、認証サーバ装置4が動作停止状態であるか否かを判定する動作状態チェック処理を行う(ステップS202)。ここでは、認証サーバ装置4は動作を停止しているため、アクセスポイント装置2の記憶部25が記憶する状態情報は「動作停止状態」を示している。

【0041】

次に、アクセスポイント装置2は、上述したステップS28により、受信した認証情報に含まれるユーザ名に関連付けて記憶部25が記憶する権限情報のレベルを判定する権限チェック処理を行う(ステップS303)。ここでは、記憶部25が、受信した認証情報に含まれるユーザ名に関連付けて、管理者ユーザレベルの権限を示す権限情報を記憶しているものとする。そのため、アクセスポイント装置2は、上述したステップS24により、受信した認証情報と記憶部25に記憶されている認証情報とを比較して認証処理を行う(ステップS304)。

そして、アクセスポイント装置2は、認証結果に基づいて、ステップS25、またはステップS26により、クライアント装置1にネットワークへの接続の可否を示す応答パケットを送信する(ステップS305)。

【0042】

このように、本実施形態によれば、認証サーバ装置4が動作停止状態にあるときは、管理者権限を付与されたユーザによるネットワーク接続のみを許可することができる。そのため、アクセスポイント装置2によって、認証サーバ装置4で変更または削除を行った認証情報を用いたネットワーク接続を許可することを防ぐことができ、かつ、所定の権限を有するユーザによるネットワークへの接続を確保することができる。

【0043】

以上、図面を参照してこの発明の一実施形態について詳しく説明してきたが、具体的な構成は上述のものに限られることはなく、この発明の要旨を逸脱しない範囲内において様

10

20

30

40

50

々な設計変更等を行うことが可能である。

例えば、本実施形態では、アクセスポイント装置 2 が認証処理の代行を行う場合を説明したが、これに限られず、例えば、それぞれの処理部をプロキシサーバ装置 3 に格納し、プロキシサーバ装置が認証処理の代行を行っても良い。

【0044】

また、本実施形態では、認証サーバ装置とアクセスポイント装置 2 との間にプロキシサーバ装置 3 を 1 つ備える場合を説明したが、これに限られず、複数台のプロキシサーバ装置 3 を備えても良いし、プロキシサーバ装置 3 を備えない構成としても良い。

また、本実施形態では、認証サーバ装置 4 が動作停止状態にある場合に、権限情報が管理者権限を示すユーザのみ認証処理を行う場合を説明したが、これに限られず、例えば、管理者権限を示すユーザとデバッグユーザ権限を示すユーザに対して認証処理を行うようにしても良いし、管理者権限を示すユーザによって予め指定されたユーザに対しても認証処理を行うようにしても良い。

10

【0045】

なお、本実施形態では、認証プロトコルとして R A D I U S プロトコルを用いる場合を説明したが、これに限られず、他の認証プロトコルを用いても良い。

また、本実施形態では、認証システムを、無線 L A N によるネットワーク接続の認証に用いる認証システムに実装する例を説明したが、これに限られず、例えば、有線のネットワークへの接続の認証や、コンテンツ提供サービスにおける認証に用いる認証システムに実装しても良い。

20

【0046】

上述のアクセスポイント装置は内部に、コンピュータシステムを有している。そして、上述した各処理部の動作は、プログラムの形式でコンピュータ読み取り可能な記録媒体に記憶されており、このプログラムをコンピュータが読み出して実行することによって、上記処理が行われる。ここでコンピュータ読み取り可能な記録媒体とは、磁気ディスク、光磁気ディスク、C D - R O M、D V D - R O M、半導体メモリ等をいう。また、このコンピュータプログラムを通信回線によってコンピュータに配信し、この配信を受けたコンピュータが当該プログラムを実行するようにしても良い。

【0047】

また、上記プログラムは、前述した機能の一部を実現するためのものであっても良い。さらに、前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるもの、いわゆる差分ファイル（差分プログラム）であっても良い。

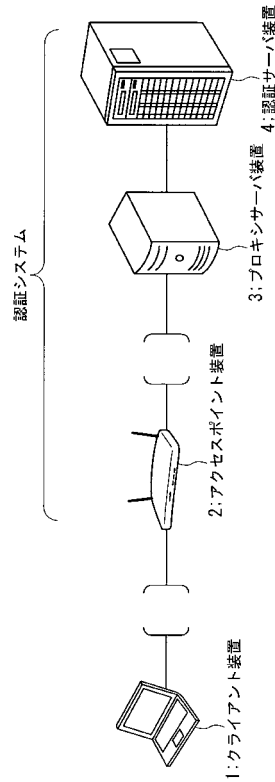
30

【符号の説明】

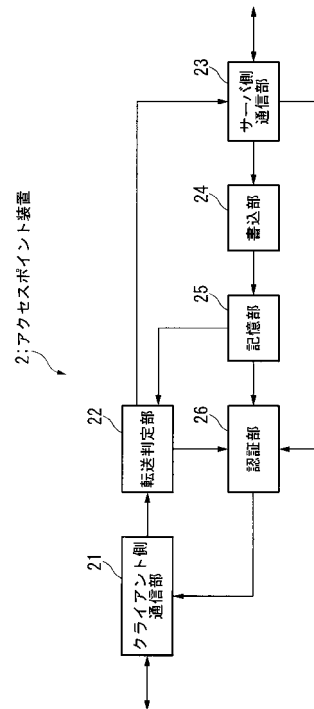
【0048】

1 …クライアント装置 2 …アクセスポイント装置 3 …プロキシサーバ装置 4 …認証サーバ装置
2 1 …クライアント側通信部 2 2 …転送判定部 2 3 …サーバ側通信部
2 4 …書込部 2 5 …記憶部 2 6 …認証部

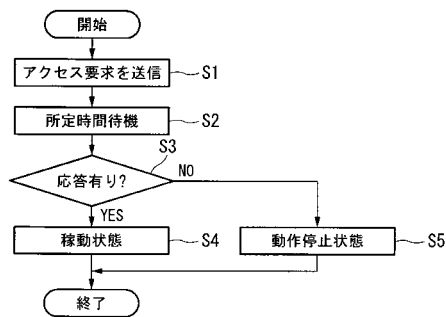
【図 1】



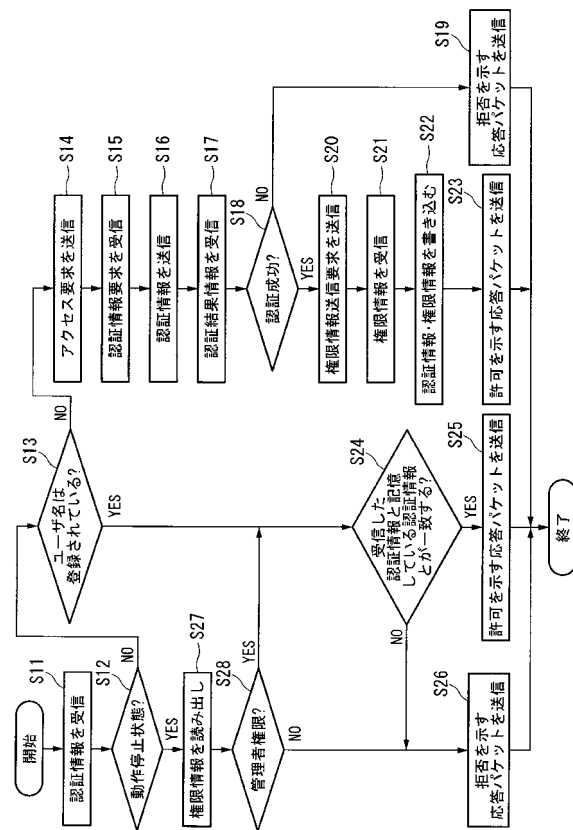
【図 2】



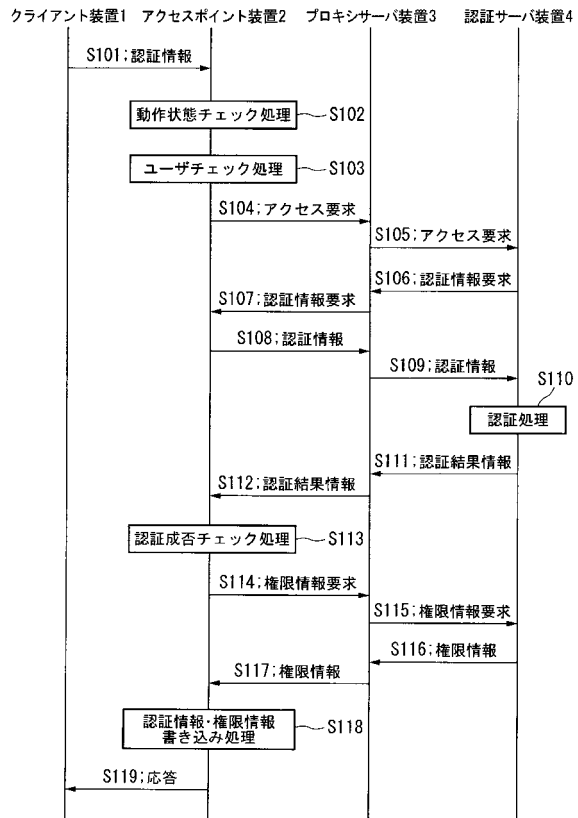
【図 3】



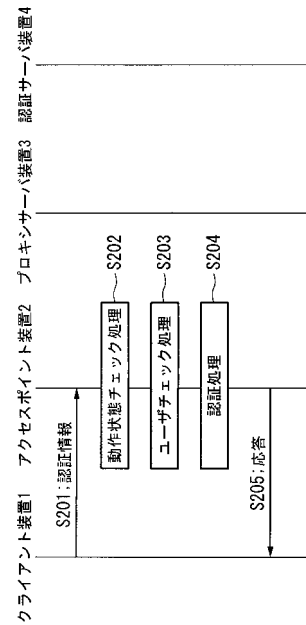
【図 4】



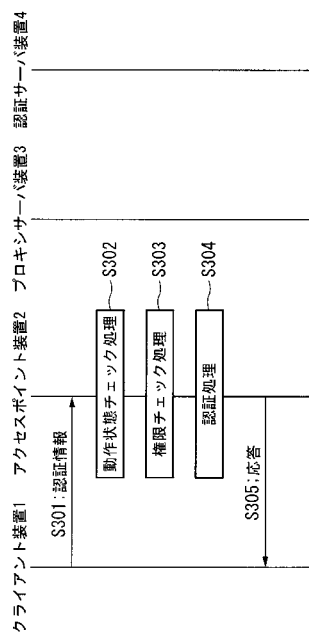
【図 5】



【図 6】



【図 7】



フロントページの続き

- (56)参考文献 特開2006-092018 (JP, A)
特開2004-318546 (JP, A)
特開平11-355266 (JP, A)
特開2009-116660 (JP, A)
特開2008-033855 (JP, A)

- (58)調査した分野(Int.Cl., DB名)
G06F 21/31