(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2010-98713
(P2010-98713A)
(43)公開日　平成22年4月30日(2010.4.30)

(51)Int.Cl.		F I			テーマコード（参考）
H04W 24/04	(2009.01)	H04Q	7/00	242	5K067
H04W 84/12	(2009.01)	H04Q	7/00	630	5K201
H04M 3/18	(2006.01)	H04M	3/18		

審査請求 未請求　請求項の数 41　ＯＬ　（全 46 頁）

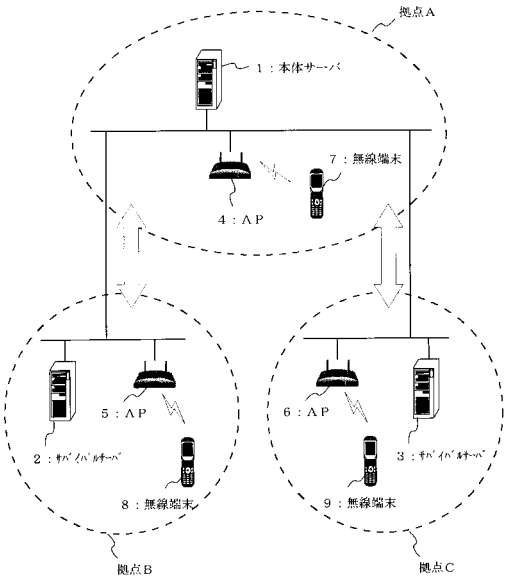
(21)出願番号　特願2009-133810 (P2009-133810)
(22)出願日　平成21年6月3日 (2009.6.3)
(31)優先権主張番号　特願2008-242278 (P2008-242278)
(32)優先日　平成20年9月22日 (2008.9.22)
(33)優先権主張国　日本国 (JP)

(71)出願人　000000295
沖電気工業株式会社
東京都港区西新橋三丁目１６番１１号
(74)代理人　100085198
弁理士　小林　久夫
(74)代理人　100098604
弁理士　安島　清
(74)代理人　100087620
弁理士　高梨　範夫
(74)代理人　100125494
弁理士　山東　元希
(72)発明者　武田　玄
東京都港区西新橋三丁目１６番１１号　沖電気工業株式会社内

最終頁に続く

(54)【発明の名称】無線通信システム、アクセスポイント、コントローラ、ネットワーク管理装置及びアクセスポイントのネットワーク識別子設定方法

(57)【要約】
【課題】同一のネットワーク識別子でのサーバ切り替えに対応していない無線端末であっても、サーバ切り替えを行うことができる無線通信システム、アクセスポイント、コントローラ、ネットワーク管理装置及びアクセスポイントのネットワーク識別子設定方法が望まれていた。
【解決手段】無線により情報通信を行う無線端末と、無線端末と無線通信接続するアクセスポイントと、無線端末の回線接続を管理する本体サーバ１と、本体サーバ１に代わって、無線端末の回線接続を管理するサバイバルサーバとを備え、アクセスポイントは、本体サーバ１及びサバイバルサーバと当該アクセスポイントとの間の通信状態を検出し、該通信状態に応じて当該アクセスポイントのＳＳＩＤを設定し、無線端末は、ＳＳＩＤを用いてアクセスポイントと無線通信し、当該ＳＳＩＤに応じて、本体サーバ１又はサバイバルサーバと情報通信を行う。
【選択図】図１



【特許請求の範囲】
【請求項１】
無線により情報通信を行う無線端末と、
前記無線端末と無線通信接続するアクセスポイントと、
前記アクセスポイントとネットワークを介して接続され、前記無線端末の回線接続を管理する本体サーバと、
前記アクセスポイントとネットワークを介して接続され、前記本体サーバに代わって、前記無線端末の回線接続を管理するサバイバルサーバと
を備え、
前記アクセスポイントは、
前記本体サーバ及び前記サバイバルサーバと当該アクセスポイントとの間の通信状態を検出し、該通信状態に応じて当該アクセスポイントのネットワーク識別子を設定し、
前記無線端末は、
前記ネットワーク識別子を用いて前記アクセスポイントと無線通信し、当該ネットワーク識別子に応じて、前記本体サーバ又は前記サバイバルサーバと情報通信を行うことを特徴とする無線通信システム。
【請求項２】
前記アクセスポイントは、
前記本体サーバと当該アクセスポイントとの間の通信が正常のとき第１のネットワーク識別子を設定し、
前記本体サーバと当該アクセスポイントとの間の通信に障害が生じ、且つ前記サバイバルサーバと当該アクセスポイントとの間の通信が正常のとき第２のネットワーク識別子を設定し、
前記無線端末は、
前記第１のネットワーク識別子を用いて前記アクセスポイントと無線通信するとき、前記本体サーバと情報通信を行い、
前記第２のネットワーク識別子を用いて前記アクセスポイントと無線通信するとき、前記サバイバルサーバと情報通信を行うことを特徴とする請求項１記載の無線通信システム。
【請求項３】
前記アクセスポイントは、
前記本体サーバ及び前記サバイバルサーバの少なくとも一方の負荷状態を検出し、該負荷状態及び、前記通信状態に応じて当該アクセスポイントのネットワーク識別子を設定することを特徴とする請求項１又は２記載の無線通信システム。
【請求項４】
前記アクセスポイントは、
前記本体サーバと当該アクセスポイントとの間の通信が正常、且つ、前記本体サーバが高負荷状態でないとき第１のネットワーク識別子を設定し、
前記本体サーバが高負荷状態であり、且つ、前記サバイバルサーバと当該アクセスポイントとの間の通信が正常であって、前記サバイバルサーバが高負荷状態でないとき第２のネットワーク識別子を設定し、
前記無線端末は、
前記第１のネットワーク識別子を用いて前記アクセスポイントと無線通信するとき、前記本体サーバと情報通信を行い、
前記第２のネットワーク識別子を用いて前記アクセスポイントと無線通信するとき、前記サバイバルサーバと情報通信を行うことを特徴とする請求項３記載の無線通信システム。
【請求項５】
前記アクセスポイントは、
複数のネットワーク識別子が記憶される記憶部と、

前記本体サーバ及び前記サバイバルサーバと当該アクセスポイントとの間の通信障害を検出する監視部と、
前記複数のネットワーク識別子のうち、前記通信障害の有無に応じて選択したネットワーク識別子を用いて、前記無線端末と無線通信する無線ＬＡＮ通信部と
を備えたことを特徴とする請求項１～４の何れかに記載の無線通信システム。
【請求項６】
前記監視部は、
ＩＣＭＰ　ｐｉｎｇ、又はＳＩＰに基づくメッセージを用いて、前記本体サーバ及び前記サバイバルサーバに接続し、前記本体サーバ及び前記サバイバルサーバと当該アクセスポイントとの間の通信障害を検出することを特徴とする請求項５記載の無線通信システム。
【請求項７】
無線により情報通信を行う無線端末と、
前記無線端末と無線通信接続するアクセスポイントと、
前記アクセスポイントとネットワークを介して接続され、前記無線端末の回線接続を管理する本体サーバと、
前記アクセスポイントとネットワークを介して接続され、前記本体サーバに代わって、前記無線端末の回線接続を管理するサバイバルサーバと
を備え、
前記アクセスポイントは、
前記本体サーバ及び前記サバイバルサーバの少なくとも一方の負荷状態を検出し、該負荷状態に応じて当該アクセスポイントのネットワーク識別子を設定し、
前記無線端末は、
前記ネットワーク識別子を用いて前記アクセスポイントと無線通信し、当該ネットワーク識別子に応じて、前記本体サーバ又は前記サバイバルサーバと情報通信を行うことを特徴とする無線通信システム。
【請求項８】
前記アクセスポイントは、
前記本体サーバが高負荷状態でないとき第１のネットワーク識別子を設定し、
前記本体サーバが高負荷状態であって、且つ、前記サバイバルサーバが高負荷状態でないとき第２のネットワーク識別子を設定し、
前記無線端末は、
前記第１のネットワーク識別子を用いて前記アクセスポイントと無線通信するとき、前記本体サーバと情報通信を行い、
前記第２のネットワーク識別子を用いて前記アクセスポイントと無線通信するとき、前記サバイバルサーバと情報通信を行うことを特徴とする請求項７記載の無線通信システム。
【請求項９】
前記アクセスポイントは、
複数のネットワーク識別子が記憶される記憶部と、
前記本体サーバ及び前記サバイバルサーバの少なくとも一方の負荷状態を検出する監視部と、
前記複数のネットワーク識別子のうち、前記負荷状態に応じて選択したネットワーク識別子を用いて、前記無線端末と無線通信する無線ＬＡＮ通信部と
を備えたことを特徴とする請求項７又は８記載の無線通信システム。
【請求項１０】
前記監視部は、
ＳＮＭＰ、ＳＮＭＰ　ｖｅｒｓｉｏｎ　２、又はＳＮＭＰ　ｖｅｒｓｉｏｎ　３のメッセージタイプを用いて、前記本体サーバ及び前記サバイバルサーバの少なくとも一方の、ＣＰＵ使用率、メモリ使用率、及びＮＷリソース使用率の少なくとも１つを検出すること

を特徴とする請求項９記載の無線通信システム。
【請求項１１】
前記無線端末は、
前記複数のネットワーク識別子と、該ネットワーク識別子に対応する前記本体サーバ又は前記サバイバルサーバの識別情報とが記憶され、
当該無線端末が通信可能な前記アクセスポイントのネットワーク識別子を用い、当該ネットワーク識別子に対応する本体サーバ又はサバイバルサーバと情報通信を行うことを特徴とする請求項５又は９記載の無線通信システム。
【請求項１２】
前記アクセスポイントは、
前記本体サーバ及び前記サバイバルサーバと当該アクセスポイントとの間の通信状態に応じて、前記無線端末が当該アクセスポイントを捕捉するスキャン方式を変更することを特徴とする請求項１～１１の何れかに記載の無線通信システム。
【請求項１３】
前記アクセスポイントは、
前記本体サーバ及び前記サバイバルサーバと当該アクセスポイントとの間の通信状態に応じて、当該アクセスポイントの前記ネットワーク識別子を複数設定し、
設定した前記複数のネットワーク識別子ごとに、前記無線端末が当該アクセスポイントを捕捉するための制御信号を送出することを特徴とする請求項１～１２の何れかに記載の無線通信システム。
【請求項１４】
前記アクセスポイントは、
当該アクセスポイントに設定した前記ネットワーク識別子に応じて、前記無線端末と当該アクセスポイントとの間の無線通信におけるセキュリティの設定又は変更を行うことを特徴とする請求項１～１３の何れかに記載の無線通信システム。
【請求項１５】
無線により情報通信を行う無線端末と、
前記無線端末と無線通信接続するアクセスポイントと、
前記アクセスポイントと接続するコントローラと、
前記コントローラとネットワークを介して接続され、前記無線端末の回線接続を管理する本体サーバと、
前記コントローラとネットワークを介して接続され、前記本体サーバに代わって、前記無線端末の回線接続を管理するサバイバルサーバと
を備え、
前記コントローラは、
前記本体サーバ及び前記サバイバルサーバと当該コントローラとの間の通信状態を検出し、該通信状態に応じて前記アクセスポイントのネットワーク識別子を設定し、
前記アクセスポイントは、
設定された前記ネットワーク識別子を用いて前記無線端末と無線通信し、
前記無線端末は、
前記ネットワーク識別子を用いて前記アクセスポイントと無線通信し、当該ネットワーク識別子に応じて、前記本体サーバ又は前記サバイバルサーバと情報通信を行うことを特徴とする無線通信システム。
【請求項１６】
前記コントローラは、
前記本体サーバと当該コントローラとの間の通信が正常のとき第１のネットワーク識別子を前記アクセスポイントに設定し、
前記本体サーバと当該コントローラとの間の通信に障害が生じ、且つ前記サバイバルサーバと当該コントローラとの間の通信が正常のとき第２のネットワーク識別子を前記アクセスポイントに設定し、

前記無線端末は、
前記第１のネットワーク識別子を用いて前記アクセスポイントと無線通信するとき、前記本体サーバと情報通信を行い、
前記第２のネットワーク識別子を用いて前記アクセスポイントと無線通信するとき、前記サバイバルサーバと情報通信を行うことを特徴とする請求項１５記載の無線通信システム。
【請求項１７】
前記アクセスポイントを複数備え、
前記コントローラは、前記複数のアクセスポイントと接続し、
前記本体サーバ及び前記サバイバルサーバと当該コントローラとの間の通信状態を検出し、該通信状態に応じて前記複数のアクセスポイントのネットワーク識別子を、それぞれ設定することを特徴とする請求項１５又は１６記載の無線通信システム。
【請求項１８】
前記コントローラは、
前記本体サーバ及び前記サバイバルサーバの少なくとも一方の負荷状態を検出し、該負荷状態及び、前記通信状態に応じて前記アクセスポイントのネットワーク識別子を設定することを特徴とする請求項１５～１７の何れかに記載の無線通信システム。
【請求項１９】
前記コントローラは、
前記本体サーバと当該コントローラとの間の通信が正常、且つ、前記本体サーバが高負荷状態でないとき第１のネットワーク識別子を前記アクセスポイントに設定し、
前記本体サーバが高負荷状態であり、且つ、前記サバイバルサーバと当該コントローラとの間の通信が正常であって、前記サバイバルサーバが高負荷状態でないとき第２のネットワーク識別子を前記アクセスポイントに設定し、
前記無線端末は、
前記第１のネットワーク識別子を用いて前記アクセスポイントと無線通信するとき、前記本体サーバと情報通信を行い、
前記第２のネットワーク識別子を用いて前記アクセスポイントと無線通信するとき、前記サバイバルサーバと情報通信を行うことを特徴とする請求項１８記載の無線通信システム。
【請求項２０】
前記コントローラは、
複数のネットワーク識別子が記憶される記憶部と、
前記本体サーバ及び前記サバイバルサーバと当該コントローラとの間の通信障害を検出し、該通信障害の有無に応じて、前記複数のネットワーク識別子のうち何れかを選択する監視部と、
選択された前記ネットワーク識別子を、前記アクセスポイントに設定するアクセスポイント制御部と
を備えたことを特徴とする請求項１５～１９の何れかに記載の無線通信システム。
【請求項２１】
前記監視部は、
ＩＣＭＰ　ｐｉｎｇ、又はＳＩＰに基づくメッセージを用いて、前記本体サーバ及び前記サバイバルサーバに接続し、前記本体サーバ及び前記サバイバルサーバと当該コントローラとの間の通信障害を検出することを特徴とする請求項２０記載の無線通信システム。
【請求項２２】
前記コントローラは、
前記本体サーバ及び前記サバイバルサーバと当該コントローラとの間の通信状態に応じて、前記アクセスポイントに対するアクセス制御及びトラヒック制御の少なくとも一方を行うことを特徴とする請求項１５～２１の何れかに記載の無線通信システム。
【請求項２３】

前記コントローラは、
前記本体サーバ及び前記サバイバルサーバと当該コントローラとの間の通信状態に応じて、前記無線端末が前記アクセスポイントを捕捉するスキャン方式を変更することを特徴とする請求項１５～２２の何れかに記載の無線通信システム。
【請求項２４】
前記コントローラは、
前記本体サーバ及び前記サバイバルサーバと当該コントローラとの間の通信状態に応じて、前記アクセスポイントの前記ネットワーク識別子を複数設定し、
設定した前記複数のネットワーク識別子ごとに、前記無線端末が前記アクセスポイントを捕捉するための制御信号を前記アクセスポイントに送出させることを特徴とする請求項１５～２３の何れかに記載の無線通信システム。
【請求項２５】
前記コントローラは、
前記アクセスポイントに設定した前記ネットワーク識別子に応じて、前記無線端末と前記アクセスポイントとの間の無線通信におけるセキュリティの設定又は変更を行うことを特徴とする請求項１５～２４の何れかに記載の無線通信システム。
【請求項２６】
無線により情報通信を行う無線端末と、
前記無線端末と無線通信接続するアクセスポイントと、
前記アクセスポイントとネットワークを介して接続され、前記無線端末の回線接続を管理する本体サーバと、
前記アクセスポイントとネットワークを介して接続され、前記本体サーバに代わって、前記無線端末の回線接続を管理するサバイバルサーバと、
前記アクセスポイントとネットワークを介して接続されるネットワーク管理装置と
を備え、
前記ネットワーク管理装置は、
前記本体サーバ及び前記サバイバルサーバと当該ネットワーク管理装置との間の通信状態を検出し、該通信状態に応じて前記アクセスポイントのネットワーク識別子を設定し、
前記アクセスポイントは、
設定された前記ネットワーク識別子を用いて前記無線端末と無線通信し、
前記無線端末は、
前記ネットワーク識別子を用いて前記アクセスポイントと無線通信し、当該ネットワーク識別子に応じて、前記本体サーバ又は前記サバイバルサーバと情報通信を行うことを特徴とする無線通信システム。
【請求項２７】
前記ネットワーク管理装置は、
前記本体サーバと当該ネットワーク管理装置との間の通信が正常のとき第１のネットワーク識別子を前記アクセスポイントに設定し、
前記本体サーバと当該ネットワーク管理装置との間の通信に障害が生じ、且つ前記サバイバルサーバと当該ネットワーク管理装置との間の通信が正常のとき第２のネットワーク識別子を前記アクセスポイントに設定し、
前記無線端末は、
前記第１のネットワーク識別子を用いて前記アクセスポイントと無線通信するとき、前記本体サーバと情報通信を行い、
前記第２のネットワーク識別子を用いて前記アクセスポイントと無線通信するとき、前記サバイバルサーバと情報通信を行うことを特徴とする請求項２６記載の無線通信システム。
【請求項２８】
前記アクセスポイントを複数備え、
前記ネットワーク管理装置は、前記複数のアクセスポイントとネットワークを介して接

続し、
前記本体サーバ及び前記サバイバルサーバと当該ネットワーク管理装置との間の通信状態を検出し、該通信状態に応じて前記複数のアクセスポイントのネットワーク識別子を、それぞれ設定することを特徴とする請求項２６又は２７記載の無線通信システム。
【請求項２９】
前記ネットワーク管理装置は、
前記本体サーバ及び前記サバイバルサーバの少なくとも一方の負荷状態を検出し、該負荷状態及び、前記通信状態に応じて前記アクセスポイントのネットワーク識別子を設定することを特徴とする請求項２６～２８の何れかに記載の無線通信システム。
【請求項３０】
前記ネットワーク管理装置は、
前記本体サーバと当該ネットワーク管理装置との間の通信が正常、且つ、前記本体サーバが高負荷状態でないとき第１のネットワーク識別子を前記アクセスポイントに設定し、
前記本体サーバが高負荷状態であり、且つ、前記サバイバルサーバと当該ネットワーク管理装置との間の通信が正常であって、前記サバイバルサーバが高負荷状態でないとき第２のネットワーク識別子を前記アクセスポイントに設定し、
前記無線端末は、
前記第１のネットワーク識別子を用いて前記アクセスポイントと無線通信するとき、前記本体サーバと情報通信を行い、
前記第２のネットワーク識別子を用いて前記アクセスポイントと無線通信するとき、前記サバイバルサーバと情報通信を行うことを特徴とする請求項２９記載の無線通信システム。
【請求項３１】
前記ネットワーク管理装置は、
複数のネットワーク識別子が記憶される記憶部と、
前記本体サーバ及び前記サバイバルサーバと当該ネットワーク管理装置との間の通信障害を検出し、該通信障害の有無に応じて、前記複数のネットワーク識別子のうち何れかを選択する監視部と、
選択された前記ネットワーク識別子を、前記アクセスポイントに設定するアクセスポイント制御部と
を備えたことを特徴とする請求項２６～３０の何れかに記載の無線通信システム。
【請求項３２】
前記監視部は、
ＩＣＭＰ　ｐｉｎｇ、又はＳＩＰに基づくメッセージを用いて、前記本体サーバ及び前記サバイバルサーバに接続し、前記本体サーバ及び前記サバイバルサーバと当該ネットワーク管理装置との間の通信障害を検出することを特徴とする請求項３１記載の無線通信システム。
【請求項３３】
前記ネットワーク管理装置は、
前記本体サーバ及び前記サバイバルサーバと当該ネットワーク管理装置との間の通信状態に応じて、前記アクセスポイントに対するアクセス制御及びトラヒック制御の少なくとも一方を行うことを特徴とする請求項２６～３２の何れかに記載の無線通信システム。
【請求項３４】
前記ネットワーク管理装置は、
前記本体サーバ及び前記サバイバルサーバと当該ネットワーク管理装置との間の通信状態に応じて、前記無線端末が前記アクセスポイントを捕捉するスキャン方式を変更することを特徴とする請求項２６～３３の何れかに記載の無線通信システム。
【請求項３５】
前記ネットワーク管理装置は、
前記本体サーバ及び前記サバイバルサーバと当該ネットワーク管理装置との間の通信状

態に応じて、前記アクセスポイントの前記ネットワーク識別子を複数設定し、
　設定した前記複数のネットワーク識別子ごとに、前記無線端末が前記アクセスポイントを捕捉するための制御信号を前記アクセスポイントに送出させることを特徴とする請求項２６～３４の何れかに記載の無線通信システム。
【請求項３６】
　前記ネットワーク管理装置は、
　前記アクセスポイントに設定した前記ネットワーク識別子に応じて、前記無線端末と前記アクセスポイントとの間の無線通信におけるセキュリティの設定又は変更を行うことを特徴とする請求項２６～３５の何れかに記載の無線通信システム。
【請求項３７】
　前記無線端末は、
　前記複数のネットワーク識別子と、該ネットワーク識別子に対応する前記本体サーバ又は前記サバイバルサーバの識別情報とが記憶され、
　当該無線端末が通信可能な前記アクセスポイントのネットワーク識別子を用い、当該ネットワーク識別子に対応する本体サーバ又はサバイバルサーバと情報通信を行うことを特徴とする請求項２０又は３１記載の無線通信システム。
【請求項３８】
　無線端末と無線通信接続すると共に、前記無線端末の回線接続に関する処理をする第一の装置、及び前記第一の装置に代わって前記無線端末の回線接続に関する処理をする第二の装置とネットワークを介して接続されるアクセスポイントであって、
　前記第一の装置及び前記第二の装置と当該アクセスポイントとの間の通信状態を検出し、該通信状態に応じて当該アクセスポイントのネットワーク識別子を設定し、
　前記ネットワーク識別子を用いて前記無線端末と無線通信し、
　前記ネットワーク識別子に応じて、前記無線端末と前記第一の装置又は前記第二の装置とを情報通信させることを特徴とするアクセスポイント。
【請求項３９】
　無線端末と無線通信接続するアクセスポイントと接続すると共に、前記無線端末の回線接続に関する処理をする第一の装置、及び前記第一の装置に代わって前記無線端末の回線接続に関する処理をする第二の装置とネットワークを介して接続されるコントローラであって、
　前記第一の装置及び前記第二の装置と当該コントローラとの間の通信状態を検出し、該通信状態に応じて前記アクセスポイントのネットワーク識別子を設定し、
　前記ネットワーク識別子を用いて、前記アクセスポイントと前記無線端末とを無線通信させ、
　前記ネットワーク識別子に応じて、前記無線端末と前記第一の装置又は前記第二の装置とを情報通信させることを特徴とするコントローラ。
【請求項４０】
　無線端末と無線通信接続するアクセスポイントとネットワークを介して接続されると共に、前記無線端末の回線接続に関する処理をする第一の装置、及び前記第一の装置に代わって前記無線端末の回線接続に関する処理をする第二の装置とネットワークを介して接続されるネットワーク管理装置であって、
　前記第一の装置及び前記第二の装置と当該ネットワーク管理装置との間の通信状態を検出し、該通信状態に応じて前記アクセスポイントのネットワーク識別子を設定し、
　前記ネットワーク識別子を用いて、前記アクセスポイントと前記無線端末とを無線通信させ、
　前記ネットワーク識別子に応じて、前記無線端末と前記第一の装置又は前記第二の装置とを情報通信させることを特徴とするネットワーク管理装置。
【請求項４１】
　第一のネットワークと第二のネットワークとの間に介在し通信を中継するアクセスポイントのネットワーク識別子設定方法であって、

前記第二のネットワーク中に配備され前記第一のネットワーク中の無線端末の回線接続に関する処理をする第一の装置と、前記アクセスポイントとの間の通信状態を検出する工程と、

前記第二のネットワーク中に配備され前記第一の装置に代わって前記無線端末の回線接続に関する処理をする第二の装置と、前記アクセスポイントとの間の通信状態を検出する工程と、

検出された前記通信状態に応じて、前記無線端末と前記第一の装置又は前記第二の装置とを情報通信させる前記アクセスポイントのネットワーク識別子を抽出する工程と、

抽出された前記ネットワーク識別子を前記アクセスポイントに設定する工程と

を有するアクセスポイントのネットワーク識別子設定方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、無線通信システム、アクセスポイント、コントローラ、ネットワーク管理装置及びアクセスポイントのネットワーク識別子設定方法に関するものである。

【背景技術】

【０００２】

従来の技術においては、例えば「プロファイル毎に、プロファイル名、ＳＳＩＤ（Service Set Identifier：サービスセット識別子）、ＩＰ（Internet Protocol）アドレス設定、ＤＮＳ（Domain Name System：ドメインネームシステム）設定、Ｐｒｏｘｙ設定、通信チャネル設定、セキュリティ方式設定（例えばＷＥＰ（Wired Equivalent Privacy））およびＳＩＰサーバ設定等の情報が記憶されている。無線ＬＡＮ端末１００は、このプロファイルに従って、接続先のアクセスポイント２００、２００ａ、２００ｂ、２００ｃをスキャンして探索するスキャン動作し、応答があったアクセスポイントと無線接続する。」無線ＬＡＮ端末が提案されている（例えば、特許文献１参照）。

【先行技術文献】

【特許文献】

【０００３】

【特許文献１】特開２００６－３１１０７７号公報

【発明の概要】

【発明が解決しようとする課題】

【０００４】

従来、各拠点にメインサーバ（本体サーバ）の代替手段となるサーバ（サバイバルサーバ）を設置し、本体サーバに障害が発生した場合、無線端末に関する管理を本体サーバからサバイバルサーバに切り替え、拠点内の情報通信を継続するものが知られている。

【０００５】

しかしながら、同一のネットワーク識別子（ＥＳＳＩＤ：Extended Service Set Identifier：以下「ＳＳＩＤ」ともいう。）でのサーバ切り替えに対応していない無線端末（無線ＬＡＮ端末）においては、例えば、障害等により本体サーバからサバイバルサーバへ切り替えが行われた場合、サバイバルサーバへの登録（情報通信）ができないため、サバイバルサーバを用いた通信を行うことができず、サービス利用不可となる、という問題点があった。

【０００６】

また、このようなサバイバルサーバへの登録ができない状態において、無線端末が本体サーバに対する登録を繰り返すことにより、ネットワーク輻輳が生じる、という問題点があった。この問題は端末台数が多くなるにつれて顕著である。

【０００７】

また、上記特許文献１に記載の技術は、プロファイルにより、利用するＳＳＩＤ、及びＳＩＰサーバを決定する。又は、ＳＳＩＤにより、利用するプロファイル、及びＳＩＰサーバを決定する。

【０００８】
しかしながら、複数のアクセスポイントが、同一のＳＳＩＤに設定されて構成された無線通信システムにおいては、同一のＳＳＩＤでのサーバ切り替えに対応していない無線端末では、利用するサーバ（ＳＩＰサーバ）を切り替えることができない、という問題点があった。
【０００９】
したがって、同一のネットワーク識別子でのサーバ切り替えに対応していない無線端末であっても、サーバ切り替えを行うことができる無線通信システム、アクセスポイント、コントローラ、ネットワーク管理装置及びアクセスポイントのネットワーク識別子設定方法が望まれていた。
【課題を解決するための手段】
【００１０】
本発明に係る無線通信システムは、無線により情報通信を行う無線端末と、前記無線端末と無線通信接続するアクセスポイントと、前記アクセスポイントとネットワークを介して接続され、前記無線端末の回線接続を管理する本体サーバと、前記アクセスポイントとネットワークを介して接続され、前記本体サーバに代わって、前記無線端末の回線接続を管理するサバイバルサーバとを備え、前記アクセスポイントは、前記本体サーバ及び前記サバイバルサーバと当該アクセスポイントとの間の通信状態を検出し、該通信状態に応じて当該アクセスポイントのネットワーク識別子を設定し、前記無線端末は、前記ネットワーク識別子を用いて前記アクセスポイントと無線通信し、当該ネットワーク識別子に応じて、前記本体サーバ又は前記サバイバルサーバと情報通信を行うものである。
【００１１】
本発明に係るアクセスポイントは、無線端末と無線通信接続すると共に、前記無線端末の回線接続を管理する本体サーバ、及び前記本体サーバに代わって前記無線端末の回線接続を管理するサバイバルサーバとネットワークを介して接続されるアクセスポイントであって、前記本体サーバ及び前記サバイバルサーバと当該アクセスポイントとの間の通信状態を検出し、該通信状態に応じて当該アクセスポイントのネットワーク識別子を設定し、前記ネットワーク識別子を用いて前記無線端末と無線通信し、前記ネットワーク識別子に応じて、前記無線端末と前記本体サーバ又は前記サバイバルサーバとを情報通信させるものである。
【００１２】
本発明に係るコントローラは、無線端末と無線通信接続するアクセスポイントと接続すると共に、前記無線端末の回線接続を管理する本体サーバ、及び前記本体サーバに代わって前記無線端末の回線接続を管理するサバイバルサーバとネットワークを介して接続されるコントローラであって、前記本体サーバ及び前記サバイバルサーバと当該コントローラとの間の通信状態を検出し、該通信状態に応じて前記アクセスポイントのネットワーク識別子を設定し、前記ネットワーク識別子を用いて、前記アクセスポイントと前記無線端末とを無線通信させ、前記ネットワーク識別子に応じて、前記無線端末と前記本体サーバ又は前記サバイバルサーバとを情報通信させるものである。
【００１３】
本発明に係るネットワーク管理装置は、無線端末と無線通信接続するアクセスポイントとネットワークを介して接続されると共に、前記無線端末の回線接続を管理する本体サーバ、及び前記本体サーバに代わって前記無線端末の回線接続を管理するサバイバルサーバとネットワークを介して接続されるネットワーク管理装置であって、前記本体サーバ及び前記サバイバルサーバと当該ネットワーク管理装置との間の通信状態を検出し、該通信状態に応じて前記アクセスポイントのネットワーク識別子を設定し、前記ネットワーク識別子を用いて、前記アクセスポイントと前記無線端末とを無線通信させ、前記ネットワーク識別子に応じて、前記無線端末と前記本体サーバ又は前記サバイバルサーバとを情報通信させるものである。
【００１４】

本発明に係るアクセスポイントのネットワーク識別子設定方法は、無線ネットワークと有線ネットワークとの間に介在し通信を中継するアクセスポイントのネットワーク識別子設定方法であって、前記有線ネットワーク中に配備され前記無線ネットワーク中の無線端末の回線接続を管理する本体サーバと、前記アクセスポイントとの間の通信状態を検出する工程と、前記有線ネットワーク中に配備され前記本体サーバに代わって前記無線端末の回線接続を管理するサバイバルサーバと、前記アクセスポイントとの間の通信状態を検出する工程と、検出された前記通信状態に応じて、前記無線端末と前記本体サーバ又は前記サバイバルサーバとを情報通信させる前記アクセスポイントのネットワーク識別子を抽出する工程と、抽出された前記ネットワーク識別子を前記アクセスポイントに設定する工程とを有するものである。

【発明の効果】

【００１５】

本発明においては、アクセスポイントは、本体サーバ及びサバイバルサーバとアクセスポイントとの間の通信状態を検出し、該通信状態に応じてアクセスポイントのネットワーク識別子を設定し、無線端末は、前記ネットワーク識別子に応じて、本体サーバ又はサバイバルサーバと情報通信を行うので、同一のネットワーク識別子でのサーバ切り替えに対応していない無線端末であっても、サーバ切り替えを行うことができる。

【図面の簡単な説明】

【００１６】

【図１】実施の形態１に係る無線ＩＰ電話システムの構成図である。
【図２】実施の形態１に係るアクセスポイントの構成図である。
【図３】ＡＰの記憶部に記憶されたプロファイルデータを示す図である。
【図４】無線端末に記憶されたプロファイルデータを示す図である。
【図５】実施の形態１に係る通信障害時のネットワーク接続を示す図である。
【図６】実施の形態１に係るサーバ切り替え動作を示すシーケンス図である。
【図７】実施の形態１に係る通信障害時のネットワーク接続を示す図である。
【図８】実施の形態１に係るサーバ切り替え動作を示すシーケンス図である。
【図９】ＡＰの記憶部に記憶された負荷の閾値を示す図である。
【図１０】実施の形態３に係る無線ＩＰ電話システムの構成図である。
【図１１】実施の形態３に係るコントローラの構成図である。
【図１２】実施の形態３に係るアクセスポイントの構成図である。
【図１３】実施の形態３に係る通信障害時のネットワーク接続を示す図である。
【図１４】実施の形態３に係るサーバ切り替え動作を示すシーケンス図である。
【図１５】実施の形態３に係る通信障害時のネットワーク接続を示す図である。
【図１６】実施の形態３に係るサーバ切り替え動作を示すシーケンス図である。
【図１７】実施の形態４に係る無線ＩＰ電話システムの構成図である。
【図１８】実施の形態４に係るネットワーク管理装置の構成図である。
【図１９】実施の形態４に係る通信障害時のネットワーク接続を示す図である。
【図２０】実施の形態４に係るサーバ切り替え動作を示すシーケンス図である。
【図２１】実施の形態５に係る無線ＩＰ電話システムの構成図である。
【図２２】実施の形態６に係るコントローラの記憶部に記憶されたプロファイルデータを示す図である。
【図２３】実施の形態７に係るＡＰの記憶部に記憶されたプロファイルデータを示す図である。
【図２４】実施の形態８に係る記憶部に記憶されたプロファイルデータを示す図である。

【発明を実施するための形態】

【００１７】

実施の形態１.

図１は実施の形態１に係る無線ＩＰ電話システムの構成図である。

本実施の形態においては、本発明における無線通信システムを、無線ＩＰ（Internet P

rotocol）電話システムに適用した形態について説明する。

【００１８】

図１において、本実施の形態１に係る無線ＩＰ電話システムは、本体サーバ１と、サバイバルサーバ２と、サバイバルサーバ３と、アクセスポイント（以下「ＡＰ」ともいう。）４と、ＡＰ５と、ＡＰ６と、無線端末７と、無線端末８と、無線端末９とから構成されている。

【００１９】

本体サーバ１、サバイバルサーバ２、サバイバルサーバ３、ＡＰ４、ＡＰ５、及びＡＰ６は、それぞれ有線ＬＡＮで接続され、互いに通信が行える。

無線端末７、無線端末８、及び無線端末９（以下、区別しないときは単に「端末」ともいう。）は、それぞれ、ＡＰ４、ＡＰ５、及びＡＰ６（以下、区別しないときは単に「アクセスポイント」又は「ＡＰ」ともいう。）の何れかと無線ＬＡＮにより接続され、無線により情報通信が行える。

ＡＰ４、ＡＰ５、及びＡＰ６は、それぞれ、有線ＬＡＮと無線ＬＡＮとの間で通信を中継する。

【００２０】

ここで、図１に示す無線ＩＰ電話システムには、拠点Ａ、拠点Ｂ、拠点Ｃが存在する。

拠点Ａには、本体サーバ１、ＡＰ４、及び無線端末７が含まれる。

拠点Ｂには、サバイバルサーバ２、ＡＰ５、及び無線端末８が含まれる。

拠点Ｃには、サバイバルサーバ３、ＡＰ６、及び無線端末９が含まれる。

【００２１】

例えば、１つの地区や地域において電話システムが構成される場合、その電話システムが包含する範囲を拠点という。

例えば、拠点Ａが東京地区、拠点Ｂが大阪地区、及び拠点Ｃが名古屋地区といえる。

【００２２】

尚、図１では、拠点として拠点Ａ～Ｃの場合を示しているが、本発明はこれに限るものではなく、同様の機能を持つ拠点を複数備えるようにしても良い。

また、各拠点における端末及びアクセスポイントの設置台数は、特に限定されるものではなく、複数台であっても良い。

【００２３】

本体サーバ１、サバイバルサーバ２、及びサバイバルサーバ３（以下、区別しないときは単に「サーバ」という。）は、ＩＰ網に接続可能な呼処理装置である。

例えば、ＩＰインターフェースを有するＩＰ－ＰＢＸやＳＩＰサーバなどにより構成される。

本体サーバ１は、主要として設置された呼処理装置である。

サバイバルサーバ２及びサバイバルサーバ３は、副次的に設置された呼処理装置である。後述する動作により、サバイバルサーバ２及び３は、本体サーバ１に障害が発生した場合などに、本体サーバ１に代わって動作する。

これらの呼処理装置は、それぞれ異なるＩＰアドレスが予め設定され、拠点毎に設置されている。

【００２４】

尚、「本体サーバ１」は、本発明における「第一の装置」に相当する。

また、「サバイバルサーバ２」及び「サバイバルサーバ３」は、本発明における「第二の装置」に相当する。

【００２５】

ＡＰ４、ＡＰ５、及びＡＰ６は、端末を無線ＬＡＮに接続する基地局である。

ＡＰ４、ＡＰ５、及びＡＰ６は、有線ＬＡＮインターフェースと無線ＬＡＮインターフェースとを有し、それぞれのＬＡＮに接続し、有線ＬＡＮと無線ＬＡＮとの間で通信を転送する。

ＡＰ４、ＡＰ５、及びＡＰ６は、サーバと当該アクセスポイントとの間の通信状態を検

出し、この通信状態に応じて当該アクセスポイントのネットワーク識別子となるＳＳＩＤを設定するものである。

【００２６】

尚、「無線ＬＡＮ」は、本発明における「第一のネットワーク」に相当する。

また、「有線ＬＡＮ」は、本発明における「第二のネットワーク」に相当する。

【００２７】

このＡＰ４、ＡＰ５、及びＡＰ６には、予め、ＳＳＩＤが同一となるように設定され、拠点毎に設置されている。

本実施の形態１では、定常時においては、ＡＰ４～ＡＰ６のＳＳＩＤとして、「ＳＳＩＤ１」が予め設定されたものとして説明する。

【００２８】

図２は実施の形態１に係るアクセスポイントの構成図である。

図２に示すように、アクセスポイントは、有線ＬＡＮ通信部１０１と、無線ＬＡＮ通信部１０２と、記憶部１０３と、監視部１０４とにより構成されている。

【００２９】

有線ＬＡＮ通信部１０１は、有線ＬＡＮと接続する。

無線ＬＡＮ通信部１０２は、無線ＬＡＮと接続する。

有線ＬＡＮ通信部１０１と無線ＬＡＮ通信部１０２とは互いに接続し、通信を中継できる。

記憶部１０３は、複数のプロファイルが記憶される。

監視部１０４は、記憶部１０３が記憶するプロファイルに基づきサーバを監視する。

次に、記憶部１０３に記憶されるプロファイルのデータ構成について図３により説明する。

【００３０】

図３はＡＰの記憶部に記憶されたプロファイルデータを示す図である。

図３（ａ）はＡＰ４の記憶部１０３に記憶されたプロファイルを示している。

図３（ｂ）はＡＰ５の記憶部１０３に記憶されたプロファイルを示している。

図３（ｃ）はＡＰ６の記憶部１０３に記憶されたプロファイルを示している。

【００３１】

図３に示すように、記憶部１０３に記憶されるプロファイルは、ＡＰごとに異なる。

各プロファイルは、プロファイル名と、ＳＳＩＤと、監視対象サーバのＩＰアドレスと、対応するスキャン方式と、監視対象フラグとにより構成されている。

【００３２】

図３（ａ）、図３（ｂ）、図３（ｃ）に示すように、各ＡＰの記憶部１０３に記憶されているプロファイルにおいて、本体サーバ１のＩＰアドレスを含むプロファイルの監視対象フラグは「ＯＮ」に設定されている。

また、当該アクセスポイントが設置された拠点に、サバイバルサーバ２又は３が設置されている場合には、当該サバイバルサーバのＩＰアドレスを含むプロファイルの監視対象フラグは「ＯＮ」に設定されている。

【００３３】

つまり、拠点ＡにはＡＰ４と本体サーバ１が設置されているので、図３（ａ）のように、ＡＰ４の記憶部１０３では、「本体サーバ１のＩＰアドレス１」が「監視対象フラグＯＮ」と予め設定される。

また、拠点ＢにはＡＰ５とサバイバルサーバ２とが設置されているので、図３（ｂ）のように、ＡＰ５の記憶部１０３では、「本体サーバ１のＩＰアドレス１」、及び「サバイバルサーバ２のＩＰアドレス２」が「監視対象フラグＯＮ」と予め設定される。

また、拠点ＣにはＡＰ６とサバイバルサーバ３が設置されているので、図３（ｃ）のように、ＡＰ６の記憶部１０３では、「本体サーバ１のＩＰアドレス１」、及び「サバイバルサーバ３のＩＰアドレス３」が「監視対象フラグＯＮ」と予め設定される。

【００３４】

ＡＰ４～ＡＰ６の監視部１０４は、当該アクセスポイントの記憶部１０３に記憶されたプロファイルの監視対象フラグに基づき、「監視対象フラグＯＮ」に設定されている本体サーバ１、サバイバルサーバ２及び３を監視する。

【００３５】

つまり、ＡＰ４の記憶部１０３は、図３（ａ）のように、「本体サーバ１のＩＰアドレス１」が「監視対象フラグＯＮ」に設定されているので、ＡＰ４の監視部１０４は、「本体サーバ１のＩＰアドレス１」に基づいて監視する。

また、ＡＰ５の記憶部１０３は、図３（ｂ）のように、「本体サーバ１のＩＰアドレス１」、及び「サバイバルサーバ２のＩＰアドレス２」が「監視対象フラグＯＮ」に設定されているので、ＡＰ５の監視部１０４は、「本体サーバ１のＩＰアドレス１」、及び「サバイバルサーバ２のＩＰアドレス２」に基づいて監視する。

また、ＡＰ６の記憶部１０３は、図３（ｃ）のように、「本体サーバ１のＩＰアドレス１」、及び「サバイバルサーバ３のＩＰアドレス３」が「監視対象フラグＯＮ」に設定されているので、ＡＰ６の監視部１０４は、「本体サーバ１のＩＰアドレス１」、及び「サバイバルサーバ３のＩＰアドレス３」に基づいて監視する。

【００３６】

監視部１０４は、サーバと当該アクセスポイントとの間の通信状態を監視（検出）する。このような通信状態を監視する手段としては、例えばＲＦＣ（Request for Comments）７９２に基づくメッセージタイプを用いたＩＣＭＰ（Internet Control Message Protocol）　ｐｉｎｇ、及びＲＦＣ３２６１に基づくＳＩＰメッセージを用いたＳＩＰプロトコルの少なくとも一方で接続要求し、サーバから接続応答を得ることで通信状態を検出する。

つまり、監視部１０４は、接続要求し、サーバから接続応答を得ることができるとき、接続が成功し、サーバと当該アクセスポイントとの間の通信は正常であると認識する。

また、監視部１０４は、接続要求し、サーバから接続応答を得ることができないと、接続が失敗し、サーバと当該アクセスポイントとの間の通信に障害が生じていると認識する。

監視部１０４はＩＣＭＰ　ｐｉｎｇ、及びＳＩＰメッセージによる接続要求を実現するためにプロトコルスタックを有しており、このプロトコルスタックを介して接続要求を生成し送信し、接続応答を得るときは、このプロトコルスタックを介して受信することで接続応答を解釈する。このプロトコルスタックを拡張することで、拡張されたＩＣＭＰ　ｐｉｎｇ、及び拡張されたＳＩＰメッセージによる接続要求の送信と接続応答の受信が可能となる。

【００３７】

ここで、ＳＩＰメッセージを用いた接続要求について説明する。

ＳＩＰメッセージを用いた接続要求とは、具体的にはＲＥＧＩＳＴＥＲやＩＮＶＩＴＥのメッセージを用いた接続要求である。

ＳＩＰメッセージを用いた接続要求を行う場合、監視部１０４には、予め、ＲＥＧＩＳＴＥＲ若しくはＩＮＶＩＴＥのどちらを接続要求に用いるかの設定と、当該ＳＩＰメッセージの送出周期の設定（例えば、１秒～３６００秒の間）と、ＳＩＰ　ＵＲＩ（Uniform Resource Identifier）（電話番号）の設定とを設定しておく。

尚、ＲＥＧＩＳＴＥＲ及びＩＮＶＩＴＥの双方を接続要求に用いるようにも設定できる。この場合、設定された周期でＲＥＧＩＳＴＥＲとＩＮＶＩＴＥとを交互に送出する。例えば、ＲＥＧＩＳＴＥＲを送出後にＩＮＶＩＴＥを送出する順番で交互に送出する。

【００３８】

監視部１０４に設定する上記のＳＩＰ　ＵＲＩは、本体サーバ１、サバイバルサーバ２及びサバイバルサーバ３で利用可能（登録可能）なＳＩＰ　ＵＲＩであり、主に通信状態の検出に用いるＳＩＰ　ＵＲＩである。このＳＩＰ　ＵＲＩは、ＡＰごとに異なるＳＩＰ　ＵＲＩを設定しておく。

【００３９】

まず、ＲＥＧＩＳＴＥＲのメッセージを用いる場合の接続要求について説明する。
ＲＥＧＩＳＴＥＲとは、ＳＩＰ　ＵＲＩと、ＳＩＰ　ＵＲＩを利用する装置とを関連付けてＳＩＰサーバに登録し、ＳＩＰ　ＵＲＩで電話サービスを受けられるようにするメッセージである。
監視部１０４は、監視対象のサーバに対し、自身に設定されるＳＩＰ　ＵＲＩを含めたＲＥＧＩＳＴＥＲを送出（接続要求）する。
このＲＥＧＩＳＴＥＲを受けた監視対象のサーバは、ＲＥＧＩＳＴＥＲに基づき登録処理をし、登録に成功するとＳＩＰメッセージの２００ＯＫの応答信号を返送（接続応答）する。
監視部１０４は、２００ＯＫを受信すると接続応答を得たとして１回の監視を終える。
以降、同様に、監視部１０４は、自身に設定されるメッセージの送出周期で周期的にＲＥＧＩＳＴＥＲを送出する。
こうして、監視部１０４は、ＲＥＧＩＳＴＥＲのメッセージを用いて接続要求し、接続応答を得ることで通信状態を検出できる。

【００４０】

次に、ＩＮＶＩＴＥのメッセージを用いる場合の接続要求について説明する。
ＩＮＶＩＴＥとは、電話サービスにおける発呼のメッセージである。
監視部１０４は、監視対象のサーバに対し、自身（当該ＡＰ）に設定されるＳＩＰ　ＵＲＩを、ＩＮＶＩＴＥのＴｏ及びＦｒｏｍのヘッダーフィールドに含めて送出（接続要求）する。
つまり、このＩＮＶＩＴＥは、自身（当該ＡＰ）に発呼していることになる。
このＩＮＶＩＴＥを受けた監視対象のサーバは、ＩＮＶＩＴＥに基づき発呼処理をし、ＴｏとＦｒｏｍが同一なので、４８６　Ｂｕｓｙ　Ｈｅｒｅを返送（接続応答）する。
監視部１０４は、４８６　Ｂｕｓｙ　Ｈｅｒｅを受信すると接続応答を得たとして１回の監視を終える。このとき、監視部１０４は、ＡＣＫを返送し、４８６　Ｂｕｓｙ　Ｈｅｒｅを受信したことを通知し、送信したＩＮＶＩＴＥを正常終了させる。
以降、同様に、監視部１０４は、自身（当該ＡＰ）に設定されるメッセージの送出周期で周期的にＩＮＶＩＴＥを送出する。
こうして、監視部１０４は、ＩＮＶＩＴＥのメッセージを用いて接続要求し、接続応答を得ることで通信状態を検出できる。

【００４１】

尚、以下の説明では、監視部１０４は、例えばＲＦＣ７９２に基づくメッセージタイプを用いたＩＣＭＰ　ｐｉｎｇを用いて通信状態を検出する場合について説明する。

【００４２】

ＡＰ４～ＡＰ６の監視部１０４は、サーバに接続が失敗し、障害と認識すると、記憶部１０３に記憶されたプロファイルのうち、監視対象フラグがＯＮ、且つ、接続に成功するサーバが含まれるプロファイルのＳＳＩＤ、及び対応するスキャン方式を無線ＬＡＮ通信部１０２に設定する。

【００４３】

つまり、例えば、ＡＰ５の監視部１０４では、図３（ｂ）に示した記憶部１０３の設定に基づき、「本体サーバ１のＩＰアドレス１」、及び「サバイバルサーバ２のＩＰアドレス２」を監視する。
例えば、本体サーバ１の接続確認が失敗し、サバイバルサーバ２の接続確認が成功する状態においては、監視部１０４は、「プロファイル名２」に基づき、ＳＳＩＤを「ＳＳＩＤ２」として、及び対応するスキャン方式を「アクティブ」として、無線ＬＡＮ通信部１０２に設定する。
尚、プロファイルのスキャン方式に何も記憶されていない場合は、無線ＬＡＮ通信部１０２にスキャン方式を設定しない。

【００４４】

ところで、無線ＬＡＮでは、サービスエリアに設置したＡＰと端末との間を接続するた

めに、端末によりＡＰを検索（スキャン）し、通信が可能なＡＰを捕捉する。
検索方法として、アクティブスキャン（Active scan）方式、又はパッシブスキャン（Passive scan）方式が用いられる。
【００４５】
アクティブスキャンとは、端末が接続要求信号（Probe Request）を送出し、ＡＰは受け取った接続要求信号（Probe Request）に対し、当該ＡＰに設定されているＳＳＩＤを含めた接続応答信号（Prove Response）を送出し、端末はＡＰからの接続応答信号（Prove Response）を受け取ると、当該端末と同じＳＳＩＤであるＡＰに接続処理を行う。
【００４６】
パッシブスキャンとは、ＡＰが定期的に送出する制御信号（ビーコン）を端末がモニタし、制御信号（ビーコン）に含まれるＳＳＩＤが当該端末に設定されたＳＳＩＤと同じである場合は、ＡＰに接続処理を行う。
【００４７】
一般的には、通常のスキャンでは、まずアクティブスキャンを実施してＡＰを検索し、ＡＰを捕捉することができないと、パッシブスキャンに切り替えてパッシブスキャンを実施し、その後、ＡＰを見つけることができない場合には、交互にアクティブスキャンとパッシブスキャンとを繰り返す。
【００４８】
本実施の形態１において、各ＡＰの無線ＬＡＮ通信部１０２は、監視部１０４からＳＳＩＤ、及び対応するスキャン方式が設定されると、無線ＬＡＮに切断信号（Deauthentication）のメッセージを送出し、更に、設定された情報に基づき無線ＬＡＮと接続することで再帰処理を実施する。
スキャン方式に何も設定されていない場合は、上述した通常のスキャンに対応する。
【００４９】
つまり、例えば、ＡＰ５において、本体サーバ１の接続確認が失敗し、サバイバルサーバ２の接続確認が成功する状態においては、ＡＰ５の無線ＬＡＮ通信部１０２は、「プロファイル名２」に基づいて、ＳＳＩＤが「ＳＳＩＤ２」に設定され、対応するスキャン方式が「アクティブ」に設定される。
このとき、ＡＰ５の無線ＬＡＮ通信部１０２は、無線ＬＡＮに切断信号（Deauthentication）のメッセージを送出し、再帰処理を実施する。そして、端末から接続要求信号（Probe Request）を受信すると、自身に設定されている「ＳＳＩＤ２」を含めた接続応答信号（Prove Response）を送出する。
【００５０】
また、例えば、ＡＰ６において、本体サーバ１の接続確認が失敗し、サバイバルサーバ３の接続確認が成功する状態においては、ＡＰ６の無線ＬＡＮ通信部１０２は、「プロファイル名３」に基づいて、ＳＳＩＤが「ＳＳＩＤ３」に設定され、対応するスキャン方式が「パッシブ」に設定される。
このとき、ＡＰ６の無線ＬＡＮ通信部１０２は、無線ＬＡＮに切断信号（Deauthentication）のメッセージを送出し、再帰処理を実施する。そして、自身に設定されているＳＳＩＤを含めた制御信号（ビーコン）を送出する。
【００５１】
再び図１において、無線端末７、無線端末８、及び無線端末９は、無線ＩＰ電話端末である。この無線端末７～９は、無線ＬＡＮインターフェースを有し、無線ＬＡＮに接続し、無線により情報通信を行う。また、無線端末７～無線端末９は、電話の発呼（発信）と、着呼（着信）とを行うことができる。
これらの端末は、アクセスポイントに設定されたＳＳＩＤと同一のＳＳＩＤを用いて、アクセスポイントと無線通信する。また、設定されたＳＳＩＤに応じて、本体サーバ１、又はサバイバルサーバ２若しくは３と情報通信を行う。
【００５２】
尚、無線端末７～９は、例えば、携帯電話のような電話端末であっても、ＰＣにＩＰ電

話アプリケーションをインストールしたソフトフォンであっても良い。

【００５３】

図４は無線端末に記憶されたプロファイルデータを示す図である。

図４に示すように、各端末は、複数のプロファイルが予め設定される。

各プロファイルは、プロファイル名と、ＳＳＩＤと、接続先のサーバのアドレスとにより構成されている。

本実施の形態では、定常時においては、各端末のＳＳＩＤとして、「ＳＳＩＤ１」が予め設定されたものとして説明する。

【００５４】

尚、「本体サーバ１のＩＰアドレス１」、「サバイバルサーバ２のＩＰアドレス２」、及び「サバイバルサーバ３のＩＰアドレス３」は、本発明における本体サーバ又はサバイバルサーバの識別情報に相当する。

【００５５】

以上、無線ＩＰ電話システムを構成する各機器の詳細構成について説明した。

次に、定常時における無線ＩＰ電話システムの動作について説明する。

【００５６】

図１において、無線端末８と無線端末９とが通話する場合について説明する。

定常時においては、無線端末８及びＡＰ５は共に「ＳＳＩＤ１」が設定される。

無線端末８は、上述した通常のスキャン方式により、ＡＰ５に接続処理を行う。無線端末８は、無線端末９に対して発呼する際、発呼信号を「ＳＳＩＤ１」での接続先サーバである「本体サーバ１のＩＰアドレス１」宛に送信する。これにより、無線端末８からの発呼信号がＡＰ５を介して本体サーバ１へ到達する。

本体サーバ１は、無線端末８からの発呼信号に基づき呼処理をする。

一方、定常時においては、無線端末９及びＡＰ６は共に「ＳＳＩＤ１」が設定される。

無線端末９は、上述した通常のスキャン方式により、ＡＰ６に接続処理を行う。

本体サーバ１の呼処理により、無線端末９に対して着信信号が送出されると、ＡＰ６を介して無線端末９に着信信号が到達する。

これにより、無線端末９が着呼することで無線端末８と無線端末９との通話が確立される。

尚、「ＳＳＩＤ１」は、本発明における第１のネットワーク識別子に相当する。

【００５７】

次に、本体サーバ１とアクセスポイントの間の通信に障害が生じた場合の動作について説明する。

【００５８】

図５は実施の形態１に係る通信障害時のネットワーク接続を示す図である。

図６は実施の形態１に係るサーバ切り替え動作を示すシーケンス図である。

まず、図５に示すように、ＡＰ５と本体サーバ１との間の通信に障害が生じ、ＡＰ５とサバイバルサーバ２との間の通信が正常の場合の動作を、図６に基づき説明する。

【００５９】

（Ｓ１０１）

ＡＰ５の監視部１０４は、記憶部１０３に記憶されたプロファイルに基づき、「監視対象フラグＯＮ」である「本体サーバ１のＩＰアドレス１」、及び「サバイバルサーバ２のＩＰアドレス２」との通信状態を、有線ＬＡＮ通信部１０１を介して監視する。

図５の状態においては、監視部１０４は、本体サーバ１との接続に失敗するため、ＡＰ５と本体サーバ１との間の通信に障害が生じていると認識する。

また、監視部１０４は、サバイバルサーバ２との接続に成功するため、ＡＰ５とサバイバルサーバ２との間の通信は正常であると認識する。

【００６０】

（Ｓ１０２）

ＡＰ５の監視部１０４は、本体サーバ１に接続が失敗し、障害と認識すると、記憶部１

０３に記憶されたプロファイルのうち、監視対象フラグがＯＮ、且つ、接続に成功するサバイバルサーバ２が含まれる「プロファイル名２」に基づいて、ＳＳＩＤを「ＳＳＩＤ２」とし、及び対応するスキャン方式を「アクティブ」として、無線ＬＡＮ通信部１０２に設定する。

尚、「ＳＳＩＤ２」は、本発明における第２のネットワーク識別子に相当する。

【００６１】

（Ｓ１０３）

ＡＰ５の無線ＬＡＮ通信部１０２は、監視部１０４からＳＳＩＤが「ＳＳＩＤ２」、及び対応するスキャン方式が「アクティブ」に設定されると、無線ＬＡＮに切断信号（Deauthentication）のメッセージを送出し、再帰処理を実施する。

【００６２】

（Ｓ１０４）

無線端末８は、ＡＰ５から切断信号（Deauthentication）のメッセージを受信すると、ＡＰ５との接続を切断する。そして、再び「ＳＳＩＤ１」に設定されているアクセスポイントをスキャンするため、接続要求信号（Probe Request）のメッセージを送出する。

ここで、ＡＰ５は、「ＳＳＩＤ２」に設定されているので応答しない。

【００６３】

（Ｓ１０５）

無線端末８は、「ＳＳＩＤ１」に設定されたアクセスポイントを捕捉できないとき、当該無線端末８に記憶されている別のプロファイルに含まれる「ＳＳＩＤ２」に設定されているアクセスポイントをスキャンするため、接続要求信号（Probe Request）のメッセージを送出する。

【００６４】

（Ｓ１０６）

ＡＰ５は、「ＳＳＩＤ２」に設定されているので、受け取った接続要求信号（Probe Request）に対し、当該ＡＰ５に設定されている「ＳＳＩＤ２」を含めた接続応答信号（Prove Response）を送出して応答する。

【００６５】

（Ｓ１０７）

無線端末８は、ＡＰ５からの接続応答信号（Prove Response）を受け取ると、当該無線端末８と同じ「ＳＳＩＤ２」であるＡＰ５に接続処理を行い、「ＳＳＩＤ２」で無線ＬＡＮと接続をする。

以降、無線端末８は、発呼する際、「ＳＳＩＤ２」での接続先サーバである「サバイバルサーバ２のＩＰアドレス２」宛に発呼信号を送信する。

これにより、無線端末８からの発呼信号がＡＰ５を介してサバイバルサーバ２へ到達する。そして、サバイバルサーバ２は、無線端末８からの発呼信号に基づき呼処理をする。

【００６６】

図７は実施の形態１に係る通信障害時のネットワーク接続を示す図である。

図８は実施の形態１に係るサーバ切り替え動作を示すシーケンス図である。

次に、図７に示すように、ＡＰ６と本体サーバ１との間の通信に障害が生じ、ＡＰ６とサバイバルサーバ３との間の通信が正常の場合の動作を、図８に基づき説明する。

【００６７】

（Ｓ２０１）

ＡＰ６の監視部１０４は、記憶部１０３に記憶されたプロファイルに基づき、「監視対象フラグＯＮ」である「本体サーバ１のＩＰアドレス１」、及び「サバイバルサーバ３のＩＰアドレス３」との通信状態を、有線ＬＡＮ通信部１０１を介して監視する。

図７の状態においては、監視部１０４は、本体サーバ１との接続に失敗するため、ＡＰ６と本体サーバ１との間の通信に障害が生じていると認識する。

また、監視部１０４は、サバイバルサーバ３との接続に成功するため、ＡＰ６とサバイバルサーバ３との間の通信は正常であると認識する。

【００６８】
（Ｓ２０２）
ＡＰ６の監視部１０４は、サーバに接続が失敗し、障害と認識すると、記憶部１０３に記憶されたプロファイルのうち、監視対象フラグがＯＮ、且つ、接続に成功するサバイバルサーバ３が含まれる「プロファイル名３」に基づき、ＳＳＩＤを「ＳＳＩＤ３」とし、対応するスキャン方式を「パッシブ」として、無線ＬＡＮ通信部１０２に設定する。
尚、「ＳＳＩＤ３」は、本発明における第２のネットワーク識別子に相当する。
【００６９】
（Ｓ２０３）
ＡＰ６の無線ＬＡＮ通信部１０２は、監視部１０４からＳＳＩＤが「ＳＳＩＤ３」、及び対応するスキャン方式が「パッシブ」に設定されると、無線ＬＡＮに切断信号（Deauthentication）のメッセージ、及び当該ＡＰ６に設定されてた「ＳＳＩＤ３」を含めた制御信号（ビーコン）を送出し、再帰処理を実施する。
【００７０】
（Ｓ２０４）
無線端末９は、ＡＰ６から切断信号（Deauthentication）のメッセージを受信すると、ＡＰ６との接続を切断する。更に、無線端末９は、ＡＰ６から「ＳＳＩＤ３」を含めた制御信号（ビーコン）を受信する。
無線端末９は、ＡＰ６から「ＳＳＩＤ３」を含めた制御信号（ビーコン）を受け取ると、当該無線端末９のＳＳＩＤを「ＳＳＩＤ３」に設定し、ＡＰ６に接続処理を行い、「ＳＳＩＤ３」で無線ＬＡＮと接続をする。
以降、無線端末８は、発呼する際、「ＳＳＩＤ３」での接続先サーバである「サバイバルサーバ３のＩＰアドレス３」宛に発呼信号を送信する。
これにより、無線端末９からの発呼信号がＡＰ６を介してサバイバルサーバ３へ到達する。そして、サバイバルサーバ３は、無線端末９からの発呼信号に基づき呼処理をする。
【００７１】
次に、通信障害が復旧した場合の動作について説明する。
例えば、図５に示した、ＡＰ５と本体サーバ１との間の通信障害が復旧した場合を例に説明する。
【００７２】
ＡＰ５の監視部１０４は、定期的又は継続して通信状態の監視を行う。
ＡＰ５の監視部１０４は、記憶部１０３に記憶されたプロファイルに基づき、「監視対象フラグＯＮ」である「本体サーバ１のＩＰアドレス１」、及び「サバイバルサーバ２のＩＰアドレス２」との通信状態を、有線ＬＡＮ通信部１０１を介して監視する。
通信障害が復旧した場合においては、監視部１０４は、ＡＰ５と本体サーバ１及びサバイバルサーバ２との間の通信は正常であると認識する。
【００７３】
ＡＰ５の監視部１０４は、本体サーバ１との接続が成功すると、本体サーバ１が含まれる「プロファイル名１」の「ＳＳＩＤ１」を無線ＬＡＮ通信部１０２に設定する。
尚、プロファイル名１のスキャン方式には何も記憶されていないので、無線ＬＡＮ通信部１０２にスキャン方式を設定しない。このとき無線ＬＡＮ通信部１０２は、上述した通常のスキャンに対応する。
【００７４】
ＡＰ５の無線ＬＡＮ通信部１０２は、無線ＬＡＮに切断信号（Deauthentication）のメッセージを送出し、再帰処理を実施する。
【００７５】
無線端末８は、ＡＰ５から切断信号（Deauthentication）のメッセージを受信すると、ＡＰ５との接続を切断する。
以下、上述した動作と同様に、アクティブスキャン又はパッシブスキャンにより、ＡＰ５を捕捉し、当該無線端末８のＳＳＩＤを「ＳＳＩＤ１」に設定し、ＡＰ５と接続処理を

行い、「ＳＳＩＤ１」で無線ＬＡＮと接続をする。
以降、無線端末８は、発呼する際、「ＳＳＩＤ１」での接続先サーバである「本体サーバ１のＩＰアドレス１」宛に発呼信号を送信する。
これにより、無線端末８からの発呼信号がＡＰ５を介して本体サーバ１へ到達する。そして、本体サーバ１は、無線端末８からの発呼信号に基づき呼処理をする。
【００７６】
以上のように本実施の形態においては、アクセスポイントは、サーバと当該アクセスポイントとの間の通信状態を検出し、この通信状態に応じて当該アクセスポイントのＳＳＩＤを設定し、端末はＳＳＩＤに応じて、本体サーバ１又はサバイバルサーバ２若しくは３と情報通信を行う。
このため、同一のＳＳＩＤでのサーバ切り替えに対応していない端末であっても、サーバ切り替えを行うことができる。これにより、サービス利用が不可となるのを回避することができる。
【００７７】
また、障害などにより情報通信（登録）ができないサーバに対して、端末から登録を繰り返すことがないため、ネットワーク輻輳を防止することができる。
【００７８】
また、端末は、通信可能なアクセスポイントに設定されたＳＳＩＤを、当該端末のＳＳＩＤに設定し、このＳＳＩＤに対応するサーバを接続先のサーバに設定する。
このため、端末が拠点間を移動した場合であっても、当該拠点のアクセスポイントとサーバとの間の通信状態に応じて、適切なサーバに対して登録を行うことができる。
つまり、例えば無線端末８が、拠点Ｂにおいて、本体サーバ１とＡＰ５との間に通信障害が生じて、「ＳＳＩＤ２」を用いてサバイバルサーバ２と情報通信を行った後、拠点Ｃに移動した場合、ＡＰ６に設定された「ＳＳＩＤ１」により本体サーバ１と情報通信を行うことができる。
【００７９】
また、端末は、通信可能なアクセスポイントに設定されたＳＳＩＤを、当該端末のＳＳＩＤに設定し、このＳＳＩＤに対応するサーバを接続先のサーバに設定する。
このため、端末は、サーバとアクセスポイントとの間の通信状態を監視することなく、接続先のサーバを切り替えることができる。これにより、端末を簡易な構成とすることができる。
【００８０】
尚、本実施の形態１では、ＳＳＩＤ、及び対応するスキャン方式を設定する際、無線ＬＡＮに切断信号（Deauthentication）のメッセージを送出する場合を説明したが、本発明はこれに限るものではなく、無線ＬＡＮに切断信号（Deauthentication）のメッセージを送出しなくても良い。
この場合、ＡＰがＳＳＩＤを変更すると端末はＡＰと通信できなくなる。そうすることで、ＡＰから切断信号を送出しなくても、端末はＡＰを捕捉できないとき、当該端末に記憶されている別のプロファイルに含まれるアクセスポイントをスキャンすることにより、再帰処理がなされる。
【００８１】
実施の形態２．
上記実施の形態１では、ＡＰはサーバとの通信状態を監視したが、本実施の形態２では、ＡＰはサーバの負荷状況を監視する。
本実施の形態２における各ＡＰの記憶部１０３には、上述したプロファイルデータに加え、負荷の閾値データが記憶される。
【００８２】
尚、本実施の形態２における無線通信システムの構成は、上記実施の形態１と同様であり、同様の構成には同様の符号を付する。
【００８３】

図９はＡＰの記憶部に記憶された負荷の閾値データを示す図である。
図９においては、ＡＰ４の記憶部１０３に記憶された負荷の閾値データの一例を示している。

【００８４】
図９に示すように、負荷の閾値データは、監視対象サーバのＩＰアドレスと、ＣＰＵ使用率の閾値と、メモリ使用率の閾値と、ＮＷリソース使用率の閾値とにより構成されている。

【００８５】
以下、ＡＰ４に記憶された負荷の閾値データの例に基づいて、本実施の形態２における動作について説明する。

【００８６】
監視部１０４は、ＳＮＭＰ（Simple Network Management Protocol）（ＲＦＣ１１５７など）、ＳＮＭＰ ｖｅｒｓｉｏｎ ２（ＲＦＣ１４４１など）およびＳＮＭＰ ｖｅｒｓｉｏｎ ３（ＲＦＣ３４１１など）に基づくメッセージタイプを用いて、ＣＰＵ使用率、メモリ使用率、及びＮＷリソース使用率の情報要求を、監視対象サーバに行う。
つまり、ＡＰ４の監視部１０４は、「本体サーバ１のＩＰアドレス１」、「サバイバルサーバ２のＩＰアドレス２」、及び「サバイバルサーバ３のＩＰアドレス３」に対して情報要求を行う。
監視部１０４は、ＳＮＭＰ、ＳＮＭＰ ｖｅｒｓｉｏｎ ２及びＳＮＭＰ ｖｅｒｓｉｏｎ ３に基づくメッセージタイプを用いて情報要求を実現するためにプロトコルスタックを有しており、このプロトコルスタックを介して情報要求を生成し送信し、情報応答を得るときは、このプロトコルスタックを介して受信することで情報応答を解釈する。このプロトコルスタックを拡張することで、拡張されたＳＮＭＰのメッセージタイプを用いた情報要求の送信と情報応答の受信が可能となる。

【００８７】
尚、ＣＰＵ使用率、メモリ使用率、及びＮＷリソース使用率の少なくとも１つは、本発明における負荷状態に相当する。

【００８８】
ＡＰ４からの情報要求を受けた本体サーバ１、サバイバルサーバ２及びサバイバルサーバ３は、当該サーバのＣＰＵ使用率、メモリ使用率、及びＮＷリソース使用率の情報をＡＰ４に応答する。

【００８９】
ＡＰ４の監視部１０４は、本体サーバ１、サバイバルサーバ２及びサバイバルサーバ３からの情報応答を得る。
そして、情報応答に含まれるＣＰＵ使用率、メモリ使用率、及びＮＷリソース使用率情報と、負荷の閾値データとを照合し、閾値で定められた条件に合致する場合は、当該サーバが高負荷状態である認識する。

【００９０】
ここで、図９に示すように、負荷の閾値データにおいて、ＣＰＵ使用率、メモリ使用率、及びＮＷリソース使用率のうち、閾値が設定されていない部分（空白の部分）は、情報応答との照合を行わない。
つまり、ＡＰ４の監視部１０４は、サバイバルサーバ２についてはＣＰＵ使用率が９０％以上であるか否かを照合し、サバイバルサーバ３についてはＣＰＵ使用率が９０％以上であるか否かを照合し、さらに、メモリ使用率８５％以上であるか否かを照合する。

【００９１】
各ＡＰは、このような負荷状態の検出を常時又は定期的に行う。

【００９２】
次に、ＡＰの監視部１０４は、情報要求を行ったサーバが高負荷状態と認識すると、記憶部１０３に記憶されたプロファイルのうち、監視対象フラグがＯＮ、且つ、接続に成功し、且つ、高負荷状態ではないサーバが含まれるプロファイルのＳＳＩＤ、及び対応する

スキャン方式を無線ＬＡＮ通信部１０２に設定する。
例えば、ＡＰ５において、本体サーバ１が高負荷状態と認識し、サバイバルサーバ２は高負荷状態でないと認識した場合であって、サバイバルサーバ２との接続に成功するときには、図３（ｂ）に示した、「プロファイル名２」に基づいて、ＳＳＩＤを「ＳＳＩＤ２」とし、及び対応するスキャン方式を「アクティブ」として、無線ＬＡＮ通信部１０２に設定する。
【００９３】
以降の動作は、上記実施の形態１と同様である。
【００９４】
以上のように本実施の形態においては、アクセスポイントは、サーバの負荷状態を検出し、この負荷状態に応じて当該アクセスポイントのＳＳＩＤを設定し、端末はＳＳＩＤに応じて、本体サーバ１又はサバイバルサーバ２若しくは３と情報通信を行う。
これによりＡＰは、サーバが高負荷状態で障害となる可能性があると、障害にいたる前にＳＳＩＤを切替え、端末を別のサーバに接続させることができる。
【００９５】
尚、上記実施の形態１においては、監視部１０４はＲＦＣ７９２に基づくメッセージタイプを用いたＩＣＭＰ　ｐｉｎｇ、及びＲＦＣ３２６１に基づくＳＩＰメッセージを用いたＳＩＰプロトコルの少なくとも一方で接続要求し障害と認識することによりＳＳＩＤを切り替えた。
また、実施の形態２においては、監視部１０４は、ＳＮＭＰ、ＳＮＭＰ　ｖｅｒｓｉｏｎ　２、又はＳＮＭＰ　ｖｅｒｓｉｏｎ　３のメッセージタイプを用いた情報要求で高負荷状態と認識することによりＳＳＩＤを切り替えた。
本発明はこれに限るものではなく、通信障害及び高負荷状態の何れか一方、又は双方に基づいてＳＳＩＤを切り替えるようにしても良い。
つまり、監視部１０４に対し障害認識、及び負荷認識の設定をすることで、監視部１０４は障害認識のみを行うか、負荷認識のみを行うか、それとも、障害認識、及び負荷認識を行うかを選択するようにしても良い。
【００９６】
実施の形態３．
上記実施の形態１では、ＡＰがサーバとの通信状態を監視し、通信状態に基づいてＡＰのネットワーク識別子（ＳＳＩＤ）を設定した。また、上記実施の形態２では、ＡＰがサーバの負荷状態を監視し、負荷状態に基づいてＡＰのネットワーク識別子を設定した。
本実施の形態３では、コントローラがサーバとの通信状態を監視し、通信状態に基づいてＡＰのネットワーク識別子を設定する。
以下、本発明における無線通信システムを、コントローラ型無線ＩＰ電話システムに適用した形態について説明する。
【００９７】
まず、本実施の形態３における無線通信システムの構成について、上記実施の形態１との相違点を中心に説明する。尚、上記実施の形態１と同様の構成には同様の符号を付する。
【００９８】
図１０は実施の形態３に係る無線ＩＰ電話システムの構成図である。
図１０に示すように、本実施の形態３に係る無線ＩＰ電話システムは、上記実施の形態１の無線ＩＰ電話システム（図１）の構成に加え、コントローラ１０、コントローラ１１、及びコントローラ１２を備える。
尚、サーバ１、サバイバルサーバ２及び３、無線端末７～９の構成は、上記実施の形態１と同様である。
【００９９】
コントローラ１０、コントローラ１１、及びコントローラ１２（以下、区別しないときは単に「コントローラ」ともいう。）は、本体サーバ１、サバイバルサーバ２、サバイバ

ルサーバ３と、それぞれ有線ＬＡＮで接続され、互いに通信が行える。

【０１００】

コントローラは、それぞれ拠点ごとに設置される。コントローラは、当該拠点内のＡＰを収容（接続）する。このコントローラは、収容したＡＰを制御して、無線ＬＡＮを運用するものである。

尚、本実施の形態３では、コントローラ１０～１２のそれぞれが収容するＡＰが１つずつである場合を示すが、複数のＡＰを収容することも可能である。

【０１０１】

コントローラは、ＡＰに対する設定制御を行う。詳細は後述する。

また、コントローラは、ＡＰに対するアクセス制御及びトラヒック制御を行うことが可能である。

例えば、ＡＰから流入するトラヒックに対するアクセス制御（ＦＷ（Firewall）、ＰＦ（Packet Filtering）など）がある。

また、ＡＰから流入するトラヒックに対するトラヒック制御（ＱｏＳ（Quality of Service）など）がある。

また、バックボーンから流入するトラヒックに対するアクセス制御がある。

また、バックボーンから流入するトラヒックに対するトラヒック制御がある。

尚、バックボーンとは、コントローラ１０の場合は本体サーバ１が接続する拠点ＡのＬＡＮである。

【０１０２】

本実施の形態３では、コントローラがＡＰに対する設定制御をすることでＡＰのネットワーク識別子（ＳＳＩＤ）を設定する。

このため、実施の形態３では、コントローラがサーバとの通信状態を監視し、通信状態に基づいてＡＰのネットワーク識別子を設定する。

【０１０３】

各端末は、ＡＰとコントローラとを介して、本体サーバ１、又はサバイバルサーバ２若しくは３と情報通信を行う。

例えば、拠点Ｂに存在する無線端末８は、ＡＰ５及びコントローラ１１を介して、本体サーバ１又はサバイバルサーバ２と情報通信し、各拠点内の端末（例えば無線端末７等）と通信する。

【０１０４】

次に、コントローラの構成を説明する。

【０１０５】

図１１は実施の形態３に係るコントローラの構成図である。

図１１に示すように、コントローラは、第一有線ＬＡＮ通信部２０１と、第二有線ＬＡＮ通信部２０２と、記憶部２０３と、監視部２０４と、ＡＰ制御部２０５とにより構成されている。

【０１０６】

第一有線ＬＡＮ通信部２０１は、拠点の有線ＬＡＮと接続する。

第二有線ＬＡＮ通信部２０２は、有線ＬＡＮと接続してＡＰと接続する。

第一有線ＬＡＮ通信部２０１と第二有線ＬＡＮ通信部２０２とは互いに接続し、通信を中継できる。

記憶部２０３は、複数のプロファイルが記憶される。

【０１０７】

コントローラ１０～１２の記憶部２０３に記憶されるプロファイルデータは、上記実施の形態１においてＡＰ４～６の記憶部１０３に記憶されたプロファイルデータ（図３）と同様である。

【０１０８】

即ち、ＡＰ４を収容するコントローラ１０の記憶部２０３は、図３（ａ）に示すプロファイルを記憶している。

また、ＡＰ５を収容するコントローラ１１の記憶部２０３は、図３（ｂ）に示すプロファイルを記憶している。
また、ＡＰ６を収容するコントローラ１２の記憶部２０３は、図３（ｃ）に示すプロファイルを記憶している。
このように、記憶部２０３に記憶されるプロファイルは、コントローラごとに異なる。
【０１０９】
尚、１つのコントローラが複数のＡＰを収容する場合は、記憶部２０３には複数のＡＰごとの複数のプロファイルが記憶される。
この場合、ＡＰごとに複数のプロファイルを参照できるように、例えばＡＰの名前やＩＰアドレスなどのＡＰ別識別子と、複数のＡＰごとの複数のプロファイルとを対にして記憶する。これにより、ＡＰ別識別子をキーにＡＰごとに複数のプロファイルを参照できるようになる。
【０１１０】
コントローラ１０～１２の監視部２０４は、記憶部２０３が記憶するプロファイルに基づきサーバを監視する。
監視部２０４は、記憶部２０３に記憶されたプロファイルの監視対象フラグに基づき、「監視対象フラグＯＮ」に設定されている本体サーバ１、サバイバルサーバ２及び３を監視する。
【０１１１】
つまり、コントローラ１０の記憶部２０３は、図３（ａ）のように、「本体サーバ１のＩＰアドレス１」が「監視対象フラグＯＮ」に設定されているので、コントローラ１０の監視部２０４は、「本体サーバ１のＩＰアドレス１」に基づいて監視する。
コントローラ１１、１２も同様に、記憶部２０３のプロファイルに基づき監視する。
【０１１２】
尚、「本体サーバ１のＩＰアドレス１」、「サバイバルサーバ２のＩＰアドレス２」、及び「サバイバルサーバ３のＩＰアドレス３」は、本発明における本体サーバ又はサバイバルサーバの識別情報に相当する。
【０１１３】
監視部２０４は、サーバと当該コントローラとの間の通信状態を監視（検出）する。
通信状態を監視する手段は、上記実施の形態１と同様に、ＩＣＭＰ　ｐｉｎｇ、及びＳＩＰメッセージを用いたＳＩＰプロトコルの少なくとも一方で接続要求し、サーバから接続応答を得ることで通信状態を検出する。
監視部２０４は、接続要求し、サーバから接続応答を得ることができるとき、接続が成功し、サーバとコントローラとの間の通信は正常であると認識する。
また、監視部２０４は、接続要求し、サーバから接続応答を得ることができないと、接続が失敗し、サーバとコントローラとの間の通信に障害が生じていると認識する。
【０１１４】
コントローラの監視部２０４は、サーバに接続が失敗し、障害と認識すると、記憶部２０３に記憶されたプロファイルのうち、監視対象フラグがＯＮ、且つ、接続に成功するサーバが含まれるプロファイルのＳＳＩＤ、及び対応するスキャン方式をＡＰ制御部２０５に与える。
尚、プロファイルのスキャン方式に何も記憶されていない場合は、スキャン方式を設定しない。
【０１１５】
ＡＰ制御部２０５は、監視部２０４の監視に基づきＡＰを制御する。
また、ＡＰ制御部２０５は、ＡＰを制御するために、ＡＰに設定するＳＳＩＤ及び対応するスキャン方式を保持する。
尚、プロファイルのスキャン方式に何も記憶されていない場合は、スキャン方式の保持をしない。
【０１１６】

このＡＰ制御部２０５によるＡＰに対する設定制御について説明する。
まず、ＡＰ制御部２０５は、コントローラが起動した直後の制御として、ＡＰに対する初期設定制御を行う。
ＡＰ制御部２０５は、当該コントローラが起動すると、記憶部２０３に記憶されたプロファイルからＳＳＩＤを保持する。そして、当該コントローラに接続するＡＰに対し、当該ＳＳＩＤの情報を含む設定信号を、第二有線ＬＡＮ通信部を介して送出する。これによりＡＰにＳＳＩＤを設定する。
起動時に設定するＡＰのＳＳＩＤは、拠点ごとのＡＰで同一となるよう設定するようにするため、記憶部２０３に記憶されたプロファイルのうち、最上段に示されるＳＳＩＤを初期設定制御で設定するＳＳＩＤとする。

【０１１７】
つまり、例えば、コントローラ１０の記憶部２０３は、図３（ａ）のように、最上段で「ＳＳＩＤ１」と示されているので、コントローラ１０のＡＰ制御部２０５は初期設定制御でＡＰ４に「ＳＳＩＤ１」を設定する。
コントローラ１１、１２も同様に、記憶部２０３に記憶されたプロファイルの最上段で示される「ＳＳＩＤ１」をＡＰ５、ＡＰ６に設定する。

【０１１８】
このような初期設定制御により、それぞれのコントローラが収容するそれぞれのＡＰのＳＳＩＤを同一とする設定がなされる。

【０１１９】
尚、上述の初期設定制御は、コントローラが起動したときＡＰにＳＳＩＤを設定する場合を説明したが、これに限るものではない。例えば、ＡＰが起動時にコントローラへの設定依頼をする場合には、設定依頼を受けたコントローラは、ＡＰ制御部２０５で保持するＳＳＩＤ及び対応するスキャン方式を、設定依頼をするＡＰに設定するようにすることもできる。

【０１２０】
次に、ＡＰ制御部２０５は、監視部２０４の監視に基づく制御として、ＡＰに対する設定制御を行う。
ＡＰ制御部２０５は、初期設定制御の後に、監視部２０４がサーバとの接続に失敗し、サーバとコントローラとの間の通信に障害が生じていると認識するとき、監視部２０４から与えられるＳＳＩＤ、及び対応するスキャン方式をＡＰに設定する。
この設定は、ＡＰに設定するＳＳＩＤ、及び対応するスキャン方式の情報を含む設定信号を、第二有線ＬＡＮ通信部２０２を介して送出することにより行う。
尚、プロファイルのスキャン方式に何も記憶されていない場合は、スキャン方式を設定しない。

【０１２１】
尚、コントローラが複数のＡＰを収容する場合は、上記の初期設定制御及び設定制御において、設定信号に設定対象となるＡＰのＡＰ別識別子を含めて、設定対象のＡＰを判断できるようにしても良い。

【０１２２】
次に、ＡＰの構成を説明する。

【０１２３】
図１２は実施の形態３に係るアクセスポイントの構成図である。
図１２に示すように、ＡＰは、有線ＬＡＮ通信部３０１と、無線ＬＡＮ通信部３０２とにより構成されている。
有線ＬＡＮ通信部３０１は、有線ＬＡＮと接続しコントローラと接続する。
無線ＬＡＮ通信部３０２は、無線ＬＡＮと接続する。
有線ＬＡＮ通信部３０１と無線ＬＡＮ通信部３０２とは互いに接続し、通信を中継できる。

【０１２４】

また、無線ＬＡＮ通信部３０２は、コントローラからの初期設定制御及び設定制御によりＳＳＩＤ、及び対応するスキャン方式（設定される場合に限る）が設定される。

【０１２５】

この設定を具体的に説明する。

コントローラのＡＰ制御部２０５の初期設定制御及び設定制御において、設定信号が送出される。この設定信号はＡＰの有線ＬＡＮ通信部３０１に到達する。

そして、図１２に図示されていないＡＰの制御部が、設定信号に基づいて無線ＬＡＮ通信部３０２を設定する。

ここで、ＡＰの制御部とは、ＡＰ内部に存在するＣＰＵ（Central Processing Unit）やＤＳＰ（Digital Signal Processor）などである。

【０１２６】

尚、コントローラが複数のＡＰを収容する場合は、コントローラからの設定信号にＡＰ別識別子を含めて送出する。ＡＰの制御部は、設定信号にＡＰ別識別子が含まれているときは、このＡＰ別識別子に基づいて自身（当該ＡＰ）を含むＡＰが設定対象であるか否かを判断する。そして、自身（当該ＡＰ）が設定対象の場合に、当該設定信号に基づいて無線ＬＡＮ通信部３０２を設定する。

【０１２７】

次に、本体サーバ１とコントローラとの間に障害が生じた場合の動作を説明する。

【０１２８】

図１３は実施の形態３に係る通信障害時のネットワーク接続を示す図である。

図１４は実施の形態３に係るサーバ切り替え動作を示すシーケンス図である。

まず、図１３に示すように、コントローラ１１と本体サーバ１との間の通信に障害が生じ、コントローラ１１とサバイバルサーバ２との間の通信が正常の場合の動作を、図１４に基づき説明する。

【０１２９】

（Ｓ３０１）

まず、コントローラ１１のＡＰ制御部２０５は、記憶部２０３で記憶されたプロファイルの最上段で示される「ＳＳＩＤ１」を保持し、初期設定制御によりＡＰ５に「ＳＳＩＤ１」を設定する。

ここで、ＡＰ５は、ＳＳＩＤが設定されると、設定された「ＳＳＩＤ１」を含めた制御信号（ビーコン）が送出可能となる。

このとき、ＡＰ５は、対応するスキャン方式が設定されていないので、通常のスキャンに対応することになる。

【０１３０】

定常時においては、上記実施の形態１で説明した通常のスキャン方式により、無線端末８はＡＰ５に接続処理を行う。そして、無線端末８は、発呼信号を「ＳＳＩＤ１」での接続先サーバである「本体サーバ１のＩＰアドレス１」宛に送信する。

これにより、無線端末８からの通信情報が、ＡＰ５及びコントローラ１１を介して本体サーバ１へ到達することとなる。

尚、定常時における呼処理、通話の確立等の動作は、上記実施の形態１と同様である。

【０１３１】

（Ｓ３０２）

コントローラ１１の監視部２０４は、記憶部２０３に記憶されたプロファイルに基づき、「監視対象フラグＯＮ」である「本体サーバ１のＩＰアドレス１」、及び「サバイバルサーバ２のＩＰアドレス２」との通信状態を、第一有線ＬＡＮ通信部２０１を介して監視する。

図１３の状態においては、監視部２０４は、本体サーバ１との接続に失敗するため、コントローラ１１と本体サーバ１との間に障害が生じていると認識する。

また、監視部２０４は、サバイバルサーバ２との接続に成功するため、コントローラ１１とサバイバルサーバ２との間の通信は正常であると認識する。

【０１３２】
（Ｓ３０３）
コントローラ１１の監視部２０４は、本体サーバ１に接続が失敗し、障害と認識すると、記憶部２０３に記憶されたプロファイルのうち、監視対象フラグがＯＮ、且つ、接続に成功するサバイバルサーバ２が含まれる「プロファイル名２」に基づいて、ＳＳＩＤを「ＳＳＩＤ２」とし、及び対応するスキャン方式「アクティブ」の設定情報をＡＰ制御部２０５に与える。
続いて、コントローラ１１のＡＰ制御部２０５は、与えられた設定情報に基づいて設定制御をして、ＡＰ５の設定をする。
このとき、ＡＰ制御部２０５は、「ＳＳＩＤ２」及び対応するスキャン方式「アクティブ」とする設定情報を含む設定信号を、第二有線ＬＡＮ通信部２０２を介して送出する。
【０１３３】
（Ｓ３０４）
ＡＰ５の無線ＬＡＮ通信部３０２は、到達した設定信号に基づき、自身に「ＳＳＩＤ２」、及び対応するスキャン方式を「アクティブ」と設定する。
ＡＰ５の無線ＬＡＮ通信部３０２は設定を終えると、無線ＬＡＮに切断信号（Deauthentication）のメッセージを送出し、再帰処理を実施する。
【０１３４】
（Ｓ３０５）
無線端末８は、ＡＰ５から切断信号（Deauthentication）のメッセージを受信すると、ＡＰ５との接続を切断する。そして、再び「ＳＳＩＤ１」に設定されているアクセスポイントをスキャンするため、接続要求信号（Probe Request）のメッセージを送出する。
ここで、ＡＰ５は、「ＳＳＩＤ２」に設定されているので応答しない。
【０１３５】
（Ｓ３０６）
無線端末８は、「ＳＳＩＤ１」に設定されたアクセスポイントを捕捉できないとき、当該無線端末８に記憶されている別のプロファイルに含まれる「ＳＳＩＤ２」に設定されているアクセスポイントをスキャンするため、接続要求信号（Probe Request）のメッセージを送出する。
【０１３６】
（Ｓ３０７）
ＡＰ５は、「ＳＳＩＤ２」に設定されているので、受け取った接続要求信号（Probe Request）に対し、当該ＡＰ５に設定されている「ＳＳＩＤ２」を含めた接続応答信号（Probe Response）を送出して応答する。
【０１３７】
（Ｓ３０８）
無線端末８は、ＡＰ５から接続応答信号（Probe Response）を受け取ると、当該無線端末８と同じ「ＳＳＩＤ２」であるＡＰ５に接続処理を行い、「ＳＳＩＤ２」で無線ＬＡＮと接続をする。
以降、無線端末８は、発呼する際、「ＳＳＩＤ２」での接続先であるサーバである「サバイバルサーバ２のＩＰアドレス２」宛に発呼信号を送信する。
これにより、無線端末８からの発呼信号がＡＰ５とコントローラ１１を介してサバイバルサーバ２へ到達する。そして、サバイバルサーバ２は、無線端末８からの発呼信号に基づき呼処理をする。
【０１３８】
尚、「ＳＳＩＤ１」は、本発明における第１のネットワーク識別子に相当し、「ＳＳＩＤ２」は、本発明における第２のネットワーク識別子に相当する。
【０１３９】
図１５は実施の形態３に係る通信障害時のネットワーク接続を示す図である。
図１６は実施の形態３に係るサーバ切り替え動作を示すシーケンス図である。

次に、図１５に示すように、コントローラ１２と本体サーバ１との間の通信に障害が生じ、コントローラ１２とサバイバルサーバ３との間の通信が正常の場合の動作を、図１６に基づき説明する。

【０１４０】

（Ｓ４０１）

まず、コントローラ１２のＡＰ制御部２０５は、記憶部２０３で記憶されたプロファイルの最上段で示される「ＳＳＩＤ１」を保持し、初期設定制御によりＡＰ６に「ＳＳＩＤ１」を設定する。

ここで、ＡＰ６は、ＳＳＩＤが設定されると、設定された「ＳＳＩＤ１」を含めた制御信号（ビーコン）が送出可能となる。

このとき、ＡＰ６は、対応するスキャン方式が設定されていないので、通常のスキャンに対応することになる。

【０１４１】

定常時においては、上記実施の形態１で説明した通常のスキャン方式により、無線端末９はＡＰ６に接続処理を行う。そして、無線端末９は、発呼信号を「ＳＳＩＤ１」での接続先サーバである「本体サーバ１のＩＰアドレス１」宛に送信する。

これにより、無線端末９からの通信情報が、ＡＰ６及びコントローラ１２を介して本体サーバ１へ到達することとなる。

尚、定常時における呼処理、通話の確立等の動作は、上記実施の形態１と同様である。

【０１４２】

（Ｓ４０２）

コントローラ１２の監視部２０４は、記憶部２０３に記憶されたプロファイルに基づき、「監視対象フラグＯＮ」である「本体サーバ１のＩＰアドレス１」、及び「サバイバルサーバ３のＩＰアドレス３」との通信状態を、第一有線ＬＡＮ通信部２０１を介して監視する。

図１５の状態においては、監視部２０４は、本体サーバ１との接続に失敗するため、コントローラ１２と本体サーバ１との間に障害が生じていると認識する。

また、監視部２０４は、サバイバルサーバ３との接続に成功するため、コントローラ１２とサバイバルサーバ３との間の通信は正常であると認識する。

【０１４３】

（Ｓ４０３）

コントローラ１２の監視部２０４は、本体サーバ１に接続が失敗し、障害と認識すると、記憶部２０３に記憶されたプロファイルのうち、監視対象フラグがＯＮ、且つ、接続に成功するサバイバルサーバ３が含まれる「プロファイル名３」に基づいて、ＳＳＩＤを「ＳＳＩＤ３」とし、及び対応するスキャン方式「パッシブ」の設定情報をＡＰ制御部２０５に与える。

続いて、コントローラ１２のＡＰ制御部２０５は、与えられた設定情報に基づいて設定制御をして、ＡＰ６の設定をする。

このとき、ＡＰ制御部２０５は、「ＳＳＩＤ３」及び対応するスキャン方式「パッシブ」とする設定情報を含む設定信号を、第二有線ＬＡＮを介して送出する。

【０１４４】

（Ｓ４０４）

ＡＰ６の無線ＬＡＮ通信部３０２は、到達した設定信号に基づき、自身に「ＳＳＩＤ３」、及び対応するスキャン方式を「パッシブ」と設定する。

ＡＰ６の無線ＬＡＮ通信部３０２は設定を終えると、無線ＬＡＮに切断信号（Deauthentication）のメッセージ、及び当該ＡＰ６に設定された「ＳＳＩＤ３」を含めた制御信号（ビーコン）を送出し、再帰処理を実施する。

【０１４５】

（Ｓ４０５）

無線端末９は、ＡＰ６から切断信号（Deauthentication）のメッセージを受信すると、

ＡＰ６との接続を切断する。さらに、無線端末９は、ＡＰ６から「ＳＳＩＤ３」を含めた制御信号（ビーコン）を受信する。

無線端末９は、ＡＰ６から「ＳＳＩＤ３」を含めた制御信号（ビーコン）を受け取ると、当該無線端末９のＳＳＩＤを「ＳＳＩＤ３」に設定し、ＡＰ６に接続処理を行い、「ＳＳＩＤ３」で無線ＬＡＮと接続する。

以降、無線端末９は、発呼する際、「ＳＳＩＤ３」での接続先サーバである「サバイバルサーバ３のＩＰアドレス３」宛に発呼信号を送信する。

これにより、無線端末９からの発呼信号がＡＰ６とコントローラ１２を介してサバイバルサーバ３へ到達する。そして、サバイバルサーバ３は、無線端末９からの発呼信号に基づき呼処理をする。

【０１４６】

尚、「ＳＳＩＤ１」は、本発明における第１のネットワーク識別子に相当し、「ＳＳＩＤ３」は、本発明における第２のネットワーク識別子に相当する。

【０１４７】

以上のように本実施の形態においては、コントローラは、サーバと当該コントローラとの間の通信状態を検出し、この通信状態に応じてアクセスポイントのＳＳＩＤを設定し、端末はＳＳＩＤに応じて、本体サーバ１又はサバイバルサーバ２若しくは３と情報通信を行う。このため、上記実施の形態１と同様の効果を奏することができる。

【０１４８】

また、コントローラによりサーバの通信状態の監視を行い、ＡＰに対してＳＳＩＤの設定制御を行う。

このため、ＡＰの構成を簡素化することが可能となる。また、既存のネットワークシステムにおいても、当該コントローラを追加する構成とすることで、サーバ切り替えを行うことができるシステムを構築することが可能となる。

【０１４９】

尚、本実施の形態３は、通信状態に基づいてＡＰのＳＳＩＤを設定する形態について説明したが、本発明はこれに限るものではなく、上記実施の形態２で説明したサーバの負荷状態に基づいてＡＰのＳＳＩＤを設定しても良い。

また、通信障害及び高負荷状態の何れか一方、又は双方に基づいてＳＳＩＤを切り替えるようにしても良い。

つまり、コントローラの監視部２０４に対し障害認識、及び負荷認識の設定をすることで、監視部２０４は障害認識のみを行うか、負荷認識のみを行うか、それとも、障害認識、及び負荷認識を行うかを選択するようにしても良い。尚、この場合、監視部２０４による負荷監視は、上記実施の形態２の監視部１０４と同様の動作を行うことができる。

【０１５０】

実施の形態４．

上記実施の形態３では、コントローラがサーバとの通信状態を監視し、通信状態に基づいてＡＰのネットワーク識別子（ＳＳＩＤ）を設定した。

本実施の形態４では、ネットワーク管理装置がサーバとの通信状態を監視し、通信状態に基づいてＡＰのネットワーク識別子を設定する。

以下、本発明における無線通信システムを、ネットワーク管理装置により管理された無線ＩＰ電話システムに適用した形態について説明する。

【０１５１】

まず、本実施の形態４における無線通信システムの構成について、上記実施の形態１及び３との相違点を中心に説明する。尚、上記実施の形態１及び３と同様の構成には同様の符号を付する。

【０１５２】

図１７は実施の形態４に係る無線ＩＰ電話システムの構成図である。

図１７に示すように、本実施の形態４に係る無線ＩＰ電話システムは、上記実施の形態１の無線ＩＰ電話システム（図１）の構成に加え、ネットワーク管理装置２０を備える。

尚、本体サーバ１、サバイバルサーバ２及び３、無線端末７～９の構成は、上記実施の形態１と同様である。

【０１５３】

ネットワーク管理装置２０は、ネットワークを介してＡＰと接続される。

このネットワーク管理装置２０は、ＳＮＭＰ、又はＳＮＭＰｖ２のメッセージタイプを用いて、ネットワーク上のノード（サーバ及びＡＰを含む）に情報要求し、ノードから情報を取得してネットワーク管理をする装置である。したがって、図１７に示す無線ＩＰ電話システムにおいては、ネットワーク管理装置２０により管理された無線ＬＡＮを運用する。

また、ネットワーク管理装置２０は、サーバの通信状態の監視（検出）をするものである。

したがって、ネットワーク管理装置２０は、ネットワーク管理と通信状態の監視を行うものである。

【０１５４】

尚、ネットワーク管理装置２０は、ネットワーク管理機能を有するシステム及びサービスであっても良い。この場合、後述するＡＰ制御部４０５、監視部４０４及び記憶部４０３をシステム及びサービス内に含むことになる。

【０１５５】

次に、ネットワーク管理装置２０の構成を説明する。

【０１５６】

図１８は実施の形態４に係るネットワーク管理装置の構成図である。

図１８に示すように、ネットワーク管理装置２０は、有線ＬＡＮ通信部４０２と、記憶部４０３と、監視部４０４と、ＡＰ制御部４０５とにより構成されている。

【０１５７】

有線ＬＡＮ通信部４０２は、有線ＬＡＮと接続してＡＰ及びサーバと接続する。

【０１５８】

記憶部４０３は、各ＡＰごとに、複数のプロファイルが記憶される。

記憶部４０３は、ＡＰごとの複数のプロファイルを参照できるように、ＡＰの名前やＩＰアドレスなどのＡＰ別識別子と、各ＡＰごとの複数のプロファイルを対にして記憶する。これにより、ＡＰ別識別子をキーに、ＡＰごとに複数のプロファイルを参照できる。

【０１５９】

記憶部４０３に記憶されるプロファイルデータは、上記実施の形態１においてＡＰ４～６の記憶部１０３に記憶されたプロファイルデータ（図３）と同様である。

具体的には、記憶部４０３は、ＡＰ４のＡＰ別識別子と、図３（ａ）のプロファイルを対にして記憶している。また、ＡＰ５のＡＰ別識別子と、図３（ｂ）のプロファイルを対にし、ＡＰ６のＡＰ別識別子と、図３（ｃ）のプロファイルを対にして記憶している。

【０１６０】

監視部４０４は、記憶部４０３が記憶するプロファイルに基づきサーバを監視する。

監視部４０４は、記憶部４０３のプロファイルを参照し、プロファイルの監視対象フラグに基づき、「監視対象フラグＯＮ」に設定されている監視対象を監視する。

【０１６１】

具体的には、監視部４０４は、図３（ａ）を参照し「監視対象フラグＯＮ」に設定されている「本体サーバ１のＩＰアドレス１」に基づいて監視する。

同様に、図３（ｂ）を参照し「監視対象フラグＯＮ」に設定されている「本体サーバ１のＩＰアドレス１」、及び「サバイバルサーバ２のＩＰアドレス２」に基づいて監視する。

同様に、図３（ｃ）を参照し「監視対象フラグＯＮ」に設定されている「本体サーバ１のＩＰアドレス１」、及び「サバイバルサーバ３のＩＰアドレス３」に基づいて監視する。

【０１６２】

尚、「本体サーバ１のＩＰアドレス１」、「サバイバルサーバ２のＩＰアドレス２」、及び「サバイバルサーバ３のＩＰアドレス３」は、本発明における本体サーバ又はサバイバルサーバの識別情報に相当する。

【０１６３】

監視部４０４は、サーバと当該ネットワーク管理装置２０との間の通信状態を監視（検出）する。

監視部４０４による監視は、本体サーバ１とサバイバルサーバ２及びサバイバルサーバ３を接続するＬＡＮを通して監視する。

通信状態を監視する手段は、実施の形態１と同様に、ＩＣＭＰ　ｐｉｎｇ、及びＳＩＰメッセージ等を用いる。

【０１６４】

監視部４０４は、接続要求し、サーバから接続応答を得ることができるとき、接続が成功し、サーバとネットワーク管理装置２０との間の通信は正常であると認識する。

また、監視部４０４は、接続要求し、サーバから接続応答を得ることができないと、接続が失敗し、サーバとネットワーク管理装置２０との間の通信に障害が生じていると認識する。

監視部４０４は、サーバに接続が失敗し、障害と認識すると、記憶部４０３に記憶されたプロファイルのうち、監視対象フラグがＯＮ、且つ、接続に成功するサーバが含まれるプロファイルのＳＳＩＤ、及び対応するスキャン方式をＡＰ制御部４０５に与える。

尚、プロファイルのスキャン方式に何も記憶されていない場合は、スキャン方式を設定しない。

【０１６５】

ＡＰ制御部４０５は、監視部４０４の監視に基づきＡＰを制御する。

ＡＰ制御部４０５は、上記実施の形態３のＡＰ制御部２０５と同様に、ＡＰに対する設定制御を行う。ただし、ＡＰ制御部４０５は、初期設定制御を行わない点でＡＰ制御部２０５と相違する。

【０１６６】

ＡＰ制御部４０５は、監視部４０４の監視に基づく制御として、ＡＰ４～６のそれぞれに対して設定制御を行う。

ＡＰ制御部４０５は、監視部４０４がサーバとの接続に失敗し、サーバとネットワーク管理装置２０との間の通信に障害が生じていると認識するとき、監視部４０４から与えられるＳＳＩＤ、及び対応するスキャン方式をＡＰに設定する。

この設定は、ＡＰに設定するＳＳＩＤ、及び対応するスキャン方式の情報を含む設定信号を、有線ＬＡＮ通信部４０２を介して送出することにより行う。

尚、この設定信号には、設定対象となるＡＰのＡＰ別識別子を含めて、設定対象のＡＰを判断できるようにする。

尚、プロファイルのスキャン方式に何も記憶されていない場合は、スキャン方式を設定しない。

【０１６７】

次に、ＡＰの構成を説明する。

【０１６８】

本実施の形態４におけるＡＰ４～６の構成は、上記実施の形態３（図１２）で説明したＡＰと同様に、有線ＬＡＮ通信部３０１と、無線ＬＡＮ通信部３０２とにより構成されている。

【０１６９】

本実施の形態４における無線ＬＡＮ通信部３０２では、予め、ＳＳＩＤ、及び対応するスキャン方式（設定する場合に限る）が設定されている。

これは、本実施の形態４においては、上述したように、ＡＰ制御部４０５は初期設定制御を行わないためである。

【０１７０】

ここで、予め設定されるＳＳＩＤ、及び対応するスキャン方式（設定する場合に限る）は、記憶部４０３に記憶されたプロファイルのうち、最上段に示されるＳＳＩＤを設定する。

具体的には、ＡＰ４（図３（ａ））がＳＳＩＤ１、ＡＰ５（図３（ｂ））がＳＳＩＤ１、ＡＰ６（図３（ｃ））がＳＳＩＤ１と予め設定されている。

【０１７１】

また、ＡＰ４～６の無線ＬＡＮ通信部３０２は、ネットワーク管理装置２０からの設定制御によりＳＳＩＤ、及び対応するスキャン方式（設定される場合に限る）が設定される。

【０１７２】

この設定を具体的に説明する。

ネットワーク管理装置２０のＡＰ制御部４０５の設定制御において、設定信号が送出される。この設定信号はＡＰの有線ＬＡＮ通信部３０１に到達する。

そして、図示されていないＡＰの制御部は、設定信号にＡＰ別識別子が含まれているとき、このＡＰ別識別子に基づいて自身（当該ＡＰ）を含むＡＰが設定対象であるか否かを判断する。

そして、自身（当該ＡＰ）が設定対象の場合に、当該設定信号に基づいて無線ＬＡＮ通信部３０２を設定する。

【０１７３】

次に、本体サーバ１とネットワーク管理装置２０との間に障害が生じた場合の動作を説明する。

尚、定常時における呼処理、通話の確立等の動作は、上記実施の形態１と同様である。

【０１７４】

図１９は実施の形態４に係る通信障害時のネットワーク接続を示す図である。

図２０は実施の形態４に係るサーバ切り替え動作を示すシーケンス図である。

以下、図１９のようにネットワーク管理装置２０と本体サーバ１との間の通信に障害が生じ、ネットワーク管理装置２０とサバイバルサーバ２及びサバイバルサーバ３との間の通信が正常の場合の動作を、図２０に基づき説明する。

【０１７５】

（Ｓ５０１）

監視部４０４は、記憶部４０３に記憶されたプロファイルに基づき、「監視対象フラグＯＮ」である「本体サーバ１のＩＰアドレス１」、「サバイバルサーバ２のＩＰアドレス２」及び「サバイバルサーバ３のＩＰアドレス３」との通信状態を、有線ＬＡＮ通信部４０２を介して監視する。

図１９の状態においては、監視部４０４は、本体サーバ１との接続に失敗するため、ネットワーク管理装置２０と本体サーバ１との間に障害が生じていると認識する。

また、監視部４０４は、サバイバルサーバ２及びサバイバルサーバ３との接続に成功するため、ネットワーク管理装置２０とサバイバルサーバ２及びサバイバルサーバ３との間の通信は正常であると認識する。

【０１７６】

（Ｓ５０２）

ネットワーク管理装置２０の監視部４０４は、本体サーバ１に接続が失敗し、障害と認識すると、記憶部４０３に記憶された複数のＡＰごとのプロファイルのうち、監視対象フラグがＯＮ、且つ、接続に成功するサーバが含まれるプロファイルのＳＳＩＤ、及び対応するスキャン方式（設定されている場合に限る）と、ＡＰ別識別子とをＡＰ制御部４０５に与える。

【０１７７】

具体的には、ネットワーク管理装置２０と本体サーバ１との間の障害と認識され、ネットワーク管理装置２０とサバイバルサーバ２及びサバイバルサーバ３の間が接続に成功する場合は、次のようになる。

監視部４０４は、記憶部４０３に記憶されたプロファイルのうち、監視対象フラグがＯＮ、且つ、接続に成功するサバイバルサーバ２又は３が含まれるプロファイルを、最上段から最下段に向け参照する。

これにより、監視部４０４は、ＡＰ５に対応するプロファイル（図３（ｂ））において、「ＳＳＩＤ２」及び対応するスキャン方式「アクティブ」を得る。

次に、監視部４０４は、ＡＰ５に対応するプロファイル（図３（ｂ））と対に記憶されたＡＰ５のＡＰ別識別子を得る。

この結果、監視部４０４は、ＡＰ５への設定情報として、ＡＰ５のＡＰ別識別子、「ＳＳＩＤ２」及び対応するスキャン方式「アクティブ」を、ＡＰ制御部４０５に与える。

【０１７８】

同様に、監視部４０４は、記憶部４０３に記憶されたプロファイルのうち、監視対象フラグがＯＮ、且つ、接続に成功するサバイバルサーバ２又は３が含まれるプロファイルを、最上段から最下段に向け参照する。

これにより、監視部４０４は、ＡＰ６に対応するプロファイル（図３（ｃ））において、「ＳＳＩＤ３」及び対応するスキャン方式「パッシブ」を得る。

次に、監視部４０４は、ＡＰ６に対応するプロファイル（図３（ｃ））と対に記憶されたＡＰ６のＡＰ別識別子を得る。

この結果、監視部４０４は、ＡＰ６への設定情報として、ＡＰ６のＡＰ別識別子、「ＳＳＩＤ３」及び対応するスキャン方式「パッシブ」を、ＡＰ制御部４０５に与える。

【０１７９】

続いて、ネットワーク管理装置２０のＡＰ制御部４０５は、与えられた設定情報に基づいて設定制御をして、ＡＰ５及び６の設定をする。

このとき、ＡＰ制御部４０５は、ＡＰ５のＡＰ別識別子、「ＳＳＩＤ２」及び対応するスキャン方式「アクティブ」の設定情報を含む設定信号を、有線ＬＡＮ通信部４０２を介して送出する。

さらに、ＡＰ制御部４０５は、ＡＰ６のＡＰ別識別子、「ＳＳＩＤ３」及び対応するスキャン方式「パッシブ」の設定情報を含む設定信号を、有線ＬＡＮ通信部４０２を介して送出する。

【０１８０】

（Ｓ５０３）

ＡＰ５の無線ＬＡＮ通信部３０２は、到達した設定信号のうちＡＰ５のＡＰ別識別子を含む設定信号に基づき、自身に「ＳＳＩＤ２」及び対応するスキャン方式を「アクティブ」と設定する。

ＡＰ５の無線ＬＡＮ通信部３０２は設定を終えると、無線ＬＡＮに切断信号（Deauthentication）のメッセージを送出し、再帰処理を実施する。

【０１８１】

（Ｓ５０４～Ｓ５０７）

無線端末８及びＡＰ５は、上記実施の形態３のＳ３０５～Ｓ３０８の動作と同様に、接続処理を行う。

これにより、無線端末８からの発呼信号がＡＰ５を介してサバイバルサーバ２へ到達する。そして、サバイバルサーバ２は、無線端末８からの発呼信号に基づき呼処理をする。

【０１８２】

（Ｓ５０８）

ＡＰ６の無線ＬＡＮ通信部３０２は、到達した設定信号のうちＡＰ６のＡＰ別識別子を含む設定信号に基づき、自身に「ＳＳＩＤ３」及び対応するスキャン方式を「パッシブ」と設定する。

ＡＰ６の無線ＬＡＮ通信部３０２は設定を終えると、無線ＬＡＮ切断信号（Deauthentication）のメッセージ、及び当該ＡＰ６に設定された「ＳＳＩＤ３」を含めた制御信号（ビーコン）を送出し、再帰処理を実施する。

【０１８３】

（Ｓ５０９）
無線端末９及びＡＰ６は、上記実施の形態３のＳ４０５の動作と同様に、接続処理を行う。
これにより、無線端末９からの発呼信号がＡＰ６を介してサバイバルサーバ３へ到達する。そして、サバイバルサーバ３は、無線端末９からの発呼信号に基づき呼処理をする。
【０１８４】
尚、「ＳＳＩＤ１」は、本発明における第１のネットワーク識別子に相当し、「ＳＳＩＤ２」及び「ＳＳＩＤ３」は、本発明における第２のネットワーク識別子に相当する。
【０１８５】
以上のように本実施の形態においては、ネットワーク管理装置２０は、サーバと当該ネットワーク管理装置２０との間の通信状態を検出し、この通信状態に応じてアクセスポイントのＳＳＩＤを設定し、端末はＳＳＩＤに応じて、本体サーバ１又はサバイバルサーバ２若しくは３と情報通信を行う。このため、上記実施の形態１と同様の効果を奏することができる。
【０１８６】
また、ネットワーク管理装置２０によりサーバの通信状態の監視を行い、ＡＰに対してＳＳＩＤの設定制御を行う。
このため、ＡＰの構成を簡素化することが可能となる。また、既存のネットワークシステムにおいても、当該ネットワーク管理装置２０を追加する構成とすることで、サーバ切り替えを行うことができるシステムを構築することが可能となる。
【０１８７】
尚、本実施の形態４は、通信状態に基づいてＡＰのＳＳＩＤを設定する形態について説明したが、本発明はこれに限るものではなく、上記実施の形態２で説明したサーバの負荷状態に基づいてＡＰのＳＳＩＤを設定しても良い。
また、通信障害及び高負荷状態の何れか一方、又は双方に基づいてＳＳＩＤを切り替えるようにしても良い。
つまり、ネットワーク管理装置２０の監視部４０４に対し障害認識、及び負荷認識の設定をすることで、監視部２０４は障害認識のみを行うか、負荷認識のみを行うか、それとも、障害認識、及び負荷認識を行うかを選択するようにしても良い。尚、この場合、監視部４０４による負荷監視は、上記実施の形態２の監視部１０４と同様の動作を行うことができる。
【０１８８】
実施の形態５．
上記実施の形態３では、拠点ごとにコントローラを設け、コントローラごとにＡＰを収容する構成について説明した。
上述したように、コントローラは複数のＡＰを収容することも可能である。また、拠点をまたいで複数のＡＰを収容することも可能である。
本実施の形態５では、１つのコントローラで複数のＡＰを収容する場合について説明する。
【０１８９】
まず、本実施の形態５における無線通信システムの構成について、上記実施の形態１及び３との相違点を中心に説明する。尚、上記実施の形態１及び３と同様の構成には同様の符号を付する。
【０１９０】
図２１は実施の形態５に係る無線ＩＰ電話システムの構成図である。
図２１に示すように、本実施の形態に係る無線ＩＰ電話システムは、１つのコントローラ１０が、拠点をまたいで複数のＡＰを収容する構成である。
尚、本体サーバ１、サバイバルサーバ２及び３、無線端末７～９の構成は、上記実施の形態１と同様である。また、ＡＰ４～６の構成は、上記実施の形態３と同様である。
【０１９１】

コントローラ１０は、拠点Ａに設置される。
コントローラ１０は、拠点ＡのＡＰ４、拠点ＢのＡＰ５、及び拠点ＣのＡＰ６を収容（接続）している。
また、コントローラ１０とそれぞれのＡＰは、ＡＰ収容専用のＬＡＮで接続されている。また、コントローラ１０とサーバとは、有線ＬＡＮにより接続されている。

【０１９２】
本実施の形態５におけるコントローラ１０の構成は、実施の形態３（図１１）で説明したコントローラと同様に、第一有線ＬＡＮ通信部２０１と、第二有線ＬＡＮ通信部２０２と、記憶部２０３と、監視部２０４と、ＡＰ制御部２０５とにより構成されている。

【０１９３】
本実施の形態５における記憶部２０３は、各ＡＰごとに、複数のプロファイルが記憶される。
記憶部２０３は、ＡＰごとの複数のプロファイルを参照できるように、ＡＰの名前やＩＰアドレスなどのＡＰ別識別子と、各ＡＰごとの複数のプロファイルを対にして記憶する。これにより、ＡＰ別識別子をキーに、ＡＰごとに複数のプロファイルを参照できる。

【０１９４】
コントローラ１０の記憶部２０３に記憶されるプロファイルデータは、上記実施の形態１においてＡＰ４～６の記憶部１０３に記憶されたプロファイルデータ（図３）と同様である。
具体的には、コントローラ１０の記憶部２０３は、ＡＰ４のＡＰ別識別子と、図３（ａ）のプロファイルを対にして記憶している。また、ＡＰ５のＡＰ別識別子と、図３（ｂ）のプロファイルを対にし、ＡＰ６のＡＰ別識別子と、図３（ｃ）のプロファイルを対にして記憶している。

【０１９５】
コントローラ１０の監視部２０４は、記憶部２０３が記憶するプロファイルに基づきサーバを監視する。
監視部２０４は、記憶部２０３のプロファイルを参照し、プロファイルの監視対象フラグに基づき、「監視対象フラグＯＮ」に設定されている監視対象を監視する。

【０１９６】
具体的には、監視部２０４は、図３（ａ）を参照し「監視対象フラグＯＮ」に設定されている「本体サーバ１のＩＰアドレス１」に基づいて監視する。
同様に、図３（ｂ）を参照し「監視対象フラグＯＮ」に設定されている「本体サーバ１のＩＰアドレス１」、及び「サバイバルサーバ２のＩＰアドレス２」に基づいて監視する。
同様に、図３（ｃ）を参照し「監視対象フラグＯＮ」に設定されている「本体サーバ１のＩＰアドレス１」、及び「サバイバルサーバ３のＩＰアドレス３」に基づいて監視する。

【０１９７】
次に、本体サーバ１とコントローラ１０との間に障害が生じた場合の動作を、上記実施の形態３との相違点を中心に説明する。

【０１９８】
監視部２０４は、サーバと当該コントローラ１０との間の通信状態を監視（検出）する。
監視部２０４による監視は、本体サーバ１とサバイバルサーバ２及びサバイバルサーバ３を接続するＬＡＮを通して監視する。つまり、ＡＰ収容専用のＬＡＮではないＬＡＮを通して監視する。
この通信状態を監視する手段は、実施の形態１と同様に、ＩＣＭＰ　ｐｉｎｇ、及びＳＩＰメッセージ等を用いる。

【０１９９】
監視部２０４は、接続要求し、サーバから接続応答を得ることができるとき、接続が成

功し、サーバとコントローラ１０との間の通信は正常であると認識する。
　また、監視部２０４は、接続要求し、サーバから接続応答を得ることができないと、接続が失敗し、サーバとネットワーク管理装置２０との間の通信に障害が生じていると認識する。
　監視部２０４は、サーバに接続が失敗し、障害と認識すると、記憶部２０３に記憶された複数のＡＰごとのプロファイルのうち、監視対象フラグがＯＮ、且つ、接続に成功するサーバが含まれるプロファイルのＳＳＩＤ、及び対応するスキャン方式をＡＰ制御部２０５に与える。
　尚、プロファイルのスキャン方式に何も記憶されていない場合は、スキャン方式を設定しない。
【０２００】
　具体的には、コントローラ１０と本体サーバ１との間の障害と認識され、コントローラ１０とサバイバルサーバ２及びサバイバルサーバ３の間が接続に成功する場合は、次のようになる。
　監視部２０４は、記憶部２０３に記憶されたプロファイルのうち、監視対象フラグがＯＮ、且つ、接続に成功するサバイバルサーバ２又は３が含まれるプロファイルを、最上段から最下段に向け参照する。
　これにより、監視部２０４は、ＡＰ５に対応するプロファイル（図３（ｂ））において、「ＳＳＩＤ２」及び対応するスキャン方式「アクティブ」を得る。
　次に、監視部２０４は、ＡＰ５に対応するプロファイル（図３（ｂ））と対に記憶されたＡＰ５のＡＰ別識別子を得る。
　この結果、監視部２０４は、ＡＰ５への設定情報として、ＡＰ５のＡＰ別識別子、「ＳＳＩＤ２」及び対応するスキャン方式「アクティブ」を、ＡＰ制御部２０５に与える。
【０２０１】
　同様に、監視部２０４は、記憶部２０３に記憶されたプロファイルのうち、監視対象フラグがＯＮ、且つ、接続に成功するサバイバルサーバ２又は３が含まれるプロファイルを、最上段から最下段に向け参照する。
　これにより、監視部２０４は、ＡＰ６に対応するプロファイル（図３（ｃ））において、「ＳＳＩＤ３」及び対応するスキャン方式「パッシブ」を得る。
　次に、監視部２０４は、ＡＰ６に対応するプロファイル（図３（ｃ））と対に記憶されたＡＰ６のＡＰ別識別子を得る。
　この結果、監視部２０４は、ＡＰ６への設定情報として、ＡＰ６のＡＰ別識別子、「ＳＳＩＤ３」及び対応するスキャン方式「パッシブ」を、ＡＰ制御部２０５に与える。
【０２０２】
　続いて、コントローラ１０のＡＰ制御部２０５は、与えられた設定情報に基づいて設定制御をして、ＡＰ５及び６の設定をする。
　このとき、ＡＰ制御部２０５は、ＡＰ５のＡＰ別識別子、「ＳＳＩＤ２」及び対応するスキャン方式「アクティブ」の設定情報を含む設定信号を、第二有線ＬＡＮ通信部２０２を介して、ＡＰ収容専用のＬＡＮに送出する。
　さらに、ＡＰ制御部４０５は、ＡＰ６のＡＰ別識別子、「ＳＳＩＤ３」及び対応するスキャン方式「パッシブ」の設定情報を含む設定信号を、第二有線ＬＡＮ通信部２０２を介して、ＡＰ収容専用のＬＡＮに送出する。
【０２０３】
　こうすることでＡＰ５及びＡＰ６に設定信号が到達する。
　ＡＰ５の無線ＬＡＮ通信部３０２は、到達した設定信号のうちＡＰ５のＡＰ別識別子を含む設定信号に基づき、自身に「ＳＳＩＤ２」及び対応するスキャン方式を「アクティブ」と設定する。
　ＡＰ５の無線ＬＡＮ通信部３０２は設定を終えると、無線ＬＡＮに切断信号（Deauthentication）のメッセージを送出し、再帰処理を実施する。
　そして、無線端末８及びＡＰ５は、上記実施の形態３のＳ３０５～Ｓ３０８の動作と同

様に、接続処理を行う。
　これにより、無線端末８からの発呼信号がＡＰ５を介してサバイバルサーバ２へ到達する。そして、サバイバルサーバ２は、無線端末８からの発呼信号に基づき呼処理をする。
【０２０４】
　また、ＡＰ６の無線ＬＡＮ通信部３０２は、到達した設定信号のうちＡＰ６のＡＰ別識別子を含む設定信号に基づき、自身に「ＳＳＩＤ３」及び対応するスキャン方式を「パッシブ」と設定する。
　ＡＰ６の無線ＬＡＮ通信部３０２は設定を終えると、無線ＬＡＮ切断信号（Deauthentication）のメッセージ、及び当該ＡＰ６に設定された「ＳＳＩＤ３」を含めた制御信号（ビーコン）を送出し、再帰処理を実施する。
　そして、無線端末９及びＡＰ６は、上記実施の形態３のＳ４０５の動作と同様に、接続処理を行う。
　これにより、無線端末９からの発呼信号がＡＰ６を介してサバイバルサーバ３へ到達する。そして、サバイバルサーバ３は、無線端末９からの発呼信号に基づき呼処理をする。
【０２０５】
　以上のように本実施の形態においては、サーバの通信状態に応じて複数のＡＰのネットワーク識別子を、それぞれ設定する。このため、１つのコントローラ１０で複数のＡＰを収容している場合でも、各ＡＰに対してＳＳＩＤ及び対応するスキャン方式を設定できるようになる。
【０２０６】
実施の形態６．
　上記実施の形態３では、コントローラがＡＰに対する設定制御をすることで、ＡＰのネットワーク識別子（ＳＳＩＤ）を設定した。
　本実施の形態６では、ＡＰの設定制御に加え、ＡＰに対するアクセス制御及びトラヒック制御の設定を行う形態について説明する。
【０２０７】
　尚、本実施の形態６における無線通信システムの構成は、上記実施の形態３と同様であり、同様の構成には同様の符号を付する。
【０２０８】
　本実施の形態６に係るコントローラは、サーバと当該コントローラとの間の通信状態に応じて、ＡＰに対するアクセス制御及びトラヒック制御の少なくとも一方を行う。
【０２０９】
　ここで、コントローラがＡＰに対して行う制御は、上述したＡＰに対する設定制御に加え、ＡＰから流入するトラヒックに対するアクセス制御（ＦＷ（Firewall）、ＰＦ（Packet Filtering）など）がある。
　また、ＡＰから流入するトラヒックに対するトラヒック制御（ＱｏＳ（Quality of Service）など）がある。
　また、バックボーンから流入するトラヒックに対するアクセス制御がある。
　また、バックボーンから流入するトラヒックに対するトラヒック制御がある。
　尚、バックボーンとは、コントローラ１０の場合は本体サーバ１が接続する拠点ＡのＬＡＮである。
【０２１０】
　例えば、コントローラの記憶部２０３で記憶するプロファイルとともに、上述した制御に関する情報を対にして記憶する。これにより、ＡＰへのＳＳＩＤの設定をするとともに、コントローラの制御の設定も行えるようになる。
【０２１１】
　図２２は実施の形態６に係るコントローラの記憶部に記憶されたプロファイルデータを示す図である。
　具体的には、図２２に示すように、例えばコントローラ１１の記憶部２０３に記憶されるプロファイル（図３（ｂ）の内容）に加え、上から２番目のプロファイル「プロファイ

ル名２」に、「バックボーンから流入するトラヒックに対するアクセス制御」及び「バックボーンから流入するトラヒックに対するトラヒック制御」に関する設定情報を対にして記憶しておく。

【０２１２】

こうすることで、コントローラ１１は、上記実施の形態３と同様の動作により、図２２の最上段のプロファイルに基づいて、ＡＰ５に「ＳＳＩＤ１」を設定する。

そして、監視動作によって障害を認識すると、ＡＰ５に「ＳＳＩＤ２」及び対応するスキャン方式「アクティブ」をＡＰ５に設定する。

また、この設定とともに、「バックボーンから流入するトラヒックに対するアクセス制御」、及び「バックボーンから流入するトラヒックに対するトラヒック制御」に関する設定情報を読み込み、コントローラ１１自身に設定する。

以降、コントローラ１１は、ＡＰ５に対し、バックボーンから流入するトラヒックに対するアクセス制御、及びバックボーンから流入するトラヒックに対するトラヒック制御を行う。

【０２１３】

以上のように本実施の形態においては、上記実施の形態３の効果に加え、コントローラとサーバとの間の通信状態に応じて、アクセス制御及びトラヒック制御を行うことができる。

【０２１４】

尚、本実施の形態６においても、上記実施の形態２で説明したサーバの負荷状態に基づいてプロファイルを選択してＳＳＩＤの設定、アクセス制御及びトラヒック制御を行っても良い。また、通信障害及び高負荷状態の何れか一方、又は双方に基づいてプロファイルを選択するようにしても良い。

【０２１５】

尚、本実施の形態６では、コントローラによりアクセス制御及びトラヒック制御を行う場合を説明したが、本発明はこれに限るものではない。

例えば上記実施の形態４で説明したネットワーク管理装置２０を備える構成において、ネットワーク管理装置２０の記憶部４０３に、プロファイルと対にしたアクセス制御及びトラヒック制御の情報を保持し、選択したプロファイルに応じて、ＡＰに対してアクセス制御及びトラヒック制御の設定をする。これにより、ＡＰにアクセス制御及びトラヒック制御をさせるようにしても良い。

【０２１６】

実施の形態７.

上記実施の形態１～６では、端末がＡＰを補足する際に、ＡＰから送出する制御信号（ビーコン）は、１つのＳＳＩＤを含めた一種類の制御信号（ビーコン）を用いる場合を説明した。

本実施の形態７では、サーバの通信状態に応じて、ＡＰのＳＳＩＤを複数設定し、設定した複数のＳＳＩＤごとに、複数種類の制御信号（ビーコン）を送出する形態について説明する。

【０２１７】

尚、本実施の形態７における無線通信システムの構成は、上記実施の形態１と同様であり、同様の構成には同様の符号を付する。

【０２１８】

本実施の形態７におけるＡＰは、複数のネットワーク識別子の制御信号（ビーコン）を送出できるものである。例えば、２つのネットワーク識別子（ＳＳＩＤ）を１つのＡＰに設定し、第１のＳＳＩＤと第２のＳＳＩＤとを同時に利用し、この第１のＳＳＩＤを含めた制御信号（ビーコン）と、第２のＳＳＩＤを含めた制御信号（ビーコン）とを送出する。

【０２１９】

図２３は実施の形態７に係るＡＰの記憶部に記憶されたプロファイルデータを示す図で

ある。
　具体的には、図２３に示すように、例えば、ＡＰ５の記憶部１０３で記憶するプロファイルのうち、「プロファイル名２」について、「ＳＳＩＤ２」及び「ＳＳＩＤ３」を設定する。
【０２２０】
　ＡＰ５は、図２３のプロファイルに基づいて本体サーバ１とサバイバルサーバ２を監視する。ここでは、本体サーバ１との間で障害を認識し、サバイバルサーバ２との間で接続に成功したとする。
【０２２１】
　この場合、ＡＰ５は、図２３に示すプロファイルのうち、監視対象フラグがＯＮ、且つ、接続に成功するサーバが含まれるプロファイルのＳＳＩＤ、及び対応するスキャン方式を自身に設定する。
　尚、スキャン方式に何も設定されていない場合は、上述した通常のスキャンに対応する。
【０２２２】
　具体的には、「ＳＳＩＤ２」及び対応するスキャン方式を「パッシブ」と設定し、「ＳＳＩＤ３」及び対応するスキャン方式を「パッシブ」と設定する。
　これにより、ＡＰ５は、「ＳＳＩＤ２」と「ＳＳＩＤ３」の制御信号（ビーコン）を送出できるようになる。つまり、ＡＰ５は、「ＳＳＩＤ２」を含めた制御信号（ビーコン）と「ＳＳＩＤ３」を含めた制御信号（ビーコン）送出する。
【０２２３】
　尚、例えば図２３において、「ＳＳＩＤ３」の対応するスキャン方式が「アクティブ」の場合であっても同様に適用できる。
　この場合、「ＳＳＩＤ２」及び対応するスキャン方式を「パッシブ」と設定し、「ＳＳＩＤ３」及び対応するスキャン方式を「アクティブ」と設定する。
　これにより、ＡＰ５は、「ＳＳＩＤ２」を含めた制御信号（ビーコン）を送出する。そして、端末から「ＳＳＩＤ３」に設定されているＡＰをスキャンするための接続要求信号（Probe Request）を受けたときは、当該ＡＰ５に設定されている「ＳＳＩＤ３」を含めた制御信号（ビーコン）を送出する。
【０２２４】
　以上のように本実施の形態においては、ＡＰのＳＳＩＤを複数設定し、設定した複数のＳＳＩＤごとに、複数種類の制御信号（ビーコン）を送出する。
　このため、複数種類の制御信号（ビーコン）を送出可能なＡＰにおいて、通信状態に応じて、複数のＳＳＩＤを設定することが可能となる。
【０２２５】
　尚、本実施の形態７では、上記実施の形態１の構成の場合について説明したが、本発明はこれに限るものではなく、上述した実施の形態２～６の何れの構成においても、同様の動作を行うことができる。
【０２２６】
　尚、本実施の形態７においても、上記実施の形態２で説明したサーバの負荷状態に基づいてプロファイルを選択してＳＳＩＤ及びスキャン方式の設定を行っても良い。また、通信障害及び高負荷状態の何れか一方、又は双方に基づいてプロファイルを選択するようにしても良い。
【０２２７】
実施の形態８．
　本実施形態８では、ＡＰに設定したネットワーク識別子（ＳＳＩＤ）に応じて、端末とＡＰとの間の無線通信における暗号化や認証などに関するセキュリティの設定又は変更を行う形態について説明する。
【０２２８】
　尚、本実施の形態８における無線通信システムの構成は、上記実施の形態１と同様であ

り、同様の構成には同様の符号を付する。

【０２２９】

図２４は実施の形態８に係る記憶部に記憶されたプロファイルデータを示す図である。

図２４に示すように、ＡＰの記憶部１０３で記憶するプロファイルにおいて、各ＳＳＩＤごとに対応するセキュリティの設定情報を含めておく。

そして、上記実施の形態１と同様に、通信状態に応じてＳＳＩＤを設定する際、設定するＳＳＩＤに対応するセキュリティの設定又は変更を行う。

ここで暗号化の種類としては、例えば、ＷＥＰ（Wired Equivalent Privacy）、ＷＰＡ（Wi-Fi Protected Access）のＴＫＩＰ（Temporal Key Integrity Protocol）及びＷＰＡ２（Wi-Fi Protected Access 2）のＡＥＳ（Advanced Encryption Standard）などから適宜に選択してプロファイルに設定しておく。

また、認証の種類としては、ＭＡＣアドレス（Media Access Control address）フィルタリング、ＩＥＥＥＥ８０２．１Ｘ、及びＰＳＫ（Pre-Shared Key）などから適宜に選択してプロファイルに設定しておく。ＭＡＣアドレスフィルタの設定には許可するＭＡＣアドレスの情報を含み、ＩＥＥＥＥ８０２．１Ｘの設定には利用するＲＡＤＩＵＳ（Remote Authentication Dial In User Service）サーバの情報を含み、ＰＳＫの設定には認証及び又は暗号化鍵生成に用いる情報を含んでいる。

【０２３０】

具体的には、図２４においては、「プロファイル名２」の「ＳＳＩＤ２」に対応する暗号化を「ＡＥＳ」及び認証を「ＰＳＫ」と記憶しておく。

この場合、ＡＰに「ＳＳＩＤ２」を設定すると共に、ＡＰと端末との間の無線通信について「ＡＥＳ」による暗号化通信と「ＰＳＫ」による認証を行う。

【０２３１】

以上のように本実施の形態においては、ＡＰに設定したネットワーク識別子（ＳＳＩＤ）に応じて、端末とＡＰとの間の無線通信におけるセキュリティの設定又は変更を行う。

このため、通信状態に応じて、端末とＡＰとの間の通信のセキュリティを設定することが可能となる。

【０２３２】

尚、本実施の形態８では、上記実施の形態１の構成の場合について説明したが、本発明はこれに限るものではなく、上述した実施の形態２～７の何れの構成においても、同様の動作を行うことができる。

【０２３３】

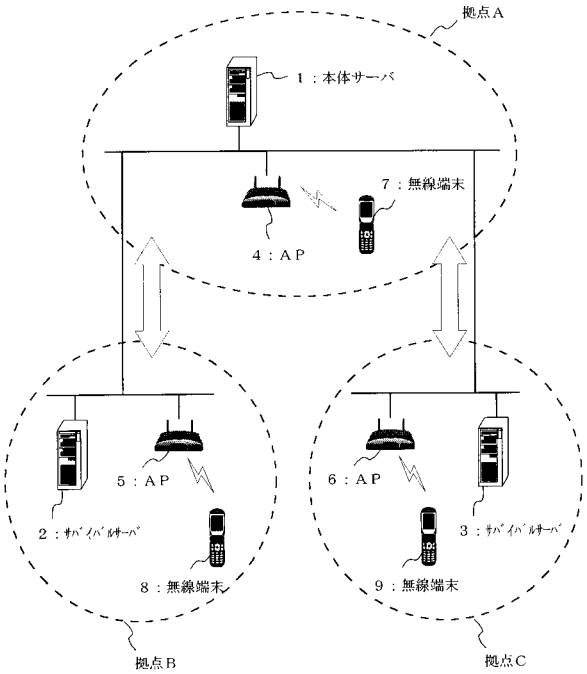
尚、本実施の形態８においても、上記実施の形態２で説明したサーバの負荷状態に基づいてプロファイルを選択してセキュリティの設定又は変更を行っても良い。また、通信障害及び高負荷状態の何れか一方、又は双方に基づいてプロファイルを選択するようにしても良い。

【符号の説明】

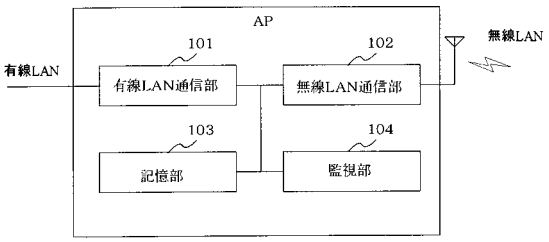
【０２３４】

１　本体サーバ、２　サバイバルサーバ、３　サバイバルサーバ、４　ＡＰ、５　ＡＰ、６　ＡＰ、７　無線端末、８　無線端末、９　無線端末、１０　コントローラ、１１　コントローラ、１２　コントローラ、２０　ネットワーク管理装置、１０１　有線ＬＡＮ通信部、１０２　無線ＬＡＮ通信部、１０３　記憶部、１０４　監視部、２０１　第一有線ＬＡＮ通信部、２０２　第二有線ＬＡＮ通信部、２０３　記憶部、２０４　監視部、２０５　ＡＰ制御部、３０１　有線ＬＡＮ通信部、３０２　無線ＬＡＮ通信部、４０２　有線ＬＡＮ通信部、４０３　記憶部、４０４　監視部、４０５　ＡＰ制御部、Ａ　拠点、Ｂ　拠点、Ｃ　拠点。

【図１】



【図２】



【図３】

(a)

AP4の記憶部

プロファイル名1	SSID1	本体サーバ1のIPアドレス1		監視対象フラグON
プロファイル名2	SSID2	サバイバルサーバ2のIPアドレス2		監視対象フラグOFF
プロファイル名3	SSID3	サバイバルサーバ3のIPアドレス3		監視対象フラグOFF

(b)

AP5の記憶部

プロファイル名1	SSID1	本体サーバ1のIPアドレス1		監視対象フラグON
プロファイル名2	SSID2	サバイバルサーバ2のIPアドレス2	アクティブ	監視対象フラグON
プロファイル名3	SSID3	サバイバルサーバ3のIPアドレス3		監視対象フラグOFF

(c)

AP6の記憶部

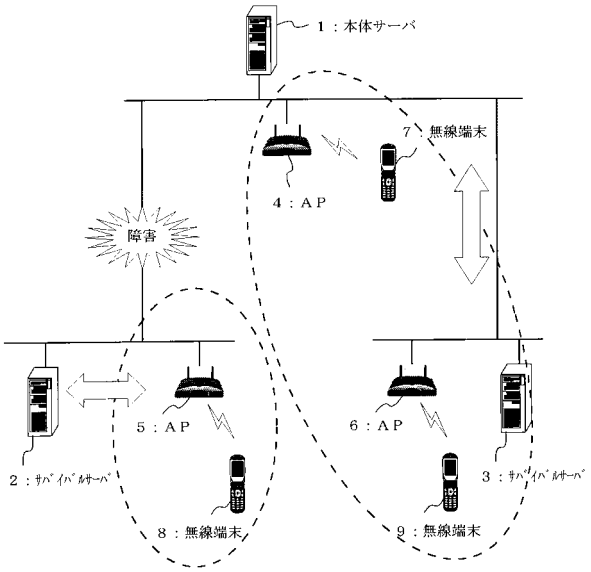
プロファイル名1	SSID1	本体サーバ1のIPアドレス1		監視対象フラグON
プロファイル名2	SSID2	サバイバルサーバ2のIPアドレス2		監視対象フラグOFF
プロファイル名3	SSID3	サバイバルサーバ3のIPアドレス3	パッシブ	監視対象フラグON

【図４】

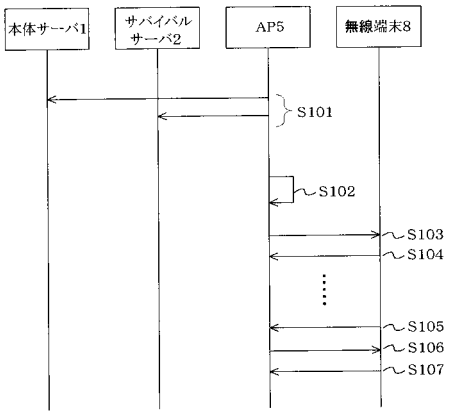
端末のプロファイル情報

プロファイル名1	SSID1	本体サーバ1のIPアドレス1
プロファイル名2	SSID2	サバイバルサーバ2のIPアドレス2
プロファイル名3	SSID3	サバイバルサーバ3のIPアドレス3

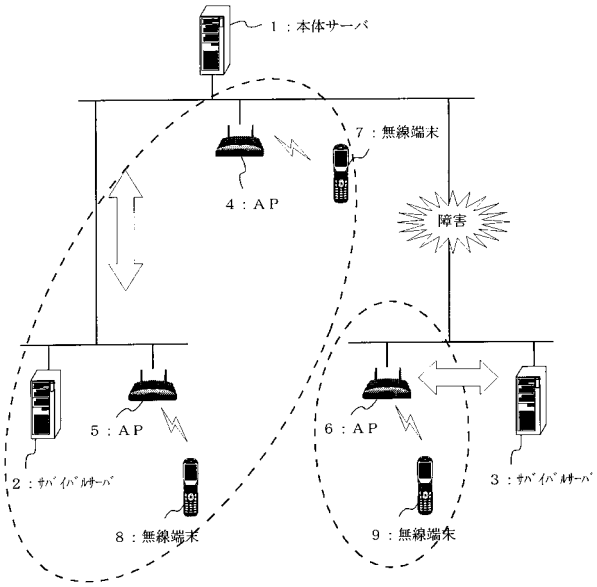
【図５】



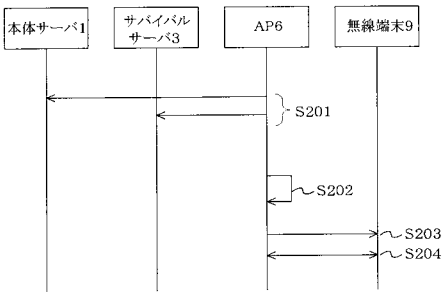
【図６】



【図７】



【図８】

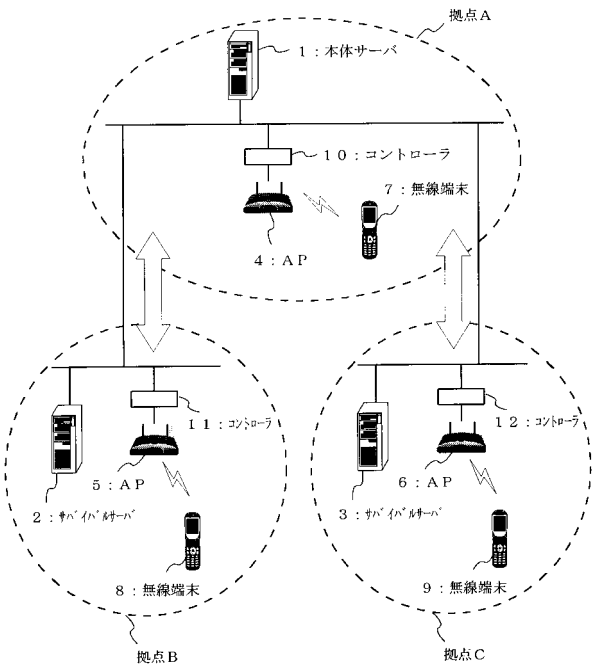


【図９】

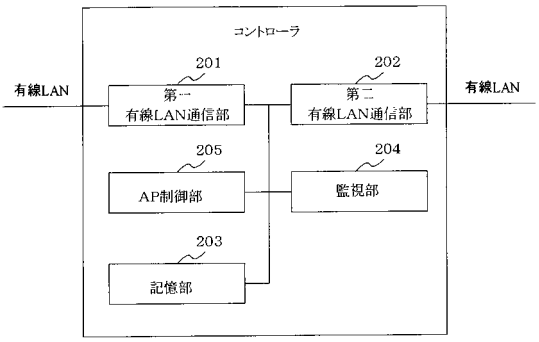
AP4の記憶部で記憶する負荷の閾値

本体サーバ1のIPアドレス1	CPU使用率 70%以上	メモリ使用率 70%以上	NWリソース使用率 85%以上
サバイバルサーバ2のIPアドレス2	CPU使用率 90%以上		
サバイバルサーバ3のIPアドレス3	CPU使用率 90%以上	メモリ使用率 85%以上	

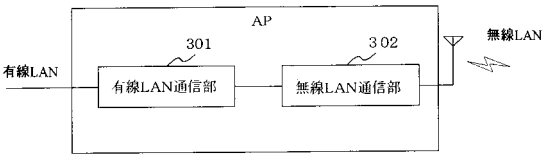
【図１０】



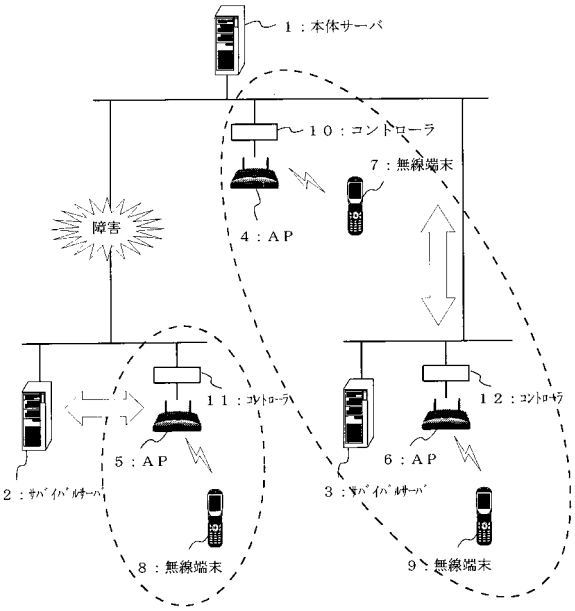
【図１１】



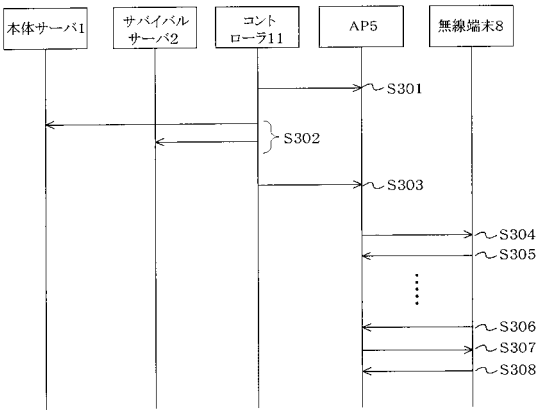
【図１２】



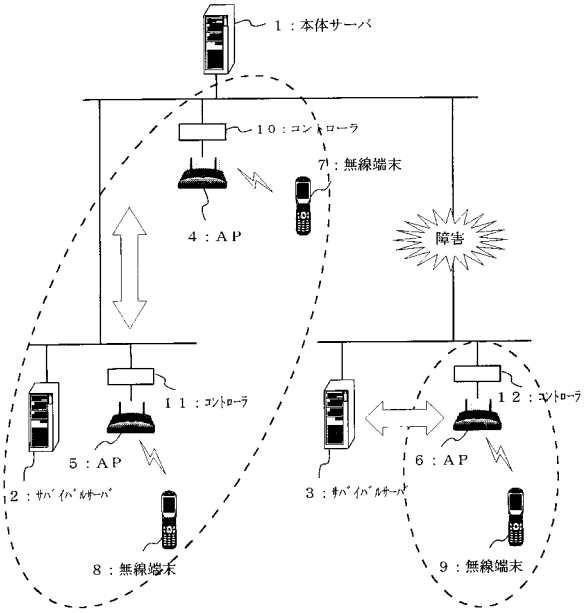
【図１３】



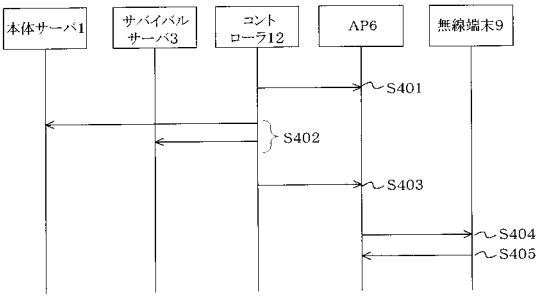
【図１４】



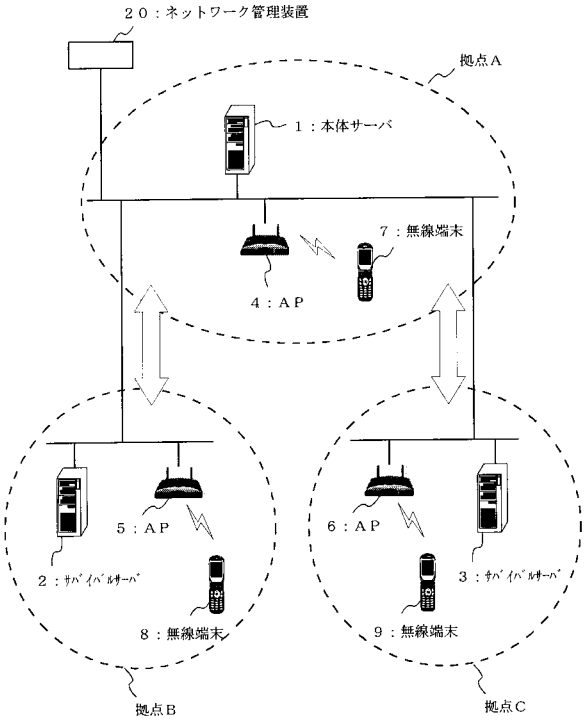
【図１５】



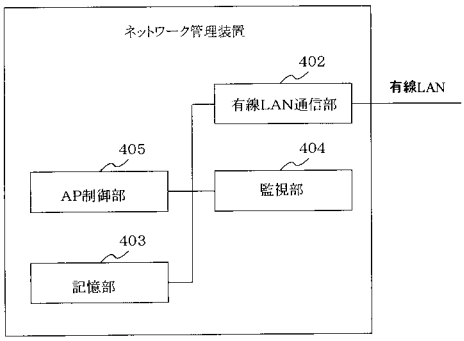
【図１６】



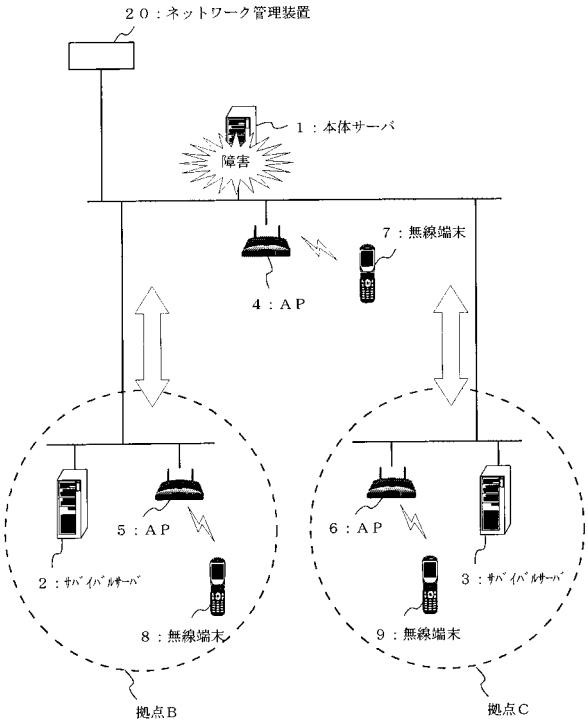
【図１７】



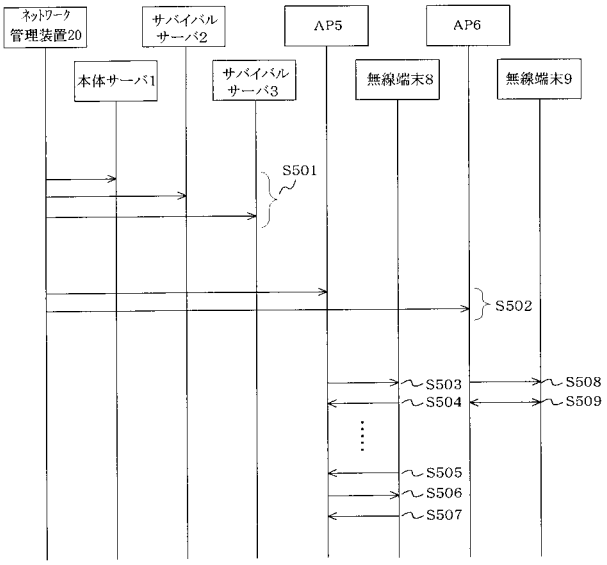
【図１８】



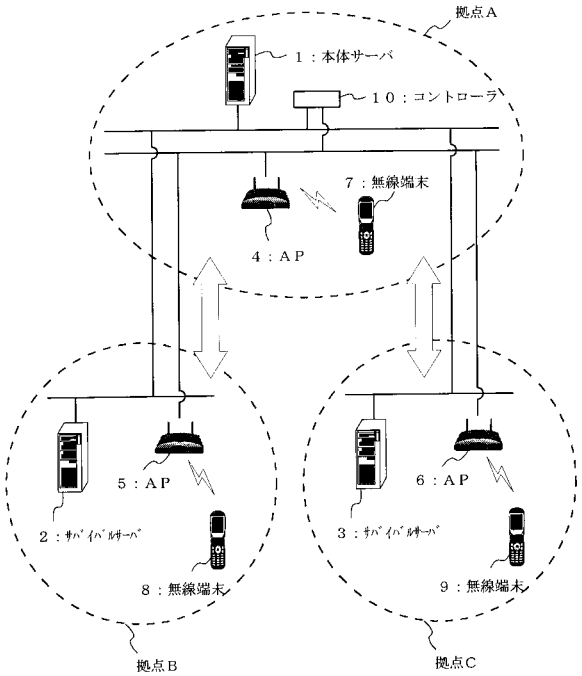
【図１９】



【図２０】



【図２１】



【図２２】

コントローラ11の記憶部

プロファイル名1	SSID1	本体サーバ1の IPアドレス1		監視対象フラグON	
プロファイル名2	SSID2	サバイバルサーバ2の IPアドレス2	アクティブ	監視対象フラグON	バックボーンから流入するトラヒックに対するアクセス制御の設定情報
					バックボーンから流入するトラヒックに対するトラヒック制御の設定情報
プロファイル名3	SSID3	サバイバルサーバ3の IPアドレス3		監視対象フラグOFF	

【図２３】

AP5の記憶部

プロファイル名1	SSID1	本体サーバ1の IPアドレス1		監視対象フラグON
プロファイル名2	SSID2	サバイバルサーバ2の IPアドレス2	パッシブ	監視対象フラグON
	SSID3	サバイバルサーバ2の IPアドレス2	パッシブ	
プロファイル名3	SSID4	サバイバルサーバ3の IPアドレス3		監視対象フラグOFF

【図２４】

記憶部のプロファイル

プロファイル名1	SSID1	本体サーバ1の IPアドレス1			監視対象フラグON
プロファイル名2	SSID2	サバイバルサーバ2の IPアドレス2	アクティブ	AES PSK	監視対象フラグON
プロファイル名3	SSID3	サバイバルサーバ3の IPアドレス3			監視対象フラグOFF

フロントページの続き

(72)発明者　斎藤　牧人
東京都港区西新橋三丁目１６番１１号　沖電気工業株式会社内
(72)発明者　吉田　敏之
東京都港区西新橋三丁目１６番１１号　沖電気工業株式会社内

Ｆターム(参考) 5K067 AA21 BB21 CC08 EE02 EE10 EE16
5K201 AA02 CB03 CD09 DA01 EA05 EB07 EC08 ED06 FA08