

【公報種別】特許法第 17 条の 2 の規定による補正の掲載

【部門区分】第 7 部門第 3 区分

【発行日】平成 17 年 3 月 17 日 (2005.3.17)

【公開番号】特開 2003-188885 (P2003-188885A)

【公開日】平成 15 年 7 月 4 日 (2003.7.4)

【出願番号】特願 2001-385869 (P2001-385869)

【国際特許分類第 7 版】

H 0 4 L 12/28

G 0 6 F 13/00

G 0 6 F 15/00

【F I】

H 0 4 L 12/28 3 0 0 Z

G 0 6 F 13/00 5 1 0 A

G 0 6 F 15/00 3 3 0 C

【手続補正書】

【提出日】平成 16 年 4 月 16 日 (2004.4.16)

【手続補正 1】

【補正対象書類名】明細書

【補正対象項目名】発明の名称

【補正方法】変更

【補正の内容】

【発明の名称】通信システム及びサーバ装置及びクライアント装置、ならびにそれらを制御するための方法及びそれらを実施するためのプログラム

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

通信システムにおいて、

クライアント端末が第 1 のアクセスポイントを介してネットワークと接続することが許可されている場合に、上記クライアント端末と上記第 1 のアクセスポイント間の通信で使用される暗号化キーを生成する生成手段と、

上記生成手段により生成された暗号化キーを上記第 1 のアクセスポイントに通知する通知手段とを有し、

上記通知手段は、上記クライアント端末が第 2 のアクセスポイントを介して上記ネットワークと接続する場合に、上記第 2 のアクセスポイントに対して上記第 1 のアクセスポイントに通知した暗号化キーと同じ暗号化キーを通知することを特徴とする通信システム。

【請求項 2】

サーバ装置において、

クライアント端末が第 1 のアクセスポイントを介してネットワークと接続することが許可されている場合に、上記クライアント端末と上記第 1 のアクセスポイント間の通信で使用される暗号化キーを生成する生成手段と、

上記生成手段により生成された暗号化キーを上記第 1 のアクセスポイントに通知する通知手段と、を有し、

上記通知手段は、上記クライアント端末が第 2 のアクセスポイントを介して上記ネットワークと接続する場合に、上記第 2 のアクセスポイントに対して上記第 1 のアクセスポイン

トに通知した暗号化キーと同じ暗号化キーを通知することを特徴とするサーバ装置。

【請求項 3】

上記クライアント端末が第 2 のアクセスポイントを介して上記ネットワークと接続を行う場合は、上記第 1 のアクセスポイントに上記暗号化キーを消去するよう指示する指示手段とを備えたことを特徴とする請求項 2 に記載のサーバ装置。

【請求項 4】

上記通知手段が上記第 2 のアクセスポイントに通知する暗号化キーは、上記生成手段により暗号化キーを生成した際に記憶した暗号化キー、もしくは、上記第 1 のアクセスポイントから受信した暗号化キーであることを特徴とする請求項 2 に記載のサーバ装置。

【請求項 5】

クライアント端末がアクセスポイントを介して通信する際に使用する暗号キーを上記アクセスポイントに通知するサーバ装置において、
上記クライアント端末が第 1 のアクセスポイントを介した通信から、第 2 のアクセスポイントを介した通信に移行したことを判定する判定手段と、
上記判定手段の判定に基づいて、上記第 1 のアクセスポイントに通知した暗号キーと同じ暗号キーを上記第 2 のアクセスポイントに通知する通知手段と、を有することを特徴とするサーバ装置。

【請求項 6】

サーバ装置において、
アクセスポイントを介して接続されるクライアント装置のネットワーク接続を許可する可否かを認証する認証手段と、
上記認証手段による認証結果に応じて、上記クライアント装置が接続するアクセスポイントに暗号化キーを通知する通知手段と、
上記認証手段に認証を求めてきたクライアント装置が、既に認証済みのクライアント装置か否かを判別する判別手段と、を有し、
上記通知手段は、上記判別手段による判別に応じて、上記クライアント装置が接続しているアクセスポイントに対して新たな暗号化キーを通知することを特徴とするサーバ装置。

【請求項 7】

上記通知手段は、認証を求めてきたクライアント装置が未認証であると上記判別手段により判別された場合は、上記クライアント装置が接続しているアクセスポイントに対して新たな暗号化キーを通知し、既に認証済みのクライアント装置であると判別された場合は、以前に認証した際にアクセスポイントに通知した暗号化キーと同じ暗号化キーを上記クライアント装置が現在接続しているアクセスポイントに対して通知することを特徴とする請求項 6 に記載のサーバ装置。

【請求項 8】

アクセスポイントを介してネットワークと接続するクライアント端末において、
第 1 のアクセスポイントとの通信に使用する暗号化キーを生成する生成手段と、
上記生成手段により生成した暗号化キーを使用して上記第 1 のアクセスポイントとの暗号化通信を行う通信手段と、を有し、
上記通信手段は、ネットワークに接続する際に接続するアクセスポイントを、上記第 1 のアクセスポイントから第 2 のアクセスポイントに切り換えた場合にも、上記第 1 のアクセスポイントとの暗号化通信に使用していた暗号化キーを使用することを特徴とするクライアント装置。

【請求項 9】

更に、上記ネットワークへの接続の許可通知を認証サーバから受信する受信手段を有し、
上記生成手段は、上記受信手段による上記許可通知の受信に応じて、暗号化キーを生成することを特徴とする請求項 8 に記載のクライアント装置。

【請求項 10】

通信システムの制御方法において、
クライアント端末が第 1 のアクセスポイントを介してネットワークと接続することが許可

されている場合に、上記クライアント端末と上記第１のアクセスポイント間の通信で使用する暗号化キーを生成するための生成工程と、
上記生成工程において生成された暗号化キーを上記第１のアクセスポイントに通知するための通知工程と、を有し、
上記通知工程は、上記クライアント端末が第２のアクセスポイントを介して上記ネットワークと接続する場合に、上記第２のアクセスポイントに対して上記第１のアクセスポイントに通知した暗号化キーと同じ暗号化キーを通知するための処理を行うことを特徴とする通信システムの制御方法。

【請求項１１】

サーバ装置の制御方法において、
クライアント端末が第１のアクセスポイントを介してネットワークと接続することが許可されている場合に、上記クライアント端末と上記第１のアクセスポイント間の通信で使用する暗号化キーを生成するための生成工程と、
上記生成工程において生成された暗号化キーを上記第１のアクセスポイントに通知するための通知工程と、を有し、
上記通知工程は、上記クライアント端末が第２のアクセスポイントを介して上記ネットワークと接続する場合に、上記第２のアクセスポイントに対して上記第１のアクセスポイントに通知した暗号化キーと同じ暗号化キーを通知するための処理を実行することを特徴とするサーバ装置の制御方法。

【請求項１２】

クライアント端末がアクセスポイントを介して通信する際に使用する暗号キーを上記アクセスポイントに通知するサーバ装置の制御方法において、
上記クライアント端末が第１のアクセスポイントを介した通信から、第２のアクセスポイントを介した通信に移行したことを判定するための判定工程と、
上記判定工程における判定に基づいて、上記第１のアクセスポイントに通知した暗号キーと同じ暗号キーを上記第２のアクセスポイントに通知するための通知工程とを有することを特徴とするサーバ装置の制御方法。

【請求項１３】

サーバ装置の制御方法において、
アクセスポイントを介して接続されるクライアント装置のネットワーク接続を許可する可否を認証するための認証工程と、
上記認証工程における認証結果に応じて、上記クライアント装置が接続するアクセスポイントに暗号化キーを通知するための通知工程と、
上記認証工程での認証を求めてきたクライアント装置が、既に認証済みのクライアント装置か否かを判別するための判別工程と、を有し、
上記通知工程は、上記判別工程における判別に応じて、上記クライアント装置が接続しているアクセスポイントに対して新たな暗号化キーを通知するための処理を行うことを特徴とするサーバ装置の制御方法。

【請求項１４】

アクセスポイントを介してネットワークと接続するクライアント端末の制御方法において、
第１のアクセスポイントとの通信に使用する暗号化キーを生成するための生成工程と、
上記生成工程において生成した暗号化キーを使用して上記第１のアクセスポイントとの暗号化通信を行うための通信工程と、を有し、
上記通信工程は、ネットワークに接続する際に接続するアクセスポイントを、上記第１のアクセスポイントから第２のアクセスポイントに切り換えた場合にも、上記第１のアクセスポイントとの暗号化通信に使用していた暗号化キーを使用するための処理を行うことを特徴とするクライアント装置の制御方法。

【請求項１５】

請求項１０から１４のいずれかに記載の制御方法を実行することを特徴とするプログラム

。

【手続補正 3】

【補正対象書類名】明細書

【補正対象項目名】0008

【補正方法】変更

【補正の内容】

【0008】

【課題を解決するための手段】

上記課題を解決するために本発明は、通信システムにおいて、クライアント端末が第1のアクセスポイントを介してネットワークと接続することが許可されている場合に、上記クライアント端末と上記第1のアクセスポイント間の通信で使用される暗号化キーを生成する生成手段と、上記生成手段により生成された暗号化キーを上記第1のアクセスポイントに通知する通知手段とを有し、上記通知手段は、上記クライアント端末が第2のアクセスポイントを介して上記ネットワークと接続する場合に、上記第2のアクセスポイントに対して上記第1のアクセスポイントに通知した暗号化キーと同じ暗号化キーを通知することを特徴とする通信システムを提供する。

【手続補正 4】

【補正対象書類名】明細書

【補正対象項目名】0009

【補正方法】変更

【補正の内容】

【0009】

また、サーバ装置において、クライアント端末が第1のアクセスポイントを介してネットワークと接続することが許可されている場合に、上記クライアント端末と上記第1のアクセスポイント間の通信で使用される暗号化キーを生成する生成手段と、上記生成手段により生成された暗号化キーを上記第1のアクセスポイントに通知する通知手段と、を有し、上記通知手段は、上記クライアント端末が第2のアクセスポイントを介して上記ネットワークと接続する場合に、上記第2のアクセスポイントに対して上記第1のアクセスポイントに通知した暗号化キーと同じ暗号化キーを通知することを特徴とするサーバ装置を提供する。

【手続補正 5】

【補正対象書類名】明細書

【補正対象項目名】0010

【補正方法】変更

【補正の内容】

【0010】

また、クライアント端末がアクセスポイントを介して通信する際に使用する暗号キーを上記アクセスポイントに通知するサーバ装置において、上記クライアント端末が第1のアクセスポイントを介した通信から、第2のアクセスポイントを介した通信に移行したことを判定する判定手段と、上記判定手段の判定に基づいて、上記第1のアクセスポイントに通知した暗号キーと同じ暗号キーを上記第2のアクセスポイントに通知する通知手段と、を有することを特徴とするサーバ装置を提供する。

【手続補正 6】

【補正対象書類名】明細書

【補正対象項目名】0011

【補正方法】変更

【補正の内容】

【0011】

また、サーバ装置において、アクセスポイントを介して接続されるクライアント装置のネットワーク接続を許可するか否かを認証する認証手段と、上記認証手段による認証結果に

応じて、上記クライアント装置が接続するアクセスポイントに暗号化キーを通知する通知手段と、上記認証手段に認証を求めてきたクライアント装置が、既に認証済みのクライアント装置か否かを判別する判別手段と、を有し、上記通知手段は、上記判別手段による判別に応じて、上記クライアント装置が接続しているアクセスポイントに対して新たな暗号化キーを通知することを特徴とするサーバ装置を提供する。

【手続補正 7】

【補正対象書類名】明細書

【補正対象項目名】0012

【補正方法】変更

【補正の内容】

【0012】

また、アクセスポイントを介してネットワークと接続するクライアント端末において、第1のアクセスポイントとの通信に使用する暗号化キーを生成する生成手段と、上記生成手段により生成した暗号化キーを使用して上記第1のアクセスポイントとの暗号化通信を行う通信手段と、を有し、上記通信手段は、ネットワークに接続する際に接続するアクセスポイントを、上記第1のアクセスポイントから第2のアクセスポイントに切り換えた場合にも、上記第1のアクセスポイントとの暗号化通信に使用していた暗号化キーを使用することを特徴とするクライアント装置を提供する。

【手続補正 8】

【補正対象書類名】明細書

【補正対象項目名】0013

【補正方法】変更

【補正の内容】

【0013】

また、通信システムの制御方法において、クライアント端末が第1のアクセスポイントを介してネットワークと接続することが許可されている場合に、上記クライアント端末と上記第1のアクセスポイント間の通信で使用される暗号化キーを生成するための生成工程と、上記生成工程において生成された暗号化キーを上記第1のアクセスポイントに通知するための通知工程と、を有し、上記通知工程は、上記クライアント端末が第2のアクセスポイントを介して上記ネットワークと接続する場合に、上記第2のアクセスポイントに対して上記第1のアクセスポイントに通知した暗号化キーと同じ暗号化キーを通知するための処理を行うことを特徴とする通信システムの制御方法を提供する。

【手続補正 9】

【補正対象書類名】明細書

【補正対象項目名】0014

【補正方法】変更

【補正の内容】

【0014】

また、サーバ装置の制御方法において、クライアント端末が第1のアクセスポイントを介してネットワークと接続することが許可されている場合に、上記クライアント端末と上記第1のアクセスポイント間の通信で使用される暗号化キーを生成するための生成工程と、上記生成工程において生成された暗号化キーを上記第1のアクセスポイントに通知するための通知工程と、を有し、上記通知工程は、上記クライアント端末が第2のアクセスポイントを介して上記ネットワークと接続する場合に、上記第2のアクセスポイントに対して上記第1のアクセスポイントに通知した暗号化キーと同じ暗号化キーを通知するための処理を実行することを特徴とするサーバ装置の制御方法を提供する。

【手続補正 10】

【補正対象書類名】明細書

【補正対象項目名】0015

【補正方法】変更

【補正の内容】

【0015】

また、クライアント端末がアクセスポイントを介して通信する際に使用する暗号キーを上記アクセスポイントに通知するサーバ装置の制御方法において、上記クライアント端末が第1のアクセスポイントを介した通信から、第2のアクセスポイントを介した通信に移行したことを判定するための判定工程と、上記判定工程における判定に基づいて、上記第1のアクセスポイントに通知した暗号キーと同じ暗号キーを上記第2のアクセスポイントに通知するための通知工程とを有することを特徴とするサーバ装置の制御方法を提供する。

【手続補正11】

【補正対象書類名】明細書

【補正対象項目名】0016

【補正方法】変更

【補正の内容】

【0016】

また、サーバ装置の制御方法において、アクセスポイントを介して接続されるクライアント装置のネットワーク接続を許可するか否かを認証するための認証工程と、上記認証工程における認証結果に応じて、上記クライアント装置が接続するアクセスポイントに暗号化キーを通知するための通知工程と、上記認証工程での認証を求めてきたクライアント装置が、既に認証済みのクライアント装置か否かを判別するための判別工程と、を有し、上記通知工程は、上記判別工程における判別に応じて、上記クライアント装置が接続しているアクセスポイントに対して新たな暗号化キーを通知するための処理を行うことを特徴とするサーバ装置の制御方法を提供する。

【手続補正12】

【補正対象書類名】明細書

【補正対象項目名】0017

【補正方法】変更

【補正の内容】

【0017】

また、アクセスポイントを介してネットワークと接続するクライアント端末の制御方法において、第1のアクセスポイントとの通信に使用する暗号化キーを生成するための生成工程と、上記生成工程において生成した暗号化キーを使用して上記第1のアクセスポイントとの暗号化通信を行うための通信工程と、を有し、上記通信工程は、ネットワークに接続する際に接続するアクセスポイントを、上記第1のアクセスポイントから第2のアクセスポイントに切り換えた場合にも、上記第1のアクセスポイントとの暗号化通信に使用していた暗号化キーを使用するための処理を行うことを特徴とするクライアント装置の制御方法を提供する。

【手続補正13】

【補正対象書類名】明細書

【補正対象項目名】0018

【補正方法】変更

【補正の内容】

【0018】

また、上記制御方法のいずれかを実行することを特徴とするプログラムを提供する。