請求の範囲

[請求項1] 第１ユーザが属する第１組織とは別の組織である他組織の認証システムであって、

前記第１ユーザのクライアント証明書用の登録トランザクションを受け付けるトランザクション受付部と、

前記第１ユーザの前記クライアント証明書用の登録トランザクションが受け付けられた場合に前記第１ユーザの前記クライアント証明書をクライアント証明書ブロックチェーンに登録するブロックチェーン管理部と、

前記第１ユーザが前記第１組織のユーザ端末から前記他組織のサービスにアクセスした場合に前記クライアント証明書ブロックチェーンの中の前記第１ユーザの前記クライアント証明書を用いて前記第１ユーザの認証を行う認証部と

を備える認証システム。

[請求項2] 前記認証システムは、証明書検証部を備え、

前記トランザクション受付部は、前記第１ユーザのログアウト時に、前記第１ユーザの前記クライアント証明書用の失効トランザクションを受け付け、

前記ブロックチェーン管理部は、前記第１ユーザの前記クライアント証明書用の前記失効トランザクションが受け付けられた場合に前記第１ユーザの前記クライアント証明書を失効リストブロックチェーンに登録し、

前記証明書検証部は、前記第１ユーザが前記第１組織の前記ユーザ端末から前記他組織のサービスにアクセスした場合に、前記第１ユーザの前記クライアント証明書が前記失効リストブロックチェーンに登録されているか判定し、

前記認証部は、前記第１ユーザの前記クライアント証明書が前記失効リストブロックチェーンに登録されていない場合に、前記第１ユー

ザの前記クライアント証明書を用いて前記第１ユーザの認証を行う
請求項１に記載の認証システム。

[請求項3] 前記認証システムは、証明書検証部を備え、

前記トランザクション受付部は、前記第１組織の認証局証明書用の登録トランザクションを受け付け、

前記ブロックチェーン管理部は、前記第１組織の前記認証局証明書用の前記登録トランザクションが受け付けられた場合に前記第１組織の前記認証局証明書を認証局証明書ブロックチェーンに登録し、

前記証明書検証部は、前記第１ユーザの前記クライアント証明書用の前記登録トランザクションが受け付けられた場合に前記認証局証明書ブロックチェーンの中の前記第１組織の前記認証局証明書を用いて前記第１ユーザの前記クライアント証明書を検証し、

前記ブロックチェーン管理部は、前記第１ユーザの前記クライアント証明書が正しい場合に前記第１ユーザの前記クライアント証明書を前記クライアント証明書ブロックチェーンに登録する
請求項１に記載の認証システム。

[請求項4] 前記認証部は、前記第１ユーザが前記第１組織の前記ユーザ端末から前記他組織のサービスにアクセスした場合にハローメッセージを第１組織システムに送信し、前記第１組織システムから前記ハローメッセージに対応する署名メッセージを受信し、前記第１ユーザの前記クライアント証明書を用いて前記署名メッセージを検証し、前記署名メッセージが正しい場合に前記第１ユーザが正当なユーザであると判定する
請求項３に記載の認証システム。

[請求項5] 前記第１組織システムは、前記第１組織の認証装置を備え、

前記第１組織の前記認証装置は、前記第１ユーザのクライアント秘密鍵を用いて前記ハローメッセージを暗号化し、暗号化されたハローメッセージを前記署名メッセージとして前記認証システムに送信する

代理証明部を備え、

前記認証部は、前記署名メッセージを受信し、前記第１ユーザの前記クライアント証明書から前記第１ユーザのクライアント公開鍵を取得し、前記第１ユーザの前記クライアント公開鍵を用いて前記署名メッセージを復号し、復号後の署名メッセージが前記ハローメッセージと一致する場合に前記署名メッセージが正しいと判定する

請求項４に記載の認証システム。

[請求項6] 前記第１組織システムは、前記第１組織の前記ユーザ端末を備え、

前記第１組織の前記ユーザ端末は、前記第１ユーザのクライアント秘密鍵を用いて前記ハローメッセージを暗号化し、暗号化されたハローメッセージを前記署名メッセージとして前記認証システムに送信する自己証明部を備え、

前記認証部は、前記署名メッセージを受信し、前記第１ユーザの前記クライアント証明書から前記第１ユーザのクライアント公開鍵を取得し、前記第１ユーザの前記クライアント公開鍵を用いて前記署名メッセージを復号し、復号後の署名メッセージが前記ハローメッセージと一致する場合に前記署名メッセージが正しいと判定する

請求項４に記載の認証システム。

[請求項7] 前記第１組織システムは、前記第１組織の認証局装置を備え、

前記第１組織の前記認証局装置は、前記第１組織の認証局秘密鍵を用いて署名を生成し、生成した署名を含めて前記第１ユーザの前記クライアント証明書を生成する証明書生成部を備え、

前記証明書検証部は、前記第１ユーザの前記クライアント証明書用の前記登録トランザクションが受け付けられた場合に前記第１組織の前記認証局証明書から前記第１組織の認証局公開鍵を取得し、前記第１組織の前記認証局公開鍵を用いて前記署名を検証し、前記署名が正しい場合に前記第１ユーザの前記クライアント証明書が正しいと判定する

請求項５または請求項６に記載の認証システム。

[請求項8] 前記認証部は、前記第１ユーザが前記第１組織の前記ユーザ端末から前記他組織のサービスにアクセスした場合にハローメッセージを第１組織システムに送信し、前記第１組織システムから前記ハローメッセージに対応する署名メッセージを受信し、前記第１ユーザの前記クライアント証明書を用いて前記署名メッセージを検証し、前記署名メッセージが正しい場合に前記第１ユーザが正当なユーザであると判定する

請求項１または請求項２に記載の認証システム。

[請求項9] 前記第１組織システムは、前記第１組織の認証装置を備え、

前記第１組織の認証装置は、前記第１ユーザのクライアント秘密鍵を用いて前記ハローメッセージを暗号化し、暗号化されたハローメッセージを前記署名メッセージとして前記認証システムに送信する代理証明部を備え、

前記認証部は、前記署名メッセージを受信し、前記第１ユーザの前記クライアント証明書から前記第１ユーザのクライアント公開鍵を取得し、前記第１ユーザの前記クライアント公開鍵を用いて前記署名メッセージを復号し、復号後の署名メッセージが前記ハローメッセージと一致する場合に前記署名メッセージが正しいと判定する

請求項８に記載の認証システム。

[請求項10] 前記第１組織システムは、前記第１組織の前記ユーザ端末を備え、

前記第１組織の前記ユーザ端末は、前記第１ユーザのクライアント秘密鍵を用いて前記ハローメッセージを暗号化し、暗号化されたハローメッセージを前記署名メッセージとして前記認証システムに送信する自己証明部を備え、

前記認証部は、前記署名メッセージを受信し、前記第１ユーザの前記クライアント証明書から前記第１ユーザのクライアント公開鍵を取得し、前記第１ユーザの前記クライアント公開鍵を用いて前記署名メ

ッセージを復号し、復号後の署名メッセージが前記ハローメッセージと一致する場合に前記署名メッセージが正しいと判定する
請求項８に記載の認証システム。

[請求項11] 前記第１組織システムは、前記第１組織の認証局装置を備え、
前記第１組織の認証局装置は、前記第１ユーザの前記クライアント秘密鍵を生成する秘密鍵生成部を備える
請求項９または請求項１０に記載の認証システム。

[請求項12] 第１ユーザが属する第１組織とは別の組織である他組織の認証システムのための認証プログラムであって、
前記第１ユーザのクライアント証明書用の登録トランザクションを受け付けるトランザクション受付処理と、
前記第１ユーザの前記クライアント証明書用の登録トランザクションが受け付けられた場合に前記第１ユーザの前記クライアント証明書をクライアント証明書ブロックチェーンに登録するブロックチェーン管理処理と、
前記第１ユーザが前記第１組織のユーザ端末から前記他組織のサービスにアクセスした場合に前記クライアント証明書ブロックチェーンの中の前記第１ユーザの前記クライアント証明書を用いて前記第１ユーザの認証を行う認証処理と
をコンピュータに実行させるための認証プログラム。