

(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2004-348308

(P2004-348308A)

(43) 公開日 平成16年12月9日(2004.12.9)

(51) Int.Cl.⁷

G 0 6 F 15/00

H 0 4 L 9/32

F I

G 0 6 F 15/00

H 0 4 L 9/00

3 3 O F

6 7 3 D

テーマコード (参考)

5 B 0 8 5

5 J 1 0 4

審査請求 未請求 請求項の数 9 O L (全 20 頁)

(21) 出願番号 特願2003-142838 (P2003-142838)

(22) 出願日 平成15年5月21日 (2003.5.21)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(74) 代理人 100075096

弁理士 作田 康夫

(72) 発明者 磯部 義明

神奈川県川崎市麻生区王禅寺1099番地

株式会社日立製作所システム開発研究所
内

(72) 発明者 比良田 真史

神奈川県川崎市麻生区王禅寺1099番地

株式会社日立製作所システム開発研究所
内

最終頁に続く

(54) 【発明の名称】 本人認証システム

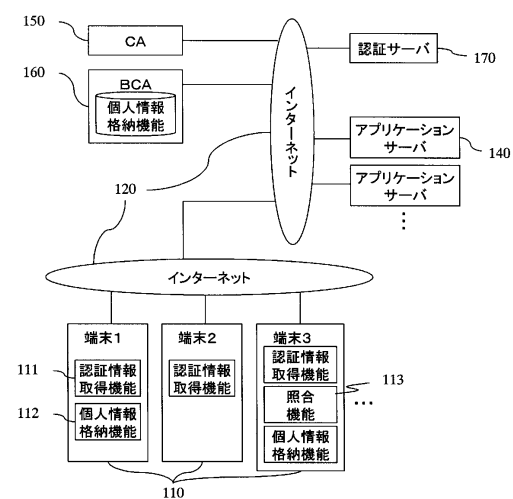
(57) 【要約】

【課題】さまざまなシステム構成のバイオメトリクスに対して、ユーザの希望やサーバのポリシーに応じた本人認証を提供する。

【解決手段】サーバとクライアントの双方が、機能として備える生体認証を含んだ本人認証方法を管理し、サーバとクライアントが、所有する本人認証方法を交換してサーバのアプリケーションのポリシーとユーザの希望に合致した本人認証方法を選択する。さらに、サーバが、クライアントでの生体照合を認める場合は、選択結果に追加する。また、プライバシー保護のため、クライアントからサーバへ送付する生体情報の利用範囲を限定する要求情報送付する。また、クライアントで生体照合を行う方法を選択した場合、照合結果と基準となったテンプレートをサーバに通知する。また、サーバが信用する本人認証機能を持つ他のサーバに生体照合を依頼する場合、当該他のサーバの情報を追加する。

【選択図】 図1

図1 (システム構成)



【特許請求の範囲】

【請求項 1】

情報サービスを提供するサーバと、前記情報サービスを享受するクライアントの間で行う本人認証システムであって、
前記サーバは、実施可能な生体認証方法を前記クライアントに通知し、
前記クライアントは実施可能な生体認証方法を選択して通知し、
前記サーバは、自サーバのセキュリティポリシーに合致する生体認証方法を、選択され通知された中から決定して、クライアントに通知し、
前記クライアントは、前記決定された生体認証方法に従う生体情報を前記サーバへ送付し、
前記サーバは、送付された前記生体情報により生体照合を実行して本人認証する。

10

【請求項 2】

情報サービスを提供するサーバと、前記情報サービスを享受するクライアントの間で行う本人認証システムであって、
前記サーバは、実施可能な生体認証方法を前記クライアントに通知し、
前記クライアントは実施可能な生体認証方法を選択して返信し、
前記サーバは、自サーバのセキュリティポリシーに合致する生体認証方法を、選択され通知された中から決定して、チャレンジコードと共にクライアントに通知し、
前記クライアントは、前記決定された生体認証方法に従う生体情報と、公開鍵暗号のユーザ秘密鍵にて前記サーバからの前記チャレンジコードを暗号化した結果とを前記サーバへ送付し、
前記サーバは、公開鍵暗号に基づくユーザ公開鍵により前記暗号化データを復号化して前記チャレンジコードを検証し、
当該生体情報により生体照合を実行して本人認証する。

20

【請求項 3】

請求項 2 に記載の本人認証システムであって、
前記クライアントは、前記サーバが実施可能な生体認証方法として、前記クライアントでの生体認証が含まれることが通知された場合に、前記クライアントが持つ生体認証方法を前記選択結果に追加して返信する。

【請求項 4】

請求項 2 に記載の本人認証システムであって、
前記クライアントは、前記生体照合において、前記クライアントのユーザに関わる生体情報の利用範囲を限定する要求情報を添付して前記サーバへ送付する。

30

【請求項 5】

請求項 2 に記載の本人認証システムであって、
前記クライアントで生体照合を行う方法を選択した場合、前記クライアントでの生体照合で本人と確認された場合に、公開鍵暗号におけるユーザ秘密鍵で前記サーバからのチャレンジコードを暗号化し、生体照合の結果とともに、照合の基準となった登録情報を前記サーバへ送付し、前記サーバでユーザの登録情報の有効性を確認する。

【請求項 6】

請求項 2 に記載の本人認証システムであって、
前記サーバは、前記サーバの生体認証方法を通知する情報に、認証サーバの生体認証方法の情報を追加する。

40

【請求項 7】

請求項 2 に記載の本人認証システムであって、
前記サーバのセキュリティポリシーの判定基準に、前記クライアントに関わる安全性保証レベルを用いる。

【請求項 8】

請求項 2 に記載の本人認証システムであって、
前記サーバで設定するセキュリティポリシーの判定基準として、生体照合方法における他

50

人受入率を用いる。

【請求項 9】

請求項 2 に記載の本人認証システムであって、
前記サーバで設定するセキュリティポリシーの判定基準として、本人認証のために入力された情報の質により評価した結果である安全性を用いる。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、非対面でサービスを提供するサーバ装置と、情報サービスを受けるクライアント装置の間の本人認証プロトコルに関する。

【0002】

【従来の技術】

ブロードバンドや携帯電話の普及により非対面の認証の安全性への要求が高まっている。この要求に基づき、従来、高セキュリティのエリアの入退室に利用されていた生体認証技術を応用した認証システムが提案されている。

【0003】

上記に関連する従来技術として、以下がある。

【0004】

従来の生体認証と連携した本人認証では、PC と接続するインターフェース (USB) を持った名刺大の筐体に静電容量方式の指紋入力機能と指紋登録機能と指紋認証機能と公開鍵暗号機能 (PKCS) に準拠した機能を持っており、あらかじめ筐体に登録した指紋情報に基づいた指紋照合の結果により筐体内の秘密鍵を活性化し、その活性化した秘密鍵を用いて PKI による本人認証や署名を行っている (例えば、非特許文献 1 に記載の装置を参照。)

【0005】

また、複数のバイオメトリクスの登録データを一元管理して照合する認証サーバを設置し、認証サーバでは、認証を提供する電子決裁や ERP アプリケーション毎に認証手段の組合せポリシーを AND や OR で設定する機能を持ち、端末の認証では、端末のソフトを介して認証に必要なテンプレートをダウンロードして端末にて本人認証する。また、端末ソフトでは、別途インストールした本人認証や署名を行う PKI の端末ソフトと連動する (例えば、非特許文献 2 に記載のシステム)。

【0006】

また、PKI と連携したバイオメトリクスの認証において、バイオメトリクスの登録データと PKI の証明書に関連付ける情報を持ち、バイオメトリクス登録データと PKI の証明書の情報について、ユーザの同一性の確認を行う上でバイオメトリクスの認証を行う本人認証システムが提案されている (例えば、特許文献 1 参照)。

【0007】

また、X. 509 の拡張領域にバイオメトリクステンプレートデータのフィールドを設け、バイオメトリクスデータを格納したの PKI 証明書の書式について提案しているものもある (非特許文献 3 参照。)

【0008】

【非特許文献 1】

「Bio-Keys Sony FIU-710」, PC Magazine, Vol. 20, No. 11, PP. 174 (2001/7/12)

【非特許文献 2】

Mandy Andress, 「Centralized security key - Authentication Suite 4.0 means managing multiple authentication schemes is easy and cheap」, InfoWorld, Aug. 13, 2001, Vol. 23, i33, p44

10

20

30

40

50

【特許文献1】

特開2000-215280号公報

【非特許文献3】

S. Santesson 他, 「Internet X.509 Public Key Infrastructure Qualified Certificates Profile」, RFC3039, Page11 (2001/1)

【0009】

【発明が解決しようとする課題】

従来技術では、次のような課題がある。

【0010】

非特許文献1の技術では、指紋照合の結果を受けて、サーバとPKIの本人認証を行うが、サーバ側では、クライアント側で実行した秘密鍵の持ち主の認証をどのように実行しているか不明である。このため、アプリケーションが要求するセキュリティポリシーを判断できない。また、秘密鍵の持ち主認証方法が、トークンに実装された単一のバイオメトリクスに限定されるため、マスマユーザーに展開した場合に、対応できない場合があるという生体認証特有の問題がある。

【0011】

非特許文献2の技術は、組織内ネットワークを対象にしたシステムであり、あらかじめ組織が導入したバイオメトリクスに限定して、ネットワークアプリケーションサーバにバイオメトリクス認証機能を提供する。このため、インターネットなどの公衆網を介した不特定多数のユーザーを対象とした場合のバイオメトリクス認証を想定した場合に、それぞれのユーザーの要求に応える本人認証を実現できない。また、ユーザーのプライバシー情報である生体情報をネットワークで転送する必要があるため、プライバシー保護に問題がある。また、認証ポリシーは、認証サービスを行うサーバに管理されており、サービスを提供するアプリケーションのポリシーを動的にコントロールできない。

【0012】

特許文献1の技術は、クライアントでのバイオメトリクスを認証するシステムであり、さまざまなバイオメトリクス認証モデルのシステムに対応していない。

【0013】

非特許文献3は、証明書にフィールドを定義したのみで、様々な特有な問題（経年変化や未対応など）のあるバイオメトリクスと連携した本人認証をどのように実行するか何も定義していない。

【0014】

【課題を解決するための手段】

本発明は、サーバとクライアントの双方が、それぞれが機能として所有する生体認証を含んだ本人認証方法を管理し、サーバとクライアントとの間のセッションにおいて、お互いの所有する本人認証方法を交換してサーバのアプリケーションのポリシーとユーザーの希望に合致した本人認証方法を選択する本人認証システムを提供する。

【0015】

また、サーバのポリシーによって、クライアントでの生体照合まで行う本人認証方法を認める場合は、この本人認証方法を選択に追加してもよい。

【0016】

また、プライバシーを保護するため、クライアントからサーバへ送付する情報に生体情報の利用範囲を限定する要求情報を添付してもよい。

【0017】

また、クライアントで生体照合を行う方法を選択した場合、照合の結果と照合の基準となった登録情報をサーバに通知してもよい。

【0018】

また、サーバが信用する本人認証サーバ機能を持つ他のサーバに生体認証を依頼する場合、生体認証方法として、上記他のサーバの情報を追加してもよい。

10

20

30

40

50

【0019】

【発明の実施の形態】

本発明の実施の形態を以下の順で説明する。

- (1) システム構成
- (2) 本人認証モデル
- (3) 生体認証プロトコル
- (4) クライアントの機能構成
- (5) サーバの機能構成
- (6) 認証サーバの機能構成
- (7) 各種情報の設定画面の例
- (1) システム構成

10

図1に本実施例全体のシステム構成を示す。

【0020】

本実施例のシステムは、望ましくは公開鍵基盤上に構築されており、各装置やサーバ装置はインターネットなどの通信網（以下、インターネットという）に接続され、相互にIP（インターネットプロトコル）で通信できるようになっている。

【0021】

各ユーザはそれぞれのユーザが所有する端末装置（以下、クライアントという）110より、インターネット120に接続し、各サーバ装置（以下、APサーバという）140へサービスを要求する。インターネット120へは、公開鍵を認証する認証局装置（以下、CA（Certificate Authority）という）150、生体認証の登録情報（以下、テンプレートという）を認証するバイオメトリック認証局装置（以下、BCA（Biometric Certificate Authority）という）160、生体照合をAPサーバ140の依頼で代行する認証サーバ装置（以下、認証サーバという）170などが接続されている。

20

【0022】

クライアント110が備える生体認証機能はそれぞれの方法により、次の3つの場合がある。

- ・ 認証情報取得機能111と個人情報格納機能112をクライアント110が持つ。
- ・ 認証情報取得機能111のみをクライアント110が持つ。
- ・ 認証情報取得機能111と照合機能113と個人情報格納機能112をクライアント110が持つ。

30

【0023】

各APサーバ140は、各ユーザに対してサービスを提供しており、それぞれのサービスに対する本人認証ポリシーを管理し、クライアント110から提示された情報に基づいて本人認証を実行する機能を備える。

【0024】

CA150は、ユーザやクライアント110、APサーバ140、BCA160、認証サーバ170の公開鍵を認証し、その証明書を発行する。

【0025】

BCA160は、ユーザの生体認証のためのテンプレートを認証し、その証明書を発行する。

40

【0026】

認証サーバ170は、APサーバ140に代わってさまざまな生体認証機能を用意し、APサーバ140へ生体認証結果を提供する。

【0027】

本実施例は、このように生体認証方法の多様性に対して、APサーバ140へサービスを要求するユーザが正当な権限を持つ人物か確認を行うため、公開鍵による電子認証と生体認証を連携させるプロトコルを提供する。

【0028】

50

図1に示す各装置の機能構成を図2に示す。各装置は、処理装置（CPU）210に接続された、情報入力装置240、表示装置220、記憶装置250、通信装置230から構成されている。処理手順（プログラム）は記憶装置250に記憶されており、処理装置210はプログラムを呼び出し、実行することにより、表示装置220を用いてユーザへ操作要求を行ったり、情報入力装置240からユーザからの入力を受け付けたり、通信装置230により外部装置と情報のやり取りを行ったり、各装置が備えるその他の機能を実現したりする。

【0029】

上記プログラムは、あらかじめ記憶装置250に格納されているか、可搬型記憶媒体または通信媒体（通信ネットワークまたは通信ネットワークを伝播する搬送波）を介して他の装置から記憶装置250に格納されてもよい。

（2）本人認証モデル

（2-1）PKIの本人認証モデル

公開鍵基盤を用いたクライアント110とAPサーバ140との間の本人認証モデルについて説明する。

【0030】

ユーザはあらかじめ、公開鍵と対となる秘密鍵（private key）を生成し、CA150に認証を受け、公開鍵証明書を発行して貰う。ユーザのクライアント110は、認証された公開鍵と対となる秘密鍵を保管している。

【0031】

本人認証では、クライアント110よりサービスを要求されたAPサーバ140が、乱数生成機能が生成したチャレンジコードをクライアント110へ送付し、クライアント110の署名機能が秘密鍵でチャレンジコードを暗号化してデジタル署名を生成し、APサーバ140へ返送する。APサーバ140は、証明書の公開鍵を使って復号したデータがチャレンジコードと一致するか検証することにより、サービスを要求した証明書の人物であるか確認する。

【0032】

この本人認証は、本人だけが秘密鍵を持っていることを認証の拠り所とした、所有物による本人認証となっている。

（2-2）クライアント照合型の生体認証モデル

生体認証の照合処理をクライアント110側で行う処理のモデルを図3に示す。このモデルは生体認証のテンプレートの管理方法により次の2つに分けられる。

- ・クライアント110側でテンプレートを管理するクライアント管理方法
- ・サーバ側（BCA160での管理も含む）で各ユーザのテンプレートを一括管理するサーバ管理方法。

【0033】

クライアント管理方法では、あらかじめBCA160に認証されたテンプレート15をクライアント110にインストールしておく。このテンプレート15と認証情報取得機能111が収集した生体情報とを照合機能113が照合し、本人認証結果をAPサーバ140へ送付する。

【0034】

サーバ管理方法では、同様にBCA160に認証されたテンプレート15を認証時にクライアント110へ送付し、このテンプレート15と認証情報取得機能111が収集した生体情報とを照合機能113が照合し、本人認証結果をAPサーバ140へ送付する。

（2-3）サーバ照合型の生体認証モデル

生体認証の照合処理を（アプリケーション）サーバ側で行う処理のモデルを図4に示す。このモデルは生体認証のテンプレートの管理方法により次の2つに分けられる。

- ・サーバ側（BCAでの管理も含む）で各ユーザのテンプレートを一括管理するサーバ管理方法。
- ・クライアント110側で各ユーザがテンプレートを管理するクライアント管理方法

サーバ管理方法では、クライアント 110 の認証情報取得機能 111 が収集された生体情報とユーザの ID を A P サーバ 140 へ送付し、A P サーバ 140 では、ユーザの ID により検索したテンプレート 15 と生体情報とを照合機能 113 が照合することで本人認証を行う。

【0035】

クライアント管理方法では、クライアント 110 の認証情報取得機能 111 が収集した生体情報とテンプレートとを A P サーバ 140 へ送付し、A P サーバ 140 は、送付されたテンプレート 15 と生体情報を照合することで本人認証を行う。

【0036】

ここで、テンプレート 15 は B C A 160 により、あらかじめ認証されていることとする 10

(2-4) 課題

(2-1) で示した P K I の本人認証と、(2-2) (2-3) で示した生体認証を単純に併用しただけでは、以下の問題がある。

- ・生体認証と P K I の本人認証と、それぞれ付与した ID の人物の同一性が保証されていない。

- ・(2-2) (2-3) で説明したように、さまざまな生体認証方法が提案されており、それぞれの生体認証方法を運用時に選択して本人認証するためのプラットフォーム（プロトコル）がない。

- ・クライアント 110 側で生体認証を完了するモデルでは、アプリケーションを提供する側で、どのような本人認証が行われて本人であると判定されたかを知るプラットフォーム（プロトコル）がない。 20

【0037】

これらの課題に対し、本実施例は、クライアント側とサーバ側の持つ機能について折衝し本人認証を行う生体認証機能を決定するプロトコルを明確にし、そのための折衝機能を備えるシステムを提供する。また、生体認証と P K I の本人認証で付与された ID の同一性については、たとえば、特許文献 1 に開示されている B C A によるデジタル署名により保証する。

(3) クライアント機能構成

図 5 にクライアント 110 の機能構成を示す。

30

【0038】

クライアント 110 は、通信機能 201、暗号機能 202、証明書や秘密鍵の管理機能 203、認証方法交渉機能 204、認証方法設定機能 205、認証方法管理機能 206、クライアント 110 が持つ認証機能 2100、2200、2300、2400 などから構成されている。クライアント 110 が持つ認証機能として、次の 4 種類の場合がある。

- ・テンプレート格納機能 212 と照合機能 213 と認証情報取得機能 211 を持ち、クライアントで照合を行う認証機能 2100。

- ・テンプレート格納機能 222 と認証情報取得機能 221 を持ち、サーバで照合を行う認証機能 2200。

- ・認証情報取得機能 231 を持ち、サーバで照合を行う認証機能 2300。 40

- ・照合機能 243 と認証情報取得機能 241 を持ち、サーバから転送されたテンプレートを使ってクライアントで照合を行う認証機能 2400。

【0039】

クライアント 110 が、異なる認証機能を重複して所有したり、ある構成に関して欠落したりするので、本実施例はクライアント 110 の構成に関わらずにサーバクライアント間の本人認証を成立させるもので、サーバの状況によって、認証機能を選択する。

【0040】

図 6 にクライアント 110 のもつ認証機能の管理テーブルを示す。この管理テーブルは、各ベンダの各認証機能を一意に特定する ID と、認証モデルのタイプとで構成されている。認証モデルは、次の 4 つのタイプに分類される。

50

- ・タイプS：サーバ側でテンプレートを管理し、サーバで照合するタイプ
- ・タイプC：クライアントでテンプレートを管理し、クライアントで照合するタイプ
- ・タイプD：サーバ側でテンプレートを管理し、クライアントで照合するタイプ
- ・タイプA：クライアントでテンプレートを管理し、サーバで照合するタイプ

それぞれの認証機能がどのモデルで本人認証を行うか、で識別を行う。

【0041】

図7にクライアント110を利用するユーザによる、認証機能に関する設定項目を示す。認証機能に関する設定項目は、次の5つからなる。

- ・ユーザ情報：ユーザを一意に識別するIDやユーザの証明書情報（例えば、発行したCA名+シリアル番号）
- ・テンプレート情報：ユーザが所有するテンプレートとその数
- ・優先テンプレート：ユーザが最も照合に使いたいテンプレート
- ・プライバシーモード：生体情報について、秘匿通信を行うかどうかを指定
- ・利用範囲限定の宣言：アプリケーションに対して、生体情報の利用範囲を要求するアプリケーションを利用するための本人認証に限定する宣言をするかどうかを指定

上記、クライアント110の持つテンプレート情報の管理テーブルを図8に示す。テンプレート管理テーブルは、テンプレートを一意に識別するID（テンプレート発行機関BCAとそのシリアル番号）と、そのテンプレートの人物のユーザIDと、テンプレートを照合する認証機能を一意に特定するIDからなる。

（4）サーバ機能構成

図9にAPサーバ140の機能構成を示す。APサーバ140は、通信機能301、暗号機能302、証明書や秘密鍵などの管理機能303、認証方法交渉機能304、認証方法設定機能305、認証方法管理機能306、APサーバ140の持つ認証機能310、320、330、認証機能の結果を判定する機能307を持つ。APサーバ140で機能を持つ認証機能は、次の3種類がある。

- ・テンプレート管理機能312と照合機能313とを持ち、サーバで照合する第1の認証機能。
- ・テンプレート管理機能322のみを持ち、クライアント110で照合する第2の認証機能。
- ・照合機能330のみを持ち、クライアント110から送付されたテンプレートと生体情報をサーバで照合する第3の認証機能。

【0042】

クライアント110でテンプレートを管理して照合する場合は、APサーバ140では対応する認証機能を持つ必要はない。

【0043】

クライアント110と同様に、本実施例はそれぞれの機能構成に依存せずに、サーバークライアント間で本人認証を成立させることを特徴としており、クライアントの状況によって、認証機能を選択する。

【0044】

なお、認証サーバ170もAPサーバ140と同様の構成を備える。

【0045】

図10にAPサーバ140が持つ認証方法（アルゴリズム）の管理するためのテーブルを示す。この管理テーブルは、方法アルゴリズムを一意に識別するIDと、テンプレートの管理タイプとで構成される。テンプレートの管理タイプには、次の3つがある。

- ・タイプS：APサーバ140で管理するタイプ
- ・タイプC：クライアントで管理するタイプ
- ・タイプO：BCAなど他のサーバで管理するタイプ

図11にAPサーバ140の本人認証方法に関する安全レベルを設定するテーブルを示す。本テーブルは、アルゴリズムIDと照合タイプと照合アルゴリズムの安全レベルからなる。このテーブルにより、APサーバ140が提供するアプリケーションのポリシーに応

10

20

30

40

50

じて認証方法の安全レベルを選択できる。ここで、安全レベルとして、次の例がある。

- ・照合ソフトの識別性能（他人受入率など）によるレベル付け
- ・照合ソフトが実装されたクライアント 1 1 0 の安全性評価レベル（ISO 15408 の EAL など）
- ・照合ソフトの認証モデルによるレベル付け

これらを勘案して、各 A P サーバ 1 4 0 のポリシーによって、それぞれの照合ソフトの安全レベルを設定する。

【0046】

図 1 2 に A P サーバ 1 4 0 のポリシーを設定するテーブルを示す。このテーブルは次のような構成となっている。

- ・サービス ID： A P サーバ 1 4 0 の提供するサービスを識別するコード
- ・要求する認証モデル：このサービスが要求する認証モデル
- ・要求する安全レベル：このサービスが要求する安全性レベル（例えば、ISO 15408 の EAL など）
- ・要求する FAR：このサービスが要求する FAR 値
- ・有効性検証フラグ：このサービスにおける有効性検証の処理内容

また、上記に、

- ・入力された画像などの生体情報の質に関するレベル：画質レベルを考慮したポリシーを追加しても良い。

【0047】

このような A P サーバのセキュリティポリシーを満たすため、それぞれの生体認証アルゴリズムは次のような機能を持つ。

- （a）入力された画像の画質のノイズレベルを S / N 比として出力する機能。通常の利用した場合のノイズレベルと比較して、著しく変動がある入力画像を排除する効果がある。
- （b）連続して収集した画像の変動量を出力する機能。通常の場合の変動量と比較して、変動がない場合、写真などの偽造として入力画像を排除する効果がある。
- （c）入力された特徴の過不足を出力する機能。顔照合の場合、顔の構造が過不足なく入力されているか評価することで、照合確度を上げることが期待できる。

（5）認証プロトコル

本実施例の認証フローを図 1 3 に示す。

【0048】

まず、クライアント 1 1 0 からサービス要求 8 1 1 が、A P サーバ 1 4 0 へ送付される。

【0049】

本実施例のプロトコルを実装した A P サーバ 1 4 0 が、要求されたサービスが本人認証を必要とするサービスかどうか判定する（8 2 1）。本人認証が必要なサービスであれば、A P サーバ 1 4 0 が持つ認証方法のリストを含む本人認証要求 8 3 1 をクライアント 1 1 0 へ送付する。

【0050】

クライアント 1 1 0 では、上記認証方法のリストから、クライアント 1 1 0 が管理する認証情報取得機能で対応できる認証方法を選択する。さらに、クライアント 1 1 0 が管理する照合機能を選択されたリストに追加する（8 0 1）。もし、作成したリストのうち、最も優先的に照合に使いたいテンプレートを使った認証方法があれば、リストの最上位に並び替える。このようにして作成した本人認証スペック 8 1 2 を A P サーバ 1 4 0 へ返送する。

【0051】

A P サーバ 1 4 0 は、要求されたサービスに最も適した認証方法をポリシー管理テーブルにより決定する。安全性レベルおよび FAR を満たす認証方法が多数ある場合で、ユーザ希望の認証方法（リスト最上位の認証方法）があれば、ユーザ希望の認証方法を選択する（8 2 2）。クライアント 1 1 0 で付け足された認証方法の安全性レベルが不明の場合は方法、当該認証方法を開発したベンダやその性能を認証する B C A などの FAR の情報を

10

20

30

40

50

オンラインで入手し、安全性レベルを満たすかどうかを判定する。

【0052】

以上で決定された本人認証方法とアプリケーションで生成したチャレンジコードをクライアント110へ通知する。上記のポリシーに適合する認証方法がない場合は、セッションの終了を通知する(832)。

【0053】

クライアント110では、決定された認証方法に従って、認証情報を収集する(802)。

【0054】

クライアント110でテンプレートを管理・照合する認証方法の場合は、802で収集した
認証情報を照合する(803)。

【0055】

クライアント110で、チャレンジコードと802で収集した認証情報に対して、テンプレートのユーザの秘密鍵で署名を生成する(804)。

【0056】

収集した認証情報とユーザ署名813を、クライアント110からアプリケーションへ返送する。

【0057】

APサーバ140は、証明書の正当性、ユーザ署名813、テンプレートの正当性などを
署名検証処理により検証する(823)。

【0058】

さらに、APサーバ140では、証明書、テンプレートの有効性を認証局、BCAの情報により検証する(824)

APサーバ140でテンプレートを管理・照合する場合は、テンプレートと送付された認証情報を照合する(825)。

【0059】

照合の結果情報と823、824の検証結果より、FARを満たす照合スコアであったか、有効な情報で検証が行われたかを確認し、サービスを提供して良いか判定する(826)。

【0060】

APサーバ140からクライアント110へ認証結果を通知する。826で、サービスを提供してよいと判定すれば、サービスを提供する(833)。

【0061】

図14に、APサーバ140・クライアント110以外にテンプレートが管理されている場合を示す。図13とは、ステップ805が追加されていることと、ステップ824の代わりにステップ827が実行されるという点である。図13と同じ番号を付している他のステップは、重複しているため説明を省略する。

【0062】

ステップ802の後、クライアント110で照合する認証方法の場合で、クライアント110でテンプレートを管理していない場合は、テンプレートを管理するBCAなどへテンプレートを要求し、送付してもらう(805)。その後で、ステップ802で収集した認証情報を照合する(803)。

【0063】

ステップ823の後、クライアント110よりテンプレートが送付された場合、BCAが管理するテンプレートの有効性情報に基づき、有効性を検証する(824)

APサーバ140では、ステップ823の後、APサーバ140で照合する場合で、テンプレートがBCAなど他のサーバで管理している場合には、テンプレートをBCAへ要求して、送信してもらう(827)。その後、クライアント110から送付された認証情報の照合(825)に移る。

10

20

30

40

50

【0064】

A Pサーバ140からの本人認証を要求する通信データ831を図15に示す。この本人認証要求する通信データ831は、次のようなデータで構成されている。

【0065】

データ識別コード：この本人認証を要求する通信データを識別するコード

サービス要求情報：ユーザが要求したサービスのセッション情報

要求する本人認証モデル：A Pサーバ140が要求する本人認証モデルを指定する情報。

例えば、0：PKI認証だけを実行、1：クライアント110で生体照合を実行、2：A Pサーバ140で生体照合を実行、3：クライアント、A Pサーバ140のどちらかで生体照合を実行と指定

10

認証方法のリスト数：A Pサーバ140の持つ認証方法の数

認証方法のリスト：上記の認証方法のリスト。例えば、認証方法を一意に指定するIDとその照合モデルのフラグなどを列記

クライアント110からのクライアント110の持つ機能を反映した本人認証要求の返答データ812を図16に示す。この本人認証要求の返答データ812は、次のようなデータで構成されている。

【0066】

データ識別コード：この本人認証要求の返信データを識別するコード

サービス要求情報：ユーザが要求したサービスのセッション情報

認証方法のリスト数：A Pサーバ140の認証方法の中からクライアント110で生体を取得可能な認証方法に、クライアント照合する認証モデルをA Pサーバ140が許す場合のクライアント110で生体取得し照合できる認証方法を追加した数

20

認証方法のリスト：上記の認証方法のリスト。例えば、認証方法を一意に指定するIDとその照合モデルのフラグなどを列記

A Pサーバ140からの本人認証方法の決定通知データ832を図17に示す。この本人認証方法の決定通知データは、次のようなデータで構成されている。

【0067】

データ識別コード：この本人認証方法の決定通知データを識別するコード

サービス要求情報：ユーザが要求したサービスのセッション情報

決定した認証方法：本セッションで照合する認証方法。

30

【0068】

チャレンジコード：PKIによる本人認証のためのA Pサーバ140が発生した乱数。

【0069】

クライアント110からのユーザ署名と認証情報の通信データ813を図18に示す。この通信データは、次のようなデータで構成されている。

【0070】

データ識別コード：このクライアントか110らの通信データを識別するコード

サービス要求情報：ユーザが要求したサービスのセッション情報

決定した認証方法：本セッションで照合する認証方法。

【0071】

40

認証情報：認証情報は次の3つの場合がある。

【0072】

1) テンプレートをA Pサーバ140で管理して、A Pサーバ140で照合するモデルの場合、クライアント110で収集した生体情報

2) クライアント110で照合するモデルの場合、クライアント110で照合した照合結果とテンプレート

3) テンプレートをクライアント110で管理して、A Pサーバ140で照合するモデルの場合、クライアント110で収集した生体情報と、テンプレート

ユーザ署名：ユーザの秘密鍵でチャレンジコードを暗号化して生成した署名。

以上の通信データを構成するデータとチャレンジコードに対する署名を添付しても良い。

50

【0073】

A Pサーバ140からの本人認証結果の通知データ833を図19に示す。この結果通知データは、次のようなデータで構成される。

【0074】

データ識別コード：この本人認証結果の通知データを識別するコード

サービス要求情報：ユーザが要求したサービスのセッション情報

行った認証方法：本セッションで行った認証方法

結果：本セッションで行った認証結果。例えば、0：本人認証成功、1：PKIによる認証失敗、2：生体テンプレート失敗、3：生体照合失敗

A Pサーバ140の署名：以上の結果に対する、A Pサーバ140の秘密鍵による署名
(6) 認証サーバを介した場合の認証プロトコル

多数のユーザが生体認証方法を使用する場合、単一の生体認証では、対応できずにユーザの可用性を損なうおそれがある。このため、複数の認証方法をA Pサーバ140で用意することが望ましい。しかし、A Pサーバ140が様々な認証方法を持つと、構築コストがかかるため、様々な認証方法を用意する認証サーバに照合処理を委託してもよい。また、全ての照合処理を認証サーバへ委託すると処理時間がかかるので、部分的に認証サーバへ委託してもよい。以下、認証サーバへ生体照合を委託するプロトコルを示す。

【0075】

A Pサーバ140は、あらかじめ認証サーバとの間に信用関係を構築しておく必要がある。本実施例では、認証サーバの照合結果をA Pサーバ140が信用することを前提としている。

【0076】

A Pサーバ140は、予め、認証サーバの持つ認証方法に関する情報を入手しておき、認証サーバの持つ認証方法について、セキュリティポリシーを決定しておく。

【0077】

また、クライアント110からA Pサーバ140が信用関係を構築していない認証サーバを介した認証方法を提案されることも想定される。この場合は、提案された認証サーバが信用できるか、PKIの枠組みで検証を行ったうえ、認証サーバへ照合を委託することも考えられる。この場合、認証サーバとクライアント110が結託して、なりすましを試みることが想定されるので、信頼のおける組織から、(PKIの) 認証を受けた認証サーバであることが、信用の条件である。A Pサーバ140では、これらの信用に関するポリシーの設定をしておく必要がある。また、未知の認証サーバの持つ認証方法がアプリケーションの安全性ポリシーに合致するかを検証する必要がある。このため、他人を受け入れる確率FARの要件を満たしているか、信頼できる評価結果により、判断する。この仕組みは、本出願人による特願2002-50884号に開示する認証方法により可能である。

【0078】

図20に認証サーバに生体の照合を委託する場合の処理フローを示す。以下、図13に示す処理フローとの相違点である、

照合ステップ825を認証サーバに委託する点について説明する。また、本人認証要求831は、A Pサーバ140が持つ認証方法、および、認証サーバの持つ認証方法のリストを含む。

【0079】

ステップ824の後、認証サーバで照合するため、テンプレートと送付された認証情報を認証サーバへ送付する(952)。

【0080】

認証サーバでは、受信したテンプレートと認証情報を照合(941)し、結果をA Pサーバ140へ返送し(962)、ステップ826に進む。

【0081】

(7) 各種情報の設定画面の例
各種情報の設定画面の例を示す。

【0082】

図23にクライアント110における各ユーザの設定画面の例を示す。

【0083】

個人情報として、個人を特定する氏名や住所の他、PKIの公開鍵の証明書情報が表示される。複数の機関から、証明書の発行を受けるため、証明書ごとにこの設定画面を切り替えて表示できるようになっている。

【0084】

テンプレート情報として、切り替え表示された個人IDに対して発行されたテンプレートを全て表示できるようにしている。また、ユーザが希望するテンプレートの優先度の順に表示されており、テンプレートを指定した上で優先順位上昇、下降ボタンを押下することで、変更可能になっている。 10

【0085】

セキュリティ情報として、チェックボックスにより、秘匿通信および利用範囲限定宣言を指定できるようになっている。

【0086】

図24にAPサーバ140におけるアプリケーションのセキュリティポリシーの設定画面の例を示す。

【0087】

APサーバ140が持つアプリケーションごとに、クライアント110に要求する安全性レベル（EAL保証レベルなど）や認証に要求するFAR、認証モデル、テンプレートの有効性検証の必要性を設定できるようになっている。 20

【0088】

図25にAPサーバ140における認証方法のセキュリティポリシーの設定画面の例を示す。APサーバ140が許可する認証方法について、それぞれのFARや照合タイプ、安全性レベルをサーバ事業者のポリシーに応じて設定できるようになっている。

【0089】

上記各実施例の本人認証システムによれば、次のような顕著な効果を奏する。

【0090】

まず、APサーバ140と、サービスの提供を受けるクライアント110において、それぞれが持つ本人認証方法を管理し、サービス提供のセッションに先立ち、APサーバ140のポリシーとユーザの希望に沿った本人認証方法を選択できる。 30

【0091】

また、APサーバ140のポリシーが、クライアント110で生体照合を行う本人認証方法を認める場合は、選択肢に追加できる。

【0092】

また、プライバシーを保護するため、クライアント110からAPサーバ140へ送付する情報に、生体情報の利用範囲を上記サービス利用のための認証処理に限定する要求情報を添付できる。

【0093】

また、クライアントで生体照合を行う方法を選択した場合、照合の結果と照合の基準となったテンプレートをサーバに通知できる。 40

【0094】

また、サーバが信用する本人認証サーバ機能を持つ他のサーバに生体認証を依頼する場合、サーバの生体認証方法として、そのサーバの情報を追加できる。

【0095】

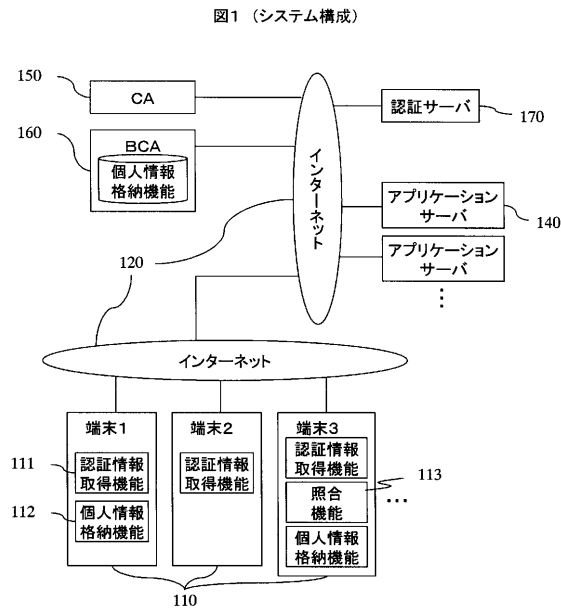
【発明の効果】

以上により、不特定多数の参加するネットワークにおける情報サービスの授受において、クライアントとサーバのそれぞれの機器構成に依らずに、サーバポリシーに応じた本人認証を実現できる。

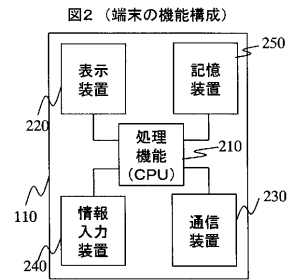
【図面の簡単な説明】

- 【図 1】 実施例におけるシステム全体の構成図である。
- 【図 2】 実施例におけるクライアント 110 の構成図である。
- 【図 3】 実施例における、クライアント側で生体照合を行う第 1 の生体認証モデルの説明図である。
- 【図 4】 実施例における、サーバ側で生体照合を行う第 2 の生体認証モデルの説明図である。
- 【図 5】 実施例におけるユーザのクライアント 110 の機能構成を示すブロック図である。
- 【図 6】 実施例におけるユーザクライアント 110 にて所有する本人認証アルゴリズムを管理するテーブルである。 10
- 【図 7】 実施例におけるユーザクライアント 110 の設定項目のテーブルである。
- 【図 8】 実施例におけるユーザクライアント 110 で所有するユーザテンプレートの管理テーブルである。
- 【図 9】 実施例における A P サーバ 140 の機能構成を示すブロック図である。
- 【図 10】 A P サーバ 140 にて所有する本人認証アルゴリズムを管理するテーブルである。
- 【図 11】 A P サーバ 140 の各本人認証方法に関して安全レベルに関してポリシーを設定するテーブルである。
- 【図 12】 A P サーバ 140 のサービスごとに安全性レベルを設定する項目のテーブルである。 20
- 【図 13】 クライアントと A P サーバ 140 との間で行われる本人認証の第 1 の全体処理フローである。
- 【図 14】 クライアントと A P サーバ 140 の間で行われる本人認証において、テンプレートが照合を実行する装置以外に格納されている場合の第 2 の全体処理フローである。
- 【図 15】 A P サーバ 140 からクライアントへ本人認証を要求するメッセージの項目を示すテーブルである。
- 【図 16】 図 15 のメッセージに対してクライアントのレスポンスメッセージの項目を示すテーブルである。
- 【図 17】 実施例における図 16 のメッセージに対するクライアントへの返答とチャレンジコードを含むメッセージの項目を示すテーブルである。 30
- 【図 18】 実施例における図 17 のメッセージに対するサーバへのレスポンスメッセージの項目を示すテーブルである。
- 【図 19】 実施例における図 18 のメッセージに対するクライアントの本人認証結果を含む通知メッセージの項目を示すテーブルである。
- 【図 20】 実施例におけるクライアントと A P サーバ 140 との間の本人認証において、認証サーバがアプリケーションの生体認証処理を代行する場合の第 3 全体処理フローである。
- 【図 21】 実施例における認証サーバが生体認証処理を代行する場合の A P サーバ 140 から認証サーバへの認証情報を送付するメッセージの項目を示すテーブルである。
- 【図 22】 実施例における認証サーバが生体認証処理を代行する場合の認証サーバから照 40
合結果を A P サーバ 140 への通知メッセージの項目を示すテーブルである。
- 【図 23】 クライアント 110 のユーザによる設定画面例である。
- 【図 24】 サーバにおけるアプリケーションごとのセキュリティポリシーの設定画面例である。
- 【図 25】 サーバにおける各認証方法のセキュリティポリシーの設定画面例である。
- 【符号の説明】
- 110・・・ユーザクライアント 110、120・・・インターネット（公衆網）、140・・・A P サーバ、150・・・C A、160・・・バイOMETリック認証局 B C A、170・・・認証サーバ。

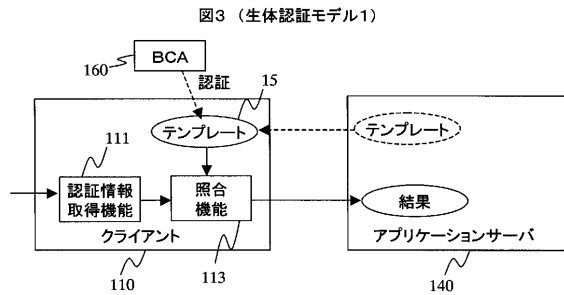
【図 1】



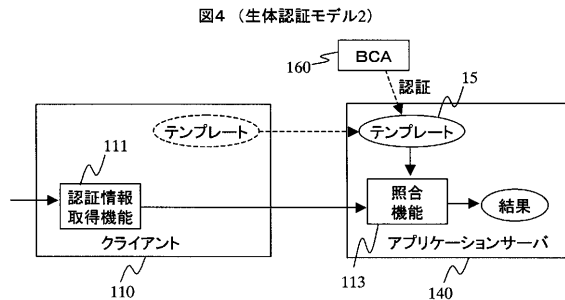
【図 2】



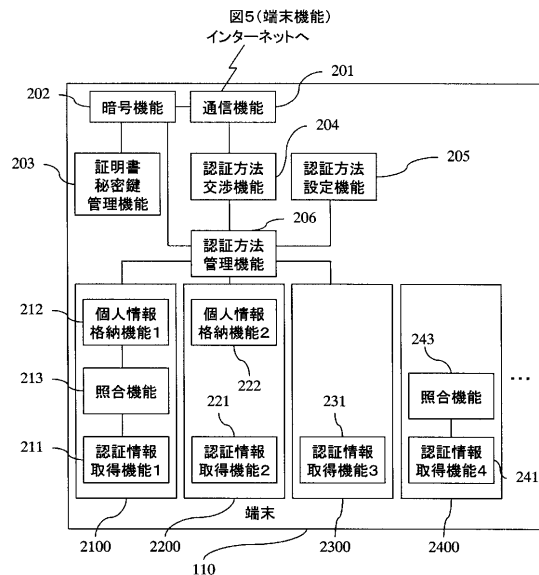
【図 3】



【図 4】



【図 5】



【図 6】

図6 (クライアントアルゴリズム管理)

KeyID	アルゴリズムID	Type	内容
1	001-002-001	S	ベンダ001の002照合ソフトV1 対応の生体収集装置
2	001-002-002	S	ベンダ001の002照合ソフトV2 対応の生体収集装置
3	011-001-003	S	ベンダ011の001照合ソフトV1 対応の生体収集装置
4	015-005-006	C	ベンダ015の005照合ソフトV6 の生体照合装置
	...		...
m	051-011-009	C	ベンダ051の011照合ソフトV9 の生体照合装置

【図 7】

図7 (ユーザ設定項目)

#	項目	内容
1	ユーザ情報	ユーザIDや証明書情報など
2	テンプレート情報	ユーザが所有するテンプレートの数
3	優先テンプレート	最も照合にしたいテンプレート
4	プライバシーモード	生体情報について、秘匿通信の 設定のON/OFF
5	利用範囲の限定宣言	利用範囲限定の宣言のON/OFF

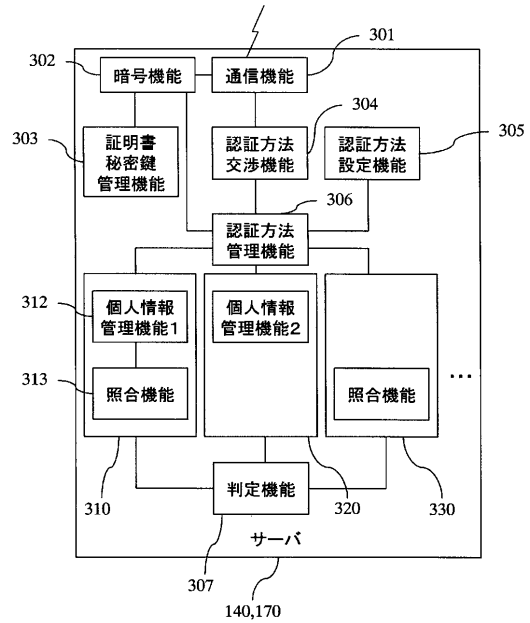
【図 8】

図8(クライアントのテンプレート管理)

KeyID	ユーザID	テンプレートID	アルゴリズムID
1	001	BCA1.co.jp_126	001-002-001
2	001	BCA1.co.jp_267	001-002-001
3	001	BCA2.co.jp_10693	011-001-003
4	045	BCA5.co.jp_381	015-005-006
	...	...	...

【図 9】

図9(サーバ機能)



【図 10】

図10(サーバアルゴリズム管理)

KeyID	アルゴリズムID	管理タイプ	内容
1	001-002-001	S	ベンダ001の002照合ソフト Ver.1
2	001-002-002	C	ベンダ001の002照合ソフト Ver.2
3	015-001-001	S	ベンダ015の001照合ソフト Ver.1
	...		...
n	032-005-021	O	ベンダ032の005照合ソフト Ver.21

S:サーバ、C:クライアント、O:アウトソース

【図 12】

図12(サーバ設定機能)

#	項目	内容
1	サービスID	サーバの提供するサービスのID
2	要求する認証モデル	このサービスが要求する認証モデル
3	要求する安全レベル	このサービスが要求する安全性レベル
4	要求するFAR	このサービスが要求するFAR
5	有効性の検証フラグ	有効性の検証の設定フラグ

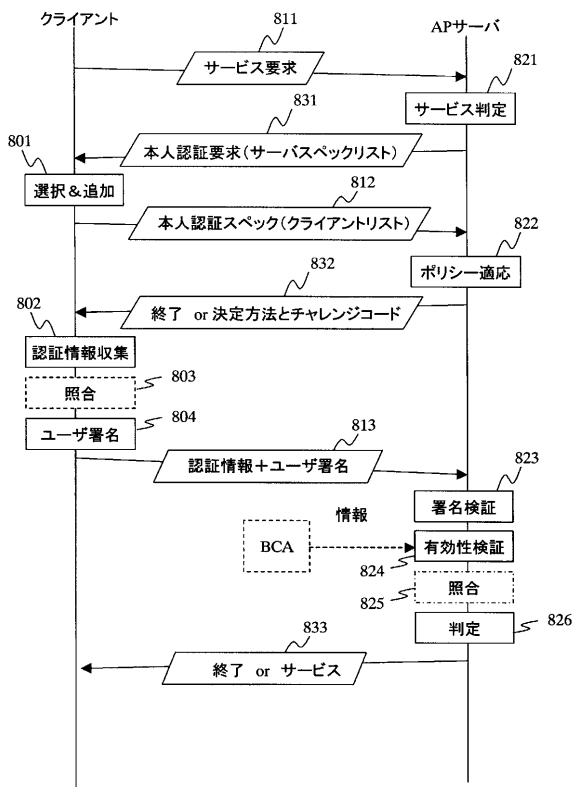
【図 11】

図11(サーバポリシー管理)

KeyID	アルゴリズムID	照合タイプ	安全レベル	内容
1	001-002-001	SS	1	照合ソフト001-002-001のS管理S照合タイプ
2	001-002-001	OS	1	照合ソフト001-002-001のO管理S照合タイプ
3	001-002-001	OC	1	照合ソフト001-002-001のO管理C照合タイプ
4	001-002-001	SC	1	照合ソフト001-002-001のS管理C照合タイプ
5	001-002-002	CC	2	ベンダ001の002照合ソフト Ver.2
6	015-001-001	SS	4	ベンダ015の001照合ソフト Ver.1
	...			...
n	032-005-021	OS	3	ベンダ032の005照合ソフト Ver.21

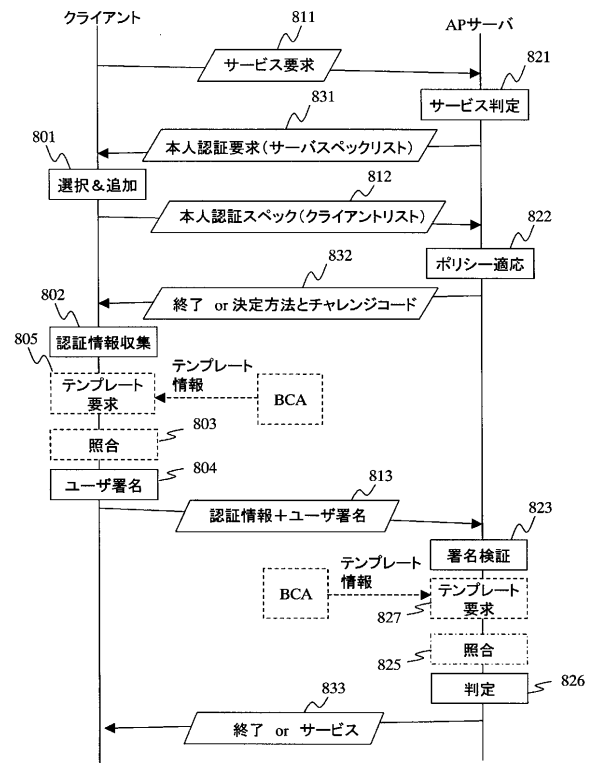
【図 13】

図13(認証フロー)



【図 14】

図14(認証フロー-2)



【図 15】

図15(本人認証要求)

項番	項目	内容
1	データ識別コード	クライアントへの認証要求とサーバスペックリストの通知コード
2	サービス要求情報	ユーザが要求したサービスの情報
3	要求する本人認証Flag	0: PKI認証のみ、1: クライアントで照合、2: サーバで照合、3: 両方可
4	生体照合リスト数	サーバの持つ生体照合機能の数(N)
5~N-4	生体照合アルゴリズム ID-1~N+Type	生体照合アルゴリズムのID(と照合モデルFlag)のリスト

【図 16】

図16(本人認証スペック)

項番	項目	内容
1	データ識別コード	クライアントスペックの通知コード
2	サービス要求情報	ユーザが要求したサービスの情報
3	生体照合リスト数	クライアントが対応できる生体照合機能の数(N)
4~N-3	生体照合アルゴリズム ID1~N+Type	生体照合アルゴリズムのID(と照合モデルFlag)のリスト

【図 17】

図17(決定方法とチャレンジコード)

項番	項目	内容
1	データ識別コード	照合方式の決定通知コード
2	サービス要求情報	ユーザが要求したサービスの情報
3	生体照合アルゴリズム IDX	本セッションで行う生体照合アルゴリズムのID(と照合モデルFlag)
4	チャレンジコード	PKIによる本人認証のための乱数(本人認証の各セッションごとに生成)

【図 18】

図18(認証情報とデジタル署名)

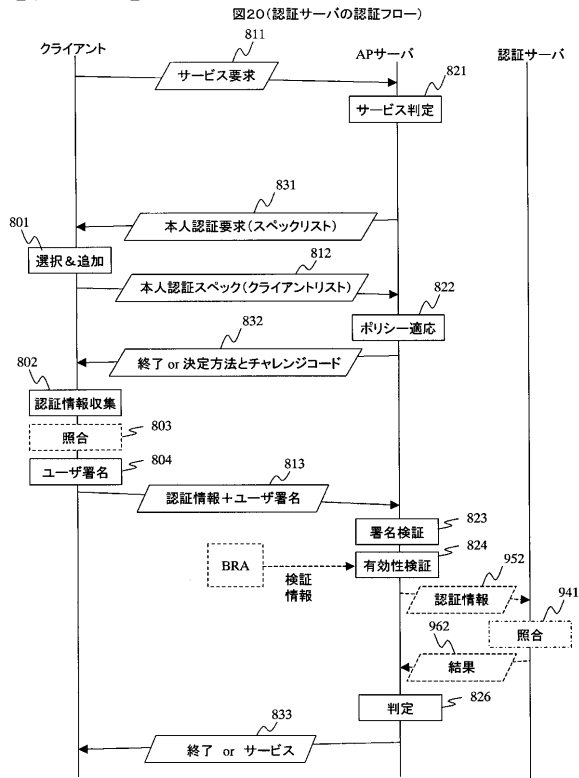
項番	項目	内容
1	データ識別コード	サーバへの本人認証情報提示コード
2	サービス要求情報	ユーザが要求したサービスの情報
3	要求する本人認証Flag	0: PKI認証のみ、1: クライアント認証、2: サーバ認証、3: 両方可
4	生体照合アルゴリズム ID-X	生体照合アルゴリズムのID(と照合モデルFlag)
5_1	認証情報1	サーバ認証の場合: ・収集した生体情報
5_2	認証情報2	クライアント(ダウンロード)認証の場合: ・照合結果と照合したテンプレートのID
5_3	認証情報3	アタッチド認証の場合: ・収集した生体情報 ・テンプレート(BCAの署名つき)
6	ユーザ署名	チャレンジコードに対するユーザ署名

【図 19】

図19(終了通知)

項番	項目	内容
1	データ識別コード	クライアントへの結果通知コード
2	サービス要求情報	ユーザが要求したサービスの情報
3	行った本人認証Flag	0: PKI認証のみ、1: クライアント認証、2: サーバ認証
4	生体照合アルゴリズム ID-X	生体照合アルゴリズムのID(と照合モデルFlag)
5	結果Flag	0: 本人認証OK 1: PKI認証NG 2: 生体テンプレートNG 3: 生体照合NG
6	サーバ署名	上記内容のサーバ署名

【図 20】



【図 21】

図21(認証情報)

項番	項目	内容
1	データ識別コード	認証サーバへの認証情報提示コード (セッションID含む)
2	生体照合アルゴリズム ID-X	生体照合アルゴリズムのID(と照合モデル Flag)
3_1	認証情報1	サーバ認証の場合: ・収集した生体情報とユーザID
3_2	認証情報2	アタッチド認証の場合: ・収集した生体情報 ・テンプレート(BCAの署名つき)
4	サーバ署名	上記データのサーバ署名

【図 22】

図22(結果情報)

項番	項目	内容
1	データ識別コード	クライアントへの結果通知コード (セッションIDを含む)
2	生体照合アルゴリズム ID-X	生体照合アルゴリズムのID(と照合モデル Flag)
3	照合結果Flag	1: OK/NG 2: 照合スコア 3: FAR
4	照合結果	3によって決定された値
5	認証サーバ署名	上記内容のサーバ署名

【図 23】

図23(ユーザ設定画面の例)

□ ユーザ設定画面

個人情報

氏名 Taro Hiatachi

住所 Kanda-Surugadai 4chome, Chiyoda, Tokyo

ユーザ名 E = taro@ponpon.hitachi.co.jp
CN = Taro HITACHI(20021004)
O = Hitachi, Ltd. C = JP

証明書 SN = 45
E = admin@ponpon.hitachi.co.jp
CN = ponponCA1
O = Hitachi, Ltd. C = JP

テンプレート情報

優先度

1 顔 A社アルゴリズム

2 指紋(左示指) B社アルゴリズム

3 指紋(左中指) B社アルゴリズム

4 PIN C社アルゴリズム

セキュリティモード

☐ 秘匿通信

☐ 利用範囲の限定宣言

【図 24】

図24(サーバ設定画面の例)

□ サーバ設定

認証サービス管理

サービスID	サービス	認証モデル	安全性レベル	FAR	有効性検証フラグ
001	口座振込	S	3	0.01%	必須
002	口座振替	S	3	0.01%	必須
003	新規預金	S-C	2	0.1%	不要
004	繰取引	C	3	0.05%	バッチ
005	証券取引	S	3	0.05%	必須
006	残高照会	S-C	1	0.1%	不要
007	デビット	C	2	0.05%	バッチ
008	キャッシング	C	2	0.01%	必須

新規 修正 削除

□ サービスプロフィール

サービスID

サービス内容

認証モデル ☐ サーバ照合 ☐ クライアント照合

安全性レベル

FAR

有効性検証

登録 キャンセル

【図 25】

図25(サーバのアルゴリズム管理例)

☐ ポリシー設定

ポリシー管理

アルゴリズムID	アルゴリズム	照合タイプ	安全性レベル	FAR
001-0002-001	001社照合ソフト0002のVer1	S	3	0.01%
001-0002-002	001社照合ソフト0002のVer2	S	3	0.01%
002-0001-003	002社照合ソフト0003のVer3	C	2	0.1%
001-0005-001	001社照合ソフト0005のVer1	S	3	0.05%
010-0001-023	010社照合ソフト0001のVer23	S	3	0.05%
021-0052-001	021社照合ソフト0052のVer1	O	1	0.1%
258-1004-006	258社照合ソフト1004のVer6	C-O	2	0.05%
369-0007-008	369社照合ソフト0007のVer8	S-O	2	0.01%

新規

修正

削除

フロントページの続き

(72)発明者 瀬戸 洋一

神奈川県川崎市麻生区王禅寺1099番地 株式会社日立製作所システム開発研究所内

Fターム(参考) 5B085 AA08 AE25 AE26 AE29 BA06 BG02 BG03 BG07

5J104 AA07 GA05 KA01 KA05 KA16 NA02 NA05 NA27 NA38 PA07