(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2019-92031
(P2019-92031A)
(43)公開日　令和1年6月13日(2019.6.13)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/32	(2006.01)	H04L	9/00	675D	5J104
G06F 21/44	(2013.01)	H04L	9/00	675B	
G06F 21/64	(2013.01)	G06F	21/44	350	
H04L 9/08	(2006.01)	G06F	21/64		
		H04L	9/00	601F	

審査請求 未請求　請求項の数 5　ＯＬ　（全 12 頁）

(21)出願番号　特願2017-219266 (P2017-219266)
(22)出願日　平成29年11月14日 (2017.11.14)

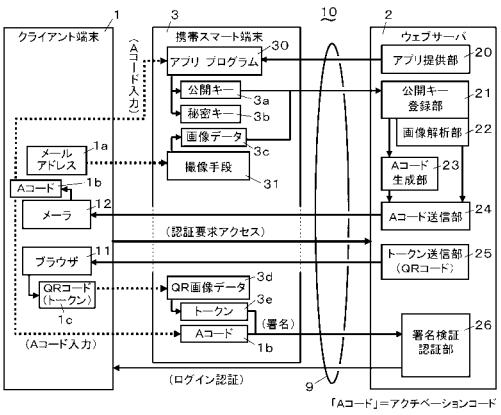
（特許庁注：以下のものは登録商標）
１．ＱＲコード

(71)出願人　500037528
株式会社サイバーリンクス
和歌山県和歌山市紀三井寺８４９番地の３
(74)代理人　100084375
弁理士　板谷　康夫
(74)代理人　100121692
弁理士　田口　勝美
(74)代理人　100125221
弁理士　水田　慎一
(74)代理人　100142077
弁理士　板谷　真之
(72)発明者　村上　恒夫
和歌山県和歌山市紀三井寺８４９番地の３
株式会社サイバーリンクス内

最終頁に続く

(54)【発明の名称】相互認証システムおよび相互認証方法

(57)【要約】
【課題】本発明は、クライアント端末がウェブサーバに認証を求める際に予めユーザ情報を保存しているキャリアサーバを必要とせず、ＩＤやパスワードを用いることなくセキュリティを確保して簡単に操作でき、任意サーバによりシステムを柔軟に構成できる相互認証システムおよび認証方法を提供する。
【解決手段】相互認証システム１０はクライアント端末１とウェブサーバ２との相互認証に携帯スマート端末３を用いる。スマート端末３はサーバ２から得たプログラム３０を用いて公開キー３ａと秘密キー３ｂを生成し、メールアドレスの画像データ３ｃと公開キー３ａとをサーバ２に送信し、Ａコード１ｂを受け取る。スマート端末３はプログラム３０を用いて、クライアント端末１に送信され表示されたＱＲコード１ｃの画像からトークン３ｅを取得し、Ａコード１ｂと共に秘密キー３ｂで署名してサーバ２に送信する。サーバ２は公開キー３ａで署名を検証し認証する。
【選択図】図２



【特許請求の範囲】
【請求項１】
クライアント端末とウェブサーバとの間で相互認証を行う相互認証システムであって、
ブラウザが格納されている前記クライアント端末と、
前記クライアント端末と所定の関係にあるユーザが保有する携帯スマート端末と、
不特定多数または特定多数のユーザに対して所定のサービスを提供する前記ウェブサーバと、を備え、
前記ウェブサーバは、前記携帯スマート端末からのアクセスに応じて、公開キーを生成するためのアプリケーションプログラムを前記携帯スマート端末にインストール可能に提供し、かつ、任意のクライアント端末からのアクセスに応じてランダムなトークンが埋め込まれたＱＲコードを前記アクセスのあったクライアント端末に送信し、
前記携帯スマート端末は、前記アプリケーションプログラムをインストールすることによって公開キーと秘密キーを生成し、前記携帯スマート端末の撮像手段により撮影した画像データであって前記クライアント端末と所定の関係にあるユーザへの連絡先となるメールアドレスまたは居所情報を含む画像データと、生成された前記公開キーとを前記ウェブサーバに送信し、
前記ウェブサーバは、前記携帯スマート端末から送信された前記公開キーの登録時にアクティベーションコードを作成し、当該アクティベーションコードを前記画像データ上の前記メールアドレスまたは前記居所に送信または配送し、
前記携帯スマート端末は、ユーザによって前記アクティベーションコードが入力されることで、前記アプリケーションプログラムが有効となり、
前記クライアント端末は、前記ウェブサーバに認証を求める際に、前記ブラウザにより前記ウェブサーバにアクセスしてログイン画面を呼び出し、前記ウェブサーバから送信された前記ＱＲコードを表示し、
前記携帯スマート端末は、前記撮像手段により前記ＱＲコードを撮影することにより前記アプリケーションを用いて前記トークンを取得し、前記トークンと前記アクティベーションコードとを前記秘密キーで署名して前記ウェブサーバに送信し、
前記ウェブサーバは、前記携帯スマート端末から送信された前記署名を前記公開キーで検証し、正しければ前記クライアント端末を認証してログイン可能とすることを特徴とする相互認証システム。
【請求項２】
前記メールアドレスは、前記クライアント端末上、または前記携帯スマート端末上のメールアドレスである、ことを特徴とする請求項１記載の相互認証システム。
【請求項３】
前記ウェブサーバは、前記アプリケーションプログラムの他に、暗号化用公開キーを前記携帯スマート端末に提供し、
前記携帯スマート端末は、前記トークンと前記アクティベーションコードとを前記秘密キーで署名したデータを、前記暗号化用公開キーを用いて暗号化して前記ウェブサーバに送信する、ことを特徴とする請求項１または請求項２に記載の相互認証システム。
【請求項４】
前記ウェブサーバは、前記ウェブサーバとは異なる事前に認証済みの他のウェブサーバに対する前記クライアント端末によるログインを許可する権限を有し、前記クライアント端末を認証することによって、前記クライアント端末から前記他のウェブサーバへのログインを許可するサーバとして動作する、ことを特徴とする請求項１乃至請求項３の何れか一項に記載の相互認証システム。
【請求項５】
ブラウザが格納されているクライアント端末と、前記クライアント端末と所定の関係にあるユーザが保有する携帯スマート端末と、不特定多数または特定多数のユーザに対して所定のサービスを提供するウェブサーバと、を備えるシステムにおいて、前記クライアント端末と前記ウェブサーバとの相互認証を行う相互認証方法であって、

前記ウェブサーバは、前記携帯スマート端末からのアクセスに応じて、公開キーを生成するためのアプリケーションプログラムを前記携帯スマート端末にインストール可能に提供し、かつ、任意のクライアント端末からのアクセスに応じてランダムなトークンが埋め込まれたＱＲコードを前記アクセスのあったクライアント端末に送信し、
前記携帯スマート端末は、前記アプリケーションプログラムをインストールすることによって公開キーと秘密キーを生成し、前記携帯スマート端末の撮像手段により撮影した画像データであって前記クライアント端末と所定の関係にあるユーザへの連絡先となるメールアドレスまたは居所情報を含む画像データと、生成された前記公開キーとを前記ウェブサーバに送信し、
前記ウェブサーバは、前記携帯スマート端末から送信された前記公開キーの登録時にアクティベーションコードを作成し、当該アクティベーションコードを前記画像データ上の前記メールアドレスまたは前記居所に送信または配送し、
前記携帯スマート端末は、ユーザによって前記アクティベーションコードが入力されることで、前記アプリケーションプログラムが有効となり、
前記クライアント端末は、前記ウェブサーバに認証を求める際に、前記ブラウザにより前記ウェブサーバにアクセスしてログイン画面を呼び出し、前記ウェブサーバから送信された前記ＱＲコードを表示し、
前記携帯スマート端末は、前記撮像手段により前記ＱＲコードを撮影することにより前記アプリケーションを用いて前記トークンを取得し、前記トークンと前記アクティベーションコードとを前記秘密キーで署名して前記ウェブサーバに送信し、
前記ウェブサーバは、前記携帯スマート端末から送信された前記署名を前記公開キーで検証し、正しければ前記クライアント端末を認証してログイン可能とする、ことを特徴とする相互認証方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、クライアント端末とウェブサーバとの相互認証システムおよび相互認証方法に関する。
【背景技術】
【０００２】
従来、クライアント端末がウェブサーバに認証を求める際にキーロガーやフィッシング詐欺を防ぎ、プライバシーを保ち、簡単に操作できるように、携帯電話端末とキャリアサーバとを援用する相互認証システムおよび相互認証方法が知られている（例えば、特許文献１参照）。このシステムおよび方法において、キャリアサーバは、ユーザ情報、ウェブサーバ情報、および認証用情報を保存しており、ウェブサーバは、クライアント端末に２次元バーコードでセッションＩＤとウェブサーバ情報を送信する。２次元バーコードは、携帯電話端末で撮影されて、携帯電話固有情報と共に、キャリアサーバに送信される。キャリアサーバは、携帯電話固有情報を参照してユーザを特定することによりクライアント端末とウェブサーバとの認証を行う。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２００８－１７６４４９号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、上述した特許文献１に示されるような相互認証システムと方法は、携帯電話固有情報を検証できるキャリアサーバを通じて認証するものであり、ユーザ情報などを予め保存しているキャリアサーバを用いることなく任意のサーバによる認証ができず、システムを柔軟に構成することができない。

【０００５】
本発明は、上記課題を解消するものであって、クライアント端末がサーバに認証を求める際にユーザ情報などを予め保存しているキャリアサーバを用いることなく、また、携帯電話固有情報やパスワードを必要とすることなくキーロガーやフィッシング詐欺等から防護して、任意サーバとクライアント端末との相互認証が可能な相互認証システムおよび相互認証方法を提供することを目的とする。
【課題を解決するための手段】
【０００６】
上記課題を達成するために、本発明の相互認証システムは、クライアント端末とウェブサーバとの間で相互認証を行う相互認証システムであって、ブラウザが格納されているクライアント端末と、クライアント端末と所定の関係にあるユーザが保有する携帯スマート端末と、不特定多数または特定多数のユーザに対して所定のサービスを提供するウェブサーバと、を備え、ウェブサーバは、携帯スマート端末からのアクセスに応じて、公開キーを生成するためのアプリケーションプログラムを携帯スマート端末にインストール可能に提供し、かつ、任意のクライアント端末からのアクセスに応じてランダムなトークンが埋め込まれたＱＲコードをアクセスのあったクライアント端末に送信し、携帯スマート端末は、アプリケーションプログラムをインストールすることによって公開キーと秘密キーを生成し、携帯スマート端末の撮像手段により撮影した画像データであってクライアント端末と所定の関係にあるユーザへの連絡先となるメールアドレスまたは居所情報を含む画像データと、生成された公開キーとをウェブサーバに送信し、ウェブサーバは、携帯スマート端末から送信された公開キーの登録時にアクティベーションコードを作成し、当該アクティベーションコードを画像データ上のメールアドレスまたは居所に送信または配送し、携帯スマート端末は、ユーザによってアクティベーションコードが入力されることで、アプリケーションプログラムが有効となり、クライアント端末は、ウェブサーバに認証を求める際に、ブラウザによりウェブサーバにアクセスしてログイン画面を呼び出し、ウェブサーバから送信されたＱＲコードを表示し、携帯スマート端末は、撮像手段によりＱＲコードを撮影することによりアプリケーションを用いてトークンを取得し、トークンとアクティベーションコードとを秘密キーで署名してウェブサーバに送信し、ウェブサーバは、携帯スマート端末から送信された署名を公開キーで検証し、正しければクライアント端末を認証してログイン可能とすることを特徴とする。
【０００７】
本発明の相互認証方法は、ブラウザが格納されているクライアント端末と、クライアント端末と所定の関係にあるユーザが保有する携帯スマート端末と、不特定多数または特定多数のユーザに対して所定のサービスを提供するウェブサーバと、を備えるシステムにおいて、クライアント端末とウェブサーバとの相互認証を行う相互認証方法であって、ウェブサーバは、携帯スマート端末からのアクセスに応じて、公開キーを生成するためのアプリケーションプログラムを携帯スマート端末にインストール可能に提供し、かつ、任意のクライアント端末からのアクセスに応じてランダムなトークンが埋め込まれたＱＲコードをアクセスのあったクライアント端末に送信し、携帯スマート端末は、アプリケーションプログラムをインストールすることによって公開キーと秘密キーを生成し、携帯スマート端末の撮像手段により撮影した画像データであってクライアント端末と所定の関係にあるユーザへの連絡先となるメールアドレスまたは居所情報を含む画像データと、生成された公開キーとをウェブサーバに送信し、ウェブサーバは、携帯スマート端末から送信された公開キーの登録時にアクティベーションコードを作成し、当該アクティベーションコードを画像データ上のメールアドレスまたは居所に送信または配送し、携帯スマート端末は、ユーザによってアクティベーションコードが入力されることで、アプリケーションプログラムが有効となり、クライアント端末は、ウェブサーバに認証を求める際に、ブラウザによりウェブサーバにアクセスしてログイン画面を呼び出し、ウェブサーバから送信されたＱＲコードを表示し、携帯スマート端末は、撮像手段によりＱＲコードを撮影することによりアプリケーションを用いてトークンを取得し、トークンとアクティベーションコード

とを秘密キーで署名してウェブサーバに送信し、ウェブサーバは、携帯スマート端末から送信された署名を公開キーで検証し、正しければクライアント端末を認証してログイン可能とする、ことを特徴とする。

【発明の効果】

【０００８】

本発明の相互認証システムおよび認証方法によれば、ウェブサーバから携帯スマート端末に提供した所定のプログラムと携帯スマート端末の撮像手段とを用いて認証作業を進め、ユーザ情報などを予め保存しているキャリアサーバを用いることなく、所定のプログラムを提供できる任意サーバとクライアント端末との相互認証を実現でき、キーロガーやフィッシング詐欺を防ぐシステムを柔軟に構成することができる。

【図面の簡単な説明】

【０００９】

【図１】本発明の実施形態に係る相互認証システムの構成を示す模式図。

【図２】同相互認証システムを構成するクライアント端末、携帯スマート端末、およびウェブサーバの各構成と相互関連を説明するブロック図。

【図３】同相互認証システムの動作および一実施形態に係る相互認証方法を説明するシーケンス図。

【図４】他の実施形態に係る相互認証システムの構成を示す模式図。

【図５】さらに他の実施形態に係る相互認証システムを構成するクライアント端末、携帯スマート端末、およびウェブサーバの各構成と相互関連を説明するブロック図。

【図６】同相互認証システムにおいて実行される相互認証方法を説明するシーケンス図。

【発明を実施するための形態】

【００１０】

以下、本発明の実施形態に係る相互認証システムおよび認証方法について、図面を参照して説明する。図１、図２に示すように、相互認証システム１０は、互いにインターネットなどのネットワーク９によって双方向通信可能に接続されたクライアント端末１とウェブサーバ２との間で相互認証を行うシステムである。相互認証システム１０は、その相互認証に際して、クライアント端末１と所定の関係にあるユーザが保有する携帯スマート端末３を用いる。携帯スマート端末３は、移動電話回線やネットワーク９を介してウェブサーバ２とデータ通信を行うことができる端末である。

【００１１】

クライアント端末１は、ブラウザ１１と、メーラ１２とを有している。携帯スマート端末３は、移動電話回線やネットワーク９を介してウェブサーバ２とデータ通信を行うことができる。携帯スマート端末３は、撮像手段３１を有し、撮像手段３１で撮像した画像のデータ、例えば、メールアドレスが書かれた紙片３ｘの画像データをウェブサーバ２に送信することができる。

【００１２】

ウェブサーバ２は、不特定多数または特定多数のユーザであるクライアント端末に対して所定のサービスを提供するサーバである。ウェブサーバ２は、クライアント端末の認証に用いる構成要件として、アプリ提供部２０、公開キー登録部２１、画像解析部２２、アクティベーションコード（Ａコードと略記する）１ｂを作成するＡコード生成部２３、Ａコード送信部２４、トークン送信部２５、および署名検証認証部２６を備えている。Ａコード１ｂは、受付番号または整理番号の機能を有する他、後述のアプリケーションプログラム３０を活性化して有効化するためのコードとしての機能を有する。特定多数のユーザは、相互認証システム１０が、例えば、企業、大学、団体等で用いられる場合に、それらに属するクライアント端末１を使用する複数の社員や構成員である。

【００１３】

アプリ提供部２０は、携帯スマート端末３において用いられるアプリケーションプログラム３０を、携帯スマート端末３からのアクセスに応じて携帯スマート端末３にインストール可能に提供する。アプリケーションプログラム３０は、本実施形態ではウェブサーバ

２から携帯スマート端末３にダウンロードによって提供される例を示すが、ウェブサーバ２とは異なるサーバーからダウンローしてもよく、またダウンロード以外の他の方法で提供してもよい。アプリケーションプログラム３０は、公開キー３ａと秘密キー３ｂとを生成するために用いられる。これらの公開キー３ａと秘密キー３ｂの生成は、例えば、ＲＳＡ暗号技術を用いて行われる。公開キー登録部２１は、アプリケーションプログラム３０をダウンロードした携帯スマート端末３から送信されてきた公開キー３ａを、後の署名検証に用いるために登録する。画像解析部２２は、携帯スマート端末３から公開キー３ａと共に送信されてきた画像データを解析して、画像データ上のメールアドレス１ａを読み出す。

【００１４】

Ａコード生成部２３は、携帯スマート端末３から送信された公開キー３ａが登録される際にＡコード１ｂを作成する。Ａコード送信部２４は、Ａコード１ｂを、クライアント端末１のメーラ１２が管理するメールアドレス１ａに送信する。なお、メールアドレス１ａは、クライアント端末１上のメーラ１２が管理するメールアドレスに限られず、クライアント端末１と所定の関係にあるユーザが保有するメールアドレスであればよく、例えば、携帯スマート端末３上のメーラが管理するメールアドレスであってもよい。メールアドレス１ａは、ウェブサーバ２からクライアント端末１または携帯スマート端末３のユーザへの連絡先である。

【００１５】

トークン送信部２５は、任意のクライアント端末の１つであるクライアント端末１からのアクセスに応じて、ランダムなトークン３ｅが埋め込まれたＱＲコード１ｃを、アクセスのあったクライアント端末１に送信する。トークン３ｅは、ログインによって開設されるセッションを識別するセッションＩＤとなる。署名検証認証部２６は、携帯スマート端末３を介して署名されて送信されてくるトークン３ｅとＡコード１ｂを、公開キー３ａで検証し、正しければクライアント端末１を認証してログイン可能とする。ＱＲコード１ｃは、クライアント端末１と携帯スマート端末３とを一意的に繋ぐためだけの情報であるトークン３ｅが埋め込まれたものであればよく、例えば、ランダムな２次元模様で構成される。従って、ＱＲコード１ｃは、解読されても問題のない一般的なものであり、一時的なものである。

【００１６】

次に、図１，図２に加えて、図３を参照して、相互認証システム１０において実行される相互認証方法を時系列に説明する。ここで、説明の簡単のため、クライアント端末１のユーザと、携帯スマート端末３のユーザとは同じであるとするが、異なっていてもよい。ウェブサーバ２による認証を受けたいクライアント端末１のユーザは、携帯スマート端末３を用いて、ウェブサーバ２に対して、相互認証に用いられるアプリケーションプログラム３０のダウンロードによる提供を要求する（Ｓ１）。ウェブサーバ２は、携帯スマート端末３からアプリケーションプログラム３０のダウンロード要求があると、アプリ提供部２０がアプリケーションプログラム３０を携帯スマート端末３に送信する。携帯スマート端末３は、そのダウンロードを実行する（Ｓ２）。アプリケーションプログラム３０は、ウェブサーバ２のアプリ提供部２０からダウンロードされる。携帯スマート端末３は、アプリケーションプログラム３０をインストールして実行することにより、公開キー３ａと秘密キー３ｂとを生成する（Ｓ３）。

【００１７】

携帯スマート端末３は、ユーザによる操作により、クライアント端末１のメーラ１２の管轄下のメールアドレスが記載された名刺を撮像手段３１によって撮像し（Ｓ４）、その画像データ３ｃを、公開キー３ａと共に、ウェブサーバ２に送信する（Ｓ５）。携帯スマート端末３のユーザは、画像データ３ｃをウェブサーバ２に送信することにより、ウェブサーバ２からＡコード１ｂをメールで受け取ることが可能になる。画像データ３ｃは、名刺の画像に限られず、メールアドレス１ａが記載された紙片などの画像であってもよい。

【００１８】

ウェブサーバ２は、携帯スマート端末３から公開キー３ａと画像データ３ｃの送信があると、公開キー登録部２１が公開キー３ａをメモリに保存して登録し、画像解析部２２が画像データ３ｃからメールアドレス１ａを読み出して取得し、Ａコード生成部２３がＡコード１ｂを生成する（Ｓ６）。ウェブサーバ２は、作成されたＡコード１ｂを、画像データ３ｃから読み出されたメールアドレス１ａに、Ａコード送信部２４から送信する（Ｓ７）。クライアント端末１は、ウェブサーバ２のＡコード送信部２４から送信されたメールをメーラ１２で受信する。Ａコード送信部２４からのメールには、Ａコード１ｂが記載されている。

【００１９】

クライアント端末１のユーザは、メーラ１２に届いたメールを開いてＡコード１ｂを表示し（Ｓ８）、読み取ったＡコード１ｂを、携帯スマート端末３におけるアプリケーションプログラム３０に対し手入力する（Ｓ９）。これにより、携帯スマート端末３は、クライアント端末１のメーラ１２がウェブサーバ２から受信したメールに記載されたＡコード１ｂを、ユーザ操作によって、アプリケーションプログラム３０に対して入力される。また、アプリケーションプログラム３０は、Ａコード１ｂが入力されることにより、相互認証作業に用いられる機能の１つである、ＱＲコード１ｃの画像からトークン３ｅを読み出す機能が、有効化される（Ｓ１０）。

【００２０】

クライアント端末１のユーザは、所望のＵＲＬにログインする認証を求めて、ブラウザ１１を用いてウェブサーバ２にアクセスする（Ｓ１１）。ウェブサーバ２は、クライアント端末１から認証要求のアクセスがあると、ウェブサーバ２のトークン送信部２５が、トークン３ｅを埋め込んだＱＲコード１ｃをクライアント端末１に送信する（Ｓ１２）。クライアント端末１のブラウザ１１には、ウェブサーバ２のログイン画面が表示され（Ｓ１３）、その画面にＱＲコード１ｃが表示される（Ｓ１４）。このようにして、クライアント端末１は、ブラウザ１１を介してウェブサーバ２の所定のＵＲＬにアクセスすることにより、ウェブサーバ２のトークン送信部２５から送信されるＱＲコード１ｃをブラウザ１１上に表示する。

【００２１】

携帯スマート端末３のユーザは、撮像手段３１を用いて、ブラウザ１１上に表示されたＱＲコード１ｃを撮像し、アプリケーションプログラム３０を用いて、そのＱＲ画像データ３ｄからトークン３ｅを取得する（Ｓ１５）。すなわち、携帯スマート端末３は、クライアント端末１のブラウザ１１に表示されたＱＲコード１ｃの画像を、ユーザが操作する撮像手段３１によって撮像してＱＲ画像データ３ｄとして取り込む。携帯スマート端末３は、Ａコード１ｂの入力によって事前に有効化されたアプリケーションプログラム３０によって、ＱＲ画像データ３ｄからトークン３ｅを読み出す。

【００２２】

携帯スマート端末３におけるアプリケーションプログラム３０は、ＱＲ画像データ３ｄから読み出されたトークン３ｅとユーザによって入力されたＡコード１ｂとを、秘密キー３ｂによって署名し（Ｓ１６）、ウェブサーバ２に送信する（Ｓ１７）。ウェブサーバ２は、携帯スマート端末３からトークン３ｅとＡコード１ｂが秘密キー３ｂによって署名されて送信されてくると、署名検証認証部２６が、署名されたトークン３ｅとＡコード１ｂを公開キー３ａを用いて検証する（Ｓ１８）。ウェブサーバ２は、署名が正しいことを検証できた場合に、クライアント端末１を認証し、クライアント端末１によるログインを可能とする認証通知を行う（Ｓ１９）。クライアント端末１が認証通知を受け取ることにより、相互認証作業が完了し、所定のＵＲＬにログインが成功する（Ｓ２０）。

【００２３】

このログインに際し、ユーザがクライアント端末１に対して行う操作は、ブラウザ１１を用いてウェブサーバ２にアクセスするだけであり（Ｓ１１）、このアクセス時の操作は通常の操作であり、キーロガー、盗聴、フィッシング等に対処する必要がある固有情報の入力は行われない。認証に必要な情報の送信は、携帯スマート端末３を介して行われてい

る。また、クライアント端末１から携帯スマート端末３への情報転送は、クライアント端末１に対する物理的な接触や接続なしで実現される。つまり、この情報転送は、Ａコード１ｂをユーザが視認して携帯スマート端末３に手入力し、ＱＲコード１ｃを携帯スマート端末３によって撮像してトークン３ｅを取得することにより、行われる。

【００２４】

本実施形態の相互認証システムおよび相互認証方法によれば、ウェブサーバ２からダウンロードしたアプリケーションプログラム３０と携帯スマート端末３の撮像手段３１とを用いて認証を進めるので、ログインの手続にパスワードが不要である。従って、スパイウェアに対する情報漏洩防止とフィッシング詐欺対策を実現でき、クライアント端末１によるウェブサイトへのアクセスの際のセキュリティを確保して簡単に操作でき、安全性を向上できる。また、本実施形態によれば、携帯スマート端末３における電話回線のキャリア情報そのものは認証に用いないので、ウェブサーバ２は、ユーザ情報などを予め保持しているキャリアサーバなどの特定のサーバに限定されない。従って、任意のサーバをウェブサーバ２に用いて柔軟に相互認証システムや相互認証方法を構築できる。

【００２５】

また、メールアドレスを通知する際の画像データ３ｃに名刺の画像データを用いることにより、本人確認を名刺を利用して強化できる。ビジネス上ほとんどの人が名刺を持っており、本人すなわち名刺となる。他人の名刺を使うことも可能であるが、その名刺に書かれたメールアドレスにＡコード１ｂを送信することにより、２要素認証に近い簡易的な、なりすまし防止機能を実現できる。また、運用者と利用者間で本人確認を名刺画像という簡便な方法で実現できる効果がある。運用者がサービス提供者である場合に、利用者登録と利用者認証を、この名刺画像データを用いて簡易化できる。

【００２６】

（変形例）

この変形例の相互認証システムおよび相互認証方法は、携帯スマート端末３からウェブサーバ２に送信するデータを、ウェブサーバ２が提供する公開キー（暗号化用公開キーという）によって暗号化して送信する。ウェブサーバ２は、アプリケーションプログラム３０の他に、暗号化用公開キーを携帯スマート端末３に提供する。暗号化用公開キーは、ダウンロードされるアプリケーションプログラム３０に含めて提供してもよく、アプリケーションプログラム３０とは別途に提供してもよい。

【００２７】

携帯スマート端末３は、トークン３ｅとＡコード１ｂとを秘密キー３ｂで署名したデータを、さらに暗号化用公開キーを用いて暗号化してウェブサーバ２に送信する。携帯スマート端末３は、メールアドレス１ａを撮像した画像データ３ｃをウェブサーバ２に送信する場合においても、画像データ３ｃを暗号化用公開キーを用いて暗号化して送信してもよい。ウェブサーバ２は、暗号化されて送信されたトークン３ｅ等のデータや画像データ３ｃを、自己の有する秘密キーを用いて複合する。これにより、情報漏洩をより厳密に防止できる。

【００２８】

（他の実施形態）

図４は、他の実施形態に係る相互認証システムを示す。この実施形態に係る相互認証システム１０には、ウェブサーバ２とは異なる１つまたは複数の他のウェブサーバ４が関与する。ウェブサーバ２は、他のウェブサーバ４に関するセキュリティ上の安全性を事前に検証してその旨、認証済みである。また、ウェブサーバ２は、他のウェブサーバ４に対する任意のクライアント端末のログインを許可または拒否する権限を有している。

【００２９】

クライアント端末１は、ウェブサーバ２を介して他のウェブサーバ４に対してログインすることができる。例えば、ウェブサーバ２は、図３に示した相互認証方法の手順と同様の手順に基づいて、クライアント端末１を認証し、他のウェブサーバ４のＵＲＬにリダイレクトすることにより、クライアント端末１から他のウェブサーバ４へのログインを許可

する。ウェブサーバ２は、クライアント端末１から他のウェブサーバ４へのログインを許可する認証用のサーバとして動作する。

【００３０】

なお、本発明は、上記構成に限られることなく種々の変形が可能である。例えば、上述した実施形態や変形例の構成を互いに組み合わせた構成とすることができる。Ａコードは、メールアドレスの定期的な存在確認に用いてもよい。また、携帯スマート端末３は、携帯スマート端末３と同等の機能を有する通信デバイスまたは通信デバイス等の組合せ、例えば、携帯撮像手段が接続されたコンピュータ端末、によって代替してもよい。

【００３１】

（さらに他の実施形態）

図５、図６は、本実施形態に係る相互認証システム１０と相互認証方法を示す。図５に示すように、本実施形態の相互認証システム１０は、クライアント端末１がメーラおよびメールアドレスを必須要件とはしていない。この相互認証システム１０は、図２、図３に示した実施形態におけるＡコード１ｂをメールアドレス１ａに送信する構成に代えて、クライアント端末１と所定の関係にあるユーザ５の居所に郵便や宅配便によってＡコード１ｂを配送する構成となっている。ユーザ５は、例えばクライアント端末１の使用権限を有する所有者またはユーザである。ユーザ５は、説明の簡単のため、携帯スマート端末３のユーザと同じとするが、異なっていてもよい。

【００３２】

図５に加えて、図６を参照して、相互認証システム１０において実行される相互認証方法を、図２、図３に示した実施形態と異なる点に注目して説明する。ユーザ５は、ユーザ５への連絡先となる住所（居所）１ｆが記載された書面を、撮像手段３１によって撮像し（Ｓ４０）、その居所情報を含む画像データ３ｃを、公開キー３ａと共に、ウェブサーバ２に送信する（Ｓ５０）。ユーザ５は、画像データ３ｃをウェブサーバ２に送信することにより、ウェブサーバ２からＡコード１ｂを郵便または宅配便等の配送によって受け取ることが可能になる。書面としては、ユーザ５の住所１ｆが記載された保険証、免許証、または公的証明書などが挙げられる。

【００３３】

ウェブサーバ２は、携帯スマート端末３から公開キー３ａと画像データ３ｃの送信があると、公開キー登録部２１が公開キー３ａをメモリに保存して登録し、画像解析部２２が画像データ３ｃから住所１ｆを読み出して取得し、Ａコード生成部２３がＡコード１ｂを生成する（Ｓ６０）。ウェブサーバ２は、作成されたＡコード１ｂを、画像データ３ｃから読み出された住所１ｆに、Ａコード送信部２４を経て送信する（Ｓ７０）。この送信は、例えば、Ａコード送信部２４がＡコード１ｂを印刷出力した紙片を、郵便または宅配便等によって配送することによって行われる。

【００３４】

ユーザ５は、ウェブサーバ２から配送された送信物を開封してＡコード１ｂを受け取り（Ｓ８０）、読み取ったＡコード１ｂを、携帯スマート端末３におけるアプリケーションプログラム３０に手入力する（Ｓ９）。以下の動作は、図２、図３に示した実施形態における動作と同様である。

【００３５】

本実施形態の相互認証システム１０および相互認証方法によれば、メールアドレスを必須要件とすることなく認証作業を進めることができる。ユーザ５への連絡先である住所１ｆの画像データ３ｃは、ユーザ５を認証するための傍証とすることができる。傍証としての有効性を高めるには、例えば、健康保険証、車両運転免許証、マイナンバーカードなどの公的機関が発行した証明書の画像データに限定し、その画像に写っている内容に対する品質等の条件を適切に設定して、画像データの段階での認証可否判断を行うようにすればよい。

【００３６】

なお、より強いセキュリティが要求される場合には、ウェブサイトの認証に生体認証機

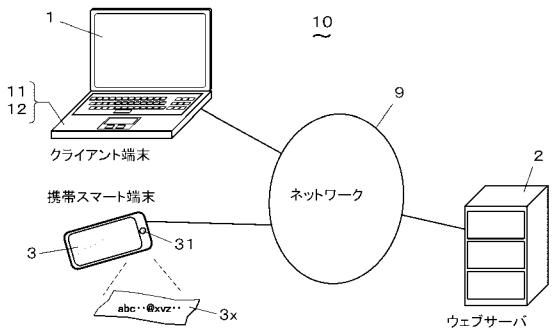
能と同等の機能を付加してもよい。この場合、携帯スマート端末３に指紋認証機能や顔認証機能などがあれば、アップリケーションを起動する前に生体認証される。携帯スマート端末３に指紋認証や顔認証などの機能がない場合は、携帯スマート端末３が持つ機能（カメラ、指紋リーダ、マイクなど）を使って生体認証を実現するための機能を、アプリケーションプログラム３０に付加すればよい。また、生体認証機能を用いるには、生体情報などの所要事項を、事前にウェブサーバ２に登録しておく必要がある。

【符号の説明】

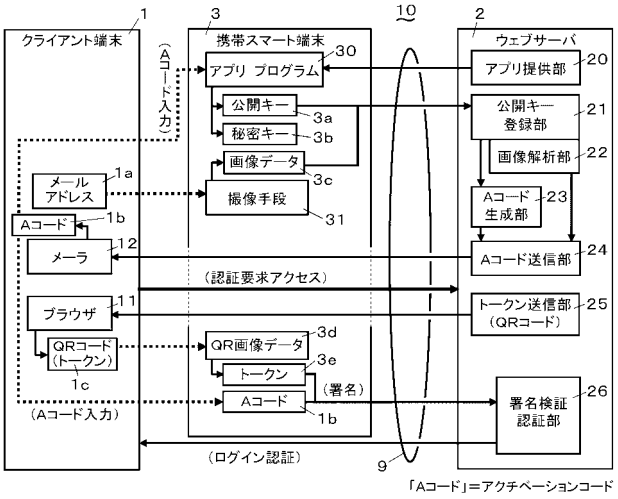
【００３７】

１　クライアント端末
１ａ　メールアドレス
１ｂ　Ａコード（アクティベーションコード）
１ｃ　ＱＲコード
１ｆ　住所
１０　相互認証システム
２　ウェブサーバ
３　携帯スマート端末
３ａ　公開キー
３ｂ　秘密キー
３ｃ　メールアドレスまたは居所情報を含む画像データ
３ｅ　トークン
３０　アプリケーションプログラム
３１　撮像手段
４　他のウェブサーバ
５　ユーザ

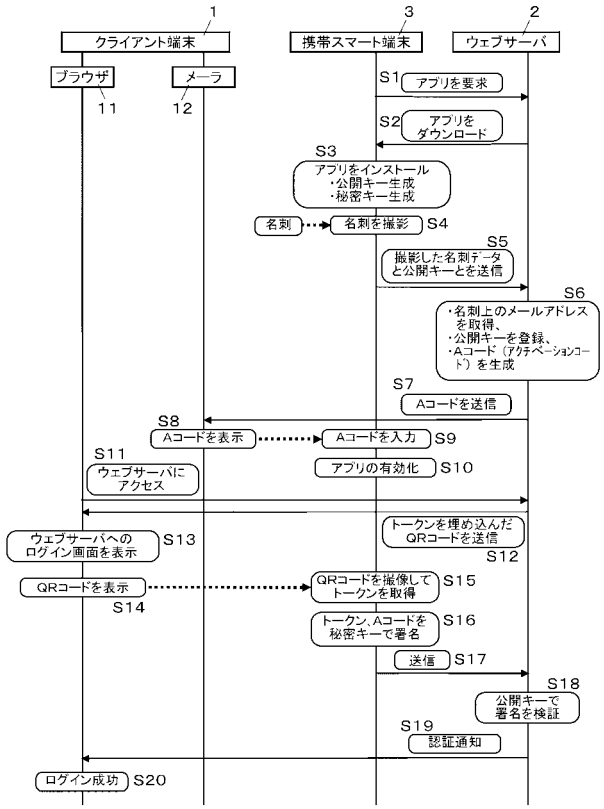
【図１】



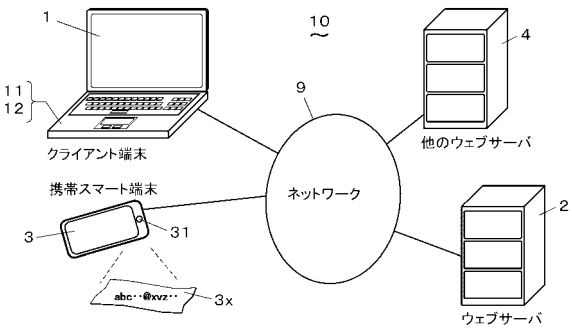
【図２】



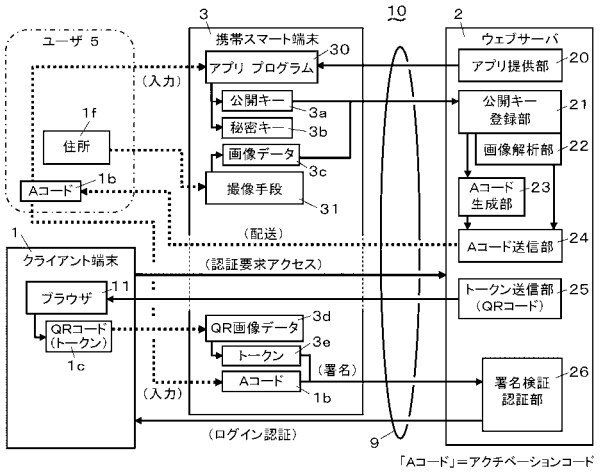
【図３】


クライアント端末
携帯スマート端末
ウェブサーバ
ブラウザ
メーラ
S1 アプリを要求
S2 アプリをダウンロード
S3 アプリをインストール ・公開キー生成 ・秘密キー生成
名刺
名刺を撮影 S4
S5 撮影した名刺データと公開キーとを送信
S6 ・名刺上のメールアドレスを取得、 ・公開キーを登録、 ・Aコード（アクチベーションコード）を生成
S7 Aコードを送信
S8 Aコードを表示
Aコードを入力 S9
アプリの有効化 S10
S11 ウェブサーバにアクセス
トークンを埋め込んだQRコードを送信 S12
ウェブサーバへのログイン画面を表示 S13
QRコードを表示 S14
QRコードを撮像してトークンを取得 S15
トークン、Aコードを秘密キーで署名 S16
送信 S17
S18 公開キーで署名を検証
S19 認証通知
ログイン成功 S20

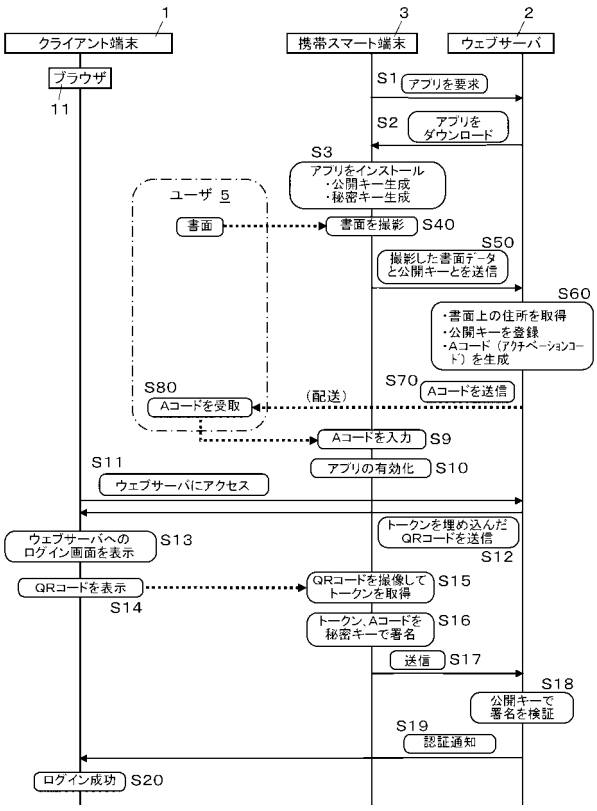
【図４】


クライアント端末
他のウェブサーバ
携帯スマート端末
ネットワーク
ウェブサーバ
abc・・@xyz・・
3x

【図５】


ユーザ 5
携帯スマート端末
ウェブサーバ
アプリ プログラム
アプリ提供部
公開キー
公開キー登録部
秘密キー
画像データ
画像解析部
撮像手段
Aコード生成部
住所
Aコード
クライアント端末
ブラウザ
Aコード送信部
トークン送信部（QRコード）
QRコード（トークン）
QR画像データ
トークン
Aコード
署名検証認証部
（入力）
（配送）
（認証要求アクセス）
（署名）
（ログイン認証）
「Aコード」＝アクチベーションコード

【図６】


クライアント端末
ブラウザ
携帯スマート端末
ウェブサーバ
S1 アプリを要求
S2 アプリをダウンロード
S3 アプリをインストール ・公開キー生成 ・秘密キー生成
ユーザ 5
書面
書面を撮影 S40
S50 撮影した書面データと公開キーとを送信
S60 ・書面上の住所を取得 ・公開キーを登録 ・Aコード（アクチベーションコード）を生成
S70 Aコードを送信
（配送）
S80 Aコードを受取
Aコードを入力 S9
アプリの有効化 S10
S11 ウェブサーバにアクセス
トークンを埋め込んだQRコードを送信 S12
ウェブサーバへのログイン画面を表示 S13
QRコードを表示 S14
QRコードを撮像してトークンを取得 S15
トークン、Aコードを秘密キーで署名 S16
送信 S17
S18 公開キーで署名を検証
S19 認証通知
ログイン成功 S20

フロントページの続き

(72)発明者　水間　乙允
和歌山県和歌山市紀三井寺８４９番地の３　株式会社サイバーリンクス内

Ｆターム(参考) 5J104 AA07　AA08　KA02　KA05　LA03　LA06　NA02　NA37　PA02