(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6650513号
(P6650513)

(45)発行日　令和2年2月19日(2020.2.19)　(24)登録日　令和2年1月22日(2020.1.22)

(51)Int.Cl.			F I		
H04L	9/32	(2006.01)	H04L	9/00	675B
H04L	9/14	(2006.01)	H04L	9/00	641
G09C	1/00	(2006.01)	G09C	1/00	640E
G06F	21/31	(2013.01)	G06F	21/31	
G06F	21/33	(2013.01)	G06F	21/33	

請求項の数 22　(全 34 頁)

(21)出願番号　特願2018-515096(P2018-515096)
(86)(22)出願日　平成28年9月13日(2016.9.13)
(65)公表番号　特表2018-532326(P2018-532326A)
(43)公表日　平成30年11月1日(2018.11.1)
(86)国際出願番号　PCT/CN2016/098815
(87)国際公開番号　WO2017/050147
(87)国際公開日　平成29年3月30日(2017.3.30)
審査請求日　平成30年4月12日(2018.4.12)
(31)優先権主張番号　201510604244.5
(32)優先日　平成27年9月21日(2015.9.21)
(33)優先権主張国・地域又は機関
中国(CN)

(73)特許権者　510330264
アリババ・グループ・ホールディング・リミテッド
ＡＬＩＢＡＢＡ　ＧＲＯＵＰ　ＨＯＬＤＩＮＧ　ＬＩＭＩＴＥＤ
英国領，ケイマン諸島，グランド・ケイマン，ジョージ・タウン，ワン・キャピタル・プレイス，フォース・フロア，ピー．オー．ボックス　８４７
(74)代理人　100099759
弁理士　青木　篤
(74)代理人　100123582
弁理士　三橋　真二
(74)代理人　100114018
弁理士　南山　知広

最終頁に続く

(54)【発明の名称】情報を登録および認証する方法およびデバイス

(57)【特許請求の範囲】

【請求項１】

各段階が、少なくともプロセッサとメモリとを有するコンピュータによって実行され、該メモリに記憶された各アプリケーションが、該コンピュータを手段として機能させる、情報登録方法であって、

基準情報を登録するための要求を認証サーバに対して送信する段階と、

前記認証サーバによりフィードバックされた第一認証情報を受信する段階と、

基準情報獲得要求を生成し、該基準情報獲得要求および前記第一認証情報をセキュリティ情報手段に対して送信し、且つ、前記セキュリティ情報手段が前記第一認証情報の認証を承認した後、前記セキュリティ情報手段により返信された署名済み基準情報と前記基準情報の身分識別子とを獲得する段階であって、前記署名済み基準情報は前記セキュリティ情報手段により第二認証情報を用いて署名されている、という段階と、

前記署名済み基準情報、前記基準情報の前記身分識別子、および、前記第一認証情報を前記認証サーバに対して送信することで、該認証サーバにより、該認証サーバが、前記第一認証情報の認証を承認し且つ前記署名済み基準情報に従い前記第二認証情報の認証を承認した後に、前記基準情報と前記基準情報の前記身分識別子とを登録させる段階と、

を備えて成る情報登録方法。

【請求項２】

前記認証サーバによりフィードバックされた第一認証情報を受信する前記段階は、

前記認証サーバにより送信されると共に、該認証サーバ自体の第一暗号鍵を用いて署名

された証明書を受信し、且つ、前記署名済み証明書を前記第一認証情報として用いる段階、
を備えて成る、請求項１に記載の方法。
【請求項３】
各段階が、少なくともプロセッサとメモリとを有するコンピュータによって実行され、該メモリに記憶された各アプリケーションが、該コンピュータを手段として機能させる、情報登録方法であって、
ビジネス手段により送信された第一認証情報および基準情報獲得要求を受信する段階と、
前記第一認証情報を認証し、且つ、認証が承認された後、前記ビジネス手段に対し、第二認証情報を用いて署名された基準情報を返信し且つ前記基準情報の身分識別子を返信することで、前記ビジネス手段により、前記署名済み基準情報と前記基準情報の前記身分識別子とを認証サーバに対して送信させ、且つ、前記認証サーバにより、該認証サーバが前記第一認証情報の認証を承認し且つ前記署名済み基準情報に従い前記第二認証情報の認証を承認した後、前記基準情報と前記基準情報の前記身分識別子とを登録させる段階と、
を備えて成る情報登録方法。
【請求項４】
第二認証情報を用いて署名された基準情報と前記基準情報の身分識別子とを前記ビジネス手段に対して返信する前記段階は、
ユーザにより入力された基準情報を受信する段階と、
前記第二認証情報を用いて前記基準情報に署名し、且つ、前記基準情報に対して該基準情報の身分識別子を決定する段階と、
前記署名済み基準情報と前記基準情報の前記身分識別子とを前記ビジネス手段に対して返信する段階と、
を備えて成る、請求項３に記載の方法。
【請求項５】
前記基準情報の前記身分識別子は前記基準情報の身分鍵情報を備えて成り、且つ、前記身分鍵情報は前記ユーザのアカウント情報に対して関連付けられる、請求項４に記載の方法。
【請求項６】
前記第一認証情報は前記認証サーバの署名済み証明書を備えて成り、且つ、
前記第一認証情報を認証する前記段階は、前記認証サーバの第一暗号鍵に対応する第一復号鍵を用いて、前記署名済み証明書を復号して認証する段階、を備えて成る、
請求項３に記載の方法。
【請求項７】
前記第二認証情報は、事前に前記認証サーバにより合意された第二鍵情報であり、前記第二鍵情報は第二暗号鍵および第二復号鍵を備えて成り、且つ、
前記第二認証情報を用いて前記基準情報に署名する前記段階は、事前に前記認証サーバにより合意された前記第二暗号鍵を用いて前記基準情報に署名する段階、を備えて成る、
請求項４に記載の方法。
【請求項８】
各段階が、少なくともプロセッサとメモリとを有するコンピュータによって実行され、該メモリに記憶された各アプリケーションが、該コンピュータを手段として機能させる、情報登録方法であって、
認証サーバにより、ビジネス手段により送信された基準情報を登録するための要求を受信する段階と、
基準情報を登録するための前記要求に従い、第一認証情報を生成し、且つ、該第一認証情報を前記ビジネス手段に対してフィードバックする段階と、
前記ビジネス手段により送信された、署名済み基準情報、前記基準情報の身分識別子、および、前記第一認証情報を受信する段階であって、前記署名済み基準情報は、セキュリ

ティ情報手段により第二認証情報を用いることにより署名されており且つ前記ビジネス手段に対して送信されているという段階と、
前記第一認証情報を認証し、且つ、前記署名済み基準情報に従い前記第二認証情報を認証する段階と、
前記第一認証情報および前記第二認証情報の認証を承認した後、前記基準情報と前記基準情報の前記身分識別子とを登録する段階と、
を備えて成る情報登録方法。
【請求項９】
基準情報を登録するための前記要求に従い第一認証情報を生成し、且つ、前記第一認証情報を前記ビジネス手段に対してフィードバックする前記段階は、
基準情報を登録するための前記要求に従い、前記認証サーバ自体の証明書を呼び出す段階と、
前記認証サーバ自体の第一暗号鍵を用い、前記第一認証情報として前記証明書に署名し、且つ、前記第一認証情報を前記ビジネス手段に対してフィードバックする段階と、
を備えて成る、請求項８に記載の方法。
【請求項１０】
前記第一認証情報を認証する前記段階は、
第一復号鍵を用いて前記第一認証情報を復号して認証する段階、
を備えて成る、請求項８に記載の方法。
【請求項１１】
前記第二認証情報は、事前に前記認証サーバおよび前記セキュリティ情報手段により合意された第二鍵情報を備えて成り、前記第二鍵情報は第二暗号鍵および第二復号鍵を備えて成り、前記署名済み基準情報は前記第二暗号鍵を用い前記セキュリティ情報手段により署名されており、且つ、
前記署名済み基準情報に従い前記第二認証情報を認証する前記段階は、事前に合意された前記第二鍵情報に従い、事前に前記セキュリティ情報手段により合意された前記第二復号鍵を用いて、前記第二認証情報を認証するために前記署名済み基準情報を復号する段階、を備えて成る、
請求項８に記載の方法。
【請求項１２】
少なくともプロセッサとメモリとを有する情報登録デバイスであって、該メモリに記憶された各アプリケーションが、該デバイスを手段として機能させる、情報登録デバイス、であって、
基準情報を登録するための要求を認証サーバに対して送信すべく構成された登録要求モジュールと、
前記認証サーバによりフィードバックされた第一認証情報を受信すべく構成された受信モジュールと、
基準情報獲得要求を生成し、該基準情報獲得要求および前記第一認証情報をセキュリティ情報手段に対して送信し、且つ、前記セキュリティ情報手段が前記第一認証情報の認証を承認した後、前記セキュリティ情報手段により返信された署名済み基準情報と前記基準情報の身分識別子とを獲得すべく構成された獲得モジュールであって、前記署名済み基準情報は前記セキュリティ情報手段により第二認証情報を用いて署名されている、という獲得モジュールと、
前記署名済み基準情報、前記基準情報の前記身分識別子、および、前記第一認証情報を前記認証サーバに対して送信することで、該認証サーバにより、該認証サーバが、前記第一認証情報の認証を承認し且つ前記署名済み基準情報に従い前記第二認証情報の認証を承認した後に、前記基準情報と前記基準情報の前記身分識別子とを登録させるべく構成された送信モジュールと、
を備えて成る情報登録デバイス。
【請求項１３】

前記受信モジュールは、前記認証サーバにより送信されると共に、該認証サーバ自体の第一暗号鍵を用いて署名された証明書を受信し、且つ、前記署名済み証明書を前記第一認証情報として用いるべく構成される、請求項１２に記載のデバイス。

【請求項１４】

少なくともプロセッサとメモリとを有する情報登録デバイスであって、該メモリに記憶された各アプリケーションが、該デバイスを手段として機能させる、情報登録デバイス、であって、

ビジネス手段により送信された第一認証情報および基準情報獲得要求を受信すべく構成された受信モジュールと、

前記第一認証情報を認証し、且つ、認証が承認された後、前記ビジネス手段に対し、第二認証情報を用いて署名された基準情報を返信し且つ前記基準情報の身分識別子を返信することで、前記ビジネス手段により、前記署名済み基準情報と前記基準情報の前記身分識別子とを認証サーバに対して送信させ、且つ、前記認証サーバにより、該認証サーバが前記第一認証情報の認証を承認し且つ前記署名済み基準情報に従い前記第二認証情報の認証を承認した後、前記基準情報と前記基準情報の前記身分識別子とを登録させるべく構成された署名モジュールと、

を備えて成る情報登録デバイス。

【請求項１５】

前記署名モジュールは、ユーザにより入力された基準情報を受信し、前記第二認証情報を用いて前記基準情報に署名し、前記基準情報に対して該基準情報の身分識別子を決定し、且つ、前記署名済み基準情報と前記基準情報の前記身分識別子とを前記ビジネス手段に対して返信すべく構成される、請求項１４に記載のデバイス。

【請求項１６】

前記基準情報の前記身分識別子は前記基準情報の身分鍵情報を備えて成り、且つ、前記身分鍵情報は前記ユーザのアカウント情報に対して関連付けられる、請求項１５に記載のデバイス。

【請求項１７】

前記第一認証情報は前記認証サーバの署名済み証明書を備えて成り、且つ、前記署名モジュールは、前記認証サーバの第一暗号鍵に対応する第一復号鍵を用いて、前記署名済み証明書を復号して認証すべく構成される、請求項１４に記載のデバイス。

【請求項１８】

前記第二認証情報は、事前に前記認証サーバにより合意された第二鍵情報であり、前記第二鍵情報は第二暗号鍵および第二復号鍵を備えて成り、且つ、

前記署名モジュールは、事前に前記認証サーバにより合意された前記第二暗号鍵を用いて前記基準情報に署名すべく構成される、

請求項１５に記載のデバイス。

【請求項１９】

少なくともプロセッサとメモリとを有する情報登録デバイスであって、該メモリに記憶された各アプリケーションが、該デバイスを手段として機能させる、情報登録デバイス、であって、

ビジネス手段により送信された基準情報を登録するための要求を受信すべく構成された登録要求受信モジュールと、

基準情報を登録するための前記要求に従い、第一認証情報を生成し、且つ、それを前記ビジネス手段に対してフィードバックすべく構成されたフィードバック・モジュールと、

前記ビジネス手段により送信された、署名済み基準情報、前記基準情報の身分識別子、および、前記第一認証情報を受信する登録情報受信モジュールであって、前記署名済み基準情報は、セキュリティ情報手段により第二認証情報を用いることにより署名されており且つ前記ビジネス手段に対して送信されているという登録情報受信モジュールと、

前記第一認証情報を認証し、且つ、前記署名済み基準情報に従い前記第二認証情報を認証すべく構成された認証モジュールと、

前記第一認証情報および前記第二認証情報の認証を通した後、前記基準情報と前記基準情報の前記身分識別子とを登録すべく構成された登録モジュールと、
を備えて成る情報登録デバイス。
【請求項２０】
前記フィードバック・モジュールは、基準情報を登録するための前記要求に従い、前記認証サーバ自体の証明書を呼び出し、前記認証サーバ自体の第一暗号鍵を用い、前記第一認証情報として前記証明書に署名し、且つ、それを前記ビジネス手段に対してフィードバックすべく構成される、請求項１９に記載のデバイス。
【請求項２１】
前記認証モジュールは、第一復号鍵を用いて前記第一認証情報を復号して認証すべく構成される、請求項１９に記載のデバイス。
【請求項２２】
前記第二認証情報は、事前に前記認証サーバおよび前記セキュリティ情報手段により合意された第二鍵情報を備えて成り、前記第二鍵情報は第二暗号鍵および第二復号鍵を備えて成り、前記署名済み基準情報は前記第二暗号鍵を用い前記セキュリティ情報手段により署名されており、且つ、
前記認証モジュールは、事前に合意された前記第二鍵情報に従い、事前に前記セキュリティ情報手段により合意された前記第二復号鍵を用いて、前記第二認証情報を認証するために前記署名済み基準情報を復号すべく構成される、
請求項１９に記載のデバイス。
【発明の詳細な説明】
【技術分野】
【０００１】
本出願は、コンピュータ技術の分野に関し、特に、情報の登録および認証のための方法およびデバイスに関する。
【背景技術】
【０００２】
情報技術の発展に伴い、ユーザは、（たとえば携帯電話、タブレット・コンピュータなどの）端末にインストールされた（たとえばソフトウェア開発業者、ウェブ・サイトなどの）サービス・プロバイダによるアプリケーション・プログラム（以下においては、“ビジネス・アプリケーション”）を介して種々のビジネス・サービスを便利に且つ迅速に受信し得る。ビジネス・アプリケーションにおいて提供されるビジネス・サービスに関し、支払サービス、転送サービスなどの如き或る種類のビジネス・サービスは、比較的に高いセキュリティ・レベルを有している。比較的に高いセキュリティ・レベルを有するビジネス・サービスは通常、ユーザに対し、（たとえば、パスワード、バイオメトリック情報などの）対応するセキュリティ情報を提供することを要求すると共に、該ビジネス・サービスは、ユーザにより提供されたセキュリティ情報が認証された後においてのみ、完了され得る。
【０００３】
ユーザがセキュリティ情報を提供することを要求する前記ビジネス・サービスに対し、ユーザのセキュリティ情報は典型的に、ユーザにより後続的に入力されるセキュリティ情報との比較のために、ユーザが初めて前記ビジネス・サービスを使用する前に、基準情報として獲得される（該基準情報は、後続的な認証プロセスにおいて認証基準として使用される）。ユーザのセキュリティ情報を獲得する過程において、ビジネス・アプリケーションは、端末におけるセキュリティ情報アプリケーション（たとえば、ユーザにより入力されたバイオメトリック情報の収集および記憶を取り扱うバイオインフォマティック管理アプリケーションであり、該バイオインフォマティック管理アプリケーションは、端末製造者により端末にインストールされている）を使用してユーザのセキュリティ情報を獲得することが必要である。
【０００４】

ビジネス・アプリケーションとセキュリティ情報アプリケーションとの間におけるアプリケーション起動および情報伝送を促進するために、先行技術における（たとえば Android M システムなどの）端末システムは、リッチ実行環境（REE）と称されるアーキテクチャにおいてセキュリティ情報アプリケーションを動作させている。REE は、REE において動作しているセキュリティ情報アプリケーションが、種々のビジネス・サービスにより更に便利に且つ迅速に起動され得ると共に、全てのビジネス・アプリケーションにより要求された情報を更に便利に且つ迅速に伝送し得る如く、多くの起動サポートを保有している。

【０００５】

但し、REE は安全な環境ではない。セキュリティ情報アプリケーションとビジネス・アプリケーションとの間における情報伝送の過程において、セキュリティ情報は、伝送の間において不正操作者により傍受かつ改竄される傾向がある。特に、基準情報に対しては、該基準情報が真なのか偽なのかを確認することが不可能であり、と言うのも、サービス・プロバイダは、ユーザにより提供された該基準情報を先行して保存してはいないからである。基準情報が伝送の間に一旦改竄されたとしても、サービス・プロバイダは依然として、改竄された基準情報を、後続的な認証プロセスにおける認証基準として受信する。故に明らかに、不正操作者は、前記ユーザの名において種々のビジネス・サービスを獲得する。

【発明の概要】

【０００６】

本出願の各実施形態は、セキュリティ情報が登録のために使用されるときにセキュリティが不十分であるという先行技術の問題を解決する、情報の登録および認証のための方法およびデバイスを提供する。

【０００７】

本出願の実施形態により提供される情報登録方法は、基準情報を登録するための要求を認証サーバに対して送信する段階と、前記認証サーバによりフィードバックされた第一認証情報を受信する段階と、基準情報獲得要求を生成し、該基準情報獲得要求および前記第一認証情報をセキュリティ情報アプリケーションに対して送信し、且つ、前記セキュリティ情報アプリケーションが前記第一認証情報の認証を承認した後、前記セキュリティ情報アプリケーションにより返信された署名済み基準情報と前記基準情報の身分識別子とを獲得する段階であって、前記署名済み基準情報は前記セキュリティ情報アプリケーションにより第二認証情報を用いて署名されている、という段階と、前記署名済み基準情報、前記基準情報の前記身分識別子、および、前記第一認証情報を前記認証サーバに対して送信することで、該認証サーバにより、該認証サーバが、前記第一認証情報の認証を承認し且つ前記署名済み基準情報に従い前記第二認証情報の認証を承認した後に、前記基準情報と前記基準情報の前記身分識別子とを登録させる段階と、を備えて成る。

【０００８】

本出願の実施形態により更に提供される情報登録方法は、ビジネス・アプリケーションにより送信された第一認証情報および基準情報獲得要求を受信する段階と、前記第一認証情報を認証し、且つ、認証が承認された後、前記ビジネス・アプリケーションに対し、第二認証情報を用いて署名された基準情報を返信し且つ前記基準情報の身分識別子を返信することで、前記ビジネス・アプリケーションにより、前記署名済み基準情報と前記基準情報の前記身分識別子とを認証サーバに対して送信させ、且つ、前記認証サーバにより、該認証サーバが前記第一認証情報の認証を承認し且つ前記署名済み基準情報に従い前記第二認証情報の認証を承認した後、前記基準情報と前記基準情報の前記身分識別子とを登録させる段階と、を備えて成る。

【０００９】

本出願の実施形態により更に提供される情報登録方法は、認証サーバにより、ビジネス・アプリケーションにより送信された基準情報を登録するための要求を受信する段階と、基準情報を登録するための前記要求に従い、第一認証情報を生成し、且つ、該第一認証情

報を前記ビジネス・アプリケーションに対してフィードバックする段階と、前記ビジネス・アプリケーションにより送信された、署名済み基準情報、前記基準情報の身分識別子、および、前記第一認証情報を受信する段階であって、前記署名済み基準情報は、セキュリティ情報アプリケーションにより前記第二認証情報を用いることにより署名されており且つ前記ビジネス・アプリケーションに対して送信されているという段階と、前記第一認証情報を認証し、且つ、前記署名済み基準情報に従い前記第二認証情報を認証する段階と、前記第一認証情報および前記第二認証情報の認証を承認した後、前記基準情報と前記基準情報の前記身分識別子とを登録する段階と、を備えて成る。

【００１０】

本出願の実施形態により更に提供される情報認証方法は、認証対象情報に対する照合要求を認証サーバに対して送信する段階と、前記認証サーバによりフィードバックされた第一認証情報を受信する段階と、認証対象情報獲得要求を生成し、該認証対象情報獲得要求および前記第一認証情報をセキュリティ情報アプリケーションに対して送信し、且つ、前記セキュリティ情報アプリケーションが前記第一認証情報の認証を承認した後、前記セキュリティ情報アプリケーションにより返信された認証対象情報と、該認証対象情報の認証対象身分識別子と、を獲得する段階と、前記認証対象情報、前記認証対象身分識別子、および、前記第一認証情報を前記認証サーバに対して送信することで、該認証サーバにより、前記第一認証情報、前記認証対象身分識別子、および、前記認証対象情報を認証させ、認証結果を生成させ、且つ、前記認証結果を前記ビジネス・アプリケーションに対してフィードバックさせる段階と、を備えて成る。

【００１１】

本出願の実施形態により更に提供される情報認証方法は、ビジネス・アプリケーションにより送信され且つ第一認証情報を担持する認証対象情報獲得要求を受信する段階と、前記第一認証情報を認証し、且つ、認証が承認された後、前記認証対象情報と該認証対象情報の身分識別子とを前記ビジネス・アプリケーションを介して認証サーバに対して送信することで、該認証サーバにより、前記第一認証情報、前記認証対象身分識別子、および、前記認証対象情報を認証させ、認証結果を生成させ、且つ、該認証結果を前記ビジネス・アプリケーションに対してフィードバックさせる段階と、を備えて成る。

【００１２】

本出願の実施形態により更に提供される情報認証方法は、認証サーバにより、ビジネス・アプリケーションにより送信された認証対象情報に対する照合要求を受信する段階と、前記照合要求に従い、第一認証情報を生成し、且つ、該第一認証情報を前記ビジネス・アプリケーションに対してフィードバックする段階と、前記ビジネス・アプリケーションにより送信された、前記認証対象情報、前記認証対象情報の認証対象身分識別子、および、前記第一認証情報を受信する段階と、前記第一認証情報、前記認証対象身分識別子、および、前記認証対象情報を夫々認証して、認証結果を生成し、且つ、該認証結果を前記ビジネス・アプリケーションに対してフィードバックする段階と、を備えて成る。

【００１３】

本出願の実施形態により更に提供される情報登録デバイスは、基準情報を登録するための要求を認証サーバに対して送信すべく構成された登録要求モジュールと、前記認証サーバによりフィードバックされた第一認証情報を受信すべく構成された受信モジュールと、基準情報獲得要求を生成し、該基準情報獲得要求および前記第一認証情報をセキュリティ情報アプリケーションに対して送信し、且つ、前記セキュリティ情報アプリケーションが前記第一認証情報の認証を承認した後、前記セキュリティ情報アプリケーションにより返信された署名済み基準情報と前記基準情報の身分識別子とを獲得すべく構成された獲得モジュールであって、前記署名済み基準情報は前記セキュリティ情報アプリケーションにより第二認証情報を用いて署名されている、という獲得モジュールと、前記署名済み基準情報、前記基準情報の前記身分識別子、および、前記第一認証情報を前記認証サーバに対して送信することで、該認証サーバにより、該認証サーバが、前記第一認証情報の認証を承認し且つ前記署名済み基準情報に従い前記第二認証情報の認証を承認した後に、前記基準

情報と前記基準情報の前記身分識別子とを登録させるべく構成された送信モジュールと、を備えて成る。

【００１４】

本出願の実施形態により更に提供される情報登録デバイスは、ビジネス・アプリケーションにより送信された第一認証情報および基準情報獲得要求を受信すべく構成された受信モジュールと、前記第一認証情報を認証し、且つ、認証が承認された後、前記ビジネス・アプリケーションに対し、第二認証情報を用いて署名された基準情報を返信し且つ前記基準情報の身分識別子を返信することで、前記ビジネス・アプリケーションにより、前記署名済み基準情報と前記基準情報の前記身分識別子とを認証サーバに対して送信させ、且つ、前記認証サーバにより、該認証サーバが前記第一認証情報の認証を承認し且つ前記署名済み基準情報に従い前記第二認証情報の認証を承認した後、前記基準情報と前記基準情報の前記身分識別子とを登録させるべく構成された署名モジュールと、を備えて成る。

【００１５】

本出願の実施形態により更に提供される情報登録デバイスは、ビジネス・アプリケーションにより送信された基準情報を登録するための要求を受信すべく構成された登録要求受信モジュールと、基準情報を登録するための前記要求に従い、第一認証情報を生成し、且つ、それを前記ビジネス・アプリケーションに対してフィードバックすべく構成されたフィードバック・モジュールと、前記ビジネス・アプリケーションにより送信された、署名済み基準情報、前記基準情報の身分識別子、および、前記第一認証情報を受信する登録情報受信モジュールであって、前記署名済み基準情報は、セキュリティ情報アプリケーションにより前記第二認証情報を用いることにより署名されており且つ前記ビジネス・アプリケーションに対して送信されているという登録情報受信モジュールと、前記第一認証情報を認証し、且つ、前記署名済み基準情報に従い前記第二認証情報を認証すべく構成された認証モジュールと、前記第一認証情報および前記第二認証情報の認証が両方とも承認された後、前記基準情報と前記基準情報の前記身分識別子とを登録すべく構成された登録モジュールと、を備えて成る。

【００１６】

本出願の実施形態により更に提供される情報認証デバイスは、認証対象情報に対する照合要求を認証サーバに対して送信すべく構成された登録要求モジュールと、前記認証サーバによりフィードバックされた第一認証情報を受信すべく構成された受信モジュールと、認証対象情報獲得要求を生成し、該認証対象情報獲得要求および前記第一認証情報をセキュリティ情報アプリケーションに対して送信し、且つ、前記セキュリティ情報アプリケーションが前記第一認証情報の認証を承認した後、前記セキュリティ情報アプリケーションにより返信された認証対象情報と、該認証対象情報の認証対象身分識別子と、を獲得すべく構成された獲得モジュールと、前記認証対象情報、前記認証対象身分識別子、および、前記第一認証情報を前記認証サーバに対して送信することで、該認証サーバにより、前記第一認証情報、前記認証対象身分識別子、および、前記認証対象情報を認証させ、認証結果を生成させ、且つ、前記認証結果を前記ビジネス・アプリケーションに対してフィードバックさせるべく構成された送信モジュールと、を備えて成る。

【００１７】

本出願の実施形態により更に提供される情報認証デバイスは、ビジネス・アプリケーションにより送信され且つ第一認証情報を担持する認証対象情報獲得要求を受信すべく構成された受信モジュールと、前記第一認証情報を認証し、且つ、認証が承認された後、前記認証対象情報と該認証対象情報の身分識別子とを前記ビジネス・アプリケーションを介して認証サーバに対して送信することで、該認証サーバにより、前記第一認証情報、前記認証対象身分識別子、および、前記認証対象情報を認証させ、認証結果を生成させ、且つ、該認証結果を前記ビジネス・アプリケーションに対してフィードバックさせるべく構成された署名モジュールと、を備えて成る。

【００１８】

本出願の実施形態により更に提供される情報認証デバイスは、ビジネス・アプリケーシ

ョンにより送信された認証対象情報に対する照合要求を受信すべく構成された認証要求受信モジュールと、前記照合要求に従い、第一認証情報を生成し、且つ、それを前記ビジネス・アプリケーションに対してフィードバックすべく構成されたフィードバック・モジュールと、前記ビジネス・アプリケーションにより送信された、前記認証対象情報、前記認証対象情報の認証対象身分識別子、および、前記第一認証情報を受信すべく構成された認証情報受信モジュールと、前記第一認証情報、前記認証対象身分識別子、および、前記認証対象情報を夫々認証して、認証結果を生成し、且つ、認証結果を前記ビジネス・アプリケーションに対してフィードバックすべく構成された認証モジュールと、を備えて成る。

【００１９】

本出願の実施形態は、情報を登録および認証する方法およびデバイスを提供する。ユーザが、ビジネス・サービスを使用している間に、基準情報を登録することを必要とするとき、ビジネス・アプリケーションは、基準情報を認証サーバに対して登録するための要求を開始すると共に、認証サーバによりフィードバックされた第一認証情報を受信する。その後、ビジネス・アプリケーションは、基準情報獲得要求を生成すると共に、該基準情報獲得要求および前記第一認証情報をセキュリティ情報アプリケーションに対して送信する。セキュリティ情報アプリケーションによる第一認証情報の認証が承認された後、該セキュリティ情報アプリケーションは、それ自体の第二認証情報を使用して基準情報に署名し、基準情報の身分識別子を決定し、且つ、その後に、署名済み基準情報と基準情報の身分識別子とを、ビジネス・アプリケーションに対してフィードバックする。結果として、ビジネス・アプリケーションは、セキュリティ情報アプリケーションからのフィードバックと前記第一認証情報とを認証サーバに対して送信することで、認証の後で、基準情報、および、それの身分識別子を認証サーバに対して登録させる。前記方法からは、認証サーバの識別子としての第一認証情報によれば、セキュリティ情報アプリケーションが基準情報登録者の身分を決定することが可能とされ、認証サーバに対する第一認証情報の返信によれば、該認証サーバは、前記情報が伝送の間に改竄されたか否かを決定し得る一方、認証サーバに対する署名済み基準情報の返信によれば、該認証サーバは、基準情報が端末におけるセキュリティ情報アプリケーションにより提供されたか否かを決定し得ることが理解され得る。斯かる方法によれば効果的に、認証サーバは、伝送の間に改竄された基準情報を正確に確認し得ることが確実とされ得ることで、基準情報登録の安全性が効果的に向上され得る。

【図面の簡単な説明】

【００２０】

本明細書における添付図面は、本出願の更なる理解のために提供されると共に、本出願の一部を構成する。本出願の代表的実施形態およびその説明は、本出願を説明するために使用されるが、本出願に対する不適切な制限を構成するものでない。

【００２１】

【図１】図１乃至図３は、本出願の実施形態に係る情報登録方法を示す図である。

【図２】図１乃至図３は、本出願の実施形態に係る情報登録方法を示す図である。

【図３】図１乃至図３は、本出願の実施形態に係る情報登録方法を示す図である。

【図４】本出願の実施形態に係る、代表的な応用状況における情報登録方法を示す図である。

【図５】図５乃至図７は、本出願の実施形態に係る情報認証方法を示す図である。

【図６】図５乃至図７は、本出願の実施形態に係る情報認証方法を示す図である。

【図７】図５乃至図７は、本出願の実施形態に係る情報認証方法を示す図である。

【図８】本出願の実施形態に係る、代表的な応用状況における情報認証プロセスを示す図である。

【図９】図９乃至図１１は、本出願の実施形態に係る情報登録デバイスの構造的概略図である。

【図１０】図９乃至図１１は、本出願の実施形態に係る情報登録デバイスの構造的概略図である。

【図１１】図９乃至図１１は、本出願の実施形態に係る情報登録デバイスの構造的概略図である。
【図１２】図１２乃至図１４は、本出願の実施形態に係る情報認証デバイスの構造的概略図である。
【図１３】図１２乃至図１４は、本出願の実施形態に係る情報認証デバイスの構造的概略図である。
【図１４】図１２乃至図１４は、本出願の実施形態に係る情報認証デバイスの構造的概略図である。
【発明を実施するための形態】
【００２２】
本出願の目的、技術的解決策および利点を更に明確にするために、本出願の技術的解決策は以下において、本出願の好適実施形態および添付図面を参照して更に明確に且つ完全に記述される。明らかに、記述される実施形態は、本出願の実施形態の全てではなく、幾つかにすぎない。本出願の実施形態に基づき、且つ、発明的な努力なしで当業者により実現され得る全ての他の実施形態は、本出願の有効範囲内に包含されるものとする。
【００２３】
上述された如く、サービス・プロバイダが初めて基準情報を受信したとき、該基準情報が伝送の間に改竄されたか否かを正確に決定することはできない、と言うのも、該プロバイダは、前記基準情報に関するセキュリティ情報を先行しては保存していないからである。しかし、サービス・プロバイダおよび端末が、事前に一連の認証情報に合意すると共に、該認証情報を使用して前記基準情報を認証するならば、前記基準情報が伝送の間に改竄されたか否かを確認することが可能である。このことに基づき、本出願においては、以下の情報登録および認証方法が提供される。
【００２４】
本出願の実施形態に従い、情報登録方法が提供されると共に、図１に示された如く、該方法は以下の各段階を備えて成る：
【００２５】
Ｓ１０１：基準情報を登録するための要求を認証サーバに対して送信する段階。
【００２６】
代表的な応用状況において、ユーザが、ビジネス・アプリケーションにおいて提供される比較的に高いセキュリティ・レベルのビジネス・サービス（たとえば、指紋式支払サービス）を使用するとき、該ユーザは典型的に、（たとえば指紋情報などの）対応するセキュリティ情報を提供することが要求される。特に、ユーザがビジネス・サービスを初めて使用するとき、該ユーザは典型的に、ビジネス・サービスの後続的な使用時に該ユーザにより入力されるセキュリティ情報に対する比較および照合のために、基準情報としてセキュリティ情報を入力することを要求される。
【００２７】
換言すると、ユーザが初めてビジネス・サービスを使用するとき、該ユーザにより提供される基準情報を、ビジネス・アプリケーションを介して、対応する認証サービスに登録することが必要である。故に、本出願の実施形態の前記段階において、端末の内部で動作するビジネス・アプリケーションは、基準情報を登録するための要求を認証サーバに対して送信し得る。
【００２８】
此処で、本出願において示される端末としては、限定的なものとしてでなく、携帯電話、タブレット・コンピュータ、および、スマート・ウォッチの如き移動端末が挙げられると共に、幾つかの状況展開においては、コンピュータ端末でもあり得る。前記認証サーバは、サービス・プロバイダのバックエンド・サービス・システムにおけるセキュリティ認証のためのサーバ、または、セキュリティ認証のための専用のサード・パーティのサーバであり得る。当然乍ら、これらのものは本出願に対する制限を構成するものでない。
【００２９】

Ｓ１０２：認証サーバによりフィードバックされた第一認証情報を受信する段階。
【００３０】
前記第一認証情報は、基準情報を登録するための要求を送信するビジネス・アプリケーションに対し、認証サーバによりフィードバックされた識別情報であり、且つ、該認証サーバの身分を表すべく使用される。本出願の実施形態の状況展開において、第一認証情報は、認証サービスの証明書を構成し得る。
【００３１】
Ｓ１０３：基準情報獲得要求を生成し、該基準情報獲得要求および第一認証情報をセキュリティ情報アプリケーションに対して送信する段階であって、該セキュリティ情報アプリケーションが前記第一認証情報の認証を承認した後に、セキュリティ情報アプリケーションにより返信された、署名済み基準情報、および、基準情報の身分識別子を獲得するという段階。
【００３２】
此処で、署名済み基準情報は、セキュリティ情報アプリケーションにより、第二認証情報を用いて署名されている。
【００３３】
認証サーバによりフィードバックされた第一認証情報を受信すると同時に、ビジネス・アプリケーションは、端末におけるセキュリティ情報アプリケーションに対し、登録のために必要な基準情報を提供することを要求する基準情報獲得要求を生成する。
【００３４】
本出願におけるセキュリティ情報アプリケーションは、前記端末において動作しているローカル・アプリケーションであり、且つ、ビジネス・サービスに対して必要な（基準情報を含む）セキュリティ情報を前記ビジネス・アプリケーションに対して提供すべく使用されることを銘記すべきである。但し、セキュリティ情報は、ユーザ自身の鍵情報である。前記セキュリティ情報アプリケーションに対してユーザのセキュリティ情報を不正操作者が要求することを阻止するために、セキュリティ情報アプリケーションは、基準情報を使用する者の身分を認証する。このことに基づき、ビジネス・アプリケーションがセキュリティ情報アプリケーションに対して基準情報獲得要求を送信するとき、ビジネス・アプリケーションは前記第一認証情報もセキュリティ情報アプリケーションに対して送信する。すると、セキュリティ情報アプリケーションは、第一認証情報を認証して認証サーバの身分を決定し、且つ、該セキュリティ情報アプリケーションは、該アプリケーションにより前記第一認証情報の認証が承認された後でのみ、前記基準情報を提供する。
【００３５】
セキュリティ情報アプリケーションにより提供された前記基準情報が、実際の適用において伝送の間に改竄され得ることを考慮すると、セキュリティ情報アプリケーションは、前記基準情報は端末における該セキュリティ情報アプリケーションにより送信されることを表すために、本出願において、前記基準情報をフィードバックする前に、該基準情報に対する署名操作を実施する。一方、基準情報は前記ユーザにより提供されることも考慮すると、基準情報が前記ユーザにより提供されたことを表すために、該基準情報の身分識別子が決定され得る。その故に、セキュリティ情報アプリケーションによりビジネス・アプリケーションに対してフィードバックされた基準情報に対しては二つの識別子があり、それらは夫々、前記基準情報は前記端末におけるセキュリティ情報アプリケーションにより送信されたこと、および、前記基準情報は前記ユーザにより提供されたことを表すべく使用される。
【００３６】
一例において、本出願におけるセキュリティ情報アプリケーションは、前記第二認証情報を使用して前記基準情報に署名することで、該基準情報は該セキュリティ情報アプリケーションにより送信されたことを表す。本出願において、第二認証情報は、本明細書中で詳細には限定されないが、認証サーバと、端末におけるセキュリティ情報アプリケーション（または、該端末自体）と、の間で事前に合意された第二鍵情報であり得る。前記基準

情報の身分識別子もまた、セキュリティ情報アプリケーションにより決定され得る。本出願において、基準情報の身分識別子は、該基準情報の身分鍵情報を構成し、且つ、該身分鍵情報は典型的には、ユーザのアカウント情報に対して関連付けられる。換言すると、ひとつのアカウント情報に対しては一意的に一対の身分鍵情報が対応し、このことは、前記基準情報が前記ユーザに属することも表し得る。当然乍ら、本明細書中にては特定の限定は為されない。

【００３７】

Ｓ１０４：署名済み基準情報、基準情報の身分識別子、および、第一認証情報を、認証サーバに対して送信することで、該認証サーバが、第一認証情報の認証を承認し、且つ、署名済み基準情報に従い第二認証情報の認証を承認した後で、該認証サーバにより基準情報および基準情報の身分識別子を登録させる段階。

【００３８】

セキュリティ情報アプリケーションによる前記フィードバックの受信と同時に、ビジネス・アプリケーションは、セキュリティ情報アプリケーションによりフィードバックされた署名済み基準情報と基準情報の身分識別子とを、認証サーバにより送信された第一認証情報と共に、認証および登録のために認証サーバに対して送信する。

【００３９】

ビジネス・アプリケーションにより送信された前記情報の受信と同時に、認証サーバは、受信した情報に対する認証を実施する。認証が承認されたなら、それは、セキュリティ情報アプリケーションにより送信された基準情報が伝送の間に改竄されていないことを表し、その後、認証サーバは、基準情報、および、それの身分識別子を登録し得る。登録された基準情報、および、それの身分識別子は、その後、ユーザにより後続的に提供されるセキュリティ情報の認証および確認のために使用され得る。

【００４０】

上記の各段階によると、ユーザが、ビジネス・サービスを使用している間に、基準情報を登録することを必要とするとき、ビジネス・アプリケーションは、基準情報を認証サーバに対して登録するための要求を開始すると共に、認証サーバによりフィードバックされた第一認証情報を受信する。その後、ビジネス・アプリケーションは、基準情報獲得要求を生成すると共に、該基準情報獲得要求および前記第一認証情報をセキュリティ情報アプリケーションに対して送信する。セキュリティ情報アプリケーションによる第一認証情報の認証が承認された後、該セキュリティ情報アプリケーションは、それ自体の第二認証情報を使用して基準情報に署名し、基準情報の身分識別子を決定し、且つ、その後に、署名済み基準情報と基準情報の身分識別子とを、ビジネス・アプリケーションに対してフィードバックする。結果として、ビジネス・アプリケーションは、セキュリティ情報アプリケーションからのフィードバックと前記第一認証情報とを認証サーバに対して送信することで、認証の後で、基準情報、および、それの身分識別子を認証サーバに対して登録させる。前記方法からは、認証サーバの識別子としての第一認証情報によれば、セキュリティ情報アプリケーションが基準情報登録者の身分を決定することが可能とされ、認証サーバに対する第一認証情報の返信によれば、該認証サーバは、前記情報が伝送の間に改竄されたか否かを決定し得る一方、認証サーバに対する署名済み基準情報の返信によれば、該認証サーバは、基準情報が端末におけるセキュリティ情報アプリケーションにより提供されたか否かを決定し得ることが理解され得る。斯かる方法によれば効果的に、認証サーバは、伝送の間に改竄された基準情報を正確に確認し得ることが確実とされ得ることで、基準情報登録の安全性が効果的に向上され得る。

【００４１】

前記第一認証情報に関し、該第一認証情報は、認証サーバの識別子であると共に、認証サーバの身分を確認すべく使用される。たとえば、認証サーバ自体の証明書が、第一認証情報として使用され得る。伝送の間におけるセキュリティを考慮すると、認証サーバは、それ自体の鍵情報を使用して、その証明書に対する署名操作を実施し得る。その場合、本出願の実施形態の選択的様式として、認証サーバによりフィードバックされた第一認証情

報を受信する前記Ｓ１０２の段階は、認証サーバにより送信されると共に認証サーバ自体の第一暗号鍵を用いて署名された証明書を受信する段階、および、署名済み証明書を第一認証情報として使用する段階を備えて成る。

【００４２】

更に、代表的な用途の幾つかの状況展開においては、認証サーバからビジネス・アプリケーションに対してフィードバックされる第一認証情報中に、チャレンジ・コードが更に含まれる。ビジネス・アプリケーションが認証サーバに対して要求を送信した後、該認証サーバは、ビジネス・アプリケーションに対してフィードバックされる第一認証情報中に担持される一意的なチャレンジ・コードを生成する。ひとつのチャレンジ・コードは、一回のビジネス要求にのみ対応することが考えられ得る。チャレンジ・コードを採用すると、リプレー・アタックを阻止し得る。

【００４３】

上記の内容は、端末におけるビジネス・アプリケーションの角度から記述されている。基準情報を提供するセキュリティ情報アプリケーションに関しては、本出願の実施形態において情報登録方法が更に提供されると共に、図２に示された如く、そのプロセスは以下の各段階を備えて成る：

【００４４】

Ｓ２０１：ビジネス・アプリケーションにより送信された第一認証情報および基準情報獲得要求を受信する段階。

【００４５】

本実施形態における第一認証情報および基準情報獲得要求は、上述されたものと同一であり、本明細書中では繰り返されない。

【００４６】

Ｓ２０２：第一認証情報を認証する段階であって、認証が承認された後、ビジネス・アプリケーションに対し、第二認証情報により署名された基準情報を返信し且つ基準情報の身分識別子を返信することで、署名済み基準情報と基準情報の身分識別子とをビジネス・アプリケーションにより認証サーバに対して送信させることで、認証サーバが、第一認証情報の認証を承認し且つ署名済み基準情報に従い第二認証情報の認証を承認した後で、該認証サーバにより基準情報および基準情報の身分識別子を登録させる段階。

【００４７】

ビジネス・アプリケーションにより送信された第一認証情報および基準情報獲得要求を受信すると同時に、セキュリティ情報アプリケーションは、まず、第一認証情報を認証して、基準情報登録者の身分を決定する。セキュリティ情報アプリケーションが認証サーバの身分を決定した後においてのみ、該セキュリティ情報アプリケーションは、ユーザにより提供された基準情報に署名し、基準情報の身分識別子を決定し、且つ、署名済み基準情報と基準情報の身分識別子とを、ビジネス・アプリケーションに対してフィードバックし得る。その後、ビジネス・アプリケーションは、セキュリティ情報アプリケーションによりフィードバックされた一連の情報を、第一認証情報と共に、認証サーバによる後続的な認証のために該認証サーバに対して送信する。更に、認証が承認されたとき、認証サーバは、基準情報と基準情報の身分識別子とを登録する。此処における内容は、先の方法におけるプロセスと同一であり、本明細書中では繰り返されない。

【００４８】

前記の各段階によると、認証サーバの身分は、該認証サーバにより提供された第一認証情報を以て確認され得ると共に、セキュリティ情報アプリケーションによる第一認証情報の認証によれば、不正操作者がセキュリティ情報アプリケーションから基準情報を獲得することが阻止され得る。セキュリティ情報アプリケーションが、ユーザにより提供された基準情報に署名する様式は、基準情報が該セキュリティ情報アプリケーションにより送信されたことを表すべく使用される一方、基準情報の身分識別子の決定は、該基準情報がユーザにより提供されたことを表すべく使用される。明らかに、セキュリティ情報アプリケーションによりビジネス・アプリケーションに対してフィードバックされた基準情報は、

二つの識別子を備えて成る。もし、基準情報が伝送の間に改竄されたなら、基準情報の二つの識別子は、いずれも変更される。斯かる方法は、基準情報が伝送の間に改竄されたか否かを効果的に反映することから、最終的に登録の間において認証サーバの安全性を確実とし得る。

【００４９】

第二認証情報を用いて署名された基準情報、および、該基準情報の身分識別子をビジネス・アプリケーションに対して返信する段階は、ユーザにより入力された基準情報を受信する段階、第二認証情報を用いて基準情報に署名する段階、基準情報に対して該基準情報の身分識別子を決定する段階、および、署名済み基準情報と基準情報の身分識別子とを、ビジネス・アプリケーションに対して返信する段階を備えて成る。

【００５０】

上述された如く、本出願における基準情報の身分識別子は、基準情報の身分鍵情報を備えて成り得ると共に、該身分鍵情報は典型的に、ユーザのアカウント情報に関連付けられる。伝送の間における身分鍵情報の安全性を確実とするために、セキュリティ情報アプリケーションは、本出願の実施形態の選択的様式において、第二認証情報を使用して身分鍵情報（すなわち、基準情報の身分識別子）にも署名し得る。当然乍ら、このことは本出願に対する制限を構成するものでない。

【００５１】

同様に、上述された如く、第一認証情報は、認証サーバの身分を表し得る一方、本出願のひとつの様式において、第一認証情報は認証サーバ自体の証明書を構成する。斯かる場合、第一認証情報の認証は、認証サーバの第一暗号鍵に対応する第一復号鍵を用いて、署名済み証明書を復号して認証する段階を備えて成る。

【００５２】

第二認証情報に関し、本出願の実施形態に係るひとつの方法において、該第二認証情報は、事前に認証サーバにより合意された第二鍵情報を備えて成り、その場合、第二鍵情報は、第二暗号鍵および第二復号鍵を備えて成る。斯かる状況展開において、第二認証情報を用いて基準情報に署名する段階は、事前に認証サーバにより合意された第二暗号鍵を用いて基準情報に署名する段階を備えて成る。

【００５３】

基準情報の身分識別子が、該基準情報の身分鍵情報を備えて成る場合、前記第二認証情報は、身分鍵情報に署名すべく使用され得る。此処における内容は、前記様式の内容と同様であり、本明細書中では繰り返されない。

【００５４】

前記の内容は、端末において動作しているセキュリティ情報アプリケーションの角度からの説明である。認証サーバに関しては、本出願の実施形態において情報登録方法が更に提供されると共に、図３に示された如く、そのプロセスは以下の各段階を備えて成る：

【００５５】

Ｓ３０１：認証サーバにより、ビジネス・アプリケーションにより送信された基準情報を登録するための要求を受信する段階。

【００５６】

Ｓ３０２：基準情報を登録するための要求に従い、第一認証情報を生成し、且つ、該第一認証情報をビジネス・アプリケーションに対してフィードバックする段階。

【００５７】

Ｓ３０３：ビジネス・アプリケーションにより送信された、署名済み基準情報、基準情報の身分識別子、および、第一認証情報を受信する段階であって、署名済み基準情報は、セキュリティ情報アプリケーションにより、第二認証情報を用いて署名されていると共に、ビジネス・アプリケーションに対して送信されているという段階。

【００５８】

Ｓ３０４：第一認証情報を認証し、且つ、署名済み基準情報に従い第二認証情報を認証する段階。

【００５９】
Ｓ３０５：第一認証情報および第二認証情報の認証を承認した後、基準情報と基準情報の身分識別子とを登録する段階。
【００６０】
図１および図２に示された前記方法と同様に、ビジネス・アプリケーションにより送信された基準情報を登録するための要求を受信すると同時に、認証サーバは、基準情報を登録するための要求をビジネス・アプリケーションがセキュリティ情報に対して送信した後、セキュリティ情報アプリケーションは、第一認証情報に従い認証サーバの身分を決定し得ると共に、その後にセキュリティ情報アプリケーションは、第二認証情報を用いて署名された基準情報と基準情報の身分識別子とをビジネス・アプリケーションに対してフィードバックする如く、認証サーバ自体の身分を表し得る第一認証情報をビジネス・アプリケーションに対してフィードバックする。ビジネス・アプリケーションにより返信された署名済み基準情報および第一認証情報を受信すると同時に、認証サーバは、第一認証情報に対する認証を実施し、且つ、署名済み基準情報に従い第二認証情報に対する認証を実施する。もし前記認証が両方ともに承認されたなら、そのことは基準情報が伝送の間に改竄されていないことを表すと共に、その後、認証サーバは、後続的なプロセスにおける認証および確認のために、基準情報およびその身分識別子を登録する。
【００６１】
上述された如く、認証サーバ自体の証明書は、該認証サーバの身分を効果的に立証し得る。他方、セキュリティ情報アプリケーションにより受信された証明書の有効性を確実とするために、認証サーバは典型的に、それ自体の証明書に署名する。するとセキュリティ情報アプリケーションは、前記証明書が伝送の間に改竄されたか否かを確認し得る。故に、前記段階Ｓ３０２に関し、基準情報を登録するための要求に従い、第一認証情報を生成し、且つ、該第一認証情報をビジネス・アプリケーションに対してフィードバックする段階は、基準情報を登録するための要求に従い、認証サーバ自体の証明書を呼び出す段階、認証サーバ自体の第一暗号鍵を用いて、第一認証情報としての前記証明書に対して署名する段階、および、第一認証情報をビジネス・アプリケーションに対してフィードバックする段階を備えて成る。
【００６２】
先の方法における内容と同様に、本出願の実施形態の状況展開において、認証サーバは、第一認証情報中にチャレンジ・コードを更に備えて成り、認証サーバ自体の第一暗号鍵を使用して署名してから、それをビジネス・アプリケーションに対して送信し得る。このことは、本出願に対する制限を構成するものでない。
【００６３】
ビジネス・アプリケーションが署名済み基準情報および第一認証情報を認証サーバに対して送信した後、該認証サーバは、第一認証情報に対する認証を実施し、且つ、署名済み基準情報に従い第二認証情報に対する認証を実施する。
【００６４】
一例において、第一認証情報に対する認証を実施する段階は、第一復号鍵を用いて第一認証情報を復号して認証する段階を備えて成る。認証サーバは、それ自体の第一復号鍵を使用して第一認証情報を復号して認証する。もし復号済み証明書（またはチャレンジ・コード）が変化しているなら、そのことは前記証明書（またはチャレンジ・コード）が伝送の間に改竄された可能性が高いことを表す。故に、認証サーバは、認証が承認されないことを決定する。復号済み証明書（またはチャレンジ・コード）が、認証サーバによる復号の後で変化していなければ、認証は承認される。
【００６５】
第二認証情報に関し、該第二認証情報は、事前に認証サーバおよびセキュリティ情報アプリケーションにより合意された第二鍵情報を備えて成り、これは先の方法における内容と同様であり、その場合、第二鍵情報は第二暗号鍵および第二復号鍵を備えて成る。更に、署名済み基準情報は、第二暗号鍵を用いてセキュリティ情報アプリケーションにより署

名されている。斯かる状況展開において、署名済み基準情報に従い第二認証情報を認証する段階は、事前に合意された第二鍵情報に従い、事前にセキュリティ情報アプリケーションにより合意された第二復号鍵を用い、第二認証情報を認証するために、署名済み基準情報を復号する段階を備えて成る。

【００６６】

認証サーバが、合意された第二復号鍵を使用して、署名済み基準情報を復号すると共に、基準情報を獲得するなら、そのことは、基準情報が伝送の間に改竄されなかったと見做され得ると共に、認証が承認される。復号の後で使用不能な情報が獲得されたなら、そのことは、署名済み情報が、事前に合意された第二暗号鍵により署名されたのではないことを表すと共に、前記署名済み情報は改竄された情報である可能性が高い。結果として、認証は承認されない。

【００６７】

認証サーバによる認証が承認された後においてのみ、該認証サーバは、基準情報と基準情報の身分識別子とを登録し得る。

【００６８】

図１乃至図３に示された前記の情報登録方法によれば、認証サーバは、基準情報が伝送の間に改竄されたか否かを効果的に確認し得ることから、ユーザは、ビジネス・サービスを使用している間に不正操作者により影響されないことが確実とされる。

【００６９】

前記の情報登録方法は、端末がビジネス・アプリケーションを介してビジネス・サービスを獲得するという任意の状況展開において適用され得る。更に、前記認証サーバは、サービス・プロバイダのバックエンド・サービス・システムにおいて認証機能を有するサーバであり得る。代表的な応用状況において、支払サービス、転送サービスなどの如き比較的に高いセキュリティ・レベル要件を有するビジネス・サービスを提供し得るサービス・プロバイダは、通常、インターネット・ファイナンス認証アライアンス（Internet Finance Authentication Alliance）（IFAA）と称されるネットワーク式身分認証アーキテクチャを使用して、比較的に高いセキュリティ・レベル要件を備えるビジネス・サービスにより要求される身分認証サポートを実現する。換言すると、IFAA は、前記の登録プロセスを実施する認証サーバを提供する。

【００７０】

斯かる状況展開において、種々の機器製造業者は、IFAA により提供される身分認証アーキテクチャも採用することで、それらにより製造された端末における身分認証により必要とされるインタフェースまたはサービスを提供する。

【００７１】

本出願における前記登録方法を明確に記述するために、一例として、IFAA により提供される身分認証アーキテクチャの下での登録を以て詳細な説明が提供される。

【００７２】

図４は、本実施形態に係る、端末と IFAA 認証サーバとの間における登録の代表的な適用方法を示しており、該端末においてはビジネス・アプリケーションおよびセキュリティ情報アプリケーションが動作する。ビジネス・アプリケーションは、サービス・プロバイダのビジネス・サービス・アクセス・ポートとして、端末のユーザに対する種々のビジネス・サービスを提供し得る一方、セキュリティ情報アプリケーションは、ビジネス・アプリケーションにより要求される（本実施形態においては基準情報である）セキュリティ情報を提供すべく使用される。図４に示されたプロセスは、以下の各段階を備えて成る：

【００７３】

Ｓ４０１：ビジネス・アプリケーションは、基準情報を登録するための要求を IFAA 認証サーバに対して送信する。

【００７４】

ユーザがビジネス・アプリケーションにおいて初めてビジネス・サービスを使用するとき、ユーザの生体情報を基準情報として IFAA 認証サーバ内に登録することが必要である

。この時点において、ビジネス・アプリケーションは、基準情報を登録するための要求をIFAA 認証サーバに対して送信する。

【００７５】

Ｓ４０２： IFAA 認証サーバは、チャレンジ・コードと証明書とを備えて成る署名済みデータ・パックを、ビジネス・アプリケーションに対してフィードバックする。

【００７６】

此処で、前記チャレンジ・コードはリプレー・アタックを阻止し得ると共に、前記証明書は、IFAA 認証サーバ自体の身分を表すべく使用される。前記署名済みデータ・パックは、前記登録方法における第一認証情報であると考えられ得る。

【００７７】

これに加え、この段階において、IFAA 認証サーバは IFAA 鍵情報を使用して前記データ・パックに対して署名すると共に、該 IFAA 鍵情報は IFAA 認証サーバ自体により生成されることを銘記すべきである。他方、IFAA 認証サーバ自体の証明書は BIOM（バイオメトリック管理）鍵情報により署名されると共に、該 BIOM 鍵情報は、前記ビジネス・サービスを提供する所定形式のサービス・プロバイダを表すべく使用される。

【００７８】

Ｓ４０３：ビジネス・アプリケーションは、基準情報獲得要求を生成すると共に、該基準情報獲得要求および署名済みデータ・パックを、IFAA サービスを介してセキュリティ情報アプリケーションに対して送信する。

【００７９】

此処で、IFAA サービスは、端末内に配設された IFAA 身分認証アーキテクチャにより提供されるサービスである。代表的な応用状況に対するひとつの方法において、ビジネス・アプリケーションは、本明細書中にて詳細には限定されない IFAA SDK（IFAA 身分認証アーキテクチャに基づく通信ツール）を介して IFAA サービスを呼び出し得る。

【００８０】

Ｓ４０４：セキュリティ情報アプリケーションは、署名済みデータ・パックを認証し、且つ、認証が承認された後、基準情報に署名する。

【００８１】

セキュリティ情報アプリケーションは、先ず、署名済みデータ・パックを復号することが必要であり（たとえば、復号は、本明細書中では詳細に限定されない IFAA 鍵情報を用いて実施され得る）、且つ、復号の後、認証データ・パックにおける証明書（証明書の復号および認証のために BIOM 鍵情報が使用され得る）が使用されて、それが IFAA 登録基準情報であるか否かを認証することを銘記すべきである。

【００８２】

認証が承認された後、セキュリティ情報アプリケーションは、ユーザにより基準情報として入力された生体情報を獲得すると共に、DA（デバイス認証コード）鍵情報を使用して基準情報に署名し、その場合、DA 鍵情報は端末の固有性を表すべく使用される（一例において、DA 鍵情報はセキュリティ情報アプリケーションの固有性を示し得る一方、セキュリティ情報アプリケーションは、機器製造業者により端末内に載置されることから、DA鍵情報は、端末の固有性も示す）。

【００８３】

Ｓ４０５：署名済み基準情報に従い、基準情報の身分鍵情報を決定する段階。

【００８４】

本実施形態において、基準情報の身分鍵情報は典型的に、ビジネス・アプリケーションにおいてユーザにより使用されるアカウント情報に対して関連付けられることで、基準情報が属するユーザを表す。代表的な応用状況において、基準情報の身分鍵情報を生成するために、IFAA サービスは、KeyStore（REE 環境における安全記憶用標準呼出しインタフェース）を介して KeyMaster（安全記憶モジュール）を呼び出し得ると共に、KeyMasterは身分鍵情報を生成する。

【００８５】

伝送の間における身分鍵情報の安全性を確実とするために、セキュリティ情報アプリケーションは、DA 鍵情報を使用して身分鍵情報に署名し得ることを銘記すべきである。

【００８６】

Ｓ４０６：セキュリティ情報アプリケーションは、端末証明書、署名済み基準情報、および、署名済み身分鍵情報を、ビジネス・アプリケーションに対して返信する。

【００８７】

Ｓ４０７：端末証明書、署名済み基準情報、および、署名済み身分鍵情報を、IFAA サービスを介して IFAA 認証サーバに対して送信する段階。

【００８８】

前記端末証明書は、機器製造業者により製造された機器における IFAA 身分認証アーキテクチャに関与している該製造業者により提供された認証コード証明書とも称されることを銘記すべきである。換言すると、端末証明書は、その端末が IFAA 身分認証アーキテクチャを使用するか否かを表し得る。

【００８９】

本実施形態に係る方法において、前記チャレンジ・コードおよび IFAA 認証サーバ自体の証明書もまた、IFAA 認証サーバに対して同時に返信され得る。その故に、IFAA 認証サーバは、チャレンジ・コード、および、該 IFAA 認証サーバ自体の証明書を更に認証し得る。

【００９０】

Ｓ４０８：IFAA 認証サーバは、受信された情報を認証し、且つ、認証が承認された後、基準情報、および、その身分鍵情報を登録する。

【００９１】

IFAA 認証サーバは先ず、端末証明書を認証することを銘記すべきである。たとえば、IFAA 認証サーバは、受信した情報を、IFAA 鍵情報を使用して復号すると共に、端末証明書の有効性を認証し得る。認証が承認された後、IFAA 認証サーバは DA 鍵情報を使用し、身分鍵情報を復号して認証する。両方とも承認されたなら、基準情報は伝送の間に改竄されていないと考えられ得ると共に、IFAA 認証サーバは、基準情報およびその身分鍵情報を登録する。

【００９２】

Ｓ４０９：登録結果をビジネス・アプリケーションに対してフィードバックする段階。

【００９３】

前記実施形態からは、代表的な応用状況において、基準情報が伝送の間に改竄されたか否かを正確に決定するために種々の鍵情報が使用され得ることが理解され得る。

【００９４】

前記内容は、基準情報登録方法を記述している。基準情報が登録された後、ユーザは対応するビジネス・サービスを使用し得る。ユーザがビジネス・サービスを使用しているとき、該ユーザのセキュリティ情報を提供することが必要である。対応して、認証サーバは、ビジネス・サービスを使用している間にユーザにより提供されたセキュリティ情報に従い、認証を実施し得る。故に、本出願の実施形態においては、情報認証方法が更に提供されると共に、図５に示された如く、該方法は以下の各段階を備えて成る：

【００９５】

Ｓ５０１：認証対象情報に対する照合要求を認証サーバに対して送信する段階。

【００９６】

ユーザがビジネス・アプリケーションにおける（たとえば、指紋式支払サービスなどの）ビジネス・サービスを使用しているとき、ユーザは、先行して登録された基準情報との比較のために自分自身のセキュリティ情報（たとえば指紋情報）を提供する必要があることが多い。この時点において、ビジネス・アプリケーションは、ユーザのセキュリティ情報を認証対象情報として獲得すると共に、認証および照合のために次続的に認証サーバに対して送信する。

【００９７】

前記の状況において、ビジネス・アプリケーションは、認証対象情報に対する照合要求を認証サーバに対して送信する。

【００９８】

Ｓ５０２：認証サーバによりフィードバックされた第一認証情報を受信する段階。

【００９９】

前記登録方法と同様に、第一認証情報は認証サーバの身分を表すものであり、本明細書中では繰り返されない。

【０１００】

Ｓ５０３：第一認証情報に従い認証対象情報獲得要求を生成し、認証対象情報獲得要求をセキュリティ情報アプリケーションに対して送信し、且つ、セキュリティ情報アプリケーションにより提供された認証対象情報および該認証対象情報の認証対象身分識別子を獲得する段階。

【０１０１】

同様に、セキュリティ情報アプリケーションは、第一認証情報に従い、認証されるべき対象者の身元を決定する。認証されるべき対象者の身元が有効であると決定され且つ認証が承認された後、セキュリティ情報アプリケーションは更に、ユーザにより提供された認証対象情報およびその認証対象身分識別子をビジネス・アプリケーションに対して返信する。

【０１０２】

前記の登録方法とは異なり、認証対象情報に署名すべく第二認証情報を使用することは必要でない。

【０１０３】

Ｓ５０４：認証対象情報、認証対象身分識別子、および、第一認証情報を認証サーバに対して送信し、該認証サーバにより、第一認証情報、認証対象身分識別子、および、認証対象情報を認証させ、認証結果を生成させ、且つ、認証結果をビジネス・アプリケーションに対してフィードバックさせる段階。

【０１０４】

前記内容からは、第一認証情報および認証対象身分識別子により、認証対象情報が伝送の間に改竄されたか否かが確認され得る。前記認証が承認された後、認証サーバは、認証対象情報に対する認証を実施し得る。

【０１０５】

本出願の実施形態においては、情報認証方法が更に提供されると共に、図６に示された如く、該方法は以下の各段階を備えて成る：

【０１０６】

Ｓ６０１：ビジネス・アプリケーションにより送信されると共に第一認証情報を担持する認証対象情報獲得要求を受信する段階。

【０１０７】

Ｓ６０２：第一認証情報を担持する基準情報獲得要求に従い、認証対象情報、および、該認証対象情報の身分識別子を、ビジネス・アプリケーションを介して認証サーバに対して送信することで、該認証サーバにより、第一認証情報、認証対象身分識別子、および、認証対象情報を認証させ、認証結果を生成させ、且つ、認証結果をビジネス・アプリケーションに対してフィードバックさせる段階。

【０１０８】

前記段階Ｓ６０２に関し、第一認証情報を担持する基準情報獲得要求に従い、認証対象情報、および、認証対象情報の身分識別子をビジネス・アプリケーションに対して戻し送信する段階は、基準情報獲得要求中に担持された第一認証情報を認証し、認証が承認された後に、ユーザにより入力された認証対象情報を受信する段階、認証対象情報が属する基準情報を識別し、基準情報に一致する身分基準を、認証対象情報の認証対象身分識別子であると決定する段階、および、認証対象情報、および、認証対象情報の認証対象身分識別子をビジネス・アプリケーションに対して返信する段階を備えて成る。

【０１０９】
本出願の実施形態においては、情報認証方法が更に提供されると共に、図７に示された如く、該方法は以下の各段階を備えて成る：
【０１１０】
Ｓ７０１：ビジネス・アプリケーションにより送信された認証対象情報に対する照合要求を、認証サーバにより受信する段階。
【０１１１】
Ｓ７０２：照合要求に従い、第一認証情報を生成し、且つ、第一認証情報をビジネス・アプリケーションに対してフィードバックする段階。
【０１１２】
Ｓ７０３：ビジネス・アプリケーションにより送信された、認証対象情報、認証対象情報の身分識別子、および、第一認証情報を受信する段階。
【０１１３】
Ｓ７０４：第一認証情報、身分識別子、および、認証対象情報を夫々認証して認証結果を生成し、且つ、認証結果をビジネス・アプリケーションに対してフィードバックする段階。
【０１１４】
前記段階Ｓ７０４に関し、認証サーバは、ビジネス・アプリケーションにより送信された各情報を夫々認証することを銘記すべきである。一例において、第一認証情報、身分識別子、および、認証対象情報を認証する段階は夫々、第一認証情報に関しては、認証サーバの第一復号鍵を用いて第一認証情報を復号すると共に、復号済み証明書を認証する段階を備えて成り、身分識別子に関しては、登録済み基準情報の身分識別子に従い、該身分識別子が登録済み基準情報の身分識別子に一致するか否かを決定し、且つ、認証対象情報を認証のために登録済み基準情報と比較する段階を備えて成る。
【０１１５】
代表的な応用状況において、認証サーバは、該認証サーバによるいずれかの情報の認証が認証プロセスの間に承認されなければ、失敗の通知をフィードバックすると共に、全ての情報が認証サーバによる認証を通過したときにのみ成功の通知をフィードバックし得る。一例において、認証結果を生成し且つ認証結果をビジネス・アプリケーションに対してフィードバックする段階は、第一認証情報に関しては、認証が承認されたなら、認証対象情報および認証対象身分識別子を認証し、その他の場合には認証失敗の通知を返信する段階を備えて成り、身分識別子に関しては、認証が承認されたなら、認証対象情報を認証し、その他の場合には、認証失敗の通知を返信する段階を備えて成り、且つ、認証対象情報に関しては、認証が承認されたなら、成功の通知を返信し、その他の場合には、認証失敗の通知を返信する段階を備えて成る。
【０１１６】
前記登録プロセスに対応して、本出願における前記認証方法を明確に記述するために、一例として、IFAA により提供される身分認証アーキテクチャの下での認証を以て詳細な説明が提供される。
【０１１７】
図８は、本実施形態における端末と IFAA 認証サーバとの間の代表的な適用方法を示している。示されたプロセスは、以下の各段階を備えて成る：
【０１１８】
Ｓ８０１：ビジネス・アプリケーションは、IFAA 認証サーバに対して認証対象情報照合要求を送信する。
【０１１９】
Ｓ８０２：IFAA 認証サーバは、チャレンジ・コードと証明書とを備えて成る署名済みデータ・パックをビジネス・アプリケーションに対してフィードバックする。
【０１２０】
Ｓ８０３：ビジネス・アプリケーションは、認証対象情報獲得要求を生成し、且つ、認

証対象情報獲得要求および署名済みデータ・パックを、IFAA サービスを介してセキュリティ情報アプリケーションに対して送信する。

【０１２１】

Ｓ８０４：セキュリティ情報アプリケーションは、署名済みデータ・パックを認証し、認証が承認された後、前記登録プロセスにおいて認証対象情報により使用された身分鍵情報に署名する。

【０１２２】

Ｓ８０５：セキュリティ情報アプリケーションは、署名済み認証対象情報をビジネス・アプリケーションに対して返信する。

【０１２３】

Ｓ８０６：署名済み認証対象情報を、IFAA サービスを介して IFAA 認証サーバに対して送信する段階。

【０１２４】

Ｓ８０７：受信した署名済み認証対象情報に関し、IFAA 認証サーバは、登録された身分鍵情報を使用して、署名済み認証対象情報を認証し、認証が承認された後、認証のために、認証対象情報を登録済み基準情報と比較する。

【０１２５】

Ｓ８０８：認証結果をビジネス・アプリケーションに対して返信する段階。

【０１２６】

前記情報伝送方法は、本出願の種々の実施形態により上述された。更に、本出願の実施形態は、情報登録デバイスを更に提供する。図９に示された如く、前記デバイスは：基準情報を登録するための要求を認証サーバに対して送信すべく構成された登録要求モジュール 901 と；認証サーバによりフィードバックされた第一認証情報を受信すべく構成された受信モジュール 902 と；基準情報獲得要求を生成し、該基準情報獲得要求および第一認証情報をセキュリティ情報アプリケーションに対して送信し、且つ、セキュリティ情報アプリケーションが第一認証情報の認証を承認した後にセキュリティ情報アプリケーションにより返信された署名済み基準情報と基準情報の身分識別子とを獲得すべく構成された獲得モジュールであって、署名済み基準情報は第二認証情報を使用してセキュリティ情報アプリケーションにより署名されているという獲得モジュール 903 と；署名済み基準情報、基準情報の身分識別子、および、第一認証情報を認証サーバに対して送信し、認証サーバが、第一認証情報の認証を承認し且つ署名済み基準情報に従い第二認証情報の認証を承認した後で、認証サーバにより、基準情報と基準情報の身分識別子とを登録させるべく構成された送信モジュール 904 と；を備えて成る。

【０１２７】

受信モジュール 902 は、認証サーバにより送信され且つ該認証サーバ自体の第一暗号鍵を用いて署名された証明書を受信し、且つ、署名済み証明書を第一認証情報として使用すべく構成される。

【０１２８】

図１０に示された如く、本出願の実施形態は、情報登録デバイスを更に提供すると共に、該デバイスは：ビジネス・アプリケーションにより送信された第一認証情報および基準情報獲得要求を受信すべく構成された受信モジュール 1001 と；前記第一認証情報を認証し、認証が承認された後に、ビジネス・アプリケーションに対し、第二認証情報を用いて署名された基準情報を返信し且つ基準情報の身分識別子を返信することで、ビジネス・アプリケーションにより署名済み基準情報および基準情報の身分識別子を認証サーバに対して送信させ、且つ、認証サーバにより、該認証サーバが、第一認証情報の認証を承認し且つ署名済み基準情報に従い第二認証情報の認証を承認した後、基準情報と基準情報の身分識別子とを登録させるべく構成された署名モジュール 1002 と；を備えて成る。

【０１２９】

署名モジュール 1002 は、ユーザにより入力された基準情報を受信し、第二認証情報を使用して基準情報に署名し、基準情報に対して該基準情報の身分識別子を決定し、且つ、

署名済み基準情報、および、基準情報の身分識別子をビジネス・アプリケーションに対して返信すべく構成される。

【０１３０】

基準情報の身分識別子は、基準情報の身分鍵情報を備えて成り、該身分鍵情報はユーザのアカウント情報に関連付けられていることを銘記すべきである。

【０１３１】

第一認証情報が認証サーバの署名済み証明書を備えて成るという状況展開において、署名モジュール 1002 は、認証サーバの第一暗号鍵に対応する第一復号鍵を使用して、署名済み証明書を復号して認証すべく構成される。

【０１３２】

第二認証情報は、事前に認証サーバにより合意された第二鍵情報を備えて成り、該第二鍵情報は、第二暗号鍵および第二復号鍵を備えて成る。署名モジュール 1002 は、事前に認証サーバにより合意された第二暗号鍵を使用して基準情報に署名すべく構成される。

【０１３３】

図１１に示された如く、本出願の実施形態は情報登録デバイスを更に提供し、該デバイスは：ビジネス・アプリケーションにより送信された、基準情報を登録するための要求を受信すべく構成された登録要求受信モジュール 1101 と；基準情報を登録するための要求に従い、第一認証情報を生成し、且つ、それをビジネス・アプリケーションに対してフィードバックすべく構成されたフィードバック・モジュール 1102 と；ビジネス・アプリケーションにより送信された、署名済み基準情報、基準情報の身分識別子、および、第一認証情報を受信する登録情報受信モジュールであって、署名済み基準情報は、第二認証情報を使用することにより署名されており、且つ、セキュリティ情報アプリケーションによりビジネス・アプリケーションに対して送信されているという登録情報受信モジュール 1103 と；第一認証情報を認証し、且つ、署名済み基準情報に従い第二認証情報を認証すべく構成された認証モジュール 1104 と；第一認証情報および第二認証情報の認証が両方ともに承認された後で、基準情報と基準情報の身分識別子とを登録すべく構成された登録モジュール 1105 と；を備えて成る。

【０１３４】

一例において、フィードバック・モジュール 1102 は、基準情報を登録するための要求に従い、認証サーバ自体の証明書を呼び出し、認証サーバ自体の第一暗号鍵を用いて、第一認証情報として証明書に署名し、且つ、それをビジネス・アプリケーションに対してフィードバックすべく構成される。

【０１３５】

認証モジュール 1104 は、第一復号鍵を用いて、第一認証情報を復号および認証すべく構成される。

【０１３６】

第二認証情報は、事前に認証サーバおよびセキュリティ情報アプリケーションにより合意された第二鍵情報を備えて成り、その場合、第二鍵情報は第二暗号鍵および第二復号鍵を備えて成り、署名済み基準情報は、第二暗号鍵を用いてセキュリティ情報アプリケーションにより署名されている。斯かる状況展開において、認証モジュール 1104 は、事前に合意された第二鍵情報に従い、事前にセキュリティ情報アプリケーションにより合意された第二復号鍵を使用して、第二認証情報を認証すべく署名済み基準情報を復号すべく構成される。

【０１３７】

図１２に示された如く、本出願の実施形態は、情報認証デバイスを更に提供し、該デバイスは：認証対象情報に対する照合要求を認証サーバに送信すべく構成された認証要求モジュール 1201 と；認証サーバによりフィードバックされた第一認証情報を受信すべく構成された受信モジュール 1202 と；認証対象情報獲得要求を生成し、認証対象情報獲得要求および第一認証情報をセキュリティ情報アプリケーションに対して送信し、且つ、セキュリティ情報アプリケーションが第一認証情報の認証を承認した後で該セキュリティ情報

アプリケーションにより返信された認証対象情報、および、認証対象情報の認証対象身分識別子を獲得すべく構成された獲得モジュール 1203 と；認証対象情報、認証対象身分識別子、および、第一認証情報を認証サーバに対して送信することで、該認証サーバにより、第一認証情報、認証対象身分識別子および認証対象情報を認証させ、認証結果を生成させ、且つ、認証結果をビジネス・アプリケーションに対してフィードバックさせるべく構成された送信モジュール 1204 と；を備えて成る。

【０１３８】

図１３に示された如く、本出願の実施形態は情報認証デバイスを更に提供し、該デバイスは：ビジネス・アプリケーションにより送信されると共に第一認証情報を担持する認証対象情報獲得要求を受信すべく構成された受信モジュール 1301 と；第一認証情報を認証し、認証が承認された後、認証対象情報および認証対象情報の身分識別子を、ビジネス・アプリケーションを介して認証サーバに対して送信することで、該認証サーバにより、第一認証情報、認証対象身分識別子、および、認証対象情報を認証させ、認証結果を生成させ、且つ、認証結果をビジネス・アプリケーションに対してフィードバックさせるべく構成された署名モジュール 1302 と；を備えて成る。

【０１３９】

一例において、署名モジュール 1302 は、基準情報獲得要求内に担持された第一認証情報を認証し、認証が承認された後、認証対象情報が属する基準情報を確認し、基準情報に一致する身分基準を、認証対象情報の認証対象身分識別子であると決定し、且つ、認証対象情報と認証対象情報の認証対象身分識別子とをビジネス・アプリケーションに対して返信すべく構成される。

【０１４０】

図１４に示された如く、本開示内容の実施形態は、情報認証デバイスを更に提供し、該デバイスは：ビジネス・アプリケーションにより送信された認証対象情報に対する照合要求を受信すべく構成された認証要求受信モジュール 1401 と；照合要求に従い、第一認証情報を生成すると共に、それをビジネス・アプリケーションに対してフィードバックすべく構成されたフィードバック・モジュール 1402 と；ビジネス・アプリケーションにより送信された、認証対象情報、認証対象情報の認証対象身分識別子、および、第一認証情報を受信すべく構成された認証情報受信モジュール 1403 と；第一認証情報、認証対象身分識別子、および、認証対象情報を夫々認証し、認証結果を生成し、且つ、それをビジネス・アプリケーションに対してフィードバックすべく構成された認証モジュール 1404 と；を備えて成る。

【０１４１】

認証モジュール 1404 は、第一認証情報に関しては、情報認証デバイスの第一復号鍵を用いて第一認証情報を復号すると共に、復号済み証明書を認証し、認証対象身分識別子に関しては、登録済み基準情報の身分識別子に従い、認証対象身分識別子が登録済み基準情報の身分識別子と一致するか否かを決定し、且つ、認証対象情報を認証のために登録済み基準情報と比較すべく構成される。

【０１４２】

認証モジュール 1404 は、第一認証情報に関しては、認証が承認されたなら、認証対象情報および認証対象身分識別子を認証し、その他の場合には認証失敗の通知を返信し、身分識別子に関しては、認証が承認されたなら、認証対象情報を認証し、その他の場合には認証失敗の通知を返信し、且つ、認証対象情報に関しては、認証が承認されたなら、成功の通知を返信し、その他の場合には認証失敗の通知を返信すべく構成される。

【０１４３】

典型的な構成において、コンピュータ処理デバイスは、ひとつ以上の中央処理ユニット（CPU）、入力／出力インタフェース、ネットワーク・インタフェース、および、記憶装置を含んでいる。

【０１４４】

前記記憶装置としては、揮発性メモリ、ランダム・アクセス・メモリ（RAM）、および

／または、たとえば読出専用メモリ（ROM）もしくはフラッシュ RAM などの不揮発性メモリの如き、コンピュータ可読媒体が挙げられる。前記記憶装置は、コンピュータ可読媒体の一例である。

【０１４５】

コンピュータ可読媒体としては、任意の方法または技術により情報記憶を実施し得る持続性、揮発性、および、固定的な媒体が挙げられる。前記情報は、コンピュータ可読命令、データ構造、プログラム・モジュール、または、他のデータであり得る。コンピュータの記憶媒体の例としては、限定的なものとしてではなく、相変化 RAM（PRAM）、スタティック RAM（SRAM）、ダイナミック RAM（DRAM）、他の形式のランダム・アクセス・メモリ（RAM）、読出専用メモリ（ROM）、電気消去可能プログラマブル読出専用メモリ（EEPROM）、フラッシュ・メモリもしくは他のメモリ技術、コンパクト・ディスク読出専用メモリ（CD-ROM）、デジタル多用途ディスク（DVD）もしくは他の光学メモリ、カセット、カセットおよびディスクメモリ、もしくは、他の磁気メモリ・デバイス、または、コンピュータ処理デバイスに対して利用可能な情報を記憶すべく使用され得る他の任意の非伝送媒体が挙げられる。本明細書中における定義に依れば、前記コンピュータ可読媒体は、変調されたデータ信号および搬送波の如き一時的媒体を包含しない。

【０１４６】

“含む（包含する）”、“備える（備えて成る、具備する）”、または、それらの他の一切の変化形は、一連の要素を備えて成るプロセス、方法、商品、または、デバイスが、これらの要素を備えて成るだけでなく、詳細に列挙されない他の要素も備えて成り、または、該プロセス、方法、商品またはデバイスに対して本来的である要素を更に備えて成る如く、非排他的包含物を包括することを意図していることを銘記すべきである。更なる限定が無い場合、“ひとつの…を備えて成る”という説明により定義された要素は、前記要素を備えて成るプロセス、方法、商品またはデバイスが付加的な同一要素を更に備えて成ることを排除しない。

【０１４７】

当業者であれば、本出願の各実施形態は、方法、システム、または、コンピュータ・プログラム製品として提供され得ることを理解すべきである。故に、本出願は、完全なハードウェア実施形態、完全なソフトウェア実施形態、または、ソフトウェアおよびハードウェアを組み合わせた実施形態として実現され得る。更に、本出願は、コンピュータ使用可能なプログラム・コードを自身内に含む（限定的なものとしてではなく、磁気ディスクメモリ、CD-ROM、光学メモリなどの）一種類以上のコンピュータ使用可能な記憶媒体上に実現されたコンピュータ・プログラム製品の形態であり得る。

【０１４８】

前記においては本出願の実施形態のみが記述されたが、本出願を限定すべく使用されてはいない。当業者によれば、本出願は種々の改変および変更を行い得る。本出願の精神および原理の範囲内で為される一切の改変、等価的置換、または、改良は、本出願の各請求項により包含されるものとする。

本発明の実施態様の一部を以下の〔態様１〕－〔態様３４〕に記載する。

〔態様１〕

情報登録方法であって、

基準情報を登録するための要求を認証サーバに対して送信する段階と、

前記認証サーバによりフィードバックされた第一認証情報を受信する段階と、

基準情報獲得要求を生成し、該基準情報獲得要求および前記第一認証情報をセキュリティ情報アプリケーションに対して送信し、且つ、前記セキュリティ情報アプリケーションが前記第一認証情報の認証を承認した後、前記セキュリティ情報アプリケーションにより返信された署名済み基準情報と前記基準情報の身分識別子とを獲得する段階であって、前記署名済み基準情報は前記セキュリティ情報アプリケーションにより第二認証情報を用いて署名されている、という段階と、

前記署名済み基準情報、前記基準情報の前記身分識別子、および、前記第一認証情報を

前記認証サーバに対して送信することで、該認証サーバにより、該認証サーバが、前記第一認証情報の認証を承認し且つ前記署名済み基準情報に従い前記第二認証情報の認証を承認した後に、前記基準情報と前記基準情報の前記身分識別子とを登録させる段階と、
を備えて成る情報登録方法。
〔態様２〕
前記認証サーバによりフィードバックされた第一認証情報を受信する前記段階は、
前記認証サーバにより送信されると共に、該認証サーバ自体の第一暗号鍵を用いて署名された証明書を受信し、且つ、前記署名済み証明書を前記第一認証情報として用いる段階、
を備えて成る、態様１に記載の方法。
〔態様３〕
情報登録方法であって、
ビジネス・アプリケーションにより送信された第一認証情報および基準情報獲得要求を受信する段階と、
前記第一認証情報を認証し、且つ、認証が承認された後、前記ビジネス・アプリケーションに対し、第二認証情報を用いて署名された基準情報を返信し且つ前記基準情報の身分識別子を返信することで、前記ビジネス・アプリケーションにより、前記署名済み基準情報と前記基準情報の前記身分識別子とを認証サーバに対して送信させ、且つ、前記認証サーバにより、該認証サーバが前記第一認証情報の認証を承認し且つ前記署名済み基準情報に従い前記第二認証情報の認証を承認した後、前記基準情報と前記基準情報の前記身分識別子とを登録させる段階と、
を備えて成る情報登録方法。
〔態様４〕
第二認証情報を用いて署名された基準情報と前記基準情報の身分識別子とを前記ビジネス・アプリケーションに対して返信する前記段階は、
ユーザにより入力された基準情報を受信する段階と、
前記第二認証情報を用いて前記基準情報に署名し、且つ、前記基準情報に対して該基準情報の身分識別子を決定する段階と、
前記署名済み基準情報と前記基準情報の前記身分識別子とを前記ビジネス・アプリケーションに対して返信する段階と、
を備えて成る、態様３に記載の方法。
〔態様５〕
前記基準情報の前記身分識別子は前記基準情報の身分鍵情報を備えて成り、且つ、前記身分鍵情報は前記ユーザのアカウント情報に対して関連付けられる、態様４に記載の方法。
〔態様６〕
前記第一認証情報は前記認証サーバの署名済み証明書を備えて成り、且つ、
前記第一認証情報を認証する前記段階は、前記認証サーバの第一暗号鍵に対応する第一復号鍵を用いて、前記署名済み証明書を復号して認証する段階、を備えて成る、
態様３に記載の方法。
〔態様７〕
前記第二認証情報は、事前に前記認証サーバにより合意された第二鍵情報であり、前記第二鍵情報は第二暗号鍵および第二復号鍵を備えて成り、且つ、
前記第二認証情報を用いて前記基準情報に署名する前記段階は、事前に前記認証サーバにより合意された前記第二暗号鍵を用いて前記基準情報に署名する段階、を備えて成る、
態様４に記載の方法。
〔態様８〕
情報登録方法であって、
認証サーバにより、ビジネス・アプリケーションにより送信された基準情報を登録するための要求を受信する段階と、

基準情報を登録するための前記要求に従い、第一認証情報を生成し、且つ、該第一認証情報を前記ビジネス・アプリケーションに対してフィードバックする段階と、
前記ビジネス・アプリケーションにより送信された、署名済み基準情報、前記基準情報の身分識別子、および、前記第一認証情報を受信する段階であって、前記署名済み基準情報は、セキュリティ情報アプリケーションにより前記第二認証情報を用いることにより署名されており且つ前記ビジネス・アプリケーションに対して送信されているという段階と、
前記第一認証情報を認証し、且つ、前記署名済み基準情報に従い前記第二認証情報を認証する段階と、
前記第一認証情報および前記第二認証情報の認証を承認した後、前記基準情報と前記基準情報の前記身分識別子とを登録する段階と、
を備えて成る情報登録方法。
〔態様９〕
基準情報を登録するための前記要求に従い第一認証情報を生成し、且つ、前記第一認証情報を前記ビジネス・アプリケーションに対してフィードバックする前記段階は、
基準情報を登録するための前記要求に従い、前記認証サーバ自体の証明書を呼び出す段階と、
前記認証サーバ自体の第一暗号鍵を用い、前記第一認証情報として前記証明書に署名し、且つ、前記第一認証情報を前記ビジネス・アプリケーションに対してフィードバックする段階と、
を備えて成る、態様８に記載の方法。
〔態様１０〕
前記第一認証情報を認証する前記段階は、
第一復号鍵を用いて前記第一認証情報を復号して認証する段階、
を備えて成る、態様８に記載の方法。
〔態様１１〕
前記第二認証情報は、事前に前記認証サーバおよび前記セキュリティ情報アプリケーションにより合意された第二鍵情報を備えて成り、前記第二鍵情報は第二暗号鍵および第二復号鍵を備えて成り、前記署名済み基準情報は前記第二暗号鍵を用い前記セキュリティ情報アプリケーションにより署名されており、且つ、
前記署名済み基準情報に従い前記第二認証情報を認証する前記段階は、事前に合意された前記第二鍵情報に従い、事前に前記セキュリティ情報アプリケーションにより合意された前記第二復号鍵を用いて、前記第二認証情報を認証するために前記署名済み基準情報を復号する段階、を備えて成る、
態様８に記載の方法。
〔態様１２〕
情報認証方法であって、
認証対象情報に対する照合要求を認証サーバに対して送信する段階と、
前記認証サーバによりフィードバックされた第一認証情報を受信する段階と、
認証対象情報獲得要求を生成し、該認証対象情報獲得要求および前記第一認証情報をセキュリティ情報アプリケーションに対して送信し、且つ、前記セキュリティ情報アプリケーションが前記第一認証情報の認証を承認した後、前記セキュリティ情報アプリケーションにより返信された認証対象情報と該認証対象情報の認証対象身分識別子とを獲得する段階と、
前記認証対象情報、前記認証対象身分識別子、および、前記第一認証情報を前記認証サーバに対して送信することで、該認証サーバにより、前記第一認証情報、前記認証対象身分識別子、および、前記認証対象情報を認証させ、認証結果を生成させ、且つ、前記認証結果を前記ビジネス・アプリケーションに対してフィードバックさせる段階と、
を備えて成る情報認証方法。
〔態様１３〕

情報認証方法であって、
ビジネス・アプリケーションにより送信され且つ第一認証情報を担持する認証対象情報獲得要求を受信する段階と、
前記第一認証情報を認証し、且つ、認証が承認された後、前記認証対象情報と該認証対象情報の身分識別子とを前記ビジネス・アプリケーションを介して認証サーバに対して送信することで、該認証サーバにより、前記第一認証情報、前記認証対象身分識別子、および、前記認証対象情報を認証させ、認証結果を生成させ、且つ、該認証結果を前記ビジネス・アプリケーションに対してフィードバックさせる段階と、
を備えて成る情報認証方法。
〔態様１４〕
前記第一認証情報を担持する基準情報獲得要求に従い、前記認証対象情報と該認証対象情報の身分識別子とを前記ビジネス・アプリケーションに対して返信する前記段階は、
前記基準情報獲得要求中に担持された前記第一認証情報を認証する段階と、
前記認証が承認された後、ユーザにより入力された認証対象情報を受信する段階と、
前記認証対象情報が属する基準情報を識別し、且つ、前記基準情報に一致する身分基準を、前記認証対象情報の認証対象身分識別子として決定する段階と、
前記認証対象情報と該認証対象情報の前記認証対象身分識別子とを、前記ビジネス・アプリケーションに対して返信する段階と、
を備えて成る、態様１３に記載の方法。
〔態様１５〕
情報認証方法であって、
認証サーバにより、ビジネス・アプリケーションにより送信された認証対象情報に対する照合要求を受信する段階と、
前記照合要求に従い、第一認証情報を生成し、且つ、該第一認証情報を前記ビジネス・アプリケーションに対してフィードバックする段階と、
前記ビジネス・アプリケーションにより送信された、前記認証対象情報、前記認証対象情報の認証対象身分識別子、および、前記第一認証情報を受信する段階と、
前記第一認証情報、前記認証対象身分識別子、および、前記認証対象情報を夫々認証して、認証結果を生成し、且つ、該認証結果を前記ビジネス・アプリケーションに対してフィードバックする段階と、
を備えて成る情報認証方法。
〔態様１６〕
前記第一認証情報、前記身分識別子、および、前記認証対象情報を夫々認証する前記段階は、
前記第一認証情報に関しては、前記認証サーバの第一復号鍵を用いて前記第一認証情報を復号し、且つ、復号済み証明書を認証する段階と、
前記認証対象身分識別子に関しては、登録済み基準情報に従い、前記認証対象身分識別子が登録済み基準情報の身分識別子と一致するか否かを決定する段階と、
認証のために、前記認証対象情報を前記登録済み基準情報と比較する段階と、
を備えて成る、態様１５に記載の方法。
〔態様１７〕
認証結果を生成し、且つ、該認証結果を前記ビジネス・アプリケーションに対してフィードバックする前記段階は、
前記第一認証情報に関しては、認証が承認されたなら、前記認証対象情報および前記認証対象身分識別子を認証し、その他の場合には認証失敗の通知を返信する段階と、
前記身分識別子に関しては、認証が承認されたなら、前記認証対象情報を認証し、その他の場合には、認証失敗の通知を返信する段階と、
前記認証対象情報に関しては、認証が承認されたなら、成功の通知を返信し、その他の場合には、認証失敗の通知を返信する段階と、
を備えて成る、態様１６に記載の方法。

〔態様１８〕
情報登録デバイスであって、
基準情報を登録するための要求を認証サーバに対して送信すべく構成された登録要求モジュールと、
前記認証サーバによりフィードバックされた第一認証情報を受信すべく構成された受信モジュールと、
基準情報獲得要求を生成し、該基準情報獲得要求および前記第一認証情報をセキュリティ情報アプリケーションに対して送信し、且つ、前記セキュリティ情報アプリケーションが前記第一認証情報の認証を承認した後、前記セキュリティ情報アプリケーションにより返信された署名済み基準情報と前記基準情報の身分識別子とを獲得すべく構成された獲得モジュールであって、前記署名済み基準情報は前記セキュリティ情報アプリケーションにより第二認証情報を用いて署名されている、という獲得モジュールと、
前記署名済み基準情報、前記基準情報の前記身分識別子、および、前記第一認証情報を前記認証サーバに対して送信することで、該認証サーバにより、該認証サーバが、前記第一認証情報の認証を承認し且つ前記署名済み基準情報に従い前記第二認証情報の認証を承認した後に、前記基準情報と前記基準情報の前記身分識別子とを登録させるべく構成された送信モジュールと、
を備えて成る情報登録デバイス。
〔態様１９〕
前記受信モジュールは、前記認証サーバにより送信されると共に、該認証サーバ自体の第一暗号鍵を用いて署名された証明書を受信し、且つ、前記署名済み証明書を前記第一認証情報として用いるべく構成される、態様１８に記載のデバイス。
〔態様２０〕
情報登録デバイスであって、
ビジネス・アプリケーションにより送信された第一認証情報および基準情報獲得要求を受信すべく構成された受信モジュールと、
前記第一認証情報を認証し、且つ、認証が承認された後、前記ビジネス・アプリケーションに対し、第二認証情報を用いて署名された基準情報を返信し且つ前記基準情報の身分識別子を返信することで、前記ビジネス・アプリケーションにより、前記署名済み基準情報と前記基準情報の前記身分識別子とを認証サーバに対して送信させ、且つ、前記認証サーバにより、該認証サーバが前記第一認証情報の認証を承認し且つ前記署名済み基準情報に従い前記第二認証情報の認証を承認した後、前記基準情報と前記基準情報の前記身分識別子とを登録させるべく構成された署名モジュールと、
を備えて成る情報登録デバイス。
〔態様２１〕
前記署名モジュールは、ユーザにより入力された基準情報を受信し、前記第二認証情報を用いて前記基準情報に署名し、前記基準情報に対して該基準情報の身分識別子を決定し、且つ、前記署名済み基準情報と前記基準情報の前記身分識別子とを前記ビジネス・アプリケーションに対して返信すべく構成される、態様２０に記載のデバイス。
〔態様２２〕
前記基準情報の前記身分識別子は前記基準情報の身分鍵情報を備えて成り、且つ、前記身分鍵情報は前記ユーザのアカウント情報に対して関連付けられる、態様２１に記載のデバイス。
〔態様２３〕
前記第一認証情報は前記認証サーバの署名済み証明書を備えて成り、且つ、前記署名モジュールは、前記認証サーバの第一暗号鍵に対応する第一復号鍵を用いて、前記署名済み証明書を復号して認証すべく構成される、態様２０に記載のデバイス。
〔態様２４〕
前記第二認証情報は、事前に前記認証サーバにより合意された第二鍵情報であり、前記第二鍵情報は第二暗号鍵および第二復号鍵を備えて成り、且つ、

前記署名モジュールは、事前に前記認証サーバにより合意された前記第二暗号鍵を用いて前記基準情報に署名すべく構成される、
態様２１に記載のデバイス。
〔態様２５〕
情報登録デバイスであって、
ビジネス・アプリケーションにより送信された基準情報を登録するための要求を受信すべく構成された登録要求受信モジュールと、
基準情報を登録するための前記要求に従い、第一認証情報を生成し、且つ、それを前記ビジネス・アプリケーションに対してフィードバックすべく構成されたフィードバック・モジュールと、
前記ビジネス・アプリケーションにより送信された、署名済み基準情報、前記基準情報の身分識別子、および、前記第一認証情報を受信する登録情報受信モジュールであって、前記署名済み基準情報は、セキュリティ情報アプリケーションにより前記第二認証情報を用いることにより署名されており且つ前記ビジネス・アプリケーションに対して送信されているという登録情報受信モジュールと、
前記第一認証情報を認証し、且つ、前記署名済み基準情報に従い前記第二認証情報を認証すべく構成された認証モジュールと、
前記第一認証情報および前記第二認証情報の認証を通した後、前記基準情報と前記基準情報の前記身分識別子とを登録すべく構成された登録モジュールと、
を備えて成る情報登録デバイス。
〔態様２６〕
前記フィードバック・モジュールは、基準情報を登録するための前記要求に従い、前記認証サーバ自体の証明書を呼び出し、前記認証サーバ自体の第一暗号鍵を用い、前記第一認証情報として前記証明書に署名し、且つ、それを前記ビジネス・アプリケーションに対してフィードバックすべく構成される、態様２５に記載のデバイス。
〔態様２７〕
前記認証モジュールは、第一復号鍵を用いて前記第一認証情報を復号して認証すべく構成される、態様２５に記載のデバイス。
〔態様２８〕
前記第二認証情報は、事前に前記認証サーバおよび前記セキュリティ情報アプリケーションにより合意された第二鍵情報を備えて成り、前記第二鍵情報は第二暗号鍵および第二復号鍵を備えて成り、前記署名済み基準情報は前記第二暗号鍵を用い前記セキュリティ情報アプリケーションにより署名されており、且つ、
前記認証モジュールは、事前に合意された前記第二鍵情報に従い、事前に前記セキュリティ情報アプリケーションにより合意された前記第二復号鍵を用いて、前記第二認証情報を認証するために前記署名済み基準情報を復号すべく構成される、
態様２５記載のデバイス。
〔態様２９〕
情報認証デバイスであって、
認証対象情報に対する照合要求を認証サーバに対して送信すべく構成された登録要求モジュールと、
前記認証サーバによりフィードバックされた第一認証情報を受信すべく構成された受信モジュールと、
認証対象情報獲得要求を生成し、該認証対象情報獲得要求および前記第一認証情報をセキュリティ情報アプリケーションに対して送信し、且つ、前記セキュリティ情報アプリケーションが前記第一認証情報の認証を承認した後、前記セキュリティ情報アプリケーションにより返信された認証対象情報と該認証対象情報の認証対象身分識別子とを獲得すべく構成された獲得モジュールと、
前記認証対象情報、前記認証対象身分識別子、および、前記第一認証情報を前記認証サーバに対して送信することで、該認証サーバにより、前記第一認証情報、前記認証対象身

分識別子、および、前記認証対象情報を認証させ、認証結果を生成させ、且つ、前記認証結果を前記ビジネス・アプリケーションに対してフィードバックさせるべく構成された送信モジュールと、
を備えて成る情報認証デバイス。
〔態様３０〕
情報認証デバイスであって、
ビジネス・アプリケーションにより送信され且つ第一認証情報を担持する認証対象情報獲得要求を受信すべく構成された受信モジュールと、
前記第一認証情報を認証し、且つ、認証が承認された後、前記認証対象情報と該認証対象情報の身分識別子とを前記ビジネス・アプリケーションを介して認証サーバに対して送信することで、該認証サーバにより、前記第一認証情報、前記認証対象身分識別子、および、前記認証対象情報を認証させ、認証結果を生成させ、且つ、該認証結果を前記ビジネス・アプリケーションに対してフィードバックさせるべく構成された署名モジュールと、
を備えて成る情報認証デバイス。
〔態様３１〕
前記署名モジュールは、前記基準情報獲得要求中に担持された前記第一認証情報を認証し、前記認証が承認された後、前記認証対象情報が属する基準情報を識別し、前記基準情報に一致する身分基準を、前記認証対象情報の認証対象身分識別子として決定し、且つ、前記認証対象情報と該認証対象情報の前記認証対象身分識別子とを、前記ビジネス・アプリケーションに対して返信すべく構成される、態様３０に記載のデバイス。
〔態様３２〕
情報認証デバイスであって、
ビジネス・アプリケーションにより送信された認証対象情報に対する照合要求を受信すべく構成された認証要求受信モジュールと、
前記照合要求に従い、第一認証情報を生成し、且つ、それを前記ビジネス・アプリケーションに対してフィードバックすべく構成されたフィードバック・モジュールと、
前記ビジネス・アプリケーションにより送信された、前記認証対象情報、前記認証対象情報の認証対象身分識別子、および、前記第一認証情報を受信すべく構成された認証情報受信モジュールと、
前記第一認証情報、前記認証対象身分識別子、および、前記認証対象情報を夫々認証して、認証結果を生成し、且つ、それを前記ビジネス・アプリケーションに対してフィードバックすべく構成された認証モジュールと、
を備えて成る情報認証デバイス。
〔態様３３〕
前記認証モジュールは、前記第一認証情報に関しては、当該情報認証デバイスの第一復号鍵を用いて前記第一認証情報を復号し、且つ、復号済み証明書を認証し、前記認証対象身分識別子に関しては、登録済み基準情報に従い、前記認証対象身分識別子が登録済み基準情報の身分識別子と一致するか否かを決定し、且つ、認証のために、前記認証対象情報を前記登録済み基準情報と比較すべく構成される、態様３２に記載のデバイス。
〔態様３４〕
前記認証モジュールは、前記第一認証情報に関しては、認証が承認されたなら、前記認証対象情報および前記認証対象身分識別子を認証し、その他の場合には認証失敗の通知を返信し、前記身分識別子に関しては、認証が承認されたなら、前記認証対象情報を認証し、その他の場合には、認証失敗の通知を返信し、且つ、前記認証対象情報に関しては、認証が承認されたなら、成功の通知を返信し、その他の場合には、認証失敗の通知を返信すべく構成される、態様３３に記載のデバイス。

【図１】

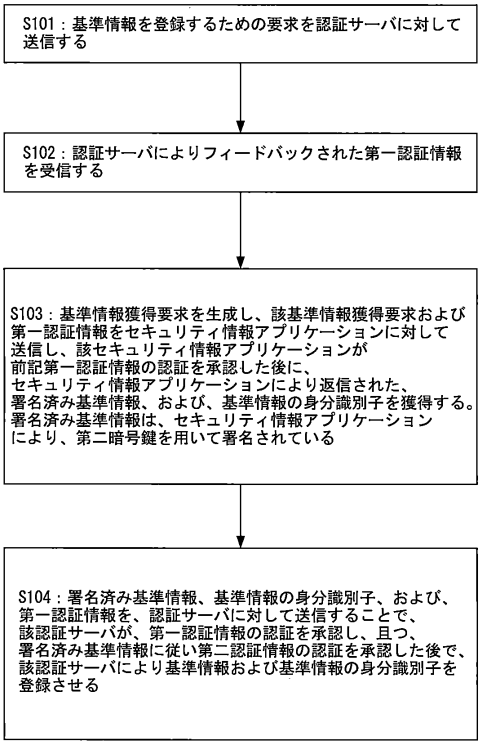

FIGURE 1

【図２】

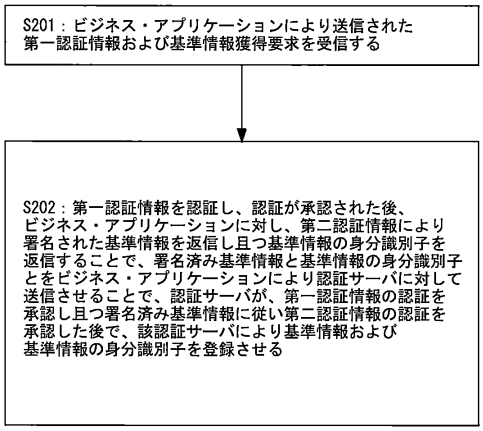

FIGURE 2

【図３】

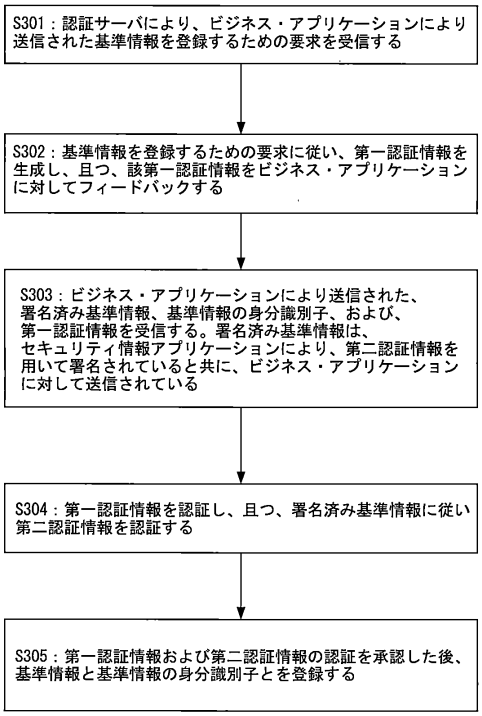

FIGURE 3

【図４】

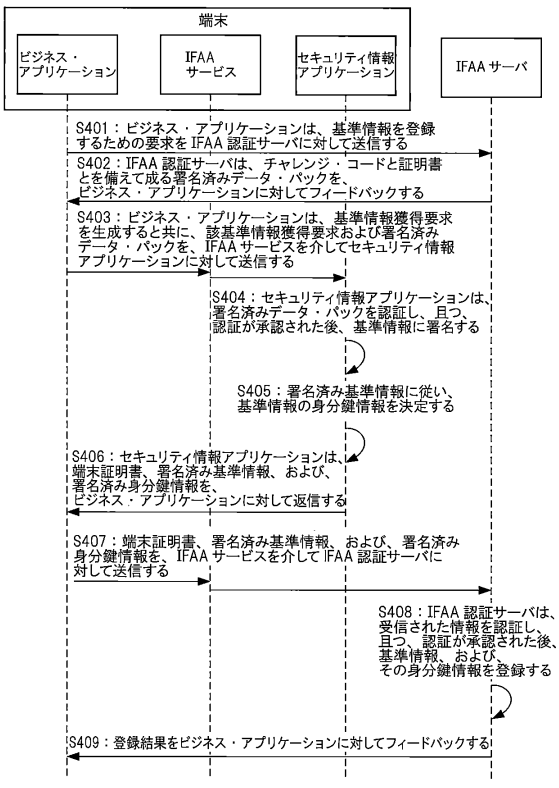

FIGURE 4

【図５】

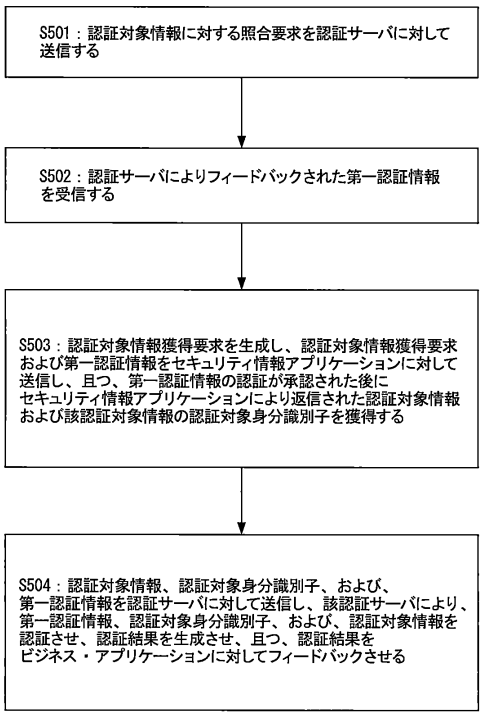

FIGURE 5

【図６】

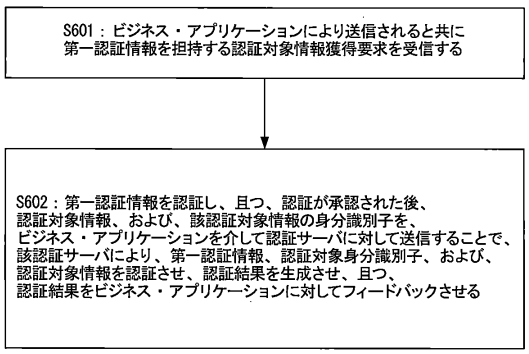

FIGURE 6

【図７】

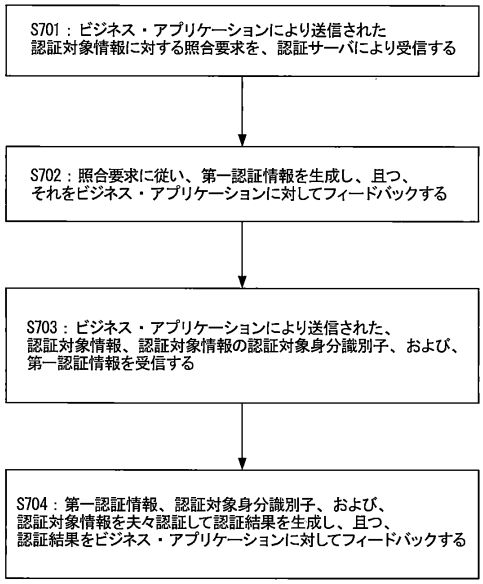

FIGURE 7

【図８】

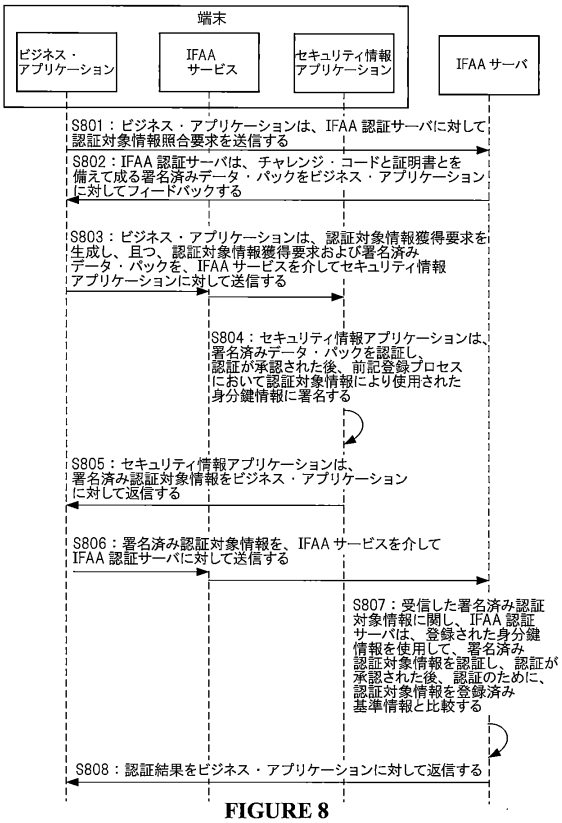

FIGURE 8

【図９】

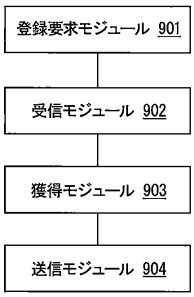

FIGURE 9

【図１０】

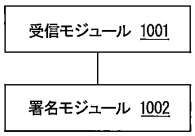

FIGURE 10

【図１１】

FIGURE 11

【図１２】

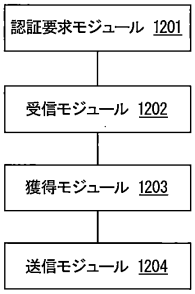

FIGURE 12

【図１３】

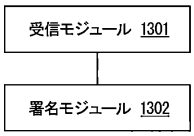

FIGURE 13

【図１４】

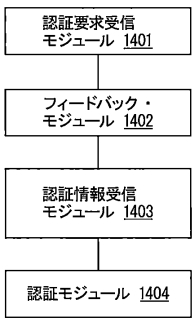

FIGURE 14

フロントページの続き

(74)代理人 100180806
弁理士 三浦 剛
(74)代理人 100141254
弁理士 榎原 正巳
(72)発明者 スン ユアンポー
中華人民共和国, ジョージアーン ３１１１２１, ハーンジョウ ユイハーン ディストリクト, ウエスト ウェンイー ロード ナンバー９６９, ビルディング ３, ５／フロア, アリババ グループ リーガル ディパートメント

審査官 青木 重徳

(56)参考文献 中国特許出願公開第１０２２１７２７７（ＣＮ, Ａ）
特開２０１３－１２２６８０（ＪＰ, Ａ）
特開２０１２－０４４６７０（ＪＰ, Ａ）
国際公開第２００７／００１０４６（WO, Ａ１）
米国特許出願公開第２０１４／０１８９８０９（ＵＳ, Ａ１）

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ ２１／３１
Ｇ０６Ｆ ２１／３３
Ｇ０９Ｃ １／００
Ｈ０４Ｌ ９／１４