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

特許第5207776号
(P5207776)

(45)発行日　平成25年6月12日(2013.6.12)　(24)登録日　平成25年3月1日(2013.3.1)

(51)Int.Cl.		F I		
G06F 21/31	(2013.01)	G06F	21/20	131A
G06F 21/32	(2013.01)	G06F	21/20	132
H04L 9/32	(2006.01)	H04L	9/00	675D
G09C 1/00	(2006.01)	G09C	1/00	640E

請求項の数 10　(全 17 頁)

(21)出願番号　特願2008-55581(P2008-55581)
(22)出願日　平成20年3月5日(2008.3.5)
(65)公開番号　特開2009-211566(P2009-211566A)
(43)公開日　平成21年9月17日(2009.9.17)
審査請求日　平成22年8月12日(2010.8.12)

(出願人による申告)平成１９年度、総務省「情報家電の高度利活用技術の研究開発」委託研究、産業技術力強化法第１９条の適用を受ける特許出願

(73)特許権者　399035766
エヌ・ティ・ティ・コミュニケーションズ株式会社
東京都千代田区内幸町一丁目１番６号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　田島　誠二
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内
(72)発明者　竹内　一雅
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内

最終頁に続く

(54)【発明の名称】認証システム、情報機器、認証方法、及びプログラム

(57)【特許請求の範囲】
【請求項１】
通信ネットワークに接続された情報機器からユーザ認証要求を受信し、ユーザ認証を行う認証システムであって、
所定の認証方式に対応した機能を備えていない第１の情報機器から、ユーザ認証要求を受信するユーザ認証要求受信手段と、
前記第１の情報機器の機器証明情報を当該第１の情報機器から受信し、当該機器証明情報を用いて前記第１の情報機器の機器認証を行う機器認証手段と、
前記所定の認証方式に対応した機能を備えていない情報機器毎に、当該情報機器の代理として前記所定の認証方式に基づくユーザ認証を行う1つ又は複数の情報機器の識別情報を優先順位とともに格納する代理認証連携情報格納手段と、
前記ユーザ認証要求に係る認証の方式が、前記所定の認証方式である場合において、前記代理認証連携情報格納手段を参照することにより、前記機器認証に成功した前記第１の情報機器の代理認証機器として、前記所定の認証方式に対応した機能を備えた第２の情報機器を決定する代理認証機器決定手段と、
前記第１の情報機器に対して、前記第２の情報機器の識別情報を含む代理認証要求依頼を通知する代理認証機器通知手段と、
前記第１の情報機器から代理認証要求を受けた前記第２の情報機器からユーザ認証情報を受信し、当該ユーザ認証情報に基づき、前記所定の認証方式に基づくユーザ認証を行い、当該ユーザ認証に成功した場合に、前記第１の情報機器からの前記ユーザ認証要求に係

るユーザ認証に成功したと判定するユーザ認証制御手段と
を備えたことを特徴とする認証システム。
【請求項２】
前記認証システムは、前記所定の認証方式に対応した機能を備えた情報機器について、当該情報機器を代理のユーザ認証に使用できるか否かを示す情報を格納する情報格納手段を備え、
前記代理認証機器決定手段は、前記情報格納手段を参照することにより、代理認証機器として決定した情報機器を使用できないと判断した場合に、前記代理認証連携情報格納手段を参照して、当該情報機器よりも優先順位の低い情報機器を選択する
ことを特徴とする請求項１に記載の認証システム。
【請求項３】
請求項１又は２に記載の認証システムにおいて使用される前記第１の情報機器として機能する情報機器であって、
前記認証システムにユーザ認証要求を送信するユーザ認証要求送信手段と、
前記認証システムから、前記所定の認証方式に基づく認証処理を行う代理認証機器として前記第２の情報機器の識別情報を含む代理認証要求依頼を受信する代理認証要求依頼受信手段と、
前記第２の情報機器の識別情報に基づき、前記第１の情報機器の代理として前記認証システムにアクセスするよう要求する代理認証要求を前記第２の情報機器に対して送信する代理認証要求手段と
を備えたことを特徴とする情報機器。
【請求項４】
通信ネットワークに接続された情報機器からユーザ認証要求を受信し、ユーザ認証を行う認証システムが実行する認証方法であって、
前記認証システムは、所定の認証方式に対応した機能を備えていない情報機器毎に、当該情報機器の代理として前記所定の認証方式に基づくユーザ認証を行う1つ又は複数の情報機器の識別情報を優先順位とともに格納する代理認証連携情報格納手段を備え、
前記所定の認証方式に対応した機能を備えていない第１の情報機器から、ユーザ認証要求を受信するユーザ認証要求受信ステップと、
前記第１の情報機器の機器証明情報を当該第１の情報機器から受信し、当該機器証明情報を用いて前記第１の情報機器の機器認証を行う機器認証ステップと、
前記ユーザ認証要求に係る認証の方式が、前記所定の認証方式である場合において、前記代理認証連携情報格納手段を参照することにより、前記機器認証に成功した前記第１の情報機器の代理認証機器として、前記所定の認証方式に対応した機能を備えた第２の情報機器を決定する代理認証機器決定ステップと、
前記第１の情報機器に対して、前記第２の情報機器の識別情報を含む代理認証要求依頼を通知する代理認証機器通知ステップと、
前記第１の情報機器から代理認証要求を受けた前記第２の情報機器からユーザ認証情報を受信し、当該ユーザ認証情報に基づき、前記所定の認証方式に基づくユーザ認証を行い、当該ユーザ認証に成功した場合に、前記第１の情報機器からの前記ユーザ認証要求に係るユーザ認証に成功したと判定するユーザ認証制御ステップと
を備えたことを特徴とする認証方法。
【請求項５】
前記認証システムは、前記所定の認証方式に対応した機能を備えた情報機器について、当該情報機器を代理のユーザ認証に使用できるか否かを示す情報を格納する情報格納手段を備え、
前記代理認証機器決定ステップにおいて、前記認証システムは、前記情報格納手段を参照することにより、代理認証機器として決定した情報機器を使用できないと判断した場合に、前記代理認証連携情報格納手段を参照して、当該情報機器よりも優先順位の低い情報機器を選択する

ことを特徴とする請求項４に記載の認証方法。
【請求項６】
認証システムと、所定の認証方式に対応した機能を備えていない第１の情報機器と、所定の認証方式に対応した機能を備えた第２の情報機器とが通信ネットワークを介して接続されたシステムにおいて実行される認証方法であって、
前記認証システムは、前記所定の認証方式に対応した機能を備えていない情報機器毎に、当該情報機器の代理として前記所定の認証方式に基づくユーザ認証を行う1つ又は複数の情報機器の識別情報を優先順位とともに格納する代理認証連携情報格納手段を備え、
前記第１の情報機器が前記認証システムにユーザ認証要求を送信するステップと、
前記第１の情報機器が当該第１の情報機器の機器証明情報を前記認証システムに送信し、当該認証システムが、当該機器証明情報を用いて前記第１の情報機器の機器認証を行う機器認証ステップと、
前記ユーザ認証要求に係る認証の方式が前記所定の認証方式である場合において、前記認証システムが、前記代理認証連携情報格納手段を参照することにより、前記機器認証に成功した前記第１の情報機器の代理認証機器として、前記第２の情報機器を決定する代理認証機器決定ステップと、
前記認証システムが、前記第１の情報機器に対して、前記第２の情報機器の識別情報を含む代理認証要求依頼を通知するステップと、
前記第１の情報機器が前記第２の情報機器に対して代理認証要求を送信するステップと、
前記代理認証要求を受信した前記第２の情報機器が、ユーザからユーザ認証情報を取得し、当該ユーザ認証情報を前記認証システムに送信するステップと、
前記認証システムが、前記ユーザ認証情報に基づき、前記所定の認証方式に基づくユーザ認証を行い、当該ユーザ認証に成功した場合に、前記第１の情報機器からの前記ユーザ認証要求に係るユーザ認証に成功したと判定するステップと
を備えたことを特徴とする認証方法。
【請求項７】
前記認証システムは、前記所定の認証方式に対応した機能を備えた情報機器について、当該情報機器を代理のユーザ認証に使用できるか否かを示す情報を格納する情報格納手段を備え、
前記代理認証機器決定ステップにおいて、前記認証システムは、前記情報格納手段を参照することにより、代理認証機器として決定した情報機器を使用できないと判断した場合に、前記代理認証連携情報格納手段を参照して、当該情報機器よりも優先順位の低い情報機器を選択する
ことを特徴とする請求項６に記載の認証方法。
【請求項８】
コンピュータを、通信ネットワークに接続された情報機器からユーザ認証要求を受信し、ユーザ認証を行う認証システムとして機能させるプログラムであって、
前記コンピュータは、所定の認証方式に対応した機能を備えていない情報機器毎に、当該情報機器の代理として前記所定の認証方式に基づくユーザ認証を行う1つ又は複数の情報機器の識別情報を優先順位とともに格納する代理認証連携情報格納手段を備え、前記コンピュータを、
所定の認証方式に対応した機能を備えていない第１の情報機器から、ユーザ認証要求を受信するユーザ認証要求受信手段、
前記第１の情報機器の機器証明情報を当該第１の情報機器から受信し、当該機器証明情報を用いて前記第１の情報機器の機器認証を行う機器認証手段、
前記ユーザ認証要求に係る認証の方式が、前記所定の認証方式である場合において、前記代理認証連携情報格納手段を参照することにより、前記機器認証に成功した前記第１の情報機器の代理認証機器として、前記所定の認証方式に対応した機能を備えた第２の情報機器を決定する代理認証機器決定手段、

前記第１の情報機器に対して、前記第２の情報機器の識別情報を含む代理認証要求依頼を通知する代理認証機器通知手段、
前記第１の情報機器から代理認証要求を受けた前記第２の情報機器からユーザ認証情報を受信し、当該ユーザ認証情報に基づき、前記所定の認証方式に基づくユーザ認証を行い、当該ユーザ認証に成功した場合に、前記第１の情報機器からの前記ユーザ認証要求に係るユーザ認証に成功したと判定するユーザ認証制御手段、
として機能させるためのプログラム。
【請求項９】
前記コンピュータは、前記所定の認証方式に対応した機能を備えた情報機器について、当該情報機器を代理のユーザ認証に使用できるか否かを示す情報を格納する情報格納手段を備え、
前記代理認証機器決定手段は、前記情報格納手段を参照することにより、代理認証機器として決定した情報機器を使用できないと判断した場合に、前記代理認証連携情報格納手段を参照して、当該情報機器よりも優先順位の低い情報機器を選択する
ことを特徴とする請求項８に記載のプログラム。
【請求項１０】
コンピュータを、請求項１又は２に記載の認証システムにおいて使用される前記第１の情報機器として機能させるプログラムであって、コンピュータを、
前記認証システムにユーザ認証要求を送信するユーザ認証要求送信手段、
前記認証システムから、前記所定の認証方式に基づく認証処理を行う代理認証機器として前記第２の情報機器の識別情報を含む代理認証要求依頼を受信する代理認証要求依頼受信手段、
前記第２の情報機器の識別情報に基づき、前記コンピュータである前記第１の情報機器の代理として前記認証システムにアクセスするよう要求する代理認証要求を前記第２の情報機器に対して送信する代理認証要求手段、
として機能させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ユーザが、ネットワークアクセス機能を有する情報機器を用いてネットワークサービスを利用する際に必要となるユーザ認証に関するものであり、特に、特定の認証方式に対応していない情報機器から、当該特定の認証方式に基づくユーザ認証を必要とするネットワークサービスを利用する場合でも、ユーザ認証を行って当該ネットワークサービスを利用することを可能にする技術に関するものである。
【背景技術】
【０００２】
インターネット等の通信ネットワークへのアクセス機能を持つ情報家電機器が増加してきている。例えば、ビデオカメラ等の情報家電機器がインターネットに接続することにより、インターネット上で提供されるストレージサービスを利用して映像を保存し、保存した映像を他の情報家電機器を使用して視聴するといったことが可能となり、情報家電機器の利便性が向上する。
【０００３】
上記のストレージサービスのようなネットワークサービスでは一般に予め登録されたユーザアカウントに基づきサービスの提供がなされることから、サービスの利用に際してユーザ認証が必要になる。
【０００４】
情報家電機器等の認証処理に関する従来技術としては特許文献１に記載された技術がある。特許文献１に記載された技術では、情報機器に安全な方法で機器認証情報を組み込んでおき、認証システムが情報機器から送られる機器認証情報を用いて機器認証を行い、更に、ユーザが情報機器にパスワードを入力することにより認証システムでユーザ認証を行

っている。
【特許文献１】特開２００４－３５５３９６号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
さて、一般に、ネットワークサービスではパスワードによりユーザ認証がなされる場合が多いが、サービス提供者側が特に高いセキュリティを必要とする場合には、ユーザ認証としてICカード認証や生態認証等の認証（高セキュリティ認証と呼ぶ）が要求される場合がある。
【０００６】
パスワードであれば、リモコン等の操作手段を用いることにより、ほとんどの情報家電機器から入力することが可能である。しかし、ICカード認証や生態認証等の高セキュリティ認証については、このような認証手段を持つ情報家電機器は限られている。
【０００７】
従って、たとえユーザ宅内に高セキュリティ認証に対応した情報家電機器があったとしても、ユーザが特定のネットワークサービスを利用するために用いたいと考える情報家電機器は高セキュリティ認証に対応していない場合が多く発生すると考えられる。このような場合、ユーザは高セキュリティ認証を必要とするネットワークサービスを利用できなくなってしまう。
【０００８】
本発明は上記の点に鑑みてなされたものであり、所定の認証方式に対応した情報家電機器を代理認証機器として利用することにより、所定の認証方式に対応していない情報家電機器からでも、当該所定の認証方式に基づくユーザ認証を必要とするネットワークサービスを利用することを可能にする技術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】
【０００９】
上記の課題を解決するために、本発明は、通信ネットワークに接続された情報機器からユーザ認証要求を受信し、ユーザ認証を行う認証システムであって、所定の認証方式に対応した機能を備えていない第１の情報機器から、ユーザ認証要求を受信するユーザ認証要求受信手段と、前記第１の情報機器の機器証明情報を当該第１の情報機器から受信し、当該機器証明情報を用いて前記第１の情報機器の機器認証を行う機器認証手段と、前記所定の認証方式に対応した機能を備えていない情報機器毎に、当該情報機器の代理として前記所定の認証方式に基づくユーザ認証を行う1つ又は複数の情報機器の識別情報を優先順位とともに格納する代理認証連携情報格納手段と、前記ユーザ認証要求に係る認証の方式が、前記所定の認証方式である場合において、前記代理認証連携情報格納手段を参照することにより、前記機器認証に成功した前記第１の情報機器の代理認証機器として、前記所定の認証方式に対応した機能を備えた第２の情報機器を決定する代理認証機器決定手段と、前記第１の情報機器に対して、前記第２の情報機器の識別情報を含む代理認証要求依頼を通知する代理認証機器通知手段と、前記第１の情報機器から代理認証要求を受けた前記第２の情報機器からユーザ認証情報を受信し、当該ユーザ認証情報に基づき、前記所定の認証方式に基づくユーザ認証を行い、当該ユーザ認証に成功した場合に、前記第１の情報機器からの前記ユーザ認証要求に係るユーザ認証に成功したと判定するユーザ認証制御手段とを備えたことを特徴とする認証システムとして構成される。
【００１０】
前記認証システムは、前記所定の認証方式に対応した機能を備えた情報機器について、当該情報機器を代理のユーザ認証に使用できるか否かを示す情報を格納する情報格納手段を備え、前記代理認証機器決定手段は、前記情報格納手段を参照することにより、代理認証機器として決定した情報機器を使用できないと判断した場合に、前記代理認証連携情報格納手段を参照して、当該情報機器よりも優先順位の低い情報機器を選択するようにしてもよい。

【００１１】
また、本発明は、前記認証システムにおいて使用される前記第１の情報機器として機能する情報機器であって、前記認証システムにユーザ認証要求を送信するユーザ認証要求送信手段と、前記認証システムから、前記所定の認証方式に基づく認証処理を行う代理認証機器として前記第２の情報機器の識別情報を含む代理認証要求依頼を受信する代理認証要求依頼受信手段と、前記第２の情報機器の識別情報に基づき、前記第１の情報機器の代理として前記認証システムにアクセスするよう要求する代理認証要求を前記第２の情報機器に対して送信する代理認証要求手段とを備えたことを特徴とする情報機器として構成することもできる。
【００１２】
また、本発明は、認証システムと、所定の認証方式に対応した機能を備えていない第１の情報機器と、所定の認証方式に対応した機能を備えた第２の情報機器とが通信ネットワークを介して接続されたシステムにおいて実行される認証方法であって、前記認証システムは、前記所定の認証方式に対応した機能を備えていない情報機器毎に、当該情報機器の代理として前記所定の認証方式に基づくユーザ認証を行う1つ又は複数の情報機器の識別情報を優先順位とともに格納する代理認証連携情報格納手段を備え、前記第１の情報機器が前記認証システムにユーザ認証要求を送信するステップと、前記第１の情報機器が当該第１の情報機器の機器証明情報を前記認証システムに送信し、当該認証システムが、当該機器証明情報を用いて前記第１の情報機器の機器認証を行う機器認証ステップと、前記ユーザ認証要求に係る認証の方式が前記所定の認証方式である場合において、前記認証システムが、前記代理認証連携情報格納手段を参照することにより、前記機器認証に成功した前記第１の情報機器の代理認証機器として、前記第２の情報機器を決定する代理認証機器決定ステップと、前記認証システムが、前記第１の情報機器に対して、前記第２の情報機器の識別情報を含む代理認証要求依頼を通知するステップと、前記第１の情報機器が前記第２の情報機器に対して代理認証要求を送信するステップと、前記代理認証要求を受信した前記第２の情報機器が、ユーザからユーザ認証情報を取得し、当該ユーザ認証情報を前記認証システムに送信するステップと、前記認証システムが、前記ユーザ認証情報に基づき、前記所定の認証方式に基づくユーザ認証を行い、当該ユーザ認証に成功した場合に、前記第１の情報機器からの前記ユーザ認証要求に係るユーザ認証に成功したと判定するステップとを備えたことを特徴とする認証方法として構成してもよい。

【００１３】
更に、本発明は、上記認証システムの各手段をコンピュータに実現させるプログラム、及び上記情報機器の各手段をコンピュータに実現させるプログラムとして構成することもできる。
【発明の効果】
【００１４】
本発明によれば、所定の認証方式に対応した機能を備えていない第１の情報機器から、所定の認証方式に係るユーザ認証要求を受信した場合でも、第１の情報機器の代理認証機器として、所定の認証方式に対応した機能を備えた第２の情報機器を決定し、第２の情報機器で所定の認証方式に対応したユーザ認証処理を行うようにし、第２の情報機器でのユーザ認証に成功した場合に、第１の情報機器からのユーザ認証要求に係るユーザ認証に成功したと判定することとしたので、所定の認証方式に対応していない情報機器からでも、所定の認証方式に基づくユーザ認証を必要とするネットワークサービスを利用することが可能となる。
【発明を実施するための最良の形態】
【００１５】
以下、図面を参照して、本発明の実施の形態について説明する。
（システム構成及び動作シーケンス）

図１に本発明の実施の形態におけるシステム構成を示す。図１に示すように、本実施の形態におけるシステムは、生体認証（本実施の形態では一例として指紋認証とする）を行うための機能を備えた情報家電機器Ａ、生体認証を行うための機能を備えていない情報家電機器Ｂ、ユーザ認証等を行う認証システム１、及び、ネットワークサービスを提供するサービス提供システム２を有している。情報家電機器Ａ及び情報家電機器Ｂは例えば家庭内に配置され、家庭内ＬＡＮ等の通信ネットワーク３に接続され、通信ネットワーク３を介して互いに通信を行うことが可能である。

【００１６】

認証システム１、サービス提供システム２、及び通信ネットワーク３は、インターネット等の通信ネットワーク４に接続されている。認証システム１及びサービス提供システム２は、これらの通信ネットワークを介して情報家電機器Ａ及び情報家電機器Ｂと通信を行うことが可能である。

【００１７】

次に、図２に示すシーケンスチャートを参照して、本実施の形態における全体の処理の流れの例を説明し、その後に、装置の機能構成及び動作、テーブル構成等について詳細に説明することにする。

【００１８】

図２に示すシーケンスチャートの例は、ユーザが生体認証機能を備えていない情報家電機器Ｂを利用して、サービス提供システム２により提供されるネットワークサービスを利用しようとする場合の例であり、サービス提供システム２が提供するネットワークサービスを利用するには生体認証（指紋認証）が必要であるものとする。また、サービス提供システム２のためのユーザ認証を認証システム１が行うものとする。

【００１９】

まず、情報家電機器Ｂは、サービス提供システム２が提供するサービスを利用するための認証要求を認証システム１に送信する（ステップ１）。

【００２０】

より具体的には、例えば、ユーザが情報家電機器Ｂを用いてサービス提供システム２にアクセスするための操作を行うことにより、情報家電機器Ｂはサービス提供システム２にサービス利用のための認証要求を送信し、サービス提供システム２は、認証要求を含むリダイレクト要求を情報家電機器Ｂに送信し、そのリダイレクト要求に基づき、情報家電機器Ｂは認証要求を認証システム１に送信する。また、認証システム１がネットワークサービス提供機能を含む場合等には、上記のようなリダイレクトをすることなく、ユーザ操作に基づき情報家電機器Ｂが認証システム１にサービス利用のための認証要求を送ることとしてもよい。

【００２１】

また、ステップ１で、サービス提供システム２が提供するサービスを利用するための認証要求を受信した認証システム１は、当該サービスの提供のためには生体認証が必要であると判断する。この判断は、例えば、認証システム１がサービスサイト毎の認証方式の種類をデータベースに保持しておくことで実現される。

【００２２】

情報家電機器Ｂから認証要求を受信した認証システム１は、情報家電機器Ｂに対する機器認証を実施する（ステップ２）。具体的には、例えば、認証システム１は、情報家電機器Ｂにデジタル証明書の送信を要求し、情報家電機器Ｂが認証システム１にデジタル証明書を送信し、認証システム１が、情報家電機器Ｂから受信したデジタル証明書を用いて情報家電機器Ｂに対するクライアント認証を行う。この処理により、認証システム１と情報家電機器Ｂとの間で共通鍵が共有され、ＳＳＬ等の暗号通信路が設定される。

【００２３】

情報家電機器Ｂの機器認証に成功した認証システム１は、ユーザＩＤ確認要求を情報家電機器Ｂに送信する（ステップ３）。ユーザＩＤ確認要求には、情報家電機器Ｂの使用を許可されたユーザのＩＤのリストが含まれる。ユーザＩＤ確認要求を受信した情報家電機

器Ｂは、例えば図３（ａ）に示すような、リストに含まれるユーザの中から特定のユーザを選択させるための画面を情報家電機器Ｂの表示部に表示する。

【００２４】

ユーザ（本実施形態では、ＩＤが"０１"のユーザ１であるものとする）が、この画面から自分を選択すると、そのユーザＩＤが認証システム１に送信される（ステップ４）。

【００２５】

認証システム１は、後述するテーブルデータを参照することにより、情報家電機器Ｂは生体認証を行うための機能を持たないこと、及び、情報家電機器Ｂの代理としてユーザ１の生体認証を行う情報家電機器Ａ（代理認証機器と呼ぶ）が存在することを確認する（ステップ５）。

【００２６】

次に、認証システム１は、情報家電機器Ｂに対して代理認証要求依頼を送信する（ステップ６）。この代理認証要求依頼には、情報家電機器Ｂにおいて表示される画面データと、代理認証機器を指定するデータである情報家電機器Ａの識別情報と、情報家電機器Ａが認証のためにアクセスするアクセス先情報（認証システム１のＵＲＬ等）が含まれる。

【００２７】

情報家電機器Ｂは、認証システム１から送信された代理認証要求依頼を受信し、代理認証要求依頼に含まれる画面データに基づき、例えば図３（ｂ）に示す画面を表示する。なお、ここで、情報家電機器Ａで生体認証を行うことを示す画面の中に確認のためのボタン（開始ボタン等）を設け、そのボタンが押されたときに、次の処理（情報家電機器Ａへの代理認証要求送信処理）に進むようにしてもよい。

【００２８】

情報家電機器Ｂは、図３（ｂ）に示す画面を表示するとともに、情報家電機器Ａの識別情報を用いて情報家電機器Ａに接続し、情報家電機器Ａに対して、情報家電機器Ｂの代理として認証システム１にアクセスし、ユーザ１の生体認証を行うことを要求する代理認証要求を送信する（ステップ７）。当該代理認証要求には、認証システム１のＵＲＬと、情報家電機器Ｂの識別情報と、ユーザ１のＩＤが含まれる。

【００２９】

情報家電機器Ａの識別情報は、通信ネットワーク内で情報家電機器Ａを識別するための情報であり、例えば、アドレス、名前等である。識別情報が名前である場合、名前から情報家電機器Ａのアドレスを取得するための機能（アドレス解決機能）が通信ネットワーク３内に備えられる。そのような機能として例えば、ＵＰｎＰ（Universal Plug and Play）があり、その場合、情報家電機器Ａと情報家電機器ＢがそれぞれＵＰｎＰの機能を備え、ステップ７において、情報家電機器Ｂがブロードキャストにより情報家電機器Ａの識別情報を名前として持つ機器を通信ネットワーク内に問い合わせ、情報家電機器Ａから応答を受けることにより、情報家電機器Ａにアクセスすることが可能になる。

【００３０】

情報家電機器Ｂから代理認証要求を受信した情報家電機器Ａは、代理認証要求に含まれるＵＲＬ（認証システム１）にアクセスし、認証要求を送信する（ステップ８）。この認証要求には、この認証要求が、情報家電機器Ｂを利用するユーザ１を認証するためのものであることを示す情報を含む（少なくとも情報家電機器Ｂの識別情報及びユーザ１のユーザＩＤ０１を含む）。

【００３１】

情報家電機器Ａから認証要求を受信した認証システム１は、ステップ２における処理と同様にして、情報家電機器Ａに対する機器認証を行う（ステップ９）。

【００３２】

認証システム１は、情報家電機器Ａに対する機器認証に成功すると、情報家電機器Ａに対してユーザ認証情報要求を送信する（ステップ１０）。このユーザ認証情報要求には、情報家電機器Ａにおける生体認証のための機能を動作させる指示が含まれる。ユーザ認証情報要求を受信した情報家電機器Ａは、例えば図３（ｃ）に示す画面を表示する。また、

情報家電機器Ａは、生体認証機能部（指紋読み取り部等）を発光させてもよい。

【００３３】

ユーザＡは、情報家電機器Ａの生体認証機能部に指をかざす。これにより、生体認証機能部により指紋情報（ユーザ認証情報）が読み取られ、それが情報家電機器Ａから認証システム１に送信される（ステップ１１）。

【００３４】

認証システム１は、受信したユーザ認証情報を用いてユーザ１に対する認証を行い、認証に成功する（ステップ１２）。認証システム１は、後述するテーブルを参照して、情報家電機器Ａから行われたユーザ１に対する生体認証が、情報家電機器Ｂの代理で行われていることを確認すると、情報家電機器Ｂを利用するユーザ１のユーザ認証が成功したと判定する。つまり、ステップ１において情報家電機器Ｂから受信する認証要求に対するユーザ認証が成功したと判定する。

【００３５】

その後、認証システム１は、情報家電機器Ｂの識別情報を含む認証成功通知を情報家電機器Ａに送信する（ステップ１３）。情報家電機器Ａは、ステップ７での情報家電機器Ｂからの代理認証要求に対する応答として、代理認証が成功したことを示す情報を含む制御応答を情報家電機器Ｂに送信する（ステップ１４）。

【００３６】

当該制御応答を受信した情報家電機器Ｂは、サービス提供システム２にアクセスする（ステップ１５）。ここでは、例えば、ステップ１４において情報家電機器Ａは、情報家電機器Ｂを自動的にサービス提供システム２にアクセスさせる情報（リダイレクト要求）と、ユーザ認証が成功したことを示す情報とを制御応答に含めて情報家電機器Ｂに送信し、情報家電機器Ｂは、上記リダイレクト要求に基づき、ユーザ認証が成功したことを示す情報を含むサービス利用要求をサービス提供システム２に送信する。

【００３７】

また、ステップ１５の中で、情報家電機器Ｂがまず認証システム１にアクセスし、認証システム１が、テーブルを参照することにより情報家電機器Ｂについてユーザ認証が成功していると判定し、ユーザ認証が成功であったことを示す認証成功情報と、サービス提供システム２にアクセスするためのリダイレクト要求とを情報家電機器Ｂに送信し、情報家電機器Ｂが、そのリダイレクト要求に基づき、認証成功情報を含むサービス利用要求をサービス提供システム２に送ることとしてもよい。ステップ１５の後、サービス提供システム２から情報家電機器Ｂに対してサービス提供がなされる（ステップ１６）。

【００３８】

なお、認証システム１がサービス提供システム２のためにユーザ認証を行う方式としては種々の方式があり、本発明は特定の方式に限定されるものではない。

【００３９】

（装置構成）

次に、情報家電機器Ａ、Ｂと認証システム１の機能構成例について説明する。図４に情報家電機器Ｂの機能構成図を示す。図４に示すように、情報家電機器Ｂは、情報家電本来の機能を提供する本体部１１、通信ネットワークを介してデータ通信を行うためのネットワーク通信部１２、本実施の形態における機器認証や代理認証を行うために必要な処理等を行う制御部１３、操作情報の入力を行うための入力部１４、各種画面を表示する表示部１５、及び本実施の形態における処理に用いるデータを格納するデータ格納部１６を備える。

【００４０】

図２を参照して説明した情報家電機器Ｂにより実行されるデータ送受信処理は制御部１３により行われる。つまり、制御部１３は、認証システム１にユーザ認証要求を送信するユーザ認証要求送信手段と、認証システム１から、生体認証方式に基づく認証処理を行う代理認証機器として情報家電機器Ａの識別情報を含む代理認証要求依頼を受信する代理認証要求依頼受信手段と、情報家電機器Ａの識別情報に基づき、情報家電機器Ｂの代理とし

て認証システム１にアクセスするよう要求する代理認証要求を情報家電機器Ａに対して送信する代理認証要求手段とを有する。

【００４１】

情報家電機器Ｂは、ＣＰＵと記憶装置等を有するコンピュータの機能を備えており、制御部１３の機能は、当該コンピュータにプログラムを実行させることにより実現される。当該プログラムは情報家電機器Ｂに可搬メモリ等の記録媒体から予めインストールしておくこととしてもよいし、図２に示す処理の中で、当該プログラムを認証システム１からダウンロードすることとしてもよい。

【００４２】

情報家電機器Ａの構成を図５に示す。情報家電機器Ａは、情報家電機器Ｂに生体認証機能部１７が追加された構成を有しており、その他の構成は情報家電機器Ａと同じである。ただし、図２で説明したように、情報家電機器Ａが実行する処理は、情報家電機器Ｂが実行する処理と異なる。

【００４３】

図６に認証システム１の機能構成図を示す。図６に示すように、認証システム１は、通信ネットワークを介してデータ通信を行うためのネットワーク通信部３１、機器認証を行うための機器認証部３２、ユーザ認証を行うためのユーザ認証部３３、認証結果に基づくテーブルデータの更新や、代理認証機器の決定、代理認証機器の通知、代理認証要求元の認証成功判定等を行う認証制御部３４、及び、認証に関する登録情報や各種テーブルデータを格納する格納手段であるデータ格納部３５を備えている。機器認証部３２、ユーザ認証部３３、認証制御部３４はそれぞれ適宜データ格納部３５に格納されたデータを参照して処理を行う。また、特に、認証制御部３４は、情報家電機器Ｂの代理認証機器として、生体認証機能を備えた情報家電機器Ａを決定する代理認証機器決定手段と、情報家電機器Ｂに対して、情報家電機器Ａの識別情報を含む代理認証要求依頼を通知する代理認証機器通知手段と、情報家電機器Ｂから代理認証要求を受けた情報家電機器Ａからユーザ認証情報を受信し、当該ユーザ認証情報に基づきユーザ認証を行い、当該ユーザ認証に成功した場合に、情報家電機器Ｂからのユーザ認証要求に係るユーザ認証に成功したと判定するユーザ認証制御手段とを含んでいる。

【００４４】

認証システム１は、例えば通信機能を持つコンピュータを用いて実現できる。この場合、データ格納部３５は当該コンピュータの記憶装置により実現され、機器認証部３２、ユーザ認証部３３、及び認証制御部３４は当該コンピュータにプログラムを実行させることにより実現できる。当該プログラムは可搬メモリ等の記録媒体からコンピュータにインストールすることもできるし、ネットワーク上のサーバからダウンロードすることもできる。また、認証システム１を複数台のコンピュータで実現してもよい。例えば、データ格納部３５をデータベースサーバとし、その他の部分を認証処理サーバとしてもよい。

【００４５】

（テーブルの詳細）

図７に、データ格納部３５に格納される主要なテーブルの例を示す。図７に示すように、データ格納部３５は、機器認証状態テーブル（図７（ａ））、機器利用可能ユーザ情報テーブル（図７（ｂ））、ユーザ認証状態テーブル（図７（ｃ））、代理認証連携情報テーブル（図７（ｄ））を少なくとも格納する。

【００４６】

図７（ａ）に示す機器認証状態テーブルは、情報家電機器の識別情報毎にその機器が機器認証済みか否かを示す情報を格納するテーブルである。図２で示したシーケンスにおいて、ある情報家電機器に対して機器認証が成功した場合に、当該機器の識別情報に対して"認証済み"が設定される。また、当該機器によるネットワークサービスサイトとの通信のセッションが終了すれば"未認証"になる。

【００４７】

図７（ｂ）に示す機器利用可能ユーザ情報テーブルは、情報家電機器の識別情報毎に当

該機器を利用できるユーザのＩＤを格納するテーブルである。図７（ｂ）の例では、例えば、ＩＤが０１、０２、０３のユーザが機器Ａを利用できることが示されている。なお、情報家電機器の識別情報（名前等）は、ユーザ側のネットワークにおいても各機器を識別することが可能な識別情報である。

【００４８】

図７（ｃ）に示すユーザ認証状態テーブルは、情報家電機器毎に、その機器が生体認証機能を有しているか否かを示す情報、その機器を利用するユーザのユーザ認証が済んでいる状態か否かを示す情報、及び、その機器がユーザ認証を代理している他の機器があるか否かを示す認証連携予約情報を格納している。

【００４９】

図７（ｄ）に示す代理認証連携情報テーブルは、ユーザ毎に、生体認証機能を持たない機器（代理認証要求機器）と、その代理認証要求機器の代理として代理認証を実行し得る代理認証実行機器と、代理認証要求機器に対応する複数の代理認証実行機器における優先順位とを対応付けて格納する。

【００５０】

（認証システム１の動作フロー）

次に、認証システム１が図２に示すシーケンスの処理を行う場合における認証システム１の動作を、テーブル図を適宜参照しながら図８、図９のフローチャートの手順に沿って説明する。

【００５１】

まず、認証システム１が情報家電機器Ｂから認証要求を受信する（ステップ２１）。認証システム１の機器認証部３２は、情報家電機器Ｂに対する機器認証処理を行う（ステップ２２）。ここでは、例えば、情報家電機器Ｂにデジタル証明書の送信を要求し、送信されてきたデジタル証明書を用いて情報家電機器Ｂの機器認証を行う。また、認証システム１は、デジタル証明書の情報に基づき、アクセスしてきた機器を識別し、機器認証状態テーブルにおける当該情報家電機器Ｂの機器認証状態を"認証済み"にする。

【００５２】

続いて、認証システム１の認証制御部３４は、機器利用可能ユーザ情報テーブルを参照し、情報家電機器Ｂを利用可能なユーザのユーザＩＤ（０１、０２、０３）を取得し、当該ユーザＩＤを含むユーザＩＤ確認要求を情報家電機器Ｂに送信し、情報家電機器Ｂを利用しているユーザのユーザＩＤ（本実施形態では、ユーザ１のＩＤ"０１"であるものとする）を受信する（ステップ２３）。認証制御部３４は、機器認証が完了した情報家電機器Ｂから受信したユーザＩＤ（０１）を情報家電機器Ｂの識別情報と対応付けて保持しておく。

【００５３】

そして、認証システム１の認証制御部３４は、情報家電機器Ｂの識別情報を用いてユーザ認証状態テーブルを参照し、情報家電機器Ｂに対応するユーザ認証状態が"未認証"であるかどうか判定する（ステップ２４）。本実施形態では、ここでは情報家電機器Ｂに対応するユーザ認証状態は"未認証"なのでステップ２５に進む。もし、ユーザ認証状態が"未認証"でなければ、例えば他のユーザが使用中である等のメッセージを送信するエラー処理を行う（ステップ４０）。

【００５４】

ステップ２５において、認証制御部３４は、ユーザ認証状態テーブルを参照して、情報家電機器Ｂに生体認証機能があるか否かを確認する(ステップ２５）。生体認証機能がある場合、生体認証処理を行う（ステップ４１）ことになるが、本実施の形態では、情報家電機器Ｂには生体認証機能がないので、ステップ２６に進む。

【００５５】

そして、認証制御部３４は、代理認証連携情報テーブルを参照し、ユーザ１（ユーザＩＤ：０１）と、代理認証要求機器としての情報家電機器Ｂとに対応する代理認証実行機器として、情報家電機器Ａと情報家電機器Ｃがあることを確認し、情報家電機器Ａと情報家

電機器Ｃのうちの優先順位の高いほうの機器である情報家電機器Ａを代理認証実行機器として決定する（ステップ２６）。

【００５６】

続いて認証制御部３４は、ユーザ認証状態テーブルにおける情報家電機器Ａ（代理認証実行機器）に対応するユーザ認証状態が"未認証"であり、なおかつ、認証連携予約が"なし"であるかどうかを確認する（ステップ２７）。本実施形態では、この時点で情報家電機器Ａに対応するユーザ認証状態が"未認証"であり、なおかつ、認証連携予約は"なし"なので、図９のステップ２８に進む。

【００５７】

図９のステップ２８において、認証制御部３４は、代理認証要求機器である情報家電機器Ｂの識別情報を、代理認証実行機器である情報家電機器Ａに対応する認証連携予約の欄に記録する（ステップ２８）。この状態にあるユーザ認証状態テーブルを図１０（ａ）に示す。認証連携予約の欄に情報家電機器の識別情報が記録されていることは、その欄に対応する情報家電機器（図１０（ａ）の場合では情報家電機器Ａ）が、その欄に記録されている情報家電機器（図１０（ａ）の例では情報家電機器Ｂ）に対する代理認証を行うことが予約されていることを示す。

【００５８】

続いて、認証制御部３４は、情報家電機器Ｂに対して、決定された代理認証実行機器（情報家電機器Ａ）の識別情報と、認証を行うためのアクセス先（認証システムのＵＲＬ等）とを含む代理認証要求依頼を情報家電機器Ｂに送信する（ステップ２９）。

【００５９】

図２に示したステップ７の処理を経て、認証システム１は、情報家電機器Ａから認証要求を受信する（ステップ３０）。前述したとおり、この認証要求には、この認証要求が、情報家電機器Ｂを利用するユーザ１を認証するためのものであることを示す情報を含む（少なくとも情報家電機器Ｂの識別情報及びユーザ１のユーザＩＤ０１を含む）。

【００６０】

認証要求を受信した認証システム１は、機器認証部３２において情報家電機器Ａに対する機器認証を行い、ユーザ認証部３３がユーザ認証情報要求を情報家電機器Ａに送信する（ステップ３１、３２）。そして、認証システム１のユーザ認証部３３は、情報家電機器Ａからユーザ１のユーザ認証情報（指紋情報）を受信し、ユーザ１のユーザＩＤとそのユーザ認証情報を用いてデータ格納部３５を検索することによりユーザ認証を行う（ステップ３３）。なお、この例では、特定のユーザＩＤに対応する指紋情報があるか否かを判定する処理を行っているが、ユーザＩＤを用いず、指紋情報がデータ格納部３５にあるか否かを判定することによりユーザ認証を行う処理とすることもできる。

【００６１】

ここではユーザ認証に成功する。そして、情報家電機器Ａを用いたユーザ認証に成功したことを示す情報がユーザ認証部３２から認証制御部３４に通知され、認証制御部３４は、ユーザ認証状態テーブルにおける情報家電機器Ａに対応する認証連携予約の欄に情報家電機器Ｂの識別情報"Ｂ"が記録されていることを確認することにより、情報家電機器Ｂを利用するユーザ１のユーザ認証が成功したと判定する。つまり、情報家電機器Ｂから受信する認証要求に対するユーザ認証が成功したと判定する。

【００６２】

そして、認証制御部３４は、ユーザ認証状態テーブルにおける情報家電機器Ａに対応するユーザ認証状態を"未認証"から、ユーザ１のユーザＩＤである"０１"とするとともに、ユーザ認証状態テーブルにおける情報家電機器Ｂに対応するユーザ認証状態を、"未認証"からユーザ１のユーザＩＤである"０１"とする（ステップ３４）。これにより、情報家電機器Ｂにおいてユーザ１の認証がＯＫになったことが記録されたことになる。この状態に対応するユーザ認証状態テーブルを図１０（ｂ）に示す。

【００６３】

そして、認証制御部３４は、ネットワーク通信部３１を介して、情報家電機器Ａに対し

て情報家電機器Ｂの識別情報を含む認証成功通知を送信する（ステップ３５）。そして、図２に示したステップ１４の処理を経て、例えば、認証システム１が、情報家電機器Ｂからユーザ１に係るサービス提供システム２へのアクセス要求を受信し、認証システム１がユーザ認証状態テーブルを参照して、情報家電機器Ｂにおいてユーザ１は認証がＯＫであることを確認し、サービス提供システム２へのリダイレクト要求を情報家電機器Ｂに送信する。これにより、情報家電機器Ｂはサービス提供システム２にアクセスし、サービスの提供を受ける。

【００６４】

次に、ステップ２７における判断がＮｏである場合の例を説明する。ここでは、ステップ２７の時点で、既に情報家電機器Ａからユーザ３が生体認証を行い、ネットワークサービスを利用しているものとする。この場合のユーザ認証状態テーブルを図１０（ｃ）に示す。

【００６５】

この状態では、情報家電機器Ｂの代理認証機器として情報家電機器Ａを使用することはできない。そこで、図８のステップ４２において、認証制御部３４は、情報家電機器Ｂの代理認証機器として優先順位が情報家電機器Ａよりも低い情報家電機器Ｃを代理認証連携情報テーブルから選択し（ステップ４２のＹｅｓ）、ステップ２７の処理を再度行う。この場合、情報家電機器Ｃについては、ユーザ認証状態が"未認証"であり、かつ、認証連携予約が"なし"なので、情報家電機器Ｃは、上述した情報家電機器Ａを代理認証機器として使用する場合と同様にして情報家電機器Ｂの代理認証機器として使用される。情報家電機器Ｃを情報家電機器Ｂの代理認証機器として使用して、ユーザ認証が成功した場合におけるユーザ認証状態テーブルを図１０（ｄ）に示す。

【００６６】

他の例として、ステップ２７の時点で、ユーザ認証状態テーブルが図１０（ｃ）に示す状態にある場合において、ユーザ１ではなくユーザ２が情報家電機器Ｂを用いてネットワークサービスを利用しようとしており、ステップ１からの処理を行い、ステップ２７のＮｏに至った場合を想定する。ユーザ２と、代理認証要求機器としての情報家電機器Ｂとの組み合わせに対応する代理認証実行機器は、情報家電機器Ａのみであるので、この場合は、ステップ４２において情報家電機器Ｂの代理として生体認証処理を実行する他の情報家電機器は存在しない。従って、この場合は、例えば、情報家電機器Ｂに対して利用不可を示すメッセージを送る等のエラー処理が行われる（ステップ４３）。

【００６７】

また、他の例として、ユーザ認証状態テーブルが、図１０（ｂ）に示す状態である場合、すなわち、ユーザ１が、情報家電機器Ｂの代理としての情報家電機器Ａを利用してユーザ認証に成功し、情報家電機器Ｂからネットワークサービスを利用している状態において、例えば、ユーザ３が情報家電機器Ｄを利用してサービスサイトにアクセスしようとし、ステップ１からの処理を行ってステップ２７に至った場合を想定する。

【００６８】

この場合、ステップ２６で代理認証実行機器として情報家電機器Ａが選択されるが、ステップ２７においては、ユーザ認証状態テーブルにおける情報家電機器Ａに対応する"ユーザ認証状態"は"未認証"でなく、また、認証連携予約は"なし"ではなく、また、ステップ４２において、他の代理認証機器が存在しないことからエラー処理が行われることになる。

【００６９】

ただし、この状態は、情報家電機器Ａにおいてユーザ１による生体認証処理が終了してある程度の時間が経過しており、情報家電機器Ａ自体は全く使用されていない状態である可能性がある。従って、生体認証機能を持つ情報家電機器が代理認証機器として使用され、ユーザ認証状態テーブルにおける"ユーザ認証状態"が"未認証"でなく、また、認証連携予約が"なし"ではない状態になった後に、認証制御部３４がタイマーをセットし、所定の時間が経過したら、上記"ユーザ認証状態"を"未認証"とし、また、認証連携予約を"なし"

とし、ユーザ認証の代理を受け付けるようにしてもよい。

【００７０】

なお、これまでに説明した実施の形態では、ユーザが利用する機器として情報家電機器を例にとったが、ユーザが利用する機器は情報家電機器に限られない。例えば、ネットワーク通信機能を持つＰＣや、携帯電話機等の情報機器も使用することができる。また、指紋認証を行うための機器としては、将来普及することが予想される無線LANにより家庭内LANに接続可能な指紋認証機能付き携帯端末も対象になる。

【００７１】

また、本実施の形態では、認証システム１とサービス提供システム２とが分かれている場合を例にしたが、本発明は、認証システム１とサービス提供システム２との関係を限定するものではない。例えば、認証システム１の中にサービス提供システム２が含まれる構成、認証システム１が認証機能部として１つのサービス提供サーバの中に含まれる構成等でも本発明を適用できる。

【００７２】

本発明は、上記の実施の形態に限定されることなく、特許請求の範囲内において、種々変更・応用が可能である。

【図面の簡単な説明】

【００７３】

【図１】本発明の実施の形態におけるシステム構成を示す図である。

【図２】本発明の実施の形態における処理の流れを示すシーケンスチャートである。

【図３】情報家電機器に表示される情報の例を示す図である。

【図４】情報家電機器Ｂの機能構成図である。

【図５】情報家電機器Ａの機能構成図である。

【図６】認証システム１の機能構成図である。

【図７】データ格納部３５に格納される主要なテーブルの例を示す図である。

【図８】認証システム１の動作を説明するためのフローチャートである。

【図９】認証システム１の動作を説明するためのフローチャートである。

【図１０】ユーザ認証状態テーブルの状態例を示す図である。

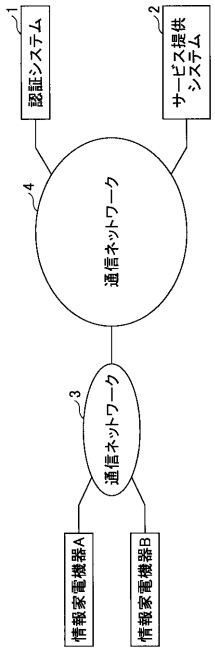
【符号の説明】

【００７４】

Ａ、Ｂ　情報家電機器
１　認証システム
２　サービス提供システム
３、４　通信ネットワーク
１１　本体部
１２　ネットワーク通信部
１３　制御部
１４　入力部
１５　表示部
１６　データ格納部
１７　生体認証機能部
３１　ネットワーク通信部
３２　機器認証部
３３　ユーザ認証部
３４　認証制御部
３５　データ格納部

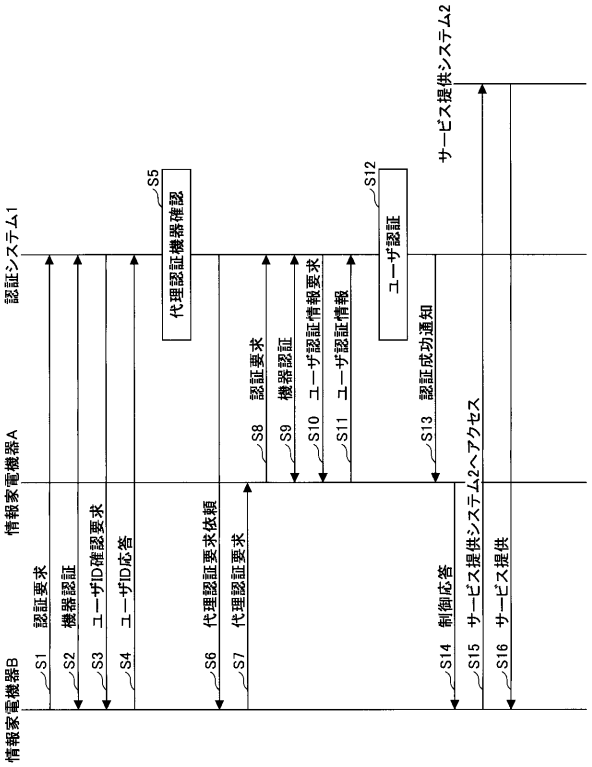
【図１】

本発明の実施の形態におけるシステム構成を示す図



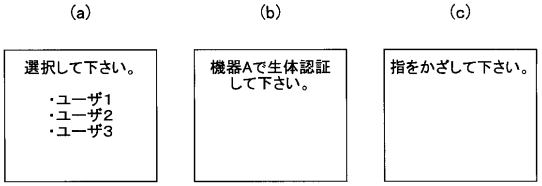
【図２】

本発明の実施の形態における処理の流れを示すシーケンスチャート



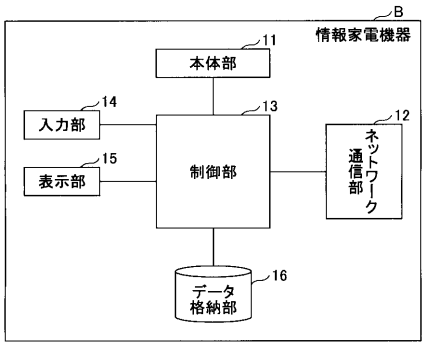
【図３】

情報家電機器に表示される情報の例を示す図



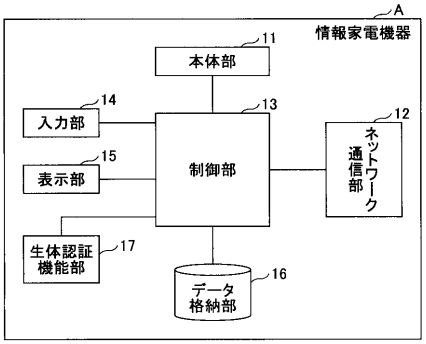
【図４】

情報家電機器Bの機能構成図



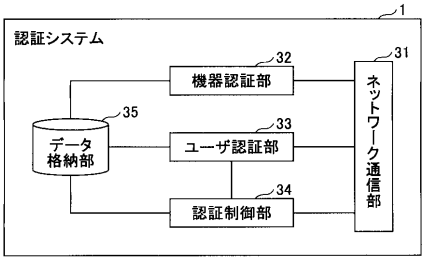
【図５】

情報家電機器Aの機能構成図



【図６】

認証システム1の機能構成図



【図７】

データ格納部35に格納される主要なテーブルの例を示す図

(a) 機器認証状態テーブル

機器	認証状態
A	認証済み
B	認証済み
C	未認証
D	未認証

(b) 機器利用可能ユーザ状態テーブル

機器	機器利用可能ユーザ			
A	01	02	03	
B	01	02	03	
C	01	02	03	
D	01		03	

(c) ユーザ認証状態テーブル

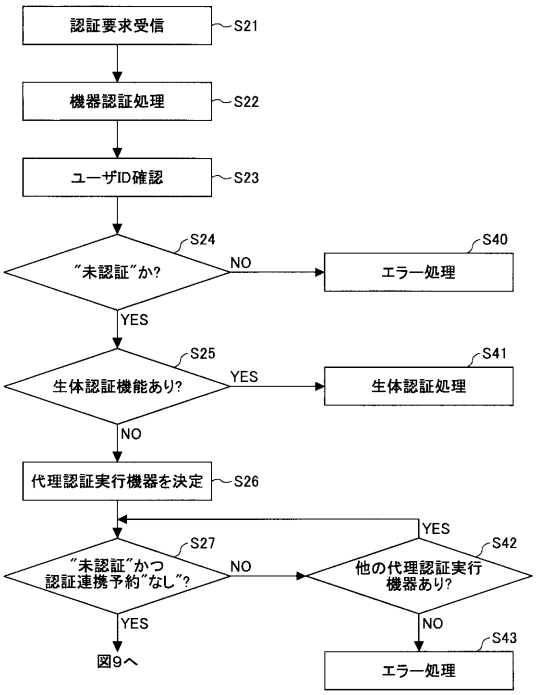
機器	生体認証	認証状態	認証連携予約
A	あり	未認証	なし
B	なし	未認証	なし
C	あり	未認証	なし
D	なし	未認証	なし

(d) 代理認証連携情報テーブル

ユーザ	代理認証要求機器	代理認証実行機器	優先順位
#1	B	A	1
		C	2
	D	A	1
		C	2
#2	B	A	1
#3	B	A	1
		C	2
	D	A	1

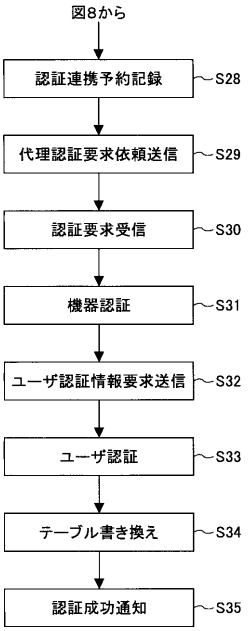
【図８】

認証システム1の動作を説明するためのフローチャート



【図９】

認証システム1の動作を説明するためのフローチャート



【図１０】

ユーザ認証状態テーブルの状態例を示す図

(a)

機器	生体認証	認証状態	認証連携予約
A	あり	未認証	B
B	なし	未認証	なし
C	あり	未認証	なし
D	なし	未認証	なし

(b)

機器	生体認証	認証状態	認証連携予約
A	あり	01	B
B	なし	01	なし
C	あり	未認証	なし
D	なし	未認証	なし

(c)

機器	生体認証	認証状態	認証連携予約
A	あり	03	なし
B	なし	未認証	なし
C	あり	未認証	なし
D	なし	未認証	なし

(d)

機器	生体認証	認証状態	認証連携予約
A	あり	03	なし
B	なし	01	なし
C	あり	01	B
D	なし	未認証	なし

フロントページの続き

(72)発明者　澤村　直行
東京都千代田区内幸町一丁目１番６号　エヌ・ティ・ティ・コミュニケーションズ株式会社内

審査官　戸島　弘詩

(56)参考文献　特開２００４－１２８５３２（ＪＰ，Ａ）
特開２００６－１４５７８５（ＪＰ，Ａ）
国際公開第２００７／１３８６６３（WO，Ａ１）
特開平０４－３４１０３５（ＪＰ，Ａ）
特開２００７－０２６２９４（ＪＰ，Ａ）
国際公開第２００７／０６４８０（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ２１／３１－２１／４３
Ｇ０９Ｃ１／００
Ｈ０４Ｋ１／００
Ｈ０４Ｌ９／００