(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4301997号
(P4301997)
(45)発行日　平成21年7月22日(2009.7.22)　(24)登録日　平成21年5月1日(2009.5.1)

(51)Int.Cl.　　F I
H04Q 9/00 (2006.01)　　H04Q 9/00 311F
H04M 11/00 (2006.01)　　H04Q 9/00 311Q
　　H04M 11/00 302

請求項の数 7　(全 25 頁)

(21)出願番号　特願2004-138698 (P2004-138698)
(22)出願日　平成16年5月7日 (2004.5.7)
(65)公開番号　特開2005-323070 (P2005-323070A)
(43)公開日　平成17年11月17日 (2005.11.17)
審査請求日　平成18年7月18日 (2006.7.18)

(73)特許権者　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100078237
弁理士　井出　直孝
(74)代理人　100083518
弁理士　下平　俊直
(72)発明者　望月　伸晃
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　渡邊　茂道
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】携帯電話による情報家電向け認証方法

(57)【特許請求の範囲】
【請求項１】
通信手段を備えた情報家電端末と、
この情報家電端末と通信する手段を備えた携帯電話端末と、
この携帯電話端末の利用者に対する前記情報家電端末またはその関連装置へのアクセス許可の認証を行う手段を備えた認証サーバと
を備えた情報家電システムに適用される認証方法において、
前記携帯電話端末から前記情報家電端末に機器特有のＩＤ番号（以後、機器ＩＤ）の取得要求を行い、
前記情報家電端末から前記機器ＩＤを前記携帯電話端末に転送し、
前記携帯電話端末から登録済みの利用者ＩＤと前記機器ＩＤを前記認証サーバに送信し、
前記認証サーバで利用者認証および機器認証が行われ、
認証に成功した場合には前記認証サーバから前記携帯電話端末に認証情報として前記関連装置を特定するアドレスおよび情報家電端末用リモコン・プログラムが送信され、
前記アドレスを前記携帯電話端末から前記情報家電端末に転送し、
前記アドレスを元に前記情報家電端末から前記関連装置への接続を行い、
前記リモコン・プログラムを用いて前記携帯電話端末を前記情報家電端末のリモコンとして用いる
ことを特徴とする認証方法。

【請求項２】
通信手段を備えた情報家電端末と、
この情報家電端末と通信する手段を備えた携帯電話端末と、
この携帯電話端末の利用者に対する前記情報家電端末またはその関連装置へのアクセス許可の認証を行う手段を備えた認証サーバと
を備えた情報家電システムに適用される認証方法において、
前記携帯電話端末から前記情報家電端末に登録済み利用者ＩＤとアクセスする前記認証サーバのアドレスとを送信すると共に、
前記情報家電端末に前記認証サーバへ機器ＩＤと前記利用者ＩＤの送信要求を行い、
前記情報家電端末から前記機器ＩＤと前記利用者ＩＤを前記認証サーバに送信し、
前記認証サーバで利用者認証および機器認証が行われ、
認証に成功した場合には前記認証サーバから前記情報家電端末に認証成功を通知すると共に、前記携帯電話端末に前記関連装置を特定するアドレスおよび情報家電端末用リモコン・プログラムが送信され、
前記アドレスを前記携帯電話端末から前記情報家電端末に転送し、
前記アドレスを元に前記情報家電端末から前記関連装置への接続を行い、
前記リモコン・プログラムを用いて前記携帯電話端末を前記情報家電端末のリモコンとして用いる
ことを特徴とする認証方法。
【請求項３】
前記情報家電端末から機器ＩＤと前記利用者ＩＤとを前記認証サーバに送信するのと併せて、
前記携帯電話端末から登録されている前記利用者ＩＤを前記認証サーバに送信し、
前記認証サーバで利用者認証および機器認証を行う
請求項２記載の認証方法。
【請求項４】
前記認証サーバには、前記携帯電話端末の利用者毎に、前記情報家電端末またはその関連装置の内で、その利用者にアクセス許可される範囲を示すアクセス制限情報があらかじめ保持され、
前記認証サーバで利用者認証および機器認証が行われる際に、前記アクセス制限された前記情報家電端末またはその関連装置を除いてアドレス許可の認証を行う
請求項１ないし３のいずれかに記載の認証方法。
【請求項５】
前記認証サーバは、装置に対するアクセス権のない利用者から当該装置への接続を要求された場合に、
前記認証サーバより登録されている当該装置の利用権の所有者に対して当該装置の利用申請を行い、
前記利用権の所有者が前記アクセス権のない利用者の当該装置への接続を認めた場合に、
前記認証サーバよりアクセス権のない利用者に認証情報として当該装置を特定するアドレスを送信する
請求項４記載の認証方法。
【請求項６】
前記携帯電話端末には前記情報家電端末の限定された一部の機能を決定する基本的なリモコン・プログラムが常時設けられ、この基本的なリモコン・プログラムによるリモコン操作に連動して、前記情報家電端末の機器ＩＤの取得要求または機器ＩＤと利用者ＩＤの送信要求が行われる
請求項１ないし５のいずれかに記載の認証方法。
【請求項７】
前記携帯電話端末において生体情報を用いて利用者の特定を行い、

前記利用者が正当な利用者ならば前記携帯電話端末から前記情報家電端末および前記認証サーバに利用者ＩＤを送信する

請求項１ないし６のいずれかに記載の認証方法。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、情報家電端末に利用する。特に、携帯電話端末を用いた認証技術に関する。

【背景技術】

【０００２】

従来のサービスまたはシステムを利用する際の認証方式は、利用者を特定するための利用者認証と機器を認証するための機器認証、さらにはそれらを組み合わせた認証とが存在する。

【０００３】

利用者認証には利用者がＩＤとパスワードを用いて認証する方式や利用者の入力を簡易にするためそれをＩＣカードで代用する方式、さらには利用者の生体情報を利用するバイオメトリクス認証方式がある。

【０００４】

機器認証には予め機器固有の情報を事前に登録しておくことで正当な機器からのサービス要求であるかどうかを認証する機器認証方式がある。また機器認証においては、その機器を所有する人と機器とを一対一に対応させておくことで機器の認証をもって利用者との認証を代替する場合もある。

【０００５】

さらにはこれら方式を組み合わせて認証を行う方式がある。

【特許文献１】特開２００２－３５４５５７号公報

【特許文献２】特開２００３－４４４４３号公報

【非特許文献１】“認証技術の基礎”、［ｏｎｌｉｎｅ］、［２００４年４月２１日検索］、インターネット＜ＵＲＬ：http://www5d.biglobe.ne.jp/~engineer/doc/security/security_ch3_02.htm＞

【非特許文献２】“本人認証記述の現状に関する調査報告書”、［ｏｎｌｉｎｅ］、２００３年３月、情報処理振興事業協会セキュリティセンター、［２００４年４月２１日検索］、インターネット＜ＵＲＬ：http://www.ipa.go.jp/security/fy14/reports/authentication/authentication2002.pdf＞

【発明の開示】

【発明が解決しようとする課題】

【０００６】

従来のサービスまたはシステムを利用する際の認証方式を情報家電端末に適用する場合には、利用者認証にＩＤとパスワードを用いる場合は、利用者がＩＤとパスワードを忘れることにより認証ができなくなる課題や利用者が故意にＩＤとパスワードを広めることでサービス提供者が不利益を被るといった課題がある。

【０００７】

また、特定のために必要なＩＤとパスワードを入力する装置自体がないために利用できないことや従来の情報家電端末の利用時には想定できない利用時の煩雑さを発生させるといった課題、さらには煩雑さのため個人によっては機器そのものの使用ができなくなるといった課題がある。

【０００８】

認証の煩雑さを軽減するために一部デジタル放送に代表されるような情報家電端末においては、ＩＣカードによるユーザ認証と機器認証を実現しているが、この方式の場合、ＩＣカードを落とした場合のリスクが有ることはもとより、各機器にＩＣカードの読み取り装置が必要となるため機器の高価格化を招くことやカードが標準的なカードでない場合、カードが機器毎に必要となり、カードを複数の持つことによるリスクが増大するといった

課題がある。

【０００９】

認証の煩雑さを軽減する別の方法としては生体情報を用いたバイオメトリクス認証を利用した機器も存在するが、情報家電端末個々にバイオメトリクス認証を搭載させた場合には、情報家電端末個々の価格が高額になることや生体情報を個々の端末に登録する場合には、個人のプライバシーに関わる情報がたくさんの機器に記憶されることになり、これはプライバシー情報の拡散の可能性を増大させるといった新たな課題を発生させる。

【００１０】

一方、煩雑さを回避するために機器認証のみ提供する場合には、その機器を使ってサービスを受ける場合に利用者を特定できないために、宅内で使用する場合に、サービス利用者として登録されている人と実際の利用時に利用する人が異なることにより、家族とはいえ見られたくない情報や見せたくない情報（未成年者に対する好ましくない映像等）も見られてしまうこと（例えば親が契約しているＲ指定のコンテンツを子供が見てしまうこと）や新たなサービス提供を受けるかどうかの判断を行う際に情報家電端末の利用に対する支払い者と利用者が異なることによる課金時の不整合等が発生するといった利用者の意図しない課金が発生する(親が契約するＶＯＤサービスを利用して子供が親の知らぬ間に契約外のサービスの提供を受ける)といった課題がある。

【００１１】

宅外で使用する機器で機器認証を用いた場合、落とした場合に不正に利用されるといった課題はもとより、機器認証だけでは利用者を特定できないため利用者の嗜好に応じた情報の提供等もできないという課題がある。

【００１２】

仮に、前述の利用者認証および機器認証のそれぞれの課題を克服できるように、機器認証と利用者認証とを併用しかつ利用者認証においてバイオメトリクス認証を用いた場合においても、先に触れたとおり、情報家電端末個々の価格が高額になることや生体情報を個々の端末に登録する場合には、個人のプライバシーに関わる情報がたくさんの機器に記憶されることになり、これはプライバシー情報の拡散の可能性を増大させるといった課題が残る。

【００１３】

本発明は、上述の課題を解決し、情報家電端末において、認証のための煩雑さを除きつつ、従来の情報家電端末と同じ使い勝手で、個人の特定を可能とする新たな認証方式を提供することにより、安全かつ便利な情報家電端末の提供に資するものである。

【課題を解決するための手段】

【００１４】

本発明は、通信手段を備えた情報家電端末と、この情報家電端末と通信する手段を備えた携帯電話端末と、この携帯電話端末の利用者に対する前記情報家電端末またはその関連装置へのアクセス許可の認証を行う手段を備えた認証サーバとを備えた情報家電システムに適用される認証方法である。

【００１５】

ここで、本発明の特徴とするところは、前記携帯電話端末から前記情報家電端末に機器特有のＩＤ番号（以後、機器ＩＤ）の取得要求を行い、前記情報家電端末から前記機器ＩＤを前記携帯電話端末に転送し、前記携帯電話端末から登録済みの利用者ＩＤと前記機器ＩＤを前記認証サーバに送信し、前記認証サーバで利用者認証および機器認証が行われ、認証に成功した場合には前記認証サーバから前記携帯電話端末に認証情報として前記関連装置を特定するアドレスおよび情報家電端末用リモコン・プログラムが送信され、前記アドレスを前記携帯電話端末から前記情報家電端末に転送し、前記アドレスを元に前記情報家電端末から前記関連装置への接続を行い、前記リモコン・プログラムを用いて前記携帯電話端末を前記情報家電端末のリモコンとして用いるところにある（請求項１）。この認証方法は、認証および接続の動作中に利用者は最初の取得要求のみの動作でよい利点がある。

【００１６】
あるいは、本発明の認証方法は、前記携帯電話端末から前記情報家電端末に登録済み利用者ＩＤとアクセスする前記認証サーバのアドレスとを送信すると共に、前記情報家電端末に前記認証サーバへ機器ＩＤと前記利用者ＩＤの送信要求を行い、前記情報家電端末から前記機器ＩＤと前記利用者ＩＤを前記認証サーバに送信し、前記認証サーバで利用者認証および機器認証が行われ、認証に成功した場合には前記認証サーバから前記情報家電端末に認証成功を通知すると共に、前記携帯電話端末に前記関連装置を特定するアドレスおよび情報家電端末用リモコン・プログラムが送信され、前記アドレスを前記携帯電話端末から前記情報家電端末に転送し、前記アドレスを元に前記情報家電端末から前記関連装置への接続を行い、前記リモコン・プログラムを用いて前記携帯電話端末を前記情報家電端末のリモコンとして用いることを特徴とする（請求項２）。

【００１７】
この認証方法は、認証および接続の動作中に利用者は最初の取得要求のみの動作でよい利点がある。また、この認証方法では、携帯電話端末は、単に、認証サーバからの情報を受信するだけでよく、携帯電話端末と認証サーバとの間の通信手順を簡単化することができる。

【００１８】
また、この認証方法では、認証サーバまでは情報が情報家電端末から送信され、認証サーバから携帯電話端末へは携帯電話のネットワークを経由して情報が送信されるリング型の認証形態をとることにより、送受信を同一のネットワークを利用して行う場合に比べセキュリティをより強固にすることができるという利点がある。

【００１９】
さらに、この認証方法で、前記情報家電端末から機器ＩＤと前記利用者ＩＤとを前記認証サーバに送信するのと併せて、前記携帯電話端末から登録されている前記利用者ＩＤを前記認証サーバに送信し、前記認証サーバで利用者認証および機器認証を行うことができる（請求項３）。

【００２０】
これによれば、利用者ＩＤは、情報家電端末と携帯電話端末との双方から認証サーバに送られる。これにより、利用者認証を確実かつ速やかに実行することができる。一般的に、利用者認証に成功しなければ、機器認証に成功しても無意味であるので、機器認証に先んじて利用者認証を行うことは有効である。

【００２１】
また、本発明の認証方法は、前記認証サーバには、前記携帯電話端末の利用者毎に、前記情報家電端末またはその関連装置の内で、その利用者にアクセス許可される範囲を示すアクセス制限情報があらかじめ保持され、前記認証サーバで利用者認証および機器認証が行われる際に、前記アクセス制限された前記情報家電端末またはその関連装置を除いてアドレス許可の認証を行うことができる（請求項４）。

【００２２】
これによれば、同一の情報家電端末を利用する複数の利用者間で、そのアクセス許可される範囲を可変に設定することができる。したがって、家族とはいえ見られたくない情報や見せたくない情報（未成年者に対する好ましくない映像等）も見られてしまうこと（例えば親が契約しているＲ指定のコンテンツを子供が見てしまうこと）や新たなサービス提供を受けるかどうかの判断を行う際に情報家電端末の利用に対する支払い者と利用者が異なることによる課金時の不整合等が発生するといった利用者の意図しない課金が発生する(親が契約するＶＯＤサービスを利用して子供が親の知らぬ間に契約外のサービスの提供を受ける)といった従来の課題を解決することができる。

【００２３】
さらに、この認証方法で、前記認証サーバは、装置に対するアクセス権のない利用者から当該装置への接続を要求された場合に、前記認証サーバより登録されている当該装置の利用権の所有者に対して当該装置の利用申請を行い、前記利用権の所有者が前記アクセス

権のない利用者の当該装置への接続を認めた場合に、前記認証サーバよりアクセス権のない利用者に認証情報として当該装置を特定するアドレスを送信することができる（請求項５）。

【００２４】

これによれば、アクセス権のない利用者であっても、アクセス権のある利用者の許可があれば、所望する装置へのアクセスが可能となり、サービス提供の際の柔軟性を向上させることができる。

【００２５】

また、本発明の認証方法は、前記携帯電話端末において前記情報家電端末の機器ＩＤの取得要求または機器ＩＤと利用者ＩＤの送信要求が、通常利用者が前記情報家電端末を操作するための行為と同等の行為に連動して行われることが望ましい（請求項６）。

【００２６】

すなわち、このような認証手順を実行することは必要不可欠ではあるが、利用者にとって、煩わしい操作を伴うものであっては困る。したがって、例えば、情報家電端末の電源を投入するスイッチや処理の実行を決定するためのスイッチなどのように、通常利用者が情報家電端末を操作するための行為と同等の行為に連動して行われることが望ましい。

【００２７】

また、本発明の認証方法は、前記携帯電話端末において生体情報を用いて利用者の特定を行い、前記利用者が正当な利用者ならば前記携帯電話端末から前記情報家電端末および前記認証サーバに利用者ＩＤを送信することもできる（請求項７）。例えば、指紋認識などにより利用者の特定を行うことにより、情報家電端末が不正に利用される事態を回避することができる。

【００２８】

また、本発明の認証方法は、認証成功後に前記認証サーバより前記関連装置を特定するアドレスを送信する代わりに、前記情報家電端末から前記機器ＩＤと共に前記情報家電端末のＩＰアドレスが前記携帯電話端末に送信され、前記機器ＩＤおよび前記利用者ＩＤと共に前記ＩＰアドレスが前記携帯電話端末から前記認証サーバに転送されるか、または前記情報家電端末から前記認証サーバに直接前記ＩＰアドレスが送信され、認証が成功したならば、前記ＩＰアドレスが前記関連装置に転送され、前記関連装置が前記情報家電端末との接続を行うことができる（請求項８）。

【００２９】

これによれば、情報家電端末側から関連装置への接続を行う必要がなく、情報家電端末における接続処理を軽減させることができる。情報家電端末における複雑な処理を省くことは、情報家電端末がメンテナンスが困難な一般家庭に置かれる状況を考慮したときに有効である。

【発明の効果】

【００３０】

本発明を用いることにより、情報家電端末においても、従来と同じ使い勝手で、個人の特定を可能とすることにより、これまで以上に安全かつ便利な情報家電端末の提供を可能にするものである。

【００３１】

具体的には、利用者は従来の使い勝手で利便性を確保したまま、利用者を特定することにより従来からの課題であった、第三者による不正利用や不正な利用者によるサービス提供者側の不利益をなくすといったことや、さらには移動先にある端末を利用してのサービスの提供を受けることが可能となる。

【００３２】

また、本発明は利用者の特定および機器の特定を可能とすることから、特定した情報をもとにアクセスを管理することで著作権管理や利用者毎、あるいは特定した利用者の嗜好情報を予め登録しておく等で利用者の嗜好に応じた情報を提供するサービス等への応用を可能とするプラットフォームとして提供することも可能である。

【発明を実施するための最良の形態】
【００３３】
本発明の携帯電話を用いた情報家電端末と利用者の認証の実施例を図１～図２９を参照して説明する。本実施例のブロック構成図には、本実施例の説明に必要な機能ブロックを図示した。例えば、携帯電話端末における携帯電話通信に関わる機能ブロックなどは図示を省略した。
【００３４】
（第一実施例）
第一実施例を図１～図５を参照して説明する。図１は第一実施例の携帯電話による情報家電向け認証方法の構成例である。図２は第一実施例の情報家電端末のブロック構成図である。図３は第一実施例の携帯電話端末のブロック構成図である。図４は第一実施例の認証サーバのブロック構成図である。図５は第一実施例の認証手順を示すシーケンス図である。
【００３５】
第一実施例は、図２に示すように、ＮＷストレージ通信部１および携帯電話端末通信部２を備えた情報家電端末１０１と、図３に示すように、この情報家電端末１０１と通信する情報家電端末通信部１１を備えた携帯電話端末１０２と、図４に示すように、この携帯電話端末１０２の利用者に対する情報家電端末１０１またはＮＷストレージ１０４へのアクセス許可の認証を行う認証実行部３０を備えた認証サーバ１０３とを備えた情報家電システムに適用される認証方法である。
【００３６】
ここで、第一実施例の特徴とするところは、図５に示すように、携帯電話端末１０２から情報家電端末１０１に機器特有のＩＤ番号である機器ＩＤの取得要求を行い、情報家電端末１０１から前記機器ＩＤを携帯電話端末１０２に転送し、携帯電話端末１０２から登録済みの利用者ＩＤと前記機器ＩＤを認証サーバ１０３に送信し、認証サーバ１０３で利用者認証および機器認証が行われ、認証に成功した場合には認証サーバ１０３から携帯電話端末１０２に認証情報として前記関連装置を特定するアドレスおよび情報家電端末用リモコン・プログラムが送信され、前記アドレスを携帯電話端末１０２から情報家電端末１０１に転送し、前記アドレスを元に情報家電端末１０１からＮＷストレージ１０４への接続を行い、前記リモコン・プログラムを用いて携帯電話端末１０２を情報家電端末１０１のリモコンとして用いるところにある（請求項１）。携帯電話端末１０２からのリモコン操作信号を機器制御部５が受けて家電機器の制御を行う。
【００３７】
次に、第一実施例の認証手順を図５を参照して説明する。認証サーバ１０３の認証情報保持部３２にはあらかじめＮＷストレージ１０４の正当な利用者と接続可能な情報家電端末の情報が登録されている。利用者が携帯電話端末１０２を用いて、情報家電端末１０１の機器情報の取得を要求するためのボタンを押すことをトリガーとして、情報家電端末１０１に対して赤外線通信（ＩｒＤＡ）により機器認証に用いる端末のＩＤ（以後、機器ＩＤ）の取得要求を行う（１）。
【００３８】
それに対して情報家電端末１０１から携帯電話端末１０２に対して赤外線通信により機器ＩＤ保持部４に保持されている機器ＩＤが送信される（２）。機器ＩＤを取得する行為は携帯電話端末１０２の特定のボタンを押下する等、通常利用者が情報家電端末１０１を操作するために行う電源ボタンを押下する等の行為と同等の行為に連動して行われるものでもよい。

【００３９】
ここでの情報家電端末１０１と携帯電話端末１０２の間で機器ＩＤの送信等に用いられる通信方式には赤外線通信以外にＢｌｕｅｔｏｏｔｈおよびＺｉｇｂｅｅ等々が考えられる。携帯電話端末１０２の利用者ＩＤ保持部１２にはＳＩＭカード等により利用者認証に

用いるＩＤ（以後、利用者ＩＤ）が登録されている。

【００４０】

機器ＩＤを機器ＩＤ記憶部１３に取得した後、利用者ＩＤと機器のＩＤが認証サーバ通信部１０により携帯電話端末１０２から認証サーバ１０３に送信される（３）。ただし、この際実際の利用者が登録されている利用者かどうかを特定するため、生体情報（指紋等）を用いて利用者の認証を行い、正当な利用者ならば利用者ＩＤを送信することとしてもよい（請求項７）。

【００４１】

認証サーバ１０３の認証実行部３０ではそれぞれのＩＤから認証情報保持部３２を検索して利用者認証および機器認証を行い、認証成功の場合は認証成功ということを示す認証チケットとＮＷストレージ・アドレス情報保持部３３に格納されているＮＷストレージ１０４のＩＰアドレスを携帯電話端末通信部３１により携帯電話端末１０２に返送し（４）、認証失敗の場合には認証が失敗であることを通知する（図示省略）。また、認証成功の場合は携帯電話端末１０２が認証の取れた情報家電端末１０１のリモコンとして動作することが可能なリモコン・プログラムをリモコン・プログラム保持部３４から選択して携帯電話端末１０２に送信し（４）、携帯電話端末１０２ではそのプログラムを取得してリモコン・プログラム記憶部１５に記憶し、利用者がリモコンとして動作可能な状態にする（６）。この場合には携帯電話端末１０２にＯＫまたはＮＧの表示をしてもよい。

【００４２】

さらに携帯電話端末１０２は情報家電端末１０１に対して、返送されたアクセス可能なＮＷストレージ１０４のＩＰアドレスを情報家電端末通信部１１による赤外線通信により転送し、情報家電端末１０１はそのＩＰアドレスを用いてＮＷストレージ通信部１によりルータ１０５を経由してＮＷストレージ１０４と接続する（７）（８）。

【００４３】

この機器認証および利用者認証およびＮＷストレージ１０４への接続のシーケンスは、利用者が最初に機器情報の取得を要求するためのボタンを押す行為を行って以降利用者がなにかしらの動作をしなくても、自動的に進行するものである。ただし、途中で利用者にシーケンスの認証を得る等の動作を促してもよい（この点は第二実施例以降について明示しないが同様である）。

【００４４】

利用者はリモコンとなった携帯電話端末１０２を利用することで、情報家電端末１０１の利用が可能となり、またリモコンで利用可能なチャネル情報にＮＷストレージ１０４へのアクセスを明示することによって、ユーザがＮＷストレージ１０４の選択（孫閲覧、町内お知らせ情報閲覧等）を実現する。

【００４５】

また、接続可能なＮＷストレージ１０４が複数に分かれている場合など、認証サーバ１０３から送信されるＩＰアドレス、すなわち情報家電端末１０１からのアクセス先はＮＷストレージ１０４を統括するストレージ・サーバ、またはそれに代わるものであってもよい。

【００４６】

（第二実施例）

第二実施例を図６～図１０を参照して説明する。図６は第二実施例の携帯電話による情報家電向け認証方法の構成例である。図７は第二実施例の情報家電端末のブロック構成図である。図８は第二実施例の携帯電話端末のブロック構成図である。図９は第二実施例の認証サーバのブロック構成図である。図１０は第二実施例の認証手順を示すシーケンス図である。

【００４７】

第二実施例は、図７に示すように、携帯電話端末通信部２および認証サーバ通信部６およびＮＷストレージ通信部１を備えた情報家電端末１０１と、図８に示すように、この情報家電端末１０１と通信する情報家電端末通信部１１を備えた携帯電話端末１０２と、こ

の携帯電話端末１０２の利用者に対する情報家電端末１０１またはＮＷストレージ１０４へのアクセス許可の認証を行う認証実行部３０を備えた認証サーバ１０３とを備えた情報家電システムに適用される認証方法である。

【００４８】

ここで、第二実施例の特徴とするところは、携帯電話端末１０２の情報家電端末通信部１１から情報家電端末１０１に利用者ＩＤ保持部１２に保持された登録済み利用者ＩＤと認証サーバ・アドレス保持部１８に保持されたアクセスする認証サーバ１０３のアドレスとを送信すると共に、情報家電端末１０１に認証サーバ１０３へ機器ＩＤと前記利用者ＩＤの送信要求を行い、情報家電端末１０１の認証サーバ通信部６から前記機器ＩＤと前記利用者ＩＤを認証サーバ１０３に送信し、認証サーバ１０３の認証実行部３０で認証情報保持部３２を検索して利用者認証および機器認証が行われ、認証に成功した場合には認証サーバ１０３の情報家電端末通信部３５から情報家電端末１０１に認証成功を通知すると共に、携帯電話端末１０２に携帯電話端末通信部３１からＮＷストレージ・アドレス情報保持部３３に保持されたＮＷストレージ１０４を特定するアドレスおよびリモコン・プログラム保持部３４に保持された情報家電端末用リモコンプログラムが送信され、前記アドレスを携帯電話端末１０２の情報家電端末通信部１１から情報家電端末１０１に転送し、前記アドレスを元に情報家電端末１０１のＮＷストレージ通信部１からＮＷストレージ１０４への接続を行い、リモコン・プログラム記憶部１５に保持された前記リモコンプログラムを用いてリモコン制御部１６により携帯電話端末１０２を情報家電端末１０１のリモコンとして用いるところにある（請求項２）。

【００４９】

次に図６の構成例について説明する。図１の構成との差分は、携帯電話端末１０２の情報家電端末通信部１１から情報家電端末１０１に利用者ＩＤ保持部１２に保持されている利用者ＩＤと認証サーバ・アドレス保持部１８に保持されている認証サーバ・アドレスが送信され、情報家電端末１０１の認証サーバ通信部６から利用者ＩＤ記憶部７および機器ＩＤ保持部４に保持されているこれらの機器ＩＤおよび利用者ＩＤを認証サーバ１０３に送信する点である。

【００５０】

次に、図１０を参照して第二実施例の認証手順を説明する。認証サーバ１０３の認証情報保持部３２にはあらかじめＮＷストレージ１０４の正当な利用者と接続可能な情報家電端末１０１の情報が登録されている。利用者が携帯電話端末１０２を用いて、情報家電端末１０１の機器情報の取得を要求するためのボタンを押すことをトリガーとして、情報家電端末１０１に対して赤外線通信（ＩｒＤＡ）により、認証サーバ・アドレス、利用者ＩＤと機器ＩＤの送信要求を行う（１）。それにより情報家電端末１０１は認証サーバ１０３のアクセス先を取得し、認証サーバ通信部６により利用者ＩＤと機器ＩＤを認証サーバ１０３に送信する（２）（３）。

【００５１】

認証サーバ１０３の認証実行部３０ではそれぞれのＩＤから本人認証および機器認証を行い、認証成功の場合は認証成功ということを示す認証チケットを情報家電端末通信部３５により情報家電端末１０１に返送し（４）（５）、認証失敗の場合には認証が失敗したことを通知する（図示省略）。また、認証成功の場合は、これと同時に、リモコン・プログラム保持部３４に保持されている携帯電話端末１０２が認証の取れた情報家電端末１０１のリモコンとして動作することが可能なリモコンプログラムと、ＮＷストレージ・アドレス情報保持部３３に保持されているＮＷストレージ１０４のＩＰアドレスを携帯電話端末１０２に送信し（６）、携帯電話端末１０２では、認証情報受信部１７によりそのプログラムを取得してリモコン・プログラム記憶部１５に記憶し、リモコン制御部１６により利用者がリモコンとして動作可能な状態にする。

【００５２】

この場合に、携帯電話端末１０２にも認証成功または失敗の表示をしてもよい。このとき認証サーバ１０３には登録済みの利用者情報として利用者ＩＤから携帯電話端末１０２

の情報（アドレス等）を取得可能であるとする。ただし、利用者情報登録時に携帯電話端末１０２の情報を登録していない場合には利用者ＩＤと一緒に情報家電端末１０１を介して認証サーバ１０３に送信してもよい。

【００５３】

携帯電話端末１０２は取得したＮＷストレージ１０４のＩＰアドレスを情報家電端末１０１に送信する（７）。情報家電端末１０１はそのＮＷストレージ１０４のＩＰアドレスを用いてルータ１０５を経由してＮＷストレージ１０４と接続する。利用者はリモコンとなった携帯電話端末１０２を利用することで、通常情報家電端末１０１の利用が可能となり（８）、またリモコンで利用可能なチャネル情報にＮＷストレージ１０４へのアクセスを明示することによって、ユーザがＮＷストレージ１０４の選択を実現する。

【００５４】

（第三実施例）

第三実施例を図１１～図１３を参照して説明する。図１１は第三実施例の携帯電話による情報家電向け認証方法の構成例である。図１２は第三実施例の携帯電話端末１０２のブロック構成図である。図１３は第三実施例の認証手順を示すシーケンス図である。第三実施例における情報家電端末１０１および認証サーバ１０３のブロック構成は第二実施例（図７、図９）と共通である。

【００５５】

第三実施例は、図１２に示すように、情報家電端末１０１の認証サーバ通信部６から機器ＩＤと利用者ＩＤとを認証サーバ１０３に送信するのと併せて、携帯電話端末１０２の認証サーバ通信部１０から利用者ＩＤ保持部１２に登録されている利用者ＩＤを認証サーバ１０３に送信し、認証サーバ１０３の認証実行部３０で利用者認証および機器認証を行う（請求項３）。

【００５６】

第三実施例の認証手順を図１３に示す。図１３では、図１０と比較すると携帯電話端末１０２から認証サーバ１０３に利用者ＩＤを送信する手順が追加されている。これによれば、利用者ＩＤは、情報家電端末１０１と携帯電話端末１０２との双方から認証サーバ１０３に送られる。これにより、利用者認証を確実かつ速やかに実行することができる。一般的に、利用者認証に成功しなければ、機器認証に成功しても無意味であるので、機器認証に先んじて利用者認証を行うことは有効である。

【００５７】

（第四実施例）

第四実施例を図１４～図１６を参照して説明する。図１４は第四実施例の携帯電話による情報家電向け認証方法の構成例である。図１５は第四実施例の認証情報保持部３２のテーブルを示す図である。図１６は第四実施例の認証手順を示すシーケンス図である。

【００５８】

なお、第四実施例の情報家電端末２０１、携帯電話端末２０２、２０３、認証サーバ２０４、２０５のブロック構成は、第一実施例で説明したブロック構成（図２～図４）と共通である。ただし、情報家電端末２０１にはローカル・ストレージ２０９が外付けされている。

【００５９】

第四実施例は、認証サーバ２０４または２０５の認証情報保持部３２には、図１５に示すように、携帯電話端末２０２および２０３の利用者毎に、情報家電端末２０１またはローカル・ストレージ２０９またはＮＷストレージ２０６、２０７の内で、その利用者にアクセス許可される範囲を示すアクセス制限情報があらかじめ保持され、認証サーバ２０４または２０５で利用者認証および機器認証が行われる際に、前記アクセス制限された情報家電端末２０１またはローカル・ストレージ２０９またはＮＷストレージ２０６、２０７を除いてアドレス許可の認証を行う（請求項４）。

【００６０】

次に、図１４の構成例について説明する。ローカル・ストレージ２０９のついた情報家

電端末２０１にはそのストレージを使用できる利用者があらかじめ登録され、さらに認証サーバ２０４、２０５の認証情報保持部３２には、図１５に示すように、あらかじめＮＷストレージ２０６、２０７およびローカル・ストレージ２０９の正当な利用者と接続可能な情報家電端末２０１の情報が登録されている。

【００６１】

次に、図１６を参照して第四実施例の認証手順を説明する。ローカル・ストレージ２０９の利用許可が登録されている利用者を仮にＡさんとする。利用者が携帯電話端末２０２、２０３を用いて、情報家電端末２０１の機器情報の取得を要求するためのボタンを押すことをトリガーとして、携帯電話端末２０２、２０３の情報家電端末通信部１１から情報家電端末２０１に対して赤外線通信（ＩｒＤＡ）により機器ＩＤの取得要求を行う（１）。それに対して情報家電端末２０１の携帯電話端末通信部２から携帯電話端末２０２、２０３に対して赤外線通信により機器ＩＤが送信される（２）。

【００６２】

携帯電話端末２０２、２０３の利用者ＩＤ保持部１２にはＳＩＭカード等により利用者が登録されている。登録されている利用者ＩＤと機器ＩＤ記憶部１３に記憶されている機器ＩＤが携帯電話端末２０２、２０３の認証サーバ通信部１０より認証サーバ２０４、２０５に送信される（３）。ただし、この際、実際の利用者が登録されている利用者かどうかを特定するため、生体情報（指紋等）を用いて利用者の認証が行い、正当な利用者ならば利用者ＩＤを送信することとしてもよい（請求項７）。

【００６３】

認証サーバ２０４、２０５の認証実行部３０ではそれぞれのＩＤから本人認証および機器認証を行う。認証を行う際に、利用者によって情報家電端末２０１やローカル・ストレージ２０９、ＮＷストレージ２０６、２０７に対するアクセス権が変わってくる。Ａさんが携帯電話端末２０２から認証を行った場合は、図１５に示すように、ローカル・ストレージ２０９の利用はＡさんのみ認められているので、ＡさんにはＮＷストレージ２０６、ローカル・ストレージ２０９、および情報家電端末２０１の利用権が認められる。すなわち、認証サーバ２０４からＮＷストレージ２０６およびローカル・ストレージ２０９の使用許可を示す認証チケットとＮＷストレージ２０６のＩＰアドレスが携帯電話端末２０２に返送される（４）。これに対してＢさんが携帯電話端末２０３から認証を行った場合には、図１５に示すように、ＢさんにはＮＷストレージ２０７と情報家電端末２０１の利用権のみが認められるため、認証サーバ２０５からＮＷストレージ２０７の使用許可を示す認証チケットとＮＷストレージ２０７のＩＰアドレスが携帯電話端末２０２に返送される（４）。また、ＡさんとＢさん以外の利用者がアクセスした場合には認証失敗となり、そのときの携帯電話端末に認証の失敗が通知される（図示省略）。さらに、認証成功の場合は携帯電話端末２０２、２０３が認証の取れた情報家電端末２０１のリモコンとして動作することが可能なリモコン・プログラムを携帯電話端末２０２、２０３に送信し（４）、携帯電話端末２０２、２０３ではそのプログラムを取得してリモコン・プログラム記憶部１５に記憶し、リモコン制御部１６により利用者がリモコンとして動作可能な状態にする（６）。

【００６４】

さらに、携帯電話端末２０２、２０３の情報家電端末通信部１１は情報家電端末２０１に対して、返送されたアクセス可能なＮＷストレージ２０６、２０７のＩＰアドレスを赤外線通信により転送し（５）、情報家電端末２０１のＮＷストレージ通信部１はそのＩＰアドレスを用いてルータ２０８を経由してＮＷストレージ２０６、２０７と接続する（７）（８）。利用者はリモコンとなった携帯電話端末２０２、２０３を利用することで、情報家電端末２０１の利用が可能となる（６）。

また、リモコンで利用可能なチャネル情報にＡさんの場合はＮＷストレージ２０６およびローカル・ストレージ２０９へのアクセスを、Ｂさんの場合はＮＷストレージ２０７へのアクセスを明示することによって、利用者に応じたＮＷストレージ２０６、２０７やローカル・ストレージ２０９の選択を実現する。

【００６５】
（第五実施例）
第五実施例を図１７～図２０を参照して説明する。図１７は第五実施例の携帯電話による情報家電向け認証方法の構成例である。図１８は第五実施例の携帯電話端末のブロック構成図である。図１９は第五実施例の認証サーバのブロック構成図である。図２０は第五実施例の認証手順を示すシーケンス図である。第五実施例における情報家電端末１０１のブロック構成は第一実施例（図２）と共通である。
【００６６】
第五実施例では、認証サーバ２０５のアクセス申請処理部３６は、装置に対するアクセス権のない利用者から当該装置への接続を要求された場合に、認証サーバ２０５の認証情報保持部３２より登録されている当該装置の利用権の所有者に対して当該装置の利用申請を行い、前記利用権の所有者が前記アクセス権のない利用者の当該装置への接続を認めた場合に、認証サーバ２０５の携帯電話端末通信部３１よりアクセス権のない利用者に認証情報として当該装置を特定するアドレスを送信する（請求項５）。
【００６７】
すなわち、図１７に示すように、通常、Ｂさんのローカル・ストレージ２０９へのアクセス権は認められていないが、Ｂさんが接続を要求してきた場合に、認証サーバ２０５からローカル・ストレージ２０９へのアクセスが許可されているＡさんの携帯電話端末２０２のアクセス申請処理部１９にＢさんが接続を要求してきたことを通知し、アクセス申請処理部１９は、他利用者情報保持部２０を検索してＢさんがローカル・ストレージ２０９を利用してもよい利用者であることを認識した場合には、Ｂさんのローカル・ストレージ２０９への接続を認めるとしてもよい。このとき、携帯電話端末２０２が他利用者情報保持部２０を持っていない場合には、Ｂさんが接続を要求してきたことを画面表示し、Ａさん自身が認証行為を行うようにしてもよい。
【００６８】
また、携帯電話端末２０３側で情報家電端末２０１から送信された登録されている利用許可者のＩＤと、指紋等を用いて認証された現在の利用者を認証し、正当な利用者ならば認証サーバ２０５とアクセスし、正当な利用者ではない場合には認証サーバ２０５とアクセスしないようにすることも可能である。
【００６９】
次に、図２０を参照して第五実施例の認証手順を説明する。Ｂさんが携帯電話端末２０３の電源をＯＮすることより、情報家電端末通信部１１は、機器ＩＤ取得要求を情報家電端末２０１に対して行う（１）。情報家電端末２０１の携帯電話端末通信部２は、機器ＩＤ保持部４に保持されている機器ＩＤを携帯電話端末２０３に対して送信する（２）。機器ＩＤを機器ＩＤ記憶部１３に記憶した携帯電話端末２０３は、認証サーバ通信部１０により機器ＩＤと利用者ＩＤ保持部１２に保持されているＢさんの利用者ＩＤを認証サーバ２０５に送信する（３）。
【００７０】
認証サーバ２０５の認証実行部３０では、認証情報保持部３２を検索してＢさんの認証を実行するが、このときに、Ｂさんにはローカル・ストレージ２０９へのアクセスが許可されていないとする。また、アクセス許可が出た後は、Ｂさんは、情報家電端末２０１、ローカル・ストレージ２０９およびＮＷストレージ２０７にアクセス可能であるとする。
【００７１】
Ｂさんのアクセス許可を得るために、アクセス申請処理部３６は、Ａさんの携帯電話端末２０２に対してＢさんのアクセス申請を行う（４）。Ａさんの携帯電話端末２０２のアクセス申請処理部１９は他利用者情報保持部２０を検索し、Ｂさんがローカル・ストレージ２０９にアクセス可能か否かを識別する。その結果、Ｂさんがアクセス可能であることが判明すると、認証サーバ２０５に対してアクセス許可を送信する（５）。認証サーバ２０５のアクセス申請処理部１９では、Ａさんからのアクセス許可を受け取ると、Ｂさんに認証成功を通知すると共に、ＮＷストレージ２０７のＩＰアドレスと情報家電端末２０１

を操作するためのリモコン・プログラムをＢさんの携帯電話端末２０３に送信する（６）。

【００７２】

Ｂさんの携帯電話端末２０３では、受け取ったＮＷストレージ２０７のＩＰアドレスをＮＷストレージ・アドレス記憶部１４に記憶し、このＩＰアドレスを情報家電端末通信部１１により情報家電端末２０１に送信すると共に、受け取ったリモコン・プログラムをリモコン・プログラム記憶部１５に記憶し、このリモコン・プログラムを用いてリモコン制御部１６により携帯電話端末２０３を操作する（８）。

【００７３】

ＮＷストレージ２０７のＩＰアドレスを携帯電話端末通信部２により受け取った情報家電端末２０１は、このＩＰアドレスをＮＷストレージ・アドレス記憶部３に記憶し、このＩＰアドレスを用いてＮＷストレージ通信部１によりルータ２０８を介してＮＷストレージ２０７に接続する（９）（１０）。

【００７４】

これにより、Ｂさんの携帯電話端末２０３は、ローカル・ストレージ２０９およびＮＷストレージ２０７にアクセス可能となる。

【００７５】

（第六実施例）

第六実施例を図２１～図２４を参照して説明する。図２１は第六実施例の携帯電話による情報家電向け認証方法の構成例である。図２２は第五実施例の携帯電話端末のブロック構成図である。図２３は第五実施例の認証サーバのブロック構成図である。図２４は第六実施例の認証手順を示すシーケンス図である。第六実施例における情報家電端末１０１のブロック構成は第一実施例（図２）と共通である。

【００７６】

第一～第五実施例で説明したように、認証成功後に認証サーバ１０３よりＮＷストレージ１０４のＩＰアドレスを送信する代わりに、第六実施例では、情報家電端末１０１から機器ＩＤと共に情報家電端末１０１のＩＰアドレスが携帯電話端末通信部２により携帯電話端末１０２に送信され、携帯電話端末１０２では、このＩＰアドレスを端末アドレス情報記憶部２１に記憶し、機器ＩＤおよび利用者ＩＤと共にこのＩＰアドレスが認証サーバ通信部１０により携帯電話端末１０２から認証サーバ１０３に転送される。認証サーバ１０３では、携帯電話端末通信部３１によりこのＩＰアドレスを受信して端末アドレス情報記憶部３８に記憶する。

【００７７】

認証サーバ１０３の認証実行部３０により携帯電話端末１０２の認証が成功したならば、前記ＩＰアドレスがＮＷストレージ１０４にＮＷストレージ通信部３７により転送され、ＮＷストレージ１０４が情報家電端末１０１との接続を行う（請求項８）。

【００７８】

図２１の構成例について説明する。第一～第五実施例との差分はあらかじめ情報家電端末１０１のＩＰアドレスが携帯電話端末１０２を通じてＮＷストレージ１０４に転送され、認証が成功した場合にはＮＷストレージ１０４から情報家電端末１０１にアクセスする点である。

【００７９】

次に、図２４を参照して第六実施例の認証手順を説明する。携帯電話端末１０２の電源ＯＮと共に、情報家電端末１０１の機器ＩＤ取得要求が情報家電端末通信部１１により情報家電端末１０１に送信される（１）。これを受けて情報家電端末１０１の携帯電話端末通信部２から携帯電話端末１０２に対して赤外線通信により機器ＩＤと情報家電端末１０１のＩＰアドレスが送信される（２）。

【００８０】

これを受けて携帯電話端末１０２の認証サーバ通信部１０から認証用サーバ１０３に対して、機器認証用ＩＤと本人認証用ＩＤおよび情報家電端末１０１のＩＰアドレスが送信

される（３）。このＩＰアドレスは、端末アドレス情報記憶部３８に記憶される。認証サーバ１０３の認証実行部３０ではそれぞれのＩＤから認証情報保持部３２を検索して本人認証および機器認証を行い、認証が成功した場合には送信された情報家電端末１０１のＩＰアドレスを端末アドレス情報記憶部３８からＮＷストレージ通信部３７によりＮＷストレージ１０４に転送し（４）、失敗の場合には携帯電話端末１０２に認証が失敗であることを通知する（図示省略）。ＮＷストレージ１０４はルータ１０５を経由して転送されたＩＰアドレスを有する情報家電端末１０１と接続する（６）（７）。

【００８１】

また、認証サーバ１０３は、携帯電話端末通信部３１により携帯電話端末１０２に対して認証成功の通知と共にリモコン・プログラムを送信する（５）。これを受けた携帯電話端末１０２は、このリモコン・プログラムをリモコン・プログラム記憶部１５に記憶し、リモコン制御部１６を用いて情報家電端末１０１のリモコンとしてアクセスする（８）。

【００８２】

（第七実施例）

第七実施例を図２５～図２７を参照して説明する。図２５は第七実施例の携帯電話による情報家電向け認証方法の構成例である。図２６は第七実施例の認証サーバのブロック構成図である。図２７は第七実施例の認証手順を示すシーケンス図である。また、第七実施例における情報家電端末１０１のブロック構成は第二実施例（図７）と共通であり、携帯電話端末１０２のブロック構成は第六実施例（図２２）と共通である。

【００８３】

第一～第五実施例で説明したように、認証成功後に認証サーバ１０３よりＮＷストレージ１０４のＩＰアドレスを送信する代わりに、第七実施例では、情報家電端末１０１から機器ＩＤが認証サーバ通信部６により認証サーバ１０３に送信され、さらに、情報家電端末１０１の認証サーバ通信部６から認証サーバ１０３に直接、情報家電端末１０１のＩＰアドレスが送信される。認証サーバ１０３では、情報家電端末通信部３５によりこのＩＰアドレスを受信して端末アドレス情報記憶部３８に記憶する。

【００８４】

認証サーバ１０３の認証実行部３０により携帯電話端末１０２の認証が成功したならば、前記ＩＰアドレスがＮＷストレージ１０４に、認証サーバ１０３のＮＷストレージ通信部３７により転送され、ＮＷストレージ１０４が情報家電端末１０１との接続を行う（請求項８）。

【００８５】

図２５の構成例について説明する。第一～第五実施例との差分はあらかじめ情報家電端末１０１のＩＰアドレスが情報家電端末１０１自身によりＮＷストレージ１０４に転送され、認証が成功した場合にはＮＷストレージ１０４から情報家電端末１０１にアクセスする点である。

【００８６】

次に、図２７を参照して第七実施例の認証手順を説明する。携帯電話端末１０２の電源ＯＮと共に、情報家電端末通信部１１により情報家電端末１０１に利用者ＩＤ保持部１２に保持されている利用者ＩＤおよび認証サーバ・アドレス保持部１８に保持されている認証サーバＩＰアドレスが送信される（１）。これを受けて情報家電端末１０１の認証サーバ通信部６からルータ１０５に対して機器ＩＤおよび利用者ＩＤおよび端末ＩＰアドレスが送信される（２）。ルータ１０５はこれらを認証サーバ１０３に転送する（３）。このＩＰアドレスは、認証サーバ１０３の端末アドレス情報記憶部３８に記憶される。なお、情報家電端末１０１自身の端末ＩＰアドレスは、認証サーバ通信部６およびその他の通信部があらかじめ保持しており、これを用いて各種通信を行っているので、自己の端末ＩＰアドレス情報を保持する機能は各通信部が内蔵しているものとして機能ブロックの図示はしていない。認証サーバ１０３の認証実行部３０では認証情報保持部３２を検索してそれぞれのＩＤから本人認証および機器認証を行い、認証が成功した場合には認証成功をルータ１０５を経由して情報家電端末１０１に送信する（４）（５）。また、認証サーバ１０

３は、情報家電端末１０１のＩＰアドレスをＮＷストレージ通信部３７によりＮＷストレージ１０４に転送する（６）。認証失敗の場合には認証サーバ１０３は情報家電端末１０１および携帯電話端末１０２に認証が失敗であることを通知する（図示省略）。ＮＷストレージ１０４はルータ１０５を経由して転送されたＩＰアドレスを有する情報家電端末１０１と接続する（８）（９）。

【００８７】

また、認証サーバ１０３は、携帯電話端末１０２に対して認証成功の通知と共にリモコン・プログラムを送信する（７）。これを受けた携帯電話端末１０２は、このリモコン・プログラムをリモコン・プログラム記憶部１５に記憶し、リモコン制御部１６を用いて情報家電端末１０１のリモコンとしてアクセスする（１０）。

【００８８】

（第八実施例）

第八実施例を図２８を参照して説明する。図２８は第八実施例を説明するための回路図である。携帯電話端末において情報家電端末の機器ＩＤの取得要求または機器ＩＤと利用者ＩＤの送信要求が、通常利用者が情報家電端末を操作するための行為と同等の行為に連動して行われる（請求項６）。

【００８９】

すなわち、図２８に示すように、携帯電話端末がリモコン基本制御部４０によって情報家電端末のリモコンとして働くときに、情報家電端末の電源スイッチあるいは処理の実行を決定するスイッチと連動して認証処理制御部４１が起動する。

【００９０】

なお、本実施例では、認証成功後の最終段階としてリモコン・プログラムが認証サーバから携帯電話端末に送信されるとして説明したが、情報家電端末の電源をＯＮとしたり、あるいは処理の実行を決定するような基本的なリモコン・プログラムについては、携帯電話端末が常時持っていることとする。

【００９１】

（第九実施例）

第九実施例を図２９を参照して説明する。図２９は第九実施例の携帯電話端末の外観図である。携帯電話端末において生体情報を用いて利用者の特定を行い、利用者が正当な利用者ならば携帯電話端末から情報家電端末および認証サーバに利用者ＩＤを送信する（請求項７）。

【００９２】

すなわち、図２９に示すように、指紋判定部４２を備えた携帯電話端末を用い、指紋判定に適合した正当な利用者である場合のみ本実施例で説明した認証手順を受け付けることとする。

【産業上の利用可能性】

【００９３】

本発明によれば、情報家電端末において、認証のための煩雑さを除きつつ、従来の情報家電端末と同じ使い勝手で、個人の特定を可能とする新たな認証方式を提供することにより、安全かつ便利な情報家電端末の提供に資することができる。したがって、情報家電端末の普及に寄与することができる。

【図面の簡単な説明】

【００９４】

【図１】第一実施例の携帯電話による情報家電向け認証方法の構成例を示す図。

【図２】第一実施例の情報家電端末のブロック構成図。

【図３】第一実施例の携帯電話端末のブロック構成図。

【図４】第一実施例の認証サーバのブロック構成図。

【図５】第一実施例の認証手順を示すシーケンス図。

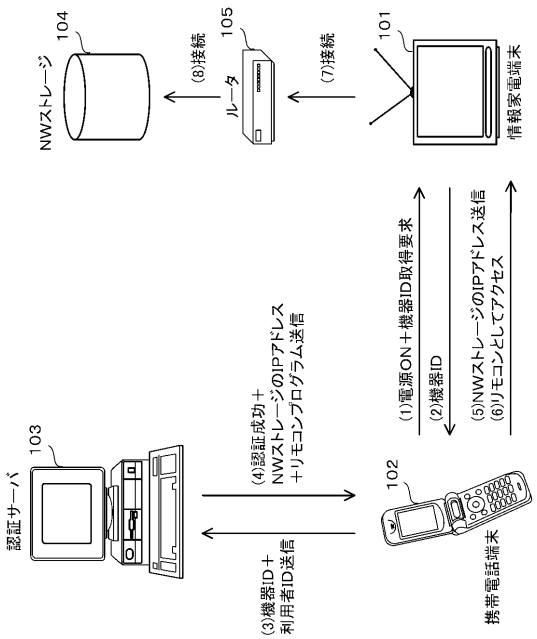
【図６】第二実施例の携帯電話による情報家電向け認証方法の構成例を示す図。

【図７】第二実施例の情報家電端末のブロック構成図。

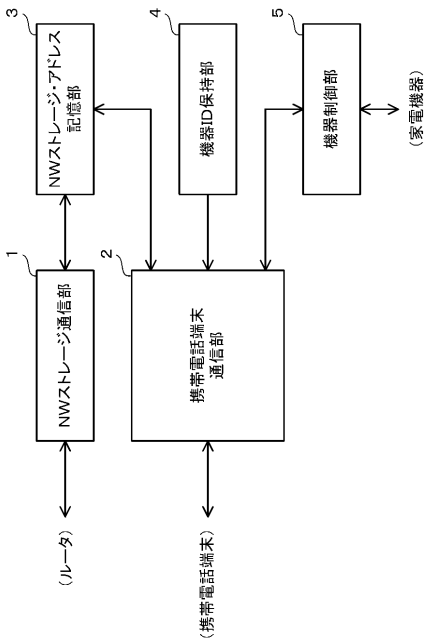
【図８】第二実施例の携帯電話端末のブロック構成図。
【図９】第二実施例の認証サーバのブロック構成図。
【図１０】第二実施例の認証手順を示すシーケンス図。
【図１１】第三実施例の携帯電話による情報家電向け認証方法の構成例を示す図。
【図１２】第三実施例の携帯電話端末のブロック構成図。
【図１３】第三実施例の認証手順を示すシーケンス図。
【図１４】第四実施例の携帯電話による情報家電向け認証方法の構成例を示す図。
【図１５】第四実施例の認証情報保持部のテーブルを示す図。
【図１６】第四実施例の認証手順を示すシーケンス図。
【図１７】第五実施例の携帯電話による情報家電向け認証方法の構成例。
【図１８】第五実施例の携帯電話端末のブロック構成図。
【図１９】第五実施例の認証サーバのブロック構成図。
【図２０】第五実施例の認証手順を示すシーケンス図。
【図２１】第六実施例の携帯電話による情報家電向け認証方法の構成例を示す図。
【図２２】第五実施例の携帯電話端末のブロック構成図。
【図２３】第五実施例の認証サーバのブロック構成図。
【図２４】第六実施例の認証手順を示すシーケンス図。
【図２５】第七実施例の携帯電話による情報家電向け認証方法の構成例を示す図。
【図２６】第七実施例の認証サーバのブロック構成図。
【図２７】第七実施例の認証手順を示すシーケンス図。
【図２８】第八実施例を説明するための回路図。
【図２９】第九実施例の携帯電話端末の外観図。
【符号の説明】
【００９５】
１、３７　ＮＷストレージ通信部
２、３１　携帯電話端末通信部
３、１４　ＮＷストレージ・アドレス記憶部
４　機器ＩＤ保持部
５　機器制御部
６、１０　認証サーバ通信部
７　利用者ＩＤ記憶部
１１、３５　情報家電端末通信部
１２　利用者ＩＤ保持部
１３　機器ＩＤ記憶部
１５　リモコン・プログラム記憶部
１６　リモコン制御部
１７　認証情報受信部
１８　認証サーバ・アドレス保持部
１９、３６　アクセス申請処理部
２０　他利用者情報保持部
２１、３８　端末アドレス情報記憶部
３０　認証実行部
３２　認証情報保持部
３３　ＮＷストレージ・アドレス情報保持部
３４　リモコン・プログラム保持部
４０　リモコン基本制御部
４１　認証処理制御部
４２　指紋判定部
１０１、２０１　情報家電端末
１０２、２０２、２０３　携帯電話端末

１０３、２０４、２０５　認証サーバ
１０４、２０６、２０７　ＮＷストレージ
１０５、２０８　ルータ
２０９　ローカル・ストレージ

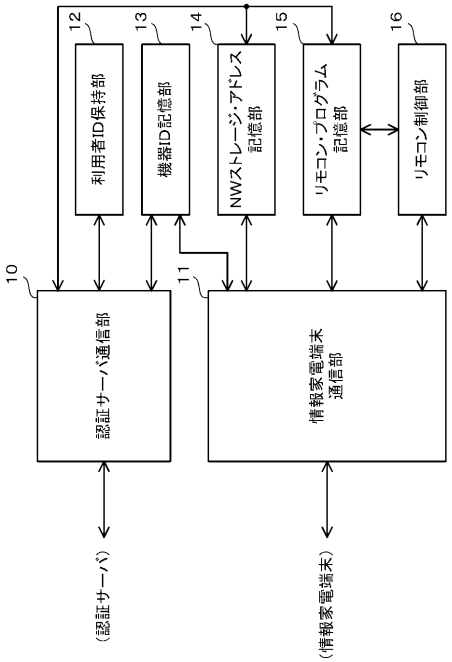
【図１】



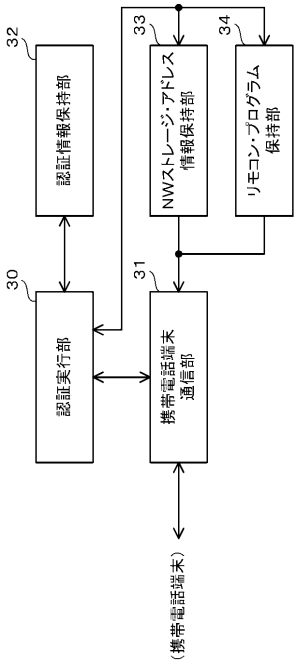
【図２】



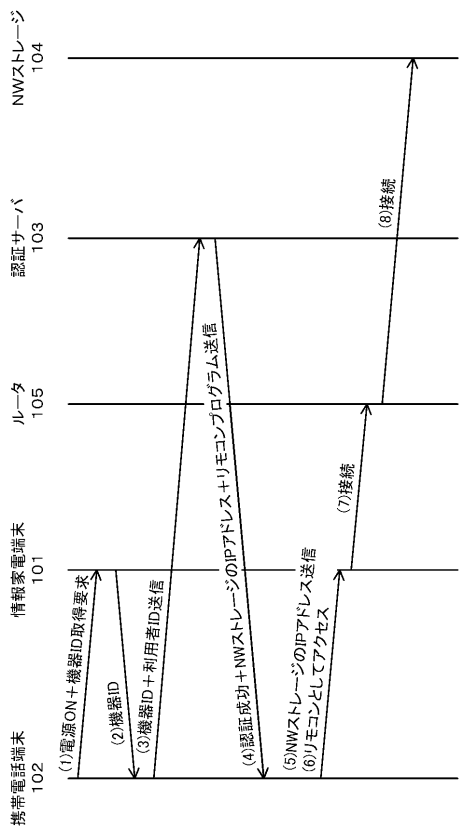
【図３】


10
11
12
13
14
15
16
利用者ID保持部
機器ID記憶部
NWストレージ・アドレス記憶部
リモコン・プログラム記憶部
リモコン制御部
認証サーバ通信部
情報家電端末通信部
（認証サーバ）
（情報家電端末）

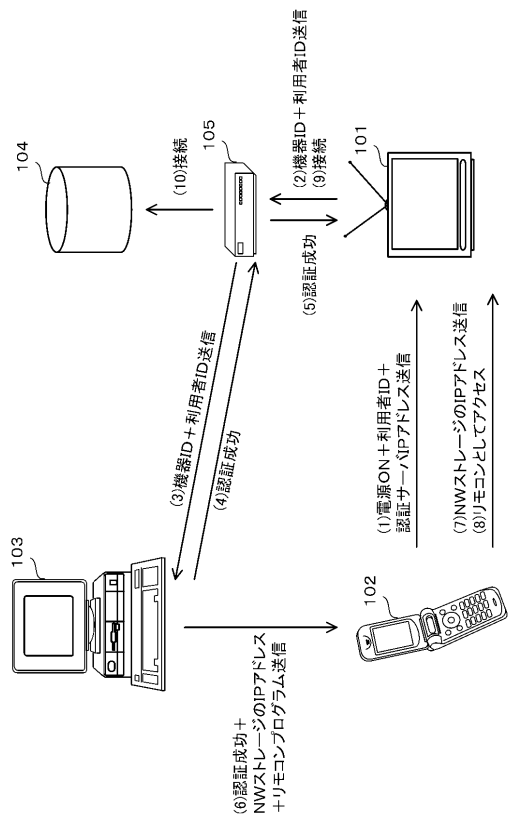
【図４】


30
31
32
33
34
認証情報保持部
NWストレージ・アドレス情報保持部
リモコン・プログラム保持部
認証実行部
携帯電話端末通信部
（携帯電話端末）

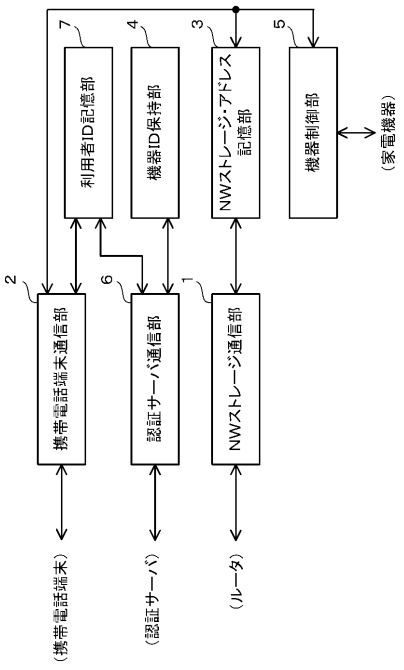
【図５】


携帯電話端末 102
情報家電端末 101
ルータ 105
認証サーバ 103
NWストレージ 104
(1)電源ON＋機器ID取得要求
(2)機器ID
(3)機器ID＋利用者ID送信
(4)認証成功＋NWストレージのIPアドレス＋リモコンプログラム送信
(5)NWストレージのIPアドレス送信
(6)リモコンとしてアクセス
(7)接続
(8)接続

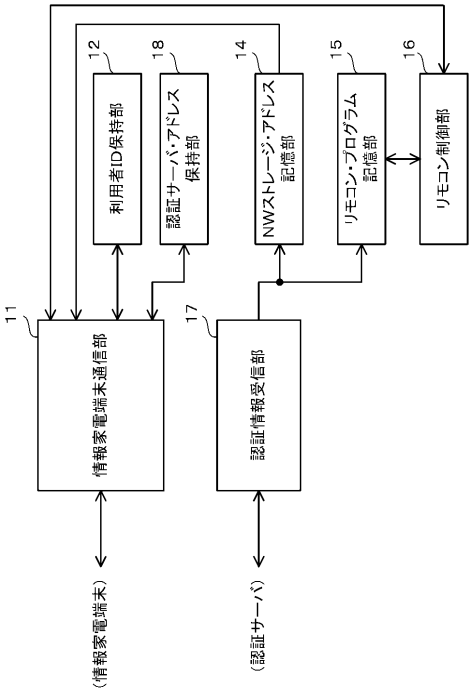
【図６】


104
105
101
103
102
(10)接続
(2)機器ID＋利用者ID送信
(9)接続
(5)認証成功
(3)機器ID＋利用者ID送信
(4)認証成功
(1)電源ON＋利用者ID＋認証サーバへIPアドレス送信
(7)NWストレージのIPアドレス送信
(8)リモコンとしてアクセス
(6)認証成功＋NWストレージのIPアドレス＋リモコンプログラム送信

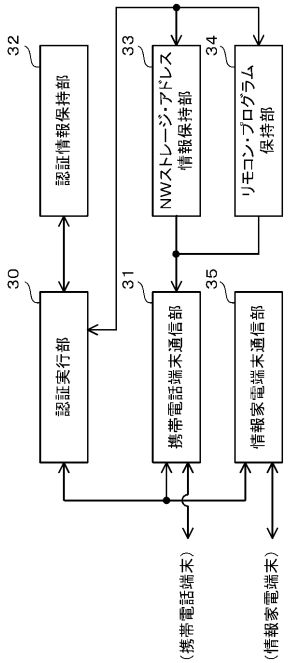
【図７】


携帯電話端末通信部
認証サーバ通信部
NWストレージ通信部
利用者ID記憶部
機器ID保持部
NWストレージ・アドレス記憶部
機器制御部
（家電機器）
（携帯電話端末）
（認証サーバ）
（ルータ）
1
2
3
4
5
6
7

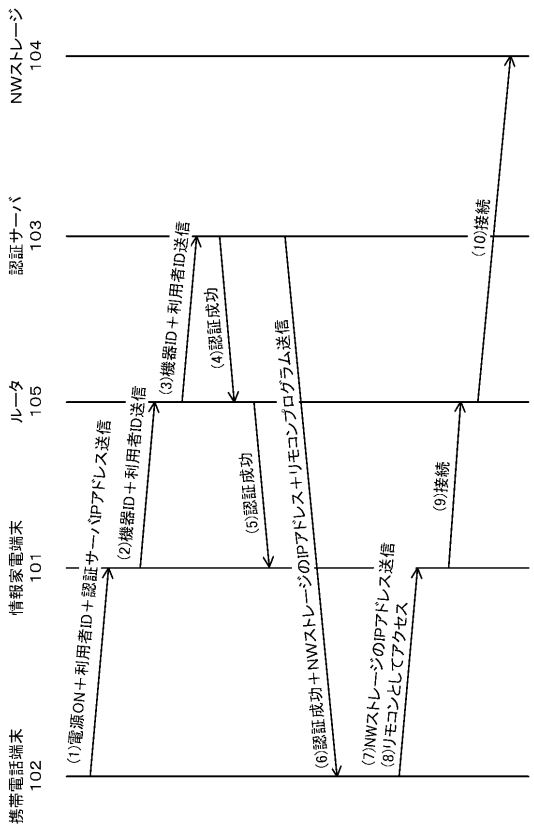
【図８】


情報家電端末通信部
認証情報受信部
利用者ID保持部
認証サーバ・アドレス保持部
NWストレージ・アドレス記憶部
リモコン・プログラム記憶部
リモコン制御部
（情報家電端末）
（認証サーバ）
11
12
14
15
16
17
18

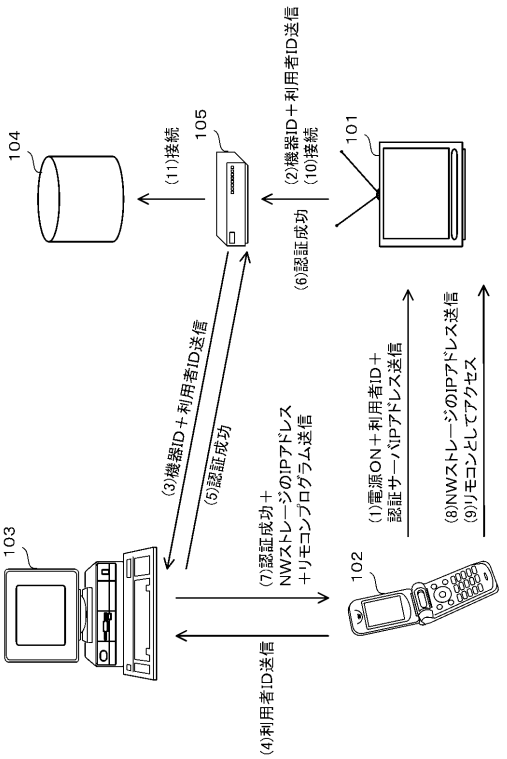
【図９】


認証実行部
認証情報保持部
携帯電話端末通信部
NWストレージ・アドレス情報保持部
情報家電端末通信部
リモコン・プログラム保持部
（携帯電話端末）
（情報家電端末）
30
31
32
33
34
35

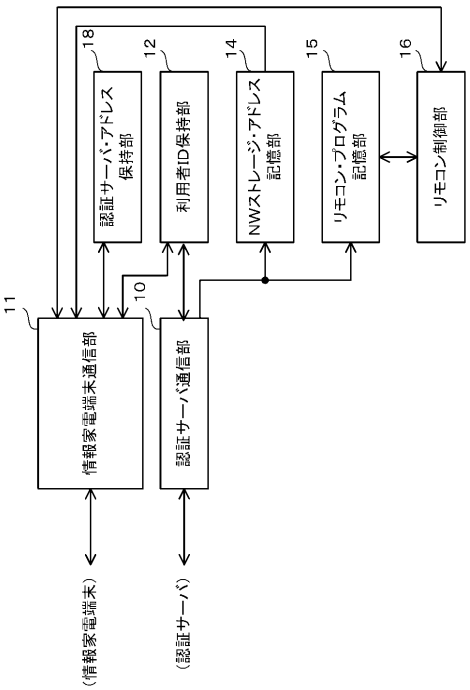
【図１０】


携帯電話端末 102
情報家電端末 101
ルータ 105
認証サーバ 103
NWストレージ 104
(1)電源ON＋利用者ID＋認証サーバIPアドレス送信
(2)機器ID＋利用者ID送信
(3)機器ID＋利用者ID送信
(4)認証成功
(5)認証成功
(6)認証成功＋NWストレージのIPアドレス＋リモコンプログラム送信
(7)NWストレージのIPアドレス送信
(8)リモコンとしてアクセス
(9)接続
(10)接続

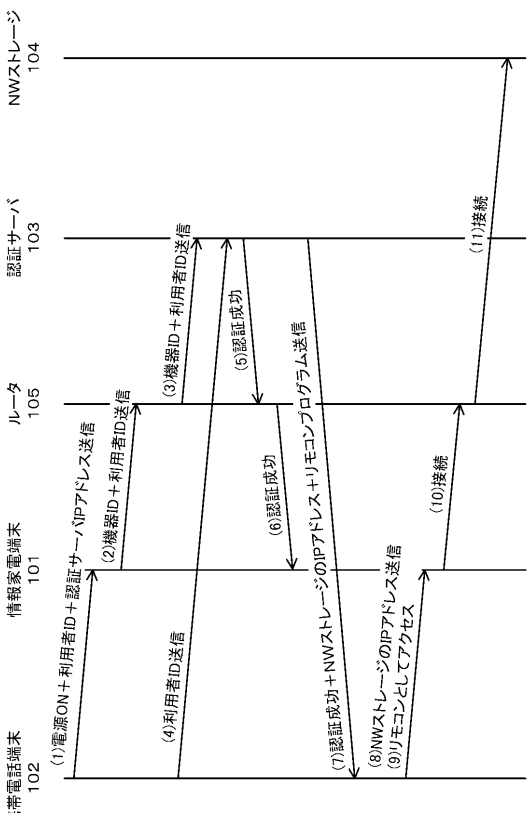
【図１１】



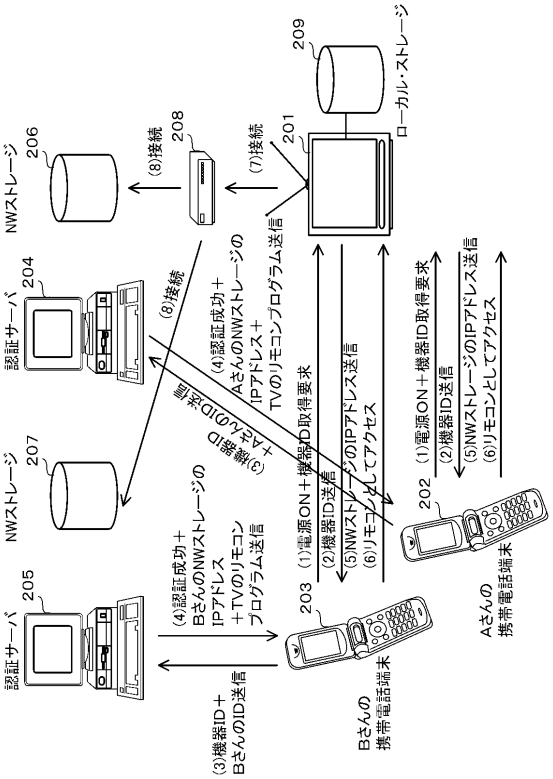
【図１２】



【図１３】



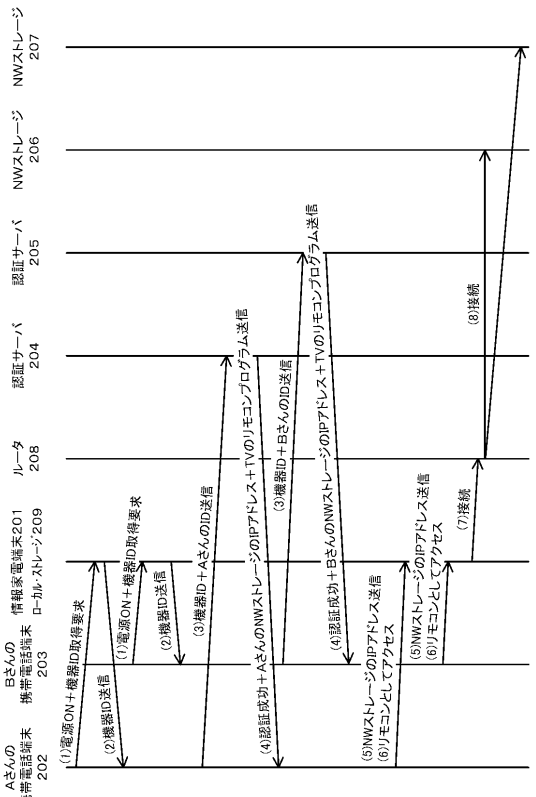
【図１４】



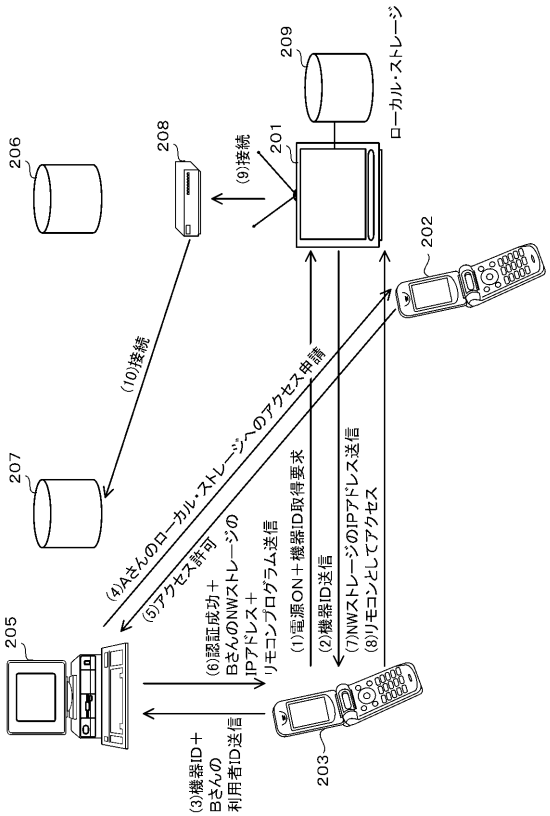
【図１５】

ユーザ名	アクセス範囲
A	NWストレージ206，ローカル・ストレージ209，情報家電端末201
B	NWストレージ207，情報家電端末201

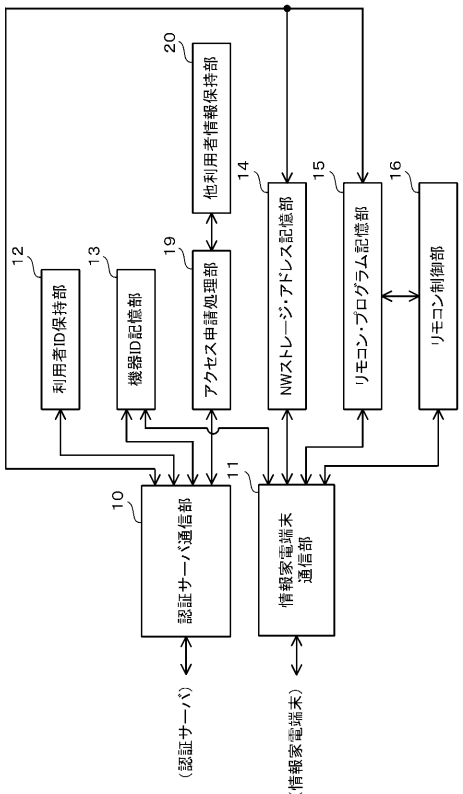
【図１６】



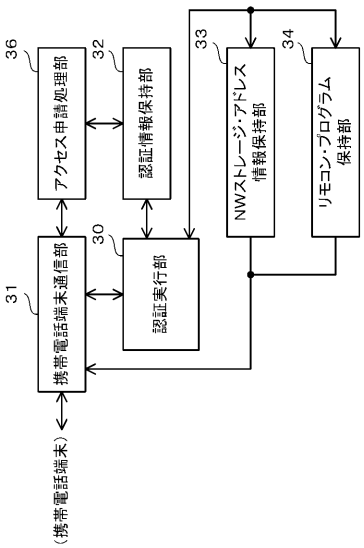
【図１７】



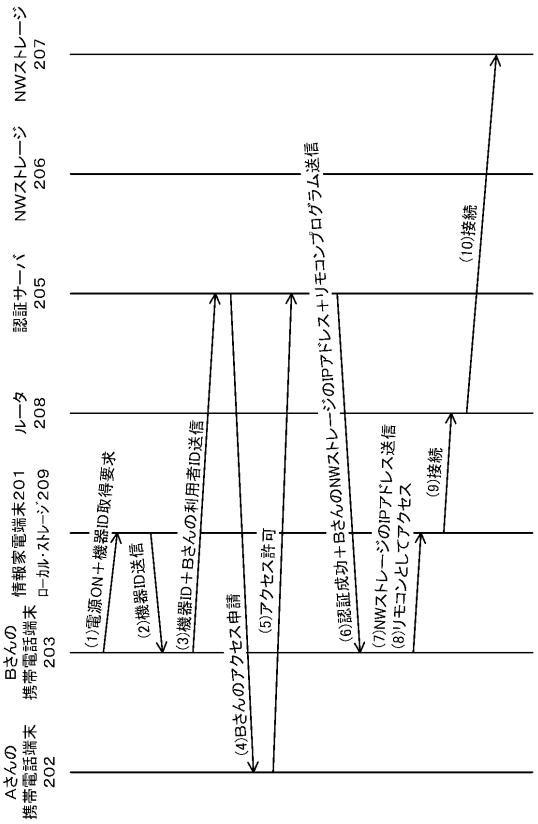
【図１８】



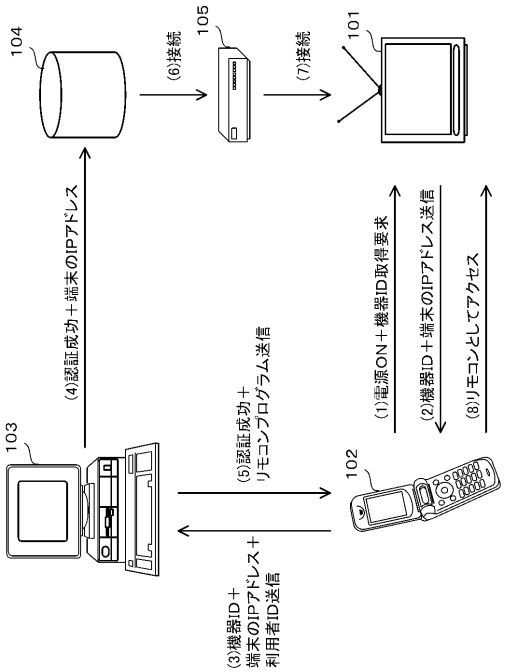
【図１９】



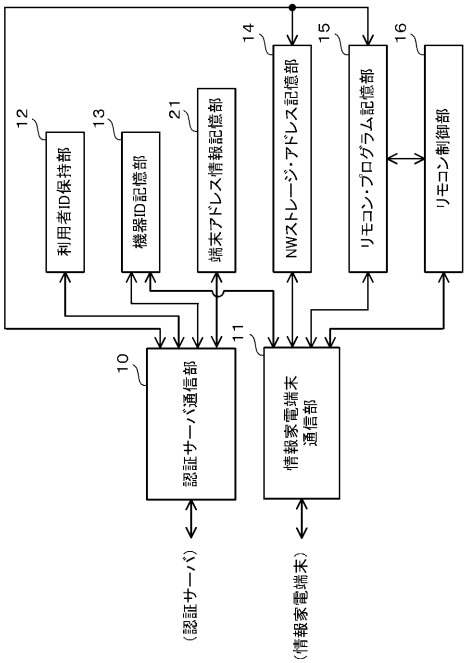
【図２０】



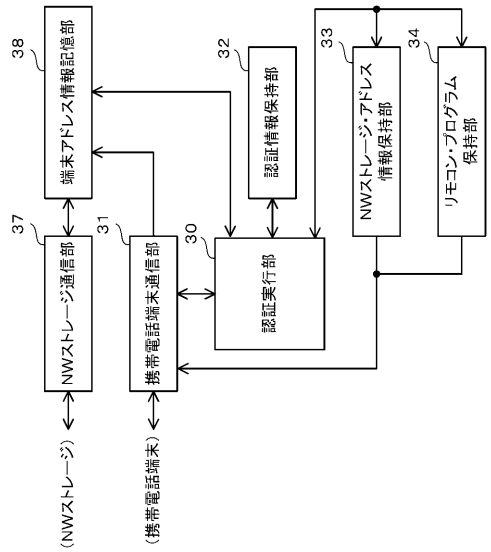
【図２１】



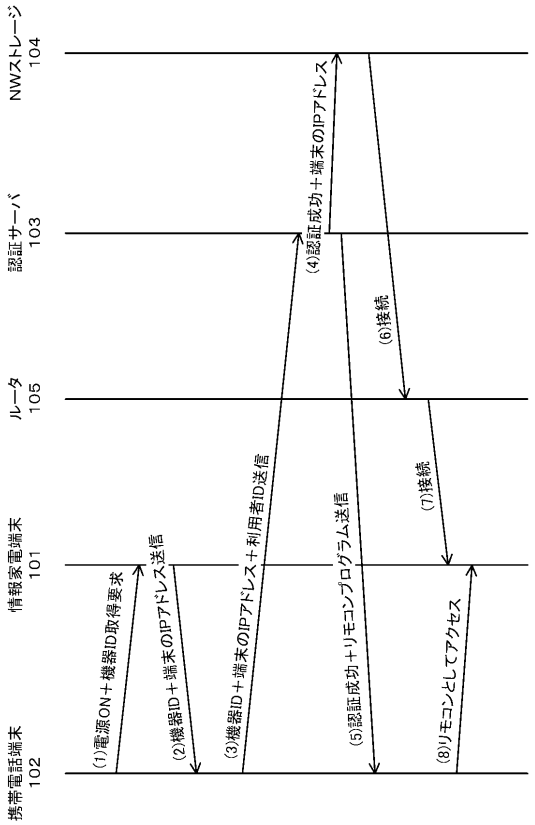
【図２２】



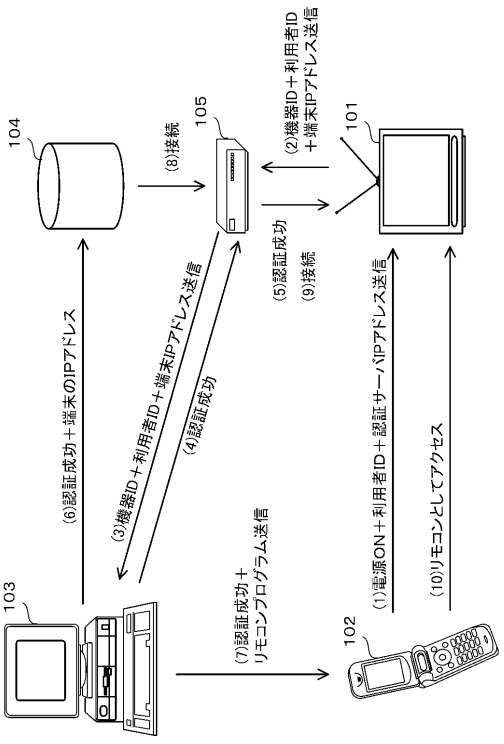
【図２３】



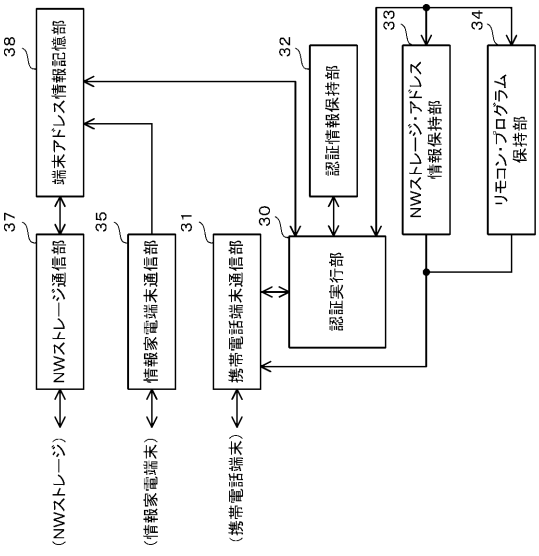
【図２４】



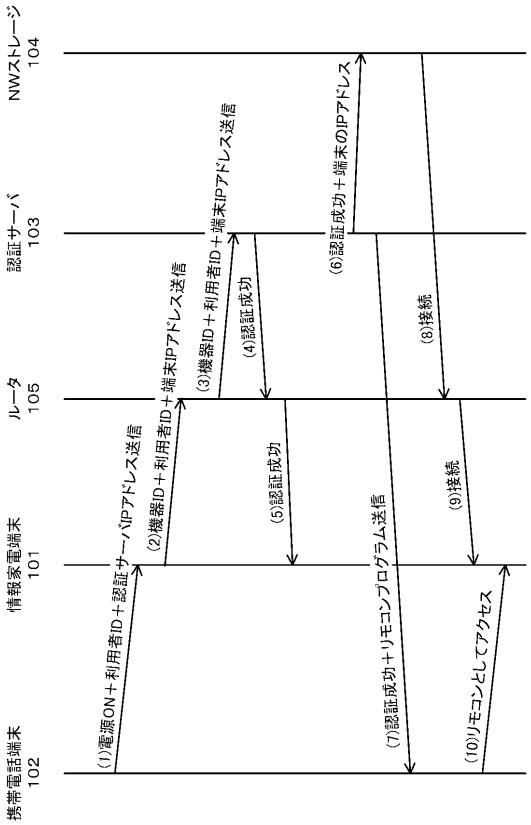
【図２５】



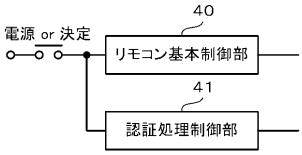
【図２６】



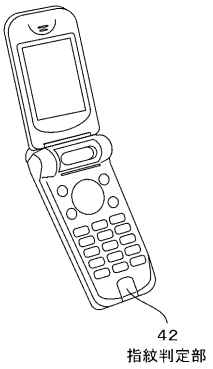
【図２７】


NWストレージ 104
認証サーバ 103
ルータ 105
情報家電端末 101
携帯電話端末 102
(1)電源ON＋利用者ID＋認証サーバIPアドレス送信
(2)機器ID＋利用者ID＋端末IPアドレス送信
(3)機器ID＋利用者ID＋端末IPアドレス送信
(4)認証成功
(5)認証成功
(6)認証成功＋端末のIPアドレス
(7)認証成功＋リモコンプログラム送信
(8)接続
(9)接続
(10)リモコンとしてアクセス

【図２８】


電源 or 決定
40
リモコン基本制御部
41
認証処理制御部

【図２９】


42
指紋判定部

フロントページの続き

(72)発明者　中川　真一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　斎藤　洋
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

審査官　宮田　繁仁

(56)参考文献　国際公開第０２／０７８３０７（WO，Ａ１）
特開２００３－１０２０７８（ＪＰ，Ａ）
特開２００４－１０４６５３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０３Ｊ　９／００－　９／０６
Ｈ０４Ｍ　３／００
Ｈ０４Ｍ　３／１６－　３／２０
Ｈ０４Ｍ　３／３８－　３／５８
Ｈ０４Ｍ　７／００－　７／１６
Ｈ０４Ｍ　１１／００－１１／１０
Ｈ０４Ｑ　９／００－　９／１６