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

特許第4677784号
(P4677784)

(45)発行日　平成23年4月27日(2011.4.27)　(24)登録日　平成23年2月10日(2011.2.10)

(51)Int.Cl.　　F I
H04L 9/32 (2006.01)　　H04L 9/00 675A
G06F 21/20 (2006.01)　　H04L 9/00 675D
　　G06F 15/00 330E

請求項の数 10　(全 14 頁)

(21)出願番号　特願2005-2306(P2005-2306)
(22)出願日　平成17年1月7日(2005.1.7)
(65)公開番号　特開2006-191429(P2006-191429A)
(43)公開日　平成18年7月20日(2006.7.20)
審査請求日　平成19年9月18日(2007.9.18)

(73)特許権者　000208891
ＫＤＤＩ株式会社
東京都新宿区西新宿二丁目３番２号
(74)代理人　100074930
弁理士　山本　恵一
(72)発明者　松中　隆志
埼玉県上福岡市大原二丁目１番１５号　株式会社ＫＤＤＩ研究所内
(72)発明者　杉山　敬三
埼玉県上福岡市大原二丁目１番１５号　株式会社ＫＤＤＩ研究所内

審査官　新田　亮

最終頁に続く

(54)【発明の名称】集合型宅内ネットワークにおける認証方法及びシステム

(57)【特許請求の範囲】
【請求項１】
複数の端末が接続されたグループ内ネットワークと、複数のグループ内ネットワークとインターネットとの間に接続された網接続装置と、該網接続装置と通信可能な認証サーバとを有するシステムにおける認証方法であって、
前記グループ内ネットワーク毎にホームステーションが備えられており、
前記ホームステーションが、前記網接続装置を介して前記認証サーバに対して認証要求メッセージを送信することによって、前記認証サーバとの間で第１の共通鍵が共有され、前記認証サーバが前記網接続装置へ前記第１の共通鍵を送信する第１のステップと、
前記網接続装置が、前記グループ内ネットワークに対する第２の共通鍵を決定し、前記第１の共通鍵を用いて暗号化した前記第２の共通鍵を前記ホームステーションへ送信する第２のステップと、
前記端末が、前記網接続装置を介して前記ホームステーションに対して認証要求メッセージを送信することによって、前記ホームステーションとの間で第３の共通鍵が共有され、前記ホームステーションが前記網接続装置へ前記第３の共通鍵を送信する第３のステップと、
前記網接続装置が、前記第３の共通鍵を用いて暗号化した前記第２の共通鍵を前記端末へ送信する第４のステップと
を有することを特徴とする認証方法。
【請求項２】

ＩＥＥＥ８０２．１ｘ認証方式が適用され、
前記第１のステップは、前記ホームステーションをSupplicantとし、前記網接続装置をAuthenticatorとし、前記認証サーバをAuthentication Serverとして機能させ、
前記第２のステップは、前記端末をSupplicantとし、前記網接続装置をAuthenticatorとし、前記ホームステーションをAuthentication Serverとして機能させることを特徴とする請求項１に記載の認証方法。
【請求項３】
前記第１のステップは、ＥＡＰ－ＴＬＳ方式が適用され、
前記第２のステップは、ＥＡＰ－ＴＬＳ方式又はＥＡＰ－ＭＤ５方式が適用されることを特徴とする請求項２に記載の認証方法。
【請求項４】
前記第２の共通鍵が、前記網接続装置と前記端末との間で通信されるデータフレームの暗号化に用いられることを特徴とする請求項１から３のいずれか１項に記載の認証方法。
【請求項５】
前記グループ内ネットワークは、宅内ネットワークであって、電力線搬送通信ネットワークであることを特徴とする請求項１から４のいずれか１項に記載の認証方法。
【請求項６】
複数の端末が接続されたグループ内ネットワークと、複数のグループ内ネットワークとインターネットとの間に接続された網接続装置と、該網接続装置と通信可能な認証サーバとを有するシステムであって、
前記グループ内ネットワーク毎にホームステーションが備えられており、
前記認証サーバは、前記網接続装置を介して前記ホームステーションから認証要求メッセージを受信することによって、前記ホームステーションとの間で第１の共通鍵を共有する認証手段と、該第１の共通鍵を前記網接続装置へ送信する共通鍵送信手段とを有し、
前記ホームステーションは、前記網接続装置を介して前記認証サーバへ認証要求メッセージを送信し、前記認証サーバとの間で第１の共通鍵を共有する認証サーバ機能手段と、前記端末から前記網接続装置を介して前記認証要求メッセージを受信し、前記端末との間で第３の共通鍵を共有する認証端末機能手段とを有し、
前記網接続装置は、前記グループ内ネットワークに対する第２の共通鍵を決定するグループ共通鍵決定手段と、前記第１の共通鍵を用いて暗号化した前記第２の共通鍵を前記ホームステーションへ送信する第１の送信手段と、前記第３の共通鍵を用いて暗号化した前記第２の共通鍵を前記ホームステーションへ送信する第２の送信手段と
を有することを特徴とするシステム。
【請求項７】
ＩＥＥＥ８０２．１ｘ認証方式が適用され、
前記ホームステーションにおける前記認証サーバ機能手段はAuthentication Serverとして機能し、前記認証端末機能手段はSupplicantとして機能することを特徴とする請求項６に記載のシステム。
【請求項８】
前記ホームステーションにおける前記認証サーバ機能手段には、ＥＡＰ－ＴＬＳ方式が適用され、前記認証端末機能手段には、ＥＡＰ－ＴＬＳ方式又はＥＡＰ－ＭＤ５方式が適用されることを特徴とする請求項７に記載のシステム。
【請求項９】
前記網接続装置は、前記端末へ送信すべきデータフレームを前記第２の共通鍵を用いて暗号化し、前記端末から受信したデータフレームを前記第２の共通鍵を用いて復号する暗号化／復号手段を更に有し、
前記端末は、前記網接続装置へ送信すべきデータフレームを前記第２の共通鍵を用いて暗号化し、前記網接続装置から受信したデータフレームを前記第２の共通鍵を用いて復号する暗号化／復号手段を更に有する
ことを特徴とする請求項６から８のいずれか１項に記載のシステム。

【請求項１０】
前記グループ内ネットワークは、宅内ネットワークであって、電力線搬送通信ネットワークであることを特徴とする請求項６から９のいずれか１項に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、集合型宅内ネットワークにおける認証方法及びシステムに関する。
【背景技術】
【０００２】
図１は、従来技術における集合型宅内ネットワークのシステム構成図である。
【０００３】
宅内ネットワークは、電話線、電力線、イーサネット（登録商標）等を用いて一般に構築されており、通信機能を有する家庭電化製品（パーソナルコンピュータ、テレビ、エアコン等）３が接続される。また、複数の宅内ネットワークは、集合ネットワークを介して網接続装置１に接続される。網接続装置１は、ＡＤＳＬ（Asymmetric Digital Subscriber Line：非対称デジタル加入者線）、光ファイバ等によってインターネットアクセス網５に接続され、更にＩＳＰ(Internet Service Provider)事業者網６を介して、インターネット７に接続される。ＩＳＰ事業者網６には、ユーザ認証のためにＩＳＰ認証サーバ４が備えられている。ＩＳＰ認証サーバ４は、契約したユーザ情報を保持する登録データベースと、ユーザ認証部とを有する。図１のようなネットワーク形態を、以下では集合型宅内ネットワークと称する。
【０００４】
図１によれば、同一建物内にあって異なる宅内ネットワークが、同一の集合ネットワークを共有する構成になっている。この場合、ある宅内ネットワークから送信された通信データが、他の宅内ネットワークに接続された端末によって傍受されるという事態が起こり得る。このような事態を防ぐため、通信データの暗号化とそのための共通鍵とを、通信を行う二者間で共有する必要がある。従来技術によれば、宅内ネットワークに接続された端末のそれぞれが、ＩＳＰ認証サーバ４に対して認証を要求し、共通鍵を共有する必要がある。
【０００５】
【特許文献１】特開２００２－３４５０５１号公報
【特許文献２】特開２００３－１７９６９９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかしながら、将来的に家庭電化製品の多くに通信機能が搭載されることを考慮すると、１つの宅内ネットワーク当たりの通信端末の数も多くなる。結果的に、集合ネットワークに接続される通信端末の数は膨大な数になる。この場合、各通信端末が認証を要求するとすると、網接続装置にとっては過負荷となってしまう。また、複数の通信端末でグループを構成し、グループ単位で共通鍵を管理しようとすると、網接続装置による処理が更に煩雑になり、現実的ではない。
【０００７】
また、近年、テレビ、エアコン等に通信機能を持たせる情報家電ネットワーク等、グループ単位での通信の秘匿性を必要とする場面が多くなっているため、グループ単位で暗号化のための共通鍵を共有する技術が必要となってきている。
【０００８】
そこで、本発明は、集合型宅内ネットワークに接続された端末における共通鍵の管理の煩雑さを低減することができる認証方法及びシステム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】

本発明は、複数の端末が接続されたグループ内ネットワークと、複数のグループ内ネットワークとインターネットとの間に接続された網接続装置と、該網接続装置と通信可能な認証サーバとを有するシステムに関する。

【００１０】

本発明における認証方法は、

グループ内ネットワーク毎にホームステーションが備えられており、

ホームステーションが、網接続装置を介して認証サーバに対して認証要求メッセージを送信することによって、認証サーバとの間で第１の共通鍵が共有され、認証サーバが網接続装置へ第１の共通鍵を送信する第１のステップと、

網接続装置が、グループ内ネットワークに対する第２の共通鍵を決定し、第１の共通鍵を用いて暗号化した第２の共通鍵をホームステーションへ送信する第２のステップと、

端末が、網接続装置を介してホームステーションに対して認証要求メッセージを送信することによって、ホームステーションとの間で第３の共通鍵が共有され、ホームステーションが網接続装置へ第３の共通鍵を送信する第３のステップと、

網接続装置が、第３の共通鍵を用いて暗号化した第２の共通鍵を端末へ送信する第４のステップとを有することを特徴とする。

【００１１】

本発明の認証方法における他の実施形態によれば、ＩＥＥＥ８０２．１ｘ認証方式が適用され、

第１のステップは、ホームステーションをSupplicantとし、網接続装置をAuthenticatorとし、認証サーバをAuthentication Serverとして機能させ、

第２のステップは、端末をSupplicantとし、網接続装置をAuthenticatorとし、ホームステーションをAuthentication Serverとして機能させることも好ましい。

【００１２】

また、本発明の認証方法における他の実施形態によれば、第１のステップは、ＥＡＰ－ＴＬＳ方式が適用され、第２のステップは、ＥＡＰ－ＴＬＳ方式又はＥＡＰ－ＭＤ５方式が適用されることも好ましい。

【００１３】

更に、本発明の認証方法における他の実施形態によれば、第２の共通鍵が、網接続装置と端末との間で通信されるデータフレームの暗号化に用いられることも好ましい。

【００１４】

更に、本発明の認証方法における他の実施形態によれば、グループ内ネットワークは、宅内ネットワークであって、電力線搬送通信ネットワークであってもよい。

【００１５】

本発明におけるシステムによれば、

グループ内ネットワーク毎にホームステーションが備えられており、

認証サーバは、網接続装置を介してホームステーションから認証要求メッセージを受信することによって、ホームステーションとの間で第１の共通鍵を共有する認証手段と、該第１の共通鍵を網接続装置へ送信する共通鍵送信手段とを有し、

ホームステーションは、網接続装置を介して認証サーバへ認証要求メッセージを送信し、認証サーバとの間で第１の共通鍵を共有する認証サーバ機能手段と、端末から網接続装置を介して認証要求メッセージを受信し、端末との間で第３の共通鍵を共有する認証端末機能手段とを有し、

網接続装置は、グループ内ネットワークに対する第２の共通鍵を決定するグループ共通鍵決定手段と、第１の共通鍵を用いて暗号化した第２の共通鍵をホームステーションへ送信する第１の送信手段と、第３の共通鍵を用いて暗号化した第２の共通鍵をホームステーションへ送信する第２の送信手段とを有することを特徴とする。

【００１６】

本発明のシステムにおける他の実施形態によれば、ＩＥＥＥ８０２．１ｘ認証方式が適用され、ホームステーションにおける認証サーバ機能手段はAuthentication Serverとし

て機能し、認証端末機能手段はSupplicantとして機能することも好ましい。
【００１７】
また、本発明のシステムにおける他の実施形態によれば、ホームステーションにおける認証サーバ機能手段には、ＥＡＰ－ＴＬＳ方式が適用され、認証端末機能手段には、ＥＡＰ－ＴＬＳ方式又はＥＡＰ－ＭＤ５方式が適用されることも好ましい。
【００１８】
更に、本発明のシステムにおける他の実施形態によれば、
網接続装置は、端末へ送信すべきデータフレームを第２の共通鍵を用いて暗号化し、端末から受信したデータフレームを第２の共通鍵を用いて復号する暗号化／復号手段を更に有し、
端末は、網接続装置へ送信すべきデータフレームを第２の共通鍵を用いて暗号化し、網接続装置から受信したデータフレームを第２の共通鍵を用いて復号する暗号化／復号手段を更に有することも好ましい。
【００１９】
更に、本発明のシステムにおける他の実施形態によれば、グループ内ネットワークは、宅内ネットワークであって、電力線搬送通信ネットワークであってもよい。
【発明の効果】
【００２０】
本発明における認証方法及びシステムよれば、集合型宅内ネットワークに接続された端末における共通鍵の管理の煩雑さを低減することができる。宅内ネットワーク毎（グループ毎）にそのネットワークに接続された端末に同一共通鍵を共有させることができ、他の宅内ネットワークに接続された端末に対して秘匿性を確保することができる。
【００２１】
また、宅内ネットワーク毎の認証を認証サーバに任せ、宅内ネットワーク内の端末の認証をホームステーションに任せることによって、認証サーバにかかる負荷を軽減することができる。
【００２２】
更に、ＩＳＰ認証サーバ４にとっては、宅内ネットワーク単位（グループ単位）で認証処理が行われるために、認証毎に課金処理を行うことによって、家庭毎に対する課金処理を容易にすることができる。
【発明を実施するための最良の形態】
【００２３】
以下では、図面を用いて、本発明を実施するための最良の形態を詳細に説明する。
【００２４】
図２は、本発明における集合型宅内ネットワークのシステム構成図である。
【００２５】
本発明によれば、宅内ネットワーク及び集合ネットワークが、電力線搬送通信ネットワークであることによって、図２のようなネットワーク構成が想定される。即ち、電力線がネットワークに用いられることによって、集合型住宅においては、複数の宅内ネットワークが接続された構成が想定される。
【００２６】
図２は、図１と比較して、ホームステーション２を更に備えている。ホームステーション２は、通信制御部２１と、送受信部２２と、グループ内登録端末データベース２３と、Supplicant機能部２４と、Authenticator Server機能部２５と、認証情報記憶部２６と、共通鍵復号部２７と、共通鍵記憶部２８と、暗号化／復号部２９とを有する。
【００２７】
送受信部２２は、宅内ネットワークと称されるグループ内ネットワークに接続されており、データパケットを送受信する。通信制御部２２は、データフレームの生成及び解析を行い、他の機能部と関連して動作する。グループ内登録端末データベース２３は、当該宅内ネットワークに接続されている端末の識別子（ＩＤ：IDentifier）と、その情報とを記

憶している。

【００２８】

Supplicant機能部２４は、ＩＥＥＥ８０２．１ｘによれば、Authenticatorである網接続装置１を介して、ＩＳＰ認証サーバ４に対するSupplicantとして機能する。従って、Supplicant機能部２４は、ＩＳＰ認証サーバ４との間で共通鍵Ｋａを共有することができる。

【００２９】

Authenticator Server機能部２５は、ＩＥＥＥ８０２．１ｘによれば、Authenticatorである網接続装置１を介して、Supplicantである端末３に対するAuthentication Serverとして機能する。従って、Authenticator Server機能部２５は、端末３との間で共通鍵Ｋｂを共有することができる。

【００３０】

認証情報記憶部２６は、ＩＳＰ認証サーバ４との間で共有した共通鍵Ｋａと、端末３との間で共有した共通鍵Ｋｂとを記憶する。

【００３１】

共通鍵復号部２７は、暗号化された共通鍵Ｋ１を復号する。共通鍵Ｋ１は、当該宅内ネットワークの全ての端末に割り当てられる鍵であって、網接続装置１から、共通鍵Ｋａを用いて暗号化して送信される。復号するための共通鍵Ｋａは、Supplicant機能部２４から通知される。

【００３２】

共通鍵記憶部２８は、共通鍵復号部２７によって復号された共通鍵Ｋ１を記憶する。

【００３３】

暗号化／復号部２９は、送信すべきデータフレームを共通鍵Ｋ１によって暗号化し、又は、受信したデータフレームを共通鍵Ｋ１によって復号する。

【００３４】

図２によれば、本発明による網接続装置１は、図１と比較して、更なる機能を有する。網接続装置１は、通信制御部１１と、インターネット側送受信部１２と、宅内ネットワーク側送受信部１３と、Authenticator機能部１４と、グループ共通鍵決定部１５と、グループ共通鍵データベース１６と、ホームステーション側グループ共通鍵送信部１７と、端末側グループ共通鍵送信部１８と、暗号化／復号部１９とを有する。

【００３５】

通信制御部１１は、データフレームの生成及び解析を行い、他の機能部と関連して動作する。インターネット側送受信部１２は、インターネットアクセス網５に接続されており、インターネット７及びＩＳＰ認証サーバ４とデータパケットを送受信する。宅内ネットワーク側送受信部１３は、複数の宅内ネットワークが接続された集合ネットワークに接続されており、ホームステーション２及び端末３とデータパケットを送受信する。

【００３６】

Authenticator機能部１４は、ＩＥＥＥ８０２．１ｘによれば、Supplicantであるホームステーション２に対して及びＩＳＰ認証サーバ４に対して、Authenticatorとして機能する。また、Authenticator機能部１４は、Supplicantである端末３に対して及びAuthentication Serverであるホームステーション２に対して、Authenticatorとしても機能する。

【００３７】

グループ共通鍵決定部１５は、ホームステーション２とＩＳＰ認証サーバ４との間で認証が完了した際に、そのホームステーション２が存在する宅内ネットワークに接続された端末に割り当てる共通鍵Ｋ１を決定する。共通鍵Ｋ１の決定方法は、任意の既存技術によって行われる。

【００３８】

グループ共通鍵データベース１６は、グループ共通鍵決定部１５によって決定された共通鍵Ｋ１を、宅内ネットワーク識別子（グループ識別子）HID1に対応付けて蓄積する。例

えば、宅内ネットワーク識別子HID1に対応付けて、共通鍵Ｋ１が蓄積されている。

【００３９】

ホームステーション側共通鍵送信部１７は、グループ共通鍵決定部１５によって決定された共通鍵Ｋ１を、Authenticator機能部１４によってＩＳＰ認証サーバ４との間で共有された共通鍵Ｋａによって暗号化して、ホームステーション２へ送信する。

【００４０】

端末側共通鍵送信部１８は、グループ共通鍵決定部１５によって決定された共通鍵Ｋ１を、Authenticator機能部１４によってホームステーション２との間で共有された共通鍵Ｋｂによって暗号化して、端末３へ送信する。

【００４１】

暗号化／復号部２９は、宅内ネットワークに対して送信すべきデータフレームを共通鍵Ｋ１によって暗号化し、又は、宅内ネットワークから受信したデータフレームを共通鍵Ｋ１によって復号する。

【００４２】

図３は、本発明における概念的な認証のシーケンス図である。

【００４３】

ホームステーション２と認証サーバ４との間の認証方式には、ＩＥＥＥ８０２．１ＸのＥＡＰ－ＴＬＳ(Extensible Authentication Protocol - Transport Layer Security)が適用されている。ＥＡＰ－ＴＬＳは、クライアント及びサーバの双方に、認証局が発行した証明書によって相互に認証する方式である。これにより、従来、固定であったセッションキーを自動的に生成することができ、電子証明書による認証を行うことによって、セキュリティを強化することができる。

【００４４】

図３のＳ３０１～Ｓ３０７によれば、ホームステーション２はSupplicantとして機能し、網接続装置１はAuthenticatorとして機能し、ＩＳＰ認証サーバ４はAuthentication Serverとして機能する。一方、Ｓ３０８～Ｓ３１８によれば、端末３はSupplicantとして機能し、網接続装置１はAuthenticatorとして機能し、ホームステーションはAuthentication Serverとして機能する。尚、図３、図４及び図５の対応関係を明らかにするために、同じシーケンス番号は、同じ機能を意味する。

【００４５】

（Ｓ３０１～Ｓ３０５）ホームステーション２と網接続装置１との間は、ＩＥＥＥ８０２．１ｘにおけるEAPOL(EAP over LAN)が適用され、網接続装置１とＩＳＰ認証サーバ４との間はEAPoverRADIUSが適用される。これにより、ホームステーション２とＩＳＰ認証サーバ４との間で、共通鍵Ｋａが共有される。このとき、網接続装置１は、共通鍵Ｋａを知らない。

（Ｓ３０６）ＩＳＰ認証サーバ４は、共通鍵Ｋａを網接続装置１へ送信する。これにより、網接続装置１も、ホームステーション２も共通鍵Ｋａを共有することができる。

（Ｓ３０７）網接続装置１は、宅内ネットワークに対する共通鍵Ｋ１を決定する。共通鍵Ｋ１は、共通鍵Ｋａを用いて暗号化されて、網接続装置１からホームステーション２へ送信される。ホームステーション２は、暗号化された共通鍵Ｋ１を、共通鍵Ｋａを用いて復号し、共通鍵Ｋ１を取得する。これにより、ホームステーション２も共通鍵Ｋ１を共有することができる。

【００４６】

（Ｓ３０８～Ｓ３１５）端末３と網接続装置１との間は、ＩＥＥＥ８０２．１ｘにおけるEAPOL(EAP over LAN)が適用され、網接続装置１とホームステーション２との間はEAPoverRADIUSが適用される。これにより、端末３とホームステーション２との間で、共通鍵Ｋｂを共有することができる。このとき、網接続装置１は、共通鍵Ｋｂを知らない。

（Ｓ３１６）ホームステーション２は、共通鍵Ｋｂを網接続装置１へ送信する。これにより、網接続装置１も、共通鍵Ｋｂを共有することができる。

（Ｓ３１８）網接続装置１は、共通鍵Ｋ１を共通鍵Ｋｂを用いて暗号化して、端末３へ送

信する。端末３は、暗号化された共通鍵Ｋ１を、共通鍵Ｋｂを用いて復号し、共通鍵Ｋ１を取得する。これにより、端末３と網接続装置１との間で、共通鍵Ｋ１を共有することができ、端末３は、インターネットにアクセスすることが可能となる。

【００４７】

図４は、本発明における具体的な認証の第１のシーケンス図である。

【００４８】

（Ｓ３０１）ホームステーション２は、EAPOL-Startを網接続装置１へ送信する。

（Ｓ３０２）EAPOL-Startを受信した網接続装置１は、識別子要求のためのEAP-Requestをホームステーション２へ送信する。

（Ｓ３０３）EAP-Requestを受信したホームステーション２は、EAP-Responseを網接続装置１へ送信する。EAP-Responseは、宅内ネットワークを示すグループ識別子HID1と、ホームステーション２の端末識別子IDst1と、自らがホームステーションであることを示すフラグ情報とを含む。これに対し、網接続装置１は、フラグ情報によってEAP-Responseの送信元端末がホームステーションであることを認識した場合、RADIUS Access RequestをＩＳＰ認証サーバへ送信する。RADIUS Access Requestは、宅内ネットワークのグループ識別子HID1を含む。

【００４９】

（Ｓ３０４）ＩＳＰ認証サーバ４は、予め登録ユーザリストを保持している。RADIUS Access Requestによって受信されたグループ識別子が、登録ユーザリストに存在するか否かを判断する。登録ユーザリストに当該グループ識別子が存在する場合、ＥＡＰ－ＴＬＳ認証を開始する旨を示すRADIUS Access Challenge(TLS Start)を網接続装置１へ送信する。RADIUS-Access Challengeを受信した網接続装置１は、EAP-Requestをホームステーション２へ送信する。

（Ｓ３０５）ホームステーション２と認証サーバ４との間でＴＬＳネゴシエーションが行われる。これにより、ホームステーション２と認証サーバ４との間で共通鍵Ｋａが共有される。

【００５０】

（Ｓ３０６）認証が成功すると、ＩＳＰ認証サーバ４は、認証が成功したことを示すRADIUS-Access Successを網接続装置１へ送信する。RADIUS-Access Successには、共通鍵Ｋａが含まれる。これにより、網接続装置１も共通鍵Ｋａを共有することができる。尚、共通鍵Ｋａは、網接続装置１とＩＳＰ認証サーバ４との間で予め共有した共通鍵で暗号化されて、RADIUS-Access Successに付加される。RADIUS-Access Successを受信した網接続装置１は、その共通鍵Ｋａを保持した上で、ホームステーション２へEAP-Successを送信する。

【００５１】

（Ｓ３０７）網接続装置１は、ホームステーション２を含む宅内ネットワークに接続された全ての端末３に割り当てる共通鍵Ｋ１を決定する。この共通鍵Ｋ１は、共通鍵Ｋａで暗号化されてホームステーション２へ送信される。このとき、網接続装置１は、グループ識別子HID1と共通鍵Ｋ１とを対応付けて、グループ共通鍵データベース１６に登録する。更に、網接続装置１は、全てのホームステーションで共有する共通鍵ＫＢも生成する。この共通鍵ＫＢは、共通鍵Ｋａで暗号化されてホームステーション２へ送信される。ホームステーション２と網接続装置１との間で、共通鍵Ｋ１及びＫＢが共有される。

【００５２】

（Ｓ３０８）端末３は、EAPOL-Startを網接続装置１へ送信する。

（Ｓ３０９）EAPOL-Startを受信した網接続装置１は、識別子要求のためのEAP-Requestを端末３へ送信する。

（Ｓ３１０）EAP-Requestを受信したホームステーション２は、EAP-Responseを網接続装置１へ送信する。EAP-Responseは、宅内ネットワークを示すグループ識別子HID1と、端末３の端末識別子IDaと、自らがホームステーションでないことを示すフラグ情報とを含む。

（Ｓ３１１）網接続装置１は、フラグ情報によってEAP-Responseの送信元端末がホームステーションでないことを認識した場合、RADIUS Access Requestをホームステーション２へ送信する。RADIUS Access Requestは、端末識別子IDaを含む。

【００５３】

（Ｓ３１２）ホームステーション２は、端末データベース２３に、登録端末識別子リストを保持している。RADIUS Access Requestによって受信された端末識別子IDaが、登録端末識別子リストに存在するか否かを判断する。登録端末識別子リストに当該グループ識別子が存在する場合、ＥＡＰ－ＴＬＳ認証を開始する旨を示すRADIUS Access Challenge(TLS Start)を網接続装置１へ送信する。

（Ｓ３１３）RADIUS-Access Challengeを受信した網接続装置１は、EAP-Requestを端末３へ送信する。

（Ｓ３１４）ホームステーション２と端末３との間でＴＬＳネゴシエーションが行われる。これにより、ホームステーション２と端末３の間で共通鍵Ｋｂが共有される。

【００５４】

（Ｓ３１６）認証が成功すると、ホームステーション２は、認証が成功したことを示すRADIUS-Access Successを網接続装置１へ送信する。RADIUS-Access Successには、共通鍵Ｋｂが含まれる。これにより、網接続装置１も共通鍵Ｋｂを共有することができる。

（Ｓ３１７）RADIUS-Access Successを受信した網接続装置１は、その共通鍵Ｋｂを保持した上で、端末３へEAP-Successを送信する。

【００５５】

（Ｓ３１８）網接続装置１は、共通鍵Ｋ１を共通鍵Ｋｂで暗号化して、端末３へ送信する。端末３は、共通鍵Ｋｂを用いて復号し、共通鍵Ｋ１を取得する。端末３と網接続装置１との間で、共通鍵Ｋ１を共有することができ、端末３は、インターネットにアクセスすることが可能となる。

【００５６】

図５は、本発明における具体的な認証の第２のシーケンス図である。

【００５７】

図５は、図４と比較して、Ｓ３１２～Ｓ３１７のみが異なる。従って、以下ではＳ３１２～Ｓ３１７のみついて説明する。

【００５８】

図５によれば、端末３とホームステーション２との間の認証方式には、ＩＥＥＥ８０２．１ＸのＥＡＰ－ＭＤ５認証を適用している。ＥＡＰ－ＭＤ５は、パスワードによるハッシュ値を利用したものであって、一方向認証のみである。ＥＡＰ－ＭＤ５は、ＥＡＰ－ＴＬＳと比較して認証が簡易であって、ホームステーションをAuthentication Serverとして機能させる場合に、ホームステーションの実装が比較的容易となる。

【００５９】

（Ｓ３１２）ホームステーション２は、RADIUS Access Requestによって受信された端末識別子IDaが、登録端末識別子リストに存在するか否かを判断する。登録端末識別子リストに端末識別子が存在する場合、ホームステーション２は、乱数ｒａを生成する。そして、ホームステーション２は、ＥＡＰ－ＭＤ５認証を開始する旨を示すRADIUS Access Challengeを網接続装置１へ送信する。RADIUS Access Challengeには、乱数ｒａが含まれる。

（Ｓ３１３）RADIUS Access Challengeを受信した網接続装置１は、EAP-Requestを端末３へ送信する。EAP-Requestには、乱数ｒａが含まれる。

【００６０】

（Ｓ３１４）端末３は、自らの端末識別子（ＩＤａ）と、EAP-Requestに含まれた乱数ｒａと、ホームステーション２との間で予め共有しているパスワードＰａとに基づいて、ＭＤ５のハッシュ関数を用いてハッシュ値を計算する。そして、端末３は、そのハッシュ値を含むEAP-Responseを網接続装置１へ送信する。パスワードＰａは、宅内ネットワーク即ちグループで共通であってよいし、セキュリティ上の観点から端末毎に異なるものであってもよい。

（Ｓ３１５）網接続装置１は、EAP-Responseによって受信されたハッシュ値を含むRADIUS Access Responseをホームステーション２へ送信する。
（Ｓ３１６）ホームステーション２は、自らの端末識別子（ＩＤｓｔ１）と、EAP-Responseに含まれた乱数ｒａと、端末３との間で予め共有しているパスワードＰａとに基づいて、ＭＤ５のハッシュ関数を用いてハッシュ値Ｋｂを計算する。そして、ホームステーション２は、RADIUS Access Responseによって受信されたハッシュ値と、計算されたハッシュ値Ｋｂとを比較して、一致するか否かを判断する。一致した場合、認証が成功したこと示すRADIUS Access Acceptを網接続装置１へ送信する。RADIUS Access Acceptには、ハッシュ値Ｋｂが共通鍵として含まれる。
（Ｓ３１７）網接続装置１は、受信したRADIUS Access Acceptからハッシュ値Ｋｂを取得する。そして、網接続装置１は、端末３へ認証成功を示すEAP-Successを送信する。これにより、網接続装置１と端末３との間で共通鍵Ｋｂが共有される。
【００６１】
図６は、端末とインターネットとの間のデータパケットのシーケンス図である。
【００６２】
（Ｓ４０１）端末３は、データフレームのＭＡＣ層ヘッダに、自端末識別子IDaと宅内ネットワークの識別子HIDとを含む。また、データフレームに、自端末識別子IDaと宅内ネットワークの識別子HIDと共通鍵Ｋ１とを用いて算出したデータフレームのＭＡＣ(Message Authentication Code)を付与する。更に、共通鍵Ｋ１を用いてデータフレームを暗号化する。このデータフレームは、端末３から網接続装置１へ送信される。データフレームは、例えば表１のようになる。
【００６３】
【表１】

PHY 層 ﾍｯﾀﾞ	MAC 層 ﾍｯﾀﾞ	IDa	HID	MAC 層ﾍﾟｲﾛｰﾄﾞ部	MAC	FCS
	<----MAC 層ﾍｯﾀﾞ ----->			<------暗号化部分-------->		

【００６４】
（Ｓ４０２）網接続装置１は、データフレームに含まれるHIDに対応する共通鍵Ｋ１を検索する。そして、共通鍵Ｋ１を用いてペイロード部分を復号する。更に、付与されたＭＡＣを当該共通鍵で検証する。検証が成功した場合、データフレームを再構築し、インターネットアクセス網に転送する。検証に失敗した場合は、当該フレームを破棄する。
【００６５】
（Ｓ４０３）インターネットアクセス網から送られてきたデータフレームを受信した網接続装置１は、当該データフレームから端末識別子IDaを抽出する。
（Ｓ４０４）網接続装置１は、全てのホームステーション２に対して、当該端末がどこのグループに所属するかを問い合わせる。尚、このメッセージは、全てのホームステーションで共有している共通鍵ＫＢで暗号化されている。
【００６６】
（Ｓ４０５）各ホームステーションは当該メッセージを共通鍵ＫＢで復号する。そして、当該端末が自身の配下に存在する場合、網接続装置１に対して当該端末が自身のグループに属していることを通知する。図６によれば、端末IDaがグループHID1に属しているため、当該グループのホームステーションIDstが、網接続装置１に対して端末IDaが所属しているグループＩＤ（HID1）を通知する。
【００６７】
（Ｓ４０６）当該端末の所属グループを知った網接続装置１は、端末ＩＤ、グループＩＤ及び共通鍵Ｋ１を用いて算出したデータフレームのＭＡＣを付与したデータフレームを作成し、更に共通鍵Ｋ１を用いてデータフレームを暗号化して端末ＩＤａに送信する。
【００６８】
尚、セキュリティの観点から、網接続装置１にてデータフレームの検証を行う際に、デ

ータフレームの送信元である端末が正規のユーザであるかどうかを、ホームステーションに問い合わせた後、データフレームの転送又は破棄を決定することも好ましい。

【００６９】

前述した本発明における種々の実施形態によれば、本発明の技術思想及び見地の範囲の種々の変更、修正及び省略を、当業者は容易に行うことができる。前述の説明はあくまで例であって、何ら制約しようとするものではない。本発明は、特許請求の範囲及びその均等物として限定するものにのみ制約される。

【図面の簡単な説明】

【００７０】

【図１】従来技術における集合型宅内ネットワークのシステム構成図である。

【図２】本発明における集合型宅内ネットワークのシステム構成図である。

【図３】本発明における概念的な認証のシーケンス図である。

【図４】本発明における具体的な認証の第１のシーケンス図である。

【図５】本発明における具体的な認証の第２のシーケンス図である。

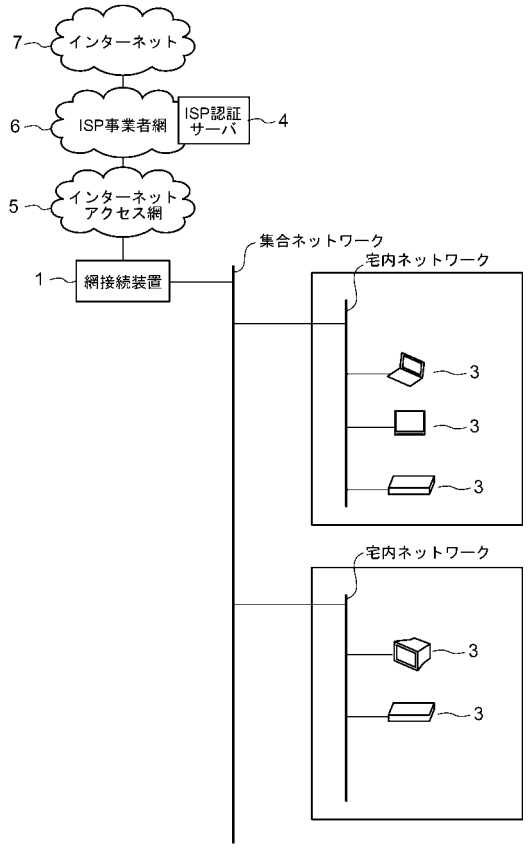
【図６】端末とインターネットとの間のデータパケットのシーケンス図である。

【符号の説明】

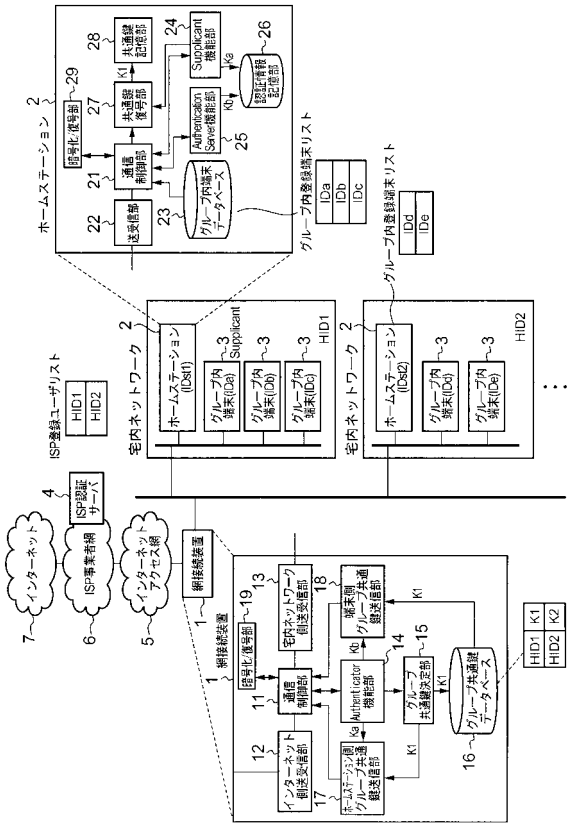
【００７１】

１　網接続装置
１１　通信制御部
１２　インターネット側送受信部
１３　宅内ネットワーク側送受信部
１４　Authenticator機能部
１５　グループ共通鍵決定部
１６　グループ共通鍵データベース
１７　ホームステーション側グループ共通鍵送信部
１８　端末側グループ共通鍵送信部
１９　暗号化／復号部
２　ホームステーション
２１　通信制御部
２２　送受信部
２３　グループ内端末データベース
２４　Supplicant機能部
２５　Authenticator Server機能部
２６　認証情報記憶部
２７　共通鍵復号部
２８　共通鍵記憶部
２９　暗号化／復号部
３　端末
４　ＩＳＰ認証サーバ
５　インターネットアクセス網
６　ＩＳＰ事業者網
７　インターネット

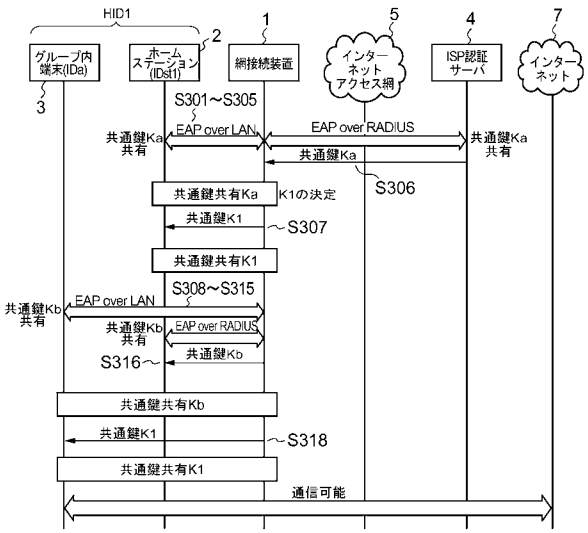
【図１】


7
インターネット
6
ISP事業者網
ISP認証サーバ
4
5
インターネットアクセス網
1
網接続装置
集合ネットワーク
宅内ネットワーク
3
3
3
宅内ネットワーク
3
3

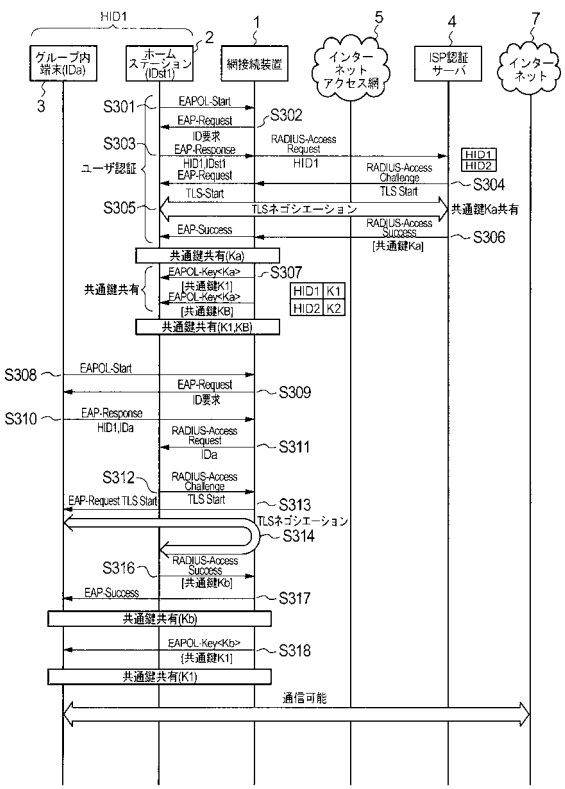
【図２】


ホームステーション 2
共通鍵記憶部 28
Supplicant機能部 24
認証情報記憶部 26
暗号化復号部 29
共通鍵復号部 27
Authenticator機能部 25
通信制御部 21
送信信部 22
グループ内端末データベース 23
グループ内登録端末リスト
IDa
IDb
IDc
IDd
IDe
ISP登録ユーザリスト
HID1
HID2
宅内ネットワーク
ホームステーション(IDst1)
グループ内端末(IDa)
グループ内端末(IDb)
グループ内端末(IDc)
ホームステーション(IDst2)
グループ内端末(IDd)
グループ内端末(IDe)
ISP認証サーバ 4
インターネット 7
ISP事業者網 6
インターネットアクセス網 5
網接続装置 1
宅内ネットワーク制御部 13
端末側グループ共通鍵送信部 18
暗号化復号部 19
通信制御部 11
Authenticator機能部 14
グループ共通鍵決定部 15
グループ共通鍵データベース 16
インターネット側送受信部 12
ホームステーション側グループ共通鍵送信部 17
K1
K2

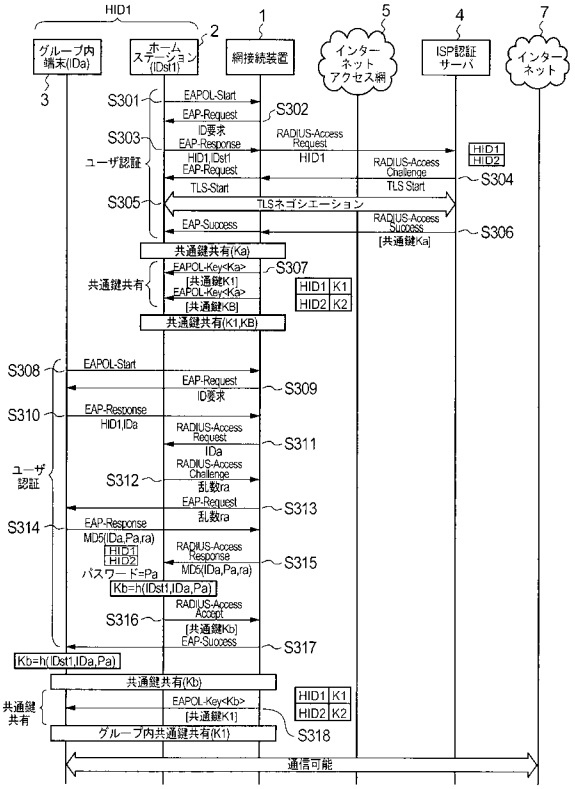
【図３】


HID1
グループ内端末(IDa) 3
ホームステーション(IDst1) 2
網接続装置 1
インターネットアクセス網 5
ISP認証サーバ 4
インターネット 7
S301～S305
EAP over LAN
EAP over RADIUS
共通鍵Ka共有
共通鍵Ka
S306
共通鍵共有Ka
K1の決定
共通鍵K1
S307
共通鍵共有K1
S308～S315
共通鍵Kb共有
EAP over LAN
EAP over RADIUS
共通鍵Kb
S316
共通鍵共有Kb
S318
通信可能

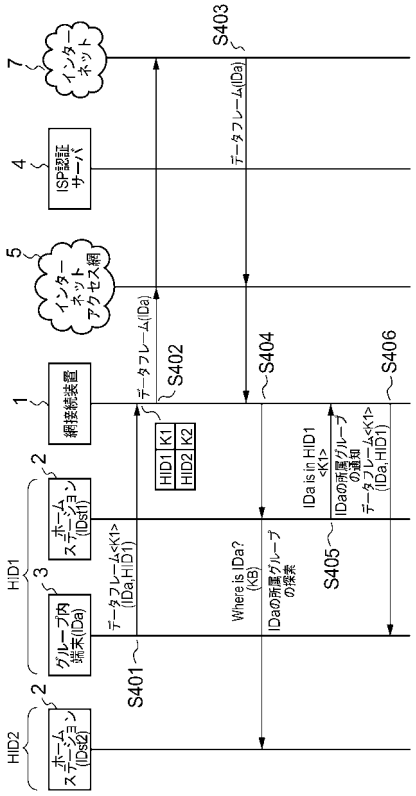
【図４】


HID1
グループ内端末(IDa) 3
ホームステーション(IDst1) 2
網接続装置 1
インターネットアクセス網 5
ISP認証サーバ 4
インターネット 7
S301 EAPOL-Start
S302 EAP-Request ID要求
S303 EAP-Response HID1,IDst1
RADIUS-Access Request HID1
ユーザ認証
RADIUS-Access Challenge TLS Start
S304
HID1 HID2
S305 TLS-Start
TLSネゴシエーション
共通鍵Ka共有
EAP-Success
RADIUS-Access Success [共通鍵Ka]
S306
共通鍵共有(Ka)
EAPOL-Key<Ka> [共通鍵K1] EAPOL-Key<Ka> [共通鍵Kb]
S307
共通鍵共有
HID1 K1
HID2 K2
共通鍵共有(K1,Kb)
S308 EAPOL-Start
EAP-Request ID要求
S309
S310 EAP-Response HID1,IDa
RADIUS-Access Request IDa
S311
S312 RADIUS-Access Challenge EAP-Request TLS Start
TLS Start
S313
TLSネゴシエーション
S314
S316 RADIUS-Access Success [共通鍵Kb]
EAP-Success
S317
共通鍵共有(Kb)
EAPOL-Key<Kb> [共通鍵K1]
S318
共通鍵共有(K1)
通信可能

【図５】


HID1
グループ内端末(IDa)
3
ホームステーション(IDst1)
2
網接続装置
1
インターネットアクセス網
5
ISP認証サーバ
4
インターネット
7
S301
EAPOL-Start
EAP-Request
S302
S303
ID要求
EAP-Response
RADIUS-Access Request
HID1
HID1
HID2
ユーザ認証
HID1,IDst1
EAP-Request
RADIUS-Access Challenge
S304
TLS-Start
TLS Start
S305
TLSネゴシエーション
EAP-Success
RADIUS-Access Success
[共通鍵Ka]
S306
共通鍵共有(Ka)
EAPOL-Key<Ka>
S307
共通鍵共有
[共通鍵K1]
EAPOL-Key<Ka>
HID1 K1
HID2 K2
[共通鍵KB]
共通鍵共有(K1,KB)
S308
EAPOL-Start
EAP-Request
S309
ID要求
S310
EAP-Response
HID1,IDa
RADIUS-Access Request
S311
IDa
ユーザ認証
S312
RADIUS-Access Challenge
乱数ra
EAP-Request
S313
乱数ra
S314
EAP-Response
MD5(IDa,Pa,ra)
HID1
HID2
RADIUS-Access Response
S315
MD5(IDa,Pa,ra)
パスワード=Pa
Kb=h(IDst1,IDa,Pa)
RADIUS-Access Accept
S316
[共通鍵Kb]
EAP-Success
S317
Kb=h(IDst1,IDa,Pa)
共通鍵共有(Kb)
共通鍵共有
EAPOL-Key<Kb>
HID1 K1
HID2 K2
[共通鍵K1]
S318
グループ内共通鍵共有(K1)
通信可能

【図６】


S403
7
インターネット
データフレーム(IDa)
4
ISP認証サーバ
5
インターネットアクセス網
データフレーム(IDa)
S402
S404
S406
1
網接続装置
HID1 K1
HID2 K2
2
ホームステーション(IDst1)
IDa is in HID1 <K1>
IDaの所属グループの通知
データフレーム<K1>(IDa,HID1)
HID1
3
グループ内端末(IDa)
データフレーム<K1>(IDa,HID1)
Where is IDa? (KB)
IDaの所属グループの探索
S405
S401
2
ホームステーション(IDst2)
HID2

フロントページの続き

(56)参考文献 特開２００３－１１１１５６（ＪＰ，Ａ）
特開２００２－２７１３０９（ＪＰ，Ａ）
特開２００４－２９７２９２（ＪＰ，Ａ）
特開２００１－０５３７７９（ＪＰ，Ａ）
特開２００４－２７４３５９（ＪＰ，Ａ）
特開２００４－１９４０１６（ＪＰ，Ａ）
特開２００４－３２０１３９（ＪＰ，Ａ）
斉藤　健　他，デジタル家電の接続を考慮したホームゲートウェイアーキテクチャ，電子情報通信学会１９９８年通信ソサイエティ大会講演論文集２　PROCEEDINGS OF THE 1998 COMMUNICATIONS SOCIETY CONFERENCE OF IEICE，１９９８年　9月，第266頁

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／３２
Ｇ０６Ｆ　２１／２０