

I Tマンションにおけるサービス認証システムの開発

中本 与一[†] 牧元 喜宣[†] 澤村 伸一[†]日立製作所 システム開発研究所[†]

1. 緒言

マンション等の集合住宅において、エレベータやホール等の共用部分及び玄関の電気錠やエアコン等の専有部の家電機器をネットワーク対応にした IT マンション[1]が普及しつつある。近年、ネットワーク対応機器の高機能化、多様化に伴い、従来サービスである宅外からの電気錠操作等に加え、VoD (Video On Demand) やヘルスケアサービスなど様々な IT マンション向けサービスの開発が進められている。

一方、様々な機器がマンション内の IP ネットワークに接続されるようになると、盗聴、改ざん、成りすまし等の脅威への対策が必須となる。本報では、サービス利用時にユーザおよび機器の正当性を保証する、サービス認証システムの開発を行う。

2. IT マンションシステム

ITマンションシステムの概略図を図 1に示す。ITマンションシステムでは、各住戸にホームサーバが設置されており、マンション居住者であるユーザはホームサーバにアクセスすることで、宅内機器の状態取得や制御を実現する。マンション内はLAN (Local Area Network) が構築され、マンションルータを介してインターネットに接続されている。また、各住戸でVLAN (Virtual LAN) が構築されており、各ホームサーバには、マンション内からは各住戸内のPC、マンション外からはデータセンタからのみアクセス可能である。そのため外出先から携帯電話等でホームサーバにアクセスする場合は、データセンタを経由する必要がある。データセンタでは、ITマンションのユーザ情報が管理されており、インターネットを通じて、各ITマンション内のホームサーバ、宅内機器、マンション設備のリモート制御や保守管理を実現している。データセンタとITマンションのホームサーバ間は、相互認証および通信路の暗号化によって、セキュアな通信路が確保されている。

従来サービスでは、制御対象となる機器は、ホームサーバに直接接続された非 IP 機器のみで

あったため、セキュリティ対策はホームサーバのみに行われていた。今後、マンション向けサービスの多様化に伴い、ユーザが自由にマンション LAN に接続可能な IP 機器も対象となるため、機器および利用者の正当性を保証する認証システムが必要となる。

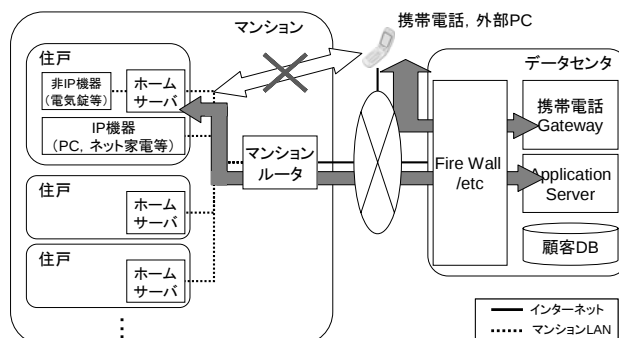


図 1 IT マンションシステム概略図

3. サービス認証システムの開発

3.1 従来のユーザ認証の問題点

通常、サービスを提供する際は、サービス利用者の正当性を保証するために、各種認証ファクタを用いたユーザ認証が行われる[2]。認証ファクタおよびその特徴について表 1に示す。

表 1 従来の認証ファクタ

認証ファクタ	本人性	利便性	端末コスト
パスワード	△	×	○
トークン	△	△	△
生体情報	○	△	×

本人性に関しては、生体情報が最も優れており、パスワードやトークンは、盗難や貸与により容易に他人が成りすますることが可能である。利便性に関しては、いずれの認証ファクタも毎回の入力作業が必要であり、特にパスワードは煩雑性が高い。端末コストに関しては、パスワードは特別な追加ハードウェアは不要であるため低コストであるが、トークンや生体情報は、専用の入力装置が必要となるため高コストとなる。

上記の通り、従来の認証ファクタは、本人性、利便性、端末コストに関して一長一短である。そこで、IT マンション向けサービス認証システ

「Development of a Service Authorization System for IT Condominium Buildings」

[†] Yoichi, NAKAMOTO Yoshinobu, MAKIMOTO Shin'ichi, SAWAMURA

[†] Systems Development Laboratory, Hitachi Ltd.

ムの開発にあたり、従来のユーザ認証の欠点を補う新たな認証方式として、ホームサーバを認証ファクタに用いる居室認証方式を考案した。

3.2 居室認証方式

居室認証方式は、サービス利用者本人の認証を行う代わりに、サービスを利用している居室が正当なサービス契約者の住戸内であるかを認証する、認証方式である。サービスの利用居室の特定には、ホームサーバを利用する。ホームサーバは、IT マンション内の各住戸に 1 台ずつ設置されており、設置されている住戸以外からはアクセスできない。そこで、ホームサーバをアクセスポイントとして利用し、サービス利用者が利用する機器（サービス機器）とサービス提供サーバ（データセンタ）間の通信をホームサーバ経由で行うことで、サービスの利用居室を特定する。

3.3 サービス認証システムの基本原理

居室認証方式を適用したサービス認証システムの基本原理を図 2 に示す。ホームサーバには固有のホームサーバ ID (HSID) が格納され、ユーザが利用するサービス機器には固有の機器 ID が格納されている。データセンタでは機器 ID およびその機器を利用可能な契約者宅のホームサーバ ID の組があらかじめ登録されている。

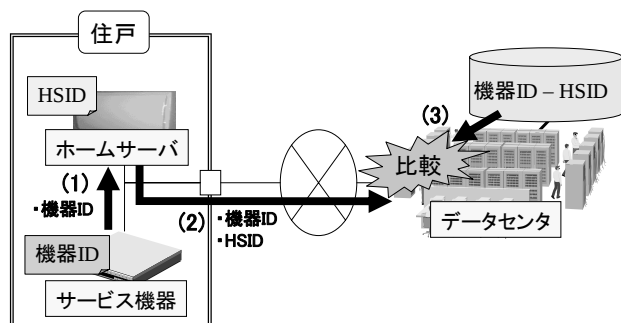


図 2 サービス認証システム基本原理

以下、図 2 の (1)～(3) に従って認証手順を説明する。

- (1) 宅内機器利用時に、まず宅内機器が機器 ID を居室内のホームサーバに送信する。
- (2) ホームサーバは受信した機器 ID と自身のホームサーバ ID をデータセンタに送信する。
- (3) データセンタは受信した機器 ID およびホームサーバ ID の組を、あらかじめ登録されている ID の組と比較する。正しい組の場合は認証成功とし、不正な組の場合は認証失敗とする。

3.4 プロトタイプシステムの構築

前節で述べた基本原理を基に、サービス認証システムのプロトタイプシステムを構築した。サービス機器として Web ブラウザ搭載のセットトップボックス (STB) を用い、ホームサーバおよびデータセンタサーバは実際の IT マンションシステムとほぼ同等の機器を用いた。本システムにおいて、ユーザが STB の Web ブラウザを用いて、ホームサーバ経由でデータセンタ上の Web コンテンツを取得するまでの一連の処理の動作検証を行った。

3.5 検証結果

動作検証の結果、正当な機器を正当な居室で使用する場合のみ、サービスを利用可能であることを確認した。居室認証方式の本人性は、現状の IT マンションシステムで保証されている、ホームサーバの本人性と同等であり、成りすましが困難であるため、パスワードやトークンよりも優れていると考えられる。利便性に関しては、ユーザの入力処理が一切不要であるため、従来のどのユーザ認証よりも優れている。端末コストに関しては、追加のハードウェアコストが一切不要であり、パスワード認証とほぼ同等のコストであると考えられる。

以上より、本サービス認証システムは IT マンションシステムにおいて従来よりも優れた認証システムであると考えられる。ただし、今回は通信データが比較的小容量の Web コンテンツであり、VoD サービス等の大容量コンテンツの通信を行う場合には、ホームサーバの負荷が増大することにより、他のマンション向けサービスに悪影響を及ぼす可能性も十分考えられる。そのため、実サービスに適用するためには、通信データ量が大容量の場合の認証方式についての検討が必要であり、今後の課題である。

4. 結言

IT マンション向けのサービス認証システムを構築するため、従来のユーザ認証に代わる認証方式として、本人性、利便性、低コスト性の全てに優れた居室認証方式を考案した。本方式を適用したサービス認証システムのプロトタイプシステムにて動作検証を行い、本システムの有効性を確認した。

参考文献

- [1] 例えば、日立 IT マンションシステム net@ITEM, <http://www.hitachi.co.jp/Prod/elv/jp/tosi/mansion/index.html>, (2004. 3).
- [2] Richard E. Smith, 認証技術～パスワードから公開鍵まで～, オーム社 (2003. 4) .