3F-01

宅内情報通信システムのためのセキュリティ方式の一検討

*大須賀 勝美、 *西島 正憲、 **村田 松寿、 **瀬川 卓見、 **坂東 達夫

*ＮＴＴエレクトロニクス株式会社 **松下電送システム株式会社

１．はじめに

ネットワーク技術の急速な進歩により、近い将来、家庭で利用される電化製品のほとんどが宅内でネットワークに接続されるとまで言われている。また、一般家庭にもインターネットへの常時接続が普及すると予想されている。そこで、宅内の情報通信システムに必要となるセキュリティ機能について検討を行い報告した。[1][2] 本稿では、その実現方式について検討を行い、その結果を提案する。

２．セキュリティ機能への要求

以下のようなセキュリティ機能の要件を考える。

(1)宅外からインターネット経由で宅内へアクセスする際のアクセス制御

(2-1)個人の秘密情報や重要情報などを保護するためのリソース管理

(2-2)ネットワークに接続された家電機器に対する適切な権限に基づく制御

(3)緊急時における安否確認などのための特定な第三者への一時的なアクセス許可と重要情報の退避

３．システム構成

全体構成として図１のようなシステムを考える。セキュリティ機能として宅内サーバにはアクセス管理およびリソース管理を行うサーバモジュールと管理用のコマンドが存在し、管理者が操作する。宅内端末と宅外端末にはセキュリティモジュールとコマンドが存在し、家族の構成メンバである利用者がアプリケーションによって処理を行う。セキュリティモジュールはファイルシステムへ組み込まれ、アプリケーションからリソースに対する操作を監視し、自動的にサーバとの間での通信を暗号化する。

サーバ側には管理用の情報を格納するため、利用者認証リスト(UAL)、利用者グループリスト(UGL)、アクセス制御リスト(ACL)、コマンド実行リスト(CEL)、の４つのリストが存在する。

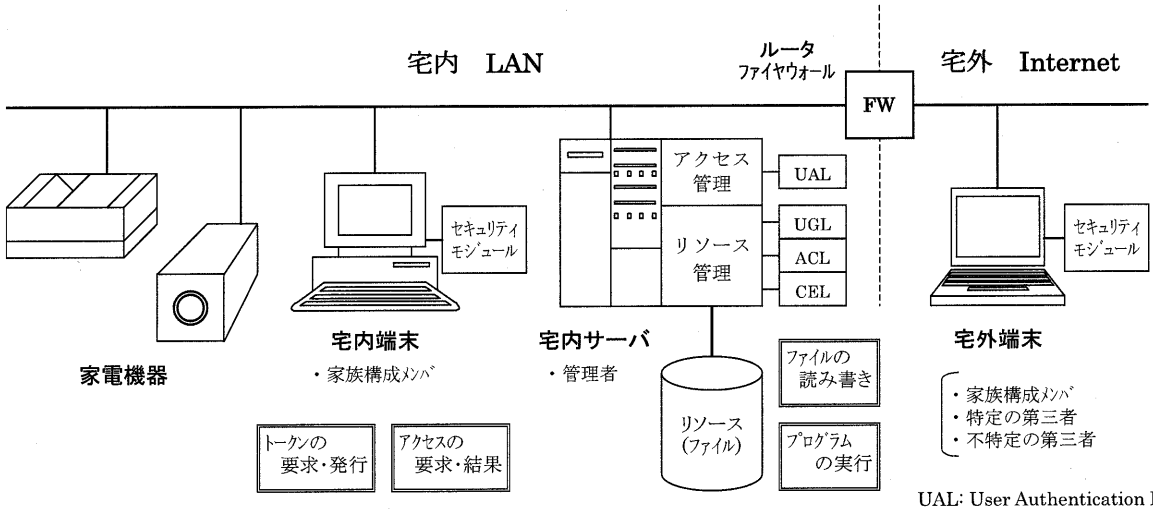

図１ システムの全体構成

A Study of Security System for an Intelligent Home Networking.

*Katsumi Osuga, *Masanori Nishijima, **Matsutoshi Murata, **Takumi Segawa, **Tatsuo Bando

*NTT Electronics Corporation, **Matsushita Graphic Communication Systems, Inc.

4．アクセス管理

宅内サーバのアクセス管理機能と端末側のセキュリティモジュールにより実現する。公開鍵暗号方式に基づいたICカードを利用した個人認証を考える。

UAL には利用者が利用する鍵ペアに対する証明書を登録する。UAL の情報に基づいて利用者の電子署名により個人認証を行い、トークンを発行する。発行されたトークンは有効期限を有し、端末側で保持され、次章で述べるリソース管理で利用される。

あらかじめ家族を UAL に登録することにより、ネットワーク経由のアクセスを制限する。また、公開鍵暗号方式を利用した個人認証により、パスワードによる認証方式より厳密な認証を可能とする。

5．リソース管理

宅内サーバのリソース管理機能と端末側のセキュリティモジュールにより実現する。データの内容やプロトコルに依存せずリソースを管理するために、ネットワークファイルシステムにセキュリティ機能を実装することを考える。

5.1 ファイルへのアクセス

UGL には複数の利用者が所属するグループを設定し、ACL には利用者あるいはグループに対して許可あるいは禁止するアクセス権限を設定する。トークンによりアクセスを要求している利用者を確認し、ACL に設定されている情報に基づいてファイルの読み書きなどのアクセス要求に対する制御を行い、結果を利用者に戻す。端末とサーバ間の通信は暗号化され、ネットワーク経由での操作を保護する。

利用者はあらかじめアクセス管理サーバからトークンを取得する必要があり、これにより個人認証に基づいたリソースへのアクセス権の制御を可能とする。トークンを取得できない不特定の第三者はリソースへのアクセスは一切禁止となるので、重要情報はすべてサーバ上で管理する。また、トークンを利用して正当性を検証することにより、アクセス管理サーバによる操作毎の認証は不要となる。

5.2 プログラムの実行

宅内の家電機器にはセキュリティモジュールを組み込まず、サーバ上の制御プログラムに対する実行権を制御してリソース管理することを考える。

CEL には利用者あるいはグループに対して実行可能なプログラム名を登録する。同様にトークンにより要求者を確認し、CEL の情報に基づいて許可されたプログラムをサーバ上で実行し、ネットワーク経由の通信で接続されている家電機器を制御する。

あらかじめ適切な操作を設定することにより、家電機器に対する正しいリモート操作を可能とする。

6．緊急時の動作

災害などの緊急時と平常時でサーバの状態を切り替え、UAL と UGL に緊急時限定として利用者やグループを登録することを考える。

あらかじめ信頼できる特定の第三者を緊急時限定として登録することにより、緊急時に宅内へアクセスして家族の安否確認や状況の監視が可能となる。また、家族であっても緊急時限定のグループにより通常とは異なるリソースへのアクセスを可能とする。データを自動的な暗号化機能を用意し、緊急時としてアクセスした重要情報を宅外へ退避させる。

7．まとめ

宅内情報通信システムにおけるセキュリティ方式を提案した。企業などの大規模システムでなくても、家庭においても容易に実現可能な方式を目指す。

現在、プロトタイプを作成して個々の機能について検証を行っているが、今後実際的な宅内情報通信システムへ組み込み、実証実験を行う。

謝辞

本稿は、通信・放送機構の委託研究テーマ「次世代の住宅情報化に関する技術の研究開発」の一環として行われたものである。

参考文献

[1] 多田、沢田、坂東、山下、小柳津：次世代の宅内情報通信システムのためのアクセス管理ゲートウェイの一方法，信学総合大会, D-9-12 (2000).

[2] 酒井、沢田、坂東、山下、山口：次世代の宅内情報通信システムのためのリソース操作の制御管理の一方法，信学総合大会, D-9-13 (2000).