暗号技術を用いた組込み型機器認証システムの開発

電子情報部　○林克明
金沢大学　　中川弘勝　木村春彦

１．目　的

近年，家電製品や産業機械などの機器間の接続に汎用の規格を用いることが可能となり，接続が容易になっている。その反面，接続ミスや悪意ある不正な接続による事故や破損，情報漏洩などの危険性が想定され，それを防止するには機器間の認証が必要となっている。認証とは，対象物が正当かどうかを確認する作業である。本研究では，広範な機器間での認証を実現するため，接続する機器に認証用ソフトウェアを直接搭載して実行するのではなく，マイクロコントローラ(以下，マイコン)などの記憶演算装置に認証システムを実装することで，独立したハードウェア部品とみなせる機器認証システム(以下，本システム)を開発する。

２．内　容

2.1 開発システムの特徴

日常的に多く行われている認証は，パソコンのログインやATMの利用など機械を操作する人間を確認することである。これに対して本研究で着眼した認証とは，機械や装置間での認証であり，暗号技術を用いた組込み型機器による認証である。

一般に，装置に実装されている認証システムは，暗号アルゴリズムをソフトウェアにより実現した装置の一部であることが多い。しかし，装置によってはプログラムを搭載することができないまたは，搭載していない場合がある。認証をソフトウェアだけで実現する場合は，認証用の部品スペースが不要なことや，プログラムを最適化できることにメリットがある反面，プログラムを搭載し，実行するためのプロセッサが必要となる。それに対して，本システムでは，プロセッサも含めた認証用の部品として提供するため，プロセッサなどを搭載していない広範な装置にでも組込みまたは接続することによって使用できるメリットがある。

2.2 開発システムにおける認証方法

図1に，機器1に対して機器2を接続するときの認証方法を模式的に示す。本試作においては，機器1とその認証システムをパソコンでエミュレートし，機器2に本システムをRS232Cで接続した。認証の流れは次のとおりである。1)機器1から乱文を機器2へ送信し，2)機器2においてその乱文を暗号化して機器1へ返信する。3)機器1において暗文を復号化し元の乱文と比較して一致すれば，機器2は正当な装置であると確認される。

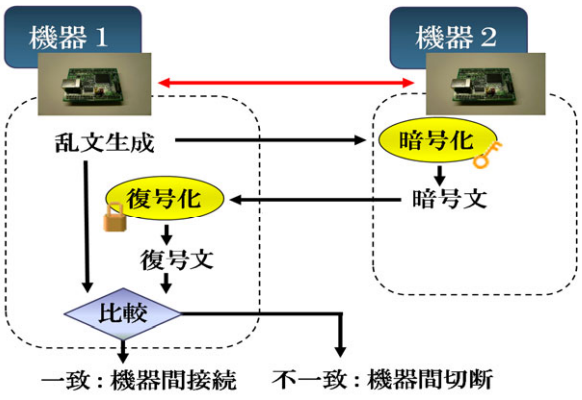

図1　機器間認証の信号の流れ

2.3 開発システムの構成

図2に，8ビットマイコンで実現した試作品を示す。本システムでは，マイコンに入出力機能を付加して完全な独立部品として

使用することも，認証を必要とする機器にマイコンを装着して使用することも可能である。このような汎用の認証システムを開発することにより，当初の目標どおりにコンピュータやプロセッサなどの演算機能を有しない機器であっても，接続時認証が可能となり，1)接続ミスの防止，2)不正接続の防止，さらに，3)機器使用時のアクセスレベル制御，などの利用効果が期待できる。

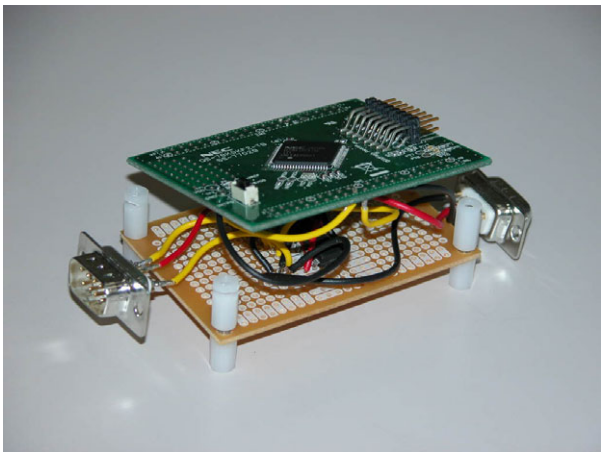

図2　8ビットマイコン版の試作システム

なお，本システムではNECエレクトロニクス社製の8ビットと32ビットのマイコンを用い，暗号アルゴリズムには，電子政府推奨暗号のひとつである64ビットブロック暗号を用いた。32ビットマイコンはメモリ容量も大きく，入出力インタフェースが充実していたため，プロトタイプとしてプログラムの動作確認やシステムの検証が容易であった。ただし，機器へ搭載する場合，設置スペースの問題がある。そこで，できるだけコンパクトに納めるには，8ビットマイコンが優れるため，8ビットでのシステム構築を実施した。最小の32ビットマイコンのサイズは10mm×10mm×1.4mm厚であるが，8ビットマイコンでは，汎用パッケージで7mm×6mm×1.2mm厚，BGAパッケージでは2.1mm×2.6mm×0.4mm厚と省スペース化が可能である。また，処理速度は暗号化処理時間で，32ビット：4m秒，8ビット：133m秒であり，通信時間も含めて，8ビットでも十分実用性があると思われる。

2.4 開発システムの用途

本システムの適用例として，次のものが考えられる。本体装置の用途によって，いくつかのオプション機器が接続可能な装置において，使用時の用途に適合したオプション機器が適正に接続されているかを認証し，チェックする用途が考えられる。さらに，本研究の目的とした機器間認証だけでなく，被接続機器(図2の機器1)から接続機器(図2の機器2)の制御を管理することもできるので，被接続機器の使用者に応じて，操作できる接続機器を制限することも可能である。なお，8ビットマイコンはサイズが小さいが，メモリ容量も少ないため，例えば公開鍵暗号を用いるなど，他のプログラムを搭載する余裕が無い。そのため，それらが必要となる場合には，設置スペースを犠牲にしてでも，32ビットマイコンを選択するなど，本システムを組込む装置側に必要となる機能，及び価格やサイズ等を勘案して，使用するマイコンを柔軟に選択することが可能である。

３．結　果

本システムの試作および実験結果から，マイコンによる独立したハードウェアによる機器間認証の動作を確認した。本システムにより，接続ミスや不正接続を防止するなどの用途を見込めるが，さらに実装の小型化など組込み型機器認証装置としての改良が必要である。今後は用途開発を進めることによって，新たな利用分野への機器間認証の応用を図っていく予定である。