機器間接続認証システムの開発

林克明[*]　中川弘勝[**]　前川雅俊[**]　木村春彦[**]

機器と機器を接続することは，規格の統一化や汎用化が進み，日常的に行われるようになってきた。その反面，誤接続や不正な接続の恐れが生じている。これを防止するには，認証技術の応用が考えられるが，プロセッサがないために認証用プログラムを実行できない機器がある。そこで，本研究では，機器同士の接続の正当性を保証するため，ハードウェア部品として扱える認証システムを開発した。具体的には本システムは，プロセッサを有しない機器間に接続して使用するものとする。認証用プログラムはパソコン上で開発し，動作検証後に，FPGAまたはマイクロコントローラで実行できるように移植した。さらに，FPGAを用いたシステムでの認証実験やマイクロコントローラのシステムでの処理時間の計測を行い，それらの有効性を確認した。

キーワード: 認証，FPGA，マイクロコントローラ

Development of an Authentication System for Improvement of Safe Device Connection

Katsuaki HAYASHI, Hirokatsu NAKAGAWA,Masatoshi MAEKAWA and Haruhiko KIMURA

Unification and universalization of product standards have made it possible to connect devices more easily. However, there is a greater possibility of false connection or unauthorized connection than before, since devices are connected more routinely. Authentication is effective in preventing these problems. In this study, we developed an authentication system in the form of a hardware component, which can be applied to the connection of devices without processors. The program for the system for PCs was developed first, and then modified for FPGAs and microcontrollers. Finally, we measured processing time and confirmed the effectiveness of our system by means of an authentication experiment.

Keywords : Authentication, FPGA, Microcontroller

１．緒　　言

機器と別の機器を接続する機会は，以前と比べてインタフェースの統一化や規格の汎用化が進むことで容易になり，多くなっている。これにより利便性は向上する反面，誤接続や不正な接続の増加が懸念され，接続時に機器間認証を行う必要性が生じている。通常の認証システムは，機器制御用コンピュータや機器内に組込まれたプロセッサのソフトウェア機能の一部として実現される。しかし，プロセッサなどを搭載していない装置が存在する。そこで，本稿では認証用プロセッサを別途用意することで認証プログラムを実行できるようにしたシステムを試作したので報告する。

２．内　　容

２．１　認証の概要

認証とは，対象が正しい人であるかまたは物であるかを確認する行為であり，利用者の正当性を認証する相手認証やデータの正当性を認証するディジタル署名などがある[1)]。本研究における認証は相手認証であるが，その対象は人間ではなく，機械・装置が対象であり，機器間認証であることが特徴である。認証システムを取り入れた機器間接続の概念図を図1に示す。これまでの接続では，コネクタ形状が合致する場合，直に接続が可能であった。しかし，機器間認証を取り入れることで，接続時に，被接続機器の正当性をチェックでき，接続ミスや不正接続を防止することが可能になる。

[*]電子情報部　[**]金沢大学

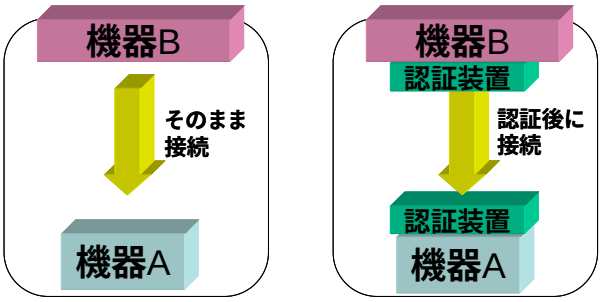

図1　機器間認証の概念図

表1　プロセッサの仕様

プロセッサ	クロック周波数	ROM	RAM
FPGA	51.6MHz	8MB	32MB
32ビットマイコン	20MHz	256kB	24kB
8ビットマイコン	20MHz	128kB	7kB

２．２　目的と研究の位置付け

本研究の目的は機器間接続認証システムの開発である。認証システムは，暗号技術を用いたソフトウェアおよび，それを実行するプロセッサにより構成される。プロセッサとして，FPGAまたは，マイクロコントローラ（以下、マイコン）などを想定している。本システムの特徴は，制御部などを有しない機器であっても認証の実行が可能なことである。そのため，機器外部のプロセッサで認証機能を実行させるシステムとして実現した。これにより，認証機能をハードウェア部品として個別に扱えるようになり，認証機能だけを独立したことでより汎用性を持たせることが可能となる。

機器に既に搭載または組込まれている一般の認証システムの特徴として以下が挙げられる。

1)メリット　ソフトウェアで構成されているので，他の部品スペースが不要であり，さらに認証プログラムを最適化できる。

2)デメリット　認証プログラムを他の装置へ流用しようと考えた場合，搭載プロセッサの相違により，加工し直す工数が必要となる。

一方，本システムのメリット及びデメリットは以下の通りである。

1)メリット　認証システム用のプロセッサは既に用意されているので，どのような機器へも接続が可能である。

2)デメリット　プロセッサやインタフェース変換ICなどのハードウェア部品の設置スペースが必要となる。

このような機器による機器の認証を行うシステムに類似する技術としては，

a)ドングル　パラレルやシリアルポート，USBに接続してソフトウェアのライセンス認証を行うためのハードウェアキーとして使用される

b)セキュリティチップ　パソコンのセキュリティ強度を高める専用LSIであり，主にハードディスクの持ち出しなどによる情報漏洩を防ぐために使用されるなどが挙げられる。また，機器接続の選択，制限だけに限れば，コネクタ形状の違いを利用して物理的に接続を制御する方法もあるが，インタフェースの汎用性は欠如する。極言すると，ドングルはソフトウェアライセンスの管理のみを行い，セキュリティチップは暗号鍵の保護だけを行う。すなわち，これらは用途を限定しているのに対して，本システムは汎用的なインタフェースを対象として，幅広い用途を実現するための開発といえる。

２．３　使用プロセッサ

今回，認証プログラムを実行するプロセッサとして，アットマークテクノ社製のFPGA(Filed Programmable Gate Array)SZ130-SILおよび，NECエレクトロニクス社製のマイコンV850ES/JG2（32ビット）と78K0/KF2（8ビット）を用いた。最初にFPGAを用いたシステムを試作して認証の実験を行い，次にマイコンを用いたシステムを試作した。今回の実験で使用したFPGAとマイコンの仕様を表1に示す。

２．４　認証システムとプロセス

システムのプログラムはC言語で記述し，暗号アルゴリズムには，電子政府推奨暗号[2)]の一つである共通鍵暗号の64ビットブロック暗号[3)]を使用した。機器間認証のプロセスを図2に示す。機器Aと機器Bが通信し，正当な接続機器同士であるかを認証する。そのプロセスは以下である。

1)機器Aで乱文Mを作成し，機器B側へ送信する。

2)機器Bでは乱文Mを暗号化してXとし機器Aへ送信する。

3)機器Aでは，Xを復号化してM’とし，最初に送出したMと比較を行う。

4)MとM’が同一ならば，機器Bは正しい接続機器と判断する。

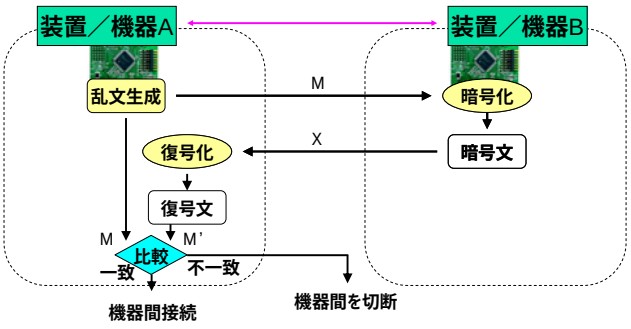

図2　機器間認証のプロセス

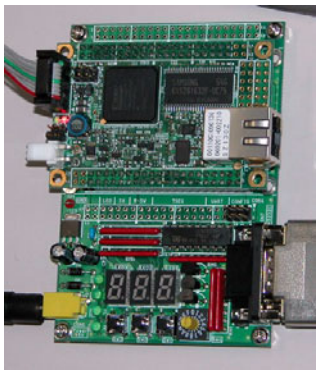

図3　FPGAによるシステムの外観図

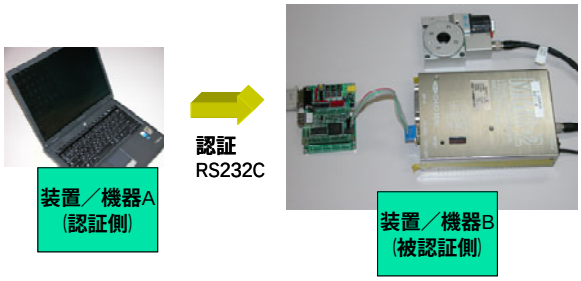

図4　FPGAでの認証実験

という流れで行われる。ここで，図2において機器A側と機器B側とでは異なる処理をしているが，搭載しているプログラムは同一である。すなわち，作成した認証システムはパラメータの設定変更で，機器A，Bどちら側の処理も可能である。

2．5　FPGAでのシステム構築と評価

図3にFPGAで作成したシステムを示す。FPGAをプロセッサとして用いることのメリットは，メモリ容量が大きいためにシステム構築が容易なことと，インタフェースが充実していること，が挙げられる。認証の実験では，図3のシステムを図2における機器Bの認証装置として用いた。また，機器A及びその接続認証装置にはFPGAではなく，それをシミュレートするものとしてパソコンを使用した。これは，実験中の信号や認証の正否の確認を容易に行うためである。実験では，図4のように機器Aからの被接続機器Bの認証を行った。なお，機器BがインタフェースにRS232Cを有していたため接続にはRS232Cを用いた。実際の機器Aにおける認証時のメッセージを図5に示す。同図は，正しい機器が接続された場合を示している。実験では，正しいと認証された場合，機器Aから機器Bを制御することを可能とし，正しくないと認証された場合，機器Aと機器B間の通信を電気的に遮断し，機器Bの制御を行えないようなプログラムも機器Aに搭載した。

```
*OPEN AND INITING COM PORT...
*COM PORT BUFFER CLEAR
送信した乱文
 cf67de58b4417d15ec4f
暗号化された乱文
 9387b697c8dfa9449e2d1c0240e80df4
暗号化された乱文を復号化
 cf67de58b4417d15ec4f
認証OK!
```

図5　機器Aにおける認証画面

2．6　マイコンでのシステム構築と評価

マイコンは，32ビットと8ビットのものを使用した。ただし，マイコン単体ではなく，それぞれ必要とされるインタフェース関連の回路が搭載されている市販のターゲットボードを利用した。そのため，認証の動作に不要な回路などもある。図6に，8ビットマイコンを利用した認証装置を示す。8ビットマイコンはメモリが32ビットよりも少ないため，暗号化ルーチンの一部を別に演算し，その数値結果をマイコンに搭載することで，認証システムの実行を可能にした。また本来，本システムは装置内に組込むことを想定しているが，試作品は実験用のため装置の改変を不要とするために外部接続用コネクタを使用して通信を行った。また，マイコンのシステムでは動作速度の検証を行った。これは，マイコン内部での暗号処理にかかる時間，及び，通信時間も含めたすべての認証処理にかかる時間を計測した。その結果を表2に示す。おおよそ500ms以下

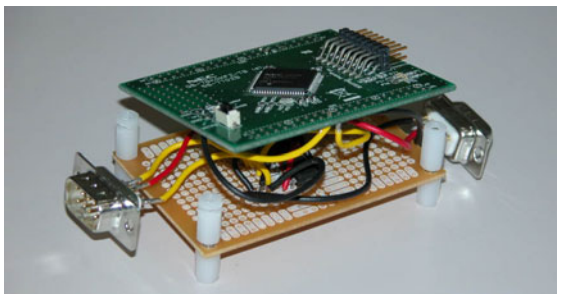

図6　8ビットマイコンの試作装置

表 2　マイコンの処理時間比較

	暗号処理時間	認証処理時間
8 ビット	133ms	250ms
32 ビット	4ms	203ms

の待ち時間ならば一般的な用途では問題ないと考えられるので，この結果からは処理速度に関しては実用的と思われる。

２．７　開発システムの用途

本システムの適用例として，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た上で，動作を可能にする応用が考えられる。さらに，被接続機器（図２の機器A）から接続機器（図２の機器B）を制御するだけでなく，使用者に応じて操作できる被接続機器の捜査範囲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，設置スペースやコストを検討して32ビットマイコンを選択する必要がある。本システムは，組込む装置側に必要となる機能，及び価格やサイズなどを勘案して，使用するマイコンを柔軟に選択することが可能とする。ただし，表1に示したように，FPGAは本システムを実行するには，十分なメモリ容量と機能を有し，認証機能単独で使用するのは過剰性能といえる。そこで，FPGAで本システムを使用する場合は，認証専用機能としてではなく，すでにFPGAで何らかのシステムが存在する状態で，付加機能として本認証機能を搭載する，という使用方法が望ましいと考えられる。

３．結　　言

以上，機器間認証システムの試作とその評価実験について述べた。本認証システムは，独立したハードウェア部品として扱うことができ，これまで認証を取り入れることができなかった機器や装置でも認証を可能にすることができる。また，認証システムに使用するプロセッサとして，FPGAとマイコンを使用できるようにした。これにより，被組込み側機器の設置スペースや用途に応じたプロセッサの選択を可能とした。今後は，実装組込みに向けた小型化などを実施し，用途開発を図っていきたい。

謝　　辞

本研究を遂行するに当たり，終始適切なご助言を頂いたNECソフトウェア北陸の広田昭彦氏，久保博靖氏に謝意を表します。

参考文献

1) 岡本龍明．“暗号と情報セキュリティ”．日経BP社，1998，p.52.
2) 電子政府推奨暗号リスト．http://www.cryptrec.go.jp/list.html (参照 2008-07-30)
3) 岡本龍明，山本博資．“現代暗号”．産業図書，1997，p.79.