特集

セキュリティ機能を搭載したネットワーク家電向けシステムLSI

System-on-Chip with Security Module for Network Home Electronic Appliances

あらまし

家電機器をインターネットなどのネットワークに接続すると，情報やサービスが手軽に利用できるようになる一方，情報流出や外部からの攻撃などの危険も増える。このような背景から，ネットワークに接続される家電機器にもセキュリティ機能の搭載が求められている。

本稿では，家電機器に最適なCPUや各種周辺機能に加え，このようなネットワークとの接続機能，セキュリティ機能を内蔵した，ネットワーク家電製品向けの1チップシステムLSIについて述べる。本LSIは，デジタル家電機器システムのメインプロセッサとして，機器の制御やデータ処理だけでなくネットワーク機能やセキュリティ機能を1チップで処理できる。また，本LSIを既存のシステムにスレーブプロセッサとして接続して，簡単にネットワーク機能やセキュリティ機能を実現することも可能である。

Abstract

Linking home electronic appliances to the Internet and other networks enables easy access to a variety of information and services. However, this also increases a user's exposure to information leaks, external intrusions, and other risks. Therefore, home electronic appliances linked to the network require proper security functions. This paper describes a single-chip System-on-Chip specifically designed to protect home electronic appliances that are connected to the network. When used as the main processor of a home system, this LSI can provide networking and security functions, control devices, and process the relevant data of those devices. Moreover, this LSI can be connected as a slave processor to an existing system for easy realization of networking and security functions. This paper also describes the optimum CPU for home electronic appliances and the various peripheral functions these appliances should have.

藤山博之（ふじやま　ひろゆき）

システムマイクロ事業部第一設計部
所属
現在，ネットワーク，セキュリティ関連のLSI，および放送コンテンツ権利保護LSIの研究開発に従事。

セキュリティ機能を搭載したネットワーク家電向けシステムLSI

ま え が き

昨今，インターネットは，その利用範囲が一般家庭まで広がっており，また，接続される機器も，PCだけではなく，従来ネットワークに無関係であった一般の家電製品にまで広がりを見せている。

家電製品がインターネットなどのネットワークに接続されると，外部の情報やサービスを手軽に利用できるようになる一方，ネットワークを介しての情報流出や外部からの攻撃などの危険も増えてくる。このような背景からネットワークに接続された家電製品においてもセキュリティ機能が求められてきている。

本稿で紹介するネットワーク家電向けシステムLSIは，上記に述べた家電製品に最適なCPUや各種周辺機能とともに，ネットワークとの接続機能，セキュリティ機能を内蔵した1チップシステムLSIである。本LSIは，機器の制御やデータ処理とともに，ネットワーク機能やセキュリティ機能を1チップで処理することが可能である。また，既存のシステムに本LSIをスレーブプロセッサとして接続し，簡単にネットワーク機能やセキュリティ機能を実現することが可能となる。

ネットワーク家電向けシステムLSIの開発

インターネットの普及はPCを中心に進んでいるが，プロトコルレベルでも従来のIPv4（Internet Protocol Version 4）に加え，セキュリティの標準サポートや接続の容易性などの特徴を持つIPv6への対応も進んでいる。また非PC分野においても，ネットワークとは無縁であった家電製品などもネットワークに接続され，より便利な使われ方が期待されている。こうした分野ではローコストで手軽にネットワークに接続できる手段の開発が普及のかぎとなる。その一つの解としてセキュリティ機能を搭載したネットワーク家電向けのシステムLSIの開発を行うことにした。

家電製品では，ネットワークに接続されることで便利になる一方，ネットワークで流れる情報のプライバシー保護など，セキュリティ機能がより重要となってくるが，アプリケーションから意識することなく簡単で確実に利用できることが望ましい。こうしたセキュリティ機能はインターネットプロトコルでは，IPsec（IPsecurity）として規定されており，IPv6では標準で搭載が考えられている。しかしIPsecはソフトウェア処理の負荷が重く，一般的な家電製品で利用される組込み向けのマイコンで実現するのは性能の面で難しく，また性能を上げるとコストや消費電力などが増加するという問題があった。

そこで，性能，コスト，消費電力の問題を解決し，セキュリティ機能を搭載したネットワーク家電向けシステムLSIを開発した。本LSIでは，暗号処理でソフトウェアの負荷の重い部分をハードウェア化することで処理効率を上げ，CPUの負荷を減らすことでセキュリティ機能の処理に対応し家電製品に最適なシステムLSIを実現した。

また，本LSIは，既存の家電製品などで一般に使われるマイコンをベースにネットワーク接続のインタフェース機能と，ネットワークに必要なプログラム群をファームウェアとして実装することによりローコストで手軽にネットワーク接続を実現した。

以下，ネットワーク家電向けシステムLSIとして，高機能汎用タイプMB91401，ROM/RAM内蔵タイプMB91402/MB91403を紹介する。

高機能汎用タイプMB91401

セキュリティ機能搭載ネットワーク家電向けシステムLSIの最初の製品であるMB91401は，FR（富士通オリジナル32ビットRISCマイコン）をCPUコアとして使用し，ネットワーク機能，セキュリティ機能を搭載している。CPUへの負荷をかけずにセキュリティ機能やIPv6に対応できるような工夫を加えるとともに，いろいろな家電製品で簡単に利用できるように豊富なインタフェース機能を搭載している。MB91401のブロック図を**図**-1に示す。

以下にネットワーク機能，セキュリティ機能について特徴的な機能を示す。

(1) ネットワーク機能

ネットワークへの接続機能として，IEEE802.3に準拠した10/100 M MAC（Media Access Control）を搭載している。標準的なMII（Media Independent Interface）を持ち，一般的なPHY（物理層）デバイスとの接続が簡単に行える。また，内部のレジスタは従来のLANコントローラにできるだけ合わせることでドライバなどのミドルウェアの流用や開発を容易にしている。

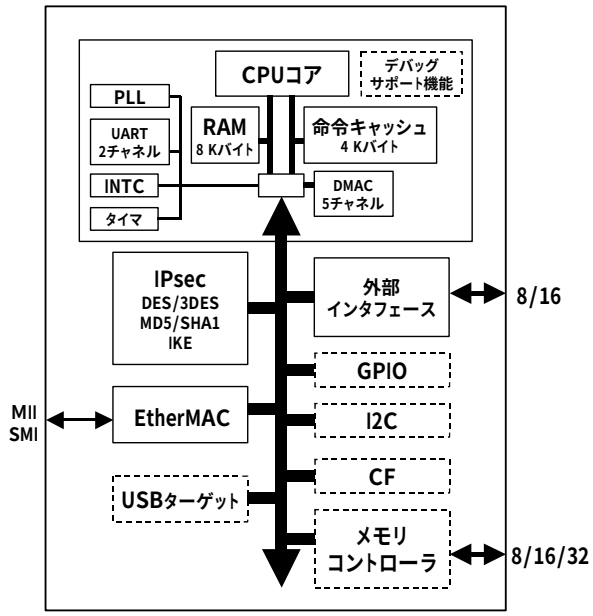

図-1　MB91401ブロック図
Fig.1-MB91401 block diagram.

特徴としてはネットワークのL2/L3/L4各層でのパケットフィルタリング機能をハードウェアでサポートしている。LSIの入り口で必要なパケットのみを通過させることにより，不要なパケットの処理でCPUに余分な負荷をかけることを防止することができる。ソフトウェアが介在せずに不要なパケットを排除できるためセキュリティの面でも有効である。

またフィルタリングの設定は，IPv4，IPv6の指定を行うことで，両者のプロトコルのヘッダ部の違いに対応が可能である。MACでは，IPv6での最大パケットである1.5 Kバイトの送信バッファを内蔵している。また，受信側は，瞬間的に100 Mbpsでのパケットが来ても取りこぼしなく受信できるように9 Kバイトの大容量受信バッファを内蔵している。

(2)　ハードウェアによるセキュリティ機能搭載

インターネットでは，プロトコルのセキュリティ機能としてIPsecが標準で使用される。IPsecでは，盗み読みを防止する暗号機能，通信相手への「成り済まし」を防止する認証機能，安全に暗号鍵を交換する機能などが規定されている。本LSIでは，これらIPsecの機能をハードウェアでサポートしている。秘密鍵暗号方式としてDES(注1) TripleDES（3DES）(注2)，ハッシュ関数として標準的なMD5(注3) SHA-1(注4)に対応している。また，IKE（鍵交換）や公開鍵暗号で利用可能な専用演算器を内蔵している。

主なサポート機能を以下に示す。

・DES-ECB/DES-CBC/3DES-ECB/3DES-CBモード対応
・MD5/SHA-1/HMAC-MD5/HMAC-SHA-1モード対応
・鍵交換　DHグループ：1（MODP 768ビット）
　　2（1,024ビット）

これらのセキュリティ機能のデータ転送を専門に受け持つIPsecマネージャを搭載することで，CPUのみの処理で転送する場合に比較し約5倍の高速化を実現しており，同時にCPUの負荷を1/5以下に低減している。セキュリティ機能のハードウェア化と，IPsecマネージャの搭載により，暗号処理を本LSIのCPUを利用しソフトウェアのみで処理した場合と比較して200倍程度，また，鍵交換アルゴリズムでは約100倍程度の高速化を実現している。

セキュリティ機能は，ネットワークのIPsec以外でも利用可能であり，外部メモリ上のデータのセキュリティのために暗号化やハッシュ関数を利用することもできる。提供ドライバにより，アプリケーションから関数として簡単に利用することができる。

(3)　外部インタフェース

本LSIにはCPUコアに割込みコントローラ（INTC），タイマ（Timer），DMAコントローラ（DMAC），シリアルインタフェース（UART）など標準的な周辺回路を内蔵している。このため，単独で家電製品などの制御用コントローラとしても使用でき，さらには，家電製品などシステムとして構成された機器に付加し，セキュリティに対応したネットワーク接続機能を提供することも可能である。

システムのメモリバスにIOとして簡単に接続可

(注1)　Data Encryption Standardの略。広く使用されている秘密鍵暗号方式。
(注2)　DESを3重に繰り返し暗号強度を上げた秘密鍵暗号方式。
(注3)　Message Digest 5の略。広く使用されるハッシュ関数の一つ。
(注4)　Secure Hash Algorithm-1の略。広く使用されるハッシュ関数の一つ。

能な外部インタフェースを内蔵しており，大容量送受信FIFOと通信用のレジスタを装備しているため，データの入出力を行う形で，簡単にネットワーク機能を既存のシステムに付加できる。本LSIを既存のシステムにスレーブプロセッサとして接続することで簡単に既存のシステムにセキュリティ機能を実現できる。

(4) 周辺インタフェース

本LSIにはネットワークの機能以外にも，USBターゲット機能，カードインタフェース，I2Cインタフェースを搭載しており，機器の目的に合わせて接続方式が選べる。USBを通じてファイルの暗号エンジンとして使用したり，カードインタフェースに無線LANカードを接続したりするなどの応用も可能である。

ROM/RAM内蔵タイプMB91402/MB91403

MB91401は豊富なインタフェースにより，いろいろな機器でネットワーク機能を利用できることを目指したが，さらに比較的コストの安い家電製品やFA（Factory Automation）などの組込み用途でもネットワーク接続機能を簡単に利用できることを目的とし，大容量のROMとRAMを内蔵したMB91403を開発した。MB91402/MB91403のブロック図を**図**-2に示す。

本LSIとMB91401の大きな違いは256 KバイトのROMと64 KバイトのRAMの大容量メモリを内蔵したことである。さらにUSB，カードインタフェースを省略して端子数をMB91401の240本から144本に削減し実装の容易なQFP（Quad Flat Package）パッケージへの変更や，電源を3.3 V単一電源とするなどシステムの小型化，コストダウンに最適なLSIを目指した。一方では，次世代の標準暗号方式として広がりつつあるAES(注5)を新規に追加，3DESの効率化などセキュリティ機能も向上している。メモリの内蔵はコストダウンに効果があるほか，LSI内部でデータ処理を行えるためセキュリティ対策としても有効である。モード設定により外部メモリにも対応可能であるため，さらに大容量のメモリが必要な場合にも対応可能である。また，製品開発時や初期製品では書換え可能なフラッシュメモリを外部メモリとして使用するといった利用も可能である。

IPv4での利用やゲートウェイ内部などセキュリティの不要な用途向けにMB91403からセキュリティ機能を省略したMB91402も同時に開発した。MB91403とは端子互換があるため，本LSIを使用したシステムでは，セキュリティが必要になった時点でMB91403に載せ換えも可能である。各LSIの機能比較を**表**-1に示す。

ソフトウェア，開発環境

ここでは，本LSIの性能，機能を最大限活用するソフトウェアと，本LSIを使用したデジタル家電製品の開発をサポートする開発環境について述べる。

(1) ソフトウェア

ネットワーク機能実現のための，IPv4/IPv6対応TCP/IPプロトコルスタックもLSIと同時に準備した（**図**-3）。セキュリティ機能のDES，AES暗号やハッシュ関数もアプリケーションから関数として簡単に利用できるようにドライバとして開発した。さらにRSAなど各種暗号アプリケーションの対応も準備中である。

(2) 開発環境

本LSIは，富士通製の統合開発環境SOFTUNE V6が利用可能である。また，リアルタイムデバッグが可能なFRファミリ用エミュレータMB2198-01

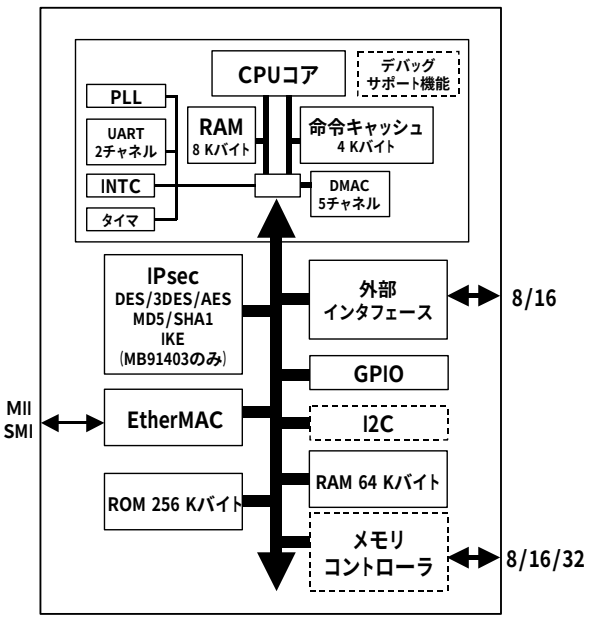

図-2 MB91402/MB91403ブロック図
Fig.2-MB91402/MB91403 block diagram.

(注5) Advance Encryption Standardの略。米国標準局で，DESの後継として新規に制定した秘密鍵暗号方式。

表-1　機能比較表

項目			MB91401	MB91402/MB91403
CPU	FRコア		FR60シリーズコア	FR60シリーズコア
	命令キャッシュ		4 Kバイト	4 Kバイト
	RAM		8 Kバイト	8 Kバイト
	UART		2チャネル	2チャネル
	外部割込み		3チャネル＋NMI	2チャネル
	DMA（外部端子なし）		5チャネル	5チャネル
	リロードタイマ		3チャネル	3チャネル
	デバッグサポート機能		搭載	搭載
周辺モジュール				
	MACコントローラ		○	○
		受信FIFOサイズ	9 Kバイト	3 Kバイト
	外部インタフェース		○	○
		受信FIFOサイズ	3 Kバイト	1.5 Kバイト
	メモリIF		○	○
		アドレスビット	24ビット	23ビット
		データビット	8/16/32ビット	8/16ビット
		チップセレクト	3	2
		応デバイス	ROM/RAM	ROM/RAM/SDRAM
	I2C IF		○	○
		対応モード	標準（100 kbps）	標準/高速（400 kbps）
	GPIO		8ピン（最大）	26ピン（最大）
		入力変化割り込みポート	－	○（4ピン）
	暗号/認証マクロ		○	○
		DES/3DES	○	○（MB91403のみ）
		AES	－	○（MB91403のみ）
		HMAC-MD5/SHA1	○	○（MB91403のみ）
		REDC	○	○（MB91403のみ）
		IPsec Manager	○	－
	大容量ROM		－	○（256 Kバイト）
	大容量RAM		－	○（64 Kバイト）
	シリアルダウンローダ機能		－	○
	USB IF		○（FSモード）	－
	カードIF		○（CFカード）	－
パッケージ			FBGA-240	LQFP-144
動作周波数			66 MHz（MAX）	33 MHz（MAX）
電源			2電源（1.8/3.3 V）	1電源（3.3 V）

シリーズに対応している。

MB91401の評価用ボードを**図**-4に示す。本ボードは，MB91401の豊富な周辺インタフェースを利用できるようにUSBやカードコレクタなどを実装している。また，メモリバスに任意の回路を書込み可能なFPGAを搭載しているため，利用時に簡単に回路が追加できる。

MB91402/MB91403の評価用ボードを**図**-5に示す。本ボードは，MB91402/MB91403の特徴を生かすため評価に必要な最小限の機能に絞って小型化しており，実際に機器に組み込んで評価することも可能である。

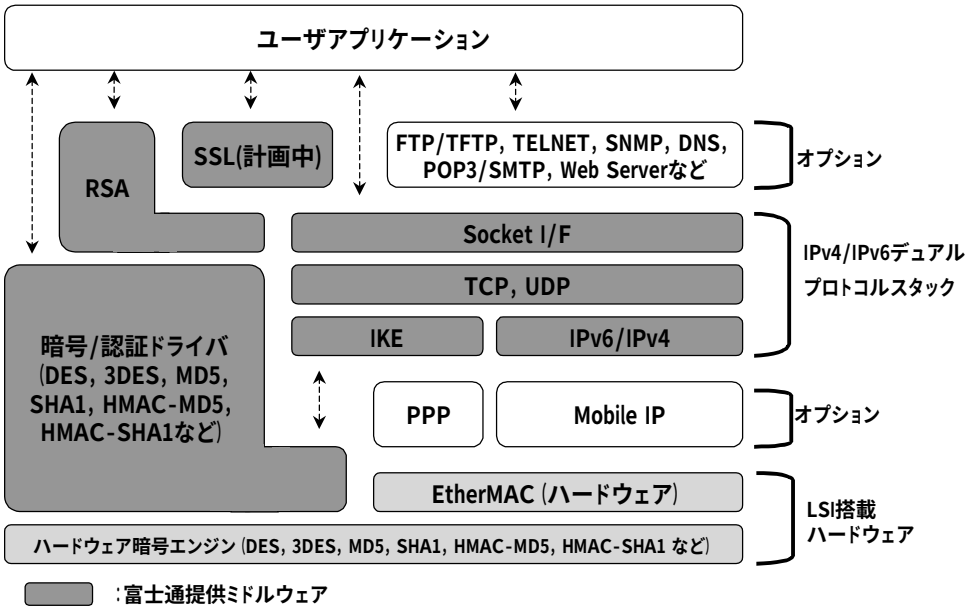

図-3　ネットワーク機能，セキュリティ機能を実現するソフトウェア構成
Fig.3-Software for network and security.

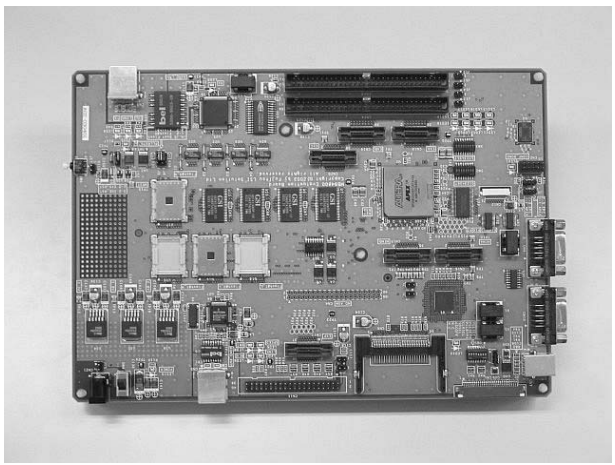

図-4　MB91401評価用ボード
Fig.4-Board for evaluation of MB91401.

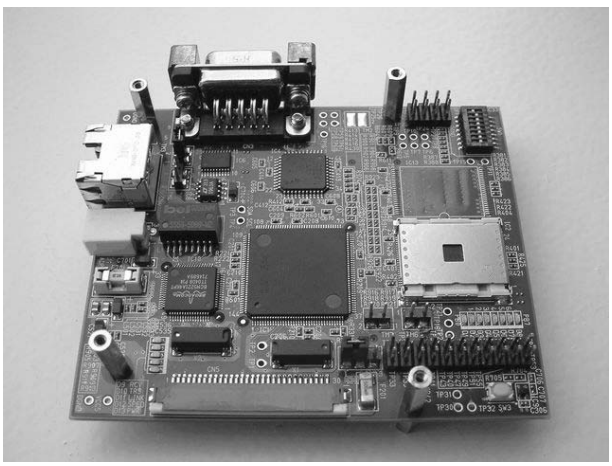

図-5　MB91402/MB91403評価用ボード
Fig.5-Board for evaluation of MB91402/MB91403.

む　す　び

本稿では，セキュリティ機能を搭載したネットワーク家電向けシステムLSI MB91401，MB91402，MB91403について説明した。本LSIにより，従来，性能や安全性の面からネットワークへの接続が難しかった機器を簡単で安全にネットワークに接続することが可能になる。

今後は，ますます広がりを見せるネットワーク社会の情報家電の多様な用途の広がりに合わせ，さらに性能や機能などを最適化したLSIを検討していくとともに，簡単で安全なネットワーク利用技術も同時に提供できるようにしていきたい。