

# セキュリティ機能を搭載した ネットワーク家電向け1チップシステムLSI MB91401

ネットワーク家電向けに、家電の制御に最適なCPUコアや周辺マクロ、ネットワーク接続機能、セキュリティ機能を1チップに内蔵したシステムLSIです。

## 概要

デジタル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ます。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ます。

本製品は、デジタル家電機器に最適なCPUや各種周辺機能に加え、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です。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チップで処理できます。また、外部CPUとの高速データ通信を可能とする接続専用のパスを搭載しているため、既存のシステムに本製品を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できます。

## 特長

### ●ネットワーク機能

本製品は、IEEE802.3に準拠した10/100M MACに対応します。また通信用のパッファメモリとして、送信パッファに1.5Kバイト、受信パッファに9Kバイトを内蔵しています。MIIインタフェースによりPHYデバイスとの接続が行えます。さらに、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おり、不要な通信処理によるCPU負荷を排除します。

### ●ハードウェアによるセキュリティ機能搭載

暗号マクロとハッシュ関数マクロを内蔵しており、通信中にデータの暗号化/復号化を行う秘密鍵暗号方式のDES/TripleDESと、通信データの改ざんチェックを行う認証方式のHMAC-SHA1/HMAC-MD5をハードウェアでサポートします。また、これらの暗号やハッシュ関数の実行時に、データの設定/転送を連続して実行

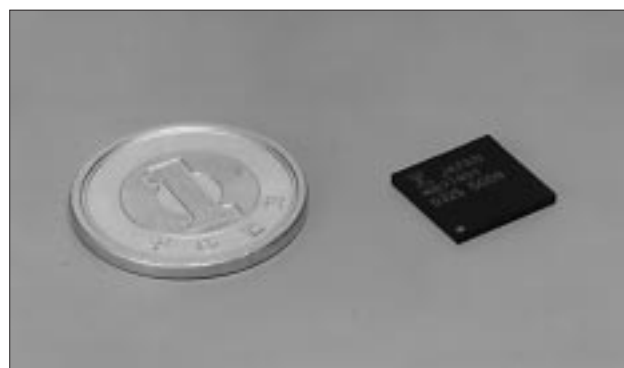


写真1 外観

できるハードウェア機構( IPsecマネージャ )を内蔵しています。IPsecマネージャがデータの設定/転送を効率的に行うことで、CPUがソフトウェアで設定/転送を行う場合に発生するオーバーヘッドを回避できます。これにより、暗号・認証ハードマクロとソフトウェアを組み合わせた処理と比べて5倍、ソフトウェアのみの場合と比べて150~200倍の性能向上を実現します。また、同時に暗号・認証処理に携わるCPUの処理負荷率を1/5以下に低減できます。

本製品はさらに、ソフトウェアでの処理負荷が非常に重い公開鍵暗号方式などのアルゴリズムで頻繁に使用する処理を、ハードウェアで実行するアクセラレータ機能を内蔵しています。これにより、ソフトウェアでの処理時間と比べて約100倍の高速化を実現します。

これらの機能により本製品は、インターネットのネットワーク層で使用するセキュリティ機能であるIPsecに対応できます。また、暗号や認証機能を上位のアプリケーションから関数として簡単に利用でき、RSAやSSLなどの暗号アプリケーションの高速化にも利用できます。

### [ハードウェア対応機能]

- ・ DES-ECB/DES-CBC/3DES-ECB/3DES-CBCモード対応
- ・ MD5/SHA-1/HMAC-MD5/HMAC-SHA-1モード対応
- ・ DHグループ: 1( MODP 768ビット )/2( 1024ビット )対応

### ●通信機能付外部インタフェース

本製品はCPUコアを内蔵しているため、単体で機器の制御やデータ処理を実行できますが、スレーブプロセッサとしても使用できます。システムのメインプロセッサに簡単に接続できるよう専用外部インタフェースを持っており、システムにネットワーク機能やセキュリティ機能を簡単に付加できます。汎用的なSRAMインタフェースであるI/Oとして、メインプロセッサのメモリバス上に本製品を接続することができます。本製品の外部インタフェースは、メインプロセッサとの間で大量のデータ送受信を実現するため、送信1.5Kバイト、受信3Kバイトの大容量送受信FIFOと、通信用のレジスタを装備しています。

### ●高性能32ビットFRコア採用

本製品にはCPUコアとして、当社オリジナルアーキテクチャの高性能マイコンであるFRを内蔵しています。CPUコアは、命令キャッシュを4Kバイトとデータ用RAMを8Kバイト内蔵しており、システムの高付加価値化・高性能化に十分追従できる性能を実現します。また、組み込み用途に最適な16ビット長命令コードにより、コンパクトなプログラムサイズを実現します。

### ●豊富な周辺機能

本製品では、いろいろな機器との接続や制御を簡単に実現するため、DMAコントローラ、タイマ、割り込みコントローラなどの周辺機能や、USB2.0 Full Speedに対応したUSBターゲットインタフェース、I<sup>2</sup>Cインタフェース、コンパクトフラッシュインタフェースなどの豊富なインタフェース機能を内蔵しています。

図1にネットワークチップブロック図を示します。

### ●ミドルウェアソリューション

本製品は、ネットワーク機能実現のためのプロトコルスタックとして、(株)エルミックシステムのKASAGOと富士通デバイス株のeTCP/IPが利用できます。また、RSAなど各種暗号アプリケーションの対応を準備中です。

図1 ネットワークチップブロック図

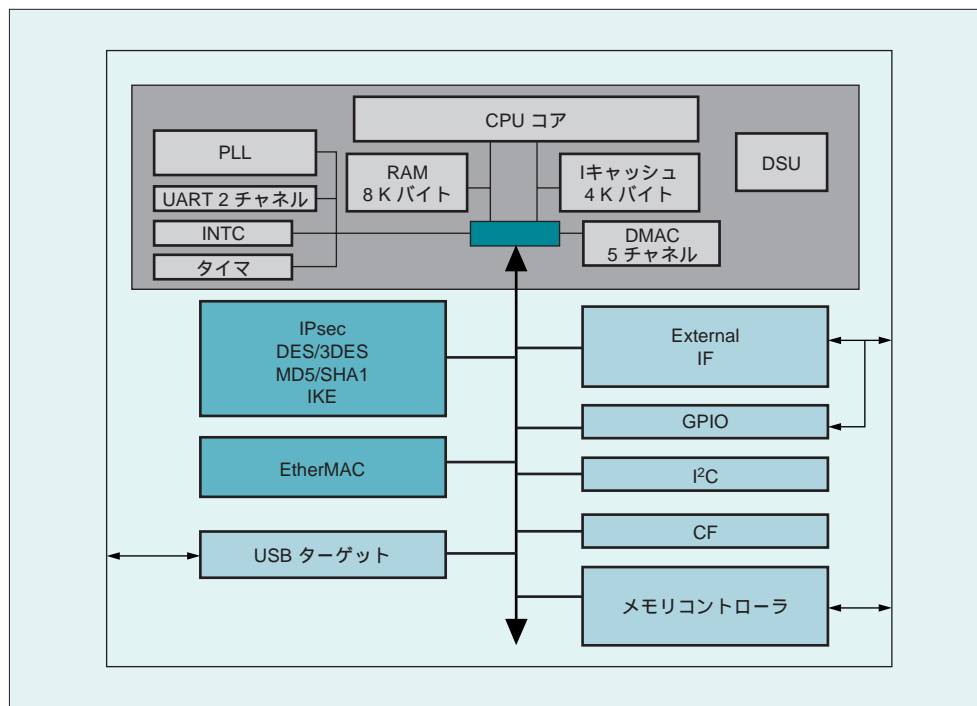


表1 開発ツール構成

ハードウェア	メインユニット MB2198-01
ソフトウェア	SOFTUNE V6 ワークベンチ
	SOFTUNE V6 Cコンパイラ
	SOFTUNE V6 アセンブラ
	SOFTUNE V6 Cアナライザ
	SOFTUNE V6 Cチェッカ
	SOFTUNE V6 REALOS/FR

表2 評価ボード

型 格	概 要
MB91941EB	開発ツール(MB2198)に対応 ネットワーク接続可能 ユーザ回路をFPGAに追加可能

## 開発環境

本製品は、当社統合開発環境SOFTUNE<sup>®</sup> V6でサポートしています。SOFTUNEは、プログラム開発者のさまざまな要求に応えるべく開発され、使いやすさを追求したソフトウェアです。ハードウェアは、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シリーズに対応しています。

表1に開発ツール構成を、表2に評価ボードを示します。

## 応用分野

本製品は、オーディオ、デジタルTVなどのデジタル家電や産業機器などの用途向けに、システム制御とデータ処理を1チップで行うための最適なパフォーマンスを実現しています。また、現在のシステム構成をそのままに、ネットワーク専用チップとして接続することで、ネットワーク機能や暗号機能が簡単に付加できるなど、システムの高性能化・高付加価値化・コンパクト化を強力に支援します。

\* SOFTUNEは富士通株式会社の登録商標です。

\* 文中に記載されている製品名などは、各社の商標または登録商標です。