

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 MB91402/MB91403

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バ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

表1に本製品の機能を示します。

●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。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。また通信用のバッファメモリとして、送信バッファに1.5Kバイト、受信バッファに3Kバイトを内蔵し、CPUの負荷を軽減した通信が行えます。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(MB91403のみ)

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/3DES/AESと、通信データの改ざんチェックを行う認証方式のHMAC-

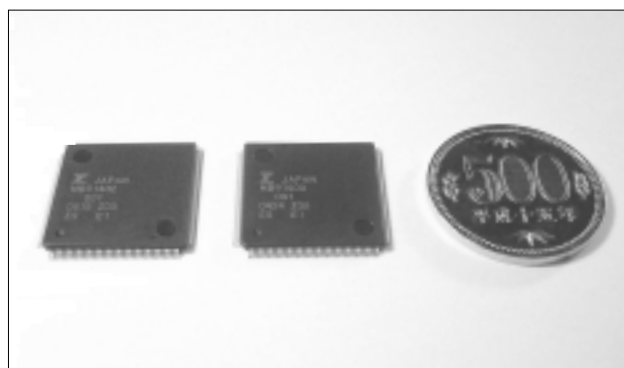


写真1 外観

SHA1/HMAC-MD5をハードウェアでサポートします。これにより、ソフトウェアのみでサポートする場合と比べて2桁の性能向上を実現します。

本製品はさらに、ソフトウェアへの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数10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され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る、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。

*セキュリティ機能を搭載しているのはMB91403のみです。

[ハードウェア対応機能]

- ・DES/3DES/AES(Key length = 128/192/256ビット)のECB/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

データ処理ができますが、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1.5K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、I²Cインタフェース、汎用I/Oポート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。

表1 MB91401/MB91402/MB91403の機能

		MB91401	MB91402	MB91403
CPU	FRコア	FR60シリーズコア	FR60シリーズコア	FR60シリーズコア
	I\$	4Kバイト	4Kバイト	4Kバイト
	D-RAM	8Kバイト	8Kバイト	8Kバイト
	UART	2チャンネル	2チャンネル	2チャンネル
	外部割り込み	3チャンネル+NMI	2チャンネル	2チャンネル
	DMA(外部端子なし)	5チャンネル	5チャンネル	5チャンネル
	リロードタイマ	3チャンネル	3チャンネル	3チャンネル
	DSU	3	3	3
周辺モジュール	MACコントローラ			
	受信FIFOサイズ	9Kバイト	3Kバイト	3Kバイト
	外部インタフェース			
	受信FIFOサイズ	3Kバイト	1.5Kバイト	1.5Kバイト
	メモリインタフェース			
	アドレスビット	24ビット	23ビット	23ビット
	データビット	8/16/32ビット	8/16ビット	8/16ビット
	チップセレクト	3	2	2
	対応デバイス	ROM/RAM	ROM/RAM/SDRAM/FCRAM	ROM/RAM/SDRAM/FCRAM
	I ² Cインタフェース			
	対応モード	標準(100Kbps)	標準/高速(400Kbps)	標準/高速(400Kbps)
	GPIO	8ピン(最大)	26ピン(最大)	26ピン(最大)
	入力変化割り込みポート		(4ピン)	(4ピン)
	暗号/認証マクロ			
	DES/3DES			
	AES			
	HMAC-MD5/SHA1			
	REDC			
	IPsecマネージャ			
	大容量ROM		(256Kバイト)	(256Kバイト)
大容量RAM		(64Kバイト)	(64Kバイト)	
USBインタフェース	(FSモード)			
カードインタフェース	(CFカード)			
パッケージ	FBGA-240	LQFP-144	LQFP-144	
動作周波数	66MHz(最大)	CPU:50MHz(最大) 周辺:33MHz(最大)	CPU:50MHz(最大) 周辺:33MHz(最大)	
電源	2電源(1.8/3.3V)	1電源(3.3V)	1電源(3.3V)	

● 大容量ROM/RAM内蔵

チップ内に大容量ROM(256Kバイト)と大容量RAM(64Kバイト)を搭載しているため、本製品のみでシステムを実現できます。またチップ内部でデータ処理が行えるので、外部端子のモニタリングによるデータの漏洩などのセキュリティ対策にも有効です。

● ミドルウェアソリューション

本製品では、ネットワーク機能を実現するためのプロトコルスタックとして、当社製のKASAGOと富士通デバイス㈱のeTCP/IPが利用できます。また、RSAなどの各種暗号アプリケーションへの対応を準備中です。

図2にサポートミドルウェアを示します。

開発環境

本製品は、当社統合開発環境SOFTUNE® 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2に開発ツール構成を、表3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, REALOSは富士通株式会社の登録商標です。

表2 開発ツール

ハードウェア	MB2198-01(ICE本体)
	MB2198-1Q(DSUケーブル)
ソフトウェア	SOFTUNE Workbench プロフェッショナルパック(統合開発環境)
	REALOS/FR (ITRON3.0準拠リアルタイムOS)

表3 評価ボード

型格	概要
MB9194xEB(開発中)	MB91403, LAN-PHY, FLASH, SRAM搭載済み LANポート x1, RSポート x2

図1 MB91402/MB91403ブロック図

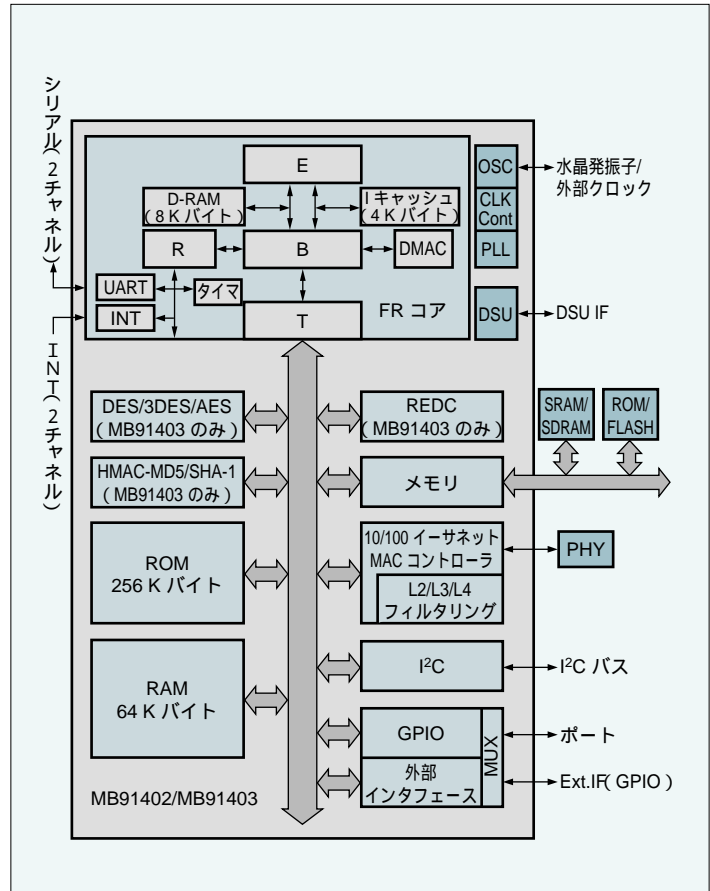


図2 サポートミドルウェア

