システムを堅牢にするマルチコアプラットフォームFIDES

井上 浩明・佐藤 直樹

要　旨

今後のデジタル家電や携帯電話、車載システムでは、出荷後のソフトウェア追加による機能拡張が必要となると考えられています。本稿では、そのようなシステムを堅牢にする非対称型マルチコアプラットフォームFIDESについてご説明します。このFIDESプラットフォームは、マルチコアによる高性能性と省電力性だけでなく、システムの基本機能と、ダウンロードアプリケーションなどの追加機能とを、物理的に異なるプロセッサ上で実行することで、より高い信頼性を実現します。

キーワード

●マルチコア　●ネイティブアプリケーション　●動的追加・実行機能　●セキュリティ

1.はじめに

デジタル家電や携帯電話、車載といったシステムの高性能化は、半導体の微細化に基づいた周波数向上の恩恵によって支えられてきたといって過言ではありません。しかしながら、近年、その微細化は、周波数向上といった恩恵だけでなく、消費電力の劇的な増大といった問題を引き起こしています。この消費電力の問題を解決するための1つのアプローチとして、周波数向上による高性能化の代わりに、処理に含まれる並列性を活用することで性能を向上させるマルチコア技術が注目されています。

NECおよびNECエレクトロニクスは、低消費電力化を実現するマルチコア技術にいち早く着目し、その結果、非対称型マルチコア技術を業界で始めて適用した携帯電話向けアプリケーションプロセッサMP211[1~4]や、ARM社との共同開発による対称型マルチコアMPCore、自動並列化を実現する制御並列型マルチコアPinot[5]といった、組み込み分野での数多くの研究成果を創出しています。

さらに、NECおよびNECエレクトロニクスは、マルチコア技術による高性能化・低消費電力化といった価値だけでなく、コアを複数有するマルチコア技術の特徴を再定義することで、出荷後のソフトウェア追加による機能拡張が今後必要となるデジタル家電や携帯電話、車載といったシステムに対して、高信頼性(堅牢性)という新しい価値を提供するマルチコア技術の研究開発を進めています。

図1は、NECおよびNECエレクトロニクスにおけるマルチコア技術の位置付けを示しています。本稿では、今後様々なシステムがサポートすると考えられるネイティブアプリケーションの動的追加(ダウンロード)・実行機能に向けて研究開発中のマルチコアプラットフォームFIDES[6]について紹介します。

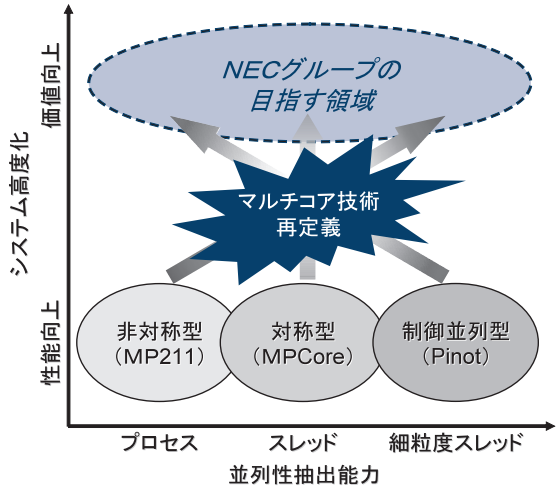

図1　NECグループでのマルチコア技術の位置付け

2.マルチコアプラットフォームFIDESとは

今後様々なシステムが、ネイティブアプリケーションの動的追加・実行機能をサポートすると考えられています。ネイティブアプリケーションは、Javaといった従来の非ネイティブアプ

リケーションと異なり、システムを構成する基本アプリケーションと同一の実行環境で動作可能であるため、非常に高速でかつ柔軟な機能を実現することが可能です。そのため､ユーザは、システムの利用開始後に自分の好きな機能を自由に組み合わせることが可能となります。

しかしながら、もしそのダウンロードされたネイティブアプリケーションに不具合があった場合には、システムが正常に動作できなくなる可能性があります。さらに、もしウイルスであった場合には、システムが悪用される危険性もあります。このように、ネイティブアプリケーションの動的追加・実行機能には、その柔軟性ゆえに、システムの堅牢性をいかに保つかというジレンマがありました。

そこで､NECおよびNECエレクトロニクスは、システムにおける基本機能と、ダウンロードアプリケーションなどの追加機能とを、物理的に異なるプロセッサ上で実行することで、高い信頼性を実現するマルチコアプラットフォームFIDESを開発しました。ちなみに、このFIDESとは、ラテン語で「信頼」を意味する単語です。

図2は､3つのプロセッサコアからなる非対称型マルチコアプラットフォームFIDESの構成を示しています。この例では、それぞれのプロセッサ上に、基本ドメイン、信頼ドメイン、および非信頼ドメインと呼ばれる実行環境が動作しています。ここで、基本ドメインは、システムの基本機能を担うアプリケーションを実行するために用意されています。すなわち、外部からダウンロードされたネイティブアプリケーションは基本ドメイン内では一切実行されません。一方、信頼ドメインおよび非信頼ドメインは、ダウンロードアプリケーションなどの追加機能を実行するために用意されています。そのうち、信頼ドメインは信頼できると保証されたアプリケーションを、非信頼ドメインはそれ以外のアプリケーションの実行を担当します。これにより、基本機能と追加機能間だけでなく、追加機能同士に対してもより高い安全性を実現することができます。

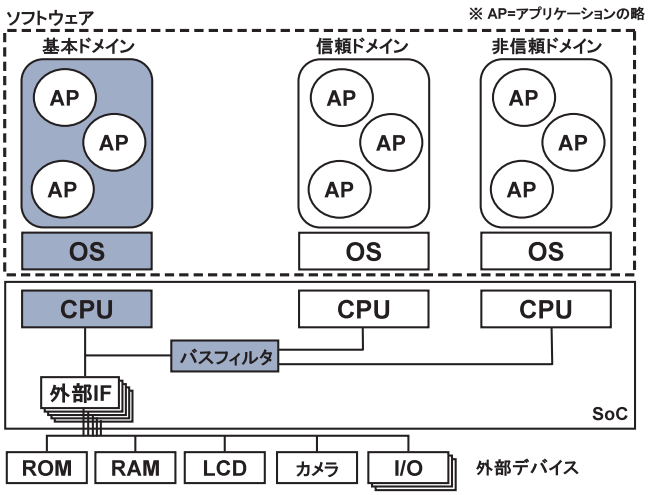

図2　マルチコアプラットフォームFIDES

つまり、本プラットフォームは、ネイティブアプリケーションの信頼度に応じて、異なるプロセッサコア上の実行環境を提供する点に特徴があります。これにより、もしダウンロードアプリケーションに不具合やウイルスが含まれていたとしても、その影響は信頼ドメインないし非信頼ドメインに限定されるので、基本ドメイン上のアプリケーションには何の影響もありません。さらに、信頼ドメインないし非信頼ドメインは異なるプロセッサコア上で動作しているため、たとえそれらのドメインが不具合やウイルスの影響を受けたとしても、それらのドメインを基本ドメインとは独立に復旧することが可能となります。

3. FIDESプラットフォームを支える技術

第2章でご紹介したマルチコアプラットフォームFIDESの実現にあたっては､3つの大きな技術的課題がありました。

1) プロセッサコア間で共有される資源の分離
2) 複数の実行環境によるメモリ量の増大
3) 各プロセッサコアのセキュリティレベル制御

NECおよびNECエレクトロニクスは、今回それぞれの課題を解決する技術を適用することで、高信頼性を提供する組み込み向けマルチコアプラットフォームを世界で初めて実現しました。以下に、それぞれの技術詳細について説明します。

3.1 バスフィルタ論理

一般のマルチコアプラットフォームでは、図2に示されるように、メモリや液晶、カメラといった外部資源は、すべてのプロセッサコアから共有できるように設計されます。しかしながら、もし信頼ドメインないし非信頼ドメイン内のダウンロードアプリケーションに不具合やウイルスが発生した場合、その影響は、共有資源を通じて、基本ドメイン内の基本アプリケーションへ大きな影響を与えます。たとえば、メモリ資源に関していえば、そのような不具合やウイルスは、基本ドメイン内のアプリケーションが利用しているメモリ領域を破壊すること

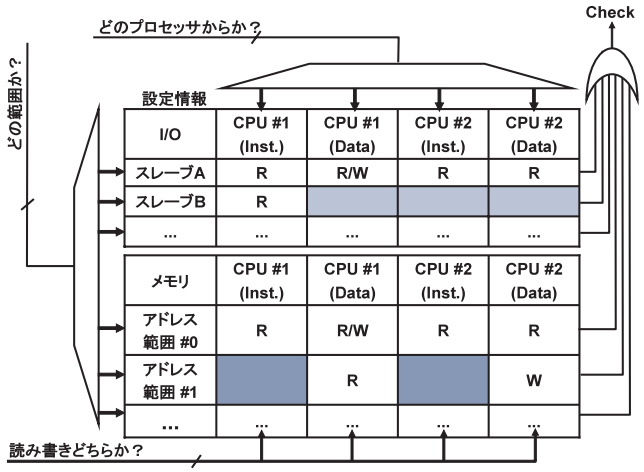

図3 バスフィルタ論理

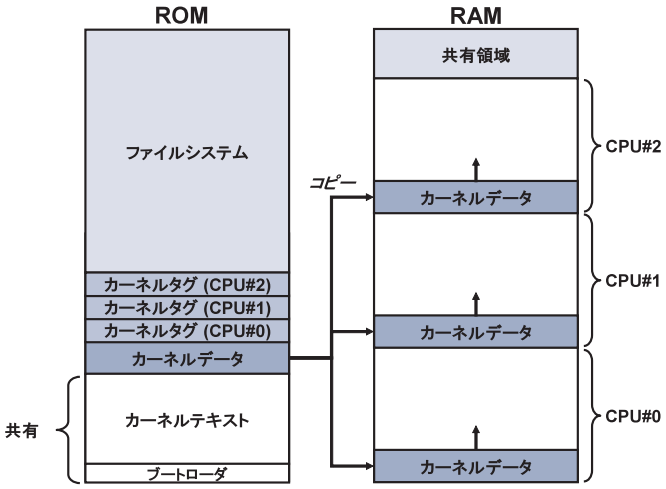

図4　複数カーネルXIP

で、基本機能の動作を止めることが可能となります。したがって、そのような共有資源への不正アクセスを制御するための技術、バスフィルタ論理が必要となります。

図3は、バスフィルタ論理の構成を示しています。この論理は、チップ内のシステムバスに接続され、そして、与えられた設定情報に基づいて、共有資源への不正アクセスについて監視します。なお、どのプロセッサコアがどの外部資源のどの範囲をアクセスできるかを指定する設定情報は、基本ドメインからのみ更新できるようにしています。たとえば、図3では、CPU#1はアドレス範囲#0のメモリを読み書きできますが、一方アドレス範囲#1のメモリは読み出ししかできません。これにより、信頼ドメインないし非信頼ドメインからの万一の不正アクセスから、基本ドメインを保護することができます。

3.2 複数カーネルXIP

一般のマルチコアプラットフォームにおいて、プロセッサごとに実行環境(カーネル)を提供することは、システムを堅牢にする利点の代償として、必要メモリ量が増大してしまう、すなわち、組み込みシステムのコストアップにつながります。従来、単体カーネルの必要メモリ量を削減する技術として、カーネルの持つ命令領域と読み出し専用データ領域をROM上に配置し、そして、通常データ領域をRAMにコピーするXIP(Execute-In-Place)技術が利用されていました。そこで、当社はマルチコアプラットフォームにおける必要メモリ量を削減するため、単体カーネルの必要メモリ量を削減するXIP技術に着目し、そして、それをマルチコアプラットフォーム向けに拡張した複数カーネルXIP技術を開発しました。

図4は、複数カーネルXIPのコンセプトを示しています。この技術は、単体カーネルの持つ命令領域および読み出し専用データ領域を複数のカーネル間でROM上にて共有し、そして、通常データ領域をそれぞれのカーネルに固有なRAM領域にコピーすることによって、マルチコアプラットフォーム総計で必要とされるメモリ量の削減を図ります。もちろん、すべてのカーネルはシングルコアでのカーネルと同じ仮想アドレスで動作することが可能です。これにより、OSとしてLinuxカーネルを利用した時に、複数カーネルXIP技術を適用しない場合と比べて、その必要な静的メモリ量を約182%削減することができました。

3.3 セキュリティドメイン分離技術

ネイティブアプリケーションをダウンロードし、端末上で実行する場合、信頼ドメイン、非信頼ドメインのいずれで動作させるかを決定する必要があります。FIDESでは、ネイティブアプリケーションの実行ドメイン識別のため、証明書を使用しています。ネイティブアプリケーションが信頼しても良いことを示す証明書とともにダウンロードされた場合、そのアプリケーションは信頼ドメインで実行し、証明書がない場合には非信頼ドメインで実行します。ダウンロード処理や証明書の確認は、基本ドメイン上にあるアプリケーションマネージャと呼ぶソフトウェアによって行う構成をとっています。アプリケーションマネージャは、ダウンロードしたアプリケーションを起動する

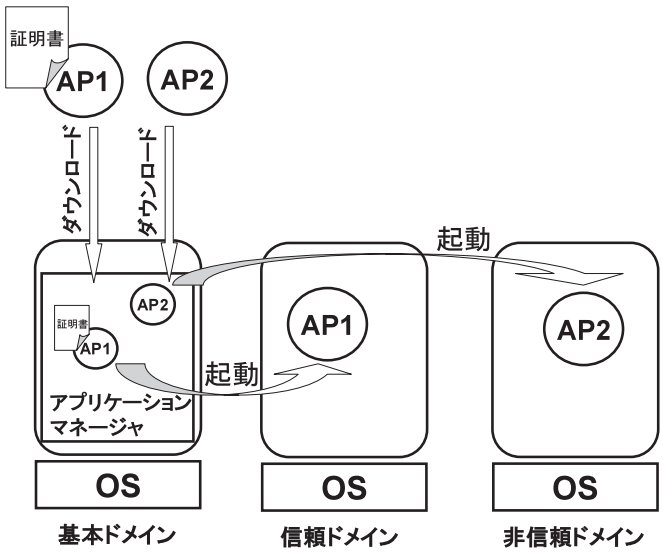

図5　アプリケーションマネージャ

際、信頼ドメイン、非信頼ドメインの割り当ても行います（図5）。

システムでアプリケーションを動作させる場合、アプリケーションの信頼度に応じて使用できるライブラリ、システムコール、アクセスできるファイルを制御する必要があります。FIDESでは、バスフィルタ論理技術による共有資源へのアクセス制御とともに、OSレベルのソフトウェアによるライブラリ、システムコール、ファイルへのアクセス制御も行います。このアクセス制御は、信頼ドメイン、非信頼ドメインそれぞれに用意されたポリシに従って行われます。この機能により、たとえばあるシステムファイルは、信頼ドメインからのみアクセスでき、非信頼ドメインからはアクセスできないなどの制御が可能となります。ハードウェアのアクセス制御とOSレベルのアクセス制御により、より高い信頼性を実現しています。

4. おわりに

本稿では、出荷後のソフトウェア追加による機能拡張が今後必要となるデジタル家電や携帯電話、車載システムに対して、高信頼性(堅牢性)という新しい価値を提供するマルチコアプラットフォームFIDESについて紹介しました。

その応用例として、ネイティブアプリケーションの動的追加・実行機能に対して、システムにおける基本機能と、ダウンロードアプリケーションなどの追加機能とを、物理的に異なるプロセッサ上で実行することで、高い信頼性を実現できることを説明しました。

また、その実現にあたっての3つの大きな技術的課題を解決する、バスフィルタ論理技術および複数カーネルXIP技術、セキュリティドメイン分離技術といった、NECおよびNECエレクトロニクスの有する技術を紹介しました。

今後は、デジタル家電や携帯電話、車載といった幅広い分野への適用をめざして、さらなる研究開発を進めていく所存です。

参考文献

1) 枝廣ほか；「マルチコア向けソフトウェア・プラットフォームを開発し、携帯電話機に適用」，日経エレクトロニクス 2005年3月28日号, pp.125-136, 2005.
2) Torii, S. et al. ; "Asymmetric Multi-Processing Mobile Application Processor MP211", NEC Journal of Advanced Technology, Vol.2, No.3, pp.204-210, 2005.
URL http://www.nec.co.jp/techrep/en/r_and_d/a05/a05-no3/a0503p204.html
3) Torii, S. et al. ; "A 600MIPS 120mW 70uA Leakage Triple-CPU Mobile Application Processor Chip", ISSCC 2005 Proceedings, pp.136-137, 2005.
4) Sakai, J. et al. ; "Multi-tasking Parallel Method on MP211 Multi-core Application Processor", COOLChips VIII Proceedings, pp.198-211, 2005.
5) Ohsawa, T. et al. ; "Pinot: Speculative Multi-threading Processor Architecture Exploiting Parallelism over a Wide Range of Granularities", MICRO-38 Proceedings, pp.81-92, 2005.
6) Inoue, H. et al. ; "FIDES: An Advanced Chip Multiprocessor Platform for Secure Next Generation Mobile Terminals", CODES+ISSS 2005 Proceedings, pp.178-183, 2005.
7) 稗田ほか;「携帯端末用Linuxにおけるリソース管理の実現」,情報処理学会論文誌:コンピューティングシステム, Vol.SIG03(ACS8), No.1, pp.1-11, 2005.

執筆者プロフィール

井上 浩明
中央研究所
システムデバイス研究所
主任

佐藤 直樹
中央研究所
システムプラットフォーム研究所
研究部長

●本論文に関する詳細は下記をご覧ください。

関連URL: http://www.labs.nec.co.jp/Overview/soshiki/device/systemlsi.html