

# Wind River VxWorks MILS プラットフォーム 2.0

防衛、ネットワーク、インダストリアルといった分野や、その他の世界的なインフラストラクチャなど、影響力の大きいシステムの構築を担う企業は、ますます多くの機能を必要とするだけでなく、意図的または不注意による脅威やエラーからの防御を極めて高度に保証する、セキュアかつ安全な運用も求められています。同時に、こうしたシステムは、制限されたスペース、重量、消費電力 (SWaP: Space, Weight, and Power) という厳しい条件下で運用しなければならない場合がしばしばあります。

このような難しい要求に対処するために、Multiple Independent Levels of Security(MILS) と呼ばれる新しいシステムアーキテクチャが登場しました。MILSオペレーティングシステムは、単一のプロセッサを複数のソフトウェアコンポーネント間で分割(パーティショニング)し、開発者やシステムインテグレータが定めたセキュリティポリシーに適合するように、時間とスペースのリソース割り当て、情報フロー、故障分離のすべてを厳密に実施するものです。

MILSアーキテクチャを使用すると、ハードウェア統合によりSWaPの縮小が可能になります。機密データや重要データを扱うセキュリティクリティカルなアプリケーションは、MILSによって、中・低レベルのセキュリティのアプリケーション(非セキュアなチャンネルに接続したり、厳密な高セキュリティ保証検査に合格していないアプリケーション)と同一システム上に共存できるようになります。MILSは、セキュリティレベルの異なるコンポーネントを使用するマルチレベルセキュア(MLS)システムと、異なる領域からのデータを扱うコンポーネント(たとえば連合体の各種メンバー)を使用するクロスドメインソリューション(CDS)システムの両方を実現するアーキテクチャです。

Wind River VxWorks MILSプラットフォームは、セキュリティ認証を取得したパーティション分割システム用に開発されました。Wind River VxWorks MILSプラットフォーム2.0は、セキュリティ、堅牢性、パフォーマンスのすべてが高度に要求されるMLSおよびCDSデバイスのソフトウェア開発に適したソリューションです。また、VxWorks MILSプラットフォームは、MLSおよびCDSシステムの基盤となるように設計されています。

VxWorks MILSプラットフォームが提供する機能は以下のとおりです。

- 単一プロセッサ上で異なるデータセキュリティレベルを持つソフトウェアコンポーネントを実行
- 単一プロセッサ上で異なるデータ領域を持つソフトウェアコンポーネントをセキュアに実行
- 単一プロセッサ上で異なるセキュリティレベルのネットワークを実行
- セキュリティクリティカルなコードをサブコンポーネントに分離し、保証評価費用を最適化
- 独立したチームによるサブコンポーネントレベルでの並行作業を実現
- 出荷後にサブコンポーネント単位でのテクノロジーリフレッシュを実現

- テクノロジーリフレッシュ後に必要となる保証レベルの再評価を、費用対効果を上げながら実現

## Development Suite

XML Configuration	Agent-Based Debugging
GNU Compiler	Wind River ICE 2*
Wind River Workbench	Wind River Workbench, On-Chip Debugging Edition*

## Software Partners

Common Criteria Certification Services	Ada for VxWorks
Formal Methods Analysis	Java Virtual Machine
MIL-STD-1553	OpenGL Graphics
Simulation	DDS

## Operating System

VxWorks MILS
--------------

## Hardware Partners

COTS Boards
-------------

## Services

Education and Installation	Platform Customization	
System Design	Hardware/Software Integration	Design Services

\*Optional Components

図1: Wind River VxWorks MILS プラットフォーム

## コモンクライテリアの評価

情報技術セキュリティ評価のためのコモンクライテリア(ISO/IEC 15408)は、認定機関がデバイスソフトウェアを評価し、製品のセキュリティ要件に合致しているかどうかを判断できるようにする国際規格です。国家情報保証連合(NIAP: National Information Assurance Partnership)が、コモンクライテリア評価検証スキーム(CCEVS: Common Criteria Evaluation and Validation Scheme)に基づいて米国におけるコモンクライテリアを管理する米国政府イニシアチブとなっています。

## 特長と利点

Wind River VxWorks MILSプラットフォーム2.0は、防衛機器開発チームに以下のようなさまざまな利点をもたらします。

- **強力な2レベルスケジューリングアーキテクチャ:** VxWorks MILSは、より優れたシステムパフォーマンスの得られる2レベルスケジューラを実装しています。VxWorks MILSプラットフォームをベースにしたシステムは、処理に要する電力が比較的少なくすむため、製品コストの削減も同時に実現します。
- **高保証アプリケーションのサポート:** アプリケーション、ミドルウェア、ドライバなど、高レベルの保証を必要とするユーザコンポーネントは、システムインテグレータが設定した厳密なポリシーの制御下で、複数のパーティションにまたがってセキュアなパーティション間通信を利用できます。
- **中・低保証アプリケーションのサポート:** 中・低レベルの保証を必要とするユーザコンポーネントは、VxWorksのゲストOSサポートを利用できるため、VxWorksをベースにした既存の知的財産の再利用が可能です。
- **開発環境 Wind River Workbench:** VxWorks MILSプラットフォームには、広く採用されているEclipseのフレームワークをベースにした開発環境Workbenchが含まれています。Workbenchは、JTAGや他の接続によるハードウェア立ち上げから、プラットフォームやアプリケーションの開発、パーティション内でのエージェントベースのデバッグ、その後のテストと配備に至るまで、ソフトウェアの設計開発ライフサイクル全体をサポートする豊富な機能を提供。さらに、企業全体でひとつの共通した開発環境を使用することによる標準化を実現します。
- **コンフィギュレーションおよびパーティション構築用ツール:** VxWorks MILSプラットフォームには、RTCA DO-297/EUROCAE ED-124統合化アビオニクス(IMA)開発ガイドンスおよび認証取得要件に基づくツールが含まれており、ユーザコードのコンフィギュレーションとパーティション構築をサポート。製品のライフサイクル全体を通じて、完全なアプリケーション分離を実現します。これにより、初期開発、統合、認証取得のための時間とコストが削減できるだけでなく、開発段階の後期における変更やメンテナンスの費用も削減できます。
- **モジュラーXMLコンフィギュレーションデータおよびセキュリティポリシー:** ユーザコンポーネントごとに独立したXMLベースのコンフィギュレーションデータとセキュリティポリシーにより、認証取得と認証更新のスピードアップを支援し、陳腐化回避にかかるコストを削減します。
- **コモンライテリアEAL6+認証取得:** Wind River VxWorks MILSプラットフォームは、コモンライテリア(ISO/IEC 15408)の評価保証レベル6+/NSAのhigh robustness(高度な堅牢性)の認証を取得するため現在評価中です。

Wind River VxWorks MILSプラットフォーム2.0は、高度な堅牢性を要する環境におけるセパレーションカーネルの米国政府プロテクションプロファイル(SKPP: U.S. Government Protection Profile for Separation Kernels in Environments Requiring High Robustness)バージョン1.03に従って、CCEVSに基づくEAL6+/NSA High Robustness(高度な堅牢性)に適合しているかどうかの評価中であると、NIAPにより正式に発表されました。ユーザは、VxWorks MILSプラットフォームを使用することにより、ユーザコンポーネントの開発と認証取得に集中して努力を傾けることが可能です。

## 高度な堅牢性のためのセパレーションカーネル

VxWorks MILSは、パーティション分割された環境で2レベルのMILS OSアーキテクチャを使用します。また、VxWorks MILSセパレーションカーネルは、低レベルのOSを構成。上位レベルのユーザパーティションは、すべてのユーザコンポーネント(たとえばアプリケーション、ミドルウェアコンポーネント、ドライバ)を実行する場です。VxWorks MILSセパレーションカーネルは、SKPPバージョン1.03に準拠したセパレーションカーネルのセキュリティ仕様を満たすように設計されています。

VxWorks MILSプラットフォーム2.0では、アプリケーションのユーザモード実行環境が仮想ボード上で2つ提供されます。高保証環境(HAE)は、コモンライテリアEAL6+レベルの認証を必要とする高セキュリティ、シングルスレッドのアプリケーション用小型エグゼクティブです。VxWorksゲストOSは、より強力な環境であり、VxWorks 5やVxWorks 6のカーネルと多くのAPIを共有するマルチタスクアプリケーション用です。開発者は、ドライバ、アプリケーション、ミドルウェアをVxWorks 5や6から移植して、VxWorks MILSプラットフォーム用に中・低保証のコンポーネントを作成できます。VxWorks MILSプラットフォームランタイムの他の重要な機能としては、セキュアなパーティション間通信(SIPC)、共有メモリのサポート、セキュリティおよび安全性監査などがあります。

## 最適化された統合開発環境

VxWorks MILSプラットフォームには、EclipseベースのWind River Workbenchが含まれています。この開発環境は、開発、デバッグ、テストに至るセキュリティデバイスの開発段階すべてを通じて、ひとつの共通したインタフェースを提供。Workbenchには、プロジェクトビルドシステム、JTAG接続を介した強力なデバッグ環境、OSを意識したランタイムデバッグエージェント、XMLベースのシステムコンフィギュレーション、GNUコンパイラ、仮想ボードごとに独立したコンソールウィンドウを可能にするアプリケーション多重I/O(AMIO)などの機能があります。

Workbenchは、DO-297 IMA開発ガイドンスおよび認証取得要件に準拠しており、知的財産データのセキュリティセパレーションをロールベースで実行できます。このセパレーションの一環として、開発者は、XMLベースのコンフィギュレーションにより、システム全体の再ビルドや再テストを行わずに、アプリケーションやシステム構成情報を変更できます。さらに、独立したアプリケーションの変更も、他のアプリケーションや基盤となるOSの再テストや再認証を必要とせずに行うことができます。このため、初回認証取得時にかかる時間だけでなく、デバイスのライフサイクル全体を通じて、変更、メンテナンス、認証更新の費用も大幅に削減できます。

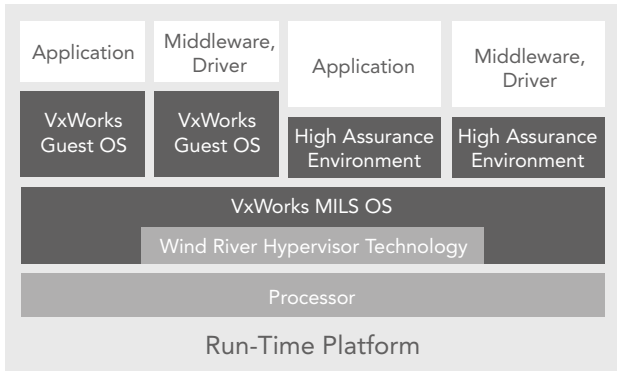


図2: Wind River VxWorks MILS プラットフォーム ランタイム

### 信頼性の高い実績あるパートナー

コモンクライテリアの高EAL/高堅牢性の評価は、精密さが要求されるプロセスであるため、お客様とOSベンダの間に非常に緊密な協力関係が必要となります。その上、MILS上に構築されたマルチレベルセキュアシステムの評価には、数年の年月を要します。こうした取り組みは、OSとミドルウェアのほかに、お客様のアプリケーションについても実行しなければなりません。ウインドリバーのプロフェッショナルサービスチームは、安全かつセキュアなシステムの設計とインプリメントにおける長年のノウハウを活かし、お客様の具体的な評価要件の支援をお約束します。

### パートナー エコシステム

スマートデバイス搭載ソフトウェアの最適化(DSO)業界で、最も包括的かつ最高のサポートを提供するウインドリバーのグローバルなパートナーエコシステムは、弊社のテクノロジーと、ソリューション構築のために選ばれた一流のハードウェアおよびソフトウェア企業が持つテクノロジーを、強固に統合するものです。パートナー企業は、重要なテクノロジーの統合とサポートをすぐに使える形で提供することにより、ウインドリバーの開発およびランタイムプラットフォームの機能拡張を支援しています。

### カスタマーサポートとプロフェッショナルサービス

VxWorks MILSプラットフォームを利用するお客様は、ウインドリバーのグローバルなテクニカルサポートをフル活用し、さまざまな手段による製品サポートとトレーニングを年中無休で受けることができます。またウインドリバーは、専門的なMILSサービス・プラクティスを実施しています。セキュリティアプリケーションに対応した設計、統合、最適化サービスを提供するほか、国際武器取引規制(ITAR)の技術データを保護し、政府会計局の要求に対応できる万全の備えがあります。

## WIND RIVER ウインドリバー株式会社

東京本社  
〒150-0012 東京都渋谷区広尾1-1-39 恵比寿プライムスクエアタワー  
TEL.03-5778-6001(代表) FAX.03-5778-6002

大阪営業所  
〒532-0011 大阪市淀川区西中島7-5-25 新大阪ドイビル  
TEL.06-6100-5760(代表) FAX.06-6100-5761

E-mail: info-jp@windriver.com <http://www.windriver.co.jp>

登録商標: Wind River, Wind Riverロゴ, Tornado, VxWorksは、Wind River Systems, inc.の登録商標または商標です。記載されているすべての名称は、各社の登録商標、商標またはサービスマークです。

### ■販売代理店