

Wind River High-Assurance Solutions for Aerospace & Defense

ウインドリバーの航空宇宙・防衛向け高保証ソリューション

戦場で戦う兵士たちがミッションを漏洩させないようにするとき、本国での防衛担当者がテロ攻撃を阻もうとするとき、そして、救援隊員が緊急事態への備えを強化させようとするとき、信頼できるデータの提供とセキュアな情報の共有は、デバイスのスペース、重量、消費電力、運用コストの低減と並行して、極めて重要になります。その解決策は、マルチレベル・セキュア(MLS)システム。単一のプロセッサ上において、セキュリティや安全性のレベルが異なるアプリケーションを、さまざまな機関から、または多国籍の連合組織において実行することができます。しかも、独立した各アプリケーションは、精密に定義されたセキュリティ・ポリシーに従ってのみ他のすべてと通信を行うという、極めて高度な保証を得られるシステムです。

今、何が問題となっているのでしょうか。現在のテクノロジーでは事実上、マルチレベル・セキュア・システムを単一のプロセッサで構築できません。既存のマルチレベル・セキュア・システムが極めて高度な保証を保ちながら精密に定義されたセキュリティ・ポリシーに従って情報を処理できる場合とは、従来、物理的に分離された複数のハードウェア要素によって、すなわち、別個のコンピュータ、フィールドプログラマブルゲートアレイ (FPGA) 上の別個のエリア、別個のディスプレイ、あるいは別個のネットワークで構築されているシステムを意味していました。すべて、多大なコストのかかる装置と運用手順を要します。

スマートデバイス搭載ソフトウェアの最適化 (DSO) のリーダーであるウインドリバーは、VxWorks MILSプラットフォームの開発によって、こうした状況から脱することに取り組み始めました。オープンスタンダード、実績あるオペレーティングシステムテクノロジー、開発ツールをベースにしたVxWorks MILSには、包括的なユーザ・トレーニング、サポート及びサービスが付属しており、何よりも重要な、お客様との緊密なパートナーシップが含まれています。ウインドリバーは、この関係こそが、高性能なMLSシステムの構築と認証取得に不可欠であると考えます。お客様と力を合わせて、システム全体を成功へと導きます。ウインドリバーは、安全、セキュアで、認証取得済みマルチレベル・システムの実現に向けて、お客様を支援します。

必要なもの:セキュアで安全なリアルタイムOS(RTOS)

お客様の開発者が、次の要件を満たすマルチレベル・セキュア・システムを立案、設計、構築、認証、認可できるとしたら、どうでしょうか。

- 厳しい制約のあるデバイス用にハードウェア、消費電力、冷却、重量、スペースを低減
- 国内や、より広大なグローバル・インフォメーション・グリッド (GIG) にあるさまざまな国内外のシステム間のセキュアな通信
- 不正なアクセス攻撃に対する適切な対処制限措置

「20年前なら、同じようなMLSシステムの開発に10年以上かかっただろう。しかも、巨大でセキュアなオペレーティングシステムの評価に5千万ドルから1億ドルの費用がかかったはずだ。」

— マーク・ヴァンフリート (数学者、INFOSECセキュリティアナリスト、国家安全保障局、MILSコミュニティリーダー)

「アプリケーションとリアルタイムOS (RTOS) の双方を含む、極めて堅牢なMLS/CDSシステムの開発、評価、NSA認証には3年以上の年月がかかり、リアルタイムOS (RTOS) の評価には300万ドルから500万ドルのコストがかかると予想される。」

— ベン・カロニ博士 (ロックフィード・マーティン社ソフトウェアセキュリティ特別研究員、MILSコミュニティリーダー)

- 情報への不正アクセスを阻止しながら、セキュリティ許可と認証手続きの異なるユーザによる同時アクセスを実現 (個人の許可レベルとタスクの整合)
- 開発、認証、認可の時間とコストを低減
- システムの再構成、アプリケーションの追加にかかる時間を短縮し、コストを低減
- スペア装置やトレーニングにかかるメンテナンス費用を低減
- 妥当かつ予測可能な範囲内の時間とコストで、セキュリティ評価、認証、認可を達成

国防総省 (DoD) プログラム用の情報保証 (IA) 製品調達を管理するガイドラインに準拠しながら、上記の要件を満たせるとしたら、どうでしょうか。

技術の進歩と脅威によって、コンピューティング・システムと通信システムの保護に関する考え方が激変したことを認識した米国政府は、国防総省 (DoD) プログラム用のIA製品調達を管理するポリシー、NSTISSP No. 11 (National

Security Telecommunications and Information Systems Security Policy) を発行しました。2002年7月以降、すべてのCOTS (commercial-off-the-shelf: 市販の既製品)IA製品は、ITセキュリティ国際規格CCITE(Common Criteria for Information Technology Security Evaluation)に従って、民間認定機関による評価、検証、認証を受けなければなりません。つまり、これらのマルチレベル・システムは、適切な評価保証レベル(EAL)を満たす必要があることを意味しているのです。米国におけるクリティカルなマルチレベル・システムに関する国家安全保障局(NSA)の要件は「high robustness (高度な堅牢性)」であり、これはコモンライテリア規定のEAL6+に相当します。

ウインドリバーは、MILS (Multiple Independent Levels of Security) が上記すべての要件の解決策であると考えます。

解決策:Multiple Independent Levels of Security

MILSは、マルチレベル対応システムの開発、認証、認可、配備をより実用的、実現可能、かつ入手できるソフトウェア・アーキテクチャです。安全かつセキュアな高度保証システムを構築する際、プロテクションを著しく向上させ、開発時間を短縮し、スケジュールリスクを低減することが可能です。MILSは1980年代に開発されたものの、最近になるまでその恩恵を受けられるほどに業界のテクノロジーが進歩していなかったため、これまでに実装された高性能システムはありませんでした。

MILSリアルタイムOS (RTOS) 単独では、システムがマルチレベルでセキュアであると保証できません。その上、MILSやコモンライテリアの認証取得は、システムが機能的に適切であるとか、十分な性能を持っているとか、耐用年数において満足のいく総所有コストを達成できるといったことを保証するものではありません。ミドルウェア、アプリケーション、通信の個々の特性だけでなく、全体的なシステムアーキテクチャとして、セキュリティ要件と同様に、機能要件やパフォーマンス要件もすべて満たしている必要があります。しかし、オープンスタンダードをベースにしたCOTS製品を使用するMILSであれば、高保証、高性能なマルチレベル・セキュリティ・システムを成功させる基盤となりえます。そこで、ウインドリバーの出番なのです。

そこで、ウインドリバーのMILSソリューションは、レイヤ化されたソフトウェア・アーキテクチャ(リアルタイムOS(RTOS)、ミドルウェア、アプリケーション、通信)を提供し、適切に厳密な認証プロセスと組み合わせることで、開発者がマルチレベル・セキュア・システムを開発できるようにします。

VxWorks MILSプラットフォーム

ウインドリバーのVxWorks MILSプラットフォームは、OSとツールを組み合わせたもので、ミドルウェア、包括的なユーザ・トレーニング、サポートやサービスとあわせて提供します。

他の商用MILSの実装と異なり、ウインドリバーのソリューションは、全体的なシステムがパフォーマンス要件を確実に満たせるようなドライバ、ミドルウェア及びアプリケーションの性能優位性を持っています。VxWorks MILSは、システムに必要なパーティションがほんの数個なのか、あるいは数十個に及ぶのかにかかわらず、一貫性のある、ディターミニスティック(決定論的: 応答性に対する時間保証)な、業界最高のシステム性能を維持します。ウインドリバーはVxWorks MILSを、機能に妥協せず設計しますので、お客様はニーズに合ったシステムの開発と拡張が可能です。つまり、システム開発者の立場からVxWorks MILSを使用するときも、リアルタイムOS (RTOS) の拡張性や柔軟性を心配

する必要がないのです。

VxWorks MILSの利点は、上記のような優れた性能に留まりません。ウインドリバーでは、お客様の組織と緊密に協力し、システムアーキテクチャ全体の定義と改良を支援するとともに、コモンライテリアの評価プロセスの案内役を務めます。航空宇宙・防衛市場で競争力を持つためには、デバイスメーカーは、限られた予算と厳しさの増すスケジュールの中で、ますます複雑になる製品を納品しなければなりません。VxWorks MILSは、お客様のこうしたビジネス目標の達成を支援します。

ウインドリバーのVxWorks MILSには、オプションでWind River Trusted Stackを搭載できます。これは、コモンライテリアの最高レベルの認証を満たしたネットワークスタックです。さらに、ウインドリバーのパートナーであるオブジェクトブ・インターフェース・システムズ(Objective Interface Systems)のパーティション通信システムであるPCsexpressもTrusted Stackを補完するものとして利用可能で、システム内やシステム間のセキュアな通信を可能にします。

デバイスを構築する開発者が市場投入までの時間を短縮できるよう、VxWorks MILSプラットフォームには標準Eclipseベースの開発環境であるWind River Workbenchが含まれています。Wind River Workbenchは、MILSの開発、デバッグ、テストの全段階で開発者に共通したインタフェースを提供します。

VxWorks MILSの機能と利点

アーキテクチャの開発と配備

完全なMILSアーキテクチャ実装のためにVxWorks MILSを使用すれば、次のような機能を活用できます。

- セキュアなカーネル: コモンライテリアに基づくセパレーション・カーネル・プロテクション・プロファイル (SKPP) に合致した堅牢な時間およびスペースのパーティショニング(分割)を提供、高EAL評価に適合します。
- セキュリティ・ポリシー・データベース: アプリケーションとミドルウェア、アプリケーション間の通信、ヘルスマonitoring、セキュリティ監査ログ、その他の機能で利用可能なリソースを定義します。
- リファレンス・モニタ: アプリケーションがセキュリティ・ポリシー・データベースに適合するよう保証します。
- セキュア監査ログ: セキュリティ・ポリシー違反未遂となった全てのログを提供し、信頼できるアプリケーションのレポートにアクセスできます。
- 柔軟なドライバモデル: ドライバがカーネル、ミドルウェア、アプリケーションレイヤや、2または3つのレイヤにまたがることを許可し、所定のセキュリティ要件内のパフォーマンスを最大にします。
- 高性能なミドルウェアレイヤ: デバイスドライバ、ファイルシステム、ネットワークスタック、CORBA、PCsexpress、その他のコンポーネントをサポートします。
- セキュアブート: ブートされたOS、ミドルウェア、アプリケーションが、お客様のもとで認証取得/開発したものと同一になるよう確認します。
- セキュアデリバリ: 納入されたモジュールが、お客様のもとで認証取得/開発したものと同一になるよう証明します。

高度な柔軟性と移植性

ウインドリバーのVxWorks MILSソリューションは、パーティションレベルのオペレーティングシステム用APIとして、VxWorks、ARINC 653、POSIXの3つを提供します。複数のAPIを提供することにより、柔軟性が増し、VxWorks 5.5、VxWorks 6 カーネルモード、ARINC 653、およびPOSIXのアプリケーションをベースにしたレガシーアプリケーションをVxWorks MILSに移植する際の作業量を減らすことができます。

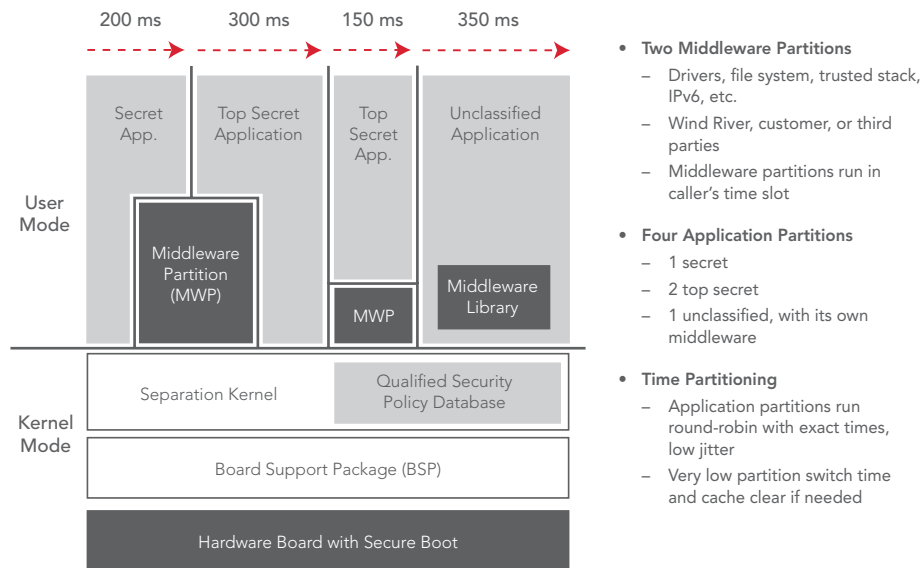


図1: VxWorks MILSシステムアーキテクチャの例

XMLを使った高速コンフィギュレーション

VxWorks MILSは、強力で適格なXMLベースの高速コンフィギュレーション・ツールを搭載しており、新しいアプリケーションやセキュリティ・ポリシーを他者に公開することなく追加したり、再構築することが可能です。これにより、初期の開発および認証時はずもとより、後にデバイスのライフサイクル途中でアプリケーションの再構成や再認証が必要な場合においても、時間とコストが大幅に削減することができます。

コンフィギュレーション・ツールの主な機能は以下のとおりです。

- セキュリティ・ポリシー・データベースを含め、すべてのMILSアプリケーションに必要な静的なコンフィギュレーションレコードを容易に定義可能
- 変更を加えることによって他のアプリケーションやシステム全体に影響が及ぶ「不適格」なシステムと異なり、システム全体の再ビルド、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行わずに、独立したアプリケーションおよび/またはコンフィギュレーション情報を変更可能
- プラットフォームプロバイダ、アプリケーション開発者、システムインテグレータ間で、あるいは、セキュリティ・レベルの異なるアプリケーション開発者間で、知的財産とセキュリティを完全に分離
- DO-297統合化アビオニクス(IMA)開発ガイダンスおよび認証交付文書に完全準拠

結果: マルチレベル・セキュア・システム(例えば、最高機密、極秘、非機密、および/または多国籍のデータが混在するシステム)の迅速な配備と再配備が、セキュリティや安全性のどの要素も損なわずに実現できます。

強力な開発環境

企業独自の開発ソリューションの多くは柔軟性に制限があり、システムの相互運用性が限定されるため、開発コストが事実上増大することになります。ウインドリバーは、MILSシステムを開発する顧客を成功に導くため、異なるアプローチをとりました。EclipseプラットフォームをベースにしたWind River Workbench開発環境により、VxWorks MILSを使ってデバイスを構築する開発者は、市場投入までの時間を短縮できます。Workbenchは、ウインドリバーのリアルタイムOS(RTOS)との強固な統合によって、デバイスソフトウェアの設計、開発、デバッグ、テスト、管理を行う

ための唯一のEnd-to-Endでオープンスタンダードをベースにしたツール群を提供します。

このプラットフォームでユニークなのは、パーティショニングされたOS環境における認証取得済みアプリケーションの実装を支援する3つの高性能なツールです。これらのツールにより、開発者は以下を実行できます。

- アプリケーション別、またはすべてのアプリケーションによるCPU使用率の測定
- ヒープ、スタック、ポート、ヘルスマonitoringデータを含む、OS内のさまざまな領域のメモリ使用量をレポート
- 個々のパーティションにおけるサンプリングポートと待機ポートにわたってトラフィックを監視

ツールとそのレポートインタフェースは、OSと共にテスト済みで適格であり、お客様のアプリケーションの実装環境における認証取得用ドキュメントをテストし、収集するための他に類を見ない機能を提供します。

Wind River Trusted Stack

DoDプログラムにおける接続性、クリティカルリティ、脅威が増しているため、NSAは、実績ある保証と堅牢性に対して高EALの評価を受けた、規格ベースでRFC準拠のIPv4/IPv6プロトコルによるネットワークスタックの必要性を認識しています。こうした要件に対処するために、ウインドリバーは、EAL7を含むコモンクライトリアの高EAL認証取得に向けた信頼できるスタックを提供します。この新しいスタックは、ウインドリバーのネットワークスタック・テクノロジーでの広範な経験を活かし、既存のAPIを使用してセキュアなネットワーク環境への迅速な移行を可能にします。

Wind River Trusted Stackの機能には、次のようなものがあります。

- UDP、IPv4/IPv6、TCP
- 複数アプリケーションで共有可能、または、複数のインスタンス化が可能
- カーネル/スタック/アプリケーション間、またはスタックインスタンス別に、異なるセキュリティ・ポリシーの作成が可能
- 定義可能なセキュリティ・ポリシーと「接続関係」
- DO-178BレベルA評価

- 将来的な高EAL評価取得
- スモールフットプリント
- 高性能
- 現行のすべてのRFC (標準) に準拠
- ハードウェアからの独立性

(ご要望に基づいて詳細をお知らせします。)

Objective Interface SystemsのPCSexpress

PCSexpressは、ウインドリバーのパートナーであるObjective Interface Systemsの高性能リアルタイム通信ソフトウェアで、システム間でセキュアに分離された通信チャンネルを提供します。PCSexpressを使えば、開発者は、高性能でGIG接続された定義域間ソリューション (CDS) を簡単に作成できます。CDSはNSAのSuite B指定の暗号処理を実装し、コモンクライテリアEAL6+、DCID 6/3 PL 5、DO-178B レベルA、FIPS 140-2の認証に適合します。

PCSexpressは、Trusted Stackを補完するものとして、point-to-point(例えばTCP,UDP,SCTP,RapidIO,Infiniband,VME,PCI)とpoint-to-multipoint(例えばIP Multicast, FireWire, USB, Link16)を含むさまざまな通信プロトコルを介して、システム間のセキュアな通信と、強力なノード/アプリケーションの認証を可能にします。詳細については、www.ois.com/pcsをご覧ください。

航空宇宙・防衛業界向けの強力な基盤

20年前、ウインドリバーのハードリアルタイムOSであるVxWorksをご購入いただいた2番目のお客様は、米国防総省でした。それ以来、ウインドリバーは、全世界の航空宇宙・防衛関連企業にとって、先端を行くテクノロジーの選択肢であり続けています。ウインドリバーのVxWorks MILSソリューションは、その伝統を受け継いでいます。

ウインドリバーのVxWorks MILSは、実績ある、信頼性をもった高性能なVxWorks 653リアルタイムOS(RTOS)をベースにしています。このOSは、非クリティカルなアプリケーションの移植性や再利用性にかかわる要件はもとより、ミッションクリティカルなアプリケーションの安全性とセキュリティにかかわる要件に対応するために、航空宇宙・防衛関連企業が必要とする厳格な基盤を提供します。ウインドリバーのデバイスソフトウェア・ソリューションは、軍用や商用の航空機に搭載され世界中を飛び、NASAが開発した宇宙ロケットの多くにも搭載され、太陽系をまわっています。具体的には、ウインドリバーのVxWorks 653リアルタイムOS (RTOS) は、ボーイング787ドリームライナー、ボーイングC-130 AMP、ボーイング767タンカーや、その他の航空機で使用されています。

ウインドリバー MILSアプローチ

高性能なセキュア・システムに関するパートナーシップ

コモンクライテリアの高EALに適合するような、リアルタイムのマルチレベル・セキュア・システムの構築と認証取得には、数年の歳月を要します。しかし、高EALの認証取得それ自体は、適切な機能性やパフォーマンスを保証するものではありません。VxWorks MILSは、MILSアーキテクチャとCOTS OSをベースにした、初めての高性能マルチレベル・セキュア・システムです。

ウインドリバーは、高EAL・高性能なマルチレベル・セキュア・システムの構築と認証取得には、お客様と緊密なパートナーシップを築くことが不可欠であると考えています。このパートナーシップは、ウインドリバーのMILSソリューションの重要なコンポーネントです。

ウインドリバーは、次のような形でお客様の成功を支援します。

- MILSによって複数アプリケーションの共存を保証しながら、全体的なシステムアーキテクチャの定義と改良を行い、適切なパフォーマンスを実現します。アプリケーションのパーティショニング、ドライバの配置、OS/ミドルウェア/アプリケーションにまたがる通信、アプリケーション間の通信がその例です。
- お客様のシステムに基づく具体的なパフォーマンスやセキュリティのニーズに見合うように、セパレーション・カーネル、ボード・サポート・パッケージ (BSP)、ミドルウェアレイヤを変更または増強します。
- 必要なプロテクション・プロファイル (PP) とセキュリティ要件を選択または開発します (用語の定義については付録Aをご参照ください)。
- SKPP以外のPPについて必要に応じて共同作業をします。
- お客様に必要なコンポーネントを含めて、セキュリティターゲットを完成します。
- ハードウェア/ソフトウェアの明確な評価対象を定義します。
- セキュアブートを備えたハードウェア及び関連のソフトウェアを作成します。
- セキュアなデリバリプロセスを作成します。
- BSPを作成し評価します。

ウインドリバーは、お客様、Common Criteria Testing Laboratory (CCTL)、National Information Assurance Partnership (NIAP) と緊密に協力し、マルチレベル・セキュア・システム全体の最終評価をサポートします。これには、OS、BSP、ミドルウェア、アプリケーションなど、システムのセキュリティ要件が必要とするものすべてが含まれます。

高性能MILSシステムの実現

実績あるオープンスタンダード。セキュリティ、安全性、コスト、スケジューリングの制御。ウインドリバーのVxWorks MILSは、そのすべてを可能にします。実際には、MILSは他のシステムのアーキテクチャも変容させる様相を見せていると、ウインドリバーは考えます。クリティカルな公衆安全、エネルギー生成、エネルギー供給から、資産抽出と分配、通信、輸送、医療、財務、その他のアプリケーションに至るまでのすべてが、より小さいフットプリント、費用対効果のより大きなプラットフォーム上で高度に保証されたパフォーマンスを要求するようになるでしょう。ウインドリバーは、その構築を支援する準備をします。

VxWorks MILSは、世界最高レベルのパートナーエコシステム、包括的なプロフェッショナルサービス (受託開発)、高いレベルの顧客サポートによってバックアップされています。ウインドリバーのプロフェッショナルサービスは、すべてのプロセス領域でCapability Maturity Model Integration (CMMI) SW/SE レベル3を獲得しました。サービスのプランニング、エンジニアリング、デリバリーといった領域における、高レベルの品質と価値の証しです。

付録A: コモンクライテリア

ITセキュリティ国際規格CCITE(Common Criteria for Information Technology Security Evaluation) (ISO/IEC 15408) は、以下を可能にする国際基準です。

- ITユーザは、製品のセキュリティ要件を指定できます。
- ベンダは、製品についてセキュリティ要求ができます。
- 民間認定機関は、製品を評価し、要求内容を満たしているかどうかを判断できます。
- 各国の認証機関は、評価を検討、承認し、認証することができます。

コモンクライテリアは、カナダ、フランス、ドイツ、オランダ、英国、および米国の政府によって開発されました。

NSAの米国政府イニシアチブであるNational Information Assurance Partnership(NIAP)と、National Institutes of Standards and Technology(NIST)が、米国におけるコモンクライテリアを管理しています。コモンクライテリア評価検証スキームについてのウェブサイトは<http://www.niap-ccevs.org/cc-scheme/>で、NIAPが保持しています。

コモンクライテリアに基づく評価

コモンクライテリアは、順に厳格さが増す保証要件の各パッケージを定義するために、EALを使用します。EAL1(最下位の保証)からEAL7(最高位の保証)までの番号が振られた各パッケージは、

コモンクライテリアで定義済みの保証スケールのどの位置にあるかを示します。EALによって、IT製品またはシステムのセキュリティ機能が、一定の信頼水準にあるとみなされます。EAL1からEAL4までの評価を得た製品は、コモンクライテリア承認アレンジメント(CCRA: Common Criteria Recognition Agreement)に基づき、24カ国の参加各国が相互承認しますが、EAL5以上の評価を受けた国家機密情報を処理するクリティカルなシステムでは、一般に、メンバー国ごとの認証取得を必要とします。米国では、NIAP評価検証プログラムがそれに当たります。暗号処理製品に関してはFederal Information Processing Standards(FIPS)の検証プログラムが使用されます。

連続する評価レベルは、評価を受ける特定のITシステムの5つの内容に関して、更なる厳密さを定義しています。その5つとは、セキュリティ要件モデル、機能仕様、上位レベル設計、詳細または下位レベル設計、実装です。EALレベル別の内容はそれぞれ、数学的表記を使った形式的記述、構造化された自然言語を使った準形式的記述、または非形式的な記述のいずれかによります。直前の内容との同等性があることを示す「証拠」が要求される規則があり、表現の種類(形式的、準形式的、非形式的)に応じた「証拠」が必要です。たとえば、EAL7では、セキュリティモデルと機能仕様の両方が形式的に記述されなければならない、それらと同等の内容が数学的に証明されなければなりません。

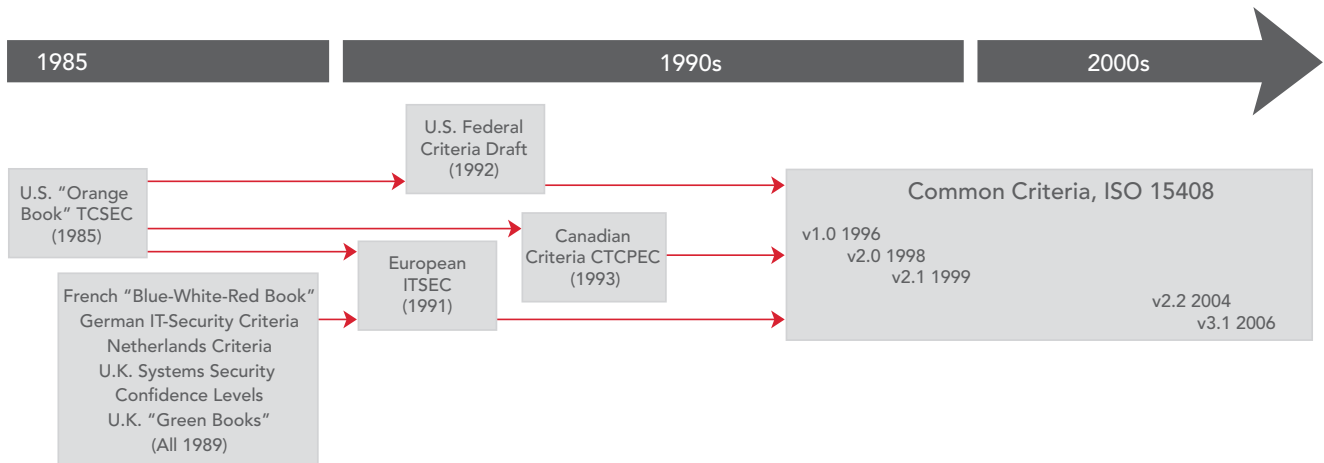


図2: コモンクライテリアの歴史

EAL	Definition	Requirements	Functional Specification	HLD	Covert Channel Analysis
EAL1	Functionally tested	Informal	Informal	Informal	No
EAL2	Structurally tested	Informal	Informal	Informal	No
EAL3	Methodically tested and checked	Informal	Informal	Informal	No
EAL4	Methodically designed, tested, and reviewed	Informal	Informal	Informal	Obvious vulnerabilities
EAL5	Semiformally designed and tested	Formal	Semiformal	Semiformal	Moderate attack potential
EAL6	Semiformally verified design and tested	Formal	Formal	Semiformal	Systematic
EAL7	Formally verified design and tested	Formal	Formal	Formal	Systematic

図3: コモンクライテリア評価保証レベル

レベル別の要件を図3に示します。

コモンクライテリア試験所

米国では、NIAPのもと、NISTが責任もって評価機関を認定します。現在、9名の評価機関が認定されており、これらはCommon Criteria Testing Laboratory(CCTL)と呼ばれます。NSAが「検証組織」にスタッフを配置し、すべての評価の認証に責任を負うと同時に、EAL6およびEAL7における徹底的なコバートチャネルの侵入テストにも責任を負います。

お客様とウインドリバーの協力の重要性

コモンクライテリアの高EAL/高堅牢性の評価は、お客様とOSベンダの間で極めて緊密な協力を要する、厳密さの求められるプロセスであり、MILS上で構築するマルチレベル・セキュア・システムの評価は数年を要します。

こうした作業は、お客様のアプリケーションはもとより、OSとミドルウェアの両方についても実施しなければなりません。ウインドリバーは、このプロセスにおいてお客様とCCTLを支援します。これには次の重要な3種類の文書が関与します。

- **プロテクション・プロファイル**: コンシューマの具体的なニーズを満たすIT製品のカテゴリに対する、実装に依存しないセキュリティ機能要件と保証要件。約60種類のプロテクション・プロファイルから成る最新リストは、www.commoncriteriaportal.orgで入手可能です。MILSが発展途上にあるため、お客様は現存しないPPを必要とする場合がありますが、ウインドリバーが責任を持ちます。
- **セキュリティターゲット**: 特定の製品またはシステムの評価基盤として使用される一連のセキュリティ機能要件、保証要件、および仕様(セキュリティ要求は、特定のPPを参照して行われることがよくあります)。
- **評価対象**: PP、もしくは、より一般的には高EALについてセキュリティターゲットに記載されるIT製品またはシステム。評価対象はセキュリティ評価の対象となる構成要素です。

コモンクライテリアは、情報システムのセキュリティ・ポリシーに関する最新の動向です。

詳細については、www.commoncriteriaportal.orgをご覧ください。

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、ウインドリバー株式会社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