

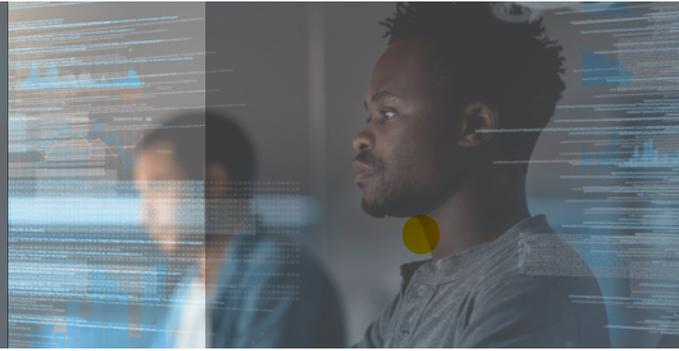


Container Technology Energizes Edge Computing

コンテナを使用した最新VxWorksで実現する
インテリジェントエッジのリアルタイムソリューション



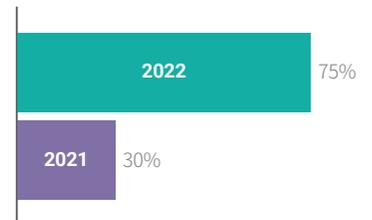
コンテナ技術がもたらす 新たな機会



コンテナ技術のセキュリティ、ポータビリティ、アジリティは、最先端のリアルタイムOS (RTOS) であるVxWorks®の実証済みの機能を補完し、インテリジェントエッジでのコンテナによるデプロイをサポートします。

アプリケーションやその動作を支えるインフラが複雑化すると、新たな攻撃ベクトルが発生し、巧妙化するハッカーに狙われる恐れがあります。組込みシステムにおけるコンテナ技術は、こうした状況下でアプリケーションをインテリジェントエッジに迅速かつ安全に配信するための手段となります。コンテナ技術の活用により、航空宇宙・防衛関連企業、エネルギー事業者、大手メーカー、医療機関などで稼働する最も要求の厳しいアプリケーションに低遅延・高帯域幅というメリットを享受することができます。

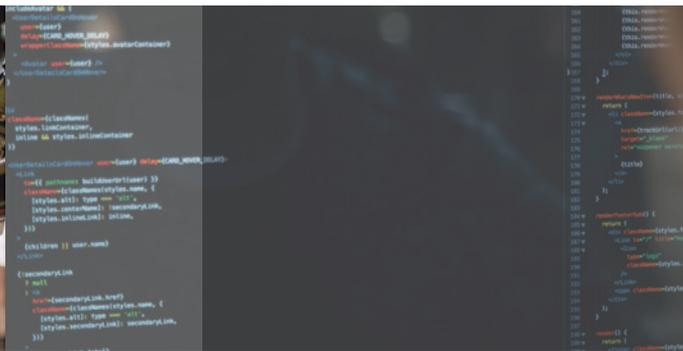
Harry Forbes氏は、ARC Advisory Groupの「Industrial Edge Containers」で次のように述べています。「コンテナがもたらす新たな機能や活用方法を考えるにつれ、組込みシステムとエッジコンピューティングを分ける明確な境界線は、長年かけてどんどん曖昧になっていくように思います¹。いずれは組込み型リアルタイムアプリケーションが、広義のエッジアプリケーション(今日のクラウドアプリのデプロイ形態と同様にコンテナ化され、オーケストレーション機能をもつ、という意味)の中で特殊な存在になる日が来るかもしれません」



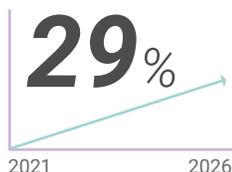
ガートナーは、現在コンテナベースのアプリケーションを本番運用している企業は全世界でわずか30%未満ですが、2022年までにはこの割合が75%を超えるだろうと予測しています²

¹ Forbes, Harry, "Industrial Edge Containers," ARC Advisory Group, June 2019

² "Gartner Forecasts Strong Revenue Growth for Global Container Management Software and Services Through 2024" (press release), Gartner, June 2020



このトレンドがよくわかる例を見てみましょう。アビオニクスシステムは、もともとはハードウェアベースのソリューションでしたが、アジャイルでアップグレードしやすいソフトウェア定義型インフラへと進化しています。これにより、ハードウェアを大々的に入れ替えずに、新たな技術をその場でシステムに取り入れることができます。ソフトウェアのコンテナ技術は、迅速なアップデートやパッチによってサイバーセキュリティの脅威に対応する効果的な手段であり、民間航空や航空宇宙・防衛セクターの両方にメリットをもたらすことが期待されています。しかし、セキュリティ面におけるコンテナ技術の特性を完全に理解し、必要なセキュリティ対策をDevSecOpsプロセスの一貫としてソリューションに統合しなければ、ソフトウェアのコンテナ化による真のメリットは享受できません。



2021年～2026年までのアプリケーション
コンテナ市場の年平均成長率予測³

「インテリジェントエッジにおけるコンテナ活用を考えてみましょう。個々のシステムは、VxWorksやLinux、あるいはその他のプラットフォーム上で稼働しています。システムごとにワークフローが変わらないようにするには、どうすればいいのでしょうか？ ソフトウェアをプッシュ可能なエッジクラウドを想像してみてください。これこそ、ウインドリバーの目指すビジョンです」

—ミッシェル・シャプロウ
ウインドリバー
プロダクトマネージメント
シニアディレクター



³ “Global Application Container Market (2021 to 2026)” (press release), ResearchAndMarkets.com, February 2021

コンテナ技術の進化

ウインドリバーは、最小限のフットプリントを必要とするライフサイクルの長い組み込みソリューションを簡単に構築できるよう、2019年にWind River Linuxにコンテナ技術を搭載しました。

OCI準拠のコンテナをサポートするVxWorks

ウインドリバーは、ミッションクリティカルなアプリケーション開発をさらに強化するために、VxWorksでOCI準拠のコンテナをサポートしたことを発表しました。これにより、開発者が慣れ親しんだIT環境と同じクラウドインフラストラクチャ、ツール、ワークフローを利用できるようになりました。

ウインドリバーは、VxWorksのコンテナサポートを開発することで、リアルタイムOSアプリケーションの技術的進歩のパイオニアとして、さまざまな業界の重要なエッジコンピューティングアプリケーションに十分な堅牢性を備えた、小型の組み込みソリューションを可能にする新しい時代を切り開きます。

DockerやCoreOSをはじめとするコンテナ技術のリーダーは、コンテナを使用する際の基本原則や仕様を策定し、オープンスタンダードへの準拠を実現しています。オープンスタンダードの詳細およびツールやサンプルコードはOpen Container InitiativeおよびGitHubリポジトリに公開されています。

Open Container Initiative (OCI)

コンテナ技術の発展と統一をするためにDockerなどが、コンテナランタイムとコンテナイメージの二つを標準仕様としました。コンテナランタイム仕様は、file system bundle、OCIイメージのダウンロードと展開方法を規定しています。展開されたfile system bundleは、OCIランタイムで実行されるOCI Runtime file system bundleとなります。VxWorksはこれらのOCI仕様に完全準拠しています。

[詳細はこちら](#)

市場を変える自動運転技術

Docker、rkt、Railcar、LXC、CRI-Oなどのコンテナランタイムソフトウェアにはクライアント／ホスト型アーキテクチャが採用されています。図1は、VxWorksのコンテナ実装に適用されるDevSecOpsのプロセスを示しています。

VxWorksでのコンテナの作成・配布

- OCI準拠
 - イメージフォーマット
 - ランタイム仕様
- ランタイム
 - イメージの解析／検証
 - コンテナのインスタンス化
 - アプリケーションの実行
- マネージャ
 - コンテナレジストリからのダウンロード (pull) ロジック
 - 開発／テスト用コマンドラインツール

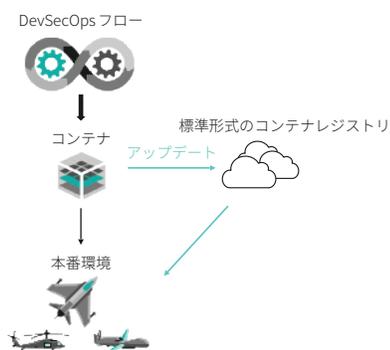
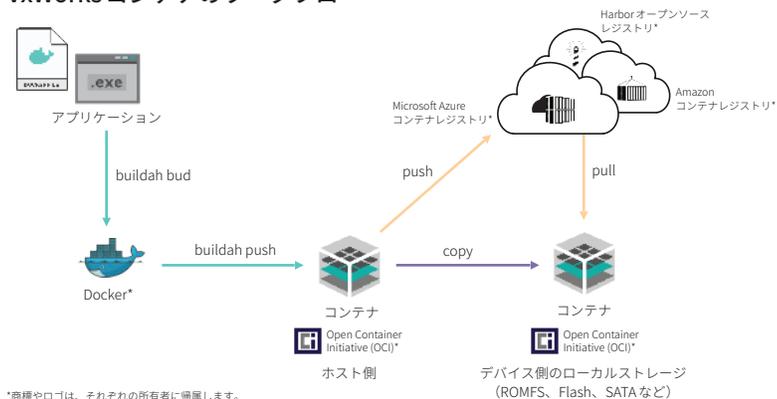


図1. 本番環境におけるVxWorksベースのコンテナ作成・アップデートプロセス

VxWorksベースのコンテナが使われる典型的なDevSecOps環境では、セキュリティフレームワークのベストプラクティスをもとにアプリケーションコードが作成されます。アプリケーションはコンテナとして、VxWorksベースのデバイスなど、対象となるエンドポイントであるホストおよびコンテナレジストリにもリリースされます。コードのアップデートやパッチは、レジストリにプッシュ（アップロード）して保存し、ホストシステムが必要に応じてレジストリからプル（ダウンロード）することができます。航空機からコネクテッドカー、変電所に至るまで、コンテナを使ってコードを配布するシステムすべて（自動車、医療機器、IoT装置、製造現場など）がホストシステムとなり得ます。

VxWorks コンテナのワークフロー



*商標やロゴは、それぞれの所有者に帰属します。

図2. コンテナを作成・配布するエンドツーエンドのワークフロー



アプリケーションのバイナリが開発された後、標準 Docker ファイルを生成します。続いて、オープンソースツールである Buildah が、アプリケーションのコンポーネントを含むパッケージ化された file bundle である コンテナイメージを作成します。このコンテナはコンテナレジストリにプッシュされ、ターゲット側ホストにもコピーされます。コンテナレジストリ (DockerHub、Amazon ECR、Harbor、その他 OCI 準拠レジストリ) を利用することで、アプリケーションのライフサイクルを通じてコンテナに安全な形でアクセスできます。レジストリに公開されたアップデートは、コンテナにパッケージされたアプリケーション (またはアプリケーション群) を使用している正規のホストであれば、自動的または手動で取得することができます。(前ページの図2を参照)

コンテナ配布プロセスには何通りかの方法があります。たとえば着陸後の飛行機が整備場までタキシングして空港内のサービスインフラに接続した後、システムサーバーのレジストリから最近更新されたコンテナを取り込み、航空機システムにアップデートを反映するといったケースもあります。最新の無線機能が搭載された自動車が 5G 通信基地局の周辺を通過する際にコンテナ内の更新情報を受信し、自宅に戻ってガレージに駐車した時点でアップデートを自動でインストールすることもできます。

VxWorks のコンテナ実装技術は OCI ガイドラインに完全準拠しているため、「OCI の標準規格ベースのインフラで正常に機能し、高い信頼性を発揮する」という安心感をもってコンテナを開発していただけます。一方、第三者が独自に開発したソフトウェアデプロイソリューションは、標準ベースのソリューションに比べて予測性や俊敏性に欠けるため、業界での普及はあまり進んでいません。OCI に準拠したツールは、イメージフォーマット仕様とランタイム仕様の両方に準拠しており、コンテナプラットフォームやコンテナエンジン、標準ベースのクラウドプロバイダー環境やオンプレミスのインフラからなるエコシステムに効果的に対応しています。

「ウインドリバーは、VxWorks ならではの特性や、VxWorks が稼働する組込みシステム自体を改変せずにコンテナ対応を実現したいと考えていました。パフォーマンスを犠牲にせず、従来通りのパフォーマンスレベルや製品の DNA、ディターミニズムを継承し、フットプリントを最小限に抑えた設計を活用することを目指しました。VxWorks のコンテナエンジンは合計 400KB 未満、実際のランタイムはわずか 100KB 未満です」⁴

—ミッシェル・シャプロウ
ウインドリバー
プロダクトマネージメント
シニアディレクター

⁴ Expert Discussion: Cybersecurity and Container Usage for Avionics at the Intelligent Edge, Avionics International, March 3, 2021

コンテナのセキュリティ確保

ソフトウェアのデプロイにおいて、セキュリティの徹底は不可欠です。厳格なセキュリティが求められる環境（航空宇宙・防衛、車載アプリケーション、電力網や送電サブシステム、ロボット技術の実装など）でコンテナ技術を普及させるためには、ソリューションの安全性を強化するための追加対策が必要です。

クラウドネイティブなオープンソースレジストリでコンテナを利用する際は通常、多層的なセキュリティ対策が適用されます。たとえばHarborでは、コンテナコンポーネントを保護するためにポリシーやロールベースのアクセス制御を実装しています。コンテナイメージを個別にスキャンして既知の脆弱性がないことを確認し、信頼できるコンテナとしてTrust署名を得てから配信されます。機密性が高いミッションクリティカルシステムへのデプロイ時には、クラウドネイティブのコンピューティングプラットフォーム間でコンテナを移動する際に、一定レベルのセキュリティがHarborで保証されます。

ソフトウェア開発におけるDevSecOpsのベストプラクティスを踏襲することも、コンテナの安全性を確保する上で非常に効果的です。米国国防総省は2020年10月、コンテナのセキュリティ強化に関するガイド「Container Hardening Guide」を公表しました。このガイドには、コンテナをセキュリティ侵害から防御する上で重要なDevSecOpsのプロセス概要が記載されています。

VxWorksのコンテナエンジンは、デジタル署名の検証など、VxWorksで利用可能なセキュリティ機能を活用しています。システムアーキテクトは、コンテナをデプロイする際の攻撃対象や動作環境に応じて、セキュリティレベルを設定することができます。システムの起動から電源オフまでのプロセス全体で、様々な防御対策を利用することができます。VxWorksコンテナのセキュリティ対策には、CIAトライアド原則（CIA＝機密性、完全性、可用性の頭文字）の基本概念が反映されています。

45%



「コンテナ利用時のセキュリティポリシーやツールが社内で整備されている」と回答したセキュリティテクノロジーリーダーの割合（世界全域での調査）⁵

5 Best Practices for Container Security, Forrester, July 2020

技術の融合がもたらす インテリジェントエッジ



要件充足という観点から、アプリケーションパフォーマンスにおける「低遅延・高帯域幅」がますます重要になっています。これに伴い、インテリジェントエッジ向けに最適化されたコンピュータソリューションのニーズも高まっています。

インテリジェントエッジでは、必要な性能を実現するために、5G ネットワーク、AI、機械学習、IoT、先進モビリティなどの新興技術を何種類も取り入れており、コンテナ技術の採用も加速しています。

以下は、エッジコンピューティングにおける課題を解決するためにコンテナ技術が役立つユースケースの一例です。

- **製造オペレーションおよび産業ロボット**：AIベースの自動化は、組み込みRTOSが提供するミッションクリティカルな信頼性を必要とするコンパクトで省電力のインストールによって強化されます。
- **革新的な医療サービスの提供**：COVID-19 パンデミックに対処するために医療機関で行われている遠隔医療、モニタリングシステム、カウンセリングなどの医療サービスにとって、コンテナ技術のセキュリティとアジリティは有効です。
- **自動運転車およびスマートシティの運用**：AIで制御する自動車、車車間通信、交通量監視、先進運転支援システム (ADAS)、都市全体の警告・アラート発信システムなど、多くの組み込みシステムのユースケースでは、軽量・省電力化が重要な要素となります。
- **小売業サービスのパーソナライズおよびコミュニケーション**：自動情報端末、デジタルサイネージ広告のパーソナライズ、リッチメディアを活用した商品ディスプレイ、オンライン注文システムなどのインテリジェントエッジにコンテナ技術を取り入れることで、コンテナの柔軟性やパワーを享受できます。

「インテリジェントエッジを活用すれば、インフラ、ネットワーク、クラウド、データセンターの管理業務だけでなく、センサー、アクチュエーターやデバイスなどが相互接続されたエンドポイントの管理も効率化できます。クラウドゲームや拡張現実 (AR)、仮想現実 (VR) など、超低遅延が要求される消費者向けのユースケースもサポートできます。さらに、業務や顧客に関する大量のデータの集約、セキュリティ確保および分析といったエンタープライズ向けユースケースもインテリジェントエッジで可能になります。工場のフロアや組み立てライン、物流のモニタリングなど、産業機器分野における管理プロセス (品質、材料、エネルギー使用状況の管理) も改善できます」⁶

— Deloitte Insights

⁶ Arkenberg, Chris, Sanket S. Nesargi, Ariane Bucaille, Dan Littmann, "Gaining an Intelligent Edge: Edge Computing and Intelligence Could Propel Tech and Telecom Growth," Deloitte Insights, December 2020



VxWorksベースのコンテナを活用した分割構造のアビオニクスシステム

図3は、VxWorksコンテナによる分割型システム実現の一例です。この事例にある戦闘機システムでは、複数のエッジシステムをリンクさせ、セントラルサーバーに接続しています。セントラルサーバーは通常、航空機の重心近くに設置されます。こうしたアプローチにより、Wind River LinuxやVxWorksをはじめとする複数のOSが混在する環境でも効果的にソフトウェアを管理できるため、ライフサイクル全体にわたり、高い安全性と信頼性をもってアプリケーションを徹底管理できます。

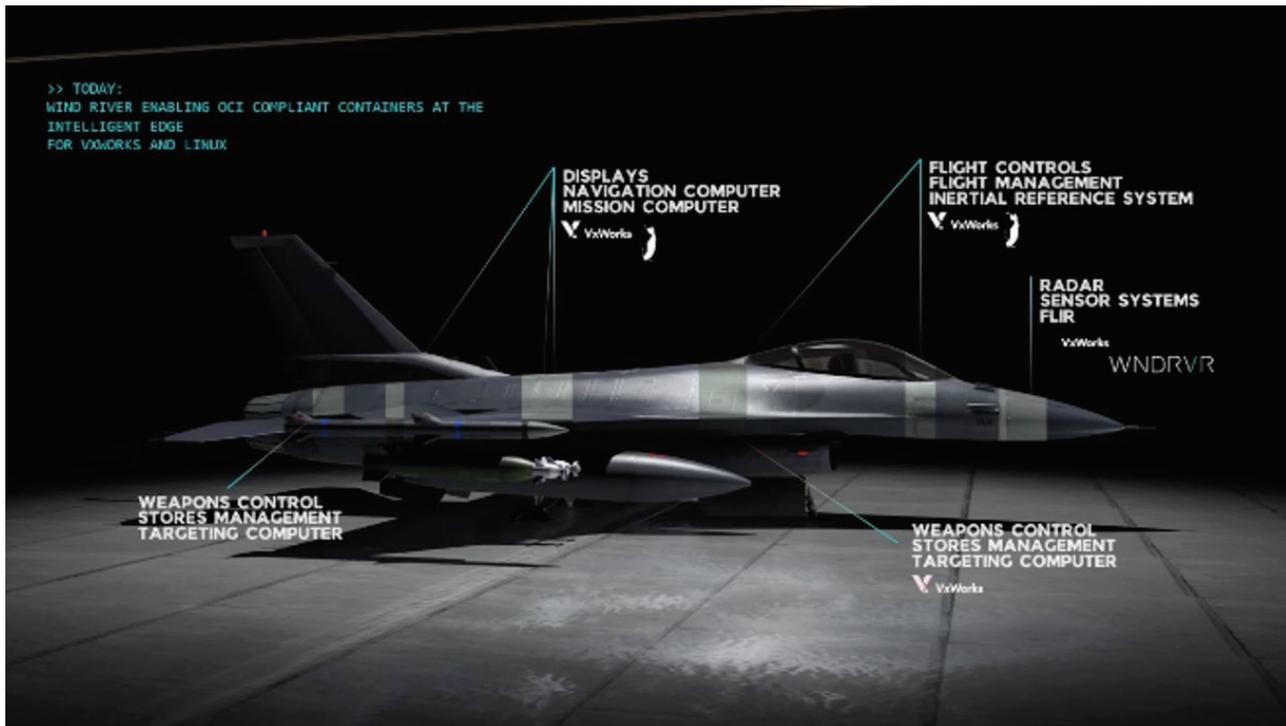
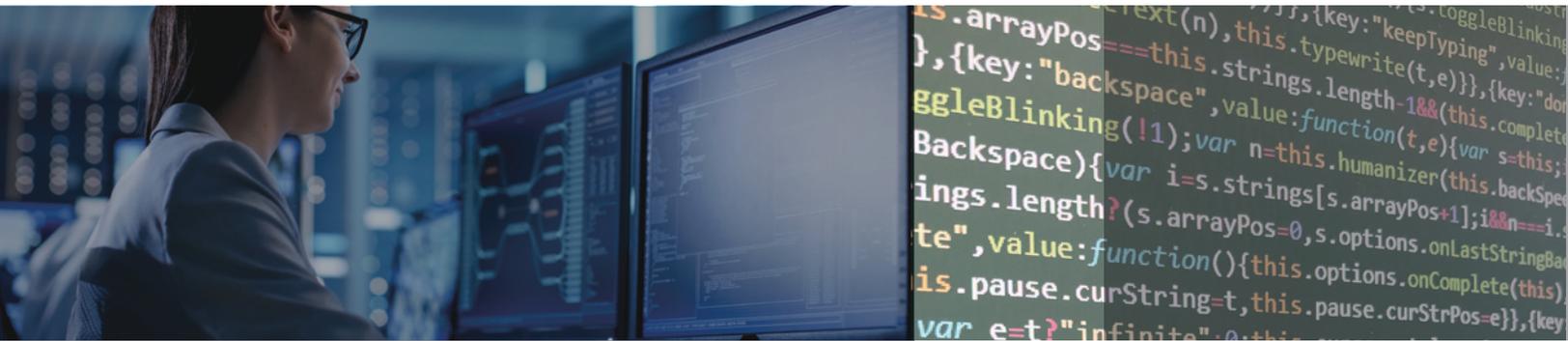


図3. VxWorksベースのコンテナをエッジに実装した分割型アビオニクスシステム



稼働中のシステムでライブコンテナアップデートを実行する際のプロセスをわかりやすく解説するために、プロダクトマネージメントシニアディレクターのミッシェル・シャブロウがデモ動画を作成しました。

デモ動画ではPythonのWebサーバーを使い、手動によるend-of-fieldアップデートプロセスの必要性について説明しています。シャブロウは動画の中で、次のように述べています。「このアップデートプロセスではアプリケーションをシャットダウンして、コンテナレジストリから最新バージョンを取り込みます。デモ動画ではDocker Hubを使っていますが、Iron Bankのようにエッジに配置された他のコンテナレジストリも使用することができます。動画では、コンテナをレジストリから取り込み、最新バージョンのアプリケーションを再起動するまでの流れを説明しています。

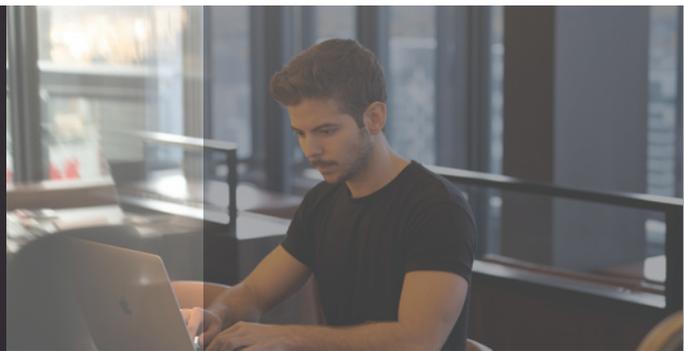
VxWorksがコンテナ対応可能になったため「稼働中のシステムから直接、更新データを取り込むことができるようになりました。一般的なシステムの更新プロセスと同じように、エッジ側のVxWorksがOCIコンテナを取り込んでくれます」と解説しています。Docker Hubのデータから、コンテナがダウンロードされたことが確認できます。検証ロジックを使ってコンテナのデータに齟齬がないことを確認することもできます。

デモ動画では、本番稼働中のVxWorksシステムにおいて簡単に、コンテナデプロイや、シャットダウンして最新バージョンを再起動するアプリケーションのアップデート、一般的なIT環境におけるコンテナのデプロイと同じようにコンテナを運用できる点をご確認いただけます。

「このアップデートでは、アプリケーションをシャットダウンして、コンテナレジストリから最新バージョンを取り込みます。VxWorksでは稼働中のシステムから直接、更新データをプルすることができるようになりました。一般的なシステムのアップデートと同じように、エッジ側のVxWorksがOCIコンテナをプルします」

—ミッシェル・シャブロウ
ウインドリバー
プロダクトマネージメント
シニアディレクター

VxWorksとコンテナの エッジ運用で実現する 未来のアプリケーション



VxWorksのコンテナ対応によって、インテリジェントエッジにおける組込みアプリケーションやユースケースの実現機会が大きく広がります。

VxWorksのコンテナ対応によって、様々な業種で求められる厳格な要件を満たす軽量・省電力・低遅延のソリューションを実現できるようになりました。今後さらなる普及が見込まれる5Gネットワークによって、エッジデータ（およびコンテナ）の配信手段が標準化されていくでしょう。また、3GHzの基地局と28GHzのsmallセルに相互接続されたファイバー網を介してローカルデータセンターとセントラルデータセンターを連携することも可能になるでしょう。これにより、VxWorksで実現可能なソリューションの種類がますます広がります。こうした概念は、航空宇宙業界に大きな影響をもたらす可能性があります。高い安全性と信頼性をもってインテリジェントエッジにアクセスできれば、衛星、無人航空機、通信、ミッションフライトコントロールなどのシステムなどをさらに強化することができます。

- **VxWorks** : 世界をリードする商用リアルタイムOS (RTOS)。航空宇宙・防衛向け、ロボティクスや自動プロセス制御を含む産業機器向け、インテリジェントな車載向けの高性能なアプリケーションに強みを発揮します。最新バージョンではコンテナにも対応し、スペースや電力が制限される組込みシステムのデプロイに適したコンパクトなRTOS機能を提供します。IEC 61508 SIL3、ISO 26262 ASIL D、IEC 62304の認証取得要件にも適合しています。
- **VxWorks 653** : 統合化アビオニクス (IMA) システムの安全性認証取得プラットフォームとして開発された製品です。ARINC 653仕様に適合しており、重要な航空アプリケーションを単一プラットフォームにデプロイできます。VxWorks 653は、FACE™オペレーティングシステムセグメント (OSS) Safety Base プロファイルに適合しています。
- **Wind River Studio** : 複雑な5Gエッジネットワークの構築を補完・管理するインテリジェントエッジのデプロイに必要なすべての機能を提供する統合プラットフォームです。
- **Wind River Studio developer capabilities** は、デジタルスケールのインテリジェントシステムのための唯一のフルライフサイクル管理統合プラットフォームです。開発ワークフローをソリューションセット化し、開発コストの削減のほか、エッジでの構築、テスト、デプロイを加速します。
- **Wind River Simics®** : 複雑なエッジコンピューティングシステムや組込みソリューションの設計、開発、テストプロセスを効率化する包括的なシミュレーション環境です。Simicsはソフトウェアのアジャイル開発およびDevSecOps開発に対応しているため、開発サイクルを短縮できるほか、物理ハードウェアの制約を受けずに組込みシステムの設計を徹底的にテストできます。
- **Wind River Partner Ecosystem** : 幅広いパートナーエコシステムを通じてサードパーティ製のハードウェアやソフトウェアソリューションをご利用いただけます。充実したツールやサービスを取り揃えたパートナーエコシステムで、プロジェクトの開発期間短縮や迅速な市場投入を支援します。

ウィンドリバーは、インテリジェントエッジ向けソフトウェアを提供する世界的なリーディングカンパニーです。そのテクノロジーは1981年の設立時より世界で最も安全かつセキュアなデバイスに搭載され、数十億を超える製品に使用されています。ウィンドリバーのソフトウェアと専門性は、最高水準のセキュリティ、安全性、信頼性を提供しながら、より優れたコンピューティングとAI機能が要求されるミッションクリティカルなインテリジェントシステムのデジタルトランスフォーメーションを加速しています。