DevSecOps in the Automotive Sector

自動車のセキュリティ、安全性、信頼性を実現するために実践する不可欠なこと

WNDRVR

ソフトウェアが自動車のユビキタスとなった今、セキュリティが最重要課題に

自動車のセキュリティ確保は、アドオンソリューションではもはや適切に対応できない課題となっています。最新のベストプラクティスはDevSecOpsを導入し、セキュリティ保護や長期テストの自動化に、開発の初期段階から取り組むことです。

自動車メーカーや、自動車用ソリューションの開発を担う独立系ソフトウェアベンダーは、セキュリティ保護を強化し、運転時の安全性を高める目的でDevSecOpsの採用を進めています。設計における重要作業として、潜在的な脆弱性を開発の初期段階で評価、排除することにより、より安全性の高いソリューションをリリースできるだけでなく、より効率的なコードのメンテナンスが実現できます。

DevSecOpsは既存のDevOpsから派生した概念で、タスクを自動化し、コード開発に一貫性と構造化をもたらします。リスク要因を特定・軽減しようとする場合、既存の開発では、開発期間や現行保守業務の一部としてコードをリリース／レビューする、セキュリティを監視する、シミュレーションを実施するといった手法が採用されています。自動運転車や半自動運転車が普及する昨今では、DevSecOpsによるセキュリティ向上が、顧客信頼の維持、増加するサイバーセキュリティ問題への対処、走行時の安全性強化の観点から不可欠となっています。

2025年におけるサイバー犯罪で生じる年間コスト（予測）[1]

— Cybercrime Magazin

1 “Industry 4.0 and AI Best Practices,” Connected World, July 2020: connectedworld.com/

DevSecOpsとは

DevOpsから派生したDevSecOpsプロセスにより、ソフトウェアの開発と運用を単一の循環型プロセスに統合

このサイクルを実現するには、迅速なコードリリース、厳密なテストおよびフィードバックの実施、ソフトウェア製品の全ライフサイクルの把握が重要となります。ソフトウェアのビルドとアップデートを行うための基本的かつ有効な概念として多くの企業で採用されているDevOpsは、DevSecOpsへと変化し、図1に示すように、セキュリティのプロセスを組み込んだ概念となりました。コードの設計、作成、およびテストの進捗や、脅威の緩和、スキャン、修復、リリース済み各種コードの継続的監視といったセキュリティ課題をこのサイクルに含めることにより精査します。

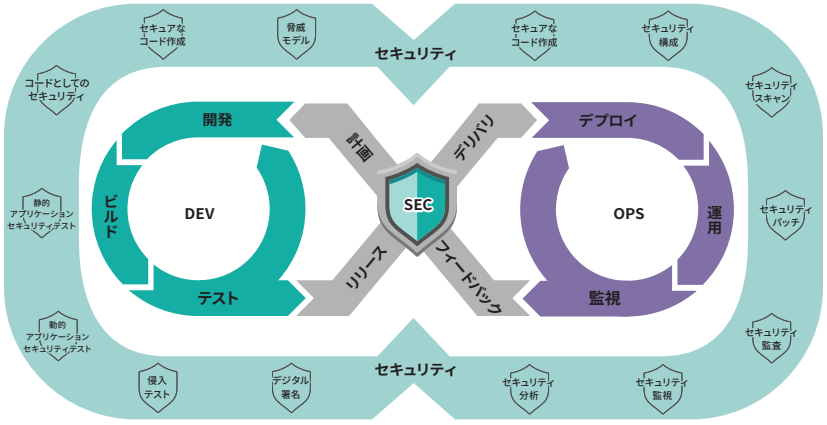
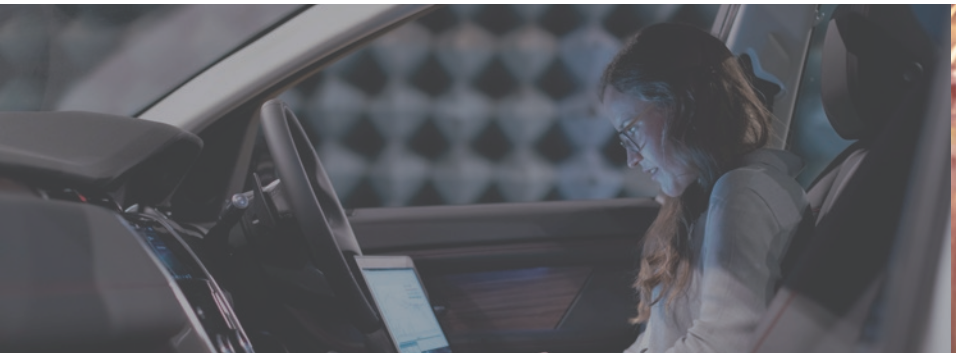


図1：DevSecOpsとは、既存のDevOpsにセキュリティを加えた概念

自動車のセキュリティ保護は、電子制御装置（ECU）および自動運転支援システム（ADAS）の設計および使用において最優先事項となっています。自動車のECUやADASがドライバー以外の第三者によって外部からハッキングされる、制御権を奪われてしまうなどの事態が発生した場合、安全性とプライバシーの両面で甚大な被害につながりかねないからです。

> 「最新型自動車のサイバーセキュリティに対する懸念が広く高まっている現状を受け、国際連合欧州経済委員会（UNECE）は、メーカーと消費者両者による新たなリスクへの対応・管理を支援する目的で、サイバーセキュリティおよびソフトウェアセキュリティに関し、新たに2つの国際基準を整備しました」
>
> — SecurityBoulevard.com



交通システムや公共福祉の保護を担う組織は、リスク要因に対し積極的に取り組むようになっています。たとえば、Security Boulevard の Stephen Gates 氏は次のように述べています。

「最新型自動車のサイバーセキュリティに対する懸念が広く高まっている現状を受け、国際連合欧州経済委員会（UNECE）は先日、メーカーと消費者両者による新たなリスクへの対応・管理を支援する目的で、サイバーセキュリティおよびソフトウェアセキュリティに関し、新たに2つの国際基準を整備しました。このように法的拘束力を持つ基準の設定は、自動車セキュリティ領域で初の国際協調による取り組みとなっています。これらの基準は乗用車、ワゴン車、トラック、バスに適用され、2021年1月から施行されるもので、今日の自動車に150を越える電子制御装置（ECU）が搭載され、1億行ものソフトウェアコードが組込まれているという現状を法整備の主な根拠としています。この数字は、最新戦闘機のおよそ4倍と推定されています」[2]

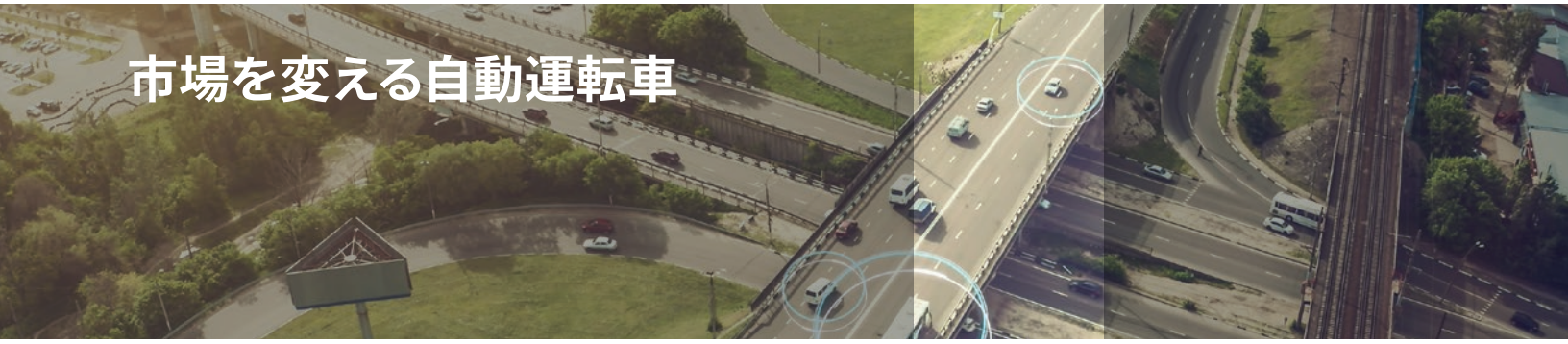
自動車、トラック、その他の車両が「動くソフトウェアプラットフォーム」となりつつあることから、同様の規制が国家レベル、そして国際レベルでも適用されるようになることが期待されます。ウインドリバーは、自動車向けのセキュリティ強化に早い段階から取り組んでおり、サイバー攻撃に強い組込みセキュリティソリューション提供に、幅広い実績をもっています。

米国国家道路交通安全局は自動車セクターに属するメーカーやシステム開発者に対し、自動運転システムの構築（安全基準を含む）、推奨する安全性評価テスト、各種シミュレーションの使用、および教育・研修を支援するガイドラインを提供しています。その全体像について説明した報告書として、「Ensuring American Leadership in Automated Vehicle Technologies」が2020年1月に発行されています。

> 「2023年には、7億7,500万台を超える自動車がテレマティックスまたは車載アプリケーションによって接続される見込みです（2018年は3億3,000万台）」[3]
>
> — Juniper Research

2 securityboulevard.com/2020/07/on-the-road-to-devsecops-securing-the-software-driving-mobility

3 www.juniperresearch.com/press/press-releases/in-vehicle-commerce-opportunities-exceed-775mn



市場を変える自動運転車

自動運転車の普及に合わせた安全システムとセキュリティ保護が不可欠な時代に

自動運転車の世界市場は2019年から2026年の間に、年間成長率39.5%[4]で拡大すると予測されています。自動車の複雑化が急激に進むなか、それに呼応するように組込み式の安全・セキュリティメカニズムの必要性が叫ばれています。このような現状と急激な環境の変化が重なり、DevSecOpsの価値が大幅に高まっています。ソフトウェア更新やパッチ適用、脆弱性の定期的な監視、重要ソフトウェアコンポーネントのライフサイクルメンテナンスを実現するテクノロジーを備えるだけでなく、これらの機能を体系的に提供するシステムを実装する必要があります。

560億6,700万ドルに

2026年までに自動運転車の世界市場が到達すると予測される規模[5]

— Allied Market Research

ADASでは5段階の運転支援レベルが定義されています。完全自動運転の時代に向け、現在は図2に示されるレベル2の段階にあります。人工知能の進化（特にディープランニング）は、完全自動運転への移行完了に必須となるでしょう。この領域に到達するには、安全性の配慮、ハッカー攻撃に対する複数のシステムの保護、より高度な制御システムの導入が必要です。

「深刻な自動車事故の94%は人的ミスが原因です。2018年の米国では36,560人が自動車関連の事故で死亡しており、救命機能を備えた運転支援テクノロジーの必要性が明らかとなっています」[6]

—米国運輸省

0 自動運転なし
ドライバーが、常時、全ての運転操作を行う。

1 運転支援
運転支援システムが走行環境に応じたハンドル操作、あるいは、加減速のいずれかを行うとともに、システムが補助をしていない部分の運転操作をドライバーが行う。

2 特定条件下での自動運転
運転支援システムが走行環境に応じたハンドル操作と加減速を行うとともに、システムが補助をしていない部分の運転操作をドライバーが行う。

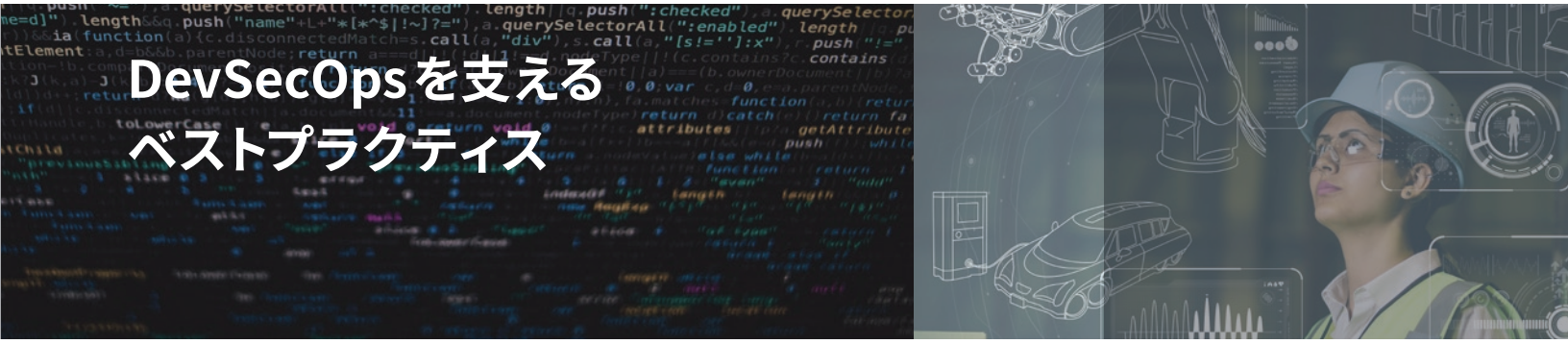
3 条件付自動運転
システムからの運転操作切り替え要請にドライバーは適切に応じるという条件のもと、特定の運転モードにおいて自動化された運転システムが車両の運転操作を行う。

4 特定条件下における完全自動運転
システムからの運転操作切り替え要請にドライバーが適切に応じなかった場合でも、特定の運転モードにおいて自動化された運転システムが車両の運転操作を行う。

5 完全自動運転
ドライバーでも対応可能ないかなる道路や走行環境条件のもとでも、自動化された運転システムが、常時、車両の運転操作を行う。

図2：自動運転のレベル分け[7]

4 www.alliedmarketresearch.com/autonomous-vehicle-market
5 www.alliedmarketresearch.com/autonomous-vehicle-market
6 www.nhtsa.gov/technology-innovation/automated-vehicles-safety#topic-road-self-driving
7 www.nhtsa.gov/technology-innovation/automated-vehicles-safety#topic-road-self-driving



DevSecOpsを支えるベストプラクティス

DevSecOpsを導入する組織が増加し、ベストプラクティスの共通性も進化

ソフトウェア実装時に以下のベストプラクティスを参考にすることで、ワークフローにセキュリティ保護を組み込んでフレームワークを構築することができます。推奨されるガイドラインとして、以下の項目があります。

1. 開発の初期段階で、自動セキュリティ制御とテストシーケンスを組み込む。
2. セキュリティ管理とテストは、開発ライフサイクルの早い段階から、また、開発のあらゆる場所に組み込まれている必要がある。
3. コード開発時にコードをスキャンできるツールを使用して、セキュリティ上の問題を早期に発見する。
4. コードの依存関係（オープンソース）をチェックしてセキュリティの脆弱性を発見する。
5. 静的アプリケーションセキュリティテスト（SAST）ツールを使用して、ソースコードまたはコンパイル済みコードを解析してセキュリティ上の欠陥を見つける。
6. ハッカーの攻撃を模倣するため、自動化されたブラックボックステスト技術として動的アプリケーションセキュリティテスト（DAST）を適用する。
7. 脅威のモデル化による脆弱性の発見とセキュリティ対策のギャップを修正。

このように厳密かつ徹底的な自動化アプローチをセキュリティの設計およびテストに適用することで、ソフトウェアソリューションに不可欠な「脅威の特定及び排除」機能を確実に実装することができます。図3に示すとおり、コードの選択から分析、リリースからライフサイクル管理に至るまで、すべての段階がパイプライン上に網羅されています。また、コードの更新、パッチ適用、および通常の脆弱性テスト実行時に完全なセキュリティを維持するという、最善の成果を得るため、多くの場合、AIコンポーネントが使用されています。AIが更新スケジュールやデプロイ状況を管理するほか、テストを頻繁に実行することにより、未知の脅威検出をサポートしています。クラウドを利用したソフトウェアの配布が一般的になってきており、自動車内にセキュアなソフトウェア環境を安全かつ効率よく維持するために、コンテナの利用が進んでいます。

自動車テクノロジーの進化における ウインドリバーの役割

ウインドリバーが提供するソリューションは、最高レベルの信頼性、セキュリティ、安全性が求められる要求の厳しい業種（重要インフラの構築・保守、産業機械製造、航空宇宙・防衛など）が信頼を寄せるコンポーネントとして、長年にわたる実績を誇ります。
リアルタイムOS（RTOS）であるVxWorks®は、現在注目を集める宇宙探査など、ミッションクリティカルな環境で最大限の信頼性を必要とする多くの企業に選ばれています。ウインドリバーは、5G通信を駆使したインテリジェントエッジコンピューティングの開発および改良にも優れ、未来のスマートシティの交通システムや自動運転車の分野でもより一層重要性が高まるであろう、複雑なインテリジェントエッジ導入にも対応しています。また、コンテナベースの車載ソフトウェアコンポーネント向けクラウドテクノロジーの領域でも、ウインドリバーは豊富なノウハウを備えています。

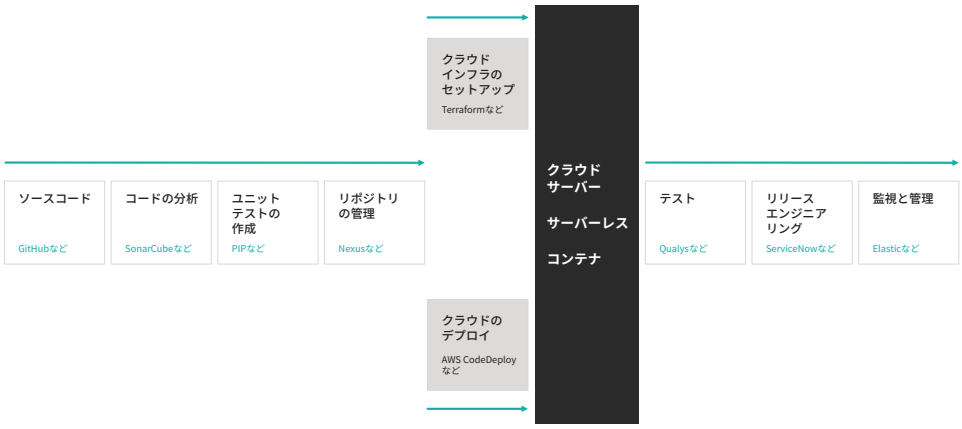


図3：開発サイクル全体で自動テストを重視したDevSecOpsパイプライン

派生製品が複数ある場合でも、DevSecOpsツールを使用して各製品で想定されるあらゆるケースを自動的にテストすることにより、ソフトウェアの完全性を確保することができます。この領域でもAIによるプロセス管理が可能なため、人間の意思決定ミスによるエラーを低減することできます。

車両とその操作に関するデータの収集、クラウドへの送信を定期的に実行するため、ソフトウェア安全性の常時分析、予知保全チェックによるコンポーネント障害のアラート（対ドライバー／修理スタッフ）、安全性課題対応を考慮したプログラミング調整など、さまざまな目的に機械学習機能を利用することができます。

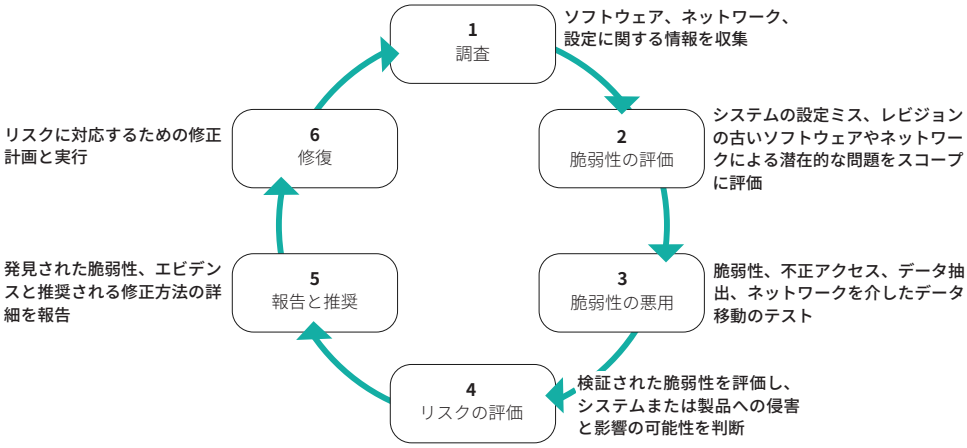
「典型的な次世代型自動車は、多くの場合、5つ以上の領域をベースとするソフトウェアアーキテクチャを備え、車体およびクラウドの両方に数百もの機能コンポーネントを装備しています。これらは、インフォテインメントからADAS、マッピング、テレマティックス、サードパーティ製アプリケーションに至るまで、すべてに対応しています。通常、このアーキテクチャを構築するOEMは、多数のソフトウェアプロバイダーと連携することで、多様な機能を構築します。その過程で、開発言語、OS、ソフトウェア構造などが多角的に自動車に組み込まれていきます。このような断片的なアプローチが業界トップ企業で広く採用されているのは、このようなクロスシステムのニーズすべてに対応できる単一ソフトウェアプラットフォームが市販されていないからなのです」[8]

ーマッキンゼー・アンド・カンパニー
（2020年1月）

8 www.mckinsey.com/industries/automotive-and-assembly/our-insights/the-case-for-an-end-to-end-automotive-software-platform

シミュレーションテストがDevSecOpsの中核に

DevSecOpsモデルで効果を得るためには、適切に定義したパイプラインに従って一貫性の高いテストを頻繁に実行するだけでなく、繰り返し実行する必要があります。また、ハードウェア、OS、ネットワーク、周辺機器、および基板の機能をモデル化するフルシステムシミュレータを使用することで、アジャイル開発を効率よく行うことができます。Wind River Simics®は、コンポーネントの動作を正確に再現できる強力なフレームワークを提供します。その結果、新規コードの設計および実行、脆弱性チェック、検出された問題を解決する修正プログラムの作成、自動車システム全体的な整合性の評価に利用可能なテストベッドを手に入れることができます。
図4に示すとおり、ソフトウェアコンポーネントを常に最新の状態に保ちつつ不正な侵入を防御するためには、侵入テストが不可欠です。これにより、新たなハッキング手法を特定すると同時にハッキングの脅威を軽減することが可能になります。シミュレーションでの侵入テストは、あらゆるセキュリティ保護を強力に突破することで既知の脅威への対処方法を見出すことを目的としており、交通量の多い一般道路で実際に自動車を走らせて行うといった危険なテストを実施する必要がありません。図に示すとおり、このテストはいくつかの段階に分かれており、脆弱性評価を繰り返し行うように設計された循環したサイクルの一部です。このプロセス全体を自動化し必要に応じた頻度で実行することにより、最高レベルのソフトウェア完全性とセキュリティが維持できるようになります。



シミュレーションテストにより、作業時間およびコスト削減が可能になると同時に、実際の機器を使ったテストの実施が不要に

図4：侵入テストによるセキュリティフレームワーク内の脆弱性の特定

ウインドリバーのソリューション

ソフトウェア デファインド ビーグルによる自動車運転が普及し、さまざまな課題が呈されていますが、ウインドリバーが提供するソリューションポートフォリオを利用することで、これらの課題に的確に対応することができます。自動車セクターでの採用実績を誇るVxWorks、Wind River Linux、Wind River Helix™ Virtualization Platform、Simicsに加え、統合型クラウドプラットフォーム、Wind River Studioが新たにポートフォリオに追加されました。ウインドリバーのソリューションは、エネルギー、航空宇宙、防衛、医療、製造をはじめとするミッションクリティカルシステムに幅広く採用されており進化が続けられています。これらのコンポーネントをプラットフォームソリューションやインフラの構成要素として使用することにより、認証取得要件を迅速に満たすことができます。

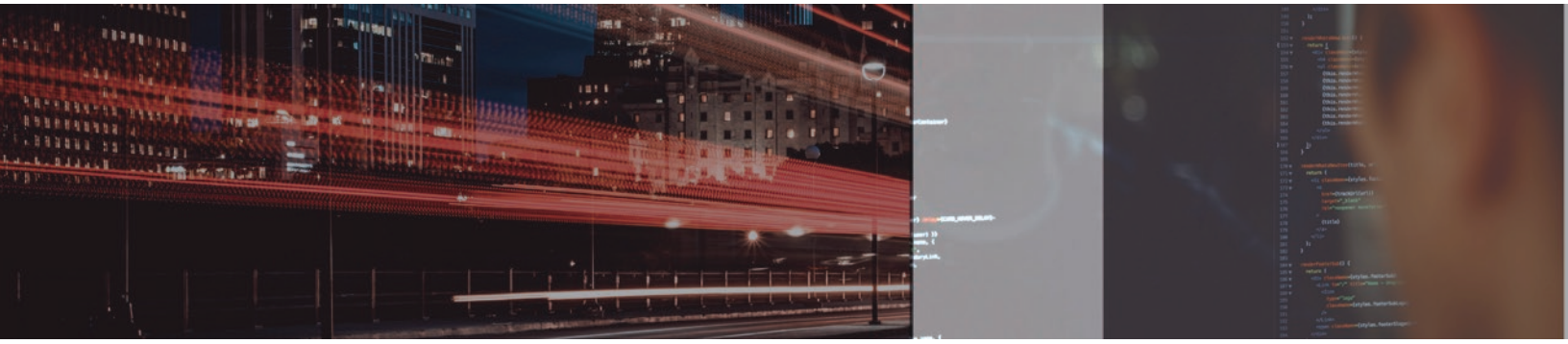
- **VxWorks：**業界をリードする商用リアルタイムOS（RTOS）であるVxWorksは、インテリジェントな車載アプリケーション構築に必要なDevSecOpsワークフローを強力にサポートし、開発段階におけるソースコードの作成、コード分析、ユニットテストの構築、リポジトリ管理に対応します。また、VxWorksは、車載ECU共通標準の確立を目的として自動車業界の開発パートナーシップにより発足した、Adaptive AUTOSAR（AUTomotive Open System ARchitecture）もサポートしています。

- **Wind River Linux：**Wind River Linuxは組込み開発向け商用グレード機能を備え、車載アプリケーションに役立つ機能を提供します。コンテナテクノロジーを使用したマイクロサービスやソフトウエアの更新などさまざまな機能を利用できます。

- **Wind River Studio：**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。Studioは、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。

> 「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、組込みデバイスのセキュリティ強化において数十年に及ぶ実績を誇り、サイバーセキュリティ脅威から組込みデバイスを保護します」[9]

9 blogs.windriver.com/wind_river_blog/2020/03/tools-for-agile-development



- **Wind River Helix Virtualization Platform：**仮想化フレームワークをサポートするソフトウェアプラットフォーム。その実績ある手法により、DevSecOpsワークフローの一環として本番環境にコードをリリースできます。Helix Virtualization Platformは重要度が異なる複数のOSの実行が可能なため、機能安全規格ISO 26262の厳しい要件を満たしながら、セーフティクリティカルなアプリケーションと汎用アプリケーションを同時に実行できます。

- **Wind River Simics：**さまざまなタイプのハードウェアやOSの機能を実行できるフルシステムシュミレータ。安全性とセキュリティを確保するメカニズムを実現しながら、複雑な自動車システムの設計、開発、テストを加速します。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。

今後の方向性

多くの成熟したテクノロジーを融合させることで自動車の安全性とセキュリティの進歩に貢献し、これらを相互運用させることで、車車間（V2V）通信や車車間／路車間（V2X）通信を実現します。DevSecOpsを取り入れた自動車ソリューションは通常、仮想化、クラウドコンピューティング、詳細なシミュレーション、応答性の高いRTOS、5G通信、およびマルチコアアプリケーションをサポートし、冗長性、信頼性、パフォーマンスを実現するハードウェアプラットフォームを必要とします。ウインドリバーは、ダイナミックかつグローバルなエコシステムを構成するパートナーと志を共有し、協力しながら、半自動運転車と自動運転車の開発および実用化に向け、安全かつセキュアな未来の実現を支援いたします。

ウインドリバーは、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、数十億台を超える製品に使用されています。ウイ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、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。