

顧客事例

米国国立標準技術研究所 (NIST) が公開する SSDFサイバーセキュリティタスクへの 準拠を効率化

世界的な電子機器メーカーがウインドリバーのセキュリティサービスを活用し、ソフトウェア開発ライフサイクル全体でのギャップを特定して、SSDFタスクへの準拠に道筋

SSDFの要件対応コストを削減しつつ、開発プロジェクトを スピードアップ

システムやソフトウェアを開発する企業にとって、米国政府および連邦機関が定めるサイバーセキュリティ基準を満たすことは簡単なものではないことは誰もが知っています。しかし、Secure Software Development Framework (SSDF) のタスクを迅速、確実、かつ低コストで満たすために、ソフトウェア開発ライフサイクル (SDLC) を最適化する秘訣はあるのでしょうか？

ウインドリバー製品を利用しているある世界的電子機器メーカー（防衛、米国国土安全保障、医療機器などに組み込まれるインテリジェントな先端エレクトロニクスシステムの製造業者）にとって、その答えはウインドリバーの**セキュリティサービス**を利用することでした。

具体的には、お客様はウインドリバーの**セキュリティアセスメントとSSDFギャップ分析**サービスを利用しました。ウインドリバーのエキスパートがお客様のSDLC全体を厳格に評価し、SSDFが定めるタスクの自社立証に影響を及ぼしうるギャップを洗い出して、ギャップ解消に向けた詳細な修復案を提案しました。

こうした現状評価やギャップ分析は、お客様にとってきわめて重要なものでした。これは、多くの企業にとっても他人事ではありません。なぜなら米国政府機関向けに重要なソフトウェアを提供する事業者は、米国行政管理予算局 (OMB) の覚書「OMB Memorandum M-22-18」に従い、2022年半ばから2023年初頭までにサイバーセキュリティ・インフラセキュリティ庁 (CISA) の共通フォームに自社立証の結果を記入し、提出することが義務付けられているためです。

ハイライト

米国市場で広く事業展開している防衛電子機器のグローバルメーカーは、大統領令14028条 第4e項のサイバーセキュリティ要件を確実に満たすために、自社のSDLCをSSDFのタスクに照らして欠けている項目（ギャップ）を洗い出し、優先順位を付け、修復する必要がありました。これに対応することで、国家安全保障の強化に貢献し、自信をもってより多くの事業機会を開拓することができるようになりました。

お客様の課題

- SDLCを改善し、大統領令14028条に定める厳格な米国政府のサイバーセキュリティ要件を満たすことが求められていた
- 要件の対応に必要なシステム構築にかかる設備投資を最小限に抑える必要があった
- サイバーセキュリティ要員を過剰に投入したり負担を強いることなく、確実に要件に準拠する必要があった

VxWorks® と Wind River Linux の長年のユーザである同社は、ウインドリバーと成功を収めてきた歴史があり、ウインドリバーの専門知識とアセスメント能力に深い信頼を寄せていました。

ウインドリバーはお客様に「自動化および一元化されたDevSecOpsパイプラインの活用」を提案しました。以下は、DevSecOpsにおけるギャップ解消に必要なタスクの提案内容の一例です。

- Infrastructure-as-CodeやConfiguration-as-Code（インフラや構成のコード化）によるオートメーション手法を取り入れてベースとなる汎用パイプラインを構築することで、単一のチームがオートメーションを適宜活用しながらパイプラインを一元的に作成できる体制を整える
- すべてのパイプラインに、セキュリティゲートの自動チェック機能を付加する
- すべてのパイプラインでアプリケーションセキュリティテストツール（SAST、SCA、DASTなど）を利用可能な状態にして、必須化する
- ソフトウェア構成管理にセキュリティ要件を組み入れる

お客様は、ウインドリバーによる分析と是正策の提案をもとに、SDLCの変更箇所に優先順位を付け、作業要員やコストを量的に見積り、体系的かつコスト効率良く変更を完了することができました。

さらに、Wind River Studioの機能は、是正案の実装要件に非常によく適合していました。このお客様の場合はパイプラインマネージャー、ワークフローの自動化、デジタルフィードバックループ、外部ツールとの連携機能などをうまく活用することで是正策を実施できる状態でした。

サービスご利用後

最終的にお客様は、米国政府の定める厳格なサイバーセキュリティ基準に対応するためにSDLCを素早く調整し、今後必要となる自社立証に関わる要求事項を短期間かつ低コスト、高い信頼性で確実に満たすことができるようになりました。

ウインドリバーのセキュリティアセスメントサービスの詳細は、こちらをご覧ください。

www.windriver.com/japan/resource/professional-services-security-assessment-datasheet

活用したウインドリバーのソリューション

- セキュリティサービス：セキュリティアセスメントおよびSSDFギャップ分析
 - お客様のSDLCをウインドリバーの専門チームが分析
 - SDLCとSSDFとの間のギャップを特定
 - 特定されたギャップの解消に向けた緩和策の提案
 - DevSecOpsチームと協力して緩和作業の優先順位を付け戦略を決定
- 将来的にWind River Studio Developerへ移行
 - SSDFギャップ分析で提案された緩和策を効率的に実装するための機能を多数搭載
 - お客様が利用中のVxWorksおよびWind River Linuxプラットフォームに合わせて最適化

導入効果

- NISTのSSDFのプラクティスに効率的に対応するための、既存のDevSecOpsチームのキャパシティと能力を見極めることができた
- 量的かつ客観的なデータから導き出された投資配分案をもとにリソースを確保し、DevSecOps業務の生産性を大幅に高められた
- 要員配置案をもとに、最適なスキルミックスで適正人数のスタッフを手配できた
- NISTのSSDF準拠が前提条件となる事業機会を開拓するための道が開けた

WINDRIVER

ウインドリバー株式会社

〒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

www.windriver.com/japan

ウインドリバーは、ミッションクリティカルなインテリジェントシステム向けのソフトウェアを提供する世界的なリーダーです。40年以上にわたり、イノベーターかつパイオニアとして、最高レベルのセキュリティ、安全性、信頼性を数十億台を超えるデバイスやシステムに提供しています。ウインドリバーのソフトウェアと専門性の高い包括的なポートフォリオは、あらゆる業界のデジタルトランスフォーメーションを加速させています。