Vdoo securing the connected everything

Vdoo による UNECE WP.29 自動車サイバーセキュリティ コンプライアンスの加速

ソリューションの概要

japan_info@vdoo.com

https://www.vdoo.jp

自動車サイバー・セキュリティへの注目

デジタル化、接続性、自動化の普及により、自動車業界は技術的な変化の大きな波を受けています。技術の発展により OEM は自動車を継続的に進化させ、新しい機能を追加し、新たなサービスを実現し、リコールの件数を減らすことができます。しかし一方で、車内に搭載され外部のシステムと通信する接続型コンポーネントの急増により、データのプライバシーや身体的な安全性に悪影響を及ぼしかねない新たなサイバーセキュリティのリスクが生まれているのも事実です。

このようなサイバーリスクの増加に対応するため、自動車のサイバーセキュリティに関する基準や規制が導入され始めています。その中でも最も重要なのが、2020 年半ばに国連欧州経済委員会（UNECE）WP.29 により採用された、2 つの新しいサイバーセキュリティ関連規制です。

UNECE WP.29 規制

UNECE 自動車基準調和世界フォーラム（WP.29）には、自動車、自動車のサブシステム、部品の安全性と環境性能に関する規制を確立する法的権限があります。WP.29 には、車両の自動化や接続型の車両、サイバーセキュリティ、無線アップデートを扱うサブグループや特別委員会があります。

最も新しく、2021 年 1 月に施行されたこの 2 つの規制には、自動車メーカーのサイバーセキュリティ管理とソフトウェアアップデートに関する要件が定められています。

- **サイバーセキュリティおよびサイバーセキュリティ管理システムに関する国連規制**
（ECE/TRANS/WP.29/2020/79）には、車両に影響を与える可能性があるサイバーセキュリティの脅威および脆弱性と、そのようなリスクを解決するための措置が記されています。また、技術仕様に加えて、OEM 各社がそれぞれの型式の車両の規制への準拠を確認するために従うことが義務付けられた、正式な承認プロセスも定められています。

- **ソフトウェアアップデートおよびソフトウェアアップデート管理システムに関する国連規制**
（ECE/TRANS/WP.29/2020/80）は、ソフトウェアアップデートのドキュメントや品質保証に関するより全般的な規制で、技術的なソフトウェアアップデートプロセスに関連する技術的なサイバーセキュリティ要件もいくつか定められています。

この資料には、Vdoo による自動車メーカーのサイバーセキュリティおよびサイバーセキュリティ管理システムに関する国連規制へのコンプライアンスのサポートについて解説されています。

Vdoo による車両のサイバーセキュリティリスクの管理

自動車 OEM はセキュリティ体制を管理し規制要件に従うために、さまざまな型式や複雑なサプライチェーンにまたがる多数の接続型車載コンポーネントおよびシステムのセキュリティを確保する必要があります。

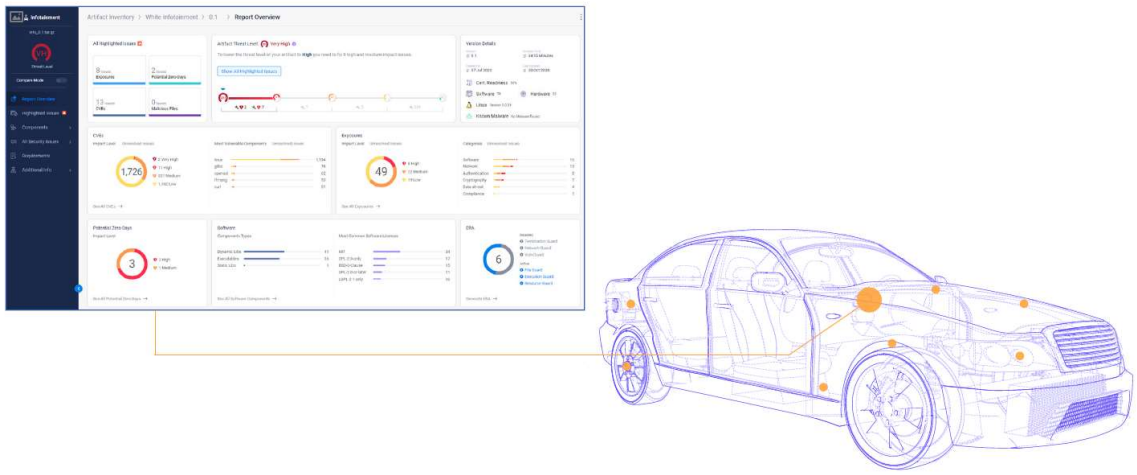
Vdoo の自動製品セキュリティプラットフォームにより、自動車メーカーは車両のサイバーセキュリティリスクを効率的かつ大規模に管理できます。Vdoo プラットフォームは、生産前と生産後の両方で潜在的なリスクを把握し、車両のすべての ECU のセキュリティを確保するためのさまざまな機能を提供し、車両の電子システムをサイバー脅威から守ります。これらの機能には、自動セキュリティ分析と影響評価、問題解決ガイダンス、継続的な脆弱性の監視、ランタイム保護などがあります。

また、自動プラットフォームに加え、Vdoo は自動車のコンポーネントやシステムのセキュリティアーキテクチャ、脅威・リスク評価（TARA）など、自動車メーカーの製品セキュリティのニーズをサポートする追加サービスも提供しています。

Vdoo の製品とサービスは、ソフトウェアアーキテクチャと脆弱性調査、リバースエンジニアリング、バイナリーコード分析における世界的な専門家で構成された Vdoo チームの、豊富な経験に基づき開発されています。

Vdoo のメリット

- 多様なコンポーネントのセキュリティを迅速かつ自動的に分析
- ソースコードにアクセスすることなく他社製ソフトウェアコンポーネントを完全に可視化
- 既知の脆弱性、マルウェア、セキュリティ保護されていない構成などのセキュリティリスク、ゼロデイ攻撃の可能性を包括的に検出
- 実際にリスクのあるセキュリティの問題を優先し、明確な解決ガイダンスで効果的に対処
- あらゆるコンポーネントに対する継続的な脆弱性監視・管理機能
- 生産中・生産後の新たな脅威を迅速に特定し、優先順位を付け、対応



自動製品セキュリティ機能

Vdoo プラットフォームは、開発から生産、生産後まで、製品のライフサイクル全体を通してセキュリティプロセスを自動化します。自動セキュリティ分析機能により、侵入テスト、ファジング、コンプライアンステスト、セキュリティ強化など、従来手作業で行われ、製品セキュリティの豊富な専門知識を必要とし、多くのリソースを消費する作業を、迅速かつ効率的に実行できます。

Vdoo は製品のソフトウェアをバイナリー形式で分析することで、攻撃者のアプローチやテクニックを模倣し、セキュリティのギャップを発見しそれらに優先順位を付け、実際にサイバーセキュリティリスクとなる問題から順に対処できます。Vdoo は、開発中にソースコードレベルでソフトウェアを検査するのでは検出できない脆弱性やセキュリティリスクに関する、包括的な情報を提供します。バイナリー分析は他社製のバイナリーに加え自社開発のソフトウェアにも利用できるため、ベンダーに提供される情報に頼らず、ソースコードにアクセスせずに、ソフトウェアサプライチェーンを含む製品全体のセキュリティ分析が可能になります。最後に、このアプローチでは製品全体のコンテキストで個々の問題をインテリジェントに分析できるため、より正確なリスク評価、優先順位付け、解決が可能になります。

ソフトウェア構成分析

Vision は完全なセキュリティ分析の前に、ソフトウェア構成分析 (SCA) を行い、分析されたソフトウェアの詳細な BOM を提供します。BOM にはオープンソースコンポーネントとそれぞれのライセンス、CVE の情報が含まれています。このシステムは CVE と CVSS スコアを提供するだけでなく、詳細なセキュリティテストを行うため、メーカーは実際のシナリオで重要となる、影響力が強く悪用される可能性が高い CVE の修正に集中できます。

セキュリティ監査

構成分析の後、プラットフォームが自動的にセキュリティ監査を行い、分析されたバイナリーのセキュリティリスクを検出します。検出されるリスクには、セキュリティ上の欠陥 (コンパイラのセキュリティフラグの欠如など)、安全でない構成 (セキュリティで保護されていないアクセス権限など)、脆弱な認証、脆弱な暗号化スキームなど、さまざまなものがあります。

ゼロデイ検出

さらに、ソフトウェアの自動詳細分析では、メモリーの破損やコマンドインジェクションなどのゼロデイ攻撃への脆弱性も検出されます。このプラットフォームは高度な分析手法を組み合わせ、詳細な静的解析、ファジング、記号実行、データフロー分析などの脆弱性を検出・検証します。

解決ガイダンス

Vdoo は特定されたそれぞれの問題に対して、コスト効率の高い方法で問題を解決または緩和するための、包括的な手順を提示します。これらのガイダンスは開発者や製品セキュリティアーキテクト、研究者のニーズに合わせて作成されており、コード内の特定の発見事項に対するステップバイステップの解決手順から、問題をより深く理解するための背景やコンテキストが解説された詳細記事まで、さまざまなものがあります。

コンプライアンス検証

Vdoo はコンプライアンス対策が容易に素早く行えるよう、何十種類もの最新の業界基準に対するセキュリティリスクのマッピングも提供します。特定されたリスクの一覧は、WP.29 サイバーセキュリティ規制などの特定の標準に従ってフィルタリングできます。これにより、コンプライアンスを達成するために修正が必要なセキュリティギャップを簡単に把握できます。

継続的な脆弱性監視

Vdoo は、新たに公開されたエクスプロイトや攻撃方法により、以前分析された製品に新たな CVE が発生していないか、既存の CVE によるリスクレベルが上がっていないかを、継続的に監視することができます。Vdoo は最新情報を追跡し、セキュリティ分析の段階で収集されたソフトウェア構成情報に基づいてその情報を影響がある製品に関連付けます。これにより、新しい脅威が発見された際の優先順位付けと対応が迅速かつ容易に行えます。

ランタイム保護とセキュリティ監視

分析結果に基づき、Vdoo はフットプリントが小さく、カスタマイズされたランタイムセキュリティエージェントを自動的に作成します。このエージェントを製品に統合することで、既知の脅威と未知の脅威の両方に対する予防的なリアルタイム

の保護が可能になり、導入済みのアセットをリアルタイムで監視するためのセキュリティアラートも利用できるようになります。

Vdoo による WP.29 規制へのコンプライアンスのサポート

サイバーセキュリティおよびサイバーセキュリティ管理システムに関する国連規制では、自動車メーカーによるサイバーセキュリティ管理システム（CSMS）の導入と、CSMS が規制に定められた仕様に準拠していることを確認する正式な認定の取得が義務付けられています。

型式承認を得るために、メーカーは対象の型式に関連し規制に従った CSMS を導入し、車両のサイバーセキュリティに対する適切な対策を講じていることを証明する必要があります。

Vdoo は、この規制における CSMS の機能に関するセクションへのコンプライアンスをサポートします。これらのセクションには CSMS の仕様（第 7 項）、型式承認に必要なサイバーセキュリティ対策が導入されていることの確認（第 5 項）、および CSMS の対象となる自動車におけるサイバーセキュリティの脅威とそれらの解決（付属書 5）が定められています。

	Security Analysis	Vulnerability Monitoring	Risk Mitigation	Runtime Protection	Real Time Security Monitoring
Section 5 Approval	✓	✓			
Section 7 Specifications	✓	✓	✓	✓	✓
Annex 5A Threats	✓	✓	✓		
Annex 5B+5C Mitigations	✓	✓	✓	✓	✓

第 5 項: 承認

WP.29 規制の第 5 項には、承認機関が対象の型式のサイバーセキュリティに関して型式承認を与える条件が定められています。その要件の 1 つに、自動車メーカーが必要なサイバーセキュリティ対策を導入したことの書類とテストによる確認があり、次のような項目が対象となります。

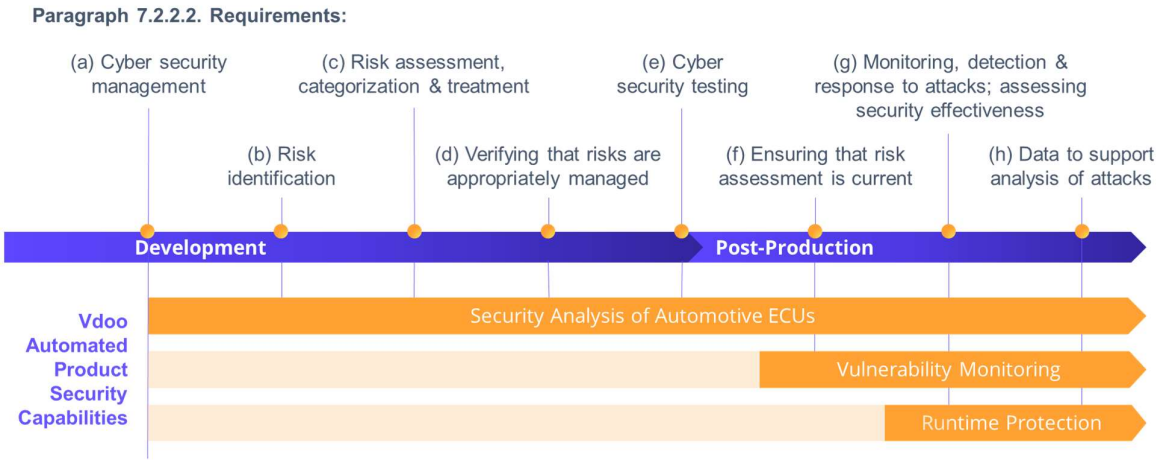
- サプライチェーンからの情報の収集と検証
- リスクの評価と対策
- セキュアな設計
- 攻撃の検出と対応
- 攻撃の検出とフォレンジック分析をサポートするデータの記録

Vdoo はリスク評価、検出されたセキュリティの問題、それらが解決されたかどうかなどのセキュリティ分析の結果を記録した詳細なドキュメントを提供することで、承認要件へのコンプライアンスをサポートします。サプライヤーからバイナリー形式で提供されたソフトウェアの自動セキュリティ分析は、特にサプライチェーンのセキュリティ情報の検証に役立ちます。

第 7 項: 仕様

CSMS の仕様は、規制の第 7.2 項に定められています。CSMS は開発から生産後まで、車両のライフサイクルの全段階に適用することが義務付けられています。さらにこの規制には、CSMS がこれらの段階全体でサポートする必要があるプロセス（第 7.2.2.2 項）も指定されており、それらのプロセスが付属書 5 に記載されているサイバー脅威とそれらの解決手段に対応したものであることも要件として定められています。

下図とその下に記された詳細の通り、Vdoo は自動車メーカーに義務付けられている CSMS プロセスへのコンプライアンスを実現します（アルファベットは規制の第 7.2.2.2 項のものと一致しています）。



(a) サイバーセキュリティ管理

Vdoo は、適切なサイバーセキュリティ管理を保証する手段として、車両のライフサイクル全体にわたり自動セキュリティ分析、脆弱性監視、ランタイム保護機能をシームレスに統合できるようにすることで、自動車メーカーのサイバーセキュリティ管理をサポートします。たとえば、自動セキュリティ分析スキャンを継続的な統合・継続的な開発（CI/CD）ワークフローに取り入れることで、メーカーが要修正と定義したセキュリティの問題が開発段階で解決されていることを確認できます。

(b) リスクの特定

Vdoo は車両の ECU の自動分析を行い、脆弱なソフトウェアコンポーネント、安全ではない接続構成、その他のセキュリティの問題から生じるサイバーセキュリティリスクを特定できます。分析は、自動分析用の ECU ソフトウェアイメージをアップロードすることで簡単に開始できます。Vdoo プラットフォームは、詳細なソフトウェア部品表（BOM）を素早く作成し、分析されたそれぞれのイメージのセキュリティギャップを包括的に表示します。

Vdoo はソースコードではなくバイナリー形式で製品のソフトウェアイメージを分析するため、OEM がベンダーから提供される情報のみに頼ることなく、サプライチェーンから提供された ECU ソフトウェアを独自に分析することができます。

さらに、Vdoo はより広範な車両レベルおよびシステムレベルのセキュリティ分析を行うために、Vdoo 自動プラットフォームからの詳細なセキュリティ情報と Vdoo のセキュリティチームの豊富な経験を活用した、脅威分析・リスク評価（TARA）を追加サービスとして提供しています。

(c) リスクの評価、分類、対策

Vdoo は自動分析により、完全なセキュリティ情報（CVE、リスク、ゼロデイ攻撃の可能性など）を数分で提供します。また、セキュリティ問題のインテリジェントな評価と優先順位、複数の基準に基づく分類、問題を迅速かつ最も効率的に解決するためのステップバイステップの実用的なガイダンスも提供します。

特定されたセキュリティ問題のリスクは、公開されている攻撃方法、特定の製品の構成および特性を考慮した悪用の可能性の有無、悪用の容易性など、複数の要素に基づき評価されます。これにより、さらに正確な優先順位に基づき、実際にリスクがある問題に効率的に対処できるようになります。

(d) リスクが適切に管理されていることの確認

分析は自動で行われるため、OEM は新しいソフトウェアバージョンに対して簡単に繰り返しスキャンを行い、問題が適切に対処されていて、新たな脅威が生まれていないことを確認できます。

(e) サイバーセキュリティテスト

Vdoo プラットフォームは ECU の自動サイバーセキュリティテストを行い、その結果をさまざまな形式 (CSV、PDF、API) でエクスポートしテストの証拠を提供することで、コンプライアンスをサポートします。

(f) 最新のリスク評価の維持

Vdoo は、以前分析されたすべてのソフトウェアイメージの脆弱性を継続的に監視します。また、ソフトウェアコンポーネントに関する新たに公開された脆弱性も、Vdoo の豊富な知識ベースを活用して追跡し、監視します。分析時に収集されたソフトウェア構成情報により、新たな脆弱性が発見されるとすぐに影響を受ける ECU や型式を把握できます。これにより、リスク評価を常に最新のものに保つことができます。

さらに、以前に分析したソフトウェアの更新バージョンを分析して、新たなサイバー脅威や脆弱性が発生していないことを確認することもできます。

(g) 攻撃の監視、検出、対応、およびセキュリティ効果の継続性評価

Vdoo の埋め込み型ランタイム保護エージェントを車載 ECU に統合することで、デバイスへのサイバー攻撃をリアルタイムで監視、検出、防止できます。

脆弱性の監視と繰り返しの分析により、新たなサイバー脅威を確実に特定し、セキュリティ対策の必要性を評価できます。

(h) データによる攻撃の分析のサポート

Vdoo は、攻撃が発生した際に分析をサポートするための豊富なセキュリティデータを提供します。提供されるデータには、分析されたすべての ECU に検出された脆弱性およびセキュリティリスクに関する包括的な情報や、埋め込み型のランタイムエージェントによって収集されたランタイムセキュリティデータのログなどが含まれています。

付属書 5: 脅威とそれぞれに対する解決手段のリスト

付属書 5 には、自動車メーカーが考慮する必要のあるサイバー脅威の包括的なリストと、それらの脅威から保護するために導入が義務付けられている解決手段が記載されています。

Vdoo プラットフォームは、この規制の付属書 5 に記載されている脅威に対する解決手段が導入されていることを自動的に検証します。分析が行われたそれぞれの ECU ソフトウェアイメージに対して、検出されたセキュリティリスクのリストを提供し、それぞれのリスクは付属書 5 の関連部分に詳細にマッピングされています。

たとえば、暗号化キーとアルゴリズム、データの暗号化、ユーザーアクセス構成、ソフトウェアアップデートプロセスなどに関するセキュリティリスクなどが検出されます。

さらに、Vdoo プラットフォームはソフトウェアのセキュリティ評価、マルウェア検出、不正アクセスの検出と防止、整合性保護など、同付属書に記載されている対策機能も提供します。

Vdoo について

Vdoo は自動デバイスセキュリティプラットフォームを提供し、企業による IoT、接続型、埋め込み型デバイスの、開発から導入後までを網羅した最善のセキュリティの迅速かつ大規模な実現をサポートしています。Vdoo は、サイバーセキュリティ企業の Cyvera 社を Palo Alto Networks 社に売却し、エンドポイントおよび埋め込み型システムのセキュリティに関する豊富な知識を持ちあわせた数人の起業家によって設立されました。Vdoo は、83North、Dell、WRVI、GGV、NTT ドコモ、MS&AD 各社をはじめとするトップレベルの投資　　家の支援を受けています。Vdoo は米国、ヨーロッパ、日本、イスラエルにオフィスを構え、世界的に有名な多数のお客様にご利用いただいています。

詳細につきましては、japan_info@vdoo.com にお問い合わせいただくか、弊社ウェブサイト https://www.vdoo.jp をご覧ください。