自動車サイバーセキュリティの全貌

セキュリティ対策への取り組みが生み出す
ビジネスチャンスと展望

Empowering Tomorrow's Automotive Software
www.etas.com

ETAS

概要

自動車がライフサイクル全体を通して、外部ネットワークとつながることが“あたりまえ”の時代になっています。自動車のデジタル化とカーコネクティビティの進化により、インターネット接続やOTA（無線）によるアップデートが普及し、さらには車両とインフラ間（V2I）通信（路車間通信）が瞬時に行われるようになっています。さらには、これらの進化に伴う課題への取り組みが、車両の信頼性向上、道路利用者の安全確保、およびプライバシー保護の基盤となる堅牢なサイバーセキュリティフレームワークの構築にもつながっています。実際、サイバーセキュリティは、モビリティエコシステムにおける新たなビジネスモデルの創出につながるビジネスチャンスをもたらします。

サイバーセキュリティ対策は、開発・製造プロセスからコネクテッドモビリティネットワーク内での相互作用に至るまで、車両のライフサイクル全体を通して必要不可欠です。リモートアップデート、スマートフォンとの連携、充電スタンドのシームレスな登録といった新機能が標準となるにつれて、これらのイノベーションにおけるセキュリティ確保がますます重要になってきます。開発者は、潜在的なリスクを常に先回りして洗い出し、ビークルエコシステムを継続的に強化することで、ユーザーが最先端技術の恩恵を十分に享受できるようにする必要があります。こうしたサイバーセキュリティへの「取り組みの進化」によって、車両開発におけるイノベーションや車両特性の最適化が促進されます。

このホワイトペーパーは、自動車サイバーセキュリティのダイナミックな世界をナビゲートする戦略ガイドになります。自動車メーカーが直面している主要な課題とビジネス機会を特定し、電子制御ユニット（ECU）に組み込まれたソフトウェアからビークルコンピューターまで、車両のライフサイクルと業界を取り巻くビジネス環境全体を見据えた包括的な視点を提示します。従来のメーカー、サプライヤー、ソフトウェア主導のスタートアップ企業のいずれであっても、サイバーセキュリティの確保は戦略的な優位性をもたらします。従来の開発プロセスを見直すことで、広範囲にわたる最適化のための大きな可能性を引き出すことができます。また、本書では4つの主要なセキュリティ原則を適用することで、DevSecOpsやVモデルといった開発アプローチを強化する方法を探り、安全で革新的な未来の自動車ソフトウェア開発を実現するためのロードマップを示します。

目次

1. はじめに

デジタル化は、OTA（無線）によるソフトウェアアップデート、先進運転支援システム（ADAS）、インターネット対応のエンターテインメントシステムなどを通じて、車両の使い勝手の良さや利便性を高めています。これによって、製造業者やサプライヤーは、ハード面での物理的な変化とは異なる、ユニークなイノベーションを生み出しています。アフターサービス領域での新たなビジネス展開など、自動車のライフサイクル全体にわたる継続的な収益確保に向けた「サービスモデル」の開発も進んでいます。技術的ブレイクスルーは、新たなビジネスチャンスをもたらします。今や自動車は、機械式と呼ばれる物理的な仕組みからコンピューターを搭載した「車輪の付いたコンピューター」（スマートカー）へと進化しています。それに伴い、サイバーセキュリティの領域では、新たな課題が次々と出現しています。成長とイノベーションの過程では、機密性の高い個人データを保護し、車両モデル全体を潜在的なサイバー攻撃から守る責任も生じます。これらのリスクを先読みし積極的に対処することで、メーカーはより強力でレジリエントな（復元力のある）システムを構築し、デジタル化が進む自動車業界において長期的な成功と信頼の基盤を築くことができます。

自動車のデジタル化におけるサイバーセキュリティの確保は、モビリティ領域における重要なトピックの1つです。最近の市場調査[1]によると、サイバーセキュリティのリスクは、自動車メーカーの成長を阻害する最大の外的要因として認識されています。業界内のこの高い意識は、概して積極的かつ前向きな姿勢を生み出しています。新しいリスクが認識され、それらに対処し管理するためのアプローチの開発も進んでいます。これは、OEM（自動車メーカー）に限った懸念事項ではありません。現代のクルマは、車載／非車載を問わず、さまざまなソフトウェアおよびハードウェアコンポーネントの相互作用によって機能しています。これを支えているのが、開発から運用に至るまでの安全性の確保に寄与しているサプライヤーおよびソフトウェア主導企業のグローバルネットワークです。サプライチェーン内のすべての企業が、脅威の現状を認識し、リスクを最小限に抑え、必要なすべての規制を遵守し、車両の包括的なセキュリティに貢献する責任を負っています。

サイバーセキュリティの強化は、業界の自発的な努力だけで進んでいるわけではありません。さまざまな法規制や標準が、包括的なサイバーセキュリティの指針を示し、特に道路利用者の安全を維持するために整備されています。こうした動きもサイバーセキュリティの強化に影響しています。特定の脅威領域を深く掘り下げ課題を浮き彫りにするには、自動車サイバーセキュリティ法規制の現状を正確かつ明確に把握することが大切です。

2.　自動車サイバーセキュリティの規制状況

自動車メーカーとサプライヤーの多くが、複数の国や地域で製品を販売しています。そのため、ソフトウェアや部品、車両を輸出する市場のすべての規制を把握し、遵守する必要があります。こうした規制は絶えず変化しており、サイバーセキュリティの脅威が拡大するにつれて、新しい要件が追加されています。法規制に加え、業界共通の標準やベストプラクティスも重要な役割を果たしています。こうした標準への準拠は強く推奨され、義務付けられている場合もあります。グローバル化が進むにつれ、モビリティを取り巻く環境は複雑さを増しており、自動車業界の企業にとって重要な課題となっています。図1に示すように、自動車メーカーには、乱立し変化し続ける複雑な法規制への対応が求められています。

国連欧州経済委員会（UNECE）の56の加盟国に製品を販売する自動車メーカーにとって、2021年に発効された国連の協定規則UN-R 155は、法的拘束力のある最も重要な規制です。現在、この規則は、乗用車、バス、トラック、トレーラーを対象としています。この規則は、サイバーセキュリティマネジメントシステム（CSMS）の導入を義務付けており、ガイドラインとして「ISO/SAE 21434：自動車のサイバーセキュリティエンジニアリングに関する国際標準規格」を参照しています。近い将来、この規制はオートバイやスクーターにも拡大され適用される可能性があり、これらの業界においてもサイバーセキュリティ対策が求められることになります。中国、米国、インドもそれぞれ独自の法規制を設けています。そのため、グローバル自動車市場向けの車両モデルは、同時に複数の標準を満たすか、販売地域ごとに仕様の変更を迫られるかもしれません。

新たな義務規制の導入は、道路利用者の高い安全性を確保する一方で、業界のOEMやサプライヤーに重大な経済的影響を及ぼす可能性があります。すでに開発された一部の車両モデルは、法的拘束力のある新しい規制の枠組みに準拠するために再設計が必要になるかもしれません。その結果、ポルシェ718 Boxter[2]やフォルクスワーゲンup![3]のようにモデル全体が生産終了になったり、一部の国でしか販売できなくなったりする可能性もあります。これらの事例は、サイバーセキュリティに適切に対処するには、現在の規制を厳格に遵守するだけでなく、組織全体に柔軟性と将来的な展望が必要になることを示しています。したがって、変化し続ける環境で競争力を維持するには、主要なサイバーセキュリティの脅威を理解することが不可欠です。しかし、こうした複雑な環境に単独で対処する必要はありません。経験豊富で国際的な実績のあるパートナーが、必要なサポートとツールを提供するため、その都度ゼロから始める手間を省けます。

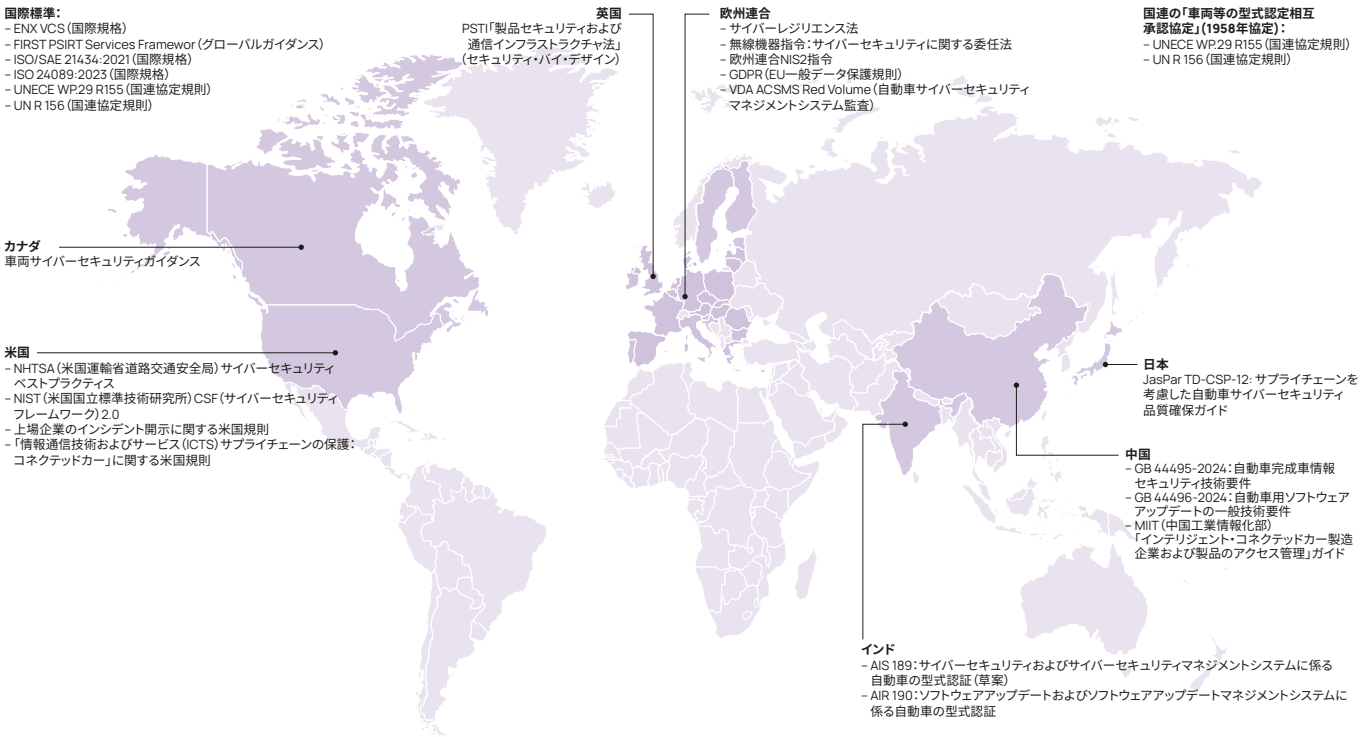

図1：コネクテッドデバイスのサイバーセキュリティ規制

3.　主要なサイバーセキュリティの脅威 – 概要

ETASは、自動車セキュリティ分野を牽引するソリューションプロバイダーとして、世界中のお客様から高い評価を受けています。多くのユースケースを創出するとともに、自動車業界の動向を常に把握しています。積み重ねてきた豊富な実績と経験をベースとして、ETASは3つの主要な脅威領域を特定しました。1つ目は、コンポーネント／アーキテクチャレベルの脆弱性とリスク、2つ目は複雑なサプライチェーンとアフターサービスがもたらすリスクとサイバーセキュリティの課題です。そして3つ目は、拡大するエコシステムに起因する課題です。自動車メーカーとサプライヤーは、最終製品で包括的なサイバーセキュリティを実現するために、これらの脅威を認識し、早い段階で対処する必要があります。

THREAT #1

3.1　コンポーネント／アーキテクチャレベルのソフトウェア脆弱性

まず、ECUから見てみましょう。車載ECUは、自動車のさまざまな機能において「頭脳」としての重要な役割を担っています。自動車の安全性にとっても、不可欠なコンポーネントです。1台の車両には最大で150個のECUが搭載され、優れたリアルタイム処理機能によって、エンジンの動作、排気、変速、ブレーキシステムを監視し、制御しています。ECUは入力に即座に反応し、あらゆる状況で運転者の安全を確保します。そのため、ソフトウェアデファインドビークル（SDV）への移行が進むとしても、ECUは将来のE/Eアーキテクチャで重要な要素であり続けるはずです。

ECUは車両の安全性を担うプロセスに関わっています。攻撃の手口は進化を続けており、ECUが外部から改変されれば、新たなリスクが発生します。たとえば、外部からCANバスにアクセスされ、車両の機能全体をハイジャックされたり、プログラムが脆弱な認証プロセス（隠蔽によるセキュリティ）を悪用されたりするかもしれません。攻撃者は、インターネット接続を介してシステムが更新されるデジタルな経路を悪用できるため、車両の近くにいる必要もありません。

車両のECUは、運転者の安全、快適性、車両の性能を支える中心的な役割を担っています。そのため、初期段階からあらゆる脅威を排除し、車両のライフサイクル全体で最新の認証プロセスを確保するには、ソフトウェア開発のすべてのフェーズをカバーするセキュリティコンセプトが重要になります。残念ながら、多くの場合、ECUソフトウェアは、サイバー脅威の急速な進化に対処できない、「無防備」で脆弱なレガシーシステムで開発されています。さらに、顧客の関心を惹く機能を早く開発することに重点が置かれているため、基本的なECUソフトウェアの改良は軽視されがちです。

新しいトレンドとして、複数のドメインをビークルコンピューターに統合する、ゾーン型アプローチへの移行（図2）が進んでいますが、これが新しいセキュリティの課題を生んでいます。この課題に対処するには、専用の仮想マシン、ハードウェアセキュリティモジュール、TEE（Trusted Execution Environments）、ファイアウォールシステム、侵入検知メカニズムを備えた多様で堅牢なセキュリティフレームワークが求められます。
この取り組みは、家電のアプリ開発と同じように、開発プロセスを大幅に簡略化するというビークルコンピューターの利点を最大限に活用するうえで不可欠です。

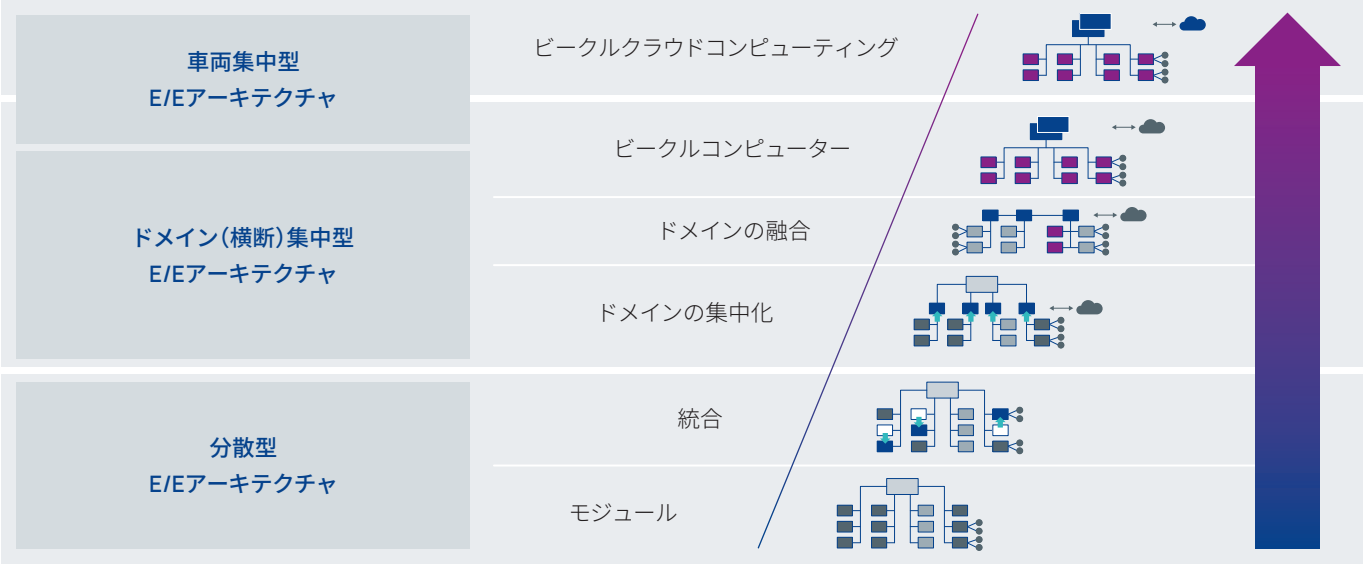

図2：分散型から集中型へと進化し続ける車両E/Eアーキテクチャ

THREAT #2

3.2 複雑なサプライチェーンとアフターサービスがもたらすサイバーセキュリティの課題

自動車のサプライチェーンは、多数のステークホルダー、契約業者、下請け業者、ソフトウェアプロバイダー、共有の開発プラットフォームが関わるきわめて複雑なエコシステムです。コンポーネントとシステムでは、サプライチェーンの早い段階から、アクセスと更新が可能であることが必須の条件になっています。こうしたシステムの防御が不十分な場合、攻撃の標的になり、マルウェアやデータ窃取の経路が増加します。最適なパートナーを選択し、パートナーがすべての標準に準拠し、契約上の義務を遵守しているかどうかを確認することが、第三者の脆弱性を減らし、エンドツーエンドのサイバーセキュリティを実現するうえで重要なステップになっています。

車両の利用が開始されると、OEMは最新の車両が備えているネットワーク接続機能を介して、ソフトウェアを更新することが可能になります。ソフトウェアの更新は、新たな脆弱性への迅速な対応や、追加の機能やアフターサービスの提供など、さまざまなユースケースできわめて重要です。こ実行方法がOTA、ケーブル、OBDスティックのいずれであっても、メーカーに更新義務が課されます。UN-R156は、ソフトウェアの更新が可能なすべてのコンポーネントに対して、適切なソフトウェア更新管理システム（SUMS）の確立を義務付けています。SUMSの機能は外部機関によって監査され、型式認証にはその証明書を提出する必要があります。この監査は3年ごとに実施されます。さらに、個別の更新が取得済みの型式認証に及ぼす影響の評価は、メーカーが責任を負っています。その結果、特定のコンポーネントを更新可能にすることも、メーカーにとって経済的な考慮事項になっています。しかし、全体としては、複雑なコンポーネントを通信可能にすることで得られる利点の方が、それによって増える手間を上回っています。たとえば、バグが発見されたときも、コストのかかるリコールを避けることができます。

OTA接続は、明らかに最もユーザーフレンドリーな方法です。整備工場でソフトウェアを手動で更新する必要がないため、多数の車両を管理している場合は大幅に時間を節約できます。OTAアップデートには、ソフトウェアOTA（SOTA）、ファームウェアOTA（FOTA）、OTAサービスプロビジョニング（OTASP）など、さまざまな種類があります。また、車両のテスト段階で利用されていた認証済みのソースとの間にも、多様な無線接続方法が存在します。セキュリティの観点では、いずれの接続方法も複数のレベルでシステムに侵入可能で、E/Eアーキテクチャのさまざまなコンポーネントをターゲットにすることができます。こうした無線接続の共通点は、不正なソフトウェアがシステムに侵入するための入口になり得るということです。

最近はメーカーの間で、車両ユーザーにさまざまな有料サービスを提供し、OTAインターフェースをデジタル収益源として利用する動きが広がっています。それに伴い、決済情報や利用情報もやり取りされるため、さらにセキュリティ対策が必要になります。しかし、OTAによるアクセスの最大のリスクは、機能やデータストレージのクラウドへの移行（ビークルクラウドコンピューティング）や（恒久的な）接続のセットアップなどによって、モバイルネットワークやWi-Fi、その他の無線接続を介して、外部のホストやプロバイダーと双方向接続が確立されることです。車内と車外の境界線がなくなることで、マルウェアの侵入やデータの抜き取りを可能にするさまざまな経路が新たに生まれます。部品メーカーにとっては、走行時の挙動、消耗や損傷、故障に関するデータは継続的な改善を可能にするために重要な意味を持ちますが、その一方で、データ転送の頻度が増えると、リスクも多くなります。ハッカーはあらゆる脆弱性を解析し、多数の実例から学習しています。

THREAT #3

3.3　進化を続けるコネクテッドエコシステムにおける課題

ここまでは、自動車メーカーとサプライヤーがセキュリティ管理で重要な役割を果たすシナリオを中心に見てきました。しかし、最新の車両は実際に利用が開始されると、無許可の整備工場での作業やユーザーによるアップデート（サードパーティソースの利用など）、充電スタンドや交通管理ステーションへの接続など、潜在的リスクを伴うさまざまな状況にさらされます。こうしたV2X（「車両」と「あらゆるモノ」）をつなげる通信接続の可能性（場合によっては義務）は、今後も増加し続けるでしょう。V2V（車両間通信）、V2I（車両とインフラストラクチャ間の通信）、V2P（車両と歩行者間の通信）、V2N（車両とネットワーク間の通信）は、自律（および準自律）走行車両の実現を支える基盤技術になるだけでなく、商業物流や公共交通を新しいレベルに引き上げることになります。

さらにモバイル通信やコンピューティング分野からソフトウェア企業の参入が増えることで、新しい動きが生まれます。これらのプロバイダーは、個人ユーザーやフリート向けにクラウドやデータストレージ、データ分析サービスを提供します。しかし、これらのサービスは、各国で異なるセキュリティ規制の下で運用されることもあるため、データ主権や不正使用のリスクについて重大な懸念も生じます。こうしたイノベーションの恩恵を受けながら、データの安全性を確保することは、自動車業界が発展し続けるうえできわめて重要です。

モビリティがすべてに接続するという未来が現実味を帯びているなか、新しい機能の実装とサイバーセキュリティ脅威の増加が密接に関連していることは明らかです。ライフサイクル、エコシステム、サプライチェーンという3つの領域（図3）でエンドツーエンドでコネクテッドモビリティを継続的に保護するには、さらなる取り組みが求められます。したがって、全体を見据えながら、現在の開発プロセスを抜本的に改革するときが来ています。

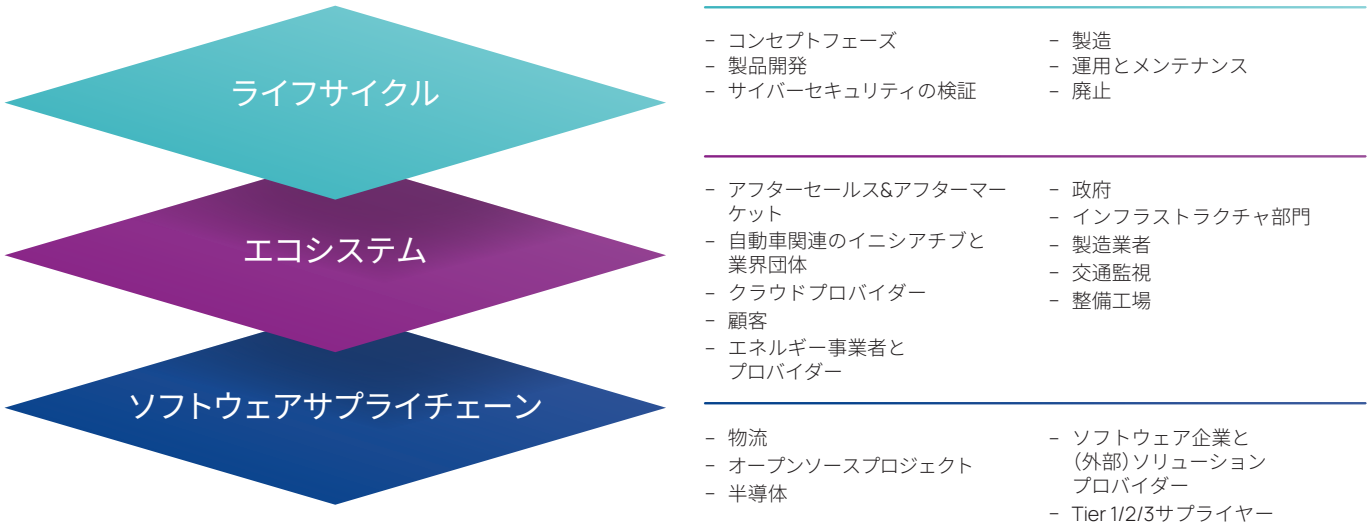

図3：現代の車両に影響を与えるあらゆる要素をカバーするライフサイクル、エコシステム、サプライチェーンの3領域

4.　DevSecOpsとVモデル：いずれのアプローチにもサイバーセキュリティの実装は不可欠

現代の車両は、板挟みの状態にあります。安全な運転を支えるために、多数の重要な車両機能が深く組み込まれている一方で、革新的なSDVアプリの需要に応えるために、ビークルコンピューターを基盤とするゾーン型アーキテクチャへの再構築が進んでいます。車両内で安全性に関わるドメインとそれ以外のドメインを完全に分離することはできません。多くの機能が両者の連携に依存しているからです。それにもかかわらず、車両ソフトウェアの開発では、Vモデル（図5）とDevOpsサイクル（図4）というまったく異なる2つの方法が採用されています。どちらの方法も、進化し続ける脅威と安全性およびセキュリティの法的要件に適応する必要があります。

ハードウェアとソフトウェアの密接な関係が（一部に）まだ存在しているため、車両に深く組み込まれた機能については、セキュリティを強化したVモデルが推奨されます。Vモデルでは、抽象度に応じてプロセスが明確に分離されています。開発の終了が明確で、特定の重要な機能を担うようにハードコードされた最終製品が完成します。

DevOpsサイクルは、安全性に関連しない機能に対応するモデルであり、量産開始以降も、運用を含めて、継続するソフトウェア開発プロセスとして設計されています。ETASでは、エンドツーエンドでセキュリティを確保するという新しい要件を完全に満たすために、DevOpsサイクルがDevSecOps（開発、セキュリティ、運用）サイクルに進化しています。DevSecOpsサイクルは、工程を大きく変更する必要はなく、第5章で紹介する4つのセキュリティ原則に従って、ツールの機能をアップグレードするだけで実装できます。

一般的に、Vモデルを「V-Secモデル」に移行する場合も、同様の変更が必要になります。開発プロセスの全段階でセキュリティを積極的に考慮するという前提に立って、要件仕様の段階からセキュリティ原則を導入する必要があります。そうすることで、必要な反復サイクルやアジャイルな開発プロセスをVモデルに取り込めるようになります。これはVモデルの基本概念と矛盾するものではありません。なぜなら、Vモデルは決して直線的なプロセスではないからです。モデルの抽象度は、検証および妥当性確認の各作業に整合している必要がありますが、その順序は変更可能です。各ステップにセキュリティを実装する必要があるということが基本方針になります。リソースに制限があるECUでは、これは簡単なことではありません。軽量で効率的なセキュリティプロトコルを採用し、パフォーマンスを損なうことなく、堅牢な保護を実現する必要があります。

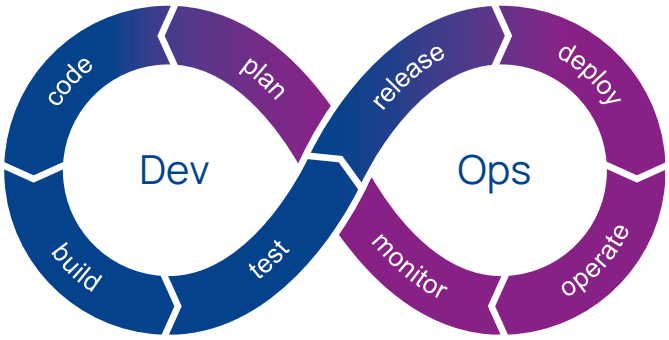

図4：車両ソフトウェア開発のDevOpsサイクル

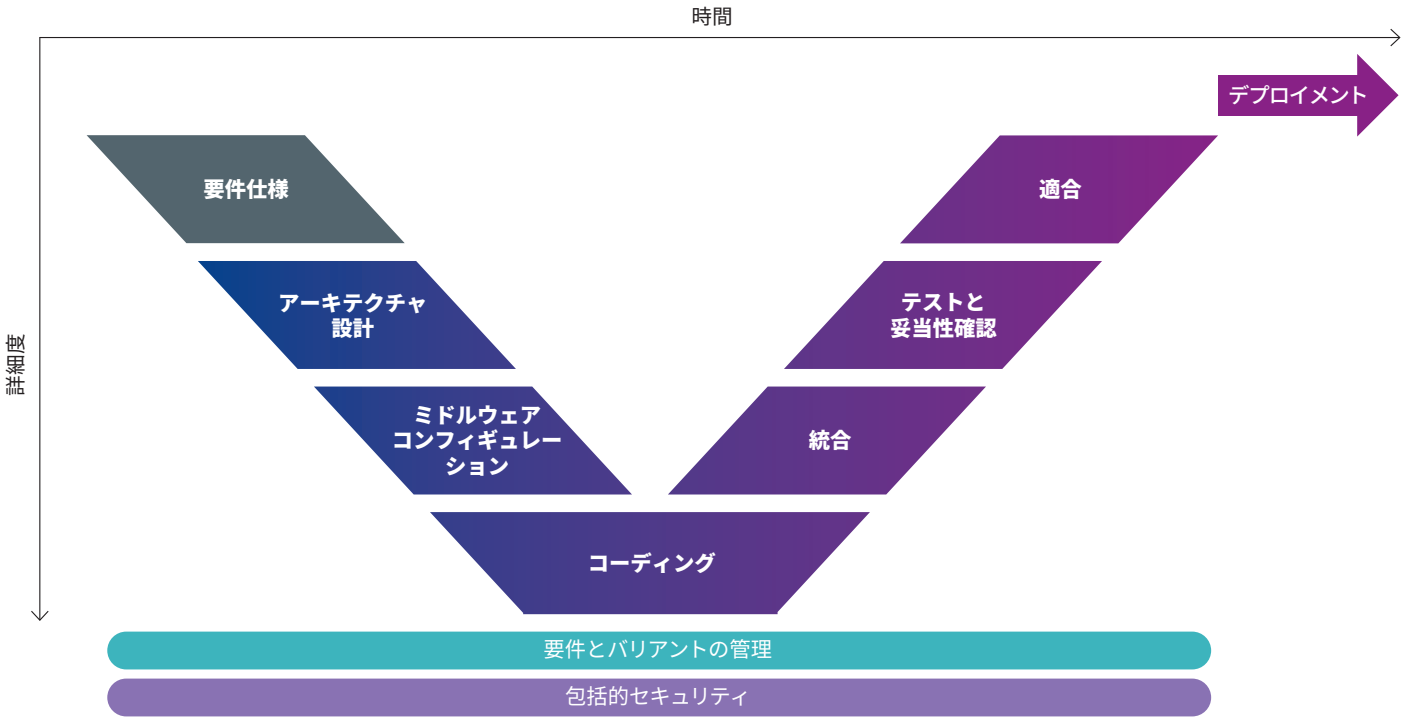

図5：ソフトウェア開発を2つの工程に分けるVモデル（ECUソフトウェア開発プロセスに適応したバージョン）

サイバーセキュリティを重視すると、図6のように最終的に2つの開発アプローチの融合が進むことになります。E/Eアーキテクチャがビークルコンピューターとシステムオンチップ(SoC)構成に移行し、クリティカルな機能と汎用的な機能の境界があいまいになっていくことを考えると、2つの開発アプローチの融合は不可欠です。たとえば、ブレーキシステムが、物体認識に連動して実行される高度な自動運転機能に組み込まれている場合、標準的なVモデルで求められる「完全な完了」に至ることは決してありません。そのため、V-Secモデルに運用(Ops)を追加し(またはDevSecOpsにVモデルの構造を導入し)、このクリティカルな機能を継続的に最適化できるようにする必要があります。4つのセキュリティ原則を導入することで、開発プロセスをセキュリティ要件に適応させながら、包括的なサイバーセキュリティ管理に移行できるようになります。

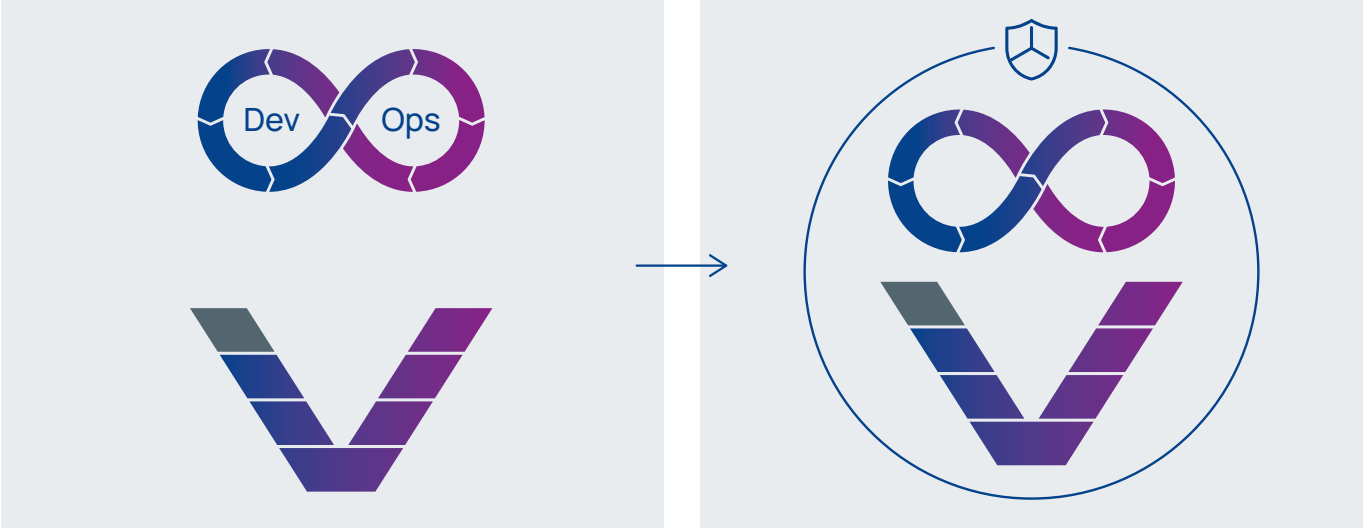

図6：VモデルとDevOpsサイクルのプロセス全体を通じたサイバーセキュリティの包括的な統合によって生じた両者のあいまいな境界

5.　4つのセキュリティ原則

変化の必要性を認識することと現実的な実装へのアプローチは、どちらもきわめて重要です。この戦略的なアプローチは、具体的なプロセスに変換できる要素に段階的に分解していく必要があります。その指針となるのが、4つのセキュリティ原則です。すなわち、セキュリティ・バイ・デザイン、多層防御、リスク管理と監視、そして組織的セキュリティです。これらは、エンドツーエンドのサイバーセキュリティを実現するために、ライフサイクル、エコシステム、ソフトウェアサプライチェーンの3つの側面に沿って高い成熟度レベルで適用し、活用することが重要です。これらの原則には、組織における製品セキュリティのプロセス、テクノロジー、情報、そして人材と企業文化といったあらゆる重要な要素が盛り込まれています。

5.1　原則1：セキュリティ・バイ・デザイン

セキュリティは、(法的な)安全規制の遵守や適切なセキュリティアーキテクチャの導入を含め、開発プロセスの最初期から各ステップで考慮されます。DevSecOpsでもVモデルでも、開発プロセス全体でセキュリティのあらゆる側面を常に考慮することで、プロジェクトの後工程や引き渡し後の手戻り作業で発生する高額なコストを回避できます。セキュリティ・バイ・デザインの原則に従って開発されたソフトウェアは、ライフサイクル全体にわたって堅牢で障害に強くなります。この原則を現在の脅威に応じて拡張することで、どの段階であっても脆弱性を最短の時間で修正できるようになります。

5.2　原則2：多層防衛

複数の防衛線を設けることで、1つが破られても直ちにセキュリティが危険にさらされることがなくなります。これが、多層防衛の基本的な考え方です。多数の防御メカニズムを構築しておけば、1か所が突破されてもシステム全体が侵害されることはありません。従来のE/Eアーキテクチャでは、車両に深く組み込まれたコンポーネントから最上層(車載ネットワーク)までの階層ごとにセキュリティを実装するアプローチが理想とされていました。また、ハードウェアベースの機能の分離と隔離も活用することができました。現在では、車両アーキテクチャの中央集約化とビークルクラウドコンピューティングの登場により、「仮想」レイヤーを追加して複雑性に対処する必要があります。その延長線上にあるのが、ゼロトラストセキュリティアプローチです。

5.3　原則3：リスク管理とモニタリング

潜在的なリスクが増えるなか、的確かつ包括的な管理が不可欠になっています。たとえば、脅威分析とリスク評価（TARA）の実施は、ISO/SAE 21434規格の主要コンポーネントです。これにより、メーカーやサプライヤーは潜在的な脅威を特定し、適切な保護対策を策定するための指針を得ることができます。脅威分析フェーズでは、車両に対するすべてのサイバーセキュリティ脅威が体系的に特定されます。その一環として、潜在的なサイバー攻撃のシナリオも評価され、適切な対策が講じられます。リスク評価フェーズでは、これらのリスクの優先順位が決定され、開発プロセスへの影響が分析されます。総合的な目標は、セキュリティ・バイ・デザインや多層防御の原則を一貫して適用することなどにより、可能な限り脅威レベルを低く保つことです。開かれたエコシステムと変化し続ける脅威についても再検討が必要です。従来の開発システムの多くは、継続的にリスクを評価、分析し、セキュリティギャップを埋めるための適切なツールとプロセスを欠いているためです。

5.4　原則4：組織全体で取り組むセキュリティ管理

サイバー攻撃に対する包括的な耐性を高めるには、組織全体の変革が必要です。特に重要なのが、関係者全員の意識改革です。複雑で進化し続ける脅威に対処するには、協力、柔軟性、コミュニケーション、さらに単なる「チェックリストの確認」にとどまらない積極的なサイバーセキュリティ意識が求められます。法的要件でも、組織的なセキュリティ体制を詳細に定めています。たとえば、UNECEの規定では、運用、リスク管理／コンプライアンス、内部監査を含む、包括的なCSMSを義務付けています。いわゆる「3つの防衛線」の枠組みに従うと、セキュリティ対策は個別の部署が扱う課題ではなく、すべてのプロセスで実行され、製品のライフサイクル全体が対象になります。組織的なセキュリティ体制の構築には、時間がかかり、調整も必要になります。組織とソフトウェアサプライチェーン内のすべてのステークホルダーも巻き込む場合はなおさらです。

6.　モビリティ専門家のガイダンスとソリューションを活用した複雑さの克服

脅威の現状認識や規制や標準の把握、4つの原則の理解など、理論的な知識を実践に活かすには、専門家のサポートが必要です。これまで述べてきたように、最新のサイバーセキュリティを実現するには、自動車メーカーとサプライヤーの開発、製造、アフターセールスのプロセスを根本的かつ包括的に再構成する必要があります。最終的には、ソフトウェアやハードウェアのソリューション、開発ツール、個別の手順を通じて、こうした考え方を日常業務に落とし込む必要があります。

たとえば、原則1と2に従って多層的なセキュリティアーキテクチャを採用する場合、最新の暗号化、認証、侵入検知、セキュアブートの仕組みを既存のシステムに組み込むことになります。これをゼロから構築するには、サイバーセキュリティ専用の部署が必要です。そのため、多くの企業が外部のサポートを利用して複雑さに対処すると同時に、時間とリソースを節約しています。このトレンドは、自動車サイバーセキュリティ市場の予測にも表れています。2024年から2031年までの年平均成長率（CAGR）は18.93%になると予想され、市場規模は2023年の78.3億ドルから2031年には313.4億ドル[4]に増加すると見込まれています（図7）。

しかし、外部のサイバーセキュリティソリューションの導入には、ベンダーロックイン、互換性、統合の難しさといった固有の課題もあります。そのため、個別の状況やレガシーシステムを考慮に入れた、包括的で将来を見据えたサイバーセキュリティ方針を作成するために、最適なパートナーを選択することがきわめて重要です。規制の遵守については、具体的で体系的なガイドラインが非常に重要です。法規制はどの企業にとっても同じく、かつ等しく適用されるため、独自に個別のソリューションを何度も開発する必要はありません。ETASは、サイバーセキュリティの効率を最適化する実証済みの戦略を活用し、ESCRYPT「製品セキュリティ組織フレームワーク（PROOF）」を開発しました。このフレームワークでは、お客様の成熟度に合わせて、原則4に基づくCSMSを8つのステップに従って構築できます。

ETASは、プロセスの最適化に重点的に取り組むだけでなく、ソフトウェアとハードウェアの両面でソリューションを提供できます。手作業を最小化するユーザーフレンドリーなツールや管理プラットフォームを含むポートフォリオは、高度な自動化機能を備え、精力的に開発が継続されています。ETASの製品ポートフォリオ（図8）は、セキュリティの設計、実装、管理に分類されているため、サイバーセキュリティソリューションに必要なサポートを個別に選択できます。

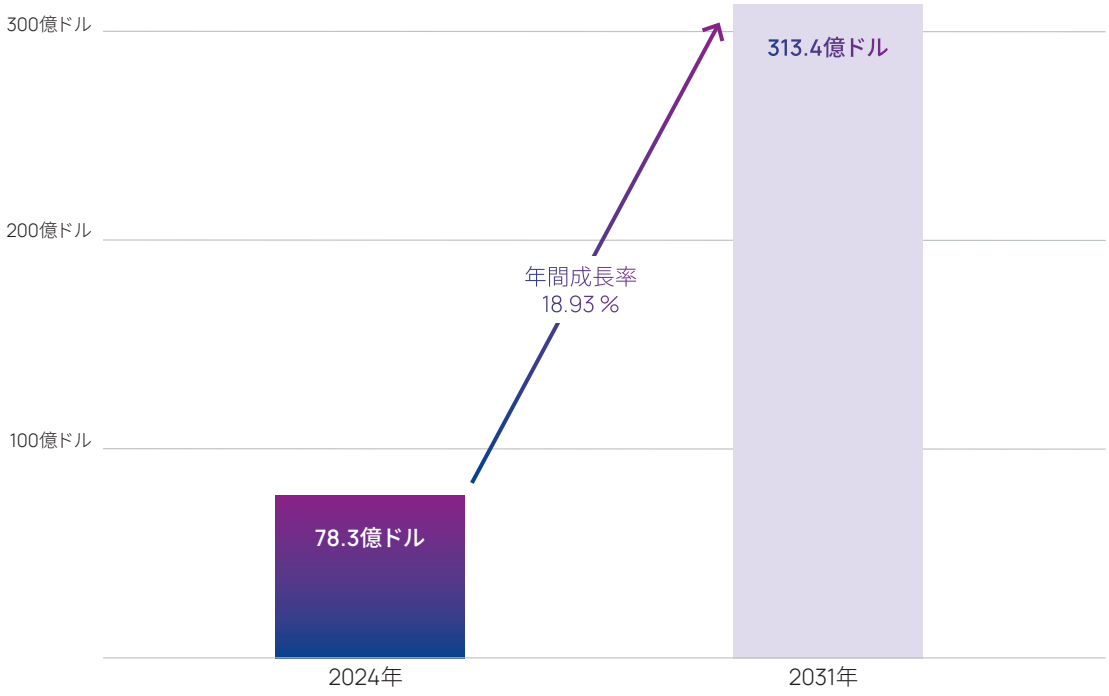

図7：自動車サイバーセキュリティの市場予測（2024 ～ 2031年）

セキュリティ設計

ETASは、ISO21434の準拠を目的とした「製品セキュリティ組織フレームワーク（PROOF）」、リスク管理のための各種セキュリティツール、およびペネトレーション／ファジングテストサービスを提供しています。

ESCRYPTのPROOFによるサイバーセキュリティマネジメントシステム
サイバーセキュリティの効率を最適化する実証済みの戦略

ESCRYPT CycurFUZZ
車載システム用スマートファジングツール

ESCRYPT CycurRISK
脅威分析とリスクアセスメントのためのソフトウェアツール

セキュリティ実装

ETASは、暗号鍵の漏洩や悪用を防止するための組み込みソフトウェア製品として、ハードウェアセキュリティモジュールやマイクコントローラーおよびビークルコンピューター（SoC）向けの暗号ライブラリを提供しています。さらに、データ改ざんや不正アクセスを防止する車載ファイアウォールのほか、さまざまな侵入検知/防止ソリューションもご用意しています。

ESCRYPT CycurHSM
ECU向けの強力なセキュリティソフトウェア

ESCRYPT CycurSoC
ソフトウェアデファインドビークル（SDV）の安全性と信頼性を実現

ESCRYPT CycurGATE
高性能な車載イーサネット/IPファイアウォール＆ルーター

セキュリティ管理

ETASは、世界中の車両フリートに統合型の侵入検知/防止サービスを提供しています。車載侵入検知システムによるセキュリティ管理、車両セキュリティオペレーションセンター（VSOC: Vehicle Security Operations Center）によるコネクテッドフリート全体のセキュリティ監視、OTA（無線）アップデートによる継続的なリスク管理を実現します。

ESCRYPT CycurIDS
CANおよびEthernetネットワーク向け組み込み型侵入検知システム

ESCRYPT脆弱性管理ソリューション
効果的なリスクベースの脆弱性管理によって製品セキュリティを強化

ESCRYPT車両セキュリティオペレーションセンター
車両フリートと車両バックエンドシステムからのイベントソースを統合するといった、車両フリートのニーズに合わせた管理型セキュリティサービス

ESCRYPT侵入検知・防御ソリューション
車両フリートの常時監視により増大するセキュリティ脅威を特定、専用のインシデントレスポンスを構築、ライフサイクル全体にわたり安定したセキュリティレベルを維持

図8：ETASの自動車サイバーセキュリティポートフォリオ：セキュリティの設計、実装、管理に分類

7. まとめ

サイバーセキュリティは、自動車業界の最重要課題の1つです。自動車のコネクテッド化が進むにつれ、その重要性は今後さらに高まっていきます。プロセスを包括的なサイバーセキュリティ戦略に適応させることは、決して面倒な義務ではなく、そのように捉えるべきでもありません。何よりもまず、自動車メーカーとサプライヤーの双方にとって、開発力と生産性を新たなレベルに引き上げ、これまでにないアフターサービスによって市場競争力を積極的に活用する絶好のビジネスチャンスと捉えることが重要です。ETASの「自動車サイバーセキュリティ成熟度レポート2024」[5]によると、成熟度レベルが高い企業ほど、競争の激しい今日の市場において自社が優位なポジションにあると認識しています。サイバーセキュリティの取り組みがどの段階であっても、あらゆる成熟度、サイバー脅威、規制要件に対して、ETASのようなパートナーがすでにソリューションを用意し、新しい対策を開発しています。ETASのサポートは、企業のプロセス全体の設計からECUやビークルコンピューター向けの具体的なソフトウェアソリューションまで多岐にわたります。サポートサービスやソリューションを一括購入することも、独自リソースの構築や維持に要する負担やコストを削減できる継続的なマネージドサービスとして利用することもできます。お客様との緊密なコラボレーションを通じて、サイバーセキュリティの課題をビジネスチャンスに変え、道路利用者の安全性を最高レベルで永続的に確保していくことが可能になります。

i ETASについて

ETAS GmbHは、1994年にボッシュ・グループの完全子会社として設立されました。現在では欧州、北米、南米、アジアの各国に拠点を構え、グローバルに事業を展開しています。

ETASは、ソフトウェアデファインドビークル(SDV)の実現に向け、ソフトウェア開発ソリューション、車両オペレーティングシステム(OS)、自動車用クラウドサービス、データ収集・処理ソリューション、顧客向け統合ソリューション、サイバーセキュリティといった分野で包括的なソリューションを提供しています。

自動車サイバーセキュリティの分野では、業界のパイオニアとして各種オンボードおよびオフボードソフトウェア製品を取り揃えているほか、お客様がサイバーセキュリティ関連の複雑さをコントロールし、サイバーリスクを軽減し、ビジネスの可能性を最大限に引き出すためのプロフェッショナルサービスも提供しています。

ETASの自動車セキュリティソリューションは、すでに世界中の何百万台もの車両システムに導入され、ソフトウェアデファインドビークルのサイバーセキュリティ標準を確立しています。

参考文献

1) Rockwell Automation、「9th Annual State of Smart Manufacturing Report: Automotive Edition」、https://www.rockwellautomation.com/content/dam/rockwell-automation/documents/pdf/campaigns/state-of-smart-2024-automotive/2024-state-of-smart-manufacturing-for-automotive.pdf（アクセス日：2024年11月10日）

2) Forbes、https://www.forbes.com/sites/michaelharley/2024/03/28/eu-cybersecurity-laws-kill-porsches-718-boxster-and-cayman-early/（アクセス日：2024年11月11日）

3) Automotive IT、https://www.automotiveit.eu/technology/volkswagen-streicht-modelle-wegen-cybersecurity-vorgaben-99-311.html（アクセス日：2024年11月11日）

4) Faist Group、https://www.faistgroup.com/news/growth-challenges-automotive-cybersecurity/（アクセス日：2024年11月11日）

5) ETAS Cyber Maturity Report、https://www.etas.com/download-center-files/DLC_products_ESCRYPT/etas-automotive-cyber-maturity-report-2024-en-20240719.pdf（アクセス日：2024年11月11日）

お問い合わせ先

Christian Schleiffer
LinkedIn
お気軽にお問い合わせください。
www.etas.com/wesecurethefuture

本書に記載されているすべての情報は一般的性質のものであり、特定の個人または団体の状況に対処することを意図したものではありません。当社は正確かつ最新の情報の提供に努めていますが、そのような情報を取得した時点での正確性や将来における継続的な正確性を保証することはできません。本書の情報に基づいて行動する場合は、専門家の適切な助言を受け、対象となる状況の事実を十分に調査してください。
© ETAS GmbH. All rights reserved.

最終更新：2024年12月