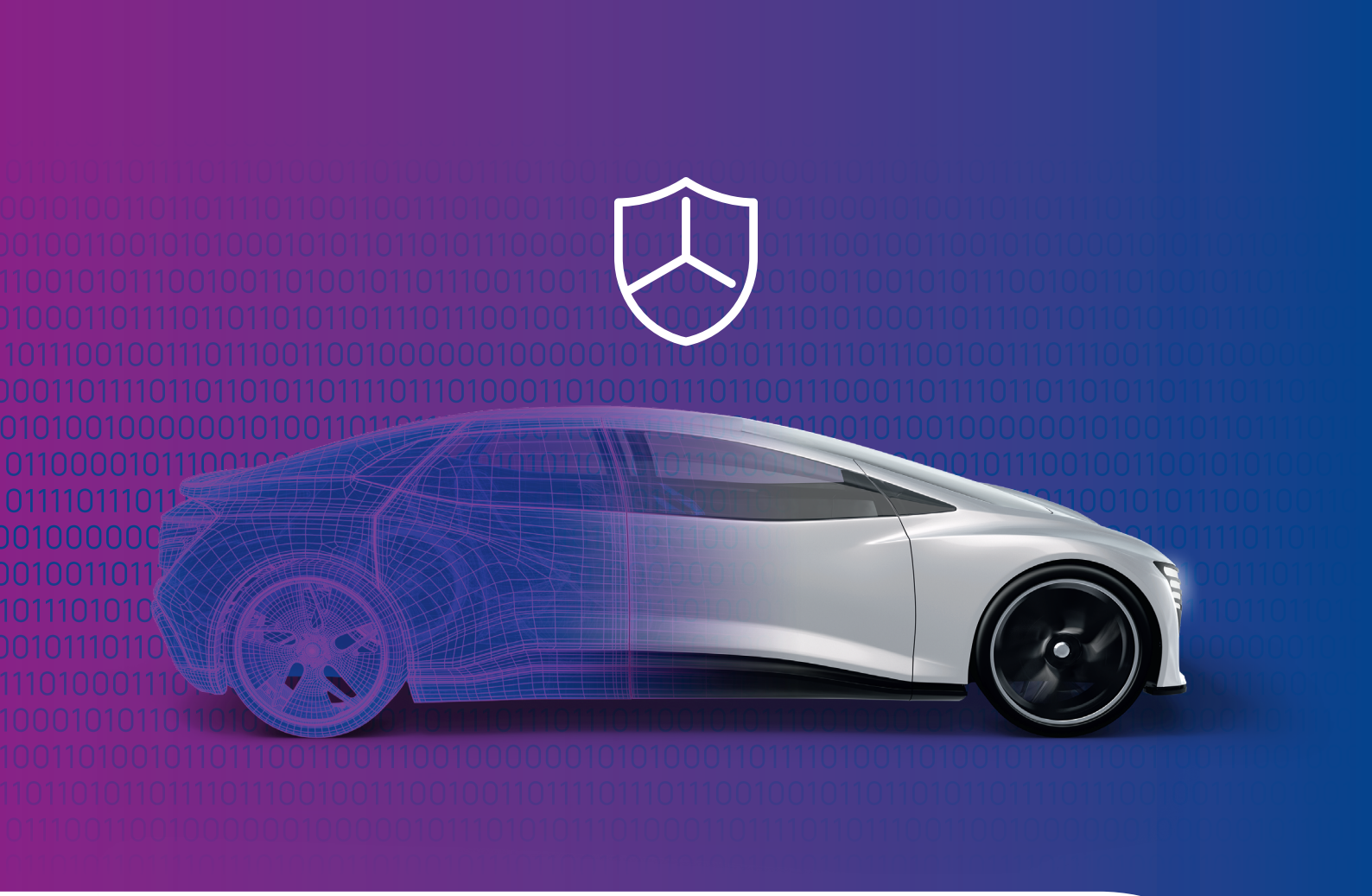

ソフトウェアデファインドビークルのサイバーセキュリティ

2023 年 5 月 Michael Lüke、Moritz Minzlaff（Dr.）著

Empowering Tomorrow's Automotive Software
www.etas.com

目次

1. 自動車開発の境界と概念を覆すソフトウェアデファインドビークル

サイバーセキュリティ対応が現代の自動車業界にとって経営上の大きな要素となっています。ソフトウェアの脆弱性がリコールにつながり [1]、自動車固有の法規制により、市場ではセキュリティ対策が義務付けられ [2][3]、製造業と自動車メーカーの大多数が最近、サイバーインシデントのリスクを経営上のリスクのトップ 5 に位置づけました [4]。

自動車用ソフトウェアは、自動車用セキュリティと密接に関連しています。業界がいわゆるソフトウェアデファインドビークル（SDV）への移行を進める中、サイバーセキュリティに対する確実な理解が求められています。このホワイトペーパーは、リスクをうまく避けるための羅針盤と地図を示すものです。

消費者の観点からいうと、SDV は、スマートフォンと同様のアプリストアと、オフボードでのデータ処理を要する機能を備えています。たとえば、ラジオの設定から座席の構成、空調管理まで、利用者の好みに合わせて自動的に環境設定されるレンタカーを想像してみてください。また、メーカーの観点からいうと、SDV は、最近の一部の自動車にすでに搭載されている従量課金機能などの、データを中心とした新しいビジネスモデルを実現します。SDV は、車両コンピュータと車両クラウドという、実車両からの抽象化を可能とする 2 つの先進技術を基盤としています。これらの技術革新によって、従来の自動車の境界と概念が覆されます。そのため、自動車メーカーは、自動車セキュリティに対する取り組みを変更する必要があります。つまり、SDV のサイバーセキュリティは、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 つの領域にわたって徹底して確保する必要があります（図 3 を参照）。

1.1 オンボードとオフボードの境界を無くすために

ソフトウェアデファインドビークルは、車両クラウドコンピューティングと呼ばれるオフボード機能を活用し、これに依存します。スマートフォンとのやり取り、バックエンドでのデータ処理、これらすべてが、車両の行先のほか、車両と運転者、乗客、道路利用者とのやり取りに直接影響を及ぼします。オフボードセキュリティの問題は、オンボードシステムに影響を及ぼす可能性があります [5][6]。セキュリティの観点からいうと、オンボードとオフボードの境界がなくなります。自動車メーカー、IT システム会社は、SDV と道路利用者の安全とを守るために、自動車エコシステム（図 1 を参照）におけるセキュリティを確保しなければなりません。

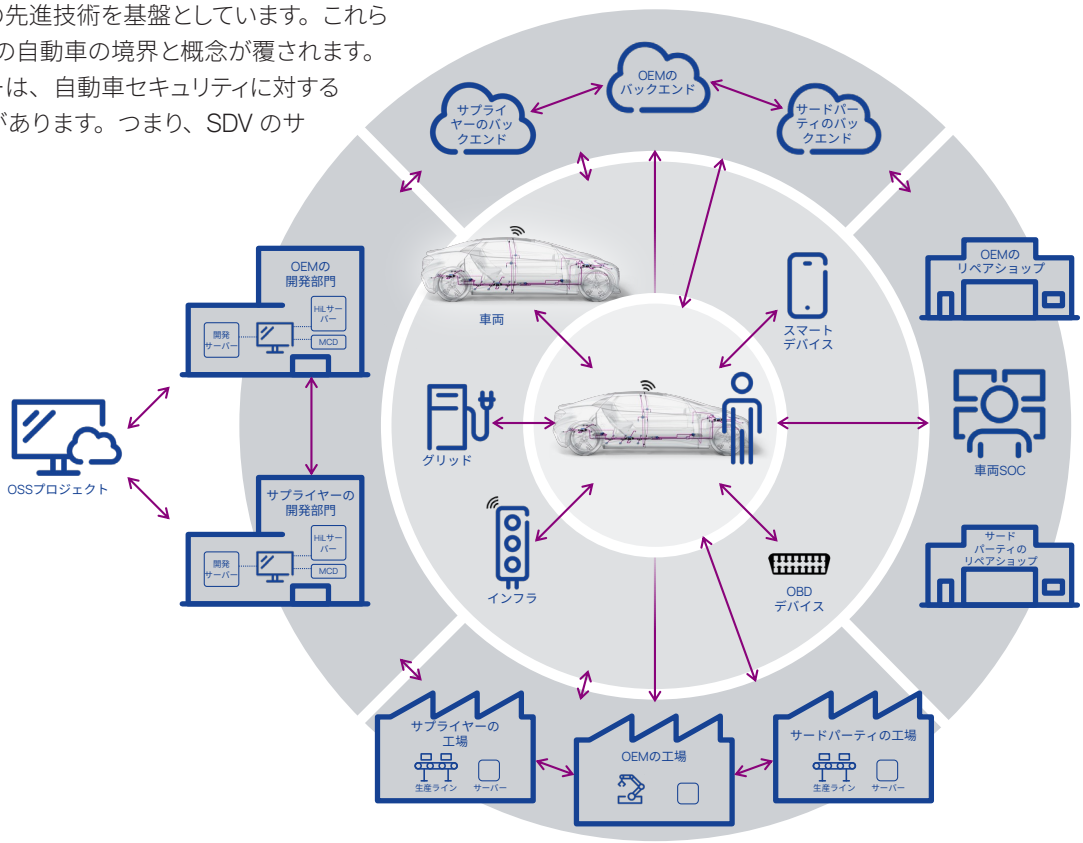

図 1：自動車エコシステムと、エコシステムの参加者間でのデータの流れ

図 2：SDV は、従来の深く組み込まれたソフトウェアのほか、新たに多くの種類の自動車ソフトウェアを導入している。

1.2 自動車ソフトウェアに関する前提の崩壊

SDV は、単にインターネット接続機能を備えた車両ではありません。車載コンピュータ内の新しいソフトウェアにも車両クラウドの新しいソフトウェアにも、他との差別化を図る重要な機能が実装されています。その結果、コードの行数が増加して、脆弱性を含む可能性が増えます。さらに重要なこととして、この変化により、自動車用ソフトウェアとは何かという既存の前提が崩れます。車載コンピュータと車両クラウドでは、新しいプログラミング言語、仮想化技術、サーバー技術、多数のオープンソースコンポーネント、新しい第三者的要素が使われます（図 2 を参照）。これらのコンポーネントやソースのいずれかにソフトウェアの脆弱性があると、SDV のセキュリティに影響が出ます。SDV は、飛躍的に拡大し多様化したソフトウェアのサプライチェーン全体で保護する必要があります。

1.3 開発者マインドへの挑戦

この新しい自動車用ソフトウェアには、もう 1 つの新しい重要な点があります。それは、ソフトウエアが決して完成されたものではなく、常に進化するということです。自動車の開発は生産の開始をもって終了するという考え方はもはや過去のものです。SDV は常に進化しており、頻繁な更新が特徴となっています。従来のオンボードとオフボードの境界がない SDV は、常に進化を続けることによる脅威にさらされています。その結果、自動車に対するサイバー攻撃が増加しており、特に SDV のライフサイクルのどの時点でも起こりうるリモート接続を介した攻撃が報告されています [7]。こういった攻撃は、製造段階でも行われます。2020 年から 2021 年にかけて、「製造段階での攻撃は昨年の（全攻撃のうち）7% から 22% に増加」し、「日和見的に標的を定めた攻撃は最大 300% 増加」しました [8]。自動車メーカーやサプライヤーは、ライフサイクル全体を通じて一貫して迅速に、ソフトウェアを監視、保護、更新する必要があります。

1.4 新たなエンドツーエンドセキュリティ

新たなエンドツーエンドセキュリティとは、どういったものでしょうか。それは、設計から生産、さらには製品の利用期間の終了まで（ライフサイクルの面）、顧客からメーカー、さらにはオープンソースソフトウェアのプロジェクトをはじめ、活気に満ちた新たなソフトウェアサプライヤーまで（ソフトウェアサプライチェーンの面）、車載コンポーネントからモバイルデバイス、車両クラウド、インフラ販売業者、インフラ運用業者まで（エコシステムの面）の範囲で、確実な保護を行わなければならないことを意味します。

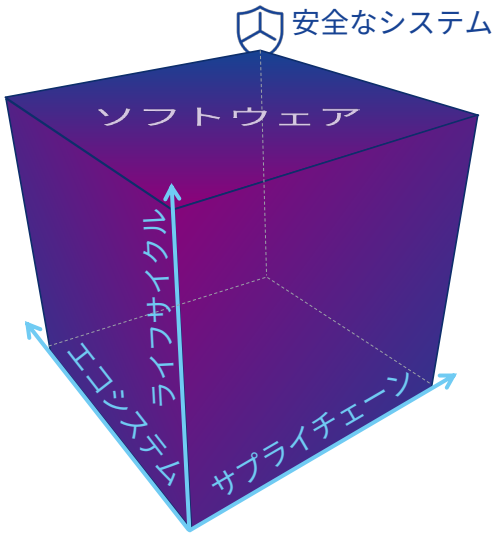

図 3：SDV のサイバーセキュリティは、ライフサイクル、エコシステム、ソフトウェアサプライチェーンの 3 領域においてエンドツーエンドで確保する必要がある。

自動車メーカーがこの新たなエンドツーエンドセキュリティを導入できるよう支援してきた当社の経験を基に、このホワイトペーパーは、以下のとおり構成されています。セクション 2 では、ソフトウェア業界とハイテク業界が得た教訓、特に DevOps の枠組みについて見ていき、自動車業界固有の事情について論じます。これにより、セクション 3 で、SDV のサイバーリスクの高まりに合わせた、SDV レベルの新たなサイバーセキュリティ成熟度を定義できます。セクション 4 で、このホワイトペーパーは、自動車メーカーがこの SDV レベルのサイバーセキュリティ成熟度をどのようにして達成できるかに関する見解を示して締めくくります。

2. ソフトウェア開発の速度への対応

SDV はすでに現実のものとなっているため、より実績あるソフトウェア業界から教訓やベストプラクティスを得ることが求められます。高い業績を誇るソフトウェア企業でひときわ目立つ重要な要素は、自動化のレベルとソフトウェア配信能力です。自動車メーカーとサプライヤーがソフトウェアシステムの問題解決や修正をより迅速に行えば行うほど、サイバー攻撃から顧客とビジネスモデルをより確実に保護することができます。インシデントはどうしても発生しますが、包括的な一連の対策を適切に導入することにより、高度な標的型攻撃 [9]、マルウェア攻撃 [10]、または単純なバグ [11] に関連するサイバーリスクを、許容可能な程度まで低減できます。こうした中で重要となる指標は、平均検出時間（MTTD）と平均修復時間（MTTR）であり、高いセキュリティ意識とサイバー成熟度がハイテク企業の信頼の証となります。

2.1 DevSecOps – 開発、セキュリティ、運用

どんなに優れた開発手法を用いても、どうしても未確認または未対応のバグがある程度残り、ソフトウェアが攻撃されやすい状態のままとなります。こうした中で、「脆弱なソフトウェアへのパッチ適用を確実に実施すれば、大部分のハッカーの攻撃を完全に防ぎ、リスクを大幅に低減できることが判明しています」[12]。DevOps は、正しく行えば、明らかにこの確実なパッチ適用を実施するのに役立ち、ソフトウェアライフサイクル全体を通してソフトウェアの開発と展開を加速させやすくなります。

ただし、今日のサイバーセキュリティの状況では、ソフトウェアサプライチェーンのエンドツーエンドのセキュリティを確保するために DevSecOps を採用することで、DevOps を次の段階に引き上げることが極めて重要です。DevSecOps は、ソースコードからソフトウェア開発者およびソフトウェアシステムに関わるすべての人の心理に至るまで、ソフトウェアの開発と運用にセキュリティ機能を組み込むものです（図 4 を参照）。

従来の自動車用ソフトウェアと IT ソフトウェアの統合が進んでいることを考えると、DevSecOps の採用は、もはや単なる任意事項ではなく、重要な必須事項です。たとえば、ブレーキシステムは、深く組み込まれたソフトウェアに依存しているため、今後もセキュリティを強化した V モデルを使用して開発されます。しかし、従来の自動車用ソフトウェアと IT ソフトウェアの統合が進むにつれ、特に車載コンピュータやシステムオンチップ（SoC）アーキテクチャの場合、DevSecOps に対するより焦点を絞った取り組みが求められます。これらのシステムでは、安全保障機能と汎用的機能が統合され、従来のブレーキシステムと路上物体認識などの車内外の機能との境界が曖昧になっています（図 6 を参照）。

ソフトウェアを開発してこのような SoC アーキテクチャに展開するには、自社製か社外のサードパーティ製か、オープンソースかクローズドソースかにかかわらず、コンポーネントとソースコードの厳密な検証が必要です。この検証は、ソフトウェアサプライチェーンに求められるエンドツーエンドセキュリティの重要な一面を表しています。ゼロデイ攻撃はどのようなコード行からも発生する可能性があり、悪意のあるソースコード操作はソフトウェアの世界では目新しいものではないため、ソースコードレベルから手を付けることが重要です。標的型攻撃には、このような脆弱性を悪用するものだけでなく、最初に脆弱性を挿入するものもあります。このようなサイバー攻撃を防止するには、正しい心構えを育むことが重要であり、そのためには、技術的な対策と組織的な対策の両方を含む多角的なアプローチが必要です。

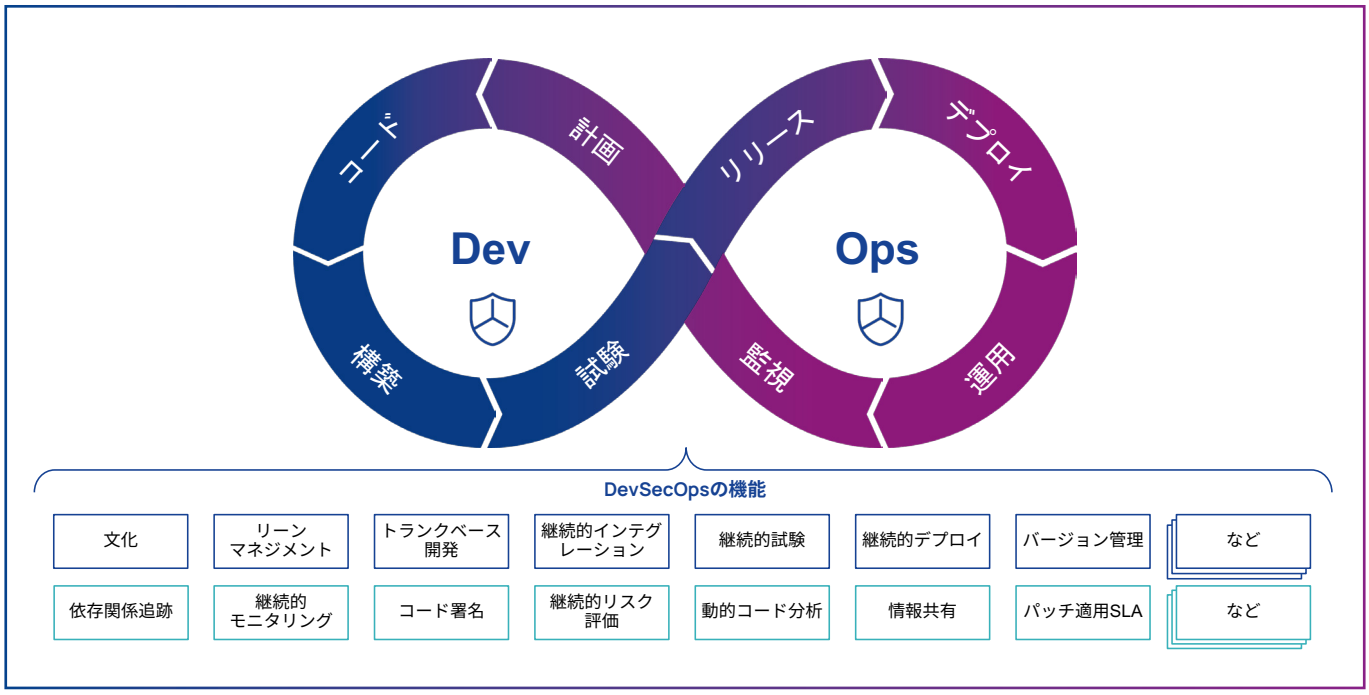

図 4：DevSecOps とは、DevOps に専用セキュリティ機能（緑）を加えた概念である。

このような状況におけるサイバーセキュリティにまつわる複雑さは、エコシステム、サプライチェーン、およびタイムラインにおいて使用されるソフトウェアの量が増え続けていることに起因しています（図 5 を参照）。この複雑さに効果的に対処するには、システムと組織がこの絶え間ない拡大に対応する必要があります。これが、SDV にもたらされるリスクに効果的に対処する唯一の方法なのです。

この問題を過小評価すべきではありません。この問題に効果的に対処するには、チームが円滑に連携し、情報を異なるツール間および部門間でスムーズに伝達する必要があります。セキュリティエンジニアリングでは、スピードが重要であり、自動化が不可欠です。このレベルの協力と透明性を実現するには、部門を超えたチームワーク、特に部署の境界と組織の枠をも超えた優れた技能が求められます。このように効果的に協力できることが DevSecOps の成功に欠かせない要素であり、安全なシステムを維持するために不可欠な要素です。セクション 3 と 4 では、引き続きこのトピックについて述べ、サイバーリスクを管理し、SDV の可能性を生かす方法を提示します。

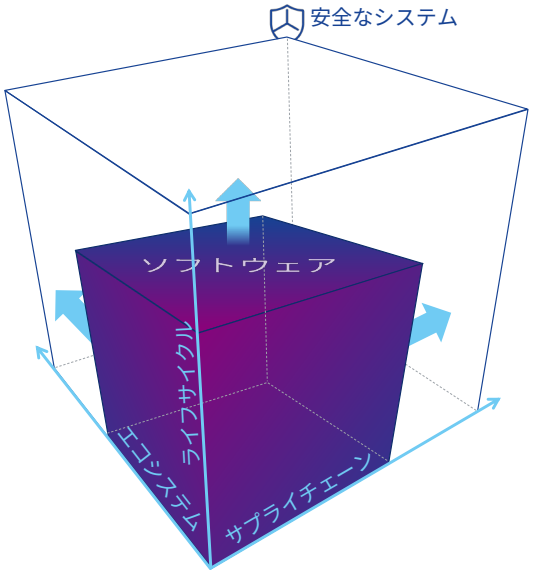

図 5：自動車エコシステムにおけるソフトウェアの量の増大に伴い、サイバーリスクスペースが増大している。

2.2 3つのフェーズでソフトウェアデファインドビークルへ

ソフトウェア業界は、数年前に DevOps を採用し、透明性が生み出す価値の大きさと縦割り組織の打破方法について多くのことを学びました。この新しいレベルの通信は、E/E アーキテクチャの開発が続けられ、車載コンピュータとクラウドベースの機能の実装が進むにつれて、自動車メーカーにも同様に重要な意味を持ってきます（図 7 を参照）。車両集中型アーキテクチャは、かつての車載機能と車外機能の境界を打ち破るものです。しかしながら、企業で縦割り組織構造が残っていると、組織内および組織間で互換性のないリスク評価や整合性のないソフトウェアパッチ適用方針などの弱点が生じます。

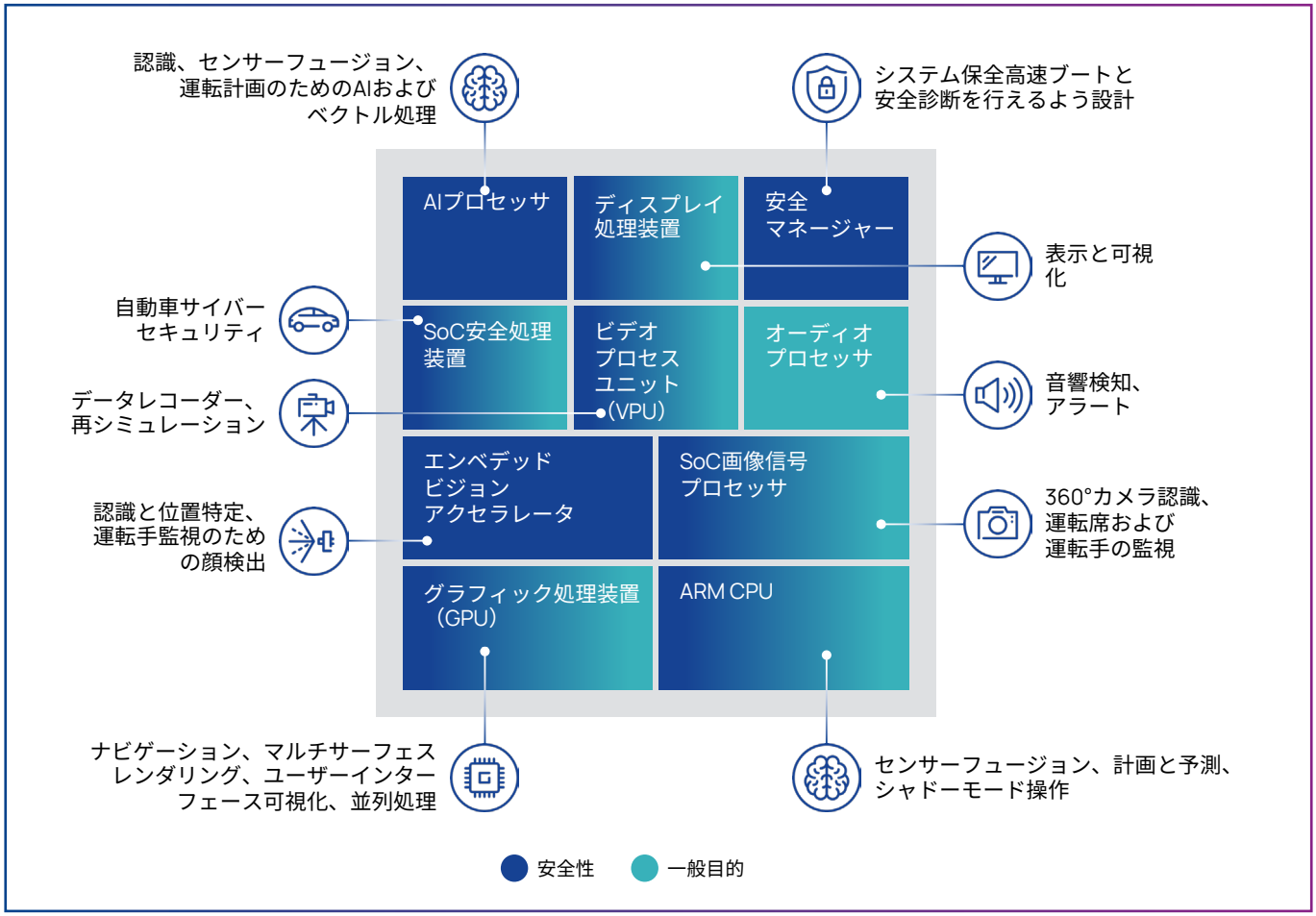

図 6：車載コンピュータで使用されるシステムオンチップにより、重要性が異なる機能（安全性、データ保護、インフォテインメント）が統合される。

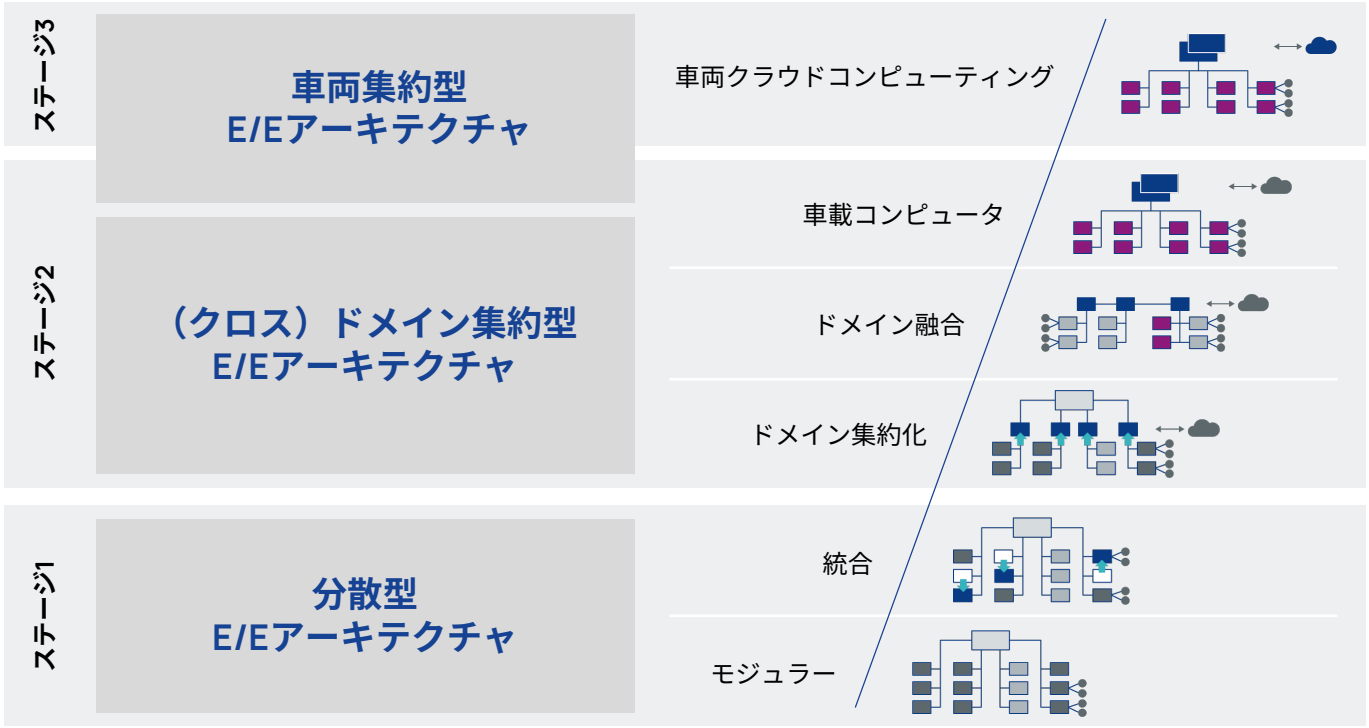

図 7：E/E アーキテクチャの開発による SDV の実現

そこで、自動車業界は、ソフトウェア業界から学んで、得られた教訓を、たとえば製品ライフサイクルの延長など、自動車業界特有の要件に合わせて適用できます。さらに、自動車業界における機能安全に関する要件と規制により、徹底した検証と妥当性確認が求められるため、DevSecOps は、安全面にも注意を払って実施する必要があります。ただし、DevOps と自動化によって、この検証をより迅速に進めることができます。また、すべての機能が安全性に関連するわけではないため、自動車業界は、同じ製品に対しても異なる速度で作業することを学ぶ必要があります。

さらに、自動車業界は、ソフトウェア業界の最新の進歩についていかなければなりません。たとえば、ゼロトラスト構想は、コネクテッドビークルの各種コンポーネント間の通信とデータ交換の安全性を確保するためのセキュリティフレームワークを提示するものであるため、SDV の将来にとって重要です。

ゼロトラストアプローチを採用すれば、許可を受け、検証された事業者のみが車両システムとデータにアクセスできることが保証され、このことが、車両、乗員ともにセキュリティとプライバシーを維持するにあたり、きわめて重要となります。自動車ビジネスへの採用は、たとえ今すぐではなくとも、フェーズ 3（図 8 を参照）では必須となります。

時間とリソースの浪費を避けるには、物事を一からやり直さないことが重要です。DevOps の手法は、自動車業界が誇りを持って模倣し、実情に合わせて変更し、開発部門と IT 運用部門の間の縦割りを取り払うアプローチとともに適用する必要があります。継続的インテグレーションと継続的デリバリーを適切に実施するには、協力体制の強化とフィードバックループの迅速化が必要であり、さらに、これを迅速かつ安全に実施するためのセキュリティの感覚も求められます。

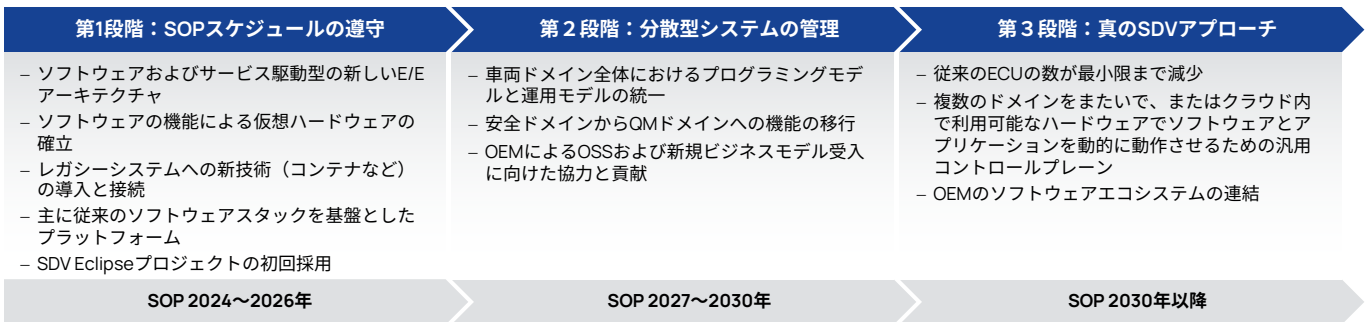

図 8：SDV は 3 段階で実現される。

3. SDV レベルのサイバーセキュリティ成熟度を確保するためのセキュリティ 4 原則

セキュリティプログラムは、「セキュアな製品設計」、「多層防御」、「リスク管理と監視」、「組織的セキュリティ」という 4 つの原則を遵守することで成果を挙げることができます。これらの原則を守っている組織が、人材、プロセス、および技術によって製品のセキュリティを確立できています。しかしながら、SDV は、既存の境界と概念を覆すものです。リスク領域が拡大（図 5 を参照）する中、自動車業界は、セキュリティによってリスクを軽減するために、これらの 4 原則を再考する必要があります。製造業者とサプライヤーは、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（図 9 を参照）の各側面において、SDV をエンドツーエンドで適切に保護するために、従来よりも高い成熟度でこれらの原則を実践する必要があります。DevOps ループの個々の活動が単独では限られた影響力しか持たないのと同様に、組織が 4 原則すべてを SDV レベルの成熟度で実践し、サイバー攻撃に対する十分な復元力を獲得して初めて、SDV のサイバーセキュリティに完全に対応できます。

3.1 原則その 1：セキュアな製品設計

セキュアな製品設計とは、最初から製品にセキュリティ機能が組み込まれることをいいます。これは、多くの場合、プロセス中心の原則となります。この原則の実践例として有名なのは、セキュリティが強化された V モデルです。SDV がサイバー攻撃者の攻撃にさらされ続けることを考慮すると、自動車メーカーはさらに、セキュアな製品設計とは、SDV のライフサイクル全体にわたって脆弱性の平均修復時間を絶え間なく最適化することでもある、と認識する必要があります。DevOps ループを完結させるには、高度な自動化と弾力性確保への注力が必要となります。

3.2 原則その 2：多層防御

多層防御とは、製品全体を危険にさらすような単一障害点を発生させることなく、複数の保護機構を確立する取り組みをいいます。具体的なセキュリティ技術（ソフトウェアとハードウェア）がこの原則の焦点となります。SDV 以前、これは一般的に、末端のコンポーネントから車載ドメイン、車両ネットワーク全体までの階層構造を意味していました。車載コンピュータと車両クラウドを利用する新しい車両集中型アーキテクチャでは、ゼロトラストへの進化を含め、車載コンポーネントと車外コンポーネントの階層を加えたエコシステムレベルの認識が求められます。

他とは異なる考えを持ち、異なる行動をとる成熟した組織

図 9 に示す成熟度の向上に関する説明は、ETAS が数十年にわたり自動車メーカーのサイバーセキュリティを支援してきた経験と、業界をリードする ESCRYPT 自動車サイバーセキュリティ成熟度調査に基づくものです。データから興味深い現実がわかります。つまり、成熟度の高い企業は、サイバーセキュリティ関係者に対する関わり、規制要件の優先順位付け、サイバーセキュリティに対する予算設定の点で、他の企業とは異なっています。サイバーセキュリティ成熟度の向上は、満足度の向上、DevSecOps に対する心構えの向上、エンドツーエンドでのセキュリティ対応の向上と相関しています。世界中の自動車関係者から寄せられた数百件の回答に基づく、2022 年版自動車サイバーセキュリティ成熟度レポートの全文をご覧ください。また、ETAS のソーシャルメディアチャンネルをフォローしていただくと、今年のレポートや今後の調査についてのお知らせをご覧いただけます。

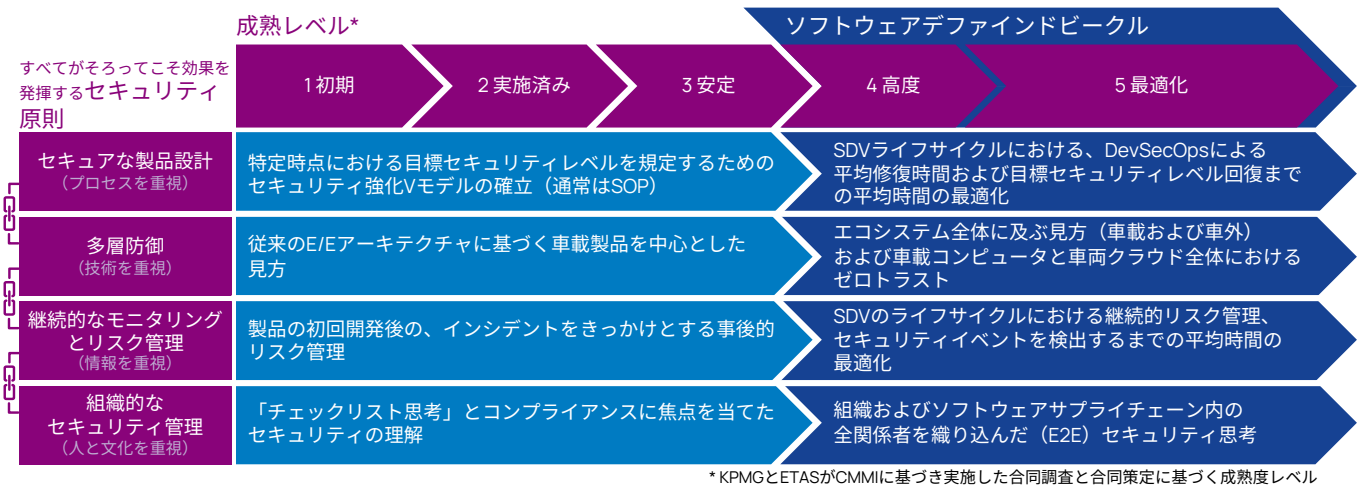

図 9：SDV では、セキュリティ 4 原則のそれぞれで新たなレベルのサイバーセキュリティ成熟度が求められる。

3.3 原則その 3：リスク管理と監視

リスク管理と監視は、すべてのセキュリティ活動の中心に据えるべき原則です。この原則は、SDV エコシステム内の情報とデータ資産に焦点を当てたものです。脅威とリスクの分析（TARA）は、自動車メーカーが成熟度の初期から確立期へと進む際に最初に取り組むステップの 1 つです。TARA は、リスクを特定し、たとえばセキュアな製品設計と深層防御の原則を一貫して適用することにより、リスク軽減策によってリスクが許容可能な程度まで低減されるかどうかを測定します。ただし、メーカーやサプライヤーが確立している初期プロセスやツールは、SDV に求められる高頻度の変更には適さないことが多いとされます。SDV の耐用期間が終了するまで、エコシステム内の脆弱性を含む脅威の状況を継続的に監視し、セキュリティイベントを検知するまでの平均時間をなるべく短縮して、TARA を迅速に更新することは、成熟度が進んでいるか成熟度が絶えず最適に保たれている組織の特徴です。

3.4 原則その 4：組織的なセキュリティ管理

近年のサイバーインシデントを振り返ると、セキュリティ確保には技術的・組織的な解決策が必要であることがわかります。そこで、この原則では、人と文化に焦点を当てています。自動車メーカーやサプライヤーは、業務、リスク管理とコンプライアンス、内部監査（いわゆる「3 つの防衛線」）においてサイバーセキュリティ管理システムを導入する必要があります。全部を構築するには時間と労力がかかるため、成熟度が初期段階の組織では通常、たとえば「コンプライアンス」とそれに関連するチェックリストの考え方に明確に焦点を当てるなど、1 つの防衛線だけに注力します。これは当然のことであり、これによって企業が初期段階で事業を継続しやすくなります。しかしながら、データ中心のビジネスモデルを持つ SDV では、3 つの防衛線すべてに対応し、ソフトウェアサプライチェーンを含むすべての関係者を統合する、より広範なセキュリティの考え方が必要となります（図 10 を参照）。

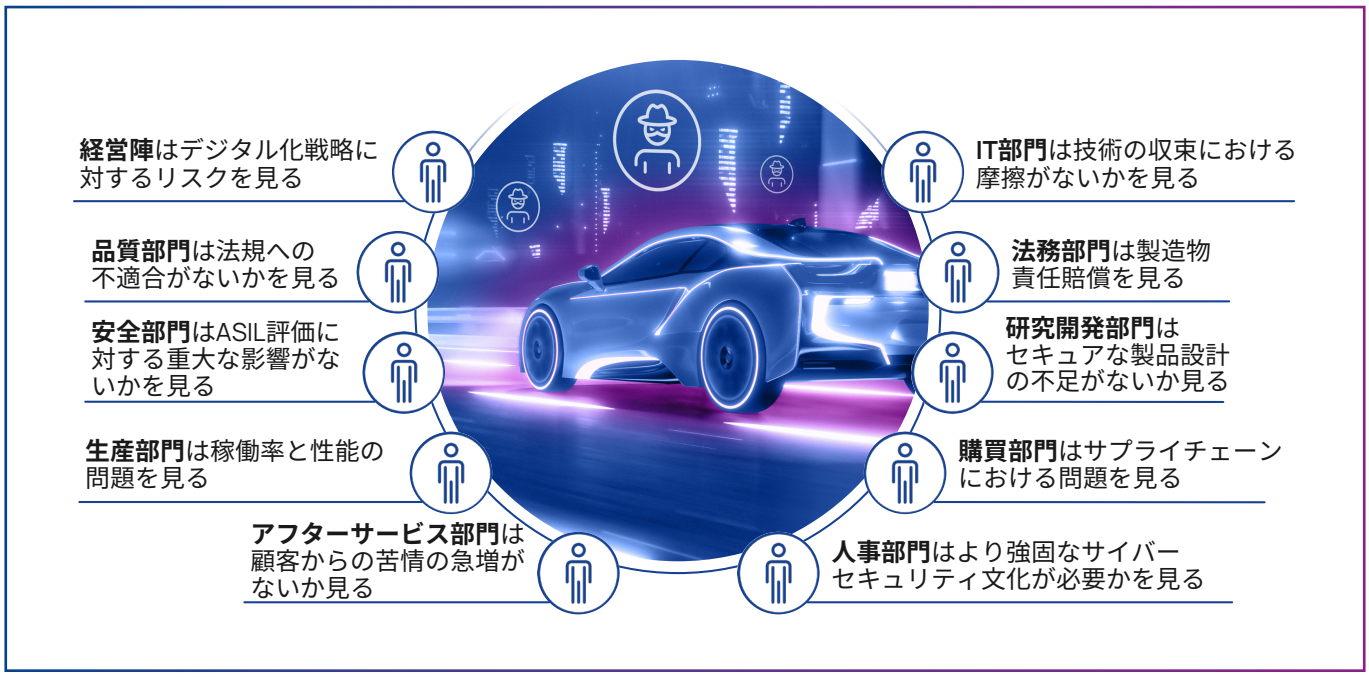

図 10：成熟度の高いセキュリティ組織は、社内の全関係者、顧客、ソフトウェアサプライチェーンの視点をまとめて反映させている。

4. SDV レベルのサイバーセキュリティ成熟度への到達

ETAS は、自動車メーカーとサプライヤーのサイバーセキュリティ成熟度を向上させる独自の専門知識を持っています。ESCRYPT サイバーセキュリティソリューションは、約 20 年にわたり、自動車業界におけるサイバーセキュリティ関連のマイルストーンに対応し、これを乗り越える支援を行ってきました。2000 年代初頭の最初の研究論文の執筆から、何百万台もの自動車へのハードウェアセキュリティモジュールの実装、数時間から数分でパッチを展開できる DevSecOps 組織の確立まで、自動車業界のサイバーセキュリティ成熟度向上を実現できる実績のあるパターンを見出すことができます。SDV レベルのサイバーセキュリティ成熟度には、1）現在の成熟度を評価する、2）成熟度目標を設定する、3）ギャップ解消プログラムを実行する、という 3 段階のプロセスを経て到達できます（図 11 を参照）。では、それぞれについて順番に見ていきましょう。

4.1 現在の成熟度の評価

現時点での人材とプロセスのサイバーセキュリティ成熟度を評価することで、組織が、目標とする新しい成熟度を迅速かつ高い費用対効果で達成する上で最も貢献度の高い部分にリソースを集中させることができます。実際、当社のコンサルティングプロジェクトでは、ソフトウェアや機能安全領域など、企業がより迅速に高度な製品セキュリティ機能を構築するための土台となる既存の機能を発見することがよくあります。ESCRYPT 自動車サイバーセキュリティ成熟度調査の回答によってこの点が裏付けられています。つまり、成熟度が初期段階の企業の回答者は、多くの人がよく理解している領域である機能安全性規格を、サイバーセキュリティプログラムに関連性の高いものとして選択しました。これが、自動車メーカーが自社の成熟度を評価するために利用できる PROOF 自動車サイバーセキュリティ成熟度モデル（テキストボックスを参照）を当社が設計した理由です。

同様に、技術レベルでの現状把握は、E/E アーキテクチャがゼロから設計されておらず、レガシーアーキテクチャが（暗黙の）セキュリティ対策を備えている可能性があるブラウンフィールドの状況において、特に意義を持ちます。重要なこととして、人、プロセス、技術における現状を評価するには、組織そのものだけでなく、エコシステムの中で誰とどのように協力しているか、さらには組織のサプライチェーンについても、考慮する必要があります（図 12 を参照）。

PROOF 自動車サーバーセキュリティ成熟度モデル

図 9 は、PROOF（製品セキュリティ組織フレームワーク）からの抜粋です。2019 年の発表以来、自動車メーカーは、専門サプライヤーから世界的に有名なメーカーに至るまで、PROOF を採用してきました。

自動車業界向けに考案された PROOF
- 120 件を超える自動車業界に特化した指標により、サイバーセキュリティ成熟度を診断
- 自動車のセキュリティに関する国内外の規則と規格（UNECE、ISO、CN、EU、JasPar、NHTSA など）を考慮

規格に基づく PROOF
- ISO 33000 シリーズが土台（Automotive SPICE を参照）
- CMMI と同様、5 段階の成熟度を採用
- ドイツの ETAS と KPMG が、長年にわたるサイバーセキュリティ対策の向上と安全な自動車システムの構築の経験を生かして考案

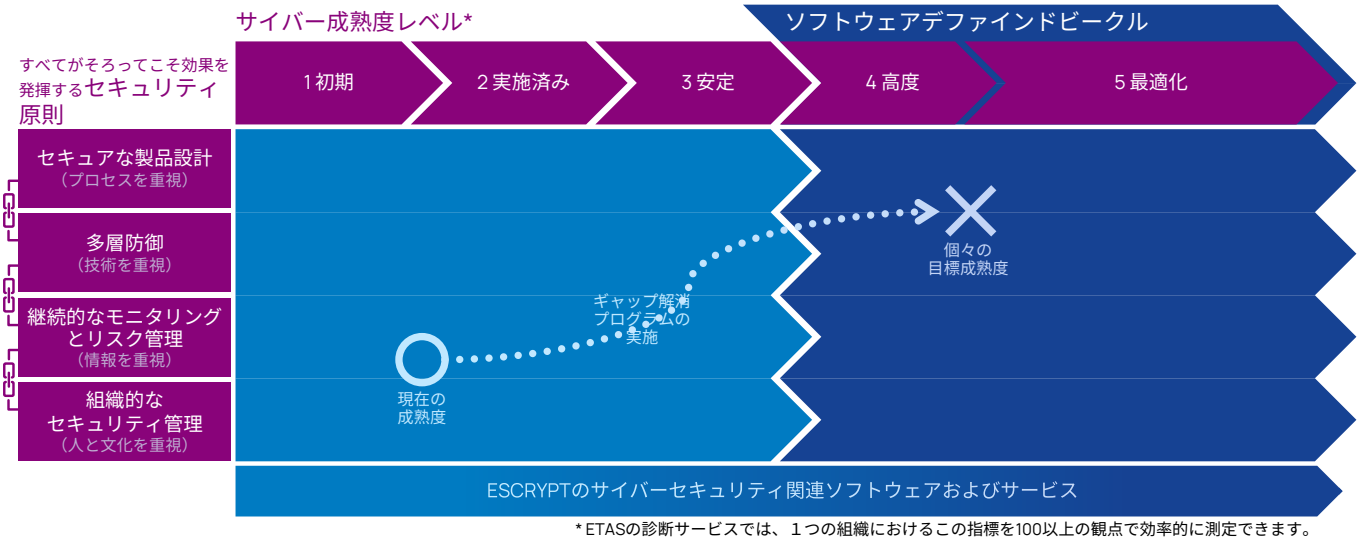

図 11：SDV のサイバーリスクに合わせてサーバーセキュリティ成熟度を確保することは、現在の成熟度の評価、成熟度目標の設定、ギャップ解消プログラムの実行の 3 段階のプロセスによって実現する。

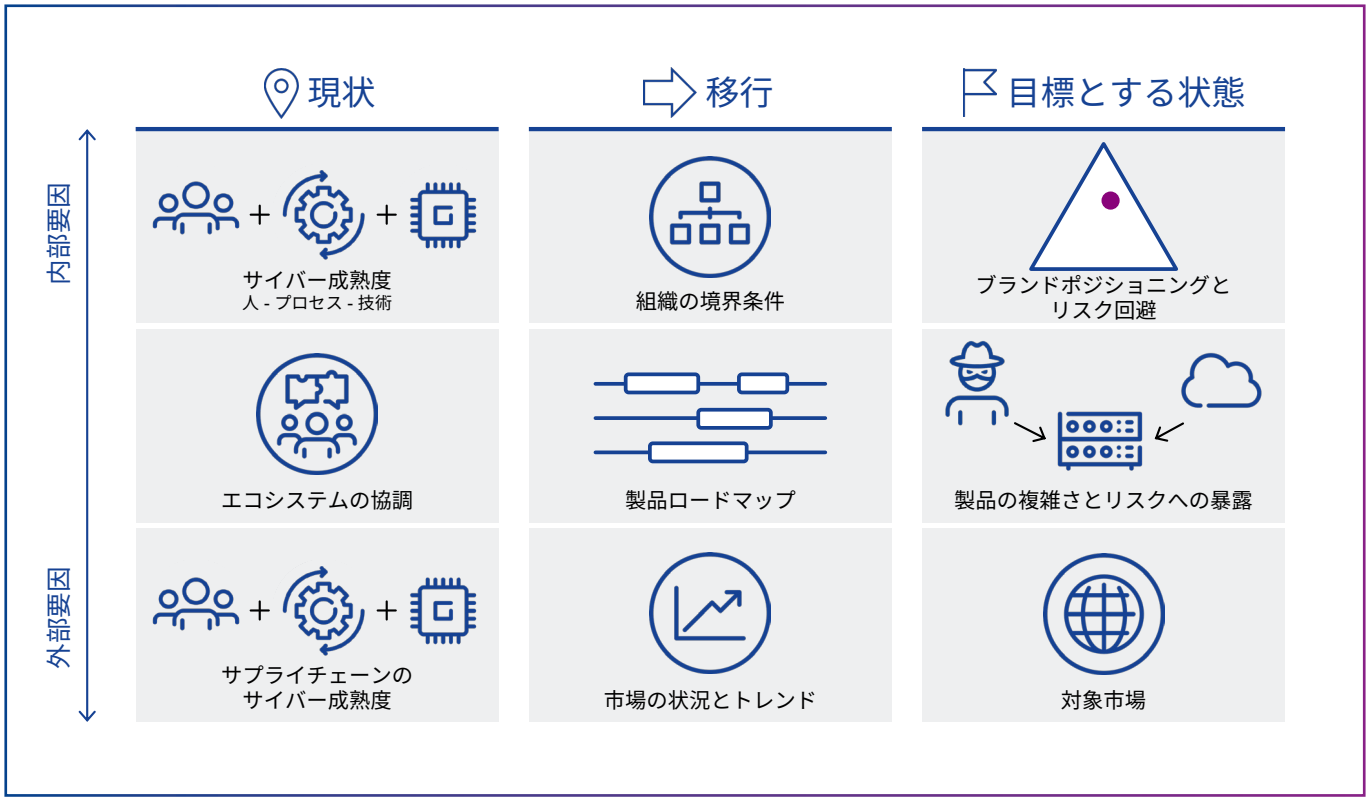

図 12：この自動車サイバーセキュリティ成熟度の図では、サイバーセキュリティ成熟度向上プログラムの関連要素を 2 つの次元、つまり組織内と組織外の要素と、現状、移行期、および目標となる状態に関連する要素に分類している。

4.2 成熟度目標の設定

成熟度目標を設定することは、SDV のサイバーリスクの増大に合わせて、道路利用者、顧客、ビジネスモデルを保護するための機能を高める上で必要となります。攻撃者（攻撃者となる可能性のある者を含む）の能力と攻撃機会の増大（図 5 を参照）が組織の成熟度を上回れば、受け入れがたいビジネスリスクがもたらされます。逆に、新たな成熟度目標を高く設定しすぎると、リソースを浪費したり、必要な変更を取り込んで実施する組織の能力を過度に拡大したりすることになり、それによってサイバーセキュリティプログラムが失敗に終わるリスクが出てきます。当社は、3 つの主な要因によって目標の程度が決まることを確認しました。3 つの主な要因とは、企業のブランドポジショニングとリスク回避、製品の複雑さとリスクへの暴露、規制要件やコンプライアンス要件などの対象市場からの要件です（図 12 を参照）。これらの各要因は、一般的に時間の経過とともに変化するため、当社は、これらの要因に起因する要件だけでなく、企業が考慮する組織的セキュリティ対策と技術的セキュリティ対策とを絶えず橋渡しする措置を導入することが有用であることを確認しました。

4.3 ギャップ解消プログラムの実施

SDV に向けた技術的進化が複数段階を経て行われるのと同様に、新しい目標に向けた組織の成熟も複数段階を経て行われます（図 8 を参照）。サイバーリスクの増大に合わせてサイバー成熟度を向上させることが目標であるため、このことは理にかなっています。前節で述べたとおり、リスクと成熟度のバランスが著しく悪いと、失敗につながります。

成熟度が初期段階の組織は、ウォーターフォール形式で計画されたプロジェクトにおける所定の成熟度の入り口までは到達できますが、所定の成熟度から SDV レベルの成熟度まで飛躍するには、大規模な組織変革構想に特有の複雑さが伴います。

成熟度の初期段階では、試験済みのテンプレートやプロセス概要の当社の包括的なライブラリを直接活用できます。テクニカルセキュリティベースライン（別名セキュリティアーキテクチャ）は、組織内だけでなく、サプライヤーや顧客も交えてセキュリティ管理体制を整える上で効果的であることが実証されています。製品ロードマップとともにこのベースラインを進化させることで、セキュリティ対策が、増大する攻撃対象領域からの保護能力を十分に維持できるようになります。

組織がより高い成熟度に達するにつれて、反復的な手法がより一般的になります。企業は頻繁に成熟度を評価し、より小規模で的を絞った変更を通じて高度な機能を開発します（図 13 を参照）。この方法により、組織は、より広範なデジタル化戦略や急速な市場発展などの境界条件に対応できるようになります。

ETAS 独自の経験により、このような状況で必要とされる反復処理の回数を大幅に減らすことができます。ETAS は、自動車メーカーやサプライヤーのサイバーセキュリティを数多く支援してきた実績豊富なプロフェッショナルサービス部門を擁する自動車関連企業として、自動車工学を含む関連部門の要件に合わせて変更を導入支援することを得意としています。

結論として、組織は、ETAS とのパートナーシップにより、サイバーリスクを低減し、SDV の潜在能力を引き出すことができます。ETAS が提供する、ソフトウェアとサービスを駆使した包括的な自動車サイバーセキュリティソリューションの手法では、セキュリティの 4 原則すべてに対応しています。当社は、一丸となってこの課題を克服し、安全で信頼性の高い SDV を実現します。

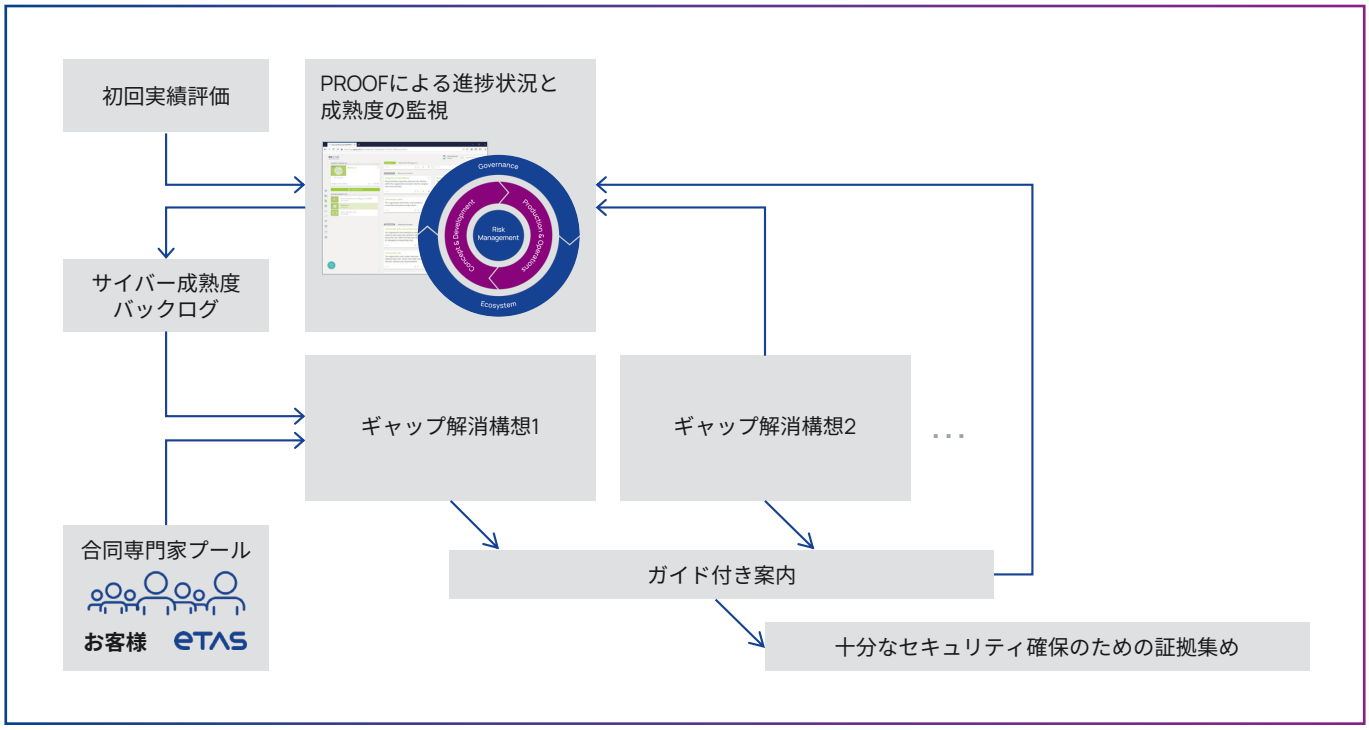

図 13：焦点を絞った迅速な反復処理（「ギャップ解消構想」）と現在の成熟度の透明性のある監視により、企業は、効果的かつ的を絞って成熟度を向上させることができる。

ETAS について

1994 年に設立された ETAS GmbH は、ボッシュ・グループの完全子会社であり、欧州、北米、南米、アジアのすべての主要自動車市場に拠点を展開しています。

ETAS は、ソフトウェア開発ソリューション、車載オペレーティングシステム、車両クラウドサービス、データ収集・処理ソリューション、統合カスタマーソリューション、サイバーセキュリティの各分野で、ソフトウェアデファインドビークルの実現のための包括的ソリューションを提供しています。

ETAS は、サイバーセキュリティ業界のパイオニアとして、実績のある車載・車外ソフトウェア製品ポートフォリオと専門セキュリティサービスにより、お客様がサイバーセキュリティ関連の複雑性に対処し、サイバーリスクを低減し、お客様のビジネス成長力を最大限に引き出せるよう支援しています。

ETAS の車載セキュリティソリューションは、世界中で何百万台もの車両システムを保護しており、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の標準となっています。

参考文献

[1] **NHTSA,** “Safety Issues & Recalls (NHTSA ID 15V461000),” 2015 年 7 月 23 日。（オンライン）。利用可：**https://www.nhtsa.gov/recalls** 2022 年 11 月 10 日にアクセス）。

[2] **UNECE,** “UN Regulation No. 155 - Cyber security and cyber security management system,” 2021 年 3 月 4 日。（オンライン）。利用可：**https://unece.org/sites/default/files/2021-03/R155e.pdf** [2022 年 10 月 27 日にアクセス）。

[3] **The State Council / The People’s Republic of China,** “Opinions on Strengthening the Access Management of Intelligent Connected Vehicle Manufacturers and Products,” 2021 年 8 月 12 日。（オンライン）。利用可：**http://www.gov.cn/zhengce/zhengceku/2021-08/12/content_5630912.htm**（2022 年 10 月 28 日にアクセス）。

[4] **Allianz,** Allianz Risk Barometer 2022、ミュンヘン、2022 年。

[5] **E. Montalbano,** “Hackers remotely steer Tesla Model S using autopilot system (The security ledger),” 2019 年 4 月 3 日。（オンライン）。利用可：**https://securityledger.com/2019/04/hackers-remotely-steer-tesla-model-s-using-autopilot-system/**（2022 年 10 月 27 日にアクセス）。

[6] **S. Curry,** “Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More,”（オンライン）。利用可：**https://samcurry.net/web-hackers-vs-the-auto-industry/**（2023 年 4 月 2 日にアクセス）。

[7] **Upstream,** “Upstream’s 2022 Global Automotive Cybersecurity Report,” 2022 年 1 月 26 日。（オンライン）。利用可：**https://www.israel21c.org/cyberattacks-on-cars-increased-225-in-last-three-years/**.（2022 年 9 月 5 日にアクセス）。

[8] “NTT Global Threat Intelligence Report,” 2021 年 5 月 11 日。（オンライン）。利用可：**https://services.global.ntt/ja-jp/newsroom/ntt-global-threat-intelligence-report-2021**（2022 年 9 月 5 日にアクセス）。

[9] **E. Gately,** “Insured Losses from SolarWinds Hack Mount, But Could Be Worse,” 2021 年 1 月 20 日。（オンライン）。利用可：**https://www.channelfutures.com/mssp-insider/insured-losses-from-solarwinds-hack-mount-but-could-be-worse**

[10] **A. Bannister,** “NPM maintainer targets Russian users with data-wiping ‘protestware’” 2022 年 3 月 21 日。（オンライン）。利用可：**https://portswigger.net/daily-swig/npm-maintainer-targets-russian-users-with-data-wiping-protestware**（2023 年 5 月 11 日にアクセス）。

[11] **CIS Center for Internet Security,** “Log4j Zero-Day Vulnerability Response,” 2022 年 1 月 7 日。（オンライン）。利用可：**https://www.cisecurity.org/log4j-zero-day-vulnerability-response**（2023 年 5 月 11 日にアクセス）。

[12] **R. A. Grimes,** “Zero-days aren’t the problem – patches are,” 2016 年 6 月 1 日。（オンライン）。利用可：**https://www.csoonline.com/article/3075830/zero-days-arent-the-problem-patches-are.html**（2023 年 5 月 16 日にアクセス）。

連絡先

Michael Lüke
シニアマネージャー
michael.lueke@etas.com

Dr. Moritz Minzlaff
専門セキュリティサービス部門長
moritz.minzlaff@etas.com