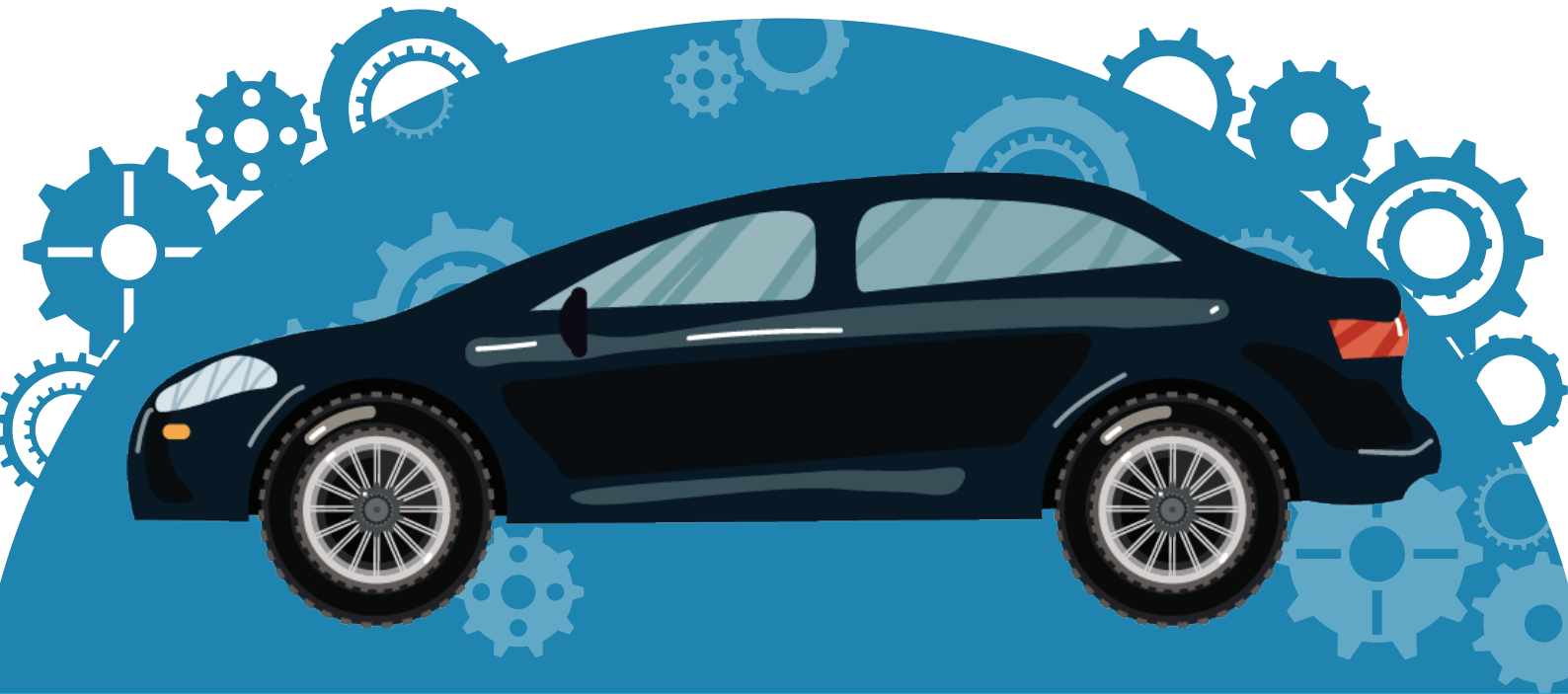
BLACKDUCK

自動車業界におけるオープンソースソフトウェアの管理と安全確保

エグゼクティブサマリー

自動車業界は変革の真っ只中にいます。現代の自動車はもはや、単に場所を移動する手段という領域を超えて、クラウドからストリーミングで音楽を入手したり、ハンズフリー通話を可能にしたり、さらにはリアルタイムで交通情報やパーソナライズされたロードサービスまで提供するものに変貌を遂げています。

また、現代の自動車では、速度監視、燃費追跡、排気ガスレベルの監視などの最新機能の多くがデジタル化されることで、運転者による操作性の改善、より良い情報の提供が可能になっています。自動車業界における技術革新は加速しています。自動運転車両を制御するために必要なコンピューティング能力は増大し、車両周辺障害物を検知するシステム向けの低コストのセンサーも開発されています。最近の技術革新では、高速道路上での位置を車両自体が監視し調整することが可能になり、車線から外れた場合には運転者に警告し、別の車に近づきすぎれば自動的に減速もします。私たちの心の準備ができているかどうかにかかわらず、自動運転車で道路を走る時代はすぐそこまできているのです。



現代の自動車は、エンジンのパワーと同様に、統合されたテクノロジーのパワーが大きな役割を果たしています。 自動車業界において技術革新を推進しているのはソフトウェアであり、そのソフトウェアはオープンソースを中核として構築されています。

Black Duckのオンデマンド監査によると、自動車向け商用アプリケーションではオープンソースのコンポーネントが平均23%を占めます。

オープンソースの使用は、自動車業界を含むあらゆる業界に浸透しています。最近のForrester Researchの報告書によると、アプリケーションの分野ではオープンソースが広く普及していることが示されています。現在、商用アプリケーションに占めるカスタムコードの割合は、わずか10～20%です。Black Duckによる商用アプリケーションのオンデマンド監査でも、自動車アプリケーションの23%がオープンソースコンポーネントで構成されていることが確認され、Forrester Researchと同様の傾向が報告されています。

オープンソースを支持する理由はシンプルです。オープンソースは開発コストを削減し、開発期間を短縮し、イノベーションを加速します。ソフトウェアに関しては、すべての自動車メーカーは、コアオペレーティングシステムやさまざまな要素を結びつけるコンポーネントなどのコモディティになる部分に費やす時間を短縮し、ブランドを差別化するための画期的機能の開発に注力したいと考えています。オープンソースモデルは、アジャイルな製品開発をあらゆる側面で効率よくサポートします。

自動車ソフトウェアのアプリケーション&プラットフォームのセキュリティ、ライセンス準拠、コード品質を維持するには、オープンソースの可視性と制御が不可欠です。

しかし、リーン生産方式とISO-9000の実行が自動車業界に俊敏性と高品質をもたらしたように、自動車ソフトウェアアプリケーションやプラットフォームのセキュリティ、ライセンス準拠、コード品質を維持するには、オープンソースの可視性と制御が不可欠です。

本レポートでは、自動車業界にサービスを提供する自動車メーカーやサプライヤー、テクノロジー企業が、自動車ソフトウェアサプライチェーン全体でオープンソースソフトウェアの使用を管理するための課題を検証し、推奨事項を提示します。

自動車業界におけるオープンソース

オープンソースのコンセプトは25年以上前に導入されました。それ以来、オープンソースソフトウェアの採用は加速しています。「オープン」とは、特定のライセンス条件のもとで開発者が自由にソースコードを利用できることを意味します。多くのオープンソースライセンスにおいて、開発者はソフトウェアを好きなように変更して誰にでも配布する権利を有します。

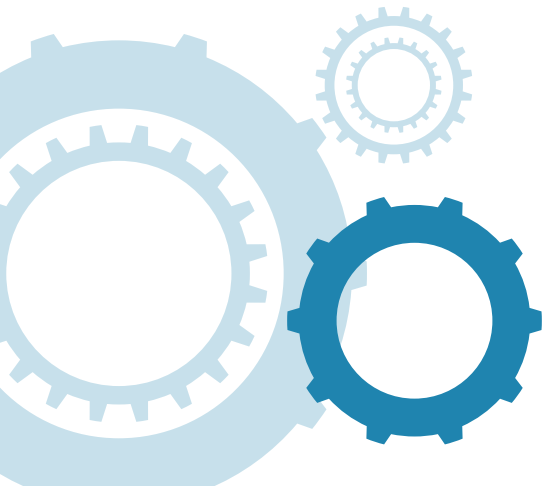
Linuxオペレーティングシステムは、世界のあらゆるオペレーティングシステムの中で最大規模のインストール数を誇る、オープンソースの代表例です。

Linuxオペレーティングシステムは、世界のあらゆるオペレーティングシステムの中で最大規模のインストール数を誇る、オープンソースの代表例です。多種多用なニーズに応えるため、多くのバージョンのLinuxが生み出されました。中でもオープンソースの共同プロジェクトである「Automotive Grade Linux (AGL)」は、コネクテッドカー向けに完全にオープンなソフトウェアスタックの開発および導入を加速することを目的に、自動車メーカーやサプライヤー、テクノロジー企業が集結した取り組みです。AGLは、Linuxを中核として、実質的な業界標準として機能するオープンプラットフォームをその土台から開発することで、新しい機能や技術の迅速な開発を可能にしています。

また「オープンオートモーティブアライアンス」は、テクノロジー企業と自動車企業からなるグループで、Apache v2オープンソースライセンスのもとでリリースされた携帯電話向けLinuxベースのプラットフォームであるAndroidの高い価値を、ドライバー目線（運転中にできるだけ気が散らないような方法）でシームレスに自動車に導入しようとしています。

もう1つ、自動車業界でよく知られているオープンソースプロジェクトがGENIVI®です。この非営利の業界連合は、車内エンターテイメント（ICE）または車載インフォテインメント（IVI）の開発をサポートするオープンスタンダードを策定しています。GENIVI規格は、多様なブランド、データの所有権、ビジネスモデルに適合するアプリケーションの提供をサポートします。この業界連合には、BMWなどの自動車OEM、Boschなどの自動車サプライヤー、Black Duckソフトウェアなどの世界的なソフトウェアおよびサービスサプライヤーを含む140社以上のメンバーが加盟しています。

2,000を超えるBlack Duckのお客様には、GENIVIやGENIVI Allianceのメンバーを含む、自動車業界の企業も多く加盟しています。



2,000を超えるBlack Duckのお客様には、GENIVIやGENIVI Allianceのメンバーを含む、自動車業界の企業も多く含まれています。これらの企業は、業界をリードするBlack Duckの製品を使用して、オープンソースソフトウェアの安全確保と管理のプロセスを自動化し、セキュリティ脆弱性やコンプライアンス、運用リスクに関連する課題を解決しています。

車のコネクティビティのセキュリティ対策は遅れをとっている

“車に新技術を持ちこめば、セキュリティの課題に直面する”

- セキュリティの研究者がインターネット経由でJeepに侵入し、ブレーキやトランスミッションを乗っ取ることができることを明らかにしました。これにより、クライスラー社は、これを重大なセキュリティリスクと判断し、その攻撃を可能にするバグを修正するために140万台の車両をリコールしました
- GM社の何百万台もの車やトラックは、5年近くに渡って、リモートで車両追跡から高速でブレーキをかけたり、ブレーキを無効するなどあらゆることが可能なエクスプロイト対しての脆弱性がありました。
- テスラのモデルSのインフォテインメントシステムには、4年前から、攻撃者が完全な遠隔地からハッキングし、車を始動させたりエンジンを切ったりできる可能性を持った脆弱性がありました。.

自動車メーカーは、サイバーセキュリティアプローチを導入し、車のソフトウェアそのものがさらされる危険だけでなく、ソフトウェアに含まれるオープンソースコンポーネントによる隠れた脆弱性にも対処する必要があります。

オープンソースの安全性とセキュリティ問題

自動車の安全がソフトウェアの機能に依存するのであるならば、ソフトウェアセキュリティに関する課題解決は、必要不可欠です。コネクテッドカーといった新しい分野や、自動運転車の登場は、ソフトウェアセキュリティが担う役割の重要度を高めました。コネクテッドカーが自動車業界に豊富な機会をもたらす一方で、自動車メーカーとそのサプライヤーは、コネクテッドカーにおけるユーザーのプライバシーとセキュリティを考慮する必要があります。

オープンソースの利用は、自動車業界を含めあらゆる業界に広まっています。Black Duckのオンデマンド監査によると、オープンソースコンポーネントは自動車向け商用アプリケーションの平均23%を占めています。オープンソースがアプリケーション開発において重宝されるのには十分な理由があります。開発コストを低減し、開発期間を短縮し、イノベーションを加速するからです。しかし、使っているオープンソースを企業が十分に追跡し管理できていなければ、オープンソースのメリットもリスクになってしまいます。

ソフトウェアのセキュリティリスクは、自動車メーカーがその攻撃を可能にするバグを修正するために140万台の車両をリコールするという重大なものになりました。

オープンソースは、カスタムコードと比べても安全性に遜色はありません。しかしオープンソースには、一般的なコンポーネントの脆弱性がハッカーにとって非常に魅力的な標的になるという特徴があります。オープンソースは、事実上あらゆる形の商用および内部アプリケーションで広く利用されています。ハッカーは、オープンソースの脆弱性を攻撃することで大きな見返りがあるのです。たった1つの弱点でも、何十万ものアプリケーションとウェブサイトを危険にさらす可能性があります。オープンソースは、さまざまな経路から車載アプリケーションに侵入してきます。自動車メーカーは、数多くのコンポーネントおよびアプリケーションサプライヤーに依存しています。これらのサプライヤーは、オープンソースコンポーネントを使ってソリューションを開発すると共に、GENIVIなどのオープンソースプラットフォームを拡張する役割を担っています。

サプライヤーや自動車OEMメーカーが車両ソフトウェアに使われているオープンソースを認識できていなければ、それらのオープンソースコンポーネントの脆弱性を標的とする攻撃を防ぐことはできません。

多くの自動車メーカーとそのソフトウェアサプライヤーは、セキュリティ問題の原因となるコーディングエラーを特定するため、スタティック（静的）およびダイナミック（動的）アプリケーションセキュリティ試験（SASTおよびDAST）ツールなどの試験ツールを導入しています。SASTもDASTも、内部開発者が記述したコードに含まれるバグを特定するためには効果的ですが、現在のアプリケーションの主要コンポーネントを公開したままの状態では、サードパーティによるコードのオープンソース脆弱性を特定するためには効果的なツールであるとは言えません。2004年以降、脆弱性情報データベース（NVD）によって74,000件以上の脆弱性が公開されていますが、SASTおよびDASTツールで検出されたのはそのうち13件だけです。

国家安全保障局（NSA）は、平均的なSASTツールは、アプリケーションに含まれる問題のうちわずか14%しか発見できなかったと報告しています。同様に、DASTもコンプライアンスの検証や設定ミスの問題の発見には役立ちますが、オープンソース経由でコードに取りこまれる脆弱性を特定するためには効果的ではありません。

サプライヤーや自動車OEMメーカーが、製品のソフトウェアに使われているすべてのオープンソースを認識できていなければ、それらのオープンソースコンポーネントの脆弱性を標的とする攻撃を防ぐことはできません。企業が、コネクテッドカー技術を活用するつもりならば、そうした機能を提供するために使うソフトウェアのエコシステムを研究・検証し、セキュリティプログラムによってオープンソースの識別と管理に責任を持つ必要があります。

ソフトウェア脆弱性への対処として効果的なアプローチ

- カスタムソースコードに脆弱性がないか開発段階で精査する (SAST)
- コンパイルしたアプリケーションに共通ランタイム脆弱性がないかテストする (DAST)
- オープンソースを使用することでセキュリティ脆弱性が取りこまれていないことを開発段階で確認し、アプリケーションの展開後は、新たに報告された脆弱性を監視する(OSVM – オープンソース脆弱性管理)

オープンソースのライセンスおよびコンプライアンスのリスク

オープンソースのセキュリティリスクは多くの組織が最重要視しています。これは、HeartbleedやApache Struts 2の脆弱性へのエクスプロイトが世界中の組織に数千もの攻撃をもたらしたことが広く知られたことによるものです。オープンソースのリスクを低減していく上で、ライセンスコンプライアンスの重要性を併せて認識することも大切です。

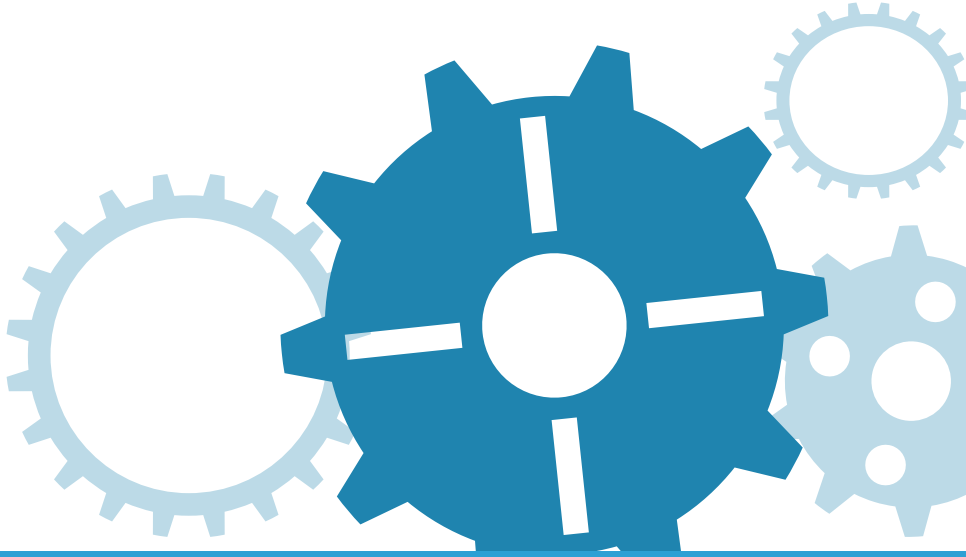
オープンソースコンポーネントのほとんどは、既知のオープンソースライセンス約2,500のいずれかの管理下にあります。その多くに義務が課せられ、様々なレベルの制限がかけられています。これらのライセンス要件は、そのライセンス要件で管理されているオープンソースコンポーネントが特定されている場合にのみ、管理および適合させることができます。オープンソースライセンスに適合していないと、企業は訴訟や知的所有権を損なうなどの重大なリスクにさらされる危険性があります。

> オープンソースコンポーネントのほとんどは既知のオープンソースライセンス約2,500のいずれかの管理下にあり、その多くに義務が課せられ、様々なレベルの制限がかけられています。

現代の自動車ソフトウェアエコシステムは、多層のデジタルサプライチェーンによって構成されています。独立した開発者はさまざまなライセンスのもとでコードを提供することができます。例えば、コンポーネントメーカーは、GENIVIコードベースを修復・増補したりして特定の自動車サブシステムに合わせるだけでなく、GENIVIプラットフォーム上で動作するソフトウェアを開発することも可能です。 この複雑さがゆえに、オープンソースコンポーネントを含んだ独自コードの所有権を含むライセンスおよびIP管理の課題が存在しています。

> 監査したアプリケーションの85%にライセンスに抵触するコンポーネントが含まれていた。

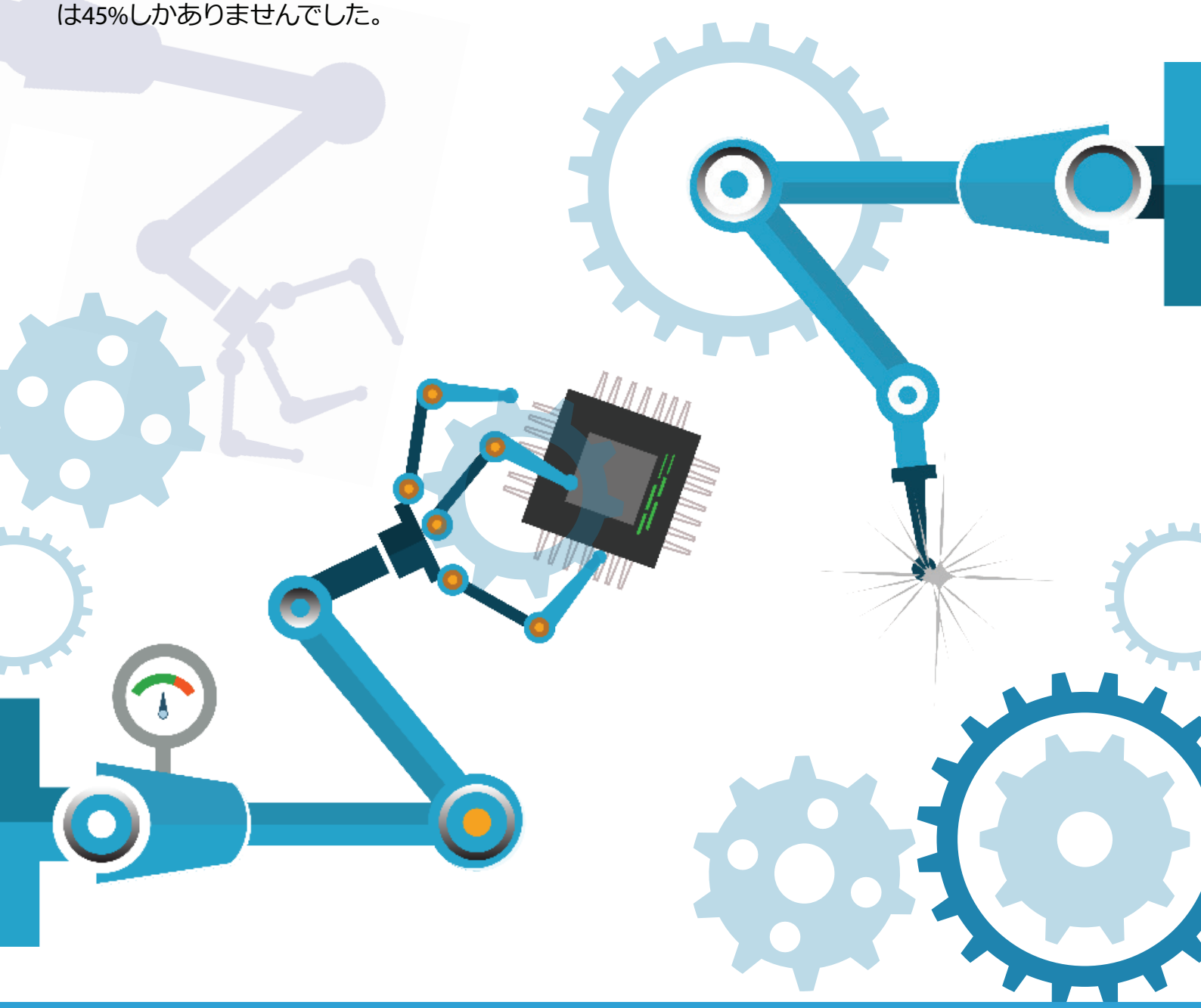
いわゆる「寛容な」オープンソースライセンスでも、使用承認や、再配布や文書化といった義務を求められるのが一般的です。また、識別可能なライセンス条件がないオープンソースコンポーネントも問題になる可能性があります。ライセンスを持たないソフトウェアとは、一般に、そのソフトウェアを使用、変更、または共有する許可を作成者から受けていないものを指します。クリエイティブな作業（コードを含む）は、デフォルトで排他的著作権のもとにあります。ライセンスによって別途指定されているのでないかぎり、他の誰も訴訟のリスクを負うことなくその作業を使用、コピー、配布、または変更することはできません。権利および義務について明確な記述がない場合、そのオープンソースを使用する組織にとって「隠れた」用語の違反リスクが高くなってしまいます。



オープンソースソフトウェアを使用する際のベストプラクティスとしては、コード内にどのコンポーネントおよび関連するライセンスがあるか、オープンソースの使用によってどのような義務が生じるかを開発者が理解することが重要となります。しかし、オープンソース使用を手動で管理することはとてつもない無駄な作業になりかねません。そのことは、Black Duckのオープンソースリサーチ&イノベーションセンター(COSRI)が行った、1,000以上の商用コードベースに対するオンデマンド監査の2017年度報告書でも報告されています。

監査によって、オープンソースライセンスへの抵触が広がっていることが明らかになった。

この監査で、オープンソースライセンス使用における「利害対立」が拡大していることがわかりました。監査したアプリケーションには、平均して147のオープンソースコンポーネントが含まれていました。つまり、膨大な数のライセンス義務を把握しなければならないということです。また、監査されたアプリケーションの85%に、ライセンスに抵触するコンポーネントが含まれていました。もっとも一般的な課題は、GPLライセンス違反です。アプリケーションの75%にGPLファミリのライセンス下にあるコンポーネントが含まれていますが、そのうちGPLの義務を遵守していたアプリケーションは45%しかありませんでした。



自動車サプライチェーン全般にわたってオープンソースリスクを管理するためのベストプラクティス

自動車OEMメーカーがソフトウェアプロバイダとの連携を強める中、ますます多くのオープンソースコンポーネントが自動車システムに進出しています。オープンソースコードは、無数のサプライチェーンを通じて、自動車エコシステムのほとんどどこにでも入り込んでいます。

オープンソースのセキュリティ脅威とコンプライアンスのリスクに対する防御策を強化・推進するため、自動車OEMとそのサプライヤーは、次のようなオープンソース管理手法を導入する必要があります。

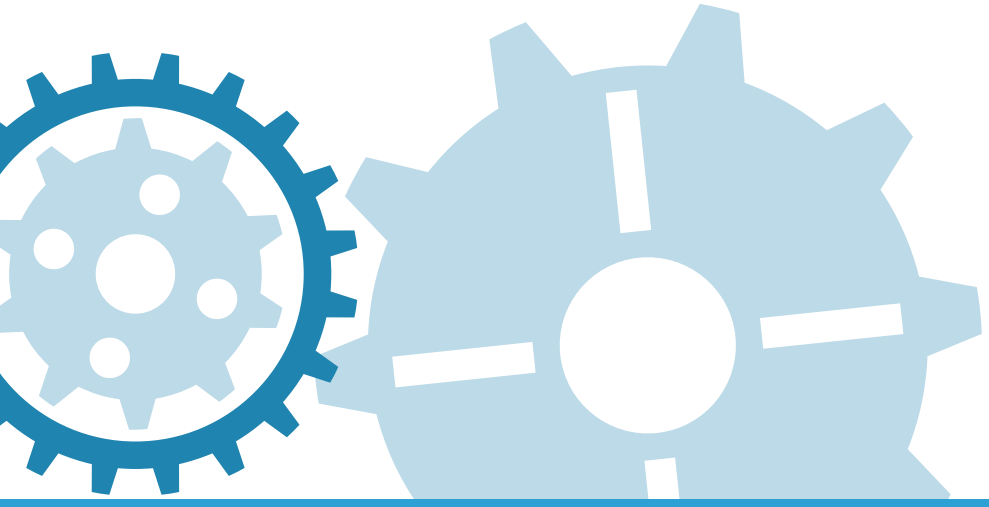
オープンソースソフトウェアの完全な棚卸：組織は、存在すら知らない脅威に対して守りを固めることはできません。アプリケーションに使用されているオープンソースの完全かつ正確な棚卸（部品表）が不可欠です。

既知のセキュリティ脆弱性にオープンソースをマッピング：脆弱性情報データベース（NVD）などの公開ソースが、オープンソースに含まれる公開されている脆弱性に関する情報を提供しています。組織はこれらのソースを参照して、使用しているオープンソースコンポーネントのどれが脆弱であるのかを特定する必要があります。

ライセンスおよび品質リスクを特定：オープンソースライセンスに準拠していないと、組織は訴訟や知的財産権の侵害などの重大なリスクにさらされる恐れがあります。同様に、古くなった、あるいは品質の低いコンポーネントを使用すると、それらを使用したアプリケーションの品質も低下してしまいます。これらのリスクも追跡して管理する必要があります。

オープンソースのリスクポリシーを強化：多くの組織では、リスクの緩和に役立つオープンソースポリシーの基本的な文書化と執行すら行われていません。手作業によるポリシーのレビューが最低限の要件とはいえ、ソフトウェア開発がさらに自動化されるにつれて、オープンソースポリシーの管理も必須になります。

新たなセキュリティ脅威に対してアンテナを張る：毎年3,500以上の新しいオープンソース脆弱性が発見されているため、アプリケーションの開発が終わってからも脆弱性を追跡し監視する仕事は続きます。アプリケーションが稼働している限り、新たな脅威を継続的に監視していく必要があります。



結論

自動車業界ではオープンソースの使用が増え続けているため、オープンソースセキュリティおよびライセンスコンプライアンスのリスクを効果的に管理することがますます重要になってきます。Black Duckなどのプロセスと自動化ソリューションをソフトウェアサプライチェーンに統合することで、自動車業界にサービスを提供している自動車メーカーやサプライヤー、テクノロジー企業は、リスクを効果的に管理しながらオープンソースのメリットを最大限に活かすことができます。

> 企業がコネクテッドカー技術を活用するつもりならば、セキュリティプログラムによるオープンソースの識別と管理も共に行う必要があります。

Black Duck Softwareソリューションは、使用するすべてのオープンソースの識別を自動化することで、コンプライアンスの問題だけでなくあらゆる既知のオープンソースセキュリティ脆弱性への可視性を提供します。オープンソースの使用とリスクポリシーを定義して実行するとともに、現在使用している車両に影響を与える可能性のある新たな脆弱性を継続的に監視します。

Black Duckのオンデマンド・オープンソース監査は、迅速かつ完全なオープンソースソフトウェアの棚卸、ライセンスコンプライアンス、セキュリティ、IPリスクの質の特定が必要な内部監査だけでなく、吸収合併（M&A）時のオープンソース適正評価の業界標準としても認められています。

組織がソフトウェアサプライチェーン全体でオープンソースのリスクを管理し安全を確保するためにBlack Duckができることについて、さらに詳しい情報はblackducksoftware.com をご覧ください。

Black Duck Softwareについて

世界中の組織がBlack Duck Software の製品を使ってオープンソースソフトウェアの安全確保と管理のプロセスを自動化し、セキュリティ脆弱性やライセンスコンプライアンス、運用リスクに関連する悩みの種を排除しています。Black Duck は、マサチューセッツ州バーリントンに本社を置き、カリフォルニア州サンノゼ、バンクーバー、ロンドン、ベルファスト、フランクフルト、香港、東京、ソウル、北京にも事業所があります。詳しい情報はこちらのサイトをご覧ください。www.blackducksoftware.com

お問い合わせ

より詳しい情報についてはこちらまでご連絡ください。
info-japan@blackducksoftware.comまたは 03-5456-5490
追加情報はこちらで提供しています。 www.blackducksoftware.com/ja