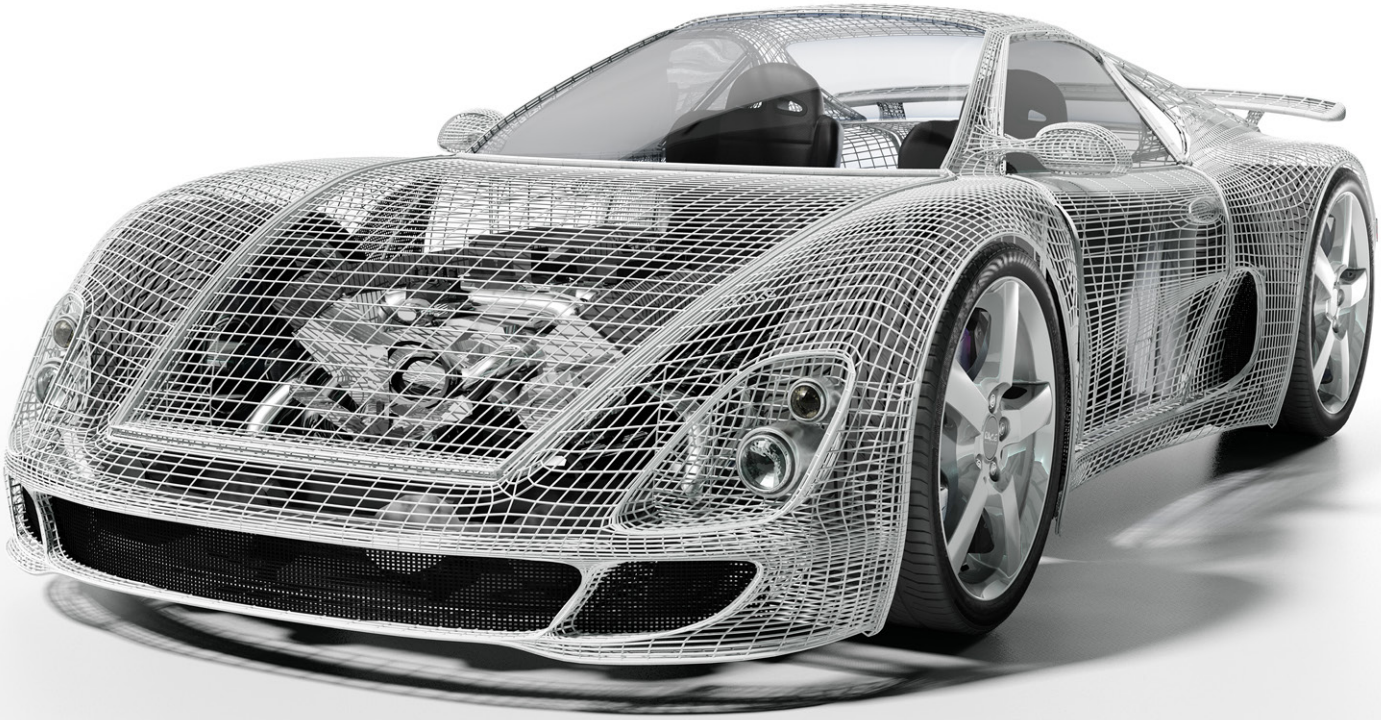
Ponemon INSTITUTE

最先端の自動車セキュリティ：

自動車業界のサイバーセキュリティ・プラクティスに関する調査



SAE International™ とシノプシスの委託による独立調査レポート

SAE INTERNATIONAL and SYNOPSYS®

目次

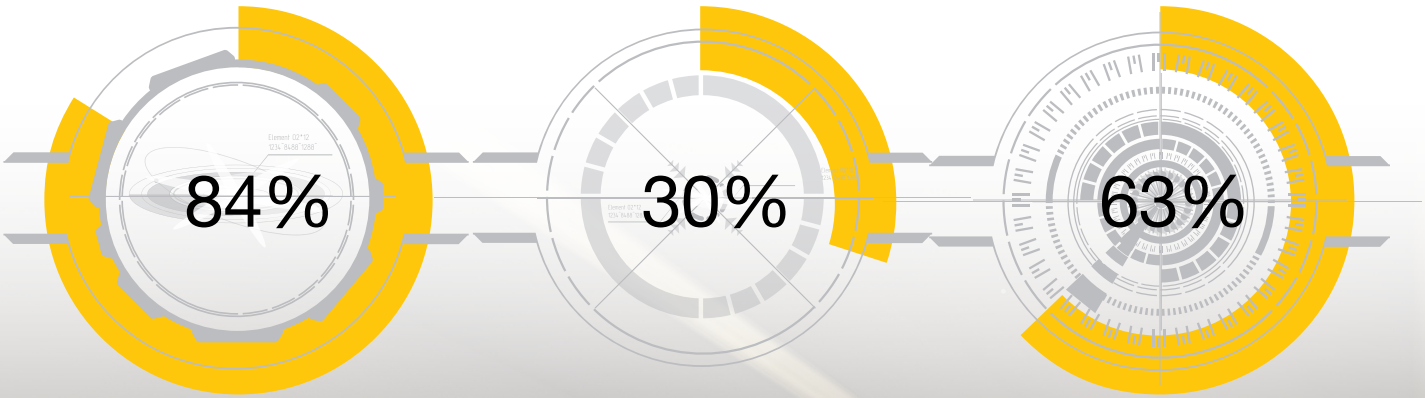
概要

今日の自動車は、ネットワーク機能を備えた「走るコンピュータ」へと変貌しており、自動車業界はサイバーセキュリティ・リスクというこれまで経験したことのない問題への対処に迫られています。自動車メーカーは今やソフトウェア企業としての顔を持ち、ソフトウェア・セキュリティに関するあらゆる課題に直面しています。

これまで、自動車業界ではサイバーセキュリティの現状とソフトウェアに支えられたコネクテッド・カーに内在するソフトウェア・セキュリティ・リスクを理解するためのデータが欠けていました。このレポートは、こうしたギャップを埋めることを目的として、シノプシスと SAE International からの委託を受けた Ponemon Institute が自動車業界における現在のサイバーセキュリティ・プラクティスについて独立調査を実施したものです。今回の調査は、車載コンポーネントのセキュリティの実装または評価に携わっている 593 人のプロフェッショナルを対象に実施しました。

自動車業界のテクノロジの変化にソフトウェア・セキュリティが追いついていない現状が明らかに

ソフトウェアが自動車の安全を左右するようになった今、特にコネクテッド・カーや自動運転車などの新しい領域では、ソフトウェア・セキュリティの課題が特に重要になっています。しかし今回の調査で明らかになったように、自動車メーカー（OEM）とサプライヤは製品に使用しているテクノロジのセキュリティ対策に大きな課題を抱えています。今回の調査では、刻々と変化するセキュリティ動向にサイバーセキュリティ・プラクティスが追いついていないと懸念していると回答者が 84% にのぼっています。



「サイバーセキュリティ・プラクティスがテクノロジの変化に追いついていない」と答えた回答者

「製品サイバーセキュリティに関する正式なプログラムやチームを設立していない」と答えた回答者

「全体の半分未満しかハードウェア、ソフトウェア、その他のテクノロジの脆弱性テストを実施していない」と答えた回答者

自動車業界の企業は、サイバーセキュリティに必要なスキルとリソースを増強しつつありますが、まだ十分なレベルに達していません。今回、セキュリティ・プロフェッショナルから寄せられた回答によると、自動車業界の企業で製品サイバーセキュリティ管理プログラムにフルタイムで従事している従業員は平均 9 人にとどまっていることがわかりました。製品のサイバーセキュリティに関する正式なプログラムやチームを設立していないと答えた企業も 30% にのぼっています。また、ハードウェア、ソフトウェア、その他のテクノロジの半分未満しか脆弱性テストを実施していないと答えた回答者は 63% にのぼっています。

ソフトウェア脆弱性が生じる主な要因としては、製品納期までの余裕がない、意図しないコーディング・エラー、セキュア・コーディング・プラクティスに関するトレーニングの欠如、製品リリース・プロセスの終盤まで脆弱性テストが行われていない、などの点が挙げられています。今回の調査では、セキュア・コーディングのトレーニング、ソース・コードの不具合とセキュリティ脆弱性の自動検知ツール、サプライヤによって導入されたサードパーティ・コンポーネントを特定するソフトウェア・コンポジション解析ツールなど、サイバーセキュリティをより一層重視する必要があることが明らかになっています。

自動車サプライチェーンではソフトウェアが大きなリスクに

ほとんどの自動車メーカー（OEM）がまだ自社生産の装置も手がけていますが、それよりも研究開発、車両の設計・販売、部品サプライチェーンの管理、および最終製品の組み立てが主な強みとなっています。OEM は数百社もの独立系ベンダーから納入されるハードウェア / ソフトウェア・コンポーネントを利用して、最先端の車両テクノロジ / デザインを完成させています。

今回の調査では、回答者の 73% がサードパーティから納入される車載テクノロジのサイバーセキュリティに非常に懸念を持っていると答えています。ただし、上流サプライヤから供給される製品に対してサイバーセキュリティに関する要求事項を課していると答えた企業は 44% にとどまっています。

コネクテッド・カー特有のセキュリティ課題

OEM とサプライヤは、コネクテッド・カーがコンシューマのプライバシーとセキュリティに与える影響も考慮する必要があります。コネクテッド・カーの普及に伴い、悪意のあるハッカーがセルラー・ネットワーク、Wi-Fi、あるいは物理的な接続を利用して自動車にアクセスし、ソフトウェア脆弱性を悪用できるようになっています。こうしたリスクに対処できないと、消費者からの信頼、個人のプライバシー、ブランドの評判などの面で非常に大きな損害を被るおそれがあります。

今回の調査では、特にリスクの大きいテクノロジとして、無線テクノロジ（Wi-Fi、Bluetooth など）、テレマティクス、自動運転車などが挙げられています。このことは、安全系以外のシステムやコネクティビティが攻撃の格好の標的となるため、特に重点的なサイバーセキュリティ対策が必要であることを示唆しています。

まとめ

この後のレポートで詳細を示すように、今回の調査では業界のさまざまなセクターの回答者がサイバーセキュリティの問題を大いに認識しており、改善に向けた強い意欲を持っていることが明らかになりました。気がかりなのは、回答者の 69% がこうした懸念を上層部に報告する権限がないと感じていることです。このレポートが、取締役 / 理事レベルの方に問題の所在を可視化する上で一助となることを期待します。

リーン生産方式と ISO 9000 のプラクティスが自動車産業に品質向上をもたらしたのと同様、サイバーセキュリティに対する厳格なアプローチは、品質、安全、短納期を維持しながら最先端の車載テクノロジのメリットを最大限に引き出す上で重要な役割を果たします。

組織の現状と課題

多くの回答者が危険の存在を明確に認めているものの、サイバーセキュリティに関する懸念を上層部に報告できる権限がないと感じています。

今後 12 か月のうちに車載テクノロジに対する攻撃（セキュリティ研究者による実験を含む）を受ける可能性が高い、または非常に高いとした回答は 62% ありましたが、そのような懸念を上層部に報告する権限を与えられていないと感じている回答者が 69% にのぼっています。

図 1 に示すように、回答者の半数以上（52%）がサードパーティまたは自社で開発した車載テクノロジにセキュリティ不具合があった場合、ドライバーに危険が及ぶ可能性があることを認識しています。ただし、セキュリティに関する懸念を上層部に報告できる権限が与えられていると感じている回答者は 31% にとどまっています。

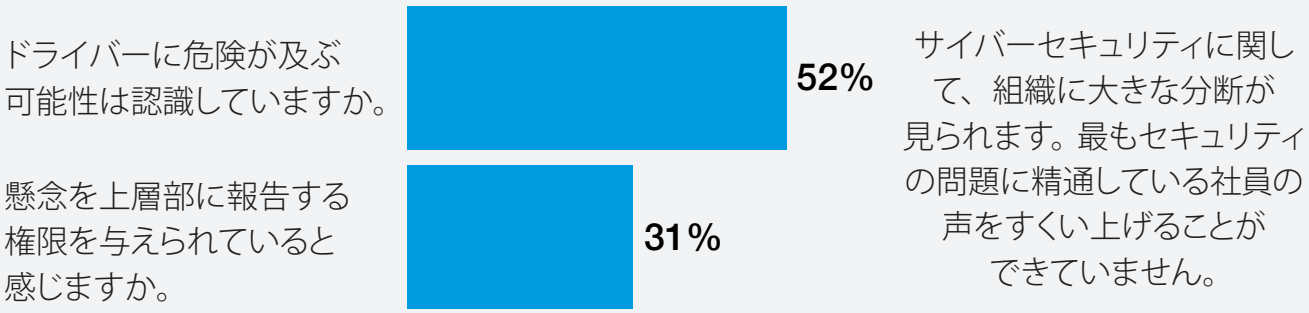


図 1：ドライバーに危険が及ぶ可能性は認識されているものの、その懸念は声なき声に終わっています。（「はい」の回答を集計）

こうした懸念があるにもかかわらず、製品のサイバーセキュリティに関するチームやプログラムの設立は進んでいません。

あなたの企業が開発または使用している車載ソフトウェア / テクノロジ / コンポーネントが、今後 12 か月のうちに攻撃（セキュリティ研究者による実験を含む）を受ける可能性がどれだけあると考えますか。	**・ 非常に高い 27%**
	・ 高い 35%
	・ やや高い 23%
	・ 低い 15%

車載テクノロジのセキュリティに関する懸念を、あなたの企業の上層部に報告する権限が与えられていると感じますか。	・ はい 31%
	・ いいえ 69%

回答者全体の 30% が、製品のサイバーセキュリティに関する正式なプログラムやチームを設立していないと答えています。複数の製品開発チームを指導、サポートする製品サイバーセキュリティ・チームを中央に設置していると答えた企業は 10% にとどまっています。

あなたの企業の製品サイバーセキュリティに対するアプローチとして、最もあてはまるものを 1 つ選んでください。	・ 伝統的な IT サイバーセキュリティ・チームが（主に全社的な CISO の指揮のもとで）製品のサイバーセキュリティを担当している	20%
	・ 機能安全チームが製品のサイバーセキュリティを担当している	17%
	・ 複数の製品開発チームを指導、サポートする製品サイバーセキュリティ・チーム（センター・オブ・エクセレンス）を中央に設置している	10%
	・ 中央ではなく、個々の製品開発チームごとにサイバーセキュリティ専門家を含む製品サイバーセキュリティ・チームを設置している	23%
	・ 製品のサイバーセキュリティに関する正式なプログラムやチームを設立していない	**30%**

上記のデータを OEM/ サプライヤ別に見てみると（図 2）、製品のサイバーセキュリティに関する正式なプログラムやチームを設立していないと答えた回答者は、OEM では 18% ですが、サプライヤでは 41% に達しています。

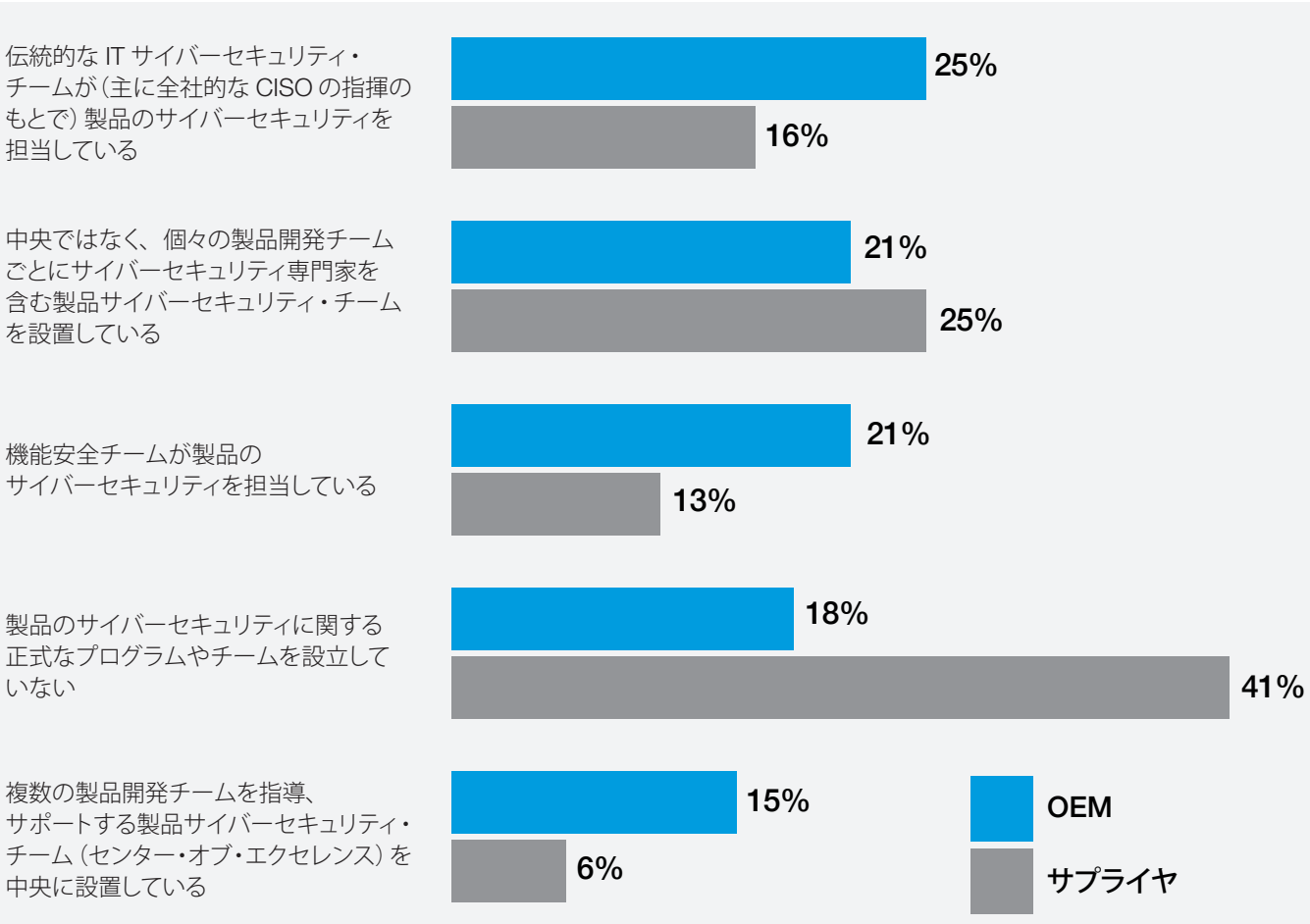


図 2：あなたの企業の製品サイバーセキュリティに対するアプローチを 1 つ選んでください。

設計フェーズから廃棄まで製品開発プロセス全体を通じて、専門家チームがセキュリティ・テストを実施することがベスト・プラクティスとされていますが、非常に多くのサプライヤがこの点を見落としています。

自動車業界の企業では、サイバーセキュリティに関するリソースとスキルが不足しています。

回答者の大半が、自動車業界におけるサイバーセキュリティの脅威に対抗するのに必要なリソースが不足していると考えています。

平均して、企業の製品サイバーセキュリティ管理プログラムにフルタイムで従事している従業員は 9 人しかいません。62% の企業が、サイバーセキュリティに必要なスキルが不足していると答えています。また、サイバーセキュリティ・リスクに対処するのに十分な予算と人的資源が割り当てられていないと答えた回答者も半分以上 (51%) に達しています。

あなたの企業はサイバーセキュリティに十分なリソース (予算および人的資源) を割り当てていますか。	・ はい	49%
	・ いいえ	**51%**
あなたの企業は製品開発に必要なサイバーセキュリティ・スキルを備えていますか。	・ はい	38%
	・ いいえ	**62%**
あなたの企業の製品サイバーセキュリティ管理プログラムに従事する従業員のフルタイム当量は何人分ですか。	**・ 5 人未満**	**30%**
	・ 5 ～ 10 人	**44%**
	・ 11 ～ 20 人	**18%**
	・ 20 人以上	8%

技術の現状と課題

現在の自動車は、制御システム、膨大なデータ、インフォテインメント、さまざまなプロトコルを利用した無線メッシュ接続などで構成された「モバイル IT エンタープライズ」の様相を呈しています。このコネクティビティにより、自動車はドライバーが所有する電子機器、他の車両や道路インフラ、さらにはインターネットを介して OEM やアフターサービス・アプリケーションにも接続しており、これらがすべてサイバー攻撃の標的となってしまいます。車両ネットワークへの不正なリモート・アクセスにより、安全系システムが攻撃を受けてしまうと、ドライバーの個人情報だけでなく、身体の安全も危険にさらされることになります。

今回の調査では、自動車エンジニア、製品開発者、IT プロフェッショナルにセキュリティ上の大きな懸念を聞くとともに、リスク軽減のために使用しているセキュリティ・コントロールについても挙げてもらいました。

SPEED LIMIT 10

回答者のほとんど (84%) は、サイバーセキュリティ・プラクティスがテクノロジの変化に追いついていないことを懸念しています。

あなたの企業のサイバーセキュリティ・プラクティスが車載テクノロジの変化に追いついていない懸念はありますか。 (1 = 懸念がない、10 = 非常に懸念がある)	・ 1 ～ 2	5%
	・ 3 ～ 4	11%
	・ 5 ～ 6	**25%**
	・ 7 ～ 8	**22%**
	・ 9 ～ 10	**37%**

特にリスクの大きいテクノロジとして、無線テクノロジ、テレマティクス、自動運転車が挙げられています。自動車への採用が進む先端テクノロジのうち、これら 3 つはサイバーセキュリティにとって最も大きなリスクになると考えられています。したがって、企業のリソースをこれらテクノロジのリスク軽減に重点的に割り当てることが推奨されます。

また、車載テクノロジに脆弱性が混入する主な要因としては、製品納期までの余裕がない (71%)、セキュア・コーディング・プラクティスに対する理解 / トレーニングの欠如 (60%)、意図しないコーディング・エラー (55%) が挙げられています。主要なスタッフに対してセキュア・コーディングのトレーニングを実施することにより、自動車におけるソフトウェア脆弱性の最大要因の 2 つを改善できます。

次のテクノロジのうち、サイバーセキュリティにとって最も大きなリスクとなるのはどれですか。 当てはまるものをすべて選んでください。	・ インフォテインメント・システム	31%
	・ パワートレイン制御ユニット	46%
	・ SoC (システム・オン・チップ) ベースのコンポーネント	44%
	・ 自動運転車	**58%**
	・ ソフトウェア主体のサービス・プロバイダ (クラウド、保険業者、ストリーミング・サービスなど)	51%
	・ テレマティクス	**60%**
	・ 操舵システム	45%
	・ 電動化部品	17%
	・ カメラ	29%
	・ 無線テクノロジ (Wi-Fi、Bluetooth、ホットスポットなど)	**63%**

あなたの企業が開発または使用している車載テクノロジに脆弱性が混入する主な要因は何ですか。 最もあてはまるものを4つ選んでください。	**・意図しないコーディング・エラー**	**55%**
	・セキュアでない / 最新でないオープンソース・ソフトウェア・コンポーネントの使用	40%
	・開発段階の不正なコード・インジェクション	23%
	・セキュリティ要件を明確化した社内ポリシー / ルールの欠如	26%
	・セキュア・コーディング・プラクティスに関する理解 / トレーニングの欠如	**60%**
	・製品納期までの余裕がない	**71%**
	・品質保証およびテストの手順が確立されていない	50%
	・製品開発ツールに内在するバグ	39%
	・不適切なパーミッション	19%
	・脆弱なバックエンド・システム	15%

セキュリティ・パッチ / アップデートが課題となっています。

重大なセキュリティ脆弱性に迅速に対応できるソフトウェア・アップデート配布モデルを採用していると答えた回答者は 39% にとどまっています。

あなたの企業のソフトウェア・アップデート配布モデルは、重大なセキュリティ脆弱性に迅速に対応できていますか。	・はい	39%
	・いいえ	**61%**

図 3 に示すように、販売後の車両に対するセキュリティ・パッチ / アップデートは、65% が外部調達したソフトウェア、コンポーネント、システムを利用して提供しています。51% は、ユーザーが所有する電子 / コンピューティング機器との無線通信を利用すると答えています。

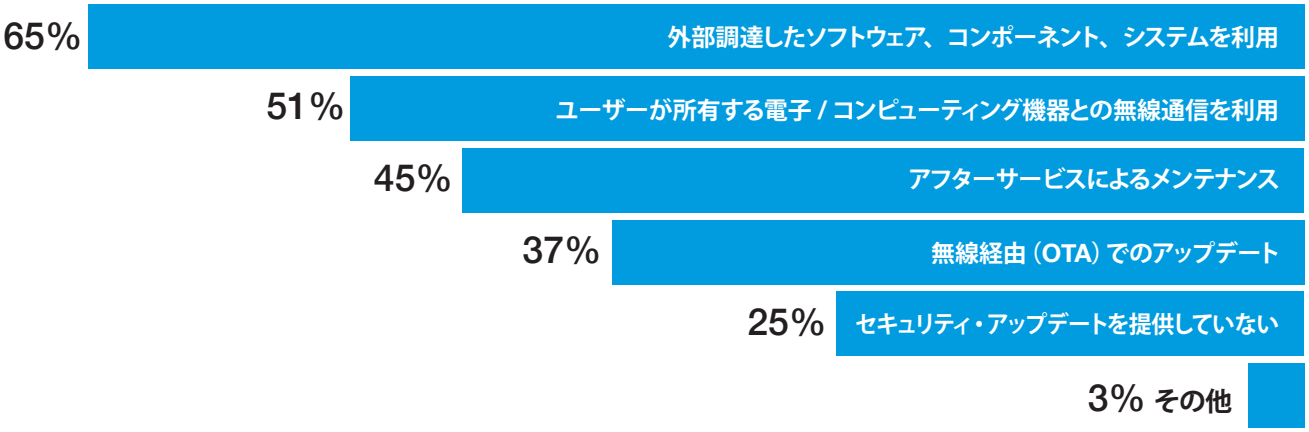


図 3：あなたの企業では、どのような方法で販売後の車両にセキュリティ・パッチ / アップデートを配布していますか。

現在、無線経由（OTA）でセキュリティ・パッチを配布していると答えた回答者は 37% でしたが、今後 5 年以内にその計画があると答えた回答者は 50% を超えています。このことは、セキュアな OTA アップデートに関する業界標準の必要性を示唆しています。

現在 OTA によるアップデートを提供していないと答えた方は、今後その計画がありますか。	**・ 1 ～ 3 年以内**	**33%**
	・ 3 ～ 5 年以内	**23%**
	・ 5 年以上	**9%**
	・ OTA アップデート提供の計画なし	35%

車両に搭載されるセキュリティ・コントロールとして最も一般的なのが、ファイアウォールとゲートウェイです。

主要なセキュリティ・コントロールとしてファイアウォールを挙げた回答者は 64%、ゲートウェイを挙げた回答者は 59% でした。

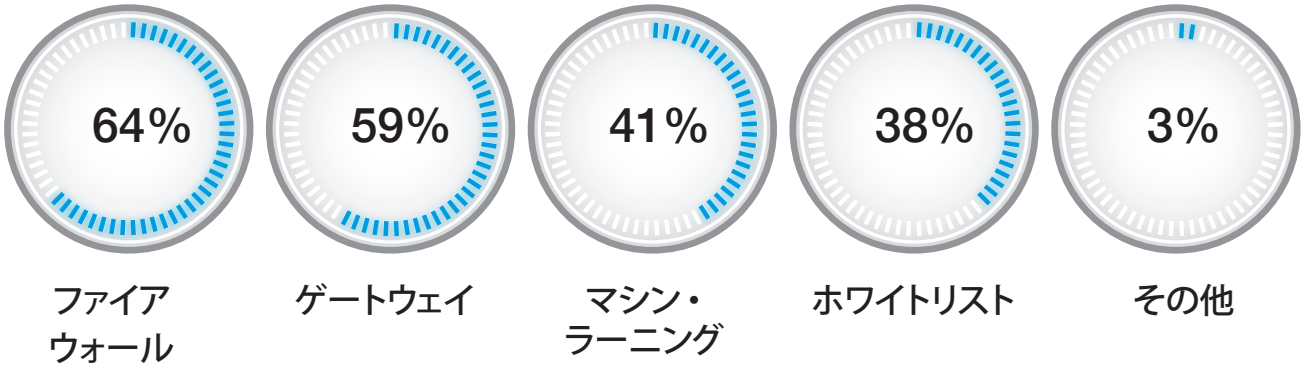


図 4：あなたの企業では、車両に何らかのセキュリティ対策を採用していますか。

大半の企業が鍵管理システムを使用していますが、43% がまだ手動プロセスに頼っています。

鍵管理システム（暗号鍵の管理：生成、交換、保管、使用、置換を含む）を使用していると答えた企業は 63% ありました。図 5 に示すように、56% が中央の鍵管理システム / サーバを使用しており、45% が正式な鍵管理ポリシーを使用しています。しかし 43% は手動プロセスによる鍵管理に頼っており、セキュリティ向上の効果が十分に現れていません。

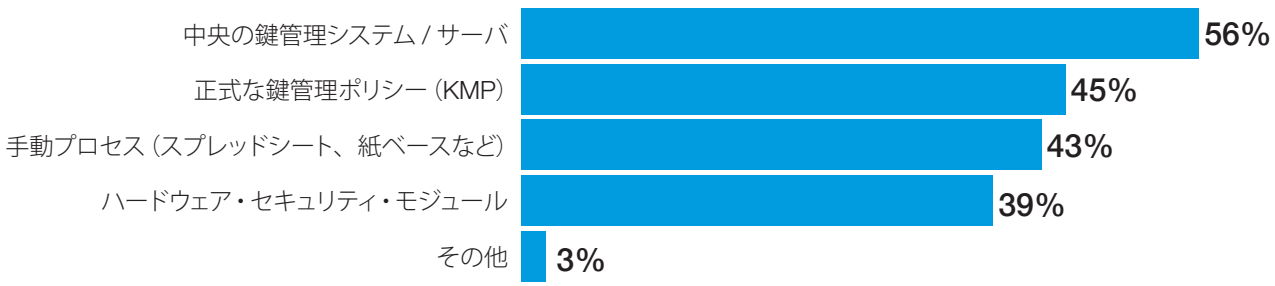


図 5：あなたの企業では現在どのような鍵管理システムを使用していますか。

製品開発およびセキュリティ・テストのプラクティス

今回の調査では、企業が製品開発に採用しているセキュリティ・プラクティスについても質問しました。サイバーセキュリティにおいて、リスク・ベースのプロセス駆動型アプローチを製品開発ライフサイクル全体に統合して使用することがベスト・プラクティスとして確立されています。

今回の調査では、セキュリティ脆弱性の評価が製品リリース・プロセスの終盤まで行われていないことが明らかになりました。

要件定義 / 設計フェーズ、または開発 / テスト・フェーズで脆弱性を評価している企業は 47% にとどまっています（図 6）。

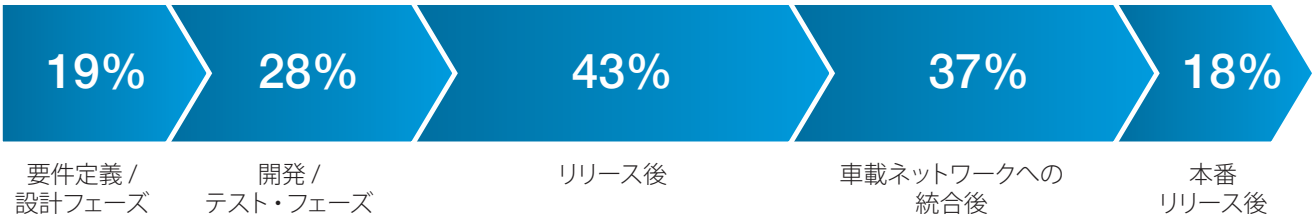


図 6：あなたの企業では、開発ライフサイクルのどの時点で車載ソフトウェア / テクノロジ / コンポーネントのセキュリティ脆弱性を評価していますか。

『SAE J3061™ Cybersecurity Guidebook for Cyber-Physical Vehicle Systems』[1] ではサイバーセキュリティを製品開発ライフサイクル全体に統合したリスク・ベースのプロセス駆動型アプローチが提唱されていますが、現状は違います。

セキュリティを製品開発に統合することの利点

1. 製品設計にセキュリティ・コンセプトを統合した方が、本番リリース後にセキュリティ・コントロールを適用するよりも高いセキュリティを実現できます。
2. リスクと脆弱性を早期段階で特定し、適切なセキュリティ・コントロールを適用できます。
3. こうすると、限りあるサイバーセキュリティ・リソースをはるかに有効に適用でき、サイバーセキュリティのコストを製品開発の重要な一部として標準化できます。

J3061 は世界初の自動車向けサイバーセキュリティ・スタンダードで、サイバーセキュリティ・プロセスを製品開発に組み込むためのツールとして非常に役立ちます。

[1] 『SAE J3061™ Cybersecurity Guidebook for Cyber-Physical Vehicle Systems』SAE International、2016 年 1 月

セキュリティ・テストが不十分であることにより、脆弱性が見落とされています。

回答者の 63% が、ハードウェア、ソフトウェア、その他のテクノロジの半分未満しか脆弱性テストを実施していないと答えています。また、製品納期までの余裕がないことがセキュリティ脆弱性の最大の要因であると答えた回答者は 71% にのぼっています。このことは、製品の納期遅れを防ぐためにソフトウェア / テクノロジ / コンポーネントのテストが十分に実施されていないことを示唆しています。

あなたの企業が使用している車載テクノロジの何パーセントがサイバーセキュリティ脆弱性のテストを受けていますか。	**・ なし**	**25%**
	・ 25%以下	**12%**
	・ 26% ～ 50%	**26%**
	・ 51% ～ 75%	23%
	・ 76% ～ 100%	14%
	合計	100%
あなたの企業が使用している車載テクノロジにセキュリティ不具合があった場合、ビジネスにどのような悪影響が及びますか。	・ セキュリティ問題によるリコール	21%
	・ サプライチェーンのパートナー関係への損害	54%
	・ 納期の遅れ	**67%**
	・ コンポーネント間の意図しない行動を統合テストで発見	**59%**
	・ 法律違反による制裁措置や罰金	5%
	・ 悪影響が生じることは認識していない	29%
あなたの企業が使用している車載テクノロジに脆弱性が混入する最大の要因は何ですか。	・ 意図しないコーディング・エラー	55%
	・ セキュアでない / 最新でないオープンソース・ソフトウェア・コンポーネントの使用	40%
	・ 開発段階の不正なコード・インジェクション	23%
	・ セキュリティ要件を明確化した社内ポリシー / ルールの欠如	26%
	・ セキュア・コーディング・プラクティスに関する理解 / トレーニングの欠如	60%
	・ 製品納期までの余裕がない	**71%**
	・ 品質保証およびテストの手順が確立されていない	50%
	・ 製品開発ツールに内在するバグ	39%
	・ 不適切なパーミッション	19%
	・ 脆弱なバックエンド・システム	15%

脆弱性を防ごうと努力する一方で、納期までの余裕がないためにセキュリティ・テストを十分に実施できていないことが、脆弱性が見落とされる要因となっています。

脆弱性および品質の問題が生じる原因は、セキュア・ソフトウェア開発ライフサイクル（SSDLC）プラクティスを一貫して適用していないことにあります。

回答者の 36% が、広く認知された SSDLC プラクティスを採用しておらず、セキュア・コーディング・プラクティスに対する理解 / トレーニングが欠如していると答えた回答者も 60% ありました。

あなたの企業は、車載ソフトウェア / テクノロジ / コンポーネントに対して社内または外部で発行されたセキュア・ソフトウェア開発ライフサイクル（SSDLC）プロセスに従っていますか。	・ はい（社内のプロセス）	35%
	・ はい（社外のプロセス）	29%
	・ いいえ	**36%**

回答者の60%が、セキュア・コーディング・プラクティスに対する理解/トレーニングの欠如が車載ソフトウェア/テクノロジ/コンポーネントの脆弱性につながっていると答えています。意図しないコーディング・エラーを挙げた回答者も 55% ありました。

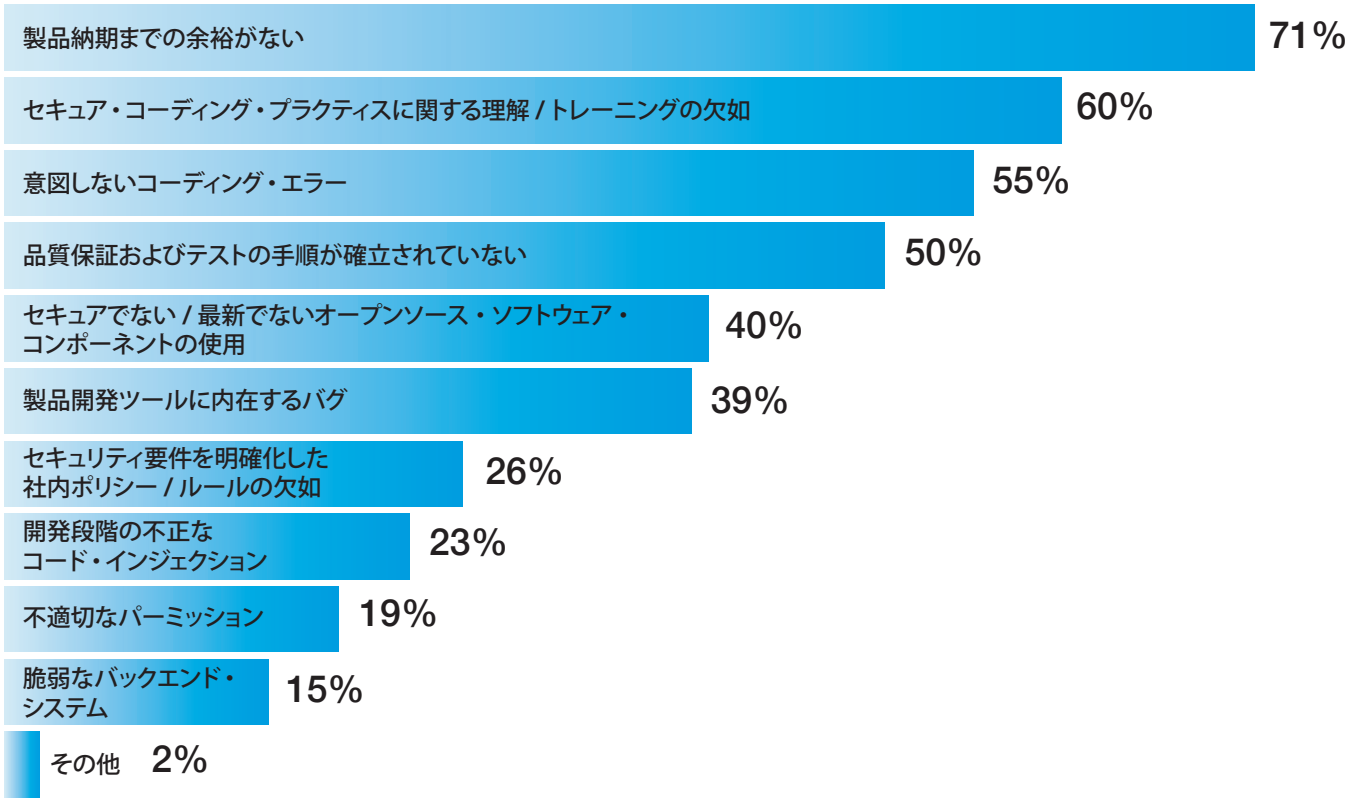


図 7：車載ソフトウェア / テクノロジ / コンポーネントに脆弱性が混入する最大の要因は何ですか。

セキュリティ・アクティビティとして業界で最もよく実施されているのが、セキュリティ・パッチ管理、ペネトレーション・テスト、ダイナミック・アプリケーション・セキュリティ・テスト（DAST）です。

車載テクノロジのセキュリティを確保する手法として多くの回答者が挙げたのは、セキュリティ・パッチ管理（61%）、ペネトレーション・テスト（56%）、ダイナミック・アプリケーション・セキュリティ・テスト /DAST（49%）でした。興味深いのは、これらはいずれもライフサイクルの終盤に使用される手法であるということです。

ここでも、サイバーセキュリティがシステム開発ライフサイクル（特に初期の要件定義、設計、テストおよび開発フェーズ）に十分に統合されていない事実がうかがえます。

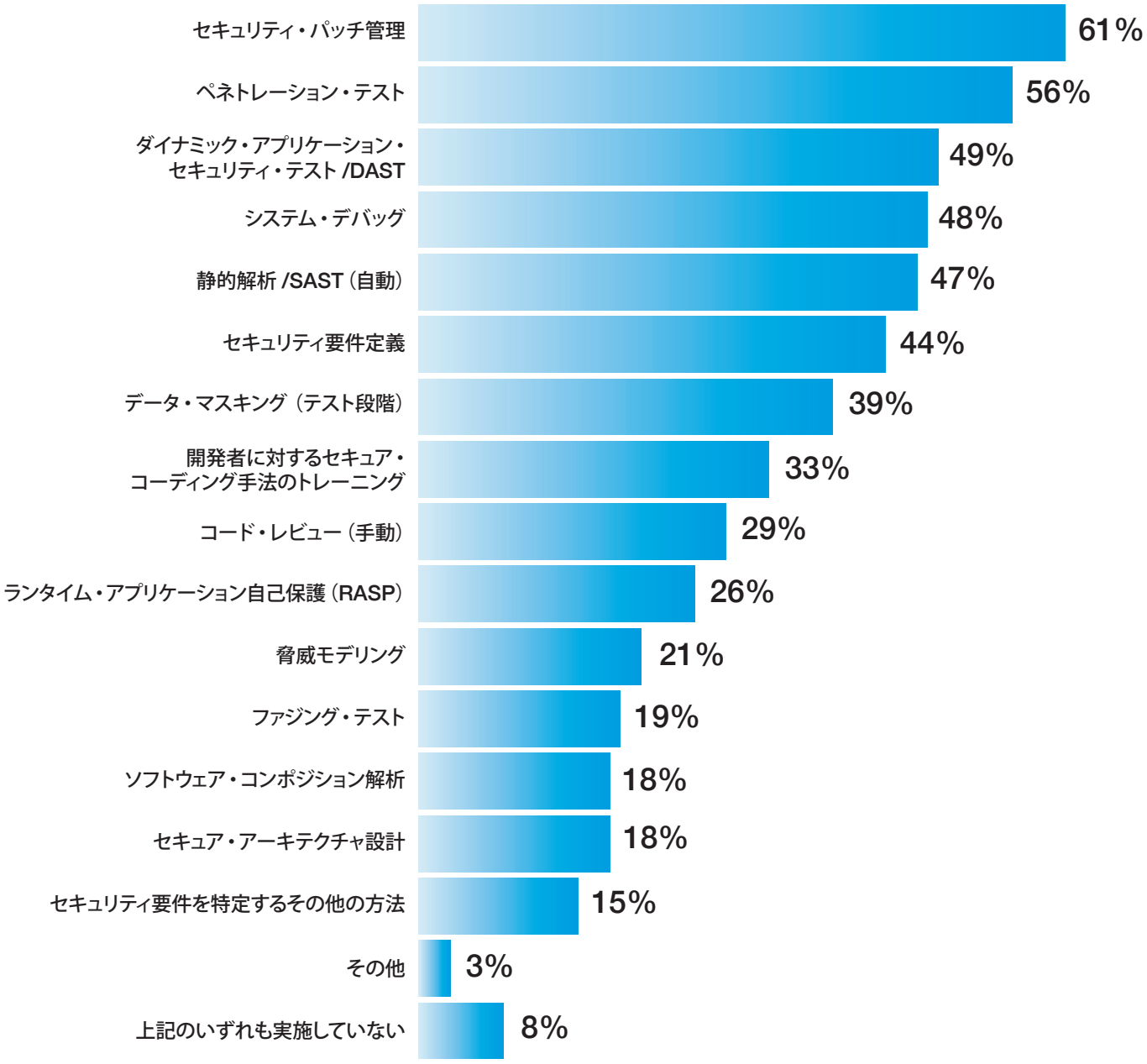


図 8：あなたの企業では、車載ソフトウェア / テクノロジ / コンポーネントのセキュリティを確保するためにどのようなアクティビティを実施していますか。

サプライチェーンおよび サードパーティ・コンポーネントの課題

自動車業界のサプライチェーンは多様な要素が複雑に絡み合って構成されており、このことが品質の問題、ひいてはセキュリティ脆弱性を生む大きな要因となっています。OEM は、サードパーティ製のコンポーネント、ソフトウェア、通信プロトコル、アプリケーションの頻繁な統合によって生じる攻撃経路に対処する必要があります。今回の調査からは、これらの要因に関連する重要な知見がいくつか得られています。

自動車業界では、サプライチェーンの脆弱性が大きなリスクとなっています。

回答者の 73% が、サードパーティから納入される車載テクノロジのサイバーセキュリティに非常に懸念を持っていると答えています。自動車業界全体としてのサイバーセキュリティに非常に懸念を持っているという回答者も 68% ありました。

上流サプライヤから供給される製品に対してサイバーセキュリティに関する要求事項を課していると答えた企業は 44% にとどまっています。メーカーには、サプライヤから納入されるソフトウェア / ハードウェア / システムに対する技術的な要求事項だけでなく適切なセキュリティ要求事項も作成する取り組みが求められます。

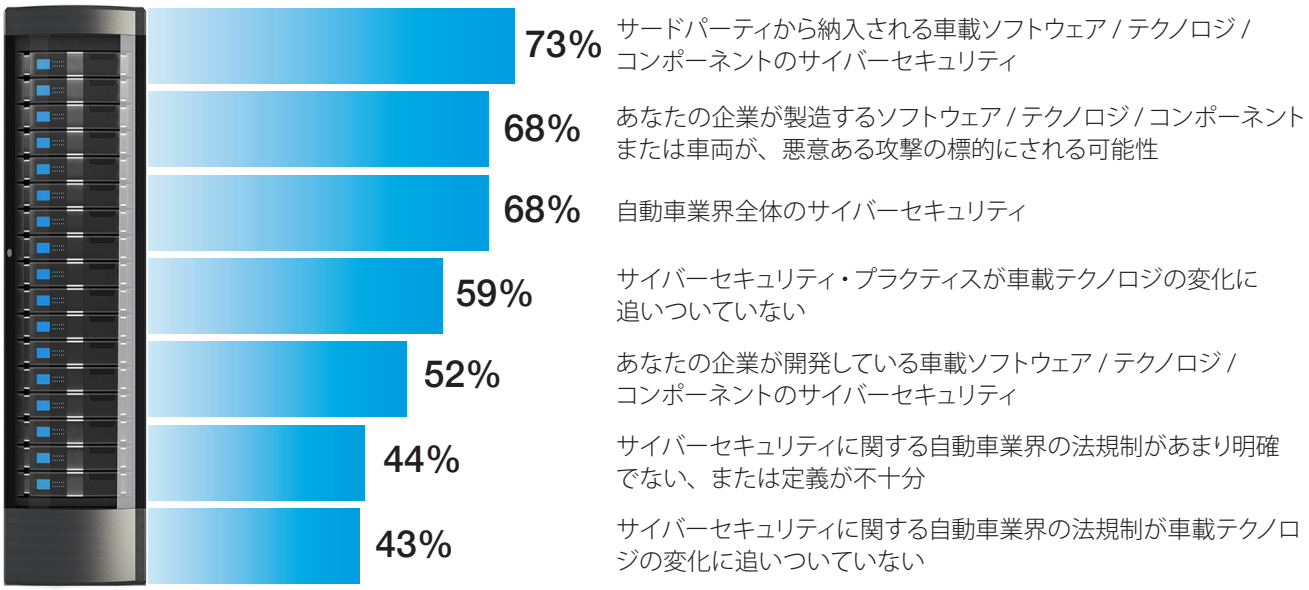


図 9：サイバーセキュリティとそのプラクティスに対して非常に高い懸念
（1 = 懸念がない、10 = 非常に懸念がある、として 7 以上の回答を集計）

セキュア・コーディング手法のトレーニングに重点が置かれていません。

セキュア・コーディング手法のトレーニングを実施している企業は 33% にとどまっています。そして回答者の 60% が、セキュア・コーディング・プラクティスに対する理解 / トレーニングの欠如が脆弱性につながる最大の要因であると答えています。

あなたの企業では、車載ソフトウェア / テクノロジ / コンポーネントのセキュリティを確保するためにどのようなアクティビティを実施していますか。	**・ 開発者に対するセキュア・コーディング手法のトレーニング**	**33%**

まとめ

今回の調査で、回答者はサイバーセキュリティの課題に直面していることを十分に認識し、改善に向けた意欲も持っているものの、こうした問題を上層部へ報告する権限が与えられていないと感じているため、その意欲が十分に発揮されていないことが明らかになりました。サイバーセキュリティでおそらく最も重要なのは、製品開発プロセス全体に統合することですが、回答者はそのことを非常によく理解しています。

人、プロセス、テクノロジの最適な組み合わせを見つけることが成功の鍵を握ります。すでにセキュリティ・イニシアティブに携わっているセキュリティ・プロフェッショナル、および効率的かつ効果的なアプローチの開発に初めて携わる方にとって参考になるソリューションとして、以下のリソースがあります。

- 『SAE J3061™ Cybersecurity Guidebook for Cyber-Physical Vehicle Systems』で説明されているサイバーセキュリティ・プロセスのフレームワークをベースにして、企業は車両システムを設計してサイバーセキュリティを組み込む際の社内向けサイバーセキュリティ・プロセスを策定できます。
- 米国国立標準技術研究所（NIST）からは、セキュリティの知識とベスト・プラクティスについて役立つリソースが無償で提供されています（NIST SP800 シリーズなど）。
- 『セキュア開発成熟度モデル（BSIMM）』およびシノプシスの「オートモーティブ・セキュリティ」リソース・ページでは、企業がセキュリティ・イニシアティブを策定し、車載ソフトウェアのセキュリティ、安全、信頼性、コンプライアンス要件を満たすのに役立つ情報を提供しています。

これらのソリューションでは、サイバーセキュリティを製品開発ライフサイクルおよびセキュア・ソフトウェア開発ライフサイクル全体に統合したリスク・ベースのプロセス駆動型アプローチを作成、利用することが提唱されています。

今回の調査では、サイバーセキュリティに関するトレーニングが十分でないことを多くの回答者が指摘していました。トレーニングへの投資は、こうした課題を解決するだけでなく、企業全体でセキュリティ文化を育成することにもつながるため、長期的に大きな意味があります。

また、自動車業界には最新のセキュリティ課題およびトレンドに関する知識の習得、プロフェッショナル同士のネットワーク作り、および業界全体のセキュリティ向上への貢献に役立つリソースもあります。

- Automotive Information Sharing and Analysis Center（Auto-ISAC）のフォーラムでは、セキュリティ・プロフェッショナル同士が自動車に対する最新のサイバーセキュリティ・リスクについての情報を交換、分析でき、自動車業界全体としてサイバーセキュリティの強化が促されます。
- SAE International では、いくつかのグループがサイバーセキュリティに関するスタンダード、ガイドライン、ベスト・プラクティスを策定しているほか、専門能力開発トレーニングの実施、各種カンファレンス / イベントの主催を通じ、自動車業界に最先端のプラクティスを広める活動を展開しています。

このレポートで指摘したように、サプライチェーンのリスクに関する懸念は、開発ライフサイクルの要件定義フェーズに十分な注意を払うことによって対処、軽減できます。そのためには、サプライヤと緊密に協力し、コンポーネントの設計またはアーキテクチャに潜む弱点を洗い出す作業も必要になることがあります。サプライヤのサイバーセキュリティ・プロセスを定期的に評価し、サプライヤ契約にサイバーセキュリティの保証に関する要求事項を盛り込むことによって、さらに高い保証レベルを達成できます。

サイバーセキュリティをコスト・センターと見なして開発プロセスの終盤に後付けで対処するのではなく、システム・エンジニアリング・プロセスのすべての工程にサイバーセキュリティを組み込み、製品開発ライフサイクル全体をサイバーセキュリティ主導で進め、セキュア・ソフトウェア開発ライフサイクル（SSDLC）を確立することが推奨されます。幸い、他の業界で作成された既存のガイダンス、ベスト・プラクティス、スタンダードが数多く存在しており、自動車業界の企業はこれらのソリューションも利用できます。

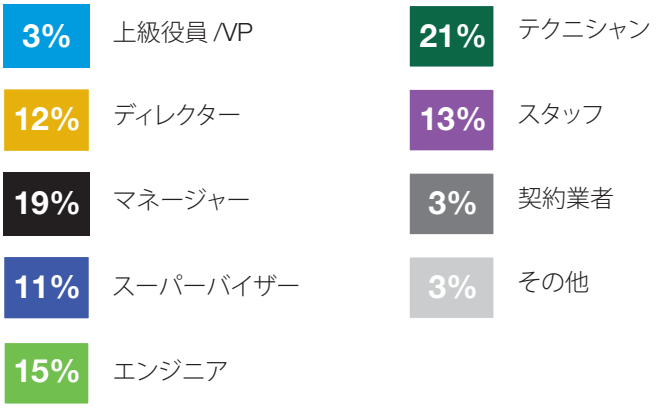
セキュリティ、品質、短納期を維持しながら安全性を高めていくには、このような厳格なアプローチでサイバーセキュリティに取り組むことが不可欠です。

調査方法

今回の調査では、自動車業界の IT セキュリティ専門家およびエンジニアを参加者として選びました（サンプル抽出枠 15,900 人）。適切な知識を有する方からの回答を得るため、回答者は車載コンポーネントのセキュリティの実装または評価に携わっている方に限定しました。表 1 に示すように、全回答数は 677 でした。スクリーニングと信頼性チェックの結果、84 件の回答を除外しました。最終的にサンプルとして残ったのは 593 件の回答で、回答率は 3.7% でした。

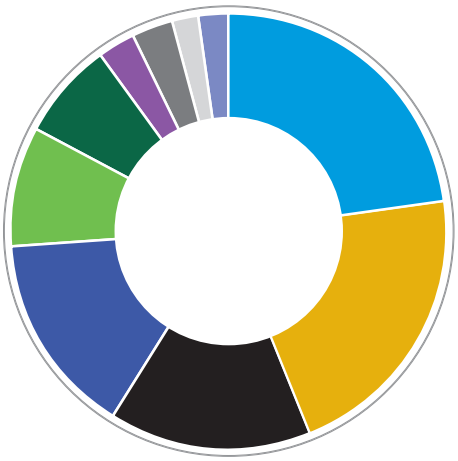
表 1：サンプルからの回答	**件数**	**割合（%）**
• サンプル抽出枠	15,900	100.0%
• 全回答数	677	4.3%
• 除外した回答数	84	0.5%
• 最終サンプル数	593	3.7%

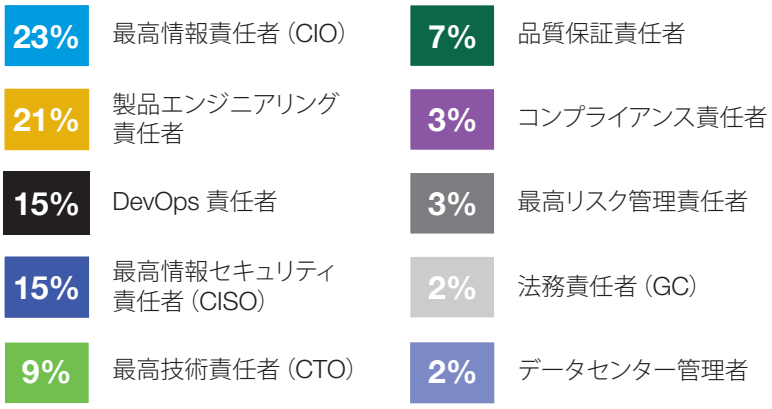
グラフ 1 に、回答者の企業における役職を示します。今回の調査の意図を反映して、半数以上（60%）がエンジニア以上の上級職に就いています。



グラフ 1：回答者の現在の役職

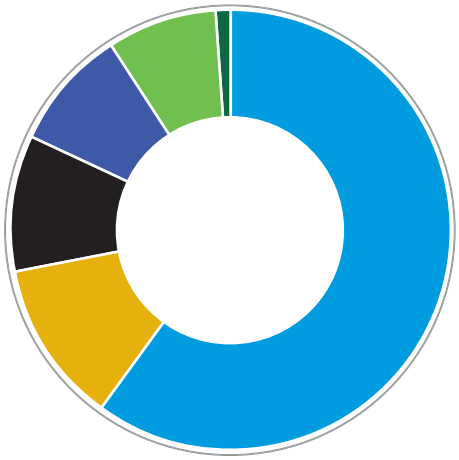
グラフ 2 に示すように、回答者の直属の上司としては最高情報責任者（23%）、製品エンジニアリング責任者（21%）DevOps 責任者（15%）、最高情報セキュリティ責任者（15%）が多く挙げられています。





グラフ 2：回答者（または回答者のリーダー）の直属の上司

グラフ 3 に示すように、回答者の大半（60%）は米国に本社のある企業に勤務しています。その他の本社所在地は、ヨーロッパが 12%、カナダが 10% でした。



60% 米国
12% ヨーロッパ
10% カナダ
9% 中南米（メキシコを含む）
8% アジア太平洋
1% 中東 / アフリカ

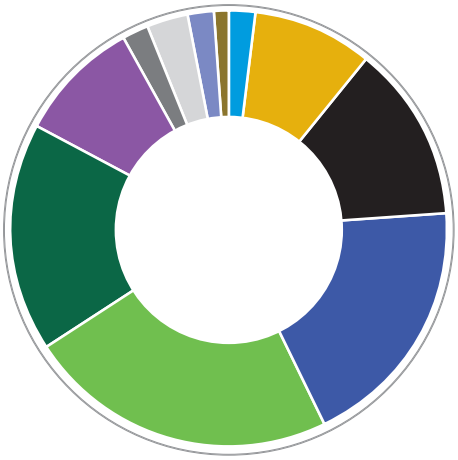
グラフ 3：本社所在地

グラフ 4 に示すように、回答者の 66% は全世界の従業員数 5,000 人超の企業に勤務しています。

34% 5,000 人未満
31% 5,000 ～ 10,000 人
16% 10,001 ～ 25,000 人
11% 25,001 ～ 75,000 人
8% 75,000 人以上

グラフ 4：全世界の従業員数

テクノロジ、人的リソース、マネージド（外注）サービス、その他の現金支出を含め、車載コンポーネントのセキュリティに対する年間投資額を尋ねたところ、100 万ドル超と答えた回答者が 57% ありました（グラフ 5）。



2% $1 ～ $100,000
9% $100,001 ～ $250,000
13% $250,001 ～ $500,000
19% $500,001 ～ $1,000,000
23% $1,000,001 ～ $2,500,000
17% $2,500,001 ～ $5,000,000
9% $5,000,001 ～ $10,000,000
2% $10,000,001 ～ $25,000,000
3% $25,000,001 ～ $50,000,000
2% $50,000,001 ～ $100,000,000
1% $100,000,000 以上

グラフ 5：車載コンポーネントのセキュリティに対する年間投資額。補外値 $6,098,000

本調査についての注意事項

調査データから結論を導出する際には、その調査に内在する制限事項に十分留意する必要があります。ほとんどのウェブ・ベースの調査には、以下に示す制限事項があります。

- 非回答バイアス：本レポートに示した知見は、返答のあった調査サンプルに基づいています。ある特定の層を代表するサンプルに調査票を送信し、これらの個人から多数の有効回答を得ました。非回答者に対するテストも実施しましたが、回答のあった人となかった人では意見が大きく異なる可能性は常に存在します。

- サンプル抽出枠バイアス：調査の精度は、被験者の役職が自動車業界で車載コンポーネントのセキュリティの実装または評価に携わっている IT セキュリティ専門家およびエンジニアであるかどうかによって左右されます。また、調査結果がメディアによる報道など外部イベントによるバイアスを受ける可能性もあります。最後に、今回の調査ではウェブを利用して回答を収集したため、郵送や電話などウェブ以外の方法で回答を収集した場合とは異なるパターンの知見が得られている可能性もあります。

- 自己報告による結果：アンケート調査の品質は、被験者から寄せられた秘密の回答の品質によって左右されます。調査プロセスにある程度のチェックおよび調整機構を組み込むことは可能ですが、被験者から寄せられた回答が正確でない可能性は常に存在します。

付録：調査結果の詳細

ここでは、この調査の全設問に対する回答数またはその割合を表にして示します。調査の回答は、2018 年 7 月 19 日～ 2018 年 8 月 3 日の期間に回収しました。

サンプルからの回答	**件数**	**割合 (%)**
・ サンプル抽出枠	15,900	100.0%
・ 全回答数	677	4.3%
・ 除外した回答数	84	0.5%
・ 最終サンプル数	593	3.7%

第 1 部：スクリーニング

S1a. 車載コンポーネントのセキュリティを実装または評価する立場の役職に就いていますか。	・ はい (大いに関与している)	32%
	・ はい (ある程度関与している)	50%
	・ はい (やや関与している)	18%
	・ 関与していない (ここで回答を終了してください)	0%
	合計	100%
S1b. (S1a で「はい」と答えた方) 車載機器のセキュリティを実装または評価する業務に何年携わっていますか。	・ 1 年未満	8%
	・ 2 ～ 4 年	25%
	・ 5 ～ 7 年	33%
	・ 8 ～ 10 年	19%
	・ 10 年以上	15%
	・ わからない (ここで回答を終了してください)	0%
	合計	100%
	補外値	6.31
S2. 車載テクノロジ / コンポーネントの開発におけるあなたの企業の役割として、最もあてはまるものを選んでください。	・ サプライヤ	21%
	・ メーカー	50%
	・ サービス・プロバイダ	29%
	・ 上記以外 (ここで回答を終了してください)	0%
	合計	100%

第 2 部：バックグラウンド / 組織の現状

Q1. 自動車業界におけるあなたの企業のポジションとして最もあてはまるものはどれですか。	・ OEM	47%
	・ ティア 1	36%
	・ ティア 2	12%
	・ ティア 3 以降	3%
	・ その他	2%
	合計	100%

Q2. あなたの企業は現在、どれくらいの種類の車載コンポーネント / 機能を製造していますか。	・ 5 未満	19%
	・ 6 ～ 25	34%
	・ 26 ～ 50	30%
	・ 50 以上	17%
	合計	100%
	補外値	27.63
Q3. あなたの企業ではどのような種類の車載ソフトウェア / テクノロジ / コンポーネントを設計・開発していますか。あてはまるものをすべて選んでください。	・ インフォテインメント・システム	31%
	・ パワートレイン制御ユニット	37%
	・ SoC（システム・オン・チップ）ベースのコンポーネント	17%
	・ 自動運転車	40%
	・ ソフトウェア主体のサービス・プロバイダ（クラウド、保険業者、ストリーミング・サービスなど）	30%
	・ テレマティクス	49%
	・ 操舵システム	21%
	・ 電動化部品	36%
	・ カメラ	28%
	・ 無線テクノロジ（Wi-Fi、Bluetooth、ホットスポットなど）	46%
	・ その他（具体的に）	2%
Q4. あなたの企業の製品サイバーセキュリティに対するアプローチとして、最もあてはまるものを 1 つ選んでください。	・ 伝統的な IT サイバーセキュリティ・チームが（主に全社的な CISO の指揮のもとで）製品のサイバーセキュリティを担当している	20%
	・ 機能安全チームが製品のサイバーセキュリティを担当している	17%
	・ 複数の製品開発チームを指導、サポートする製品サイバーセキュリティ・チーム（センター・オブ・エクセレンス）を中央に設置している	10%
	・ 中央ではなく、個々の製品開発チームごとにサイバーセキュリティ専門家を含む製品サイバーセキュリティ・チームを設置している	23%
	・ 製品のサイバーセキュリティに関する正式なプログラムやチームを設立していない	30%
	合計	100%
Q5. あなたの企業の製品サイバーセキュリティ管理プログラムに従事する従業員のフルタイム当量は何人分ですか。	・ 5 人未満	30%
	・ 5 ～ 10 人	44%
	・ 11 ～ 20 人	18%
	・ 20 人以上	8%
	合計	100%
	補外値	9.21
Q6. あなたの企業はサイバーセキュリティに十分なリソース（予算および人的資源）を割り当てていますか。	・ はい	49%
	・ いいえ	51%
	合計	100%

Q7. あなたの企業は製品開発に必要なサイバーセキュリティ・スキルを備えていますか。	・ はい	38%
	・ いいえ	62%
	合計	100%

Q8. 車載テクノロジのセキュリティに関する懸念を、あなたの企業の上層部に報告する権限が与えられていると感じますか。	・ はい	31%
	・ いいえ	69%
	合計	100%

第 3 部：自動車業界におけるソフトウェアのセキュリティ・リスクに関する認識

Q9. 次のテクノロジのうち、サイバーセキュリティにとって最も大きなリスクとなるのはどれですか。あてはまるものをすべて選んでください。	・ インフォテインメント・システム	31%
	・ パワートレイン制御ユニット	46%
	・ SoC（システム・オン・チップ）ベースのコンポーネント	44%
	・ 自動運転車	58%
	・ ソフトウェア主体のサービス・プロバイダ（クラウド、保険業者、ストリーミング・サービスなど）	51%
	・ テレマティクス	60%
	・ 操舵システム	45%
	・ 電動化部品	17%
	・ カメラ	29%
	・ 無線テクノロジ（Wi-Fi、Bluetooth、ホットスポットなど）	63%
	・ その他（具体的に）	2%

Q10. あなたの企業が開発または使用している車載ソフトウェア / テクノロジ / コンポーネントにセキュリティ不具合があった場合、ビジネスにどのような悪影響が及ぶと認識していますか。あてはまるものをすべて選んでください。	・ セキュリティ問題によるリコール	21%
	・ サプライチェーンのパートナー関係への損害	54%
	・ 納品の遅れ（またはキャンセル）	67%
	・ コンポーネント間の意図しない行動を統合テストで発見	59%
	・ 法律違反による制裁措置や罰金	5%
	・ 悪影響が生じることは認識していない	29%

Q11. あなたの企業が開発または使用している車載ソフトウェア / テクノロジ / コンポーネントにセキュリティ不具合があった場合、自動車のドライバーに危険が及ぶ可能性があると認識していますか。	・ はい	52%
	・ いいえ	48%
	合計	100%

Q12. あなたの企業が開発または使用している車載ソフトウェア / テクノロジ / コンポーネントが、今後 12 か月のうちに攻撃（セキュリティ研究者による実験を含む）を受ける可能性がどれだけあると考えますか。	・ 非常に高い	27%
	・ 高い	35%
	・ やや高い	23%
	・ 低い	15%
	合計	100%

以下の設問について、10 段階評価で答えてください。(1 = 懸念がない、10 = 非常に懸念がある)

Q13. あなたの企業が開発している車載ソフトウェア/テクノロジ/コンポーネントのサイバーセキュリティに懸念はありますか。	・ 1 ～ 2	13%
	・ 3 ～ 4	12%
	・ 5 ～ 6	23%
	・ 7 ～ 8	26%
	・ 9 ～ 10	26%
	合計	100%
	補外値	6.30
Q14. サードパーティからあなたの企業に納入されている車載ソフトウェア / テクノロジ / コンポーネントのサイバーセキュリティに懸念はありますか。	・ 1 ～ 2	8%
	・ 3 ～ 4	4%
	・ 5 ～ 6	15%
	・ 7 ～ 8	30%
	・ 9 ～ 10	43%
	合計	100%
	補外値	7.42
Q15. 自動車業界全体のサイバーセキュリティに懸念はありますか。	・ 1 ～ 2	9%
	・ 3 ～ 4	6%
	・ 5 ～ 6	17%
	・ 7 ～ 8	28%
	・ 9 ～ 10	40%
	合計	100%
	補外値	7.18
Q16. あなたの企業のサイバーセキュリティ・プラクティスが車載テクノロジの変化に追いついていない懸念はありますか。	・ 1 ～ 2	5%
	・ 3 ～ 4	11%
	・ 5 ～ 6	25%
	・ 7 ～ 8	22%
	・ 9 ～ 10	37%
	合計	100%
	補外値	7.00
Q17. サイバーセキュリティに関する自動車業界の法規制が車載テクノロジの変化に追いついていない懸念はありますか。	・ 1 ～ 2	12%
	・ 3 ～ 4	16%
	・ 5 ～ 6	29%
	・ 7 ～ 8	23%
	・ 9 ～ 10	20%
	合計	100%
	補外値	5.96

Q18. サイバーセキュリティに関する自動車業界の法規制があまり明確でない、または定義が不十分という懸念はありますか。	・ 1 ～ 2	10%
	・ 3 ～ 4	19%
	・ 5 ～ 6	27%
	・ 7 ～ 8	25%
	・ 9 ～ 10	19%
	合計	100%
	補外値	5.98
Q19. あなたの企業が製造するソフトウェア / テクノロジ / コンポーネントまたは車両が、悪意ある攻撃の標的にされる懸念はありますか。	・ 1 ～ 2	15%
	・ 3 ～ 4	7%
	・ 5 ～ 6	10%
	・ 7 ～ 8	33%
	・ 9 ～ 10	35%
	合計	100%
	補外値	6.82
Q20. あなたの企業で車載ソフトウェア / テクノロジ / コンポーネントのセキュリティ脆弱性を出荷前に見つけることができる自信はありますか。 （1= 自信がない、10 = 非常に自信がある）	・ 1 ～ 2	44%
	・ 3 ～ 4	25%
	・ 5 ～ 6	12%
	・ 7 ～ 8	4%
	・ 9 ～ 10	15%
	合計	100%
	補外値	3.92
Q21. あなたの企業で車載ソフトウェア / テクノロジ / コンポーネントのセキュリティ脆弱性を出荷前に見つけるのは難しいですか。 （1 = 難しくない、10 = 非常に難しい）	・ 1 ～ 2	7%
	・ 3 ～ 4	5%
	・ 5 ～ 6	23%
	・ 7 ～ 8	25%
	・ 9 ～ 10	40%
	合計	100%
	補外値	7.22
Q22. あなたの企業では、車載ソフトウェア / テクノロジ / コンポーネントにサイバーセキュリティ関連のコントロールを適用する必要に迫られていますか。 （1 = 今は必要ない、10 = ただちに必要）	・ 1 ～ 2	10%
	・ 3 ～ 4	10%
	・ 5 ～ 6	13%
	・ 7 ～ 8	41%
	・ 9 ～ 10	26%
	合計	100%
	補外値	6.76
Q23. 次の要因のうち、あなたの企業で予算の増額に影響すると考えられるのはどれですか。最もあてはまるものを 2 つ選んでください。	・ 新しい法律の施行	35%
	・ セキュリティ研究者による脆弱性の開示	49%
	・ 自社の車載コンポーネントに対する重大なハッキング・インシデント	54%
	・ 強制リコール	60%
	・ その他（具体的に）	2%
	・ 上記のいずれも該当しない	0%

第 4 部：SDLC におけるセキュリティ・プラクティス

Q24a. あなたの企業では、ソフトウェア開発者に対してセキュア開発に関するトレーニングを実施していますか。	・ はい（任意トレーニングとして）	21%
	・ はい（必須トレーニングとして）	25%
	・ はい（一部のチームのみ）	24%
	・ いいえ	30%
	合計	100%
Q24b.（Q24a で「はい」と答えた方のみ）あなたの企業のセキュア開発に関するトレーニングは効果をあげていますか。	・ 非常に効果あり	15%
	・ 効果あり	21%
	・ やや効果あり	24%
	・ 効果なし	40%
	合計	100%
Q25. あなたの企業は、車載ソフトウェア / テクノロジ / コンポーネントに対して社内または外部で発行されたセキュア・ソフトウェア開発ライフサイクル（SSDLC）プロセスに従っていますか。	・ はい（社内のプロセス）	35%
	・ はい（社外のプロセス）	29%
	・ いいえ	36%
	合計	100%
Q26. 平均して、あなたの企業が開発または使用している車載ソフトウェア / テクノロジ / コンポーネントの何パーセントがサイバーセキュリティ脆弱性のテストを受けていますか。	・ なし	25%
	・ 25% 未満	12%
	・ 26% ～ 50%	26%
	・ 51% ～ 75%	23%
	・ 76% ～ 100%	14%
	合計	100%
	補外値	39%
Q27. あなたの企業では、開発ライフサイクルのどの時点で車載ソフトウェア / テクノロジ / コンポーネントのセキュリティ脆弱性を評価していますか。当てはまるものをすべて選んでください。	・ 要件定義 / 設計フェーズ	19%
	・ 開発 / テスト・フェーズ	28%
	・ リリース後	43%
	・ 車載ネットワークへの統合後	37%
	・ 本番リリース後	18%

Q28. あなたの企業では、車載ソフトウェア / テクノロジ / コンポーネントのセキュリティを確保するためにどのようなアクティビティを実施していますか。あてはまるものをすべて選んでください。	・ 開発者に対するセキュア・コーディング手法のトレーニング	33%
	・ セキュア・アーキテクチャ設計	18%
	・ 脅威モデリング	21%
	・ セキュリティ要件を特定するその他の方法	15%
	・ セキュリティ要件定義	44%
	・ コード・レビュー（手動）	29%
	・ 静的解析 /SAST（自動）	47%
	・ システム・デバッグ	48%
	・ ファジング・テスト	19%
	・ ソフトウェア・コンポジション解析	18%
	・ ダイナミック・アプリケーション・セキュリティ・テスト /DAST	49%
	・ ペネトレーション・テスト	56%
	・ データ・マスキング（テスト段階）	39%
	・ セキュリティ・パッチ管理	61%
	・ ランタイム・アプリケーション自己保護（RASP）	26%
	・ その他（具体的に）	3%
	・ 上記のいずれも実施していない	8%
Q29. あなたの企業が開発している車載ソフトウェア / テクノロジ / コンポーネントにはオープンソース・コードを使用していますか。	・ オープンソース・コードを使用しており、使用中のオープンソース・コードのインベントリ作成および管理に関するプロセスが確立されている	26%
	・ オープンソース・コードを使用しているが、使用中のオープンソース・コードのインベントリ作成および管理に関するプロセスは確立されていない	32%
	・ オープンソース・コードは使用していない	42%
	合計	100%
Q30. あなたの企業が開発または使用している車載ソフトウェア / テクノロジ / コンポーネントに脆弱性が混入する最大の要因は何ですか。最もあてはまるものを 4 つ選んでください。	・ 意図しないコーディング・エラー	55%
	・ セキュアでない / 最新でないオープンソース・ソフトウェア・コンポーネントの使用	40%
	・ 開発段階の不正なコード・インジェクション	23%
	・ セキュリティ要件を明確化した社内ポリシー / ルールの欠如	26%
	・ セキュア・コーディング・プラクティスに関する理解 / トレーニングの欠如	60%
	・ 製品納期までの余裕がない	71%
	・ 品質保証およびテストの手順が確立されていない	50%
	・ 製品開発ツールに内在するバグ	39%
	・ 不適切なパーミッション	19%
	・ 脆弱なバックエンド・システム	15%
	・ その他（具体的に）	2%
Q31. あなたの企業には、重大な脆弱性が開示された場合のインシデント・レスポンス計画はありますか。	・ はい	43%
	・ いいえ	57%
	合計	100%
Q32. あなたの企業では、車両に何らかのセキュリティ対策を採用していますか。当てはまるものをすべて選んでください。	・ ゲートウェイ	59%
	・ ファイアウォール	64%
	・ マシン・ラーニング	41%
	・ ホワイトリスト	38%
	・ その他（具体的に）	3%

Q33a. あなたの企業では、ソフトウェア / テクノロジ / コンポーネントの開発または製造プロセスにおいて鍵管理システムを採用していますか。	・ はい	63%
	・ いいえ	37%
	合計	100%
Q33b. (Q33a で「はい」と答えた方のみ) あなたの企業では現在どのような鍵管理システムを使用していますか。当てはまるものをすべて選んでください。	・ 形式的な鍵管理ポリシー (KMP)	45%
	・ 手作業 (スプレッドシート、紙ベースなど)	43%
	・ 中央の鍵管理システム / サーバ	56%
	・ ハードウェア・セキュリティ・モジュール	39%
	・ その他	2%
Q34. あなたの企業では、どのような方法で販売後の車両にセキュリティ・パッチ / アップデートを配布していますか。	・ 無線 (OTA) によるアップデート	37%
	・ アフターサービスによるメンテナンス	45%
	・ ユーザーが所有する電子 / コンピューティング機器との無線通信を利用	51%
	・ 外部調達したソフトウェア、コンポーネント、システムを利用	65%
	・ セキュリティ・アップデートを提供していない	25%
	・ その他	3%
Q35. 現在 OTA によるアップデートを提供していないと答えた方は、今後その計画がありますか。	・ 1 ～ 3 年以内	33%
	・ 3 ～ 5 年以内	23%
	・ 5 年以上	9%
	・ OTA アップデート提供の計画なし	35%
	合計	100%
Q36. あなたの企業のソフトウェア・アップデート配布モデルは、重大なセキュリティ脆弱性に迅速に対応できていますか。	・ はい	39%
	・ いいえ	61%
	合計	100%

第 5 部：サプライチェーンのサイバーセキュリティ・プラクティス

Q37a. あなたの企業は、上流サプライヤから供給される車載ソフトウェア / テクノロジ / コンポーネントに対してサイバーセキュリティに関する要求事項を課していますか。	・ はい	44%
	・ いいえ (Q38 へ進んでください)	56%
	合計	100%
Q37b. (Q37a で「はい」と答えた方のみ) あなたの企業では、サプライヤによるセキュリティ要求事項への遵守をどのように徹底していますか。当てはまるものをすべて選んでください。	・ サプライヤがセルフチェックを実行し、検証結果を提出している	51%
	・ 独立系の第三者機関が評価を実施し、検証結果を提出している	25%
	・ 自社で直接サプライヤのセキュリティ評価を実施している	38%
	・ セキュリティ要求事項をサプライヤ契約書に明示的に定義している	49%
	・ サプライヤがセキュリティ要求事項に従うことを徹底する正式なプロセスが存在しない (Q38 へお進みください)	40%

Q37c.（Q37a で「はい」と答えた方のみ）あなたの企業では、サプライヤに対してセキュリティ保証をどの程度の頻度で要求していますか。	・ 1 年ごと	33%
	・ 四半期ごと	9%
	・ 主要リリースごと	26%
	・ コード変更時ごと	29%
	・ その他	3%
	合計	100%

第 6 部：今後の自動車業界のプラクティス

Q38. 今後、車両のセキュリティを強化すると考えられるネットワーク・アーキテクチャは、次のどれですか。	・ 車載 Ethernet	44%
	・ FlexRay	50%
	・ 5G	54%
	・ その他（具体的に）	8%
	・ 上記のいずれも該当しない	26%

Q39. 車両ネットワークのセキュリティとレジリエンス（回復力）を強化すると考えられる具体的なスタンダード / ガイドライン / テクノロジは、次のどれですか。	・ セキュリティ・モジュール	29%
	・ ゲートウェイ	50%
	・ IDS	54%
	・ セキュア OTA アップデート	63%
	・ ホワイトリスト	47%
	・ その他（具体的に）	5%

Q40. セキュリティ保証テスト / 認定 / 運用承認アプローチとして最も効果的で達成可能なものは、次のどれですか。	・ 自己認定	20%
	・ プロセス・スタンダードに準拠した自己認定	40%
	・ 定期的評価による自己認定	32%
	・ 型式認定	8%
	・ その他（具体的に）	0%
	合計	100%

第 7 部：回答者 / 企業の属性

D1. あなたの現在の役職に最もあてはまるものは次のどれですか。	・ 上級役員 /VP	3%
	・ ディレクター	12%
	・ マネージャー	19%
	・ スーパーバイザー	11%
	・ エンジニア	15%
	・ テクニシャン	21%
	・ スタッフ	13%
	・ 契約業者	3%
	・ その他	3%
	合計	100%

D2. あなた（またはあなたのリーダー）の直属の上司は次のどれですか。	・ 最高財務責任者（CFO）	0%
	・ 最高執行責任者（COO）	0%
	・ 法務責任者（GC）	2%
	・ DevOps 責任者	15%
	・ 製品エンジニアリング責任者	21%
	・ 品質保証責任者	7%
	・ 最高情報責任者（CIO）	23%
	・ 最高技術責任者（CTO）	9%
	・ 最高情報セキュリティ責任者（CISO）	15%
	・ 最高セキュリティ責任者（CSO）	0%
	・ コンプライアンス責任者	3%
	・ データセンター管理者	2%
	・ 最高リスク管理責任者	3%
	・ その他	0%
	合計	100%
D3. あなたの企業の本社所在地は次のどこですか。	・ 米国	60%
	・ カナダ	10%
	・ ヨーロッパ	12%
	・ 中東 / アフリカ	1%
	・ アジア太平洋	8%
	・ 中南米（メキシコを含む）	9%
	合計	100%
D4. あなたの企業の全世界の従業員数は次のどれですか。	・ 5,000 人未満	34%
	・ 5,000 ～ 10,000 人	31%
	・ 10,001 ～ 25,000 人	16%
	・ 25,001 ～ 75,000 人	11%
	・ 75,000 人以上	8%
	合計	100%
D5. 車載コンポーネントのセキュリティに対するあなたの企業の年間支出額は、およそいくらですか。テクノロジ、人的リソース、マネージド（外注）サービス、その他の現金支出を含む投資総額として、最もあてはまるものを選んでください。	・ なし	0%
	・ $1 ～ $100,000	2%
	・ $100,001 ～ $250,000	9%
	・ $250,001 ～ $500,000	13%
	・ $500,001 ～ $1,000,000	19%
	・ $1,000,001 ～ $2,500,000	23%
	・ $2,500,001 ～ $5,000,000	17%
	・ $5,000,001 ～ $10,000,000	9%
	・ $10,000,001 ～ $25,000,000	2%
	・ $25,000,001 ～ $50,000,000	3%
	・ $50,000,001 ～ $100,000,000	2%
	・ $100,000,000 以上	1%
	合計	100%
	補外値（US$）	$6,098,000

責任ある情報管理を推進

Ponemon Institute は、独立した調査と教育の実施を通じ、企業および政府において責任ある情報 / プライバシー管理プラクティスを推進することを目指しています。人々や組織に関する機密情報の管理 / セキュリティに影響する重大な問題について、高品質な実証研究を実施することを使命としています。

データの機密性、プライバシー、調査倫理に関しては厳密な基準を設けています。個人調査において個人を特定できる情報（企業調査において企業を特定できる情報）を収集することは一切ありません。また、不適切あるいは無関係な質問をしないように厳格な品質基準も設定しています。

お問い合わせ先：research@ponemon.org または電話 800.887.3118