

Automotive SPICE for Cybersecurity ドラフト版のご紹介

(山内)

今回のメルマガでは、自動車のサイバーセキュリティの法規対応が施行される中、2021年2月から公開されている Automotive SPICE for Cybersecurity（以降、Automotive SPICE for CS）のドラフト版（公開は、2021年5月末までの予定）についてご紹介いたします。以前、intacs のワーキンググループが Cybersecurity SPICE の策定を進めているとお伝えしましたが、intacs が検討成果を VDA のワーキンググループに引き渡す形で今回の CS SPICE ドラフトの策定となりました。Automotive SPICE for CS は、2021年5月末までドラフト版のフィードバックを行い、正式版として2021年秋頃に発行予定です。

まず、過去のメルマガでもお伝えしましたが国連の自動車基準調和世界フォーラム(WP.29)が新しいレギュレーションとして発行した UNECE R-155（サイバーセキュリティ及びサイバーセキュリティマネジメントシステム）は、サプライチェーンにおけるサイバーセキュリティリスクの特定および管理を自動車メーカーに要求しています。その対応の中で Automotive SPICE は、自動車業界で求められるプロセスの目的やプロセスの成果を体系的にまとめたものであり、アセスメントを実施することにより、プロセス関連の製品リスクを特定するための有効な方法となっております。Automotive SPICE for CS は、サイバーセキュリティ関連のプロセスを Automotive SPICE の対象プロセス範囲に組み込むために、サイバーセキュリティエンジニアリングのプロセス参照およびアセスメントモデル（Cybersecurity PAM）が追加で定義されています。ただし、ISO/SAE 21434 で要求されているサイバーセキュリティ管理、継続的なサイバーセキュリティ活動、開発後のフェーズ、廃止措置などの製品開発のライフサイクルにおける開発フェーズ以外の活動については、Automotive SPICE for CS の範囲には含まれていません。これらの活動は、VDA から発行されている Automotive Cybersecurity Management System Audit の対象範囲となっております。

Automotive SPICE for Cybersecurity の構成は、Part.1：サイバーセキュリティエンジニアリングのためのプロセス参照およびアセスメントモデル、Part.2：サイバーセキュリティエンジニアリングに対する評価ガイドライン（能力レベル1）の2部構成となっております。Part.1 は、Automotive SPICE 3.1 および Automotive SPICE ガイドライン（第1版）を補足し、サイバーセキュリティ関連の開発プロセスのアセスメントを可能にしています。Part.2 は、既存の Automotive SPICE ガイドライン（第1版）を補完することを目的としています。この内容には、Part.1 で定義されたプロセスの解釈とアセスメントのガイドラインが含まれています。

Automotive SPICE for CS では、Automotive SPICE 3.1 からの新しいプロセスグループとして SEC（Security engineering process group）が追加されており、そのほかに ACQ.2、MAN.7 が追加され、ACQ.4 が Automotive SPICE 3.1 から内容が一部変更されています。

■ Automotive SPICE for CS で定義されているプロセス

- SEC.1 Cybersecurity requirement elicitation
- SEC.2 Cybersecurity implementation
- SEC.3 Risk treatment verification
- SEC.4 Risk treatment validation
- ACQ.2 Supplier request and selection
- ACQ.4 Supplier monitoring
- MAN.7 Cybersecurity risk management

Automotive SPICE for CS によるアセスメントは、Automotive SPICE 3.1 のアセスメントと組み合わせて実施する場合と、Automotive SPICE for CS のみの実施の2つのパターンで実施することが可能です。過去に VDA スコープのアセスメントを実施していた場合は、追加で Automotive SPICE for CS のみの実施することが出来ます。過去に VDA スコープのアセスメントを実施していない場合は、Automotive SPICE for CS のアセスメントと Automotive SPICE 3.1 のアセスメントの両方を実施する必要があります（CS と VDA スコープのアセスメントは、分割して実施可能）。もし、組み合わせて実施する場合は ACQ.4 はそれぞれ個別のプロセスインスタンスとしての実施が推奨されています。

今後は、自動車メーカーが従来の Automotive SPICE に加えて、Automotive SPICE for CS を用いてアセスメントを実施し、サイバーセキュリティに対するサプライヤーの能力を評価するように検討が進んでいます。皆さんも今後のサイバーセキュリティ対応として既存の Automotive SPICE と共に Automotive SPICE for CS をセキュリティ対策の体系的なアプローチの構築にご活用頂ければと思います。

弊社は、ISO/SAE 21434 に対して Automotive SPICE for CS を含めたプロセス改善のご支援やトレーニングを行っております。ご興味がある方は是非、弊社までお問い合わせください。

今後も弊社はメルマガやセミナーなどで Automotive SPICE for CS や Automotive SPICE 4.0 などの最新の情報をお伝えしていきます。

※注意事項：本メルマガの内容はドラフト版に基づいて作成しております。後に発行される正式版では内容が異なる場合がございます。

2021/4/23 [山内 誠](#)