

## サイバーセキュリティ対応における CSMS の構築について その2

### ～MAN.5 : リスク管理～

2021年1月のWP29によるサイバーセキュリティ規則の発行が迫ってきました。そのため、車両メーカーおよび部品メーカーは、サイバーセキュリティ規則対応のためにISO 21434への対応が急務となっております。弊社では、その対応を支援するために[2021年2月26日に「サイバーセキュリティ概論トレーニング」](#)を開催いたします。

そこで今回は、[10月号「CSMSを構築するためのAutomotive SPICEの活用について」](#)のACQ.3,ACQ.4の活用が続いて、CSMSを構築するためにリスクをどのように管理するかヒントとなる、MAN.5:リスク管理の活用を紹介したいと思います。

最初に、MAN.5:リスク管理プロセスですが、VDA16といったサプライヤー能力評価で使われる対象プロセスセットには現時点では対象になっていません。そのため、あまりMAN.5を参照されることは少ない傾向にあります。しかし、実際にはMAN3:プロジェクト管理プロセスのリスクに関する内容の詳細として参照することができ、CSMS(サイバーセキュリティマネジメントシステム)でもリスク管理の基本的な考え方として大きく役立てることが出来ます。そこで、CSMSの構築を始める最初の一步として、MAN5:リスク管理プロセスを参照し、自分たちのリスク管理に関する活動に対応するための確認の観点を解説いたします。

まず、Automotive SPICE3.1に記載されているリスク管理プロセスの目的ですが、「継続的にリスクを識別し、分析し、対応し、監視することである。」と記載されています。これは、体系的なリスク管理の構築を目的としていることを読み取ることが出来ます。ここで気を付けたいのは、Automotive SPICEで求めているリスク管理は、技術的な側面だけではなく管理面のリスクも含めたリスクが対象となっております。プロセス成果には以下の内容が記載されております。

- 1) 実施すべきリスク管理の範囲が特定されている。
- 2) 適切なリスク管理戦略が定義され、実装されている。
- 3) プロジェクト実施中に発生したリスクが識別されている。
- 4) リスクが分析され、これらのリスク対応にリソースを投入するための優先順位が決定されている。
- 5) リスク測定項目が定義され、適用され、リスクのステータス変更および対応活動の進捗を判断するために評価されている。
- 6) リスクの影響を是正または回避するために、優先順位、発生確率、および影響度、または他の定義されたリスク閾値に基づいて適切な対応が講じられている。

<Automotive SPICE3.1より抜粋>

それでは、それぞれの確認の観点を簡単に解説したいと思います。

まず、1)は「リスク管理の範囲」についてです。これはプロジェクトが行うリスク管理と、組織が行うリスク管理の範囲が明確になっている必要があります。一般的には組織としてのリスク管理方針を定め、プロジェクトが従うこととなります。

2)は「リスク管理の戦略(考え方)」についてです。リスク管理の戦略(考え方)が策定されていること



が求められ、戦略には、リスクの識別（どういったものをリスクとして扱うのか）、リスクに対する許容の考え方、軽減策や監視方法などが含まれます。

3) は、「リスクの識別」についてです。プロジェクト開始時のリスクやプロジェクト実施中のリスクに対して、戦略に記載したリスクの識別に従い、実際のリスクを識別しているか確認します。ここでは、技術面、管理面の方の識別も求められます。

4) は、「リスクの分析」についてです。プロジェクトで発生したリスクに対して、戦略で記載された分析方法に従い、どのリスク対策を優先するのかなどを決めているかを確認します。

5) は、「リスクの評価」についてです。抽出されたリスクをプロジェクト中に監視を行い、各リスクの発生や軽減策の効果も含め評価出来ていることとなります。

最後に 6) は、「リスクの対応」についてです。5) で評価されたリスクに対して戦略に従い、リスクの対応が適切に出来ていることを確認します。プロジェクトが、それぞれリスクに対して、リスク対策の優先度や影響度に基づいた対応が正しく行われていることが求められています。

上記の観点で MAN.5 : リスク管理プロセスを確認すれば、自分たちのプロジェクトがリスク管理を体系的に行われているかを知ることができ、今後の CSMS を構築するうえで改善すべき点を自分たちで得ることができます。この機会に一度 MAN.5 を活用し、体系的なリスク管理が出来ているかを確認してみることをお勧めいたします。

弊社では、ISO 21434 に関するトレーニングや今回ご紹介した Automotive SPICE を活用した CSMS の構築などのトレーニングを今後、開催していく予定です。ご興味がある方は是非トレーニングをお申し込みください。

2020/12/21 [山内 誠](#)