Cybersecurity SPICE と ISO/SAE 21434 の動向

今年 7 月のメールマガジンでは、Cybersecurity SPICE（以下、CS SPICE）の策定が進んでいる旨をご紹介いたしましたが、今回のメールマガジンでは、その CS SPICE として策定されているプロセスの内容や、関連する規格の動向についてご紹介いたします。

CS SPICE は Automotive SPICE V3.0 以降のプラグインコンセプトに基づくプラグインモデルとして位置づけられ、すでに発行済みの SPICE for Mechanical Engineering と同様に、新たなプロセスが追加されます。CS SPICE では、"Security"の最初の 3 文字を取って ID に"SEC"が付き、SEC.1～6 の合計 6 個のプロセスが定義される予定です。

SEC 系プロセスとして追加される 6 プロセスのうち、技術的な観点としては、システムレベルとソフトウェアレベルそれぞれに「セキュリティリスク分析およびセキュリティコンセプト」が追加されます。これらのプロセスは、システムレベルにおける脅威分析と、ソフトウェアレベルにおける脆弱性分析を含めたセキュリティリスクの分析・評価と、抽出されたリスクに対する対策の策定を求めています。また、別のプロセスとして、独立した立場からのセキュリティアセスメントも求められています。

CS SPICE のもう一つの特徴としては、SOP 後のすべてのライフサイクルを対象としていることにあります。これは、製品が市場にリリースされた後に見つかる脅威や脆弱性に対しても、必要な対策を講じるため仕組みの構築や維持に該当します。

さらに、Automotive SPICE 本体のプロセスに対しても、いくつかのプロセスのプロセス成果、アウトプット作業成果物、基本プラクティスとその備考に追加定義が行われます。（これは、CS SPICE としての追加定義であり、ASPICE 本体への変更は発生しません。）たとえば、MAN.3 プロジェクト管理プロセスにおいては、セキュリティ計画に関する考慮点が追加されます。

このように、CS SPICE はサイバーセキュリティ対策に必要なプロセスを含んでいますが、これらの内容は現在策定中の車載システム向けサイバーセキュリティ規格 ISO/SAE 21434 や国連欧州経済委員会（UNECE）の規制要件を反映する形で策定が進められており、高い親和性を持ちます。

ISO/SAE 21434 については、まもなく DIS 版のドラフトが公開されますが、正式発行に向けて各社ともサイバーセキュリティ対応に向けた体制構築やプロセス構築への取り組みを急がれている状況かと思います。特に、プロセス構築においては、前述のように SOP までの開発プロセスだけでなく、製品リリース後の対応に関するプロセスが必要になるため、プロセス全体の見直しが必要です。

弊社では、CS SPICE を活用したサイバーセキュリティ対策の支援に向けて準備を進めており、CS SPICE および ISO/SAE 21434 に関する最新情報をご提供すべくセミナーも計画しております。詳細が決まり次第、改めてメールマガジンにて案内をさせていただきます。

2019/10/25　田渕　一成