サイバーセキュリティのための Automotive SPICE

～エンジニアリングにおける SEC プロセスの位置づけ～

今回のメルマガでは、「サイバーセキュリティのための Automotive SPICE」（以降：本文書では CS SPICE と表記）に定義されている、サイバーセキュリティエンジニアリングプロセスについてお話します。

先日 2025 年 3 月に、CS SPICE の Ver.2.0（英語版）が公開されました。新しいバージョンの PAM では、土台となる Automotive SPICE の Ver.が 3.1 から 4.0 に更新され、それに伴って対象ドメインにハードウェアが追加されるなどの変更がなされています。現時点でも CS SPICE は、欧州を中心とした OEM によるサプライヤ評価等ですでに活用されていますが、このバージョンアップによってその活用はさらに拡大されると考えられます。

さて、この CS SPICE をプロセス改善に役立てる際に多く聞かれる疑問として、従来のエンジニアリングプロセスと、サイバーセキュリティエンジニアリングプロセス（SEC）との関係があります。SEC プロセス群では、TARA（脅威分析およびリスク評価）を除くサイバーセキュリティ関連のエンジニアリング活動が一括して取り扱われています。プロセス改善の現場では、Automotive SPICE 上のプロセス構造に従ってサイバーセキュリティエンジニアリングを従来のシステム、ソフトウェア、ハードウェアエンジニアリングから完全に独立したものとして実装しようとするアプローチが散見されます。しかしこのようなアプローチは効果的なサイバーセキュリティリスク管理の妨げとなる場合があります。SEC プロセスの本来の役割と立ち位置を理解することが、CS SPICE 活用の最初の一歩として大切です。

SEC プロセスは他のプロセスから独立して存在するのではなく、システムやソフトウェア、ハードウェアエンジニアリング活動に統合する形で実施されるべきです。セキュリティの分析、設計、検証といった活動が、各エンジニアリング工程の適切なタイミングに組み込まれていくことが理想です。図 1 はエンジニアリングプロセスと SEC プロセスの典型的な関係を表しており、各エンジニアリング活動の一部として SEC プロセスの要素が実装されることを表現しています。実際、欧州 OEM によるアセスメントでは、SEC プロセス単体ではなく、SYS や SWE の中でセキュリティ関連活動の妥当性や実装状況を併せて確認するケースが一般的です。

さらに、同じ SEC プロセスであっても、開発領域やタイミングによって求められる活動は異なります。例えば、SEC.3 プロセスは検証工程のほとんど全体に関係しますが、車載製品としての統合が完了したタイミングでは製品単体のファジングテスト、製品を車両に組み込んだタイミングでは車両レベルのネットワークテストといったように、製品特性や開発領域、タイミングに合わせて適切な活動をエンジニアリング工程に追加するという方針が重要になります。

Copyright 2025 Business Cube & Partners, Inc. All rights reserved.

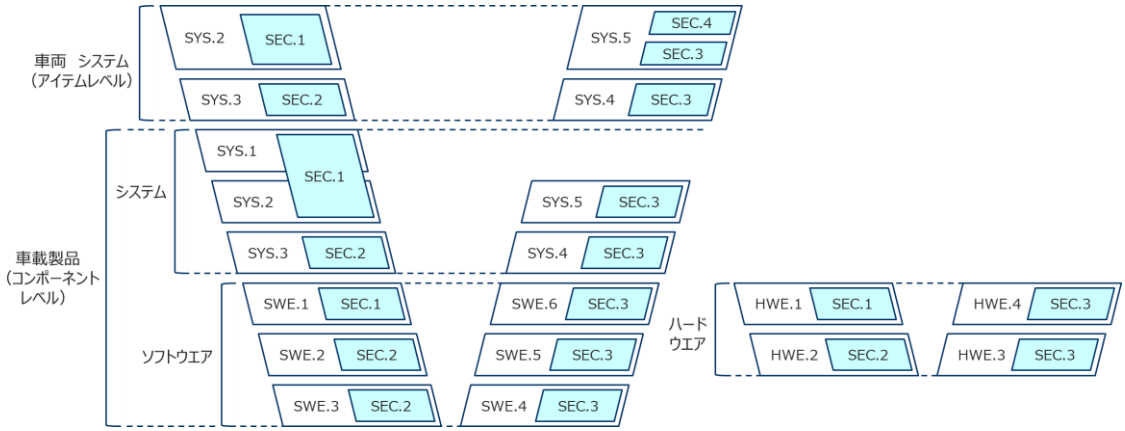

図１　アイテム/コンポーネント各レベルのエンジニアリングプロセスと SEC プロセスの関係

「SEC プロセス群」という枠組みは、プロセスを改善/評価する際の視点を示しているにすぎません。サイバーセキュリティ関連プロセスの構築においては、SEC プロセスという枠組みに囚われず、エンジニアリング全体との融合を意識することが重要です。自社の開発プロセスが、こうした観点で効果的に整備できているか、今一度見直してみてはいかがでしょうか。サイバーセキュリティプロセスのギャップ分析や、第三者視点からのチェックをご検討の際は、ぜひ弊社までご相談ください。

2025/5/29 大野　貴正

Copyright 2025 Business Cube & Partners, Inc. All rights reserved.