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 3

～サプライヤーマネージメント～

（山内）

サイバーセキュリティ関連の規格として 2021 年 5 月に ISO/SAE FDIS 21434 が発行されました。ISO としての正式発行が近づいて来ており、自動車メーカーや各サプライヤーは ISO21434 への対応を開始していると思います。

今回は、ISO/SAE FDIS 21434 の第 7 節で要求されている「分散サイバーセキュリティ活動」に対するプロセス構築のヒントとして Automotive SPICE：取得プロセス群（ACQ）とのマッピングをご紹介したいと思います。

まず、取得プロセス群（ACQ）は、「製品および／またはサービスを取得するために、顧客が実施するプロセス、またはサプライヤーが別のサプライヤーにとっての顧客となる際にサプライヤーが実施するプロセスで構成される。」と規格に記載されており、顧客とサプライヤー間の受発注に関連するプロセス群となっております。取得プロセス群のプロセスは、以下の図のように関係性があります。

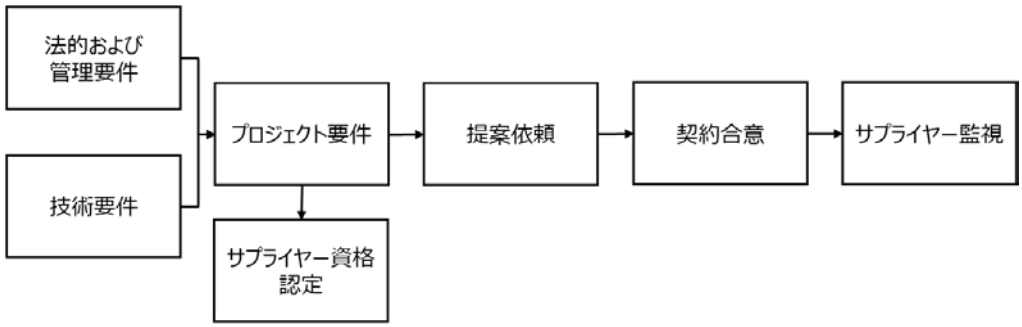

図 1. 取得プロセス群のプロセスの関係性

次に ISO/SAE FDIS 21434 の分散サイバーセキュリティ活動は以下のように構成されており、顧客とサプライヤーとのサイバーセキュリティに関する要求事項が定義されております。ここでの顧客とサプライヤーとの関係は、OEM と Tier1、Tier1 と Tier2 といった関係を意味します。

7. 分散サイバーセキュリティ活動
7.4.1 サプライヤーの能力
7.4.2 見積依頼
7.4.3 責任の調整

「7.4.1 サプライヤーの能力」では、サプライヤーが ISO/SAE 21434 に従って開発を行うことの出来る能力があることを評価することが求められています。また、サプライヤーは顧客の評価を支援するためにその能力の証拠を提供することが推奨されています。

「7.4.2 見積依頼」では、顧客がサプライヤーへ見積り依頼の内容を求めており、ISO/SAE 21434 への準拠やサイバーセキュリティにおけるサプライヤーの責任、サプライヤーが開発するアイテムやコンポーネントに対するサイバーセキュリティゴールやサイバーセキュリティ要件などが含まれています。
「7.4.3 責任の調整」では、顧客とサプライヤーの責任についての要求事項となっております。サイバーセキュリティインターフェースとして、顧客とサプライヤーがそれぞれ実施する活動や互いに共有する情報、作業成果物などの規定を行い、合意することが必要になります。
それでは、上記 3 つの要求に対して、ACQ 群のプロセスを活用するために要求事項と参照するプロセスのマッピングをご紹介いたします。
「7.4.1 サプライヤーの能力」は、「ACQ.15 サプライヤー資格認定」が活用できます。このプロセスの目的は、「サプライヤー候補が提案／入札評価プロセスに参加するために必要な資格を持っているかを評価し、判断することである。」と記載があります。この目的からわかるようにサイバーセキュリティ活動を行う資格があるかを評価するためのプロセスとして参照することができます。
「7.4.2 見積依頼」は、「ACQ.11 技術要件」「ACQ.12 法的及び管理要件」「ACQ.13 プロジェクト要件」「ACQ.14 提案依頼」が活用できます。まず、ACQ.11 および ACQ.12 でサイバーセキュリティ以外の要件も含め技術面、管理面の要件を抽出し、ACQ.13 でサプライヤーへの要件としてプロジェクト要件をまとめます。このプロジェクト要件を ACQ.14 に従い、サプライヤーへサイバーセキュリティ準拠が必要となるアイテム／コンポーネント開発の提案を依頼します。図.1 のようなプロセスの関係性を理解し参照すれば、要件定義から見積依頼までの流れを参照することができます。
「7.4.3 責任の調整」は、「ACQ.3 契約合意」が活用できます。ACQ.3 では顧客とサプライヤーとの間での両者の期待事項、責務などを明確かつあいまいさを残さずに定義し、合意・契約することが成果と求められています。よって、サイバーセキュリティに関する責任の調整もこのプロセスを活用することができます。
今回は「分散サイバーセキュリティ活動」に対して Automotive SPICE を活用したプロセス構築を行うためにプロセスとのマッピングをご紹介いたしました。これらのプロセスは、サプライヤー能力評価で一般的に使われるアセスメント対象プロセス（VDA16 など）ではありません。Automotive SPICE には、上記のように対象外であっても開発ライフサイクルに活用できるプロセスが定義されていますので、是非、アセスメント対象外のプロセスも参照していただければと思います。

弊社では、9 月に ISO/SAE 21434 の関連トレーニングとして「サイバーセキュリティ概論トレーニング」や「サイバーセキュリティ規格詳細解説トレーニング」を実施いたします。また、秋ごろに正式発行される予定の Automotive SPICE　For Cybersecurity 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。

2021/8/25 山内 誠

CSMS の構築に関する過去のメールマガジンはこちら（https://biz3.co.jp/download）
・2020 年 10 月 23 日　CSMS を構築するための Automotive SPICE の活用について（山内）
・2020 年 12 月 21 日　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～(山内)