SYNOPSYS®

WHITE PAPER

ISO 21434に基づくサイバーセキュリティを意識したSoC開発のベスト・プラクティス

米国シノプシス

シニア・サイバーセキュリティ・エンジニア
Gulam Ashrafi

概要

サイバー攻撃を仕掛ける側のリソースと能力は、日々増大しています。既製のツールや手法が広く公開され、誰もがアクセスできるようになっているため、より多くの主体が高度な攻撃を仕掛けられるようになっています。攻撃者の能力が向上することで、これまで以上に攻撃対象が拡大しており、セキュア設計手法を使用せずに開発されたSoCは、脆弱性を悪用されるようになっています。製品開発者は、過去にサイバー攻撃を受けたことのない製品であっても、セキュアなハードウェア・ソリューションを開発する必要に迫られています。

車載アプリケーションの電子化が進むことにより、道路利用者を脅かすサイバー攻撃はますます増加し、巧妙化しています。車載アプリケーションが危害の要因になりかねない現在、自動車業界の部品サプライヤーにとって、サイバーセキュリティを意識した開発手法を採用することが急務となっています。「ISO/SAE 21434:2021 Road vehicles — Cybersecurity Engineering（路上走行車 — サイバーセキュリティ工学）」では、サイバーセキュリティを意識した製品開発活動を実現できることが正式な要求事項として定められています。これには、IP開発やSoCへのIP統合などのプロセスが含まれます。本稿では、ISO/SAE 26262と比較しながらISO/SAE 21434の概要をご紹介した後、ISO/SAE 21434の要求事項に基づいた製品開発のためのサイバーセキュリティ・プロセスとベスト・プラクティスについてご説明します。

はじめに

自動車業界は現在、ADASから自動運転車へと移行する過渡期にあります。自動運転車では非常に多くのセンサーが必要となるため、自動車用センサーとそれらを管理する電子コントローラへの需要が急速に増大しています。GVR社の市場調査レポートによると、自動車の電子部品は車両コスト全体の約50%を占めると見られています。車載センサーが車両内の他のコンポーネントやインターネットと接続することで、ロボタクシー、車両追跡と物流管理、農耕車両など新しい画期的なアプリケーションが数多く実現しています。また、5Gなど無線技術の高速化と低遅延化により、車車間（V2V）通信が現実のものとなっています。しかし、こうした技術の進歩には光と影の両面があります。車載アプリケーションでインターネットに接続されたすべてのセンサーが、今や犯罪活動の潜在的な標的となっており、このようなアプリケーションを使用することのリスクが非常に高くなっています。このため、適切なセキュリティ対策なしにインターネットに接続することは現実的でありません。先進のアプリケーションにサイバーセキュリティを組み込むことは、アプリケーションそのものを開発することと同じくらい重要になっているのが現状です。

自動車業界の場合、ニュースになるようなサイバー犯罪は金融業界やインフラ産業ほどは多くありませんが、だからと言って車載アプリケーションが攻撃から無縁というわけではありません。特に自動車業界がインターネット接続を採用するようになってからは、リスクが高まっています。昔は、銀行強盗を働くには犯罪者自らも銀行へ行くというリスクを冒す必要がありました。しかしインターネット接続が登場してからは、犯罪者は地球の反対側にあるカフェに居ながら、身分を明かすことなく銀行からお金を盗むことができるようになっています。これと同じことが自動車業界でも起こっており、遠隔からの攻撃を受けるリスクが高まっています。しかも、こうした攻撃がもたらす結果は、他の業界よりもはるかに重大なものになる可能性があります。Craig Smith著「Car Hacker’s Handbook」の第9章にあるように、攻撃者が無線インターフェイスを利用してリモートで車両のCANバスへのアクセスに成功すると、車両位置の追跡やCANバス・ネットワークへのジャミングなどの攻撃を仕掛けることができ、最悪の場合、ドライバーが車両を制御できなくなることもあります。

かつて車載アプリケーションがインターネットに接続していなかった時代には、製品開発においてサイバーセキュリティが意識されることはありませんでした。ところが最近は車両内外のさまざまな電子部品同士を連携させた高度なアプリケーションが導入されるようになっており、サイバーセキュリティを意識した製品を求める声に応える形で新しい規格の策定が進められています。個々のIPコアに始まり、ECU、複数のECUを使用したシステム、クラウド・アプリケーションまで、あらゆる製品がこれらのアプリケーションと安全に連携する必要があります。ISO/SAE 21434は、業界全体でサイバーセキュリティ・プラクティスを標準化し、サプライチェーンに属するサプライヤーとベンダ間の協業を合理化する必要性に対処します。このようにISO/SAE 21434を採用することにより、サプライチェーン全体で組織ごとに異なるプロセスの溝を埋め、生産性と製品のサイバーセキュリティ保証を改善することができます。

ISO/SAE 21434とは

ISO/SAE 21434は、「ISO 26262 Road Vehicles—Functional Safety（路上走行車 — 機能安全)」を基盤とした規格で、車載製品ライフサイクルのサイバーセキュリティ面に対処します。これら2つの規格には、規格の意図から製品ライフサイクルのさまざまなステージで生成される文書のフォーマットに関するガイドラインまで、多くの類似点があります。例えば、ISO 21434で使用される用語とその定義も、ISO 26262の用語に似ているか、そこから着想を得たものが多く存在します。

ISO 21434はISO 26262と同じような構成となっており、製品開発の各ステージでのさまざまなグループの責任について説明しています。

- 組織でサイバーセキュリティ工学を促進する際には、経営幹部から製品開発チームまでが連携した取り組みを展開する。
- ベンダまたはサプライヤーとサプライチェーンの次の階層の組織との間で役割と責任を標準化する。これにより、業界全体で技術用語を標準化できるなど多くの利点が得られる。
- 製品ライフサイクルを複数のステージに分け、各ステージで出力され次のステージに入力する成果物を明確に定義する。
- ハザード分析とリスク評価（HARA）と同様に、TARA（脅威分析とリスク評価）を記述して製品のサイバーセキュリティ・リスクを評価する。
- 製品開発ライフサイクルのいくつかのステージの目標達成に役立つサポート・プロセスを定義する。

文書全体の構成だけでなく、規格の各トピックも同じような構成となっています。いずれのトピックも最初に明確な目標が示されており、その後に入力、必須条件、詳細情報が述べられた後、要件、推奨事項、作業成果物について説明されています。

新しい規格を理解する際には新しい用語が障害となることがよくありますが、ISO 21434はISO 26262と似た用語を採用しているため、ISO 26262の知識があれば容易に理解できます。両規格に共通している用語には、以下のものがあります。

- アイテム
- コンポーネント
- リスク
- 影響度/深刻度
- 道路利用者
- ダメージ・シナリオ/危険事象

このため、ISO 26262に準拠したプロセスを既に確立している組織は、ISO/SAE 21434の導入に関して有利な立場にあります。

サイバーセキュリティの課題に前向きに取り組む

製品にサイバーセキュリティを組み込むことは容易ではありません。何らかのサイバーセキュリティ保証レベルを確保するには、製品開発チームは、開発ライフサイクルのあらゆる段階でこれまで以上に多くの事項を考慮し、手順をこなす必要があります。しかも、特にユーザビリティや性能に関する製品要件とサイバーセキュリティの要件が競合することも珍しくありません。簡単な例として、暗号化を利用して個人情報を管理する場合、暗号化の機能を追加すると、データを平文で保存および転送する場合に比べコストが増大し、性能が低下します。自動車のリアカメラなどのエッジ機器にはセンシティブな個人情報が写り込む可能性もありますが、このような機器は低コストが求められるだけに、撮影した動画をインフォテインメント・システムに転送する前に暗号化を実行できるだけのCPU性能もハードウェア・リソースも搭載されていないことが考えられます。しかし転送される動画を暗号化していないと、中間者攻撃によってセンシティブなな情報が盗まれかねません。また、リアカメラとインフォテインメント・システムの間のチャネルを非対称暗号化で保護するには膨大な計算が必要であり、これによってインフォテインメント・システムへの動画転送に遅延が生じる可能性があります。このような遅延があると、動画転送のタイミング要件を満たせなくなります。

また、安全とセキュリティの要件が競合するようなケースもあります。例えば、自動車メーカーが車両のルーフに大きな衝撃が加わった場合にドアを解錠する安全機能を追加したとします。これは、横転事故があった場合にドアを解錠して乗員を車外へ脱出させるための機能です。しかしこの機能を悪用すると、駐車中の自動車のルーフの上で人が飛び跳ねてドアを解錠し、セキュリティ機能を破ることができます。性能への影響であればプラットフォームの性能を強化することで問題を解決できますが、安全とセキュリティの要件が競合する場合はアーキテクチャを変更するか、何らかの製品を追加して安全とセキュリティの両方の要件が満たされるようにする必要があります。要するに、サイバーセキュリティには何らかのコストが伴います。

現状

SAEとシノプシスが実施した自動車業界のサイバーセキュリティに関する独立調査では、回答者の52%が明らかな危険を認識していますが（図1）、サイバーセキュリティに関する懸念を上層部に報告する権限がないと感じている回答者が69%にのぼっています。このことは、サイバーセキュリティ保証を伴う製品開発には、経営幹部による指令が必要であるという事実を物語っています。サイバーセキュリティの意識向上はボトムアップ方式では効果がなく、トップダウンのアプローチをとる必要があります。

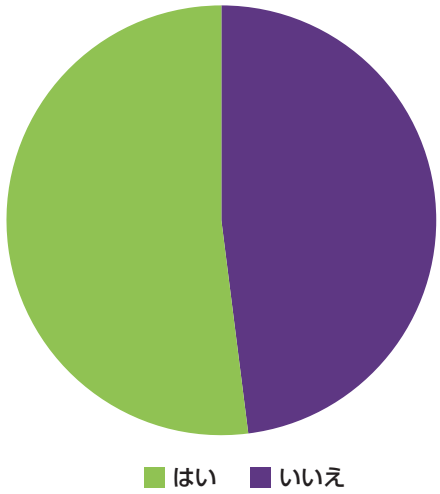

図1：サイバーセキュリティの懸念を組織に報告していますか

サイバーセキュリティ対策を組織のビジョンに組み込み、そこから裾野のR&Dおよびサポート・チームへ広がっていくことによってサイバーセキュリティ工学のためのリソースとツールを作成することが望まれます。上記の調査では、サイバーセキュリティの懸念に対処するための能力やツールを備えた正式な製品サイバーセキュリティ・プログラムやチームが存在しないと答えた回答者が41%にのぼっています。

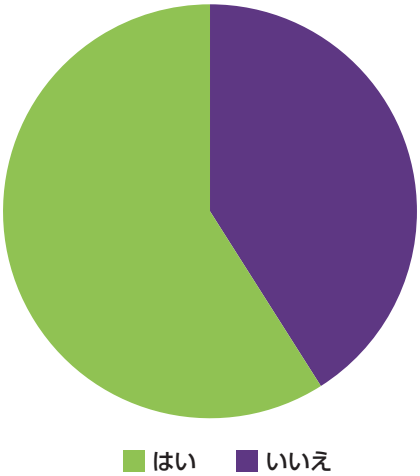

図2：正式なサイバーセキュリティ・プログラムを設立していますか（自動車サプライヤーへの質問）

経営幹部によるコミットメントの必要性

前述の通り、ISO 21434はISO 26262と同様に経営陣の責任に関する具体的なガイドラインを示すことにより、サイバーセキュリティに対する経営幹部のコミットメントの重要性を強調しています。さらに、この規格はサイバーセキュリティのルールとプロセスを執行するサイバーセキュリティ・ポリシーを定義することも要求しています。このポリシーは、まずこれらのルールとプロセスを執行するサイバーセキュリティの役割を定義し、ポリシーの実施に必要なリソースを規定します。この規格では、ポリシー、役割、リソースを文書化した作業成果物が定義されています。

一般的な組織では、図3に示すように専門のサイバーセキュリティ・チームがポリシーの定義と執行を担当します。このチームの役割は製品のサイバーセキュリティ保証を管理することにあり、製品開発スケジュールなどのコミットメントによって適正評価の実施が損なわれることのないように、製品開発チームから独立したマネージメント・チェーンの下で十分な精査を行う必要があります。サイバーセキュリティ保証チームは、以下のものを作成/創出し、維持する責任を負います。

- サイバーセキュリティ・ポリシー
- サイバーセキュリティ・プロセスおよび手続き
- サイバーセキュリティへの意識
- 設計チームのサイバーセキュリティ能力
- 製品のサイバーセキュリティ保証
- 製品のサイバーセキュリティ評価

前出の調査では、自動車のサプライヤー・エコシステムの半数でこれらの重要な役割や責任が存在していないことが判明しています。51%の回答者がサイバーセキュリティに対処できるだけのリソースが組織に存在しないと答えており、組織に十分なサイバーセキュリティ・スキルが備わっていないと答えた回答者は62%にのぼっています。サイバーセキュリティ保証チームは、サイバーセキュリティ工学に必要なテクノロジ・ツールを提供します。そして、このチームがサイバーセキュリティ保証を達成するためのプロセスを執行します。これらのプロセスによって、ISO 21434などの業界標準に準拠したエビデンスが生成され、これを監査プロセスの入力として使用します。

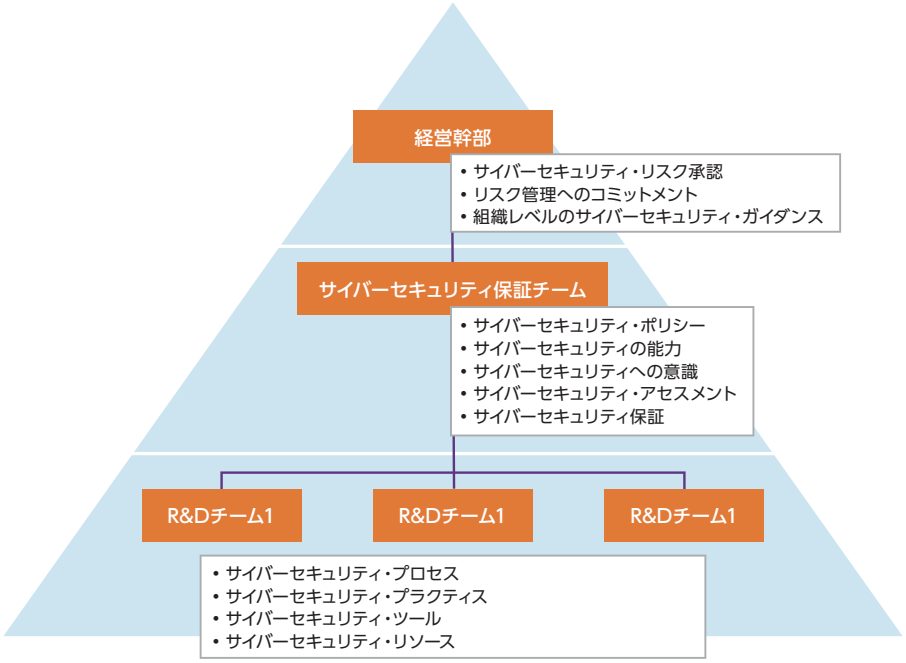

図3：組織の全階層にまたがるサイバーセキュリティ・チーム

サイバーセキュリティを意識した SoC 開発のプロセスとプラクティス

ポリシー、プロセス、プラクティスを理解することは、設計チームが製品およびサービスのセキュリティ態勢を高めるのに役立ちます。必要なプロセスやプラクティスは組織が策定し、提供する製品に合わせて調整しながら継続的に改善を図っていきます。

継続的な改善によって自己修正メカニズムが備わり、策定されたプロセスが効果的に機能し続けることが可能となります。継続的な改善をプロセスに組み込むには、各プロセスの客観的指標を定義することが1つの方法となります。このような指標は、プロセスのパフォーマンスが意図した通りであるかどうかを測る物差しとなります。プロセスのパフォーマンスを指標に照らし合わせて定期的に評価することにより、プロセスの効果と効率を維持するために必要な是正措置をとることができます。

サイバーセキュリティ・プロセス

ISO 21434規格には、業界プラクティスと一致したサイバーセキュリティ・プロセスが規定されています。これらのプロセスは、組織が開発する製品またはサービスのあらゆる面を考慮しています。開発サイクルのすべての段階に関係するものもあれば、サイバーセキュリティの特定の面のみに対処するものもあります。本稿では、以下のプロセスについてご説明します。

- セキュア開発ライフサイクル
- サイバーセキュリティ・リスクの評価と管理
- サプライチェーンのセキュリティ
- インシデント対応と脆弱性管理

セキュアな開発ライフサイクル

セキュア開発ライフサイクル（SDL）は、Microsoft社が提唱しているサイバーセキュリティ・プロセスで、製品開発のあらゆる段階にサイバーセキュリティを組み込みます。SDLでは、開発の各段階で実行すべき具体的な活動の内容と達成すべき基準が明記されており、これらの基準を満たさないと、その開発段階は完了したとは見なされません。また、SDLでは各開発段階における個々の活動に関して収集すべきエビデンスと、これらのエビデンスに対する要件も定義されています。このような要件を満たすエビデンスは、指定された手順に従わないと生成できないため、開発チームは必ずすべての手順に従うことになります。

SDLが適切に策定されれば、製品にサイバーセキュリティが組み込まれ、製品開発のなるべく早い段階で生成されたエビデンスを通じてサイバーセキュリティ保証がもたらされます。これにより、製品開発の観点からシフト・レフトが可能となり、開発ライフサイクルの最も早い段階でサイバーセキュリティを考慮することで、サイバーセキュリティの問題をいち早く見つけることが可能になります。SDLの最初のステップは、製品のコンセプト段階よりも先に開始します。SDLでは、設計チームに対してセキュア設計、

セキュア・コーディング、セキュア・テスト、脅威モデリング、プライバシーなどサイバーセキュリティのベスト・プラクティスについてトレーニングを実施することが要求されています。これにより、サイバーセキュリティ全般に関するチームの能力が向上します。また、トレーニング・プログラムの内容をプロジェクト要件に合わせて調整することにより、開発ライフサイクルが始まる前にベスト・プラクティスをチームに浸透させることができます。ISO 21434規格でも指摘されているように、トレーニング・プログラムは製品開発においてベスト・プラクティスが考慮されたことを証明するエビデンスとしての役割を果たすため、このようなトレーニングは製品のサイバーセキュリティ保証を高めます。

SDLでは、製品の早期コンセプト段階で脅威モデリングを実施することが要求されています。脅威モデリングは製品の成熟度が進むにつれて繰り返し実施すべきものですが、コンセプト段階で実施しておくと、サイバーセキュリティ保証レベルの目標達成に必要なセキュリティ対策をいち早く特定できます。これにより、サイバーセキュリティ保証の要求を満たすために必要な部品表（BOM）、設計チームのスキルセット、能力、CI/CDインフラストラクチャ、リソース、ツールなど、技術面以外の要件を決定できるようになります。

脅威モデルの例：ボディ制御モジュール ECU

ここでは、集中ドアロック、パワー・ドア、パワー・ウィンドウなど、車両のボディ機能を電子的に監視・制御するボディ制御モジュール（BCM）ECUの例を考えてみます。車両ドアの現在の状態をヘッドアップディスプレイに表示するには、これらの状態を車載インフォテイメント（IVI）に伝える必要があるため、BCMとIVIの間には何らかの通信チャネルが存在するものと考えられます。ほとんどの場合、これらのECUは両方とも同じCANバス上に存在します。ここで、IVIシステムはWiFiまたはRF接続によってインターネットに接続されていると仮定します。BCMは、ユーザー・コマンドおよび特定の条件（例えば車速が5km/hを超えたらドアを開けない、など）に基づいてソレノイド機構を制御し、機械部品を動かす（または動かさない）というシンプルなECUであるのが理想です。これまでがそうであったように、このように単純なユース・ケースでは特別なセキュリティ対策は必要ありません。

しかし、インターネットに接続されたIVIは、大きな脅威にさらされます。IVIが侵害されると、BCMにCANメッセージを送信してドアを開けることも可能となります。そうすると、車両の盗難を招くだけでなく、乗員の安全を脅かすなどさまざまな被害が生じることが考えられます。脅威モデルは、このようなシナリオを特定するためのプロセスです。早期段階で脅威モデリングを実施すれば、アーキテクチャの大幅な変更を必要とするような要件をいち早く取り入れることができます。この例では、BCMが受信した車両ドア操作コマンドが認証済みであることを保証するメカニズムが必要になります。このような大幅な変更が製品開発の終盤になって見つかると、製品の予算、範囲、スケジュールへの大きな影響が避けられません。

SDL の策定フェーズの要件

SDLの策定フェーズでは、チームがトレーニングを受けたセキュア・プラクティスを取り入れていることを証明するエビデンスの生成が義務付けられています。このエビデンスには、セキュリティ設計レビュー、セキュリティ検証計画レビュー、プライバシー設計レビューのほか、シノプシスのCoverityなどのツールで生成されるソフトウェア・コード・カバレッジ・レポートのような製品メトリクス、およびシノプシスのBlack Duckなどのツールで生成されるコンポジション解析レポート（製品に使用されている既製品のソフトウェア・コンポーネントの脆弱性や、既製品コンポーネントの使用によって生じるサードパーティ・ライセンスの競合などを検出したもの）が含まれます。これ以外のポストモーテム・ツールを使用して製品のセキュリティ態勢と成熟度を検証することもできます。製品のセキュリティ態勢を検証するには、ファジング・ツールやペネトレーション・テスト・ツールなどの特別なツールを使用することがSDLでは強く推奨されています。また、これらのツールによって生成されるレポートは、製品のサイバーセキュリティ・リードによる検証を受けることがSDLでは要求されています。しかしこれらの特別なツールを利用するにはコストがかかる上、機微な情報を扱う製品でなければ特に適用する必要もありません。このため、SDLでは適切に正当化できる場合はこれらのツールを省略できるようになっています。

最後に、製品リリース後のサポート準備を整えるため、SDLでは量産後のセキュリティ対策に関する要件を仕様に落とし込むことが必須とされています。これらの要件は、製品がサプライチェーンを流れている間や運用環境にある間に、製品のサイバーセキュリティを保証する上で重要な役割を果たします。例えば、あるデバイスが運用環境において一意であることを保証するために秘密鍵が必要な場合、漏えいの可能性を小さくするためにデバイス内で一意な鍵を生成する必要があります。デバイス内で生成された鍵は、製品内部の安全な鍵保管庫に保管されていれば、外部に漏えいすることは決してありません。しかしローエンドのデバイスでは、非対称鍵を生成すると性能が低下し、ブート・タイミングなど製品の動作要件を満たさなくなる可能性があるため、このレベルのセキュリティを利用できないことがあります。特に、大きな素数を使用するRSA鍵の生成には困難が伴います。このような鍵を専用の暗号化ハードウェアで生成しようとすると、BOMコストに大きく影響します。このような場合、製造フロアで

秘密鍵を製品にプロビジョニングし、公開鍵を一意のデバイス識別子とペアリングする必要があります。製品が運用環境に到達するまで製品のセキュリティ態勢が維持されるように、製造後に実行されるこれらのサイバーセキュリティ関連プロセスの要件を規定することがSDLでは義務付けられています。

サプライチェーンのセキュリティ

ここでは、サードパーティが開発したSoCを内蔵するECUに秘密鍵をプロビジョニングする場合を例に考えてみます。ごく一般的なプラクティスとして、ECUメーカーがSoCメーカーから提供されるスタックをリファレンスとして使用しながら、ユース・ケースを実現するために独自のソフトウェア・スタックを開発することがよくあります。ソフトウェア・スタックが異なると暗号ライブラリも異なるため、鍵の扱いも変わってきます。SoCの暗号化フレームワーク（暗号化アクセラレータなど）を開発したチームと、暗号化フレームワークを使用するチームは異なります。そこで、SoCメーカーがECUメーカーに対してSoCの暗号機能とセキュリティへの影響について詳細な情報を伝えることが重要となりますが、これは通常のデータシートやリファレンス・スタックでは不可能です。この場合、脅威モデルやサイバーセキュリティ・リスク評価レポートなど、セキュリティへの影響を詳細に記述した、サイバーセキュリティに関する包括的な文書が必要となります。このような文書があれば、ECUメーカーはサイバーセキュリティ保証の目標を達成するためのセキュリティ対策に必要なすべての情報を手にすることができるため、セキュアなアプリケーションを開発する上ではるかに有利になります。

このことは、製品のコンポーネントやソフトウェア・スタックの1つ1つがサプライチェーンのさまざまな企業から供給され、1つの製品が多くの組織の協業によって開発されるような統合型の産業では、サイバーセキュリティは独力では達成できないという事実を物語っています。サイバーセキュリティ保証の目標を達成するには、サプライチェーンに属するすべての組織がサイバーセキュリティを意識して協業する必要があります。最終製品は共同開発によるものであり、顧客に販売している製品は（OEMが販売する製品を除き）最終製品ではないことをサプライチェーンに属するすべての組織が認識し、受け入れる必要があります。このような考え方を持って開発活動を計画すれば、顧客側は開発サイクルの中でサプライヤーからサイバーセキュリティに必要なすべての情報の提供を受けられるようになり、サプライヤー側は顧客がサイバーセキュリティの観点から製品を完全に理解できるように自身の開発サイクルでサイバーセキュリティに関する十分な文書が生成されるようにできます。

図4：サプライチェーンのすべての組織間でのサイバーセキュリティに関する協業

サプライヤーと顧客は、それぞれの製品開発ステージをばらばらに考えるのではなく、最終製品の開発の一部と捉えるのが理想です。しかし、部品サプライヤーのほとんどは特定の1社のために製品を製造しているわけではないため、これは困難です。サプライヤーが製造する製品のほとんどは汎用品であり、その用途は特定の顧客1社のユース・ケースには限定されません。サプライヤーと顧客が一体となって製品開発を進めることが難しいとしても、それぞれがばらばらに開発作業を進めるという状態を改善することは可能です。そのためには、サプライヤーと顧客がそれぞれどのように活動を分担するかを定義し、互いの責任を明確に定義するようにします。例えば、顧客がサプライヤーに対して製品のサイバーセキュリティ・リスク評価を要求したり、製品に対するサイバーセキュリティ・バリデーションの実施を要求したりできます。このような役割分担は、CIA（Cybersecurity Interface Agreement）に盛り込むようにします。CIAは、RFQ（見積もり依頼）の一部に含める場合もあります。

サプライヤーは、顧客にサプライヤーのサイバーセキュリティ能力を評価する機会を与えるようなサイバーセキュリティ・プラクティスをこのCIAに定めておくことが推奨されます（図5）。この情報により、顧客はサプライヤーが自社のサイバーセキュリティ・プロセスをサポートできるかどうかを把握できるようになります。顧客のサイバーセキュリティ・プロセスには、製品開発中のプロセスだけでなく、セキュリティ・インシデント対応など製造後のプロセスも含まれます。サプライヤーが自身のサイバーセキュリティ・プロセスを十分にサポートできていなければ、顧客が自社製品のサイバーセキュリティを保証することはできません。例えば、ECUメーカーにセキュリティ・インシデントが報告され、そのセキュリティ・インシデントを引き起こした脆弱性がSoCに存在することが判明した場合、ECUメーカーはその問題をSoCメーカーのインシデント対応システムに報告する必要があります。脆弱性に迅速に対処するにはインシデント対応プロセスを確立しておく必要があるため、SoCメーカーがそのようなプロセスを実装していなければ、脆弱性がゼロデイ攻撃を受ける可能性が非常に高くなります。サプライヤーのサイバーセキュリティ・プロセスは、サプライヤーのセキュリティ能力を測る指標となるため、顧客はサプライヤーにプロジェクトを発注する際に、十分な情報に基づいた判断を下せるようになります。

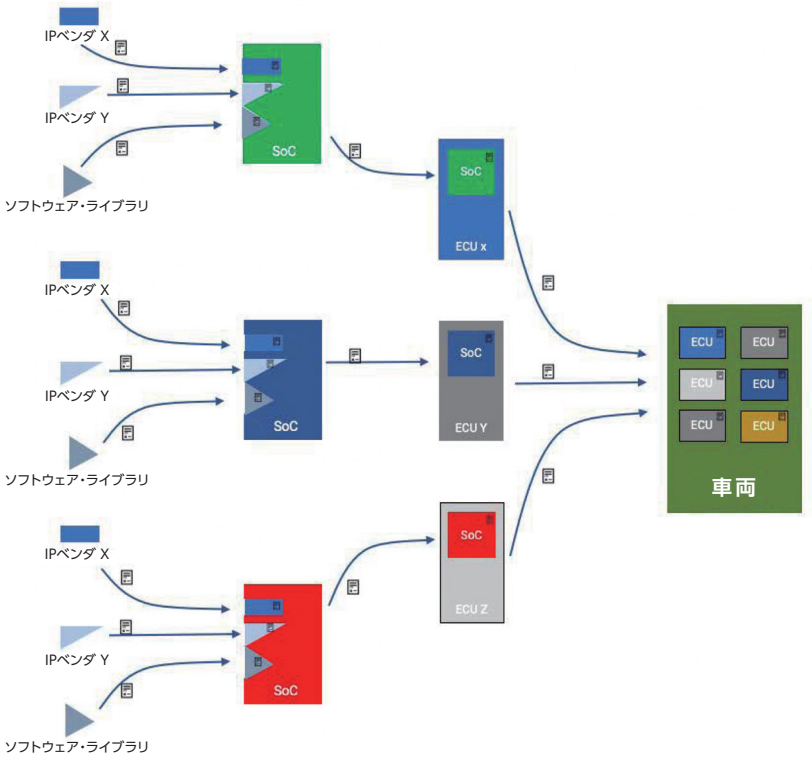

図5: サプライチェーンにおけるサイバーセキュリティ契約

これまで、サプライチェーンのサイバーセキュリティに関する議論は、最終製品が運用環境で受ける攻撃のシナリオしか考慮していませんでした。しかし、サプライチェーン自体も攻撃に対して非常に脆弱です。このため、サプライチェーンのサイバーセキュリティ問題を解決することは不可能であると考えるセキュリティ専門家もあります。この状況を難しくしているのが、サプライチェーンの多様性です。1つの製品のサプライチェーンが世界中に張り巡らされていることもあるため、サイバーセキュリティ攻撃を受ける可能性のある潜在的な脅威表面は広範囲にわたります。清掃業者であれ設計エンジニアであれ、情報システムに物理的または仮想的な手段でアクセスできる者が、数十から数百ものコンポーネントのうち、たった1つを侵害するだけで製品全体が侵害されます。しかも、こうした侵害は高い確率で検出をくぐり抜けます。このような侵害を受けると、製品に影響するだけでなく、その運用環境も侵害される可能性があります。

サプライチェーンのセキュリティは複雑で大きなテーマであり、入念な議論を必要とします。このため、サイバーセキュリティ保証の観点からサプライヤーと顧客が強力な協業を進めることが必要となります。サプライヤーは、自身が販売するコンポーネントの完全性と真正性を検証する信頼できるメカニズムを構築する必要があります。サプライチェーンは非常に脆弱であるため、ゼロトラストの原則が重要な要件となります。つまり、顧客はサイバーセキュリティに関するサプライヤーの信頼度にかかわらず、サプライヤーから受け取るすべてのコンポーネントについて、それらを製品やエコシステムに組み込む前に検証することが求められます。

リスクの評価と管理

サイバーセキュリティに関しては、製品を徹底的に調査し、内在するリスクや運用環境で使用した場合に生じる可能性のあるリスクを特定し、これらのリスクが攻撃者によって悪用されないように適切な軽減策を適用できるようにする必要があります。サイバーセキュリティ・リスクの深刻度は、4つの要因によって決まります。これら4つの要因を使用してリスク・スコアを求め、このスコアに基づいてリスクへの対処方法を決めることにより、客観的な意思決定が可能となります。

図6に示すように、リスク・スコアの算出に使用する要因とは、脅威シナリオ、脅威が製品に与える影響、攻撃経路、攻撃の実現可能性の4つです。脅威シナリオと脅威が製品に与える潜在的影響の2つの要因により、製品およびその運用環境に与える被害の大きさが決まります。攻撃経路は、製品において脅威がどのように悪用されるかを決定します。攻撃の実現可能性は、攻撃経路の実現がどれだけ容易かを評価するものです。攻撃経路とその実現可能性の2つの要因を組み合わせることにより、攻撃を受ける可能性が決まります。そして、脅威がもたらす潜在的な被害の大きさと攻撃を受ける可能性の2つの要因を組み合わせることによって、製品に対するリスクが決まります。これら4つの要因について詳しく論じる前に、まずリスク評価で使用される一般的な用語についてご説明します。

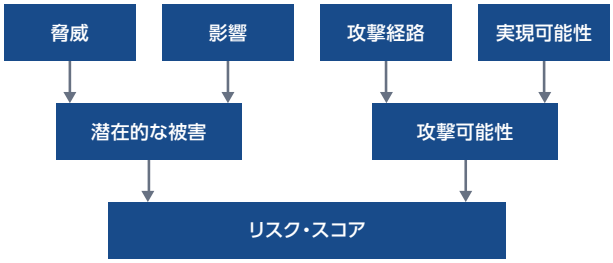

図6：リスク・スコアの要素

- **サイバーセキュリティの属性**：機密性、完全性、可用性
- **資産**：ユーザーまたは攻撃者にとって価値あるものすべて。資産は一次資産と二次資産に分類されます。二次資産とは、それ自体には価値がない資産のことで、攻撃者は二次資産を利用して一次資産にアクセスし、それによって製品を侵害します。
- **脆弱性**：悪用することで製品の動作を変えることができるような弱点。
- **脅威**：製品の通常の動作を変えてしまうような、製品に対して加えられる危害。
- **脅威モデリング**：製品およびその動作環境に対する脅威を特定するための構造的なアプローチ。
- **脅威シナリオ**：攻撃者が製品に存在する脆弱性またはバグをどのように悪用して製品の1つ以上の資産を侵害するかを想定したもの。

脅威モデリングの実行方法には、資産中心、STRIDE、PASTA、ペルソナ・ノン・グラータ（PnG）など多くの方法があり、これらはそれぞれアプローチが異なります。どの脅威モデリング手法を使用するかは、製品のアーキテクチャおよびその動作環境に基づいて選択します。ただし、組み込み製品で最も一般的なのは、資産中心の脅威モデリングです（図7）。資産中心の脅威モデリングでは、最初に資産を特定します。このようにして、脅威モデリング・プロセスで製品の最も重要な面へと焦点を絞り込んでいきます。

図7：資産中心の脅威モデリング

次に、資産の脆弱なサイバーセキュリティ属性を特定します。これらの属性は、過去の攻撃シナリオ、CVEデータベース、セキュリティ専門家による製品アーキテクチャのレビュー、暗号プリミティブの使用などに基づいて特定できます。次に、これらの脆弱なサイバーセキュリティ属性の 1 つが悪用された場合に製品にもたらされる脅威を特定します。この段階で、製品に存在する潜在的な脅威シナリオが特定されます。ここでも、製品およびその運用環境に基づき、製品に対する脅威アクターをプロファイリングします。脅威アクターを特定すると、これらの脅威アクターが脅威シナリオを実現するための手段とする潜在的な攻撃経路を特定しやすくなります。脅威モデリングの最後には、セキュリティ対策を導入して攻撃経路を防ぐ、またはアーキテクチャに存在する弱点に対処して脅威そのものを取り除く、などの軽減策を提言します。

脅威モデリングは、リスク・スコアの決定に使用する 2 つの要因、すなわち脅威シナリオと攻撃経路を特定します。残りの 2 つの要因は、製品のサイバーセキュリティ・リスク評価の中で特定する必要があります。脅威シナリオの影響度は、運用環境においてその脅威が製品に与える悪影響を分析して決定します。このような悪影響として、ISO 21434 規格では運用環境における人体の安全への影響、金銭的損失、製品の運用上の障害、機微な個人情報の流出が挙げられています。影響度とは、これらすべての面を考慮し、脅威によって生じる被害の深刻度を示したものです。そして、この被害の深刻度に基づき、脅威への対処方法を客観的に決定します。

最後に、攻撃経路を分析して攻撃の実現可能性を決定します。攻撃の実現可能性を決定するには、攻撃経路の実現に必要なツール、手法、スキルセット、リソースを調査する必要があります。攻撃の実現可能性を「高い」と「非常に低い」の間で評価するアプローチはいくつもあります。ISO 21434 規格では、攻撃の可能性に基づくアプローチ、攻撃ベクターに基づくアプローチ、CVSS に基づくアプローチなどが説明されており、これらの各アプローチを採用する際に考慮すべき要因、および考慮した指標に基づいて攻撃の実現可能性レベルを決定するためのガイダンスも示されています。また、脅威モデリングで実施した攻撃者プロファイリングを考慮することも重要です。攻撃の実現可能性はスキルセットやリソースなどに基づいて決定されるため、攻撃者プロファイルによって大きく左右されます。政府からの資金援助を受けてサイバー戦争を仕掛けるサイバーセキュリティ・チームの方が単な

るサイバー犯罪者よりもリソース・レベルがはるかに高く、全般にスキルセットも高いため、サイバー犯罪者に対して「中」と評価される実現可能性であっても、国家主体に対しては「高」と評価されることがあります。このため、攻撃の実現可能性を評価する際には攻撃者のプロファイルを考慮することが重要です。

次に、4 つの要因すべてを総合してリスク・スコアを決定します。ISO 21434 規格には、リスク値の決定方法についても 2 つの例が説明されており、どちらを採用するかは製品のニーズに応じて決めることができます。簡単なのは、マトリックスを使用してリスク値を決定する方法で、実現可能性と影響度の 2 次元マトリックスを使用し、それぞれの評価に基づいて 1 ～ 5 のリスク値を割り当てます。ただしこの方法では、実現可能性と影響度の評価段階が少ないため（高、中、低など）、きめ細かなリスク値を柔軟に割り当てることができません。しかも、最終的なリスク・スコアへの影響を勘案しながら実現可能性や影響度のスコアを評価者が調整することもできません。例えば、影響度のスコアが同じ「高」なら、I2C インターフェイス IP であっても暗号化アクセラレータ・セキュリティ IP であっても、リスク値に与える影響は同じになります。

これに対し、数式を使用してリスク値を決定する方法では、各要因が最終的なリスク値に与える影響を調整することができます。この方法では、影響度と攻撃の実現可能性の各評価レベルに数値を割り当て、運用環境に対する製品の重大度に基づいてこれらの数値を調整できるため、キーストアや暗号化アクセラレータのように機微な情報を扱う重要なセキュリティ IP に対しては、それ以外の IP よりも高いリスク値を与えることができます。例えば、影響度の評価「重大」に対し、I2C デバイスでは 1.5 を割り当て、暗号化アクセラレータでは 2 を割り当てるといったことが可能です。このようにしてリスクを数式（例：リスク値 = 影響度の評価 x 実現可能性の評価 + 1）で計算すると、実現可能性の評価が同じであっても暗号化アクセラレータに対して I2C デバイスよりも高い値を割り当てることができます。

脅威のリスク値を決定する根本的な理由とは、リスクへの対処法を客観的に判断し、製品がサイバーセキュリティ保証レベルの目標を達成できるようにすることにあります。リスクへの対処方法は、リスク値に応じて次の 4 つがあります。

- **軽減**：製品に対する脅威の影響を軽減するような変更を加えます。例えば、脅威を防ぐためにアーキテクチャに変更を加える（機微なデータに対する読み出しポリシーを「読み出し」から「使用」へ変更するなど）、サイバーセキュリティ対策を組み込んで攻撃経路にチェックポイントを導入する（SoC 内の 2 つの IP 間で交換されるメッセージを暗号化して機密性を保護するなど）、などがあります。
- **回避**：脅威を生み出すような機能を取り除きます。例えば、ABS など高リスクの SoC では OTA アップデート機能を取り除き、インターネット経由での攻撃による悪用を防ぎます。
- **移転**：保険に加入するなどの契約によってリスクの影響を共有します。
- **受容**：リスクに対処するための活動を何も行いません。一般的には、製品に対する影響度が低いか、攻撃の実現可能性が低いためにリスク値が非常に低く、しかもリスクを防ぐための対策にかかるコストがリスクそのものを上回るような場合が該当します。

サイバーセキュリティの製造後サポート

一般に、サイバーセキュリティ対策とは、将来いずれかの時点で侵害されるという前提で実装されています。このため、最新のサイバーセキュリティ侵害を常に監視し、製品とサービスをそのような攻撃から保護するための対策を組織のサイバーセキュリティ・ポリシーに盛り込むことが必要です。このプロセスは 2 つの部分から成り、製品が意図した通りのサイバーセキュリティ保証を確実に維持できるようにするには、どちらも非常に重要です。

- 脆弱性管理：組織が開発した製品に既知の脆弱性が存在していないかを能動的にチェックします。
- インシデント対応：製品が侵害を受けた場合、製品のサイバーセキュリティ保証またはその動作環境に直接影響するセキュリティ・インシデントに対処します。これは受動的なアプローチです。

脆弱性管理とは、製品リリース時に確約した製品のサイバーセキュリティ保証を継続的に監視するプロセスです。この保証レベルを維持するための取り組みは、サイバーセキュリティの観点から製品が廃棄されるまで続きます。これは継続的なプロセスであるため、製品に存在する既知の脆弱性を定期的にチェックする必要があります。この作業は 2 つのステップで構成されます。最初のステップでは、製品に関連する脆弱性データベース、自主的な情報開示、最新の侵害事例を調査し、新しい発見や情報開示をトリアージします。次のステップでは、新たに発見された脆弱性が製品のサイバーセキュリティ保証に与える影響について分析します。

脆弱性をスキャンする間隔は、バランスを考慮して決めることが重要です。間隔が長すぎると、脆弱性が広く知れ渡る前に検出して対処することができず、侵害を招く可能性があります。逆に間隔が短すぎると、リソースを過剰に消費します。

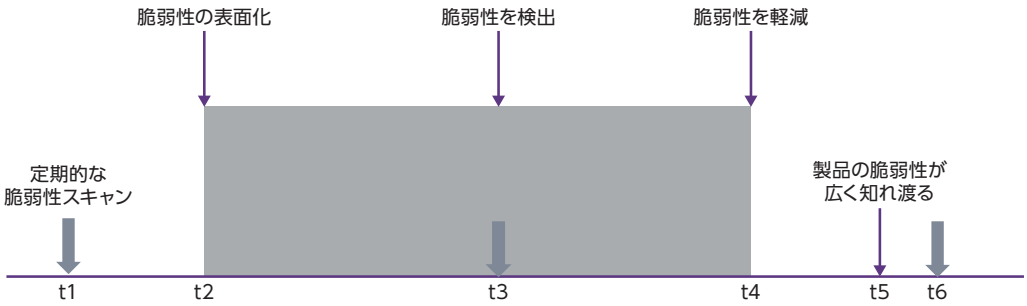

図8：バランスのとれた脆弱性スキャンの間隔

脆弱性管理の目標は、t5の前にt4を完了することです。ただし、すべての場合にこれが可能とは限りません。特に、オープン設計による製品ではt2 = t5となること、すなわち、脆弱性がパブリック・ドメインで表面化した直後に、製品の機能にその脆弱性があることが広く知れ渡ることがあります。このような場合は、脆弱性を回避するのではなく、その影響度を軽減することを目標とします。このような場合に必要となるのが、サイバーセキュリティ・インシデント管理です。

サイバーセキュリティの世界では、悪用される前にすべての脆弱性を修正するのが理想です。しかし、これはさまざまな理由で不可能です。広く知られている脆弱性が悪用されると（または悪用されたと考えられると）、サイバーセキュリティ・インシデントが発生します。広く知られた脆弱性の影響度を抑制するには、十分に定義されたサイバーセキュリティ・インシデント対応プロセスを確立しておく必要があります。インシデント対応プロセスでは、報告されたインシデントを迅速に処理し、それを適切な設計チームに伝達して軽減してもらえるようにトリアージ計画を定義する必要があります。このプロセスでは、脆弱性を素早く処理するためにすべての設計チームが担うべき役割を定義する必要があります。

サイバーセキュリティ・インシデント対応プロセスは、組織外部から製品に存在する脆弱性の報告を受けた時点で開始します。例えば、顧客が統合テストやシステム・テスト時に製品の脆弱性を発見して報告する場合や、セキュリティ研究者が調査中に脆弱性を発見した場合などがこれに該当します。このプロセスでは、まだ一般に公開されていないセキュリティ・インシデントを扱うため、組織に対してインシデントを秘密裏に報告できるようなメカニズムが必要です。報告メカニズムがセキュアでないと、組織に報告されるすべての脆弱性が攻撃者に筒抜けになるため、脆弱性の悪用が容易になります。また、このプロセスでは、報告された脆弱性に関する情報にアクセスできる人員を、組織内でその情報を本当に必要とする者に限るよう、厳密に管理する必要があります。組織に不満を持った従業員が金銭目的で脆弱性に関する情報をリークすることもあります。このため、このプロセスではインシデントの報告に関してだけでなく、トリアージ、軽減、および運用環境での製品への解決策の導入時にも機密性を維持できるようなメカニズムを用意しておく必要があります。

解決策の導入には、影響を受ける当事者（製品を最終製品に統合した顧客や、エコシステムに製品を導入した顧客など）に脆弱性の存在を知らせ、その解決策を提供することも含まれます。既製品のコンポーネントなど、広く運用される製品の場合は、インシデント管理プロセスの一環として責任ある脆弱性開示メカニズムを用意し、影響を受けるすべての当事者が脆弱性情報を入手して迅速に是正措置を講じられるようにする必要があります。

まとめ

自動車業界が新しい可能性を求めて電子化を進める中、道路利用者に対する潜在的な危害は指数関数的に増大しており、サイバーセキュリティへの取り組みが必須となっています。この指数関数的な増大は、自動車業界におけるエレクトロニクスの導入とサイバーセキュリティの脅威の両方が急速に拡大していることに原因があります。このように脅威への露出が増えたことにより、顧客は今後、製品の安全および品質保証と同様にサイバーセキュリティ保証を求めるようになってきます。また、顧客は単なる認証だけでなく、サプライヤーのサイバーセキュリティ・プロセスに関する詳細も要求してくる可能性があります。コンポーネント・サプライヤーが自動車市場で競争力を維持するには、標準化が進められているサイバーセキュリティの原則とプロセスを採用することが不可欠となっています。