第 4 回自動車サイバーセキュリティ講座
質疑未回答分

9 月 3 日
自動車セキュリティ概論
Q.複数の団体がプロセス（ベストプラクティス）を定義しているようですがそれらには差異があり、仕向け国などに応じて対応を変えないといけないような状況なのでしょうか？

A. セキュリティによらず国によって異なる規制が適用されている場合は、各国規則に従う必要があります。セキュリティに関しては、58 協定国であれば基本的に国連規則に従い、58 協定国以外（アメリカや中国など）は独自規則になります。すでに中国は独自 GB/T の内容が策定されています。
また Best Practice は複数存在し、かつ時代とともに変化していきますが、どの国でも満足する先進的なグローバル統一対策をするか、各国別に対策を作り分けるかの判断は、台数やコスト、および国ごとの提供サービスや接続先など様々な要因から、技術的観点と商品戦略の観点で決定することになると考えています。

Q.パーソナルデータについて国ごとに法規が異なるとのお話でしたが、例えばドラレコの録画データについて取扱を定めている法規はありますか？
A. 車両内に保有するデータに対して、自動車向け法規の存在は認識していません。一方、車内データをセンターなどとの通信によって車外に持ち出した場合は、GDPR などの法規制に従うことになります。
（参考）
ドラレコではありませんが、Event Data Recorder に対して、VDA が以下最終ページで記載しています。
但し、ドラレコは車外画像が含まれるため、この事例には該当しないという認識です。
https://www.pdpjournals.com/docs/99009.pdf

自動車用サイバーセキュリティ法規の概要
Q.P33 Slide17　4-3 国内法規適用時期（'20/7/10 案）・「第 21 項」はどの法規を指しているのでしょうか。・「OTA なし、SU あり」とは、有線による SU という理解でよろしいでしょうか。・「OTA なし、SU なし」の非自動運転車は、令和4年7月以降にも CS と SU が適用除外という理解でよろしいでしょうか。 P38～P39 Slide27~30 ・赤字部分の「審査マニュアル」はどこに公開されているのでしょうか。

A.「第 21 項」とは、この 8 月に発行された特定改造等の許可に関する省令、

自動車の特定改造等の許可に関する技術上の基準に係る細目等を定める告示の規定に記載された条項になります。

・「OTA なし、SU あり」とは有線による SU のことです。

・「OTA なし、SU なし」の非自動運転車の時期につきましては、資料としては「？」としており、いまだ国交省殿と交渉中です。

・「審査マニュアル」についてですが、当局以外には、自工会、部工会、自動車輸入組合、車体工業会　にのみ開示されている資料です。ですので、それ以外の方には開示されておりません。

Q. スライド p.21　7.2 節の適合認定書に基づき 7.3 節の型式認可が得られたとしまして、もし適合認定書の更新ミスや取り消された場合は、あわせて型式認定も取り消されるのでしょうか？　背景：SU Regulation には、SU の適合証明書が取り消されても型式認定は取り消されないと記されていますが、CS Regulation にはその旨が記載されていないではと捉えております。

A. 法規本文には、型式認定の取り消しは記載されておりません。

CSMS が効力を失うと、次に出荷する車両の型式認定が取れなくなると理解しています。

Q. 「脅威に関連する脆弱性又は攻撃方法」と、開発のコンセプトフェーズで実施する脅威分析とはどう関連するのでしょうか。型式要件 3.3 で各項目「考慮しろ」となっていますが、例えば、マッピングして各項目の可能性の程度を示すべきなのでしょうか。また、講義の中で、この別添の作成経緯や WP での議論を説明いただきましたが、もう一度この表の意図を説明いただきたいです。

A. 型式要件の３．３でリスク特定～アセスを実施する際に、Annex５の脆弱性、攻撃方法を考慮したか？という要件です。

考慮したのであれば、Yes として回答。内容を問われれば、どのように考慮したかを説明することになります。この説明は千差万別で、全体を俯瞰して該当する箇所のみ採用して使用もありと思います。

この表はあくまで Annex なので、要件そのものではなく、Shall 要件でもありません。

Q. p.71 7.3.8 Cryptographic "module"ですが、暗号処理の HW チップ（SHE などの HSM）ではなく、暗号アルゴリズム、パラメータセット、暗号ライブラリなどの SW 要件と捉えて宜しいでしょうか？

質問の背景ですが、限られた時間枠でのご説明の中、お聞きする限りでは選択する"暗号アルゴリズム"が対象と捉えました。ただ、過去の Interpretation Document には、コンセンサス標準として ISO/IEC 19790:2012 や FIPS 140-3 という例が記載されており、暗号アルゴリズムのみならず

"実装"レベルで標準に沿う必要があるのではと捉えての質問でございます。

A. このモジュールの対象は、ソフトウェアでもハードウェアとも限定していません。
両方あり得ます。
またソフトウェアだけで説明もあり得ます。説得性次第です。

セキュリティインシデント事例

Q. 脅威や対策を考える上で確立している手法を用いたシステマチックな方法はあると思いますが、セキュリティのスペシャリストの経験によるところも大きいのでしょうか。例えば、最新の攻撃手法を知らないと脆弱性の考慮の漏れが出やすい、とか。各社そういう人材はなかなかいないと思うので、業界としての支援のありかたなど、考えをお聞かせねがえますか。

A. 設計時のセキュリティ対策を検討する際の、所謂、脅威分析やセキュリティ分析と呼ばれる分析手法に関するご質問と捉えて回答します。
現在、様々な手法が提案されていますが、どの手法についても特に具体的な脅威を記述する点に関して分析者の知見に依存しているところは大きいと思います。脅威に抜けがあれば必要な対策を講じることができませんので、それが脆弱性になり得ます。私の経験的には、最新の攻撃などに関する知識も重要ですが、まずは分析手法に慣れ親しみ、分析に必要となる考え方を掴んで頂くことが非常に重要だと思います。
業界の支援という観点では、トレーニングの提供や、最新の脅威などの情報共有などが必要と考えます。前者については本講座を企画しております委員会におきましても、セキュリティ分析等の演習を企画しております。また後者については各種コミュニティやサービスで入手頂けると思います。
ご質問への直接の回答ではありませんが、セキュリティのリスクは経営上のリスクです。人材育成等に必要なリソースの確保や体制構築に対する責任を、経営層は認識する必要があります。最後に、技術者の観点では、今やセキュリティは誰もが知っておくべき、身に着けておくべき知識や技術となりました。“セキュリティはよくわからない”という言葉を耳にすることもありますが、この講座や私の科目が、セキュリティにより興味を持って頂けたり、親しみを感じて頂けたりする、契機の一つになりましたら幸いです。

自動車セキュリティ技術①　自動車のセキュリティ開発

Q. スライド 26「他のアイテムとの相互作用」の例は、設計が進んでから決まるものもあるのかなと思うのですが、こういったものはイテレーティブに実施して詳細されるものもあるということですか。

A.「他のアイテムとの相互作用」の例に限らずイテレーティブに実施することは必要です。ご指摘いただいた設計が進んでから決まるものとして、スライド 43 に脆弱性分析の結果として新たな要件を追加しております。脆弱性分析の結果からどの程度のリスクがあり、リスクに対処すべきか、追加要件が妥当か否かは上流工程に戻って判断することが必要になります。
実開発においては、イテレーティブに実施すること、そして工程間のコミュニケーションをとることが要求の一貫性を確保するために重要と考えています。

9・4

自動車セキュリティ技術②　クルマにおける脆弱性ハンドリングとインシデント対応

Q.PSIRT の規模とはどれくらいのものなのでしょうか。例えば、インシデント対応フロー（スライド 25）に、PSIRT メンバーとして「製品領域担当」があります。この人は製品の知識とセキュリティの知識両方を兼ね備えることが期待されますが、そういう人が各領域にいて PSIRT に参加するイメージですか。

A.まず PSIRT の規模ですが会社の規模や組織体制に応じて大きく変わるとお考え下さい。

特に従来の組織の枠組み（例えば品質保証体制、等）を利用して整備、もしくは専任組織化するかでは大きく違ってくると思います。
特に 2 つ目のご質問にある様に製品とセキュリティ両方の知識を有する方は各社において非常に貴重な存在です。その方々の専任化を前提に PSIRT を構築することは非常に難しいと思います。従って入手した脆弱性やインシデントに応じて適切なエキスパートメンバーが招集できる仕組み等の整備と併せて御社の PSIRT 体制をご検討頂ければと思います。

Q.コネクティッドカーへの対策として、通信停止などの緊急対策と、パッチ開発･適用の根本対策があるのかと考えておりますが、p.24 のインシデント対応フローの中に、時間軸の異なる対策を上手く埋め込むコツがございましたら、ご教授頂けないでしょうか？

A.インシデント対応フローに時間軸の異なる対策を上手く埋め込むコツという事ですが P.24 の対応フローの従来プロセスの部分を少し詳細化すれば時間軸の異なる対策も埋め込めると思います。従来プロセスに例示記載させて頂いております品質プロセスには品質問題、特に安全に関わる課題を解決するプロセスがどこの OEM でも定められていると思います。このプロセスにはご質問に例示されている緊急対策と根本対策（恒久対策）の概念が既に織り込まれており、自動車 OEM としては既存の概念かつ両対策を並行して進めて行くことは特に特別なことではないと認識しています。詳細プロセスにつきましては関係外秘

となって居りますのでここではご容赦願いたいと思います。

Q.既存な開発プロセスの各段階にセキュリティ活動を追加しなければならないと思いますが、開発期間は以前より大幅に長くなりますか？

A.開発期間に関するご質問ですが確かにセキュリティの要求事項が増えるのは事実ですから検討すべき事や検証すべき事が増えます。
確かに従来の開発プロセスと並行、もしくは直列でセキュリティの開発プロセスを実行する場合はそうなるかもしれません。
しかし実際には従来ある開発プロセスにセキュリティの要求事項を上手に織り込めば開発期間が大幅に伸びることは無いとの認識です。

Q.インシデント対応で訓練される とのことですが防災訓練などのようにシナリオを用意してインシデントイベントを突発的・計画的に発生させ、対応フローが正常に機能しているのかをチェックしているのでしょうか？ 具体例などありましたらご教授いただけないでしょうか

A.訓練についてのご質問ですが防災訓練同様にその訓練で何を明らかにするのか、つまり目的に応じて各社訓練を実施されています。
この講座で何回か登場している J-Auto-ISAC で行っている訓練を一例として紹介しますと、
１、準備したシナリオをベースに社内の PSIRT メンバーや関係部門が手順通りに対応できるかを検証
２、準備したシナリオをベースにインシデントに関係するサプライチェーンの会社と連携しながら対応できるか検証
等を行い個社やサプライチェーンのウィークのあぶり出しやサプライチェーン間での役割分担等、訓練を重ねて加盟各社が PDCA を重ねてきています。
従って、訓練を計画される際に目的を明確にすることでより実践に即した訓練が行えると思います。

サイバーフィジカルセキュリティ技術　基礎・暗号・計測セキュリティ

Q.カメラやセンサは、ありのままを伝えることが機能的役割だと思います。攻撃対策はシステムで考えるべきで、カメラやセンサ単独による対策は不可能でしょうか。研究トレンドなどご教示お願いします。

A.カメラ、センサもシステムといえますので、カメラ単独やセンサ単独をどのように規定するかにより答えが変わって参ります。

撮像素子とかアナログフロントエンドの単位で考えた場合は、距離偽装攻撃に耐えるように対策をとることは難しそうにも思われますが、信号処理まで含めるならば、例えば ToF 方式であれば計測のために送信する信号の波形を工夫するとか、受信した信号の処理を送信した信号との関連でどのように行うか、などのセンサ単独でのセキュリティ強化策は有りえます。
もちろん、センサフュージョンに代表されるシステム的な対策は有効で本命かと思われますが、カメラ、センサへの攻撃により、通常の擾乱を越えた影響がある場合でも、カメラ、センサからのデータを用いた処理・制御に与えるインパクトを抑える工夫は様々にとらえられます。
応用面から末端のカメラ、センサに求められる要件を導き、それを満たすカメラ、センサを開発するといったシナリオが現実的ではないかと考えられます。
詳しい点は別途議論できましたら幸いです。

Q.自動車による事故・事件が起きた時、それが車載システムが攻撃されたことに起因するものか否かを問われる可能性があるかと思います。 LIDAR については、事後に検証可能なログ等を蓄えているものなのでしょうか。

A.LIDAR のデータは莫大となりますが、計測したデータ自体を一定の期間であれば蓄えておくことは可能です。LIDAR のデータだけでなく、制御のために用いた素材データを関連付けて蓄えることは有益です。ただ、実際の個別の自動車でログをどこまで取るかは、方針次第で様々ではないかと考えられます。