自動車セキュリティの義務化
全車種に拡大されるまで残り時間わずか

AUTOCRYPT

22年7月からセキュリティ実装の義務化

国連の自動車基準調和世界フォーラム（WP29）が採択した国際法規により、22年7月以降に生産される新型車はWP29が求めているサイバーセキュリティ管理システム（CSMS）とソフトウェアアップデート管理システム（SUMS）の要件を満たしていることを認証機関に証明する必要があります。技術サービス企業による分析及び検証を行い、その結果を基に、各国の認証機関で審査、車両型式認証が発行される形で証明されます。

OEM及びサプライヤーが準備すべき項目一覧

サイバーセキュリティ管理システム（CSMS）UN-R155

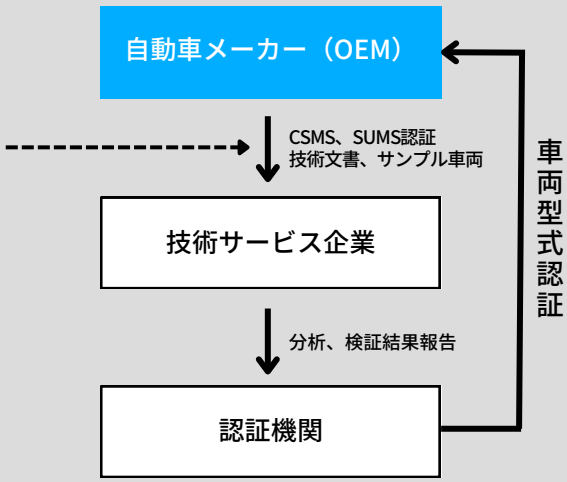
- OEMだけでなく、サプライチェーン全体まで網羅すること
- リスク特定、分析、評価、セキュリティインシデント分析、対応プロセス及び持続的な脆弱性検知プロセス構築など

ソフトウェアアップデート管理システム（SUMS）UN-R156

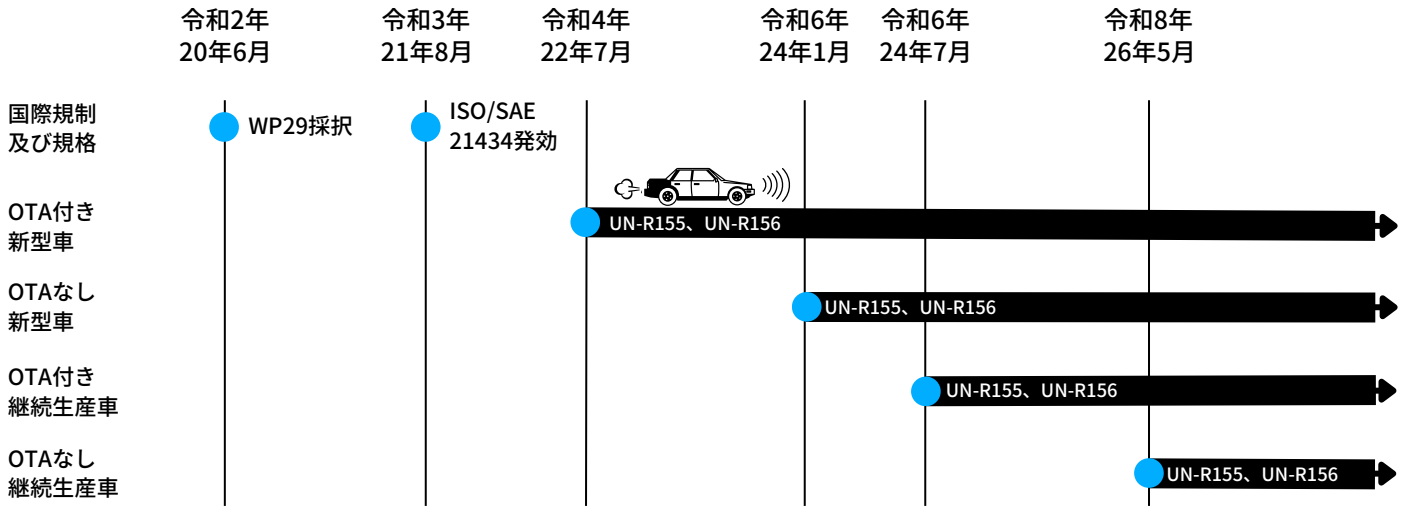
- RxSWINでソフトウェアバージョン管理プロセスを構築すること
- 危険なソフトウェアアップデートの防止、ソフトウェアアップデート時の安全性評価、ユーザへの更新情報通知プロセス構築など

*RxSWIN（Software Identification Number for Regulation X）とは？
：ソフトウェアのバージョンを管理するための基準

車両型式認証の流れ



自動車サイバーセキュリティに関する国内規制開始スケジュール*

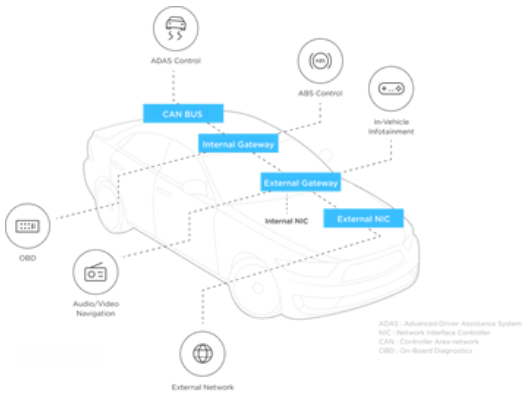


OTA：Over The Air

ソフトウェアアップデートがない自動車の場合、新型車は24年7月から、継続生産車は26年5月からUN-R155適用

*国土交通省の資料より作成：https://www.mlit.go.jp/report/press/content/001379922.pdf

AUTOCRYPTのコンサルティング
国際基準への完全対応サポート



サポート項目

WP29の実際参照先として多く使われているISO/SAE 21434の基準に沿い、自動車の開発プロセス、生産後メインテナンスなどの自動車ライフサイクル全般を考慮したサイバーセキュリティ対策を構築しなければなりません。対策だけでなく、国際基準に準拠した組織の構築、セキュリティインシデントに対して持続的な監視及び対応などが求められています。当社は組織の構成、教育からセキュリティインシデント対応まで、国際基準の要件を満たすために必要な全てのコンサルティングサービスを提供しています。

組織プロセス

- トレニンーグ
- CSMS構築コンサルティング
- 検証、認証サポート

車両別プロセス

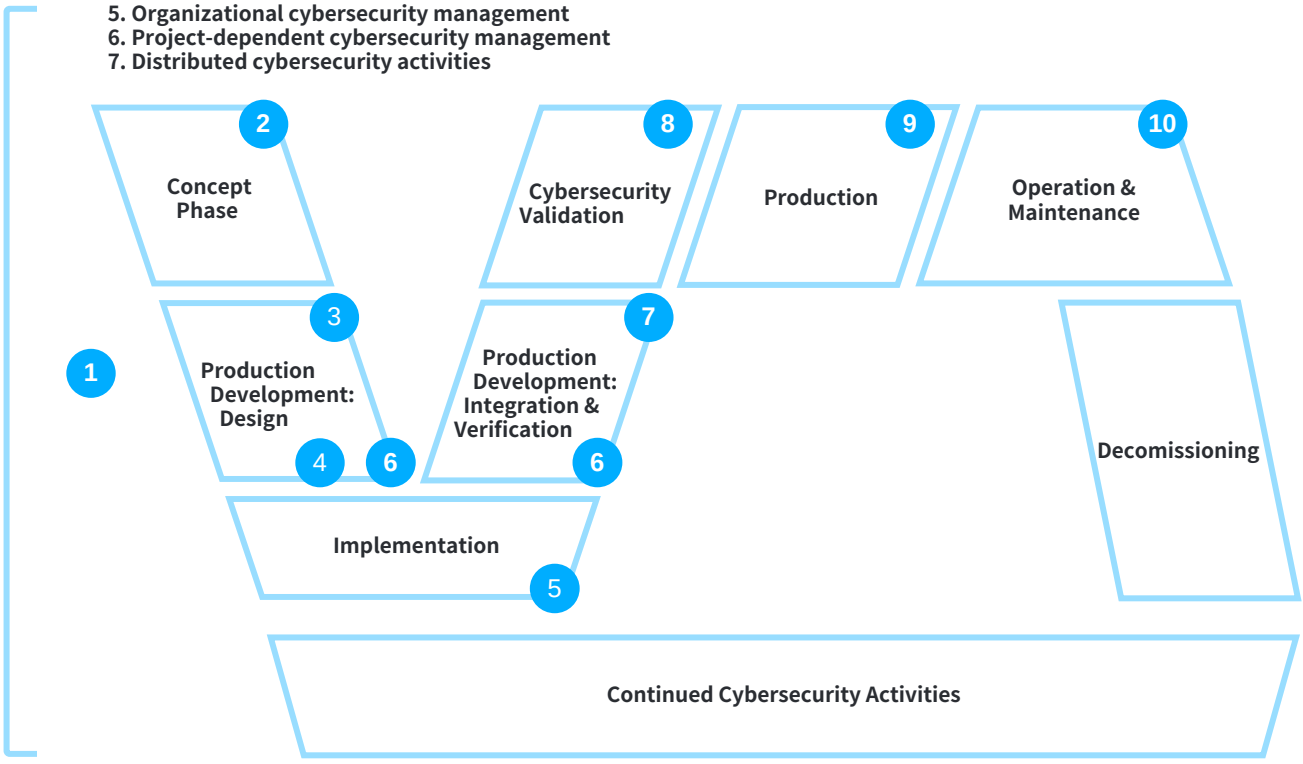
- 車両別セキュリティ構築
- サイバーセキュリティ開発
- テスト及び検証
- 車両評価及び認証サポート

生産後運用プロセス

- 車両SOC支援
- インシデント対応
- SIRT*活動サポート

*SIRT：Security Incident Response Team

AUTOCRYPTが提供する
包括的なマネジメントソリューション



AUTOCRYPT Solutions Offerings

1. CSMS / ISO 21434 consulting
2. TARA (Threat Analysis and Risk Assessment)
3. OEM requirement analysis
4. Security design & engineering
5. Security solution implementation (porting, customizing)
6. Vulnerability analysis and management
7. Fuzzing test
8. Penetration test
9. Incident response
10. Production-line integration

1 CSMS / ISO 21434 コンサルティング

- ギャップ分析によるプラン策定
- CSMS構築サポート

2 TARA分析 (Threat Analysis and Risk Assessment)

＋

3 OEM requirement analysis

- 企業の要求、条件分析
- 保護対象及びサイバー脅威特定
- 攻撃シナリオ作成、分析
- セキュリティゴール設定

4 Security design & engineering

- 企業ごとに異なる状況に合わせてセキュリティ設計
  ：セキュアブート、アクセス制御
  ：IDPS/ファイアウォール等車両に必要な
  セキュリティサービス提供

5 Security solution implementation (porting, customizing)

- セキュリティ設計を基に、サイバーセキュリティ実装
  ：「AutoCrypt IVS（In-Vehicle System）」
  ソリューション提供可能

6 Vulnerability analysis and management

- 専用分析ツール「AutoCrypt Security Analyzer」提供
  ：スニペット単位まで分析
  ：SBOM提供によるオープンソースの
  脆弱性及びライセンス違反を一元管理

7 Fuzzing test

- 専用分析ツール「AutoCrypt Security Fuzzer」提供
  ：AIを活用したテストの自動化
  ：CAN-FD利用でテスト時間短縮

8 Penetration test

- Red Teamによる専門的なファジングテスト
- 脆弱性検知・攻撃シナリオ作成
- 対策の有効性検証
- 改善策の提案

9 Incident response

- 車両SOC（Security Operation Center）提供
- 自動車のライフサイクル全体にわたる
  セキュリティ状況監視・管理可能

10 Production-line integration

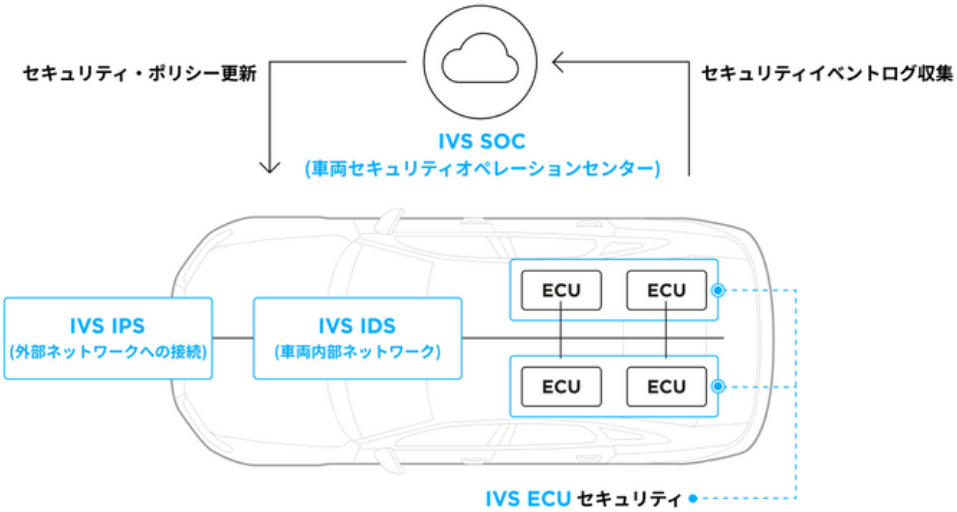
- 生産向け暗号鍵管理システム（KMS）及び
  公開鍵暗号基盤（PKI）提供

AUTOCRYPT IVS

AUTOCRYPT

SOLUTION: AUTOCRYPT IVS

アウトクリプトは、ECU セキュリティ、侵入検知・防御システム（IDPS）、車両 SOC など、 セキュアな車載アーキテクチャの実装と、セキュリティ対策の導入から運用まで一元的なサポートを提供します。車載システムに必要な多彩なサイバーセキュリティ対策を総合的なソリューションに体系化したものであり 、お客様に最適な形で提供することも可能です。



- IVS-ECU：IVS-ECUを通じてECUのセキュアブートやセキュアストレージのためのファイアウォールとモニタリング機能を提供し、ECUセキュリティにおける包括的なセキュリティ対策をサポートします。
- IVS-IDPS：CAN、CAN-FD、Ethernetなど、車載プロトコルにおける高度な侵入検知システム（IDS）及び防御システム（IPS）を提供します。
- IVS-SOC：AutoCrypt IVSから送信される車両データとの連携によってモニタリング機能を強化し、新なタイプの脅威や攻撃に対する素早い対応を支援します。

AUTOCRYPT
Secure First, Then Ride

アウトクリプト株式会社
〒162-0843
東京都新宿区市谷田町3-8市ヶ谷科学技術イノベーションセンタービル2F

ホームページ www.autocrypt.jp
お問い合わせ japan@autocrypt.io