Penta SECURITY

Asian Cyber Security Vendor of the Year

20 year Anniversary

Past & Future of Connected Car Security

「つながる車」のためのセキュリティの現在と未来。AUTOCRYPT

2017年2月

Penta Security Systems, Inc.

SL4 PUBLIC

目次

I. 「つながる車」とセキュリティの必然性

1. 「つながる車」時代の始まり
2. 「つながる車」のセキュリティを考える
3. ハッキング事例：JEEP Cherokee (2015.07)
4. 「つながる車」の安全は、セキュリティから始まる
5. 「つながる車」をターゲットとする脅威

II. AutoCrypt® ご紹介

1. AutoCrypt® 概要
2. AutoCrypt® 機能概要
3. AutoCrypt® V2X
4. AutoCrypt® PKI
5. AutoCrypt® KMS
6. AutoCrypt® AFW

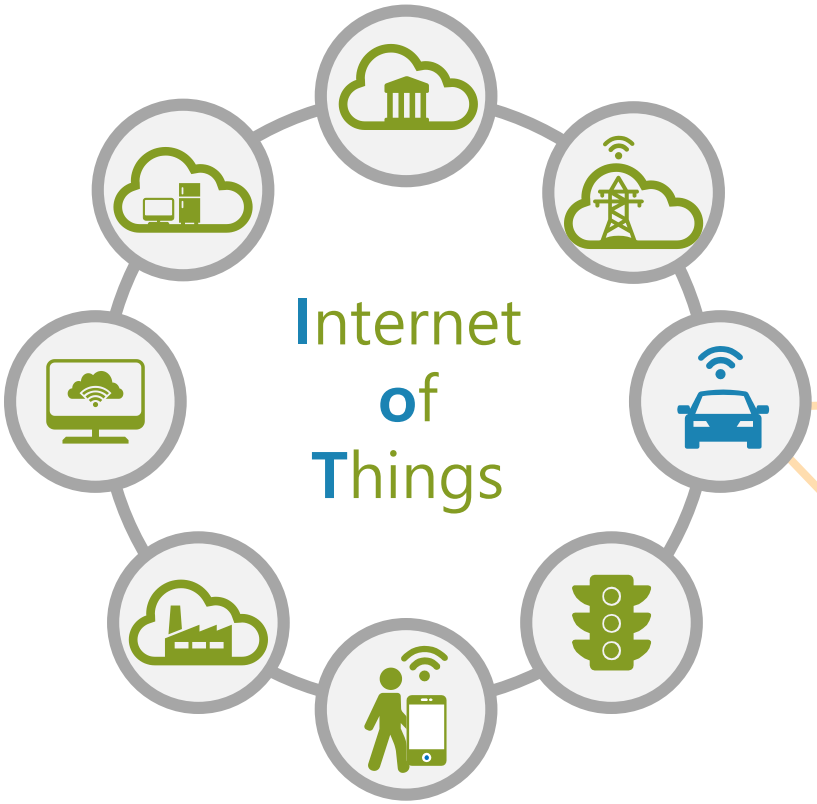
Penta SECURITY

20 year Anniversary

I. 「つながる車」とセキュリティの必然性

1. 「つながる車」時代の始まり
2. 「つながる車」のセキュリティを考える
3. ハッキング事例：JEEP Cherokee (2015.07)
4. 「つながる車」の安全は、セキュリティから始まる
5. 「つながる車」をターゲットとする脅威

「つながる車」時代の始まり

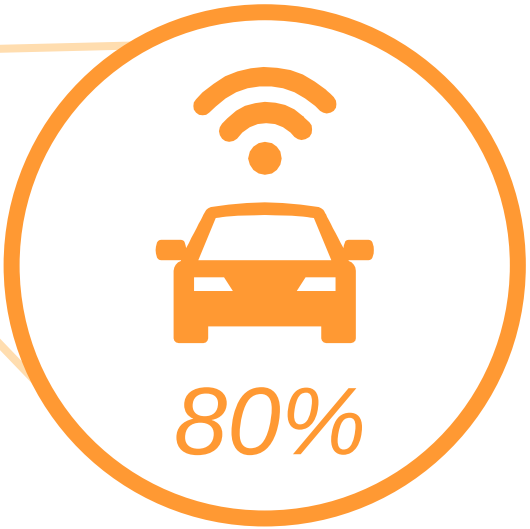


自動車の80%は、2020年までに接続される

80% of cars will be connected by 2020

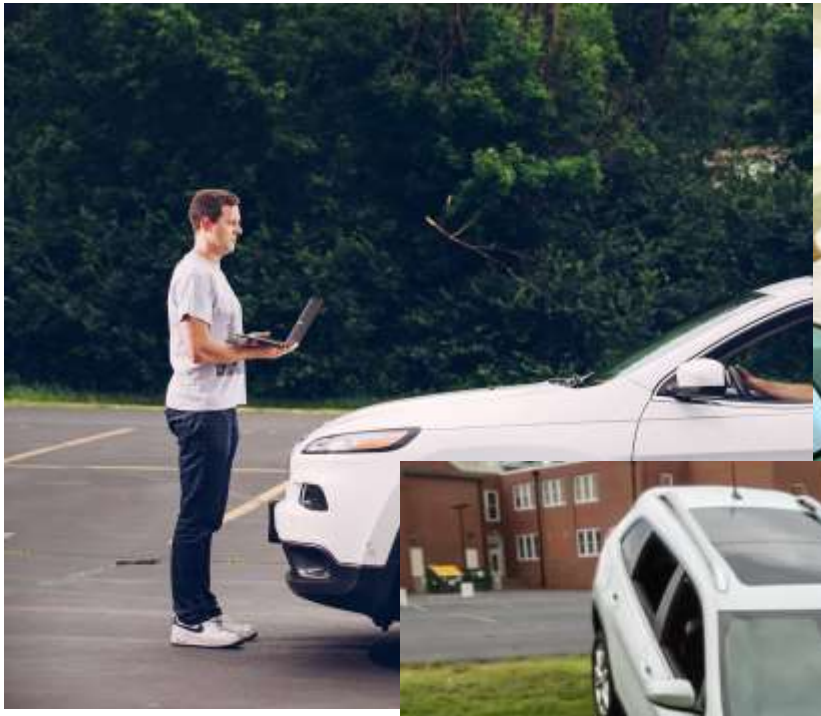
Gartner Market Trend Report, January 2016

Gartner states that by the 2020, roughly 80% of new vehicle models will have built-in data connectivity. This new channel has great potential as an attack vendor for hackers.



「つながる車」のセキュリティを考える

ハッキング事例：JEEP Cherokee (2015.07)

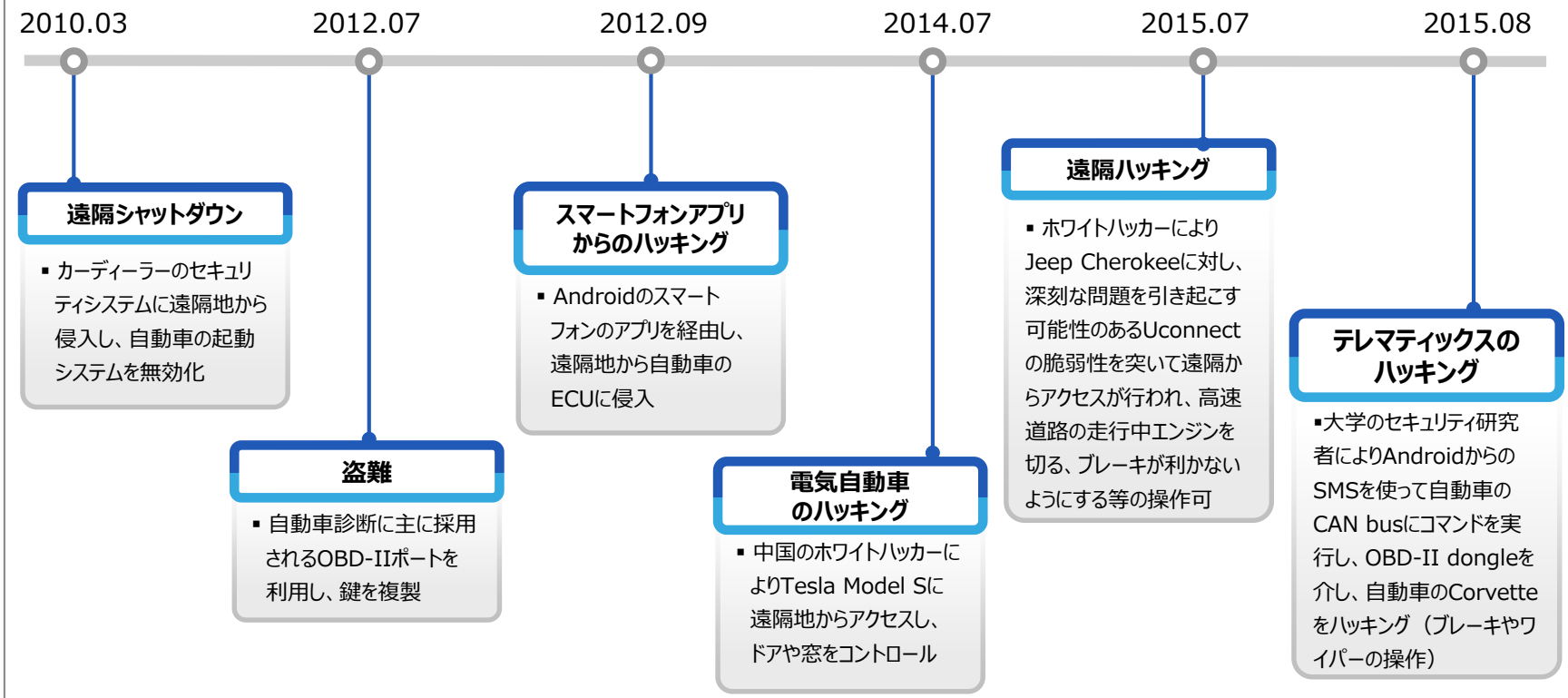


「つながる車」の安全は、セキュリティから始まる

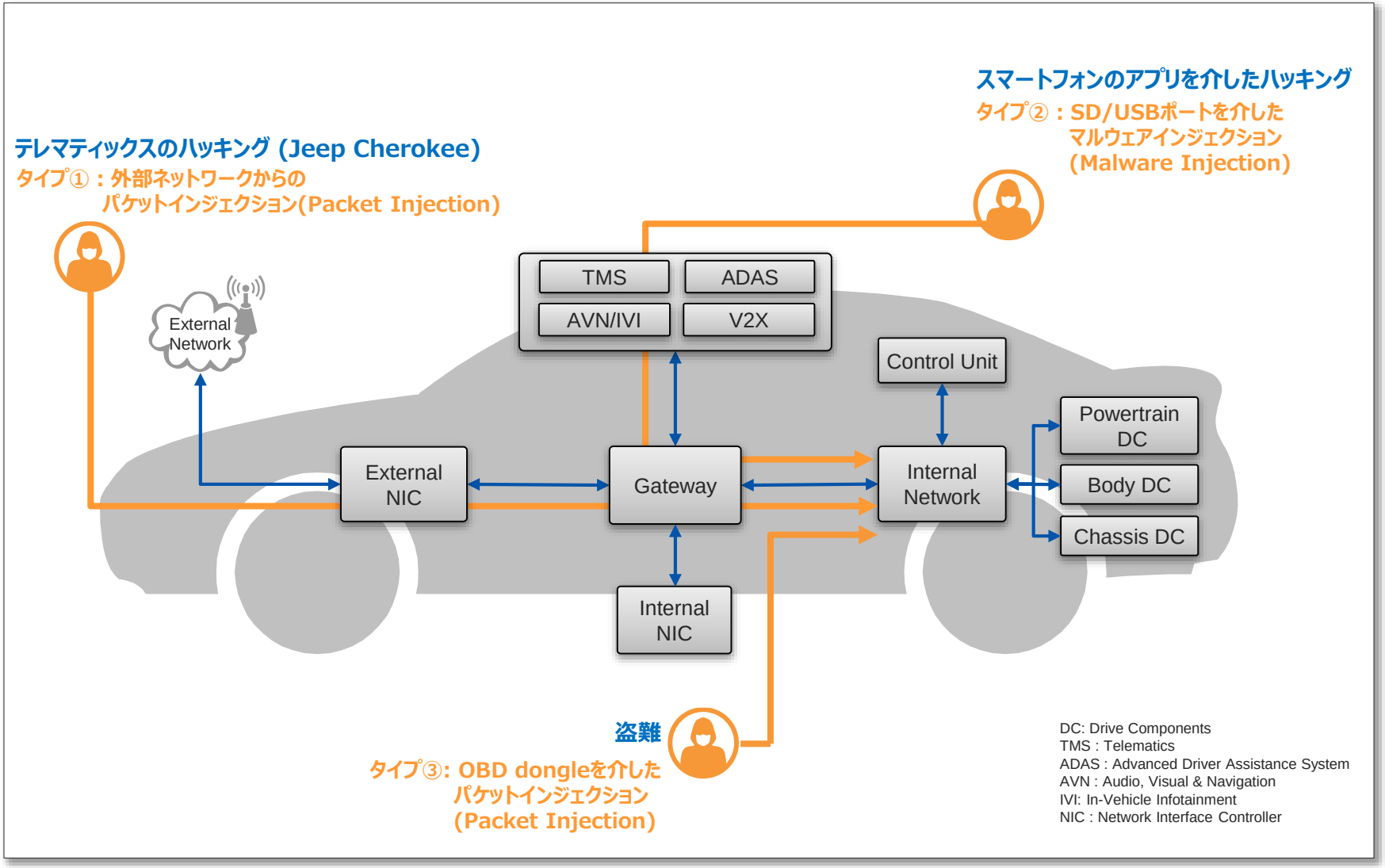
“Safety begins with Security”

安全は、セキュリティから始まる

今までのサイバー空間での脅威は、人に金銭的・物理的な損害を与えてきた。
自動車にセキュリティを実現しなければならない理由は、人命に関わるためである



「つながる車」をターゲットとする脅威



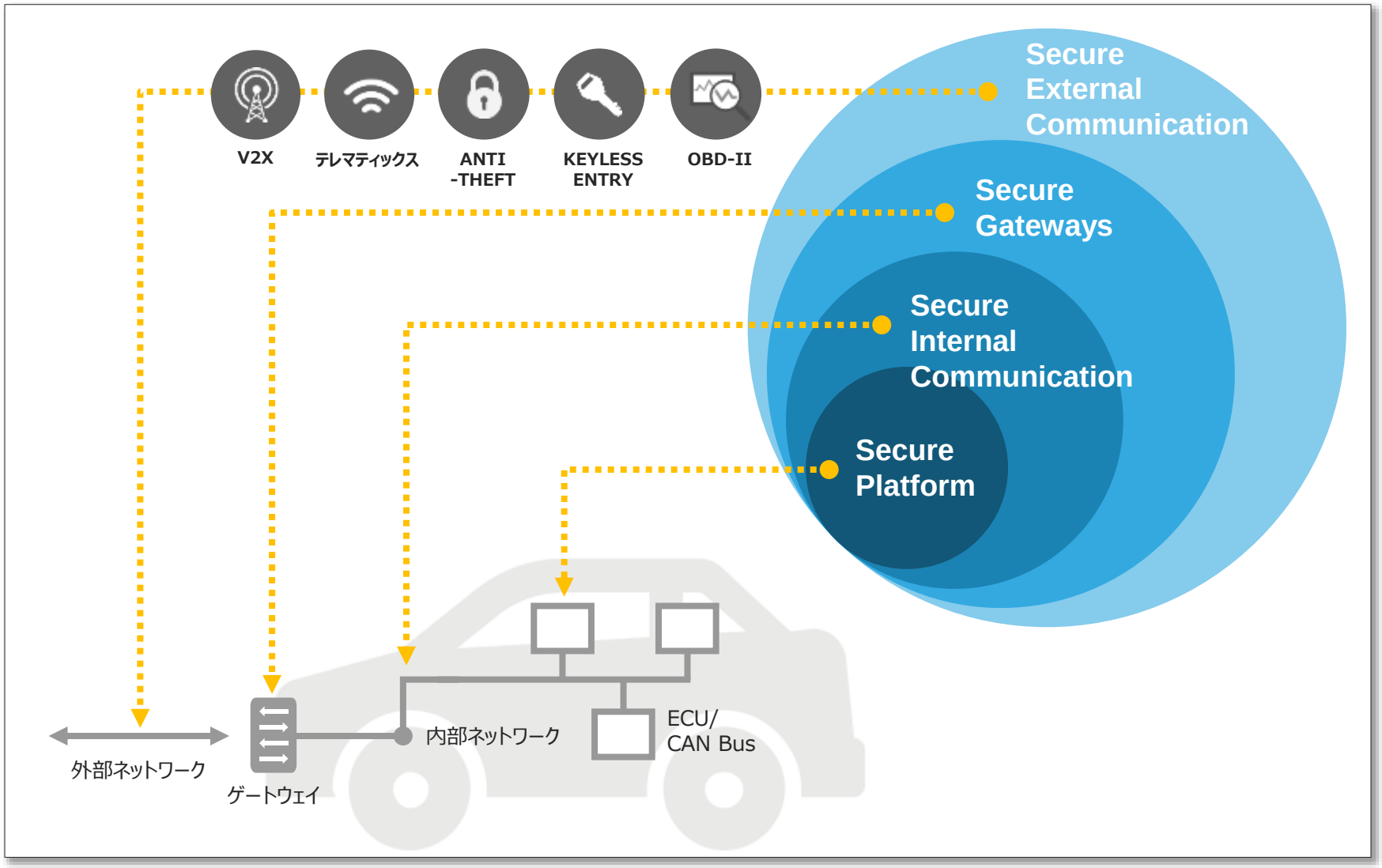
Penta SECURITY

20 year Anniversary

II. AutoCrypt® ご紹介

1. AutoCrypt® 概要
2. AutoCrypt® 機能概要
3. AutoCrypt® V2X
4. AutoCrypt® PKI
5. AutoCrypt® KMS
6. AutoCrypt® AFW

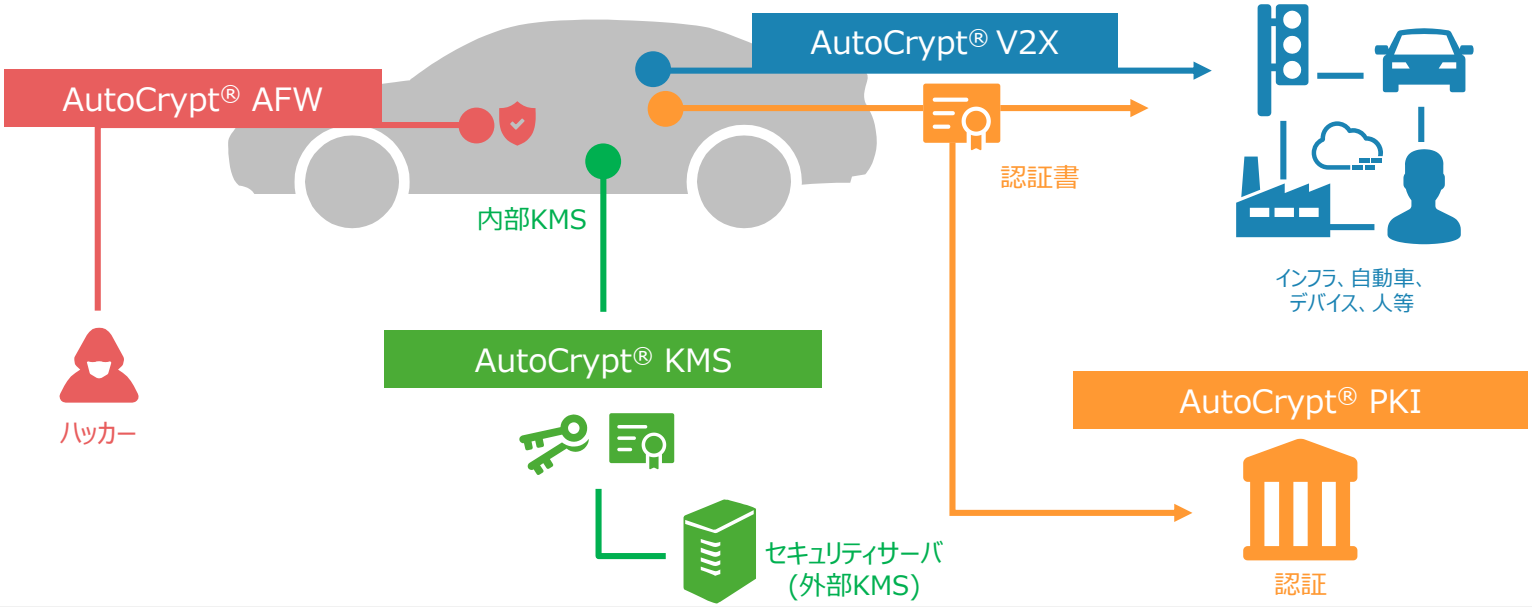
スマートカーのセキュリティ・レイヤー



AutoCrypt® 概要

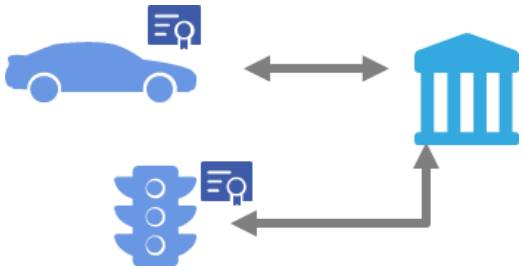
AutoCrypt®は、自動車の “セキュリティ” を実現し、ユーザの “安全” を確保するソリューションであり、次世代知能型交通システム(C-ITS)とスマートカーのためのセキュリティとして、AutoCrypt® V2X、AutoCrypt® PKI、AutoCrypt® KMS、AutoCrypt® AFWのコンポーネントで構成されています。

- **AutoCrypt® V2X: Vehicle-to-Anything**
- **AutoCrypt® PKI: Public Key Infrastructure**
- **AutoCrypt® KMS: Key Management System**
- **AutoCrypt® AFW: Advanced FireWall**

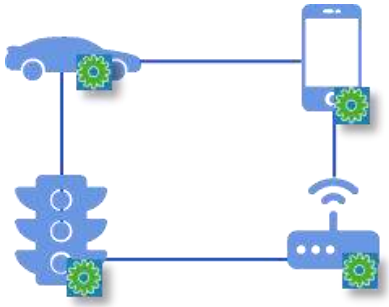


AutoCrypt® 機能概要

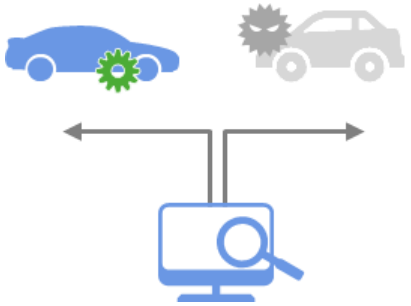
1 自動車PKI
Public Key Infrastructure



2 暗号化通信



3 誤用·盗用等
異常動作レポート



4 不正アクセスの検出および遮断

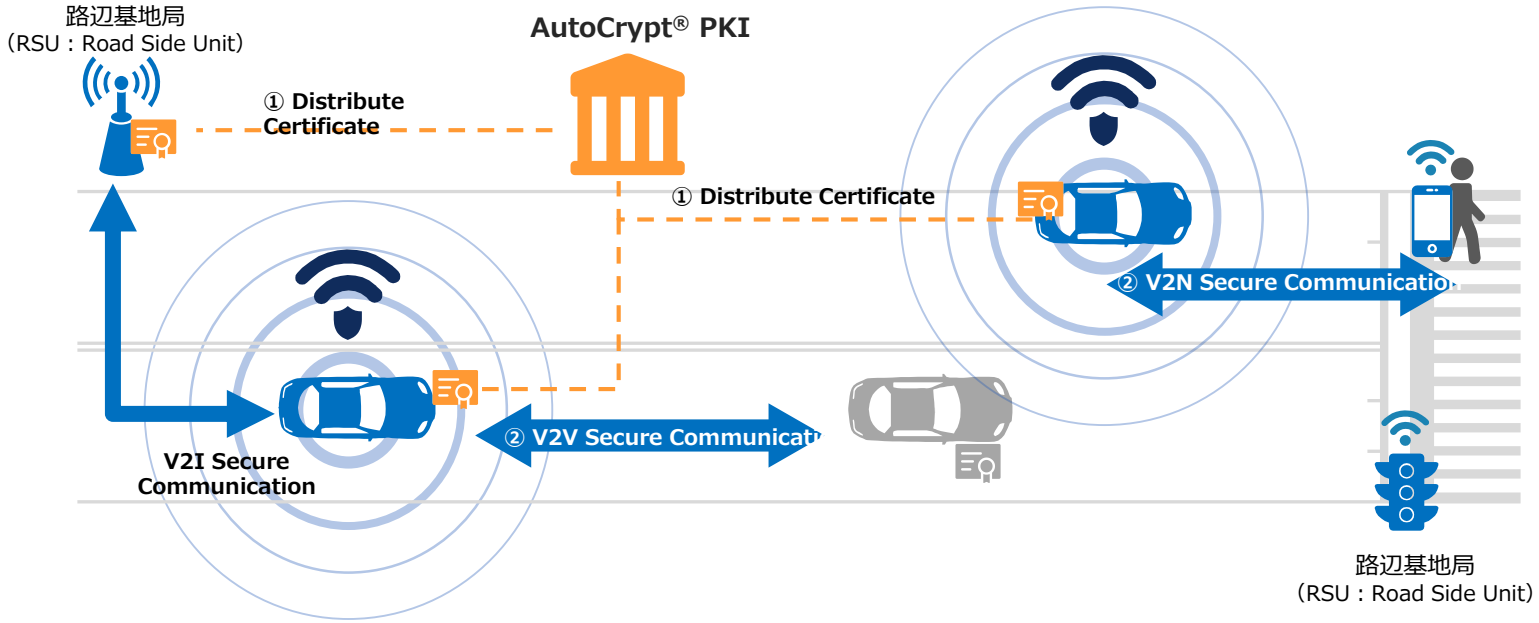
5 鍵管理

6 匿名技術にて
プライバシー保護

AutoCrypt® V2X

自動車間、自動車とインフラ間等自動車関連通信確立時は、AutoCrypt® V2XとAutoCrypt PKIより配布した証明書を採用し、行われます。

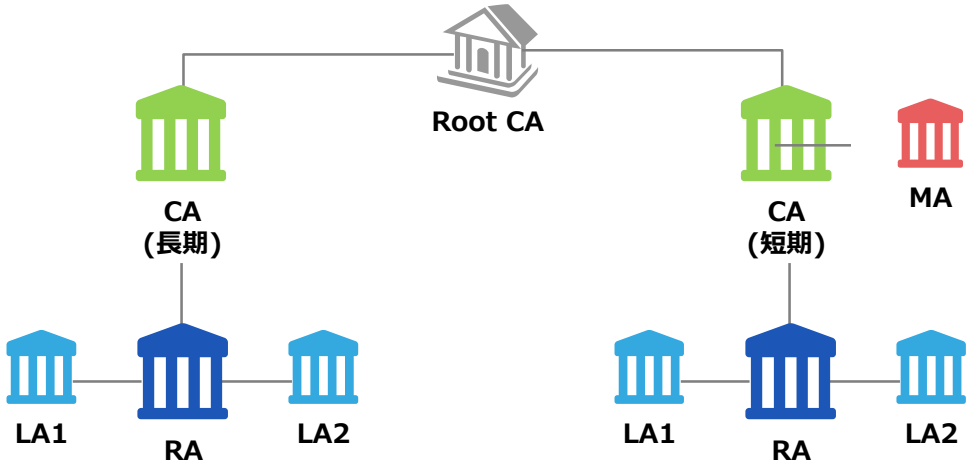
- 自動車間、自動車と路辺基地局(RSU：Road Side Unit)間、道路と信号システム間安全な通信確立のため、暗号化機能を提供
- AutoCrypt® V2Xは、IEEE1609.2* の自動車通信セキュリティ規格を基盤とし、CAMP VSC3*に準拠
- 自社独自開発したソフトウェアのモジュールを搭載し、自動車間、その他オブジェクト間安全な通信確立と認証システムを提供

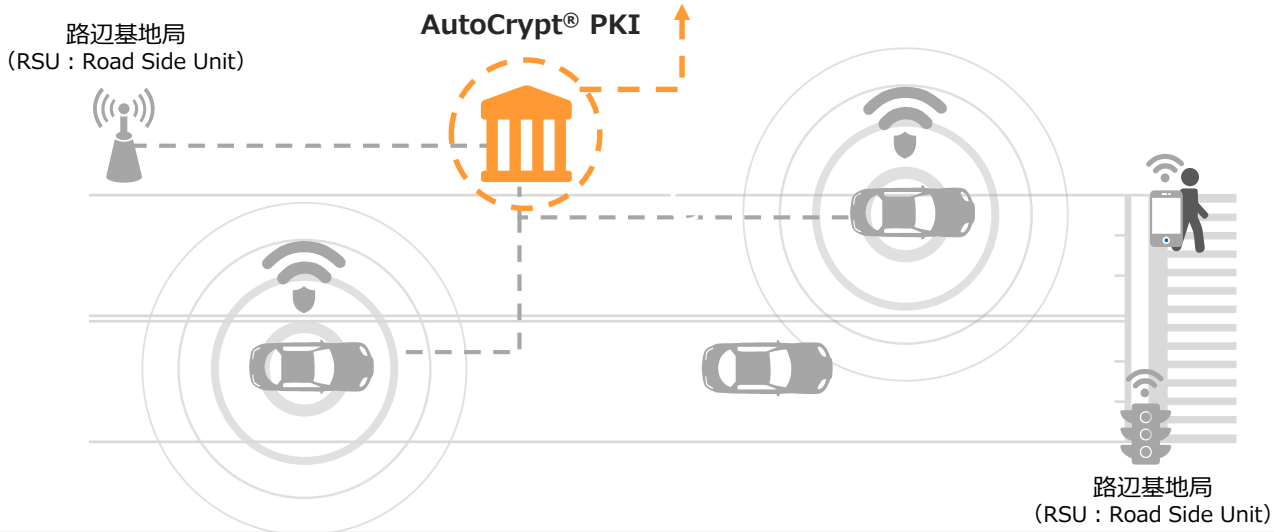


* IEEE1609.2: Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages
* CAMP VSC3: Crash Avoidance Metrics Partnership - Vehicle Safety Communications 3

AutoCrypt® PKI

- **CA : Certificate Authority**
  - ✓ V2X 認証に必要な自動車用証明書を生成
- **MA : Misbehavior Authority**
  - ✓ 証明書の誤用および盗用等を監視
- **RA(Registration Authority)**
  - ✓ V2X 認証に必要なPKI証明書を発行
- **LA(Linkage Authority).**
  - ✓ 匿名証明書(Pseudonym Certificates) 生成のための匿名IDを提供
  - ✓ 自動車運転者のプライバシー(位置情報等)の露出防止

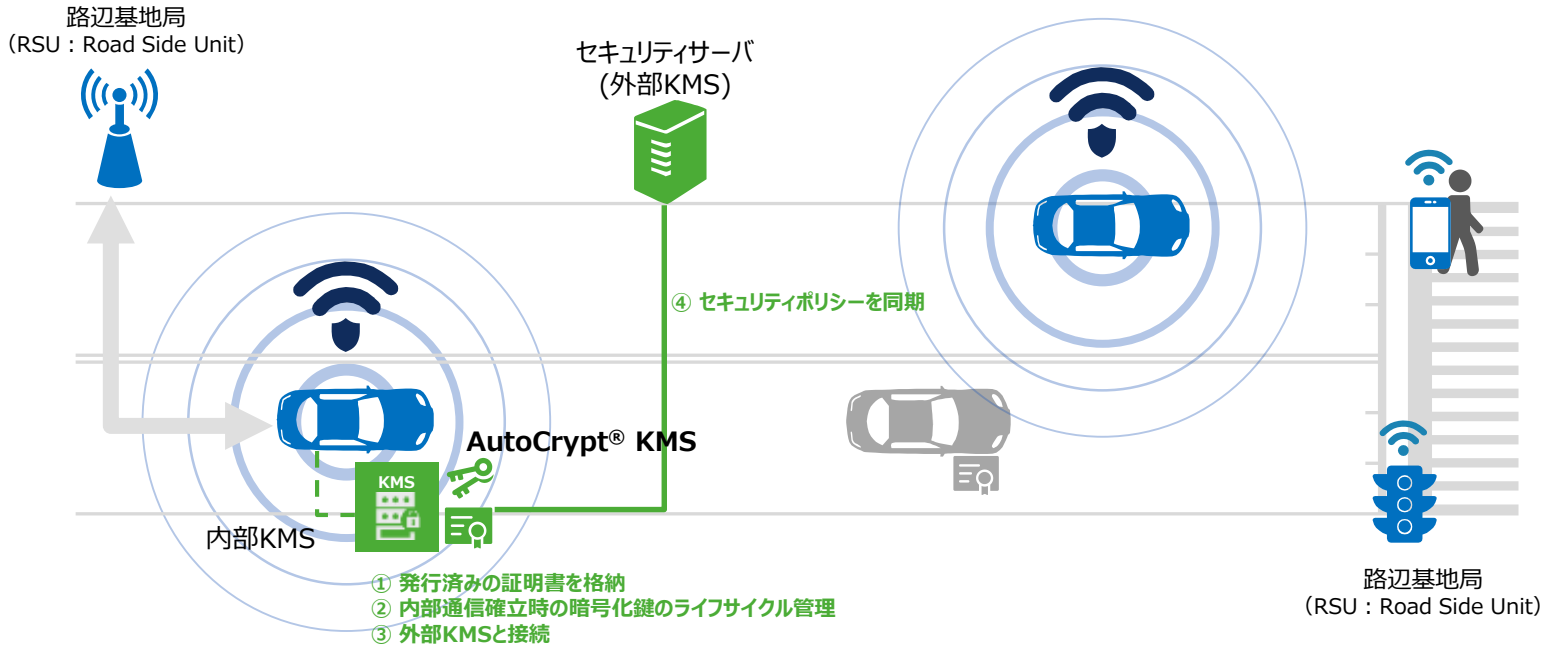




AutoCrypt® KMS（1/3）

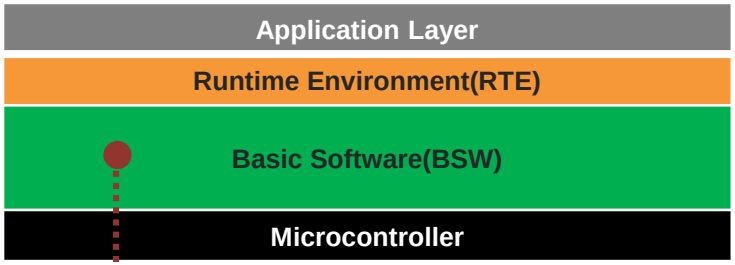
暗号化鍵および証明書のライフサイクルを管理します。

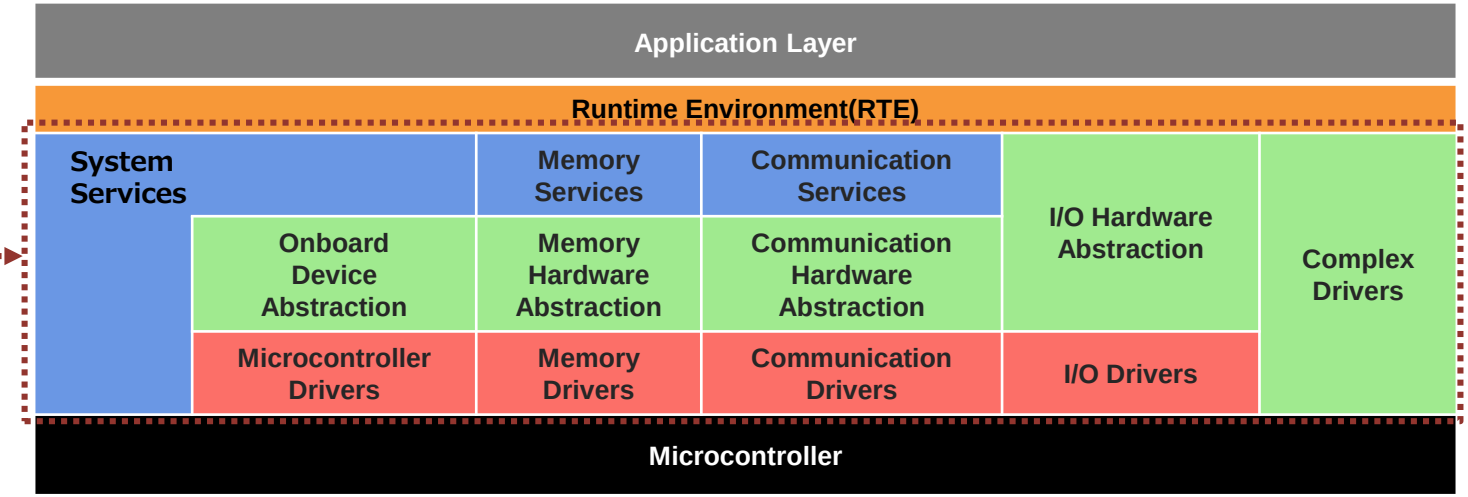
- 自動車内部通信確立時の暗号化鍵のライフサイクルを管理
- 証明書発行機関から発行された証明書を格納および管理
- 自動車外部の暗号化通信確立時の暗号化鍵のライフサイクルを管理
- 外部KMS(セキュリティサーバ)と内部KMSのセキュリティポリシーを同期し、KMSの安定運用を確保



AutoCrypt® KMS（2/3）

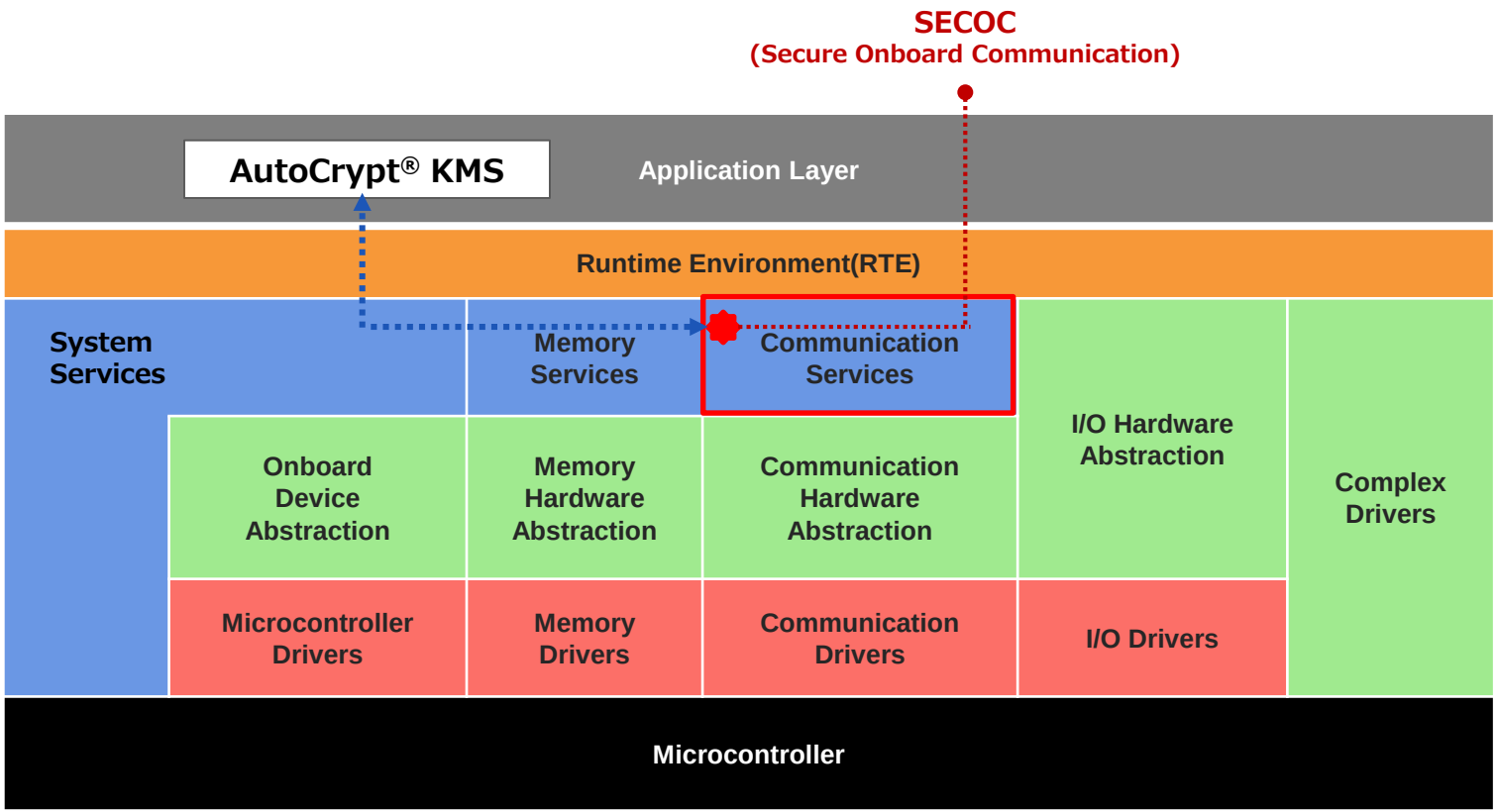
オートザー(AUTOSAR)アーキテクチャー：Basic Software Layers





AutoCrypt® KMS（3/3）

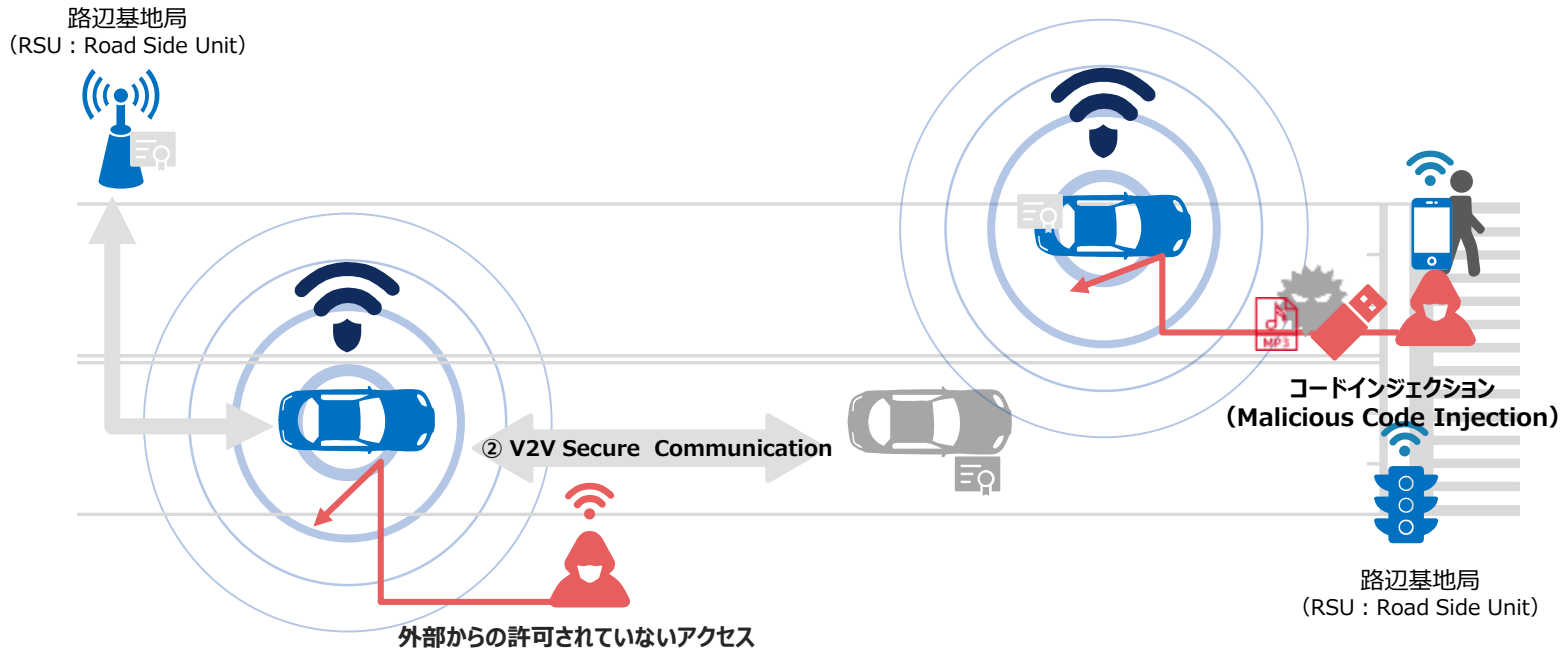
オートザー(AUTOSAR)に対応するAutoCrypt® KMS



AutoCrypt® AFW（1/3）

不正な侵入を検出および遮断するアドバンスド･ファイアウォール（Advanced FireWall）です。

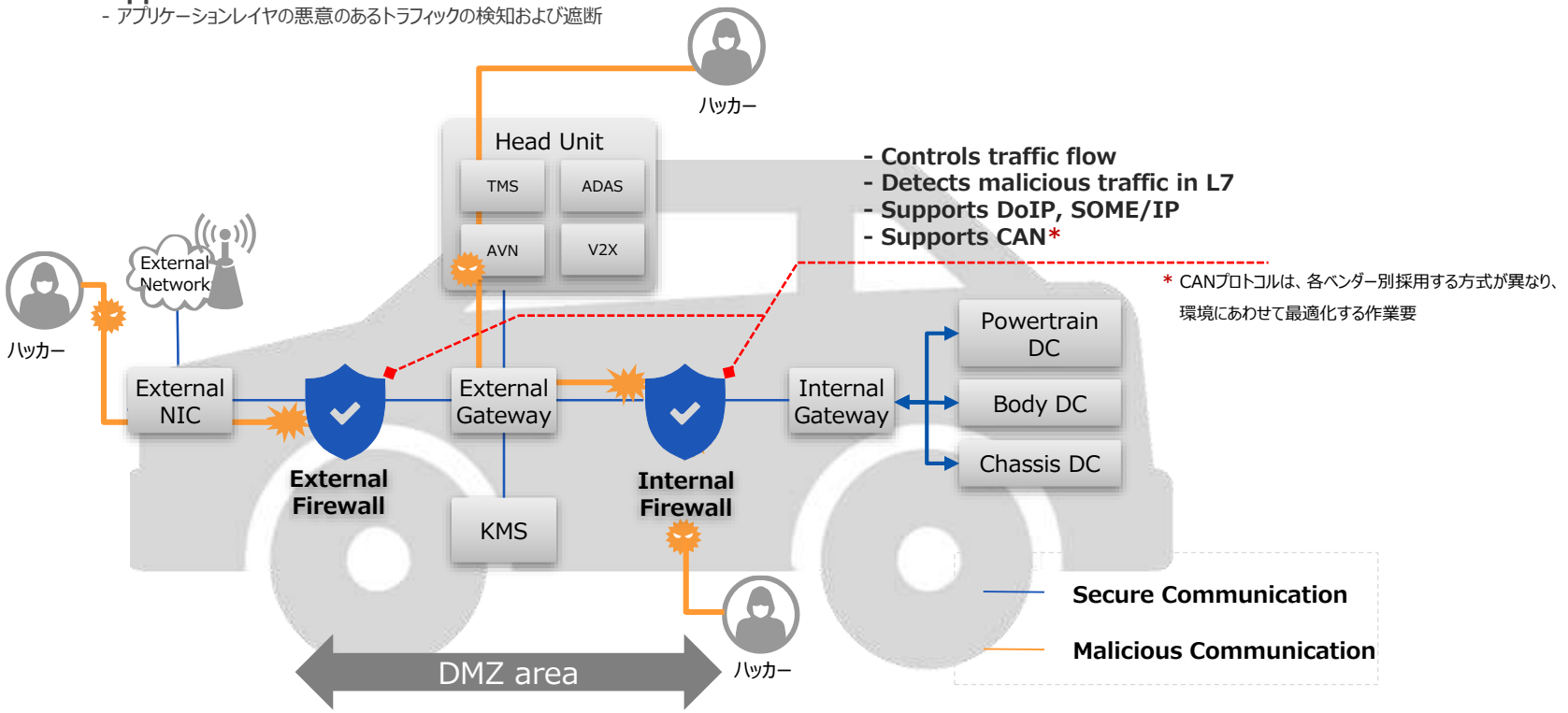
- 自社独自開発した特許技術を基盤とするシグネチャーのアップデートが不要である知能型論理分析エンジンを搭載し、新種･亜種の攻撃に対応可
- テレマティックス(Telematics)、AVN/IVIへ侵入する悪意のあるパケットを検出し、対応
- 自動車内部のプロトコル-CAN, Ethernet(SOME/IP, DoIP)等対応
- ブラックリスト/ホワイトリストを管理



AutoCrypt® AFW（2/3）

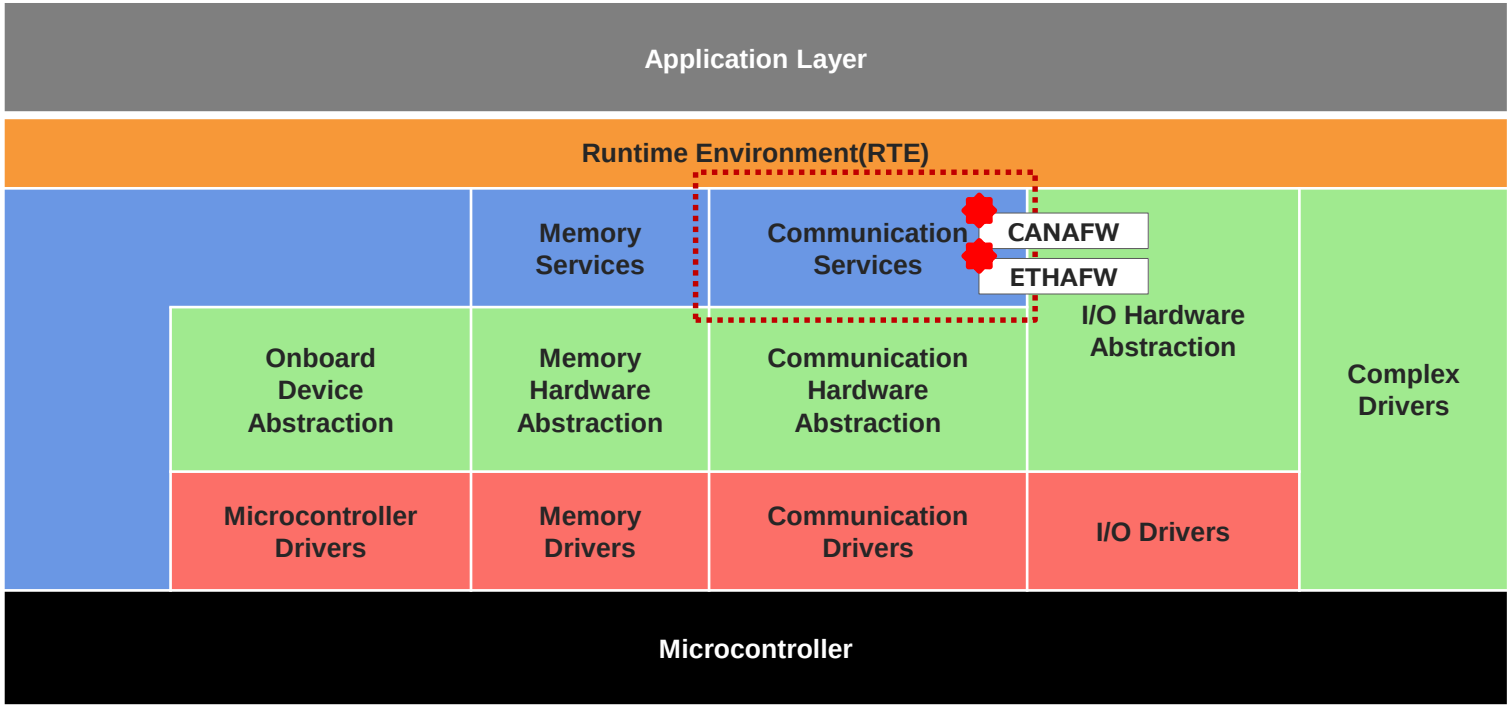
- ネットワークトラフィックの経路を制御
- ポジティブ・セキュリティ・モデル (Positive Security Model)で指定されたプロトコルおよびアプリケーションのみ使用許可し、対象外は遮断

- **Network Firewall**
  - ネットワークトラフィックの制御
  - Positive Security Modelを採用したプロトコルおよびアプリケーション管理
- **Application Firewall**
  - アプリケーションレイヤの悪意のあるトラフィックの検知および遮断
- **IDS/IPS**
  - Deep Packet Inspection
  - Black List/White List管理による異常アクセス防止
  - トラフィックのセッション別管理によるリアルタイム検知



AutoCrypt® AFW（3/3）

オートザー(AUTOSAR)に対応するAutoCrypt® AFW



http://core0.staticworld.net/images/article/2015/03/car_wireless_internet_security_privacy_security_locks-100437820-primary.idge-100572642-primary.idge.jpg

t h a n k **y o u**

Penta SECURITY

KOREA Yeouido, Seoul www.pentasecurity.co.kr (HQ)
U.S.A. Houston, Texas www.pentasecurity.com
JAPAN Shinjuku-Ku, Tokyo www.pentasecurity.co.jp

AUTOCRYPT