Cyber Security for Automotive/Mobility

～Linux搭載の車載機器向けセキュリティからクラウドまで、トータルでセキュリティを考える～

トレンドマイクロ株式会社

2021年2月12日

Agenda

1. 会社紹介
2. 自動車サイバーセキュリティ法規
3. 考え方・アプローチ
4. Trend Microの取組とソリューション
5. まとめ

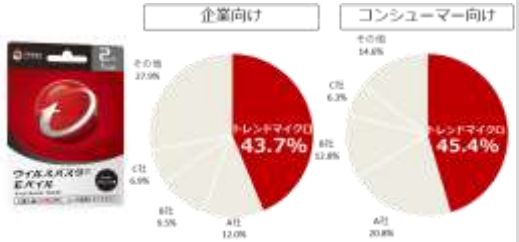
1. 会社紹介

1. 会社紹介
1-1. 会社概要

IT、デジタルの進化に伴って増加するセキュリティ課題・懸念に対し、
セキュリティソリューションを提供することで、安心・安全を届けています。

What We Do

- IT環境のセキュリティにおけるリーダー
- 革新的なセキュリティソリューションを提供
- ビジネス利用・個人利用双方のお客様を保護



How We Do It

世界の脅威解析の知能を集結

- 世界13ヶ所にある脅威解析センターに約1,200名のスタッフと約1,500名のR&Dエンジニアが在籍。
- TREND MICRO SMART Protection Network™
- 世界中の脅威情報を収集、分析・特定し、お客様へリアルタイムでソリューションを提供するクラウド型のセキュリティインフラ。

Who We Are

エバ・チェン
代表取締役社長
兼 CEO

大三川 彰彦
取締役副社長

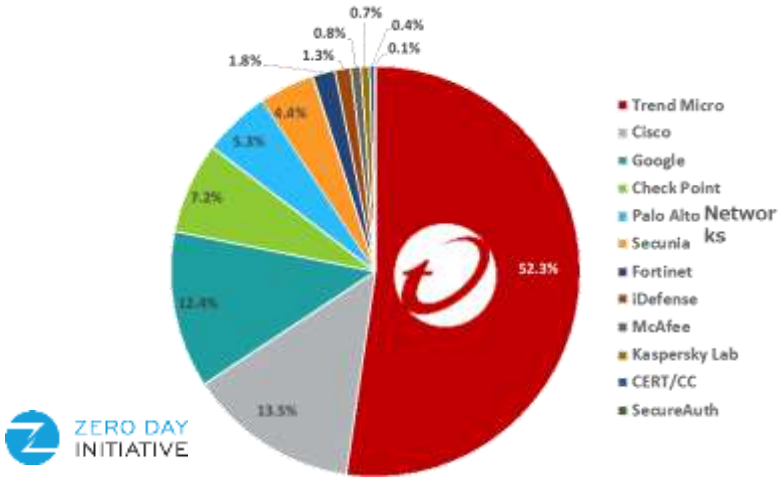
創業	1988年
本社	東京（日経225に選出）
従業員数(全世界)	6,854名※
資本金	188億2,200万円※
売上高	1,651億9,500万円※

※2019年12月31日付

1. 会社紹介
1-2. セキュリティ貢献活動実績

脆弱性発見実績やMITRE ATT&CK評価テストでも高い実績・評価を得ています。

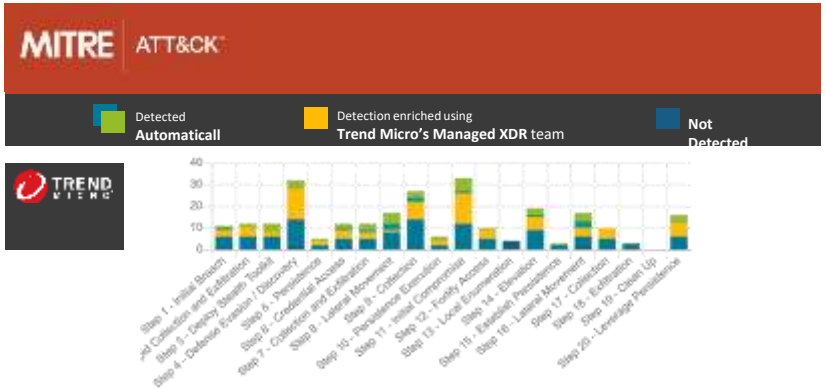
脆弱性情報公開実績



トレンドマイクロが運営する ZERO DAY INITIATIVE（ZDI）は、**2018年に全体の52.3%※となる半数以上の脆弱性を発見した実績**があります。

出典：：IHS Markit, 2018 Public Cybersecurity Vulnerability Market

MITRE ATT&CK評価テスト



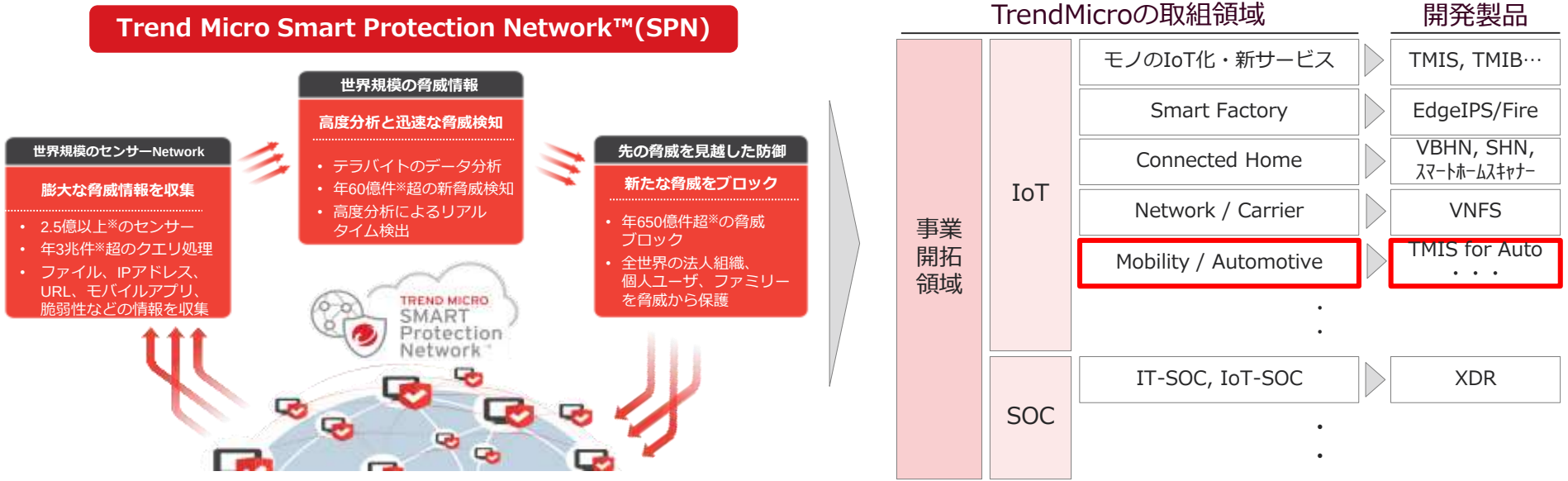
トレンドマイクロのMITRE ATT&CK評価テスト結果
すべての攻撃ステップで検知を記録

MITRE ATT&CK評価テスト※1 APT29の疑似攻撃によるテスト（設定変更なし）において、**検知率91%で1位の結果**。

出典：：https://attackevals.mitre.org/APT29/results/trendmicro/

1. 会社紹介
1-3. コアテクノロジーと新事業分野の開拓

脅威情報ネットワーク『SPN』コアとし、新事業分野の開拓を推進しています。
IoT分野の開拓も進めており、その一つの領域としてMobilityに注力しています。



※2018年 トレンドマイクロ調べ

2. 自動車セキュリティ動向

2. 自動車セキュリティ動向
2-1. 自動車関連セキュリティインシデント例

コネクテッドや電動化等、テクノロジーの進化と共に様々なインシデントが発生。
Data活用、システム化に伴い、更なるインシデントが発生する懸念があります。

研究・解析

Connected, Electric

インターネット接続システムの
脆弱性をつき、走行中の車を乗っ取り

出典：https://wired.jp/2015/07/23/connected-car-bug/

研究・解析

Connected, Electric

ハッキングコンテスト「Pwn2Own」
でModel 3のWebブラウザをハック

出典：https://www.bleepingcomputer.com/news/security/tesla-model-3-hacked-on-the-last-day-of-pwn2own/

攻撃・実害

Connected, Sharing

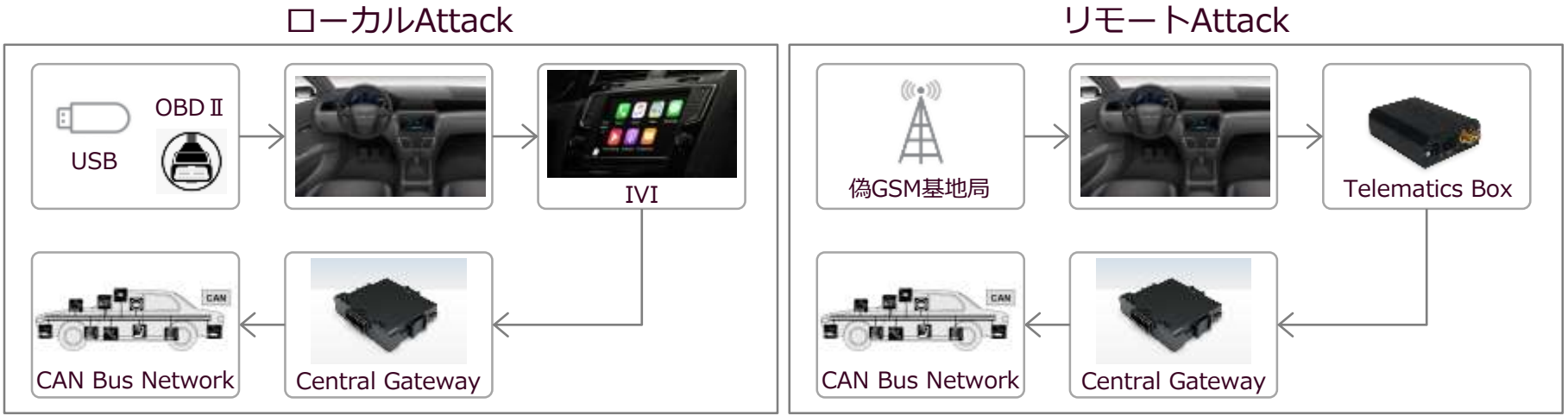
カーシェアアプリのハッキング被害
最大100台の車両が盗難

ダイムラーとBMWのカーシェアサービスがハッキング、最大100台盗難か

出典：https://newspicks.com/news/3833978/

2. 自動車セキュリティ動向
2-2. インシデント例 ～2018年 BMW 研究報告内容～

2018年にある研究でBMWの車両機器について幾つかの脆弱性が報告されました。
また、合わせて、Attack経路例についても報告されました。



- インフォテインメントシステム（IVI）、テレマティクスコントロールユニット(TCU)、セントラルゲートウェイモジュールの3カ所の**脆弱性（14件）**を確認
- 8件はUSBやOBD Ⅱなどの物理的なアクセスを必要とするもので、意図的に細工されない限り影響は受けない
  しかし、残り6件は、BluetoothやGSM等の通信を介して悪用することが可能で、**走行中の車を乗っ取ることも可能**

2. 自動車セキュリティ動向
2-4. 法規制・ガイドラインの動向

グローバルで法規制やガイドラインの改正や新設が進んでいます。
WP29が6/24に内容FIXし、今後、ISO21434も最終版が発行される予定です。

項目	内容	状況
国際標準	• WP29（自動車基準調和世界フォーラム） ➢ サイバーセキュリティに関するRegulationづくり	内容確定済
	• ISO21434（国際標準規格） ➢ 車ライフサイクル全体のサイバーセキュリティに関するプロセスを定義	2021年上期発行
	• UL 4600（Standard for Safety for Evaluation of Autonomous Products）	リリース済
日本の法規制・ガイドライン	• 2019年9月　自動運転車の安全技術ガイドライン • 2019年12月　道路交通法改正／道路運送車両法改正 • 2020年5月　自動運転車使用による罰則、違反点、罰金の制定	リリース済
	• 2020年11月　車載ソフトウェアの無線通信アップデートの許可制度創設	予定

2. 自動車セキュリティ動向
2-5. WP29、ISO21434及び国内法規の今後の予定

国内外でサイバーセキュリティ法規の整備・策定が進められており、
2022年以降に新型車、2024年以降には継続車での対応が必須となる見込み。

出典：Trend Micro調べ

2. 自動車セキュリティ動向
2-6. WP29法規基準と要求事項

WP29では自動運転車の開発～生産～市場投入後におけるサイバーセキュリティの対策と管理・運用を求めています。

7.2.1 認証取得のためCSMS※を整備する　※Cyber Security Management System

7.2.2 CSMSの要件

7.2.2.1 適用対象工程

企画開発 ～ 生産 ～ 市場	全行程

7.2.2.2 整備すべきプロセス

a) 組織全体としてのCSMSプロセス	全行程
b) リスク特定のプロセス	開発
c) リスクの評価/分類/処置のプロセス	
d) リスク管理のプロセス	
e) 車両のCSテストプロセス	
f) リスク評価を最新に保つプロセス	市場
g) 車両に対するサイバー攻撃や脅威・脆弱性を監視・検出し、対応するプロセス	

7.2.2.3

インシデントには迅速に対応	市場

7.2.2.4 整備すべきプロセス

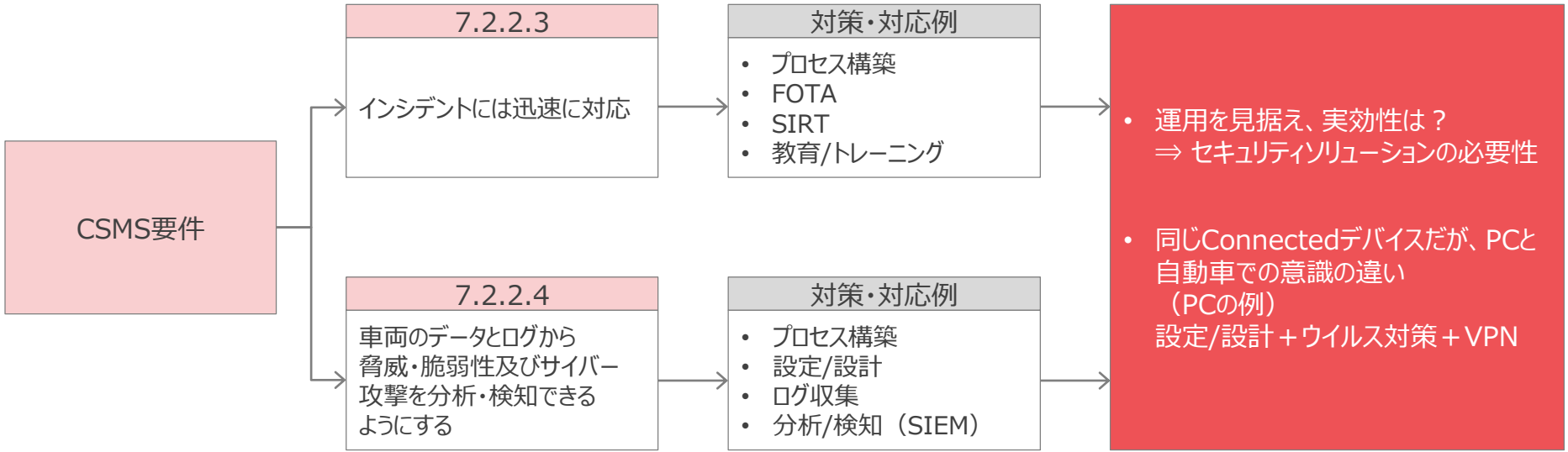
a) 市場でも車両を監視する	市場
b) 車両のデータとログから脅威・脆弱性及びサイバー攻撃を分析・検知できるようにする。 その際、当該車両の所有者/運転手の同意を得、プライバシーを保護すること	

7.2.2.5

サプライチェーンとアフターマーケットサービス全体のCSを担保する	全行程

2. 自動車セキュリティ動向
2-7. 実際の運用を見据えた実効性は？

法規への対応と実際のセキュリティ対応・運用とは別軸で考える必要があるのではないでしょうか？



3. 考え方・アプローチ

3. 考え方・アプローチ
3-1. WP29、ISO21434への対応ポイント

対応すると言っても、何から対応するのか？
⇒ ３つの観点で考えましょう。

サプライチェーン全体でのサイバーセキュリティの確保

プロセスや作業成果物、エビデンスによる裏付、証明

リスク評価とプライオリティ設定

3. 考え方・アプローチ
3-2. 実際の脅威について ー WP29 Annex 5より

Part A. Vulnerability or attack method

脅威に対する脆弱性と攻撃手法

1. High level descriptions of threats and relati
in Table A1.

Table A1
List of vulnerability or attack method related to th

High level and sub-level descriptions of vulnerability/ threat			
4.3.1 Threats regarding back-end servers related to vehicles in the field 車両に繋がるサーバー関連脅威	1	Back-end servers used as a means to attack a vehicle or extract data 自動車やデータへの攻撃にサーバーを利用	1.1 1.2
	2	Services from back-end server being disrupted, affecting the operation of a vehicle	2.1
	3	Vehicle related data held on back-end servers being lost or compromised ("data breach")	3.1 3.2 3.3 3.4 3.5
4.3.2 Threats to	4	Spoofing of messages or data	4.1

Part B. Mitigations to the threats intended fo

車両を対象とした脅威軽減

1. Mitigations for "Vehicle communication channels

Mitigations to the threats which are related to "Ve
listed in Table B1.

Table B1
Mitigation to the threats which are related to "Vehicl

Table A1 reference	*Threats to "Vehicle communication channels"*	*Ref*	
4.1	Spoofing of messages (e.g. 802.11p V2X during platooning, GNSS messages, etc.) by impersonation メッセージのなりすまし（802.11p、V2X、GNSS等）	M10	The inte
4.2	the road)	M11	受 sec stor Sec
5.1	Communication channels permit code injection into vehicle held data/code, for example tampered software binary might be injected into the communication stream	M10 M6	The inte Sys min
5.2	Communication channels permit manipulation of vehicle held data/code	M7	Acc app
5.3	Communication channels permit overwrite of vehicle held data/code		
5.4 21.1	Communication channels permit erasure of vehicle held data/code		
5.5	Communication channels permit introduction of data/code to vehicle systems (write data code)		
6.1	Accepting information from an	M10	The

Part C. Mitigations to the threats outside of vehicles

車両外への脅威軽減

1. Mitigations for "Back-end servers"

Mitigations to the threats which are related to "Back-end servers" are listed in Table C1.

Table C1
Mitigations to the threats which are related to "Back-end servers"

Table A1 reference	*Threats to "Back-end servers"*	*Ref*	*Mitigation*
1.1 & 3.1	Abuse of privileges by staff (insider attack) スタッフの権利悪用（内部による攻撃）	M1	Security Controls are applied to back-end systems to minimise the risk of insider attack バックエンドシステムへのセキュリティの適用
1.2 & 3.3	server (enabled for example by backdoors, unpatched system software vulnerabilities, SQL attacks or other means)	M2	unauthorised access. Example Security Controls can be found in OWASP
1.3 & 3.4	Unauthorised physical access to the server (conducted by for example USB sticks or other media connecting to the server)	M8	Through system design and access control it should not be possible for unauthorised personnel to access personal or system critical data
2.1	Attack on back-end server stops it functioning, for example it prevents it from interacting with vehicles and providing services they rely on	M3	Security Controls are applied to back-end systems. Where back-end servers are critical to the provision of services there are recovery measures in case of system outage. Example Security Controls can be found in OWASP
3.2	Loss of information in the cloud. Sensitive data may be lost due to attacks or accidents when data is stored by third-party cloud service providers	M4	Security Controls are applied to minimise risks associated with cloud computing. Example Security Controls can be found in OWASP and NCSC cloud computing guidance
3.5	Information breach by unintended sharing of data (e.g. admin errors, storing data in servers in garages)	M5	Security Controls are applied to back-end systems to prevent data breaches. Example Security Controls can be found in OWASP

出典：ECE-TRANS-WP29-2020-079-Revised.pdf

3. 考え方・アプローチ
3-3. Connected Carにおける脅威抽出（例）

前述のWP29 Annex5の内容も踏まえ、Connected Carにおける脅威を29種抽出

Attack Vectors		
Spoofing V2X messages being broadcast to the ecosystem	Remotely hijacking vehicles via compromised CAN bus	Conducting social engineering attacks such as creating fake RDS-TMC messages, phishing, and map poisoning
Passively sniffing V2X messages being broadcast to the ecosystem	Dumping firmware to recover credentials and configurations	Launching distributed denial-of-service (DDoS) attacks using a compromised ITS infrastructure
Sending incorrect or improper commands to back-end ITSs	Installing malicious third-party apps in a connected car's infotainment system	Launching DDoS attacks on an ITS infrastructure so that it fails to respond to requests
Sending MitM communications and false data to back-end ITSs	Deleting local files in a compromised connected car's file system	Credential brute-forcing and abusing weak authentication methods
Sniffing network traffic between a connected car and back-end ITSs	Installing a malicious app on a connected mobile phone	Injecting malicious scripts via malvertising
Remotely transmitting and installing malicious firmware and/or apps	Electronically jamming a connected car's safety systems, such as radar and lidar	Performing traditional attacks such as SQL (Structured Query Language) injection,59 cross-site scripting (XSS),60 session hijacking,61 and DNS (Domain Name System) spoofing62
Electronically jamming wireless transmissions to disrupt operations	Attacking the camera system's image processing with specially crafted visuals	Pivoting a connected car as a trusted entry point to the V2X network
Performing an MitM attack with wireless transmission to intercept and modify car data	Installing malware or spyware in a connected car	Compromising a third-party software supply chain to push malicious updates
Exploiting vulnerabilities in software, hardware, operating systems, and protocols	Identifying and abusing device misconfigurations	Scanning the V2X network from a connected car to discover topology and nodes
Using RF modules to access the head unit via complex exploit chains	Discovering and abusing vulnerable remote systems using Shodan, a search engine for internet connected Devices58	

システムに送信されるなりすましメッセージ

CAN経由での不正アクセスと車両の乗っ取り

偽RDS-TMCメッセージ、フィッシング、マップポイズニング等のソーシャルエンジニアリング攻撃

システムへ送信されるV2Xメッセージの傍受

不正または不適切なコマンドをバックエンドITSに送信

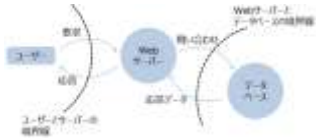
偽のデータをバックエンドITSに送信

3. 考え方・アプローチ
3-4. 脅威モデリング

脅威の抽出、モデリングは重要であり、SOC（Security Operation Center）での分析、運用時の優先度/緊急度の判断等に有効です。

DFD（Data Flow Diagram）

- 情報システムにおけるデータの流れを図式化
- システム境界で起こりえる問題抽出、対応箇所の検討が可能



STRIDE

- 脅威を6つの特性より導出
- Spoofing(なりすまし), Tampering(改ざん), Repudiation(否認), Information Disclosure, (情報漏えい), Denial of Service(サービス妨害), Elevation of Privilege(権限昇格)

Attack Tree

- 脅威が発生する原因を列挙する際に利用する方法
- 脅威を頂点とした木構造で表現され、各ノードに脅威の発生につながる原因を記載
- 攻撃の手段と手順を網羅的に整理することができる

DREAD

リスク高：12～15
リスク中：8～11
リスク低：5～7

3. 考え方・アプローチ
3-5. DREADによる採点

前述の抽出した脅威をDREADで採点。このように採点、定量表現することで、客観的な基準で評価することが可能となります。

Attack vector	D	R	E	A	D	Rating
Remotely transmitting and installing malicious firmware and/or apps	3	1	1	1	1	Low
Using RF modules to access the head unit via complex exploit chains	3	1	1	1	1	Low
[illegible] compromised CAN bus	3	1	1	1	1	Low
Deleting local files in a compromised connected car's file system	1	1	1	1	1	Low
Installing malware or spyware in a connected car	2	2	1	1	1	Low
Spoofing V2X messages being broadcast to the ecosystem	2	2	2	2	2	Medium
Passively sniffing V2X messages being broadcast to the ecosystem	1	3	2	1	3	Medium
Sending incorrect or improper commands to back-end ITSs	3	1	2	2	2	Medium
Sending MitM communications and false data to back-end ITSs	3	1	2	2	2	Medium
Sniffing network traffic between a connected car and back-end ITSs	1	3	2	1	3	Medium
Performing an MitM attack with wireless transmission to intercept and [illegible]	3	1	2	1	2	Med
Dumping firmware to recover credentials and configurations	2	2	2	1	2	Med
Installing malicious third-party apps in a connected car's infotainment system	1	2	2	1	2	Med
Installing a malicious app on a connected mobile phone	2	3	3	1	2	Med
Exploiting vulnerabilities in software, hardware, operating systems, and protocols	3	1	1	2	3	Med
Attacking the camera system's image processing with specially crafted visuals	2	2	1	1	3	Med
Identifying and abusing device misconfigurations	3	2	2	2	2	Med
Conducting social engineering attacks such as creating fake RDS-TMC messages, phishing, and map poisoning	1	2	2	1	2	Med
Credential brute-forcing and abusing weak authentication methods	2	3	2	1	3	Med
Injecting malicious scripts via malvertising	1	2	3	2	3	Med
Performing traditional attacks such as SQL (Structured Query Language) injection, cross-site scripting (XSS), session hijacking, and DNS (Domain Name System) spoofing	2	1	2	1	2	Medium	This primarily targets the head unit or middleware that runs in the car.
Pivoting a connected car as a trusted entry point to the V2X network	1	2	2	1	2	Medium	The connected car is a trusted endpoint that could be abused to get into the ITS infrastructure.
Compromising a third-party software supply chain to push malicious updates	2	1	2	2	2	Medium	This targets third-party apps installed in the head unit or are running on top of middleware.
Scanning the V2X network from a connected car to discover topology and nodes	1	3	3	1	3	Medium	This is an extension of passive scanning. The goal here is to discover ITS infrastructure topology.
Electronically jamming a connected car's safety systems, such as radar and lidar	3	3	3	1	3	High	Lidar is a detection system based on the principle of radar, but uses light from a laser.
Electronically jamming wireless transmissions to disrupt operations	3	3	3	1	3	High	2G, 3G, LTE, 4G, 5G, Wi-Fi (802.11p), RDS-TMC, or cellular-satellite connectivity is jammed.
Discovering and abusing vulnerable remote systems using Shodan, a search engine for internet-connected [illegible]	3	3	3	2	3	High	This technique could be used to find exposed ITS infrastructures that could then be compromised.
[illegible] (DDoS) attacks using a compromised ITS infrastructure	2	2	2	3	3	High	The goal is to overwhelm the connected car with excess data from the ITS infrastructure.
Launching DDoS attacks on an ITS infrastructure so that it fails to respond to requests	3	3	3	3	3	High	The goal is to knock the ITS infrastructure offline so that the connected car cannot send or receive messages.

マルウェアや悪意あるアプリを遠隔から送信、インストール

REモジュールを介したヘッドユニットへのアクセス

システムに送信されるなりすましメッセージ

システムへ送信されるV2Xメッセージの傍受

無線通信を利用し、中間者攻撃を実行データを傍受して

レーダーやLidar等の安全システムの妨害

無線通信妨害による操作の断絶・中断

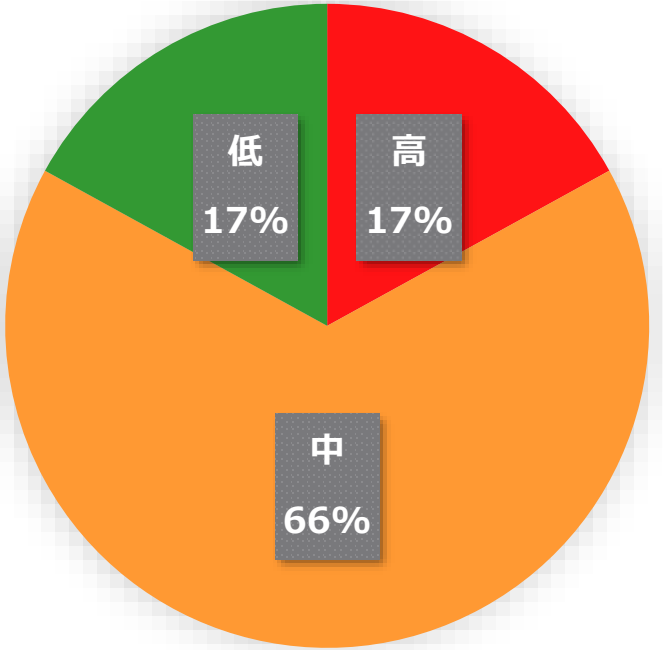
Shodanを利用しInternet接続デバイスを検索

脆弱なリモートシステムの発見

出典：当社White Paperより引用

3. 考え方・アプローチ
3-6. DREADによる採点（結果まとめ）

リスク中以下が全体の80%以上を占めている状況。ただし、DREADは現在を踏まえた採点となっており、技術の進化と共に見直す必要がある。



リスク高	• 内部動作について限られた理解のみ必要。電波妨害など、熟練度の低い攻撃者でも実施できる可能性 • DDoS攻撃、Shodan等のネットワークスキャンサービスを使用した公開サービス／サーバーの発見が含まれる。公開されたITSインフラストラクチャに対するDDoS攻撃は比較的容易
リスク中	• 専門的な技術と知識が必要であり、簡単ではない ＜例＞ ✓ 悪意のあるファームウェアを無線でインストールする ✓ 車両制御のリモートハイジャック ✓ 不正または不適切なコマンドをITSバックエンドに送信する
リスク低	• 高度な技術スキルとコネクテッドカーに関する深い知識が必要 • 攻撃は不可能ではないが、大規模に実行することは困難 一部にのみ影響 • マルウェアもリスク低に含まれている

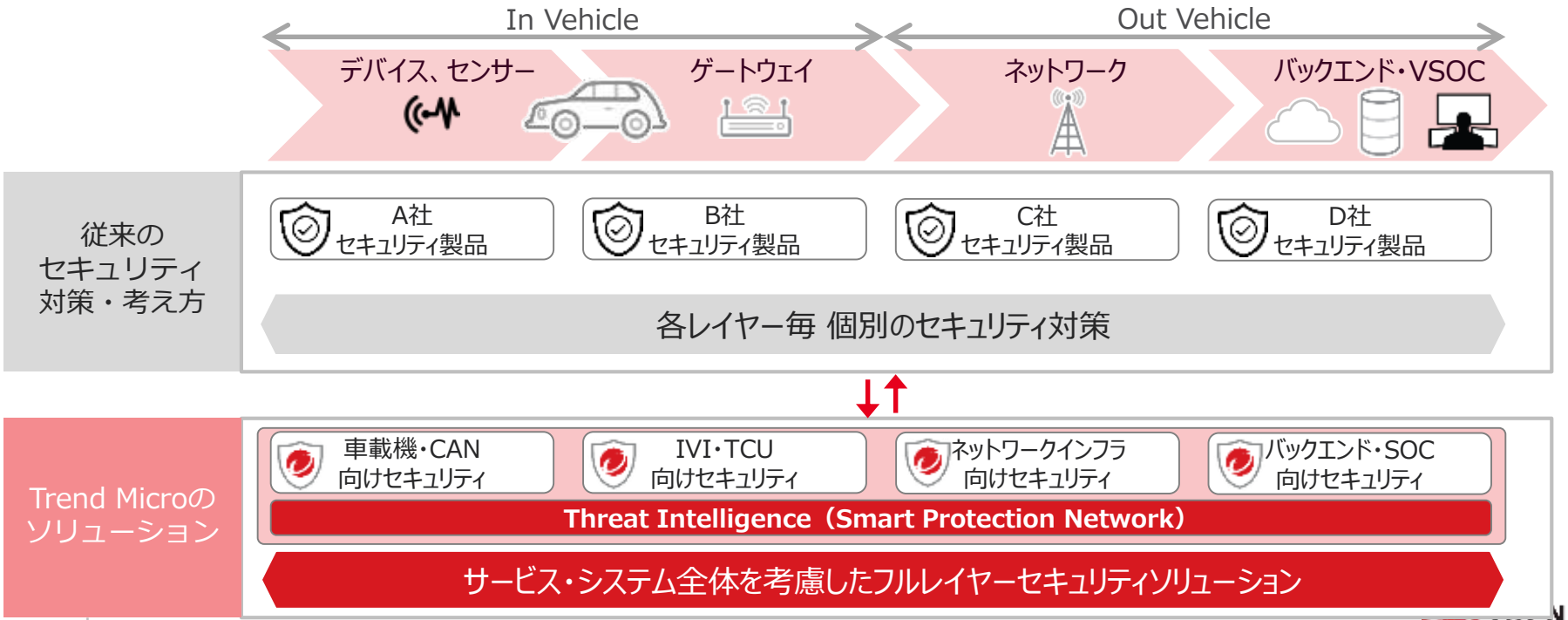
出典：当社White Paperより引用

3. 考え方・アプローチ
3-7. セキュリティ対策例

セキュリティ検討時に個々のレイヤー、個々の製品・技術に注視してしまう傾向があります。セキュリティ対策手法は1つではありません。

3. 考え方・アプローチ
3-8. Trend Microのソリューションコンセプト

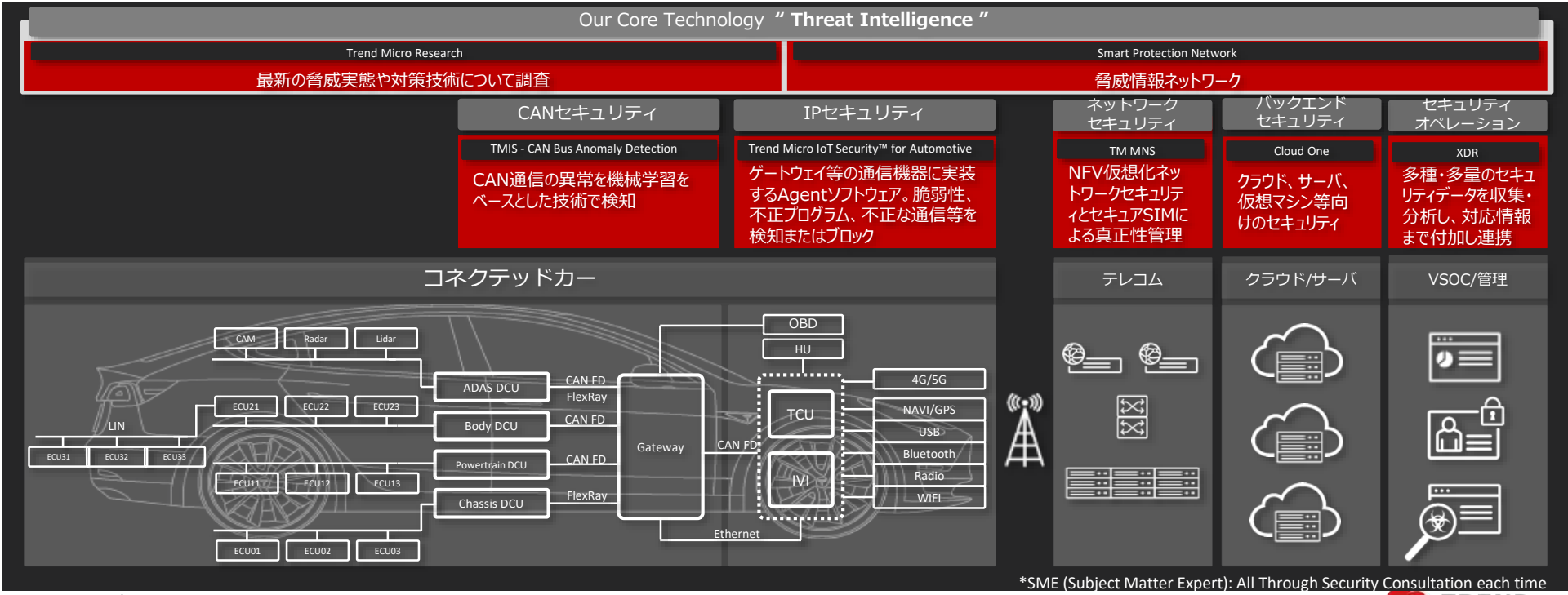
機能レイヤー毎にバラバラのセキュリティ対策ではなく、サービス全体を考慮したセキュリティをご提供します。



4. Trend Microの取組とソリューション

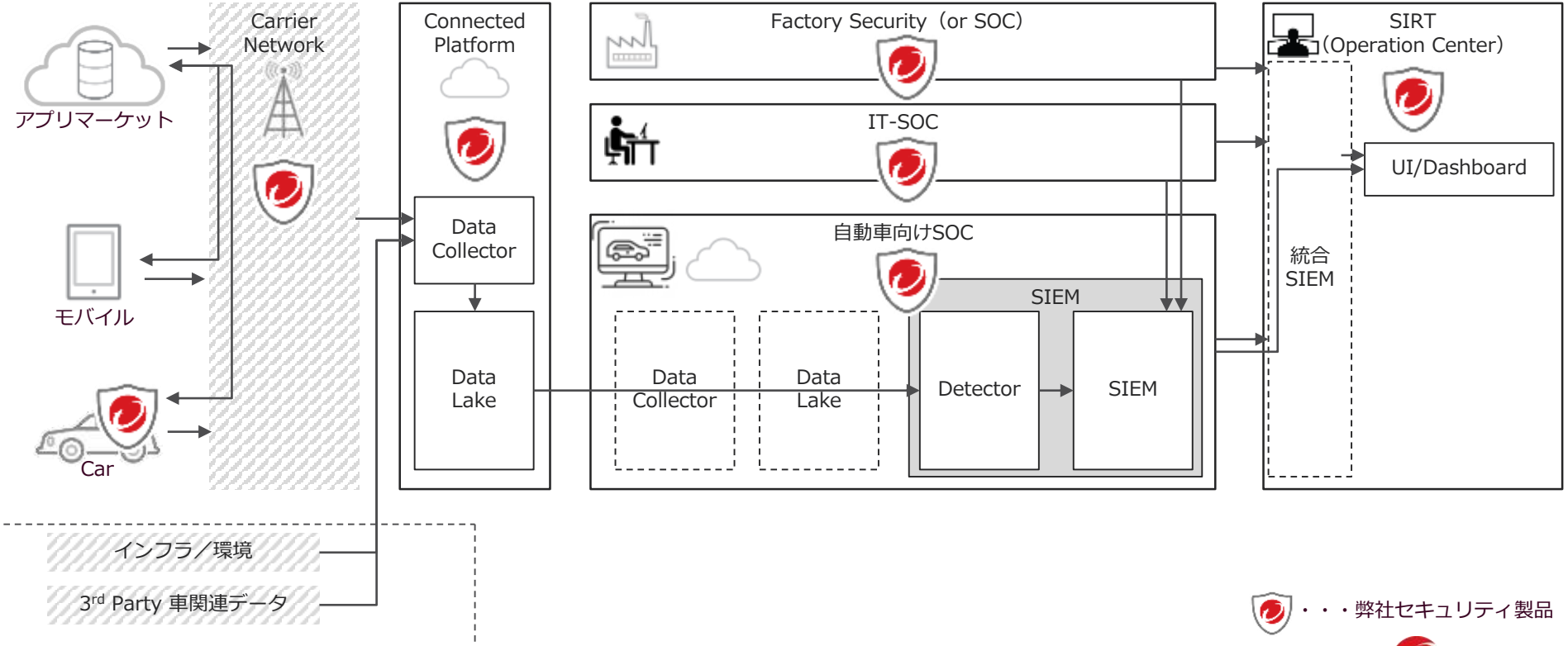
4. Trend Microの取組とソリューション
4-1. Automotive/Mobility Securityソリューションマップ

IT系Securityを軸に、In Vehicleのエッジから、ネットワーク、バックエンド、VSOCまでフルレイヤーのセキュリティソリューションを提供しています。

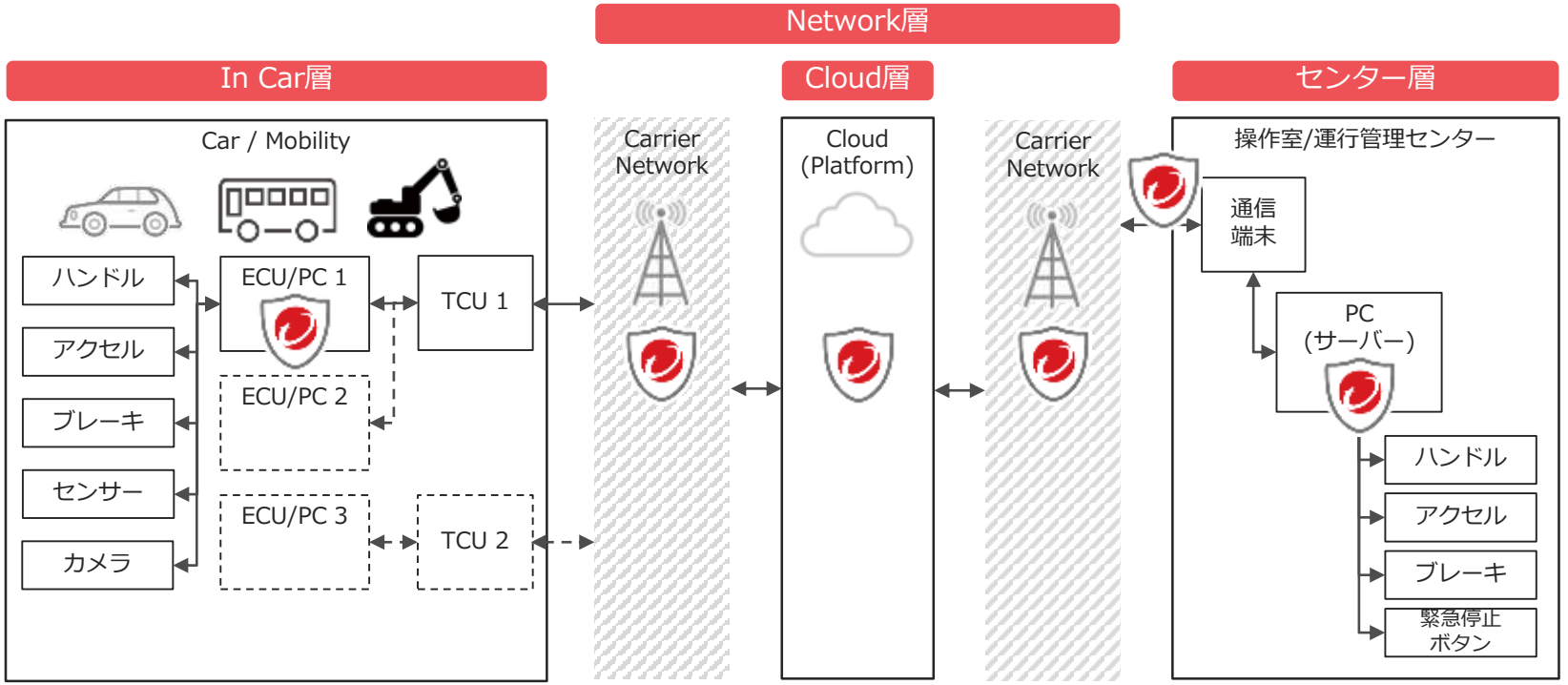


*SME (Subject Matter Expert): All Through Security Consultation each time

4. Trend Microの取組とソリューション
4-2. 取組例：Vehicle SOC（Security Operation Center）



4. Trend Microの取組とソリューション
4-3. 取組例：自動運転向けセキュリティ

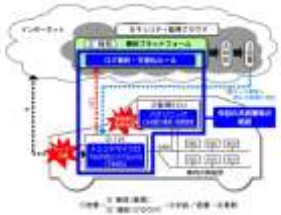


・・・弊社セキュリティ製品

4. Trend Microの取組とソリューション
4-4. 取組例：活動全体像

新製品・機能づくり/コラボレーション

Automotive向けソリューション



Panasonic社との協業

業界団体・業界イベント活動

自動運転関連団体での活動

業界イベントでの展示・講演

リサーチ・研究

自動車関連White Paper

Car Hacking Demo

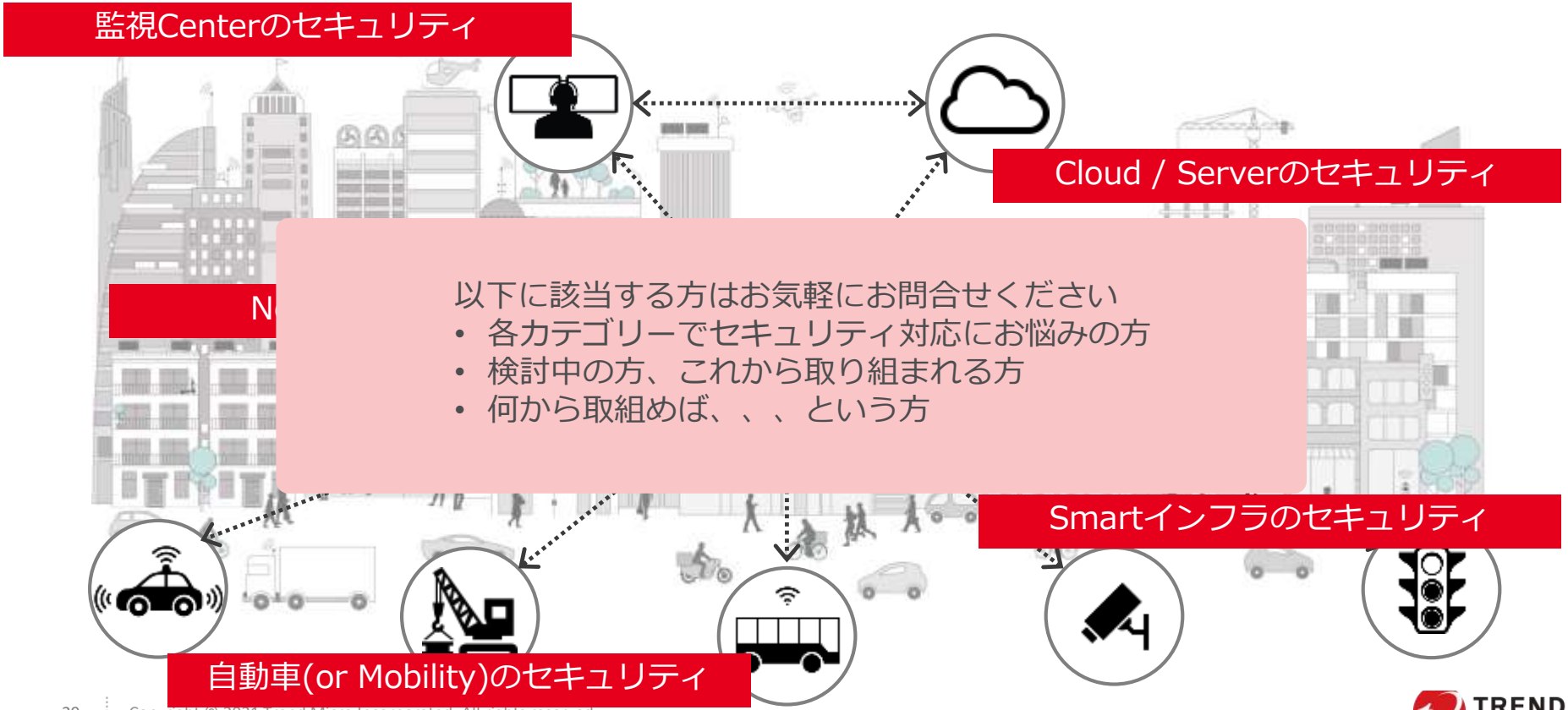
教育・トレーニング

Cybersecurity Center of Excellence

インシデントレスポンス
トレーニングプログラム

5. まとめ

5. まとめ
5-1. コラボレーションイメージ



出典：https://www.am.pictet/de/germany/global-articles/2019/expertise/thematic-equities/life-in-a-smart-city

5. まとめ
5-2. 問合せ先情報

- 担当者情報
  - 所属

    トレンドマイクロ株式会社

    IoT事業推進本部　ネットワークセキュリティ推進部
  - 担当者名

    小田　章展（Oda Akinobu）
  - ご連絡先

    TEL：03-5334-3635（会社）　／ 070-4504-5841（Mobile）

    e-Mail：akinobu_oda@trendmicro.com

Thank you

TREND MICRO