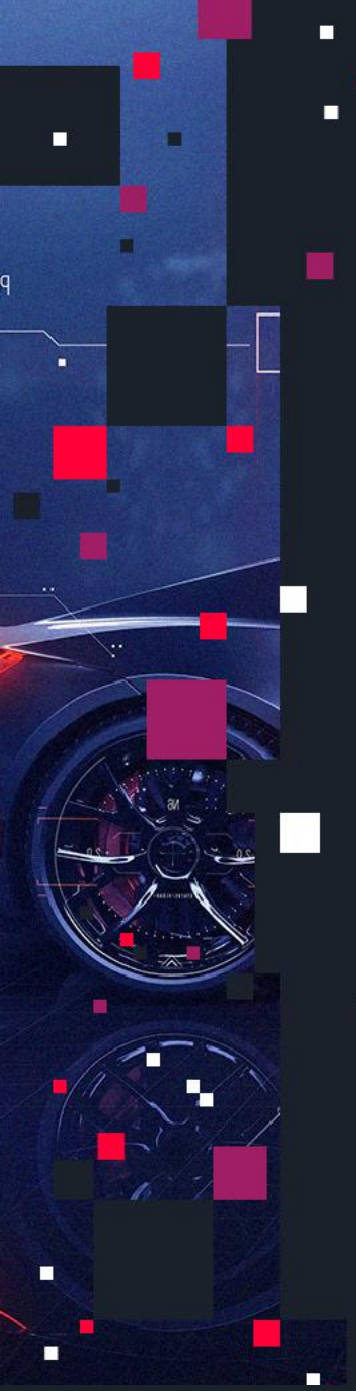
Intrusion Detection Protection Systems: Today and Future

VicOne Corporation
Seiki Hara

May 22, 2025

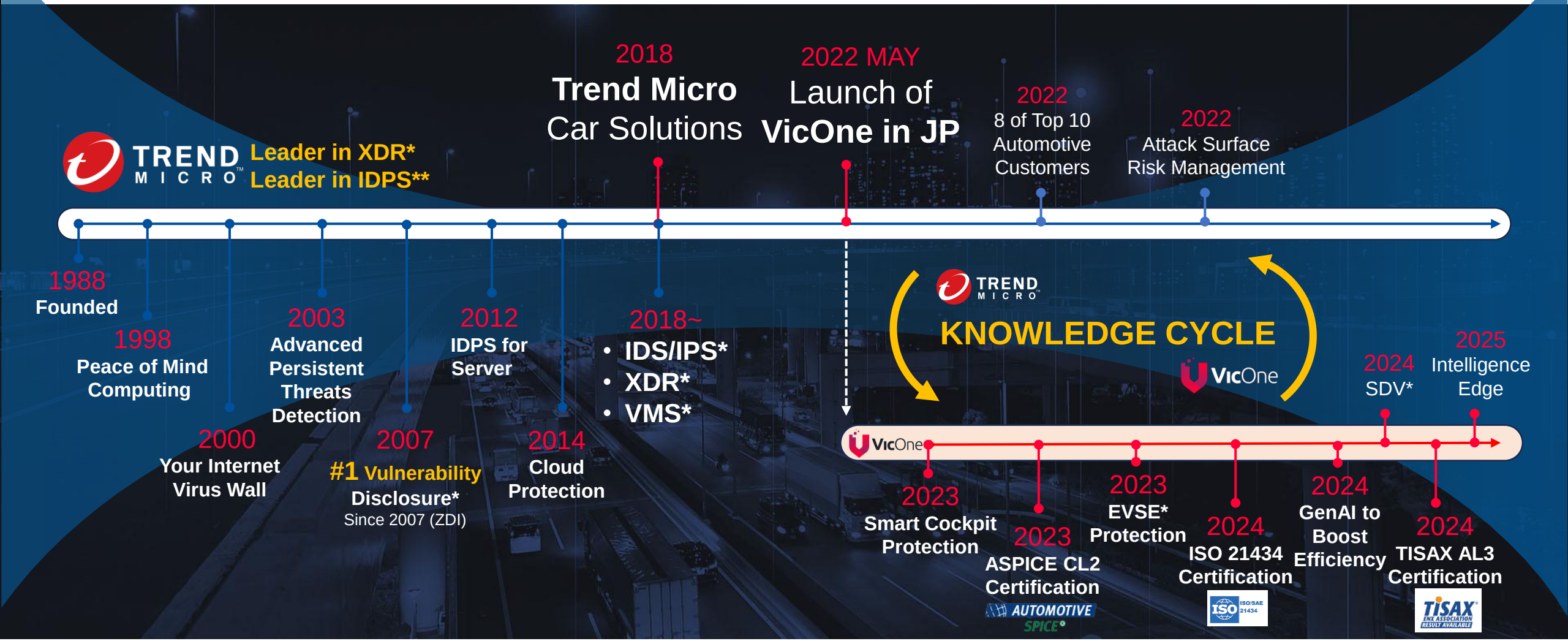
VicOne
Driving Automotive Cybersecurity Forward



About VicOne

About VicOne (1 of 2)

From Trend to VicOne: Always Anticipating, Adapting



1. *Forrester Wave, Extended Detection and Response (XDR), Q4, 2021*
2. *Gartner, Enterprise Network Equipment by Market Segment, Worldwide, 2021.*
3. *Quantifying the Public Vulnerability Market, Omdia, June 2024*

- IDS/IPS = Intrusion Detection and Prevention System
- XDR = Extended detection and response
- VMS = Vulnerability management system
- EVSE = Electric Vehicle Supply Equipment (charging station)
- SDV = Software-defined vehicle

About VicOne (2 of 2)

VicOne: A Global Network, With a Local Footprint

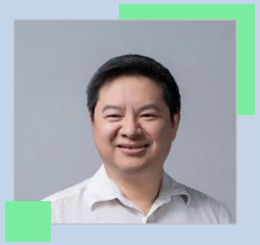
OUR MISSION

Driving Automotive Cybersecurity Forward

Future-ready vehicle protection reinforced with proven automotive threat intelligence

VicOne's Executive Leadership

Max Cheng
Chief Executive Officer



Ziv Chang
VP of Automotive Threat Research Lab

Pender Chang
VP of Research and Development

William Dalton
VP and Managing Director for Europe & US

Baker Lu
Managing Director for AMEA

(HQ & R&D)

(R&D)

Akinobu Oda
VP of Japan

自動車サイバーセキュリティの業界リーディング活動

産業界への貢献と共に、活動で得られた知見を製品技術に活かしています

Pwn2Own Automotive（2025年1月実施）


17 ビジネス 11版

テスラ、ハッカーと連携

バグ発見で賞金総額5億円

自動運転ソフト 安全確保

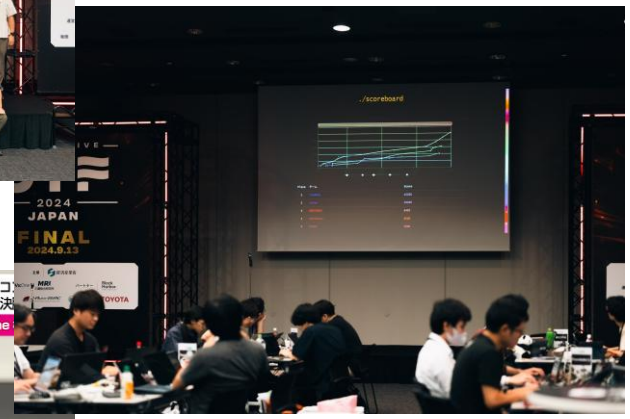
ハンガリーのチームは車載インフォテインメントをハッキング

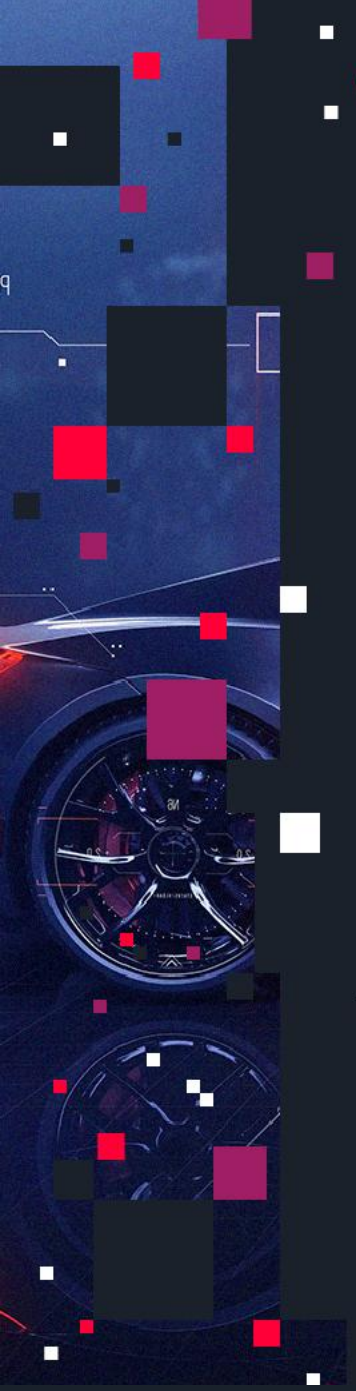
Business Daily

写真1. トレンドマイクロの脅威研究部門バイスプレジデント Brian Gorenc（左）と、VicOneのCEO Max Cheng。Pwn2Own Automotive 2025の開会式にて

写真2. ハードコードされた暗号化キーを使用して、Sina Kheirkhah氏はUbiquiti Connect EV Station充電器を再び「リックロール」しました。

Automotive CTF（2024年7～10月実施）





From VicOne 2025 Automotive Cybersecurity Report

SDV
が直面する重要な サイバーセキュリティ課題

車両がよりスマートに、よりコネクテッドになる時代において、SDVは進化し続ける複雑なサイバーセキュリティ課題に直面しています。過去10 年間の脆弱性データは、安全な自動車の未来のために取り組むべき最も重要な領域と脅威を浮き彫りにしています。

83% 最も脆弱な領域 **15%**

オンボードシステム

ECU(電子制御ユニット)からインフォテインメントシステム、ADAS(先進運転支援システム)に至るまで、オンボードシステムは最も大きく、最も露出している領域です。

クラウドインフラ

データ処理と接続性のためにクラウドベースのサービスへの依存度が高まるにつれて、この領域の脆弱性が増加し、車両が大規模な攻撃にさらされる可能性が高まっています。

主要なセキュリティ懸念事項*

1,564件 サプライチェーンの脆弱性

サプライヤーやサードパーティが車両エコシステムに深く組み込まれているため、この複雑なネットワークのすべてのリンクにわたってセキュリティを確保することは、非常に困難な課題です。

308件 サードパーティ連携

車両が外部サービスへの依存度を高めるにつれて、サードパーティ技術の統合により攻撃対象領域が拡大し、予期せぬリスクをもたらしています。

295件 車両ハイジャック

SDVソフトウェアを標的とするエクスプロイト脆弱性攻撃は、攻撃者に重要な車両システムの遠隔制御を可能にし、安全性とセキュリティの両方を危険にさらす可能性があります。

*2014年から2024年に公開された **SDV関連の脆弱性合計2,271件**に基づく

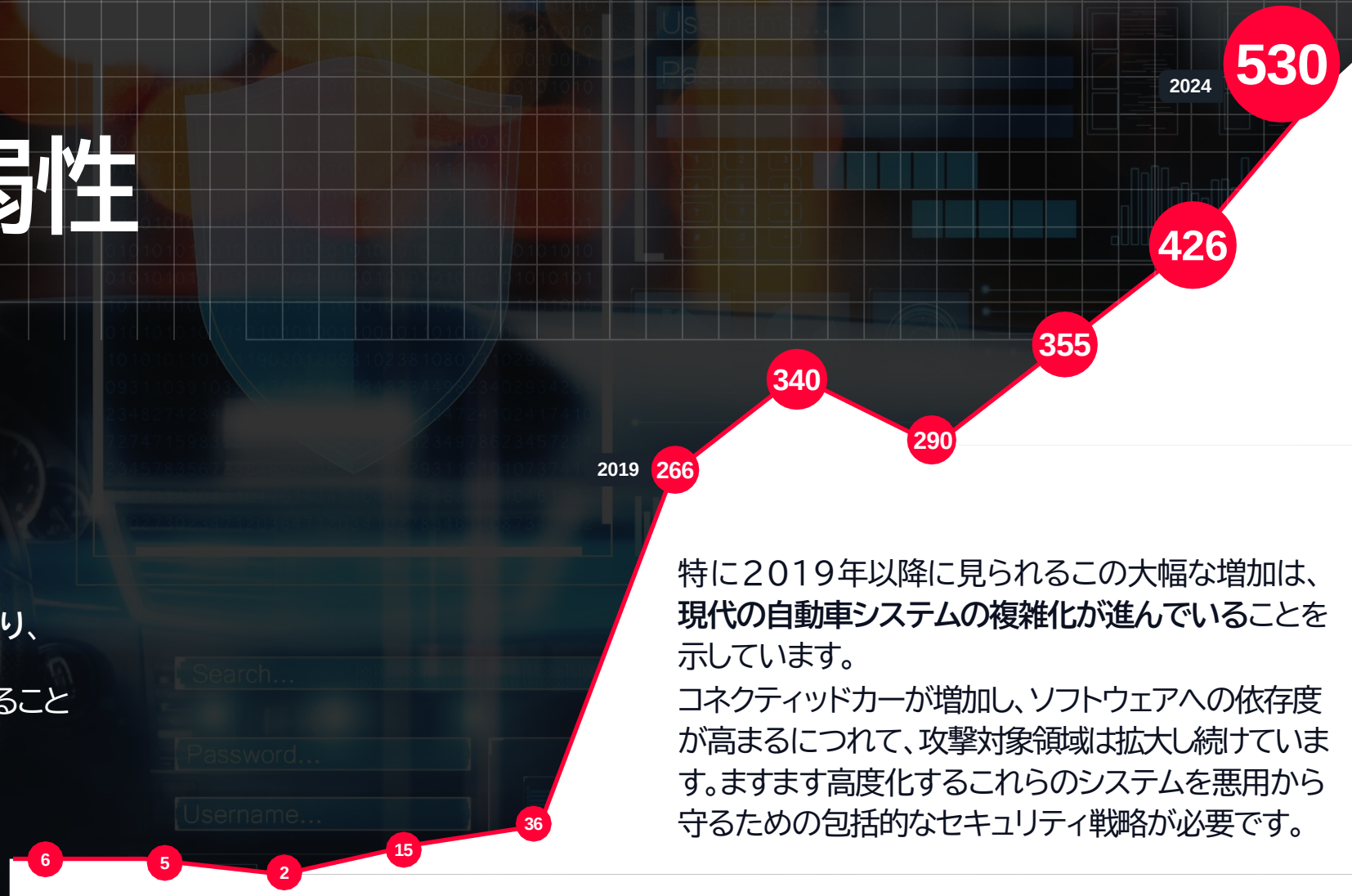
増加傾向にある

自動車の脆弱性

2024年には、

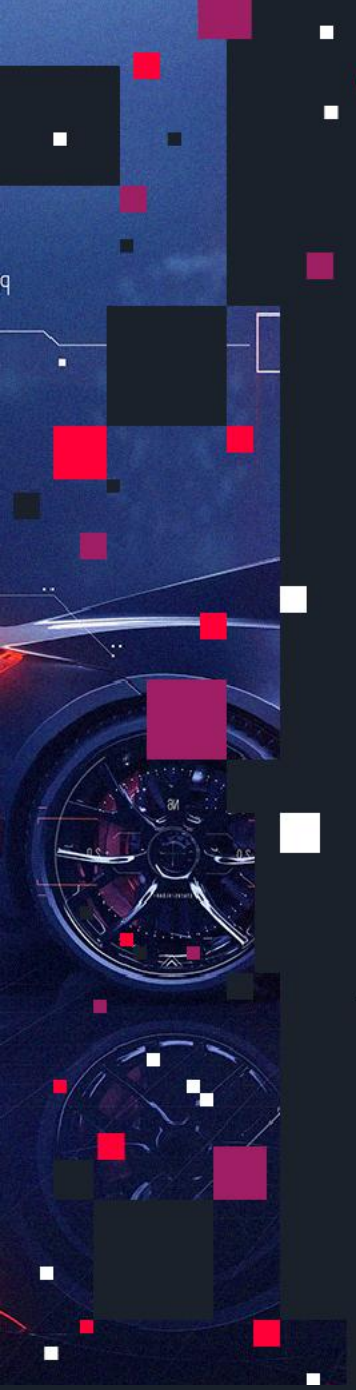
530 件の自動車関連の脆弱性が見つかり、

車両関連のセキュリティリスクが大幅に増加していることを示しています。



特に2019年以降に見られるこの大幅な増加は、**現代の自動車システムの複雑化が進んでいる**ことを示しています。

コネクティッドカーが増加し、ソフトウェアへの依存度が高まるにつれて、攻撃対象領域は拡大し続けています。ますます高度化するこれらのシステムを悪用から守るための包括的なセキュリティ戦略が必要です。

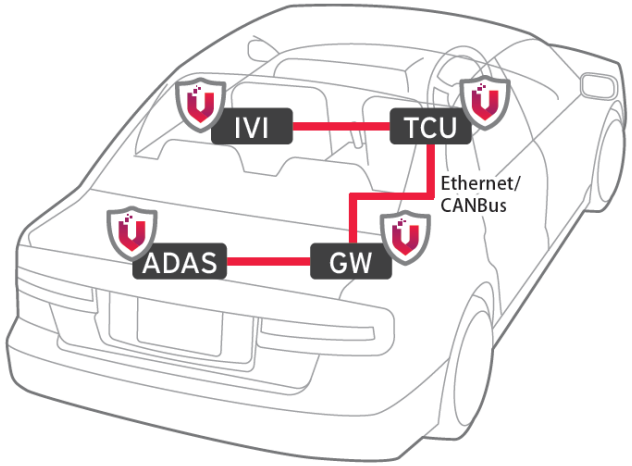


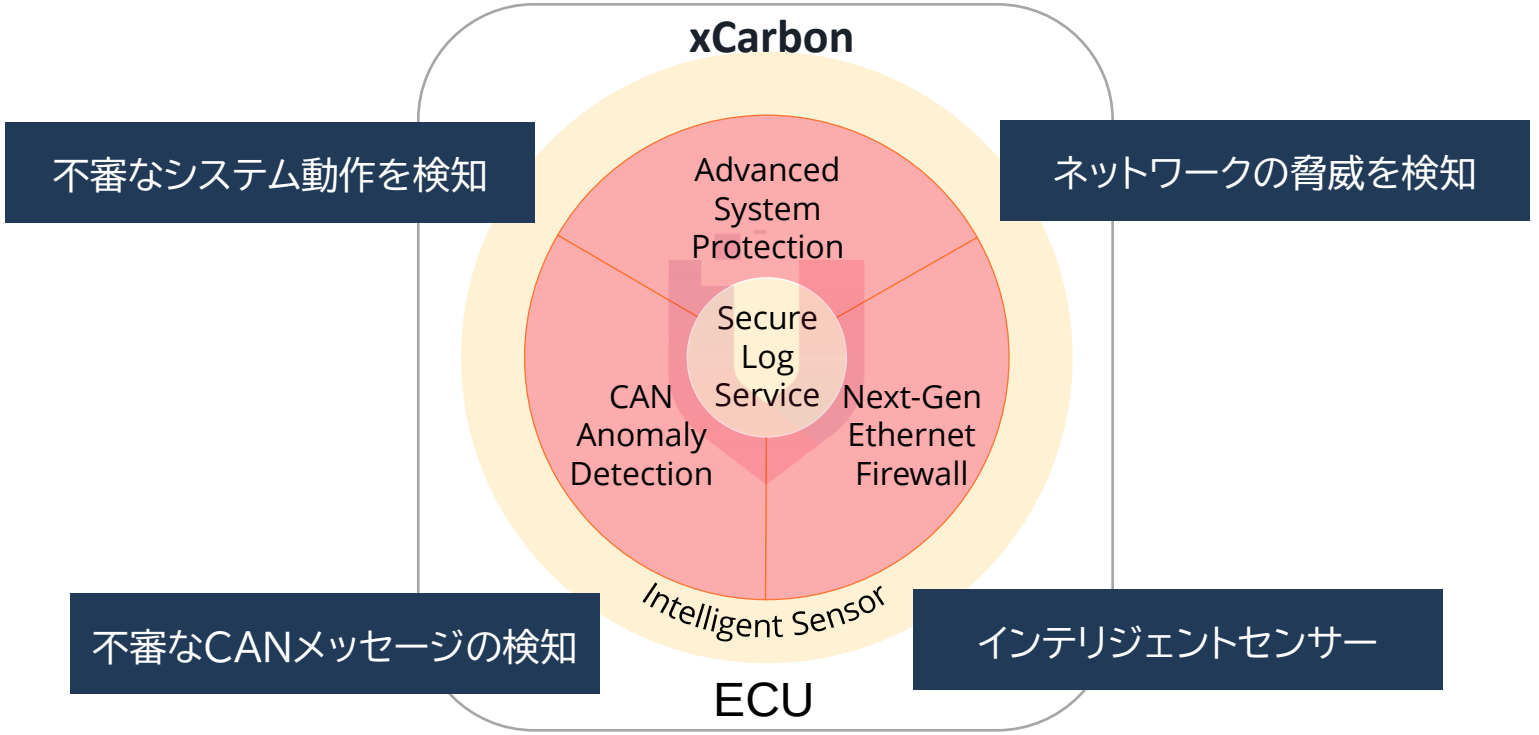
Intrusion Detection Protection Systems TODAY

VicOne’s IDPS Solution – xCarbon

xCarbon

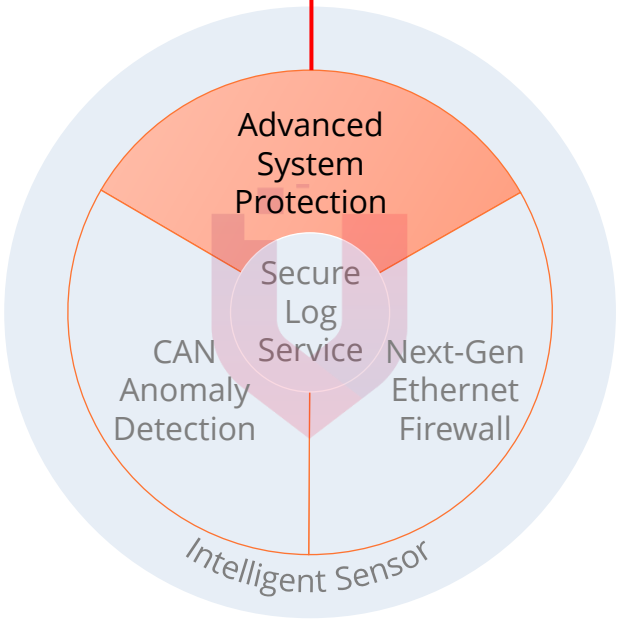
xCarbonはECUに対する、ソフトウェアベースのセキュリティソリューションです。
CANおよびEthernet向けのIDPS機能を搭載。さらにシステム内の不振な挙動を検出、ブロック。
VicOneのVSOCソリューションのxNexusとの連携により、詳細な分析が可能です。

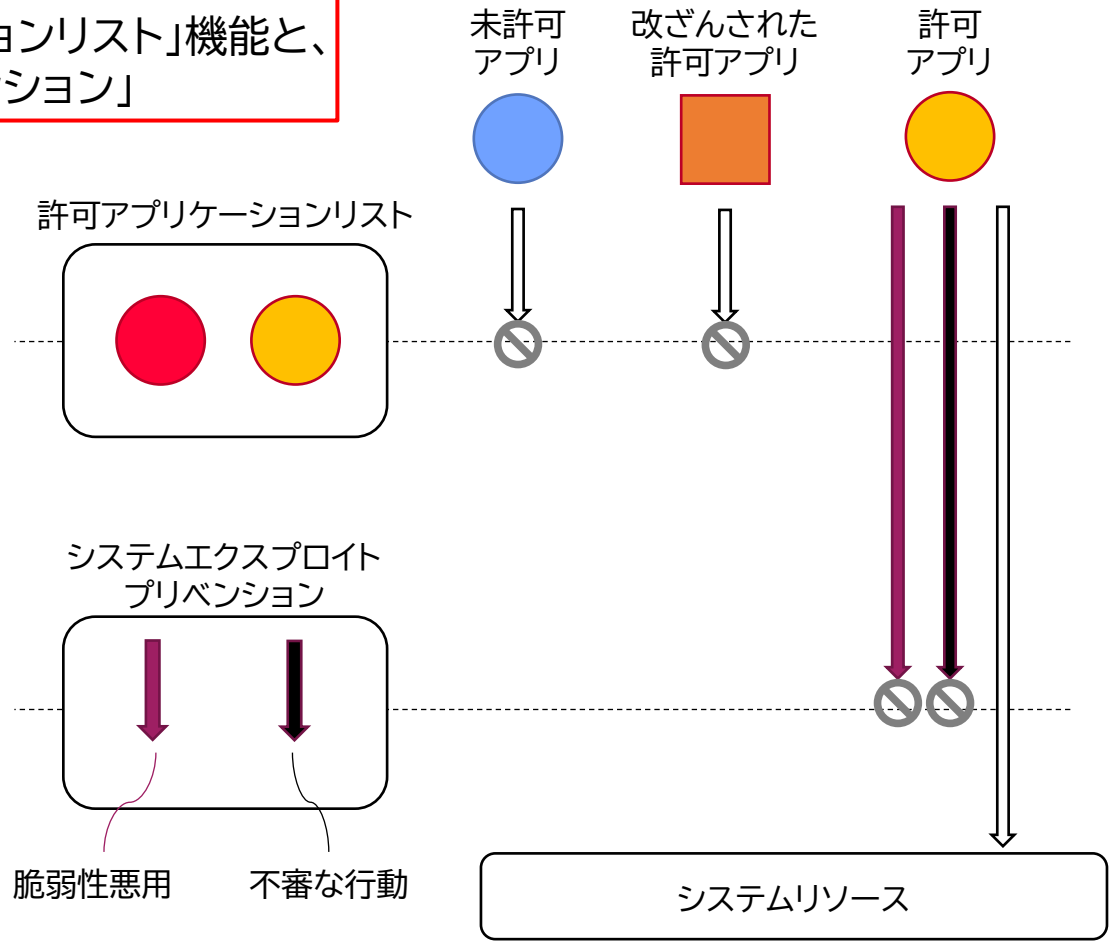




不審なシステム動作を検知

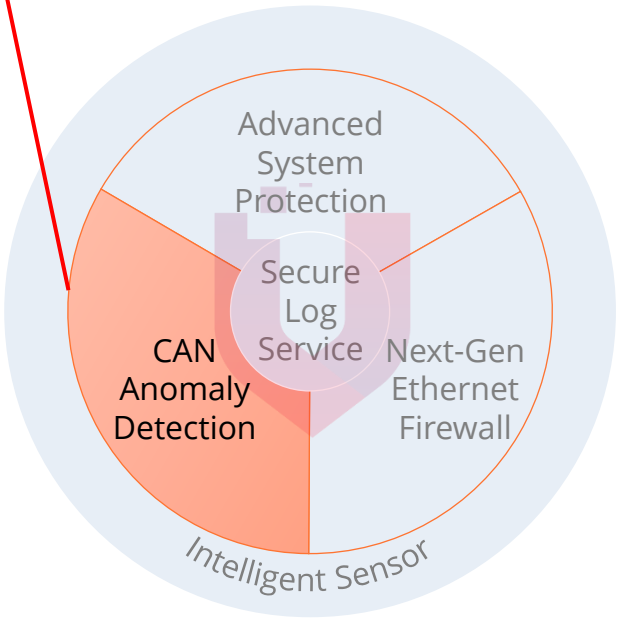
Advanced System Protection
許可されたアプリの起動のみを許可する「許可アプリケーションリスト」機能と、
システムの挙動を監視する「システムエクスプロイト・プリベンション」

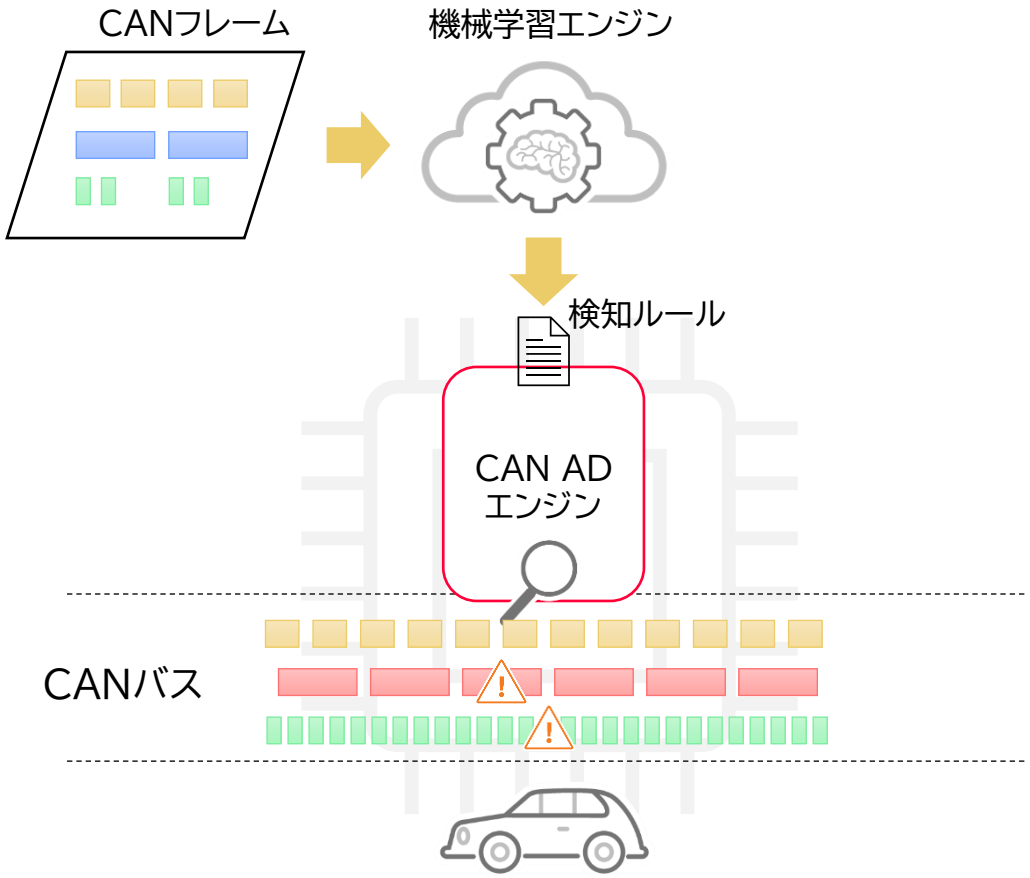




不審なCANメッセージの検知

CAN Anomaly Detection
xCarbonのCAN Message向けIDPSは、固定の検知ルールによる不審なCAN Messageの検出や、AIの学習に基づく異常検知が可能。





xCarbonのCAN異常検知の2つの提供方法

固定のルールに基づく CAN異常検知

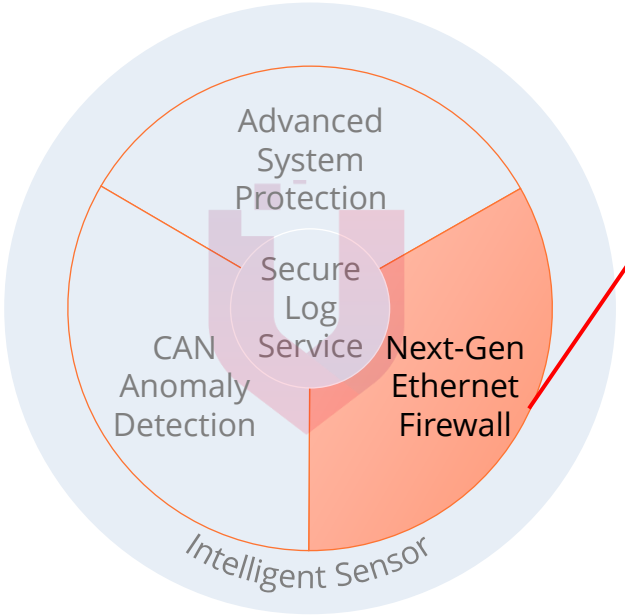
- **利点**
  - 基本的な既知の攻撃の検知が可能
  - CAN IDのリストのみでルール作成が可能なため、短期間での提供可能
- **必要な情報**
  - 対象車両のCAN IDリスト
  - DBCファイル

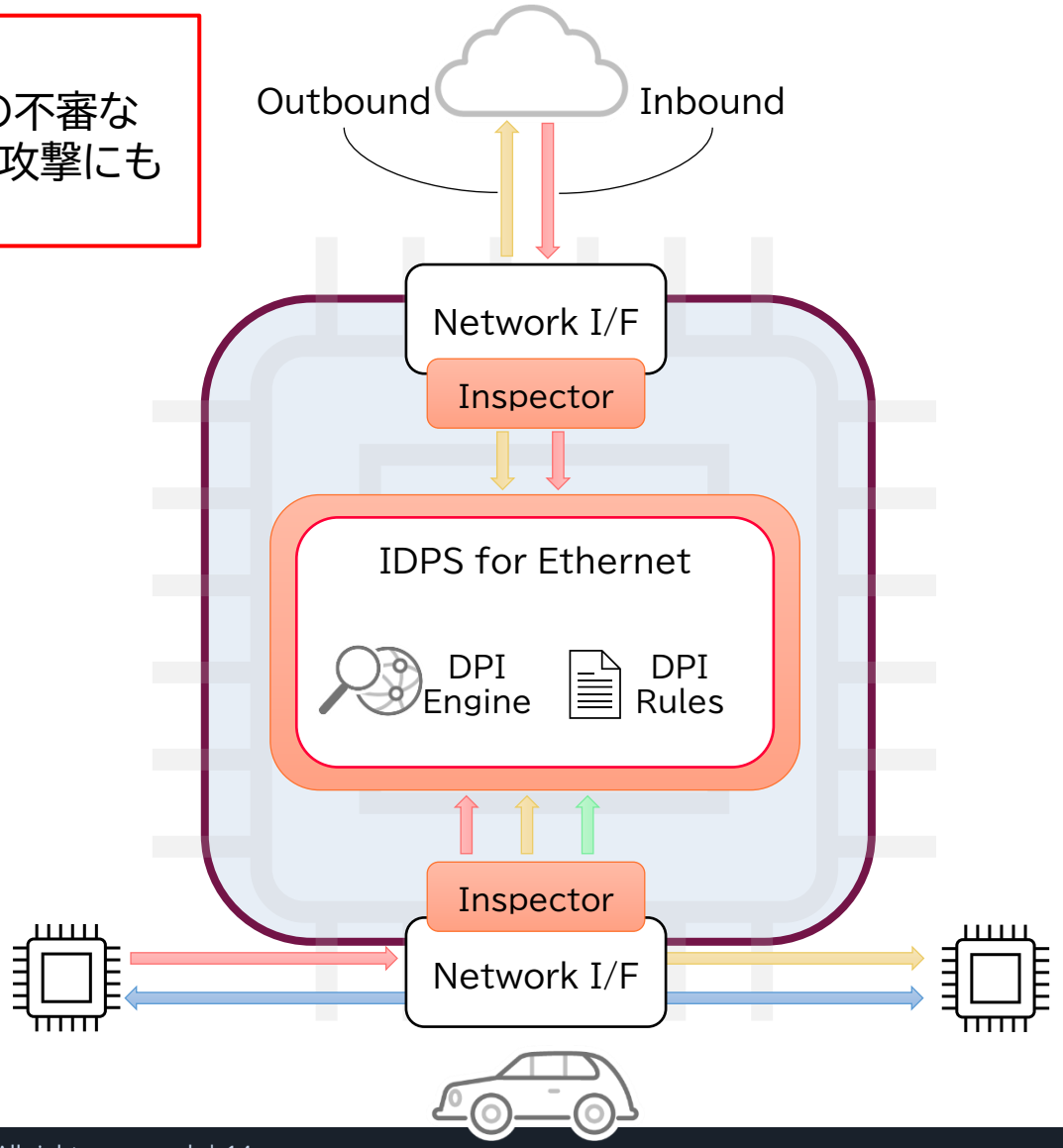
機械学習に基づく CAN異常検知

- **利点**
  - 対象車両のCANメッセージを機械学習することで、その車両に適切な検出ルールの提供
- **必要な情報**
  - 対象車両のCAN IDリスト
  - DBCファイル
  - 実車両でのCANメッセージデータ

ネットワークの脅威を検知

Next-Gen Ethernet Firewall
DPI技術により、DoS攻撃やポートスキャンなど、イーサネットの不審な通信を検知・防止。脆弱性攻撃検知ルールの更新により、最新の攻撃にも対応。

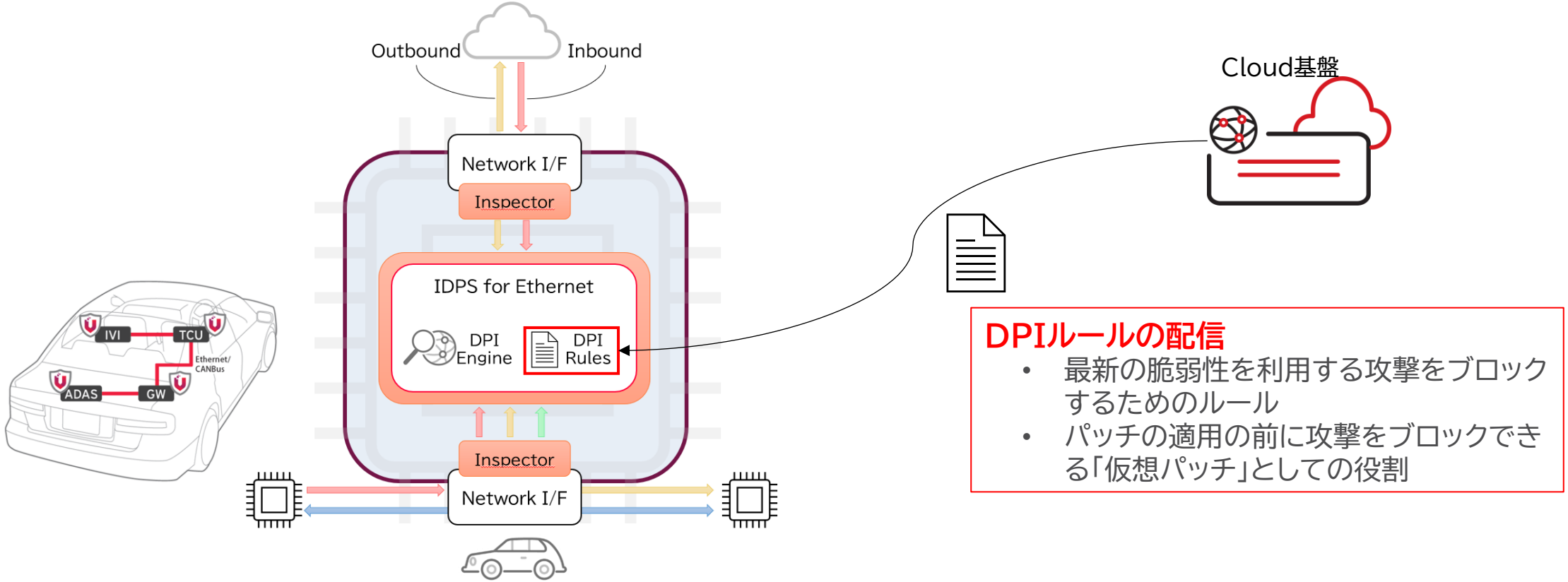




最新の攻撃への対応

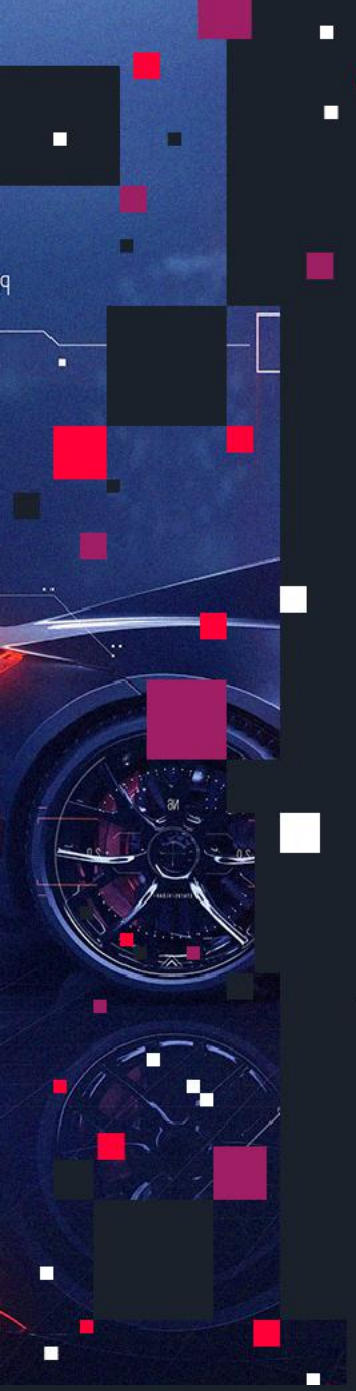
「仮想」パッチとしてのIDPSルール配信

日々発生するEthernetを利用する攻撃は、最新の脆弱性を狙うものが多い。xCarbonのEthernet向けIDPS機能では、DPIエンジンに対応した最新ルールを配信することで、最新の攻撃の検知・ブロックが可能。



DPIルールの配信

- 最新の脆弱性を利用する攻撃をブロックするためのルール
- パッチの適用の前に攻撃をブロックできる「仮想パッチ」としての役割



Intrusion Detection Protection Systems With TEE

攻撃者にとって大きな障害はセキュリティソフト

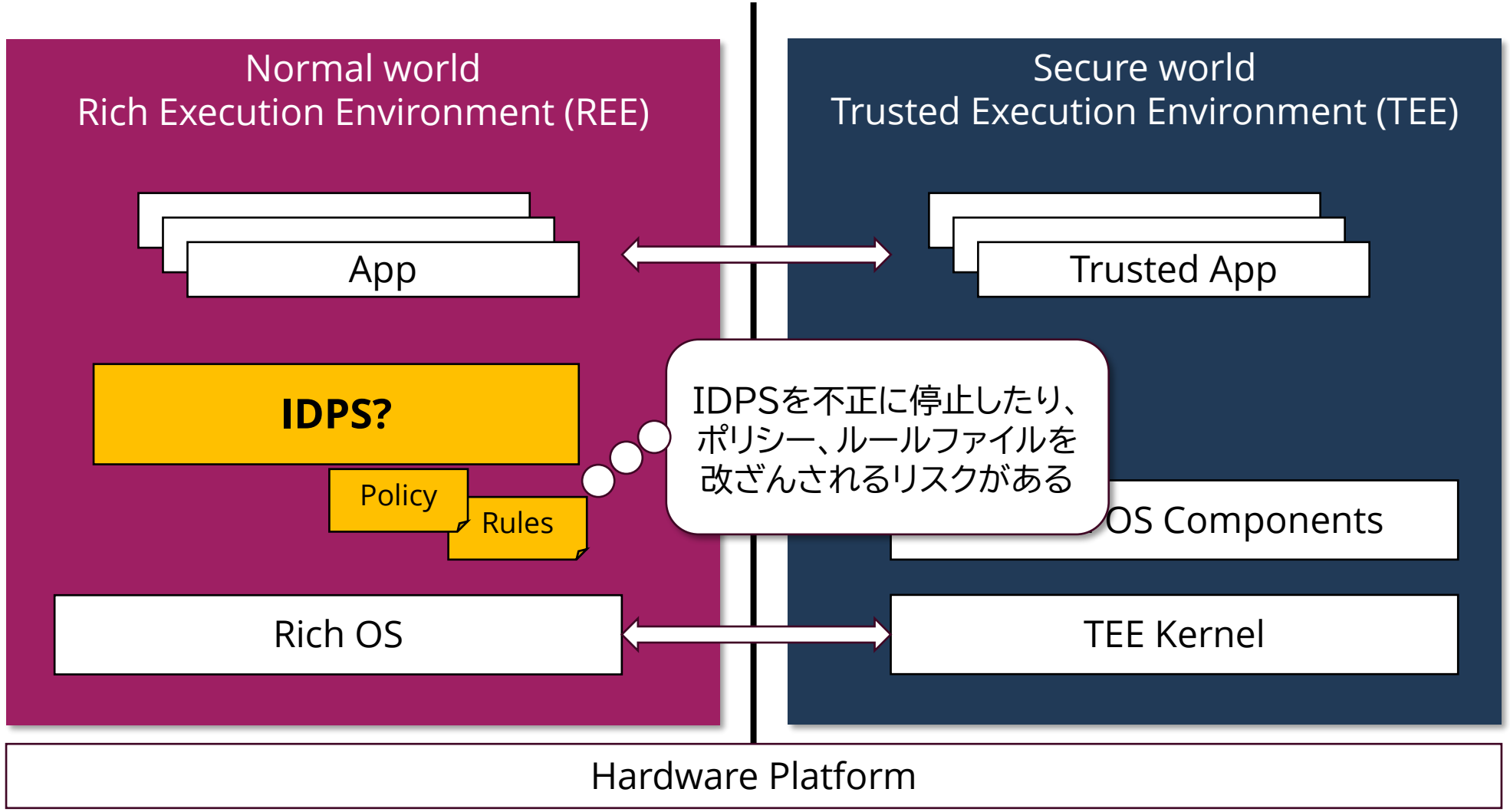
攻撃者はセキュリティソフトの無効化を攻撃ステップの1つに組み込むことがある。そのためIDPSを含むセキュリティソフトそのもののプロテクションが重要

https://www.trendmicro.com/ja_jp/jp-security/23/g/securitytrend-20230727-01.html

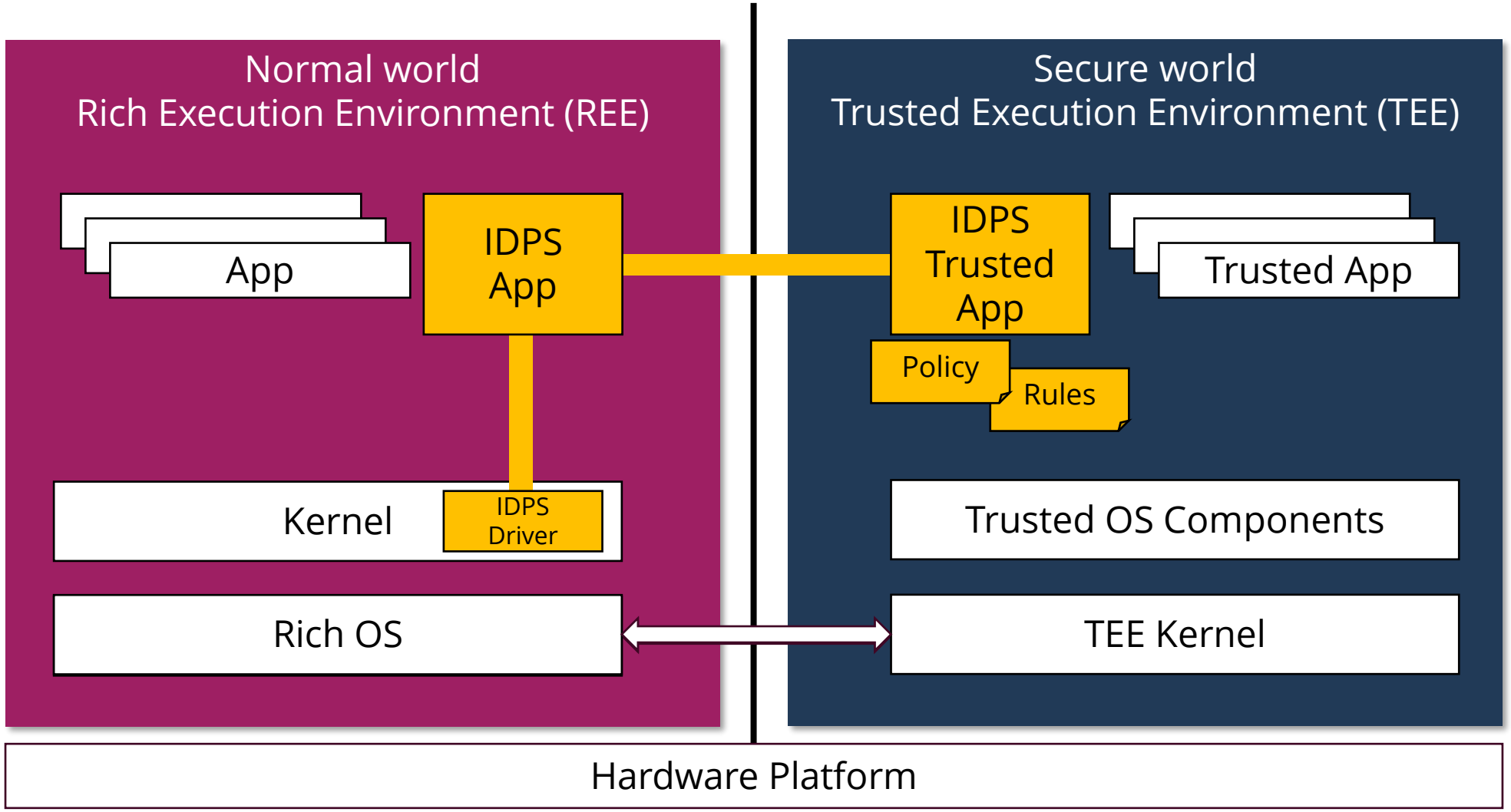
Trusted Execution Environment (TEE)

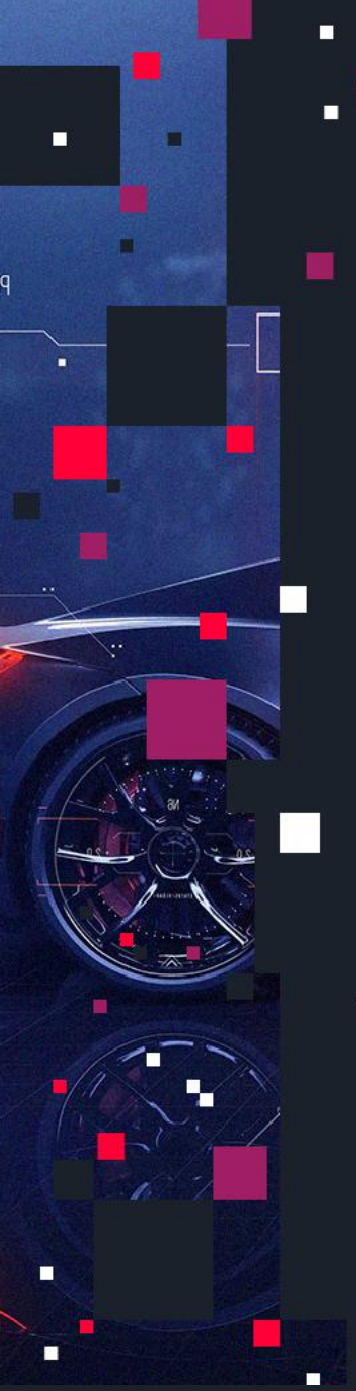
- Trusted Execution Environment（TEE）は、CPUなどのハードウェア支援によってシステム内部に隔離された安全な領域を作り出し、機密データや重要な処理を外部から保護しながら実行するための技術です。
- TEE内で動作するプログラムやデータは、通常のOSやアプリケーションからアクセス・改ざんされることがなく、暗号化や認証などのセキュリティ機能を安全に実行できます。
- 代表的な実装例として、ARM TrustZoneやIntel SGXなどがあり、スマートフォンやIoT機器、クラウド環境など幅広い分野で活用されています

通常環境にIDPSを設置することは安全とは言えない



TEEの利用によりセキュアなIDPS環境を実現





Intrusion Detection Protection Systems

FUTURE

IDPSの現在と将来

現在のIDPS

現在の車両のIDPSは、CAN通信の監視が中心であり、限定的な利用になっている。固定的な攻撃の検知にとどまるため、脅威の進化に追いつかない可能性がある。

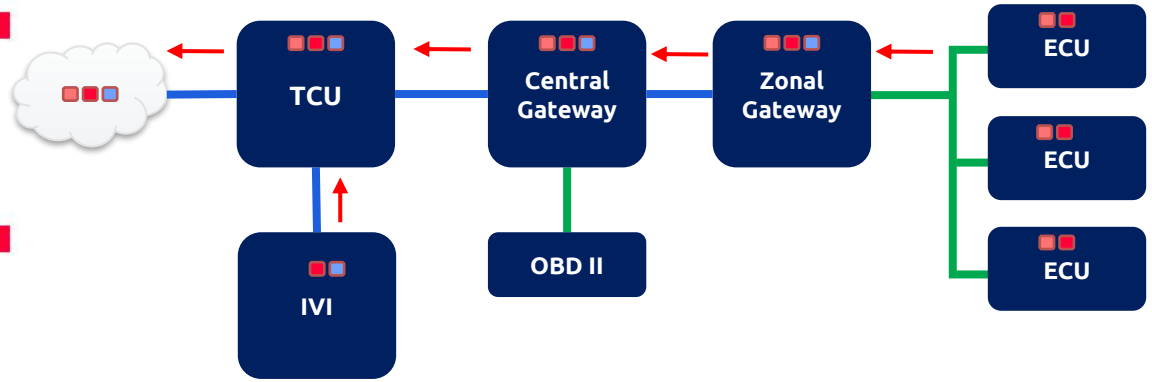
将来のIDPS

SDV時代に向け、OTAによる迅速な防御が可能となり、AIによる分析も進む。IDPS自身もTEE等との連携により、よりセキュアな運用が可能となる

項目	現在	将来（今後5年以内）
検出方式	シグネチャ中心	AI/MLによる異常検知
配置場所	ゲートウェイ中心	ECU・ゲートウェイ＋クラウド
防御対応	通知・ログ記録が主	通信遮断・制御も可能に
柔軟性	固定的	ソフトウェア定義、OTA対応
未知攻撃対応	弱い	強化される（自己学習など）
他システムとの連携	限定的	セキュアブート・TEE等と連携

将来のIDPSは導入・運用コストの低減にも貢献

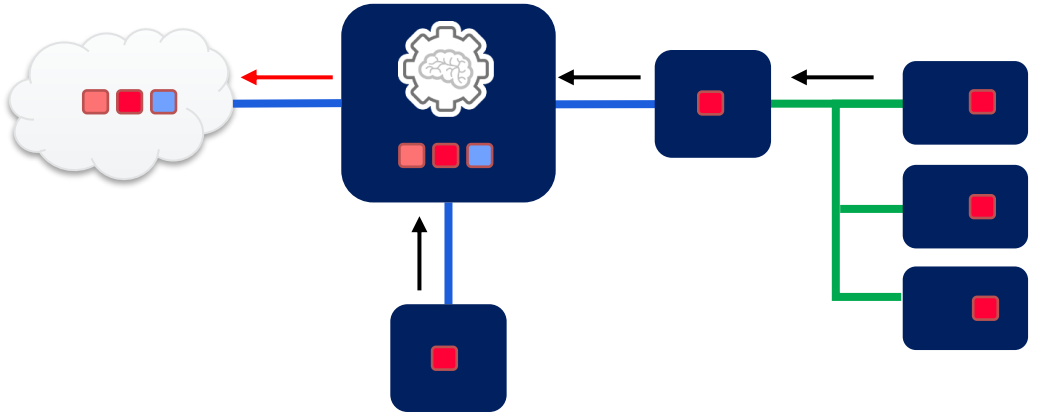
TODAY
各ECUにサイバーセキュリティを実装??



課題
- Gateway中心のIDPS設置ではすべての攻撃を検知できない
- 逆に言うと、すべての攻撃を検知するにはすべてのECUにIDPSを導入する必要がある
- 検知できる攻撃は限定的

NEXT
特定のECUにサイバーセキュリティ機能を集中化

AIを活用した集中化

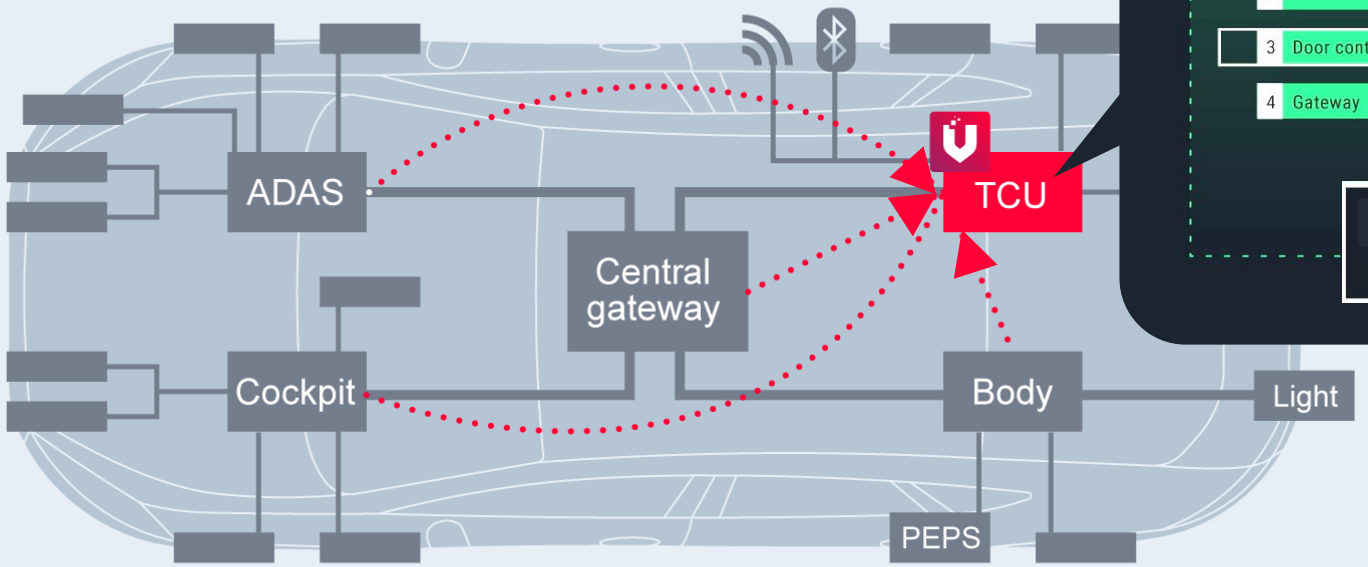


解決策
- 各ECUには最低限の機能を導入
- HPC等の導入に伴い、特定ECUにセキュリティ機能を集中化
- AIを使った分析により、新しい攻撃の検知も可能に

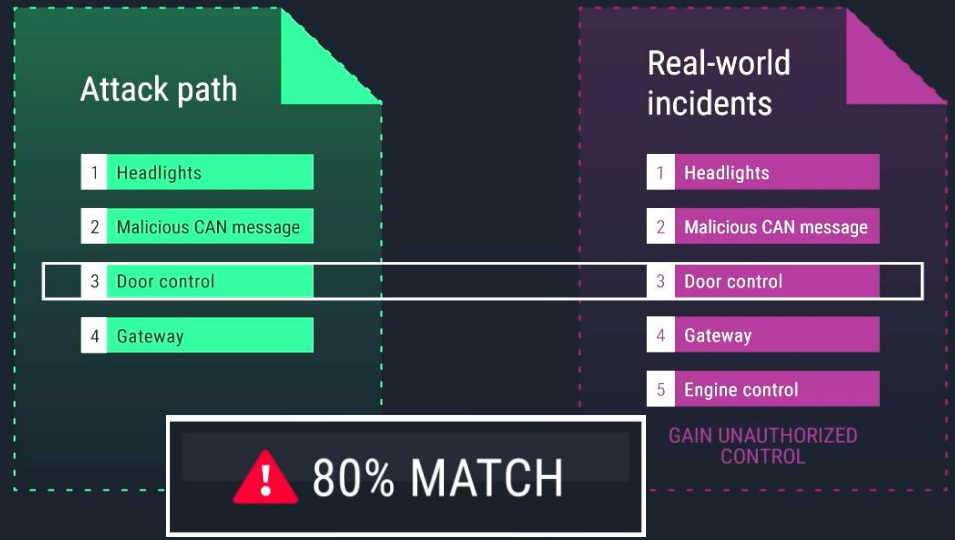
VicOne xCarbon Edge AI (特許出願中)

自己防衛機能を備えたスマート車両に

複数のECU間で車両データとセキュリティイベントを関連付けます。



散在するデータを文脈に応じた攻撃経路に変換。xCarbonは、これらの攻撃経路を実際のインシデントと比較します。



まとめ

🔍 現在のIDPSの課題

- シグネチャ検知では未知の攻撃に対応しきれない
- ゲートウェイ集中型では全体の把握に限界
- ソフト更新の頻度が低く、脅威の進化に追いつけない

🚀 今後のIDPSの進化ポイント

- AI・機械学習による未知攻撃のリアルタイム検知
- クラウド・OTA連携による即時防御と柔軟なセキュリティアーキテクチャ
- TEEによる、セキュアな環境

🎯 最終メッセージ

- “車載IDPSは、単なる監視ツールから能動的な防御基盤へと進化する”
- これからの車両セキュリティは、「常時進化する防御力」が鍵。

THANK YOU

VicOne

Driving Automotive Cybersecurity Forward

