PLAXIDITYX

GO EVERYWHERE

攻撃者も**AI**を使う時代へ
自動車サイバーセキュリティに不可欠な**AI**戦略

2025年**11**月**5**日 (水) 第**45**回**ReVision Webinar**
「**SDV** と**AI**によるクルマの進化とサイバーセキュリティのあり方を捉える」

喜田　由伎於

自己紹介

- 自動車業界にて、ソフトウェア開発からテスト自動化、車載ネットワーク、CI/CT、そして現在の自動車サイバーセキュリティまで、一貫して技術的な課題解決に従事。複雑な技術要件を分かりやすく伝え、顧客やパートナー企業様と共に実践的なソリューションを構築し、ビジネス価値を最大化することに強みを持っている。

経歴

- 2023年 - 現在: PlaxidityX (旧 Argus) / Senior Presales Engineer
- 2022年 - 2023年: ティアフォー/ Test Engineer
- 2016年 - 2022年: ベクター・ジャパン/ Field Application Engineer
- 2011年 - 2016年: ヤマハ発動機 / Software Engineer

専門領域・スキル

- 専門領域: 自動車サイバーセキュリティ (UNR155), プリセールス, テスト自動化, CI/CT, 車載ネットワーク
- システム統合スキル: Python, C, C++, CANoe, Autoware, プロジェクトマネジメント, ペネトレーションテスト

PLAXIDITY X
GO EVERYWHERE

Agenda

- PlaxidityXについて
- 自動車におけるAIの活用とサイバーセキュリティ
- サイバーセキュリティを強化するAIの活用
- 結論

PlaxidityX - 自動車サイバーセキュリティのグローバルリーダー

7,200万台+の自動車

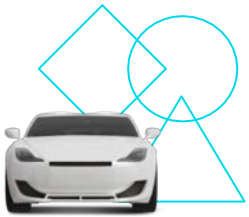
2021年以降、100社以上、52の
プロジェクトにおいて
PlaxidityXの技術が車両に搭載/搭載予定

グローバル展開

日本、ドイツ、フランス、米国にオフィス、
全世界で事業を展開

特許数

自動車サイバーセキュリティ
関連の特許



End-to-End ソリューション

DevSecOpsから車両セキュリティ、
そしてフリート保護技術・サービスまで、自動車メーカーとそのサプライヤー向けに包括的なソリューションを提供

品質管理

ASIL-Bに対応し、ASPICEレベル2
要件に準拠した開発

パートナーシップ

Microsoft、dSPACE、AWS、NXPなど、業界をリードする企業との
パートナーシップ

PLAXIDITY X
GO EVERYWHERE

自動車におけるAI

- AIが世界を動かす -

ほぼあらゆる分野において意思決定を加速し、自動化し、強化している

自動車産業もこの革命に加わっている
車両開発プロセスと車載機能の両方

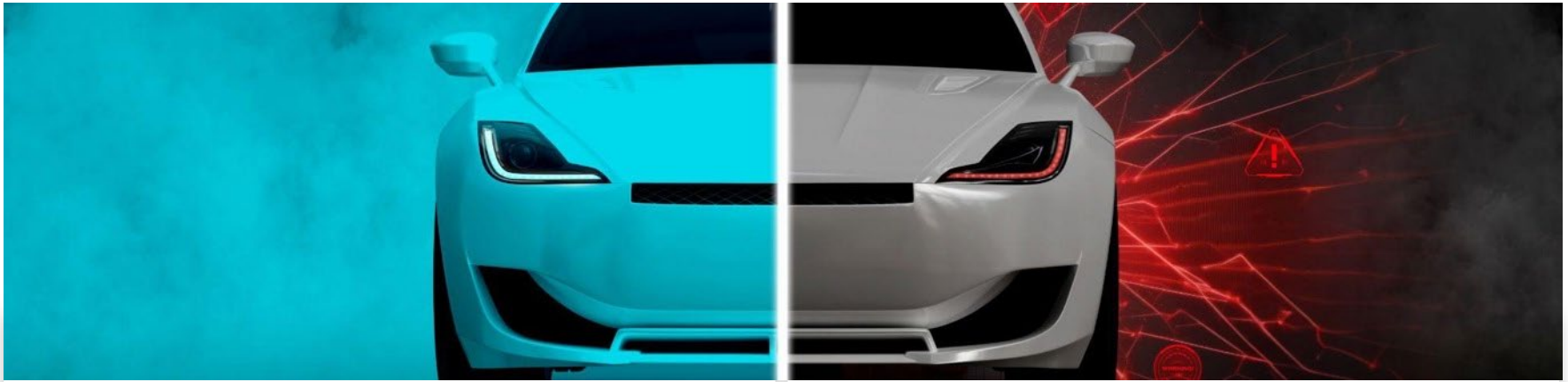
興味深い一例として、音声アシスタントからAIアシスタント 、あるいはAI強化型運転支援システムへの移行が挙げられる

メルセデス・ベンツ、Googleの会話型AIを車載バーチャルアシスタントに搭載

BYD、DeepSeekのAIを活用した運転支援技術の導入

AIは、自動車のサイバーセキュリティに何をもたらすのか？

自動車サイバーセキュリティにおけるAI：両刃の剣



車両開発プロセスの加速

AIベースの検知、監視、分析

AIを活用した車載セキュリティイベントの管理

AIが攻撃の手段として利用される可能性

攻撃者はAI機能を操作または悪用しようとする可能性

PLAXIDITY X
GO EVERYWHERE

PlaxidityX ケーススタディ - 中国OEM向けのペンテスト

PlaxidityX には、車両の「弱点」を見つけ出すペネトレーション専門のリサーチチームがおり、

約1年前、ある車両全体の侵入テストを実施した際のことです。

あるECUの権限を奪取後、予想外の “抜け穴” を発見しました。その“抜け穴”はというと・・・

「音声アシスタント」でした！

我々テスターは、システムを制御する強力な権限を持っていませんでしたが、

その「音声アシスタント」は、我々が持たない "特権" を保持していたのです！

我々は音声アシスタントを「遠隔で操り」...

車内ネットワーク（CAN）への攻撃に成功しました。

PLAXIDITYX
GO EVERYWHERE

車載AIを攻撃者から保護する

AI関連の規制は監視し、遵守すべきである

- ISO/PAS 8800:2024 自動車 — 安全性および人工知能
- EU規則2024/1689 – AI法

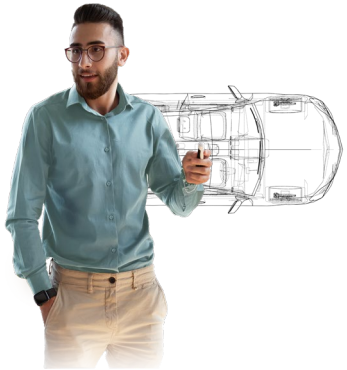
AI産業で既に学んだ教訓を活かす

- 権限の削減
- 入力フィルタリング
- 逸脱防止ルールを定義

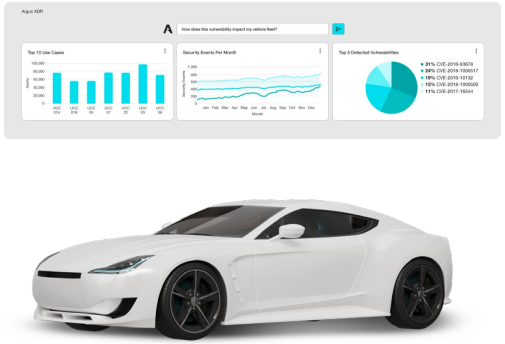
必要に応じてAIモデルをOTAで更新する機能

PLAXIDITY X
GO EVERYWHERE

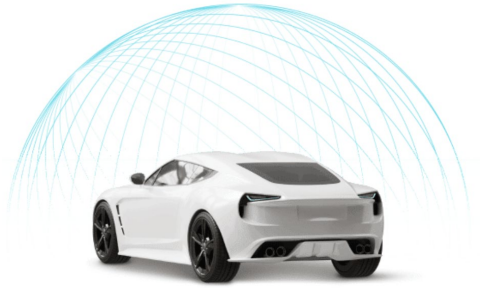
PlaxidityXが提案する3つのAI活用ツール



TARAプロセスの加速



AIによる
「ノイズ」と「真の脅威」の分離



サイバー窃盗防止ソリューション

現代における自動車サイバーセキュリティの課題

サイバーセキュリティ人材不足

2030年までに、世界全体で8,500万人のセキュリティ人材が必要となる（世界経済フォーラム）

自動運転車の安全確保には高度に専門化された技術が必要

リアルタイムデータ分析

大量のデータにより、脅威の迅速な検出が困難になる

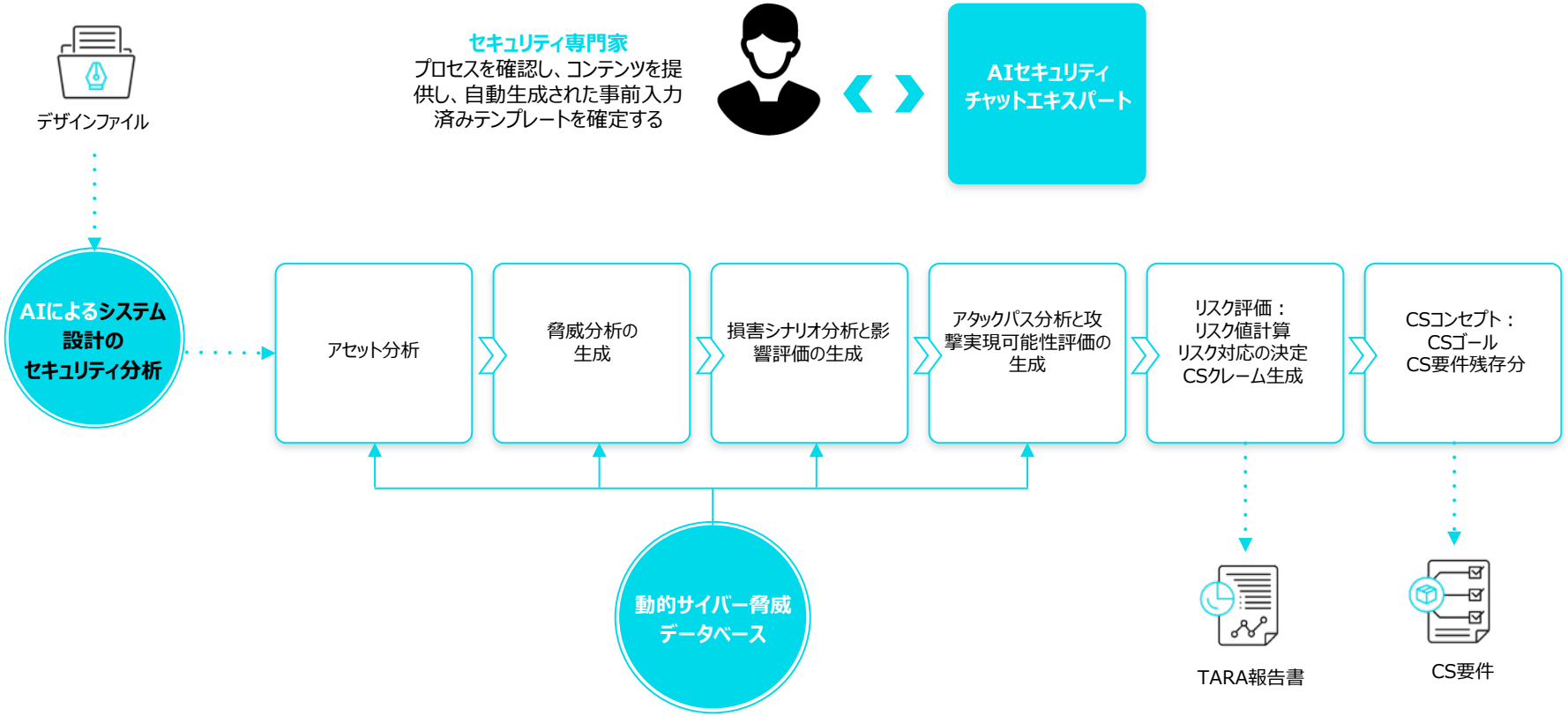
セキュリティチームは、誤検知により監視疲労に陥る

接続された車両からの膨大なデータ

車両は、より多くの情報源に接続され、正規化を必要とする膨大な非構造化データを生成する

進化する脅威への適応は、継続的な学習システムなしでは困難となる

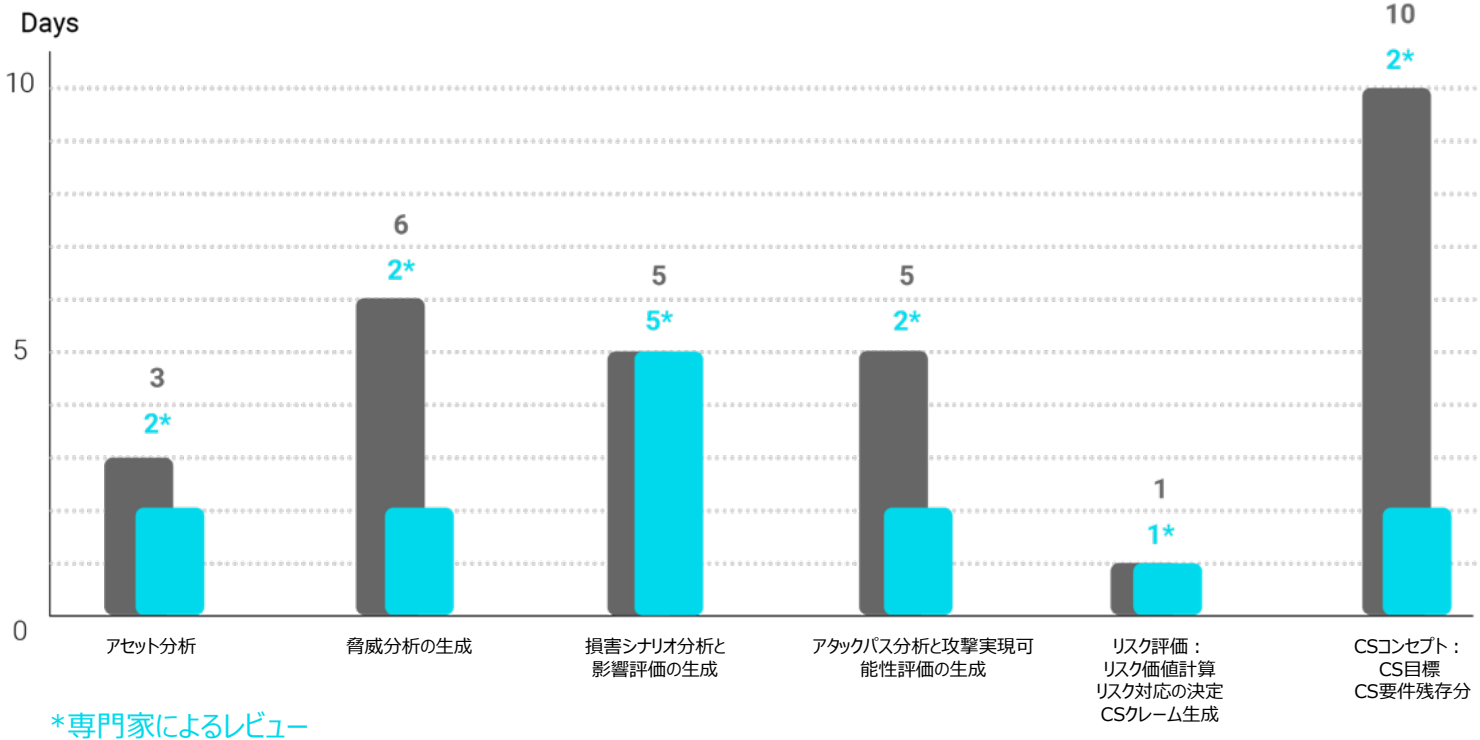
Use Case #1 - TARAプロセスの加速



PLAXIDITY X
GO EVERYWHERE

Use Case #1 - TARAプロセスの時間短縮

時間節約: 50%以上



*専門家によるレビュー

PLAXIDITY X
GO EVERYWHERE

Use Use Case #2 - 異常検知におけるAIの実世界応用

事例研究1： 車載ネットワーク（CANバス）異常検知

アルゴリズム: LSTM（長短期記憶）
フォーカス: 車両通信ネットワークにおけるRPMやギア偽装などの攻撃の検出
なぜLSTMなのか？: 時間経過に伴うデータシーケンスの分析に最適で、ネットワークトラフィックのパターン検出に理想的
結果: これらの攻撃を100%の精度で特定し、車両のセキュリティを強化

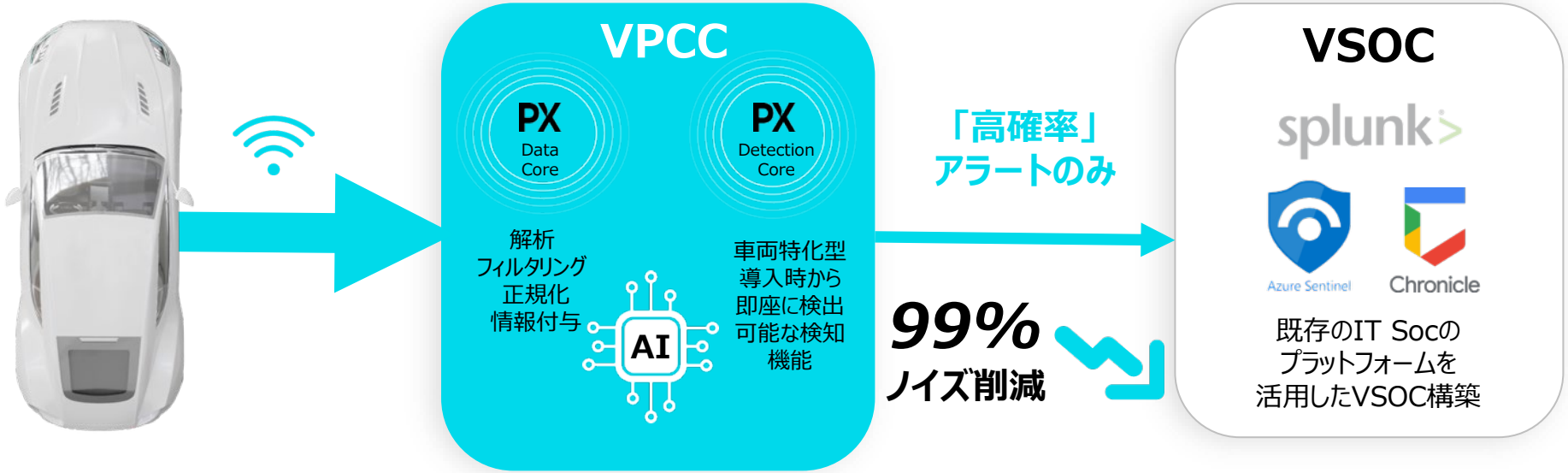
出典: Mansourian, P. et al. (2023). IEEE Transactions on Intelligent Transportation Systems.

事例研究2：車両センサーを用いた侵入検知

アルゴリズム: CNN（畳み込みニューラルネットワーク）とCWT (連続ウェーブレット変換)
フォーカス: 複数車両センサー（例：カメラ、GPS）を横断した攻撃の検知
なぜCNNなのか？: 画像やセンサーデータ内のパターン認識に優れており、異常行動の検知に最適である
結果: センサーベースの脅威検出において99%以上の精度を実現し、信頼性の高い保護を保証

出典: Wang, L. & Zhang, X. (2023). Applied Sciences.

Use Case #2 - AIによる「ノイズ」と「真の脅威」の分離



PLAXIDITY X
GO EVERYWHERE

Use Case #2 - ノイズから本物のアラートを抽出

適合率(P)：

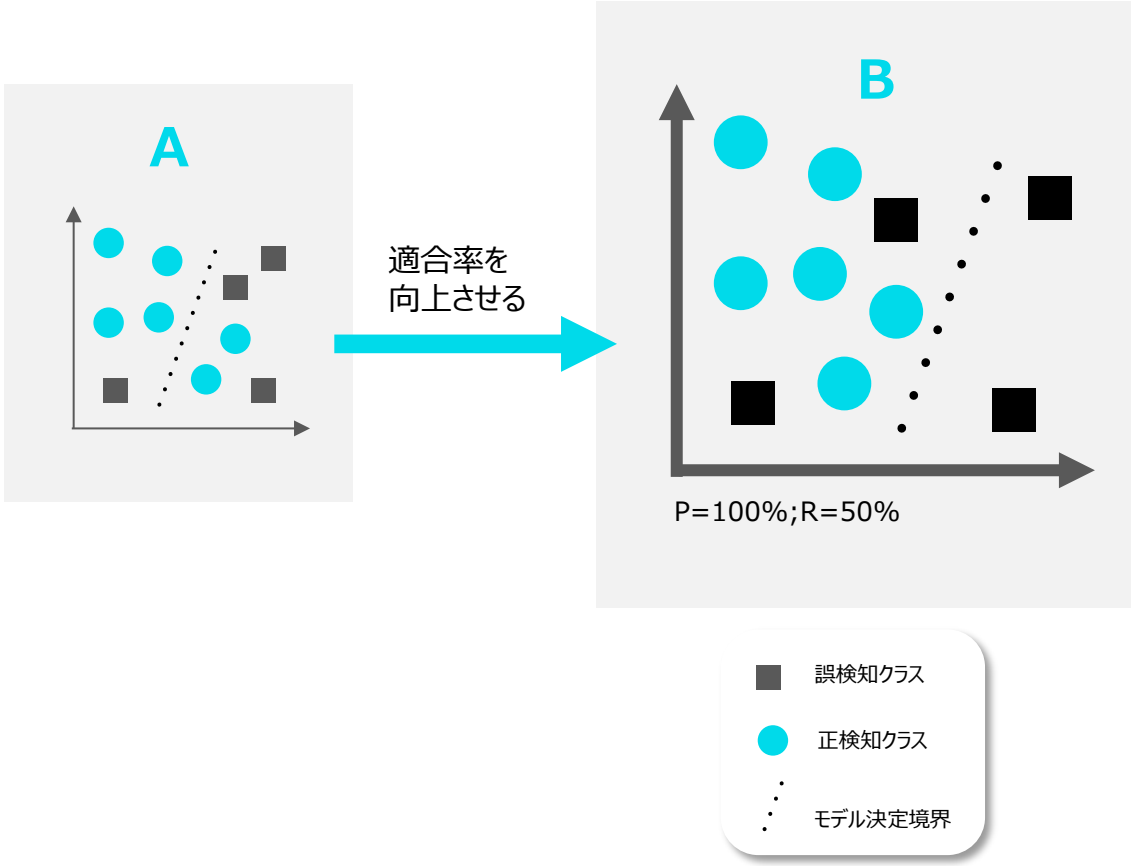
- 検出した異常のうち、どれだけが本当に異常だったかを示す指標

再現率／感度(R)：

- 実際に存在する異常を、システムがどれだけ見つけられているかを示す指標

F1スコア：

- 適合率と再現率のバランスを取った総合的な指標（一般に適合率と再現率の調和平均で表される）



PLAXIDITY X
GO EVERYWHERE

Use case #3 - 自動車盗難 ～世界的大流行～

1M+

米国の車両盗難

2023年の統計によると、盗難発生率は2019年比で42%増加

75%

英国で車両盗難が急増

2024年には13万台以上の車が被害に、過去10年間で増加

$1.5B

カナダの保険損失

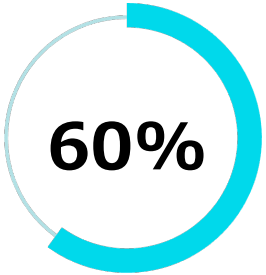
2023年の損失額は、2018年比で254%増加

226K

インターポールの警告

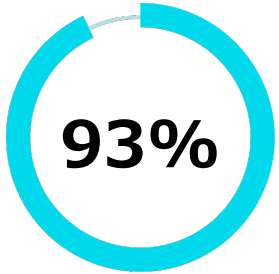
盗難車両の国境越え、組織犯罪との関連性

現代の自動車盗難に関する主要統計



車両盗難の手口（世界）

CANインジェクション およびキー複製によるもの

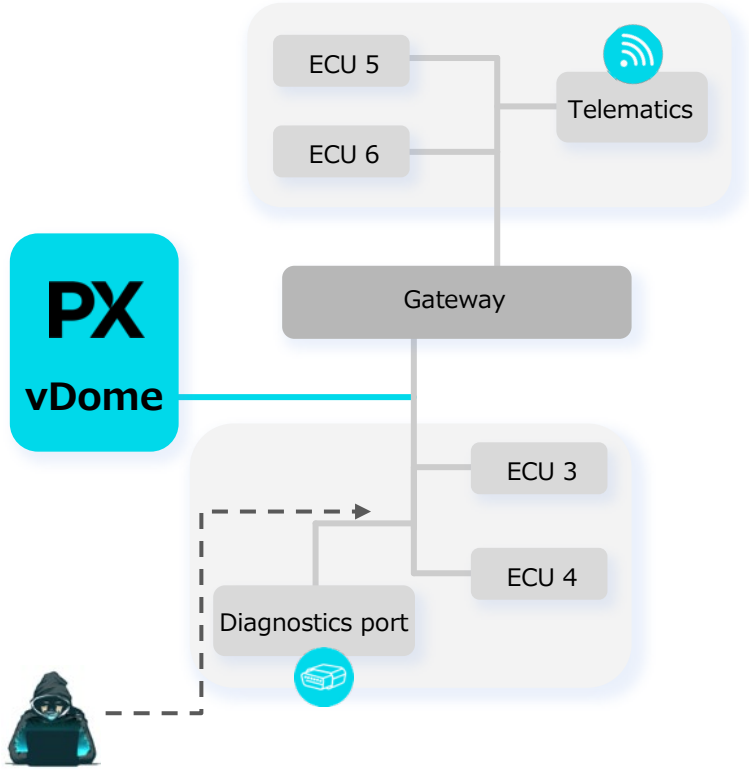


鍵なしで盗難

欧州で回収された盗難車両のうち、所有者の鍵なしで盗難された割合

PLAXIDITY X
GO EVERYWHERE

vDome: AIを活用したサイバー窃盗防止ソリューション



AIを活用した将来を見据えた対策

AI駆動の更新により、進化する脅威に対抗。専門家による支援付き。

OEMが新たな攻撃手法に先んじることを可能に。

誤検知なしで正確に

サイバー窃盗を瞬時に、かつ偽陽性ゼロで検知。

攻撃手法に関する重要な知見を提供。

真の予防、単なる検出ではない

盗難の試みを即座に阻止し、イモビライザーを無効化。

車両が動く前に窃盗犯を阻止。

PLAXIDITY X
GO EVERYWHERE

結論：よりスマートで安全なフリートの未来を切り開く

AIが車両の安全性を強化

AIによる異常検知により、脅威の検出がより迅速かつ正確になり、安全性が向上する

サイバーセキュリティチームの強化

AIはチームを代替するのではなく支援し、複雑な課題を効率的に処理できるようにする

サイバー脅威に先手

攻撃者がAIを活用する中で、防御側でもAIの活用が一歩先を行くために不可欠となる

PLAXIDITY X
GO EVERYWHERE

ご清聴ありがとうございました

製品やサービスの詳細については、
以下の連絡先にお願いします。

PlaxidityX
喜田　由伎於
yukio.kita@plaxidityx.com
https://plaxidityx.com/ja/

PLAXIDITYX
GO EVERYWHERE