# EV充電システムの保護

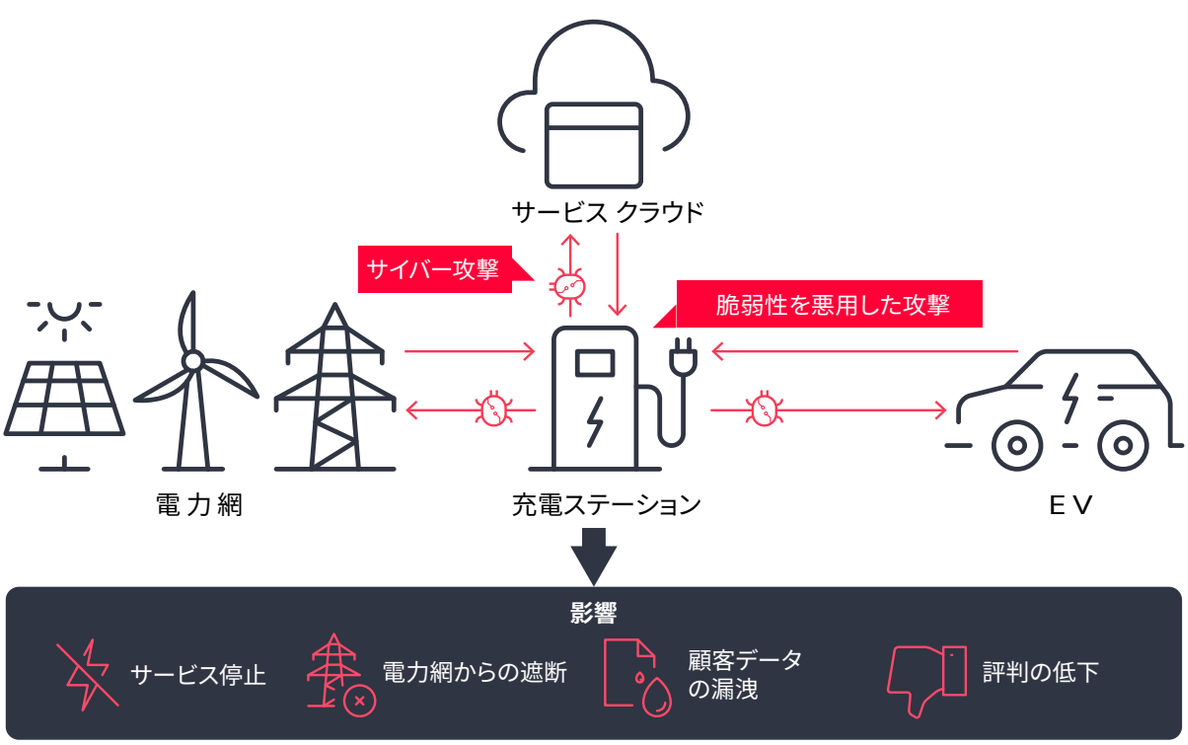
## ソフトウェアの脆弱性を常時監視し、高度な防御機能でEV充電システムを保護

## セキュア バイ デザインだけでは不十分

EV充電システムに対する最近の攻撃事例により、攻撃方法として次の2つが多いことが明らかになっています。

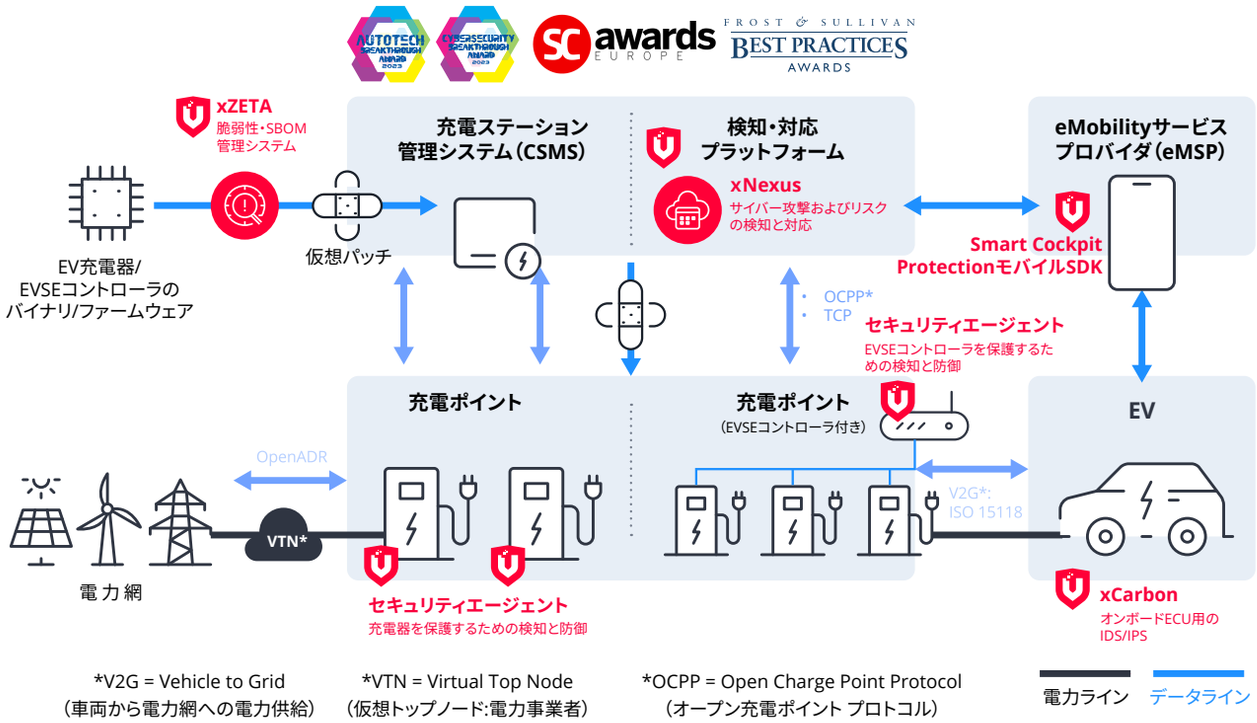
- **EV充電システムに対するオープンソースの脆弱性の悪用**
- **充電ポイントに向けたサービスクラウド、EV、電力網へのサイバー攻撃**

これらの攻撃ベクトルは、これまで原則とされてきた「セキュアバイデザイン」の枠組みの限界を浮き彫りにしています。現行のセキュリティ基準ではこの種の脅威を阻止し、システムを防御するには不十分であることが明らかになっています。 その結果、こうした脅威に包括的に対処するソリューションを義務付ける規制が増えています。



# 受賞実績のある全方位的なEV充電システムの保護

VicOneのEV充電システム保護ソリューションにより、脆弱性の悪用やマルウェアなどの脅威に対する保護を拡張することでセキュア バイ デザインを補強することができます。




## 主な機能・特長

### セキュリティリスクの検出と対応

VicOneのクラウドベースのXDRプラットフォームは、ハードウェアの変更を必要とせずCSMSデータに基づいたセキュリティリスクやサイバー攻撃をタイムリーに検出および対応を可能にします

### 継続的な脆弱性の特定

VicOneの脆弱性管理ソリューションは、ソフトウェア部品表(SBOM)を自動生成し、EV充電機のバイナリおよびファームウェアにおけるゼロデイ脆弱性やランサムウェアなどの脅威を継続的に検出できます

### サイバー攻撃に対するレジリエンス

統合セキュリティエージェントが、充電ポイントに対するDoS(サービス拒否)攻撃などの攻撃を即座に検知し、ブロックします

### 独自の仮想パッチ技術*

*特許出願中

VicOneの仮想パッチ技術は、ベンダーによる正規パッチが提供されるまでの平均102日間、早期保護を提供します

### 顧客の成功事例

電源およびエネルギー管理ソリューションの世界的リーダーであるデルタ電子社(Delta Electronics, Inc.)は、EV充電インフラのセキュリティ保全にVicOneのソリューションを採用しています

## 導入メリット

- システムを変更することなく、平均102日間の早期保護を得ることができます
- VicOneのソリューションは、NIST IR 8473サイバーセキュリティフレームワークプロファイル、ETSI EN303 645およびISA/IEC62443サイバーセキュリティ標準、英国のEVスマート充電規制の推奨事項を満たしています
- 脆弱性管理プロセスを6ヶ月から2週間に短縮できます
- ゼロデイイニシアティブ(ZDI)*による独自のゼロデイ脆弱性インテリジェンスを活用し、未然に防ぐ先進的な保護を実現します

*2007年以来、脆弱性発見数No.1

EV充電システムの保護_2024.10

Copyright © 2024 VicOne Corp.
All Rights Reserved.

詳しくはVicOneウェブサイトをご覧ください
(vicone.com/jpもしくは右のQRコードよりアクセス)