# EV充電システムをサイバー攻撃から守る

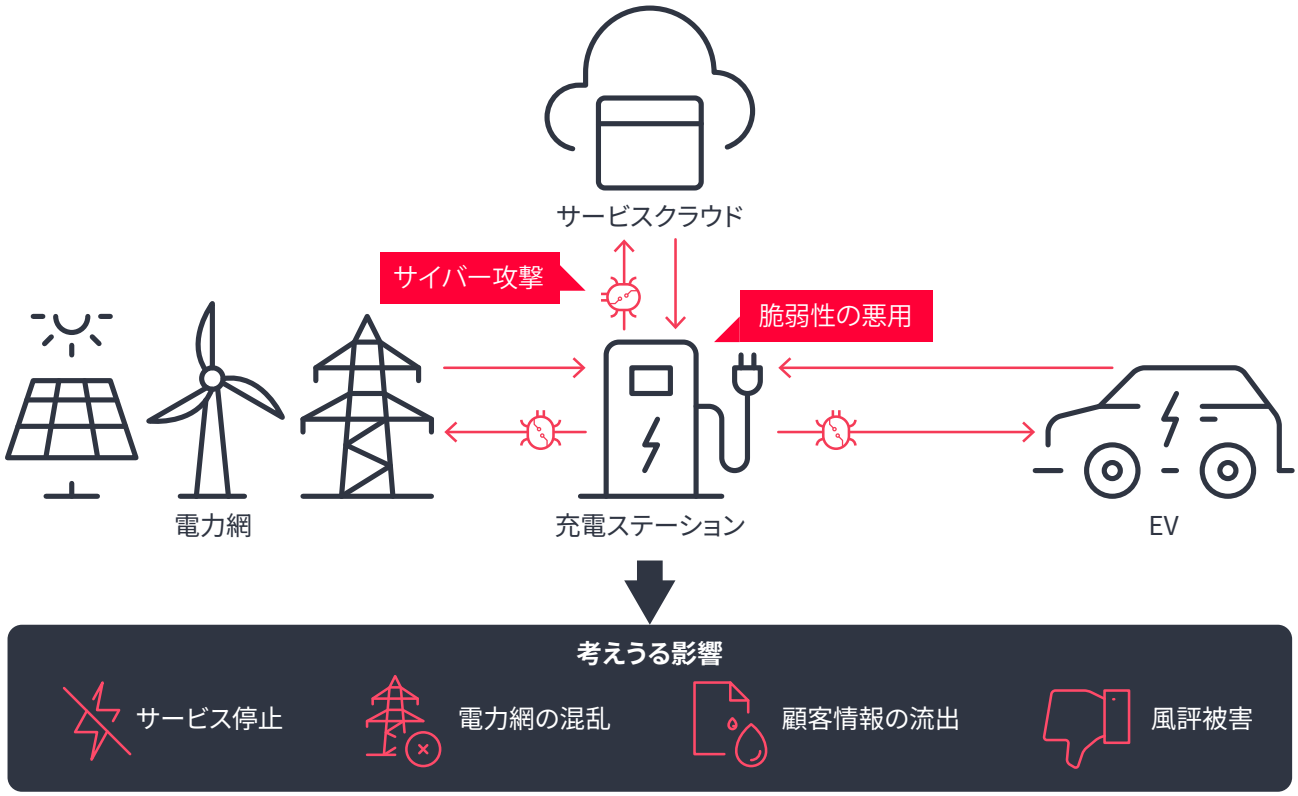
ソフトウェア脆弱性の監視によりEV充電システムを保護し、サイバー攻撃レジリエンスを確保。

## 「セキュア・バイ・デザイン」だけで安心でしょうか？

近年発生したEV充電システムに対するインシデントにおいて、2つの一般的な攻撃手法が明らかになりました。

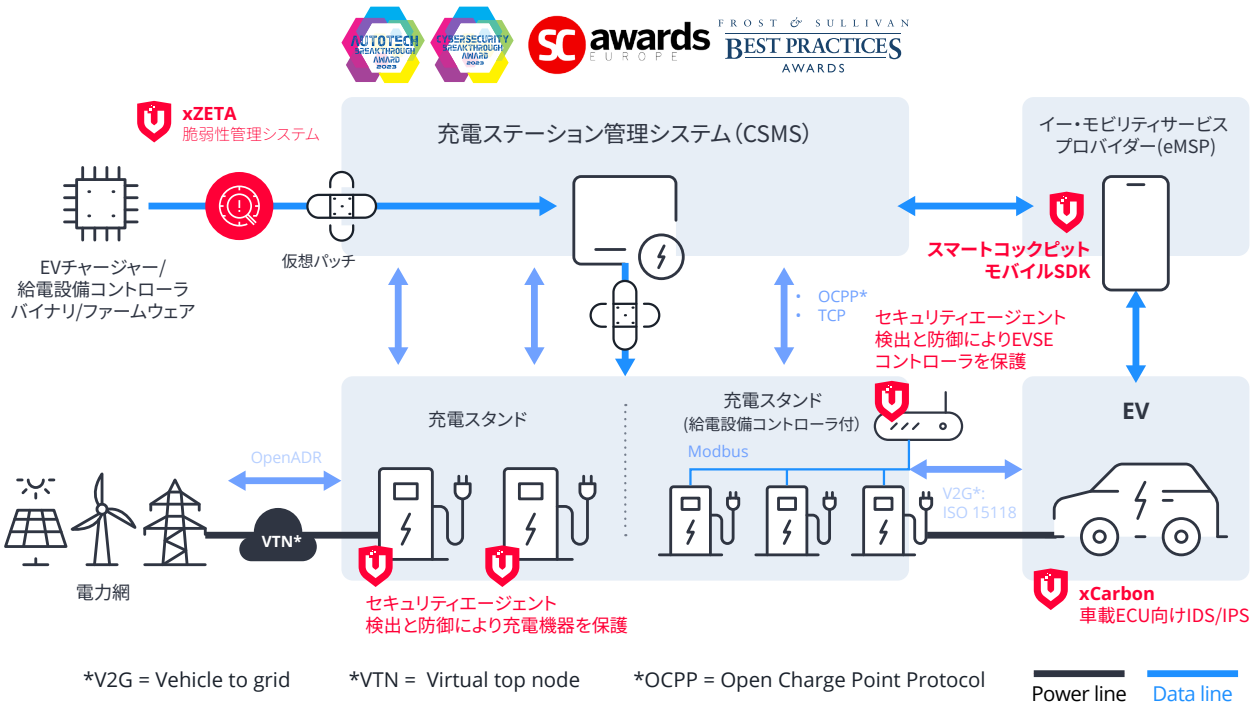
- EV充電システムにおけるオープンソースの脆弱性の悪用
- EV充電ステーションを介した、サービスクラウド、EV、電力網へのサイバー攻撃

これらの攻撃ベクトルの出現は、セキュア・バイ・デザイン原則の限界を浮き彫りにしているといえます。現行の規格はこの種の脅威からEV充電システムを防御することを想定しておらず、市場の多くのEV充電システムは脆弱なままです。今後、これらの脅威に対処するための包括的な対策が義務付けられるようになると予測されます。



# 第三者機関に評価された、VicOneの EV充電ステーションプロテクション

VicOneのEV充電システム保護ソリューションは、脆弱性を突いた攻撃や不正アプリケーション等の脅威から充電ステーションを保護します。




## 主な特長

- **継続的に脅威を検出**
  EV チャージャーのバイナリやファームウェアに含まれ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し、ソフトウェア部品表（SBOM）を自動生成することができます。
- **サイバー攻撃に対する耐性**
  統合されたセキュリティエージェントが、充電スタンドに対するサービス妨害（DoS）攻撃などを即座に検出し、ブロックします 。
- **独自の仮想パッチ技術**
  当社の仮想パッチ技術は、ベンダーの更新プログラムリリースに最大102日先んじたゼロデイ攻撃からの保護を可能にします。
- **未承認アプリケーションのブロック**
  アプリケーション セーフリストにより、許可されたアプリケーションのみが給電設備で実行され、安全な運用環境が維持されます。
- **カスタマー・サクセス**
  当社のソリューションは、電力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Delta Electronics社に採用され、EV充電インフラを保護しています。

## メリット

- システムを変更することなく最大102日間の早期保護開始が可能
- ETSI EN 303 645サイバーセキュリティ規格および英国のEVスマートチャージ規制に適合
- 脆弱性管理プロセスを6ヶ月から2週間に短縮
- Zero Day Initiative（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、プロアクティブな保護を実現

*2007年以来、脆弱性情報公開において開示数No.1


EV Charging System Protection


より詳しい情報は、こちらのQRコードをスキャンして VicOne.com/jp にアクセス