digicert

EV 充電の進歩を推進

サイバーセキュリティのリスクに対処しながら、コンプライアンスの確実な達成と EV 充電の採用を促進する

二酸化炭素排出の削減と気候変動への対応が喫緊の課題となる中、電気自動車（EV）の普及に向けた世界的な動きが加速しています。このような電気化への移行は、増加する EV 車をサポートするための、セキュアで信頼性の高い EV 充電インフラを確立する重要性を浮き彫りにしています。自動車メーカーをはじめ、チャージポイント開発業者、グリッドオペレーター、都市プランナー、政策立案者など、各分野の関係者が、新世代の EV 車の需要を満たすために堅牢な電気インフラストラクチャとチャージポイントの構築に積極的に取り組んでいます。しかし、このように拡大する EV 充電エコシステムは、サイバー脅威の格好の標的になっており、普及の障壁になる数々の課題も抱えています。

EV 充電が抱える信頼性の問題

EV 充電が抱えている重要な課題の 1 つは「走行距離の不安」です。つまり、目的地に到達するのに十分な電気がないかもしれないという不安です。この懸念を増大させているのは、現在の充電インフラの不十分な普及です。今後 EV の購入を検討している消費者でも、EV を持ったら、充電ステーションに行きつけずに立往生してしまうのではないかと恐れています。さらに、EV 市場においては、それぞれの CPO（Charge Point Operator：チャージポイントオペレーター）間の規格が標準化されていません。そのため、各種 EV モデルに対応する充電ステーションの相互運用性について混乱を招いています。

digicert®

EV リスクについての消費者の認識

充電なしで車が止まってしまう可能性から、サイバーセキュリティの脅威に至るまで、消費者の頭の中にあるのはハイテク EV のセキュリティ上の懸念です。Deloitte の調査によると、消費者の **53%** が EV セキュリティに関して懸念を示しています。[1] これは EV 否定派のみの意見ではありません。また、EV 所有者の **64%** が公共の充電ステーションのセキュリティに関して懸念を示しています。[2] この注目度の高い業界では、消費者は EV 車のメリットとリスクについてよく知っています。そして、この懸念は杞憂ではありません。Market Scoop によると、自動車業界では直近の **3 年間**においてサイバー攻撃件数が **225%** も増加しました。[3]

これらの課題に対応するために、関係者は EV 充電エコシステムのサイバーセキュリティの強化にともに取り組んで、そのインフラのアクセシビリティとユーザー操作性を改善する必要があります。これには、充電プロトコルとコネクタを標準化したり、充電ステーションの密度と視認性を改善したりすることが含まれます。また、個々のステーションにおいて EV の充電方法に関する明確でユーザーフレンドリーな情報を提供することも含まれます。

53%

の消費者が、EV のセキュリティについて懸念を示している

64%

の EV 所有者が公共の充電ステーションのセキュリティについて懸念を示している

自動車業界では、
直近の **3 年間**において
サイバー攻撃件数が

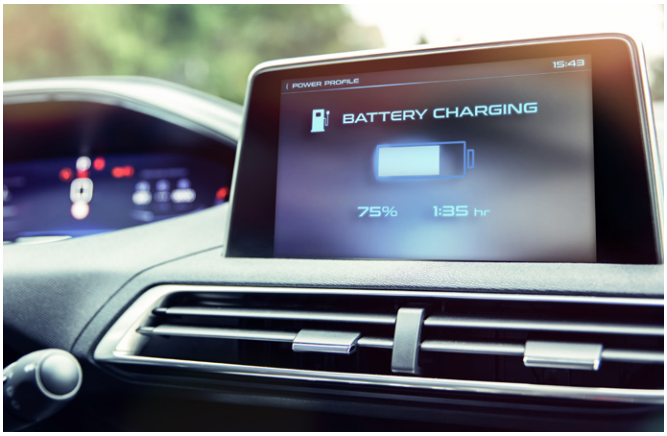
225%

も増加した

[1] https://www2.deloitte.com/us/en/pages/about-deloitte/articles/press-releases/deloitte-affordability-concerns-slow-the-road-to-an-electrified-future.html
[2] Ponemon Institute、「Securing the EV Infrastructure: A Survey of Electric Vehicle Drivers in the United States」
[3] https://scoop.market.us/automotive-cyber-security-rises-the-autonomous-driving-technology

消費者が EV により惹きつけられ、持続可能な電気化された輸送システムへの移行が加速するようにするには、自動車業界は、次の重大なサイバーセキュリティリスクに優先的に対応していく必要があります。

1. 不正アクセス：サイバー攻撃者が EV 充電システムに不正アクセスし、充電プロセスを操作したり、機密データにアクセスしたりする事態が起きる可能性があります。
2. データ侵害：EV 所有者の個人情報や支払情報が漏えいし、プライバシーの意図しない公開や金融詐欺につながる恐れがあります。
3. サービス拒否（DoS）攻撃：攻撃者の攻撃により充電サービスの中断を招き、ユーザーの不都合や EV 充電インフラのダメージが生じる可能性があります。
4. ファームウェアの改ざん：悪意のあるファームウェアアップデートにより、充電ステーションや EV 自体の機能の危殆化を招く恐れがあります。
5. 中間者（MitM）攻撃：攻撃者が EV と充電ステーション間の通信を傍受して、データを盗んだり、悪質なコマンドを仕込んだりする可能性があります。



リスク軽減のための対策：OCPP 2.0.1 および ISO 15118-2

オープンソースの通信規格によって、消費者が恐れているサイバーセキュリティリスクに対応することで、EV の普及を促進できます。

充電ネットワーク全体でのセキュアな通信

- OCPP 2.0.1 は、高度な認証メカニズムとセキュアなファームウェアアップデートを実装することで、EV 充電インフラのサイバー脅威に対する耐性を大幅に強化します。これにより、不正アクセスとデータ侵害のリスクが著しく減少します。改善された認証メカニズムやセキュアなファームウェアアップデートなど、セキュリティプロファイルや機能が新たに導入されています。また、OCPP 2.1 では、TLS 1.3 の実装が必須となっており、サーバー側証明書とクライアント側証明書の両方で相互認証が必要です。

EV と充電器の間のセキュアな通信

- ISO 15118-2 は、EV と充電ステーションの間の安全な通信に焦点を当てています。この規格はプラグ＆チャージ機能をサポートしているため、人間が介在せずに認証と請求を自動的かつセキュアに行えます。ISO 15118-2 では、暗号化された通信用の TLS（Transport Layer Security）が採用されているため、中間者（MitM）攻撃からの保護が実現されます。また、この規格で求められる認証により、規格に準拠した証明書を使用する必要があるため、許可されたデバイスとユーザーしか充電サービスにアクセスできないようになります。

これらの規格に準拠することで、EV、EVSE（Electric Vehicle Supply Equipment：電気自動車給電装置）のOEM、チャージポイントオペレーター、モビリティオペレーターは、EV 充電エコシステムのセキュリティを大きく向上させることができます。ISO 15118-2 準拠の証明書を使用して TLS を実装することで、EV と充電ステーションの間でやり取りされるデータが暗号化されるため、盗聴やデータ侵害から保護されます。さらに、OCPP 2.0.1 の高度なセキュリティ機能が、不正アクセスとサービス拒否（DoS）攻撃を防ぐため、ファームウェアアップデートの完全性が確保されます。OCPP 2.0.1 および ISO 15118-2 の両規格の導入は、EV 充電エコシステムに対するサイバーセキュリティリスクを軽減するうえで欠かせません。こうすることで、セキュアな通信、認証、データ保護に向けた堅牢なフレームワークを実現できます。これにより、EV 充電インフラのセキュリティ態勢を全体的に強化でき、電気自動車の普及が推進されます。

EV 充電エコシステムのセキュリティ確保：自信を持って進める

EV 業界のサイバーセキュリティをめぐる広範な課題に対処するために、デジサートは、デバイストラストを向上させる重要なソリューション（ISO 15118-2 規格準拠）を提供しています。TrustCore SDK（FIPS 140-3 準拠）と連携する Device Trust Manager は、組み込みソフトウェアの主要なセキュリティ開発ツールです。OEM やチャージポイントオペレーター（CPO）はこのツールを活用することで、デバイスとネットワークのセキュリティを迅速に向上させることができます。

Device Trust Manager では、デバイス ID とクレデンシャルの管理を簡潔化できるため、EV 充電エコシステム内の各コンポーネントが十分に認証されて信頼された状態に保たれます。一方、TrustCore SDK に備わっている堅牢なセキュリティ機能スイートは FIPS 140-3 の厳しい要件を満たしており、デバイスソフトウェア開発の安全な基盤として機能します。

これらのツールを統合することにより、EV の OEM、EV チャージポイントやチャージポイントオペレーター（CPO）は、EV と充電ステーションの間でセキュアな通信が行われるようにできます。また、データのやり取りの暗号化、アクセス制御、不正アクセスやサイバー攻撃などのリスクの軽減を実現できます。デジサートの包括的なソリューションは、今日のサイバーセキュリティ上の懸念に対処し、安全でスケーラブル、かつ相互運用可能な EV インフラの開発をサポートします。デジサートは、今日の問題に対処しつつも将来の課題を見据えることで、お客様の信頼を築いてきました。デジサートは、電気自動車の普及を推進していきます。

デジサートは、全世界の大手自動車メーカーの 83% のデジタル完全性を確保しています。具体的には、堅牢なサイバーセキュリティソリューションを提供することにより、機密データの保護と自動車サービスの信頼性の確保を実現しています。デジサートの専門知識により、当社のソリューションは EV メーカーと充電インフラプロバイダの個々のニーズを満たすだけでなく、自動車産業のセキュリティ環境という広い視野を念頭に置いて設計されています。これにより、EV 充電システムのセキュリティと信頼性をさらに向上させています。2018 年以降、デジサートは SAE ITC および EV PKI（Public Key Infrastructure：公開鍵基盤）コミュニティと証明書ポリシー（CP）の開発に積極的に取り組んでおり、ISO 15118-2 規格の準拠と堅牢な実施を目指しています。デジサートは、ChargePoint 社や Eonti 社と共同でホワイトペーパーを執筆しました。この中で、上記の規格においてセキュリティ、相互運用性、拡張性が不十分であったところ、適切なガバナンスポリシーやコントロールがないところが明示されました。この重要な調査を踏まえて、SAE は新たに EV PKI コンソーシアムを招集することにし、結果的にデジサートは、証明書トラストリスト（CTL）の開発の契約を受注するに至りました。この CTL は、包括的な証明書ポリシー（CP）をインスタンス化することを目的としており、既存の規格が対応していなかったいくつかの重大な課題に直接対処します。このようにデジサートのリーダーシップとインサイトによって、安全で相互運用可能かつ拡張性のある EV 充電エコシステムに欠かせない拡張の開発が促進されています。これは、電気自動車インフラという現実の世界にデジタルトラストを確立するうえで大きな一歩となっています。

将来を見据えた充電：まとめと展望

電気自動車（EV）業界は、重大な岐路に立っています。全世界の二酸化炭素の排出量を減らし、気候変動に対応することが証明されている革新的なソリューションを提供していますが、消費者の抱く懸念が普及の足かせになっています。その懸念の多くは、サイバーセキュリティ上の既存の脆弱性に関するものです。こうしたリスクは EV エコシステムの完全性の脅威となるだけではなく、業界の成長の妨げとなっています。これらの脆弱性を信頼できる包括的なサイバーセキュリティソリューションで対応するのは、EV のデジタルインフラを保護するうえで不可欠なだけでなく、消費者の信頼を築くうえで重要なステップであると言えます。これにより、日常生活に電気自動車が溶け込むようになり、さらには持続可能な輸送の未来も確かなものになるのです。

EV トランスフォーメーションを進めるには、技術革新を戦略的ポリシーやインフラ開発と組み合わせた多面的なアプローチが必要です。EV 業界が OCPP 2.1、ISO 15118-2 などの規格に準拠しつつ、デジサートの Device Trust Manager と TrustCore SDK を統合して導入することで、EV 充電エコシステムをサイバー脅威から守ることができます。これらの対策によって、EV 充電のセキュリティとトラストの向上を図れるだけでなく、消費者の電気自動車に対する信頼も高まります。EV は、実現可能かつ持続可能な輸送手段とみなされるようになるでしょう。

電気自動車への移行を加速させるには、自動車メーカー、チャージポイント開発業者、テクノロジー企業の間の戦略的提携が不可欠です。これにより、安全かつ効率的で、誰でもアクセスできる EV 充電ネットワークへの道筋が開けます。このような共同の取り組みは、安全で誰でもアクセスできる、ユーザーフレンドリーな充電インフラを生み出します。このインフラは、現在また将来の EV 所有者のニーズを満たすものになります。

500 億台

2030 年までの EV 車

2030 年までに、公道を走る電気自動車の数は 5 億台にも上ると予測されています。[4] そのため、広範囲に及ぶ強固な充電インフラの構築は急務になっています。EV 業界が進化と革新を続けるにつれ、デジサートが掲げるビジョンである「完全に電気化された輸送エコシステム」の実現は近づいています。この取り組みにおいて、サイバーセキュリティリスクへの対処と消費者の懸念の解消は重要なステップであり、電気自動車への移行を早めるものでもあります。この移行は、全世界の二酸化炭素排出の大幅な削減をもたらしうることから、EV 業界は、「持続可能な電気化された将来」への取り組みの最前線に位置付けられています。充電インフラの中核にデジタルトラストを据えることで、電気化への道筋を安全に保護するだけでなく、地球環境に対するコミットメントを果たすことになります。それこそが現実の世界を見据えたデジタルトラストです。より環境に優しく、セキュアな将来を実現できるからです。

デジサートの優位性

デジサートと提携して、デバイスの取り組みを向上させるセキュリティの土台を築きましょう。デジサートのセキュリティがコンプライアンスを保証するだけでなく、EV 充電のイノベーションにつながることを確認するために、digicert.com/contact-us までお問い合わせください。

[4] https://www.iea.org/reports/by-2030-evs-represent-more-than-60-of-vehicles-sold-globally-and-require-an-adequate-surge-in-chargers-installed-in-buildings