太陽光発電のサイバーセキュリティ基準を設定する

世界のエネルギー部門に高まる脅威

今日、相互接続された世界において、エネルギー産業は多方面からサイバー攻撃の主要なターゲットとして、大きな脅威に晒されています。このような脅威はサイバー犯罪者による金銭的な攻撃から、国家ぐるみで組織された政治的な動機による攻撃まで多岐にわたります。

2023年だけでも、世界中のあらゆる業界でサイバー攻撃の被害者が、ランサムウェア攻撃を受けて11億ドルもの巨額な金額を支払っています。- 報告されている件だけでこの額です。*

40,000

オランダ政府は、オランダの家庭や企業に設置された太陽光発電システム4万台が、遠隔制御に対して脆弱であると認めた (2022年7月)

130,000

いくつかのPCSメーカーの太陽光発電システム13万台は、サイバー攻撃に対して脆弱であるとサイバーセキュリティ企業が報告 (米国、2023年7月)

2億ドル

2013年に米国で空調制御プロバイダーのネットワークがハッキングされ、ターゲットにされた企業の被った推定損失額。

脆弱な太陽光発電システムによる甚大なビジネスリスク

太陽光発電は、世界のエネルギー構成の中で急成長しており、オランダ、ドイツ、米国などの多くの国々で総エネルギー生産の大部分を占めています。すでに多くの企業にとって、電力コストを削減し、ビジネスの継続を確保するための重要なエネルギー源となっています。しかし、太陽光発電システムは、持続可能なエネルギーソリューションを提供する一方で、サイバー脅威の新たな手段にもなっています。各システムの中心にあるパワーコンディショナは、通常はインターネットに接続するIoTデバイスで、システム監視と制御を可能にします。そのため、ガスや石炭の発電所に比べ、サイバー攻撃を受けやすくなります。

蓄電池、EVチャージ、空調制御システムなどのサイト内のエネルギー負荷の電力供給に太陽光が使われるようになり、エネルギー管理システムの時代に移行するにつれ、ますますその傾向が強まるでしょう。脆弱な太陽光発電システムは、ビジネスの継続性を脅かすだけではありません。エネルギー負荷だけでなく、組織の広範なデジタルプラットフォームに知らぬ間にハッカーがアクセスできてしまう入口となる可能性があり、物質的および金銭的な損害や企業価値の低下をさらに引き起こしかねません。

* www.chainalysis.com/blog/ransomware-2024

一般的なサイバーリスクは、以下の通り

データ漏洩とペナルティ

ハッカーは脆弱な太陽光発電システムを利用して、組織の内部ネットワークに存在する個人データを盗み出し、その結果、被害者が多額の金銭を支払わなければならないようなデータ漏洩を引き起こす危険性があります。

遠隔操作とサービス拒否（DoS）

DoS攻撃や遠隔制御の侵害といった被害に遭った場合、企業は大きな混乱に直面します。ランサムウェアは重要なデータを人質とし、遠隔制御やDoS攻撃・侵害によって、重要なサービスを完全に停止する恐れがあります。

コンプライアンス違反

新たなサイバー規制が導入されるにつれ、太陽光発電所のオーナーは自社のシステムがコンプライアンスを遵守し、ネットワークが侵害された場合の製品回収や金銭的罰則のリスクを回避するために、積極的な対策を講じなければなりません。

太陽光発電システムに関する新たな規制が始まる

太陽光発電は重要なエネルギーインフラとなり、各国の規制機関から大きな注目を集めている。
このことは、今後予定されている新たな法規制の「潮流」にすでに現れはじめている。

UL 2941
スマートインバータと分散型エネルギー源のサイバーセキュリティに特化した国際規格(2025年予定)

The “U.S Cyber Trust Mark”
米国IoT製品のサイバーセキュリティ、ラベリングプログラム (2025年予定)

National Association of Regulatory Utility Commissions (NARUC/NASEO)
配電システムとDERのサイバーセキュリティ・ベースライン(2025年予定)

IEEE P1547.10
分散型エネルギー資源（DER）ゲートウェイプラットフォーム作業部会(継続中)

UK PSTI (2023)
製品セキュリティと電気通信インフラの英国の法案

RED 2014/53/EU
欧州無線機器指令

Cyber Resilience Act
IoTと接続機器のサイバーセキュリティに関するEU広域の法規制(2026-2027年予定)

NIS 2指令
EU全体で高水準のサイバーセキュリティを実現するためのEU広域指令(2024年10月発効)

ソーラーエッジ - 太陽光発電サイバーセキュリティのグローバルリーダー

ソーラーエッジは、何百万台ものIoTデバイスをグローバルに展開する太陽光発電業界のリーダーです。太陽光発電資産所有者が直面するサイバーセキュリティリスクやエネルギーグリッドへの脅威を認識する上で最適な立場にあります。

当社は太陽光発電の安全性に関して豊富な実績があり、米国内外で重要な太陽光発電の安全基準の確立に貢献してきました。そして、太陽光発電のサイバーセキュリティにおいても同様に取り組むことを目指しています。

お客様の安全保障をビジネスの中心に据える

当社は継続的なサイバー対策を指揮する専門家チームを招聘するため、多大な投資を行っています。

国際的なサイバー基準の策定を支援

当社は、様々な技術委員会に積極的に参加し、当社の製品設計が今後の規制に沿ったものとなるよう取り組んでいます。当社のデバイスは、最新のガイドラインとDERサイバーセキュリティ規格の基準に準拠しています。

サイバーセキュリティを最優先に開発されたソーラーエッジ製品

、ソーラーエッジのソフトウェアやハードウェアは、、製品設計のあらゆる段階で対策を講じ、日々進化するサイバー脅威からお客様を常に保護するよう努めております。

サイバーEDGEを最大限に活用

ソーラーエッジとの連携により、システム寿命期間を通じて防御力を強化することができます。サイバーセキュリティに対する当社の段階的なアプローチは、発電所の試運転の段階から電力の生産に至るまで、データの完全性、通信および業務運営を保護することを目的としています。

システムの接続性と機能性、顧客データを保護するために、ソーラーエッジはサイバーインフォームドエンジニアリング（CIE）の原則に従い、初期設計段階から情報セキュリティメカニズムを製品に組み混んでいます。進化し続ける需要や規制基準に沿うよう、継続的にソリューションを適応、強化しています。

当社は、お客様のセキュリティチームのニーズを最優先し、製品を安全に設計するだけでなく、最大限の可視性と制御性を確保できるよう設計しています。

エネルギーサブネットワークは、お客様の組織のITおよびOTネットワークと安全に統合されるために構成されたセキュリティです。

顧客情報タや電気使用量データが安全に転送・保存されることで、最大限にプライバシーを保護し、サイバー脅威から守ります。

ソーラーラーエッジ パワーコンディショナは、太陽光発電システムの要であり、他の当社機器とともに、太陽光発電システム全体のサイバー攻撃を防止および検出するように設計されています。

太陽光発電の安全性と同様、太陽光発電サイバーセキュリティにも妥協は許されません

ソーラーエッジをパートナーとして選択することで、サイバーリスクを最小限に抑え、進化し続ける脅威に対して、ビジネスを安全かつ堅牢なものにします。

ソーラーエッジについて

ソーラーエッジは、再生可能エネルギー技術のグローバルリーダーとして、世界トップレベルのエンジニアリングとイノベーションを駆使し、太陽光発電システムの発電および管理方法を革新するインテリジェントパワーコンディショナソリューションを開発しています。これにより、住宅、産業、公共施設向けに、エネルギーの発電、蓄電、管理、消費を最適化したソリューションを提供します。ーラーエッジが提供するDC最適化技術は、世界140カ国以上、数百万世帯に導入されており、フォーチュン100企業の50%以上の屋根上に設置されています。スマートエネルギーを推進し続けるソーラーエッジは、あらゆる場所でエネルギーを最適化する持続可能なエネルギーネットワークへの変革を加速しています。