

# 分散電源化の進展に伴い 急速に注目を集めるサイバーセキュリティ ～リスクと対策の両面で先進する米国の事例と日本企業への方策～

— 講師 —

クリーンエネルギー研究所 代表 阪口 幸雄 氏

日時 2025年3月5日(水) 午後2時～5時  
受講方法 会場受講／ライブ配信／アーカイブ配信(2週間、何度でもご視聴可)  
会場 SSK セミナールーム 東京都港区西新橋2-6-2 ザイマックス西新橋ビル4F

## [重点講義内容]

電力システムは現代社会を支える重要なインフラの一部であり、電力業界におけるサイバーセキュリティは極めて重要である。エネルギー部門への侵害は、停電、経済混乱、国家安全保障への脅威など、広範囲にわたる影響を及ぼす。

重要なインフラ電力システムは、交通、医療、製造などの他の部門を支えるため、重要なインフラとして分類されている。また、現代の電力システムは、スマートグリッド、モノのインターネット(IoT)デバイス、分散型エネルギー資源(DER)などの先進技術に依存しているが、それにより攻撃対象領域が拡大している。国家、サイバー犯罪者、ハクティビスト集団は、電力システムが戦略的に重要であることを理由に、そのシステムを標的にすることが多い。

米国では、2020年のSolarWinds攻撃、2021年のフロリダ州の水道会社へのハッキング等、ほぼ恒常的に攻撃が仕掛けられており、被害が出始めている。

ソーラーパネル、風力タービン、エネルギー貯蔵システム、電気自動車(EV)などの『分散型エネルギーリソース(DERs)』へのサイバー攻撃は、配電網がより分散化され相互接続されたシステムへと進化するにつれ、懸念が高まっている。標準化の欠如や、小規模な分散電源所有者が持つ低いサイバーセキュリティ意識が、攻撃を容易にしている。特に、インバーターは無防備なケースがほとんどである。

これらについて、リスクと対策の両面で先進の米国を研究することにより、日本はどうあるべきかを、米国在住40年のエネルギー問題の専門家が解説する。

1. 大型の電力施設および分散型エネルギーリソースの脆弱性
2. サイバー攻撃の種類
3. 攻撃による潜在的な影響
4. リスク軽減に向けた米国と日本の取り組み
  - (1) 政策および規制(米国と日本)
  - (2) テクノロジーとベストプラクティス
5. 事例研究と注目すべき事例(インシデント)
6. サイバーセキュリティ関連の標準化
  - (1) NIST Cybersecurity Framework
  - (2) NERC CIP Standards
  - (3) IEEE 1547-2018 / IEC 62443 / ISO/IEC 27001
  - (4) SunSpec Alliance
7. 継続中の課題
8. 提言と日本企業のビジネスチャンス
9. 質疑応答

※プログラムは最新状況に応じて変更する場合があります

