CASE STUDY

北米の電気協同組合が MSP 提供のセキュリティ ファブリックで IT / OT ネットワークを強化

人口の少ないテキサス州東部の 9 つの郡をカバーしている送電網は、5,000 マイル（約 8,000km）の送電線で 2 万 5,000 戸弱の組合員に電力を供給しており、国家が支援するハッカーやサイバー犯罪者が標的にするような公共事業とは思えません。

Shelby Vance 氏は、今後もそうであってほしいと願っています。ヒューストン郡電気協同組合（HCEC）の IT ディレクターである Vance 氏は、自分たちはサイバー脅威の影響を受けない、などという幻想は抱いていません。地域の電力供給協同組合である HCEC を所有しているのは、顧客である組合員たちです。「HCEC は、クレジットカード、社会保障番号、電話番号、住所、E メールアドレスなど、多くの攻撃者が欲しがる組合員データを保有しています。」と同氏は説明しています。

HCEC は、主に無人の変電所、スイッチ、SCADA（Supervisory Control And Data Acquisition：監視制御 / データ取得）システム、自動検針インフラ、分散型発電システム（太陽光発電など）で構成されるオペレーショナルテクノロジー（OT）ネットワークも維持しています。Vance 氏は次のように語っています。「世界中で基幹電力系統（BES）への攻撃が行われています。変電所設備に何者かが侵入し、電力を停止させるのではないか、という不安があります。HCEC のシステムが不正アクセスを受けた場合、組織と地域社会に壊滅的な影響がもたらされる可能性があります。私たちにとっての真の課題は、すべてのリソースを確実に保護することです。」

小さな電気事業者にのしかかるセキュリティの重荷

Vance 氏は、北米電力信頼度協議会が発行した重要インフラ保護（NERC CIP）標準で定められているベストプラクティスを参考に、HCEC のネットワークセキュリティの強化に着手しました。このイニシアチブには 2 つの大きな目標がありました。まず、HCEC のネットワークをセグメンテーションする必要がありました。

「HCEC のネットワークとインフラストラクチャはこれまで、セキュリティを考慮して設計されていませんでした。」と Vance 氏は語っています。「国土安全保障省と協力してネットワーク評価を行ったところ、HCEC のネットワークは非常にフラットであることがわかりました。そのため、簡単にネットワークを横断することができていました。」セグメンテーションの一環として、IT ネットワークと OT ネットワークの間にエアギャップを設け、IT 側で発生したセキュリティ侵害が OT システムに飛び火して送電網をダウンさせないようにしたいと Vance 氏は考えました。

次に、HCEC のセキュリティツールを最新のものにする必要がありました。「HCEC の設備はどれも耐用年数が過ぎているか、サポートを受けられなくなっていました。」と Vance 氏は説明しています。

HCEC
A Touchstone Energy® Cooperative

「フォーティネットの製品ライン、ソフトウェアおよびサポートに、SkyHelmのスキル、経験、専門知識、サービスを組み合わせることで、重要な電力インフラの保護、監視、保守を効率的かつコスト効率の高い方法で行うことができ、セキュリティ上大きなメリットがもたらされました。」

– ヒューストン郡電気協同組合（HCEC）ITディレクター Shelby Vance 氏

詳細

顧客：ヒューストン郡電気協同組合（HCEC）

フォーティネットのパートナー：SkyHelm Technology

業種：エネルギー / 公益事業

所在地：米国テキサス州クロケット

導入の効果

- HCEC で IT スタッフを増員することなくセキュリティ態勢を大幅に強化
- SkyHelm で、フォーティネット セキュリティ ファブリックの活用と、フォーティネットとのコラボレーションにより、サービス成長への確実なロードマップが実現

どちらも立派な目標ですが、達成するにはスタッフが必要です。Vance 氏は、新しいセキュリティ環境を組織内で管理するためには、現在の約 2 倍の IT スタッフが必要だと見積もりました。また、大都市圏がスキルギャップに直面しているのであれば、東テキサスの田舎でセキュリティ人材を確保するのがどれほど難しいかは想像に難くありません。Vance 氏自身、HCEC では PC サポート、サーバー管理、ネットワーキングインフラストラクチャ、計画と予算管理など多くの役割を担っています。HCEC のネットワークセキュリティを NERC CIP 標準に適合させることは、誰の助けも借りずに取り組めるタスクではありませんでした。Vance 氏は次のように説明しています。「私が求めていたのは、使いやすさ、管理のしやすさ、そしてネットワーク上で何が起こっているかを直ちに確認できることでした。何が起きているのかを把握するために一日中コンソールを見ている時間などありません。」

ソリューション

- FortiGate
- FortiSwitch
- FortiManager
- FortiAnalyzer
- FortiSIEM

「フォーティネットの製品群に興味を持った理由の一つは、当時使用していた複数の他社製品を機能強化したソリューションが1つのパッケージとして提供されることでした。そうすることで、HCECのネットワークから他のベンダー数社を排除することができました。」

– ヒューストン郡電気協同組合（HCEC）ITディレクター Shelby Vance 氏

多くの電気協同組合から頼りにされる MSP

Vance 氏は、同業者からの推薦に基づき、電力供給協同組合向けのサイバーセキュリティを専門とするマネージドサービスプロバイダー（MSP）である SkyHelm Technology 社に連絡を取りました。SkyHelm のサイバーセキュリティサービス「TITAN」は、フォーティネット セキュリティ ファブリックに大きく依存する包括的なソリューションです。TITAN には、オンプレミスのネットワークセキュリティと、FortiGate 次世代ファイアウォール（NGFW）や FortiSwitch Ethernet スイッチなどの LAN エッジテクノロジーが組み込まれています。SkyHelm では、米国を拠点とする 24 時間 365 日体制のセキュリティオペレーションセンター（SOC）から、FortiManager と FortiAnalyzer ソリューション（総称「ファブリック管理センター」）を使用して、セキュリティツールの構成と管理を行っています。TITAN は、FortiSIEM（セキュリティ情報 / イベント管理）を利用して、顧客に潜在的な脅威を警告し、迅速かつ効果的な対応を行っています。

SkyHelm の共同創業者で CTO の Jeremy Dreyer 氏は、「これらの製品に SkyHelm 独自の付加価値サービスをバンドルし、月額料金で当社のチームがすべて管理 / 監視します。」と説明しています。「小規模な電気協同組合の多くは、TITAN を利用することで、すべての機能を自社で構築するよりも、コスト効率に優れた方法でセキュリティ目標を達成できます。」

SkyHelm は、TITAN によって顧客の安全性が高まることを証明するために、NRECA（National Rural Electric Cooperative Association：全米地方電力協同組合）が最近開発した RC3（Rural Cooperative Cybersecurity Capabilities：地方協同組合サイバーセキュリティ能力）評価ツールを使用して、TITAN サービスの加入前と加入後の顧客のセキュリティ態勢を評価しています。Dreyer 氏は次のように述べています。「サービスに加入したお客様のセキュリティ態勢は、3 ～ 4 倍と大幅に改善されています。」

SkyHelm の高い専門性により、電気協同組合がセキュリティインフラストラクチャの計画と導入に費やす時間は大幅に短縮されます。SkyHelm のシニアソフトウェア開発者 Casey Davis 氏は次のように述べています。「SkyHelm はこれまで数多くの協同組合と仕事をした経験から、ファイアウォールのルールや検知プロファイル、アラートの設定など、すべてにおいて標準構成を推奨しています。また、これらのソリューションを実装する際には、協同組合向けにカスタマイズされたベストプラクティスに照らして適切な構成がなされていることを確認しています。」

TITAN が稼働を開始すると、顧客の施設にあるセキュリティデバイスからのすべてのログデータとアラートが SkyHelm の SOC に転送されます。また、SkyHelm はクライアントダッシュボードも開発し、Vance 氏のような協同組合の IT ディレクターが、注意を要する問題を一目で確認できるようにしました。

セキュリティを強化しながら、負荷を軽減

これこそ、Vance 氏が求めていた管理面での安心感でした。同氏は次のように述べています。「SkyHelm とのマネージドサービスプロバイダー契約のおかげで、ハイエンドの NOC（ネットワークオペレーションセンター）や SOC を独自に導入することなく利用できるようになりました。私の仕事は、日々アラートを追跡して何が起きているのかを把握するといった細かい作業から、プロジェクト管理へと変わりました。今では SkyHelm があらかじめ評価を行い、問題があれば私に知らせてくれます。また、私が気になったことがあれば、SkyHelm のチームに連絡を取ると、10 分から 20 分後には答えが返ってきます。そのおかげで、私はより大局的に課題に集中できるようになりました。」

現在、テキサス州クロケットにある HCEC の本部には、FortiGate ファイアウォールと FortiSwitch Ethernet スイッチが導入されています。今後は、変電所にも FortiGate ファイアウォールを導入して、大手ネットワーキングベンダーのレガシーシステムを置き換える計画です。Vance 氏は次のように述べています。「フォーティネットの製品群に興味を持った理由の 1 つは、当時使用していた複数の他社製品を機能強化したソリューションが 1 つのパッケージとして提供されることでした。これにより、HCEC のネットワークから他のベンダー数社を排除することができました。」

セキュリティ ファブリックを活用して包括的なサービスを提供

SkyHelm は、2014 年からフォーティネットのソリューションを自社のサービスに取り入れています。Dreyer 氏は次のように述べています。「SkyHelm は、多くのベンダーと比較してフォーティネットを高く評価しました。結果、フォーティネットは最適なテクノロジーを適切な価格で提供していることが明らかになりました。FortiGate と FortiSwitch は当社のお客様に最適なソリューションであり、それに加えて FortiSIEM などの他のソリューションも提供してきました。また、近日中に FortiEDR（エンドポイントの脅威検知と対応）を追加する予定です。他にも、FortiNAC（ネットワークアクセスコントロール）や FortiAuthenticator（ユーザー認証）など、当社が販売 / 提供しているフォーティネット製品がありますが、これらも近いうちに TITAN に統合する予定です。」

HCEC では、古くなったネットワーク / セキュリティ製品を FortiGate と FortiSwitch の統合ソリューションに置き換えたことで、IT と OT の両ネットワークのセキュリティ、信頼性、効率性が大幅に改善されました。FortiSwitch が FortiLink を介して FortiGate NGFW に直接統合されたことで、直接制御の構成と管理、および FortiGate のポートと同レベルの検査が可能となっています。HCEC における導入後の RC3 評価は現在も進行中ですが、SkyHelm は他の電気協同組合の顧客と同様の改善が見られると期待しています。

> *「SkyHelmは、多くのベンダーと比較してフォーティネットを高く評価しました。結果、フォーティネットは最適なテクノロジーを適切な価格で提供していることが明らかになりました。」*
>
> *– SkyHelm Technology 社*
> *共同創業者兼CTO*
> *Jeremy Dreyer 氏*

しかし、Davis 氏によれば、製品パフォーマンスの利点は語られるべき話の半分に過ぎません。「フォーティネットを選んだ大きな理由は、セキュリティ ファブリックのパワーです。」と同氏は述べています。「他の製品を統合することもできますが、すぐに統合可能な製品があるというのは非常に大きな利点です。FortiGate ファイアウォールと FortiSIEM を組み合わせれば、フォーティネットが両製品に搭載したテクノロジーによって、SCADA システムで起きていることを正確に把握できます。つまり、SCADA システムだけでなく、FortiGate ファイアウォールの監視対象すべてのセキュリティ管理を簡素化することができるのです。」

Davis 氏は、セキュリティ ファブリックがもたらすメリットが MSP の運用面にも及んでいると考えています。同氏は次のように述べています。「全顧客のセキュリティハードウェアの管理に要する時間が短縮され、起こっていることの全体像を容易に把握できるため、より迅速に脅威を確認して対応できます。また、フォーティネットと協力して、電気協同組合向けのベストプラクティスを共同開発しています。この共同開発にフォーティネットは大きな投資をしてきました。」

地方の協同組合の先駆者として

今のところ、NERC CIP 標準への準拠を証明する書類を提出する義務があるのは、投資家が所有する電力会社や自治体の公益事業など、米国の大手電気事業者に限られています。小規模な電力供給協同組合の準拠については、現時点では任意です。しかし、世界各地に脅威が広がる中、小規模な事業者であっても、近い将来同じベストプラクティスに従わなければならなくなります。Vance 氏の熱心な取り組みにより、HCEC は今後 10 年以内に浸透するであろう基準を先取りしています。

同氏の取り組みはそれだけでは終わりません。「私は今、無線インフラストラクチャのすべてを FortiAP ワイヤレスアクセスポイントに移行することを検討しています。なぜなら、FortiLink と同様の統合と自動化が可能だからです。フォーティネットの製品ライン、ソフトウェア、サポートに、SkyHelm のスキル、経験、専門知識、サービスを組み合わせることで、重要な電力インフラの保護、監視、保守を効率的かつコスト効果の高い方法で行うことができ、セキュリティ上大きなメリットがもたらされています。」

フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

CS-Houston-County-Electric-Cooperative-202105-R1