Deloitte.
Insights

特集

電力業界のサイバーリスク経営

サプライチェーンと制御システムに対する脅威の高まり

Steve Livingston、Suzanna Sanborn、Andrew Slaughter、Paul Zonneveld

電力業界は、サイバー攻撃の脅威に絶えずさらされており、米国においては最初にサイバー脅威に対する強制的な規制を導入した業界でもあります。しかし、脅威がさらに進化しその影響が制御システム（ICS）とサプライチェーンに及びつつあることから、さらなるリスク管理の必要性に迫られています。

発電所と企業や家庭を結ぶ送配電網は、世界各国、とりわけ先進国で、最も重要なインフラのひとつと見なされています。同時にこれらの送配電網は、絶えずサイバー攻撃の標的とされており、電力業界のみならず、社会全体に影響を及ぼす可能性があります[1]。

世界中の多くの国々にとり、電力インフラは社会が機能するうえで欠かせない重要インフラです。米国政府は、「送配電網が機能停止したり破壊されたりすれば、国の安全保障、経済保障、および国民の公衆衛生と国民の安全を脅かす影響がある」として、エネルギー分野を極めて重要な16のインフラセクターのひとつに分類しています[2]。特に電力分野は、すべての重要インフラセクターを「稼動させる機能」を提供していることから、非常に重要とされています[3]。広域にわたり、長期間の停電が発生すれば、金融、通信、交通、上下水道をはじめ、電力依存度の高いシステムが深刻な打撃を被り、人々は移動や通信手段を失い暗闇に取り残されることとなります。要するに、社会全体の弱点といえます。

本書は、電力業界におけるサイバーリスクが増大する原因を見極め、進化する脅威と攻撃者、および脆弱性について概説するとともに、電力業界の脆弱性のひとつのうち、最も課題が多いサプライチェーンに対するサイバーリスクについて考察します。さらに、サイバーサプライチェーンにどのような性質のリスクがあるかを検討したうえで、最近の電力業界のサプライチェーンで発生したサイバー攻撃と影響、これらのリスクに対処するための課題について説明します。そして最後に、電力会社がサプライチェーン全体にわたるサイバーリスクを管理するために取るべきステップを解説していきます。

世界中の多くの国々にとり、電力インフラは社会が機能するうえで欠かせない重要インフラです。

「から騒ぎ」ではない：増加する電力業界のサイバーリスク

エネルギー業界は、米国でサイバー攻撃を受けた件数が多い3つの業界のひとつです。エネルギー業界が報告したインシデントは2016年だけで59件と重要インフラ業界合計290件の20%を占めました[4]。インシデント報告件数がエネルギー業界よりも多かったのは重要製造業と通信の2業界のみでした。これは米国だけの傾向ではありません。エネルギー業界は、ヨーロッパや日本でも主な標的のひとつです。またオーストラリアでは、重要インフラに関するインシデントおよびニア・インシデントの報告件数が最も多い業界とされました[5]。さらに、各電力会社は侵入の試みが絶え間なく行われ、そのほとんどは失敗に終わっているものの、攻撃そのものは活発化していることを報告しています。米国エネルギー省（DoE）のリック・ペリー長官は、この種の侵入が「1日数十万件という単位で発生している」と述べています[6]。また、2018年には、北米の電力系統を標的としたサイバー攻撃が「急増」したとされています[7]。

問題は攻撃の増加だけではありません。サイバーセキュリティの専門家や情報機関の関係者によると、サイバー攻撃者の数が増加し、その攻撃能力も向上しています[8]。ヒューマンエラーのほか、不満を抱えた社員や契約社員などの内部的な脅威は一般に最もよくある脅威です。しかし、国家組織や組織犯罪も活発化しており、不穏なことに、これらの関係者が連携している可能性もあります[9]。国家組織の関係者は、組織犯罪グループと契約することで自らの関与を否定しているというのが一部の見方です[10]。また、組織的な知識や技術的な知識をほとんど持たないハッカーですら、通常のインターネットとは異なる運営がされているダークウェブを介し高度なツールにアクセスするようになっていることが、問題をさらに悪化させています。図1は、米国の電力系統に脅威をもたらしうる各種

の攻撃者と、影響の深刻さを示しています。この脅威のプロファイルは、通常、時間の経過や国ごとに変わります。

電力業界で最も多発している攻撃手法のひとつがフィッシングです。メールを糸口とする攻撃で、受信者にリンクをクリックするよう働きかけ、クリックするとその受信者が使っているシステムにマルウェアを送り込む手口、あるいは受信者に個人データを入力するよう働きかけ、ネットワークへのアクセスを不正に入手する手口などがあります。2017年に米国の電力情報共有・分析センター（E-ISAC）がホームページで開示した226件のサイバー報告のうち、30%以上がフィッシングによるものです[11]。他の攻撃手法には、ウォータリングホール攻撃（水飲み場型攻撃）、認証情報窃取マルウェア、DoS攻撃、リモートアクセス型トロイの木馬などがあります。

攻撃者は制御システムとサードパーティを標的に

電力会社は、何年も前からサイバーリスクを認識してきました。米国においては、2007年に北米電力信頼度協議会（NERC）による重要インフラ保護（CIP）基準を制定し、サイバーセキュリティ管理を義務付けることで、サイバーリスクに最初に対処した業界のひとつとなりました。それにもかかわらず、脅威は進化を続けています。 攻撃者は制御システム（ICS）を主な標的とし、電力業界のサプライチェーンにおけるサードパーティを介しICSへのアクセスを企てるようになりました。

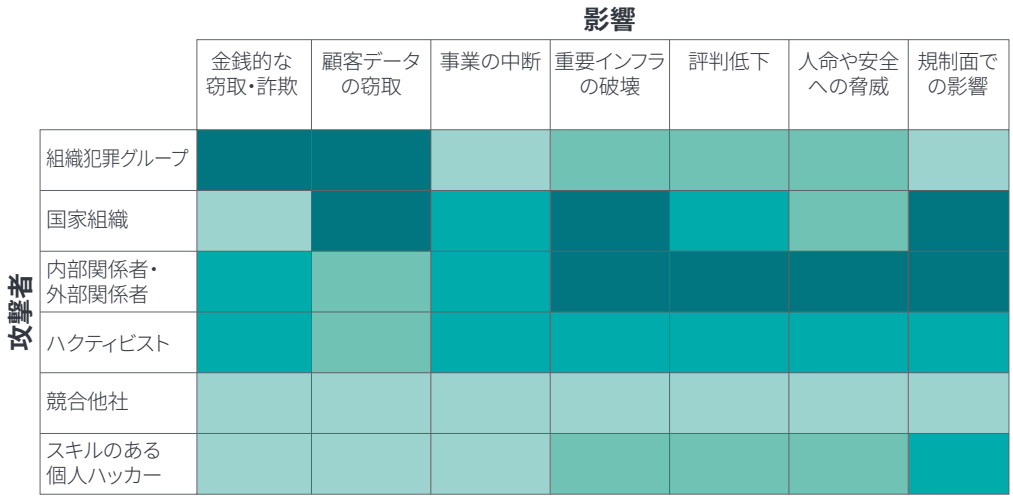
サイバー攻撃か物理攻撃かを曖昧にする制御システム（ICS）の標的化

もうひとつの気がかりな傾向が、ICSを標的としたサイバー攻撃の増加です。この種の攻撃は、電力系統に物理的な危害を加えるための下準備である可能性があります。これまで、攻撃者は主に電力会社のITシステムを標的とし、データの窃取や金銭的利益を目的としたランサムウェアを用いていました。しかし、最近では国家組織や組織化された犯罪に関係するハッカーが電力会社のICSに侵入しようとした例が複数報告され、脅威がより深刻化していま

図1

米国の電力業界におけるサイバー脅威のプロファイル：最も危険な3大攻撃者

■ 非常に高い ■ 高 ■ 中 ■ 低



出所：デロイトの分析より

す。攻撃者はシステムの操作方法を学ぶことで、発電所、変電所、送配電網などの物理的な重要資産を制御できるようになり、電力供給の遮断や資産の破壊を目標においていると見られています。

過去10年以上に渡り発達してきたICSが標的になることは、サイバー攻撃と物理攻撃の境界を曖昧にし、多くの国で国家安全保障の懸念を生じさせています。ICSへの攻撃は、世界的にその範囲と目的の両面で進展が見られています（図2）。攻撃者は、ShodanやMetasploitなど正当な目的で開発されたソフトウェアを悪用し、インターネットに接続されたコンポーネントやデバイスを見つけます。そして、監視制御システム（SCADA）やその他のICSソフトウェアに攻撃を仕掛けます。これらの攻撃はすべて政治的な目的を達成しようとする国家組織により実行またはサポートされているか、その疑いがある共通点があります。そして、こうした活動が増えつつあると見られています。2017年にICSへの妨害を目標とした攻撃では、TrisisやTritonと呼ばれるウイルスが、サウジアラビアの石油化学工場の安全計装システムに侵入しました。調査によれば、この攻撃は、コンピュータのコードのバグのために失敗に終

図2

2009年以降におけるICSへのソフトウェアとマルウェアによる攻撃の系譜

出所：デロイトの分析より;Hank Kenchington著「DOE strategy for energy sector cybersecurity」（エネルギーセクターのサイバーセキュリティに対するエネルギー省の戦略）、米国エネルギー省、2018年9月14日、p. 7;ニュース報道。

わりましたが、死傷者が生じる可能性のある施設の爆発を意図したものであったことが分かりました[12]。

世界各国の送配電網に対する脅威の高まりの背景は、送配電網の近代化により、潜在的なサイバーの脆弱性が増加していることにあります。送配電網のデジタル化や近代化は、無限のメリットをもたらす一方で、電力会社への攻撃対象、すなわちハッカーがシステムに侵入する経路を増やしかねません。情報通信技術とネットワークにつながった組込機器で送配電網が「スマート」になるにつれて、システムはますます複雑化し、アクセスポイントの数が増えていきます。さらに、一般的なソフトウェアや情報技術をオペレーションに導入することで、攻撃者にとってシステムへのアクセスが容易になります。また、機能の自動化が進むにつれ、攻撃による影響が拡大する可能性があります。まとめると、これらのすべての要因が、脆弱性の高まりを引き起こしています。

「鎖の強度は最も弱い環で決まる」：サイバーサプライチェーンのリスク

これまで、電力会社はサイバーリスクをITシステムかOTシステムのいずれかで脆弱性を考慮していました。ITシステムとは、データや他の情報を処理するソフトウェアやハードウェアなどの技術、OTシステムとは、ICSを含む物理的なデバイス、資産、プロセスを監視制御するソフトウェアやハードウェアなどの技術です。しかし、近年、この2つのシステムは「スマートグリッド」を含む電力業界版IoTやデジタル化により融合してきています。電力会社にとって、自社の重要な資産の特定・防護は、それだけでも困難ですが、すべてが互いに絡み合う今日の世界では、巨大かつ広範なグローバルサプライチェーンの安全確保が求められています。

電力会社は、世界中の業者から、情報、ハードウェア、ソフトウェア、サービスなどを購入しているため、関係者が故意の有無を問わず、システムのライフサイクルのあらゆるポイントで危殆化されたコンポーネントをシステムに持ち込むことができます。それは頻繁にダウンロードされるソフトウェアアップデートや「パッチ」を通じて、あるいは悪意のあるコードを埋め込んでおき、後日、適用されるファームウェアを通じて行われることもあります。また、電力会社がOTシステムに設置するハードウェアにも侵害することができます[13]。

2017年にサウジアラビアの石油化学プラントで生じた攻撃（図2）では、世界中の約18,000の製造プラントで使用されているブランドの制御装置を通じTrisis／Tritonと呼ばれるウイルスが遠隔から侵入し、死傷者の出る爆発事故が引き起こされるおそれが生じました[14]。この制御装置は核施設、水処理施設、精製所および化学プラントで、電圧、圧力および温度を制御するなどの安全機能を確保します。このウイルスは、プラントの機能を破壊させるためのものでした。このマルウェアのスケーラビリティはそれほど高くありませんが、攻撃の手法は、世界中の他の場所で同様の機器を破壊させようとする者たちにヒントを与えると、調査担当者らは示唆しています[15]。

この脅威をさらに分析するため、サプライチェーンから発生し、電力業界に影響を及ぼした最近のサイバー攻撃の3つの事例を検証しました（図3）。3事例うち2つはICSを標的とした攻撃で、もう1つはITシステムに対する攻撃です。驚いたことに、いずれの3つの攻撃も、金銭的利益目的ではなく、ICSの直近または将来の潜在的な破壊を目的としているようです。

サプライチェーンの関係者は、故意の有無に関わらず、システムライフサイクルのあらゆるポイントで、危殆化されたコンポーネントをシステムへ導入できます

電力に関わる企業は、サプライチェーンのサイバーリスク対策に多くの課題を抱えています。第一に、サイバーサプライチェーンの説明責任と管理責任は通常、社内で明確に定義された組織や部門、契約先の範疇に収まることはなく、供給と調達、情報セキュリティ、クラウド、インフラ、法務、IT、OTなどの様々な部署に影響を与える可能性があります。ほとんどの最高情報セキュリティ責任者（CISO）はサプライチェーンの管理権限を有しておらず、サプライチェーンのサイバーリスク分析に関与できない可能性もあります。サイバーサプライチェーンのリスクを低減するには、オーナーシップと説明責任の明確化が必須となります。

第二に、事業者においてはシステム環境を自社からクラウドに移行するプロジェクトが多く見受けられます。クラウドに移行する際に、運用を移行することに目を奪われがちとなり、クラウドプロバイダーがセキュアかどうかの検討が十分に行われていないことがあります。しかし、多くの場合、サプライヤのリスク管理プロセスと、そのプロセスが自社の業務に与える影響を十分に見通せていません[28]。十分に時間をとれば、サイバー攻撃の潜在的な影響を分析し、回復力のあるソリューションをマッピング、計

図3

サプライチェーンを通じ電力業界に脅威をもたらした3件のサイバー攻撃

攻撃
ハッカーが電力会社の複数のサプライチェーンパートナーを介し、米国および他の国々の電力会社のICSに侵入した（2016～2017年）。

攻撃者／犯人
Dragonfly、別名：Energetic Bear[16]

手法
- 攻撃者は、よく訪れる業界のウェブサイト（水飲み場）の改ざんにより悪意のあるコンテンツを拡散し、訪問者の認証情報（パスワード）を収集した。その後、信頼関係のある協力会社に対して攻撃を仕掛けた。
- 最終的には、攻撃者はITサービスプロバイダと事業者の企業ITネットワークへのアクセスが可能になり、ICSのファイアウォール突破に役立つ文書を探し出した[17]。

被害
- 米国、トルコ、スイスの数百もの公益企業と他産業の施設のICSにアクセスがあった[18]。
- 偵察が行われ、制御システムの設計、機能、脆弱性が評価された[19]。
- 設定情報とインターフェース画面をコピーされた。

考察
- Dragonflyが国家組織の手先として、標的型攻撃による情報収集を行うとともに、将来の攻撃のための土台を築いていた可能性がある。
- 国の安全保障の専門家は、これらの侵入と影響を深刻に懸念している[20]。

攻撃
小規模なクラウドサービスプロバイダへの攻撃により、米国の天然ガス、石油、電力業界に影響を及ぼした（2018年4月）[21]。

攻撃者／犯人
不明または非開示

手法
- 手法は開示されていないが、アナリストは、攻撃者が会社のコンピュータをフリーズさせ、ファイルの暗号を解読するための鍵と引き換えに支払いを要求するランサムウェアの可能性を指摘している[22]。

被害
- 少なくとも5社の天然ガスパイプラインの通信が遮断され、ガス供給のトラッキングとスケジューリングが滞った[23]。
- 一部の大手電力供給会社における電力取引用価格決定モデルと需要予測モデルの提供プラットフォームとの連携が停止したことにより、概算の請求書しか発行できなかった。
- 一部のプロバイダは請求書の発行が遅れ、顧客向けのための電力購入量を過小または過大に見積もられるリスクがあった。

考察
- ガスおよび電力の供給に支障はきたさなかったが、2つの業界間の相互依存関係とサプライチェーンへの攻撃による広範囲な障害に対する脆弱性が明らかになった。
- サイバー攻撃によってサプライチェーンに問題が生じた場合の計画と準備の重要性が浮き彫りになった。
- この種の電子データ交換（EDI）システムでは、侵入者はITシステムからICSへと乗り移ることができる[24]。

攻撃	攻撃者／犯人
NotPetya攻撃は、多数の部門の業務運営に支障をきたし、全世界で少なくとも100億米ドル以上の損害を被った（2017年春）[25]。	国家組織が支援する集団

手法

- 攻撃者は、ウクライナの会計ソフトウェアプロバイダのサーバーに侵入し、更新版として不正なソフトウェアを世界中のクライアントに配信した。このソフトウェアに含まれるマルウェアは、ファイルを暗号化してランサムウェアを模倣したが、身代金の要求をしなかった。

被害

- 攻撃により少なくとも6社の現地電力会社が感染し、いくつかの大手グローバル企業のウクライナ支社にも感染が及んだ。
- 感染は世界中に広まり、海運、製薬、建設、消費財などの事業運営に支障をきたした。
- 港湾ではトラックが滞り、倉庫に積み上げられた商品、重要なワクチンの供給に支障をきたした。
- 被害額は少なくとも100億米ドル（約1兆円）に達した[26]。

考察

- これは初めて世界規模でのサプライチェーンに加えられた攻撃であり、このような攻撃による破壊力を示すものとなった。同様の攻撃が起きれば、同等かそれ以上の被害が出ることがある。
- 攻撃者は、被害が世界中に及ぶことすら厭わなかったという点で、新たな攻撃のモデルを示した。本来の標的ではない企業も、被害を免れない可能性がある。
- この攻撃は、国家組織による非常に悪質なサイバー戦争の武器使用例と言える[27]。公益企業やその他の企業は、このような攻撃に対する脆弱性を評価し、攻撃への対処を検討しなければならない。

出所：デロイトの分析より

画、構築することができます。これは、運用をクラウドに移行する前に行う必要があります。特に、運転データとエネルギー管理システムは、ハッキングされた場合に信頼性に影響を及ぼすことに留意すべきです。

上記以外によく起こる課題は、評価すべき膨大な数のサプライヤに対応するマンパワーが不足していることがあげられます。北米の20社の電力およびガス会社の調査によると、現状取引のあるサプライヤが平均3,647社、戦略的提携関係にあるパートナーが平均39社あり、対外支出総計の80%は140社のサプライヤで占められていました[29]。企業は一部のサプライヤにアクセスできない可能性があります。またセキュリティのルールを取り入れることができない、あるいはその意思がないサプライヤの可能性もあります。さらに、潜在的なサイバー脅威の中には、サプライチェーンのファームウェアアップデートのように、通常業務として行われるため、侵入のリスクが見逃されてしまうものもあります。現時点では、ほとんどの電力会社は、サプライヤの行為をほとんど管理できていません。ようやくサプライヤに注意を払い、説明責任を求め、インテグリティを要求するようになったばかりです。

とは言え、諦めることはありません。特にサプライチェーンにおいて、企業がサイバーリスクに取組むことのできるステップがいくつかあります。

全社とサプライチェーンすべてにわたるサイバーリスクの管理：今後のステップ

全社にわたるサイバーリスク低減のための検討として、最初のステップでは、資産とその接続先を識別してマッピングし、重要度による優先順位付けを行います。次に、重要な資産（システムと設備）とネットワークに既知の脆弱性があるか、また、悪用され得るかどうかを判断します。例えば、脆弱性にはインターネット検索で入手できるハードコーディングされた初期パスワードを使用した制御システムがあります。3番目のステップでは、予防として脅威を管理するために、制御システムのサイバーセキュリティ成熟度を評価します。これには、デロイトのサイバーセキュリティ成熟度モデルをはじめ、確立したモデルを使うことが有益です[30]。最後のステップは、人、プロセスおよびテクノロジーを活用して、重

要な資産の予防、発見、回復を高めるためのフレームワークを構築します（図4）。

サプライチェーンのサイバーリスク管理

電力会社のサプライチェーンに含まれるサイバーリスクを管理するには、資材調達部門に働きかけることから始めます。全員を一堂に会し部門横断的なサイバーリスク管理の在り方を検討することが有効です。調達ガイドラインを用い、サプライヤの評価やサイバーセキュリティにおける与信情報（リスクインテリジェンス）を入手します。最初は取引規模の大きなベンダーに注力し、取引のないベンダーは後回しにします。また、事業分析を行い、攻撃によりビジネス影響が生じた場合に備えた復旧計画を立案します。

調達実務の改善

新しいサプライヤとの取引を検討する際の審査では、そのサプライヤの成熟度、およびネットワークに接続する製品やサービスのセキュリティ対策状況を理解することが重要です。企業はベンダーのリスク評価およびサイバーセキュリティにおける与信情報の継続的な入手を自社で実施するか、あるいは専門のサイバーセキュリティ会社やコンサルタントを介して実施します。

具体的には、サプライヤのプロセスがセキュリティ

図4

サイバーセキュリティ成熟度を高めるための予防、発見、回復のフレームワーク

	人	プロセス	テクノロジー
予防 (Secure)	悪意ある関係者をスクリーニングするなどして、従業員とベンダーの**サイバーリスクの潜在性**を評価する。 サプライチェーン調達部門を参加させ、サプライヤが適切なセキュリティ対策を講じていることを確認する。 サプライヤの数を減らす。	制御システムや他の高リスクのサイバーおよび物理インターフェースに対するアクセスを**制限し文書化**する。 デフォルトのパスワードではなく、独自のシステムパスワードを使用する。 通常業務（例：ベンダーのファームウェアアップデートなど）におけるリスクの見逃しを精査・管理する。	エアギャップ、または**プラントレベルのIoTインフラ**を含む高いリスクのプロセスを事務ネットワークから分離する。 ソフトウェアの出所を追跡するためにソフトウェア「BOM（部品表）」管理を要求するか、またはブロックチェーンを使用し製品のライフサイクル全体を追跡する。
発見 (Vigilant)	**機密システム**に直接携わる従業員だけでなく、すべての従業員にセキュリティ意識向上トレーニングを実施する。 信頼できるサプライヤのセキュリティにおける与信情報（リスクインテリジェンス）を継続的に入手する。	**優先順位付けの手順**を策定し、サプライチェーンパートナーへ起こり得るサイバーインシデントを特定と、リスクの重要度を評価する。	**自動監視ソフトウェア**を導入し、潜在的な違反や機器の操作ミスや障害を特定する。 製品の導入後も、ベンダーのセキュリティ管理状況を継続的に知っておく。
回復 (Resilient)	影響を削減し、将来の侵入を予防するため、ITとOTの主な担当者を対象に、インシデント対応プロセスを整備・文書化し、**フォレンジックのトレーニングプログラム**を開発する。 主なサプライヤおよびパートナーとの訓練に参加する。	**変更管理の対象**を拡大し、組織変更および事業戦略の変更におけるサイバーセキュリティへの影響を対象に含める。 主なサプライチェーンパートナーに対する攻撃に備える。	物理的な機器のサイバー／物理インターフェースの二重化、ソフトウェアのバックアップなどにより、主要プロセスに**冗長性を確立する。** 主要なサプライヤが攻撃された場合に備え、互換性の技術を提供している代替サプライヤを特定する。

注：予防、発見、回復のフレームワークの詳細は、Andrew Slaughter、Paul Zonneveld、「An integrated approach to combat cyber risk: Securing industrial operations in oil and gas」（サイバーリスクに対する包括的アプローチ：石油・ガス業界における安全操業のあり方とは）、Deloitte、2017年5月、p. 9ご覧ください。
出所：デロイトの分析より

手順に従っているかどうかに焦点を当て、導入や販売された製品やサービスの安全性を確認する取組みを行います。このような取組みには、脅威インテリジェンス、パッチおよび脆弱性管理などがあります。製品の調達の際には、製品ベンダーの社内プロセスにおいて製品やサービスの設計にセキュリティが抜け落ちていないかを確認する仕組みの有無に着目します。例えば、企業はサプライヤにサイバーセキュリティのチェックシートへの回答を求め、セキュリティリスク評価の実施を示す証拠提示を求めることもできます。

電力会社がサイバーセキュリティを調達プロセスに組入れる際の参考として、以下の実例があります。

- **製品の優先順位を付けるための判断基準を確立します。**例えば、製品やサービスの信頼性や導入規模の大きさが優先度の判断基準となります。
- **調達に先立ち収集すべき情報のリストを作成し、その情報の評価を行います。**評価は、単純な属性ベースのチェックリストから、個別のニーズやセキュリティ方針に基づく総合的なコントロールベースの評価まで多岐にわたる評価が存在します。
- **資材調達部門や営業部門から、サービスプロバイダに対して交渉を開始します。**製品メーカーやサービスプロバイダは、資材調達部門から最初に話を持ちかけたほうが、協力的に対応していただける可能性が高くなります。
- **適切なスタッフの関与とプロセスオーナーを確認します。**製品メーカーとサービスプロバイダに関連する領域の専門家（エンジニアなど）が関与することで、知見に基づいた意見が得られます。
- **プロセスの統合、自動化、ツール化、スケール化により効率を高めます。**組織の賛同を得ること、組織横断でコラボレーションすること、ツールを用いること、学習効率を高めることにより、サイバーセキュリティを調達プロセスへ組入れる際のコストと時間が大幅に削減されます。

このほかにも、電力会社が調達のセキュリティレベルを向上させるために実践できることは多数あります。多くの企業は、ソフトウェアBOM（部品表）の作成やサプライチェーン全体のシステムのソフトウェアコンポーネントを逐一把握分析し、潜在的な問題点を明らかにする取組みを行っています。このような調達ガイドラインは、一般に使われている商用、オープンソースおよびサードパーティのソフトウェアコンポーネントを開示し、さらに一般に入手できるデータベースにリスト化されている欠陥がある場合はそれらもすべて開示するよう要求することが含まれます[31]。

同業他社や政府機関との協力

サプライチェーンと自社の両方のサイバーリスク管理をさらに強化するには、個々の企業の努力を超える取組みも検討すべきです。これは、脅威の情報を同業他社や政府機関と交換し、新しい技術や革新的なプロセスをテストする業界標準や認証プログラムの策定に貢献することを意味します。

標準や認証プログラムの策定に貢献する

電力業界のサイバーリスクを地方、国、地域、さらにはグローバルで低減するためには、取組んでいる業界他社や政府機関との協力が求められます。具体的には、国内外の標準化の取組みへの参加や、グローバル規模でのサイバーリスクの低減を目指す共通フレームワーク策定の活動への参加、業界他社や政府機関と連携した脅威や脆弱性についての情報交換のほか、地域、国、およびグローバルなサイバーセキュリティの演習―例えば、北米電力信頼度協議会（NERC）のGridExや電力インフラセキュリティ（EIS）評議会の多国間演習EarthExなど―への参加が挙げられます[32]。また、常に開発中のサイバーリスク管理技術やプロセスへの情報収集を行うことが重要です。

新しいサプライヤとの取引を検討する際の審査では、そのサプライヤの成熟度、およびネットワークに接続する製品やサービスのセキュリティ対策状況を理解することが重要です。

グローバルな標準化策定の動きに貢献するには、国際計測制御学会（ISA）や複数の業界を対象とした産業用オートメーション・制御システム（IACS）のためのサイバーセキュリティ標準としてIEC 62443シリーズを策定した国際電気標準会議（IEC）に

参加します[33]。多くのITシステムでは、さまざまなソフトウェアを使うことができますが、OTのデバイスやシステムは、他のソフトウェアシステムと互換性がないため、一般に受け入れられているOT標準のセットが開発されています。これらの標準は、SCADA、ネットワーク化された電子センシング、監視・診断システムなどのハードウェアとソフトウェアに適用されるほか、それに関連するヒューマンインターフェース、ネットワークインターフェース、マシンインターフェースにも適用されます[34]。

また、別の選択肢として、重要なハードウェア、ソフトウェア、ネットワークをサイバー脅威から保護するための包括的なフレームワーク策定の取組みに参加することです。例えばSiemens社は、ミュンヘンセキュリティカンファレンスや官民の他のパートナー（AES社やEnel社などのグローバルな電力会社）と手を組んで、「信頼性憲章（Charter of Trust）」イニシアチブを立ち上げました[36]。このイニシアチブは、拘束力のある規則と標準を策定して、サイバーセキュリティを強化し、デジタル化を進めることを目的としています。ビジネスパートナーや同業者のパートナーに対し、ネットワークアクセスに関してより堅牢な認証手順を使用し、暗号化とファイアウォールの使用を拡大し、継続的な監視とウイルス対策の実施、さらにIEC 62443をはじめとする国際標準の使用を促します[37]。

さらに、いくつかの認証に関する動きも、進行中です。例えば、サイバー製品国際認証（CPIC）委員会は、ハードウェアおよびソフトウェア製品を認証し、継続的な検証プロセスを提供するため、業界主導の中央集権的な仕組みを創設しようとしています[38]。ほかには、欧州ネットワーク情報セキュリティ機関（ENISA）は、情報・通信技術セキュリティのための認証フレームワークを策定しています[39]。現在、国際標準化機構（ISO）や国際電気標準会議（IEC）などの組織は、ITおよびIACSの製品とプロセスのための標準と認証をグローバルに提供しており、加えてサイバーセキュリティ関連の標準も策定中です。さらに他の多くのイニシアチブの中でもEaton社は、安全性の認証とコンサルティングを手がける非営利の認証機関（Underwriters Laboratories（UL））と協力し、ネットワークに接続された電力管理の製品やシステムのサイバーセキュリティ標準を開発しています[40]。

どのサイバーセキュリティフレームワークや認証制度が採用されるかにかかわらず、企業が求めているのは、コンプライアンスを怠ってでも競争力を得ようとするインセンティブを回避するために、世界中の同業他社がそれを講じる状況、もしくは義務付けられる状況です。究極的にこの種の努力が奏功するには、顧客がサイバーセキュリティの価値を理解し、その対価を支払う必要がなければなりません。電力系統の安全コストを確保しないと、結局高くつく可能性があります。

電力業界でのサプライチェーンを含むサイバーリスクの低減のための義務付け

北米電力信頼度協議会（NERC）が策定した重要インフラ保護（CIP）基準は、サイバーリスクに対応するための規制を確立したという点で、他の業界に先立つ先進的な事例となりました。2007年、NERC-CIP基準は大規模電力システム（BES）の保有者、運営者、利用者を対象とした法的な規制となりました。また、NERCは2018年に新しい基準（NERC-CIP 013）を追加し、これまでの2つの基準を改正し、サイバーサプライチェーンのリスクへ対処しました。しかし、NREC-CIP基準は、影響度が高から中レベルのBES事業体や電力会社のみを対象としており、そのサプライヤとベンダー、および影響度が低い事業体は含まれていません。基準に適応しない場合では、システムや資産が潜在的なリスクにさらされます[35]。

脅威情報を同業他社や政府機関と交換する

電力系統に対するサイバー脅威と物理的な脅威と脆弱性に関する情報を交換するための協力を行います。多くの国が情報共有・分析センター（ISAC）と呼ばれる機関を設置しています。米国では、北米電力信頼度協議会（NERC）が管理する電力情報共有・分析センター（E-ISAC）がそのひとつです。E-ISACは、データの収集・分析・共有、インシデント管理の調整およびリスクの低減戦略を共有・連携することにより、業界の対応力を高めようとしています。また、E-ISACはエネルギー業界のパートナーと協力することで脅威情報の共有と重要インフラの保護に役立つツールの開発を行うサイバーセキュリティリスク情報共有制度と呼ばれる官民パートナーシップも運営しています。

一部の国には、電力業界のコンピュータセキュリティインシデント対応チーム（CSIRT）やコンピュータ緊急事態対応チームを設置していることもあります。米国では、国土安全保障省（DHS）、エネルギー

省（DoE）、および情報機関が、サイバー脅威と脆弱性に関する実用的なインテリジェンス情報の業界と連携し、共有を促進することを目指しています[41]。

政府の情報機関だけでなく、インテリジェンスアナリストの経験者を擁する多くの民間のサイバーセキュリティコンサルティング会社もリアルタイムのサイバー脅威・脆弱性の監視サービスを電力会社に提供することができます。さらに、サプライヤのリスク評価やサードパーティの脅威インテリジェンスを提供している会社もあります。

新技術を導入・活用したサイバーリスク管理

新技術の導入は、電力会社とそのサプライヤがサイバーサプライチェーンのリスクを低減するための最先端の取組みになります。政府、大学、民間の研究所は、こうした取組みをサポートする新しいツールや技術を開発しています。こうした技術を企業として取込むためには、デバイス、コンポーネント、プロセスの再設計が求められます。例えば、一部のサプライヤは、製造業務を自動化して、人間の介入に伴うリスクを軽減しています。または、新しい追跡プログラムを導入して、コンポーネントの初期IDを取得し、調達情報に関連付けることにより、出所を確認していることもあります。今では多くのデバイスにコンピュータチップが搭載され、製品ライフサイクルを通じたスキャンや監査が追跡できるようになっています。これにより、企業はブロックチェーンを使用してサイバーリスクを低減し、データを効率良く処理し、このデータを安全にアーカイブする方法（下記コラム参照）を整備することができます。

米国では、エネルギー省（DoE）とその傘下の国立研究所、および研究パートナーが、コンポーネントのハードウェア、ファームウェア、ソフトウェアにおける悪意のある機能をサプライチェーンの各段階で特定するツールと技術を開発しています[43]。研究者はネットワーク上の疑わしいトラフィック、侵入、異常を監視および検出する方法をすでに開発しています。内部からの攻撃やスプーフィング（なりすまし）データ、悪意のあるコマンドを発見し、新たな脅威を認識してリアルタイムで対応するための方法が開発されています。例えば、サプライチェーンの脅威への対応に利用できるツールの一例として、プログラムを実行せずに、プログラムがどのように動作するかを調べ、オペレータがプログラムを導入する前に、その挙動を確認し、改ざんを検出できる便利なツールがあげられます[44]。

業界全体にわたるサイバーセキュリティフレームワークを成功させるには、企業が広範に関与し、セキュリティの対価を支払う顧客がいなければなりません。

研究者は、重要エネルギーデータの改変を防ぐ暗号化キーを安全に交換できるようにすることで、攻撃対象を減らす技術など、サイバーインシデントの防止に役立つ技術を研究しています[45]。さらに、研究者は予期しないサイバー活動がエネルギー供給システム上で一切起こらないようにする、すなわち仕様外のあらゆる動作を防止し、さらに制御システムの設定を動的に変更することで、標的を刻々と

サプライチェーン全体のコンポーネント追跡を可能にするブロックチェーン

自動分散台帳とも呼ばれるブロックチェーン技術は、取引のトランザクション追跡や、調達ライフサイクルの各段階において物理的に辿るコンポーネントの追跡が行えるなど、どこで誰にアクセスされたかという情報を、正確かつ変更不可能なデジタル記録にすることができます。ほぼ絶え間なく発生するサイバー攻撃を回避するため、北欧のエストニアでは政府の業務をほぼ完全にデジタル化し、ブロックチェーンに入れています[42]。この技術の暗号プロトコルは、ハッカーが傍受するよりも速くデータを再暗号化できるため、仮想セーフティネットとして機能しています。ブロックチェーンは、エコシステム内のすべてのデータをコピーし、分散型のノードに生成することで、クラウドコンピューティングの安全性を高める可能性もあります。各レコードは多数の場所に存在するため、1つのレコードを改変するよりも難しくなります。

変化させ、偵察や攻撃の計画をしにくくするツールも研究しています[46]。これらのツールは、2017年のDragonflyあるいはEnergetic Bearのような攻撃に対抗する方法として有用です。

分析とビジュアルによるサイバーリスクプロファイルのリアルタイム監査

サイバーリスクを低減するうえで、内部監査は重要な役割を果たします。会社のサイバーリスクプロファイルをリアルタイムに可視化するため、アナリストは関連するデータを収集し、分析モデルへ取込み、カスタマイズされたリアルタイムダッシュボードを構築します。そして、ダッシュボードを用い、リアルタイムでサイバーリスクの追跡を確認します。

結論

電力業界に対するサイバー攻撃の脅威は急速に進化、拡大しており、今まで以上に攻撃が多発し、多様な脅威関係者が関与し、ますます高度なマルウェアとツールが広く利用可能になり、無差別に使われるようになっています。電力会社は最も頻繁に攻撃される標的のひとつとなっており、ICSの停止や破壊すら引き起こそうとする攻撃者が国家組織であるケースが出てきています。そして、対応が最も難しい脆弱性のひとつが、サプライチェーンにおけるサイバーリスクです。そして、今日のサプライチェーンの広がりと複雑化が、このリスクを増大させています。サイバーサプライチェーンの説明責任と管理責任は、多くの企業であまり明確に定義されておらず、ほとんどの最高情報セキュリティ責任者（CISO）は、会社内のサプライチェーンの管理権限がなく、サプライチェーンのサイバーリスクインテリジェンスやサプライヤのリスク管理プロセスに対する可視性にほとんどアクセスできていない可能性があります。しかも、人員が不足し、膨大な数のサプライヤと取引が発生している現実も考えると、これがいかに大きな課題であるかが理解できます。現時点では、ほとんどの企業が、ようやくサプライヤの意識を高め、説明責任を求め、サプライヤのインテグリティを要求し始めたところです。

サイバーリスクは対応の難しい課題ですが、事業全体にわたる重要な資産を特定してマッピングすることから着手できます。そして、サイバーセキュリティ成熟度モデルを使ってコントロール環境の成熟度を評価し、予防、発見、回復のためのフレームワークを構築することができます。

こうして自社のサイバーセキュリティ対策をサプライチェーン全体で可視化し、リスクを低減することで、電力会社は、同業他社、政府機関、サプライヤ、および他業界とも協力し、インテリジェンスの共有、演習への参加、新しい標準とフレームワークの策定および新しい技術を試行していくことができます。新しいツールが数多く入手できるようになり、リアルタイムでネットワークを監視し、脅威を発見し、それに対応する能力も、急速に進歩しています。電力会社がこれらの機会をとらえれば、自社のリスクを著しく抑制できるだけでなく、電力業界全体、ひいては電力サービスに依存している社会全体のリスクをも大幅に低減できます。

巻末注

1. National Cybersecurity and Communications Integration Center、「*FY 2016 incidents by sector*」、U.S. Department of Homeland Security、2018年10月28日にアクセス、p. 1。
2. U.S. Department of Homeland Security、「Critical infrastructure sectors」、2018年10月28日にアクセス。
3. U.S. Department of Homeland Security、「Energy Sector」、2018年10月28日にアクセス。
4. National Cybersecurity and Communications Integration Center、「*FY 2016 incidents by sector*」。
5. Australia Cyber Security Centre、「*2016 threat report*」、2018年10月にアクセス、p. 15。
6. Jeff St. John、「U.S. government accused Russia of hacking into energy infrastructure」、Greentechmedia、2018年3月19日。
7. Rich Heidorn, Jr.、「Expert sees 'extreme uptick' in cyberattacks on utilities」、*RTO Insider*、2018年2月19日。
8. 同上。
9. Matthew J. Schwartz、「Cybercrime groups and nation-state attackers blur together」、Bankinfosecurity.com、2018年6月28日。
10. Lillian Ablon、「Data thieves: The motivations of cyber threat actors and their use and monetization of stolen data」、The Rand Corporation, testimony presented before the House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance、2018年3月15日、p. 6。
11. E-ISAC serves as the primary security communications channel for the electricity industry。参照：North American Electric Reliability Corporation、「*State of reliability 2018*」、2018年6月、p. 40。
12. Nicole Perlroth、Clifford Krauss、「A cyberattack in Saudi Arabia had a deadly goal. Experts fear another try」、New York Times、2018年3月15日。
13. Paul Stockton、「*Securing critical supply chains*」、Electric Infrastructure Security Council、2018年6月19日。
14. 同上。
15. Robert M. Lee、「*TRISIS: Analyzing safety system targeted malware*」、Dragosのブログ、2017年12月14日。
16. United States Computer Emergency Readiness Team、「Alert (TA18-074A): Russian government cyber activity targeting energy and other critical infrastructure sectors」、U.S. Department of Homeland Security、2018年3月15日。
17. 同上。
18. Security Response Attack Investigation Team、「Dragonfly: Western energy sector targeted by sophisticated attack group」、Symantecのブログ、2017年10月20日。
19. United States Computer Emergency Readiness Team、「Alert (TA18-074A): Russian government cyber activity targeting energy and other critical infrastructure sectors」。
20. 同上。
21. Naureen S. Malik、Ryan Collins、「The cyberattack that crippled gas pipelines is now hitting another industry」、Bloomberg、2018年4月5日。
22. Blake Sobczak、「Attack on natural gas network shows rising cyberthreat」、*E&E News*、2018年4月6日。
23. Malik、Collins、「The cyberattack that crippled gas pipelines is now hitting another industry」。
24. Sobczak、「Attack on natural gas network shows rising cyberthreat」。
25. Andy Greenberg、「The untold story of NotPetya, the most devastating cyberattack in history」、*Wired*、2018年8月22日。
26. 同上。

27. Scott Shane、Nicole Perlroth、David E. Sanger、「Security breach and spilled secrets have shaken the N.S.A. to its core」、*New York Times*、2017年11月12日。

28. Beau Woods、Andy Bochman、「Supply chain in the software era」、The Atlantic Council、2018年5月30日、p. 4。

29. Tim Schmidt、「Three critical procurement best practices for electric utilities: Are you doing these?」、Procureware.com、2016年7月1日。

30. Andrew Slaughter、Paul Zonneveld、「*An integrated approach to combat cyber risk: Securing industrial operations in oil and gas*」（サイバーリスクに対する包括的アプローチ：石油・ガス業界における安全操業のあり方とは）、Deloitte、2017年5月、p. 7。

31. Woods、Bochman、「Supply chain in the software era」。

32. North American Electric Reliability Corporation、「GridEx」、2018年11月6日にアクセス。Electric Infrastructure Security Council、「EarthEx 2017」、2018年8月22日。

33. The International Society of Automation、「ISA99, industrial automation and control systems security」、2018年11月6日にアクセス。

34. 同上。

35. North American Electric Reliability Corporation、「*Reliability Standards for the Bulk Electric Systems of North America*」、2018年7月3日更新。

36. Siemens、「Time for action: Building a consensus for cybersecurity」、2018年5月17日。

37. 同上。

38. Stockton、「*Securing critical supply chains*」。

39. The European Commission、「The EU cybersecurity certification framework」、2018年8月22日。

40. Eaton、「Eaton establishes cybersecurity collaboration with UL, announces industry's first lab approved for participation in UL program for cybersecurity testing of intelligent products」、2018年2月13日。

41. Cyber GRX、「CyberGRX is transforming third-party cyber risk management」、2018年10月にアクセス。

42. Nathan Heller、「Estonia, the digital republic」、*New Yorker*、2017年12月18日、25日。

43. Stockton、「*Securing critical supply chains*」、p. 19。

44. Office of Electricity Delivery & Energy Reliability、「*Multiyear plan for energy sector cybersecurity*」、U.S. Department of Energy、2018年3月。

45. 同上、p. 34。

46. 同上。

著者紹介

Steve Livingstonは、Deloitte & Touche LLPのプリンシパルで、過去24年以上にわたり情報セキュリティとリスク管理を担当してきました。IDおよびアクセス管理（IAM）、エンタープライズリソースプランニング（ERP）セキュリティ、ガバナンス・リスク・コンプライアンス（GRC）、セキュリティ情報・イベント管理（SIEM）の導入をはじめとする幅広いサイバー関連プロジェクトを手がけています。拠点はシアトルです。LinkedInの連絡先：www.linkedin.com/in/stlivingston/

Suzanna Sanbornは、Deloitte's Research & Insightsチームのシニアマネジャーとして、グローバルなエネルギートレンドを分析し、特にエネルギーおよび再生可能エネルギーセクターを専門としています。電力、石油、ガス、再生可能エネルギーセクターのリサーチ、分析、マーケティング、コミュニケーション、プログラム管理で20年以上の経験を有しています。拠点はバージニア州マクリーンです。LinkedInの連絡先：www.linkedin.com/in/suzanna-sanborn-510164/

Andrew Slaughterは、Deloitte Center for Energy Solutionsの上級ディレクターです。デロイトの資源・エネルギー・生産財グループと協力して、同センターの戦略を開発・実行・管理するほか、エネルギー関連リサーチプロジェクトの開発と実行、さらに同センターの定評とソートリーダーシップの開発を統括しています。専門は、戦略、市場ファンダメンタルズ分析、組織デザイン、政策アドバイスです。拠点はヒューストンです。LinkedInの連絡先：www.linkedin.com/in/slaughterandrew/

Paul Zonneveldは、Deloitteのカナダ法人のパートナーで、過去25年以上にわたり、石油・ガス、鉱山、電力、公益事業分野の顧客にサービスを提供してきました。資源・エネルギー・生産財セクターの顧客が直面する事業課題、すなわちデジタル、イノベーション、サイバー、サステナビリティ、エネルギー取引、オペレーションリスク管理などの深い知識を有しています。また、カナダ法人の最大顧客の一社であるHusky Energyのグローバル責任者も務めています。拠点はカナダ・カルガリーです。LinkedInの連絡先：www.linkedin.com/in/paul-zonneveld-917b7a3/

謝辞

本書のために見識を共有くださった電力会社と業界団体のエグゼクティブ、および業界の専門家の方々にお礼を申し上げます。また、Deloitte Support Services India Pvt. Ltd.の**Jaya Nagdeo**氏と**Deepak Vasantlal Shah**氏から、リサーチをサポートいただきました。Deloitte USの**Sharon Chand**氏、**Michael Prokop**氏、**Brad Singletary**氏、**Nick Sikorski**氏、**Steve Batson**氏、Deloitte Canadaの**Adam Crawford**氏、Deloitte UKの**Charlie Hosner**氏、**Dave Clemente**氏から、サイバーセキュリティに関する専門知識を共有いただきました。深くお礼を申し上げます。

デロイト トーマツ サイバーは、クライアントがデジタル世界で勝ち抜く力をつけ、安心して未来を築くビジネス展開をするため、サイバーリスクにかかわる様々な課題の解決に貢献します。
社会が「どこへでも」発展していけるよう「どこででも」垣根なく、サイバー空間を管理し、よりスマートで高速、コネクテッドな未来を実現したいと考えています。このサイバーリスクのサービスは、ICSとOTシステムのセキュリティ保護だけでなく、ICSとOTを取り巻く脅威を網羅的に明らかにすることで、電力業界の特有の脅威に効率良く対応するための筋道を提示します。

日本のコンサルタントにおける見解

1. 日本におけるサイバーセキュリティの現状

かねてより、日本の電力業界はサイバーの脅威に強いという認識が広まっていました。また、従来の電力会社（一般電気事業者）は総括原価方式により、生じた費用を電力料金に上乗せすることが可能であったため、各電力会社は送配電網の安定化に向けた系統運用、系統制御、配電自動化などの高度化を進めてきました。高度化されたシステムは電力会社各社の独自仕様となっています。

こうした電力の安定供給に資する設備は閉鎖的なネットワークで構成されており、保安用の通信回線は電力会社が独自に整備しています。また、複数事業者をまたいで電力を提供する欧米とは異なり広域停電となりにくい送電網であることも、サイバーの脅威に強いという環境を生み出していました。

その環境下においても、社会的要請を背景に国から重要インフラを担う電力業界に対し、サイバーセキュリティ対策が強く求められ、2016年には電力制御システムセキュリティガイドライン、およびスマートメーターシステムセキュリティガイドライン、が施行されました。電力各社は従来取組んできたITのサイバーセキュリティ対策の推進はもとより、OTのサイバーセキュリティ確保にも取組んでいます。

こうした背景から、海外で電力の制御システムに対する攻撃事例が出始めても、日本国内においては「日本の電力制御システムへの攻撃は、攻撃者にとり、コストが高くつくので標的となりにくい」「万が一攻撃されたとしても、制御設備への物理的被害にまで影響を及ぼすことはあり得ない」として、具体的な脅威にはなりえないという認識が広まっています。

しかし、今一度、サイバー攻撃に対する認識を改め、今まで以上の備えが必要になってきています。その理由として、日本の電力業界を取り巻く以下のような環境の変化が挙げられます。

- 国際競争力の強化と託送コスト削減に向けた国際標準仕様の機器・技術の採用増加（技術のオープン化進展）
- 需給予測、予防保全などのデータ分析の普及、分析に伴うIT/OTの融合（IoT・アナリティクスの普及）
- 電力サプライチェーンに対する国家組織による攻撃を含む世界的な攻撃リスクの顕在化（攻撃のグローバル化進展）

この環境の変化こそ、日本固有のクローズされた電力制御システム環境のリスク対策からグローバルと同等のリスク対策へと見直しが求められる要因です。

特に、サプライヤを経由してOTネットワーク内部に不正なソフトウェアが侵入する可能性が現実的になり、サプライチェーンに対するリスク対策は、早急に強化すべきです。この点は、国際的な動向と日本とで大きな差はないと考えられます。そして、日本においては現在、特にサプライチェーン領域を含め、サイバーセキュリティ対策の推進に向けた「サイバー・フィジカル・セキュリティ対策フレームワーク」としてガイドラインが策定され、電力分野も産業サイバーセキュリティ研究会の下、サブワーキンググループとして検討が進められています。このことも日本でのサプライチェーン領域におけるサイバーセキュリティ対策の必要性を裏付けています。

2. 日本の電力会社特有の考慮点

日本国内の電力業界は、これまでのクローズドな発展の流れから急速に世界標準化が進み、技術の進展に合わせITの融合が進んでいきます。この変化において制御セキュリティの対策を早急に進めるには、日本国内で培われた電力業界独自の組織・文化に起因する「4つの壁」への考慮が必要です。

組織間の壁――設備部門ですべてを完遂できる体制

日本の電力会社における設備部門は、長年の努力の継続により独自仕様による高度化を進めてきました。設備担当者とその請負業者は深い業務知見とノウハウを持ち、日本の高い電力品質を維持し続けています。それは電力社内の体制や人材にも言え、設備系部門はその内部だけで業務が完結できるだけの体制と業務プロセスが確立しており、計画、設計から運転、保守および廃棄までをやり切る人材の厚みと能力を有しています。

しかし、これが近年になって起こり始めたサイバーセキュリティへの対応となると、そのすべてを部門内で完結できる体制こそがリスクになりかねません。

サイバー攻撃は、複雑に連携するシステムを経由して目に見えないところで幅広く影響を及ぼす可能性があるため、業務で区切られた一組織・部門だけの対応にとどまらず、IT/OT全体を俯瞰した上での対策が必要となります。また、サイバーインシデント発生時点では見極めきれない影響度合いを想定しつつ、ビジネス影響や特に安全面への影響についてのシナリオを立て、都度経営レベルの判断を行っていかなければなりません。企画、広報、危機管理、情報系部門などの社内部門に加え、関係省庁、メーカーやセキュリティ専門家など、より多くの関係者と共に一丸となって対応に当たる必要があり、その体制を事前に整備し訓練などで経験しておかなければ、危機的なインシデントが生じた際に後手に回り、影響の拡大を止められない事態となる可能性があります。

また、一部門で業務を完遂できるような体制が整備されていることが、電力会社内での部門をまたいだ業務の標準化・汎用化自体を難しくしている状況もサイバーセキュリティ対応においてはボトルネックになり得ます。 部門ごとに固有の「業務」単位で仕事が完結してしまうため、送配電、発電など同じ「設備」部門において同様の対策を導入できる可能性があるにも関わらず、個別に検討・対策導入を行いがちになります。全社として対策レベルを上げるべきところが、一部の部門で推進に遅れが生じ、非効率だけでなくセキュリティホールとなり得る可能性があります。

セキュリティ人材育成・採用の壁――ジェネラリスト育成の人材配置と平等な処遇

電力業界では、所属組織とは別に複数組織をまたぐ「部門」という考え方があります。そして、発電、送電、配電、小売といった部門がその配下の人材の異動・配置権限を持ちます。従来の日本の電力会社の社員は、部門レベルで電力会社内の様々な組織を数年単位で異動し、電力業界の一定領域のジェネラリストとしての能力を伸長していきます。また、電力会社の社員は誰もが統合された、単一の報酬制度の下で働くことが補償されており、どこの組織に異動しても、一定のテーブルに従い、自身のランクに基づいた報酬を得ることができます。

これは電力事業の全体像の理解、また経営としての視点を養い不正を予防する観点としては非常に効果的ですが、こうした制度構造が、セキュリティなど専門領域のスペシャリストが育ちにくい状況を生んでいます。

サイバー攻撃への対応はICT系から始まったため、一般的に情報・通信系のバックグラウンドを持つセキュリティ知見者は多いものの、設備・制御システムのバックグラウンドを持つセキュリティ知見者の育成はまだ進んでいないのが現状です。情報・通信系の部門に属する人材は、セキュリティなどの専門スキルを伸ばしやすい環境にありますが、設備部門に属する人材は、専門業務への従事経験も含め、定期異動することがキャリアアップにつながるため、専門業務以外の知識――一般的にはIT組織に必要と思われている知識――を得るために、一部の組織に留まり続けることが許されない、または希望されない環境があります。

また、セキュリティなどの専門家を電力会社として中途採用することも検討されてはいますが、日本の電力会社の環境下では、現在人材マーケットにおいて価値が高まりつつあるセキュリティ人材に対し、他の事業会社のように報酬面で好待遇を提示することが難しく、“重要インフラである電力を守る”といった社会的な役割へのやりがいを求める人材、電力会社のある地域での活躍を希望する人材などに範囲が狭められます。さらに、制御システムには電力会社の独自仕様が残っており、一般的なセキュリティ人材だけでは知識不足であるという状況を生じます。

こうした状況から、電力会社、特に制御の領域でセキュリティの専門家を育成するには、従来の異動・配置、育成の仕方や、報酬制度の在り方を柔軟に見直していく必要があります。

意思決定の壁――ボトムアップ型

日本の電力会社は、業務を推進する主体である各組織の課長～部長層が具体的な取組みにおける意思決定の中心で、経営層はその計画や対策の承認を行う、という役割認識が定着しています。通常、何らかの答えを持たないまま経営層に方向性や意思決定を問うようなことはありません。経営に何事かを諮る場合は、その組織の実務責任者が具体的なアクションを明示し、それに対して経営がコメントをするという形での意思決定が行われます。

こうした日本の電力会社独自の意思決定構造は、現場の担当者がその状況を見て自ら考え判断することが求められる災害現場などでの対応には非常に有効です。しかし、サイバーセキュリティインシデントを想定した場合、最適解が得られにくい状

況、かつ影響範囲が見通せず、組織の担当範囲を超えて急速に広まる可能性のある状況下において、一組織の実務者レベルが状況整理と対策検討を行い、経営に諮る従来のプロセスでは、対策の決定に遅れが生じる可能性があります。

また、特に制御システムのサイバーセキュリティ対策は最悪の状況を想定しつつ、安全確保やビジネス影響の最小化を図るために複数組織が一丸となって対応に当たるべきです。その体制づくりにおいても実務者レベルからのエスカレーション型の意思決定では、他組織の巻き込みに遅れが生じる可能性があります。実務者レベルでの対策案検討は最短に済ませ、対策が見いだせない状況においても経営層を巻き込み、刻一刻と変化する状況と想定リスクをリアルタイムで認識し、意思決定をしていく環境が求められます。

ボトムアップ型意思決定による弊害はもう1点あります。それは、実務者が経営層の認識レベルを前提として計画を説明し承認されるというプロセスを経ることから、経営層向けに抽象度を上げた内容で意思決定を諮ることとなるため、PDCAサイクルが正しく機能しないことです。

本来PLANは、具体的かつ測定可能なものであるべきです。しかしこれが経営層への説明を経ることで抽象化してしまい、抽象化された目標・計画に基づいて実施後の評価が行われるため、今後の改善につながる具体的なアクションが導き出せないことがあります。

サイバーセキュリティ対策やサイバーインシデント対応において、抽象的な評価では対外的な説明や自社の改善には役立たないだけでなく、大きな取組みの抜け漏れを見逃すことにもなりかねません。サイバーセキュリティに関しては、経営層も一定の知識を持つ、または第三者の目による評価などを活用し、具体的なレベルでのPDCAサイクルを回すことが求められます。

調達の壁――多重請負構造、発注先との強い信頼関係

これまで日本の電力会社は、設備の納入メーカーと確固たる関係を築き、自社の設備・システム環境を熟知するメーカーとの信頼関係の下で設備の高度化を行ってきました。また、設備を納入したメーカーが保守することで、電力会社は何か不明の事象が起こった場合はメーカーに連絡すれば対応して貰えるような関係性が構築されていきました。

この長い関係性の中で、「過去に納入された機器に関する仕様の詳細を電力会社側が把握していない」状況や「仕様や納入条件を細かく指定しなくても、メーカーは分かった上で最適な機能を提供してくれるはず」という認識が生まれ、万が一の場合の責任の分界点を明確にすることなく契約を結んでいる可能性があります。また、設備を導入する際、「機能」の単位で一括購入することが多いため、殆どのケースで機能レベルでの仕様は共有されても、その機能を形成する機器の詳細仕様や詳細のソフトウェア・プログラムはメーカーからは共有されていません。

前述の通り、多くの関与者がいるサプライチェーンの中で、契約先メーカーが詳細の仕様すべてを把握しているとは限りません。また、過去からの関係性の中であっても、電力側の運営体制やシステム環境まで熟知しているメーカー担当者がいつまでも電力会社に関わり続けるとは限りません。このような状況は、近年、脅威となったサイバー攻撃への対策の実装と攻撃を受けた際の対応体制について詳細を決めずにおくことは、ビジネス上非常に大きなリスクとなります。

また、発注規模の大きい日本の電力会社では多重請負構造が定着化しており、業務や設備の調達を1社に発注した場合、実際はその配下に多くの下請けの会社が作業や装置・機器を提供していくケースが多くあります。直接契約した相手先企業のサイバーセキュリティ対策状況を確認し、対策レベルの向上を働きかけたとしても、その対策が下請けの会社にも適用されているとは限りません。契約先のその先まで確認を徹底しなければ、セキュリティ対策上の漏れが生じる可能性があります。

日本の電力各社は、セキュリティ対策として資材調達プロセスに対し、一定のセキュリティ対策状況のチェックを導入し、その適用状況を評価する手順を組み込んではいます。しかし、資材調達プロセスを経ない個別部門の調達も未だに残存しており、資材調達プロセス上のコントロールが及んでいない場合があります。また、チェック自体が提出書類の表面的な確認のみで、内容の精査には及んでいない可能性があります。

3. どのような対策が今、必要か?

上記のような日本の電力会社独自の環境や経緯を踏まえ、取るべき対策として3つの取組みを挙げます。

①ガバナンスの見直し

日本の電力会社は部門間の連携体制を構築・対応する必要性が薄く、特に設備・サービスの調達のような個別組織の業務に密接にかかわる業務の場合、全社としてルールを定め運用するのが難しい状況にありました。しかし、サイバーセキュリティ対策としては、サプライチェーン全体を通じて侵入口を作らない網羅的な取組みと、万が一インシデントが発生した際のスピーディな意思決定体制が求められます。

そのためにはまず、セキュリティ部門と各組織が連携し、調達プロセス全体を見通した対策を行います。連携体制の中で、調達仕様へのセキュリティ対策の組込み、下請けを含む発注先事業者のセキュリティ対策状況の確認といった手順を各組織共通のルールとして規定する必要があります。

こうした取組みを効果的に推進するため、各組織の個別業務プロセスの中にセキュリティ対策項目を入れ込み、「本来業務として」実施できるような形を整え徹底させることが重要です。セキュリティ対策だけを後付けで各部門に実施させることにすると、本来業務とは離れた形で対応する必要が生じ、負担感・実施漏れが生じる可能性があります。

また、セキュリティ対策の実施状況をセキュリティ部門が個別に評価すると組織の主体性が失われ、形骸化していく原因にもなりえます。組織の業務としてセキュリティ評価を実施させることがポイントとなります。さらに、セキュリティ対策に関する第三者評価を個別の業務プロセスに組み込めれば、より強固な対策となります。

②自社設備情報の把握と管理

メーカーとの信頼関係や、機能レベルでの設備一括導入を行ってきた背景から、日本の電力会社は、特に制御設備に関し、詳細レベルの機器・ソフトウェアの情報を入手・管理することは殆どありませんでした。

しかし、日々更新されるサイバー脅威情報や機器・ソフトウェアの脆弱性情報を基にセキュリティ対策を検討する場合、自社への影響範囲を確認するために、自社設備機器の詳細レベルの仕様、情報を把握しておくことが説明責任を果たす上でも必要不可欠です。規制により対応が進んでいる海外の電力会社と同様、日本においてもソフトウェアを含む設備構成管理（コンフィグレーションマネジメント）の仕組みの導入が求められます。

③意識醸成と教育

日本の電力会社は、その設備や送配電網を独自に進化させたことで、サイバー攻撃から一線を画していると認識されていた時期は確かにありました。しかし、前述の通り、技術・標準化の進展などにより、サイバーセキュリティインシデントの発生リスクは海外同様に高まりつつあります。

しかし、未だにサイバーセキュリティのリスクは低いと考えている経営層や実務担当者も確実に存在しています。旧来通りの認識でいる方々へ、現在の電力を取り巻くサイバー脅威について正しい理解を促し、対策の必要性を理解して頂くための意識醸成が急務といえます。

また、サプライチェーン全体のセキュリティレベルを高めるために、従来のICTバックグラウンドを持ったセキュリティ担当者の育成だけでなく、OTや資材調達系のバックグラウンドを持った担当者へもセキュリティ教育を行い、一定以上の専門知識を持つレベルまで育成していく必要があります。

まとめ

ここまで述べてきたサイバーセキュリティ強化に向けた取組みは、日本の電力会社が個別組織・業務ごとに高度化させてきた道程によって培った体制、風土・文化を変えていく必要があり、その推進は非常に難しいものと考えます。米国などですでに進められているサプライチェーン対策の取組みに関する最新情報の入手はもとより、サプライチェーン全体を俯瞰した連携体制づくり、業務の汎用化による共通施策の並行推進、詳細に至る設備構成の可視化と管理、膨大なサプライヤのコントロールなど、実施すべきことは多岐に渡り、また、それらの対策推進に向け前提となる関係者の意識醸成など、難易度の高いものが多くあります。短期間ですべての対応を行うことは現実的ではありません。

まずは電力サプライチェーン全体を通じて潜在・顕在リスクを俯瞰的に整理し、人、プロセス、テクノロジー、サプライヤ対応など、自社が優先的に取組むべきテーマを定めた上で、より高度化しつつあるサイバーセキュリティリスクへの対応を一歩、二歩と着実に進めて行かれることを推奨します。

日本のコンサルタントにおける見解執筆者

デロイト トーマツ サイバー合同会社
望月　武志
takeshi. mochizuki@tohmatsu.co.jp

デロイト トーマツ コンサルティング合同会社
東　美津子
mitazuma@tohmatsu.co.jp

岩國　知彦
tiwakuni@tohmatsu.co.jp

Japan Contacts

北野　晴人
デロイト トーマツ サイバー 合同会社
エネルギー担当
パートナー
haruhito.kitano@tohmatsu.co.jp

神薗　雅紀
デロイト トーマツ サイバー 合同会社
チーフ テクノロジー オフィサー
サイバーセキュリティ先端研究所 所長
パートナー
masaki.kamizono@tohmatsu.co.jp

丸山　満彦
デロイト トーマツ サイバー 合同会社
チーフ ビジネス ディベロップメント オフィサー
パートナー
mitsuhiko.maruyama@tohmatsu.co.jp

下田　健司
デロイト トーマツ コンサルティング合同会社
エネルギーユニットリーダー
執行役員
keshimoda@tohmatsu.co.jp

須山　雅文
デロイト トーマツ コンサルティング合同会社
エネルギー担当
執行役員
masuyama@tohmatsu.co.jp

Global Contacts

Scott Smith
Vice chairman
US Power & Utilities leader
Deloitte LLP
+1 619 237 6989
ssmith@deloitte.com

Sharon Chand
Risk Advisory principal
Cyber Risk Services leader
Energy, Resources & Industrials
Deloitte & Touche LLP
+1 312 486 4878
shchand@deloitte.com

Steve Livingston
Risk Advisory principal
Cyber Risk Services leader
Power & Utilities
Deloitte & Touche LLP
+1 206 716 7536
slivingston@deloitte.com

David Nowak
Risk Advisory principal
Cyber Risk Services
Deloitte & Touche LLP
+1 312 486 4126
danowak@deloitte.com

Paul Zonneveld
Global Risk Advisory leader—Energy, Resources & Industrials
Deloitte Canada
+1 403 503 1356
pzonneveld@deloitte.ca

Brian Murrell
Global Risk Advisory leader—Power & Utilities
Deloitte US
+1 212 436 4805
bmurrell@deloitte.com

Felipe Requejo
Global Sector leader—Power & Utilities
Deloitte Touche Tohmatsu Limited
+34 914 381 655
frequejo@deloitte.es

Rajeev Chopra
Global leader—Energy, Resources & Industrials
Deloitte Touche Tohmatsu Limited
+44 20 7007 2933
rchopra@deloitte.co.uk

Jonathan Giliam
Risk Advisory leader—Power & Utilities
Deloitte Africa
+27 112 027 317
jgiliam@deloitte.co.za

Hendri Mentz
Risk Advisory leader—Power & Utilities
Deloitte Australia
+61 8 9365 7367
hmentz@deloitte.com.au

Anthony Hamer
Sector leader—Power & Utilities
Deloitte Canada
+1 416 643 8409
anhamer@deloitte.ca

Tsutomu Yamada
Risk Advisory leader—Power & Utilities
Deloitte Japan
+81 906 520 3928
tsutomu1.yamada@tohmatsu.co.jp

Andreas Langer
Risk Advisory leader—Power & Utilities
Deloitte Germany
+49 711 1655 47289
anlanger@deloitte.de

Charles Hosner
Risk Advisory leader—Power & Utilities
Deloitte North West Europe: UK
+44 20 7007 2827
chosner@deloitte.co.uk

Arup Sen
Risk Advisory leader—Power & Utilities
Deloitte India
+91 22 6185 6610
arupsen@deloitte.com

Richard Kuang
Risk Advisory leader—Power & Utilities
Deloitte China
+86 1085 207 401
rkuang@deloitte.com.cn

Deloitte.
Insights

Deloitte Insights の登録はこちらから www.deloitte.com/insights

@DeloitteInsightをフォローしてください

Deloitte Insights contributors
Editorial: Kavita Saini, Abrar Khan, Rupesh Bhat, and Preetha Devan
Creative: Kevin Weier and Molly Woodworth
Promotion: Nikita Garia
Cover artwork: Infomen

Deloitte Insights について

Deloitte Insights は、企業、公共部門、NGO に洞察を提供する独自の記事、レポート、定期刊行物を刊行しています。我々の目標は、プロフェッショナルサービス組織全体を通した調査と経験、更には大学・研究機関とビジネスにおける共著者の経験を駆使し、企業経営者や政府指導者が関心を持つ幅広いトピックについて会話を進めることです。

Deloitte Insights は、Deloitte Development LLC が作成しています。