電力制御システムのセキュリティ向上策に関する提言

平成３０年１１月２１日
産業サイバーセキュリティ研究会
ワーキンググループ１(制度・技術・標準化)
電力サブワーキンググループ

はじめに

我が国の産業界が直面するサイバーセキュリティの課題を洗い出し、関連政策を推進していくため、平成２９年１２月に「産業サイバーセキュリティ研究会」が設置され、制度・技術・標準化を検討するワーキンググループ１では、産業分野ごとのサブワーキンググループを設置した。

重要インフラたる電力分野においても、これまで経営層の関与のもと、取り組みが進められてきたが、平成２８年の電力小売の全面自由化等により新規参入者が拡大するとともに、発電・送配電事業者を中心としてデジタル技術の活用が広がる中、サイバーセキュリティ対策強化に向けたさらなる取り組みが求められている。

また、重要インフラの情報セキュリティ対策に係る第４次行動計画（平成３０年７月２５日内閣サイバーセキュリティ戦略本部改定）においても、基本的な考え方として、重要インフラ事業者等における情報セキュリティ対策は、一義的には当該重要インフラ事業者等が自らの責任において実施するものであるとしており、経営層が中心となって対応を進めるべきものである。

これらの状況を踏まえ、電力分野のサイバーセキュリティに関する今後の取り組みについて検討を行うため、電力サブワーキンググループ（以下、電力 SWG と言う。）を設置し、第２回まではサイバー攻撃を前提とした電力制御システムに関するセキュリティ向上策について議論を行ってきた。また、第３回目以降は電力分野における新たなサイバーリスクや海外連携等について議論を行う予定である。

本資料は第２回までの電力 SWG における議論を取り纏めた提言である。これを踏まえ、２０２０年の東京オリンピック・パラリンピックも見据え、電力分野で取り組むべきサイバーセキュリティ対策として、電気設備の技術基準の解釈にも引用されている電力制御システムセキュリティガイドラインの見直しを含め、効果的かつ実効性のある方法を検討・導入していくことが望ましい。併せて、上記ガイドラインへの対応を進め、自己点検及び外部有識者を交えた取り組みの客観的なレビュー等の継続的な実施が望まれる。

提言

（1） サイバーインシデントに対応する体制の強化

■ 危機管理体制との連携強化

サイバーインシデントの一般的な特徴として、停電等の原因がサイバー攻撃に拠るものか否かの判断が難しい点、及び初動対応が遅れると被害が拡大する点が挙げられる。

サイバー攻撃を受けた際にその被害を極小化するためには、危機管理体制や必要に応じたサイバーインシデント対応体制の迅速な立ち上げ、及び各体制内・体制間での密接な情報共有等の連携強化が重要である。

また、電力制御システムの不具合事象については、サイバー攻撃の疑いについても分析・検討対象から除外することなく、当初は被害が小さくても、今後の被害拡大の可能性が見込まれる場合には、危機管理体制とサイバーインシデント対応体制が連携できるよう役割や手順を予め定めておくことが期待される。

一例として、ある事業者では非常災害時の危機管理に係る体制内にサイバーセキュリティに関する班を設置し、サイバーインシデント対応体制と危機管理体制の連携強化を図ることができるよう役割と手順を定めている。

■ 情報システム（IT）部門と制御システム（OT）部門の密な連携

一般的に OT システムでは、安全性に次いで可用性の確保（電力分野の場合は、電力制御システムの安定稼働による電力の安定供給）が優先され、IT システムでは機密性の確保が優先されるといった基本的な考え方の違いがある。この IT システムと OT システムの間にある考え方の違いを双方の部門の関係者が認識した上で、個々の事業者における状況を踏まえた体制の構築や人材育成・交流、教育等を通じてこの差を補完していくことが重要である。

また、事業運営とサイバーセキュリティの確保をバランスよく両立させ、かつ実効性を高めていくためには、リスクアセスメントに代表されるセキュリティマネジメントを適切に実施できることも必要となる。そのため、IT システムに携わる者と OT システムに携わる者が互いに協力しながら、セキュリティ向上を目指していく必要がある。

現時点においても、相互理解と情報共有の促進、セキュリティインシデント対応能力の向上を目指しており、IT システムと OT システム双方の部門の要員からなるセキュリティ組織を設置している事業者もある。また、独立行政法人 情報処理推進機構の産業サイバーセキュリティセンター（以下、ICS-CoE と言う。）の中核人材育成プログラムでは、IT と OT の両部門からの研修生が協力しながら様々な課題を解決しなければならない環境で訓練を受けており、同プログラムでは、IT と OT を統括するセキュリティ管理組織の設置を推奨している。こうした取り組みをさらに進めていくことが必要である。

（２） 人材の育成・確保

■ 「戦略マネジメント層」の役割及び育成

「戦略マネジメント層」には、セキュリティ戦略の検討やインシデント対応における中核を担い、経営層との橋渡し役になることだけではなく、サイバーセキュリティをビジネスリスクのひとつとして認識した上で、セキュリティ面を踏まえた経営計画や投資計画の策定にも関与していくといった役割が期待されている。

「戦略マネジメント層」を構成する人材は、セキュリティ分野のみの知見だけではなく、OTシステムや経営企画に関わる幅広い知見を有することが望ましく、組織として、経験豊富なベテラン社員やセキュリティ対応要員として育成される社員がバランスよく適材適所で配置されることが重要である。

なお、セキュリティ分野の育成手法のひとつとして、ICS-CoE の育成プログラムや情報処理安全確保支援士等の資格制度を活用する取り組みが行われている。

■ セキュリティ人材の確保

一般的にセキュリティ人材はどの業界でも必要とされ不足していることもあり、人材の流動が激しい。そのような中、優秀な人材を育成し、社内に定着させるためには、社内のセキュリティ人材に求められる役割・機能を明確にし、キャリアパスや育成プランを用意することが望ましい。キャリアパスが存在することで、セキュリティ人材のモチベーション向上や、効率的かつ効果的な人材育成が可能になるものと期待される。

このため、電力分野においても、個々の事業者における状況を踏まえ、セキュリティ対応体制や要員の充実を図っていく取り組みが必要である。

（３） 事象発生時の対応強化

■ 社外連携の強化

サイバーインシデントが疑われる場合には、事案の影響等を勘案し、一般利用者への広報のみならず、地域の企業、自治体、警察、セキュリティ専門機関、情報共有組織（例えば電力ISAC）等との適宜の情報共有、とりわけ、既存の危機管理対応等の枠組みと連携を取りながら情報共有を行うことが重要であり、さらにその後の状況に応じた柔軟な対応が必要である。

このため、地域や電力業界に設置されているセキュリティ連絡会もしくはインフラ防護目的で設置されている組織等での活動機会を活用し、他の電力事業者や他分野の重要インフラ事業者、自治体等のセキュリティ担当者間で人的な関係を構築する等、社外との連携を強化することで自組織のみならず利害関係者全体のサイバーレジリエンスをより強化することが望まれる。

■ 危機管理体制の実効性向上

サイバーインシデントの発生と連鎖障害の拡大等を想定したシナリオを設定し、既存のマニュアルやルール、プロセスや体制に関する課題、改善策を抽出する「演習」を行うことが有効である。また、社内での演習だけでなく、例えば上述の地域や電力業界に設置されているセキュリティ連絡会もしくはインフラ防護目的で設置されている組織等での活動機会を活用し、自治体や警察、消防、新規参入者、地域内の重要インフラ事業者との合同演習や業界内での演習を行うことは、さらに大きな効果が期待できる。

さらに、この演習への参加は、使用するリスクシナリオの作成過程自体が人材育成や社内外の人材交流の機会になるとともに、経営層も含めた意識付け、理解促進にもつながるものと期待される。

一例として、ある事業者では、地域の大学や行政、警察、重要インフラ事業者、企業等からなるセキュリティ連絡組織の一員として、セキュリティ管理部署が窓口となり情報共有や合同演習に参加する取り組みを開始しており、情報共有や知見の獲得、有事対応能力の強化に加えて、セキュリティ人材の育成の観点でも有用な取り組みと位置付けている。

（4） その他

■ 中長期課題への対応

サプライチェーンリスク等の中長期課題については、産業界横断的な課題でもあることから、その観点での議論が進んでいるところである。このような動向も見据えつつ迅速に対応していくために、電力分野においても、関係者による引き続きの議論や検討を進めていくことが重要である。

以上