掲載日:2021年01月06日, 面名:総合・企画, 記事ID:K1J20210106_A1014000108000005
(C)電気新聞

ゼミナール

電力流通

224 国際規格ＩＥＣ61850の国内適用とそのサイバーセキュリティーの課題は？

変電所向けに仕様作成
通信時の認証強化重要

ＩＥＣ６１８５０は、主に保護監視制御装置（ＩＥＤ：Ｉｎｔｅｌｌｉｇｅｎｔ Ｅｌｅｃｔｒｏｎｉｃ Ｄｅｖｉｃｅ）の相互運用性確保のための国際規格である。２０００年頃までは変電所監視制御システムを対象としていたが、現在は制御所―変電所間通信、水力／火力発電所、配電自動化、分散型電源等に適用可能な規格となっている。ここでは、ＩＥＣ６１８５０の国内適用への取り組みと、関連するサイバーセキュリティーについて解説する。

【国内適用に向けた取り組み】

ＩＥＣ６１８５０ではＩＥＤのデータ構造、基本的な内部処理、監視制御時の通信の手順、エンジニアリングの作法、設定ファイルのフォーマット、装置の耐環境性、プロジェクト管理およびＩＥＤの適合性試験の方法を定めている。一方で、規格で用意されたデータ定義に曖昧なものがあり、国内の電力会社が利用する機能の一部がサポートされていない。しかし、電力会社が独自にこれら機能の適用検討を行うと、相互運用性の確保が困難になる。また、ＩＥＣ６１８５０が国内で普及するためには、ＩＥＤが機能仕様の記載通りに動作するか評価試験するシステムや、レガシー系の通信方式とＩＥＣ６１８５０を相互変換する装置が必要になる。

電力中央研究所では、相互運用性を確保しつつ、ＩＥＣ６１８５０を国内に適用するため、変電所監視制御に関する機能とデータ、通信について機能仕様を作成した。現在は、変電所―制御所の監視制御に用いる機能とデータおよび通信の検討とともに、国内普及に向けた開発に取り組んでいる。

【ＩＥＤの脆弱性】

ＩＥＤと関連する製品に対するソフトウエアの不具合や設計ミスが原因となる脆弱性について、対応策と合わせて積極的に公開されるようになっている。米国土安全保障省の組織ＩＣＳ―ＣＥＲＴでは、制御システムに関連する脆弱性の深刻度とその対応策について報告している。２０２０年12月現在、米国内の学会や論文誌で紹介、もしくは米国内の研究機関や大学で利用されているＩＥＤと、その開発ツールに関する脆弱性について、海外重電４社と制御装置メーカー２社のものがＩＣＳ―ＣＥＲＴのウエブサイトに掲載されている。

これら脆弱性の深刻度評価は、当該装置・ソフトウエアへの影響を評価する、情報システムに対する評価手法が用いられており、関連する電力系統や主回路機器への影響は考慮されない。そのため、実際に脆弱性が利用されて攻撃を受けたとしても電力系統にほとんど影響がないケース、脆弱性のある装置と通信可能となった段階（攻撃者が電力制御用通信ネットワーク内部に侵入している状態）でより致命的な攻撃が可能なケースが存在する。電力設備のセキュリティーリスクをより正確に把握するためには、自社設備に関連する脆弱性情報を把握し、運用状況を考慮した上で、ＩＥＤや関連ソフトウエアがサービス停止や不正操作などに陥った影響を分析する必要がある。

【ＩＥＤのセキュリティー対策】

サイバーセキュリティーに関する国際規格であるＩＥＣ６２３５１では、ＩＥＣ６１８５０が用いる通信プロトコルのセキュリティー、暗号や認証に用いる鍵の管理、アクセス制御について規定している。一方、ＩＥＤ本体の物理セキュリティー、ＩＥＤのＯＳやファームウエア、メーカーが独自実装した機能のセキュリティー対策は対象外である。ＩＥＣ６２３５１において、電力制御用通信ネットワークからのサイバー攻撃によるＩＥＤの不正操作を防ぐ最も有効な対応策は、ＩＥＤの制御通信の認証と認証局による鍵の管理である。ＩＥＣ６２３５１が推奨する通信の認証と鍵の管理を行うことで、ＩＥＤおよびＩＥＤと通信を行う端末が正規であることの確認と、通信の改ざん検知が可能になる。

しかし、異なるベンダーのＩＥＤと認証局の相互運用性、認証局本体とその通信の信頼性、証明書失効への対策、制御通信の認証に対応するＩＥＤや鍵管理ツールの入手方法など課題が存在する。今後、ＩＥＤのセキュリティー対策を強化するためには、ＩＥＤの制御通信の認証と鍵管理に関する研究開発と実用化が求められる。

（隔週で掲載します）

電力中央研究所　システム技術研究所
主任研究員
上田　紀行
うえだ・のりゆき＝２０１５年度入所、専門は電力保護制御システムのプロトタイピング、セキュリティー