電力制御システムのサプライチェーン・セキュリティ向上策に関する提言

令　和　6　年　3　月　2　2　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サイバーセキュリティ対策強化に向けたさらなる取組が求められているところ、電力分野のサイバーセキュリティに関する今後の取組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。）を平成 30 年６月に設置し、これまで 16 回の会合を開催してきた。平成 30 年 11 月には、第２回電力 SWG までの議論を取りまとめた提言である「電力制御システムのセキュリティ向上策に関する提言」を発表したほか、以降の電力 SWG では、大手電力事業者、小売電気事業者、小規模発電設備等に求められるサイバーセキュリティ確保の方策に関する議論や電力分野におけるサイバーセキュリティリスク点検ツールに関する議論を行ってきた。

重要インフラ全体の取組としては、「重要インフラのサイバーセキュリティに係る行動計画」（以下、行動計画と言う。）が令和４年６月に策定され、官民連携による重要インフラ防護の一層の強化が進められている。また、行動計画に基づき、重要インフラ分野に共通して求められるサイバーセキュリティの確保に向けた取組を整理した「重要インフラのサイバーセキュリティに係る安全基準等策定指針」（以下、安全基準等策定指針と言う。）及び安全基準等策定指針で示すセキュリティ確保に向けた取組についての参考情報を記載した「重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書」が令和５年７月に策定された。安全基準等策定指針では、リスクマネジメントによる事前対応と、危機管理の両面からサイバーセキュリティの確保に取り組むことの重要性が明記されており、具体的なリスクマネジメントの一つとして、サプライチェーン・リスクに対するサプライチェーン・リスクマネジメントを求めている。

本資料は、安全基準等策定指針の策定を踏まえ、電力制御システムのサプライチェーン・リスクに対するセキュリティ向上策について、電力 SWG における議論を取りまとめた提言である。これを踏まえ、電力分野で取り組むべきサプライチェーン・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。あわせて、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組の客観的なレビュー等の継続的な実施が望まれる。

提言

電力制御システムのサプライチェーン・リスクとは、電気事業者へ電力制御システムが納入されるまでの開発や製造に係る一連の工程に加え、調達・運用・保守・廃棄を含むシステムライフサイクル全般のサプライチェーンにおけるサイバーセキュリティ上のリスク（サイバーセキュリティ基本法に定めるサイバーセキュリティを欠く可能性のうち、経営、人、技術又は取引によりもたらされるもの）を意味する。対応すべき代表的なサプライチェーン・リスクとして、以下のリスクが挙げられる。

- 電力制御システムの開発・製造段階における部品（ハードウェア及びソフトウェア）の不正な改造、不正機能の埋め込み
- 電力制御システムの運用・保守段階における外部関連サービス（保守サービス、クラウドサービス等）の供給途絶
- 電力制御システムの運用・保守段階における海外拠点、グループ組織、取引先等を経由したサイバー攻撃
- 電力制御システムに関連する外部サービスにおける情報の不適切な取扱い（機密情報の漏えい等）

実際にサプライチェーン・リスクが顕在化した事例も複数存在するところ、電気事業者においては、想定されるリスクに対して適切な対策を講じることが求められる。特に、安全基準等策定指針の記載や諸外国の取組等を踏まえ、以下の取組を実施することが求められる。

■ サプライチェーン・リスク管理

電気事業者は、電力制御システム等に関連する委託先等の役割と責任範囲を明確化するほか、電力制御システム等のサプライチェーンの依存関係及び委託先等のセキュリティ対策状況を把握する。また、電力制御システム等のサプライチェーン・リスクに関するリスク分析を行い、それに基づいた対策を講じるとともに、対策の状況を定期的に把握し、把握結果に基づき対策の見直しを検討する。リスク分析の実施に当たっては、情報処理推進機構（IPA）の「制御システムのセキュリティリスク分析ガイド」等を参照し、自組織の事業環境等を踏まえて、シナリオベースや資産ベースのリスク分析等、適切な分析手法を選択又は相互補完的に組み合わせて分析することが想定される。さらに、対策状況の把握に当たっては、資源エネルギー庁「電力システムにおけるサイバーセキュリティ対策状況可視化ツール」等を活用することが想定される。

■ セキュリティ仕様の確認

電気事業者は、電力制御システム等の調達時にセキュリティ仕様を発注仕様書等において明確にするほか、電力制御システム等がセキュリティ仕様通りに設計、製造されていることを確認する。また、セキュリティに影響を与える可能性がある変更を適切に管理する。

■ 機器・外部記憶媒体の管理

電気事業者は、電力制御システム等に関わる機器・外部記憶媒体を、システムライフサイクル（運用・保守段階だけでなく、廃止段階も含む）を通じて管理し、保護する。

事業者における効果的かつ実効性のある取組の実施に向け、「電力制御システムセキュリティガイドライン」を発行する日本電気協会及び策定に携わる電気事業連合会等のその他の機関においては、ガイドラインの見直しを検討することが望まれる。

政府においては、電気事業者におけるこれらの取組に向けた環境整備や実施を支援していくべきである。また、電気事業連合会等や電気事業者は、事業者に求められる対応を詳細化した手引き文書の策定等、より実効性のある対応を進めていくべきである。さらに、サプライチェーン全体での対策実効性を高めるために、政府又は事業者はサプライチェーン全体での教育・訓練の実施等に向けた方策について検討を進めるべきである。加えて、電気事業者は、経済安全保障の観点を踏まえ、サイバーセキュリティ上のリスクだけでなく、物理的な妨害行為等のリスクも考慮した包括的な対策を検討することが望まれる。加えて、政府においては、事業者がサプライチェーン・リスクに対応するために必要な情報を取得、提供及び利用できるようにするための取組について、法律等において妨げるものがないか、考え方を整理することが望まれる。これらの検討に当たっては、他分野との相互依存性を踏まえ、電力分野以外の動向も踏まえた検討が必要となる。

サプライチェーン・リスクは日々高度化・複雑化していることを踏まえ、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