

IoT 普及・拡大に向けたシステムセキュリティ特別調査専門委員会
設置趣意書

電気システムセキュリティ特別技術委員会

1. 目的

電気エネルギーシステムに代表される社会インフラシステムや、近年、進展著しい IoT (Internet of Things) システムなどについては、従来にも増してサイバー脅威が顕在化しており、そのサイバーセキュリティ (以下、セキュリティ) 確保が極めて重要になっている。本特別調査専門委員会では、Society5.0¹ やそれに伴う技術開発に伴い、今後発生すると想定される脅威に対して、的確に保護するため、これらに関わるセキュリティ動向や内外の取組みを広く調査するとともに、電気学会として取り組むべき課題と方向性を明らかにする。

2. 背景および内外機関における調査活動

Society5.0 では、社会インフラ、産業インフラ、生活インフラ、環境インフラ等の様々なフィジカル空間に埋め込まれた IoT 機器が現場の情報を収集し、様々なネットワークを利用してクラウド等のサイバー空間と連携され、膨大に蓄積されたデータから AI (Artificial Intelligence) やビッグデータ等の技術によって知識・知見を産み出すことにより、フィジカル空間の高度化・効率化に繋げてゆくことが期待されている。

一方、サイバー攻撃の対象となるシステムは IT システムから他のシステムへと拡大しつつあり、攻撃手法も日々進化している状況である。特に、産業や生活に新たな価値を生み出す IoT システムの普及・拡大に伴い、サイバー攻撃の影響はサイバー空間だけでなく、フィジカル空間にも及ぶことが想定される。これにより、IoT 時代に対応した社会全体の安全・安心を確保する技術の確立が急務となってきている。

これに対し、国内ではサイバーセキュリティ基本法 (2015 年 1 月施行) や、NISC (National center of Incident readiness and Strategy for Cybersecurity; 内閣セキュリティセンター) の重要インフラの情報セキュリティ対策に係る第四次行動計画 (2018 年 7 月改訂) によって、重要インフラ事業者が取り組むべき事項として、安全基準の整備と浸透、情報共有体制や障害対応体制の強化、リスクマネジメントを踏まえた対処体制の整備等を示している。また、CSSC (Control Systems Security Center; 技術研究組合制御システムセキュリティセンター) において、重要インフラ分野のテストベッド構築やテストベッドを用いた演習等が行われ、分野横断的に活用可能な技術基盤が構築されてきている。一方、電力分野では、スマートメータの拡大や電力自由化、発送電分離等に合わせて、分野固有のセキュリティガイドラインが策定された。

このような中、CPSS (Cyber-Physical Systems Security) (第 I 期) (第 II 期) 特別調査専門委員会では、電力分野に限らず Cyber Physical Systems のセキュリティに関する動向の調査活動を行い、分野横断的に適用可能な技術やガイドラインが存在する点、各分野個別に検討を行うべき点があることを明らかにした。また、社会インフラのセキュリティ強化に向け、これまで以上に強制力を持った政府や業界団体が主導する規則やガイドラインの策定、また、明確なインセンティブがある情報共有体制の必要性、日本

¹ サイバー空間 (仮想空間) とフィジカル空間 (現実空間) を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会 (Society)

https://www8.cao.go.jp/cstp/society5_0/index.html

および海外における法規制やガイドライン整備等の方向性を明らかにした。これらの調査結果を踏まえ、Cyber Physical Systemsに関する動向は把握できたものの、より広範囲な概念である Society5.0 や日々進歩する技術やセキュリティ面で強化される規制・ガイドライン動向については継続的な調査が必要といった課題が挙げられた。

3. 調査検討事項

電気エネルギーシステムなどの社会インフラシステムや産業用制御システムに関して、Society5.0 を支える IoT 機器が今後普及・拡大することを念頭に、そのセキュリティに関わる以下の事項を実施する。

- (1) SIP (cross-ministerial Strategic Innovation promotion Program; 戦略的イノベーション創造プログラム) 第一期で研究開発された技術やその適用事例、および第二期で研究開発予定の技術に関する調査
- (2) Society5.0 社会において、分野横断的に適用可能な技術 (AI, RPA (Robotic Process Automation), 監視分析技術, 次世代通信技術, 組込機器向けの技術等) のセキュリティ観点での課題の調査
- (3) 日本および海外における国家・業界のセキュリティに関する施策 (法規制, ガイドライン整備等) の調査
- (4) 上記調査によるサイバーセキュリティを取り巻く状況や問題を踏まえ、セキュアな社会インフラシステムなどの構築における課題, 対応についての考察, および情報発信や提言

4. 予想される効果

将来の社会インフラシステムのサイバーセキュリティについて、国内外の取り組みや動向などを調査・整理し、電気システム分野に携わる技術者の共通認識とすることで、今後ますます重要となる、将来のセキュアな社会インフラシステム構築における合理的な判断に資する。

5. 調査期間

2019年10月～2021年9月 (2年間)

6. 活動予定

委員会	4回/年	幹事会	必要に応じて開催
見学会	1回/年		

7. 報告形態

電気学会誌の特集記事、もしくは電気学会全国大会または部門大会のシンポジウム (企画セッション) での発表をもって成果報告とする。