2021年春の年会

核不拡散・保障措置・核セキュリティ連絡会セッション

原子力施設のサイバーセキュリティに関する現状と課題
Status and Challenges on Cyber Security for Nuclear Facilities

（1）原子力施設におけるサイバーセキュリティの現状および将来展望

―システムベンダーの立場より―

(1) Current status and future prospects of cyber security for nuclear facilities
-From the standpoints of a system vendor-

*石場　光朗[1]
[1]株式会社　日立製作所

1. はじめに

過去にはイランの核燃料生成プラントを標的とした Stuxnet ウイルスやウクライナの電力システムに対するサイバー攻撃被害などの事例があり、原子力システムや電力システムを含む重要インフラシステムでのサイバーセキュリティ脅威が顕在化している。また、原子力施設以外の産業分野では、IoT、DX の進展により産業・制御システムと情報システムとの連携や先進技術の適用が進んでおり、システムの連携や新規ソフトウェアの脆弱性を利用したサイバー攻撃の脅威が次々と出現し、産業・制御システムを含めたサイバーセキュリティ対策が喫緊の課題になっている。ここでは、他産業分野での動向および対策状況も踏まえ、システムベンダーでの立場から原子力施設におけるサイバーセキュリティ対策について、現状および将来の展望について紹介する。

2. セキュリティ対策の現状および将来展望

2-1. 脅威の動向およびリスク対策

サイバー攻撃は、個人情報や企業の機密情報の入手および金銭を目的とした攻撃が盛んである。また、事業活動の妨害を目的にインフラサービスをターゲットにした攻撃が懸念され、一部実際に攻撃されている。セキュリティ対策は、複数の事例を参考に脅威シナリオを特定し、リスクを低減させる視点が必要である。

2-2. 他産業分野での IoT、DX の進展およびセキュリティ対策状況

一方、他産業分野では IoT、DX が著しく進展している。原子力施設以外の産業・制御システムおよび情報システムも取り扱うシステムベンダーの立場より、他分野で導入が進む IoT、DX 技術の適用事例を類型化し、セキュリティ対策を検討している。このうような活動は、原子力施設に IoT、DX が導入された場合のセキュリティ対策を講じうるうえで有用である。

2-3. 原子力施設でのセキュリティ対策の現状および将来展望

原子力施設でのセキュリティ対策の現状について整理するとともに、他分野の動向も踏まえ、原子力施設における運用・保守の高度化を見据え、制御システムおよび情報システムが高度化した場合のセキュリティ対策の展望を紹介する。

3. まとめ

原子力施設における運用・保守の高度化を目指すと、他産業分野で適用されている各種先進技術が部分的かつ段階的に原子力施設に導入されていくが予想される。そういった中で、既設システムと IoT システムの共存を想定し、他分野で導入されているセキュリティ施策を参考に対策を進めていく必要がある。

*Mitsuaki Ishiba[1]
[1]Hitachi, Ltd.