資料１－２

サイバーセキュリティ対策導入自主ガイド（案）について

2019年7月23日

原子力エネルギー協議会

目次

※「サイバーセキュリティ対策導入自主ガイド（案）」を以下、「自主ガイド（案）」という

自主ガイド（案）の目的

① 我々の生活環境における脅威は自然災害やテロ等多様化しているが、特にサイバー攻撃の脅威については、マルウェアによるコンピュータの動作異常や個人情報の窃取等、個人や企業の社会全体への影響が年々増大しており、サイバーセキュリティの確保が喫緊の課題となっている。

② 国内原子力規制においては、発電用原子炉施設及び特定核燃料物質の防護に関する情報システムへの外部からの不正アクセス防止（遮断）策を講じることが規制要求となっている。

③ 海外の原子力規格であるIAEAガイドやNEIガイドは近年強化されており、ATENAは、それぞれの最新知見を踏まえ国内原子力産業界共通の基本方針や性能規定を具現化・明文化することが、サイバー攻撃の脅威に対する防護強化に有効であると考え、発電用原子炉施設のコンピュータ設備、特に、原子炉安全に関わるコンピュータ設備をサイバー攻撃から多層的に守ることを目的として、自主ガイド（案）を作成している。

サイバーセキュリティ対策に関する海外の最新知見

原子力規格であるIAEAガイドやNEIガイド及び米国NRCの法規制において、以下のように整備されている。

◎IAEAの状況

IAEAは、核物質防護対策の国際的な基本文書である「核物質及び原子力施設の物理的防護に関する核セキュリティ勧告 (INFCIRC/225/Rev5)」において、原子力施設で使用されるコンピュータシステムに対する防護要件を示し、更にその詳細を記載した、「原子力施設におけるコンピュータセキュリティ(Nuclear Security Series No.17)」を2011 年に発行、2018 年に計装制御システム向けの技術指針「原子力施設の計装制御システムにおけるコンピュータセキュリティ(Nuclear Security Series No.33-T)」を発行している。

◎米国の状況

米国NRC においては、原子力施設のサイバーセキュリティに関する法規制(10CFR73.54/Regulatory Guide5.71等)整備が進み、NEIをはじめとする産業界も対応している(NEI08-09,10-4,13-10他)。また、米国一般産業向けにはNIST文書（SP800-53）が規格化されている。

自主ガイド（案）全体構成

1．サイバーセキュリティマネジメント

- 組織及び責任
- 資産管理
- リスク及び適合性の評価
- 要員管理
- 調達管理

2．セキュリティ要件

- 多層防護
- セキュリティレベルについて

添付資料　セキュリティ対策

- セキュリティ対策の基本設計
- 技術対策例

3．運用管理

- ライフサイクルのセキュリティ
  発注(調達)／製作／輸送／運用／保管／廃棄
- 既存設備の評価

4．インシデント対応

- インシデントの判別
- 異常時の対処

設備対策　　マネジメント対策

今後の進め方

近年、サイバー攻撃の脅威が益々増大している中で、サイバーセキュリティの確保は、原子炉の安全及び核物質防護の両方の観点から重要と考えており、今後、規制当局へATENAが作成している自主ガイド（案）の内容を具体的に説明するので、ご意見をいただきたい。

自主ガイドを用いた各事業者、メーカーにおける対策実施

① ATENAは、今年9月頃目途に自主ガイドを制定し、各事業者に通知して対策実施を指示する。
② ATENAは、各事業者への通知に合わせて自主ガイド対策項目全てについて、各事業者に反映計画書の提出を要求する。
ATENAは、各事業者の計画書の内容を確認し、不十分なものがあれば事業者に必要な修正を求める。
③ ATENAは、各事業者の対策進捗状況について定期的に確認する。
④ ATENAから各メーカーに対しては、情報システムに関連する製品の製作及び輸送の段階におけるセキュリティ対策の強化を要求する。