核不拡散・保障措置・核セキュリティ連絡会セッション

核不拡散・保障措置・核セキュリティに関する研究開発の動向と今後

Present Status of R&D Activities for Nuclear Non-proliferation, Safeguards and Security

(2) 原子力施設のサイバーセキュリティターゲット同定手法の開発

(2) Development of Cyber Security Target Identification Method for Nuclear Facilities

*出町 和之[1]

[1]東京大学

原子力施設のサイバーセキュリティに資するため，放射性物質の過大放出(HRC)を発生させるシーケンスを対象にIAEA の Technical Guidance の No.16 を用いてターゲットセット(TS)を求め，サイバー攻撃の対象となる各システムの制御内容とサイバー攻撃の手段で分類することで，対象となるコンピュータを抽出した。

キーワード：サイバーセキュリティ，核セキュリティ，ターゲットセット

1. 緒言

原子力発電所の核セキュリティ事象は，悪意を持つ人間・集団による妨害破壊行為が起因となるため，その発生確率を求めて PRA に似たリスク評価を行うことは困難である。そのため，同時に機能喪失することで安全機能が失われて重大事故に至るような重要機器・設備の組み合わせ（TS:ターゲットセット）を導出し，これらを防護するための対策を講じることが必要となる。IAEA の Technical Guide（TG）である IAEA Nuclear Security Series No.16, "Identification of Vital Areas at Nuclear Facilities"では，TS への攻撃を防ぐために必ず防護せねばならない区域（PS：Protect Set）を導出するための VAI(Vital Area Identification)が解説されている。ただし，通常の VAI 手法では悪意を持つ人間・集団がその区域に物理的に侵入する場合を想定した枢要区域を導出できるが，サイバーセキュリティに対してはコンピュータネットワーク空間上の枢要区域の導出が求められる。そこで本研究では，VAI 手法をコンピュータネットワーク空間に適用し，サイバーセキュリティ上の TS を導出することを目的とした[1]。

2. 手法

VAI 手法をコンピュータネットワーク空間に適用するにあたり，サイバー攻撃の対象範囲を以下とした。

- 逆走防止効果のあるダイオード設置が考えられるため，外部からのサイバー攻撃は想定しない。
- 内部脅威者が中央制御室の端末や各所のローカルネットワークボードから攻撃を行うことを想定する。

また，サイバー攻撃により重大事故に至る機能喪失を発生させ得る手段として，次の３つを想定した。

- 安全系設備の起動信号に対する妨害
- 安全系設備の制御プログラムの改竄
- 安全対策の人為的ミスの誘発を目的とした，中央制御室モニター誤表示のためのプログラム改竄

これらの対象範囲，サイバー攻撃手段を対象に，新規制基準に示されている放射性物質の過大放出(HRC)を発生させるシーケンスを用い，BWR と PWR について TS を求めた。

3. 結論

サイバー攻撃の対象となる各システムの制御内容を各システムの運転制御を考慮して整理し，それをサイバー攻撃の手段で分類した。これにより攻撃対象となるコンピュータを抽出する手法を示すことができた。

参考文献

[1] 出町和之，「枢要区域特定手法による原子力施設のサイバーセキュリティに関する核セキュリティ研究」平成 29 年度 JAEA 委託研究報告書

*Kazuyuki Demachi[1], [1]The University of Tokyo