

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・核セキュリティに関する諸課題とその対策

Challenges and Solutions of Nuclear Non-proliferation and Nuclear Security

(2) 原子力施設においてサイバーセキュリティ事案が発生する要因と現実的な対策

(2) The Causes and Practicable Measures for Computer Security Incidents in Nuclear Facilities

名和 利男¹¹サイバーディフェンス研究所**1. 原子力施設を取り巻くサイバー環境の変化**

ここ数年、サイバー環境は国家レベルから個人レベルまで大きく変化し、社会生活や経済生活に大きな影響を与えている。これに変化の中で、原子力施設もさまざまな領域で巻き込まれ始めている。この状況を原子力施設の「外的変化」及び「内的変化」の観点で眺めると、現在及び今後のサイバーセキュリティ事案の発生を許してしまう環境が理解できる。

1-1. 外的変化

- 重要インフラを標的とした「サイバー攻撃の発生頻度の向上」
- サイバー攻撃技術の極端な高度化及び巧妙化による「検知不能領域の拡大」
- 自動制御システム計装エンジニアリングにおける「汎用的な技術及び製品」の浸透

1-2. 内的変化

- HMI 及び計測制御装置における「汎用的な技術及び製品」への依存度の高まり
- 「エアギャップネットワーク」に対する IT 情報機器のアクセス頻度の向上
- 敷地内及び施設内における電子機器及びネットワークの「共用化」

2. 主なサイバーセキュリティ事案とその発生要因

さまざまな制約や要求の厳しさが増している原子力施設において、高品質・低コスト・短納期を実現し、かつシステム稼働の安定性が確保された「汎用的な技術及び製品」の導入が段階的に行われている。この状況に、上述の外的変化及び内的変化の影響が加わることで、「通常利用する可搬記憶媒体」、「管理不足の IT 情報機器やネットワーク」そして「持ち込み電子機器」等を介したサイバーセキュリティ事案の発生可能性が高まってきている。さらに、多層請負構造の中で発生する「設置時にハードウェア内部に組み込まれたモジュール」や IT 情報機器の扱いに慣れた「施設内部の業務従事者」による不正活動に起因した事案も発生も強く懸念されている。

2-1. 「業務利用する可搬記憶媒体」を介した不正プログラムによる不正挙動

- 情報（業務）システムに対して計測・制御システムの計測データ等を取り込む等のために「業務利用する可搬記憶媒体」は、不正プログラムの展開手段として攻撃利用されることがある。その多くは、情報（業務）システムの内部に、それを実行する別の不正プログラムが検知回避された状態で存在している。

2-2. 「管理不足の設備機器のネットワーク」を介した不正侵入

- 原子力施設におけるレガシーシステム（計算機システム等）の多くは、特注の専用システムであることが多く、段階的に進んだネットワーク化された全体構成が十分に文書化されていないため、運

ユーザーがネットワークの接続形態を正確に把握できていない領域が発生している。

2-3. 「持ち込み電子機器」を介した不正侵入

- プライベート利用或いは保守管理の目的で原子力施設に持ち込まれる電子機器は、悪意のある高度なプログラムが内在されていた場合、一定条件下で非接触通信により不正侵入が成功する可能性がある。

2-4. 「調達時にハードウェア内部に組み込まれた不正モジュール」による不正挙動

- 調達時に十分な技術的審査を行っていない場合、製造或いはキッティング時にハードウェア内部に不正モジュールが組み込まれるケースが発生している。この不正モジュールは、計測・制御システムの設備を停止させてしまう可能性がある。

2-5. 「施設内部の業務従事者」によるシステムの不正操作

- 施設内部の業務従事者に対するセキュリティ文化の醸成や個人の信頼性確認制度の導入の不徹底が続いた場合、業務従事者による不正操作を許す職場環境が作られてしまう懸念がある。

3. 現実的な対策

サイバーセキュリティ事案に対する現実的な対策は、“情報（資産）”を対象とする「情報セキュリティ体制」ではなく、“設備とプロセス”を対象とする「（サイバーセキュリティ）事案対応態勢」を構築する必要がある。

3-1. 「情報セキュリティ体制」と「事案対応態勢」の違い

- 「情報セキュリティ体制」は管理策（Security Control）に基づいた各担当者の役割分担を重要視するが、「事案対応態勢」は想定事案に相応する対応行動及びその能力維持を重要視する。

3-2. 「事案対応態勢」の構築のための重要ポイント

- 全ての関係者が、徹底的な状況認識（Situation Awareness）を行うこと。
- 専任されたチームが、検知（Detect）→トリアージ（Triage）→対応行動（Respond）の各プロセスを確立及び実務能力の構築を行うこと。

3-3. 「事案対応態勢」の継続強化ためのアクションアイテム

- 状況認識（Situation Awareness）の共有や向上のために、サイバーセキュリティ事案への対応態勢関係者による定例会及び外部の専門家を招聘した勉強会を実施。
- 連絡体制の維持のために、定期的な疎通確認訓練（Communication Check Drill）或いは電話会議（Teleconference）を実施。
- 意思決定能力の向上及び最新の脅威動向の把握のために、脅威シナリオをベースにした TTX（Table Top Exercise; 机上演習）を実施。

Toshio Nawa¹

¹ Cyber Defense Institute, Inc.