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

（2）原子力施設におけるサイバーセキュリティと主観的リスク認知

(2) Cybersecurity and Subjective Risk Recognition in Nuclear Facilities

*高橋　信 [1,2]
[1] 東北大学 / [2] 制御システムセキュリティセンター(CSSC)

1. 制御システムセキュリティ

サイバーセキュリティという言葉は広くネットワーク上の情報全てに関するセキュリティを意味しているが、制御システムセキュリティはその一部であり、主にネットワークを介して制御を行っているプラントやインフラシステムへのサイバー攻撃を主に扱う。潜在的な社会への脅威という観点からは、情報漏洩等が主に問題となる情報セキュリティと比較してもより深刻な側面を持っている。現在、工場や様々な工業施設における制御システムは、いわゆるインターネットプロトコルを用いて相互に接続され管理されている。1980年代においても制御系が独自のバスにより接続され統合的に運用されるという形態は存在したが、現在では一般的なインターネットプロトコル（TCP/IP）を用いて相互接続され運用されている形態が大勢を占めている。一般的なプロトコルを利用することにより相互接続が容易になり、システム開発も加速された面があることは否めない。しかし制御システムのOSが標準化されることにより、一度OSの脆弱性が発見されると、その影響はこれまで以上に広く及ぶことになる。近年利便性を重視しネットワークがプラント内に張り巡らされるようになってはいるが、制御用システムが繋がるネットワークは外部ネットワークからは隔離されていることになっている。このような隔離によるセキュリティ対策は常識的なものであるが、内部のネットワークを外部から隔離するファイアーウォールも必ずしも完全ではなく、更には内部犯行者によるUSB等からのマルウェアの感染を防ぐことは物理セキュリティという面からも簡単ではない。原子力に関係する事例で最も重大と考えられているのがStuxnetと呼ばれるマルウエアである。ウラン濃縮施設の遠心分離機を制御するシステムがUSBを使った内部犯行によりStuxnetに感染し、その結果として遠心分離器の回転数が上昇し破損に至るという事象も発生している[1,2]。原子力プラントに関しては、制御系はメーカー固有のプロトコルが利用され、外部からは完全に遮断されているという前提でサイバーリスクは比較的低いと言われているが、デジタルアップグレードによって新しい制御系が導入される場合には、内部犯行者の可能性も含めて他の産業分野と同じようなリスクがあると考えるべきである。

3. サイバーセキュリティにおけるヒトの重要性

サイバー攻撃は明確な悪意をもった人間により意図的に行われるものであり、ヒューマンエラー等の意図しない人間のネガティブな寄与とは明確に区別される。サイバーセキュリティの問題に関しては、攻撃に対する防護策を向上させると更に攻撃がエスカレートするという難しい側面を持っており、犯罪心理学等からのアプローチも必要である。

サイバー攻撃への防御策としては、システムレベルでのセキュリティ対策が推奨されている。システム構成を堅牢にしてハードウエア的な面から防御を固めることはもちろん重要であるが、全ての考えられる攻撃にリスクに対応することは原理的に不可能であり、レジリエントなシステムを実現するには、人間の柔軟な対応能力を十分に活用する必要がある。ここで重要なポイントは、サイバー攻撃の変化は急激であり攻撃方法の新規性が高いために、従来のリスクベースの考え方（事前にリスク源を網羅的に

調査するアプローチ）での対応は不十分になる場合が多い。サイバー攻撃に対応する組織自体がレジリエントである必要がある。

加えてサイバーセキュリティに関してはヒューマンインタフェースの観点も重要な関係を持っている。一般的な制御システムにおいて Human Machine Interface: HMI は一つの重要なコンポーネントであり、オペレータは HMI を通じてプラント情報を獲得し運転操作を行う。この HMI も当然のことながらネットワークを経由して DCS(Digital Control System)やサーバーに接続されているが、この HMI と制御システム間の通信に対して攻撃を行い、正しい情報のやりとりを妨害するサイバー攻撃の形態がある（Man in the middle)。例えば、実際のプラントでは反応容器の圧力が上がっているにもかかわらず HMI 上ではその変化を表示させないようにするといった「情報詐称」という攻撃形態がある。このような攻撃は HMI の基本である情報を正しく伝えるという機能を阻害するものであり、運転員に気づかせないようにしてシステムに対してダメージを与えることを可能にする。このような攻撃に対しては、プラント全体の情報の整合性を確認するロジックとそれを的確に運転員に伝える可視化の方法が対抗策として考えられる。

4. サイバー攻撃に対するリスク認知の重要性

インターネット利用による利便性が向上すればするほど、サイバー攻撃のリスクも増大する。現実にも数多くの攻撃の事例が報告されているが、現在日本におけるサイバー攻撃に関するリスク認知は極めて低いと言わざるを得ない。今後、電気やガス等の主要なエネルギー供給システムがインターネットで相互接続された場合、サイバー攻撃によって引き起こされうる社会への影響は極めて大きい。テロリストによるスマートメーターへのハッキングに端を発する欧州での大規模停電の可能性を描いた小説「Black Out」は、サイバー攻撃が引き起こしうる悪夢のような惨状をリアルに描いている[1]。サイバー攻撃に対してレジリエントなシステムを構成するために、それに見合うコストを掛ける必要がある。しかしながらサイバー攻撃により引き起こされるインシデントによる具体的なリスクが見えにくいために、サイバー攻撃には対するリスク認知が低くなり､その結果としてサイバー攻撃に対する対策のための投資に対して積極的に取り組まないという傾向が生まれる可能性がある。更に、全ての人間は「認知バイアス」を持っており、的確にリスクの程度を認識することは極めて難しい。特に、攻撃の形態が多岐にわたるサイバー攻撃に場合は、現実的にリスクを認識すること自体が困難な場合多い。

講演では人間の認知バイアスの具体的な例を示し、その負の側面を認識しながらも、最終的には人間中心のサイバー攻撃に対するレジリエンス向上に向けた方策について述べる。

参考文献

[1] 日本シーサート協議会: マルウェア Stuxnet(スタクスネット) について,
http://www.nca.gr.jp/2010/stuxnet/, 2010.
[2] ニューズウィーク日本語版：産業サイバー兵器スタックスネットの防ぎ方,
http://www.newsweekjapan.jp/stories/world/2010/10/post-1683.php, 2010.10
[3] マルク・エルスベルグ (著), 猪股 和夫 (訳),ブラックアウト (上/下), (角川文庫),2012.

*Makoto Takahashi[1,2]
[1]Tohoku Univ., [2]Control System Security Center (CSSC)