



制御システムセキュリティの考え方と コア人材の育成

名古屋工業大学 社会工学専攻 助教

あおやま ともみ
青山 友美



1. 制御システムを狙ったサイバー攻撃

2010年のStuxnet、2012年のBlackenergy2、2013年のHavexに続き、産業制御システム（ICS）を狙ったサイバー攻撃は増加している。2016年にはCRASHOVERRIDE（クラッシュオーバーライド）によってウクライナで停電が発生した。また、2017年11月には産業制御システムのなかでも、プラントの運転に必要な安全を担保する安全計装システムを狙った初のマルウェアTRISISが発見された。

また、情報システム（IT）を基盤とした企業ネットワークと、制御システムを含む、プラントの運用に必要なOTネットワークの境界が曖昧になり、OTネットワークがITの脅威にもさらされるようになった。2016年に世界中のIT機器で感染が観測されたWannacry・NotPetyaは、制御系でも利用されるSMBプロトコルが感染経路に利用されたこともあり、OTネットワークまで被害が拡大した。デンマークの大手海運業者Maersk社は、3億円の経済被害が発生、IT・OTネットワークの大部分の交換・再構築を余儀なくされたと報道されている。

2018年上半期には、アメリカの電力業界を狙ったロシアからのAPT攻撃が観測されている。ベンダー・ITサービスプロバイダ・政府機関を踏み台とし、幾つものノードを得て標的である電力事業者へ侵入した上、事業者で利用されている制御システムの情報収集を行ったとされている。サプライチェーン上の脆弱なノードが攻撃に利用されるケースは今後も増えると考えられる。

2. 制御システムを狙ったサイバー攻撃によるインパクト

ITシステムを狙った攻撃と、制御システムを狙った攻撃では、発生するインパクトが異なる。Krotofilら（2015）はその影響を下記の3つに分類した。

・機器・計装へのダメージ

不安定なプロセスは、機器へのストレスを増大させ、製品寿命を短縮させる。イランのウラン濃縮施設を狙ったサイバー攻撃Stuxnetは、特定のシステムにおいて遠心分離機の圧力を増大させ、かつ回転速度を上下させるようにデザインされていた。これは、超過ストレスを意図的に発生させることによる機器故障、そしてそれによる生産・開発の遅延を目的としていた。

また、意図的に安全限界を超過させることで、機器の破

損を発生させることが可能になる。例えば、バルブを急に閉止させることによってウォーターハンマーという現象を引き起こし、配管の耐性を超える衝撃によって物理的な被害をもたらすことが可能である。

・生産へのダメージ

物理的な被害のほか、製品の生産過程に影響を及ぼすことも考えられる。配合などのパラメータ変更を行えば、品質・製品率へ影響を及ぼす。これによって、意図的に製品の欠損率を増大させ、製品の市場価値を下げることも可能となる。また、同様にパージにおける原料の損失を増やしたり、触媒を不活性化させることによって、運用コストを増大させることも可能である。また、メンテナンス作業負荷を増やすことによって、生産スケジュールへ影響を与えることも考えられる。例えば、流量バルブを急速に操作すると、キャビテーション（空洞現象）が発生する。これは、流体中に気泡を形成させ、バルブの消耗、液体漏れを発生させる。これは、気泡によってプロセス制御が複雑になるほか、バルブ交換の手間を発生させる。

・コンプライアンスへのダメージ

物理的被害及びオペレーションコストへの影響に加え、安全被害、公害の発生による環境安全への被害及び生産の遅延による契約違反の発生が考えられる。

上記のように、ICSを狙った攻撃は、機器の破損のみならず、プラントの操業に影響を与えることが可能である。

3. 従来の安全対策の限界

プラント制御においては、安全解析に基づく予防対策実施が定着している。ここでは、従来の安全対策の範囲内でサイバーインシデントを防ぐことが可能かを考察する。

リスクの評価は、システム・損害の定義の下にハザードの同定を行い、そのハザードの発生構造をモデル化し、発生確率を定量化することで実施される。ハザードの同定に用いられる方法として、HAZOP（Hazard and Operability analysis：ハゾップ）がある。HAZOPは、プラントの運転状態における「設計意図からのずれ」を導出することで、プロセス異常状態を導き出す方法である。例えば、「流れ」のような設計・運転パラメータに対し、「なし/多い/少ない」などのHAZOPガイドワードを組み合わせて、「流れなし」という正



常な振る舞いから逸脱した状態を抽出する。これを、1つのラインにあてはめてプロセス異常の原因と影響・結果の考察を行う。HAZOPの特徴として、潜在的な危険性を洗い出すことができる、その網羅性の高さが挙げられる。

ハザードの発生構造のモデル化に用いられる方法に、FTA (Fault Tree Analysis: 故障の木解析) が挙げられる。FTAは、システムにとって望ましくない事柄をトップ事象として取り上げ、その発生に至る道筋をトップダウンで展開する方法である。原因事象に発生確率を付与することで、トップ事象の発生確率の定量化を行うことができる。

2章で述べたサイバー攻撃によっておきる影響は、事故や故障によっておきる影響と変わらない。つまり、従来の安全対策で防ごうとしている事象と同一である。しかし、サイバー攻撃と事故の違いは、発生までの過程に「悪意」が含まれている点である。

例えば、対策済みのプロセス異常でも、同時に複数起きることで大事故につながる可能性がある。ガス処理施設などで見られる余剰ガスを焼却するための塔（フレアスタック）は、バーンを伴うプラント停止手順をうまく計画する前提で処理量を小さくして効率化されている。一度にバーンが集まると、フレアスタックの処理量を超えて不安全な状態になる可能性がある。また、プロセスが正常であっても、オペレータが見ているプロセス監視画面上が偽装されれば、オペレータが正しい判断をしているつもりでプロセスに変更を加えてしまう可能性がある。

このような悪意の操作による同時多発や偽装は、これまでのリスク評価に含まれていない。つまり、これまでの安全対策の徹底では、セキュリティリスクの発生まで防止できない可能性がある。

4. 自動化の落とし穴ー現場力の低下

20世紀後半、第三次産業革命によって多くのシステムの自動化が進んだ。それまで隔離されていたプラントのネットワークも、情報技術によってプロセスのリモート監視の導入や受注生産の効率化が進んだ。また、自動化によってオペレーターの作業負担も減り、少ない人員で大規模なシステムの安定した運転ができるようになった。

しかし、危険物施設における火災・流出事故の総事故数は、施設数が減少しているにもかかわらず1994年と比べてほぼ倍増している。また、その内訳を見ると火災事故の約半数、流出事故の約3分の1が人的要因による事故とされている。また、過去に起きた爆発火災事故は、非定常運転時に熟練オ

ペレータの立会下発生している。

設備の高度化により定常運転時のオペレータの負担が減ったことによって、最小限の知識・スキルでも運転ができるようになったと言える。しかしそれは同時に、稀となったトラブルへの対処力や、状況認識力の低下を招いている。また、第三次産業革命時代を支えた作業員の多くは定年を迎え、作業員の世代交代が進んでいる。情報システムが3年から5年で切り替えられるのに対し、制御システムは平均でも10年から15年と言われている。中には30年を超えて利用されるコンポーネントもあり、現場担当者よりも長く現場で活躍する場合もある。熟練オペレータが経験とともに蓄積した知識をどのように継承するかが課題である。さらに、多品種少量生産型のプラントが増え、システム構造の複雑化が進み、以前にも増して運転員ら現場担当者に求められる知識レベルは上がっている。これまでの安全文化を支えてきた「現場力」に、セキュリティ事象への対応まで頼り切ることができないのが現状である。

5. リスク再考の必要性

制御システムにおけるセキュリティリスクは、安全リスク・経営リスクと密接に関係している。しかし、従来の情報セキュリティ対策は、流感にかからないように手洗い・うがいを徹底するように、流行りの攻撃ベクトルへの対策や定期的なセキュリティパッチ当てなどルーチン対策とルールを徹底する「サイバー空間の衛生」に焦点を当てがちであり、非標的型攻撃への対策でしかない。これだけでは、高度な標的型攻撃への対応や、サイバー攻撃によってプラントのオペレーションに被害が出る可能性まで議論できていないとは言えない。セキュリティリスクが発生することを防ぐためにセキュリティリスク単体で議論するよりも、これまでの安全・経営リスクの要因のひとつとしてセキュリティリスクに起因するその影響に焦点を当ててリスクを再考する必要がある。

セキュリティリスクの考え方の見直しは国内外で進んでおり、2016年に米国アイダホ国立研究所 (Idaho National Lab: INL) は制御システムセキュリティを発生確率中心でなく、結果事象中心で考える防御戦略のフレームワークを発表している。CCE (Consequence-driven Cyber-informed Engineering) と呼ばれるこのフレームワークは、4つのステップで構成されている。まず、第1ステップとして経営の視点に基づいて結果事象の優先順位付けを行う。組織のミッション達成に必要な基幹機能・サービスを特定し、企業にとって「起きたら困ること=コンセクエンス」の順位を決定する。これは、企業としての社会的使命（機能保証）や、火災や爆発などの安全に



関わる影響や、経済損失などを含め多角的に評価する。次に、第2ステップとして、安全の視点でシステムの分解を行う。第1ステップで定めた基幹機能・サービスの実施に影響を及ぼす重要システム・デバイス・コンポーネントを、システム分解によって特定する。このプロセスは、システム工学に基づいて実施することが可能であり、FTAなどこれまでの安全解析で培った方法論で展開することが可能である。この時点では、システムの関連性にのみ着目し、事象の発生要因（故障・事故・ヒューマンエラー・サイバー攻撃など）の絞り込みは行わない。そして、第3ステップではじめて、サイバー攻撃の特徴である攻撃者の「悪意」の視点で結果事象を基に対象の絞り込みを実施する。組織が想定する脅威エージェントのアセスメントを基に、標的システムに特定の影響を与える方法を、“How（=どのようにして達成可能か）”の視点で分析する。結果事象につながるどのノードが、どのように利用されるかを議論することにより、キルチェーンが特定される。最後の第4ステップでは、セキュリティの視点で、第3ステップで特定されたキルチェーンのプロセスを防ぐための対策を実施する。このフレームワークでは、実施するセキュリティ対策が、どのような攻撃に対し効果を発揮するか、費用対効果の見通しがききやすい。システム全体を見渡しながらセキュリティ対策の実施を行うことができる。

6. 制御システムセキュリティに求められる中核人材

5章で紹介したCCCEのフレームワークは、制御システムに対するセキュリティ対策を考える上で、どのような視点を持つ人材が必要かを示唆している。対策を進めるには、情報セキュリティの知識だけ、または制御システムの知識だけでは不十分である。組織の中核となる人材として、ITシステムと制御システム双方の知識・スキルをベースとした上で、サイバーセキュリティ対策の必要性を組織の経営リスク思想で議論できる力が求められる。2017年、IPA（情報セキュリティ推進機構）内に設立された産業サイバーセキュリティセンターでは、このような人材を将来企業の経営層と現場担当者をつなぐ「中核人材」の理想像とし、1年間かけて社会インフラ・産業基盤事業者の若手人材を育成する中核人材育成プログラムを提供している。

7. 名古屋工業大学制御システムセキュリティワークショップの歩み

名古屋工業大学では、プラントの操業現場に必要なセキュリティの在り方を議論し、制御システムセキュリティの定着化を

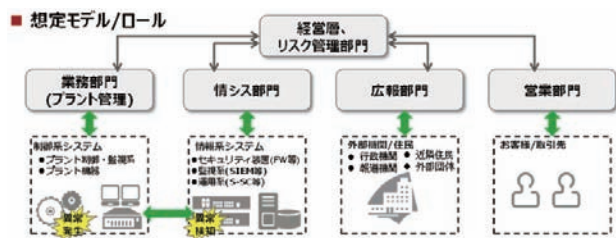


図1. 名古屋工業大学制御システムセキュリティワークショップの歩み

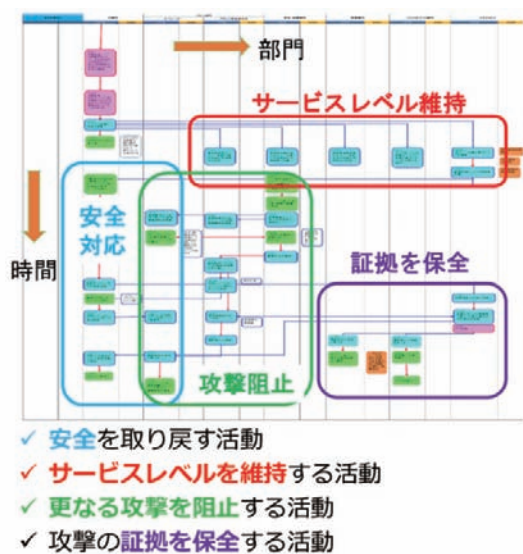
推進することを目的とし、制御システムセキュリティワークショップを2015年より実施している。過去6回開催し、制御システムベンダー・ユーザー企業・セキュリティベンダー・政府機関などから累計約260名（140組織）が参加した。

大学で保有する水循環プラントを模擬したデモシステムを基に制御系を狙ったサイバー攻撃のデモンストレーションを実施した第1回に始まり、第2回から第4回までの机上演習では、テストベッドの構成を基にした仮想企業におけるインシデント対応を予兆・緊急対応・復旧の3フェーズに分けて参加者グループで議論し、仮想企業の各部門が取るべき対応を時系列にスイムレーン図で記述する形式をとった。机上演習の結果、どのグループもプラントの挙動に基づいてオペレータのリモート監視画面と現場機器のクロスチェックや、自動制御からローカル制御への切り替えなど、安全対応に必要な操作を迅速に行うことができていた。安全を取り戻すための対応については、習熟していると言える。しかし、異常の原因がサイバー攻撃であると判明して以降の対応では、後方支援を担う部門との連携の在り方や、意思決定機関などに各グループばらつきが見られた。安全に関する意思決定は順調にできても、セキュリティや、経営に関わる意思決定は現場での情報だけでは実施できない。プラントの構成に依存する安全対応と異なり、各企業の組織構成や意思決定構造に合った対応体制を構築することが必要である。

インシデント対応においては、特にIT部門と制御システムを運用する現場が密接に連携する必要がある。しかし、IT技術者は制御ネットワークの状態やプラントの状況が分からず、早期検知にはOT技術者の物理的な変化の検知が頼りとなる。また、現場からIT技術者へ早期に異常状態を伝達できたとしても、お互いの対話プロトコルが合っていないと必要な対応につながらない可能性がある。例えば、「制御ネットワーク内の機器に対して通信のリトライが発生している」と現場



■図2. 机上演習で想定した仮想企業の構造



■図3. 机上演習で利用したワークシート

へ伝えても、それが今現場で起きている異常とどう関係するのか、OT技術者に認識されない可能性がある。運転、計装、設備、情報ネットワーク等の文化内での用語を他文化の人にも有用にするためのプロトコル合わせも対策として重要であると言える。第5回目以降のワークショップでは、この部門間のコミュニケーションの在り方をロールプレイ形式で体感できるチャットシステムを開発し、このシステムを利用した演習のシナリオ作成から実施までを行っている。

8. おわりに

現在プラントで利用されている制御システムの多くは、セキュリティの概念なしに設計されている。このようなシステムを脅威から守るには、情報セキュリティと連携しながら、経営リスク思想でバランスの良い対策を考える必要がある。情報セキュリティ部門・プラントの運用部門・経営層の連携を可能にする、コア人材が必要である。そして、安全文化が定着していったのと同様、セキュリティの考え方もプラント運転に必要な基礎知識として現場担当者に定着させていく努力が必要である。

参考文献

- ・ Dragos Report INDUSTRIAL CONTROL SYSTEM THREATS
<https://www.dragos.com/yearinreview/2017/>
- ・ Maersk had to reinstall all IT systems after NotPetya infection
<https://www.itnews.com.au/news/maersk-had-to-reinstall-all-it-systems-after-notpetya-infection-481815>
- ・ Marina Krotofil, Jason Larsen, Rocking the pocket book: Hacking chemical plants for competition and extortion, white paper, DefCon23, 2015.
<https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/DEFCON-23-Marina-Krotofil-Jason-Larsen-Rocking-the-Pocketbook-Hacking-Chemical-Plants-WP-UPDATED.pdf>
- ・ ウォーターハンマー発生メカニズム
https://www.tlv.com/ja/steam_story/0902water_hammer1.html
- ・ 高度化する設備と作業員の技能レベルが乖離 工場事故多発で化学業界が得た苦い教訓
<http://diamond.jp/articles/-/29207>
- ・ 危険物施設における事故発生件数の推移等
http://www.fdma.go.jp/neuter/topics/houdou/h29/05/290530_houdou_3.pdf
- ・ HAZOP&プラント安全促進協会
http://hazop.jp/hazop_basic.html
- ・ 安全分析基礎とその説明手法の紹介
<https://www.ipa.go.jp/files/000046844.pdf>
- ・ 故障の影響解析 (FMEA) と、故障の本解析 (FTA) の活用
http://www.jspmi.or.jp/system/l_cont.php?ctid=130403&rid=831
- ・ 後藤伸寿、重盛正哉。“フォールトツリー解析及びイベントツリー解析によるリスク評価の事例。” みずほ情報総研技報 (2015): 33-40.
https://www.mizuho-ir.co.jp/publication/giho/pdf/007_06.pdf
- ・ Freeman, Sarah G et al. Consequence-driven cyber-informed engineering (CCE). doi: 10.2172/1341416.
<https://www.osti.gov/biblio/1341416>
- ・ Consequence-driven engineering needed for critical systems and processes
<https://www.controleng.com/single-article/consequence-driven-engineering-needed-for-critical-systems-and-processes/e0b51f03f18d3175a71bb23ce438d880.html>
- ・ IPA 中核人材育成プログラム
https://www.ipa.go.jp/icscoe/program/core_human_resource/index.html