巻頭言
Foreword

Cyber security インシデントとプラントオペレーションのリスク

工学院大学 名誉教授　**木村　雄二**
Yuji Kimura

2024年2月5日衆議院予算委員会での質疑応答によれば、日本国内の政府機関等へのサイバー攻撃の件数は2023年4月からの半年で、政府機関120件、政府関係法人132件（JAXAを含む）であることが報告されている。

通常、リスク評価には脅威の発生可能性と望ましくない結果の重大性を縦・横軸にとりリスクマトリックスを作成しリスクレベルを評価するのが基本となるが、Cyberインシデントの場合には、これらに加えて、脆弱性ならびに標的の魅力度が追加され、リスクは4つの鍵となる要因に基づいてアセスメントされるのが常である。

このようにして、実際にサイバーセキュリティのリスク・アセスメントを行う最初のステップの1つとして、調査に適した手法を選択することが挙げられ、アセスメントの目的（リスクの同定または設計確認）と詳細さのレベル（定量的または定性的）に基づき、多くの異なるアセスメント手法が選択されている。

Cyber securityの管理の必要性の認識の醸成を背景として、一部のPSM（Process safety management）ガイドラインの中にもSM（サブマネジメント）の要素としてCyber securityが取り入れられる状況が実現しており[1]、また新たな経済産業省の化学コンビナート認定制度の認定要件の第4番目に「Cyber securityなど関連リスクへの対応」が明示された[2]。

したがって、今後、認定プロセスの中でCyber securityが実際にどのように取り扱われていくのかについては多方面から注目されている。

これと時を同じくしてCCPSから出版された“Managing Cybersecurity in the Process Industries: A Risk-based Approach”の翻訳書である「プロセス産業のためのサイバーセキュリティ：リスクに基づくアプローチ」が化学工学会 安全部会 監修・濱口孝司 訳で丸善から出版され、出版記念講演会が本年3月7日に開催された。

同書籍では、産業用オートメーションおよび制御システム（IACS: Industrial automation and control system）が、従来のITネットワークと、より密接に統合され続けるなか、システム設計の間に、IACSが直面する固有のリスクと難題を適切に考慮することが重要であることを述べている。また、設計プロセスにおいて適切なセキュリティを適用するには、ITとOTのリスク・マネジメント戦略の違いを理解し、関連するプロセス安全技術をレビューし、さらには、多重防御、ネットワーク分割、システム・ハードニング（堅牢化）、セキュリティ・モニタリングなど、サイバーセキュリティのベスト・プラクティスを実装することが要求されることを指摘している。

したがって、堅牢なサイバーセキュリティ・マネジメント・システム（CSMS：Cybersecurity Management System）の開発とプロセス安全との統合、すなわち安全とCyber securityに対する統合的なアプローチの実装がどのように実現されるかについてこれからも注視して行きたい。

参考資料

1）公益社団法人 化学工学会 安全部会 編，業務に基づくプロセス安全ガイドライン，化学工業日報社，2022.
2）https://www.meti.go.jp/shingikai/sankoshin/hoan_shohi/koatsu_gas/pdf/024_01_00.pdf

公益財団法人総合安全工学研究所 理事・監事

理事長	田村昌三	東京大学名誉教授	
専務理事	中村　順	(公財)総合安全工学研究所	
常務理事	新井　充	東京大学名誉教授	
常務理事	福富洋志	大阪大学特任教授	
理事	小川輝繁	横浜国立大学名誉教授	
理事	高木伸夫	システム安全研究所	
理事	谷　質生	日油技研工業(株)川越工場長	
理事	三宅淳巳	横浜国立大学教授	
理事	安原　洋	東京大学名誉教授	
理事	若倉正英	(特非)保安力向上センター常務理事	
監事	河野晴行	(公社)日本煙火協会専務理事	
監事	田中保正	元(一社)日本芳香族工業会専務理事	