SE Report

セーフティやセキュリティにおけるリスクの受容とは？

名古屋工業大学名誉教授
IPA 産業サイバーセキュリティセンター専門委員
橋本　芳宏 *Yoshihiro Hashimoto*

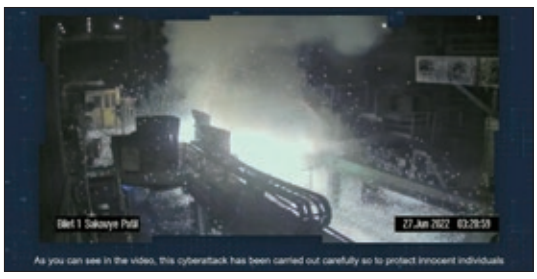
1. プラントが危ない？

本稿では、プラントの操業現場の安全を破綻する可能性があるサイバー攻撃のリスクをどのように評価し、対応するかという課題に、この雑誌の読者である安全担当のみなさんがどう加担すべきかを論じる。

サイバー攻撃は、悪意からなるもので、従来の安全対策で対象としてきた誤動作、不動作、誤操作などとは異なり、周到に準備して同時に多箇所に多様な攻撃を行うことも考えられる。その一例として、2022年にイランの製鉄所で起こったサイバー攻撃を見ていただきたい。**図1**は、犯行グループがX(Twitter)に投稿した動画の一場面である。Gonjeshke Darande Iranian Steel で検索すると、このXへのリンクが得られるので、ぜひ、動画を再生してチェックしていただきたい。

製造現場の監視カメラをのっとり、攻撃のタイミングを見計らって、製造ラインの制御装置を操作している。それにより、溶鉄が撒き散らされて、消火放水が始まっている動画が、犯行声明と共に、犯行当日にXに投稿された。

図１　イランの製鉄所へのサイバー攻撃の動画（Xより）



2010年に Stuxnet というマルウェアが、イランの核燃料施設の遠心分離機を破壊し続けたことをご存じの方は多いと思うが、イランは被害にあうだけでなく、彼らもサイバー攻撃を他国に対して実施しており、サイバー戦争真っ只中の国であるので、このイランの製鉄所が、日本の製造現場よりサイバーセキュリティの意識が低かったといえるとは思えない。

日本のプラントは大丈夫なのだろうか？

2. 大丈夫って？

はて、ここで素朴に「大丈夫？」という疑問を呈したが、安全の専門家としては、どう答えるのであろうか？

安全の世界では、すでに様々な事故を経験しながら、事故を防止するシステマティックなアプローチが開発されてきた。機器の故障率や人間の誤判断、誤操作の発生確率も数値的にとらえて、故障があっても、誤操作があっても、事故に至らないように対策をとった結果の残存事故発生確率を算出して、その発生確率が、運用するうちに悪化してしまわないように運転・保全を管理することが、すでに実現されていると理解している。

安全対策においては、事故の原因は、装置の故障や作業員の誤りだけでなく、台風、地

震や津波、火山噴火などの自然災害も考慮され、そのプラントの立地やレイアウトまで対策設計の考慮対象になっている。**表1**のリスクマトリックスに示すように、深刻な被害が発生するシナリオでは、発生頻度が非常に低くなるように､深刻ではない事故に関しては、発生確率はそれほど低くなくてもよいように、そのプラントへの安全対策を設計する。

3. 事故の発生確率って？

安全における事故の発生確率を算定する手法としては、LOPA（Layer Of Protection Analysis）がよく知られている。安全対策は、独立で多重な防御層で構成されており、一つの防御層では守り切れなくても、次の防御層があり、それが機能すれば、深刻な被害を避けることができる。全体で、事故の発生確率を、ALARP（As Low As Reasonably Practicable）なレベルまで、低減する防護層の設計を実施する。

4. サイバー攻撃の確率って？

サイバー攻撃の場合、人間の悪意を発端としているので､新たな手口が発明され続ける。セキュリティ対策自体も攻撃対象になり、その有効性を維持し続けることも容易ではなく､新たな対策も高頻度で開発される｡セキュリティパッチの対象である脆弱性は、システム開発者のミスというよりも、サイバー攻撃者の発明というべきものも少なくなく、たとえセキュアに開発していても発生してしまうものだという認識が必要である。

例えば、冒頭で示したイランの製鉄所を襲ったようなサイバー攻撃が自社のプラントを襲う確率って、どう考えたらいいのであろうか。

厳密にいえば、サイバー攻撃の発生確率の算出は無理という結論が最も適切であると考える。

制御システムセキュリティの国際標準である IEC 62443では、Security Level を、防御可能な攻撃者の能力に応じて**表2**のように分類していて、発生確率ではなく、どれくらい高度な攻撃に対応できるように防御するかを検討することを提唱している。

この基準をもとに、原子力発電所なら、SL4が求められるけど、うちの企業であれば、SL2の防御でいいのではないか、めざすとしても SL3だけど、まだ先でいいよねというような議論がされることになる。しかし、安全第一をうたっている企業でも、それでよいのだろうか？

プロセス安全の中心的な存在である CCPS/AIChE（Center of Chemical Process Safety/American Institute of Chemical Engineers）から2022年4月に出版され、2024年1月に翻訳本が発行された「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

表１　リスクマトリックス

		重大度→				
		1	2	3	4	5
↑発生可能性	Very High					
	High					
	Medium					
	Low					
	Very Low					

表２　セキュリティレベル（IEC 62443）

Security Level	セキュリティ対策技術的評価
SL4	巧妙な手法、拡張リソース、産業用制御システムに特化したスキルを有し、かつ高い動機を持つ攻撃者による意図的なセキュリティ違反から保護できる。
SL3	巧妙な手法、中程度のリソース、産業用制御システムに特化したスキルを有し、かつ中程度の動機を持つ攻撃者による意図的なセキュリティ違反から保護できる。
SL2	単純な手法、限られたリソース、一般的なスキルを有し、かつ低い動機を持つ攻撃者による意図的なセキュリティ違反から保護できる。
SL1	偶発的なセキュリティ違反から保護できる。
SL0	セキュリティ保護がない。

ローチ」[1] では、サイバー攻撃のリスクをプロセス安全のリスクと同様のアプローチで評価する方法（以下では、CS-LOPA 法[1] と呼ぶことにする）が提案され、その付録 B において、具体的なプロセス例で解説されている。

そこでは、サイバー攻撃者の能力に応じて、攻撃の発生確率が異なるとして、**表3**に示される整理が示されている。すでに筆者が無理とコメントしたサイバー攻撃の発生確率に数字を設定しているのである。

5. 受容可能な発生確率って？

サイバー攻撃により発生する事故の受容可能な発生頻度は、**表4**のように重大度（被害の深刻度）を基準に定める。

このアプローチ自体は、安全解析の LOPA と共通であり、この受容可能とする数値が、国際標準や国の規制で決まっているわけではないのも、安全と共通である。

ALARP では、受容できないレベルを満たしたうえで、Reasonably Practicable をめざすとしている。安全では、過去の多くの事故の経験から、消防法や環境規制などで、さまざまな数値規制が与えられていて、その数値を満たさないことが受容できないレベルと想定できる。

しかし、世界的にみても、サイバー攻撃で非常に深刻な人身被害、環境汚染が発生した例はまだなく、テロ等の手段にされてはなら

表 3　発生可能レベル（CS-LOPA 法[1]）

サイバー攻撃発生可能性	
VH	非常に高い（内部の非意図的、非標的） 年間10回以上
H	高い（攻撃スキルを持たない標的型） 年間1回程度
M	中程度（攻撃スキルを持った標的型） 年間10^{-1}回程度
L	低い（国家的） 年間10^{-2}回程度
VL	非常に低い（通常、対策後のみ） 年間10^{-3}回程度

表 4　被害重大度と受容可能発生頻度（CS-LOPA 法[1]）

重大度レベル	重大性の側面			許容可能な事故発生頻度
	ビジネス	環境	安全	
1	軽微な影響を生じる侵害（5万ドル未満）	環境に軽微な影響を生じる侵害	安全に軽微な影響を生じる侵害	1.00×10^{-2}/y
2	アクセスが妨害され、ビジネスに軽微な悪影響が生じる（5万～100万ドル）。	アクセスが妨害され、制御を監視できず、環境に軽微な悪影響が生じる。	アクセスが妨害され、制御の停止で設備に軽微な悪影響が生じる。	1.00×10^{-3}/y
3	情報漏洩が発生し、ビジネスに中程度の悪影響が生じる（100万～2500万ドル）。	制御が不調になり、一時的に放出、および数週間での浄化	制御の誤動作で、記録すべき傷害が生じる。	1.00×10^{-4}/y
4	ビジネスに大きな悪影響が生じる（2500万～1億ドル）。	一時的な環境破壊と、数か月から数年間での浄化	単独のオンサイト死亡事故	1.00×10^{-5}/y
5	ビジネスに重大な悪影響が生じる（1億ドル以上）。	重大な環境破壊、10年以上での浄化	複数のオンサイト死亡事故	1.00×10^{-6}/y

ないという意識で、法的にもサイバーセキュリティが取り入れられるようになってきているが、具体的な数値規制はない。

高圧ガス保安法の改定[2]においても、サイバーセキュリティが必須になり、継続的な取り組みが必要とされているが、ここまでやっていれば、事故が起こっても私の落ち度ではないとする基準を設定することは難しい。

ALARPでは、その実現可能の観点には、技術的な問題だけでなく、経済的な側面も含んでいるため、Reasonably Practicableは意思決定者であるその企業のものであり、たとえ、他の機関がLOPAの結果を認証したとしても、認証したのは、その数値ではなく手続きの適切さである。

また、事故が発生したときに、事故原因の発生確率（例えば地震の発生確率）が適切であったかを論じても、その検証は難しい。たとえ、1000年に1回の確率だからといって、今日発生しないと言っているわけではない。想定する原因によって、低減するのに必要な対策の厳重さが異なることを調整するパラメータでしかないと考えられる。

その意味では、**表3**に示すサイバー攻撃の発生確率も、攻撃により要求される対策の差異を表現していることになる。高度なサイバー攻撃者は、襲ってくる確率が下がるので、発生する事故が同じ重大度であれば、必要となる対策による低減は少なくて済むことになる。しかし、高度な攻撃者であるほど、その攻撃シナリオにおいて想定する被害の重大度は大きくなるはずなので、結果として、より厳重な防護をすることになると考えられるが、要求される対策による低減は、**表3**と**表4**から求められる攻撃発生確率と受容可能な事故発生確率の相対値により定まる。

6. 対策の効果の計算

サイバー攻撃に対する事故防護の対策としては、ファイアーウォールやホワイトリストなどの情報セキュリティの対策以外にも、入退室の警備などの物理的セキュリティ対策や、安全弁やリレーによる緊急遮断装置のような情報システムを利用しない安全対策も有効である。これらの対策の効果を、CS-LOPA法[1]では、**表5**のように整理している。

表6にCS-LOPA法[1]で作成されるリスクアナリシスのスプレッドシートの一部を示す。この表では、3つのシナリオに対する残存リスクを算出している。残存リスクが1を超えるシナリオに対してはさらなる対策を検討することになる。なお、紙面の制約のため、**表6**ではスプレッドシートを三分割して掲載していることに注意していただきたい。

この表での整理の有用性は、どのような対策がどのような効果を目指して設置され、管理されているかが、明記されていることであり、数値の正確さではない。

そして、被害が発生するシナリオは数多く考えられるが、重大なものから検討することがCS-LOPA法[1]では提唱されている。起こっ

表5　対策の効果評価の例（CS-LOPA法[1]）

対策	発生可能性レベルの低減
各々が個別のアクセス・アカウントを持つ。必要な担当者のみにアクセス権を制限する。アクセス権は毎年レビューされる。	1段階低減（10の−1乗）
基本制御システム用エンジニアリング・ワークステーションは、必要な担当者のみがアクセスできるように、鍵のかかったキャビネットに保管されている。	1段階低減（10の−1乗）
DMZ（DeMilitarized Zone）が業務ネットワークと制御システムネットワークの間に設置され、DMZと制御ネットワーク間には、ファイアーウォールが設定されている。	1段階低減（10の−1乗）
基本制御システム用PLC（Programable Logic Controller）のアプリケーション・プログラムに未承認の変更がなされていないか、毎年レビューする。	0.5段階低減（10の−0.5乗）
反応器に圧力安全弁が設置されており、圧力制御に障害が発生した場合を想定したサイズになっている。	2段階低減（10の−2乗）

表 6　Cyber Securty-PHA/LOPA で作成した解析表例

脅威ベクトル	シナリオ	攻撃者スキル	発生可能性	望ましくない結果	カテゴリ	重大性	受容可能発生確率	リスクレベル	攻撃発生確率
ソーシャル・エンジニアリング	スキルをもった攻撃者によるフィッシング活動により制御システムの認証情報が搾取された。	3	M	基本制御用エンジニアリグ・ワークステーションの侵害により、制御用 PLC のプラグムが改ざんされ、圧力制御が破綻する。劇毒物の環境への放出、さらに装置破裂によるオンサイトでの複数の死者が発生する可能性がある。	安全	5	10^{-6}/y	4	0.1/y
物理的アクセス	協力会社が意図せずにランサムウェアに感染した機器を基本制御のエンジニアリング・ワークステーションに接続した。	0	VH	ランサムウェアにより制御システムが利用できなくり、操業を停止して制御システムの入れ替えなど対応完了までのコストと操業できなかった損失が発生する。	ビジネス	2	10^{-3}/y	3	10/y
ソフトウェア	システム・アップグレードの際に基本制御用エンジニアリング・ワークステーションで WEB サーバが稼働し、スキルのない攻撃者に対してもシステムが脆弱になる。	2	H	基本制御用エンジニアリング・ワークステーションの侵害により、制御用 PLC のプログラムが改ざんされ、圧力制御破綻する。劇毒物の環境への放出、さらに装置破裂によるオンサイトでの複数の死者が発生する可能性がある。	安全	5	10^{-6}/y	4	1/y

標的の魅力	乗数	被害人員	人員所在率	対策1	効果	対策2	効果
影響が大きい	3	現場パトロール	0.1	安全弁のサイズが圧力制御不調が想定されたサイズになっている	0.01	PLC のプログラムが未承認に変更されていないか毎年レビューされる	0.3
影響が大きい	3			基本制御用エンジニアリング・ワークステーションを必要な担当者のみがアクセスできる鍵のかかったキャビネットに保管する	0.1	各人が個別のアクセスカウントをもち、必要な担当者にのみアクセス権があたえられていて、アクセス権は毎年レビューされる	0.1
影響が大きい	3	現場パトロール	0.1	安全弁のサイズが圧力制御不調が想定されたサイズになっている	0.01	基本制御用エンジニアリング・ワークステーションを必要な担当者のみがアクセスできる鍵のかったキャビネットに保管する	0.1

対策3	効果	対策4	効果	対策後発生確率	残存リスク
情報システムと制御システム間の DMZ が制御システムに接続する場所にファイ 制御システムに接続する場所ファイ制御システムに接続する場所ファイアーウォールが設定されている	0.1	各人が個別のアクセスカウントをもち、必要な担当者にのみアクセス権があたえられていて、アクセス権は毎年レビューされる	0.1	9×10^{-7}/y	0.9
				3×10^{-1}/y	300
各人が個別のアクセスカウントをもち、必要な担当者にのみアクセス権があたえられていて、アクセス権は毎年レビューされる	0.1			3×10^{-5}/y	30

ては困る重大なことは、安全解析と共通であり、この洗い出しが安全解析でも重要である。この安全担当者の知見が CS-LOPA 法[1] でも重要で情報システム担当者のみでは困難である。

7. 安全担当者のサイバーセキュリティへの寄与とは

事業所認定審査に、サイバーセキュリティ審査機関が新たに加わることになった[2]。サイバーセキュリティの審査は従来の審査機関では難しいという経済産業省の判断からの審査体制変更であると考えられるが、受審側もサイバーセキュリティは従来の担当では難し

いので情報システムに任せるという体制にならないことを切に願う。情報セキュリティは、高速のイタチごっこになりかねない特性をもち、情報システム担当でもついていくことは容易ではない。だからこそ、安全はイタチごっこに委ねるべきでなく、地に足がついたものでなければならない。情報セキュリティの対策が破綻したとしても、安全は確保できるという体制が必要である。

CS-LOPA 法[1] の**表6**の例で示したように、安全弁やリレーによる緊急遮断システムなどの情報システムではない安全対策の寄与も考慮することが必要である。コントローラを利用せずに安全に停止できるか、緊急停止後の安全確保の二次処理を、DCS 等の情報なしに実施しうるかという検討こそが、まず、現場が実施すべきサイバーセキュリティ対策である。そして、情報セキュリティ対策が異常を検知したときに、通信を遮断し、被害が疑われるサーバーや、コントローラを切り離すのは情報システム担当かもしれないが、操業を継続できるか、安全に停止できるかを即座に判断するのは従来からの安全の担当者であろう。操業現場で理解すべきことは、サイバーセキュリティの情報技術ではなく、それらが破綻する危険性とそれらが発信する情報を、操業継続や安全確保にどのように活用できるかである。

冒頭のイランの製鉄所の例でみるように、サイバー攻撃の危険性が高くなっているのが現状である。安全に関わるみなさんには、サイバーセキュリティを他人事にせず、情報システム担当と協力して進めていただきたい。その際に、CCPS/AIChE により提唱された CS-LOPA 法[1] が両者のよいインターフェイスになり、プロセス安全に関わるステークホルダーすべてに対する対策の見える化にも貢献できるようになることを祈る。

参考文献

1） 浜口訳：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，丸善出版，2024.
2） 経済産業省：高圧ガス保安法における新たな認定制度の運用について，2024. https://www.fdma.go.jp/relocation/neuter/topics/fieldList4_16/pdf/r05/01/shiryou4-4.pdf（参照日：2024年5月23日）.

はしもと●よしひろ

1985年京都大学大学院工学研究科化学工学専攻博士課程単位取得退学（工学博士）。2023年名古屋工業大学定年退官（名誉教授）。2017年から IPA 産業サイバーセキュリティセンターで中核人材育成プログラムを担当、現在も、制御システムセキュリティの研究に従事。