Vol.2018-GN-105 No.1
Vol.2018-SPT-28 No.1
2018/5/10

IoT と CPS 時代の新たなリスク管理手法の調査

五郎丸秀樹[†1]

概要：自動車や工場などに存在する制御系システムは，近年 IoT や CPS の技術の発展によりセンサや通信機能を有するようになった．その結果，自動車の自動運転や工場の遠隔監視などの新しいサービスが実施できるようになってきた．しかし制御系システムや IoT 機器に感染する Stuxnet，Mirai や Brickerbot を代表とする新たなマルウェアによってセキュリティも開発時に考慮する必要が出てきた．本稿では，まず自然災害からセキュリティ上の脅威までの従来のリスクとリスク管理手法について整理し，現在の開発の現場から見えてくるリスク管理の問題点や課題を示す．そしてこれらの問題点や課題を解決するためにリスクの発見から対応策の策定までの思考プロセスについて吟味し，IoT と CPS 時代の新たなリスク管理手法に必要な条件について調査した

キーワード：IoT，CPS，リスクマネジメント

A Survey of New Risk Management Method for IoT and CPS

HIDEKI GOROMARU[†1]

Abstract: Recently, control systems equipped in vehicles or factories have had sensor or telecommunication functions by development of IoT or CPS. As a result, it has been possible to provide new services which are automatic driving or remote monitoring for factories. However, it has been necessary to consider security of control systems against new malwares, which are Stuxnet, Mirai or Brickerbot, infecting control systems and IoT devices. In this paper, first, we have straightened traditional risk and the risk management methods from natural disasters to security threats. Second, problems and issues about the risk management have been shown from the current field of system development. Then, in order to solve the problems and issues, process of thinking from risk identification to risk treatment have been considered. Last, we have investigated requirements about new risk management methods for IoT and CPS.

Keywords: IoT, CPS, Risk Management

1. はじめに

近年，IoT (Internet of Things)[1][2]および CPS(Cyber Physical System)[3]技術が産業界に広まり，それに伴いセンサや通信機器が車や工場などの制御系システムに組み込まれる機会が増えている[4]．その結果，故障検知や遠隔監視などの新たなサービスが実施可能となり，運用や保守のコストが削減され利便性が向上していった．また，従来の制御系システムは，インターネットなどの外部ネットワークに接続することはなく，独自の通信プロトコルや独自の機器を使用した独自システムを使っていたため，外部からのマルウェアなどによる攻撃に晒される可能性は小さく，セキュリティ対策は重視されなかった．

しかし，制御系システムでの汎用通信プロトコルや汎用機器を使用する割合が高くなり， Stuxnet，Mirai や Brickerbot [5]など制御系システムや IoT 機器に感染・攻撃をおこなうマルウェアが出現したことによって，IoT 機器および制御系システムもセキュリティ対応が必要になってきている．これからは，IoT や制御系システムにとって，故障やヒューマンエラーなどの悪意のない行為に対応しているセーフティ対策だけではなく，情報の窃盗や機器の破壊などの悪意のある行為に対応したセキュリティ対策が，開発や運用において考慮すべき重要な対策となりつつある．さらに国際的な規格上でもセキュリティの重要性は年々高くなってきている．例えば，ソフトウェアの品質を示す規格では，セキュリティは品質の機能として副特性から品質特性に格上げされ[6]，従来[7]よりも重要度が高くなってきている．

開発におけるセーフティおよびセキュリティのリスク管理（リスクマネジメント）において様々な手法[8][9]が存在している．従来は複数のリスク管理手法を順番に実施することで全体最適化を行ってきた．例えば HAZOP でハザードを抽出し，FTA で重要なハザードに対して必要な安全機能をトップダウンで調査し，FMEA で各機能要素の故障モードから安全機能への影響をボトムアップで解析することなどである．但しこのやりかたは手法が増えるに従い時間がかかる欠点がある．開発の現場では，開発期間の短縮が求められており，リスク管理に費やす時間の配分についても制限がある．そのためリスク管理手法の適用について見直す必要もある．

従来の様々なリスク管理手法の中には，ブレインストーミング[10]，デルファイ法，ディシジョン・ツリーなど創造手法[8] [11]で用いられている手法も含んでおり，リスクの特定や分析，リスクの対応で使用されている．またリス

†1 日本電信電話株式会社
NIPPON TELEGRAPH AND TELEPHONE CORPORATION

クマネジメントについて記述されている ISO 31000: 2009)[12]aでは，リスクマネジメントの原則として「a)価値を創造する」「d）不確かさに明確に対処する」ことが記述されており，リスクマネジメントでは価値を創造し保護すること(目的の明確な達成及びパフォーマンスの改善)や，想定外のリスクへの対処に創造力が求められている．リスク管理手法と創造手法には重なっているところがあり，それぞれの手法の特徴を整理することで現在のリスク管理手法の足りない箇所を見直すことが可能ではないかと考えた．

本稿では，創造手法との比較を行う前に，歴史的背景とともに従来のセキュリティやセーフティで使用されているリスク管理手法を紹介し，開発におけるリスク管理の問題点や課題を取り上げ,思考プロセスについて整理しながら，新たな手法として求められる条件を調べていくこととする．

2. これまでのリスクとリスク管理手法

本章では，自然の脅威から悪意ある人の行為の脅威までの，主要なリスクと対応するリスク管理手法について説明する．

2.1 自然の脅威

1769 年の産業革命以前では，洪水，地震や疫病といった自然の脅威が主な事故や死亡原因であった．産業革命以後の技術の進歩により自然災害への対策が進み，自然の脅威よりも産業事故が事故や死亡原因の主流になっている[13]. 例えば日本では，1960 年以前は毎年 1000 人近くが災害で亡くなっていたが，1961 年の災害対策基本法制定や行政によるインフラの整備によって発生頻度の高い中小規模の災害による死者数は 100 名以下に減少した[14].

しかし，人為的に作られた安全の裏側で個人および地域人々の脆弱性を高めていき，災害過保護という状態を作り上げてきた[15]．中小規模の災害で培ってきた経験や知識，共同体の意識がなくなり，防災は行政が行うものという考えが主となり，個人の主体性（自らの命を自らが守る）を欠くようになったこと，そのことが地域の脆弱性を高めていった．また中小規模の災害を防止できるようになったことで災害によって発生する問題点を把握する機会が失われ，大規模災害が残っているにもかかわらず，そのリスクが見えなくなってしまった．その結果，阪神大震災や東日本大震災のように統計的にも発生頻度の低い大規模災害は存在しないと考えてしまう可能性が高い [16].

2.2 技術的脅威

産業事故の中で，当初は技術（機械）自体の問題による技術的な脅威が事故の大きな割合を占めていた．そこで安全工学や信頼性工学で培われてきた RCA(1905), ドミノ理論 (1929)， FMEA(1949)， HAZOP(1960)， FTA(1961)，FMECA(1980)といった手法が出現した[17]．その他関連する手法を表 1 に示す.

表 1　IEC/ISO31010 での手法 b

Table 1　Methods on IEC/ISO 31010

分析評価手法
ブレーンストーミング
構造化又は半構造化インタビュー
デルファイ法
チェックリスト
予備的ハザード分析（PHA）
HAZOP スタディーズ
ハザード分析及び必須管理点（HACCP）
環境リスクアセスメント（毒性リスクアセスメント）
構造化“Whatif”技法（SWIFT）
シナリオ分析
事業影響度分析（BIA）
根本原因分析（RCA）
故障モード・影響解析（FMEA）
故障の木解析（FTA）
事象の木解析（ETA）
原因・結果分析（CCA）
原因影響分析（特性要因図（魚骨線図））
防護層解析（LOPA）
決定木解析
人間信頼性分析（HRA）
ちょう（蝶）ネクタイ分析
信頼性重視保全（RCM）
スニーク回路解析（SCA）
マルコフ解析
モンテカルロシミュレーション
ベイズ統計及びベイズネット
FN 曲線
リスク指標
リスクマトリックス
費用／便益分析（CBA）
多基準意思決定分析（MCDA）

技術の向上により機器の信頼度が増しハードウェアによる故障が減少して産業事故における技術的要因の事故の割合は下がった．しかし代わりに悪意のない人間の危険行為であるヒューマンエラーによる事故が増えてきた.

2.3 悪意のない人の行為の脅威

ヒューマンエラーは昔から個人の資質の問題と捉えられてきた．しかしヒューマンエラーの事故原因を調べていくうちに，ヒューマンエラーは個人だけではなく，人の周りの状況や状態といった要因（PSF: Performance Shaping Factor：行動形成要因）が人の行動に影響したと考えるようになってきた．そして「人はシステムの一部である」というヒューマンファクターズという考え方が現れた[18].

また原子力産業分野において，安全性目標を満足していることを事前に立証するために，信頼性工学の一分野である PRA(Probabilistic Risk Assessment:確率的リスクアセスメント)が急速に発展した．これは原子力の炉が公衆の了解を得て操業許可を取得するため，インシデントやニアミス事例などの経験的データに基づいて安全性目標を評価しなければならなくなったためであった[19].

そして PRA の考えを基に, 人間の信頼性を確率的かつ定量的に見積もる方法として HRA（Human Reliable Analysis：人間信頼性分析）がある．これはヒューマンエラーの起こりやすさを予測する手法であり，第一世代（人間の行動上のエラーに焦点）と第二世代（人間の認知的なエラーに焦点）に分けられる．第一世代 HRA である THERP(1983）は HEP（Human Error Probability：ヒューマンエラー確率）を

a 最新は ISO31000:2018 である.

b 参考文献[12]を基に筆者が手を加え作成したものである.

種々の条件に応じて PSF で修正するものである[19]．HEP が主で PSF が従の関係である．1979 年のスリーマイル島原発事故以降では，スリーマイル島の原発事故の反省から「人は正しく行動しているが，周りの環境の影響が大きいため，人は環境の影響で認識を誤る」という認知的な考え方に変わっていった．その結果，PSF が主の関係である第二世代 HRA：ATHEANA(1996)が生まれた[19]．その他関連する手法を表 2 に示す[20].

表 2　HRA の概要 c

Table 2　Summary of HRA Methods

種類	手法
第一世代	THERP（ Technique for Human Error Rate Prediction）
	ASEP（ Accident Sequence Evaluation Program）
	HEART（ Human Error Assessment and Reduction Technique）
	SPAR-H（ Standardized Plant Analysis Risk Human Reliability Analysis）
	HRMS(Human Reliability Management System)
	JHEDI(Justified Human Error Data Information)
第二世代	ATHEANA(A Technique for Human Error Analysis)
	CREAM(Cognitive Reliability and Error Analysis Method)
	CAHR(Connectionism Assessment of Human Reliability)
	CESA(Commission Errors Search and Assessment)
	CODA(Conclusions from occurrences by descriptions of actions)
	MERMOS(Method d'Evaluation de la Realisation des Missions Operateur pour la Surete)

HRA ではリスクを定量化したが，この定量化の精度については意見が分かれている．例えば事故事象連鎖の中では既に発生した部分の影響を考慮した「条件付確率」だけを使用しなければならないが，多くの場合，各事象は独立したものと想定しており，共通モード故障 d[21]が存在する可能性を無視したものである．そして物事には既知の部分と未知の部分があり，信頼性の議論はこの既知の部分の信頼性を組み合わせることにより，より高い信頼性を得ようとしているだけであり，未知の部分についての評価が数字上ではなされていない[22]．個人の人間だけでもこれだけの課題があるが，組織の定量化は更に難しい．組織は故障しないため，機器の故障確率と同様に考えることには意味がなく，ヒューマンエラー確率のように組織をエラー確率の計算に含め定量化することは困難であるためである[23]．また，いくら機械の信頼性を上げても，人間の予想外の問題は防げない．例えば，ヒューズの故障頻度は年間 10^{-6} から 10^{-7} だが，切れたときに面倒がって銅線で代用する確率は 10^{-3} である[13].

2.4 組織事故

1979 年のスリーマイル島原発事故から 1986 年のスペースシャトルチャレンジャー事故，チェルノブイリ原発事故という事故を経て，事故原因を個人よりも組織の影響が大きいと考える「組織事故」という事故の捉え方から，複数の防御に穴が開き複数の潜在的要因が重なることにより事故が発生すると考えるスイスチーズ理論(1990)，AcciMap (1997), HFACS(2003), HINT-HFC (2006), H2-SAFER(2007)といった手法が生まれた[17][24].

ヒューマンエラー，ヒューマンファクターズ，組織事故などの人的要因による事故は，現在でも産業災害で大きな割合を占めている．例えば 2010 年における産業災害の要因の 7 割以上がヒューマンファクター（人的要因）であり，2016 年での情報漏えいの要因（管理ミスは 34.0%，誤操作は 15.6%，紛失・置き忘れは 13.0%，設定ミスは 4.7%）の 7 割弱が人的要因による情報漏えいとなっている[25][26].

2.5 機能共鳴事故

従来はシステムの個々の要素機能の不具合について焦点が当たっていた．システムを構成要素で分割し階層化して分析する還元主義アプローチは，リスクを単純化して検討し対策を行うことにより，単純なシステムでの事故に対しては効果があった．特に，多層防御・深層防御，フェールセーフのように冗長化を増やすことは，システムの個々の構成要素の故障を原因とする事故への適切な対策になる．

しかし，CCF（Common Cause Failure：共通原因故障）や CMF（Common Mode Failure：共通モード故障）など同時多発の複雑線形的な事故や，システムが大規模になるにつれ，複雑化し事故が伝播しやすくなったことで複数の要素機能間の共鳴による事故である「機能共鳴事故」に焦点が当てられ始めた[25]．冗長化による効果は，複雑で構成要素間の相互作用のあるシステムでは単純なシステムのような効果はなく，反対に冗長化自体が事故の一因になるくらい複雑さを増す原因になる場合もある [13]．対応する手法として STAMP(2002)，FRAM(2004)がある[17].

2.6 悪意のある人の行為の脅威

2002 年に制御系システムのセキュリティ規格である ISA99 発行が発行されたが一般に注目されることはなかった．しかし 2010 年のイランの核燃料濃縮プラントを操業妨害した Stuxnet の出現により，制御系システムはセーフティだけではなくセキュリティも考慮することが迫られている[27]．そして Mirai や Brickerbot のようなマルウェアにより，制御系システムだけでなく IoT まで拡張してセキュリティ対策が必要になりつつあり，さらにセキュリティとセーフティの両立が求められてきている[28]．セキュリティ分野では， ATA(Attack Tree Analysis)(1994)， Misuse Cases(2001)，STRIDE(2002)といった脅威分析手法がある[29] [30]．これらをセーフティのセキュリティに使用することが考えられる．セキュリティの統合について safety and security co-engineering という名称で様々な分析手法が提案されている[4]．例えば EFT(2009)，Extended CFT(2013)，FMVEA(2014) ， Unified Security and Safety Risk Assessment(2014)，FACT Graph(2015)，CHASSIS(2015)，SAHARA(2015)といった統合手法が提案[4][31][32] されて

c 参考文献[20]を基に筆者が手を加え作成したものである．
d 単一の要因によって，冗長機器が同じモードで同時に故障するもの．この故障は多重化・多様化によっても軽減できない[21]

おり，セーフティ手法とセキュリティ手法を組み合わせたものや 1 つの手法をセーフティとセキュリティに使い分けたものがある[31]（表 3）．もちろん既存手法を単純に組み合わせたものではなく，適用の仕方などで工夫がなされている．例えば FMVEA は分析対象を決めた後に，故障モードと脅威モードを分けて並列に分析しマージすること，従来の FMEA を使って故障モードを特定し， STRIDE を使って脅威モードを特定している[33].

表 3　セーフティとセキュリティのための統合手法 e

Table 3　Integrated Methods for Safety and Security

統合手法	セーフティ手法	セキュリティ手法
EFT	FTA	ATA
Extended CFT	FTA	ATA
FMVEA	FMEA	STRIDE
Unified Security and Safety Risk Assessment	NIST 800-30	
FACT Graph	FTA	ATA
CHASSIS	Misuse Cases	
SAHARA	HARA	STRIDE

しかしセーフティおよびセキュリティの対策を策定するため，セーフティ対応機能とセキュリティ対応機能を開発で組み込むことは簡単ではなく，調整なしに別々に実施すると機能の不整合がシステムに残る可能性がある．つまり一方の改善がもう一方の新たなリスクになる場合がある．不整合の有無の確認や新たな仕様の変更などのセーフティの専門家とセキュリティの専門家の間で調整が必要になる．例えば，暗号化，ウイルススキャンやネットワーク監視などのセキュリティ対策を採用する場合，リアルタイム性を重視したシステムでは制限時間内に処理が終わらなくなるリスク[4]があり，反対にリアルタイム性を重視すれば暗号化に短い鍵長の秘密鍵を使用せざるを得なくなるため脆弱性が残るリスクや，処理速度向上ための迂回路による新たな脆弱性の発生のリスクの可能性がある．新たなソフトウェアやハードウェアを設置したためにネットワーク上でノイズが混入し，機器が異常動作を引き起こすリスクも考えられる．これらは機能共鳴事故に似ている．

またコストの問題もある．特にレガシーシステムやセンサなど安さを売りにしたシステムやモジュールの場合，セキュリティ技術を導入することで値段が高くなることに抵抗がある．そしてセーフティでは一度正常に動いているのであれば手を加えないようにするが，セキュリティでは次々に新たな攻撃が出現するたびに手を加えて対応を取らざるを得ないため対応の仕方にも違いがある．

ISO や IEC といった標準化団体ではセーフティとセキュリティの統合に向けた動きが出ている．例えば，セーフティでは，IEC/TC65，IEC/TC44，ISO/TC199 [34]，セキュリティでは ISO/IEC JTC1 SC27，ISO/IEC JTC1 SC41 である．

3. 残存の問題や課題

各リスクに対して対応策やリスク管理手法があるが，問題や課題は残っている．ここでは主な残存の問題や課題を取り上げていく．

3.1 リスク測定および定量化の限界

自然災害も技術的脅威も発生頻度の高い事故に対する対策は十分であるが，発生頻度の低い事故については現在も対策が不十分である．その理由として発生頻度の高い事故は統計データが豊富であるが，発生頻度の低い事故はデータが殆どないためである．そのため発生頻度の低い特に大規模事故の場合は，事故に至るモデルを構築して計算されるが，実際は目に見える測定可能な部分だけしか計算ができない[13]．つまり定量化には限界があり，未知の部分についての評価が数字では表すことができず，これらは想定の適用外としてリスク対応の検討から外されるため，既知の部分を組み合わせて定量化しているだけである．

また条件付確率を使わなかったり，多重防御を無効にする共通モード故障を考慮していなかったりして，現状とは異なる条件で計算されていることが多い．頻度の低い事故に関する主要な要因は，氷山と同様に表に出ていない測定不可能な部分であり，かつ現状とは異なる条件で計算されているため，数字の根拠は乏しい．不確実性の高い部分については創造力が求められる．

3.2 網羅性の限界

網羅性を確保するために伝統的な還元主義アプローチがよく使われる．システムやプロセスを多段に分解し，その分解した構成要素の中で自由連想（例：ブレインストーミング）を実施することで任意の網羅性を担保することが多い（例：PHA，FMEA）．そしてこれをさらに徹底するため，５W1H，時間や因果関係を軸として認識できる範囲内での精緻を行っている（例：VTA，FTA）[35].

しかし還元主義アプローチは機能共鳴事故対応には不十分であり，またこの階層的な手法は構造的に不足する情報への気づきが困難[36]である．複雑なシステムの場合，還元主義アプローチだけでは構成要素間の相互作用については考慮されないため，構成要素間の相互作用によるリスクが抜け落ちてしまう．そのため全体を把握していく俯瞰的アプローチも求められる．システム理論では俯瞰的アプローチとして，個々の構成要素だけでなく構成要素間の相互作用を含めたものとしてシステムを見ている[13]．これは STAMP の Control Structure Diagram[37] や FRAM でモデル化されている．但し，これらのモデルからリスクを抽出するには抽象的であるため，ブレインストーミングのような自由連想では限界がある．そのためガイドワードと呼ばれる誘導語（ヒント）を使った制限連想を用いられることが多い．

また，ガイドワードを用いる HAZOP はハザードを網羅的に抽出する手法と言われている．しかし取り扱う対象は原則としてシステム内部のプロセスや運転の異常状態であり，外部要因や事象（外部火災，停電，地震等）は取り扱

e 参考文献[31] 基に筆者が手を加え作成したものである．

わない．そのためチェックリストとの併用でカバーする工夫がなされていることが多い[38]．つまりガイドワードも万能ではなく，対象に合わせた別のガイドワードが必要となる．HAZOP や STAMP/STPA のガイドワードはセーフティのガイドワードである．しかしセキュリティに対応したガイドワードについては用意されていなかったため，新たなガイドワードの提案 [39][40]や HAZOP や STRIDE が流用されたりしている．

ガイドワードと呼ばれる制限連想を用いたリスク特定については改めて考える必要がある．人を変えるだけでなく，同じ人でも時間帯や場所や見方を変えると新たなリスクを特定することがある．同様にガイドワードを変えただけでも新たなリスクが特定できる．ガイドワードの効果は脅威やシステム構成によっても変わる．また，人々の関心や対策の浸透度によっても変わる[41]．対象のシステムや脅威のトレンドなどから可変的に適切なガイドワードを作成していくことや，ガイドワードよりも更に効率の良いリスク抽出方法を考えていく必要がある．

還元主義アプローチと俯瞰的アプローチとガイドワードを組合せることで任意の網羅性を確保できるが，論理的に網羅性確保を完全に実施することは非常に難しい．そのため，ヒューリスティックに網羅性確保を行うことが現実の解として考えられる．例えば，一定の評価を受けている既存リスト fを適用することで一般的な対象範囲の網羅性を担保し，かつシステム固有のリスクのみをリスク管理手法で特定することである．

3.3 人の行為への対応の限界

事故の原因としてヒューマンエラーに突き当たれば分析を停め，エラーを起こした人に責任を求めることが多い．しかしヒューマンエラーは事象であり背後要因まで調べなければ一時的な対策しかでてこない．心情的に人は原因を環境ではなく人に求めることが多い．しかし人は周りの環境に影響されやすく，人を代えても周りの環境を変えなければ変わらず，また周りの環境を変えただけでは人はその環境に慣れてしまうと安心して更に高いリスクを取るようになる．そのため，人の意識を変え適切な行動を続ける仕組みを設けるか，または上流の根本的な要因を変えない限りは，同じような事故が繰り返される[42]．

また根本的な要因がわかったとしても，利害関係（原因と深く関係する部署の抵抗等），役職の力関係（上司と部下，労働者と経営者等），職場の雰囲気（経費や職員等のリソース削減，納期などの時間制約，不正を受け入れる隠蔽体質，モチベーションの低下等）により無視されたり横槍を入れられたりすることもある．特に現場の労働者や製品を購入した利用者よりも，現場から離れている経営者の方が環境よりも人に原因を求める傾向が高い[13]．そして経営者は，リスクの低減や安全よりも，利益やコスト削減の方に力を入れやすい．例えばフォード社の Pinto 車の事故やインドのボパールの Union Carbide 社の化学プラント事故などは少数の人々の利益のために大多数の人々にリスクを負わせる権力が問題となった．許容可能なリスクレベルを決める意思決定者は，多くの場合利益を得る人であり，リスクを負う人ではない．

そのため，意思決定者にリスクを負わせる（例えば工場の近くに家を構えさせる），リスクを負う人に任意の権限を与える（例えば事故発生時の対応の権限），または意思決定者とリスクを負う人が互いに協力できる関係を持つこと，などの対応がある．特に意思決定者が，リスクを負う人々が居る現場での検討の場へ出席し共感することが大切である．意思決定者が出席することで現場では解決できない問題を組織の力で早期に解決できるように仕向けることができるためである．これを実現するには早期にリスクを減らすことがコスト削減や企業倫理（コンプライアンス）に繋がることを意思決定者に理解してもらう仕掛けが必要である[43]．

またヒューマンエラーを回避するために機械化または自動化することによってリスクが低減されるが，保守や修理といった業務へのシフト，より高度な管理制御や意思決定へのシフト[13]，自動化システム不具合時の手動での代替運用，など自動化によってシステムから人間がいなくなることは無く，システムが複雑になるにつれて意思決定も更に難しくなる．特に自然災害と同様，手動時には体験することができた小規模な失敗を体験することがなくなる．そのためシステム不具合時の対応は誰も対応したことの無い未経験な状態から対応せざるを得なくなる．

3.4 外部要因への対応の限界

開発後の事故や開発の遅延などの問題が発生した場合，ステークホルダーだけでなく外部要因としての法律も重要となる．日本の裁判において，システム開発でセキュリティ要件が仕様や契約上で詳細に載っていない場合でも，契約時に対応策が公開されている脆弱性に対してはベンダがセキュリティ対応をしなければならない判決や [44]．発注元が要件変更を出した際，専門家であるべきベンダがその影響を説明しなければならない判決[45]が出ている．また「追加開発を実施すればシステムの稼働が予定日に間に合わなくなる」とベンダが繰り返し説明していたこと，および「今後一切の追加要望を出さない」という仕様凍結の合意をベンダが発注元に取り付けていたことにより，ベンダ側にはプロジェクトマネジメントでの義務違反はないという判決も出ている[46]．どの判決も最高裁の判決ではないが，開発に影響を与えそうな新たなセキュリティ情報をウォッチングする必要が有ることと同時に，セキュリティのリスク特定から対応までの対象の実施範囲についてステークホルダーへの説明と合意が必要であることが

f 国際標準規格，関連法令，社内外の規約，ガイドライン，チェックリスト，データベース等

わかる．実施範囲については発注元の要求内容によって変わる．任意の標準規格，業界標準，ガイドライン，会社の規約などへの対応など，最初にリスク管理を実施する対象範囲を決めておく必要がある．

また標準化の動きも外部要因として重要である．セーフティとセキュリティの統合の課題に対して様々な提案が提出されている．セーフティ分野では，制御系安全を扱う IEC/TC65，機械安全を扱う IEC/TC44，ISO/TC199 が活発な活動を行っている．またセキュリティ分野では ISO/IEC JTC1 SC27/WG4，ISO/IEC JTC1 SC41 で標準化の動きがある．

制御系安全を扱う IEC/TC65 では，機能安全の IEC61508 を手本に制御セキュリティとして IEC62443 にコンポーネントレベルのセキュリティを入れようとしている[34]．例えば，サイバーセキュリティを対象とする IEC 62443-2-1（CSMS 認証），組込デバイスのセキュリティを対象とする IEC 62443-4-1,2（EDSA 認証）がある．しかし機能安全と制御セキュリティには類似点だけでなく相違点もあるため，日本が提案国になり安全・セキュリティ連携規格の開発に着手（IEC TR63069：一般的制御システムにおける安全とセキュリティの分析・対応）した[27].

そして機械安全（IEC 側）を扱う IEC/TC44 では，セキュリティの機械の SRCS (Safety Related Control Systems)への影響は TC44 が主体となって作るべきだと考えており，IEC 63074（既存安全制御システムのためのセキュリティ対策）という規格に着手した[27]．機械安全（ISO 側）を扱う ISO/TC199 でも機械系のリスクアセスメントの規格である ISO12100 によるリスクアセスメントプロセスにおけるセキュリティ側面のガイド（ISO TR22100-4）開発の動きがある．問題が発生しないように，または発生したとしても適切な対処をしたことを示すためにも，今後もセーフティとセキュリティの統合への影響を考え，これらの標準化動向をウォッチングしていく必要がある．

3.5 リスク管理手法自体の問題

リスク管理手法は，専門家がいない場合でも，ある一定以上のスキルの者が専門家と同等以上の結果を出せるように支援することが可能な道具であり，そのことによって現場に受け入れられ，定期的に改良されていくことが理想である．実際は，余計な道具の導入によって新たな稼動が増えることに対する現場での導入に向けた抵抗があり，法律や規制や会社・職場の方針などで強制的に使用が義務付けられているもの，業界標準の手法であること，もしくは以前大きな事故が発生しその教訓として使用しているものではない限り，ある特定の手法を現場で続けて使用することは少ない．そして上記の問題以外でも下記のように古くて新しい問題や課題が残っている．

3.5.1 リスク管理時間

リスク管理において 1 つのリスク管理手法だけでは求められている要求を満たすことができないため，複数の手法を組み合わせることが多い．例えば，システムのプロセスの正常状態からのずれには HAZOP，システムの機能全体の各構成要素の個別故障の影響には FMEA，任意の事象の発生メカニズムを明確にした発生頻度の定量評価には FTA，事故シナリオに基づき多層防御の効果や事故に至るまでの発生頻度の定量的評価には ETA，リスク評価には SIL（Safety Integrity Level：安全度水準）などがあり，これらを組み合わせると，①HAZOP→②FMEA→③FTA・④ETA→⑤SIL となり５つの工程がある[47]．そのため，最初の開発だけきちんと実施し，軽微な改良では HAZOP や FMEA の代わりに What-If や PHA，FTA や ETA の代わりに定性的評価のリスクグラフや LOPA を使う，といった使い分けもある．また関係者が集まることができない場合には半構造化インタビューやデルファイ法などを代用としたり，電話会議，TV 会議，Web 会議，SNS の掲示板を活用するなどグループウェアを利用したりする方法もあるが限界もある．

さらにシステム全体を俯瞰し機能間の不具合対応として STAMP，セキュリティ手法として STRIDE と ATA を加えると，①STAMP→②HAZOP→③FMEA→④STRIDE→⑤FTA・⑥ETA・⑦ATA→⑧SIL となり８つの工程に膨れ上がる．開発の限られた時間でこれら全てを実施することは難しいため何らかの工夫が求められる．例えば，各手法を分解し似た機能を削ることや別の効率的な手法を適用するなどが考えられる．

3.5.2 属人性の排除

同じ手法を使っても，実施した人によって作成結果の内容が異なる場合がある．例えば THERP は経験を積んだ人々が使用した場合は極めて有効だが，経験の浅い人々が使用した場合は有効性が疑わしい[19]．また STAMP も同じシステムであるにも拘らず異なる Control Structure（制御構成図）が作られることが報告されている[48].

反対に様々な人々が出した一見異なるリスクや解決策が，よく読むと同じ内容のものであり表現が異なっているだけのものもある．また技術的に詳しい人が記述すると細かなところまでリスクや対策案を記述するが，その作業がシステムの全体を把握すべきところであれば，その粒度は相応しくなく抽象度を高めた記述にする必要がある．これらの事から要求条件をまとめると下記のようになる．

- 結果の有効性の確保
  - 同じ手法を使っても発生する，実施者のスキルの違いによる結果の揺らぎの低減
- 表記の標準化
  - 異なる表現であっても同じ内容である文言の不統一の是正
- システム構成の階層にあわせた記述粒度
  - システムの全体から部分までの各階層にあわせた内容の粒度の調整

3.5.3 全体の結果の評価

個々のリスクや個々の対策案については定性的または定量的な評価を行うが[19][28]，リスク全体，対策案全体，リスクと対策案を含めた全体の結果の評価手法は存在しない．部分では最適な評価結果であっても，全体では最適な結果であるのかどうかが不明である．特に報告者が報告したリスク情報に対して、きちんと評価されているかどうかが見えなければモチベーションが保てない可能性もある。

3.5.4 要因調査の限界

事故の要因を調査すると様々なバイアスにより分析に偏りが出てくる可能性がある．特にヒューマンエラーが発見されると原因を探すことを止めてしまうことが多い[49]．例えば警察による捜査や刑事事件の裁判，マスコミによる犯人探しなどはその典型である．基本的帰属錯誤のバイアスにより他人の行為はその人の特質から出てきたものと認識してしまうことが多い．2.3 節および 2.4 節でも述べているが，実際は個人よりも組織も含む人を取り巻く周りの影響の方が大きく，ヒューマンエラーは単なる事象であり，その背後要因の分析が重要である．

また事故の直接要因まではばらつきは少ないが，背後要因となると分析者のスキルや立場によって偏りが生じやすく，ばらつきが多くなる．RCA（根本原因分析）ではどこまで分析すればよいのか，何を持って分析を終わればよいのか目安が無く．事実の記載のみとなったり，抽象化しすぎたり，対策に合わせる形で誘導したりすることがある．分析する目的や目標を決め，分析後の評価の視点を予め用意しておき，その限界を認知しながら進めていくことが考えられる．

4. 新たなリスク管理手法について

ISO31000:2009[12]の思考プロセス（図 1）を基に，これまでの議論から新たなリスク管理手法の要求事項として下記のようにまとめた．

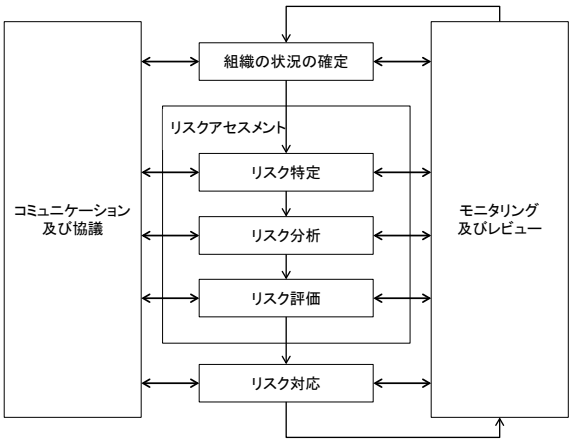

図 1　リスクマネジメントプロセス g

Figure 1　Risk management process

(1) 組織の状況の確定

- リスク管理に影響のある外部要因（例：新たなセキュリティ情報，標準化技術，ガイドライン，社内規定）を入手し管理できること

(2) リスクアセスメント

- 俯瞰的アプローチ（サブシステム間の相互作用を含む全体把握），還元主義アプローチ（構成要素把握）からシステムを把握できること
- リスク特定を促すこと（自由連想，制限連想およびその他の方法）ができること
- 不確実性の高いリスク（例：発生頻度の低い大規模災害，悪意のある人の行為）をモデル化し影響等の分析を支援すること
- 背後要因の分析では，バイアスの影響を低減させ分析できること
- 属人性を排除（スキルの違いを軽減，表記の標準化，記述粒度の平準化）できること
- 数字の根拠が必要でなければ，定量評価は数字の根拠がなく時間がかかるため，できるだけ定量評価（順序尺度レベル）とすること

(3) リスク対応

- セーフティ機能とセキュリティ機能の不整合を発見できること
- IT 技術によるリスク対応による副作用として，人がトラブル対応の経験を失うことへの対応も考慮できること
- 多重防御・深層防御などの冗長化は，共通モード故障には無効であり，機能共鳴事故を誘発する副作用があることを考慮できること

(4) コミュニケーション及び協議

- ステークホルダー（例：発注元）に提案し内容について合意（例：管理の対象範囲，仕様書の内容）できること
- ステークホルダー（例：意思決定者）が現場での検討の場へ出席しリスクを共感してもらい意思決定を行うことができること

(5) モニタリング及びレビュー

- セーフティ専門家とセキュリティ専門家に提案・議論し合意（例：仕様書の内容）できること
- 結果（特にリスク全体，対策案全体，作業全体）を評価できること
- 時間短縮・効率化および使用者のモチベーション維持のため，手法自体を評価し，各手法の機能の統廃合や変更ができること

g 参考文献[12]を基に筆者が手を加え作成したものである．

5. おわりに

今回はリスク管理手法の歴史的背景を中心に残存する問題や課題を抽出し，これからのリスク管理手法に必要な要求事項をまとめた．今後はリスク特定において創造手法の思考プロセス[11]との比較を行い，更に効率的なリスク特定の方法について検討していく．

参考文献

[1]“That 'Internet of Things' Thing”. http://www.rfidjournal.com/articles/pdf?4986, (参照 2018-01-18).
[2]Brian Russell, Drew Van Duren. Practical Internet of Things Security. Packt Publishing, 2016.
[3]Khaitan et al. Design Techniques and Applications of Cyber Physical Systems: A Survey. IEEE Systems Journal, 2014.
[4]田口研治．①IoT の伸展に伴うセーフティとセキュリティのリスクと課題．情報処理学会学会誌，Vol.58 No.11 Nov. 2017
[5]“Five nightmarish attacks that show the risks of IoT security”. http://www.zdnet.com/article/5-nightmarish-attacks-that-show-the-risks-of-iot-security/, (参照 2018-01-18).
[6]日本工業規格．システム及びソフトウェア製品の品質要求及び評価（SQuaRE）−システム及びソフトウェア品質モデル．JIS X 25010: 2013.
[7]日本工業規格. ソフトウェア製品の品質―第 1 部:品質モデル. JIS X 0129-1: 2003.
[8]日本工業規格．リスクマネジメント-リスクアセスメント技法．JIS Q 31010: 2012.
[9]Adam Shostack. Threat Modeling: Designing for Security. Wiley, 2014.
[10]A. F. オズボーン，上野一郎（訳）．独創力を伸ばせ．ダイヤモンド社，1971.
[11]高橋 誠．新編 創造力事典．日科技連出版社，2007.
[12]日本工業規格．リスクマネジメント−原則及び指針．JIS Q 31000: 2010.
[13]ナンシー・G・レプソン，松原友夫（監訳）．セーフウェア．翔泳社，2011
[14]“平成 28 年版 防災白書｜附属資料 8　自然災害における死者・行方不明者数”, http://www.bousai.go.jp/kaigirep/hakusho/h28/honbun/3b_6s_08_00.html(参照 2018-01-18).
[15]片田敏孝．人が死なない防災．集英社新書，2012.
[16]中田 亨．仕事の段取りべからず 71．JIPM ソリューション，2013.
[17]Erik Hollnagel, Josephine Speziali. Study on Developments in Accident Investigation Methods: A Survey of the “State-op-the-Art”. Swedish Nuclear Power Inspectorate, SKI Report 2008:50, 2008.
[18]首藤由紀．事故・災害のヒューマンファクターズ．2005 予防時報 223，2005.
[19]James Reason. Human Error. Cambridge University Press, 1990.
[20]Julie Bell & Justin Holroyd. Review of human reliability assessment methods. Health and Safety Laboratory, 2009.
[21]JEMIMA 機能安全規格の技術解説”, http://tech.jemima.or.jp/doc/func_safety_201311.pdf, (参照 2018-01-18).
[22]小林 忍．航空機事故に学ぶ　危険学の始点．講談社，2012.
[23]エリック・ホルナゲル，小松原明哲（監訳）．社会技術システムの安全分析　FRAM ガイドブック．海文堂，2013.
[24]Paul M. Salmon et. al. Human Factors Methods and Accident Analysis. Ashgate Publishing Limited, 2011.
[25]“On How (Not) To Learn from Accidents”, http://www.uis.no/getfile.php/Konferanser/Presentasjoner/Ulykkesgransking%202010/EH_AcciLearn_short.pdf(参照 2018-01-18).
[26]“２０１６年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～”, http://www.jnsa.org/result/incident/data/2016incident_survey_ver1.2.pdf.(参照 2018-01-18).
[27]神余浩夫．②機能安全と制御セキュリティの標準化動向．情報処理学会学会誌，Vol.58 No.11 Nov. 2017.
[28]金川信康，山田 勉．社会インフラストラクチャを支える制御システムにおけるセーフティとセキュリティ．情報処理学会学会誌，Vol.58 No.11 Nov. 2017.
[29]Sindre, G., & Opdahl, A. L.. Capturing Security Requirements through Misuse Cases., 2005.
[30]Adam Shostack. Threat Modeling: Designing for Security. Wiley, 2014.
[31]Sabarathinam Chockalingam. et. al.. Integrated Safety and Security Risk Assessment Methods: A Survey of Key Characteristics and Applications. Cornell University Library, 2017.
[32]Stéphane Paul. et al.. Recommendations for Security and Safety Co-engineering. MERgE ITEA2 Project, 2016.
[33]Christoph Schmittner, Zhendong Ma, and Paul Smith. FMVEA for Safety and Security Analysis of Intelligent and Cooperative Vehicles. SAFECOMP 2014 Workshops, LNCS 8696,2014.
[34]“機能安全を実現する安全制御システムにおけるセキュリティについての標準化の動き”, http://www.jmf.or.jp/content/files/hyoujunka/hyo201711_04.pdf(参照 2018-03-26).
[35]石橋 明．事故は，なぜ繰り返されるのかーヒューマンファクターの分析―．中央労働災害防止協会，2003.
[36]“時系列的分析手法を用いた出合頭事故の人的要因分析”. http://www.wul.waseda.ac.jp/gakui/honbun/4069/4069_004.pdf (参照 2018-01-18).
[37]システム安全性解析手法 WG. はじめての STAMP/STPA～システム思考に基づく新しい安全性解析手法～. 独立行政法人情報処理推進機構, 2016.
[38]“プラントの安全性評価　第２回潜在危険性の特定(その１)”. http://hazop.jp/pdf/guide2.pdf　(参照 2018-01-18).
[39]“HAZOP-based Security Analysis for Embedded Systems”, https://www.ipa.go.jp/files/000050239.pdf (参照 2018-01-18).
[40]J. Dürrwang, K. Beckers, and R. Kriesten. A Lightweight Threat Analysis Approach Intertwining Safety and Security for the Automotive Domain. Springer, SAFECOMP 2017, 2017.
[41]Baruch Fischhoff and John Kadvay. Risk A Very Short Introduction. Oxford University Press, 2011.
[42]Gerald J. S. Wilde. TARGET RISK 2 A New Psychology of Safety and Health. PDE Publications, 2001.
[43]Atul Gawande. The Checklist Manifesto: How to Get Things Ritht. Janklow & Nesbit Associates, 2009.
[44]“会社･取締役が法的義務を負っている情報セキュリティのレベルとは”. https://business.bengo4.com/category3/practice354 (参照 2018-01-18).
[45]“ある判決, 要件にないことで責任を負わされたシステム開発会社の悲劇”. http://itpro.nikkeibp.co.jp/atcl/watcher/14/334361/012100467/?P=2 (参照 2018-01-18).
[46]“失敗の全責任はユーザー側に，旭川医大と NTT 東の裁判で逆転判決”. http://itpro.nikkeibp.co.jp/atcl/column/14/346926/092501136/?ST=print (参照 2018-01-18).
[47]佐久間 晃，他 2 名．プラント・機械設備のリスク分析・安全度水準（SIL）評価サービス．東芝レビューVol.16 No.11，2006.
[48]システムモデルを用いた STAMP/STPA 試行の事例紹介”. https://www.ipa.go.jp/files/000063287.pdf (参照 2018-03-30).
[49]D. A. Norman. The Design of Everyday Things. The MIT Press,2014.