

ICT のセキュリティへの適用に向けた分析評価手法の調査

五郎丸秀樹^{†1}

概要: IoT やクラウドを代表としたデバイスやシステムがインターネット上のサービスの基盤として増加している。そして外部ネットワークへ接続することを前提としなかったシステムも利便性向上のためネットワークに接続するようになってきた。それに伴い、マルウェアへの感染、情報の漏えい・消失・使用不可、システムの異常動作などのインシデントの発生が懸念される。インシデントの発生の検出や発生後の要因分析だけでなく、発生前にリスク分析および対策案を生み出し評価する必要があるが、ICT のセキュリティへの分析評価手法の適用方法について明確に定まっていない。また対応する専門家や関係者が集まって分析や議論するための場所や時間がない場合も想定される。本稿では、既存の分析評価手法を調査し、ICT のセキュリティにおいて様々な視点から分析評価手法を適用する上での問題や課題を抽出し、新たな分析評価手法とその運用方法について検討する。

キーワード: セキュリティ, セーフティ, 分析評価手法

A Study of Analysis-Evaluation-Method Applied on Information and Communication Technology for Security

HIDEKI GOROMARU^{†1}

Abstract: Devices and systems like IoT or cloud computing have increased as platforms of services on the Internet. Systems which were without connecting external networks have come to connect external networks in order to improve user convenience. As a result, it has been concerned that malware infection, information leakage, information disappearance, unavailable information, and abnormal action in systems have been able to occur. It has been necessary to execute not only "the factor-detection and factor-analysis after occurrences of incident" but also "the risk-analysis, risk-evaluation and risk-treatment before occurrences of incident". However, the applying of Analysis-Evaluation-Method for ICT security has been not fixed clearly. In addition, it has been conceivable that there are not enough time or space in which experts and authorities concerned meet. In this paper, after surveys of the existing Analysis-Evaluation-Methods, we have investigated about the new Analysis-Evaluation-Methods and the control methods, in order to clarify the problems or issues of the applying of Analysis-Evaluation-Methods for ICT security from various viewpoints.

Keywords: Security, Safety, Analysis-Evaluation-Method

1. はじめに

近年、インターネットの普及により、IoT[1]やクラウド[2]を代表とした様々なデバイスやシステムがインターネット上のサービス基盤としてネットワークに接続され増加している[3]。そして化学プラント、製造工場、医療システムなど今まで外部のネットワークに接続することを前提としなかった分野の既存システムに対して、従来通りの USB メモリや保守用端末とのシリアルインタフェースによるシステムへの接続だけでなく、運用保守の利便性向上のためシステムを外部ネットワークへつなぐようになってきた。外部ネットワークへの接続の機会が増えるに従い、マルウェア感染、情報漏えい、情報喪失、情報の使用不可、そしてシステムの異常動作などのインシデントがシステム上で発生する機会が高まってきている[4]。

システムおよび通信も含めた ICT のセキュリティを保つ

ために、これらのインシデントの発生を検知した後に発生した要因を分析し対応するだけでなく、インシデントが発生する前にリスクを見つけ対策を施し対応しておくべきである。しかし要因やリスクを分析し評価する分析評価手法は 50 以上存在し[5]、どのような場合にどの分析評価手法を使用した方が良いのか明確に定まっていない。また、使用する分析評価手法を決めたとしても、分析や評価する専門家や関係者が同じ時間に同じ場所で議論し、同じ参加者で繰り返し議論できるとは限らない。本稿では、分析評価手法を調査し、その問題や課題の抽出、および新たな分析評価手法とその運用方法について検討する。

2. 従来の分析評価手法について

産業の安全のため、分析評価手法は古くから使用されてきた。ここでは歴史的背景と代表的なモデル、そして代表的な適用分野について述べる。

2.1 歴史的背景

Andrew Hale & Jan Hovden[6]によると産業の安全は3つの時代に分けることができる。ここでは3つの時代の代表

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

的な分析評価手法を紹介する。

2.1.1 技術の時代

18世紀の産業革命以降、事故は「技術（機械）の問題」という捉え方が出てきた。FMEA(FMECA),HAZOP,FTA[7]など信頼性工学で使用されている分析評価手法が現場で使われ、主に軍事・宇宙航空分野で適用されてきた。

2.1.2 ヒューマンファクターズの時代

技術が発達し技術的要因の事故が減っていくと、ヒューマンエラー要因の事故が徐々に目立ち始めた。特に1979年の米国のスリーマイル島での原子力発電所の事故をきっかけに、技術よりもヒューマンエラーに注目が集まった。その後、人のエラー要因には人自身よりも人以外（組織、装置、設備、手順、作業環境等）の要因の影響が大きいことが語られ始め、人もシステムの一部とみなす「ヒューマンファクターズ」の考え方が出てきた。THERPやATHEANAなどHRA(Human Reliable Analysis:人間信頼性解析)の評価分析手法が原子力分野で使われた[8]。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)であり現在でも産業事故の主要な要因である[9]。

2.1.3 安全管理の時代

1979年のスリーマイル島の原発事故、そして1986年のスペースシャトルチャレンジャー事故とチェルノブイリ原子力発電所事故から、事故要因は「個人から組織へ(組織事故)」と「要素機能の不具合から予測困難な複雑な要素機能間の共鳴へ(機能共鳴型事故)」という新たな視点が変わった。「組織事故」に対しては、CDM(1989)、AcciMap(1997)などの新しい手法が出現し[10]、「機能共鳴型事故」に対しては、従来のRCA(Root cause analysis)[11]の手法では分析しきれないため、システムを構成する要素機能同士の変動がどのように連鎖し共鳴して事故が起こるかという関係性を示す新たな手法として、STAMP(2002)[12]、FRAM(2004)[13]が現れた。特にSTAMPはSTPA(ハザード分析手法)、CAST(事故分析手法)、STPA-sec(サイバーセキュリティなどに特化した事故分析手法)などの手法が編み出されている[14]。

2.1.4 新たな時代の問題

組織や機能共鳴型の事故要因が増えてきているが、これはシステムの要素機能単体の不具合が減り、周りの環境(組織も含む)や要素機能間の相互関係によって発生する予期せぬ不具合が増えてきていることを示している。ICT分野においても、既存システムの統合化やネットワークを介したクラウド上での運用などでシステムの要素機能が爆発的に増え複雑化かつ不透明化してきた。そして悪意のある攻撃も標的型メールのように技術的手法だけでなく人的手法も加わり巧妙化し多種多様化してきたことで正常と異常の判別がしづらくなったため、さらにインシデント発生時の要因の特定が難しくなっている。

2.2 産業事故のモデル

ここでは、産業安全の各時代背景から代表的な産業事故のモデルを紹介する。

2.2.1 単純線形モデル

古くから使われているモデルとしてHeinrichのドミノモデル(1930)[15]が有名である(図1)。これは5つの要素①育ってきた背景および社会的な環境、②人による失敗、③不安全行動・設備的・身体的な危険、④事故、⑤傷害)のドミノ連鎖反応により傷害が発生するが(図1左側)、例えば③を取り去れば傷害は発生しない(図1右側)という単純線形モデルである。現在では5つに拘らず、ドミノそのものを様々な要因とみなし「要因や連鎖を排除することによって防ぐことができる」という考え方となっている。RCAやAcciMap(1997)はこのモデルに近い分析評価手法である[10]。しかし、このモデルは単一故障(1つの根本原因)には対応しているが、複数同時故障には対応していない。

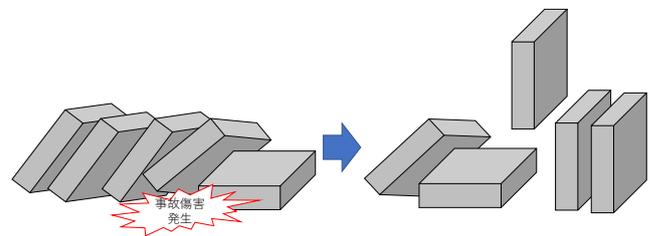


図1 Heinrichのドミノモデル[a]

Figure 1 Heinrich's domino theory.

2.2.2 複雑線形モデル

最も有名で実用的なモデルは、Reasonのスイスチーズモデル(1990)[16]である(図2)。これは疫学(複雑線形)モデルとも呼ばれ、産業事故を防ぐように設計されている防護壁(人・組織・設備等)が劣化(人のモラル低下や組織の安全への予算削減など)し多様性を失い、複数のエラーや潜在的脆弱性が重なり事故が発生することを示したモデルであり、多重防御と防護壁の維持により事故を防ぐ仕組みでもある。HFACS航空事故分析法(2003)、事故分析フレームワーク(2005)などで使用されている[10]。このモデルは組織事故を想定しているが、システムや要素の相互間の複合原因による機能共鳴型事故には十分対応していない。

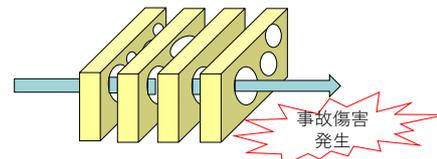


図2 Reasonのスイスチーズモデル[b]

Figure 2 Reason's Swiss cheese model.

2.2.3 非線形モデル

新しい産業事故のモデルが機能共鳴モデルである(図3)。この機能共鳴モデルは、非線形モデル[17]やシステム

a) 参考文献[15]を基に著者が手を加えて記述した。

b) 参考文献[16]を基に著者が手を加えて記述した

ックモデル [18]ともも言われている。開発するシステムが大規模になり、システムの要素機能間の相互作用も複雑化すると、システムやシステムを構成する各要素機能が動的に変動していく中で変動の周期が共鳴し予想外の大きな変動により安全限界を超えて事故が発生することを示すモデルである。STAMP[19], FRAM [20]がこのモデルに対応可能な分析評価手法である。

STAMP では、事故は要素機能の問題ではなく要素機能間の制御の問題としてとらえている。「安全がどのように制御されているのか」という動的な構造に主眼を置いた手法である[13]。FRAM では、STAMP のように特定の機能をあらかじめ定義したり特定の方法で体系化したりすることを仮定せず、定常的な事象や活動を機能の観点から記述する。FRAM は手法を生み出すためのシステムのモデル化ではなく、新たなモデルを生み出すための手法である。

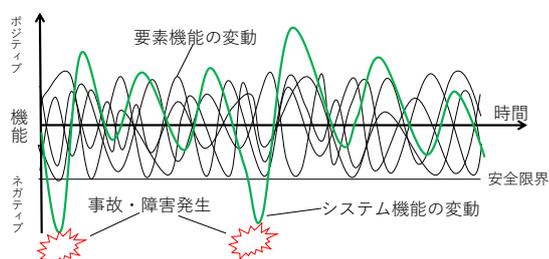


図 3 機能共鳴モデル[c]

Figure 3 Functional resonance model.

2.2.4 STAMP と FRAM の弱点

STAMP は、「システムの構造化（階層構造や因果関係）について多くの仮定が含まれるシステム理論モデルを基にした線型因果分析手法」である。構造化したモデルから、要素機能や制御などの不具合を原因とした単一あるいは複合的な因果パスを伴う線型構造の分析となるため、基のモデルの妥当性が重要となる[13]。FRAM は、モデル化までに多くの作業が必要であり従来の手法にくらべ時間がかかる場合がある[13]。

STAMP も FRAM も要素機能間を線で結び、HAZAP のようにガイドワードで通常と異なる振る舞いの異常想定をしている。しかしインシデントなどの事象は、必ずしも決まった要因によって発生するとは限らず、想定していない複数の要因が絡み合っ発生する可能性も否定できない。またウィルス対策ソフトウェアのアノマリ検知のように「正常」の定義を決めることが必ずしもできるとは限らない。例えばうつ病のような慢性的な病気は何を持って「正常」であるかを定義することは難しい。要素機能間を線で結び、ガイドワードによる異常想定は重要だが、更に異なる視点での分析評価手法が求められる。

2.3 各分野での分析評価手法

現在、分析評価手法は分野によってさまざまな種類が存在する。ここでは分析評価手法が使用されている代表的な

c) 参考文献[18]を基に著者が手を加えて記述した。

業界で主に使われている手法について紹介する。

2.3.1 航空業界

この業界は、事故が大量死に直接結びついているため危機意識がある。特に分析評価手法がいち早く取り入れられた業界でもある。

(1) 4M-4E・SHEL

表に埋めることで網羅的に要因を抽出する手法[7]。

(2) RCA

根本原因を深堀する手法。例えば連関図，時系列図，FTA,TVA 等[11][7]。

(3) ASRS(Aviation Safety Reporting System)

インシデント報告制度として法律で刑事免責を確立し匿名性も確保しパイロット等が安心してインシデントを報告できる米国の航空安全報告システム[7]。1975年に発足した。

2.3.2 原子力業界

炉心溶解に至る確率を計算するためなど確率論的リスク評価 PRA(Probabilistic Risk Assessment) [7]が発展してきた。PRA には HRA[8]という人間のエラー確率を予測する解析方法がある。

(1) 第一世代の HRA

人間のエラー確率に PSF (Performance Shaping Factor: 人間の行動に影響を与える要因) の要素を加えた分析評価手法である[7]。人間をシステムの一部として見なし、規程通りの行動が重視された。その代表的な手法として THERP (Technique for human error rate prediction)[8]などがある。

(2) 第二世代の HRA

人間のエラーは人間よりも環境 (PSF) の影響に依存する、という考えに基づいて、人的・環境要因の人間の認知への影響を系統的に分析する分析評価手法である[7]。その代表的な手法として ATHEANA(A Technique for Human Event Analysis) [8]などがある。

(3) HPES (Human performance enhancement system)

人間行動改善システム。航空業界の ASRS を基に米国で 1982 年に開発された[7]。日本では 1990 年に J-HPES が開発され[7]、2005 年に人的過誤の事象の時系列の整理と背後要因分析を体系的に行うことができる H²-SAFER(Hiyari Hatto - Systematic Approach For Error Reduction) や HINT-HFC (Human performance Incidents analysis tool - Human factors Research center)が開発された[7][21]。

(4) C&C (Cause and Consequence Analysis)

CCA とも呼ばれ、ETA(Event Tree Analysis)や FTA(Fault Tree Analysis)を統合した分析評価手法である[22]。

2.3.3 医療業界

“患者取り違い事故”により業務システムの改善が求められ、他業界の分析評価手法を医療の実態に合わせ変更した分析評価手法が使われ始めた。

(1) VA-RCA(Veterans Affairs National Center of Patient Safety - RCA)

米国退役軍人病院の患者安全センターで開発された根本原因を深堀する手法[7].

(2) Medical SAFER

原子力業界で使用されていた H²-SAFER を元に医療の実態に合わせて作られた [7][23][24].

2.3.4 化学プラント業界

規格や業界標準の分析評価手法として HAZOP[7]が推奨され定着した.

(1) HAZOP(Hazard and operability study)

正常状態からの逸脱を示すガイドワード (more, less など) を用い潜在的な危険を抽出する手法である HAZOP が 1960 年代に英国で開発されて以来,長い実績を持つ [7][23].

(2) HAZOP 以外

HAZOP の補助または代替りとして,相対危険度分析手法,チェックリスト法,PHA(Preliminary Hazard Analysis:予備的危険解析),FMEA,What-If 解析 (What-If Analysis),FTA,ETA が挙げられている[25].

2.3.5 自動車業界

規格や業界標準の分析評価手法として FMEA[7]が業界で推奨されていたため定着した.

(1) FMEA

自動車業界の品質管理システムの技術仕様を定めた ISO TS 16949 で FMEA を参照している[26]. また自動車の機能安全規格である ISO 26262 が 2011 年に発行されている.そして HAZOP, FTA, FMEA を組み合わせることで網羅的に解析を行い,解析の漏れを防ぐ提案もある[27].

2.3.6 ICT 分野

情報セキュリティ上の脅威の分析評価手法として STRIDE, ATA (Attack Tree Analysis), Attack Libraries (チェックリスト, 文献レビュー, CAPEC, OWASP Top 10 など) が挙げられる[28]. 要求工学やソフトウェア工学で使用されている Assurance Case (GSN, CAE, D-Case 等)を使用する場合もある[29]. また SOX 法 (J-SOX 法) で提出が義務付けられている「内部統制報告書」のリスク・コントロール・マトリクス (RCM) は, IT 統制のリスクを分析する方法として利用されている[30].

2.3.7 求められる条件

(1) 業界特有の観点

各業界での分析評価手法の違いについては,各業界での重視している観念の違いに反映されている.例えば,人と人を取り巻く環境(他の人,機械など),人の過誤率,人的要因の特定,分析評価手法の利用に対する専門知識の有無,正常時からの逸脱の有無,人の悪意の有無,評価対象(ハードウェア,業務のプロセス等),業界での推奨・標準への準拠などである.分析評価手法の適用対象の分野で求められる観念を見つけ出す作業が必要となる.

(2) 手法の理解と複数手法の組合せ

各業界の分析評価手法は,独自に発展したり他の業界の

手法を取り入れたりしてきたため,分析評価手法の種類は多種多様であり,複数の手法を組み合わせる場合もある.例えば医療業界は航空業界や原子力業界で使用されてきた分析評価手法を取り入れ自分のものにしてきた.

ICT 分野では,プラントなどのセーフティ分野で使われていた制御系システムと,クラウドなどのセキュリティ分野でよく使われているネットワーク上のシステムを,インターネットを介して接続して利用者の利便性を上げているが,同時に外部からの攻撃 [4] の機会も増えてきている.分析評価手法も悪意のない事故を対象とするセーフティと悪意のある事故を対象とするセキュリティを分ける必要はなく,他分野の分析評価手法の特徴を把握し,互いに補完した使い方が求められる.

3. 分析評価手法の特徴

分野によって異なった観点での分析や評価が必要となったため,数多くの種類の分析評価手法が生まれ,対象分野にあった手法が適用されてきた.しかし異なる分析評価手法ではあっても似たような機能を持った手法も存在しているため整理する必要がある.ここでは標準規格である ISO や JIS を活用して,先ず分析評価手法単体の内部のマイクロの特徴を示し,次に製品のライフサイクルのどの段階に分析評価手法を適用するのかマクロの特徴を示すこととする.

3.1 分析評価手法のマイクロの特徴

3.1.1 国際標準と分析評価手法の機能分類について

国際標準規格 ISO31000:2009 を使用して,分析評価手法の内部の機能の説明をすることとする.以前,国際標準規格の中でも用語の定義が流動的であった時期があり,例えば「リスク」という用語は分野毎に異なる定義がなされていた.そこで定義統一のため ISO31000:2009 が発行され,この規格を基に関連用語の統一が行われた[31].この規格を JIS 化した JIS Q 31000:2010[32],および JIS Q 31000:2010 の補完となる JIS Q 31010:2010[33]を使用することとする.最初に, JIS Q 31000:2010 のプロセス図を図 4 に示す.

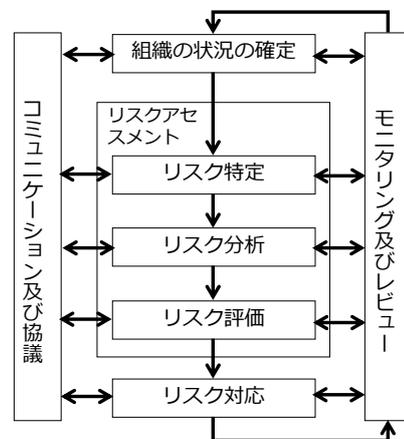


図 4 リスクマネジメントプロセス
Figure 4 Risk Management Process.

このプロセスに基づき JIS Q 31010:2010 に載っている分析評価手法のプロセスを詳細化した各機能を下記に記す[d].

(1) 組織の状況の確定

調査の目的及び適用範囲の定義.

(2) リスク特定

直接要因だけでなく背後要因の特定も含む. リスク特定には主に下記3種類の方法がある.

- ① 証拠に基づく方法: 例としてはチェックリスト及び履歴データのレビュー.
- ② 系統的チームアプローチ: 専門家のチームが系統的プロセスに従って一連の体系的なプロンプト[34] [e] 又は質問によってリスクを特定する. 例えばインタビュー、質問等.
- ③ 帰能的推論法: 例えばブレインストーミング、デルファイ法、PHA、HAZOP 等.

(3) リスク分析-結果

ある事象, 状況又は事情から発生する潜在的結果の範囲のこと. 単純な結果の記述から詳細な定量化モデル又は脆弱性分析まで, 様々なものがある.

(4) リスク分析-発生確率

起こりやすさ分析及び発生確率の算定.

(5) リスク分析-リスクレベル

結果の範囲と発生確率の算定からリスクレベルを決定.

(6) リスク評価

リスクの推定レベルと, 状況の確定時に決定するリスク基準との比較を行い, 将来の行動に関する決定を下す.

(7) リスク対応-創出

リスクを消去または低減する対策を提案.

(8) リスク対応-評価

作成した対策の優先順位を決め, 対策を決定.

(9) モニタリング及びレビュー

定めた間隔で管理基準のモニタリングやレビューを実施.

3.1.2 各機能の適用度

JIS Q 31010:2010 には 31 種類の分析評価手法が紹介されている. しかし 3.1.1 の (1) ~ (9) までの機能を全て満たす単体の分析評価手法は存在しない. 分析評価手法に共通した機能は「(2) リスク特定」であり 31 件全ての分析評価手法に含まれている. 次に多い機能は「(1) 組織の状況の確定」であり 22 件, 「(3) リスク分析-結果」は 12 件, 「(7) リスク対応-創出」は 10 件, となり, (1) ~ (3) のリスク分析に関する機能と (7) のリスク対応の創出の機能が重視されている. 他の機能は 5~9 件であり, 最も少ない機能は「(9) モニタリングおよびレビュー」の 5 件である.

d) 参考文献[33]を基に著者が手を加えて記述した.

e) リスク特定を促進するために使うことができる一連のリスク区分.

これらのことから下記のようにまとめられる.

1. 「(2) リスク特定」は確実に実施.
2. 「(1) 組織の状況の確定→(2) リスク特定」の分析評価手法が主流.
3. 「(1) 組織の状況の確定→(2) リスク特定→(3) リスク分析-結果」または「(1) 組織の状況の確定→(2) リスク特定→(3) リスク分析-結果→(7) リスク対応-創出」まで対応した単体の分析評価手法は 3 割ほど.
4. (4) リスク分析-発生確率, (5) リスク分析-リスクレベル, (6) リスク評価, (8) リスク対応-評価, (9) モニタリング及びレビュー, の機能は重要視されていない

この結果から, リスクの抽出は確実に実施するが, リスクも対応策も評価までは行わない単体の分析評価手法が多いことがわかる.

3.2 分析評価手法のマクロの特徴

ここでは製品のライフサイクルを JIS Q 31010:2010 に基づき「概念・定義段階」「設計段階」「運用段階」の 3 段階に分けた場合の適用される分析評価手法について述べる[f].

3.2.1 概念・定義段階の分析評価手法

まだ仕様が流動的であり構成が定まっていない段階であるため, データが足りない部分は「分析に含めない」または「想定して分析」せざるを得ない状態である. この段階での代表的な分析評価手法としては下記の通りである.

(1) データがない, または少ない場合に使用

- ブレインストーミング
自由発想 (創造的手法). データがない新技術, 問題の斬新な解決策が必要とされる新技術のリスクの明確化に特に有効.
- 原因影響分析
情報を特性要因図または樹形図にまとめる. 根本原因分析 (RCA) を進める方法として使用できる. ブレインストーミング用の表示技法.
- 構造化・半構造化インタビュー
質問・会話. リスクの特定・既存の管理策の有効性の評価に最も頻繁に利用. 人を集められない場合のブレインストーミングの代替として使われる.
- デルファイ法
発想と質問. 専門家が他の専門家の見解を確認しながら, 自分の意見を独自に匿名で表明. インタビューとブレインストーミングを融合したもの.
- PHA(予備的危険性評価)
発想. 簡易な帰納的分析法. 情報が限られているときも使用可. 早期にリスクの検討が可能. 詳細な評価 (HAZOP, FMEA や FTA 等) を行う前に実施.

f) 横断的などの段階でも使用できる分析評価手法が多いが, ここでは主に使用される段階を記す.

(2) データや証拠に基づいた分析

- チェックリスト
経験・過去履歴。構造化手法の代表。経験によって作成されたハザード、リスクまたは管理ミス of リスト。創造的手法の後、全検査を行うことが最も有効。
- 環境リスクアセスメント
経路分析。様々な環境ハザードへのばく（曝）露の結果として、動物、植物及び人に生じるリスクのアセスメントを網羅的に実施

(3) 簡易分析

- SWIFT(構造化 What-if 法)
系統的な What-If の質問。HAZOP の簡易代替技法として開発。HAZOP に比べて詳細さのレベルが低いシステムレベルで適用することが多い。
- シナリオ分析
将来どのようになるかについての記述的モデル展開を行う分析手法。例えば“最善のケース”、“最悪のケース”及び“予想されるケース”を表すシナリオ集を使用。モデルの仮説を基にした“what-if”形式の質問を使って、結果の“予備検証”を行う。

(4) 機能共鳴に対応した分析

- STAMP/STAP[12]
制御の相互作用の管理。構成要素間の相互作用を表すコントロールストラクチャーからプロセスモデル、安全制約を作成する。
- FRAM
理想的な機能構成を作成。機能を決め変動を定める。

3.2.2 設計段階

機能設計書など対象とするプロセスの全体図が入手可能であるが、設計変更がまだ可能な詳細設計の状態である。代表的な分析評価手法は下記の通り。

(1) 主要な分析評価手法

- HAZOP
結果と条件との差異。プロセス、システム又は手順の故障モード、その原因及び結果を特定するという点で、FMEA と類似。
- FMEA・FMECA
コンポーネント、システム又はプロセスが、どのようにして設計の意図を満たすことに失敗するかを明らかにする。FTA のような分析技法に、定性的又は定量的情報を与える。
- FTA
故障の木解析。潜在的な原因及び失敗（頂上事象）までの経路を特定。
- ETA
事象の木解析。①可能なシナリオ及び起因事象に続く一連の事象のブレインストーミング、②並びに望ましくない結果の緩和を目的とした様々な対応策、

③防壁又は管理策によって結果がどのような影響を受けるかのブレインストーミングの手がかり、④管理策の受容可能性の検討。

- CCA
FTA と ETA とを組み合わせ。

(2) 追加の分析評価手法

- LOPA (防御層解析)
原因・結果の対を選択し、好ましくない結果をもたらす原因を防ぐ防護層を特定。HAZOP や PHA に続いて、選別のプロセスを厳格に行う目的で、半定量的アプローチを採用。

3.2.3 運用段階

運用や保守など開発が終了し実際に現場で使っている状態である。特にインシデント発見および発生時に適用される。代表的な分析評価手法は下記の通り。

(1) 運用時の要因分析

- RCA (根本原因解析)
事故発生後の要因分析に使用。なぜなぜ 5 回、FMEA、FTA、特性要因図、パレート分析、根本原因マッピングなどの構造化分析の総称。

(2) 運用時のモニタリング指標値の決定

- HACCP
運用時のモニタリングのため。製品の品質に影響する事項を特定し、重要なパラメータをモニタリングでき、ハザードを管理できるプロセス管理の決定。

3.2.4 分析評価手法の適用例

概念・定義段階、設計段階、運用段階で使用される分析評価手法から適用例としては下記が考えられる。

- データがない、または少ない場合
 - ブレインストーミング（または構造化・半構造化インタビュー、またはデルファイ法、または PHA）→チェックリストまたは原因影響分析または ETA
- 後から機能仕様書などデータが手に入る場合
 - PHA→HAZOP または FMEA または FTA
- 簡易な分析を行う場合
 - SWIFT（または What-if またはシナリオ分析）
- 詳細な分析を行う場合
 - STAMP（または FRAM）→HAZOP→FTA→FMEA→LOPA

上記の通り、分析評価手法は様々な困難に合わせて手法を用意している。データが少ない開発の初期段階では、ブレインストーミングや PHA など発想的な手法を用意しており、人が一カ所に集まらない場合は、インタビューやデルファイ法など情報だけを集める手法で対処できるようになっている。また簡易に終わらせる場合や詳細に分析する場合の手法の組合せも考えられている。

3.2.5 分析評価手法を適用した時の問題

3.2.4により様々な工夫はされているが、実際の現場で使う場合での考えられる問題点は下記の通り。

(1) 手法の組合せや情報不足による実施時間の長期化

1つの分析評価手法を実施するだけでも長時間関係者を拘束することになる。複数の手法を組み合わせれば合わせるほど、更に時間が超過する。そして情報不足による分析に必要なデータがない、または不足しているのであれば想像する時間や情報入手までの待ちの時間も追加される。また、ブレインストーミングであれば1回で終わる検討が、インタビューやデルファイ法であれば集約する日時がかかり検討時間よりも長くなる。

(2) 専門家の検討する日時や場所の制約

時間短縮のためにブレインストーミングなどで検討を行うとしても、専門家を集めて多人数で実施するとなると関係者全員同じ時間で同じ場所で議論することは難しくなる。

4. 従来分析評価手法の問題

問題点を整理すると下記の通りである。

(1) 新たなリスク特定の方法が必要

ICT分野では、システムの要素機能が爆発的に増え複雑化かつ不透明化し、悪意ある攻撃も巧妙化し多種多様化してきた。セーフティ分野よりも正常と異常の判別が難しく、想定していない複数の要因が絡み合って発生する可能性もあり、要因の特定も難しくなっている。リスクを特定する際にも要素機能や要素機能間だけでなく、他の考えられる様々な事象も含めて総合的に考えていく必要もある。

(2) 評価とモニタリングの実施の課題

分析評価手法では、リスク評価と対応策評価やモニタリング機能は重視されていない。リスクや対応策の評価が不十分であれば、要因と思われたものが実は単なる事象の一つであり、事象に対する事故は減っても背後の要因は変わらないため別な事象として事故が発生する可能性が残ってしまう。またモニタリングが不十分であれば実際は不具合が発生しても気づかない可能性が高くなる。

ICT分野で適用する場合、悪意ある攻撃が主であるため不具合が隠されてしまい、セーフティに比べさらに不具合が判りにくくなることが予想される。そのためリスク・対策の評価やモニタリングの実施がさらに重要となる。しかし優先度が低いため今後も後回しにされやすい。

(3) 人・時間・場所の制約

手法の組合せや情報集約による実施時間の長期化、専門家の検討する日時や場所の制約により、更なる改善が求められる。

5. 新たな分析評価手法について

4章での問題点に対して別の視点から解決の糸口を見出していくため、別分野の類似案件との比較を行い、その分

野での解決策を参考に検討する。

5.1 新たなリスク特定の方法について

5.1.1 認知行動療法との比較

感染症治療モデルとして、インフルエンザを例にすると、症状(事象)として「発熱」があり、その根本原因(リスク源)はインフルエンザウィルスがある。根本原因であるインフルエンザウィルスに対してワクチンを接種することで根本治療(リスク源排除)となる。これは2.2.1のドミノ理論に似ている。同様に認知行動療法モデルとして、うつ病などの行動障害に対しては、周囲の不適切な対応、悪い生活習慣、ストレスなど複数の要因が重なることで発生するメカニズムは2.2.3の機能共鳴モデルに似ている。

認知行動療法には3つの系譜がある[35]。行動療法系の第1世代、認知療法系の第2世代、そして機能共鳴モデルに似ているマインドフルネス認知療法などの第3世代である。マインドフルネス認知療法は、心のコントロールよりも受け入れること、自分の行動の仕方、および考え方を受け入れていく療法である。また「受け入れる」ということで自分があるがままにしていけることが森田療法[36]と同様である[35]。心の問題の根本原因追及にはこだわらず、実際の生活でどうすれば楽になるのか今より良い生活になるのか、この考え方はレジリエンス工学の「安全を向上させるためには、うまくいかなかった物事について、その数を減らそうとするよりも、多数のうまくいった物事についてさらに改良を図るほうが、より容易でもあるし効果的でもある」[37]という考えにも近い。

5.1.2 発想法との比較

分析評価手法でもあるブレインストーミングやチェックリストは発想法でもある。「創造力辞典」[38]から分類された一部をピックアップしたものを下記に記す[g]。

1. 発散技法

- (ア) 自由連想法：ブレインストーミング
- (イ) 強制連想法：チェックリスト
- (ウ) 類比発想法：NM法、シネクティクス

2. 収束技法

- (ア) 空間型：図書分類、KJ法、クロス法
- (イ) 系列型：因果法(特性要因図)、時系列法(PERT法)

これらの中で注目すべきはKJ法である。これは川喜田二郎が考案した日本で代表的な「衆知を集める発想法」であり、先ほどの森田療法でも使用する場合がある[36]。特に分析評価手法では、図書分類のように予め決められた表に埋めていく収束技法はあるが、KJ法のように集められたデータを基に似たものをグループ化していく手法は分析評価手法にはない。このKJ法を用いて要素機能間の異常にとらわれず、背後要因を見つけていくことを提案していき

g) 参考文献[3833]を基に著者が手を加えて記述した。

たい。具体的な適用方法については今後の課題とする。

5.2 分析評価手法の一部機能のシステムによる支援

リスク・対応策の評価やモニタリング、および人・時間場所の制約については人手で実施するには限界がある。そこでシステムによる支援が考えられる。分散環境でも共同作業ができる発想支援システムを使用し、いつでもどこでも実施できる環境を提供することも可能である。例えば分散環境で KJ 法が利用できる発想支援システム[39]を使用することでリスク・対応策の評価も実施できる可能性がある。またモニタリングについては、例えばセンサ付きのウェアラブルデバイスを用いネットワークを介して状況をモニタすることが可能になる[40]。

6. おわりに

本稿では、ICT のセキュリティへの分析評価手法の適用方法について既存の分析評価手法について調査を行い、問題点の抽出と新たな運用方法について検討した。今後は新たな分析評価手法の適用方法やシステム化について検討を続けていく予定である。

参考文献

- [1] 株式会社 NTT データ。絵で見てわかる IoT/センサの仕組みと活用。翔泳社, 2015.
- [2] “The NIST Definition of Cloud Computing, National Institute of Standards and Technology” .
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf/>, (参照 2017-01-31).
- [3] “平成 28 年版情報通信白書” .
<http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/pdf/28honopen.pdf>, (参照 2017-01-31).
- [4] “重大な経営課題となる制御システムのセキュリティリスク” .
<https://www.ipa.go.jp/files/000051552.pdf>, (参照 2017-01-31).
- [5] 五郎丸 秀樹, 石本 英隆, 秋葉 淳哉, 元田 敏浩. 情報セキュリティへのヒューマンファクターズ分析評価手法の適用に関する考察 情報処理学会, vol. 2015-CSEC-71 No.4, p. 1-8, 2015.
- [6] ANDREW R. HALE and JAN HOVDEN. "Management and culture: the third age of safety. A review of approaches to organizational aspects of safety, health and environment". In Anne-Marie Feyer and Ann Williamson (Eds), Occupational Injury: Risk Prevention and Intervention, Taylor & Francis (1998).
- [7] 行待武生 他. ヒューマンエラー防止のヒューマンファクターズ. (株)テクノシステムズ, 2004
- [8] 松岡俊介. プラントの安全性評価 第 3 回 潜在危険性の特定 (その 2) . HAZOP & プラント安全促進会, 第 3 0 巻 第 1 号, pp.7-12, 2007.
- [9] “On How (Not) To Learn from Accidents” .
http://www.uis.no/getfile.php/Konferanser/Presentasjoner/Ulykkesgransking%202010/EH_AccLearn_short.pdf, (参照 2017-01-31).
- [10] ボール・サーモン 他 5 名, 小松原 明哲 訳. 事故分析のためのヒューマンファクターズ手法. 海文堂出版, 2016.
- [11] 日本規格協会. JIS Q 31010:2012 リスクマネジメントーリスクアセスメント技法, 2012.
- [12] システム安全性解析手法 WG. はじめての STAP/STPA. IPA, 2016.
- [13] Erik Hollnagel, 小松原 明哲 訳. 社会技術システムの安全分析 FRAM ガイドブック. 海文堂出版, 2013.
- [14] IPA/SEC. STAMP 手法に関する調査報告書. IPA, 2015.
- [15] H.W. Heinrich. Industrial Accident Prevention, 3rd edition. McGraw-Hill Book Company Inc., 1950.
- [16] James Reason. Human error: models and management. British Medical Journal 320 (7237), pp.768-770, 2000.
- [17] “Health Care: Safety and Resilience” .
<http://www.shotuk.org/wp-content/uploads/3.-Safety-II-SHOT-presentation-final-2.pdf>, (参照 2017-01-31).
- [18] “レジリエンス工学 残留リスクにどう向き合えばいいのか” .
http://www.meti.go.jp/committee/sougouenergy/denryoku_gas/genshiryoku/anzan_wg/pdf/006_04_00.pdf, (参照 2017-01-31).
- [19] システム安全性解析手法 WG. はじめての STAP/STPA. IPA, 2016.
- [20] Erik Hollnagel, 小松原 明哲 訳. 社会技術システムの安全分析 FRAM ガイドブック. 海文堂出版, 2013.
- [21] “HINT-HFC ヒューマンパフォーマンス事象分析支援ツール” . http://criepi.denken.or.jp/research/pamphlet/hint_hfc.pdf, (参照 2017-01-31).
- [22] 松岡俊介. プラントの安全性評価 第 2 回 潜在危険性の特定 (その 1) . HAZOP & プラント安全促進会, 第 2 9 巻 第 3 号, p.12-17, 2007.
- [23] 高野研一. 「安全率を考える」第 5 大規模システムと安全率.” J. of the Jpn. Landslide Soc”, Vol.44 No.6 421 p.78-83, 2008.
- [24] “ImSAFER によるヒューマンエラー事例分析” .
<http://www.jichi.ac.jp/msc/wordpress/wp-content/uploads/2010/08/ImSAFER-PPT5.pdf>, (参照 2017-01-31).
- [25] 野村紀男, 鹿志村芳範. 稼働中の核燃料施設における安全評価手法の検討 (技術報告) . 核燃料サイクル開発機構, JNC TN9410 2003-009, 2003.
- [26] ISO. "Quality management systems - Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations". "ISO/TS 16949:2009", 2009.
- [27] "ISO26262 におけるソフトウェア安全解析の検討(2012)".
<http://www.ipa.go.jp/files/000004108.pdf>, (参照 2017-01-31).
- [28] Adam Shostack. "Threat Modeling: Designing for Security". John Wiley & Sons, Inc., 2014.
- [29] IPA/SEC. つながる世界のセーフティ&セキュリティ設計入門. IPA, 2016.
- [30] “内部統制の評価と文書化のポイント” .
http://www.cac.co.jp/softtechs/pdf/st3001_02.pdf, (参照 2017-01-31).
- [31] “ISO 31000 の概要” .
<http://www.jsa.or.jp/stdz/iso/mngment/risk03.html>, (参照 2017-01-31).
- [32] 日本規格協会. リスクマネジメント?原則及び指針 JIS 31000:2010. 日本規格協会, 2010.
- [33] 日本規格協会. リスクマネジメント?リスクアセスメント技法 JIS 31010:2010. 日本規格協会, 2010.
- [34] PMI, PMI 日本支部監訳. プロジェクト・リスクマネジメント実務標準. PMI 日本支部, 2010.
- [35] 下山 晴彦, 神村 栄一. 認知行動療法. 放送大学教育振興会, 2014.
- [36] 川喜田二郎. KJ 法実践叢書② 人間のルネッサンス. プレジデント社, 1984.
- [37] Erik Hollnagel 他 2 名, 北村正晴, 小松原明哲監修. 実践レジリエンスエンジニアリング. 日科技連, 2014.
- [38] 高橋 誠. 新編 創造力事典 (第 3 版) . 日科技連, 2007.
- [39] 由井 隆也, 宗森 純. 発想支援グループウェア郡元の効果～数百試用実験より得たもの～. 人工知能学会論文誌 19 巻 2 号 SP-B, 2004.
- [40] 五郎丸秀樹. ヒューマンファクターズの対策方法と情報セキュリティへの適用の考察. FIT2016 情報科学技術フォーラム講演論文集, L-011, 2016.