Vol.2015-CSEC-71 No.4
2015/12/4

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

五郎丸秀樹[†1]　石本英隆[†1]　秋葉淳哉[†1]　元田敏浩[†1]

概要：近年，標的型攻撃メールや内部関係者による情報漏えいが話題となっている．これらの人間の行為によって発生する情報漏えいの分析に，ヒューマンエラーの防止を含む学問分野であるヒューマンファクターズの分析評価手法を適用することが考えられる．ヒューマンファクターズの分析評価手法を情報セキュリティに適用するには分析評価手法の特徴を理解した上で選別する必要がある．その分析評価手法は 50 以上存在し，かつ業界ごとに個別の発展を遂げているが，網羅的にかつプロセスごとに分析評価手法を分類したものはなかった．そこで各分析評価手法のプロセスのうち“要因と対策”および“対策前と対策後”に着目し，各業界で使われているヒューマンファクターズの分析評価手法を分類したところ，要因分析は対策分析に比べ多くの手法があることが判った．また情報セキュリティに適用するために，分析評価手法の問題点と課題を取り上げ，今後の進め方について検討する．

キーワード：ヒューマンファクターズ，情報セキュリティ，分析評価手法

Study on Applying Human Factors Analysis-Evaluation-Method to Information Security

HIDEKI GOROMARU[†1]　HIDETAKA ISHIMOTO[†1]
JYUNYA AKIBA[†1] and TOSHIHIRO MOTODA[†1]

Abstract: In recent years, information leakages by targeted attacks via e-mail or internal illegal operators have been spreading. In order to analyze the information leakages by human acts, it has been conceivable to apply analysis-evaluation-method of human factors which is a branch of knowledge with prevention of human error. We have needed to select the analysis-evaluation-method after understanding the characteristics of every analysis-evaluation-method. The number of type of the analysis-evaluation-method has been over 50 and the analysis-evaluation-method has been developed in individual industries. However, there have not been comprehensive and fine classification methods which classify every phase of process of analysis-evaluation-method. Therefore, we have focused on “Factor and Countermeasure” and “Before countermeasure and After countermeasure” in the process of analysis-evaluation-method and have classified every analysis-evaluation-method in individual industries. The results have shown “Factor analysis” is more than “Countermeasure analysis” in the number of classes of analysis-evaluation-method. For applying to information security, we clarify the issues and problems and discuss the direction of the future studies.

Keywords: Human factors, Information security, analysis-evaluation-method

1. はじめに

近年，実在する職場関係者を語ったメールや職場関係者にとって興味のある内容を含んだメールのように，不信感を持たせない巧妙な手口で，メールを受取った者を攻撃者の思い通りの行動へと誘導する標的型攻撃メールが現れている[1][2]．また従業員や出入りの業者など，本来は信頼できる内部の関係者が社内の規定に違反して情報を持ち出したり紛失したりしている場合がある[3]．このように技術的要因ではなく人的要因によって情報が流出する事例が報告されており，これらの事例は故意または過失も含め，従来の技術的なアプローチでは防ぐことは難しい．

例えばソーシャル・エンジニアリング[4]を用いて機密情報を獲得することも考えられる．ターゲットとなる会社のホームページから情報を入手したり会社の外にいる従業員の世間話を聞いたりして事前に準備することで，ターゲットの会社の受付や警備員を信頼させ会社に侵入するだけでなく，従業員から普通の会話をしているように見せかけて会話を誘導し，巧妙に目的の情報を入手することなどがあり得る．これらの人的要因による情報漏えいに対して，ヒューマンファクターズで用いられる分析評価手法※1を適用し，要因分析から対策の有効性の評価までを実施することも考えられ，先行研究では情報セキュリティ分野に一部の評価手法を適用した事例もある．しかし分析評価手法は様々な業界で独自に発展しており，どのような種類があり，各手法の機能の違いや適用先の範囲，手法と手法の関係について網羅的に示したものはなかった．そこでヒューマンファクターズが適用されている主要な業界および関連業界の分析評価手法を調査し，既存の分類方法や分析評価手法

†1 日本電信電話株式会社
Nippon Telegraph And Telephone Corporation

※1　分析評価手法は，分析手法，評価手法，そして手法は技法，技術とも呼ばれている．本稿では組織の状況の確定（情報収集・状況の把握），要因の特定・分析・評価，対策の策定・確定・実施・評価，の各フェーズのうち，その全てまたは一部のフェーズを持つ手法を分析評価手法と定義する．

ごとの内部処理と機能の類似性を基に分析評価手法のプロセスモデルを作成し，このプロセスモデルから分析評価手法の分類を行った．

本稿では，まず第 2 章で情報セキュリティ分野での情報漏えいの傾向を示し，ヒューマンファクターズで用いられている手法の適用事例について説明する．第 3 章では調査の目的と目標および方針について述べる．第 4 章では各業界で使用されている分析評価手法を紹介する．第 5 章では参考にすべき分析評価手法の分類について述べる．第 6 章で分析評価手法のプロセスをモデル化し，第 7 章で分析評価手法の分類を行い，その特徴を示す．最後に第 8 章で今後の方針について述べる．

2. 情報セキュリティ分野とヒューマンファクターズとの関係

2.1 情報漏えいの傾向

情報漏えいについて，世界 11 カ国（米国，英国，独国，豪州，仏国，ブラジル，日本，伊国，印国，アラブ首長国連邦，サウジアラビア，カナダ）で Ponemon Institue 社[5]が調査した．その結果，悪意ある攻撃または犯罪者による攻撃が 47%，システムの欠陥が 29%，人的ミスが 25%となった．人的ミスと悪意ある攻撃または犯罪者による攻撃を人的要因とみなすと全体の 72%が人的要因による情報漏えいであることがわかる．日本では，日本ネットワークセキュリティ協会[6]が調査した．その結果，誤操作は 34.9%，管理ミスは 32.3%，紛失・置き忘れは 14.3%となっており，「誤操作」「管理ミス」「紛失・置き忘れ」を人的要因とみなすと全体の 8 割以上が人的要因による情報漏えいであることがわかる．

日本でも世界でも 7 割以上が人的要因による情報漏えいが発生していることがわかる．情報漏えいにおいて人的要因が主要な要因になっていることから，従来の技術的な対策だけでは対応しきれなくなってきていることが考えられる．そのため情報漏えいに対する新たな対策を立案し評価する場合，人的要因への対応のため，ヒューマンファクターズで用いられている分析評価手法を適用することが考えらえる．

2.2 ヒューマンファクターズの定義

「ヒューマンファクターズ」には様々な定義が存在する．Meister[7]は同じ「ヒューマンファクターズ」という名称でも様々な内容があることを指摘している．行待ら[8]は「人々の能力や限界に適合するように機器，作業，そして作業環境を設計・改善するための学問分野である」という定義を紹介している．また「ヒューマンファクターズ」は「ヒューマンファクター」とも呼ばれており，川越ら[9]は人間/機械系における人間側の要素として「人間の特性」と定義し，佐相[10]は複数の使い方（人間の行動，諸要因の総称，学問体系）があることを指摘している．首藤[11]は，「ヒューマンファクター」は「ヒューマンエラー」から代わった新しい概念であり，これは人のエラーの要因には，人だけではなく人以外の背景（装置，設備，手順，作業環境等）に様々な問題があり，「ヒューマンエラー」では表現しきれないためである．そしてその学問体系を「ヒューマンファクターズ」と呼んでいる．

情報漏えいには，防御する情報通信技術だけでなく，情報の価値を示す手法を持つ経済学や人の行動をモデル化する心理学などの様々な分野の要素が複雑に絡んでいる．そのため，ある領域に特化した狭い範囲ではなく，分析評価手法について幅広く調査を行うことが有益であると考えた．本稿では，「ヒューマンファクターズ」を学問分野（体系）として広く扱うこととする．これらのことにより狭い意味での「ヒューマンファクターズ」や「ヒューマンエラー」だけでなく，その関連する他の分野も含め，幅広い意味での「ヒューマンファクターズ」とする．

2.3 情報セキュリティへの分析評価手法の適用事例

佐々木ら[12]は，情報セキュリティに適用する分析評価手法を示した．その手法として 4 M 分析（4 M-5E）[13]，SHEL モデル（m-SHEL）[8] および「発想手順マトリックス」[8] を紹介している．またヒューマンエラーの対策案の中身として対処療法的対策が多く，それゆえ対策が多くなる問題を指摘している．

富樫ら[14]は，ISMS を導入しても人的要因の情報漏えいが多発しているため現在のリスクアセスメントが期待通りに機能していないことを指摘し，脅威と脆弱性を含めたリスク規定や，（非技術的・技術的）ヒューマンエラー管理強化を述べている．要因分析に，時系列事象関連図[8]，いきさつダイヤグラム[8] ，VTA[8] を比較検討し，事象の整理と問題点の把握において他の手法よりも優れた VTA と，対策立案に，H^2-SAFER の 4 STEP/M[8]と m-SHEL[8]の組合せでメールでの情報漏えいを模擬し要因分析と対策立案を行った．

安藤ら[15]は，Medical SAFER (Medical Systematic Approach For Error Reduction) [16]，FTA (Fault tree analysis) [17]，FMEA(Failure Mode and Effect Analysis)[17]を情報セキュリティに適用し比較を行った．その結果，リスク分析においてはヒヤリハットをできるだけ洗い出せる FTA がよく，FTA で洗い出したリスクを「発想手順マトリックス」を用いて対策案を作成すると効率が良いことがわかった．

これらの事例から，ヒューマンファクターズを情報セキュリティ分野で用いる際の留意点が示され，一部の分析評価手法が情報セキュリティ分野に適応可能であることはわかった．しかし分析評価手法の種類がどれだけ存在し，ど

ういう特徴の違いがあるのか網羅的に述べたものはなかった．適用した手法が最適な手法なのか，さらに適切な手法があるのかなどが課題として残っている．

3. 調査の目的と目標および方針

ヒューマンファクターズで用いられている分析評価手法について不明点が多い．そのため分析評価手法による情報セキュリティ分野での人的要因の情報漏えいへの対応を目的とするが，情報セキュリティ分野の特徴に合わせた分析評価手法の適用方法の検討の前に，まず分析評価手法の特徴を把握し分類することまでを目標とした．そして分析評価手法の基本プロセスモデルの構築を手段として，下記の方針で調査を実施した．

（1） 分析評価手法の調査

ヒューマンファクターズが適用されている業界，および分析評価手法の既存分類から，分析評価手法の現状を把握し，分析評価手法を抽出する．

（2） 分析評価手法のプロセスモデルの構築

抽出した分析評価手法のプロセスを分析し，その特徴を把握して共通部分を見つけ出し，新たな共通のプロセスモデルを構築する．

（3） 分類の実施

作成したプロセスモデルの各フェーズに分析評価手法を当てはめ分類を実施する．

4. 各業界での分析評価手法の調査

4.1 各業界の現状把握

航空業界は，人的要因による分析評価手法をいち早く開発し大きく発展した分野である．その理由として，事故が人間の大量死に直接結びついているため危機意識があり，以前から人と人との意思疎通や機械との取り扱いが重要視されていた．昔から危ないことを行っている自覚があったことを示す例として「ハンガーフライト」と呼ばれるパイロットたちの経験談の口伝による情報共有の場があったことが挙げられる [8] [18]．そのためインシデントが収集しやすくなるように4M-4EやSHELという表に埋めることで網羅的に要因を抽出する分析評価手法がいち早く取り入れられたと考えられる．

原子力業界では大事故が発生すると甚大な被害を与える可能性がある．炉心溶解に至る確率を計算するためPRA(Probabilistic Risk Assessment:確率論的リスク評価)※2, QRA(Quantitative Risk Assessment:定量的リスク評価)などのリスク評価が発展してきた[19]．分析評価手法では人的過誤率を考慮した THERP(Technique for human error rate prediction) や ATHEANA(A Technique for Human Event Analysis)など HRA(Human Reliability Analysis:人間信頼性解析) [20]系の誤操作による事故発生確率を推定する分析評価手法が開発されてきた[21].

医療業界は，類似した医療事故が再発していたが，病院および業務システムは多様な特徴を持ち複雑であったため根本的な解決に至らず航空業界や原子力業界に比べて遅れていた．しかし“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[18]．医療の現場では，人的要因の特定が重視され，不慣れな医療従事者にも専門的な知識なしに分析や対策に取り組みやすい分析評価手法が望まれている．そのため専門知識が必要なFMEA(Failure Mode and Effects Analysis:故障モード影響解析)よりも VA-RCA(Veterans Affairs National Center of Patient Safety – RCA)や Medical SAFER といった分析評価手法が用いられている[8].

化学プラント業界では，規格などで分析評価手法としてHAZOP(Hazard and operability study)が推奨されていたため定着した．また HAZOP は流量などの内部におけるプロセスや運転の正常状態からの乖離を確認する手法であり，火災や地震といった外部要因については取り扱わないためチェックリストとの併用が行われている[22].

自動車業界では，規格などで分析評価手法として FMEA が業界で推奨されていたため定着した．FMEA は故障モードを設定しシステムの機能への影響や危険事象を特定する技法であり，自動車だけでなく製造系や宇宙産業等の大規模かつ複雑なハードウェアシステムの信頼性解析に幅広く使用された手法でもある[23].

各業界で分析評価手法が定着した要因としては，業界自体が事故に対して大きな危機意識を持つことや，規格や業界で推奨されている分析評価手法であることが考えられる．また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箇所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，評価対象（ハードウェア，業務のプロセス等）などである．このように各業界で重視している箇所に合わせて独自に発展し分析評価手法の種類が増えたために網羅的な分類が難しくなったと考えられる．

4.2 各業界の分析評価手法

航空業界は， 4M-4E, RCA(Root cause analysis), SHEL 等の手法が考案され，インシデント報告制度として，米国では ASRS(Aviation Safety Reporting System:航空安全報告システム)が 1975 年に発足した[8][18][24]. 法律で刑事免責を確立し匿名性も確保しているため，パイロット等が安心してインシデントを報告できるようになり，かつデータベース

※2 PRA は PSA(Probabilistic Safety Assessment:確率論的安全評価)とも呼ばれており，PRA＝RSA＝頻度・確率×影響・被害 となる．

で管理できるようにもなっている[8].

原子力業界は,航空業界の ASRS を基に米国で 1982 年に HPES（Human performance enhancement system:人間行動改善システム）を開発した[8]. 日本では 1990 年に米国の HPES の日本版として J-HPES を開発し，さらに 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 H^2-SAFER(Hiyari Hatto - Systematic Approach For Error Reduction) や HINT-HFC (Human performance Incidents analysis tool – Human factors Research center)を開発した[8][25][26][27]．またリスク評価として，PRA と QRA があり，ETA(Event Tree Analysis)や FTA(Fault Tree Analysis), これらを統合した C&C（Cause and Consequence Analysis）※3といった分析評価手法で使用されている[19]. 特に PRA には, HRA という人間のエラー確率を予測する解析方法というものがある[20]．第一世代の HRA である THERP は人間のエラー確率に PSF の要素を含む分析評価手法である[28]. また第二世代の HRA である ATHEANA は，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ことを可能にした分析評価手法である[29].

医療業界は，4M-4E や RCA など航空業界で使用されていた手法を医療業界に適用している．米国退役軍人病院の患者安全センターで開発された VA-RCA や原子力業界で使用されていた H^2-SAFER を元に医療の実態に合わせて作られた Medical SAFER などがある. そして VA-RCA の考え方を取り入れ Medical SAFER を拡張した ImSAFER (Improvement SAFER)も使われている[8] [18] [30]

化学プラント業界は，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 [8] [18]. また HAZOP 以外にも複数の手法を使用している．例えば，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[31].

自動車業界では，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[32]. 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[33].

5. 既存分類からの分析評価手法の調査

Hollnagel ら[34]は，Perrow[35]の”The coupling-intercation diagram”を活用してシステム内のアイテム間の緊密度(Coupling)を縦軸に，精密度（Description）を横軸にして 9 種類の手法を図で分類した．その結果，①RCA, J-HPES , HERA(Human Error in European Air Traffic Management)などは製造業などの事故が単発でかつ扱いやすいシステム（低い緊密度かつ低い精密度）で利用され，②MTO (Man – Technology – Organization)などはダムや電車など事故が拡大しやすくかつ扱いやすいシステム（高い緊密度かつ低い精密度），③FRAM（the FUNCTIONAL RESONANCE ANALYSIS METHOD）[36]などは原子力発電所や金融相場など事故が拡大しやすくかつ扱いにくいシステム（高い緊密度かつ高い精密度）で用いられる手法と示した．さらに Hollnagel は改良した図を用いて 24 種類の手法を分類した[37]．しかし情報システムは各業界で用いられているため，情報セキュリティ分野を上記の①②③のどのカテゴリーに含めるのかは難しい．例えば製造業の情報セキュリティでは①となるが原子力業界の情報セキュリティであれば③になり, 情報セキュリティ分野はこの分類では適用できない.

尾崎ら[38]は，縦軸を定量的・定性的，横軸を事前・事後に分けた．定量的の範囲では，事前分析は THERP などの HRA，事後分析は ETA, FTA, VTA などである．定性的の範囲では, 事前分析はガイドライン評価やチェックリスト，事後分析はなぜなぜ分析（RCA）に分類される．この分類では，リスク分析は事前分析にも事後分析にも含まれるため，別の軸が必要となり不十分である.

JIS Q 3110[17]は，リスクアセスメントの観点から分類している．31 種類の手法をプロセス（リスク特定，リスク分析, リスク評価）と影響要因の関与度（資源及び人の能力，リスクの不確かさの性質及び程度，問題の複雑さ，定量的アプトプットの可否）で分けている．この分類ではリスク分析しか述べられておらず，対策の評価については述べられていない.

そしてこれらの分類では，分類する評価者の観点の違いから取り扱う手法の粒度や範囲が異なるため，同じ次元での網羅的な評価がなされていない．例えば Hollnagel は 24 種類，JIS Q 3110 では 31 種類の手法を挙げているが，重なっている手法は 4 種類であること，尾崎らや JIS Q 3110 では複数の手法を HRA として一括りにまとめているが，Hollnagel は THERP , ATHEANA, CREAM (Cognitive Reliability & Error Analysis Method) など HRA を細かく分けている.

6. 分析評価手法のプロセスモデルの構築

4 章の各業界の分析評価手法および 5 章の既存分類から，分析評価手法の業界横断的な分類は無く，既存分類においても一部の分析評価手法にしか対応しておらず，どうやって網羅的に分析評価手法を把握していくのか課題がある．そこで我々は網羅的に分析評価手法を把握していくために分析評価手法のプロセスに着目して新たな分類手法を考案することとした．まず各分析評価手法のプロセスを比較し

※3 C&C は CCA と呼ばれる場合もある.

て見ると下記の事がわかった．

- 「要因」と「対策」の共通項があることが多い．
- 対策前と対策後では同じ「要因」や「対策」であっても，必ずしも同様の分析評価手法を使うわけではないこと．
- 数が多く軽微なヒヤリハットなどの危険度の低いインシデントには 4E-4M や SHEL などの簡易手法が使われている．反対に数は少ないが重大事故などの危険度の高いインシデントには HAZOP や FMEA または複数の手法の組み合わせなどの詳細手法が使われている．またシステム設計，建設，改造などでも詳細手法が使われており，場面によって分析評価手法が使い分けられている．

そこでリスクマネジメントプロセス[39]を参考に用語とフェーズを定義し全体のプロセスを決めていった（図 1）．まず全体のプロセスを「対策前」「対策後」に大きく 2 つに分けた．次に「①リスク調査」「②対策案調査」「対策後」「③対策後調査」「④要因調査」の 4 つのフェーズに分けた．

①リスク調査は，どのようなインシデントが発生するのかを予想しながら考えられる要因をできるだけ多く網羅的に作成する作業に対し，④要因調査では，既に発生した具体的なインシデントに対しての要因，場合によっては背後要因を絞り込んでいく作業であるため，使用する分析評価手法が異なる場合がある．また，②対策案調査は，①で抽出された要因に対しての対策を数多く考案し適切な対策に絞り込んでいく作業であり，③対策後調査は，対策を実施した効果を調べる分析（③-A）と，長期にわたって得られたデータから新たな傾向を発見する分析（③-B）の 2 つの作業に分けられる．②と③-A と③-B はそれぞれ異なる作業であるため異なる分析評価手法を使用することとなる．

そして「1 状況の確定」から「8 要因の査定」までの 8 つのフェーズに分け簡易フローを作成した．詳細は下記の通り．

1. 状況の確定：リスクマネジメント[39]の「組織の状況の確定」にあたる．情報を収集し，状況（作業）の分析と確定（把握）を行う．
2. 要因の査定：リスクマネジメントの「リスクアセスメント」にあたる．リスク（要因）を特定し，リスク（要因）を分析し，リスク（要因）を評価する．
3. 対策の創出：リスクマネジメントの「リスク対応」の前半にあたる．リスク（要因）への対策案を創出する．
4. 対策の査定：リスクマネジメントの「リスク対応」の後半にあたる．対策案を分析し，対策案を評価し対策案を決定する．
5. 対策の実行：決定した対策案からシステムを構築したり組織のルールを変更したりするなど対策を実施し運用する．必要に応じて監視を実施しデータの収集や状況の予測を行う．
6. 対策の査定：対策後の効果を評価する．対策前と対策後の比較を行い効果の有無を確認，または長期に貯めた蓄積データを分析して傾向や相関があるのかを確認したりする．
7. 状況の確定：リスクマネジメントの「組織の状況の確定」に近い．インシデント発生後の情報収集および状況（事象）の分析と確定（把握）を行う．
8. 要因の査定：リスクマネジメントの「リスクアセスメント」に近い．要因を特定し，場合によってはさらに背後の要因を分析し，要因を評価する．

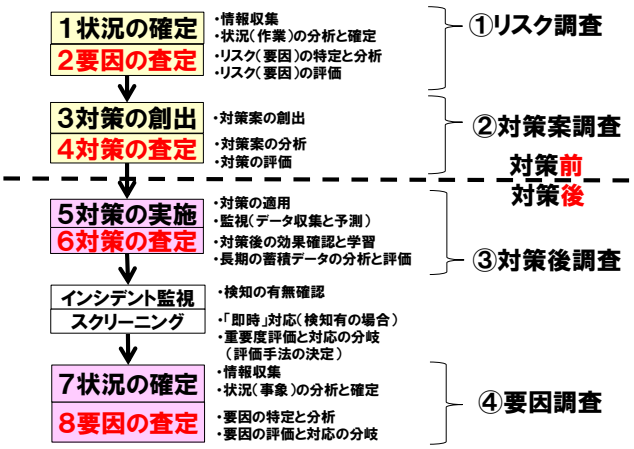

図 1　分析評価手法の簡易プロセス
Figure 1 A simple process of evaluation method.

また図 1 は簡易モデルであって，実際の運用では処理の順番が変わる．「開発時：設計・建設・能増・改造」，「運用時：運用・定期調査」，「事故時：事故・要因調査」の 3 つの状態での分析評価手法のプロセス例を図 2，図 3，図 4 に示す．

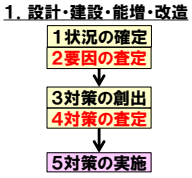

図 2　開発時の分析評価手法の詳細プロセス例
Figure 2 An example of detailed process of analysis-evaluation-method in development.

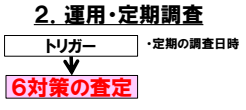

図 3 運用時の分析評価手法の詳細プロセス例
Figure 3 An example of detailed process of analysis-evaluation-method in operation.

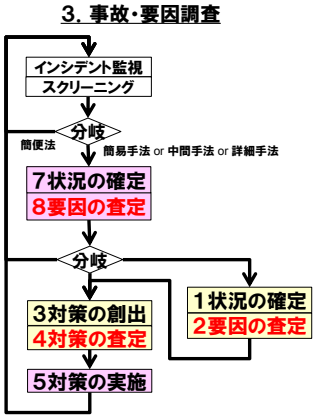

図 4 インシデント発生時の分析評価手法の詳細プロセス例
Figure 4 An example of detailed process of analysis-evaluation-method in incident occurrence.

7. 分析評価手法の分類の実施

7.1 分類の方針

図 1 の簡易モデルから分類のための表を作成する．手法のレベルは厚生労働省指針[40]や ImSAFER の事例[30]を参考にして分析評価手法の分析のレベルの使い分け（簡易分析，中間分析，詳細分析など）を行った．その結果を表 1 に示す．

表 1 分析評価手法の手法レベルを含んだ区分
Table 1 A classification containing method levels for analysis-evaluation-method.

項番	プロセスのフェーズ		手法レベル
1	①リスク調査	1 状況の確定	-
2-1		2 要因の査定	1 簡易手法
2-2			2 中間手法
2-3			3 詳細手法
3-1	②対応策調査	3 対策の創出	1 簡易手法
3-2			2 中間手法
3-3			3 詳細手法
4		4 対策の査定	-
5	③対策後調査	5 対策の実施	-
6		6 対策の査定	-
7	④要因調査	7 状況の確定	-
8-0		8 要因の査定	0 簡便手法
8-1			1 簡易手法
8-2			2 中間手法
8-3			3 詳細手法

分析評価手法の種類が多く全てを提示することは難しい．また，分析評価手法は複数のフェーズにまたがるものや，複数の分析評価手法を集めて一つの分析評価手法にしたもの，同じフェーズでも手法レベルによって使い分けされるものもある．そのため下記の方針とする．

（1） 同じ源の分析評価手法は，大きな違いが無ければ同じグループに含め代表的な名前を付ける．

- 4M-4E, 4M-5E, 5M-7E などは 4M-4E とする．
- SHEL, m-SHEL, P-mSHEL, C-SHEL は SHEL とする．
- H2-SAFER，Medical-SAFER，ImSAFER は SAFER とする．
- FMEA, FMECA, HFMEA などは FMEA とする．

（2） 同じ分野の分析評価手法は，大きな違いがなければ同じグループに含め代表的な名前を付ける．

- OAT(Operator Action Tree)，TRC(Time Reliability Correlation)，HCR(Human Cognitive Reliability correlation)，THERP，SLIM-MAUD，INTENT，CREAM ATHEANA，MERMOS，ADS-IDS，SAMARA などは HRA とする．

（3） 複数のフェーズにまたがる分析評価手法は，それぞれのフェーズで個別に表示する．

（4） 分析評価手法内またはグループ内のフェーズに固有の名前がある場合は固有の名前も表示する．

7.2 分類の実施と特徴の確認

7.1 節の方針に基づき分類した表を表 2 に記す．

表 2 各フェーズで使用される分析評価手法の一覧 ※4
Table 1 A list of analysis-evaluation-method which is used in every phase.

項番	分析評価手法
1	1-1 FMEA [サブプロセス化]、1-2 BPMN(ビジネスプロセスモデリング表記法)[41]、1-3 SAFER[時系列事象関連図]、1-4 ＰＳＦに基づくヒューマンエラー防止手法[42] [いきさつダイヤグラム]、1-5 VTA、1-6 FRAM
2-1	2-1-1 チェックリスト、2-1-2 4M-4E、2-1-3 What-IF、 2-1-4 デルファイ法、2-1-5 PHA
2-2	2-2-1 FMEA [エラーモード→RPN]、2-2-2 共通要因分析、2-2-3 FTA、2-2-4 ETA、2-2-5 CCA、2-2-6 JSA/HRA、2-2-7 HAZOP、2-2-8 シミュレーション法、2-2-9 VaR、2-2-10 コートニィ理論、2-2-11 ALE、2-2-12 GMITS、2-2-13 RR、2-2-14 JRMS、2-2-15 CRAMM
2-3	2-3-1 FRAM→HAZOP→FTA→FMEA→HRA、2-3-2 HAZOP→FTA→FMEA→HRA，2-3-3 HAZOP→FTA→FMEA、2-3-4 ＰＳＦに基づくヒューマンエラー防止手法 [リファレンス・リスト（PSF 抽出） → 要因マトリックス（仕分け）]、2-3-5 潜在危険性抽出(HAZOP or What-If /チェックリスト)→特に重要な危険性の深堀(FTA or ETA or CCA)
3-1	3-1-1 4M-4E
3-2	3-2-1 SAFER [発想手順マトリクス]、3-2-2 FMEA [対策案作成]
3-3	3-3-1 ＰＳＦに基づくヒューマンエラー防止手法 [Multi-Facet 対策支援法]
4	4-1 FMEA [HFMEA:SPN]、4-2 SAFER [対策決定・効果評価]、4-3 ＰＳＦに基づくヒューマンエラー防止手法 [対策案の評価]
5	5-1 IRS(インシデントレポートシステム)、5-2 アンケート（インタビュー）
6	6-1 単純集計、6-2 統計的分析
7	1-3 SAFER[時系列事象関連図]、1-4 ＰＳＦに基づくヒューマンエラー防止手法 [いきさつダイヤグラム]、1-5 VTA
8-0	8-0-1 軽微事象対応（安全啓発シート作成等）
8-1	8-1-1 SAFER [QuickSAFER] 2-1-2 4M-4E、2-1-3 SHEL
8-2	8-2-1 SAFER [背後要因関連図] 、8-2-2 VA-RCA[出来事流れ図]、8-2-3 TapRoot、8-2-4 HINT-HFC(J-HPES) [要因関連図] 2-2-1 FMEA [エラーモード→RPN]、2-2-2 HAZOP、2-2-3 FTA、2-2-4 共通要因分析、2-2-5 ETA、2-2-6 CCA
8-3	2-3-1 FRAM→HAZOP→FTA→FMEA→HRA、2-3-2 HAZOP→FTA→FMEA→HRA，2-3-3 HAZOP→FTA→FMEA、2-3-4 ＰＳＦに基づくヒューマンエラー防止手法 [リファレンス・リスト（PSF 抽出） → 要因マトリックス（仕分け）]、2-3-5 潜在危険性抽出(HAZOP or What-If /チェックリスト)→特に重要な危険性の深堀(FTA or ETA or CCA)

※4 [8][30][31][33][40][41][42]を元に著者が手を加え作成した．

また図 1 の８つのフェーズを見ると，２と８は「要因の査定」，４と６は「対策の査定」がある．これらは要因関連および対策関連の処理を表しており，対策前と対策後でそれぞれ分かれている．そこで全体の特徴を見るために図 1 の①～④のフェーズを参考に各分析評価手法を分類した（図 5）．その結果，図 5 の①④の要因の査定に手法が集中しているが，図 5 の②③の対策の査定は手法が少なく，特に③は殆ど言及がないことが判った．これは，事実の把握が最も重要であり，事象の流れが明らかになれば分析はほぼ終わったようなもの，という考え方[43]があるためである．つまり「要因の査定」は「対策の査定」よりも重視しているということである．

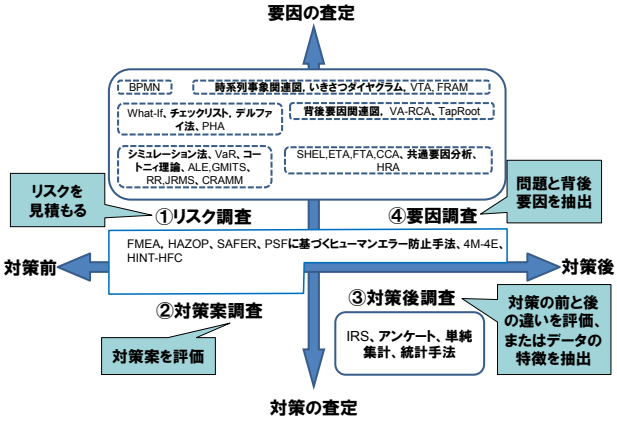

図 5　ヒューマンファクターズにおける分析評価手法の分類

Figure 5 A classification map of analysis-evaluation-method of human factors.

8. 今後の方針

表 1 と表 2 を作成し分析評価手法を分類したが，まだ情報セキュリティに適用する場合に分析評価手法を選択する上での問題や課題は残っている．例えば，「各手法の使い分けの基準」の問題がある．これは，分析評価手法を各フェーズでレベルごとに分けたとしても複数の分析評価手法があり，その全ての分析評価手法を実際に適用し比較検討を実施していないため何を基準にして選択すればよいのかが分かっていない．そして分析評価手法には結果の値として，定量値を出すものや定性値を出すもの，絶対値または相対値を出すものなどがある．また簡易手法であれば便利だが解析結果が不十分なものになり，精度を高めた詳細手法であれば手間や時間がかかるため敬遠され分析評価手法が使われなくなる危険性がある．

上記の例も含め，分析評価手法を使用する上での分析評価手法自体の課題を表 3 に示す．これらの課題に全て答えることは難しいため，段階的に規模を拡大し解決していくこととする．まずはスモールスタートとして現場での定着を目指し（図 6），次の方針とする．

- 導入期は簡便な手法を選択

  特殊な訓練や情報が入手しづらい手法は避ける．体制づくりやシステム作り，ログや報告のデータベース構築等 [表 3 の a-1, a-2, b-1, b-2, e-1] ．また将来複雑な手法を取り入れることを考慮する．
- 各手法の適切な運用（使い分け・組合せ）

  簡易手法の不足を補い，要因と対策の偏りや具体性のなさを回避する[表 3 の a-1, a-2, b-1, b-2, c-1, c-3, d-1, e-1].
- 対策案の評価で定着度やプライバシーも考慮

  改善策の未実施または不完全な運用を避ける（例えば評価項目に含める等)[表 3 の c-4, c-5, c-6] ．
- 他分野の方策を導入

  対策の効果向上と情報セキュリティの要求条件を尊守する（例:行動学や心理学等のアプローチを取り入れる） [表 3 の b-3, c-4, c-5, c-6].
- 対策の高度化

  自動化などフールプルーフ化を進めることと同時に，安全文化を適用し，人が状況に応じてシステムを守るという視点で評価する [表 3 の c-2].

今後は実際に情報セキュリティ分野に適用し，分析評価手法の比較を行う予定である．

表 3　分析評価手法を使用する上での課題

Table 2 The issues of using analysis-evaluation-method.

区分	課題
a.共通	a-1. 各手法の使い分けの基準はどうするか a-2. 指標は、定量値か定性値か、絶対値か相対値か、予測や対策をどこまで実施するか
b.リスク分析	b-1. リスト(要因やエラーリスト、チェックリスト等)の準備はどうするか b-2. リスク(発生確率と被害の大きさ)のデータの準備はどうするか b-3. 人の属性についてはどう対処するか
c.対策案分析	c-1. 対策の偏りを低減するにはどうするか c-2. ヒューマンエラーの低減範囲はどうするか c-3. 対策内容を具体化するにはどうするか c-4. 対策の実効性を高めるにはどうするか c-5. プライバシーへの配慮をどうするか c-6. セキュリティ対策疲れを回避するにはどうするか
d.要因分析	d-1. インシデント取得の範囲はどうするか
e.対策後分析	e-1. 対策後の評価手法についての言及が少ないが大丈夫か

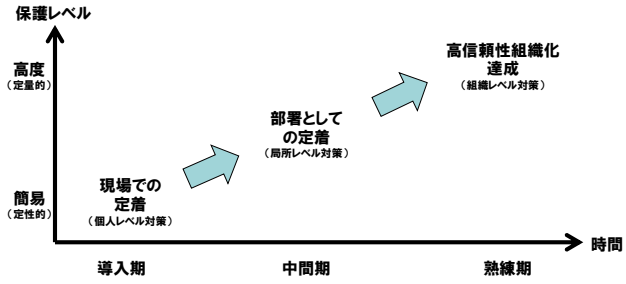

図 6　今後の分析評価手法の適用方針

Figure 6 Future policies for applying analysis-evaluation-method.

参考文献

1) 不正アクセスによる情報流出事案に関する調査委員会：不正ア

クセスによる情報流出事案に関する調査結果報告，日本年金機構 (2015), http://www.nenkin.go.jp/files/kuUK4cuR6MEN2.pdf (参照 2015.10.13).
2) 岡野裕樹，木邑 実，辻 宏郷，青木眞夫：IPA テクニカルウォッチ「標的型攻撃メールの例と見分け方」，独立行政法人情報処理推進機構 技術本部 セキュリティセンター(2015), https://www.ipa.go.jp/files/000043331.pdf.(参照 2015.10.13).
3) 佐藤栄俊：情報セキュリティ編～情報漏洩における人的リスク～, SPN リスクフォーカスレポート vol.02, 株式会社エス・ピー・ネットワーク 総合研究室(2013), https://www.sp-network.co.jp/pdf/riskfocusreport_02_1306.pdf (参照 2015.10.13).
4) クリスオファー ハドナジー（翻訳：成田光彰）：ソーシャル・エンジニアリング，日経 PB 社(2012).
5) Ponemon Institute 社 : “2015 年 情報漏えい時に発生するコストに関する調査:グローバル分析”，IBM(2015).
6) NPO 日本ネットワークセキュリティ協会 セキュリティ被害調査ワーキンググループ，情報セキュリティ分大学院大学 原田研究室 廣松研究室 : 2013 年情報セキュリティインシデントに関する調査報告書(2012).
7) Meister,D.: “Human Factors: Theory and Practice (Wiley series in human factors)”, John Wiley & Sons Inc(1971).
8) 行待武生：ヒューマンエラー防止のヒューマンファクターズ，株式会社テクノシステムズ(2004).
9) 川越秀人, 内田勝也 : 情報セキュリティのヒューマンファクタ，情報処理学会 研究報告，2008-CSEC-41(2), pp.7-12 (2008).
10) 佐相邦英：原子力教科書 ヒューマンファクター概論，オーム社（2009）.
11) 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), https://www.sonpo.or.jp/archive/publish/bousai/jiho/pdf/no_223/yj22342.pdf (参照 2015.10.13).
12) 佐々木崇裕，原田要之助：運用におけるヒューマンファクターに着目した情報セキュリティ対策について，情報処理学会研究報告，Vol.2014-EIP-63 No.13(2014).
13) 岡田有策：ヒューマンファクターズ概論－人間と機械の調和を目指して，慶応大学出版会(2005).
14) 富樫由美子，佐藤嘉則，藤井康広：企業の情報セキュリティ対策におけるヒューマンエラー管理実践に向けた検討，情報処理学会研究報告，Vol.2009-SE-164 No.1(2009).
15) 安藤玲未，芦野祐樹，島 成佳：IT システム運用時におけるインシデント分類に関する一考察，情報処理学会研究報告，Vol.2014-SPT-8 No.33(2014).
16) ImSAFER 研究会，http://www.medicalsafer-kts.com/index.html (参照 2015.10.13).
17) 日本規格協会：リスクマネジメントーリスクアセスメント技法，“JIS 3110:2012”（2012）.
18) 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 pp.78-83 (2008).
19) 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２９巻 第３号, pp.12-17 (2007).
20) 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３０巻 第１号, pp.7-12 (2007).
21) 土屋 仁：HAZOP を用いた医療事故分析，鈴鹿医療科学大学大学院(2014), http://www.suzuka-u.ac.jp/information/bulletin/pdf/2014/15_01_tuchiya.pdf (参照 2015.10.13).
22) 高野研一：原子力プラント運転操作に係わる人間特性分析・評価手法の開発と適用，名古屋大学(1995).
23) 財団法人 電力中央研究所：HINT-HFC ヒューマンパフォーマンス事象分析支援ツール（2009），http://criepi.denken.or.jp/research/pamphlet/hint_hfc.pdf (参照 2015.10.13).
24) 財団法人 電力中央研究所:知的財産報告書 2007 年度版(2008), http://criepi.denken.or.jp/result/pub/chiteki/2007/2007.pdf (参照 2015.10.13).
25) 財団法人 電力中央研究所：研究の歩み, http://criepi.denken.or.jp/jp/hfc/main/history.html (参照 2015.10.13).
26) 国立研究開発法人産業技術総合研究所：詳細リスク評価テクニカルガイダンスー 詳細版 －その４ 分布のあるデータの処理－ より定量的なリスク評価のために －, https://unit.aist.go.jp/riss/crm/mainmenu/tech_guidance04.pdf (参照 2015.10.13).
27) 独立行政法人 原子力安全基盤機構：平成 21 年度 PSA に係る人間信頼性解析手法の高度化検討に関する報告書（2011）, http://www.nsr.go.jp/archive/jnes/content/000117644.pdf (参照 2015.10.13).
28) 尾崎禎彦，大井 忠：原子力プラント運転・保守におけるヒューマンエラー評価技術に関する研究-分析・評価ツール-，福井工業大学研究紀要 第 41 号(2011).
29) 独立行政法人 原子力安全基盤機構:平成 22 年度 PSA に係る人間信頼性解析手法の整備に関する報告書(2012), http://www.nsr.go.jp/archive/jnes/content/000123426.pdf (参照 2015.10.13).
30) 河野龍太郎: ImSAFER によるヒューマンエラー事例分析 (2010), http://www.jichi.ac.jp/msc/wordpress/wp-content/uploads/2010/08/ImSAFER-PPT5.pdf (参照 2015.10.13).
31) 野村紀男，鹿志村芳範：稼動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).
32) 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).
33) 株式会社 OTSL : 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 2015.10.13).
34) Erik Hollnagel, Josephine Speziali: Study on Developments in Accident Investigation Methods: A Survey of the State-of-the-Art (2008), https://hal.archives-ouvertes.fr/hal-00569424/document (参照 2015.10.13).
35) Charles Perrow: “Normal Accidents: Living With High-Risk Technologies (Princeton Paperbacks)”, Princeton Univ Pr(1998).
36) Erik Hollnagel (翻訳：小松原 明哲) : 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).
37) Erik Hollnagel: The Requisite Variety of Risk Assessment:Catching up with nature (2011), http://www.cambrensis.org/wp-content/uploads/2012/05/Plenary-lecture-3-by-Erik-Hollnagel1.pdf (参照 2015.10.13).
38) 尾崎禎彦，大井 忠：原子力プラント運転・保守におけるヒューマンエラー評価技術に関する研究-分析・評価ツール-，福井工業大学研究紀要 第 41 号(2011).
39) 日本規格協会：リスクマネジメント−原則及び指針，“JIS 3100:2010”(2010).
40) 松岡俊介: プラントの安全性評価 最終回 リスクアセスメント, HAZOP & プラント安全促進会，第３１巻 第１号, pp.12-18(2007).
41) 梅田正隆：プロセス図の描き方とお作法--実は超簡単 !, ZDNet Japan (2009), http://japan.zdnet.com/print/20389449/(参照 2015.10.13)
42) 行待武生: : PSF に基づくヒューマンエラー防止手法(2008), http://qasg.com/d_repo/121-1.pdf/(参照 2015.10.13)
43) VA-RCA と Medical SAFER の違い（１）―出来事流れ図と時系列事象関連図―，Medical Human Factors TOPICS（2010），http://www.jichi.ac.jp/msc/wordpress/wp-content/uploads/2010/06/mhf-120.pdf (参照 2015.10.13).