Vol.2009-SE-164 No.1
Vol.2009-EMB-13 No.1
Vol.2009-CSEC-45 No.1
2009/5/28

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

冨樫由美子[†]　佐藤嘉則[†]　藤井康広[†]

本研究では，情報記録媒体紛失，メール誤送信などのヒューマンエラーに起因する情報セキュリティ事故発生のリスクを最小化することを目的とし，情報セキュリティ分野向けのヒューマンエラー管理フレームワーク(FW)の確立を目指す．ヒューマンエラー管理 FW 実現のための技術として，主に医療分野で使われているエラー分析・対策立案手法をセキュリティ事故事例へ実験的に適用し，手法の活用可能性を検討した．

Human Errors Management Framework in Information Security

Yumiko Togashi[†]　Yoshinori Sato[†]　Yasuhiro Fujii[†]

In this study, it aims to minimize the risk of the information security accident that occurs in human errors: record medium loss and e-mail wrong transmission and so on. Our goal is to establish human error management framework in information security. This paper describes case studies of applying the human error analysis and the measures plan techniques that have been chiefly used in the medical field.

1. はじめに

近年，情報漏えい事故に対する社会的関心が非常に高まり，多くの企業や行政組織で様々な情報漏洩対策がなされている．しかし，情報漏えい事故はいっこうに収まる様子がなく，さらに事故原因の半数以上は管理の手違い，情報格納媒体の紛失，FAX や電子メール誤送信など，ヒューマンエラーに起因するとの報告が出ている[1].

本研究は，ヒューマンエラーに起因する情報セキュリティ事故発生のリスクを最小化することを目的とし，情報セキュリティ分野向けのヒューマンエラー管理フレームワークの確立を目指す．具体的には，ヒューマンエラー管理フレームワークの実現技術の一つとして，要因分析・対策立案を体系的に行える手法が開発目標となる．

本研究では，情報セキュリティ向けのヒューマンエラー管理手法を確立すべく，まずは電力，医療など他の分野で利用実績のある要因分析・対策立案手法を出発点としてとして，情報セキュリティ向けの手法を新たに確立するアプローチをとる．本稿では，既存の要因分析・対策立案手法を情報セキュリティ事故に試験適用した結果について述べる．

2. 関連研究

情報セキュリティ分野のヒューマンエラー研究は，SPT（情報セキュリティ心理学とトラスト）における研究が代表的である．SPT は 2008 年に発足した研究グループであり，セキュリティに関する研究を心理学，人間工学，安全工学等の面から進めている．ヒューマンエラー対策に関しては，川越らが認知科学的アプローチに基づいた研究の提案を行っている．川越らは，情報セキュリティ分野においても，ヒューマンエラー対策のためには，エラーを誘発する要因(PSF: Performance Shaping Factor)を分析し，評価する，組織的エラー管理が不可欠であると指摘している[2]．本研究は，このようなヒューマンエラー管理に関わるものである．

また，電力，鉄道，航空，医療など，人間系の誤りが人命に直結するミッションクリティカルな分野では既にエラー要因分析，対策立案を行う組織的施策を導入しており，事故事例やヒヤリハット事例の収集，対策の教育などの組織的取り組みの他，エラー発生を未然に防ぐための作業環境改善に取り組んでいる[3][4][5][6].

3. 情報セキュリティのヒューマンエラー管理のコンセプト

前章で述べたとおり，人間系を含むシステムでは，ヒューマンエラーを減少させるための継続的なシステム改善活動が不可欠である．ヒューマンエラーの認識，分析，対策立案，対策導入，対策効果測定の組織的な仕組み（フレームワーク），及び仕組み

[†] 株式会社日立製作所　システム開発研究所
Hitachi, Ltd., Systems Development Laboratory

ⓒ2009 Information Processing Society of Japan

Vol.2009-SE-164 No.1
Vol.2009-EMB-13 No.1
Vol.2009-CSEC-45 No.1
2009/5/28

を実現するためのしかけは情報セキュリティにおいても共通と考えられる．

一方，ヒューマンエラーに起因する情報セキュリティ事故は，セキュリティ事故の中の一つである．そこで，本研究ではヒューマンエラー管理フレームワークを現存するセキュリティリスク管理の中に体系づけることを目標とする．

人間系を含むシステム総体として情報セキュリティシステムを運用する仕組みとして代表的なものに，ISO/IEC 27001 などの標準規格に基づいた ISMS(Information Security Management System)がある．ISMS とは，企業や組織が自身の情報セキュリティを確保・維持するために，ルール（セキュリティポリシー）に基づいたセキュリティレベルの設定やリスクアセスメントの実施などを継続的に運用する枠組みである．組織が管理すべき情報資産に対して，想定されるセキュリティ上のリスクをアセスメントし，許容できないリスクに対して技術的対策，非技術的対策と運用計画を策定，PDCA(Plan, Do, Check, Action)サイクルを回すことで情報セキュリティを維持する．非技術的対策は人的対策，物理的対策，管理的対策に大別される．このうち，人的対策がヒューマンエラー対策に相当する．一般に ISMS が想定する人的対策は，監視，教育などである．

本研究が提案するヒューマンエラー管理を新たに含む情報セキュリティ管理フレームワークの全体像を，図１に示す．本研究のヒューマンエラー管理フレームワークは，ISMS の非技術的対策のうち，人的対策を強化するものと位置づけることができる．また，ISMS の技術的対策には， CIA(Confidentiality : 機密性，Integrity : 完全性，

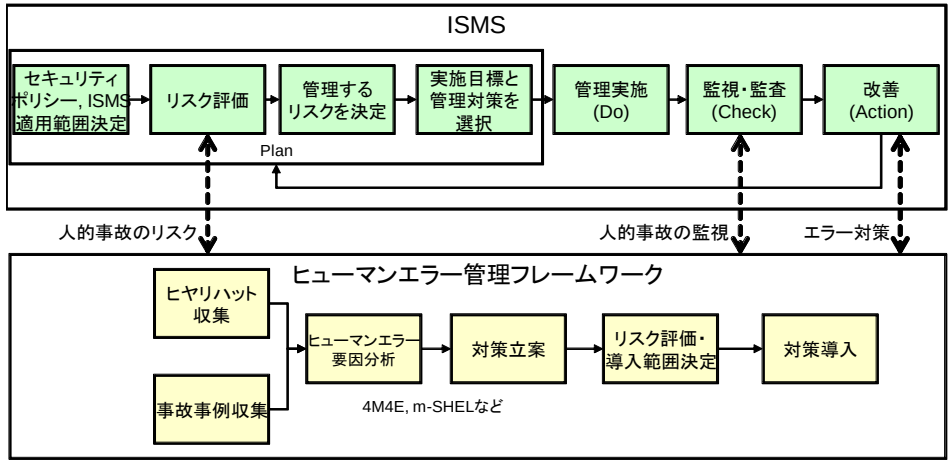

図１　フレームワークの概要

Availability : 可用性)を維持するための認証，アクセス制御などのセキュリティ技術が該当するが，ヒューマンエラー管理フレームワークはこれらのセキュリティ技術の実装において，ユーザが直接触れるツールや端末における，フールプルーフ，エラープルーフを強化するための設計要件を導出する道具立てと位置づけることができる．

ISMS などの情報セキュリティ管理の実効性を上げるため，ヒューマンエラー管理フレームワークが実現すべき目標を以下に述べる．

(1) リスクアセスメントの最適化

世界的に見ても特に日本国内大企業が ISMS を積極的に導入しているが， ISMS 導入組織でもヒューマンエラーに起因する情報漏えい事故が多発している．このことから，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という仮説が成り立つ．

基本的には情報セキュリティのリスクは次式の通り規定される．

リスク＝(予想被害額)×(発生頻度)＝(情報資産価値)×{(脆弱性)×(脅威)}…(式 1)

ヒューマンエラー管理フレームワークの目標の一つは，(式１)において脅威が不当に低いと見なされているエラーを正しく評価できるようにすることである．ヒューマンエラー管理フレームワークにより，人的な脅威＝ヒューマンエラーの発生メカニズムを正しく理解し，どのような場合に脅威が顕在化するのか，このようなケースがどれぐらい起こりえるのかを把握できるようにする．

(2) 非技術的対策の強化

想定されるリスクに対しては脆弱性，脅威に対してそれぞれ非技術的対策，技術的対策がありえ,通常はリスクの大きさや対策コストに応じて必要なものが選択される．

通常，ISMS では人間は組織の期待通りに正しい手順で情報を利用するという前提に基づいて，人的な脅威＝ヒューマンエラーを算定している．この前提を担保する仕組みは，教育，承認制度，監査による利用者への意識向上に頼っているものの，ヒューマンエラー管理が不十分なために，以下の図式が生じている．

(i) 人的脅威＝ヒューマンエラーの発生確率を低く見積もる
(ii) 事故の結果，再教育などの人的対策強化を関係者全員に実施するが効果があがらない
(iii) セキュリティリスクを抑えるため，脆弱性を低下させるための施策を導入する

ヒューマンエラーの発生要因を正しく理解していない限り，対策の効果は期待できず，事故は起こり続ける．ヒューマンエラー1 件 1 件への理解が深まれば，教育素材の洗練化，承認体制の見直しの基礎材料とすることができる．ヒューマンエラー管理フレームワークの狙いの一つは,(式 1)における脅威を合理的に抑える施策を実現することである．これにより，非技術的対策における脅威対策と脆弱性対策のバランス改

ⓒ2009 Information Processing Society of Japan

Vol.2009-SE-164 No.1
Vol.2009-EMB-13 No.1
Vol.2009-CSEC-45 No.1
2009/5/28

善も期待できる．ミッションクリティカル分野ではエラー発生時の作業環境，労働環境を含めてエラー発生要因を理解し，対策を立てることにより効果を上げている．現状,情報セキュリティ分野においては注意欠如にエラーの理由を求めることが多いが，これだけではヒューマンエラーを削減する上で効果が低いことは知られており，より合理的なアプローチを新たに導入する必要がある．特に情報記憶媒体の紛失を例に考えると，紙媒体など，非技術的な対策以外に有効な手段が存在しないケースがある．このような場合にはヒューマンエラー管理強化による対策強化が不可欠である．

(3) 技術的対策の強化

技術的な脅威対策が可能なヒューマンエラーの例としては，メール誤送信が挙げられる．現在のメール普及状況や利用形態を鑑みると，脆弱性対策（送信者や送信先を限定する）では誤送信が起こりえる全ケースの網羅は困難である．また，脅威対策（メールアドレスや本文キーワードによるフィルタリング）には判定精度に技術的限界があり，過剰な警告あるいは誤送信の見逃しの可能性を排除できない．

ヒューマンエラー管理により，エラー発生時の状況をより詳細に把握できるようになれば,例えばクライアントPCにおけるアプリ操作,ユーザの作業状態を監視して，エラー発生状況が生じたときに，メール送信前に警告する，あるいはエラーは起きていないが類似した状況が起きていたユーザにヒヤリハット事例として知らせるなど，新たな防止策への展開が期待できる．

4. 要因分析・対策立案手法の検討

ヒューマンエラー管理フレームワークを支える実現技術として要因分析・対策立案手法を検討する．これは，図１のヒューマンエラー要因分析と対策立案に対応するものである．要因分析手法により，情報セキュリティ事故が起きた後で，ヒューマンエラーを誘発した根本原因をつきとめる．対策立案手法では，根本要因に対する有効な対策を立案する．

本研究が提案するヒューマンエラー管理フレームワークでは，事故の当事者が対策決定までを行う．医療現場で働く人が，専門的な知識を必要とせずに分析や対策立案を行えるようにまとめられた分析・対策のためのフレームワークとしてH^2-SAFERがある[7][8]．そこでまず，情報セキュリティ分野と医療分野の相違を考慮に入れつつ，実績のあるフレームワークであるH^2-SAFERの手順に沿った分析・対策立案手法で分析，対策立案を行うこととする．

4.1 検討対象

情報の媒体や通信方法が多様化する中で，情報セキュリティ事故も，情報媒体の紛失・盗難，メールやFAXの誤送信，誤廃棄，不正アクセスやウィルス感染など多様化している．様々ある情報セキュリティ事故の中から，1)どの部署でも，誰もが利用する，2)電子媒体であるためシステム的な対策が容易である，3)一度に多人数に大量のデータをやり取りが可能であり大規模な漏えいとなる可能性がある,などの理由から，まず電子メールの誤送信を分析・対策立案の対象とした．

一般的に，結果として同じ事故（「PCの紛失」や「メールの誤送信」など）が起きた場合でも，その発生要因は事故により異なる．そして，それぞれのエラー発生要因に対して，立てうる（立てるべき）対策は様々考えられ，それらは発生要因ごとに異なってくる．そこで，要因分析対策立案を検討するにあたり，事前準備としてメール誤送信の要因を**表2**のとおり定義した．

表２　メール誤送信原因の分類

要因箇所	詳細要因	説明
宛先	誤選択・誤入力	本来送信すべき人と異なる人へ送信した
	不要 Cc	本来送信すべき人以外に送信する必要のない人へも送信した
	To, Cc / Bcc	Bcc で送信すべきメールを To または Cc で送信した
	設定・登録	メーラーの設定を誤った アドレスをアドレス帳やメーリングリストに登録する時点，またはそれ以前で誤りがあった
内容	誤選択・誤入力	送信すべき内容と異なる内容を送信した
	不要添付	本来送信する必要のない内容を送信した
システム	—	システムのバグにより誤送信が発生した

4.2 要因分析手法

本節では，情報セキュリティ事故に適した分析手法として，H^2-SAFERで推奨される時系列事象関連図[9]および時系列事象関連図に似た手法であるいきさつダイヤグラム[10]，VTA(Variation Tree Analysis)[11]についても比較検討を行う．各手法の概要は以下の通りである．本稿では，各手法の記法は省略する．詳細は各参考文献を参照されたし．

- 時系列事象関連図

  時系列事象関連図は，H^2-SAFERで推奨される分析手法である．時系列事象関連図は，事実をもとに事象を時系列に整理することで事実を正しく理解するために用いられ，横軸にシステム名称，関係者などをとり，縦軸を時間軸とし，事象を並べる[9]．時系列事象関連図の作成のポイントは，「なぜ？」を繰り返して情報不足や不明点を洗い出すこと，事実と推定を区別すること，客観的視点と主観的視点で見ることなどである．

ⓒ2009 Information Processing Society of Japan

Vol.2009-SE-164 No.1
Vol.2009-EMB-13 No.1
Vol.2009-CSEC-45 No.1
2009/5/28

- いきさつダイヤグラム
  いきさつダイヤグラムは不具合（トラブル，失敗）の経緯，発生したヒューマンエラー，およびエラー要因を視覚的に整理するための記述法であり，「作業ステップ」，「エラー・困った現象」，「エラー要因」の三つの欄から構成される[10]．いきさつダイヤグラムのねらいは，不具合に至った経緯をわかりやすく示すことであり，ヒューマンエラーの分析によって得られたすべての情報を盛り込むというよりは，要点を抜き出して整理することになる．
- VTA
  VTA は，事象の関連を時系列的に記述することで事故の細部を検討するものである[11]．バリエーションツリーは，正常な状態・判断・作業などから外れたものを変動要因として探り，時間軸に沿って記述することで，不具合に至った経緯を図式化し，図式化されたツリーの中から，不具合に至る流れを確実に断ち切ることのできる箇所を明らかにし，その上で具体的な対策を策定していくものである．バリエーションツリーは，事故や不具合の発生経緯を図式的に表す中央のツリー部と，ツリー部を詳しく説明する欄外から構成される．ツリー部には関係した企業，部署，個人をあらわす軸ごとに，変動要因を時間経過に従い整理して並べる．各事象は**正常な作業**，**逸脱した作業など**を示すシンボルを用いて記述する．

いくつかの事例を 3 つの手法を用いてトライアル分析し，手法の有効性を検討した結果を**表3**で示し，検討結果の詳細を以下で述べる．現段階では，情報をより多く盛り込めることを重視し，事象の整理，問題点の把握において他の手法より優れた VTA が最も適した分析手法であると考え，実際の分析には VTA を用いることとする．ただし，分析者間における分析結果の差異を少なくするために，記号の用い方を事前に一致させておくことに注意する．記号の使い方を一致させておくことで使いやすさも向上すると考えられる．

表３　分析手法の検討結果

	時系列 事象関連図	いきさつ ダイヤグラム	VTA
(1) 使いやすさ	○	○	×
(2) 事象の整理	○	○	◎
(3) 問題点の把握	×	○	◎
(4) 対策立案へつながりやすさ	×	×	○
(5) 分析者間の結果のばらつきの少なさ	◎	○	×
(6) 第三者からみたわかりやすさ	○	○	○

◎：要件を充足しかつ他手法より特に優れている，○：充足する，×：充足していない

(1)　使いやすさ
時系列事象関連図は事象を時系列に沿って記述していくものであり，いきさつダイヤグラムは要点を抜き出して記述するものであるため，要素がシンプルで，初めて使う人にも使いやすい手法であるといえる．一方 VTA は，事象に対して詳細な情報を記述するために記号を用いるため，初めて使う場合は多少使いにくい．
(2)　事象の整理
どの手法も事象を整理できている．その中でも，VTA は詳細な情報を記述するため，よりよく事象が整理できている．
(3)　問題点の把握
時系列事象関連図は事象の記述のみで，エラーの発生要因がわかりにくいため，問題点も把握しにくいといえる．いきさつダイヤグラムでは，エラー・困った要因について記述するため，問題点は把握できるものの，複数のエラーや要因がある場合，各エラーの重大性と「誰が」という視点がわかりにくい．VTA は，エラー要因やブレイクポイントなどにより重大なエラーはどこか記述するため，問題点も把握しやすいといえる．
(4)　対策立案へのつながりやすさ
対策立案へのつながりやすさは問題点が把握できているかに関わる．そのため，問題点が把握しにくい時系列事象関連図といきさつダイヤグラムは対策立案へつなげにくいといえる．
(5)　分析者間の結果のばらつきの少なさ
時系列事象関連図が特に充足している．分析者間の結果のばらつきは，事象の記述では少なく，エラー要因の記述に多く見られる．特に VTA は記号の用い方の意識が異なる場合，記述にばらつきが生じやすい．
(6)　第三者からみた判りやすさ
いずれの手法も第三者から見て判りやすいものである．

4.3　対策立案手法の検討

対策立案においては，抜けもれなく対策を立案することが望ましい．そのため，H^2-SAFERでは 4STEP/Mとm-SHELの組合せを用いた対策立案法が用いられる[7]．4STEP/Mとm-SHELの組合せ表を用いた対策立案法では，

- 要素が細かく分かれているため，対策が立案しやすい
- 網羅的に対策を立案できる

という利点がある．

4STEP/M は以下の 4 つのステップで対策立案を行っていく手法である．4STEP/M の考え方の詳細を**図2**に示す．

ⓒ2009 Information Processing Society of Japan

Vol.2009-SE-164 No.1
Vol.2009-EMB-13 No.1
Vol.2009-CSEC-45 No.1
2009/5/28

<table>
<tr><td>システム安全のプロセス</td><td colspan="9">1. エラー発生防止
Prevention</td><td colspan="3">2. エラー拡大防止
Mitigation</td></tr>
<tr><td>戦略的エラー対策の4M</td><td colspan="2">(STEP1)
エラーや危険を伴う作業遭遇数を減らす
Minimum encounter</td><td colspan="7">(STEP2)
各作業においてエラーをする確率を低減する
Minimum probability</td><td colspan="2">(STEP3)
多重のエラー検出策を設ける
Multiple detection</td><td>(STEP4)
エラーに備える
Minimum damage</td></tr>
<tr><td>ブレークダウン</td><td colspan="2">エラー発生可能のある作業や危険を伴う作業に遭遇しないようにする</td><td colspan="3">エラーを誘発しない環境にする</td><td colspan="4">エラーを誘発されないようにする</td><td>エラーに気づく</td><td>エラー発生を検出する仕組みにする</td><td>エラー発生に備える</td></tr>
<tr><td rowspan="2">ブレークダウン</td><td colspan="2" rowspan="2">排除</td><td rowspan="2">物理的制約</td><td colspan="2" rowspan="2">負担軽減</td><td colspan="4">正しい</td><td rowspan="2">自己検出</td><td rowspan="2">検出</td><td rowspan="2">影響緩和</td></tr>
<tr><td>知覚</td><td>認知(予測)</td><td>判断</td><td>実行</td></tr>
<tr><td>戦略的エラー対策の原理</td><td>(a)
作業の排除</td><td>(b)
危険の排除</td><td>(c)
物理的制約</td><td>(d)
認知的負担軽減</td><td>(e)
身体的負担軽減</td><td>(f)
基準感覚知覚能力の保持</td><td>(g)
エラー予測</td><td>(h)
安全優先の判断</td><td>(i)
タスク遂行能力の保持</td><td>(j)
エラー発見</td><td>(k)
検出</td><td>(l)
影響緩和</td></tr>
<tr><td>エラー対策の発想手順</td><td colspan="2">(1)
やめる
（なくす）</td><td>(2)
できないようにする</td><td>(3)
わかりやすくする</td><td>(4)
やりやすくする</td><td>(5)
知覚させる</td><td>(6)
予測させる</td><td>(7)
安全を優先させる</td><td>(8)
能力を持たせる</td><td>(9)
自分で気づかせる</td><td>(10)
検出する</td><td>(11)
備える</td></tr>
</table>

図２　4STEP/M

(1) エラーや危険を伴う作業の遭遇数を減らす(Minimum encounter)
(2) 各作業においてエラーをする確率を低減する(Minimum Probability)
(3) 多重のエラー検出策を設ける(Multiple detection)
(4) エラーに備える(Minimum damage)

m-SHEL はエラーの要因を m(management), S(Software), H(Hardware), E(Environment), L-L(Livewires)に分け，分析する手法である．つまり，風土・組織を変える(m)，手順書・手順・表示を変える(S)，設備を変える(H)，作業環境を変える(E)，人による支援体制を整える(L-L)，ということを念頭におき，対策立案を行っていく．

トライアル分析結果を用いて対策立案を行った．その結果，4STEP/M と m-SHEL の組合せ表を用いた対策立案手法は，基本的に情報セキュリティ事故対策においても有効であると判断した. 例えば,「メールの内容を確認しなかった」という問題に対して，特に対策立案手法を使わなくとも「内容を確認する」という対策を考えることができる．これに対し，4STEP/M と m-SHEL モデルの組合せを用いて対策立案した場合，1)操作者による事前確認，2)操作者による事後確認，3)周りの人による事前のダブルチェック，4)周りの人による事後のダブルチェックのように網羅的に立案できる．ただし，m-SHEL の各要素が情報セキュリティ分野にうまく対応していないことがわかった．そのため，m-SHEL を情報セキュリティ事故に適用するには分類要素の再整理が必要と考えられる．今後，様々な情報セキュリティ事故に対して検討を行い定めていく必要があるが，まずは E を省略し，表４のように区分することとする．

表４　m-SHEL の分類

	既存の分類	情報セキュリティに対応させた分類
m（マネジメント）	風土，組織を変える	風土，組織を変える（変更なし）
S（ソフトウェア）	手順書，手順，表示を変える	人間による操作を変える
H（ハードウェア）	設備を変える	システムを変える
E（環境）	作業環境を変える	―
L-L（周りの人）	人による支援体制を整える	人による支援体制を整える（変更なし）

5. 事故事例への適用実験

5.1 実験概要

過去の実事例に基づいて分析を行った．ただし，ここでは仮想事例を用いて述べる．実験では，VTA による分析，4STEP/M と m-SHEL モデルの組合せによる対策立案を行った．なお，仮想事例を用いた分析，対策立案は複数人でそれぞれ行い，その結果を相互に検証した．

以下の宛先の登録エラーによるメール誤送信の事例について，分析と対策立案を行った結果の一例をそれぞれ**図3**，**表5**に示す．対策立案後は表５の中からコストなどを評価し，実施する対策を決定する．

【事故内容】
8 月 1 日
A さんが, 社内の B さんのメールアドレスをアドレス帳に登録しようとした際，誤って顧客のメールアドレスを登録.
その後，アドレス帳のデータをもとにメールを作成，送信
8 月 8 日
A さんが見積書を添付したメールを作成，送信.
メール同報者が漏洩に気づき，A さんに通知.
8 月 9 日
A さんが情報漏洩を認識.

ⓒ2009 Information Processing Society of Japan

Vol.2009-SE-164 No.1
Vol.2009-EMB-13 No.1
Vol.2009-CSEC-45 No.1
2009/5/28

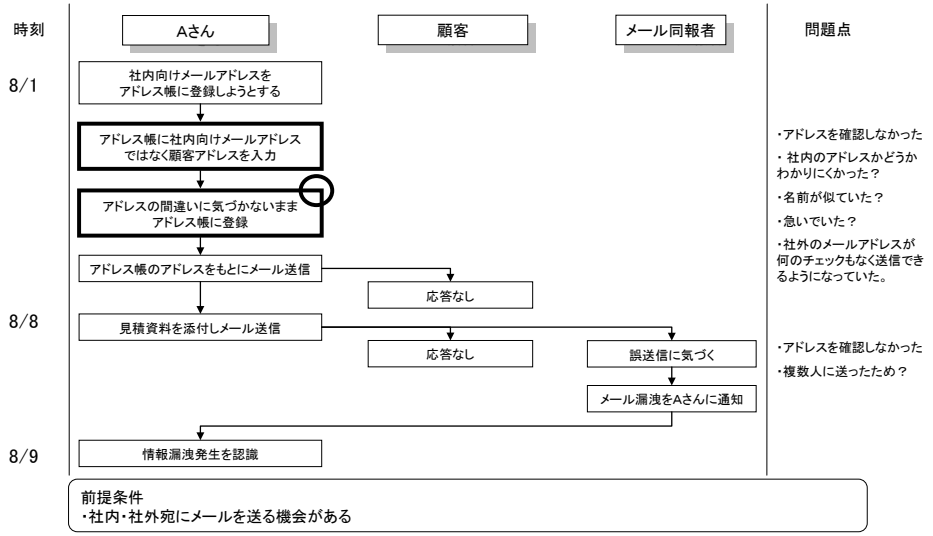

図３　VTA による要因分析例

表５　4STEP/M と m-SHEL モデルの組合せによる対策立案例

対策の対象	エラーを伴う作業を減らす	エラーをする確率を低減する							多重のエラー検出策を設ける		エラーに備える
エラー対策の発想手順 / m-SHEL	1 やめる	2 できないようにする	3 分かりやすくする	4 やりやすくする	5 知覚能力を持たせる	6 予測させる	7 安全を優先させる	8 遂行能力を持たせる	9 自分で気づかせる	10 検出する	11 備える
m(マネージメント) 風土、組織を変える	メール禁止		Ccで送る場合は送信者全員の名前記載		ストレスチェック	事故、ヒヤリハットの共有		教育		ダブルチェック	事故発生時の対応の事前確認 ヒヤリハット、事例の収集、共有
S(ソフトウェア) 人間による操作を変える	手作業による入力をやめる	自動補完ができないようにする	メールの作成の仕方を一貫させる						送信後の送信内容を確認	送信後の送信内容確認	アドレス帳他のアドレスの再確認
H(ハードウェア) システムを変える	メーラーを変える	社内/社外でアドレス帳を分け、社内分への社外のアドレス登録不可能にする	社内/社外で異なるアドレスの表示方法 ポップアップによる警告 プレビュー画面	送信先が複数人宛の場合、アドレスの前に番号を表示する	PCの連続作業時間からストレスチェック					社外アドレス時のポップアップ	暗号化 ログをとる
L-L(周りの人) 人による支援体制を整える				他の人によるチェック			他の人に任せる			ダブルチェック	事故、ヒヤリハット共有

5.2 考察

様々な事例を用いて VTA による分析, 4STEP/M と m-SHEL による対策立案を行い，情報セキュリティ事故に対する有効性，改善すべき点について以下のような知見が得られた．

(1)　手法の有効性

(1-1) VTA

- 各事象を時系列に整理できる
- エラーの発生元とエラー要因がわかりやすく，問題点が把握しやすい

(1-2) 4STEP/M と m-SHEL による対策立案法

- 網羅的に立案できる
- 対策の目的と対象が共有化できる

(2)　改善すべき点

(2-1) VTA により得られた分析結果から 4STEP/M と m-SHEL による対策立案を行う段階でギャップがある

VTA で事象の整理はできるものの，そこから問題点を洗い出していき，問題の背後要因を突き止める手順が不明確である．背後要因を分析する手順を強化することで，対策立案に効果が期待できる．

(2-2) 4STEP/M と m-SHEL による対策立案では，立案された各対策間での依存関係が不明である

4STEP/M と m-SHEL による対策立案では表を埋めていく方式であるため，対策の依存関係がわかりにくい．例えば，メールの誤送信の場合，メールそのものをやめたら他のメール誤送信対策は不要になる．対策の依存関係を把握しやすくすることで，その後のステップである対策の評価，決定が容易になると考えられる．

(2-3) 4STEP/M，m-SHEL の分類区分がわかりにくい

対策対象の分類が細かいと，網羅的に対策立案しやすくなる．しかしその一方で，初めて手法を用いる人は項目ごとの違いを判別しにくい．そこで，メール誤送信以外でも実験を行い，情報セキュリティ事故対策に適切な分類区分を検討するとともに，各セルに対応する対策例などの指針を示すことで，対策立案が容易に行えるようになると考えられる．

これらの利点，改善すべき点はメール誤送信事故固有の問題ではなく，一般的に分析・対策立案を行ううえで共通の性質であると思われる．そのため，VTA および 4STEP/M と m-SHEL による対策立案手法を改良していくことは，メールの誤送信だけでなく，今後の情報セキュリティ分野全般に重要であるといえる．

ⓒ2009 Information Processing Society of Japan

Vol.2009-SE-164 No.1
Vol.2009-EMB-13 No.1
Vol.2009-CSEC-45 No.1
2009/5/28

また，様々な要因のメール誤送信の事例で 4STEP/M と m-SHEL による対策立案を行った結果，事例ごとに固有の対策のほかに，メールの誤送信という事例全てに用いることのできる対策も存在した．医療など他の分野では要因分析・対策立案の結果をデータベース化することで，作業の支援を行っている[12]．そのため，情報セキュリティ分野でも再利用性・共有性を向上することで，質の高い要因分析・対策立案が可能になるとともに，作業の手間を減らすことが可能になると考えられる．

6. まとめ

本稿では，ヒューマンエラーに起因する情報セキュリティ事故発生のリスクを最小化することを目的とし，情報セキュリティ情報セキュリティ分野向けのヒューマンエラー管理フレームワークを提案した．また，ヒューマンエラー管理フレームワークを支える実現技術の一つとして，情報セキュリティ向けのヒューマンエラー分析手法，対策立案手法の検討結果について述べた．

今後は，本研究をふまえ，情報セキュリティ向けに要因分析手法，対策立案手法を確立する予定である．また，医療や航空分野等と情報セキュリティ分野の共通点ならびに相違点の明確化，要因分析の網羅性向上に向けた検討を考えている．

謝辞　ご協力頂いた皆様に，謹んで感謝の意を表する．

参考文献

1) 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：「2007 年情報セキュリティインシデントに関する調査報告書」，Ver. 1.2，(2008 年 6 月)
2) 川越秀人 他：「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 Vol.2008, No.45, pp13-18
3) 日吉和彦：「航空機の整備方式とヒューマンファクターへの取り組み」，技術と経済 2008.6 ，pp.16-22，（2008 年 6 月）
4) 楠神健：「安全研究所における最近のヒューマンファクター研究」，JR East Technical Review, No.21, pp.11-14
5) 鈴木史比古 他：「JR 東日本版 4M4E 分析手法の開発と導入・展開」，JR East Technical Review, No.21, pp.31-34
6) 厚生労働省医療安全対策検討会議：「医療安全管理者の業務指針および養成のための研修プログラム作成指針」，（2007 年 3 月）
7) 行待武生 監修，「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
8) 株式会社テプシス,「ヒューマンエラーの分析ガイド～事例検討思考手順H^2-SAFERの考え方とポイント～」，2001
9) 河野龍太郎，医療事故分析の意義とその手法，医療安全，5(1)，8-25，2008
10) 独立行政法人宇宙航空研究開発機構，「ヒューマンファクタ分析ハンドブック補足版 (CRR-01015A)」，p.23(2002)
11) Leplat, J. and Rasmussen, J. “Analysis of human errors in industrial incidents and accidents for improvement of work safety”, New Technology and Human Error， Rasmussen, J., et al., (Eds.), (John Wiley & Sons), pp.157-168(1987)
12) 印出井明子 他 「医療事故防止対策システムの開発」，第 22 回医療情報学連合大会 医療情報学, 22 (Suppl.), pp. 94-95, 2002

ⓒ2009 Information Processing Society of Japan