Vol.2014-EIP-63 No.13
2014/2/21

運用におけるヒューマンファクターに注目した情報セキュリティ対策について

佐々木崇裕[†1]　　原田要之助[†2]

情報セキュリティ事故の一つである情報漏えい事故は，高い割合で「ヒューマンファクター（人的要因）」により引き起こされていることがわかる．そこで，ヒューマンファクターが関与して発生した事故原因の種類を人間の行動を基に分類を示し，m-SHEL モデルや割れ窓理論などといったヒューマンファクターの分析モデルを紹介する．また，ヒューマンファクターが介在して発生する事故に対する対策は示されているが，対処療法的で数が多いという問題点を示し，研究の方向性を探る．

The provision against an information security which observed the human factor in employment

TAKAHIRO SASAKI[†1]　　YONOSUKE HARADA[†2]

Human factor is one of main reasons of information leakage. The previous studies have provided a couple of analytical frameworks of human factor, based on classification of root causes of incidents incurred by human behavior. This paper introduces some analytical frameworks of human factor such as m-SHEL model and Broken Windows Theory. And also, issues are identified, related to present measures to avoid from incidents incurred by human factor, e.g. difficulty in selecting the right measure from too many option or case by case approach. Then, direction of further study is proposed.

1. はじめに

NPO 日本ネットワークセキュリティ協会及び情報セキュリティ大学院大学が公開した，「2011 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」 [1]に図 1 の情報漏えいの事故の傾向が示されている．

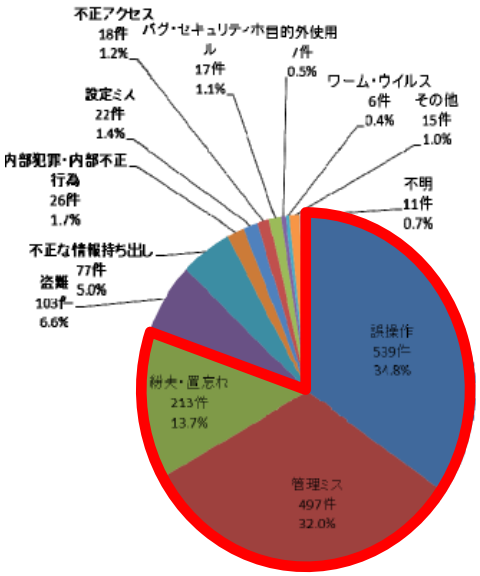

図 1　漏えい原因比率（件数） [1]に加筆

それによると，『2011 年は「誤操作」，「管理ミス」，「紛失・置き忘れ」で約 80%を占めた.』とあり，「誤操作」，「管理ミス」，「紛失・置き忘れ」は，人が介在して発生した事故であり，また同報告書によれば『「誤操作」および「紛失・置き忘れ」はヒューマンエラーである.』としている．
つまり，情報漏えい事故は多くの場合ヒューマンエラーや規則違反といったヒューマンファクターが多く絡んでいることがわかる．

また，図 2 の漏えい原因比率の経年変化（件数）を見ると，「誤操作」，「管理ミス」，「紛失・置き忘れ」といった人が介在して発生した事故の割合は，データのある 2005 年以降，高い割合を占めていることがわかる．

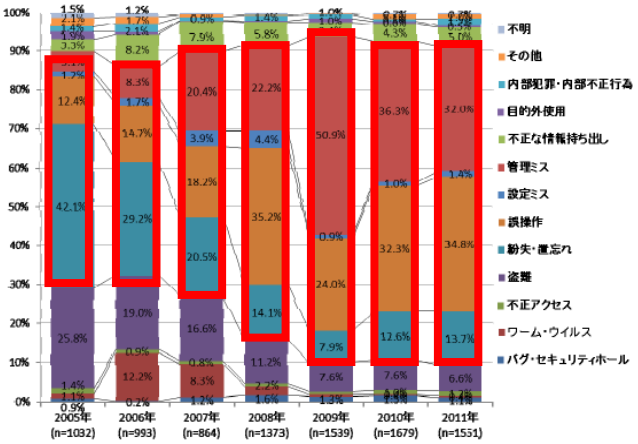

図 2　漏えい原因比率の経年変化（件数） [1]に加筆

†1 情報セキュリティ大学院大学
Institute of Information Security
†2 情報セキュリティ大学院大学
Institute of Information Security

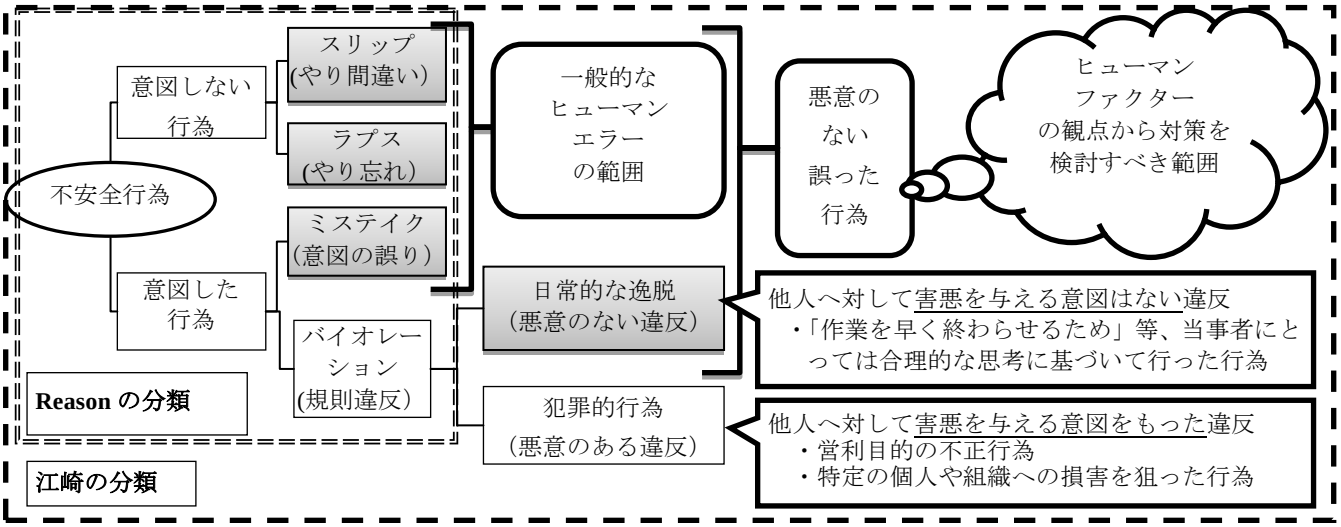

図 3　ヒューマンエラーの分類 [4] [5]を図式化

2. ヒューマンファクター

ヒューマンファクターやヒューマンエラーの研究及びそれに基づく対策は，航空や原子力の分野で導入・発展し，医療の現場にも導入されるようになった．このような業種の特徴は，些細な事故が人命に害なすような重大な事故に発展するケースがあるということである．

情報セキュリティの分野においてのヒューマンファクターの研究については，川越 [2]の研究が参考となる．

2.1 ヒューマンファクターの定義

ヒューマンファクターとは，どのようなことを指すのかを見てみる．ヒューマンファクターという言葉は，直訳すると人的要因となり，その内容は多岐にわたり不明確である．佐相 [3]は，総じていえば以下の３つの使い方があるといっている．

『 ①システムに影響を与えた人間の行動
人間の操作ミス（ヒューマンエラー）や規則違反など
②人間の振る舞いに影響を与える諸要因の総称
インターフェース，マニュアル，環境．人間自身のもつ特性・性質を含む
③人間の行動を適正化するための学問体系
人間工学，心理学等の人間の行動を最適化するために活用する学問』

運用における情報セキュリティは上記３つのどれに当てはまるかを「2011 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」 [1]の基礎データで確認したところ，情報漏えい事故のほとんどが①の「システムに影響を与える人間の行動」に当てはまった．このことから運用における情報セキュリティにおいては，①の「システムに影響を与える人間の行動」が重要であると考えられ，本稿においてはそれに焦点をあてることとする．

2.2 ヒューマンエラーの定義

ヒューマンエラーの定義もいくつかある[a][b]．代表的なものとしては，デイペンダビリティ（信頼性）用語の規格である JIS Z8115:2000 の,『意図しない結果を生じる人間の行為.』，心理学分野では，Reason [4]の『計画された知的または物理的な活動で，意図した結果が得られなかったときで,これらの失敗がほかの出来事によるものでないときの,すべての場合を包含する本質的な項目として，エラーを考える.』という定義がある．

なお，川越[2]は『少なくともヒューマンエラーが，特別で異常な行動を意味しているわけではなく，人間の正常な行動の一つであることと，ヒューマン・マシン・システムにおける事故分析又は事故防止の観点で用いられる概念であることは間違いない.』とも書いている．

本稿では，ヒューマンエラーの発生に至る過程に注目することから JIS ではなく，川越の用いた Reason をベースとして用いることとする．

2.3 ヒューマンファクターの分類

ヒューマンファクターは，Reason [4]及び江崎ら [5]の指摘をもとに，図式化した．それを図 3 に示す．

まず，Reason の分類である．Reason はヒューマンファクターを不安全行為と表現し，不安全行為は意図したかしないかで分類されるとしている．ここで「意図しない行為」とは，「正しい意図」を持ちながらも，実際には「意図とことなる行為」をしてしまったことをさす．さらに，意図しない行為は，「スリップ（やり違い)」と「ラプス（やり忘れ)」に分類される．

意図しない行為の具体例はとして，スリップは「電子メールを送信する際に，CC と BCC を間違える」，ラプスは「PC の置き忘れ（による紛失)」があげられる．

a) 日本公定書教会　編:医療事故の防止に向けて―医薬品・医療用具からのアプローチ―,エルゼビア・サイエンス株式会社　ミクス,P.15,(2002).
b) Linda T. Kohn, Janet M. Corrigan, and Molla S. Donaldson: To Err Is Human-Building a Safer Health System, NATIONAL ACADEMY PRESS, P.54,(2000).

一方,「意図した行為」は，正しいつもりで意図したが結果的には誤りであったという「ミステイク（意図の誤り）」，正しくないと認識しながらも，あえて行為に及ぶ「バイオレーション（規則違反）」に分類される．さらに，江崎ら [5] によると規則違反は,『人間が所属する組織に対する悪意の有無によって日常的な逸脱と犯罪的行為の 2 つに分類できる.』としている．『バイオレーションのうち日常的な違反は，厳密には正しくないという認識を伴いつつも，「作業を早く終わらせるため」など当事者にとっては合理的な思考に基づくものである.』と論じている．また，『犯罪的行為以外のヒューマンエラーは，ヒューマンファクターの観点から対策を検討すべき対象となる.』としている．

意図した行為の具体例として，ミステイクは「（持出し禁止ルールがない環境においての）情報の持出し」，悪意のない違反は「（持出し禁止ルールがある環境においての）個人作業の効率化のための情報の持出し」，悪意のある違反は「自身が売却益を得るための，情報の持出し」があげられる．

以上の考察から現時点においては, 2.1 で定義した通り，図 3 に示される分類全てをヒューマンファクターの対象に含めることとする．

2.4 ハインリッヒの法則

ヒューマンエラーや規則違反行為によって事故が起きた場合，それを端緒に，事故が起きるまでのストーリーに気付くことは可能である．しかし，事故が起きなくとも事故につながりそうなミスや事象にヒヤリとしたり，ハッとしたりして気づくこともある．いわゆるヒヤリ・ハットといわれるものである．

ヒヤリ･ハットの関連として,ハインリッヒの法則（図 4，別名：1:29:300 の法則）[c][d]が知られている．これは，アメリカの安全技師であったハインリッヒが，労働災害 5000 件以上を統計学的に調べた結果見いだしたものである．内容は，「1 件の重傷を伴う事故の背景には同じ要因で 29 件の軽傷事故が発生しており，さらにけがはないものの同じ要因で発生した 300 件もの事象がある.」というものである．

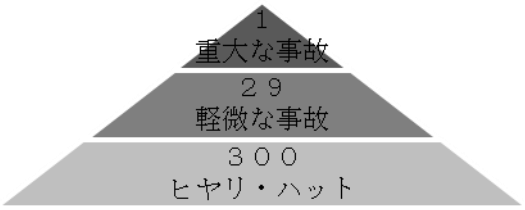

図 4　ハインリッヒの法則

この法則は労働災害における事故だけではなく様々な分野で流用され，ビジネス分野においては，クレーム対策といった面で活用されている[e]．しかし，公表されている情報漏えい事故は，重大または軽微な事故のみであり，ヒヤリ・ハットが公表された例はほとんどない．

3. ヒューマンファクターの分析モデル

2 章においては，図 3 でヒューマンファクターの分類を示した. また, 図 4 でハインリッヒの法則として知られる，重大な事故の背景には同じ要因による多くのヒヤリ・ハットが存在することを示した．本章では，実際の事故やヒヤリ・ハットで得たストーリーの分析モデル等について，ヒューマンエラーと規則違反 2 つに分けて述べる．

3.1 ヒューマンエラーの分析モデル

3.1.1 4M 分析と 4M-4E 分析

4M とは，Man，Machine，Media，Management という 4 つを意味しており，これを図 5 に示す [6]．図 5 はこれら 4 つの視点で事故や不具合の要因の抽出を図る．図 5 の 4 つの視点の具体的な内容を以下に示す．

Man : 作業に何らかの形でかかわる人すべてを指す．作業者にかかわる身体的・心理的要因，資質，技量，知識も含む．

Machine：装置や機器などの物的なものを指す．

Media：取扱説明書や手順書等の媒体・環境に関係するもので，機器の使い方を含む作業の方法・手順，チーム内のコミュニケーション，職場の状況などを含む．

Management : 組織や管理規定等の管理に関係するもので，安全法規類などの規則，作業計画，教育訓練などを指す．

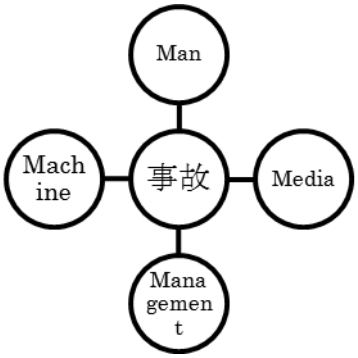

図 5　4M モデル [6]

次に 4M-4E 分析法であるが，4E とは 4M に対応する対策のことで，Education，Engineering，Enforcement，Example をいう. これに Environment を加えて 5E ということもある．これら 5 つの視点で対策を検討するが，各視点の具体的内容は次の通りである [6].

c) 石丸秀治: 情報セキュリティニュース 2010 年度 No.6 情報管理におけるヒューマンエラー対策．ｲﾝﾀｰﾘｽｸ総研, (2011). 2013 年 9 月 25 日閲覧, http://www.irric.co.jp /risk_info/bcm/pdf/joho-security_201101.pdf

d) 医療経営人材育成事業ワーキンググループ: 経済産業省サービス産業人材育成事業 医療経営人材育成テキスト［Ver. 1.0］⑬リスク管理 おわりに, KPMG ヘルスケアジャパン, (2006).2013 年 10 月 23 日閲覧, http://www.meti.go.jp/report /downloadfiles/g60828a14j.pdf

e) 黒坂昭一: 滞納整理における処理促進のための一考察－リスク管理及び滞納事案の類型別アプローチ手法を中心に－,”税大論叢 53 号,(2007).

Education：知識・意識教育，技量向上訓練など
Engineering：設備機器の改善，作業工程の改善，基準の見直しなど
Enforcement：作業手順の明確化，指導など
Example：参考となる事例及び実施対策の例示
Environment：作業環境の改善

4M-4E(4M-5E)分析を具体的に利用する場合は，表 1 の 4M5E 表を準備し，各マトリックスを埋めることを行う．この方法のメリットとしては，表を利用して分析するので，要因抽出に偏りがあることが見つけやすく，また対策に関しても，複数の対策案を示すことができる．そのため解析者の先入観などをある程度は排除できるというものがある．デメリットとしては，トラブル事例の分析を目的とした手法である為，ヒューマンエラー自体が，要因の中に入ってしまい，ヒューマンエラーの要因分析が行われないままに分析が終わってしまう恐れがある [6].

表 1　4M5E 表 [6]

	Man 人	Machine 機械	Media 環境	Management 管理
内容 （要因）				
Education （教育・訓練）				
Engineering （技術）				
Enforcement （強化・徹底）				
Example （模範・事例）				
Environment （作業環境）				

3.1.2 SHEL モデル

SHEL とは，Software，Hardware，Environment，Liveware（Liveware は作業者と他者に分けられる．）という５つの要素を，事故や不具合の原因を評価する手法であり，各要素の具体的内容は以下のとおりである [7].

Software：手順書，マニュアルなど
Hardware：機械など　４M における Machine と同義
Environment：作業環境
Liveware-1：作業者の個人特性
Liveware-2：人間関係，コミュニケーションなど，チーム的な要素

SHEL のそれぞれの要素は，その周辺部分が波のように凹凸で示されているが，この波は Liveware においては，人間の特性や限界を示している．この Liveware の凹凸とそれを取り巻く Hardware の凹凸が合致していなければ不具合が生じていることを示している．すなわち対策としては Liveware 側 Hardware 側双方から凸凹を埋めるようなアプローチが必要になる [7].

さらに，河野 [8]はこれに management の m を加えて，図 6 で示される m-SHELL モデルを提案している．ここでいう，management とは管理要素のことであり，具体的には，組織の管理体制の構築や，安全に関わる企業風土作りなど指す．

なお，説明の関係で SHEL モデルを，ヒューマンエラーの分析モデルに分類しているが，規則違反の分析にも適用できると考えられる．

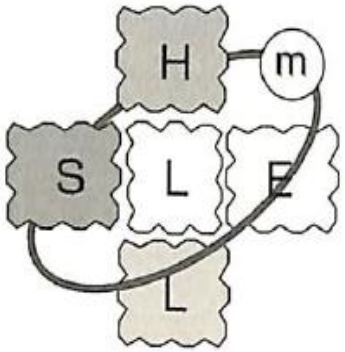

図 6　m-SHELL [8]

3.1.3 m-SHEL モデルを用いた先行研究

新原 [9]が m-SHEL モデルを応用した情報セキュリティインシデントに関するヒューマンエラー対策の実施手順を提案している．ここでは，実証実験を行い，インシデント発生が抑制することを確認した．

新原は，河野の m-SHEL モデルの定義を情報セキュリティに即した内容に修正した．さらに，河野 [8]が提案した「エラー対策の思考手順」を情報セキュリティに応用するため，情報セキュリティ対策の思考手順を図 7 のように修正した．

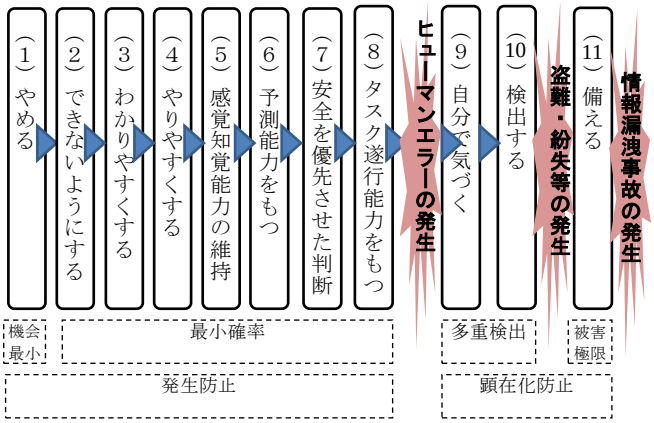

図 7　情報セキュリティ対策の思考手順 [9]

河野は「エラー対策の思考手順」と m-SHEL モデルを組み合わせた「エラー対策の発想手順マトリックス」を考案している [8]．新原も，河野の手順に合わせて，「情報セキュリティ対策の思考手順」と m-SHEL モデルを組み合わせ，表 2 に示す「情報セキュリティ対策の発想手順マトリクス」を提案した [9]．このマトリクスの良い点は，空欄すべてについて対策の有無を検証することにより，考えうる対策の網羅性が検証される．

表 2　情報セキュリティ対策の発想手順マトリクス [9]

		情報セキュリティ対策の思考手順										
		①やめる（なくす）	②できないようにする	③わかりやすくする	④やりやすくする	⑤知覚能力を持たせる	⑥認知・予測させる	⑦安全を優先させる	⑧できる能力を持たせる	⑨自分で気づかせる	⑩検出する	⑪備える
m-SHELモデル	m（マネジメント）											
	S（ソフトウェア）											
	H（ハードウェア）											
	E（環境）											
	L（本人）											
	L（周りの人）											

3.2 規則違反に関連する理論

ここでは，規則違反の観点から応用できる理論について述べる．

3.2.1 割れ窓理論

割れ窓理論(Broken Windows Theory）とは，J. Q. Wilson と G. L. Kelling [10]が考案した．この理論では，ビルのたった 1 枚の割れた窓を放置しておくだけで，誰も割れた窓に関心を持っておらず，他の窓ガラスを壊して構わないというサインになり，他のすべての窓が割られてしまうという理論である．これは，軽犯罪を取り締まることで，犯罪全般を抑止できるという応用をすることができる．ニューヨークの市長であったジュリアーニがこの理論を応用して治安が良くなったとのことから，多くの場所で応用されている [11]．

なお，ニューヨークの治安の回復した理由を，割れ窓理論の応用によるものではなく，もともと全米全体で回復し始めていた環境にあったこと，ジュリアーニの前の市長が警察官の数を増やしたことによるものという，理論とは無関係とする主張もある [12]．

3.2.2 割れ窓理論に関する先行研究

規則違反に関しては，山本 [13]による『日本の組織における組織文化・風土と情報セキュリティ逸脱行為の関係』についての研究がある．研究の中で機密情報に触れると考えられる職種に就く正社員を対象にアンケート調査を行い，分析の結果「割れ窓理論」から「情報セキュリティ逸脱行為」への相関が認められなかったが，「上司による逸脱許容傾向」は「情報セキュリティ逸脱行為」を助長することを見いだしている．

3.2.3 ルーティンアクティビティ理論

マルカス・フェルソンが唱えた理論で，図 8 で犯罪が発生するには，「ふさわしいターゲット」，「動機づけられた犯罪者」，「有能な監視者の不在」の 3 つの要素が必要とあるとしている．

本理論は，情報セキュリティにおける内部犯行について調べた社会安全研究財団の報告書 [14]や独立行政法人情報処理推進機構のレポート [15]において取り上げられ，内部犯行に対する対策が提言されている．

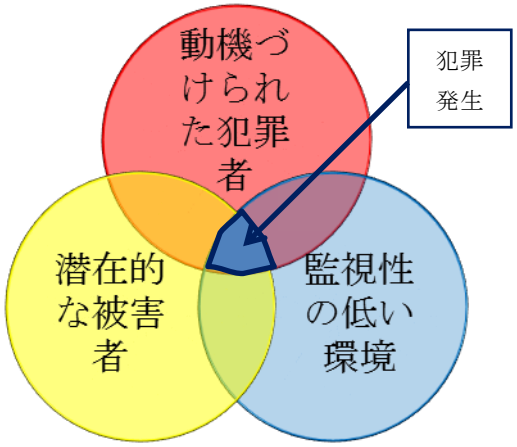

図 8　犯罪発生に必要な条件 [14]

4. ヒューマンファクター対策の現状

4.1 ヒューマンエラーの対策の現状

ヒューマンエラーに対する対策についてであるが，2007 年にシステム監査学会情報セキュリティ研究プロジェクトが，ヒューマンエラーの事例とその影響をタイプ別に分類して，具体的かつ詳細に記述したうえで，具体的な対策例も示したものを公表している．具体的には，『「ルールを徹底する」，「複数人でチェックする」，「監査を実施する」』[16]といったものである．

この対策を確認すると，対処療法的なものが多い．対処療法的対策があるがゆえに，対策が多くなり，適用にあたっては膨大なリストを毎回チェックしなければならず，何らかの体系化，整理が必要と考える．

4.2 規律違反の対策の現状

3.2.3 に述べているとおり，規律違反に対する対策についても，提言されており具体的には，『システムの開発・運用は複数の者で担当する.』,『チェックシステムを導入しておく.』,『職場全体のコミュニケーションをよくしておく.』[14]などが挙げられている.

ヒューマンエラーの対策と同様にこちらも対策数が多いという問題点が残されている.

5. 今後の研究の方向性

現在のヒューマンファクターに関した情報セキュリティ対策は対処療法的な対策がほとんどであることが分かった.今後は，4 章に述べた対処療法的な対策ではなく，各個人が簡潔なモデルを用いて自発的に情報セキュリティ対策取るといった，応用性の高い情報セキュリティ対策をヒューマンファクターに注目して検討･提唱したいと考えている.

謝辞 本研究にご協力いただいた原田研究室の先輩，同僚の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, 情報セキュリティ大学院大学 原田研究室 廣松研究室: 2011 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).
2) 川越秀人: 情報セキュリティのヒューマンファクタ, 2007 年度情報セキュリティ大学院大学特定課題研究報告書.
3) 佐相邦英: 原子力教科書ヒューマンファクター概論, 株式会社オーム社, (2009).
4) James Reason: ヒューマンエラー ―認知科学的アプローチ―, 海文堂出版, (1994).
5) 江崎郁子, 大橋毅夫 , 上野信吾: 個人情報漏洩防止のためのヒューマンエラー対策, 三菱総合研究所, (2005).
6) 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, 慶応義塾大学出版会, (2005).
7) 篠原一光 , 中村隆宏: 心理学から考えるヒューマンファクターズ―安全で快適な新時代へ, 有斐閣, (2013).
8) 河野龍太郎: 医療におけるヒューマンエラー―なぜ間違えるどう防ぐ, 医学書院, (2004).
9) 新原功一 , 原田要之助: 情報セキュリティインシデントに対するヒューマンエラー対策の提案, FIT2013（第 12 回情報科学フォーラム）, (2013).
10) George L. Kelling, Jame Q.Wilson: Broken Windows-The police and neighborhood safety, (1982). 2013 年 10 月 13 日閲覧, http://www.theatlantic.com/magazine/print/1982/03/broken-windows/304465/.
11) マイケル・レヴィン: 「壊れ窓理論」の経営学 犯罪学が解き明かすビジネスの黄金律, (2006).
12) スティーヴン・D・レヴィット , スティーヴン・J・ダブナー: ヤバい経済学, 東洋経済新報社, (2006).
13) 山本哲寛: 日本組織における組織文化・風土と情報セキュリティ逸脱行為の関係に関する一考察, 2010 年度情報セキュリティ大学院大学修士論文.
14) 社会安全研究財団 情報セキュリティにおける人的脅威対策に関する調査研究会: 情報セキュリティにおける人的脅威対策に関する調査研究報告書, (2010). 2013 年 5 月 2 日閲覧 http://www.syaanken.or.jp/wp-content/uploads/2012/05/cyber2203_01.pdf
15) 情報処理機構 技術本部 セキュリティセンター: 『組織の内部不正防止への取り組み』に関するレポート, (2012).2013 年 5 月 2 日閲覧 http://www.ipa.go.jp/about/technicalwatch/pdf/120315report.pdf
16) システム監査学会 情報セキュリティ研究プロジェクト: ヒューマンエラーの事例と影響, (2007).2013 年 9 月 28 日閲覧 http://www.sysaudit.gr.jp/seika/humanerror.pdf