IT システムにおけるヒューマンエラーに関する傾向と考察

安藤 玲未† 島 成佳†

†NEC クラウドシステム研究所
211-8666 神奈川県川崎市中原区下沼部 1753
r-ando@ap.jp.nec.com，shima@ap.jp.nec.com

あらまし ITシステム上の脅威が今まで以上に高度化・多様化していることから，情報セキュリティ対策が重要になっている．情報セキュリティ対策を検討する際は，システム，制度，人の3要素について検討する必要があるが，近年，人のミスによるセキュリティインシデントが増加傾向にあることから，筆者らはヒューマンエラーを低減する研究に取り組んでいる．ヒューマンエラーを低減するために，本研究ではセキュリティ心理学の観点からヒューマンエラーの発生メカニズムを明らかにするアプローチを考えている．本稿では，ヒューマンエラーの発生メカニズムを明らかにするために必要となる的確なヒューマンエラー情報を収集し，整理を行ったので報告する．

A consideration of Trends in Human Error for IT System

Remi Ando† Shigeyoshi Shima†

†Cloud System Laboratories, NEC Corporation
1753, Shimonumabe, Nakahara-Ku, Kawasaki, Kanagawa, 211-8666, JAPAN
r-ando@ap.jp.nec.com，shima@ap.jp.nec.com

Abstract Information security has become important because threats on IT systems are sophisticated and diverse.When considering information security measures, there is a need to consider three factors ITsystem, system, human.We focus on human error because human error contines to be a major computer security issue.In order to reduce human error, we consider the approach reveals the occurrence mechanism of human error from the point of view of security psychology in this study.In this paper,we report to collect and organize human error information.

1 はじめに

医療システムや航空管制等の重要インフラサービスにおけるITシステムへの依存度が高くなっている．これらのITシステムやITシステムを繋ぐネットワークにトラブルが発生すると，社会活動に深刻な影響を及ぼす．例えば，ファーストサーバの例のように，プログラムのバグによりデータが消去される障害が原因で業務に支障をきたす事例もある[1]．また，標的型攻撃に代表されるサイバー攻撃に伴う脅威は増大しており[2]，重要な情報を盗むだけでなく，Stuxnetのように制御系システムを攻撃した例もある[3]．近年ではこのようにITシステム上の脅威が今まで以上に高度化・多様化していることから，情報セキュリティ対策が重要になっている．

情報セキュリティ対策を立てる際には，図1に示す，(a)システム，(b)制度，(c)人の3要素を検

討する必要があると筆者らは考える. (a)システムとは, アクセス制御や暗号化等の IT システム自体に施される対策である. (b)制度は, ISMS(Information Security Management System)[4]や ITIL(Information Technology Infrastructure Library)[5], IT システムの運用に必要なマニュアルや手順書などをさす. (c)人は, 教育や訓練に挙げられるような人のミスなどを抑制するための仕組みをさす.

これまでの情報セキュリティ対策はシステムを対象とした研究(図 1 の(a))が中心に行われてきた. 一方で, 人を対象とした研究(図 1 の(c))は急務である. その理由は, ヒューマンエラーが原因でセキュリティインシデントに発展するインシデント件数が年々増加している点である[6]. また, 図 2 は 2013 年に発生したセキュリティインシデントを原因別に, その発生割合を示したグラフだが[7], ヒューマンエラーによるセキュリティインシデント(図 2 中の枠内)が上位を占めていることが分かる. Verizon では, ヒューマンエラーに対しての対策の 1 つとして, 情報漏えい対策(DLP:Data Loss Prevention)[8]の導入を挙げている[9]. このようにヒューマンエラーへの対策のうち, 人にミスを警告する(気づかせる)対策(図 1 の(X))が特に必要になると筆者らは考える. 例えば標的型攻撃メールは, 知人の名前を名乗り, 内容もごく日常的なものであるため, 安易に添付ファイルや URL をクリックしてしまう脅威がある. このような人のミスを誘発させることで被害を拡大させようとする攻撃に対しては, セキュリティ心理学を考慮に入れた対策を検討する必要がある.

そこで本研究では, ヒューマンエラーの発生メカニズムをセキュリティ心理学の観点から明らかにし, ヒューマンエラーを低減するシステムを作ることを目指す. そのために, まず的確な情報を収集し, 整理することが, 効果的な対策を講じるために必要であると考えた. 今回は, 情報の収集およびその情報の整理を行ったので報告する.

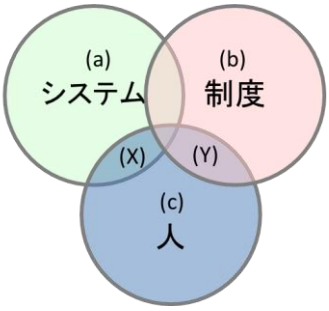

図 1 情報セキュリティ対策の3要素

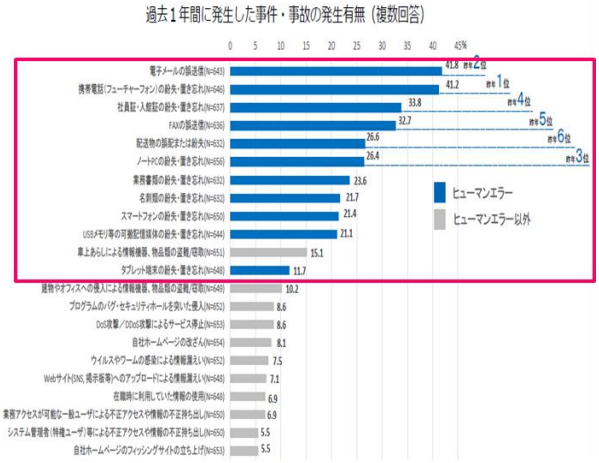

図 2 セキュリティインシデント(2013 年)

2 課題

システムを対象としたセキュリティ対策と, 本研究がターゲットとする人を対象としたセキュリティ対策の比較を行う. 更に, 本研究の課題について述べる.

システムを対象としたセキュリティ対策は, 図 3 のようにシステム間で入出力があった際に, システムの処理に誤りがないかを検出する手法が検討されてきた. これは主にセキュア開発や脆弱性診断ツールなどの手法が確立されている. 一方, 本研究が対象とする人を対象としたセキュリティ対策は, 図 4 に示す, 人がシステムを扱う環境における検討である. この環境では, 仮に脆弱性のないシステムを使っていたとしても, そのシステムを使う人が何らかのミスをするとセキュリティインシデントにつながる可能性がある. ここで課題となるのが, 人の思考・行動に基づいたミスの研究が IT 分野においてまだ確立されていない点である.

文献[10]では, 人間工学に基づいた他分野

(医療)での人のミスの研究について調査した．これらはヒューマンエラーの分析手法や分析結果に対する対策の立て方に関する研究であり，制度を対象とした人の研究(図 1 の(Y))にあたる．IT システム運用の現場においても，制度を対象とした人の対策が取られていることがヒアリングから明らかになった．具体的な対策としては，ヒューマンエラーを分析した後に手順書やマニュアルに対策を追加する，というようなものである．このような対策は再発防止対策が主であり，未然防止の観点から対策を検討することは難しい．人のミスを低減するためには，未然防止対策，再発防止対策を共に検討する必要があるため，本研究では既存研究とは別のアプローチから検討する．

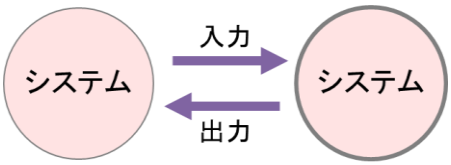

図 3 システムを対象としたセキュリティ対策

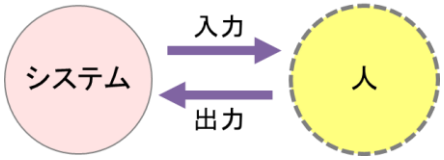

図 4 人を対象としたセキュリティ対策

3 アプローチ

本研究はヒューマンエラーの発生メカニズムの分析を行うことを目的としている．分析を行う際にはヒューマンエラーの実データが必要になる．しかし，内部不正に関わる事故と同様に[11]インシデントは組織内部で処理されてしまう傾向にあり，組織の外部に知られることは稀である．このことから，まずは現場へのヒアリングを行った．その結果，現場ではヒューマンエラーの分析，対策は行われているがエラーの分類はうまく行われていないことが明らかになった．ヒューマンエラーの内容は多彩であり，それぞれ対策を考える上での検討課題が異なる．ヒューマンエラーの発生要因を何らかの観点で整理する必要があると考え，まずヒューマンエラーを分類する．その後，分類結果に沿ってヒューマンエラーの検討・分析，防止対策の立案を図る．

本章では，本稿で行うヒューマンエラーの分類について述べる．

3.1 ヒューマンエラーの分類方法

ヒューマンエラーの分類には様々な分類方法があるが，認知心理学の視点から，代表的な以下の 3 つを挙げる[12]．

a) 行動観察からの分類

人の行動の種類によって分類する方法である．代表的な行動観察に基づく分類に Swain による分類がある．

・オミッションエラー：するべきことを省いた行為，やり忘れエラー

・コミッションエラー：するべきことと違うことを行うこと，やり間違いエラー

オミッションエラーとコミッションエラーは，事象としての重なりがないため，誰もが正確に分類することができる．しかし，結果としての行動のみによる分類のため，この分類だけでは，そのエラーに至った経緯を知ることができない．

b) 人間の情報処理過程からの分類

人間の情報処理過程の観点による分類の 1 つに，Reason による分類がある．

・スリップ：意図・意思は正しかったが，行為の段階で誤ってしまったヒューマンエラー．

・ミステイク：判断(意図)自体が間違っていたことによるエラー．情報把握の間違い，状況認識の間違い，行動選択の間違いなどがこれにあたる．

・ラプス：記憶の失念によって生じるエラー

c) SRK モデルに沿った分類

人の認知過程を表すモデルには J.Rasmussen が提唱した SRK モデルがある．SRK モデルは，人間の認知行動を次の 3 つのカテゴリに分けて捉えるものである．

・スキルベース：行動パターンとして意識しないで実行される行動．

・ルールベース：教育や訓練などを通じて培ったルール（例えば作業手順）に基づいて

実行される行動.

・ナレッジベース:過去に経験がない，あるいはほとんど経験がないといった不慣れな状況などにおける，試行錯誤や状況の理解，効果の予測などを実行する行動.

今回ヒアリングを行った運用の現場では，人への教育が行われていること，また，人のスキルに頼る運用フレームワークにはなっていないことからSRKモデルは使用しない.

本研究では，ヒューマンエラーの発生に至る過程を明らかにできる「b)人間の情報処理過程からの分類の観点」で分類を行う.

3.2 人の情報処理過程

図5は人の情報処理過程を示している. 人はシステムから入力があると，認知，意図，行動のプロセスを経てシステムへ何らかの出力を行う. 認知とは，目や耳より入力される物理的な刺激を情報としてまとめる段階である. 意図とは，意思決定の段階であり，これまでの知識や経験をもとに，認知した情報から行動の内容を決める段階である. 行動とは，認知・意図における情報処理が終了した後，その決定された意思に従って実際に行動に移す段階である.

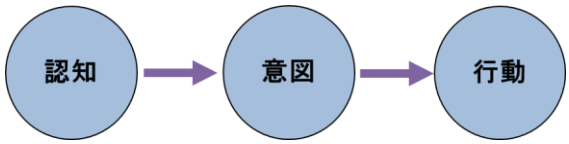

図5 人の情報処理過程

人は認知，意図，行動のプロセスにおいて，それぞれ認識ミス(ラプス)，判断ミス(ミステイク)，操作ミス(スリップ)を起こす可能性がある. どのフェーズのヒューマンエラーから詳細に調べていくかを決めるために，次章にてインシデントの分類実験を行う.

4 ヒューマンエラーの分類実験

4.1 データの収集

本実験の主旨に賛同頂いた A 社より，過去に発生したITシステム運用中のインシデントデータを頂いた. このうち，ヒューマンエラーに関する 51 種類を選び，これを今回の実験対象のデータとした. データの詳細に関しては守秘義務の関係で本稿には記載しない.

4.2 データの分類

4.2.1 実験概要

分類手法は，IT システム運用者の経験を考慮し，運用者の視点で分類が行えるオープン・カードソート[13][14]を選択した.

本実験は，2014年6月27日～2014年7月14日を実施期間とし，ITシステムの運用者 10 名から回答を得た. 一人あたり約 1 時間の作業時間であった. 以下，カードソート実験及び実験結果の分析について述べる.

4.2.2 カードソートとは

カードソートは情報アーキテクチャリサーチのツールで[13]，EC サイトの設計時などに用いられる手法である. カードソートの種類には，オープン・カードソート，クローズド・カードソート，デルファイ・カードソートがあり，今回はオープン・カードソートを用いる.

オープン・カードソートは，コンテンツ名のついたカードを自由に分類し，分類ごとにカテゴリ名を自由に名づける方法である. そのため，被験者の知見に基づいて分類を行うことができる. 今回は，インシデント内容が書かれた51枚のカードを被験者に渡し，被験者が納得できるようなグループに分けてもらう.

4.2.3 手順

カードソート実験の実施要領と，実験のイメー

ジ図を以下に示す.

実施要領:

IT システム運用中のインシデントについて、以下の要領でカードを並べ替えてください.

1. 「似ている」と思うインシデントをまとめて, グループ分けを行ってください.
2. どのような基準で「似ている」と判断するかに正解はありません. また, その基準を正確に決めなくても構いませんので, あなたが直感的に「似ている」と思うものをグループとしてまとめてください.
3. 1 つのグループに含めるカードの数には, 特に制限はありません. 他のどれとも似ていないと思ったら, 1 つのカードを 1 つのグループとして扱っても結構です. また, 1 つのカードが 2 つのグループにまたがって所属していても構いません.
4. グループ数についても特に制限はありません.
5. 並べ終わりましたら, グループに名前をつけてください.

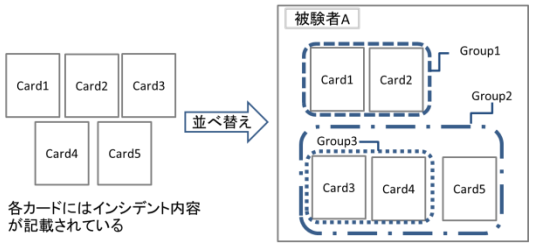

図 6 カードソート実験のイメージ

4.3 実験結果の分析

カードソートの結果を分析する際はクラスタ分析が用いられる. 分析のイメージを図 7, 図 8 に示す.

まず, 全てのカードの組み合わせに対し, 被験者がどのカードを同じグループに分類したか(類似度)を算出した(図 7). 図 7 の縦, 横の 1～5 の番号はカード番号を示している.

次に, 最も発生件数の多いインシデントから対策を検討するため, 階層クラスタ分析を行った(図 8). デンドログラムを作成する際, クラスタ間の距離測定方法には最短距離法を用いている. また, 今回の分析には R を使用した.

	1	2	3	4	5
1		0.1	0.2	0.3	0.4
2			0.1	0.2	0.3
3				0.1	0.2
4					0.1
5					

図 7 類似度の算出

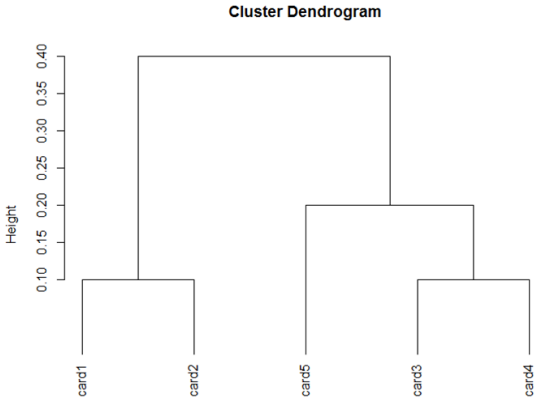

図 8 デンドログラムの作成

4.4 分析結果

4.3 に記載した方法により, 10 人のカードソート結果を分析したところ, 大きく 4 つのクラスタに分けることができた. それぞれを認知, 意図, 行動に分類すると以下のようになる.

・認知:思い込みによるミス(7 件),
　　コミュニケーション不足によるミス(3 件)
・意図:テスト不足によるミス(7 件)
・行動:オペレーション中のミス(17 件)
・上記のどれにも分類されなかったミス(17 件)

このうち, 行動に分類されたオペレーション中のミスによるインシデント件数が最も多かったため, 今後は該当するインシデントの要因を洗い出し, 分析を行う.

4.5 考察

今回, 人の情報処理過程(認知, 意図, 行動)いずれにも分類できないヒューマンエラーがあ

った. これらは意図(テスト不足)及び行動(オペレーションミス)の間で判断に迷い, 類似度が低くなった結果だと考えられる. また, これらの分類結果に関して被験者からは納得感があるとのフィードバックを得た.

5 おわりに

本稿では, 実際の IT システム運用の現場から得たインシデントデータを人の情報処理過程の観点で分類した. 分類手法はカードソートを用い, 現場の運用者の知見に基づいて分類を行った. 分類結果に対しクラスタ分析を行ったところ, IT システム運用中のオペレーションミスが最も多かったことから今後はインシデントの要因を詳細に調べ, ヒューマンエラーの発生メカニズムを明らかにしていく.

参考文献

[1] http://www.nikkei.com/article/DGXNASFK2600L_W2A620C1000000/

[2] 独立行政法人 情報処理推進機構 セキュリティセンター:情報セキュリティ 10 大脅威～複雑化する情報セキュリティ あなたが直面しているのは？～(2014)

[3]http://itpro.nikkeibp.co.jp/article/COLUMN/20111005/370190/

[4] 日本規格協会 : ISO/IEC27001(JIS Q 27001) 情報セキュリティマネジメント(2014).

[5] http://www.itsmf-japan.org/aboutus/itil.html

[6] JNSA: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～個人情報漏えい編～(2011)

[7] NRI セキュア:企業における情報セキュリティ実態調査 2013 第 2 版(2013)

[8]http://itpro.nikkeibp.co.jp/article/Keyword/20081028/317943/

[9] Verizon:2014 年度 データ漏洩/侵害調査報告書(2014)

[10] 安藤玲未: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, 第 8 回 SPT 研究会(2014)

[11] 独立行政法人 情報処理推進機構 組織における内部不正防止ガイドライン(2013)

[12] 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－, 慶應義塾大学出版会(2005)

[13] L. Rosenfeld. and P. Morville.: Information Architecture for the World Wide Web (Second Edition). Oreilly & Associates Inc (2002)

[14] D. Maurer.:Card Sorting. Rosenfeld Media,http://www.rosenfeldmedia.com/books/cardsorting/ (2007)