電話受付業務における情報セキュリティ事故防止のための自己診断システムの開発

松井　裕子

原子力安全システム研究所
919-1205　福井県三方郡美浜町佐田 64
matsui@inss.co.jp

あらまし 電話受付業務では、ヒューマンエラーに起因する情報セキュリティ事故の防止が課題となっている。本研究では、業務担当者が自己啓発に利用することを意図した情報セキュリティ事故リスク診断システムを開発し、実際の業務担当者に試行と評価を求めたので、その過程および結果を報告する。システム開発に当たっては、過去に発生した情報セキュリティ事故のタイプを分類し、事故報告書から推測された事故の要因と性格特性に関する項目からなる質問紙調査を実施し、その結果から、情報セキュリティ事故の起こしやすさの判別式を得て、診断システムに実装した。

Development of self-assessment system for prevention of information security accidents in call center operation

Yuko Matsui

Institute of Nuclear Safety System, Inc.
Sada 64 Mihama, Mikata, Fukui 919-1205, JAPAN
matsui@inss.co.jp

Abstract It is important for call center operators to prevent information security accidents caused by human errors. In order that the operators know about their risk of information security accidents, the self-assessment system was developed and tested on the operators. The system was implemented several prediction expressions to discriminate for risk of eight types of information security accidents, which were derived from questionnaire including factors of the actual previous accidents and personality traits.

1　はじめに

個人情報漏えいの原因はヒューマンエラーがほとんどであるとされ[1]、社内ルールの厳格化、ハードウエアのエラープルーフ化や教育・啓発などの対策が採られている。一方、ヒューマンエラーの起こしやすさには個人差があることが指摘されており[2]、性格特性や認知特性との関係が検討されてきた[2][3][4]。多くは日常生活におけるヒューマンエラーを対象としているが、中央労働

災害防止協会（中災防）は、業務上のトラブル経験もまた性格特性のいくつかとの間に関連がある可能性を示している[5]。またヒューマンエラーの発生率は業務特性や業務環境によって異なることも明白である。

電話受付業務においてもヒューマンエラーによる情報漏えいの発生の防止が課題となっている。事前のトレーニングやマニュアルの整備等により、その発生率は相当に低く抑えられているが、顧客とオペレータが直接に対話するという業務特性のために、ハードウエアや教育、業務環境等の改善による対策には限界があり、最終的にはオペレータ自身の努力に依存せざるを得ないところがある。そこで本研究では、オペレータ個人が、自らの置かれている業務環境や性格特性にひそむ情報セキュリティ事故の要因を把握するための自己診断ツールを開発することとした。開発は、①過去の事故報告書からの事故要因の抽出、②抽出された事故要因と性格検査等からなる質問紙調査の実施と調査結果からの情報セキュリティ事故の発生予測のための予測式の抽出、③予測式を実装した自己診断システムの試行・評価の過程を経て行われた。本発表では、このうち②③について報告する。

2　質問紙調査

電話受付業務における情報セキュリティ事故について、情報セキュリティ事故を起こす可能性の有無を判別するための関係式を得るために、質問紙調査を行った。

2.1　方法

1.　調査対象

電話受付業務の担当者101名

2.　調査方法

調査票の配布・回収は、調査対象企業の担当者が行った。回答は無記名とし、回答者自身が調査票を封筒に入れて封をして回収するように依頼した

3.　質問紙の作成

主な項目は以下の通りであった。

1)性格特性に関する質問（q1：48項目）。業務上のトラブル経験との関連が示されている安全行動調査（中災防、1991）の性格項目を利用した。「あてはまる」から「あてはまらない」の4段階評定を求めた。

2)業務に関する質問（q2：33項目）。過去3年の情報セキュリティ事故報告書から事故要因と推測される事柄を抜き出し、件数の多い要因について実際の業務内容に即して文章化した。性格特性と同様に4段階評定とした。

3)情報セキュリティ事故経験に関する質問（q3：9項目）。同様に事故報告書に基づき、発生件数の多い事故種別（番号の誤特定、処理忘れ、誤登録、コミュニケーションの失敗、誤入力、住所の誤特定、口頭漏えい、紛失、その他）について、「経験あり」「しそうになったことがある」「経験なし」の選択肢で経験の有無を尋ねた。

2.2　結果：判別式の抽出

回収率は100%であった。回答者は女性86名、男性11名、無回答4名であった。図1に、各情報セキュリティ事故の経験の有無の回答分布を示す。

ここでは、各情報セキュリティ事故の起こしやすさを判別することが目的であるので、関係式の目的変数となるセキュリティ事故経験を問う項目（q3）の回答について、「2. しそうになった」と「3. した」を統合し 2 値データに変換した。また、説明変数となる性格特性や業務に関する項目（q1,2）についても、「1.あてはまらない」と「2.どちらかといえばあてはまらない」、および、「3.どちらかといえばあてはまる」と「4.あてはまる」を統合し2値データに変換した。

q3の各問とq1, 2の全項目との間でクラメールの連関係数(独立係数)を算出し、q1,2の中から、q3との連関係数の高い14項目を説明変数の候補として選択した。目的変数(q3)ごとに数量化Ⅱ類を実施し、カテゴリスコアと相関比、判別的中率を算出した。得られた関係式が、判別的中率75%以上かつ相関比0.250以上を満たせば採用とした。

結果として、9個の目的変数のうち、q3-1～q3-8の8個について、有効な関係式が得られた。それぞれの判別的中率と相関比を表1に示す。

以下、紙幅の都合で、q3-3についてのみ数量化Ⅱ類の結果を示す。「q3-3　お客さま番号などを間違えて登録しそうになった(した)ことがありますか」については、7個の説明変数で構成される関係式が得られた。関係式の各項の係数となるカテゴリスコアを図2に示す。カテゴリスコアが正のカテゴリ(選択肢)は、当該の情報セキュリティ事故を起こさなかった人の特徴であり、事故を起こすリスクを低減する方向で寄与していることを示す。逆に、カテゴリスコアが負のカテゴリは、当該の情報セキュリティ事故を起こした(または、起こしそうになった)人の特徴であり、事故を起こすリスクを高める方向で寄与していることを意味する。

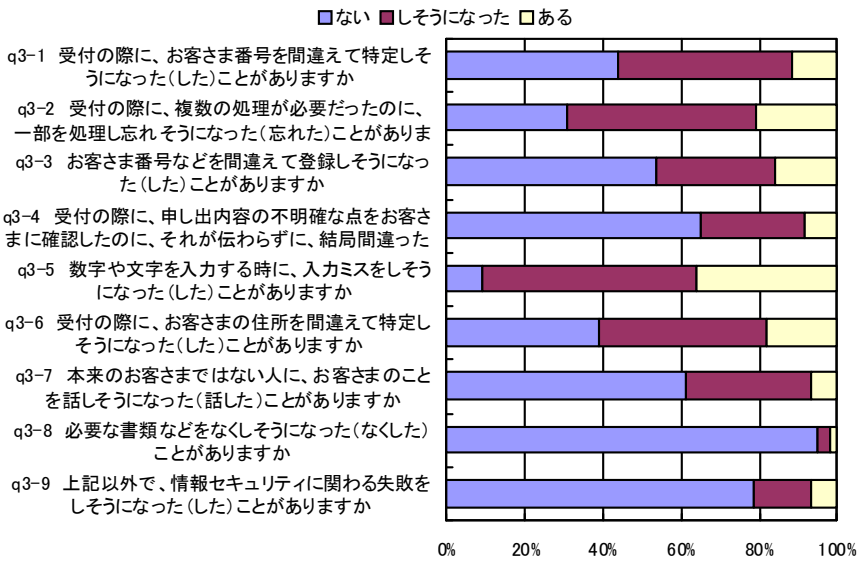

図1　情報セキュリティ事故の経験の有無

表 1　各情報セキュリティ事故に関する関係式の判別的中率と相関比

	目的変数	判別的中率	相関比	説明変数の数
q3-1	受付の際に、お客さま番号を間違えて特定しそうになった(した)ことがありますか	79.4%	0.38	9
q3-2	受付の際に、複数の処理が必要だったのに、一部を処理し忘れそうになった(忘れた)ことがありますか	78.4%	0.26	10
q3-3	お客さま番号などを間違えて登録しそうになった(した)ことがありますか	78.9%	0.43	7
q3-4	受付の際に、申し出内容の不明確な点をお客さまに確認したのに、それが伝わらずに、結局間違った処理になりそうになった(なった)ことがありますか	78.8%	0.33	11
q3-5	数字や文字を入力する時に、入力ミスをしそうになった(した)ことがありますか	91.5%	0.27	8
q3-6	受付の際に、お客さまの住所を間違えて特定しそうになった(した)ことがありますか	83.0%	0.33	9
q3-7	本来のお客さまではない人に、お客さまのことを話しそうになった(話した)ことがありますか	82.5%	0.29	10
q3-8	必要な書類などをなくしそうになった(なくした)ことがありますか	88.5%	0.27	9
q3-9	上記以外で、情報セキュリティに関わる失敗をしそうになった(した)ことがありますか	71.7%	0.20	6

3　試行による評価

前項の分析において得られたカテゴリスコアに基づく関係式が実装された「情報セキュリティ事故リスク自己診断システム」に対するユーザーによる試行、評価を行った。

3.1　情報セキュリティ事故リスク自己診断システム

このシステムでは、前述のカテゴリスコアを用いた関係式に含まれる質問文(41 項目)が回答画面(図 3)に提示された。回答者は、画面に表示された質問文に対してプルダウンメニューに示された選択肢からあてはまるものを選択することによって回答した。全ての問に回答した後に「判別ボタン」を押すと、各事故のサンプルスコアが、レンジが0～5となるように変換され、レーダーチャートで表示される(図 4)。基準値を3として、基準値より大きければ当該事故を起こしやすく(リスクが高く)、小さければ起こしにくい(リスクが低い)と判定された。回答は記録されず、何度でも回答および判定をし直すことができた。

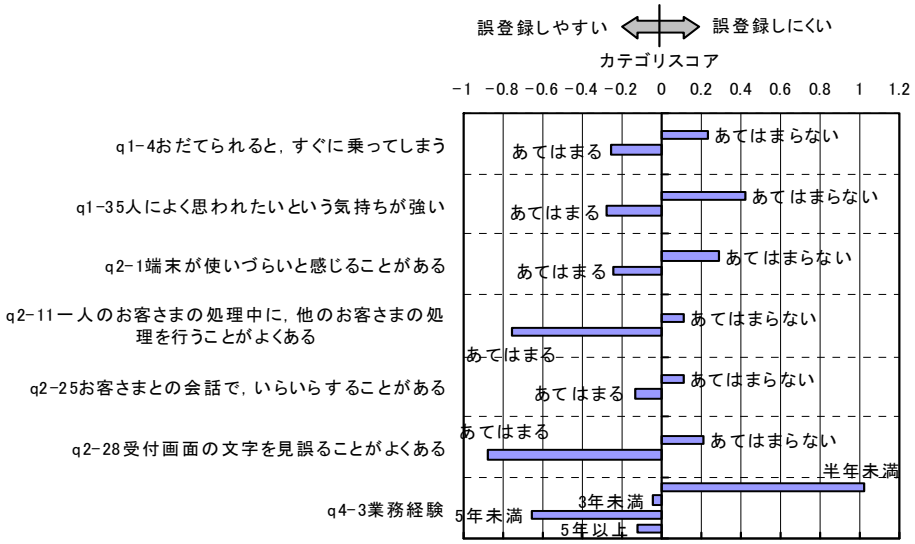

図 2 「誤登録」の要因のカテゴリスコア

本システムについて、実際の電話受付業務担当者に試行を求め、①回答のしやすさや出力された結果に対する納得感、システムの有用性などについて使用者の実感を把握し、改善点の抽出を行う。

3.2　方法

1.　対象者

電話受付業務の担当者100名

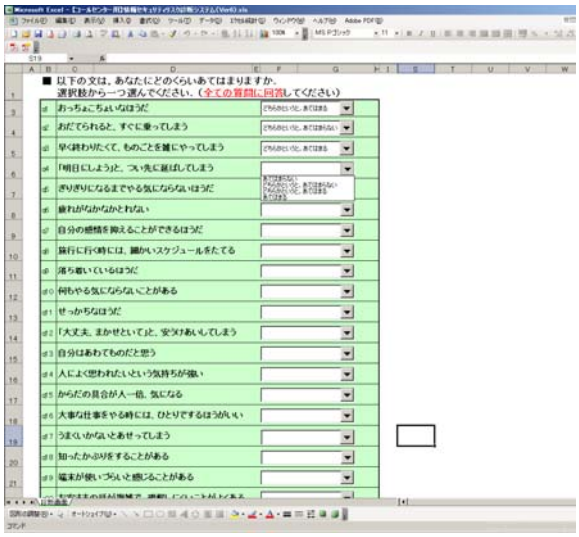

図 3　自己診断システムの回答画面

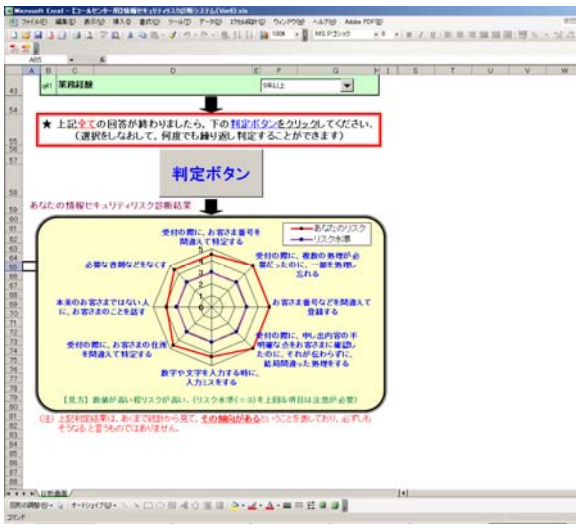

図 4　自己診断システムの結果出力画面

2. 評価方法

会議室にシステムが搭載されたノートパソコンを設置しておき、調査対象者が各自で空き時間にシステムを試用することとした。調査対象者は、自分自身の判定結果を見た後で、使用感に関する質問紙に回答した。質問紙は無記名で、開封できない回収ボックスに調査対象者自身が投入するようにして、匿名性を確保した。

質問紙は、①質問文のわかりやすさ、②質問項目数、③結果のわかりやすさ、④結果に対する納得感、⑤システムの有用性の5問で構成され、それぞれ5段階評価であった。①③については、否定的な意見の理由を自由記述する欄が設けられた。あわせて、⑥システムが本格運用となる場合に要望すること、⑦その他意見を自由記述で尋ねた。

3.3 結果

各質問項目に対する回答を集計した(表 2)。

1. 質問文のわかりやすさ

質問項目「情報セキュリティリスク診断システム」の各質問の聞き方(質問文の分かりやすさ)についてお答え下さい」に対して、「大変わかりやすい」と「ややわかりやすい」を合わせ、62%が質問文をわかりやすいと評価した。わかりにくいと評価した10%の回答者から得られた11件の自由記述を内容の類似したものをグループ化して整理したところ、以下の5つに大別された;選択肢が選びにくい(4件)、具体的な状況が想像しにくい・業務内容に合わない(3件)、当然のことを聞かれている(2件)、個人的な質問の必要性がわからない(1件)、その他(1件)。

2. 質問項目数の適切さ

質問項目「情報セキュリティリスク診断システム」の質問数についてお答え下さい」については、現状の41項目に対して、63%が「現状でよい」と回答した。

3. 結果のわかりやすさ

質問項目「「情報セキュリティリスク診断システム」のグラフ(結果)についてお答え下さい」に対して、「大変わかりやすい」「ややわかりやすい」をあわせて55%がわかりやすいと回答したが、「どちらともいえない」が38%であった。わかりにくい点に関する自由記述6件を内容の類似性で分類したところ、以下の4つに大別された;①結局何に注意すればよいかわからない(2件)、②質問と結果の関係性がわからない(2件)、③よしあしが判断できない(1件)、④

表2 「情報セキュリティリスク診断システム」の評価結果

(1)質問文のわかりやすさ	大変わかりやすい	ややわかりやすい	どちらともいえない	少しわかりにくい	とてもわかりにくい	計
度数	25	37	27	9	1	99
(2)質問項目数の適切さ	多い	やや多い	現状でよい	やや少ない	少ない	
度数	6	27	63	3	1	100
(3)結果のわかりやすさ	大変わかりやすい	ややわかりやすい	どちらともいえない	少しわかりにくい	とてもわかりにくい	
度数	24	31	38	6	1	100
(4)結果に対する感想	自分にもそのようなリスクがあると改めて認識した	自分にはなんとなくそのようなリスクがありそうに思う	どちらともいえない	自分にはあまりそのようなリスクはないように思う	自分にはそのようなリスクは絶対にないと思う	
度数	40	29	20	11	0	100
(5)有用さの評価	大変役に立つ	やや役に立つ	どちらともいえない	あまり役に立たない	まったく役に立たない	
度数	21	34	32	12	1	100

ネガティブな表現でよくない（1件）。

4. 結果に対する感想

質問項目「「情報セキュリティリスク診断システム」の診断結果（グラフ）を見てどう感じましたか」に対して、自分の持つリスクを再認識したり、なんとなく当該のリスクがありそうな感じがするなど、出力された結果にある程度の納得感を感じたと回答したのは69%であった。

5. 有用さ

質問項目「情報セキュリティリスク診断システム」は，情報セキュリティ意識を高める上で役に立つと思いますか」に対しては、「大変役に立つ」「やや役に立つ」をあわせた55%が役に立つと回答したが、「どちらともいえない」も32%あった。

6. 本格実施に向けての要望

質問項目「今後、「情報セキュリティリスク診断システム」の本格実施に向けて、ご要望があれば以下にお書きください」に対して、33名からのべ36件の記述が得られた。

内容を分類した結果、システムに対して肯定的な記述内容が2件、条件付き肯定的なものが3件、提案および具体的な批判が28件、具体的でない批判が2件であった。提案および具体的な批判については、質問内容があいまいなどの質問内容に関する記述が8件、選択肢が質問文と合わないなど質問文に関する記述が2件、改善点を具体的に示してほしいなど結果の出力に関する記述が12件、入力しにくいなど実施方法に関する記述が6件であった。

3.4 改善すべき点

質問紙への回答から、出力結果そのものに対しては、69%が一定の納得を示していると言える。有用さについては、55%が「役に立つ」と感じているが、同時に32%が「どちらともいえない」と回答しており、有用さの評価は決して高いとは言えない。自由記述で得られた回答から、特に以下の点を改善することによって評価の向上が期待できる。

①実施目的についての事前説明の充実：診断システムが評価や査定のためではなく、あくまでも個人の内省および注意喚起のためのものであることを十分に説明しておく必要がある。また、システムが業務情報を含めた多数の質問項目から統計的に関連が認められた項目で構成されていることを説明することにより、システムや出力結果に対する納得感が高まることが期待される。

②出力内容の充実：情報セキュリティ事故のタイプとそのリスクだけでは、回答者が考えるための情報が少ない。具体的にどの質問項目がリスクの高さに結びついたのかを提示することにより、具体的な改善項目を把握しやすくなると考えられる。可能なものについては、改善方法を提示できれば最善である。

③納得のいかない結果の受け止め方の提示：回答者によっては、自分の思っていた結果と乖離していると感じられる場合があったようである。そのような場合に、結果をより前向きに受け止められるよう、表現を工夫したり、とらえ方を提示したりすることが必要である。例えば、一定のリスクがありながら現在まで事故を起こしていないことを、日頃の努力の結果としてとらえることができれば、情報セキュリティ事故に対する感度を保ち続けることにつながるかもしれない。

4 おわりに

実際の情報セキュリティ事故の事例に基づき、電話受付業務で発生しやすい情報セキュリティ事故のタイプを示した。それらの事故報告書から読み取れた事故の要因（業務特性と行動特性）および業務担当者の性格特性と情報セキュリティ事故の起こしやすさとの関係を明らかにするため、質問紙調査を実施し、その結果から各事故タイプとその要因との関係式を抽出した。さらに、関係式を利用して作成された「情報セキュリティ事故リスク

自己診断システム」の試行および評価を実施し、改善点を見出した。今後は、改善点として指摘された、実施目的の事前説明の充実、出力内容の充実、納得のいかない結果の受け止め方の提示について改善していく予定である。

参考文献

[1] 情報サービス産業協会(2011). 平成 22 年度「個人情報の取扱いにおける事故報告」の傾向と注意点 <http://www.jisa. or.jp/privacy/pr/110525.pdf>(2013 年 5 月 8 日)

[2]広瀬文子(2007). ヒューマンエラー傾向測定手法作成の試み(その 1)ー調査票作成ならびにエラーと性格特性に関する検討ー 電力中央研究所報告 Y06014.

[3]山田尚子(1999). 質問傾向質問紙の作成及び信頼性・妥当性の検討 教育心理学研究 47 501-510.

[4]篠原一光・山田尚子・神田幸治・臼井伸之介(2007). 日常生活における注意経験と主観的メンタルメンタルワークロードの個人差 人間工学 43 201-21.

[5]中央労働災害防止協会(1991). 不安全行動と作業者の心理的要因の調査研究委員会報告書(第 3 報)