情報セキュリティ意識レベルの評価手法確立

リスクテイキング・スコアによる定量化

Creation of a Method to Assess the Information Security Awareness Level

Quantification with risk-taking score

（火力部　技術G）

IT（情報技術）を活用した業務が一般化してきたなかで貴重な社内情報を適切に管理するためには、社員一人一人の情報セキュリティに対する意識向上が重要となっている。このため、情報セキュリティ意識レベルの実態が定量的に評価できる手法を確立したので報告する。

(Engineering Section, Thermal Power Department)

As operations utilizing IT (Information Technology) have become widespread, it is imperative to improve employeesÅf awareness of information security in order to ensure the appropriate management of valuable in-house information. We have established an assessment method that enables quantitative evaluation of the actual information security awareness level, which can then be reported on in detail.

1 研究の背景と目的

電力自由化による本格的な競争時代を迎え、社内業務は、従来にも増して高度化・多様化が求められており、IT（情報技術）を駆使した各種情報システムが、これを支援するための有効なツールとなっている。

しかし、情報システムの利用が拡大するのに伴い、情報や情報システムの不適切な取扱いによる貴重な社内情報（個人情報、技術ノウハウ等）の漏えいや第三者による不正アクセスなど情報セキュリティに係わるリスクも増大してくる。

このため、社員一人一人の情報セキュリティ意識を高め、維持することが重要となるが、企業、部門、部署単位などの組織として意識レベルを評価する方法は、アンケート調査による各質問項目の回答割合から相対的に傾向を推定する程度に留まっており、重要度の割には実態を定量的に把握することができない状況である。

本研究は、アンケート調査結果を基に、組織としての情報セキュリティ意識レベルを定量化し、実態把握が容易となる評価手法の確立を目的として実施した。

2 研究の概要

(1) リスクテイキング・スコアの考え方

リスクテイキングとは、「危険と知りながら敢えて不安全（リスキー）な行動をすること」をいうが、ここでは「情報セキュリティ意識の低い人は総じて情報セキュリティ確保に対しリスキーな行動をしている」とした。

リスクテイキング・スコアは、アンケート質問項目のうち「行動」に関する13問の回答選択肢それぞれに、リスクレベルに応じて「低リスク：1p～高リスク：7p」を配点しておき（第1表）、一人一人の回答データをこの配点に置き換えて合計することにより求め、情報セキュリティ意識レベルを定量評価できるようにしたものである。

(2) リスクテイキング・スコアでの評価方法

ここで得られたリスクテイキング・スコアは、

・最小値　1p×13問＝13p（低リスク）

・最大値　7p×13問＝91p（高リスク）

となる。また、回答選択肢の非リスク側の配点を合計した最大値30pを超えた人は、「何らかのリスクを持った不安全な行動をしている」と推察できる。

これを展開し、回答者全員の平均値を求めること

第1表　アンケート質問項目と配点

	質問項目	回答選択肢 数	配点［上段:非リスク　下段:リスク］	
1	自宅のパソコンにウイルス対策をしているか	5	最新ソフトをインストール	1
			（その他の回答）	4～7
2	会社のパソコンのパスワードに何を設定しているか	9	その他で設定している	1
			（その他の回答）	7
3	会社のパソコンのパスワードを他人に教えているか	3	教えていない	1
			（その他の回答）	5、7
4	会社のパソコンのパスワードをメモしているか	3	以前からメモしていない 以前はあったが今はない	1 2
			現在もメモがある	7
5	会社のパソコンのパスワードが他人に知られたとき速やかに変更したか	3	変更した	1
			（その他の回答）	4、7
6	会社のパソコンのパスワードを更新しているか	3	定期的に更新している 不定期に更新している	1 3
			更新していない	7
7	FD、MOを廃棄する際に上書きや物理的な破壊をしているか	7	行っている	1～3
			廃棄したことがない 行っていない	4 5～7
8	仕事で取り扱っている文書やデータを第三者にみせてよいか判別できるか	6	判別できる	1～3
			判別できない	5～7
9	紙で配布したり保管する必要がない電子メールや電子文書を印刷するか	4	印刷しない	1、3
			印刷する	6、7
10	離席時には取扱いに注意を要する文書類を裏返すか片付けているか	6	行っている	1～3
			行っていない	5～7
11	取扱いに注意を要する文書・帳票類は夜間・休日に施錠して保管しているか	6	行っている	1～3
			行っていない	5～7
12	文書類の廃棄時にゴミ箱とシュレッダーのどちらで処分するかの区別ができるか	6	区別できる	1～3
			区別できない	5～7
13	文書類の廃棄時にゴミ箱とシュレッダーのどちらで処分するか1枚1枚確認しているか	6	確認している	1～3
			確認していない	5～7

で、組織としての総合評価ができると考えた。

(3) 妥当性の検証

平成15年1月および平成16年2月の2回実施したアンケート調査結果を基に、回答者全員のリスクテイキング・スコアを求めてヒストグラム化したところ、いずれも正規分布に近い形態を示したことから、配点方法は適切であったと評価できる（第1図）。

また、平均値はそれぞれ44.3p、39.7pであり、この差については、平成15年1月の調査後に、パスワード管理方法改善を主体とした周知や教育を行ったことによる効果が、平成16年2月のデータに4.6p減として現れたものである。

その裏付けとして、アンケート質問項目毎のスコアを算出し確認したところ、パスワード管理に関するスコアが約1p減と、他の項目と比べて大きく減少していた（第2表）。

これらの結果から、リスクテイキング・スコアによる評価手法の妥当性が実証できた。

3 研究の成果

本評価手法を適用することで、情報セキュリティ意識レベルの実態把握が容易となり、弱点となる項目の見極めや対策後の効果確認なども定量的に管理していくことが可能となった。

また、リスクテイキング・スコアは、組織の情報セキュリティニーズに合わせて質問項目の追加削除や配点のウエイト変更を行うことができるため、適用先を制約しない自由度も有している。

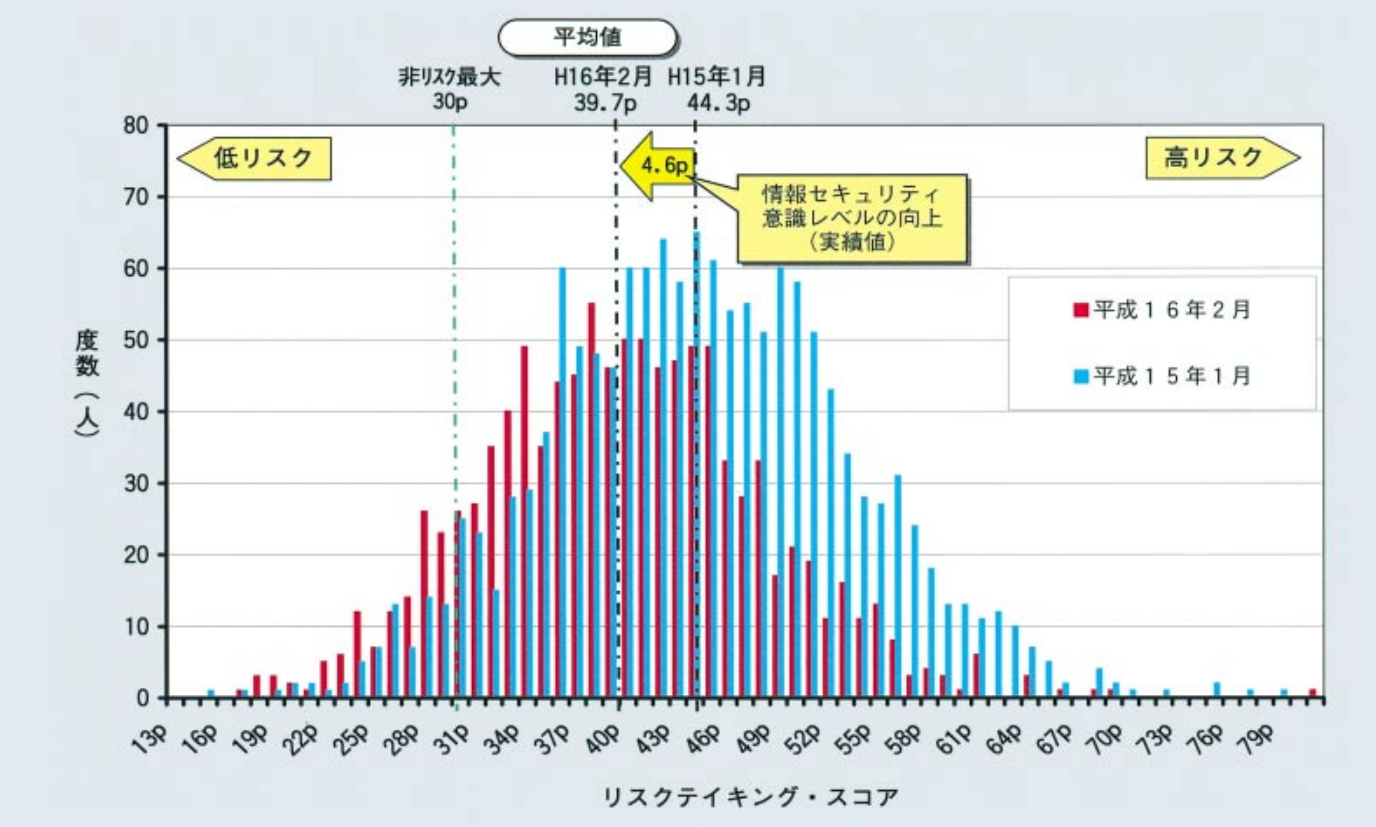
4 今後の展開

リスクテイキング・スコアを部門の情報セキュリティ意識向上を図るための指標として活用していく。

また、リスクテイキング・スコアをセルフチェックすることで、社員一人一人の意識付けにも役立つと考えられるため、その展開について検討を進める。

第2表　リスクテイキング・スコア算出表

質問項目＼調査結果		H16/2 (A)	H15/1 (B)	差 (A-B)
1	自宅のパソコンにウイルス対策をしているか	4.03	4.49	▲ 0.46
2	会社のパソコンのパスワードに何を設定しているか	4.44	5.43	▲ 0.99
3	会社のパソコンのパスワードを他人に教えているか	1.69	2.63	▲ 0.94
	：	：	：	：
13	文書類の廃棄時にゴミ箱とシュレッダーのどちらで処分するか1枚1枚確認しているか	2.07	2.15	▲ 0.08
合計スコア		39.7	44.3	▲ 4.6



第1図　リスクテイキング・スコアの分布

執筆者／疋田昌浩
Hikita.Masahiro@chuden.co.jp