Vol.2010-DPS-142 No.52
Vol.2010-CSEC-48 No.52
2010/3/5

従業員のリスク行動に対する企業の取り組みモデルの提案

大和田竜児[†]　　内田勝也[†]

2009 年，筆者が所属する情報セキュリティ大学院大学内田研究室で各企業の管理者に情報セキュリティに関するアンケートを実施した．この結果の内，情報セキュリティ事故原因を見ると，従業員のリスク認知意識の欠如からなる規則違反が原因と考えられる事象が上位を占めていた．
本稿は，こうしたリスク行動に対処すべく，3 つの柱からなる情報セキュリティ対策モデルを提案している．1 つ目の柱は，教育を中心としたリスク認知能力向上施策である．2 つ目は，従業員に対してリスク分析を行い，情報セキュリティマップを作成する事である．3 つ目は，リスク顕在化を想定した未然防止策について，データを主体とした手法で実現する事である．
この 3 つの施策は，個々に実施する事も可能であるが，連携する事で相乗的なメリットがある．

A Proposal for The Risk Management Model of Employee in The Company

Ryuji Owada[†] and Katsuya Uchida[†]

I am a member of the Uchida Laboratory in the INSTITUTE of INFORMATION SECURITY. They conducted a questionnaire survey about information security to the manager of each company in the year 2009. Information security incidents caused by violation of rules rank upper in this result. The factor of this violation would be lack in employee awareness to recognize the risk.
I propose a model of information security measures to deal with this risk. This model consists of three elements. The first one is measures that improve the employee awareness to recognize the risk. The second one is to create a map of information security. What we need is a risk analysis of employee to make this map. Thirdly, we must assume the risk is developing the incident, and to prevent from occurring it. In order to realize it, I propose the measures focusing on the attribute of data.
We can implement one of three measures independently. But, we better implement these measures together because each measure cooperates to make large effect.

1. はじめに

企業における情報セキュリティ対策は，一般的に，技術面，管理面，人的側面の 3 つの側面での対策が必要とされている．技術面では，日進月歩で確認される新たな驚異に対応すべく，日々発展を遂げている．管理面においても，情報セキュリティマネジメントシステムである ISO/IEC 27000 シリーズを代表とし，ガイドラインの標準化において一定の確立を見せている．人的側面での対策では，教育の実施や規則の制定，労働開始時の関連契約締結といった方法が主だったものである．しかし，昨今の情報セキュリティ事故の実態を見ると，現在の人的側面における対策に問題があるのではないかと考えられる．本稿では，従業員自らが情報セキュリティを考え，行動するために人的側面においてどの様な対策が必要かを述べていく．

2. 情報セキュリティ事故の実態

筆者が所属する情報セキュリティ大学院大学内田研究室にて，情報セキュリティ事故の実態に関するアンケート調査を実施した[1]．結果を見ると，ウイルス感染（50%），ノート PC 等の盗難（15%）が上位を占めている．少なくともこれらの対策は，企業内の情報セキュリティ規則に明文化されているであろう．これは，普段の情報機器利用において，従業員のリスク認知意識が欠如している事に起因していると考えられる．なぜ従業員は，規則に反する様なリスク行動をとってしまうのであろうか[a]．

3. 従業員によるリスク行動の発生

3.1 なぜリスク行動を起こすのか

従業員は，前述した規則や注意事項を一度は目にしているはずである．それにもかかわらず，リスク行動を起こす背景としては，仕事のやり方と関係がある様に思われる．例えば，ある従業員が，締め切り間際の顧客提案資料を自宅で作成するため，規則で禁じられている顧客データの持ち出しを実行してしまう事を考える．この時，違反の意識よりも顧客提案が成功した場合の会社に対するメリットが優先されてしまう．ここにおいて，従業員は個人よりも組織を優先するという善意の基では，違反に対する罪悪感が薄れてしまう事が想定される．岡本，今野ら（2006）が行った従業員が犯す違反に関するアンケートの分析結果を示す[2]．主因子分析の結果，違反は，個人的違反と組織的違反の 2 つに大別できるとしている．更に各因子の関係を見るべく共分散構造分析を行っている．合わせてその結果を図 1 に示す．

[†] 情報セキュリティ大学院大学
Graduate School of Information Security INSTITUTE of INFORMATION SECURITY

a) 本稿では，自分の意識に基づいて行う行動で，結果的にリスクを伴うものを対象として研究を行った．

ⓒ2010 Information Processing Society of Japan

Vol.2010-DPS-142 No.52
Vol.2010-CSEC-48 No.52
2010/3/5

- 個人的違反：就業中に仕事をさぼったり，備品を持ち出し私物化したりする．
- 組織的違反：作業効率化のためにルールを破る．誠実より組織への貢献をとる．

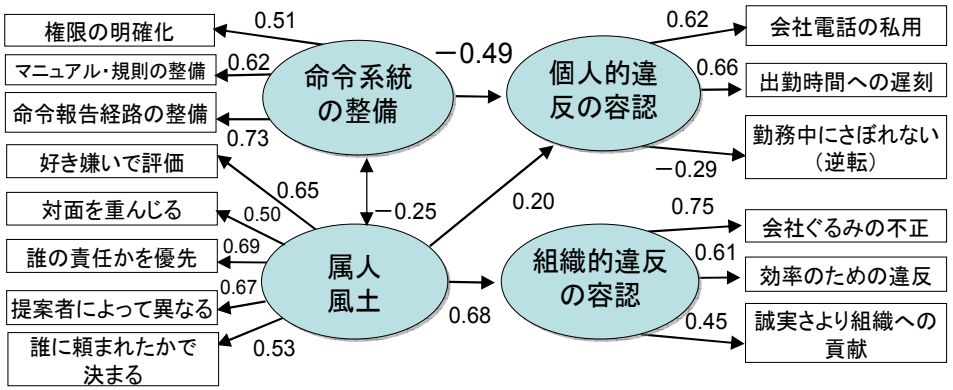

図 1 違反と組織風土に関する共分散構造分析[2]

図 1 より，規則や命令系統の整備は，個人的違反の規定要因となっているが，組織的違反の原因にはなっていない事が分かる．組織的違反については，これまで行ってきた対策以外にも何か必要である事を示している．前述の通り，情報セキュリティにおける事故事例では，組織的違反がその大きな要因としてあげられているのである．

3.2 リスク行動への対策方針

従業員が起こすリスク行動に，どの様な観点で対策を行う必要があるのだろうか．本稿では，以下に示す視点が必要であると考える．

- 情報セキュリティに関する従業員のリスク認知力を高め，組織あるいは自らへの影響を予測できる能力を醸成する．
- 従業員のリスク行動に起因する事故が顕在化する事を想定し，予防策を講じる．

それぞれ片方だけで，作用するには効果が薄い．2 つの施策を有機的に連携させ，相乗的に効果を高めていく必要がある．この「リスク認知能力向上」と「リスクを想定した未然防止策」に加え，これらを連携する「従業員の情報セキュリティマップ作成」の 3 つの柱からなる人的セキュリティ対策モデルを提案する．

以下に提案モデルの概要図を示す．以降では，この詳細について述べていく．

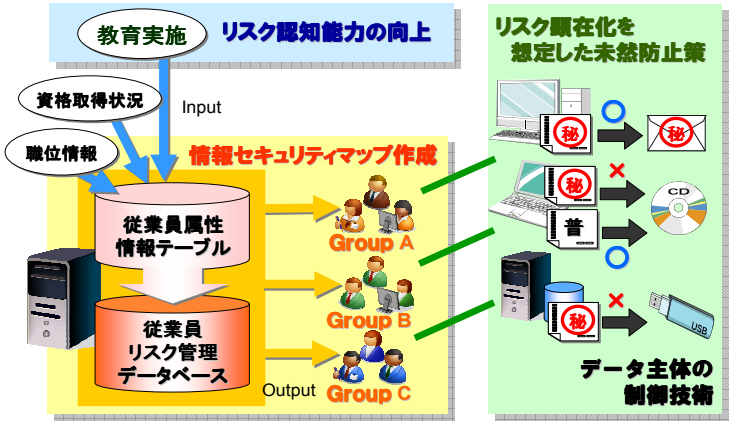

図 2 提案モデルの概要図

4. リスク認知能力の向上

まず，1 つ目の柱として，リスク認知能力向上に関する施策について記載する。現在，企業が実施している情報セキュリティの人的側面への施策としては，「従業員教育の実施」，「規則の作成」，「雇用開始時等に守秘義務の締結」等が考えられる．これらは，それぞれ必要不可欠なものである。ここでは，リスクを認知するための「能力向上」という積極的な命題に対し，従業員教育に関する検討を行う。

4.1 企業における情報セキュリティ教育の現状

企業における情報セキュリティ教育の現状を示す調査結果を見ると，教育を実施していない企業が約 4 割弱存在し，実施しても目的の達成度が半分以下である場合が，約 7 割を占めている[1][3]．これでは，従業員のリスク認知能力向上は，見込めない．問題は，現在の企業教育の形態が，集合教育や e ラーニングでの知識や情報提供に依存しているからではないかと考えている．更には，教育実施後のアンケートやペーパーテストで，正しく教育の効果を測定できていないからではないだろうか．これでは，定期教育を何度実施しても目標となる効果を得る事が難しい．以降では，教育の流れを基に情報セキュリティ教育の実施形態を再考する．

4.2 企業教育の流れ

企業教育の流れを図 3 に示す．本稿では，この流れの中でステップ 3，ステップ 4 に着目した．それぞれ，実態とそれに対する問題点を纏めたものを表 1 に示す．

ⓒ2010 Information Processing Society of Japan

Vol.2010-DPS-142 No.52
Vol.2010-CSEC-48 No.52
2010/3/5

表 1 教育段階における実態と問題点

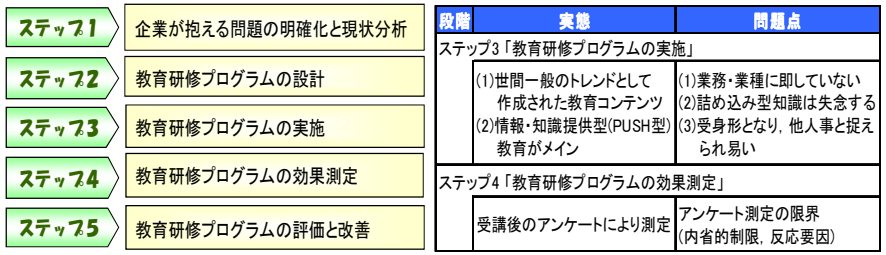

図 3 企業における教育の流れ[b]

段階	実態	問題点
ステップ3「教育研修プログラムの実施」		
	(1)世間一般のトレンドとして作成された教育コンテンツ (2)情報・知識提供型(PUSH型)教育がメイン	(1)業務・業種に即していない (2)詰め込み型知識は失念する (3)受身形となり，他人事と捉えられ易い
ステップ4「教育研修プログラムの効果測定」		
	受講後のアンケートにより測定	アンケート測定の限界 (内省的制限，反応要因)

表 1 の内，アンケート測定の限界について補足事項を加筆する．先述した，岡本・今野らは，アンケートやペーパーテストにおける制限として，「測定結果を歪める 2 つの危険性があることが知られている」としている[2]．1 つは，内省的制限であり，「回答者の内省能力には限界があり，自身が思う程，理解出来ない.」としている．もう 1 つは，反応要因であり，「回答する際，客観的にみて望ましいと思われる回答を選ぼうとする.」というものである．つまり，現在用いられている方法では，これらの心理的な限定要因によって，正しい測定結果が得られていない可能性がある．特に企業が従業員に対して行う調査では，自身への評価の懸念から反応要因が強く働く事が想像できる．以降では，このステップ 3，4 について改善するための方法論を提案する．

4.3 教育研修プログラムの実施

前述では，知識提供型教育の問題点を指摘したが，これは決してそれ自体を否定するものでは無い．合わせて，＋α の研修形式が必要である事を示しており，本稿では，KYT（Kiken Yochi Training：危険予知訓練）を提案する．

KYT は，安全工学の研究分野から発展してきた．製造工場や工事現場等で，作業者が事故や災害につながる予兆を事前に察知する能力を身に付けるためのトレーニング方法である．研修では，教材（作業現場等のイラストや写真，ビデオ，動画，音声等）を参照し，4～5 人のグループでどの様な危険が潜んでいるか，事前の対策はどうするかといった議論を行う事で，リスクに対する気付きを与えている．

情報セキュリティの分野では，リスクが顕在化した場合の被害の大きさを口頭で説明しても実感し難い．このため，既に一部の企業において，こうした KYT が従業員教育に既に用いられている．本稿では，更に ETA，FTA といった 2 つの観点から再考し，より効果のあるものにする事を提案したい．ETA，FTA の模式図を以下に示す．

b) 堤ら（2007）「はじめての教育効果測定」pp.75 掲載の図を基に加筆[4].

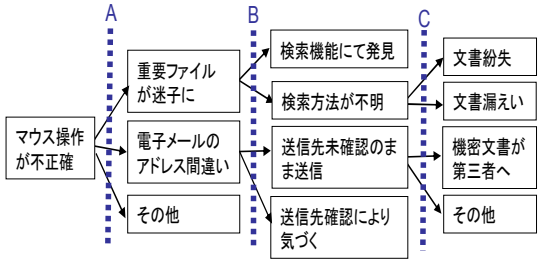

図 4 動的流れの中での ETA

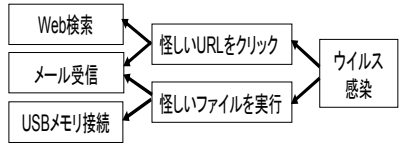

図 5 FTA による事故経路の推測

(1) **ETA**

ETA（Event Tree Analysis）とは，きっかけ演繹法とも訳されている．一つの事象から発生する事象を枝分岐で列挙していき，次に発生する事象を網羅的に把握するための危険予知方法である．事故を顕在化させないためには，ヒヤリハットと事故との境を把握し，事故につながる事象の連鎖を早い段階で切断する必要がある．静止画での KYT だけで無く，図 4 中 A，B，C で示す各時点の様に，動的な流れの中で判断力を養わせる．各時点で自らが選択した行動が，どの様な結果を及ぼすかについて即時に知る事ができるというメリットがある．

(2) **FTA**

一方，FTA（Fault Tree Analysis）は，事故原因帰納法と訳されている．ETA とは逆の発想で，事故から原因となる事象を論理的に推定し，列挙していく方法である．元来，KYT は ETA での観点で構成されている事が多い．ETA は，一つの事象を起点としているが，日々の業務では，様々な事象に遭遇しており，必ずしも同じ起点事象では無い．だからと言って，想定される起点事象を増やしていく事にも限界がある．そこで，事故を起点とした FTA の観点で，事故につながる経路を逆算する事により，業務に内在するリスクが事故へつながるイメージができるようになる．

この様に，シミュレーション形式の KYT を実施する事で，講義や e-ラーニング等による知識提供を補う事が可能である．これを裏付けるデータを図 6 に示す[5]．シミュレーションが他の研修より，知識の定着率が 2～15 倍も高い．

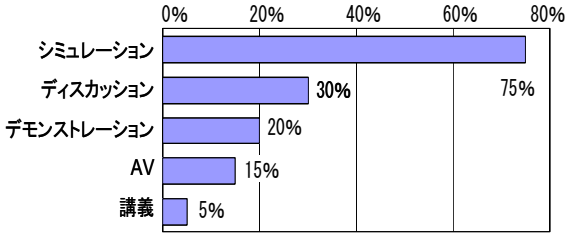

図 6 研修別に見た知識の定着率の比較

ⓒ2010 Information Processing Society of Japan

Vol.2010-DPS-142 No.52
Vol.2010-CSEC-48 No.52
2010/3/5

4.4 教育研修プログラムの効果測定

次に，企業教育の流れで問題点として指摘した教育実施後の効果測定について考察する．一般的に教育の効果測定方法として広く用いられているアンケートでは，質問を見て考えてから回答する事で，前述したバイアスが発生すると考えられる．そこで，より潜在的な態度を測定する手法として，IAT（Implicit Association Test：潜在連合テスト）を紹介する．これは，1998 年にグリーンワルドとバナジ（Greenwald and Banaji）が開発し，人種への潜在的な偏見やナショナリズムの度合いを測定する方法として，以降，研究や実証がなされている．本稿では，IAT の情報セキュリティ分野への適用可否について，筆者が行った実証実験の内容及び分析結果について示す．

4.5 効果測定方法の実証実験

今回、IAT の仕様[6]に従い，筆者はコンピュータ上で実施する測定プログラムを作成した．実験概要は以下の通りである．

実験対象者：何らかの組織に属する従業員　　調査期間：2009/10/4～11/13
依頼方法　：知人・関係者へ E メールで依頼　回収方法：E メールが自動で送付
回収数　　：130（有効回答数 103）　　IAT 概要　：図 7，表 2，表 3 参照

図 7 IAT 測定画面例

表 2 カテゴリ及び刺激語

カテゴリ1	良い	悪い
刺激語	嬉しさ	苦悩
	愛情	ひどい
	平和	恐ろしい
	素晴らしい	意地の悪い
	楽しみな	邪悪な
	輝かしい	すさんだ
	笑い	失敗
	幸せな	害する
カテゴリ2	慎重派	行動派
刺激語	注意深い	大胆
	じっくり	アクティブ
	事前確認	直感
	プロセス重視	結果重視
	熟考	即決
	用心する	単刀直入

表 3 各ステージの概要

ステージ	カテゴリー 左上	カテゴリー 右上	試行回数	位置づけ
1	良い	悪い	20	練習
2	慎重派	行動派	20	練習
3	良い+慎重派	悪い+行動派	20	本試行
4	良い+慎重派	悪い+行動派	40	本試行
5	悪い	良い	20	練習
6	悪い+慎重派	良い+行動派	20	本試行
7	悪い+慎重派	良い+行動派	40	本試行

IAT は，図 7 の画面の様に中央に表示される刺激語が，左右どちらのカテゴリに含まれるかを回答する単純なテストである．刺激語とカテゴリの関係は，表 2 の通りであり，表 3 に示す各ステージで関連する刺激語がランダムに表示される．回答速度を分析する事で，慎重派と行動派のどちらに潜在的に迎合しているかを測定出来る．

今回は，IAT と合わせてアンケートを行った[c]．以下の設問で「ある」又は「ない」と回答したそれぞれの群の IAT 測定結果について，t 検定を用いて比較した[d]．

(ア) パスワードを他人に教えたり，業務上関係無い社内データを許可無く参照したことがある？
(イ) 業務データを許可無く持ち帰ったことがある？
(ウ) 会社のパソコンで業務上関係無いホームページを閲覧したり，私的な電子メールを送受信したことがある？

結果は，情報セキュリティ違反に関する設問である（ア），（イ）のいずれも IAT 測定結果に有意な差を認める事が出来なかった．但し，情報セキュリティ違反では無いが，業務外利用の有無に関する設問（ウ）では，有意な差を認める事が出来た[e]．この事から，従業員の態度を測定する方法として IAT を用いる事は可能だが，情報セキュリティに関する態度を測定するためには，今回，実験に用いたカテゴリ及び刺激語について再考する必要がある．より精度を高めるために実験を繰り返す必要がある．

以上，リスク認知能力の向上施策として，教育実施段階では，ETA，FTA からなる KYT を，また，効果測定段階では，IAT における手法を用いる事を提案する．但し，IAT については，今後の実験により精度向上が必要である．

5. 従業員の情報セキュリティマップの作成

次に 2 つ目の柱として位置づけている従業員の情報セキュリティマップの作成について述べる．マップは，従業員に対してリスク分析を行って作成する．情報セキュリティにおけるリスク分析は，組織がかかえる機密情報等に対して行われるのが一般的である．本稿では，なぜ従業員を対象としてリスク分析を行う必要があるとしているか．その理由を，以下に 2 つ示す．

- 情報セキュリティ施策を展開する管理者の一方的な想いと従業員の順守意識の間に不均衡が発生している
- 組織内で起きた事故の原因を分析する際，「人」に言及したものが不足している

こういった実態を踏まえ，情報セキュリティ施策の展開を効果的に行うために必要なのが，従業員に対するリスク分析なのである．これまで通り，保護対象となる情報

c) アンケートでは，先に示したバイアスを回避するために，組織外における調査である旨を明示した．
d) 有意水準は，いずれも 5%で算出．
e) 各検定結果．（ア）(t=-0.23,df=101,p<.05)，（イ）(t=-0.15,df=14,p<.05)，（ウ）(t=2.74,df=101,p<.05)

ⓒ2010 Information Processing Society of Japan

Vol.2010-DPS-142 No.52
Vol.2010-CSEC-48 No.52
2010/3/5

のリスク分析を行うのは，当然の事として実施する必要はあるが，それだけでは不足している．なぜなら，「扱う人」にはそこまで深く言及していないからである．同じデータでもそれを取扱う人間にとって如何様にもリスクは変動する．現在のリスク分析方法から対策を選定するプロセスでは，データを扱う従業員自体のリスク分析が出来ているかと言えば不十分であると言わざるを得ない．

こうした従業員の組織感情や事故の分析結果，再発防止策における問題点に対し，本稿では，従業員の情報セキュリティマップの作成を提案する．

5.1 非情報セキュリティ関連属性でのリスク分析の必要性

マップ作成にあたり，従業員に対してどの様にリスク分析を行うか．対象が人間となるため，データの様に機密性，完全性，可用性といった属性を持たない．そのため，前述した教育の受講状況や関連資格の取得状況等を属性情報とする事が考えられる．しかし，対象が人間である以上，感情等の不確定要因が考えられるため，より多角的な情報を基に分析を行う事で結果を補完する必要がある．そこで，情報セキュリティに関連する属性情報だけで無く，それ以外のデータも含めて用いる事で，従業員のリスク分析を行う．その根拠となるデータを示す．以下は，前章の IAT の実証実験で採取したアンケート結果をクロス集計した結果である．

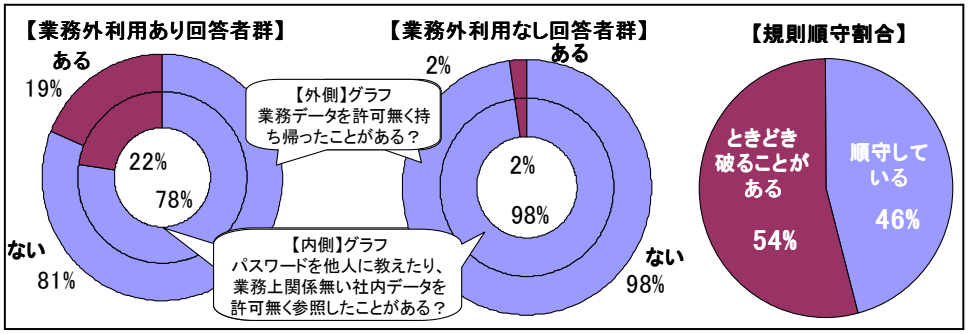

図 8 業務外利用と情報セキュリティ規則順守度の関係

前章でも示した「会社のパソコンで業務上関係無いホームページを閲覧したり，私的な電子メールを送受信したことがある？」という業務外利用に関する設問で「ある」と回答した群の情報セキュリティ違反状況（左）と業務外利用は「ない」と回答した群の状況（中央）を比べたものである．これを見ると，普段，業務外利用が「ある」回答者群の方が，「ない」回答者群に比べ，情報セキュリティ違反を起こす割合が高い事が見て取れる．更に，右側の円グラフは，「いずれかの情報セキュリティ違反」及び「業務外利用」の両方とも経験がある回答者の情報セキュリティ規則への順守状況を示したものである．これを見ると，「順守している」と「ときどき破ることがある」の間にほとんど差が無い事がわかる．つまり，これらの従業員に対しては情報セキュリティ規則の存在が意思決定に影響を及ぼす可能性は低いと考えられる．この事から，規則による抑制だけでは，効果を得られる可能性は低く，それ以外の対応が必要であると考えられる．今回の調査結果から分かる事は，図 8 に示す通り，業務外利用有無といった非情報セキュリティ関連属性との関係性もあるということである．

これは，業務外利用意外にも，「営業職は，データの持ち出しが多い」，「フリーソフトウェアを多く利用している場合，マルウェアが存在する可能性も高い」等といった様に非情報セキュリティ関連属性が事故要因になるケースも想定できる．こういった様々な属性を整理し，リスク分析を行うべく従業員の情報セキュリティマップの作成が必要であると考えた．以降，その作成のプロセスについて述べていく．

5.2 情報セキュリティマップ作成のステップ

実際に情報セキュリティマップを作成するには，以下に示す 4 つのステップで行うことが可能であると考える．以降では，この 4 つのステップについて順に述べていく．

- 従業員属性情報テーブルの作成
- 管理者による各属性へのリスク値の定義付け
- 各従業員の情報を入力して従業員毎にリスク値を算出
- 従業員情報セキュリティマップの作成

(1) 従業員属性情報テーブルの作成

従業員は組織に属して業務を行っている以上，図 9 に示す通り，様々な特徴を持ちえている．本稿では，便宜上，これらの特徴を従業員の属性情報と呼ぶ事とする．

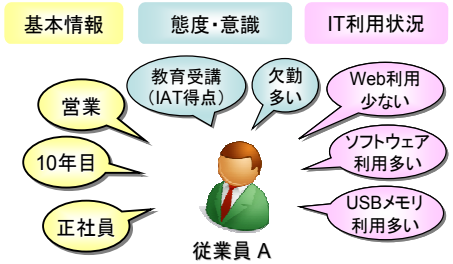

図 9 従業員の属性情報

表 4 従業員属性情報テーブル作成例

大別	属性	属性値
基本情報	性別	男性，女性
	年代	10代，20代，30代，40代，50代，60代
	職種	管理職，専門・技術職，事務職，営業職等
	役職	幹部相当，部長相当，課長相当，役職無し等
	雇用形態	正社員，派遣社員，パートタイマー等
態度・意識	IAT得点	−1.0〜−0.4，−0.5〜0，0〜0.4，0.5〜1.0
	欠勤数(月)	0日，1〜5日，6〜10日，11〜15日以上等
	職務満足度	悪い，やや悪い，普通，やや良い，良い 等
IT利用状況	社外Web閲覧	0回，1〜20回，20〜30回，30回以上等
	追加ソフト数	0，1 〜 3，3 〜 6，6 〜 9，10以上等
	外部記憶媒体利用回数(日)	0，1 〜 3回，3 〜 6回，6回以上等

ⓒ2010 Information Processing Society of Japan

Vol.2010-DPS-142 No.52
Vol.2010-CSEC-48 No.52
2010/3/5

この属性情報は，客観的な情報として採取することが可能であり，それを基に表 4 の様な従業員属性情報テーブルを作成する．勿論，自社の業種や業務形態によって属性値は異なる．当初は，人事部門等と協力し，なるべく多くの属性値を列挙しておく事が望ましい．その分，多角的にリスク分析をするための元データに出来るからである．尚，本稿では，表 4 に示す通り，属性を，「基本情報」，「態度・意識」，「IT 利用状況」に分類した．最終的にマップを作成する際，この分類を活用する．

(2) 管理者による各属性へのリスク値の付加

次に，情報セキュリティ管理者は，個々の属性値に対してどれくらいのリスクがあるかを値として付加していく．始めは，どの様にリスク値を付加していけばよいか迷うところであろう．いきなり全てを正しく入力しようとするのは，不可能に近い．そこで，以下の方法を順に行い，次第に精度をあげていく方法が現実的であると考える．

(ⅰ) リスク値を何段階評価にするかを決める
本稿では、例としてリスク無しを 0 として低い方から順に 1～5 の 6 段階とした。

(ⅱ) 各段階のリスク値を付加する基準を作成する
定義した段階毎にリスク値を付加する基準を作成する。下表は、本稿での例。

表 5 管理者によるリスク値 付加基準例

リスク値	付加基準
0	情報セキュリティ上のリスクは発生しないと判断できる場合。過去に本属性に該当する従業員が，既存のヒヤリハットや事故を起こして無い事が前提
1	過去に本属性に該当する従業員が，既存のヒヤリハットや事故を起こしているわけでは無いが，必ずしも，リスクが無いと判断できない場合
2	過去に本属性に該当する従業員から既存のヒヤリハットの報告が若干，あげられている場合
3	過去に本属性に該当する従業員から既存のヒヤリハットの報告が多く，あげられている場合
4	過去に本属性に該当する従業員が，対外的な報告まではいかなかったが，業務に影響を及ぼす様な事故を発生させてしまっている場合
5	過去に本属性に該当する従業員が，社外発表を余儀なくされ，業績に影響を及ぼす様な大きな事故を発生させてしまっている場合

(ⅲ) 各属性に初期値としてリスク値を「1」で定義する．
始めから正確なリスク値の定義は難しい．まずは，全ての属性に「1」を付加する．

(ⅳ)ヒヤリハット報告や事故事例からリスク値を修正する
最後に，過去のヒヤリハット報告や事故事例から，表 5 の基準に基づきリスク値を定義する．この際，社内の事例はもとより，他社事例を参考にしてもよい．

この様に，上記 4 つのステップを基に，なるべく属人性を排除する形で従業員属性情報テーブルの各属性にリスク値を付加していく．組織によって基準は異なると思われるため，上記 4 ステップが必ずしもベストな方法とは言い切れ無いが，こういった形で，情報を蓄積していき，精度を向上させていく事が望ましいと考える．

(3) 各従業員の情報を入力して従業員毎にリスク値を算出

管理者によって，従業員属性情報テーブルにリスク値が付加されれば，後は人事部門や情報システム部門等から情報を入手し，各従業員の属性情報を入力していけばよい．これにより，各従業員のリスク値を算出する事が可能となる．この際，単純に全ての属性のリスク値を合計して各従業員のリスク値としても良いが，最終的に類型化して情報セキュリティマップを作成するため，表 4 で分類した「基本情報」，「態度・意識」，「IT 利用状況」毎にリスク値を合計する．

(4) 従業員情報セキュリティマップの作成

最後に，3 つの分類を軸とした 3 次元散布図に，各従業員のリスク値をプロットしていく．この結果，リスク度が高い従業員を類型化（グループ化）する事が可能になる．この 3 つのグループに対して，特徴をつかむ事で，情報セキュリティ教育等を行う際の参考データとする事が出来る．以下に，今回の最終的な作成例を示す．

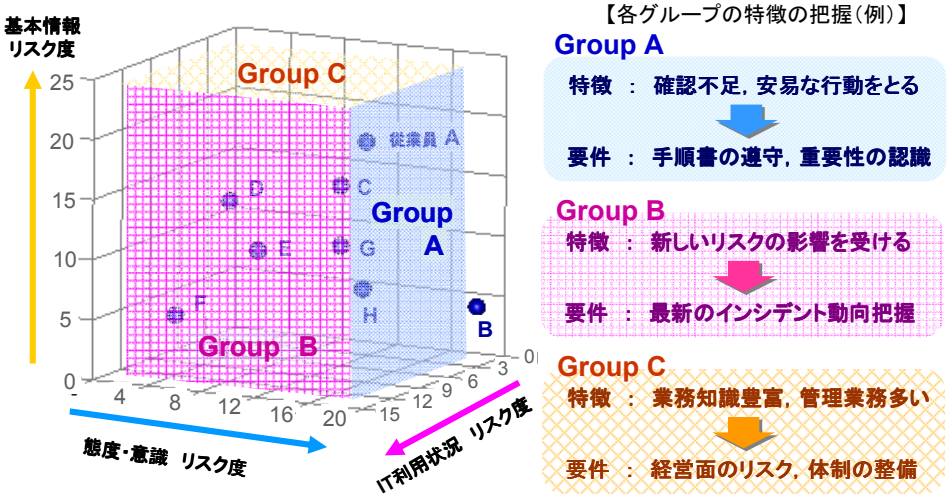

図 10 従業員情報セキュリティマップの作成例

ⓒ2010 Information Processing Society of Japan

Vol.2010-DPS-142 No.52
Vol.2010-CSEC-48 No.52
2010/3/5

6. リスク顕在化を想定した未然防止策

最後に, 3 つ目の柱であるリスク顕在化を想定した未然防止策を述べる. 本稿では, ここまで, 教育の実施方法や従業員のリスク分析手法を述べてきた. しかし, これら施策を推し進める中で, 大多数の従業員がリスクに対して的確に判断し, 行動する様になるまでには時間を要する. 一方, 冒頭で示した通り, 従業員のリスク行動が要因となり事故につながっているという現実を考えると未然防止策が急務となる. これには, 意識向上施策とは別の観点で行う必要があり, 技術的な対策が求められる. この際重要なのは, 意識向上施策が浸透するまでの経過措置として対策を並行で実施するのでは無く, 先に示したリスク能力向上施策や従業員の情報セキュリティマップと連携し, 一貫性を持った対策を進めるという点である. 連携によるメリットは後述することとして, 本章では, 技術的な仕組みとしての未然防止策について考察する.

6.1 機密情報取扱方法の問題点

まず, 現在行われている機密情報の取扱方法の問題点について述べる. 個々の対策技術の組み合わせによる場合, 図 11 で示す様にそれぞれが独立して機能していると考えられる. これにより,「権限がある社員が入手した非機密情報も持ち出しできない. 又は, 持ち出せても煩雑な手続きを要する.」といった形で利便性の面で難が生じ, 結果として違反を行ってしまう等, 利便性と機密性のバランスがとれていなかった. そこで, これまで境界制御を前提とした対策技術ありきで考えられていた機密情報の保護について, 本来リスク分析の対象となるデータを主体として対策が行われる必要があると考えた.

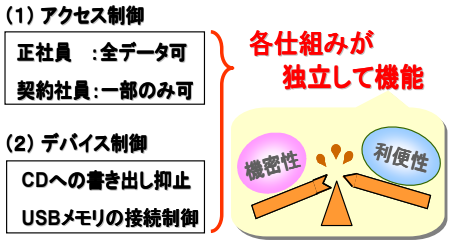

図 11 既存の情報制御技術の問題点

6.2 データ主体の対策

データを主体とした管理方法を考えるにあたり, まず, データのライフサイクルをおさえておく必要がある. なぜなら, 現代の情報インフラの発展に伴い, データは非常に流動的であり, 時間や存在箇所, 保有者等様々な場面において活用されているからである. 図 12 に示す通り, データの作成から廃棄に至るまで, 様々なイベントが発生していることがわかる[f].

f) 竹井 (2004)「情報の価値とライフサイクル管理」pp.15-16 掲載の図を基に加筆[7]

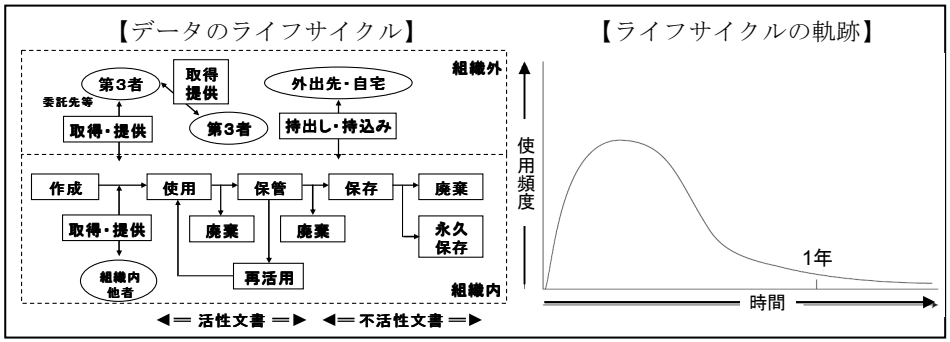

図 12 データのライフサイクルとライフサイクルの軌跡[7]

アクセス制御, デバイス制御といった対策技術を用いた場合, 効力を発揮するのは, 組織内外でのデータ移動時であろう. しかし, 正しい手続きを経て委託先等の第 3 者へデータを提供した場合, 更に別の第 3 者へ提供されることまでは制御が難しい. また, 組織内の場合でも, 権限を持った従業員から権限を持たない他の従業員へ渡ることも考えられる. これらは, 境界制御で対策する事が難しい.

この様に情報のライフサイクルの観点からも, データ主体での管理が必要である事が分かる. ではどの様にデータ主体の管理方法を実現するか. その仕組みとして, DLP (Data Loss Prevention 又は, Data Leak Prevention) と連携する事が, 現時点では有効であると考えている. これまで, 職位や部署等を基準としたアクセス制御やデバイス制御が, 人や物を視点としているのに対し, DLP は, データを主体とした考え方である. DLP の考え方を基に, データを主体としたあるべき管理方法について考察する.

6.3 データの属性

データ主体の管理方法を考えた場合, データ自体にどの様な属性を持たせて管理するかを検討する. 情報セキュリティの観点からすると「機密区分」,「保有者」,「廃棄期限」といった内容が盛り込まれる必要があると考える. 以下に詳細を記載する.

(1) 機密区分

最も重要な属性であると同時に定義方法が難しい. 管理者が, 区分するのでは, 大量のデータを扱う事になり, 適正な設定が困難となる. そこで, データの作成や取得時点で, 各々が必ず設定する仕組みを設ける必要がある. 管理者は, それが適正化どうかを判断するといった程度で済む. この方法は, 作成者が機密区分のルールを理解している必要があるため, 明確な基準の作成と教育等による意識付けが必要となる.

ⓒ2010 Information Processing Society of Japan

Vol.2010-DPS-142 No.52
Vol.2010-CSEC-48 No.52
2010/3/5

(2) 保有者

データ自身に保有者の情報を自動で付与する．時系列で追記していく事で，いつ，誰が作成したり複製したりしたものかが分かる．万が一，情報漏洩等の有事の事態が発生した際，漏洩元を特定する事以外にも，事前の心理的な抑制効果も期待できる．この際，実際の氏名は個人情報にあたるため，社員番号等当該組織内においてのみ判別可能な情報を属性として持たせる形となる．

(3) 廃棄期限

データが廃棄されれば，少なくとも当該データ自体がそれ以上広まる事は無いが，実際は，残ってしまう場合の方が多いのでは無いだろうか．図 12 の右図に示した通り，竹井（2004）によれば，「文書の使用は，90%が半年以内に作成された文書であり，99%%が 1 年以内のものであるといわれている．」と述べている[7]．機密区分にもよるが，作成時点で廃棄期限を強制的に定義付けすることで，廃棄漏れを防ぐ事が可能になる．必要であれば，時期が近づいた時点で注意喚起を行う仕組みにし，延長すればよい．

以上， 3 つの属性の必要性を述べたが，上記以外にも既存技術である「印刷不可」や「文字列のコピー不可」等も必要に応じて付与する．DLP では，データからフィンガープリントを取得することで，データの同一性を図る技術が用いられている．採用する手法にもよるが，対象文字列を変更した程度であったり，ファイルの中身をコピーして作成したファイルであったりしても同一のファイルとして管理する事ができる．この技術により，今回示した属性情報をそのまま引き継ぐ事が可能であると考える．

7. 3 つの施策の連携

ここまで示した 3 つの施策について，個々に行う事も可能だが，右図に示す通り，連携する事でその効果を発揮出来ると考えている．この様に，3 つの施策が相互に補完し合うことで相乗効果が生まれ，より一貫性をもった人的セキュリティ施策となる．

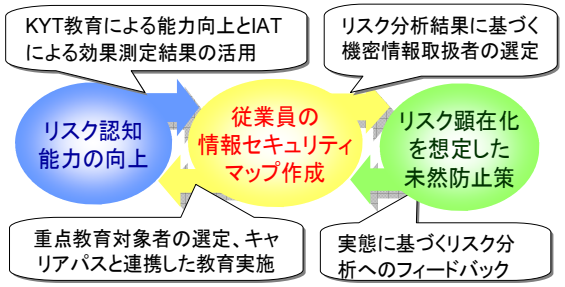

図 13 連携によるメリット

個々の施策をそれぞれで実施する限り，段階的な投資が可能だが，成熟してくると利便性の面において難が生じる事態になりかねない．相互連携を想定した一貫性をもった施策の実現が求められる．

8. まとめ

企業の管理者に対するアンケート結果より，情報セキュリティに関する事故において従業員のリスク行動が影響している可能性がある事が分かった．そこで，本稿では，「リスク認知能力の向上」，「従業員の情報セキュリティマップの作成」，「リスク顕在化を想定した未然防止策」の 3 つの柱からなる対策モデルを提案した．

リスク認知能力の向上では，従業員教育に着目し，ETA や FTA の観点からなる KYT を行う必要がある事を述べた．教育効果の測定方法として IAT を用いた情報セキュリティに関する潜在態度の測定を提案した．

次に，従業員の情報セキュリティマップ作成の必要性とその作成方法について述べた．作成時に，非情報セキュリティ関連の情報を用いて従業員のリスク分析を行う有効性を述べた．マップの作成により，リスクが高い従業員を類型化することが可能になり，教育を始め，各種情報セキュリティ施策の根拠としていく事が出来ると考えた．

3 つ目の施策として，リスク顕在化を想定した未然防止策について述べた．境界制御の対策を個別に実施する事で，利便性と機密性の不均衡が発生していることを指摘した．その対策として，データ主体の観点での対策の必要性を示し，機密区分，保有者，廃棄期限といった属性をデータ持たせる必要がある事を述べた．

最後に，これら 3 つの施策を連携して実施する事によるメリットを述べた．

今回，本稿で示した内容は，現在企業がかかえる問題を指摘し，対策のために必要な観点を示したに過ぎず，今後，より具体化していく必要がある．提案モデルを検討する事で，企業における人的セキュリティの対策が少しでも促進できれば幸いである．

参考文献

1) 情報セキュリティ大学院大学 内田研究室「第 6 回情報セキュリティ調査」
http://lab.iisec.ac.jp/~uchida_lab/enq/csi/2008/JSSM_23nd_E-2-1.pdf
2) 岡本浩一，今野裕之：組織健全化のための社会心理学，新曜社, pp.26-30(2006)
3) NRI セキュアテクノロジーズ 「企業における情報セキュリティ実態調査 2008」
http://www.nri-secure.co.jp/news/2008/1127_report.html
4) 堤宇一，青山征彦：はじめての教育効果測定，日科技連,pp59-79(2007)
5) アクセンチュアテクノロジーコンサルティング：強い IT 戦略，東洋経済新報社, pp.24(2008)
6) Anthony G. Greenwald「Summary of Improved Scoring Algorithm」
http://faculty.washington.edu/agg/IATmaterials/Summary%20of%20Improved%20Scoring%20Algorithm.pdf
7) 竹井潔：情報の価値とライフサイクル管理，聖学院大学論叢，第 17 巻，第 1 号，pp.15-16(2004)

ⓒ2010 Information Processing Society of Japan