社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2008－CSEC－42（38）
2008 / 7 / 25

Best Match Security
－個人に適したセキュリティ対策を講じるシステムの提案－

中澤 優美子[1] 加藤 岳久[2] 漁田 武雄[3] 山田 文康[3] 西垣 正勝[4,5]

[1]静岡大学大学院情報学研究科 〒432-8011 浜松市中区城北 3-5-1
[2]東芝ソリューション(株) IT 技術研究所 〒183-8512 東京都府中市片町 3-22
[3]静岡大学情報学部 〒432-8011 浜松市中区城北 3-5-1
[4]静岡大学創造科学技術大学院 〒432-8011 浜松市中区城北 3-5-1
[5]独立行政法人科学技術振興機構，CREST
E-mail: [1]gs08051@s.inf.shizuoka.ac.jp, [2]Kato.Takehisa@toshiba-sol.co.jp, [4]nisigaki@inf.shizuoka.ac.jp

あらまし あらゆるシステム・ネットワークがIT化した現在において，情報セキュリティマネジメントの重要性が益々高まっている．一方，セキュリティ意識やサービスの利用環境はユーザで異なるため、画一的なセキュリティ対策を提供するだけではシステムやサービス全体のセキュリティを確保することは難しい．このため，現在のセキュリティ対策はその効果が十分に発揮されているとは言い難く，対策が利用されていないことさえ多い．本研究では，性向，経験，環境の要因を基に，個人ごとに好適なセキュリティ対策を講じるシステムの実現を目指す．本稿ではシステムの基本構成、実装方針、利用例を概観する．
キーワード セキュリティマネジメント，セキュリティ対策，セキュリティ意識，性向，性格検査

Best Match Security
－The proposal of a knowledge-based system for selection of security countermeasures according to user disposition.－

Yumiko NAKAZAWA[1] Takehisa KATO[2] Takeo ISARIDA[3] Humiyasu YAMADA[3]
Masakatsu NISHIGAKI[4,5]

[1]Graduate School of Informatics, Shizuoka University
[2]Advanced IT Laboratory, TOSHIBA Solutions Corporation
[3]Faculty of Informatics, Shizuoka University
[4]Graduate School of Science and Technology, Shizuoka University
[5]Japan Science Technology and Agency, CREST
Email: [1]gs08051@s.inf.shizuoka.ac.jp, [2]Kato.Takehisa@toshiba-sol.co.jp, [4]nisigaki@inf.shizuoka.ac.jp

Abstract The importance of security measures are considerably increasing in the recent information society. The service providers are supplying security countermeasures to users. Because of different considerations towards security and environment for the usage of services among individuals, however, those measures do not make sufficient effect and not useful. Here in this paper, we propose to construct a knowledge-based system to recommend the most suitable security countermeasures to each user based on his/her individual disposition, experience and environment.
Keyword security management, security measures, security consciousness, preference disposition, personality test

1. 背景

近年，不正アクセスやコンピュータウイルス，情報漏洩などに関する事件の多発から，企業の情報管理に対する関心が急速に高まっている．ISMS（情報セキュリティマネジメントシステム）認証を受ける組織が増加しており，今や情報マネジメントは各組織にとっての最重要課題の一つと認識されている．

その一方で，ISMS に対応した規定を設けても事故が減らず，組織内の運用に問題があることが調査によって明らかになった．例えば，Verizon Business 社が発表した企業の情報流出事件に関する実態調査報告書[1]では，情報漏洩の 87%は適切な対策を講じれば防止できたと指摘している．同時に，情報が流出した企業のうち 59%はセキュリティポリシーと手順を定めておきながら実行していなかったなどの事実も判明し，企業だけでなく情報を扱う人間の意識にも問題があることも浮き彫りとなった．これは，情報を利用する上で情報マネジメントの機能や運用だけでなく，システムを利用するユーザの人間性も考慮する必要性を裏付ける結果である．

また現在では，ネットワーク環境が整備されて様々な環境でサービスがシームレスに使えるようになった．特に携帯端末の進展に伴い，自宅や職場だけでなく移動中など場所を選ばすに様々な場所でインターネットを利用することができる．このため，安全確保のセキュリティ対策も一層重要なものになっている．

ところが，IT サービスの安全性を確保するために，サービスを利用する全てのユーザに対して一律で同じセキュリティ対策（例えば，Web ページや携帯電話におけるパスワード認証や生体認証等）が講じられていることがほとんどである．このような「サービスプロバイダから提供される一元的なセキュリティ対策」では期待される効果が得られていない可能性がある．

例えばパスワード認証に対しては，パスワードの忘却を恐れて自分の誕生日など安易なパスワードを設定しているユーザが少なくない[2]．また、ユーザの利便性を大きく損なうようなセキュリティ対策を導入してしまった場合には、サービスそのものの利用が敬遠される場合もあり得る。このように、サービスを提供する上でも、利用者であるユーザの人間性を考慮することが慣用となる。

以上のように、ユーザ個々人の性向、経験、環境に応じたセキュリティ対策を講じることは、情報マネジメントの実効的な運用管理を正しく機能させるために、また、IT サービスの利用を阻害することなく十分な安全性を確保するために極めて重要となる。そこで本研究では，ユーザの個性をも考慮した上で好適なセキュリティ対策およびセキュリティシステムを Proactive に決定するシステムの実現を目指す．

具体的には，ユーザの性向やセキュリティ意識を分析することで，一律に考えられていた情報システムの運用管理およびセキュリティ対策を，ユーザ個別に判定できると考えた．そこで，ユーザごとに着目した情報マネジメントの新しい設計指標を提案する．これにより、情報システムおよびサービスを利用するユーザ像に合わせて、最も好適なセキュリティソリューションを事前に決定することができるようになると期待される。

2. セキュリティ対策の実効度の判定

2.1. コンセプト

例えば，面倒くさがり屋や利便性を最優先する人は，必要最低限のセキュリティ対策以外は設定を無効にしていると推測される．また，過去に携帯電話の紛失などの失敗や苦い経験を持つユーザや，もともと心配性のユーザは，不安を解消するために使いづらいが厳重なセキュリティ対策を施しているだろう．このように，本人の好みや気質、各個人が持つ経験に伴う行動や思考などによって特徴づけられる性向（類型的な性質の傾向）に応じ，ユーザが各セキュリティ対策の強度をどの程度に設定し，どの様に利用するかが異なると考えられる．また、システムの使用環境や扱う情報の価値からも，セキュリティ対策は影響を受けると予想される．

以上から，セキュリティ意識と性向との相関を調べてやることにより，ユーザごとの性向、経験、環境を入力することによて、当該ユーザのセキュリティ対策に対する実効度を得ることができると考えられる．これをシステムとして実装した場合の概観を図 1 に示す．

本システムでは，ユーザを類別する指標として「性向」，「経験」，「環境」の 3 つを用いる．また，ユーザの安全性への関心度や各セキュリティ対策の嗜好を客観的に表す指標として「セキュリティ意識」を用いる．これらの指標に関しては質問紙等をユーザに実施することでデータを収集する．相関 DB は，性向，経験，環境とセキュリティ意識との間の相関（例えば，「几帳面な人はパスワードを適切に管理する傾向にある」，「大雑把な人はパスワードを覚えるより持ち物認証を好む傾向にある」など）に関する知識を集約し，これをデータベース化したものである．

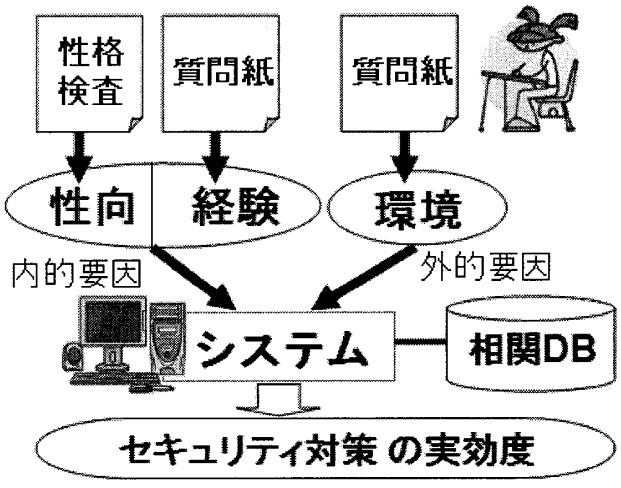

図 1. 提案システムの概観

システムは，性格検査や質問紙などを用いユーザの情報（性向，経験，環境）を受け取り，相関 DB と照合・分析を行うことによって，ユーザ個人の各セキュリティ対策における実効度を提示する．ここで実効度とは，例えばパスワード認証においては，乱数性の高いパスワードを設定しているか、十分な長さのパスワードを設定しているか、定期的にパスワードを更新しているかなどの、それぞれのセキュリティ対策をユーザがどの程度正しく運用しているか／運用できると予想されるかを示す度合いである．

セキュリティ対策の実効度を考慮することで，ユー

ザのニーズや嗜好に合致したセキュリティ対策を決定することができると考えられる．すなわち，ユーザごとに最も高い実効度が望めるセキュリティ対策を見つけて採用してやることにより、ユーザが不便を感じてセキュリティ設定をオフにしたり，セキュリティ機能を不適切に運用したりするという「セキュリティ対策における理想と現実の乖離」が抑えられ，IT社会のセキュリティレベルが底上げされると期待できる．

2.2. 相関 DB

本研究では，ユーザを内的要因（性向，経験）および外的要因（環境）に着目して類別する．相関 DB の構築に対しては，事前に多数のユーザに対して性向，経験，環境とセキュリティ意識に関する大規模な調査を行い，そこから要因間の相関関係を抽出し，これを体系化する．以下に，性向，経験，環境，セキュリティ意識に関して説明する．

【性向】 性向は，神経質，のんき等，様々な要因から構成されていると考えられている[3]．性向を構成する要因それぞれの影響力は個人ごとに異なり，それによって個性が形成されていると考えられる[4]．ユーザの性向は性格検査によって調査する．

【経験】 本研究では，過去の体験から現在の自分自身に生かされている教訓，サービスに対するアプリケーションの習熟度（例：タイピング）等を経験として定義する．似通った性向を持つ者同士でも，対象（サービス）によって経験が異なるため，安全性への関心が変わってくると予想される．ユーザの経験は，ユーザにアンケートを実施することにより回答を得る．

【環境】 サービスを受ける場所，利用限度金額，保障の有無等がこれに該当する．ユーザの置かれた状況が安全か危険か，脅威が発生した際の被害の大きさ等によって心理的不安が変化し，ユーザの安全性への関心が変動すると考えられる．ユーザの環境は，そのサービスを利用するにあたっての利用形態をユーザに回答してもらうことによって調査する．

【セキュリティ意識】 ユーザ各個人における安全性への関心や各セキュリティ対策の嗜好と定義する．普段何文字のパスワードを利用しているか，利便性と安全性のどちらに重きを置いているか，生体認証の利用（生体情報の登録）に抵抗がないか，などの質問を通じてユーザから収集する．

2.3. 性向からのセキュリティ実効度の導出

本システムでは、まず、内的・外的要因とセキュリティ意識の相関 DB を作成する．相関 DB が一旦構築できてしまえば、後は、ユーザの性向、経験、環境を提案システムに入力すれば、相関 DB の知識を利用して、当該ユーザの各種セキュリティ対策に対する実効度を計算することが可能である。

ここで、ユーザの性向を入力するにあたり，直接的な質問を用いないことは心理学において注意すべきである[5]．なぜなら，人間にはどうしても自己弁護，虚栄，同調の気持ちがあるため，直接的な質問をした場合にはそれらによって回答が歪められてしまうからである．これを実験者効果（ピグマリオン効果）と呼ぶ[6]．また，自分自身で気が付いていない心理もあり，直接的な質問からは計り知ることができない．すなわち、本システムを構築するにおいては、各種セキュリティ対策に対する実効度をユーザから直接ヒヤリングすることは得策ではない。以上のことから、本システムでは、ユーザの性向を性格検査によって取得し、これを相関 DB と照らし合わせて分析することによって、当該ユーザの各種セキュリティ対策に対する実効度を計算する．

性格検査（人格テスト）は，人格という人間の基本的な行動傾向を推測する手段のひとつである．人格を正しく診断することは極めて難しく，古くから多種多様の方法が工夫されてきた．具体的には，質問紙法，投影法，作業法などの種類が存在する。その中で本システムでは質問紙法を採用した．質問紙法は，診断しようとする人格の特性や構成要因に基づく具体的行動例によって質問項目群を設定し，それに対する回答を求める方法である[7]．

実際に性格検査を実社会に取り入れた例として，企業の入社試験に使われる適性検査，自動車教習所で用いられる OD 式安全性テストの一部などがある．これらの試験は，普段から自分で意識することのない行動傾向を測ることができることから，自己を見つめ直したり，事故に繋がる危険を回避したりするための手段として利用されている．

本システムにおいても，性格特性とセキュリティ意識の相関からユーザの特徴を診断することで，セキュリティに関してユーザが自分自身では普段気付かなかった一面を指摘できると考えている．また、本システムによって、セキュリティ対策の運用時に起こしやすいミスをユーザに指摘することができれば，利用する以前からユーザが自分自身の行動に注意を向けることも可能となる．

実用的な情報システム・サービスの開発を目指す研究の中で，本研究のようにシステムやサービスを実際に利用する人間に焦点を当てた研究は少なく，今後も必要不可欠な発展すべき課題であると考える．

2.4. 情報システムの Proactive な設計

相関 DB は，「どのような性向，経験，環境」のユーザが「どのようなセキュリティ対策」を「どのように感じ」，「どのように使用しているのか」という知識のデータベースである．また，これを分析することにより，ユーザのタイプごとに間違いやすい失敗や陥りやすいトラブルを類型化することもできるだろう．

この相関 DB を利用して、情報マネジメントを実施するにあたっての Proactive な評価システムを構築できると考える．具体的な手順は以下の通りである．

(1) ユーザは，あるサービスの利用を開始する前に，本システムに自分の性向や経験，そのサービスの環境（利用形態）をシステムに入力する．

(2) システムは，相関 DB を利用することで，そのようなタイプのユーザが各セキュリティ対策においてどの程度の実効度となる傾向にあるのか知ることができる．

(3) システムは，(2)の結果から、そのユーザに好適なセキュリティ対策の組合せ（最も実効度が高くなるセキュリティ対策の組合せ）を選定し，ユーザに提示する．

現状の情報マネジメントは PDCA のサイクルによりセキュリティレベルを継続的に改善している[8]. PDCA サイクルを正しく維持するためには，日々変化する業務に対応すべく，定期的に PLAN の見直しを行う必要がある．その際に重要となるのが、PLAN のフェーズにおける適正な手順（情報セキュリティ対策の具体的な対策）の選択である。例えば、いくら不正ユーザの侵入を排除しなければいけないという大きな要求があったとしても、「16 桁のパスワードを毎日更新する」というようなユーザが到底実施することができない手順を選択することはナンセンスである。ユーザが無理なくそれを徹底することができる手順でなければ、想定された安全レベルを達成することはできない。

ここで、本システムが効果的に機能する．PLAN のフェーズで選択された手順（情報セキュリティ対策の具体的な対策）に対し，本システムを用いて全ユーザ（例えば全社員）の実効度を計算することによって、その手順が現実的に適正に稼動するかどうかを Proactive に評価することができる（図 2)。また、PLAN のフェーズで選択された手順に対して、ユーザ（社員）一人ひとりの実効度をチェックしてやることで，ユーザごとに，どの様な問題が起こ易いか，どのようなセキュリティ対策を選択すればスクが最小限に抑えられるかなどを診断することもできる．

このように、本システムを活用してユーザの内面的な要因を評価・分析に加えることによって、従来のような機能や運用面だけを考えた情報マネジメントから，人間性をも加味した情報マネジメントの設計が可能となる。この結果，人間のミスが原因となり引き起こされる事故についてもその多くを抑制できると期待できる．

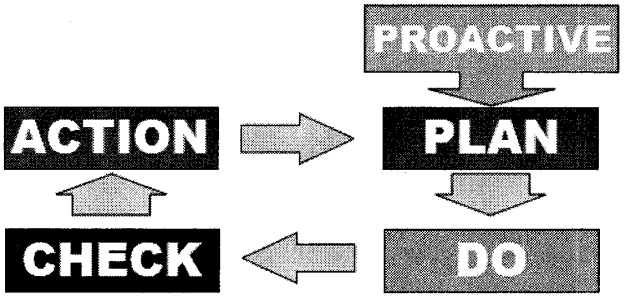

図 2. 提案方式を取り入れた PDCA サイクル

3. 提案システムを実現するための研究手順

提案システムを実現するためには，相関 DB の構築が重要である．そこで，相関 DB を実現するための具体的なプロセスを以下に述べる．なお，まずはユーザの性向にのみ焦点をあて，PIN 認証，持ち物認証，生体認証の利用に関するセキュリティ意識との相関 DB を構築していく予定である．

STEP1　被験者に性格検査を受けてもらう．

STEP2　被験者にセキュリティ意識に対する質問に回答してもらう．

STEP3　セキュリティ意識の似ている被験者に共通する性向を調べることにより，セキュリティ意識と性向の関係を分析する．

STEP1 で用いる性格検査には，柳井らが開発した新性格検査[9]を採用する．本検査は，性格の特性理論に基づき，性格の多面的特性を測定するための検査である．12 の下位尺度と 1 つの虚構性尺度を含む，社会的外向性，活動性，共感性，進取性，持久性，規律性，自己顕示性，攻撃性，非協調性，劣等感，神経質，抑うつ性，虚構性の 13 特性を，130 項目の質問（各特性 10 項目ずつ）を通じて点数化する．

STEP2 では，「持ち物認証」，「PIN 認証」，「生体認証」の 3 種類の本人認証技術に着目して調査を行う．各対策案についての意識を測るための質問紙を作成する．各認証方式に対する以下の 2 つの観点からの質問で構成する．

1）各認証方式を実際にどの程度適正に／安全に使っているか

2）各認証方式の利用に関し、どの程度の負荷（記憶負荷、利便性の低下など）を許容できるか／許容しているか

本調査では純粋な意識調査を行うために，経験や性向に起因する側面をできるだけ排除し、事実だけを淡々

と問う形のアンケートにする必要がある.

STEP3 では，STEP2 で得た被験者の回答を集計して点数化を行い，セキュリティ意識が似ている被験者ごとに分類する．この点数が「各対策案に関してどの程度のセキュリティ意識を持っているか」を表す指標、すなわち実効度である．そして、これによって分類された被験者群ごとに，STEP1 により得られた 13 の性向特性に対するグループ内の平均値と分散値を比較することにより，「どういうタイプの被験者」が「どういうセキュリティ意識」を有しているか考察する.

4. 本システムの具体的な適用例

本システムを，実社会に適応させた例を以下に示す（図 3）.

多くの社員を抱える会社などの組織は，自社の情報資産を守るため，可能な限りのセキュリティ対策を施す．同時に，社員全員に対して高いセキュリティ意識を持って対策を守って欲しいと望む．そこで，安全性・機密性・可用性をバランス良く維持した情報マネジメントを実施する.

今、会社が自社の情報資産を調査したところ、100 万円の資産と 1000 円の資産が存在していたとする。高額な情報資産ほど「安全度」の高いユーザ認証によってアクセス制限をかけることになるが、ここでは、100 万円の資産には安全度が 45 点以上のユーザ認証が、1000 円の資産には安全度が 20 点以上のユーザ認証が適用されることが決められているとする。以下、この安全度を「必要安全度」と呼ぶことにする。

一方、各ユーザ認証方式には、ユーザが正しくこれを運用した場合（例えば、PIN 認証の場合には「推測され易い数字列を使用しない」、「3 ヶ月ごとに暗証番号を更新する」などのすべての運用ルールを適正に守った場合）の理想状態の「安全度」が指定されている。ここでは、PIN 認証の理想状態の安全度は 25 点、バイオメトリクスは 60 点、トークンは 40 点、PIN とトークンを併用した場合は 50 点、PIN とトークンの併用に加え PIN の回数制限（3 回間違えたらアカウントをロックする）も適用した場合には 70 点と定められているとする。以下、この安全度を「理想安全度」と呼ぶことにする。

既存の情報マネジメントでは、各認証方式の理想安全度だけを考えて、必要安全度以上の安全度を持つ認証方式を採用していた。しかし、実際には、すべての社員がユーザ認証に対して正しい運用をしているとは限らない。そこで、本稿で提案しているシステムを用い、各社員のそれぞれの認証方式に対する実効度を評価する。

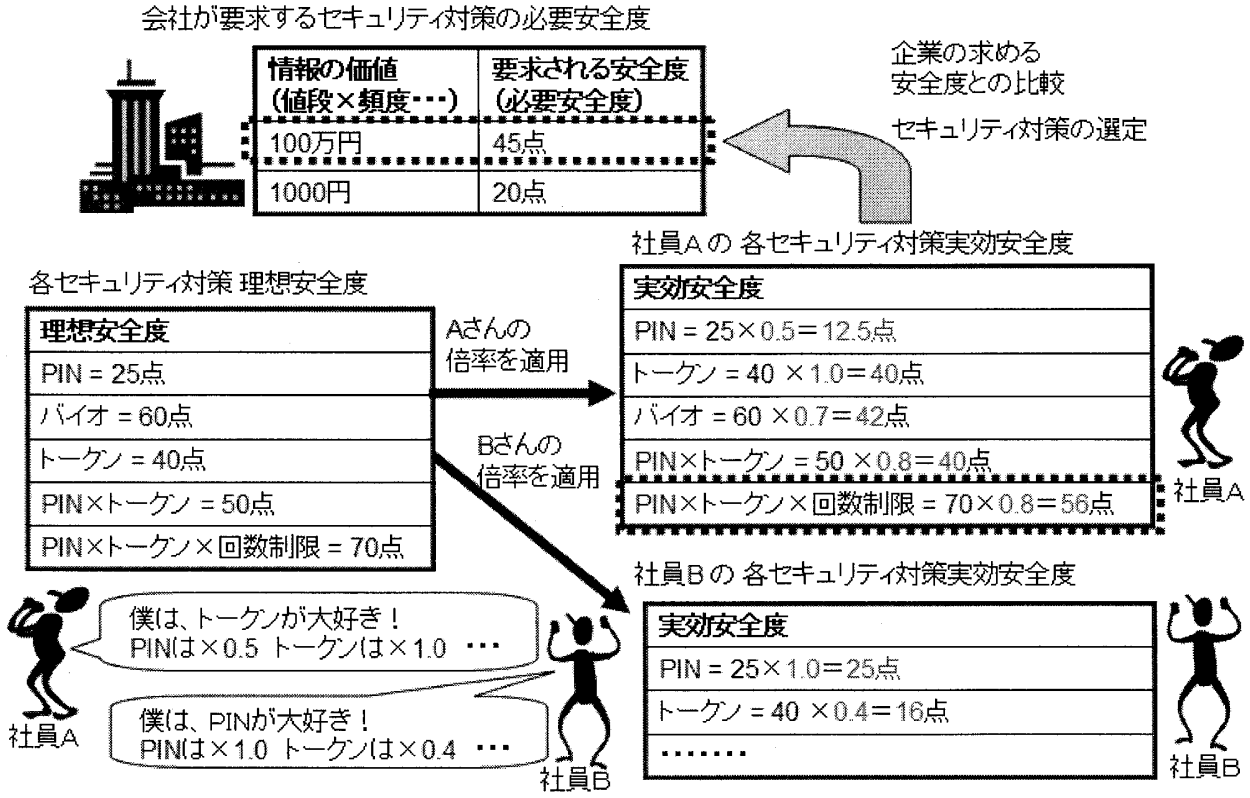

図 3. 提案方式の実用

例えば、社員 A は持ち物に対しては几帳面な性格であるが、物覚えは悪いとする。この場合、社員 A の PIN 認証に対する実効度が 0.5 であったとすると、理想安全度と実効度を乗じて実効的な安全度は 12.5 点となる。以下、この安全度を「実効安全度」と呼ぶことにする。同様に、トークン認証に対しては実効度が 1.0 であったとすると、実行安全度は理想安全度と同じ 40 点となる。一方、社員 B は PIN 認証に対する実効度が 1.0、トークン認証に対する実効度が 0.4 であったと仮定すると、それぞれの理想安全度は 25 点と 16 点となる。この結果、実際の社員一人ひとりの運用の適正度を考慮して、各認証方式の実効安全度に対して、必要安全度以上の安全度を持つ認証方式を採用することが可能となる。

会社は、守りたい資産が大きければ大きいほど，認証方式の必要安全度を大きく設定するだろう。これは、より強固なユーザ認証を社員に義務付けることになる．しかし、社員に対して否応なしに強固なユーザ認証を要求すると，例えばパスワードの場合，社員は複雑なパスワードを記憶することが出来ずメモ書きを机に貼ることになる．これは、セキュリティ対策がユーザに対して負荷を与えてしまったことによって，逆に組織が危険に晒されてしまう例である．ユーザ一人ひとりのセキュリティ対策の実効度を考慮すれば、組織はユーザに合致したセキュリティ対策を与えることができるようになるため，ユーザにとっても過負荷にならないセキュリティ対策によって、適切なレベルの安全性が確保できると期待される．

5. まとめ

本稿では，性向，経験，環境の要因を基に，個人ごとに好適なセキュリティ対策を講じるシステムの基本構成、実装方針、利用例を概観した．

本システムには，

- ユーザの特性を尊重したセキュリティ対策を導入することで，環境に応じた安全性を確保するだけでなく，ユーザにとって快適なセキュリティ対策の導入が可能であると考えられる．
- 従来の情報マネジメントにおける PDCA サイクルの中の PLAN のフェーズに，Proactive な評価を追加することができる。導入するセキュリティ対策の実効度が事前に評価できるので、サービスを運用する以前の段階でリスクを明確化することができる．
- 全ユーザに画一的なセキュリティ対策を採用しなければいけないときには、全ユーザの特性を調査して，マジョリティを占める特性に合うセキュリティ対策を選定するとユーザ全体（組織）の実効度を維持できると考えられる．
- 年代ごと・職業ごとなど，特定フィールドに属するユーザごとの特性が分かれば，企業が製品を開発する場合に，当該製品のターゲットとなるユーザ層の特性から「その製品のセキュリティ対策としては何を採用すれば消費者に受け入れられるのか」を推定することができるようになると思われる。

などの特長がある．

今後は，本システムの実装の第一段階としてユーザの性向にのみ焦点をあてて PIN 認証の利用に関するセキュリティ意識との相関 DB を構築していくことを通じ，本方式の実現可能性を検証していきたい．

謝辞

今回の研究にあたり，静岡大学情報学部 竹内勇剛准教授には本方式に関しての助言を頂いた．ここに深く謝意を表する．また，本研究は一部，（財）セコム科学技術振興財団の研究助成を受けた．

参考文献

[1] Verizon Business, 2008 Data Breach Investigations Report,http://www.verizonbusiness.com/resources/security/databreachreport.pdf.

[2] 情報処理推進機，2007 年度第 1 回情報セキュリティに関する脅威に対する意識調査報告書，http://www.ipa.go.jp/security/fy19/reports/ishiki01/documents/200701_ishiki.pdf

[3] 辻岡美延，新性格検査法 - ＹＧ性格検査・応用・研究手引き-，日本心理テスト研究所（2000）

[4] 大村政男，図解雑学 心理学，ナツメ社（1999）

[5] 日本マーケティング・リサーチ協会（編），新版マーケティング・リサーチ用語辞典，同友館（1998）

[6] 中島義明・安藤清志・子安増生・坂野雄二・繁桝算男・立花政夫・箱田裕司（編），心理学辞典，有斐閣（1999）

[7] 松原達哉（編），第 4 版心理テスト法入門～基礎知識と技術習得のために～，日本文化科学社（2005）

[8] 相戸浩志，よくわかる最新情報セキュリティ技術の基本と仕組み，秀和システム（2003）

[9] 国生理枝子，柳井晴夫，柏木繁男：プロマックス回転法による新性格検査の作成について（Ｉ）-，心理学研究，Vol.58，No.3，pp158-165（1987）