人の行動特性に基づくセキュリティ対策

Security Measures Based on Human Behavior Characteristics

● 寺田剛陽　● 片山佳則　● 鳥居　悟　● 津田　宏

あらまし

近年，組織や個人を対象に文面だけでは検知が難しい巧妙な標的型メールを送りつけて情報窃取をするといった標的型攻撃が急増している。また，メールの誤送信に代表されるヒューマンエラーや内部不正による大規模な情報漏えい事件も発生している。富士通は，メール誤送信対策として宛先の選択ミスや添付ファイルの取り違えに対して，送信時にリアルタイムに注意喚起する製品を開発した。また，標的型メールに対しても，過去のメールのヘッダー情報履歴などとの乖離（かいり）から不審な受信メールを注意喚起する製品を開発した。更に，「ウイルス感染」「詐欺被害」「情報漏えい」を経験した人の心理特性，およびパソコン操作上の行動を分析することで，ICT被害リスクの高い人の行動特性の検出技術も開発した。これらの技術により，人や組織のリスク特性に合わせた柔軟なセキュリティマネジメントが可能になると考える。

本稿では，こうした人に起因するセキュリティリスクを低減するために富士通が取り組んでいる，注意喚起型のユーザーインターフェースによる対策や，人の心理・行動分析によるリスク判定技術などを紹介する。

Abstract

Recently, the number of targeted attacks has been rapidly increasing. Those attackers limit their target to specific organizations or users and send a targeted e-mail that cannot be easily identified as being malicious. In addition, large-scale information leakage accidents have occurred due to human errors represented by missending of e-mail and internal fraud. As a measure against missending of e-mail, Fujitsu has developed a tool that warns its users about making a mistake with regards to the recipients or attachments at the time of sending. To deal with targeted e-mail, we have extended the tool that alerts users to suspicious incoming e-mail based on the difference with the header information of e-mails they have received so far. Furthermore, we have also developed a technology to detect behavioral characteristics of individuals who have vulnerability to ICT-based attacks by examining psychological characteristics and PC operation behavior of people who have experienced virus infection, fraud or information leakage. These technologies will enable flexible security management based on the risk characteristics of individuals and organizations. This paper presents our technologies that reduce users' security risks such as user interfaces that warn of e-mail missending and give alerts when there is suspicious incoming e-mail, and the risk assessment technology based on analysis of human psychological and PC operation behavior.

ま え が き

組織内の情報漏えいの大半は「人」に起因しており，セキュリティにおいても人のマネジメントはますます重要な課題となってきている。例えば，米IBM社が行った調査によると，全ての情報漏えいの47％が内部不正または悪意のある攻撃，25％がヒューマンエラー，29％がシステム脆弱性によるものとなっている。(1)

組織内部の不正による情報漏えい事件も続いており，次の個人情報保護法の改訂ではデータベース漏えい罪の導入も検討されている。また，ヒューマンエラーの代表であるメール誤送信事故は依然として新聞紙面を賑わせている。

外部からの悪意のある攻撃として近年話題になっている標的型攻撃においても，ソーシャルエンジニアリングによる偵察や巧妙な標的型メールを第一歩としてシステムに侵入した後，セキュリティ意識の低い人が狙われている。標的型メールは，顧客や関係者を巧妙に装うなど，一般ユーザーには見抜くことは難しい。したがって，標的型攻撃に対する訓練や教育によるセキュリティ意識の底上げも含めた取組みが重要である。

本稿では，こうした人に起因するセキュリティリスクの低減に向けて，注意喚起型のインターフェースによる対策や，心理・行動特性の分析技術の取組みを紹介する。

メール誤送信対策ツール

メール誤送信はヒューマンエラーの典型であり，今なお送信先のCCやBCCの取り違え事故などが続いている。メール誤送信には様々な要因がある。筆者らは社内事例を分析し，その大半の要因が宛先アドレスの選択ミスやファイルの取り違えであることが分かった。そこで，多くの人が間違えやすいパターンのメールを，メール送信時にリアルタイムに注意喚起するツールを開発した（**図-1**）。

本ツールの利用ログ約1万4000件のメールを分析したところ，取戻し率（本ツールの注意喚起によって送信を中止した割合：潜在的な誤送信確率）は約1％であった。これは，当初想定していた誤送信率より高かった。取戻しを行った対象者へのヒアリングによると，送信時にワンクッションあることで誤送信と言うほどではない書き忘れなどのミス

図-1　メール誤送信対策ツール

を思い出したというようなケースも多かった。また，午後1 ～ 3時は平均誤送信率が2％近くに上昇し，注意力が低下する時間帯であることが明らかになった。このように，本ツールを利用することで誤送信を未然に防ぐ効果があることが実証された。

一方，注意喚起型の対策ツールの欠点として，同じようなアラートが続くとユーザーが次第に慣れてしまうという問題がある。それに対して，本ツールでは人の記憶モデル（忘却曲線）に基づき，送信履歴から頻度の高い送信先を自動で学習し，頻繁に同じチェックをしなくても済むような工夫をしている。なお，本ツールは，富士通ソーシアルサイエンスラボラトリより「SHieldMailChecker誤送信対策」として販売している。[2] 富士通社内でも標準ツールとして約10万人の従業員が使用している。

標的型メール対策ツール

標的型メールでは，顧客や関係者などを装うケースが多く，一般ユーザーには文面からは見抜くことが難しい。また，通常のウイルス対策ソフトウェアでは検知できないような種類のマルウェアが用いられ，ファイル検査ツールにより検知することも難しい。更に，標的型メールの手法も，顧客を装って何回かやり取りをした後に感染させるやり取り型や，対象者がよくアクセスするWebサイトにマルウェアを仕込んでおく水飲み場攻撃など，新たな手法が次々と開発されている。

こうした不審なメールに対するユーザーの検知力を向上させ，標的型攻撃のリスクを減らすことは現実的な対策と言える。例えば，メールのヘッダーのFrom（送信元メールアドレス）を詐称したなりすましによる標的型メールは，文面上は見抜くことが難しい。しかし，メールヘッダーの特長を利用することで，ある程度ユーザーに不審なメールであることを気づかせることができる。そこで，筆者らは同一人物からの過去メールのメールヘッダーにおけるReceived，Reply-Toなどの特徴値を学習し，受信メールのヘッダーと比較することで，なりすましメールをリアルタイムに注意喚起するツールを開発した（**図-2**）。[3]

本ツールの利用者20名と非利用者33名に対して標的型メールを送信し，開封するかどうかを評価するテストを行ったところ，開封したのは本ツールの利用者は1名，非利用者は11名という結果であった。標的型メールに対しても，一定以上の注

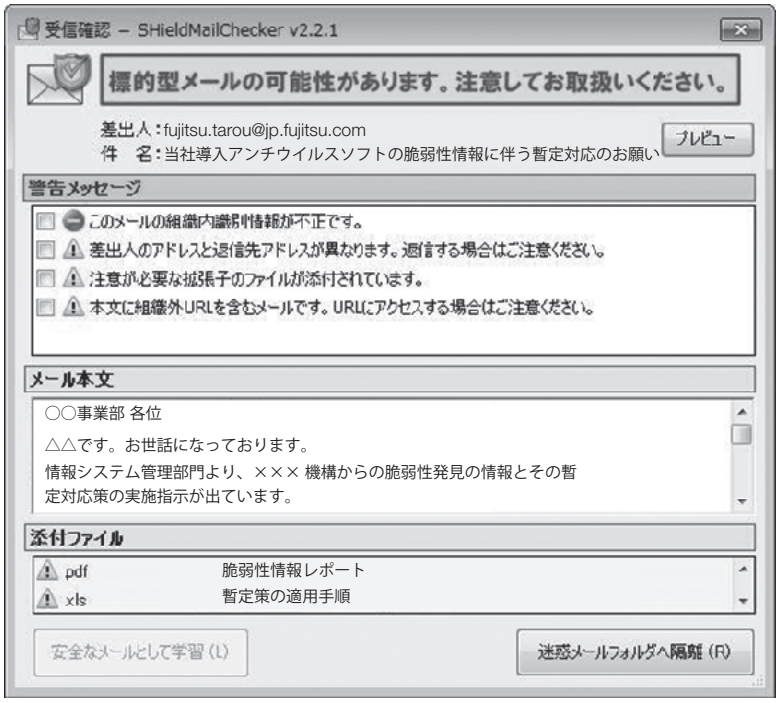

図-2　標的型メール対策ツール

意喚起の効果があると考えられる。なお，本ツールも富士通ソーシアルサイエンスラボラトリより「SHieldMailChecker標的型メール対策」として製品化されている。

ICT被害経験者の心理特性

標的型メールや不正なWebサイトへのアクセスなどによる「ウイルス感染」や，フィッシングメールなどによる金銭やアカウントの「詐欺被害」の原因は，ユーザー側にもあると考えられる。多忙のあまり，ICT管理部門が定めるセキュリティ対策を怠る，仕事を早く終わらせたくて受信メールやWebページの不審な点に気づかない，自分はパソコンやインターネットを使いこなせていると過信している，などの心理状態も原因と考えられる。前章で述べた注意喚起型のユーザーインターフェースを更に有効なものとするためには，そもそも人がなぜ情報漏えいや詐欺などの被害に遭うのかを分析する必要がある。特に，顧客情報や機密情報を意図しない相手にメールやSNSなどで公開してしまう「情報漏えい」では，ユーザー側の原因を掘り下げるべきである。

社会心理学の分野における研究によると，災害や感染症など現実世界のリスクに対する人の認知は，上述のようなユーザー側の心理状態に応じて変わることが分かっている。リスクに対する人の認知に作用する心理のこれまでの知見を以下に紹介する。

(1) コスト認知

物事のリスクを小さくする対策がある場合に，それに対して感じる心理的な負担の度合いを示す。この認知が低い人は，情報セキュリティ対策についても面倒がらずに実施すると考えられる。

(2) ベネフィット認知

物事のリスクよりもメリットを優先する度合いを示す。この認知が強い人は，不審なメールであってもその内容に興味を引かれて被害に遭いやすいと考えられる。

(3) コントローラビリティ

物事のリスクを自分でコントロールできるという認識の程度を示す。この認識が高すぎると自信過剰な心理状態であるということができ，パソコンやインターネットにおいても不用意な操作をしがちになると考えられる。

(4) 現状維持傾向

惰性で行動しようとする心理傾向を示す。この傾向が強い人は，メールやWebサイトのURLに少々怪しさを感じてもいつものようにクリックしてしまい，被害に遭いやすいと考えられる。

筆者らは，上記の従来知見を参考に「ウイルス感染」「詐欺被害」「情報漏えい」という三つのうちいずれかを過去2年以内に経験した約2000名について，特徴的な心理を調べるためアンケートを実施した。[4] 対象者は，業務の大半でパソコンを使用している日本全国のインターネットユーザーである。

三つの被害それぞれの経験者に見られた主な心理特性を**表-1**に示す。分析の結果，ベネフィット認知が強いユーザーは，ウイルス感染や詐欺被害の経験が多く，パソコンの扱いに「自信過剰」なユーザーは情報漏えいの経験が多い傾向が見られた。こうした傾向を弱める対策，例えば，ユーザーにとって身近な人たちの被害事例を周知することで，ユーザーのリスク認知は高まり，被害件数を削減できると考えている。

表-1　IT被害経験者の心理特性

特性	特性の説明	ウイルス	情報漏えい	詐欺
心理的負担が強い	セキュリティ対策がとても面倒		✓	✓
ベネフィット認知が強い	リスクが多少高くてもメリットを優先する傾向（赤信号で道路を渡るなど）	✓		✓
現状維持傾向が強い	惰性で行動する傾向（TVやネットを見続けるなど）		✓	
自信過剰である	パソコンを使いこなしているという過信		✓	
情報共有意思が低い	業務上なんらかのミスをした際に周りに相談せず自分で解決しようとする		✓	
コスト認知が高い	リスクを減らす手間を惜しむ	✓		

パソコン行動特性によるリスク判定ツール

企業内において，前章で述べた心理特性を被害からユーザーを日常的に守る用途で活用しようとすると，セキュリティ対策部門は，従業員の心理特性の危険な水準への変化をすぐに捉えるため，頻繁にアンケートを実施する必要がある。しかし，これは従業員とセキュリティ対策部門の双方にとって大変な負担である。また，心理特性は状況によって強く表れたり表れなかったりすると考えられる。例えば，急な仕事が舞い込んだり，抱えている仕事の量が多かったり，体調が良くなかったりすると，心理特性は変化すると考えられ，普段はリスクの低い人であっても，精神的な負荷が高まると被害を受けるリスクが高まる可能性がある。そこで筆者らは，心理特性とパソコン操作ログとの間の関係を調べることで，パソコン操作ログの分析から心理特性を推定することで被害リスクを判定し，リスクが高い状態になっているユーザーを検知する技術の開発を進めている。[5]

まず，心理特性とパソコンのキーボードやマウスの操作ログの関係を調べるため，開発関係者30名に対するアンケート実施とパソコン操作ログ収集を行った。分析の結果得られた傾向を基に，ユーザーが被害を受けるリスクを判定するデモツールを試作した。パソコンにインストールするアプリケーションの形態で試作し，社内複数部門の従業員221名に操作してもらった。本ツールは「あなたのITリスクを診断します」という題名で10問のアンケートに回答してもらうと同時に，回答中の操作ログを記録する。ログ取得の許可は，事前にアンケートの利用規約への同意により得た。アンケートへの回答後，主に以下の二つの結果が表示される。

(1) 利用規約画面表示中のキーボードやマウス操作

パソコン操作上の行動特性の一つとして，アプリケーションやソフトウェアの導入時に表示される利用規約をきちんと見ているかを調査するものがある。その目的のため，アンケート回答の前に利用規約画面を用意した。この画面が表示された時点からログ取得は開始されるが，「規約に同意する」ボタンを押さずに規約画面を閉じた場合はログが破棄される。次のアンケートの回答が完了すると，マウスカーソルの軌跡およびヒートマップと利用規約画面を表示していた時間が表示される。ヒートマップは利用規約の画面を格子で分割し，それまでに協力してくれた各ユーザーのマウスカーソルの軌跡の有無をマス目ごとに集計し，その頻度を色で表したものである（**図-3**）。図左上の濃いマスは，実際の画面では色は赤で表示されているが，赤に近いほどそのマスを多くのユーザーが通過したことを表す。分析の結果，利用規約をしっかり確認する人はマウスの軌跡が画面の各所にあり，画面表示時間が長い傾向が見られた一方，あまり確認しない人は画面右下に配置したアンケート開始ボタンに向かって一直線の軌跡を描き，画面表示時間が短い傾向が見られた。

(2) リスク判定結果

図-4では，3種類の被害「ウイルス感染」「詐欺被害」「情報漏えい」のそれぞれについて，取得したアンケート回答および操作ログから被害リスク値（本誌では非表示）をユーザー全体の平均値とともにレーダーチャートの形で表示している。被害リスク値の平均を業種別や職種別で比較すると，差がある傾向が見られた。

221名のアンケート回答とその回答時の操作ログ

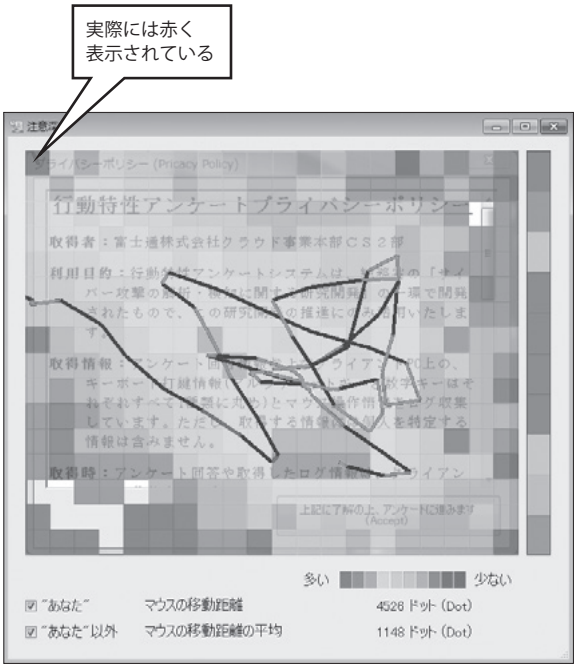

図-3　利用規約画面上のマウス軌跡

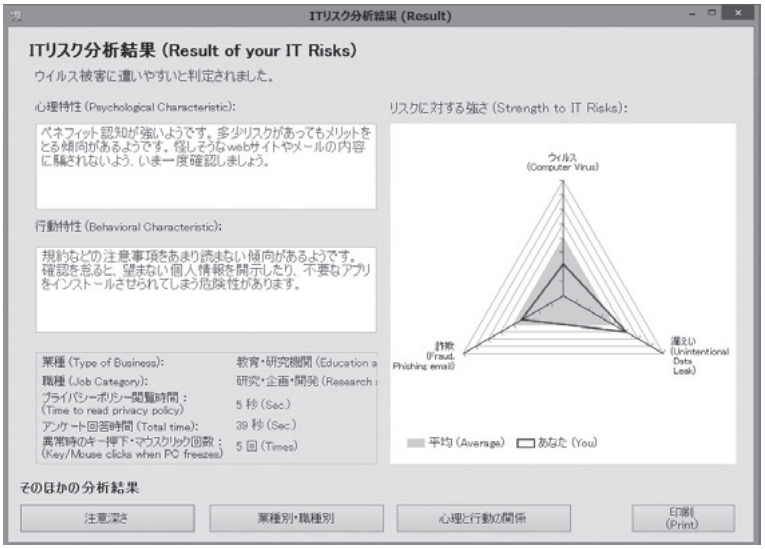

図-4　リスク判定画面

表-2　被害経験者の心理特性と行動特性の関係

		パソコン行動特性
心理特性	ベネフィット認知が強い	規約画面表示時間が短い
	リスクを避けたがる	パソコンフリーズ時のキー押下回数が少ない
	コスト認知が低い	規約画面表示時間が長い
そのほかの属性	30代	規約画面表示時間が短い
	役職あり，20代以外	パソコンフリーズ時のキー押下回数が少ない

の関係の分析結果を**表-2**に示す。ベネフィット認知やコスト認知の高い人は規約画面表示時間が短く，リスクを避けたがる人はパソコンがフリーズしたときのキー押下回数が少ない傾向が見られた。ここで，パソコンのフリーズは本ツールのアンケート回答時に一定の秒数だけキー入力を受け付けなくする仕掛けにより実現した。また，30代はほかの世代（20代，40代以降）と比べて規約をあまり読まない傾向や，役職を持つ人はパソコンフリーズ時のキー押下回数が少ない傾向が見られた。

むすび

本稿では，ヒューマンエラーや巧妙な標的型攻撃による情報セキュリティ事故を減らす富士通の取組みを紹介した。注意喚起インターフェースによるメール誤送信や標的型メール対策技術は，社内利用で一定の効果を確認し，実用化している。

上記技術の強化のため，ウイルス感染，詐欺被害，情報漏えいという3種類の被害別に，それぞれの被害経験者の心理特性を調べたアンケートを行った。その結果，ベネフィット認知の強い人，自信過剰な人は被害経験が多い傾向が見られた。また，パソコン操作ログの分析から心理特性を推定することで被害リスクが高くなっているユーザーを自動で検知する技術の取組みにおいては，ベネフィット認知・コスト認知の高さと利用規約を読む時間の短さには相関関係があることが分かった。今後，被害経験者の心理特性分析技術やパソコン行動特性による被害リスク判定技術を確立することで，ユーザーや管理部門の負担なくリスクの高い状態にあるユーザーや部門を事前に検知し，ユーザー・部門に応じた予防的な対策が可能になると考えている。

本研究の一部は，総務省委託研究「サイバー攻撃の解析・検知に関する研究開発」の成果である。

参考文献

（1）IBM，Cost of Data Breach Study，2015.

（2）竹林知善ほか：情報漏えい防止セキュリティ技術開発への取組み．FUJITSU，Vol.60，No.5，p.444-450（2009）．
http://img.jp.fujitsu.com/downloads/jp/jmag/vol60-5/paper13.pdf

（3）吉岡孝司ほか：電子メールの特徴情報を用いた標的型メールへのクライアント対策技術の提案．情報処理学会論文誌，Vol.55，No.10，p.2290-2299，Oct. 2014.

（4）寺田剛陽ほか：IT被害に遭いやすい心理的・行動的特性に関する調査．マルチメディア，分散，協調とモバイルDICOMO2014シンポジウム，情報処理学会，2014.

（5）片山佳則ほか：ユーザー行動特性分析による個人と組織のITリスク見える化の試み．SCIS（Symposium on Cryptography and Information Security）2015，4D1-3，電子通信学会，2015.

著者紹介

寺田剛陽（てらだ　たけあき）
知識情報処理研究所
データ・プライバシー保護プロジェクト兼クラウド事業本部マネージドセキュリティ事業部 所属
現在，サイバーセキュリティに関する研究開発に従事。

鳥居　悟（とりい　さとる）
知識情報処理研究所
データ・プライバシー保護プロジェクト兼クラウド事業本部マネージドセキュリティ事業部 所属
現在，サイバーセキュリティに関する研究開発に従事。

片山佳則（かたやま　よしのり）
知識情報処理研究所
プライバシー保護プロジェクト兼クラウド事業本部マネージドセキュリティ事業部 所属
現在，サイバーセキュリティに関する研究開発に従事。

津田　宏（つだ　ひろし）
知識情報処理研究所
データ・プライバシー保護プロジェクト兼クラウド事業本部マネージドセキュリティ事業部 所属
現在，情報漏えい対策の研究開発に従事。