4H1-3

# 利用者の行動特性分析に基づくセキュリティリスク判定技術の試作

## Behavior-based anti-spoofing technology for Users Vulnerable to Cyber Attack

片山 佳則[*1] 寺田 剛陽[*1] 鳥居 悟[*1] 津田 宏[*1]
Yoshinori Katayama Takeaki Terada Satoru Torii Hiroshi Tsuda
[*1] 富士通株式会社
FUJITSU LIMITED

The technique of cyber-attack assaults are sophisticated such as target e-mail attack and a remote access Trojan (RAT) attack. To cope with these threats, countermeasure must be required from not only systems but users' risk cognition. This paper shows an approach to behavior-based anti-spoofing technology for targeted e-mail, by analyzing users' behavioral trait of operation logs in sending e-mail, such as e-mail headers, contents, key input pattern, and mouse movements.

## 1. はじめに

近年，サイバー攻撃はますます高度化している．攻撃者はメールや Web サイトなどユーザーが業務上使わざるを得ない通信手段に，標的となるユーザーの興味関心や業務内容に合わせた罠を仕掛けることで，ユーザーの心理の隙を突いて社内に侵入しようとする[1]．一方で，これまでのセキュリティ対策の状況から，ユーザーの業務内容や作業時間によりリスクも変わることもわかっている．これからのセキュリティ対策は，被害に遭いそうなユーザーを早期に検知して，人や組織に合わせたきめ細かい対策技術が必要となると考える．

我々は，IT 被害に遭うユーザーに特徴的な心理特性および行動的・環境的特性を，約 2,000 名に対するアンケート調査を元にいくつか抽出した[2]．

今回我々は，ユーザーの PC 操作ログを取得可能な，ユーザー行動ログ収集ツールを開発し，社内複数部門 221 名の協力を得て，アンケート調査で得た複数の特性と行動ログとの相関関係を分析した．今回の分析で得た知見により，従来のような画一的なセキュリティ対策ではなく，ユーザーや部門に応じた対策が可能となる．

## 2. 研究の背景と課題

IT リスクとユーザーの心理的・行動的特性との関係を調べた研究として，セキュリティ行動をとるユーザーの特性を調べた研究[3]，IT 被害経験者の心理や行動の調査研究[4]がある．

表 1 IT 被害に関連する特性情報

| 種別 | 特性 | 特性の内容 | ウイルス感染 | 情報漏洩 | 詐欺 |
|---|---|---|---|---|---|
| 心理特性 | 対策の心理的負担が強い | セキュリティ対策をやるのが面倒と感じている人 | − | ＋ | ＋ |
| | コントローラビリティがある | PC習熟度が高いと自信過剰な人 | | ＋ | |
| | ベネフィット認知が強い | リスクが多少高くても得られる利益を優先する人 | ＋ | | |
| 行動習慣 | コスト認知が低い | 規約文を面倒くさがらずにきちんと読む人 | − | | ＋ |
| | 現状維持傾向が強い | 惰性で行動することが多い人 | | ＋ | |

### 2.1 IT 被害経験者の心理特性・行動習慣

これまでの研究結果[4]による IT 被害経験者に特徴的な心理特性や行動習慣の情報を表 1 に示している．表の“－”はその特性と負の相関があること，“＋”はその特性と正の相関があることを表す．たとえば「対策の心理的負担が強い」ユーザーはウイルス感染には遭いにくい一方，プライバシ漏洩や詐欺被害には遭いやすいことを示している．

### 2.2 行動特性のポイント

上記の特性の知見を活かすには，毎回アンケートを行う必要がある．しかし，アンケートの実施は，大きな負担であり，また，仕事量等の負荷の違いや体調などユーザーの状況変化に対応できない．そこで，ユーザーの業務中の行動を PC 操作ログから観測し，アンケート調査で抽出した心理特性や行動習慣との相関関係を調べることで，ユーザーの行動ログの観測だけから IT 被害に遭う可能性が高いユーザーを検知し，対策する技術の開発を進めている（図 1）．

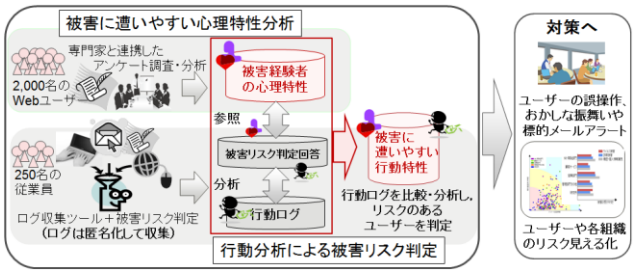


図1 ユーザー行動特性に基づくセキュリティ対策

## 3. セキュリティリスク判定技術

今回，社内の複数部門の従業員 221 名を対象に，10 問のアンケートに回答するという被害リスク判定実験を行った．本実験は，アンケート回答から「IT リスクを診断する」という体験型デモの形式をとり，協力者には，その場で診断結果を提示している．

### 3.1 被害リスク判定ツール

この体験型デモでは，アンケート回答中のユーザーの行動特性を評価するツールが連動している．本ツールは，アンケート回答データおよび回答中の PC 操作ログ（マウス，キーボード，プロセス監視等）を集計・分析して結果をユーザーに提示する機能を持っている．

### 3.2 実践

被害リスク判定において特に着目した行動は，(1)プライバシーポリシー(規約)表示中のマウスやキー操作，(2)規約確認時間，アンケート回答時間，(3)疑似的に PC の異常状態を起こした際のキーボード操作やマウス操作である．属性情報や心理要因に関する問い（普段の振舞いに関するアンケート）の回答と同

連絡先：片山佳則，富士通株式会社，神奈川県川崎市中原区上小田中 4-1-1，katayama.yoshin@jp.fujitsu.com

時にこれらの行動情報を抽出する. これにより, 心理特性と行動特性の関連を導き, 最終的に回答行動から IT 被害リスクを算出し, 被害リスク結果をフィードバックしている.

### 3.3 分析結果

被害リスク判定ツールの提供情報は, 前回研究[2]の知見をふまえた注意すべき被害リスクおよび, 心理特性と行動特性の概要と組織別の IT リスク指数の見える化情報である(図2). 今回の結果では, 営業部門の指数が他に比べて高くなっている.

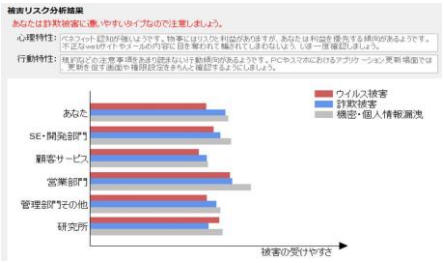


図 2 IT リスク診断結果の例

これらの結果に加えて, 以下では, 特に着目した行動に関して, 各基本属性との関係を算出した.

#### ① 規約表示中の操作について

規約の確認に関するアンケート回答と, 実際の規約表示のスクロール操作の結果は7割の人は回答と行動に整合性があり, 残り 3 割はアンケートできちんと確認すると回答していても全くスクロールしていないという関連結果である.

#### ② 処理時間の分布について

処理時間に関して, 図3が示すように, 営業部門のアンケートの処理時間が他に比べて早い傾向が出ている. 規約の参照に関しては, SE/開発や顧客管理などの部門は時間をかけている傾向が見られる.

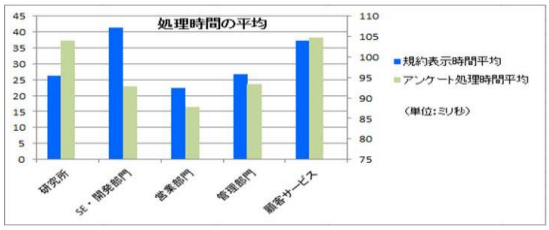


図 3 処理時間の平均値

#### ③ 疑似的な異常時の操作について

性別による異常時のマウス操作の分布には, 違いは見られない. 役職属性では, 役職ありの方がマウスクリックの比率は低く被害リスクは低い傾向と言える. 一方, キーボードの打鍵の分布に関しては, 性別でも, 役職の有無でも違いはない.

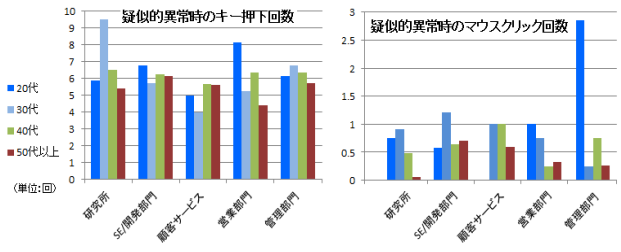


図 4 抑止時の属性ごとのキー・マウスの度数

組織と年齢の分布を見てみると, 研究所は 30 代のキーボード押下が多く, 営業部門は 20 代のキーボード押下が多いという被害リスクに関して組織と年代の傾向が出ている(図4左).

マウス操作に関しては, 管理部門の 20 代のクリック回数が多く, マウス操作の依存性と組織には傾向がありそうである(図4右).

また, 異常時のキーボードの連続打鍵, 特殊キー(Del, SP, 矢印, Enter 等)の連続打鍵など、キーの連続打鍵と, 被害リスクとの関連等も分析しているが, 特に傾向は得られていない.

### 3.4 考察

今回の被害リスク判定情報から IT リスクに関係する心理特性「ベネフィット認知の強さ」は「規約表示時間」に関係することが質問内容と実際の行動からもわかった. ベネフィット認知の強さは, アンケート調査結果からウイルス感染と正の相関がある[2]. また, 規約表示時間の短いユーザーはウイルス感染被害に遭いやすいとも関係づけられている. これらのことから, 対策への活用としては, web アクセス等における警告画面の表示時間の短いユーザーに対してウイルス感染の注意喚起を行うなどが考えられる. また, 営業部門はアンケート回答時間および規約表示時間が短い傾向にあり, ベネフィット認知が強いといえる. さらに管理部門は, コスト認知が部門全体の中で低いため, ウイルスに感染しにくいといえる. よって, 管理部門のコスト認知の低さに影響している特性を調査し, その特性を IT リスクの高い部門への対策に活かすことが考えられる. このように組織間の特性を対策に活かすことは, サイバー攻撃に対する組織全体のセキュリティの底上げにつながる.

## 4. まとめ

我々はアンケートに回答している最中の操作ログを収集・分析するための行動特性評価ツールを開発し, 体験型デモの形で社内の複数部門約 200 名に実験にご協力いただいた. この結果, IT リスクの低い部門と高い部門があること, IT リスクに関係する行動特性についての知見や基本属性との関連などを得た. 今回の知見をもとに, IT リスクに関係する行動特性を詳細化し, 行動ログの観測から被害可能性のあるユーザーを検知する技術ならびに, ユーザー特性に応じたアラートや各種の支援対策技術, 組織間の特性に基づく対策技術の開発につなげる.

### 謝辞

本稿の内容には, 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」の成果が含まれます. また, データ分析において多くの助言をいただいた東京大学の高木大資 助教に感謝いたします.

### 参考文献

[1] 情報処理推進機構, “「標的型メール攻撃」対策に向けたシステム設計ガイド”, 2013.
[2] 寺田, 津田, 片山, 鳥居,“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.
[3] 小杉, 安野, 瀧澤, “情報セキュリティ対策におけるリスク認知の影響”, 日本心理学会第 78 回大会, ポスター発表, 2014.
[4] 片山, 寺田, 鳥居, 津田, “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.