

# 人間の脆弱性を利用した標的型攻撃への防御手法の検討

八藤後 菜央<sup>†</sup> 小倉 加奈代<sup>†</sup> Bhed Bahadur Bista<sup>†</sup> 高田 豊雄<sup>†</sup>

岩手県立大学岩手県立大学ソフトウェア情報学部<sup>†</sup>

## 1 はじめに

情報システムのセキュリティホールを埋める方法は数多く考案され、ネットワークの外側からシステムの脆弱性を突破し内部に侵入する攻撃の難度は日々高くなっている。ネットワーク外からの侵入が難しくなるにつれて、攻撃者たちは機密情報を窃取するために人間のセキュリティホールを利用するようになった。例えば、2008年に悪意ある攻撃者がIPAセキュリティセンターになりすまし、マルウェアを仕掛けたファイルを添付したなりすましメールを流布した事例もある[1]。この事例では、メールの差出人が被害組織の現職職員に偽装されており、メール本文も信憑性のある文章であった。このような人間の心理や行動の脆弱性をつく巧妙な騙しのテクニックを使った攻撃手法はソーシャルエンジニアリングと呼ばれ、機密情報を引き出される危険がある。

本稿では、ソーシャルエンジニアリングを応用した標的型攻撃の新たな防御手法を検討するために、対象の心理的な特性と、対象が人間の脆弱性を狙った攻撃に人がどう対応するかをアンケートで調査した結果を報告する。また、この結果を踏まえて心理的特性と攻撃者との対話を想定した攻撃の場面で標的がとる行動の関係を分析する。

## 2 関連研究

ソーシャルエンジニアリングに関する研究はまだ少ないが、人間の心理的脆弱性をついた犯罪行為に関連する研究は多く存在する。鈴木らの研究報告[2]では、人間の脆弱性を利用した振り込め詐欺について分析し、物事を経験に基づき一般化しようとする認知的構造欲求の高い群は振り込め詐欺の被害を受けやすいことを示した。この傾向は詐欺と同じように人間の心理的脆弱性を利用するソーシャルエンジニアリングにも適用できると考えられる。

## 3 調査手法

本調査では著者の所属する学部学生113名を対象にアンケートを実施した。以下より各設問について説明する。

### 3.1 設問1:人間の脆弱性を狙った攻撃への対応

本設問では、日常で人間の脆弱性を狙った攻撃が行われた場合、どのように対応するかを調査する。今回、ハドナジーが人間の脆弱性としてあげる「返礼」、「義務感」、「譲歩」、「希少性」、「権威」、「言質と一貫性」、「好意」、「コンセンサスもしくは社会的証明」の8点[3]を取り上げる。8つの脆弱性それぞれを利用した攻撃シナリオを作成し、攻撃に対しどのように行動するかを回答者は、選択肢から1つ選択し回答する。なお、「返礼」、「義務感」、「譲歩」に関しては、組み合わせることでさらに効果的に使用できるため、1つのシナリオとして作成した。

### 3.2 設問2:回答者の心理的特性

本設問では、認知的構造欲求尺度と認知欲求尺度を利用した。2章で述べたように、認知的構造欲求はソーシャルエンジニアリングにも関連性が見られると予測されるため調査に利用する。さらに、努力を要する認知活動に参加し、それを楽しむ内発的な傾向を調査する認知欲求尺度も合わせて利用する。

認知的構造欲求尺度についての項目は鈴木ら[4]の項目を用いる。この尺度は「構造に対する願望」と「構造欠如に対する反応」という2つの因子を持つ。尺度は10項目から構成され、「非常に当てはまる」から「非常に当てはまらない」までの6段階評定で、得点が高いほど認知的構造欲求が高いことを示す。

認知欲求尺度に関する質問項目は、神山ら[5]の項目を用いる。尺度は15項目から構成され、「非常に当てはまる」から「非常に当てはまらない」の7段階評定で、得点が高いほど認知欲求が高いことを示す。

## 4 結果

設問1の回答を攻撃シナリオごとに攻撃者の期待する行動を行う場合、行わない場合に分け、認知的構造欲求尺度、認知欲求尺度とt検定を行った。その結果、「返礼、義務感、譲歩」、

「希少性」, 「コンセンサスもしくは社会的証明」を利用した3つのシナリオにおいて5%の有意水準で「攻撃者の期待する行動を行うことに心理特性的な差はない」という帰無仮説が棄却された. 有意差が認められた3つの脆弱性についてさらに分析を行った.

#### 4.1 認知的構造欲求と有意差のあるシナリオ

「希少性」は認知的構造欲求尺度の構造欠如に対する反応項目とのt検定において有意差が認められた.

鈴木ら[4]より認知的構造欲求の構造欠如に対する反応の得点平均3.45より高い得点回答者を構造欠如に対する反応が強い, 低い得点回答者を反応が弱いとする. 回答結果を表1に表す. なお, 表1の比率は, 攻撃者の期待する行動を選択した人の割合を表す.

表1. 「希少性」のシナリオに対する回答

	期待する行動を		比率(%)
	行う	行わない	
構造欠如に対する反応が強い	34	24	58.62
構造欠如に対する反応が弱い	27	28	49.09
合計	113		

構造欠如に対する反応が強い人は構造欠如に対する反応が弱い人と比較してその攻撃を回避できない可能性がやや高い傾向にある.

#### 4.2. 認知欲求尺度と有意差のあるシナリオ

「返礼, 義務感, 譲歩」, 「コンセンサスもしくは社会的証明」は認知欲求尺度に有意差が認められた. 神山ら[5]より認知欲求尺度の得点平均4.33より高い回答者を認知欲求が高い, 低い回答者を認知欲求が低いとする. 回答結果を表2, 表3に示す. なお, 比率は, 表1同様に, 攻撃者の期待する行動を選択した人の割合を表す.

表2. 「返礼, 義務感, 譲歩」のシナリオに対する回答

	期待する行動を		比率(%)
	行う	行わない	
認知欲求が高い	33	2	94.29
認知欲求が低い	64	14	82.05
合計	113		

表3. 「コンセンサスもしくは社会的証明」のシナリオに対する回答

	期待する行動を		比率(%)
	行う	行わない	
認知欲求が高い	22	13	62.86
認知欲求が低い	35	43	44.87
合計	113		

「返礼, 義務感, 譲歩」のシナリオでは, 全体的に攻撃者の期待する行動を選択する回答者が多かった. 中でも認知欲求が高い回答者は認知欲求の低い回答者と比較して攻撃を回避できない傾向にあると予想できる.

「コンセンサスもしくは社会的証明」のシナリオでは, 認知欲求が高い人の方が攻撃者の要求に従う人が多い傾向にあることがわかった.

認知欲求の高い人は物事に関して考えて行動

することを好むタイプいえるが, その物事の危険性にまで思考が向かないと, 攻撃者に心理的な脆弱性を逆に利用される恐れがある.

## 5 まとめと課題

本稿ではソーシャルエンジニアリング攻撃を受けたとき, その標的はどのような行動をとるか, また心理的特性により行動傾向に差はあるかを調査した. 結果として, 認知的構造欲求や認知欲求の高い人は低い人と比較すると, 「返礼, 義務感, 譲歩」, 「希少性」, 「コンセンサスもしくは社会的証明」の心理的脆弱性を利用した攻撃を回避しにくい傾向にあることがわかった. 大切な情報を守るためには, それぞれの心理的特性に合わせて攻撃の危険性を意識させる必要がある.

今回のアンケート調査では全ての間を合わせて攻撃者の期待する行動を選択した回答者は全体の約64%という結果であった. 回答者が大学生のみであったため, 他の年代, 属性においても調査を行うことでさらに正確な分析を行う必要がある. また, 今回はアンケート形式だったため一部回答に客観性がみられた. 今後は回答の主観性についても考慮したい.

謝辞 本研究はJSPS科研費16K01025の助成をうけたものである.

### 参考文献

- [1] 独立行政法人情報処理推進機構セキュリティセンター: ソーシャル・エンジニアリングを巧みに利用した攻撃の分析と対策—脆弱性を狙った脅威の分析と対策について— (2009年2月6日), (オンライン) 入手先 <<http://www.ipa.go.jp/files/000017739.pdf>> (参照2017-01-12)
- [2] 鈴木護: 恐怖喚起アピールの視点による振り込め詐欺の被害過程及び被害防止対策に関する研究, 2009年度~2010年度科学研究費補助金若手研究(B)研究成果報告書(2012), (オンライン) 入手先 <<https://kaken.nii.ac.jp/ja/file/KAKENHI-PROJECT-21730510/21730510seika.pdf>> (参照2017-01-12)
- [3] Hadnagy, C. (著), 成田光彰 (訳): ソーシャル・エンジニアリング, pp. 206-231, 日経BP社 (2012)
- [4] 鈴木公基, 認知的構造欲求尺度の試み, 筑波大学心理学研究, 第21号, pp. 135-149 (1999)
- [5] 神山貴弥, 藤原武弘: 認知欲求尺度に関する基礎的研究, 社会心理学研究, 6(3), pp. 184-192 (1991)