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

2008－CSEC－41 (13)
2008／5／23

ソーシャルエンジニアリングの実例分析による被害過程モデルの提案

沼田 晋作† 荒金 陽助†1 柴田 賢介† 神谷 造† 佐野 和利† 金井 敦†2
† 日本電信電話株式会社 NTT 情報流通プラットフォーム研究所

概要 重要情報を不正に取得するための手法は，なりすましやハッキングなど多くの手法が存在する．本論は，ソーシャルエンジニアリングの具体的な実例を分析し，人が演じる「ロール（役）」とそのロールによって取得できる「情報」によって，ソーシャルエンジニアリングのモデル表現を試みる．そして，得られたモデルによって説明が可能な実例を示し，説明が困難である実例を課題として述べる．
キーワード ソーシャルエンジニアリング, モデル化, 情報セキュリティ

The proposal of the damage process model by analysis of Social Engineering example

Shinsaku Numata† Yosuke Aragane† Kensuke Shibata† Itaru Kamiya† Kazutoshi Sano† Atsushi Kanai†
† NTT Information Sharing Platform Laboratories, NTT Coporation

Abstract The technique to acquire the critical information illegally has a lot of techniques like hacking and the disguise, etc. The main discourse analyzes a concrete example of the social engineering, and tries modeling by "Information" that can be acquired by "Role (posision)" that the person performs and the role. And the model explain some of the techniques of social engineering, but it could not explain some of the techniques of social engineering.
Keywords Social Engineering, Modeling, Information Security

1 はじめに

企業の重要情報を格納する手段としてＩＴシステムが普及するにつれて，それらの重要情報を不正に入手しようと，企業のＩＴシステムに対して，様々な手法を用いた攻撃が行われている [1]．それらの攻撃手法の中には，システムを構成するソフトウェアの脆弱性を攻撃する手法と，システムを使用する人間の脆弱性を攻撃する手法が存在する．

前者をシステム攻撃と呼称すると，システム攻撃ではその対象となる脆弱性を持つ箇所が特定可能であり，その脆弱性への攻撃方法とその効果を一意に記述できるため，対策や検知が行いやすく，企業は様々な対策を施すことが可能である．

一方で，後者をソーシャルエンジニアリング攻撃と呼称すると，ソーシャルエンジニアリング攻撃は攻撃対象の脆弱性を持つ箇所も，また，脆弱性への攻撃方法とその効果についても一意に記述することが難しく，検知や対策が行いにくい．

ソーシャルエンジニアリング攻撃への対策として，矢竹らがアクセス制御の提案 [2] を行っている．同提案は，ユーザのロールのレベルやアクセス対象となる情報の区分をより明確かつ詳細に定義し，アクセス制御を厳しくすることで，情報の不正入手への対策としている．

本研究では，ソーシャルエンジニアリング攻撃をモデル表現により視覚的に表現することで，その検知と対策を行いやすくすることを目的としている．本稿では，そのためのソーシャルエンジニアリング攻撃のモデル表現の提案と，提案するモデルの課題点について述べる．まず，2 章にてモデル表現のための要素となる軸について述べ，3 章にてその軸を使用したモデル表現を提案する．4 章にてモデルの課題点を述べ，最後に 5 章で今後の課題を述べる．

2 実例分析から導かれた２つの要素とその関係

我々は，文献 [3] より実例を取り上げ分析することにより，攻撃者が用いた攻撃内容をモデル表現するための，軸となる要素や，それら要素の関係について検討を行った．

分析の結果，多くのソーシャルエンジニアリング攻撃において，攻撃者はなりすまし行為を多用していることがわかった．攻撃者はなりすましにより，ロール（役割，役職，権限）

[1]現所属は東日本電信電話株式会社
[2]現所属は法政大学

を取得し，そのロールにとって得ることが容易な範囲で，情報の入手を行っていること，さらに，得た情報を再利用し，それらの情報でなりすますことが可能な，更に高いロールになりすましていることが分かった．

また，攻撃者は目的の情報に性急にたどり着くのではなく，小刻みにロールや情報をステップアップさせ，最終目的の情報を入手している事も分かった．

これらの分析の結果より，我々はソーシャルエンジニアリングとは,「ロール」と「情報」の細かな積み重ねにより，大きな情報へたどり着くものと考えた．

そこで，ソーシャルエンジニアリング攻撃の攻撃手法を記述するための軸とその関係について以下のような仮説を立て，これらの仮説の下，ソーシャルエンジニアリング攻撃のモデル表現を試みることとした．

- ロールとは課長や部長などの役職や，客，家主などのように金銭や権力を持つ人などのような，人の持つ権限の事である
- 情報とは，電話番号やフルネームのような識別子や，パスワードやIDカードのような何かへのアクセスを行うために必要となる鍵などの事柄である
- ロールと情報の間には「尤度」が存在し，あるロールには「ふさわしい情報（＝そのロールで手に入れることができる情報）」と「ふさわしくない情報（＝そのロールで手に入れることができない情報）」があり，ある情報には「ふさわしいロール（＝その情報でなりすませるロール）」と「ふさわしくないロール（＝その情報でなりすませないロール）」が存在する[3]．

3 モデル表現

3.1 階段モデル

2章で述べたように，我々は「ロール」と「情報」および，その2つの要素の「尤度」がソーシャルエンジニアリング攻撃をモデル表現する際に有用であると考え，それら2軸によるモデルを考案した．

このモデルを図1に示す．図1にて表されるモデルを階段モデルと呼称する．このモデルにおいて，横軸は「ロール」を示しており，縦軸は「情報」を示している．斜めの直線は「尤度」を示しており，この直線をロールと情報の均衡直線と呼称する．

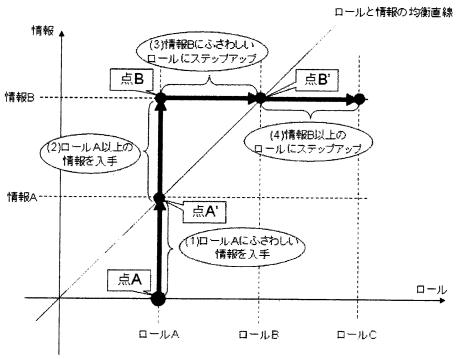

図 1: 階段モデル

この均衡直線に"近付く/離れる"と"上方向/右方向"の組み合わせで表現される4つの矢印で，ソーシャルエンジニアリング攻撃のモデル表現を行う．

例えば，図1中 (1) 点Aから均衡直線に近付く上方向の矢印で示すものは，ロールAにふさわしい情報Aの入手である．そして，同様ににて点A'から均衡直線から離れる上方向の矢印で示すものは (図1中 (2))，ロールにふさわしくない情報Bの入手である．次に，点Bから均衡直線に近付く右方向の矢印で示すものは (図1中 (3))，情報Bにふさわしいロール B へのなりすましである．最後に点B'から均衡直線から離れる右方向の矢印で示すものは (図1中 (4))，情報Bにふさわしくないロール C へのなりすましである．

この階段モデルを用いて,「昨日お店を訪れた客を装い，店員のフルネームと店頭にいる時間を聞き出す」というソーシャルエンジニアリング攻撃の実例を，階段モデルにてモデル表現する．図2にてその表現を示し，図中の各ステップの内容を以下で説明する[4]．

(1) 攻撃者は，店頭に電話をかけ,「昨日店に行った客」であることを告げ「誰かと話をして，買うことになったら電話をすることになっていた」と告げる (→)

(2) 店員は「だれでしょう？ウィリアムかな？」と，めぼしい名前をあげる (↑)

(3) 攻撃者は「そうかもしれないな」と応える (→)

(4) 攻撃者は,「どんな体型の人？」と聞く (→)

(5) 店員は，ウィリアムの体型を告げる (↑)

[3]例えば「内線番号からの電話」という情報は,「内部の人間」というロールになりすますのにふさわしく,「内部の人間」というロールでは「この電話番号の所属部署」という情報を手に入れるのにふさわしいロールである，など

[4]この例は，店員になりすまして安く携帯電話の端末を手に入れるソーシャルエンジニアリング攻撃の一部を抜き出したものである．店員になりすます際に必要な，なりすます相手のフルネームと，実際に本人が店頭にいない時間帯を聞き出すことが目的である．

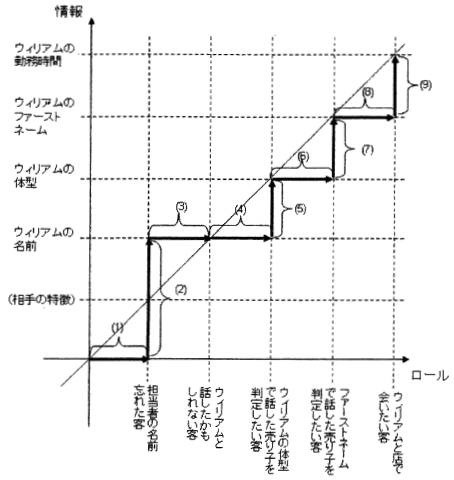

図 2: 階段モデルを用いた表現

(6) 攻撃者は，体型では分からないため，ファーストネームを尋ねる (→)

(7) 店員は，ウィリアムのファーストネームを告げる (↑)

(8) 攻撃者は，話した相手がウィリアムであったことを告げ，ウィリアムの勤務時間を訪ねる (→)

(9) 店員は，ウィリアムの勤務時間を告げる (↑)

図 2 のようにして，攻撃者は徐々にロールをステップアップすることで，取得を目的としていた「実在する店員のフルネーム」と「その店員の勤務時間」という情報を得ることができている事が分かる．

このように，階段モデルを使用し，ソーシャルエンジニアリング攻撃における，ロールや情報のステップアップを表現することが出来た．しかし，階段モデルでは，ステップアップの発生原因を表現できていない．例えば (1)，(4) の様に，攻撃者は，情報にふさわしくないロールへとロールをステップアップさせている．そがどのようにして行われたのか，なぜロールをステップアップさせても店員は不審に思わなかったのか，その原因が表現できていない．

この点について検討した結果，階段モデルの縦軸で表現されている「情報」は加害者が入手した情報のみが記述されており，図 2 において (1) や (4) のように，ロールをステップアップさせる際に，加害者が被害者に提示した情報は記述されていないことが分かった．

つまり，階段モデルでは，加害者の視点と被害者の視点を分けて記述しておらず，このために「情報」の軸も加害者の視点である「加害者が入手した情報」のみが記述されており，このことが先の課題の原因になっているのではないかと考えた．

そこで次に，情報とロールそれぞれについて，攻撃者と被害者の視点から記述したモデルを考案した．

3.2 被害過程モデル

3.1 節にて，ソーシャルエンジニアリング攻撃による情報の不正入手を階段モデルにより表現することを試みたが，階段モデルでは説明し切れていない点が存在した．そして，その原因は攻撃者と被害者の視点を分けて記述していないことであると考えた．そこで，それまで 2 軸 1 象限で表現されていた階段モデルに対し，4 軸 4 象限に拡大したモデルを考案し，被害過程モデルと呼称した．

被害過程モデルにおいては，ロールと情報について以下のように再度仮説を立て，それぞれをモデル表現に使用する軸とした．

- 被害者が認識するロールとは，被害者が加害者により提示された情報やロールを受けて認識するロールである
- 被害者が提供する情報とは，被害者が認識したロールや情報を元に被害者から加害者に提供を行う情報である
- 加害者が提供する情報とは，被害者より得た情報などを元に加害者が被害者に提供する情報である
- 加害者が提示するロールとは，加害者が提示する情報を元に加害者がなりすますロールである

次に，それぞれの軸を使用して以下のように 4 象限を表現し，被害過程モデルとした．被害過程モデルを図 3 に示す．

- 第 1 象限で，被害者が認識したロールと被害者が提供する情報の尤度を表現する
- 第 2 象限で，被害者が提供する情報とその情報を用いて加害者が提供する情報を表現する
- 第 3 象限で，加害者が提供する情報と加害者がなりすますロールの尤度を表現する
- 第 4 象限で，加害者が提示するロールとそれを元に被害者が認識するロールを表現する

被害過程モデルの 4 つの象限において，均衡直線を超える矢印（ステップアップ）が何を表現しているかを説明する．

第 1 象限においては被害者が「相手にこの情報を教えてはいけないと思うが，教えている」ことを示す．これは恐喝・買収などの手法が考えられる (図 3 中 (a))．次に，第 2 象限では，加害者が被害者から得た情報に新たに情報が付加され

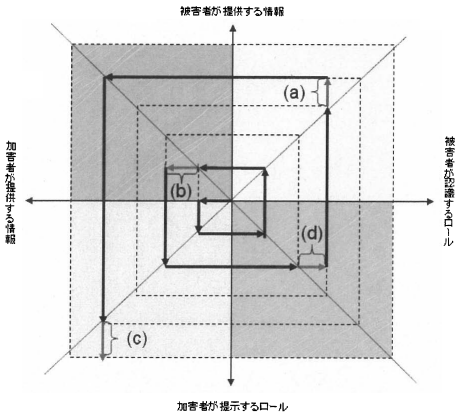

図 3: 被害過程モデルを用いた表現

たことを示している (図 3 中 (b)). 第 3 象限では，加害者が情報にふさわしくないロールになりすますことを示している (図 3 中 (c)). これは実例分析では余り見ることができなかった. 第 4 象限では，加害者が提示したロールを被害者が過大に解釈してしまうようことを示している (図 3 中 (d)).

このように，被害過程モデルでは，どの象限において均衡直線を越えたかによって，攻撃者の攻撃方法を表現することが可能である.

この被害過程モデルを使用して，3.1 節にて取り上げた実例のモデル表現を行い，図 4 に示す. 以下に図 4 における各ステップの内容を記述する.

(1) 加害者は被害者（店員）に昨日店に行ったという情報を提示し，昨日店に行った客というロールを提示する

(2) 被害者は加害者が提示したロールを受け入れる

(3) 加害者は被害者に昨日店で話した店員の名前が思い出せないという情報を付け加えて提示し，店員の名前を忘れた客というロールを提示する

(4) 被害者は加害者が提示したロールを受け入れる

(5) 被害者は加害者の提示したロールにふさわしい情報として，店員の名前を提供する

(6) 加害者は提供された情報に，体型が分かれば誰か分かるという情報を付け加えて提示し，体型が分かればどの店員と話したか分かる客というロールを提示する

(7) 被害者は加害者が提示したロールを受け入れ，ロールにふさわしい情報として体型の情報を提供する

(8) 加害者は提供された情報に，ラストネームが分かればどの店員と話したのか分かるという情報を付け加えて提示し，ラストネームが分かればどの店員と話したのか分かる客というロールを提示する

(9) 被害者は加害者の提示したロールを受け入れ，ロールにふさわしい情報としてラストネームの情報を提供する

(10) 加害者は提供された情報に，自分が話した相手がウィリアムであるという情報を付けて提示し，ウィリアムと話した客であるというロールを提示する

(11) 被害者は加害者の提示したロールを受け入れる

(12) 被害者はウィリアムの勤務時間を知りたいという情報を提示し，ウィリアムの予定を知りたがっている客というロールを提示する

(13) 被害者は加害者の提示したロールを受け入れ，ロールにふさわしい情報としてウィリアムの勤務時間という情報を提供する

階段モデルとの差異として，ロールと情報がそれぞれ加害者と被害者の両面から記述されている. また，被害者の認識したロールを加え，この被害者が認識したロールに対しふさわしい情報をプロットできる.

これにより，階段モデルでは被害者はロール以上の情報を提供したように見えたが，それは被害者の認識したロールからするとふさわしい情報であり，加害者による情報のステップアップが，そのロールになりすます要因であることがわかった.

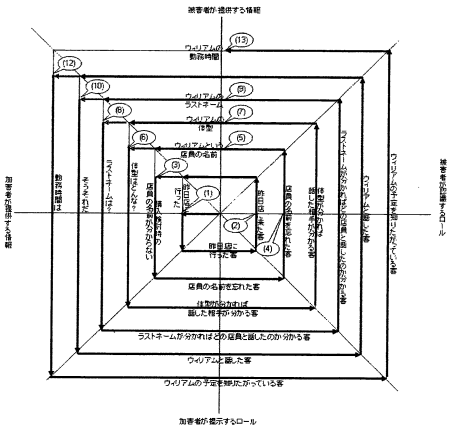

図 4: 被害過程モデルでの表現

3.3 モデル表現のまとめ

本章では，実例の分析から導かれたロールと情報という 2 軸によって，ソーシャルエンジニアリング攻撃をモデル表現することを試みた．

当初考えていた 2 軸の情報での表現である階段モデルは，ロールと情報の間の尤度を用いてソーシャルエンジニアリング攻撃を表現するモデルである．階段モデルは，ロールや情報のステップアップの発生原因について正確に表現できていなかった．

この原因を，ソーシャルエンジニアリングに関係している加害者と被害者の 2 者の視点を分けて記述していないため，ではないかと考え，それら加害者と被害者の視点でロールと情報を分けて記述するモデルとして，被害過程モデルを考案した．

被害過程モデルを使用した実例の表現では，加害者がどの様な順序でロールや情報を利用した攻撃を仕掛け，どの様にロールや情報のステップアップさせたのかを，4 つの象限において表現することが可能になった．

これにより，ソーシャルエンジニアリング攻撃において，これまで明確に表現することができなかった加害者の用いた攻撃を視覚的に表現することが可能となった．

4 被害過程モデルの課題

これまでの節で，ソーシャルエンジニアリング攻撃には，ロールと情報の 2 つの要素が関係していること，それら 2 つの要素を加害者の視点と被害者の視点に分けて記述を行う被害過程モデルで，ソーシャルエンジニアリング攻撃をモデル表現できることを説明した．

本章では，この被害過程モデルにおける課題を述べる．

4.1 ロールや情報の幅

被害過程モデルにおいては，ステップアップの幅を常に一定に定めている．これは，今回モデル表現を検討するに際し，まずはロールや情報のステップアップの有無について表現し，ステップアップの定量的表現については対象外として検討していたためである．

しかし，モデルによって情報の飛躍の幅を示すことができれば，実用の面で非常に有用であると考えており，ロールや情報の定量化は今後検討する必要があると考えている．

4.2 ロールと情報の尤度判定

被害過程モデルでのソーシャルエンジニアリングの実例分析は，ロールと情報の尤度判定に課題がある．

例えば，同じ「課長」という役職であっても，情報についての権限は会社によって異なることが多いため，ある課長がある情報にアクセスした時に，それが均衡直線の上にあるのか下にあるのかの判定が，その組織のルールに従うため，一意に決定することが出来ない．

これは，被害過程モデルの適用先が，ロールと情報の尤度を規定したルールを持つ領域内であることを示しており，モデルの適用先を広げるためには，広範囲に適用可能なロールと情報の尤度を規定したルールが必要になると考えている．

4.3 親しさの表現

加害者が提示するロールに変化が無いまま被害者とコンタクトを取る回数を重ねることによってのみ，尤度より大きい情報が入手できる実例が存在した．その原因としては，加害者がコンタクトを取る回数が増えたことにより，被害者が加害者に親しみを感じることが考えられるが，親しみが認識させるロールや提供する情報に影響を与えているのか，他の要因とすべきなのかの更なる検討が必要である．

仮に親しみがロールや情報の尤度に影響を与えるとすると，モデルの均衡直線の傾きを変化させて表現することが出来る．傾きを変化させ，親しさを表現した被害過程モデルを図 5 に示す．

しかし，このモデル表現においてもどれくらい傾きを変化させれば適切なのかという課題が残り，4.1 節と同様に，情報やロールの定量化が必要となってくると考えられる．

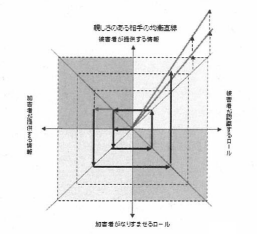

図 5: 被害過程モデルにおける親しさの表現

4.4 複数の被害過程モデルを要するソーシャルエンジニアリング

被害過程モデルにて表現された1つの図では，最終目的の情報にふさわしいロールに近付くために，1つずつ情報を使用し，その情報によってロールをステップアップさせている過程を表現している．

このため，最終目的の情報にふさわしいロールに近付くために，複数の情報を同時に使用したり，必要な情報を別のソーシャルエンジニアリング攻撃で入手するような実例を1つの被害過程モデル図で表現することが出来ない．

例えば，ソーシャルエンジニアリングの中で，2つのの情報を事前に入手しておき，その2つの情報を使用して，最終目的の情報に近付く実例が存在する．図6にてその例を簡略化して示す[5]．

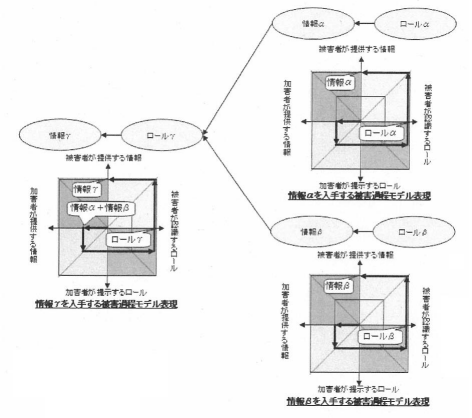

図 6: 被害過程モデルで表現できない事例

この実例におけるソーシャルエンジニア攻撃者の最終目標は情報γである．情報γを得るためにはロールγがふさわしいロールとして存在する．攻撃者はロールγになりすます必要があるが，ロールγになりすますにはロールγにふさわしい情報として情報αと情報βが別個に存在する．この情報αと情報βに関連性はなく，それぞれ別の入手経路から入手できる情報であるが，入手する順番はどちらが先でも構わない．

この実例を表現するには，情報αを入手する過程，情報βを入手する過程，情報γを入手する過程をそれぞれ別個の被害過程モデルに表現し，それらを並記することで表現する必要があり，以下のように3つの被害過程モデルを使用して表現する必要がある．

[5]文献 [3] 第 11 章　テクノロジとソーシャルエンジニアリングの併用より刑務所内の人間とコンタクトを取る実例より

ソーシャルエンジニアは，図6右上の被害過程モデルで表現されるように，ロールαになりすまし情報αを入手し，それとは別に図6右下の被害過程モデルで表現されるように，ロールβになりすまし情報βを入手する．そして，これらの情報αと情報βを元にロールγになりすまし，最終目的の情報γにたどり着く．

5 今後の課題

本研究では，ソーシャルエンジニアリング攻撃を用いた情報の不正な取得への対策を取ることを目的として，その攻撃をモデル表現することを試みた．

ソーシャルエンジニアリング攻撃の表現に必要な要素とその関係を，ロールと情報の2軸とその尤度であると仮説を立て，モデル化の検討を行った．その中で加害者と被害者の視点を盛り込むことが必要となることを明らかにし，それらロールと情報の2軸を加害者と被害者の視点に分けて表現した4軸でソーシャルエンジニアリング攻撃を表現する被害過程モデルを提案した．

被害過程モデルを用いた実例分析において，4つの象限のどこで均衡直線を越えるステップアップがあったのかを記述することで，ソーシャルエンジニアリング攻撃をモデル表現することが可能になった．モデル表現により，情報やロールのステップアップを可視化して記述することで，ロールや情報を利用してどのような攻撃が行われたのかを一意に表現することが可能になり，ソーシャルエンジニアリング攻撃の対策へつなげることが出来ると考えている．

被害過程モデルの課題の1つは，ロールや情報の定量的表現である．今後は，定量的な被害過程モデルの表現のための，ロールや情報の定量化の検討が必要であると考えている．

参考文献

[1] 情報処理推進機構, 国内におけるソーシャル・エンジニアリングの実態調査,2000/01

[2] 矢竹清一郎, 内田勝也, ソーシャルエンジニアリングの分析およびアクセス制御の提言, 2007-CSEC

[3] ケビン・ミトニック, ウィリアム・サイモン, 岩谷宏 [訳], 欺術－史上最強のハッカーが明かす禁断の技法, ソフトバンク　パブリッシング株式会社,2003/06

[4] 日本数理社会学会, 社会を＜モデル＞でみる　数理社会学への招待, 勁草書房,2004/03