1ZA-06

詐欺プログラム対策のための詐欺プロセスモデルの検討

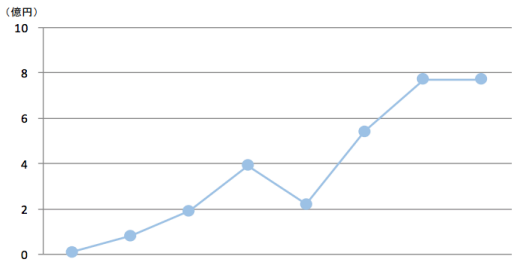
山越 祐希† 八槇 博史†
東京電機大学†

１．はじめに

近年，SNSの普及に伴いLINEでプリペイドカードを購入させるような詐欺や有名人を装ってメッセージを送りフィッシングサイトに誘導する詐欺が出てくるなど，詐欺は多様化してきている．詐欺の状況については図１を見てほしい．図１は警察庁のデータ[1]である．詐欺の被害は増加傾向にあり，２９年には電子マネー型の詐欺だけでも約１５億円の被害額になっている．

そして，多様化する詐欺の中で新たな脅威が出てきている．それがタイトルにある詐欺プログラムである．詐欺プログラムとはSNSのBOTサービスを悪用して詐欺を自動化するプログラムのことである．詐欺の自動化の脅威については過去の研究[2]で検討しており，検討した脅威について３章に記述する．

このように新たな詐欺の脅威が出てきているのに，システム側での詐欺対策はほとんど行われておらず，ほとんどの詐欺対策がユーザーへの注意喚起であることが現状である．どれだけ注意喚起を行ったとしても騙されやすい人間は存在して被害に遭ってしまう．そこで，システム側で詐欺を対策する方法について検討していくことが本研究の目的となっている．



区分＼年次	26年上半期	26年下半期	27年上半期	27年下半期	28年上半期	28年下半期	29年上半期	29年下半期
被害額	0.1	0.8	1.9	3.9	2.2	5.4	7.7	7.7

図１．電子マネー型詐欺の被害額の推移

Investigation of Fraudulent Process Model
for Countermeasures against Fraudulent Programs
† Yamakoshi Yuki , Tokyo Denki University
† Yamaki Hirofumi , Tokyo Denki University

２．先行研究調査

今期の研究では詐欺をモデル化していくというアプローチをとるのだが、それに関連する先行研究を紹介する．「サイバー犯罪におけるソーシャルエンジニアリングに対する被害過程モデルの適用」という論文[3]である．詐欺の過程をモデル化するという点では同じ方針であると言える．上記の論文では，加害者と被害者のやりとりに着目してモデルを作成している．このモデルは加害者が質問内容をずらしながら段階的に情報を収集していく過程を視覚的に示している．本研究との違いはモデルを作成する際に着目した点にある．本研究では詐欺師の発話に含まれる要素のみに着目してモデル化している．

３．詐欺の自動化による脅威

- 自律的に詐欺を行うので同時にたくさんの人に詐欺を行うことが可能である．騙されやすい人間はある程度存在し，ターゲットの総体数が増えれば被害者が増えるだろう．
- SNS上での会話は比較的単純なやりとりが多いので，対話システムの実装が比較的容易である．また，プリペイドカードを買わせる詐欺は日本語がネイティブではない人たちが台本を使って行っていることが多く，そのレベルでも被害が出るのだからBOTでも十分に置き換えることが可能である．
- 詐欺を成功させなくても騙す相手の情報収集が可能である．具体的には，あらかじめ詐欺のシナリオを用意してそれに基づき詐欺を行うことで，途中まででもシナリオ通りに会話してくれた相手を騙されやすい人物としてターゲットリストに追加することが可能である．

４．詐欺の台本の識別器

まずは，詐欺かどうかを識別する方法について考えた．図２が詐欺台本分類器の概要図である．分類器は事前に，詐欺の台本と詐欺ではない台本を用意してラベル付けした状態で学習データとして与えて学習させておく．処理の手順は次の通りである．

1. 台本から詐欺の要素（金銭要求・儲け話など１１項目用意した）を基にしてベクトル化する．より疑わしい要素により大きい値を設定．
2. １で得たベクトルをナイーブベイズ分類によって詐欺の台本か詐欺ではない台本か分類する．

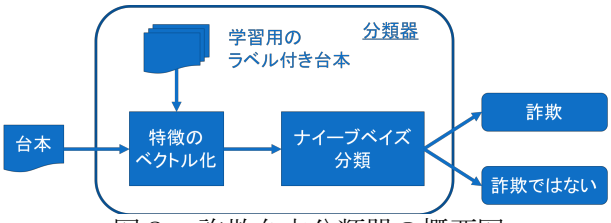


図２．詐欺台本分類器の概要図

５．詐欺師の発話プロセスモデル

５．１　モデルの説明

４章の識別器では詐欺かどうかを識別することはできたが，詐欺の種類まで特定することはできなかった．詐欺の種類が特定できれば，より具体的な警告を出すシステムを開発することができる．そこで，詐欺プロセスのモデル化をしてみることにした．本研究で作成したモデル（図３）は，詐欺師（騙す側）の発話に含まれる要素に着目して騙すまでの過程をまとめたものである．このモデルは詐欺の台本や詐欺関連本[4][5][6]で紹介されている詐欺の手口を頼りに手作業で作成している．

モデルについて具体的に説明していく．四角い枠で囲まれているのが詐欺師の発話に含まれる詐欺の要素である．角のない枠に囲まれている下部４つが詐欺の種類である．青色の実線の矢印が次に出現する詐欺の要素を示している．緑色の点線の矢印がプロセスに対する詐欺の種類を示している．

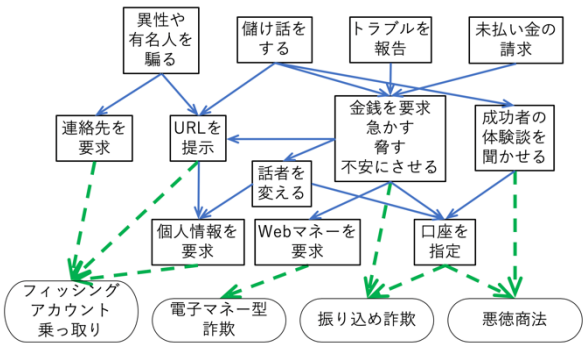


図３．詐欺師の発話プロセスモデル

５．２　モデルを用いた詐欺対策の考察

まず，このモデル（図３）に対して詐欺の台本を複数適用してみた．その結果，詐欺師の発話プロセスにはいくつかのパターンがあることがわかった．パターンを詳しく調べておくことで，会話のやりとりの途中で詐欺のパターンを特定して詐欺の目的別に警告を出すシステムに応用することが可能だろう．

また，図３のモデルには強みがある．それは，詐欺師の発話に含まれる詐欺の要素のみを拾っているので，相手の身分・アカウント情報・会話の長さなどに影響されないという点である．身分が変わった時の会話への影響を気にする必要がないということ，アカウントが公式・非公式・企業・個人のものであることを気にする必要がないということ，プロセスの途中で詐欺とは関係のないやりとりが行われても影響しないということ，詐欺のシナリオがシンプルでも複雑でも問題ないということである．

６．まとめ

本研究では今後想定される詐欺の脅威について考えながら，詐欺警告システムを開発するために詐欺プロセスモデルを作成した．このモデルは詐欺師の発話に含まれる詐欺の要素に着目して作成した．そして，プロセスモデルに対して詐欺の台本を適用してみたところ，詐欺にはいくつかのプロセスのパターンがあることがわかった．今後はプロセスのパターンをより詳細に調べていき，詐欺の種類を特定して警告を出すシステムの開発に応用したい．そのためのモデルの改良も必要だと考えていて，より実用性を追求していくつもりである．

参考文献

[1] 警察庁，“平成 29 年の特殊詐欺認知・検挙状況等について（確定値版）“，警察庁 Web サイト刊行物，July 2018.
[2] 山越祐希，八槇博史，“対話エージェントを通じた誘導型サイバー攻撃の検討“，電子情報通信学会総合大会，2017.
[3] 柴田賢介，荒金陽助，沼田晋作，神谷造，佐野和利，金井敦，“サイバー犯罪におけるソーシャルエンジニアリングに対する被害過程モデルの適用”，情報処理学会，2008.
[4] 西田公昭，『だましの手口』，2009 年，PHP 新書.
[5] 坂口孝則，『営業と詐欺のあいだ』，2008 年，幻冬舎.
[6] 多田文明，『【図解】なぜ、詐欺師の話に耳を傾けてしまうのか？』，2013 年，彩図社.