4G1-4

利用者の行動特性を用いたサイバー攻撃における成りすまし対策技術

Behavior-based anti-spoofing technology for targeted cyber attack

片山 佳則[*1] 寺田 剛陽[*1] 津田 宏[*1]
Yoshinori Katayama Takeaki Terada 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

標的型メール攻撃のような，情報搾取を意図したサイバー攻撃の手口は巧妙化している．業務内容のやり取りメールに見せかけた攻撃や，PC の乗っ取り，また SNS に代表されるソーシャルメディアの乗っ取りによる誘導も確認されている[IPA 2013]．本論文では，利用者の行動特性を利用して攻撃に対する人の検知力を高める対策について述べる．

2. 行動特性を利用した標的型攻撃メール対策

サイバー攻撃のリスクは，人や部門，業務，状況などにより異なる．我々も社内のメール状況を分析して，メール誤送信が昼過ぎに多い(食後注意力が低下するためであろう)とか，標的メール訓練の開封率が部署により大きく異なるということを確認している．ユーザに過度に負担を掛けさせずに，サイバー攻撃の被害を最小化するためには，人や部門に合わせたきめ細かな対策が必要であり，そのためは利用者の行動特性を用いた攻撃対策が必要と考える．

2.1 標的型メール攻撃対策

標的型メール攻撃への対策として，高度なりすましメールを検知することが求められている．具体的な対策として，メール訓練等により利用者の意識を向上させたり[IPA 2013]，受信メールの経路や受信状況などから怪しいメールに注意喚起をさせたり[吉岡 2012]，また SPF などのドメイン認証を利用した対策などがある．しかし，標的型メール攻撃は，より巧妙にヘッダーを改ざんするため，ヘッダーのチェックや経路ドメインの整合性だけでは，必ずしも本人のメールであるか分からないなどの課題がある．高度なメール攻撃に対処するには，送信者本人が作成したメールであるかを正しく判定することが求められる．

PC 操作ログを利用して本人確認を行う技術として，打鍵認証があるが，これはログイン時のパスワード入力など特定な操作に限られる．[角野 2009]は，メール編集時の削除キー等の入力情報から，どの程度推敲したなど言外の情報を伝えるものである．これをさらに，PC 上のアプリやキーボード，マウス等の操作ログや，メール送受信状況などの個人の行動特性全般に拡大することで，PC 乗っ取りなどのサイバー攻撃への対策につなげることを考えたい．

2.2 行動特性を利用した標的型メール対策

図 1 は，送信者の行動特性を利用した成りすましメール対策の概要である．メール送信時の送信者の行動を抽出するために，クライアント端末上の，キーボード情報やマウス情報，アクティブウインドウの切換えなど行動ログを蓄積する．メール送信先毎に，こうしたログを蓄積することで，利用者自身の特徴を得ることができ，それによって受信者は正規送信者か否かを判別することが可能になる．

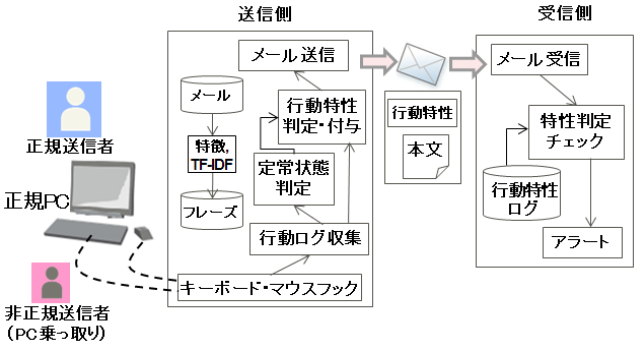

図 1 送信者行動特性を用いた成りすましメール対策

送信者毎にメールの文面は異なるため，打鍵認証のように同一のキーワードに対する特徴を行動特性として取るということはできない．しかし「よろしくお願いします」のように多くのメールで利用されるフレーズや，“研究所）佐藤さん”のように特定の相手に対して良く使われるフレーズは存在する．そこで，過去の送信メールから，比較的多くのメールで使われる特徴フレーズ，送信者毎に使われるフレーズを辞書として構築する．送信者側で蓄積される特徴フレーズの例を表 1 に示す．

表1 送信側で蓄積される特徴フレーズ

ID	特徴フレーズ
1	各位
2	お世話になっております
3	宜しくお願いいたします
4	サイバー攻撃対策
5	田中部長殿
6	研究所）佐藤殿
…	…

表2 個別に添付される行動特性

田中さんへ

項目ID	値
1	0.60
2	0.57
3	0.33
5	0.56
…	…

佐藤さんへ

項目ID	値
1	0.60
2	0.57
3	0.33
4	0.55
6	0.33
…	…

頻度の高いものと，メールごとに特徴的なものの 2 種類がある．この特徴フレーズを用いて，送信メール作成時に送信先ごとの行動特性を算出する(表2)．算出した行動特性をメールに

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

付与して送信する. 送信側の状況変化は, 特徴フレーズの更新 ID によって対応され, 基本的仕組みは変更せずに対応できる.

メール受信者は, 過去の受信メールにおける特徴フレーズの行動特性を蓄積しておき, 新たに受信したメールの特性を比較することで, このメールが正規送信者によって送られたものかを判別することができる. これにより, 標的メール攻撃対策としても課題であった正規 PC の乗っ取りによる成りすましメールにも対処できると考えられる.

3. メール送信者の行動特性

標的型攻撃メールの判定の仕組みにおいて, 送信者側の行動特性として特徴フレーズの規定方法が重要になる. 宛先アドレス毎に, 特徴的なフレーズとキー入力などの組合せで送信者の行動特徴をモデル化することで, 受信者が送信者の正当性を判定することができる.

3.1 行動特性としての特徴フレーズ

メール作成過程において, 認証処理など特定の処理により送信者が本人であることを判定することは提案されているが, 標的型攻撃では攻撃者の付入る隙になってしまう. そこで, 宛先ごとに蓄積したメールから特徴フレーズを自動的に抽出することで, 利用者の普段の行動特徴をとることを考える.

行動ログ抽出ツールとして, 起動アプリの利用状況, キーボード操作, マウス操作を詳細に取得するツールを試作し, これらをメール作成に限定して活用することで, 特徴フレーズの選出対象をメール宛先ごとに絞り込んだ. 基本的には, TF-IDF により過去のメール文面に出現するキーワードを抽出すると共に, キー入力行動の情報としてさらに, 下記のような特徴を選んでいる.

- 特徴的な打鍵組合せのある個所
- 通常と異なる打鍵スピードの個所
- 登録単語を含む個所
- 本文の先頭部分
- N-gram 方式での高頻度個所

これらの入力パターンの特徴を算出し, 複数人での比較により特徴判定が可能であるかを試行した.

3.2 特徴フレーズの行動特性抽出実験

複数のメールを同時に作成することもあるため, 本ログ収集ツールでは, 作成メールごとにキー入力データを分離して保存することで, 複数メールの作成画面を同時に開いて交互に入力作業が行われても, それぞれ個別に検証できるようにしている.

メール作成処理中の, 漢字変換した確定文字の取得は容易には行えず, 現状では, キー入力からの切り分けによって対象を絞り込んで処理している.

＜判定チェックテスト＞

今回は, PC 乗っ取りによるなりすましメールをターゲットとして, ある利用者1が通常利用している PC 本体そのものを用いて, 3名に利用者1がメール本文によく使用する文書表現を含めたなりすましメール本文の入力を行っていただき, 作成本文中の特徴的操作や違いなど判定可能な結果が得られるかどうかをチェックした.

今回チェック対象とした文書表現は,「各位」,「お世話になっております. ○○です」,「サイバー攻撃対策技術について」,「宜しくお願いいたします」など頻度の高い、簡単な語句を含んだ任意のメール本文の入力操作を行った.

表3 正規 PC による特徴フレーズのキー入力データ

入力データの値は, 左から打鍵数,時間(秒),特殊キー回数(Sp,-Ent-BS)

フレーズ	利用者本人	なりすましA	なりすましB	なりすましC
各位	16,02-03,1-2	18,01,1-2	18,01-02,1-3	17,02-03,1-3
お世話になっております。	60,01,1-2	90,06,1-2-8	74,03-05,1-2-8	65,05-07,1-3-2
サイバー攻撃対策	40,03-06,2-4	38,02-03,1-4	38,02-03,2-2	36,02-03,3-3
宜しくお願いいたします	50,04-07,1-2	50,02-04,1-2-2	48,05-07,2-3	48,05-07,2-4
・・・				

表 3 に示すように, 各フレーズに対する, キーボードの打鍵数, 打鍵スピード, Space-Enter-BS など特殊キーの打鍵組合せ情報などほぼすべてにおいて, 利用者本人とは異なる特徴が表れている. 特殊キー回数は, 短いフレーズを対象としたことで, 異なる特徴が得られている. このように, フレーズをうまく選択することで, PC 乗っ取りによるなりすましメールの自動検知につなげるなどが考えられる. 行動特性として, 今回は頻度の高いフレーズを対象として実験したが, 大量の打鍵情報などからの推定や絞込みも必要になる. また, また, マウス操作など, キーボード打鍵以外の要素も特徴として扱えるものがある.

4. まとめ

本論文では, PC 遠隔操作など, 標的型メール攻撃者の巧みな攻撃に対処するために, メール宛先毎の特徴フレーズのキー打鍵という行動特性を活用した成りすまし対策方式を提案した. ここでは, 打鍵上の特徴として特定のパターンを考えたが, 複数種類のアプリのログデータやタスクプロセスの切り替えパターンなど, 複数のログ系列から, 時系列パターンを抽出する手法[安部 2012]などにより, より本人も気づいていない行動特徴をマイニングすることが考えられる. また今後, 個人だけでなく組織やグループのパターンマイニングへの展開を広げていきたい.

個人や組織でリスクは異なるため, 一律のセキュリティ対策では, 効率が悪くなったり, 効果がなかったりということがある. 行動特性は検知だけでなく, 対策にも大きく寄与する可能性がある. 今後は, これまでに行ったメール訓練での心理的分析に基づき, 利用者の心理的な属性も考慮することで, 受信側の行動特性と心理特性に配慮して, 利用者にとって有用な対策を実現するサイバー攻撃対策の研究開発を進めていく予定である.

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.

参考文献

[IPA 2013] (独)情報処理推進機構: 情報セキュリティ白書, IPA , 2013.

[吉岡 2012] 吉岡, 片山, 津田, 森永, 深澤: 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, 情処研究報告 2012-SPT-4, 37, pp.1-8, 2012.

[角野 2009] 角野, 西本:言外の情報としての編集過程情報を伝えるメールシステムの提案と評価, 情報処理学会論文誌, 50(1), 2009.

[阿部 2012] 阿部, 津本:重複系列の発生パターンに関する時系列マイニングとその医療応用, 人工知能学会誌, Vol.27,No.2, 2012/3