Computer Security Symposium 2017
23 - 25 October 2017

OSINT を利用した標的型メール攻撃手法に関する基礎検討

上原 航汰[†1]　向山 浩平[†1]　藤田 真浩[†1]
西川 弘毅[†2]　山本 匠[†2]　河内 清人[†2]　西垣 正勝[†1]

概要：近年は，企業や個人に関する多くの情報が OSINT（Open Source Intelligence）によって容易に入手できる状況にあり，標的型メール攻撃をはじめとするソーシャルエンジニアリングの脅威は従前よりも格段に大きくなっている．このような現状に鑑みるに，OSINT と標的型メール攻撃の相乗効果をモデル化することは，対策検討に資する有効な知見となると考えられる．そこで本稿では，攻撃者が OSINT ツールを用いて攻撃対象の情報を収集していく過程を状態遷移モデルとして体系化し，その各状態において攻撃者が生成可能な標的型メールを類型化する．今回の分析結果は，被害者が標的型メールの内容から攻撃の深度を見積り，それに応じた事後対策を講ずるために活用できる．今後，この分析を拡張することにより，AI（Artificial Intelligence）と標的型メール攻撃の相乗効果のモデル化を達成し，将来予測され得る AI を悪用した標的型攻撃に対する事前対策の整備へとつなげていきたい．

キーワード：ソーシャルエンジニアリング，標的型メール，OSINT

A basic study on targeted mail attack method using OSINT

Kota Uehara[†1]　Kohei Mukaiyama[†1]　Masahiro Fujita[†1]　Hiroki Nishikawa[†2]
Takumi Yamamoto[†2]　Kiyoto Kawauchi[†2]　Masakatsu Nishigaki[†1]

Abstract: In recent years, attackers could get much information on companies and individuals easily by OSINT (Open Source Intelligence), and the threat of targeted attacks has been increased. In light of such a situation, modeling the synergistic effect of OSINT and targeted attack is the effective contribution for taking measure against the targeted attacks. In this paper, we construct a state transition model which defines the process of attackers, who gathers the target's information by using OSINT tools. Then we categorize targeted e-mails that attackers can generate in each state. The analysis result can be used for the victim to estimate the depth of attack from the contents of the targeted e-mail and to take measures.

Keywords: Social Engineering, Targeted email, OSINT

1. はじめに

近年，標的型メール攻撃の被害が急増している．標的型メール攻撃はソーシャルエンジニアリングの典型例の一つであり，攻撃対象者を騙すことで対象者に被害を与える（例えば，情報や金銭を搾取する，PC を不正に操る）．標的型メール攻撃を成功させるためには，攻撃対象者に標的型メールを正規のメールと信じ込ませることが不可欠であり，このため攻撃者は，攻撃対象者に関する情報を収集しようと試みる．

この情報収集に関しては，従前の攻撃者は，攻撃対象者に関する情報を自力で収集する必要があった．管理者を装って攻撃対象者に近付いて本人から直接情報を聞き出したり，攻撃対象者の周囲の人物から情報を収集する Human Intelligence（HUMINT）や，攻撃対象者の通信や信号を盗聴して情報を収集する Signals Intelligence（SIGINT）が代表的な収集方法としてあげられる．しかし近年では，企業やユーザが自身の情報をオウンドメディアやソーシャルメディアに自ら発信することが当たり前の時代になってきた．今や，Web 上や SNS 上には企業や個人に関する情報が氾濫しており，公開されているパーソナル情報を組み合わせることによって個人情報やプライバシ情報を得ることが可能であるとも報告されている[1][2]．このような情報収集は Open Source Intelligence（OSINT）と呼ばれ，最近では OSINT 活動をサポートするツールも出回っている．攻撃者は OSINT ツールを利用することで，より信憑度の高い（より対象者が騙されやすい）標的型メールを作成することが可能であり，標的型メール攻撃の脅威は従前よりも格段に大きくなっている[3]．防御側の観点からは，これら OSINT を利用した標的型メール攻撃をあらかじめ検討しておくことが重要となる．

このような現状に鑑み，本稿では，OSINT と標的型メール攻撃の相乗効果をモデル化することを試みる．具体的には，OSINT ツールを利用した標的型メール攻撃[3]を想定し，攻撃者が OSINT ツールを用いて攻撃対象の情報を収集していく過程を「状態遷移モデル」として体系化する．さらに，その各状態において攻撃者が生成可能な標的型メールを類型化する．本分析結果は，被害者が標的型メールの内容から攻撃の深度を見積り，それに応じた事後対策を講ず

†1 静岡大学
Shizuoka University
†2 三菱電機株式会社
Mitsubishi Electric Corporation

るための有効な知見になると考えられる．また，今後，OSINT ツールが進化し AI（Artificial Intelligence）化された暁には，攻撃者は AI を悪用して標的型メール攻撃を行なってくるだろう．本研究の知見は，AI と標的型メール攻撃の相乗効果を分析するにあたっての足掛かりとなり得る．

2. OSINT を利用した標的型メール攻撃

2.1 OSINT によるソーシャルエンジニアリングの高度化

OSINT とは Open Source Intelligence の略称で，公開されている情報の中から必要な情報を収集する諜報活動をいう．公開されている情報（以下，OSINT データと呼ぶ）とは，新聞の報道，政府の公報から電話帳に書かれている情報まで幅広い範囲が含まれる．近年は，SNS や Web サイト上で，多くの個人や企業が自身に関わる情報を発信しており，個人や企業に関わる膨大な OSINT データが入手可能な現状となっている．

OSINT データは，経済予測や流行分析などといった目的で有用な情報である．しかし，これら OSINT データは，標的型メール攻撃，より正確には，ソーシャルエンジニアリングをしかける攻撃者にとっても有益な情報となる．OSINT データを組み合わせることによって個人情報やプライバシ情報を得ることが報告されており[4]，また，OSINT 活動をサポートするツールも出回っている．今や攻撃者は，HUMINT や SIGINT 等の「手間のかかる諜報活動」を行わずとも，OSINT データから攻撃対象者に関する情報を収集することが可能な状況にある．そして，その情報を利用することによって，攻撃者は信憑度の高い（対象者が騙されやすい）標的型メールの作成が可能である．

以下に，これら脅威について具体例をあげて説明する．下線部が OSINT データに対応する部分である．

【具体例】

攻撃者が，大学教授である A 氏に標的型メールを送信する場面を想定する．

1. 攻撃者は A 氏の名前を用いて，メールアドレスを Web 検索し，ドメインが「*.ac.jp」であるメールアドレスを得る．
2. 攻撃者は名前やメールアドレスを用いて関連する Web ページを検索し，研究室の HP から，A 氏がどのような研究を行い，業績を挙げているか調べる．
3. 攻撃者は続けて関連する Web ページを調査し，A 氏が以前，X 社で講演したという情報を得る．
4. 攻撃者は X 社について Web 検索して関連する Web ページを調べ，現在注力している事業や社員のメールアドレスの書式といった情報を得る．
5. 攻撃者はメールのヘッダを偽装し X 者の社員になりすまし，以前の講演が素晴らしかったこと，現在注力している事業が A 氏の研究と関連していること，A 氏に再び講演して欲しいことをメールに記載し，詳細は添付ファイルを参照して欲しいと述べ，エクスプロイトコードを含む PDF ファイルを添付し A 氏にメールを送信する．

本シナリオにおける攻撃者は，当初，A 氏の名前と職業に関する情報しか有してなかったが，Web 上から多くの OSINT データを収集することができた．その結果，攻撃者は，手順 5 に示したような信憑度の高い標的型メールを作成することに成功している．

2.2 OSINT ツール

OSINT ツールとは，Web 上にある膨大な OSINT データの中から，検索対象に関わる OSINT データだけを効率的に入手する為に用いられるツールである．Maltego, Creepy など，既に数多くの OSINT ツールが公開されている．以下に，OSINT ツールの代表例である Maltego と Tinfoleak を利用して，OSINT ツールの詳細な動作を説明する．

Maltego は Paterva 社によって開発されたデータ収集・可視化ツールである．名前，ドメイン，URL のいずれか，または，その組合せを入力すると，それに紐づくありとあらゆる情報を Web 上から自動的に収集する．例えば，Maltego に対して名前「Masakatsu Nishigaki」を入力した場合，図 1 の形式で電話番号，メールアドレス，関連 Web サイトのリストが得られる．本例では SNS アカウントが見つからなかったが，Twitter や Facebook 上で一致するアカウント名が存在する場合は，該当アカウントの情報も取得することが可能である．

また，ここで得られた情報を更に入力することによって，連鎖的に情報を収集していくこともできる．例えば，名前を入力することによって得たドメイン名「minamigaki.cs.inf.shizuoka.ac.jp」（図 1）を Maltego に入力した場合，PDF ファイル，関連 Web サイト，関連ドメイン，Web サーバソフトウェア情報，メールアドレス，IP アドレス，IP アドレスから求まる位置情報が得られる（図 2）．

このように，前節のシナリオにおける手順 1〜4 の検索作業の多くが，Maltego によって半自動的に実施可能であることが分かる．

Tinfoleak は，TwitterID を入力情報と以下の情報を得ることができる． Maltego が Web 上全体を検索対象としているのに対し，Tinfoleak は特定サービス（Twitter）上に限定した情報収集を行う．

- ユーザの基本情報（名前，画像，所在，フォロワー等）
- ユーザが使用するデバイスと OS
- ユーザが使用するアプリケーションと連携 SNS
- ツイートに付与された位置情報（座標）
- ユーザが投稿した写真
- ユーザが使用したハッシュタグと使用された時刻
- ユーザと親密な関係にある他ユーザの特定
- ユーザが興味を示すトピック（趣味等）

これらの情報は，本来，対象ユーザの Twitter におけるプ

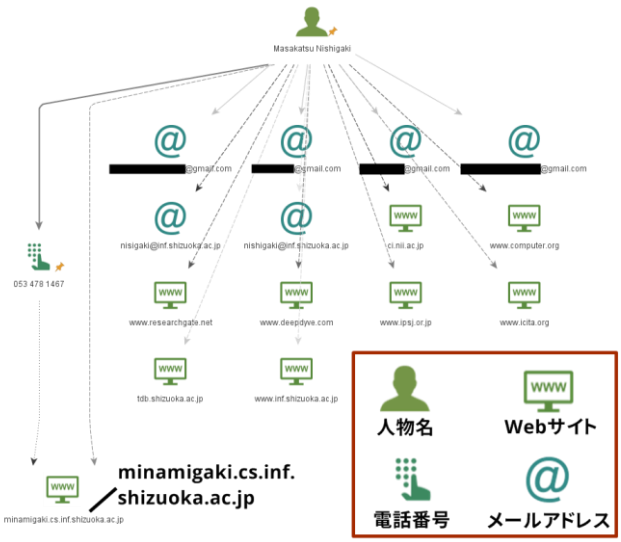

図 1　Maltego による結果 1（入力：名前）

図 2　Maltego による結果 2（入力：ドメイン名）

ロフィールやツイート，他ユーザとのやりとりをくまなくチェックして分析を行ったり，位置情報が付与されているツイートを手作業で探し出したりすることで得られる情報である．Tinfoleak は，これらの情報を自動的かつ瞬時に提供する．

これら OSINT ツールは，正規ユーザが，自身のパーソナル情報がどの範囲まで拡散しているか確認したり，自身が利用しているサーバの脆弱性を診断する（デーモンやアプリケーションのバージョンを確認する），といった場面で非常に有用である．しかし，場合によっては，標的型メール攻撃（より正確には，ソーシャルエンジニアリング）を支援するツールとして攻撃者に悪用されてしまうという二面性を有する．

3. OSINT ツールと標的型メール攻撃の相乗効果

3.1 状態遷移モデルによる脅威分析

OSINT ツールを利用した標的型メール攻撃の検討を行うにあたり，本稿では「OSINT ツールと標的型メール攻撃の相乗効果」のモデル化を試みる．まず，攻撃者が OSINT ツールを用いて攻撃対象の情報を収集していく過程を状態遷移モデルとして体系化する．そして，その各状態において攻撃者が生成可能な標的型メールを類型化する．

本研究の第一歩となる本稿においては，標的型メール攻撃の攻撃対象が「特定の個人」である場合に焦点を当ててモデル化を行う．「特定の部署に所属する任意の構成員」を攻撃対象とする標的型メール攻撃も同手順でモデル化を行うことが可能であると考えているが，詳細については今後の検討項目とする．

3.2 攻撃者が保有する情報の遷移

OSINT ツールを利用した標的型メール攻撃では，攻撃者が

1. その時点で攻撃者が有する攻撃対象者に関する情報を OSINT ツールに入力して，新たな情報を収集する．
2. 1.で入手した情報を更に OSINT ツールに入力して，連鎖的に情報を収集する．

という手順を経ることに鑑みて，攻撃者が OSINT ツールを用いて攻撃対象の情報を収集していく過程を状態遷移モデルとして体系化する．

初期状態において，攻撃者が保有する「攻撃対象者に関わる情報」を{X0}と記す．攻撃者が OSINT ツールに{X0}を入力することによって，攻撃対象者に関わる新たな情報 X1 が入手できた場合，状態は（{X0}から）{X0, X1}に遷移する．引き続き，攻撃者が OSINT ツールに{X0, X1}を入力することによって，攻撃対象者に関わる更に新たな情報 X2 が入手できた場合，状態は（{X0, X1}から）{X0, X1, X2}に遷移する．以降，これが繰り返される．

例えば，攻撃者が攻撃対象の｛名前，電話番号｝という情報を保有している状態において，OSINT ツールに「名前」，「電話番号」，あるいはその両方を入力することによって，攻撃対象の「住所」が入手できた場合，攻撃者の状態は｛名前，電話番号，住所｝という情報を保有している状態に変化する．

攻撃者は，任意の OSINT ツールを自由に使用して，上述の手順 1〜2 の OSINT 活動を繰り返していく．今回は，攻撃者が使用する OSINT ツールとして，OSINT 収集用 Linux 仮想マシンである Buscador [5]に標準で用意されている OSINT ツール群（Recon-NG，Maltego，Creepy，Metagoofil，Tinfoleak，EmailHarvester，theHarvester，SpiderFoot，ExifTool の 9 つの OSINT ツール）を想定した[a].

a 各 OSINT ツールはそれぞれの特徴を有しており，OSINT ツールに対する「入力情報」と，その入力情報から出力として得られる「収集可能な情報」は，ツールごとに部分的に異なる．紙面の関係上，それぞれの OSINT ツールの「入力情報」と「収集可能な情報」の一覧については掲載を省略する．

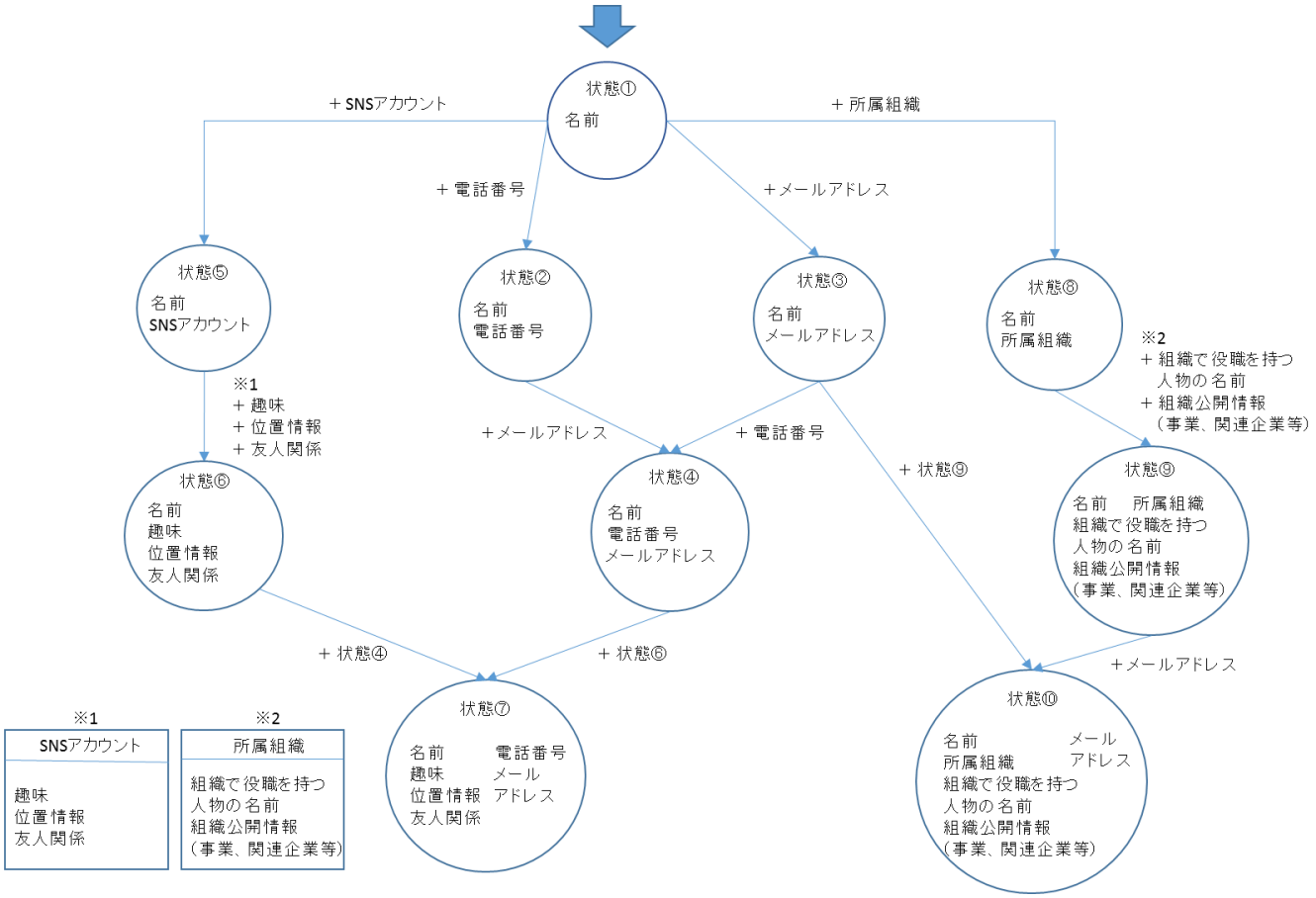

図 3　攻撃者が情報を収集していく過程の状態遷移モデル

3.3 状態遷移モデルの構築

著者らが攻撃者の立場になり，前節に示した 9 種の OSINT ツールを実際に利用して OSINT 活動を試行することによって，「攻撃者が，OSINT ツールを用いて，攻撃対象者に関する情報を次々と取得していく過程」を状態遷移モデルとして体系化した（図 3）.

なお，今回構築する状態遷移モデルにおいては，モデルの簡素化のために，以下の前提を設けている.

- 取り扱う OSINT データの種類を，名前，電話番号，メールアドレス, SNS アカウント, 趣味, 位置情報，友人関係, 所属組織名, 組織における役職者の名前，組織の公開情報（事業，関連企業等）に限定する.
- 攻撃者が攻撃対象の｛名前｝のみを保有している状態を初期状態と仮定して状態遷移モデルを構築する.
- 各保有情報から推測されうる情報は考慮しない.（例えば, 攻撃対象のメールアドレスのドメインが ac.jp であることが分かった時点で, 対象者が教育機関に属することが容易に推測できるが，今回は，そのような演繹は一切行わないこととする.）
- OSINT ツールに SNS アカウントを入力すると，そのアカウントの人物の趣味，位置情報，友人関係に関する情報については必ず取得できるとする（図 3 中の※1）.（実際には，例えば Twitter でツイートに位置情報を含める者がいる一方，全く含めない者もいるが，今回は簡単化のため，SNS から概ねこれら 3 つの情報が分かるという前提を置く.）
- 現在多くの組織が Web ページにおいて IR 情報等を公開していることから, OSINT ツールに所属組織を入力すると，その組織の役職者の名前，事業内容，グループ企業に関する情報については必ず取得できるとする（図 3 中の※2）.
- 今回は標的型メール攻撃（電子メールを介した標的型攻撃）を分析対象とするため，郵便に関する情報である「住所」については，取り扱う OSINT データから除外する[b].

3.4 各状態において攻撃者が生成可能な標的型メール

図 3 の状態遷移モデルの中で，メールの送信が可能な 4 つの状態（状態③，④，⑦，⑩）において，攻撃者が作成可能な標的型メールの典型例をそれぞれ図 4〜図 8 に示す.

b 今回，著者らが実際に OSINT 活動を試行したところでは，OSINT ツールによって住所が取得できたケースは稀（設定ミスによって顧客管理データベースが公開状態にある等の場合のみ）であった．このため，今回の分析において住所を除外することは，住所が「OSINT ツールによって容易に取得できる情報ではない」という意味からも妥当であると言えるかもしれない.

● 状態③（図 4）：

状態③では，攻撃者が保有している攻撃対象に関する情報が「メールアドレス」と「名前」だけなので，メールの文面は，攻撃対象者に依らない内容になる．メールの文面に名前が記されているため標的型メールと言えるが，内容的には一般的なフィッシングメールに近い．

● 状態④（図 5）：

状態④のでは，攻撃者はメールの文面の中に，攻撃対象者の「電話番号」を含めることできる．身に覚えがないメールであっても，メールの本文に記載されている情報が確かに自分のものであるので，攻撃対象者が騙される（メールに記されているリンク先にアクセスする）可能性は高まると考えられる．また，メールの送信者に自分の電話番号が知られているという空恐ろしさは，攻撃対象者の不安を煽り，冷静な判断を失わせる可能性もある．

なお，今回は，攻撃対象者の「住所」については検討の対象外としたが，もし攻撃者が攻撃対象者の（電話番号の代わりに）住所を取得できた場合には，図 6 のような標的型メールが作成可能である．

● 状態⑦（図 7）：

状態⑦では，攻撃者は，攻撃対象者の SNS アカウント名から，本人の趣味，位置情報，友人関係に関する情報を取得できているので，攻撃対象者の友人になりすました標的型メールを作成することが可能である．この状態では，攻撃対象者のプライベートな情報をメールに盛り込むことが可能であり，信憑度の高い標的型メールを作成できる．また，親密な他者を偽って送信されるメールには，受信者を盲目的にする効果があることが知られている[6]ため，脅威の度合いは高いと考えられる．

● 状態⑩（図 8）：

状態⑩では，攻撃者は，2015 年 5 月に日本年金機構が起こした大規模な情報流出事件[7]のきかっけとなった標的型メールを作成できる．この事件の際には，メールの件名や本文に，日本年金機構が Web ページで公開していた事業内容や役職者名を記載することによって，信憑度の高い標的型メールが作成され，使用された．

図 4　状態③の標的型メール

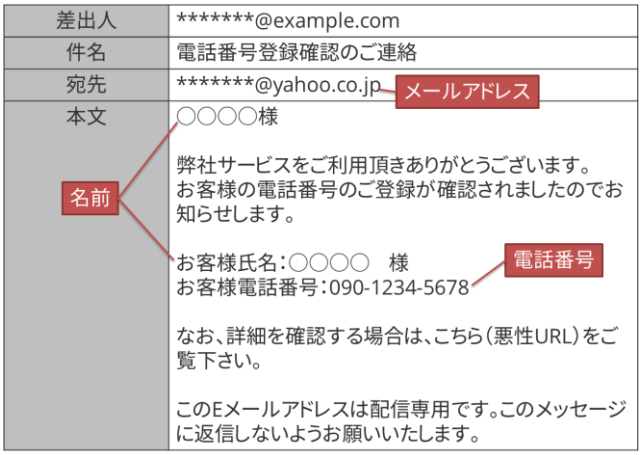

図 5　状態④の標的型メール

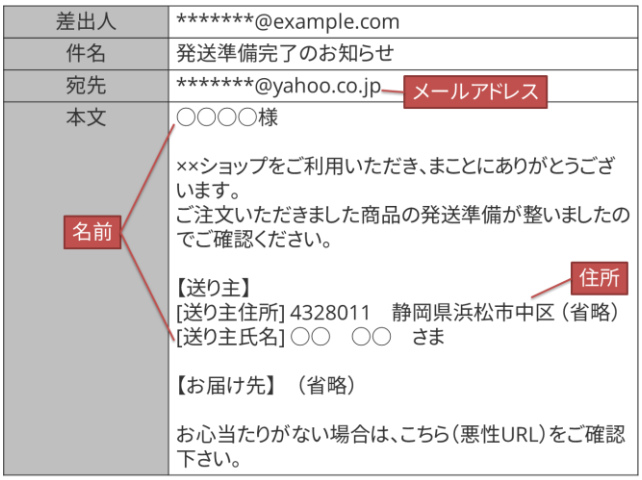

図 6　攻撃者が｛名前，メールアドレス，住所｝を取得した状態の標的型メール

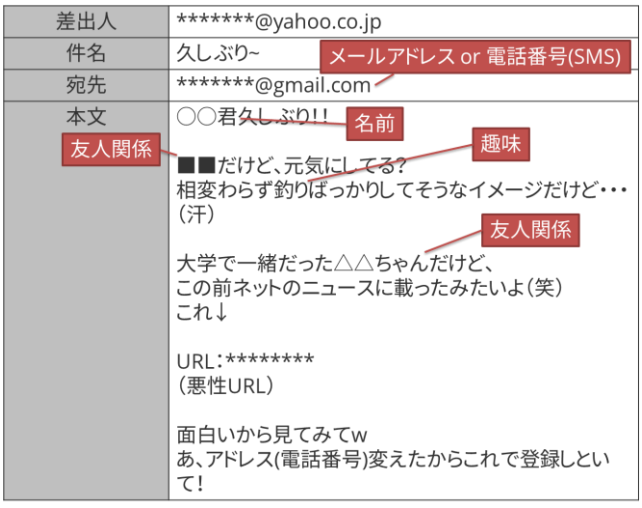

図 7　状態⑦の標的型メール

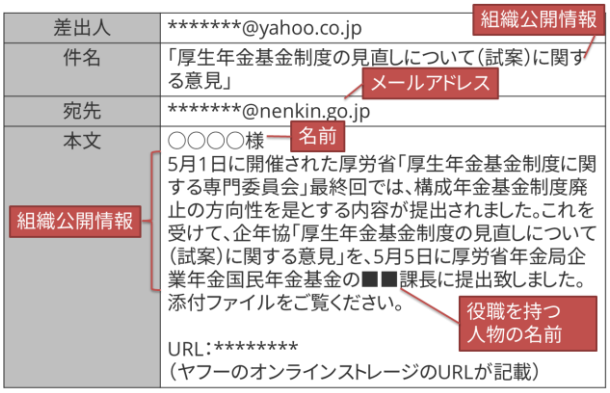

図 8　状態⑩の標的型メール

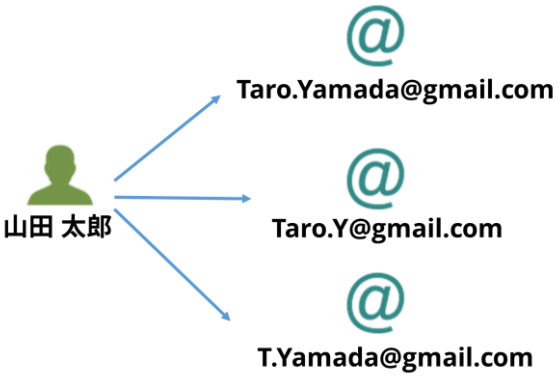

図 9　個人を一意に特定できない状態

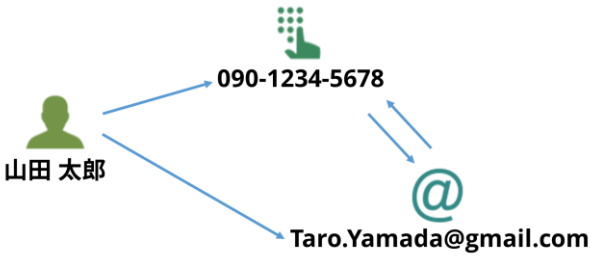

図 10　個人を一意に特定できる状態

4. 考察

4.1 各状態における標的型メールのタイプ

3.1 節で述べたように，本稿では標的型メール攻撃の攻撃対象を「特定の個人」に絞ったが，ここでは，「特定の個人」を更に 3 つのカテゴリに分類する（表 1）．まず，攻撃対象が「特定の組織に所属する個人」であるか否かによって，「特定の個人」を 2 つに分ける．そして，攻撃対象が一意に特定されるか否か（攻撃対象となり得る人物の数 k が 1 であるか 2 以上か）によって，両者を更に 2 つに分ける．表 1 に示したように，この内の 3 つのタイプを「特定個人型」，「絨毯爆撃型」，「特定構成員型」と呼称することとする．

例えば，状態①の攻撃者が，OSINT 活動によって「攻撃対象者の名前に関連する Gmail アドレス」を取得することができたとしても，それが同性同名の別の人物のメールアドレスである可能性も存在する．つまり，状態③の状態では，攻撃対象者を一意に特定できるとは言えない（図 9）．このような状況は，攻撃者の目的が「複数の同姓同名の人物の内のいずれかを欺くこと」である場合などに生じ得る．すなわち，状態③における標的型メールは，複数の同姓同名の攻撃対象者に同一文面で送られる（絨毯爆撃型）．

これに対し，電話番号や所属組織は特定の個人を識別するためのユニークな情報であると言える（図 10）[c]．したがって，状態④や状態⑧における標的型メールは，攻撃者が「特定の人物を欺くこと」あるいは「特定の組織に所属する特定の人物を欺くこと」を目的として，その攻撃対象者のみを狙って送信される形となる（特定個人型，特定構成員型）．

表 1　標的型メールのタイプ

攻撃対象	攻撃対象者の数 k	
	k = 1	k >= 2
特定の個人	特定個人型	絨毯爆撃型
組織に属する個人	特定構成員型	

c 構成人員の多い大規模な組織の場合は同姓同名の人物が存在する場合もあるが，ここでは適度な規模の組織を考えることとする．

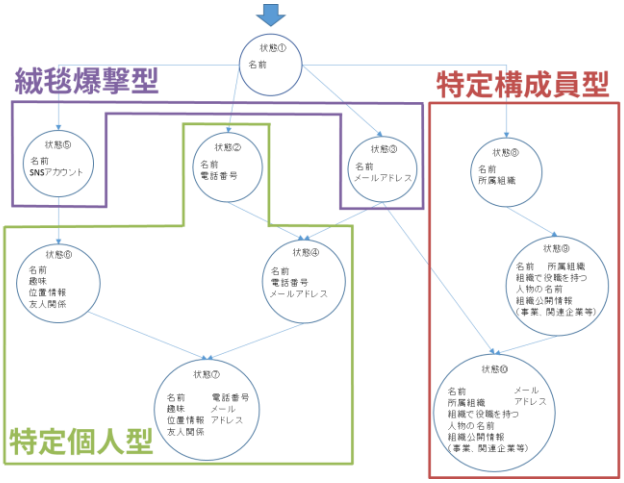

図 11　各状態における標的型メールのタイプ

各状態における標的型メールのタイプの傾向を図 11 に示す．

4.2 本モデル及びテンプレートの活用先

攻撃者が攻撃対象者の情報を収集していく過程の状態遷移と，各状態で作成される標的型メールの類型化は，以下に述べる 3 つの知見として活用できると期待される．

1 つ目は，標的型メール攻撃の深度の把握である．自分の手元に標的型メールが送られてきた際に，攻撃者が自分に対する情報をどの程度収集できているのか目算できる．また，今後，攻撃者の情報収集が進んだ際にどのような文面の標的型メールが送られてくる可能性があるのか予測できる．これにより，予想される標的型メールに対する注意

喚起や，別の攻撃者が似たような標的型メールを送信してくる可能性に気を配ることができる．すなわち，リスク分析や事前対策に役立つと考えられる．

2 つ目は，自分が公開している「自身に関する情報」の中で，どの情報の公開を止めれば，信憑度の高い標的型メールを攻撃者に作成されてしまうことを回避できるかの把握である．図 3 の状態遷移モデルからは，例えば，攻撃者を状態⑦に至らせないためには，自分の名前（実名）と SNS アカウントが共起する形での情報公開を控えることが効果的であることが見て取れる．

3 つ目は，個人や組織の情報公開の度合いに応じた標的型メール対策の導入が可能となることである．OSINT によって得られる情報が多いほど，信憑度の高い標的型メールが送られてくる可能性を考慮し，標的型メール攻撃に対する対策を高める必要がある．

5. 関連研究

ソーシャルエンジニアリングにおける OSINT の有効性について，文献[3]，[8]，[9]の研究が行われている．

Ball らは，世界中で蓄積されるデータ量が指数関数的に増加していることから，OSINT がソーシャルエンジニアリングに活用され，犯罪行為に利用されてしまう可能性について言及し，OSINT を使用して組織の従業員にスピアフィッシングメール攻撃を仕掛ける方法について議論している[3]．その中で，攻撃者が情報収集のために OSINT ツールを使用することや，スピアフィッシングを行うために専用のツールを使用する方法について紹介している．

Edwards らは OSINT データを，Bootstrap（攻撃のきっかけとして利用されるデータ）と Accentuator（攻撃の有効性を高めるために補助的に使用されるデータ）の 2 つに分類し，ソーシャルエンジニアリングにおいて，それらのデータがどのように用いられるかを示した[8]．また，水道・ガス・電気などの公共事業を担う企業について，従業員の名前や電話番号，メールアドレスといった情報が，OSINT からどの程度集めることができるのかを調査し，それらがもたらすソーシャルエンジニアリングの脅威について明らかにしている．

Silic らは，フォーチュン 500 の企業を対象として，SNS を活用したソーシャルエンジニアリングの有効性について検証を行っている[9]．具体的には，OSINT を活用して，攻撃対象の企業の従業員になりすました「偽の SNS アカウント」を作成し，正規の従業員により構成される SNS プライベートグループのメンバーになることで，企業に関する情報を入手することが可能であるかの実験を行った．その結果，従業員は容易に欺かれ，ソーシャルエンジニアリングの被害を受けやすいことや，組織は現状，SNS メディアからのセキュリティ脅威を制御する術がないことが明らかになっている．

本稿は，複数の OSINT ツールを調査して攻撃者の情報収集プロセスを「状態遷移図」として体系化し，標的型メール攻撃に焦点を当てて各状態における情報の具体的な活用方法（標的型メールの作成）を分析しており，上記の既存研究を補完あるいは補強する関係にある．

機械学習とソーシャルエンジニアリングについて文献[10]のような研究が行われている．

Singh らは，標的型攻撃の対象を企業の CFO（最高財務責任者）として，その人物が「標的となるか（騙されやすいか）」を機械学習によって予測する学習モデルを提案している[10]．学習データには，CFO の年齢や性別，Twitter のフォロワーやツイート数，Twitter や LinkedIn 経由のフィッシング成功の有無などを用いている．学習によって，80%の精度で標的になる（騙される）人物の特定が可能であるという結果が出ており，機械学習を用いたソーシャルエンジニアリングの進化について明らかにしている．

標的型メールの自動生成に関しては，岩田らが標的型メール攻撃対策訓練における，訓練メールの自動生成のための受信メールの分析手法の提案を行っている[11]．ユーザの受信 BOX メールを分析して，どのようなメールを信頼して開封しているか確認した上で，「普段のメールと似ているが，標的型攻撃メールだと気づくことができる不自然さ」をメールに盛り込むことによって，訓練メールが作成される．

Singh らや岩田らの研究は，攻撃者がビッグデータ技術や AI 技術の活用することによって，洗練されたソーシャルエンジニアリングを実行可能であることを示している．今後は，より高度なソーシャルエンジニアリングや標的型メールに対して備えることが重要であると考えられる．

6. まとめと今後の課題

本稿では，攻撃者が OSINT ツールを用いて攻撃対象の情報を収集していく過程を状態遷移モデルとして体系化し，その各状態において攻撃者が生成可能な標的型メールの類型化を行った．

得られた知見は，攻撃の深度の把握，情報を公開することでどのような標的型メールを受ける可能性があるかの想定，必要なセキュリティ対策の選定といったリスク分析や事前・事後対策に活用できると期待される．

今回は主に，「特定の個人を標的とした標的型メール攻撃」を中心に分析を行ったが，今後「組織を標的とした標的型メール攻撃」についても調査していく．また，今回は OSINT ツールで機械的に収集できる情報しか考慮に入れていなかったが，それらの情報から推測され得る情報や，ユーザが意図せず公開してしまっている情報（公開ファイルのメタデータなど）についての議論も必要であると考えられる．今後は，それらの情報も考慮に入れ，状態遷移モデルを改良していく．

謝辞　本研究を進めるにあたり，OSINT ツールの調査に協力して下さった西垣研究室の同期・先輩の皆様に感謝いたします.

参考文献

[1] Acquisti A, Gross R, Stutzman F (2014) Face recognition and privacy in the age of augmented reality. Journal of Privacy and Confidentiality 6(2): 1–20.

[2] Rainie, L., Kiesler, S., Kang, R., Madden, M., Duggan, M., Brown, S., & Dabbish, L. (2013). Anonymity, privacy, and security online. Pew Research Center, 5.

[3] Ball LD, Ewan G, Coull NJ. Undermining-social engineering using open source intelligence gathering, in: KDIR 2012: Proceedings of the 4th International Conference on Knowledge Discovery and Information Retrieval, Barcelona, Spain, October 4–7, SciTePress-Science and Technology Publications, 2012.

[4] Best, C. (2012, August). OSINT, the Internet and Privacy. In EISIC (p. 4).

[5] Buscador OSINT VM，入手先 <https://inteltechniques.com/buscador/index.html>，（参照 2017-08-03）

[6] Chen, S. E. R. E. N. A., Fitzsimons, G. M., Andersen, S. M. (2007). Automaticity in close relationships. Social psychology and the unconscious: The automaticity of higher mental processes, 133-172.

[7] 日本年金機構，不正アクセスによる情報流出事案に関する調査結果報告，入手先 <https://www.nenkin.go.jp/files/kuUK4cuR6MEN2.pdf>, (参照 2-17-08-07)

[8] Edwards, M., Larson, R., Green, B., Rashid, A., & Baron, A. (2016). Panning for gold: Automatically analysing online social engineering attack surfaces. Computers & Security.

[9] Silic, M., & Back, A. (2016). The dark side of social networking sites: Understanding phishing risks. Computers in Human Behavior, 60, 35-43.

[10] Singh, A., Thaware, V. (2017). WIRE ME THROUGH MACHINE LEARNING, Black Hat USA 2017, Black Hat (2017).

[11] 岩田一希，中村嘉隆，稲村浩，高橋修．標的型メール攻撃対策訓練における訓練メール自動生成のための受信メール分析手法の検討．マルチメディア，分散協調とモバイルシンポジウム 2016 論文集, 2016, 819-825.