Vol.2021-DPS-186 No.1
Vol.2021-CSEC-92 No.1
2021/3/15

フィッシング詐欺のビジネスプロセス分類

林 憲明[1] 唐沢 勇輔[2] 中村智史[3] 坂本美子[4] 柘植 悠孝[5] 岡田雅之[6]
加藤雅彦[7]

概要：フィッシング詐欺とは，ソーシャルエンジニアリングとクレデンシャル窃盗を組み合わせたオンライン詐欺の一つである．フィッシング詐欺には，ウェブサイトを模倣したもの，偽のアプリを利用したもの，電子メールやテキストメッセージ，音声メッセージを利用したものなど，様々な種類がある．このため，これら様々なタイプのフィッシング詐欺に対抗可能な本質的な方法は未だ確立されていないのが現状である．従って，効率的な対策方法を特定するために，フィッシング詐欺の全体像を把握することが不可欠である．本稿では，フィッシング詐欺をビジネスであると定義し，その営利活動におけるプロセスを分類することを試みる．その手法として，2 つの事例分析を実施した．その結果，提案手法が実際のフィッシング詐欺を特定するためのプロセスとして適用可能であることを確認した．提案手法を用いることで，フィッシング詐欺におけるプロセスを体系的に理解し，フィッシング詐欺の脅威を予測することが容易になった．

キーワード：フィッシング，詐欺，サイバー犯罪，サイバーセキュリティ，ビジネスプロセス分析，ダークマーケット

Business process classification of a phishing scam

Noriaki Hayashi[†1] Yusuke Karasawa[†2] Tomofumi Nakamura[†3] Yoshiko Sakamoto[†4] Yutaka Tsuge[†5] Masayuki Okada[†6] Masahiko KatoA[†7]

Abstract: Phishing, which combines social engineering and credential theft, is one of the most widespread online scams. There is many of types to undertake a phishing scam such as mimicking web sites, using fake apps and phishing via email, text message or voice messages. Because of this, we still don't find the essential way to stop against those various type of fishing attacks. In order to find the efficient way of countermeasure, it is necessary to determine an overall picture of phishing scams. We consider phishing a kind of business and attempt to classify the processes used. By conducting two case studies, we confirm that our proposed method is an applicable process for identifying actual phishing campaigns. The proposed method makes it easier to systematically understand the phishing process and predict the threat of a phishing scam.

Keywords: phishing, fraud, cybercrime, cybersecurity, business process analysis, dark market

1. はじめに

オンラインサービスを利用する消費者の増加 [1] に伴い，フィッシング詐欺と呼ばれるオンライン詐欺の種類が増加している．フィッシング詐欺は，最も普及しているオンライン詐欺の 1 つで，ソーシャルエンジニアリング [2] とクレデンシャル盗難を組み合わせたものである．

犯罪者は，フィッシング詐欺で集めた資格情報を転売することで収益を得ている．Anti-Phishing Working Group によれば，2019 年に世界で 162,155 件のフィッシングサイトが観測され，前年比 17%の増加が確認されている [3]．また，数百万ドル相当のユーザー名やユーザー情報が闇市場で販売されており，クレデンシャルの違法な売買が拡大していることが報告されている [4]．この問題に対し，複数のソリューション実装や，提案が行われている [5]．近年のフィッシング詐欺は，様々な犯罪者とプロセスが絡み合って成立している．Web サイトを模倣するもの，偽アプリを利用するもの，偽の電子メールやテキストメッセージを送信するなどの手法が用いられている．フィッシング詐欺に関する研究では，対策を論考するものは存在するが，フィッシング詐欺そのもののプロセスを体系的に整理した研究は少ない．よって，研究はまだ抜本的な対策に至っていない．より効果的な対策を検討するにあたり，まずフィッシング詐欺の全体的なプロセスを理解することが必要不可欠である．

本稿では，第 2 章で先行研究について説明し，第 3 章では我々が提案するフィッシング詐欺ビジネスプロセスの詳細を説明する．そして，第 4 章では 2 つのケーススタディを通じて提案プロセスの妥当性を実証する．第 5 章では提

1 トレンドマイクロ(株)
Trend Micro Incorporated
2 Japan Digital Design(株)
Japan Digital Design, Inc.
3 LINE(株)
LINE Corporation
4 (株)日立システムズ
Hitachi Systems, Ltd.
5 トビラシステムズ(株)
Tobila Systems Inc.
6 長崎県立大学
University of Nagasaki
7 長崎県立大学
University of Nagasaki

Vol.2021-DPS-186 No.1
Vol.2021-CSEC-92 No.1
2021/3/15

案された方法論を議論し，第 6 章で結論を述べる．

2. 先行研究

提案するフィッシング詐欺ビジネスプロセスと既存の分析との違いを明確にするために，以下の先行研究を確認した．

フィッシング詐欺の分類法について，Rastenis らは電子メールの分類法を提案し [6], Gupta らはフィッシング詐欺の歴史と攻撃者の動機に基づく分類法を提案した [7]. Oest らは，フィッシング詐欺における URL の種類と侵害されたインフラの利用との間に相関関係があることを明らかにし，フィッシング URL の分類法を提案している [8]. Abad らは, フィッシングネットワークとインフラの調査分析に基づき，フィッシング詐欺の手法と使用されたインフラとの関係を記述している．しかし，捕捉された情報がどのように扱われるかは考慮していない [9]. その代わりに，彼らは特定のフィッシング詐欺に焦点を当てていた．これに対して，Holz ら[4]は，盗まれたデジタル認証情報を取引する地下経済を研究することで，攻撃者の動機と地下市場の性質について提案した．しかし，この研究は，前述の文献と同様にフィッシング詐欺の包括的な全体像を提供するものではない．前述の研究は，研究者が確認できたフィッシング詐欺の現象を要約したものである．したがって，フィッシング詐欺が全体における，どの段階まで進行しているのかを捉えることはできず，これらの研究から効率的なフィッシング対策を見いだすことは困難である．

Pienta らは，フィッシングプロセスを明らかにするためにエコシステムの考え方を提唱した [5]. この研究では，フィッシング詐欺の経済的な目的，侵入前・侵入中・侵入後の攻撃サイクルを俯瞰し，本稿と同様の仮説を提示している．しかし，本稿では「フィッシング詐欺のビジネスプロセス」の仮説を立てるだけでなく，実例と照らし合わせて検証も行っている．これにより，本稿は，全体像をより明確にし，フィッシング詐欺に対する根本的な対策に資する提案ができると考える．

3. フィッシング詐欺ビジネスプロセス

フィッシング詐欺の最終的な目的は，利益を得ることである．サイバー犯罪者は，効率的に利益を得るために様々な手法を組み合わせ，ビジネスを行っていると概念化することができる．その手法としては，多くの人を騙して情報を入手したり，貴重な情報を入手したりすることが挙げられる．フィッシング詐欺の手法は様々存在するため，一連の流れをビジネスプロセスとして整理し，一つのルールで分析できるようにしている．ISO 15288:2015 [10] では，プロセスを「インプットをプロセスアクティビティにて処理し，アウトプットに変換する活動」と定義している．本稿では，フィッシング詐欺をビジネスとして捉え，ISO 15288:2015 に基づいたフィッシング詐欺ビジネスプロセスを提案する．フィッシング詐欺を「計画」「調達」「構築」「誘導」「詐取」「収益化」の 6 つの活動で定義し（図 1），3.1 より，各活動について説明する．

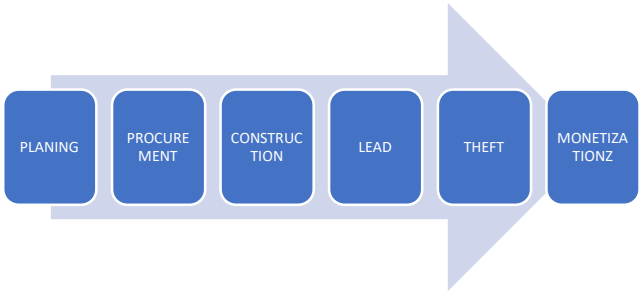

図 1　本稿でのフィッシング詐欺ビジネスプロセス
Figure 1　Our phishing business processes.

3.1 計画

この活動は，対象となる組織の選定，組織の調査など，フィッシング詐欺の計画を立てるために行われる．犯罪者は計画に基づき，次の行動に移す．

3.2 調達

この活動は，フィッシング詐欺を行うために必要なツールや情報を調達するために行われる．計画段階で決めた標的組織や利用者に応じて，必要なアイテムを闇市場や一般市場から調達を行う．まれに，犯罪者が自らアイテムを開発する場合もあり，その際には以下のいずれか，または複数のアイテムが含まれる．

- Phishing Kit の購入
- サーバ証明書の取得
- ドメインの取得
- 企業ブランドロゴやデータの取得
- 防弾サーバの準備
- ホスティングサーバの準備
- フィッシングメールの送信先一覧の取得
- 偽スマホアプリの入手

3.3 構築

この活動は，フィッシング詐欺に必要なシステムを構築するために行われる．以下のいずれかの行為を含む．

- フィッシング詐欺サイトの構築
- 正規サイトに侵入しフィッシング詐欺サイトを構築
- 詐取した ID などのデータを送信するサーバを準備

Paganini [11]は Phishing Kit の利用方法が説明されており，Newell [12]は Facebook のフィッシング詐欺サイトの構築方法を解説している．

3.4 誘導

この活動は，犯罪者が利用者へ状況に対する疑念を抱かれることなく，資格情報を入力させるフォームへと誘導するために行われる．

疑念を払拭する手段として，経路と文面が組み合わせられている．経路として，次の項目があげられる．

- 電子メール
- SMS，テキストメッセージ
- 検索エンジンポイズニング（SEO ポイズニング）
- 中間者攻撃などを利用した通信経路の汚染
- 偽アプリのインストール
- 類似ドメイン，酷似文字を使用したホモグラフ攻撃
- 短縮 URL
- QR コード

いずれも，攻撃を受ける側の何らかの行動によって誘導が行われている．

また，文面においては，利用者による合理的な思考プロセスを出し抜く工夫が施される．

Cialdini[13]は，人間の行動は基本的な心理学的原則に支配されており，次の 6 つの原則を利用すれば，相手から承諾や情報などを簡単に得ることができることを示している．

1. consistency（一貫性）
2. reciprocation（返報性）
3. social proof（社会的証明）
4. authority（権威）
5. liking（好意）
6. scarcity（希少性）

フィッシング詐欺の文面においても 6 つの原則に関する特徴をみることができる．

3.5 詐取

この活動は，ID やパスワード，二要素認証などの認証情報を提供するように利用者を騙すために行われる．

例えば，**エラー! 参照元が見つかりません。**の場合，誘導先のフィッシング詐欺サイトは正規のログインフォームを模している．このため，利用者は疑念を抱くことなく，要求されたメールアドレスやパスワードの入力が行われる．

3.6 収益化

この活動は，犯罪者が盗みだした情報を基に金銭的な利益を得るために行われる．具体的には，以下の方法で収益化を行う．

- ボーナスポイントやマイルを利用し別の商品を入手して転売する
- 盗んだ情報を転売する
- ID 不正利用により別口座に現金を振り込む

一旦，収益化のステップが成功すると，犯罪者はそのフィッシング詐欺の強化・拡大を狙う場合がある．改めて計画，標的の拡大を練り，同時に監視回避，対策ベンダーなどによる調査の妨害などの巧妙化策が講じられることがある．こうした対策を回避しようとする試みは，犯罪者の経験値が増えるにつれ，フィッシング詐欺ビジネスプロセスにおける計画活動に組み込まれる．

4. ケーススタディ

本稿では，2 つのフィッシング詐欺に関する実例について検討を試みている．事例 1 においては，同一の PhaaS 提供者による変遷に注目する．事例 2 においては，同一の標的を狙う詐欺師の変遷に注目する. それぞれの実例に対し，フィッシング詐欺ビジネスプロセスを適用し，フィッシング詐欺に対する全体像が明確となることを示す.

4.1 事例 1: 16Shop フィッシングキット

一連のフィッシング詐欺で犯罪者が使用しているスキームを論じるため, 2018 年 7 月から観測されている 16Shop フィッシングキット流通網によるキャンペーンをケーススタディとして使用する. 16Shop は分業体制によって広範囲に展開されているフィッシング詐欺である．従って，我々の提案が有効かどうかを確認するには最適なケーススタディの一つであると考える．

(1) 計画

16Shop において，二種類の犯罪者によって計画が企てられている．一つ目は一連の犯罪基盤となる 16Shop の供給者，二つ目はその犯罪基盤を利用し正当なサービスの利用者から ID やパスワードなど，アカウント情報を集め何らかの手段により換金を試みる需用者である．

(a) 犯罪基盤 16Shop「供給者」と計画の推定

「16shop-apple-v1.8.1」に残された「credit.txt」には，“Quote of the day:”のインドネシア語の記述が確認された．これらより，16Shop の開発者はインドネシア語の話者である「Riswanda/devilscream」（以下，Riswanda）と推定されている. McAfee Labs[14]によれば, 2017 年末, Riswanda は Facebook グループを立ち上げ，Apple をターゲットにした 16Shop のライセンスやサポートの提供を開始した．このことから，犯罪基盤の供給者による計画とその時期を推定することができる．

(b) 犯罪基盤 16Shop 「需用者」と計画の推定

我々はフィッシングメールに含まれるフィッシングサイトの URL について解析を行った．その結果，Punycode（RFC 3492）により,「xn--id-zb4axila5esc1e1f9bvhzd4a6fe」

（アップルジャパンのログイン ID）を表示する事例を確認した．このほかにも，日本語を含む事例を複数確認している．また，McAfee Labs によれば，16Shop フィッシングキャンペーンにおける最頻国が日本であったと報告している．このことから，犯罪基盤の需用者による計画において選定された標的を推定することができる．

(2) 調達

16Shop において調達とは，16Shop の供給者や需用者が，その計画に基づき，必要なツールやサービス，金銭や労働力を手配することである．本稿では，ツールやサービスに注目し，その分析を行った．

(a) バックエンドホスト

ホストの手配手段は主に二通りである．一つ目は，犯罪者自らがホスティングサービスと契約すること．二つ目は，正規のサイトを侵害し，そこへ自らのコンテンツを蔵置することである．いずれの場合においても，フィッシング詐欺サイトのコンテンツはホスティング会社によって撤去される可能性がある．

- 16Shop ライセンス管理サーバのホスティング先

16Shop では，16Shop を設置したサイトのトップページにアクセスすると，ライセンス管理サーバに対し鍵情報が送信され，キットの利用許諾状況が確認される．そこで，ライセンス管理サーバのドメイン名を特定し，16Shop 供給者によって調達されたホストを分析した．

いずれのサーバも DigitalOcean, LLC（AS14061）による運用であった．DigitalOcean は，他のクラウドサービスと比較した場合，月額の運用コストが最も低かった [15].

- 16Shop Admin パネルのホスティング先

16Shop 需用者は，用意したホストに対してキットを設置する．設置ホスト上の“/admin” ディレクトリに 16Shop Admin パネルの存在を確認することができる（図 2）．

我々は，120 件のユニークな 16Shop Admin パネルの URL を対象に分析を行った．

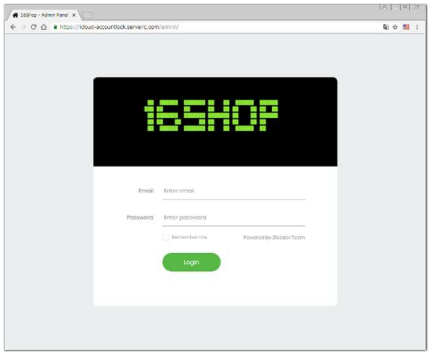

図 2　16Shop Admin パネル
Figure 2　16Shop admin panel.

まず，トップレベルドメイン（TLD）を分析した．その結果，“.com”が 66 件と全体の 57.4%を占めていた．

多くの 16Shop 需用者は，“.com”ドメインまたは generic TLD を調達していた．しかし，少数ではあるが new generic top-level domains（nTLD）が調達された．その背景として，日本を標的としている場合，“.jp” や “.tokyo” を調達することで，地理的表示に基づく信頼の誤認を狙っている可能性が推定できる．また，“.business” や “.support” は，正規サービスとの混同を生じさせる効果を期待していると推定できる．

次に，IP アドレスから経路広告された Autonomous System Number（AS）番号を分析した．その結果，AS14061 が 26 件（21.7%）を占めていた．

16Shop 需用者においても，AS14061 からの調達が最も顕著であった．ドメインの 50%が AS14061，AS46606，AS15169 の TOP3 サービスプロバイダによって占められていた．

一連の調査から PhaaS の供給者，需用者によるホストの調達先は類似傾向にあるといえる．

(b) フィッシングメール配信基盤

16Shop 基盤を利用したフィッシング詐欺サイトへ誘導するフィッシングメールのメッセージヘッダーについて分析した．結果として，“X-Sender: Sendinbox Professional”[16] を含む事例を確認した．また，Sendinbox の GitHub リポジトリや Sendinbox の流出ソースコード [17] などのアーティファクトも確認した．

Sendinbox の流出ソースコードにはコメント “Author. Eka Syahwan” の記載が含まれていた．Eka Syahwan は，マスメーラー購入者向けのコミュニティ “bmarket[.]or[.]id”（インドネシア，AS58477，TLS : Let's Encrypt Authority X3）と中継サーバを提供していたことを確認した．BMarket コミュニティが，フィッシング詐欺ビジネスを実現するための調達市場の役割を担っていると考える．

(3) 構築

16Shop において構築とは，16Shop の需用者が，供給者からから受け取ったキットをホスティングサービスへ展開し，設定ファイルにライセンス情報と利用者個別のパラメータを設定することである．

PHaaS として提供されている 16Shop の構築は簡易である．簡易であるゆえに，上位ディレクトリへ横断可能なケースなど設定上の不備がみられるフィッシング詐欺サイトも複数確認されている．このことから，16Shop 需用者について構築状況から技術習熟度が，設定値から帰属情報を推定することができる．

(4) **誘導**

(a) フィッシングメール上の工夫

To ヘッダにおける表示名として，ブランド名（Apple.com）やサービス名の文字列とともに，受信者に対してアクションを求める動詞（確認，通知）を組み合わせた事例を確認した．

また，本文中に「親愛なる %宛先メールアドレス%」の記述が見られるケースを確認している．これは宛先毎の最適化策とみられるが，本文の他の箇所においては宛先を特定する記述は確認できない．

フィッシングメールの宛先は不特定である．特定の組織を狙う傾向はみられなかった．差出人のドメインには「secure-appstore」文字列を含むケースを確認している．この点より，一連のフィッシングキャンペーンを実施するために用意したアカウントからの送信と推定する．

(5) **詐欺**

16Shop におけるフィッシングサイトでは，画像や CSS ページなど，元の Web サイトのリソースの一部を利用している．

被害者の接続環境に応じた言語表示を行う工夫を確認した．

また，同一フィッシングサイトへ 2 度目以降の接続を試みた場合，正規の Apple 社ウェブサイトへ転送する仕掛けも確認した．

(6) **収益化**

16Shop において収益化とは，犯罪者の立場によって収益を得るための仕組みは大きく異なる．そこで本稿では，犯罪インフラである 16Shop 供給者とその需用者について区分して検討する．

(a) 16Shop 供給者の収益化

16Shop は SaaS モデルを採用し，購入することで利用することができる．つまり，ユーザーは 16Shop を利用する期間を選択し，料金を支払い，機能の提供を受ける．

16Shop 供給者による囲い込み戦略として，継続的な機能強化を確認した．手法としては，標的ブランドの拡張，検出迂回機能，リアルタイムで更新されるダッシュボードによる統計機能などがあげられる．

また，これらの機能を階層化し，機能ごとに課金額を変更する仕組みが実装されている．このような戦略により，16Shop 供給者は需用者の利用状況に合わせた機能や料金プランを提供することで，需用者が 16Shop を継続して利用し，利益を得られるようにしている．

(b) 16Shop 需用者の収益化

16Shop 需用者は，16shop フィッシングキットを介して資格情報を収集し，その資格情報を使用した金銭詐取またはデジタルアイデンティティそのものを販売することで，収益化が可能となる．

日本サイバー犯罪対策センター（JC3）の調査 [18] によれば，窃取したクレジットカード情報を利用し，旅行サービス（宿泊施設，航空券，テーマパークのチケットなど）の不正転売に利用されている．商品を仕入れることなく先に出品し転売することが可能であるため，在庫リスクのないビジネス展開が可能である．

次に，デジタルアイデンティティを商品として販売する例を検討する．Top10VPN [19] の調査によれば，3 つのダークマーケットプレイス（Dream, Point, Wall Street Market）におけるアカウントの平均販売価格は，Apple ID が 15 ドル，クレジットカード情報が 50 ドルであった．

また，16Shop 需用者による直接販売の例として，「カーディングフォーラム」（クレジットカード情報やログイン情報の売買を行うオンラインフォーラム）での売買を依頼した[20].

「16Shop Apple Scam」から入手したデータを要求する投稿も確認している．

16Shop はカーディングフォーラムで一定の知名度と信頼を得ているが，直販モデルによるデジタルアイデンティティの販売は成約率が低いと考えられる [21][22].

4.2 事例 2: LINE を騙るフィッシング詐欺

一連のフィッシング詐欺で同一の標的を狙う犯罪者のアクティビティを論じるため，2016 年 10 月より観測を継続している LINE を騙るフィッシング詐欺をケーススタディとして使用する．

LINE は，LINE 株式会社が提供するコミュニケーションアプリ [23]．その基本機能は，無料の音声/ビデオ通話/チャットである．

LINE を騙るフィッシング詐欺とは，コミュニケーションアプリ LINE のアカウントを盗む目的で Web アプリを構築し，標的を URL に誘導し，盗んだアカウントを使って金銭を要求する，これら一連の行為とする．そこで，一連の LINE を騙るフィッシング詐欺に対して本プロセスの適用を試みる．なお本稿では，日本国内の LINE アカウント保有者を標的としたフィッシング詐欺のみを対象とする．

(1) **計画**

(a) LINE 利用者を標的とする動機

LINE 利用者の状況を LINE 株式会社が公表する資料 [24][25] より分析した．2020 年 4 月末時点での公表値を整理した結果，次の特徴を得た．月間アクティブユーザー

（MAU）の規模は約 8300 万人で，日本の人口の 65%に相当した．日本市場に限定すれば，属性を問わず大多数の人が毎日利用しており，日常的に利用されているサービスといえる．

試行回数を増やし続けられる標的は犯罪の成功確率を高め，犯罪者にとって成功時の予測メリット（予測獲得利益×予測成功確率）を高めることができる．

標的ブランドとしての LINE は利用者への誘導を大量に仕掛けることが可能である．従って，犯罪者が無差別なアカウント情報の収集を狙っている場合，LINE 利用者を標的とすることは予測成功確率の観点から合理的な選択であるといえる．

(2) 調達

LINE 事例における調達では，フィッシング詐欺師による Web アプリケーション，URL，ホスティングの調達に注目し，その分析を行った．

(a) Web アプリケーション

Web アプリケーションの基本機能は一貫している．ユーザーインターフェース（UI）は正規の LINE に実装されている認証画面を模倣しているが，UI を構成する画像ファイルや JavaScript，CSS を直接参照しているわけではない．

2016 年 10 月以降，正規の LINE のデザインや仕様の変更を追随するように修正が続けられている．

Web アプリケーションは，ThinkPHP [32][33] を使用して開発されている．ThinkPHP は中華人民共和国で普及している．また，フレームワークに依存しない実装部分に残されたコメントが簡体字で記載されている．開発者には中華人民共和国の言語話者が含まれていると考える．

(b) URL

我々はフィッシングサイトで使用されている URL を分析した．このドメインは，Web アプリケーションが動作を開始する 1 週間から 1 日前に調達されていた．このドメインを含む FQDN に使用されている文字列は，「linerk.cn」，「linkebn.cn」，「linkeuk.cn」など，一定期間にわたって類似性を持つことを確認した．しかし，この類似性は繰り返されることがない．なお，証明書も FQDN ごとに調達されている．

ドメインの TLD を集計し，14 種類を確認した．上位 3 件は「.cn」（437 件 43%），「.com」（393 件　39%），「.me」（64 件 6%）であった．また，IP アドレスのみでドメインを持たない運用も 8 件確認した．

使用率上位 3 件のドメインは，一定期間で優位性が入れ替わっていた．すなわち，2016 年 10 月から 2017 年 3 月までは「.me」が最も高く，2017 年 3 月から 2018 年 8 月までは「.cn」が最も高く，執筆時点では 2018 年 8 月から 2020 年 5 月までは「.com」が最も高くなっていた．

(c) ホスティング

我々は Web アプリケーションがインストールされているホスティングサーバを分析した．IP アドレスからの逆引きにより，51 種類の ASN と Org-name を収集した（図 16 参照）．上位 3 件は AS135544（286 件 28%），XUANKANG INTERNATIONAL CO. LIMITED（201 件 20%），AS55933（85 件 8%）であった．なお IP アドレスの記録漏れが 9 件ある．このうち，CLOUDFLARENET は CDN（コンテンツデリバリーネットワーク）を利用している．他に CDN を利用している例は確認されておらず，その他のケースでは，フィッシングサイトがレンタルサーバー上で直接ホストされていた．

(3) 構築

URL とインフラを利用した Web サービスを構築したのは，誘導メールを送信した前日からその日の午前中までであった．この場合，ホスティング Web サービスの初期設定でみられるページで応答する．誘導メールを送信した日の午前に Web アプリケーションが設置されていた．Web アプリケーションの設置環境下には認証機能付きページがあり，Web アプリケーションが起動した状態でブラウザからの操作が可能であることを示している．

Web アプリケーションのインストール後，これまで Web サービスでは見られなかった動作であるフィッシング対策のためのアクセス制御を確認した．確認された具体例として，クラウド型ファイアウォールによる遮断や，Web アプリケーションのページに応答せずに HTTP 404 などの無害な情報を返すなどがみられた．

(4) 誘導

(a) フィッシングメール上の工夫

Web アプリケーションの動作開始前に配信されたフィッシングメールの分析を行った．このとき誘導先の URL が間違っているケースを確認した．誤った誘導先 URL を含むフィッシングメールは配信され続け，その訂正は翌日以降に実施されていた．Web アプリケーションが動作を停止した場合でもメールは配信され続けていた．これらの点から Web アプリケーションの運営者とメール配信の運営者が異なる可能性を示している．

疑念払拭の手法として，LINE 株式会社の公式な通知であると装っていることが確認できる．ただし，その手口は送信者のメールアドレスと表示名を実在しない文字列に設定するのみであった．

誘導メールの件名や本文の内容は，受信者に LINE アカウントが利用できなくなると誤認させる旨が書かれていた．このように，受信者にアカウントが使えなくなると誤解さ

Vol.2021-DPS-186 No.1
Vol.2021-CSEC-92 No.1
2021/3/15

せる脅しは一貫している．本文はリッチテキスト形式または HTML 形式が使用されていた．誘導先の URL を目視によって確認できないように，無害な文字列のハイパーリンクへ誘導先の URL が設定されていた．また，LINE 株式会社やグループ会社が過去に公開している文章を引用するなどの工夫も見られた．

(b) LINE の機能による誘導

LINE 自体の機能を用いた誘導プロセスを分析した．この種の誘導プロセスは，2020 年 2 月から 1 ヶ月弱の期間で確認された[26]．盗まれた LINE アカウントの権限で，トーク機能やタイムライン機能を使って URL が拡散された．メールで確認された文言は転用されておらず，盗まれた LINE アカウントの属性（年齢や性別など）をもとに内容の最適化が図られていた．

(5) 詐取

Web アプリケーションは利用者にメールアドレスとパスワード，電話番号，電話番号に届く認証番号の 4 つの情報入力を促す．

図 3 は，LINE フィッシングの流れを例示している．

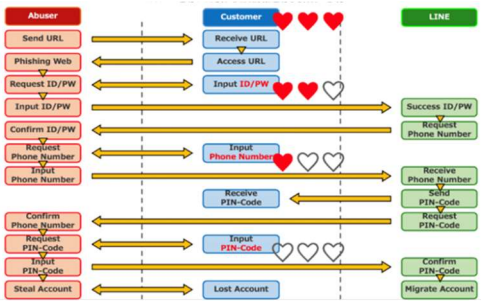

図 3　LINE フィッシングのユースケース
Figure 3　Line phishing use case.

LINE 利用者が 4 つの情報をすべて入力すると，フィッシング詐欺の実行者が管理する端末で LINE アカウントが利用可能になる．

LINE アカウントの取得に成功した後，Web サイトでは，被害者にしばらく待つよう促すメッセージが表示する場合がある．この待ち時間は，被害者がフィッシング詐欺だと気づくのを遅延させる効果がある．

(6) 収益化

2 種類の収益化行動を確認した．1 つ目は，金銭情報を盗むことを目的とした行動．詐欺師は，盗まれた LINE アカウントに友だちとして登録されているアカウントに対してソーシャルエンジニアリングを実行する．詐欺師は友人にプリペイド式の電子マネーの購入を依頼し，その電子マネーに関する秘密情報を教えるように誘導する．この手口は，ソフトウェアではなく，犯罪者が被害者に対し直接働きかけることを確認した．2 つ目は，より多くの LINE のアカウントを詐取することを目的とした行動．詐欺師は盗んだ LINE アカウントの友だちとして登録されているアカウントに対してもソーシャルエンジニアリングを実行する．今度は詐欺師が直接会話やフィッシングサイトへの誘導によって LINE アカウントの引き継ぎに必要な情報を聞き出す．

5. 考察

本稿では，我々が提案したフィッシング詐欺ビジネスプロセスの分類を，観測できた 2 つのケーススタディに適用した．6 つの活動におけるプロセスを体系的に理解し，各活動にて結果を引き起こす因子を明らかにするに至った．計画における因子は，犯行に至る動機，機会，標的，詐欺の開始時期，誘導試行回数の期待値，詐取を狙う eKYC である．調達の因子は，調達先の傾向，調達サービスを支えるコミュニティの存在である．構築の因子は，技術習熟度，帰属情報，構築期間，設置のタイミングである．誘導の因子は，疑念払拭の手法，作業の品質である．詐取の因子は，被害認知に至るまでの引き延ばし工作である．最後に，収益化の因子は換金対象，二次被害である．表 1 にフィッシング詐欺ビジネスプロセスと判明した因子の対応表を示す．

表 1　フィッシング詐欺ビジネスプロセスと因子の対応表
Table 1　Phishing Business Process and Factor Correspondence Table.

フィッシング詐欺ビジネスプロセス	16Shop事例分析により判明した因子	LINE事例分析により判明した因子
計画	動機、機会、標的、詐欺の開始時期、詐取を狙うeKYC	動機、機会、標的、誘導試行回数の期待値、詐取を狙うeKYC
調達	調達先の傾向、調達サービスを支えるコミュニティ	調達先の傾向
構築	技術習熟度、帰属情報	構築期間、設置のタイミング
誘導	疑念払拭の手法、作業品質	疑念払拭の手法、作業品質
詐取	被害認知に至るまでの引き延ばし工作	被害認知に至るまでの引き延ばし工作
収益化	換金対象、二次被害	換金対象

このように，両ケースにおいて我々のフィッシング詐欺ビジネスプロセスの適用が可能であり，その適用により脅威を予測する上で重要な因子を明らかにするに至った．

6. 結論

本稿では，フィッシング詐欺をビジネスであると定義し，過去の事例を分析することでプロセスを分類した．事例研究を行うことで，提案手法が実際のフィッシングキャンペーンに普遍的に適用可能なプロセスであることを確認し，フィッシング詐欺を体系的に理解し，各活動にて結果を引

き起こす因子を明らかにすることで，脅威を予測することが容易になることを確認した．

今後の研究では，活動ごとの対策の有無と対策の有効性を評価する．

(1) 提案プロセスの妥当性

本稿では，フィッシング詐欺の全体像を明らかにするために，フィッシング詐欺をビジネスとして捉え，そのプロセスの解明を試みた．具体的には，第 4 章では，2 つの事例についてプロセスを明らかにし，これらのフィッシング詐欺の概要を示した．実際に発生したいずれのケースにおいても，計画から収益化までの活動の存在が確認され，提案プロセスによるフィッシング詐欺の活動分類の活用が検証された．これらの結果から，フィッシング詐欺をビジネスと定義することは妥当である．

(2) 提案プロセスの有効性

フィッシング詐欺は，被害が発生した時やフィッシングメールが確認された時に顕在化する．初期の段階では行動が明らかになることが少ないため，被害が発生してから対策が明らかになる傾向がある．提案するプロセスは，フィッシング詐欺の全貌を明らかにすることで，2 つのメリットがある．1 つ目は，被害が発生する前に活動を認識しやすくなることである．2 つ目は，途中で疑われる事象が発生した場合，それ以前の活動の存在を確認することで，それがフィッシング詐欺に関連した活動であるかどうかを推察することが可能となる．

(3) 今後の方向性

本稿では，フィッシング詐欺をビジネスとして捉え，人やモノを使ってお金を稼ぐプロセスを明らかにしている．しかし，実際の対策を考案するためには，それぞれの活動におけるアクター（フィッシング詐欺）とモノ（武器）を明確にする必要がある．これを今後の研究における方向性として示す．

参考文献

[1]“2017 Global Online Consumer Report”. https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/01/the- truth-about-online-consumers.pdf
[2] “Avoiding Social Engineering and Phishing Attacks”. https://www.us-cert.gov/ncas/tips/ST04-014
[3] “Phishing Activity Trends Report, 4th Quarter 2019”. https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf
[4] “Learning More about the Underground Economy: A Case-Study of Keyloggers and Dropzones” . https://www.researchgate.net/publication/220270794_Learning_More _about_the_Underground_Economy_A_Case-Study_of_Keyloggers_and_Dropzones
[5] “A Taxonomy of Phishing: Attack Types Spanning Economic, Temporal, Breadth, and Target Boundaries” . https://aisel.aisnet.org/wisp2018/19/
[6] "E-mail-Based Phishing Attack Taxonomy”. https://www.mdpi.com/2076- 3417/10/7/2363/pdf
[7] “Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions”. https://www.researchgate.net/publication/317044956_Defending_against_Phishing_Attacks_Taxonomy_of_Methods_Current_Issues_and_ Future_Directions
[8] “ Inside a Phisher’s Mind: Understanding the Anti-phishing Ecosystem Through Phishing Kit Analysis”. https://docs.apwg.org/ecrimeresearch/2018/5349207.pdf
[9] “The Economy of Phishing: A Survey of the Operations of the Phishing Market”. https://www.cloudmark.com/releases/docs/the_economy_of_phishing.pdf
[10] ISO/IEC/IEEE 15288:2015. Systems and software engineering−System life cycle processes
[11] “How attackers use phishing kits for their campaigns”. https://securityaffairs.co/wordpress/33658/cyber-crime/attackers-use-phishing-kits-campaigns.html
[12] “Complete Guide to Creating and Hosting a Phishing Page for Beginners”. https://null-byte.wonderhowto.com/forum/complete-guide-creating-and-hosting- phishing-page-for-beginners-0187744/
[13] B. Robert B. Cialdini. Influence: The Psychology of Persuasion. December 26, 2006
[14] “16Shop Now Targets Amazon” . https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/16shop-now-targets-amazon/
[15] “DigitalOcean” . https://www.digitalocean.com/pricing/calculator/
[16] https://urlscan.io/result/d7a17622-9d20-47aa-b973-b5c02cf23e2b
[17] https://github.com/leakedtools/sendinbox
[18] “Implementation of measures against illegal travel” . https://www.jc3.or.jp/topics/travel_fraud.html
[19] “TOP10VPN DarkWebMarketPriceIndex(USEdition)” . https://www.top10vpn.com/research/investigations/dark-web-market-price-index-feb-2018-us/
[20] “Carder.tv”. http://carder.tv/index.php?/topic/6680-want-japanese-cc- fullzdob%E3%80%80data/
[21] “丝绸之路担保交易平台场 (Eng. Silk Road Chinese Escrow Platform) ”. hxxp[:]//shoptwgap2x3xbwy[.]onion
[22] “暗网交易平台-时光之路(Eng. Dark Net Trading Platform — Road of Time) ”. hxxp[:]//v7osuzczwawdb2fl[.]onion
[23] https://linecorp.com/
[24] “LINE for Business 媒体資料”. https://www.linebiz.com/jp/download/
[25] “LINE for Business 統計”. https://www.linebiz.com/system/files/jp/download/LINE%20Business %20Guide_202001-06.pdf