第92回CSEC合同研究発表会-情報処理学会,
2021年3月15日

フィッシング対策協議会
Council of Anti-Phishing Japan

フィッシング詐欺のビジネスプロセス分類

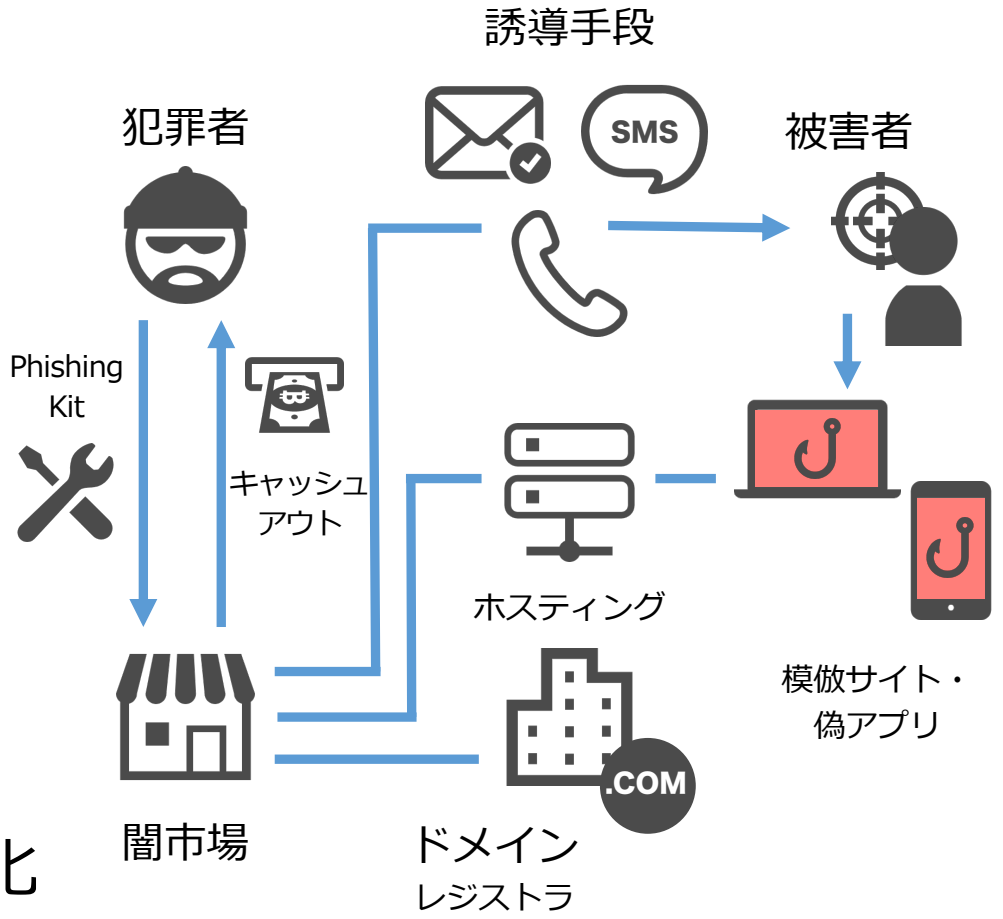
フィッシング対策協議会 学術連携プロジェクト

**林憲明, 唐沢勇輔, 中村智史, 坂本美子,
柘植悠孝, 岡田雅之, 加藤雅彦**

研究背景：根本的な対策に至っていない

拡大を続けるフィッシング詐欺被害

- **フィッシングサイトの件数**
  全世界で162,155件観測, 前年比17%増*1
- **利用者情報の違法取引が拡大**
  闇市場で最も活性な商品は盗難アカウント
  600フォーラムで4,954,825スレッドを観測*2
- **合理的かつ効率的な利益追求**
  サービス, 配信, マネタイズ 役割の分業, 複雑化



フィッシング詐欺の全体的なプロセス理解が必要不可欠

*1 “Phishing Activity Trends Report, 4th Quarter 2019”. https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf
*2 ”Shifts in Underground Markets”. https://documents.trendmicro.com/assets/white_papers/wp-shifts-in-the-underground.pdf

フィッシング対策協議会
Council of Anti-Phishing Japan

先行研究における課題

根本的な対策に資する提案が必要

- **分類法の検討**
  電子メール*1, フィッシングURL*2
- **観測結果に基づく体系化**
  フィッシング詐欺の歴史・動機*3
  犯罪利用されたインフラの調査*4
  詐取情報の取引市場の調査*5

- **未解決な課題**
  包括的な全体像の提供に至っていない

  フィッシング詐欺全体における進行段階を捉えていない

  実例との照らし合わせによる検証が行われていない

プロセスを俯瞰し，進行段階の特定を実現．仮説の検証を実施．

*1 "E-mail-Based Phishing Attack Taxonomy". https://www.mdpi.com/2076- 3417/10/7/2363/pdf
*2 "Inside a Phisher's Mind: Understanding the Anti-phishing Ecosystem Through Phishing Kit Analysis". https://docs.apwg.org/ecrimeresearch/2018/5349207.pdf
*3 "Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions". https://www.researchgate.net/publication/317044956_Defending_a gainst_Phishing_Attacks_Taxonomy_of_Methods_Current_Issues_ and_ Future_Directions
*4 "Learning More about the Underground Economy: A Case-Study of Keyloggers and Dropzones" . https://www.researchgate.net/publication/220270794_Learning_M ore _about_the_Underground_Economy_A_Case-
*5 "The Economy of Phishing: A Survey of the Operations of the Phishing Market". https://www.cloudmark.com/releases/docs/the_economy_of_phishing.pdf

研究目的：ビジネスプロセスで分類

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る

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．ISO 15288:2015

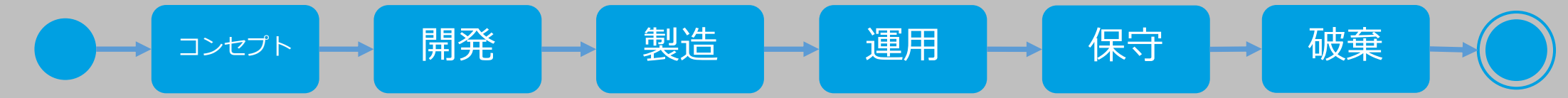


図: 一般的なシステムライフサイクルフェーズ

フィッシング詐欺をビジネスとして捉える．6つの活動を定義

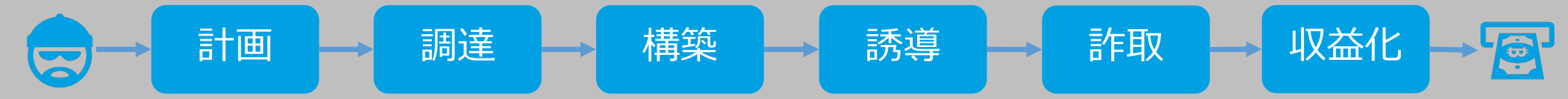


図: フィッシング詐欺ビジネスプロセス

フィッシング詐欺ビジネスプロセスの提案．共通ルールで分析

フィッシング対策協議会
Council of Anti-Phishing Japan

研究方法：ケーススタディ

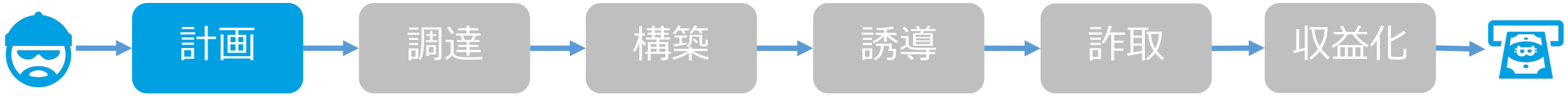
フィッシング詐欺ビジネスプロセスを2つの実例に対し照合

- **事例1: 16Shop フィッシングキット**
  同一の**「Phishing as a Service (PHaaS)」供給・需要者**による変遷に注目
- **事例2: LINEを騙るフィッシング詐欺**
  同一の**「標的」を狙う詐欺者**の変遷に注目

	16Shop事例分析	LINE事例分析
観測期間	2018年7月 – 2018年8月	2016年10月 – 2020年5月
調査対象数	115 URLs （無作為に抽出）	1,025 URLs
TLD	22 件	14件
AS番号	39 件	51件

※件数はすべて重複を除く、ユニーク件数

研究結果: 計画



16Shop事例分析

- **PHaaSの供給者と需要者**
  供給者はインドネシア語の話者.
- **標的に応じたカスタマイズ**
  標的（日本人, 偽装サービス）に応じたPHaaSのカスタマイズを観測.
  成功経験をもとに標的が拡張.

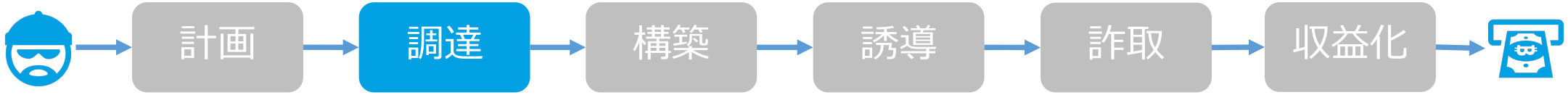
観測から標的が読み取れる

LINE事例分析

- **公表値から利用者数を考察**
  日本の人口の65%がLINEを利用.
- **無差別なアカウント収集**
  試行回数を増やし続けられる.
  予測メリットを高めることが可能.

狙われた理由が読み取れる

研究結果: 調達



16Shop事例分析

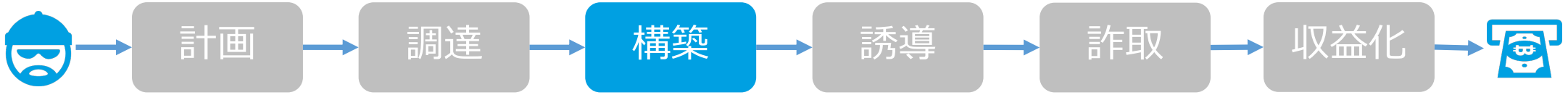
- **サイトのホスティング先**
  維持費を重視した選択を観測.
- **誘導手段（メール配信）**
  配信サービスのユーザーグループによる支援体制を観測.

LINE事例分析

- **サイトのホスティング先**
- **特定のOSSを利用**
  帰属に繋がる偏りのある傾向を観測.
- **誘導URL**
  取得から展開までの期間を観測.
  文字列に規則性を観測.

反復作業の効率化, コスト削減を重視した調達が読み取れる

研究結果: 構築



16Shop事例分析

- **犯罪者の技術習熟度**

  PHaaSの構築は簡単.

  ディレクトリ横断可能な設定不備を複数観測.

  需用者の技術習熟度は必ずしも高くない.

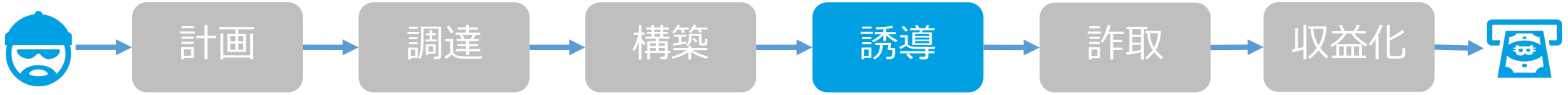
LINE事例分析

- **作業期間の特定**

  Webアプリケーションの展開からコンテンツの配置までの空白時間を観測.

犯罪者の技術習熟度を把握. 調達から構築までの期間を特定.

研究結果: 誘導



16Shop事例分析

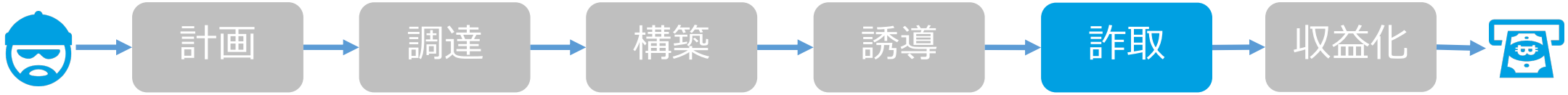
- **フィッシングメール上の工夫**
  Toヘッダの表示名にブランド/サービス名とアクションを求める動詞（確認, 通知）.
  本文に宛先毎の最適化策.
  「親愛なる %メールアドレス%」

LINE事例分析

- **分業体制を示す痕跡**
  Web Apps停止後もメール配信継続.
- **LINE機能による誘導**
  トークまたはタイムライン機能を使ってURLの拡散を確認.

利用者の合理的な思考プロセスを出し抜く文面と経路を確認.

研究結果: 詐取



16Shop事例分析

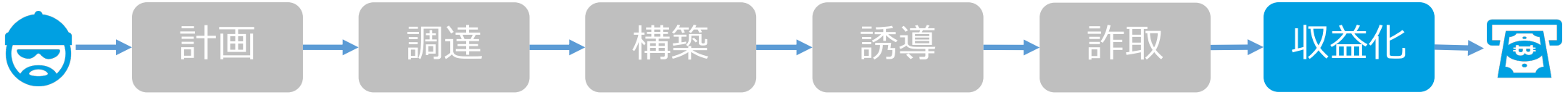
- **詐取の標的**
  氏名, 住所, メールアドレス, パスワード, クレジットカード情報
- **被害認知に至るまでの引き延ばし工作**
  2度目以降の接続を試みた場合, 正規サイトへの転送.

LINE事例分析

- **詐取の標的**
  メールアドレス, パスワード, 電話番号, 電話番号に届く認証番号
- **被害認知に至るまでの引き延ばし工作**
  被害者に対して待機を促すメッセージ表示（処理中と誤認させる）.

フォーム模写のみならず, クローキング/意図的な遅延処理を確認

研究結果: 収益化



16Shop事例分析

- **PHaaS供給者の収益化**
  利用料収入, オプション機能の提供により継続利用を促す.
- **PHaaS需用者の収益化**
  資格情報を利用した金銭詐取またはID等の転売.

LINE事例分析

- **金銭情報を盗む行動**
  被害者へ接触し電子マネーの購入依頼, 秘密情報の提供を要求.
- **LINEアカウント情報の更なる取得**
  詐取に成功したアカウントを踏み台とした誘導メッセージの配信.

盗んだ情報の転売の他, 犯罪の強化・拡大を狙う傾向を確認

考察

プロセスの体系的な理解により，各段階の主要因子を特定

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

主要因子の観測により進行段階の特定，脅威予測/対策を支援する

※補足　**水色**の表記はどちらか一方の事例のみで判明した因子

結論

フィッシング詐欺をビジネスと捉えることは妥当であり有効

- **提案プロセスの妥当性**

  2つの実例検証の結果, いずれにおいても「計画」「調達」「構築」「誘導」「詐取」「収益化」までの存在を確認

- **提案プロセスの有効性**

  1. 被害が発生する前より疑わしき活動を定義することが可能
  2. 犯罪者による準備行為を認知した際にその内容を精査することでフィッシングに関連した活動であるかどうかを推察可能

プロセスを俯瞰し, 進行段階の特定を実現. 仮説の検証を実施.