JPAAWG 5th General Meeting
アカデミック領域におけるフィッシング詐欺対策研究の
最新動向と研究事例紹介

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

学術研究WG活動と研究動向の紹介

フィッシング対策協議会 副運営委員長
学術研究WG 主査
唐沢勇輔

アジェンダ

- 自己紹介
- フィッシング対策協議会について
- 学術研究WGの活動
- フィッシング詐欺研究の最新動向

アジェンダ

- **自己紹介**
- フィッシング対策協議会について
- 学術研究WGの活動
- フィッシング詐欺研究の最新動向

自己紹介

唐沢 勇輔（からさわ ゆうすけ）

- **フィッシング対策協議会 学術研究WG 主査（本日の肩書）**
- Japan Digital Design, Inc Head of TDD / VP of Security（本業）
  https://japan-d2.com/
- 日本ネットワークセキュリティ協会(JNSA) 社会活動部会 副部会長
- OpenID ファウンデーション・ジャパン 理事

アジェンダ

- 自己紹介
- **フィッシング対策協議会について**
- 学術研究WGの活動
- フィッシング詐欺研究の最新動向

フィッシング対策協議会について

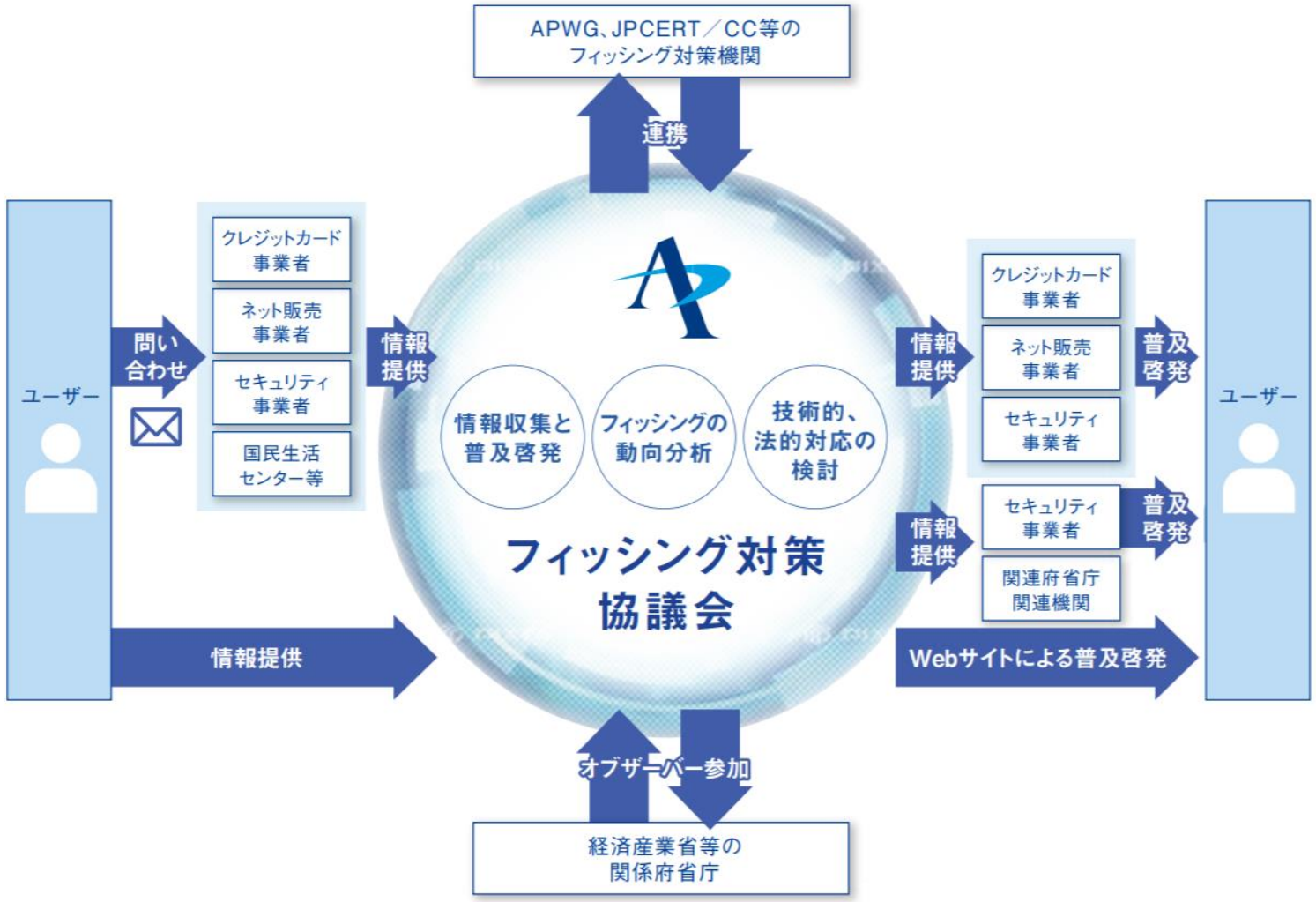
概要

- 設立　2005年4月
- 名称　フィッシング対策協議会 / Council of Anti-Phishing Japan
- 目的　フィッシング 詐欺に関する事例情報、技術情報の収集及び提供を中心に行うことで、日本国内におけるフィッシング詐欺被害の抑制を目的として活動
- 会員+オブザーバー 118　※2022年11月時点
  - 正会員：91、リサーチパートナー：5、関連団体：15
  - オブザーバー：7組織
  - 金融機関、信販会社、オンラインサービス、セキュリティベンダーなど

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

フィッシング対策協議会について

活動内容



情報発信（事業者／一般向け）
- 緊急情報／お知らせ
- ガイドライン改訂（WG活動）
- フィッシングレポート 等

学術研究
- フィッシングサイト早期検知
- フィッシング詐欺の全容解明

会員間の情報交流
- 総会／情報交換会
- 勉強会
- ワーキンググループ活動 等

啓発活動
- フィッシング対策セミナー
- STOP.THINK.CONNECT.

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

ぜひTwitterフォローしてください

https://twitter.com/antiphishing_jp

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

アジェンダ

- 自己紹介
- フィッシング対策協議会について
- **学術研究WGの活動**
- フィッシング詐欺研究の最新動向

学術研究WG活動背景

- 各事業者、利用者ともにフィッシング詐欺への対応コストが増加
- フィッシングサイトの稼働時間もどんどん短くなっており、後追い対応では追いつかない
- 少し長い目で対策を研究することが必要ではないか？
- 我々事業者だけでなくアカデミック領域との連携も必要ではないか？

今までの活動

- **2018年3月**　暫定PJとして活動開始し、情報処理学会で発表
  - フィッシング対策協議会と長崎県立大学の 共同研究プロジェクト「フィッシングサイトの早期検知に関する研究」について
- **2021年3月**　「フィッシング詐欺のビジネスプロセス分類」公開
  - 第92回コンピュータセキュリティ合同研究発表会にて発表
- **2021年6月**　WGとして恒久的な活動へ

研究紹介

「フィッシング詐欺のビジネスプロセス分類」

:: 協議会からのお知らせ

「フィッシング詐欺のビジネスプロセス分類」を公開 (2021/03/16)

2021年03月16日

協議会は、長崎県立大学との 共同研究プロジェクト の活動成果の１つとして、学術論文「フィッシング詐欺のビジネスプロセス分類」を公開しました。

この内容は、3月15日(月)に第186回マルチメディア通信と分散処理・第92回コンピュータセキュリティ合同研究発表会にて発表いたしました。

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、様々な種類があります。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す。したがって、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す。本研究では、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ました。その手法として、2 つの事例分析を実施しました。結果として、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することができました。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りました。

フィッシング詐欺のビジネスプロセス分類（論文） (PDF : 817KB)

フィッシング詐欺のビジネスプロセス分類（CSEC発表資料） (PDF : 1.10MB)

研究紹介：フィッシング詐欺の全体プロセス

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

研究紹介：ケーススタディを実施

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)」提供者**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

研究紹介：考察

体系的な整理で、各段階の結果を引き起こす主要因子を特定

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

研究紹介：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

アジェンダ

- 自己紹介
- フィッシング対策協議会について
- 学術研究WGの活動
- **フィッシング詐欺研究の最新動向**

最近のフィッシング研究動向

- 過去２年間(2021-2022)に公表された論文をリサーチ
- 英語圏の研究は**250件**の論文が公開されている
  - IEEE ExplorerでTitle/Key Wordに”Phishing”が入っているもの
- 日本でフィッシング詐欺に関する論文は**15件**（少ない！）
  - 情報学広場で抄録に「フィッシング」が含まれるもの
- 傾向
  - 海外論文は何はともあれ機械学習による検出精度向上（URLベースの判定、メール判定などなど）
  - COVID-19詐欺サイトに特化したものも数件あった
  - 変わらないのは、対策手法に関するものが多いという点、ユーザビリティ/アウェアネスに類するものがあるという点

論文紹介①

- GUI-Squatting Attack: Automated Generation of Android Phishing Apps
  - 著者：Sen Chen; Lingling Fan; Chunyang Chen; Minhui Xue; Yang Liu; Lihua Xu
  - Androidプラットフォーム上でフィッシングアプリを自動生成するという攻撃手法
  - Repackingより容易で、偽アプリの対策手法をすべてバイパスできる
  - ただし、偽アプリをユーザーにインストールさせる手法は本研究のスコープ外

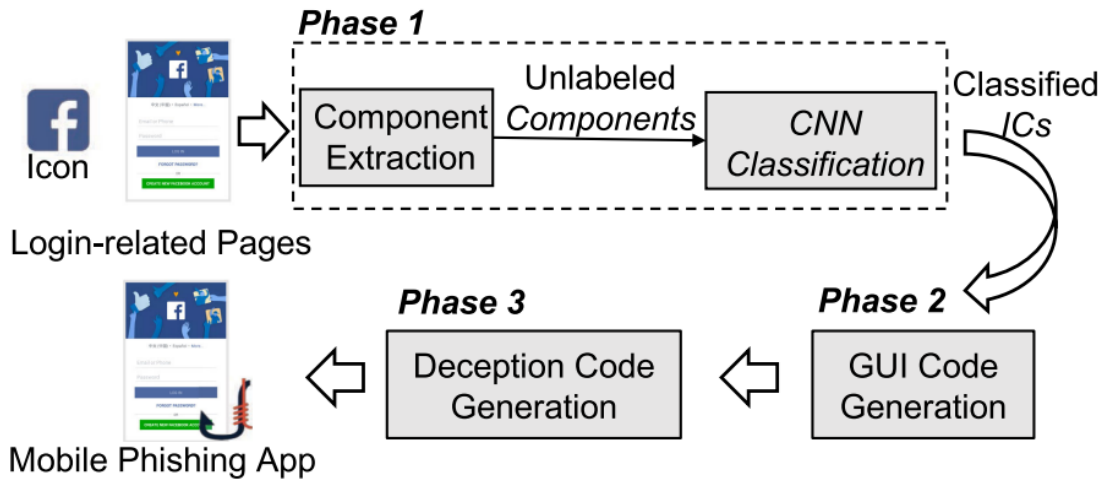


Fig. 1. Workflow of our approach (ICs is short for interactive components).

論文紹介②

- An Empirical Analysis of Machine Learning Techniques in Phishing E-mail detection
- 著者：Arriane Livara; Rowell Hernandez
- メールが正規のものかフィッシングかを判定する機械学習モデルの提案。99%の精度でフィッシングメールを見分けることに成功。

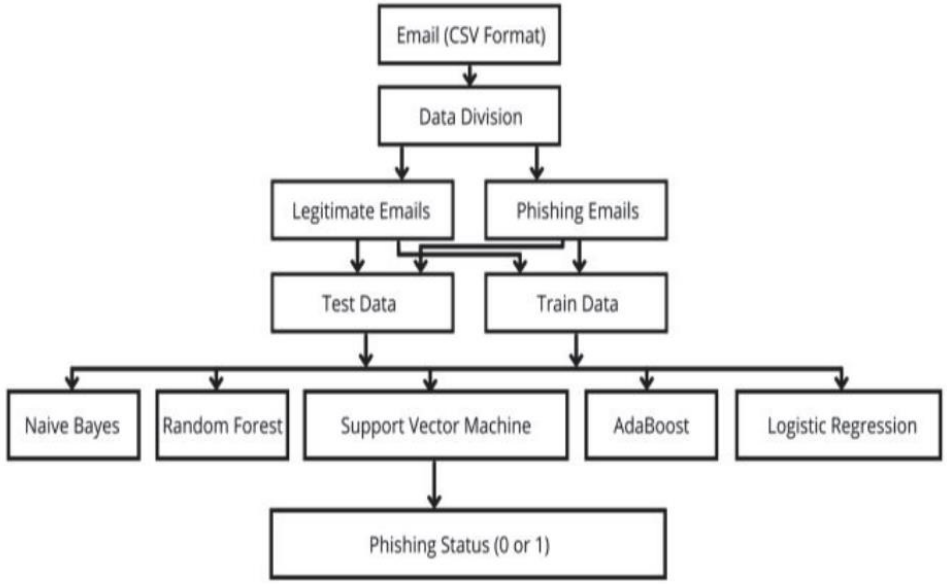


Fig. 1. Model Architecture

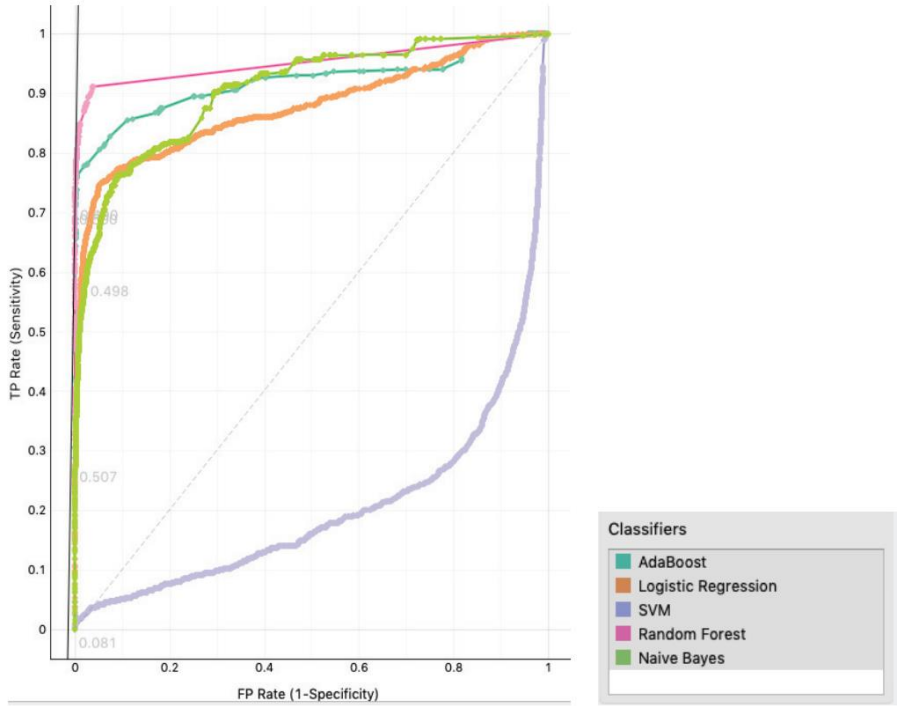


Fig. 7. ROC Analysis

論文紹介③

- 安物に悪者が出る:構築コストに基づく悪性ウェブサイト検知手法
  - 著者：伊藤 大貴、高田 雄太、神薗 雅紀
  - フィッシング，マルウェアホスト，フェイクニュースの3種類の悪性サイトについて構築コストを推定
  - 8割以上の精度で安物と判定できている（フィッシングは9割以上）

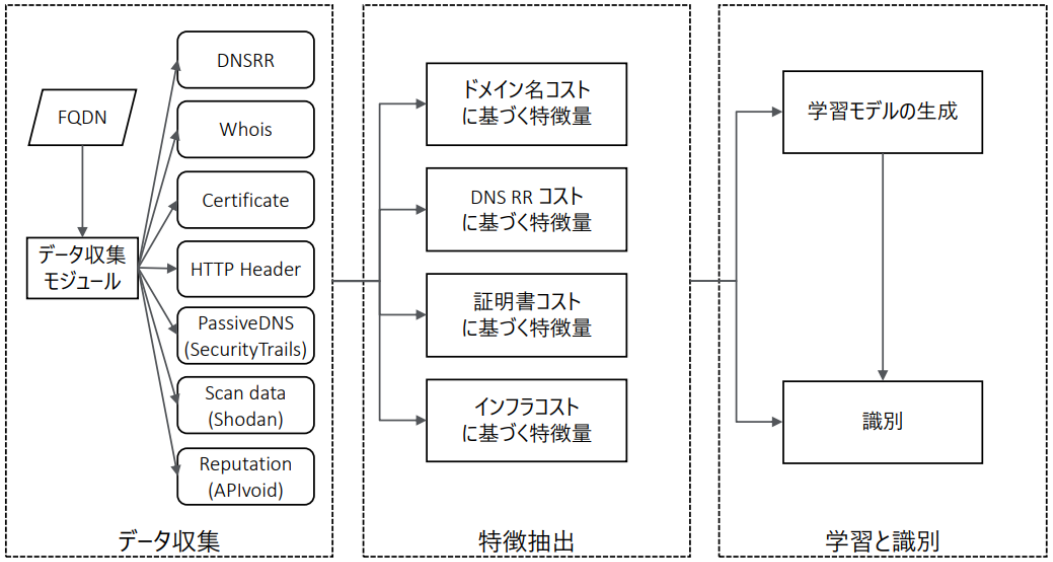
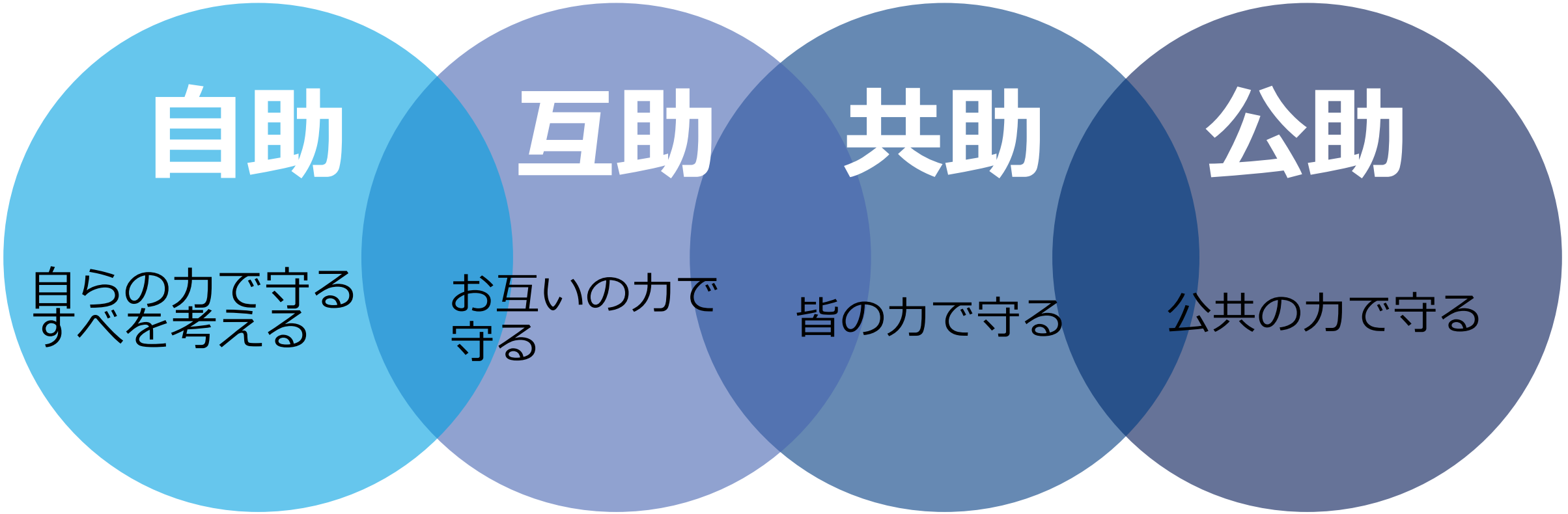


図 1　提案手法のプロセス

表 6　識別に有効な特徴量トップ 10

順位	フィッシング	マルウェアホスト	フェイクニュース
1	ドメイン名の運用年数	ドメイン名の運用年数	ワイルドカード証明書の利用
2	CNAME レコード	CNAME レコード	Alexa ランク
3	MX レコード	開放ポート数	A レコード
4	証明書の有効期間	Passive DNS	CDN
5	開放ポート数	DMARC レコード	CNAME レコード
6	無料/格安証明書の利用	ホスティング	NS レコード
7	Passive DNS	NS レコード	無料/格安証明書
8	SPF レコード	X-Content-Type-Options	ドメイン名の運用年数
9	無料のドメイン名	X-Frame-Options	HTTP Strict Transport Security
10	DMARC レコード	証明書の有効期間	AAAA レコード

皆さんの参画をお待ちしています。



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

ありがとうございました

- フィッシング対策協議会
  - フィッシングサイト・メール報告：
    info@antiphishing.jp
  - Webサイト:
    https://www.antiphishing.jp/
    （入会案内・会則）
    https://member.antiphishing.jp/about_ap/enrollment.html
  - Twitter:
    https://twitter.com/antiphishing_jp

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