色相を利用して自動的に検知範囲を拡大可能なフィッシングサイト検知法

慶應義塾大学　春田秀一郎，山崎史貴，朝比奈啓，笹瀬巌

研究背景

ユーザの個人情報を狙うフィッシングサイト(PWS:Phishing Website)の検知が急務，
視覚情報を用いた検知方式に注目

従来方式（シグネチャベース検知）

PWSは標的サイトを模倣して作成されるため，標的サイト，同一の標的を持つPWS間でレイアウトや色の位置などの視覚情報が類似

➡視覚情報を「シグネチャ」と呼ばれる特徴マップに記述，データベースに格納し，これに類似するシグネチャを持つサイトをPWSと判定（図1）

問題点

従来方式のシグネチャはPWSの亜種間の類似度の差異が大きいため(図2)，多くのタイプのPWSを検知するためには人力による多くのシグネチャの登録が必要 ➡ ゼロデイ攻撃が発生しやすい

・シグネチャを自動的に追加していく機構が必要

提案方式

PWSは標的サイトおよび他の亜種を元に作られ，それらの亜種間では類似した色相が用いられる(図3)ため，色相の類似する亜種を追跡することで多くの亜種が検知可能 ➡ データベースに登録されている検知済みPWSと似た色相を持つサイトを登録済みのPWSの亜種として検知し，データベースに自動的に追加することで，検知範囲を拡大

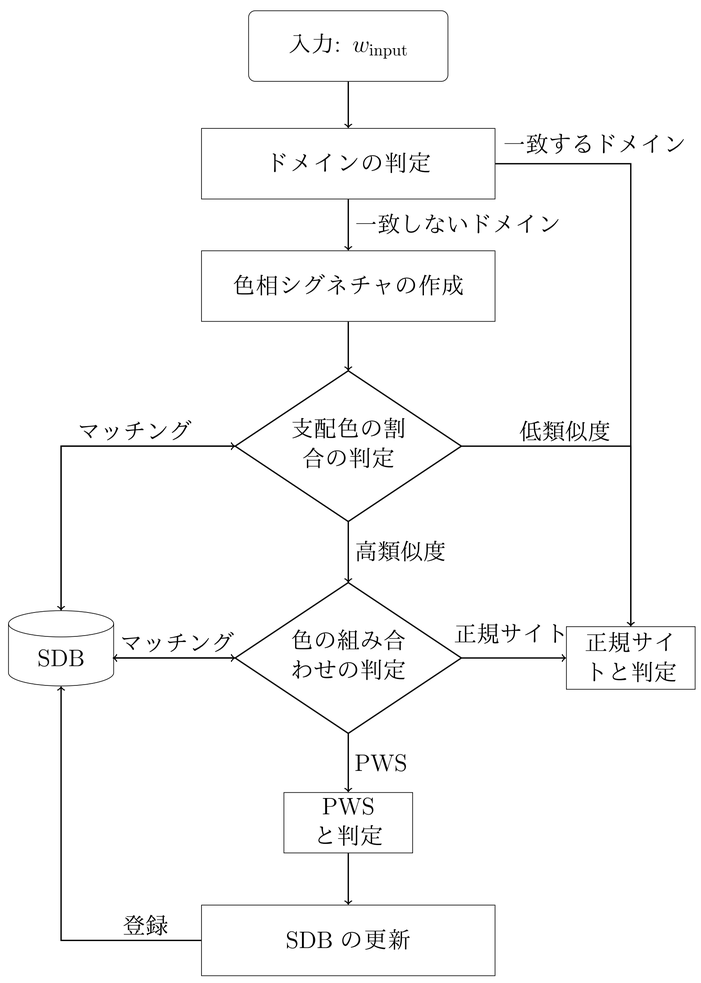


図4 提案方式の検知フロー

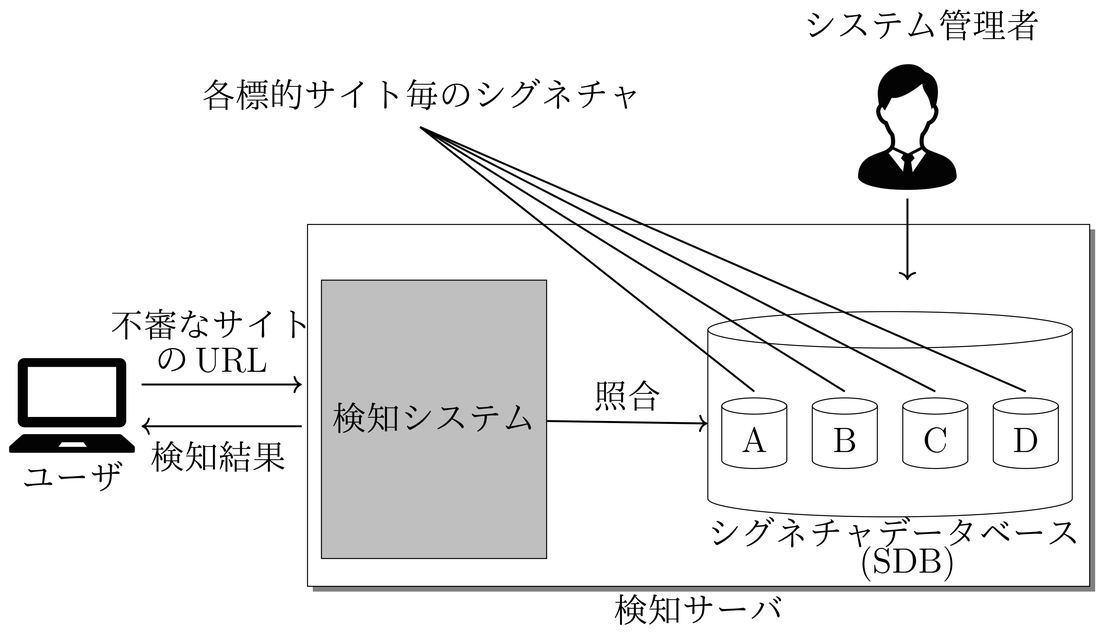
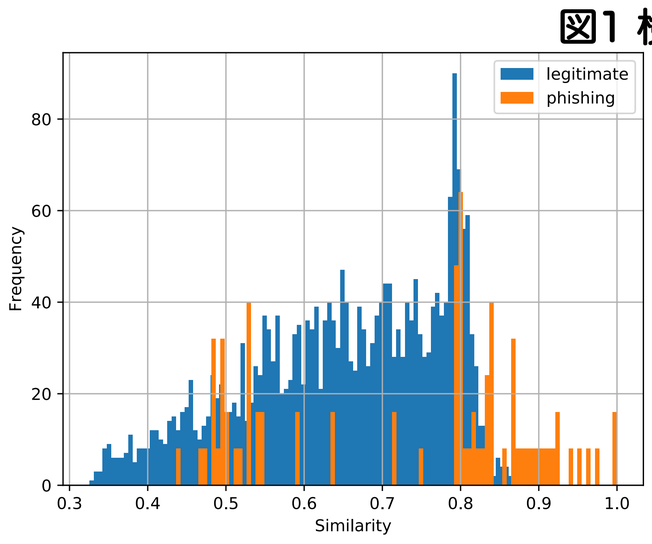


図1 検知システム



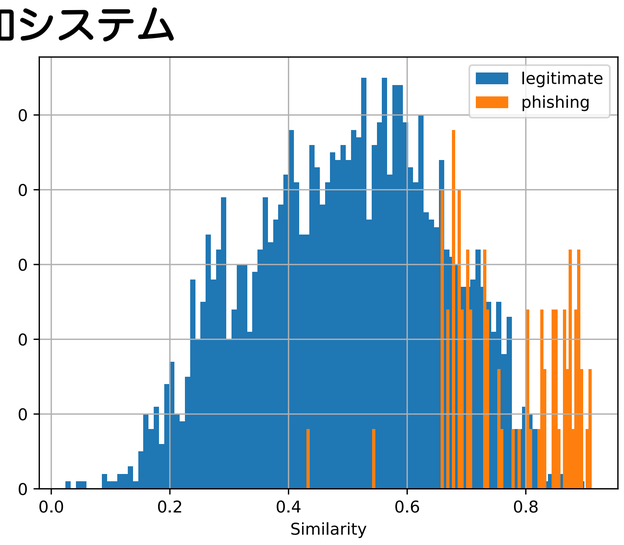
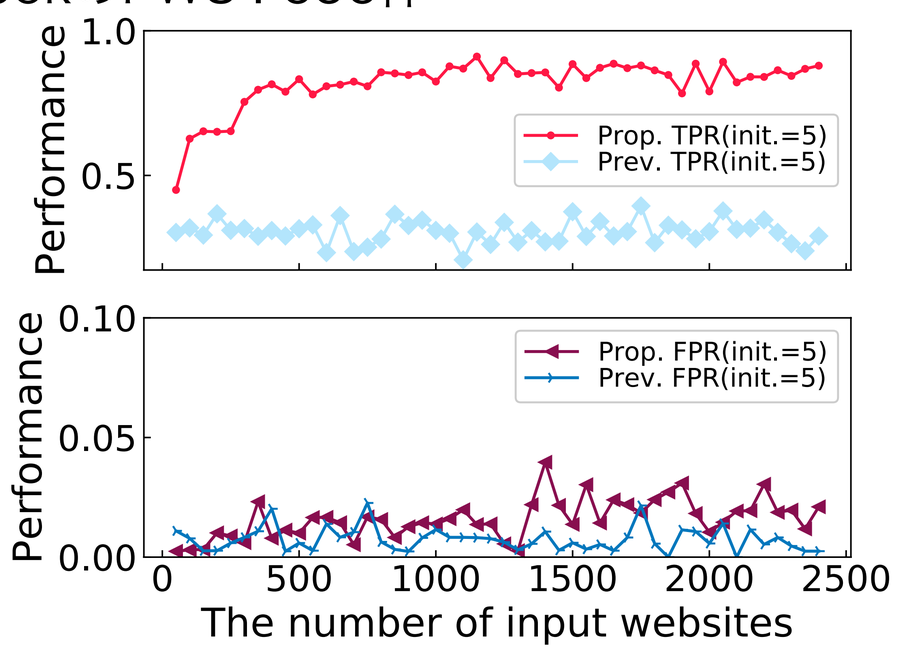


図2, 3 従来，提案におけるPWSの亜種の類似度の分布(Facebookデータセット)

特性評価

正規サイト:1800件
FacebookのPWS : 656件



・FPR(False Positive Rate) を低く抑制しつつ
・TPR(True Positive Rate)は入力サイト数増加に伴い上昇

結論

本研究では，色相を利用して自動的に検知範囲を拡大可能なフィッシングサイト検知法を提案した.
シミュレーションにより，提案した色相シグネチャを自動更新と共に用いることで検知範囲を描くだ可能であることを示した.

本研究の業績

[1] S. Haruta, H. Asahina, F. Yanazaki, and I. Sasase, “Hue Signature Auto Update System for Visual Similarity-based Phishing Detection with Tolerance to Zero- day Attack, ” IEICE Trans. on Information and Systems Vol.E102-D, No.12, pp.2461-2471, Dec. 2019
[2] S. Haruta, F. Yamazaki, H. Asahina, and I. Sasase, “A Novel Visual Similarity- based Phishing Detection Scheme using Hue Information with Auto Updating Database, ” in IEEE APCC, Ho Chi Minh city, Vietnam, Nov. 6-8, 2019.
[3] 春田秀一郎, 山崎史貴, 朝比奈啓, 笹瀬巌, “色相を利用して自動的に検知範 囲を拡大可能なフィッシングサイト検知法,” 電子情報通信学会通信方式研 究会、CS2019-14, pp.7-12, 2019 年 7 月 4 日.