平成２８年度研究開発成果概要書

採 択 番 号 ：19001
課　題　名 ：Web 媒介型攻撃対策技術の実用化に向けた研究開発
個別課題名 ：
副　　題 ：Web 媒介型攻撃の網羅的な観測・分析に基づくユーザ環境のセキュリティ高度化

（１）研究開発の目的

Web サイトを改ざんして攻撃サイトを構築し、当該サイトへアクセスしてきた利用者を攻撃する Web 媒介型攻撃が深刻な問題となっている。Web 媒介型攻撃は、Ⅰ)脆弱性攻撃手法・攻撃ツールの開発や流通、Ⅱ)脆弱サイトの探索や攻撃サイトの構築、Ⅲ)攻撃サイトへのエンドユーザの誘導と乗っ取り、といった一連の不正活動から構成されると考えられる。本研究課題では、これらの不正活動を網羅的に観測、分析することによって、攻撃の構造を正確に把握し、攻撃サイト等を効率的に検出することで利用者を保護する技術を確立することを目的とする。

（２）研究開発期間

平成 28 年度から平成 30 年度（3 年間）

（３）実施機関

株式会社 KDDI 総合研究所＜代表研究者＞
株式会社セキュアブレイン
国立大学法人横浜国立大学（実施責任者　准教授　吉岡克成）
国立大学法人神戸大学（実施責任者　教授　小澤誠一）
株式会社構造計画研究所
国立大学法人金沢大学（実施責任者　教授　満保雅浩）
国立大学法人岡山大学（実施責任者　准教授　山内利宏）

（４）研究開発予算（契約額）

総額 599 百万円（平成 28 年度 200 百万円）
※百万円未満切り上げ

（５）研究開発項目と担当

研究開発項目１：新型ブラウザセンサの研究開発
A. 新規 Windows 系ブラウザセンサ開発(Safari、Chrome 等)（セキュアブレイン）
B. Mac OS 系ブラウザセンサ開発(Safari、Firefox、Chrome 等)（セキュアブレイン）
C. ブラウザ内分析機能強化（セキュアブレイン）
D. センサアップデート機能開発（セキュアブレイン）

研究開発項目２：新型観測機構の研究開発
A-1. AI 技術を応用した大規模クローリング機構(人間-AI 連携型ディープ/ダーク Web クローラ)（神戸大学）
A-2. AI 技術を応用した大規模クローリング機構(脆弱・改ざん・攻撃サイトクローラ)（横浜国立大学）
B-1. モバイル機器向け観測機構開発(Android の Web ブラウザを経由しない Web アクセス観測機構)（岡山大学）
B-2. モバイル機器向け観測機構開発(Android SMS センサ)（セキュアブレイン）

C-1. IoT 機器向け観測機構開発(IoT ハニーポット)（横浜国立大学）
C-2. IoT 機器向け観測機構開発(IoT セキュリティゲートウェイ)（セキュアブレイン）
D. DRDoS 攻撃観測機構（横浜国立大学）

研究開発項目３：攻撃情報分析基盤の研究開発
A-1. 基盤内分析機能強化(プラットフォーム構築)（KDDI 総合研究所）
A-2. 基盤内分析機能強化(機械学習技術を応用した分析)（構造計画研究所）
A-3. 基盤内分析機能強化(プライバシを考慮した分析)（金沢大学）
B. Web プロキシログ、DNS クエリログ等との連携機能開発（KDDI 総合研究所）
C. ユーザ環境へのアクティブクローリング機能開発（横浜国立大学）
D. Web サーバ型ハニーポット開発（横浜国立大学）
E. 基盤アップデート機能開発（KDDI 総合研究所）

研究開発項目４：大規模・長期実証実験
A. 1,000 ユーザ規模（KDDI 総合研究所）
B. 10,000 ユーザ規模（KDDI 総合研究所）
C. ユーザのインセンティブ向上に資する研究開発を実施（KDDI 総合研究所）
D. 個人情報保護等の観点から、技術的及び法的な検討を実施（KDDI 総合研究所）

（6）これまで得られた成果（特許出願や論文発表等）

		累計（件）	当該年度（件）
特許出願	国内出願	2	2
	外国出願	0	0
外部発表	研究論文	3	3
	その他研究発表	38	38
	プレスリリース・報道	43	43
	展示会	1	1
	標準化提案	0	0

（7）具体的な実施内容と成果

研究開発項目１：新型ブラウザセンサの研究開発
Windows 版 Chrome と Mac 版 Chrome で基本機能が動作するブラウザセンサを実装し、ブラウザ AddOn がアクセス情報を収集し、ブラウザ本体と通信し情報を送信する仕組みを開発した。また、収集する情報として Web コンテンツ、Javascript の動作状況などを取得する方法の調査・検討を行った。
PC 内部の収集する項目を Windows、Mac で検討し初期の項目を決定した。またブラウザセンサ本体の実装に利用する開発基盤を調査し、この開発基盤を用いて Plug-In 形式で解析ロジックを追加する仕組みの検討を行った。
Plug-In 形式の解析ロジックに搭載するエンジンの一つとして、Deface 改ざんサイトを調査し検知方法を検討した。検知ロジックを試作して検知性能の評価を行った。
ブラウザセンサ本体の開発基盤に搭載されている、配布ソフトウェアの自動更新機能について調査し、アップデート機能への利用について検討を行った。

研究開発項目２：新型観測機構の研究開発
A-1 AI 技術を応用した大規模クローリング機構(人間-AI 連携型ディープ/ダーク Web クローラ)
ディープ/ダークネットサイトを自動的にクローリングして、サイバー攻撃に関連した Web コン

テンツを高速に収集するAIディープ/ダークWebクローラを開発した。10～100個のTorクライアントを同時起動し、Webページの取得を並列化することで、1秒当たり10～30ページの取得が可能となった。これにより、4,270のTorサイトを発見し、うち985サイトはAhmiaのウェブ検索サービスではindexされてないサイトであった。また、サイバー攻撃情報をやり取りしていると考えられる14のフォーラムサイトを特定した。

A-2 AI技術を応用した大規模クローリング機構(脆弱・改ざん・攻撃サイトクローラ)

目標：ブラウザセンサ、大規模実運用システム(PhishWall) および、Web 検索エンジンから得られる膨大な検査対象 URL から Web 媒介型攻撃に悪用される恐れのある脆弱サイト、既に脆弱性が攻撃されて改ざんされているサイト、クライアントに対して脆弱性を突いて攻撃をしてくる攻撃サイトを抽出するための方式を検討する。

実施内容及び成果：検査対象の URL について簡易的かつ高速に良悪性判定処理を行うスーパーフィルタの開発及びその判定基準について調査・研究を行った。

B-1 モバイル機器向け観測機構開発(Androidの Webブラウザを経由しない Webアクセス観測機構)

WebViewを利用したWebアクセスの処理の流れを調査し、Webアクセス内容を取得するデータ収集箇所を明らかにした。また、この調査結果に基づき、Web アクセスのデータ観測機構を設計し、プロトタイプの実装により、HTTP通信の内容を取得できることを明らかにした。

B-2 モバイル機器向け観測機構開発(Android SMS センサ)

Androidモバイル機器のSMSメッセージ処理の方法を調査し、SMSメッセージ受信を常時監視するSMS センサアプリケーションの実装を行った。SMS センサが収集する項目を検討し、初期の項目を決定した。また、分析基盤とのインタフェースにおいて、個人情報保護の観点を踏まえ検討を行い、初期のインタフェースを決定した。

C-1 IoT 機器向け観測機構開発(IoTハニーポット)

目標：ルータ、IPカメラ、情報家電をはじめとするIoT機器の有する管理用のWebインタフェースに対する攻撃を観測する方式を検討する。

実施内容及び成果:Webインタフェースのセキュリティ上の問題に起因する脅威の現状を把握するため、IoT機器のWebインタフェース等を模擬するIoTハニーポットを構築し、実インターネット上に設置することで、攻撃を観測する方式を検討した。

C-2 IoT 機器向け観測機構開発(IoT セキュリティゲートウェイ)

IoT セキュリティゲートウェイでのネットワーク処理の仕組みを調査し、パケット監視ツールの実装を行った。パケット監視ツールを用いた観測より、攻撃パケットの特徴を観測した。攻撃パケットを遮断する仕組みを検討し、パケット遮断ツールの実装を行った。また、分析基盤とのインタフェースにおいて、遮断ルールの定義方法、配信方法についての検討を行い、初期のインタフェースを決定した。

D DRDoS攻撃観測機構

目標:WebサイトへのDoS(サービス妨害)攻撃の1つであるDRDoS攻撃(反射型分散サービス妨害攻撃)を観測する方式と攻撃対象のWebサイトの分析方法を検討する。

実施内容及び成果：(1)DNSの正引き情報を用いて作成されたデータベースを利用してDRDoSハニーポットで観測された被攻撃IPアドレスとの突合を行い、どのような組織がDRDoS攻撃の被害組織となっているかを明らかにした。(2)UDPベースのプロトコルのうち、要求よりも応答の方が通信量が増幅されるプロトコルを、「プロトコル非準拠ハニーポット」により早期に発見する手法を開発した。(3)CDN（Content Delivery Network）を回避して配信元サーバを直接狙うDoS攻撃の実態を解明した。

研究開発項目３：攻撃情報分析基盤の研究開発

A-1 基盤内分析機能強化(プラットフォーム構築)

攻撃情報分析基盤の設計を行うために、Web アクセス履歴のなかで PhishWall から得られるアクセス履歴について、定期的に収集・蓄積および簡易な分析を行う構成を設計・実装した。また、実装したソフトウェアを用いて、連続して１ヶ月以上の動作を確認することによって、設計の検証を行った。Web アクセス履歴の処理には、Amazon 社が用意するクラウド環境 AWS（Amazon Web Service）を利用した。このクラウド環境によって、大規模実証実験において多くのユーザが殺到した場合でも、柔軟に計算機資源を追加できることを見込んでいる。また、簡易分析には、今後の分析の基準として、Google 社が提供している GSB（Google Safe Browsing）を利用した。分析の結果、PhishWall のアクセス履歴には、GSB において悪性サイトと判定されている URL へアクセスしている履歴が一定数含まれていることが分かった。また、PhishWall のアクセス履歴については、分析を研究項目としている共同受託者に対して、分析できる形で提供した。また、IP アドレス、ドメイン名のように頻繁に出現する項目については、データの格納方法について、机上検討して設計を完了した。

A-2 基盤内分析機能強化(機械学習技術を応用した分析)

新たな脅威の観点から Web of Things における識別子と位置の正当性の課題について検討し、課題の解決策の提案と国内特許出願をおこなった。また、攻撃情報アラートを配信し、管理者の負担を軽減できる検知情報配信のしくみを考案し国内特許出願を行なった。

A-3 基盤内分析機能強化(プライバシを考慮した分析)

プライバシ分析に関して、調査研究を行うと共に、プライバシ分析の評価尺度として、差分プライバシと k-匿名化の関係性について考察し、実データにおいて、ユーザ特定につながるリスクについて予備的な考察を行った。また、プライバシ保護手法に関して、調査研究を行うと共に、データサイズの減少を抑える匿名化手法の一検討を行った。

B Web プロキシログ、DNS クエリログ等との連携機能開発

ISP のキャッシュ DNS サーバのような大容量トラヒックが観測される設備にて効率的に概観を把握するためのキャプチャツールの開発を行った。また Web プロキシログなどと既存の URL ブラックリストとの突合を行い、Whois 情報を追加で解析することで URL ブラックリストのリッチ化が可能であることを示した。

C ユーザ環境へのアクティブクローリング機能開発

目標：ブラウザセンサのユーザに対して能動的にアクセスを行い、ルータ等のゲートウェイ機器のセキュリティ設定や脆弱性の有無を検査する方式を検討する。

実施内容及び成果：ユーザ環境クローラ機能開発の事前調査として、インターネット上に公開されているルータやネットワークカメラなどの IoT 機器を外部からスキャンするシステムを開発し、調査を行った。

D Web サーバ型ハニーポット開発

目標：脆弱な Web サーバ、および、Web アプリケーションを模した囮システムにより、Web サーバ､Web アプリケーションへの攻撃とコンテンツの改ざんを観測するための方式を検討する。

実施内容及び成果：脆弱性を有する Web アプリケーションについて調査するとともに、インターネット上で発生している攻撃を観測するためのハニーポットのデザインの検討を行った。また、ハニーポットに割り当てる IP アドレスの数を増やすため、Web サーバのレンタルを行うサービスの調査を行った。

E 基盤アップデート機能開発

本件研究項目は、3-A-1、A-2 および A-3 に関係が深いため、それぞれの要件を考慮し設計を行った。

研究開発項目４：大規模・長期実証実験

実証実験に向けて課題の洗い出しを行うために、収集情報のリストアップを行った。

ユーザインセンティブについて、大規模な実証実験を有用なものにするために、コミックス・アニメの一つである攻殻機動隊の技術を研究開発によって実現する目的をもつ攻殻機動隊 REALIZE PROJECT と連携をするという方針を決定した。特に、攻殻機動隊のなかに登場して、主人公たちをサポートする役割をもつタチコマを起用して、実証実験の参加者に対して、攻撃遮断機能を提供したり、攻撃回避のためのアドバイスをしたりする方針である。 これらのコンセプトについて、2017 年３月 25 日に開催されたイベント Anime Japan において発表展示するとともに、プレスリリースを発行した。