様式 1-4-2 (2019-1)

平成 30 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
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 32 年度（5 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
国立大学法人 神戸大学
株式会社構造計画研究所
国立大学法人 金沢大学
国立大学法人 岡山大学

（4）研究開発予算（契約額）

総額 999 百万円（平成 30 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）特許出願、論文発表等

		累計（件）	当該年度（件）
特許出願	国内出願	5	1
	外国出願	0	0
外部発表	研究論文	16	10
	その他研究発表	174	65
	プレスリリース・報道	112	45
	展示会	2	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
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）
大規模実証実験に向けて Windows Google Chrome 版 ブラウザセンサを開発提供した。これにより、エンドユーザにおける攻撃遭遇の実態把握に向けた情報収集、およびエンドユーザへの攻

撃遮断を可能とした。また、収集情報について閲覧履歴情報の拡充、およびプロセス情報の拡充を行い、より詳細な分析を可能とした。

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）

大規模実証実験に向け、MacOS Google Chrome 版 ブラウザセンサを開発提供した。これにより、エンドユーザにおける攻撃遭遇の実態把握に向けた情報収集、およびエンドユーザへの攻撃遮断を可能とした。また、収集情報について閲覧履歴情報の拡充、およびプロセス情報の拡充を行い、より詳細な分析を可能とした。

C. ブラウザ内分析機能強化（セキュアブレイン）

ブラウザ内分析機能の強化に向け、分析手法について下記研究を行った。これらにより、悪性サイトの識別/分類に向けた特徴抽出手法について一定の有効性が確認できており、精度向上等を含め今後の研究のベースを確立した。

- AI を用いた悪性 JavaScript 検知に関する研究
- AI を用いた偽 EC サイト検知に関する研究
- Web 閲覧履歴の関係性の分析

D. センサアップデート機能開発（セキュアブレイン）

大規模実証実験に向けブラウザセンサのセンサアップデート機能を開発提供した。これにより、実証実験ユーザに対してブラウザセンサのアップデート制御が可能となり、研究開発項目 1-A、1-B で行った機能拡充の自動アップデートを実現した。

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）（神戸大学）

- ダークウェブ Tor の HTML コンテンツを自動収集し，悪性サイトへのリンクを抽出するクローリング機構を開発した。2018 年 4 月 1 日～2019 年 1 月 23 日までダークウェブの 8,910 ドメインをクローリングし、VirusTotal API と GRED エンジンを用いて悪性度を判定した。その結果，VirusTotal で 1 つ以上の検知器が悪性と判定したサイトは 1,444 件であり、GRED エンジンでは VirusTotal とは異なる 11 の悪性サイトを見つけた。また、悪性サイトのリンクをもつことの多いウェブページのジャンルを判定する識別器を作成したところ、F 値で 0.82 の判定精度を得た。
- WarpDrive 分析基盤で収集された悪性 URL から HTML を収集し、サイトの悪性度を HTML コンテンツで判定可能かを、Saxe らが提案した深層学習モデルで検証した。訓練データには、DNS-BH が提供している 2,488 の悪性 HTML と RedditList で提供された 4,544 の良性 HTML データを用い、WarpDrive で提供されている 2018 年 6 月 1 日～2018 年 7 月 15 日に収集された悪性サイトの判定精度を調べた。分析基盤で付加された悪性ラベルに基づいて評価した結果、F 値で 0.875 の検知精度が得られた。
- JavaScript の悪性度を判定するため、ソースコードを AST 表現に変換してから Doc2Vec で文書ベクトルを取得し、SVM で悪性度判定を行う方法を提案した。訓練データには D3M データセットで提供されている 40 の悪性 JS を使用し、良性には Jsunpack が Web based Portal で提供している 40 の良性 JS を使用した。その結果、F 値で 0.89 の検知精度が得られた。

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）（横浜国立大学）

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として前年度実装を開始したシステムの実装を継続すると共に、悪性サイトのブラックリスト抽出を進め、実証実験のデータを用いてブラックリストのシミュレーションベースの評価を行った。

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）（岡山大学）

モバイル機器向けの観測の中で、Android における Web ブラウザを経由しない Web アクセスのうち、WebView ライブラリを用いた HTTP 通信の観測機構の実現方式の検討を行った。具体的には、SPDY と HTTP/2 への対応を行い、これまで観測できなかったプロトコルに対応した。また、実現した観測機構を用いて、WebView を利用したアプリを実行し、Web アクセスのデータを取得する実験を行った。この実験から、WebView を利用した Web アクセスによる脅威を分析した。具体的には、特に偽警告画面を表示する Web ページへの遷移を詳細に分析し、遷移の仕組みを明らかにした。さらに、簡易的な実装を行い、悪性サイト IP アドレスなどをブラックリストに用いることで、WebView 内で悪性サイトへのアクセスをブロックできる可能性を示した。

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）

セキュアブレイン社内環境において、昨年度に開発した Android SMS センサを用いた悪性 SMS の観測を行ったが悪性の事象をうまく誘い込むことができなかったため、モバイル端末でのエンドユーザにおける攻撃遭遇の実態把握に向け、モバイルを対象とした大規模な実証実験を行うことの承認を頂き、平成 31 年度の実証実験開始に向けた準備（モバイル端末における情報収集手法の検討）を開始した。また、並行して、ソーシャルネットワークサービス（SNS）の一つである Twitter で情報周知・共有される Android アプリの収集機構（Twitter 情報収集システム）を開発し、Android アプリおよび関連情報を収集。サードパーティマーケットで配布されるアプリの特徴を明らかにした。

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）

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 インターフェイスに対する攻撃を観測する機構を構築した。昨期に実装を開始した IoT ハニーポットの Web インターフェイス拡張の実装を継続し、その評価を行った。昨年度はルータ、カメラ、Wi-Fi ストレージなど7機種を用いた拡張を実施したが、今年度は攻撃元のブラウザや攻撃ツールを判定するためのブラウザフィンガープリンティング機能を実装し、観測された攻撃をより詳細に分析できるよう拡張を行った。

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)（セキュアブレイン）

エンドユーザ LAN 内のセキュリティ向上と健全化に向け、IoT セキュリティゲートウェイに関する下記研究を行った。これらにより、ゲートウェイの位置（内部 LAN と外部 WAN との境界）に存在することで可能となるセキュリティ維持機能の有効性を明らかにし、実用化に向けた基礎研究として今後の研究の方向性を定めた。

- IoT ゲートウェイに擬似 C&C サーバを設置することによる、IoT マルウェア駆除手法の検

討と評価
- 攻撃の検知、防御状況等をユーザへ通知する機能の検討
- AI を用いた攻撃パケットの分析

D. DRDoS 攻撃観測機構（横浜国立大学）

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 サイトの分析方法として前年度実装を開始したシステムの実装を継続すると共に評価を行った。

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)（KDDI 総合研究所）

- 大規模実証実験を行うための分析基盤の設計および実装を完了した。分析基盤では、ユーザの PC にインストールしたセンサ側から収集するデータとして、Web アクセス履歴収集機能、悪性サイト収集機能、OS 環境情報収集機能を実装した。
- 新型ブラウザセンサにおいて、悪性サイトをブロックするためのブラックリスト配信機能を実装した。
- このプラットフォームを用いて実証実験を開始した。

A-2. 基盤内分析機能強化(機械学習技術を応用した分析)（構造計画研究所）

ユーザ環境の Web アクセスログを分析し、Rig Exploit Kit（Rig EK）による Web 媒介型攻撃の継続を裏付ける観測結果を得た。また、悪性 URL サンプルに共通する特徴量の抽出と、その特徴量を利用することで効率的に大規模な Web アクセス履歴から悪性 URL を検知する手法の有効性を確認した。

一方、Rig EK は攻撃の特徴である Indicators of Compromise（IOC)によって検知されるが、踏み台サイトの取り締まりや攻撃検知の回避のために IOC が変化してしまうため、長期間にわたって攻撃を継続的に追跡観測することが困難であるという課題があった。この課題に対して、変化する IOC を自動的に導出する検知方式を提案し、IOC の変化に追従して新しい IOC を導出できることを確認した。

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）

プライバシ評価指標として提案を行っている仮 ID の再同定手法において、複数の異なる類似度を適用することにより、再同定率への影響を評価した。そして、この仮 ID 再同定手法を用いて、Web アクセス履歴データの有用性を保ちつつ、プライバシリスクを低減するための適切な仮 ID の更新頻度の設定手順について考察を行った。更に、データ構造を保ちつつプライバシを保護したデータ分析を実現するために、Set-valued database に対する解析者の事前知識を考慮したデータ匿名化手法を検討し、データ構造を保ちつつ、データ解析の有用性が維持されていることを示した。

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）

- キャッシュ DNS サーバのデータの外観を把握するためのツールをつかって、Web アクセス履歴においける悪性サイトのドメイン名の名前解決との突合分析を行った。DNS キャッシュサーバでも悪性サイトの名前解決クエリが観測されることが分かった。
- Rig EK の活動を複数の地点で観測するため、DNS サーバにおける観測を行った。DNS トラヒックに対して、Web アクセス履歴において観測された 2,119 件の 2nd レベルドメインの観測状況を調査した。

C. ユーザ環境へのアクティブクローリング機能開発（横浜国立大学）

ブラウザセンサのユーザの IP アドレスにインターネット経由で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として前年度実装を開始した内容の実装を継続し、当該機能（アクティブクローリング機能）の評価の枠組みを検討した。

D. Web サーバ型ハニーポット開発（横浜国立大学）

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として前年度実装を開始したシステムの実装を継続すると共に評価を行った。

E. 基盤アップデート機能開発（KDDI 総合研究所）

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

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）

- 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１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 と連携した実証実験計画を策定した。
- 攻殻機動隊の中のタチコマをつかった新型ブラウザセンサのユーザインターフェースを開発した。
- NICT におけるパーソナルデータ取り扱いマニュアルに沿って個人情報保護やパーソナルデータの取り扱いに関する実証実験計画をまとめた。この計画を NICT におけるパーソナルデータ（PD）委員会に提出して、実証実験を実施することの承認を得た。
- 2018 年６月１日から実証実験を開始して、約 6,500 名の実証実験参加者を得た。１日あたり約 1,500 万 URL を収集し、悪性サイトと疑われるサイトを約 230 件/件発見している。

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）

ログデータの安全な第三者提供が可能なプロトコルの検討を行い、実装およびその有効性を評価する。具体的には情報銀行のような集中型 PDS（Personal Data Service）を検討し、データ提供者のパーソナルデータを暗号化した状態のまま、プライバシを保護した形態（k-匿名化など）へ加工した上で第三者提供を行うようなプロトコルを検討する。その後、実際に提案プロトコルの実装を行い、データサイズと通信量および計算時間との関係を評価する。

以上