様式１－４－２

平成 29 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 599 百万円（平成 29 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	2	0
	外国出願	0	0
外部発表	研究論文	6	3
	その他研究発表	109	71
	プレスリリース・報道	67	23
	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

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）

Web ブラウザからコンテンツ、JavaScript 関数、JavaScript 関数の Call 回数を収集する機能を実装し、Windows の Chrome 版のブラウザセンサを開発した。項目３の攻撃情報分析基盤、項目 4 の可視化部と連携し、ユーザのアクセス情報を基盤へ送信、またはブラックリストによってアクセスをブロック、基盤からの情報を可視化部へ転送する機能などを実現した。

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）

Web ブラウザからコンテンツ、JavaScript 関数、JavaScript 関数の Call 回数を収集する機能を実装し、MacOS · Chrome 版のブラウザセンサを開発した。項目３の攻撃情報分析基盤、項目 4 の可視化部と連携し、ユーザのアクセス情報を基盤へ送信、またはブラックリストによってアクセスをブロック、基盤からの情報を可視化部へ転送する機能などを

実現した。

C. ブラウザ内分析機能強化（セキュアブレイン）

ユーザ PC 内で分析を行う機能として、センサ本体でブラウザ AddOn からの情報を処理できる仕組み実装した。攻撃情報分析基盤から更新されるブラックリスト等と照合を行い、ブラウザ AddOn と連携してユーザのアクセスのブロックを行う。

D. センサアップデート機能開発（セキュアブレイン）

センサ本体部分は、サーバに新バージョンの有無を問い合わせ、アプリケーション自身を更新する機能を実装した。ブラウザ AddOn 部分は AddOn 配布サイト等を通じてインストールと更新が行われる。

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）

SNS, 掲示板、セキュリティニュースサイトなどの表層 Web に加え、Tor における AlphaBay, DreamMarket といったメージャーなマーケットサイトなどをクローリングし、サイバー攻撃関連の情報収集を行う仕組みを作った。

文字情報をベクトルに変換する Doc2Vec などの機械学習モデルにより、精度よく収集コンテンツの分類や悪性 JavaScript の判定に利用できることを確認した。

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）（横浜国立大学）

昨年度に引き続き、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判定基準について調査・研究を行った。

また、スーパーフィルタの適用後検査対象の URL にアクセスした際に攻撃が発動するかを詳細に分析するための高対話ブラウザ型ハニーポットの開発及び判定基準について調査・研究を行った。判定基準の検討を行うため、クローラを実装し、悪性サイトにアクセスした際に取得されるコンテンツの調査を行ったところ、複数のサイトから悪性なコンテンツを取得することに成功した。

さらに、大規模 Web アクセスログから効率的に悪性サイトを抽出する手法を提案した。同手法では、良悪性判定のための前段処理（高速フィルタリング）として、１）悪性 URL に共通するパターンを用いたフィルタリング（URL パターンベース）と２）悪性 URL にアクセスする確率の高いユーザ群を用いたフィルタリング（ユーザベース）の二種の手法を考案した。１）２）の評価実験を行ったところ、膨大な Web アクセスログから、GSB で未検知の URL を効率的に抽出できることが確認できた。１）については、悪性 URL に関する事前情報や詳細な分析を必要とせず、RigEK により作成された悪性サイトの URL に共通するパターンを抽出できることが分かった。２）については、ユーザベースのフィルタリングについては、ブラックリストで未検知であった悪性サイトの URL を多数抽出できることが分かった。

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）

Android において Web ブラウザを経由せずに Web コンテンツを表示する WebView ライブラリを改変し、WebView の Web アクセス観測機構を設計し、実現した。Google Play ストアや Twitter 経由で収集した Android アプリを分析し、90%以上の Android アプリが WebView を利用していることを確認し、WebView の通信を観測する重要性が高いことを確認した。また、実現した観測機構の性能を評価し、実際に配布されている WebView を用いた Android アプリについて、WebView を用いた通信を Web アクセス観測機構で観測し、通信内容を取得できることを確認した。

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）

Android モバイル機器に配信される悪性 SMS を検知/通知する機能を実装 した。この機能においてブラックリストを用いることによって 特定の SMS 本文を検知できることを確認した。また、分析基盤との連携のため、SMS 情報のアップロード、ブラックリスト取得の仕組みを実装した。個人情報保護を念頭に、アップロードする SMS 情報を切り替えできるように設計した。

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）

実機を用いたハニーポットを用いて、組込み機器の WebUI に対するサイバー攻撃を観測し、分析した。IP カメラ、ルータ、ポケットルータ等を用いたハニーポットを設置し観測していたところ、WebUI を介して機器のネットワーク設定情報を取得する自動化された攻撃が複数観測された。また、IP カメラのハニーポットでは、人手によるものと思われるカメラ映像の覗き見が複数回観測された。

IoT マルウェアの動的解析により、DDoS 攻撃の観測と分析を行った。実際に IoT マルウェアを C&C サーバに接続し、攻撃観測実験とダミーC&C サーバを用いた攻撃再現実験を行った。攻撃観測実験により、DoS 攻撃の観測には一定期間の動的解析による観測が必要であることが分かった。また、攻撃再現実験により、大多数の IoT マルウェア検体は DoS 攻撃機能を有していることや，アプリケーションレイヤの DoS 攻撃の実態が把握できた。また、実機での攻撃再現実験により低価格の IoT デバイスでも、100Mbps 程度の攻撃トラフィックが生成されうることを確認した。

実行環境依存性（機器環境により挙動に差が現れる性質）を示す IoT マルウェア検体の有無を調査した。調査した検体のうち約 4 割の検体が実行環境依存性を示すことを明らかにした。また、実行環境毎に解析可能な検体数が最大で 3 倍程度異なることが分かった。さらに、実行環境依存性は広く様々なマルウェアファミリに表れていることを明らかにした。検体収集に用いた機器と同製品の機器での検体実行により、攻撃者が機器の種別を意識せずに攻撃を行っている場合があることを明らかにした。

IoT マルウェアの持続的感染の成立要因を分析し、実機において検証した。OS に Linux を使用する IoT 機器は、読み取り専用のファイルシステムを用いることでマルウェアをダウンロードする攻撃に対して持続的感染を防止するが、その一方でファームウェア改変による感染は持続的感染を引き起こす可能性があることを示した。実機を用いた検証では、改変したファームウェアを用いてファームウェア更新を実施することにより、悪性プログラムの持続的感染が実現することや機器が故障に至る可能性を示した。さらに、インストーラーがファームウェアに含まれる場合において，インストーラーの改変による攻撃が成立する可能性を実証した。これらの攻撃の成立条件を分析し，対策方法の提案を行った。

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）

IoT セキュリティゲートウェイにおいて、パケット観測により得られた攻撃パケットの特徴を解析した。Mirai や Wannacry などのマルウェアによる攻撃パケット)の特徴をルール化した。このルールを基に、NFQUEUE による攻撃パケット遮断機能を実装した。実装した攻撃パケット遮断機能の、実際の攻撃に対する防御の有効性を検討

D. DRDoS 攻撃観測機構（横浜国立大学）

DNS の正引き情報を用いて作成されたデータベース（DNSDB）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、標的となった IP アドレスに対応するドメイン名を収集した。収集したドメイン名からコンテンツのカテゴリを調べることができるデータベースを用いて被害組織について分析を行った。被害組織のドメイン名をカテゴリ別に分類した場合、およそ 86%のドメイン名はなんらかのカテゴリに分類できることを確認した。また、被攻撃対象として注目度の高い Stock Advice and Tools や Government や Financial Services などのドメイン名について、概ね正しくカテゴライズされていることを人手で確認した。

プロトコル非準拠ハニーポット（全てのリクエストにランダム文字列を返信する、アプリケーションプロトコルに依存しない DRDoS ハニーポット)をインターネット上に設置し、観測された攻撃通信の分析を行なった。観測される攻撃件数は増加傾向にあり、主に 389/udp（コネクションレス型 LDAP プロトコルが存在）の攻撃件数の急激な増加によるものと思われる顕著な攻撃件数の増加が２０１７年９月から１１月にかけてあったことがわかった。また、11211/udp（memcached サービス）の応答を悪用した攻撃を２０１８年2月下旬から観測した。さらに、プロトコル非準拠ハニーポットでの観測結果（現在悪用されているプロトコルとその攻撃手法の知見）に基づいて、検査対象サーバが DRDoS 攻撃の踏み台となるかどうかを判定する踏み台検知スキャナを構築した。

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)（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ー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。また、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。研究項目 1 において開発した新型ブラウザセンサの結合試験を行って、それぞれのデータが正常にアップロードされること、ブラックリストが定期的に配信できることを確認した。

また、大規模実証実験に先立って実験の有効性を検証するために、あるセキュリティベンダのツールから収集されるデータをこの攻撃情報分析基盤において分析した。その結果、ブラックリストのひとつである Google Safe Browsing（以下 GSB）において悪性サイトと判定されるサイトへのアクセスが発生していることが分かった。さらに、悪性サイトのなかでブラウザを攻撃するエクスプロイットキットのひとつである RIG エクスプロイットの特徴をもつ URL が、月間数千件記録されていることが分かった。また、GSB の登録時期とアクセスが観測された時期の比較をしたところ、約 30%がユーザのアクセスよりも後に GSB に登録されたことが分かった。さらに、RIG エクスプロイットキットについては、32%が GSB 登録日と観測日が同一であるものの、36%が翌日以降、31%が登録されないことが分かった。

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）

セキュリティベンダから提供を受けたユーザ環境における大規模Webアクセスログの分析により、RIG エクスプロイトキットの攻撃 URL には数時間以内の短い活動期間のドメイン名が大量に使用されている実態を明らかにした。また、大規模なテイクダウン（攻撃サイトの閉鎖）が行われた後も IP アドレスを直接指定した URL による攻撃が継続していることを確認した。これらの攻撃に共通して見出された特徴を利用したフィルタリング方式により、大量のアクセスログから効率的に RIG エクスプロイトキットの攻撃 URL を発見可能であることが分かった。

A-3. 基盤内分析機能強化(プライバシを考慮した分析)（金沢大学）

プライバシ評価指標として、匿名加工データを再識別する上での多変量データ集合向け類似度指標や、仮 ID を再同定する上での評価指標を提案し、その性能について評価を行った。適切な仮 ID の更新頻度を設定することにより、Web アクセス履歴データにおけるプライバシリスクを低減することができる。また、プライバシを保護したままデータ分析するための要素技術を調査研究すると共に、解析者の事前知識を考慮した Set-valued database に対する匿名化手法を検討し、その性能について評価を行った。

B. Web プロキシログ、DNS クエリログ等との連携機能開発（KDDI 総合研究所）

本年度は、昨年度開発したキャッシュ 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。約 2 週間分の 1/64 サンプリングした DNS キャッシュサーバのログと頻繁に観測される RIG エクスプロイットキットのドメインを比較したところ、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。

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）

ユーザ環境クローラ機能開発の事前調査として昨年度に開発した、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について、スキャン結果の画像データを階層的クラスタリングすることで分析の効率化を試みた。実験の結果、IoT 機器の UI のうち管理 WebUI の画像について、同一または類似する画像が同一クラスタに凝集する傾向が強く、そのようなクラスタを優先的に調査することで、効率的に IoT 機器を発見可能であることが分かった。

D. Web サーバ型ハニーポット開発（横浜国立大学）

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。

Apache Struts の脆弱性に対する攻撃を観測するためのハニーポットを実現し、インターネット上に公開した。実験の結果、Apache Struts の脆弱性を突いて Linux サーバや Windows サーバに対してコマンドインジェクションが行われる様子を観測した。攻撃者は、攻撃対象のリソースを狙った攻撃や攻撃対象が Web サーバであることを悪用した攻撃など、様々な目的で Apache Struts の脆弱性を悪用することが分かった。

実機を用いたマルウェア動的解析システムを、環境復元ソフトウェアを用いて構築する方法を提案した。評価実験では、仮想環境を検知する RAT 検体と実マルウェア検体を用い

て提案手法の有効性を評価した。

ハニーポットを検知する攻撃の実態を明らかにするため、シグネチャベースの検知を用いたオープンソースハニーポットの運用実態の調査を行った。実験の結果、幾つかの VPS の IP アドレスレンジにおいてハニーポットを検知した。また、検知した SSH ハニーポットのバナーを分析することで、多くのハニーポットがデフォルト設定のまま運用されていることが分かった。実際に、攻撃者に悪用された可能性のあるハニーポットを発見した。

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

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 と連携する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。攻殻機動隊におい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機能を実装した。

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。

以上