様式 1-4-2 (2020-2)

令和２年度研究開発成果概要書

採 択 番 号 19001
研究開発課題名　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 年度から令和２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 1000 百万円（令和２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、外部発表等

		累計（件）	当該年度（件）
特許出願	国内出願	13	5
	外国出願	0	0
外部発表等	研究論文	34	9
	その他研究発表	273	43
	標準化提案・採択	0	0
	プレスリリース・報道	174	38
	展示会	7	5
	受賞・表彰	29	5

（7）具体的な実施内容と成果

<u>研究開発項目１：新型ブラウザセンサの研究開発</u>
1-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）
前年度までに実装してきた Windows Google Chrome ブラウザセンサについて、保守及び改修を行った。ブラウザセンサは、Google Chrome のブラウザ拡張機能を利用して実装している。Google では、このブラウザ拡張の仕様を Manifest version２（MV2）から version３（MV3）へ大幅に変更することを計画していることから、実証実験を継続する場合にブラウザセンサに適用するブラウザ拡張を MV2 から MV3 へ変更する方法を検討した。

1-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）
前年度までに実装してきたMac Google Chrome ブラウザセンサについて、保守及び改修を行った。

1-C ブラウザ内分析機能強化（セキュアブレイン）
前年度実施したWeb 閲覧履歴を利用した悪性サイトの検知について新たな特徴を取り入れ、事前検知に重点を置いた研究を行い、検知精度を向上させた。研究成果から得られた URL 事前検知ロジックをPlug-In 解析ロジックとしてブラウザセンサに実装するための検討及び実装を行った。

1-D センサアップデート機能開発（セキュアブレイン）
前年度までに実装してきたブラウザセンサのアップデート機能に対して、保守及び改修を行った。

研究開発項目２：新型観測機構の研究開発

2-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）

- ウェブ閲覧時に実行されるJavaScript(JS)の悪性判定を行う２種類の機械学習モデルを開発した。一つ目のモデルでは、難読化を解読してAST 表現に変換した後、FastText で JS 埋め込みベクトルを求めて、Support Vector Machine (SVM)で悪性度判定する。二つ目のモデルでは、AST 表現の木構造をGraph Convolutional Network (GCN)で学習し、それによって悪性度判定を行う。約 16 万件の JS データセット（悪性：約４万件、良性：約 12 万件）に対し、２つの提案モデルはそれぞれ、F 値で 0.953 と 0.996 と高い検知精度をもつことが示された。
- URL の文字列特徴で悪性判定を行う深層学習モデルに、非危険ワードと危険ワードに基づく判定を加えたURL 悪性判定システムを開発した。悪性判定の精度は再現率で約 0.7 を達成し（学習データが十分に与えられた状態での精度)、VirusTotal の検知器数が１以上で悪性と定義する場合、GSB で未検知だった悪性サイトを 17 カ月間で 9,895 件（約 19 件/日）発見した。なお、VirusTotal の検知器数が３以上で悪性と定義する場合であっても、17 カ月間で 1,394 件（2.7 件/日）の未発見悪性サイトが見つかった。

2-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(セキュリティ製品ログ)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までに検討、構築、改良したシステムの評価を行った。
- ユーザが悪性サイトへ到達することを未然に防止することを目的として、悪性サイトに到達しやすい危険検索ワードを検出するシステムを用いて実証実験参加ユーザに対して注意喚起を行った。また、当該ユーザに危険検索ワードを検索した時の状況についてアンケートを実施し、前年度までに検討、構築、改良したシステムの評価を行った。
- ブラウザセンサや大規模実運用システム(セキュリティ製品ログ)から得られる膨大な検査対象URL をカテゴライズツールと突合し、悪性サイトに到達するリスク比の高いカテゴリの URL を詳細分析することで悪性サイトを検出するシステムを開発した。また、作成したブロックリストをブラウザセンサログとマッチングすることで、構築したシステムの評価を行った。

2-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）

- Web アクセス観測機構で Android における Web アクセスを解析する中で、利用者の意図しない Web サイト遷移の発生が利用者の利便性を低下させることに着目し、検知と利用者への警告を表示する機構を実現した。また、実証実験を行うことにより、提案機構が利用者の意図しない Web サイト遷移を検出でき、利用者に適切な警告を表示できることを確認した。
- Web アクセス観測機構を利用して利用者の意図しない Web サイト遷移を可視化することで、Web サイト遷移の解析を支援する機構を実現した。
- 利用者の意図しない Web サイト遷移を発生させる Web サイトの特徴を解析し、ドメイン名やファイル名をキーワードとしたブラックリストを作成する手法を実現した。また、ブラックリストに登録されたキーワードをもとに実証実験データを検索することで、これまでに発見されていなかった利用者の意図しない Web サイト遷移を発生させる Web サイトを発見した。

2-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）

ユーザ参加型大規模実証実験向けモバイルセンサアプリについて、脅威検知・警告機能（リパッケージアプリ、多段リダイレクト、危険検索ワード）を実装し、収集するデータ項目を拡充した。また、モバイルセンサアプリで収集されたデータに関する調査分析を実施した。さらに、本分析により発見したリパッケージアプリの検知リストを実証実験向けに配信した。

2-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 インターフェースに対する攻撃を観測するハニーポットの評価を行い、継続的にマルウェア検体が収集できることを確認し、他の受託者や外部研究者に検体等提供を行った。
- これまで構築したハニーポットシステムの統合を行い、観測結果を統合的に格納、分析するためのデータベースを構築した。これにより日々取得される各ハニーポットの観測データを、１日程度で集約して分析できるようになった。

2-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）

実環境においても駆除が行えるかを検証するために IoT ゲートウェイを 10 か所配置した環境を模擬した小規模実験環境を構築し、複数の機器およびアーキテクチャ上でマルウェアを動作させ、駆除が行えることを確認した。また、ブラウザセンサとの連携として駆除結果を通知する機能の開発を行い、小規模実験環境上でブラウザセンサを経由して駆除結果の通知が可能であることを確認した。

2-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)を観測すると共に攻撃対象の Web サイトがうけた影響の度合いを測定するシステムについて評価を行った。
- 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)を観測し、特に Memcached 攻撃の攻撃元に関わる情報に着目することで、DRDoS 攻撃の攻撃元を推定し、その活動の実態を分析した。分析により、高々７つ程度の AS が主要な攻撃の拠点となっているという結果が得られた。

研究開発項目３：攻撃情報分析基盤の研究開発

3-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）

- これまで構築・運用してきた Amazon Web Service(AWS)/Google Cloud Platform(GCP)

/物理サーバからなる実証実験基盤の機能強化および運用を行った。受託メンバーである他の 6 者に対して、Elastic Search/Kibana による分析基盤、AWS による分析基盤など統合的な分析環境を提供した。

- AWS の機能のひとつ Amazon QuickSight および Amazon Athena を利用して、S3 上に蓄積したデータの統計値の分析および可視化を行った。2020 年 4 月から 2020 年 12 月 31 日までの期間に、PC 版実証実験、モバイル版実証実験、セキュリティツールから提供のログをあわせると 120,939 件の悪性サイトを発見した。内訳は PC 版実証実験 12,545 件、モバイル版 480 件、セキュリティツールから提供されるログが 107,914 件であった。これによって、Google SafeBrowsing（GSB）に登録されている悪性サイトへのアクセス状況や悪性サイトの GSB への登録遅れの実態を明らかにした。
- 定期的なレポートとして、新しい実証実験参加者の状況や、実証実験参加者のデータ提供状況などを研究受託各者へ提供した。
- 実証実験参加者の実証実験終了依頼および提供データ削除依頼に対して対応した。

3-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）

- ユーザから収集した Web ブラウジング情報から抽出したリダイレクト情報を構造分析することによって、リダイレクト構造の特徴を機械学習やネットワーク分析手法により分析し、悪性リダイレクトチェーンに固有の特徴を捉えた悪性リダイレクトチェーンを特定するための新しい方式を提案した。
- 複数のユーザから収集したリダイレクト情報を用いて、アソシエーション分析の機械学習手法やネットワーク分析手法で提案方式を評価した結果、悪性サイトへのリダイレクトを正確に特定する上で非常に効果的であることを実証した。

3-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の調査研究：データ分析や加工に関して、プライバシの保護の度合いを定量的に評価するための指標として、データの特性を考慮したユーザ間類似度指標を検討した。具体的には、Bookmark を考慮した場合と時系列を考慮した場合を取り上げ、プライバシの保護の度合いを測定して利用者に情報を提供するための評価指標の作成につなげた。
- プライバシ保護データ分析手法の調査研究:データの種類や解析手法に応じた適切な分析手法の選定につなげるために、プライバシを保護したままデータを分析するための要素技術を調査研究し、また集合値データに対する匿名加工手法の提案と評価を行った。
- 大規模・長期実証実験 個人情報保護等の観点からの技術的及び法的な検討: 開発に参画したプライバシフィルタを通して収集された大規模ログデータに対して、提案するユーザ間類似度を用いて、データの特性を考慮したユーザ推定を行い、プライバシリスク分析を実施した。
- プライバシ保護に関わるガイドライン（案）の作成に向けた調査研究: Web アクセス履歴に関して、パーソナルデータを活用する際に配慮すべき事項や対処法等をまとめたガイドラインを作成した。

3-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）

- - Web サイトのリソース統計情報を用いたフィッシング検知システムの提案と国際会議での発表を行った。提案方式は、Web サイトを構成する HTML ファイルや画像などのリソース構成情報の類似性からフィッシングサイトを検知するものである。その結果、提案方式は、高い精度で高リスク遷移を検知でき，低リスク遷移の中でも実際には悪性サイトへ遷移するようなリスクの高い遷移を検知できることが分かった。
- - Web サイトの遷移の特徴を用いた悪性サイトへ至る遷移の推定手法の提案を行い、研究会で

の発表を行った。悪性サイトへ至るまでの遷移と良性サイトへ至るまでの遷移の間には特徴の差異が見られると仮定して推定手法を検討した。PC 版の実証実験のデータを分析して、悪性サイトへ至る直前までの遷移と良性サイトへ至る直前までの遷移の特徴を抽出した。

3-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）

- ユーザクローラを用いて、ブラウザセンサのユーザが接続するネットワークのゲートウェイ機器のポート開放状況を検査し、ブラウザセンサと連動して検査結果をユーザに直接提示する実証実験を前年度から継続して実施した。
- 実証実験による評価の結果、累計 58 名に通知を行い、注意喚起ページに到達したのは 26 名（約 45%）であり、視覚的にユーザが気づきやすいデザインなど改善の余地があることがわかった。一方、通知ページに到達した 26 名のうち、意図的なポート開放を行っておらず、改善が必要であることが確認できた7名のうち、6名は最終的に改善が確認できた。このことから、ブラウザセンサを介した注意喚起には一定の効果が認められた。

3-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までに検討、構築、改良したシステムの評価を行った。
- 前年度までに Amazon EC2 上に Docker を用いて構築したハニーポット群により、Web アプリケーションフレームワーク、Web アプリケーションサーバ、および、Web アプリケーション等を狙った攻撃を観測した。具体的には、2020/04/1～2020/12/31 で累計 264 万件超の攻撃を観測し、789 件のユニークなマルウェア検体を収集した。

3-E　基盤アップデート機能開発（KDDI 総合研究所）

- 2020 年４月５月６月にかけてモバイル版の実証実験アプリのアップデートを行った。これにともなって、攻撃情報分析基盤の機能のアップデートも行った。具体的には、研究開発項目 2-B-3 のモバイル機器向け観測機構開発において開発したアプリケーションのためのサーバ側機能を追加した。また、実証実験参加者に対して、個別に注意喚起やアンケートを実施するための機能にともなって、アンケートの配布など基盤側機能を整備した。
- モバイル版実証実験について、毎週提供している質問を作成して 2020 年度分を追加した。
- 実証実験終了のシナリオについて検討した。実証実験を終了する場合に必要な作業をリストアップして手順をまとめた。また、実証実験を一部変更して継続する場合の方法についても、シナリオおよび手順をまとめた。

研究開発項目４：大規模・長期実証実験

4-A,B 10,000 ユーザ規模（KDDI 総合研究所）

- PC 版実証実験については、2018 年６月から開始しており、2020 年４月１日において参加者が 9,513 名に達した。さらにその後、2021 年３月 31 日の時点において目標としていた 10,000 名を越えて約 10,500 名を達成した。
- モバイル版の実証実験については、2020 年３月から開始しており、2020 年３月 31 日時点において、参加者が 3270 名に達した。また、実証実験の参加終了を申し出て、提供データの削除を求めてきた参加者は、累積で 225 名であった。メールでの問合せは合計 29 件あって、その多くは、スマートフォン機種変更におけるデータのバックアップとリストアによるものであった。

4-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）

- Twitter アカウントを作成して 2020 年度の 1 年間を通して、1 週間に 2 から 3 回程度の投稿を行って実証実験の参加者を募集した。
- Twitter 上において参加者の募集キャンペーンを行ってモバイル版の実証実験参加者を新たに約 250 名増加させることに成功した。
- モバイル版実証実験におけるアプリにおいて、悪性サイトや問題のあるアプリがインストールされたときに参加者へ通知を行うリアルタイム通知機能を実装した。
- 具体的には、悪性サイトをリダイレクトの特徴に基づいて検知する悪性リダイレクト検知、悪性サイトへ誘導される可能性が高い危険な検索ワードに対して警告を発する危険検索ワード検知、リパッケージという手法によって正規アプリを装って配布されるアプリ検知の 3 つの検知機能の実装を行った。
- 悪性リダイレクト検知、悪性リパッケージ検知、危険キーワード検知のそれぞれに対して、攻殻機動隊のキャラクターであるトグサ・サイトウ・パズを割り当てて、それぞれのキャラクターが危険を通知するインタラクティブな機能を実装した。

4-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

- 実証実験の参加規約については、PC 版実証実験およびモバイル版実証実験の両方において、NICT におけるパーソナルデータ委員会において 2019 年度以前に承認済みであるため、2020 年に変更を行わなかった。
- 個人情報保護法の改正やデータ保護のあり方についての情報を収集して、実証実験への影響がないことを確認した。

（8）研究開発成果の展開・普及等に向けた計画・展望

計画

本研究開発では、Web ブラウザ拡張および Android 向けのアプリによるデータ収集機構の開発と、IoT ハニーポットやクローラによる新たな脅威の発見に大きく分類できる。

まず、Web ブラウザ拡張および Android 向けのアプリによるデータ収集機構については、得られた知見をセキュアブレインのフェイクサイトブロッカーといった製品において取り入れていくことを検討する。また、収集したデータを蓄積する分析基盤については、一定期間、取得済みのデータを使って、研究開発を継続できる基盤として運用して、追加の研究成果につなげて、要素技術の社会実装をさらに目指す。

新たな脅威の発見では、研究期間中に 2 つのベンダにおいて製品への展開を実現できた。1 つ目は、株式会社バッファローの Wi-Fi ルータにおける危険 UPnP ブロック・警告機能である。この機能は、新たな脅威の一つとして発見した Wi-Fi ルータにおけるユーザが意図しない UPnP ポートの開放をブロックもしくは警告するものである。2 つ目は、アルプス システム インテグレーション株式会社（ALSI）のフィルタにおいて、研究成果のハニーポットから採取した脅威データを提供した。

新たな脅威に限らず、今後もこれらのように研究開発のなかで得られた知見をベンダへ提供していくことを検討する。また、研究開発ならびに実証実験を通して得られた悪性サイトやそれに関する情報を継続的に収集する仕組みから得られたブロックリストを広く活用する方法を検討する。情報・ブラックリストの提供先としては、NICT/NISC/ICT-ISAC などを検討している。

展望

5 年間の研究開発を通して、Web 媒介型攻撃を取り巻く環境が大きく変化してきている。計画段階では、パーソナルコンピュータの Web ブラウザを対象にした研究であったが、スマートフォンの爆発的な普及によって、モバイル端末にシフトしてきた。さらに、新たな脅威として、IoT 端末における脅威の研究開発をしてきたが、Society 5.0 の推進によってサイバーフィジカルの境界領域への注目がさらに集まることが予想され、フィジカル空間のモノがこれまで以上につながってくることが予想される。

今回の研究開発によって、ユーザ参加型の実証実験を行うためのノウハウや、集まったデータについて、プライバシを確保しながらサイバーセキュリティに関する分析を行う基礎的な技術が確立できたと考える。このような基礎的な技術を使って、まずは研究開発のためのプラットフォームとして実証実験システムの運用を続けて、そのなかに IoT やサイバーフィジカルシステムの新たな脅威を取り扱える機能を具備していくことによって、実用化することができるのではないかと考える。

また、これまでと同様に、研究開発によってもたらされる個別の研究成果については、今回のバッファローや ALSI のように、ニーズがあるベンダに対してタイムリーに提供する実用化が考えられる。このように逐次研究成果と実用化を繰り返しながら、多くの学術的に価値のある研究成果も同時に出せるような研究開発を継続していきたい。