平成29年度研究開発成果概要図 （目標・成果と今後の研究計画）

採択番号：19001

１．研究課題・受託者・研究開発期間・研究開発予算

◆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　：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
◆実施機関　　：(株)KDDI総合研究所、(株)セキュアブレイン、横浜国立大学、神戸大学、(株)構造計画研究所、金沢大学、岡山大学
◆研究開発期間：平成28年度～平成32年度（5年間）
◆研究開発予算：総額599百万円（平成29年度200百万円）

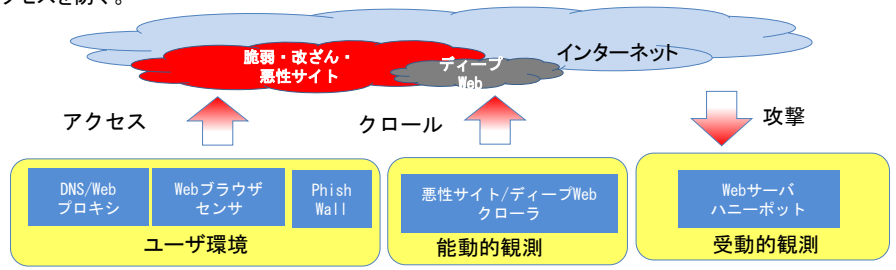
２．研究開発の目標（2019年3月末）

実験参加者を1,000ユーザ集めて大規模実証実験を実施する。本研究開発の課題全体において1日当たり50URL以上の悪性サイト（改ざん・攻撃サイト）を新たに検出する。また、検出された悪性サイトのうち、検知ロジックやブラックリストへの追加が間に合わず、ユーザが当該サイトにアクセスしてしまうケースを全体の1%未満に抑える。

３．研究開発の成果

悪性Webサイトによるサイバー攻撃の観測と対策

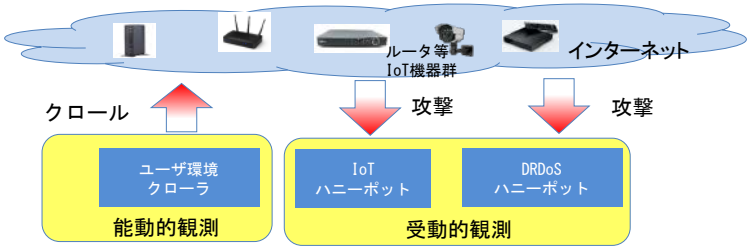
目標:
ユーザ環境・能動的観測・受動的観測の組み合わせによって、インターネットにおける悪性サイトを観測して実態を把握する。ユーザ環境のWebブラウザセンサによって、ユーザの悪性サイトへのアクセスを防ぐ。



研究成果：
・ユーザ環境Webブラウザセンサの開発、キャラクターを使ったユーザインタラクション機能および攻撃分析基盤の実装。
・PhishWallログ分析において、15から30万ユニークユーザの条件の下で、公開ブラックリスト（Google Safe Browsing）に登録されていない悪性サイトをURLパラメータによる検知方式において23件/日、高リスクユーザによる検知方式のおいて300件/日発見。
・RIG ExploitKit(EK)による攻撃を観測。RIG EKがドメインを短時間で変更している実態を把握。また、RIG EKに共通して観測されるURLを発見。
・キャッシュDNSサーバとの突合分析によって、RIG EKのDNSクエリを観測。
・ディープWebクローラーでは、AlphaBayやHansaMarketなどのアンダーグラウンド取引サイトのコンテンツ実態を把握。
・Webサーバハニーポットによって、Struts2を狙った攻撃および付随する検体収集に成功。

Webに関する新たなサイバー攻撃の観測と対策

目標:
IoTハニーポット・DRDoSハニーポット・ユーザ環境クローラなどによって、Webに関する新たなサイバー攻撃の観測。関係機関（ **ICT-ISAC, JPCERT, NISC, メーカー**）への情報提供。



研究成果：
・IoTハニーポットを13か国・地域へのセンサ拡大、累計4万検体以上を収集、Miraiを含むIoTマルウェア大量感染の観測。
・9種類の実機を導入し、WebUI（管理画面）への攻撃の観測を開始、人間の攻撃者によるVPN, DDNS等を用いた踏み台化や自動化された機器情報収集攻撃を観測。
・IoTマルウェア収集後，15分以内に実機ベースの動的解析を行う環境を構築、IoT機器の駆除方法を解析、IoTマルウェア永続感染メカニズムの解析、機器を故障させる新たなIoTマルウェアを世界に先駆けて発見・報告。
・DRDoS攻撃の観測・分析、観測された攻撃の詳細分析により、DDoS対策に用いられるCDN(Contents Delivery Network)を迂回する攻撃を確認。
・これまで知られていないサービスを踏み台として悪用したDRDoS攻撃を観測、ハニーポットを用いたアラートシステムによる国内ISPやオリパラ組織委員会等へのアラート提供。

4. 特許出願、論文発表等、及びトピックス

国内出願	外国出願	研究論文	その他研究発表	プレスリリース報道	展示会	標準化提案
2 (0)	0 (0)	6 (3)	109 (71)	67 (23)	1 (1)	0 (0)

※成果数は累計件数、( )内は当該年度の件数です。

成果アピール・トピック

（1）攻殻機動隊 REALIZE PROJECTとの連携

サイバーセキュリティの実証実験においてアニメーション作品攻殻機動隊を活用することについて、昨年度のAnimeJapan（2017年3月25日）から継続的に反響を得ている。KDDI株式会社のオウンドメディアあである「Time & Space」において取り上げられた(6/5)。また、主婦向けの生活情報雑誌「婦人画報（8月号）」および日本経済新聞でも取り上げられる（7/26）など反響を呼んでいる。

（2）IoT機器に対する攻撃の観測

IoT機器への攻撃の観測では、観測網を13カ国・地域に拡大して観測し、累計4万検体を収集。その結果を学会にて発表することによって、CSS2016学生論文賞、CSS2017奨励賞・学生論文賞、SCIS2017論文賞を獲得。新たなマルウェアを世界に先駆けて発見することによってNHKや日経新聞などにも取り上げられた。さらに、収集した検体情報を20カ国50以上の研究期間に提供。報道発表36件(うちTV報道6件、新聞12件、Web報道多数)、招待講演・基調講演27件、表彰・受賞9件。

（3）ユーザ環境クローラによる調査

家庭用ルータ等のセキュリティ実態調査として、国内アドレスの広域スキャンを実施し、管理用WebUI等が脆弱なホームルータを多数発見した。脆弱性情報を国内メーカ4社に情報提供した。家庭用ルータに留まらず、**重要インフラ**を含む重要施設に設置されている可能性のある重要IoT機器の管理WebUI等のアクセス制御が脆弱である例を**100件強発見**し、NISC、総務省、JPCERT/CC等に報告した。またその結果は、NHK, 読売新聞などで報道された。

5. 今後の研究開発計画

- 1,000規模のユーザを集める大規模な実証実験を実施する。実証実験および本研究開発の課題全体において1日当たり50URL以上の悪性サイト（改ざん・攻撃サイト）を新たに検出する。また、検出された悪性サイトのうち、検知ロジックやブラックリストへの追加が間に合わず、ユーザが当該サイトにアクセスしてしまうケースを全体の1%未満に抑える。
- Webブラウザセンサについては、対応OSやブラウザを追加開発することによって、より幅広いユーザが参加できる環境を構築する。また、ブラウザ内での攻撃検知機能を追加することによって充実させる。
- Webに関する新たな攻撃の観測では、昨年度から成果を上げているIoTハニーポット、DRDoSハニーポット、ユーザ環境クローラを拡張することによって、多様な攻撃を観測できるようにする。