平成30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

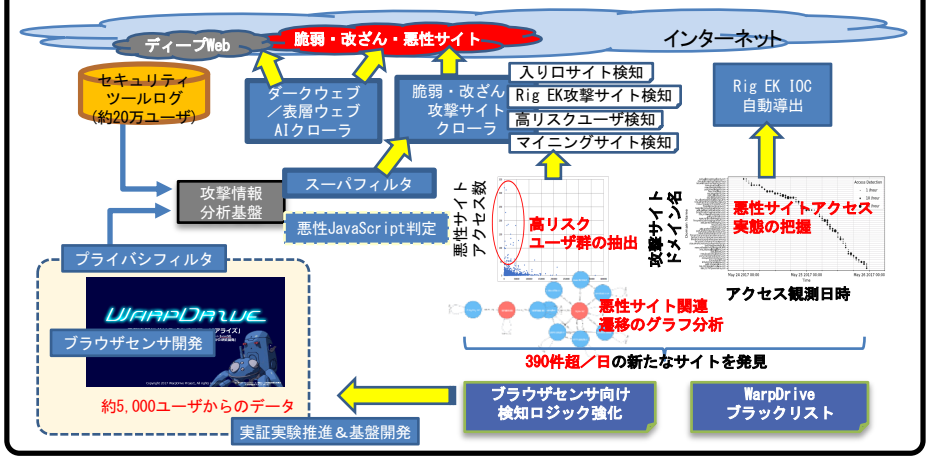
◆課題名　：Web媒介型攻撃対策技術の実用化に向けた研究開発
◆個別課題名　：Web媒介型攻撃の網羅的な観測・分析に基づくユーザ環境のセキュリティ高度化
◆実施機関　：(株)KDDI総合研究所、(株)セキュアブレイン、横浜国立大学、神戸大学、(株)構造計画研究所、金沢大学、岡山大学
◆研究開発期間：平成28年度～平成32年度(5年間)
◆研究開発予算：総額999百万円(平成30年度200百万円)

2．研究開発の目標

10,000ユーザ規模の実証実験時にシステム全体で1日当たり100URL以上の改ざん・攻撃サイトを新たに検出することを目標とする。また、検出された改ざん・攻撃サイトのうち、URLブラックリストへの追加や検知ロジックによる検知が間に合わずに新たなユーザが当該サイトにアクセスしてしまうケース、もしくはブロックの仕組みが提供されないユーザについて警告表示ができないケースが、全体の0.1%未満となることを目標とする。なお、ネットワークセキュリティ上の脅威の移り変わりの速度を考慮し、中間評価の結果を加味して適宜最終目標も修正することとする。

3．研究開発の成果

悪性Webサイトによる攻撃の分析・検知・対策



悪性Webサイトによる攻撃の分析・検知・対策

・攻撃ツールRig Exploit Kit(Rig EK)を使った悪性サイトの実態把握、高リスクユーザに紐づく悪性サイト発見、入り口サイト検知、マイニングサイト検知、悪性サイト関連遷移グラフ分析などを実施した。
・Google社のブラックリストGSB（GSB: Google Safe Browsing）およびマルウェア解析サイトVirusTotalを用いた評価によって新たな悪性サイト*1を390件超/日発見した。
・Rig EK攻撃サイトに関して新たな被害の発生を0に抑制、悪性URL全体を用いると約10人/日のユーザを保護可能な見込みを得た*2。
・これらのブラックリスト配信機構ならびにブロック機能の実装を完了した。

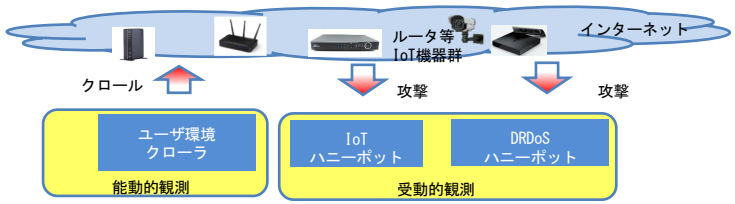
大規模実証実験

・ユーザ環境の情報を収集するWebブラウザセンサ・攻殻機動隊*3のキャラクタ タチコマ*3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を完了した。
・大規模実証実験開始（2018年6月～）。実証実験開始から10ヶ月で7,830インストール数を達成した。これによって、3年目の目標1,000ユーザを大幅に上回った。1日あたり約1,500万URLを定常的に収集している（2019年4月現在）。

*1：未知の悪性サイトはGSBによって検知できなかったURLとしている。
*2 RigEK攻撃サイトの分析と入り口サイトの分析により悪性URLブラックリストを生成の翌日にブラウザセンサに適用したと仮定した場合に、新たな被害の発生を防止できることを確認した
*3：(c) 士郎正宗・Production I.G/講談社・攻殻機動隊製作委員

新たな脅威の発見と対策

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る、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。



新たな脅威の発見と対策

・IoTハニーポット・DRDoSハニーポット、Webサーバハニーポットのそれぞれを開発および運用し、収集した情報を国内外の関係機関へ提供した。
　・IoTマルウェアに関して先進的な成果を上げて27カ国70超の組織への情報提供した。
　・DR-DoS攻撃の観測結果を、国内ISP等へ情報提供した。
・ユーザ環境クローラ
　・国内のユーザ環境クロールの結果として脆弱なホームルータを多数発見し、国内メーカ4社への情報提供した
　・100以上の重要インフラWebユーザインターフェースの問題を発見し、NISC、総務省、JPCERT/CCへ情報提供した。

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
5 (1)	0 (0)	16 (10)	174 (65)	112 (45)	2 (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)学術的成果および対外発表

論文等の発表は合計64件を達成した。内訳として国際会議(査読付き収録論文)6件(最難関国際会議(NDSS)、難関国際会議(DIMVA)での発表が含まれる)、論文誌10件、収録論文(査読なし)13件、一般口頭発表43件を達成した。成果発信としてプレスリリースを7件行ったほか、報道などに取り上げられた件数が38件に上った。受賞が3件あった他、研究成果を他の研究機関へ提供は、相手先が27カ国以上70件以上あった。成果情報の提供先機関には、政府機関、研究機関、機器ベンダが含まれる。

(2)Web媒介型攻撃観測・対策のための大規模実証実験

Web媒介型攻撃を観測するための基盤およびWebブラウザセンサの研究開発を完了した。実証実験の実施にあたって、参加ユーザ募集およびユーザインタラクションのために、アニメーション作品 攻殻機動隊と連携した。2018年6月1日から実証実験を開始して2019年3月時点で合計7,830名のインストールを実現した。実証実験では、既知の悪性サイトを1日につき200件程度観測した。また、セキュリティソフトウェアから収集したWebアクセスログを活用して、未知の悪性サイトを1日あたり約390件発見した。

(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て国内メーカ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。その結果は、NHK, 読売新聞など報道機関より報道された。

5. 今後の研究開発計画

・**ユーザ環境のセキュリティ向上への働きかけ**：実験参加ユーザの中に不要ポート開放事例を176件発見→ ユーザ通知の重要性が明らかになった一方で対応促しの難しさに直面した。タチコマを介した危険性の通知とユーザ反応の調査およびヒューマンファクタ研究プラットフォームとしてWarpDriveの一層の活用を図る。

・**モバイルの脅威への対応**：スマートフォンでは悪用可能な通信経路が多い。SMS、SNS、ブラウザを介さないアプリ自身によるWeb通信等→ ブラウザセンサでは脅威の検知や対処が限定的であるため、端末の設定変更（提供元不明アプリの許可等）、アプリインストール等々、Webアクセス以外の様々なタイミングを捉え脅威の検知・警告を行う仕組みを開発する。

・**Web上の新たな脅威への対応**：ユーザの計算機資源の盗用による仮想通貨マイニングなど攻撃者の狙いが多様化→ 新たな検知ロジックの開発やエンドポイントへの組み込むことを検討する。