令和元年度研究開発成果概要図 （目標・成果と今後の研究計画）

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～令和2年度（5年間）
◆研究開発予算：総額999百万円（令和元年度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

モバイル向け実証実験開始
・これまでのPC向けのWebブラウザセンサに加えてスマートフォン向けのWeb媒介型観測センサを搭載したアプリの研究開発の完成。
・開発したアプリはアニメ作品攻殻機動隊S.A.C.と連携して、登場するキャラクターのひとつであるタチコマをモチーフにしたアプリとして実装。
・アプリを一般ユーザ向けに配布する実証実験を2020年3月16日に開始。
・2020年3月16日に実証実験を開始して1週間で1,000名以上のインストール数を達成。

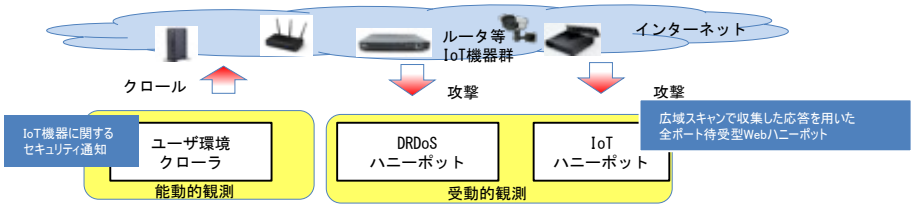
悪性サイトに到達しやすい危険単語の検知
・ユーザがWebアクセスをする際に検索エンジンから悪性サイトへ誘導される確率が最大11倍になる危険単語群を自動的に生成する方式を提案。提案が評価されてCSS2019にて優秀研究賞を受賞。

Torクローラを用いたダークウェブにおける悪性URLの探索
・Torによって構成されるダークウェブをAIによってクローリングする方式を提案。ダークウェブの掲載情報から悪性URLを発見する手法を提案。提案が評価されて情報処理学会奨励賞を受賞。

リパッケージ（改造版）アプリ検知・リダイレクトによる攻撃検知
・Androidにおいて配布されているアプリに第三者が無断で機能を 追加・変更するリパッケージという手法によるマルウェアに着目し リパッケージアプリの検知方式を検討。
・リダイレクトのタイミングから悪性サイトへの誘導を検知する方式の研究開発の完成。

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。



・IoT機器に関するセキュリティ通知
無線Wi-Fiルーターなど家庭内のIoT機器がマルウェアに感染する事例が多く報告されている。マルウェアに感染してしまう恐れのあるIoT機器を効率的に発見する手法を提案して、PC版の実証実験の基盤を通じてユーザに通知する実験を実施。

・広域スキャンで収集した応答を用いた全ポート待ち受け型Webハニーポット
全ポート待ち受けして広域スキャン結果を応答に反映する新型IoTPOTを開発(CSS2019で発表、最優秀論文賞)。広域スキャン結果から実質的に静的に利用されているIPアドレスを抽出し、ポート待ち受け状況とハニーポットへのアクセス状況を調べ、十数種類の機器について感染状況がより明確に把握できることがわかった。

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	標準化提案	プレスリリース 報道	展示会	受賞・表彰
8 （2）	0 （0）	25 （1）	230 （57）	0 （0）	136 （26）	2 （0）	22 （5）

※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）スマートフォンを対象とした大規模な実証実験の開始

スマートフォン向けのWeb媒介型観測機構の実装を完成して大規模な実証実験を開始した。スマートフォン向けの観測エンジンでは、スマートフォンのOSなどを改変することなくインストールすることができるため、通常のアプリ配布サイト経由で配布することができ、開始から1週間で1,000を越える参加者を集めることができた。また、アプリ開発にあたって、アニメ作品攻殻機動隊S.A.C.との連携を継続して、作品登場するタチコマをモチーフにしたユーザインターフェースを開発した。

（2）学術的成果および対外発表

論文等の発表件数として合計79件を達成した。内訳としては、国際会議（査読付き収録論文）6件（難関国際会議（IEEE IMでの発表が含まれる）、論文誌10件など多くの学術的な成果を達成した。また、上記のスマートフォンを対象にした実証実験について、プレスリリースを受託7者から7件行ったほか、リリース後1週間で日経新聞を含む7つのメディアにおいて取り上げられた。

（3）ユーザ環境のセキュリティ向上への働きかけ実験の実施

昨年度から発見されている不要なポートが解放されているなどの脆弱なユーザ環境の実証実験参加者に対して、実証実験の基盤及びアニメキャラクターを通した働きかけの実験を行った。ユーザに対して通知をするとともに、アンケートおよびメールによるフィードバックを得た。

5. 研究開発成果の展開・普及等に向けた計画・展望

・ユーザ参加型の実証実験基盤:

2020年3月に開始したモバイル版の実証実験の参加者の維持および増加。PC版・モバイル版ともに収集データを分析し、より多くの新しい攻撃の事例を発見するとともに攻撃対策を検討する。モバイル版の収集データについて集中的に分析を進め、スマホ特有の攻撃事例を発見する。プロジェクト終了以降におけるユーザ参加型の実証実験基盤の研究開発への活用方法および実用化の方法を策定する。

・基盤を活用したユーザ環境へのセキュリティ向上働きかけ:

2019年度に引き続いて実証実験基盤を活用したユーザ環境へのセキュリティ向上の働きかけを行う。脆弱な設定のIoT機器を持つユーザへの通知実験や危険なセキュリティの振る舞いをしているユーザへの通知実験を行う。

・Web上の新たな脅威への対応の拡充:

これまで多くの成果を挙げてきたIoTハニーポット・DRDoSハニーポットについては、すでに継続的に活用されているが、新しく登場する攻撃などに柔軟に対応できるようさらに拡張して攻撃観測インフラとしての完成度を上げる。