平成28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・実施機関・研究開発期間・研究開発予算

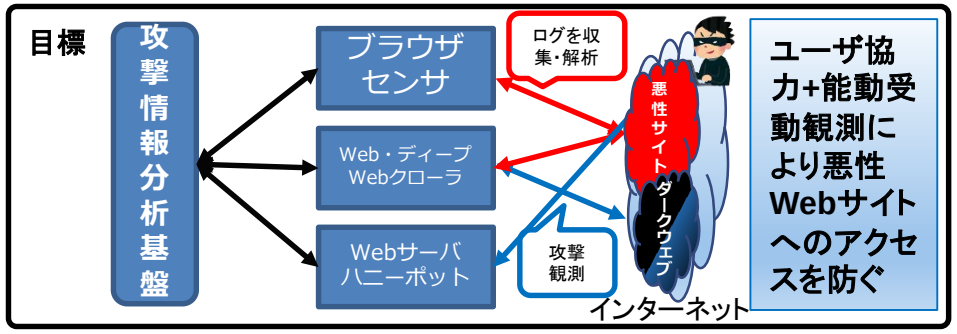
◆課題名　：Web媒介型攻撃対策技術の実用化に向けた研究開発
◆副題　：Web媒介型攻撃の網羅的な観測・分析に基づくユーザ環境のセキュリティ高度化
◆実施機関　：(株)KDDI総合研究所、(株)セキュアブレイン、横浜国立大学（吉岡克成）、神戸大学（小澤誠一）、(株)構造計画研究所、金沢大学（満保雅浩）、岡山大学（山内利宏）
◆研究開発期間：平成28年度～平成30年度（3年間）
◆研究開発予算：総額599百万円（平成28年度200百万円）

2. 研究開発の目標（2019年3月末）

1,000ユーザ規模の実証実験時に提案システム全体で1日当たり50URL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が、全体の1%未満となることを目標とする。

3. 研究開発の成果

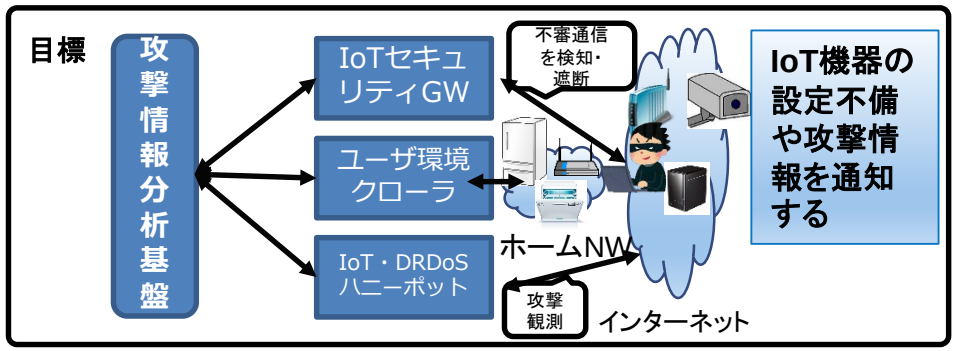
悪性Webサイトによるサイバー攻撃の観測と対策



成果

1) Windows版 ChromeとMac版 Chromeで基本機能が動作するブラウザセンサを実装し、ブラウザAddOnがアクセス情報を収集し、ブラウザ本体と通信し情報を送信する仕組みを開発した。
2) AI技術を用いてディープ/ダークWebサイトを自動的にクローリングし、サイバー攻撃に関連したWebコンテンツを高速に収集するAIディープ/ダークWebクローラを開発し、サイバー攻撃関連サイトを14発見した。
3) 攻撃情報分析基盤の基本機能として大規模なWebアクセスログとブラックリストの突合を行う構成を実装した。
4) 大量に収集されるURLについて高速に良悪性判定を行うスーパーフィルタを開発し、その判定基準について研究を行った。
5) 大規模実証実験開始に向け攻殻機動隊 REALIZE PROJECTとの連携を開始した。

Webに関する新たなサイバー攻撃の観測と対策



成果

1) IoTマルウェアに関連する攻撃パケットの特徴を調査し、IoTセキュリティGWに攻撃パケットの検知遮断を行う機能を実装した。
2) IoT機器が有する管理用のWebインターフェイスに対する攻撃を観測するハニーポット（IoTハニーポット）を構築し、実インターネット上での観測を行った。
3) IoT機器のユーザ環境をクローリングする機能開発の事前調査として、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を開発し、調査を行った。
4) Androidにおけるブラウザを経由しないWebアクセスを観測する手法について検討し、プロトタイプ実装から実現可能であることを明らかにした。
5) 数十万ユーザ規模のアクセスログからユーザ特定につながるリスクについて考察を行った。

4. これまで得られた成果（特許出願や論文発表等）

	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
Web媒介型攻撃対策技術の実用化に向けた研究開発	2 （ 2 ）	0 （ 0 ）	3 （ 3 ）	38 （ 38 ）	43 （ 43 ）	1 （ 1 ）	0 （ 0 ）

※成果数は累計件数、（ ）内は当該年度の件数です。

（1）攻殻機動隊 REALIZE PROJECTとの連携開始

実証実験参加者を十分確保するために、攻殻機動隊 REALIZE PROJECTと連携を開始した。当該プロジェクトはアニメ・コミックス「攻殻機動隊」の技術を研究開発によって実現することを目的に活動している。本研究開発の実証実験では攻殻機動隊のキャラクターを起用し、実証実験の参加者に対して攻撃遮断の通知をしたり、攻撃回避のためのアドバイスをしたりすることで実証実験参加継続を促す。これらのコンセプトについて、2017年3月25日に開催されたイベントAnime Japan 2017において発表展示するとともに、ポータルサイト(https://warpdrive-project.jp/)を構築した。

（2）脆弱なIoT機器に関する情報提供

IoT機器へのサイバー攻撃を観測するハニーポットの高度化を進め、観測結果を公的機関等に提供すると共に学会等で発表を行った。このことについて、TV報道6件、新聞報道7件、Webでの報道が10件あった。特に、脆弱なIoT機器が非常に短時間、短いものでは38秒でマルウェアに感染するほど、サイバー攻撃が頻繁に発生していることを実験により示したが、この内容は驚きをもって広く報道された。また、国内メーカ2社の製品においてもマルウェア感染している事実を発見し、ユーザに情報提供を行い、対策に貢献した。ユーザ環境のルータ等ネットワーク機器の設定に不備があったり、脆弱性が存在しないかを遠隔から確認するためのユーザクローラ技術を開発する目的でネットワーク探索を実施したが、副産物として家庭用ルータ以外の多様な機器においてアクセス制御に不備があることを発見し、公的機関に情報提供を行った。

5. 今後の研究開発計画

- ブラウザセンサは実証実験の実施に向けて、情報の収集、ブロック機能、Plugin解析エンジンの機能を実装する。ブラウザ本体のインストーラ、ブラウザに種類ごとのマーケット等にブラウザAddOnを配置して、センサ機能を一般利用者が利用できる状態にする。
- ディープ/ダークWebサイトクローリングでは探索先優先度の決定にヒューリスティックスや学習メカニズムを導入して新規ドメインの発見確率を改善し、高速かつ大規模にTor hidden serviceの情報を収集できるような設計・構築をする。これにより、Torで見つかっている5,205ドメインを超えるドメインを検索できるようにし、サイバー攻撃に関するサイトやフォーラムをモニタリングできるようにする。また、開発したディープ/ダークWeb AIクローラを他のhidden service（I2PやFreenetなど）にも適用し、情報収集することを検討する。
- ブラウザセンサのユーザ環境内の機器に対して能動的にアクセスを行い、ルータ等のゲートウェイ機器のセキュリティ設定や脆弱性の有無を検査する方式を実装する。
- 実証実験に向けて収集データの要件を確定し、第三者委員会等の承認を得る。承認された内容に沿ってセンサ等の実装を行う。