令和2年度研究開発成果概要図 （目標・成果と今後の成果展開）

1．研究課題・受託者・研究開発期間・研究開発予算

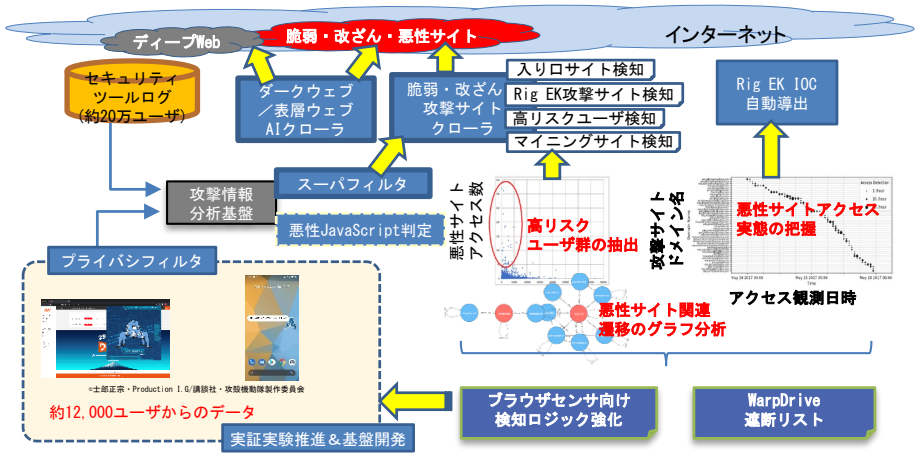
◆研究開発課題名 ：Web媒介型攻撃対策技術の実用化に向けた研究開発
◆副題 ：Web媒介型攻撃の網羅的な観測・分析に基づくユーザ環境のセキュリティ高度化
◆実施機関 ：株式会社KDDI総合研究所、株式会社セキュアブレイン、国立大学法人横浜国立大学、国立大学法人神戸大学、株式会社構造計画研究所、国立大学法人金沢大学、国立大学法人岡山大学
◆研究開発期間 ：平成28年度～令和2年度（5年間）
◆研究開発予算 ：総額1000百万円（令和2年度200百万円）

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。

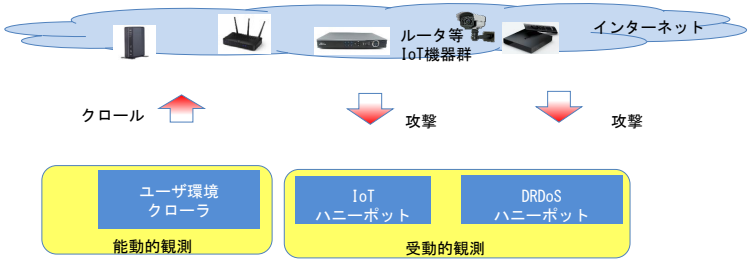
3．研究開発の成果

悪性Webサイトによる攻撃の分析・検知・対策



・Webブラウザにおいて広く実装されている悪性サイト遮断方式としてGoogle社による遮断GSB（GSB: Google Safe Browsing）とウィルス対策ソフトや悪性サイト遮断サービスを横断的に検索できるVirusTotalによって「未知の悪性サイト」を定義。
・アニメ作品攻殻機動隊と連携した大規模な実証実験を実施、2018年6月からPCのWebブラウザ向け実験、2020年3月からスマートフォン向けの実験を行い、合計12,000名以上の参加者を集めた。
・入りロサイト検知・RIGEK攻撃サイト検知・高リスクユーザからの悪性サイト抽出・危険検索ワードによるリスク通知・ディープダークウェブクローリングによる悪性サイト収集など、悪性サイト検知/遮断アルゴリズムを15以上提案して研究会発表や論文発表を行った。
・PC版の実証実験・モバイル版の実証実験により得られたデータ、セキュリティツールログ、クローリングによって収集したURLに、それらのアルゴリズムを適用することによって、1日あたり少なくとも428件の未知の悪性サイトを発見した。

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ハニーポット：他の研究に先駆けてIoTハニーポットの取り組みを開始して、観測範囲を16カ国に拡大して、連続して5年間運用を行った。結果として攻撃検体を158,779発見して、32カ国・地域の105の組織へ提供した。学術論文は、国内研究会で論文賞を多数受賞したほか、NHKや読売新聞にて報道された。
・DRDoSハニーポット：これまでに知られていない悪用されるサービス（memcachedなど）を発見してDRDoS攻撃を観測、攻撃の標的になっている組織を特定して、オリパラ組織委員会や国内ISPへ通知、攻撃インフラの特定や活動を分析した。
・ユーザ環境クローラ：ホームルータに留まらず、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500件強発見し、NISC、総務省、JPCERT/CC等に報告した。

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	標準化提案	プレスリリース報道	展示会	受賞・表彰
13 （ 5 ）	0 （ 0 ）	34 （ 9 ）	273 （ 43 ）	0 （ 0 ）	174 （ 38 ）	7 （ 5 ）	29 （ 5 ）

※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S.A.Cとの連携による実証実験

実証実験の参加者募集および継続的な参加を促すためアニメーション作品攻殻機動隊S.A.C.との連携を決定、2017年AnimeJapanにて発表、2018年作品中のキャラクタータチコマを起用したPC版の実証実験を開始、2020年タチコマを起用したモバイル版の実証実験を開始した。それぞれプレスリリースを行ってメディアに多数取り上げられた。

(2) IoT機器セキュリティに関する先駆的な研究

IoTハニーポットおよびDRDoSハニーポットには、世界に先駆けて取り組んでおり、収集した検体や攻撃の標的情報を国内外の様々な組織へ提供した。オリパラ組織委員会ほかNISC/総務省/JPCERT等に報告。また、研究成果がバッファローのWi-FiルータやALSIの製品に組み込まれて実用化された。

(3) 学術的成果および対外発表

研究論文34件、査読付き収録論文25件、収録論文93件と多数の学術的な成果を挙げており、目標を大幅に上回っている。進行中の研究がいくつか残っているため、さらに成果が上振れする見込みである。学術成果の中には、セキュリティにおけるトップカンファレンスのひとつNDSSや難関国際会議IEEE IM/DIMVA/RAIDが含まれている。また、研究成果がテレビ・新聞・ニュースサイトなどにも174件取り上げられた。

5. 研究開発成果の展開・普及等に向けた計画・展望

・本研究開発の成果は、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ーによる新たな脅威の発見に大きく分類できる。
・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PhishWallなどの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、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つのベンダーにおいて製品への展開を実現できた。ハニーポットから得られた情報は、32カ国・地域の105の組織へ提供しており、国内ではオリパラ組織委員会、国内ISP、NISC、総務省、JPCERT/CCへ報告した。情報提供はそれぞれの組織の要望に応じて継続提供し、普及を図っていく予定である。