終了評価研究開発成果概要図 （目標・成果と今後の成果展開）

採択番号：161

1. 研究課題・実施機関・研究開発期間・研究開発予算

◆課題名　　：ドライブ・バイ・ダウンロード攻撃対策フレームワークの研究開発
◆副題　　：巧妙化・組織化するサイバー攻撃に対抗できる利用者参加型 互助自警フレームワーク
◆実施機関　　：（株）ＫＤＤＩ研究所、（株）セキュアブレイン
◆研究開発期間：平成24年7月1日～平成28年3月31日
◆研究開発予算：４７２百万円（平成27年度　１０７百万円）

2. 研究開発の目標

本研究開発では、利用者参加型 互助自警フレームワークという新しいフレームワークを提案して、一般参加者およびセキュリティ研究者・研究機関への浸透させることを最終目標とする。

3. 研究開発の成果

研究成果1：DBD攻撃対策フレームワークの実証実験

- 1,000人規模の参加者を募った実証実験を実施し、目標である1,000人の参加、1日5万以上のアクセス先情報の収集に対し、それぞれ1,676人の参加者、最大で11万URL/日を得た。さらに450万件ほどのWebサイトのデータが収集され、その中で23件のDBD攻撃サイトのデータ(*1)が収集された。

(“1) 詳細な解析の結果、マルウェアへの感染は確認されなかった

実証実験で得られたデータ

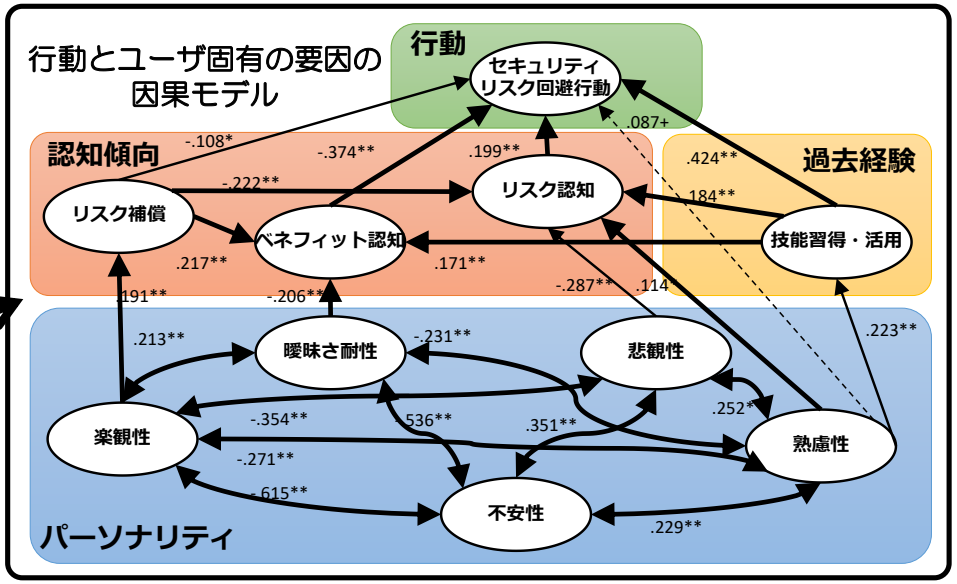
登録ユーザ数	1,676 (12/1現在)
総Webブラウジング情報数 (1日あたりのWebブラウジング情報数)	4,425,689 (81,747)
総ユニークURL数 (総ユニークホスト数)	2,178,381 (34,195)
1日あたりのユニークURL数	50,913

研究成果2：コンテンツ解析によるDBD攻撃検出技術

- 静的解析において、悪性JavaScriptを検知する手法を検討し、それぞれの手法における精度を測定するために良性および悪性コンテンツの収集、およびこれらのコンテンツを使用した評価を行った。その結果、文字出現頻度＋SVMによる良性・悪性判定とフィルタリング処理を併用する手法により99.9%以上の判定精度を達成した。

研究成果3：ユーザのセキュリティリテラシ向上のための検討

- アンケート調査に基づき、セキュリティリスク（セキュリティ被害やインシデントなど）を回避する行動習慣とユーザ固有の要因（認知傾向，学習や被害の経験，性格などのパーソナリティなど）の関係性を解析し、リスクを回避する行動は認知傾向や経験から影響を受け、さらに認知傾向や経験はパーソナリティから影響を受けるという二段構成の因果モデルが存在することを明らかにした。この結果を情報処理学会論文誌に投稿した。



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
ドライブ・バイ・ダウンロード攻撃対策フレームワークの研究開発	8 (3)	0 (0)	3 (0)	26 (8)	1 (1)	0 (0)	0 (0)

※成果数は累計件数、( )内は当該年度の件数です。

（1）トピックス

2015年8月5日にKDDI研究所・セキュアブレインからフレームワークの開発・実験開始に関してプレスリリースを発表した。マイナビ・CNET・インプレスなど大手ニュースメディア5つに取り上げられた。

5. 研究開発成果の展開・普及等に向けた計画・展望

・本研究開発を行っている中でDBD攻撃を取り巻く環境が大きく変わってきている。これまで狙われることがなかったブロードバンドルーターやWebカメラといったIoT機器がDBD攻撃環境の構築に悪用され始めている。また、本研究開発では、PCのWebブラウザを対象にしてきたが、今後スマートフォン・タブレットなどの機器が普及してくることが考えられる。したがって、スマートフォン・タブレット向けのDBD攻撃が増加してくることが予想される。したがって、本件研究開発のフレームワークの対象をIoTやスマートフォンへ拡大して、より幅広い観測フレームワークへと発展させる必要がある。
・これまで収集したデータは、限られた研究者だけで共有されてきた。収集データには、今後のセキュリティ研究へ活用できる見込みが高いため、大学や他の研究組織と共有して分析をすることが考えられる。また、収集データの分析を通した、セキュリティ人材の育成が考えられる。
・今後このような対策のフレームワークをセキュリティリテラシの低いユーザへと普及させることが考えられる。セキュリティリテラシが低いユーザへ対しては、このフレームワークへ参加することに対する動機付けが必要である。したがって、ゲーム性を持たせて教育を促すゲーミフィケーションなどの導入によって、フレームワークの裾野を拡げていくことを検討している。