平成 27 年度研究開発成果概要書

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
採 択 番 号 ：161
個別課題名 ：
副　　題 ：巧妙化・組織化するサイバー攻撃に対抗する利用者参加型互助自警フレームワーク

（1）研究開発の目的

本研究開発では、利用者が自ら参加することによってセキュリティに対する知識を深めたり意識を高めたりしつつ、相互に情報を共有しながら自警的な活動をすることによって、ドライブ・バイ・ダウンロード攻撃（DBD 攻撃）をはじめとする巧妙化・組織化するサイバー攻撃に対抗することを目的とする利用者参加型 互助自警フレームワークの構築を目的とする。

本フレームワークは、利用者ブラウザにおけるセンサと利用者向けのセンタという構成をとる。利用者はブラウジングしながら情報を提供し、攻撃サイトを発見した際にはそれを通報する。一方、センタは収集した DBD 攻撃サイト情報を利用者に配信して被害の拡大を防御する。ここで、利用者は一方的な通報者となるだけでなく、当フレームワークへの参加によってセキュリティの知識を習得するなど何らかの利益が得られる仕組みを提供する。また、センタ側は、収集した攻撃に関する情報をセキュリティ研究者やセキュリティ対策企業との間で交換することによって、セキュリティ対策コミュニティへ還元する。

（2）研究開発期間

平成 24 年度から平成 27 年度（4 年間）

（3）実施機関

株式会社 KDDI 研究所＜代表研究者＞、株式会社セキュアブレイン

（4）研究開発予算（契約額）

総額　472 百万円（平成 27 年度　107 百万円）
※百万円未満切り上げ

（5）研究開発課題と担当

課題 1：DBD 攻撃大規模観測網構築技術の開発
- 課題 1-a.　観測用センサの開発（(株)KDDI 研究所）
- 課題 1-b.　大規模センタの開発 （(株)KDDI 研究所）

課題 2：DBD 攻撃分析・対策技術
- 課題 2-a. DBD 攻撃分析技術の開発
- 課題 2-a-1. リンク構造解析および動的解析 （(株)KDDI 研究所）
- 課題 2-a-2. 静的解析 （(株)セキュアブレイン）
- 課題 2-b. DBD 攻撃対策技術の開発 （(株)KDDI 研究所）
- 課題 2-c. 他の研究機関・組織との連携 （(株)KDDI 研究所）

課題 3：DBD 攻撃対策フレームワーク実証実験
- 課題 3-a. 実利用者参加による実証実験参加者対応（(株)セキュアブレイン）
- 課題 3-b. 実利用者参加による実証実験 （(株)KDDI 研究所）

（6）これまで得られた成果（特許出願や論文発表等）

		累計（件）	当該年度（件）
特許出願	国内出願	8	3

	外国出願	0	0
外部発表	研究論文	3	0
	その他研究発表	26	8
	プレスリリース・報道	1	1
	展示会	0	0
	標準化提案	0	0

（7）具体的な実施内容と成果

課題１：

- 大規模センタ、観測センサにおいて、データ受信機能のロードバランシングなどシステム面の強化、およびプログラムの不具合の修正などを実施し、フレームワークを用いた実証実験を無事終了させた。
- 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。

課題２：

- 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。
- リンク構造解析において、リダイレクト段数にもとづいて悪性コンテンツのダウンロードを検出する手法の評価を行い、３段以上を悪性とみなす場合において 4.2%の偽陽性が確認された。フレームワークへ導入したところ、11 件検出されたがいずれも誤検知であった。

課題３：

- 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(マルウェアの感染には至っていない)が収集された。