# 平成 26 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 26 年度　114 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 | 5 | 3 |
| | 外国出願 | 0 | 0 |
| 外部発表 | 研究論文 | 3 | 1 |
| | その他研究発表 | 18 | 10 |
| | プレスリリース・報道 | 0 | 0 |
| | 展示会 | 0 | 0 |
| | 標準化提案 | 0 | 0 |

（7）具体的な実施内容と成果

- 大規模センタ、動的・静的解析システムを統合して実証実験システムを構築し、実際に 100 人程度の参加者にブラウザセンサを配布して、セミクローズドな実証実験を実施した。
  - セミクローズドな実証実験の実施において、大学、関係会社等へ実証実験参加を募り、100 名の参加者を得た。
  - 実証実験の実施に先駆けて、有識者を評価委員として招いて実証実験の実施内容の検討会を実施し、参加者のプライバシ保護の観点から実証実験の実施内容、規約など文書の内容に問題がないか確認した。検討会での指摘事項をもとに実施内容、各文書を修正し、参加者のプライバシに適切に配慮した形で実証実験を実施した。
- Web サイトのリンク構造の解析にもとづく悪性サイトの検出手法において、ダウンロード時のページ遷移の振る舞いに着目したドライブ・バイ・ダウンロードを検出する方法､Web サイトの遷移元/遷移先サイトの数にもとづき攻撃サイトを検出する方法を考案し、基礎評価にて効果を確認した。
  - 各方法について特許出願(3 件)を実施した。また、基礎評価の結果について外部発表を行った(国際会議(研究論文)1 件、その他研究発表 5 件)。
  - ダウンロード時のページ遷移の振る舞いに着目したドライブ・バイ・ダウンロードの検出方法について、実際に大規模センタに実装して実証実験による試験運用を開始した。
  - Web サイトからリダイレクトされるサイトの変化に着目して改ざんされた Web サイトを検出する方法について、リダイレクト先のサイトのリンク構造を加味して判定を行うように手法を改良し、偽陽性率を 1.5%に低減した。
- 静的解析について追加の評価と手法の改良を実施した。
  - インターネットから収集した良性データ 1,000 件と悪性データ 950 件を用いて静的解析エンジンの評価を実施し、文字出現頻度による判定方法の評価において 90%以上の高い正答率を得られた。ベイジアンフィルタによる判定方法の評価においては正答率 77.5%という結果が得られた。
  - 文字出現頻度判定におけるフォールスネガティブの低減策として、ベイジアンフィルタによる判定方法との併用について検討、評価したところ、文字出現頻度判定で良性と判定された 150 件に対してベイジアンフィルタ判定を併用することで 25 件を悪性と判定することができた。
- 最終年度に実施する 1000 人規模の一般のユーザを募った実証実験の実施に向けた準備を進め、参加申し込みサイト、申し込み受付業務フロー、電話および電子メールによるサポート業務フローの設計を完了した。