平成２５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
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）委託先

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 25 年度　121 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）これまで得られた研究開発成果

		（累計）件	（当該年度）件
特許出願	国内出願	2	1
	外国出願	0	0
外部発表	研究論文	2	1
	その他研究発表	8	5
	プレスリリース	0	0
	展示会	0	0
	標準化提案	0	0

（７）具体的な成果実施内容と成果

(1) 大規模センタ・観測用センサについて機能拡張、チューニングを実施し、実証実験のためのフレームワークの環境整備を完了した。

・(ブラウザ型センサ) 実証実験での配布に向けて、ユーザがセンサによって収集される情報を制限できる仕組み、サポート機能を新たに導入した。さらに、リダイレクトのもととなる JavaScript を特定する機能を追加し、センタに有益な情報を送信できるように機能を強化した。

・(Web プロキシ型センサ、DNS サーバ型センサ) 設置先のネットワーク環境に応じた設置が可能となるように、また、センサの故障が設置先ネットワークに与える影響を軽減するために、ネットワーク上のトラヒックを監視して必要な情報を抽出し、センタに送信する機能を新たに導入した。

・(大規模センタ) 100 万ユーザからのログの送信に耐えられるように、ログの受信機能を分散して処理負荷を軽減するようにシステム設計を改良した。設計の変更にあわせてセンサとのプロトコルの修正を実施した。

(2) DBD 攻撃分析・対策技術について、各解析手法の基礎検討を完了した。各解析手法の連携により、悪性サイトを効果的に検出する方法について基本方針を確立した。

・(動的解析) PDF ファイルを動的解析に対応させるとともに、PDF に埋めこまれた、JavaScript をエミュレーション環境で動作させ、情報を収集できるようになった。また、動的解析の結果から解析対応コンテンツの良性悪性を判定し、センタに通知する機能を新たに導入した。目標値であるコンテンツ投入から 10 分以内の解析を達成した。

・(静的解析) JavaScript の抽象構文木を用いた単純ベイズ分類器による悪性 JavaScript 分類手法の実装を行った。また、JavaScript の文字出現頻度を特徴パラメーターとしてサポートベクターマシンを用いて学習し、悪性 JavaScript を検出する手法を提案した (研究発表 1 件)。評価の結果、いずれも 90%以上の高い適合率を示し、提案手法の有効性を確認した。

・(リンク構造解析) 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､改ざんされた Web サイトを検出する手法を考案し特許を出願した(特許出願 1 件)。Web アクセスサーバのログから、改ざんサイト、正常サイトのリンク構造を解析し、一部サイトにおいては当該手法にて検出できることを確認した。評価結果を国際会議、国内研究会などで発表した(研究論文 1 件、研究発表 4 件)。一部の正常サイトにおいて、リダイレクト先のサイトが大きく変動する現象がみられたため、引き続き手法の精査を進める。

(3) 実証実験に向け､参加者に配布する利用規約､実験同意書のドラフトの作成、参加者のサポート体制の整備を進めた。

・参加者に配布する実証実験参加規約、実験参加同意書、ブラウザ型センサ資料許諾約款等必要書類を専門家の意見を基に草稿を作成した。
・参加者の注意を促すために、実証実験参加規約、実験参加同意書の内容を説明する資料を Web で公開するよう原稿を作成した。