(26-1)

平成26年度「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」の研究開発目標・成果と今後の研究計画

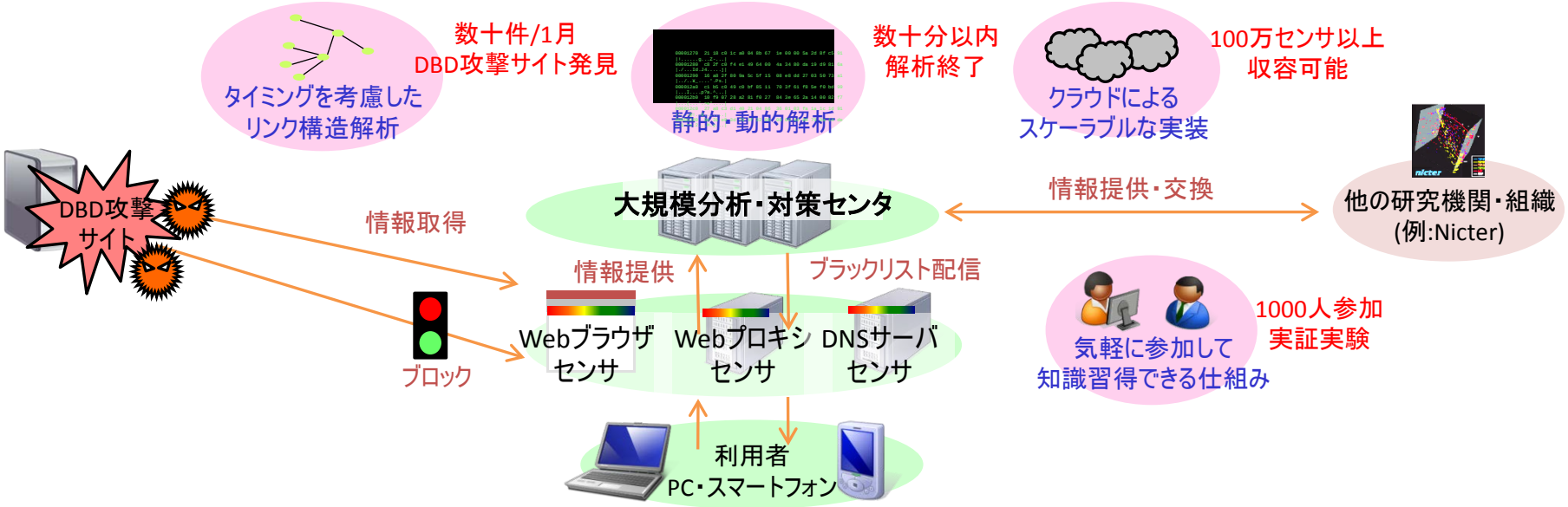
1. 実施機関・研究開発期間・研究開発予算

◆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
◆研究開発期間　平成24年度から平成27年度（4年間）
◆研究開発予算　総額472百万円（平成26年度 114百万円）

2. 研究開発の目標

【全体】 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、Webプロキシセンサ、DNSサーバ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。



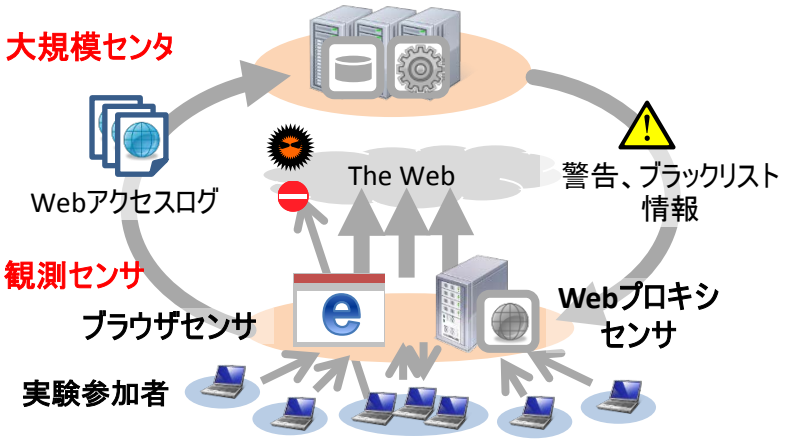
【平成26年度】 100名規模の参加者によるセミクローズドな実証実験を実施する。当該実験の中で顕在化したソフト面、システム面、運用、サポート面での課題について改善する。当該実験で得られたデータをもとに各種解析方式の検証、高度化を実施する。利用者の参加を促す仕組みについて引き続き検討を行い、翌年度の実証実験での運用を目指す。

研究開発目標

研究開発成果

DBD攻撃対策フレームワーク実証実験

開発したDBD攻撃対策フレームワークを用いて、100人規模のセミクローズドな実証実験を実施する

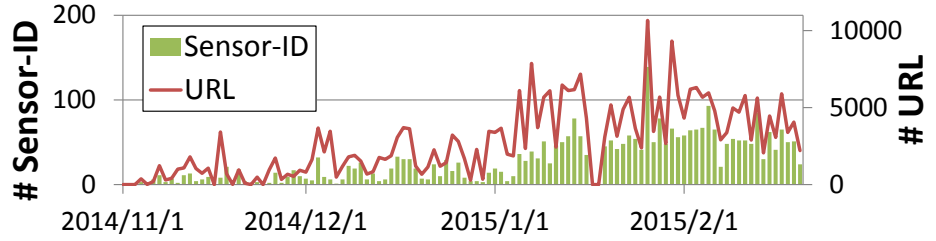


研究開発成果: 100人規模のセミクローズな実証実験を実施

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。

□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の上、実験を実施した

- 2014年11月～2015年2月の実施で、1日平均4,431URLのデータが収集された



DBD攻撃分析・対策技術

リンク構造解析: リダイレクト先ホストの変化にもとづく悪性サイトの検出手法の検証、さらにリンク遷移のグラフの構造の変化に着目するなど検出手法の高度化を実施する

静的解析: 静的解析による検知の仕組みを確立する

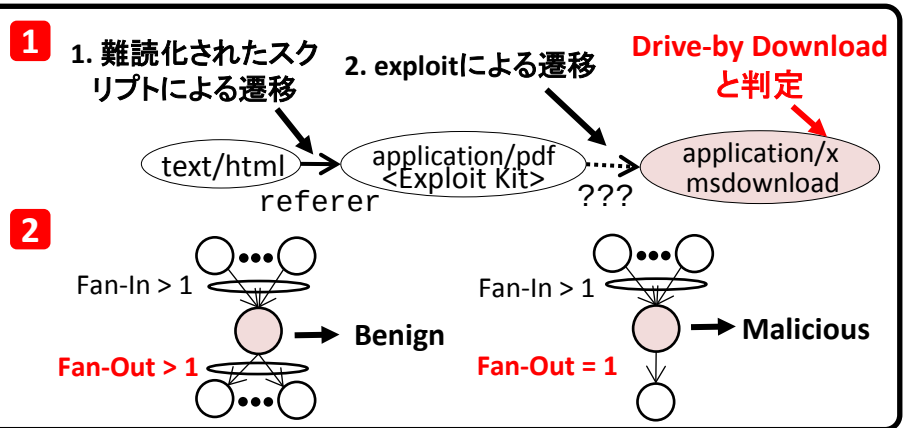
研究開発成果: JavaScriptの静的解析技術

□インターネットから収集したデータ(良性1,000件、悪性950件)での評価で、文字出現頻度による判定方法は90%以上、ベイジアンフィルタによる判定方法は77.5%の正答率であった

- 上記2つの判定手法の併用について検討、評価し、文字出現頻度による判定の検知見逃し数を150件から25件に改善できた

研究開発成果: Webサイトのリンク構造の解析にもとづく攻撃検出技術

- (1)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、(2)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
- 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



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	5 (3)	0 (0)	3 (1)	18 (10)	0 (0)	0 (0)	0 (0)

※成果数は累計件数、（ ）内は当該年度の件数です。

5. 今後の研究開発計画

・1,000名規模の一般参加者によるフレームワークの実証実験を実施する。当該実験の実施にさきがけ、ソフト面、システム面の最終調整を実施する。
・上記実証実験で得られたデータをもとにフレームワーク全体の有用性の評価、ならびに各種解析方式の検証、評価を実施する。得られた成果を対外的に発表する。