平成25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に関する研究開発」の研究開発目標・成果と今後の研究計画

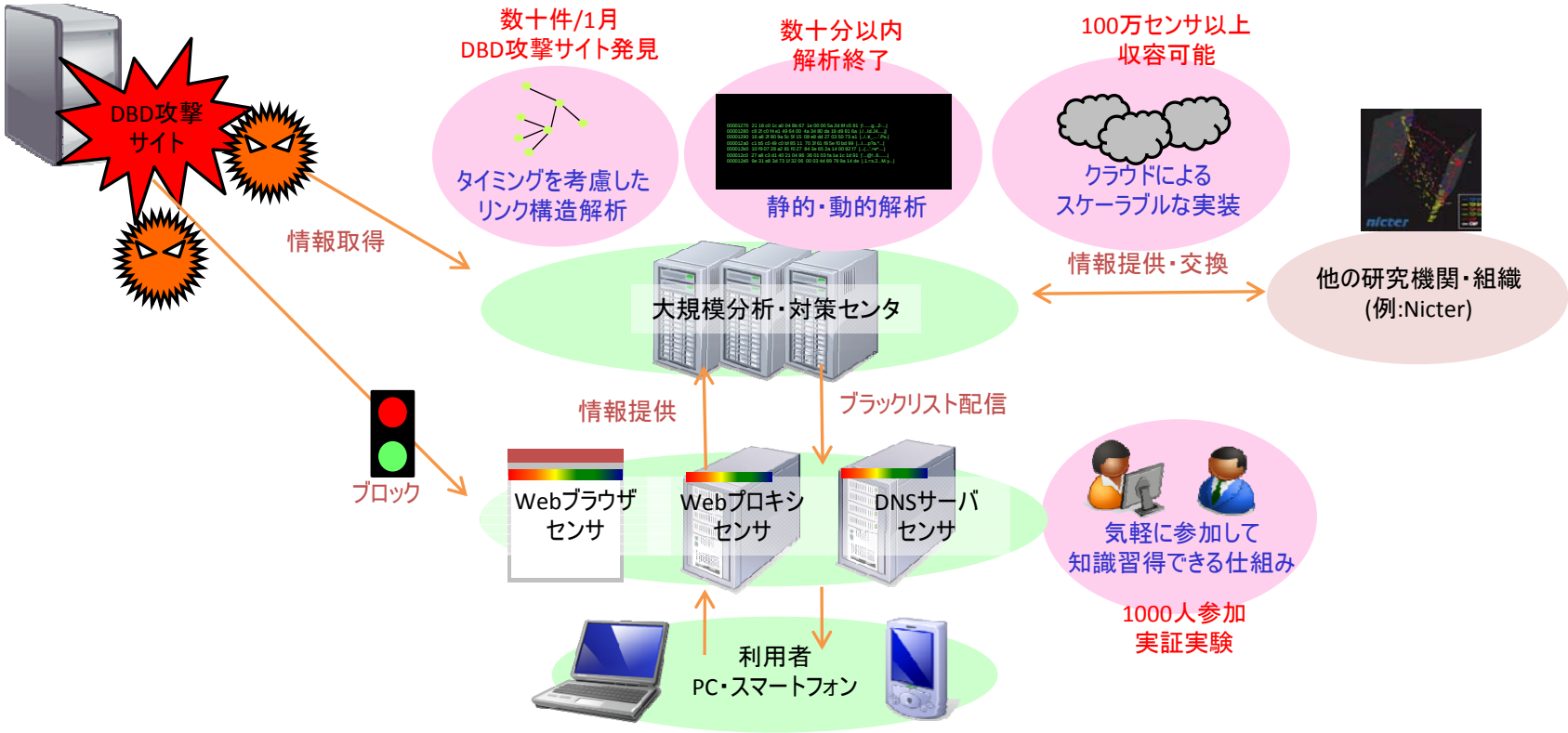
1. 実施機関・研究開発期間・研究開発費

- 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）
- 研究開発費: 総額472百万円（平成25年度 121百万円）

2. 研究開発の目標

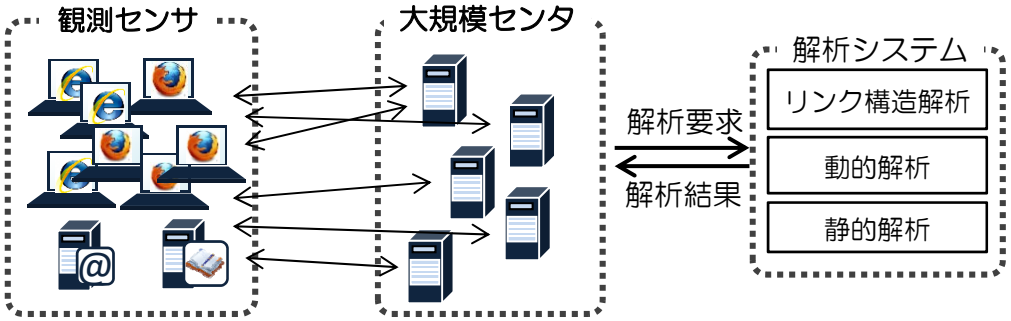
本研究開発では、利用者が自ら参加することによってセキュリティに対する知識を深めたり意識を高めたりしつつ、相互に情報を共有しながら自警的な活動をすることによって、ドライブ・バイ・ダウンロード攻撃（DBD攻撃）をはじめとする巧妙化・組織化するサイバー攻撃に対抗することを目的とする利用者参加型 互助自警フレームワークの構築を目的とする。

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。



3. 研究開発の成果

大規模観測フレームワークの開発



大規模センタ・観測用センサの機能拡張、チューニングを実施し、実証実験の実施に向けたDBD攻撃対策フレームワークの開発実装を完了

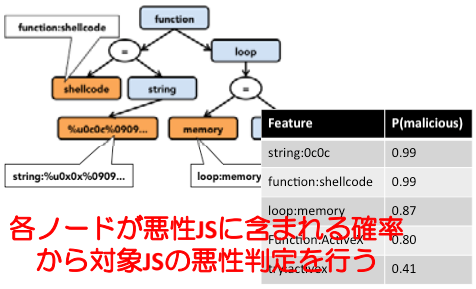
- ブラウザ型センサ: 実証実験での配布に向けた、センサによって収集される情報を制限できる仕組みなどサポート機能の導入。センタに送信する情報の追加(リダイレクトのもととなるJavaScriptの特定など)
- Webプロキシセンサ、DNSサーバセンサ: センサの故障が設置先ネットワークに与える影響を軽減するため、ネットワーク上のトラヒックから必要な情報を抽出してセンタに送信する機能を新たに導入
- 大規模センタ: 100万ユーザからのログの送信に対応すべく、ログの受信機能を分散して処理負荷を軽減するようにシステム設計を改良

各解析技術の考案、基礎検証

静的解析

悪性JavaScriptの抽象構文木、文字出現頻度における特徴をもとに機械学習を用いて良性・悪性判定を行う手法により、90%以上の判定精度を達成

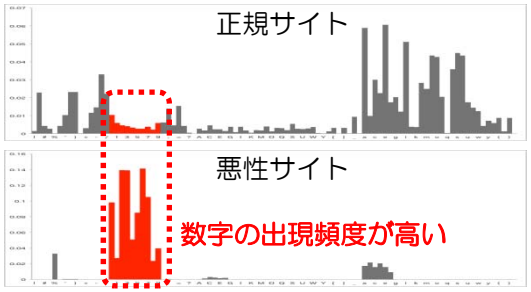
1. 抽象構文木＋単純ベイズ分類器



Feature	P(malicious)
string:0c0c	0.99
function:shellcode	0.99
loop:memory	0.87
Function:ActiveX	0.80
JS/ActiveX	0.41

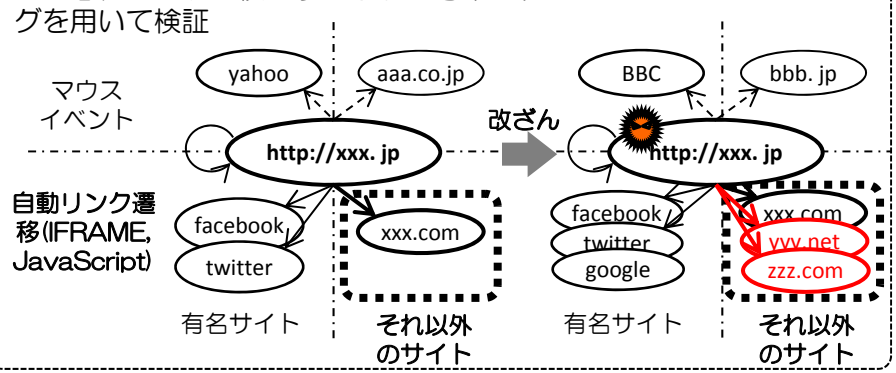
各ノードが悪性JSに含まれる確率から対象JSの悪性判定を行う

2.文字出現頻度＋SVM



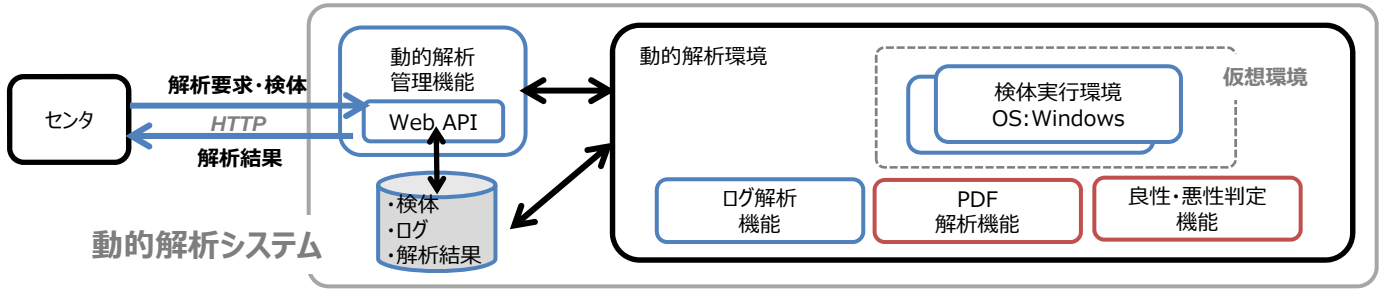
リンク構造解析

IFRAMEタグ、JavaScriptなどによる自動的なリンク遷移に着目して悪性サイトを検出する手法を考案し、Webアクセスサーバのログを用いて検証



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。



4. これまで得られた成果（特許出願や論文発表等）　※成果数は累計件数と（ ）内の当該年度件数です。

	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	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に関する研究開発	2 (1)	0 (0)	2 (1)	8 (5)	0 (0)	0 (0)	0 (0)

5. 研究成果発表等について

（1）国際会議、研究会等での研究成果発表

各解析手法の基礎検討の結果を国際会議、国内の研究会等に投稿、発表し、研究成果を対外的にアピールした。会議中に総務省委託研究「国際連携によるサイバー攻撃の予知技術の研究開発」のプロジェクトメンバーをはじめとする国内外の研究者と、互いの研究動向、攻撃検知技術の最新動向の情報交換、議論を展開した。

- 主な研究成果の発表先
  - 国際会議
    - ✓ AsiaJCIS 2014: T.Matsunaka, et al., *Detecting and Preventing Drive-by Download Attack via Participative Monitoring of the Web*
  - 国内研究会
    - ✓ SCIS 2014: 松中他,ドライブ・バイ・ダウンロード攻撃対策フレームワークにおけるリンク構造解析による改ざんサイト検出手法の一検討
    - ✓ CSEC研究会: 西田他,文字出現頻度をパラメータとした機械学習による悪質な難読化JavaScriptの検出

6. 今後の研究開発計画

- 100人規模のセミクローズドな実証実験を実施する。実証実験により顕在化した課題について、実験の実施体制の改良、フレームワークの改修、チューニングを行い、最終年度の1,000人規模の実証実験に向けた準備を完了する。
- 100人規模の実証実験で得られたデータにもとづき各種解析手法の評価を実施する。評価結果をもとに解析手法を改良する。得られた成果を適宜外部発表等により対外的にアピールする。