平成24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

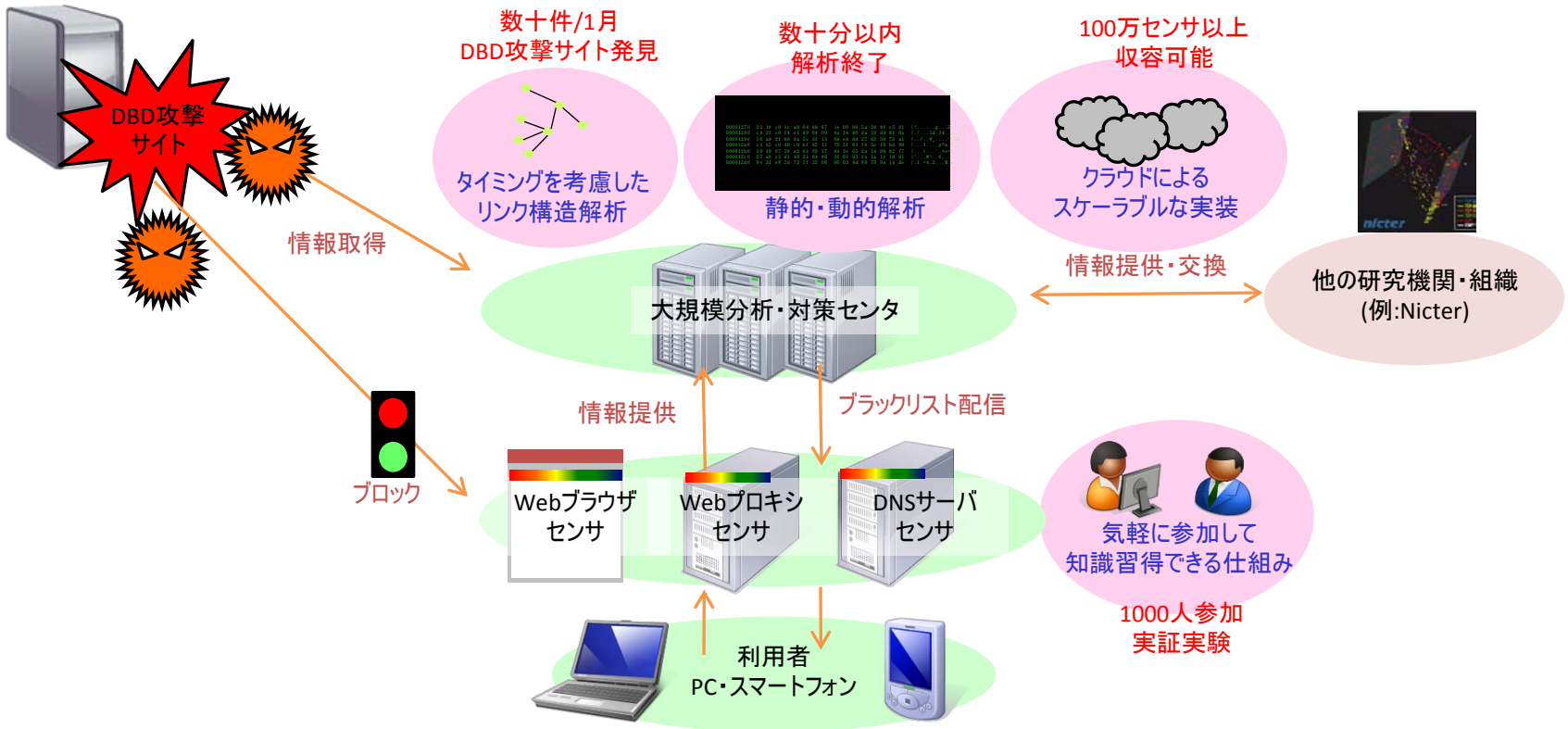
1. 実施機関・研究開発期間・研究開発費

- 実施機関: 株式会社KDDI研究所（幹事者）、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476百万円（平成24年度 130百万円）

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。

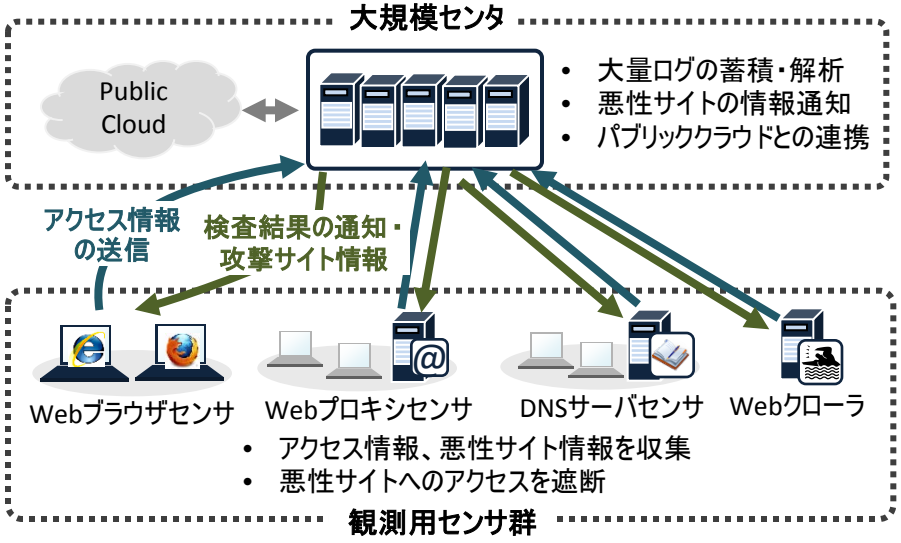
本フレームワークは、利用者ブラウザにおけるセンサ、Webプロキシセンサ、DNSサーバセンサと利用者向けのセンタという構成をとる。利用者はブラウジングしながら情報を提供し、攻撃サイトを発見した際にはそれを通報する。一方、センタは収集したDBD攻撃サイト情報を利用者に配信して被害の拡大を防御する。ここで、利用者は一方的な通報者となるだけでなく、当フレームワークへの参加によってセキュリティの知識を習得するなど何らかの利益が得られる仕組みを提供する。また、センタ側は、収集した攻撃に関する情報をセキュリティ研究者やセキュリティ対策企業との間で交換することによって、セキュリティ対策コミュニティへ還元する。



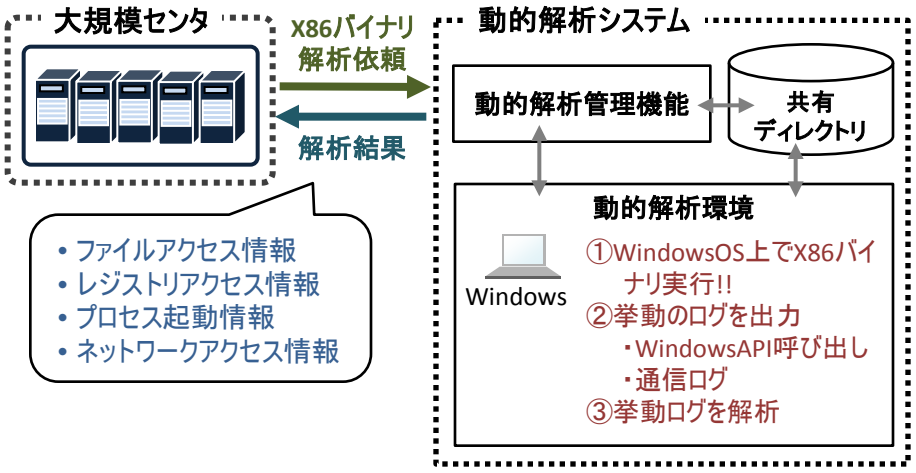
3. 研究開発の成果

①大規模センタ・観測用センサの開発

利用者のアクセス情報を収集しセンタに送信する観測用センサと、センサ側から送信された大量の情報を解析・分析し、攻撃サイトの情報をフィードバックする大規模センタを開発



②DBD攻撃分析・対策技術: x86バイナリ動的解析システムの開発



研究開発成果：大規模センタ・観測用センサの開発

大規模センタ・観測用センサを開発し、DBD攻撃対策フレームワークのプロトタイプを完成させた。

- ブラウザ型センサの開発に関して、Internet Explorer用(Windows版)、Firefox用(Windows版/MacOS版)のプラグインとしてプロトタイプを開発。ユーザがアクセスしたWebサイトの情報、コンテンツを収集してセンタへ送信する機能、判定結果に基づいて悪性サイトへのアクセスを強制的に遮断する機能を実装。
- Webプロキシセンサ、DNSサーバセンサの開発に関して、ネットワーク内の利用者のアクセス情報を収集してセンタへ送信する機能、センタからの攻撃サイト情報をもとに利用者からの当該サイトへのアクセス要求を遮断する機能を実装。センタから悪性が疑われるサイトの情報を取得し、当該サイトのコンテンツを収集してセンタに送信するWebクローラを開発。
- センタの開発に関して、センサから送信される大量の情報を解析する機能、センサがアクセスしたWebサイトの検査結果をセンサに通知する機能、攻撃サイトの情報をセンサに通知する機能、計算処理リソースの確保のためにパブリッククラウドと連携する機能を実装。また、DNSサーバセンサのログ情報を有効活用するために、当該ログ情報からネットワーク内のOSごとの端末数を推定する手法を考案、従来のOS Fingerprintingの推定精度と同程度の精度を実現。当該手法をセンタに実装。

研究開発成果：x86バイナリ動的解析システムの開発

x86バイナリ対応の動的解析システムを開発。疑似ネットワーク環境下でファイルを実行させ、動作ログを収集、解析する機能、大規模センタからコンテンツの解析要求を受け、解析結果を通知する機能を実装。

その他DBD攻撃対策技術の確立に向けて以下の内容を実施。

- 静的解析について、DBD攻撃で利用されるエクスプロイトキットを収集。収集したデータをもとにブラウザやアプリケーションの脆弱性を悪用するJavascriptを解析し、悪性のスクリプトと正規サイトのスクリプトの違いを抽出。
- 悪性コンテンツ配布サイトへのアクセスログを解析し、同サイトのリンク構造を抽出。またWebアクセスログサーバー上に蓄積されているログを解析し、アクセス数上位のドメインサイトとそれ以外のサイトにおけるリンク構造の違いを抽出。

実証実験に向けて以下のとおり検討を実施。

- インターネット利用者のセキュリティに関する意識調査を実施。
- 3年目のセミクローズドな実証実験、4年目の実証実験の基本方針を策定。
- 具体的に参加者の検討や、実装実験の内容、実験時のサポート体制の基本方針を策定。また、ユーザのプライバシに関して、法的に検討を行い、技術的な対応策等の基本方針を確立。

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	1 （1）	0 （0）	1 （1）	2 （2）	0 （0）	0 （0）	0 （0）

5. 研究成果発表会等の開催について

（1）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」との相互連携

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」との連携によるDBD攻撃分析・対策技術の機能向上、相乗効果などについて、委託研究チーム間で議論。

6. 今後の研究開発計画

- 平成24年度で開発した観測用センサと大規模センタを試験環境下で運用し、利用者参加型・互助自警フレームワークの運用方法の検討、実行効率面の改善を行い、実証実験に向けた準備を完了する。
- DBD攻撃分析・対策技術を確立する。動的解析はJavascriptなどスクリプトの解析を可能とする。静的解析は得られた知見をもとに静的解析システムの試作と評価を行う。リンク構造解析にもとづく検知手法については得られた知見をもとに基本機能を確立し、センタに機能を実装する。
- センタの解析結果に加えて、外部機関からの情報、Web上の情報を有効活用して、利用者を攻撃サイトから防御する機能を強化する。
- 利用者の参加を促す仕組み、利用者のリテラシを向上させるために効果的なフィードバック方法について、調査結果にもとづき検討を進め手法を確立、実現する。