平成２４年度研究開発成果概要書
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（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）ＫＤＤＩ研究所＜幹事者＞、（株）セキュアブレイン

（４）研究開発予算（百万円単位切上げ）

平成２４年度	１３０（契約金額）
平成２５年度	１２３（契約金額）
平成２６年度	１１５（契約金額）
平成２７年度	１０８（契約金額）

（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研究開発
- 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	1	1
	外国出願	0	0
外部発表	研究論文	1	1
	その他研究発表	2	2
	プレスリリース	0	0
	展示会	0	0
	標準化提案	0	0

具体的な成果

(1)　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。実証実験の開始に向けて引き続き動作検証、品質向上に努める。

・(ブラウザ型センサ)Internet Explorer 用(Windows 版)、Firefox 用(Windows 版/MacOS 版)のプラグインとしてブラウザセンサのプロトタイプを開発し、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および、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した。ブラウザ型センサで収集した情報の真正性を確認するための仕組みを検討し、本年度はセンサの認証機能を実装した。

・ DNS センサから収集されたトラヒックログからネットワーク内に存在する端末 OS とその数を推定する手法を考案し、大規模センタに実装した。従来の OS Fingerprinting の推定精度と同程度の精度を実現した。

(2) DBD 攻撃分析・対策技術について以下の内容を実施した。

・ (動的解析)x86 バイナリの動的解析システムのプロトタイプを開発した。大規模センサからの解析要求・解析結果通知要求に応答するインタフェースやデータベースについても実装した。

・ (静的解析)DBD 攻撃を行う攻撃者が利用するエクスプロイトキットを収集し、ブラウザやアプリケーションの脆弱性を悪用する Javascript を解析した。また攻撃サイトと正規サイトの Javascript の違いを抽出した。さらに本知見に基づく攻撃サイト検出手法を検討した。

・ 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した。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した。上記の知見にもとづく攻撃サイトの検出手法の考案は来年度に予定している。

(3) 利用者の参加を促す仕組みの検討に先駆け、インターネット利用者のセキュリティ、インターネットサービスに関する意識調査を実施した。具体的な仕組みの検討、実装は来年度に予定している。

・ 実利用者参加による実証実験に向けて、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した。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した。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立てた。

（7）研究開発イメージ図

（別紙参照）