5-2　DBD 攻撃対策フレームワーク

笠間貴弘　松中隆志　山田　明　窪田　歩　藤原信代　川守田和男　岡田晃市郎

Web ブラウザやプラグインの脆弱性を悪用することで、Web サイトにアクセスしたユーザに気づかれないうちにマルウェアに感染させる Drive-by-Download 攻撃（以下、DBD 攻撃）の被害が多発している。本稿では、この DBD 攻撃対策を目的として研究開発を進めている DBD 攻撃対策フレームにワークについて概説し、1,600 名以上の一般ユーザの協力の下で行った実証実験の結果について示す。

1　はじめに

2009 年に発生した Gumblar 攻撃では、攻撃者が正規の Web サイトを改ざんし、当該 Web サイトにアクセスしたユーザを DBD 攻撃によってマルウェアに感染させた。さらに、感染させたマルウェアは当該マシンが管理している別の Web サーバの FTP アカウント情報を攻撃者に漏えいさせ、攻撃者は取得した FTP アカウント情報を利用して改ざんを行うことで次々に日本の大手企業等の Web サイトを改ざんし、多数のユーザに被害が発生した。

Gumblar 攻撃以降も DBD 攻撃の被害は多数発生しており、近年のマルウェア感染の主要な原因の一つとなっている。DBD 攻撃の特徴として、ユーザから悪性 Web サイトへのアクセスを攻撃の起点とする、受動的な攻撃手法であることが挙げられる。そのため、ダークネット観測のような待ち受け型の観測手法では DBD 攻撃を観測が難しく、脅威把握のためには異なる観測手法が必要である。DBD 攻撃を観測する主要な方法の一つであるクライアントハニーポットを用いた手法では、脆弱なユーザマシンを模擬した環境でインターネット上の Web サイトに対して能動的にアクセスすることで DBD 攻撃を観測する。しかし、インターネット上に存在する Web サイトは膨大な数にのぼり、その全てを検査することは困難である。そのため、悪性 Web サイトを効率的に見つけるためには、不審な URL を適切に選択して検査を行う必要がある。

また昨今、エクスプロイトキットと呼ばれるツールの登場によって、攻撃者は容易に悪性 Web サイトを構築できるようなっている。その結果として、検知を困難にする目的で悪性 Web サイトを数日から数週間程度の短期間で使い捨てる場合が多く、いかに迅速に発見できるかが重要となっている。

そこで我々は、一般ユーザ 1,600 名以上の協力の下、各ユーザ環境に Web アクセス観測用のセンサを大規模展開することで Web 空間上の巨視的な挙動を観測するシステムを構築、センサから集約された Web アクセス情報を分析し、悪性 Web サイトの出現や正規サイトの改ざんなどを検知するための DBD 攻撃対策フレームワークの研究開発を進めている。本稿では、我々の開発した DBD 攻撃対策フレームワークの概要について述べ、1,600 名以上の一般ユーザの協力の下で実施したユーザ参加型の実証実験の結果について示す。

2　DBD 攻撃の概要

図 1 に DBD 攻撃の典型的な流れを示す。あらかじめ攻撃者は正規の Web サイトを改ざんし、攻撃用に準備したサイト群（攻撃サイト）に誘導するためのスクリプトを挿入する。改ざんされた Web サイトへアクセスしたユーザは、まず、入口サイトへ転送される。入口サイトでは、ユーザの環境（OS、ブラウザの種類・バージョン、プラグインの種類・バージョン、IP アドレス、リファラ情報など）を調査し、条件を満たす場合のみ攻撃サイトへユーザを転送させる。また、入

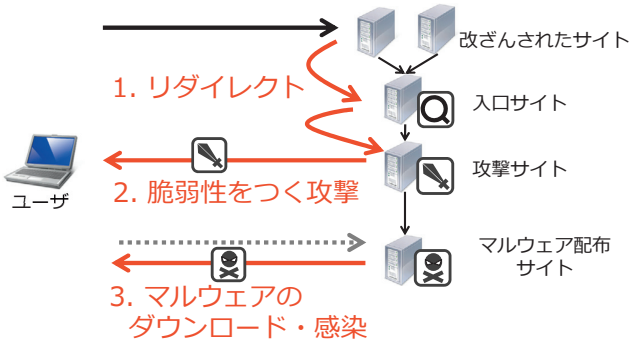

図 1　DBD 攻撃の典型的な流れ

口サイトではIPアドレスやリファラ情報などを基にクライアントハニーポットによるアクセスを判断し、正規のWebサイトに転送することで検知を回避する仕組み（クローキング）が備わっていることも多い。入口サイトから攻撃サイトへの誘導では複数の中継サイトを経由する場合があるが、最終的に攻撃サイトに誘導されたユーザは、ユーザ環境に合わせた脆弱性を攻撃するコンテンツをダウンロードし、攻撃が成功するとマルウェア配布サイトからマルウェアを強制的にダウンロードされて感染する。

さらに、近年ではBlackhole Exploit KitやAnglerといったエクスプロイトキットと呼ばれるツールが開発され、DBD攻撃に利用されていることが報告されている。エクスプロイトキットには複数の脆弱性を突く攻撃コードが用意されているほか、攻撃コードの難読化処理やクローキング機能、管理用のWebインターフェースなど、DBD攻撃を行うための各種機能やツールが備わっている。攻撃者は、これらを利用することで攻撃のための仕組みを自前で準備しなくても比較的簡単にDBD攻撃を行うことができるようになった。このことがDBD攻撃の被害拡大にも大きく影響している。

3　DBD攻撃対策フレームワーク

前述したように、我々は、DBD攻撃において攻撃の実態把握が困難であるという課題に対して、実際の一般ユーザの協力に基づいてWeb空間におけるユーザの巨視的な挙動を観測し、集まった大量のWebアクセス情報を統合的に分析することでDBD攻撃の発生を早期に検知するためのDBD攻撃対策フレームワークの研究開発を進めている[1]–[3]。当該フレームワークの全体像を図2に示す。

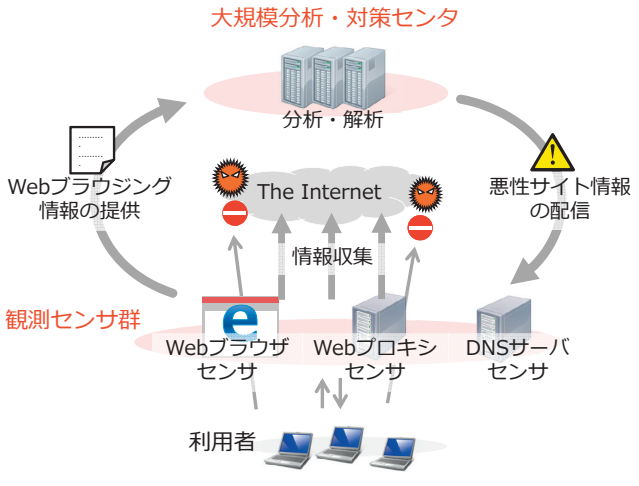

図2　DBD攻撃対策フレームワークの概要図

まずユーザのWebアクセス情報を収集するセンサとして、我々は3種類のセンサを用意した。主なセンサとしてはWebブラウザのプラグイン形式として実装されたWebブラウザセンサを用いるが、プラグインの導入ができない状況も想定してWebプロキシとして動作するセンサやDNSサーバセンサも開発している。しかし、これらのセンサで収集できる情報はユーザ端末上で動作するWebブラウザセンサよりも少なくなるため、以降では基本的なセンサであるWebブラウザセンサの動作のみを説明する。

3.1　フレームワークにおける処理の流れ

Webブラウザセンサ（以下、センサ）は各ユーザ端末上で動作するWebブラウザのプラグインソフトウェアとして実装されており、現状では、Internet ExploreとFirefoxのWebブラウザに対応している。表1にセンサが収集するセンサ環境情報やWebブラウジング情報の主な内容を示す。センサはWebブラウザが起動されると同時に起動し、自身のIDをランダム生成した上で当該IDとブラウザの種類・バージョン、Webブラウザにインストール済みの他のプラグインソフトウェアの種類・バージョンといった自身のセンサ環境情報を大規模分析・対策センタ（以下、分析センタ）に送信する。またWebブラウザから各Webサイトへのアクセスごとにセンサは Webブラウジング情報を生成し、分析センタに送信する。

図3にDBD攻撃対策フレームワークにおける大まかな処理フローを示す。センサによってWebブラウジング情報が分析センタに送信された際、分析センタ

表1　センサによる主な収集情報

センサ環境情報
センサID（起動毎にランダム生成）
Webブラウザの種類
Webブラウザのバージョン
プラグインの種類・バージョン
Webブラウジング情報
センサID（起動毎にランダム生成）
タブID（タブ毎にランダム生成）
アクセス先URL
アクセス先IPアドレス
HTTP Rewuest/Responseヘッダ
コンテンツのハッシュ値
リダイレクトの有無
マウスイベントの有無

側ではまず既知の悪性サイトや悪性コンテンツに一致するか否かを判定するためにブラックリスト判定を行う。このブラックリストは外部公開されている情報を用いるほか、後述する各種分析エンジンの分析によって悪性判定されたサイトの URL やコンテンツのハッシュ値も含む。また、ブラックリスト判定に加えて、ページ遷移の振る舞いやリダイレクト段数など、いくつかの特徴を基に悪性判定を行うヒューリスティックエンジン [4][5] による判定も行われる。アクセス先の Web サイトが悪性判定された場合は、その判定結果がセンサに渡され、センサはユーザにダイアログ等で警告を表示、ユーザの判断を仰いだ上でアクセスを遮断することで攻撃の被害を防止する。また、悪性判定された際には必要に応じて、分析センタからセンサに対してブロックされた当該 Web コンテンツのアップロード要求が送信され、ユーザが許可した場合には当該 Web コンテンツが分析センタ側に送信され各種解析エンジン [6][7] による詳細な解析が実施される。Web アクセスごとのリアルタイムな悪性判定に加えて、多数のユーザから収集した Web ブラウジング情報を集約・分析し Web サイト間のリンク構造等から悪性 Web サイトを検知するエンジン [8][9] も定期的に動作している。

3.2　ユーザプライバシに関する配慮

Web サイトのアクセス情報にはユーザの趣味嗜好や行動パターンが反映されるため、フレームワークに参加したユーザのプライバシへの配慮が重要となる。そこで本フレームワークにおいては、いくつか技術面での対応を実施している。まず、収集した Web アクセス情報から参加者個人の Web アクセス履歴が過度に追跡されないように、ブラウザセンサにおいては Web ブラウザが起動されるごとにセンサ ID をランダムに生成するようにした。これにより、ブラウザや OS の再起動時には同一ユーザであっても毎回異なるセンサ ID が生成されるため、センサ ID のみでは長期間にわたって同一ユーザの Web ブラウジング情報を追跡できない。その他にも、デフォルトでは HTTP ヘッダ情報のみを収集し、コンテンツを収集する際にはダイアログによってユーザの承認を得る、HTTPS での通信や Cookie、認証情報などは収集しない、収集対象の情報は各項目別にユーザ側で許可する／しないを設定できる、といった各種プライバシ対策を実現した。また後述するユーザ参加型実証実験においては、ユーザへ収集する Web ブラウジング情報を説明する各種文書や約款等を整備し、それらの文書内容を含めた実証実験全体について問題が無いことを有識者による第三者委員会によって確認している。

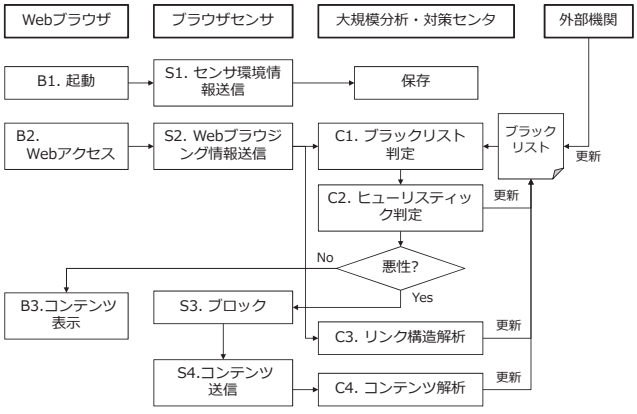

図 3　DBD 攻撃対策フレームワークの処理フロー

4　ユーザ参加型実証実験

本フレームワークの有効性を検証するために、2015 年 7 月 1 日～ 11 月 30 日の期間において、1,000 名規模のユーザ参加型の実証実験を実施した。期間中は順次参加ユーザを募集し、2015 年 10 月 21 日には参加ユーザ数は 1,676 名に達し、以降はそのユーザ数で実験を継続した。表 2 に実証実験で収集されたデータの統計を示す。

実験期間中にセンサによって観測されたユニーク URL 数は計 217 万 URL であり、これらの観測された URL を Alexa の日本でのドメイン別アクセスランキングと比較したところ、Alexa の上位 100 ドメインのうち全てのドメインに対してアクセスが観測されていた。この結果から、1,600 名規模でも主要な Web サイトへのアクセスは漏れなく観測されており、仮にこれらの主要な Web サイトが改ざん等の被害を受け、DBD 攻撃に悪用された場合には、攻撃活動を観測できる可能性が十分にあることがわかる。

DBD 攻撃対策フレームワークでは、多数のユーザによる Web アクセスを観測・分析することで悪性 Web サイトを検知することを想定しているため、1 度しかアクセスされない Web ページに対してはその効果は限定的なものになる。そこで表 3 に実証実験において複数回アクセスが観測された Web ページ数とア

表 2　実証実験における統計情報

ユーザ数	1,676
全センサID数	49,146
全Webアクセス情報数	4,425,689
ユニークアクセスURL数	2,178,381
ユニークアクセスFQDN数	34,195

表３　２回以上アクセスが観測された Web ページ数とアクセス数の統計

ユニークWebページ数	2,178,381
2回以上アクセスされたWebページ数	212,804 (9.8%)
Alexa日本上位100ドメイン上のWebページ数	56,692 (2.6%)
Alexa日本上位100ドメイン以外のWebページ数	156,112 (7.2%)
総アクセス数	4,425,689
2回以上アクセスされたWebページへのアクセス数	2,460,112 (55.6%)
Alexa日本上位100ドメイン上のWebページへのアクセス数	668,537 (15.1%)
Alexa日本上位100ドメイン以外のWebページへのアクセス数	1,791,575 (40.5%)

クセス数の統計を示す。表３を見ると、２回以上アクセスが観測された Web ページ数は約 21 万 URL であったが、この中の約 15 万 URL については Alexa の上位 100 ドメインに含まれない Web ページであった。これらの Web サイトについては、少なくとも Alexa 上位ドメイン上のサイトをクローリングしているだけでは観測できないため、一般ユーザの Web アクセスを観測する我々のフレームワークでは、アクセスの多い Web サイトに限らず幅広く Web 空間上を観測することができていることがわかる。

悪性判定エンジンの結果に関して、文献 [3] で提案した、ダウンロード遷移を明示的に把握できない実行ファイルへのアクセスを検知する手法については、実験期間中に悪性判定されたアクセスは存在しなかった。また、リダイレクト段数による多段リダイレクト検知については、11 件のアクセスが悪性判定された。これらの悪性判定されたアクセスについて詳細解析を行った結果、特に悪性なコンテンツのダウンロードでは無いと判断されたため、この 11 件については誤検知であると判断した。一方、Google が提供する Safe Browsing API を用いて観測した URL を検査したところ 23 件が悪性判定されたが、同じく当該アクセスを調査した結果、実際にマルウェアのダウンロードまでは発生しておらず、誤検知の可能性が高いと判断した。結果として、今回の実証実験においては見逃しの可能性は残るものの、実際の DBD 攻撃の観測はできていない可能性が高いと判断した。そのため、更なる検知エンジンの研究開発に加えて、より多くのユーザ規模での実証実験を行うことで実際の DBD 攻撃の観測と検知エンジンの評価を行う必要があると考えている。

5　まとめ

本稿では、DBD 攻撃対策フレームワークの概要と一般ユーザの協力の下に実施した実証実験の結果について報告した。結果として、1,600 名規模であっても著名な Web サイトへのアクセスを含む多数の Web サイトへのアクセスが観測されており、正規サイトに関するアクセスについては網羅的な観測ができていることが明らかになった。しかし一方で、悪性サイトの検知に関しては、誤検知が何件か発生したのみで実際の DBD 攻撃については観測されていない。このため、各種検知エンジンの高度化に加えて、参加ユーザ数を増加させた再実験を行うことで、実際の攻撃活動の観測と更なる評価を進める必要がある。

【参考文献】

1　笠間 貴弘，井上 大介，衛藤 将史，中里 純二，中尾 康二，" ドライブ・バイ・ダウンロード攻撃対策フレームワークの提案，" 情報処理学会コンピュータセキュリティシンポジウム 2011（CSS2011），2011 年 10 月．

2　T. Matsunaka, J. Urakawa, and A. Kubota, “Detecting and Preventing Drive-by Download Attack via Participative Monitoring of the Web,” In Proceedings of the 8th Asia Joint Conference on Information Security (AsiaJCIS 2013), July 2013.

3　T. Matsunaka, J. Urakawa, A. Nakarai, A. Kubota, K. Kawamorita, Y. Hoshizawa, T. Kasama, M. Eto, D. Inoue, and K. Nakao, "FCDBD: Framework for Countering Drive-by Download," The 9th International Workshop on Security (IWSEC2014), poster session, Aug. 2014.

4　笠間 貴弘，神薗 雅紀，井上 大介，"Exploit Kit の特徴を用いた悪性 Web サイト検知手法の提案，" 情報処理学会 マルウェア対策研究人材育成ワークショップ 2013（MWS2013），2013 年 10 月．

5　T. Matsunaka, A. Kubota, and T. Kasama, "An Approach to Detect Drive-by Download by Observing the Web Page Transition Behaviors," In Proceedings of the 9th Asia Joint Conference on Information Security (AsiaJCIS 2014), Sept. 2014.

6　西田 雅太，星澤 裕二，笠間 貴弘，衛藤 将史，井上 大介，中尾 康二，" 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，" 情報処理学会 第 158 回 DPS・第 64 回 CSEC 合同研究発表会，2014 年 3 月．

7　神薗 雅紀 , 岩本 一樹 , 笠間 貴弘 , 衛藤 将史 , 井上 大介 , 中尾 康二 , “解析環境に依存しない文書型マルウェア動的解析システムの開発 ,” 電子情報通信学会 信学技報 , vol.114, no.71, 2014 年 6 月 .
8　松中 隆志 , 半井 明大 , 浦川 順平 , 窪田 歩 , “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竄サイト検出手法の一検討 ,” 電子情報通信学会 2014 年暗号と情報セキュリティシンポジウム (SCIS 2014), 2014 年 1 月 .
9　笠間 貴弘 , 衛藤 将史 , 神薗 雅紀 , 井上 大介 , " クライアント環境に応じたリダイレクト制御に着目した悪性 Web サイト検出手法 ," 電子情報通信学会 電子情報通信学会 信学技報 , vol.114, no.71, 2014 年 6 月 .

笠間貴弘　（かさま　たかひろ）
サイバーセキュリティ研究所
サイバーセキュリティ研究室
研究員
博士 (工学)
サイバーセキュリティ

松中隆志　（まつなか　たかし）
KDDI 株式会社
セキュリティオペレーションセンター
課長補佐
ネットワークセキュリティ

山田　明　（やまだ　あきら）
株式会社 KDDI 総合研究所
ネットワークセキュリティグループ
研究主査
ネットワークセキュリティ

窪田　歩　（くぼた　あゆむ）
株式会社 KDDI 総合研究所
ネットワークセキュリティグループ
グループリーダー
ネットワークセキュリティ

藤原信代　（ふじわら　のぶよ）
株式会社セキュアブレイン
先端技術研究所
シニアプロジェクトマネージャ
プロジェクトマネジメント

川守田和男　（かわもりた　かずお）
株式会社セキュアブレイン
先端技術研究所
ディレクタ
Web サービスセキュリティ、Web クローラ

岡田晃市郎　（おかだ　こういちろう）
株式会社セキュアブレイン
先端技術研究所
所長
Web サービスセキュリティ、マルウェア解析