平成２４年度 委託研究
「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」
研究計画書

独立行政法人
情報通信研究機構

１．研究開発課題

『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』

２．研究開発の目的

近年、攻撃者の改竄によって多くの Web サイトに悪性サイトへのリダイレクト命令を埋め込まれ、それらサイトにアクセスしたユーザが悪性サイトへ誘導されてマルウェアに感染するといった被害が拡大している。これは、ブラウザやプラグインの脆弱性を悪用し、強制的にマルウェアをダウンロード・実行させるドライブ・バイ・ダウンロード攻撃（Drive-by-Download attack：以下 DBD 攻撃）が原因である。

この DBD 攻撃は従来のリモートエクスプロイト攻撃とは異なり、ユーザの Web アクセスを攻撃の起点とするため、ダークネット観測のような従来の受動的な攻撃観測手法ではその脅威を捉えられない。一方、能動的に Web サイトをクローリングし検査を行うクライアントハニーポットのようなシステムを用いて、検知した悪性サイトの URL をブラックリストとして提供することで攻撃を防止する対策手法も存在する。しかし膨大な数の Web サイトが存在し、なおかつ悪性サイトはその URL を短期間で遷移させているという状況において、効果的な対策とするためには、シード（クローリングの起点）をどこに設定するかという問題点と、如何に検査した URL の鮮度を保つか（再検査までの期間を短くするか）という問題点が存在するなど、セキュリティ分野で未だ決定打となる対策が打ち出せていない状況が続いている。

情報通信研究機構（以下、「機構」という。）ではこれまで、インシデント分析センタ nicter を構築し、主にリモートエクスプロイト型マルウェアの活動の迅速な把握と原因分析のための技術確立を行ってきた。さらに委託研究「マルウェア対策ユーザサポートシステムの研究開発」（平成 21～23 年度）にてマルウェアの迅速かつ簡易的な駆除を可能にするユーザサポートシステムの構築を図っている。しかしながら、前述の通り、DBD 攻撃は nicter のダークネット観測網では原理的に観測不能である。そのため、機構の自主研究では新たに、DBD 攻撃に対抗するための観測・分析・対策の基本アーキテクチャを考案し、そのプロトタイプ開発を行ってきている[1]。

本研究開発では、機構が検討してきた基本アーキテクチャ及びプロトタイプを踏まえた上で、DBD 攻撃についてその脅威の解明し、安心・安全なネットワーク社会の実現に向け、DBD 攻撃対策フレームワークの確立に資することを目指す。

３．採択件数、研究開発期間及び予算

採択件数： １件

研究開発期間：契約締結日から平成 27 年度末までの４年間。

予算：平成 24 年度は総額 130 百万円を上限とする。提案の予算額の調整を行った上で採択する場合がある。

なお、平成 25 年度以降は対前年度比で 6%削減した金額を上限として提案を行うこと。

４．研究開発の到達目標

DBD 攻撃対策フレームワークは、下記（１）及び（２）で開発する技術群を核とし、Web クローリングや Web レピュテーション、スパム解析等の技術と連携可能な統合的システムとして構成する。また（３）においてフレームワークの有効性検証を実施する。

（１）DBD 攻撃大規模観測網構築技術

DBD 攻撃の大規模観測網を構築するため、ユーザが Web ブラウジングする際の URL やブラウザの内部挙動等のリアルタイムな収集を可能にする、ユーザ端末インストール型の観測モジュール（以下、「センサ」という。）を開発する。また、多数のユーザからの情報を集約するスケーラブルな中央集中型システム（以下、「センタ」という。）を開発する。

ユーザの Web ブラウザ上の挙動をミリ秒～秒オーダで準リアルタイムに観測可能な大規模観測網構築技術を確立するため、下記の研究開発を実施すること。

（ａ）観測用センサの開発

- センサはブラウザプラグイン型やプロキシ型等で適宜実装すること
- 少なくとも Windows と Mac OS に対応することとし、IE、Firefox、Safari 等の一般的なブラウザに対応すること
- ユーザの Web アクセスやマウスイベント等を収集できること、また不審な Web コンテンツ等を収集できること
- 収集した情報を安全にセンタに送信できること
- ユーザの Web アクセスをブロックする機能及びユーザに警告を表示する機能を有すること
- Web アクセスの履歴等や不正サイト等へのアクセスをブラウザ上で可視化できること
- 収集する情報をユーザが確認及び選択できること

（ｂ）大規模センタの開発

- 観測用センサからの情報を安全に収集・蓄積する機能及び観測用センサと相互認証する機能を有すること
- 不正なセンサからのアクセスをブロックする機能を有すること
- 正当なセンサからの要求により蓄積情報を破棄する機能を有すること
- センサ群のセンタへの接続状況を一元的に確認・管理できること
- 100 万以上のセンサを収容できるスケーラブルな設計となっていること

なお、提案で、観測対象とするユーザの挙動を具体的に挙げるとともに、観測の所要時間、観測可能とするユーザ数の目標値を示すこと。

（2）DBD 攻撃分析・対策技術

DBD 攻撃を検出し適切な対策実行を可能にするため、収集したユーザ群のマクロな挙動分析に基づく Web 空間での異常検知技術を開発する。また、センタ側からユーザ端末に対策（例えば不正サイトへのアクセスのブロック）を自動展開する技術を開発する。

（1）の観測網から得られたユーザ群の巨視的な Web アクセスの挙動等を数秒～数分オーダで自動分析する DBD 攻撃分析・対策技術を確立するため、下記の研究開発を実施すること。

（a）DBD 攻撃分析技術の開発

- ユーザ群の Web アクセス（リダイレクトを含む）を大規模解析できること
- ユーザ群の挙動等から DBD 攻撃の発生や不審サイトを検出できること
- Web クローリングや Web レピュテーション、スパム解析等の技術を用いて（または既存システムと連携し）不審サイトを検査できること
- 分析結果の統計情報を蓄積すること
- 新たに不正と判定されたサイトは Web レピュテーションに反映すること

（b）DBD 攻撃対策技術の開発

- 不正サイトへのアクセスをブロックする指令をセンサに自動展開できること
- センサに各種の警告情報等を送信できること
- 対策結果の統計情報を蓄積すること

なお、提案で、自動分析の所要時間の目標値、検出対象とする事象を具体的に示すとともに、対策の自動展開の手法について記述すること。

（3）DBD 攻撃対策フレームワーク実証実験

DBD 攻撃対策フレームワークの有効性やスケーラビリティ等を検証するために、ユーザ参加型の大規模な実証実験を行い、社会還元に繋げる。

上述した（1）DBD 攻撃大規模観測網構築技術、（2）分析・対策技術の各研究開発項目の機能検証及び、フレームワーク全体の有効性検証を行うため、下記のようなユーザ参加型実証実験及びそれに必要となる検証等を実施すること。

- 研究開発期間 3 年目を目途に 100～1000 センサ（具体的な数値は提案すること）の特定の組織のユーザを対象にしたセミクローズドな実証実験、研

究開発期間 4 年目を目途に 1000 センサ以上の一般ユーザの参加を募った実証実験を実施すること
- 実証実験では、参加ユーザ数の推移や、検出された不正サイト数、適切にブロックされた Web アクセス数等の統計情報を収集し、フレームワークの有効性を示すこと
- 実証実験の準備段階において、ユーザのプライバシに関する技術的及び法的検討を行い、必要であれば上述の技術課題にフィードバックを行うこと
- ユーザに実証実験への参加を促す方策や、ユーザとの間の約款等について検討・具現化を行うこと
- 実証実験で得られた観測データは、nicter システムにリアルタイムに提供すること

なお、実証網の運用・保守、一般ユーザの参加を募った実証実験のユーザ展開方法、ユーザからの問い合わせ対応、トラブル発生時の対応体制について、提案書で説明すること。また、研究開発終了後のシステム運用計画についても提案書で説明すること。研究開発成果については、研究会や論文誌等で積極的に公表すること。

5．研究開発の運営管理及び評価について

研究開発に当たっては、機構の自主研究（ネットワークセキュリティ研究所サイバーセキュリティ研究室）との連携を図ること。本研究開発の過程で得られた情報や成果については、逐次自主研究の nicter システムと統合を図り、他の攻撃との関係の調査や分析等に資すること。

また、平成 25 年度にセンサ及びセンタの開発状況等についての公表を行い、平成 27 年度に連携実証実験及び終了評価を行う。

なお、本研究開発で新たに開発されたソフトウェア等の著作権について、機構がその著作物の利用に必要な範囲において、機構が利用する権利及び機構が第三者に利用を許諾する権利を、許諾するものとする。

6．参考

（1）関連研究

論文[2,3]では、インターネット上の DBD 攻撃サイトの実態に関する大規模調査結果が報告されている。論文[3]の報告では、1 年間で数十億の URL のコンテンツを検査し、その内の約 45 万の URL が DBD 攻撃サイトと判定されている。

DBD 攻撃対策手法としては、まずプロキシベースでの対策手法が存在する。論文[4]ではプロキシ上で Web コンテンツを静的検査し、JavaScript などの実行可能コンテンツが含まれる場合は、プロキシ上の仮想マシン内のブラウザで読み込んだ際の挙動を検査することで、攻撃を検知する手法を提案している。論文[5]では、ホストベースの対策手法として、カーネルレイヤでのイベントフックによってブラウザによるファイルダウンロード時の同意確認ダイアログとそれに対するユーザ入

力を監視し、同意の確認できないファイルの実行を制限することで DBD 攻撃を防止している。またブラウザベースの対策手法としては、論文[6]で JavaScript コードから特徴を抽出し機械学習によって悪性 JavaScript の判定を行う手法が提案されている。また論文[6]では、ブラウザの JavaScript エンジンを拡張する形で提案手法を実装しコンパイル関数をフックすることで、難読化の影響を受けずに判定を可能としている。

Internet Explorer 8 から搭載された SmartScreen フィルタ[7]では、ユーザが Web サイトへアクセスする際に、ローカルマシン上に保存されたホワイトリストに含まれない URL については Microsoft に送信され、ブラックリストとの照合が行われる。ブラックリストと一致した場合は Web サイトへのアクセスがブロックされ、警告ページが表示される。

一方、Firefox、Google Chrome、Safari などのブラウザには、Google セーフブラウジング API[8]を用いた機能が搭載されている。基本的な動作としては、まず初回起動時に Google からブラックリスト（URL のハッシュ値（SHA-256）先頭 32 ビット）を取得する。 その後 Web サイトへのアクセス時にアクセス先の URL のハッシュ値が計算されブラックリストとマッチングが行われる。先頭 32 ビットが一致した場合は、Google に対して本来のハッシュ値（256 ビット）を要求し、256 ビット同士で再度マッチングが行われる。完全一致した場合は Web サイトへのアクセスがブロックされる。Google から取得したブラックリストは定期的に更新される。

（2）機構で検討しているドライブ・バイ・ダウンロード攻撃対策フレームワーク

（a）ドライブ・バイ・ダウンロード攻撃について

図 1 では DBD 攻撃を活用した攻撃手法である Gumblar 攻撃の流れを示している。Gumblar 攻撃では、まず攻撃者が正規サイトを改竄しリダイレクト命令を挿入する。改竄されたサイトへアクセスしたユーザは悪性サイトへと誘導され、ブラウザやプラグインの脆弱性を突く攻撃コードが送り込まれることで自動的にマルウェアがダウンロード・実行される。マルウェアは感染したマシン上からユーザの FTP アカウント情報を収集し、攻撃者に送信する。収集したアカウント情報を用いて攻撃は別の Web サイトへリダイレクト命令を挿入する。この Gumblar 攻撃によって次々と正規サイトが改竄され、多数のユーザがマルウェアに感染した。

DBD 攻撃の特徴としては、ユーザの Web サイトへのアクセスを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、従来のインターネット上における攻撃観測手法としては、未使用の IP アドレス範囲（ダークネット）に届く攻撃通信を観測する手法が効果的であったが、DBD 攻撃においてはその攻撃通信が未使用の IP アドレスに対して届くことはない。そのため、その脅威を把握するためには、ダークネット観測とは異なる観測手法が必要である。

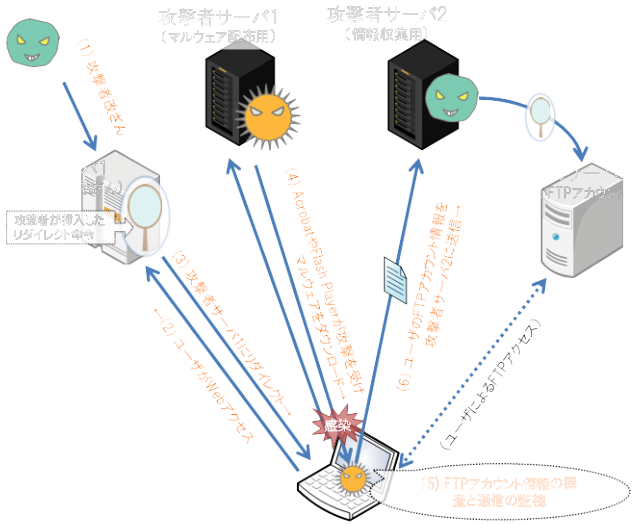

図 1　Gumblar攻撃の流れ

（b）フレームワークの方針

本フレームワークにおける DBD 攻撃対策の基本的な方針は（1）で述べた、Google セーフブラウジングや Smart Screen フィルタと同じ、URL ブラックリストを用いたアクセスブロックによる DBD 攻撃の阻止である。しかし、これらの URL ブラックリストを用いた攻撃検知手法には以下のような問題点がある。

- ブラックリスト作成時のクローリングのシード（クローリングの起点）設定の問題
- URL の鮮度（再検査までの期間）の問題

まず、膨大な数の Web サイトが存在し、なおかつ悪性サイトはその URL を短期間で遷移させている[6]という状況において、悪性サイトを効果的に検知するためには、どのような情報を基にどこにクローリングのシードを設定するかが非常に重要な点になる。加えて、一度検査をした URL についても、検査後に Web サイトが攻撃者によって改竄されたり、またサイト管理者によって改竄から復旧したりすることが当然考えられ、ブラックリストが更新されない場合見逃しや誤検知が発生する。そのため一度検査した URL の鮮度を保つ、つまり再検査までの期間を短くする必要があるが、全ての URL を頻繁に再検査するのは現実的ではない。そのため如何に正規サイトの改竄や改竄からの復旧などを推測し、効果的に再検査できるかが重要な点となる。

これらの問題点を解決するために、本フレームワークでは、以下の方針によって情報収集と悪性サイトの検査を行う。

- ユーザ環境で動作するセンサによって Web ブラウジング時の情報を収集する。
- 収集した情報を自動分析し、分析結果から悪性サイトの出現や正規サイトの改竄、改竄からの復旧などを推測し検査を行う。

センサを大規模展開することで Web 空間上におけるユーザ群の巨視的な挙動

を観測し、従来の観測手法では捉えられなかった DBD 攻撃の脅威把握を可能とする。加えて、収集した情報を分析した結果をクローリングのシードとして活用することで、効果的な検査を可能とする。

（ｃ）機構の提案しているフレームワーク

図２に DBD 攻撃対策フレームワークの全体図を示す。本フレームワークはセンサ、情報収集システム、情報分析システムからなる。

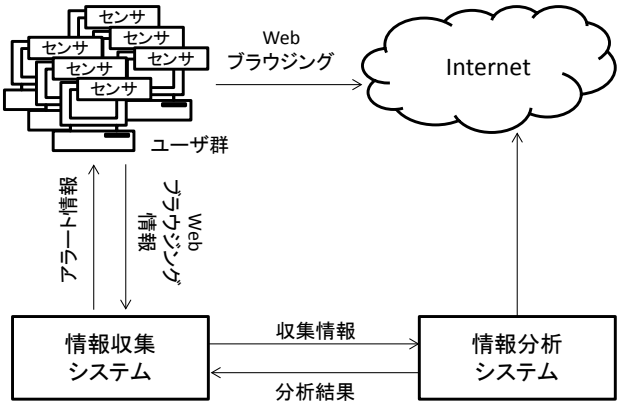

図２　フレームワークの全体像

① ブラウザ組込型センサ

センサの実装形態についてはブラウザのプラグイン形式での実装を採用した。プラグインで実装することによってユーザはセンサ導入時に煩雑な処理を必要とせずセンサをインストールすることが可能になる。また、既存のアンチウイルスソフトとの併用も容易になる。

リダイレクト判別機能：　プラグイン実装のもう一つの利点として、ユーザの Web ブラウザ上でのマウスクリック等の挙動をセンサで把握できるため、ユーザのリンククリック等による通信とリダイレクト等のブラウザによる自動的な通信を区別する。

Web ブラウジング情報の収集・送信機能：　導入されたセンサは、ユーザが Web アクセスを行う際に、情報収集システムに対してアクセス URL、アクセス日時、センサの IP アドレス、センサ ID、リダイレクトの有無、マウスイベントの有無、リダイレクト元 URL、HTTP リクエストなどの情報を収集しリアルタイムに送信する。

アクセスブロック機能：　センサにはアクセスブロック機能が搭載されており、情報送信時に情報収集システムからアラート情報が送られてきた場合は、ユーザの Web アクセスを強制ブロックし警告画面を表示することで攻撃を回避する。

② 情報収集システム

情報収集システムは、各センサからの情報を収集し、情報分析システムに渡す。

情報分析システムによって悪性サイトと判定された場合は、センサに対してアラート情報を展開し、攻撃を阻止する。

③ 情報分析システム

情報分析システムは、情報収集システムから受け取った情報を基に、ユーザ群の巨視的な挙動を分析する。大規模なユーザ群の挙動を収集・分析し異常検知を行うことで、膨大な Web サイトの中から不審な Web サイトを検出し、改竄されたサイトや悪性サイトの効果的な検知を可能とする。また、情報分析システムには複数の分析エンジンが存在し、新たな分析エンジンを追加することで分析機能の拡張が容易になっている。

悪性サイト検査エンジン： 悪性サイト検査エンジンは、クライアントハニーポットを用いて検査対象 Web サイトへクローリングを行い、悪性サイトか否かの判定を行う。クライアントハニーポットとしては、実際の Web ブラウザを用いた高対話型と、Web ブラウザを模擬したエミュレータなどを用いた低対話型の 2 種類に分けられるが、本フレームワークでは未知の攻撃にも対応可能な高対話型のクライアントハニーポットを用いて検査を行う。センサからの収集情報を活用することで、悪性サイトが攻撃対象とするブラウザやプラグインの種類やバージョンを適切に設定することが可能になる。また、悪性サイトの中には Referer ヘッダなどによって特定のサイト経由からのアクセスに対してのみ攻撃を行うものが存在するが、そのようなタイプの悪性サイトにも収集した情報を基に対応が可能である。

既知悪性サイト判定エンジン： 既知悪性サイト判定エンジンは、過去に悪性サイト検査エンジン等によって悪性サイトと判定された Web サイトの URL ブラックリストと、センサで収集した URL とのマッチングを行う。

リンク構造解析エンジン： リンク構造解析エンジンは、センサから収集した情報から Web サイト間のリンク構造に着目し、改竄されたサイトや悪性サイトの疑いのある Web サイトを検出する。検出された Web サイトは悪性サイト検査エンジンで疑いの真偽を確認することができる。 センサで収集した情報から不審な Web サイトを検出する詳細な手法については、今後の検討課題であるが、例えば一例として以下のような基準に基づいた検出手法が考えられる

（ｉ）未知 Web サイトへの強制リダイレクト

例えばある正規 Web サイトにアクセスしているユーザ群が、ある時点を境に未知の Web サイトに強制的に（マウスクリック等のユーザイベントなしに）リダイレクトされ始めた場合、その正規サイトが攻撃者に改竄され悪性サイトへのリダイレクト命令が仕掛けられた可能性がある。このような未知の Web サイトへの強制リダイレクトを検出し、検査を行う手法が考えられる。

（ⅱ）外部サイトからのリダイレクトリンク数

DBD 攻撃においてはリダイレクトによる遷移が多用されるが、それら Web サイト間のリンク構造に着目すると、実際に攻撃コードを送信するサイトには、

改竄された正規サイトやその他の多数の誘導サイトからリダイレクトリンクが張られているという特徴がある[9]。そこで、センサで収集した情報を基に多くのサイトからリダイレクトリンクを張られているサイトを検出し、検査を行う手法が考えられる。

（ⅲ）多段のリダイレクトによる遷移

DBD 攻撃では、解析や検知を難しくするために、多段のリダイレクトによって複数の踏み台サイトを経由したのちに実際の攻撃サイトなどに到達させるという特徴がある。そこで、センサの情報を基に、個々の Web サイトにアクセスするまでのリダイレクトの回数を調べ、それがある一定数を超えるものを検出し、検査を行う手法が考えられる。

④ 他システムとの連携

情報分析システムでは他のシステムとの連携による分析も積極的に行う。以下はその一例である。

- nicter との連携

機構の自主研究は広域のネットワークモニタリングとマルウェア解析技術を融合させた nicter[10]の研究開発を進めている。この nicter との連携として、悪性サイト検査エンジンによるクローリングによって取得されたファイルを、nicter のマルウェア動的解析システム[11]に投入し解析を行い、解析結果を分析に用いる。また、過去の動的解析システムによる解析結果（マルウェアがアクセスする URL 情報）なども分析に用いることができる。

- Web レピュテーションシステムとの連携

Web レピュテーションとは、個々の Web サイトに対してある評価基準を基に危険度を評価し、その値を基にアクセス制御を行う技術である。評価基準としては、ドメイン名の特徴や Web サイトの登録日、リンク情報など複数の情報が用いられている。このような Web レピュテーションシステムとの連携も行い、危険度のスコアに応じてアラートを送信することも検討する。また、危険度の高いサイトに対しては悪性サイト検査エンジンによる検査を行ったり、センサからの情報を基にユーザのアクセス頻度の高いサイトについては頻繁にレピュテーションのスコアの再計算を行うなどの相互の連携が考えられる。

- スパム分析システムとの連携

機構の自主研究は既にスパムメールの分析システムを構築しており、この分析結果も活用することができる。例えば、センサから送られてきた URL が収集したスパムメールに含まれていた URL リストに含まれる場合にアラートを送信したり、それらのスパムに含まれる URL に対して悪性サイト検査エンジンによる検査を行ったりするなどの連携が考えられる。また、スパムメールの分析だけではなく、最近増加している SNS 経由でのスパムメッセージの収集も行い、それらに含まれる URL 情報も活用することを検討する。

（d）まとめ

機構で検討しているドライブ・バイ・ダウンロード攻撃対策フレームワークでは、ユーザ環境で動作するセンサを大規模展開することで Web 空間上のユーザ群の巨視的な挙動を観測する。また、センサからの収集情報を自動分析し、その結果をクローリング検査に活用することで、従来のクローリング検査の問題点であったクローリングのシード設定の問題や、ブラックリストなどの URL の鮮度の問題を解消することを目指す。今後の検討課題としては以下の点が挙げられる。

① 悪性サイト検知時の対策

本フレームワークでは、未知の悪性サイトを検知した場合、今後のユーザのアクセスを遮断する他に、センサで収集した情報を基に、過去にその悪性サイトにアクセスしておりマルウェアに感染した可能性の高いユーザが判別できる。そこで当該ユーザに対してアラート情報を送信することに加えて、動的解析システムによるマルウェアの解析結果を基に駆除ツールを生成し、ユーザに提供するような仕組みも検討する。

② サイト検知時の対策

本フレームワークでは、ユーザ側のパフォーマンス低下を回避するために、分析作業は情報分析システム側で行う仕組みになっている。しかし、まったく未知の悪性サイトによる感染も防止するためには、ユーザマシン上でその場で攻撃を検知し遮断する機能が重要になってくる。そこで、センサの拡張として展開可能な、軽量な攻撃検知手法についても検討を進める。

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,” コンピュータセキュリティシンポジウム 2011, 3B4-1, 2011.
[2]N. Provos, P. Mavrommatis, M. A. Rajab, and F. Monrose, “All your iframes point to us,” In Proceedings of 17th USENIX Security Symposium, 2008.
[3]N. Provos, D. McNamee, P. Mavrommatis, K. Wang, and N. Modadugu, “The ghost in the browser analysis of web-based malware,” In 1st Workshop on Hot Topics in Understanding Botnets, 2007.
[4]A. Moshchuk, T. Bragin, D. Deville, S. D. Gribble, and H. M. Levy, “SpyProxy: Execution-based detection of malicious web content,” In Proceedings of 16th USENIX Security Symposium, 2007.
[5]L. Lu, V. Yegneswaran, P.A. Porras, and W. Lee, “BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections,” in Proceedings of 17th ACM Conference on Computer and Communications Security, 2010.
[6]C. Curtsinger, B. Livshits, B. Livshits, C. Seifert, “ZOZZLE: Fast and Precise In-Browser JavaScript Malware Detection,” In Proceedings of 20th USENIX Security Symposium, 2011.
[7]Windows Internet Explorer 8 Privacy Statement,
http://windows.microsoft.com/en-US/internet-explorer/products/ie-8/privacy-

statement#services
[8]Developer’s Guide (v1) – Google Safe Browsing API - Google Code, http://code.google.com/intl/ja/apis/safebrowsing/developers_guide.html
[9]M. Akiyama, M. Iwamura, Y. Kawakoya, K. Aoki, and M. Itoh, ″Design and Implementation of High Interaction Client Honeypot for Drive-by-Download Attacks,” In Proceedings of IEICE Transactions, Vol. 93, No 4, pp.1131-1139, 2010.
[10] K. Nakao, K. Yoshioka, D. Inoue, M. Eto, “A Novel Concept of Network Incident Analysis based on Multi-layer Observations of Malware Activities,” Proc. of the 2nd Joint Workshop on Information Security (JWIS2007), 2007.
[11] D. Inoue, K. Yoshioka, M. Eto, Y. Hoshizawa, K. Nakao, “Malware Behavior Analysis in Isolated Miniature Network for Revealing Malware’s Network Activity,” IEEE International Conference on Communications (ICC 2008), pp.1715-1721, 2008.