Exploit Kit の変化への適応を目的とした サイバー攻撃検知システムの改良

益子 博貴† 重田 真義† 大谷 尚通†

†株式会社 NTT データ
135-8671 東京都江東区豊洲 3 丁目 3-9 豊洲センタービル
{mashikoh,ootanihs,shigetam}@nttdata.co.jp

あらまし 我々は，ネットワーク機器のログを監視してサイバー攻撃を検知するシステムを開発し，運用している．本システムは，Exploit Kitの挙動の特徴を用いたDrive-by Download攻撃検知を得意とするが，利用している特徴が変化すると，新たな特徴を用いたシステムの改良が必要になる．そこで，Exploit Kitの挙動の変化に追従してシステムを改良するとともに，Exploit Kit以外の特徴にも着目し，その特徴を用いた検知方式を実装した．本発表では，MWS2015データセットにおける検知率評価，および独自データセットを用いた検知数評価の結果をもとに，改良したシステムの有効性を評価する．

Improving Cyber Attack Detection System To Adopt The Changing Of Exploit Kit

Hiroki Mashiko† Hisamichi Ohtani† Masayoshi Shigeta†

†NTT DATA Corporation.
Toyosu 3-3-9, Koto-ku, Tokyo 135-8671, JAPAN
{mashikoh,ootanihs,shigetam}@nttdata.co.jp

Abstract We have developed the cyber attack detection system, which is monitoring logs of network appliances. The system captures characteristics of Exploit Kits, and has advantages in detection of Drive-by Download Attack. Therefore, if the characteristics of Exploit Kits are changing, the system needs updating. So, not only we have improved the system to catch up the changing of Exploit Kits, but also we implemented a new method which capture another characteristics of Drive-by Download Attack. In this paper, we describe the detection rate of this system by using MWS2015 Datasets, and discuss about the advantages of a new method which we implemented to improve the system.

1 はじめに

我々はネットワーク機器のログを監視してサイバー攻撃を検知するシステムを開発し，運用している．本システムは Exploit Kit の定性的特徴を利用した Drive-by Download 攻撃（以下，「DbD 攻撃」）の検知を得意とする．しかし 2014 年以降，Exploit Kit に大

きな変化が生じており，本システムの改良が必要となっている．本研究では，本システムを Exploit Kit の変化に追従させるとともに，システムの Exploit Kit の変化に対する耐性の向上を目指し，改良を行う．

2 現状と問題

2.1 本システムの検知方式

北野ら[1]は，感染端末の振る舞いに着目して複数の感染事例を分析し，Exploit Kit による DbD 攻撃は，図 1 に示す 5 つのステップを踏んで進行すると定義した．

【図 1 Exploit Kit による DbD 攻撃ステップ】

① Redirect ステップ
攻撃者は正規サイトを改ざんし，アクセスしたユーザを，一旦別のサーバを経由してから，pre-Exploit を実行するサーバへリダイレクトさせる．

② pre-Exploit ステップ
攻撃者は，ユーザの端末にインストールされているブラウザやプラグインのバージョンなどを調査し，悪用できる脆弱性を判断する．

③ Exploit ステップ
攻撃者は，pre-Exploit ステップの調査結果をもとに，脆弱性を悪用する Exploit コードを配信する．Exploit ステップが成功すると，攻撃者はユーザ端末の権限を奪うことができる．

④ pre-DL ステップ
ユーザ端末の権限を奪った攻撃者は，Downloader と呼ばれる，マルウェアをダウンロードするためのコードを送り込み，ユーザ端末上で実行する．

⑤ malware-DL ステップ
ユーザ端末で実行された Downloader は，インターネット上からマルウェア本体をダウンロードし，実行する．なお，pre-DL ステップは Exploit ステップと同一のサーバから実行コードを配信するが，malware-DL ステップでは Expolit ステップとは異なるサーバからマルウェアをダウンロードする特徴がある．最近は pre-DL ステップでマルウェア本体を配信することもあり，この場合は malware-DL ステップは実行されない．

ここで，各ステップの働きを説明するため，Nuclear Exploit Kit を用いて DbD 攻撃が実行された際の通信ログを表 1 に示す．

【表 1 DbD 攻撃の例】

line	url	user_agent
(1)	http://h**e.com/	Mozilla/5.0 ... MSIE 10.0;...
(2)	http://www.c**r.cl/clik.php?id=6985669	Mozilla/5.0 ... MSIE 10.0;...
(3)	http://h**j.c**r.pw/.../...f23b3764d.html	Mozilla/5.0 ... MSIE 10.0;...
(4)	http://h**j.c**r.pw/.../1390510620.jar	Mozilla/4.0 ... Java/1.7.0_15
(5)	http://h**j.c**r.pw/... /2	Mozilla/4.0 ... Java/1.7.0_15

表 1 のログのうち，(1)は改ざんされたサイト，(2)は Redirect ステップ，(3)は pre-Exploit ステップ，(4)は Exploit ステップ，(5)は pre-DL ステップにあたる．

(3)pre-Exploit ステップから(5)pre-DL ステップに着目すると，サーバ「h**j.c**r.pw」へのアクセスの中で，ファイル suffix や UserAgent が表 2 のように変化している．

【表 2 DbD 攻撃の遷移による変化】

ステップ	(3)pre-Exploit ステップ	(4)Exploit ステップ	(5)malware-DL ステップ
suffix	html	jar	なし
UserAgent	MSIE	Java	Java

表 2 の(3)は難読化された Javascript を含む HTML ファイルである．この HTML ファイルは iframe を使用して読み込まれるため，通常の Web アクセスと同様に UserAgent は Internet Explorer の環境をもとに決定され，suffix も html になっている．HTML に含ま

れる Javascript が実行されると，ブラウザやプラグインのバージョンが調査され，脆弱性を悪用する準備が行われる．この例では Java プラグインに脆弱性があったため，JRE を起動して(4)を読み込ませている．(4)は JRE の脆弱性 CVE-2013-2423 を悪用する Exploit コードである．この Exploit コードは(3)で起動された JRE によって読み込まれるため，通常の Web アクセスと同様に UserAgent は JRE の環境をもとに決定され，suffix も jar になっている．Exploit コードが実行されると，(5)のダウンロードと実行が行われる．(5)は Windows の実行可能ファイルで，Zbot 系マルウェアである．このファイルは，脆弱性を悪用された JRE がダウンロードして実行するため，UserAgent は JRE の環境をもとに決定される．

このように，JRE の脆弱性を悪用する場合は，JRE を起動してから悪意のあるコードを読み込ませるため，ファイル suffix や UserAgent が必ず変化する．したがって，攻撃者がこの特徴を故意に変更することは非常に困難である．例えば Nuclear Exploit Kit が Java の脆弱性を悪用する攻撃では，この特徴は約 6 ヶ月にわたって変化していないことを確認している．

本システムは，このように②pre-Exploit ステップから④pre-DL ステップに出現する Exploit Kit の定性的特徴を用いて，DbD 攻撃を検知している．

2.2 攻撃手法の変化

Tokyo SOC レポート[2][3]によると，2013 年に観測された DbD 攻撃の約 90%は JRE の脆弱性を利用していたが，2014 年上半期に観測された DbD 攻撃では約 65%に低下した．一方で，Adobe Flash Player 等の脆弱性を悪用した DbD 攻撃は，2013 年の約 10%から 2014 年の約 34%へ増加した．

また Cisco 2014 Midyear Security Report [4]では，FlashPack や Angler，Fiesta，RIG といった JRE 以外を攻撃する Exploit コードを取り入れた Exploit Kit の観測数が増加し，Exploit Kit の勢力図が変化しつつあることが示されている．これは JRE のセキュリティレベルが向上し，脆弱性を悪用することが難しくなったため，攻撃者が攻撃対象のソフトウェアを変更したことによるものと思われる．このように 2014 年以降，Exploit Kit には大きな変化が生じている．

2.3 本システムへの影響

新しい Exploit Kit が出現した場合や，Exploit Kit の攻撃するソフトウェアが変化した場合は，定性的特徴にも変化が生じる．特に 2014 年以降は，攻撃対象のソフトウェアが JRE から Adobe Flash Player 等へ変化したため，これまで JRE への攻撃を検知するパターンを中心に開発していた本システムにおいては，新たな定性的特徴を用いる検知パターンを早期に追加する必要がある．

このように Exploit Kit が大きく変化している状況の中では，Exploit Kit の変化を迅速に察知して検知パターンを追加・改良するだけでなく，Exploit Kit の変化に左右されないような検知パターンの開発も必要である．

3 問題解決に向けた調査と検討

3.1 調査方法

2.1 で説明した通り，Exploit Kit の定性的特徴は②pre-Exploit ステップから④pre-DL ステップに現れやすく，これまでは本システムも，その 3 ステップに着目して検知パターンを開発していた．一方で，①Redirect ステップや⑤malware-DL ステップには，Exploit Kit の特徴が現れにくいことが分かっている．ここから，この 2 ステップの特徴を用いれば Exploit Kit の変化の影響を受けにくい検知パターンの開発が可能と考えた．

そこで，まず上述の仮説を確認するため，2014 年 8 月～9 月に本システムで観測した

DbD 攻撃ログや，外部情報源から入手した DbD 攻撃ログ 69 件を用いて，①Redirect ステップおよび⑤malware-DL ステップと Exploit Kit の関係性を調査した.

3.2 Redirect ステップの分析

本研究で収集したログのうち，Redirect ステップが類似しているログは 8 種類 47 件あった．このうち，異なる Exploit Kit が使用されているにも関わらず，Redirect ステップが共通しているログが 5 種類あった．以下にその例を 2 つ示す.

A) ブログパーツ改ざんの事例

2014 年 8 月，TrendMicro 社は，国内ブログでよく利用されるパーツが改ざんされ，FlashPack Exploit Kit に誘導される事例を報告した[6]．このブログパーツを悪用した DbD 攻撃について，本システムで検知した URL の遷移パターンを図 2 に示す.

(1) ブログパーツを使用している Web ページの URL
(2) ブログパーツの URL
(3) http://r**7.a**l.net/index.php?o={base64}…①
(4) http://r**4.a**l.net/index2.php …①
(5) http://r**7.a**l.net/c**r/index.php …②
(6) http://r**7.a**l.net/c**r/client_do.swf …③
(7) http://5.**.**.**/c**r/gate.php?id=** …③

【図 2 FlashPack に誘導される例】

図 2 では(3)～(4)が①Redirect ステップ, (5)以降が②pre-Exploit / ③Exploit ステップにあたる．(5)以降に FlashPack Exploit Kit に特徴的な遷移が現れている.

このブログパーツについてさらに調査を行ったところ，2014 年 9 月に遷移が図 3 のように変化したことが分かった.

(1) ブログパーツを使用している Web ページの URL
(2) ブログパーツの URL
(3) http://2**f.k**e.com.pl/index.php?w={base64}…①
(4) http://2**c.k**e.com.pl/index2.php…①
(5) http://q**e.a**s.com/?PHPSSESID={base64}…②

【図 3 RIG に誘導される例】

図 3 において，(3)～(4)の Redirect ステップは，2014 年 8 月時点の例である図 2 と共通しているが，(5)以降の URL の特徴が RIG Exploit Kit のものに変化している．ここから，このブログパーツを悪用した DbD 攻撃において，①Redirect ステップと，②pre-Exploit ステップ以降は独立していることが分かった.

なお，Redirect ステップにこのような特徴が現れる攻撃は，Windigo と呼ばれる攻撃グループに関連することが知られている[5].

B) 攻撃サーバ「r**k.ru」の事例

2014 年 9 月 1 日に外部情報源から入手した攻撃ログの中に，図 4 のように遷移するログが見つかった.

(1) 改ざんされたサイトの URL
(2) http://r**k.ru/dzqhrxs.cgi?default … ①
(3) http://n**q.p**s.com/?PHPSSESID=… … ②
(4) http://n**q.p**s.com/index.php?req=mp3&… … ③

【図 4 RIG に誘導される例】

図 4 では，(2)が①Redirect ステップ，(3)以降が②pre-Exploit / ③Exploit ステップにあたる．(3)以降に RIG Exploit Kit に特徴的な遷移が現れている．この例で，Redirect ステップが実行されたドメイン「r**k.ru」は，以前，別の DbD 攻撃で使用されたドメインである．そこで，このドメインについて調査を行ったところ，9 月末に遷移が図 5 のように変化したことが分かった.

(1) 改ざんされたサイトの URL
(2) http://r**.ru/wlkzkir.cgi?default … ①
(3) http://p**e.v**9.com/TbC…EQ … ②
(4) http://p**e.v**9.com/TbC…EQ/e.html … ②
(5) http://p**e.v**9.com/TbC…EQ/djIhQ.swf … ③

【図 5 NullHole に誘導される例】

図 5 では，(2)が①Redirect ステップ，(3)以降が②pre-Exploit / ③Exploit ステップにあたる．Redirect ステップの URL は図 4 と類似しているが，(3)以降の遷移が，NullHole Exploit Kit と思われるものに変化している．ここから，この攻撃においても，①Redirect ステップと，②pre-Exploit ステップ以降は独立していることが分かる.

これらの調査結果から, DbD 攻撃に使用される Exploit Kit が変化し，それにともなっ

て②pre-Exploit ステップから④pre-DL ステップが変化しても，その影響は必ずしも①Redirect ステップには及ばないことが分かった．したがって，①Redirect ステップの特徴を捉える検知パターンを開発すれば，Exploit Kit に拠らない検知が可能になると考えられる．

3.3 malware-DL ステップの分析

本研究で収集したログのうち，⑤malware-DL ステップが含まれていたものは 4 件しか存在しなかった．そのため，Exploit Kit と malware-DL ステップの関係性を明らかにすることができず，今回は malware-DL ステップの検知パターンは開発できなかった．サンプル数が少なかった原因は，最近では④pre-DL ステップでマルウェア本体をダウンロードしてしまい，⑤malware-DL ステップを実行しない攻撃があること，仮想環境上では Downloader が動作しない場合があること，本システムの運用環境ではセキュリティ対策が有効に機能しているため，DbD 攻撃が malware-DL ステップへ遷移する前に通信がブロックされること等がある．

4 検知パターンの開発・改良

4.1 Redirect ステップ検知パターン開発

Redirect ステップの検知パターン開発にあたっては，まず既存の検知パターンと同様に定性的特徴を用いた開発が可能か検討した．しかし，Redirect ステップは Proxy ログ上では 1～2 行程度しかなく，一般的な Web アクセスと DbD 攻撃との間に，明確な定性的特徴の違いを見つけにくいため，定性的特徴を捉えた検知パターンの開発が難しかった．そこで本研究では，URL 中の文字列を用いて検知パターンを作成することにした．

文字列を検知パターンとして使用する場合，ある程度の文字列の変化に耐えられるように，通常は正規表現を用いて一般化した文字列を検知パターンとする．しかし，単に一般化するだけでは，誤検知も増加してしまうという問題がある．

そこで本研究では，URL 中の文字列の意味を分析し，今後の変化も予測して，文字列を可能な限り一般化して表現しつつ，誤検知を低減した検知パターンを開発した．ここでは，図 4 で示したブログパーツ改ざんの例を用いて，誤検知を低減した例を説明する．

図 4 の(3)の{base64}部分をデコードすると，ブログパーツを使用している Web ページのドメインと URL パス，ユーザが Web ページにアクセスした時刻などの情報が含まれていた．さらに他の DbD 攻撃においても，Redirect ステップの URL に改ざんされた Web ページの情報が含まれている事例を確認できた．ここから攻撃者は Redirect ステップで，改ざんした Web ページの情報を収集し，効果が高い攻撃方法を分析していると考えられる．

もし，攻撃者が自身の攻撃の効果を測定するために，Redirect ステップを使って改ざんした Web ページの情報を収集しているなら，Web ページの情報を送信する手法は継続的に利用されると考えられる．すなわち，その手法から現れる特徴は変化しにくいと言える．本研究では，この仮説をもとに，情報の内容や送信量を鍵として誤検知を減らしつつ，可能な限り文字列を一般化して，検知パターンを作成した．

本研究では，本システムで観測した DbD 攻撃のログと，外部情報源から入手した DbD 攻撃のログを分析して，以下 5 つの DbD 攻撃の検知パターンを実装した．

(i) サーバを乗っ取り，正規のファイルへのアクセスがあった際に，ステータスコード 302 を発行してリダイレクトさせる DbD 攻撃
(ii) Movable Type の脆弱性を突いてページを改ざんし，リダイレクトさせる DbD 攻撃
(iii) リダイレクトを発生させる Flash ファイル読み込ませる DbD 攻撃
(iv) Wordpress の脆弱性を突いてページを改ざんし，Internet Explorer でアクセスした

場合にのみリダイレクトさせるDbD攻撃

(v) 複数のサイトを改ざんし，リダイレクト先を全ての改ざんサイトで定期的に切り替えることで検知の撹乱を図るDbD攻撃

4.2 Exploitステップ検知パターンの改良

Redirectステップ検知パターンの開発とあわせて，Exploit Kit自体の変化にも追従できるように②pre-Exploitステップから④pre-DLステップを捉える検知パターン（以下，「Exploitステップ検知パターン」）の開発・改良にも取り組んだ．特に、既存の検知パターンでは対応できないことが分かっているExploit Kitのうち，運用環境における危険度が高いと思われるものについて，本システムの運用中に検知したDbD攻撃のログや，外部情報をもとに，検知パターンの開発・改良を実施した．

具体的には，JRE以外のExploitを積極的に取り入れており，かつ盛んに使用されていた，以下の7つのExploit Kitについて，パターンの開発・改良を行った．

(a) 検知パターンを新規に開発したもの
RIG, Fiesta, Angler, FlashPack

(b) 既存の検知パターンを改良したもの
Nuclear, Neutrino, Magnitude

5 D3M Datasetsによる評価

5.1 評価手法

D3M(Drive-by Download Data by Marionette) Datasets 2015には，2種類のデータが含まれている．

A) Web クライアント型ハニーポット(Marionette)が悪性URLを巡回して得たDbD攻撃の通信データ

B) Marionetteが取得したマルウェアをサンドボックス(Botnet Watcher)上で実行して得たC&C通信データ

本研究ではDbD攻撃の検知パターンを開発したため，(A)のデータを使用して検知率を測定した．データはpcap形式で提供されているため，評価にあたってはpcapファイルからHTTP通信のみを抽出し，本システムが処理可能なProxyログ形式へ変換した．また(A)のデータには，直接マルウェアを取得する場合など，②pre-Exploit,③Exploit,④pre-DLのステップを経ないデータも含まれている．このようなデータは除いて検知率を評価した．

こうして作成したProxyログ形式のデータ283個に対して，本システムを適用し検知率を集計した．

5.2 評価結果

表3にデータの取得年ごとの検知率を示す．

【表 3 取得年ごとの検知率】

取得年	データ数	検知数	検知率
2011年	116	64	55.2%
2012年	110	98	89.1%
2013年	42	40	95.2%
2014年	12	1	8.3%
2015年	3	0	0.0%
合計	283	203	71.7%

2011年の検知率は55.2%と低いが，2012年と2013年は検知率80%以上を達成し，2013年の検知率95.2%が最も高くなった．一方で，2014年と2015年に取得されたデータのうち，本システムで検知できたものは1個のみであった．これは，我々が昨年D3M Datasets 2014を用いて実施した評価の結果[7]と，ほぼ同様の結果である．

検知できなかったデータのうち，2015年に取得されたものを分析したところ，全てのデータにおいて，Angler Exploit Kitと思われる特徴がURLに現れていた．しかし，本システムのAngler Exploit Kit向け検知パターンで用いている定性的特徴が現れていないために，検知できなかったことが分かった．

そこで，Proxyログ形式に変換する前のpcapファイルを分析したところ，3個のうち2個は，Exploitステップにおいて，サーバか

ら受信したデータ量が 0byte～数十 byte と極めて小さいことが分かった．ここから，Exploit コードが配信されず攻撃が中断したため，定性的特徴が現れなかったと考えられる．しかし，残り 1 個は Exploit コードと思われるファイルが配信されて攻撃が進行しており，危険度が高いことが分かった．本システムの検知パターンで用いている定性的特徴は，Internet Explorer の脆弱性を悪用した DbD 攻撃の場合，現れないケースがあることが分かっている．このデータが，そのケースに該当した可能性が考えられる．

6　独自データセットによる評価

D3M Datasets には，Redirect ステップを含むログがなかった．そこで独自に作成したデータセットを用いて評価した．

6.1　評価手法

独自データセットは，2015 年 4 月～7 月に外部情報源等から収集したデータ，全 30 個を用いて作成した．

まず，Redirect ステップ検知パターンの検知能力を調べるため，独自データセットに Redirect ステップ検知パターンを適用して検知数を集計した．また，Redirect ステップ検知パターンは，攻撃が中断したデータについても検知するため，Redirect ステップで検知したデータについては攻撃が進行したか調べ，危険度を判断した．

次に，Redirect ステップ検知パターンと，Exploit ステップ検知パターンの検知範囲の重複度合いを調べるため，独自データセットに Exploit ステップ検知パターンを適用して検知数を集計した．そして，Redirect ステップ検知パターンで検知したデータ群と，Exploit ステップ検知パターンで検知したデータ群を比較し，検知範囲の重複を調べた．

6.2　評価結果

まず，独自データセットに Redirect ステップ検知パターンを適用した．結果，24 個を検知でき，検知率は 80%となった．また，検知したデータを調べたところ，Exploit ステップまで進行しているデータが 6 個あり，そのうち 5 個については，Exploit コードと思われるファイルが配信されており，危険度が高いことが分かった．

次に，独自データセットに Exploit ステップ検知パターンを適用した．結果，6 個のデータを検知できた．

最後に，Redirect ステップ検知パターンで検知したデータうち，危険度の高い攻撃のデータ 5 個と，Exploit ステップ検知パターンで検知したデータ 6 個を比較した．結果，重複して検知したデータは一つもなかった．

ここから，Exploit ステップ検知パターンと，Redirect ステップ検知パターンの検知範囲は，重複していないことが分かった．

7　誤検知率評価

最後に，本システムの運用環境で得られたデータをもとに誤検知率を評価した．

2015 年 6 月 1 日～6 月 30 日に，本システムは約 5 億 4,915 万行の Proxy ログを分析しており，約 10 万行の誤検知が発生していた．ここから誤検知率は約 0.018%と分かった．昨年の誤検知率は 1 日あたり最大で約 0.011%であり，今年もほぼ同様の結果となった[7]．

8　考察

本評価により，検知率・誤検知率ともに昨年と同水準を維持できていることが確認された．また Redirect ステップ検知パターンと，Exploit ステップ検知パターンの検知範囲は，重複していなかった．ここから，Redirect ステップ検知パターンによって，本システムの検知能力を補強できたと考えている．

一方で，Exploit コードが配信されている

にも関わらず，Exploit ステップ検知パターンで用いている定性的特徴が現れていないケースがあった．このケースについては，別の定性的特徴が現れていることを確認している．ここから，特に JRE 以外の脆弱性を悪用する攻撃については，検知パターンで用いる定性的特徴を再検討し，パターンを改良する必要があると考えている．

9　まとめと今後の課題

本研究では，我々の開発したサイバー攻撃検知システムについて，Exploit Kit の挙動の変化に追従した改良を行った．そこで Exploit ステップの検知パターンを追加・改良するとともに，これまで未開発だった Redirect ステップの検知パターンを開発した．評価により，本システムの検知率・誤検知率を維持できたこと，Redirect ステップ検知パターンにより検知能力を補強できたことを確認した．また，Exploitコードが配信されているにも関わらず，Exploit ステップ検知パターンで用いている定性的特徴が現れないケースを確認した．

現在の Redirect ステップ検知パターンは定性的特徴を用いていない．そのため攻撃の変化に弱く，特定の攻撃しか検知できない．本システムの検知能力を長期間維持するには，Redirect ステップの定性的特徴を解明し，検知パターンを開発することが効果的と思われる．あわせて，JRE 以外への攻撃における定性的特徴を再分析し，Exploit 検知パターンを検討する必要がある．

また本研究では，malware-DL ステップの通信ログを十分に収集できなかったため，対応する検知パターンの開発を行わなかった．しかし，malware-DL ステップ以降の通信は，Downloader やマルウェア本体によって行われるため，通信の特徴が Exploit Kit の変化に左右されない可能性が高い．本システムには，現在も Downloader やマルウェア本体の C&C 通信の特徴を捉える検知パターンは存在するが，今後はこれらの検知パターン開発にも注力して取り組んでいきたい．

参考文献

[1] 北野美紗，大谷尚通，宮本久仁男，Drive-by Download 攻撃における通信の定性的特徴とその遷移を捉えた検知方式，MWS 2013

[2]2013 年下半期 TokyoSoc 情報分析レポート，https://www-935.ibm.com/services/multimedia/tokyo-soc-report2013-h2-jp.pdf

[3]2014 年上半期 TokyoSoc 情報分析レポート，https://www-304.ibm.com/connections/blogs/tokyo-soc/resource/PDF/tokyo_soc_report2014_h1.pdf

[4]Cisco 2014 Midyear Security Report, http://www.cisco.com/web/offers/lp/midyear-security-report/index.html

[5]Olivier Bilodeau, Operation Windigo, http://www.welivesecurity.com/wp-content/uploads/2014/03/operation_windigo.pdf

[6]Walter Liu, “Website Add-on Targets Japanese Users, Leads To Exploit Kit”, http://blog.trendmicro.com/trendlabs-security-intelligence/website-add-on-targets-japanese-users-leads-to-exploit-kit/

[7]大谷尚通，益子博貴，重田真義，実環境におけるサイバー攻撃検知システムの有効性評価および検知範囲の拡大に向けた検討，MWS2014