# ネットワーク通信の相関性に基づく Drive-by Download 攻撃検知手法

寺田 成吾† 小林 峻† 小出 和弘† 羽藤 逸文†
瀬戸口 武研† 道根 慶治† 山下 康一†

†株式会社 PFU

220-8567 神奈川県横浜市西区 みなとみらい 4 丁目 4-5 横浜アイマークプレイス

**あらまし** 年々高度化が進むマルウェアは，様々な検知回避手法を用いて組織ネットワークの出入口やエンドポイントにおけるセキュリティ対策を巧妙にすり抜けている．そこで本稿では，Drive-by Download攻撃（以下，DbD攻撃）が正規アプリケーションには見られない特有の通信挙動を示すことに着目し，ネットワーク通信を監視することで，攻撃者およびマルウェアに察知されることなく，DbD攻撃による感染端末を検出する手法を提案する．本手法では，端末の通信を監視し，マルウェア活動遷移モデルへ通信挙動を当てはめ，相関分析することにより組織内に潜む感染端末を検知する．また，検証として，DbD攻撃一連の通信データを含むMWS Datasetsを使用し，本手法の有効性を評価した．

# Drive-by Download Detection Method based on Network Traffic Correlation

Seigo Terada† Takashi Kobayashi† Kazuhiro Koide† Itsufumi Hato†
Mugen Setoguchi† Keiji Michine† Kouichi Yamashita†

†PFU LIMITED
YOKOHAMA i-MARK PLACE 4-5 MinatoMirai 4-chome, Nishi-ku, Yokohama-shi, Kanagawa
220-8567, JAPAN

**Abstract** Annually, improved Malware have invaded into a network by various evasion techniques. In this paper, therefore, we focus on Drive-by Download attacks (DbD attacks) has specific network traffic behaviors are different from formal applications, and propose the method detects devices infected by DbD attacks by observing on a network traffic without notification to attacker or malware. Furthermore, the method deals with correlation analysis using malware activity transition model which based on common traffic behaviors of malware. Also, for testing, we evaluated the effectiveness of the method by using MWS Datasets has some traffic flow data of DbD attacks.

## 1. はじめに

昨今，マルウェア感染により様々な組織の情報漏えいが騒がれ，年々高度化するマルウェアへの対応が必要となっている．マルウェアの感染経路は様々あるが，Web 経由で端末を感染させる攻撃手法の 1 つとして，Web ブラウザや端末内アプリケーションの脆弱性を利用する Drive-by Download 攻撃(以下，DbD 攻撃)がある．DbD 攻撃は，標的とする組織や個人が閲覧する Web サイト上に脆弱性攻撃を行う悪性コンテンツを用意し，Web サイトを閲覧した利用者の端末へ秘密裏にマルウェアをダウンロードさせる攻撃手法である．

DbD 攻撃のような外部からのマルウェア侵入を防ぐためのセキュリティ製品として，アンチウィルス製品やサンドボックス製品など様々なものがある．しかし，近年の高度なマルウェアは，対策技術と同様に進化を遂げており，例えば，実行コードの難読化や自身の動作環境に応じた隠蔽手法を用いて，これらセキュリティ製品の検知機構を回避する．DbD 攻撃においては，攻撃の特性上，HTTP コンテンツの遷移が起こるため，HTTP メッセージの遷移を監視する手法が研究されている [1] [2] [3] [4] [5].

本研究では，マルウェアの活動をネットワーク通信の観点で 8 つの活動フェーズに整理した“マルウェア活動遷移モデル”を定義し，監視する端末の通信を各フェーズに当てはめ，活動フェーズの遷移を相関分析する手法により DbD 攻撃の検知を行う. また, 本手法では，ネットワークを監視し，HTTP リクエストおよびレスポンスメッセージを検査することで活動フェーズを識別する．実際の脆弱性攻撃やマルウェアによる活動通信を端末の外部から監視するため，攻撃者やマルウェアに察知されることなく，DbD 攻撃が行われた端末を検出することができる.

本手法の有効性を確認・検証するために MWS Datasets 2015 [6]で提供される D3M，および Barracuda Labs が提供している Threatglass [7]の DbD 攻撃に関する通信データを用いて評価を行った.

## 2. 関連研究

HTTP 通信の遷移に注目した DbD 攻撃の検知に関する研究として，寺田ら [1]は，Web ページアクセス時の遷移の特徴を抽出し，DbD 攻撃の判別に Web アクセス遷移の考慮が有効であることを示している．大谷ら [2]と北野ら [3]は，組織内のネットワーク機器やセキュリティ機器のログから DbD 攻撃の定性的な特徴を抽出し，統合分析をすることで DbD 攻撃を検知する方式を提案している．また，松中ら [4]は，ユーザが使用するブラウザおよび Web プロキシに観測センサを設置し DbD 攻撃に関わる脅威をリアルタイムに把握するフレームワークを提案している．進藤ら [5]は, HTTP レスポンスヘッダに含まれる Content-Type 情報を用いる DbD 攻撃検知手法を提案している.

HTTP 通信のリクエストラインやリクエストおよびレスポンスのヘッダー情報のみを信じて，HTTP 通信の遷移を相関的に検査する場合，マルウェアによるコンテンツ偽装に対して耐性が低くなってしまう．そのため本手法では，HTTP 通信のボディ情報も検査し，ヘッダー情報との一致性を確認し，コンテンツの真偽性を検査している．ただし，ファイル／コンテンツ自体の悪性(不正なコードや攻撃コードの有無)を検査すると膨大な解析を行う必要があるため，コンテンツ自体の悪性検査は行っていない．つまり，本手法は，コンテンツ自体の悪性を検査する手法よりも軽量かつ，マルウェアによるコンテンツ偽装に対する耐性が高い手法を目指す.

## 3. 検知手法

### 3.1. マルウェア活動遷移モデル

まず，本手法で定義する“マルウェア活動遷移モデル”について説明する．本モデルは，マルウェアの侵入と活動をネットワーク通信の観点で 8 つの活動フェーズに整理し(表 1)，それぞれの活動フェーズから別の活動フェーズへの遷移を整理したものである(図 1).

| **Phase 番号** | **マルウェア活動** |
|---|---|
| Phase1 (P1) | 侵入 |
| Phase2 (P2) | 探索 |
| Phase3 (P3) | 感染・浸潤 |
| Phase4 (P4) | 実行形式ファイルのダウンロード |
| Phase5 (P5) | C&C サーバ検索 |
| Phase6 (P6) | C&C 通信 |
| Phase7 (P7) | 搾取情報のアップロード |
| Phase8 (P8) | 攻撃活動 |

**表 1　マルウェア活動フェーズ**

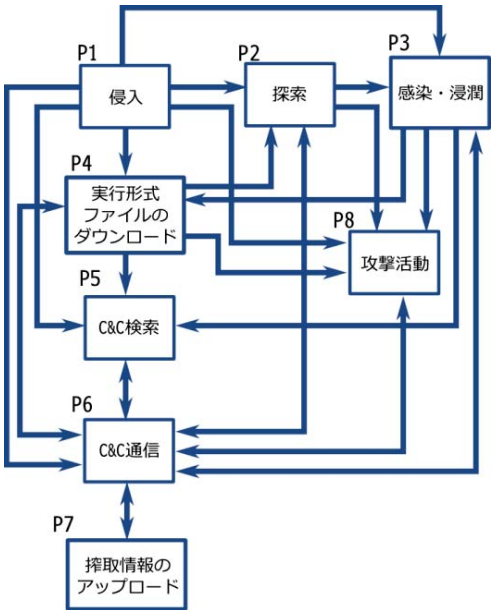


**図 1 マルウェア活動遷移モデル**

ここでは，侵入フェーズ，実行形式ファイルのダウンロードフェーズについて説明する．侵入フェーズ(Phase1)は, メールなどに添付された悪性コンテンツへのリンク URL のクリック, 改ざんされた正規の Web サイトへのアクセスなどを契機に，悪性コンテンツが侵入するフェーズである．本手法において検査対象とする悪性コンテンツ候補は，下記 5 種類としている．

1 Java Package
2 Silverlight
3 Flash
4 PDF
5 HTML/JavaScript (Internet Explorer)

悪性コンテンツ候補を識別するための検査は，まず，HTTP の GET リクエストメッセージを検査し，URI に上記悪性コンテンツ候補のファイル拡張子が設定されている(.jar や.xap, .swf など)，または，HTTP リクエストヘッダーが上記悪性コンテンツ候補をダウンロードする際の特徴を満たしている(User-Agent ヘッダーに Java の User-Agent が設定されているなど)場合，HTTP レスポンスメッセージの Content-Type ヘッダー, または, ボディ部のデータに含まれるファイルのマジックナンバーを検査し，悪性コンテンツ候補のダウンロードを判定する．

実行形式ファイルのダウンロードフェーズ(Phase4)は, 上記侵入フェーズで攻撃コードが送り込まれたのち，マルウェアの配布サイトからマルウェア本体をダウンロードするフェーズである．また，C&C サーバからの指令に従って，既に端末内に潜むマルウェアが新しい機能の追加などを目的に新たな実行形式ファイルをダウンロードする場合も本フェーズに含まれる．実行形式ファイルを識別するための検査は， HTTP レスポンスメッセージの Content-Type ヘッダーとボディ部のコンテンツの整合性検査，または，ボディ部のデータに対し実行形式ファイルの MZ シグネチャと PE ヘッダーの存在，zip 等のアーカイブファイルである場合はアーカイブされたファイルの拡張子(.exe や.dll など)を検査し，実行形式ファイルのダウンロードを判別する．

### 3.2. DbD 攻撃の相関分析

DbD 攻撃は以下の流れで実行される(図 2).

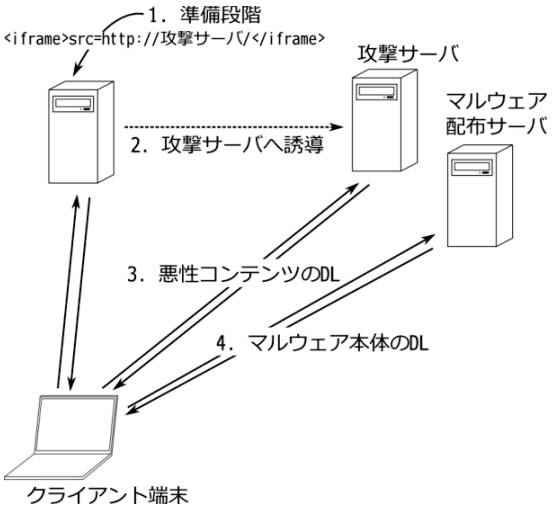


**図 2 DbD 攻撃の流れ**

**1. 準備段階**

攻撃者は，標的がアクセスする正規の Web サイトを改ざんし, 攻撃サーバへ誘導(リダイレクト)するリンクを挿入する．

**2. 攻撃サーバへの誘導**

標的が改ざんされたサイトにアクセスすると, 標的は, サイトに埋め込まれた「攻撃サーバへ誘導するリンク」に従って，攻撃サーバへ誘導される.

**3. 悪性コンテンツのダウンロード**

攻撃サーバから標的に対して，標的が使用する Web ブラウザや各種プラグイン・ソフトウェアの脆弱性を利用する悪性コンテンツが送り込まれる.

**4. マルウェア本体のダウンロード**

悪性コンテンツによる脆弱性を利用した攻撃が成功すると，標的に対してダウンロードコードが読み込まれ，マルウェア本体が自動的にダウンロードされる.

本手法では，上記“3. 悪性コンテンツのダウンロード”を侵入フェーズ，“4. マルウェア本体のダウンロード”を実行形式ファイルのダウンロードフェーズへ当てはめ，DbD 攻撃の条件を満たすか相関分析を行う．相関分析の条件を表 2 に示す．表 2 内に示す“TCP コネクション”，“接続先サーバ”の条件は，Phase1 と Phase4 の通信の TCP コネクション，または，接続先サーバが同一かどうかの条件である．“HTTP 通信の割り込み”の条件は，Phase1 と Phase4 の通信間に Phase1 と同一のサーバとの HTTP 通信を行ったかどうかの条件である.

| 相関条件 | TCP コネクション | 接続先サーバ | HTTP 通信の割り込み |
|---|---|---|---|
| CA1 | 同一 | — | — |
| CA2 | 異なる | 同一 | なし |
| CA3 | 異なる | 同一 | あり(1 つ許容) |

**表 2　Phase1-Phase4 の相関条件**

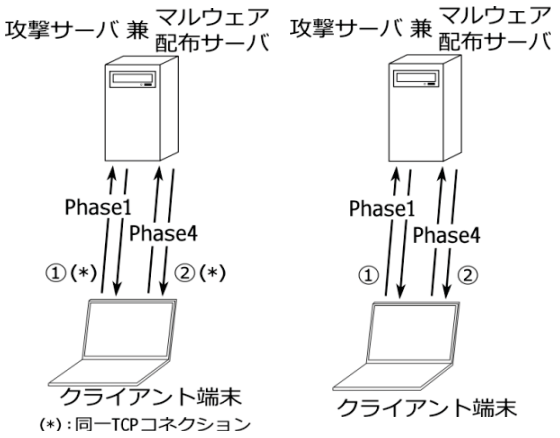


**図 3　相関条件 1 (左)および相関条件 2 (右)**

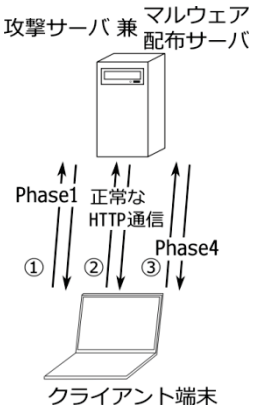


**図 4　相関条件 3**

例えば，Angler Exploit Kit (Angler EK)は，表 3，図 5 のように CA2 の条件に一致する特徴があるため DbD 攻撃を検知することができる．表 3 における番号①～③は，図 5 における HTTP 通信①～③にそれぞれ対応する.

| 番号 | TCP コネクション | 接続先サーバ | Phase |
|---|---|---|---|
| ① | Conn-A | ドメイン A | — |
| ② | Conn-B | ドメイン B | 1 |
| ③ | Conn-C | ドメイン B | 4 |

**表 3　Angler EK の攻撃シーケンスまとめ**

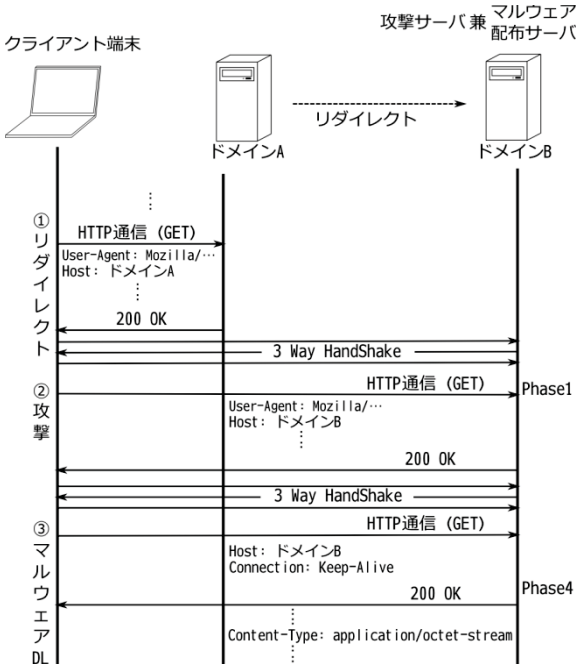


**図 5　Angler EK の攻撃シーケンス**

## 4.　評価試験

### 4.1.　試験方法

本評価では，本手法を実装したプログラムを Linux マシン上で動作させ，通信をプロミスキャスモードでモニタリングさせた．そして，パケット送信用マシンから，tcpreplay プログラムを用いて DbD 通信を含むパケットキャプチャファイルを再生・送信し，試験プログラムが動作するマシンへ送出することで評価を行った．

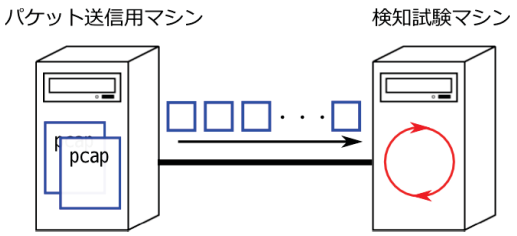


**図 6　検知試験の構成**

### 4.2.　D3M 2015 による評価

D3M (Drive-by Download Data by Marionette) は，マルウェア対策研究人材育成ワークショップで配布されているデータセットの 1 つである．このデータセットには，秋山らが開発した高対話型ハニークライアント (Marionette) [8]が巡回した DbD 攻撃に関連する URL にアクセスした際のパケットキャプチャファイルが収められている．しかし，ハニークライアントが巡回した際，攻撃サーバが停止している，DL した攻撃スクリプトの実行に失敗するなどして，マルウェア本体をダウンロードしていない通信が多く見られた．本手法では，マルウェア本体がダウンロードされなければ，Phase4 を検出できないため，DbD 攻撃を検知しない．そのため， D3M からマルウェア本体のダウンロードを行っている通信シーケンス 11 個を抜粋し，DbD 攻撃を検知できるか評価を行った．

| | D3M 2015 |
|---|---|
| 巡回 URL 数 | 299 |
| マルウェアを DL した数 | 11(2) |
| DbD 検知数 | 9 |
| 検知率 (%) | 81.8 |

**表 4　D3M による評価結果**

※　()内はマルウェア検体のユニーク数

| | D3M 2015 | CA 割合(%) |
|---|---|---|
| DbD 検知数 | 9 | — |
| CA1 | 1 | 11.1 |
| CA2 | 8 | 88.9 |
| CA3 | 0 | 0.0 |

**表 5　D3M にて一致した DbD 条件**

本評価では，上記表 4 の結果の通りの検知率を示し，表 5 の結果から DbD 攻撃シーケンスは，ほぼ CA2 の条件に当てはまるものが検出された．これは，検体ユニーク数からわかるように，同一 URL へ異なる日にアクセスを行った通信シーケンスや URL は異なるが同一サーバへアクセスした通信シーケンスがあり，それぞれ同一攻撃シーケンスを記録したためである．

今回検知した DbD シーケンスの 1 つとして，Content-Type ヘッダーを image/gif と詐称した上でマルウェア本体(exe)ファイルをダウンロードしているものが見られた．本手法で

は，Content-Type ヘッダーとボディ部の一致性を確認しているため, このタイプの DbD シーケンスを問題なく見つけることができた．

また，マルウェア本体のダウンロードが行われなかった 288 ファイルについては，攻撃に失敗しているため，Phase4 が検出されず，DbD 攻撃の検知は期待通り行われなかった．

検知できなかった通信パターン 2 件については，URL は異なるが下記表 6 のように同一サーバへのアクセスであり，ほぼ同一の通信パターンを示した．この通信パターンが相関条件に一致せず，検知に至らなかった．

| パターン | URL |
|---|---|
| 1 | http://www.zi**.pl/ |
| 2 | http://zi**.pl/ |

**表 6　検知できなかった URL**

### 4.3.　Threatglass **[7]**による評価

Threatglass は, バラクーダネットワークス社がマルウェアに感染した Web サイトの情報を公開しているコミュニティサイトである．感染サイトに対する意識向上と，攻撃方法の理解を目的に様々な情報が公開されており，パケットキャプチャも入手することができる．本評価では，D3M 同様に，DbD 攻撃に関して Exploit からマルウェア本体のダウンロードまでの通信シーケンスが含まれるファイル 65 個を抜粋して評価を行なった．ただし，Threatglass のキャプチャファイルは，数 kB を超えるジャンボフレームが含まれており，そのままではパケット送信用マシンからパケットを正しく送出することができない．このため，tcpreplay に含まれる tcpedit を用いて，ジャンボフレームを MTU に収まるように分割したキャプチャファイルを作成し，評価を行った．

| | Threatglass |
|---|---|
| キャプチャファイル数 | 65 |
| DbD 検知数 | 65 |
| 検知率 | 100% |

**表 7　Threatglass による評価結果**

| | Threatglass | CA 割合(%) |
|---|---|---|
| DbD 検知数 | 65 | - |
| CA1 | 14 | 21.5 |
| CA2 | 51 | 78.5 |
| CA3 | 0 | 0 |

**表 8　Threatglass にて一致した DbD 条件**

Threatglass による評価では, 表 7 に示す通りの検知率を示した．一致した CA 条件の割合としては，CA1 条件が 21.5%，CA2 条件が 78.5%であり，DbD 攻撃シーケンスとして，D3M Dataset と同じく Phase1 から Phase4 の遷移は同一 TCP コネクション上, または, HTTP 割り込みが無い別 TCP コネクションのパターンの 2 種類が見られた．ただし，D3M に比べて CA1 の条件の割合が増え，CA1 の条件の有効性が示された．

### 4.4. NCD in MWS Cup 2014 による評価

NCD データセットは，MWS Datasets 2015 に含まれ，2014 年 10 月 22 日に開催された MWS Cup 2014 [9]期間中の通信をホワイト通信として提供するものである．ここでは，このデータには DbD 攻撃に関する通信は含まれていないものとして，誤検知に関する評価を行なった．提供されたキャプチャファイルの統計情報を表 9 にまとめた．

| | |
|---|---|
| パケット収集期間 | 9:34:37～12:05:57 |
| パケット数 | 6,864,565 |
| 通信バイト数 (GB) | 5.72 |
| 宛先ユニークホスト数 | 1884 |
| HTTP リクエスト数 | 43,100 |
| 実行ファイルの DL 数 | 84 |

**表 9　大会期間中の統計情報**

結果としては，DbD 攻撃を検知することはなかったが, これは大会期間が短かったため, DbD 攻撃シーケンスに似た通信が少なかったことが考えられる．しかし，DbD 攻撃ではなく, C&C 通信(Phase6)として検知した HTTP 通信が複数あった．DbD 攻撃以外の事象についても，引き続き評価を行っていきたい．

## 5. まとめ

ネットワーク通信を監視し，端末が行うHTTP 通信をマルウェア活動遷移モデルにおける侵入フェーズ(Phase1), 実行形式ファイルのダウンロードフェーズ(Phase4)を相関分析する本手法により DbD 攻撃を検知できることを示した．D3M を用いた評価では，DbD 攻撃シーケンスで，Content-Type が偽装された場合も問題なく検知できることを示し，HTTP レスポンスメッセージの Content-Type ヘッダーとボディ部のコンテンツの整合性検査を行うことの有用性を評価できた．

評価試験の問題点として，評価対象データにおける DbD 攻撃シーケンスのパターンが少ないこと，十分な誤検知評価ができていないことが挙げられるため，より豊富なデータを入手し，追加で本手法の評価を行う必要がある．

今後は，前述した評価を行うと共に，最新の DbD 攻撃の調査と対応を行っていく．また，今回検証できなかった負荷性能試験を行い，ネットワーク監視の限界性能を評価する予定である．さらに，マルウェア活動遷移モデルにおける Phase1，Phase4 以外の評価を行う必要があり，特に C&C 通信に関する Phase6 の評価を行っていく．



文献目録

[1] 寺田剛陽, 古川忠延, 東角芳樹, 鳥居悟, “検知を目指した不正リダイレクトの分析,” MWS2010, 2010.

[2] 大谷尚道, 北野美紗, 重田真義, “企業内ネットワークの通信ログを用いたサイバー攻撃検知システム,” MWS2013, 2013.

[3] 北野美紗，大谷尚道，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,” MWS2013, 2013.

[4] 松中隆志，窪田歩，星澤裕二，“Drive-by-Download 攻撃対策フレームワークにおける Web アクセスログを用いた Web リンク構造の解析による悪性サイト検出手法の提案,” Computer Security Symposium 2014, Oct 2014.

[5] 進藤康孝, 佐藤彰洋, 中村豊, 飯田勝吉, “マルウェア感染ステップのファイルタイプ遷移に基づいた Drive-by Download 攻撃検知手法,” Computer Security Symposium 2014, Oct 2014.

[6] 神薗雅紀, 秋山満昭, 笠間貴弘, 村上純一, 畑田充弘, 寺田真敏, “マルウェア対策のための研究用データセット～MWS Datasets 2015～,” 情報処理学会 研究報告コンピュータセキュリティ(CSEC) Vol. 2015-CSEC-70, No6, 2015.

[7] Barracuda Labs, “Barracuda Labs Threatglass,” Barracuda Networks, Inc, [オンライン]. Available: http://www.threatglass.com/.

[8] M. AKIYAMA, M. IWAMURA, Y. KAWAKOYA, K. AOKI , M. ITOH, “Design and Implementation of High Interaction Client Honeypot for Drive-by-Download Attacks,” IEEE Trans. of Communication, Vol. E93-B, No.5, pp. 1131-1139, May 2010.

[9] MWS2014 実行委員会, “MWS Cup について,” 2014. [オンライン]. Available: http://www.iwsec.org/mws/2014/about.html.