CSS/MWS2015
【MWSドライブ・バイ・ダウンロード】1A3-1

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

株式会社PFU
アプライアンスソフトウェア事業部 技術部
○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

2015年10月21日

アジェンダ

PFU
a Fujitsu company

1　研究背景

2　検知手法

- 概要
- 通信パターンの識別
- 通信パターンの相関分析

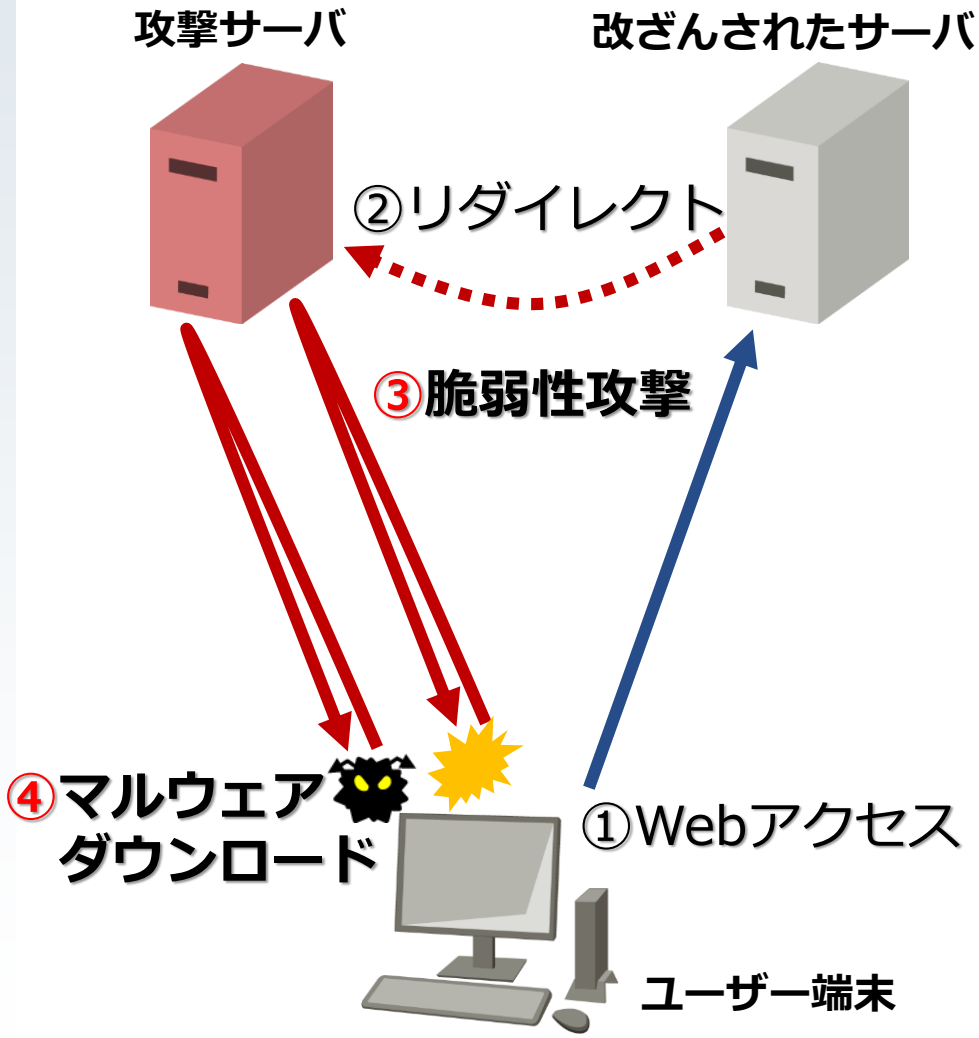
3　評価方法

4　評価結果

- D3M 2015
- Threatglass
- NCD in MWS Cup 2014

5　まとめ

Drive-by Download（DbD）攻撃の特徴



1. ユーザが改ざんされたサーバへアクセス
2. 攻撃サーバへリダイレクト
3. ユーザ端末のアプリケーションの脆弱性を攻撃
4. 秘密裏にマルウェアをDL

ユーザーは一連の攻撃に気づけない

本検知手法は、③と④に着目

他の検知手法

- **セキュリティ機器のログを用いた検知手法**
  - URIやHTTPヘッダーの特徴

➡ **攻撃者による偽装や隠蔽に弱い**

- **Webコンテンツを分析する検知手法**
  - シグネチャとのパターンマッチ
  - 難読化されたスクリプトの特徴
  - コンテンツのリンク構造
  - スクリプトやマルウェアの動的解析

➡ **解析コストが大きい**
検知回避機能をもつマルウェアの存在

研究背景

我々が考案した検知手法

ネットワークトラフィックを直接観測する方式
- ログよりも詳細な情報
- リアルタイム分析
- かんたん設置
- 攻撃者に監視されていることを察知されない

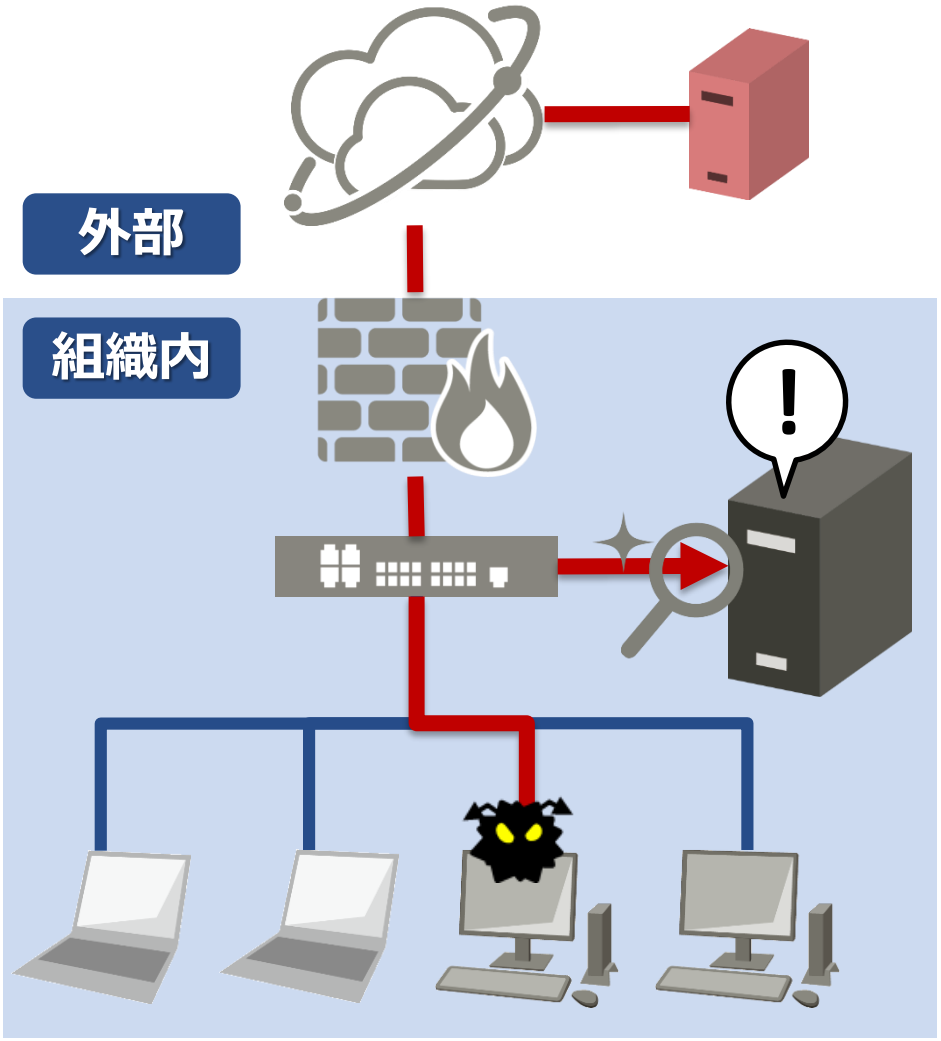
マルウェア活動の遷移モデルを使用した検知方式
- コンテンツの悪性検査を行わない軽量な実装
- マルウェアの変化に強い

検知手法の評価

未知のデータセットを用いて、
DbD攻撃における**本検知手法の有効性を評価**

検知手法（概要）

ネットワークトラフィックのモニタリング

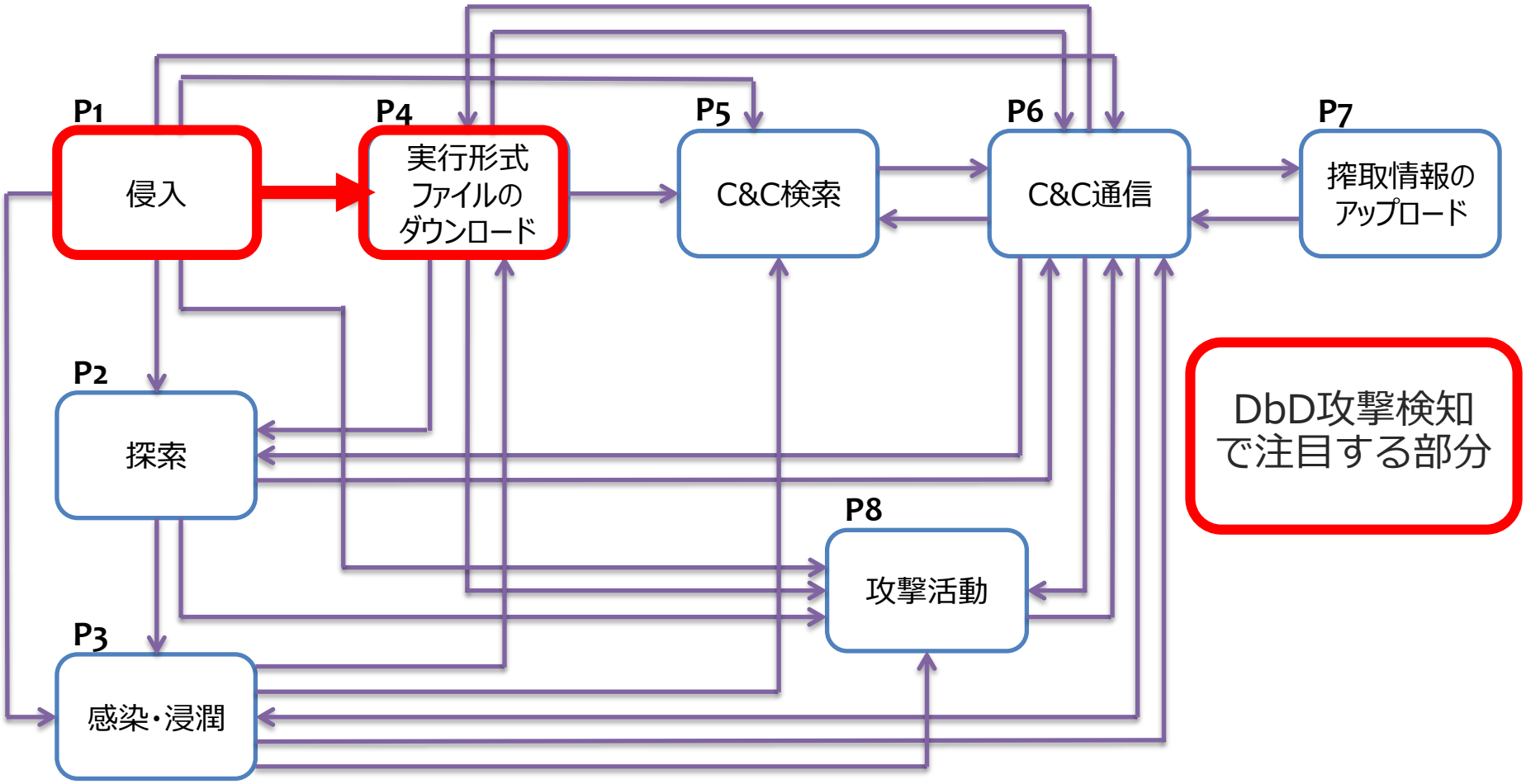


イーサネットタップやスイッチのミラーリング機能等を利用して、組織内の通信を直接モニタリング

- **セキュリティ製品のログからは得られない情報を分析**
- **リアルタイムに分析**

マルウェア活動遷移モデル

マルウェアの活動をネットワークトラフィックの観点で整理



DbD攻撃検知の流れ

1. 通信パターンの識別

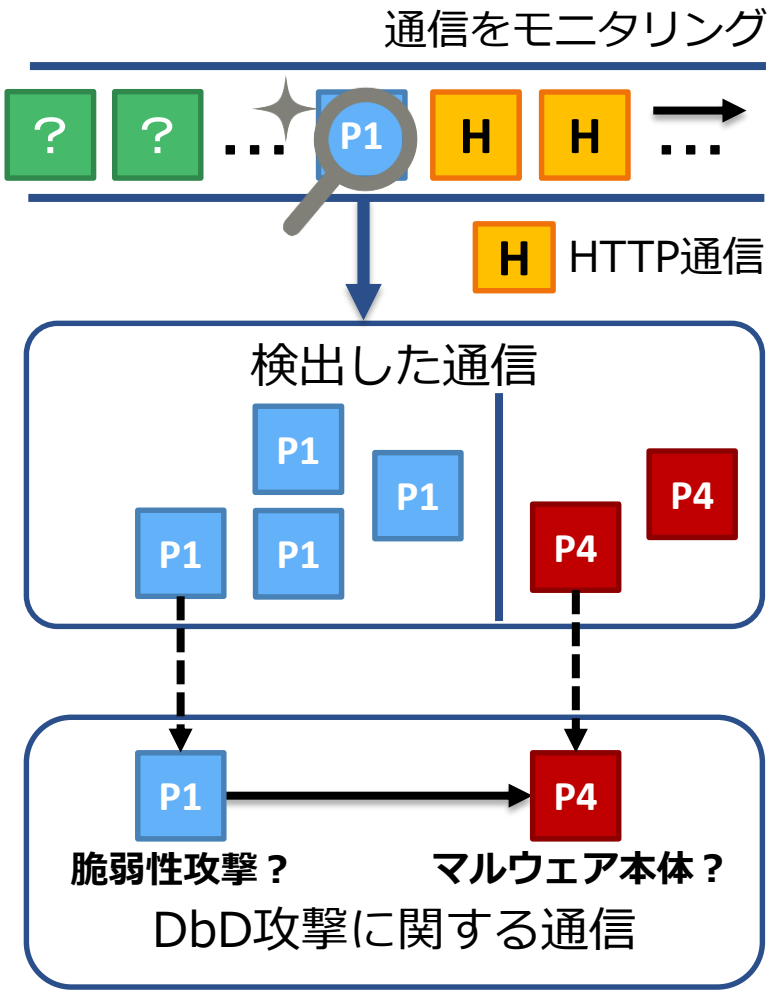
端末の通信内容を検査し、脆弱性攻撃やマルウェアのダウンロードを行った可能性がある通信を分類・収集

Phase1 (P1)
脆弱性が狙われる
アプリケーションに関わる通信

Phase4 (P4)
実行ファイルのダウンロード通信

2. 通信パターンの相関分析

あらかじめ定義した条件に基づいて、通信それぞれの相関を分析し、DbD攻撃が疑われる事象を抽出



検知手法（通信パターンの識別）

悪性コンテンツ候補侵入通信（Phase1）の識別

本検知手法では、下記いずれかのアプリケーションを対象としたデータであれば、**脆弱性を攻撃する通信であるかにかかわらず**、悪性コンテンツ候補のダウンロードであると識別

対象アプリケーション	ダウンロードデータの種類
Oracle Java Runtime	JAR, CLASS
Adobe Flash Player	SWF
Microsoft Silverlight	XAP
Adobe Reader	PDF
Microsoft Internet Explorer	HTML, JavaScript

脆弱性が狙われるアプリケーション

HTTPリクエストに含まれる**URI**や**特徴的なヘッダー**と、レスポンスに含まれる**コンテンツの識別子(マジックナンバー)**などを参照し、識別

PFU a Fujitsu company

悪性コンテンツ候補侵入通信（Phase1）の識別

例）Adobe Flash Player を対象とした通信の識別

いずれかの特徴を満たした場合、Phase1と識別

▼ HTTPリクエスト

```
GET /contents/main.swf HTTP/1.1

x-flash-version: 19.0…
```

SWFの拡張子

ブラウザに組み込まれた Adobe Flash Player がリクエストに付加するヘッダー

▼ HTTPレスポンス

```
HTTP/1.1 200 OK
Content-Length: 10000
Content-Type: application/x-shockwave-flash

CW……
```

Flashのmedia type

ボディ部に含まれるSWFのマジックナンバー

仮定

悪性コンテンツは脆弱性をもつ特定のアプリケーションによって解釈されるデータでなければならないため、**攻撃者の自由度は低く偽装が難しい**

PFU a Fujitsu company

実行ファイルダウンロード通信（Phase4）の識別

- **リクエストURI**やレスポンスの**Content-Typeヘッダーなど**が、表層的に解釈して実行ファイルであると考えられるもので、かつ**実行可能なサイズ**のコンテンツであるもの
- **実行ファイルのシグネチャ**に該当するコンテンツが含まれている

※攻撃成功後のDL通信では、ファイル拡張子やHTTPヘッダーは偽装が容易であるため、実際のコンテンツの中身を検査することが必要

※上記どちらかの条件に一致した場合、Phase4と識別

▼ HTTPリクエスト

```
GET /contents/mal.exe HTTP/1.1
Host: www.example.com
User-Agent: Mozilla/……
```

▼ HTTPレスポンス

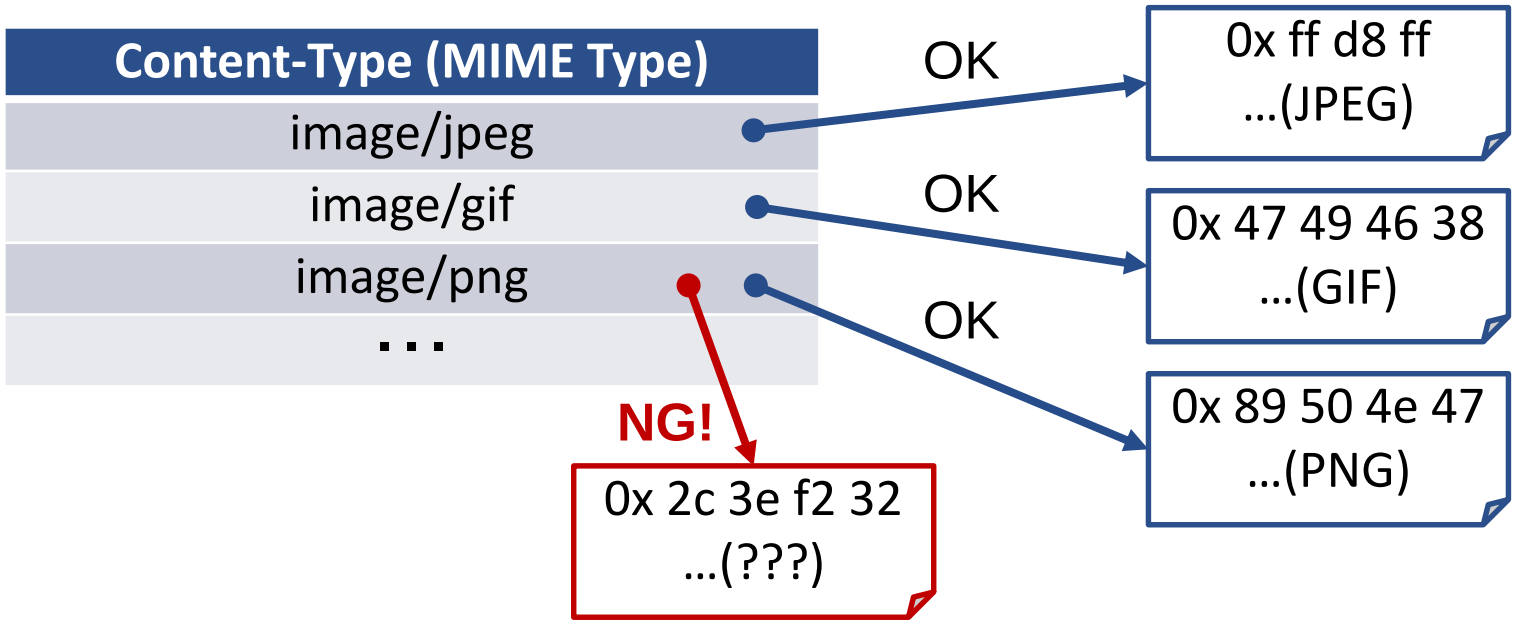
```
HTTP/1.1 200 OK
Content-Length: 10000
Content-Type: application/x-msdownload

MZ……
```

MZシグネチャおよびPEヘッダーを識別

検知手法（通信パターンの識別）

実行ファイルダウンロード通信（Phase4）の識別

Content-Typeヘッダーに示された情報から、ボディ部の整合性を検査。
整合性不一致の場合、怪しいコンテンツを実行ファイルのダウンロードの可能性がある通信とみなす



実行ファイルではないが、偽装が行なわれている状況から、
非常に怪しいコンテンツであると考え、Phase4として識別

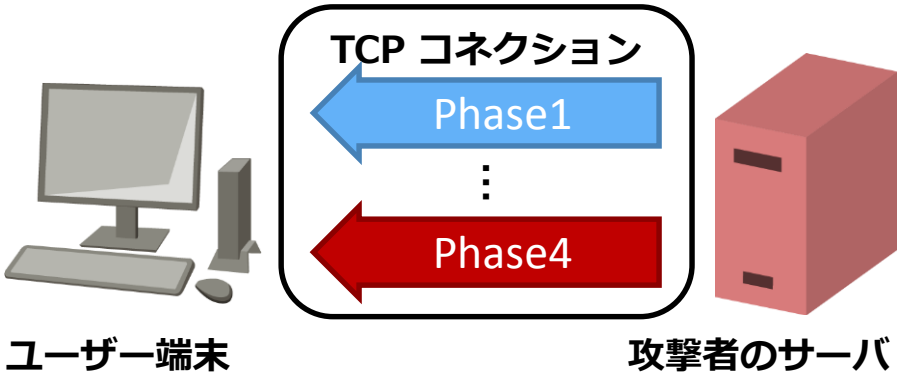
検知手法（通信パターンの相関分析）

相関分析条件

- 本検知手法ではコンテンツの内容が悪性かどうかを識別しないため、通信のふるまいから、**脆弱性を攻撃する「Phase1」**と**マルウェア本体をダウンロードする「Phase4」**を関連づけるための**相関条件（CA）**を定義
- 通常のDbD攻撃では、攻撃者のサーバに対して、**無駄なHTTP通信が行なわれない**と仮定し、以下**CA1~3**の3つの相関条件を設定

※CA = Correlation Analysis

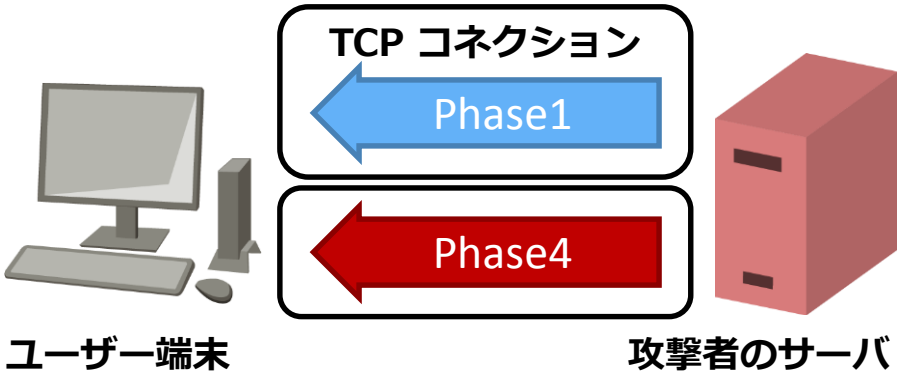
CA1の条件



同一のTCPコネクション上で、**Phase1**の後に**Phase4**を検出

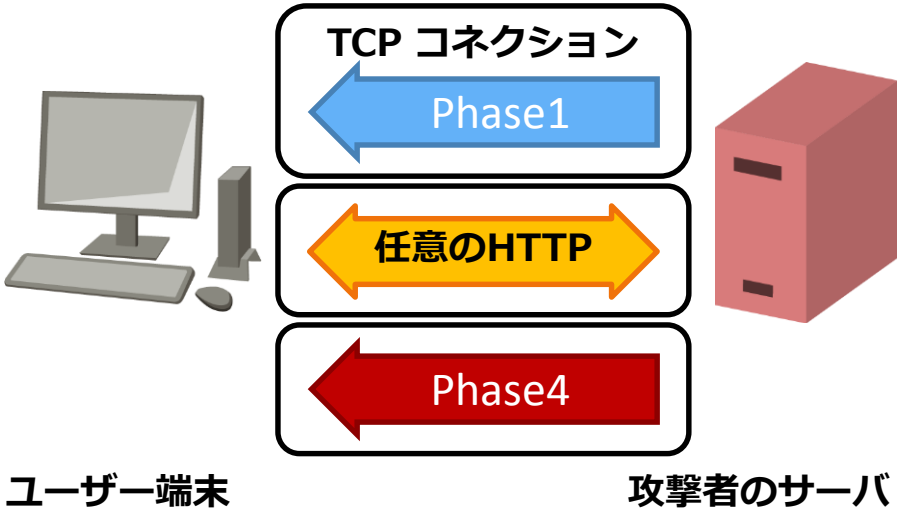
検知手法（通信パターンの相関分析）

CA2の条件



別々のTCPコネクションで、
Phase1と**Phase4**を**連続して**検出

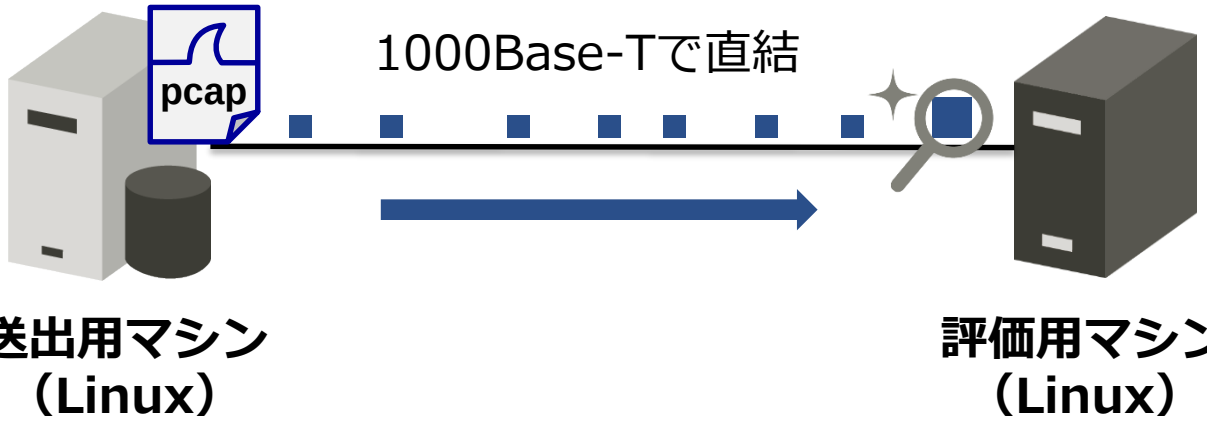
CA3の条件



別々のTCPコネクションで、
Phase1と**Phase4** を検出し、任意の正常なHTTP通信が**1つ**割り込み

評価方法

評価環境



tcpreplayコマンドを用いてpcapファイルを再生し、パケットデータを送出

プロミスキャスモードでパケットデータを取得し、本検知手法を実装したプログラムで解析

今回使用した評価データ

- **D3M Dataset 2015 (MWS)**
- **Threatglass (Barracuda)**
- **NCD in MWS Cup 2014 (MWS) ※誤検知の評価**

評価結果（D3M 2015）

評価データ

- D3Mには高対話型ハニークライアントが、URLブラックリストを巡回して得たDbD攻撃に関連するキャプチャデータが含まれている
- キャプチャファイルを巡回サイトごとに分割し、脆弱性攻撃が成立して**マルウェア本体のダウンロードが行なわれたサイト**に関連するキャプチャファイル（**11**個）をピックアップ

評価結果

	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

	検知数	割合(%)
CA1	1	11.1
CA2	8	88.9
CA3	0	0
合計	9	-

※()内はマルウェア検体のユニーク数

同一サイトへのアクセスに関する2件のDbD攻撃が、検知できなかった

評価結果（D3M 2015）

検知できたDbD攻撃通信について

実行ファイルのダウンロード通信では、Content-Typeヘッダーを
image/gifに**偽装**したものが見られた

▼ **HTTPリクエスト**

```
GET /est***tes/z***.gif HTTP/1.0
Accept: */*
Connection: Keep-Alive
User-Agent: Mozilla/4.0 (compatible; ***
Host: www.el***.es
```

※ *** :一部省略

▼ **HTTPレスポンス**

```
HTTP/1.1 200 OK
***
Content-Length: 78336
***
Content-Type: image/gif

MZ.. ...***!This program cannot be run in DOS mode.***PE***
```

URIやヘッダーの情報だけでは、
実行ファイルのダウンロード
であることには気づけない
→ **本手法の有効性**

評価結果（Threatglass）

評価データ

- Threatglass は攻撃方法の理解などを目的に、Barracuda Networks社によって公開されているデータセットである。キャプチャデータが入手可能
- 脆弱性攻撃が成立して**マルウェア本体のダウンロードが行なわれた**キャプチャファイル（**65**個）をピックアップ

※キャプチャに含まれるジャンボフレームは、tcpedit コマンドを利用し、標準的なMTU長（1500バイト）に分割

評価結果

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

	検知数	割合(%)
CA1	14	21.5
CA2	51	78.5
CA3	0	0
合計	65	-

Threatglassのデータでは100%検知することができた

評価結果（NCD in MWS Cup 2014）

PFU a Fujitsu company

評価データ

- NCDは昨年のMWS Cup開催期間中の通信をキャプチャしたもので、DbD攻撃に関する通信は含まれていないものとして評価
- 無加工で利用

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

評価結果

- DbD攻撃の検知は**なし**
- 誤検知（False-Positive）の評価としては、**時間が短く、まだ不十分**

PFU a Fujitsu company

まとめ

- DbD攻撃の特徴に着目した本検知手法によって、未知のトラフィックデータから**DbD攻撃を検知できる**ことを示した
- URIやHTTPヘッダーなど、隠蔽や偽装が可能な情報ではなく、**実際のコンテンツに着目する手法の有用性**が示せた
- **誤検知**に関するデータが少なく、**評価が不十分**

課題

ネットワークトラフィックを用いた我々の検知手法において

- 誤検知に関する十分な評価
- C&C通信フェーズ等のマルウェア活動遷移モデルの評価
- ネットワーク監視性能に関する評価