MWS2015意見交換会
「データセット活用のノウハウ共有発表」

D3Mデータセットを使った サイバー攻撃検知システム 「BotRadar」の研究開発/評価のコツ

(株)NTTデータ 情報セキュリティ推進室
NTTDATA-CERT
○大谷 尚通　益子 博貴　重田 真義

NTT DATA

もくじ

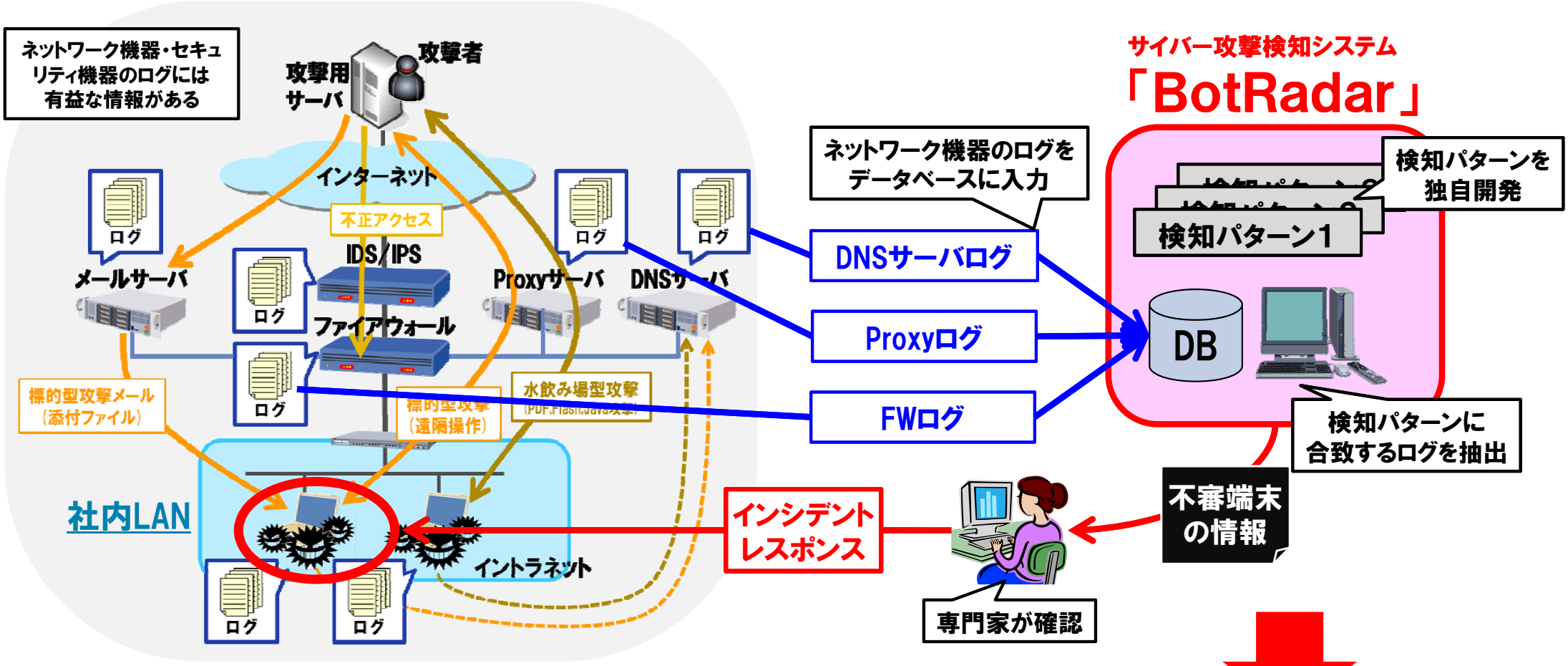
「データセット活用のノウハウ共有発表」の目的
- 基本的な分析方法/ツール
- 分析データの保存方法/形式 ○
- その他、分析のコツ/ノウハウ ○

1. サイバー攻撃検知システム「BotRadar(※)」について

(※) NTTDATA－CERT製 SIEM

1.1 BotRadarとは

設置済みのセキュリティ機器の通信ログを有効利用してサイバー攻撃を検知

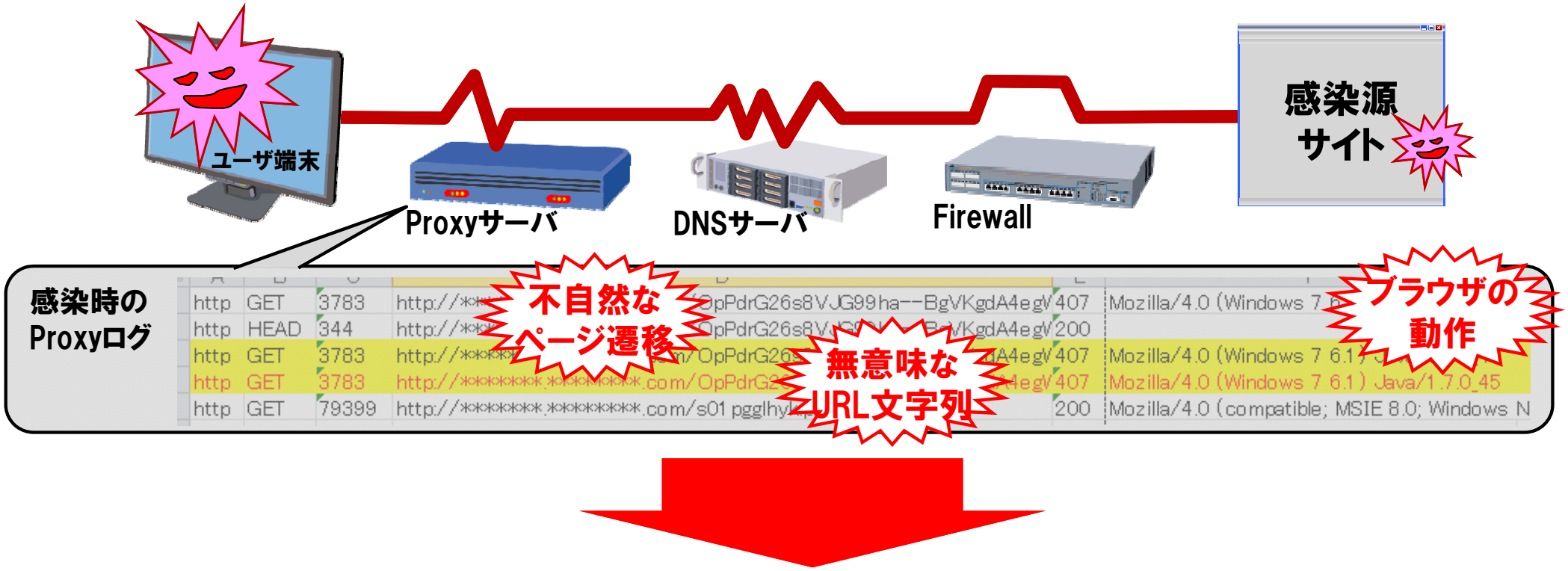


CSS/MWS2013、2014にて基本方式と
MWSデータセットを用いた検知結果を発表済み

サイバー攻撃を検知！

1.2 マルウェア検知のアーキテクチャ

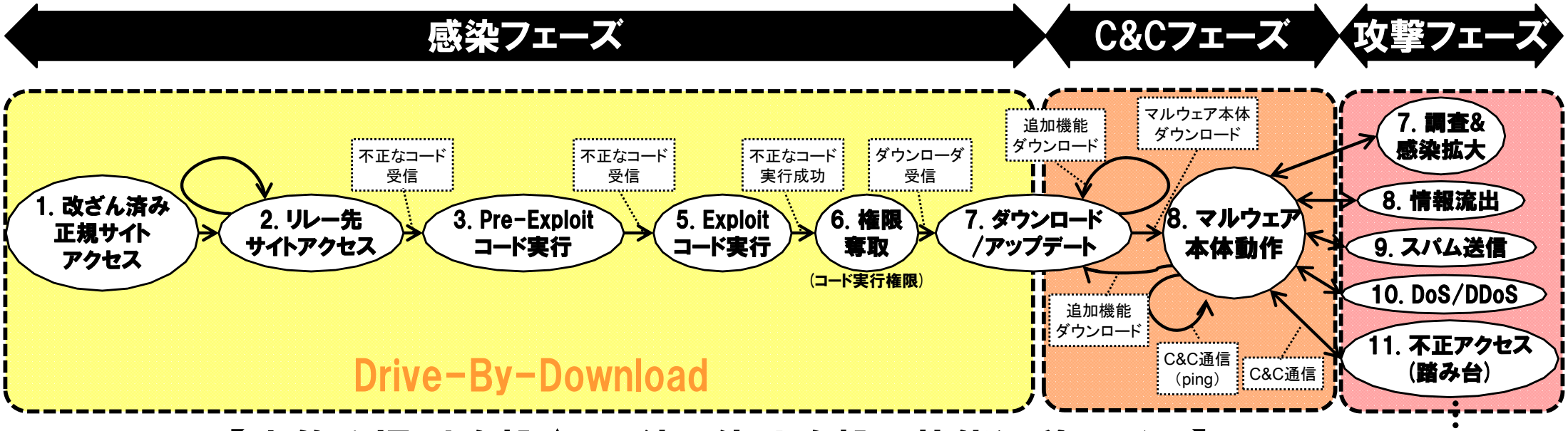
マルウェアの感染時/感染後は、正常な通信とは異なる特徴的な通信が発生



通信ログに残った特徴的な通信の痕跡をもとに
マルウェア感染している端末を検知する

1.3 サイバー攻撃の分析とモデル化

近年のサイバー攻撃は、攻撃動作が複雑化



【水飲み場型攻撃/Web待ち伏せ攻撃の状態遷移モデル】

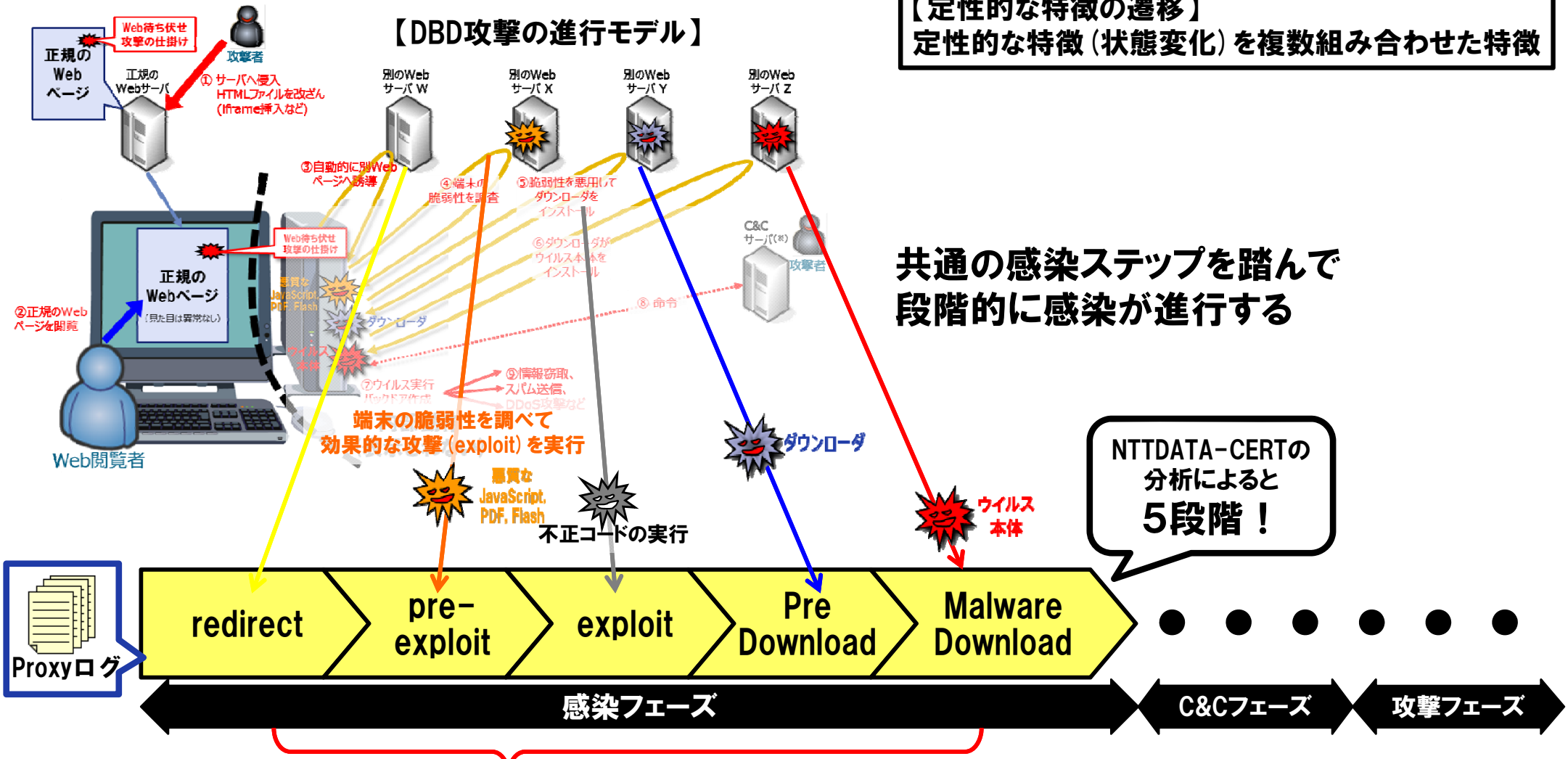
「複雑で変化の早いサイバー攻撃」の特徴を逆手に！

攻撃手法/動作をモデル化して検知方法を考案

1.4 DBD攻撃の特徴を用いた検知方式

DBD攻撃の感染フェーズにあらわれる「定性的な特徴の遷移」を用いて検知

【定性的な特徴の遷移】
定性的な特徴（状態変化）を複数組み合わせた特徴



共通の感染ステップを踏んで
段階的に感染が進行する

感染時のふるまいを捉える
汎用的なログ検知手法 **DBD攻撃検知方式**

2. D3Mを用いた検知率の評価結果

2.1 通信データ取得年別の検知率

D3M (Marionette) の通信データ 276個 に対して、DBD攻撃の検知パターン12個を実行して検知率を測定

【表1: 通信データ取得年別の検知率】

取得年	通信データ数	検知数	検知率
2011年	116	64	55.2%
2012年	110	94	85.5%
2013年	42	40	95.2%
2014年	8	0	0.0%
合計	276	198	71.7%

(88.2%)

(83.8%)

検知率 80%以上を達成

MWS2014データセットに対する検知率を評価し、D3M (Marionette) のDBD攻撃通信の**検知率 平均 71.7% / 83.8%** (直近3年) を達成

3. 分析・評価のコツ／ノウハウ

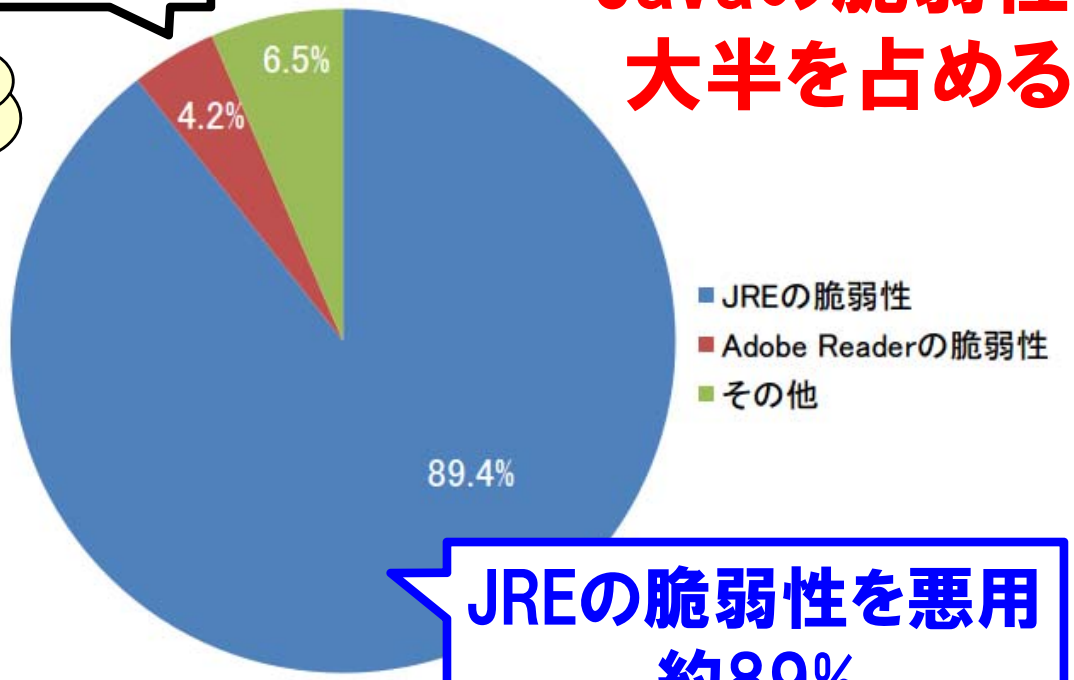
～困ったこと、苦労したこと、工夫点～

3.1 分析のコツ ～2013年～

2013年に悪用された脆弱性から感染手法の特徴を把握し、検知パターンの作成対象を決定

JRE以外
約11%

2013年上半期
JREの脆弱性を悪用
80.4%



JREの脆弱性を悪用
約89%

Javaの脆弱性が
大半を占める!!

Javaの脆弱性を悪用した
DBD攻撃/Exploit Kitの
情報を収集
↓
検知パターンを作成

検知率80.8%
(127/157件)

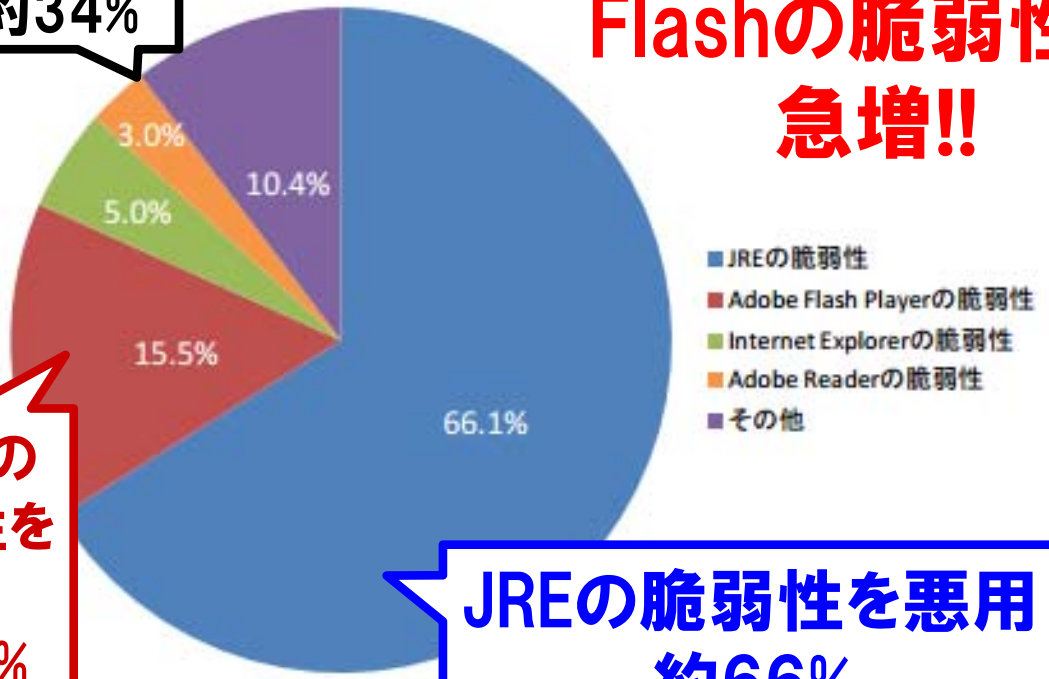
図: DBD攻撃で悪用されている脆弱性の割合
(Tokyo SOC調べ:2013年7月1日～2013年2月31日)

出典: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

3.2 分析のコツ ～2014年～

2014年に悪用された脆弱性から感染手法の特徴を把握し、検知パターンの作成対象を決定

JRE以外
約34%



Flashの
脆弱性を
悪用
約16%

JREの脆弱性を悪用
約66%

Flashの脆弱性が
急増!!

Flashの脆弱性を悪用した
DBD攻撃/Exploit Kitの
情報を収集
↓
検知パターンを作成

検知率88.2%
(134/152件)

2015年は
どんな傾向？

図：DBD攻撃で悪用されている脆弱性の割合（日本国内）
（Tokyo SOC調べ：2014年1月1日～2014年6月30日,検知総件数1,409件）

出典：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

3.3 評価データの工夫① ～選択～

NTT DATA

D3Mデータセットで自システムの検知率を評価するために

■ BotRadarは、ネットワーク機器やサービス、OSなどのログ（おもにProxyログ）を分析する。

マルウェアの通信データ（DBD攻撃通信）が含まれた
D3Mデータセット/Drive-by Download Data by Marionette を選択

【D3M通信データ】

① D3M（Marionette）の通信データ＝DBD攻撃通信（PCAP形式）
Webクライアント型ハニーポット（Marionette）が悪性URLを巡回して取得

② **D3M（Botnet Watcher）の通信データ＝C&C通信**（PCAP形式）
Marionetteが取得したマルウェアをマルウェアサンドボックス（Botnet Watcher）上で実行して取得

3.4 評価データの工夫② ～加工～

NTT DATA

D3Mデータセットで自システムの検知率を評価するために

- BotRadarは、ネットワーク機器やサービス、OSなどのログを分析する

- D3Mデータセットの通信データ（PCAP）は、
  そのままではBotRadarが取り扱えない！

おもに
Proxyログを
使用

PCAPデータからHTTP通信を抽出して、Proxyログ形式へ変換
（tsharkと自家製変換ツール@Rubyを組み合わせ）

3.5 評価データの工夫③ ～フィルタ～

NTT DATA

検知率を正しく評価するために

- BotRadarは、DBD攻撃通信（感染フェーズ）の特徴的な振る舞いを使って検知する
- D3Mデータセットには、DBDのふるまいが途中で止まっているデータが含まれる。BotRadarは検知できない/しない

DBDが途中で停止
⇒感染に失敗！
＝検知不要！

DBD攻撃（感染フェーズ）が進行した通信データのみを抽出し、
評価データへ採用（通信データ数＝276個）

データセット内から
目視/手動で
有効なデータを抽出

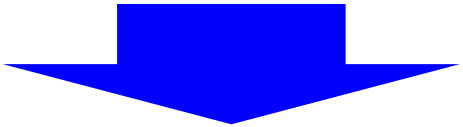
3.6 評価データの工夫④ ～評価方法～

NTT DATA

検知率を正しく評価するために

■ D3Mデータセットを使って検知パターンを作成すると
検知率を正しく評価できない

公知な情報や独自に収集した検体/ログから検知パターンを作成
（日々、最新の情報を入手して検知パターンを追加）



【問題】
新しい検知パターンは、D3Mデータセット2014から何も検知しなかった。
D3Mデータセット2014には、該当するマルウェア/Exploit Kitの通信が含まれていなかった。
CSS/MWS2014の発表では、新しい検知パターンの検知率は評価できず！

3.6 評価データの工夫⑤ ～評価方法～

NTT DATA

誤検知率 (False Positive) を評価する

■ 誤検知率も評価しなけば、実用性を示せない

実運用中のProxyログを用いて誤検知率を算出

【表: 2014年9月 (30日間) の誤検知】

#	検知パターン名	誤検知数	誤検知率
1	No.22	24	0.00152%
2	No.76	3	0.00019%
3	No.82	2	0.00013%
4	No.84	4	0.00025%
5	No.91	63	0.00400%
6	No.92	27	0.00171%
7	No.93	1	0.00006%
8	No.100	53	0.00336%
9	No.106	99	0.00628%
10	No.107	1	0.00006%
合計		277	0.00736%

2014年9月の平均アクセスFQDN数＝157万5185個/月

CSS/MWS2014 発表データ

2014年9月 (30日間) 平均
誤検知率 (FP) ＝0.0074%

平均アクセスFQDN数 ＝ 5万2506個/日
平均誤検知数 ＝ 9.2個/日

誤検知数が日々の運用で対応可能な範囲であることを示した！

3.7 分析・評価のコツ/ノウハウのまとめ

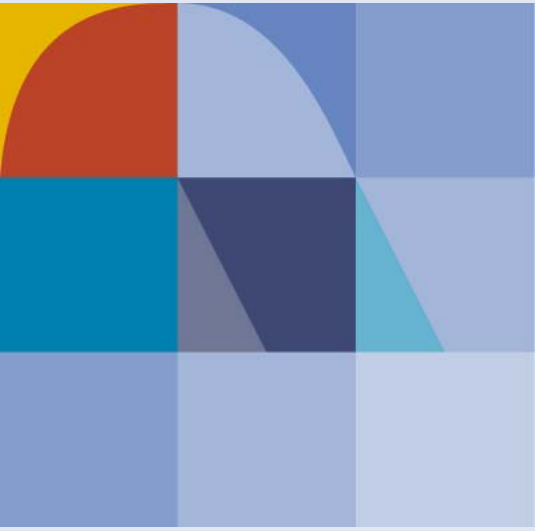
NTT DATA

企業がマルウェア対策の研究開発を実効的にすすめるために

1. DBD攻撃で悪用されている脆弱性の割合など、
   最新の攻撃状況から研究開発の方針を決定

2. 最新の検体、感染ログを収集・分析し、検知パターンを開発

3. 検知率/誤検知率(FP/FN)を適切に評価する
   - 各データセットの特性を知る。適切なデータセットを選ぶ
   - データセットから検知対象データを抽出
   - 誤検知数(FP)から運用性を評価



Global IT Innovator

NTT DATA Group

NTT DATA