1A3-4: MWS ドライブ・バイ・ダウンロード

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

2015年10月21日

株式会社NTTデータ
○益子 博貴，重田 真義，大谷 尚通

NTT DATA

INDEX

1. Drive-by Download 攻撃の定性的特徴とその変化

1.1 DbD攻撃のステップ

NTT DATA

一般に、Drive-by Download 攻撃（以下、DbD攻撃）は段階を踏んで進行する

No	ステップ	URL	User Agent
1	改ざん元サイト	http://holiday***line.com/	Mozilla/5.0 (compatible; MSIE 10.0; ...
2	Redirectステップ	http://www.com***traer.cl/clik.php?id=6985669	
3	pre-Exploitステップ	http://h***j.c***doctor.pw/.../a8e***764d.html	
4	Exploitステップ	http://h***j.c***doctor.pw/3487***0/1390***0.jar	
5	pre-DLステップ	http://h***j.c***doctor.pw/f/1390***0/3487***0/2	
6	Malware-DLステップ	http://receive***t.cc/man.php	

攻撃サイトへ誘導

脆弱性の有無を調査

脆弱性を悪用

Dropper の DL・実行

マルウェア本体の DL・実行

DbD攻撃の段階として5つのステップを定義[1]

[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

1.2 pre-Exploitステップ～Exploitステップの特徴

NTT DATA

■ pre-Exploit ステップ～Exploit ステップ

脆弱性を悪用するため、ユーザ端末上のソフトウェアが起動される

→ ソフトウェアの起動に伴い UserAgent などが変化する

No	ステップ	URL	User Agent
1	改ざん元サイト	h	; MSIE 10.0; ...
2	Redirect ステップ	h	; MSIE 10.0; ...
3	pre-Exploit ステップ	http://h***j.c***doctor.pw/.../a8e***764**l.html**	**Mozilla/5.0 (compatible; MSIE 10.0** ...
4	Exploit ステップ	http://h***j.c***doctor.pw/34 .0/1390***0**.jar**	**Mozilla/4.0 ... Java** 1.7
5	pre-DL ステップ	http:// 3487***0/2	Java/
6	Malware-DL ステップ	http://receive***t.cc/man.php	

JRE の脆弱性を悪用した攻撃
→ JREが起動される

Suffixが変化！

User Agentが変化！

1.3 DbD攻撃の定性的特徴

NTT DATA

UserAgent などの変化 → DbD攻撃の「定性的特徴」と呼称

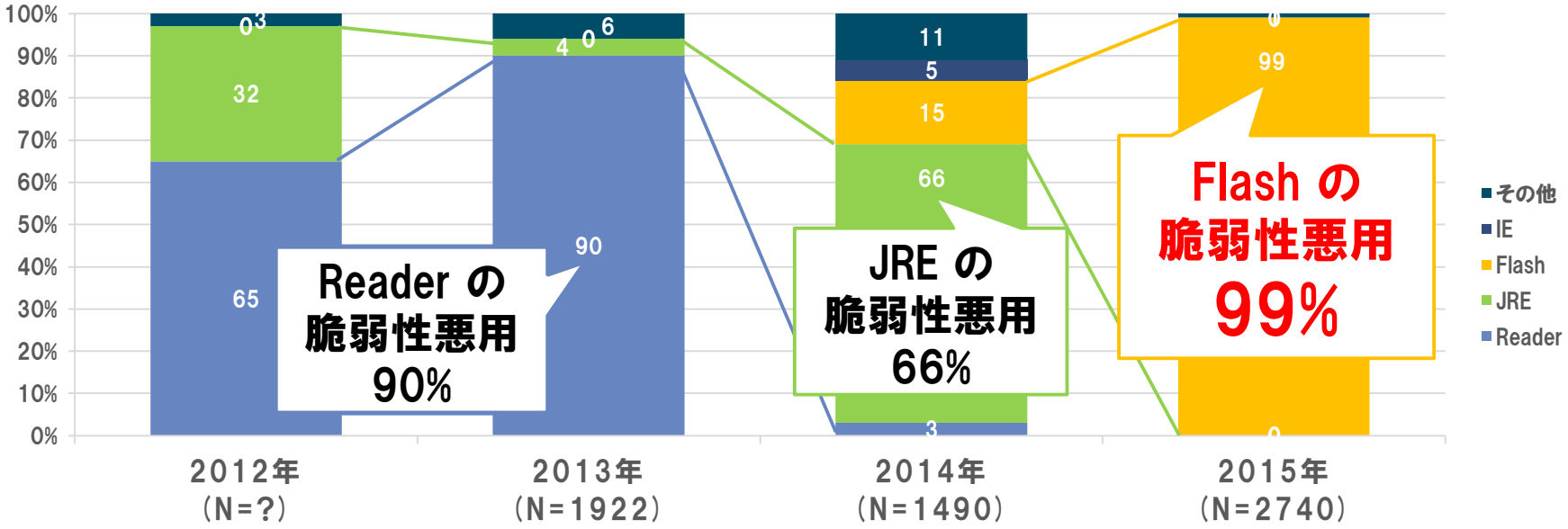
No	ステップ	URL	User-Agent
1	改ざんサイト		); ...
2	Redirec ステップ		); ...
3	pre-Exploit ステップ	http://h***j.c***doctor.pw/.../a8e***764 l.html	Mozilla/5.0 (compatible; MSIE 10.0 ...
4	Exploit ステップ	http://h***j.c***doctor.pw/3487***0/1390***0.jar	Mozilla/4.0 ... Java 1.7.0_15
5	pre-DL ステップ	http://h***j.c***doctor.pw/f/1390***0/3487***0/2	Mozilla/4.0 ... Java/1.7.0_15
6	Malware-DL ステップ	http://receive***t.cc/man.php	Mozilla/4.0

定性的特徴は脆弱性を悪用するソフトウェアの起動等によって生じるため
長期間みられる特徴

定性的特徴を用いて
サイバー攻撃を検知するシステムを開発

1.4 Exploit Kitの攻撃対象の変化

最近の Exploit Kit は Flash の脆弱性を悪用するように変化



【　図: DbD 攻撃で悪用された脆弱性の割合（IBM Tokyo SOC レポートより）】[2] 巻末に記載

Exploit Kit の挙動の変化に伴い、本システムで用いていた定性的特徴も変化

→ 検知漏れの恐れが高まる

システムの性能維持を目指し、2点の改良を実施

1.5 課題と対応

【課題】Exploit Kit の挙動の変化に伴い、定性的特徴が変化
→ 検知漏れが発生する恐れ

システムの性能維持のために改良を実施

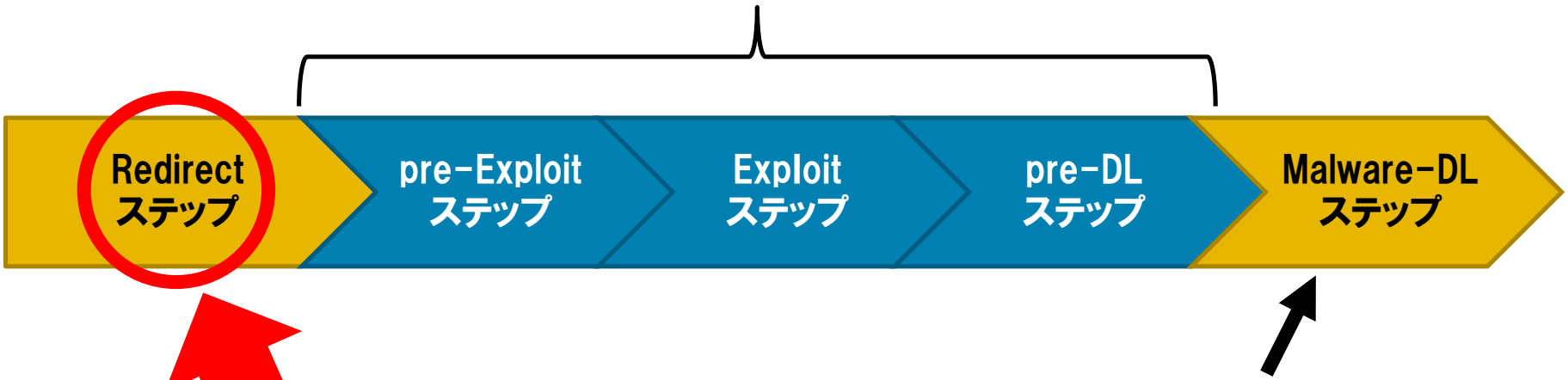
対応	説明箇所
(対応1) Exploit Kitの新しい挙動に対応する検知パターンの開発	3章で説明
(対応2) Exploit Kitの挙動に依存しない検知パターンの開発	2章で説明

主に(対応2)について発表

2. Exploit Kit の挙動に依存しない検知パターンの開発

2.1 開発方法の検討

Exploit Kit の特徴は
pre-Exploit ステップから pre-DL ステップに現れやすい
→ 現システムの主な検知範囲



Malware-DLステップは危険なマルウェアが実行される段階
安全確保のために、より早い段階で検知したい

Redirect ステップに
Exploit Kit に依存しない特徴がある可能性

→ 攻撃ログを収集・分析

2.2 Redirect ステップ分析の例

悪用されたWebサイトのアドオン、エクスプロイトキット「FlashPack」に誘導。約87%が日本のユーザに影響

投稿日: 2014年8月26日
脅威カテゴリ: 不正プログラム, サイバー犯罪, 脆弱性, Webからの脅威
執筆: Fraud Researcher - Joseph C Chen

2014年7月後半以降、「FlashPack」として知られるエクスプロイトキットを利用した攻撃が、日本のユーザに被害を与えていることが確認されています。問題のエクスプロイトキットは、感染活動にスパムメールやWebサイトの改ざんを利用しません。今回の攻撃に利用されたのは、改ざんされたWebサイト用のアドオンでした。

このWebサイト用アドオンは、Webサイトの所有者が、ソーシャルメディアの共有ボタンをWebサイトに追加したい場合に使用します。このアドオンを使用するために所有者がしなければならないことは、Webサイトのデザインテンプレートに JavaScript のコードを複数行追加するだけです。このコードは、問題のアドオンを提供するWebサイトから自由に取得することができます。

追加されたスクリプトにより、以下のような共有ボタンがWebサイトに上書きされます。

図1：追加された共有ボタン

【図：TrendMicro社のブログに掲載された記事】[3]

昨年（2014年）8月にTrendMicro社が報告したブログパーツの改ざん

多数のブログで使用されているブログパーツが悪用され FlashPack Exploit Kit に誘導される

[3] Walter Liu, 臼本 将貴, “Exploit Kit「FlashPack」に誘導Webサイトのアドオン”, http://blog.trendmicro.co.jp/archives/9715

2.3 ブログパーツとは

ブログパーツとは…
自分のブログから、パーツ提供者の提供するJavaScriptをリンクすることで、ブログに装飾などを施すことができるもの

2.4 ブログパーツ改ざんとは

パーツ提供者のサーバで改ざんが発生
→ パーツを利用する全てのブログで、FlashPack EKへの誘導が発生

2.5 ブログパーツ改ざんにおけるログの特徴

NTT DATA

Proxy ログ上には、FlashPack への誘導が以下のように記録される

ブログパーツからFlashPackに誘導される様子	
正規ブログ	http://blog.l**r.jp/l**1/archives/3**5.html
パーツ	http://c**w.net/s.js
Redirect	http://r**7.a**l.net/index.php?o={base64}
Redirect	http://r**4.a**l.net/index2.php
pre-Exploit	http://r**7.a**l.net/c**r/index.php

Flash Pack

FlashPack に誘導される直前に
不審なサーバへの Redirect が発生

2.6 誘導先の変化

NTT DATA

昨年9月以降、誘導先が RIG Exploit Kit に変化

～2014年8月以前ログ

正規ブログ	http://blog.l**r.jp/l**1/archives/3**5.html
パーツ	http://c**w.net/s.js
Redirect	http://r**7.a**l.net/index.php?o= {base64}
Redirect	http://r**4.a**l.net/index2.php
pre-Exploit	http://r**7.a**l.net/c**r/index.php

2014年9月～以降のログ

正規ブログ	http://a**o.jp/i**e/entry-1**7.html
パーツ	http://c**w.net/social.js
Redirect	http://y**f.m**t.org/index.php?q= {base64}
Redirect	http://y**b.m**t.org/index2.php
pre-Exploit	http://o**r.g**p.com/?PHPSSESID= {base64}

Redirect 特徴は 共通

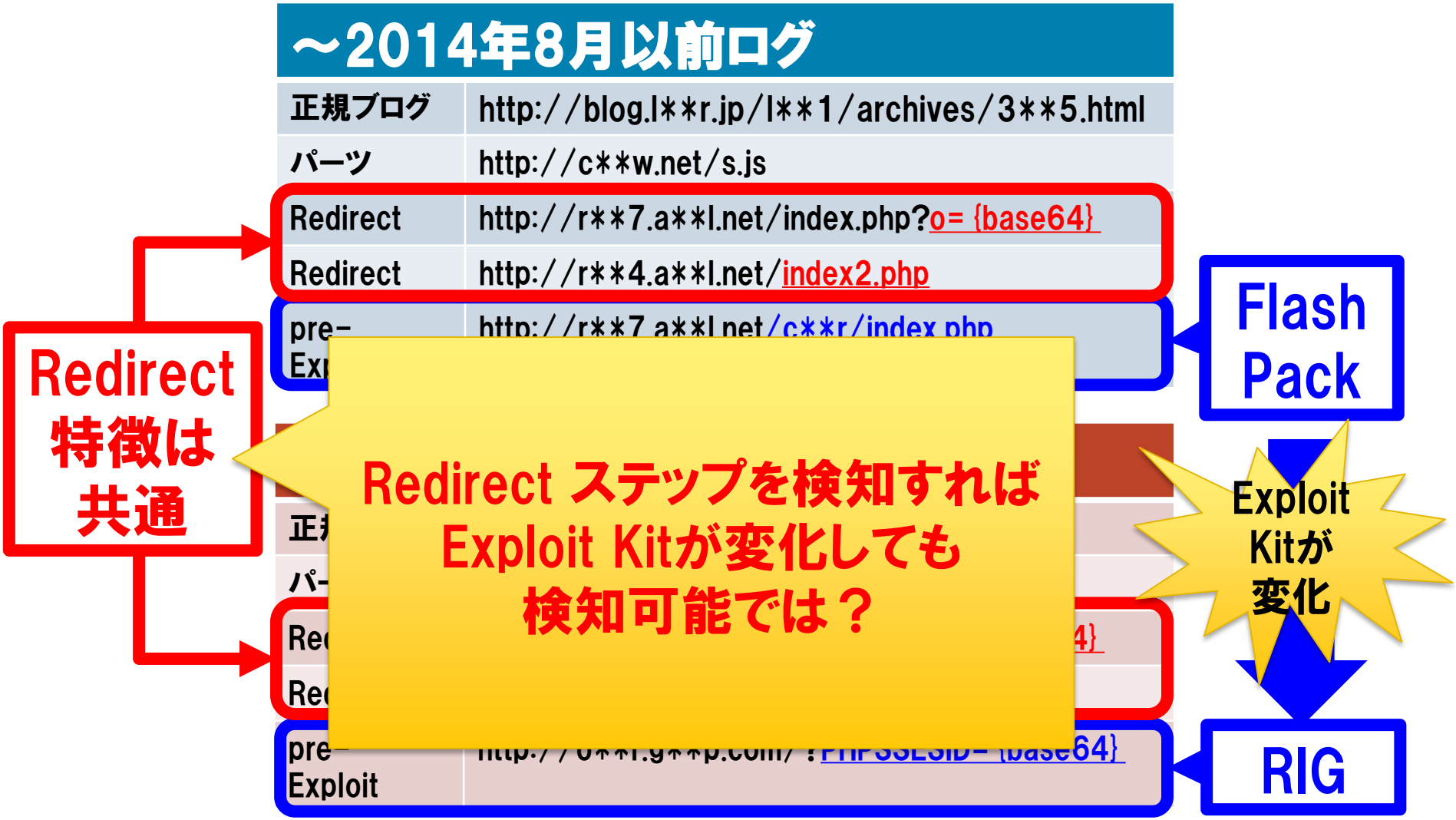
Flash Pack

Exploit Kitが 変化

RIG

2.6 誘導先の変化

昨年9月以降、誘導先が RIG Exploit Kit に変化



2.7 Redirect ステップの検知パターン化

NTT DATA

Redirect ステップは特徴が現れにくく、検知が難しい

文字列が動的に変化するため、パターン化できない

ブログパーツ改ざんにおける Redirect ステップ

http://r**7.a**l.net/index.php?**o= {base64}**

http://r**4.a**l.net/index2.php

一般的な名称であり、検知に使用できない

{base64} をデコードすると
改ざんされたサイトの情報や、アクセス日時などが出現

➡ **Redirectステップではアクセス解析を行うと推測**

{base64} 部に含まれる情報の量は今後も変化しにくいと仮定し
文字列の長さなどをもとに検知パターンを開発

2.8 開発した Redirect 検知パターン

NTT DATA

本発表で紹介した事例を含め
Redirect ステップに特徴の見られた計5つの攻撃について
5つの検知パターン(Redirect 検知パターン)を開発

本発表で紹介

1. ブログパーツを提供するサーバを改ざんし
   攻撃サイトへのリダイレクトを発生させるDbD攻撃
2. Movable Typeの脆弱性を突いてページを改ざんし
   リダイレクトを発生させるDbD攻撃
3. 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を発生させるDbD攻撃
4. 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
5. 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DbD攻撃

3. Exploit Kit の新しい挙動に対応する検知パターンの開発

3. 新しい定性的特徴を捉える検知パターンの開発

NTT DATA

2章で Redirect 検知パターンを新規開発

現システムの検知範囲 →改良を実施

Exploit Kit の**新しい定性的特徴を用いて**
検知パターン (Exploit 検知パターン) を4つ開発、3つ改良

A) 検知パターンを新規に開発したExploit Kit
→ RIG, Fiesta, Angler, FlashPack

B) 既存の検知パターンを改良したExploit Kit
→ Nuclear, Neutrino, Magnitude

4. 評価

4.1 課題と改良点のまとめ

NTT DATA

【課題】Exploit Kit の挙動の変化に伴い、定性的特徴が変化
→ 検知漏れが発生する恐れ

システムの性能維持のために改良を実施

対応	改良点
(1) Exploit Kitの新しい挙動に対応する検知パターンの開発	Exploit検知パターン7つを開発・改良
(2) Exploit Kitの挙動に依存しない検知パターンの開発	Redirect検知パターン5つを開発

4.2 改良点と評価領域

NTT DATA

■ Exploit 検知パターン、Redirect 検知パターンそれぞれについて
検知性能と**誤検知数**を評価

■ 評価には3つのデータを使用

①D3Mデータセット ←―― Redirect ステップが含まれていなかった
②運用環境のデータ
③独自データセット

【表　評価領域と使用データの関係】

	検知性能評価	誤検知数評価
Exploit 検知パターン	①D3Mデータセット を使用	②運用環境のデータ を使用
Redirect 検知パターン	③独自データセット を使用	

4.3 ①D3Mデータセットを用いた評価

NTT DATA

■評価方法

- 期間　:2011年4月～2015年2月
- データ:Marionette によって収集された DbD 攻撃時の通信ログ
- 対象　:Exploit 検知パターンの検知性能
- 手法　:pcap を proxy ログに変換後、対象外のログを除外※

※段階を踏んで進行する DbD 攻撃ログのみを使用、Exploit コードを直接DLするログなどは除外

■結果

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%

検知率は
昨年(71.7%)[4]並を
維持

未知の定性的特徴が現れるケースを確認

→ 検知パターンの改良が必要

[4] 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

4.4 ②運用環境のデータを用いた評価

NTT DATA

■評価方法

- 期間　：2015年6月1日～6月30日
- データ：運用環境で分析したログ（約5億4,915万行）
- 対象　：Redirect / Exploit 検知パターンの誤検知数
- 手法　：誤検知したログの行数を集計、割合を算出

$$\text{誤検知率}(\%) = \frac{\text{誤検知したログの行数（延べ）}}{\text{全ログの行数}} \times 100$$

■結果

	誤検知数(行)	誤検知率(%)	パターン数	パターンあたりの誤検知数(行)
Redirect検知パターン	16	0.00000291	5	3.2
Exploit検知パターン	993	0.000180	16	62.0

Redirect検知パターンは**誤検知が少ない**

Exploit 検知パターンの誤検知率
昨年（0.000482%）より低減

4.5 ③独自データセットを用いた評価 - 手法

NTT DATA

D3M では Redirect ステップが含まれていない

→ 独自にデータセットを作成し Redirect 検知パターンを評価

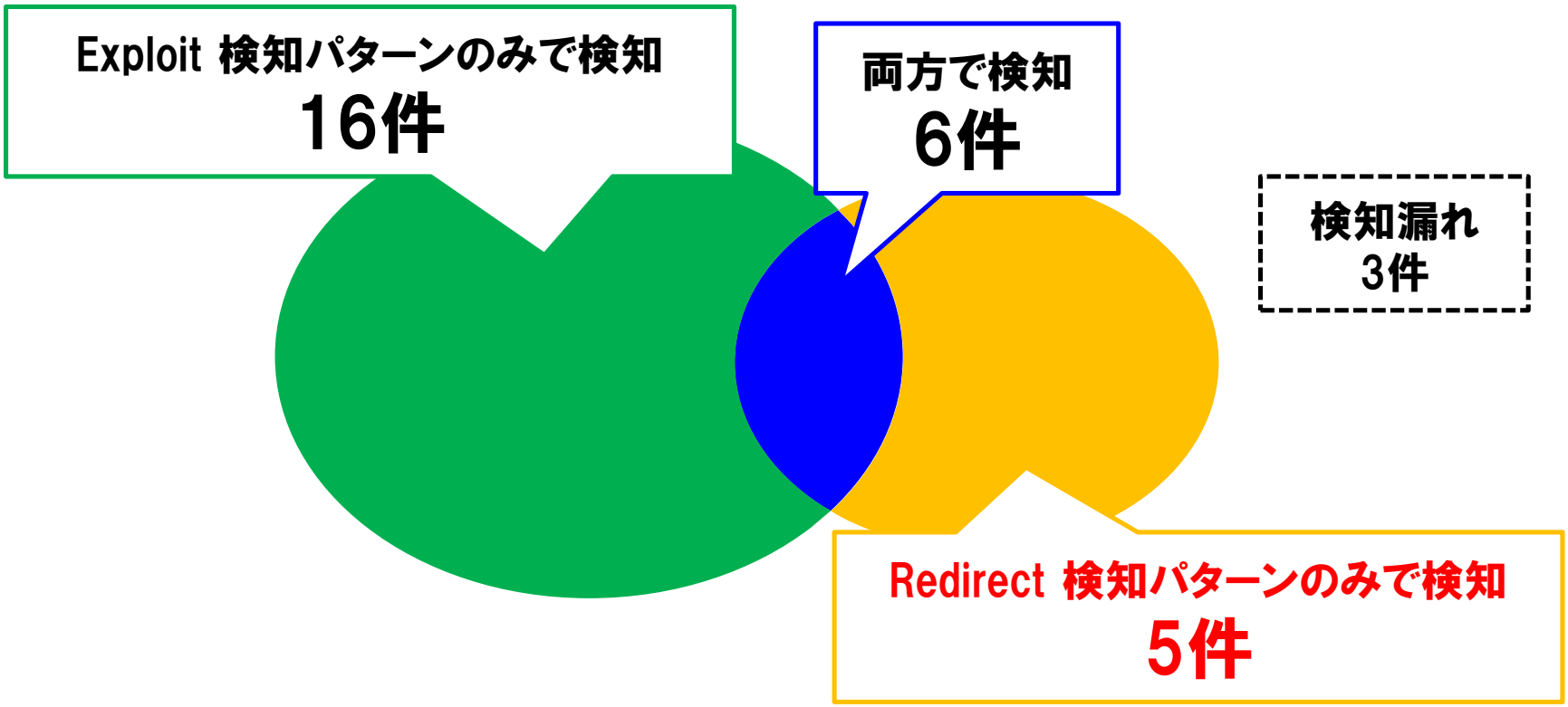
■評価方法

- 期間　:2015年4月～2015年8月
- データ:外部情報源等から収集したDbD攻撃ログ
  全30件
- 対象　:Redirect 検知パターンの検知性能
- 手法　:検知パターンの種類ごとに検知数を集計
  カバレッジを分析

4.6 ③独自データセットを用いた評価 – 分析

NTT DATA

■ 検知パターンの種類ごとの検知数



Exploit 検知パターンで未対応の攻撃を Redirect 検知パターンで検知

カバレッジ向上に寄与した

5. まとめ・今後の課題

5.1 まとめ

NTT DATA

【課題】Exploit Kit の挙動の変化に伴い、検知漏れが発生する恐れ
→ システムの性能維持するために改良を実施

【表　評価領域と評価結果】

対応		検知性能評価	誤検知数評価
(1) Exploit Kitの新しい挙動に対応する検知パターンの開発	Exploit 検知パターンの開発と改良	昨年並の検知率を維持	昨年より低減
(2) Exploit Kitの挙動に依存しない検知パターンの開発	Redirect 検知パターンの開発	カバレッジが向上できることを確認	誤検知が少ないことを確認

カバレッジの向上と、誤検知の低減を実現
システムの性能を維持することができた

5.2 今後の課題

NTT DATA

■ 課題

- Internet Explorerの脆弱性を悪用する攻撃について
  未知の定性的特徴を確認した
  - →検知パターンの改良が必要

- 現在の Redirect 検知パターンは、文字列の特徴に強く依存しており、特定の攻撃のみ検知できる
  - 汎用化に向けて改良が必要

- Malware-DLステップの検知パターン開発は未着手
  - Exploit Kit に依存しないと予想され、
    カバレッジ向上が見込まれる
  - 検知パターンの開発が可能か検討

参考文献

[2] 図「DbD 攻撃で悪用された脆弱性の割合」の作成にあたり使用した文献

- 2012年上半期 Tokyo SOC 情報分析レポート,
  https://www-935.ibm.com/services/jp/its/pdf/tokyo_soc_report2012_h1.pdf

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

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

- 2015年上半期 Tokyo SOC 情報分析レポート,
  https://www-304.ibm.com/connections/blogs/tokyo-soc/resource/PDF/tokyo_soc_report2015_h1.pdf

NTT DATA

Global IT Innovator