RIG Exploit Kitにおける攻撃傾向の調査

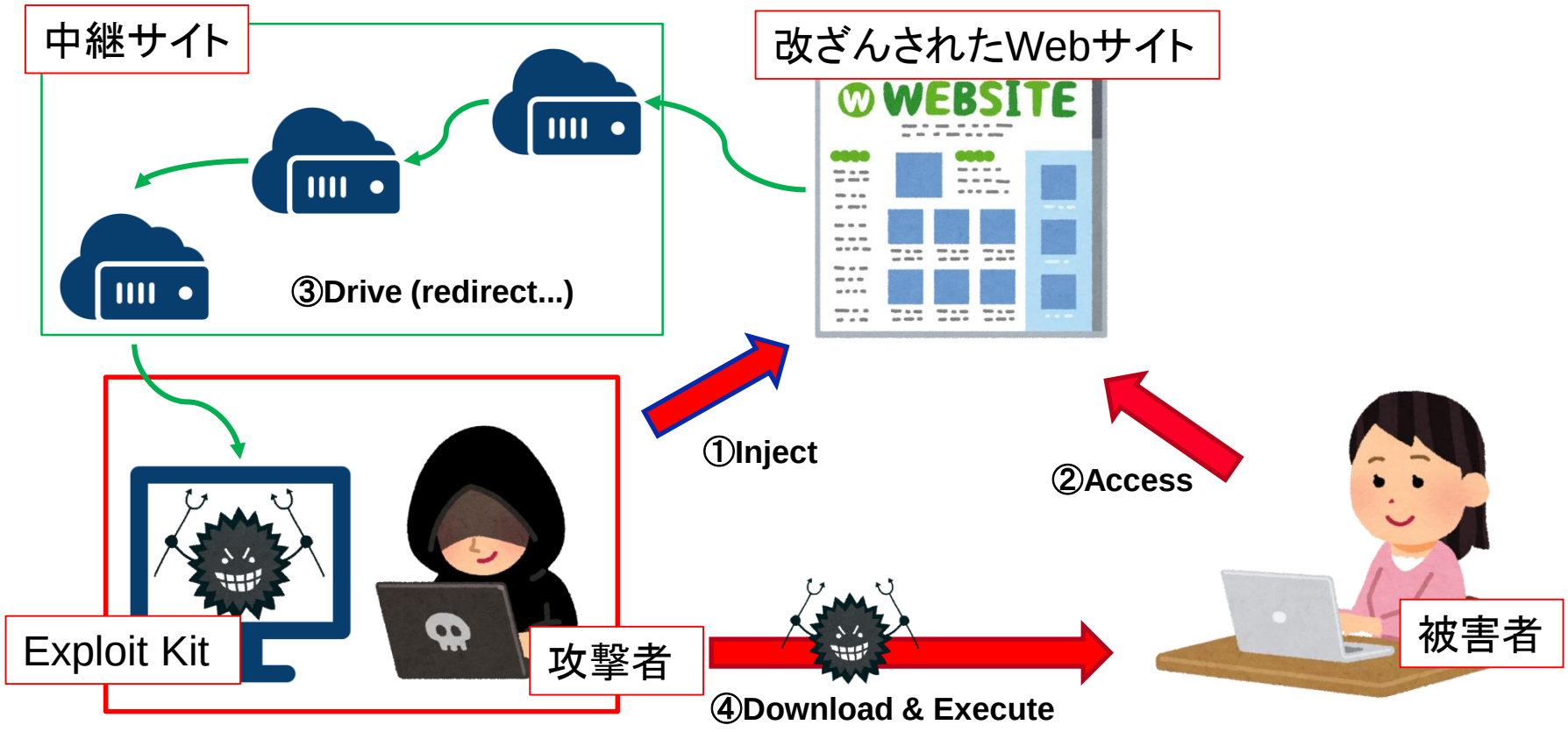
山田道洋[1]　小池倫太郎[2]　菊池浩明[2]　黄緒平[3]

1:明治大学大学院
2:明治大学
3:明治大学　研究・知財先着機構

背景：Drive-by Download攻撃

- 悪性Webサイトへ誘導された脆弱なWebブラウザに対して，そのWebブラウザの脆弱性を突くようなコードを送り込んで制御を奪い，マルウェアをダウンロード・実行させる
- 攻撃のパターン
  - メールやSNSを使って攻撃者の用意したサーバへ誘導する
    - » 最近はあまり見ない
  - 攻撃者は一般のWebサイトを改ざんし，そこへアクセスしたユーザを攻撃者が用意した攻撃サーバへ誘導する
    - » 従来の手法
  - 攻撃者は悪性Web広告を配信し，その広告を表示したWebサイトへアクセスしたユーザを攻撃者が用意した攻撃サーバへ誘導する
    - » Malvertisingと呼ばれ，最近の主流

Drive-by Download攻撃の構成図



Exploit Kit

	従来	EK as Service
攻撃キット	ソースを購入	サブスクリプション方式
設置場所	各攻撃者	運営者
例	Mpack Blackhole	RIG Astrum

- Exploit Kitの例
  - MPack
  - Phenix Exploit Kit
  - Blackhole Exploit Kit
  - Nuclear Exploit Kit
  - Angler Exploit Kit
  - Neutrino Exploit Kit
  - **RIG Exploit Kit**
  - Magnitude Exploit Kit
  - Sundown Exploit Kit
  - Astrum Exploit Kit

攻撃キャンペーン

- キャンペーン：Exploit Kitを使う一連の攻撃の特徴的なパターン

入口サイト	キャンペーン
Compromised サイト	pseudo-Darkleech
	EITest
	Good Man
	Fake Chrome Popup
	DecimalIP
Malvertising	Seamless
	HooAds
	Despicale

pseudo-Darkleech

- 観測された攻撃キャンペーンの特徴

大きくマイナスなTop値

```
<span style="position:absolute; top:-1133px; width:320px;
height:320px;">
bkya
<iframe src="http://red.JOHNVAUX.COM/?
q=znrQMvXcJwDQDoDGMvrESLtEMUjQA0KK2OH_76qyEoH9JH1vrLUSkrttgWC&
oq=elTR_aYtfrYDaQO0iEJDLgE3YpfB15Bov2qjkDVzhbOp-K_xa9UToBvdeW"
width="265" height="264"></iframe>
bledogr
</span>
huhoz
<noscript>
```

RIG Exploit Kitの特徴

- ドメインやIPアドレスは数時間で変更される
  - 「ユーザ環境におけるRIG Exploit Kitの実態調査方法の提案」（嶌田一郎，太田敏史，岡田晃一郎，山田明，第78回コンピュータセキュリティ研究発表会）
- 攻撃パターンの特徴は頻繁に変わる
  - 例：URLの更新
- 攻撃に用いられるコードが難読化されている
  - 「RIGエクスプロイトキット解析レポート」（NTTセキュリティ）

解析や対策が困難

研究目的

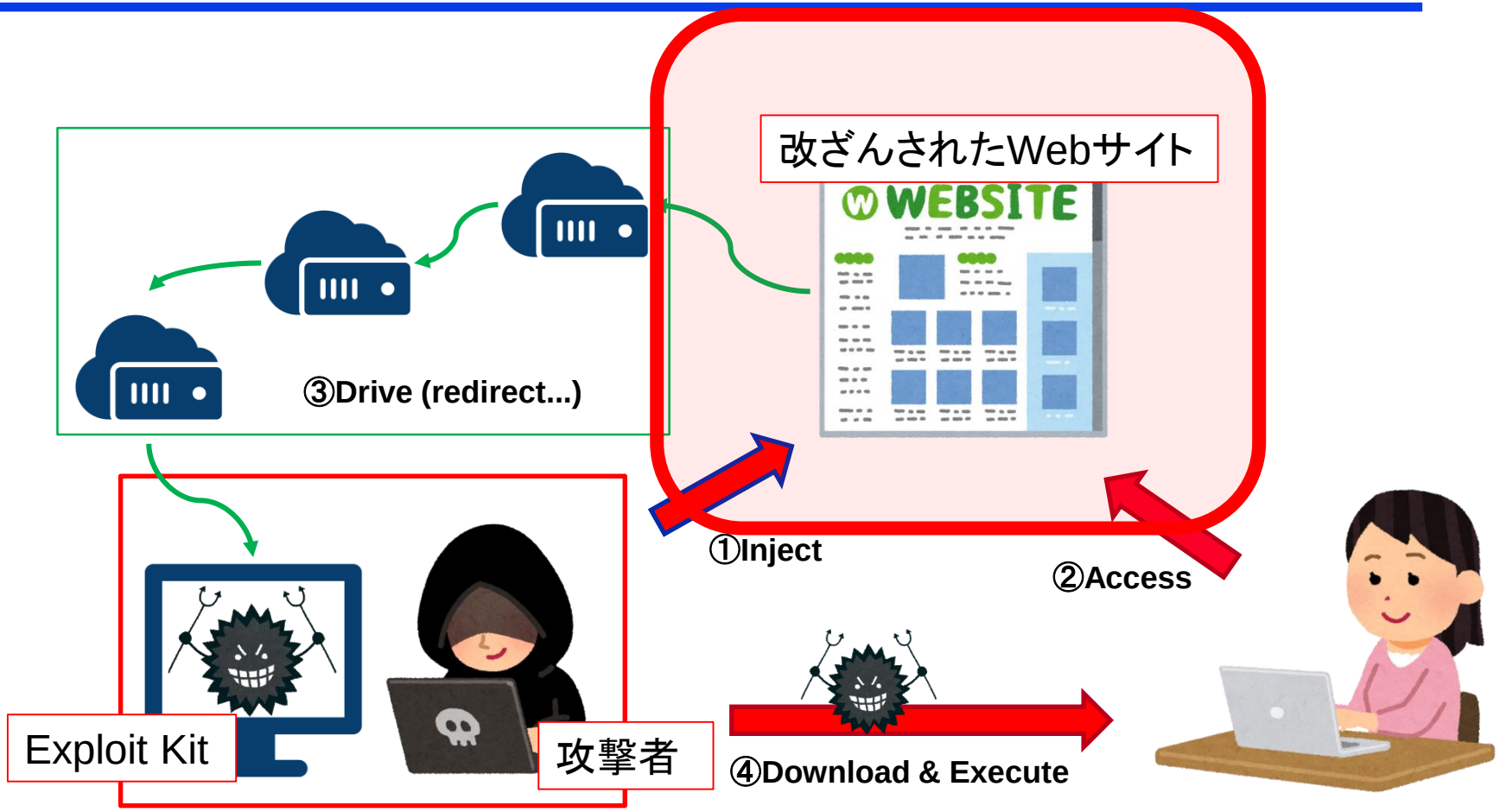
- RIG Exploit Kitを用いている攻撃キャンペーンについて調査し，どのように攻撃を行っているのか調査する
- RIG Exploit Kitを長期間に渡って調査し，用いられている解析妨害手法を明らかにする
- RIG Exploit Kitに対して有効な防衛手法を提案する

⇒2B1-2 小池
「Drive-by Download攻撃におけるRIG Exploit Kitの解析回避手法の調査」

実験概要

	実験1	実験2
目的	改ざんサイトの探索	RIGの遷移時間を明らかにする
方法	AlexaのTop1millionをクローリング	RIGの中継サイトの定期的な観測
期間	2017年2月24日～4月10日	2017年5月4日～8月15日

実験1:対象

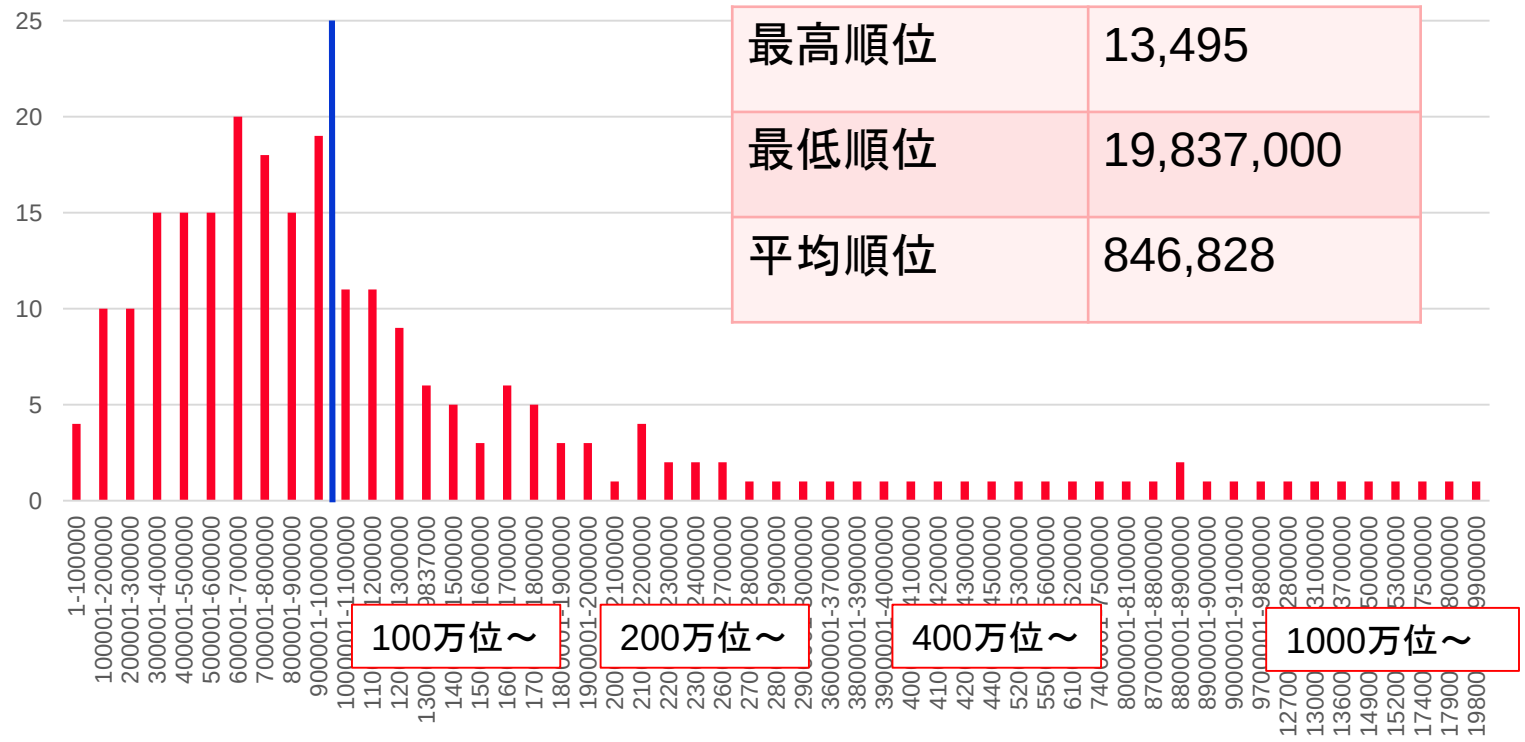

改ざんされたWebサイト
WEBSITE
③Drive (redirect...)
①Inject
②Access
Exploit Kit
攻撃者
④Download & Execute

実験結果：CMS毎の観測回数

	pseudo-Darkleech	EITest	FakeChromePopup	GoodMan	総計
WordPress1	23	17	1	0	41
WordPress2	29	5	0	0	34
WordPress3	8	5	0	0	13
WordPress4	1	21	1	0	23
Diviv. 3. 0. 10	1	0	0	0	1
Drupal7	23	1	0	0	24
Joomla!	61	7	0	5	73
MicrosoftFrontPage5. 0	0	0	0	1	1
MODx	1	0	0	0	1
w					
N/A	24	8	0	7	39
総計	171	66	2	13	252

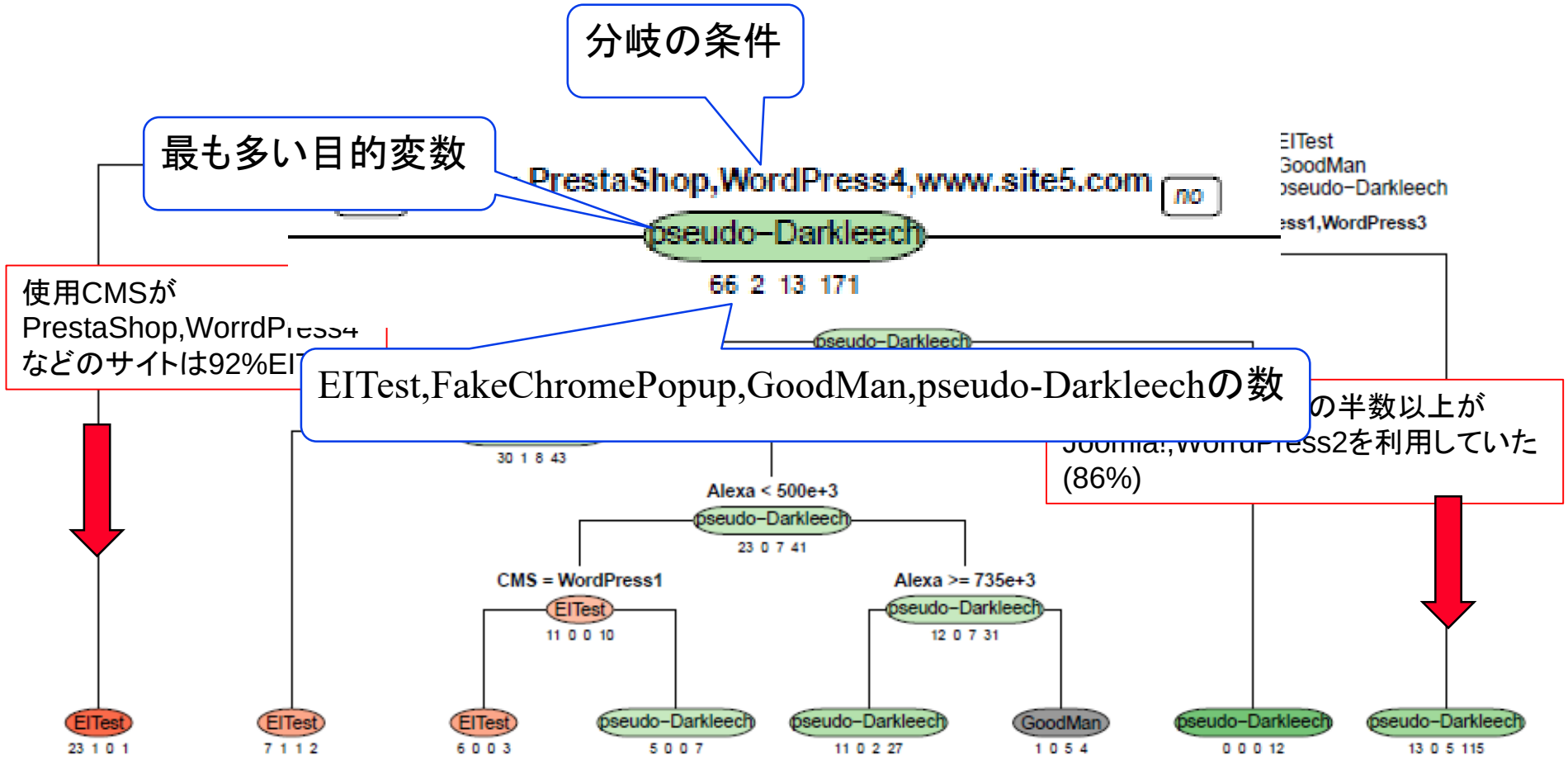
キャンペーン毎に対象となる特徴的なCMSが存在

実験結果：Alexaのランキング分布

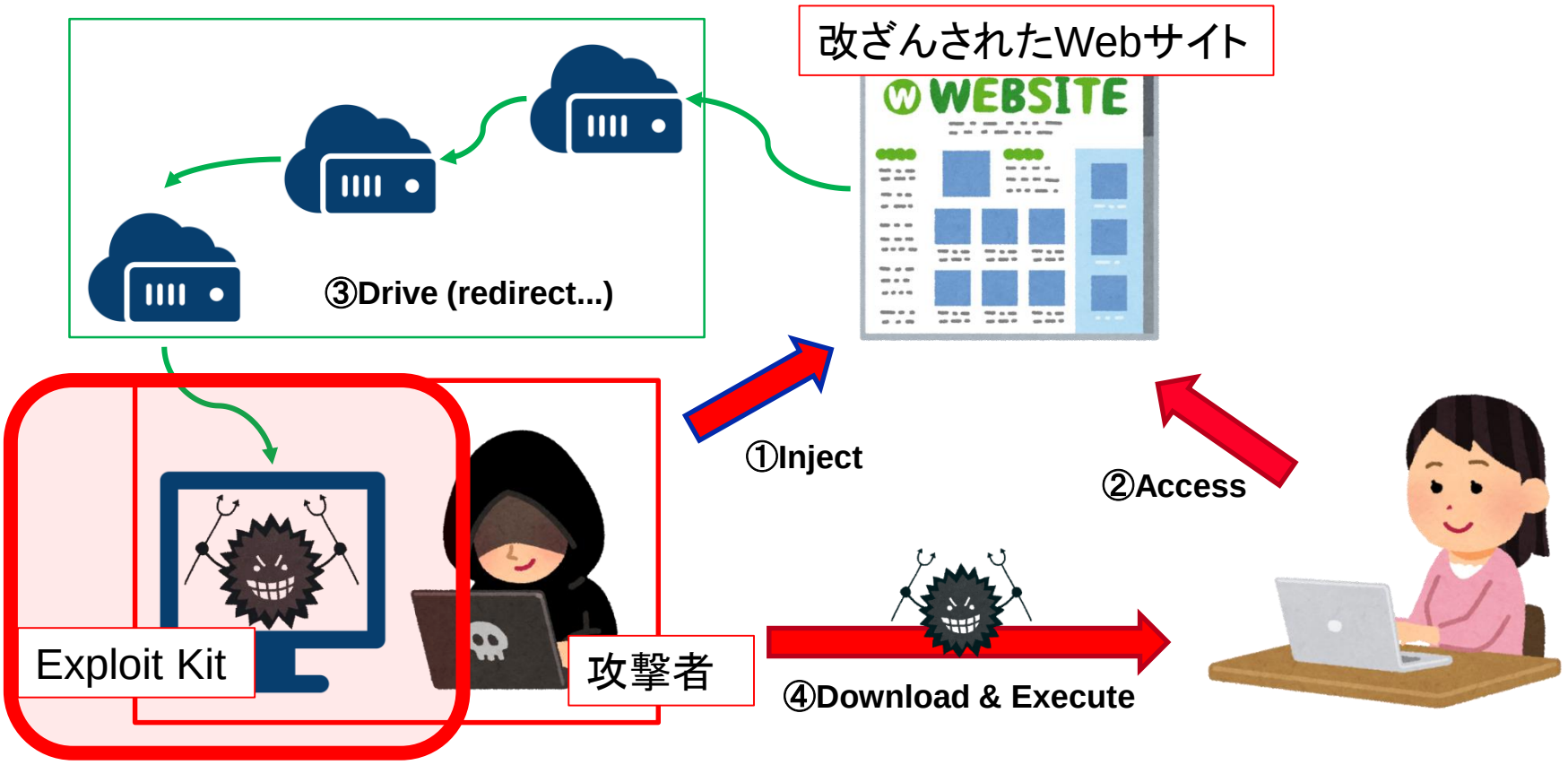


最高順位	13,495
最低順位	19,837,000
平均順位	846,828

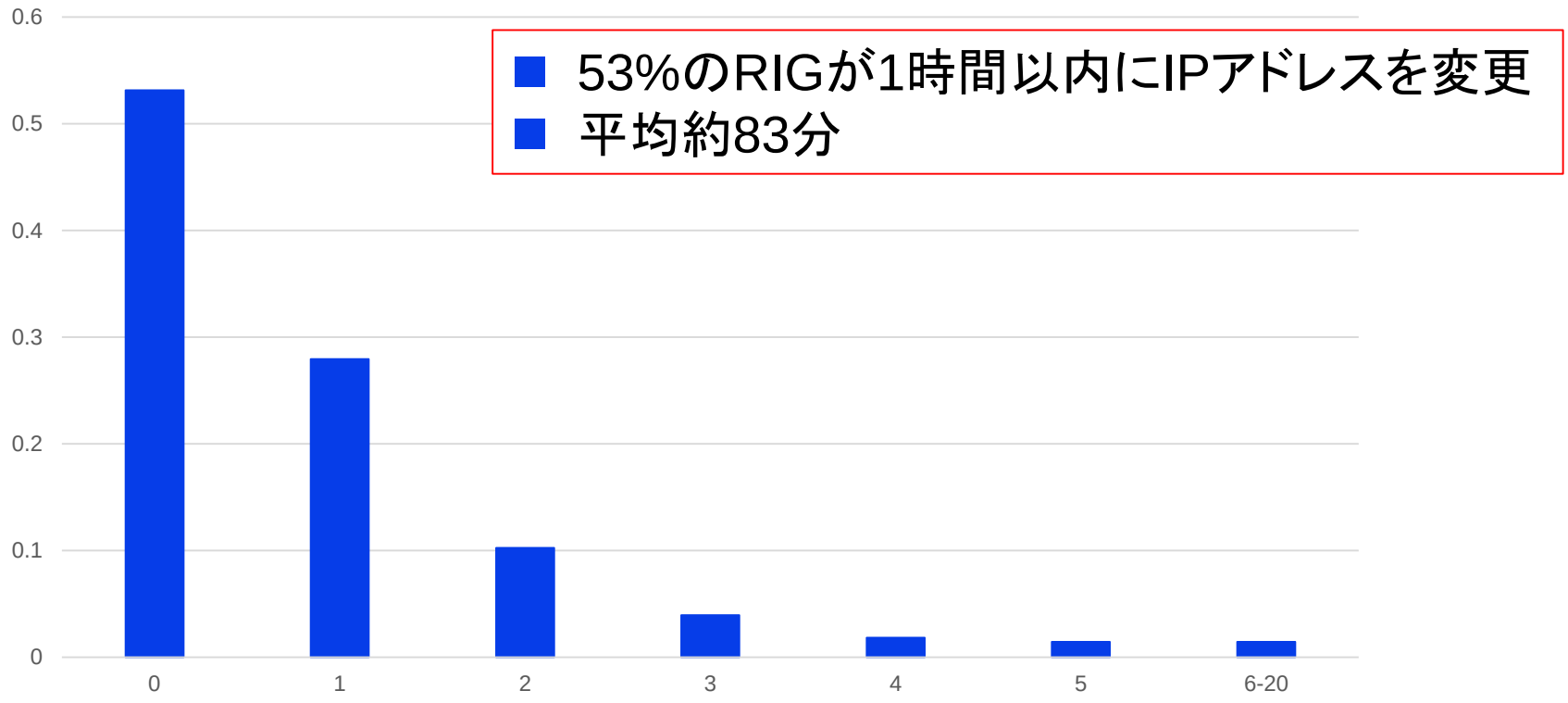
実験結果：キャンペーンを識別する決定木(R:rpart)



実験2:対象


改ざんされたWebサイト
WEBSITE
③Drive (redirect...)
①Inject
②Access
Exploit Kit
攻撃者
④Download & Execute

実験結果：RIGの変更間隔



実験結果：RIGの国の分布

- RIGのIPから国を検索
- 99%がロシア
- AS9123(www.timeweb.ru)が管理していたものが651

country	
ロシア連邦 (Russian Federation)	872
オランダ (Netherlands)	2
ウクライナ (Ukraine)	2
フランス (France)	1
カザフスタン (Kazakhstan)	1
アメリカ合衆国 (United States)	1
日本 (Japan)	1

まとめ

- CMSの分布，決定木の作成からキャンペーン毎に改ざんするサイトの使用CMSに偏りが見えた
- pseudo-DarkleechはEITestは古めのWordPressを新しめのWordPressを主なターゲットにしていた
- 53%のRIG Exploit Kitが1時間以内にIPアドレスを変更
- 99%のRIG Exploit Kitがロシアに存在
- 今後の課題
  - キャンペーンの分類自体の自動化
  - EKや，中継サイトのIPアドレスやURLの変化の特徴を明らかにしたい

WordPress1	Ver 情報不明
WordPress2	3.5.1, 3.6.1, 3.8.16 4.0.1, 4.0.15, 4.0.16 4.1, 4.1.1, 4.1.15, 4.1.16 4.2.12, 4.2.13, 4.2.3 4.3.5, 4.3.8, 4.3.9 4.4.2, 4.4.3, 4.4.7, 4.4.8 4.5.3, 4.5.6, 4.5.7
WordPress3	4.6.1, 4.6.3, 4.6.4
WordPress4	4.7.1, 4.7.2, 4.7.3

実験1

- 観測された攻撃キャンペーンの特徴
  - ❑EITest
    - » 改ざんによって挿入されるコードはbodyタグの閉じタグの直前に入り，Exploit Kitへ誘導するiframeタグを生成するJavaScriptコード
    - » 同一のIPアドレスで連続的に改ざんサイトへアクセスを行うと，正常なレスポンスを返す
    - » アクセスしてきたユーザのIPアドレスの地理的情報をもとに攻撃対象を決定する

```
 <body> </body>
<script type="text/javascript"> var nirzinr = "iframe"; var
oesnzki = document.createElement(nirzinr); var wrnfs = "";
oesnzki.style.width = "14px"; oesnzki.style.height = "6px";
oesnzki.style.border = "0px"; oesnzki.frameBorder = "0";
oesnzki.setAttribute("frameBorder", "0");
document.body.appendChild(oesnzki); wrnfs =
"http://add.localtechstops.com/?
q=znzQMvXcJwDQDoDGMvrESLtEMUfQA0KK2OH_76iyEoH9JHT1vrPUSkrttgWC&
oq=el2H_aEkk7BTNAK13kaIfwFiyotfUg9B9KGo2kjcnBbI1JOG-RK9UToBvdeW";
oesnzki.src = wrnfs; </script>
</body>
</html>
```

実験1

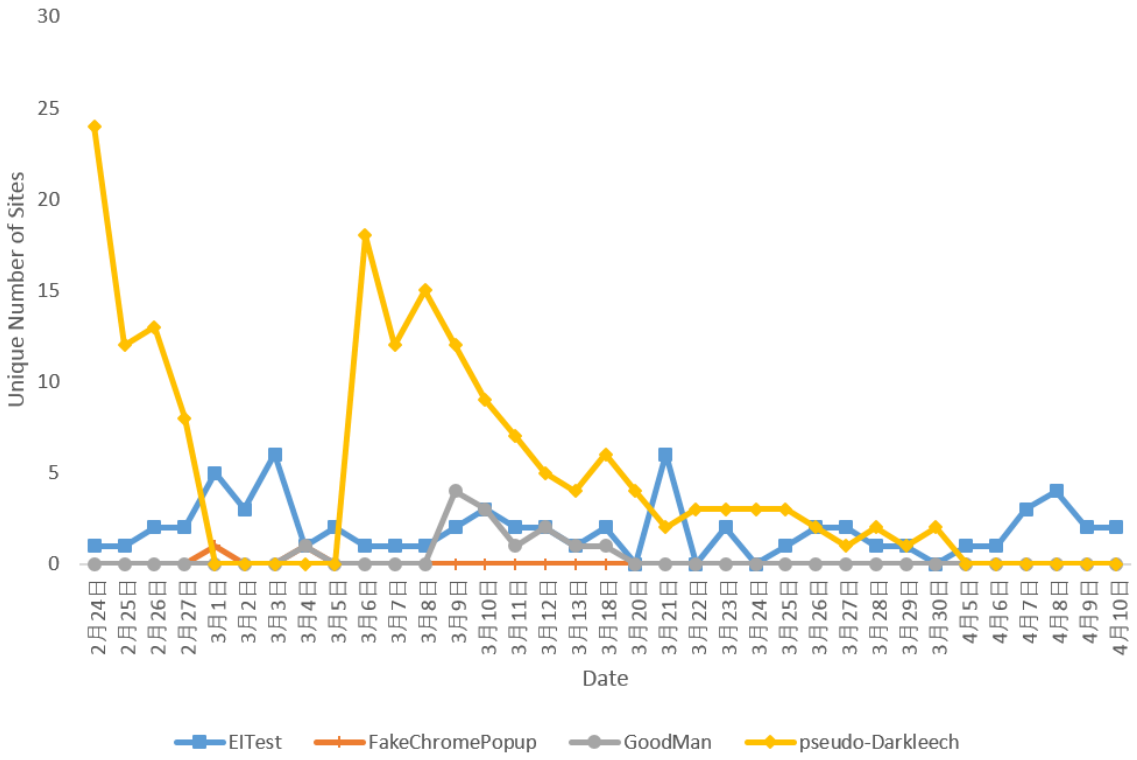
- 作成したシグネチャ

攻撃キャンペーン	シグネチャ
Afraidgate	/position:absolute; top:-([0-9]3,4)px/
EITest	/var ([a-zA-Z]4,8) = “iframe”/
GoodMan	/div style=ẃidth:1px; height:1px; pos ition:absolute; left:-500px; top:-500px;/
pseudo-Darkleech	/span style=“position:absolute; top:-([0-9]3,4)px; width:([0-9]3)px; height:([0-9]3)px;”/
Seamless	/iframe width=“0” scrolling=“no” height=“0” frameborder=“0” src=“.+” seamless=“seamless”/

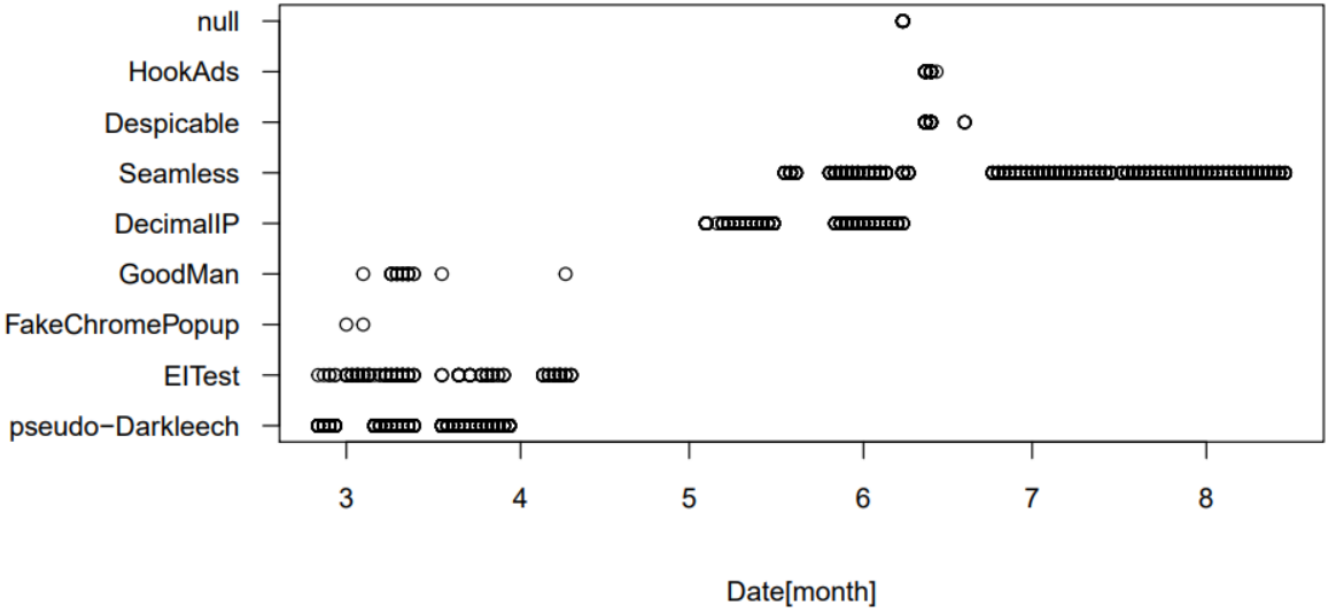
実験1

- 結果
  - 改ざんサイトの検知数

攻撃キャンペーン	検知数	誤検知率
Afraidgate	0	0%
EITest	164	4.9%
GoodMan	19	0%
pseudo-Darkleech	562	3.9%
Seamless	0	0%


30
25
20
15
10
5
0
Unique Number of Sites
2月24日
2月25日
2月26日
2月27日
3月1日
3月2日
3月3日
3月4日
3月5日
3月6日
3月7日
3月8日
3月9日
3月10日
3月11日
3月12日
3月13日
3月18日
3月20日
3月21日
3月22日
3月23日
3月24日
3月25日
3月26日
3月27日
3月28日
3月29日
3月30日
4月5日
4月6日
4月7日
4月8日
4月9日
4月10日
Date
EITest
FakeChromePopup
GoodMan
pseudo-Darkleech

キャンペーン毎の観測回数



※ちょっと詐欺

データ内容

- Compromisedサイトについて
  - URL
  - キャンペーン
  - CMS
  - 観測時刻
  - ソース
- RIGについて
  - 観測時刻
  - IPアドレス
  - キャンペーン

	Compromised サイト (ユニーク)	Exploit Kit
期間	2017/2/24～4/10	2017/5/4～8/15
N	252	2182