LAC supports your Business

We provide IT total solutions
based on advanced security technologies.

# 最近のセキュリティ事件から学ぶこと

2014年8月25日

川口　洋, CISSP
株式会社ラック
チーフエバンジェリスト
hiroshi.kawaguchi @ lac.co.jp

JSOC JAPAN SECURITY OPERATION CENTER

# 自己紹介

## 川口　洋(かわぐち　ひろし),CISSP

**株式会社ラック**

**チーフエバンジェリスト 兼 担当部長**

**ISOG-J 技術WG リーダ**

**内閣官房情報セキュリティセンター 情報統括グループ 参事官補佐**

2002年　ラック入社
社内インフラシステムの維持、運用に従事する。その他、セキュアサーバの構築サービスや、サーバのセキュリティ検査業務なども行い、経験を積む。その後、IDS や Firewall などの運用・管理業務を経て、セキュリティアナリストとして、JSOC監視サービスに従事し、日々セキュリティインシデントに対応。2005年より、アナリストリーダとして、セキュリティイベントの分析とともに、IDS/IPSに適用するJSOCオリジナルシグネチャ(JSIG)の作成、チューニングを実施し、監視 サービスの技術面のコントロールを行う。

チーフエバンジェリストとして、セキュリティオペレーションに関する研究、ITインフラのリスクに関する情報提供、啓発活動を行っている。Black Hat Japan、PacSec、Internet Week、情報セキュリティEXPO、サイバーテロ対策協議会などで講演し、安全なITネットワークの実現を目指して日夜奮闘中。

セキュリティキャンプの講師として未来ある若者の指導にあたる。また、最高の「守る」技術を持つトップエンジニアを発掘・顕彰する技術競技会「Hardening」のスタッフとしても参加し、ITシステム運用に関わる全ての人の能力向上のための活動も行っている。

川口洋のセキュリティ・プライベート・アイズ（@IT）連載中
http://www.atmarkit.co.jp/fsecurity/index/index_kawaguchi.html

# これは何の数字でしょう？

| | |
|---|---|
| 平成17年 | 19 |
| 平成18年 | 27 |
| 平成19年 | 32 |
| 平成20年 | 20 |
| 平成21年 | 15 |
| 平成22年 | 24 |
| 平成23年 | 55 |
| 平成24年 | 49 |
| 平成25年 | 109 |
| 平成26年上半期 | 87 |

# 政府の取り組み

## 政府サイバー対策で国の体制強化へ

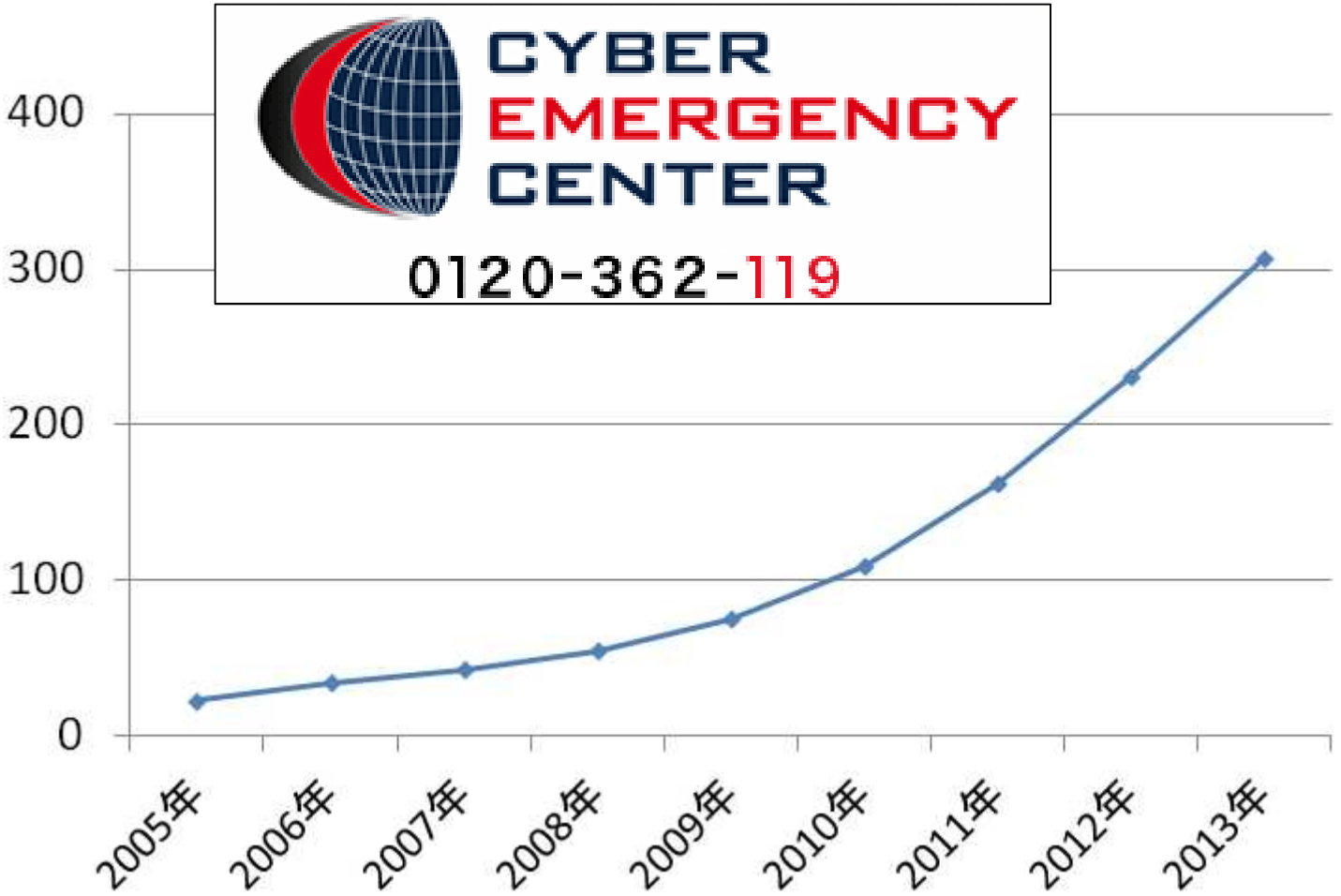
5月19日 12時57分


政府の「情報セキュリティ政策会議」が開かれ、いわゆるサイバー攻撃に対する国の体制強化に向けた方針の素案をまとめ、この会議に省庁の垣根を超えて対策を勧告する法的な権限を新たに持たせることなどが盛り込まれています。

総理大臣官邸で開かれた政府の「情報セキュリティ政策会議」で、安倍総理大臣は、「サイバー空間における脅威が一層深刻化するなか、２０２０年のオリンピック・パラリンピックに向けてサイバーセキュリティーの確保は国家の安全保障、危機管理の観点から極めて重要な課題だ。
法制の検討を含め、政府の機能を強化し積極的に取り組んでいく」と述べました。
そして会議では、「国の主導的役割を定めサイバー空間を防護することが必要だ」として、国の体制強化に向けた方針の素案をまとめました。
この中では、今の「情報セキュリティ政策会議」をサイバー対策に特化した「サイバーセキュリティ政策会議」に格上げし、政府機関が攻撃された際には各省庁にデータの提出を義務づけ、省庁の垣根を超えて対策を勧告する法的な権限を新たに持たせるほか、事務局のトップに新たに「内閣サイバーセキュリティ官」を置くなどとしています。
政府は今後、与党と連携して必要な法整備を進め、来年度の新体制発足を目指すことにしています。

# 気になるキーワード
# 「オリンピック・パラリンピック」

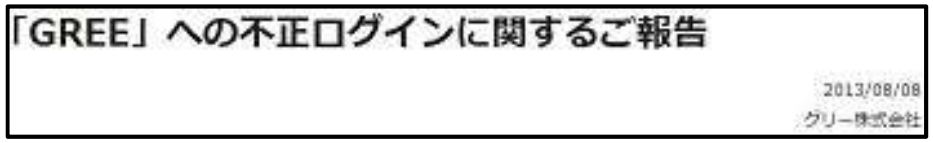
# ラック サイバー救急センターの出動件数



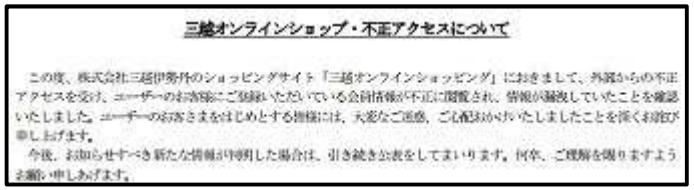

**年々、緊急対応（出動）件数が増加**
**2013年は300件を超える出動件数**

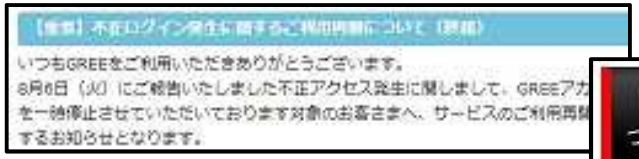
# 公開システムに対する攻撃

# 不正ログイン問題 (リスト型攻撃)

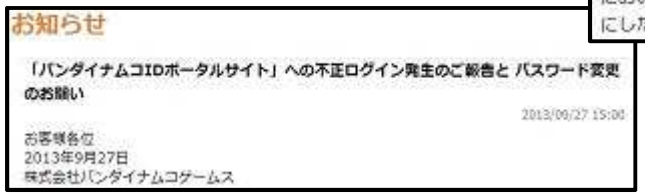




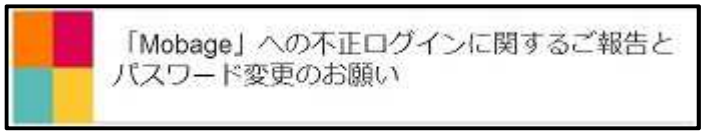



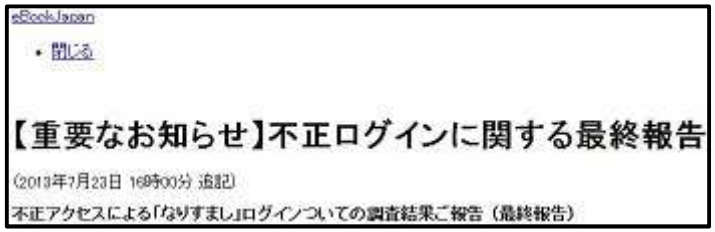


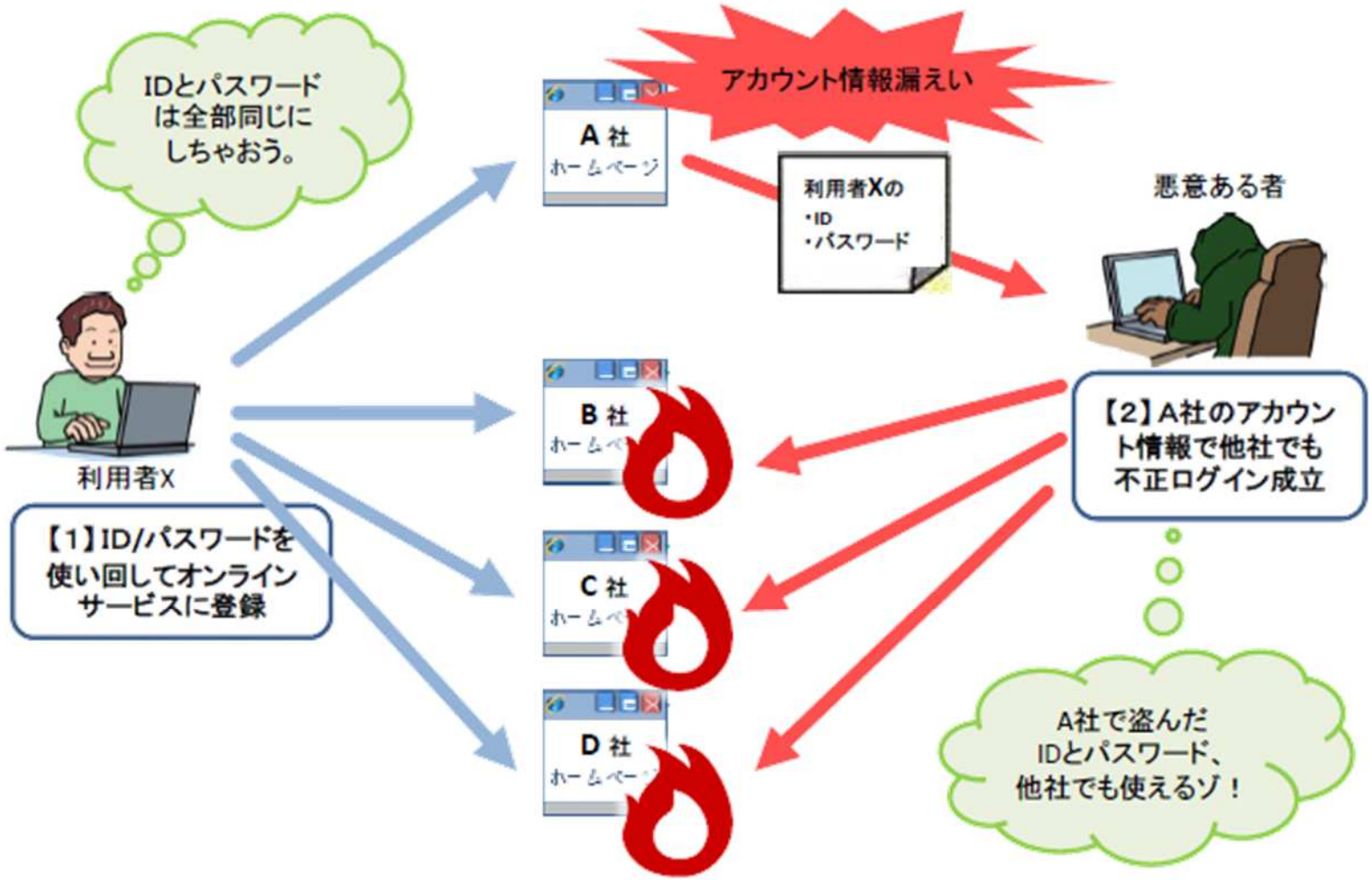







# 不正ログイン問題（リスト型攻撃）




https://www.ipa.go.jp/security/txt/2013/08outline.html

# 会場に質問（クリッカーを使用して）

- リスト型攻撃の被害にあったことが

- ある
- あるような気がする
- ない
- 今日初めて知ったのでわからない

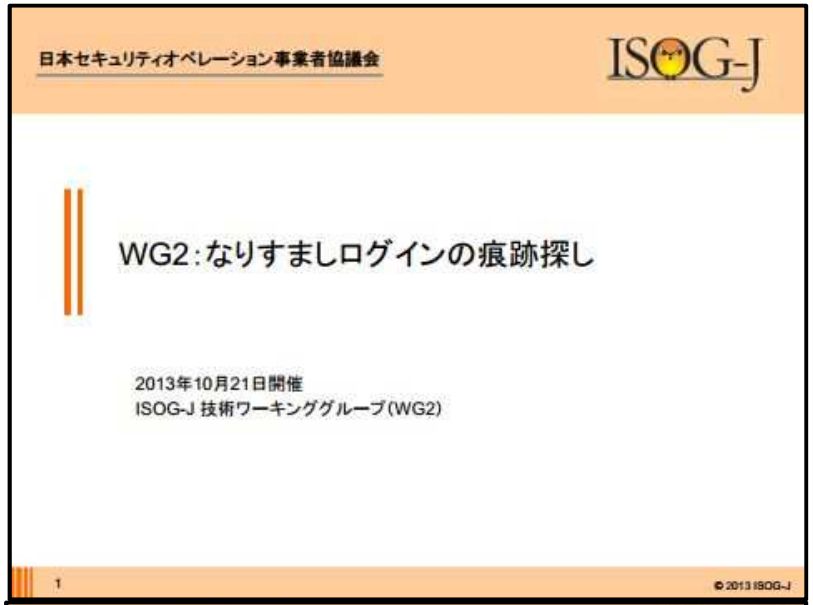
# いわゆる「なりすましログイン／リスト型攻撃」の課題

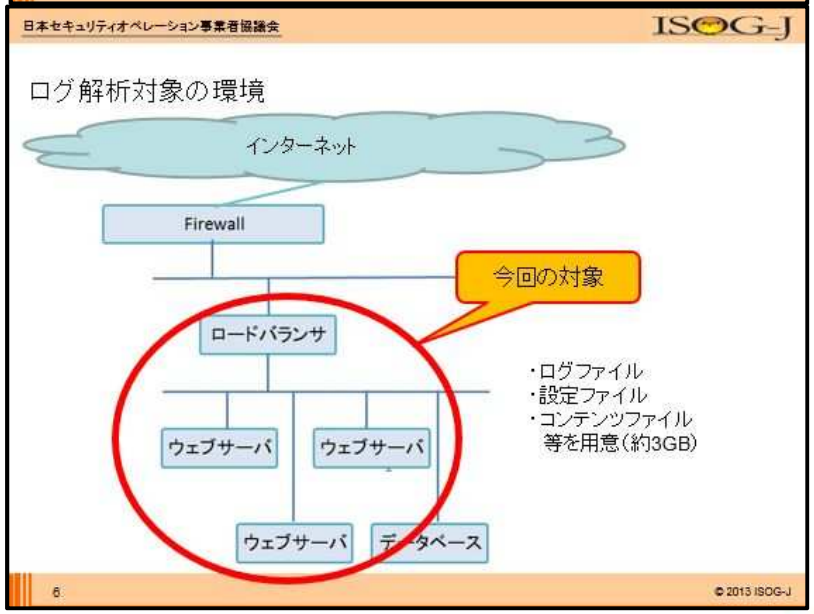
- ユーザの課題
  - 複数の会員制ウェブサイトで同じIDとパスワードを使い回している
  - 根本的にはここが課題

- サービス提供者の課題
  - コスト
    - 二要素認証、二段階認証、ログインアラート機能等の技術的対策はある
    - サービスコストは最終的にはユーザの使用料金に転嫁される（かもしれない）
  - 技術的な課題
    - 止めること
      - 誤検知、見逃し、コストの問題
    - 見つけること
      - ログ保存期間
      - 複数種類のログの相関分析
      - 時刻同期

# ISOG-J WG2でログ解析に挑戦してみた

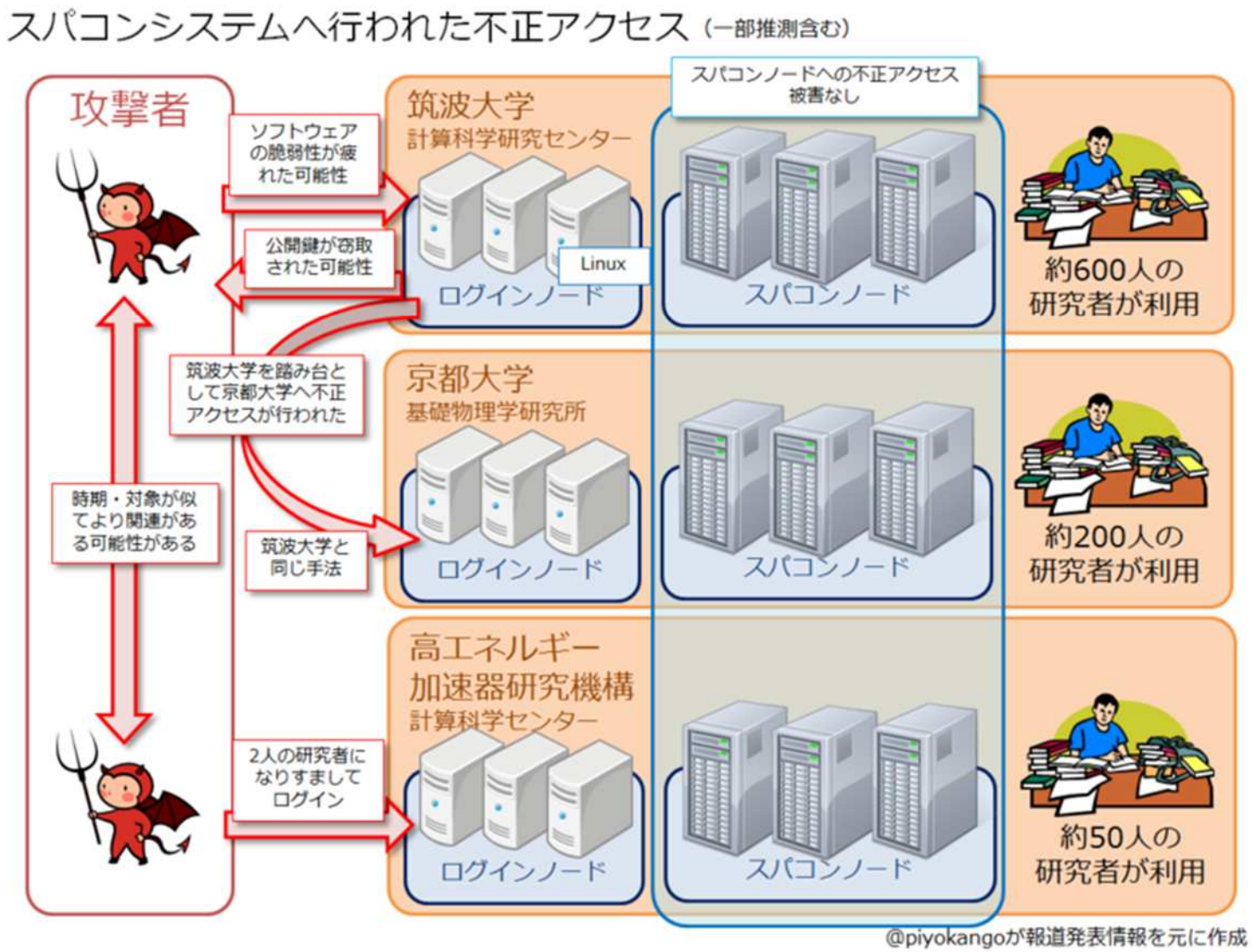
- 参加者の声
  - ログインに関するログを探した
  - エラーコードに注目した
  - 認証系のログを探した
  - 多数のアクセスがあるものに注目した
  - リクエストメソッドに注目した
  - 攻撃ツールのような動きについて注目した
  - レポート用ツールを使用してビジュアル化した
  - Excelを使用した
  - grep一本で頑張った



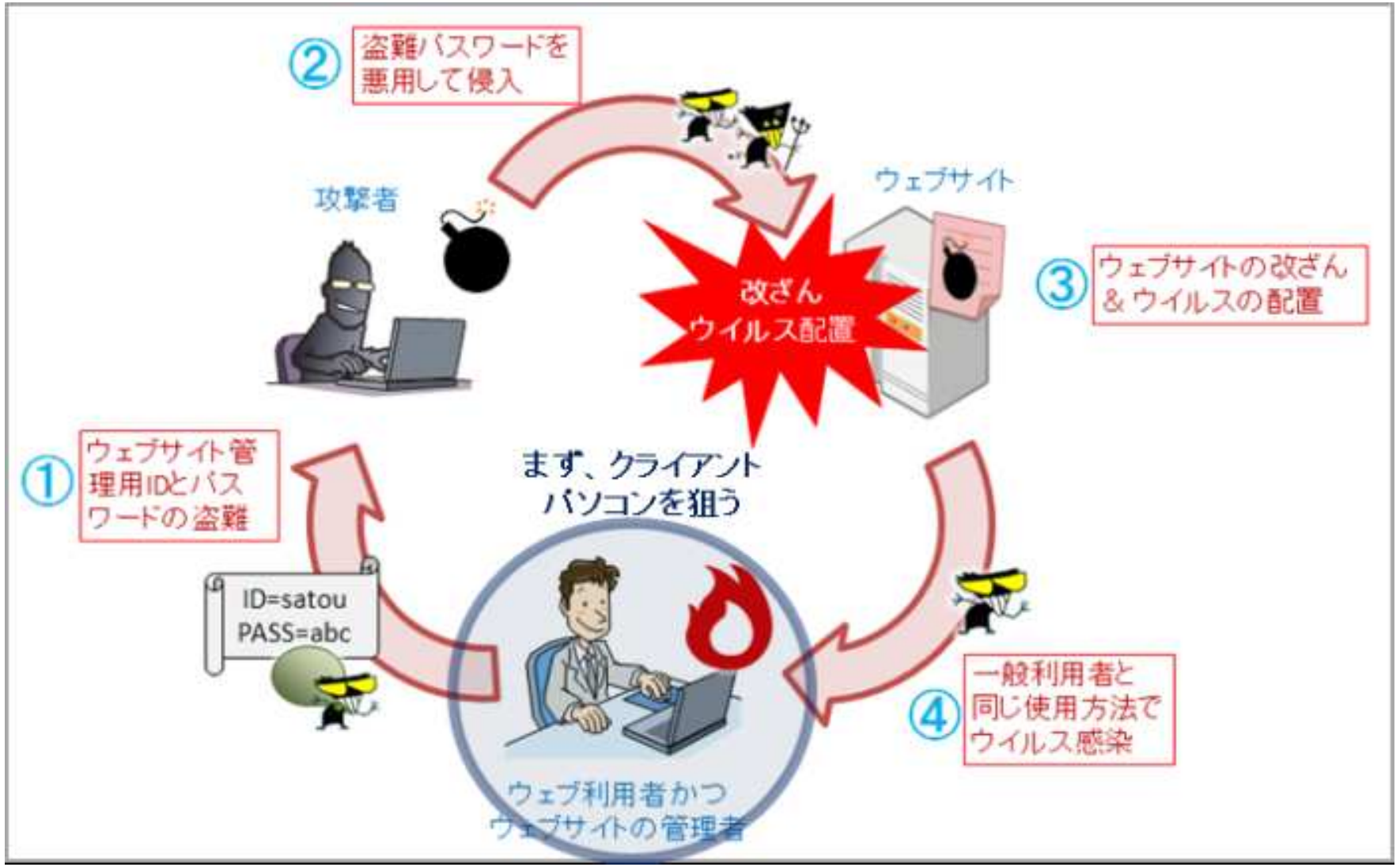

日本セキュリティオペレーション事業者協議会 (ISOG-J)
WG2：なりすましログインの痕跡探し
http://isog-j.org/output/2013/wg2-20131021.pdf

# スパコンシステムへの不正アクセス




http://d.hatena.ne.jp/Kango/20131218/1387387548

# ウェブサイト改ざん




http://www.ipa.go.jp/security/txt/2013/07outline.html

# 気づいていない利用者の事例

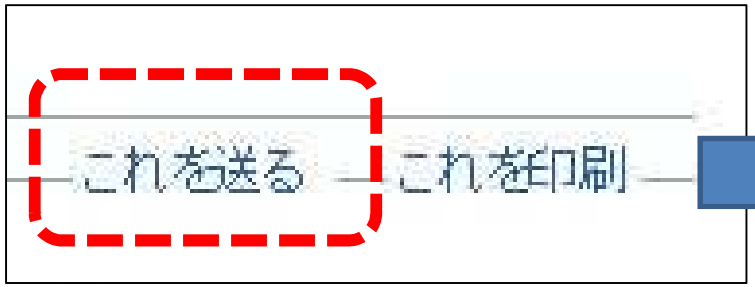
- ある百貨店
- ある不動産屋
- ある学校
- 連絡しても
  - 応答無し
  - 「問題ありません」 → いや、やられてますし
  - 「対処しました」 → まだ、改ざんされています

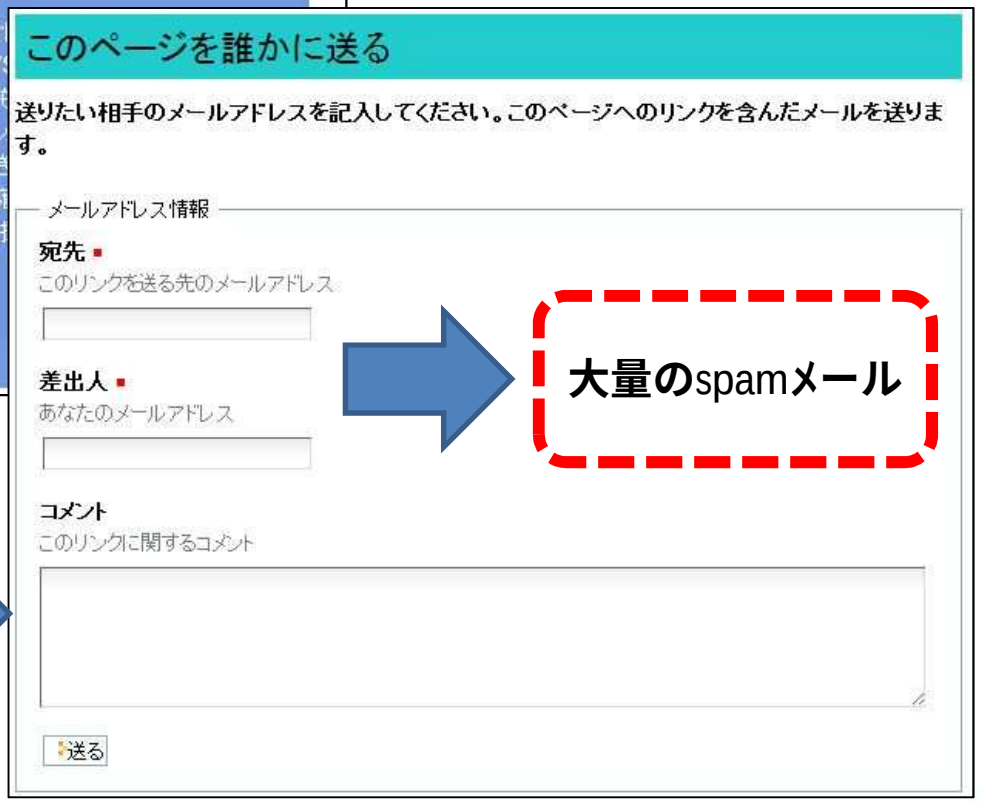
# CMSを狙った攻撃

- Movable Type
- WordPress
- Joomla!
- MODX
- Moodle
- e107
- Drupal
- Zen Cart
- osCommerce
- Plone
- phpAlbum
- pmwiki

- 攻撃内容
  - ファイルアップロード
  - アカウント追加
  - サイト改ざん
  - 情報窃取
- 問題
  - 情報が少ない＆遅い
  - 機能が複雑
  - WAFやIPSで防御できないタイプの攻撃もある
- 攻撃対象
  - 本体
  - プラグイン
  - テーマ（特に非公式サイトの無料テンプレート）

# Ploneの機能を悪用

# Strutsの脆弱性による問題

## 国税庁、「Apache Struts 1」利用の複数サービスを停止

「Apache　Struts」の脆弱性に対する攻撃が発生している問題で、国税庁は影響を受ける複数のウェブサービスを停止した。

同庁がサービスを停止したのは、ウェブ版の「e-Taxソフト」をはじめ、「確定申告書等作成コーナー」「NISAコーナー」。これらサービスにおいて、2013年4月にサポートが終了した「Apache　Struts　1」を利用していることを確認したという。

同庁では、現在対応を検討しており、対応が完了するまでサービスを一時停止。手書きによる対応や、影響がないソフトを利用するよう呼びかけている。

http://www.security-next.com/048427

## 技術者試験の一部中止に　ウェブ構築ソフトに欠陥

2014/4/29 18:02

小 中 大　保存　印刷　リプリント　▼共有

多くの政府や企業が使うウェブサイト構築ソフト「ストラッツ1」にセキュリティー上の欠陥（脆弱性）が見つかった問題で、独立行政法人の情報処理推進機構（IPA）は29日と30日、運営する国家試験の情報処理技術者試験の一部を取りやめた。2日間で合わせて約250人が受験できなくなった。IPAは受験予定者へ、後日実施する試験に再度申し込むように電子メールで通知した。

取りやめた試験は「ITパスポート試験」。紙のテストではなくパソコンを使い受験する形式。受け付けシステムにストラッツ1を使っていたという。IPAは28日夜9時までに受験予定者に試験中止と振り替えの案内を電子メールで連絡した。30日午後4時までにシステム運用を委託する日立ソリューションズと協力し、脆弱性を修正する。

http://www.nikkei.com/article/DGXNASDZ2902P_Z20C14A4TJC000/

## 「落とし物検索システム」運用停止　欠陥見つかる

鳥取県警は28日、「落とし物検索システム」の使用ソフトにセキュリティー上の欠陥が見つかり、同システムの運用を停止したと発表した。復旧のめどは立っていない。

ソフトは、官公庁などで広く利用されている「ストラッツ１」。落とし物を探す検索項目として遺失物の発見日時、場所、特徴などのデータを公表しているが、欠陥によりそれらが改ざんされる恐れがあるという。

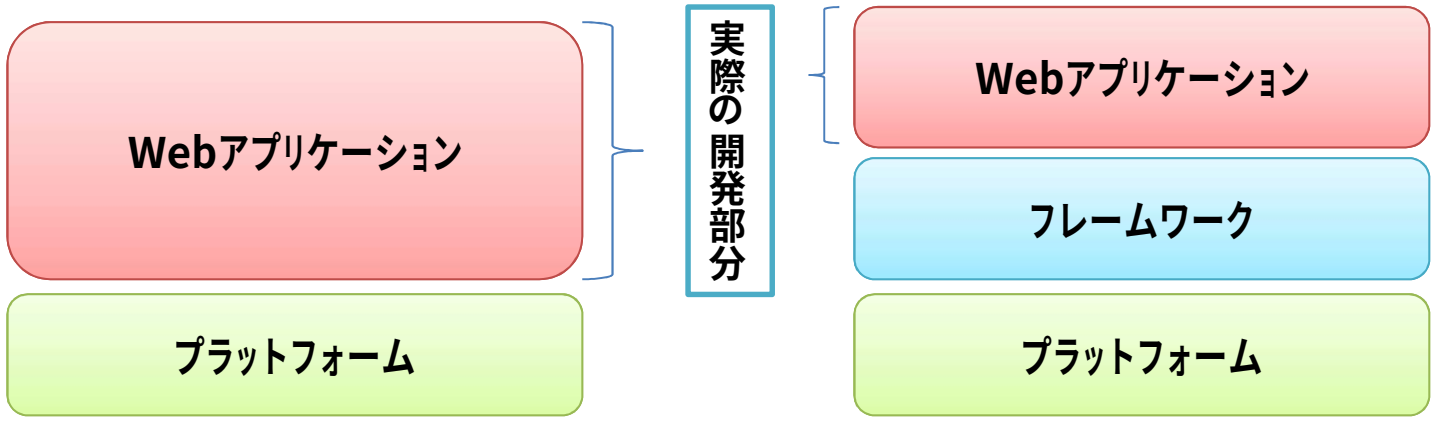
http://www.nnn.co.jp/news/140429/20140429005.html

# Strutsとは

- Java言語用の主要なWebアプリケーションフレームワークの一つ
  - Java言語

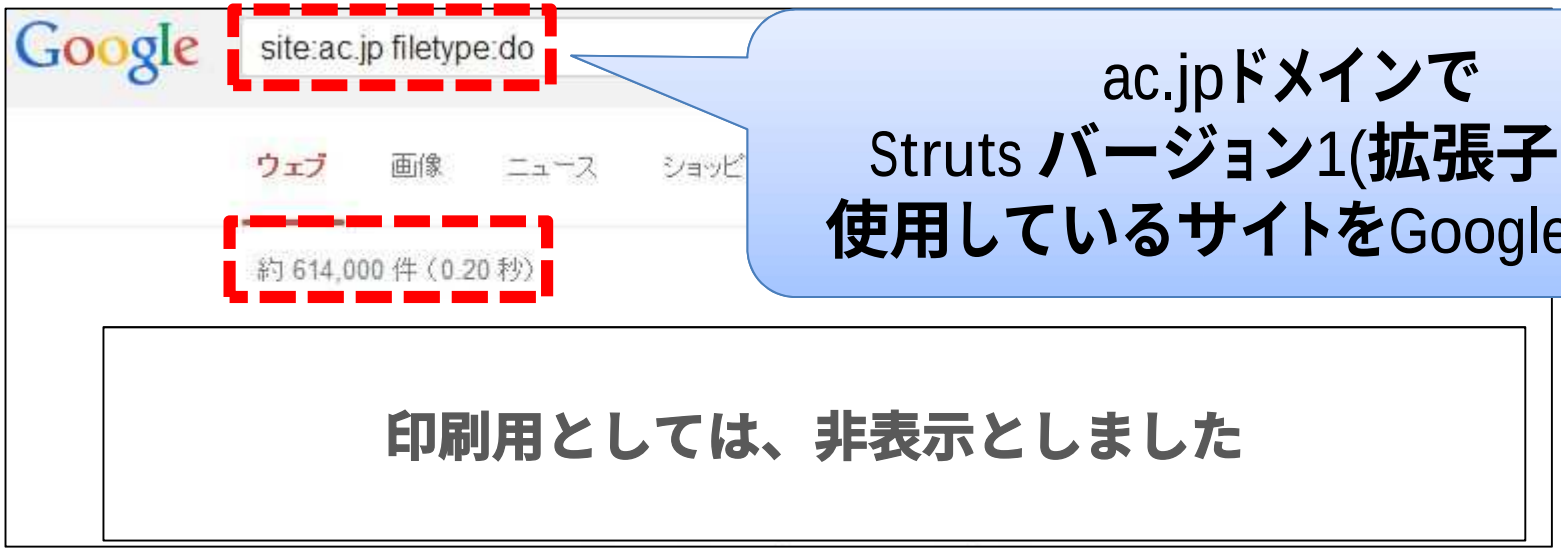
    Webアプリケーション開発用の言語として業界のデファクトスタンダード。
  - フレームワーク

    プラットフォームとWebアプリケーションの間で「枠組み」を提供するためのソフトウェア。様々なWebアプリケーションで共通して必要となる機能を集約したもの。これを利用することで余分な開発工数を削減し、体系だった開発を可能とする「通訳」のような存在。



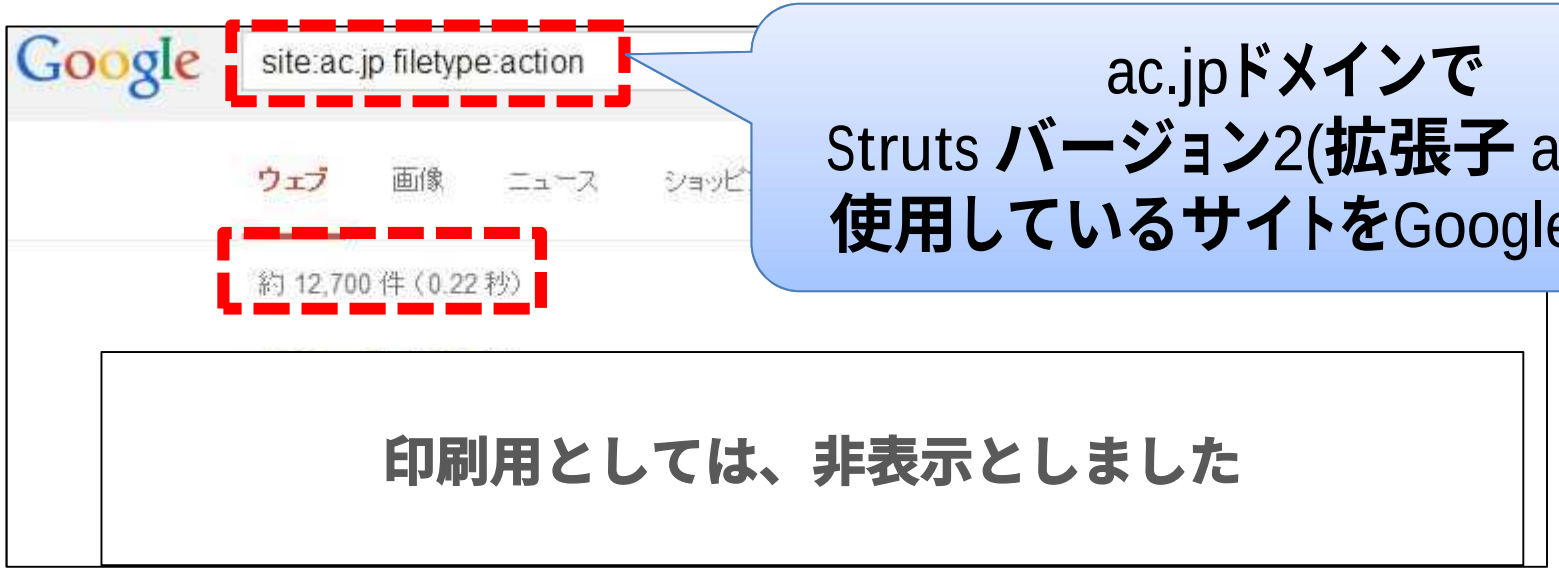

フレームワークを使用しない場合　　フレームワークを使用した場合

# ac.jpのStruts使用状況（2014年8月3日時点）




ac.jpドメインで
Struts バージョン1(拡張子 do)を
使用しているサイトをGoogleで検索

印刷用としては、非表示としました




ac.jpドメインで
Struts バージョン2(拡張子 action)を
使用しているサイトをGoogleで検索

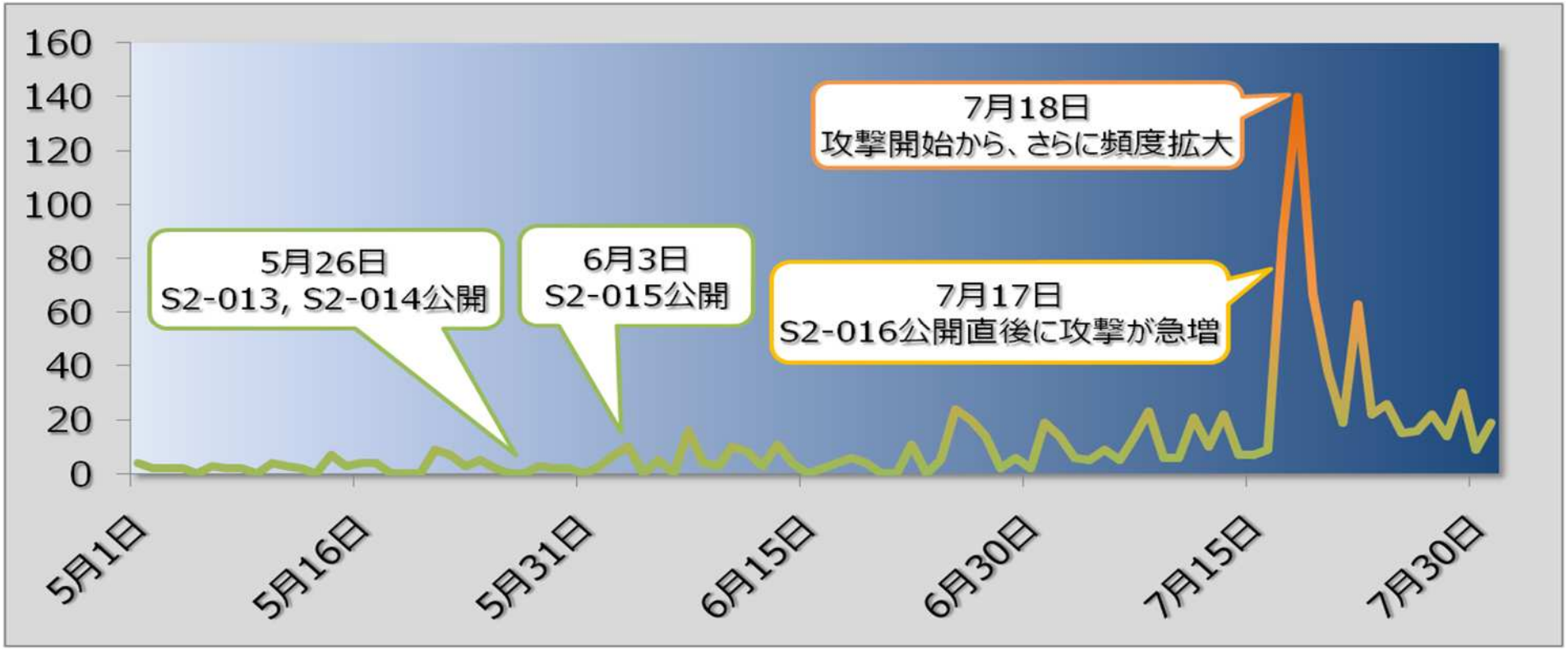
印刷用としては、非表示としました

# Struts1とStruts2の使用状況（2014年6月2日時点）


印刷用としては、非表示としました

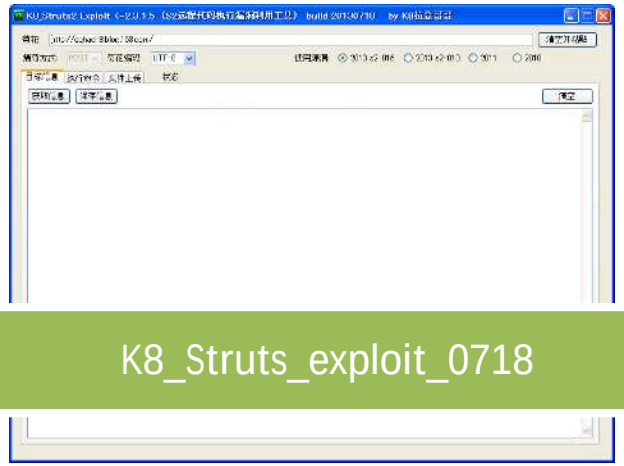

印刷用としては、非表示としました

# 2013年に行われたStruts2に対する攻撃

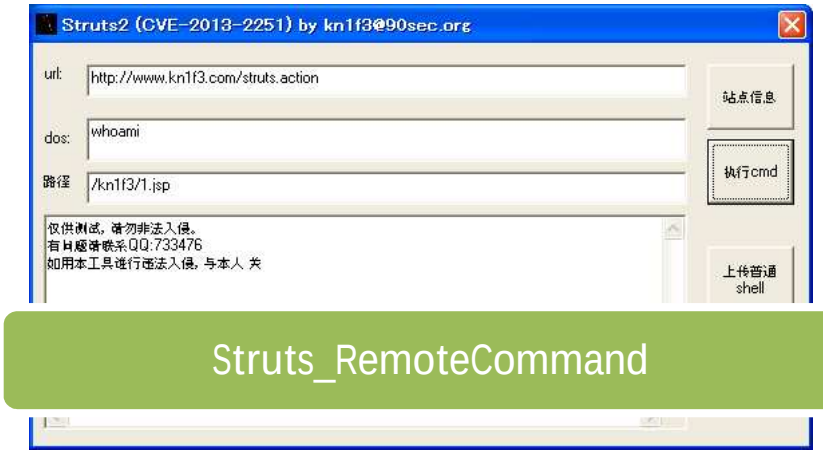



- 脆弱性情報の公開直後から攻撃が急増した
- 多くのサイトは対策をとる時間すらなく攻撃を受けた
- 7月～8月に被害情報を公開している事案の多くはこの脆弱性を悪用された可能性が高い

# S2-016を狙う攻撃ツール

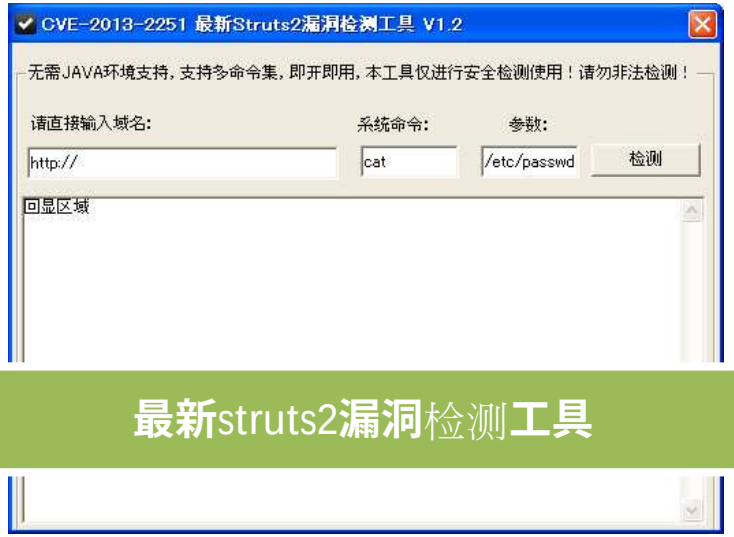


K8_Struts_exploit_0718




Struts_RemoteCommand


**鬼哥**struts2(CVE-2013-2251)**漏洞**测试**工具**




**最新**struts2**漏洞**检测**工具**

- **中国語で記載された攻撃ツールが多数リリースされている**
- **脆弱性公開1週間程度で5種類以上リリースされている**

# Strutsを内包する製品群

14/04/28 【重要】
GroupSessionで使用しているウェブアプリケーションフレームワークである「Apache Struts」について脆弱性が発見されました。
GroupSessionにおいても同脆弱性が存在いたします。

この脆弱性により第三者によって、情報を窃取されたり、任意のコードを実行されたりする等の可能性があります。

ご参考IPA | Apache Struts2 の脆弱性対策について(CVE-2014-0094)(CVE-2014-0112)(CVE-2014-0113)

Q 質問

FAQ番号:388 | 最終更新日:2014/04/30

Apache Struts で発見された脆弱性について
http://www.lac.co.jp/security/alert/2014/04/24_alert_01.html
上記URLにて公表された脆弱性の報告についてintra-mart製品は影響はないでしょうか。

A 回答

印刷

intra-mart BaseModule/WebPlatformのアプリケーションサーバであるResinでは、この脆弱性を利用して、任意のコマンドの実行や内部のファイルなどを漏洩するような操作は行えないことを確認しております。
しかし、Resinに対する一部設定(dependencyCheckIntervalなど)を変更できる可能性がある為、脆弱性に対応したパッチを用意いたしました。
以下のパッチダウンロードサイトよりダウンロードしてREADME.txtをご参照の上、適用してください。

株式会社セゾン情報システムズ

HULFT 事業部

**HULFT クラウド 脆弱性のご報告と対応について**

HULFT クラウドで使用している Web アプリケーションフレームワーク(Struts2)に脆弱性が発見されましたので、ご報告いたします。

**Apache Struts1（アパッチ ストラッツワン）の脆弱性対策向けにTERASOLUNA®Server Framework for Java用パッチを提供**

# 会場に質問（クリッカーを使用して）

- 自分の組織でStrutsを

- 使用している
- 使用していない
- 考えたこともないのでわからない
- 納入ベンダに聞かないとわからない

# 確認方法

- サーバの中で
  - struts-core-x.x.x.jar
  - struts2-core-x.x.x.jar
  - 複数バージョン存在することもある

- Google検索で
  - site:mydomain.local filetype:do
  - site:mydomain.local filetype:action

- あとは
  - 事業者に確認する

# Active! mail を使ったユーザを狙ったフィッシング

## 大学などで使用されているWebメール(Active! Mail)アカウントを狙うフィッシング(2013/12/12)

### 概要

大学などで使用されているWebメール(Active! Mail)システムのアカウントを狙うフィッシングメールが出回っています。

### メールの件名

あなたの電子メールアカウントに、いくつかの失敗したログイン試行

### 詳細内容

大学などで使用されているWebメール(Active! Mail)システムのアカウントを狙うフィッシングの報告を受けています。

1. 2013/12/12 13:00 現在フィッシングサイトの停止を確認しておりますが、類似のフィッシングサイトが公開される可能性がありますので引き続きご注意ください。

2.このようなフィッシングサイトにて、メールアドレス、ユーザーID、パスワードなどを絶対に入

3. 類似のフィッシングサイトやメールを発見した際には、フィッシング対策協議会 (info@antip

【参考情報】

Active! mailの利用ユーザー様を狙ったフィッシング詐欺にご注意ください！

http://www.transware.co.jp/news/2013/10/03_2030.html

### サイトのURL

http://activemailsecurityportal.●●●●.com/

---(メール本文ここから)----------

注意:アクティブメールユーザー

あなたのメールボックスのクォータは、Active側によって設定された格納域の制限を超えている

あなたの電子メールアカウントを検証する再には、ここをクリックしてください:

http://

正しくあなたのログイン情報を提供するために、障害になることに注意してください

私達のデータベースからメールアカウントの即時閉鎖

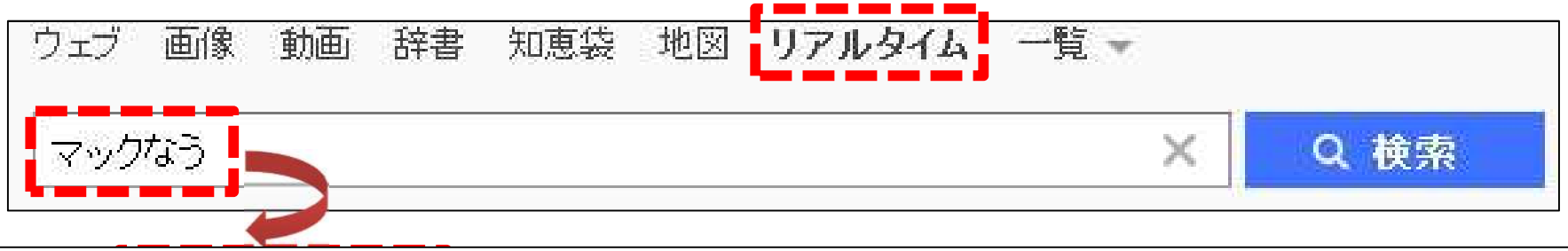
UCOM Web Mail

・1998-2010 TransWARE Co. All Rights Reserved.

---(メール本文ここまで)----------

# 閑話休題

# Yahoo!リアルタイム検索で「マックなう」を検索すると




印刷用としては、非表示としました

# 子供とネットを考える会


# 具体的な対策

# すぐにやるべき対策

| 対策ポイント | 対策内容 |
|---|---|
| システム全体 | ログ保存を行う（ログイン履歴、Outboundログは必須）<br>ログ保存期間を延ばす（最低1年）<br>リモートアクセスのログイン履歴を確認する<br>時刻同期設定 |
| サーバ | アプリのバージョンを確認する<br>（Tomcat, JBoss, Struts, ColdFusion, Joomla!, WordPress, Movable Type, MODX など）<br>ウイルス対策ソフトのスキャンログを確認する<br>cronやタスクスケジューラの中身を確認する<br>公開DNSサーバやNTPサーバがUDPアンプ攻撃に悪用されないか確認する |
| クライアント | Adobe Reader、Flash Player、Java、一太郎のアップデートを検討する<br>ウイルス対策ソフトのスキャンログを確認する<br>AutoRunの設定を確認する（特にサポート期限の切れたWindows XP）<br>ブラウザは2種類入れておく(IEの脆弱性騒ぎに対応するため)<br>(自宅の)パソコンにEMETを入れる |
| ネットワーク | FW、Proxy、URLフィルタ等のログを確認する<br>Proxy認証の認証ログを確認する<br>アクセス制御ルールに不備がないか確認する |
| 人・組織 | インシデント発生を想定した訓練を行う<br>緊急時の連絡網を整備する<br>セキュリティ情報の収集を行う<br>IPA、JPCERT、J-LIS(旧LASDEC)のコンテンツを周知する |

# EMET （オススメ！！）

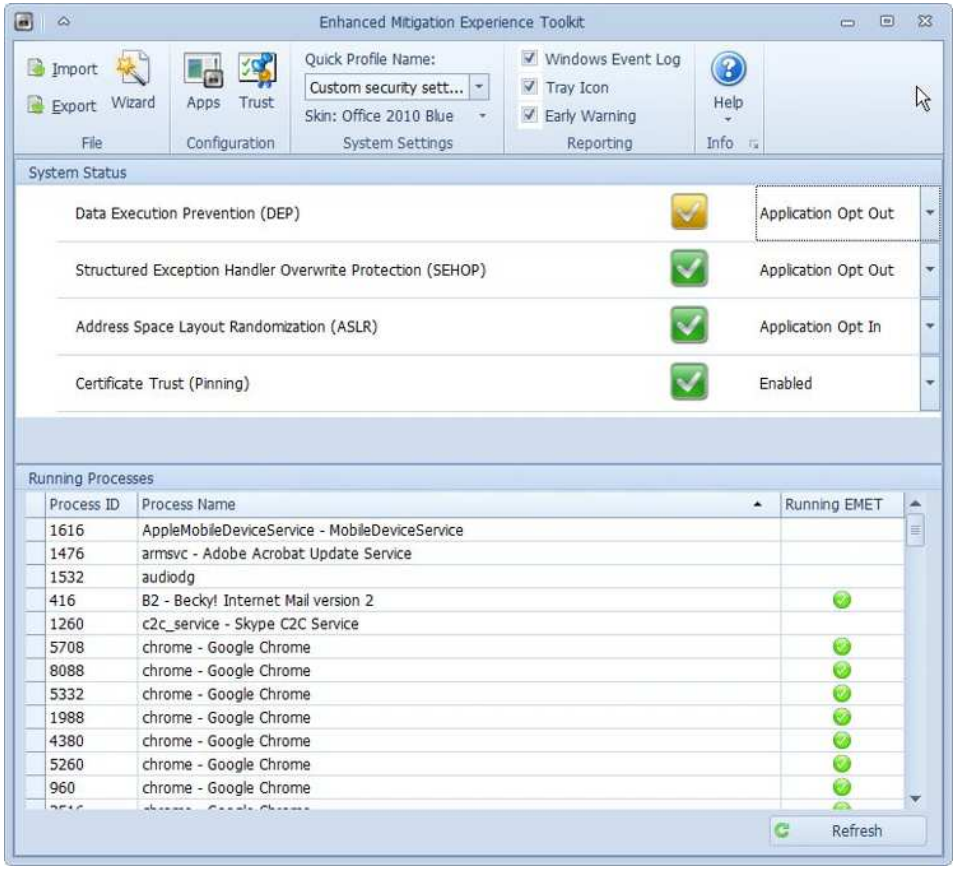




図1: セキュリティ更新プログラムにより攻撃が防御されるイメージ

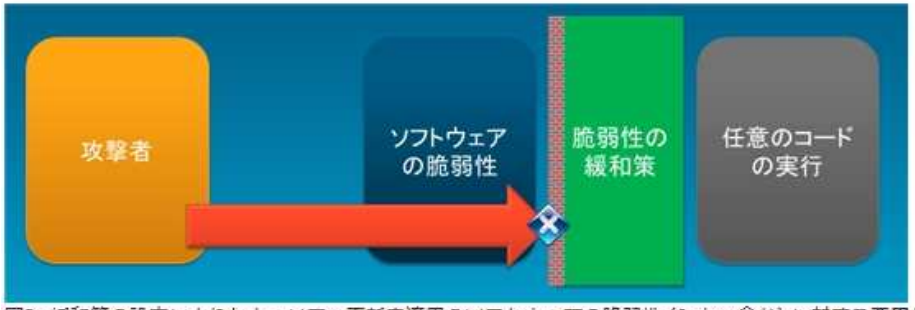



図2: 緩和策の設定によりセキュリティ更新未適用のソフトウェアの脆弱性 (0-day 含む) に対する悪用が回避されるイメージ

- マイクロソフトが公開する無償の脆弱性緩和ツール
- Windowsの保護機能を活用して、システムに対する攻撃から保護するツール
- http://support.microsoft.com/kb/2458544/ja
- バージョンがあがり設定が簡単になった
- とりあえず、Maximumを選んでおくのもいい
- ADでの大規模展開プロファイルや通知機能が強化されており、便利になった

# SECCON

SecCon CTF
SECURITY CONTEST CAPTURE THE FLAG

SECCON
SECURITY CONTEST 2013

## ハッカー大会、高専生優勝

**人材発掘狙い省庁も後援**

サイバー攻撃対策に役立つ技術を競う国内最大規模のハッカー大会「ＳＥＣＣＯＮ（セクコン）２０１３」の全国大会が１～２日、東京電機大（東京）で開かれ、高専生ら４人のチーム「０ｘ０（ゼロエックスゼロ）」が優勝した。

４人は別々の県に住み、全国大会で初めて顔を合わせたメンバーもいる。リーダーの熊本市の高専生（１９）は「問題は難しかったけど、リアルに仲間と会えて楽しかった」と話した。

セクコンは情報セキュリティー分野の人材発掘が目的で、ＮＰＯ法人「日本ネットワークセキュリティ協会」（東京）が主催、総務省や警察庁などが後援した。

(2014/03/02 18:11 | カテゴリー：暮らし・話題)


https://www.minpo.jp/globalnews/detail/2014030201001844

## ハッカー大会予選で警察庁職員健闘

2013.8.22 20:00

サイバー攻撃から情報を守る技術を競う国内最大規模のハッカー大会「ＳＥＣＣＯＮ（セクコン）２０１３」の関東地区予選が２２日、横浜市で始まった。出場していた警察庁職員６人のうち５人が２３日の最終選抜に駒を進めた。

ハッカー大会の関東地区予選に出場した警察庁情報技術解析課の野本靖之理事官（中央）＝２２日午後、横浜市

予選には社会人や中学校のパソコン部員ら１００人以上が参加。インターネットサイトなどのセキュリティーに関する問題をいかに早く正確に解くかを競い、この日は４２人が通過した。

通過した警察庁職員は、サイバー犯罪対策の担当。通過できなかった情報技術解析課の野本靖之理事官は「レベルが高く難しかったが、ほかの職員が通過できて良かった。競い合いの要素を教育に取り込むことも検討したい」と話した。

http://sankei.jp.msn.com/life/news/130822/trd13082220010015-n1.htm

LAC

# セキュリティキャンプ


セキュリティ・キャンプ中央大会2013レポート：

## 僕らのセキュリティ5日間戦争 (1/2)

8月13日～17日、4泊5日で情報セキュリティを学ぶ「セキュリティ・キャンプ中央大会2013」が千葉の幕張で開催された。その模様をお伝えする。

[谷崎朋子，@IT]

応募用紙を解析しないと応募できないクラスも：

## 「セキュリティ・キャンプ全国大会2014」、参加者募集を開始

情報処理推進機構（IPA）は2014年5月16日、22歳以下の学生・生徒を対象とする「セキュリティ・キャンプ全国大会2014」の参加者募集を開始した。応募締め切りは2014年6月16日17時だ。

[高橋睦美，@IT]

# 警察の取り組み

## 大学院生とサイバー対決　神奈川県警、犯罪対策で

日々進化するサイバー犯罪に対応するため、神奈川県警の警察官が、大学院生とサイバー技術や知識を競う競技会が14日、横浜市で開かれた。大学院側が用意した11問と、2時間半にわたって格闘した。

サイバー技術や知識の問題に取り組む神奈川県警の警察官＝14日午後、横浜市

不正アクセスの攻撃方法の解析や、コンピューターウイルス判別などの能力向上が目的。県警サイバー犯罪対策課の捜査員や技術職員と、情報セキュリティ大学院大（横浜市）の学生たちが、それぞれ4～5人のチームを2チームずつ結成して参加した。

写真データに保存されている位置情報を抽出して撮影場所を割り出したりし、解答の早さと正解数で得点を競った。

【共同通信】

http://www.47news.jp/CN/201405/CN2014051401001726.html

# 2014年、”Hardening 10 APAC”

## Hardening 10(two) APAC(Asia Pacific)は、「守る技術」とそれを支える人の価値をさらに広く訴求するための一歩を踏み出す試みです。

**沖縄は、APAC - アジアパシフィックのハブ**として知られる場所です。また、**国内外いずれからも集まりやすい**特徴もあります。3回実施してきたHardening Projectによる価値を広く訴求する優れた機会となります。すでに、全国から、システム運営技術者のエントリーが始まっています。

5/21 17:00 競技参加エントリー〆切

6/21 Hardening Day

会場：**学校法人kbc学園内会場(那覇市)**

9:30 集合　オリエンテーションとチーム編成

12:00 堅牢化競技

14:00 インターネット放送

“Hardening Project Online Conference 2014”

19:00　全チーム参加の懇親会（競技会場近辺）

6/22 Softening Day

会場：**沖縄県市町村自治会館**

10:00 全チームによる振り返りプレゼンテーション

実行委員会・オブザーバによる分析と講評

スポンサーブランド賞授与・グランプリ表彰14:30 解散

**主催：WASForum 共催：内閣府沖縄総合事務局**

**特別協力・後援　(予定含む)**

株式会社ラック、株式会社インターネットイニシアティブ、kbc国際電子ビジネス専門学校、
情報通信研究機構 サイバー攻撃対策総合研究センター（CYREC）、情報通信研究機構 北陸StarBED技術センター、
OWASP JAPAN、ISOG-J 日本セキュリティオペレーション事業者協議会、
内閣府沖縄総合事務局、沖縄県

# ITシステム運営

**ITシステム運営にかかる現実の問題を解決するのに必要なセキュリティの知識とは「壊す力」ではありません。**


**収益性($$$) = 堅牢性(安定 – 被害) × 売上 × 信頼 x …**

# Hardening Project ～守る技術の価値の最大化～

「守る技術」の価値を最大化することを目指し、最高の「守る」技術を持つトップエンジニアを発掘・顕彰するものであり、技術競技（コンペティション）の形式で実施するものです。

これにより、ウェブサイト等の安全性を追求する技術の啓蒙と人材の育成、またそうした技術の社会的認知の向上による健全なネット社会への進歩に貢献することを目指します。

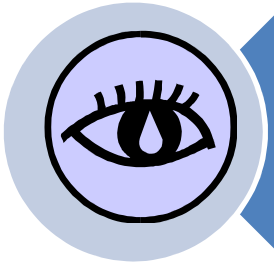
Hardening Projectは、新しい人材、新しいチーム、新しい手段を実践的に試みることにより、チームと個人の両面から、幅広い人材の挑戦の場、研鑽の場とすることをコンセプトとしています。

ビジネス継続を踏まえた防御戦略に焦点

Focus on prevention techniques

「守れる」エンジニアの顕彰と発掘

Engineering awards and discovery

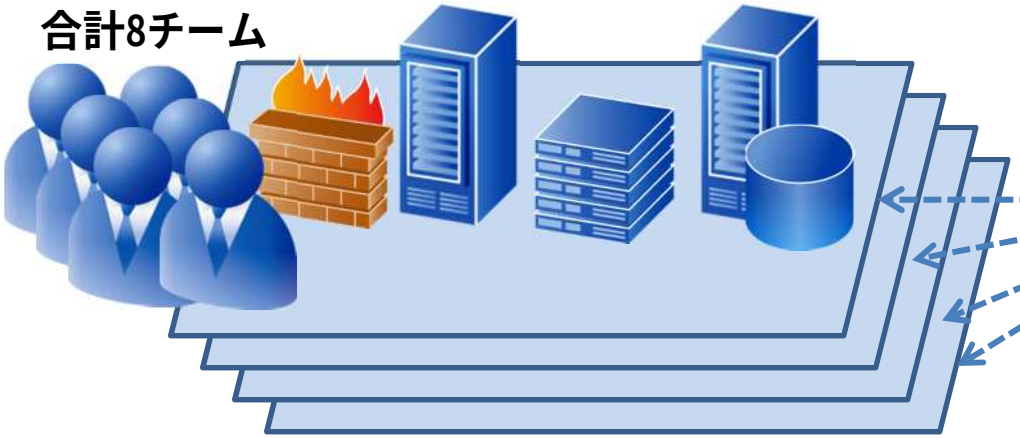


顧客・マーケット・観客の視点

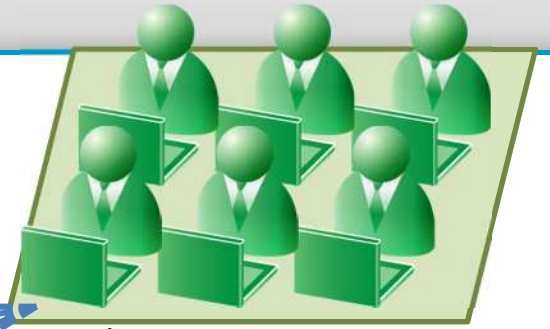
Perspective of the market

# Hardening 環境

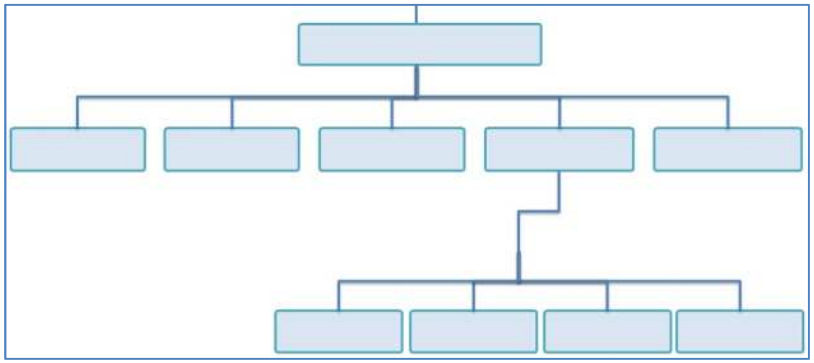
1チーム5人～ 6人
合計8チーム

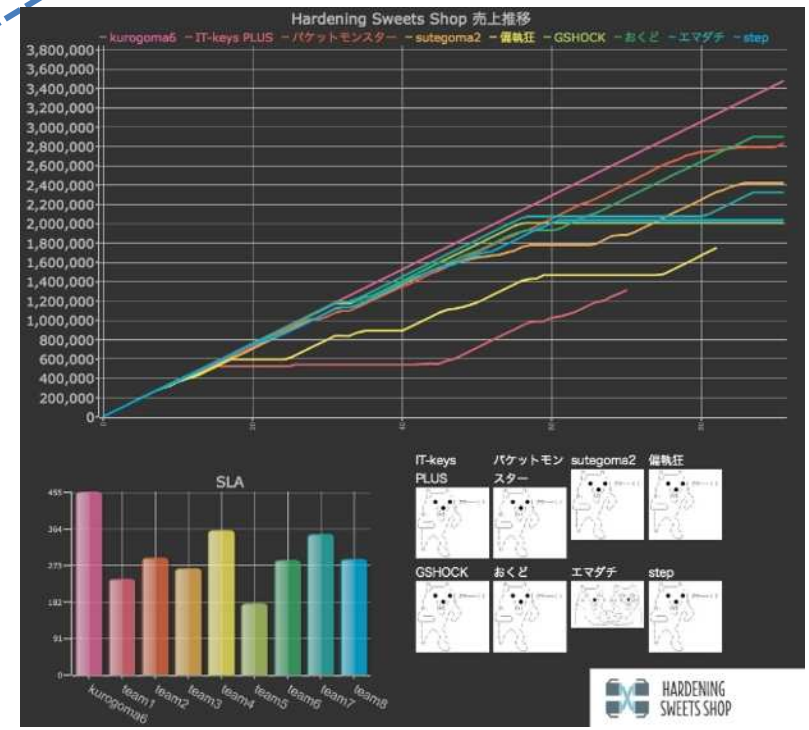


イベント発生
評価を実施



評価チーム　kuromame6






NICT StarBEDにシステムを構築
参加チームに与えられる環境

- 同じ　システム構成
- 同じ　社内システム運用ルール
- 同じ　商品
- 同じ　イベント

## 売上の推移

(限られた競技時間でどこまで伸ばせるかが勝負)

# 競技参加者が切磋琢磨し得るスキル

## 能力開発が期待できるエリア

- システム環境の状況を把握する能力
- システムの異常を発見する能力
- セキュリティインシデントを予見する能力
- セキュリティインシデントを発見する能力
- 脆弱性を発見する能力
- 脆弱性を修正する能力
- セキュリティインシデントのトリアージ能力
- チームのリソースを効率的に配分する能力
- チーム全体の（連係を含む）能力
- ユーザコミュニケーション能力
- 社内調整能力
- トラブルに負けない精神力

## 競技参加者イメージ

- 主にエンジニアの方々
- 所属団体の官民学などの属性を問いません。
- システム運用
- セキュリティインシデント対応
- ウェブ構築
- 顧客対応などの実務
- 上記の経験者あるいは関連する役割を志す方々

# 総務省 実践的サイバー防御演習 CYDER



# まとめ

**決裁者の理解を得る**
(事業継続の観点で)

**セキュリティ対策は落とし所が重要**
(予算とインパクトの兼ね合い)

**人財と情報が明暗を分ける**
(道具が同じなら使い方次第)


JSOC
JSOC
JSOC (Japan Security Operation Center)
ありがとうございました
JSOC
Japan
Security
Operation
Center