資　料　編

目　　次

発表資料

レンタルサーバのセキュリティ対策について

SAKURA internet

会社情報・数値情報

さくらインターネット株式会社

- 従業員数 495名(2017年3月)
- 売上 139億(2017年3月・連結)
- インターネットでのサーバ設置業務
  データセンターサービス
  ホスティングサービス 等を提供

サービス数値

- 共有型ホスティング
  契約件数40万件突破（2016/7）
- IaaS・VPS・占有型ホスティング
  稼働IP 11万前後

abuse（不適切な振舞の通報先）対応数値

abuse メール窓口着信数（2016年間）	数
メール受付対応数総計	約13000件
内・迷惑メール・フィッシング等	約4000件
内・セキュリティインシデント等	約4800件
内・権利侵害申立等	約3200件
内・その他法令に反するもの等	約800件

警察対応（2016年間）	数
問合せ電話対応	約700件
捜査関係事項照会書受付数	約400件
差押令状受付数	48件

対応記録管理番号発番数	数
2015年	6606件
2016年	6518件
2017年（12/14現在）	5663件

abuse窓口対応内容・対応体制

SAKURA internet

abuse 窓口が受付、対応する代表的な内容

- 違法情報・有害情報の送信防止措置 (警察, IHC, セーフライン, 他)
- 誹謗中傷・権利侵害情報等の送信防止措置、発信者情報開示、プロバイダ責任制限法対応
- 迷惑メール送信等の迷惑行為の対応
- 改ざんサイト、不正アクセス発信情報等、
  サービスのユーザーサイド・セキュリティ・インシデント対応
- 捜査関係事項照会・令状等、警察対応

窓口体制

- ネットセーフティ企画グループ・7人

「レンタルサーバ」サービス名称の種別分類とできること・できないこと

SAKURA internet

「レンタルサーバ」の種別

ユーザーがOSレベルの管理者権限を**有する**	ユーザーがOSレベルの管理者権限を**有さない**
クラウド(IaaS) 専用サーバ(占有型ホスティングサーバ, HaaS) VPS(仮想占有型ホスティングサーバ)	クラウド(PaaS, SaaS) レンタルサーバ(共有型ホスティングサーバ)

- ユーザーが「OSレベルの管理者権限を有するか否か」によりユーザーに可能な事柄の範囲が変わる
- 「レンタルサーバ」にも様々なサービス種別がある
- 「ホームページを作ることができる」「メールアカウントが作成できる」といった古典的共有型レンタルサーバと占有型サーバ・VPS・IaaSとでは可能な事柄の内実が大きく異なる

「レンタルサーバ」サービス名称の種別分類とできること・できないこと

SAKURA internet

「レンタルサーバ」のユーザーにできる事・できない事

事項	ユーザーがOS管理権限を有す	ユーザーがOS管理権限を有さない
ウェブサイトの公開	可能	可能（事業者のサービス仕様に依存）
ミドルウェアの追加インストール	可能	不可能
常駐型プログラムの実行	可能	不可能（事業者が許可しない場合が大半）
ユーザーの追加	可能	不可能（事業者のサービス仕様に依存）

「レンタルサーバ」の事業者にできる事・できない事

事項	ユーザーがOS管理権限を有す	ユーザーがOS管理権限を有さない
ログ調査	事業者は不可能	事業者が可能
個別ファイルの内容確認	事業者は不可能	事業者が可能（相当の理由がある場合に限る）
個別URLの送信防止措置	事業者は不可能	事業者が可能（例外多数）
プログラムの実行・停止	事業者は不可能	事業者が可能
ファイアウォール等の設定	事業者は不可能	事業者が可能

「不正利用」の整理

SAKURA internet

「不正利用」言葉の整理

- 社内的にも整理されていない・状況や発言者により意味が異なる

不正の4つの類型

- 虚偽の利用者情報や支払情報を用いてサービスを契約する行為・虚偽契約
- 正規利用登録者が過失により踏台にされる、ユーザーサイド・セキュリティ・インシデント
- 正規利用登録のある二次プロバイダ以下における異常
- 正規利用登録者によるグレーな利用
  法令や約款に反するとまでは言えないが適切な利用を外れている可能性のある行為

サービス契約者情報の検証・本人性確認について

契約者本人性確認. 契約時の登録電話番号有効性検証

ユーザーがOS管理者権限を有すサービスを対象に契約者情報登録電話番号の有効性検証を実施

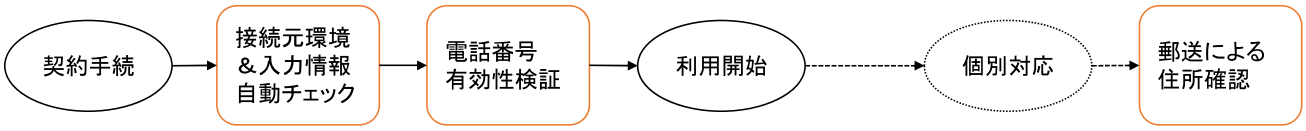
- 虚偽情報によるサービス契約を阻み、不正行為全般の発生抑止を目的とした施策
- 対象の電話番号に音声またはSMSで数字羅列のワンタイムパスワードを送信し、サービス申込サイトで同パスワードの入力を求める方式

- サービスA (2010/9 サービス開始)
  - 2017/7～ 新規ユーザー対象に電話検証開始
  - 2018(日程調整中) 全ユーザー対象としてサービス追加契約時に電話検証予定
- サービスB (2011/11 サービス開始)
  - 2011/11～ サービス提供開始時より全ユーザーに電話検証実施
- サービスC (2015/4 サービス開始)
  - 2017/8～ 全ユーザー対象としてサービス追加契約時に電話検証開始

書面郵送による契約情報登録住所の有効性確認

- 法令・約款の禁則事項に触れる可能性のあるサービス利用を認めた場合などに個別実施
- 「住所確認コード」を記した書面を郵送し、契約情報登録メールアドレスからコード記載の返信を求める
- 地方・島嶼部等は確認に時間がかかる、「宛先に訪ね当たらず」の返送受取までの期間まちまち

取組まとめ



1. 契約手続きサイト接続元環境のチェック、入力情報の型式チェック
2. 登録情報の実在確認のために電話番号の有効性検証を実施、対象とするサービス範囲は随時検討
3. 必要と判断した場合に追加して住所確認

ユーザーサイド・セキュリティ・インシデントの対応

セキュリティ・インシデントを認識するきっかけ

SAKURA internet

多くは abuse 窓口に寄せられる通報が端緒となって認識

- ポートスキャン・Bruteforce発信、迷惑メール・フィッシングメール送信等の異常通信
- ウェブサイト改ざん・フィッシングサイト・マルウェア配布サイトや、類するサイトへのリダイレクト

サービス運用保守の範囲でホスティングプロバイダが自主検出・対応するもの

- ポートスキャン・Bruteforce発信、DoS, DDoS発信
- 大量通信を発生させ正当業務行為として調査対応できるもの

困難な点

- C2, ボット等、大量通信を伴わない異常はプロバイダには検知困難
- 「正常アクセス」と「成功した不正アクセス」は対象通信の当事者でないと識別できない？

近年のabuse通報傾向

SAKURA internet

Fail2Ban を用いた自動通報が増加

- ログから認証失敗記録等を監視
  設定した回数の認証失敗が記録された場合に iptables 等で遮断するソフトウェア
- http access_log 類も監視設定可能、
  各種インジェクションコマンド類も設定次第で遮断可能
- 遮断時、blocklist.de, badips.com, dshield.org 等のブラックリストにレポーティングする機能を同梱
- 簡易IDS
  遮断発動時、指定したアドレス宛にメール通知することが可能
- **sendmail.conf を弄って、通知先をIP管理事業者に向ける人が居る**
- 連絡先情報確認は abusix https://www.abusix.com/contactdb を使用する例が多い様子？
- 攻撃者に攻撃用の踏み台を入手させないことが第一歩で有用
  通知が得られれば事業者は対応できる

究極の方向性は事業者がabuse通報受付APIを設けること？

```
[root@centos7]# yum install epel
[root@centos7]# yum install firewalld fail2ban
[root@centos7]# systemctl start firewalld
[root@centos7]# systemctl enable firewalld
[root@centos7]# cp /etc/fail2ban/jail{.conf,.local}
[root@centos7]# vi /etc/fail2ban/jail.local
[root@www fail2ban]# diff -u /etc/fail2ban/jail{.conf,.local}
--- jail.conf
+++ jail.local
@@ -226,6 +226,7 @@
 port    = ssh
 logpath = %(sshd_log)s
 backend = %(sshd_backend)s
+enabled = yes

[root@centos7]# systemctl start fail2ban
[root@centos7]# systemctl enable fail2ban
```

```
[root@www fail2ban]# ls /etc/fail2ban/action.d/*.conf
/etc/fail2ban/action.d/badips.conf
/etc/fail2ban/action.d/blocklist_de.conf
/etc/fail2ban/action.d/dshield.conf
/etc/fail2ban/action.d/sendmail.conf
```

```
$ dig www.sakura.ad.jp +short
163.43.24.70
$ dig 70.24.43.163.abuse-contacts.abusix.org txt +short
"hostmaster@nic.ad.jp"
```

当社におけるインシデント警戒・早期検出の取組

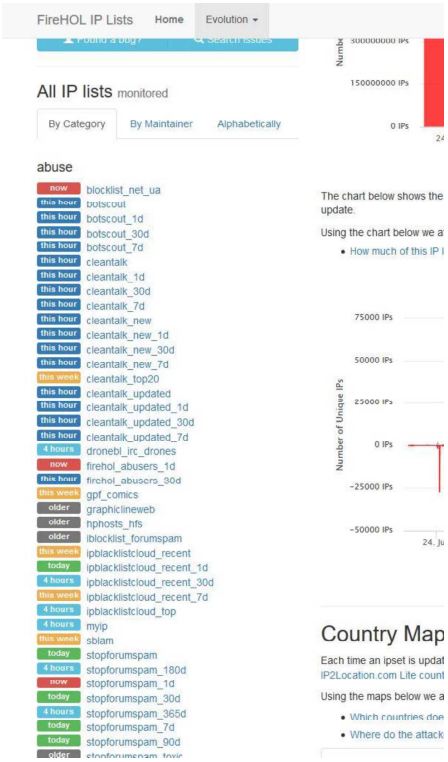
SAKURA internet

外部のブロックリスト・ブラックリストをモニター

- 迷惑メールのブロックリストはホスティングサービスのメール不達と直結することから従来よりモニターを実施
- その他のリストも調査・警戒

FireHOL IP Lists（http://iplists.firehol.org/）

- iptables + ipsetを補助するOSS、多種多様なブロックリスト横断収集してgitに公開
- CleanTalk, StopForumSpam, Blocklist.de, nix_spam, 従来より有益と認めていたリストの大半を網羅している、他に有益性未調査のリストも多数
- IPアドレス記載形式が ipset コマンド用に統一されており利用しやすい
- update-ipsets コマンドでリストを一気にぶっこぬく、
サービス運用IPと照合
- どのリストが役に立つかは地道な評価が必要
C2類は過去検出記録が混在、誤検出もあり、情報確度は個別検討必要
- 本情報のみでの被疑サイト・IPの通信停止は適切でないが、通信の秘密を侵害せずに得られる情報として有益
他のリストやabuse窓口通報等と組み合わせて判断



13

まとめ

SAKURA internet

- 外部のブロックリスト・ブラックリストを警戒することで一定の効果は得られる
- どのリストで何が検出でき、どの程度の鮮度と確度があるかの評価には時間がかかる
- それでもなお、C2の「実体がある」か否かの判断は非常に難しい
ユーザーがOS管理者権限を有するサービスでは実体有無の確定判断が原理的に困難

- 大量通信を伴わないインシデントは検出困難、通信の秘密を順守する観点から調査不可能
- 成功した不正アクセスはブロックリストに記録されない、成功した不正アクセスが問題
通秘順守の観点からプロバイダの自主検出には限界がある、外部から提供される情報が貴重
→ 関係者と情報連携する術が無いか？

- 不正アクセスに類する通信記録は提供者からの第三者転送同意が得られ難く、サービス契約者への通知指摘が難しい
→ 契約者に関する情報を開示する仕組みが設けられると良い？

14

GMOインターネットグループのご紹介と Abuse対策の現状報告

すべての人にインターネット

GMO INTERNET

2018年12月18日現在

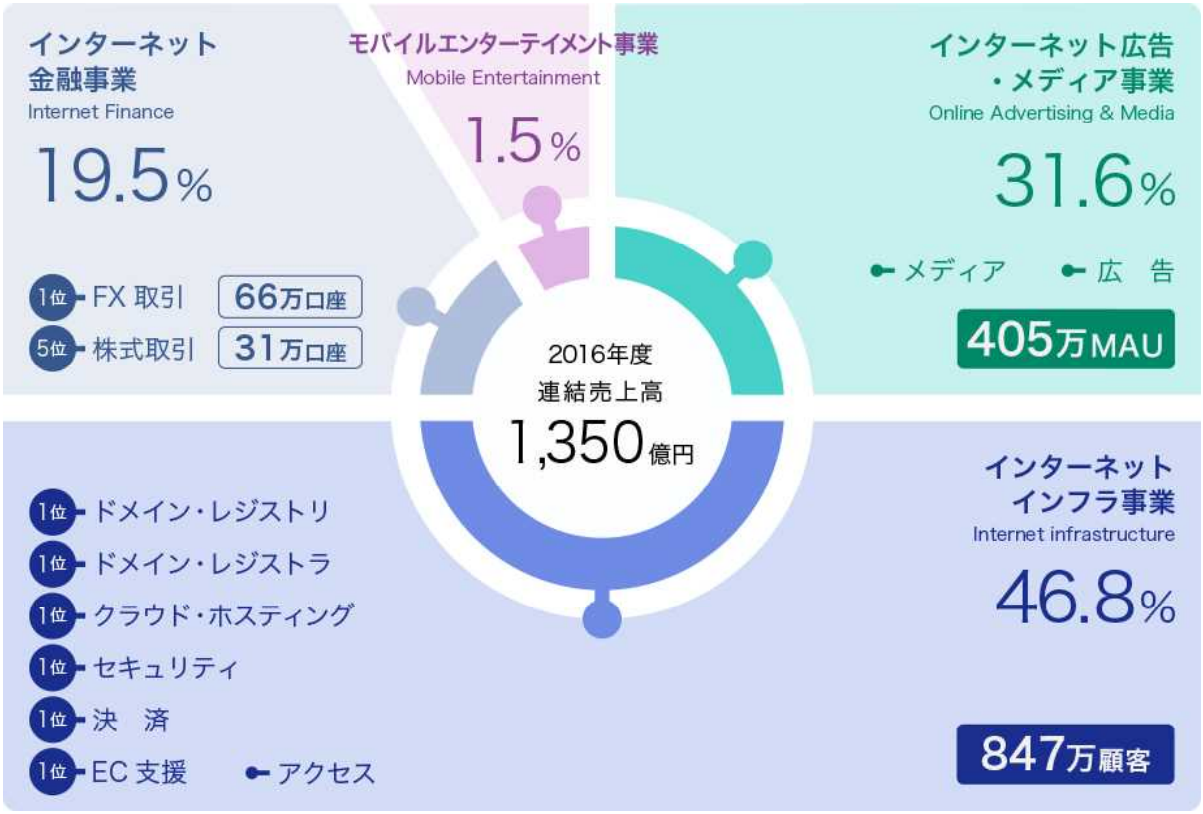
流れ

1. GMOインターネットグループのご紹介
   - ・グループ概要
   - ・セグメント別事業概要
2. GMOインターネットグループのホスティング事業
3. 当社ホスティング事業のAbuse対策
4. 不正申し込みへの対策について

グループ概要

本社	GMOインターネット株式会社
代表者	代表取締役会長兼社長　グループ代表　熊谷 正寿
本社所在地	東京都渋谷区桜丘町26-1　セルリアンタワー
設立	1991年5月24日
証券コード	9449（東京証券取引市場第一部）
事業内容	インターネットインフラ事業 インターネット広告・メディア事業 インターネット金融事業 モバイルエンターテインメント事業
資本金	50億円
連結従業員数	5,278名
グループ会社数	連結106社（2017年9月時点）

セグメント別事業概要



※売上比率はセグメント間取引消去前の数値で算出

GMOインターネットグループの
ホスティング事業について

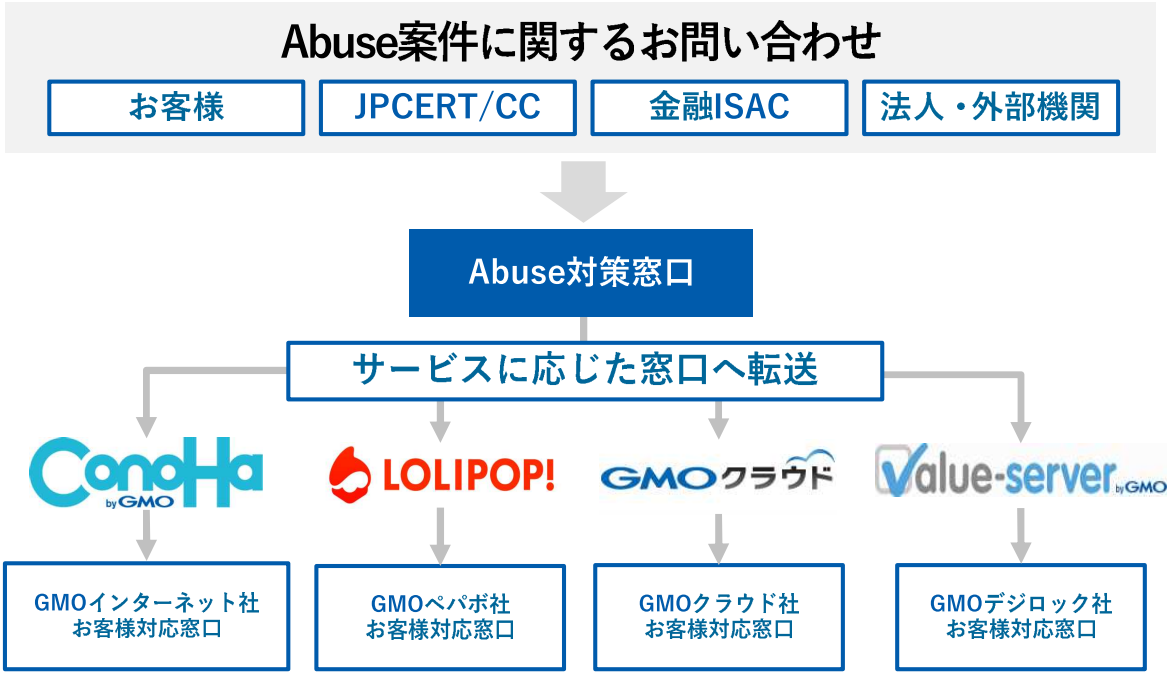
GMOインターネットグループのホスティング事業

GMO INTERNET GROUP

グループ各社それぞれ特徴の異なる
ホスティングサービスを運用

GMOインターネット	ConoHa by GMO / お名前.com レンタルサーバー by GMO / GMOアプリクラウド
GMOクラウド	GMOクラウド
GMOペパボ	LOLIPOP!
GMOデジロック	Value-server by GMO

Abuse対策窓口にお問い合わせがあった場合
内容に応じてグループ各社のお客様対応窓口へ対応を依頼



GMOインターネット
ホスティング事業の
Abuse対策

当社ホスティング事業のAbuse対策内容

前提

通信の秘密を厳密に守らなければならない
違法とならない範囲での対応・対策

共用

・サーバーのログなどで、ある程度は判明できる
・サーバー内に、どのようなファイルが設置されているかわかるが
お客様個別の同意なくサーバー領域は入れず検知・不正の判断が難しい

VPS

お客様が独自でサーバー構築を行っており、通信内容で検知が難しい

当社環境
共用サーバー　VPS

通信 → 通信内容がわからない
正当？　不正？？

当社ホスティング事業のAbuse対策内容

1 **vIDS＆FWの運用**

不正IP通信検知、内部からのアタック検知と防御

2 **DDoS対策機器の運用**（大量通信等、攻撃通信にかかる遮断）

外部からの攻撃（DDoS）の検知
検知した攻撃元から通信を自動制御

3 **共用サーバー（共用サーバーSD）にWAFの提供開始**

自動WordPressインストールに標準適用することで、
WordPressやプラグインの脆弱性による
不正プログラムの設置が減少。

当社ホスティング事業のAbuse対策内容

4 外部ブラックリストへの照会

ブラックリストに掲載されているIPアドレスやドメインから、 お客様環境の不正プログラムの設置や不正利用を確認、対応する。

5 外部機関からの通報

JPCERT/CCや金融ISACから調査依頼があった場合は、対象サーバーの調査と契約者への事実確認を行い、サービス規約に基づいて都度対応している。

Abuse対策の課題

通信の秘密を保護し、正当業務行為内において対応しなければならない。一方、違法性や損害賠償リスクがある

正当な通信か、不正な通信か判断が困難
→ サーバーを停止するというのは、多大な影響が発生する
事業者への損害賠償請求のリスクがつきまとう

個別の通信についてその特性等を把握することは、通信の秘密の侵害（知得）、把握した内容に基づき当該特性に合致する通信の遮断は通信の秘密侵害（窃用）となる
→ トラフィックで判断せざるを得ない

通信当事者（契約者）の同意は、利用規約等に基づく事前の包括同意のみでは一般的に有効な同意とされていない。不正かな？と思っても契約者の同意が得られないと契約領域に入れない
→ 包括同意の有効性が争われる可能性がある状況において
予測不能な特定の契約者領域にどうアプローチするのか

不正申し込みへの対策について

不正申し込みへの対策について

GMO INTERNET GROUP

対応	電話認証の導入（※VPS）
目的	クレジットカードの不正利用による、 チャージバックを発生させない目的と本人 確認を目的として導入
効果	架空の情報（連絡先電話番号）で申込み不可
結果	クレジットカードの不正利用による申込が減少

※不正利用者に関しては、申込み情報を保有・管理し、
同じ情報での申込みを制限。

電話認証の課題

不正申し込みは減少したが・・・

現状
・050など気軽に電話番号を発行可能
・電話番号転送サービスなどで海外にも転送が可能

実効性の問題

不正利用について

事業者が不正かどうか判断できる情報があるとよい。
（不正ＩＰリスト？リストではなく判断基準でも）そのデータを基に対応した場合の免責があると、対策までの時間が短縮される。

本人確認について

サービスの提供に影響を及ぼさないことを前提としたインターネット上で、迅速に本人確認が行える仕組みがあるとよい。

ボットネット

JPCERTコーディネーションセンター
理事　　水越一郎

JPCERT/CCとは

一般社団法人　JPCERTコーディネーションセンター

Japan Computer Emergency Response Team Coordination Center
ジェーピーサート コーディネーションセンター

- 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、ソフトウエア製品開発者等（主に、情報セキュリティ担当者）がサービス対象
- 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、ソフトウエアや情報システム・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（窓口CSIRT）

CSIRT: Computer Security Incident Response Team

※各国に同様の窓口となるCSIRTが存在する(米国のUS-CERT、CERT/CC、中国のCNCERT, 韓国のKrCERT/CC、等)

- 経済産業省からの委託事業として、サイバー攻撃等国際連携対応調整事業を実施

Botネットの特徴

- 対象システムを乗っ取る
- 乗っ取ったシステムをC2サーバ
  (Command and Control server)から制御して、悪事を働く
- C2サーバは多数のシステムを制御する

悪事の種類

- DDoS
  パケットを投げつけて攻撃対象を機能不全に
- スパムメール
  スパムメールの送信エンジン
- アドウェア(?)
  多数マシンからアクセスして広告収入
- スパイウェア
  (多数)ユーザの情報収集(パスワード等含む)
- 違法サイト構築
  中継サーバとして違法サイトへの転送

Mirai

- IoTデバイスを乗っ取る(出荷時のパスワード等)
- ソースコードが公開される 2016/9/30
  乗っ取り方法 + C2サーバの公開 →
  プラットフォーム全体を構築可能
- 実際の大規模攻撃に使われた模様

近隣国の金融機関に対するDDoS脅迫

『Armada Collective を名乗る攻撃者からの DDoS 攻撃に関する情報』

https://www.jpcert.or.jp/newsflash/2017062901.html

- 2017年6月後半に中国や韓国の金融機関に対して脅迫メールが届く
- 2015年頃に見られたDDoS脅迫との共通性
- 予備攻撃が観測される（報道によると、本攻撃はなかった）

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

In past, we launched one of the largest attacks in Switzerland's history. Use Google.

All network of [redacted] will be DDoS-ed starting [redacted]. if you don't pay 10 Bitcoins @ [redacted]

When we say all, we mean all - users will not be able to use any of your services.

Right now we will start 15 minutes attack on one of your IPs ([redacted]). It will not be hard, we will not crash it at the moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a hoax. Check your logs!

If you don't pay by [redacted], attack will start, price to stop will increase to 20 BTC and will go up 10 BTC for every day of attack.

If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long
time.

This is not a joke.

Our attacks are extremely powerful - our Mirai botnet can reach over 1 Tbps per second. So, no protection will help.

Prevent it all with just 10 BTC @ [redacted]

Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

our **Mirai** botnet can reach over 1 Tbps per second.

攻撃事例

- 2016年9月 Sucuri社(セキュリティー会社)顧客へ
  12万 HTTP RPS

- 2016年9月18-20日　OVH(ホスティング会社)へ

990Gbps～1.1Tbps

(Miraiの能力1.5Tbps)

日本のインターネット通信量(総務省発表 2017年5月)

9.6T

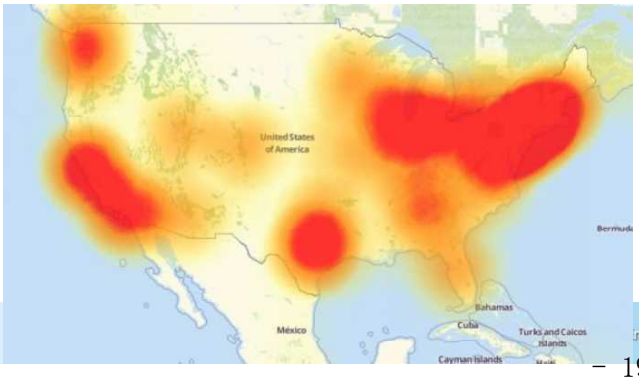
2016/10/21

- Dyn社　DNS プラットフォームへの攻撃

- 同社のプラットフォームを利用するTwitter, Reddit, GitHub, Spotify等へのアクセス障害が発生

- 攻撃規模は未検証ながら

10万台規模、1.2Tbps

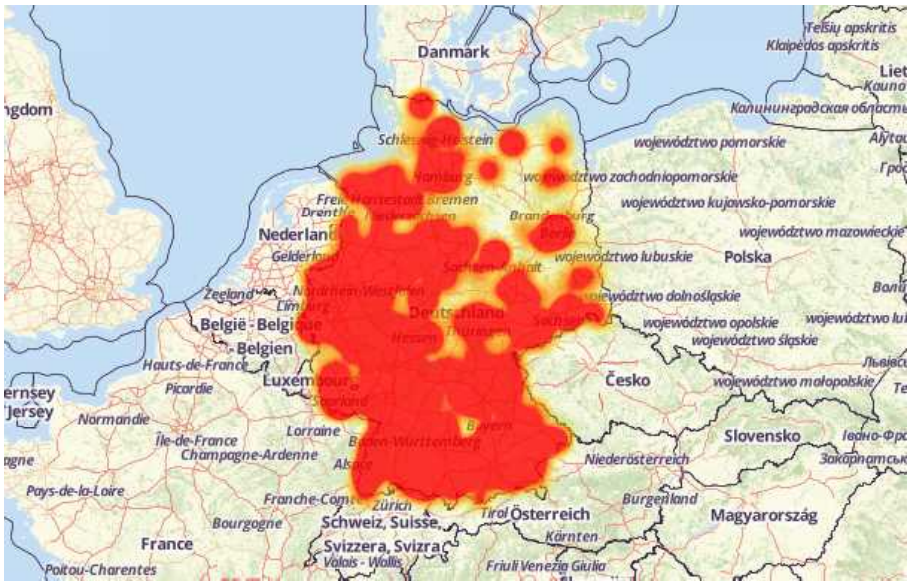


Dyn社に対する攻撃の影響

https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/より

2016/11/27

- ドイツテレコム
  90万台 (全顧客の4%)の家庭用ルータが動作停止



出典:「More than 900k routers of Deutsche Telekom German users went offline」
http://securityaffairs.co/wordpress/53871/iot/deutsche-telekom-hack.html

ドイツテレコム　発表

- パスワードではなく、新たな脆弱性を突かれた
- ダウンではなくルータへの感染が目的
- 感染しないが、過負荷でダウン

- ネットワークで感染パケットを遮断
- 更新ソフトをベンダーが開発
- 即日ソフトウェア配布開始
- 代替手段として携帯回線を１日無料に

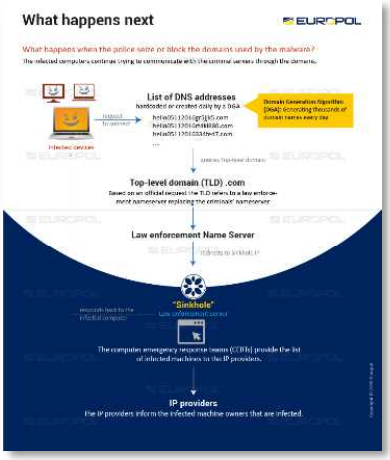
国際的な
ボットネットテイクダウン作戦

国際的なボットネットテイクダウン作戦

【2014年6月】アメリカ合衆国国土安全保障省やFBIなど、複数の企業や組織が協力しGameOver ZeuSボットネットの対策を実施。

【2016年11月】ドイツ警察が中心となり、関係各国が連携してインターネットバンキングに係わる不正送金事犯の実行者を検挙する国際的な取組「Operation Avalanche」を実施。

https://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted

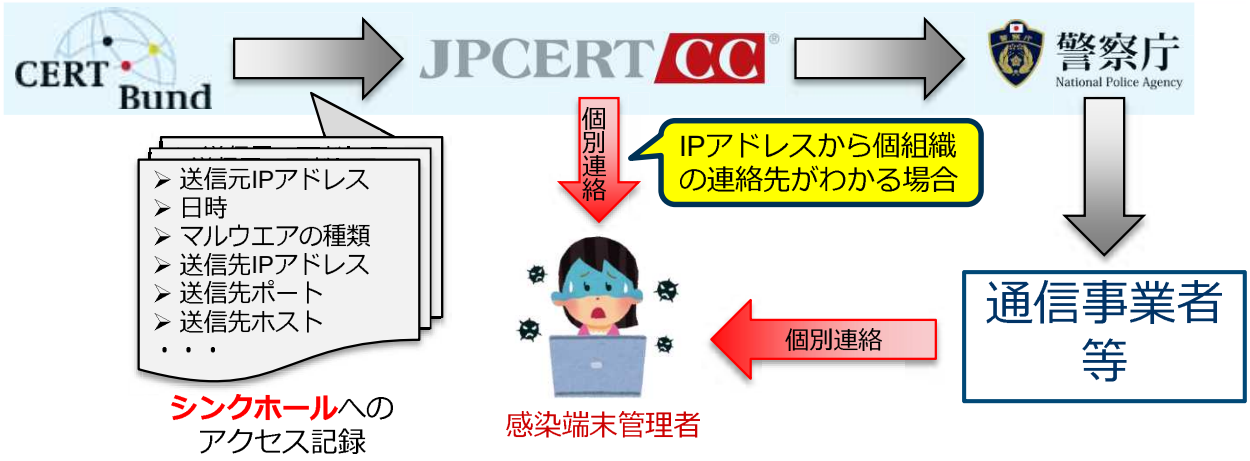


https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation

Operation Avalanche

- 2016年11月30日：EuropolなどがFBI、ドイツ警察および30地域のパートナーと協力してAvalancheを解体したと発表
  - Avalancheボットネットとは
    - 20種類のボットネットが存在し、マルウェア等の配布に使用
    - マルウエアの感染者は180ヶ国にのぼる
  - Avalancheボットネットの解体
    - 5人の容疑者を逮捕（うち1人が首謀者の可能性）
    - 39のサーバを押収、221のホスティングサーバをオフライン
    - 使用されていたドメインを**シンクホール化** or ブロック
    - 解体までに費やした捜査期間は4年以上
- 2017年3月23日：警察庁、総務省、ICT-ISAC、JPCERT/CCが国内における取り組みについて発表
  - 警察庁「インターネットバンキングに係わる不正送金の国際的な被害防止対策」
    http://www.npa.go.jp/cyber/avalanche/index.html
  - 総務省「インターネットバンキングに係るマルウェアに感染した端末の利用者に対する注意喚起の実施」
    http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000120.html
  - ICT-ISAC「インターネットバンキングに係るマルウェア感染者に対する注意喚起について」
    https://www.ict-isac.jp/news/news20170323.html
  - JPCERT/CC「インターネットバンキングに係わる不正送金の国際的な被害防止対策に協力」
    https://www.jpcert.or.jp/press/2017/20170323-avalanche.html

日本国内での取り組み



Botネット対策(乱暴な私案)

- 端末
  感染させない、駆除する
- ネットワーク
  発見する、追跡する
- C2サーバ
  発見する、制御する、逮捕する

ご清聴ありがとうございました

ボットネット・テイクダウンにおけるシンクホール実施等に関する法的課題

首都大学東京　都市教養学部法学系
星　周一郎

H30.2.20 サイバーセキュリティ政策会議

1「捜査」としてのシンクホール実施

2 ボットとC&Cサーバの通信状況把握

3 検証としてのシンクホールの実施

4 レジストリでの対応の可能性

１「捜査」としてのシンクホール実施

・シンクホールの実施（Sinkholing）
　感染端末とC&Cサーバとの通信遮断
　警察等管理サーバへのリダイレクト

＊米国マイクロソフト社の実施例
　　著作権侵害等に基づく民事訴訟

１「捜査」としてのシンクホール実施

・「捜査」の一環として行うことは可能？
　ボットネットを使用した不正送金
　　→電子計算機使用詐欺（刑246の2）
　ボットネットを使用したDDoS攻撃
　　→電算機損壊等業務妨害（刑234の2）

・現行刑事手続法において可能か？

2 ボットとC&Cサーバの通信状況把握

- 「通信の秘密」との関係
  - ①感染端末使用者からの通報
    - →当該感染端末とC&C サーバ間の通信
      - 「通信当事者の意思に反しない利用」
      - 通信の秘密の侵害に該当しない
        - ＊ガイドライン4版
      - 通信状況の把握–実況見分

2 ボットとC&Cサーバの通信状況把握

- 「通信の秘密」との関係
  - ②ボットネット全体の状況把握
    - →他のボットとC&C サーバ間の通信状況
      - 「通信」の両当事者の有効な同意なし
      - 「通信の秘密」との調整が必要

2 ボットとC&Cサーバの通信状況把握

- 「通信の秘密」との関係
  - ②違法性阻却事由にあたるか
    - 一般的には「緊急避難」該当性なし
    - 正当行為（法令行為）の該当性
      - →「検証」（刑訴法222条→128条）
    - ＊最決平11・12・16刑集53巻9号1327頁

3 検証としてのシンクホールの実施

- シンクホールの実施
  - 検証を実施するための「必要な処分」
    - 刑訴法129条

      検証については、身体の検査、死体の解剖、墳墓の発掘、物の破壊その他必要な処分をすることができる。
  - 「検証の目的を達する上で最小限度」
  - 「社会通念に従って妥当なもの」
  - ＊物の破壊可能←→プライバシーの利益

3 検証としてのシンクホールの実施

- 国外にC&Cサーバ・レジストリが存在
  当該国に必要な措置を講ずるよう協力依頼
- C&Cサーバは国外、レジストリは国内
  令状呈示は国内レジストリだけで良いか
    ＊手続の公正担保・被処分者人権保障
  cf. 通信傍受法
    管理者への令状呈示＋当事者への通知

3 検証としてのシンクホールの実施

- 「検証依存」傾向
- 立法論的検討の必要性？

4 レジストリでの対応の可能性

- 現在の刑事手続法では困難か？
  - cf. アメリカでの状況
- JPRSでの対応の可能性
  - ex. 社会的許容性を欠く場合の登録取消
    - JPRSを対象にした差止請求（停止）