サイバーセキュリティ BoF #6

議論の活発化のため事前アンケートにご協力ください

前の席にどうぞ！

JANOG45
サイバーセキュリティBoF#6

サイバー犯罪に悪用される日本国内の『踏み台』の実態と対応

JPCERT CC
Japan Computer Emergency Response Team Coordination Center
JPCERT コーディネーションセンター

capy

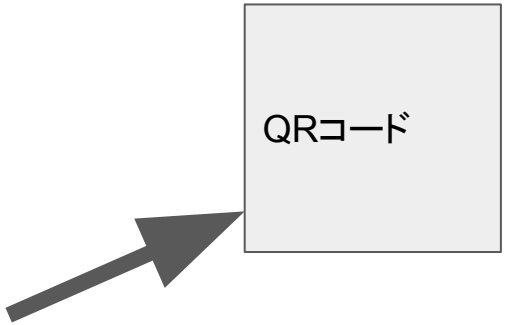
GMOペパボ

KDDI
KDDI Web Communications

NTT Communications
NTTコミュニケーションズグループ
NTTコム エンジニアリング株式会社

2020年1月22日

質問、わからない単語など
バシバシかいてください
他の質問に「👍」もしてねー



JANOG Slack で #j45サイバーセキュリティbof チャンネルもあります！

スライドは後日JANOGサイトに公開予定です

発表者

安部 広夢（一般社団法人JPCERTコーディネーションセンター）

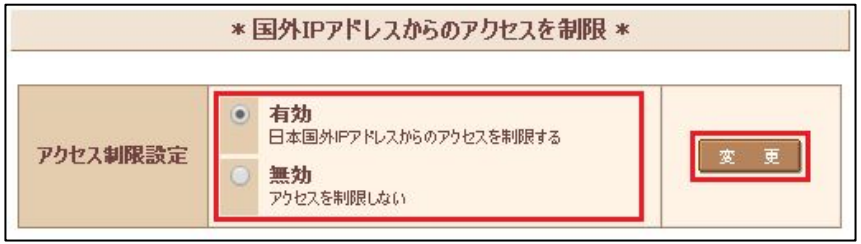
熊野 多聞（GMOペパボ株式会社）

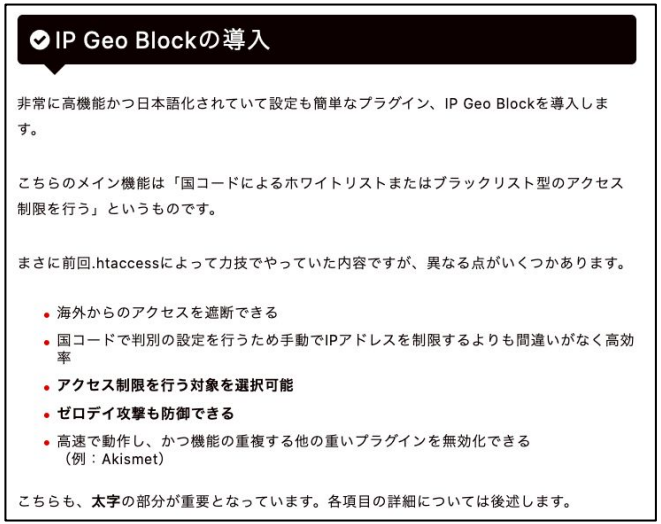
近藤 和弘（NTTコムエンジニアリング株式会社）

松本 悦宜（Capy株式会社）

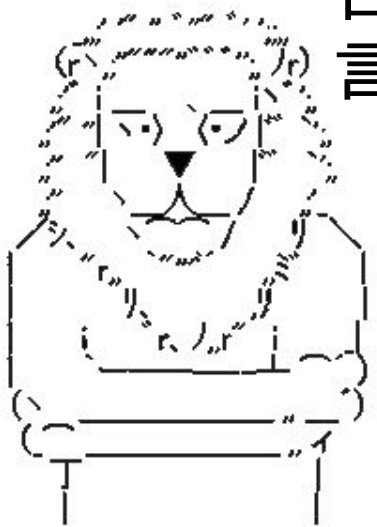
森川 慶彦（株式会社KDDIウェブコミュニケーションズ）

はじめに



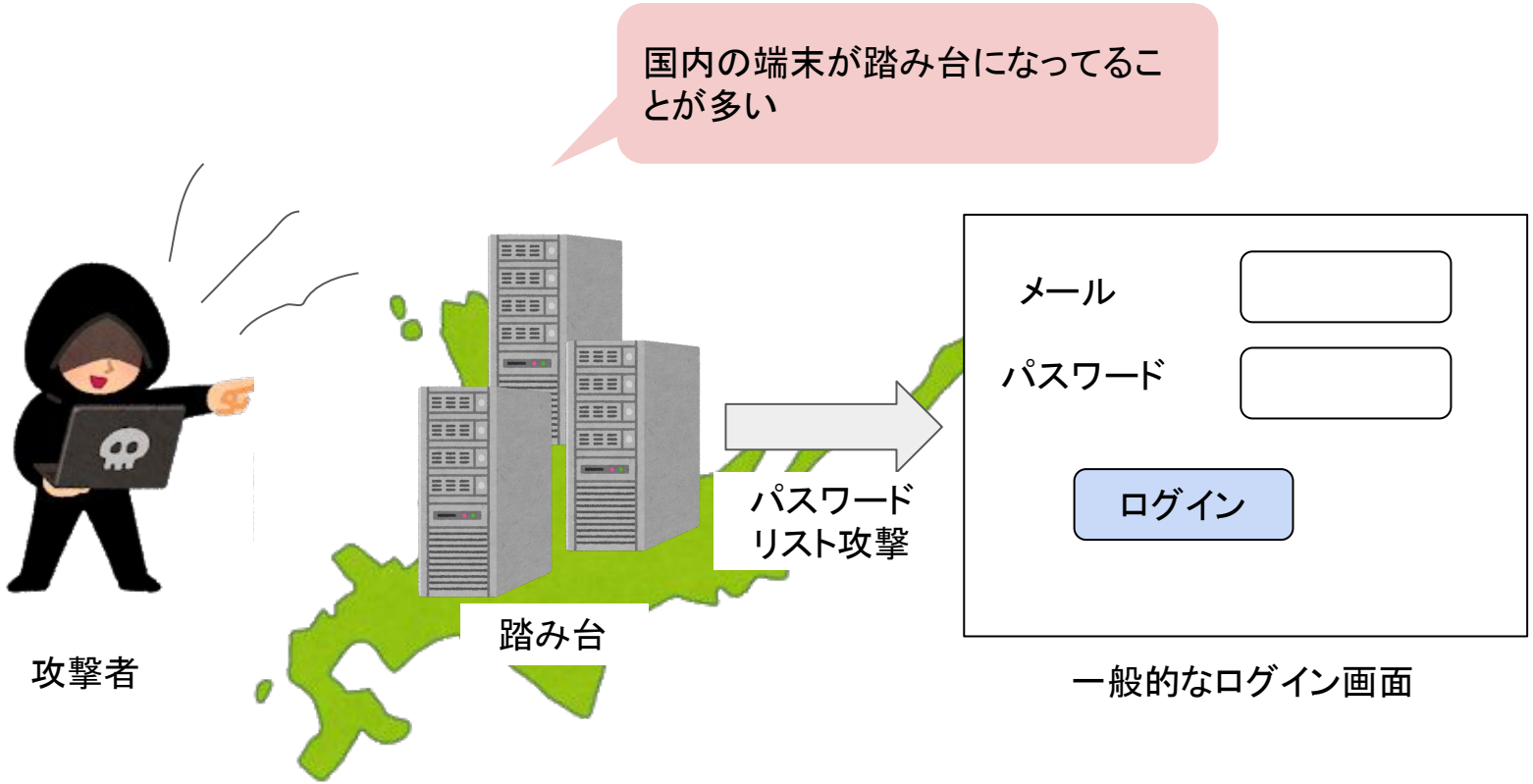


おまえ
日本のIPが安全って
言えるの？



出典：某サイト

はじめに（国内IPアドレスが踏み台に）



本日議論したいテーマ

攻撃が激化

国内のIPアドレスを使用した攻撃が継続して行われる
脆弱性を用いた例や偽造証書を使用して不正契約を行う事例が見受けられる

※ Abuse

不正使用や乱用などを意味し、インターネット上での迷惑行為やその行為を通報する事業者に設置された窓口のこと。本BoFでは、事業者がAbuse（迷惑行為）の通報を第三者から受付けること、またはその迷惑行為自体を示すことがある。

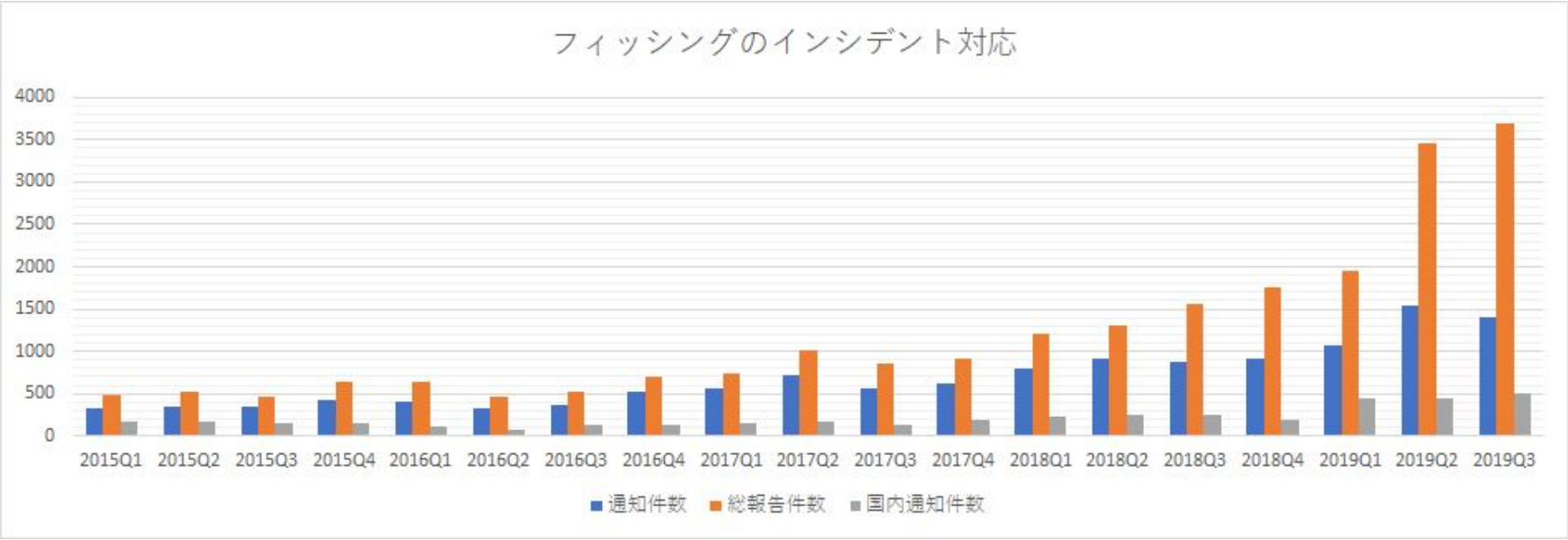
実際のデータ

```
Delivered-To: info@*******.co.jp
Received: (qmail 79054 invoked from network); 26 Nov 2019 13:49:28 +0900
Received: from unknown (HELO *****.secure.ne.jp) (122.200.***.***)
  by 0 with SMTP; 26 Nov 2019 13:49:28 +0900
Received: from p**d05.*******.ne.jp ([202.***.***.202])
  by *****.secure.ne.jp with ESMTP/TLS/ECDHE-RSA-AES256-GCM-SHA384; 26 Nov 2019 13:49:28 +0900
Received: from p**d05.*******.ne.jp (localhost.localdomain [127.0.0.1])
    by p**d05.*******.ne.jp (Proxmox) with ESMTP id 4CE0951499C7
    for <info@*******.co.jp>; Tue, 26 Nov 2019 13:49:28 +0900 (JST)
Received: from w**4.*******.ne.jp (w**4.*******.ne.jp [202.***.***.66])
    by p**d05.*******.ne.jp (Proxmox) with ESMTPS id DBADF5142EED
    for <info@*******.co.jp>; Tue, 26 Nov 2019 13:49:24 +0900 (JST)
Received: from w**4.*******.ne.jp (localhost [127.0.0.1])
    by w**4.*******.ne.jp (Postfix) with ESMTP id 8E912C05EA
    for <info@*******.co.jp>; Tue, 26 Nov 2019 13:47:50 +0900 (JST)
Received: from [127.0.0.1] (unknown [13.***.23.230])
    by w**4.*******.ne.jp (Postfix) with ESMTPSA id 75536C05D9
    for <info@*******.co.jp>; Tue, 26 Nov 2019 13:47:50 +0900 (JST)
From: CPI <*******>
To: info@*******.co.jp
```

ホスティングサービスの利用者に届いた
サービス用コンパネを模したフィッシングサイトへ
誘導するメールヘッダ。

中国のIP（13.***.23.230）から国内の別ホスティング
事業者のサーバ（w**4.*******.ne.jp [202.***.***.66]）を
踏み台として送信されている。

JPCERT/CCのデータから見えること



IPアドレスやドメインの管理者に通知をしています

JPCERT/CCのデータから見えること

	2015Q1	2015Q2	2015Q3	2015Q4	2016Q1	2016Q2	2016Q3	2016Q4	2017Q1	2017Q2	2017Q3
国内	52%	48%	46%	35%	30%	25%	38%	27%	26%	24%	25%
海外	48%	52%	54%	65%	70%	75%	62%	73%	74%	76%	75%
通知件数	330	355	349	421	399	334	364	525	559	722	557
総報告件数	491	522	474	645	642	467	521	707	736	1011	852
国内通知件数	171.6	170.4	160.54	147.35	119.7	83.5	138.32	141.75	145.34	173.28	139.25

2017Q4	2018Q1	2018Q2	2018Q3	2018Q4	2019Q1	2019Q2	2019Q3
30%	30%	27%	28%	21%	41%	29%	36%
70%	70%	73%	72%	79%	59%	71%	64%
617	789	909	878	912	1077	1546	1398
924	1214	1302	1560	1753	1947	3457	3700
185.1	236.7	245.43	245.84	191.52	441.57	448.34	503.28

事業者の行うabuse対応

Abuse行為を受けたor見聞した人から

直接の被害者からも連絡がありますが、被害者でなくともフィッシングサイト等を見つけた人からも連絡があります。

対応依頼を受け

メールやフォームで受け付けた対応依頼の内容(発信者IPアドレス・URL・メールアドレス等)からユーザを特定します。

約款・規約等に基づいた契約者対応を行う

行為が契約約款や利用規約に抵触するかを判断し、抵触している場合は、注意や利用停止・契約解除等の対応をとります。

事例紹介：解析プログラム

「リスト型攻撃」新たなプログラム判明 効率的に不正接続か
https://www3.nhk.or.jp/news/html/20200116/k10012247401000.html
メール内容から利用サービスを割り出しするリスト型攻撃についてまとめてみた
https://piyolog.hatenadiary.jp/entry/2020/01/16/145913

事例紹介：正面突破で契約してくる

JPドメインを使用した

フィッシングサイトが増えている

本人確認は実は難しい

例）偽造証書、日本のSIM

見分けられますか？

```
[Querying whois.jprs.jp]
[whois.jprs.jp]
[ JPRS database provides information on network administration. Its use is    ]
[ restricted to network administration purposes. For further information,     ]
[ use 'whois -h whois.jprs.jp help'. To suppress Japanese output, add'/e'     ]
[ at the end of command, e.g. 'whois -h whois.jprs.jp xxx/e'.                 ]

Domain Information:
[Domain Name]                   [redacted].JP

[Registrant]                    sonoda[redacted]

[Name Server]
[Signing Key]

[Created on]                    2019/09/24
[Expires on]                    2020/09/30
[Status]                        Active
[Last Updated]                  2019/09/24 14:58:46 (JST)

Contact Information:
[Name]                          SAKURA Internet Inc.
[Email]                         nic-staff@sakura.ad.jp
[Web Page]
[Postal code]                   530-0011
[Postal Address]                Osaka
                                Osaka
                                35F,4-20,ofukacho,kitaku
[Phone]                         06-6376-4800
[Fax]
```

本人確認の例

「本人確認」の例はいろいろあります

・SMS認証

・書類の提出

・架電

・郵送

・eKYCって何？

本人確認方法の対応表

	A社	B社	C社
ドメイン	✕	○	✕
レンタルサーバ	○	○	✕
VPS	―	―	○
電話系	❁	―	―
メール	―	―	✕
サイトジェネレーター	✕	✕	―

凡例

○メール以外の確認

❁書類提出

✕なすがまま

― 提供していない

Abuseを活用してください

受信窓口

- **株式会社KDDIウェブコミュニケーションズ**
  メール abuse@cpi.ad.jp
- **NTT Communications (OCN)**
  webフォーム https://www.ocn.ne.jp/info/rules/abuse/
  メール abuse@ocn.ad.jp
- **さくらインターネット株式会社**
  abuseフォーム https://abuse.sakura.ad.jp/
  メール abuse@sakura.ad.jp
- **JPCERT/CC**
  インシデント対応窓口 https://www.jpcert.or.jp/form/

IPv4 over IPv6 時代のユーザ特定の課題

IPv4 over IPv6 (≒CGN)の利用が**拡大**

特定に必要な情報は
v4アドレス　＋　時刻情報　＋
α（SRCポート）
v4アドレスだけでは特定不可

でもNATログはPPPログよりも膨大　で　保管期間は「？」検索性は「？」

⇒ **v4アドレス＋SRCポートの記録は解決策ではない**

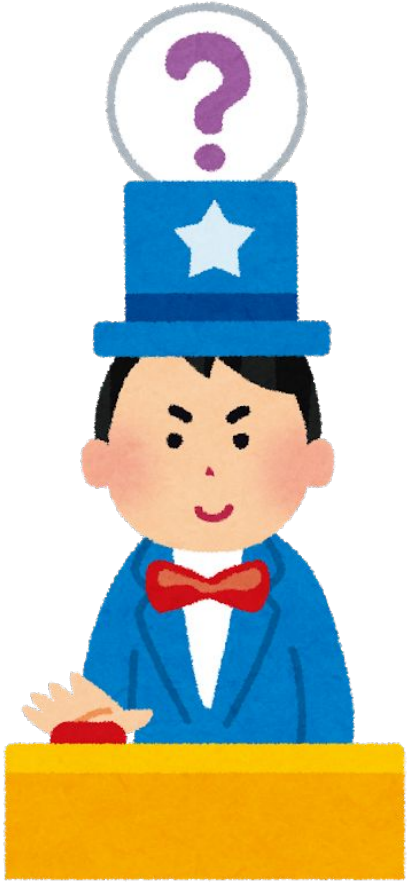
会場へ
提言

自社のサービスを守るために**サービスのIPv6対応**を

IPv4 over IPv6サービスは当然IPv6利用可能が前提。IPv6であればグローバルアドレスが割り当てられるためユーザ特定できる可能性が高い。

ユーザ特定できないのであれば、事業者へabuse申告・警察へ被害届してもその後の対応が困難に。

アンケート結果



slido

来場者からの
質問
コーナー

Audience Q&A Session

事後アンケートもお願いします！

感想、
聞いてみたかったこと、
次回以降に期待したい内容など、
ぜひご意見ください！
よろしくお願いします。