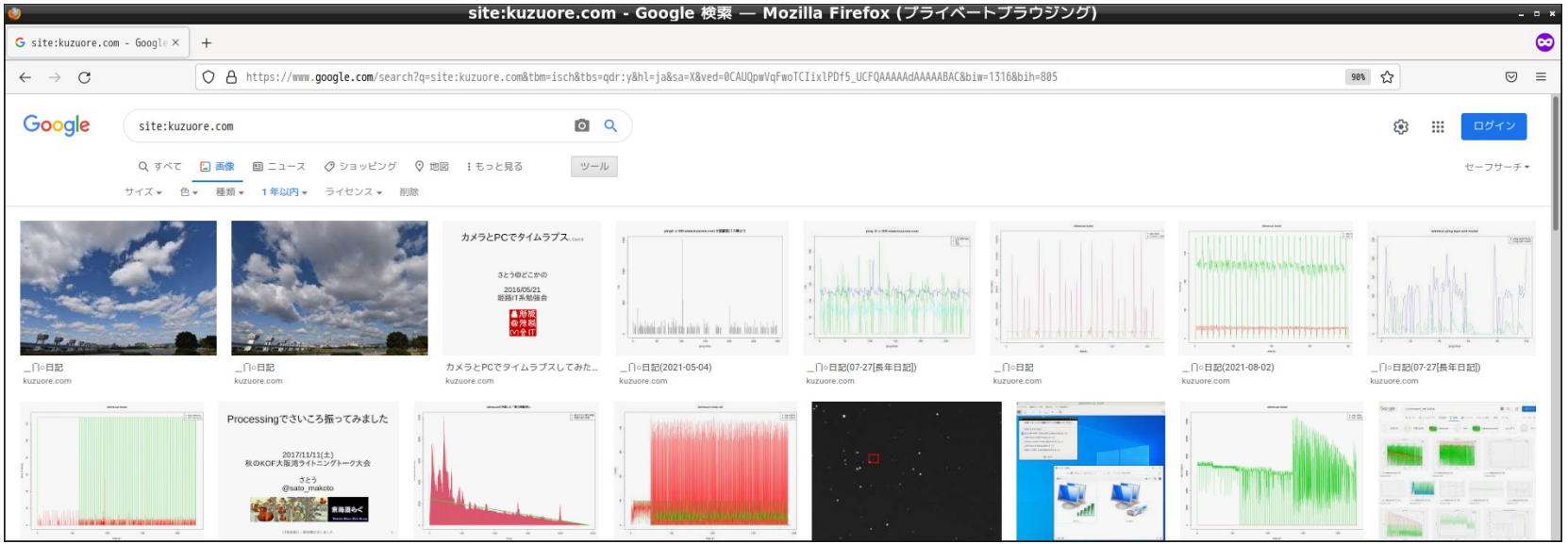
メールが蹴られたはなし

2022/2/5(土)
LILO&東海道らぐオンラインミーティング
2022-02-05
さとう at なんにも

※発表後に若干加筆訂正しました

こんにちはお久しぶりです

- Googleによると、最近一年はこんな感じです



メールサーバごちゃごちゃやってます

- 事情により、メールサーバに嵌っています
- VPSで立ち上げて、ansibleで設定を突っ込んで、テストメールを送受信して、終わったらすぐ一切を消しています
- 送受信はすべて、自分のメールアドレスです(念の為)

今どきメール?

- 「メールなんてもう古い」

  少し前、SNSで時折耳にしました
- SMTPが「プロトコルとして古すぎる」話なら、ン十年前から言われています
- でも、みんな使ってますよね?

  「既にメールアカウント全部捨てました」という人いますか?

建てるだけなら簡単です

- ひと昔前は、みんな「コウモリ本」を頼りに泣きながらメールサーバと格闘した、と聞きました
- 今はPostfixのapt get とかですっとできちゃいます

でも、送信が受け取ってもらえるかは

- 特にiCloudとOutlook.comは疑り深い印象...

Dec 23 14:37:08 $NAME postfix/smtp[10478]: D174B80067:
 host *.mail.icloud.com[$IP] refused to talk to me: 554 5.7.0 Blocked
 - see https://support.proofpoint.com/dnsbl-lookup.cgi?ip=$IP

```
$ sudo postqueue -p
-Queue ID-  --Size-- ----Arrival Time---- -Sender/Recipient-------
D174B80067      647 Thu Dec 23 14:37:07  $ACCOUNT@DOMAIN.TLD
(host *.mail.icloud.com[$IP] refused to talk to me: 554 5.7.0 Blocked
 - see https://support.proofpoint.com/dnsbl-lookup.cgi?ip=$IP)
                                         $ACCOUNT@icloud.com

-- 0 Kbytes in 1 Request.
```

他のメールサーバの信用を得るために

- TLS(Let’s Encrypt)

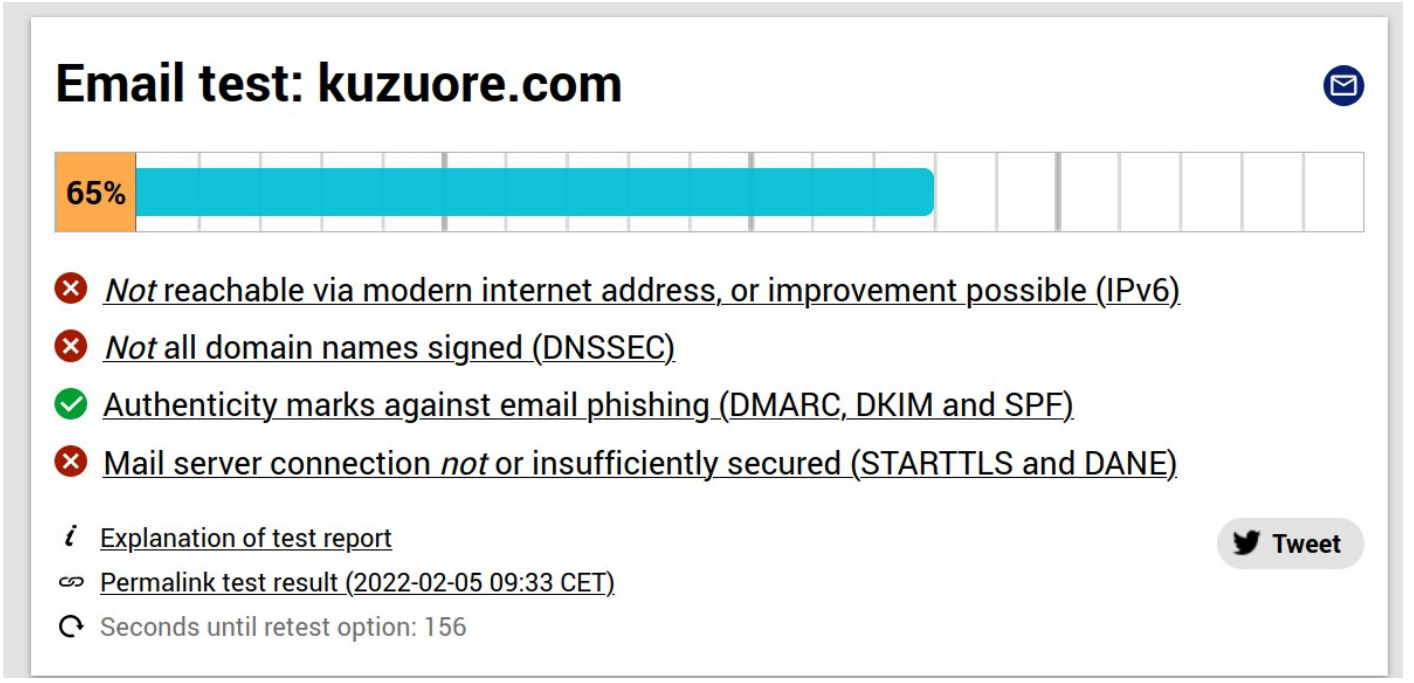
  使い捨てで何回か利用させてもらってました

  こないだからワイルドカード証明書をもらって使いまわしています
- DNSに色々登録しました

  SPF(一行書くだけ)、DomainKey、DMARC(メールサーバにも設定が必要)、MTA-STS(Webサーバも上げる必要あり)
- 悪い人もきちんとやってたりするので(たぶん構成管理ツールなどで)どこまで意味があるのか、正直のところ分からないんですが...

チェックしてもらうと、こんな感じです

- DNSSEC/IPv6が無いとかなりキツい印象



大抵は届きますが

- いちど、あちこちで受信拒否されました

Gmail:

```
Dec 21 11:30:03 localhost postfix/smtp[10934]: C4725140DF1:
 to=<$ACCOUNTgmail.com>, relay=gmail-smtp-in.*.google.com[$IP]:25, delay=2.4, delays=0.07/0.01/1.2/1.1,
dsn=5.7.1, status=bounced (host gmail-smtp-in.*.google.com[$IP] said: 550-5.7.1 [$IP_      18] Our
system has detected that this message is 550-5.7.1 likely suspicious due to the very low reputation of
the sending IP 550-5.7.1 address. To best protect our users from spam, the message has been 550-5.7.1
blocked.
 Please visit 550 5.7.1  https://support.google.com/mail/answer/188131 for more information.
u17si22054375pfk.161 - gsmtp (in reply to end of DATA command))
```

iCloud:

```
Dec 21 14:24:42 localhost postfix/smtp[12590]: 73CCB1408E2: to=<$ACCOUNT@icloud.com>,
relay=*.mail.icloud.com[$IP]:25, delay=7, delays=0.13/0.01/6.5/0.32, dsn=5.7.1, status=bounced
 (host mx02.mail.icloud.com[17.56.9.19] said: 550 5.7.1 Mail from IP $IP_ was rejected due to listing in
Spamhaus SBL. For details please see http://www.spamhaus.org/query/bl?ip=$IPv4 (in reply to RCPT TO command))
```

Outlook.comでも蹴られました。Yahooでは迷惑メール扱いです

もちろん、やれることはやっています

ドメインリスト

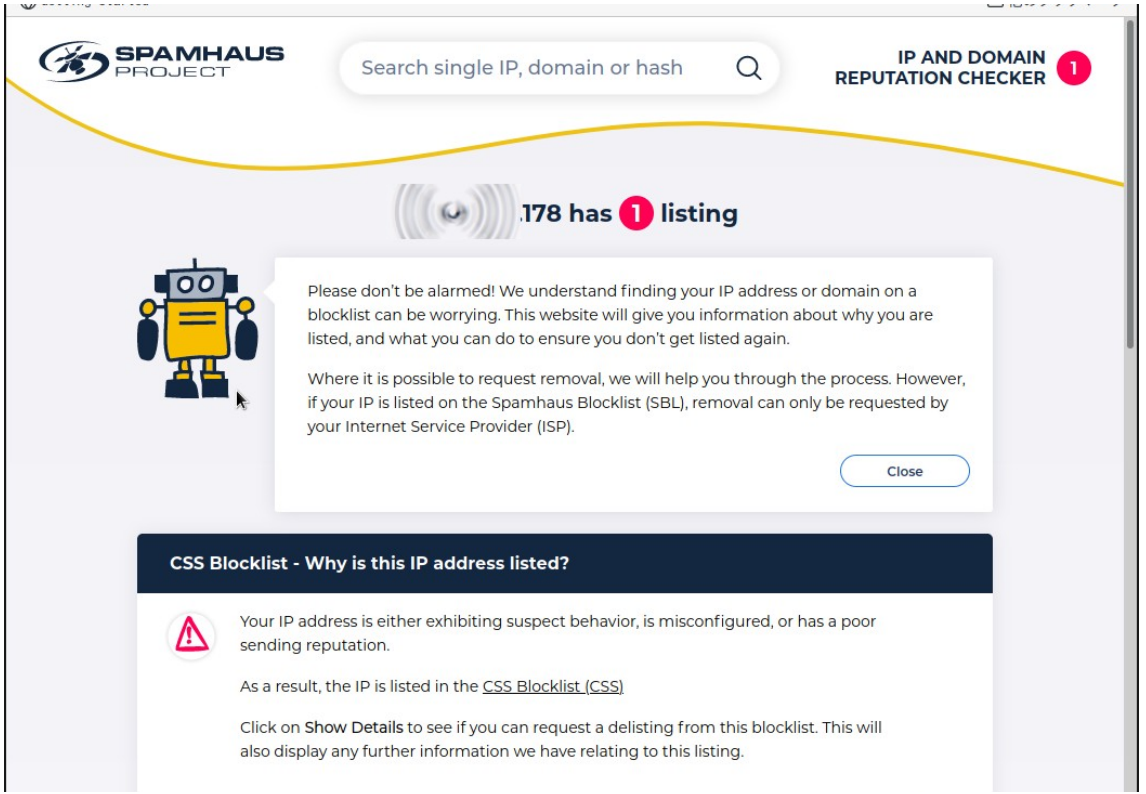
+ ドメイン

kuzuore.net

タイプ	名称	TTL	値
A(通常)	abca	600	
AAAA	abca	600	
MX	@	600	ポイント先 abca.kuzuore.net 優先度 20
NS	@	3600	ns-a
NS	@	3600	ns-a
NS	@	3600	ns-a
TXT	@	600	"v=spf1 +ip4 +ip6 mx:kuzuore.net -all
TXT	_dmarc	600	v=DMARC1 ; P=none ; rua=mailto ruf=mailto
TXT	myabca._domainkey	600	v=DKIM1; h=sha256; k=rsa; p

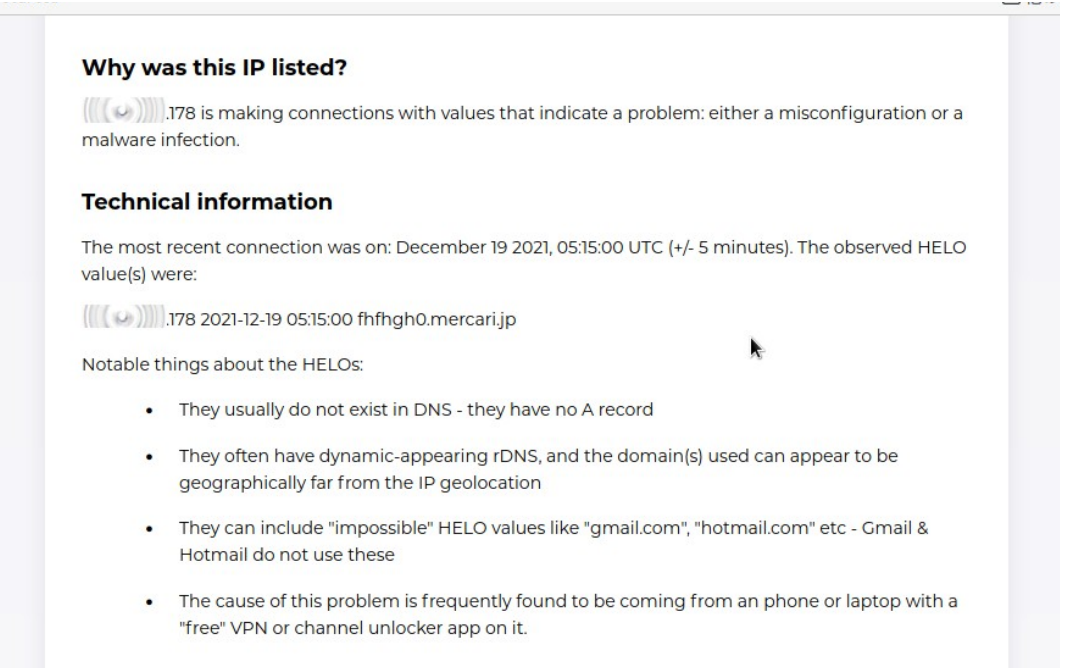
iCloud他で言及しているサイト

- SPAMHAUS
  見てみました



どうやら当該IPv4アドレスは

- つい2、3日前まで、
  変なホストが使っていたようです



Why was this IP listed?

[redacted].178 is making connections with values that indicate a problem: either a misconfiguration or a malware infection.

Technical information

The most recent connection was on: December 19 2021, 05:15:00 UTC (+/- 5 minutes). The observed HELO value(s) were:

[redacted].178 2021-12-19 05:15:00 fhfhgh0.mercari.jp

Notable things about the HELOs:

- They usually do not exist in DNS - they have no A record
- They often have dynamic-appearing rDNS, and the domain(s) used can appear to be geographically far from the IP geolocation
- They can include "impossible" HELO values like "gmail.com", "hotmail.com" etc - Gmail & Hotmail do not use these
- The cause of this problem is frequently found to be coming from an phone or laptop with a "free" VPN or channel unlocker app on it.

そのホストのやってたこと

Technical information

The most recent connection was on: December 19 2021, 05:15:00 UTC (+/- 5 minutes). The observed HELO value(s) were:

[redacted].178 2021-12-19 05:15:00 fhfhgh0.mercari.jp

Notable things about the HELOs:

- They usually do not exist in DNS - they have no A record
- They often have dynamic-appearing rDNS, and the domain(s) used can appear to be geographically far from the IP geolocation
- They can include "impossible" HELO values like "gmail.com", "hotmail.com" etc - Gmail & Hotmail do not use these
- The cause of this problem is frequently found to be coming from an phone or laptop with a "free" VPN or channel unlocker app on it.

なんか挙動不審、というより

- はっきりヤバイことやってた可能性

  ひょっとすると、メルカリを偽装して、偽サイトに誘引するメールを送ったりしてたかも(未確認)?

このVPSは

- クレジットカードなしで立てられました
- 費用も安い方のようです

- ...悪い人にも便利なように思います

えーと、これだけなのですが。

- ツッコミはありますでしょうか
- できればソフトによろしくです

  Reply:
- 特定のユーザがパスワードを漏洩してしまい、スパムの送信に悪用されて、メールサーバのIPアドレスがブロックされたことがあります
- IPアドレスが登録されると、簡単には汚名返上できないこともあります
- いまどきsendmailは無いような(qmailも)

  でも、既存のメールサーバは、なかなかリプレースできないのです...

それくらいです。

- ご静聴、ご意見ありがとうございました

終