2013 年 8 月 5 日

JPCERT/CC インターネット定点観測レポート
[2013 年 4 月 1 日～6 月 30 日]

1 概況

JPCERT/CC では、インターネット上に複数のセンサーを分散配置し、不特定多数に向けて発信されるパケットを継続的に収集し、宛先ポート番号や送信元地域ごとに分類しています。これを脆弱性情報、マルウエアや攻撃ツールの情報などを参考に分析することで、攻撃活動や準備活動の捕捉に努めています。なお、本レポートは日本宛のパケットの傾向を中心に分析しています。

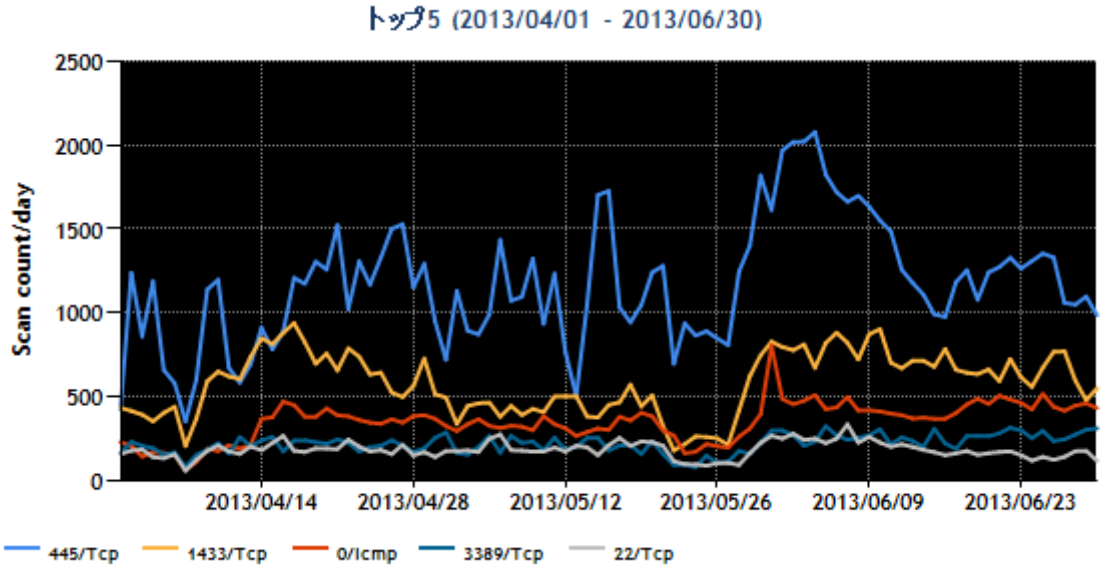
本四半期（2013 年 4 月 1 日から 6 月 30 日）に観測した宛先ポート番号別パケット観測数のトップ 5 を、[表 1]に示します。

[表 1 : 宛先ポート番号トップ 5]

	2013 年 1～3 月	2013 年 4～6 月
1	445/TCP	445/TCP
2	1433/TCP	1433/TCP
3	0/ICMP	0/ICMP
4	23/TCP	3389/TCP
5	3389/TCP	22/TCP

※各ポートで使用するサービス等については、参考文書の(1)を参照してください。

図 1 は、期間中のトップ 5 の宛先ポート番号ごとのパケット観測数の時間的な変化を示しています。



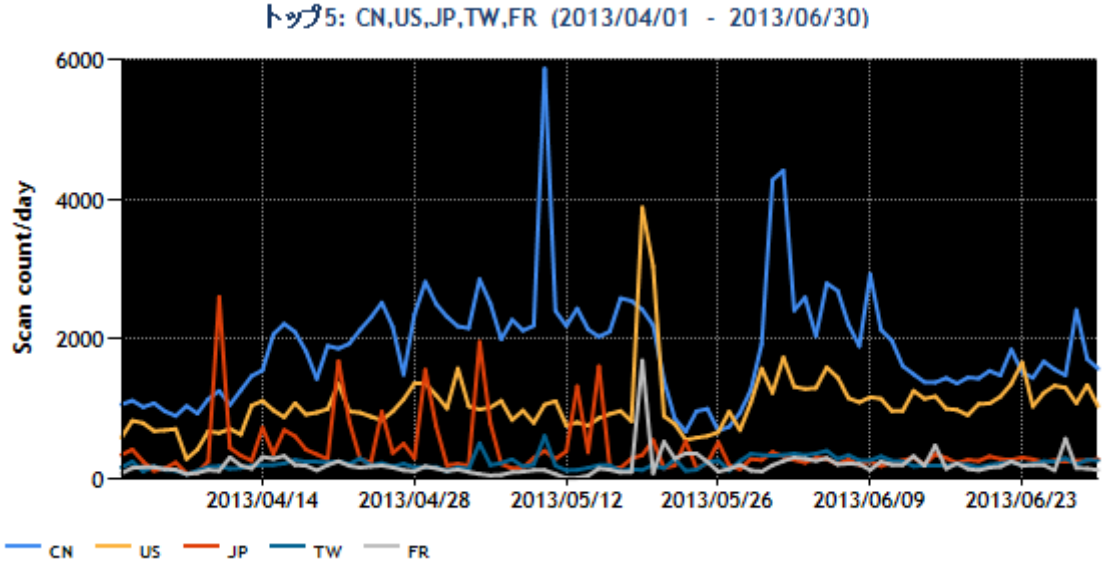
[図 1　2013 年 4~6 月の宛先ポート番号別パケット観測数トップ 5]

本四半期に観測した送信元地域トップ 5 を[表 2]に示します。

[表 2：送信元地域トップ 5]

	2013 年 1～3 月	2013 年 4～6 月
1	中国	中国
2	日本	米国
3	米国	日本
4	タイ	台湾
5	インドネシア	フランス

図 2 に期間中のパケット送信元地域トップ 5 の変化を示します。



[図 2　2013 年 4~6 月の送信元地域別トップ 5]

5 月 10 日から 11 日の間と、6 月 1 日に中国からのパケット数に大きなピークが見られます。これは、特定のセンサーが短時間に 5146/TCP、2078/UDP 宛へのパケットを多数受信した影響です。JPCERT/CC では、これらのポートを使用する製品や脆弱性などの情報を調査しましたが、該当する情報が無く、また、特定のセンサー以外では顕著な変化が見られなかったことから、広域的な脅威を示すデータではないと判断しています。

さらに、5 月 19～20 日にかけては、米国およびフランスからのパケット数に大きなピークが見られます。これは、米国およびフランスのホスティング事業者に割り当てられた IP アドレスを送信元とする、特定のセンサーの 53/UDP 宛に発信されたパケットが増加した影響です。本現象については、「2」で詳しく述べます。

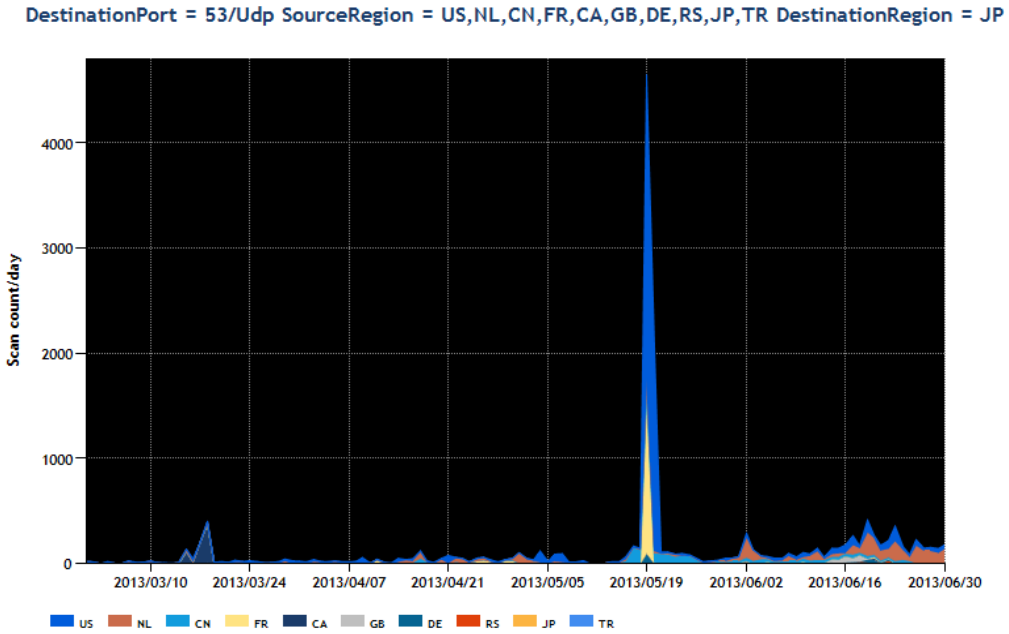
2　注目された現象

【53/UDP 宛のパケットの観測】

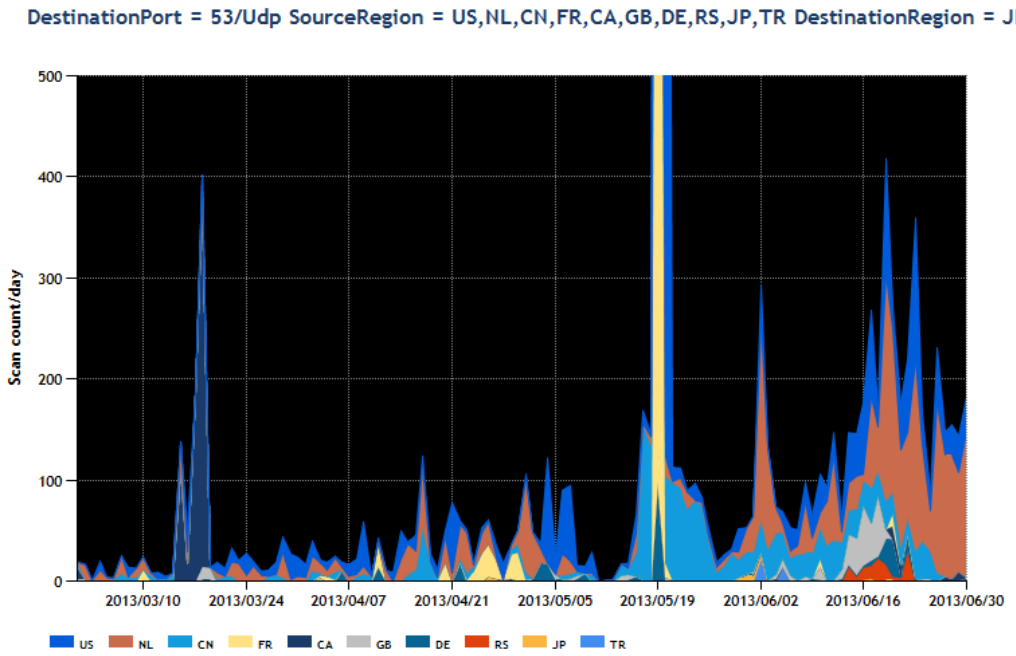
53/UDP 宛のパケット数の増加を、前四半期の「インターネット観測レポート（2013 年 1～3 月）」の「2.注目された現象」で紹介しましたが、本四半期も、この傾向が続きました。

※「インターネット観測レポート（2013 年 1～3 月）」については、参考文書の(2)を参照してください。

図 3 は、2013 年 3 月から 2013 年 6 月までの 53/UDP 宛のパケット数の時間的な変化を示しています。この中には、前四半期（2013 年 3 月）に外部からの再帰的な問い合わせを許可している DNS キャッシュサーバ (以下、オープンリゾルバ)を悪用して行われた Spamhaus Project と Cloudflare 社のサーバに対するサイバー攻撃（DDoS 攻撃）に関連すると思われるパケット数のピークが観測されています。これと、本四半期におけるピークを見比べてください。なお、図 4 は、500 パケット以下の小さなピークが見えるように拡大したグラフです。



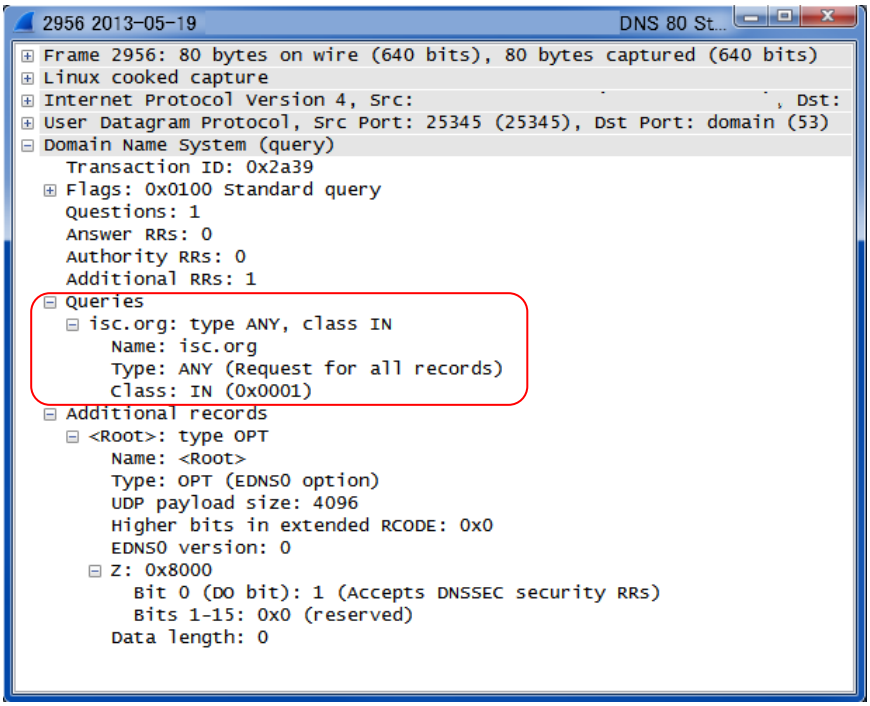
[図 3　2013 年 3 月～2013 年 6 月の 53/UDP 宛のパケット観測数]



[図 4　2013 年 3 月～2013 年 6 月の 53/UDP 宛のパケット観測数（拡大）]

5 月 19～20 日の間には、米国およびフランスのホスティング事業者に割り当てられた IP アドレスを送信元とした 53/UDP 宛のパケットを多数受信しました。この 2 日間で、最も多いのは米国のホスティング事業者を送信元とする IP アドレスで、日本時間の 5 月 19 日 22 時頃から 20 日の 7 時頃にかけて約 2900 パケットが送られていました。次いで多いのは、フランスのホスティング事業者を送信元とする IP アドレスで、日本時間の 5 月 19 日 20 時頃から 21 時頃にかけて約 1500 パケットが送られていました。

図 5 は、センサーが 5 月 19 日に大量に受信したパケットの一つです。3 月の Spamhaus Project と Cloudflare 社のサーバに対するサイバー攻撃（DDoS 攻撃）で観測したパケットは、ripe.net のドメインに登録されているすべてのレコードを検索して応答するように求めた問合せでしたが、今回確認したパケットは、オープンリゾルバに対して、isc.org のドメインに登録されているすべてのレコードを検索して応答するよう求めた問合せをしています。



[図 5　2013 年 5 月の 53/UDP 宛のパケット（Wireshark による表示）]

5 月 19～20 日の間に受信した 53/UDP 宛のパケットの数は、3 月の Spamhaus Project と Cloudflare 社のサーバに対するサイバー攻撃（DDoS 攻撃）の時と比較して、10 倍を超えるパケットの数を観測しました。DDoS 攻撃におけるピーク時トラフィックが四半期間の間に急増したことが注目されます。

上述の事案に関連したパケットを除いても、3 月以降、53/UDP 宛のパケットが増加傾向にあります。おそらく、攻撃の踏み台となるオープンリゾルバをあらかじめ探索してデータベース化するような攻撃の準備がなされていると思われます。こうしたデータベースが使われるようになれば、DDoS 攻撃におけるピーク時トラフィックが一層高まります。こうした事態の悪化を避けるため、オープンリゾルバの対策が急がれます。

参考文書：

(1)Service Name and Transport Protocol Port Number Registry
Internet Assigned Numbers Authority
http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

(2) JPCERT/CC インターネット定点観測レポート(2013 年 1～3 月)
JPCERT/CC
http://www.jpcert.or.jp/tsubame/report/report201301-03.html

(3)オープンリゾルバ(Open Resolver)に対する注意喚起
一般社団法人日本ネットワークインフォメーションセンター
https://www.nic.ad.jp/ja/dns/openresolver/

(4)DNS サーバーの不適切な設定「オープンリゾルバー」について
株式会社日本レジストリサービス
http://jprs.jp/important/2013/130418.html

(5) DNS リフレクション攻撃に対する注意喚起について
警察庁@Police
http:/www.npa.go.jp/cyberpolice/detect/pdf/20130411.pdf

(6)DNS の再帰的な問い合わせを使った DDoS 攻撃に関する注意喚起
JPCERT/CC
https://www.jpcert.or.jp/at/2013/at130022.html