ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

## ●JPドメイン名を標的とした“DNS水責め攻撃”を確認、JPCERT/CC定点観測レポート

http://cloud.watch.impress.co.jp/docs/news/20150428_700035.html
https://www.jpcert.or.jp/tsubame/report/report201501-03.html

### このニュースをザックリ言うと･･･

- 4月27日（日本時間）、一般社団法人JPCERT/CCがインターネット上の攻撃動向に関する定点観測の2015年1月～3月の結果を発表しました。

- 何らかの攻撃活動・準備活動とみられるパケットのうち、宛先ポート別で最も多いのは「telnetサービス」を狙うTCPポート23番宛で、1月上旬には1日8,000パケット近くが観測されることもあったものの、3月には1日2,000パケット前後で推移している模様です。

- 同レポートでは、この他で注目される現象として「DNS水責め攻撃」と名付けられたDDoS攻撃を挙げており、いわゆる「オープンリゾルバ」(※)状態になっている多数のDNSキャッシュサーバを踏み台にする等により、権威DNSサーバに対して大量の問合せを送信し、過剰な負荷をかけようとする攻撃が行われていた可能性が指摘されています。

### AUS便りからの所感等

- 今回確認された「DNS水責め攻撃」では、多くのJPドメインを集中して管理する権威DNSサーバが攻撃対象だったことにより、そこで管理される多くのJPドメインが影響を受けた模様です。

- 組織内で利用しているキャッシュDNSサーバ、あるいはルータ上で有効になっているキャッシュDNSサーバ機能がこういった攻撃の踏み台とされる「オープンリゾルバ」状態になっていないか、今一度設定の確認を行うことを推奨致します。

- この他、LAN上にあるDNSキャッシュサーバが同一LAN上からマルウェア等によってDDoS攻撃に悪用される可能性も考えられますが、UTMの導入により、たとえPCがマルウェアに感染したとしても、それによる大量のパケットの外部への送信を抑止できるケースもあります。


クラウド Watch

2015年5月15日

イベント AWSはパートナー各社のソリューションを紹介
NTT東日本やセールスフォース、KDDIなどの最新サービスも
[2015/05/15]

日立、2014年度連結決算は増収増益、情報・通信システム部門などS部門が前期を上回り過去最高益を達成
[2015/05/15]

「DNAに立ち返り、イノベーションを加速したい」＜富士通・山本正已社長
[2015/05/15]

PFUとFireEye、標的型攻撃対策の「多層防御ソリューション」を提供
[2015/05/15]

アイ・オー、WSS 2012 R2採用ビジネスNASのハイスペックモデル、Core i3・メモリ8GB搭載
[2015/05/15]

アライドテレシス、集中管理対応の中小ネットワーク向け無線LAN AP

ニュース

JPドメイン名を標的とした“DNS水責め攻撃”を確認、JPCERT/CC定点観測レポート

(2015/4/28 15:11)

一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）は27日、2015年1月～3月のインターネット上の攻撃動向に関する定点観測の結果を公表した。

JPCERT/CCでは、インターネット上に複数の観測用センサーを分散配置しており、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・分析することで、攻撃活動や準備活動の捕捉を行っている。

2015年1月～3月に観測された日本宛のパケットを中心に分析した結果によると、宛先ポート別ではTCP 23番ポート（telnet）が最も多く、以下、ICMP、TCP 22番ポート（ssh）、TCP 445番ポート（microsoft-ds）、TCP 1433番ポート（ms-sql-s）の順となった。送信元の地域別では、中国、米国、日本、台湾、韓国の順となっている。

TCP 23番ポート宛のパケットは減少傾向にあり、これは約54%を占めている中国を送信元とするパケットが減少したことに伴うものだという。また、国内を送信元とするパケットについては、QNAP製NAS製品のマルウェア感染に起因すると思われるパケットが増加していたが、該当IPアドレスの管理者などに対して調査を依頼するなどの活動を行ってきたこともあって、2月上旬以降は減少に転じた。


インターネット定点観測レポート(2015年1～3月)

最終更新: 2015-04-27

ツイート　メール

1 概況

JPCERT/CCでは、インターネット上に複数の観測用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、これを脆弱性情報、マルウェアや攻撃ツールの情報などと対比して分析することで、攻撃活動や準備活動の捕捉に努めています。なお、本レポートでは、本四半期に観測された日本宛のパケットを中心に分析した結果について述べます。

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]

| 順位 | 宛先ポート番号 | 前四半期の順位 |
|---|---|---|
| 1 | 23/TCP (telnet) | 1 |
| 2 | 0/ICMP | 4 |
| 3 | 22/TCP (ssh) | 2 |
| 4 | 445/TCP (microsoft-ds) | 3 |
| 5 | 1433/TCP (ms-sql-s) | 5 |

(※) オープンリゾルバ【 open resolver 】
キャッシュサーバとして動作しているDNSサーバのうち、所属するネットワークの外からの名前解決の問い合わせにも応答するようになっているもの。キャッシュサーバは自らが管理するドメインがなく、ネットワーク内のクライアントからの問い合わせを受けてインターネット上のドメイン名やIPアドレスの探索を行い、結果を返答する。通常は組織内でのみ利用され、外部からの問い合わせを受け付けるべきでないとされるが、設定の不備などでインターネット上のどこからでも問い合わせを受け付ける状態になっているものが多数存在し、そのー部がDDoS攻撃などに悪用されている。

# ●4月のフィッシング報告は1787件、金融機関が急増し7割に

https://www.antiphishing.jp/report/monthly/201504.html
http://security-t.blog.so-net.ne.jp/2015-05-08

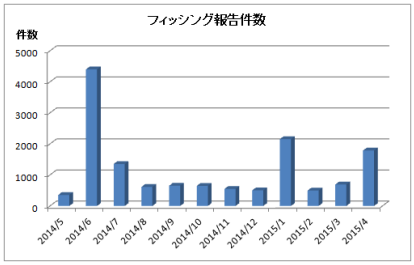
## このニュースをザックリ言うと・・・

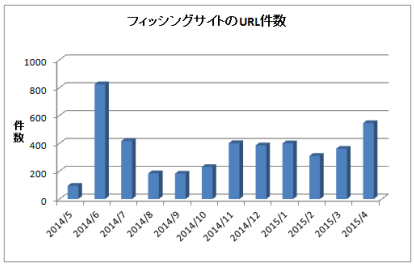
- 5月1日（日本時間）、フィッシング詐欺に関する調査・啓発を行っているフィッシング対策協議会が2015年4月の月次報告書を公開しました。

- 同協議会に寄せられた4月のフィッシング報告件数は3月度より1094件増の1787件となり、2159件が報告された1月度以来の急増となっており、フィッシングサイトのURL件数も3月度より184件増の545件で、824件を記録した昨年6月以降では最も多くなっています。

- 同協議会では、フィッシング報告件数急増の原因として、銀行などの金融機関をかたるフィッシングの報告が増加したことを挙げており、全体の約7割近くに上っているとしています。

フィッシング対策協議会
Council of Anti-Phishing Japan




## AUS便りからの所感等

- 同協議会が発表している毎月のフィッシング報告件数は、2014年1・3・6月度に4000件を超えて以降は、概ね500～600件台で推移する傾向が続いていますが、今回の1787件が1月度のような突発的なものなのか、このまま増加傾向が続くのかは未だ推測しづらいところです。

- ともあれ、そういったフィッシング件数の急増や、内容の傾向に変化があったとしても慌てることなく、フィッシングメールにあるURLを安易にクリックしない、利用している正規のサイトはブラウザのブックマークアクセスするなどの普段からの心がけ、またアンチウイルスやブラウザ・UTMに搭載されたアンチフィッシング機能の活用による防御が肝心です。

# ●ネパール地震の被災者支援に便乗する詐欺メールに注意を

http://www.itmedia.co.jp/news/articles/1505/01/news050.html
https://isc.sans.edu/forums/diary/19635

## このニュースをザックリ言うと・・・

- 4月25日（現地時間）にネパールで発生した大地震に便乗したメールによる攻撃が多発しているとして、米US-CERTおよびSANS Internet Storm Centerが注意を呼びかけています。

- US-CERTの注意喚起では、不正なリンクを含むスパムメールにより、フィッシングサイトやマルウェアに感染したWebサイトに誘導される恐れがあるとされています。

- US-CERTは、一方的に送られてきたメールはリンクをクリックしたり添付ファイルを開いたりせず、慈善団体の名でメールが届いた時は、まず信頼できる連絡先を通じてその団体に直接連絡を取るよう警告しており、SANSも募金をする際は「寄付金が確実に被災者に届くことを確認してほしい」と呼びかけています。


連報 | STUD/O | ベンチャー人 | 製品動向 | ネットの話題 | 社会とIT | セキュリティ | 企業・業界動向 | ブログ | 中堅・中小

ITmedia ニュース > セキュリティ > ネパール地震の被災者支援に便乗する詐欺メールに注...

2015年05月01日 07時20分 更新

ネパール地震の被災者支援に便乗する詐欺メールに注意を

慈善団体の名をかたる募金呼びかけの詐欺メールでリンクをクリックしたり添付ファイルを開いたりすると、マルウェアに感染したり、金銭をだまし取られたりする恐れがある。

[鈴木聖子，ITmedia]

印刷／PDF | ツイート 92 | いいね！ 281 | チェック | 1 | Pocket 3 | 通知

PR 社内コラボレーションを巡って最強の2人がガチ対決！
PR 登録でギフト券のチャンス：マーケティングハウツーをお届け

ネパールで起きた大地震の被災者を支援するための募金活動が広がる中、ユーザーの善意に付け込んで金銭をだまし取ろうとする詐欺メールが各国で流通しているという。米セキュリティ機関のUS-CERTやSANS Internet Storm Centerが注意を呼び掛けた。

自然災害などの大きなニュースに便乗するのはフィッシング詐欺の常とう手段。被災者支援を装うフィッシング詐欺では一般的に、慈善団体の名をかたるなどしてメールやWebサイトで寄付を募る手口が使われる。

しかし、ユーザーがメールに記載されたリンクをクリックしたり添付ファイルを開いたりすると、マルウェアに感染したり、金銭をだまし取られたりする恐れがある。

## AUS便りからの所感等

- 世界的な災害や事件には、それに便乗した攻撃はつきものであることは、今更言うまでもないでしょう。

- そしてそういった攻撃があるという意識のもとに、先に挙げられているような慎重な行動をとること、またマルウェアへの感染、フィッシングサイトへの誘導を防ぐため、アンチウイルスおよびUTMによる防御が確実に行われているか確認することが重要です。