平成 28 年2月 24 日

インターネット観測結果等

（平成 28 年1月期）

- 宛先ポート 53/UDP に対するアクセスが増加
- 宛先ポート 53413/UDP に対するアクセスが増加

1 宛先ポート 53/UDP に対するアクセスが増加

今期は、DNS において使用される 53/UDP を宛先ポートとするアクセスの増加を観測しました（図1-1）。

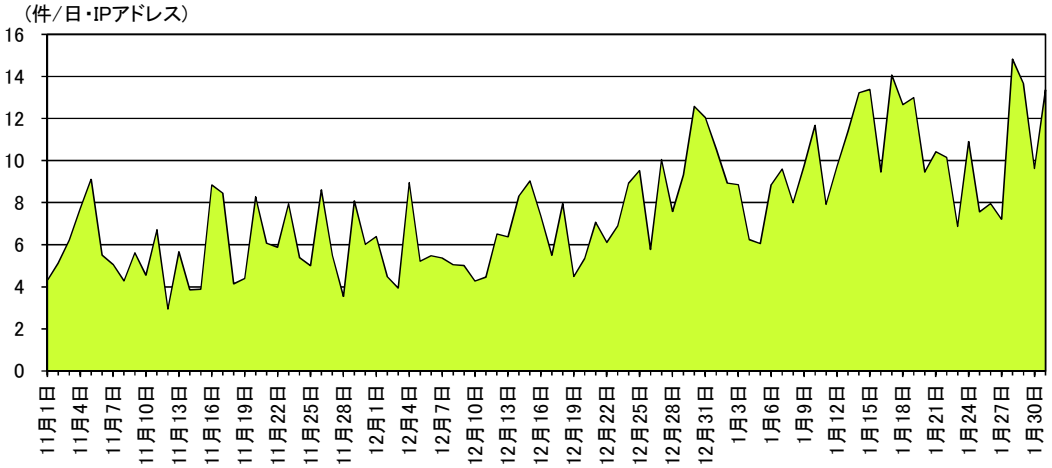

図1-1　宛先ポート 53/UDP に対するアクセス件数の推移（H27.11.1～H28.1.31）

同アクセスにおいて問合せ対象となっているドメイン名・ホスト名について調査したところ、応答サイズが 1,000 バイトを超えるもの（以下「応答サイズが大きいドメイン」という。）が 45.2%でした（図1-2及び図1-3）。

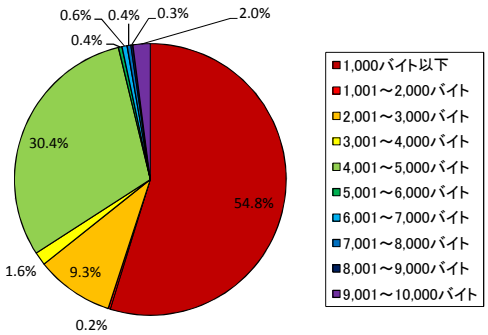

図1-2　宛先ポート 53/UDP に対するアクセス（応答サイズ別）（H27.11.1～H28.1.31）

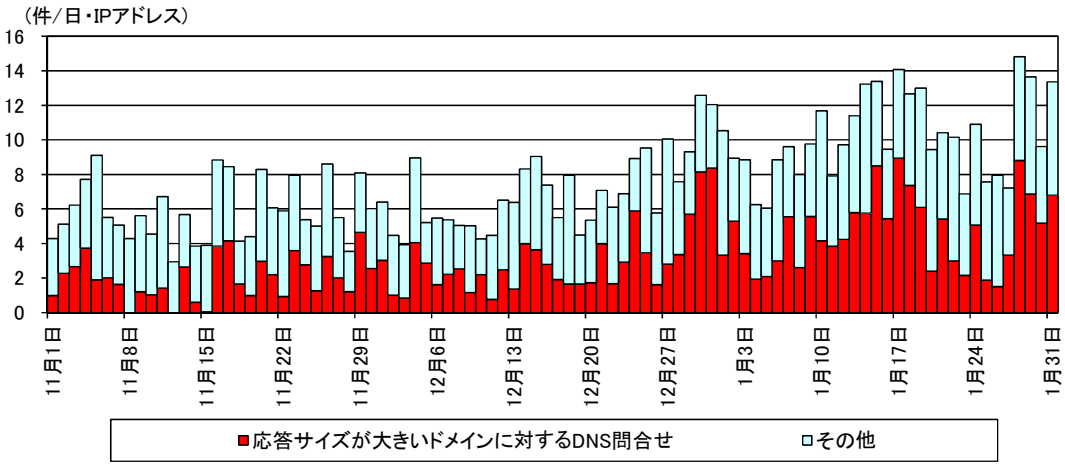

図1-3　宛先ポート 53/UDP に対するアクセス件数の推移（応答サイズ別）
（H27.11.1～H28.1.31）

また、同アクセスにおいてリソースレコード[i]タイプごとに問合せに対する応答のサイズを集計した結果、応答サイズが大きいドメインに対する問合せのリソースレコードタイプは大部分が ANY でした（表1-1、図1-4及び図1-5）。

応答サイズが大きいドメインに対する問合せのうち、リソースレコードタイプが ANY であるものに対する応答の内容を調査したところ、RRSIG レコード、DNSKEY レコード、DS レコード等を含んでいました。この調査結果から、応答サイズが大きいドメインに対する問合せに使用されている DNS サーバは、DNSSEC（DNS Security Extensions）に対応しているものと考えられます。

DNSSEC は、DNS における応答の正当性を保証するための拡張仕様であり、電子署名[ii]の仕組みを応用して DNS 応答における送信元の詐称や内容の改ざんの有無を検証することを可能とするものです。DNSSEC では、検証に必要な情報として、RRSIG レコード（電子署名）、DNSKEY レコード（公開鍵）、DS レコード（公開鍵のハッシュ値）等のリソースレコードが追加されており、応答パケットに署名情報が追加されます。このため、通常の DNS と比較してパケットサイズが増大することから、DNSSEC に対応している DNS サーバは、DNS 問合せに対する DNS 応答の増幅率が大きく、DNS リフレクター攻撃の踏み台として利用される可能性があります[iii]。

---

[i] DNS において、ドメインやホストに関する設定を定義したデータ。
ドメイン名・ホスト名に対応する IPv4 アドレスの情報である A レコード、DNS サーバ IP アドレスに対応するドメイン名・ホスト名の情報である PTR レコード、ドメインを管理するネームサーバの情報である NS レコード、ネームサーバが保持するすべてのレコード情報である ANY レコード等が RFC1035 により定義されている。
https://www.ietf.org/rfc/rfc1035.txt

[ii] メッセージの発信者のなりすましや内容の改ざんの有無を確認するためのもの。
発信者はメッセージとともに自らの秘密鍵でメッセージのダイジェストを暗号化したものを添付し、受信者は受信したメッセージから作成したダイジェストと、発信者の署名から公開鍵で復号化したダイジェストとを比較することによりメッセージ発信者及びそのメッセージの正当性を担保することが可能となる。

[iii] 「DNSSEC Targeted in DNS Reflection, Amplification DDoS Attacks」
https://blogs.akamai.com/2016/02/dnssec-targeted-in-dns-reflection-amplification-ddos-attacksduring-the-past-few-quarters-akamai-has-.html

表1-1 リソースレコードタイプごとの応答サイズ（最大、最小及び平均）

リソースレコードタイプ	最大応答サイズ（バイト）	最小応答サイズ（バイト）	平均応答サイズ（バイト）
ANY	9,033	28	3,030.1
A	3,978	34	234.4
TXT	105	105	105.0
NS	96	96	96.0
未指定	311	81	143.1
PTR	123	119	120.3
SRV	125	125	125.0

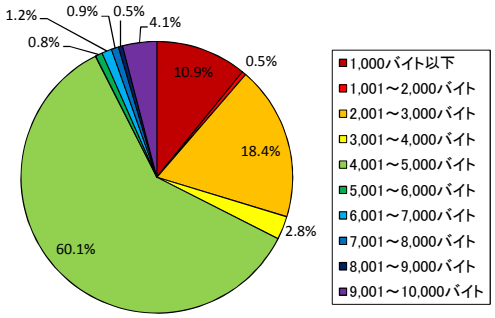

図1-4 宛先ポート 53/UDP に対するアクセス（ANY レコード）（H27.11.1～H28.1.31）

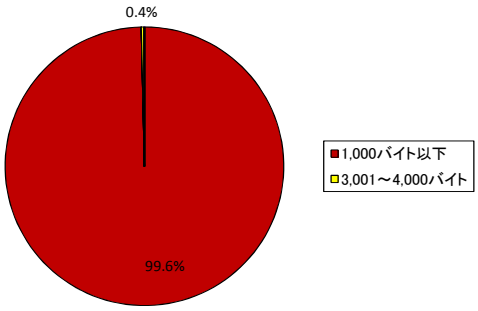

図1-5 宛先ポート 53/UDP に対するアクセス（A レコード）（H27.11.1～H28.1.31）

今期のアクセス増加は、DNSSEC に対応した DNS サーバの探索行為が活発化している可能性があります。

DNSSEC に対応している DNS サーバ等において、次の対策を実施することを推奨します。

- 外部からの DNS 問合せに応答する必要が無い場合は、外部からのアクセスを遮断する。
- 外部からの DNS 問合せに応答する必要がある場合は、イングレスフィルタリング[i]による IP アドレス詐称パケットの拒否や、応答レート制限による単位時間当たりの応答パケット制限等を行う。

[i] 送信元 IP アドレスを詐称したパケットの転送を防ぐ手法の一つで、RFC2827 により定義されている。
https://www.ipa.go.jp/security/rfc/RFC2827JA.html

2 宛先ポート 53413/UDP に対するアクセスが増加

定点観測システムでは、53413/UDP を宛先ポートとするアクセスの増加を観測しました（図2-1）。

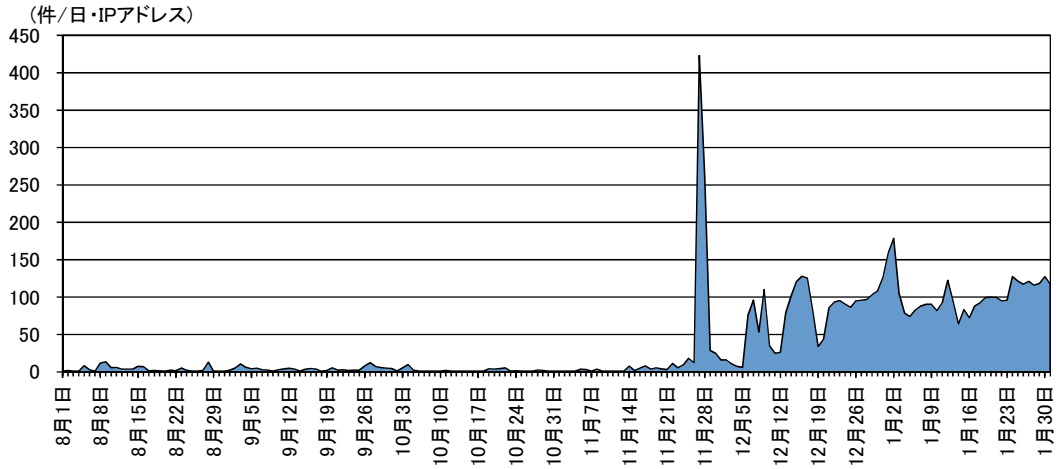

図2-1 宛先ポート 53413/UDP に対するアクセス件数の推移（H27.8.1～H28.1.31）

53413/UDP は Netis[i]社製のルータで使用されるポートであり、平成 26 年8月には外部から簡単にアクセスできる脆弱性をセキュリティ対策企業が公表[ii]しました。定点観測システムでも、同年8月 27 日にアクセスの急増を確認[iii]して以降、継続的に観測しており、平成 27 年8月のアクセス増加[iv]、11 月下旬の顕著な増加後からの継続的なアクセス増加を観測[v]しています。また、アクセスの中には当該ルータに対して不正プログラムのダウンロード及び実行を試みていると思われるものも確認でき、平成 27 年 12 月 15 日に注意喚起を実施[vi]しています。

今期のアクセス増加は、Netis 社製ルータの探索行為が更に活発化している可能性があります。また、平成 28 年1月中旬以降、当該ルータに対して不正プログラムのダウンロード及び実行を試みていると思われるアクセスが増加（図2-2）していることから、脆弱性を放置したままの状態であれば、攻撃に利用される可能性があります。このため、ルータについても、パソコン同様にセキュリティ対策を実施することが必要です。

---

[i] 2000 年に設立されたネットワーク機器メーカで、中国深圳市に本社を置く Netcore 社のグループ企業のひとつ。
http://www.netis-systems.com/

[ii] 「UDP ポートを開放した状態にする Netis 製ルータに存在する不具合を確認」
http://blog.trendmicro.co.jp/archives/9725

[iii] 「インターネット観測結果等（平成 26 年8月期）」（平成 26 年 10 月7日）
https://www.npa.go.jp/cyberpolice/detect/pdf/20141007_2.pdf

[iv] 「インターネット観測結果等（平成 27年8月期）」（平成 27 年9月 25 日）
https://www.npa.go.jp/cyberpolice/topics/?seq=16942

[v] 「インターネット観測結果等（平成 27年 12 月期）」（平成 28 年1月 25 日）
https://www.npa.go.jp/cyberpolice/topics/?seq=17624

[vi] 「IOT 機器を標的とした攻撃について」（平成 27 年 12 月 15 日）
https://www.npa.go.jp/cyberpolice/topics/?seq=17323

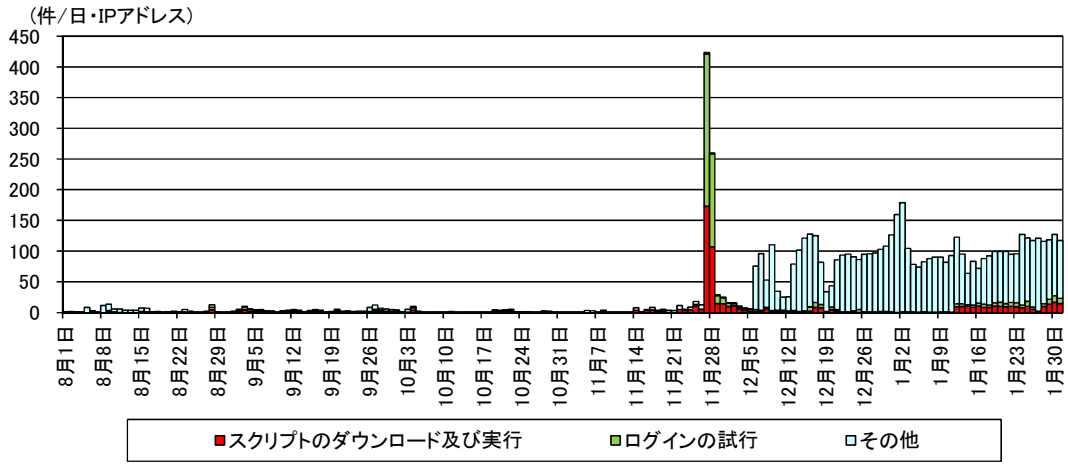

図2-2　宛先ポート 53413/UDP に対するアクセス件数の推移（目的別）
（H27.8.1～H28.1.31）

ルータのセキュリティ対策としては、以下のようなものがあります。

- 管理用のパスワードは、推測されにくいものに変更する。
- メーカのウェブサイト等で脆弱性情報を確認し、脆弱性がある場合はファームウェアのアップデート等の対策を行う。
- 管理用のインターフェースに対するアクセス制限を適切に設定し、外部ネットワークからの不要なアクセスを遮断する。