お客様各位

平成25年10月

株式会社ＵＣＯＭ

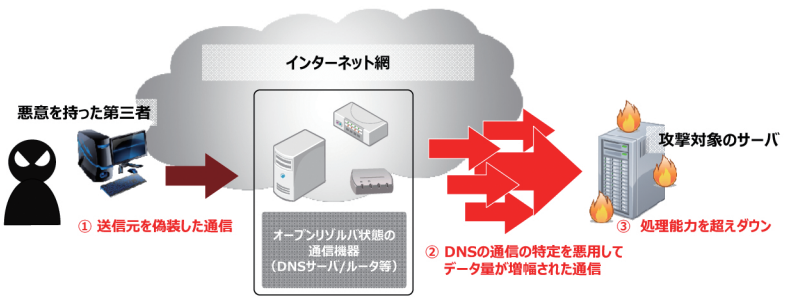
ご利用機器のセキュリティ対策のお願い

平素は弊社インターネットサービスをご利用いただき、誠にありがとうございます。

最近、オープンリゾルバと呼ばれるセキュリティ対策不足の通信機器が悪意ある第三者に利用され、標的となったサーバーをダウンさせる※1など、インターネット上で大きな問題となる事象が急増しております。
お客様のご利用環境において、通信機器が悪用された場合、不要な通信とその処理による悪影響が発生するだけでなく、攻撃の加害者となってしまう可能性がございます※2。
下記のオープンリゾルバ化対策例をご参照の上、ご利用環境の確認と適切なセキュリティ対策の実施をお願いいたします。

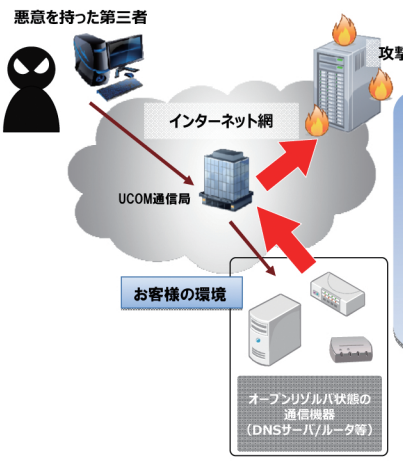
インターネット回線を安全・快適にご利用いただくため、何卒ご理解とご協力をお願いいたします。

■※1_オープンリゾルバDNSを悪用した攻撃（DDoS攻撃）とは？



**インターネット上に存在するセキュリティ対策不足の通信機器を踏み台にし、
DNSの通信の特性を悪用して、増幅した通信を攻撃対象のサーバに送信する。
これを、多数のオープンリゾルバ状態の機器に仕掛け、攻撃対象のサーバをダウンさせることが目的。**

■※2_DDos攻撃の踏み台に利用された場合の悪影響



オープンリゾルバ状態の機器を悪用された場合の影響

① **攻撃的通信の送信元（加害者）となってしまう**
→ 一部の宛先へメール送信不可・特定Webサイトの閲覧不可

② **踏み台となったルータ、DNSサーバの処理能力低下**
→ 不要な通信処理の増加により、応答速度等が低下する

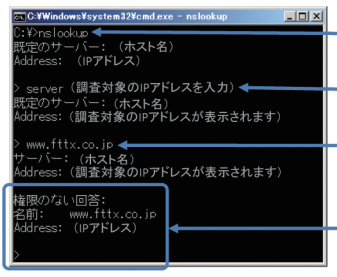
③ **インターネット回線（通信）の速度低下**
→ 意図しないトラフィックの大量発生により
Web表示遅延・ファイル転送速度の低下・通信不安定化など

■ オープンリゾルバ 確認方法と対策例

【オープンリゾルバ状態になる可能性がある機器】
・DNSサーバ　・ルータ　・WEBサーバ　・メールサーバ　・プロキシサーバ　・その他DNS機能を有する機器

【オープンリゾルバであるかの確認方法】
オープンリゾルバであるかの確認方法の1つとして、**別のインターネット回線より**、確認したい対象のDNSサーバやルータのIPアドレス宛に、DNSの再帰的な問合せを行い、**名前解決ができてしまった**場合は、外部からのDNS通信に応答するオープンリゾルバDNSである可能性があります。

※Windows（コマンドプロンプト）での確認方法の例



1.「nslookup」と入力

2.「server（調査対象のIP）」と入力

3.「www.fttx.co.jp」と入力

4.「**権限のない回答**」または「**Non-authoritative answer**」と、その結果のIPアドレスが表示された場合、DNSの再帰的問い合わせに応答がある為、オープンリゾルバである可能性があります。

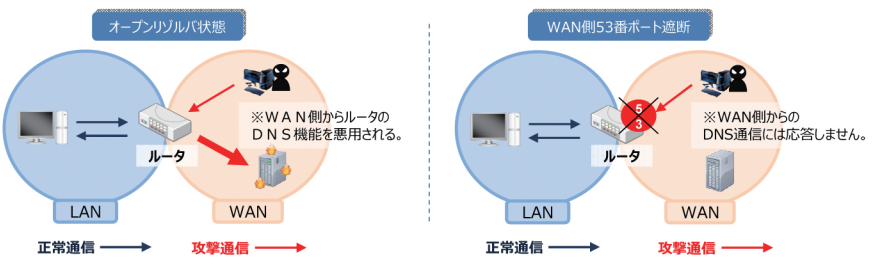
【IPアドレスを元に、オープンリゾルバであるかを確認できるWebサービス】
下記のサイトでご利用のIPアドレスを入力することにより、該当のIPアドレスがオープンリゾルバであるかの確認が行えます。

■Open DNS Resolver Project
URL： http://openresolverproject.org/
※こちらのチェックサイトで利用されているリストは週一回の更新となっております。
機器設置直後にはご利用になれません。機器設置から一週間以上経過後にご利用ください。

【DNSサーバを設置の場合の対策例】
下記のドメイン管理会社が発表した設定情報をご参考いただき、サーバ設置環境に応じた対策をお願いいたします。

■参考情報
○JPRS 設定ガイド：オープンリゾルバー機能を停止するには【BIND編】
URL：http://jprs.jp/tech/notice/2013-04-18-fixing-bind-openresolver.html
○JPRS 技術解説：「DNS Reflector Attacks（DNSリフレクター攻撃）」について
URL：http://jprs.jp/tech/notice/2013-04-18-reflector-attacks.html

【ルータをご利用の場合の対策例】
多くのルータにはDNSに関する機能（DNSリレー、DNS Proxy、DNS リカーシブサーバ、Easy DNS等）が搭載されています。
この機能は、LANからWANへの通信に対して利用するためのものですが、適切な設定がなされていない場合に、前述の機能がWAN側にも有効になり、外部からのDNS通信に応答するオープンリゾルバとなる場合があります。
ご利用されるルータの仕様をご確認いただき、任意の設定が必要な場合は、**外部（WAN側）からの53番ポートの通信を遮断し**、意図せずオープンリゾルバDNSとなることを防止していただきますようお願いいたします。
また、セキュリティを高くするために、53番ポートのほか、WAN側の利用しないポートについても、フィルタリング設定をご検討ください。



【その他ネットワーク機器をご利用の場合の対策例】
メールサーバ、プロキシサーバ等DNSの機能を主としないサーバにおいてもDNSの機能（DNSキャッシュ等）を有している場合があります。適切な設定がなされていない場合、外部からのDNS通信に応答するオープンリゾルバとなる可能性がありますので、**外部（WAN側）からの53番ポートの通信を遮断、DNSの機能を無効化する**等の適切な設定をお願いいたします。

なお、誠に恐縮ですが、機器ごとの設定に関するお問い合わせは、弊社ではお答えすることができかねます。設定については、ご利用の機器メーカー等へお問い合わせください。
また、設定変更などにより生じた結果については、弊社では、責任を負いかねますので、あらかじめご了承ください。

参考情報

各機関からオープンリゾルバに関する注意喚起が行われております。下記サイトにつきましてもご確認をお願いいたします。

■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（JPNIC）
オープンリゾルバ（Open Resolver）について
URL： https://www.nic.ad.jp/ja/dns/openresolver/
■JPCERTコーディネーションセンター（JPCERT/CC）
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
URL： https://www.jpcert.or.jp/at/2013/at130022.html
■株式会社日本レジストリサービス(JPRS)
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
URL： http://jprs.jp/important/2013/130418.html