平成 25 年 4 月 11 日
大阪府サイバーテロ
対策連絡協議会事務局

スパム対策組織「Spamhaus Project」に対する DDoS 攻撃について

1　本事案の概要

平成 25 年 3 月中旬から下旬にかけて、非営利のスパム対策組織「Spamhaus Project」に対する大規模な DDoS 攻撃が実施されたとの報道がなされた。「Spamhaus Project」の依頼により攻撃への対応を実施しているセキュリティ対策企業は、DNS サーバの再帰的な問い合わせを悪用した DNS リフレクション攻撃が使用されたと報告している。

2　DNS リフレクション攻撃について

DNS リフレクション攻撃は、「DNS アンプ攻撃」などとも呼称され、再帰的な問い合わせが許可された DNS サーバを悪用して、攻撃対象に大量の UDP トラフィックを送信する手法である。CFC では、かねてより同攻撃手法について注意喚起を実施してきたところである。[i] [ii]

今回の事案発生を踏まえ、CFC では国内重要インフラ事業者等の外部公開 DNS サーバについて調査を実施した。この結果、外部からの再帰的な問い合わせが可能になっている DNS サーバが複数存在することを確認した。これらのサーバは DNS リフレクション攻撃に悪用される可能性がある。

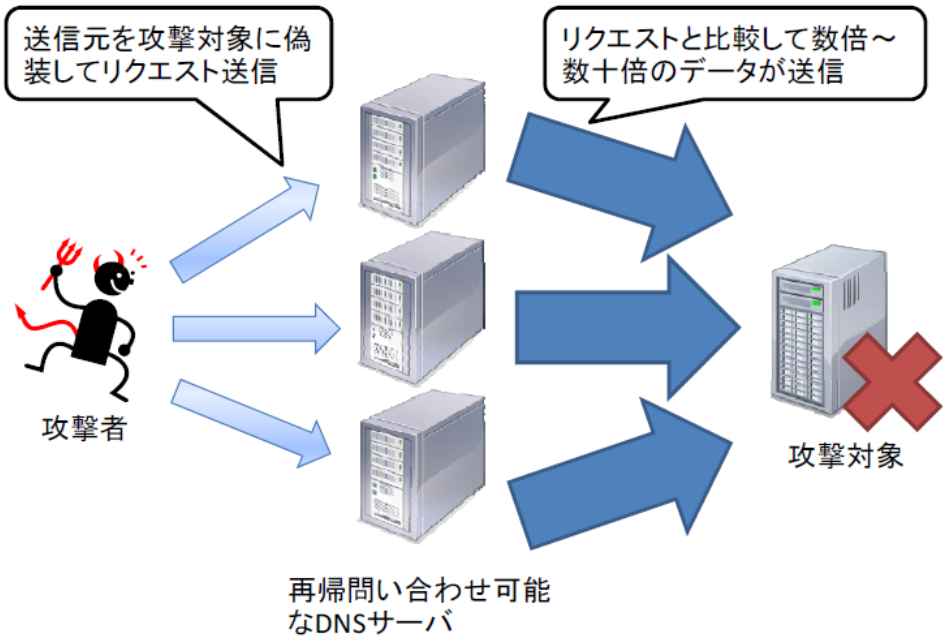

図1　DNS リフレクション攻撃の概要

DNS サーバにおいて外部からの再帰的な問い合わせが許可されていると、DNS リフレクション攻撃に悪用され、攻撃トラフィックの送信元となる可能性がある。また、キャ

ッシュポイズニング攻撃の対象になる等の他のリスクも生じる可能性がある。このため、次の対策を実施することを推奨する。

1. キャッシュサーバとコンテンツサーバ（権威サーバ）を分離する。
2. キャッシュサーバについては外部からのアクセスを遮断する。
3. コンテンツサーバ（権威サーバ）については、再帰的な問い合わせを拒否する。

3　CFC における観測状況

平成 25 年４月６日現在、「Spamhaus Project」のウェブサイトは、攻撃への対応を実施しているセキュリティ対策企業のコンテンツ配信網（CDN）によって配信されている。CFC では、このセキュリティ対策企業に割り当てられた IP アドレスからの跳ね返りパケットを多数観測した。跳ね返りパケットは３月 26 日から 29 日の間に集中しており、その多くは発信元ポートが 80/TCP であった。攻撃者が用いる攻撃手法が DNS リフレクション攻撃から、ウェブサーバに対する SYN Flood 攻撃などの他の手法に移行した可能性も考えられる。

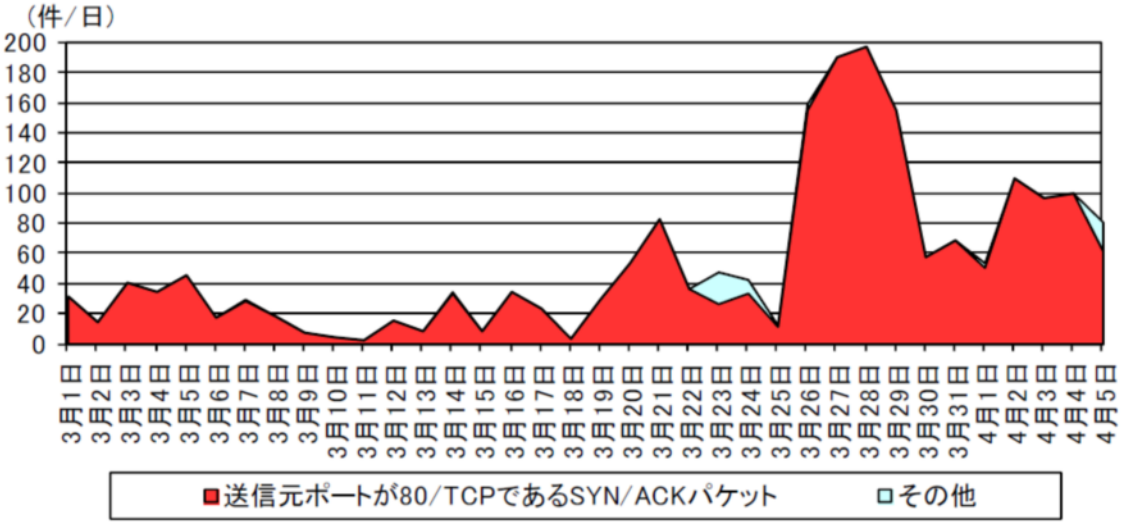

図2 「Spamhaus Project」のウェブサイトを配信する企業からの跳ね返りパケットの推移
（平成 25 年3月1日～4月5日）

4　おわりに

今回、「Spamhaus Project」が DDoS 攻撃の対象となった原因には、特定の企業をスパム発信源と判断しブロッキングリストに登録したことに関しての確執があったとの報道がなされている。どの組織においても、些細な理由でサイバー攻撃の対象となる可能性があり、また攻撃対象となれば攻撃者は有効な攻撃手法を模索して、様々な手法を試みてくることが考えられる。攻撃に備えて、平素から十分な対策を行っておく必要性がある。

また自組織が攻撃対象とはならなくても、管理する機器が攻撃に悪用された場合には社会的な責任を追及される可能性も考えられる。更に DNS リフレクション攻撃のように、大量のトラフィックにより攻撃が実施された場合には、攻撃を受けた組織のみでの対応

は困難を極める。このため、悪用される可能性のある機器を減少させ、サイバー攻撃発生の機会を低減させることが重要となる。

---

[i] DNS の再帰的な問い合わせを悪用した DDoS 攻撃手法の検証について（平成 18 年 7 月 11 日）
http://www.npa.go.jp/cyberpolice/server/rd_env/pdf/20060711_DNS-DDoS.pdf

[ii] DNS サーバの現状調査（平成 20 年 8 月 21 日）
http://www.npa.go.jp/cyberpolice/server/rd_env/pdf/20080821_DNS.pdf