ランダムサブドメインアタックへの対策例について

SCSK株式会社
服部 成浩(s.hattori@scsk.jp)

トピック

- ランダムサブドメインアッタクへ有用と思われるNominum社製 キャッシュサーバ Vantio の動作を紹介
  - 再帰問い合わせ(recursive-clients)が上限値に達した場合の動作
  - 権威サーバから多量のtruncateメッセージを受け取った場合の動作
  - 権威サーバのIPとドメインの組み合わせによる、権威サーバへのレートリミット
  - ネガティブキャッシュ

Nominum Vantioとは

- Nominum社とは
  - 本社 : San Francisco Redwood City
  - 設立 : 1999年
  - キャリアクラスの商用DNSソフトウェアの開発、販売
  - 2004年より日本にて販売開始
  - DNSを考案したポール・モカペトリスが在籍

- 権威サーバ、キャッシュサーバは別々のソフトウェアとして提供
  - キャッシュサーバ : Nominum Vantio
  - 権威サーバ : Nominum ANS

- 今回は Vantioの話

再帰問い合わせの同時要求数が上限値に達した場合

- ランダムサブドメインアタックにより、権威サーバへの問い合わせ中のクエリ(recursive-clients)が上限値に達する
  - 権威サーバへ多量のクエリが発生
  - 権威サーバからの応答が遅い、応答がない
  - 再送クエリの発生

- 問題点
  - Recursive-clientsが上限値に達した場合、新規クエリを受け付けない動作をするソフトウェアもある

再帰問い合わせの同時要求数が上限値に達した場合

- Vantioの場合
  - 名前解決に時間がかかっているクエリを破棄し、新規クエリを受け付ける
  - 破棄したクエリに関しては、servfailを返す
  - 時間がかかっているクエリは名前解決できない可能性が高く、時間がかかっているクエリを破棄し、新規クエリを受け付ける設計

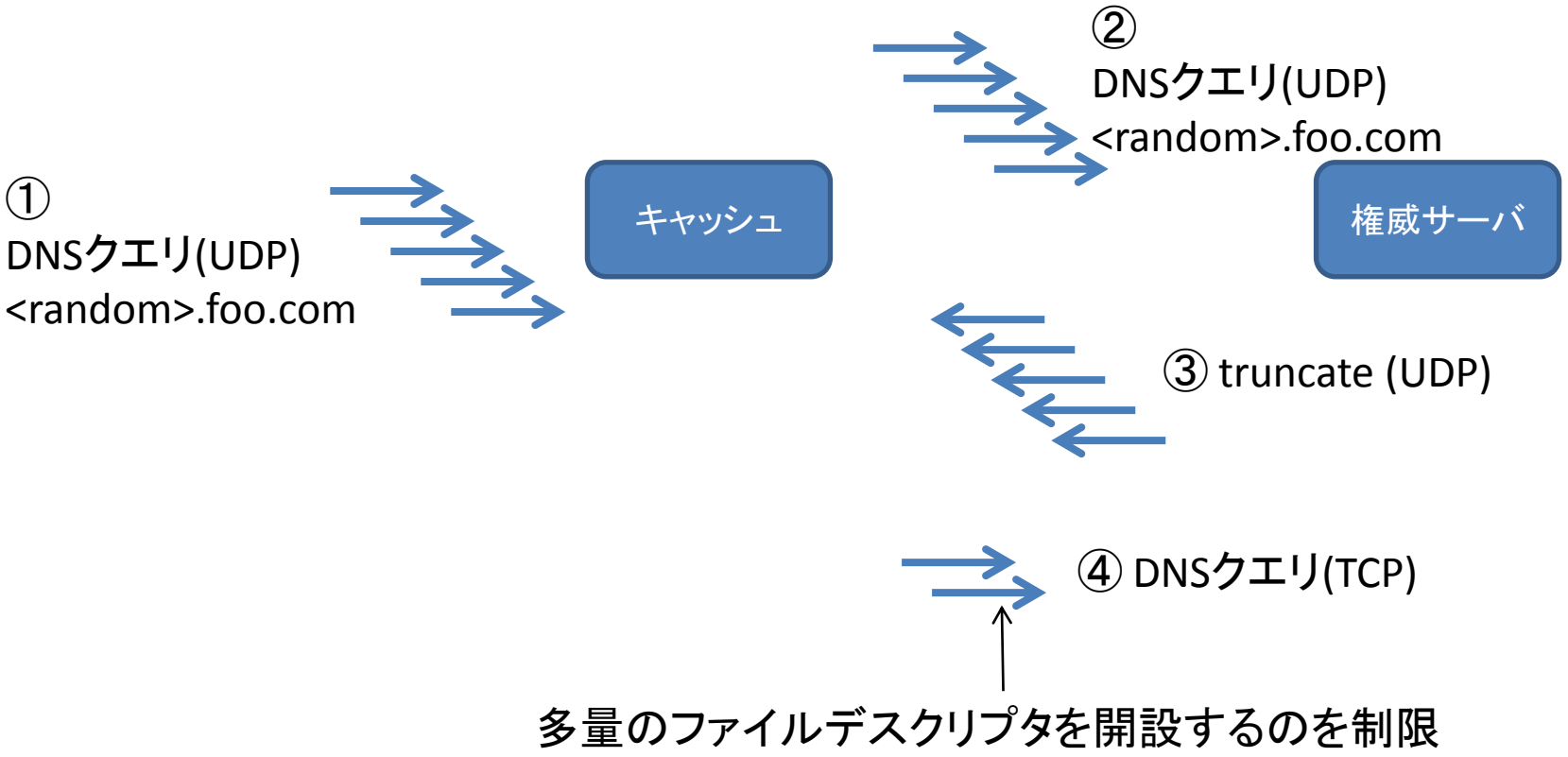
権威サーバから多量のtruncate メッセージを受け取った場合

- 権威サーバから多量のtruncateメッセージを受け取り、多量のTCPコネクションを開設してしまう
- 問題点
  - 一度に多量のTCPコネクション(ファイルデスクリプタ)を開設することによるCPU負荷、メモリ使用率の上昇

権威サーバから多量のtruncate メッセージを受け取った場合

- Vantioの場合
  - 1度に開設するファイルデスクリプタ数を制限し、リソースを保護するオプションがある
  - リミットによりTCPコネクションを開設できなかった場合は、リゾルバにservfailをかえす

権威サーバから多量のtruncate メッセージを受け取った場合



権威サーバへのレートリミット

- 権威サーバへ多量にクエリを送信してしまうことで、キャッシュサーバの負荷が上がる

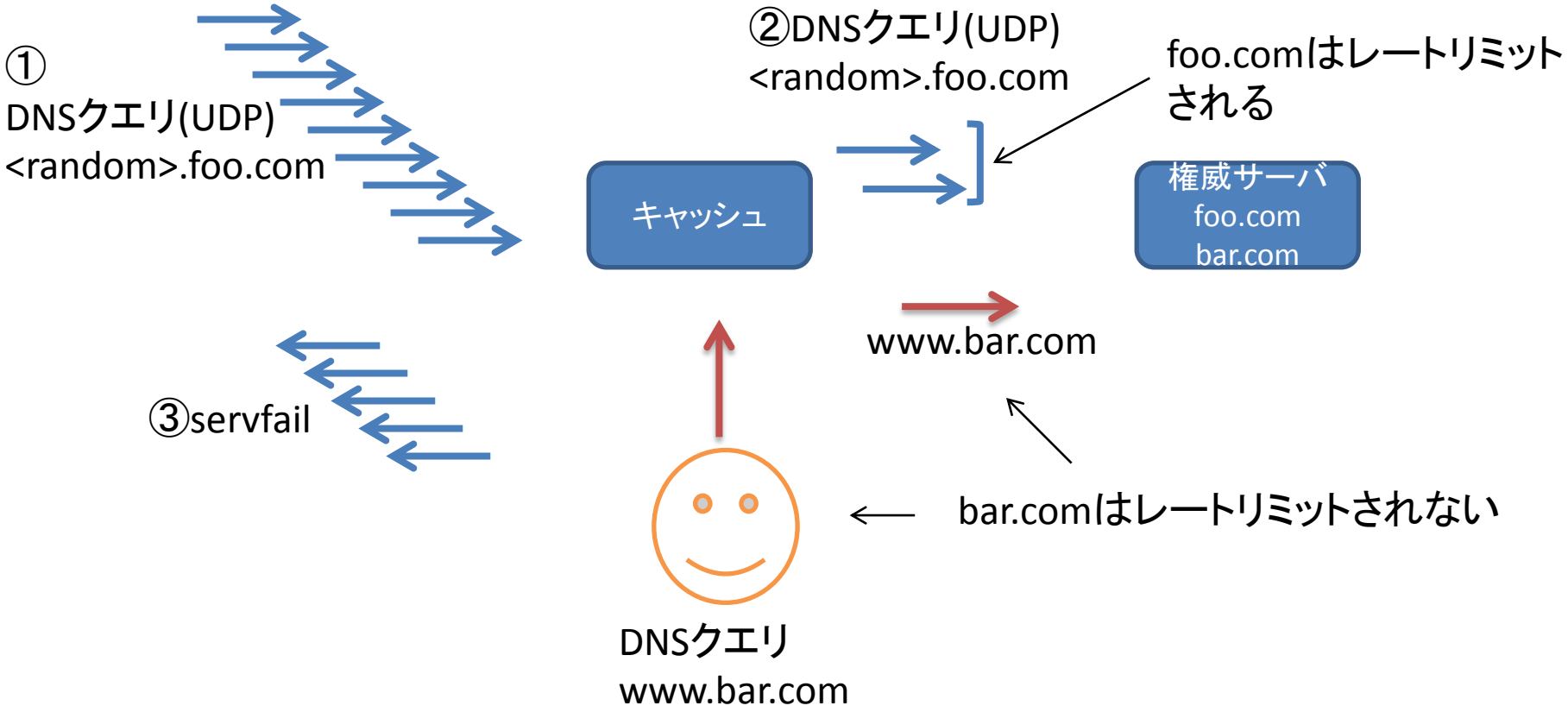
- 問題点
  - キャッシュサーバの負荷の上昇
  - recursive-clientsが上限値に達する
  - truncateレスポンスを多量に受け取ってしまう可能性がある
  - 処理できない量のクエリを権威サーバに送信してしまう

- 権威サーバへ多量にクエリを送信するのを抑えられれば、再帰問い合わせ要求数やTruncateの問題も防げそう

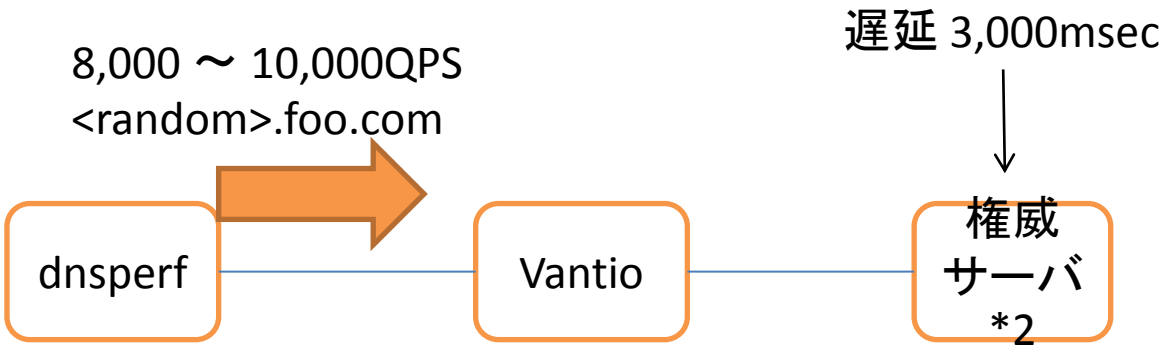
権威サーバへのレートリミット

- Vantioの場合
  - 権威サーバのIPとドメインのペアでサクセスレートを計測し、権威サーバへレートリミットを実施
  - 複数のドメインを同じIPでホスティングしている環境でも影響がないように、宛先IPとドメインのペアでレートリミット
  - レートリミットにかかったクエリは、権威サーバには問い合わせず、servfail をかえす
  - 権威サーバへ送信したクエリ量と、権威サーバから応答が得られるまでのレスポンスタイムをもとに、権威サーバに送信するクエリ量を動的に調整

権威サーバへのレートリミット



権威サーバへのレートリミット



dnsperf → Vantio　(QPS)	Vantio → 権威サーバ(QPS)
約 8,000 ～ 10,000	100　～ 300

ネガティブキャッシュ

- 到達不能な権威サーバ
  - 8秒ネガティブキャッシュ
  - 宛先IPとドメインのペアでネガティブキャッシュ
- servfailを返す権威サーバ
  - 30秒ネガティブキャッシュ

おしまい

- さんきゅー