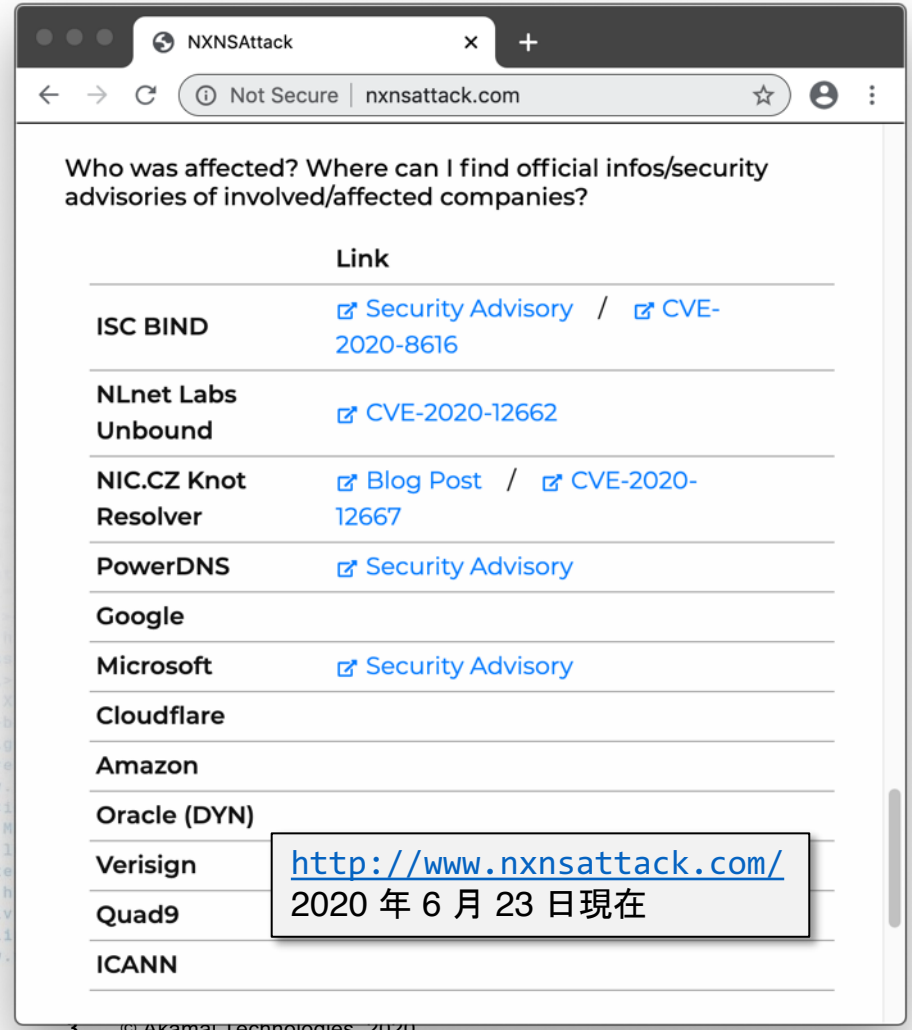
NXNSAttack の公表「CacheServe は？」

アカマイ・テクノロジーズ合同会社
シニア・ソリューション・エンジニア
松本 陽一

このプレゼンテーションにおいてなされる記述は作成者個人の見解を示すものであり、アカマイ・テクノロジーズの見解を示すものではありません。提供される情報は作成時点において正確なものであると考えておりますが、当該情報についてなんら表明又は保証を行いません。



Akamai (CacheServe) はどこ？

「…忘れられてるなんてことないよね？」

Akamai DNSi CacheServe

商用のフルリゾルバー・ソフトウェア

国内外多くの主要なキャリアや ISP で採用される

オープンソースではなく、一般の方は入手、検証の機会がなさそう

ここにいました

Acknowledgements (謝辞)

We would like to thank Michael McNally and
:
Tim April and Ralf Weber of Akamai and
:

http://www.nxnsattack.com/

- 4月上旬頃コンタクトをもらう
- 事前情報に基づいてテスト
- 研究者に対してクラウド上にテスト用の CacheServe を提供

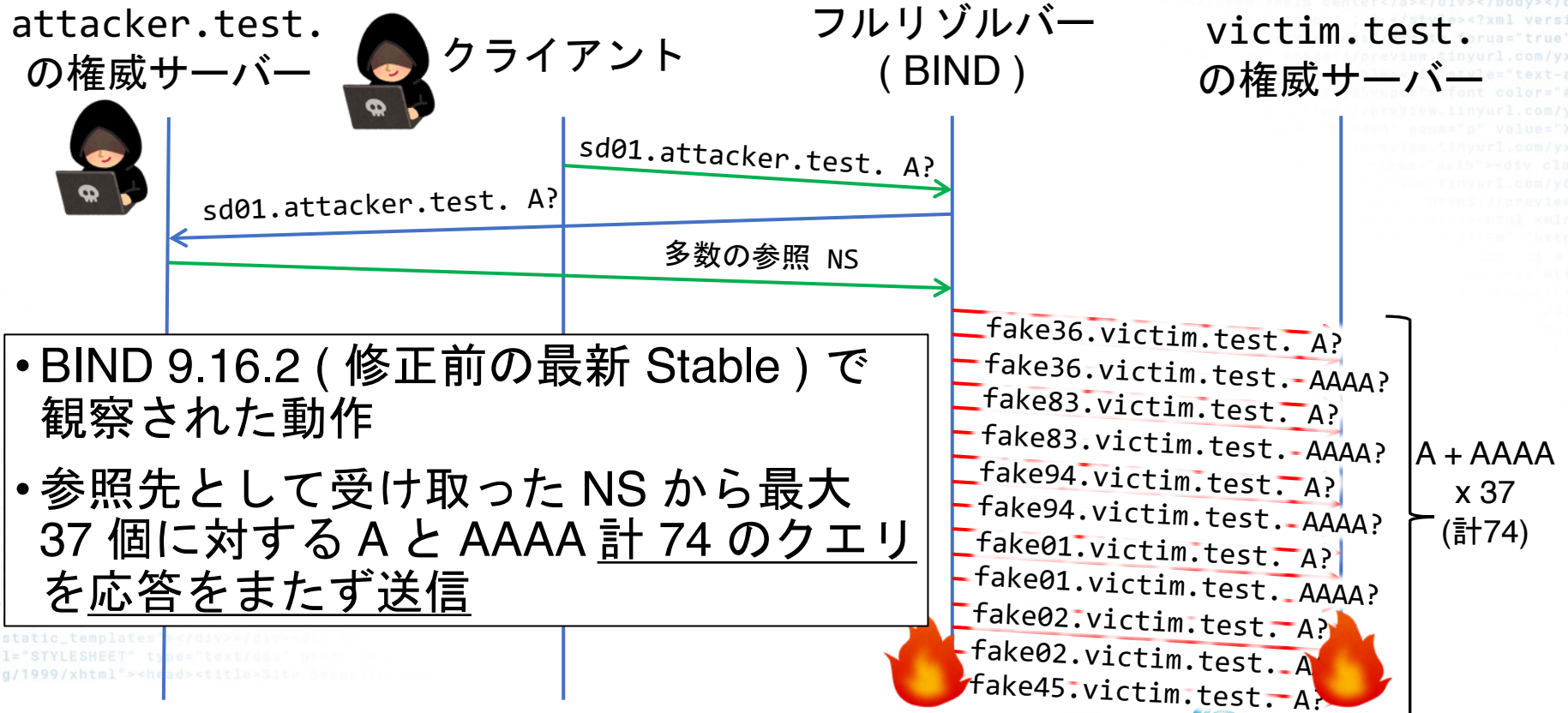
問題がないことを確認済み
（お客様からのお問い合わせに回答、アナウンス）

今日のテーマ

他の多くの実装が影響を受けると発表をする中で…

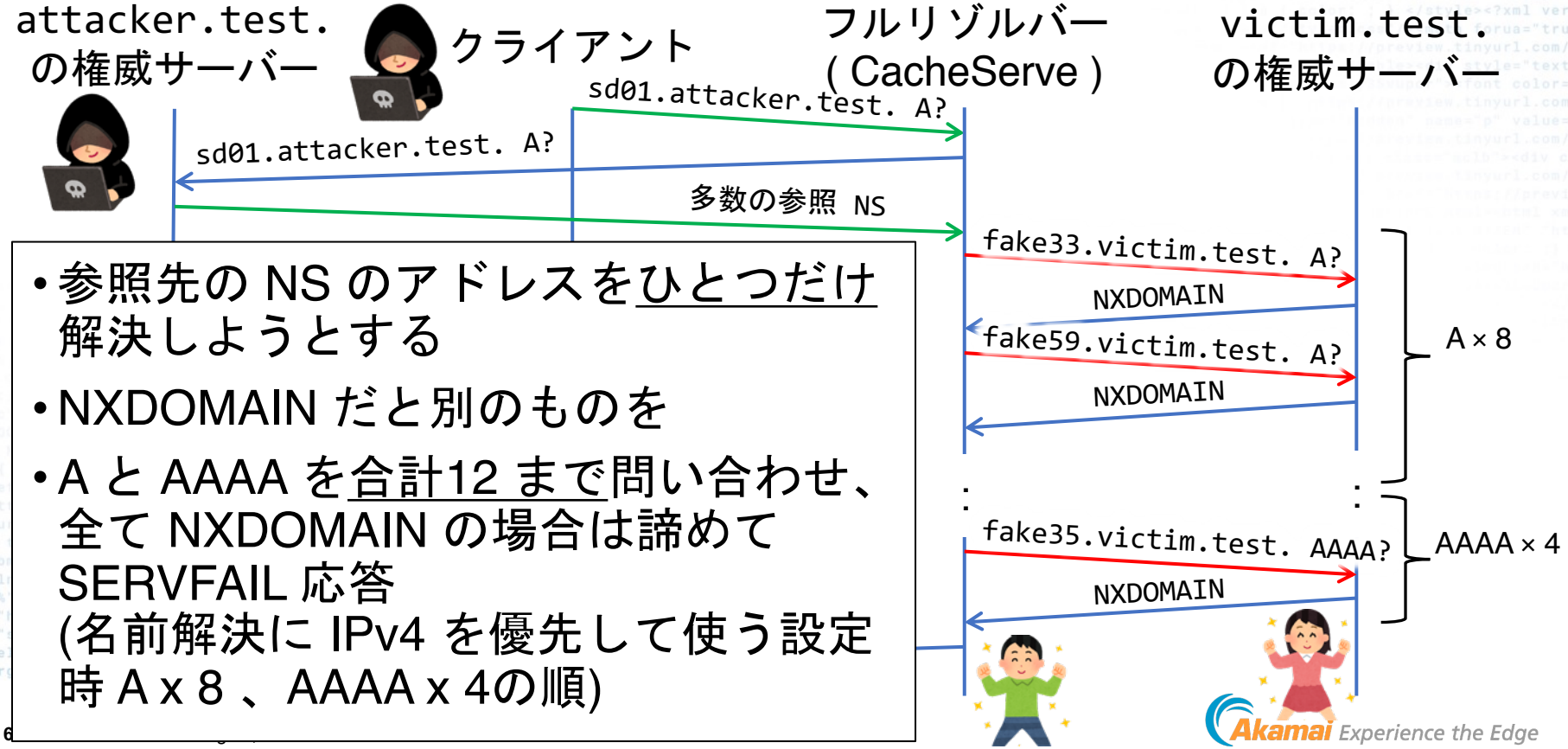
- なぜ、CacheServe は大丈夫といえるのか（具体論）
- なぜ、CacheServe は未発見の問題に準備できていたのか（背景）

問題とされたフルリゾルバーの動作の例



- BIND 9.16.2 (修正前の最新 Stable) で観察された動作
- 参照先として受け取った NS から最大 37 個に対する A と AAAA 計 74 のクエリを応答をまたず送信

CacheServe (7.5.1.1) の動作



- 参照先の NS のアドレスをひとつだけ解決しようとする
- NXDOMAIN だと別のものを
- A と AAAA を合計12 まで問い合わせ、全て NXDOMAIN の場合は諦めて SERVFAIL 応答
  (名前解決に IPv4 を優先して使う設定時 A x 8 、AAAA x 4の順)

名前解決のメッセージ数

論文は、通常の名前解決についても、理論上 3 回のクエリで済むところ非常に多くのパケットが見られると指摘

	論文 (AWSの BIND 9.12.3?)	BIND 9.16.2	CacheServe 7.5.1.1
microsoft.com. A	54 (126)	74 (194)	22 (22)
twitter.com A	388	228 (586)	28 (28)
www.gov.uk A	102	468 (1137)	90 (90)

DNSSEC validation オフ、数字は DNS メッセージ数、() 内は TCP 制御を含む IP パケット数。起動直後にクエリし落ち着くまで。

CacheServe による microsoft.com の結果 (11クエリ) の内訳

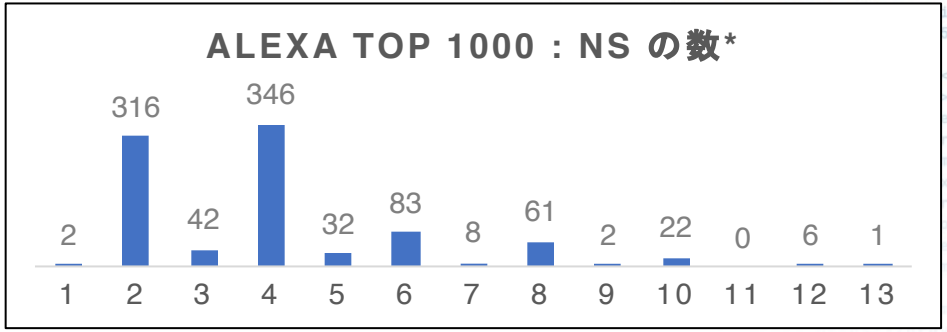
- ルート・プライミング (1)
- ルート、com.、microsoft.com. の権威サーバへのクエリと応答 (3) = 理論上のクエリ数 (広義の in-bailiwick な NS のグルーに従い解決)
- 予備的な NS のアドレス解決 (後述) (3)
- 委任インジェクション対策のために委任参照の再確認 (2+2)

参照先 NS 8 つ (12) で十分なのか？

委任の情報は通常のキャッシュとは別に丁寧に管理（右は inspection-delegation コマンドの出力より一部抜粋）

参照 NS の名前とそのアドレス解決状況(不存在を含め)保持

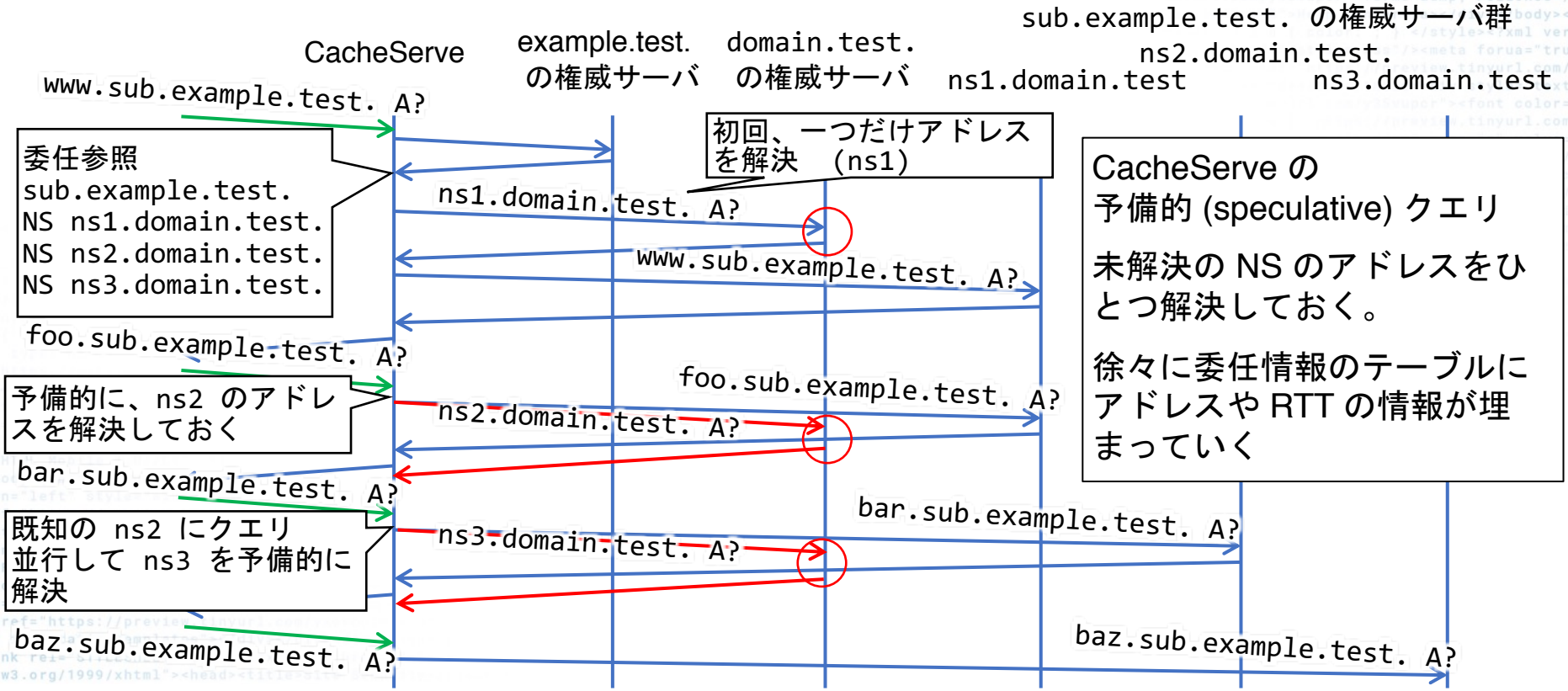
一度に(あきらめるまで)解決するのが 8 (12) までなのであり、次のクエリを処理する際にはさらに 8 (12) まで解決を行う



*委任参照ではなく、NS タイプでクエリした結果


```
"server": "ns1-205.azure-dns.com",
"addresses": [    {
        "type": "A",
        "origin": "192.42.93.30",
        "ttl": "172443",
        "glue": "true",
        "addresses": [            {
                "address": "40.90.4.205",
                "rtt": "0.008528",
                "outstanding-queries": "0"
                :
```

あらかじめ NS のアドレスを解決しておかなくていいの？



その他

Success-Based Rate-Limiting

- 権威サーバーへの問い合わせ状況と失敗をモニタし、独自のアルゴリズムで自動的にクエリを調整
- 従来型のランダムサブドメイン攻撃 (いわゆる「水責め」) でも極めて有効

Prefetch Extension

- 権威サーバーからの応答が得られない場合に限って TTL が満了したキャッシュから応答
- 2016 年の大規模な権威サーバーへの DDoS 事件を受けて追加された機能

なぜ準備できてたのか？

- 開発当初より通信事業者を主なターゲットとしてパフォーマンスだけでなく、セキュリティ、信頼性、可用性を重視
- 経験を生かしつつ、新しく作り直すことができた
  (BIND8 → BIND9 → CNS / Vantio 5 → CacheServe 7)
- 世界中の通信事業者における利用からのフィードバック
  (内容はほんとうに様々)
- 現場や研究者等からの意見に対応
  例：キャッシュ・ポイズニングに対しても、カミンスキー攻撃の発表の前にも後にも継続的に様々な対策を続けてきた

“As new DNS vulnerabilities are discovered, a layered approach such as Nominum’s will help in ensuring ongoing Internet security (Dan Kaminsky)”
「新しい DNS の脆弱性が見つかるに従い、Nominum のような多層的な手法がインターネットのセキュリティの確保に役立つだろう（ダン・カミンスキー）」


Akamai
Experience the Edge