ゾーン転送のアクセス制限に関する調査結果

DNS Summer Day 2016

2016年6月24日

株式会社日本レジストリサービス（JPRS）

阿波連（あはれん）　良尚（よしたか）

注意喚起（2016年1月12日）

- JPRSから
  - 権威DNSサーバーの設定不備による情報流出の危険性と設定の再確認について
  - <https://jprs.jp/tech/security/2016-01-12-unauthorized-zone-transfer.html>
  - JPNIC・JPCERT/CCからも同日に注意喚起を実施
- 概要
  - ゾーン転送のアクセス制限がされていない権威DNSサーバーが、日本国内に一定数存在するという情報が入った
  - 第三者がゾーン情報を入手できることは、ネットワーク構成情報の流出といった潜在的な脅威の増加につながる可能性がある
  - 意図しないゾーン転送を拒否するよう、適切な設定を行うことを強く推奨する

調査の目的(1)

- 状況の確認と改善
  - ドメイン名レジストリとして、DNSサーバーの設定状況を調査できる
    - 登録情報を用いてドメイン名の全数検査ができる
  - 指定事業者経由で、登録者に連絡できるチャネルを持っている

調査の目的(2)

- 利用者の保護
  - 組織内利用のためのドメイン名について、ゾーン情報の漏洩が潜在的なリスクとなりうる
  - ゾーン管理者のサーバーではAXFRにアクセス制限をかけていても、セカンダリ(スレーブ)でアクセス制限をかけておらず、ゾーン転送が可能になっていたという事例もある

調査方法

- JPRSのIPアドレスブロックから、AXFRクエリをTCPで送信
  - 応答の有無と応答コードを記録
  - TSIG鍵なしでゾーン転送できた場合には、「アクセス制限されていない」と判定
  - 応答内容は直ちに破棄
- 「有意な情報を含まない」ものは除外
  - 「有意な情報」ではないものとは、
    - NSレコードやMXレコードの内容に含まれるホスト名
    - 「www.（ゾーン名）」、など

調査対象

- 2016年2月
  - 全ドメイン名（.jp＋gTLD取次）
    - 1,625,107ドメイン名・73,279IPアドレス
    - のべ4,276,083件
- 2016年6月
  - 2016年2月の調査で「アクセス制限されていない」と判定されたもの（オプトアウト分を除く）
    - 60,067ドメイン名・6,967IPアドレス
    - のべ88,883件

結果

	2016年2月	2016年6月
調査対象件数	4,276,083	88,883
AXFRアクセス制限あり	2,827,588	39,908
AXFRアクセス制限なし	89,327	37,325

- アクセス制限の有無を判定できないものもある
  - AXFRクエリにNotAuthを返す
  - 委任設定ミスにより名前解決できない、など
- 指定事業者を通じて個別に注意喚起を実施
  - 2016年2月の調査結果でアクセス制限されていないサーバーが対象
  - サーバー設定方法の確認など反応あり

不適切な対策（TCPサービスの停止）

- TCPサービスを止めたサーバーが見られた
  - 12IPアドレス、3,553ドメイン名
  - 1IPアドレスが3,520個のゾーンをホストしている（海外のホスティング事業者と思われる）
- 対策として適切ではない
  - RFC 7766に準拠しなくなる
  - サイズの大きな応答でTCP fallbackできなくなる
  - DNS RRLを導入すると、応答制限した際にクライアントが応答を得られなくなる

まとめと今後の展開

- 89,327件について、AXFRのアクセス制限がされていなかった
- 個別の注意喚起の結果、37,325件まで減った
  - 意図してアクセス制限をかけていないケースも想定される
  - 一定の効果はあったと考えられる
- 次回調査は、2016年10月に実施予定