平成28年熊本地震と権威DNSサーバー

2016年6月24日

一般財団法人日本データ通信協会
テレコム・アイザック推進会議
(Telecom-ISAC Japan)
齋藤　和典

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

概要

- 平成28年熊本地震の際に、ある被災地の自治体のHPが見えなくなった。
- 原因を調べると権威DNSサーバー2台が同一サブネット上にあり、2台とも到達できなくなっていた。
- IPアドレスでアクセスすると自治体のHPは閲覧できた。
- 権威DNSサーバーを守るため、災害時にどう備えるか。

今回は、脆弱性対策、サイバー攻撃対策、他には触れていません。実際には、これらの対策も必要です。

都合により、観測データは、公開資料からは割愛させていただきます。観測データの概要は以下です。

- Telecom-ISAC Japanでは、重要インフラサイト3,000弱のレスポンスを15分に1回観測
- その中に熊本地震の被災地のある自治体HPもあった
- 4/14の前震後、地震発生30分後くらいから（アクセス集中によると思われる）接続タイムアウトを観測（2時間程度）
- 4/16の本震後は、DNSの検索エラーでアクセス不可を観測
- whoisで調べるとその自治体のドメインの権威サーバー2台は、同一サブネット上にあり、連続したIPアドレス
- 4/18AM時点で権威サーバー2台とも到達不可
- 4/18AM時点で本震直前のIPアドレスでHPにアクセスするとアクセス可能
- 4/18PMに別の権威サーバー2台は、別サーバーに変更、HPアクセスが復活

災害に備える：権威DNSサーバーを生かす

- 個々の権威DNSサーバーを守る
  - 電源確保、ネットワーク確保、耐震、防水、etc
- 複数台の権威DNSサーバーの同時アクセス不可を防ぐ
  - 複数台の権威DNSサーバーを別のネットワークに配置
    （自ら複数のネッ　トワークの用意が難しいなら）
    ISPにスレーブを預かってもらう

- もし、全滅したら
  - 新しい権威DNSサーバーを立てるので、時間がかかる

災害に備える：メンテナンス経路の確保

- 紹介した事例では、WEBサーバーは生きていた、WEBサーバーへのアクセス不可が発生した場合等には、権威DNSサーバーの登録の変更が必要になる場合がある。
- ISPにスレーブを預かってもらう場合は、直接メンテナンスできないので注意

- 災害時には、普段と異なるメンテナンス経路を利用する場合があるので、アクセス制御に注意

- リモートメンテナンスができないと、現地に行く必要があるかも

災害に備える：TTLは？

- 権威サーバーが全滅したときに備えるには、TTLは長くしたい
- WEBサーバーがダウンしたときに別のWEBサーバーに切り替えるのなら、TTLは短くしたい

- バランスが難しい