

自己紹介

名前 松下実紀(まつしたみのり)

所属 長崎県立大学

情報システム学部情報セキュリティ学科 4年

普段していること

DNSの勉強、JANOG58の実行委員 等

本調査は

福岡女子大学 4年の高木さつき さんとの共同作業です

最近ハマってること

犬の集団予防接種の動画を見る事、旅行に行くこと



このテーマに興味を持ったきっかけ

DNSへの興味

- 研究室の授業でDNSについて学んだ
- 身近な技術でありながら、想像以上に複雑な仕組みであることを知った
- digコマンドから多くの情報が得られることに面白さを感じた

テーマ選定の理由

- 岡田先生からDNSSECの普及に関する話を伺った
- 権威DNSサービスの現状に興味を持った
- 現状のDNS運用がどのように行われているのか調べてみたいと考えた

調査を通して感じたこと

DNSについて

- 身近な技術だが、想像以上に複雑
- 適切な運用・評価には専門知識が必要

調査について

- 評価基準の判断が難しい項目がある
- 「記載がないこと」の確認は特に難しい
- 調べるほど知識が深まり面白い
- 一方で根拠を探す地道な作業の連続

→根拠部分を記録しながらの作業

- ISO27017対応
 - <https://www.ij.ad.jp/svcsol/certificate/>
 - 認定書: https://www.ij.ad.jp/svcsol/certificate/iso_iec_27017_certificate-2020-002.pdf
 - dnsサービスの名前の記載あり
- SCへのログイン多要素認証
 - <https://manual.ij.jp/dp/help/53261359.html>
 - 高度な認証基盤でコントロールパネルやAPIにアクセスできる担当者を制限できます。
多要素認証が利用可能です。
- Roll Base Auth
 - <https://manual.ij.jp/dp/help/53261359.html>
 - <https://manual.ij.jp/dp/help/19004706.html#IID%E3%82%B5%E3%83%BC%E3%83%93%E3%82%B9%E3%81%A8%E9%80%A3%E6%80%BA%E3%81%99%E3%82%8B-IID%E3%82%B5%E3%83%BC%E3%83%93%E3%82%B9%E3%82%A2%E3%82%A0%E3%82%AD%E3%83%B3%E3%83%88%E3%81%B8%E7%AC%A1%E7%90%86%E8%A8%A9%E9%99%90%E3%82%92%E4%B8%BC%E3%81%99%E3%82%B8>
 - ユーザごと、契約ゾーンごとに異なる権限権限や参照権限の設定
- ゾーン転送に対応している場合TSIG対応
 - <https://manual.ij.jp/dp/help/19630444.html>
 - マネージドDNSサービスでは、安全にゾーン転送を行うためにTSIGを利用できます。
- サブドメイン名ハイジャック対策の有無
 - <https://eng-blog.ij.ad.jp/archives/5720>
 - 公式マニュアルではないが可のエンジニアのプログ
 - IJ DNSプラットフォームサービスでは、この仕様を全面的に改め、親子ゾーン同層間隔が根本的に発生しないようにしました。つまり、親子がならず別層します。親子が同層する旧サービスでは親子ゾーンから子ゾーンへの権限の譲渡がなくとも名前解決できてしまっていたが、別層する新サービスでは委譲が必須になるので、親から委譲してもらえない悪意ある第三者の子ゾーンによりハイジャックされることはありません。
 - もしくはこれ
 - <https://manual.ij.jp/dp/help/102302461.html>
 - 親ドメインのゾーンとは別に、サブドメインのゾーンを作成する
 - <https://manual.ij.jp/ds/domain-help/16187367.html>
 - 1台の権威DNSサーバが管理する範囲を「ゾーン」と呼び、そのゾーンのDNS（名前解決）のための情報を「ゾーン情報」と呼びます。ゾーン情報を構成する1件1件の情報を、「DNSレコード」または「リソースレコード」と呼びます。
 - もしくはこれ
 - <https://manual.ij.jp/dp/help/53261357.html>
 - お客様の運用するWebサーバなど各種リソースを死活監視し、正常に動作していないサーバを自動的にDNSの応答からはずすなど
- 権威サーバが地域NW的に複数展開
 - <https://manual.ij.jp/dp/help/102302456.html>
 - 本サービスでは、IJが提供するAnycast拠点に加えIJが提携する海外DNS事業者が配置した世界各地の拠点も利用できます(海外DNS事業者についてはプレミアムプランの機能)
- 適切な間隔でレスポンスレートリミットが可能であること
 - ?記載なし・見つけられなかった
- 他の権威DNSサービスとセカンダリ構成をとることが可能
 - <https://manual.ij.jp/dp/help/53261359.html>
 - ゾーン情報は複数のDNSサービスに登録できます。お客様が用意したDNSサーバ、あるいは他社DNSサービスへのゾーン転送(マネージドDNSサービス)
- 指定した地域でサービスが利用可能であること
 - ?記載なし
- SLA規定があること
 - <https://manual.ij.jp/dp/help/19634912.html>
 - プレミアムプランご契約のお客様に限りSLA（service level agreement）、サービス稼働

一社調査をしました(IIJ)

調査方法

公開マニュアルや公式サイトの調査、および事業者への直接ヒアリング

調査結果

項目	前回	今回
更新処理がDR構成になっていること	?	○
ゾーンデータの変更履歴を閲覧できること	?	○
ひとつ前の設定に容易に巻き戻しできる事	?	○
逆引きゾーンの登録に対応しているか	?	○

公式マニュアルや公開資料を調査した結果

当初は判断保留としていた項目について対応状況を確認することができた

其田さんにご協力いただきました

- 事前にマニュアルや公開資料を読み込み、不明点を整理して質問
- 疑問点が解消され、理解を深めることができた

感想

初めて企業の担当者へ直接質問し、緊張した

一つ一つの質問にとってもとっても丁寧に答えて頂いて有難かった
ありがとうございました！



今後の調査項目について

- 項目によっては評価基準が曖昧なものがある

例：サブドメインハイジャック対策

どのような機能や仕組みを対策とみなすべきか

調査項目の整理

- 現在の評価項目で十分なのか

追加すべき観点、逆に不要な項目はないか

こんな項目を追加してほしい等あればご助言をお願いします！

今後の展望として

調査の自動化についても検討したい

Webサイトやマニュアルを
クローリングして情報を収集

AIを用いて
評価項目ごとの根拠を抽出

根拠を基に評価候補の提案
(○:対応、×:対応無し、
?:記載なし・判断保留 等)

懸念点

- 同じ機能でもサービスごとに表現や記載方法が異なる
- AIによる判断だけでは誤評価の可能性がある
- 最終的な評価・判断は人が行うのが現実的？