DNSホスティング事業者のお悩み相談

NTTコミュニケーションズ株式会社
先端IPアーキテクチャセンタ
高田 美紀
2013/7/18 DNS Summer Days 2013

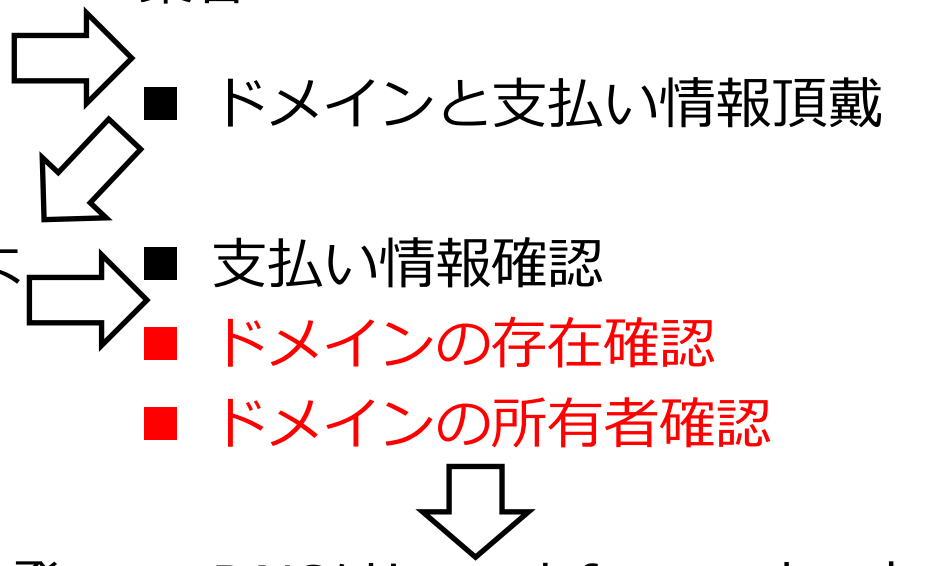
いきなりですが。。

- DNSホスティング事業者の方、挙手お願いします!
  - こわがらなくて大丈夫ですよ

前置き

- DNSホスティングって、意外と危険がいっぱい
  - わかっちゃいるけど。。という人も多いのでは
- ディスカッション形式
  - スライドにないものでもok
- プロトコル
  - 内緒の話は「ここだけの話」と前置きしてね
  - 聞いてる人は、ここを出たら忘れてね

契約の流れ



ドメインの存在確認

- そのドメイン、ほんとに存在するもの?
  - example.jp, example.com...
  - sonna-domain-arimasen-yo.jp...
- なんでチェックしなくちゃいけないの?
  - 所有者確認のため
  - 今、誰も使ってないドメインでも、明日誰かが取るかも
- どうやってチェックしてますか??
  - そもそもチェックしてますか??
- whois
  - TLDによる問い合わせ結果の違い的問題
  - 新gTLDへの対応
    - ✓ example.eco, example.shop...
- Public Suffix List
  - 管理的問題が。。

Public Suffix List

- Public Suffix
  - 直下にユーザが名前を登録できるドメイン
  - .com .org co.jp など
- Public Suffix List
  - Mozilla Foundationが管理している
    - ✓ http://mxr.mozilla.org/mozilla-central/source/netwerk/dns/effective_tld_names.dat?raw=1
  - Public Suffix Listと その問題点
    - ✓ http://dnsops.jp/bof/20080709/dnsops-jp-20080709.pdf
  - 利用API
    - ✓ http://www.dkim-reputation.org/regdom-libs/

所有者確認

- そのドメイン、ほんとにあなた(顧客)のものですか?
- なんでチェックしなくちゃいけないの?
  - ドメインハイジャック防止のため

- ちょっとおさらいしてみましょう

delegation

- 正しいdelegationとは?
  - 基本は「親のNSレコード」と「子のNSレコード」が合致
  - 間を飛ばしていないこと
  - 全てのNSがきちんと応答すること
- 正しい例
  - jp DNSでのjp zone
    - ✓ example.jp. NS ns.example.jp.
  - ns.example.jp. での example.jp. zone
    - ✓ @ NS ns.example.jp.
    - ✓ ns A 192.0.2.1
    - ✓ sub NS ns.sub.example.jp.
  - ns.sub.example.jp. での sub.example.jp. zone
    - ✓ @ NS ns.sub.example.jp.
    - ✓ ns A 192.0.2.2

delegation: 正しくない例

- 間を飛ばしている例
  - jp DNSでのjp zone
    - ✓ example.jp. NS ns.example.jp.
  - ns.example.jp. での example.jp. zone
    - ✓ @ NS ns.example.jp.
    - ✓ ns A 192.0.2.1
    - ✓ ~~sub NS ns.example.jp.~~ ←この行がない例
  - ns.example.jp. での sub.example.jp. zone
    - ✓ @ NS ns.example.jp. または
    - ✓ @ NS ns.sub.example.jp.
    - ✓ ns A 192.0.2.1
  - 自分から自分への委任であっても、delegationは必要
- でも、なくても動いちゃうんだな。これが。

delegation: 正しくない例

- lame的な事例
  - jp DNSでのjp zone
    - ✓ example.jp. NS ns1.example.jp.
    - ✓ example.jp. NS secondary.dns-hosting-jigyousha.jp.
  - ns1.example.jp. での example.jp. zone
    - ✓ @ NS ns1.example.jp.
    - ✓ @ NS secondary.dns-hosting-jigyousha.jp.
    - ✓ ns1 A 192.0.2.1
  - どちらか/両方のNSへの到達性がない
  - or example.jp. zone がない

ハイジャックの一例

ハイジャッカー

- (example.jpはdns-hosting-jigyoushaでlameになってるぽい。乗っ取れるかな)
- 契約したいんだけど
- example.jp、ほげcardだよ
- ~~.jp のDNSにhogeとfugaを登録してもらう~~
- コンパネにログイン、ゾーン編集
- ハイジャック成功!

業者

- ドメインと支払い情報頂戴
- 支払い情報確認
- ~~ドメインの存在確認~~
- ~~ドメインの所有者確認~~
- DNSはhogeとfugaです。上位DNSに登録してもらってね
- コンパネのID/パスはこれ

ドメイン名ハイジャック

- 委任先の権威DNSサーバに、そのゾーンを第三者が作成できたら?
  - ゾーン全体をハイジャックできる
  - 委任先情報の削除ミス
    - ✓ セカンダリ解約時
    - ✓ ISP解約時、など
    - ✓ レジストラント側の問題でもある
  - 正当なレジストラントかどうかの確認を怠った
    - ✓ DNSホスティング事業者側の問題
- 任意のゾーンの権威DNSサーバに、そのゾーンのサブドメインを第三者が作成できたら?
  - cookieの漏洩など
  - 正当なレジストラントかどうかの確認を怠った
    - ✓ DNSホスティング事業者側の問題

正当なレジストラントかどうか?

- そのゾーンを持っている人かどうか、確かめる
- ドメインサービスの契約者向けのDNSホスティング
  - 契約者情報を電子的にマッチング
- 他ドメインサービスの契約者向け
  - whois等の情報とのマッチングだけでは無理
    - ✓ 人手では欺かれる可能性がある
- 電子的に確認する方法
- 例: 委任情報を操作できるかどうか
  - 上位ゾーンからの委任NSレコードに、任意の文字列を設定してもらう
  - example.jp. NS nin-i-no-mojiretsu.ns.example.jp. とか
  - それを確認でき次第、deployする

電子的に確認する方法

- 委任情報を操作できるかどうか
  - 上位ゾーンからの委任NSレコードに、任意の文字列を設定してもらう
  - example.jp. NS shitei-mojiretsu.ns.example.jp. とか
  - それを確認でき次第、登録する
- 委任のない権威DNSに割り振る
  - 権威DNSサーバ(のIPアドレス)を複数用意しておく
  - 契約時、委任されているかチェック
  - 委任されていないIPアドレスの権威DNSを払い出す
  - R53方式

zone cut

- zone cut
  - A. ns.example.jp. の example.jp. zone
    - ✓ sub NS ns.sub
      - ✓ ns.sub.example.jp. の sub.example.jp. zone
        - ✓ www A 192.0.2.1
  - B. ns.example.jp. の example.jp. zone
    - ✓ www.sub A 192.0.2.1
  - Aのようにzoneを分けることを「zone cut」という

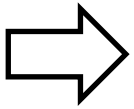
サブドメインのハイジャック防止

- zone cutしない
  - 契約はPublic Suffixの直下のみ
  - サブドメインでもzone cutしない
  - 例: hoge.co.jp, fuga.jp, hogefuga.com など
    - ✓ ×: hoge.hoge.co.jp, hoge.fuga.jp, sub.hogefuga.com など
- 親ゾーンと子ゾーンを同じDNSに存在しないようにする
  - R53方式
  - 契約時の委任チェック

解約の流れ

顧客

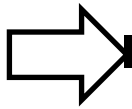
- 解約したいんだけど



業者

- 支払い状況の確認
- 上位DNSのhogeとfugaの登録を解除してもらってね

- .jp のDNSへ登録したhogeとfugaを削除
- コンパネにてゾーンを削除



- コンパネのログインIDをinactivate
- ゾーンが削除されていない場合は削除

上位からのdelegation削除チェック

- 上位から自権威DNSサーバへのdelegationが削除されたか?
- なんでチェックしなくちゃいけないの?
  - ドメインハイジャック防止のため

- 解約してゾーンがないのに「たまたま」delegationされている、という状況の危険さ
  - ドメインの所有者確認を「きちんと」やっていれば防げる、かもしれませんが...

キャッシュと権威の分離

■ 昔、聞いた話ですが。。

- 権威DNSをキャッシュとして提供
- 「浸透」問題への対応
  - ✓ ゾーンを編集したら「すぐ」反映
  - ✓ NCACHEも関係ないねー!

- その権威DNSに任意のゾーンを追加できたりすると?

- ドメインの所有者確認を「きちんと」やってない場合。。
  - ✓ ハイジャックの危険

Q&A

■ ご清聴ありがとうございました。