ネットワーク
システム管理 #13

たかさきこうや

1限 (09:00-10:45)

1

過去のお題で

- ドメイン取得についてのみ、振り返りをやってなかったので今更ですがやります
- ドメインは、基本的にレジストリの方針に従い取得の可否が決まる
- 費用は再販業者であるレジストラが決める

2

○○.co.jpについて

- JPRSがレジストリを行い、各事業者が販売する
- １法人につき、原則１個所有できる
- 日本における法人登記が必要
- したがって、皆さんが取得する場合
  「日本において、法人格を持っている組織かそれに準ずる組織に所属するメンバー」である必要がある
- 手続き上、法人格を持つことを証明する書類やお金が必要となる

3

この時

- ○○.co.jpというドメインは、「会社の」持ち物になる
- 登録担当者や技術連絡担当者は個人になるが、ドメイン自身は会社の所有物になる
- なので、個人では所有できない
  (し、個人事業主も所有できない)
  が、個人で法人登記すればco.jpを事実上所有できる

4

個人事業主

- フリーランス、個人事業主、法人の違いは、この講義の範疇ではないし僕も詳しくないので、それ系の講義を受けて勉強してください
- ただし、フリーランスより個人事業主、個人事業主より法人の方が社会的信用は増す…とされる
- 「与信」という商慣習
- 同様に、co.jpはドメインとしての格は高い

5

これに対して○○.jpは

- 日本国内に住所を持っていれば、誰でも取得可能
- フリーランス、個人事業主、法人にかかわらず取得可能
- ○○.tokyoに至っては、日本に住所がある必要すらない

6

とりあえず今から

- 9:55までは作業時間とします
- 質問があればこの間に
- なんか先週、「どこかのWebサイトを叩く」ことばかり
  フォーカスしましたが、別にtracerouteとかpingとかで
  疎通確認をする、とかでもええんやで…？

7

さて

- この講義の初回で、
  「皆さん数年後には『政策情報学部』の卒業生だ」
  「企業に就職してIT部門を押し付けられるかも」と
  そんな話をしました
- が、皆さんが
  「開業して個人事業主になったり法人を設立したり」
  する可能性だって当然あります

8

その時に

- 名刺に印刷されたドメインが
  〇〇@gmail.com とか、〇〇@yahoo.co.jp とか
  なのは論外だとしても
- 〇〇@△△.tokyo とかであるよりは
  〇〇@△△.jp とかの方が安心感があるし、
  〇〇@△△.co.jp の方が安心感が大きいのは、
  これはもう「仕方がないこと」
- 住所や電話番号に格があるのと同じで、これを工夫することで
  SEO効果が得られる

9

SEO(Search Engine Optimization)

- 検索エンジン最適化
- Google(など)で検索をするに際し、どの情報を
  上位に持ってくるか、という検索エンジン側のルールに対し、
  サイト作成側で工夫をこらすこと

10

SEOの例

- ドメイン
  - 「取得から時間が経っている」ほど信頼性が高い
  - 「ccTLDと言語が一致している」ほど信頼性が高い
    - ※.jp=日本語, .au=英語, .de=ドイツ語, など…
- Webサイト
  - 更新が頻繁であるほど信頼性が高い
  - 他のサイトからリンクされている数が多いほど信頼性が高い
  - 動的ページより静的ページの方が信頼性が高い
  - など…

11

個人事業の観点から

- 「日本から購入できる安価な海外のTLD」
  というのは、(外貨獲得のために)そのレジストリが
  取得制限を廃している、ということ
- 世界の何処からでもドメインが買えるため、
  信頼性の低いドメインが大量に増え、それが
  信頼性の低下に拍車をかける
- また、安価なTLDを運用するレジストリのネームサーバは
  概して貧弱なことが多いため到達性に難がある

12

信用されやすいドメイン

- 長く使う
- 取得時に１年とかではなく１０年で取得する
- whois情報が正しく出てくる
- 信用度の高いTLDで取得する
- 単価が高い(=レジストリにより厳格に管理されている)
  TLDを選択する

- …など、いろいろと工夫のしようはある

13

特筆事項

コロナ禍は僕たちの生活をどう変えたか

14

というスライドが

- １回目にありました

15

テレワーク

- 企業などの組織が
  『遠隔で業務を行う』
  と決め、且つあなたがネットワーク/システム担当だった場合

  あなたが考えなくてはいけないこと、とはなんでしょうか？

16

考えるべきことは4つ

- ①会社の環境は如何にすべきか
- ②自宅環境は如何にすべきか
- ③ネットワーク環境は如何にすべきか
- ④教育は如何にすべきか

17

①会社環境

- 会社には、業務遂行のための環境がある
- 物理サーバやファイルサーバがあるかもしれない
- それは社外からはアクセスできない(はず)
- NAT等があれば、そもそも直接社内環境へ到達することは
  不可能

- その「社外からアクセスできないはずのサーバ」に対し、
  アクセス手段を提供しなくてはならない

18

解決策はふたつ

- A: 社内にあるはずの環境をインターネットに出す
  - 「クラウド化」
- B: インターネットから、安全に社内にアクセスするための手段を用意する
  - 「リモートアクセス」

19

クラウド化

- クラウド＝雲
- 本来、自分でサーバを持ち、自分で運用すべきサービスをインターネット上のサービスに委ねること
- Google Driveは「本来社内にあるはずのファイルサーバをインターネットに出し、何処からでもアクセスできるように」したもの
  - Microsoft OneDriveやDropBoxも然り

20

クラウド化のポイント

- どのようなインターネットサービスを利用するか
  - ハウジング/コロケーション
  - レンタルサーバ/VPS(Virtual Private Server)
  - SaaS(Software as a Service)
  - PaaS(Platform as a Service)
  - IaaS(Infrastructure as a Service)
- そもそも、クラウドにおいてよい情報なのか
  - クラウドに適用される法律はどこの法律なのか

21

オンプレミス(on-premises)

- 自社で持つサーバ資産⇔クラウド
- サーバ内のデータの取り扱いは、サーバの所有者が決められる
- ※サーバを固定資産として購入し減価償却するか、リースを組んで費用を平準化するかは、会計の話なのでそっちで勉強してください
- この場合、社外から社内サーバにアクセスするために「リモートアクセス」する手段が要る

22

リモートアクセス

- Remote Access=遠隔からの接続
- 社外から、なにがしかの(安全な)方法で社内のサーバにアクセスする方法
- 要点は「通信経路を如何に安全にするか」と「リモートアクセスを許可する相手を如何に判別するか」

23

通信経路を安全に

- VPN(Virtual Private Network)
  - リモートアクセスしてくる相手と、リモートアクセス先を「仮想的な私的ネットワーク」として接続する方法
  - IP-Sec VPN、SSL-VPNなど、複数種類あるが基本的には「暗号通信を行って経路上で盗聴できなくする」
- ⇔専用線
  - アクセス元とアクセス先を、1対1の物理線で接続する方法
  - 高い

24

VPNの種類

- PC自身にVPNソフトをインストールし、仮想ネットワークを創る
  - リモートアクセスVPNなどとも
- ルータにVPN機能を搭載し、ルータの内側のPCはすべてリモートアクセス先のPCと同一ネットワークとする
  - 出張所、営業所などの分散拠点などで使用することが多い

25

VPNにおける認証

- ユーザ名とパスワードを利用するのが一般的
- 「ユーザ名とパスワードの組み合わせは危険」という場合は、クライアント証明書を使用することも
  - ファイルとして保管される、クライアントPCを認証する複雑な暗号
- OTP(One Time Password)を発行するトークンを利用し暗号強度を高める場合も
  - オンラインバンキングなどでは利用されている

26

しかし最終的に

- リモートアクセスを許す場合、**「今ユーザが使っているPCやネットワークは安全か」**という点が一番の問題になる
- クライアント証明書を使おうがOTPを使おうが、社員が自宅からアクセスするときに使うPCが**「家族共用PCで、家族の誰かがそのPCで不埒なことをしていた」**ら意味がない

27

②自宅環境

- 自宅から作業をするなら、自宅にPCは必要
- では、そのPCはどのように用意し、どう管理をする？

- A: 会社が用意する
- B: 社員が自分で用意する

28

会社が普通のPCを

- 用意する場合、少なくとも、
  1. PCにインストールするセキュリティソフト
  2. PCを管理するソフト
- は必要となる
- 社内に置いてあるPCの場合は、社内に管理用端末もある
- CUCの各教室のクライアントPCにも、当然「そういうソフト」が入っている

29

シンクライアント

- Thin Client
- クライアント側にはアクセス能力しか持たせず、すべての処理をサーバ側で行うよう作られたクライアント
- 安全ではないネットワーク(=自宅)に、業務端末を持ち帰らせる、という目的においては一番安全

- お金はかかる

30

BYOD

- Bring Your Own Device
- 社員が業務に私的なデバイスを利用すること
- 自宅のPCを仕事で使う場合もこれ

- まあ、褒められた行為ではないことも事実
- セキュリティソフトと管理ソフトは入れることになるが、「誰がどのような責任のもとにそんなことを強要できる」のかは疑問が残る

31

UAC

- (もはや、自宅にてPCを一家で共用するという時代は終わりを告げた感があるが)、もしそれでも普通のPCを使わなければならず、且つ、PCを家族で共用するならUAC(User Account Control)は必須
  - PCに家族分のアカウントを用意し、使う人によってデスクトップもドキュメントも切り替えること
  - 人に応じて、できること(ユーザ権限)に違いを設けること

32

③ネットワーク環境

- 少なくともテレワークを行う環境においては **「クラウドであれオンプレであれ、ネットワークの向こう側のサービスに問題なくアクセスできること」** が求められる
- それは、「帯域」「遅延」「安定性(SLA)」の観点で判断できる

33

オンライン会議や

- オンライン講義の場合、**「音声と映像」が「上りと下りで同時」に流せて「支障ない帯域と遅延であること」**である必要がある
- 1対1の高品質なビデオの場合、
  Zoom: 1.2Mbps
  Google Meet: 3.2Mbps
  MS Teams: 1.5Mbps
- だとされているが、これは帯域であって遅延ではない

34

帯域については

- うちは十分
- ダウンロード:83Mbps
- アップロード:84Mbps
- レイテンシ:2ms
- ※アンロード済み:他のトラフィックがない
- ※ロード済み:他のトラフィックがある

35

fast.comについては

- あくまで、自宅→fast.comの速度とレイテンシなので、自宅から他のネットワークへの速度が同様に出るかどうかについては担保しない
- ただしtraceroute的には、途中までは同じ経路のはずなのでそこまでの速度は担保できるはず

36

ボトルネックは

- 自宅内で有線ではなく無線を使ってる、とか
- 自宅内で無線LANを使っている最中に誰かが電子レンジを使った(2.4GHz帯)とか
- 自宅内で無線LANを使っている最中に、レーダーを受けてチャンネルを自動変更した(5GHz)とか
- 同時に2-3ストリーム流して自宅のNAPTルータのアドレス変換部分がしんどくなった、とか
- 自宅近傍で誰か他の家の人がネットワークを大量に使ったとか
- そういう原因が多い

37

④教育

- A: 自宅のネットワークとシステムの現状を把握、管理し
- B: 必要な場所やサービスまでの疎通を確保し
- C: 何らかのトラブルが発生した場合は対処し
- D: 法とセキュリティに配慮し業務を遂行する

- ことが「**一般社員にもできなくてはいけない時代**」が、コロナ禍により(不本意ながら)来てしまった

38

これは

- 教育にコストをかけるか、システム構築にコストをかけるかという天秤でしかない

- 一定のリスクを許容する、という天秤もあるけどコロナの所為で「一定のリスク」の度合いが跳ね上がった

- ※昨今のタイミングであれば、地方自治体などから助成金が出る可能性はある
  - 今後は分からないが似たような助成金は割とある

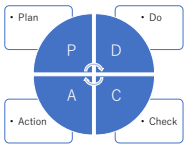
39

これらの対応を

- PDCAサイクルぶん回しつつ、自社に即した形態にもっていく(しかない)

- あたりまえだけど「一度試して駄目だった」から「全部諦める」は愚策

- 権限と予算は必要



40

この先の世界(と日本)

- ワクチンでコロナ禍が収束しないなら現在の生き方を続けるしかない
- ワクチンが完成したところで、それを全員が打たないなら撲滅はできない
- ワクチンを打っても対応できないウィルスが出たらだめ
- 就労人口は減る
- もしかしたらサービス業の業態、就労割合が変わる

41

更に

- 日本では就労人口が減ったため、効率化が求められる
  - ここ数年で「働く人が1割減る」
    - 特にサービス業で「労働力の需要」が激減すると言われてる
    - また、専門職、技術職の不足が顕著(大体どの業界も不足するけど)
    - つまり「困ったときに駆け付けてくれるサービスマン」価格が高騰する
    - 今後さらに減る

42

労働者不足への対応

- 色々なところを電子化、機械化、自動化していく必要がある
- ⇒少なくともトラブルが起きたときの一次切り分けぐらいは手元に出来る人がいないと詰む
- ⇒ネットワークとシステムの問診ぐらいは出来る人が必要だ

43

とは言え…

- ネットワークとシステムについて精通した人、というのは、世の中にそんなにいません

- その割に、ある要求を実現する方法、というのは複数あって…
  - お値段もピンキリで…
- ネットワークとサーバとシステムの全てが絡んでくる割に、それらの全てで最適解を出すのは簡単ではない

44

そういう時は

- コンサルタントを入れる、という手もありです
  - スキルによってピンキリですが…
    - 私もそういう仕事をしています
    - 「ビジネスコンサルティング」というと胡散臭い印象があるかもしれませんが…
    - 「ITコンサルティング」もそういう印象があるかもしれませんが…

45

エスカレーション

- 大事なのは「自分で問題解決すること」もですが **「問題解決が出来なさそうな時に、適切なパス(相談相手)を持つこと」**です
  - そのためにも、出来ることと出来ないことの見極めを正しくつけましょう
  - そして、可能であれば出来ることを増やしましょう

46

また、今回は

- セキュリティ関連の話はほぼしてません
- が…非常に重要です

- 個人情報保護
- 情報漏洩
- マルウェア、スパイウェア、ウィルス
- 脆弱性対策
- これらは、また別のスキルが必要です
  - 技術的な知識と、政治的な知識になりますが…

47

実際にやったネタ１

- IPによる通信に関して
  - これがちゃんと分かると、ネットワーク機器同士が、どうやって通信をしているかが分かる

  - ブロードバンド（あるいは普通の）ルータの設定等も可能
  - 社内PC群の設定も可能
- Wiresharkで通信の覗き見も行った
  - これが分かると、通信がどこでしくじっているのかが分かる

48

実際にやったネタ 2

- UNIXの操作
  - これが出来ると、ネットワークOSの操作が分かる
  - OSはシステムを運用していくに必要なので、これが分かっていると裾野が広がる
  - ネットワーク越しに「別のOSに(ログインして)いる」状態が作れるので、複数の箇所からの問診が出来る

49

実際にやったネタ 3

- DNSの運用
  - これがちゃんと分かると、通信の問題が発生した際の切り分けが可能になる
  - 通信障害の際に、回避策が明確になる

50

実際にやったネタ 4

- メール通信の仕組み
  - これがちゃんとわかると、メールトラブルが回避できる
- Web通信の仕組み
  - これがちゃんとわかると、Webのトラブルが回避できる

51

実際にやったネタ5

- コマンドやスクリプトによる情報の取捨選択
  - 情報を自分の望む姿に加工する
- ネットワーク調査、問診

52

課題について

- 中間課題1:
  IPアドレスを自動的に計算するExcelのシートを作る
- 中間課題2:
  自宅、大学間のネットワークを図示する
- 最終課題:
  「便利な」シェルスクリプトを自作する

53

課題の目指すところ

- この講義は「ネットワーク(&)システム**管理**」である
- 管理とは、「把握し、正常であるようにつとめ、よりよくする」ことである
- 中間課題はネットワークとシステムを「把握すること」、最終課題は「よくすること」を念頭においたものである
- これが自然にできるようになれば、皆さんは「ネットワーク屋」「システム屋」への扉を開いた、といえる

54

幅広くやってきましたが

- 情報スキルがある、という触れ込みで就職しようと思ったら、
  この後も続けて、色々な情報関係の科目を履修してください
  - メディア情報コース:IT
- 「ネットワークシステム管理」は、
  そういう位置づけの科目です

55

最終課題の

- 提出も頑張ってください
- PPTファイルはメールでください
  - ファイル名： c24XXXX-NSA3.pptx
    - c24XXXXの部分はアカウント名としてください
- 両方ないと評価できないので、忘れずに出すように

56

最後に

- たかさきのメールアドレスは
- kohya@cuc.ac.jp
- です
- 質問、相談、愚痴、何でもＯＫです
- もし皆さんが実際に企業のIT担当になって
  お困りのことがあれば、ビジネスベースで話は聞きます
- その場合はtakasaki@rca.co.jp　までどうぞ

57

半年間

- お疲れ様でした

58