ステップ式 最終課題の設計ガイド(基本編)
考慮するべき要件と機器や技術

reviewed 2022/07/05。 基本=前編<接触編>のみ、後編<発動編>はありません

Part I: エンジニアの仕事

インフラエンジニアの仕事のプロセスについて

- 仕事のイメージを右列に書いておきます
- インフラエンジニアというと、ふつうは**基本設計〜構築**あたりをやっています
- 法人案件は事業規模しだいで**提案の自由度は大きく異なります。** 保守や運用までやることもあれば、**(他社との差別化で)エンジニアが営業に同行して直接お客様と話す**こともあります (IIJだけ?:-)
  - そういえば最近はハイタッチ営業でエンジニア同行は普通な気がする?
  - 逆に個人向けサービスの自由度は小 (薄利多売なので、なるたけ自動化)

1. 営業
2. 要件ヒアリング
3. 提案書を提出
   - 入札の場合(入札 -> 応札 -> 落札)
4. 受注
5. 基本設計
6. 詳細設計
7. 現場調査(現調),下見
8. 現場構築(インストール)
9. 保守、運用

(脚注) ハイタッチ営業も和製英語です

エンジニアの職種について

- みなさんにはSIerの**インフラエンジニア(営業に同行)**として**基本設計と提案書の作成**をしてもらうイメージです。 IT業界用語は怪しげですが、だいたい、こんな雰囲気です

肩書	業務内容	業種
インフラエンジニア	ITインフラストラクチャの設計〜構築	プロバイダ,SIer,一般の会社も?
ネットワークエンジニア	同上(インフラエンジニアと同義語)?	同上
セールスエンジニア	営業と同行し、ヒアリング、提案書作成も	SIer(の営業技術,技術営業)
カスタマーエンジニア	障害対応やハードウエア保守の担当	フィールドサービス,サポート
フィールドエンジニア	同上	同上
ネットワークオペレータ	プロバイダの運用,ふつう顧客とは接しません	プロバイダ

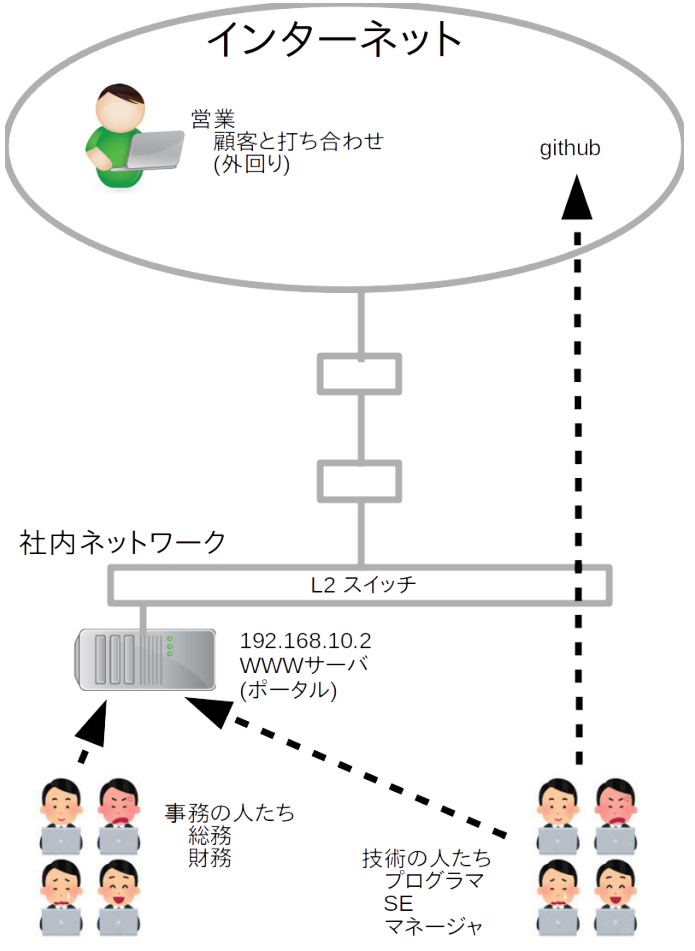
(脚注1) ネットワーク機器をいじる人は皆ネットワークエンジニア説もあり、 それだとプロバイダ〜一般企業まで該当します。 転職時には気をつけましょう (脚注2) サーバエンジニアという表現もあるそうですがサーバしかいじらないのかな? その人に発注したくないな... (脚注3) 出世するとSEになって1日中MS Officeを編集するらしいよ、何がS(=system)?

Part II: 設計の最初のステップ 基本編

参照: [大学ネットワークの設計で考慮するべき要件]

例: 組織構造: 10回目の会社を例に説明

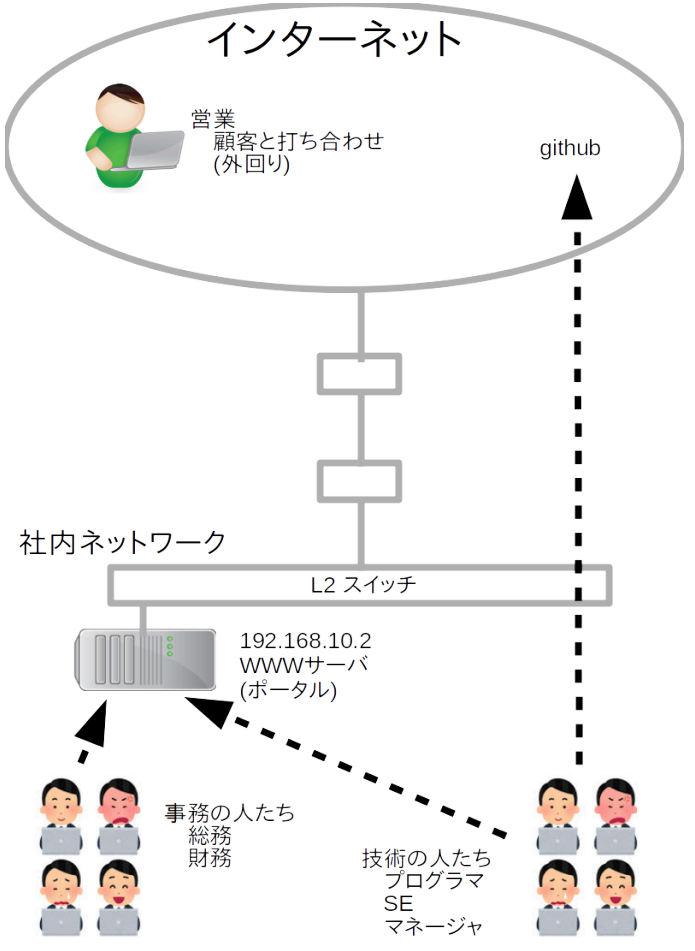
- おおまかな部署:技術、営業、総務など
- 技術 (プログラマ,SE,～マネージャ)
  - 実際にプログラムを作成するので、基本的にオフィスで仕事。 2020年からはテレワークも進む
- 営業 (見込み客の発掘～売上回収まで)
  - お客さんを発掘、訪問、ヒアリング
  - 客先訪問しないと話が進まないので外出が基本。 既存顧客とは最近ZOOMでの打ち合わせもするらしい
- 事務 (総務、人事、財務、施設管理…)
  - 基本オフィスで仕事。紙でないといけない仕事も多い。 個人情報の扱いも多いのでテレワーク化は進まず



(脚注) 仕事の仕方も違うのだから必要なIT環境も違うことがイメージできますか?

例: 組織構造と仕事の仕方

- 仕事の仕方が違うから必要なIT環境も違うはずです。 例:
  - 共通:社内ポータルは全員が使います
  - githubは技術しか使いません。 技術の人は色々なサイト(stackoverflow, qiita他)で調べ物をします
  - 事務の人は社内にある事務システム(事務用のソフトウエア製品)を使っています。 (個人や顧客の情報を扱うので)他部署には使わせません
  - 営業の人は顧客情報を含んだ提案書をノートPCに入れて持ち歩いています(危!) 提案した書類は社内ポータル(=ファイルサーバ)に置いて情報共有しています



例: 仕事の仕方とフィルタルール

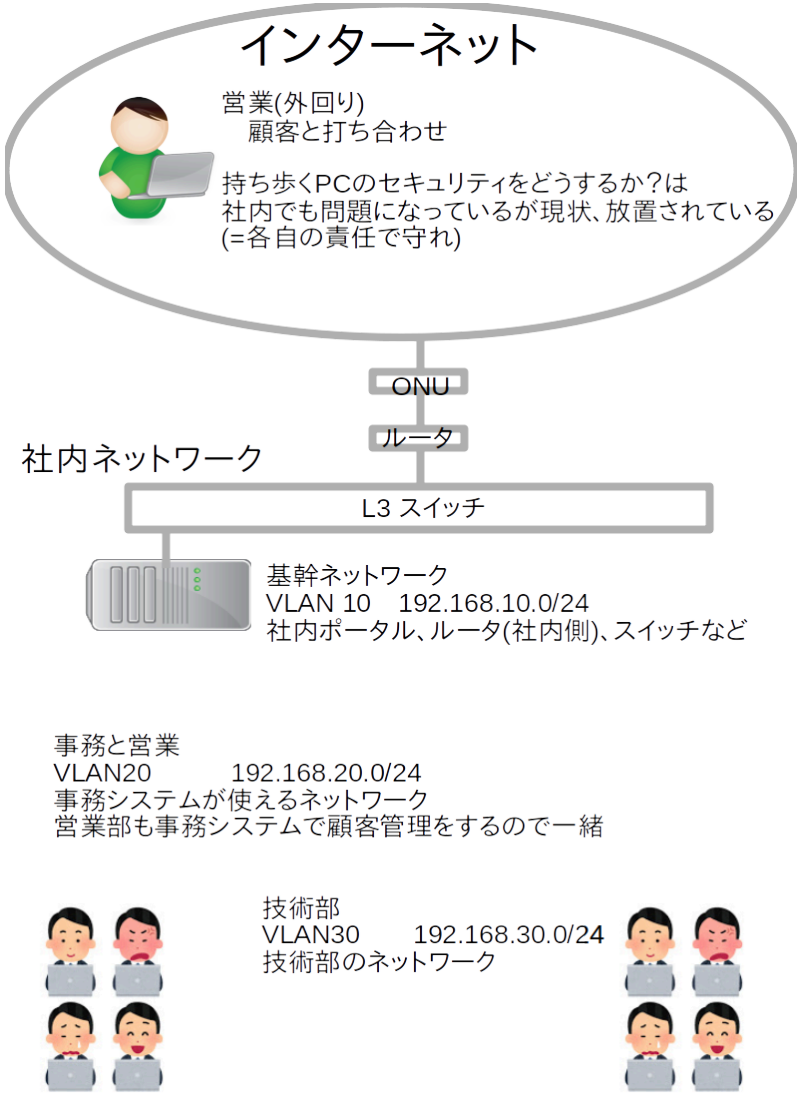
- 仕事の仕方(ネットワークの使い方)が似ている部署ごとにネットワークをまとめます
  ネットワークの設計次第で運用の難易度とくにフィルタの書きやすさが変わります
  - IPアドレスがバラバラだと簡潔にルールが書けません

```
[擬似フィルタルールの例(一部)]
! !より右側はコメント(CISCOの例)
! フィルタルールはfirst match(最初にマッチしたルールで許可/拒否を行う)

! WWWサーバには、どこからでもアクセス可
許可 FROM ANY       TO 社内WWWサーバ

! 事務システムには事務PCからのみアクセス可
許可 FROM 事務のPC TO 事務システム
拒否 FROM ANY       TO 事務システム
```

(脚注) エンジニアの腕の差が分かるということか?うむ。あと、未来予測も大事ですな

例: 10回目の会社を例にVLANを決める

- 総勢100人程度の小規模な会社
- 仕事の仕方は二種類に大別される
  - 技術部
  - それ以外(事務と営業)
- 上記の部署ごとに別のVLANを作成
  - 事務にVLAN20、技術がVLAN30
- 共用設備を置くVLAN10も作成
  - 基幹ネットワークVLAN 10
    - 社内ポータル(兼ファイルサーバ)
    - スイッチやWifiの管理画面
    - ルータの社内側IPもこのVLAN
- フィルタ
  - VLAN20は他VLANに見せない
  - 社外からVLAN10へアクセスok?
    -> よくないので後日DMZ化(#11)



STEP1: 組織構造とデータのやりとりを考える

- では、最終課題に戻ります。まず組織構造の情報は与えられていますよね?
- 自分たちが日常どのようなサービスを使っているか?を洗い出しましょう
  - 自分たちが普段つかっているサービスはイメージできますよね?
    - ただ、 **カルテ**は、 あまり使っていないようなので、 どういう情報を持っているか?このさい確認してください。 学内からしかアクセス出来ないサーバです (**VPNを使えば自宅からも利用可**です。 つまり**VPN=学内あつかい**という運用)
  - 教職員については想像する部分が大きいでしょうが考えてみてください
    - わからないところは、**お客様にヒアリング**しましょう
  - インターネット(不特定)、学生、教職員のあいだのやりとりを考えてください
    - Q: 各サービスで、どのような**アプリケーション(プロトコル)**を使っていますか?
    - Q: サービスで使う**サーバはどこに設置するべき?だれが使える?**
    - 授業のやり方に強く依存しますよね?そして2020年おおきく変わりました
      将来をどう予測しますか?(このまま、このスタイルが定着する?しない?)
- 洗い出したデータのやりとりは、あとで**ファイアウォールの設定に反映**します
- その前に、**ネットワークの基本構造(VLANとIPアドレス)**を考えます

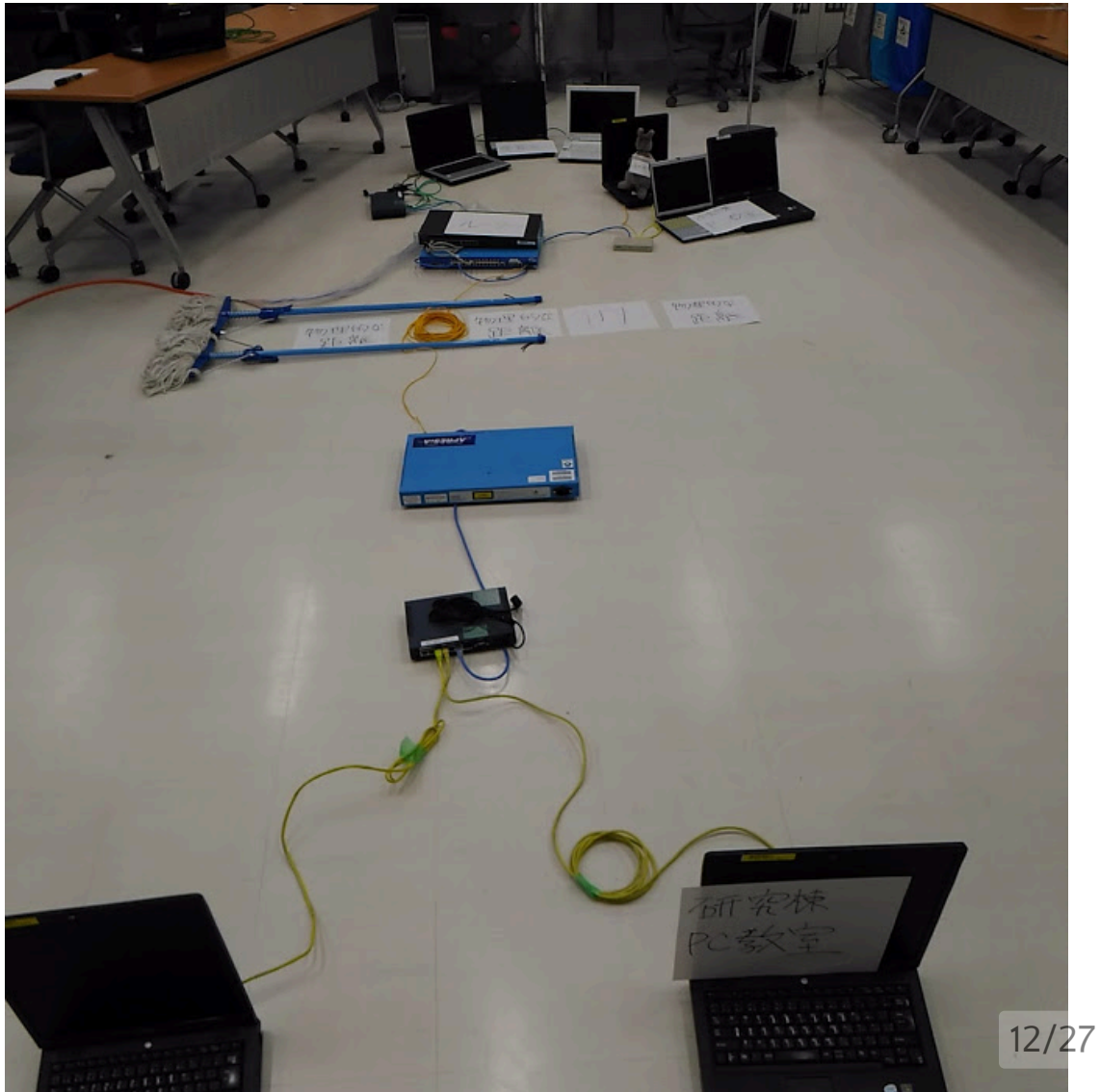
STEP2: ネットワーク構造(VLAN)の決定

- VLANとIPアドレスの割り当てを決めてください
- VLANは組織構造やネットワークの使い方と対応させたほうがいいですよ
  - Q: **いくつVLANを用意しますか?**
  - VLANつまり論理セグメントが違えば、とうぜんIPアドレスも異なります
    - 例: 実際PC教室はPC教室のVLAN(以下IDは23とする)を作っています
  - 異なるVLAN同士は分離されています、互いの通信は見えません(*)
  - PC教室はVLAN23、事務局にVLAN40、管理用に別途VLAN1などと割り振ります。
    VLAN ID(12ビット)の数字には、1〜4094が利用できます
    - 数字に深い意味はありませんが、パッと見て分かりやすいとうれしいです
      利用しているIPアドレスが連想できたりするとモアベター
    - 上の例でVLAN23なのは使っているIPが172.23.0.0/16だから
    - VLAN 1は業務用スイッチのデフォルトVLAN値です

(*) 脚注: **[セキュリティの考察]** VLANはL2的な分離を実現してくれますが暗号化はしません。原理的には、スイッチをアタックして全パケットを覗き見できれば他のVLANのパケットも見えますが、そこまでは考えず、VLANで論理的にセグメントを分ける設計をしてください

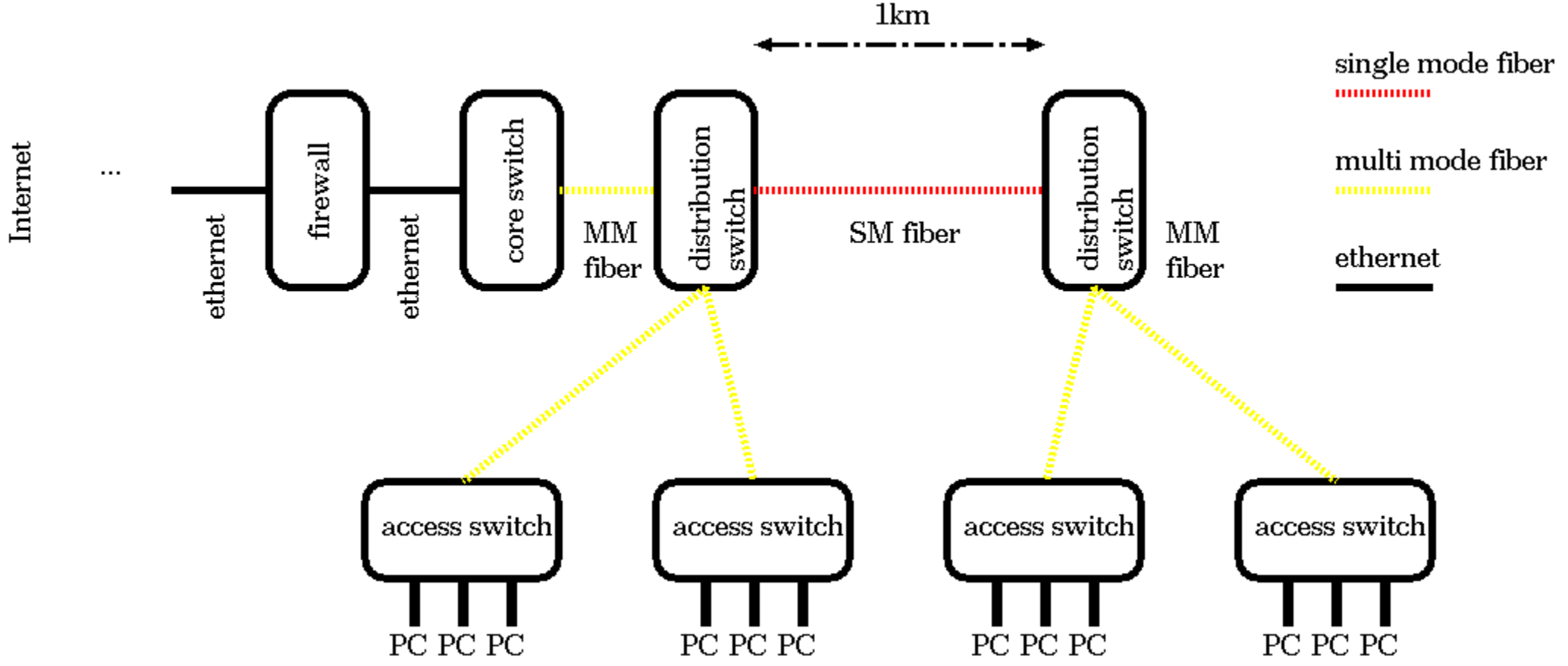
実写編: VLANと物理的機材(スイッチ,光ファイバーなど)

- 物理的にPCとスイッチと光ファイバーとケーブルと... いろいろ並べて写真と動画をとりました (力作?を堪能してね)
  - 構築するだけで5人で2時間くらい使いました (本来は、このあと設定もあるので全部やったら半日仕事)
- いやぁ物理作業って大変ですよね?
  - ブラウザでクリックすればサーバ構築できるクラウドは楽?->一見そう
  - でも、**クラウドの管理画面は、ほぼネットワークの設定です。 AWS EC2構築で思い知ってくれた?** -> 裏側のサーバやネットワークの仕組みが分からないと障害対応できません



実写編: VLANと物理的機材(スイッチ,光ファイバーなど)

- 使う配線によって速度の上限も機器の値段も変わります。 既存のファイバーは使ってOK、 Ethernetは上限1Gbps、ファイバーの場合10Gbpsと想定してください



実写編: VLANと物理的機材(スイッチ,光ファイバーなど)

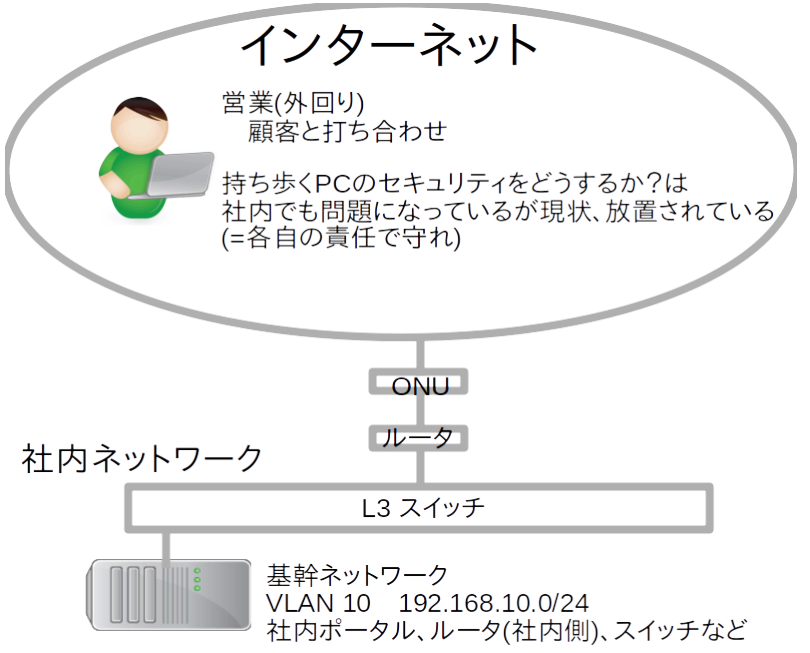
学内ネットワークのイメージ(VLAN,光ファイバー,イーサネット)

STEP3: IPアドレスの割り振り

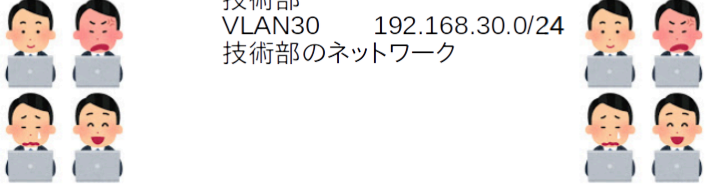
- VLANごとに利用するIPアドレスを決めないといけません
- Q: そのVLANでは**何台のデバイス(PC,スマホほか)が利用**されそうですか?
- Q: **IPアドレス(もちろんプライベート)は何をもちいて、どのように割り振りますか?**
  - 10? 172? 192? どのプライベートアドレスを使う?
  - どのくらいの大きさのネットワークに分ける?
- サブネットの大きさについて
  - ネットワークプレフィックス(e.g. /16)は何でもいいです
  - グローバルIPアドレスは有限な資源なのでギリギリであるべきですが、
    プライベートアドレスは十分大きいので、そこまできびしくしなくてもいいかなと
    - IPアドレスが余っても切れ目の良い natural mask (/8 /16 /24)を使いがちです
    - naturalのほうがネットマスクを手で設定するとき楽ですしね

例: 10回目の会社を例にVLANとIPアドレスを決める

- 総勢100人程度の小規模な会社
  - 各部署で300人体制などはなさそう
  - よってクラスC(/24)で十分でしょう
- 192.168.x.0/24を10ずつずらして割当
  - Q: 10ずつずらすのは?
    A: 将来の部署分割を想定するから
  - 例1: 事務と営業部を分ける時が来たら、192.168.20と192.168.21にする



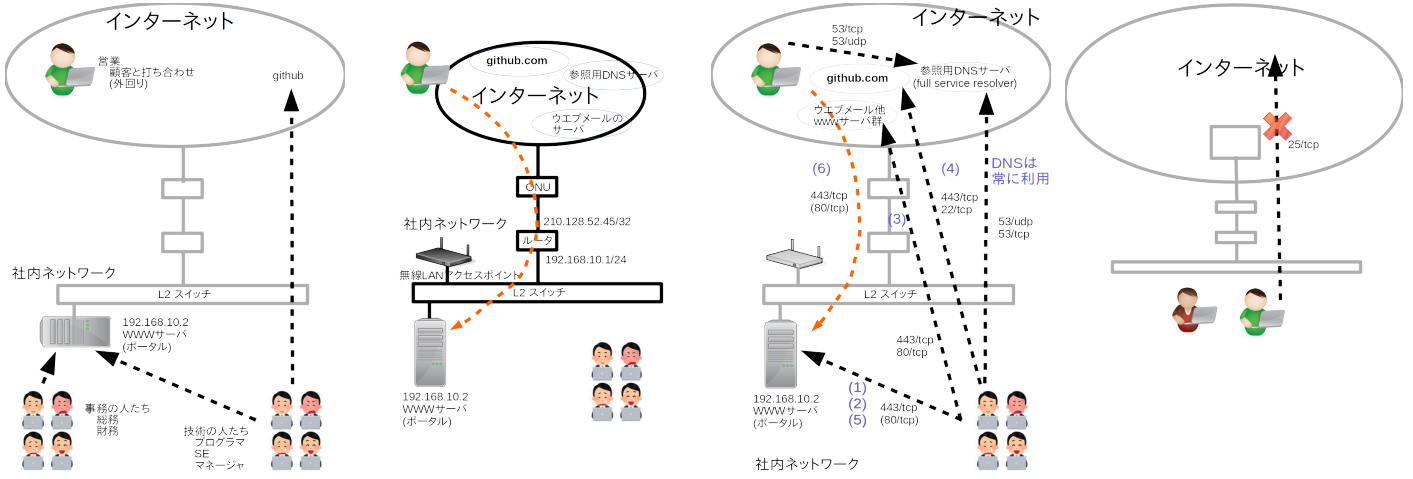
事務と営業
VLAN20　　192.168.20.0/24
事務システムが使えるネットワーク
営業部も事務システムで顧客管理をするので一緒



技術部
VLAN30　　192.168.30.0/24
技術部のネットワーク

STEP4: 通信の制限(フィルタ)

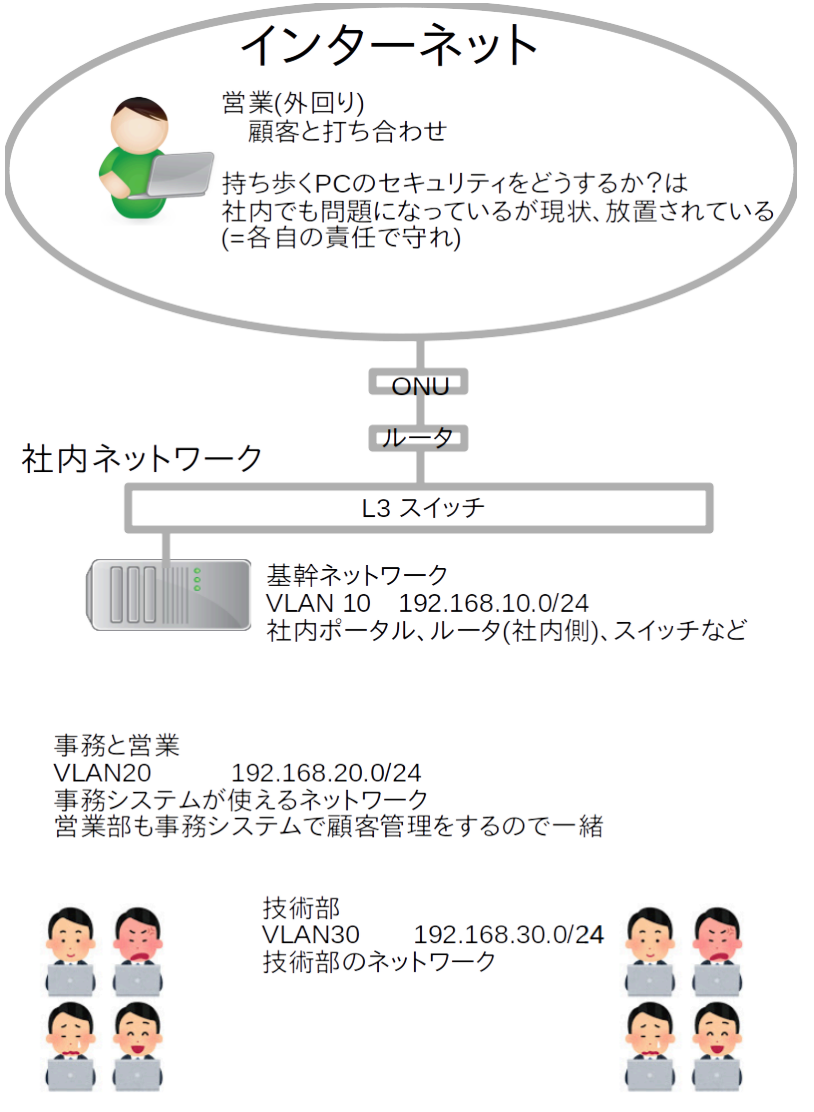
- あらかじめ不要な通信は出来ないようにしておくべきです
  - 10回目の会社の例を参照「事務システムには事務PCのみがアクセス可」
- フィルタルールは各スイッチおよびファイアウォールに設定出来ます
  - 学内間のフィルタルールはコアスイッチ
  - 学外との通信制限(フィルタ)はファイアウォール



補足: ただVLANを作るだけでは他のVLANと通信できません。 通常コアスイッチでVLAN間ルーティングを行います。 そのため学内間のフィルタルールを書くならコアスイッチです

例: 10回目の会社のフィルタ

- 部署ごとにVLAN x (192.168.x.0/24)を定義
- インターネット方向へは特別な制限なし
- 例1: 事務(VLAN 20)は個人や顧客などの漏れてはいけない情報をあつかう事務ネットワークなので、 技術部(VLAN 30)からVLAN 20は使えない
- 例2: 技術部の案件で協力会社から応援を呼びたいが応援部隊に不要な社内サービスは見せたくない。 よって彼らのPCには192.168.40.0/24を割り当てVLAN 20や30とは通信できない設定をする
- これら(社内のVLAN間の)フィルタは右図中央のL3スイッチに設定する

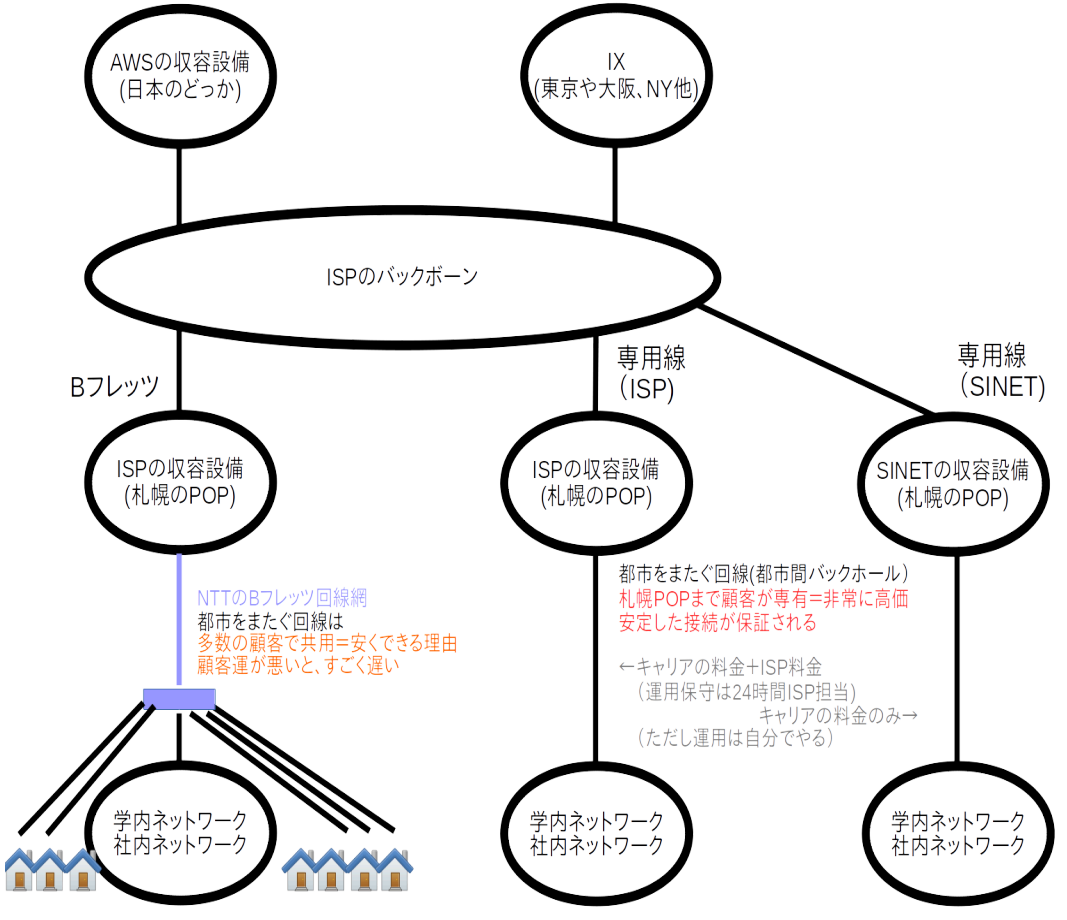


STEP5: インターネット接続回線の調達

- お客様のニーズにあわせて提案してください
  - 回線の帯域幅と価格とのかねあいが重要です
- お客様は何をお求めですか?それはヒアリングしないと分かりません。例:
  - ユーザへの安定したサービス(たとえばEL)の提供を重視したい
  - 無線LANの帯域を確保したいが、基本的におまけなので品質は求めない
  - 授業で使うZOOMの帯域を確保したい
- 回線費用は帯域によって変わるので、複数の回線を組み合わせても良いです
  - インターネットへの出口を複数用意するということです
  - そうなると、ルーティングをどうするつもりか?を考えないといけません
    - スタティックルーティング？
    - 複数の回線を使い分ける専用機材もありますけど高価です
      - 費用対効果なので専用機材を投入するメリットがあるなら提案してください

インターネット接続回線

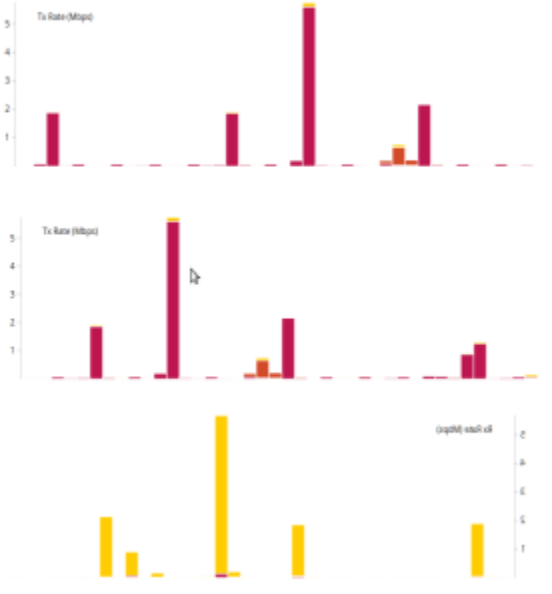
- Bフレッツ (安価)
  - たくさんの顧客で共用するから安価
- 専用線 (高価)
  - 回線を占有できるため安定した品質
  - 安心の運用: 障害は24時間ISPが対応
  - 料金は二階建て: キャリア(電話会社)から回線を買う料金 + ISPへのインターネット接続料金(運用費こみ)
- 専用線 (SINET;商用ISPよりだいぶ安い)
  - 高等教育機関向けの文科省ISP
  - ISP料金0円のかわりに、回線手配も運用も障害対応も自分でガンバレ！って国立大学は情報処理センターに人がたくさんいるからいいけど…



(脚注) SINETの運用はIIJへ依託されています。2022年秋からSINET6(100 -> 400Gbps)になります

統計多重効果とインターネット接続帯域幅の見積り(1)

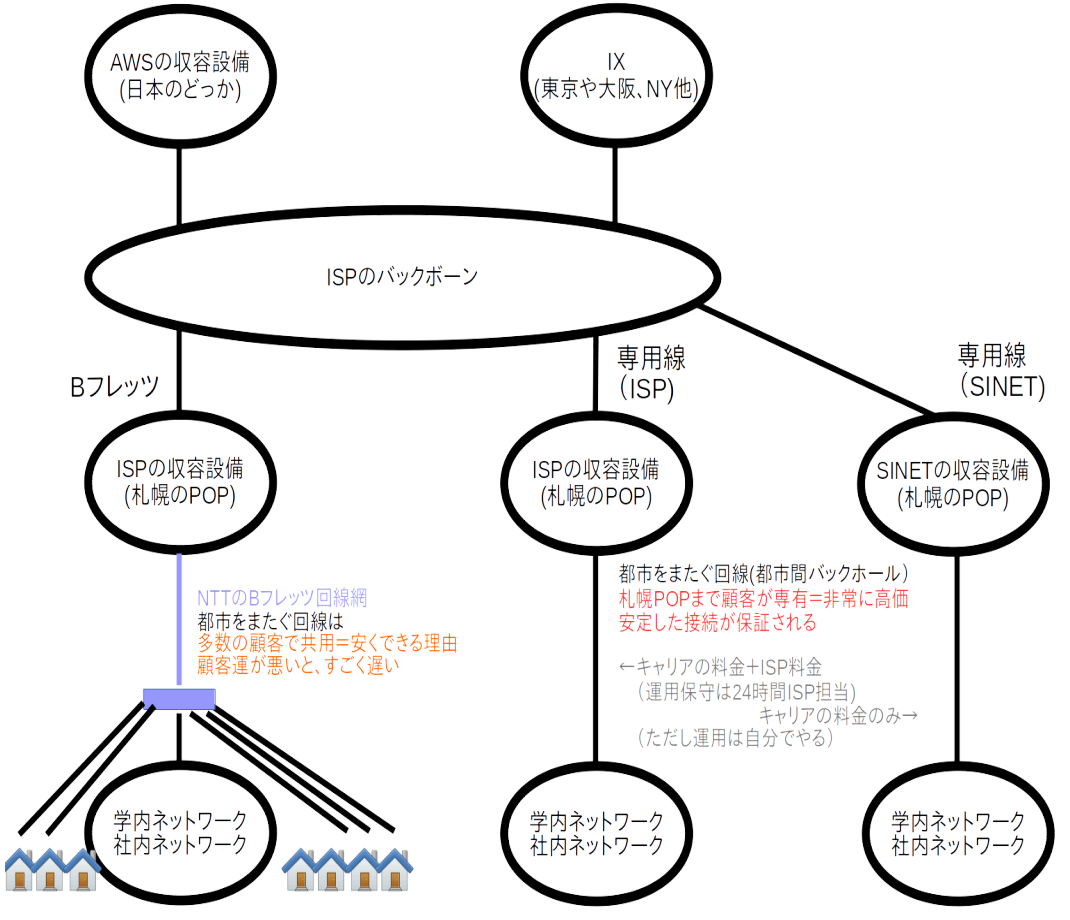
- 右図はyoutubeトラフィックの実例です
  - (場面転換?時に)5Mbpsくらいまであがり一気に転送された後、 少しずつ差分が送られているような感じに見えます。 おそらくZOOMなども同様
- 異なるアプリを使っていればデータ転送のパターンは少しずつ異なります
- 全ユーザがyoutubeを見たとしても異なる動画を見ればピークはズレます
- そのため100Mbpsの回線は「最大5Mbps使うアプリで20人が使うと限界」ではありません。 実際何人までいけるか?は状況しだいですが、 10倍収容できる説あり(上例なら5Mbpsで200人収容)



(脚注) アプリとユーザ依存; 実測すれば環境ごとに違うでしょうけど、設備を打つには怪しい仮説でもwelcome

統計多重効果とインターネット接続帯域幅の見積り(2)

- 一つの回線にどれだけユーザを収容するか?は値段に直結します
  - 低価格なBフレッツは収容人数が多い
- どれだけ収容できるか?はアプリやユーザ次第なので、 自宅のBフレッツの帯域が十分ある人もいれば、 インターネットが遅い人もいます(運悪く同じ回線にパワーユーザが収容されている?)
- 専用線は占有しているのでISPまでの帯域(千歳～札幌)は100%出ますが、 ISPのバックボーン(札幌～東京とか東京～NYなど)はユーザ間で共用なので、 契約先ISPが十分な帯域のバックボーンを用意(投資)しているか?次第です。 これがISP料金の違いになります



STEP6: さらに弊社の付加価値を提案に盛りつけよう

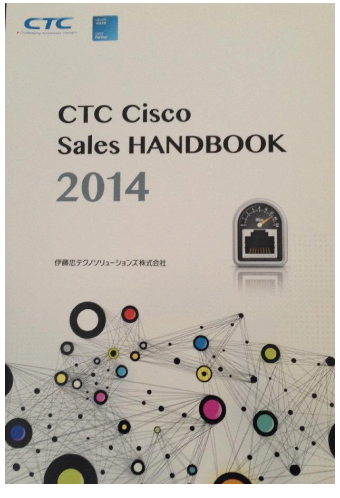
- 基本設計の必須事項としては、このくらいでしょうか
  - このへんまでは構成図の最低ラインの話で、 これに**弊社のウリ**を付け加えないと提案は通りません(-> プレゼンの評価が高くなりません)
  - そこが技術部の腕の見せ所だということです
- ウリとは**他社との差別化**のことです
  - **弊社の提案は〜について考慮しており、よりよい〜が実現できます。**例:
    - 災害対策(冗長化された回線)
    - 学内でウィルスをまいている犯人を高速に見つけられます
    - 統合運用を実現しているので運用しやすいです
    - 全員で同時にZOOMを使っても大丈夫です！
    - 授業で〜を実現でき〜が良くなります
- もちろん提案だけではだめで、**具体的に、どう実現するか?を審査します**
  - **ウリがよければ、少々高くなっても御社の提案を採用します！**

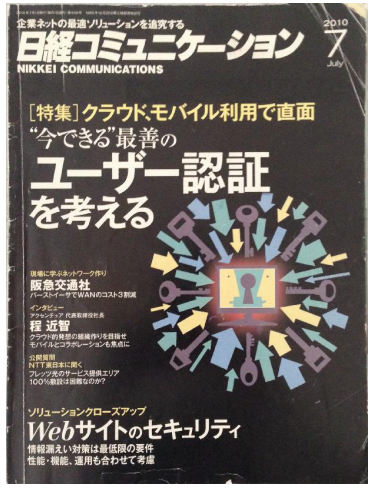
今回のお客様の評価方針

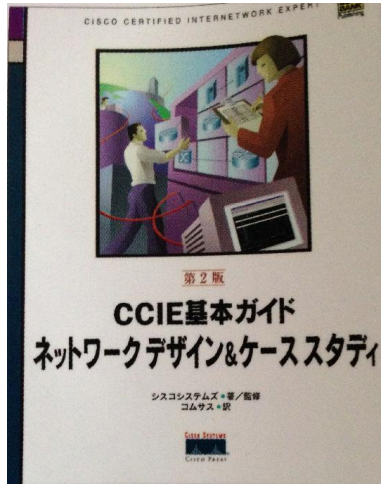
- もちろん、コストパフォーマンスも重視していますが、なにより内容重視です
  - 値段がすべてではありません、**価格にみあった提案を歓迎**します
  - ダメな例: 謎の新興メーカー製スイッチのネットワークを他社の半額で提供
- **適正利益を確保しつつ、お客様の内実をよく理解した内容のある提案**が理想です
  - 適正利益をのせていない無理な提案は、のちのち悪い結果をうみます
    - 例: しばらくすると約束どおりのサポートをしなくなったり…
    - 例: 極端にふりきった例として有名な「一円入札」とかもありますね
      - とにかく入札に勝つことが大事、そのかわり毎月いただく保守費で回収
      - ポイントは「保守費が入札でない(随意契約)」ので、この悪だくみが可能
      - あとは、ぐーぐる先生に聞いてください

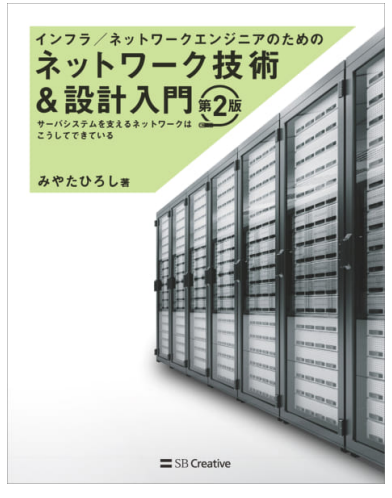
(脚注) 今回の最終課題では見積りの精度が悪いので細かい額までは見ませんが、 2倍ちがうといった極端な場合、 たとえば他社が3000万で御社が6000万の提案なら、 プラス3000万の価値を客(審査員)に納得させてください。 納得すれば買います(-> プレゼンが高評価)

参考文献









(脚注1) 左2つは業者さん用虎の巻(非売品)だけどね;-) 日経コミュニケーションのソリューションクローズアップは役立ちます。 一般には「CCIE基本ガイド」のようなCISCO社の教科書とか読むのかな?

(脚注2) 初心者向けは分からないですが、プロ向けなら、みやたひろし著「インフラ／ネットワークエンジニアのためのネットワーク技術＆設計入門（第２版）」(SBクリエイティブ,2019) あたりが良さそうです(一番右)

さいごに、はげましの言葉

- あと3回しかない！と、ドキドキかもしれませんが、がんばりましょう
  - インターンシップでネットワーク設計くらいやったことありますよと言えるといいですね!? って、あまり自慢されすぎても困りますけど…
- 大丈夫、大丈夫、ほれ、ジブリをみてみろと
- 往年の宮崎駿マニアは**最初の２つ以外はどうでもいい**と思っているものです
  1. 未来少年コナン (1978,最初のテレビ監督作品、youtubeで全話みられます)
  2. ルパン三世カリオストロの城 (1979,最初の映画監督作品)
     - **カリオストロの城なんて、こんなありさまなのに、伝説の出来ばえ**
       - 素人アニメータの集団(テレコムという会社)の新人研修教材として製作
       - 作画期間わずか3ヶ月なのに、 教育担当の作監の故大塚康生さんは途中で2週間行方不明とか(w)、 いろいろなが逸話がありますわ
- (カリ城を反省して) **宮崎駿に豊富な資金と人材と十分な制作期間をあたえたら映画がおもしろくなるのか?** と言うと…ねぇ?([自由課題] ジブリの映画群と比較してみよ)

(脚注1) ただ、カリ城、話の整合性はないけどね！いいんだよ面白いんだから

(脚注2)もちろんレーザーディスク(<-それも初版)で持ってるよ(^^)カリ城はDVDも持ってるな

[おまけメイキングページ] WARNING

- 最低ラインの案内は、ここまでです
  - あとはブレインストーミングして自由に想像するか
  - お客様にヒアリングしてください
- このあと Part III 以降では、さらに細かな話をしています
  - SIer会社の新人研修やるならこれくらい話す(かな?)という内容を語っています
    - そこそこ本気ですが、まぁ五割くらいの本気度かな
    - 全力でやったら**胃もたれ(?)**ではすまないとおもいます;-)
- よいプレゼンを作るために、このあとの解説も見て頑張ってもらえるといいな
  - とは思いますけど、かなり**脂っこい**話(<-これも業界用語?)をしてますからね:-)
  - まぁ、このあとは、いわゆる「参考」資料相当です

(脚注1) 警告ページ終わり、では、まいりましょうか！(ここまでがオリジナルのスライドでした)

(脚注2) けっきょく南極、このあとの発展的なスライドは作成されませんでした:-)

(脚注3) このスライド(基本編)で胃もたれと言われそうですわ(お嬢様部が流行なんでしょ?);_;