FAQ

(脚注) 2021年度版をもとに改良されたものです。 2022/07/05 reviewed

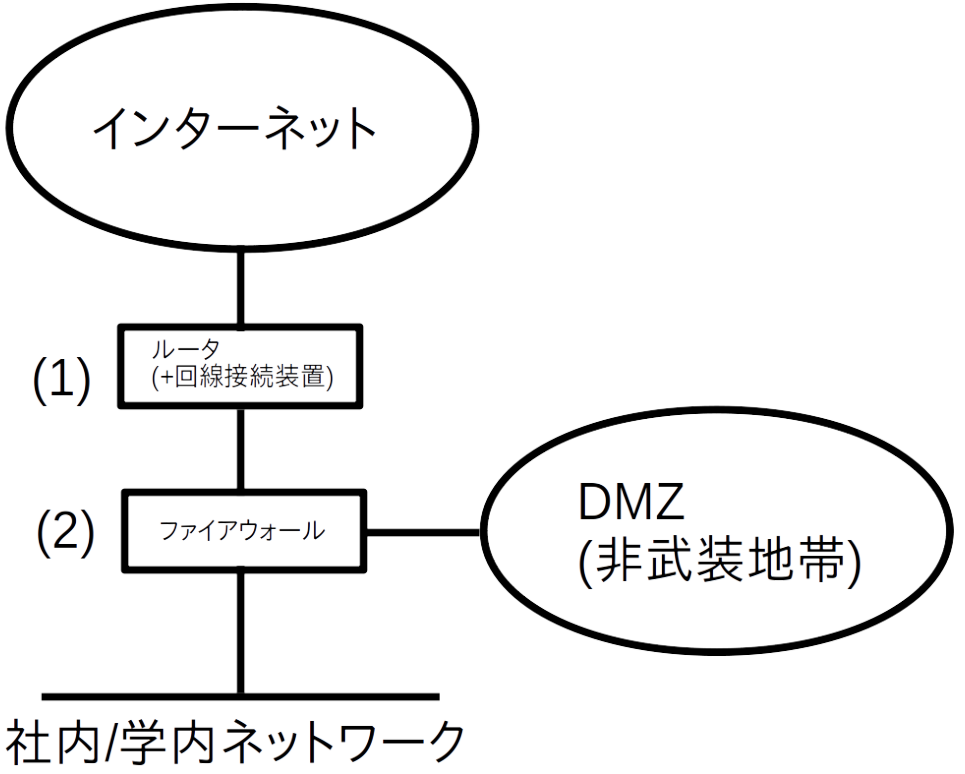
凡例

- FAQです
- 現状はどうなっていますか?のたぐいのFAQをまとめました
- 提案の相談(こういう提案はどうですかね?)は収録していません
  (それが各グループのウリだから)

FAQ: 有線ネットワーク
- おもに物理的な話 -

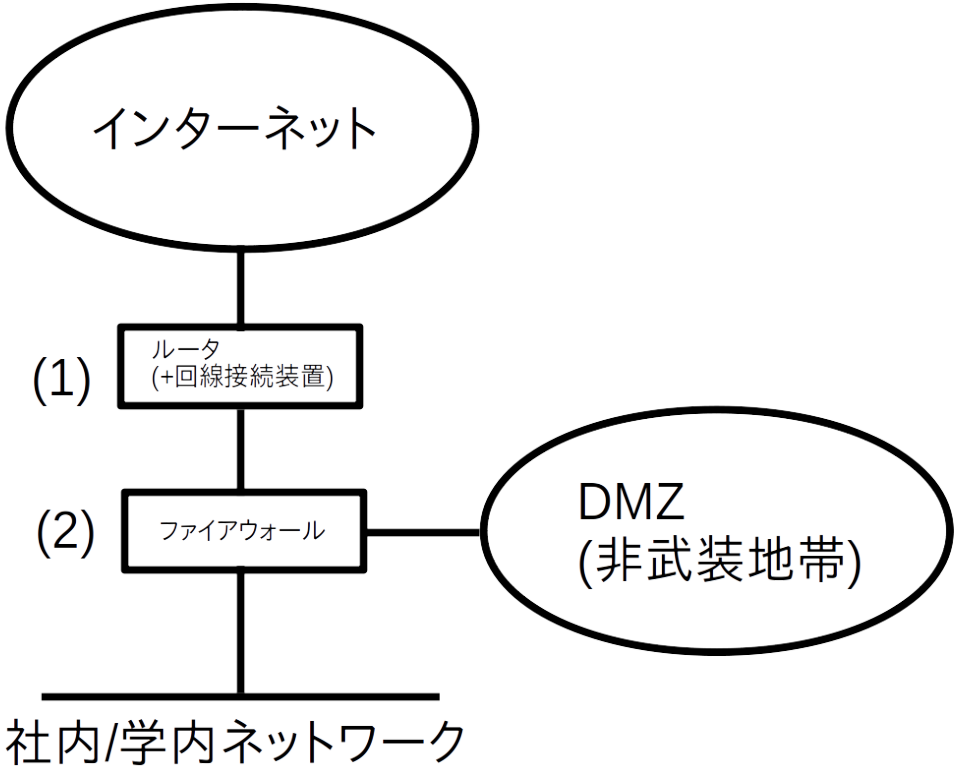
ELやポータルなどのサーバはどこにありますか?

- DMZです。以下の想定に基づく判断
  - **学内からでも自宅からでも同じように使えるサービスを提供するには DMZに置くべき**という理由 (第5回のインターネット層前半を復習)
  - 基本、授業で使うのだから、おもに学内から使うに違いない (少なくとも2019年までは正しかった)
  - 学内から安定して使えることがのぞましいです。 DMZなら、まんがいち**インターネット接続回線に障害がおきても学内からの授業は続けられます** (ここが一番大事なところ)



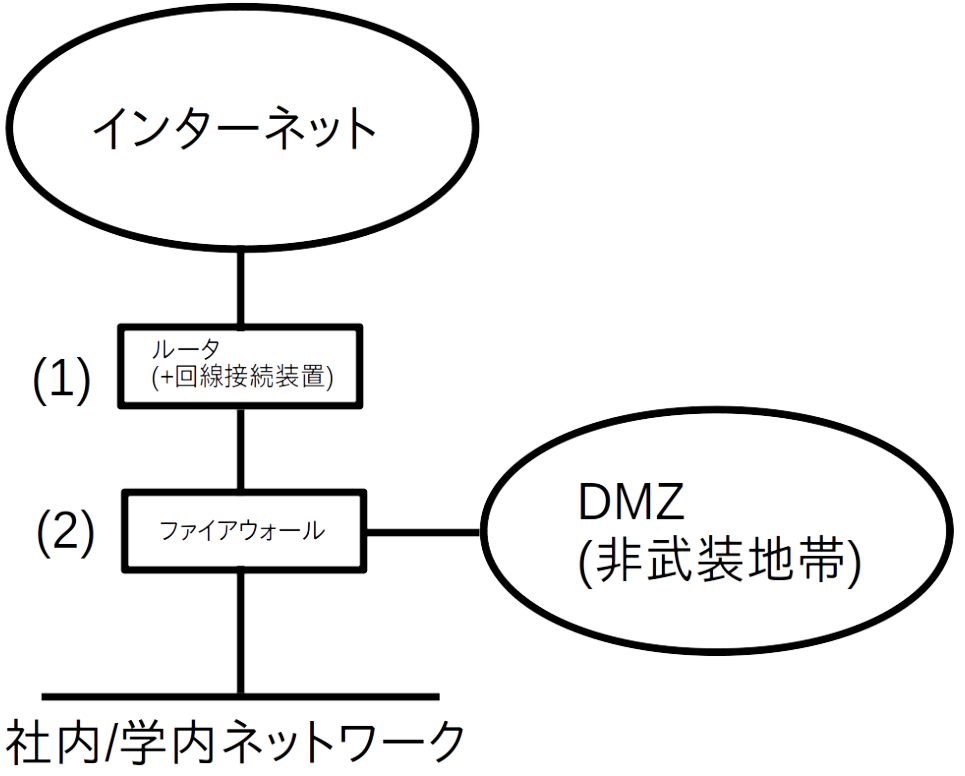
ELやポータルなどのスペックや価格は?

- たしか、サービスごとに一台ずつ物理的に存在しています
  - ポータルはポータル、ELはEL(学内用)、EL(学外用)というふうに別々のサーバがあります
  - あと(見えませんが)裏側に別途データベースサーバなどもあります
- 原価表に物理サーバ(1台)の例が出てくるので参考にしてください (ただ、たしか、もっと高価格なサーバだったような覚えがあります。 まぁ、ものすごく精密な見積り演習をするのが目的の授業ではないので、 課題としては価格表を参考に考えてもらえば十分です)



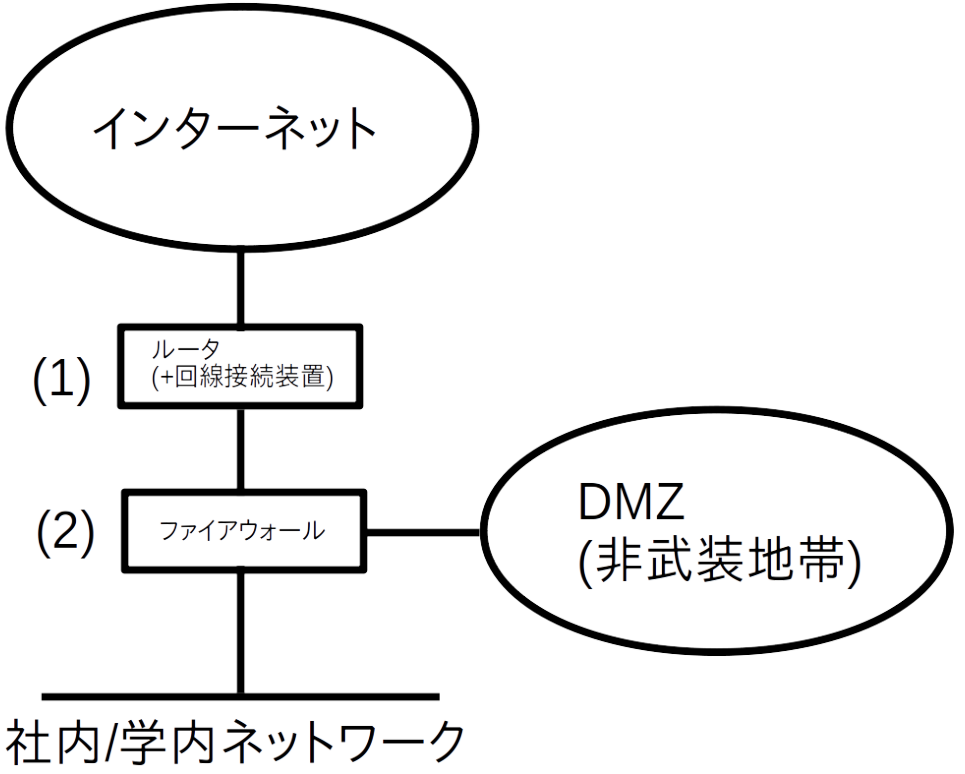
メールサーバはどこにありますか?

- 学外です
  - 現office365はマイクロソフトのデータセンター (具体的な場所は不明)
- 先代のA-Cloud(2013-2020)もクラウドメールなので学外でした
  - CTCのデータセンター、たぶん東京のあそこかあそこ(ないしょ)
- その前(2代前,1998-2012)は学内にありました、いわゆる**オンプレ**なサーバです
  - ラック一本くらいある巨大なサーバでしたね～ (ちなみにラックは**600x900x2000mm**くらいのサイズ感 (ちなみに、これが42Uユーロラックという代表的サイズ))



メールサーバのスペックや価格は?

- オンプレ時代より安いクラウドメール(A-Cloud,Office365)が候補で、 それらを探し、検討して、導入を決めました
- 法人サービスかつ教育機関向け価格なので定価は不明です (法人価格は顧客の規模や力関係などで大きく異なるため、 詳細は互いに明かさないのが業界の仁義になります、だからナイショ)
- Yahooメールが「一人あたり月額300円」らしいので参考にしてください (Office365は、メール以外の機能やOfficeライセンスもついてくるサービスなので、 メールだけのYahooよりは少し高めの価格なのではないかとおもいます)



メールサーバでgmailは検討しなかったのですか?

- 2000年代の終わりごろから大学へのgmail導入が流行していました(例: 日本大学)が、
- 日本のIT産業がダメダメなので、クラウドサービスのほとんどは外資系です
  - となると何かあって揉めたときにどうなるか?を考えておく必要があります
  - 先に裁判所に訴えた会社の最寄りの裁判所の管轄になり、 かつ、その裁判所のある現地の法律が基準になります。 Goolgeと揉めてカルフォルニアで裁判と言われたら、もうどうにもならないので、 そんな怖いサービスは買えません
- 2012年当時、国内設備のクラウドメールで価格的にOKだったのはA-Cloudだけでした
- いつものようにライバルを研究する能力ピカイチのマイクロソフトは、 2010年代のなかば以降、 Office365のデータセンターを国内に複数つくり、 「裁判は国内でOK、日本の国内法でOKです」とOffice365の仕様を変更したので、 Office365が候補として考えられるようになりました
- Googleは国内法の適用について今でも明言していません

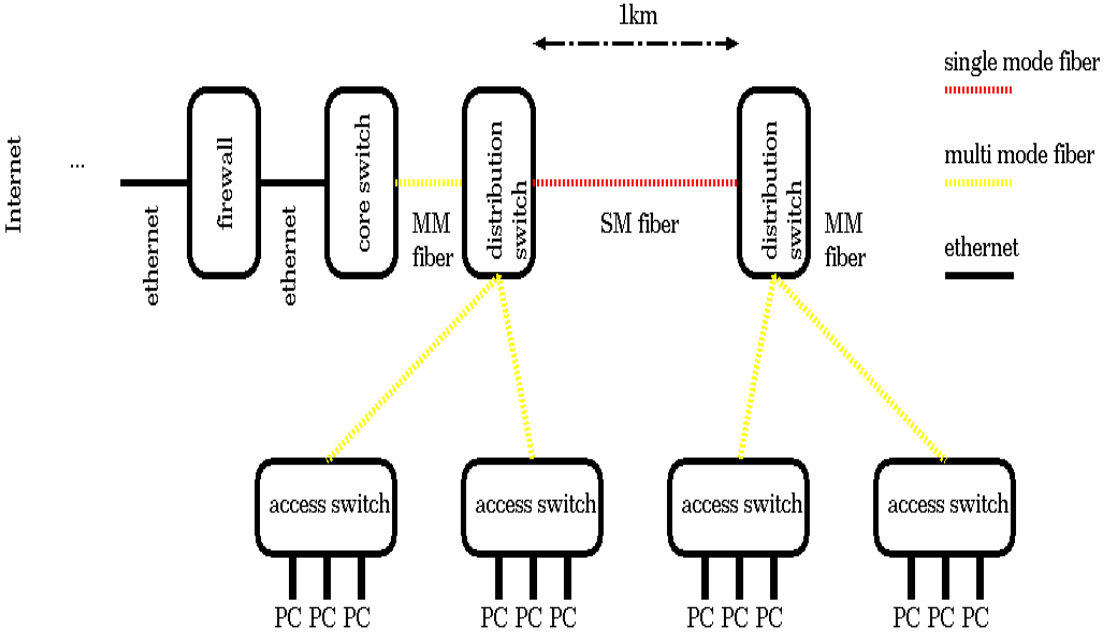
(脚注)誰にも聞かれてないけど答えておきます:-) 腕のあるエンジニアさんなら、ここまで考えて提案してくれるはず！ こういうことを考えてない企業も大学も浜の真砂の数ほどありますが、ほんと適当だよなと

新棟が増えて変化したIT環境は何ですか?

- 大きい変化は無いと思います
- ユーザ数については、プラスマイナスゼロです
  - 新棟の2F,3Fに情報システム工学科が引っ越すのですが、 単に研究棟のマイナス分が新棟プラス分になるだけなので、 大学全体としては変わらないわけです
  - ユーザ数が増えないので、利用する機器(PCやスマホ)の数も同じですよね
- 大学全体として、1つ建物が増えて部屋数が増えましたが、それだけ…じゃないかな?
  - 研究棟側で空いた1学科分の部屋は多目的に転用されてます
- 前よりゆったりとした空間になり平均人口密度は低めになったのかもしれませんが、 1つのwifi APにつながるユーザ数が減ったか?は不明。 人の集まる場所が移動しただけで集まるところには集まっているから H101とか学生ホールのwifiは今も昔も忙しそう?
- それよりも(たまたま新棟と同時に) **2022年3月ネットワーク機器(スイッチやwifi)を新しくしました。 建物よりもこの更新の影響のほうが大きいはずです**

新棟への物理的な配線は?

- コアから新棟へ光ファイバ(MM)を新設
- 建物内は他棟と同様で以下のものを事前に敷設します(設計時に前提としてOK)
  - コアからdistribution(1個)までの光ファイバ(MM)
  - 1F〜2F, 1F〜3F間の光ファイバ(MM)
  - フロア内のイーサネット配線(1本あたり1Gbpsは大丈夫)

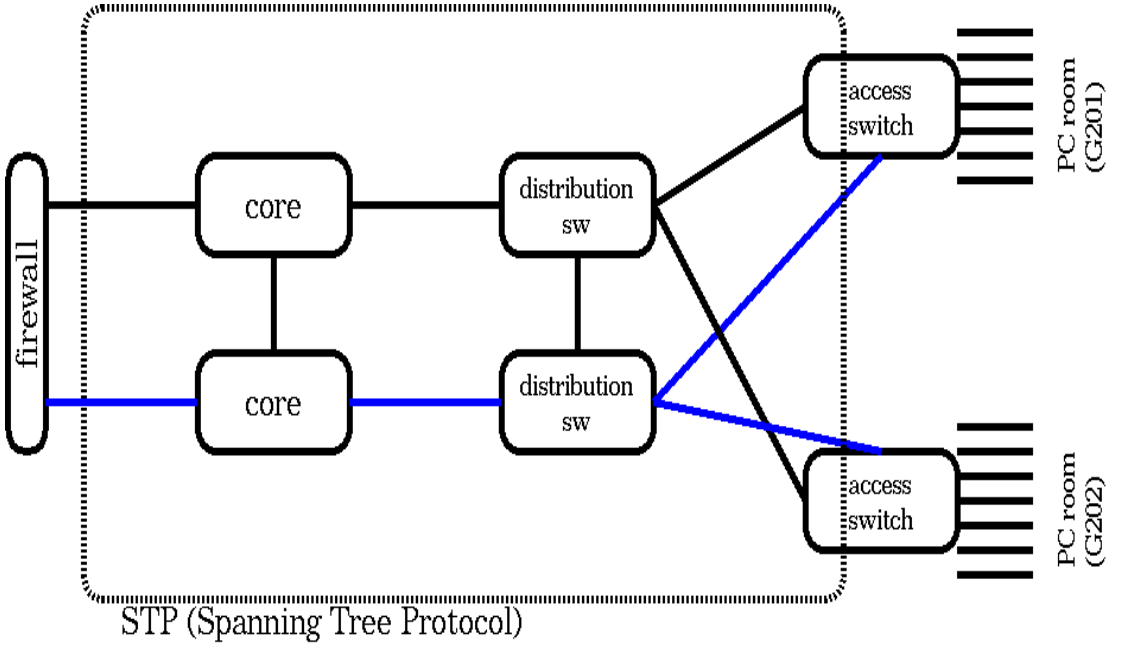


サーバは何台構成ですか?(冗長化)

- クラウドは冗長化されています(詳細は不明)
  - サービスとして買っているものは、すべてプロバイダの設備になります
  - 機器構成は非公開です
- 学内のサーバは1サービスにつき1つです(冗長化されていません)
  - それぞれのサーバが搭載している記録媒体(ストレージ,HDDやSSDのこと)は冗長化されていますが、 筐体(電源,マザーボード,CPU,メモリなど)は一つしかありません
  - 筐体に異常がある場合はサーバを停止して修理するしかありません
- 「冗長化するべきか?」と聞かれれば「出来るものなら冗長化が理想」と回答しますが、 冗長化できるようにアプリケーションが作られていなければ動作しません。 それはもうアプリケーション層の上側の(TCP/IPとは関係ない)世界の問題です

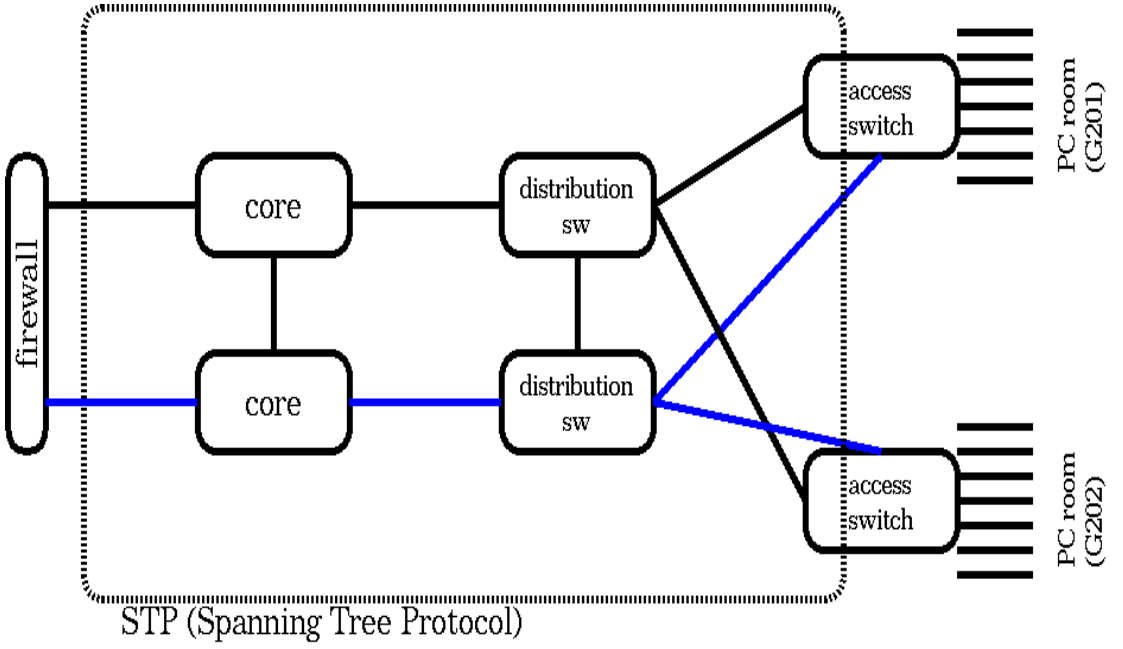
スイッチは何台構成ですか?(冗長化)

- G201,G202～コアは冗長化それ以外は1台
  - 図のようにcoreとdistribution swが2つずつあり片方壊れても大丈夫
  - G201のaccess swからのuplinkは2つのdistirubion swへ。G202も同様
- 大昔とちがい今のスイッチは壊れないです。 予備機材を1台ずつ買っておき小一時間で(大学職員が)機器交換する想定
  - PC教室での授業は止めない設計ですが、 そこ以外の講義室や研究室では対応に少し時間をもらいます。 そのかわり業者さんの現地対応が不要になり、保守費の大幅削減が可能になりました



現在のスイッチの数はどうなっていますか?

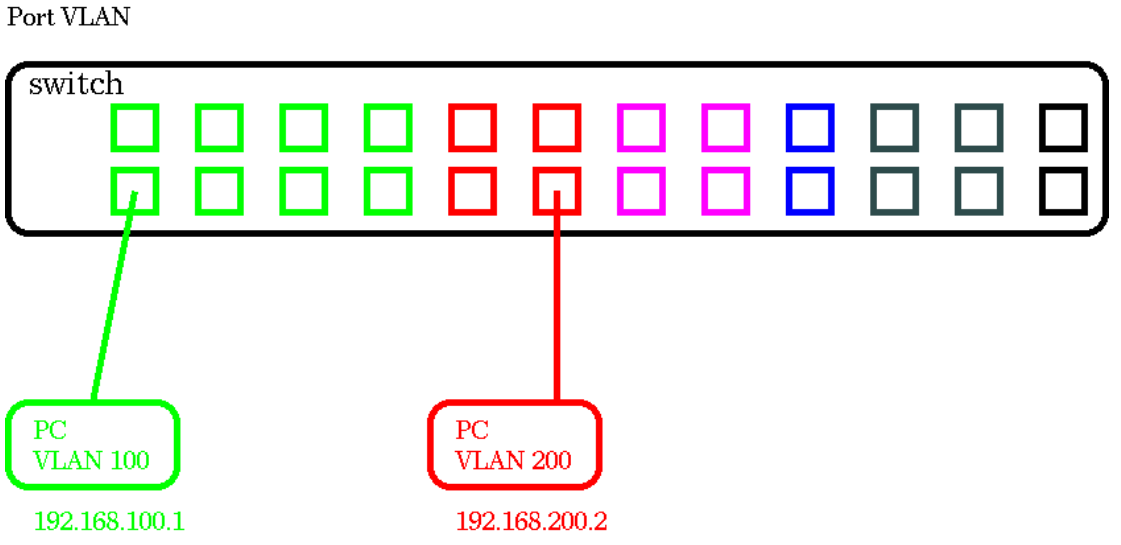
- L3(VLAN間ルーティング)機能が必須なのはコアSWだけです
- よって最小構成ではコアだけがL3、のこりはすべてL2スイッチで動作可です
  - コア～10周年記念棟間の冗長化プロトコルはL2で動くSTPが基本です
- コアのL3が2個、 各建物にdistributionが1(10周年記念棟は2)個、 あとは各フロアにアクセススイッチが平均2～3個
  - 必要なポート数(利用するデバイスの数 = おおむねユーザ数)次第
  - アクセススイッチのポート数は48もしくは24です、必要な台数分のL2スイッチを買います



(脚注) [発展] あんまりSTPは使いたくないので、LAGくむとかOSPFとか考えたいんだけどもね～

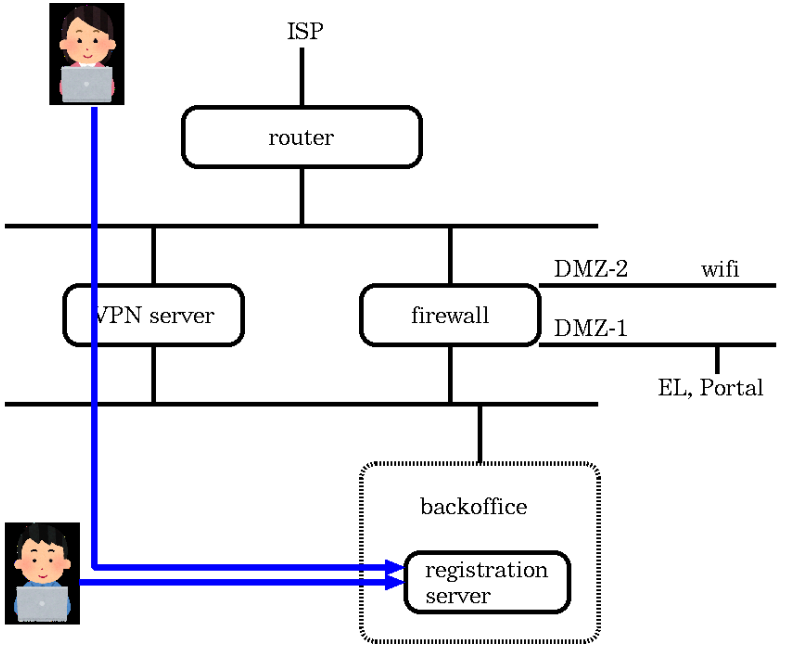
IPアドレス帯ごとに別のスイッチが必要ですか?

- 不要です
- 各スイッチへはVLANが伸びているので、 各ポートごとに異なるVLAN設定(ポートVLAN)を入れます
- スイッチの数はVLANの数ではなく物理的に必要なポート数(ポートに挿すデバイスの数)で決まります



VPNサーバはどこにありますか？

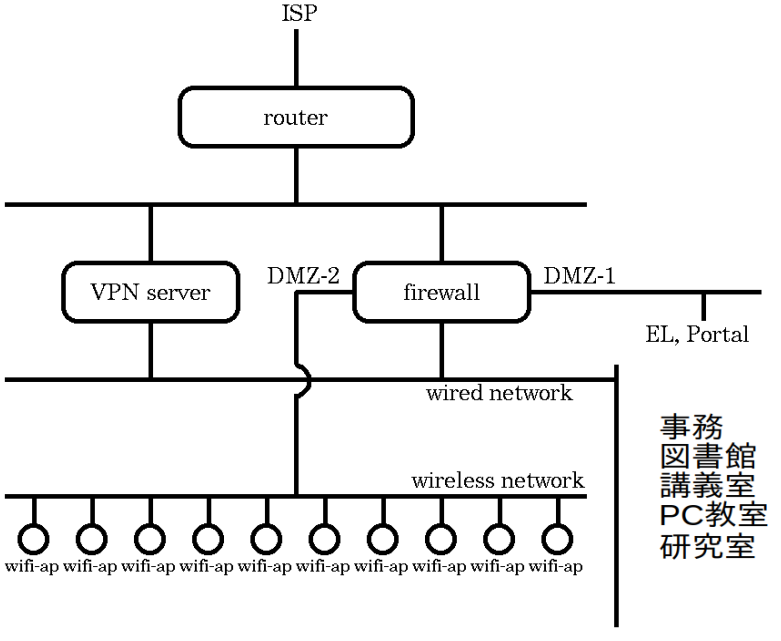
- ファイアウォール(FW)の横です
- 本学ではインターネットから見えている部分のネットワーク機器は自営ではなくISPのサービスを購入しています
  - 障害対応する人手がいないから
  - サービスなので24h365d業者が対応
- 一般にはFWに同居が多いと思います
  - FWのオプションでVPNが購入可
  - 原価表のVPN(未完)は、この構成



FAQ: 無線ネットワーク

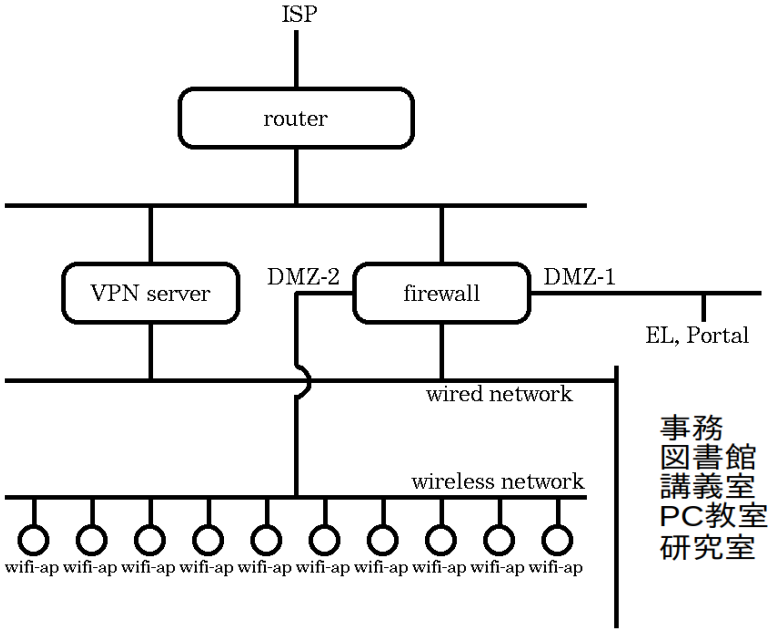
WiFiは学外にどう接続していますか?(ネットワーク構成)

- DMZその2(DMZ-2)経由でfirewallから学外に出て行きます
  - 学内のwifi AP群を収容するwifi用のVLANがあり、それがDMZ-2に相当します。 その論理セグメントの出口はfirewallです
- SSIDがkagidai(およびkagidai5)のwifiは、店舗のwifiサービスのような運用です
  - インターネットだけにアクセス
  - DMZはアクセス可
(インターネットと同等のあつかい)
  - 学内にはアクセスさせません



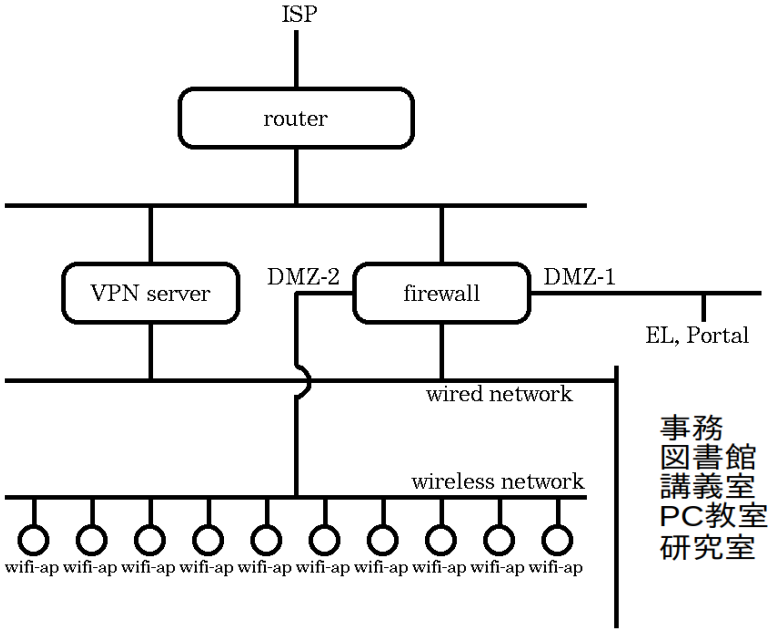
WiFiから学内は見えますか?(ネットワーク構成)

- SSIDがkagidai(およびkagidai5)のwifiからは学内が見えません
- 一世代前の無線LANでは、 ネットワーク認証(個人を特定した上でwifiを許可する)対応の無線LANを使うことで、 学内に接続を許すようにしていました (当時はパスワード認証でしたが、 いまどきの認証は単なるパスワードではなく証明書の利用が推奨されています)
  - この方式の標準規格として802.1xがあるので調べてください



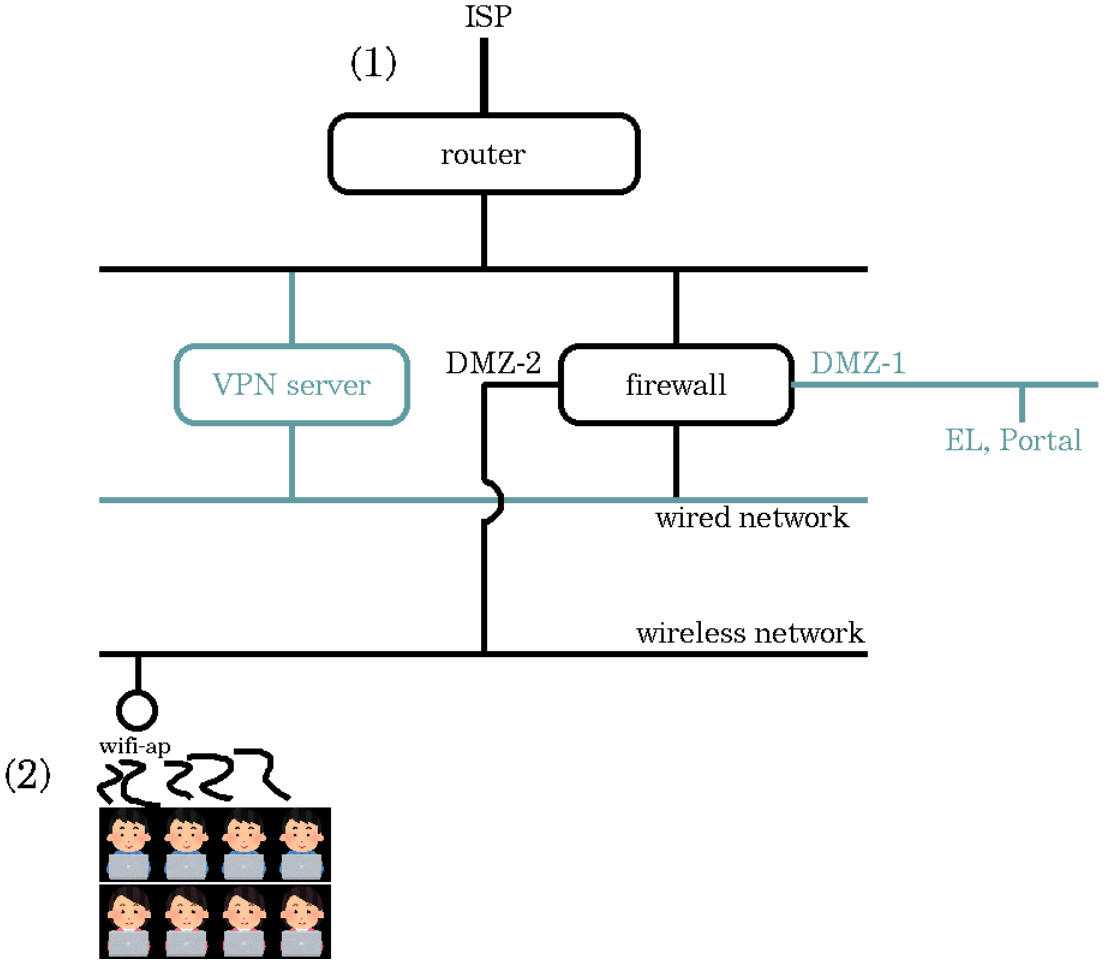
WiFiのAPは何台くらいありますか？

- 研究室(個室x1、実験室x1)、普通の講義室は2台ずつです
- 目安として30〜40人をAP1台でさばいていると考えてください。 よって、B101やH101などは、もっとたくさんのAPが必要



wifiが遅い理由には何がありますか?

- ボトルネックの主要因として (1)「インターネット接続回線の帯域」と (2)「AP自体の能力」の2箇所が考えられます
- (2)は(2.a)APの能力が低いかもしくは(2.b)APの設定チューニングが不十分
- (2)が十分でも、(1)のインターネット接続回線の帯域が不十分かもしれません
  - 2021年度までのwifiはノートPCを持ち歩くユーザ数が全体の10-20%程度、使い方もWWWの調べ物など軽い使い方を想定していました
  - 2022年度以降は、多くのユーザが同時に動画を利用することも想定しています (が、十分かどうかは要検証)



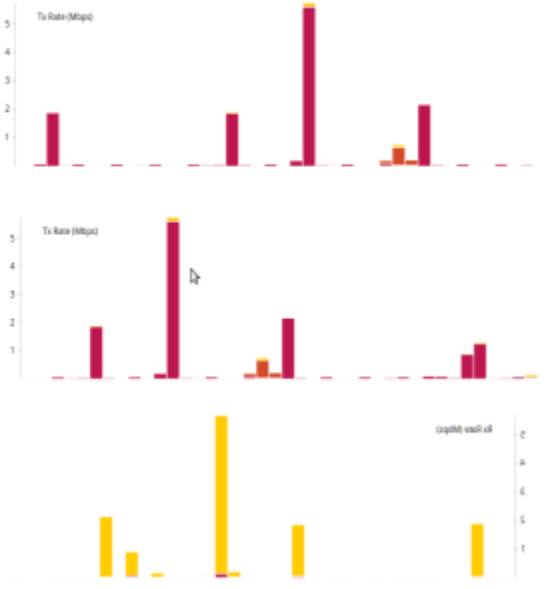
kagidaiとkagidai5のちがいは何ですか?

- 周波数帯の違いです
- 解説
  - 無線には2.4GHz帯と5GHz帯があります
  - 無線LANの設定でSSIDは一つのほうがいいか?否か?という話(派閥?)があります
    1. APが賢く、よろしく適切な周波数帯を使わせることが可能なので1つが良い
    2. そんなにうまくいかないため2.4GHzと5GHzで別のSSIDを作りユーザに選ばせる
  - 最初は前者の運用だったのですが、のちに後者の運用になったので、 kagidai (2.4GHz帯)と kagidai5 (5GHz)帯という二つの SSID があります

FAQ: インターネット回線、帯域の話題

ZOOMはどれくらいの帯域をつかいますか?

- 最近の動画ものは最大5-6Mbps(いわばピーク時)くらい使っているようです
- もし**ピークが重なると仮定**すると80人の授業で**最大480Mbpsの帯域が必要**になりますが、 そんなにピークって**重なるものですかね?** (参照: 設計ガイドの統計多重効果)



FAQ: アクセス制限

学内から学外への通信をフィルタしていますか?

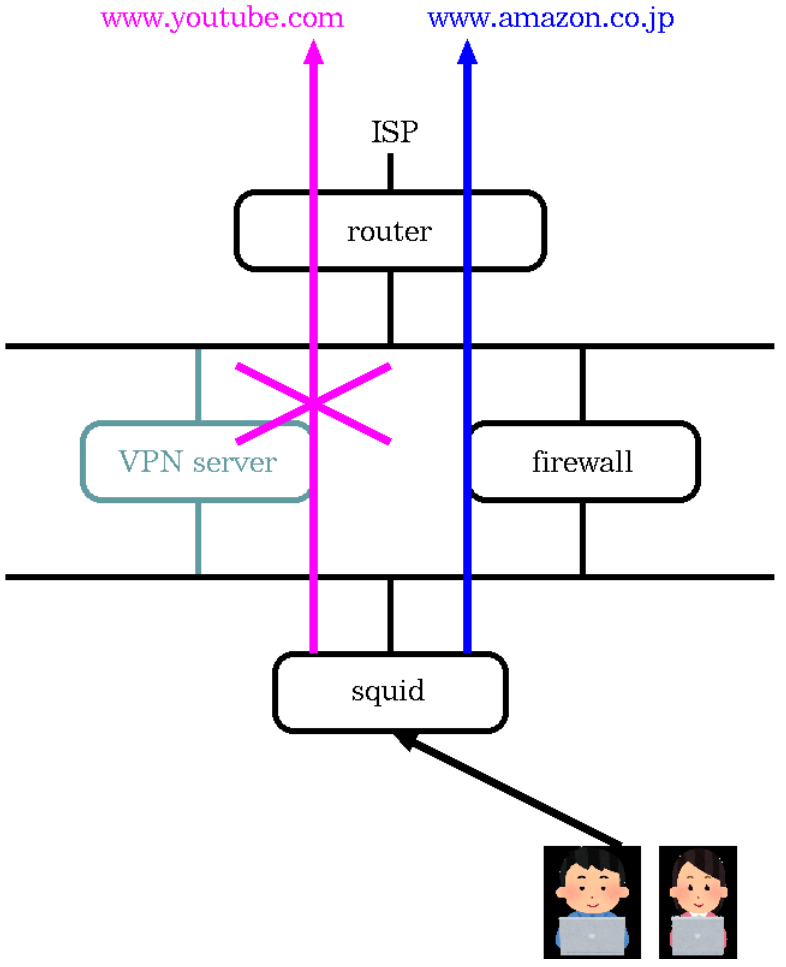
- もちろんフィルタしています
- 業務(教育、研究、事務仕事)で必要なプロトコルは通しています
  - ファイアウォールでは代表的なプロトコルを通しています
    - HTTP, HTTPS, SSH, FTP, DNSなど
    - 業務で必要なプロトコルは随時、許可しています
      - 最近ならZOOMが典型例ですね
  - 上記以外のプロトコルは通しません

学内から特定のサイトを見せないように出来ますか?(<L4)

- **FWのルールは通信先のIPとポート番号の組み合わせが基本、その範囲なら割とOK**
- 特別なアプリケーションプロトコルだけを拒否 -> OK
  - ポート番号で特定できるなら、フィルタルール一つで拒否できます
- 見せたくないサイトのサーバのIPアドレス一覧が分かる -> 条件付きでOK
  - サーバのIPアドレスが数個くらいなら現実的 -> OK
  - 相手のサーバがクラウドの場合 -> △　(条件しだい)
  - クラウドでもサーバのIPアドレス帯(数個)が分かるなら現実的 -> OK
  - サーバが世界中に分散配置されていてIPが(1000個とか)ある -> 無理
    1000個のフィルタルールを書く必要があります。 また、1000個のルールを全パケットについて検査するのでFWが遅くなります。 さらに、このサーバ群は自動的に増減するだろうから、 いま把握できていない別IPが使われる可能性もあります
- 上記以外の組み合わせ(たとえばsource IPなどとも組み合わせたルール)や、 L4より上の情報をつかったフィルタリングも出来ますが、 それらを行うとFWの負荷がものすごく高くなったり、 そもそもFWの標準機能ではなくオプションだったり別製品だったりします (つまり購入すれば出来ます -> 導入は**費用対効果しだい**)

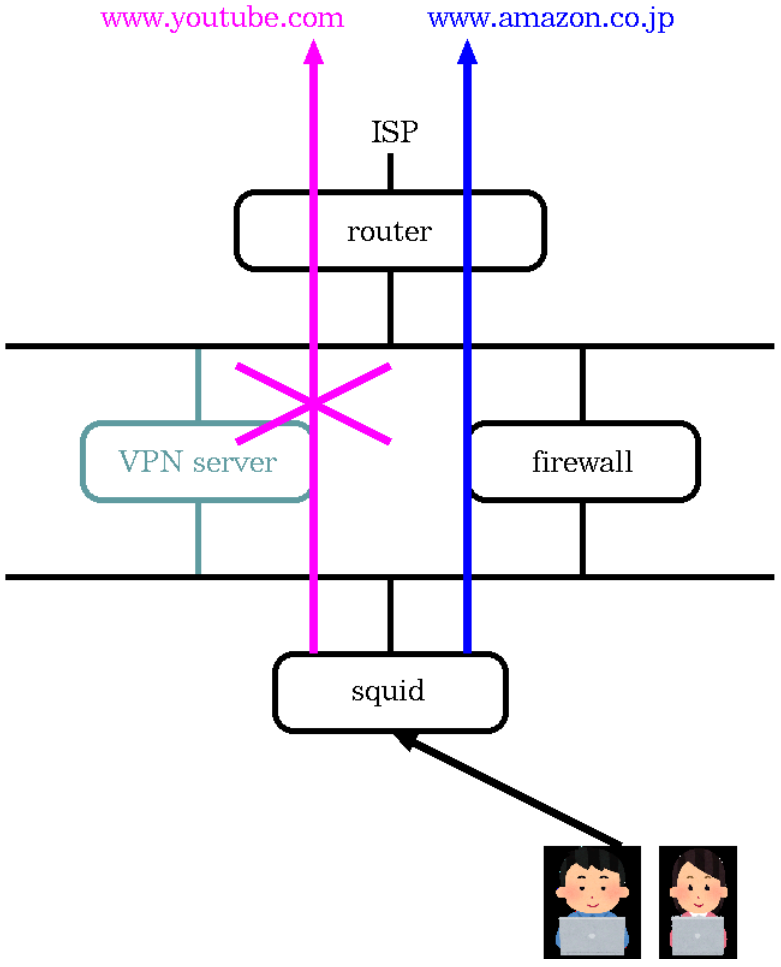
学内から特定のサイトを見せないように出来ますか?(L7)

- **特定のサービスを使わせたくない/URLを見せたくない**といったことですよね?
- 普通1つのIPで複数のWWWサーバが動いているのでIPではフィルタ出来ず、 **アプリケーションプロトコルの詳細を見ないとフィルタできません** (FW基本機能+FWオプションか別途専用製品が必要)
- **HTTP/HTTPS**については**squid**(proxyソフトウエア)を使えば、 安価に運用で逃げられます (かつて本学でも、この運用をしていました時期があります)
  - **ブラウザで「PROXYの利用」設定が必須**です。 ノートPCを持ち歩いてPROXYの利用設定が自動で切り替わらないユーザには使いづらい



学内の特定の人にだけyoutubeを許可できますか?

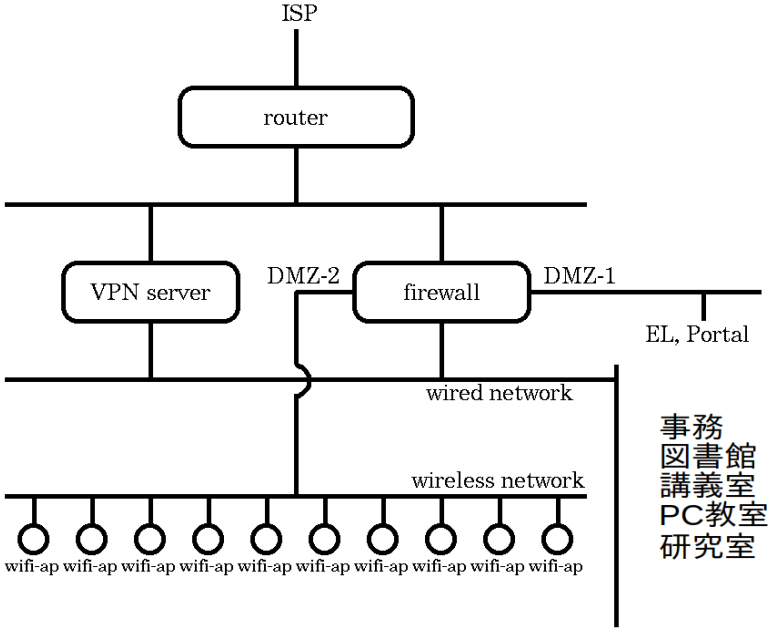
- **個人を特定する必要があり**困難
- 一般に(FWの基本機能では)無理です。
  そもそもアプリケーションプロトコルが**個人の特定(認証)を想定していません**し、 今どき認証必須のプロトコルは暗号化しているので、 通信経路途中のFWでは中身が見えず介入できません
- 部分的に運用で逃げる方法はある -> 例:
  - 学内->学外のHTTP/HTTPSは**squid経由を強制する運用を前提**(前頁)
  - squidの設定で、講義室の教卓PCはyoutubeを許可、それ以外は拒否
  - ユーザにほんの少し負担をかけますが費用がかからない (**機材の購入や自動化=金で解決がすべてでない)**好例



FAQ: 学内のサービスについて

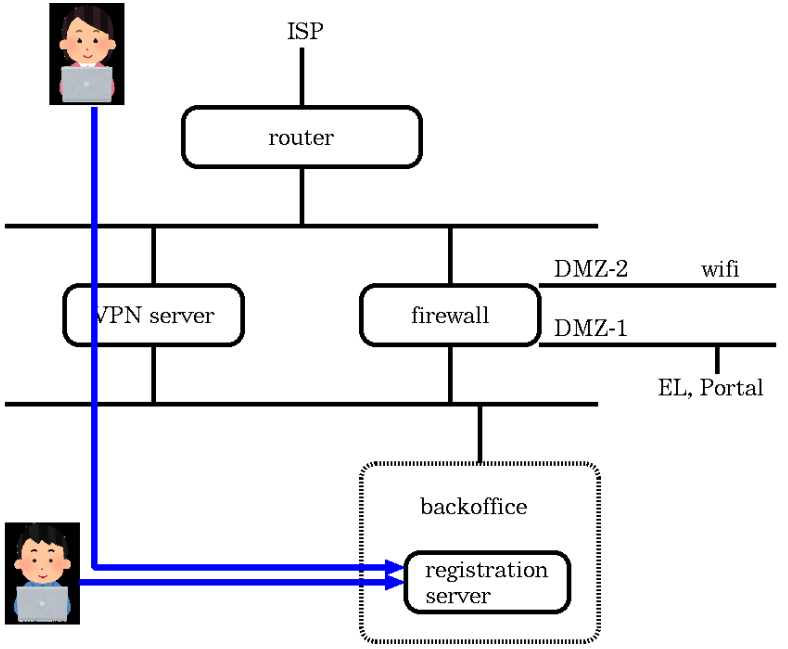
事務の部屋は散らばっていますが同じネットワーク?

- 同じネットワーク(論理セグメント)です。 **VLAN**を使い実現しています
- 例えば事務局です。 物理的に異なる場所に事務の人たちがいますが、 **論理的には同じネットワーク**を使っています
- みんな**同じ事務ソフトウエアを使うので同じネットワークにしないと不便**です
  - もちろん事務局のVLANがあり、そこに事務局のPCはつながっています



履修登録システムはどうなっていますか?

- 公立化にともない事務の履修登録システムをそのまま使うことになりました
- 事務ネットワークは学内からもアクセスさせてないのですが、しかたないので、2019年度は**期間限定かつ学内からのみ履修登録システムを使える**ことにしました (この期間だけフィルタ設定を変更)
- 2020-2021年度は、この手が使えず大変なことになっていました
- VPNを使えば学内あつかいなので家から履修登録が出来るはずです (なぜこの運用をしていないのかは不明です -> 疑問なら、お客様にヒアリングしてください)



ポータルやELがスマホでうまく見られません

- この質問をしているあなたは、この授業のテーマが分かってないぞ!
- **TCP/IPよりはるか上の層**のアプリ話はネットワークと無関係。 **ネットワークプロトコルは確実なデータ転送を行うもの、運ぶ中身(ペイロード,データ)の不具合に責任なし**
- アプリケーションの作りがスマホ対応していないということですね (よく知らないけど、たぶん)次のような何かが悪いのだと思います
  - HTML5でないとか、HTML5だけどスマホサイズを想定して作られていないとか...
  - 実は、コンテンツがPCの画面で16:9の1280x960を前提にしているとか...
  - 使っているJavaScriptがいけてない...ってことはないか;-(
    - いまどきPCでもスマホでもブラウザのエンジンは同じでは...
    - でも、その画面を構成するJSがスマホサイズを想定してないとか〜