ネットワーク
システム管理 #10

たかさきこうや

1限 (09:00-10:45)

1

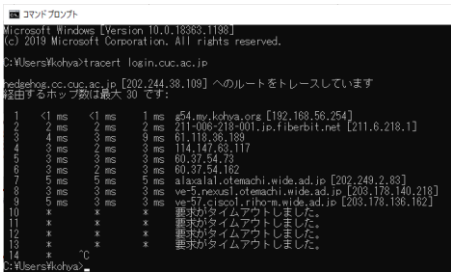
先週のおさらい

- IPアドレスを自動的に設定する
  DHCPというものがある
- ネットワークインターフェースには
  物理アドレス(MACアドレス)というものが付与されている
- OSI参照モデル、TCPヘッダ、IPヘッダ、
  イーサネットフレームヘッダ
- ping、tracert(traceroute)

2

tracertを家から学校に打つ

- うちの
  場合は
  こんな
  感じ



3

Tracerouteの特性

- 一般的に、各ルータまでの経路を3回計測する
- 3回の経路が毎度違うことがあるため、
  複数のルータが出てくることがある
- ホスト名が出てくる場合「該当のルータに逆引きの設定がされて」おり、IPアドレスからホスト名が名前解決できる
  (設定されていない場合も多々ある)
- 3つ並んで出てくる数字は「該当のルータまでの通信速度」であり、たいていの場合はms(ミリ秒)で表される
- ※ミリ秒=1/1000秒

4

わかること

- (僕の場合)9番目で、ve-57.cisco1.riho-m.wide.ad.jp
  というルータにたどり着き、そこから先は
  結果が出てこない
- →tracerouteに使う、ICMPというプロトコルが
  10番目のルータでブロックされていて通れない(よくある)
- どのルータも最大で5ms程度の速さなのでかなり早い
  (日中と夜でかなり違うので参考程度に…)
- ※宅内だと1msを切る
- ※ラウンドトリップタイム、とも言う

5

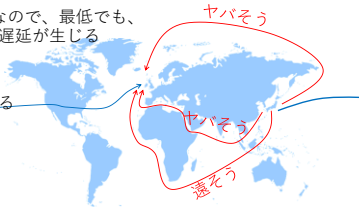
例えば

- 某bbc(英国放送協会)にtracertを打ってみる

6

目的のサーバが

- 海を渡ると、やはり物理的な距離は如何ともしがたいため時間がかかる(光ファイバ中の光の速度はおよそ20万km/秒)
- 日米間は1万キロ程度なので、最低でも、片道1/20=50ミリ秒は遅延が生じる
- 往復で100ミリ秒は
- ヨーロッパへはアメリカを経由している
- ※情勢がアレなので西へは行きにくいし



7

通信の要素

- 回線が「大容量のデータを送れる」ことはとても重要
- 1秒間あたり5Mbps送れれば、昨今の動画は(Full HDとか4K画質とかじゃなければ)問題ない

- ただし、もし「オンライン講義」とか「ビデオ会議」をするなら、遅延は**敵**
- ラウンドトリップタイムが大きい＝遅延が大きい　と見て良い

8

NA(P)Tルータの話

- 通信を行うに際し、NA(P)Tルータやファイアウォール付きのルータは
1. イーサネットフレームヘッダを剥ぎ取り
2. IPヘッダを剥ぎ取り
3. TCPヘッダを見て、場合によっては剥ぎ取る
- までする
- これは単純に、CPUが高速でなければ時間がかかる
- つまり、遅延につながる

9

キャリアグレードNATも然り

- 速度の低下が起こる
- つまり、IPv4アドレスを延命させる技術はどう頑張っても「遅延と無関係ではいられない」

- IPv6の場合、「アドレス部分が32bit→128bitに増えた」が、その分ヘッダが簡略化され、かつ経路制御も単純になっているので、純粋に遅延を抑えられる(ということになっている)

10

話を戻す

```
 1  <1 ms  <1 ms <1 ms  g54.my.kohya.org [192.168.56.254]
 2   3 ms   2 ms  1 ms  211-006-218-001.jp.fiberbit.net [211.6.218.1]
 3   2 ms   2 ms  2 ms  61.118.36.189
 4   2 ms   2 ms  2 ms  114.147.63.117
 5   2 ms   2 ms  2 ms  60.37.54.73
 6   3 ms   2 ms  2 ms  60.37.54.162
 7   4 ms   4 ms  4 ms  alaxala1.otemachi.wide.ad.jp [202.249.2.83]
 8   3 ms   2 ms  2 ms  ve-5.nexus1.otemachi.wide.ad.jp [203.178.140.218]
 9   4 ms   3 ms  3 ms  ve-57.cisco1.riho-m.wide.ad.jp [203.178.136.162]
10   *      *     *     要求がタイムアウトしました。(以下略)
```

11

これがICMPを使った場合の

- Tracertの結果だが、実はICMPを使わないtracerouteというのも存在する
- Windowsの場合はNmapというソフトが必要
- 興味がある人は入れてみると良い
- https://nmap.org/

12

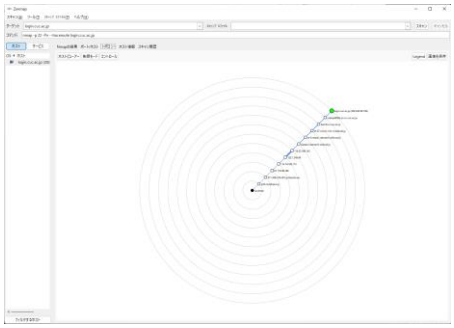
自宅のネットワークが

- Tracert(で使用するICMPやUDP)をブロックしている場合
  - 割と良くある
- Nmapで、コマンドのところに
  - nmap -p 22 -Pn --traceroute login.cuc.ac.jp
- と打ってみると、わりと正しい結果が返ってくる
  - TCPで22番ポートを用いてのtracerouteをしている

13

Nmap

- は、
  こんな
  かんじ



14

実行結果

```
 1   5.00 ms  g54.my.kohya.org (192.168.56.254)
 2   7.00 ms  211-006-218-001.jp.fiberbit.net (211.6.218.1)
 3  12.00 ms  61.118.36.189
 4   7.00 ms  114.147.63.117
 5   7.00 ms  122.1.245.53
 6   7.00 ms  122.1.245.66
 7  13.00 ms  alaxala1.otemachi.wide.ad.jp (202.249.2.83)
 8   8.00 ms  ve-5.nexus1.otemachi.wide.ad.jp (203.178.140.218)
 9   8.00 ms  ve-57.cisco1.riho-m.wide.ad.jp (203.178.136.162)
10   8.00 ms  fwsm0.cc.cuc.ac.jp (202.244.32.242)
11  10.00 ms  catalyst6509-pri.cc.cuc.ac.jp (202.244.32.228)
12   9.00 ms  hedgehog.cc.cuc.ac.jp (202.244.38.109)
```

15

ホップ数

- (僕の)自宅PCからlogin.cuc.ac.jpまでのホップ数は「12」と言う
- また、 ve-57.cisco1.riho-m.wide.ad.jp までの
  ホップ数は「9」である

16

(僕の場合)9行目の

- ve-57.cisco1.riho-m.wide.ad.jpまでは
  同じ結果になっており、そこから先は

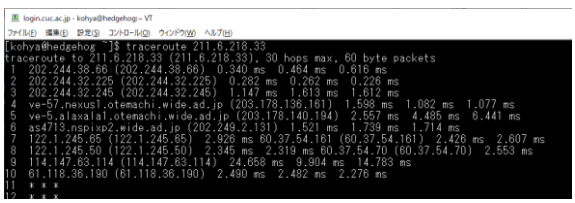
1. ve-57.cisco1.riho-m.wide.ad.jp (203.178.136.162)
2. fwsm0.cc.cuc.ac.jp (202.244.32.242)
3. catalyst6509-pri.cc.cuc.ac.jp (202.244.32.228)
4. hedgehog.cc.cuc.ac.jp (202.244.38.109)

- となっている
- 学内の経路はこれ以外ないので、
  これをそのまま使ってくれてかまいません

17

では今度は逆に

- traceroute 211.6.218.33
  (僕のアクセス元IPアドレス…とされるもの)をする



18

やはり途中で止まるが

- Ctrl-Cで実行を停止する
- そして二つの結果を見比べる
- ラウンドトリップタイムについては一旦忘れる

19

両者を見比べる

	学校→家				家→学校	
1	202.244.38.66	202.244.38.66		202.244.38.109	hedgehog.cc.cuc.ac.jp	12
2	202.244.32.225	202.244.32.225		202.244.32.228	catalyst6509-pri.cc.cuc.ac.jp	11
3	202.244.32.245	202.244.32.245		202.244.32.242	fwsm0.cc.cuc.ac.jp	10
4	ve-57.nexus1.otemachi.wide.ad.jp	203.178.136.161		203.178.136.162	ve-57.cisco1.riho-m.wide.ad.jp	9
5	ve-5.alaxala1.otemachi.wide.ad.jp	203.178.140.194		203.178.140.218	ve-5.nexus1.otemachi.wide.ad.jp	8
6	as4713.nspixp2.wide.ad.jp	202.249.2.131		202.249.2.83	alaxala1.otemachi.wide.ad.jp	7
7	122.1.245.65	122.1.245.65		122.1.245.66	122.1.245.66	6
8	122.1.245.50	122.1.245.50		122.1.245.53	122.1.245.53	5
9	114.147.63.114	114.147.63.114		114.147.63.117	114.147.63.117	4
10	61.118.36.190	61.118.36.190		61.118.36.189	61.118.36.189	3
11	?			211.6.218.1	211-006-218-001.jp.fiberbit.net	2
				192.168.56.254	g54.my.kohya.org	1

Tracerouteの方向 / Tracerouteの方向

20

そうするとそれぞれに

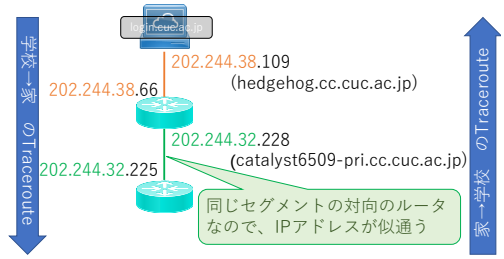
- 似ているIPアドレスが出てくることがわかる

	学校→家				家→学校	
1	202.244.38.66	202.244.38.66	⇔	202.244.38.109	hedgehog.cc.cuc.ac.jp	12
2	202.244.32.225	202.244.32.225	⇔	202.244.32.228	catalyst6509-pri.cc.cuc.ac.jp	11
3	202.244.32.245	202.244.32.245	⇔	202.244.32.242	fwsm0.cc.cuc.ac.jp	10
4	ve-57.nexus1.otemachi.wide.ad.jp	203.178.136.161	⇔	203.178.136.162	ve-57.cisco1.riho-m.wide.ad.jp	9
5	ve-5.alaxala1.otemachi.wide.ad.jp	203.178.140.194	⇔	203.178.140.218	ve-5.nexus1.otemachi.wide.ad.jp	8
6	as4713.nspixp2.wide.ad.jp	202.249.2.131	⇔	202.249.2.83	alaxala1.otemachi.wide.ad.jp	7
7	122.1.245.65	122.1.245.65	⇔	122.1.245.66	122.1.245.66	6
8	122.1.245.50	122.1.245.50	⇔	122.1.245.53	122.1.245.53	5
9	114.147.63.114	114.147.63.114	⇔	114.147.63.117	114.147.63.117	4
10	61.118.36.190	61.118.36.190	⇔	61.118.36.189	61.118.36.189	3
11	?			211.6.218.1	211-006-218-001.jp.fiberbit.net	2
				192.168.56.254	g54.my.kohya.org	1

21

推察するに

- 右の通り



22

最後の部分

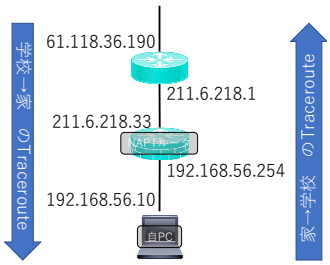
- そもそも、僕は「211.6.218.33」からログインしているようだ
- 211.6.218.1は、そのIPアドレスによく似ている
- とすると、111.6.218.1の対向のルータは、211.6.218.33ではなかろうか
- とすると、最後の1つになるのが、NAPTルータの内側にある自分自身のPCではなかろうか…？という予測が立つ

10	61.118.36.190	61.118.36.190 ⇔ 61.118.36.189	61.118.36.189	3
11	?	211.6.218.33 ⇔ 211.6.218.1	211-006-218-001.jp.fiberbit.net	2
12	My-PC	192.168.56.10 ⇔ 192.168.56.254	g54.my.kohya.org	1

23

そうすると

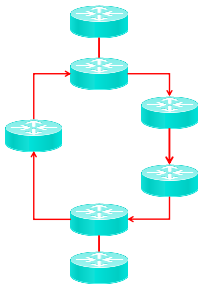
- 最後の部分を記述すると(僕の場合)こうなる



24

また、どう見ても

- 同一セグメントの
  対向ルータに見えない場合、
  それは
  「行きと帰りで
  別経路を通っている」
  という可能性が高い



25

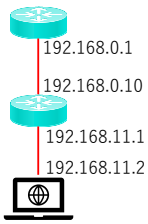
実はこれ

- 電車の経路選択に良く似てる
- 行きと帰りで、違う経路を使ったりしない？
  - 学校に行くときはJRが早いけど、帰るときは京成が早い
    - 乗り換えの都合とか、本数の問題とかで…
- インターネットも同じ
  - なるべく最良の経路を通ろうとする

26

集合住宅などで

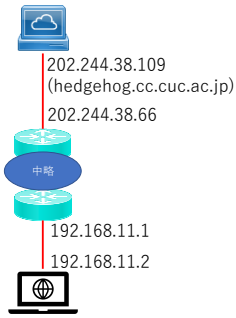
- 自宅PCからtracertをかけて、
  2回以上続けてプライベートIPアドレス
  っぽいものが出てきている場合、
  (理由はさておき)
  君のネットワークでは2回
  「NA(P)T」をしていることになる
- 当然、前述の理由により
  遅延は大きくなる
- ※リアルタイムのオンライン講義には
  あまり向かない



27

と、ここまで説明

- したところで、第2回課題です
- 自宅と学校の間のネットワークを
  tracerouteを用いた結果をもとに
  図示してください
- 右の図では中略してある部分も
  ちゃんと書きましょう



28

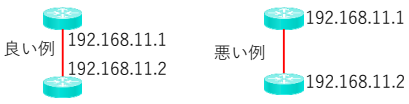
フォーマット(必須条件)

- PowerPointで1枚
- **A4 縦書き**
- 設定は以下参照

29

必須条件

- ファイル名は、
  ログイン名-NSA02.pptx とすること
- 行きと帰りの経路を書くこと
- **login.cuc.ac.jp を一番上**に、**自宅PCを一番下**に書くこと
- IPアドレスは、「インターフェースについている」ことが
  明確になるように書くこと(機械本体につくものではない)



30

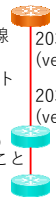
必須条件

- ルータのアイコンはCisco社のものをつかうこと
- 各々のルータの両端のIPアドレスを分かる範囲で書き込むこと
- login.cuc.ac.jpを始点に、自宅PCを終点にし、それぞれ妥当なアイコンを使うこと（右の例はサンプル）
- 各ルータの**対向のIPアドレスが同一セグメント**であることが意識して記載されていること

31

必須条件

- **ve-57.cisco1.riho-m.wide.ad.jp** から先の経路は僕が例示したものを使うこと
- 自宅の中と、大学の中が明確にわかるよう、境界線（責任分界点）を書くこと
- 自宅内に、PCとデフォルトゲートウェイ以外のホストを書くこと
- 大学内に、login.cuc.ac.jp以外のホストを複数書くこと



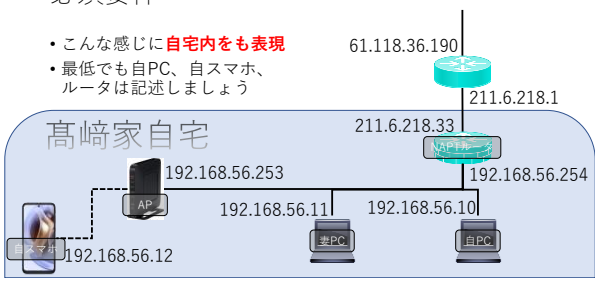
203.178.136.162
(ve-57.cisco1.riho-m.wide.ad.jp)

203.178.136.161
(ve-57.nexus1.otemachi.wide.ad.jp)

32

必須要件

- こんな感じに**自宅内をも表現**
- 最低でも自PC、自スマホ、ルータは記述しましょう



33

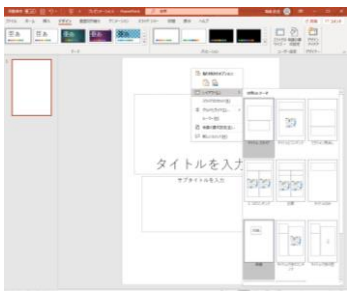
必須要件

- 学校側は、login.cuc.ac.jpとwww.cuc.ac.jpは書けるはずなので記述

34

余談

- レイアウトはちゃんと無地のものに変えておこうね…



35

余談

- 出てきているIPアドレスがグローバルIPアドレスなのかプライベートIPアドレスなのかは、把握しておくこと
- どうしてもセキュリティ上の都合で、使用しているIPアドレスが書けない、という場合は、その旨を記述し機微情報をマスクして記入すること

36

経路の話をもう少し

- 実はtraceroute(tracert)の結果は、
  割と短時間でコロコロ変わる
- 動的ルーティング、と言って、
  目的地までの距離が短い経路を
  自動的に選択する仕組みになっている
- 一般ユーザが設定することはまずない
  - というか途中経路は末端ユーザには選べない

37

デフォルトゲートウェイ

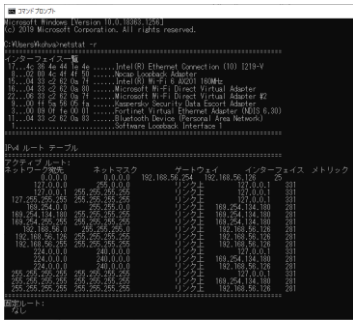
- 外と通信をしたい場合、デフォルトゲートウェイを
  通って通信が出ていく、という話はした
- あくまでも、IPヘッダに含まれるのは「送信元」と「宛先」の
  IPアドレスで、どこを経由するかはIPヘッダには含まれていない
- PC自身が、
  「自分と同一セグメントにいる端末か」
  「そうではないか」
  を判断している

38

どこで？

- コマンドプロンプトで、
  netstat –r を実行

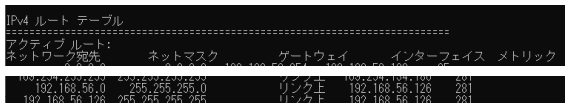
ここに注目



39

ルーティングテーブル

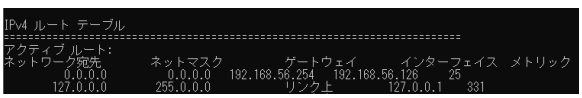
- IPv4ルートテーブル、と書かれたこれは
  「どのネットワークへの通信は、何処に投げればいいか」が
  書かれている
- ネットワーク宛先が192.168.56.0/255.255.255.0 の場合、
  リンク上…つまり、自分と同一セグメントなので、
  192.168.56.126(自分のIPアドレス)から、自分と
  同一セグメントのつもりで通信を出せばよい



40

リンク上ではない

- ネットワークについては、ゲートウェイから
  外に出ていかなくてはいけない
- 0.0.0.0/0.0.0.0については、
  192.168.56.254(デフォルトゲートウェイ)から外に出せ、と
  書いてある



41

0.0.0.0/0.0.0.0とはなにか？

- これは、ネットワークアドレスが0.0.0.0であり
  ネットマスクが0.0.0.0…つまり2進数で記述すると
  0000 0000 0000 0000 0000 0000 0000 0000
  なので、0.0.0.0から255.255.255.255までの
  「すべてのIPアドレス」という意味である
- つまり、
  「すべてのIPアドレス宛ての通信は、
  192.168.56.254から外に出せ」と書いてある

42

ここで疑問が生じる

- 「いやいや待ってよ。
  0.0.0.0/0.0.0.0 には、192.168.56.0/24も含まれない？」
- →含まれます

- つまり、このPCには、
  「192.168.56.0/24あての通信は自分と同一セグメントへ」
  「192.168.56.0/24あての通信は192.168.56.254へ」
  という、矛盾する記述が書いてある、と言える

43

ロンゲストマッチ

- 実は、経路制御は
  「常にプレフィックスが長いものが優先される」
  というルールがあります
  - これを「ロンゲストマッチ(最長一致)」と呼ぶ
  - プレフィックス=ネットマスクの「1の数」
  - 192.168.0.0/24 とか192.168.0.0/255.55.255.0は
    ネットマスクの1の個数が「24個」
  - これが多い(ロンゲスト)経路が優先される

44

ロンゲストマッチにより

- 192.168.56.10 は、

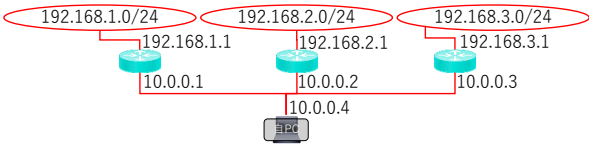
  192.168.56.0/255.255.255.0 と
  192.168.0.0/255.255.0.0 と
  0.0.0.0/0.0.0.0 の

  3つともに含まれるが、プレフィックス長が一番長い
  192.168.56.0/255.255.255.0 の記述が優先される

45

静的経路は複数指定できる

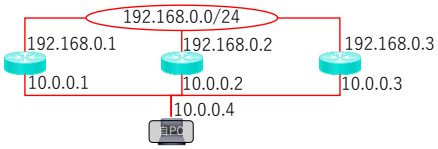
- 192.168.1.0/24 は 10.0.0.1へ
  192.168.2.0/24 は 10.0.0.2へ
  192.168.3.0/24 は 10.0.0.3へ
  というルールがPCの中に書いてあった場合、それぞれのルータ
  を通ってその向こうのネットワークにアクセスする



46

ロンゲストマッチの場合

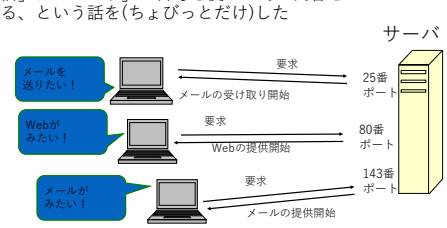
- 192.168.0.0/24(192.168.0.0～192.168.0.255)　は10.0.0.1へ
  192.168.0.0/16(192.168.0.0～192.168.255.255)は10.0.0.2へ
  0.0.0.0/0　　(0.0.0.0　　～255.255.255.255)は10.0.0.3へ
  というルールがPCの中に書いてあった場合、192.168.0.0は
  どのネットワークにも含まれるが、PCは10.0.0.1を優先する



47

ポートの話

- 先週、「通信」は「ポート」の番号を使ってその内容を
  区別している、という話を(ちょびっとだけ)した



48

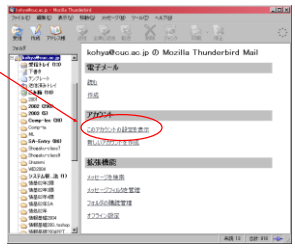
おさらい

- ポートって？
- サーバとクライアントは、IPによって通信をする
- でもIPだけでは信頼性がないので、IPの上にTCPという規格を乗せた
- TCP/IPでは、通信に「窓口番号」を付与して、同じサーバで複数のサービスが待ち受け出来るようにした
  - 語源は「船着き場」

49

この、ポートの数字は

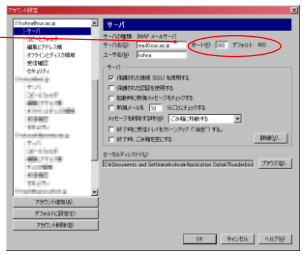
- 割と簡単に把握することが出来る
- 例えば、Thunderbirdならばここ



50

アカウント設定⇒サーバ

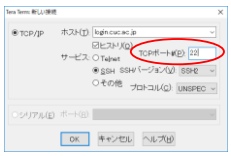
- ここに、ポート番号の設定がある
- 大抵のTCP/IP通信であればどのポートを使うかの設定は(サーバの環境に応じて)自分で設定できるようになってるはず



51

僕らが普段つかっている

- Tera Termだってそう
- Tera Termでは、
  - 「login.cuc.ac.jpというホストに繋ぐ」際に
  - 「SSH」というサービスの
  - 「バージョン SSH2」を用いて
  - 「**TCPポート22番**」を利用して
- 接続する設定が可能…なわけだ



52

mail0.cuc.ac.jpの場合…

- 993番に来たアクセスは「IMAP over SSL/TLS(暗号通信あり)」として、窓口業務のごとく捌いている
  - IMAPは、メールを読むための標準的なプロトコル
- この辺の設定を忠実に写せばスマホでも(Outlookなどの)メールアプリでメールが読める
  - 今時はWebメールで読んでも良いが、実装上直接メールサーバとIMAPでやり取りした方が早い

53

IMAPの話の前に

- 実は、Webに関するサービスは、80番ポートで行われている
  - これは世の中一般的にそうなっている
    - Webサービスは「誰でも利用したい人みんなに見せてあげたい」のでサーバ側で勝手に80番以外のポートを使ってしまうと、そのポートを探し当てられない
    - 探し当ててほしくないサービスの場合、80番以外でこっそりサービスをすることは可能
- そして、そのサービスでは一般的に「HTTP」と言うプロトコルを使って情報のやり取りを行う
  - HTTP=Hyper Text Transfer Protocol

54

Protocolって？

- 「約束事」みたいな意味
  - 正しくは「議定書」「儀礼」の意
- HyperText Transfer Protocol
  - =ハイパーテキストを送信するための約束事
- どういう約束事か、覗いてみよう！

55

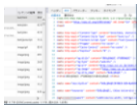
今どきのブラウザには

- 開発者モードというのがあるので、これを(F12キーとかで)開いてネットワークを覗いてみよう

56

まずわかること

- １画面のWebページを見るのに、ずいぶんと多くのファイル？を取り寄せているなあ…
- ヘッダーってのがあるなあ…
- 本文ってのがあるなあ…



57

言わんとしている事

- 通信には、決まりごとがある
- HTTPには、HTTPに相応しい決まりごとが存在している
  - そして、その決まりを守っている限り、誰がどんなソフトを作ろうが、誰がどんなソフトを使おうが問題はない

58

つまり

- 僕たちは、HTMLという言語を使ってホームページを作っている
  - OSI7階層モデル**より「上」**のレベルでの約束事
- それを、CUCのWebサーバはHTTPという通信の約束事を守って人に見せている
  - OSI7階層モデルでいうところの5-7層の約束事
- そんなWebサーバと僕らのクライアントは、IP通信をしてる
  - OSI7階層モデルでいうところの3層の約束事
- ⇒僕たちは、HTTPの通信の約束事を守り、HTMLの決まりを守るブラウザを使っているからそれを意図したとおりに閲覧できる

59

だから

- Webサーバに「データを頂戴」と要求する
  クライアントは、別にWebブラウザでなくてもかまわない
- 試してみよう！

60

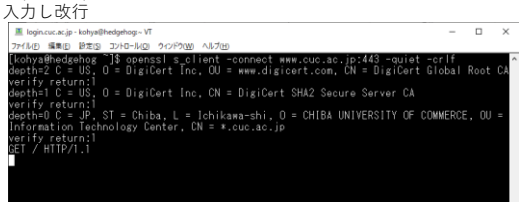
login.cuc.ac.jpにログイン

- ここで
  % openssl s_client -connect www.cuc.ac.jp:443 –quiet -crlf
  と入力

61

verify return: 1

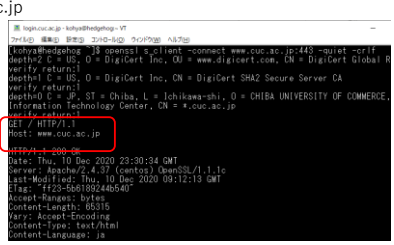
- と表示されたら接続準備完了
- GET / HTTP/1.1
  と入力し改行



62

更に

- Host: www.cuc.ac.jp
- と入力し、改行を
  2回押す



63

すると

- 一杯データが表示される
  - 入力値のおさらい
    - openssl s_client -connect www.cuc.ac.jp:443 –quiet -crlf(改行)
    - GET / HTTP/1.1(改行)
    - Host: www.cuc.ac.jp(改行)
    - (改行)
- 良く見ると、CUCのWebサイトの
  トップページと同一のデータ

64

これはなに？

- 今、openssslというコマンドを使い、ブラウザの
  フリをさせた
  - 接続先をwww.cuc.ac.jp からwww3.cuc.ac.jp に変えて、
    GET / HTTP/1.1 の代わりに、
    GET /~kohya/ HTTP/1.1 と
    打ってみよう

65

これはなにに使える？

- Webサーバの動作確認に使える
- 通信の中身をちゃんと読むこと
  が出来る

66

でもふと考える

- これじゃあ、どうやって画像を見るの？
- そこにHTTP通信の秘密がある
- 実は、ブラウザは、この通信を何度も繰り返し行っている

67

手順

- www.cuc.ac.jpの、index.htmlを手元に取り寄せる
- index.htmlのソースを解析する
- <img src=“”>などのタグを探し、読み込むべき画像を見つける
- それぞれの画像を、個別に取り寄せる
- 最終的に１枚のHTMLとして組み立てる

68

通信経路は安全ではない

- 今どき、Webコンテンツを見るのに、暗号のかかっていない通信をすると中間者攻撃をされる
  - 中間者攻撃＝経路上に悪いやつがいて、通信を盗聴したり、書き換えたりする攻撃
- 先週も話をした通り、通信は基本的に「何処を通るか分からない」
- だから、通信は「始点と終点」の間を全部暗号化し、覗かれないようにしないと安心して使えない

69

暗号化

- 相手が、なりすましではなく本物であることを担保する(真正性)
- 通信が、改竄されていないことを担保する(完全性)
- 通信が、第三者に覗き見られないことを担保する(秘匿性)

この3つは、暗号通信を行う際に必須である、とされる

- ここに、「可用性」「責任追及性」「信頼性」「否認防止性」を合わせて情報セキュリティの7大要素とか言う

70

公開鍵暗号とTLS

- TLS(Transport Layer Security)は、公開鍵暗号方式の技術
  - 公開鍵暗号=暗号時と復号時に、別の鍵を使う
    - ex:共通鍵暗号=暗号時と復号時に、同じ鍵を使う
- そのキモは、鍵を2種類作るところにある
  - 秘密鍵＝自分しか知らない鍵
  - 公開鍵＝他人に渡す鍵
  - 秘密鍵と公開鍵は、必ず一対である
  - 公開鍵から秘密鍵は作れない

71

秘密鍵と公開鍵

- AさんがBさんに、秘密の文章を渡したい
  - Bさんの公開鍵を使い、Aさんが文章を暗号化すれば、それはBさんにしか復号できない
- Bさんが該当の文章が確かにAさんからであることを確認したい
  - Aさんの秘密鍵を使い、Aさんが文章を暗号化すれば、それはAさんの公開鍵でしか復号できない
- AさんとBさんがリアル知り合いであれば、お互いにリアルで会った時にでも鍵を交換しておけばよい

72

認証局と認証基盤

- AさんとBさんがもし旧来の知り合いでなく突然通信をしたい場合（オンラインショッピングとかがそうだよね？）
- 認証局Cさんがここに登場する
  - Cさんは世界的に有名であり、Cさんの公開鍵はみんな持っている
  - Aさんは自分の公開鍵を、自分自身の公開鍵だと担保してほしい
  - そこでCさんにお金を払い、Cさんの秘密鍵で暗号化してもらう
    - Cさんはお金をもらう見返りに、Aさんに直接アプローチし、「お前本当にAさんなんだろうな？」と身分確認をしてくれる
      - 認証局はCさん以外にもいっぱいいて、まじめに身分を確認してくれる人も、そうでない人もいる

73

TLSを用いて通信経路を暗号化すると…

- 今まで平文で行っていた通信を、そのまま暗号化できる

	プロトコル	ポート番号	TLSを使った場合	ポート番号
Web	HTTP	80	HTTPS	443
メール送信	SMTP	25	SMTPS	465
メール受信	POP3	110	POP3S	995
メール受信	IMAP4	143	IMAP4S	993

- openssslコマンドは、このTLSの鍵を作ることが出来るコマンドだが、通信そのものも可能

74

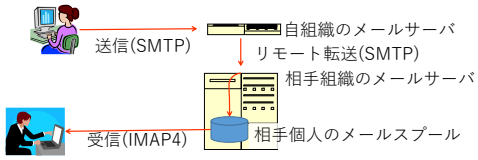
HTTP通信は分かった

- 比較的平易なSMTP通信も可能
  - SMTP(Simple Mail Transfer Protocol)
  - シンプルメール送信プロトコルの意味

75

メールの仕組み

- 「送信」と「受信」では使用するプロトコルが違う
  - 郵便物だって、出すときはポストまで持っていくけど、受け取るときは届けてくれるでしょ？



76

SMTP

- メールを出すとき
- メールサーバが他の組織宛のメールを他のメールサーバに送るとき
  - リモート転送、という
- は、SMTPを使って送信する

77

IMAP4

- サーバの「メールスプール」(私書箱のようなもの)に溜まったメールを、自分のPCで閲覧する際に、IMAP4というプロトコルを用いてメールの受信をする

- POP3という、もっと簡単なプロトコルもある
  - CUCは標準がIMAP4

78

メール送信の方法

- telnet mail.cuc.ac.jp 25
  - サーバの25番ポートへの接続
- HELO localhost
  - 最初の挨拶
- MAIL FROM: kohya@cuc.ac.jp
  - 送信者の宣言
- RCPT TO: 自分のメールアドレス
  - 誰に送るか、の宣言

79

続き

- DATA
  - 本文の宣言
- 適当に本文を書く
- 「.」のみの行を書く
- QUIT
  - 通信終了の宣言

- これでメールが送られる

80

届いたかどうか確認しよう

- 確かに届いてる
- しかも「たかさき」から届いたことになっている

- でも、僕は送ってないよ

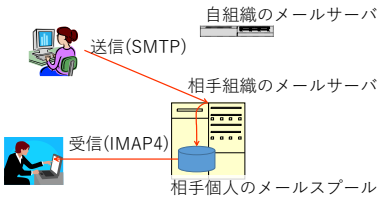
- つまり、メールの詐称が出来たことになる

- 悪用するなよ！！！

81

こんなことはできる？

- 相手の
  メールサーバに
  直接メールを
  送りつける



82

それは「やらない方がいい」

- SMTPは、シンプルってぐらいで「認証手段」がない
  - 今のSMTPにはあるけど、みんなが使ったのは「認証のない」SMTP
  - だから、メールの詐称も可能

- 故に、他人を騙ることも可能
- それを「スパムメール」と呼ぶ

83

だから世の中は

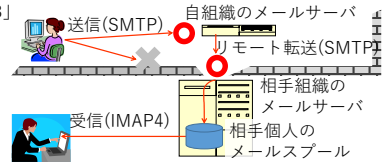
- ウィルスメールとSPAMメールで蔓延る

- SPAMもウィルスも、馬鹿正直に
  名乗る奴なんて居ないヨ！！！

84

なのでいまどきは

- 自組織内から外部へ「25番ポート」宛でつなぐ通信は「できないようになっている」
  - 唯一外に25番ポート宛てで通信出来るのが「自組織のメールサーバ」
  - これを「OP25B」なんて呼ぶ



85

みんなにこの方法を

- 知ってもらったのは、悪用して欲しいからではありません…！
- 世の悪人が、どういう方法を使っているかを知って欲しかったからです
- 繰り返すけど

悪用厳禁！！！

86

本日はお題はありません

- 課題を頑張ってください
- 締め切りは、2024年01月04日(木)です

87