STEP2を実際に行ってみて

- 自己紹介
- AITACの教育コンテンツの概要
- STEP2の概要
- STEP2実施してみて
- 良かった声と課題

自己紹介

- 名前：吉田正之
- 所属：NTTコミュニケーションズ
- 略歴：システムエンジニアとして主に中小企業を中心としたエンタープライズ向けのシステム開発・構築に従事。一般社団法人高度ITアーキテクト育成協議会(AITAC)には設立当初から事務局として活動。

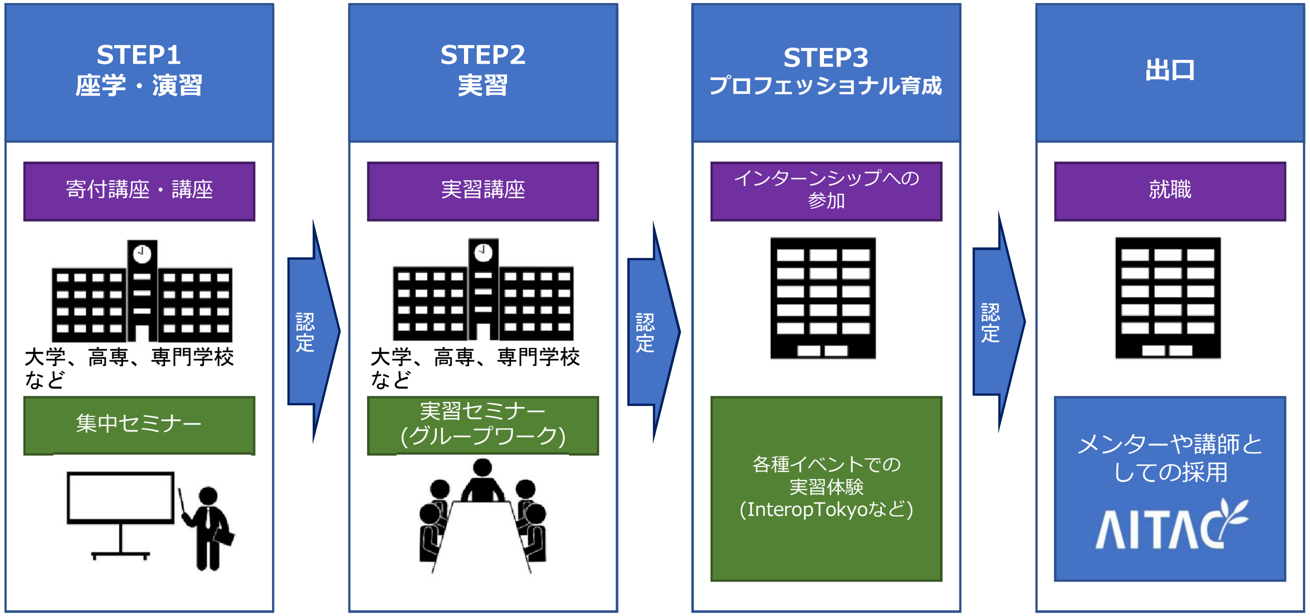
AITAC教育コンテンツの概要

AITAC が育成を目指す人材像

AITACではIoT時代のITインフラを支えるための人材として下記のような人物像の人材の育成を目指しています。

1. トップアーキテクト
   ・ICT 技術を「武器」としてアイディアをシステムに具現化できる人材
2. フルスタックエンジニア
   ・従来の区分である「ネットワーク管理者」と「サーバ管理者」の垣根を超えたハイブリッドなエンジニア
3. システムを運用できるエンジニア
   ・システムを理解しトラブルを解決できる人物
   ・インフラの監視にて得られた情報を適切に運用にフィードバックできる人物

AITACの人材育成活動 全体の流れ



各STEPごとに「修了」と「認定」が設定されています。各生徒にはSTEP1から開始し、各STEPにて用意されているコンテンツをすべて受けることで「修了」の資格が与えられ「認定」を得るためのコンテンツに挑戦する権利を得られます。「認定」の条件をクリアし、「認定」を得ることで次のSTEPに進むことができる。

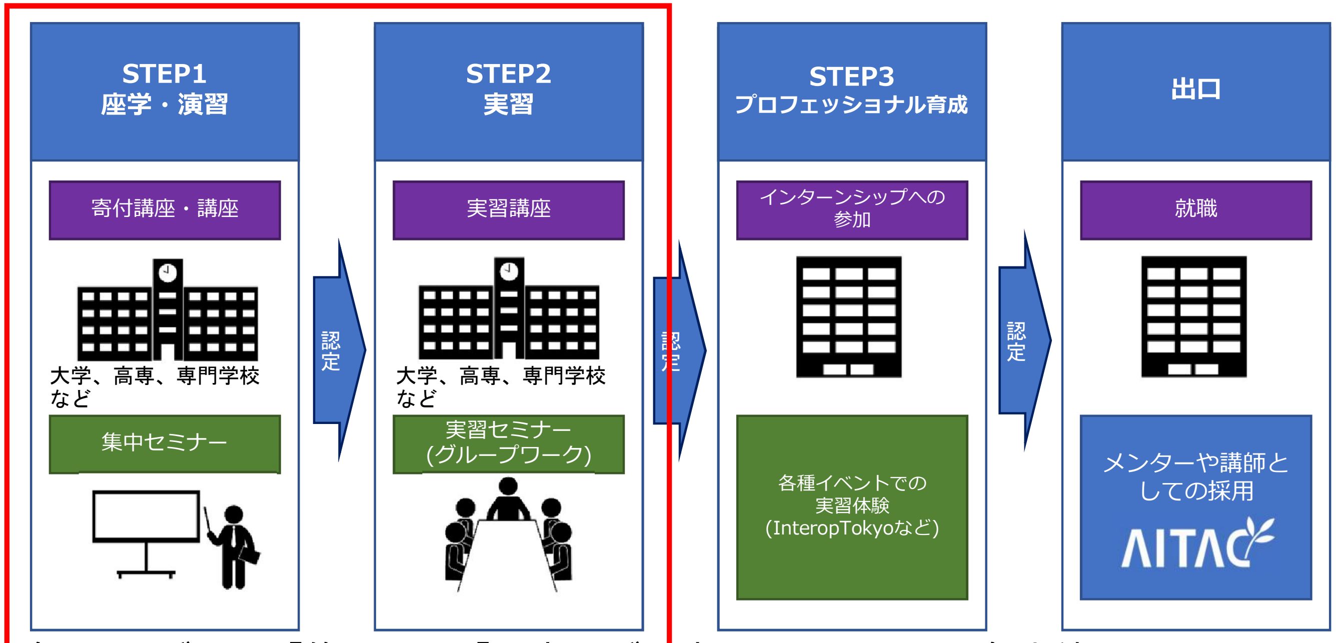
各STEPの概要

●STEP1:
座学・演習にて基礎的な技術を幅広く学ぶ。

●STEP2:
STEP1で学んだことをベースに習得できていない技術については個々で調べながら実践的に技術を学ぶ。

●STEP3:
業務を通してインフラエンジニアとしての経験を積む。

AITACの人材育成活動 全体の流れ



各STEPごとに「修了」と「認定」が設定されています。各生徒にはSTEP1から開始し、各STEPにて用意されているコンテンツをすべて受けることで「修了」の資格が与えられ「認定」を得るためのコンテンツに挑戦する権利を得られます。「認定」の条件をクリアし、「認定」を得ることで次のSTEPに進むことができる。

各STEPの概要

●STEP1:
座学・演習にて基礎的な技術を幅広く学ぶ。

●STEP2:
STEP1で学んだことをベースに習得できていない技術については個々で調べながら実践的に技術を学ぶ。

●STEP3:
業務を通してインフラエンジニアとしての経験を積む。

STEP1について

規定の授業内容を集中セミナーまたは大学の授業にて現在インフラ構築に使われている下記の４分野の技術について「座学と演習」にて幅広く学んでいただきます。

- ネットワークの基礎技術 構築・運用技術 設計方法
- サーバの基礎技術 スケーラビリティー 仮想化技術
- 最新ネットワーク制御技術 サービス仮想化 統合管理技術
- サービスインフラの 設計・構築・プログラミングを用いた設計理論

●目的

幅広くインフラの技術を学ぶ

●実施方法
各会場に集まって集合研修または授業　※eラーニングでの提供予定あり

●実施期間
- 集中セミナー：５日間
- 大学での授業：１年間

●実施回数と修了者の数

- 実施回数：11回
- 修了者：247人

STEP1認定試験の実施

受験資格	STEP1を修了していること
試験の実施方法	筆記試験にて実施
合格基準	規定の問題数を正解する
問題の内容	授業で行った範囲、または授業で行った範囲の応用
目標とする合格率	7割
実施時間	120分

名称	実施時期	受験者数	合格者数
第１回　認定試験	2018/7/27	25名	5名（合格率20%）
第２回　認定試験	2018/9/7	22名	7名（合格率32%）
第３回　認定試験	2019/2/15	26名	17名（合格率65%）
合　計		73名（のべ）	29名（合格率39%）

STEP2の概要

STEP2の概要

約1ヶ月間、業界で活躍するインフラエンジニアや学術機関の研究者などの最先端の動向に詳しいメンターから指導を受けながら、AITACにて設定した課題にグループワークで取り組むプログラム。

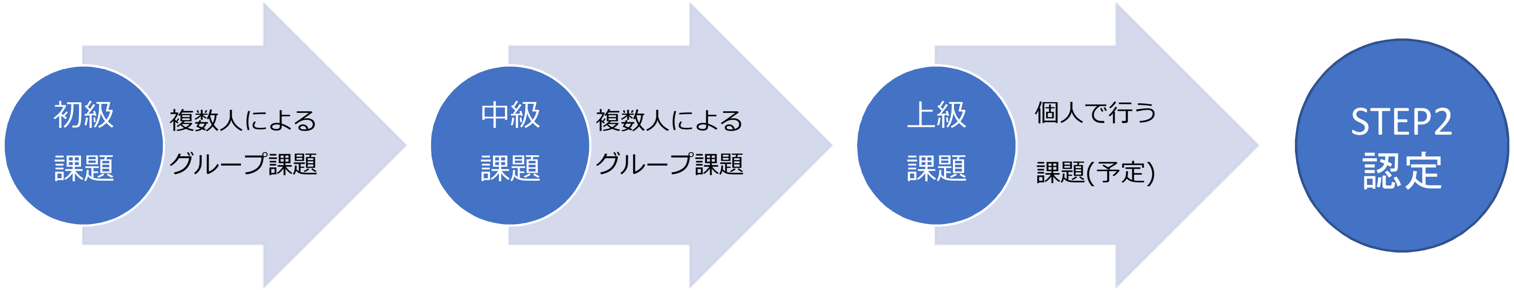
●課題の取り組み方
- 応募者同士で2～3名程度のグループを形成して行うグループワーク
- グループワークは主にオンライン上で行われ、1ヶ月の期間において6日～8日程度の時間を目安に、生徒が自分自身の時間を割いて参加していただきます。

●課題を取り組む期間
1ヶ月程度

STEP2の概要と大まかな流れ

●取り組む課題について
課題は大きく分けて「初級」「中級」「上級」の3つの難易度が設定されている。
「初級」の課題から取り組み、「中級」「上級」と順番に難易度に取り組む。

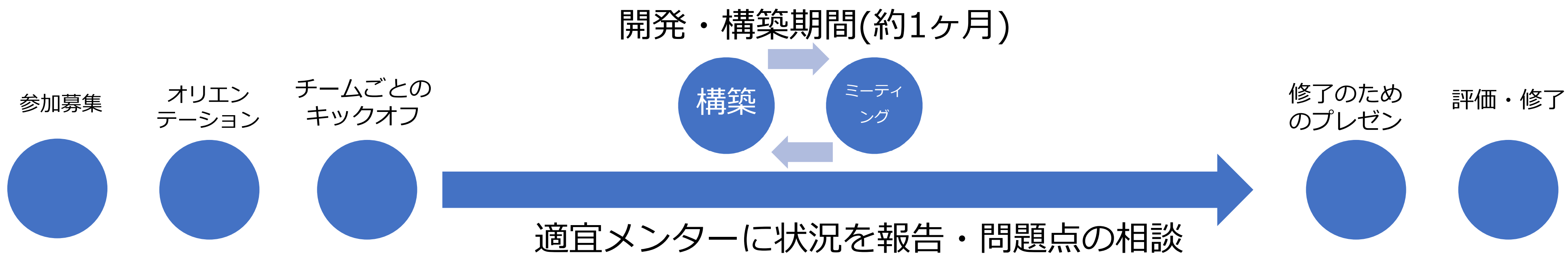
●STEP2全体の流れ



初級から始めていただき、上級課題をクリアすることでSTEP2認定となります

STEP2課題に取り組む大まかな流れ

●課題一つ実施するにあたっての全体の流れ



各チームでのキックオフ後、各チームごとに課題の計画・設計・構築とミーティングなどを繰り返しながらシステムを構築、最後に構築したシステムをプレゼンしてもらい、全体の評価を行って修了。

メンターの役割について

- メンターは課題に対しての問題点の相談
  事務局・カリキュラム委員会との橋渡し
  ※必要に応じてメンター以外の技術者へ橋渡しを行った問題の解決などもう。

  メンターは最大限、アドバイスは行いますが実際の作業で手を動かしたり、課題についてなにか決定を行うことは基本的にはない。

  生徒自身の力で課題に対するシステムを構築する。

STEP2を実施してみて

STEP2の実績

- 現在のところ、2回実施(2018年度に1回、2019年度に1階実施)
- 参加者数は合計で17名
- 進行状況としては最も進んでいる生徒で中級をクリア

実際に選択された「課題」問題

タイトル：	クラウド環境とオンプレミス環境を結ぶ社内システムの構築
課題の内容：	オンプレミスの環境のシステムとインターネット上のクラウド環境に展開されているシステムとが接続できるようネットワーク環境を構築してください。
課題の要件：	・オンプレ・AWS内にはRouter、VMが接続されていること ・機器冗長、回線情調を考慮すること ・オンプレミスとクラウド間については冗長化の設計が考慮されていること

タイトル：	エンタープライズネットワーク構築演習（初級）
課題の内容：	エンタープライズネットワークを想定した要件を提示しそれを満たすネットワーク/サーバ/セキュリティの設計と実装を実機・仮想環境を用いて行ってください
課題の要件：	・具体的には下記の機器・サービスを組み合わせて一つのネットワークと付随するサービスをを作り上げる。 ネットワーク：無線LAN, L2スイッチ，ルータ セキュリティ：ファイアウォール サービス：DHCP, DNS，VPN, web,NTP 監視：snmp, xflowモニタリング, syslog ・可能な限りクラウド環境の作成, ログ統合管理等も構築する

タイトル：	社内コミュニケーションサイトの構築
課題の内容：	オープンソースのソフトウェアを活用して社内コミュニケーションサイトの構築してください
課題の要件：	・機能をサーバ（VMを使用）にインストールして社内LANから利用できるようにする。 チャット機能/ファイル共有/社内連絡用のWebサーバ ・VM一つの中に構築すること ・使用するソフトウェアはOSSを使用すること ・チャットツール・ファイル共有についてはユーザ管理を行えること ・Webサーバについては複数の部署からの要求で違う環境をそれぞれ構築することを想定すること

テーマ別グループ初級課題1

- **タイトル：**
  クラウド環境とオンプレミス環境を結ぶ社内システムの構築
- **課題の内容：**
  ・オンプレミスの環境のシステムとインターネット上のクラウド環境に展開されているシステムとが接続できるようネットワーク環境を構築してください。
- **課題の要件：**
  ・オンプレ・AWS内にはRouter、VMが接続されていること
  ・機器冗長、回線情調を考慮すること
  ・オンプレミスとクラウド間については冗長化の設計が考慮されていること

テーマ別グループ課題2

- **タイトル：**
  エンタープライズネットワーク構築演習（初級）
- **課題の内容：**
  エンタープライズネットワークを想定した要件を提示しそれを満たすネットワーク/サーバ/セキュリティの設計と実装を実機・下層環境を用いて行ってください
- **課題の要件：**
  ・具体的には下記の機器・サービスを組み合わせて一つのネットワークと付随するサービスをを作り上げる.
  ネットワーク：無線LAN, L2スイッチ，ルータ
  セキュリティ：ファイアウォール
  サービス：DHCP, DNS，VPN, web,NTP
  監視：snmp, xflowモニタリング, syslog
  ・可能な限りクラウド環境の作成, ログ統合管理等も構築する

テーマ別グループ課題3

- **タイトル：**
  社内コミュニケーションサイトの構築
- **課題の内容：**
  オープンソースのソフトウェアを活用して社内コミュニケーションサイトの構築してください
- **課題の要件：**
  ・機能をサーバ（VMを使用）にインストールして社内LANから利用できるようにする。
  チャット機能
  ファイル共有
  社内連絡用のWebサーバ
  ・VM一つの中に構築すること
  ・使用するソフトウェアはOSSを使用すること
  ・チャットツール・ファイル共有についてはユーザ管理を行えること
  ・Webサーバについては複数の部署からの要求で違う環境をそれぞれ構築することを想定すること

テーマ別グループ中級課題

タイトル：

IoTセンサを用いた在席確認システムを構築

課題の内容：

単体でインターネットに直接接続可能なIoT機器を利用し，クラウドサービスと連動したサービスを構築してください.

課題の要件：

・センサは複数個利用すること
・席の着席はセンサによって自動で取得する
・センサは何をつかってもよく，また、主題ではないため、センサによる在席情報取得の精度は問わない
・センサデータ譌、サーバ（クラウド側）で収集し、データベースに保存する
・席の着席の状況をリアルタイムで確認できるwebシステムを作成する
・パブリックなクラウドサービスと連携（マッシュアップ）する
-- パブリックなクラウドサービスの例 (IFTTT, AWS IoT Gateway, LINE Things/Notify, など)
-- 例) 収集したセンサデータをトリガーとして、一部屋にX人以上着席したら自動で携帯に通知(LINE APIなど)を送るなど
・データ収集にあたり、プライバシ・セキュリティに配慮、工夫をする
・最後の成果発表時にデモできるようにシステムを構築する

実際に取り組んだ例(初級課題1)

● 要件

課題内容	要件
オンプレミスの環境のシステムとインターネット上のクラウド環境に展開されているシステムとが接続できるようネットワーク環境を構築してください。	● 社内ユーザ(大手町)向けWebサービスを想定 　○ オンプレのVMからクラウド上のWebサービスを閲覧 　○ VMはルータのLANに接続 　○ ルータ間はVPN接続 　○ 障害時の断時間は60秒以内 ● ルータはAWS側との接続が可能なデバイスであること ※1 ※2
オンプレ・AWS内にはRouter、VMが接続されていること	
機器冗長、回線冗長を考慮すること	● 下記を冗長化すること 　○ 機器 　○ 通信経路 ※3 　○ インターフェース・ケーブル ● 冗長が可能な機器を選定すること 　○ 例えば、スイッチならLAG/LACPが設定可能であること
オンプレミスとクラウド間については冗長化の設計が考慮されていること	

※1:Amazonが接続先機器に求める機能: IKE、IPsec tunnel、AES、BGPなど
https://aws.amazon.com/jp/vpn/faqs/#AWS_Site-to-Site_VPN_connectivity

※2:Amazonでテスト済のデバイス
https://docs.aws.amazon.com/ja_jp/vpc/latest/adminguide/Introduction.html#DevicesTested

※3: キャリアという意味で回線の冗長化はしない

実際に取り組んだ例(初級課題1)

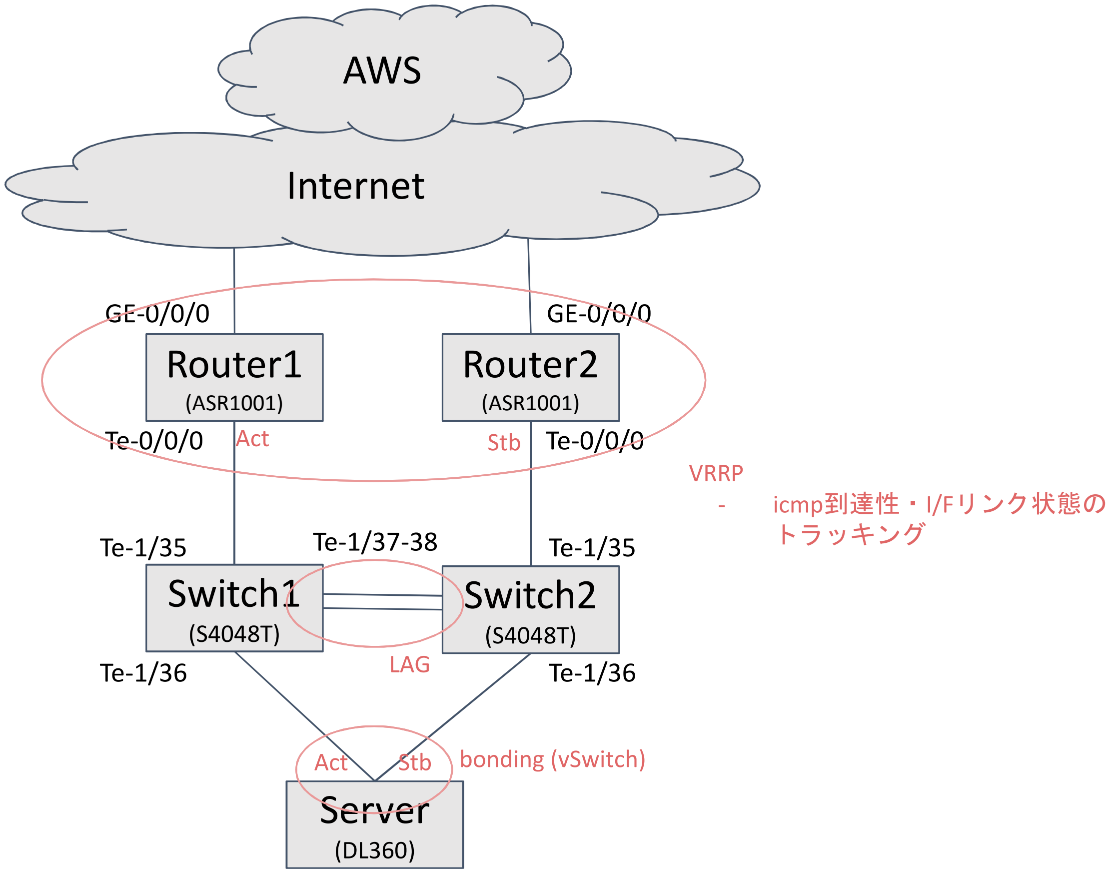
- コンセプト

物理・論理設計を行う上で下記を心がけた

- どこが切れてもサービス継続可能
  - SPOFを排除
    - ただし二重障害はスコープ外
- シンプルな設計
  - 構築・運用を容易にする
    - 構築の漏れが起こりにくい
    - 検証項目が列挙しやすい
    - 障害時に原因の切り分けがしやすい

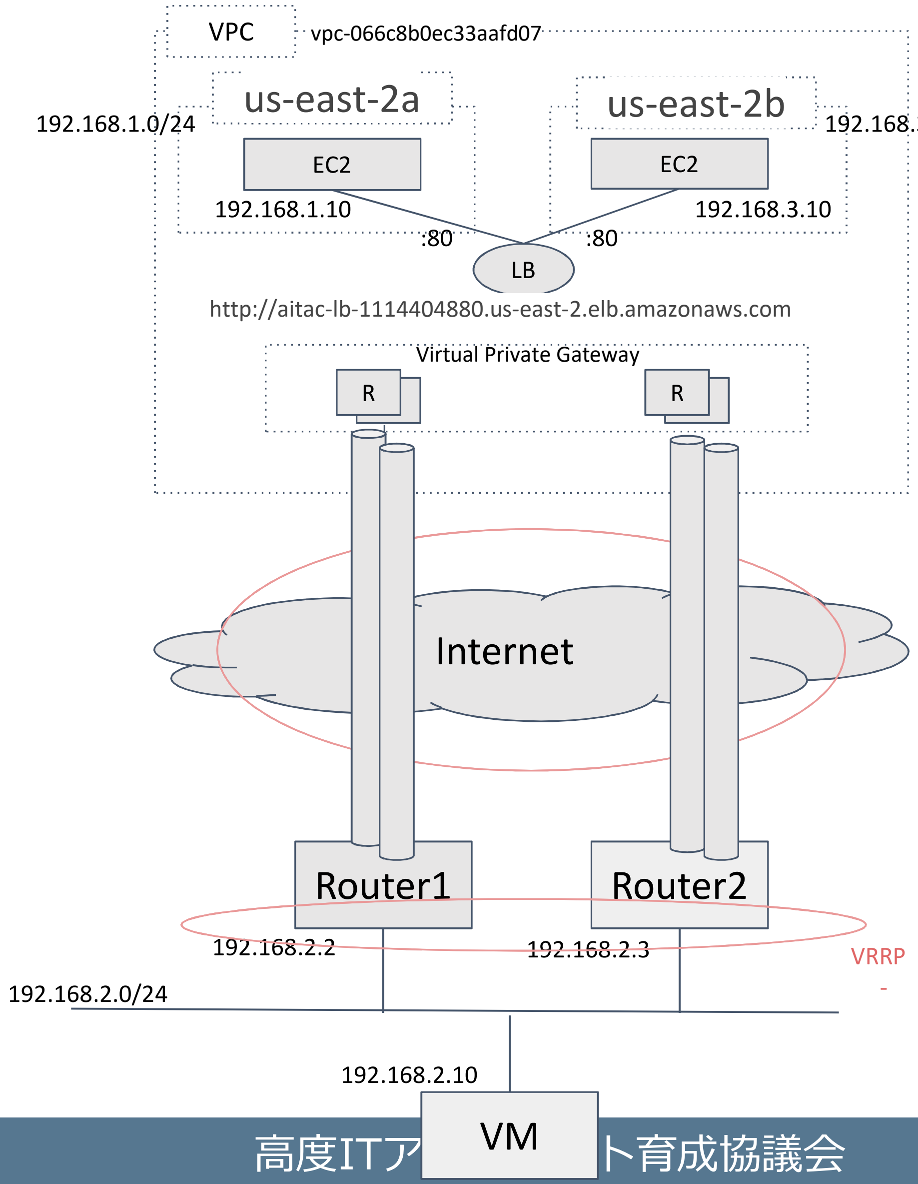
実際に取り組んだ例(初級課題1)

- 物理設計



●論理設計

AWS



LB

- ポート80向けを2VMの
  ポート80へバランシング
- ここで、Webサービスが展開
  されている、という想定

ルートテーブル(rtb-015739b4c2edd6f9f0

- 192.168.1.0/24 -> local
- 0.0.0.0/0 -> vgw-0e585acba946ef73b

大手町

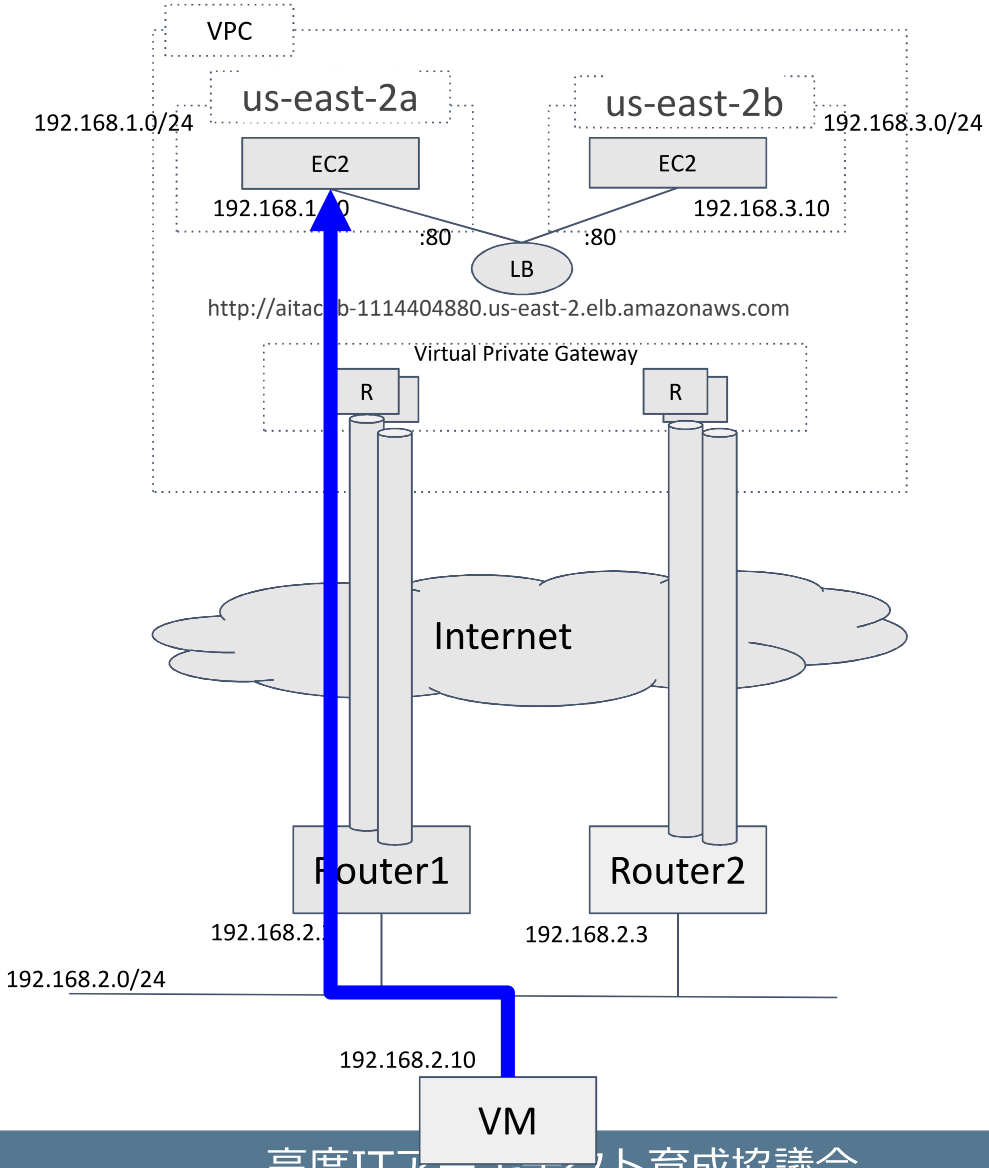
VRRP

- 192.168.2.1

●デモ (1)

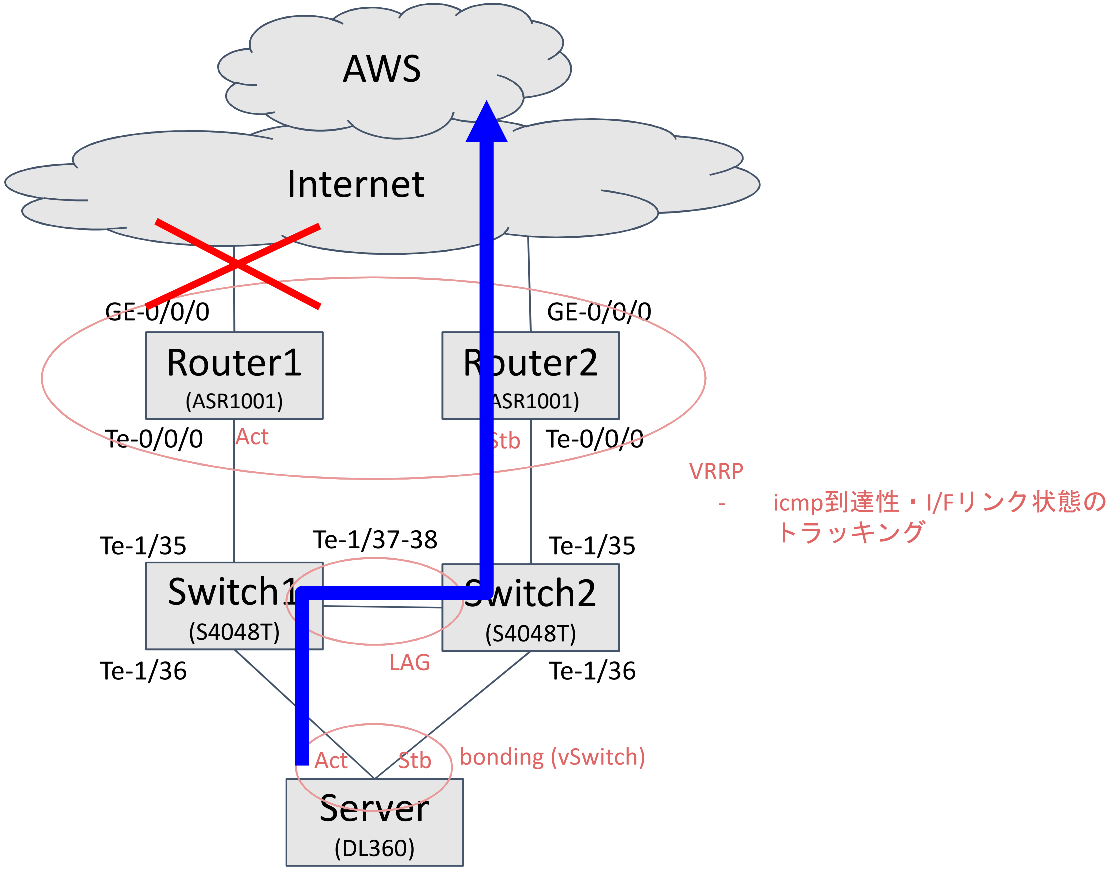
AWS

大手
町



VPC
us-east-2a
us-east-2b
192.168.1.0/24
192.168.3.0/24
EC2
EC2
192.168.3.10
:80
:80
LB
Virtual Private Gateway
R
R
Internet
Router2
192.168.2.3
192.168.2.0/24
192.168.2.10
VM

●デモ (2)


AWS
Internet
GE-0/0/0
GE-0/0/0
Router1
(ASR1001)
Router2
(ASR1001)
Te-0/0/0
Act
Stb
Te-0/0/0
VRRP
- icmp到達性・I/Fリンク状態のトラッキング
Te-1/35
Te-1/37-38
Te-1/35
Switch1
(S4048T)
Switch2
(S4048T)
LAG
Te-1/36
Te-1/36
Act
Stb
bonding (vSwitch)
Server
(DL360)

実施風景

AITAC

良かった声と課題

●良かった点：

・全体的に普段業務での経験のない技術に触れてよかったとの声が多かった

・普段関わりのない技術者との交流ができている

●課題：

・時間をとるのが苦しそう

・希望する課題がかぶると機材が不足しがち

・メンターの不足