

APRICOT-APAN 2015における ネットワークチームの取り組みについて

APRICOT-APAN 2015 ネットワークチーム

谷崎文義/高田美紀/川上雄也

APRICOT・APAN 2015

概要

APRICOT-APAN 2015 開催概要

- 日程：2015/2/24/(火)-3/6(金) ;11日間
- 会場：福岡国際会議場、JR博多シティ
- 主催：APRICOT-APAN 2015 日本実行委員会
- 構成内容
 - ・ ワークショップ、チュートリアル、コンファレンス、ワーキンググループセッション、併設展示・デモ、レセプション、ソーシャルイベント
- 参加人数：1,000名（予定）（内海外400名；60カ国）
- 対象
 - ・ アジア太平洋のインターネットコミュニティ、ネットワーク運用に携わる技術者からポリシー策定・資源管理に興味を持つ方まで、アジア各国のインターネットインフラに興味を持つ方
- 参照：<http://jp.apricot-apan.asia/>

ネットワークチームがやるべきことは何か？

- 会期は全体で2週間弱
 - ・ 2015/2/24/(火)-3/6(金) ;11日間
- 異なる2つの会場
 - ・ JR博多シティ
 - ・ 福岡国際会議場
- 性格の異なる2つの国際会議
 - ・ APRICOT
 - ・ APAN
- 来場者は世界中から1000人？
 - ・ みんな2台くらいはwifiデバイス持ってるよね？！
- **スムーズな会議運営のために安定したネットワーク環境は必須**

目的、目標

■ ネットワークチームの目的

- ・ 来場者が会期中に快適に過ごせるような会場ネットワーク環境を提供する

■ 活動の目標

- ・ 日本のエンジニアが持つ構築運用技術の高品質さを来場者にアピールする
- ・ 次の世代を担うエンジニアの育成、地方の優れた人材を発掘する

APRICOT・APAN 2015

取り組み概要：会期前の準備

- 事前準備 (2014/1/下旬にスタート)
 - ・ ネットワーク設計
 - ・ 回線の調達と事前工事
 - ・ 必要な機材の洗い出しと借用の調整
 - ・ 会場側スタッフとの打ち合わせ及び現地調査
 - ・ ネットワーク構築のための人材募集
 - ・ APAN/APIA/日本実行委員会との調整など
- ホットステージ(事前設定)
 - ・ 2014/2/16 – 2/20
 - ・ 場所：九州産業大学
 - ・ 目的：全ての機器を設計通りに一度構築し、動作を確認する
 - ・ 作業内容：
 - ✓ 借用した機材について、管理のためのラベル貼り
 - ✓ 機器を設定
 - ✓ UTPや光ケーブルでのつなぎ込み
 - ✓ 提供するすべての環境がきちんと動作しているかどうかの確認試験
 - ✓ 設計に関する議論とドキュメントのアップデート

取り組み概要：開催期間中

■ ワークショップ(JR博多シティ)

- ・ ワークショップごとに異なる有線/無線LANネットワーク、各種サービスを提供するサーバー群を構築
- ・ ワークショップ参加人数：91
- ・ 来場者の持ち込み端末総数：396

■ 本会議(福岡国際会議場)

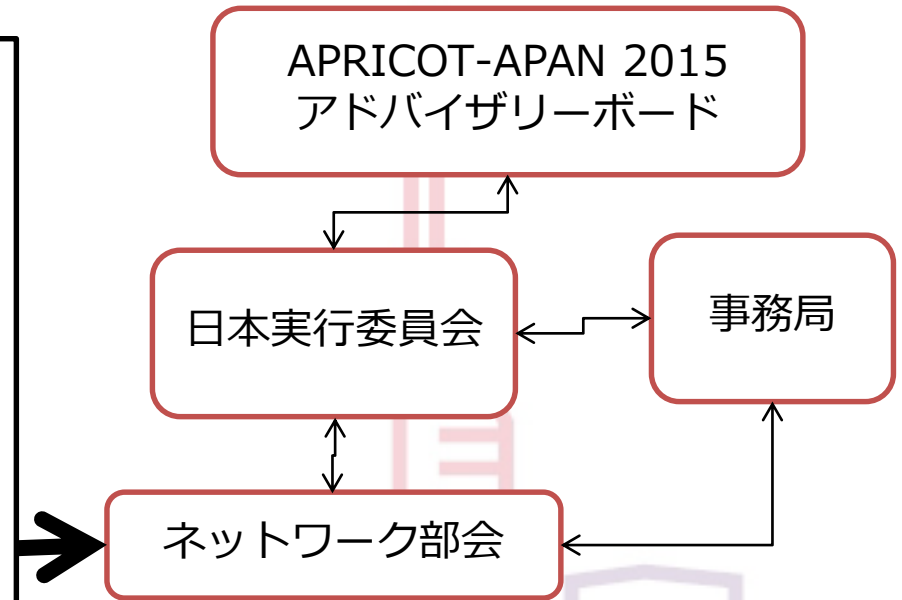
- ・ 来場者の生活用無線LANネットワーク、および会期中に行われるさまざまなデモやWeb配信、出展社ブースのための有線LANネットワーク、各種サービスを提供するサーバー群を構築
- ・ 参加人数：868
- ・ 来場者の持ち込み端末総数：1796

■ 会期中における両会場共通の取り組み

- ・ ネットワークの監視とトラブル時の対応、チューニング、機器の設定変更、無線APやスイッチ等ネットワーク機器の増設など
- ・ 来場者むけに会場ネットワークに関するサポートを行うネットワークヘルプデスクを開設

実行体制

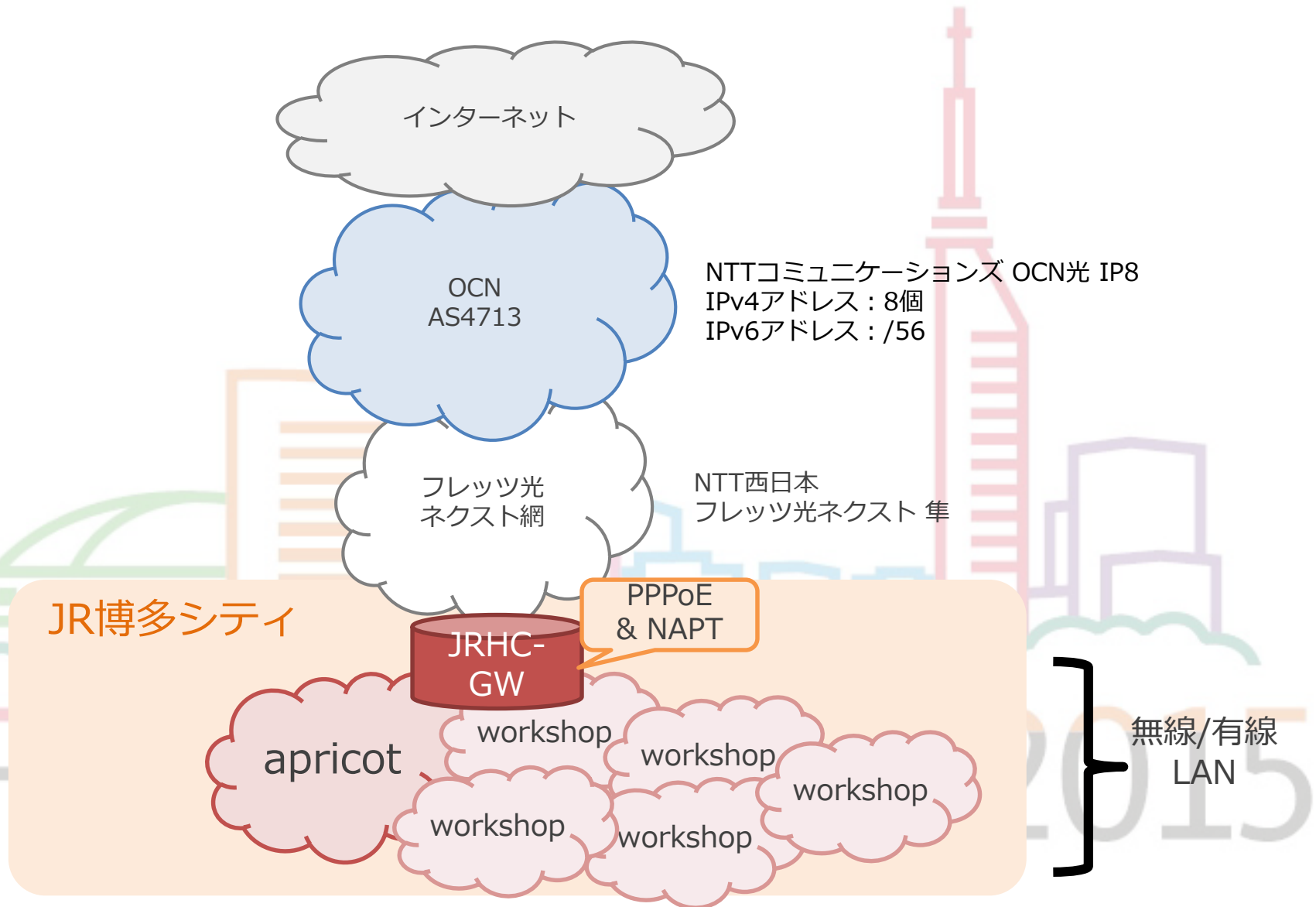
- チェア 2名 (1名)
- ネットワークデザイナー 2名
- エンジニア 22名 (6名)
- 大学教員 2名 (2名)
- スタッフ
 - ・ 社会人 5名 (4名)
 - ・ 学生 14名 (14名)
- アドバイザ 2名
- ()内は九州在住



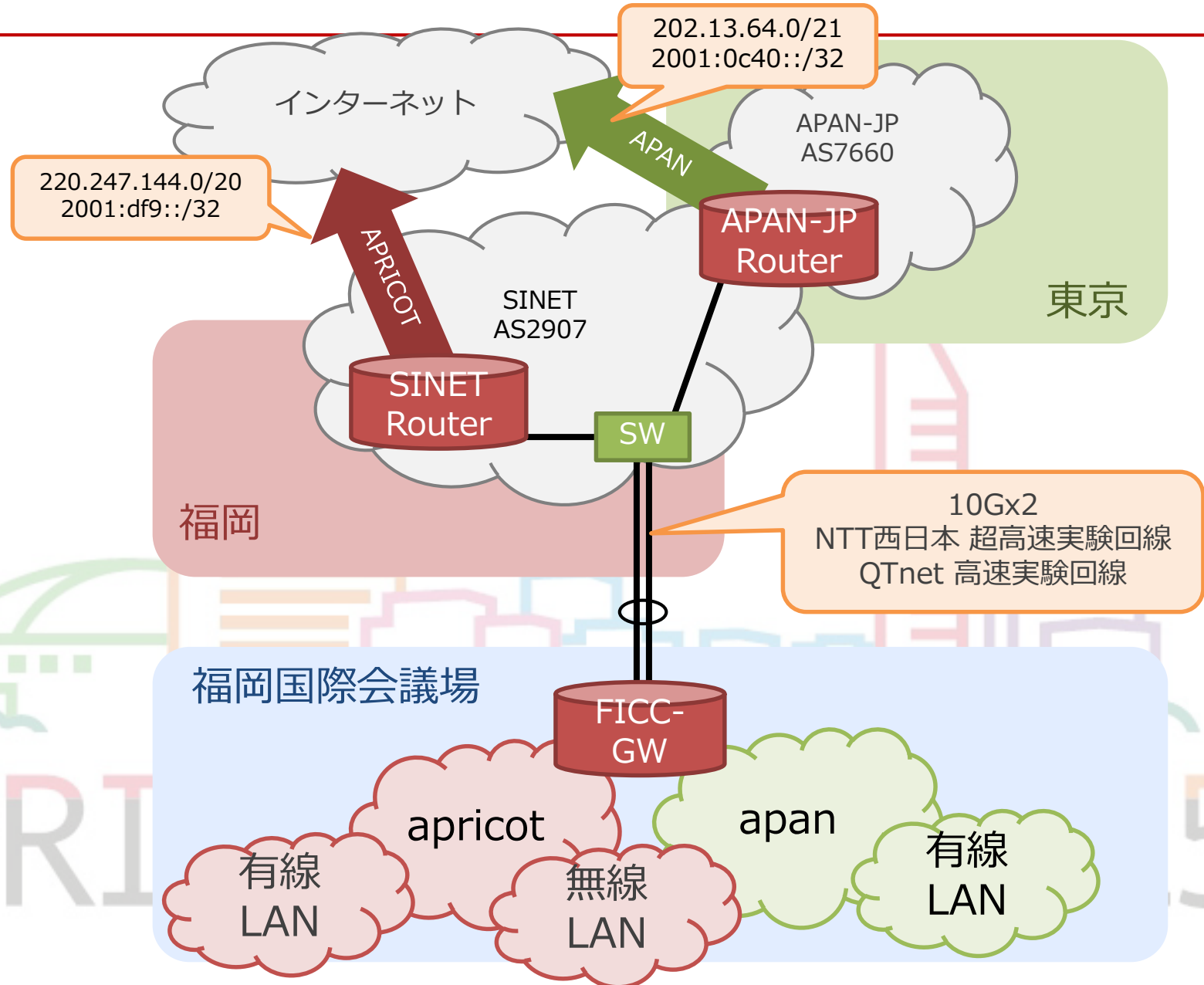
ネットワークチームのスケジュール

Mon	Tue	Wed	Thu	Fri	Sat	Sun
9	10	11	12	13	14	15
機材入荷						
16	17	18	19	20	21	22
ホットステージ(九州産業大学)						
23	24	25	26	27	28	1
JRHC NW構築	ワークショップ(JR博多シティ)				JRHC撤去 FICC構築	
2	3	4	5	6	7	8
カンファレンス(福岡国際会議場)						

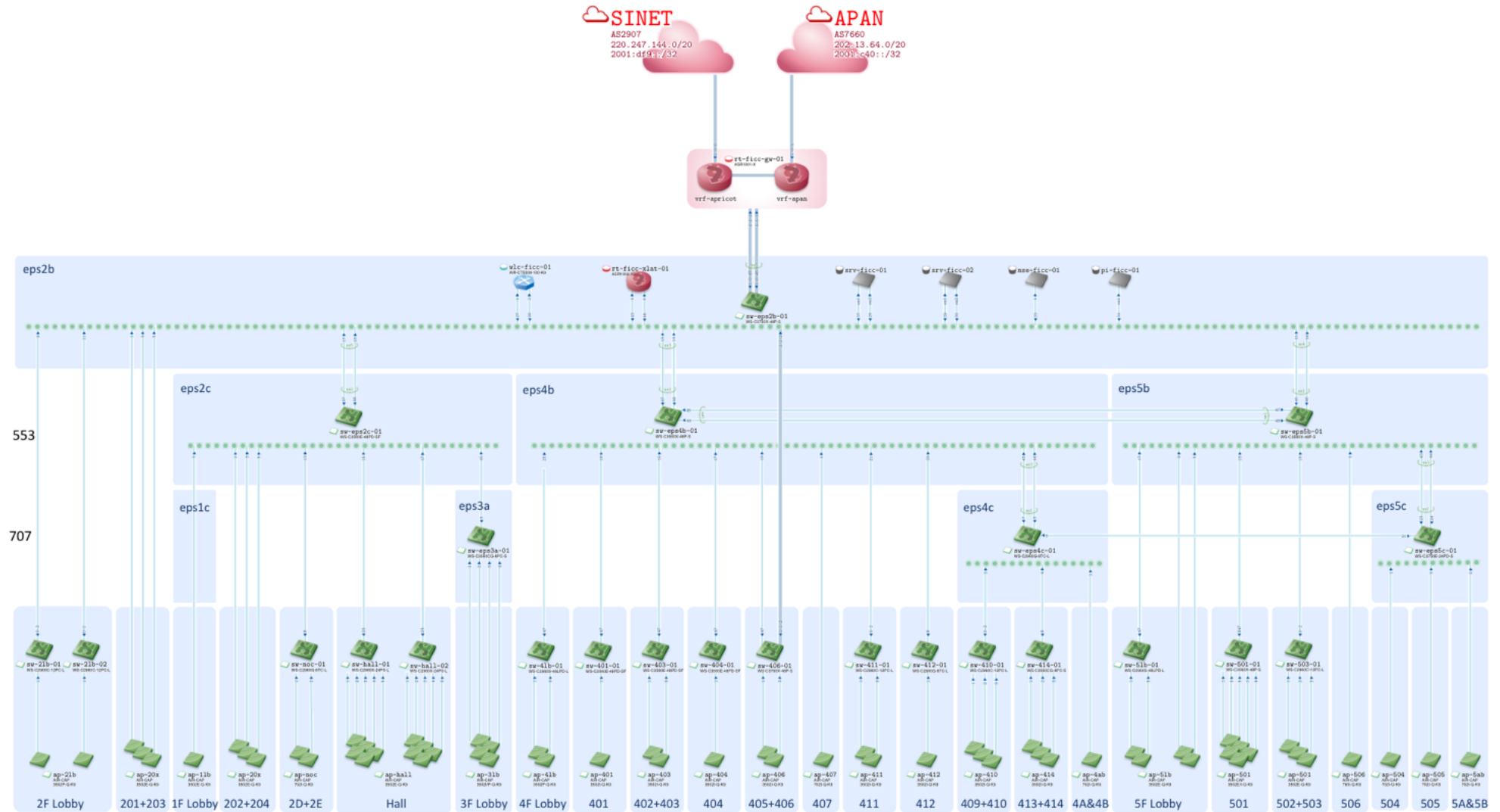
ネットワーク概要図: ワークショップ (JR博多シティ)



ネットワーク概要図: カンファレンス (福岡国際会議場)



福岡国際会議場ネットワーク全体構成概要図



無線LANについて

利用場所	SSID	規格等
用途：インターネットアクセス		
JR博多シティ 福岡国際会議場	apricot	802.11a / WPA2 PSK+AES
	apricot-g	802.11g / WPA2 PSK+AES
福岡国際会議場	apricot-xlat	802.11a/g / WPA2 PSK+AES
	eduroam	802.11a/g / WPA2 802.1X+AES
用途：ワークショップ専用		
JR博多シティ	workshop-dns	802.11a/g / WPA2 PSK+AES
	workshop-bgp	
	workshop-security	
	workshop-mpls	
	workshop-netmon	
用途：APANネットワーク専用		
福岡国際会議場	apan	802.11a / WPA2 PSK+AES
	apan-g	802.11g / WPA2 PSK+AES

借用した機材及び回線

■ 機材 (予備機を含めて借用)

- ・ シスコシステムズ合同会社様から借用
 - ✓ ルータ(ASR1001-X, ASR1002-X, C1941, C2951) : 4台
 - ✓ L2/L3スイッチ(Catalyst 3750/3560/2960) : 約30台
 - ✓ 無線LAN AP (Aironet 3502/702) : 約80台
 - ✓ テレビ会議システム(TelePresence System EX) : 2台
 - ✓ その他、無線LANコントローラ、電源や光拡張モジュールなど
- ・ KDDI様から借用
 - ✓ サーバー(Dell PowerEdge R410) : 4台

■ 回線

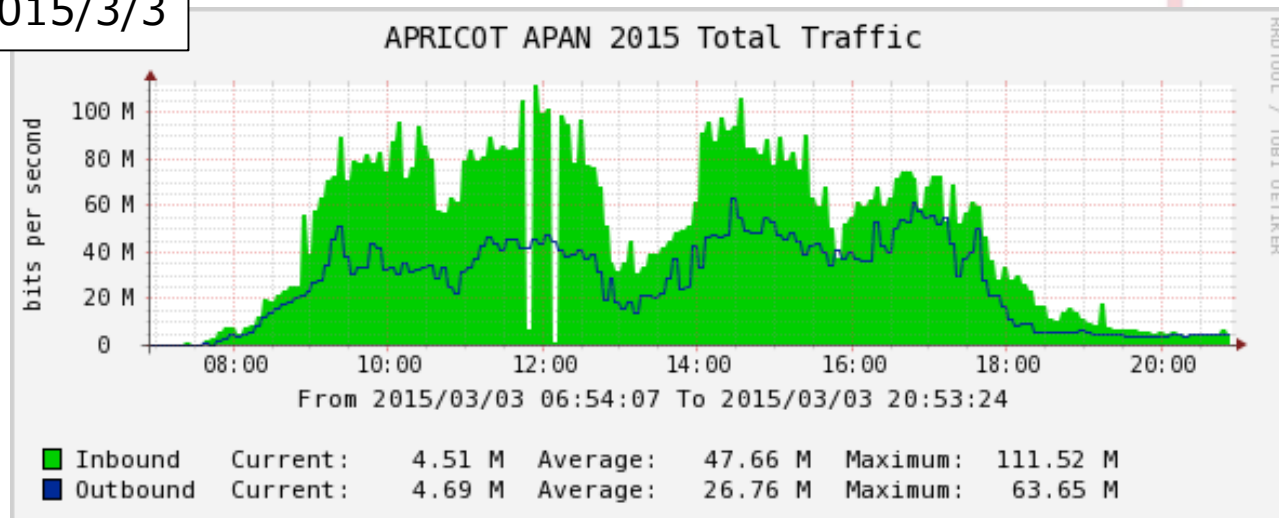
- ・ 福岡国際会議場
 - ✓ NTT西日本 超高速実験回線 : 1回線
 - ✓ QTNet 実験回線 : 1回線
- ・ JR博多シティ
 - ✓ NTT西日本
 - ✓ フレッツ光ネクスト ファミリー・スーパーハイスピードタイプ 隼 : 2回線

■ ISPアカウント

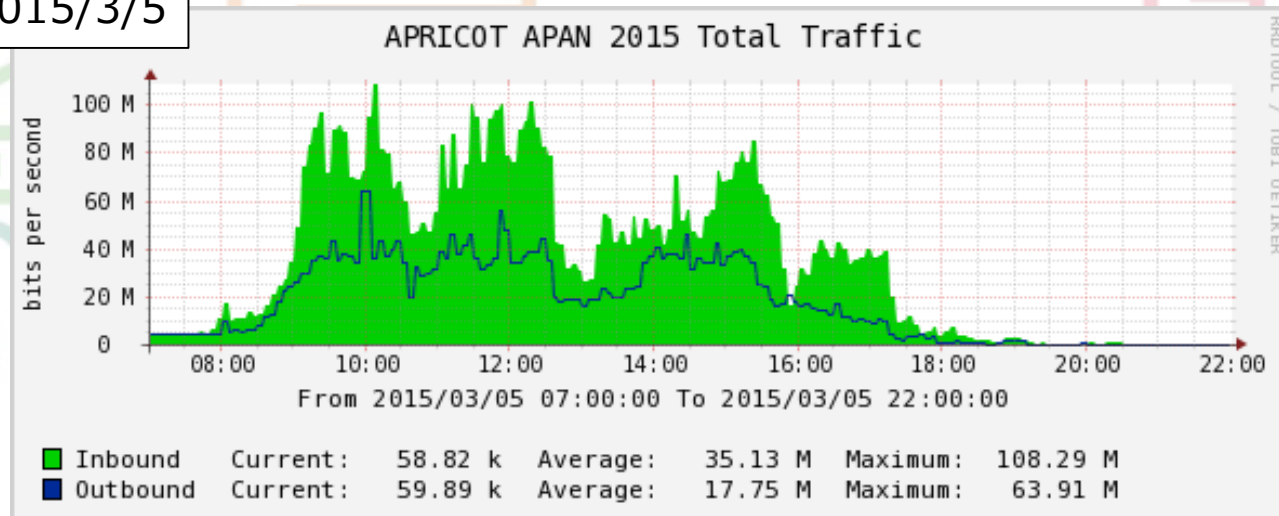
- ・ NTTコミュニケーションズ OCN光 IP8 : 2アカウント

観測：会期中の総トラフィック(福岡国際会議場)

2015/3/3



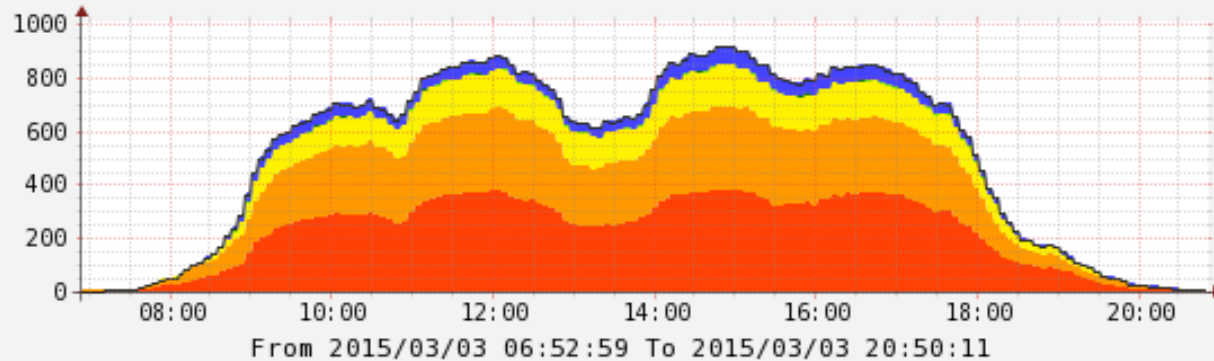
2015/3/5



観測：会期中の無線LANのSSID毎クライアント接続数 (福岡国際会議場)

2015/3/3

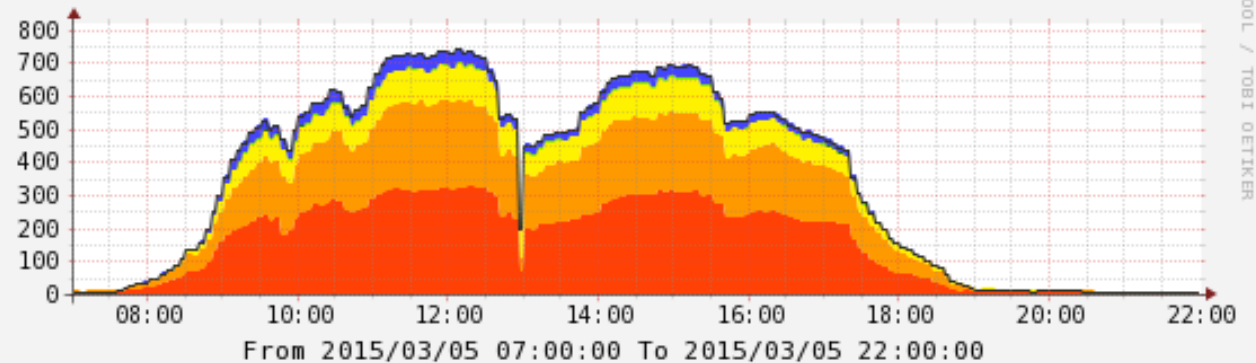
APRICOT APAN 2015 Mobile Stations per ESSID



apricot	Max:	383
apricot-g	Max:	317
apricot-xlat	Max:	159
apan	Max:	4
apan-g	Max:	3
eduroam	Max:	64
Total	Max:	919

APRICOT APAN 2015 Mobile Stations per ESSID

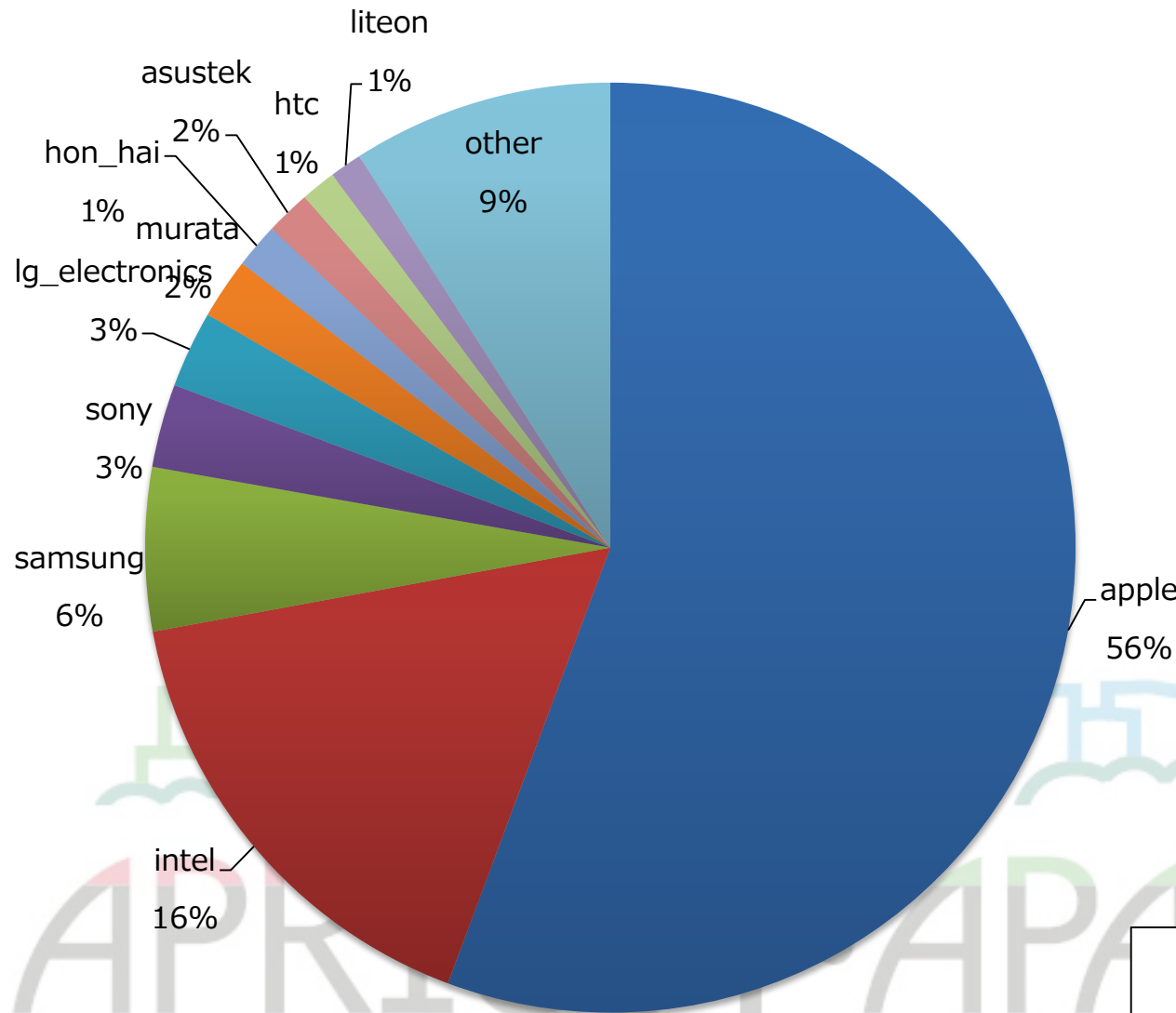
2015/3/5



apricot	Max:	328
apricot-g	Max:	269
apricot-xlat	Max:	109
apan	Max:	6
apan-g	Max:	2
eduroam	Max:	47
Total	Max:	744

APRICOT

観測：来場者持ち込み端末のMACアドレス別分析結果 (福岡国際会議場)



MACベンダ名	端末数
apple	1000
intel	295
samsung	102
sony	52
lg_electronics	48
murata	38
hon_hai	28
asustek	28
htc	22
liteon	20
other	163
合計	1796

来場者数：843名

事前準備

準備

- ネットワーク設計
- 回線の調達と事前工事
- 必要な機材の洗い出しと借用の調整
- 会場側スタッフとの打ち合わせ及び現地調査
- ネットワーク構築のための人材募集
- APAN/APIA/日本実行委員会との調整など
- ホットステージ

APRICOT・APAN 2015

設計のポイント

- APRICOTとAPANという性格の異なる二つの会議が同時に行われたが、それぞれの会議がネットワークに要求するものが異なるものであったため、それぞれの会議のコアネットワークを論理的に分け、且つ末端部分のネットワークを共有化できるようにする。
- 無線LANに関しては、様々なデバイスが多数持ち込まれる(想定台数：2000台)こととそのデバイスが接続のために実際に用いる無線LANのチャンネルが国別に異なることが想定されることから、5GHz帯と2.4GHz帯で異なるSSIDを用意し、できるだけ5GHz帯での接続を利用してもらえようようにする。
- JR博多シティと福岡国際会議場の二つの会場ネットワークを全く別のものとして設計すると、機材のやりくりや運用が煩雑になると考え、論理設計(VLAN番号やマネジメント用のIPアドレス、機器の設定ポリシー等)の共通化を行い、機材を使い回せるようにする。

事前準備スケジュール

2014年

日程	場所	内容
3/4	福岡国際会議場	会場スタッフとミーティング 現地視察
	九州大学	ネットワークチーム打ち合わせ
4/14	福岡国際会議場	会場ネットワーク担当者とミーティング
4/15	JR博多シティ	会場スタッフとミーティング 現地視察
	九州産業大学	ホットステージ会場現地調査
5/8	JR博多シティ	会場スタッフとミーティング、現地調査
9/17	福岡国際会議場	QTNet回線敷設事前調査 会場既設LANケーブルチェック
	九州産業大学	ミーティング
10/24	九州産業大学	AA2015事務局とのミーティング
11/21	天神DC	構内光ケーブル敷設工事
11/25	天神DC	福岡国際会議場-天神DC
	福岡国際会議場	QTNet回線開通工事
12/17	JR博多シティ	会場スタッフとミーティング 現地調査
12/26		第一回ネットワーク設計レビュー

2015年

日程	場所	内容
1/9	JR博多シティ	会場スタッフとミーティング 現地調査
1/27		第二回ネットワーク設計レビュー
2/12	九州産業大学	ホットステージ事前準備
2/13	九州産業大学	ホットステージ事前準備
2/16	九州産業大学	ホットステージ
2/17	九州産業大学	ホットステージ
	JR博多シティ	NTTフレッツ回線開通工事
2/18	九州産業大学	ホットステージ
2/19	九州産業大学	ホットステージ
2/20	九州産業大学	ホットステージ JR博多シティ用機材搬出
2/20	JR博多シティ	機材搬入

ホットステージ

■ 目的

- 双方の会場向けに設計したネットワークを会期前に実際に構築し動作検証を行うことで以下を実現する。
 - ✓ ネットワーク安定稼働のための課題の抽出と解決
 - ✓ 構築や運用に関わるスタッフ間での情報共有とスキルの平滑化
 - ✓ 会場での設営/撤収の時間短縮
- 実際に使用するIPアドレスやVLAN番号での構築/設定を行うことで設営時の作業項目を削減する取り組みを行ったが、これは九州ギガポッププロジェクト(QGPOP)の既設ネットワークを利用することで実現した。

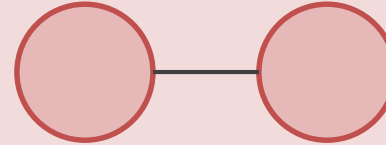
■ ポイント

- 次の世代を担うエンジニア(主に大学生)の育成
- 地方の優れた人材を発掘する場

ホットステージ人員配置図

- 東京や九州のエンジニアと、九州産業大学や九州工業大学の学生で1:1または1:2のチームを構成
- チーム単位で作業を実施

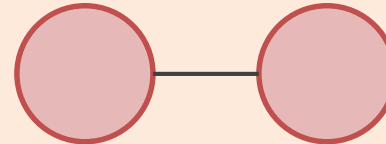
チェア(全体をマネジメント)



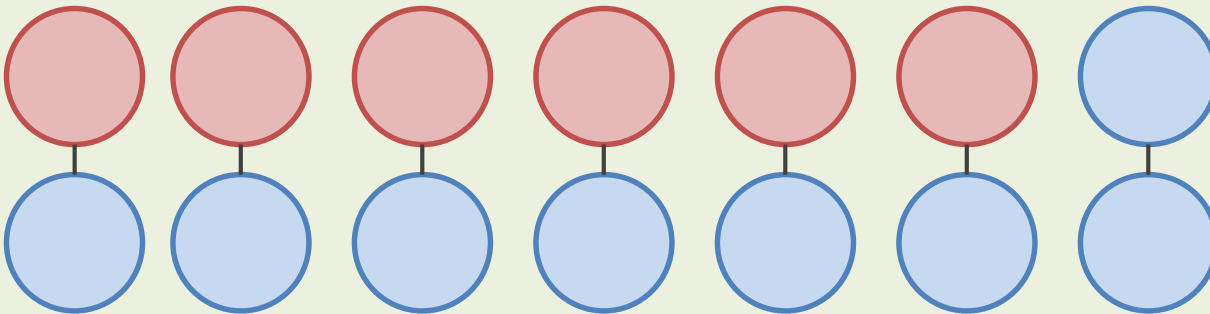
エンジニア(社会人)

大学生

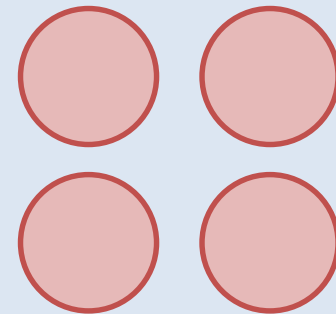
デザイナー(主に設計)



スタッフ(機器設定、試験等を担当)



技術サポート



会期中の取り組み

ヘルプデスクの開設、運用

- 来場者のために会場ネットワークに関するサポートを行うネットワークヘルプデスクを開設し、学生を中心に専任のスタッフを配置した。
 - ・ 開設時間：会期中の 8:00～18:00まで(2交代制)
 - ・ 場所：レジストレーションデスク脇
 - ・ 主な業務：ネットワークに関するサポート、業務日誌の作成、各種アラートメールの監視、トラフィック等の監視
- 体制
 - ・ スタッフ：ヘルプデスクに常駐。来場者からの問い合わせに対応。
 - ・ スタッフリーダー：スタッフのとりまとめを行う。
 - ・ エンジニア：スタッフからのエスカレーションを受け、主に技術的な支援を行う。
- 人員配置数
 - ・ JR博多シティ
 - ✓ エンジニア 2名、スタッフリーダー 1名、スタッフ 2名
 - ・ 福岡国際会議場
 - ✓ エンジニア 2名、スタッフリーダー 2名、スタッフ 4名

業務日誌

- 当日の対応状況を把握するために作成した。
 - ・ ヘルプデスクスタッフにて記入
 - ・ 対応について項番、受付者、問い合わせ内容、対応内容、状況、エスカレーション先を管理
 - ・ 翌日への申し送り事項なども記載
- 毎朝の朝礼では前日までの申し送り事項を確認した。
- 毎夕の終礼では当日の対応状況を確認、翌日への持ち越しをするかどうかの判断を行う等した。

業務日誌例

日付	2015/03/02
エンジニアシフト名	
スタッフシフト名	午前：前野、古柴、小野、高橋、門脇 午後：前野、山崎、金丸、高橋、堤

====終了ミーティングログ=====

無線の問題が少し発生。適宜対応してください。
抱えてる問題：WordPress問題。APNICのブースに有線無線出す問題。501の部屋の問題。
Opening receptionに参加しましょう！
明日の夜はしゃぶしゃぶ！
明日のヘルプデスク担当：
午前：竹田、衛藤、堤、古柴、山口、ゆーきゃん（字が綺麗）
午後：竹田、衛藤、山口、古柴、中島、興梠さん



項番	受付時刻	受付者	問い合わせ内容	対応内容、原因など	継続中/終了	エスカレーション先	memo
14	13:36	高橋	Wi-Fi に接続したプリンタから印刷できない	プリンタとAPの接続が切れた模様。リブートで復旧。	終了		
15	13:40	小野	Wi-fiのPWを入力しても接続できない	タイプミス(keyboardの反応がすごく悪い)	終了		
16	14:07	堤	Wi-Fiのパスワードを尋ねられた	パスワードを教えた	終了		
17	15:34	堤	アプリに登録したのにアカウントが見つからない	受付に案内した	終了	受付	登録したばかりなため反映が明日になる（たぶん）
18	15:32	山崎	ミーティング登録システムを見ることが出来ない。	scottさんに原因調査を依頼。	終了	scott・りえさん	APNICに原因を調べてもらう
19	16:00	堤	ACアダプターを貸してほしい	無いとお伝えした	終了		
20	16:09	堤	Wi-fiが繋がらない	接続しなおしたら繋がった	終了		移動中や人の多いところで接続が不安定になっていた
21	17:20	高橋	会場Wi-Fiについて聞かれた	SSID, PW の案内をした	終了		
22	17:25	小野	5Fへの行き方を聞かれた。	案内した。	終了		

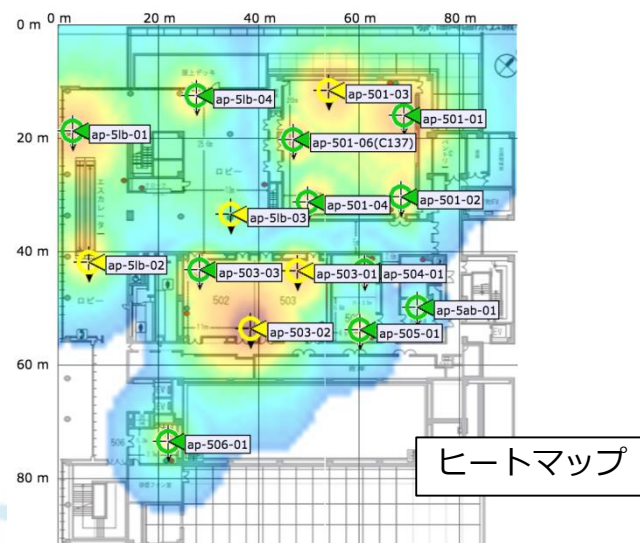
ヘルプデスク対応状況（業務日誌より集計）

日付/案件	場所	ネットワークに関する問い合わせ	それ以外の問い合わせ	合計
2015/2/23	JR博多シティ	7	1	8
2015/2/24		15	14	29
2015/2/25		12	4	16
2015/2/26		2	3	5
2015/2/27		14	7	21
2015/2/28		1	2	3
2015/3/1	福岡国際会議場	16	15	31
2015/3/2		11	15	26
2015/3/3		6	9	15
2015/3/4		4	5	9
2015/3/5		2	1	3
2015/3/6		0	3	3
	合計	90	79	169

来場者からの主な問い合わせ内容	
* ネットワーク	
1	wi-fiの情報を教えてほしい
2	wi-fiに接続できない
3	有線を使えるようにしてほしい
4	アクセスポイントを増設してほしい
* それ以外	
1	プリンタの設定をしてほしい
各種機器のアダプターなどを貸してほしい	
2	ほしい
3	プロジェクターがつかない
場所の案内(100円ショップ・ヨドバシカメラ)	
4	写真を撮ってほしい

ネットワーク監視について

- ネットワーク機器の状態を監視し、しきい値を越えた際は警報を送出する仕組みを構築し、会期中に運用を行った。
- 機器状態監視
 - ping監視 : deadman
- 無線LAN監視
 - コントローラー監視 : wlcmon
 - AP 電波状態監視 : ヒートマップ
 - 接続数監視 : cacti
- ネットワーク監視
 - トラフィック監視 : cacti
- 警報
 - SNMPトラップに伴う警報 : snmptrapd
 - pingによる死活監視に伴う警報 : Nagios
- webによる一般公開
 - ネットワークのトラフィック : weathermap



Twitterでの情報配信

- ホットステージ及び会期中にネットワークの状態やメンテナンス情報、ネットワークチームの活動の様子を広報するためにTwitter(@aa2015_nw)を活用した。
- https://twitter.com/aa2015_nw

AA2015-NW
@AA2015_NW

フォロー

Our nw-team started setup here at JR hakata city!! #AA2015NW

🔗 📷 ⭐ ...



AA2015-NW
@AA2015_NW

フォロー

Emergency maintenance:
You will have possibility to experience of
association down once due to maintenance
around 13:00[JST] #apricot2015

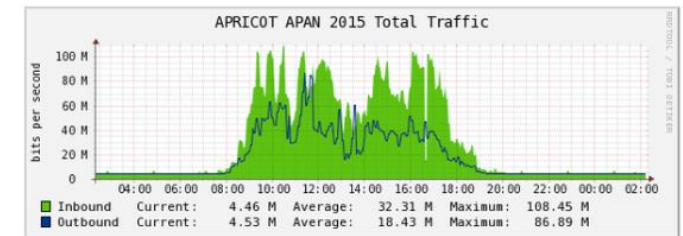
📍 福岡県 福岡市 博多区

フォロー

Today's traffic volume of the conference
network.

📍 石川県 金沢市

🔗 📷 ⭐ ...



9:25 - 2015年3月4日

スタッフ間コミュニケーション

- ネットワークチームのメンバーは地理的に分散していたため、密接なコミュニケーションや情報共有のために以下を利用した。
 - メールングリスト
 - Facebook
 - ✓ ネットワークチームの非公開グループを作成
 - ✓ グループ内掲示板投稿
 - ✓ メッセンジャーによるグループチャット
 - Googleドライブ
 - ✓ 各種資料の共有、オンラインでの共同編集
- 福岡国際会議場では業務用トランシーバーを活用した。以下の点でトランシーバーは有用性が高い。
 - 会場ネットワークの状態と関係なく音声通話が可能。
 - 特に設営や撤収時、会場ネットワークを利用できない場合に有用。
 - 操作が簡単で携帯性が高い。

スタッフ間コミュニケーションの向上

- 今回のネットワークチームのようなプロジェクトの場合、実際にスタッフが集まる期間が非常に短いことから、その限られた期間のうちに各スタッフ間の信頼関係を築くことやスタッフ各々のモチベーションを向上させることは、とても重要である。
- Lightning Talk大会
 - ・ スタッフ間交流促進のため、発表時間5分のLightning Talk大会をテーマ不問で開催した。このLightning Talk大会では、スタッフ各々の興味の対象や技術、個人の『人となり』を知ることができ、スタッフのコミュニケーション機会を増進した。特に福岡国際会議場でのLightning Talkでは学生からの積極的な参加があり、学生の経験としても有益だった。
 - ・ JR博多シティ 9F Room 1
 - ✓ 2/28 10:30-12:30
 - ✓ 15本 (社会人10人、学生5人)
 - ・ 福岡国際会議場 4F 404
 - ✓ 3/6 14:00-16:30
 - ✓ 14本 (社会人16人、学生6人)
- スタッフパーカーの制作
 - ・ ネットワークチームでは専用のスタッフパーカーを制作し着用した。スタッフパーカーは期間中ネットワークチームの制服としての役割の他、スタッフの連帯の証として機能した。



ネットワークチームパーカー

課題

課題(1) 運用面

- ネットワークの運用に関して、人的リソースの配分や必要なスキルの明確化、運用に用いるツールの選択と使用方法の明確化、それらを用いた運用のフロー化などを、会期の開始までに全て準備することができなかった。
 - ・ あるカンファレンスネットワークの運用を複数の組織から集まったメンバで行う場合、各メンバの背景となる技術スキルやそのメンバの普段の環境により素地となるものが異なる。
 - ・ カンファレンスネットワークに求められる質を定義にするとともに、その質を会期中維持するためのスキルの洗い出しやスキルの平滑化、運用手法の根本を議論し運用ポリシーの骨子を明確化することは、そのカンファレンスネットワークを安定的に運用するために重要
- 来場者全員に対して情報の周知を行う仕組みがなかったため、メンテナンス情報などを来場者に対して効果的に周知することができなかった。

課題(2) 技術面

- 会場ネットワークからインターネット上の特定のコンテンツを閲覧したとき、本来であればそのコンテンツがネットワーク上の近いサーバーから適切に配信されるが、ネットワーク上遠いサーバーから配信されたり、適切なコンテンツが閲覧できないような事象が発生した。
 - これは、APRICOT用として割り当てられているIPv4アドレスが、IPv4アドレスの登録情報(whois)はオーストラリアのものとして登録されていたこと、また、以前マレーシアや香港のAPRICOTで使われたIPv4アドレスだったことから、**CDN事業者やコンテンツ配信業者が持つデータベース上では日本もしくは福岡以外で利用されているIPv4アドレスと判断されたため**と推測される。
 - このように、時期によって物理的位置が大きく変化するようなIPv4アドレスを使用する際はIPv4アドレスの地理的な位置情報とコンテンツ配信の関係に対して注意が必要
 - **具体的な対応はそのコンテンツを配信する事業者毎に異なる**と思われる。

課題(3) 技術面

- 無線LANのトラブルについて、ホットステージや会期中に全てを解決することができなかった。無線LANでトラブルが起きた場合、国コードの違いなどにより、事象を再現させることが非常に難しい場合が多いため、効果的なトラブルシューティングを行うためにはツールや手法の充実が必要と思われる。

APRICOT・APAN 2015

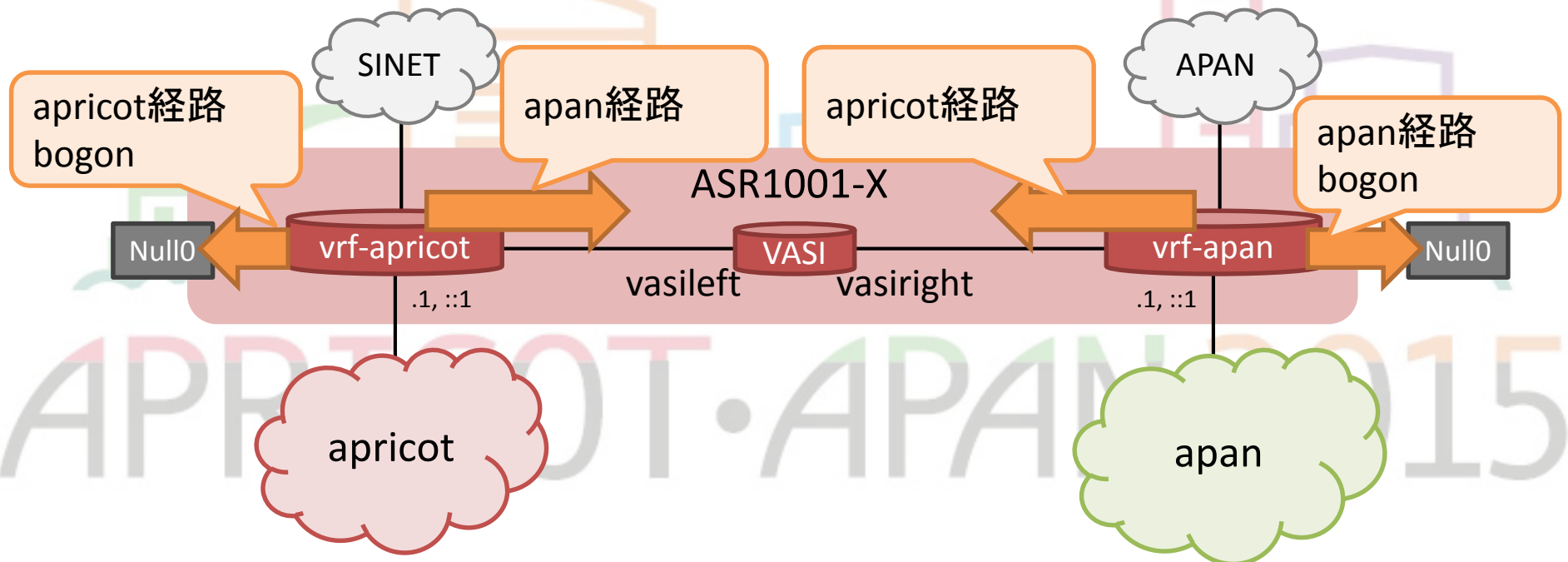
課題(4) 教育面

- 次世代のエンジニアの育成として期間中は後進の教育に取り組み、その成果は十分なものがあつた。学生からの感想として、技術的なスキルの向上のみならず、インターネットやネットワーク技術、業界そのものへの興味が深まったなどの点が挙げられた。
- しかし、学生の教育という観点でみた会期中の取り組みは、十分ななものではなかった。より効果的な取り組みという点では学生以外のスタッフを含め、以下の点に留意すると良いと思われる。
 - ・ 会期中における参加者とのコミュニケーションを促すような取り組み
 - ・ インターネットやコンピュータネットワークへの理解が深まるような取り組み
 - ・ スタッフ間でのテクニカルな交流を深めるような取り組み

付録：ネットワーク設計のポイント

ルーティング設計

- apricotセグメントとapanセグメントを分離し、VRFでそれぞれ独立してルーティングする
 - ・ 両セグメント間の通信をローカルで行うために、VASIを使って、VRF間ルーティングを行う
- Ping-Pongを防ぐため上流から受け取った経路はNull0にルーティングする
- Bogon経路はNull0にルーティングする



GWルータでのVRF/VASIの設定例

```
vrf definition vrf-apan
rd 7606:7606
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
vrf definition vrf-apricot
rd 2907:2907
!
address-family ipv4
exit-address-family
!
address-family ipv6
exit-address-family
!
interface Port-channel1.1501
description apricot-external
vrf forwarding vrf-apricot
!
interface Port-channel1.1502
description apan-external
vrf forwarding vrf-apan
!
interface Port-channel2.144
description apricot-wireless
vrf forwarding vrf-apricot
!
```

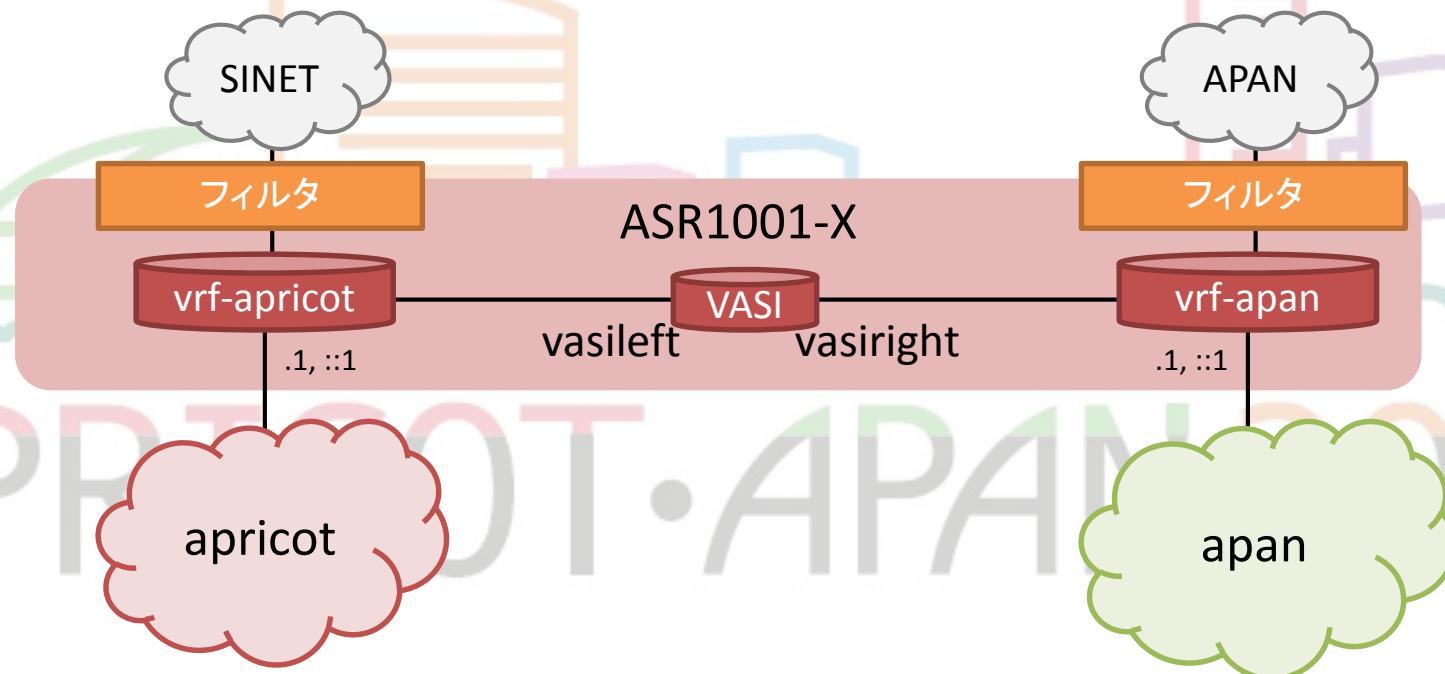
```
interface Port-channel2.1364
description apan-wireless-wired
vrf forwarding vrf-apan
!
interface vasileft1
vrf forwarding vrf-apricot
ip address 192.168.0.1 255.255.255.0
ipv6 address apricot-v6-prefix::/64
ipv6 address apricot-v6-prefix::1/64
no keepalive
!
interface vasiright1
vrf forwarding vrf-apan
ip address 192.168.1.1 255.255.255.0
ipv6 address apricot-v6-prefix:0:1::1/64
no keepalive
!
ip route vrf vrf-apan apricot-v4-prefix vasiright1
ipv6 route vrf vrf-apan apricot-v6-prefix vasiright1
!
ip route vrf vrf-apricot apan-v4-prefix vasileft1
ipv6 route vrf vrf-apricot apan-v6-prefix vasileft1
```

GWルータでのNull0ルーティングの設定例

```
ip route vrf vrf-apan apan-v4-prefix Null0 254
ip route vrf vrf-apricot apricot-v4-prefix Null0 254
!
ipv6 route vrf vrf-apan apan-v6-prefix Null0 254
ipv6 route vrf vrf-apricot apricot-v6-prefix Null0 254
!
ip route vrf vrf-apan 10.0.0.0 255.0.0.0 Null0 254
ip route vrf vrf-apan 100.64.0.0 255.192.0.0 Null0 254
ip route vrf vrf-apan 169.254.0.0 255.255.0.0 Null0 254
ip route vrf vrf-apan 172.16.0.0 255.240.0.0 Null0 254
ip route vrf vrf-apan 192.0.0.0 255.255.255.0 Null0 254
ip route vrf vrf-apan 192.0.2.0 255.255.255.0 Null0 254
ip route vrf vrf-apan 192.168.0.0 255.255.0.0 Null0 254
ip route vrf vrf-apan 203.0.113.0 255.255.255.0 Null0 254
!
ip route vrf vrf-apricot 10.0.0.0 255.0.0.0 Null0 254
ip route vrf vrf-apricot 100.64.0.0 255.192.0.0 Null0 254
ip route vrf vrf-apricot 169.254.0.0 255.255.0.0 Null0 254
ip route vrf vrf-apricot 172.16.0.0 255.240.0.0 Null0 254
ip route vrf vrf-apricot 192.0.0.0 255.255.255.0 Null0 254
ip route vrf vrf-apricot 192.0.2.0 255.255.255.0 Null0 254
ip route vrf vrf-apricot 192.168.0.0 255.255.0.0 Null0 254
ip route vrf vrf-apricot 203.0.113.0 255.255.255.0 Null0 254
!
ipv6 route vrf vrf-apan 2001:DB8::/32 Null0 254
!
ipv6 route vrf vrf-apricot 2001:DB8::/32 Null0 254
```

GWルータでのセキュリティ

- 参加者がグローバルIPアドレスを利用するため外部から攻撃を受けないようにするために、対外接続部のin方向にフィルタを設定する
 - NetBIOSなどのWindowsに対する攻撃パケット
 - UDPアンプの攻撃を引き起こすパケット
 - 自分のPrefixからのパケット
- 送信元IPアドレスを偽装したパケットがインターネットに送られないように、対外接続部のout方向にフィルタを設定する



GWルータでのフィルタの設定例(1/2)

```
interface Port-channel1.1501
description apricot-external
ip access-group firewall-in-v4 in
ip access-group firewall-out-v4 out
ipv6 traffic-filter firewall-in-v6 in
ipv6 traffic-filter firewall-out-v6 out
!
interface Port-channel1.1502
description apan-external
ip access-group firewall-in-v4 in
ip access-group firewall-out-v4 out
ipv6 traffic-filter firewall-in-v6 in
ipv6 traffic-filter firewall-out-v6 out
!
ip access-list extended firewall-in-v4
remark DNS
deny    udp any any eq domain
remark NTP
permit udp any eq ntp apricot-server-v4-prefix eq ntp
permit udp any eq ntp apan-server-v4-prefix eq ntp
deny    udp any eq ntp any eq ntp
remark SNMP
deny    udp any any eq snmp
remark SSDP
deny    udp any any eq 1900
remark NetBIOS
deny    tcp any any eq msrpc
deny    tcp any any eq 137
deny    tcp any any eq 138
deny    tcp any any eq 139
deny    tcp any any eq 445
deny    udp any any eq 135
deny    udp any any eq netbios-ns
deny    udp any any eq netbios-dgm
deny    udp any any eq netbios-ss
deny    udp any any eq 445
remark Bogon
deny    ip 0.0.0.0 0.255.255.255 any
deny    ip 10.0.0.0 0.255.255.255 any
deny    ip 100.0.0.0 0.65.255.255 any
deny    ip 127.0.0.0 0.255.255.255 any
deny    ip 169.254.0.0 0.0.255.255 any
deny    ip 172.16.0.0 0.15.255.255 any
deny    ip 192.168.0.0 0.0.255.255 any
deny    ip 198.51.100.0 0.0.0.255 any
deny    ip 203.0.113.0 0.0.0.255 any
deny    ip 240.0.0.0 15.255.255.255 any
deny    ip host 255.255.255.255 any
remark MyPrefix
deny    ip apricot-v4-prefix apricot-v4-prefix
deny    ip apan-v4-prefix apan-v4-prefix
permit ip any any
!
ip access-list extended firewall-out-v4
remark FromFICC
permit ip apricot-v4-prefix any
permit ip apan-v4-prefix any
permit ip apricot-external-v4-prefix any
permit ip apan-external-v4-prefix any
remark AllDeny
deny    ip any any
```

GWルータでのフィルタの設定例(2/2)

```
ipv6 access-list firewall-in-v6
remark DNS
deny udp any any eq domain
remark NTP
permit udp any eq ntp apricot-server-v6-prefix eq ntp
permit udp any eq ntp apan-server-v6-prefix eq ntp
remark SNMP
deny udp any any eq snmp
remark SSDP
deny udp any any eq 1900
remark NetBIOS
deny tcp any any eq msrpc
deny tcp any any eq 137
deny tcp any any eq 138
deny tcp any any eq 139
deny tcp any any eq 445
deny udp any any eq 135
deny udp any any eq netbios-ns
deny udp any any eq netbios-dgm
deny udp any any eq netbios-ss
deny udp any any eq 445
remark Bogon
deny ipv6 host :: any
deny ipv6 100::/64 any
deny ipv6 2001:DB8::/32 any
remark MyPrefix
deny ipv6 apricot-v6-prefix apricot-v6-prefix
deny ipv6 apan-v6-prefix apan-v6-prefix
permit ipv6 any any
!
```

```
ipv6 access-list firewall-out-v6
remark FromFICC
permit ipv6 apricot-v6-prefix any
permit ipv6 apan-v6-prefix any
permit ipv6 apricot-external-v6-prefix any
permit ipv6 apan-external-v6-prefix any
remark AllDeny
deny ipv6 any any
!
```

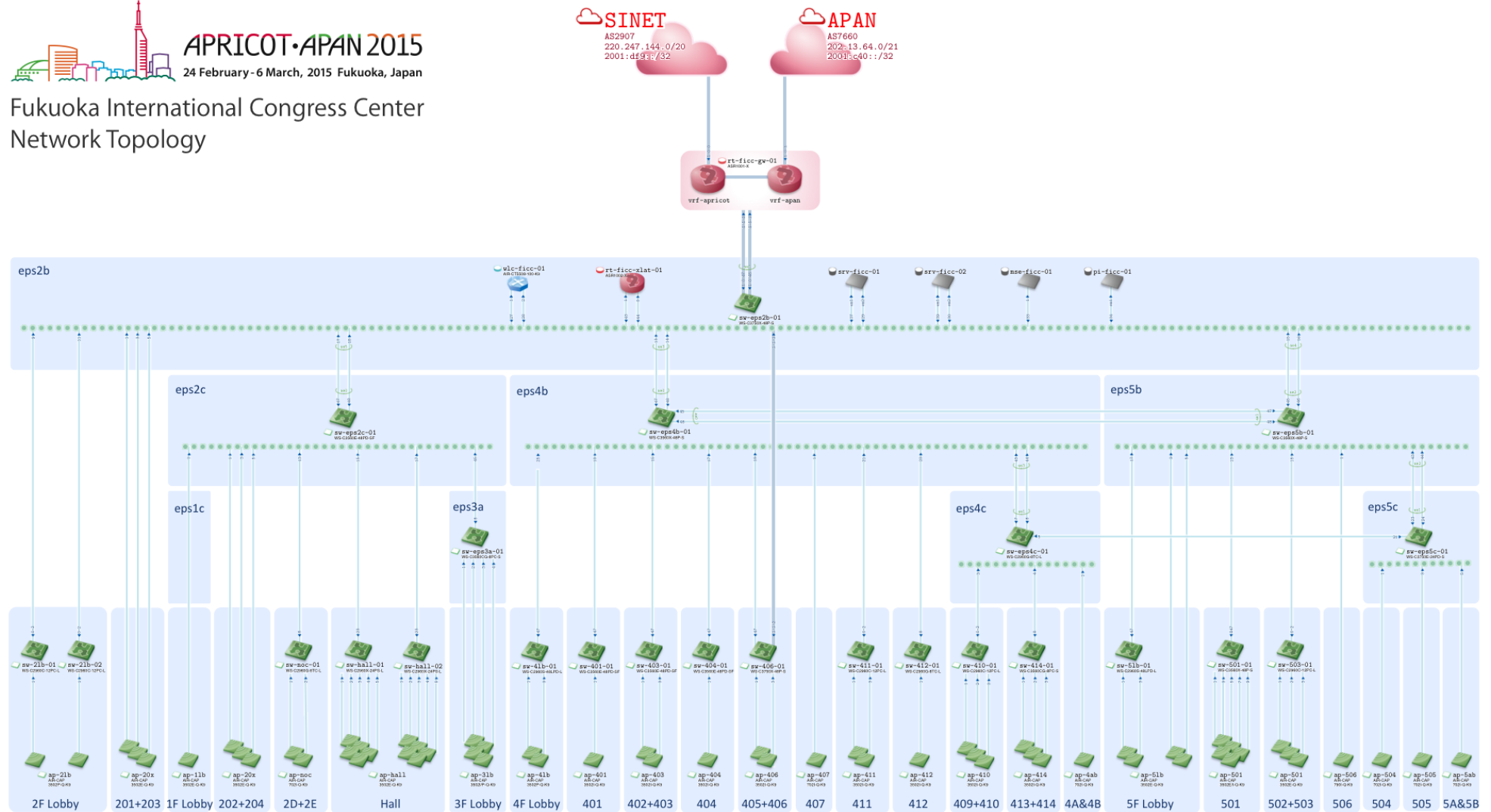
L2スイッチ24台のバックボーン



APRICOT-APAN 2015

24 February - 6 March, 2015 Fukuoka, Japan

Fukuoka International Congress Center
Network Topology



L2ネットワークの設計

- GWルータより下のネットワークはL2フラットで構成する
- スイッチ間は
 - ・ RSTPでループ防止・冗長化
 - ・ 利用する全VLANをtaggedで通す
- バックボーンのコア 6 台の機器間は
 - ・ 可能な限りリンクアグリゲーションで冗長化
 - ・ 可能な限りループ構成で冗長化
 - ・

APRICOT・APAN 2015

L2スイッチでのセキュリティ

■ 野良(Rogue) DHCP/DHCPv6/RA対策

- ・ NOC管理外の端末がDHCP Discoverに応答したりRAを吐いたりして、来場者のトラフィックを不正に吸い込む攻撃を防止する
- ・ IPv6フィルタに対応していないスイッチはその上流のスイッチで設定する

■ L2ループ対策

- ・ L2ループによるBUMストームによりネットワークの帯域が消費されることを防ぐ
 - ✓ BUM=Broadcast + Multicast + Unknown Unicast

L2スイッチの設定例

```
spanning-tree mode rapid-pvst
spanning-tree portfast bpdupfilter default
spanning-tree extend system-id
!
interface GigabitEthernet0/1
  description ap-407-01
  switchport trunk native vlan 99
  switchport trunk allowed vlan 10,51-
55,99,144,152,1364
  switchport mode trunk
  ip access-group dhcp-guard in
  ipv6 traffic-filter ra-dhcpv6-guard in
  spanning-tree portfast
  spanning-tree bpdupfilter enable
!
interface GigabitEthernet0/2
  description apan-wired
  switchport access vlan 1364
  switchport mode access
  ip access-group dhcp-guard in
  ipv6 traffic-filter ra-dhcpv6-guard in
  storm-control broadcast level 10.00
  storm-control multicast level 10.00
  storm-control unicast level 10.00
  storm-control action shutdown
  storm-control action trap
  spanning-tree portfast
  spanning-tree bpdupfilter enable
!
interface GigabitEthernet0/7
  description backbone
```

```
switchport trunk allowed vlan 10,51-
55,99,144,152,157-159,1364,1366
switchport mode trunk
spanning-tree cost 1000
!
ip access-list extended dhcp-guard
deny  udp any eq bootps any eq bootpc
permit ip any any
!
ipv6 access-list ra-dhcpv6-guard
deny icmp any any  router-advertisement
deny udp any  eq 547 any  eq 546
permit ipv6 any any
```

無線LANの設計

- トラフィックをローカルスイッチングできるようにFlexConnectを使用
 - ・ 通常はCAPWAPでWLCまでトンネルされるが、WLCの帯域が1Gしかなかったため
 - ・ mgmt VLANをNative VLANとして通す
- 周波数帯の仕様の違う色々な国の端末が接続するため、2.4GHz帯と5GHz帯を明示的に別のESSIDで提供
 - ・ 国内であれば同一ESSIDでBand Selectを有効にするのが良い
- APごとの周波数帯と電波強度は自動調整
- フロアごとにAP Groupを設定し、非常時に柔軟にコンフィグを変更できるように備える