

AIRHEADS通信

vol.

80

企業のVLAN運用、その実態は？ 「NO MORE VLAN」座談会【前編】

平素より「Airheads通信」をご愛読いただき誠にありがとうございます。
パートナー営業本部の川俣です。

昨年生まれた長女と今年6歳になる長男と休日を過ごすのが楽しい今日この頃です。

先日も子供たちの喜びそうなスポットを検討した結果、
長男の希望をかなえるべく“水族館”へ。

最近は、動物の自然な生態が体験できるよう配慮されており、
回遊型の水槽で餌も自然なタイミングで与えるため、
魚も生き生きと泳いでいるように感じられます。

そして子供たちが楽しみにしているのが
イルカのショーです（あ、シャチだったかな...）。

ダイナミックな彼らが躍動するさまは、やっぱり見ごたえのあるもの。

写真の通り、私も含めて周りは**みんなズブ濡れ**だったんですけど。



体を動かせば避けられる位置にいたものの、
結果として体が言うことを聞かず...間違いなく歳だと思いたい。

いよいよ令和という新たな時代が始まります。
Arubaでは、IEEE802.11axがReadyなAPが登場するなど、
2019年も新たなソリューションを続々と日本に展開する予定です。

寄る年波には勝てないことは重々承知していますが、
頭は柔軟に、フットワークは軽く、
令和の始まりを駆け抜けていきたいと思えます！！

ご期待ください！！

企業のVLAN運用、その実態は？ 「NO MORE VLAN」座談会【前編】



今回は、普段HPE Arubaのソリューションを扱っているインテグレーションの皆さんにお集まりいただき、大輔がモデレータとなって座談会を開催！昨今のネットワーク事情をはじめ、VLAN運用の実態、そして「NO MORE VLAN」に関するご意見などを伺った。



大輔（だいすけ）

A市役所のIT推進室から転職して、現在は世界的なお菓子メーカーであるD&W社の情報子会社に転職。ネットワーク統括部のメンバーとしてグローバルなIT基盤の運用管理を担う。実際にはITの知識があまりなく、いつも周囲に頼ってばかりいる。



美咲（みさき）

大輔と同じくA市役所職員から転職した、もと大輔の部下。大輔が所属する情報子会社の親会社にあたる、グローバル本社のD&W社システム企画部に所属。社会人歴はわずか3年ほどだが、平成生まれのデジタルネイティブ世代として、ITの知識は豊富。

【座談会にご参加いただいた方】



SCSK株式会社
プラットフォームソリューション事業部門
ITエンジニアリング事業本部
エンタープライズ第三部
技術第二課
課長
碓井 雄一郎

エンタープライズの顧客を中心にソリューションを提供するインテグレータであるSCSK株式会社にて活躍する、アカウント中心のエンジニア。ファイアウォールやロードバランサーも含め、Aruba以外のソリューションも数多く手掛けている。



伊藤忠テクノソリューションズ株式会社
流通・EPビジネス企画室
ネットワークビジネス推進第2部
ネットワークビジネス推進第6課
課長
成田 宜孝氏

エンタープライズ向けに商品を扱うインテグレータである伊藤忠テクノソリューションズ株式会社にて、ネットワークやセキュリティ関連の各種ソリューションを提供するエンジニアとして活躍。Arubaをはじめ、他社のネットワーク製品も取り扱う。



大輔さん、今日って座談会に参加するって聞いてますよ。



そうなんだよね。実はディーンが参加するはずだったのに、飲みの席が苦手だった。そこで僕に白羽の矢が立ったみたい。



まあ、お酒も雑談も好きな大輔さんならうってつけじゃないですか。で、どこでやるんです？



どうやら、大島にあるHPE 本社でやるみたい。前も行ったことのある、お酒が飲める8階のところ。



ああ、そうなんです。何をテーマにやるんです？



えっと、ちゃんと聞いてなかったな...
ああ、もう時間が！！じゃあ行ってくるねー！！



すみません、遅くなりまして。おお、もう飲み始めてますね。今日は...ええと、Arubaが提唱するコンセプト「NO MORE VLAN」をテーマに、マイクロセグメンテーションに関する取り組みや今のユーザー動向についての座談会、ということで...ええと合ってますよね。



なんか私が場を回す感じになっていますが、よろしくお願ひいたします。では最初に、今のネットワークにおけるトレンドについてお聞きしたいんですけど。最近はどうなお話が商談のなかで出てきますか？



クラウド利用が広がるなかで、WANのトラフィックをローカルブレイクアウトしたいという要望をよく聞きますね。インターネット回線が潤沢に使えるわけではないなかで、拠点ごとに太い回線にするのはコスト的に厳しい。当然ですが、お客さまはお金に対してシビアですから。



確かにOffice 365とかのトラフィックを直接流す話はよく出てきます。結局WANのトラフィックが増えているものの、1Gbpsまでアクセス回線を増強するとコストが大きく膨らんでしまう。本社に集中させて1つの回線を太くするよりも、各拠点で分散させてコストを押さえる環境を望むケースが多い印象です。



やっぱりユーザーの立場だと、コストは社内でも言われますからねえ。ただ、回線コストはそこまで意識してなかった。回線ってそんなに高いんですね。



日本のお客さまは高額だとよくおっしゃっていますよ。コスト面から100Mbpsといった帯域で何とかしようとするなかで、太くしましよと言ってもなかなか難しい。しかし、WANに比べてLANはとても速くなっており、無線もギガビットの時代ですからね。



無線の高速化に合わせて、有線側の増強などはいかがですか？
結局ボトルネックが有線部分になってしまうと元も子もないような。



でもそこまで大きな潮流にはなっていない印象です。
これからなのかもしれません。



ちょうど知り合いの会社が光ファイバの導入を検討していたな。
10GbEの世界になると光ファイバを使ったほうが安定するからって。



メタルに比べて光ファイバのほうがコスト高になるため、今のタイミングで光ファイバなどへの移行はそれほど話として出てきていませんね。
結局RJ45のインターフェースで使える10GBASE-Tを駆使して何とかしているケースが多く見られます。



メタルの品質も良くなってきているので、何とかメタルで構築を、というお客さまが多い。光ケーブルやトランシーバなどがかなり高額で、圧倒的にコストの安いメタルが好まれているのが現実です。



サードパーティのトランシーバであれば安価に調達できるかもしれませんが、メーカー保証外になってしまう。どうしても光モジュールって難しいんですよね。



そうか、もっと扱いやすくなっていると思ったんだけどな、光ファイバ。
では、他にも話題ってありますか？



ネットワークの可視化についても要望が強い。拠点から直接WANに抜けてしまうとユーザーの使い方が分からなくなり、セキュリティや管理の視点からトラブルは見えるようにしておきたいと考える管理者が増えています。今だとAirWaveを入れたいというお客さんも増えています。



有線の時代を生きてきた人からすると、やっぱり可視化しないと不安があるというのわかります。AirWaveは確かに好評で、単純に可視化できると楽しいし、一杯つながっているのを見ると、なぜかうれしくなるものです。



セキュリティの話題も多いですね。仮想環境のなかでセキュリティをかけるといったマイクロセグメンテーションはもちろん、L4のファイアウォールだけで安心していたお客さまも今はIPSを導入して機能強化を図るケースも。侵入防御や脆弱性対策なども含めた多層防御が求められている状況です。



セキュリティについては、Fortinetやパロアルトを扱う部署のメンバーから、ArubaとAPI連携してセキュリティ強化につなげる話題も出てきています。すでに社内ではデモをやったりもしているのですが、それをサービス化して収益化できるようなチャレンジを今始めているところです。



無線に関する話題はいかがです？



ファームウェアをアップグレードすればIEEE802.11axに対応できるAP-515をすでに発注いただいているお客さまもいらっしゃいますよ。日本で技適（技術基準適合証明）が通り次第、お客さまにも展開していく計画です。



じゃあここで話題を変えて、NO MORE VLANにつながるVLAN運用について。一般的な企業においては、どんな状況で運用されているのでしょうか。



現実的にはネットワークセグメントの単位がVLANで決まっている形となっており、ある意味ネットワークの単位がVLANといっても過言ではありません。もうVLANありきでネットワークが設計されているのが実態です。



VLANがセグメントの単位になっていると。そんな状況なんですね。確かにVLANの歴史は長いですからね。



実際には我々が設計するよりも、お客さまのほうからVLANを使ってセグメントをこの範囲で設定してくれと依頼を受けることがほとんど。一度設定したものを後で再設計するというケースはあまり発生していませんね。



まあ、うちもそんなに変更していないような気も。通常だと、企業全体でどの程度のVLANが設定されていますか。



通信事業者であれば、4094個のVLANセグメントではとても足りませんが、エンタープライズではそこまで使い切ることもありません。最近ではQ-in-QやVXLANなどで拡張されているVLANですが、一般企業で1000を超えることはほとんどありませんよ。



1拠点でも数個程度、用途よりも場所や部署でセグメントを変えているケースが多く見られます。用途でいえば、業務用とゲスト用、そして特殊用のVLANといったものものが一般的な印象です。病院の例では、レントゲン用のVLANといった用途ではっきり区切るケースもあることはありますが、あくまでレアケースです。



以前ISP事業者を顧客として担当していたころは、一般家庭ごとにVLANを切るには数が足りないため、全世帯同じセグメントで設定し、家庭にあるケーブルモデムに対してセンター側からポリシーを投げる形でコントロールするという、VLANという概念がない業界でした。実はClearPassを使ってセンター側からルールをスイッチやAPに展開して制御するというArubaのNO MORE VLANの考え方に近いのかもしれないですね。



お聞きしていると、VLANが当たり前に使われている印象ですが、運用のなかで課題になるケースは少ないんでしょうか。例えばVLANのメンテナンスって大変な印象ですけど。



最初にVLANを設定した後は、追加や削除に関する依頼はほとんどありません。



あるとすれば、エッジ側でポート追加する程度でしょうか。



そもそも日本ではネットワークエンジニアが足りておらず、インフラの管理だけで精一杯という側面も。ロールベースでアクセスポリシーを運用すると大変な面もあるため、一度ACLをVLAN単位に設定し、そのあとはほとんどいじらないというのが日本の運用スタイルなのかもしれません。



そうですね、聞いているお話だと、VLANそのものに苦労されているわけではないようです。



ここでNO MORE VLANというメッセージについて、どんな印象をお持ちですか？VLANでの運用を楽にするだけでなく、セキュリティ強化につなげるためのマイクロセグメンテーションを表すコンセプトだと考えていますが。



メッセージからは、VLAN1個で全てコントロールできそうな印象を受けます。先進的なお客さまからは、とにかく何ができるのかが分からないので、大風呂敷を広げてやってみましょうという声をいただいていますね。



我々も提案は行っており、次はロールベースでユーザーを制御するといった“SDN的な世界”への期待はありますね。でもなかなかハードルは高い部分があります。



どのあたりがハードルの高さにつながるのでしょうか。



私が感じているのは、VLANがあまりに浸透しすぎてしまって、論理的なセグメントを物理的な環境を意識せずとも好き勝手に分割できるという便利な仕組みに慣れてしまっています。そこから脱却することがそもそも難しい気も。



私の場合は、例えばデバイス単位でロールを決めるとしても、本当にたった1つのVLANで大丈夫なのかという懸念がお客さまのほうにもあります。ループした時どうするのか、ブロードキャストのパケットはどうなるのかといったことをいろいろお客さまと議論する場面がありますね。



いろいろトライしていかないと分からない段階ということでしょうか。



実際には上位のファイアウォールで実行している仕事もあるわけで、それらを全部やめて無線コントローラにやらせるのかといった深い話になってくると、じゃあDynamic VLAN程度にしようとか、VLANを使いながら一部だけロールを割り当てるとか、いろいろ落としどころを見つけていく。理想論としてはありますが、現実はまだそこまでいかない印象です。



概念的にワードが強すぎるんじゃないかな、NO MORE VLANって。



印象が確かに強い。イラストもVLANに手を振っているんで、どうしてもVLANが減らせるのではという期待は持たれますよ。

～次回に続く～

5月28日開催！ Airheads Tech Talk Live!

生体認証や機械学習を使った振り分析、最新セキュリティから
IoT時代の有線LANソリューションまで、デモを交えてわかりやすく解説

https://connect.arubanetworks.com/japan_airheads_tech_talk_live

Aruba製品を実際に触れるハンズオントレーニング、Airheads スクール開催中！
(東京、名古屋)

https://f-vr.jp/hpe_aruba/eng/mail_reg/airheads_ho/seminar_new_form.cgi

バックナンバー

▼ Vol.1~49

▼ Vol.50~79

バックナンバーは、下記サイトにて公開しております。

<https://www.hpe.com/jp/ja/networking/mailmagazine.html>

※最新版が掲載されていない場合もありますが、随時掲載して参りますので後日ご確認ください。