aruba
a Hewlett Packard Enterprise company

airheads COMMUNITY

AIRHEADS通信

vol. 81

マイクロセグメンテーションは企業に根付くの？「NO MORE VLAN」座談会【後編】

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山脇です。

今年は新元号への移行に伴って大型連休となったゴールデンウィークですが、
皆様、どのように過ごされたのでしょうか。

混雑が苦手なため、ゆったりと連休を過ごすことを決意したものの、
せっかくの休みにずっと家にいるのももったいない！
ということで、歌舞伎でもみようかと思いたったのですが、

混雑MAX！！

当日販売している幕見席のチケットを購入しようと歌舞伎座には向かったものの
海外の観光客の方でごった返しており、あまりの混雑に逃げ帰ったわけで。

でもすぐに撤退してしまってはあれなんで、
歌舞伎座のある晴海通りを皇居に向かって歩きながら、
普段いかない国会議事堂なんて見学してみたりして。

まあ、それはそれで有意義な休日ではありました。

そうそう、ちょうど元号が変わるタイミングなので
ここ数年収集している御朱印帳をもらいに行ってきました。

これはこれで混んでたんですけどね…

しかも、せっかくなら平成最終日と令和初日のものをゲットしたいところですが、
記念すべきタイミングを“あえて”避けるのが私らしいということで。

御朱印帳はすでに3冊目になり、ある意味ライフワークとして定着しつつあります。

神社巡りそのものを楽しむだけでなく、友達と一緒に散歩しながら
ランチすることの楽しみも、御朱印集めが続いている大きな原動力なのかもしれません。

皆様も御朱印集め、いかがでしょうか？

素敵な御朱印、レアな御朱印をゲットされた方、
ぜひ私に自慢してください！！

マイクロセグメンテーションは企業に根付くの？
「NO MORE VLAN」座談会【後編】

前回に引き続き、HPE Arubaのソリューションを扱っているインテグレータの皆さんを交えた座談会レポートをお届け！
今回は、ClearPassや「NO MORE VLAN」に関する実用性、そしてホワイトペーパーを読んだ感想などをお聞きした。

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。

【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。

すっかり夜も更けてきましたが…前回に引き続き、皆さんよろしくお願いいたします。VLANにまつわる運用の課題を解消する、コンテキストに基づいてセキュリティポリシーを適用するNO MORE VLANに必要な認証基盤について、まずはお聞きしたいのですが。もっと言えば、ArubaのClearPassについて端的にお聞きしたいですね。

NO MORE VLANの実装に関していえば、Radiusのような既存の認証基盤でどこまでできるのか、ClearPassを入れるとどこまでできるようになるのかということは、よく話題になりますね。

確かに、どちらの認証であってもロールベースでの制御は可能なのがArubaの特徴の1つですからね。

ただし、既存環境でIEEE802.1XとTLSで作り込んでいるものを全てClearPassに移せるのかというと正直難しい。それでも私のお客さまは、できればClearPassで全て制御したいと言っています。

それはやっぱり大変なのでしょうか。

確かにVLANでACLを管理するのは大変なのですが、長年の歴史の積み重ねから慣れてしまっているのが実態です。その意味でも、ClearPass自体への慣れは必要だと思っています。

日常的に触れるものであればいいですけどね。年に1度の組織改編の時だけ変更するレベルだと、確かに慣れるまで時間がかかっちゃうんだろうなぁ。

まあ運用そのものをアウトソースする企業は多いですからね。
ただし、お客さまのなかには、ClearPassを入れてもいいが、運用はしっかりと考えられるのかというご指摘をいただきます。本来は運用が楽になるために入れるはずが、従来よりも運用にコストがかかってしまっては本末転倒ですからね。

コストの面では当然ですがメリットを出していく必要があると。

無線導入はコスト面でも分かりやすく効果が示せるから納得いただきやすい。
でも、認証などは見せ方も難しく、エンドユーザーがそこに効果を感じていただくかは微妙で、足踏みするお客さまもいるのが実態です。

費用対効果は確かに大事ですもんね。

認証をやることだけでも敷居が高いお客さまもいます。
クライアントに証明書をどう配布するのかといったことから課題になるため、PEAPなどが流行っているんだと思いますよ。PEAPとMac認証を組み合わせようとすると、今度はMacアドレスの管理はどうするの？ということにも。そういった状況の現場も少なくありません。

認証を含めてセキュリティに関しては、特別に自社に実害がなければ比較的後回しにされてしまう傾向はありますからね。

どこまで行ってもコストは大事なんだということですね。

前回からお話を伺っていると、やはりVLANありきで慣れてしまっている関係上、すぐにNO MORE VLANのコンセプトに基づいたマイクロセグメンテーションの世界が描けるわけではなさそうですね。

やっぱり事例が必要だと思いますよ。これからだと思いますが、運用面でもコスト面でも効果が示せる事例が望まれます。アプローチとしては、働き方改革など別のお題目と絡めて効果を示していくことが大事だと思います。単にNO MORE VLANだけでは厳しいのが正直なところです。

決して悪いコンセプトではないのですが、正直に言えばNO MORE VLANをコストに紐づけるのは難しいのが本音です。メリットを示すのであれば、やっぱりセキュリティではないでしょうか。お金をかけずともNO MORE VLANにするとメリットがあるように持っていけるとさらにいいのですが。

そういえば、NO MORE VLANのホワイトペーパーにコスト比較もありましたが。

あれはVLANの変更をどこまで頻繁に行うのかによってコストメリットが出てくる試算ですよね。あんまりVLAN変更しない場合は、なかなか厳しいところです。正直、私はあまり構築してからの追加や変更はほとんどありません。

うちの会社って結構バーチャル組織というか、プロジェクト単位にいろんな案件が動くので、部署でVLANを設定すると大変なんですよね。
1人がいろんな肩書を持っているケースが多いので。

確かにその場合は便利かも。プロジェクトAが動き出したら、このサーバーにアクセスできるようにするといった柔軟な制御が求められますから。
まあ、実際に作るのは大変ですが、お客さまからも求められてる部分です。

この前も、社外の人がプロジェクトに入ってきたんですけど、単なるゲストというよりも、もっと深い層まで社内環境にアクセスさせる必要があったんですよ。
確かにそのときは特別なVLANを作ったな、そういえば。

そんな時こそロールベースで割り当てるということが役立つし、プロジェクトが終わり次第その設定を解除することもできるようになる。でも、ユーザー情報だけでなく端末単位に制御したいよねとなると、これはこれで大変です。

確かにマイクロセグメンテーションの世界で考えれば、端末単位に制御できるというのがありますもんね。やりたいと言ってくる方もいないとは限らない。

情報システム部門でキッティングしたPCなら把握できていますが、勝手にPCを購入できる会社もなかにはあります。申請されてきた端末が正規のものなのか、証明書はどう入れるのかといった、いろんなことを考えて運用に乗せていくとなると、運用する側からすると大変ですよ。

証明書を入れるならClearPass Onboardって機能をうちは使っていますね。

すでに購入していればよいのですが、新たなライセンスの購入では躊躇してしまうお客さまもいます。Arubaでやれることがたくさんあるのは理解していますので、コストとの兼ね合いでどこまでやるのか、取捨選択が求められます。

いろんな話が出ていますけど、これについても聞かないと。
NO MORE VLANのホワイトペーパーって読んでどうでした？

分かりやすいと感じましたが、ある程度Arubaを知っている我々だからかもしれません。本当のエンドユーザーの意見も聞いてみたいですね。

すでにArubaを導入しているエンドユーザーとしても、分かりやすかったと思っています。

しっかり図示もされていますし、誤解を招かないようスイッチでできること、他社のRADIUSサーバーでできることなど、きちんと情報が整理されて掲載されています。ちゃんと腰を据えて読めば分かるはずです。“なんでもできます”という資料ではなく、きちんと現実を見据えて書かれている印象を持ちました。

読んだ印象としては、まだここまでロールベースでの制御を追及している日本のお客さまは正直少ないでしょうね。でも競合製品含め、米国など海外ではそれなりに扱っているというのを聞いていますので、いずれという段階でしょうか。

米国などに3年ほど遅れて日本にやってくる、なんていうのはIT業界では言われていますが、これらマイクロセグメンテーションの世界はどう思われますか。

従業員単位まで詳細に制御することはなさそうですが、組織やグループ、プロジェクトなどの単位でACLを動的に制御するような仕組みは必要だと思っています。それでも、日本でではまだこれからでしょうね。まじめな日本の国民性もあるので、米国ほど細かくは制御しない可能性もありますが、読んでみて損はないかと。

今日は貴重なお時間をありがとうございました。今回はNO MORE VLANというコンセプトにおけるマイクロセグメンテーションの話題でしたが、他にも座談会でネタにしてほしいものってあります？

やっぱり実際にエンドユーザーに導入しているインテグレータ同士、こんな形で機能を実装したという事例が聞きたいですね。

私はネットワーク業界のエンジニアは今後何をして生きていくべきなのかという、もっと広義なテーマが希望です。若いエンジニアがどういう方向性を目指すのか、長年この業界にいる我々が何かの方向性を示してあげられるようにしたいですね。

想像以上にいろんなお話が聞けました。ありがとうございました！！

＝＝

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/enq/mail_reg/airheads_ho/seminar_new_form.cgi

＝＝

バックナンバー

▼ Vol.1~49
▼ Vol.50~80

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。