aruba
a Hewlett Packard Enterprise company

airheads COMMUNITY

AIRHEADS通信

vol. 78

「NO MORE VLAN」理解につながる ホワイトペーパー読解【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。

空気清浄機とアロマオイル「TEA TREE」の組み合わせによって
花粉症でやられた鼻の通りを快適にする術を身につけた、マーケティング部の井上です。

東京では、平年より数日早めとなる桜の開花宣言が3月21日に発表され、
本格的な春がやってくるタイミングを迎えました。

桜の開花とともに花粉症のムズムズも落ち着き始めているようで、
今年も何とか乗り切れそうだと胸をなでおろしているところです。

さて、先日ふと和菓子屋さんに立ち寄ったときの話。
暖簾をくぐると、普段見慣れない大きな物体が鎮座していてびっくり！！

なんと、折り紙でできた巨大な虎です。

まあ察しのよい方はすぐにピンとくるかもしれませんね、
和菓子で虎といえば“とらや”さん。

六本木にある「とらや 東京ミッドタウン店」の店内ギャラリーにて
企画展「ORIGAMI」なるものが開催されており、
折り紙の歴史や十二支になぞらえた折り紙作品が並べられていたのです。

会場の一角には、とらやだけに虎をつくるための黄色と黒の折り紙や
作り方の手順書などが用意されており、自由にチャレンジできる環境となっていました。

鶴ぐらいしか折ったことのない私ではありますが、せっかくなのでチャレンジを。

ま、何とか完成…といえるのか？

途中まではうまくいったのですが、頭の部分などはガイドを見てもチンプンカンプン、
結局私と同じく隣で戦いに挑んでいた妙齢のおじさまの器用な手先を盗み見つつ、
40分近くかけて何とか写真の通り完成となりました。

しっぽ、なんか違うんですけどね…

でも改めて折り紙を折ってみると、意外と集中できるもんですね！

黄色と黒の色紙2枚に、気づけば**40分**も使っているんですから。

貴重な体験でしたー。

「NO MORE VLAN」理解につながる ホワイトペーパー読解【前編】

これまで何度か紹介している「NO MORE VLAN」。この実態を分かりやすく紹介したホワイトペーパーを大輔が入手した！必要なコンポーネントや競合他社との違いに触れながら、コンセプトを具体的な実装に落とし込んだ本書について分かりやすく紹介。いよいよ2018年度も終わりを迎える美咲と大輔、来期に向けた活動にNO MORE VLANがつながるのか？

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。

ディーン

D&W社のシステム部門に在籍する留学生・インドネシア人。ネットワークやセキュリティのスペシャリストながら、日本の文化に傾倒、大輔や美咲よりも日本のカルチャーに詳しい。

いよいよ2018年度も終わりね。

お、どうしたの美咲くん、何かあったの？

先日上司との面談で2018年度の総括をしたんですよね。しっかり評価もいただいたので、来年度も頑張らないといけないなと改めて思いまして。

どんな評価だったの？

悪くない評価でしたよ。
来年度への期待も込めて、十分な評価をいただきました。

そうなんだ。で来年度はどんな目標を？

日々の運用負荷を減らしながら、より新しいテクノロジーを積極的に推進していこうと。
まあ詳しいところはいろいろあるんですけど、大枠はそんなところです。

具体的にはどのあたりが気になるところなの？

とにかくセキュリティを強化する一方で、運用負荷も軽減できるような仕組みづくりをやっていこうと考えています。

ソノ辺って、以前から話が出ている「NO MORE VLAN」は1つの方策だと思いマスよ。

ああ、従来のVLANに代わって、コンテキストなどによって端末を識別してポリシー適用する、あれね。

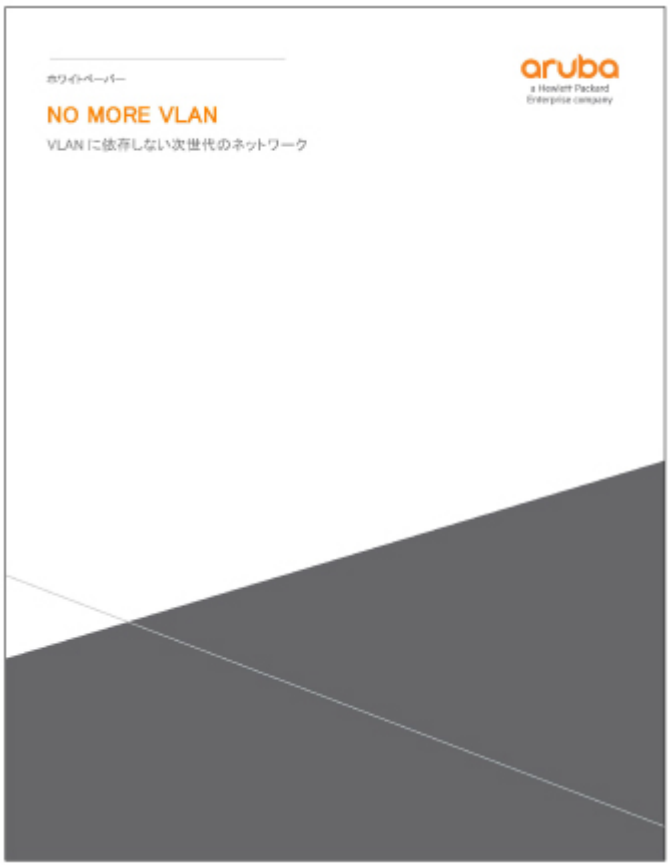
お、大輔さん、理解しているみたいじゃないですか、NO MORE VLAN。

いやね、実は昨日ホワイトペーパーをいただいてさ。ちょっと読んでみたの。

あ、そうだったんですね。いかがでした？

NO MORE VLANのコンセプトがよく理解できたよ。断片的な話が多かった印象だったので、ちゃんとまとまった資料が読めたのは大きいね。

それは大輔さんの理解力にも課題はあると思いますけど…。
実は私、まだ入手していないんですよね。ちょっと詳しく教えてくださいよ。



大きな章立てで見ると以下の通りだね。

「NO MORE VLANとは」
「NO MORE VLANを実現するアルバのソリューション」
「ロールの実装方法」
「シスコ社のソリューション〜TrustSec」
「シスコ社のソリューション〜DNA」
「アルバのソリューションの特長」

競合との違いはかなり意識されているようですね。

そうしたほうが分かりやすいし、ユーザーからしても知りたいところだと思うよ。

じゃあ少し詳しく教えてくださいよ。

まずはVLANの課題について触れながら、NO MORE VLANの特長について紹介していたな。ネットワークを見ている人からすると共感しやすいんじゃないかな。なかでもVLANは運用していても厄介だと感じるケースがあるからね。

どのあたりが課題なんでしょう？

最近はいろんな端末がアクセスするようになって、しかも固定席で使うというよりも社内も端末を持ち運んでその都度いろんな環境からアクセスしてくる。
それらを、スイッチのポートなどに紐づけて設定するVLANで管理しようとすると、そもそも難しくなってきているでしょ？

ビジネスのスピードも速いですし、数か月ごとに新たな組織に組み替える会社すらあるぐらいですから。もう1人が1つの役割とは限りませんからね。

確かに、名刺交換の時に複数枚の肩書を持った名刺をいただくことが増えてきた気がする。

そんな柔軟性を持った組織に合わせてVLANの運用をしていては、さすがに運用面で破綻しかねませんからね。

ソコで提唱されてイルのが「NO MORE VLAN」というコンセプトデス。
もうこれ以上VLANを増やさず、今の時代にマッチした形での高度な制御を行うことを目指したものデスね。

端的にいえば、どういうことなんだろ。

組織や物理的なポートに紐づいたVLANではなく、“誰が””いつ””何を””どこから””どのように”接続したのかというコンテキストを識別し、それに応じてポリシー、いわゆるロールを割り当てる仕組みということでしょうか。

細かく設定すれば、僕が業務時間内に自分の部署からアクセスしている場合と、業務時間外に出張先からアクセスしている場合をちゃんと識別して、アクセス可能なサーバを分ける、といった感じかね。

端末や人に依存した形でポリシーが適用され、ネットワーク機器からは独立した形で運用可能になりマス。さらに高度なものにナルと、Aさんと思しき人が時間外に個人情報を管理するサーバにアクセスしてイルと、普段の行動からそのアクセスが怪しいと自動検出できるようにもなりマス。

確かに実現したら便利なんだよね、それって。
全部入れ替えるタイミングがあればいいけどさ。

コンポーネントでいえば、ロールの割り当てやアクセス制御を行うClearPassをはじめ、APやスイッチなどAruba製のネットワーク機器が必要な部分はありマスが、Arubaの場合、構成するネットワーク機器を全て1つのベンダに統一する必要はないデスからネ。

そういう意味でいうと、部分的なネットワーク更改でも導入できるのはありがたい。古いネットワーク機器でも十分使えるものがあるからね。

そのあたりはArubaの特長でもあると思いますよ。

実際の動作概要もホワイトペーパー内にあったよね。

動作概要

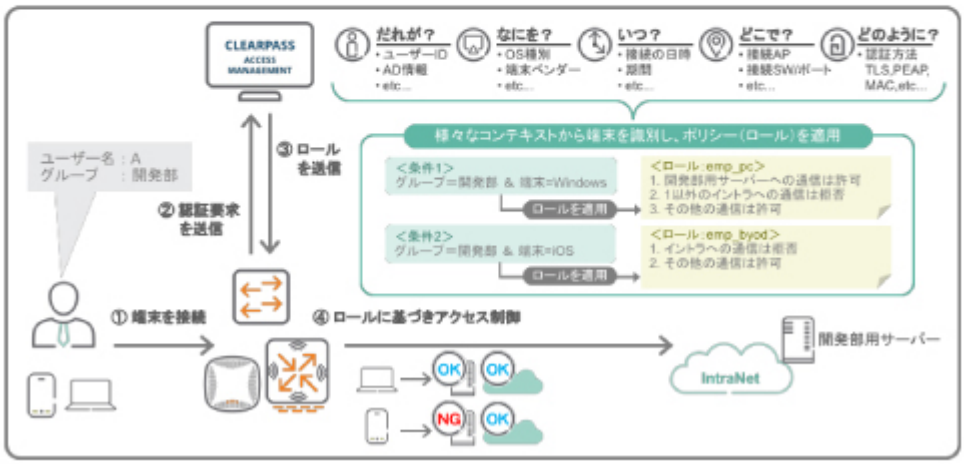
アルバのソリューションはとてもシンプルで、下記のフローで動作します。

① ユーザーが、端末を接続

② オーセンティケータ（端末からの認証要求を中継するAruba Switch/Mobility Controller）が、認証要求をClearPassへ送信

③ ClearPassが認証し、ユーザー/端末のコンテキストに基づいて指定されたポリシーをオーセンティケータへ送信

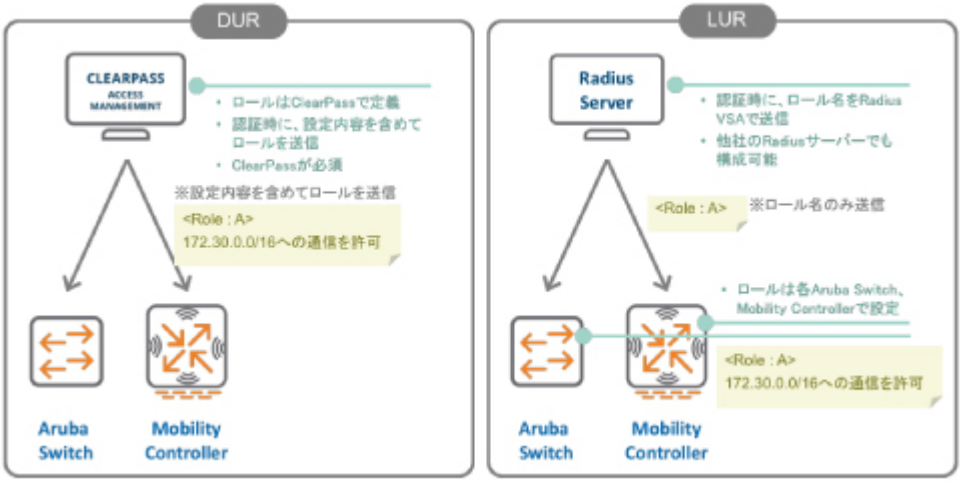
④ オーセンティケータが、受信したポリシーに基づきアクセス制御を実施



ああ、これですね。フロー的にはシンプルですよね。端末がアクセスするとClearPassが認証し、ロールを割り当ててアクセス制御を実行すると。

ソウなりマスね。

また、ロールの実装方法として、2つの方法もしっかり書かれているよ。
えーと、「DUR（Downloadable User Role）」と「LUR（Local User Role）」だね。



これって、ClearPassでロール定義を一元的に行うか、Radius Serverなどを使ってオーセンティケーター（スイッチやAP、コントローラ）それぞれに設定されたロールを実装するのかの違いですよね。

これってClearPass入れなくてもVLANから脱却した、ロールベースの制御が可能になるんでしょ。認証基盤なんて、複数メーカー指定のものが必要なものばかりだけど、ここも個別に投資せずに済むのはありがたいよね。

他にも、Mobility ControllerがアレばAruba APおよびAruba Switchの間でGREトンネルを確立してアプリケーション単位でのアクセス制御を行うコトで、端末ごとにセグメンテーションされたセキュリティを実装するコトが可能になりマス。このTunneled Nodeという仕組みについても触れていマス。

結構詳細に書かれていて、仕組みを理解するにはもってこいですね。

さらに理解を深めるには、競合他社との違いも理解したいところ。
ホワイトペーパーではその部分についてもしっかり触れていたな。

ソレについては次回紹介しまショウ。
Arubaにせよ競合他社にせよ、やりたいコトはネットワークにおける高度な制御によるセキュリティ強化と運用負荷の軽減ということデスからネ。

ちょっと私もダウンロードして改めて読み込んでおきます。
あそうだ、大輔さん。

なに？

大輔さんの会社も3月が決算期なので1年を終えることになるわけですけど、評価はどうだったんです？

そこ、聞いちゃう？いやー、いい評価もらっちゃってさ！

そうなんですか？本当なんでしょうね？

前にYoutuberとして紹介したうちの会社のお菓子がめちゃめちゃ売れたみたいでさ。インフルエンサーとしてもっと紹介して欲しいって！！

...それはプライベートの活動ですよね。会社の業務としては？？

いやー、まあそこはそれなりに。というか、まあ引き続き頑張ってよって。

結構漠然としていますね。目標とかってないんですか。

まあうちは情報子会社なので、大きな方針は美咲くんのいる親会社の意向に沿うことになるからねぇ。でもインフルエンサーとしての発信力を社内にも生かして欲しいってさ。今年はグループ会社向けの勉強会にも登壇するかも。うふふ♪

それは新たな展開！へー、ぜひ頑張ってくださいね。

来年度は、自分の個性を生かして前向きに頑張るよ！！

大輔さん、その意気込みが4月に失速しないことを祈りますね...

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝【おしらせ】＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

4月18日（木曜日）にAirheads アカデミー（東京）を開催します！

No More VLAN の実装方法をご紹介予定です。

https://connect.arubanetworks.com/ja_academy_Tokyo0418

＝＝

バックナンバー

▼ Vol.1~49
▼ Vol.50~77

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。