導入事例

関西大学 様

WADJETの可視化と自動制御機能で度重なるサイバー攻撃に対抗

幅広い利用者が気軽に利用できる学内システムの維持と、セキュリティ強化を目指す関西大学は、その一環として2016年にサイバー攻撃の可視化、自動制御機能を備えたWADJET（ウジャット）を導入。
今回、WADJETの導入・運用に携わる3名のシステム管理者に、大学ならではのセキュリティ強化の難しさと、WADJETの効果、今後のご要望についてお話を伺いました。

平日、休日問わず サイバー攻撃の対処に奔走

関西大学のネットワークは、学生、院生、教授、講師、研究員、職員から、講演会やイベントで一時的に来訪される学外の方まで、色々な特性の利用者が、様々な目的で利用しています。最近は学生のシラバス登録や成績の確認にもインターネットを利用していますので、個人のスマホや家庭のパソコンからのアクセスが非常に多くなっています。Wi-Fiだけでも1日約1万台、有線を含めると約3万台の端末がアクセスしている状況です。

スマホの普及で誰でもインターネットを利用する時代になりましたが、セキュリティの重要性についてはあまり理解が進んでいません。学内の無料Wi-Fiを使用するためにパスワードを入れるように案内すると、「どうしてそんなことをしなくてはいけないの？」と訊かれることもあります。多少パソコンに詳しい人でも、ウイルス対策ソフトを入れれば大丈夫だと思っていたり、いまだにmacOSだからセキュリティソフトは不要だと思い込んでいる人もいます。とは言え、一般企業のように使用端末の限定やソフトのインストールを義務付け、使い方を制限することもできません。

関西大学　学術情報事務局　システム管理課　西脇和彦 氏

そんな状況で、どんな人でも手軽に利用できる開かれたネットワークを提供し、なおかつ一定のセキュリティを担保しなくてはならない。これは非常に難しい課題です。

しかもサイバー攻撃は、管理者が不在の土日や祝日などを中心に狙ってきます。攻撃に気づかず放置してしまうと、踏み台にされたIPアドレスがプロバイダのブラックリストに載ってしまい、メールの送信などができなくなります。利用者から学校へクレームが入ると、私たちが休日返上で対応しなくてはいけません。場合によっては、複数のセキュリティ機関から脆弱性の指摘を受けることもあり、対応に苦慮する状況が続いていました。

待望していた可視化と自動防御機能

もちろんこれまでも、セキュリティ機器の導入など、それなりの対策は行ってきました。しかしどの機器もログがテキストでしか表示されないため、インシデント発生時に、原因特定に時間がかかるのが大きな悩みでした。サイバー攻撃によるアラートは1日に20万件近く上がることもあります。膨大なテキストのログから必要な情報を抽出するのは大変な作業で、数名の管理担当者だけでは対応が困難です。

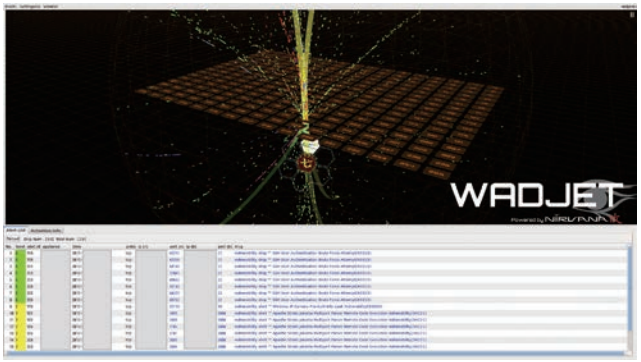
そんな時に、ネットワークの状況を3次元グラフィックで表示できる「NIRVANA」がリリースされました。ログを追ったり、検索をしなくても、視覚的にアラートが表示される私たちにとって願ってもない製品でした。

関西大学　学事局　授業支援グループ　榊原和弘 氏

関西大学　学術情報事務局　システム管理課　雨森康倫 氏

しかし私たちが抱えていた課題は、それだけでは解決できません。素早く原因を突き止め、該当する利用者に連絡をしても、連絡が取れない場合や、人員的な問題で管理者が対処できない場合が多いのが現状です。自動防御ができる装置を導入することは以前から考えていたのですが、弊学のように利用者が多いネットワークでは、ライセンスで単価がカウントされると億単位の予算になってしまいます。

WADJETの3次元グラフィック画面 ▶
トラフィック、ログがリアルタイムで可視化表示され、インシデント検知時にはアラートが拡大・回転する。アラートをクリックすると詳細情報が表示され、短時間で状況を把握することができる。



そこで、NIRVANAを開発していたNICT（情報通信研究機構）に、可視化だけではなく、自動防御機能を搭載してほしいという意見を提出して、動向を見守っていました。その後「NIRVANA改」がリリースされ、さらに商用版として「WADJET」が発表されたことで、期待が現実になりました。私たちはすぐに具体的な導入計画を開始しました。

要望に真摯に応えてくれるディアイティに相談

ディアイティとは、以前から無線LANソリューションの導入でお付き合いがありました。いつもこちらの要望に対して真摯に応えてくれるので、今回も安心して相談することができました。

システム機器の選定は、課題に対する対応力が重要なポイントで、海外メーカーが相手だと、製品は良くてもなかなか意思疎通ができず困ることがあります。例えば、何か問題が起きてそれを解決した後に、データ分析や報告用の過去ログが欲しいと要望しても、どうしてそんなものが必要なんだ？という感じで、なかなか対応してもらえません。対応してもらえたとしても多額の追加費用が必要だったりします。

今回も期待通り、ディアイティには機能面、費用面で融通を効かせていただいて、こちらの要望を形にしていただきました。例えばネットワーク全体を監視するWeb管理画面は、当初は表形式で一覧表示される仕様でした。グラフ表示にすればさらに見やすくなるのではと改善の要望をしたところ、導入後のバージョンアップで対応していただけました。おかげでアラートの状況がひと目でわかるようになり、監視の労力がさらに軽減しました。もちろん、すべての要求が通ったわけではありませんが、できるかぎり応えようという姿勢はお互いの信頼につながりますし、今後の品質向上にも期待ができます。

「WADJET」のWeb管理画面

管理はもちろん事務作業にも大きな効果

「WADJET」の一番の魅力は、やはり3次元グラフィック表示によるアラート表示の見やすさ、わかりやすさです。アラート表示の大きさや回転の速度といった視覚的な情報をもとに、インシデントのレベルや問題が発生しているエンドポイントを瞬時に判別でき、クリックすればインシデントの詳細を確認できます。テキストログを追いかけていた以前と比べ、状況を把握するまでの時間と労力が劇的に軽減されました。

ログの可視化は、実はネットワーク管理の実務だけでなく、説明資料としても非常に効果的です。例えば、研究室のサーバーがサイバー攻撃の踏み台にされてしまった場合に、サーバーを管理している先生にそのことを報告しても、従来の機器から出力されるログ内容ではなかなか納得してもらえません。ログを見せても、よくわからないと突き返されてしまいます。しかし、WADJETの3次元グラフィックなら一目瞭然。説得に時間をかけることなく、すぐに納得してもらえます。

こうした説明資料としての解りやすさは、上司への報告の際にも役立っています。えてして上司はシステムの専門家ではないことが多いので、テキストログをそのまま提出するわけにはいかず、これまでは報告のたびに時間をかけて資料を作成していました。WADJETの導入で3次元グラフィックの表示をそのまま資料として提出すると報告内容もわかりやすく、よりリアルに伝わり業務の効率化につながっています。

見やすくてわかりやすいというWADJETの特長は、利用者の啓蒙活動にも活かせると思います。例えば、ITセンターの入り口に大画面モニタを設置して、3次元グラフィックの画面をリアルタイム表示。利用者が常にネットワークの状況を見られるようにすることで、ネットワークの理解やセキュリティ意識の向上につながると思います。まだ具体的ではないですが、いずれはそんな使い方もしたいと考えています。

「ふるまい検知機能」に期待

自動防御機能については、今のところ、一定のしきい値を超えた場合のみ対象のポートを自動閉塞するように設定しています。これは特に公表している訳ではありませんが、利用者にとっては、以前と変わらない使い勝手で、いつの間にか安全になっているという理想的な状況です。今のところ大きなインシデントや利用者からのクレームはなく、順調に運用できています。

ただ、大学の性質上、時期や曜日、時間帯によるトラフィックの変動が大きく、適正なしきい値を見つけるのは容易ではありません。現状はまだ最小限の防御という状況ですので、今後はWADJETと連携する機器を増やすことで精度を高めていきたいと思います。また最近は、サイバー攻撃の手法が巧妙になっており、一度に1,000通の攻撃を投げてくるのではなく、1分間に100通ずつ小分けにし、こちらが設定したしきい値を超えないレベルで波状攻撃をしてくるようになっています。こうした問題を解決するためにも、パケットレベルでの「ふるまい検知」は有効だと思われ、今後に期待しています。パケットのフローパターンから普段と違うパターンを機械学習等で検出し、それに合わせてしきい値を自動設定してくれるような機能ができれば、非常にありがたいです。ディアイティも現在、そういった技術開発に取り組んでおられるということですので、今後ぜひ実現していただけたらと思います。

お問い合わせは
株式会社ディアイティ
〒135-0016 東京都江東区東陽三丁目23番21号 プレミア東陽町ビル
【Tel】03-5634-7651　【E-mail】info@dit.co.jp