防衛大学校情報工学科教授　中村康弘博士・
ニクサン株式会社・株式会社ネットワークバリューコンポネンツ
三者共同製品検証レポート

インタビュー実施日時：2014 年 2 月 10 日

防衛大学校

・防衛大学校情報工学科教授　中村康弘博士

「NAT 越え」とパフォーマンスで
APT 攻撃をはじめとする今日的なサイバーアタックに対処

防衛大学校において 2013 年末よりニクサン社製品である NetOmni Analytics と NetDetector の実際の環境での三者（防衛大学校・ニクサン株式会社 ・株式会社 NVC）共同製品検証が行われている。特に防衛大学校での検証担当である情報工学科教授の中村康弘博士は日本のサイバーディフェンスにけるエキスパートの一人であり、防衛大学校におけるセキュリティ面の課題とそれへの対処を通して、ソリューションの持つ実力と今後の展開の可能性について迫った。

■検証実施の背景

NAT 導入が一般化する中でいかに膨大なトラフィックをとらえ、セキュリティレベルを維持していくか

1995 年以降、日本でもインターネットの普及が一気に進んだ。当初は企業内や大学内などの組織内部のネットワークに接続される機器もグローバル IP アドレスで管理される事が通常であった。その後、各所の内部ネットワークに接続される機器は増加する傾向が強まり、NAT（Network Address Translation）と呼ばれる組織内部のネットワーク機器に個別の IP アドレス（プライベート IP アドレス）を付与して管理する手法が標準的となった。この NAT によりひとつのグローバル IP で多くの機器を管理できるようになったが、グローバル IP アドレスとプライベート IP アドレスの変換が必須となるなど、組織内のネットワーク通信の詳細を追うのに非常に多くのリソースを割かなければならない局面も増えている。

同時にネットワーク全体のトラフィック量も増加の一途をたどっている。特に世界的なブロードバンド化の流れが顕著になって以降、トラフィックの増加は目を見張るものがある。これは組織内のネットワークにおいても同様だ。個々における動画の視聴頻度の増加や、スカイプなどの VoIP アプリケーションの使用頻度の増加を想起しても、95 年当時とは比較にならないトラフィック量であるのは一目瞭然だろう。また近年は APT（Advanced Persistent Threat）攻撃と呼ばれる標的となる対象を絞り込んだ巧妙な攻撃手法が出現し、日に日にネットワークセキュリティをとりまく状況は厳しさを増している。そうした膨大なトラフィックと新たな攻撃手法を前に、組織内で導入されている NAT 環境において、正確かつ迅速にトラフィックをとらえ、セキュリティ上の対処をする必要性を防衛大学校の中村博士も感じていた。

■検証実施の経緯

防衛大学校としては、その組織の特性の上からも、必要に応じて NAT 導入後も然るべきセキュリティ対策を事あるごとに実施してきたが、NAT 特有のアドレス変換の必要性と、内部ネットワークのトラフィックの増加などからさらなるネットワークセキュリティの強化が求められていた。中村博士はこう振り返る。

「昨年度まで私は学術情報図書館のセンターのメンバーになっていました。日常的に学生がネットワークアクセスを行う環境の運用管理をする役割を担当していました。その過程で内部のネットワークトラブルや外部からの苦情がありました。そうした事を踏まえて、さまざまな事案に対処するために、ネットワークセキュリティをより強固にする方策や機器を広く探していました。

しかし、当時は『帯に短しタスキに長し』といった感じで、なかなか上手く実際の運用環境などに適合する機器やソリューションは見つけられませんでした。ちょうどその時に NVC さんに相談をさせていただく機会があり、その時に『NetOmni Analytics と NetDetector という機器がありますよ』というお話をいただいたのが直接の検証に至るきっかけです。結果として、他にはない機能をもった非常に高機能の製品を検証する事ができました。」

■これまでの防衛大学校のネットワーク上の課題

防衛大学校が検証を行う前に抱えていたネットワーク上の課題をさらに聞いた。

「防大の校内では NAT を用いていますので、個々の学生がどのようなネットワークアクセスを行っているのか、どういったセキュリティ上の問題があるのかを把握するのは、これまで非常に大変でした。1995 年当初に防大としてネットワークアクセスを開始しました。当時は全ての機器がグローバルアドレスだったのですが、途中から機器の数が増えて来たことと、外部からのアクセスの増加や、対外的な意味でのネットワークセキュリティの必要性が急速に高まってきました。そこで、その後 NAT に変更しました。
内部はプロキシを一回通す事になっているので、個々の学生を特定する事は比較的容易です。しかし、個々の学生が外部にアクセスする場合は、プロキシによってソースアドレスの変換がなされます。加えてファイアーウォールでもう一度ＮＡＴ変換しますので、内部の通信と外部の通信の分析上の整合性がとりにくくて苦労していました。」（中村博士）

つまり NAT そのものも内部ネット―ワークと外部ネットワークでアドレスの変換をしなければならいのだが、それに加えてファイアーウォールでも変換を行っているので、なにかあった時は二重にログを追う必要があったのだ。

「また、以前使っていた機器に関してはもちろんログは一応出るのですが、プロキシのログは、1 回アクセスがある毎にクライアントアドレスと接続した先のサーバーアドレスが一行ずつ記録されるわけです。これに先ほど申し上げた通りファイアーウォールがまた別にあります。ファイアーウォールに関しては 1 パケット毎に全部記録が残ります。つまり異なった形式で記録されている内容を、なにかあった時には目視、つまり目で確かめて追わないといけないわけです。これは非常に大変でした。」（中村博士）

1800 名とも言われる防衛大学校の寮生が NAT を利用して通信を行っているのに加え、ファイアーウォールの持つログと目視で整合性をとる状況は確かにネットワークを監視する立場からすると非常に大変だ。セキュリティを維持するためにファイアーウォールを設置するのはネットワークセキュリティを実施する上で基本中の基本だが、それが NAT 導入や対象となる学生数（≒機器数）の多さやトラフィックの増大に合わせて、より一層監視の手間を増やす状況になっていたのだ。

■検証実施に至ったポイント

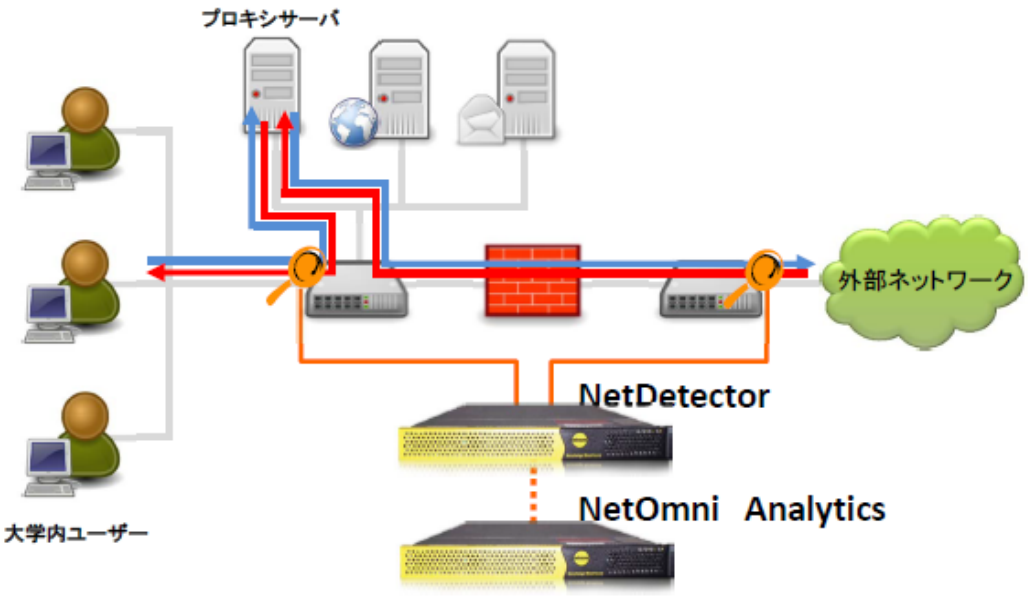
そのような課題を持っていた防衛大学校のネットワークセキュリティの現場であったが、その課題が今回の機器とソリューションの検証へとつながる事になる。

「プロキシと NAT の部分の点についてですが、本来のネット全体において、どのあたりでトラフィックの量が多いのかどうなのか、そういったトラフィックの細部まではまだ監視しきれていない状況にありました。そういったネットワークのトラフィックの細部を監視したいというニーズ

は私共としてはありました。つまり運用面での監視効率、作業効率とより詳細な監視という意味での精度向上をしたいと言う点が今回の三者検証に参加させていただいた大きな動機となります。また、ニクサン社さんはアメリカのネットワークセキュリティでは有名な企業さんで、アメリカの連邦機関のセキュリティ対策でも実績がある事は良く知っており、実際にニクサン社さんの機器を手元で試せるというのも大きなポイントとしてありました。また、POC という無償貸与の制度をご利用できたのも大きかったです。」（中村博士）

そうした防衛大学校の中村博士をはじめとする防大内のネットワーク担当者の感じていたネットワークセキュリティ上の課題への対処をしたいという具体的なニーズと、ニクサン社のソリューションが合致し、かつアメリカでのニクサン社の実績が評価されたのが今回の三者共同製品検証が実現した大きな要因となったのだ。

検証構成図



■検証の効果

今回の三者共同製品検証では、そのような経緯を経て防衛大学校の実際のネットワーク上にニクサン社の機器を導入し、その効果を検証した。果たして実際にそのソリューションを使ってみた結果はどうだったのだろうか。

「ファイアーウォールを含めて、NAT を通した場合のプライベート IP アドレスをグローバル IP アドレスの分析上の整合性を自動的にとってくれる分析機器というのは今までのあらゆる製品をみても、見る限りは皆無でした。先ほどお話したとおり、今までは目視でログを見て突き合わせる以外に方法は無かったわけです。それが、今回のニクサン社さんの製品でパケットをキャプチャして、分析のアルゴリズムを通してみますと、プライベート IP アドレスをグローバル IP アドレスがきちんと対応して出て来るところを確認できました。この機能自体は非常に画期的だと思います。つまり運用面での効率化と精度向上という意味で、とても便利だと感じました。ある意味で運用面の劇的な変化をもたらし得ると思います。」（中村博士）

中村博士は続ける。

「キャプチャをしているデータが数テラバイトというオーダーであったりするのですが、それにもかかわらず、欲しい統計上のデータはこちらが操作してから数秒から十数秒ですぐに閲覧可能になりますので、非常にパフォーマンスはいいと思います。特にこういったデータは時間が経つに従って、線形に量が増えて行くものですが、それにも関わらずパフォーマンスが落ちるという事が無くて、非常によく作られていると思いました。また操作性ですが、現在検証を行っている NetOmni Analytics と NetDetector では UI が統一化されていまして、ウインドウの個別の操作も一貫して行えるので、使いやすいです。筐体が 1U の大きさで膨大なキャプチャデータを蓄積できるのは非常に優れていると思います。加えて、4 ポート使えるので、同時に数か所をキャプチャできるのはいいと思います。」（中村博士）

課題であった「NAT 越え」とも言われる、NAT を介し、かつファイアーウォールとの分析上の整合性を取る上において、ニクサン社の機器とソリューションが充分な効果を発揮している点を確認できた。さらに機器の持つパフォーマンスと監視する上で重要な要素となるユーザーインタフェースの使い勝手についても極めて肯定的な評価となった。

■今後の展開

今回の検証を踏まえて、今後防衛大学校や防衛省や自衛隊でいかなる展開が考えられるかについて中村博士はこう述べた。

「ニクサン社さんや NVC さんとは、今後可能でしたら、実際のセキュリティ対策でノウハウを蓄積した上で相互に補完できるようなパスが構築できたら非常に良いと思います。また機器やソリューションそのものについては、非常に有用性があると個人的には感じています。これから校内ではネットワークセキュリティの専門の課程を作る事を考えています。将来的な構想の部分も大きいですが、教育をする上で機器等は必要ですので、そのための選択肢としてはあり得ると個人的には考えています。」（中村博士）

今後の展開を考える上でも機器とソリューションの実環境での検証を通して、中村博士として確かな手ごたえを感じているのが伝わって来た。そして「NAT 越え」と言われる NAT 環境でのネットワークセキュリティの強化や分析の精度向上、あるいは監視の省力化は防衛大学校のみならず日本の多くの官公庁や大学、研究機関や企業においても同様のニーズがあるものと思われる。そうしたニーズに応えて行く上で、今回の検証が非常に重要な一歩となった事は間違い無いだろう。

我が国のネットワークセキュリティ研究の第一線で活動されている防衛大学校情報工学科教授で工学博士の中村康弘先生に貴重なお話をお聞かせいただく事ができました。同時にニクサン社の NetOmni Analytics と NetDetector といった機器が実際の使用環境で充分な性能を発揮している事を確認させていただく事ができました。加えて、製品や運用面へのフィードバックに繋がる、中村教授の深い知見に基づいた多くの建設的なご指摘をいただく事ができました。今回の三者共同製品検証を通し、確かな成果がもたらされた事を確認すると共に、ここに報告いたします。

作成・文責　NIKSUN Inc. セールス＆マーケティング部
電話 03-6202-7454
E-Mail: marketing@NIKSUN.co.jp