CounterACT 導入事例

一橋大学

→ 一橋大学が、ワーム対策に
CounterACTを選んだ理由。それは・・・・

「VLAN数100のネットワーク環境です。CounterACT 1台でワーム対策ができるとは思っていませんでした」

国立大学法人 一橋大学
情報化統括責任者（CIO）補佐官
総合情報処理センター　助手　松村 芳樹 氏

一橋大学の国立キャンパスでは、無線LANエリア拡大にあたり学内ネットワークのワーム対策強化のためCounterACTを導入した。その評価について一橋大学 情報化統括責任者（CIO）補佐官兼 総合情報処理センター 助手の松村 芳樹氏に伺った。

一 橋 大 学

もくじ

無線LANエリア拡大を機にワーム対策を強化

― 一橋大学国立キャンパスのネットワーク環境について教えてください。

一橋大学国立キャンパスには、学部生、大学院生など学生と教職員合わせて7,000名強がおり、大学通りを挟む東西のキャンパスのネットワーク運用、管理を、総合情報処理センターの数名で担当しています。

学内に持ち込むPCについては、学内ネットワーク接続時にIDとパスワード入力による認証をとることにより、アクセスを提供しています。接続可能な場所としては、大学院生の部屋などが3フロアで約70部屋、学部では主に教室と図書館に有線ネットワークを用意しています。無線LANは現在図書館の一部に入っていますが、まもなく教室の6割くらいに導入される予定です。

この無線LANエリアの拡大を機に、学内ネットワークのワーム対策を強化したいと考え、本年4月、CounterACTを導入しました。

＊導入製品：ForeScout CounterACT

CounterACT 導入事例

一橋大学

大学という環境に適した仕様

― CounterACTを知ったきっかけは。

CounterACTを知ったのは、一昨年、情報セキュリティ関連の展示会でした。仕様を説明いただき本学の状況に適しているなと印象に残っていました。

― どのような点が一橋大学に適していると思われたのでしょうか。

まず、ウィルス対策ソフトなどクライアントPCにソフトウェアをインストールさせなくてよいということです。

大学のネットワークはどんなPCが持ち込まれるか分からない状況にあります。学内に持ち込まれるPCへのセキュリティ対策も充分ではありません。

業務用PCや教員の持ち込みPCについてはウィルス対策ソフトを配布し、インストールを促すことは可能です。ただこれもユーザ任せとなり最新のセキュアな状態かどうかの確認まではできません。

特に問題なのは学生のPCです。多くの学生が持ち込むPCにウィルス対策ソフトをインストールさせ、そのライセンスを管理するなどは管理上不可能です。クライアントPCへのソフトウェアインストールを前提にしないCounterACTの仕様は魅力的でした。

「どんなPCがつながるか予想できないのが大学のネットワークです」

もともと大学のネットワークは研究者用として構築され、基本的には緩やかなセキュリティポリシーで運用されています。研究のためには自由にサーバを構築することを許可する必要があり、ルールでガチガチに縛ることはできません。その緩やかなポリシーの研究者ネットワークをベースに、業務ネットワークが載るというかたちになっています。

外部からの不正アクセスの防御はもちろんですが、内部からのワームの拡散や情報漏えいを防ぐことも重要な課題になっています。ポリシーが厳しくない上に無線LAN環境を拡大することになり、ますますどのようなPCもつながる環境になりました。ソフトウェアのインストールが必要なく、どのようなPCの攻撃にも対応可能というワーム対策システムは、本学の要件にぴったりでした。

― 他のソリューションと比較していかがでしたか。

認証前であってもワームの検知と遮断ができるという点が、他の製品と比較しても本学に適していると思いました。CounterACTの場合、既知のワームでもゼロデイ攻撃でも、ネットワーク認証前でも後でも、スイッチのミラーポートにCounterACTを接続してトラフィックを監視させれば、ワーム攻撃を検知し、攻撃者と判断すると自動的にネットワークから切り離すことができます。

通常のIDSでは、認証を通過する前に不正アクセスを検知する手法がありません。これまでも、認証を行う前に狭い範囲で仲間同士が感染している状況も見受けられました。

最近では、PCが高性能化し、ウィルス感染したくらいではPCの機能が止まりません。利用者が気付かず使い続けていることも多いのです。ワームもこっそり働くパターンが多く、利用者本人が意識できるほどの負荷として現れないため、発見が難しいのです。

認証しているしていないに関わらず、自動的に攻撃PCをネットワークから切り離せるというCounterACTの仕様は、セキュリティポリシーも厳しくできず、持ち込みPCのウィルス対策も不十分という本学のネットワークの状況に適していると思いました。

CounterACTを選んだ理由

― CounterACT導入を決められた理由を教えてください。

CounterACTを選んだ理由は、以下の3つです。

1. エージェントやWindowsドメインが不要なこと
2. ピンポイントでネットワークから切り離せること
3. Tag-VLANに対応していたこと

選んだ理由１：エージェントやWindowsドメインが不要

― では一つ目、エージェントやWindowsドメインがいらないという点についてお聞かせください。

専用のエージェントソフトをインストールする必要がある検疫システムは多くありますが、先にお話したように本学の場合、学生や教職員のPCに何かインストールすることを徹底させるのは難しい状況です。

特に、文系の大学ですので、コンピュータの扱いが得意でない学生も多く、ウィルス対策ソフトのインストールのみならず、Windowアップデートさえ徹底させることが難しいのが実情です。

何かをインストールさせることは、問い合わせ対応も含め、管理者の手間を増大させますし、コスト面の負担も大きくなります。

また、検疫システムにはWindowsドメイン管理を前提としたものも多いのですが、ドメイン管理となりますと、学生が持ち込むPCに大学にいる間は大学のドメインを切らせてユーザIDとパスワードを入力させることになり、本学の学生にはさらに敷居が高くなります。

個々のクライアントPCにエージェントソフトをインストー

＊導入製品：ForeScout CounterACT

ルさせたり、Windowsドメインで管理したりを前提としたセキュリティ対策は、大学の場合、現実的ではありません。どんなPCが持ち込まれるかわからないという前提でセキュリティ対策を考える必要があり、エージェントもドメインも不要という点は抑えておきたいポイントでした。

選んだ理由２：ピンポイントでネットワークから切り離せること

― 二つ目、ピンポイントでネットワークから切り離せるとは。

CounterACTは、攻撃を検知したIPアドレスの、そのポートでの通信だけをピンポイントで自動遮断してくれます(ポートブロック設定)。そのため、検地されたエリアをまるごと隔離する必要がなくネットワーク全体に影響を与えずに済みます。

CounterACTのワーム侵入の検知と防御の方法は、攻撃者がスキャン行為を繰り返す習性を利用したものです。

攻撃者のスキャン行為を発見　=>　CounterACTから偽の情報で応答　=>　攻撃者がその偽の情報に対してアクセス　=>　CounterACTが攻撃者と判断し、その通信を遮断する。　というしくみです。

現在は、攻撃を検知したポートの通信だけを自動的に切断するポートブロック設定で動作させているので、学生は自分の端末で攻撃が検知され、特定の通信がブロックされていることに気づいていないことも多いです。Webやメールのトラフィックが止まればさすがに気づくようですが。

管理者としてはクレームも問い合わせもなく助かりますが、学生に注意を促す意味では、今後CounterACTをホストブロック設定に変更して、攻撃を検知した端末からの通信はすべて切断するようにしたほうがよいのではと思うこともあります。

選んだ理由３：Tag-VLANに対応していること

― 三つ目、Tag-VLANに対応していることについてお聞かせください。

本学はVLANを使用し、ネットワーク構造が論理的に一箇所に集まるように作っています。複数のサブネットをひとまとめにして管理しているわけですが、VLAN対応していない機器の場合、サブネットごとにいちいち監視場所を設けなければなりません。そのため、導入する機器はVLANに対応している必要がありました。

特に、Tag-VLANに対応していることは必須条件でした。Tag-VLANの場合、サブネットが一箇所にまとめられてもサブネットごとに区別することができます。院生室は、部屋ごとにサブネットを変えて管理していますが、それによって、どこの部屋の学生がアクセスしてるかが分かり、問題が起こった時の発生源の特定が容易です。

このTag-VLANに対応していたのは、検討した時点ではCounterACTしかなかったと思います。

VLAN数100のネットワーク環境でのワーム対策が、CounterACT 1台でできた

院生室でVLAN数は70、教室を含めると全体でVLAN数が100という極端に細かいネットワーク構成です。エリアとしては院生室　3フロア、教室、図書館、建物でいえば5箇所、20フロアぐらいとなります。他の製品では、建物ごとやフロアごとの設置が必要となる場合もあるので、本学の環境では20台くらい必要と言われてもおかしくないところです。この範囲のワーム検知と防御が CounterACT 1台でまかなえています。

他製品では、ログイン認証前には検疫用ネットワークにつないでおき、認証後は通常の社内LANにつなぐという認証VLANを利用したソリューションも色々ありますが、この認証VLANと絡んだ製品は結構高額です。機器1台でできるものではなく、ネットワーク機器とそれを制御する装置との組み合わせのソリューションとなるため必然的に高価になるからです。

また認証VLANを利用したソリューションでは、ネットワークスイッチから入れ替えることになり、設計変更が必要でした。それに、攻撃検知はできても、CounterACTのように防御はできません。監視すべき範囲を考えると費用対効果も見合わず、このような製品では導入検討の余地もありませんでした。

導入後の評価

― 導入後の評価をお聞かせください。

あまり意識しないで使えているのがいいですね。自動的にワーム攻撃を排除してくれているので、こんな攻撃があったんだと、後で確認する程度で放っておけます。

導入前は、管理者がネットワークをモニタリングして、ワーム攻撃と思われる通信があると、手動でスイッチのポートを遮断するなどの設定変更をしていました。

以前は、基本的に管理者がトラフィックだけをモニタリングしていました。特に大量に何かデータが流れたりすると目で確認できます。文系の学生ですから、学内LANを使うといってもほとんどが外部からのダウンロードです。学外から学内に入ってくるトラフィックがメインで、通常出て行くのは1割くらいなのですが、これが逆転するのを発見すると何かが起こっていると怪しむわけです。

エッジスイッチのポートのひとつひとつを確認することはできませんが、攻撃元となっているフロアは限定することができます。どのフロアのIPアドレスからからどのフロアが攻撃元かをトレー

＊導入製品：ForeScout CounterACT

スし、MACアドレスを探り、どのスイッチで使っているかと順に追っていき、ポートを特定します。そして、攻撃元となっていると思われるポートごと遮断するというような手間をかけていました。

学生は大体夜型です。われわれが帰宅しようとする7時、8時という時間帯から動き始めます。翌朝出勤すると、夜中にDDos攻撃でスイッチがアップアップしていたと分かることもありました。

今は、CounterACTで自動監視され、問題が発見されると即時遮断されますので、以前のようにモニタリングしたり、手動でポートを閉じる必要もありません。ログの確認は後回しにして他の業務を行える。確実に管理面での負担は減りました。

今後の期待

— CounterACTへの今後の期待をお聞かせください。

最近では、動画配信などが増え、扱うデータも大きくなっています。サーバは各研究室での管理していますが、数も増え、維持が負担になり放置してあるものも多いようです。管理者の負担も増えていますので、今回のCounterACTの導入で手間が減ったことは大変助かっています。

これまでは、無線になるとワームの感染源がアクセスポイントの近辺にいるか位しか追えず、本人の特定はできませんでした。そのため、攻撃を受けている箇所を特定し、ピンポイントで自動的に遮断してくれるCounterACTの機能には、無線環境での攻撃対策においても期待しています。

また、現在は学生にワーム攻撃があったことについて周知を行っていませんが、今後、本人にワームを流したという自覚を持たせ、セキュリティ対策を指導する必要性を感じています。CounterACTでのポップアップメッセージ送信機能やWebページでのアラート通知機能を利用していきたいと考えています。

— お忙しい中、有り難うございました。

ForeScout

お問合せ先
株式会社ソリトンシステムズ 〒160-0022 東京都新宿区新宿 2-4-3
TEL. 03-5360-3811 FAX. 03-5360-3880 MAIL. netsales@soliton.co.jp www.soliton.co.jp

Soliton®