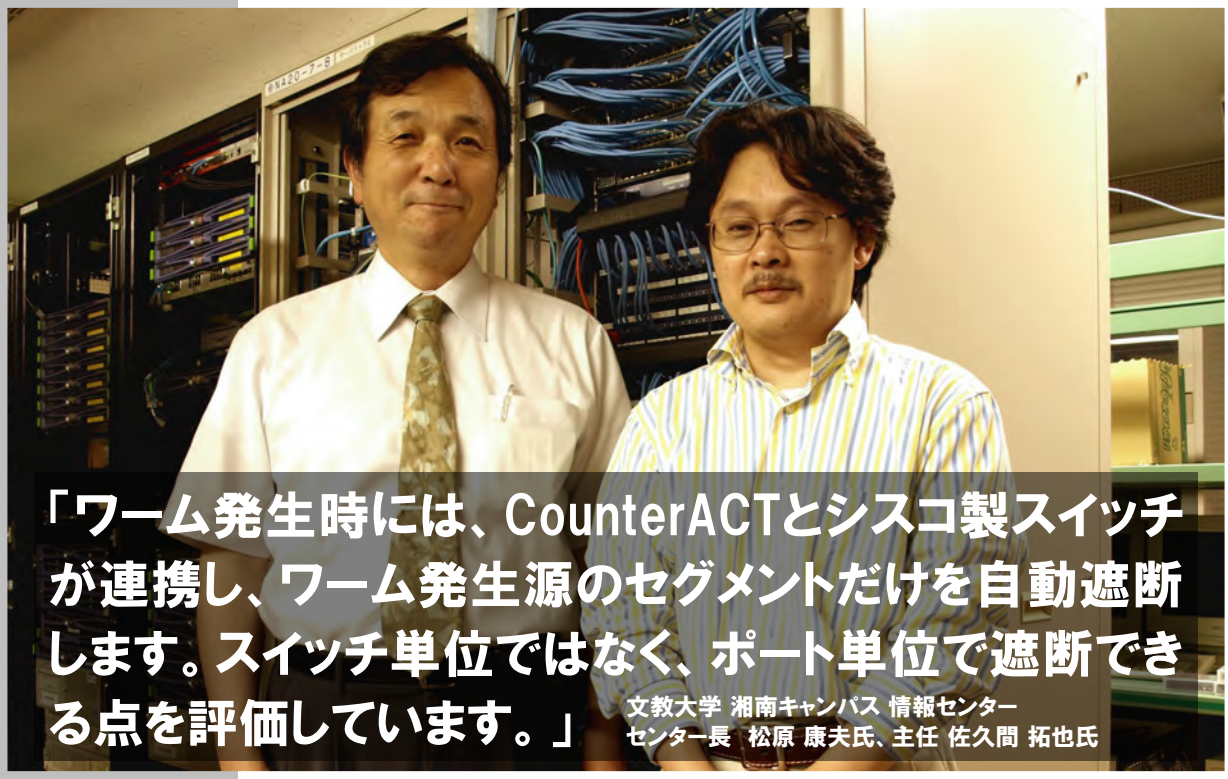
CounterACT 導入事例

文教大学（湘南キャンパス）

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



大学という「自由度を求められるネットワーク」で、どうセキュリティを確保していくか、何を運用の基本ポリシーにするべきかなどを、文教大学　湘南キャンパス情報センター　センター長　松原康夫氏と主任佐久間拓也氏に聞いた。

もくじ

文教大学ではCounterACTをどう使っているか

― 文教大学では、現在CounterACTをどう使っていますか。

CounterACT1台を導入し、キャンパスネットワーク全体のセキュリティ確保（ワーム対策）を図っています。2007年の4月1日から稼働させています。
監視エリアは、1号館～7号館および厚生棟の全8棟分に及ぶキャンパス全体です。

シスコ製スイッチとの連携への評価

― CounterACTの最も良かった点は何ですか。

CounterACTの最も良かった点は、シスコ製スイッチと連携して、ポートごとのネットワーク制御を実現できたことです。この機能があることで、以下のような運用が可能になります。

1.先生方や学生のPCには何もインストールしない。ワーム対策を行ったことも意識させない（通知もしない）。

2.ある日、どこかの研究室のPCからワームが不正通信を行おうとしたとする。対策機器がそれを見つける。

3.その時、その研究室のネットワークをキャンパスネットワー

＊導入製品：ForeScout CounterACT

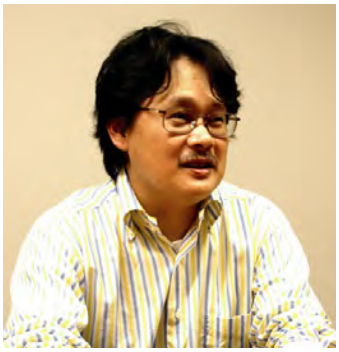
文教大学（湘南キャンパス）

クから遮断（隔離）する。他のネットワークには一切影響を及ぼさない。

4. その研究室からは、「ネットワークが止まりましたよ」とクレームが来るかも知れない。その時はじめて「ワーム対策機器がネットワークを遮断したこと」、「ネットワーク遮断の原因は、その研究室から発生したワームであったこと」、「他の研究室には被害（迷惑）を及ぼしていないこと」を伝えればよい。

5. これにより、自業自得の原則に基づく、誰にでも納得できるワーム対策が実現できる。

この運用を実現するには、スイッチごとの遮断では大ざっぱすぎます。スイッチに命令を出して、ポートごとに遮断する必要があります。



「シスコ製スイッチとの連携を高く評価しています」

学内での具体的運用イメージ

— CounterACTによる、ポートごとのネットワーク遮断の具体的イメージを教えてください。

特に重点監視している「研究室」、「ラウンジの無線LANネットワーク」、「大学院生のノートPC」、の三つを例にしてご説明します。

第一に研究室。研究室のネットワーク構造は、おおまかには、スイッチ内の各ポートに、各研究室のネットワークがぶらさがっているイメージです。仮に、どこかの研究室から、ワーム等による不正トラフィックが乱放出されそうになった場合は、CounterACTがそれを検知して、スイッチの該当ポートを自動遮断します。これにより、その研究室「だけ」がキャンパスネットワークから遮断されます。一種の検疫ネットワークです。

無線LANアクセスが可能な共有ラウンジ

第二にラウンジの無線LANネットワーク。学内のラウンジでは、学生に無線LANを解放しています。CounterACTでは、この無線LANからのワーム侵入も遮断できます。あくまで理論上の話ですが、「仮に誰かが、ワーム入りノートPCを手に持って、無線LANに接続したままの状態で、学内を走り回った」としても、各無線アクセスポイントで検出、遮断できます。

第三に大学院生のノートPC。大学院生には、ノートPCを2年間、無償貸与しています。院生は、そのノートPCを、自宅その他で、研究目的のために自由使用できます。CounterACTは、このノートPCからのキャンパスネットワークへのワーム侵入を防ぎます。実は、その防御には、すでに実績があります。

2007年6月に、大学院生が持参したノートPCの中のワームをCounterACTが見つけ、ＰＣが接続された研究室のLANを自動遮断しました。

ウイルス対策ソフトよりも、CounterACTの方がワームを早く見つけた

— ウイルス対策ソフトは、そのワームを発見しなかったのですか。

そこは若干、不思議な点です。キャンパスネットワークには、ゲートウェイ、クライアント共にウイルス対策システムを導入しています。パターンファイルも、自動的に定期更新されています（そのはずです）。発生源のノートPCのハードディスクを、ウイルス対策ソフトウエアで検査したところ、そのワームは検出されました。しかし、ワームを一番最初に見つけ、かつ、感染端末をネットワークから隔離したのはCounterACTでした。

「とりあえず自動遮断」という仕様への評価

— そうして実際にワームを検出して、どういう感想を持ちましたか。

第一に「CounterACTのように、ネットワークの”自動遮断”ができる仕組みは良いな」と思いました。普通の仕組みでは、「ワームが見つかりました。どうしますか」と管理者に問いあわせてきます。しかし、CounterACTの場合は、「とりあえず自動遮断」です。ネットワーク全部を「とりあえず遮断」されたら困りますが、CounterACTは、シスコのスイッチと連携して、良からぬポートだけを遮断します。適切な仕様だと思います。

第二に、ワームって本当に来るものなのだなと感じました。今回、ワーム対策のためにCounterACTを導入したわけですが、一方、心のどこかでは、ワームなんてホントに来るのかなとも思っていました。しかし、今回の一件で分かりました。やはり、ウイルスやワームって本当に来るのだなと。

＊導入製品：ForeScout CounterACT

CounterACT導入の経緯

— 今回、文教大学が、CounterACTのようなワーム対策システムを導入した理由は何ですか。

ワーム対策（CounterACT）は、3年に一度の、ネットワーク設備全般の更新の一環として、2007年度の予算に盛り込みました。

予算は有限なので、何かを導入すれば、何かを見送らねばなりません。学内からは、光ファイバーネットワークなどの導入を望む声も多かったのですが、今回はセキュリティ強化が最重要だと判断し、見送りました。

あらためて思うことですが、ユーザー側と、われわれ管理側とでは、設備更新に対する考え方が異なります。

— 「ユーザー側と、われわれ管理側とでは、設備更新に対する考え方が異なる」とは、具体的には。

ユーザー側は「今、何ができるか」に着目し、管理者側は「いざという時、どう対処するか」に着目します。

例えばハードディスクを購入するとします。こういう時、管理者は、「ハードディスク保守を購入しておかないと、いざという時に困るだろう。予算はそこに充てよう」と考えます。しかし、ユーザーにとっては、「いざという時」はどうでもよい。そうではなく、「今、どれだけ使いやすく、快適になるか」の方が重要です。だから、そこに予算を充てようとします。

今回のCounterACTは、「いざという時の為の」設備です。ユーザー側にとっては有り難みのない投資だったかもしれません。しかし、導入して2ヶ月後に、ワーム蔓延（寸前）という「いざという時」が来ました。やっぱりワーム対策を導入して良かった。もし、ワームが学内に蔓延していたら、われわれ情報システム部は、セキュリティ対策不足という批判を受けていたかもしれません。

CounterACTの仕様の良かった点3つ

— 数あるワーム対策製品の中から、最終的にCounterACTが選ばれた理由は何ですか。

候補となった他製品と比べ、「シスコ製スイッチとの連携」、「ミラーポートの活用」、「中央での制御」の3点で、CounterACTが相対的に優れていました。

— 「シスコ製スイッチとの連携」への評価は冒頭でお聞きしました。その他の評価点について、順々にお聞きします。「ミラーポートを活用すること」とは、具体的には。

他製品は、ブリッジ型（ゲートウェイ型）でした。この仕様の場合、パケット通信量が増加した場合、もう一台、もう二台と機器を追加せねばなりません。また、その機器が止まると、ネットワーク全体が道連れとなりダウンする可能性があります。これは良くありません。

CounterACTは、ミラーポートに流れてくるコピーデータを検査する仕様でした。つまり、CounterACTにトラブルがあっても、ネットワーク全体を止める心配はありません。良い仕様だと思います。

「ワームを出したセグメントだけが自動遮断されます」

— 良かった点 その3、「中央での制御」とは。

大学のキャンパスは広大です。一方、情報システム部門の人数はわずかです。したがって、わざわざ足を運ばなくてもトラブル対処できるよう、机上のPCからネットワークの全てを把握できるよう、「なるべく中央へ、中央へ寄せるような仕様」が重要でした。CounterACTは、中央に1台を導入すればよく、また管理コンソールが充実しており、要望を満たしていました。

今後の期待

— CounterACTは、どんな企業、団体に向いていると思いますか。

ネットワークに参加するPCが、中央の管理が届かない場所に散在している環境に向いているでしょう。つまり大学には非常に向いています。その他、自宅勤務社員を多く抱えており、かつ彼らに社内のリソースにアクセスさせねばならないような、そういう環境にも適しているでしょう。

— CounterACTへの今後の期待をお聞かせください。

今回、大学という環境でのワーム対策として、質の高いシステムが実現できたと考えています。ソリトンには、ワーム対策のみならず、様々な分野のセキュリティ対策において、今後も優れた技術や製品をご提供いただくことを期待します。

— お忙しい中、ありがとうございました。

＊導入製品：ForeScout CounterACT

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®