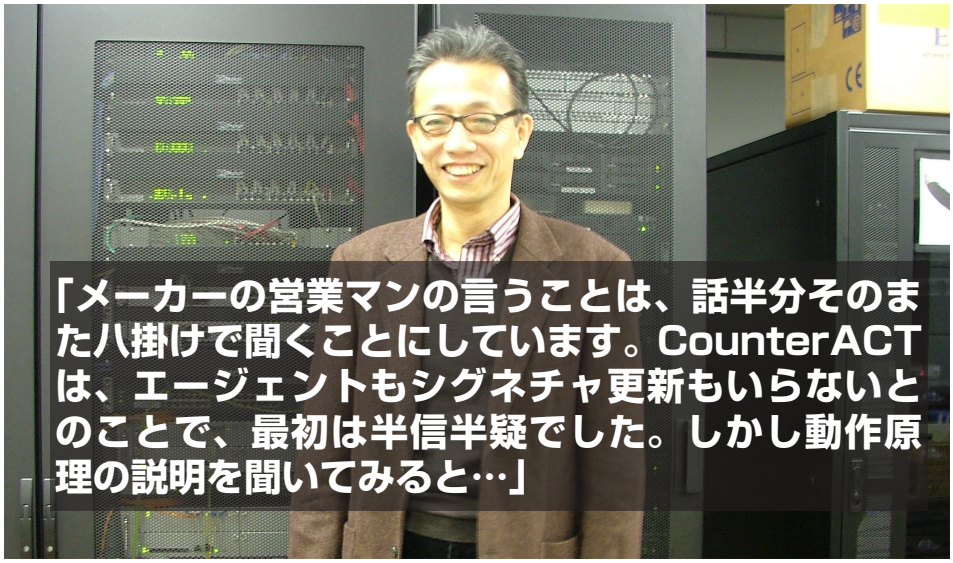
CounterACT 導入事例

武蔵大学

→ エージェント無し、シグネチャ無しの仕様が大学に適切な、その理由



武蔵大学では、ブラスタ被害を契機に、セキュリティシステムの刷新を図った。当初は本格的な検疫システムを検討したが「クライアントにエージェントをインストールするのは、大学では絶対に無理」という理由で見送った。その後、最終的に CounterACT が採用された理由と経緯につき情報システムセンター事務室の小野成志氏に詳しく聞いた。

ネットワークウイルス対策に本格的に取り組むようになった、その理由

– 武蔵大学が、ネットワークウイルス対策に本格的に取り組むようになった経緯は何でしょうか。

2003 年にブラスターワームが学内に蔓延したことが直接のきっかけですね。学外でブラスターに感染した PC が、その後、学内ネットワークにつながれてしまい、しかもその日は休日だったので、ブラスタが一日かけて、学内に蔓延する結果となってしまいました。この事故を契機に、セキュリティ体制の刷新が必要視されてきました。

– ブラスタ以前はどのようなセキュリティ対策を取っていたのでしょうか。

それ以前も、Snort などにより自前のシステムを組んだりして、ネットワークを監視していましたが、ブラスタの一件で、やはりそうした体制には限界があることを悟らされました。その後の方針として、まずセキュリティの「ポリシー」を策定し、次いで、セキュリティ「システム」を構築し、その二つを車の両輪として運営していこうと考えました。今回の CounterACT（*）導入は、その「システム」の整備の一環です。

まず最初にどこから手をつけたか？

– ワーム対策のシステム整備はどのような手順で進めたのでしょうか。

最初は、CounterACT のようなワーム対応の製品ではなく、本格的な検疫システムの導入を考えていました。しかしシステム会社の説明を聞くうち、これはちょっと無理があるなと思えてきました。

– どのような点が無理に思えたのでしょうか。

検疫システムの場合、「シグネチャのメンテナンスが必要」であり、かつ「各クライアントにエージェントをインストールしなければならない」とのことでした。それは話が重すぎる。特にエージェントのインストールが必要という仕様は大学のネットワーク運用ポリシーには合いません。

– 大学の運用ポリシーとはどのように合わないのでしょうか？

これが企業ネットワークであれば、私物 PC は持ち込み禁止、社内ネットワークへの接続も厳禁という運用も可能でしょうが、大学のネットワークの場合、「研究」が使用目的なので、先生の私物 PC（＝研究用 PC）の接続を禁ずるわけにはいきません。つまり、大学ネットワークにはどんな PC もつながりえます。したがって、全てのクライアントにエージェントのインストールを強要することは無理なのです。

– その後、CounterACT を検討するに至った経緯はどのような？

CounterACT のことは、ソリトンの営業担当の方が、飛び込みで電話をかけてきて、そこで知りました。その中で CounterACT の紹介もあり、その時「エージェント不要、シグネチャ不要、誤検知ゼロ」という説明を受けました。私としては、営業担当の言うことは、常に「話半分そのまた八掛け」で聞くことにしていますが、それにしても「エージェント不要、誤検知ゼロ」というのは、もし本当なら、すばらしい話です。ソリトンについては「インターネット黎明期以来の歴史を持つユニークな技術の会社」として認識していましたし、そのソリトンがこれだけ自信を持って電話してくるのだから、あながち変な製品でもないのだろうと思い、とにかく動作原理を聞いてみようと考えたのです。

CounterACT の動作原理への評価

– 動作原理については、どのような説明があったのでしょうか。

この製品の、ネットワークウイルス（あるいは不正攻撃者、不正プログラム）の検出原理は以下のようなものであるとのことでした。

① ポートスキャンなどの「非常に怪しい動き」を検出した場合、警戒レベルを一段上げる。
② その上で、その発信者に向けて、「偽の返答」を返してみる。
③ その「偽の返答」に、もし反応してきたなら、その段階で「発信者」を「悪質攻撃者（または、ネットワークウイルス）」と見なし、通信を遮断する

ざっと、上記のような説明でした。この説明を聞いて、なるほどこの動作原理は以下のような喩えで理解すればいいのかなと思いました。

通常の検疫システムは、空港の入国管理所のようなものである。

① 入国管理所は警察の発行した指名手配書（これがシグネチャ）を全部持っている。

＊ 導入製品 ：
CounterACT (CounterACT の、武蔵大学への納入当時の製品名は "WormScout"。当時は、ネットワークウイルスのおとり検出機能のみを備えており、検疫機能は未装備だった)

② これと入国希望者のパスポートを突き合わせてチェックする。

この手法は、確実かもしれないが、手間もかかるし高価でもある。だがベテランの税関は：

① 不審者をまず挙動で見分ける。
② グレーな不審者に対し ては、「カマ」をかけたりして、シロかクロかを判定できる。

この手法の場合、手配書が回ってきていない犯罪者（これが未知の脅威）にも対応できる。

こう考えると確かに、シグネチャ無しでも誤検知は出にくそうです。HoneyPot の原理に似ていますが、HoneyPot は解析するだけで防御は行わない。一方 CounterACT は、偽の返答をして、攻撃者をつかまえにいくわけで、これは新しいやり方だと思いました。その他、ネットワーク負荷を与えない仕様になっているのも良いと思いました。

– それはどのような仕様だったのでしょうか。
送受信の間に、インラインで割り込んで、直接に監視するのではなく、ミラーポートを流れるデータを検査する仕様だとのことで、なるほど、それならネットワークにも負荷がかからないと納得できました。

「平和なときに、何もレポートしないのはいいこと」という評価

– 現在の使用感はいかがでしょうか。
使ってみてわかりましたが、さすがに誤検知が「ゼロ」とはいかず、最初の頃は、不思議なアラートが何度が発生したことがあります。しかし学習機能がしっかりしているので、そうした問題は最初のうちだけで、最近はまったく発生していません。ということは「誤検知ゼロ」という謳い文句は、トータルな意味では、正しいと見て良いだろうという印象を持っています。

– 運用面ではいかがでしょうか。
例のブラスタの一件以来、学内にネットワークウイルスが持ち込まれることもなく、その意味では、CounterACT が直接発動することもなく、月に一回レポートが飛んでくる以外は、いたって静かな運用です。しかし、この「静かで何も起きない」というのも CounterACT の仕様の優秀性だと思います。

– なぜそう思えるのでしょうか。
例えば Snort のような IDS 系の製品はレポートやアラームがガンガン飛んできます。そうした警告は、決して無用な情報とは言えませんが、あまりにもアラームの量が多いと、重要な情報が日常的なレポートに埋もれてしまい、本当の脅威を見逃すという事故が起きる可能性があります。

それを思うと、本当の攻撃者が来たときだけ、アラームを発し、それ以外の時にはじっと黙っているという CounterACT の仕様は、なかなか良いやり方だと思います。

– CounterACT はなぜ静かなのでしょうか。
シグネチャがないからでしょうね。ウイルス対策ソフトなどを使っていると、すぐ気づくことですが、シグネチャが更新される度にレポートが来ます。シグネチャは頻繁に更新されるので、レポートも半端でない頻度でやってきます。CounterACT は、それが一切無いから静かなのでしょう。また、エージェント無しという仕様も非常に良いですね。

– やはり「エージェント無し」は重要なポイントでしょうか。
重要です。システム管理者にしてみれば、管理対象の数は少なければ少ないほど良いのです。このことを表すエピソードとして、こんな話を聞いたことがあります。ある有名なグループウエアにおいて、クライアント側ソフトのバージョンアップが必要になったので、システム管理者が一台一台、手作業でバージョンアップして回っていたところ、バージョンアップが完了した頃には、次のバージョンが出ていたという…


「大学ネットワークにつながる PC にエージェントをインストールするのは原理的に、どうにも無理があります」

– それはちょっと、笑うに笑えない話ですね。
特に大学の場合、先ほど述べたように、先生の PC をシステム管理者が管理することは事実上、不可能です。ですからエージェントレスというのは絶対の条件ですね。

CounterACT とソリトンへの今後の期待

– 今後の CounterACT に期待することなどお聞かせください。
CounterACT も、今後は、ワーム対策の機能の他に、検疫の機能もつくと聞きました。そうなると「検疫システムが、シグネチャレス、エージェントレスで組める」ということになり、当初は検疫システムの構築を狙っていた我々としてはまさに望むところです。

– 今後のソリトンに期待するのはどのようなことでしょうか
ソリトンの事は、ソリトン日本語 TCP の時代からのユニークな技術の会社として認識していました。今回の CounterACT は、ForeScout 社の製品ですが、今後も、自前の技術であるとないとに関わらず、技術の会社として選んだ「おもしろい製品」をいろいろ提案してほしいですね。私としては、ソリトンは非常にユニークな立場にあると思っていますので。

– どういう点がユニークに思えるのでしょうか。
例えば、外国からおもしろい商品を見つけてくるのが上手な会社というのはソリトンでなくてもいくつもあります。しかし、そういう会社の場合、製品の発掘力はあっても、技術がないので、導入する側としてはどうも不安なのです。一方、ソリトンは、今回の CounterACT のように、ユニークな動作原理を持つ製品を見つけてきて、しかもそれを実装する技術も備えており、これはユーザーとしては理想的です。今後も、ユニークな製品をどんどんご提案ください。楽しみにしております。

– 今日は貴重なお話を有り難うございました。

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