Soliton

CounterACT

CaseStudy | 導入事例

株式会社サイバーエージェント 様

CyberAgent

本社も関連企業も。計1600台の端末を守る「CounterACT」社員に負担をかけないポリシーチェック（検疫）とワーム・不正アクセス防御で「感染被害ゼロ」を実現

User Profile

所在地：東京都渋谷区道玄坂1-12-1
渋谷マークシティ ウエスト21階
U R L：http://www.cyberagent.co.jp/

月間2500万人以上のユーザーが利用するインターネットサービス「Ameba」で知られるサイバーエージェントはスマートフォンやPC・モバイルにおけるインターネットサービスの提供や、国内トップの売上を誇るインターネット広告代理事業を展開するインターネット総合サービス企業である。

POINT

1. 社員に負担をかけないポリシーチェック（検疫）の実現
2. ネットワークに影響を与えない導入と運用
3. アンチウイルスソフトだけでは特定できなかった新種のウイルス・ワーム感染の検知と防御

2010年初頭から増え始めたソーシャルメディアが標的の脅威

月間2500万人以上のユーザーが利用するインターネットサービス「Ameba」ブランドのブログサービスや様々な関連サービス事業を展開するサイバーエージェントでは、社員のほぼ全員が、TwitterやFacebookをはじめ、様々なソーシャルメディアを日常業務の中で利用している。そこで、新たな問題となってきたのが、ショートURLサービスを介したマルウェア感染の脅威だった。

例えば、Twitterでは最大140文字など、ソーシャルメディアの多くは文字数が限られるためにURLを簡素化するショートURLサービスを用いることが一般化したが、短縮化されたURLでは本来のドメイン名の推察が困難なことを逆手に取り、不正なプログラムを配布する危険なWebサイトへ誘導する手口が増加している。

「業務上様々なサイトを閲覧している社員の端末が、気がつかないうちにウイルスやワームに感染していたことが発覚して大きな問題となりました」と語るのは、サイバーエージェントの高場大樹氏だ。こういったケースは2010年初め頃から増え始め、幸いにも実害はなかったものの、アンチウイルスソフトの利用だけでは検知できない新たな脅威からも社内システムを防御する必要性が高まっていた。

同社では緊急に対策が話し合われ、既存のアンチウイルスソフトでの対策に加えて、OSのパッチ適用・アンチウイルスソフト更新の徹底と、万一ウイルスやワームに感染した場合にもいち早く検知して感染拡大を防ぐIPS（不正アクセス・侵入防御システム）の導入を検討した。ただし、各地に拠点を持つサイバーエージェントとその子会社を含めた約1600台の端末をカバーできることと、日常の業務を阻害せず、できる限り社員に負担をかけないことが前提条件となった。

CounterACTを選んだ3つの理由

高場氏らのチームはすぐさまソリューションの選定作業に着手。2010年2月に、10製品ほど実機を用いて検証した結果、ソリトンシステムズが提供するエージェントレス型検疫とワーム・不正アクセス防御が一体となったアプライアンス「CounterACT」の導入を決定した。高場氏はCounterACTを選んだ理由を3つ挙げている。

1. 端末に何もインストールしなくて良い

CounterACTは、完全なエージェントレスで、ポリシーチェック（検疫）を実現するユニークなソリューション。クライアント端末に専用コンポーネントを配布したりブラウザを立ち上げたりする必要もなく、社員の業務を中断することはない。

「まず、端末側に何もインストールしなくて良いところが、社員の業務を阻害しないために重要な選定ポイントとなりました。セキュリティ対策が不十分な場合、対策を促す案内画面を表示するようにしています。強制アップデートを行う運用も可能ですが、ユーザーの自主性を重んじ業務に負担をかけない運用にしています」（高場氏）

2. ネットワークへの影響が最小限

他の検疫・IPS製品はネットワークの通信経路上に設置するタイプ（インライン型）が多く、

CounterACT

株式会社サイバーエージェント 様

株式会社 サイバーエージェント
人事本部 全社人事グループ
ワークプレイスクリエイトグループ
シニアスタッフ
高場 大樹 氏

そこに障害が発生するとネットワーク全体に影響が及ぶ可能性が高いため、ネットワーク停止を防ぐには、コストをかけてでも冗長化することも多い。しかし、CounterACTは、通信経路上に挟まずにスイッチのミラーポートからトラフィックを監視する、アウト・オブ・バンド型のため、既存ネットワーク構成を変えることなく設置が可能だ。

全社インフラは会社の生命線であり、業務維持のため社内のネットワークは一時たりとも止めることはできないと考える高場氏は、「通信パフォーマンスを劣化させず、万一の障害発生時もネットワークに影響を与えない方式は、管理者として非常に安心できると感じました」と語る。

3. 新種ウイルス・ワームの検知・防御

CounterACTには、シグネチャやパターンファイルに依存しない独自手法のIPS機能が実装されており、まだパターンファイルの無い新種のウイルス・ワームのネットワーク感染（ゼロデイ攻撃）であっても検知できる。アンチウイルスソフトだけでは見つけることができなかった感染端末も、即時に特定できるようになった。

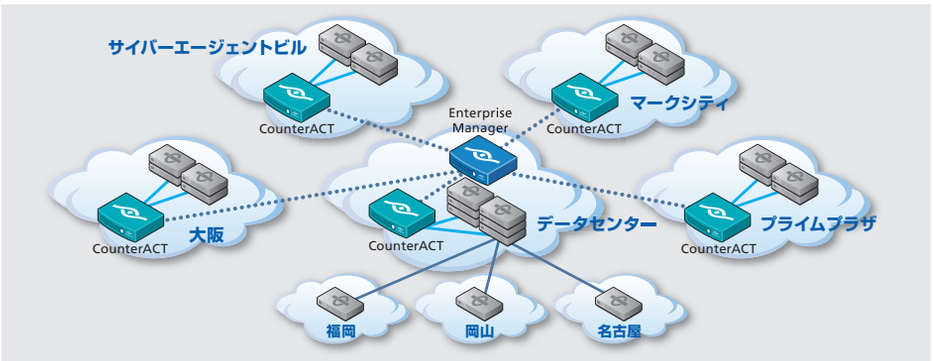
これまで把握できなかった感染元を特定 CounterACTの導入後、感染被害ゼロに

同社の行動は迅速で、導入決定の2か月後（2010年5月）には構築を完了していた。データセンターとサイバーエージェントビルに、それぞれ1000デバイス監視可能なモデルを1台ずつ、東京・大阪の3拠点に500デバイス監視可能なモデルを1台ずつ、合計5台のCounterACTを配置した。さらにデータセンターにはEnterprise Managerを設置して複数台のCounterACTを統合管理している。

「CounterACTのように検疫とIPSが両方盛り込まれている製品は他にはありませんでした。複数台のCounterACTを配置しましたが、統合管理用のEnterprise Managerを導入したことで、特に運用の手間が増えることなく、集中管理できています」（高場氏）

CounterACTの導入後、ポリシーチェック（検疫）機能で、OSパッチとアンチウイルスの更新を徹底しつつ、IPS機能によって、これまで検知できていなかった感染を多数特定した。ポートスキャンを実行するウイルスや迷惑メールを送るウイルス、Windowsアップデートやアンチウイルスソフトの稼働を阻害するものなどが検疫できたという。

「2ヶ月後には完全にクリーンになり、その後は1度も感染被害は確認していません。ほぼ安全な環境が実現しました」と高場氏は満足げだ。もし、こうした機能をCounterACT以外の製品で実現するとしたら、検疫やIPSに相当する製品を別々に導入し、手間をかけて連携させなければならず、時間もコストもかかり大変な作業になっていたと話す。



豊富な機能を使いこなしてみたいと思わせるCounterACT

「当社のビジネスはスピード感が求められるので、新たな情報システムの導入には構築から運用までいかに迅速に行動できるかが勝負になります。厳しいスケジュールにも関わらず、CounterACTは、構築から運用開始までスムーズに行うことができました」

そう述べる高場氏は、CounterACTはその豊富な機能を使いこなしてみたいと思わせる管理者好みの製品だと評し、今後は業務で利用するスマートフォンの可視化にも対応させたいと、次期バージョンアップを心待ちにしているという。

サイバーエージェントのスピード感を伴ったビジネスにあわせ、ポリシーチェックやIPSだけではなく、スマートフォンを含めた、ネットワーク接続機器の把握という側面からもセキュリティレベルの向上を支えるCounterACTに、大きな期待が寄せられている。

Soliton
株式会社ソリトンシステムズ　http://www.soliton.co.jp/
〒160-0022　東京都新宿区新宿 2-4-3
TEL 03-5360-3811　FAX 03-3356-6354　netsales@soliton.co.jp
大阪営業所 06-6821-6777　福岡営業所 092-263-0400
名古屋営業所 052-963-9700　東北営業所 022-716-0766
札幌営業所 011-242-6111