

媒体名	発行部数	掲載日	掲載面
NETWORK MAGAZINE	20,283	2007年7月号	p.84-88



最終回 検疫ネットワークと ログ管理

従業員や持ち込みPCによる内部のセキュリティが大きな問題となっている。これに対する対策として、今回はWebフィルタリングや情報漏えい対策などを紹介した。最終回はUTMの検疫ネットワークとログ管理機能について見ていこう。

【文●編集部】

持ち込みPCとLAN内のセキュリティ

ネットワークのセキュリティ対策は、これまでインターネットからの攻撃を前提にLANの入り口であるゲートウェイで守りを固めるというアプローチが中心であった。このアプローチの究極の形として、ファイアウォールやアンチウイルス、IDS・IPS、アンチスパムなど複数のセキュリティ対策機能を統合したUTMがあるわけだ。

しかし、ご存じの通り、現在ではゲートウェイだけで防御する方法では、セキュリティは確保できなくなっている。その典型例として挙げられるのが、「持ち込みPC」の問題である。

予算やスケジュールの関係で、PCを導

入できない環境では、私物のPCを業務で使わざるを得ないケースがある。私物PCではなくとも、営業がPCを社外に持ち出し、出先でインターネット接続を行ない、持ち帰ったPCをまた社内ネットワークに接続したり、委託先の業者などが社内ネットワークに接続して、業務を行なうこともあるだろう。

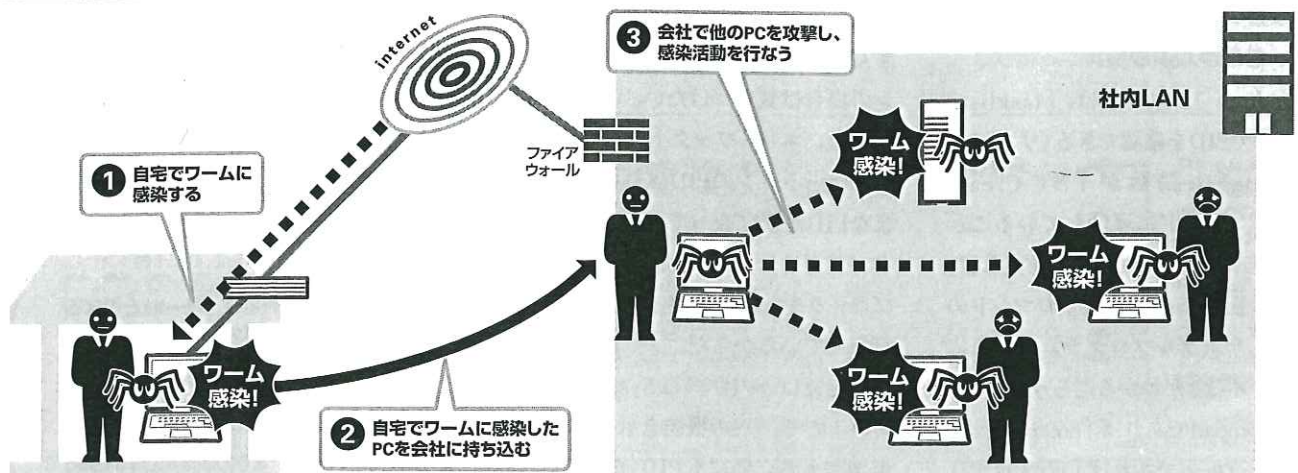
持ち込みPCの問題は、自宅や出先などでウイルス等に感染したPCを、そのまま社内ネットワークにつないでしまうことを指す。社内ネットワークに何の苦もなく侵入したウイルスは、その後他のPCを攻撃したり、データを破壊したりといった悪事を働くわけだ(図1)。

この持ち込みPCの問題は、2003年にMS Blasterが登場した際に表面化し、大

きな被害をもたらした。ファイアウォールなどに守られていることもあり、多くの社内ネットワークでは、アクセス制御はあまり行なわれておらず、セキュリティレベルは概して低い。そのため、持ち込みPCを介して、社内ネットワークに拡がったウイルスは、他のクライアントに感染したり、サーバへの不正アクセスを繰り返したようだ。

また、リモートアクセスVPN経由でも、こうしたウイルス感染の被害が出る。自宅や出張先のPCからVPNで社内ネットワークにリモートログインしてしまうと、持ち込みPCと同じような状態になってしまう。そのため、こうしたVPN経由でのウイルス感染にも注意を払わなければならない。

図1●社内ネットワークへの持ち込みPC



自宅などでウイルス感染したPCを企業に持ち込むことで、甚大な被害が起こる

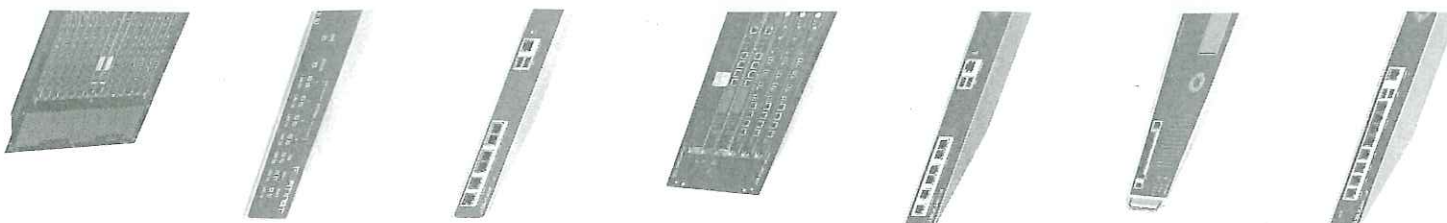
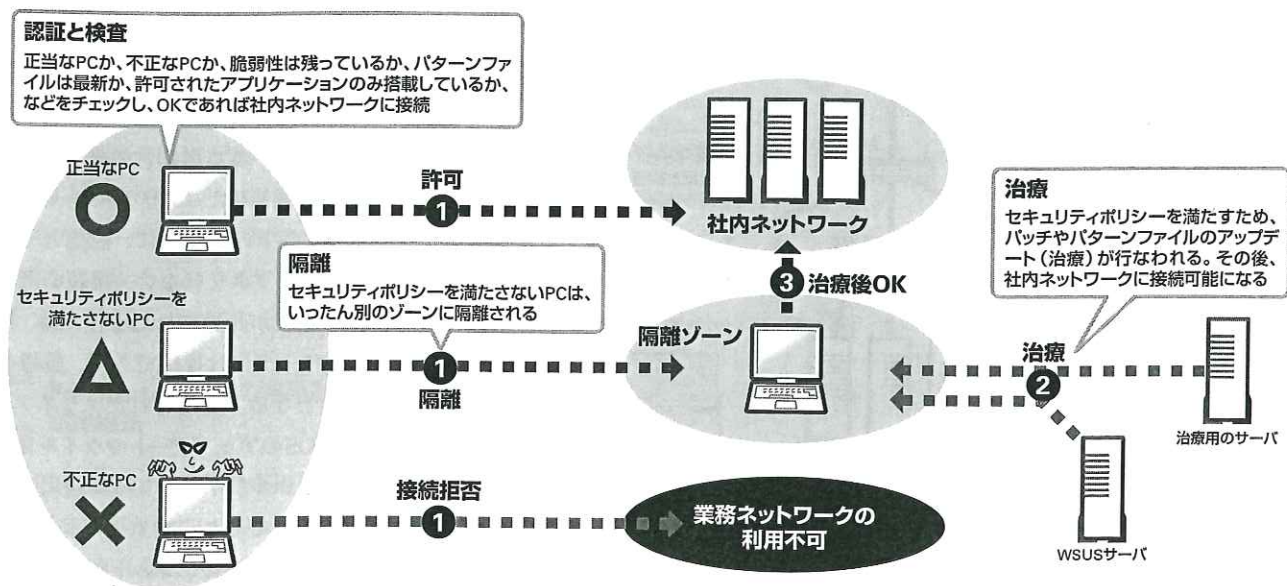


図2●検疫ネットワークの動作



接続時にクライアントPCをチェックし、拒否された場合は隔離。治療して、再度ログインする

社内のセキュリティを確保する 検疫ネットワーク

これに対して登場したのが、セキュリティポリシーを満たすクライアントPCのみネットワークへの利用を可能にする「検疫ネットワーク」である(図2)。

もとより、社内ネットワークで用いるEthernetには認証の仕組みが用意されていない。そのため、スイッチングハブのポートにケーブルを差し込めば、基本的にはどんなユーザーもネットワークを利用することが可能だ。そこで、専用スイッチを用いることで、ネットワーク接続前にユーザー認証を行なう「ネットワーク認証」やユーザーのアクセス権に合わせて異なるVLANに所属させる「認証VLAN*」などのソリューションが生まれた。検疫ネットワークは、これらネットワーク認証や

認証VLANを進化させ、持ち込みPCなどの問題を解決するために登場したものだ。

検疫ネットワークでは、クライアントPCが社内ネットワークに参加する際に、まずユーザー認証を行なったうえで、パッチの適応状況やローカルのセキュリティ設定、プログラムの有無などのセキュリティポリシーをチェックする。この結果、企業が規定したセキュリティポリシーを満たせなかった場合は、社内ネットワークとは異なる別のネットワークに隔離する。そして、OSやアプリケーションのパッチを最新にしたり、不要なプログラムをアンインストールすることで、セキュリティポリシーに適合するように「治療」を行なう。

このように検疫ネットワークの基本的には比較的シンプルだが、実装にはいくつかの種類がある。一般的なのは、クライ

アントPC側のエージェント、社内ネットワークのスイッチと検疫・治療サーバが連携して動作する検疫システムである。IEEE802.1x*などの標準プロトコルを用い、ユーザー認証とセキュリティチェックを元にクライアントPCをVLAN単位で隔離する方法だ。しかし、この方法では社内のスイッチをひとつおき置き換える必要があるため、導入の敷居が高い。

それに対して、最近注目されているのが、専用の検疫用ゲートウェイ装置を用いる方法である。これらの検疫用ゲートウェイ装置をクライアントPCとサーバ間に挟み込むようにして設置すれば、ユーザー認証や検疫を実現できる。クライアントPCの隔離はVLANではなく、偽のARPリプライを用いることで仮想的に隔離する方法がほとんどだ。

最近では、単に検疫だけではなく、ア

注●認証VLAN

認証の結果をもとに接続するVLANを動的に切り替える機能。営業部や人事部などの部署単位であらかじめアクセスできるリソースをVLAN単位で設定しておき、それぞれの部署のユーザーがアクセスしてきた場合は、アクセス権に合わせたVLANを割り当てる。Active DirectoryなどのOSの機能に比べて、より低い層でユーザーのアクセス制御が行なえる。

注●IEEE802.1x

ネットワークを利用する前に、ユーザー認証を行なうために用いられるプロトコル。認証を実現するためには、PC用のソフト(サブリケント)と、認証情報を中継するスイッチや無線LANアクセスポイント(オーセンティケータ)、そしてRADIUSなどのプロトコルに対応した認証サーバが必要になる。

いずれも専用クライアントは不要であるため、容易に検疫ネットワークを導入できる。たとえば、ゲストやパートナーなどの持ち込みPCが接続される可能性の高いサブネットに設置したり、サーバファームの手前に関所として配置したり、さまざまな導入形態が考えられる(図3)。もちろん、WANポートが搭載されているので、小規模なブランチオフィスであれば、これ1台ですべてをまかなうことも可能だ。

FortiGate-224Bの利用と想定用途

FortiGate-224Bの具体的な用途としては、工場で利用されているFAシステムやPOSレジ、ATMなどが挙げられる。こうした機器では組み込み機器向けの

Windowsなどを採用しており、セキュリティソフトやパッチの導入が難しい。にもかかわらず、ダウンの影響がきわめて大きい。そのため、FortiGate-224Bをセグメント単位で導入し、不正アクセスやウイルスの感染を防御する。他のFortiGateと同様、FortiGate-224Bもブリッジとして動作するので、導入も容易だ。

また、セグメント間のセキュリティ強化が重要な箇所でもFortiGate-224Bが役に立つ。従来、セグメント間のトラフィックの制御はレイヤ3スイッチでVLANを構築し、そのVLAN間でパケットフィルタリングを行なうというのが一般的だった。しかし、社員だけでなく外注先の職員、派遣社員、ゲストなど異なるアクセス権を持つユーザーやグループが、社内ネッ

トワークを共用するようになると、静的なフィルタでは管理が面倒になる。まして、ホテルの客室やイベント会場など、被害が他のセグメントに及ぶと大きな問題になるはずだ。こうした場合には、LAN内UTMが必要になるはずだ。



本連載では、フォーティネットの「FortiGate」をベースに、UTMについて解説してきた。複数のセキュリティ機能を統合し、オンラインサービスと連携して最新の攻撃にも対応できるUTMは、既存のファイアウォール・VPN機器の置き換えとして、すでにセキュリティ対策の本命として市民権を得ている。今後はより適用範囲を拡大し、ネットワークに「あって当たり前」の存在」となっていくに違いない。

ログ管理を実現するFortiAnalyzer

インターネットで行なわれる攻撃は多岐に渡っており、最新の脆弱性が狙われる。そのため、単に機器を設置するだけでは、長期的にセキュリティを確保することはできない。攻撃の履歴やトラフィック状態をきちんと調べ、常時セキュリティの強度を確保するというPDCA(Plan-Do-Check-Act)サイクルがきわめて重要になる。また、昨今では「コンプライアンス(法令遵守)」の観点から、ユーザーの利用状況や

攻撃などをリアルタイムに把握し、あとから検証できる体制も必要になっている。

こうした観点で注目を集めているのが、ログ管理である。アクセスログを適切に管理することで、攻撃の履歴はもちろん、ユーザーの利用状況やアクセス頻度などを把握できる。さらに、複数の機器のログを統合的に管理することで、攻撃の手口を分析することも可能になる。

FortiGateでもログの一覧機能は備えてい

るが、記録されるログの量は膨大であるため、ある程度のストレージが必要になる。また、生データを目視しただけでは、全体的な傾向はつかめない。これに対して、フォーティネットでは、「FortiAnalyzer」という専用のログ管理アプリケーションを提供している。

FortiAnalyzerは複数のFortiGate・FortiClientのログをネットワーク経由でローカルのHDDに収集し、一元管理する(図4)。収集されるログは、システムのイベントや攻撃としてフィルタリングされたデータなどで、これを元に複数のレポートを作成できる。攻撃やウイルス、イベントメールやWebの利用状況、帯域利用、プロトコルなど300以上の定型レポートが用意されている。

また、単なるログ収集だけではなく、やりとりされたコンテンツや検出されたウイルスやスパイウェアなどもまとめてアーカイブできるのも特徴。こうしたアーカイブはSOX法などの要件で特に重要になるもので、情報漏えいや犯罪時の証拠収集を実現する「フォレンジック」という用途にも役立つ。さらに、サーバの脆弱性を発見する脆弱性スキャナという機能も備えている。

FortiAnalyzerは接続台数やHDD容量、対応RAIDレベル等によって、100B、800、2000などのモデルが用意されている。

図4●FortiAnalyzerの役割

