はモバイルから、在宅勤務者は自宅のパソコンからと様々な形でネットワークにアクセスすることになります。通常、この規模ですとネットワーク専任の管理者がいないと維持できないのですが、Firebox Xで簡単にセキュアな環境を構築することができました。

また、Webの閲覧規制も、最初はアダルト、ショッピングなど大まかなカテゴリーの設定をしておいて、利用者の細かい要望にあわせて、順次、対応していくことができます。最初に設計を決めて、コンフィグレーションを設定したら変更できない、ということがありません。変えようと思ってもコストがかかるとなると運用が大変ですが、要望にあわせてマウス一つで対応できるので運用も簡単です。

3.ブラックボックスだった利用状況を「見える化」

管理側の視点からいえば、ブラックボックスだった通信トラフィックが目に見えて分かるようになりました。経営者もサーバーのログを見るようになって、内部統制という面でも全社的に意識が高まりました。

4.迷惑メール対策

利用者の視点からいうと、迷惑メールが一切こなくなりました。1日10～15分は、迷惑メールの削除に費やしていた社員もいましたので、人件費なども含めて考えるとこれは大きな効果です。しかも、IT室ではFirebox Xを導入しただけで、迷惑メール対策に関しては、まったく時間を費やしていません。

5.規模の拡張にも柔軟に対応

おかげさまで、当社は人員が増えていますが、会社の経営者は追加投資を嫌がります。もし、スタッフが急激に増えてもモデルのグレードアップだけで、利用者数を増やすことができることも大きなメリットだと感じています。

使い込むほど、製品の良さを実感

— ウォッチガードに期待することや、要望はありますか？

当社は受託製造メーカーのため、お客様のヒット商品や生産量にあわせて製造ラインを組み替えなくてはなりません。

フレキシブルにラインを動かすのであれば、ネットワークもフレキシブルに対応できなくては困ります。また、今後は、インドネシアや中国などのグローバル展開も見据えたネットワークが必要だと考えていました。

自分たちで設定できて、すぐつながって安定して動く。外出先や自宅から高いセキュリティで自由につなぐことができる。この環境をつくるためには、Firebox Xが最適でした。導入して数ヶ月ですが、使えば使うほど、いい製品だな、と実感しています。しかし、分かりやすい反面、マニュアルや教則本が充実していないので、導入セミナーなどがあるといいな、と感じています。もっとメジャーになって欲しい、という期待も込めて、積極的な取り組みをお願いいします。

— お忙しい中、ありがとうございました。

ウォッチガード・テクノロジー・ジャパン株式会社
http://www.watchguard.co.jp
〒150-8512　東京都渋谷区桜丘町26-1　セルリアンタワー15階
Tel: 03.5456.7880　Fax: 03.5456.5511

WatchGuard® Firebox X 導入事例

三生医薬株式会社

「8拠点のネットワークですが専任の管理者など置けません。今回のインフラ刷新では、3人の担当者が兼任で管理できる製品を選びました」

三生医薬株式会社　IT室　室長　堀　敦史氏

健康食品やサプリメントなどのカプセル受託製造専門の三生医薬会社は、通信インフラの老朽化に伴い、ネットワークを刷新。静岡県富士宮市の本社工場をはじめ、関東、関西、東海地区に点在する8拠点を結ぶ仮想プライベートネットワーク（VPN）の構築にWatchGuardのFirebox Xを採用した。ネットワークの構築を担当したIT室　室長の堀　敦史氏に詳しくお話を伺った。

カプセル受託製造専門の三生医薬

— 事業概要についてお聞かせください。

当社は、健康食品などのカプセルの製造を中心に、健康食品、医薬品の受託製造を行っています。当社の名前が表に出ることはありませんが、ソフトカプセル、ハードカプセル合わせて20%前後のシェアをいただいている会社です。

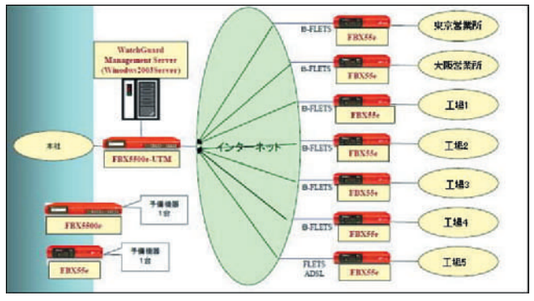
「最先端の製剤技術」「絶対の品質」「信頼される製品」を企業理念として掲げ、研究開発に力を入れています。単にお客様から依頼を受けた製品を提供するだけでなく、新しい製剤技術の開発に積極的に取り組んでいます。たとえば、2007年に、錠剤が小型化できる「タブラート」という製剤技術で特許を取っています。

こうした最新の技術と提案営業というスタイルがお客様に好評をいただき、おかげさまで年々10%売上を伸ばしています。昨年の決算では、99億円の売上を達成しています。

VPNの構築にFirebox Xを選択

— ウォッチガードのどの製品を利用していますか？

2009年7月にFirebox Xを本社の大岩工場をはじめ、東京営業所、大阪営業所を含む全国8拠点に導入し、仮想プライベートネットワーク(VPN)を構築しました。



【構成のポイント】
①UTM利用を想定しFirebox X5500e。またEdgeシリーズもFirebox X55eに統一。
②VPN設定管理も含めWatchGuard Management Serverで全てのFBXを一括管理。
③本社側のFirebox 5500eは予備機器を用意し、東京・大阪はオンサイト保守契約、その他の拠点はFirebox X55eの予備機器を用意することで、ランニングコスト圧縮。

社内プロジェクトをきっかけに、ネットワークを整備

— Firebox Xを導入された経緯を教えてください。


VPNを簡単に構築できるFirebox X。本社工場をはじめ、8拠点で稼働。

現在、当社では2015年までに売上を150億にするという「サン・150計画」を実施しています。このプロジェクトを実現する１つの取り組みとして、2009年6月にIT室が発足。室長として私が就任することになりました。

これまでの5年間、情報システムも、ネットワークも改変をせずやってきたので、早急に情報インフラを見直す必要がありました。現在、営業マンが営業しやすく、管理部門の効率があがるよう情報システムの再構築を推進しています。

最近、当社では九州などの仕事も頂けるようになり、営業エリアが全国へと広がっています。まず、新幹線やホテルでも会社と同じように仕事ができるよう営業マンの情報武装から着手しよう･･･と考えていたのですが、ネットワークに問題があり、着手することができませんでした。今後、IT化を進める上でも現状の通信インフラでは駄目だ、ということで、まずネットワークの整備から始めることにしました。

— 従来のネットワークにはどのような問題点がありましたか？

従来は、VPNが構築できるASP型のサービスを利用していましたが、従来のVPNでは様々な問題があることが分かりました。

1.ネットワークが遅く、コストが高い
ASP型のVPNサービスで光回線を使っていましたが、ネットワークが遅く、その上8拠点で月間10万円のコストがかかってました。しかし、5年契約だったため、解約できずそのまま運用していました。また、外部から社内ネットワークにアクセスするとネットワークがよく切れるという問題がありました。

2.セキュリティサーバーが設置できない
ASPサービスのため、VPNの出入り口にセキュリティサーバーを設置することができませんでした。その代わり、Linuxで構築したプロキシサーバーを介して、インターネットに接続するという方法を使っていました。しかし、前任者が辞めた後は放置状態で管理用のIDもパスワードも分からなくなっており、ブラックボックスになっていました。

3.在宅勤務者のネットワーク参加によるセキュリティ対策のジレンマ
当社には、数名の在宅勤務者がいます。社員が自宅からASP型のVPNサービスにアクセスできるようにするため、パケットIXというサービスを使っていました。このパケットIXは、仮想サーバ上に仮想ハブを設置して、仮想ハブの配下にあるパソコンは、同一ネットワークとしてみなすというサービスです。しかし、ブロックしているはずのメッセンジャーなどが使えたり、もし外部から仮想ハブにつながっても管理側からは全く分からない。情報漏えいや内部統制を図るためのVPNなのに、これでは意味がありません。

4.外出先からVPNにアクセスできない
当社は、提案営業というスタイルのため、営業マンは本社の研究開発部門のデータにアクセスし、その情報をもとに製剤のレシピなどもお客様に提案しています。また、原材料や加工費用などの情報も本社サーバにアップされており、会社のシステムにアクセスしないと見積もりできません。外出先からも処方をつくったり、見積もりを作成できるように、と考えたのですが、ASP型のVPNサービスには、外部からログインすることができないと分かり、断念しました。

5.迷惑メールが非常に多い
迷惑メールが非常に多く、社長の迷惑メールだけで1日に平均300件ありました。長期休暇になると1000～2000件のメールが溜まってしまいます。そのため、発注メールを見落としてしまい、製造開始が遅れてしまったということがありました。

このように調べれば調べるほど様々な問題があることが分かり、早急に何とかしなくては、という状況でした。

簡単にネットワークを構築でき、安定性も抜群

— ネットワークの再構築を検討されたのはいつ頃でしたか。

2009年4月頃からいろいろ調査をはじめて、本格的に検討し始めたのは、IT室が発足した6月からでした。

— 検討する上で、最も重視したポイントを教えてください。

高い安定性があることです。ネットワーク導入にあたっては、当社の規模からランニングコスト、通信速度、安定性を考えてIPSECのインターネットVPNが一番実用性があるだろうと考えていました。ASP型のVPNサービスや専用線を引いてVPNを構築するということは全く考えていませんでした。

— ウォッチガードはどのように知ったのですか？

以前、私は個人資産の投資運用をやっている会社でシステム管理を担当していました。そこでは、ホームトレードのサービスを提供しており、バックボーンにウォッチガード製品を使っていました。その時、初めてウォッチガード製品に触れたのですが、非常に使いやすくて分かりやすい、というのが印象でした。

その会社では、サーバーメンテナンスの検証は2ヶ月かかったのですが、ネットワークの検証は3日で終わりました。直観的に設定できますし、ログサーバで集計だけ見たり、管理しやすい。何よりも、何億円というお客様の個人資産を運用していたという実績から、最初からウォッチガードは有力な候補でした。

— Firebox X Peakを選んだ理由を聞かせてください。

とにかく、操作が簡単なことです。現在、IT室のメンバーは3人いるのですが、システム構築から200台のコンピュータのサポートセンターまで3人で対応しなければなりません。ネットワークだけに手をかけていられないんです。ですから、IT室の3人で制御できることを重視しました。

他社製品も検討したのですが、ネットワーク専任の担当がいないと制御できないため、我々の手に余ってしまいます。何か変更するたびに、いちいち業者に来てもらってお金を払って設定を変えてもらうということはしたくなかった。要はTCOを削減したかったんです。

ネットワーク管理者がいなくても、マウス１つで運用

— 検討から導入に至るまでは、どのような流れでしたか？

セキュリティ機能を統合したUTM製品は、手をかけないと上手く動かないという話を聞いたので、5月の展示会(情報セキュリティEXPO)で実際にデモを見に行ったり、いろいろ評判を聞いたりしました。情報漏えいや内部統制の機運が社内でも高まり、Firebox Xで1回やってみようということで6月中旬に導入を決めました。7月には運用をスタートしていましたから導入は非常にスムーズでした。


「IT化を推進する上で、通信インフラは重要です。早急に整備が必要でした」

— Firebox Xを導入して、実際に感じるメリットを教えてください。

1.TCOの削減
月々の通信コストが約半分になりました。年間で約50万円の削減です。これに加えて、ファイアウォールを構築した場合を想定すると、200クライアントのライセンスフィーなどで600～700万円の削減に相当すると感じています。

2.ネットワーク管理者がいらない
当社は、本社工場をはじめ、8拠点の営業所、さらに営業マン