



WatchGuard ソリューションガイド： 中小企業のための10の情報セキュリティ・ソリューション - シンプル、ローコスト、パワフル、だから安心 -

企業規模にかかわらず、インターネットというオープンなネットワーク環境を安全に利用するためには、セキュリティが不可欠なものとなっている。予算が限られた中小規模の企業にとっては、セキュリティのコストをいかに削減し、かつ高度なセキュリティを手に入れるかが重要課題となっている。

複数のポイントソリューションを完璧に設定することは、経験豊富なセキュリティの専門家でなければ不可能である。場当たり的なポイントソリューション導入では、導入の時点で完璧でも、一年もすればセキュリティホールがいくつも生まれてくる。

本ソリューションガイドは、UTM(Unified Threat Management = 統合脅威管理)に総称される統合セキュリティ・アプライアンスを最先端でリードする WatchGuard Firebox が実現する10のセキュリティ・ソリューションを紹介する。WatchGuardを活用することによって、この10のセキュリティ・ソリューションを一台のアプライアンスで、シンプル、ローコスト、そしてパワフルに実現することが可能である。

目次

ソリューションガイド1: 情報漏洩対策	2
ソリューションガイド2: ホスティング企業でのセキュリティ対策	3
ソリューションガイド3: P2P(Winny)対策	3
ソリューションガイド4: パグ/セキュリティホール対策	4
ソリューションガイド5: スパムメール対策	5
ソリューションガイド6: URLフィルタリング	6
ソリューションガイド7: VLANセキュリティ対策	7
ソリューションガイド8: FSM(Firebox System Manager)活用ガイド	7
ソリューションガイド9: 増加するHTTPアクセス要求への対策	9
ソリューションガイド10: VPN冗長化対策	9
まとめ	10

ウォッチガード・テクノロジー・ジャパン株式会社
2008年10月

ソリューションガイド1: 情報漏洩対策

NPO日本ネットワークセキュリティ協会の「2007年情報セキュリティインシデントに関する調査報告書」によると、漏洩人数が3,053万1,004人、想定損害賠償総額が2兆2,710億8,970万円、1件当たりの平均想定損害賠償総額が27億9,346.8万円となっている。インシデントの件数は864件となっているが、これは氷山の一角であり、実際にはこの数十倍の数に上ると推定される。前年度との大きな違いは一人当たりの平均賠償総額が増えていることである。これは、情報の価値が毎年上昇していることを意味する。この賠償総額を見れば、情報漏洩は企業の経営を揺るがす大きな問題であることは明白である。たとえば、3万件の個人情報が漏洩したとすると、平均の賠償総額は1億円を超えることになるが、中小企業にとっては、会社を倒産に追い込む数字といっても過言ではない。

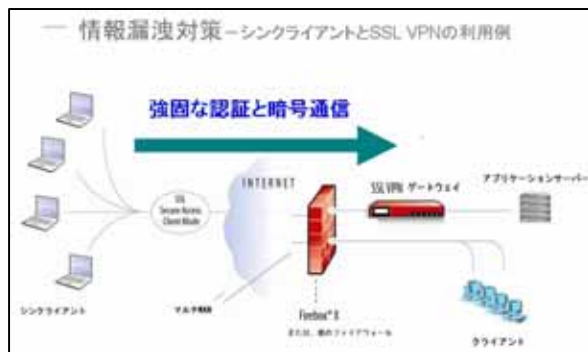
漏えい人数	3,053万1,004人
インシデント件数	864件
想定損害賠償総額	2兆2,710億8,970万円
一件当たりの漏えい人数 ^{※1}	3万7,554人
一件当たり平均想定損害賠償額 ^{※1}	27億9,346.8万円
一人当たり平均想定損害賠償額 ^{※2}	3万8,233円

出典: 『2007年情報セキュリティインシデントに関する調査報告書』
NPO 日本ネットワークセキュリティ協会

情報漏洩は企業の規模には全く関係がなく、様々な規模の企業で発生している。取引先リスト、顧客リスト、セミナー参加者リスト、メールニュース配信リスト、社内機密データ、人事情報など、対象となるものは多岐にわたる。万が一、情報が漏洩してしまえば、多大な賠償金だけではなく、企業のイメージダウンを招き、顧客や取引先を失うことになる。情報社会においては、情報漏洩は企業生命の危機を引き起こすことになる。

情報漏洩の原因を確認してみると、ネットワーク経由以外では、紙媒体の流出、パソコンの盗難や置き忘れ、USB

メモリやディスクの消し忘れなど、物理的に情報を紛失または流出させてしまう場合がある。ネットワーク経由では、誤動作や設定ミスによる流出、ソフトウェアのバグやセキュリティホール、ワームやウイルスの感染がある。誤動作のほとんどは、メールの間違った配信先への送付である。



WatchGuard Fireboxを活用することによって、様々な方法で情報漏洩への対策が可能となる。Fireboxは、従来のファイアウォールとは異なり、アプリケーションレベルでプロキシの設定が可能である。たとえば、EXEファイルの添付があるメール配信を拒否するように設定することができる。これにより、メールの誤配信によるデータの流出を防ぐことが可能となる。また、ウイルスやワームの拡散については、ゲートウェイ・アンチウイルスの機能を使うことで、社内から外へ出ることを防ぐことができる。さらに、ウェブ経由の情報漏洩はWebBlockerを使って防御することもできる。また、ユーザー認証により、ユーザー毎のアクセス管理を行うことが可能になる。WatchGuard Fireboxでは、モバイルユーザーVPNのほか、SSL-VPNとPPTPをサポートしているので、基本的なユーザーアクセス管理を可能にしている。たとえば、上の図に示すように、WatchGuard Fireboxを導入すれば、簡単にシンクライアントの環境でSSL-VPNを実現することができる。

ソリューションガイド2: ホスティング企業でのセキュリティ対策

中堅・中小企業でのホスティング・サービスの利用率は、大企業を大幅に上回る。ホスティング・サービスを利用している企業は、次のような特徴を持っていると思われる。

- サーバーを外部に委託しているため、外部から内部へのアクセスはないと安心している。
- ISPのスパム対策を利用するしか選択肢がないと考えている。
- 社内のトラフィックを把握していないので、P2Pに利用されていても気づいていない。
- 管理者がいない、または管理者は存在するが他業務と兼務している。



このような環境では、単に外部から内部へのアクセスを禁止するだけでは不十分である。たとえば、P2Pやメール添付ファイルのサイズなどを制限していないと、突然、トラフィックが一杯になるといったトラブルが発生する。

Fireboxを利用することで、P2P対策を行うだけではなく、特にホスティング・サービスを利用している環境に特化した様々なセキュリティ対策を施すことが可能である。たとえば、POP3でメールを取得する場合、ウイルスとスパムの検査。また、シグネチャーベースのアンチウイルスだけではなく、Outbreak Virus Detection機能を利用して、現在流行しているウイルスを検知して即座に遮断することが可能となる。

また、管理者不在が多いホスティング環境では、デフォルトのセキュリティを高めておくことが望ましい。たとえば、Fireboxでは、実行形式ファイルを削除して、受信しないようにするなどの設定をデフォルトにすることができる。

ほとんどの場合、ホスティング環境では、ウェブ経由のアクセスを許可している。従来は、ウェブアクセスによってウイルスやスパイウェアが侵入するケースは少なかったが、最近になってウェブ経由での侵入は一般化している。Fireboxによって、ウェブアクセスをチェックして、ウイルスやスパイウェアの遮断が必要となる。また、メールの場合と同様に、実行形式のファイルのダウンロードを禁止することでセキュリティを強化することが可能である。さらに、インスタント・メッセージング (IM) も禁止することが望ましい。IMの利用が、業務以外の私用であることも多い。Fireboxによって、IMを簡単に利用禁止することができる。

自社管理とホスティング環境では、社内とインターネットの境界は同じである。したがって、セキュリティ対策はクライアント、サーバー、境界のすべてに対して継続的に必要である。Fireboxを導入することで、社内とインターネットの境界線、スパム対策、ウイルス対策、ウェブフィルタリングを事前に行うことは、更なるコスト削減につながる。

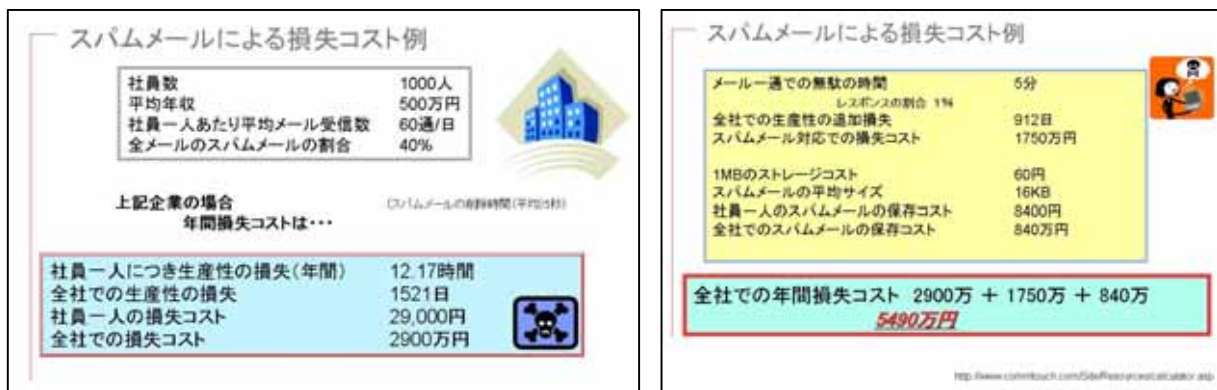
ソリューションガイド3: P2P (Winny) 対策

P2P (Winny) とはインターネット経由で不特定多数のコンピュータ間でファイルの交換を行う仕組みを提供するソフトウェアであるが、P2Pに関連する個人情報流出の事件は毎月多数発生し、大きな被害が報告されているほかに、音楽や映画などの著作権があるデータを違法に交換する温床となっており、大きな問題となっている。P2Pアプリケーションはポートをオープンにし、サーバー的な動作をする場合が多い。映画など大きなファイルをダウンロードする場合、ポートが長時間にわたり、オープンされたままの状態になる。この場合、アプリケーションにセキュリティホールが存在すると、ワームやウイルスの感染が拡大する脆弱性を持つことになる。Antinnyなどといったウイルスが仕込まれ、デスクトップやマイドキュメント内のファイルを無断でWinnyを通してダウンロードすることで、機密情報を容易に手に入れることが可能となるのである。

Fireboxを導入することで、IPSのシグネチャーベースの防御システムを利用して、既知のP2Pソフトウェアを遮断することが可能となる。また、HTTP、HTTPS、SMTP、POP3などのプロキシ設定によって内部から外部への通信を許可することで、プロキシで設定されていないプロトコルを使用するWinnyなどのP2Pソフトウェアを遮断することができる。

ソリューションガイド5: スпамメール対策

最近の調査では、スパムメールは受信メールのほぼ半分に相当すると指摘されている。また、全メールの63%がスパムメールであるという報告もある。企業のコミュニケーション・ツールとしてメールは不可欠なものとなっている今、スパムメールへの対策に多くの企業が頭を悩ませている。ISPを中心にスパムメールを排除する活動は実施されているものの、依然としてスパムメールは増加傾向にある。スパムメールがもたらす弊害には、「スパムメールを処理する時間の無駄」が筆頭にあげられるが、ビジネス現場に流れる有害コンテンツも有害サイトへの誘導やフィッシングサイトへの誘導など、さまざまな悪影響を与えている。さらに、ネットワーク・帯域幅やディスク容量の浪費にもつながっている。スパムメールによる損失コストを試算してみると、社員数200名、平均年収500万円、社員一人あたりメール受信数100通/日、全メールのスパムメールの割合50%とすると、なんと企業の年間損失コストの総計は2200万円を超える。これは、スパムメール対策が中堅から中小企業でも不可欠になっていることを明らかにしている。



しかし、さまざまな国からさまざまな言語で発信されるスパムメールへの対策は簡単ではない。また、画像メールなどさまざまな形態で発信されてくる。ブロックするキーワードを日々登録しても受信スパムメールは一向に減らない。

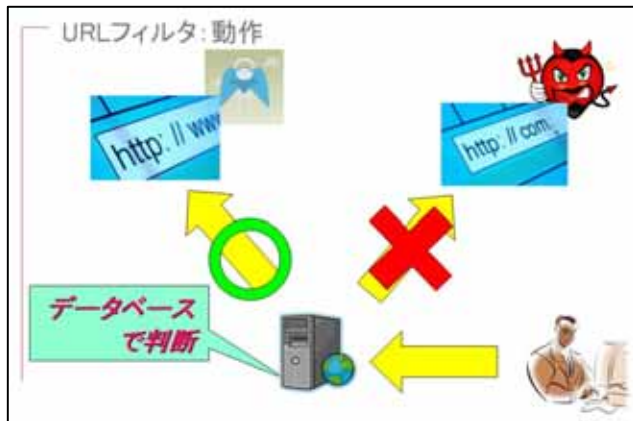
このスパムメール対策として注目されているのが、WatchGuard Fireboxである。Fireboxに標準搭載されたアンチスパム・ソリューション「spamBlocker」は2,000万ものスパム判定基準を管理する業界最高水準のCommtouch社のスパム検知エンジンを採用している。SMTP/POP3対応、日本語対応、隔離対応、レポート対応といった機能をサポートしている。Fireboxの優位性は、画像メール対応、言語に依存しない検知に加えて、シグネチャーベースのアンチウイルスだけでなく、Outbreak Virus Detection機能という現在流行しているウイルスを検知して即座に遮断する機能をサポートしていることである。これにより、97%以上の高い検知率を達成している。



もう一つの優位性は、簡単な導入と設置である。左に示す設定画面を指定するだけでよい。後は、Commtouchのスパム検知エンジンがリアルタイムにスパムメールを検知、隔離してくれる。さらに、スパムメールのDNAを分析することで、未知のスパムメールへの対応が可能になる。

ソリューションガイド6: URLフィルタリング

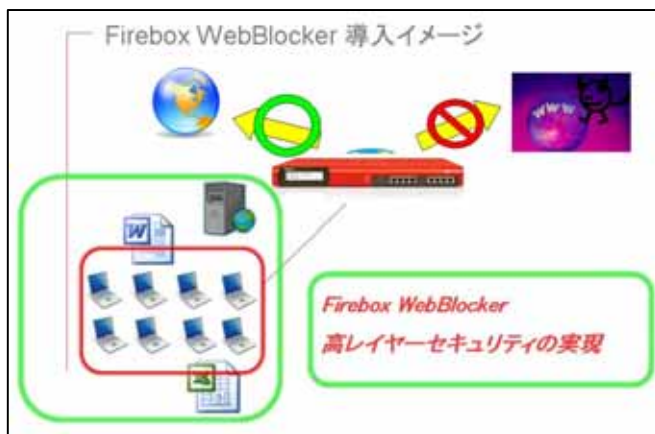
自由に書き込み、閲覧させることで、さまざまな情報を入手し、新しい発想を創出することを可能にすることが本来のインターネット活用の意義である。しかしながら、この自由の代償として、有害なサイトや情報漏洩、ウイルス感染などの危険やリスクをもたらす。たとえば、掲示板や裏サイトなどへの書き込みによって、企業や政府機関などで情報漏洩や信用・企業ブランドの失墜などといった問題を引き起こしている。また、教育現場では、いじめの温床となっていると指摘されている。このような中、多くの企業、官公庁、学校でURLフィルタの導入は進んできているが、50%以上の企業はまだURLフィルタを導入していない。



ここで、URLフィルタの仕組みについて考えてみる。URLフィルタは、有害あるいは業務に無関係なサイトへのアクセスを遮断するソフトウェアである。たとえば、管理者が「ギャンブル」に関するサイトの閲覧は禁止したいと考えたら、URLフィルタで「ギャンブル」カテゴリの閲覧を禁止する設定を行う。こうすることで、エンドユーザーは、ギャンブルに関するサイトのURLをブラウザに入力しても、ギャンブル関連のサイトへはアクセスできなくなる。「どのサイト(URL)がどのカテゴリに該当するのか」は、データベースとしてURLフィルタ製品に組み込まれている。このデータベースは、ほとんどの場合、URLフィルタリングベンダーが提供する。

新しいサイトは次から次へと生まれるので、データベースを絶えず更新する必要がある。このため、ほとんどの製品が、インターネット経由で自動的に最新データベースをダウンロードする更新機能を持つ。このデータベースの品質がURLフィルタリングの精度を決めることになる。

一般的なURLフィルタの問題点には、(1)データベースに登録されていないサイトはアクセスできてしまう、(2)掲示板への書き込みなどのコマンドを管理できない、(3)ファイルのダウンロード・アップロードの管理ができない、などがある。



FireboxのWebBlockerの優位性は、プロキシベースのファイアウォールの特性を生かすことで実現している。たとえば、フィッシングサイトへの対応、スパイウェア感染サイトへの対応、データベース未登録サイトの拒否、特定掲示板の書き込みの拒否・許可、ワード・エクセルファイルなどの拒否・許可を可能にしている。

FireboxのWebBlockerでは、URLフィルタリングのデータベースとしてこの分野のリーダーである Websense/SurfControl を採用している。HTTP/HTTPSに対応、54カテゴリをサポート、ポートも任意に設定可能(8080など)、言語に依存しない対応、各種レポート、スケジューリング機能などを提供している。

FireboxのURLフィルタリング機能は、アプリケーション層までサポートするWatchGuardの先進UTMアーキテクチャを最大限に活用し、高レイヤのセキュリティを実現している。

ソリューションガイド7: VLANセキュリティ対策

VLAN(仮想LAN)とは、クライアント端末を論理的にグループ化することである。これにより、端末の物理的な場所に依存することなく、ネットワークを構成することができる。部門間でアプリケーションサーバーのアクセスを制御し、内部の不正情報アクセスを防止できる。また、同時に、ウェブサーバー、メールサーバー、ファイルサーバーなど全社で共有できるリソースを一括管理することを可能にする。



中小規模の企業においても、VLAN構成は採用する企業が増えているが、セキュリティ面で問題を抱えている。たとえば、営業部のある端末がウイルスに感染した場合、この感染は営業部内だけではなく、共有のメールサーバーを経由して、全社へ2次感染する恐れがある。

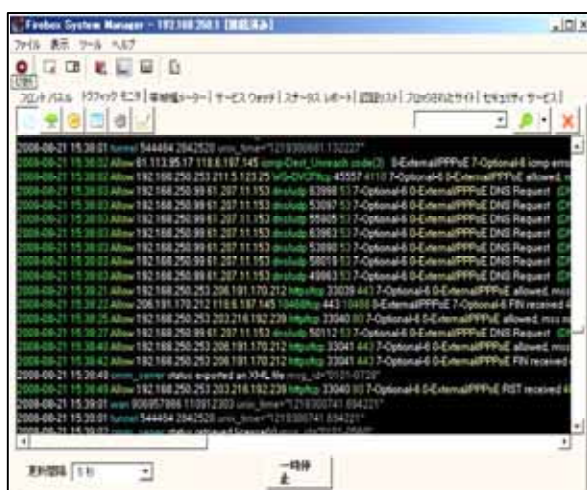
このような場合、Fireboxをレイヤ3スイッチと置き換えて、Fireboxのアンチウイルス機能を使うことによって、営業部外へのウイルス感染を防ぐことができる。

FireboxはVLANネットワークへ導入が可能である。IEEE802.1Qに準拠しており、サブVLANのテクノロジーをサポートしている。高レイヤのセキュリティを1台で

可能にし、また、QoS対応もサポートしている。IPネットワークの普及に伴い、多くの企業がIP電話やソフトフォンを採用している。これに関連して、多くの企業がこれまでのデータネットワークと音声と画像通信を統合するためにユニファイド・コミュニケーション・ネットワークの構築を開始している。QoS対応のFireboxは、このUCネットワークのスイッチとして利用することができる。

ソリューションガイド8: FSM(Firebox System Manager)活用ガイド

FSM(Firebox System Manager)は、WSM(WatchGuard System Manager)に含まれる標準のツールとして提供される。Firebox上でどのような通信が行われているかをリアルタイムに監視し、その状態を可視化できるので、Fireboxの特長の1つである「見えるファイアウォール」を実現している。

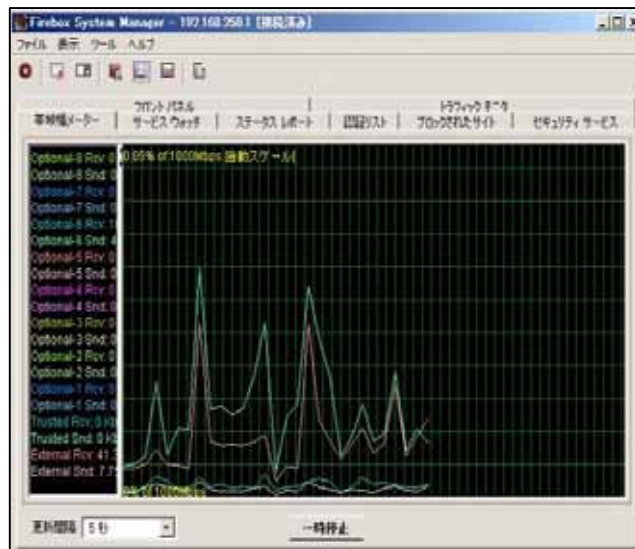
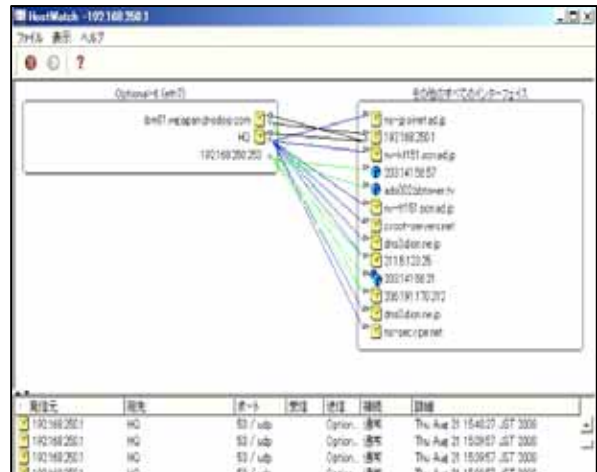


リアルタイムトラフィックモニタ

リアルタイムにFireboxを通過するログを目視しながら監視することができ、問題のある端末、パケットの判別、他のネットワーク機器を導入した際のトラブルシューティングなどに活用できる。たとえば、異常に通信量の多い、しかも赤字で拒否されている端末がある場合は、ウイルス感染の可能性など問題のある端末を確認したりできるほか、パケットの到達状況を確認することでネットワークのトラブルシューティングに活用できる。

ホストウォッチ

Fireboxに接続されている端末から外部への接続先をリアルタイムに監視することが可能。この画面からブロックサイトとして追加することもでき、問題のある通信を即座に遮断可能。線の色によって、接続の形態を確認でき、線の色でどのような通信かを一目で判断することができる。たとえば、黒の場合は通常の接続、緑の場合はNATを使った接続、青の場合はプロキシを使った接続、赤の場合は拒否された接続である。



帯域幅メーター

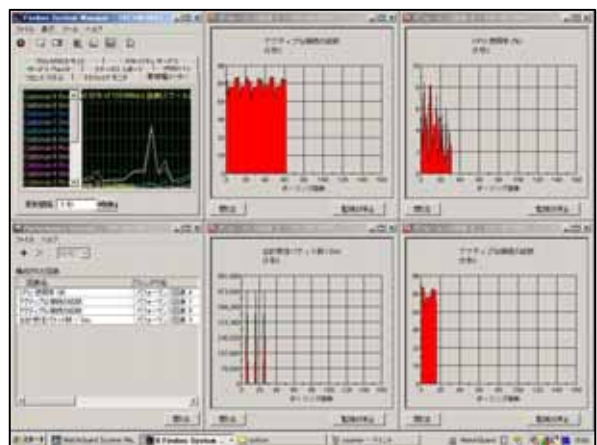
Fireboxの各ポート別にどれだけ帯域を使用しているかをリアルタイムに表示する。通常の帯域使用量を把握していれば、これに対して異常な値が発生した場合は何かネットワークに問題が発生していることを予測できる。また、この機能は、音声通信の帯域幅を確保することに活用でき、QoSの管理に応用可能である。

サービスウォッチ

Fireboxに設定されているファイアウォールポリシーごとにどのサービスがどれだけ帯域を使用しているかを表示できる。異常に帯域を使用しているサービスに問題が発生していることを予測できる。また、サービスごとの表示が可能なので、ネットワーク全体の評価、内部サーバーへのバランシング計画などへの応用が可能である。

パフォーマンスカウンタ

リアルタイムのモニタリングに加えて、FSMではパフォーマンスカウンタを備えている。リアルタイムのモニタリングは確かに便利だが、四六時中モニタの前に張り付いているわけにはいかない。パフォーマンスカウンタは、長期的なパフォーマンスデータを収集でき、長期的にトレンドを分析できる。アクティブな接続の総数、CPU使用率といった測定したい希望する項目を設定して、記録できる。右図のような、視覚的な表に表示するほか、CSVデータで書き出すことも可能である。



ソリューションガイド9: 増加するHTTPアクセス要求への対策

ウェブサイトへのアクセス件数は日々増加している。ウェブサイトは単なる情報発信の手段からビジネスの戦略ポイントへ進化している。ウェブサイトを守ることは、ウェブ上でビジネスを展開する企業にとって業務に大きな影響を与えることとなる。この対策として、多くの企業がロードバランシングを導入している。しかし、ロードバランシングは高価なものであり、簡単に導入することができない。

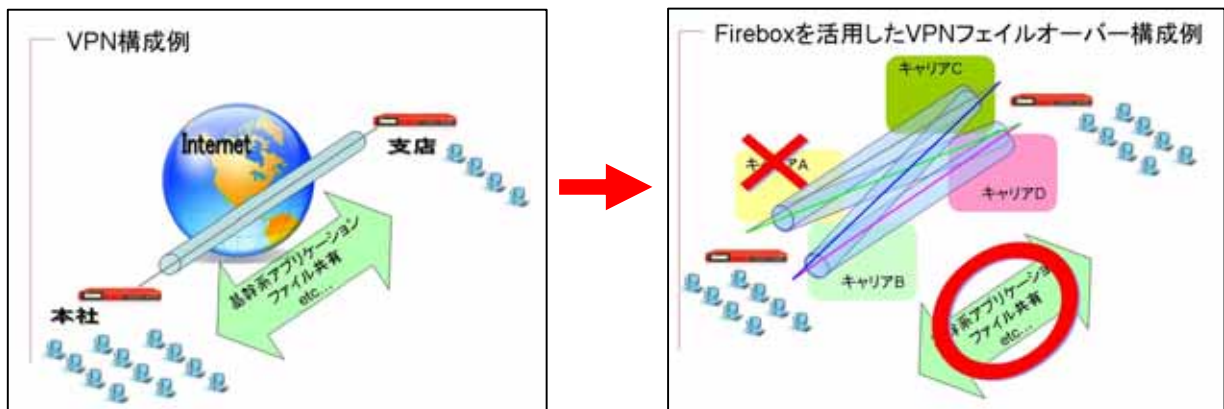


ルーター機能、ファイアウォール機能、ロードバランシング機能のすべてを併せ持つFireboxを活用した場合、一台に集約することが可能になる。一台に集約することで運用コスト削減に加え、管理負担も軽減できる。

ソリューションガイド10: VPN冗長化対策

今、多くの企業で本支店間をVPN接続で結ぶことが一般化している。ほとんどの企業が一つのキャリアに依存し、冗長構成をとっていない。この場合、万一、契約のキャリアのネットワークがダウンしてしまうと、本支店間を接続することができなくなる。

この対策として、本支店にそれぞれ1台のFireboxを導入することで、安く、簡単に対処することが可能である。事業継続計画においても、VPNの冗長化は不可欠の要件となっている。



まとめ

ますます進展するネットワーク社会。そして、ますます複雑化するネットワーク環境。その中で、ネットワークセキュリティにかかる労力と費用はますます増大している。WatchGuardは、この課題にシンプルに答えている。

WatchGuardが提供するUTMアプライアンスFireboxは、中小企業に対し、情報漏洩対策をはじめP2P (Winny)対策、スパムメール対策、URLフィルタリングなど一連のネットワークセキュリティを実現するソリューションである。更に、VLAN構成、ロードバランシング、VPN冗長化などの基本的なネットワーク設定機能も1台のUTMアプライアンスで提供できる。

ここで紹介した10のソリューションを1台のFireboxにシンプルに統合したWatchGuardは、インターネットというオープンなネットワークを安全に利用できるよう、これからのネットワークセキュリティをリードしていく。中小企業でのネットワークセキュリティの実現には、シンプル、パワフル、そしてローコストのWatchGuard UTMアプライアンスFireboxが最適で、中小企業にネットワーク活用での安心感を約束する。

ウォッチガード・テクノロジー・ジャパン株式会社

〒102-0083 東京都千代田区麹町3-12-12 麹町Mビル2階
TEL. 03-5275-5261 FAX. 03-5275-5262
Web: <http://www.watchguard.co.jp> e-Mail: info-jp@watchguard.com

WatchGuard Technologiesについて

ウォッチガード・テクノロジー社は、1996年から信頼性が高く管理しやすいセキュリティ・アプライアンスを世界中の何百何千もの企業に提供しています。Firebox Xシリーズの統合脅威管理 (UTM) ソリューションは、強力で信頼性の高いマルチレイヤのセキュリティと各用途において、最高の使いやすさと最良の組み合わせを提供します。弊社の最新製品シリーズ、WatchGuard SSLはネットワークのサイズにかかわらず、安全なリモート・アクセスを簡単に手頃な価格で提供します。全製品は革新的なサポート、メンテナンス・プログラムを提供するLiveSecurityサービスによってバックアップされています。ウォッチガードは株式非公開の米国ワシントン州シアトルに本社を置き、北アメリカ、ヨーロッパ、アジア太平洋、ラテンアメリカ全域に支社があります。詳細はウェブサイト<http://www.watchguard.co.jp>をご覧ください。

同資料における表現に保証はありません。全仕様書は変更される可能性があり、今後の製品や機能などの利用状況については弊社の意向に基づき提供します。

©2008 WatchGuard Technologies, Inc. 無断複写・転載を禁じます。WatchGuard、WatchGuardロゴ、Firebox、LiveSecurityは、米国ウォッチガード・テクノロジー社の米国およびその他の国における登録商標または商標です。その他すべての商標および商標名は各所有者に権利があります。

Part.No.WGPE66567_072408
