ネットワークマガジン
NETWORK MAGAZINE

情報漏えい対策に「UTM」は使えるか？

これからはWinnyやIMの制御も重要

個人情報保護法の施行やWinnyを媒介とした暴露ウイルスの蔓延で、情報漏えい対策への注目がかつてないほど高くなっている。もちろん、各社さまざまなソリューションを出しているが、注目を集めているのがUTM装置による情報漏えい対策である。

もう手をこまねいていられない情報漏えい対策

昨今、WinnyやShareなどのP2Pソフトを媒体とした暴露ウイルスによる情報漏えい事件が、毎日のように誌面をにぎわせている。こうした暴露ウイルスによって、顧客名簿や企業の重要な情報がいったんインターネットに流出してしまうと、もはや回収や削除はできない。機密情報が暴露されたり、社会的な信用を落としたり、業務に大きな影響を与えることになってしまう。多くの事件の例を見るまでもなく、金銭的な被害は比較的早く取り戻せたとしても、社会的な信用を回復するのは容易ではない。そのため、企業のネットワーク・セキュリティ管理者は、いち早くこうした情報漏えい対策を実践しなければならない。

こうした情報漏えい対策としては、盗難などに遭わないようパソコン自体の扱いに気を配ったり、扱っているデータを暗号化するという方法が挙げられる。また、サーバやデータベースへのアクセスを細かく制御するといった方法が挙げられる。だが、もっとも手っ取り早い対策としては、Winnyのトラフィック自体を遮断する方法になるだろう。現状、Winnyの正否はともかく、企業においては、今のところWinnyを使うべきビジネス的な理由が見あたらないからだ。そのため、Winnyのトラフィック自体を遮断してしまえれば、企業としては十分な対策になるはずだ。

しかし、既存のセキュリティ機器では、Winnyの遮断は行なえなかったのが実態である。これはWinnyというアプリケーションの特殊性に起因する。

既存のセキュリティ機器ではWinnyを遮断できない

今まで多くの企業では、インターネットとLANの間にゲートウェイとしてファイアウォールやアンチウイルスなどを設置し、セキュリティを確保していた。しかし、こうしたゲートウェイでのセキュリティにはWinnyに対して十分対抗できない（図1）。

まず、Winnyでは空いているポートを任意に使用するため、特定のポートを閉じることで通信を遮断するタイプのファイアウォールやルータではWinnyは止められない。当然、すべてのポートを塞いでしまえば、TCP/IPアプリケーションは利用不可能になるため、ポートを元にWinnyを止める方法は採れないことになる。

また、通常のアンチウイルスゲートウェイは、HTTPやメール、FTPなどのプロトコルしかチェックしないので、Winny経由で拡散するウイルスを捕捉するのは不可能だ。しかも、Winnyの通信は暗号化されているため、通信データの中身を監視することでWinnyの利用を検出するのは難しい。

もちろんP2Pに対応しているゲートウェイ製品もあるが、外資系ベンダーで国産のP2PであるWinnyに対応している製品を出しているところは皆無といってよいだろう。そのため、今まではアンチウイルスソフトで対応するのがほとんどであった。Winnyを止めるのではなく、あくまで

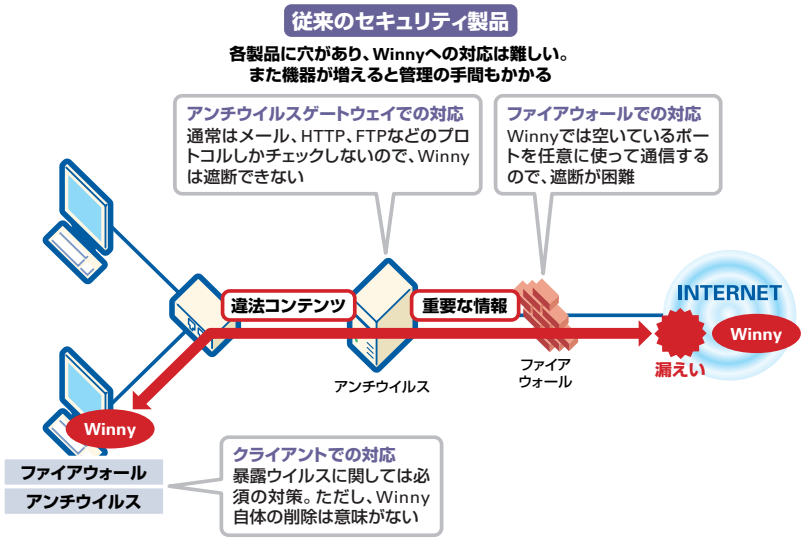


図1●Winnyへの対応が難しい既存のセキュリティ製品

暴露ウイルスに焦点を当てたわけだ。この方法であれば、暴露ウイルス自体を駆除できるが、アンチウイルス製品が導入されていないPCもあるし、企業内のPCのパターンファイルを一様に更新させるのは一苦労である。

その他、Winny自体をウイルスとして検出したり、使用できなくするという方法もある。しかし、自らの意思でWinnyを使っているユーザーに対しては、効果は薄いといわざるをえない。

最新のUTM「FortiGate」でWinnyを止める

こうした中、情報漏えい対策の切り札として注目を集めているのが、フォーティネットの「FortiGateシリーズ」だ。

FortiGateシリーズは、ファイアウォールやVPN、IDS・IDP（不正侵入検出・防御システム）、アンチウイルス、アンチスパム、コンテンツフィルタリングなど複数のセキュリティ機能を単一のハードウェアに搭載したUTM（統合型脅威管理）装置である。

UTMでは複数のセキュリティの脅威に1台で対抗できるため、管理の手間も大幅に軽減される。また、複数の機器を数珠つなぎ型で設置すると障害箇所が複数に分散してしまうが、UTMであれば1箇所に統一される。障害箇所の特定も容易になるし、サポート窓口も一本化できる。

こうしたメリットからUTMは、ファイアウォールに変わるセキュリティ対策の要として、注目を集めている。このUTMを他社に先駆け製品化したのがフォーティネットであり、その意味ではFortiGateはUTMの代名詞とすらいえるのだ。

FortiGateで画期的だったのは、今までソフトウェアと汎用CPUでしか実現できなかったウイルススキャンやWebフィルタリングが、ASICによりハードウェア処理できるようになったという点だ。これにより、パフォーマンスは既存のソフトウェアに比べ大幅に向上し、複数のセキュリティ機能を搭載することで処理能力が低下するというデメリットがなくなったのである。

写真●SOHOからキャリア向けまで幅広い製品を揃える「FortiGateシリーズ」

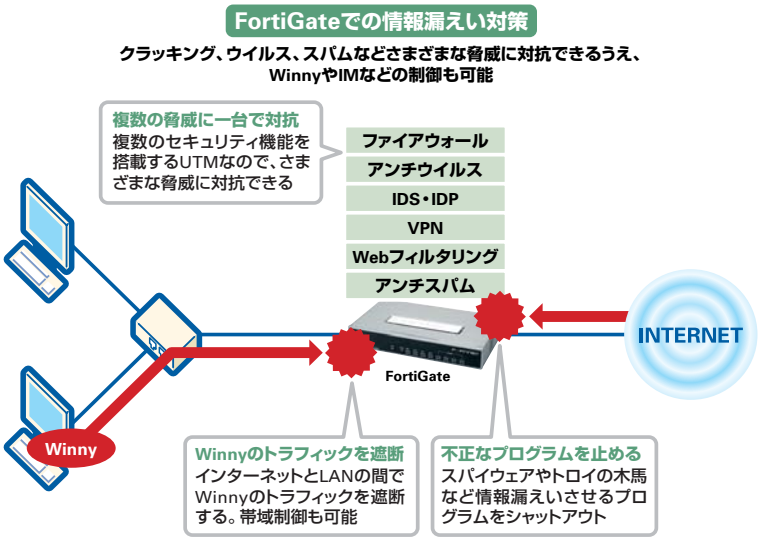


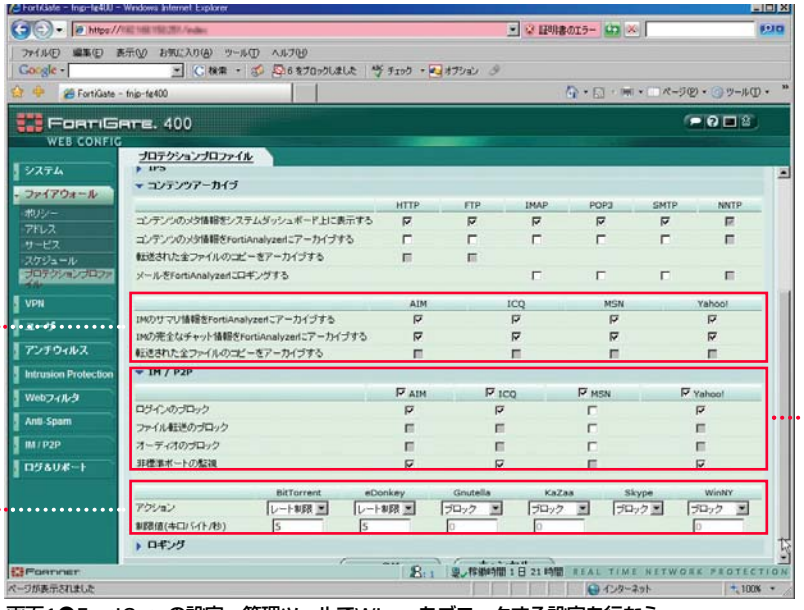
図2●Winnyの遮断やその他の情報漏えい対策を持つFortiGateのメリット

もちろん、古くから提供されているだけに、FortiGateは製品ラインナップも豊富だ。エントリーモデルのFortiGate 50A/60/100Aのほか、ミッドレンジのFortiGate 200A/300A/400A/500A/800、ハイエンドモデルのFortiGate 1000A/3000/3600/5000シリーズなどで、これらはそれぞれの顧客ニーズに合わせた筐体と処理能力を持ったハードウェアで構成されている。そして、こうしたハードウェアプラットフォームには、共通で「FortiOS」と呼ばれる堅牢で拡張性の高いソフトウェアが搭載されている。このFortiOSとASICが協調動作することで、あらゆるセキュリティの脅威を水際でストップできるようになっているのだ。

こうしたFortiGateの実績は国内でも高く、特にセキュリティ対策に大きなコスト

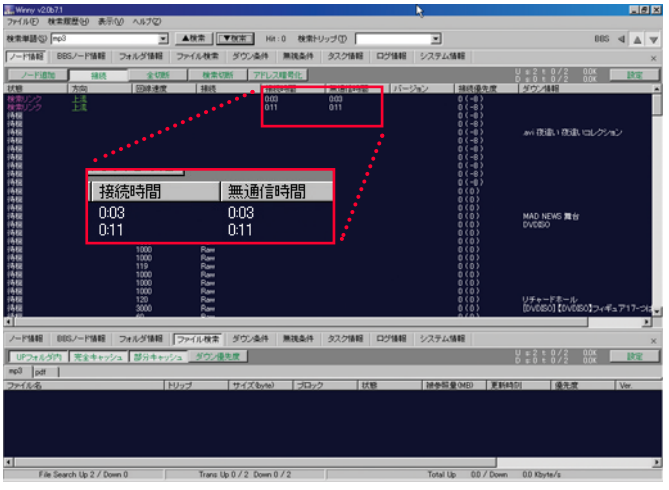
コンテンツアーカイブ
IMのチャット内容や転送ファイルを外付けの「FortiAnalyzer」にアーカイブすることも可能

P2Pはブロックと帯域制御
P2Pに関しては、ブロックとレート制限という2つのアクションがとれる

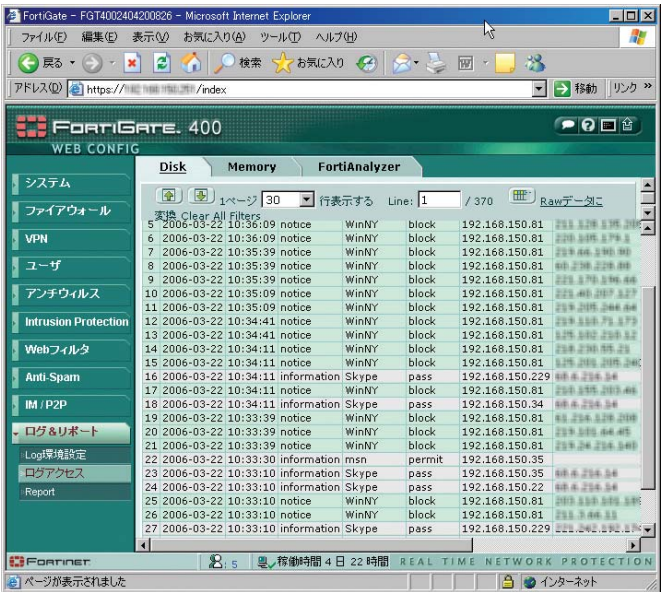


IMの動作を制御
IMに関しては、ログインやオーディオやファイルの転送などをチェックボックスで細かく制御できる

画面1●FortiGateの設定・管理ツールでWinnyをブロックする設定を行なう



画面2●Winnyがブロックされているところ。接続が完全に遮断されている



画面3●設定・管理ツールでは、WinnyをブロックしたIPアドレス等も一覧できる

のさけないSOHO・中小企業では圧倒的なシェアを誇っている。

では、FortiGateの情報漏えい対策機能はどのようなものだろうか？（図2）もとよりFortiGateには、ユーザーの情報を漏えいさせるスパイウェアやトロイの木馬の侵入を遮断するアンチウイルスのほか、掲示板やWebメールなどへのアクセスを禁止するコンテンツフィルタリング、外部からの攻撃を防ぐIPSなど情報漏えい対策に必須の機能をいくつも搭載している。そして、このFortiGateに搭載されるファームウェアの最新バージョン「FortiOS 3.0」では、Winnyを含む数多くのP2Pアプリケーションの遮断機能が追加された。

この機能ではWinny特有のトラフィックパターンを識別することで、LANとインターネットの間に設置されたFortiGateがWinnyの通信をブロック（遮断）する。つまり、持ち込まれたPCなどにWinnyが入っていたとしても、使用できない環境を構築できるのだ。

Winnyがユーザーを魅了する理由は、動画や音楽などさまざまなコンテンツが無料で簡単にダウンロードできる点である。しかし、インターネット上でコンテンツが流通しているWinnyネットワークに到達できなければ、使う意義はない。こうなれば、ユーザーも会社での使用をあきらめざるを得ないし、Winny経由で暴露ウイルスに感染することはなくなる。

実際の設定は、FortiGateの特徴である日本語対応のGUI設定ツールで「プロテクションプロファイル」を開き、「Winny」のアクションで「ブロック」を選択すればよい。また、顧客へのアプリケーション制

限をかけにくい公衆無線LANや自由度が要求される大学構内などでの利用を見込んで、Winnyが利用できる帯域を絞り込むことも可能になっている。この場合は、同じく制限値の帯域を指定すればOKだ。

その他、Winnyの利用状況に関しても表示できるほか、ログの解析も行なえる。Winnyトラフィックを発生させたPCのIPアドレスなども一覧表示可能なので、職場での抑止効果も期待できるだろう。

企業の利用が増える IM経由でのウイルス感染を阻止

また、企業のネットワーク管理者は、Winnyだけではなく、今後はインスタントメッセージング（IM）のセキュリティにも注意を払わなければならないだろう。リアルタイムにメッセージや音声、ファイルをやりとりできるIMは、メールに変わる情報交換手段として注目を集めている。メッセージを送る前に相手が在席しているかわかる「プレゼンス」機能は特に有効だ。また、ユーザーが通信相手を許諾する形態をとるので、メールと違ってスパムが送りにくい。こうした特徴から、今後は個人だけではなく企業でもIMがコミュニケーションツールとして重要視されている。

しかし、同時にIM経由でのウイルス感染や情報漏えいの脅威にも対抗していかなければならない（図3）。特にIMの場合、NATやファイアウォール等を超えて、外部のユーザーとも簡単にやりとりできる。これが仇となり、きちんとアクセス制御しないと簡単に情報が漏れてしまうことになる。

これに対してFortiOS 3.0では、多彩なIM関連のセキュリティ機能を搭載している。AOLやICQ、MSN、Yahoo!など主要なIMに対応しており、ファイル転送でウイルスチェックをかけたり、アプリケーションごとにログインやファイル転送、音声通信を制御できる。また、Winnyと同じく、現在使用しているIDをチェックしたり、特定のIDを許可／遮断するといった処理も行なえる。チャット内容の保管（アーカイビング）も可能になっているので、現在話題のSOX法などでの内部統制対策としても有効といえる。

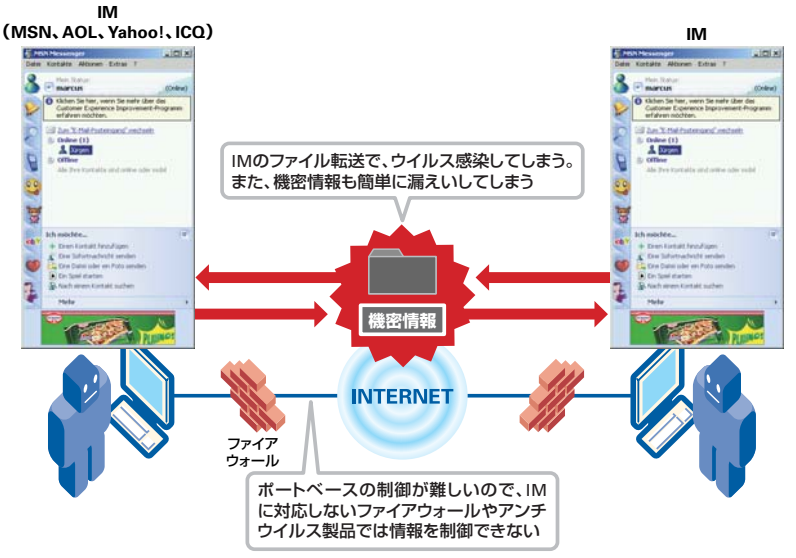
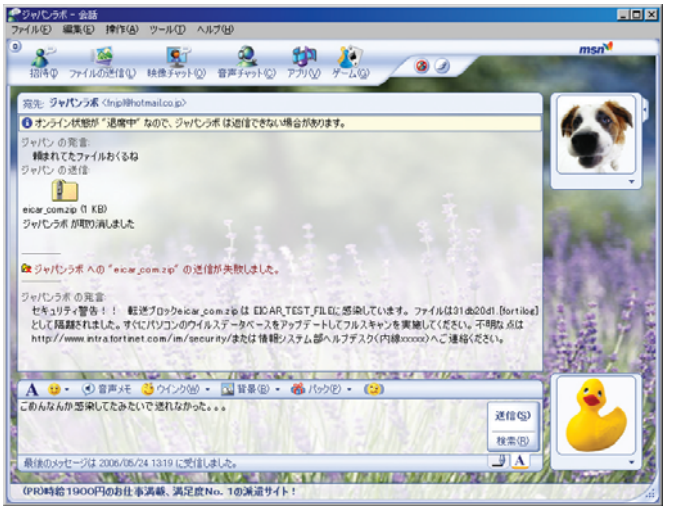


図3●情報漏えいやウイルス感染の危険があるIM



画面4●IMでのファイル転送がウイルスに感染していたため、ブロックされた

情報漏えいだけではない あらゆる脅威に対抗するUTM

FortiOS 3.0では、Winny遮断やIMのセキュリティのほか、①1台のFortiGateで、複数のUTMの機能を仮想的に実現するバーチャルドメイン拡張、②ログオンしたユーザー端末を自動的に認証するActive Directoryでのシングルサインオン、③SSL経由で安全にLAN内にリモートアクセスできるSSL-VPN、④ログやコンテンツのアーカイブなどを行なう「FortiAnalyzer」との連携機能強化、⑤USBキーへのファームウェアや設定のバックアップ、などが追加されている。

今までUTMというと高価な専用機を揃えられないユーザーのお手軽な選択肢だったかもしれない。しかし、今回紹介したFortiGateのように専用機でも追いつかないような先端的な防御機能を提供する製品もある。UTMはもはや「代替手段」ではなく、「セキュリティ対策の本命」であると言い切れるのだ。