ソフォス

新たなセキュリティ脅威からの予防保護を行う Sophos Security and Control ソリューション

ソフォス㈱
営業・企画本部長
牛込 秀樹氏

ソフォス㈱
セールスエンジニアリング
マネージャ・CISSP
兜森 清忠氏

未知のセキュリティ脅威が次々と発生し、複雑化・複合化する傾向に

法人向けセキュリティ分野をリードするグローバル企業であるソフォスは、セキュリティの脅威の最新動向について、定期的に調査を実施している。その調査結果によると、Windows以外のOSをターゲットにした、これまでにない新しいセキュリティ脅威が増えているという。特に最近では、Macintoshコンピュータがシェアを伸ばしたことにより、それらを狙った脅威が出現している。さらに、マルウェアをホスティングするサイトの約半数がApacheによるサーバを利用していたという統計が出ており、Windows端末からアクセスするプラットフォームに対する脅威となると考えられる。また、全メールの92.3%がSPAMメールという調査結果もあり、外部からの脅威として今後もトラフィックに多大なる影響を与えるとみられる。

これらの動向をふまえて、ソフォス㈱営業・企画本部長の牛込秀樹氏は次のように語っている。「情報漏洩等の致命的な事故が発生するよりも前に、企業は新しく増え続けるセキュリティ脅威に対して、然るべき対策を立てる必要があります。

弊社は、事後対策（Reactive）から一歩先へ進んで、事前対策（Proactive）、さらには予防対策（Preventive）という流れでセキュリティ対策を捉え、適切なソリューションを取り揃えています。複雑化・複合化が進むセキュリティ脅威に対して、統合化されたソリューションをお客様に提供することができます（図1参照）。」

以下、エンドポイント向けソリューションを中心に、ソフォスの最新ソリューションを紹介する。

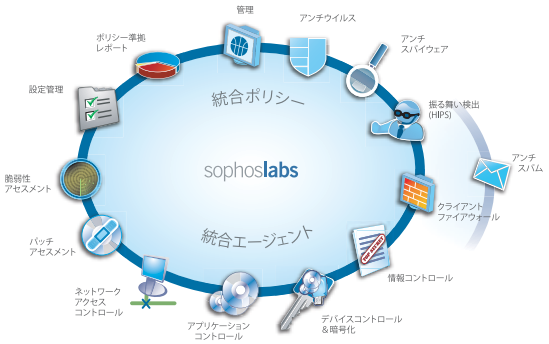

図1　ソフォスの統合セキュリティソリューションサークル

予防保護対策に最適なソフォスの統合セキュリティソリューション

ソフォスは、SophosLabs™（ソフォスラボ）の最新テクノロジーと連携し、簡易的かつ自動的にエンドポイントセキュリティ管理が可能な、統合セキュリティソリューション「Sophos Endpoint Security and Control 8.0（SESC8.0）」を提供している。このソリューションは、アンチウイルスなどの脅威対策に加え、基本的なNAC（Network Access Control）の機能を実装しているのが大きな特徴である。この機能で、ネットワークのアクセス管理も含めた統合的なセキュリティ対策を実現することができる。各エンドポイントを適切に評価し、ウイルス対策を古いままにしていたり、無効なファイアウォールを使用していたりといった、問題のある端末の検出を行える。管理対象・管理対象外・ゲスト用等、異なる種類のエンドポイントごとに識別し、問題が見つかった場合は、修復

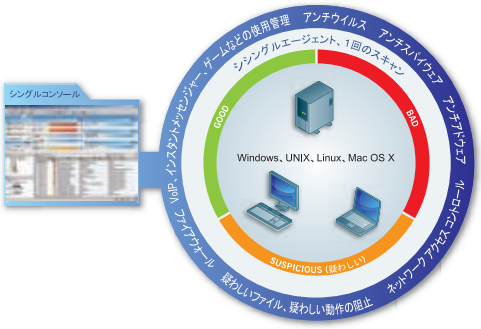

図2　シングルコンソールによる統合エージェント

図3　SESC8.0のコンソール画面

した上でネットワークにアクセスできるようにしたり、あるいはアクセスをブロックすることも可能である。

また、ユーザーは操作性に優れた集中管理コンソールを利用することで、容易にエンドポイントの評価・管理が行える（Windows、Mac、Linux、UNIX、NetApp Storage Systems及びWindows Mobile機器に対応）。従ってウイルスをはじめ、スパイウェア、アドウェア、疑わしいファイル及び動作、VoIP、IM、P2Pやゲーム等の未承認ソフトウェア、リムーバブルストレージ等の一括スキャンを実施できる（図2参照）。クライアントファイアウォールも同じコンソールで管理できる。

SESC8.0は、マルウェアや疑わしいファイル及び振る舞いを事前に検知する侵入防止テクノロジーである「Behavioural Genotype® Protection」を搭載している。この機能は、SophosLabsが提供するGenotypeテクノロジーに基づき、新たな脅威や特定の標的を狙った悪意のあるプログラムを実行前に分析し、ブロックすることができる。

ネットワーク上のリスク情報は、コンソール画面から一目で確認することができ（図3参照）、メールでも自動通知する。各エンドポイントへの保護機能の導入・アップデートや、レポート生成、セキュリティポリシー施行等の管理操作もすべてこのコンソールから行える。

各エンドポイントのセキュリティポリシーは、コンソールから「ActivePolicies™」の利用で簡単に設定できる。複数のグループや異なるプラットフォームが混在する環境でもポリシーの施行が可能である。Active Directoryと同期することで、ネットワークに追加されたばかりの端末にもセキュリティポリシーを自動的に適用することができる。

さらに、ネットワーク全般を担当する管理者が、特定のグループの管理者へ、限定された管理機能や監視権限を委任するRBA（Role Based Administration）機能や、SESC8.0のインストール・設定時に他社製品の自動削除を一括で行えるCRT（Competitor Removable Tool）機能も用意されている。

ソフォスはエンドポイント向けの他に、メールゲートウェイ向けソリューションとして、Genotypeテクノロジーに加えてリアルタイムにスパムを検知するSophos SXLテクノロジーなどを組み込んだ「Email Security and Control」を提供している。ユーザーのニーズによって、アプライアンス、またはソフトウェアを選択することができる。

また、より高度かつ柔軟なNAC機能をソフトウェアで実現する「Sophos NAC Advanced」も提供している。ソフォス㈱セールスエンジニアリングマネージャである兜森清忠氏は、「Sophos NAC Advancedをご導入いただいたグローバル製造企業様では、セキュリティパッチが提供されてから7日以内に企業内のほぼすべてのPCでの適用が実現され、PC1台あたりの脆弱性が大幅に軽減されたという効果が確認されています」と述べている。

今後の取組みについて、前出の牛込氏は次のように語っている。「脅威が複雑化する一方で、企業のIT部門はリソースやコストの削減を迫られています。弊社は今後も、大手から中小規模まであらゆる企業様向けに、複雑な脅威をシンプルに管理する統合セキュリティソリューションを提供し、磐石なセキュリティ基盤の構築と管理負荷軽減を強力に支援します。」

お問い合わせ先

ソフォス㈱　営業部
TEL：045-227-1800
E-mail：sales@sophos.co.jp
URL：http://www.sophos.co.jp/