シマンテック

シンプルかつ強固なエンドポイントセキュリティを実現する「Symantec Endpoint Protection 11.0」

㈱シマンテック
エンタープライズ営業統括本部
テレコム営業部
部長　**川崎　桂造**氏

㈱シマンテック
プロダクトマーケティング部
リージョナルプロダクトマーケティングマネージャ
広瀬　努氏

「Security2.0」コンセプトを実現する包括的なソリューション

新しい技術が通信手段に大きな変化をもたらすと同時に、新たなセキュリティリスクをもたらしている。シマンテックは昨年10月、企業や社会活動の重要な基盤であるICT環境をさまざまな脅威やリスクから総合的に守るための次世代のセキュリティ構想として、「Security2.0」を打ち出した。Security2.0は、製品、サービス、パートナーとの連携により、進化し続けるセキュリティ脅威やコンプライアンス課題に的確に対処し、顧客のつながる世界を保護するエンドツーエンドのセキュリティと信頼性を確保するためのセキュリティソリューション群から構成される。

Security2.0のコアソリューションとなるのが、エンドポイントセキュリティである。シマンテックがエンドポイントセキュリティにフォーカスする理由は、「ITシステムの拡大に伴い、管理対象となるエンドポイント数の増加、さらには、サーバやクライアントの種類、接続形態、利用者も多様化しており、管理コストの増加と管理の複雑化が大きな課題となっていることに加え、システムに密かに侵入し、不正に情報を取得するスパイウェア、ゼロデイ攻撃、意図的に標的を絞ったスピアー攻撃、亜種の氾濫など、新たなセキュリティ脅威やリスクが増加していることから、エンドポイントにおける包括的なソリューションが必要とされているからです。」(㈱シマンテック　テレコム営業部　川崎 桂造部長)

Security2.0コンセプトを担う重要なソリューションとして、シマンテックは去る6月13日、米ネバダ州ラスベガスで開催した年次カンファレンス「Symantec Vision 2007」において、ネットワークにつながるあらゆる情報端末、すなわちエンドポイントの強固なセキュリティを確保するために必要不可欠となるエンドポイントセキュリティ製品群を発表した。

「先進的な複数のセキュリティ技術を統合し、ビジネス環境のエンドポイントを多層的に保護すると同時に、ポリシーの遵守を強制するコンプライアンス機能をシームレスに統合した“Symantec Endpoint Protection 11.0（SEP 11.0）”と“Network Access Control 11.0（NAC 11.0）”を発表しました。日本市場向けには、ローカライズした製品をこの10月から販売開始します。」(川崎 桂造部長)

情報セキュリティ製品群の機能を統合したSEP 11.0

SEP 11.0は、アンチウイルスとアンチススパイウェア、ファイアウォール、IPS、デバイス／アプリケーション制御などの各機能を統合した包括的なエンドポイントセキュリ

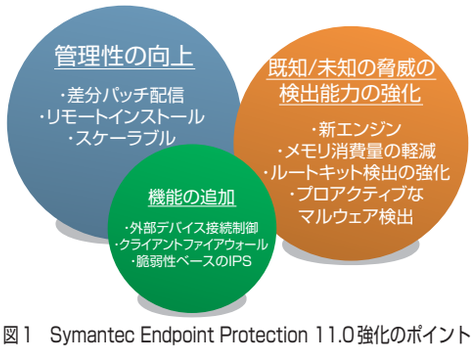

図1　Symantec Endpoint Protection 11.0強化のポイント

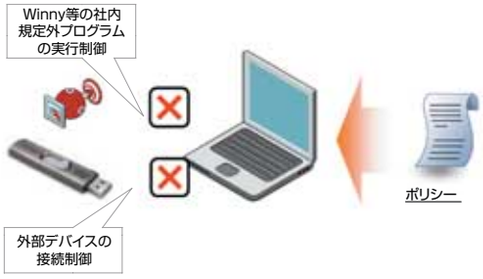

図２　ポリシーによるPCの制御

ティソリューションで、SNAC 11.0は、SEP 11.0のオプションモジュールとして提供される（検疫ネットワークとしてSNAC11.0の単独利用も可能）。

SEP 11.0について、リージョナルプロダクトマーケティングマネージャの広瀬努氏は、次のように語る。

「SEP11.0は、シマンテックの新世代セキュリティコンセプトである“Sevurity2.0”に基づいて開発された製品で、図１に示したように、管理性の向上、ウイルスやスパイウェアなど既知の脅威や、ゼロデイ攻撃など未知の脅威の検出能力の強化、さらにはデバイスの接続制御やクライアントファイアウォール、脆弱性ベースのIPS機能を追加することによって、保護・コントロール・管理機能の向上を実現すると同時に、コスト・複雑性・リスクの低減を可能にしています。」

新エンジンに加え、高度なスキャン技術等を新たに搭載

SEP 11.0は「Symantec AntiVirus Corporate Edition（SAVCE）」及び「Symantec Client Security（SCS）」の後継製品に位置づけられるが、パフォーマンス及び機能面で大幅な向上を図っている。

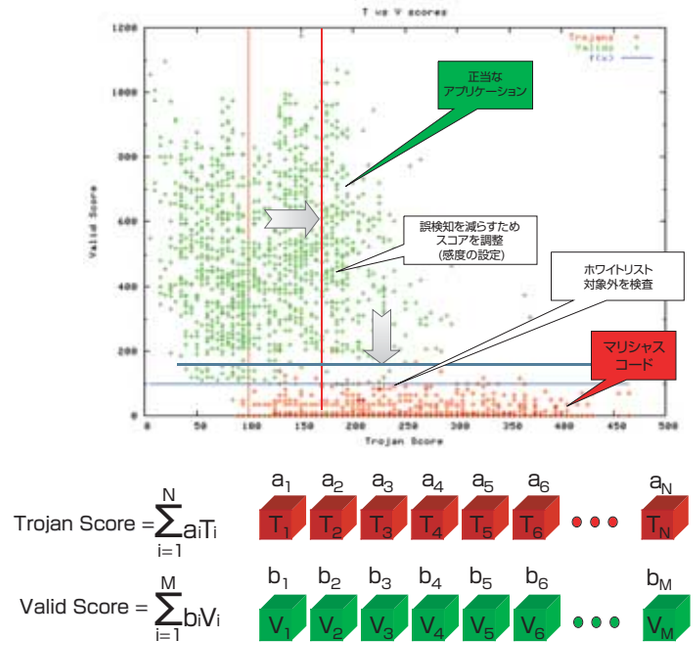

図３　プログラムの振舞いを調べる独自のアルゴリズムで未知の脅威を検出

特に、新エンジンの採用によってメモリ消費量を従来製品の約1/5に削減している。また、「RAWディスクウイルススキャン技術」や「SONAR」と呼ばれるプログラムの振る舞いを調べるアルゴリズムを新たに搭載することによって、ルートキットやそのテクニックを用いたマルウェアに対する検出／削除能力を向上させている他、ユーザーの監視が行き届きにくい未知の脅威の動作状況を高精度に検知し、削除することを可能にしている（図３）。プロアクティブなマルウェア検出の誤検知率は、10万回当たりわずかに４回（0.004％）という。

新たに追加されたデバイス／アプリケーション制御では、管理者がユーザーごとに利用を許可するデバイスやアプリケーションを指定。許可された以外のUSBメモリなどのデバイス、またアクセスポイント、業務と関係性のないアプリケーションの利用が禁止されるため、不正利用が原因となる情報漏えいなどのリスクを回避することができる。

以上、SEP 11.0の概要を紹介したが、SEP 11.0はこれまでにないシンプルかつ強固なエンドポイントセキュリティを実現する包括的なソリューションといえる。

お問い合わせ先

㈱シマンテック

＊エンドポイントセキュリティ製品に関する
購入前のお問い合わせ
URL：www.symantec.com/jp/endpoint
TEL：03-6801-1365

＊その他のお問い合わせ
エンタープライズ営業統括本部
テレコム営業部
TEL：03-5114-4160
E-mail：NTTGroup@symantec.com
URL：http://wwwsymantec.co.jp