

VENDOR NEEDS AND STRATEGIES

Fortinet社：Unified Threat Management セキュリティアプライアンス市場を牽引するマーケット・リーダー

Sally Hudson

Charles J. Kolodgy

IDCの見解

企業のIT部門にとって、複雑さへの対処は避けて通れない問題になっている。管理するネットワークは、伝送速度の高速化、通信プロトコルの多様化、ファイアウォール内外におけるユーザー数の増加といった要因により、いよいよ複雑さを増している。これらに対処するだけでも十分に困難だが、加えて、ネットワークを介したコンテンツベースの脅威が増加している。脆弱性の数、そしてそれらを悪用しようとする人間も急増している。こうした複雑さに対処するため、企業は、セキュリティアプライアンスに注目している。導入や管理が容易なこうした製品は、シンプルさと高いレベルのセキュリティを提供する。このセキュリティアプライアンス市場においては最近、新たに—Unified Threat Management—(以下、UTM/統合脅威管理)セキュリティアプライアンスの登場という進展が見られた。このカテゴリの製品は、ファイアウォール、VPN、侵入検知・防御(IDP)、ゲートウェイアンチウイルスといったさまざまなセキュリティ技術を統合している。セキュリティアプライアンスおよびUTMについて、IDCは以下のように概観する。

- ☐ 2007年までに、セキュリティソリューションの80%が、専用アプライアンスで提供されるようになる。
- ☐ UTMアプライアンスは、大規模および中小規模の企業のほか、サービスプロバイダに対しても、導入にあたって高いフレキシビリティを実現しつつ、標準的な管理プラットフォームを提供する。UTMは、搭載されるすべての機能を利用することも、特定の機能だけを活用することもできる。
- ☐ UTMセキュリティアプライアンスは当初、中小規模企業の間で注目を集めたが、ASIC(特定用途向け集積回路)ベースのプラットフォームの増加により、大規模企業やサービスプロバイダもこうしたシステムを採用しつつある。潜在的に多数の顧客が存在することから、従来のセキュリティベンダーやネットワーク機器プロバイダ、Fortinet社のような新興のセキュリティシステム企業が、引き続きこの分野の市場をターゲットにしていくとみられる。
- ☐ UTM市場を含むセキュリティアプライアンス市場では、競争が激化する。この市場で成功を収めるか否かは、パフォーマンスや機能の向上による製品の差別化がカギを握る。
- ☐ UTMセキュリティアプライアンス市場を開拓し、リードするのは、Fortinet社である。同社は、UTMアプライアンスで提供可能なソリューションのすべてをいち早く体系的に開発・統合してきた企業の一つであり、リアルタイムのアンチウイルスやIDP処理のために、専用ASICを採用している唯一のベンダーである。

調査概要

このIDC調査レポートは、セキュリティプライアンス市場におけるUTM分野をリードする株式非公開企業Fortinet社について分析したものである。Fortinet社のFortiGateアンチウイルス・ファイアウォール製品は、一連のセキュリティ技術を緊密に統合することで、スピードとパフォーマンスを重視しつつ、ネットワークおよびコンテンツのセキュリティを提供している。

概況

2000年に設立されたFortinet社は、カリフォルニア州サニーベールに本社を置く株式非公開企業である。現在、南北アメリカ、アジアおよびヨーロッパ・中近東・アフリカに拠点を置き、合わせて525人を超える従業員を擁する。同社のFortiGateアンチウイルス・ファイアウォール・システム、FortiClientソフトウェア、FortiLogシステムおよび関連製品は、堅牢なセキュリティと高いパフォーマンスを必要とする組織に、多面的なセキュリティを提供するよう設計されている。大規模企業やサービスプロバイダは、ゲートウェイ・アンチウイルス、ファイアウォール、IDP、IPSec VPNといったICSA認定の機能に注目し、Fortinet社の製品を採用するケースが多い。これらの機能はしばしば、そうした企業がすでに導入済みの、ファイアウォール、VPN、IDPといった他ベンダーのセキュリティ製品を補完する役目を果たす。小規模企業やホームオフィス・ユーザは、包括的なUTMプラットフォームとして、同社の製品を採用している。

セキュリティプライアンスとUTM

IDCは、セキュリティプライアンスを、単一あるいは複数のセキュリティ機能の提供を主な目的とし、ハードおよびソフトウェア、さらにネットワーク技術の組み合わせで構成される特定用途向けの製品と定義している。セキュリティプライアンスは、強固なオペレーティングシステム(OS)を搭載したハードウェアと限定されたアプリケーションセットで構成される。脅威をダイナミックに防御するために、補完的にクライアントソフトウェアをインストールする場合以外は、通常はユーザー側でソフトウェアのインストールは行なわれない。セキュリティプライアンスには、セキュリティ管理、ロギング、ポリシー管理、サービス品質確保(QoS)、負荷分散、ハイアベイラビリティ(HA)、帯域制御レポートといった他の機能も含まれることもあるが、あくまでもこれらの機能は、本来のセキュリティ機能をサポートすることを目的としている。

Fortinet社は、こうした市場の一分野である、UTMセキュリティプライアンスを手がけている。IDCは、UTMセキュリティプライアンスを、複数のセキュリティ機能を単一の機器に統合した製品と定義している。他の市場ではなく、このカテゴリに分類されるためには、製品は、ネットワークファイアウォール、ネットワークIDP、ゲートウェイ・アンチウイルス機能を備えている必要がある。これらすべての機能が同時に利用される必要はないが、機能自体は本来製品に含まれていなければならない。

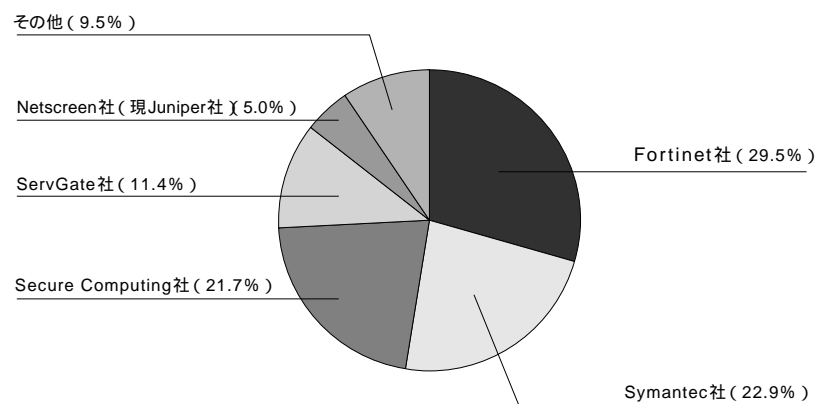
Fortinet社のアプローチ

Fortinet社のFortiGateアンチウイルス・ファイアウォールおよび関連製品ラインは、上記の基準を満たすものである。Fortinet社のシステムは、ネットワークアプリケーションのパフォーマンスを損なうことなく、ネットワークとコンテンツの統合されたセキュリティを提供し、その基礎を成す技術が、市場において自社の製品を差別化できる要素となっている。Fortinet社は、独自のASICチップ技術を採用することにより、アンチウイルスなどのセキュリティ機能のパフォーマンスを高め、リアルタイムでアンチウイルス機能を

提供できる唯一のベンダーである。さらには、このASICに組み合わせる7つの重要なUTM機能
 アンチウイルス、VPN、ファイアウォール、IDP、コンテンツフィルタリング、アンチスパム、帯域制御
 も自社内部で開発した。Fortinet社は、必要不可欠なセキュリティ機能を統合することによってUTMの
 カテゴリを開拓するという重要な役割を果たしてきた。Fortinet社は2003年、この急成長を遂げる市場
 で30%のシェアを持つトップベンダーとなった(図1)。2004年に入っても、トップの座は変わっていない。
 IDCが四半期毎に報告している『Security Appliance Quarterly Tracker』によれば、Fortinet社
 は、23%近くのシェアで市場リーダーの座を守っている(図2)。

図1

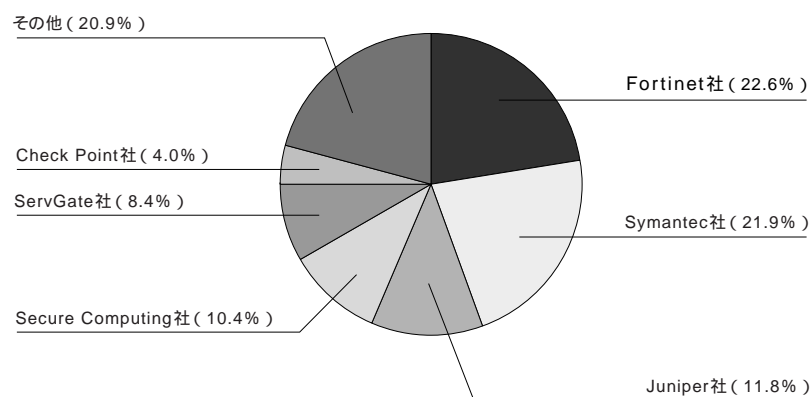
2003年 ワールドワイドにおけるアプライアンス売上高ベンダー別シェア



出典：IDC(2004)

図2

2004年上期 ワールドワイドにおけるアプライアンス売上高



出典：IDC(2004)

Fortinet社は、独自のFortiASICをベースとした一連のネットワークセキュリティ機能を顧客に提供する。OSIネットワークスタックを通過するネットワークを介した脅威をリアルタイムに保護することから、Fortinet社は、自社のソリューションを「コンプリート・コンテンツ・プロテクション」(Complete Content Protection:CCP)と呼ぶ。このアプローチは、データパケットのヘッダを調べるステートフルインスペクションや、これを高度化したディープ・パケット・インスペクションといった標準的なファイアウォール検査技術を凌いでいる。

CCPIは、ダイナミックにアップデートされる非常に高度なアプローチを採用しているが、これを可能にするのが、アンチウイルスおよびIDPシグニチャをアップデートするための自社の世界的ネットワークFortiProtectと、URLフィルタリングの対象をアップデートするためのネットワークFortiGuardである。他の手法と比べてCCP技術が特別なのは、パケットレベルのペイロードをアプリケーションレベルの対象(ファイルやドキュメントなど)に、ギガビットのネットワーク速度においてリアルタイムで再構築できる能力にある。CCP技術により、再構築したデータを数多くのウイルスおよびワームの最新情報に照らしてスキャンし、分析することが可能になる。新たなゼロ・デイ・アタックの脅威は、FortiOSのヒューリスティック技術によるビヘイビアベースの分析(シグニチャの照合ではなく、プログラムの動作の分析)によりこれを阻止する。CCPはまた、不適切なウェブコンテンツ、スパムメール、スパイウェア、フィッシング行為といった多様な脅威の検知にも威力を発揮する。

当然ながらCCPIは、プロセッサおよびメモリに依存する面があり、ステートフル / ディープ・パケット・インスペクションに比べ、パケット当たり100 ~ 1000倍の処理能力を必要とする。このような要求を十二分に満たすため、FortiGateプラットフォームは、FortiASICと汎用プロセッサの双方を活用し、単一あるいは複数のUTMセキュリティ機能向けに、アプリケーションの最適なサポートを行なう。新しいシャーシベースのFortiGate-5000シリーズのような大容量プラットフォームは、大規模企業やサービスプロバイダのセキュリティを保護するため、スモールオフィス・ユーザ向けの小規模なFortiGateシステムに比べ、より多くのメモリを必要とする。CCPソリューションのために、他ベンダーの技術を継ぎ接ぎし、従来型のサーバとネットワーク・システム上で稼働させるような製品を導入したユーザは、ネットワーク全体のパフォーマンスが劇的に低下する結果に陥っている。

FortiGateアプライアンス:FortiASICとFortiOS

この問題を回避するため、Fortinet社は、CCP環境に特化したハードおよびソフトウェアの独自アーキテクチャを開発した。FortiGateアプライアンスは、ネットワークのコアや境界部において高パフォーマンスでアプリケーションレベルのコンテンツプロセッシングを行ない、リアルタイムでセキュリティ機能を提供するよう特別に設計されたハードおよびソフトウェアの統合アーキテクチャに基づいている。Fortinet社によると、現時点でこの技術は、数ギガビット / 秒のデータレートでもリアルタイムでアプリケーション層サービス(ウイルス検知やコンテンツフィルタリングなど)を提供できる、市場で唯一のプラットフォームだという。

15機種以上におよぶFortiGate製品のキーコンポーネントとなるのが、FortiASICチップである。この専用チップに、ハードウェア・スキャンエンジン、ハードウェア暗号化、リアルタイムのコンテンツ分析といった処理能力が組み込まれている。FortiASICチップにより、ファイアウォール、暗号 / 復号化、シグニチャおよびヒューリスティック・パケットスキャン、パケットカウントやフロー計測に基づく帯域制御といった機能が高速化される。

加えて同社は、カスタムOSであるFortiOSを開発し、これにより、ファイアウォールやコンテンツセキュリティに関する高いパフォーマンスの検査能力を、単一プラットフォームで提供することを可能にした。

FortiOSは、アンチウイルス、アンチスパム、VPN、ファイアウォール、IDPといった機能と、独自のソフトウェアやASIC、そしてダイナミック・アップデートを組み合わせることにより、新たな、あるいは既存の複合型攻撃を阻止するよう設計されている。

FortiProtectインフラストラクチャ・サービス

Fortinet社は、顧客に以下のような一連のサポートサービスを提供している。

- ☐ ウイルスやワームをはじめとするネットワーク脅威に関する情報をリアルタイムで入手できるポータルとして、FortiProtectセンターが設置されている。同センターは、Fortinet社のウェブサイトや更新時にプッシュ方式で送られる通知を通じて利用できる。FortiOSの自動アップデートは、世界中のすべてのFortiGateユニットに5分未満で届くように設計されている。
- ☐ 世界各地のネットワークセキュリティ専門家で構成されるチーム、FortiProtect Threat Response Teamが、ウイルスサンプルを収集・分析し、ウイルスシグニチャを開発してFortinet社のウイルス定義リストのアップデートを行なう。このチームはまた、ネットワーク侵入防止用シグニチャも開発し、Fortinet社のネットワーク侵入防止 / スパイウェアあるいはグレイウェア検知システムをアップデートしている。
- ☐ 世界中のThreat Response Teamと共に稼働しているFortiProtect Distribution Networkは、FortiGate製品の位置するタイムゾーンや地域に関係なく、タイムリーなアップデートを自動的に提供する。

これまで述べてきたとおり、Fortinet社のFortiGateと関連するハードおよびソフトウェア製品スイートは、スピードとパフォーマンスを重視しつつ、ネットワークとコンテンツのセキュリティのために、一から徹底的に開発して統合した技術を提供する。大規模企業やサービスプロバイダ向けのクラス最高の機能から、中小規模企業向けの包括的ソリューションに至るまで、Fortinet社は、ユーザにUTMのベンチマークを提案する。

将来の展望

今日、企業は当然のことのようにインターネット技術を使用している。それと同時に、ハッカーや犯罪者をはじめとする邪悪な人々がこの技術を悪用することも、日常茶飯になっている。あらゆる規模の企業やサービスプロバイダにとって、種々の脅威は増大し、いよいよ複雑になっている。このような状況に対処するため、多くのセキュリティ技術が導入されるが、ハッカーたちは、特定の脆弱性を悪用するコードを組み合わせ、悪質な複合型脅威に狙いを定めつつある。こうした複合型攻撃はとりわけ、VPN、ファイアウォール、アンチウイルスといった単一の機能によるポイントソリューションの裏をかくように仕組まれている。

複合型脅威は、ポイントソリューションに対しては有効だが、統合型セキュリティソリューションに対しては、高い確率で失敗に終わる。IDCは、UTMセキュリティアプライアンスの開発・導入が、将来のセキュリティソリューションにとって柔軟かつ最良の答えになると考える。そのためIDCは、UTM市場が急成長し、既存のポイントソリューションとしてのファイアウォール / VPNセキュリティ製品を追いやる形になると予想している。表1は、UTMセキュリティアプライアンスとファイアウォール / VPNセキュリティ製品の売上高予測を対比したものである。2008年末までには、UTM市場が、既存のファイアウォール / VPN市場を売上規模で上回ると予想される。

表1

2003～2008年 ワールドワイドにおけるUTMセキュリティアプライアンスとファイアウォール / VPN
セキュリティ製品の売上高(単位:100万ドル)

	2003	2004	2005	2006	2007	2008	平均成長率
UTM	105	225	518	828	1,325	1,987	80.1
FW/VPN	1,479	1,668	1,792	1,804	1,623	1,462	-0.2

注:予測の根拠となる前提については、関連調査(IDC #31840, September 2004およびIDC #31839, September 2004)を参照のこと。

出典: IDC(2004)

以下に挙げる理由から、5年後にはUTMの分野が市場で優勢になると予想される。

- ☒ Fortinet社のFortiGateアンチウイルス・ファイアウォールなどのUTMアプライアンスは、大規模企業、サービスプロバイダ、あるいは中小規模企業において、単体のアプライアンス以上か、少なくとも同等のパフォーマンスを提供できる。
- ☒ UTMアプライアンスは、顧客のセキュリティに関するアプローチに合わせ、非常に柔軟なカスタマイズを可能にする。UTMは、そのすべての機能を利用することも、クラス最高の機能を特定の目的に絞って活用することもできる。
- ☒ UTMアプライアンスは、包括的な管理、レポート作成、ロギングのための機能もあり、シグニチャのアップデートやレポート作成を含むあらゆるセキュリティ機能の管理を可能にする。
- ☒ UTMセキュリティアプライアンスは、当初はとりわけ中小規模企業向けのセキュリティ製品だったが、現在では、大規模企業やサービスプロバイダにおける既存のポイントソリューションを補完する用途としても有効な高パフォーマンスを提供する。今後の成長という点で、こうした市場はかなりのポテンシャルを有している。

UTMセキュリティアプライアンスのベンダーが成功するためのカギは、パフォーマンス、価格競争力、機能セットの向上による製品の差別化にあるとIDCは考える。ベンダーは、市場をリードしているベンチマークを塗り替えることにより、傑出した存在になることが求められる。そしてこれは、数多くの要素において達成し得る。たとえば価格、パフォーマンス、製品に含まれるセキュリティ機能の組み合わせ、操作性、セキュリティ情報サービス、セキュリティ認定といった要素である。興味深いことに、Fortinet社は、これらの差別化戦略のすべてを重視している。なかでも顕著な例として、Fortinet社のアンチウイルスおよびIDP製品は、ユーザ毎のライセンスが必要な他のベンダーとは対照的に、ボックス単位のライセンス体系を採用している。この戦略だけをとって、FortiGateシステムを選択する大規模企業やサービスプロバイダに、コスト節減というメリットをもたらすことになる。

IDC の提言

15機種以上におよぶFortiGateシステムのすべてが、UTMセキュリティアプライアンスのカテゴリに入るが、この新興の市場における競争は非常に激しくなっている。2003年には、UTM製品を販売するとされるベンダーは7社あった。2004年末時点では、少なくとも16社に増えているはずである。そうした企業のなかには、ネットワークセキュリティの分野で名を馳せているベンダーのほか、アンチウイルスのトップベンダー、そしてヨーロッパやアジアの多くの小規模なアプライアンスベンダーも含まれている。

Fortinet社は、UTMというカテゴリの発展における先駆者的存在である。また同社は、すべてのソリューションをUTMアプライアンスで提供した最初の企業である。Fortinet社が市場でリーダーの座にある理由は、アンチウイルス処理のために専用ASICを採用した唯一のベンダーであり、潜在的なあらゆる顧客のニーズに対応できる幅広い製品ラインを用意していることにあるとIDCは考える。SOHO向けのFortiGate-50Aから、マルチギガビットレベルのキャリアクラスのネットワークに対応するFortiGate-5000シリーズまで用意された同社の製品ラインは、あらゆる規模の顧客企業のニーズに応える。

高速で、信頼性が高く、まさに包括的なセキュリティアプライアンス技術を求めるIT顧客にとって、Fortinet社は、検討すべきベンダーの最終候補に残るはずである。

参考資料

関連調査

- ☒ Worldwide Threat Management Security Appliances 2004-2008 Forecast Update and 2003 Vendor Shares: The Rise of the Unified Threat Management Security Appliance (IDC #31840, September 2004)
- ☒ Worldwide Firewall/VPN Software 2004-2008 Forecast Update and 2003 Vendor Shares: Desktop Firewalls on the Move (IDC #31839, September 2004)
- ☒ Worldwide Secure Content Management 2004-2008 Forecast Update and 2003 Vendor Shares: A Holistic View of Antivirus, Web Filtering, and Messaging Security (IDC #31598, August 2004)
- ☒ IDC's Software Taxonomy, 2004 (IDC #30838, February 2004)
- ☒ IDC's Enterprise Security Survey, 2003 (IDC #30653, December 2003)

Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit www.idc.com to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit www.idc.com/offices. Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or sales@idc.com for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2004 IDC. Reproduction is forbidden unless authorized. All rights reserved.

Published Under Services : Security Products; Firewalls and Security Appliances

FORTINET**フォーティネットジャパン株式会社**

〒107-0052 東京都港区赤坂2-12-10 国際溜池ビル6F
TEL. 03-5549-1640 E-mail : info_jp@fortinet.com

www.fortinet.co.jp

記載された社名、各製品名は各社の登録商標または商標です。
記載された内容は、変更する場合がありますのでご了承ください。

お問い合わせ