Linux のセキュリティ脅威

A Sophos positioning paper

January 2006

昨今、ビジネスネットワーク中で Linux サーバーが占める割合は急激に増加しています。このポジショニングペーパーでは、セキュリティ対策をとられていない Linux マシンを Windows その他のプラットフォームと混在させることでビジネスがさらされる危険性について説明します。また、セキュリティ脅威が複雑化する中でプラットフォームが混在する環境が直面するセキュリティギャップについて記述します。最後に、ソフォスの Sophos Anti-Virus による Linux 環境の保護と、マルチプラットフォームでのセキュリティ対策の長年の経験と実績をベースにソフォスが提供する統合脅威管理ソリューションによるネットワーク環境全体の保護について述べます。

ビジネス用途での使用の拡大

Linux オペレーティングシステムの歴史は、1991 年に Linus Toryalds 氏が最初の Linux カーネルをリリースした時に始まりました。すべての Linux カーネルはオープンソースの理念の下に、熱心なファンによって継続的に開発と改善を加えられ、広く一般に支持される OS となっています。

Linux は、もはや専門技術者たちだけの関心を集めるものではなくなり、多くの企業や組織の注目を集めています。ビジネス向けの Linux ディストリビューションとして Red Hat、SUSE、TurboLinux などが配布され、管理ツール、サポート、サービスなどが提供されています。電子メール、Web、ファイルサーバー、プリンタサーバーなど、ビジネス目的での Linux の導入が拡大しています。

エンタープライズレベルのビジネスネットワークでの Linux の導入は今後数年間のうちにさらに飛躍的に増加すると考えられています。IDC のアナリストは、サーバー、デスクトップ、パッケージソフトをあわせた世界のLinux市場規模は2008年までに357億ドルを突破すると予測しています。[1]

エンタープライズレベルのビジネスネットワークでの Linux の導入は今後数年間のうちに飛躍的に増加すると考えられています。

ただし、当面の間はサーバーとしての導入がほとんどを占めると考えられています。実際に、クライアントやノート PC でも Linux が採用されていますが、ビジネスレベルのマルチプラットフォーム環境では、サーバーに Linuxを採用し、クライアントに Windows や Mac を採用する組織が多くなっています。セキュリティの観点では、Linux サーバーの管理は Windows などのシステムに比べて高いスキルを要することから、より安全なプラットフォームだと考えられてきました。しかし、Linux が、企業や政府機関、教育機関などのビジネス目的で使用されるようになるに従って、その安全性が懸念されはじめています。

組織への脅威

セキュリティ対策のとられていない Linux マシンは Windows 型ウイルスのキャリアとなり得るため、他のシステムとインタラクティブに接続されている場合、ネットワーク内の他のマシンに感染をもたらし、重大な損害をもたらす危険性があります。顧客や取引先に Windows 型ウイルスを転送してしまった場合には、単に組織の評判と信用を損ねるだけでなく、法的な責任の追及に発展しかねません。Linux ベースのシステムを狙った悪意のあるコードの多くは、メールや Web プロトコルのほか、Samba や NFS などのネットワーク共有システムを利用して伝播されます。

セキュリティ対策のとられていない Linux マシンは Windows 型ウイルスのキャリアとなり得るため、組織内の他のマシンに感染をもたらし、重大な損害を与える危険性があります。

Linux OS そのものの安全性については従来から盛んに議論されています。今日、大多数のウイルス、ワーム、スパイウェア、トロイの木馬などのマルウェアは Windows システムをターゲットにして作成されていますが、これはマイクロソフト社が OS 市場を席捲しているために攻撃のターゲットにされやすいことが大きな原因と考えられます。Linux が今後主流 OS に成長するに従って、Linux をターゲットにした ― 特に金銭窃取を目的とした ― ウイルス作成者の関心を引くのは確実です。Linux のコーディング情報はインターネット上で無償で得られるため、危険性はより高いといえます。

現在、組織の IT インフラストラクチャはOS の混在が進み、より複雑しています。IT の複雑化により、ネットワークにセキュリティギャップが生じ、それをついた脅威が出現しています。最近では、Bofra と呼ばれる、ワーム、ウイルス、スパムを組み合わせた脅威が猛威をふるいました。ネットワークでの Linux の導入が拡大するとともに、すべてのプラットフォームおよびレイヤーを統括的に保護できる信頼性の高い統合ソリューションが必要となっています。

Linux セキュリティ確保の課題

マルチプラットフォーム環境のシステムがより複雑な脅威に直面する中、Linux マシンのセキュリティを確保を困難にしている要因として、リアルタイムのオンアクセススキャンへの対応、多様なカーネルの混在、カーネルのカスタマイズの3点が挙げられます。

オンアクセススキャン

オンデマンドまたはスケジュールベースのウイルススキャンのみでは、Linux マシンのセキュリティを十分に確保することは困難です。今日のネットワーク環境では、ユーザーのアクションや OS の機能によって感染したファイルにアクセスした瞬間に、被害が拡大してしまうからです。

被害の拡大を未然に防ぐためには、リアルタイムでのスキャンを行うオンアクセス機能は大変有効です。しかし従来、ウイルス対策ソフトはファイルシステムのインターセプトを行うため、カーネルに直接プラグインしなければならず、Linux でオンアクセススキャンを実現するのは難しいと考えられていました。

感染したファイルがアクセスされた瞬間から、Linux コンピュータのネットワークに脅威が蔓延する危険性があります。

その対策として、ファイルインターセプトを行うモジュールやエクステンション、インターフェース、またはフッキングメカニズムなど多くのツールが提供されています。Linux ではオープンソースのファイルインターセプトモジュールが提供されており、多くの場合、ウイルス対策ソフトと組み合わせて使用されています。しかし、ファイルインターセプトモジュールは有用で柔軟性のあるツールですが、それだけではセキュリティ脅威から組織を保護するための十分な機能を備えているとはいえません。たとえば、これらのツールでは LSM、Syscall、VFS など複数のファイルシステムやモジュールをスキャンすることができません。

カーネルの混在

Linux には多くのディストリビューション、バージョンが存在します。たとえば、ひとつのディストリビュータが同一のバージョンについてホームユーザー用、プロフェッショナル用を個別にリリースし、さらに定期的に機能拡張や機能強化を行ってバージョンアップします。

ウイルス対策ベンダーにとっては、数多くのカーネルのすべてに対応するのは非常に困難なため、多くのウイルス対策ベンダーは、カーネルのメジャーアップデートのみにあわせてウイルス対策ソフトをアップデートし、小規模なパッチには対応しないなどの対策を行っていますが、それではビジネス環境において十分なセキュリティが確保できるとはいえません。

カーネルのカスタマイズ

Linux OS を採用する利点のひとつは、特定のネットワーク環境に適応するように容易に修正できることです。たとえば、組織内独自のアプリケーションにあわせてカーネルをカスタマイズするケースなどが挙げられます。しかし、その利便性、柔軟性が、ウイルス対策ベンダーにとってはサポートの難しさを招いています。

ソフォスソリューション

ソフォスは、20 年に渡ってマルチプラットフォームのセキュリティ対策ソリューションを提供しつづけています。UNIX 対応のウイルス対策ソフトを業界で最初に提供した実績を持ちます。Sophos Anti-Virus for Linux はその実績と経験をベースに開発されており、Linux を含む複雑なマルチプラットフォームネットワークに、堅固な保護を提供します。

- Sophos Anti-Virus for Linux は、独自の高性能、高速オンアクセススキャン機能を持つファイルインターセプトモジュールを提供します。Sophos Anti-Virus for Linux は、高速、高信頼性、高確実性、高拡張性を備えたウイルス対策ソフトです。多様なファイルシステムのスキャンが可能であり、ネットワークを強力に保護します。
- Sophos Anti-Virus for Linux のオンアクセススキャン機能には Decision Caching テクノロジーが採用されています。新規または変更されたファイルのみをスキャンし、効率的なスキャンを行うことで、高速性を実現しています。
- ソフォスは幅広い Linux ディストリビューションおよびカーネルバージョンに対応しています。Sophos Anti-Virus が公式にサポートしているディストリビューションの場合、新バージョンがリリースされると Sophos Anti-Virus for Linux もアップデートされ、自動的にダウンロードされます。
- Sophos Anti-Virus for Linux はカーネルがアップデートされると自動的にリコンパイルされます。そのため、Sophos Anti-Virus のアップデートが提供される前であっても高度な保護を提供します。この機能により、カスタマイズされたカーネルにも自動的に対応できます。*

また、Sophos Anti-Virus for Linux は、ウイルス定義ファイルを自動的にアップデートし、常時最新に保ちます。以下のいずれかの方法で行うことができます。

- Linux のみで構成されている環境の場合、Linux サーバーからソフォスデータバンクに直接アクセスしてアップデートファイルをダウンロードし、配布（図1a）。
- マルチプラットフォーム環境の場合、集中管理ツールである EM Library と CID（セントラルインストールディレクトリ）を利用してアップデートファイルをダウンロードし、配布（図1b）。

これらの管理は Web GUI またはコマンドラインインターフェースを使って容易に設定、実施できます。Sophos Anti-Virus for Linux は、オンアクセス、オンデマンド、またはスケジュールベース（”at” または “cron” コマンドを使用）でスキャンを行い、ウイルスその他のマルウェアから Linux マシンを保護します。ソフォス独自のGenotype（遺伝子型）テクノロジーが組み込まれたウイルス検索エンジンが、特定のウイルス定義ファイルが提供されていないウイルス亜種を阻止します。新規の脅威が短期間でネットワークに蔓延するのを防ぎます。

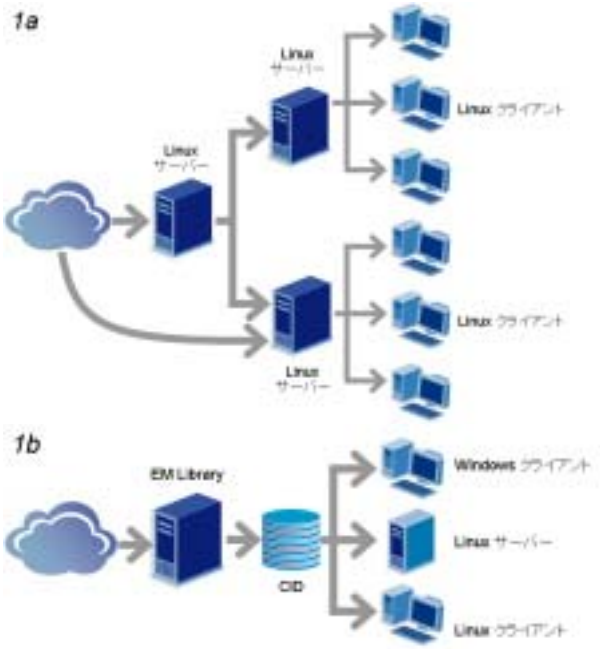

図1：Sophos Anti-Virus **の自動アップデート**
1a：Linux **のみのネットワーク**
1b：**マルチプラットフォーム環境**

* お客様が、ソフォスが正式にサポートしていない Linux ディストリビューションまたはカスタマイズした Linux カーネルをご使用の場合、ソフォスはリコンパイルのためのサポートをご提供しない権利を留保します。合理的な範囲で一次サポートを行いますが、ソフォス内で技術的なエスカレーションを行うことを含め、問題解決を保証するものではありません。

統合脅威管理

ソフォスのビジネスに特化したソリューションは、お客様の IT インフラストラクチャをトータルにカバーします。ゲートウェイとエンドポイントに統合的な脅威管理ソリューションを提供し、サーバー/クライアント、モバイル PC などをウイルス、ワーム、トロイの木馬、スパイウェア、スパムから保護します。

また、お客様のビジネス環境を確実に守るため、24 時間 365 日無休のサポートをライセンスに標準でご提供しています。また、グローバルに展開するソフォスラボが常時脅威解析を行い、最新のウイルス定義ファイルやスパムルールを迅速にご提供します。

まとめ

Linux のビジネス分野での使用が拡大するにつれて、Linux のセキュリティ脅威も深刻化し、感染時のビジネスへの影響が危惧されて始めています。脅威そのものだけでなく、IT インフラストラクチャの複雑化にしたがって生じるセキュリティギャップや、Linux マシンが Windows 型ウイルスのキャリアとなってしまう危険性も重大です。

Sophos Anti-Virus for Linux は、オンアクセススキャン、自動アップデート、直感的に操作できる使い安い管理ツールなどの機能を提供したソリューションです。

ソフォスはセキュリティ分野で 20 年以上の経験と実績をベースにした研究開発、高い技術力、および多様な脅威に対応したマルチプラットフォームアプローチによって、Linux を含めたお客様のネットワーク環境を統合的に保護いたします。

その他、ソフォス製品およびソフォス製品を使ってネットワークを保護する方法の詳細につきましては、ソフォスのサイトをご参照ください。www.sophos.com

参考

1. The Linux Marketplace. Moving From Niche to Mainstream [OSDL（Open Source Development Labs）にて発表], IDC Software Consulting, 2004年12月14日 (www.osdl.org/docs/linux_market_overview.pdf)

ソフォスとは

ソフォスは法人向けに統合脅威管理ソリューションを提供する世界的なリーディングカンパニーです。グローバル企業、SMB市場、教育機関、政府機関、金融業、製造業など、あらゆる規模、分野の組織をセキュリティ脅威から保護し、世界150カ国以上で3,500万人以上のお客様にご導入いただいております。セキュリティ分野で20年以上におよぶ実績と経験をベースに、セキュリティ解析センターが複雑な脅威に迅速に対応し、常時最新の対策をご提供しています。その高品質な技術力とサービスは多くのお客様から高い評価をいただいております。

ソフォス株式会社
〒231-0062　神奈川県横浜市中区桜木町1-1-8 日石横浜ビル15F
Tel. 045-227-1800　　E-mail. sales@sophos.co.jp

Boston, USA • Mainz, Germany • Milan, Italy • Oxford, UK • Paris, France
Singapore • Sydney, Australia • Vancouver, Canada • Yokohama, Japan

SOPHOS
WWW.SOPHOS.CO.JP