

Symantec AntiVirus™ for Network Attached Storage

処理能力、スケーラビリティ、信頼性を追求した、ネットワークストレージとの連携によるウイルス対策

製品の概要

異なるプラットフォームが混在する環境におけるデータ共有、データの二重化、処理効率の向上、ストレージ管理の簡易化、リアルタイムのバックアップ/復元など、多くのメリットが期待できるため、多くの企業でネットワークストレージ (NAS) の導入が進んでいます。NAS 上のデータは多数のユーザーによって共有されるため、NASを経由したウイルス感染は社内外を含めて危機的な被害に発展するリスクが特に高まります。そのため、NASを経由するファイル操作には、信頼性の高いウイルス対策が確実に実行される必要があります。Symantec AntiVirus for Network Attached Storageは、そのようなネットワークストレージの使用におけるウイルス対策のニーズにお応えします。

〈キーポイント〉

- ネットワークストレージ (NAS) の使用におけるウイルス対策 (NAS製品と連携)
- サービスプロバイダ事業において実力が証明されている Symantec AntiVirus Scan Engineを使用
 - ミッションクリティカルな用途のために追求された、処理能力、スケーラビリティ、そして信頼性
 - サービスの停止を必要としないウイルス定義ファイルとエンジンのアップデート等、シマンテックのアンチウイルス技術の粋を結集
 - スキャンを行うためのスレッド数を、負荷に応じて動的に増減
 - Sun Solaris、Red Hat Linux、Windows 2000、Windows Server 2003上で稼動

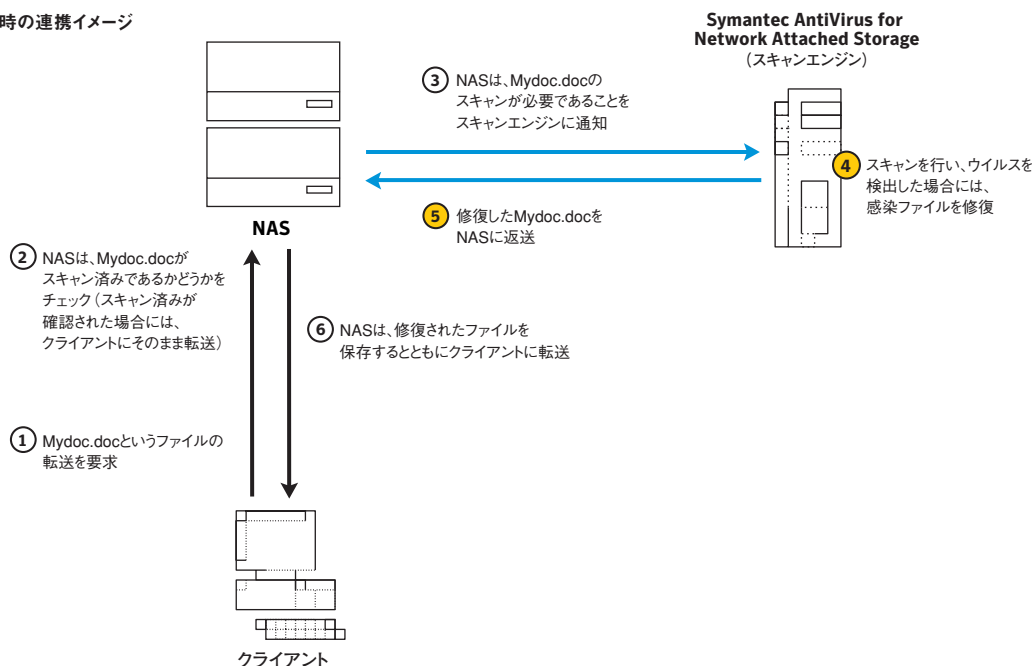
- Webベースのインターフェースで容易に管理
 - NAS上の感染データに関係するユーザー/クライアントの情報に関するログの記録とサマリーレポートの作成
 - SMTP/SNMP によるアラート発信
- 世界をリードするインターネットセキュリティの専門機関、Symantec Security Responseによる信頼のバックアップ

製品の特長

NAS製品と連携したウイルス対策

ネットワークストレージは、膨大な量のデータの格納を管理して多数のユーザーからのリクエストに対してスピーディに処理を行う必要があるため、ウイルス対策にも高いパフォーマンスとスケーラビリティが要求されます。処理能力、スケーラビリティ、そして信頼性を追求したSymantec AntiVirus for Network Attached Storageは、NAS製品と連携することによって、NASを経由したウイルス感染を防止します。クライアントにより要求されたNAS上のファイルは、Symantec AntiVirus for Network Attached Storageに転送されてウイルススキャンが行われ、感染が検出された場合にはファイルの修復が行われます。そして、NASに返送されて書き込まれると同時に、ファイル要求を行ったクライアントに転送されます。クライアントから要求されたファイルは、スキャンが行われていない場合のみ、Symantec AntiVirus for Network Attached Storageに転送されます。同様に、ファイルが保存される際には、スキャンを行った後にNASに書き込まれます。このように、NAS製品と連携するSymantec AntiVirus for Network Attached Storageは、NAS上の膨大な量のファイルに対して確実なウイルス対策を効率的に行うためのソリューションを提供します。

ファイルの読み出し時の連携イメージ



スピードとスケーラビリティ、そして信頼性を追求した Symantec AntiVirus Scan Engineを使用

Symantec AntiVirus for Network Attached Storageは、24時間絶えることのない確実な稼働が要求されるサービスプロバイダ事業において多くの採用実績がある、Symantec AntiVirus Scan Engineを使用しています。

Symantec AntiVirus Scan Engineの特長

- 高い検出能力が実証されているシマンテックのアンチウイルス技術の粋を結集
 - サービスの停止や再起動を行わずに、ウイルス定義ファイルとスキャンエンジンをアップデート可能な NAVEX™
 - NAVEXによるアップデートを自動的に実行するLiveUpdate™
 - 新種/亜種等、未知のウイルスも検出するBloodhound™
 - MIME (Base 64)、UUENCODE、BinHexなどのコーディング、Zip、LZH、TARなどの圧縮形式ファイルのスキャン（多重圧縮にも対応）
- メモリー上でのマルチスレッドスキャンによる、高い処理能力
- トラフィックの増減に対する動的な負荷分散にも対応した、高いスケーラビリティ
- プロセスが停止した場合には自動的に再起動してサービスの提供を継続可能な、高い可用性

Symantec Security Responseによる信頼のバックアップ

Symantec Security Responseは、グローバルに展開するインターネットセキュリティ全般に関するリサーチチームとテクニカルサポートチームで構成されています。ウイルスやワームをはじめ、悪意のあるプログラム、不正侵入の手法、OSやアプリケーションの脆弱性とそれを利用した攻撃方法などに関する調査/研究、また、それに基づくシマンテック製品のバックアップを行っています。そして、インターネット上における脅威の動向を365日24時間体制で監視し、情報発信、ソリューションとサポートを世界中のユーザーに提供しています。

システム要件

Symantec AntiVirus™ 4.3 for Network Attached Storage

Symantec AntiVirus Scan Engine 4.3 for Windows

- Windows 2000 Server / Advanced Server (SP2)、Windows Server 2003 Standard / Enterprise Edition
- 256 MB以上のメモリー
- 25 MB以上のハードディスク空き容量
- Microsoft Internet Explorer 6.0以降 (Webベース管理用)
- インターネット接続環境 (LiveUpdate用)

Symantec AntiVirus Scan Engine 4.3 for Sun Solaris

- Solaris 7、8、9 (SPARCプラットフォーム)
- 256 MB以上のメモリー
- 35 MB以上のハードディスク空き容量
- Microsoft Internet Explorer 6.0以降 (Webベース管理用)
- インターネット接続環境 (LiveUpdate用)

Symantec AntiVirus Scan Engine 4.3 for Red Hat Linux

- Red Hat Linux 7.3、8.0、9.0または Enterprise Linux 3.0 ES/AS
- 256 MB以上のメモリー
- 25 MB以上のハードディスク空き容量
- Microsoft Internet Explorer 6.0以降 (Webベース管理用)
- インターネット接続環境 (LiveUpdate用)

対応するNAS製品

Network Appliance Filer* (RPCを使用して連携)

Hitachi SANRISE 9900V Series NAS Blade (ICAPを使用して連携)

Sun StorageTek 9900 NAS Blade (ICAPを使用して連携)

Sun StorageTek 5220、5320、5320C (ICAPを使用して連携)

* Symantec AntiVirus Scan Engineは、Windows 2000またはWindows Server 2003にインストールする必要があります。

製品に関する最新の情報

シマンテックのWebサイトをご覧ください。

<http://www.symantec.com/region/jp/enterprise/index.html>