

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行わ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多くの実績を誇る Symantec 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

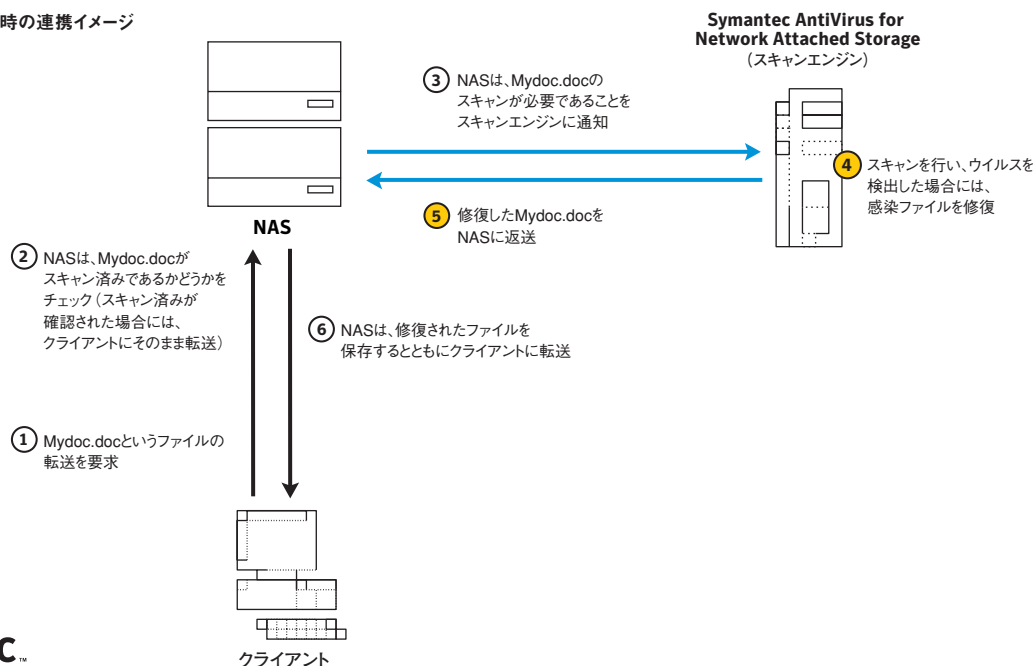
- Web ベースのインターフェースで容易に管理
 - NAS 上のデータに対する読み取り/書き込み時の脅威検出のログ記録とサマリーレポートの作成
 - SMTP/SNMP によるアラート発信
- 世界をリードするインターネットセキュリティの専門機関、Symantec Security Response による信頼の支援体制

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 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 Scan Engineを使用しています。

Symantec 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
 - セキュリティリスクとなるスパイウェア、アドウェアを検出、削除
 - 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
- Rapid Releaseによる高速な定義ファイル更新により、最新の脅威にいち早く対応

Symantec Security Responseによる信頼の支援体制

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支援を行っています。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。

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/jp/business>

システム要件

Symantec AntiVirus™ for Network Attached Storage 5.2

サポートされるオペレーティングシステム

仮想化環境 (VMware ESX/ESXi上での導入) をサポートします。

Symantec AntiVirus for NAS 5.2 for Windows

- Windows Server 2008 (32bit/64bit)
- Windows Server 2008 R2 (64bit)
- Windows Server 2003 (32bit/64bit)
- Windows Server 2003 R2 (32bit/64bit)
- Windows 2000 Server (最新のSP)

Symantec AntiVirus for NAS 5.2 for Solaris

- Solaris 9、10 (SPARC プラットフォーム)

Symantec AntiVirus for NAS 5.2 for Linux

- Red Hat Linux AS 3.0 / 4.0 (32bit)
- Red Hat Linux ES 3.0 / 4.0 / 5.0 (32bit)
- SUSE Linux ES 9 / 10 (32bit)

ハードウェアの最小構成

- 2.4 GHz Pentium 4、または 1 GHz SPARC
- Java 5、または 6
- 1 GB RAM
- 500 MB のハードディスク空き領域
- TCP/IP通信が可能なネットワークインターフェースと固定 IPアドレス

ハードウェアの最小構成

- Mozilla Firefox 1.5 以降
- Microsoft Internet Explorer 6 (SP1) 以降

対応するNAS製品

ストレージデバイス	使用するプロトコル	サポートバージョン
BlueArc Storage System	RPC	4.0以降
EMC Celerra Network Server	ICAP	CAVA 3.6.x以降
Hitachi USP/NSC NAS Blade	ICAP	03 - 07以降
Hitachi AMS/WMS with NAS Option	ICAP	04 - 03以降
Hitachi High-Performance NAS Platform	RPC	4.0以降
Network Appliance (NetApp) Filer	RPC	4.0以降
Network Appliance (NetApp) Filer	RPC	Data ONTAP version 6.1.3 R2 以降
Sun StorageTek 5000 NAS Appliance	ICAP	Sun NAS Firmware 4.20以降
Sun Storage 7000 Series	ICAP	Version 2008.10
Sun StorageTek 9990 NAS/9985 NAS	ICAP	version 03-07以降