

# Symantec AntiVirus™ Corporate Edition

## 企業ネットワークにおけるクライアントとサーバーのための、信頼性が高いウイルス対策

コンピュータウイルスの感染方法は多様化し、破壊力はより強まっています。メール送信機能を備え、ユーザーが感知しないところでメールを大量送信してしまうウイルスによるメールも減少しているとは言えません。こうしたウイルスはハードディスク上のファイルを添付して送信してしまうため、ビジネスの行方を左右してしまうような深刻な情報漏えいのリスクが発生しています。このように、全社規模にわたる個々のクライアント/サーバーにおけるウイルス対策は、ビジネス遂行のうえでクリティカルな課題となっています。

### 製品の概要

高いウイルス検出能力、迅速なアップデートと自動化された免疫システムによる新種ウイルスへの確実な対応、優れた管理機能とスケーラビリティ等、その実力が世界中で高い評価を受けている Symantec AntiVirus Corporate Editionは、企業の情報資産を最新のウイルスの脅威から保護します。

#### 〈キーポイント〉

- 信頼と実績のある高い検出率とパフォーマンス
  - Bloodhound技術により、未知のウイルスを検出
  - さまざまな圧縮形式のファイルに対応（多重圧縮を含む）
  - キャッシュ上のファイルやメモリーをスキャン
- 最新のウイルスにも速やかに対応
  - システムを再起動せずに、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
  - ウイルス定義ファイルを常に最新の状態に保つプッシュ型の更新（VDTM）とスケジューリングを行えるプル型の更新（LiveUpdate）
- セキュリティリスクとなるスパイウェア、アドウェアをリアルタイムで検出し、安全に削除
- 企業ユースに必須の優れた管理機能
  - ひとつのコンソールによって一元管理
  - クライアント/サーバーを論理的にグループ化して効率良く管理
- レポート機能統合
- VPNなどのネットワークデバイス\*接続環境におけるクライアントのポリシーチェックおよびポリシー適合の自動化（Endpoint Compliance）
  - \* Symantec, Checkpoint, Nortel, Cisco製品に対応
- 世界をリードするインターネットセキュリティ専門機関、Symantec Security Responseによる信頼のバックアップ

### 製品の特長とベネフィット

#### 実績と定評のある、信頼性が高いウイルス対策

Symantec AntiVirus Corporate Editionには、世界中で高い評価を得ているシマンテックの数々のアンチウイルス技術が活かされており、企業ネットワークのウイルス対策に欠かせない管理機能も強化されています。

- 洗練された独自の技術により、高い精度でウイルスを検出
  - ウイルス定義ファイルとスキャンエンジンの更新を一括して同時に行うため、最新のウイルスも確実に検出することができます。（NAVEX）
  - ヒューリスティックなスキャンを行うことにより、ウイルス定義ファイルの更新前でも新種/亜種などの未知のウイルスを高い精度で検出します。（Bloodhound）  
また、自らのコードを複雑に変化させていくことによって検出から逃れようとする、ポリモーフィック型のウイルスも検出します。（Striker）
  - ZIPやLZHなど、さまざまな形式の圧縮ファイルに潜むウイルスも検出してファイルを修復します。多重圧縮にも対応しています。
  - メモリー上のプロセスもスキャンし、脅威が検出された場合にはプロセスを停止します。
  - Lotus Notesメール、Microsoft Exchangeメール、POP3メールに対してもスキャンを実行します。

- 自動化された更新機能により、最新のウイルスにも的確に対処  
最新版のウイルス定義ファイルは、Symantec Security Response から迅速に提供されます。クライアント/サーバー共通のウイルス定義ファイルの更新は自動化されており、最新のウイルスにも迅速に対処することができます。

- VDTM (Virus Definition Transfer Method) による更新  
プッシュ型のVDTMによる更新では、大規模なネットワークにおいても、効率の良い確実な更新を実現します。

- マルチスレッド進行によるスピーディな配信

階層化されたサーバー、サーバー/クライアントの上位から下位の階層に向けて、マルチスレッドで複数の更新プロセスが同時に進行します。

- 差分更新によるトラフィックの負荷の抑制

ウイルス定義ファイルは差分更新が行えるため、最小限のトラフィックで更新を行うことができます。

- LiveUpdateによる更新

LiveUpdateサーバーに個別に接続して更新。設定されたスケジュールにしたがって自動的に、または必要に応じて手動で行います。差分更新に対応しているため、最小限のトラフィックで更新が行えます。社外に持ち出されたりサイト間を移動したりするノートPCタイプのクライアントの更新\*や、アウトブレイク時における個々のユーザーによる緊急更新などに適しています。

\* ネットワークに再接続されるまでの間、スケジュールを自動的に延期することも可能です。

- 自動化された免疫システムにより、未知のウイルスにも確実に対処  
Bloodhound技術によって検出された未知のウイルスに対しては、安全な隔離、Symantec Security Response への提出、解析結果にもとづいたウイルス定義ファイルの適用のプロセスを自動的に実行する Symantec Digital Immune System (デジタル免疫システム) が、確実な処理を行います。

- より高速なウイルススキャンを実現

- マルチスレッド技術の採用により、複数のファイルを同時にスキャン
- ハードディスク上のファイルだけでなく、キャッシュ上のファイルもスキャン

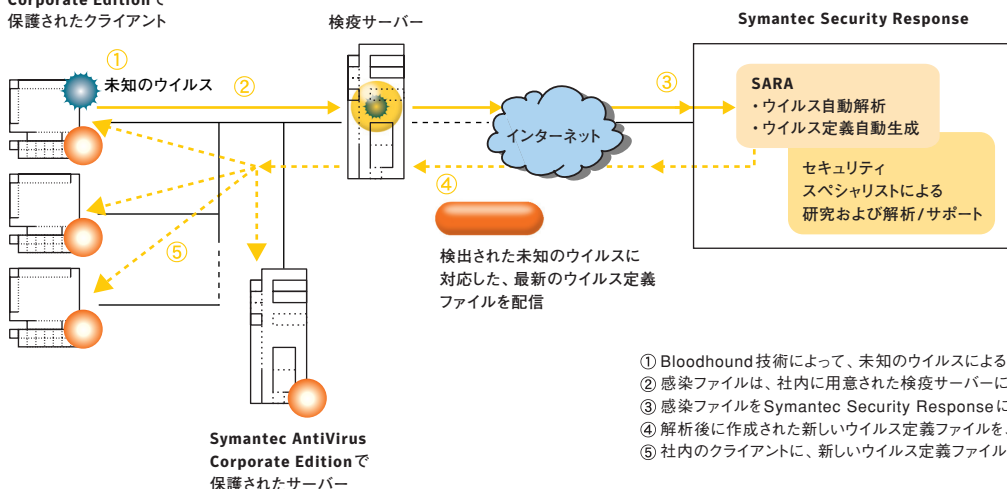
- 確実なスキャンのためにセキュリティ機能を強化

- 不適切な操作や人為的なミスでウイルスが侵入するリスクを低減
  - Symantec AntiVirus Corporate Edition の設定に関するレジストリの変更を記録
  - リアルタイムスキャンが手動で停止されていても、設定時間を経過した時点で自動的に実行
  - 最新のウイルス定義ファイルを使用していないクライアントに対して、強制的に更新を実行
- ウイルス定義ファイルの改ざんを防止

電子的な署名の確認によって、ウイルス定義ファイルを正しく更新。ウイルスや悪意ある操作によるウイルス定義ファイルの不正な変更を防止します。

#### Digital Immune System により、未知のウイルスにも的確に対処

Symantec AntiVirus Corporate Edition で保護されたクライアント



- ① Bloodhound 技術によって、未知のウイルスによる感染ファイルを検出
- ② 感染ファイルは、社内に用意された検疫サーバーに安全に隔離
- ③ 感染ファイルを Symantec Security Response に提出
- ④ 解析後に作成された新しいウイルス定義ファイルを、提出元の検疫サーバーに配信
- ⑤ 社内のクライアントに、新しいウイルス定義ファイルを適用

Symantec Security Response では、未知のウイルスの解析、駆除方法とファイルの修復方法を定義したファイルの生成、配信までの全てのプロセスが、SARA (Symantec AntiVirus Research Automation) によって自動化されています。このシステムにより、世界中で発見される新種のウイルスに対する、迅速で的確な対処が実現されています。

● 拡大を続ける情報セキュリティのニーズに対応

情報漏えいや不要な情報発信の原因となりうるスパイウェアやアドウェア、不正アクセスやハッキングの原因となりうるダイアラーやリモートアクセスツールも検出します。

- スパイウェア、アドウェアのリアルタイムでの検出と安全な削除が可能。セキュリティリスクに対してさらに積極的に対処することができます。

● スキャンは柔軟にスケジューリング可能

- パフォーマンスを優先したい場合は、スケジュールされたスキャンを延期できます。

- コンピュータを使用していない時のみスキャンを行うように、優先度を変更できます。

- ノートPCの場合には、ACアダプタ使用時のみスキャンを実行するように設定できます。

優れた管理機能により、緊急時の迅速な対応とTCOの抑制を実現

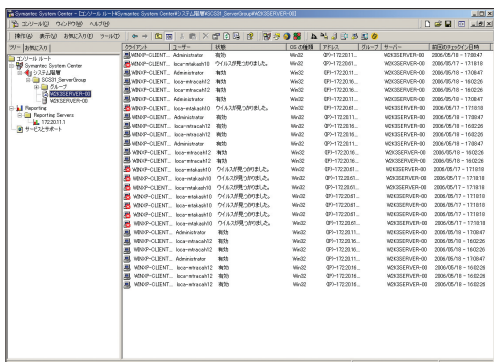
● 高機能コンソールを使用して一元的に集中管理

各機能の設定やログの監視、アップデート作業は、管理コンソール Symantec System Center を使用して一元管理できます。それぞれのクライアントの設定やセキュリティ状況をネットワーク全体にわたって把握でき、高度な管理と緊急時の的確な対応を容易に行うことができます。また、複数のクライアントやサーバーを論理グループとしてまとめ、各グループに適切なポリシーを迅速に適用することができます。

- ファイル共有により拡散するウイルスの侵入口となったコンピュータを特定

- ウイルスアウトブレイクなどの緊急時に、複数のクライアントPCに対して同時にLiveUpdateを強制的に実行

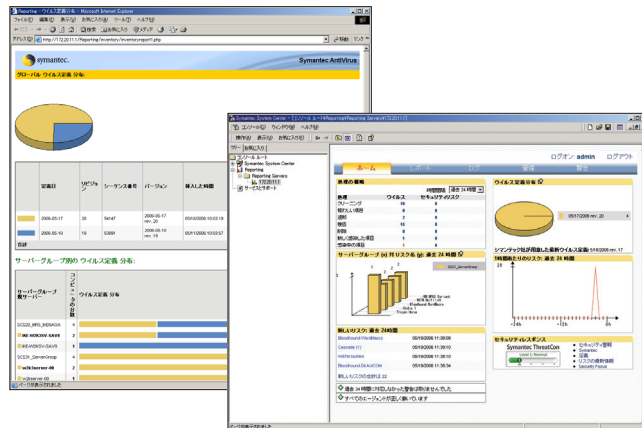
- 外部に持ち出されて使用されるノートPCのログを、ネットワーク再接続時に収集



多数のクライアント/サーバーの設定を一元管理可能な Symantec System Center

● レポート機能による的確な状況把握

ウイルス定義ファイル配布状況、Symantec AntiVirusのバージョンといったクライアント状況、ウイルスおよびセキュリティリスクの検出結果相関図などのレポートをSymantec System CenterまたはWebブラウザ上で表示することができます。管理者はこれらの情報を、設定したスケジュールで、または必要に応じて取得し、レポートをベースに最善の対策を迅速に行うことが可能となります。



レポート結果はグラフや表でわかりやすく表示

● セキュリティポリシーにもとづいた管理

VPN接続を試みるクライアントPCに対しセキュリティチェックを実行、設定されたポリシーと異なっている場合、ポリシーに適合するよう修正します。(Endpoint Compliance)

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および研究、また、それにもと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™ Corporate Edition 10.2

#### Symantec AntiVirus Corporate Edition 10.2 クライアント (32 bit)

- Windows Vista

#### Symantec AntiVirus Corporate Edition 10.1 クライアント (32 bit)

- Windows XP Home / Professional / Tablet PC Edition、  
Windows Server 2003 (32 bit) Web / Standard / Enterprise /  
Datacenter Edition (SP1およびR2)\*、  
Windows 2000 Professional / Server / Advanced Server

#### Symantec AntiVirus Corporate Edition 10.2 クライアント (64 bit)

- Intel EM64T、AMD 64 プラットフォーム
- Windows Vista

#### Symantec AntiVirus Corporate Edition 10.1 クライアント (64 bit)

- Intel EM64T、AMD 64 プラットフォーム
- Windows XP Professional x64 Edition、  
Windows Server 2003 Standard / Enterprise /  
Datacenter x64 Edition (SP1およびR2)

#### Symantec AntiVirus Corporate Edition 10.1 管理サーバー (Windows)

- Windows XP Professional、  
Windows 2000 Professional / Server / Advanced Server、  
Windows Server 2003 (32 bit) Web / Standard / Enterprise /  
Datacenter Edition (SP1およびR2)\*

#### Symantec AntiVirus Corporate Edition 10.1 管理サーバー (NetWare)

- NetWare 5.1 (SP8) 以降 / 6.0 (SP5) 以降 / 6.5 (SP2) 以降  
(NetWare SFT IIIには対応していません)

#### Symantec System Center 10.1

- Windows XP Professional、  
Windows Server 2003 (32 bit) Web / Standard / Enterprise /  
Datacenter Edition (SP1およびR2)\*  
Windows 2000 Professional / Server / Advanced Server、
- Microsoft Internet Explorer 5.5 (SP2) 以降
- Microsoft Management Console version 1.2

#### レポートサーバー

- Windows Server 2003 (32 bit) Standard/  
Enterprise Edition (SP1およびR2)  
Windows 2000 Server/Advanced Server (SP4 以降)、
- Microsoft IIS 4.0 以降
- MSDE 2000 (SP4以降) またはMicrosoft SQL Server 2000  
(SP1以降) またはMicrosoft SQL Server 2005以降
- Microsoft Internet Explorer 5.5 (SP2以降)

#### レポートエージェント

- Windows Vista  
Windows XP Professional、  
Windows Server 2003 (32 bit) Web/Standard/Enterprise/  
Datacenter Edition (SP1およびR2)\*  
Windows 2000 Professional/Server/Advanced Server、

#### 検疫サーバー

- Windows XP Professional、  
Windows Server 2003 (32 bit) Web /Standard / Enterprise /  
Datacenter Edition (SP1およびR2)\*  
Windows 2000 Professional / Server / Advanced Server、
- Microsoft Internet Explorer 5.5 (SP2) 以降

#### 検疫コンソール

- Windows XP Professional  
Windows 2000 Professional / Server / Advanced Server、
- Microsoft Internet Explorer 5.5 (SP2) 以降
- Microsoft Management Console version 1.2

\* Windows Server 2003 Web EditionはSP1のみとなります。

※ NEC社製PC-9800、PC-9821シリーズでは本製品は使用できません。

※ Windows環境での使用におけるメモリーとプロセッサの要件については、Microsoft社の推奨条件を参照してください。

※ Windows XP環境で「システムの復元」機能が動作している場合は、さらにディスク容量が必要になる場合があります。詳しくはOSのマニュアルを参照してください。

※ Windows Server上のMacintoshボリュームには対応していません。

## 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>