

# Symantec™ Client Security

アンチウイルス、クライアントファイアウォール、侵入防止システムを統合し、進化し続ける脅威からクライアントPCを適切に保護

ネットワークに接続しているだけで感染するウイルスによる被害は依然として後を絶ちません。また、ユーザーが感知しないところでハードディスク上のファイルを添付してメールを発信するウイルスも増えています。ウイルスによるメール発信には、特に情報漏えいのリスクが伴います。しかし、ゲートウェイのファイアウォールでは、社内から送信されるメールがウイルスによるものなのかを容易に識別できません。

社外に持ち出されるノートPCは、ゲートウェイのファイアウォールによる保護を受けずにインターネットに直接接続されるため、さらなるリスクに曝されています。また、社外でウイルスに感染した後に社内LANに接続されることにより、ウイルス拡散の発信源になってしまうケースも発生します。社内ハッキングや、プライバシー情報などを盗み取る悪意あるWebコンテンツやスパイウェアも増加しています。

このようなさまざまなクライアントのセキュリティ問題に対するソリューションとして、クライアントPCごとに搭載するファイアウォール、すなわち、クライアントファイアウォールを従来のウイルス対策に統合するニーズが高まっています。

## 製品の概要

Symantec Client Securityは、アンチウイルスにクライアントファイアウォールと侵入防止システムを統合し、クライアントPCを1台1台個別に保護します。ウイルススキャンに加えてPCごとの通信の制御を行うため、通信によって感染活動を行うウイルスやワーム、企業ネットワーク内部からのハッキング、DDoS 攻撃、モバイルPCのセキュリティ、情報漏えい、企業内部のアクセス管理など、さまざまなセキュリティ課題に対処することができます。

ネットワーク上に多数存在するクライアントの管理を的確かつ容易に行なうための機能も充実しています。それぞれのPC上で動作しているアンチウイルス、クライアントファイアウォール、侵入防止システムの設定とログの監視やセキュリティアップデートを、ひとつのコンソールから一元的に行うことができます。ファイアウォールのルールは企業のポリシーに応じて独自のものを作成することができ、それを容易に行うためのツールも備わっています。Symantec Client Securityは、複数の製品を組み合わせる場合と比べ、少ない導入/運用コストでハイレベルなクライアントセキュリティを実現します。

## 〈キーポイント〉

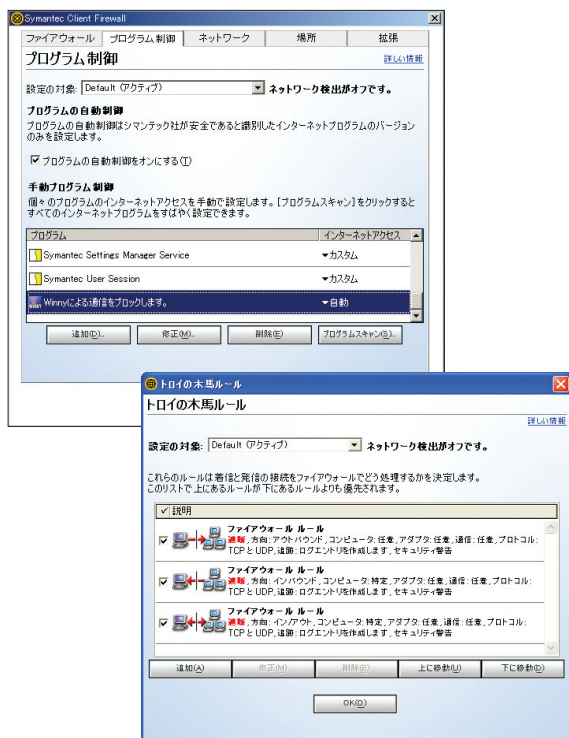
- アンチウイルスに、クライアントファイアウォールと侵入防止システムを統合
- クライアントごとのファイアウォールと侵入防止システムで、さまざまなセキュリティ課題を解決
  - ネットワークに接続するだけで感染するウイルスの侵入や、ウイルスによるメールの大量送信をブロック
  - 脆弱性を利用する攻撃に対し、より早期の段階で防御
  - ハッキング、DDoS攻撃、情報漏えいを防止
  - ポリシーにもとづいて、インターネットや社内のリソースへのアクセスをコントロール
  - モバイルPCを社外でも適切に保護
- セキュリティリスクとなるスパイウェア、アドウェアをリアルタイムで検出し、安全に削除
- 充実した管理ツールにより、少ない管理コストでセキュリティを確実に強化
  - 設定/ログの監視/アップデート/緊急時の対処を一元管理
  - 個々のクライアントのインターネットアクセスを調査し、最適なファイアウォールのルールを作成
  - 接続環境に応じ、ファイアウォールのルールを自動変更
- **NEW** レポート機能統合
- **NEW** 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

### 強力なクライアントファイアウォールと侵入防止システムを搭載

Symantec Client Securityは、クライアントファイアウォールと侵入防止システムの統合により、ウイルスやワームによる不正な通信、ハッキング、情報漏えいのリスクなどから、クライアントPCを的確に保護します。

- クライアントPCが行う通信を1台ごとに制御して保護
  - 許可されたアプリケーションソフトウェア以外による通信を禁止
    - メールソフトに依存しないウイルス自身のSMTPエンジンによる送信を防止
    - クライアントPCがDDoS攻撃の発信源として利用されることを防止
    - ネットワークゲームや業務と関係のないチャットプログラムなどの通信を禁止
  - 許可していないポートに対する外部からの通信を遮断
  - ポートスキャンやトロイの木馬による不審なアクセスを検知して遮断
  - 攻撃パターンに依存せずに、脆弱性ベースで攻撃を検知。脆弱性を利用する攻撃に対し、より早い段階で防御
  - 許可されていないWebサイトからのJavaアプレットやActiveXコントロールのダウンロードをストップ。悪意のあるWebコンテンツから保護



クライアントPCが行う通信を1台ごとに制御して保護

- インターネットゾーン制御  
IPアドレス、あるいはIPアドレスの範囲を指定することによって、クライアントごとにアクセス制御を行うことが可能です。
  - 特定のIPアドレスからの不審なアクセスが頻繁に起こる場合には、アクセスを定常的に禁止
  - 特定のサイトに対するアクセスを禁止
  - 社内間の通信に対してもアクセスを制御（開発部や人事部のネットワークリソースへのアクセス制限の実施など）
- プライバシー保護  
機密情報として取り扱う文字列をユーザーごとに定義でき、これらの情報発信を監視できます。IDやパスワードなどの情報がユーザーの感知しないところで発信されたり、Webコンテンツ中のスクリプトによって読み出されてしまうことを防止することができます。
- 広告ブロック  
Webアクセス時にダウンロードされる、バナー、ポップアップやFlashによる広告をブロックすることが可能です。不要な広告の表示、ソフトウェアの競合などを防止し、社員の生産性の低下を防ぐことができます。

### 実績と定評のあるアンチウイルスを統合

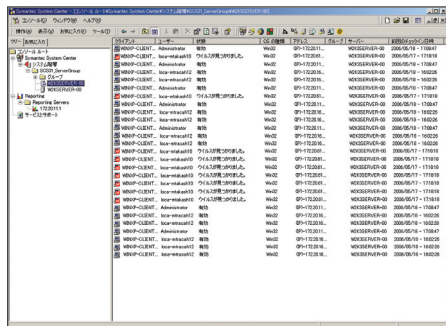
Symantec Client Securityには、管理機能が強化された企業向けクライアント/サーバー用アンチウイルス製品Symantec AntiVirus Corporate Editionが統合されています。ウイルスやワーム、トロイの木馬などの脅威に加え、さらにスパイウェア、アドウェアなどのセキュリティリスクを高い精度で検出します。

- 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、最新のウイルスも的確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/未知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。
  - 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。
- 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を検出/削除することが可能です。
- スキャンは柔軟にスケジューリング可能
  - コンピュータ使用時間以外のスキャン、ノートPCのACアダプタ使用時のみのスキャンなど柔軟なスキャンのスケジューリングが可能です。

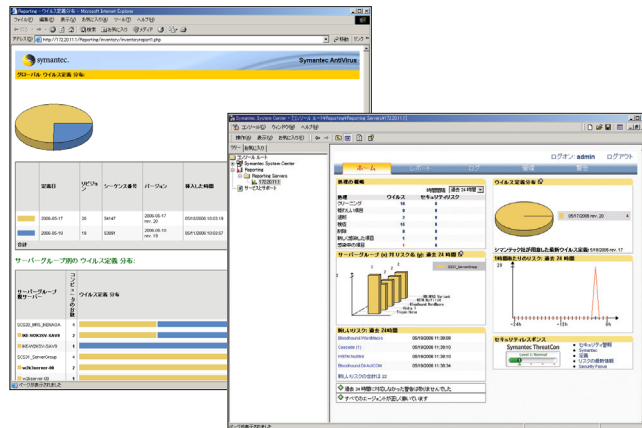
### 容易に管理し、脅威に迅速に対応

- 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

- **NEW** 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および Symantec Client Firewall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

- クライアントファイアウォールを容易に管理
  - クライアントファイアウォールと侵入防止システムの設定のためのポリシーは、専用ツール Symantec Client Firewall Administrator を使用して容易に作成、および、配布/適用が可能です。また、ポリシー作成のために、それぞれのPCがどのようなインターネットアクセスを行っているかを容易に調べることもできます。
- セキュリティポリシーにもとづいた管理を実施
  - セキュリティポリシーにもとづいた管理を行うことにより、一定のセキュリティレベルを確保することができます。
  - ネットワーク監視機能により、ウイルス対策製品がインストールされていないクライアント/サーバーを検出し、シマンテックと他社の製品を識別
  - **NEW** 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™ Client Security 3.1

#### Symantec Client Security 3.1 クライアント (32 bit)

- Windows 2000 Professional、  
Windows XP Home / Professional / Tablet PC Edition
- Microsoft Internet Explorer 5.5 (SP2) 以降

#### Symantec Client Security 3.1 クライアント (64 bit)\*1

- 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)\*2

#### Symantec Client Security 3.1 管理サーバー (Windows)\*1

- Windows 2000 Professional / Server / Advanced Server、  
Windows XP Professional、  
Windows Server 2003 (32 bit) Web / Standard / Enterprise /  
Datacenter Edition (SP1およびR2)\*2

#### Symantec Client Security 3.1 管理サーバー (NetWare)\*1

- 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 2000 Professional / Server / Advanced Server、  
Windows XP Professional、  
Windows Server 2003 (32 bit) Web / Standard / Enterprise /  
Datacenter Edition (SP1およびR2)\*2
- Microsoft Internet Explorer 5.5 (SP2) 以降
- Microsoft Management Console version 1.2

#### レポートサーバー

- Windows 2000 Server / Advanced Server (SP4 以降)、  
Windows Server 2003 (32 bit) Standard /  
Enterprise Edition (SP1およびR2)
- 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 2000 Professional / Server / Advanced Server、  
Windows XP Professional、  
Windows Server 2003 (32 bit) Web / Standard / Enterprise /  
Datacenter Edition (SP1およびR2)\*2

#### 検疫サーバー

- Windows 2000 Professional / Server / Advanced Server、  
Windows XP Professional、  
Windows Server 2003 (32 bit) Web / Standard / Enterprise /  
Datacenter Edition (SP1およびR2)\*2
- Microsoft Internet Explorer 5.5 (SP2) 以降

#### 検疫コンソール

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

#### Symantec Client Firewall Administrator

- Windows 2000 Professional / Server / Advanced Server、  
Windows XP Professional、  
Windows Server 2003 (32 bit) Web / Standard / Enterprise /  
Datacenter Edition (SP1およびR2)\*2
- Microsoft Internet Explorer 5.5 (SP2) 以降

\*1 ウイルス対策機能のみとなります。

\*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サーバー上の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>