

# Symantec™ Endpoint Protection および Symantec Network Access Control クラ イアントガイド

Microsoft Windows 用



# Symantec Endpoint Protection および Symantec Network Access Control クライアントガイド

本書で説明するソフトウェアは、使用許諾契約に基づいて提供され、その内容に同意する場合にのみ使用することができます。

Documentation version 11.00.06.00.00

## 登録商標

Copyright © 2010 Symantec Corporation. All rights reserved.

Symantec、Symantec ロゴ、Bloodhound、Confidence Online、Digital Immune System、LiveUpdate、Norton、Sygate、TruScan は、Symantec Corporation または同社の米国およびその他の国における関連会社の商標または登録商標です。その他の会社名、製品名は各社の登録商標または商標です。

Symantec 製品には、特定のサードパーティ製ソフトウェアが配布、組み込み、または同梱されている場合があります。また、本製品のインストールおよび使用にともない、サードパーティ製ソフトウェアの使用を推奨する場合があります。このライセンス対象ソフトウェアには、オープンソースのフリーウェアライセンスで利用可能なサードパーティのソフトウェアプログラム（「サードパーティプログラム」）を含めることができるものとします。本ソフトウェアに付随する使用許諾契約では、オープンソースのフリーウェアライセンスでお客様が有することのできる権利または義務は変更されないものとします。サードパーティのソフトウェアの著作権に関する情報については、本製品に付属のサードパーティ製ソフトウェアのファイルを参照してください。

本書に記載する製品は、使用、コピー、頒布、逆コンパイルおよびリバース・エンジニアリングを制限するライセンスに基づいて頒布されています。Symantec Corporation からの書面による許可なく本書を複製することはできません。

Symantec Corporation が提供する技術文書は Symantec Corporation の著作物であり、Symantec Corporation が保有するものです。保証の免責: 技術文書は現状で提供され、Symantec Corporation はその正確性や使用について何ら保証いたしません。技術文書またはこれに記載される情報はお客様の責任にてご使用ください。本書には、技術的な誤りやその他不正確な点を含んでいる可能性があります。Symantec は事前の通知なく本書を変更する権利を留保します。

本ソフトウェアは、FAR 12.212 の規定によって商用コンピュータソフトウェアと見なされ、FAR 52.227-19「Commercial Computer Software - Restricted Rights」、DFARS 227.7202「Rights in Commercial Computer Software or Commercial Computer Software Documentation」、その他の後継規制の規定により制限された権利の対象となります。米国政府による本ソフトウェアの使用、修正、複製のリリース、実演、表示または開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

弊社製品に関して、当資料で明示的に禁止、あるいは否定されていない利用形態およびシステム構成などについて、これを包括的かつ暗黙的に保証するものではありません。また、弊社製品が稼動するシステムの整合性や処理性能に関しても、これを暗黙的に保証するものではありません。これらの保証がない状況で、弊社製品の導入、稼動、展開した結果として直接的、あるいは間接的に発生した損害等についてこれが補償されることはありません。製品の導入、稼動、展開にあたっては、お客様の利用目的に合致することを事前に十分に検証および確認いただく前提で、計画および準備をお願いします。

<b>第 1 部</b>	<b>クライアントを始めましょう</b> .....	9
<b>第 1 章</b>	<b>クライアントの概要</b> .....	11
	クライアントについて .....	11
	Symantec Endpoint Protection クライアントについて .....	12
	ウイルス対策とスパイウェア対策について .....	12
	プロアクティブ脅威防止について .....	13
	ネットワーク脅威防止について .....	14
	Symantec Network Access Control クライアントについて .....	14
<b>第 2 章</b>	<b>クライアントへの応答</b> .....	15
	クライアントの介入について .....	15
	感染ファイルへの対応 .....	16
	ウイルスが原因の損傷について .....	17
	通知と警告について .....	18
	アプリケーション関連通知への応答 .....	18
	セキュリティ警告への応答 .....	21
	ネットワークアクセス制御通知への応答 .....	21
<b>第 3 章</b>	<b>クライアントの管理</b> .....	23
	集中管理下クライアントと自己管理クライアントについて .....	24
	自己管理クライアントの集中管理下クライアントへの変換 .....	25
	コンピュータの保護の更新 .....	26
	内容の即時更新 .....	27
	スケジュールに従って内容を更新 .....	27
	セキュリティポリシーについて .....	28
	ポリシーファイルを手動で更新 .....	28
	ポリシーが更新されていることの検証 .....	29
	コンピュータをただちにスキャンする .....	29
	スキャンの一時停止と遅延 .....	30
	保護技術の有効化と無効化 .....	31
	Auto-Protect の有効化または無効化 .....	33
	ネットワーク脅威防止の有効化または無効化 .....	34
	プロアクティブ脅威防止の有効化と無効化 .....	35

改変対策について .....	35
改変対策の有効化、無効化、設定 .....	36
コンピュータのセキュリティテスト .....	37
場所について .....	38
場所の変更 .....	38
通知領域アイコンについて .....	39
通知領域アイコンの非表示と表示 .....	40
管理者によるコンピュータ再起動の防止について .....	41

## 第 2 部

Symantec Endpoint Protection クライアン トでの保護の管理 .....	43
--	----

## 第 4 章

ウイルス対策とスパイウェア対策の管理 .....	45
ウイルスとセキュリティリスクについて .....	46
クライアントはウイルスとセキュリティリスクにどう応答するか .....	49
ウイルス対策とスパイウェア対策の設定について .....	50
ファイルのスキャンについて .....	50
電子メールアプリケーションが単一の受信ボックスファイルを使ってい る場合 .....	50
拡張子によるスキャンについて .....	51
すべてのファイルのスキャンについて .....	51
マクロウイルス感染の防止について .....	52
クライアントがウイルスまたはセキュリティリスクを検出した場合 .....	52
Auto-Protect について .....	53
Auto-Protect とセキュリティリスクについて .....	53
Auto-Protect と電子メールスキャンについて .....	54
暗号化電子メール接続に対する Auto-Protect 処理の無効化 .....	55
Auto-Protect スキャン統計の表示 .....	56
リスクリストの表示 .....	56
ファイルの種類を指定する Auto-Protect の設定 .....	56
Auto-Protect でのセキュリティリスクのスキャンと遮断の有効化と無効 化 .....	57
ネットワークスキャンの設定 .....	58
ウイルススキャンとスパイウェアスキャンの操作 .....	60
ウイルススキャンとスパイウェアスキャンの動作 .....	60
ウイルス定義ファイルについて .....	62
圧縮ファイルのスキャンについて .....	62
ユーザー定義スキャンのスケジュール .....	62
オンデマンドまたはコンピュータの起動時に実行されるスキャンのスケ ジュール .....	65
起動時、ユーザー定義、定時の各スキャンの編集と削除 .....	66

スキャン結果の解釈 .....	66
スキャン結果または <b>Auto-Protect</b> の結果に対する操作 .....	67
ウイルスとセキュリティリスクに対する処理の設定 .....	69
ウイルスに対する第 2 の処理を割り当てるためのヒント .....	72
セキュリティリスクに対する第 2 の処理を割り当てるためのヒント .....	73
リスクの影響評価について .....	73
ウイルスとセキュリティリスクに対する通知の設定 .....	74
スキャン対象からの項目の除外について .....	76
スキャンからの項目の除外 .....	77
検疫ファイルの処理について .....	78
検疫にある感染ファイルについて .....	79
検疫にある感染ファイルの扱い方について .....	79
セキュリティリスクに感染したファイルの扱い方について .....	80
検疫の管理 .....	80
検疫にあるファイルとファイルの詳細の表示 .....	81
検疫にあるファイルのウイルス再スキャン .....	81
修復したファイルが元の場所に戻らない場合 .....	82
バックアップ項目の消去 .....	82
検疫からのファイルの削除 .....	82
検疫からのファイルの自動削除 .....	83
感染の可能性があるファイルを分析のためにシマンテックセキュリティ レスポンスに提出 .....	84
スキャン検出についての情報のシマンテックセキュリティレスポンスへの提 出 .....	84
クライアントと <b>Windows</b> セキュリティセンターについて .....	85
<b>第 5 章</b> <b>プロアクティブ脅威防止の管理</b> .....	87
<b>TruScan</b> プロアクティブ脅威スキャンについて .....	87
<b>TruScan</b> プロアクティブ脅威スキャンで診断されるプロセスとアプリケー ション .....	88
<b>TruScan</b> プロアクティブ脅威スキャンの例外について .....	89
<b>TruScan</b> プロアクティブ脅威スキャンの検出について .....	89
誤認に対する処理について .....	90
<b>TruScan</b> プロアクティブ脅威スキャンを実行する頻度の設定 .....	91
<b>TruScan</b> プロアクティブ脅威検出の管理 .....	91
商用アプリケーションの検出に対する処理の設定 .....	92
トロイの木馬、ワーム、キーロガーの検出に対する処理と感度レベルの 指定 .....	93
<b>TruScan</b> プロアクティブ脅威スキャンが検出するプロセスの種類 の指定 .....	94
<b>TruScan</b> プロアクティブ脅威スキャン検出時の通知の設定 .....	94

シマンテックセキュリティレスポンスへの TruScan プロアクティブ脅威スキャンに関する情報の提出 .....	95
TruScan プロアクティブ脅威スキャンからのプロセスの除外 .....	96

## 第 6 章 ネットワーク脅威防止の管理 .....

ネットワーク脅威防止の管理について .....	98
ファイアウォール保護の管理 .....	98
ファイアウォールのしくみ .....	100
ファイアウォールルールについて .....	101
ファイアウォールルールの要素について .....	102
ステートフルインスペクションについて .....	104
ルール処理順序について .....	105
ファイアウォールルールの追加 .....	106
ファイアウォールルールの順序の変更 .....	107
ルールの有効化と無効化 .....	107
ルールのエクスポートとインポート .....	108
組み込みのファイアウォールルールについて .....	109
トラフィックの設定とステルス Web 参照の設定の有効化 .....	110
スマートトラフィックフィルタの有効化 .....	110
ネットワークでのファイルとプリンタの共有の有効化 .....	111
トラフィックの遮断 .....	113
アプリケーション固有の設定 .....	114
アプリケーションからの制限の削除 .....	116
侵入防止保護の管理 .....	117
侵入防止保護のしくみ .....	117
侵入防止の設定の有効化または無効化 .....	118
侵入防止の通知の設定 .....	119
攻撃側コンピュータの遮断と遮断解除 .....	120

## 第 3 部 Symantec Network Access Control クライアントでの保護の管理 .....

### 第 7 章 Symantec Network Access Control の管理 .....

Symantec Network Access Control の仕組み .....	123
ホストインテグリティ検査の実行 .....	125
ホストインテグリティポリシーの更新について .....	125
コンピュータの修復 .....	125
Symantec Network Access Control ログの表示 .....	126
クライアントがエンフォーサと連携する方法 .....	127
802.1x 認証向けのクライアントの設定 .....	127
コンピュータの再認証 .....	130

<b>第 4 部</b>	<b>監視とログ記録</b> .....	133
<b>第 8 章</b>	<b>ログの使用と管理</b> .....	135
	ログについて .....	135
	ログサイズの管理 .....	137
	ウイルス対策とスパイウェア対策ログのエントリの保持期間の設定 .....	137
	ネットワーク脅威防止ログとクライアント管理ログのサイズの設定 .....	137
	ネットワーク脅威防止ログエントリとクライアント管理ログエントリの保持 日数の設定 .....	138
	ウイルス対策とスパイウェア対策のシステムログの内容の削除につい て .....	138
	ネットワーク脅威防止ログとクライアント管理ログの内容の削除 .....	138
	リスクログと脅威ログからのリスクと脅威の検疫 .....	139
	ネットワーク脅威防止ログとクライアント管理ログの使用 .....	139
	ネットワーク脅威防止ログとクライアント管理ログの更新 .....	140
	パケットログの有効化 .....	140
	アクティブレスポンスの停止 .....	140
	ログに記録されたイベントの送信元の追跡 .....	141
	Symantec Network Access Control でのクライアント管理ログの使 用 .....	141
	ログデータのエクスポート .....	142
<b>索引</b> .....		145



# 1

## クライアントを始めましょう

- [第1章 クライアントの概要](#)
- [第2章 クライアントへの応答](#)
- [第3章 クライアントの管理](#)



# クライアントの概要

この章では以下の項目について説明しています。

- [クライアントについて](#)
- [Symantec Endpoint Protection クライアントについて](#)
- [Symantec Network Access Control クライアントについて](#)

## クライアントについて

シマンテック社では、同時または個別に使用可能な次の 2 種類のエンドポイント保護製品を用意しています。

表 1-1 エンドポイント保護クライアントの種類

クライアントの種類	説明
Symantec Endpoint Protection	Symantec Endpoint Protection は、コンピュータをインターネットの脅威とセキュリティリスクから保護します。  p.12 の「 <a href="#">Symantec Endpoint Protection クライアントについて</a> 」を参照してください。
Symantec Network Access Control	Symantec Network Access Control を使うと、コンピュータのセキュリティ設定がネットワークポリシーと必ず一致します。セキュリティ設定には、ソフトウェア、ソフトウェア設定、シグネチャファイル、パッチ、その他の要素が含まれます。  p.14 の「 <a href="#">Symantec Network Access Control クライアントについて</a> 」を参照してください。

ユーザーのコンピュータには、ユーザーまたは管理者によって、これらの Symantec クライアントソフトウェア製品のどちらか一方または両方がインストールされます。管理者がクライアントをインストールした場合、管理者がクライアントで有効にする製品を特定します。クライアントを使って実行する必要のあるタスクについては、管理者が助言できます。

コンピュータにクライアントをインストールした場合、それはスタンドアロンインストールです。スタンドアロンインストールは管理者がクライアントソフトウェアを管理しないことを意味します。

p.24 の「[集中管理下クライアントと自己管理クライアントについて](#)」を参照してください。

---

**メモ:** ユーザーまたは管理者がこれらの製品の一方のみをユーザーのコンピュータにインストールする場合、その製品名がタイトルバーに表示されます。両方の種類の保護を有効にすると、タイトルバーに **Symantec Endpoint Protection** が表示されます。

---

## Symantec Endpoint Protection クライアントについて

クライアントのデフォルト設定では、ウイルス対策とスパイウェア対策、プロアクティブ脅威防止、ネットワーク脅威防止の機能が提供されます。企業のニーズに合わせる場合、システムの処理効率を最適化する場合、適用しないオプションを無効にする場合には、デフォルト設定を調整できます。

p.12 の「[ウイルス対策とスパイウェア対策について](#)」を参照してください。

p.13 の「[プロアクティブ脅威防止について](#)」を参照してください。

p.14 の「[ネットワーク脅威防止について](#)」を参照してください。

コンピュータを保護するために次のように **Symantec Endpoint Protection** クライアントを使うことができます:

- コンピュータにウイルス、既知の脅威、セキュリティリスクがないかスキャンする  
p.29 の「[コンピュータをただちにスキャンする](#)」を参照してください。
- ポートに既知の攻撃シグネチャがないか監視する  
p.135 の「[ログについて](#)」を参照してください。
- コンピュータ上のプログラムに疑わしい動作がないか監視する  
p.87 の「[TruScan プロアクティブ脅威スキャンについて](#)」を参照してください。
- ネットワーク攻撃からコンピュータを保護する  
p.98 の「[ファイアウォール保護の管理](#)」を参照してください。

## ウイルス対策とスパイウェア対策について

ウイルス対策とスパイウェア対策は、コンピュータを既知のウイルスとセキュリティリスクから確実に保護します。ウイルスをすばやく検出してコンピュータから除去すれば、他のファイルへの伝染と損傷を防止できます。ウイルスとセキュリティリスクの影響は修復できます。**Symantec Endpoint Protection** クライアントがウイルスまたはセキュリティリスクを検出すると、デフォルトでユーザーに検出を通知します。通知が不要の場合、ユーザーまたは管理者はリスクを自動的に処理するようにクライアントを設定できます。

ウイルス対策とスパイウェア対策はシグネチャに基づくスキャンを実行します。スキャンには次のような種類があります。

■ **Auto-Protect** スキャン

**Auto-Protect** は常時実行されており、コンピュータ上の活動を監視することによってコンピュータをリアルタイムで保護します。ファイルを実行したり開くときに、**Auto-Protect** はウイルスとセキュリティリスクを検索します。ファイルに変更を加えたときにも、ウイルスとセキュリティリスクを検索します。たとえば、ファイルの名前の変更、保存、フォルダ間でのファイルの移動またはコピーなどが該当します。

p.53 の「**Auto-Protect** について」を参照してください。

p.56 の「**ファイルの種類を指定する Auto-Protect の設定**」を参照してください。

■ 定時スキャン、起動時スキャン、オンデマンドスキャン

ユーザーまたは管理者はコンピュータ上でその他のスキャンを実行するように設定できます。このようなスキャンでは、感染ファイルで未処理のウイルスシグネチャが検索されます。また、感染ファイルとシステム情報でセキュリティリスクのシグネチャも検索されます。ユーザーまたは管理者がスキャンを実行すると、コンピュータ上のファイルにウイルスまたはセキュリティリスクがないかを体系的にチェックできます。セキュリティリスクにはアドウェアまたはスパイウェアが含まれることがあります。

p.62 の「**ユーザー定義スキャンのスケジュール**」を参照してください。

p.65 の「**オンデマンドまたはコンピュータの起動時に実行されるスキャンのスケジュール**」を参照してください。

## プロアクティブ脅威防止について

プロアクティブ脅威防止には、**TruScan** プロアクティブ脅威スキャンが含まれています。これはコンピュータを未知の脅威によるゼロデイ攻撃から確実に保護します。これらのスキャンはヒューリスティックを使って、プログラムの構造、動作、その他の属性にウイルスのような性質がないか分析します。多くの場合、大量メール送信型ワームやマクロウイルスなどの脅威から保護することができます。ウイルス定義とセキュリティリスク定義を更新する前にワームやマクロウイルスに遭遇することがあります。プロアクティブ脅威スキャンは、HTML、VBScript、JavaScript の各ファイルでスクリプトベースの脅威を検索します。

p.87 の「**TruScan** プロアクティブ脅威スキャンについて」を参照してください。

プロアクティブ脅威スキャンは、悪質な目的で使われる可能性のある商用のアプリケーションも検出します。このような商用のアプリケーションには、リモート制御プログラムまたはキーロガーが含まれています。

検出を検疫するようにプロアクティブ脅威スキャンを設定できます。プロアクティブ脅威スキャンによって検疫された項目は、手動で復元できます。クライアントは検疫された項目を自動的に復元することもできます。

p.91 の「**TruScan** プロアクティブ脅威検出の管理」を参照してください。

## ネットワーク脅威防止について

Symantec Endpoint Protection クライアントには、悪質なもまたは過失によるものを問わず、コンピュータを侵入と悪用から保護するためのカスタマイズ可能なファイアウォールがあります。このファイアウォールでは、既知のポートスキャンとその他の一般的な攻撃が検出および識別されます。ファイアウォールは識別結果に基づいて、さまざまなネットワークサービス、アプリケーション、ポート、コンポーネントを許可または遮断します。危害を加えるおそれのあるネットワークトラフィックからクライアントコンピュータを保護するために、複数の種類の保護ファイアウォールルールとセキュリティ設定が含まれています。

ファイアウォールルールでは、ネットワーク接続を介してコンピュータへのアクセスを試行するインバウンドまたはアウトバウンドのアプリケーションを許可するか遮断するかが決定されます。ファイアウォールルールにより、インバウンドまたはアウトバウンドのアプリケーションと、特定 IP アドレスまたはポート間のトラフィックを体系的に許可または遮断できません。セキュリティ設定は、一般的な攻撃を検出および識別して、攻撃後に電子メールメッセージを送信し、カスタマイズ可能なメッセージを表示して、その他の関連セキュリティタスクを実行します。

p.98 の「[ファイアウォール保護の管理](#)」を参照してください。

ネットワーク脅威防止は侵入防止シグネチャも提供することで侵入攻撃と悪質なコンテンツを防止します。ファイアウォールはさまざまな基準に基づいてトラフィックを許可または遮断します。

p.117 の「[侵入防止保護の管理](#)」を参照してください。

## Symantec Network Access Control クライアントについて

Symantec Network Access Control クライアントは、社内ネットワークへの接続を許可する前に、コンピュータが適切に保護されているかどうか、および準拠しているかどうかを評価します。

クライアントは、管理者が設定したセキュリティポリシーにコンピュータが確実に準拠するようにします。セキュリティポリシーは、コンピュータがウイルス対策アプリケーションやファイアウォールアプリケーションなどの最新セキュリティソフトウェアを実行しているかどうかを検査します。コンピュータが必要なソフトウェアを実行していない場合、ユーザーまたはクライアントがソフトウェアを更新する必要があります。セキュリティソフトウェアが最新のものでない場合、コンピュータのネットワークへの接続が遮断されることがあります。クライアントは定期的に検査を実行して、コンピュータが継続的にセキュリティポリシーに準拠していることを確認します。

p.123 の「[Symantec Network Access Control の仕組み](#)」を参照してください。

# クライアントへの応答

この章では以下の項目について説明しています。

- [クライアントの介入について](#)
- [感染ファイルへの対応](#)
- [通知と警告について](#)

## クライアントの介入について

クライアントはバックグラウンドで動作して、コンピュータを悪質な活動から保護します。場合により、クライアントは、活動に関してユーザーに通知したり、ユーザーからのフィードバックを要求したりする必要があります。

次のような種類の警告または通知が表示されることがあります。

ウイルスまたはセキュリティ **Auto-Protect** またはスキャンによってウイルスまたはセキュリティリスクが検出された場合、[ **Symantec Endpoint Protection** 検知結果] ダイアログボックスが表示されます。感染についての詳細が含まれています。このダイアログボックスには、**Symantec Endpoint Protection** がリスクに対して実行した処理も表示されます。通常、ユーザーの側では、活動を確認してダイアログを閉じる以外の操作は必要ありません。ただし、必要に応じて処置を行うことができます。

p.16 の「[感染ファイルへの対応](#)」を参照してください。

アプリケーション関連通知 コンピュータ上のプログラムがネットワークへのアクセスを試みた場合、**Symantec Endpoint Protection** はユーザーに対して許可または拒否を求めることがあります。

p.18 の「[アプリケーション関連通知への応答](#)」を参照してください。

セキュリティ警告

**Symantec Endpoint Protection** は、プログラムを遮断したとき、またはコンピュータに対する攻撃を検出したときに、ユーザーに通知します。

p.21 の「[セキュリティ警告への応答](#)」を参照してください。

コンピュータで **Symantec Network Access Control** を有効にしている場合、ネットワークアクセス制御のメッセージが表示されることがあります。このメッセージは、セキュリティ設定が管理者の設定した基準と一致しない場合に表示されます。

p.21 の「[ネットワークアクセス制御通知への応答](#)」を参照してください。

## 感染ファイルへの対応

デフォルトでは、コンピュータ上で **Auto-Protect** が常に動作しています。管理外クライアントでは、コンピュータの起動時に、自動生成されたアクティブスキャンが実行されます。通常、管理下クライアントでは、完全スキャンが週に 1 回以上の割合で実行されるように管理者が設定します。**Auto-Protect** では、検出を行ったときに結果ダイアログボックスが表示されます。スキャンが実行されると、スキャンダイアログボックスにスキャン結果が表示されます。管理下クライアントでは、管理者がこのような種類の通知をオフにすることがあります。

このような種類の通知を受け取った場合、感染ファイルへの対応が必要になることがあります。

**Auto-Protect** とすべてのスキャンタイプのデフォルトオプションでは、検出時に感染ファイルからウイルスをクリーニングします。ファイルをクリーニングできない場合、クライアントはエラーをログに記録し、感染ファイルを検疫に移動します。ローカルの検疫は、感染ファイルと関連システム副作用のために確保されている専用の場所です。セキュリティリスクに関しては、クライアントは感染ファイルを検疫し、副作用を除去または修復します。ファイルを修復できない場合、クライアントは検出をログに記録します。

---

**メモ:** 検疫では、ウイルスは伝染できません。クライアントがファイルを検疫に移動させた場合、ユーザーはファイルにアクセスできません。

---

**Symantec Endpoint Protection** がウイルス感染したファイルを修復した場合、ユーザーの側でコンピュータ保護のためにそれ以上の処置を行う必要はありません。クライアントがセキュリティリスク感染ファイルを検疫して、除去および修復した場合、ユーザーの側ではそれ以上の処置は必要ありません。

ファイルへの対応は不要であっても、ファイルに対して追加的な処理を行うことはできます。たとえば、クリーニング済みファイルを元のファイルに置換する場合には、クリーニング済みファイルを削除できます。

通知を使うと、すぐにファイルに対応できます。ログ表示または検疫を使うと、あとでファイルに対応できます。

p.66の「スキャン結果の解釈」を参照してください。

p.139の「リスクログと脅威ログからのリスクと脅威の検疫」を参照してください。

p.78の「検疫ファイルの処理について」を参照してください。

### 感染ファイルに対応するには

- 1 次の処理のいずれかを実行します。
  - スキャン進捗状況ダイアログボックスで、スキャン完了時に使うファイルを選択します。
  - スキャン結果ダイアログボックスで、目的のファイルを選択します。
  - クライアントのサイドバーで、[ログの表示]をクリックし、次に、[ウイルス対策とスパイウェア対策]の隣にある[ログの表示]をクリックします。ログ表示で目的のファイルを選択します。
- 2 ファイルを右クリックし、次のいずれかのオプションを選択します。クライアントは選択された処理を実行できないことがあるため注意してください。
  - [適用した処理を元に戻す]:適用した処理を元に戻します。
  - [クリーニング](ウイルスのみ):ファイルからウイルスを除去します。
  - [永久削除]:感染ファイルとすべての副作用を削除します。セキュリティリスクについては、慎重にこの処理を行います。セキュリティリスクを削除すると、アプリケーションの機能が失われる原因になることがあります。
  - [検疫に移動]:感染ファイルを検疫に配置します。セキュリティリスクに関しては、クライアントは副作用の除去または修復も試みます。
  - [プロパティ]:ウイルスまたはセキュリティリスクに関する情報を表示します。

## ウイルスが原因の損傷について

感染の発生直後に Symantec Endpoint Protection が感染を発見した場合、感染ファイルはクライアントによるクリーニング後に十分に機能することがあります。ただし、Symantec Endpoint Protection は、ウイルスがすでに損傷した感染ファイルをクリーニングすることもあります。たとえば、Symantec Endpoint Protection はデータファイルを損傷するウイルスを発見することがあります。Symantec Endpoint Protection はウイルスを除去しますが、感染ファイル内部の損傷は修復できません。

## 通知と警告について

コンピュータ上に複数の種類の通知が表示されることがあります。通常、このような通知は状況について説明し、クライアントが問題をどのように解決しようとしているかを示します。

次のような種類の通知が表示されることがあります。

- アプリケーション関連通知  
p.18の「[アプリケーション関連通知への応答](#)」を参照してください。
- セキュリティ警告  
p.21の「[セキュリティ警告への応答](#)」を参照してください。

## アプリケーション関連通知への応答

アプリケーションまたはサービスの実行を許可するかをたずねる通知が表示されることがあります。

この種類の通知は、次のいずれかの理由で表示されます。

- アプリケーションがネットワーク接続へのアクセスを要求しています。
- ネットワーク接続にアクセスしたアプリケーションが更新されました。
- クライアントがユーザーの簡易切り替えを使ってユーザーを切り替えました。  
p.20の「[ユーザーの簡易切り替え通知](#)」を参照してください。
- 管理者がクライアントソフトウェアを更新しました。  
p.20の「[自動更新通知への応答](#)」を参照してください。

次のような種類のメッセージが表示されることがあります。このメッセージは、アプリケーションまたはサービスがコンピュータへのアクセスを試みていることを示しています。

Internet Explorer(IEXPLORE.EXE)が www.symantec.com に  
リモートポート 80(HTTP-World Wide Web)を使用して接続しようとしています。このプログラムにネットワーク

ネットワークへのアクセスを試みているアプリケーションに応答するには

- 1 メッセージボックスで[詳細]をクリックします。  
ファイル名、バージョン番号、パス名など、接続とアプリケーションに関して詳しい情報を表示できます。
- 2 次回アプリケーションがネットワーク接続へのアクセスを試みるときに備えてクライアントに選択項目を記憶させる場合、[返答を記憶して今後このアプリケーションについて確認しない]をクリックします。
- 3 次のいずれかのタスクを行います。
  - アプリケーションによるネットワーク接続へのアクセスを許可するには、[はい]をクリックします。

アプリケーションを認識でき、そのアプリケーションがネットワーク接続にアクセスすることを許可する場合にのみ、[はい]をクリックします。アプリケーションによるネットワーク接続へのアクセスを許可してよいかわからない場合、管理者に連絡します。

- アプリケーションによるネットワーク接続へのアクセスを遮断するには、[いいえ]をクリックします。

「表 2-1」では、アプリケーションの許可または遮断についてたずねる通知に対する応答方法を説明します。

表 2-1 アプリケーション許可通知

[返答を記憶して今後このアプリケーションについて通知しない]のチェックマークの有無	クリックするボタン	クライアントの処理
はい	はい	アプリケーションによるアクセスを許可し、2 回目以降にたずねることはない。
いいえ	はい	アプリケーションによるアクセスを許可し、毎回たずねる。
はい	いいえ	アプリケーションによるアクセスを遮断し、2 回目以降にたずねることはない。
いいえ	いいえ	アプリケーションによるアクセスを遮断し、毎回たずねる。

[実行中のアプリケーション]フィールドまたは[アプリケーション]リストでアプリケーションの処理を変更することもできます。

p.114 の「[アプリケーション固有の設定](#)」を参照してください。

## アプリケーション変更通知

アプリケーションが変更されたことを示すメッセージが表示されることがあります。次のメッセージは例です。

Telnet は前回開いてから変更されました。こうなったのはユーザーが更新したか新しい DLL がロードされたなどの理由による可能性があります。  
詳しくは詳細を参照してください。ネットワークアクセスを許可しますか？

このメッセージに記載されているアプリケーションがネットワーク接続へのアクセスを試みています。クライアントはアプリケーションの名前を認識できますが、前回対処した時点以降にアプリケーションに何らかの変更が加えられています。もっとも考えられるのは製品をアップグレードした場合です。製品のバージョンが新しくなるたびにそれ以前のバージョン

ンとは異なるファイルフィンガープリントファイルを使います。クライアントはファイルフィンガープリントファイルが変更されたことを検出します。

## ユーザーの簡易切り替え通知

Windows Vista/XP を使っている場合、次の通知のいずれかが表示されることがあります。

```
"Symantec Endpoint Protection is unable to show the user interface.  
If you are using Windows XP Fast User Switching, make sure all other users are  
logged off of Windows and try logging off of Windows and then log back on.  
If you are using Terminal Services, the user interface is not supported."
```

または

```
"Symantec Endpoint Protection was not running but will be started.  
However, the Symantec Endpoint Protection is unable to show the user interface.  
If you are using Windows XP Fast User Switching, make sure all other users are  
logged off of Windows and try logging off of Windows and then log back on.  
If you are using Terminal Services, the user interface is not supported."
```

ユーザーの簡易切り替えは、Windows の機能の 1 つで、コンピュータからログオフしないでユーザーをすばやく切り替えることができる機能です。複数のユーザーが 1 台のコンピュータを同時に共有でき、実行中のアプリケーションを閉じることなく互いに切り替えることができます。ユーザーの簡易切り替えを使ってユーザーを切り替えると、このようなウィンドウのいずれかが表示されます。

ユーザーの簡易切り替えメッセージに応答するには、ダイアログボックス内の指示に従います。

## 自動更新通知への応答

クライアントソフトウェアが自動更新される場合、次の通知が表示されることがあります。

```
Symantec Endpoint Protection が Symantec Endpoint Protection Manager から  
ソフトウェアの新しいバージョンが入手可能であること検出しました。  
今すぐにダウンロードしますか？
```

自動更新通知に応答するには

1 次の処理のいずれかを実行します。

- ソフトウェアをすぐにダウンロードするには、[今すぐにダウンロード]をクリックします。

- 指定時間の経過後に通知するには、[後で通知する]をクリックします。
- 2 更新されたソフトウェアのインストール処理が始まった後にメッセージが表示された場合、[OK]をクリックします。

## セキュリティ警告への応答

セキュリティ警告では、通知領域アイコンの上に通知が表示されます。[OK]をクリックして、メッセージを読んだことを知らせる必要があります。この通知は、次のいずれかの理由で表示されます。

アプリケーションメッセージの遮断	コンピュータから起動したアプリケーションが、管理者によって設定されているルールに従って遮断されました。たとえば、次のメッセージが表示されることがあります。  <b>トラフィックをこのアプリケーションが遮断しました: (アプリケーション名)</b>  このような通知は、ユーザーから「信頼できない」として指定されたトラフィックをクライアントが遮断したことを示します。クライアントがすべてのトラフィックを遮断するように設定されている場合、このような通知は頻繁に表示されます。クライアントがすべてのトラフィックを許可するように設定されている場合、このような通知は表示されません。
侵入	コンピュータに対して攻撃が開始されたため、警告は状況について通知するか、または攻撃への対処方法に関する指示を与えます。たとえば、次のメッセージが表示されることがあります。  IP アドレス 192.168.0.3 から届くトラフィックは 10/10/2006 15:37:58 から 10/10/2006 15:47:58 まで遮断されます。ポートスキャン攻撃をログに記録しました。  管理者がクライアントコンピュータの侵入防止通知を無効にしていることがあります。  クライアントが検出する攻撃の種類を確認できるようにするには、侵入防止通知の表示を有効にしてください。  p.119 の「 <a href="#">侵入防止の通知の設定</a> 」を参照してください。

## ネットワークアクセス制御通知への応答

Symantec Network Access Control クライアントは、セキュリティポリシーに従っていない場合、ネットワークにアクセスできないことがあります。この場合、ホットインテグリティチェックに失敗したために **Symantec Enforcer** がトラフィックを遮断したということを伝えるメッセージが表示されることがあります。ネットワーク管理者が、考えられる対処法をこのメッセージに追加していることがあります。メッセージボックスを閉じた後に、クライアントを開いて、ネットワークアクセスを復元する推奨手順が表示されるか確認します。

ネットワークアクセス制御通知に応答するには

- 1 メッセージボックスに表示される推奨手順に従います。
- 2 メッセージボックスで[OK]をクリックします。



# クライアントの管理

この章では以下の項目について説明しています。

- 集中管理下クライアントと自己管理クライアントについて
- 自己管理クライアントの集中管理下クライアントへの変換
- コンピュータの保護の更新
- セキュリティポリシーについて
- ポリシーファイルを手動で更新
- ポリシーが更新されていることの検証
- コンピュータをただちにスキャンする
- スキャンの一時停止と遅延
- 保護技術の有効化と無効化
- 改変対策について
- 改変対策の有効化、無効化、設定
- コンピュータのセキュリティテスト
- 場所について
- 場所の変更
- 通知領域アイコンについて
- 通知領域アイコンの非表示と表示
- 管理者によるコンピュータ再起動の防止について

## 集中管理下クライアントと自己管理クライアントについて

管理者は集中管理下クライアント(管理者が管理するインストール)または自己管理クライアント(スタンドアロンインストール)としてクライアントをインストールできます。

表 3-1 集中管理下クライアントと自己管理クライアントの違い

クライアントの種類	説明
集中管理下クライアント	<p>集中管理下クライアントはネットワークの管理サーバーと通信します。管理者は保護とデフォルトのオプションを設定し、管理サーバーはクライアントに設定をダウンロードします。管理者が保護の変更を行う場合、変更はクライアントにはほぼすぐにダウンロードされます。</p> <p>管理者はクライアントと相互作用するレベルを次のように変更できます。</p> <ul style="list-style-type: none"><li>■ 管理者がクライアントを完全に管理します。 ユーザーはクライアントを設定するように要求されません。すべての設定はロックされるか利用不能ですが、クライアントがコンピュータで実行することについての情報を表示できます。</li><li>■ 管理者がクライアントを管理しますが、ユーザーは一部のクライアント設定を変更して一部のタスクを実行できます。たとえば、ユーザーは自身自身でスキャンを実行してクライアントの更新と保護の更新を手動で取り込みます。 クライアント設定の可用性と設定されている値は、定期的に変化することがあります。たとえば、管理者がクライアント保護を制御するポリシーを更新すると、設定が変化することがあります。</li><li>■ 管理者がクライアントを管理しますが、ユーザーはすべてのクライアント設定を変更してすべての保護タスクを実行できます。</li></ul>
自己管理クライアント	<p>自己管理クライアントは管理サーバーと通信しないため管理者はクライアントを管理しません。</p> <p>自己管理クライアントは次のいずれかの種類になります。</p> <ul style="list-style-type: none"><li>■ ホームコンピュータまたはノートパソコンなど、ネットワークに接続していないスタンドアロンコンピュータ(コンピュータには、デフォルトのオプション設定または管理者が事前設定したオプション設定を使う Symantec Endpoint Protection がインストールされている必要がある)。</li><li>■ 社内ネットワークに接続するリモートコンピュータ(接続前にセキュリティの必要条件を満たす必要がある)</li></ul> <p>最初にインストールされるときクライアントにはデフォルト設定が適用されません。クライアントがインストールされた後、すべてのクライアント設定を変更してすべての保護タスクを実行できます。</p>

p.25の「[自己管理クライアントの集中管理下クライアントへの変換](#)」を参照してください。

表 3-2 に、集中管理下クライアントと自己管理クライアント間のユーザーインターフェースの相違を示します。

表 3-2 集中管理下クライアントと自己管理クライアントの機能領域ごとの違い

機能領域	集中管理下クライアント	自己管理クライアント
ウイルス対策とスパイウェア対策	クライアントはロックされた南京錠オプションを表示してユーザーが設定できないオプションはグレーで表示されます。	クライアントはロックされた南京錠またはロック解除された南京錠を表示しません。
クライアント管理とネットワーク脅威防止の設定	管理者が制御する設定は表示されません。	すべての設定は表示されます。

p.15 の「[クライアントの介入について](#)」を参照してください。

## 自己管理クライアントの集中管理下クライアントへの変換

管理外クライアントとしてインストールされているクライアントを管理下クライアントに変換することができます。管理下クライアントは管理サーバーと通信してコンテンツ定義の更新と設定情報を受信します。管理外クライアントは管理サーバーと通信しません。

p.24 の「[集中管理下クライアントと自己管理クライアントについて](#)」を参照してください。

管理外クライアントを管理下クライアントに変換するには、通信の設定を含む `sylink.xml` ファイルをインポートします。このファイルは、管理者がユーザーに送信するか、ユーザーがアクセスできる場所に保存する必要があります。このファイルのデフォルトの名前は <グループ名>`_sylink.xml` です。

この通信ファイルをインポートすると、デスクトップの右下に通知領域アイコンが表示されます。

p.39 の「[通知領域アイコンについて](#)」を参照してください。

管理外クライアントを管理下クライアントに変換するには

- 1 クライアントで、[ヘルプとサポート]をクリックし、[トラブルシューティング]をクリックします。
- 2 [管理]ダイアログボックスの[通信の設定]で、[インポート]をクリックします。
- 3 [通信設定のインポート]ダイアログボックスで、<グループ名>`_sylink.xml` ファイルを選択して[開く]をクリックします。
- 4 [閉じる]をクリックします。

## コンピュータの保護の更新

シマンテック製品は最新情報に基づいて、新しく発見された脅威からコンピュータを保護します。シマンテックでは、**LiveUpdate** を使ってこの情報をユーザーに提供します。**LiveUpdate** は、インターネット接続を使って、コンピュータ用のプログラムと保護の更新を入手します。

保護の更新とは、最新の脅威防止技術を使ってシマンテック製品を最新の状態に保つファイルです。**LiveUpdate** はシマンテック社のインターネットサイトから新しい定義ファイルを取り込んで、古い定義ファイルを置換します。受信する保護の更新は、コンピュータにインストールされている製品に応じて異なります。

保護の更新は次のファイルを含むことができます。

- ウイルス対策とスパイウェア対策のウイルス定義ファイル  
p.60の「[ウイルススキャンとスパイウェアスキャンの動作](#)」を参照してください。
- プロアクティブ脅威防止のヒューリスティックシグネチャと商用アプリケーションリスト
- ネットワーク脅威防止のIPS定義ファイル  
p.98の「[ネットワーク脅威防止の管理について](#)」を参照してください。

製品の更新とは、インストール済みクライアントの改良を意味します。一般的に、製品の更新は、オペレーティングシステムまたはハードウェアとの互換性の向上、性能問題の調整、製品エラーの修正を目的として作成されます。製品の更新は必要に応じてリリースされます。クライアントは**LiveUpdate** サーバーから製品の更新を直接受信します。集中管理下クライアントは会社の管理サーバーから製品の更新を自動的に受信することもできます。

表 3-3 コンピュータの内容を更新する方法

タスク	説明
スケジュールに従って内容を更新	デフォルトでは、 <b>LiveUpdate</b> は自動で定期的に行われます。  自己管理クライアントで、 <b>LiveUpdate</b> スケジュールを無効にしたり変更したりすることができます。  p.27の「 <a href="#">スケジュールに従って内容を更新</a> 」を参照してください。
内容をすぐに更新	セキュリティ設定に基づいて、 <b>LiveUpdate</b> をすぐに実行することもできます。  p.27の「 <a href="#">内容の即時更新</a> 」を参照してください。

**メモ:** **LiveUpdate** の通信では、HTTP はサポートされていますが HTTPS はサポートされていません。

## 内容の即時更新

LiveUpdate の使用によって定義ファイルをすぐに更新できます。次の理由のために LiveUpdate を手動で実行してください。

- クライアントが最近インストールされた
- 前回のスキャンから長い時間が経過している
- ウイルスがある疑いがある

p.27 の「[スケジュールに従って内容を更新](#)」を参照してください。

p.26 の「[コンピュータの保護の更新](#)」を参照してください。

保護をすぐに更新するには

- ◆ クライアントのサイドバーで、[LiveUpdate]をクリックします。

LiveUpdate はシマンテック社のサーバーに接続して利用可能な更新がないかチェックし、更新がある場合には、自動的に更新をダウンロードしてインストールします。

## スケジュールに従って内容を更新

ユーザーは LiveUpdate を定期的に自動で実行するためのスケジュールを作成できます。コンピュータを使わない期間に LiveUpdate を実行するようにスケジュール設定すると便利です。

p.27 の「[内容の即時更新](#)」を参照してください。

---

**メモ:** 管理者が有効にしている場合のみスケジュールに従って実行するように LiveUpdate を設定できます。

---

スケジュールに従って保護を更新するには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [クライアント管理]の隣にある[オプションの設定]をクリックします。
- 3 [クライアント管理の設定]ダイアログボックスで[定時更新]をクリックします。
- 4 [定時更新]タブで[自動更新を有効にする]にチェックマークを付けます。
- 5 [頻度]グループボックスで、更新を日単位、週単位、月単位のいずれかで実行するか選択します。
- 6 [タイミング]グループボックスで、更新を実行する曜日または週と時刻を選択します。  
[タイミング]グループボックスの設定は[頻度]グループボックスの設定によって決まります。

- 7 [試し続ける期間]にチェックマークを付けてから、クライアントが **LiveUpdate** の再実行を試みる時間間隔を指定します。
- 8 [開始日時を時間単位の±でランダム化する]にチェックマークを付けてから、時間数または日数を指定します。  
このオプションは更新を開始する予定時刻の前後の時間の範囲を設定します。
- 9 [OK]をクリックします。

## セキュリティポリシーについて

セキュリティポリシーとは、管理下クライアントの管理者が設定してクライアントに配備するセキュリティ設定を1つにまとめたものです。クライアントの設定(ユーザーによる表示およびアクセスが可能なオプションなど)はセキュリティポリシーによって決定されます。

p.24の「[集中管理下クライアントと自己管理クライアントについて](#)」を参照してください。

管理下クライアントは管理サーバーに接続されており、最新のセキュリティポリシーを自動的に受信します。ネットワークアクセスが困難な場合、管理者からポリシーファイルを手動で更新するように指示されることがあります。

p.28の「[ポリシーファイルを手動で更新](#)」を参照してください。

## ポリシーファイルを手動で更新

クライアントの保護を制御する設定はコンピュータ上のポリシーファイルに格納されます。ポリシーファイルはウイルス対策とスパイウェア対策、ネットワーク脅威防止、プロアクティブ脅威防止、Symantec Network Access Control の設定を更新します。通常、このポリシーファイルは自動的に更新されます。ただし、ポリシーファイルが更新されるまで待たなければポリシーファイルを手動で更新することもできます。

---

**メモ:** システムログを表示するとこの操作でポリシーが正常に更新されたことを確認できます。

---

p.28の「[セキュリティポリシーについて](#)」を参照してください。

p.29の「[ポリシーが更新されていることの検証](#)」を参照してください。

ポリシーファイルを手動で更新するには

- 1 Windows 通知領域で、クライアントアイコンを右クリックします。
- 2 ポップアップメニューで、[ポリシーの更新]を選択します。

## ポリシーが更新されていることの検証

クライアントのポリシーを更新するとき、クライアントがポリシーを受信したかどうかを調べることができます。

p.28の「[セキュリティポリシーについて](#)」を参照してください。

p.28の「[ポリシーファイルを手動で更新](#)」を参照してください。

クライアントコンピュータが更新済みポリシーを入手したことを検証するには

- 1 クライアントコンピュータの Symantec Endpoint Protection メインウィンドウで、[ログの表示]をクリックします。
- 2 [クライアント管理]の横にある[ログの表示]をクリックし、[システムログ]をクリックします。

シリアル番号を含んでいるポリシー更新のエントリを参照します。

## コンピュータをただちにスキャンする

ウイルスとセキュリティリスクはいつでも手動でスキャンできます。最近クライアントをインストールした場合、または最近ウイルスを受信したと考えられる場合にはコンピュータをただちにスキャンしてください。

単一のファイル、フロッピーディスク、コンピュータ全体などの任意のスキャン対象を選択します。オンデマンドスキャンには、アクティブスキャンと完全スキャンがあります。オンデマンドで実行するカスタムスキャンを作成することもできます。

p.65の「[オンデマンドまたはコンピュータの起動時に実行されるスキャンのスケジュール](#)」を参照してください。

各ダイアログボックスのオプションについて詳しくは[ヘルプ]をクリックしてください。

コンピュータをただちにスキャンするには

- ◆ 次の処理のいずれかを実行します。
  - クライアントの[状態]ページの[ウイルス対策とスパイウェア対策]の隣で、[オプション]、[アクティブスキャンの実行]の順に選択します。
  - クライアントのサイドバーで、[脅威のスキャン]をクリックします。  
次の処理のいずれかを実行します。
    - [アクティブスキャンの実行]をクリックします。
    - [完全スキャンの実行]をクリックします。
    - スキャンリストで任意のスキャンを右クリックしてから、[今すぐスキャン]をクリックします。

スキャンが開始されます。進行状況ウィンドウで、スキャンの進行状況と結果が表示されます。

スキャンを一時停止するか中止することもできます。

p.30の「スキャンの一時停止と遅延」を参照してください。

#### Windows からコンピュータをスキャンするには

- ◆ マイコンピュータウィンドウまたは Windows エクスプローラウィンドウでファイル、フォルダ、またはドライブを右クリックして、[ウイルススキャン]をクリックします。

この機能は、64 ビットオペレーティングシステムではサポートされていません。

## スキャンの一時停止と遅延

一時停止機能を使うと、スキャン中の任意の時点でスキャンを停止して、あとから再開できます。ユーザーは自分が開始したスキャンを一時停止できます。

ユーザーが管理者によるスキャンを一時停止できるかどうかは管理者が決めます。管理者が一時停止機能を無効にすると[スキャンの一時停止]オプションは利用できません。管理者が休止機能を有効にした場合、ユーザーは設定された時間、管理者による定時スキャンを遅らせることができます。

スキャンを再開すると、スキャンを停止した場所から開始されます。

---

**メモ:** クライアントが圧縮ファイルをスキャン中に一時停止した場合には、クライアントが一時的停止の要求に応答するまでに数分かかることがあります。

---

#### ユーザーが開始したスキャンを一時停止するには

- 1 スキャンの実行中に、スキャンのダイアログボックスで[スキャンの一時停止]をクリックします。

スキャンはその場で停止し、ユーザーがスキャンを再び開始するまでスキャンのダイアログボックスは開いたままになります。

- 2 スキャンを再開するにはスキャンのダイアログボックスで[スキャンの再開]をクリックします。

#### 管理者が開始したスキャンを一時停止または遅らせるには

- 1 管理者が開始したスキャンの実行中に、スキャンのダイアログボックスで[スキャンの一時停止]をクリックします。

- 2 [定時スキャン一時停止]ダイアログボックスで、次のいずれかの操作をします。

- スキャンを一時停止するには、[一時停止]をクリックします。
- スキャンを遅らせるには、[1 時間休止]または[3 時間休止]をクリックします。

管理者はユーザーに許可するスキャンの遅延時間を指定します。指定された時間が経過すると、スキャンは最初から始まります。管理者はこの機能が無効になるまでにユーザーが定時スキャンを遅らせることのできる回数を指定します。

- 一時停止しないでスキャンを続行するには、[続行]をクリックします。

## 保護技術の有効化と無効化

一般に、コンピュータの保護技術は常に有効にしておきます。

クライアントコンピュータに問題がある場合は、一時的にすべての保護技術または個別の保護技術を無効にすることができます。たとえば、動作しないまたは正しく動作しないアプリケーションの問題がある場合は、ネットワーク脅威防止を無効にすることができます。

すべての保護技術を無効にした後も問題がある場合は、問題がクライアントではないことを確認できます。

表 3-4 に各保護技術を無効にする理由を記述します。

表 3-4 保護技術を無効にする目的

保護技術	保護技術を無効にする目的
ウイルス対策とスパイウェア対策	<p>この保護を無効にする場合は、<b>Auto-Protect</b> のみを無効にします。ユーザーまたは管理者が設定している場合は定時スキャンまたは起動時スキャンが動作します。</p> <p>ユーザーまたは管理者は次の理由で <b>Auto-Protect</b> の有効と無効を切り替える場合があります。</p> <ul style="list-style-type: none"> <li>■ <b>Auto-Protect</b> はドキュメントを開くのを遮断することがあります。たとえば、マクロがある <b>Microsoft Word</b> を開く場合に、<b>Auto-Protect</b> が開くことを許可しないことがあります。ドキュメントが安全であることがわかっている場合には、<b>Auto-Protect</b> を無効にできます。</li> <li>■ ウイルスの影響によるものでないことがわかっているにもかかわらずウイルスのような活動が確認された場合には、<b>Auto-Protect</b> が警告することがあります。たとえば、新しいコンピュータアプリケーションのインストール時に警告が表示されることがあります。インストールするアプリケーションが複数あり、このような警告の表示を避けたい場合、<b>Auto-Protect</b> を一時的に無効にできます。</li> <li>■ <b>Auto-Protect</b> は <b>Windows</b> のドライバの交換と干渉することがあります。</li> <li>■ <b>Auto-Protect</b> はクライアントコンピュータの速度を低下させることがあります。</li> </ul> <p>p.33 の「<b>Auto-Protect</b> の有効化または無効化」を参照してください。</p>

保護技術	保護技術を無効にする目的
プロアクティブ脅威防止	<p>次の理由でプロアクティブ脅威防止を無効にすることがあります。</p> <ul style="list-style-type: none"> <li>■ 脅威ではないことがわかっている脅威について表示される警告が多すぎます。</li> <li>■ プロアクティブ脅威防止はクライアントコンピュータの速度を低下させることがあります。</li> </ul> <p>p.35の「<a href="#">プロアクティブ脅威防止の有効化と無効化</a>」を参照してください。</p>
ネットワーク脅威防止	<p>次の理由でネットワーク脅威防止を無効にすることがあります。</p> <ul style="list-style-type: none"> <li>■ ファイアウォールが遮断することがあるアプリケーションをインストールします。</li> <li>■ ファイアウォールルールまたはファイアウォールの設定が管理者の間違いによりアプリケーションを遮断します。</li> <li>■ ファイアウォールまたは侵入防止システムによりネットワーク接続に関する問題が発生します。</li> <li>■ ファイアウォールはクライアントコンピュータの速度を低下させることがあります。</li> </ul> <p>p.34の「<a href="#">ネットワーク脅威防止の有効化または無効化</a>」を参照してください。</p> <p>p.118の「<a href="#">侵入防止の設定の有効化または無効化</a>」を参照してください。</p>

**警告:**トラブルシューティングの操作が完了したら、コンピュータの保護を継続できるように、必ずすべての保護を有効にしてください。

いずれかの保護技術がアプリケーションに問題を起す場合は、永続的に保護を無効にするよりも例外を作成する方が適切です。

p.76の「[スキャン対象からの項目の除外について](#)」を参照してください。

いずれかの保護が無効になるとき:

- [状態]ページの先頭のステータスバーは赤くなります。
  - クライアントのアイコンに一般的な禁止記号(赤の円に斜線)が付きます。クライアントアイコンは、Windows デスクトップの右下のタスクバーに盾の形で表示されます。設定によってアイコンは表示されません。
- p.39の「[通知領域アイコンについて](#)」を参照してください。

集中管理下クライアントでは、管理者は保護をいつでも有効にできます。

[状態]ページから保護技術を有効にするには

- ◆ クライアントの[状態]ページの先頭で、[修復]または[すべてを修復]をクリックします。

タスクバーから保護技術の有効と無効を切り替えるには

- ◆ Windows デスクトップの通知領域でクライアントアイコンを右クリックして、次のいずれかの操作をします。
  - [Symantec Endpoint Protection を有効にする]をクリックします。
  - [Symantec Endpoint Protection を無効にする]をクリックします。

p.36の「[改変対策の有効化、無効化、設定](#)」を参照してください。

## Auto-Protect の有効化または無効化

ファイルとプロセス、インターネット電子メール、電子メールのグループウェアアプリケーションに対してファイルシステム **Auto-Protect** を有効または無効にできます。いずれかの **Auto-Protect** が無効になっている場合、ウイルス対策とスパイウェア対策の状態が[状態]ページに赤色で表示されます。

アイコンを右クリックすると、[Symantec Endpoint Protection を有効にする]が表示されます。

p.31の「[保護技術の有効化と無効化](#)」を参照してください。

---

**メモ:** 集中管理下クライアントでは、管理者は無効にできないように **Auto-Protect** をロックすることがあります。また、ユーザーが **Auto-Protect** を一時的に無効にできても、指定の時間が経過した時点で **Auto-Protect** が再び自動的に有効になるように管理者が指定することもあります。

---

デフォルトのオプション設定を変更しなければ、コンピュータの起動時に **Auto-Protect** がロードされて、コンピュータをウイルスとセキュリティリスクから保護します。**Auto-Protect** はプログラムの実行時にプログラムにウイルスとセキュリティリスクがないか調べます。コンピュータを監視して、ウイルスまたはセキュリティリスクの存在を示す可能性のある活動がないかも調べます。ウイルス、ウイルスらしい活動(ウイルスの影響と考えられるイベント)、セキュリティリスクが検出されると、**Auto-Protect** が警告します。

ファイルシステム **Auto-Protect** を有効または無効にするには

- ◆ クライアントで[状態]ページの[ウイルス対策とスパイウェア対策]の隣から、次のいずれかの操作をします。

電子メール用 **Auto-Protect** を有効または無効にするには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [ウイルス対策とスパイウェア対策]の隣にある[オプションの設定]をクリックします。

- 3 次の処理のいずれかを実行します。
  - [インターネット電子メール **Auto-Protect**]タブで、[インターネット電子メール **Auto-Protect** を有効にする]にチェックマークを付けるか、チェックマークをはずします。
  - [**Outlook Auto-Protect**]タブで、[Microsoft Outlook **Auto-Protect** を有効にする]にチェックマークを付けるか、チェックマークをはずします。
  - [**Notes Auto-Protect**]タブで、[Lotus Notes **Auto-Protect** を有効にする]にチェックマークを付けるか、チェックマークをはずします。
- 4 [OK]をクリックします。

## ネットワーク脅威防止の有効化または無効化

アプリケーションを開くことができない場合はネットワーク脅威防止を無効にする必要があります。ネットワーク脅威防止が問題の原因であることがわからない場合は、すべての保護技術を無効にする必要があることがあります。

p.31の「**保護技術の有効化と無効化**」を参照してください。

保護を無効に設定できる場合、いつでも有効に戻すことができます。管理者はユーザーの設定に優先していつでも保護を有効または無効にすることができます。

ユーザーが保護を無効にできるタイミングと期間について、管理者が次のような制限を設定していることがあります。

- クライアントが許可するトラフィック(すべてのトラフィックまたはアウトバウンドトラフィックのみのいずれか)
- 保護が無効になる期間
- クライアントの再起動までに保護を無効にできる回数

p.98の「**ファイアウォール保護の管理**」を参照してください。

p.120の「**攻撃側コンピュータの遮断と遮断解除**」を参照してください。

ネットワーク脅威防止を有効または無効にするには

- ◆ クライアントで[状態]ページの[ネットワーク脅威防止]の隣から、次のいずれかの操作をします。
  - [オプション]、[ネットワーク脅威防止を有効にする]の順に選択します。
  - [オプション]、[ネットワーク脅威防止を無効にする]の順に選択します。

## プロアクティブ脅威防止の有効化と無効化

スキャンが表示する警告または誤認が多すぎる場合はプロアクティブ脅威防止を無効にする必要があることがあります。誤認はスキャンが脅威ではないアプリケーションまたはプロセスを脅威として検出するときに発生します。

[トロイの木馬とワームをスキャンする]と[キーロガーをスキャンする]の両方の設定が有効な場合は、プロアクティブ脅威防止が有効になります。一方の設定が無効になっている場合、クライアントはプロアクティブ脅威防止の状態を無効として表示します。

集中管理下クライアントでは、管理者は無効にできないようにプロアクティブ脅威防止をロックすることがあります。プロアクティブ脅威防止は Windows XP x64 Edition または Windows Server 2000、2003、2008 を実行するクライアントコンピュータでは自動的に無効になります。

p.87 の「[TruScan プロアクティブ脅威スキャンについて](#)」を参照してください。

プロアクティブ脅威防止を有効または無効にするには

- ◆ クライアントで[状態]ページの[プロアクティブ脅威防止]の隣から、次のいずれかの操作をします。
  - [オプション]、[プロアクティブ脅威防止を有効にする]の順に選択します。
  - [オプション]、[プロアクティブ脅威防止を無効にする]の順に選択します。

## 改変対策について

改変対策では、シマンテック製アプリケーションに対してリアルタイム保護を提供します。改変対策は、ワーム、トロイの木馬、ウイルス、セキュリティリスクなどの悪質なソフトウェアによる攻撃を阻止します。

次の処理を実行するように改変対策を設定できます。

- 改変を遮断してイベントをログに記録する
- 改変イベントをログに記録するが、改変イベントに干渉しない

管理者がデフォルト設定を変更していないかぎり、改変対策は管理下クライアントと管理外クライアントの両方に対して有効になっています。改変対策が改変の試みを検出すると、デフォルトの処理として、改変対策ログにイベントが記録されます。改変の試みが検出されたときにコンピュータ上に通知を表示するように改変対策を設定できます。メッセージをカスタマイズすることもできます。ユーザーが機能を有効にしているかぎり、改変対策が改変の試みをユーザーに通知することはありません。

管理外クライアントを使う場合、改変対策設定を変更できます。管理下クライアントを使う場合には、管理者が許可すれば、改変対策設定を変更できます。

最初に **Symantec Endpoint Protection** を使う場合には、デフォルトのまま[イベントをログに記録のみする]に設定して、週に 1 回の割合でログを監視するのが最適な方法で

す。誤認が起きないことに満足すれば変更対策を[遮断してイベントをログに記録する]に設定します。

---

**メモ:** 迷惑なアドウェアやスパイウェアの検出機能とそれらのソフトウェアからの保護機能を備えた他社製のセキュリティリスクスキャナを使っている場合、通常、そのスキャナはシマンテック製品の処理に影響を及ぼします。変更対策を有効にした状態で他社製のセキュリティリスクスキャナを実行すると、変更対策によって大量の通知とログエントリが生成されます。常に変更対策を有効にし、大量のイベントが生成された場合には、ログフィルタリングを使うことをお勧めします。

---

p.36の「[変更対策の有効化、無効化、設定](#)」を参照してください。

## 変更対策の有効化、無効化、設定

変更対策は、ユーザーが有効または無効にすることができます。変更対策を有効にすると、シマンテック製ソフトウェアの変更の試みが検出されたときに実行される処理を選択できます。変更対策が変更の試みを知らせるメッセージを表示するように設定することもできます。メッセージをカスタマイズする場合、変更対策が適切な情報を埋め込む変数として事前定義済み変数を使うことができます。

---

**メモ:** 管理者がコンピュータを管理しており、これらのオプションに南京錠のアイコンが表示される場合には、管理者によってロックされているためこれらのオプションを変更することはできません。

---

事前定義済み変数については、[変更対策]タブの[ヘルプ]をクリックしてください。

p.35の「[変更対策について](#)」を参照してください。

**変更対策を有効または無効にするには**

- 1 メインウィンドウのサイドバーで、[設定の変更]をクリックします。
- 2 [クライアント管理]の隣にある[オプションの設定]をクリックします。
- 3 [変更対策]タブで、[シマンテック製セキュリティソフトウェアを改変または終了から保護する]をチェックするかチェックマークをはずします。
- 4 [OK]をクリックします。

**変更対策を設定するには**

- 1 メインウィンドウのサイドバーで、[設定の変更]をクリックします。
- 2 [クライアント管理]の隣にある[オプションの設定]をクリックします。

- 3 [改変対策]タブの[アプリケーションがシマンテック製セキュリティソフトウェアを改変または終了しようとした場合に適用する処理]リストボックスで、[遮断してイベントをログ記録する]または[イベントをログに記録のみする]をクリックします。
- 4 改変対策が疑わしい動作を検出したときに通知するように設定する場合は、[改変の検出時に通知メッセージを表示する]にチェックマークを付けます。  
このような通知メッセージを有効にすると、シマンテック製品の処理と Windows の処理に関して通知を受け取ることがあります。
- 5 表示されるメッセージをカスタマイズするには、メッセージフィールドのテキストを更新します。
- 6 [OK]をクリックします。

## コンピュータのセキュリティテスト

コンピュータをスキャンすることにより、外部の脅威とウイルスに対するコンピュータの有効性をテストできます。このスキャンは、コンピュータが侵入者から保護されていることを確認するための重要なステップです。スキャンの結果は、コンピュータを攻撃から保護するためにクライアントでさまざまなオプションを設定するときに役立ちます。

### コンピュータのセキュリティテスト

- 1 クライアントのサイドバーで、[状態]をクリックします。
- 2 [ネットワーク脅威防止]の隣で、[オプション]、[ネットワーク活動の表示]の順に選択します。
- 3 [ツール]、[ネットワークセキュリティのテスト]の順に選択します。
- 4 Symantec Security Check の Web サイトで、次のいずれかの操作をします。
  - オンライン脅威がないかチェックするには、[セキュリティスキャン]をクリックします。
  - ウイルスがないかチェックするには、[ウイルス検出]をクリックします。
- 5 [エンドユーザー使用許諾契約]ダイアログボックスで、[同意する]、[次へ]の順に選択します。  
ステップ 4 で[ウイルス検出]をクリックした場合、[同意する]、[次へ]の順に選択します。  
スキャンを止めるには、[中止]をクリックします。
- 6 スキャンが終了したら、ダイアログボックスを閉じます。

## 場所について

場所は、ネットワーク環境に基づいたセキュリティポリシーを参照します。たとえば、ノートパソコンを使用して自宅から職場のネットワークに接続する場合、管理者は「ホーム」という名前の場所を設定できます。職場でノートパソコンを使用する場合は、「オフィス」という名前の場所を使うことができます。その他の場所としては、VPN、支店、ホテルなどが考えられます。

セキュリティのニーズと使用状況のニーズはネットワーク環境ごとに異なることがあるため、クライアントはこれらの場所を切り替えます。たとえば、ノートパソコンからオフィスネットワークに接続するときには、管理者が設定した一連の制限ポリシーがクライアントで使われる場合があります。しかし、ホームネットワークに接続するときは、さらに多くの設定オプションにアクセスできる一連のポリシーがクライアントで使われる可能性があります。管理者は、クライアントがそのような相違を自動的に調整するようにクライアントを計画し、設定します。

---

**メモ:** 管理下環境では、管理者から必要なアクセスを与えられている場合のみ場所を変更できます。

---

p.38 の「[場所の変更](#)」を参照してください。

## 場所の変更

ユーザーは必要に応じて場所を変更できます。たとえば、同僚がコンピュータ上のファイルへアクセスできるようにする場所に切り替える必要がある場合があります。利用可能な場所のリストは、セキュリティポリシーとコンピュータのアクティブなネットワークに基づいて生成されます。

p.38 の「[場所について](#)」を参照してください。

---

**メモ:** 利用可能なセキュリティポリシーに基づいて、複数の場所にアクセスできる場合とできない場合があります。場所をクリックしたときに、その場所に切り替えることができないことがあります。この場合、ネットワーク設定がその場所に適していないことを意味しています。たとえば、「オフィス」と呼ばれる場所は、職場のローカルエリアネットワーク(LAN)が検出されたときのみ利用できます。ユーザーがそのネットワーク上にいない場合、その場所に切り替えることはできません。

---

### 場所を変更するには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [設定の変更]ページで[クライアント管理]の隣にある[オプションの設定]をクリックします。

- 3 [全般]タブの[場所のオプション]で、変更先の場所を選択します。
- 4 [OK]をクリックします。

## 通知領域アイコンについて

クライアントでは、通知領域アイコンによって、クライアントがオンラインになっているかオフラインになっているか、およびクライアントコンピュータが十分に保護されているかどうかが表示されます。このアイコンを右クリックすると、使う頻度が高いコマンドが表示されます。このアイコンは、デスクトップの右下に表示されます。

**メモ:** 集中管理下クライアントでは、管理者がこの機能を利用不能にしている場合、通知領域アイコンは表示されません。

表 3-5 に、通知領域に表示される Symantec Endpoint Protection クライアントの状態アイコンを示します。

表 3-5 Symantec Endpoint Protection クライアントの状態アイコン








アイコン	説明
	クライアントは問題なく動作しています。オフラインになっているか自己管理であるかのいずれかです。自己管理クライアントは管理サーバーに接続されません。アイコンは何も付いていない黄色のシールドです。
	クライアントは問題なく動作しています。管理サーバーに接続され、サーバーと通信しています。セキュリティポリシーのすべてのコンポーネントがコンピュータを保護しています。アイコンは緑のドットが付いた黄色のシールドです。
	クライアントに軽度な問題があります。たとえば、ウイルス定義が最新ではないなどです。アイコンは中に黒い感嘆符のある明るい黄色のドットが付いた黄色のシールドです。
	クライアントが実行されていないか、クライアントに重度の問題があるか、少なくとも1つの保護技術が無効になっています。たとえば、ネットワーク脅威防止が無効である可能性があります。アイコンは真ん中に赤い斜線のある赤く縁取られた白いドット付きの黄色のシールドです。

表 3-6 に、通知領域に表示される Symantec Network Access Control クライアントの状態アイコンを示します。

表 3-6 Symantec Network Access Control クライアントの状態アイコン

アイコン	説明
	クライアントは問題なく実行されており、ホストインテグリティ検査に成功し、セキュリティポリシーが更新されています。オフラインになっているか自己管理であるかのいずれかです。自己管理クライアントは管理サーバーに接続されません。アイコンは何も付いていない金色のキーです。
	クライアントは問題なく実行されており、ホストインテグリティ検査に成功し、セキュリティポリシーが更新されています。サーバーと通信しています。アイコンは緑のドットが付いた金色のキーです。
	クライアントは、ホストインテグリティ検査に失敗したか、セキュリティポリシーが更新されていないかのいずれかです。アイコンは中に白色の「X」がある赤のドットが付いた金色のキーです。

p.40 の「通知領域アイコンの非表示と表示」を参照してください。

## 通知領域アイコンの非表示と表示

通知領域アイコンの非表示と表示たとえば、Windows タスクバー上に空き領域が必要な場合、通知領域アイコンを隠すことができます。

p.39 の「通知領域アイコンについて」を参照してください。

---

**メモ:** 管理下クライアントでは、管理者がこの機能を制限している場合、ユーザーは通知領域アイコンを隠すことができません。

---

通知領域アイコンを表示または非表示にするには

- 1 メインウィンドウのサイドバーで、[設定の変更]をクリックします。
- 2 [設定の変更]ページで、[クライアント管理]に対して[オプションの設定]をクリックします。
- 3 [クライアント管理の設定]ダイアログボックスの[全般]タブにある[表示オプション]で、[通知領域にシマンテック製品のセキュリティアイコンを表示する]のチェックマークをはずすか、チェックマークを付けます。
- 4 [OK]をクリックします。

## 管理者によるコンピュータ再起動の防止について

通常では管理者はクライアントコンピュータに対してコマンドをリモートで実行できます。セキュリティの理由から、管理者がリモートでコンピュータを再起動することを防ぐと安全です。

クライアントコンピュータの **Windows** レジストリキーを設定し、管理サーバーからの再起動コマンドを遮断する必要があります。クライアントコンピュータで、**DisableRebootCommand** キーを **1** に設定できます。それ以降は、管理者がコンソールから[クライアントコンピュータの再起動]コマンドを選択しても、クライアントコンピュータは再起動しません。



# 2

## Symantec Endpoint Protection クライアントでの保 護の管理

- 第4章 ウイルス対策とスパイウェア対策の管理
- 第5章 プロアクティブ脅威防止の管理
- 第6章 ネットワーク脅威防止の管理



# ウイルス対策とスパイウェア対策の管理

この章では以下の項目について説明しています。

- ウイルスとセキュリティリスクについて
- クライアントはウイルスとセキュリティリスクにどう応答するか
- ウイルス対策とスパイウェア対策の設定について
- ファイルのスキャンについて
- クライアントがウイルスまたはセキュリティリスクを検出した場合
- **Auto-Protect** について
- ウイルススキャンとスパイウェアスキャンの操作
- ユーザー定義スキャンのスケジュール
- 起動時、ユーザー定義、定時の各スキャンの編集と削除
- スキャン結果の解釈
- ウイルスとセキュリティリスクに対する処理の設定
- ウイルスとセキュリティリスクに対する通知の設定
- スキャン対象からの項目の除外について
- スキャンからの項目の除外
- 検疫ファイルの処理について
- 検疫の管理

- スキャン検出についての情報のシマンテックセキュリティレスポンスへの提出
- クライアントと Windows セキュリティセンターについて

## ウイルスとセキュリティリスクについて

クライアントはウイルスとセキュリティリスクの両方をスキャンできます。デフォルトでは、ユーザー定義スキャンと Auto-Protect スキャンがウイルス、トロイの木馬、ワーム、すべてのカテゴリのセキュリティリスクの有無をチェックします。

ウイルススキャンとスパイウェアスキャンは、カーネルレベルのルートキットも検出します。ルートキットとは、コンピュータのオペレーティングシステムから隠れて悪質な目的で使われる可能性のあるプログラムです。

図 4-1 ウイルスとセキュリティリスクがコンピュータをどのように攻撃するか

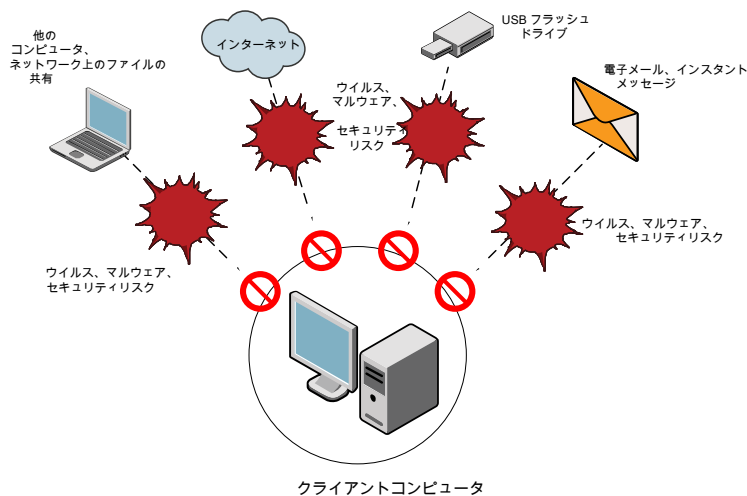


表 4-1 で、クライアントが保護する対象となるマルウェアとウイルスの種類について説明します。

表 4-1 ウイルス、トロイの木馬、ワーム

ウイルス	説明
ウイルス	<p>実行されたときに自己の複製を別のコンピュータプログラムまたはデータファイルに付着させるプログラムまたはコードです。感染したプログラムを実行したり、マクロウイルスが含まれるデータファイルを開いたりすると、付着したウイルスプログラムが実行されます。これにより、ウイルスの複製が別のプログラムやデータファイルに付着します。</p> <p>一般的に、ウイルスは発病すると、特定の日にメッセージを表示したりします。中には、プログラムを壊す、ファイルを削除する、ディスクを再フォーマットするなど、確実にデータを損傷するウイルスもあります。</p> <p>マクロウイルスは <b>Microsoft Word</b> のようなソフトウェアアプリケーションに組み込まれた言語で書き込まれるウイルスです。</p>
トロイの木馬	<p>ゲームやユーティリティなど有用なものに隠れたり偽装したりしているコードを含むプログラムです。</p>
ワーム	<p>他のプログラムに感染することなく自己を複製するプログラムです。ワームには、ディスク間で自身をコピーすることで広がるものや、メモリ上のみ複製してコンピュータの動作速度を低下させるものがあります。</p>

表 4-2 で、クライアントが保護する対象となるセキュリティリスクの種類について説明します。

表 4-2 セキュリティリスクの種類

セキュリティリスク	説明
悪意のあるインターネットボット	<p>自動化されたタスクを悪質な目的のためにインターネット上で実行するプログラムです。</p> <p>ボットは、コンピュータへの攻撃を自動化したり、Web サイトから情報を収集したりする目的で使用できます。</p>
複合型脅威	<p>ウイルス、ワーム、トロイの木馬、悪質なコードの性質を兼ね備え、サーバーとインターネットの脆弱性を悪用して攻撃を開始、感染、拡大する脅威です。複合型脅威は複数の方法や技法を使って急速に広がり、ネットワーク全体にわたって広く被害を与えます。</p>
アドウェア	<p>インターネット経由で個人情報を密かに収集し、その情報を別のコンピュータに送り返すプログラムまたは付加プログラムです。アドウェアは宣伝目的でブラウザの動作記録を追跡できます。広告コンテンツを配信することもできます。</p>
ダイヤラー	<p>ユーザーの許可なく、またはユーザーが知らないうちにコンピュータを使って、ダイヤル Q2 サービスまたは FTP サイトにダイヤルするプログラムです。通常、このようなプログラムでは利用料金が請求されます。</p>

セキュリティリスク	説明
ハッキングツール	コンピュータへの権限のないアクセスを可能にするためにハッカーが使うプログラムです。ハッキングツールの例としては、キーストロークを追跡して記録し、この情報をハッカーに送信するキーロガーがあります。ハッカーはこの情報を使って、ポートスキャンまたは脆弱性スキャンを実行できます。ハッキングツールは、ウイルスの作成にも使うことができます。
ジョークプログラム	悪ふざけや驚かせる目的でコンピュータの動作を改変または中断させるプログラムです。プログラムは、たとえば Web サイト、電子メールメッセージ、インスタントメッセージングプログラムからダウンロードされます。削除を試みたときに、マウスからごみ箱を遠ざけることがあります。マウスのクリックを逆にすることもあります。
その他	ウイルス、トロイの木馬、ワームなどのセキュリティリスクカテゴリの厳格な定義に沿わない、その他のセキュリティリスク
リモートアクセスプログラム	情報を入手したり、コンピュータを攻撃または改変したりするために、別のコンピュータからのインターネット経由のアクセスを許可するプログラムです。ユーザーは、正当なリモートアクセスプログラムをインストールすることもあります。何らかの処理で、知らないうちにこの種類のアプリケーションがインストールされることもあります。プログラムは、元のリモートアクセスプログラムを変更するかそのままの状態、悪用目的で使われます。
スパイウェア	<p>システムの活動を密かに監視し、パスワードなどの機密情報を検出して別のコンピュータに送り返すプログラムです。</p> <p>スパイウェアは Web サイト、電子メールメッセージ、インスタントメッセージと直接ファイル接続からダウンロードできます。また、ソフトウェアプログラムからのエンドユーザー使用許諾契約に同意すると、知らないうちにスパイウェアを受け取ることがあります。</p>
トラックウェア	インターネット上でのユーザーの経路を追跡して情報を対象システムに送信するスタンドアロンアプリケーションまたは付加アプリケーションです。たとえば、この種類のアプリケーションは Web サイトからダウンロードしたり、電子メールメッセージやインスタントメッセージングプログラムで受信したりする可能性があります。これにより、ユーザーの行動に関する機密情報を入手できます。

デフォルトでは、スキャンは次の処理を実行します。

- ウイルス、ワーム、トロイの木馬、複合型脅威の副作用を検出、除去、修復します。
- アドウェア、ダイヤラー、ハッキングツール、ジョークプログラム、リモートアクセスプログラム、スパイウェア、トラックウェアなどのセキュリティリスクの副作用を検出、除去、修復します。

シマンテックセキュリティレスポンス Web サイトでは、脅威とセキュリティリスクに関する最新情報を提供しています。この Web サイトには、ウイルスとセキュリティリスクについての白書や詳しい情報など、広範な参照情報もあります。

## クライアントはウイルスとセキュリティリスクにどう応答するか

クライアントは、感染源の種類に関係なく、ウイルスとセキュリティリスクからコンピュータを守ります。コンピュータは、ハードディスクドライブやフロッピーディスクから伝染する場合とネットワーク間で伝わる場合のウイルスとセキュリティリスクから保護されます。コンピュータは電子メールの添付ファイルまたはその他の方法で伝染するウイルスやセキュリティリスクからも保護されます。たとえば、インターネットにアクセスしたときに、ユーザーが知らないうちにコンピュータにセキュリティリスクがインストールされることがあります。

クライアントは圧縮ファイルに含まれるファイルをスキャンしウイルスとセキュリティリスクをクリーニングします。インターネットを媒介するウイルスに個別のプログラムやオプションの変更は必要ありません。**Auto-Protect** は圧縮されていないプログラムとデータファイルをダウンロード時に自動スキャンします。

クライアントはウイルスを検出するとデフォルトで感染ファイルからのウイルスのクリーニングを試みます。クライアントはウイルスの影響の修復も試みます。ファイルをクリーニングした場合、クライアントはコンピュータからリスクを完全に除去します。クライアントがファイルをクリーニングできない場合、クライアントは感染ファイルを検疫に移動します。ウイルスは検疫からは伝染できません。

コンピュータを新しいウイルス定義で更新すると、クライアントは検疫を自動的に調べます。ユーザーは検疫にある項目を再スキャンできます。最新の定義を使うと、前に検疫されたファイルをクリーニングまたは修復できることがあります。

---

**メモ:** 管理者は検疫にあるファイルの自動スキャンを選択できます。

---

セキュリティリスクの場合、デフォルトでクライアントが感染ファイルを検疫します。クライアントはセキュリティリスクが変更したシステム情報を以前の状態に戻します。一部のセキュリティリスクでは完全に除去しようとする、**Web** ブラウザのようなコンピュータ上にある別のプログラムで必ずエラーが発生します。ウイルス対策とスパイウェア対策の設定がリスクを自動的に処理しないこともあります。その場合、クライアントは処理を停止する前またはコンピュータを再起動する前に確認を求めます。代替りの方法として、セキュリティリスクのログ記録のみを行うように設定を変更できます。

クライアントソフトウェアはセキュリティリスクを発見すると、シマンテックセキュリティレスポンスへのリンクをスキャンウィンドウに表示します。シマンテックセキュリティレスポンス Web サイトでは、セキュリティリスクに関する詳しい情報を入手できます。管理者がカスタムメッセージを送信することもあります。

## ウイルス対策とスパイウェア対策の設定について

クライアントでは、ウイルス対策とスパイウェア対策について、ほとんどのユーザーに適しているデフォルトが設定されています。セキュリティネットワークに応じてこの設定をカスタマイズすることができます。**Auto-Protect**、定時、起動時、オンデマンドの各スキャンについてポリシー設定をカスタマイズできます。

ウイルス対策とスパイウェア対策には、次の設定があります。

- スキャン対象
- ウイルスまたはセキュリティリスクが検出されたときの処理

## ファイルのスキャンについて

ウイルススキャンとスパイウェアスキャンは、デフォルトですべてのファイルのスキャンします。定時スキャン、起動時スキャン、オンデマンドスキャンも、デフォルトですべてのファイルを診断します。

スキャンするファイルを拡張子で選択することもできますが、ウイルスとセキュリティリスクからの保護は低下します。スキャンする拡張子を選択する場合には、ウイルスによって拡張子を変更されていても **Auto-Protect** がファイルの種類を特定できます。

p.56 の「[ファイルの種類を指定する Auto-Protect の設定](#)」を参照してください。

特定のファイルのスキャンから除外することもできます。たとえば、スキャンでウイルス警告を引き起こさないファイルがわかっている場合などです。このようなファイルは、以降のスキャンから除外できます。

## 電子メールアプリケーションが単一の受信ボックスファイルを使っている場合

電子メールアプリケーションがすべての電子メールを単一のファイルに格納する場合には、集中例外を作成して、受信ボックスファイルのスキャンから除外する必要があります。**Outlook Express**、**Eudora**、**Mozilla**、**Netscape** などがこれに該当します。クライアントは、検出したウイルスを検疫するように設定されることがあります。クライアントは受信ボックスでウイルスを検出すると受信ボックス全体を検疫します。受信ボックスが検疫されると、電子メールにアクセスできなくなります。

通常は、ファイルのスキャンから除外することは推奨されません。しかし、受信ボックスファイルのスキャンから除外しても、クライアントは電子メールメッセージを開くときにウイルスを検出できます。ウイルスを検出した場合には、メッセージは安全に検疫または削除されます。

ファイルを除外するには、集中例外を設定します。

## 拡張子によるスキャンについて

クライアントは拡張子でコンピュータをスキャンできます。

以下の種類のファイルを選択できます。

文書ファイル	Microsoft Word や Excel の文書と、それらの文書に関連付けられているテンプレートファイルを含みます。クライアントは、文書ファイルがマクロウイルスに感染していないかどうかを調べます。
プログラムファイル	Dynamic Link Library (.dll)、バッチファイル(.bat)、コマンドファイル(.com)、実行可能ファイル(.exe)などのプログラムファイル。クライアントは、プログラムファイルがウイルスに感染していないかどうかを調べます。

### Auto-Protect スキャンのスキャンリストに拡張子を追加するには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [ウイルス対策とスパイウェア対策]の隣にある[オプションの設定]をクリックします。
- 3 [ウイルス対策とスパイウェア対策の設定]ダイアログボックスの[ファイルシステム **Auto-Protect**]タブにある[ファイルの種類]で、[選択した項目]をクリックします。
- 4 [拡張子]をクリックします。
- 5 追加する拡張子をテキストボックスに入力して、[追加]をクリックします。
- 6 必要に応じてステップ 5 を繰り返し、[OK]をクリックします。
- 7 [OK]をクリックします。

### オンデマンド、定時、起動時のスキャンのスキャンリストに拡張子を追加するには

- 1 クライアントのサイドバーで、[脅威のスキャン]をクリックします。
- 2 拡張子を追加するスキャンを右クリックして、[編集]を選択します。  
変更は、選択した特定のスキャンにのみ適用されます。
- 3 [スキャンオプション]タブの[ファイルの種類]で、[選択した拡張子]を選択してから[拡張子]をクリックします。
- 4 追加する拡張子を入力して、[追加]をクリックします。
- 5 必要に応じてステップ 4 を繰り返し、[OK]をクリックします。
- 6 [OK]をクリックします。

## すべてのファイルのスキャンについて

クライアントは、拡張子に関係なくコンピュータ上のすべてのファイルのスキャンできます。すべてのファイルのスキャンすることで、全体的な保護が実現されます。全ファイルの

キャンは拡張子ごとのスキャンより時間がかかりますが、ウイルスとセキュリティリスクからの保護は高くなります。

## マクロウイルス感染の防止について

クライアントは Microsoft Word と Excel のほとんどのマクロウイルスを、自動的に検出して削除します。定時スキャンを定期的に行っている場合は、コンピュータをマクロウイルス感染から保護できます。Auto-Protect も定期的にマクロウイルスを検索し、検出すればクリーニングします。

マクロウイルス感染を最大に防止するには、次の操作を実行します。

- Auto-Protect を有効にします。  
Auto-Protect はアクセスがあったファイル、または修正されたファイルを定期的にもスキャンします。
- 使用可能な場合には、電子メールに対して Auto-Protect を実行します。
- オートマクロを無効にして、グローバルなテンプレートファイルを保護します。

## クライアントがウイルスまたはセキュリティリスクを検出した場合

ファイルがウイルスやセキュリティリスクに感染したとき、クライアントの対応はリスクの種類によって異なります。クライアントはリスクの種類ごとに第1の処理を行い、それが失敗した場合には第2の処理を適用します。

デフォルトでは、ウイルスを検出するとクライアントはまず感染ファイルからウイルスをクリーニングしようと試みます。ファイルをクリーニングできない場合は、そのエラーをログに記録し、感染ファイルを検疫に移動します。

デフォルトでは、セキュリティリスクを検出するとクライアントはリスクを検疫します。また、セキュリティリスクによって加えられた変更の削除または修正も試みます。セキュリティリスクを検疫できない場合は、そのリスクをログに記録して放置します。

---

**メモ:** 検疫されれば、リスクが広がることはありません。クライアントが検疫に移動したファイルに、ユーザーはアクセスできません。クライアントは、検疫した項目に対する変更を元に戻すこともあります。

---

スキャンの各種類に対して、クライアントによるウイルスとセキュリティリスクの処理方法に関する設定を変更できます。リスクのカテゴリごとに、また各セキュリティリスクごとに異なる処理を設定することができます。

---

**メモ:** 場合によっては、アドウェアやスパイウェアのようにセキュリティリスクを含むアプリケーションを、それと気付かずインストールすることがあります。検疫してもコンピュータに支障がないことをシマンテック社がすでに確認している場合には、クライアントがリスクを検疫します。クライアントがリスクをすぐに検疫すると、その処理によってコンピュータが不安定な状態になることがあります。そのため、クライアントはアプリケーションのインストール完了を待ってからリスクを検疫します。その後、リスクの影響を修正します。

---

## Auto-Protect について

**Auto-Protect** は、ウイルスの攻撃に対する最大の防衛です。ファイルのアクセス、コピー、保存、移動を行うとき、またはファイルを開くときは常に **Auto-Protect** がファイルをスキャンして、ウイルスが含まれていないことを確認します。

**Auto-Protect** は、実行可能コードを含む拡張子と、すべての **.exe** ファイル、**.doc** ファイルをスキャンします。ウイルスによって拡張子に変更されても、**Auto-Protect** はファイルの種類を特定できます。たとえば、ウイルスは拡張子を **Auto-Protect** のスキャン対象として設定されているものとは異なる拡張子に変更する場合があります。

管理者が設定をロックしていなければ、**Auto-Protect** を有効化または無効化することができます。

## Auto-Protect とセキュリティリスクについて

デフォルトでは、**Auto-Protect** は次の処理を行います。

- アドウェアやスパイウェアなどのセキュリティリスクのスキャン
- 感染ファイルの検疫
- セキュリティリスクの副作用の除去または修復

**Auto-Protect** でのセキュリティリスクのスキャンを無効にすることができます。

p.57 の「**Auto-Protect** でのセキュリティリスクのスキャンと遮断の有効化と無効化」を参照してください。

**Auto-Protect** は、セキュリティリスクを連続的にコンピュータにダウンロードするようなプロセスを検出したとき、通知を表示して検出をログに記録します。( **Auto-Protect** から通知が送信されるように設定する必要があります)。そのプロセスが同じセキュリティリスクのダウンロードを続ける場合は、複数の通知が表示され、複数のイベントがログに記録されます。複数の通知が表示されたり、複数のイベントがログに記録されたりするのを防ぐために、**Auto-Protect** は 3 回検出を行った後に、セキュリティリスクについての通知の送信を自動的に停止します。イベントのログ記録についても、3 回の検出後に停止します。

状況によっては、**Auto-Protect** は、セキュリティリスクについての通知の送信とイベントのログ記録を停止しません。

Auto-Protect が通知の送信とイベントのログ記録を続行するのは、次のいずれかに当てはまる場合です。

- クライアントコンピュータで、ユーザーまたは管理者がセキュリティリスクのインストール遮断を無効にした (デフォルト設定は有効)。
- プロセスがダウンロードするセキュリティリスクの種類に対する処理に、[放置]が含まれる

## Auto-Protect と電子メールスキャンについて

Auto-Protect は、サポートされているグループウェア電子メールクライアントもスキャンします。

次の電子メールクライアントが保護の対象です。

- Lotus Notes 4.5x、4.6、5.0、6.x
- Microsoft Outlook 98/2000/2002/2003/2007 (MAPI、インターネット)
- Microsoft Exchange クライアント 5.0、5.5

---

**メモ:** Auto-Protect は、サポートされている電子メールクライアントに対してのみ動作します。電子メールサーバーは保護しません。

---

Auto-Protect は POP3 または SMTP の通信プロトコルを使うすべてのトラフィックを監視することによってその他のインターネット電子メールプログラムもスキャンします。クライアントソフトウェアは、着信メッセージと発信メッセージでリスクをスキャンするように設定できます。発信電子メールをスキャンすると、電子メールクライアントを利用してネットワーク上で自己を複製し配布するような脅威の拡散を防止するうえで有効です。

---

**メモ:** インターネット電子メールスキャンは、64ビットコンピュータではサポートされません。

---

Lotus Notes と Microsoft Exchange の電子メールスキャンの場合は、Auto-Protect がスキャンするのは電子メールに関連付けされた添付ファイルのみです。

POP3 または SMTP のプロトコルを使うメッセージのインターネット電子メールスキャンの場合は、Auto-Protect が次の項目をスキャンします。

- メッセージ本文
- メッセージの添付ファイル

次の条件が当てはまる場合は、添付ファイルのあるメッセージを開くと添付ファイルがすぐにコンピュータにダウンロードされ、スキャンされます。

- Microsoft Exchange クライアントまたは Microsoft Outlook (MAPI) を使用している
- 電子メールに対して Auto-Protect が有効

低速度の接続で、添付ファイルのサイズが大きいメッセージをダウンロードすると、メールのパフォーマンスに影響します。定期的に大きい添付ファイルを受信する場合には、この機能を無効にすると便利です。

p.57の「**Auto-Protect**でのセキュリティリスクのスキャンと遮断の有効化と無効化」を参照してください。

---

**メモ:** 電子メールを開くときにウイルスが検出された場合には、**Auto-Protect** がスキャンを完了するため、電子メールを開くのに数秒かかることがあります。

---

電子メールスキャンは、次の電子メールクライアントをサポートしていません。

- IMAP クライアント
- AOL クライアント
- Hotmail、Yahoo! Mail、GMAIL など Web ベースの電子メール

## 暗号化電子メール接続に対する Auto-Protect 処理の無効化

セキュアリンクを介して電子メールを送受信することができます。デフォルトでは、インターネット電子メール **Auto-Protect** で、POP3 と SMTP 接続による暗号化パスワードと電子メールがサポートされています。SSL (Secure Sockets Layer) を利用する POP3 または SMTP を使う場合に、クライアントはセキュリティで保護された接続を検出しますが、暗号化メッセージはスキャンしません。

**Auto-Protect** は、セキュリティで保護された接続を使う電子メールをスキャンしない場合でも、添付ファイルのリスクからコンピュータを保護し続けます。**Auto-Protect** は、添付ファイルをハードディスクドライブに保存するときに電子メールの添付ファイルをスキャンします。

---

**メモ:** パフォーマンス上の理由により、POP3 のインターネット電子メール **Auto-Protect** は、サーバーオペレーティングシステムではサポートされていません。

---

必要な場合には、暗号化電子メールの処理を無効にすることができます。これらのオプションを無効にすると、**Auto-Protect** は送受信された暗号化しない電子メールはスキャンしますが、暗号化電子メールは遮断します。オプションを有効にして暗号化電子メールの送信を試みた場合、**Auto-Protect** は電子メールアプリケーションを再起動するまでその電子メールを遮断します。

---

**メモ:** 暗号化接続の **Auto-Protect** 処理を無効にした場合には、**Windows** をログオフして再ログオンしないとその変更が適用されません。すぐに変更を適用する必要がある場合は、ログオフして再ログオンしてください。

---

暗号化電子メール接続に対する Auto-Protect 処理を無効にするには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [ウイルス対策とスパイウェア対策]の隣にある[オプションの設定]をクリックします。
- 3 [インターネット電子メール Auto-Protect]タブで、[拡張]をクリックします。
- 4 [接続の設定]で、[暗号化 POP3 接続を許可する]と[暗号化 SMTP 接続を許可する]のチェックマークをはずします。
- 5 [OK]をクリックします。

## Auto-Protect スキャン統計の表示

Auto-Protect スキャン統計には最後の Auto-Protect スキャンの状態、最後にスキャンしたファイル、ウイルス感染、セキュリティリスク情報が表示されます。

Auto-Protect スキャン統計を表示するには

- ◆ クライアントの[状態]ページにある[ウイルス対策とスパイウェア対策]の隣で、[オプション]、[ファイルシステム Auto-Protect 統計の表示]の順に選択します。

## リスクリストの表示

クライアントが検出する現在のリスクを表示できます。リストは、現在のウイルス定義に対応しています。

リスクリストを表示するには

- ◆ クライアントの[状態]ページにある[ウイルス対策とスパイウェア対策]の隣で、[オプション]、[脅威リストの表示]の順に選択します。

## ファイルの種類を指定する Auto-Protect の設定

Auto-Protect は、すべてのファイルをスキャンするように事前設定されています。選択した拡張子のファイルのみをスキャンするにすれば、スキャンは短時間で終了します。たとえば、次の拡張子のみをスキャンするようになります。

- .exe
- .com
- .dll
- .doc
- .xls

通常、ウイルスの影響を受けるファイルの種類は限られています。しかし、スキャンする拡張子を限定すると Auto-Protect でスキャンされないファイルがあるため、保護が低下し

ます。デフォルトの拡張子リストには、ウイルス感染のリスクがある一般的なファイルが示されています。

**Auto-Protect** は、実行可能コードを含む拡張子と、すべての **.exe** ファイル、**.doc** ファイルをスキャンします。ウイルスによって拡張子に変更されていてもファイルの種類を特定できます。たとえば、拡張子に変更されていても **.doc** ファイルをスキャンします。

ウイルスとセキュリティリスクからコンピュータを最大限に保護するためには、すべてのファイルをスキャンするように **Auto-Protect** を設定してください。

**Auto-Protect** でファイルの種類を指定するには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [ウイルス対策とスパイウェア対策]の隣にある[オプションの設定]をクリックします。
- 3 [Auto-Protect]タブの[ファイルの種類]で、次のいずれかの操作をします。
  - すべてのファイルをスキャンする場合には、[すべての種類]をクリックします。
  - リストした拡張子に一致するファイルのみをスキャンする場合には、[選択した項目]をクリックします。次に、[拡張子]をクリックしてデフォルトの拡張子リストを変更します。
- 4 [選択した拡張子]を選択した場合は、[ファイルの内容を調べることによってファイルの種類を判断する]にチェックマークを付けるか、チェックマークをはずします。
- 5 [OK]をクリックします。

## Auto-Protect でのセキュリティリスクのスキャンと遮断の有効化と無効化

デフォルトでは、**Auto-Protect** は次の処理を行います。

- アドウェアやスパイウェアなどのセキュリティリスクのスキャン
- 感染ファイルの検疫
- セキュリティリスクによる影響の除去または修復の試行

デフォルトでは、セキュリティリスクのインストールを遮断してもコンピュータの安定性に影響しない場合には **Auto-Protect** はそのインストールも遮断します。セキュリティリスクを遮断することでコンピュータの安定性が低下する可能性があるとして **Symantec** が判断した場合には **Auto-Protect** はリスクのインストールを許可します。その上で **Auto-Protect** はリスクに対して設定した処理をすぐに適用します。

しかし、**Auto-Protect** ファイルスキャンでセキュリティリスクのスキャンを一時的に無効にし、後で再度有効にする必要があることもあります。また **Auto-Protect** が特定のセキュリティリスクに反応する時間を制御するためにセキュリティリスクの遮断を無効にする必要がある場合もあります。

---

**メモ:** これらの設定を管理者がロックしている場合もあります。

---

**Auto-Protect** でのセキュリティリスクのスキャンと遮断を有効または無効にするには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [ウイルス対策とスパイウェア対策]の隣にある[オプションの設定]をクリックします。
- 3 [ファイルシステム **Auto-Protect**]タブの[オプション]で、次のいずれかの操作をします。
  - [セキュリティリスクをスキャンする]にチェックマークを付けるか、チェックマークをはずします。
  - [セキュリティリスクのインストールを遮断する]にチェックマークを付けるか、チェックマークをはずします。
  - [ネットワークドライブ上のファイルをスキャンする]にチェックマークを付けるか、チェックマークをはずします。
- 4 [OK]をクリックします。

## ネットワークスキャンの設定

ネットワークスキャンの設定には、次のオプションがあります。

- **Auto-Protect** を実行しているリモートコンピュータ上のファイルを **Auto-Protect** が信頼するかどうかの設定
- **Auto-Protect** がネットワークからスキャンしたファイルの記録を格納するためにキャッシュを使うかどうかの指定

デフォルトでは、**Auto-Protect** は、お使いのコンピュータからリモートコンピュータにファイルを書き込むときにスキャンします。リモートコンピュータからお使いのコンピュータにファイルを書き込むときにスキャンすることもできます。

逆に、リモートコンピュータ上のファイルを読み込むときには、**Auto-Protect** はファイルのスキャンしません。デフォルトでは、**Auto-Protect** はリモートコンピュータ上の **Auto-Protect** を信頼しようとします。信頼オプションが両方のコンピュータで有効になっている場合には、ローカルの **Auto-Protect** がリモートコンピュータの **Auto-Protect** 設定をチェックします。リモートの **Auto-Protect** 設定でセキュリティのレベルがローカルの設定以上である場合に、ローカルの **Auto-Protect** はリモートの **Auto-Protect** を信頼します。ローカルの **Auto-Protect** がリモートの **Auto-Protect** を信頼するとき、ローカルの **Auto-Protect** はリモートコンピュータから読み込むファイルのスキャンしません。ローカルコンピュータは、リモートの **Auto-Protect** がファイルをすでにスキャン済みであると信頼します。

---

**メモ:** ローカルの **Auto-Protect** は、リモートコンピュータからコピーするファイルを常にスキャンします。

---

信頼オプションは、デフォルトで有効になっています。信頼オプションを無効にすると、ネットワークの処理速度が低下する場合があります。

#### リモートコンピュータ上の Auto-Protect の信頼を無効にするには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [ウイルス対策とスパイウェア対策]の隣にある[オプションの設定]をクリックします。
- 3 [ファイルシステム Auto-Protect]タブで、[拡張]をクリックします。
- 4 [Auto-Protect 拡張オプション]ダイアログボックスの[追加の拡張オプション]で、[ネットワーク]をクリックします。
- 5 [ネットワークスキャンの設定]で、[Auto-Protect を実行しているリモートコンピュータ上のファイルを信頼する]のチェックマークをはずします。
- 6 メインウィンドウに戻るまで[OK]をクリックします。

ネットワークキャッシュを使う設定も可能です。ネットワークキャッシュは、Auto-Protect がリモートコンピュータからスキャンしたファイルの記録を格納します。ネットワークキャッシュを使うと、Auto-Protect が同じファイルを複数回スキャンすることを回避できます。同じファイルの複数回スキャンを回避すると、システムのパフォーマンスが向上する場合があります。Auto-Protect でスキャンして記憶するファイル(エン트리)の数を設定できます。また、コンピュータがキャッシュからエントリを削除するまでのタイムアウトも設定することができます。タイムアウト期限が切れると、そのエントリは削除されます。この場合、リモートコンピュータからそのファイルを再度要求したとき、そのファイルは Auto-Protect スキャンの対象になります。

#### ネットワークキャッシュを設定するには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [ウイルス対策とスパイウェア対策]の隣にある[オプションの設定]をクリックします。
- 3 [ウイルス対策とスパイウェア対策の設定]ダイアログボックスの[ファイルシステム Auto-Protect]タブで、[拡張]をクリックします。
- 4 [Auto-Protect 拡張オプション]ダイアログボックスの[追加の拡張オプション]で、[ネットワーク]をクリックします。
- 5 [ネットワークのスキャンの設定]ダイアログボックスで、[ネットワークキャッシュ]にチェックマークを付けるか、チェックマークをはずします。
- 6 ネットワークキャッシュを有効にする場合は、デフォルトを使うか、次のいずれかの操作をします。
  - Auto-Protect がスキャンして記憶するファイル(エン트리)の数を、矢印で指定するか入力します。

- キャッシュが消去される前にエントリがキャッシュに保存される時間を秒数で入力します。

7 メインウィンドウに戻るまで[OK]をクリックします。

## ウイルススキャンとスパイウェアスキャンの操作

**Auto-Protect** は、ウイルス感染とセキュリティリスクに対する最も強力な防衛です。**Auto-Protect** に加え、クライアントには追加の保護として何種類かのスキャンが用意されています。

表 4-3 に、スキャンの種類を示します。

表 4-3 スキャンの種類

種類	説明
カスタムスキャン	ファイル、フォルダ、ドライブ、コンピュータ全体を任意のときにスキャンします。スキャンするコンピュータの部分を選択します。
アクティブスキャン	システムメモリと、ウイルスやセキュリティリスクの攻撃を受けやすい場所を短時間でスキャンします。
完全スキャン	ブートセクタとシステムメモリを含めてコンピュータ全体をスキャンします。ネットワークドライブをスキャンする場合にはパスワードの入力が必要なことがあります。
定時スキャン	指定した頻度で無人で実行します。
起動時スキャン	コンピュータを起動してログオンするとき毎回実行します。
ユーザー定義	指定したファイルセットを任意のときにスキャンします。

**Auto-Protect** が有効なかぎり、アクティブスキャンを日単位で実行し、すべてのファイルの定時スキャンを週単位で実行すれば十分な保護が得られます。コンピュータに対するウイルス攻撃が頻繁な場合には、起動時の完全スキャンか日単位の定時スキャンを追加することを検討してください。

また、既知のリスクではなく疑わしい動作を調べるスキャンの頻度も設定することができます。

p.91 の「**TruScan プロアクティブ脅威スキャンを実行する頻度の設定**」を参照してください。

## ウイルススキャンとスパイウェアスキャンの動作

保護スキャンはコンピュータのウイルスとセキュリティリスクを識別して中和または除去します。スキャンは次のプロセスを使ってウイルスまたはリスクを除去します。

- スキャンエンジンはコンピュータのファイルと他のコンポーネントからファイル内のウイルスの痕跡を検索します。各ウイルスにはシグネチャと呼ばれる認識可能なパターンがあります。有害なウイルスコードのない既知のウイルスシグネチャを含んでいるウイルス定義ファイルがクライアントにインストールされます。スキャンエンジンは各ファイルまたはコンポーネントをウイルス定義ファイルと比較します。スキャンエンジンが一致を見つけた場合、そのファイルは感染しています。
- スキャンエンジンはウイルスまたはリスクが感染を引き起こしたかどうかを判断するために定義ファイルを使います。スキャンエンジンは感染ファイルに修復処理を適用します。感染ファイルを修復するには、クライアントはファイルをクリーニングするか、削除するか、検疫します。

表 4-4 に、クライアントがコンピュータでスキャンするコンポーネントの説明を示します。

表 4-4 クライアントがスキャンするコンピュータのコンポーネント

コンポーネント	説明
選択したファイル	<p>クライアントは個々のファイルをスキャンします。ほとんどのスキャンでは、スキャン対象のファイルを選択します。</p> <p>クライアントソフトウェアは、パターンに基づくスキャンを使ってファイルのウイルスの形跡を検索します。ウイルスの形跡は、パターンまたはシグネチャと呼ばれます。特定のウイルスを識別する方法として、各ファイルをウイルス定義に含まれる無害なシグネチャと比較します。</p> <p>ウイルスが見つかった場合、デフォルトでクライアントはファイルからウイルスをクリーニングしようとしています。ファイルをクリーニングできない場合は、コンピュータがさらに感染するのを防止するために感染ファイルを検疫します。</p> <p>また、クライアントは、ファイルと Windows レジストリキー内のセキュリティリスクの形跡をパターンに基づくスキャンによって検索します。セキュリティリスクが見つかった場合、デフォルトでクライアントは感染ファイルを検疫して、リスクの影響を修復します。検疫できない場合は、その試行をログに記録します。</p>
コンピュータメモリ	<p>クライアントはコンピュータのメモリを検索します。ファイル感染ウイルス、ブートセクタ感染ウイルス、マクロウイルスはメモリに常駐する可能性があります。メモリ常駐型のウイルスは、自己をコンピュータのメモリにコピーしています。ウイルスはトリガイベントが起きるまでメモリ上に隠れることができます。その後、ウイルスはディスクドライブのフロッピーディスクやハードディスクドライブに伝染します。ウイルスがメモリ上にある場合はクリーニングできません。しかし、メッセージに従ってコンピュータを再起動すればメモリからウイルスを除去できます。</p>
ブートセクタ	<p>クライアントは、コンピュータのブートセクタにブートウイルスがないかどうかをチェックします。パーティションテーブルとマスターブートレコードの 2 つがチェックされます。</p>

コンポーネント	説明
フロッピーディスクドライブ	ウイルスが伝染する典型的な方法として、フロッピーディスクを介した伝染があります。コンピュータを起動または停止するとき、フロッピーディスクがディスクドライブに入ったままになっていることがあります。スキャンが開始されると、クライアントはディスクドライブに入っているフロッピーディスクのブートセクタとパーティションテーブルを検索します。コンピュータの電源を切るときには、感染の可能性を防止するためにディスクの取り出しを促すメッセージが表示されます。

## ウイルス定義ファイルについて

ウイルスのファイルには、解析すると一定のパターンを示すコードが含まれています。このパターンは、感染ファイルで追跡することができます。このパターンはシグネチャとも呼ばれます。アドウェアやスパイウェアなどのセキュリティリスクにも、認識可能なシグネチャがあります。

ウイルス定義ファイルには、有害なウイルスコードを含まない既知のウイルスシグネチャのリストと、既知のセキュリティリスクシグネチャのリストが記録されています。スキャンソフトウェアは、コンピュータ上のファイルに定義ファイルに含まれる既知のシグネチャがないかどうかを検索します。ウイルスとの一致が見つかった場合、そのファイルは感染しています。クライアントは、定義ファイルを使ってどのウイルスが感染の原因になったかを判断し、その副作用を修復します。セキュリティリスクが見つかった場合、クライアントは定義ファイルを使ってリスクを検疫し、その副作用を修復します。

コンピュータ社会には、絶えず新しいウイルスやセキュリティリスクがもたらされています。コンピュータの定義ファイルが最新であることを確認する必要があります。クライアントが最新のウイルスやセキュリティリスクも検出してクリーニングできるようにしてください。

## 圧縮ファイルのスキャンについて

ウイルススキャンとスパイウェアスキャンは、圧縮ファイルのスキャンします。たとえば、.zip ファイルはスキャン対象です。圧縮ファイルを含む圧縮ファイルは、管理者がスキャンする深さを10レベルまで指定できます。サポートされる圧縮ファイルスキャンの種類については、管理者に問い合わせてください。

**Auto-Protect** が有効な場合は、圧縮ファイルのすべてのファイルがスキャンされます。

## ユーザー定義スキャンのスケジュール

定時スキャンは、脅威とセキュリティリスク防止のための重要なコンポーネントです。少なくとも1週間に1回はスキャンを実行するように設定して、コンピュータにウイルスやセキュリティリスクがないことを確認する必要があります。新しく作成したスキャンは、[脅威のスキャン]ペインのスキャンリストに表示されます。

---

**メモ:** 管理者がすでに定時スキャンを作成している場合は、[脅威のスキャン]ペインのスキャンリストに表示されます。

---

スケジュール設定によってスキャンが実行されるときには、コンピュータが起動され、Symantec Endpoint Protection サービスがロードされる必要があります。デフォルトでは、Symantec Endpoint Protection サービスはコンピュータの起動時にロードされません。

集中管理下クライアントの場合は、管理者がこれらの設定を上書きしていることがあります。

複数のスキャンを同じコンピュータ上で実行するようにスケジュール設定し、スキャンが同時に始まる場合には、スキャンは順次実行されます。1つのスキャンが終わってから次のスキャンが始まります。たとえば、同じコンピュータ上で3つの別々のスキャンが午後1時に実行されるように設定するとします。それぞれのスキャンが別のドライブをスキャンします。1つのスキャンがドライブ C、2つ目のスキャンがドライブ D、3つ目のスキャンがドライブ E をスキャンします。この例では、ドライブ C、D、E をスキャンする1つの定時スキャンを作成するほうがよいでしょう。

p.29の「[コンピュータをただちにスキャンする](#)」を参照してください。

各ダイアログボックスのオプションについて詳しくは[ヘルプ]をクリックしてください。

#### ユーザー定義スキャンをスケジュールするには

- 1 クライアントのサイドバーで、[脅威のスキャン]をクリックします。
- 2 [新しいスキャンの作成]をクリックします。
- 3 [新しいスキャンの作成 - スキャンの対象]ダイアログボックスで、スケジュール設定するスキャンの種類を次の中から選択します。

アクティブスキャン	ウイルスとセキュリティリスクによる感染の可能性が高いコンピュータ領域をスキャンします。
完全スキャン	コンピュータ全体をスキャンして、ウイルスとセキュリティリスクをチェックします。
カスタムスキャン	選択したコンピュータ領域をスキャンして、ウイルスとセキュリティリスクをチェックします。

- 4 [次へ]をクリックします。

- 5 [カスタムスキャン]を選択した場合は、該当するチェックボックスにチェックマークを付けてスキャンする場所を指定し、[次へ]をクリックします。

記号の意味は次のとおりです。

ファイル、ドライブ、フォルダが選択されていません。項目がドライブまたはフォルダの場合には、その中のフォルダとファイルも選択されていません。

個々のファイルまたはフォルダが選択されています。

個々のフォルダまたはドライブが選択されています。フォルダまたはドライブ内の項目もすべて選択されています。

個々のフォルダまたはドライブは選択されていませんが、そのフォルダまたはドライブ内の項目が1つ以上選択されています。

- 6 [新しいスキャンの作成 - スキャンオプション]ダイアログボックスでは、次のオプションを変更できます。

ファイルの種類 クライアントがスキャンする拡張子を変更します。デフォルト設定ではすべてのファイルをスキャンします。

処理 ウイルスやセキュリティリスクが見つかったときの第1の処理と第2の処理を変更します。

通知 ウイルスまたはセキュリティリスクが見つかったときに表示するメッセージを作成します。修復処理を実行する前に通知するかどうかも設定できます。

拡張 スキャン結果のダイアログボックスの表示のような付加的なスキャン機能を変更します。

スキャン拡張 クライアントがスキャンするコンピュータコンポーネントを変更します。利用可能であるオプションはステップ3で選択したものによって決まります。

集中例外 クライアントがスキャンから除外する項目を追加します。

- 7 [次へ]をクリックします。

- 8 [新しいスキャンの作成 - スキャンのタイミング]ダイアログボックスで、[指定時]をクリックしてから、[次へ]をクリックします。  
オンデマンドスキャンまたは起動時スキャンを作成することもできます。  
p.65の「[オンデマンドまたはコンピュータの起動時に実行されるスキャンのスケジュール](#)」を参照してください。
- 9 [新しいスキャンの作成 - スケジュール]ダイアログボックスで、スキャンの頻度とタイミングを指定し、[次へ]をクリックします。
- 10 [新しいスキャンの作成 - スキャン名]ダイアログボックスで、スキャンの名前と説明を入力します。  
たとえば、スキャンの名前を「金曜午前」にします。
- 11 [完了]をクリックします。

## オンデマンドまたはコンピュータの起動時に実行されるスキャンのスケジュール

コンピュータの起動時またはログオン時に必ず自動スキャンを実行して、定時スキャンを補うことができます。多くの場合、起動時スキャンは **Windows** フォルダや **Microsoft Word** と **Excel** のテンプレートを格納するフォルダなど、重要で危険度の高いフォルダに制限されます。

クライアントには自動生成アクティブスキャンと呼ばれる起動時スキャンも含まれています。自動生成スキャンは、ユーザーがコンピュータにログオンするたびにコンピュータ上の感染しやすい場所をチェックします。このスキャンは、他のオンデマンドスキャンを設定するのと同じように編集できます。ただし、メモリや他の感染しやすい場所にあるファイルのスキャンを無効にすることはできません。

定期的に同じファイルセットやフォルダセットをスキャンする場合には、それらの項目のみを対象にしたオンデマンドスキャンを作成できます。指定したファイルやフォルダにウイルスとセキュリティリスクがないことを、いつでもすばやく確認することができます。オンデマンドスキャンは手動で実行する必要があります。

複数の起動時スキャンを作成した場合は、作成された順序で順次実行されます。管理者は起動時スキャンを作成できないようにクライアントを設定することができます。

p.29の「[コンピュータをただちにスキャンする](#)」を参照してください。

各ダイアログボックスのオプションについて詳しくは[ヘルプ]をクリックしてください。

**オンデマンドまたはコンピュータの起動時に実行されるスキャンをスケジュールするには**

- 1 クライアントのサイドバーで、[脅威のスキャン]をクリックします。
- 2 [新しいスキャンの作成]をクリックします。

- 3 定時スキャンを作成するにはステップ 3 から 7 に従います。  
p.62 の「ユーザー定義スキャンのスケジュール」を参照してください。
- 4 [新しいスキャンの作成 - スキャンのタイミング]ダイアログボックスで、次のいずれかの操作をします。
  - [起動時]をクリックします。
  - [オンデマンド]をクリックします。
- 5 [次へ]をクリックします。
- 6 [新しいスキャンの作成 - スキャン名]ダイアログボックスで、スキャンの名前と説明を入力します。  
たとえば、スキャンの名前を「マイスキャン1」にします。
- 7 [完了]をクリックします。

## 起動時、ユーザー定義、定時の各スキャンの編集と削除

既存の起動時スキャン、ユーザー定義スキャン、定時スキャンは編集と削除が可能です。スキャンの種類によっては設定できないオプションもあります。

スキャンを編集するには

- 1 クライアントのサイドバーで、[脅威のスキャン]をクリックします。
- 2 スキャンリストで編集するスキャンを右クリックしてから、[編集]を選択します。
- 3 [スキャンの対象]、[スキャンオプション]、[スキャンスケジュール]の各タブで変更を行います。

定時スキャンの場合は、スケジュールも修正できます。

- 4 [OK]をクリックします。

スキャンを削除するには

- 1 クライアントのサイドバーで、[脅威のスキャン]をクリックします。
- 2 スキャンリストで削除するスキャンを右クリックしてから、[削除]を選択します。
- 3 [削除の確認]ダイアログボックスで、[はい]をクリックします。

## スキャン結果の解釈

オンデマンド、定時、起動時、ユーザー定義のいずれかのスキャンを実行したとき、クライアントソフトウェアでは、デフォルトでスキャンの進行状況ダイアログボックスが表示されて

進行状況が報告されます。また、**Auto-Protect** はウイルスまたはセキュリティリスクを検出すると常に結果ダイアログを表示します。これらの通知を無効にすることができます。

集中管理ネットワークでは、管理者が開始したスキャンの進行状況ダイアログボックスが表示されないことがあります。同様に、管理者はクライアントがウイルスまたはセキュリティリスクを検出したときに結果を表示しないように選択することもあります。

スキャン中にクライアントがリスクを検出した場合は、スキャンの進行状況ダイアログボックスに、次の情報と結果が表示されます。

- 感染ファイルの名前
- ウイルスまたはセキュリティリスクの名前
- クライアントがリスクに対して実行した処理

デフォルトでは、ウイルスまたはセキュリティリスクが検出されると必ず通知されます。

---

**メモ:** クライアントが動作しているオペレーティングシステムの言語によっては、ウイルス名に使われている文字の一部を解釈できない場合があります。オペレーティングシステムが解釈できない文字は、通知で疑問符として表示されます。たとえば、**Unicode**のウイルス名には2バイト文字が含まれることがあります。英語版のオペレーティングシステムでクライアントが動作しているコンピュータでは、このような文字が疑問符として表示されます。

---

スキャンの進行状況ダイアログボックスを表示するようにクライアントソフトウェアを設定している場合は、スキャンを一時停止、再開、中止することができます。スキャンが完了すると、結果がリストに表示されます。ウイルスやセキュリティリスクが検出されない場合には、リストは空のまま、状態は完了になります。

p.30の「[スキャンの一時停止と遅延](#)」を参照してください。

## スキャン結果または Auto-Protect の結果に対する操作

スキャンの進行状況ダイアログボックスと **Auto-Protect** の結果ダイアログボックスには、同じようなオプションがあります。クライアントがプロセスやアプリケーションを終了、またはサービスを停止する必要がある場合には、[リスクの削除]オプションが有効です。ダイアログのリスクで処理を必要とする場合でも、ダイアログボックスを閉じることができないこともあります。

表 4-5 に、スキャン結果ダイアログボックスのオプションの説明を示します。

表 4-5 スキャン結果ダイアログボックスのオプション

ボタン	説明
今すぐリスクを削除する	<p>[リスクの削除]ダイアログボックスを表示します。</p> <p>[リスクの削除]ダイアログボックスでは、それぞれのリスクに対して次のいずれかの処理を選択できます。</p> <ul style="list-style-type: none"> <li>■ はい クライアントがリスクを除去します。リスクを除去するには再起動が必要な場合があります。再起動が必要かどうかは、ダイアログボックスの情報で示されます。</li> <li>■ いいえ 結果ダイアログボックスを閉じると、ダイアログボックスが表示されません。これは、まだ処理が必要であることを確認するダイアログボックスです。ただし、[リスクの削除]ダイアログはコンピュータを再起動するまで抑止されます。</li> </ul>
閉じる	<p>どのリスクに対しても処理が必要ない場合には、結果ダイアログボックスを閉じます。</p> <p>処理が必要な場合には、次のいずれかの通知が表示されます。</p> <ul style="list-style-type: none"> <li>■ リスクの削除が必要 プロセスの終了が必要なリスクの場合に表示されます。リスクの除去を選択すると、結果ダイアログボックスに戻ります。再起動も必要な場合には、ダイアログボックスのリスクの行の情報によって、再起動が必要ことが示されます。</li> <li>■ 再起動が必要 再起動が必要なリスクの場合に表示されます。</li> <li>■ リスクの削除と再起動が必要 プロセスの終了が必要なリスクと、再起動が必要な別のリスクに対して表示されます。</li> </ul>

再起動が必要な場合には、コンピュータを再起動するまで除去または修復が完了しません。

リスクに対する処理は必要だが、今すぐにはそれを実行したくない場合もあります。

リスクは、次の手順で後から除去または修復することができます。

- リスクのログを開き、リスクを右クリックしてから処理を実行できます。
- スキャンを実行してリスクを検出し、結果ダイアログボックスを再度開くことができます。

ダイアログボックスでリスクを右クリックし、処理を選択して実行することもできます。実行できる処理は、スキャンで検出されたリスクの種類ごとに設定した処理によって異なります。

p.16の「[感染ファイルへの対応](#)」を参照してください。

## ウイルスとセキュリティリスクに対する処理の設定

ウイルスまたはセキュリティリスクを検出したときに Symantec Endpoint Protection クライアントで実行する処理を設定できます。設定できるのは、第1の処理と、それが失敗した場合に実行する第2の処理です。

---

**メモ:** 管理者がコンピュータを管理しており、これらのオプションに南京錠のアイコンが表示される場合には、管理者によってロックされているためこれらのオプションを変更することはできません。

---

どの種類のスキャンでも、処理の設定方法は同じです。スキャンごとに固有の処理の設定があります。スキャンごとに異なる処理の設定が可能です。

このオプションについて詳しくは[ヘルプ]を参照してください。

**ウイルスとセキュリティリスクに対する処理を設定するには**

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [ウイルス対策とスパイウェア対策]の隣にある[オプションの設定]をクリックします。
- 3 [ファイルシステム **Auto-Protect**]タブで、[処理]をクリックします。
- 4 [スキャン処理]ダイアログボックスのツリーで、ウイルスまたはセキュリティリスクの種類を選択します。

デフォルトでは、セキュリティリスクの各サブカテゴリには[セキュリティリスク]カテゴリ全体に設定されている処理を使うように自動的に設定されています。

- 5 あるカテゴリ、または特定インスタンスのカテゴリで異なる処理を使うように設定するには、[セキュリティリスクに設定した処理を上書きする]にチェックマークを付けてから、そのカテゴリ専用の処理を設定します。

## 6 第1と第2の処理を次のオプションから選択します。

リスクをクリーニング 感染ファイルからウイルスを除去します。これは、ウイルスに対する第1の処理のデフォルト設定です。

**メモ:**この処理は、ウイルスに対する第1の処理としてのみ利用可能です。セキュリティリスクには適用されません。

この設定は、必ずウイルスに対する第1の処理とする必要があります。ファイルから正常にウイルスがクリーニングされた場合には、他の処理を実行する必要はありません。コンピュータからはウイルスが除去され、そのウイルスがコンピュータの他の領域に伝染する危険性はなくなります。

ファイルをクリーニングするとき、クライアントは感染ファイル、ブートセクタ、パーティションテーブルからウイルスを除去します。これにより、ウイルスは伝染する能力がなくなります。クライアントは通常、コンピュータが損傷を受ける前にウイルスを見つけてクリーニングできます。デフォルトでは、クライアントはファイルのバックアップを作成します。

ただし、場合によってはクリーニングの済んだファイルが利用不可能なこともあります。ウイルスによる損傷が大きすぎるためです。

クリーニングできない感染ファイルもあります。

リスクを検疫 感染ファイルを元の場所から検疫に移動します。検疫に置かれた感染ファイルからウイルスが伝染することはありません。

ウイルスの場合は、感染ファイルを元の場所から検疫に移動します。これは、ウイルスに対する第2の処理のデフォルト設定です。

セキュリティリスクの場合は、感染ファイルを元の場所から検疫に移動し、副作用がある場合にはその除去または修復を試みます。これは、セキュリティリスクに対する第1の処理のデフォルト設定です。

検疫には、実行されたすべての処理の記録があります。クライアントがリスクを除去する前の状態にコンピュータを戻すことができます。

リスクを削除

感染ファイルをコンピュータのハードディスクドライブから削除します。ファイルを削除できない場合は、クライアントが実行した処理についての情報が[通知]ダイアログボックスに表示されます。同じ情報がイベントログにも表示されます。

この処理は、ウイルスまたはセキュリティリスクの影響を受けていないバックアップコピーに置き換えることのできるファイルに対してのみ使うようにしてください。クライアントがリスクを削除するとき、その削除は完全です。感染ファイルをごみ箱から回復することはできません。

**メモ:** セキュリティリスクに対する処理を設定するとき、この処理は慎重に行ってください。場合によっては、セキュリティリスクを削除するとアプリケーションの機能が失われることがあります。

放置する (ログのみ)

ファイルをそのまま放置します。

ウイルスに対してこの処理を使った場合には、ウイルスが感染ファイルに残ります。ウイルスはコンピュータの他の部分に伝染する可能性があります。感染ファイルの記録を残すために、リスク履歴にエントリが記録されます。

[放置する(ログのみ)]は、マクロウイルスでも非マクロウイルスでも第 2 の処理として使うことができます。

この処理は、定時スキャンのように大規模な自動化スキャンを実行するときには選択しないでください。スキャン結果を表示し、後で追加の処理を実行しようと予定している場合には、この処理を使うと便利です。このときの追加の処理には、ファイルを検疫に移動することなどが考えられます。

セキュリティリスクの場合には、この処理によって感染ファイルがそのまま放置され、リスクの記録を残すためにリスク履歴にエントリが記録されます。クライアントによるセキュリティリスクの処理方法を手動で制御する場合には、このオプションを使います。これは、セキュリティリスクに対する第 2 の処理のデフォルト設定です。

対応方法を説明するカスタムのメッセージを、管理者が送信する場合があります。

p.72 の「ウイルスに対する第 2 の処理を割り当てるためのヒント」を参照してください。

p.73 の「セキュリティリスクに対する第 2 の処理を割り当てるためのヒント」を参照してください。

- 7 特定の処理を設定したいカテゴリごとに、ステップ 1 と 6 を繰り返し、[OK]をクリックします。

- 8 セキュリティリスクのカテゴリを選択した場合には、そのセキュリティリスクカテゴリの1つ以上の特定インスタンスに対してカスタム処理を選択することができます。セキュリティリスクをスキャンから除外することもできます。たとえば、業務で使う必要があるアドウェアは除外すると便利です。
- 9 [OK]をクリックします。

## ウイルスに対する第2の処理を割り当てるためのヒント

ウイルスに対する第2の処理を選択するときには、次の点を考慮してください。

**コンピュータ上でのファイルの管理方法** バックアップを作成せずに重要なファイルをコンピュータに保存している場合には、[リスクを削除]のような処理は使わないでください。この方法ではウイルスを削除できますが、重要なデータも失う可能性があります。

もう一つ考慮すべき点は、システムファイルです。ウイルスは一般的に、実行可能ファイルを攻撃します。どのファイルが感染したかをチェックするために、[放置する(ログのみ)]または[リスクを検疫]の処理を使うことができます。たとえば、**Command.com**を攻撃するウイルスがあります。クライアントがこのウイルスによる感染をクリーニングできなかった場合には、ファイルを復元できない可能性があります。このファイルは、システムにとって重要です。ファイルにアクセスできるように、放置の処理を使う方法があります。

**コンピュータに感染したウイルスの種類** ウイルスの種類が異なれば、感染の対象になるコンピュータ領域も異なります。ブートウイルスはブートセクタ、パーティションテーブル、マスターブートレコード、時にはメモリに感染します。ブートウイルスが複合感染型である場合には、実行可能ファイルにも感染する可能性があるため、感染はファイル感染ウイルスと同じように扱うことができます。ファイル感染ウイルスは通常、**.exe**、**.com**、**.dll**の拡張子を持つ実行可能ファイルに感染します。マクロウイルスは文書ファイルと、その文書に関連付けられているマクロに感染します。回復する必要があるファイルの種類に基づいて処理を選択してください。

**コンピュータに対して実行するスキャンの種類** すべてのスキャンは、ユーザーの同意なしに自動的に処理を実行します。スキャンの前に処理を変更しなければ、デフォルト処理が使われます。その結果、デフォルトの第2の処理はウイルスアウトブレイクの状況を制御できるように設計されています。定時スキャンや**Auto-Protect**スキャンのように自動的に実行されるスキャンの場合には、永久的な効果がある第2の処理を割り当てないでください。たとえば、ファイルが感染していることがあらかじめわかっている場合には、オンデマンドスキャンを実行するようにします。[リスクを削除]や[リスクをクリーニング]の処理はこのオンデマンドスキャンに限定するようにします。

## セキュリティリスクに対する第 2 の処理を割り当てるためのヒント

セキュリティリスクに対する第 2 の処理を選択するときには、ファイルに対して必要な制御レベルを検討します。バックアップを作成せずに重要なファイルをコンピュータに保存している場合には、[リスクを削除]処理は使わないでください。たとえこの方法でセキュリティリスクを削除できるとしても、コンピュータ上の別のアプリケーションの動作を停止する危険性があります。代わりに、必要な場合にはクライアントが行う変更を元に戻せるように、[リスクを検疫]処理を使うようにします。

## リスクの影響評価について

シマンテック社では、セキュリティリスクを評価してそのコンピュータに対する影響の大きさを判定します。

次の各要因が、低、中、高で評価されます。

- プライバシーへの影響
- パフォーマンスへの影響
- ステルス
- 除去の難易度

「低」と評価された要因の影響は最小限です。「中」と評価された要因の影響は中程度です。「高」と評価された要因は、その領域に大きい影響を及ぼします。未評価のセキュリティリスクにはデフォルトの評価が使われます。セキュリティリスクは評価されたが特定の要因がそのリスクに適用されない場合には、評価なしが使われます。

既知のセキュリティリスクに対して集中例外を設定しているときには、これらの評価が[セキュリティリスク例外]ダイアログボックスに表示されます。これらの評価を利用して、どのセキュリティリスクをスキャンから除外しコンピュータ上に残すかを判断できます。

表 4-6 は、評価の要因と、「高」と評価されたときの意味をまとめたものです。

表 4-6 リスクの影響要因

評価要因	説明
プライバシーの影響	コンピュータ上にセキュリティリスクが存在するために失われるプライバシーのレベルを測定します。  この評価が高い場合は、個人情報などの機密情報が盗用される可能性があることを示します。
パフォーマンスの影響	セキュリティリスクによってコンピュータのパフォーマンスが劣化する程度を測定します。  この評価が高い場合は、パフォーマンスが大幅に劣化することを示します。

評価要因	説明
ステルス評価	セキュリティリスクがコンピュータ上に存在するかどうかを判断できる容易さを測定します。 この評価が高い場合は、セキュリティリスクがその存在を隠そうとしていることを示します。
削除の評価	セキュリティリスクをコンピュータから除去する難易度を測定します。 この評価が高い場合は、リスクの除去が難しいことを示します。
全体評価	全体評価は、他の要因の平均です。
依存プログラム	この評価は、他のアプリケーションの正常な動作がこのセキュリティリスクの存在に依存しているかどうかを示します。

## ウイルスとセキュリティリスクに対する通知の設定

デフォルトでは、スキャンでウイルスまたはセキュリティリスクが見つかる通知が表示されます。また、スキャンソフトウェアがサービスを終了またはプロセスを停止する必要がある場合にも、デフォルトで通知されます。スキャンソフトウェアは、ウイルスまたはセキュリティリスクの影響を除去または修復する必要があることもあります。

スキャンには次の通知を設定できます。

検出オプション	コンピュータでウイルスまたはセキュリティリスクが見つかったときに表示するメッセージを作成します。  ファイルシステム <b>Auto-Protect</b> を設定するときには、ダイアログボックスを表示する追加のオプションを選択できます。このダイアログボックスには、 <b>Auto-Protect</b> がコンピュータ上でリスクを見つけたときの結果が表示されます。
修復オプション	ウイルスまたはセキュリティリスクが見つかったときに通知するかどうかを設定します。また、リスクを除去または修復するためにクライアントがプロセスを終了、またはサービスを停止する必要があることも通知できます。

コンピュータで表示したい検出メッセージを作成できます。メッセージを作成するには、直接メッセージフィールドに入力します。メッセージフィールドを右クリックすると、メッセージに含める変数を選択できます。

表 4-7 は、通知メッセージで利用可能な変数フィールドを示したものです。

表 4-7                   メッセージの変数フィールド

フィールド	説明
セキュリティリスク名	見つかったウイルスまたはセキュリティリスクの名前。
適用した処理	ウイルスまたはセキュリティリスクを検出したときにクライアントが実行した処理。この処理は、設定された第 1 または第 2 の処理になります。
状態	ファイルの状態を「感染」「感染していません」「削除」のいずれかで表します。  このメッセージ変数は、デフォルトでは使用されません。情報を表示するには、この変数を手動でメッセージに追加してください。
ファイル名	ウイルスまたはセキュリティリスクに感染しているファイルの名前。
パスとファイル名	ウイルスまたはセキュリティリスクに感染しているファイルの絶対パスと名前。
場所	ウイルスまたはセキュリティリスクが見つかったコンピュータのドライブ。
コンピュータ	ウイルスまたはセキュリティリスクが見つかったコンピュータの名前。
ユーザー	ウイルスまたはセキュリティリスクが発生したときに、ログオンしていたユーザーの名前。
イベント	「リスクが見つかりました」などのイベントの種類。
ログ記録	ウイルスまたはセキュリティリスクを検出したスキャンの種類。
検出日	ウイルスまたはセキュリティリスクが見つかった日付。
ストレージ名	影響を受けるアプリケーションの領域(たとえば、ファイルシステム <b>Auto-Protect</b> や <b>Lotus Notes Auto-Protect</b> )。
処理の説明	ウイルスまたはセキュリティリスクの検出に対応して実行された処理の詳細な説明。

通知は、ユーザー定義スキャンと **Auto-Protect** に設定できます。通知の設定には、修復オプションが含まれます。修復オプションは、スキャンとファイルシステム **Auto-Protect** でのみ利用可能です。

この手順で使うオプションについて詳しくは[ヘルプ]を参照してください。

#### ウイルスとセキュリティリスクに対する通知を設定するには

1 次の処理のいずれかを実行します。

- 新しいスキャンの場合は、[新しいスキャンの作成 - スキャンオプション]ダイアログボックスで[通知]をクリックします。
- 既存のスキャンの場合は、[スキャンオプション]タブで[通知]をクリックします。

- **Auto-Protect** の場合は、[ウイルス対策とスパイウェア対策の設定]ダイアログボックスのいずれかの[**Auto-Protect**]タブで、[通知]をクリックします。
- 2 [スキャン通知オプション]ダイアログボックスの[検出オプション]で、スキャンがウイルスまたはセキュリティリスクを検出したときの通知オプションを選択できます。このオプションは、スキャンでウイルスまたはセキュリティリスクが見つかったときにコンピュータにメッセージを表示したい場合に選択します。
- 3 メッセージボックスで、次の一部またはすべての操作を行って必要なメッセージを作成します。
  - クリックしてテキストを入力、または編集します。
  - 右クリックして[フィールドを挿入]を選択してから、挿入する変数フィールドを選択します。
  - 右クリックして[切り取り]、[コピー]、[貼り付け]、[消去]、[元に戻す]のいずれかを選択します。
- 4 **Auto-Protect** 設定の場合は、[**Auto-Protect** 結果ウィンドウを表示する]にチェックマークを付けるか、チェックマークをはずします。

このパラメータを使うと、ファイルシステム **Auto-Protect** でウイルスまたはセキュリティリスクが見つかったときに、結果を示すダイアログボックスを表示するか抑止するかを選択できます。
- 5 [修復オプション]で、スキャンまたはファイルシステム **Auto-Protect** に対して設定するオプションにチェックマークを付けます。利用可能なオプションは次のとおりです。

プロセスを自動的に終了する	ウイルスやセキュリティリスクを除去または修復するためにプロセスを終了する必要がある場合にプロセスを自動的に終了するようにスキャンを設定します。プロセスを終了する前にデータ保存を促すメッセージは表示されません。
サービスを自動的に停止する	ウイルスやセキュリティリスクを除去または修復するためにサービスを停止する必要がある場合にサービスを自動的に停止するようにスキャンを設定します。サービスを停止する前にデータ保存を促すメッセージは表示されません。
- 6 [OK]をクリックします。

## スキャン対象からの項目の除外について

例外はスキャンから除外したい既知のセキュリティリスク、ファイル、拡張子、プロセスです。コンピュータをスキャンして特定のファイルが安全であることがわかっている場合、そ

れらを除外できます。場合によっては、例外はスキャン時間を減らしてシステムパフォーマンスを高めることができます。通常は、例外を作成する必要はありません。

集中管理下クライアントの場合は、管理者がスキャンに対する例外を作成していることがあります。管理者定義の例外と競合するような例外を作成した場合には、管理者定義の例外が優先されます。

表 4-8 例外の種類

種類	説明
セキュリティリスク例外	<p>次のセキュリティリスクを除外できます。</p> <ul style="list-style-type: none"><li>■ 既知のセキュリティリスク</li><li>■ ファイル</li><li>■ フォルダ</li><li>■ 拡張子</li></ul> <p>管理者はスキャンからこれらの項目を除外できないようにクライアントを設定することがあります。</p> <p>p.77 の「スキャンからの項目の除外」を参照してください。</p>
TruScan プロアクティブ脅威スキャン例外	<p><b>TruScan</b> プロアクティブ脅威スキャンからプロセスを除外できます。 <b>TruScan</b> プロアクティブ脅威スキャンが検出する既知のプロセスのために適用する異なる処理を指定できます。プロセスの検出を強制できません。</p> <p>管理者はスキャンからプロセスを除外できないようにクライアントを設定することがあります。</p> <p>p.96 の「<b>TruScan</b> プロアクティブ脅威スキャンからのプロセスの除外」を参照してください。</p>
改変対策例外	<p>改変対策からファイルを除外できます。</p> <p>改変対策はシマンテック製品以外のプロセスがシマンテック製品のプロセスに影響することを防ぎます。</p> <p>p.35 の「改変対策について」を参照してください。</p> <p>p.77 の「スキャンからの項目の除外」を参照してください。</p>

## スキャンからの項目の除外

[設定の変更] ページから例外を作成できます。ユーザー定義スキャンを作成または修正するとき、または **Auto-Protect** 設定を修正するときに例外を設定することもできます。

p.76 の「スキャン対象からの項目の除外について」を参照してください。

例外はすべてのスキャンに渡って適用されます。特定のスキャンを作成または編集するときに例外を設定した場合にも、その例外はすべてのスキャンに適用されます。

---

**メモ:** Windows Server 2008 の Server Core のインストールでは、ダイアログボックスの表示が以下の手順で説明するものと異なることがあります。

---

各ダイアログボックスのオプションについて詳しくは[ヘルプ]をクリックしてください。

#### スキャンからセキュリティリスクを除外するには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [集中例外]の隣にある[オプションの設定]をクリックします。
- 3 [集中例外]ダイアログボックスの[ユーザー定義の例外]タブで、[追加]、[セキュリティリスク例外]、[既知のリスク]の順に選択します。
- 4 [既知のセキュリティリスク例外の追加]ダイアログボックスで、スキャンから除外したいセキュリティリスクにチェックマークを付けます。
- 5 セキュリティリスクが検出されて無視されたときにイベントのログを記録する場合には、[セキュリティリスクの検出時にログに記録する]にチェックマークを付けます。
- 6 [OK]をクリックします。
- 7 [集中例外]ダイアログボックスで、[閉じる]をクリックします。

#### スキャンからファイルまたはフォルダを除外するには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [集中例外]の隣にある[オプションの設定]をクリックします。
- 3 [集中例外]ダイアログボックスの[ユーザー定義の例外]タブで、[追加]、[セキュリティリスク例外]の順に選択します。
- 4 次のいずれかのタスクを行います。
  - [ファイル]をクリックします。[セキュリティリスクファイル例外の追加]ダイアログボックスで、除外したいファイルを選択してから、[追加]をクリックします。
  - [フォルダ]をクリックします。[セキュリティリスクのフォルダ例外の追加]ダイアログボックスでフォルダを選択し、[サブフォルダを含める]にチェックマークを付けるかチェックマークをはずしてから、[追加]をクリックします。
- 5 [集中例外]ダイアログボックスで、[閉じる]をクリックします。

## 検疫ファイルの処理について

クライアントは、最新のウイルス定義セットでも除去できない未知のウイルスを検出することがあります。また、ファイルに感染の疑いがあってもスキャンでは感染が検出されない場

合もあります。検疫は、コンピュータ上の感染している可能性のあるファイルを安全に隔離します。検疫されたウイルスは、コンピュータ上でもネットワークの他のコンピュータにも伝染しません。

## 検疫にある感染ファイルについて

ユーザーは検疫にある感染ファイルを表示できます。

ファイルについて次のような情報を表示できます。

- リスク
- ファイル名
- 種類
- 元の場所
- 状態
- 日付

---

**メモ:** クライアントが動作しているオペレーティングシステムの言語によっては、リスク名に使われている文字の一部を解釈できない場合があります。オペレーティングシステムが解釈できない文字は、通知で疑問符として表示されます。たとえば、Unicode のリスク名には 2 バイト文字が含まれることがあります。英語版のオペレーティングシステムでクライアントが動作しているコンピュータでは、このような文字が疑問符として表示されます。

---

感染したファイルをクライアントが検疫に移動すると、そのリスクは自己をコピーして他のファイルに感染することはできません。この処理は、マクロウイルスと非マクロウイルスの感染の両方で推奨される第 2 の処理です。

ただし、検疫ではリスクのクリーニングは行われません。クライアントによりリスクがクリーニングされるかファイルが削除されるまで、リスクはコンピュータ上に残ります。ウイルスとマクロウイルスは検疫できます。ブートウイルスは検疫できません。通常、ブートウイルスはコンピュータのブートセクタまたはパーティションテーブルに存在するため、検疫に移動できません。

感染ファイルのプロパティを表示することもできます。

p.81 の「[検疫にあるファイルとファイルの詳細の表示](#)」を参照してください。

## 検疫にある感染ファイルの扱い方について

ファイルを検疫に移動した後には、次の操作を行うことができます。

- 選択したファイルを元の場所に復元します。
- 選択したファイルを永久に削除します。

- 更新されたウイルス定義の受信後にファイルを再スキャンします。
- 検疫の内容を、カンマ区切り(\*.csv)ファイルまたは Access データベース(\*.mdb)ファイルにエクスポートします。
- ファイルを検疫に手動で追加します。検疫に移動するファイルの場所を参照して選択できます。
- シマンテックセキュリティレスポンスにファイルを提出します。画面のウィザードの指示に従って、選択したファイルを分析するために送信します。

p.80 の「[検疫の管理](#)」を参照してください。

## セキュリティリスクに感染したファイルの扱い方について

セキュリティリスクが原因で検疫したファイルは、検疫に置いたままにすることも削除することもできます。これらのファイルは、コンピュータのアプリケーションが機能を失っていないことが確認できるまでは検疫に置いたままにしてください。

セキュリティリスクに関係するファイルを削除すると、コンピュータ上のアプリケーションが正常に機能しなくなることがあります。そのアプリケーションは、削除したファイルに依存していた可能性があります。検疫は、可逆的であるという点で安全なオプションです。依存関係にあるプログラムファイルを検疫した後でコンピュータ上のアプリケーションが機能性を失った場合には、そのファイルを元に戻すことができます。

---

**メモ:**アプリケーションが正常に動作した後であれば、ディスク領域を節約するためにファイルを削除できます。

---

## 検疫の管理

ファイルは次のいずれかの場合に検疫に置かれます。

- **Auto-Protect** またはスキャン中に検出された感染項目を検疫に移動するようにクライアントが設定されている。
- 手動でファイルを選択し、検疫に追加する。

**Auto-Protect** とすべてのスキャンタイプのデフォルトオプションでは、検出時に感染ファイルからウイルスをクリーニングします。スキャンソフトウェアは、クリーニングできないファイルを検疫に置きます。セキュリティリスクの場合は、デフォルトのオプションとして感染ファイルを検疫に置き、セキュリティリスクの副作用を修復します。

p.81 の「[検疫にあるファイルのウイルス再スキャン](#)」を参照してください。

p.82 の「[バックアップ項目の消去](#)」を参照してください。

p.82 の「[検疫からのファイルの削除](#)」を参照してください。

p.84の「[感染の可能性があるファイルを分析のためにシマンテックセキュリティレスポンスに提出](#)」を参照してください。

ファイルを手動で検疫に追加するには

- 1 クライアントのサイドバーで、[検疫の表示]をクリックします。
- 2 [追加]をクリックします。
- 3 検疫に追加するファイルを選択して、[追加]をクリックします。

## 検疫にあるファイルとファイルの詳細の表示

ユーザーは検疫に置かれているファイルを表示できます。ファイルの詳細を表示できません。この詳細には、ウイルス名と、ファイルが見つかったコンピュータの名前などが含まれます。

検疫にあるファイルとファイルの詳細を表示するには

- 1 クライアントのサイドバーで、[検疫の表示]をクリックします。
- 2 表示するファイルを右クリックして[プロパティ]をクリックします。

## 検疫にあるファイルのウイルス再スキャン

検疫にファイルが入っている場合には、定義ファイルを更新します。定義ファイルを更新すると、検疫にあるファイルがスキャン、クリーニング、または自動的に復元されます。修復ウィザードが表示された場合には、検疫にあるファイルを再スキャンできます。

p.81の「[手動によるファイルの再スキャン](#)」を参照してください。

検疫にあるファイルを再スキャンした後でもまだウイルスを除去できない場合には、感染ファイルを分析のためにシマンテックセキュリティレスポンスに提出できます。

p.84の「[感染の可能性があるファイルを分析のためにシマンテックセキュリティレスポンスに提出](#)」を参照してください。

修復ウィザードを使って検疫にあるファイルを再スキャンするには

- 1 修復ウィザードが表示されたら、[はい]をクリックします。
- 2 [次へ]をクリックします。
- 3 画面の指示に従って、検疫にあるファイルを再スキャンします。

## 手動によるファイルの再スキャン

検疫にあるファイルは、手動で再度ウイルススキャンできますが、セキュリティリスクはスキャンされません。

p.81の「[検疫にあるファイルのウイルス再スキャン](#)」を参照してください。

検疫にあるファイルを手動で再度ウイルススキャンするには

- 1 定義ファイルを更新します。
- 2 クライアントのサイドバーで、[検疫の表示]をクリックします。
- 3 ファイルを選択して[すべてを再スキャン]をクリックします。

## 修復したファイルが元の場所に戻らない場合

未感染のファイルでも、戻る場所がなくなることがあります。たとえば、感染した添付ファイルが電子メールからはく離されて検疫に置かれた場合などです。このようなファイルは、解放して場所を指定する必要があります。

クリーニング済みファイルを検疫から解放するには

- 1 クライアントのサイドバーで、[検疫の表示]をクリックします。
- 2 修復済みのファイルを右クリックして[復元]をクリックします。
- 3 クリーニング済みファイルの場所を指定します。

## バックアップ項目の消去

デフォルトでは、クライアントは感染した項目のクリーニングまたは修復を試みる前に、その項目のバックアップコピーを作成します。クライアントがウイルスを正常にクリーニングしてもバックアップファイルは感染したままなので、クリーニング後に手動で削除する必要があります。ファイルが自動的に削除されるまでの時間を設定することもできます。

p.83 の「[検疫からのファイルの自動削除](#)」を参照してください。

バックアップ項目を手動で消去するには

- 1 クライアントのサイドバーで、[検疫の表示]をクリックします。
- 2 1つ以上のバックアップファイルを選択します。
- 3 [削除]をクリックします。

## 検疫からのファイルの削除

不要になったファイルは検疫から手動で削除できます。ファイルが自動的に削除されるまでの時間を設定することもできます。

---

**メモ:** 項目を検疫に残すことのできる最大日数を、管理者が指定することがあります。その制限日数を超えると項目は自動的に検疫から削除されます。

---

p.83 の「[検疫からのファイルの自動削除](#)」を参照してください。

### 検疫から手動でファイルを削除するには

- 1 クライアントのサイドバーで、[検疫の表示]をクリックします。
- 2 1つ以上のファイルを選択します。
- 3 [削除]をクリックします。

## 検疫からのファイルの自動削除

指定された期間が経過すると自動的に検疫から項目を削除するように設定することができます。また、項目を格納するフォルダが一定のサイズに達したときに項目を削除する設定も可能です。このように設定すると、手動で削除するのを忘れてファイルがたまることなくなくなります。

p.82 の「[検疫からのファイルの削除](#)」を参照してください。

### ファイルを自動的に削除するには

- 1 クライアントのサイドバーで、[検疫の表示]をクリックします。
- 2 [ページオプション]をクリックします。
- 3 [ページオプション]ダイアログボックスで、次のいずれかのタブを選択します。
  - 検疫項目
  - バックアップ項目
  - 修正項目
- 4 設定した時間が経過するとクライアントがファイルを削除する機能は、[格納時間の限度]にチェックマークを付けるかはずして有効または無効にします。
- 5 [格納時間の限度]チェックボックスにチェックマークを付けた場合は、時間を入力するか矢印をクリックして指定します。
- 6 ドロップダウンリストから時間の単位を選択します。デフォルトは 30 日です。
- 7 [合計フォルダサイズの限度]チェックボックスにチェックマークを付けた場合は、許可する最大フォルダサイズを MB 単位で入力します。デフォルトは 50 MB です。

両方にチェックマークを付けた場合には、設定した時間が経過したすべてのファイルが先に削除されます。フォルダサイズが設定した上限をまだ超えている場合は、古い順に 1 つずつファイルが削除されます。ファイルサイズが制限範囲を下回るまで、クライアントは古いファイルから削除します。
- 8 他のタブについても、ステップ 4 から 7 を繰り返します。
- 9 [OK]をクリックします。

## 感染の可能性があるファイルを分析のためにシマンテックセキュリティレスポンスに提出

クライアントがファイルからウイルスをクリーニングできないことがあります。または、ファイルに感染の疑いがあってもクライアントが感染を検出しないことがあります。シマンテックセキュリティレスポンスにファイルを提出すると、ファイルを分析して感染していないことを確認できます。サンプルを提出するにはインターネット接続が必要です。

---

**メモ:** 管理者が提出を無効にしている場合は、シマンテックセキュリティレスポンスのオプションを利用できません。

---

p.83 の「[検疫からのファイルの自動削除](#)」を参照してください。

p.84 の「[スキャン検出についての情報のシマンテックセキュリティレスポンスへの提出](#)」を参照してください。

検疫からシマンテックセキュリティレスポンスにファイルを提出するには

- 1 クライアントのサイドバーで、[検疫の表示]をクリックします。
- 2 検疫項目のリストでファイルを選択します。
- 3 [提出]をクリックします。
- 4 ウィザード画面の指示に従って必要な情報を収集し、分析用にファイルを提出します。

## スキャン検出についての情報のシマンテックセキュリティレスポンスへの提出

Auto-Protect またはスキャン検出率に関する情報を自動的にシマンテックセキュリティレスポンスに提出するように指定することができます。検出率に関する情報は、シマンテック社がウイルス定義の更新を改善するうえで役立つ可能性があります。検出率は、お客様によって最も検出されたウイルスとセキュリティリスクを示します。シマンテックセキュリティレスポンスは、検出されなかったシグネチャを削除し、要請のあったお客様にはセグメント化したシグネチャリストを提供します。セグメント化したリストはスキャンパフォーマンスを高めます。

検出率の提出は、デフォルトで有効になっています。

---

**メモ:** 提出の設定を管理者がロックしている場合もあります。

---

検疫にある項目をシマンテック社に提出することもできます。

p.84 の「感染の可能性があるファイルを分析のためにシマンテックセキュリティレスポンスに提出」を参照してください。

スキャン検出についての情報をシマンテックセキュリティレスポンスに提出するには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [ウイルス対策とスパイウェア対策]の隣にある[オプションの設定]をクリックします。
- 3 [提出]タブで、[ウイルス対策とセキュリティリスクスキャン]の検出項目を自動的に提出する]にチェックマークを付けます。
- 4 [OK]をクリックします。

## クライアントと Windows セキュリティセンターについて

Windows XP Service Pack 2 で Windows セキュリティセンター (WSC) を使ってセキュリティの状態を監視する場合、WSC で Symantec Endpoint Protection の状態を確認できます。

WSC での保護の状態報告を表 4-9 に示します。

表 4-9 WSC の保護の状態報告

シマンテック製品の状態	保護の状態
Symantec Endpoint Protection がインストールされていない	見つかりません(赤)
Symantec Endpoint Protection が保護状態でインストールされている	オン(緑)
Symantec Endpoint Protection がインストールされているが、ウイルスとセキュリティリスクの定義が最新ではない	最新の状態ではありません(赤)
Symantec Endpoint Protection がインストールされているが、ファイルシステム Auto-Protect が有効ではない	オフ(赤)
Symantec Endpoint Protection がインストールされているが、ファイルシステム Auto-Protect が有効ではなく、ウイルスとセキュリティリスクの定義が最新ではない	オフ(赤)
Symantec Endpoint Protection がインストールされているが、Rtvscan が手動で無効にされている	オフ(赤)

WSC での Symantec Endpoint Protection ファイアウォールの状態報告を表 4-10 に示します。

表 4-10 WSC のファイアウォールの状態報告

シマンテック製品の状態	ファイアウォールの状態
シマンテック製ファイアウォールがインストールされていない	見つかりません(赤)
シマンテック製ファイアウォールがインストールされ有効である	オン(緑)
シマンテック製ファイアウォールがインストールされているが、有効ではない	オフ(赤)
シマンテック製ファイアウォールがインストールされていないか有効でないが、他社製ファイアウォールがインストールされ有効である	オン(緑)

**メモ:** Symantec Endpoint Protection では、Windows ファイアウォールはデフォルトで無効になります。

複数のファイアウォールが有効である場合、WSCは複数のファイアウォールがインストールされて有効であることを報告します。

# プロアクティブ脅威防止の管理

この章では以下の項目について説明しています。

- [TruScan プロアクティブ脅威スキャンについて](#)
- [TruScan プロアクティブ脅威スキャンを実行する頻度の設定](#)
- [TruScan プロアクティブ脅威検出の管理](#)
- [TruScan プロアクティブ脅威スキャン検出時の通知の設定](#)
- [シマンテックセキュリティレスポンスへの TruScan プロアクティブ脅威スキャンに関する情報の提出](#)
- [TruScan プロアクティブ脅威スキャンからのプロセスの除外](#)

## TruScan プロアクティブ脅威スキャンについて

TruScan プロアクティブ脅威防止には、ゼロデイ攻撃防止機能が用意されています。ゼロデイ攻撃防止は、未知の脅威や脆弱性から保護する機能です。プロアクティブ脅威スキャンでは、悪質な可能性のある動作を示すアクティブなプロセスがコンピュータにないかを診断します。未知の脅威を識別するシグネチャはないため、プロアクティブ脅威スキャンでは疑わしい動作にフラグを付けることによって潜在的なリスクを特定します。

プロアクティブ脅威スキャンは、デフォルトのスキャン設定が多くのユーザーに適しています。スキャン設定は、コンピュータに必要なヒューリスティック保護のレベルに基づいて変更できます。

プロアクティブ脅威スキャンの設定を変更する前に、次の点を確認してください。

- コンピュータに対する脅威が起きたときに通知が必要かどうか
- プロセスをスキャンする頻度と時期

■ プロアクティブ脅威スキャンに割り当てるコンピュータリソースの量

**メモ:** オプションを設定できるのは、管理者がプロアクティブ脅威スキャンの設定をロックしていない場合です。ロックされている設定には、南京錠アイコンのロックも含まれます。ロックされている設定のラベルはグレー表示されます。

p.91 の「[TruScan プロアクティブ脅威検出の管理](#)」を参照してください。

## TruScan プロアクティブ脅威スキャンで診断されるプロセスとアプリケーション

プロアクティブ脅威スキャンは、疑わしい動作を示す特定種類のプロセスまたはアプリケーションを診断します。スキャンは、トロイの木馬やワーム、キーロガーのように動作しているプロセスを検出します。この検出は、無効にもできます。

トロイの木馬、ワーム、キーロガーだけでなく、動作がアドウェアやスパイウェアに類似しているプロセスも検出されます。プロアクティブ脅威スキャンがこれらの種類の検出をどのように処理するかは設定できません。プロアクティブ脅威スキャンで検出されたアドウェアやスパイウェアをクライアントコンピュータで許可する場合には、ユーザーまたは管理者が集中例外を作成する必要があります。

p.96 の「[TruScan プロアクティブ脅威スキャンからのプロセスの除外](#)」を参照してください。

プロアクティブ脅威スキャンは、悪質な目的に利用される可能性のある既知の商用アプリケーションも検出します。シマンテック社は、これらの商用アプリケーションのリストを管理し、定期的に更新しています。このような商用アプリケーションの中には、ユーザーのキー操作を監視、記録したり、ユーザーのコンピュータをリモート制御したりするものもあります。これらが検出されたときに **Symantec Endpoint Protection** が行う処理を設定することができます。

[表 5-1](#) は、プロアクティブ脅威スキャンで検出されるプロセスです。

**表 5-1** TruScan プロアクティブ脅威スキャンによって検出されるプロセス

プロセスの種類	説明
トロイの木馬とワーム	トロイの木馬やワームの性質を示すプロセス。 プロアクティブ脅威スキャンはヒューリスティックを使ってトロイの木馬やワームと類似した動作を行うプロセスを検索します。これらのプロセスは脅威である場合と脅威ではない場合があります。
キーロガー	キーロガーの性質を示すプロセス。 プロアクティブ脅威スキャンは商用のキーロガーを検出し、さらにキーロガーの動作を示す未知のプロセスも検出します。

プロセスの種類	説明
商用アプリケーション	悪質な目的に利用される可能性のある既知の商用アプリケーション。 プロアクティブ脅威スキャンは、複数の種類の商用アプリケーションを検出します。処理を設定できる対象は、キーロガーとリモート制御プログラムの 2 種類です。
アドウェアとスパイウェア	アドウェアとスパイウェアの特性を示すプロセス。 プロアクティブ脅威スキャンはヒューリスティックを使ってアドウェアとスパイウェアに類似した動作を行う未知のプロセスを検出します。これらのプロセスにはリスクがある場合とない場合があります。

## TruScan プロアクティブ脅威スキャンの例外について

管理者が集中例外の設定をロックしていなければ、プロアクティブ脅威スキャンに対する例外を作成することができます。

管理者がプロアクティブ脅威スキャンに対して集中例外を作成する場合があります。管理者が作成する例外は修正できません。

p.96 の「[TruScan プロアクティブ脅威スキャンからのプロセスの除外](#)」を参照してください。

## TruScan プロアクティブ脅威スキャンの検出について

プロアクティブ脅威スキャンは、潜在的に悪質なプロセスを検出するとそれらをログ記録、検疫、または終了します。検出状況は、スキャン結果のダイアログボックス、プロアクティブ脅威防止のログ、または検疫リストを使って表示できます。

p.67 の「[スキャン結果または Auto-Protect の結果に対する操作](#)」を参照してください。

p.80 の「[検疫の管理](#)」を参照してください。

---

**メモ:** プロアクティブ脅威スキャンの設定は、シグネチャを使用して既知のリスクを検出するウイルススキャンとスパイウェアスキャンには影響しません。Symantec Endpoint Protection は、はじめに既知のリスクを検出します。

---

デフォルトでは、クライアントは次の処理を行います。

- 既知の商用アプリケーションの検出をログに記録
- トロイの木馬、ワーム、またはキーロガーのように動作しているプロセスの検出をログに記録
- トロイの木馬、ワーム、またはキーロガーのように動作し修復が必要なプロセスを検疫

プロアクティブ脅威スキャンは、検出対象を検査するとそのプロセスによる副作用を処理します。コンテンツアップデートをコンピュータにダウンロードした後で検出結果を再スキャンすると、クライアントがプロセスをコンピュータに復元することがあります。クライアントがプロセスを復元するのは、そのプロセスがもはや悪質でないと判断された場合です。クライアントは、プロセスのすべての副作用の復元も行います。ただし、クライアントはプロセスの自動再起動は行いません。

商用のキーロガーまたはリモート制御アプリケーションの検出に対しては、ユーザーと管理者が異なる処理を指定することができます。たとえば、商用キーロガーアプリケーションの検出を無視することもできます。クライアントがアプリケーションを無視すると、そのアプリケーションは許可され、検出がログに記録されません。

トロイの木馬、ワーム、キーロガーの検出に対しては、検出時にクライアントが常に使う特定の処理を指定することができます。

## 誤認に対する処理について

TruScan プロアクティブ脅威スキャンで、誤認が検出されることがあります。プロアクティブ脅威スキャンは、既知のウイルスやセキュリティリスクではなく、動作の疑わしいアプリケーションやプロセスを検索します。その性質上、このスキャンを行うと、検出する必要がない項目にも通常フラグが付けられます。

プロアクティブ脅威スキャンで検出されたプロセスを、ユーザーが問題ないと判断した場合には、それ以降のスキャンでそのプロセスにフラグが付けられないように例外を作成することができます。ユーザー定義の例外と管理者定義の例外が競合する場合は、管理者定義の例外が優先されます。

p.96 の「[TruScan プロアクティブ脅威スキャンからのプロセスの除外](#)」を参照してください。

誤認検出を最小限にするために、プロアクティブ脅威スキャンのシマンテック社のコンテンツが最新であることを確認してください。バージョンは、状態ページのプロアクティブ脅威防止に表示されます。最新のコンテンツは、**LiveUpdate** を実行してダウンロードできます。

---

**メモ:** 管理者が自動更新をスケジュール設定している場合があります。

---

トロイの木馬、ワーム、キーロガーの検出をユーザー自身で管理する場合には、プロアクティブ脅威スキャンの感度を変更できます。ただし、感度の変更によって変わるのは検出の総数のみであるため、誤認の数は変わらないことがあります。

p.91 の「[TruScan プロアクティブ脅威検出の管理](#)」を参照してください。

# TruScan プロアクティブ脅威スキャンを実行する頻度の設定

プロアクティブ脅威スキャンを実行する頻度を設定できます。

---

**メモ:** プロアクティブ脅威スキャンを実行する頻度を変更すると、コンピュータのパフォーマンスに影響することがあります。

---

この手順で使うオプションについて詳しくは、[ヘルプ]を参照してください。

**TruScan プロアクティブ脅威スキャンを実行する頻度を設定するには**

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [プロアクティブ脅威防止]の隣にある[オプションの設定]をクリックします。
- 3 [プロアクティブ脅威防止の設定]ダイアログボックスの[スキャン頻度]タブで、[カスタムのスキャン頻度]にチェックマークを付けます。
- 4 次のいずれか 1 つ以上の操作をします。
  - [スキャン間隔]の隣で、プロセススキャンの間隔を日数、時間、分で設定します。
  - 新しいプロセスが見つかったときにそのプロセスをスキャンする場合は、[今すぐ新しいプロセスをスキャンする]にチェックマークを付けます。
- 5 [OK]をクリックします。

## TruScan プロアクティブ脅威検出の管理

管理者が、プロアクティブ脅威検出をロックしている場合があります。設定のロックが解除されている場合、または管理外クライアントを実行している場合には、プロアクティブ脅威検出で検出されるプロセスの種類を設定できます。

p.94 の「[TruScan プロアクティブ脅威スキャンが検出するプロセスの種類](#)の指定」を参照してください。

---

**メモ:** トロイの木馬、ワーム、およびキーロガーの検出は、現在、Windows サーバーのオペレーティングシステムや 64 ビットの Windows XP Professional ではサポートされていません。またキーロガーの検出も Windows 7 ではサポートされません。サーバーオペレーティングシステムで動作しているクライアントでは、スキャンオプションは利用できません。コンピュータに適用されるポリシーで管理者がこれらのオプションを修正している場合には、オプションはチェックマークが付いた状態で、利用できません。

---

トロイの木馬、ワーム、キーロガーの検出が有効なときは、検出の管理方法を選択できます。デフォルトでは、プロアクティブ脅威スキャンはシマンテック社のデフォルトを使いま

す。つまり、検出に対する処理をクライアントが決定するということです。(ユーザーインターフェースで利用できないデフォルトは、シマンテック社のデフォルトを表すものではありません。利用できない設定は、ユーザーが手動で検出を管理するときに使うデフォルト設定を表しています。)

p.93の「トロイの木馬、ワーム、キーロガーの検出に対する処理と感度レベルの指定」を参照してください。

通常、検出の処理にはシマンテック社のデフォルト設定が最適です。しかし、コンピュータでスキャン結果を確認している場合には、処理と感度レベルを手動で設定すると便利があります。これらのパラメータを設定する場合には、シマンテック社のデフォルトオプションを無効にします。

誤認検出を最小限にするために、最初はシマンテック管理のデフォルトを使うことをお勧めします。一定期間でクライアントが検出する誤認の数を観察します。この数が少ない場合には、プロアクティブ脅威スキャンの設定を段階的に調整します。たとえば、トロイの木馬やワームの検出に対しては、感度のスライダーをデフォルトより少し高めに設定すると安全です。設定を変更してからプロアクティブ脅威スキャンを実行すると、変更前と比較できます。

---

**メモ:** 管理下クライアントの場合は通常、コンピュータに適したプロアクティブ脅威スキャンのオプションを管理者が設定します。

---

商用アプリケーションに対しては、プロアクティブ脅威スキャンで商用のキーロガーまたは商用のリモート制御プログラムが検出されたときに実行する処理の種類を指定できます。これらの設定は、トロイの木馬、ワーム、キーロガーに対する設定とは関係なく変更することができます。

p.92の「商用アプリケーションの検出に対する処理の設定」を参照してください。

## 商用アプリケーションの検出に対する処理の設定

プロアクティブ脅威スキャンで特定の種類の商用アプリケーションが検出されたときにクライアントが実行する処理を変更することができます。

この手順で使うオプションについて詳しくは、[ヘルプ]をクリックしてください。

商用アプリケーションの検出に対する処理を設定するには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [プロアクティブ脅威防止]の隣にある[オプションの設定]をクリックします。
- 3 [プロアクティブ脅威防止の設定]ダイアログボックスの[スキャンの詳細]タブの[商用アプリケーション]で、次のいずれかの操作をします。
  - 商用キーロガーの処理を[無視]、[ログ]、[終了]、[検疫]のいずれかに設定します。

- 商用リモート制御アプリケーションの処理を[無視]、[ログ]、[終了]、[検疫]のいずれかに設定します。

4 [OK]をクリックします。

## トロイの木馬、ワーム、キーロガーの検出に対する処理と感度レベルの指定

トロイの木馬、ワーム、キーロガーの検出をユーザー自身で管理する場合には、それらのプロセスが検出されたときに実行する処理を設定できます。その処理はプロアクティブ脅威スキャンが検出を行うときに常に使われます。たとえば、実行する処理をログのみに設定することができます。プロアクティブ脅威スキャンでプロセスを検出し、それが正しい認識であると分類される場合、クライアントはその検出をログに記録します。クライアントはプロセスを検疫しません。

トロイの木馬やワームの検出と、キーロガーの検出に対して異なる感度レベルを設定することもできます。感度レベルには、プロセスをスキャンするときのプロアクティブ脅威スキャンの感度を設定します。感度が高いほど、検出数も多くなります。この場合、検出結果の一部は誤認の可能性もあることに注意してください。感度の設定を変えても、プロアクティブ脅威スキャンで検出される誤認の割合は変わらず、検出の総数が変わるだけの場合もあります。検出の総数が変わるだけです。

コンピュータでプロアクティブ脅威スキャンの結果がわかるまでは、感度レベルを低く設定しておくようにします。感度レベルを低く設定したときにプロアクティブ脅威スキャンで何も検出されなければ、感度を高めます。

この手順で使うオプションについて詳しくは、[ヘルプ]を参照してください。

### トロイの木馬とワームに対する処理と感度レベルを設定するには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [プロアクティブ脅威防止]の隣にある[オプションの設定]をクリックします。
- 3 [プロアクティブ脅威防止の設定]ダイアログボックスの[スキャンの詳細]タブにある[トロイの木馬とワーム]で、[トロイの木馬とワームをスキャンする]にチェックマークが付いていることを確認してから、[シマンテック定義のデフォルト設定を使う]のチェックマークをはずします。
- 4 [感度]でスライダーを左右に動かして感度を高く、または低く設定します。
- 5 ドロップダウンリストで[ログ]、[終了]、[検疫]のいずれかをクリックします。
- 6 [OK]をクリックします。

### キーロガーに対する処理と感度レベルを設定するには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [プロアクティブ脅威防止]の隣にある[オプションの設定]をクリックします。

- 3 [プロアクティブ脅威防止の設定]ダイアログボックスの[スキャンの詳細]タブの[キーロガー]で、[キーロガーをスキャンする]にチェックマークが付いていることを確認してから、[シマンテック定義のデフォルト設定を使う]のチェックマークをはずします。
- 4 感度レベルとして、[低レベル]か[高レベル]をクリックします。
- 5 ドロップダウンリストで[ログ]、[終了]、[検疫]のいずれかをクリックします。
- 6 [OK]をクリックします。

## TruScan プロアクティブ脅威スキャンが検出するプロセスの種類の指定

プロアクティブ脅威スキャンでトロイの木馬、ワーム、キーロガーをスキャンするかどうかを設定することができます。これらの設定の一部を管理者がロックしている場合もあります。この手順で使うオプションについて詳しくは、[ヘルプ]を参照してください。

**TruScan プロアクティブ脅威スキャンが検出するプロセスの種類を指定するには**

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [プロアクティブ脅威防止]の隣にある[オプションの設定]をクリックします。
- 3 [[プロアクティブ脅威防止の設定]ダイアログボックスの[スキャンの詳細]タブにある[トロイの木馬とワーム]で、[トロイの木馬とワームをスキャンする]にチェックマークを付けるか、チェックマークをはずします。
- 4 [キーロガー]にある[キーロガーをスキャンする]にチェックマークを付けるか、チェックマークをはずします。
- 5 [OK]をクリックします。

## TruScan プロアクティブ脅威スキャン検出時の通知の設定

プロアクティブ脅威スキャンでプロセスを検出したときに表示するメッセージを設定できます。デフォルトでは、プロセスが検出されたときにメッセージを表示します。検出の結果、クライアントがサービスを終了またはプロセスを停止する必要があるときにも通知されます。

---

**メモ:** これらの設定を管理者がロックしている場合もあります。

---

このオプションについて詳しくは、[ヘルプ]を参照してください。

**TruScan プロアクティブ脅威スキャンの検出に対する通知を有効または無効にするには**

- 1 クライアントで、[設定の変更]をクリックします。
- 2 [プロアクティブ脅威防止]の隣にある[オプションの設定]をクリックします。

- 3 [プロアクティブ脅威防止の設定]ダイアログボックスの[通知]タブで、[検出時にメッセージを表示する]にチェックマークを付けます。
- 4 [プロセスを終了する前に確認する]と[サービスを停止する前に確認する]にチェックマークを付けるか、チェックマークをはずします。
- 5 [OK]をクリックします。

## シマンテックセキュリティレスポンスへの TruScan プロアクティブ脅威スキャンに関する情報の提出

デフォルトでは、プロアクティブ脅威スキャンは検出されたプロセスに関する情報をシマンテックセキュリティレスポンスに提出します。シマンテック社は、提出された情報を分析して、それが実際に脅威であるかどうかを判断します。脅威であるとシマンテック社が判断した場合には、その脅威に対応するためのシグネチャを生成します。シグネチャは、定義ファイルの更新バージョンに含まれます。

プロセスに関する情報を提出するときには、次の情報が含まれます。

- 実行可能ファイルへのパス
- 実行可能ファイル
- その脅威を参照しているファイルとレジストリロードポイントに関する情報
- 内部の状態についての情報
- プロアクティブ脅威スキャンが使ったコンテンツバージョン

ユーザーのコンピュータを特定可能な個人情報とは提出されません。

シマンテックセキュリティレスポンスへのプロアクティブ脅威スキャンの提出は、デフォルトで有効になっています。

---

**メモ:** 提出の設定を管理者がロックしている場合もあります。

---

この手順で使うオプションについて詳しくは、[ヘルプ]をクリックしてください。

### シマンテックセキュリティレスポンスへの TruScan プロアクティブ脅威スキャンに関する情報の提出

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [ウイルス対策とスパイウェア対策]の隣にある[オプションの設定]をクリックします。
- 3 [ウイルス対策とスパイウェア対策の設定]ダイアログボックスの[提出]タブで、[TruScan プロアクティブ脅威スキャンの検出項目を自動的に提出する]にチェックマークを付けるか、チェックマークをはずします。
- 4 [OK]をクリックします。

## TruScan プロアクティブ脅威スキャンからのプロセスの除外

管理者が設定をロックしていなければ、プロアクティブ脅威スキャンに対する例外を作成することができます。

p.76 の「スキャン対象からの項目の除外について」を参照してください。

例外を作成するには、現在コンピュータで利用可能なファイルを選択します。プロアクティブ脅威スキャンで、そのファイルを使うアクティブなプロセスが検出されると、クライアントは例外に指定された処理を適用します。

たとえば、`foo.exe` というファイルを使うアプリケーションをコンピュータで実行するとします。`foo.exe` が実行されるとプロアクティブ脅威スキャンが実行されます。クライアントが、`foo.exe` は悪質な可能性があると判断しました。スキャン結果のダイアログが表示され、クライアントが `foo.exe` を検疫したことが示されます。そこで、プロアクティブ脅威スキャンが `foo.exe` を無視するように指定した例外を作成します。これでクライアントは `foo.exe` を復元し、次に `foo.exe` が実行されるときには `foo.exe` を無視します。

管理者がスキャンに対して集中例外を設定する場合もあります。管理者定義の例外と競合するような集中例外を作成した場合には、管理者定義の例外が優先されます。

**TruScan プロアクティブ脅威スキャンからプロセスを除外するには**

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [集中例外]の隣にある[オプションの設定]をクリックします。
- 3 [ユーザー定義の例外]タブで、[追加]をクリックしてから[TruScan プロアクティブ脅威スキャン例外]を選択します。
- 4 [TruScan プロアクティブ脅威スキャン例外の追加]ダイアログボックスで、例外を作成する対象のプロセスまたはファイルを検索します。
- 5 [処理]ドロップダウンリストで、[無視]、[ログのみ]、[検疫]、[終了]のいずれかを選択します。
- 6 [追加]をクリックします。
- 7 [集中例外]ダイアログボックスで、[閉じる]をクリックします。

# ネットワーク脅威防止の管理

この章では以下の項目について説明しています。

- ネットワーク脅威防止の管理について
- ファイアウォール保護の管理
- ファイアウォールのしくみ
- ファイアウォールルールについて
- ファイアウォールルールの追加
- ファイアウォールルールの順序の変更
- ルールの有効化と無効化
- ルールのエクスポートとインポート
- 組み込みのファイアウォールルールについて
- トラフィックの設定とステルス Web 参照の設定の有効化
- スマートトラフィックフィルタの有効化
- ネットワークでのファイルとプリンタの共有の有効化
- トラフィックの遮断
- アプリケーション固有の設定
- 侵入防止保護の管理
- 侵入防止保護のしくみ

- 侵入防止の設定の有効化または無効化
- 侵入防止の通知の設定
- 攻撃側コンピュータの遮断と遮断解除

## ネットワーク脅威防止の管理について

Symantec Endpoint Protection クライアントは、コンピュータが送受信する情報を監視し、ネットワーク攻撃を遮断するため、コンピュータを保護できます。

表6-1に、ネットワーク攻撃からコンピュータを保護するためにネットワーク脅威防止が使う方法を示します。

表 6-1 ネットワーク脅威防止ツール

ツール	説明
ファイアウォール	<p>ファイアウォールは、権限のないユーザーが、インターネットに接続しているコンピュータやネットワークにアクセスするのを防ぎます。ファイアウォールはハッカーの攻撃の可能性を検出し、個人情報を保護し、迷惑なネットワークトラフィックの原因を除去します。ファイアウォールはインバウンドとアウトバウンドのトラフィックを許可または遮断します。</p> <p>p.100の「<a href="#">ファイアウォールのしくみ</a>」を参照してください。</p> <p>p.98の「<a href="#">ファイアウォール保護の管理</a>」を参照してください。</p>
侵入防止システム	<p>IPS (Intrusion Prevention System の略で侵入防止システムの意味) は自動的にネットワーク攻撃を検出して遮断します。IPS は攻撃シグネチャのためにコンピュータに送受信されるすべてのパケットをスキャンします。</p> <p>IPS は攻撃シグネチャの広範なリストを利用し、疑わしいネットワーク活動を検出して遮断します。シマンテック社は既知の脅威リストを提供します。このリストは、クライアントで Symantec LiveUpdate を使用することで更新できます。シマンテック社の IPS エンジンと対応する IPS シグネチャのセットは、デフォルトでクライアントにインストールされます。</p> <p>p.117の「<a href="#">侵入防止保護の管理</a>」を参照してください。</p> <p>p.117の「<a href="#">侵入防止保護のしくみ</a>」を参照してください。</p>

## ファイアウォール保護の管理

デフォルトでは、ファイアウォールはすべてのネットワークトラフィックの着発信を許可します。特定のトラフィックの種類を許可または遮断するためにファイアウォールを設定できます。

すべてのクライアントで、トラブルシューティングを行うためにネットワーク脅威防止を一時的に無効にできます。たとえば、アプリケーションを開けないことがあります。

p.34の「ネットワーク脅威防止の有効化または無効化」を参照してください。

管理者はファイアウォールルール設定、ファイアウォール設定、侵入防止設定を許可することで、クライアントで操作できるレベルを決定します。新しいネットワーク接続と問題の可能性を通知されたときのみユーザーがクライアントを操作することも、ユーザーインターフェースをすべて利用することもできます。

表 6-2 に、コンピュータを保護するために実行できるファイアウォールタスクを示します。

表 6-2 ファイアウォール保護の管理

処理	説明
ファイアウォールのしくみの理解	ファイアウォールがネットワーク攻撃からコンピュータをいかに保護するか学習します。  p.100の「ファイアウォールのしくみ」を参照してください。
ファイアウォールルールの追加	ユーザーが設定するファイアウォールルールでクライアントのデフォルトのファイアウォールルールを補います。たとえば、アドウェアアプリケーションのようなコンピュータで実行したくないアプリケーションを遮断すると安全です。  p.106の「ファイアウォールルールの追加」を参照してください。  特定の種類のトラフィックを許可する組み込みのファイアウォールルールを有効または無効にすることができます。  p.110の「トラフィックの設定とステルス Web 参照の設定の有効化」を参照してください。  p.110の「スマートトラフィックフィルタの有効化」を参照してください。
ファイアウォール保護の監視	次の内容を調べるためにコンピュータのファイアウォール保護の状態を定期的に確認することができます。 <ul style="list-style-type: none"><li>■ 作成したファイアウォールルールが正しく機能する。</li><li>■ クライアントがネットワーク攻撃を遮断した。</li><li>■ 実行すると期待したアプリケーションをクライアントが遮断した。</li></ul> トラフィックログとファイアウォールの保護の状態を調べるためにパケットログを使うことができます。  p.139の「ネットワーク脅威防止ログとクライアント管理ログの使用」を参照してください。

## ファイアウォールのしくみ

ファイアウォール保護は、インターネットに接続しているコンピュータやネットワークへの権限のないユーザーのアクセスを防止します。

インターネット経由で移動するデータパケットには次の情報が含まれています。

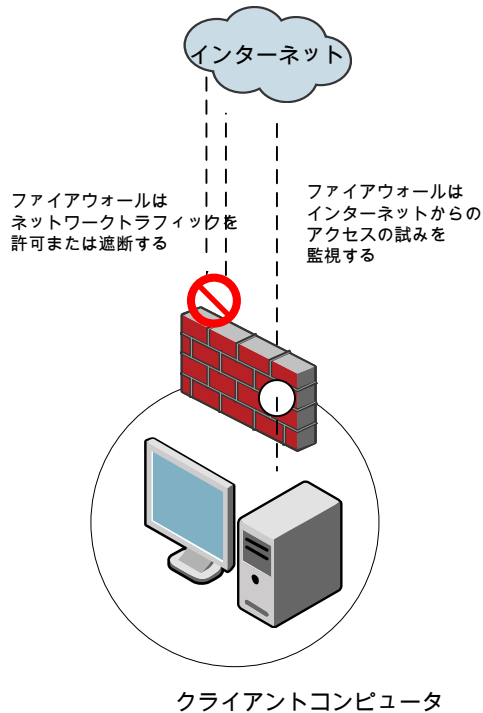
- 送信元コンピュータ
- 本来の受信者
- パケットデータの処理方法
- パケットを受信するポート

パケットは2つのコンピュータ間の情報の流れの一部である個別のデータチャンクです。パケットは送信先で組み立てられ連続したデータストリームとして表示されます。

ポートはインターネットから受信するデータのストリームを分割するチャネルです。コンピュータで動作するアプリケーションはポートで応答準備を行います。アプリケーションはポートに送られるデータを受け入れます。

ネットワーク攻撃は脆弱なアプリケーションの弱点を利用します。攻撃者はこうした弱点を利用して悪質なプログラムコードが含まれたパケットをポートに送信します。脆弱なアプリケーションがポートで応答準備を行うとき、攻撃者は悪質なコードによってコンピュータへアクセスできるようになります。

ファイアウォール保護は、バックグラウンドで実行されます。ファイアウォール保護は使っているコンピュータとインターネット上の他のコンピュータ間の通信を監視します。これによりコンピュータ上の情報へのアクセス試行を許可または遮断するシールドが作成されます。これにより他のコンピュータから接続の試みがあると警告されます。これは他のコンピュータに接続するコンピュータのアプリケーションによって接続の試みがあったことが警告されます。



ファイアウォール保護は、ネットワークトラフィックを許可または遮断するためのファイアウォールルールを提供します。

p.101 の「[ファイアウォールルールについて](#)」を参照してください。

## ファイアウォールルールについて

コンピュータが別のコンピュータへ接続を試みると、ファイアウォールは接続の種類とファイアウォールルールのリストを比較します。ファイアウォールはこれらのルールを使用して、自動的にすべてのインバウンドトラフィックパケットとアウトバウンドトラフィックパケットをチェックします。次にファイアウォールはルールで指定した情報に基づくパケットを許可または遮断します。

p.102 の「[ファイアウォールルールの要素について](#)」を参照してください。

p.106 の「[ファイアウォールルールの追加](#)」を参照してください。

## ファイアウォールルールの要素について

ファイアウォールルールは、ネットワーク接続を許可または遮断する条件を表します。たとえば、ルールでリモートポート 80 と IP アドレス 192.58.74.0 間のネットワークトラフィックを毎日午前 9 時から午後 5 時の間許可することができます。

表 6-3 に、ファイアウォールルールを定義するときの基準を示します。

表 6-3 ファイアウォールルールの条件

条件	説明
トリガ	<p>アプリケーション、ホスト、プロトコル、ネットワークアダプタ。</p> <p>複数のトリガ定義を組み合わせてより複雑なルール（たとえば特定の送信先アドレスに関して特定のプロトコルを識別するルール）を作成できます。ファイアウォールがルールを評価するとき、ルールを適用するためにはすべてのトリガが <b>true</b> である必要があります。現在のパケットに関していずれかのトリガが <b>true</b> でない場合、ファイアウォールはルールを適用できません。</p>
条件	<p>スケジュールとスクリーンセーバーの状態。</p> <p>条件パラメータはネットワーク接続に関するパラメータではありません。条件パラメータは、ルールがアクティブな状態を決定します。条件パラメータは省略可能で、定義しなくてもかまいません。スケジュールを設定したり、ルールをアクティブまたは非アクティブと見なすスクリーンセーバーの状態を指定します。パケットを受信したときに、ファイアウォールは非アクティブなルールを評価しません。</p>
処理	<p>許可するか遮断するか、ログに記録するかしないか。</p> <p>処理パラメータはファイアウォールが正常にルールと一致した場合に行う処理を指定します。受信したパケットに応じてルールが選択される場合、ファイアウォールはすべての処理を実行します。ファイアウォールがパケットを許可するか遮断するか、またログに記録するかしないかを指定します。</p> <p>ファイアウォールがトラフィックを許可する場合、ルールで指定されたトラフィックはネットワークにアクセスできます。</p> <p>ファイアウォールがトラフィックを遮断する場合、ルールで指定されたトラフィックは遮断され、ネットワークにアクセスできません。</p>

表 6-4 に、ファイアウォールルールで定義できるトリガを示します。

表 6-4 ファイアウォールルールのトリガ

トリガ	説明
アプリケーション	トラフィックを許可するルールで、アプリケーションのみをトリガに定義した場合、ファイアウォールはアプリケーションにネットワーク操作の実行を許可します。重要なのはアプリケーション自体でありアプリケーションが実行するネットワーク操作ではありません。たとえば、 <b>Internet Explorer</b> を許可し、その他のトリガを定義しない場合を考えます。ユーザーは <b>HTTP</b> 、 <b>HTTPS</b> 、 <b>FTP</b> 、 <b>Gopher</b> 、 <b>Web</b> ブラウザがサポートするその他の任意のプロトコルを使いリモートサイトにアクセスできます。管理者は追加のトリガを定義して通信を許可する特定のネットワークプロトコルとホストを記述できます。
ホスト	ローカルホストは常にローカルなクライアントコンピュータであり、リモートホストは常にネットワーク上の別の場所に配置されたリモートコンピュータです。このホストの関係の記述は、トラフィックの方向と無関係です。ホストのトリガを定義するとき、記述するネットワーク接続のリモート側のホストを指定します。
プロトコル	プロトコルトリガには、記述するトラフィックに対して意味のある 1 つ以上のネットワークプロトコルを指定します。  ローカルホストコンピュータには常にローカルポートがあり、リモートコンピュータには常にリモートポートがあります。このポートの関係の記述は、トラフィックの方向と無関係です。  次の種類のプロトコルを定義できます。 <ul style="list-style-type: none"><li>■ すべての IP プロトコル 任意のプロトコル。</li><li>■ TCP ポートまたはポートの範囲。</li><li>■ UDP ポートまたはポートの範囲。</li><li>■ ICMP 種類とコード。</li><li>■ 特定の IP プロトコル プロトコル番号 (IP の種類)。 例: タイプ 1 = ICMP、タイプ 6 = TCP、タイプ 17 = UDP</li></ul>
ネットワークアダプタ	ネットワークアダプタトリガを定義すると、ルールは指定した種類のアダプタを使用して送受信されたトラフィックのみに適用されます。任意のアダプタ、または現在クライアントコンピュータに関連付けられているアダプタを指定できます。

p.104 の「[ステートフルインスペクションについて](#)」を参照してください。

p.106 の「[ファイアウォールルールの追加](#)」を参照してください。

## ステートフルインスペクションについて

ファイアウォールはステートフルインスペクションを使用します。これは、送信元と送信先の IP アドレス、ポート、アプリケーションなどの、現在の接続に関する情報を追跡する処理です。クライアントはファイアウォールルールを検査する前にこの接続情報を使ってトラフィックフローを決定します。

たとえば、ファイアウォールルールがクライアントによる **Web** サーバー接続を許可する場合、ファイアウォールは接続情報をログに記録します。サーバーが応答すると、ファイアウォールは **Web** サーバーからクライアントに応答が送信されると判断し、ルールベースを検査することなく、接続を開始したクライアントに **Web** サーバーのトラフィックが送信されることを許可します。ファイアウォールが接続をログに記録する前に、ルールが最初のアウトバウンドトラフィックを許可する必要があります。

ステートフルインスペクションを使うと、通常は一方のみで始まるトラフィックに対して両方向のトラフィックを許可するルールを作成する必要がないため、ルールベースを単純化できます。一般的に一方に開始されるクライアントのトラフィックには、**Telnet** (ポート 23)、**HTTP** (ポート 80)、**HTTPS** (ポート 443) があります。クライアントはこのトラフィックを発信として開始するため、作成する必要があるのは、これらのプロトコルに対してアウトバウンドトラフィックを許可するルールのみです。ファイアウォールはリターントラフィックを許可します。

アウトバウンドルールのみを設定することで、クライアントセキュリティが次のように向上します。

- ルールベースの複雑さが減少します。
- アウトバウンドトラフィック用のみに設定されたポートで、ワームやその他の悪質なプログラムがクライアントと接続を開始する可能性を排除します。クライアントが開始していない、クライアントへのトラフィックに対して、インバウンドルールのみを設定することもできます。

ステートフルインスペクションは、**TCP** トラフィックを方向付けるすべてのルールをサポートします。ステートフルインスペクションは、**ICMP** トラフィックをフィルタ処理するルールをサポートしません。**ICMP** の場合、必要に応じて両方向のトラフィックを許可するルールを作成する必要があります。たとえば、クライアントが **ping** コマンドを使い応答を受信するには、両方向の **ICMP** トラフィックを許可するルールを作成する必要があります。

p.104 の「[UDP 接続について](#)」を参照してください。

## UDP 接続について

UDP 通信では、クライアントは最初の **UDP** データグラムを分析し、最初のデータグラムに対して実行される処理を、現在のプログラムセッション以降のすべての **UDP** データグラムに適用します。同じコンピュータ間のインバウンドまたはアウトバウンドトラフィックは、**UDP** 接続の一部と見なされます。

ステートフル UDP トラフィックの場合、UDP 接続が確立すると、インバウンド UDP 通信はファイアウォールルールが遮断しても許可されます。たとえば、ルールにより特定のアプリケーションに対するインバウンド UDP 通信が遮断される場合でも、アウトバウンド UDP データグラムを許可するように選択すれば、現在のアプリケーションセッションではすべてのインバウンド UDP 通信が許可されます。ステートレス UDP の場合、インバウンド UDP 通信応答を許可するファイアウォールルールを作成する必要があります。

アプリケーションがポートを閉じると UDP セッションは 60 秒後にタイムアウトになります。

p.104 の「ステートフルインスペクションについて」を参照してください。

## ルール処理順序について

ファイアウォールルールには、優先度の最も高いものから最も低いものへ、またはルールリストの一番上から一番下までの連続した順序が付けられます。1 つ目のルールでパケットの処理方法が指定されていない場合は、2 つ目のルールで検査されます。この処理はファイアウォールが一致するものを検出するまで続きます。一致するルールが見つかり、ファイアウォールではそのルールによって指定された処理が行われます。それよりも優先度の低いルールは検査されません。たとえば、最初のルールがすべてのトラフィックを遮断し、次のルールがすべてのトラフィックを許可する場合、クライアントはすべてのトラフィックを遮断します。

p.106 の「ファイアウォールルールの追加」を参照してください。

排他的にルールの順序を変更できます。最も制限の厳しいルールが最初に評価され、最も制限の緩いルールが最後に評価されます。たとえば、トラフィックを遮断するルールはルールリストの先頭の近くに配置します。リストの後ろにあるルールではトラフィックを許可します。

ルールベースを作成するためのベストプラクティスは以下の順序でルールを含んでいます。

1. すべてのトラフィックを遮断するルール。
2. すべてのトラフィックを許可するルール。
3. 特定のコンピュータを許可または遮断するルール。
4. 特定のアプリケーション、ネットワークサービス、ポートを許可または遮断するルール。

ルールや設定がファイアウォールで処理される順序を表 6-5 に示します。

表 6-5 ファイアウォールがファイアウォールルールと設定を処理する順序

優先度	設定
1 番目	カスタム IPS シグネチャ
2 番目	侵入防止の設定、トラフィックの設定、ステルス設定

優先度	設定
3 番目	スマートトラフィックフィルタ
4 番目	ファイアウォールルール
5 番目	ポートスキャンチェック
6 番目	LiveUpdate でダウンロードした IPS シグネチャ

p.107 の「[ファイアウォールルールの順序の変更](#)」を参照してください。

## ファイアウォールルールの追加

ファイアウォールルールを追加するときに、ルールの効果を決定する必要があります。たとえば、特定の送信元からのトラフィックをすべて許可したり、Web サイトからの UDP パケットを遮断することができます。

p.101 の「[ファイアウォールルールについて](#)」を参照してください。

p.102 の「[ファイアウォールルールの要素について](#)」を参照してください。

ファイアウォールルールを追加するには

- 1 クライアントのサイドバーで、[状態]をクリックします。
- 2 [ネットワーク脅威防止]の隣で、[オプション]、[ファイアウォールルールの設定]の順に選択します。
- 3 [ファイアウォールルールの設定]ダイアログボックスで、[追加]をクリックします。
- 4 [全般]タブにルールの名前を入力し、[このトラフィックを遮断する]または[このトラフィックを許可する]をクリックします。
- 5 ルールのトリガを定義するには、次のタブのいずれかを選択します。
  - ホスト
  - ポートとプロトコル
  - アプリケーション各タブのオプションについて詳しくは[ヘルプ]をクリックしてください。
- 6 ルールをアクティブまたは非アクティブにする期間を定義するには、[スケジュール]タブで[スケジュールを有効にする]をクリックして、スケジュールを設定します。
- 7 変更が終わったら、[OK]をクリックします。

- 8 [ファイアウォールルールの設定]ダイアログボックスで、有効にするルールの[ルール名]列にチェックマークが付いていることを確認します。  
ファイアウォールがルールを処理する順序を変更することもできます。  
p.107の「[ファイアウォールルールの順序の変更](#)」を参照してください。
- 9 [OK]をクリックします。

## ファイアウォールルールの順序の変更

ファイアウォールはファイアウォールルールのリストを上から順に処理します。ルールの順序を変更することで、ファイアウォールによるファイアウォールルールの処理方法を決定できます。順序を変更するときに影響を受けるのは、現在選択されている場所の順序だけです。

---

**メモ:** 保護を改善するには、最も制限の厳しいルールを最初に、最も制限の緩いルールを最後に配置します。

---

p.105の「[ルール処理順序について](#)」を参照してください。

p.106の「[ファイアウォールルールの追加](#)」を参照してください。

ファイアウォールルールの順序を変更するには

- 1 クライアントのサイドバーで、[状態]をクリックします。
- 2 [ネットワーク脅威防止]の隣で、[オプション]、[ファイアウォールルールの設定]の順に選択します。
- 3 [ファイアウォールルールの設定]ダイアログボックスで、移動するルールを選択します。
- 4 次の処理のいずれかを実行します。
  - 選択しているルールを、上のルールよりも前にファイアウォールに処理させる場合は、上向きの矢印をクリックします。
  - 選択しているルールを、下のルールよりも後にファイアウォールに処理させる場合は、下向きの矢印をクリックします。
- 5 ルールの移動が終わったら、[OK]をクリックします。

## ルールの有効化と無効化

ファイアウォールがルールを処理できるように、ルールを有効化する必要があります。ルールは、追加したときに自動的に有効化されます。

コンピュータまたはアプリケーションに対する特定のアクセスを許可する必要がある場合はファイアウォールルールを無効にできます。

p.106の「[ファイアウォールルールの追加](#)」を参照してください。

**ルールを有効または無効にするには**

- 1 クライアントのサイドバーで、[状態]をクリックします。
- 2 [ネットワーク脅威防止]の隣で、[オプション]、[ファイアウォールルールの設定]の順に選択します。
- 3 [ファイアウォールルールの設定]ダイアログボックスで、有効にするルールの[ルール名]列の隣にあるチェックボックスにチェックマークを付けます。また、無効にするルールのチェックマークをはずします。
- 4 [OK]をクリックします。

## ルールのエクスポートとインポート

他のクライアントとルールを共有することで、ルールを作成し直す必要がなくなります。別のコンピュータとの間でルールをエクスポートしたりインポートしたりできます。インポートしたルールは、ファイアウォールルールリストの一番下に追加されます。インポートしたルールが既存のルールと同一である場合でも、インポートしたルールは既存のルールを上書きしません。

エクスポートしたルールとインポートしたルールは、.sar ファイルに保存されます。

p.106の「[ファイアウォールルールの追加](#)」を参照してください。

**ルールをエクスポートするには**

- 1 クライアントのサイドバーで、[状態]をクリックします。
- 2 [ネットワーク脅威防止]の隣で、[オプション]、[ファイアウォールルールの設定]の順に選択します。
- 3 [ファイアウォールルールの設定]ダイアログボックスで、エクスポートするルールを選択します。
- 4 ルールを右クリックし、[選択したルールのエクスポート]をクリックします。
- 5 [エクスポート]ダイアログボックスにファイル名を入力し、[保存]をクリックします。
- 6 [OK]をクリックします。

**ルールをインポートするには**

- 1 クライアントのサイドバーで、[状態]をクリックします。
- 2 [ネットワーク脅威防止]の隣で、[オプション]、[ファイアウォールルールの設定]の順に選択します。

- 3 [ファイアウォールルールの設定]ダイアログボックスで、ファイアウォールルールリストを右クリックし、[ルールのインポート]をクリックします。
- 4 [インポート]ダイアログボックスで、インポートするルールを含む .sar ファイルを選択します。
- 5 [開く]をクリックします。
- 6 [OK]をクリックします。

## 組み込みのファイアウォールルールについて

ネットワーク脅威防止にはある特定のトラフィックの種類を可能にする組み込みのルールが含まれています。ファイアウォールルールを自身で追加する代わりに、これらの組み込みルールを有効または無効にすることができます。

p.106 の「[ファイアウォールルールの追加](#)」を参照してください。

管理者はこれらの設定をカスタマイズする権限をユーザーに与える場合と与えない場合があります。

デフォルトでは、ファイアウォールは IPv6 を除いてほとんどの TCP/IP トラフィックを許可します。

次に示す組み込みファイアウォールルールを有効または無効にできます。

スマートトラフィックフィルタ ほとんどのネットワークで必要とされる、特定の種類のトラフィックを許可します。このようなトラフィックには、DHCP、DNS、WINS トラフィックが含まれます。

p.110 の「[スマートトラフィックフィルタの有効化](#)」を参照してください。

トラフィックとステルスの設定 NetBIOS 保護、トークンリングトラフィック、DNS 逆ルックアップ、ステルスモード設定などのトラフィック機能を有効にします。

p.110 の「[トラフィックの設定とステルス Web 参照の設定の有効化](#)」を参照してください。

新しいソフトウェアのインストール中などの特定の時間だけ保護を無効にすることができます。

p.34 の「[ネットワーク脅威防止の有効化または無効化](#)」を参照してください。

Microsoft Windows ネットワークを設定することもできます。

p.111 の「[ネットワークでのファイルとプリンタの共有の有効化](#)」を参照してください。

## トラフィックの設定とステルス Web 参照の設定の有効化

クライアントを特定の種類のネットワーク攻撃から保護するために各種トラフィックの設定やステルス Web 参照の設定を有効にできます。トラフィックの設定を有効にすることでドライバ、NetBIOS、トークンリングを使って通信するトラフィックの検出と遮断を実行できます。オプションを設定することでより不可視の攻撃を使うトラフィックも検出できます。どのファイアウォールルールにも一致しない IP トラフィックの動作を制御することもできます。ファイアウォールがある特定の操作を完了した後、制御はいくつかのコンポーネントに渡されます。各コンポーネントは異なる種類のパケット分析を実行するように設計されています。

p.110 の「[スマートトラフィックフィルタの有効化](#)」を参照してください。

トラフィックの設定とステルス Web 参照の設定を有効にするには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [ネットワーク脅威防止]の隣にある[オプションの設定]をクリックします。
- 3 [ネットワーク脅威防止の設定]ダイアログボックスで、[ファイアウォール]をクリックします。
- 4 [ファイアウォール]タブの[トラフィックの設定]と[ステルスの設定]のグループボックス内にあるチェックボックスにチェックマークを付けて、設定を有効にします。
- 5 [OK]をクリックします。

## スマートトラフィックフィルタの有効化

スマートトラフィックフィルタでは、一部の基本的なネットワークサービスの通常のやり取りが、それらのサービスを明示的に許可するルールが定義されていなくても許可されます。処理の間、これらのフィルタはファイアウォールルールの前に評価されるため、アクティブな組み込みルールに一致するパケットが許可されます。組み込みルールは、DHCP、DNS、WINS の各サービスに対して定義できます。これらのサービスの要求はクライアントコンピュータから送信される必要があり、サーバーレスポンスは事前定義済みの 5 秒以内に起きる必要があります。このレスポンスは元のクライアント要求に対して有効であることを確認するために検証されます。

スマートトラフィックルールフィルタは要求が送信された場合にパケットを許可します。これらのフィルタはパケットを遮断しません。パケットはファイアウォールルールにより許可または遮断されます。

p.110 の「[トラフィックの設定とステルス Web 参照の設定の有効化](#)」を参照してください。

スマートトラフィックフィルタを有効にするには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [ネットワーク脅威防止]の隣にある[オプションの設定]をクリックします。

- 3 [ネットワーク脅威防止の設定]ダイアログボックスで、[ファイアウォール]をクリックします。
- 4 次のチェックボックスの1つ以上にチェックマークを付けます。
  - スマート DHCP を有効にする
  - スマート DNS を有効にする
  - スマート WINS を有効にする
- 5 [OK]をクリックします。

## ネットワークでのファイルとプリンタの共有の有効化

クライアントで、ローカルネットワーク上のファイルの共有や共有されたファイルとプリンタの参照を有効にできます。ネットワーク型攻撃を防止するために、ネットワーク上のファイルとプリンタの共有を無効にできます。

次の方法でネットワーク上のファイルとプリンタの共有を有効にできます。

- [Microsoft Windows ネットワーク]タブで、ネットワーク上のファイルとプリンタの共有設定を自動的に有効にします。  
ファイアウォールルールでこのトラフィックが遮断される場合、この設定よりもファイアウォールルールが優先されます。
- ファイアウォールルールを追加することによって、ネットワーク上のファイルとプリンタの共有を手動で有効にします。  
設定での柔軟性よりも高い柔軟性が必要な場合には、ファイアウォールルールを追加します。たとえば、ルールを作成すると、すべてのホストではなく特定のホストを指定できます。ファイアウォールルールにより、ポートにアクセスしてファイルとプリンタを参照したり共有したりすることができます。クライアントがそのファイルを共有できるように、1組のファイアウォールルールを作成します。クライアントが他のファイルとプリンタを参照できるように、もう1組のファイアウォールルールを作成します。  
管理者がクライアントでこのオプションを有効にしていないことがあります。クライアントのユーザーはこれらの設定を自動的に有効にできます。

p.109の「[組み込みのファイアウォールルールについて](#)」を参照してください。

ネットワーク上のファイルとプリンタの共有を自動的に有効にするには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [ネットワーク脅威防止]の隣にある[オプションの設定]をクリックします。
- 3 [ネットワーク脅威防止の設定]ダイアログボックスで、[Microsoft Windows ネットワーク]をクリックします。

- 4 ネットワーク上の他のコンピュータやプリンタを参照するには、[Microsoft Windows ネットワーク]タブで、[ネットワーク上のファイルとプリンタを参照する]をクリックします。
- 5 他のコンピュータがコンピュータ上のファイルを参照できるようにするには、[ネットワーク上の他のユーザーとファイルとプリンタを共有する]をクリックします。
- 6 [OK]をクリックします。

#### クライアントを手動で有効にしてファイルとプリンタを参照するには

- 1 クライアントのサイドバーで、[状態]をクリックします。
- 2 [ネットワーク脅威防止]の隣で、[オプション]、[ファイアウォールルールの設定]の順に選択します。
- 3 [ファイアウォールルールの設定]ダイアログボックスで、[追加]をクリックします。
- 4 [全般]タブにルールの名前を入力し、[このトラフィックを許可する]をクリックします。
- 5 [ポートとプロトコル]タブの[プロトコル]ドロップダウンリストで、[TCP]をクリックします。
- 6 [リモートポート]ドロップダウンリストで、**88, 135, 139, 445**と入力します。
- 7 [OK]をクリックします。
- 8 [ファイアウォールルールの設定]ダイアログボックスで、[追加]をクリックします。
- 9 [全般]タブにルールの名前を入力し、[このトラフィックを許可する]をクリックします。
- 10 [ポートとプロトコル]タブの[プロトコル]ドロップダウンリストで、[UDP]をクリックします。
- 11 [リモートポート]ドロップダウンリストで、**88**と入力します。
- 12 [ローカルポート]ドロップダウンリストで、**137, 138**と入力します。
- 13 [OK]をクリックします。

#### 他のコンピュータを手動で有効にしてクライアント上のファイルを参照するには

- 1 クライアントのサイドバーで、[状態]をクリックします。
- 2 [ネットワーク脅威防止]の隣で、[オプション]、[ファイアウォールルールの設定]の順に選択します。
- 3 [ファイアウォールルールの設定]ダイアログボックスで、[追加]をクリックします。
- 4 [全般]タブにルールの名前を入力し、[このトラフィックを許可する]をクリックします。
- 5 [ポートとプロトコル]タブの[プロトコル]ドロップダウンリストで、[TCP]をクリックします。
- 6 [ローカルポート]ドロップダウンリストで、**88, 135, 139, 445**と入力します。
- 7 [OK]をクリックします。

- 8 [ファイアウォールルールの設定]ダイアログボックスで、[追加]をクリックします。
- 9 [全般]タブにルールの名前を入力し、[このトラフィックを許可する]をクリックします。
- 10 [ポートとプロトコル]タブの[プロトコル]ドロップダウンリストで、[UDP]をクリックします。
- 11 [ローカルポート]ドロップダウンリストで、**88, 137, 138**と入力します。
- 12 [OK]をクリックします。

## トラフィックの遮断

次の状況で、インバウンドトラフィックとアウトバウンドトラフィックを遮断するようにコンピュータを設定できます。

- コンピュータのスクリーンセーバーがアクティブなとき  
コンピュータのスクリーンセーバーがアクティブなときに、ネットワークコンピュータのすべてのインバウンドおよびアウトバウンドトラフィックを遮断するように、コンピュータを設定できます。スクリーンセーバーがオフになると、コンピュータは設定以前に割り当てられていたセキュリティレベルに戻ります。
- ファイアウォールを実行していないとき  
クライアントコンピュータがオンになってからファイアウォールサービスが開始されるまで、およびファイアウォールサービスが停止してからコンピュータがオフになるまで、コンピュータは保護されません。この期間は、権限のない通信が許可される小さなセキュリティホールになります。
- インバウンドトラフィックとアウトバウンドトラフィックをすべて遮断したいとき  
特定の破壊的なウイルスが自社のネットワークやサブネットを攻撃している場合は、すべてのトラフィックを遮断できます。通常の状態では、トラフィックをすべて遮断する必要はありません。

---

**メモ:** 管理者はこのオプションを使用できないように設定している場合があります。自己管理クライアントではトラフィックを遮断できません。

---

ネットワーク脅威防止を無効にすると、すべてのトラフィックを許可できます。

p.34の「[ネットワーク脅威防止の有効化または無効化](#)」を参照してください。

p.120の「[攻撃側コンピュータの遮断と遮断解除](#)」を参照してください。

スクリーンセーバーがアクティブなときにトラフィックを遮断するには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [ネットワーク脅威防止]の隣にある[オプションの設定]をクリックします。

- 3 [ネットワーク脅威防止の設定]ダイアログボックスで、[Microsoft Windows ネットワーク]をクリックします。
- 4 [Microsoft Windows ネットワーク]タブの[スクリーンセーバーの実行中に Microsoft Windows ネットワークトラフィックを遮断する]をクリックします。
- 5 [OK]をクリックします。

ファイアウォールを実行していないときにトラフィックを遮断するには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [ネットワーク脅威防止]の隣にある[オプションの設定]をクリックします。
- 3 [ネットワーク脅威防止の設定]ダイアログボックスで、[ファイアウォール]をクリックします。
- 4 [ファイアウォール]タブの[ファイアウォールの停止後にファイアウォールが起動するまですべてのトラフィックを遮断する]をクリックします。
- 5 [DHCP と NetBIOS の初期トラフィックを許可する]をクリックするかどうかは任意です。
- 6 [OK]をクリックします。

任意の時間にすべてのトラフィックを遮断するには

- 1 クライアントのサイドバーで、[状態]をクリックします。
- 2 [ネットワーク脅威防止]の隣で、[オプション]、[ネットワーク活動の表示]の順に選択します。
- 3 [ツール]、[すべてのトラフィックを遮断]の順に選択します。
- 4 [はい]をクリックして確認します。
- 5 クライアントが使う以前のファイアウォール設定に戻すには、[ツール]、[すべてのトラフィックを遮断]の順に選択して、チェックマークをはずします。

## アプリケーション固有の設定

クライアントサービスの開始以降に実行されたか、ネットワークへのアクセスの許可を求めたアプリケーションのオプションを設定できます。

IP アドレスやポートなど、そのアプリケーションで使うことができる制限を設定できます。ネットワーク接続を通じてアクセスしようとする各アプリケーションに対してクライアントが実行する処理を表示して変更できます。特定のアプリケーションを設定することにより、アプリケーションベースのファイアウォールルールを作成します。

---

**メモ:** ファイアウォールルールとアプリケーション固有の設定の間に矛盾がある場合には、ファイアウォールルールが優先されます。たとえば、午前 1 時から午前 8 時の間のすべてのトラフィックを遮断するファイアウォールは、特定のビデオアプリケーションのスケジュールに上書きされます。

---

p.106 の「[ファイアウォールルールの追加](#)」を参照してください。

[ネットワーク活動]ダイアログボックスに表示されるアプリケーションは、クライアントサービスの開始以降に実行されたアプリケーションとサービスです。

#### アプリケーション固有の設定を行うには

- 1 クライアントのサイドバーで、[状態]をクリックします。
- 2 [ネットワーク脅威防止]の隣で、[オプション]、[アプリケーション設定の表示]の順に選択します。
- 3 [アプリケーション設定の表示]ダイアログボックスで、設定するアプリケーションを選択して[設定]をクリックします。
- 4 [アプリケーションの設定]ダイアログボックスで、[アプリケーションの信頼できるIP]ボックスに IP アドレスまたは IP アドレス範囲を入力します。
- 5 [リモートサーバーのポート]または[ローカルポート]のグループボックスで、TCP ポートまたは UDP ポートを選択します。
- 6 トラフィックの方向を指定するには、次の項目を 1 つまたは両方クリックします。
  - アウトバウンドトラフィックを許可するには、[発信接続を許可する]をクリックします。
  - インバウンドトラフィックを許可するには、[着信接続を許可する]をクリックします。
- 7 スクリーンセーバーの実行中もルールを適用するには、[スクリーンセーバーモードの間は許可する]をクリックします。
- 8 制限を有効にするまたは有効にしない期間のスケジュールを設定するには、[スケジュールを有効にする]をクリックします。
- 9 次のいずれかの項目を選択します。
  - 制限を有効にする時間を指定するには、[以下の期間]をクリックします。
  - 制限を有効にしない時間を指定するには、[下の期間を除外する]をクリックします。
- 10 スケジュールを設定します。
- 11 [OK]をクリックします。

12 アプリケーションの処理を変更するには、[アプリケーション設定の表示]ダイアログボックスでアプリケーションを右クリックしてから[許可]と[遮断]のいずれかをクリックします。

13 [OK]をクリックします。

アプリケーションまたはサービスを停止するには

- 1 クライアントのサイドバーで、[状態]をクリックします。
- 2 [ネットワーク脅威防止]の隣で、[オプション]、[ネットワーク活動の表示]の順に選択します。
- 3 [実行中のアプリケーション]フィールドで、アプリケーションを右クリックし、[終了]をクリックします。
- 4 [はい]をクリックして確定し、[閉じる]をクリックします。

## アプリケーションからの制限の削除

ファイアウォールがアプリケーションを遮断する時刻など、アプリケーションの制限は解除できます。制限を削除すると、クライアントがアプリケーションに対して実行する処理も消去されます。アプリケーションまたはサービスが再度ネットワークに接続しようとしたときに、アプリケーションの許可または遮断を確認するメッセージが再度表示されます。

コンピュータの再起動などで、アプリケーションがコンピュータに再度アクセスを試みるまで、アプリケーションまたはサービスの実行を停止できます。

p.114の「[アプリケーション固有の設定](#)」を参照してください。

アプリケーションから制限を削除するには

- 1 クライアントのサイドバーで、[状態]をクリックします。
- 2 [ネットワーク脅威防止]の隣で、[オプション]、[アプリケーション設定の表示]の順に選択します。
- 3 [アプリケーション設定の表示]ダイアログボックスで、次のいずれかの操作を行います。
  - リストから1つのアプリケーションを削除するには、アプリケーションを選択し、[削除]をクリックします。
  - リストからすべてのアプリケーションを削除するには、[すべてを削除]をクリックします。
- 4 [はい]をクリックします。
- 5 [OK]をクリックします。

## 侵入防止保護の管理

侵入防止保護は、[ポリシー]ページで管理します。

ネットワーク脅威防止の一部として侵入防止保護を管理します。

表 6-6 に、コンピュータを保護するために実行できる侵入防止タスクを示します。

表 6-6 侵入防止保護の管理

処理	説明
侵入防止の学習	侵入防止がネットワーク攻撃を検出して遮断する方法を学習します。 p.117 の「 <a href="#">侵入防止保護のしくみ</a> 」を参照してください。
侵入防止が有効に設定されていることを確認	コンピュータで侵入防止が有効になっていることを定期的 に確認します。 p.118 の「 <a href="#">侵入防止の設定の有効化または無効化</a> 」を参 照してください。
最新の IPS シグネチャのダウンロード	最新の IPS シグネチャのダウンロードデフォルトでは、 LiveUpdate が IPS シグネチャをダウンロードします。た だし、IPS シグネチャをすぐにダウンロードする場合もあ ります。 p.26 の「 <a href="#">コンピュータの保護の更新</a> 」を参照してください。

p.120 の「[攻撃側コンピュータの遮断と遮断解除](#)」を参照してください。

## 侵入防止保護のしくみ

侵入防止保護はネットワーク攻撃を自動的に検出して遮断します。侵入防止システムは、コンピュータで送受信される各パケットに対して、攻撃シグネチャが含まれていないかどうかスキャンします。攻撃シグネチャはオペレーティングシステムやプログラムの既知の脆弱性を悪用する攻撃者の試みを識別する一意の情報配列です。

侵入防止保護にはシマンテック社の広範な攻撃シグネチャリストを使います。

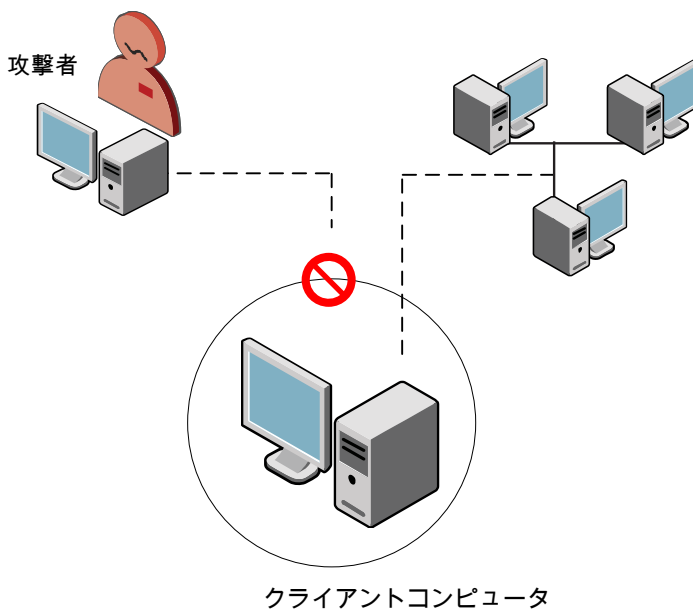
[http://www.symantec.com/ja/jp/business/security\\_response/landing/azlisting.jsp](http://www.symantec.com/ja/jp/business/security_response/landing/azlisting.jsp)

侵入防止保護ではクライアントと攻撃側コンピュータ間のすべての通信を必要に応じて一定期間遮断できます。

p.117 の「[侵入防止保護の管理](#)」を参照してください。

p.118 の「[侵入防止の設定の有効化または無効化](#)」を参照してください。

図 6-1 侵入防止保護



## 侵入防止の設定の有効化または無効化

侵入防止の設定はデフォルトでは無効になります。トラブルシューティングを行う目的で、またはクライアントコンピュータが過度の誤認を検出した場合に、IPS の設定を無効にしたい場合があります。

次の設定を有効または無効にできます。

- ネットワーク攻撃を検出および防止する、侵入防止システムのシグネチャの設定。
- ポートスキャンやサービス拒否攻撃を防止する、侵入防止の設定。
- 攻撃を送信するコンピュータを自動的に遮断する、アクティブレスポンスの設定。

一般的に、侵入防止の設定を無効にすると、コンピュータの安全性は低下します。ただし、誤認を回避したり、クライアントコンピュータのトラブルシューティングのために、これらの設定を無効にする必要がある場合もあります。

クライアントは、侵入防止システムが検出した攻撃やセキュリティイベントをセキュリティログに記録します。クライアントが、攻撃やイベントをパケットログに記録することもできます。

p.117 の「[侵入防止保護のしくみ](#)」を参照してください。

---

**メモ:** 管理者がこれらのオプションを利用できないように設定している場合もあります。

---

### 侵入防止の設定を有効または無効にするには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [ネットワーク脅威防止]の隣にある[オプションの設定]をクリックします。
- 3 [ネットワーク脅威防止の設定]ダイアログボックスで、[侵入防止]をクリックします。
- 4 設定を有効にするには、[侵入防止]タブで、次のいずれかのチェックボックスにチェックマークを付けます。
  - 侵入防止を有効にする
  - サービス拒否検出を有効にする
  - ポートスキャン検出を有効にする設定について詳しくは[ヘルプ]をクリックしてください。
- 5 [OK]をクリックします。

## 侵入防止の通知の設定

クライアントがコンピュータに対するネットワーク攻撃を検出したときや、アプリケーションによるアクセスを遮断したときに、通知を表示するように設定できます。これらの通知を表示する時間や、音声による通知を行うかどうかを設定できます。

侵入防止の通知を表示するには、侵入防止システムを有効にする必要があります。

---

**メモ:** 管理者がこれらのオプションを利用できないように設定している場合もあります。

---

### 侵入防止通知を設定するには

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [ネットワーク脅威防止]の隣にある[オプションの設定]をクリックします。
- 3 [ネットワーク脅威防止の設定]ダイアログボックスで、[侵入防止]をクリックします。
- 4 [侵入防止通知を表示する]にチェックマークを付けます。
- 5 通知を表示するときに警告音を鳴らすには、[ユーザーに通知するときにサウンドを使う]にチェックマークを付けます。
- 6 [通知を表示する秒数]フィールドに、通知を表示する時間を入力します。
- 7 [OK]をクリックします。

## 攻撃側コンピュータの遮断と遮断解除

Symantec Endpoint Protection クライアントがネットワーク攻撃を検出した場合、自動的に接続を遮断して、クライアントコンピュータの安全を確保できます。クライアントはアクティブレスポンスをアクティブにします。この機能は、設定した期間のみ攻撃側コンピュータの IP アドレスを使用するすべての通信を自動的に遮断します。攻撃側コンピュータの IP アドレスは単一の場所で遮断されます。

更新された IPS シグネチャ、更新されたサービス拒否のシグネチャ、ポートスキャンもアクティブレスポンスをトリガします。

攻撃側コンピュータの IP アドレスは、セキュリティログで確認できます。セキュリティログでアクティブレスポンスを停止することで、攻撃の遮断を解除することもできます。

p.118 の「[侵入防止の設定の有効化または無効化](#)」を参照してください。

p.113 の「[トラフィックの遮断](#)」を参照してください。

**攻撃側コンピュータを遮断するには**

- 1 クライアントのサイドバーで、[設定の変更]をクリックします。
- 2 [ネットワーク脅威防止]の隣にある[オプションの設定]をクリックします。
- 3 [ネットワーク脅威防止の設定]ダイアログボックスで、[侵入防止]をクリックします。
- 4 [攻撃者の IP アドレスを自動的に遮断する秒数]にチェックマークを付け、攻撃側コンピュータを遮断する秒数を入力します。

1 から 999,999 秒までの数値を入力します。デフォルトは 600 秒(10 分)です。

- 5 [OK]をクリックします。

デフォルトの時間を待たずに IP アドレスの遮断を解除する場合は、すぐに遮断解除できます。

**攻撃側コンピュータを遮断解除するには**

- 1 クライアントのサイドバーで、[ログの表示]をクリックします。
- 2 [クライアント管理]の隣で、[ログの表示]、[セキュリティログ]の順に選択します。
- 3 [セキュリティログ]で、[イベントの種類]列に[アクティブレスポンス]を含む行を選択し、[処理]、[アクティブレスポンスを停止する]の順に選択します。

遮断された IP アドレスを遮断解除するには、[処理]、[すべてのアクティブレスポンスを停止する]の順に選択します。アクティブレスポンスを遮断解除すると、[イベントの種類]列に[アクティブレスポンスを中止しました]が表示されます。アクティブレスポンスがタイムアウトすると、[イベントの種類]列に[アクティブレスポンスを解除しました]が表示されます。

- 4 表示されるメッセージボックスで、[OK]をクリックします。
- 5 [ファイル]、[終了]の順に選択します。

# 3

## Symantec Network Access Control クライアントでの保護 の管理

- [第7章 Symantec Network Access Control の管理](#)



# Symantec Network Access Control の管理

この章では以下の項目について説明しています。

- [Symantec Network Access Control の仕組み](#)
- [ホストインテグリティ検査の実行](#)
- [ホストインテグリティポリシーの更新について](#)
- [コンピュータの修復](#)
- [Symantec Network Access Control ログの表示](#)
- [クライアントがエンフォーサと連携する方法](#)
- [802.1x 認証向けのクライアントの設定](#)

## Symantec Network Access Control の仕組み

Symantec Network Access Control クライアントは、ネットワークに接続しようとするコンピュータのポリシーコンプライアンスの有効性を確認し、実施します。この確認と実施のプロセスは、コンピュータがネットワークに接続する以前から開始され、接続中も継続されます。ホストインテグリティポリシーは、評価と処理のすべての基礎となるセキュリティポリシーです。

[表 7-1](#)に、クライアントコンピュータのポリシーコンプライアンスを実施するために Network Access Control で行われる処理を示します。

表 7-1 Symantec Network Access Control の動作方法

処理	説明
<p>クライアントは継続的に、それ自体のコンプライアンスを評価します。</p>	<p>ユーザーがクライアントコンピュータをオンにします。クライアントはホストインテグリティ検査を実行し、管理サーバーからダウンロードしたホストインテグリティポリシーとコンピュータの設定を比較します。</p> <p>ホストインテグリティ検査は、ウイルス対策ソフトウェア、パッチ、ホットフィックス、その他のセキュリティ要件に関して、コンピュータがホストインテグリティポリシーに従っているかどうかを評価します。たとえば、ポリシーは、ウイルス定義の最新更新日、およびオペレーティングシステムに適用されている最新パッチを確認できます。</p>
<p>Symantec Enforcer はクライアントコンピュータを認証し、コンピュータにネットワークへのアクセスを許可するか、非標準コンピュータを遮断して検査します。</p>	<p>コンピュータがすべてのポリシー要件を満たしている場合、ホストインテグリティ検査は成功します。エンフォースは、ホストインテグリティ検査に成功したコンピュータに、ネットワークへのフルアクセスを許可します。</p> <p>コンピュータがポリシー要件を満たしていない場合、ホストインテグリティ検査は失敗します。ホストインテグリティ検査が失敗したときは、ユーザーがコンピュータを修復するまで、クライアントまたは Symantec Enforcer はそのコンピュータを遮断するか、検査します。検査済みコンピュータは、ネットワークへのアクセスを制限されているか許可されていません。</p> <p>p.127 の「<a href="#">クライアントがエンフォースと連携する方法</a>」を参照してください。</p>
<p>特定の要件を満たしていない場合でもホストインテグリティ検査が成功するように、管理者がポリシーを設定していることがあります。</p>	<p>ホストインテグリティ検査に成功するたびに、クライアントが通知を表示することがあります。</p> <p>p.21 の「<a href="#">ネットワークアクセス制御通知への応答</a>」を参照してください。</p>
<p>クライアントは、非標準コンピュータを修復します。</p>	<p>ホストインテグリティポリシーの要件が満たされていないことを検出すると、クライアントは必要なソフトウェアをインストールするか、またはユーザーにインストールを要求します。修復されたコンピュータは、再度ネットワークにアクセスしようとします。コンピュータが完全に準拠していれば、ネットワークはコンピュータのネットワークアクセスを認可します。</p> <p>p.125 の「<a href="#">コンピュータの修復</a>」を参照してください。</p>
<p>クライアントはコンプライアンスをプロアクティブに監視します。</p>	<p>クライアントは、クライアントコンピュータすべてについて、コンプライアンス状態をアクティブに監視します。コンピュータのコンプライアンス状態が変化する場合はいつでも、コンピュータのネットワークアクセス権も変化します。</p>

ホストインテグリティ検査の結果の詳細は、セキュリティログログで確認できます。

## ホストインテグリティ検査の実行

クライアントがホストインテグリティ検査を実行する頻度は、管理者が設定します。次の検査を待たずにホストインテグリティ検査をすぐに実行する必要がある場合もあります。たとえば、ホストインテグリティ検査に失敗したことにより、コンピュータのウイルス対策アプリケーションを更新する必要がある場合などです。クライアントでは必要なソフトウェアをすぐにダウンロードするか、またはダウンロードを延期するかを選択できます。ソフトウェアをすぐにダウンロードする場合は、ホストインテグリティ検査を再度実行して、正しいソフトウェアを入手したことを確認する必要があります。次回のホストインテグリティ検査が実行されるまで待つか、検査をすぐに実行することもできます。

ホストインテグリティ検査を実行するには

- 1 クライアントのサイドバーで、[状態]をクリックします。
- 2 [Symantec Network Access Control]の隣で、[オプション]、[今すぐに確認]の順に選択します。
- 3 ホストインテグリティ検査が実行されたことを示すメッセージが表示されたら、[OK]をクリックします。

ネットワークアクセスが遮断された場合、コンピュータを更新してセキュリティポリシーに準拠させた後にネットワークアクセス権限を再取得してください。

## ホストインテグリティポリシーの更新について

クライアントは、ホストインテグリティポリシーを定期的に更新します。テストの目的で、次の予定更新日以前にホストインテグリティポリシーを更新するように管理者がユーザーに依頼することがあります。これ以外の目的で、ユーザーがポリシーを更新する必要はありません。

p.28の「[ポリシーファイルを手動で更新](#)」を参照してください。

## コンピュータの修復

ホストインテグリティポリシーの要件が満たされていないことを検出すると、クライアントは次のいずれかの方法で応答します。

- クライアントはソフトウェア更新を自動的にダウンロードします。
- クライアントは、必要なソフトウェア更新をダウンロードするように要求するメッセージを表示します。

### コンピュータを修復するには

- ◆ 表示された **Symantec Endpoint Protection** のダイアログボックスで、次のいずれかの操作をします。
  - コンピュータが満たしていないセキュリティの必要条件を確認するには、[詳細] をクリックします。
  - ソフトウェアをすぐにインストールするには、[今すぐに復元] をクリックします。インストールを開始後にキャンセルするオプションが表示される場合と表示されない場合があります。
  - ソフトウェアのインストールを延期するには、[後で通知する] をクリックして、ドロップダウンリストから時間間隔を選択します。管理者は、ユーザーがインストールを延期する最大回数を設定できます。

## Symantec Network Access Control ログの表示

Symantec Network Access Control クライアントは動作とホストインテグリティ検査をさまざまな角度から監視するために次のログを使います。

セキュリティ	ホストインテグリティ検査の結果と状態を記録します。
システム	管理サーバへの接続、クライアントのセキュリティポリシーの更新など、クライアントの動作の変化をすべて記録します。

管理下クライアントを使う場合は、両方のログがサーバーに定期的にアップロードされることがあります。管理者はネットワークの全体的なセキュリティの状態を分析するためにログのコンテンツを使うことができます。

これらのログからログデータをエクスポートできます。

### Symantec Network Access Control のログを表示するには

- 1 クライアントのサイドバーで、[状態] をクリックします。
- 2 システムログを表示するには、[Symantec Network Access Control] の隣で、[オプション]、[ログの表示] の順に選択します。
- 3 セキュリティログを表示するには、[クライアント管理ログ - システムログ] ダイアログボックスで、[表示]、[セキュリティログ] の順に選択します。
- 4 [ファイル]、[終了] の順に選択します。  
p.135 の「[ログについて](#)」を参照してください。

## クライアントがエンフォーサと連携する方法

クライアントは Symantec Enforcer と相互作用します。エンフォーサは、保護するネットワークに接続するコンピュータすべてが、確実にクライアントソフトウェアを実行し、正しいセキュリティポリシーを有するようにします。

p.123 の「[Symantec Network Access Control の仕組み](#)」を参照してください。

エンフォーサは、クライアントコンピュータにネットワークアクセスを許可する前に、ユーザーまたはクライアントコンピュータを認証する必要があります。Symantec Network Access Control は、いくつかの種類のエンフォーサと共に動作して、クライアントコンピュータを認証します。Symantec Enforcer は、コンピュータにネットワークアクセスを許可する前に、ホストインテグリティの結果とクライアントコンピュータの ID 情報を検証するネットワークハードウェア機器です。

エンフォーサは、クライアントにネットワークアクセスを許可する前に、次の情報を確認します。

- コンピュータが実行するクライアントソフトウェアのバージョン。
- クライアントに一意の識別子 (UID) があること。
- クライアントのホストインテグリティポリシーが最新のものに更新されていること。
- クライアントコンピュータがホストインテグリティ検査に成功していること。

p.127 の「[802.1x 認証向けのクライアントの設定](#)」を参照してください。

## 802.1x 認証向けのクライアントの設定

社内ネットワークで認証に LAN エンフォーサを使用する場合、802.1x 認証を実行するようにクライアントコンピュータを設定する必要があります。ユーザーまたは管理者がクライアントを設定できます。管理者がユーザーに 802.1x 認証を設定する許可を与えていない場合もあります。

802.1x 認証プロセスには、次のステップがあります。

- 未認証のクライアントまたは他社製サブリカントが、ユーザー情報とコンプライアンス情報を管理下 802.1x ネットワークスイッチに送信します。
- ネットワークスイッチが、それらの情報を LAN エンフォーサに中継します。認証のために、LAN エンフォーサがユーザー情報を認証サーバーに送信します。RADIUS サーバーが認証サーバーです。
- クライアントがユーザーレベルの認証に失敗するか、ホストインテグリティポリシーに準拠していない場合は、エンフォーサはネットワークアクセスを遮断できます。エンフォーサは、非準拠のクライアントコンピュータを修復可能な検疫ネットワークに入れます。
- クライアントがコンピュータを修復し、準拠させると、802.1x プロトコルがコンピュータを再認証し、ネットワークへのアクセス許可を与えます。

LAN エンフォーサと連携して働くためには、クライアントは他社製または組み込みのサブ  
リカントを使用する必要があります。

表 7-2 に、802.1x 認証用に設定可能なオプションの種類を示します。

表 7-2 802.1x 認証オプション

オプション	説明
他社製サブリカント	<p>他社製の 802.1x サブリカントを使います。</p> <p>LAN エンフォーサは RADIUS サーバーおよび他社製の 802.1x サブリカントと連携して、ユーザー認証を行います。802.1x サブリカントは、ユーザーに対して、LAN エンフォーサがユーザーレベル認証のために RADIUS サーバーに渡すユーザー情報を求めます。クライアントがクライアントプロファイルとホストインテグリティの状態をエンフォーサに送信することで、エンフォーサがそのコンピュータを認証します。</p> <p><b>メモ:</b> Symantec Network Access Control クライアントを他社製サブリカントと一緒に使う場合、Symantec Endpoint Protection クライアントのネットワーク脅威防止モジュールをインストールしておく必要があります。</p>
透過モード	<p>クライアントを 802.1x サブリカントとして使います。</p> <p>管理者がユーザー認証に RADIUS サーバーを使用しないことに決めた場合、ユーザーはこの方法を使用します。LAN エンフォーサは透過モードで動作し、擬似 RADIUS サーバーとして動作します。</p> <p>透過モードとは、サブリカントからユーザー情報を要求されないことを意味します。透過モードでは、クライアントが 802.1x サブリカントとして機能します。クライアントは、スイッチの EAP チャレンジに応答して、クライアントプロファイルとホストインテグリティ状態を渡します。スイッチはこの情報を LAN エンフォーサに転送し、LAN エンフォーサは疑似 RADIUS サーバーとして機能します。LAN エンフォーサはスイッチから受信したホストインテグリティとクライアントプロファイルの情報の有効性を確認して、VLAN の許可、遮断、動的割り当てを行うことができます。</p> <p><b>メモ:</b> クライアントを 802.1x サブリカントとして使うには、他社製の 802.1x サブリカントをクライアントコンピュータからアンインストールするか、無効にする必要があります。</p>
組み込みサブリカント	<p>クライアントコンピュータの組み込み 802.1x サブリカントを使います。</p> <p>組み込み認証プロトコルには、スマートカード、PEAP、TLS などがあります。802.1x 認証を有効にした後、使用する認証プロトコルを指定する必要があります。</p>

---

**警告:**802.1x 認証用にクライアントを設定する前に、管理者に連絡してください。社内ネットワークで認証サーバーとして RADIUS サーバーを使っているかどうかを確認する必要があります。802.1x 認証を正しく設定しないと、ネットワークへの接続が途絶えることがあります。

---

他社製サブリカントを使うようにクライアントを設定するには

- 1 クライアントのサイドバーで、[状態]をクリックします。
- 2 [Symantec Network Access Control]の隣で、[オプション]、[設定の変更]、[802.1x の設定]の順に選択します。
- 3 [Symantec Network Access Control の設定]ダイアログボックスで、[802.1x 認証を有効にする]をクリックします。
- 4 [OK]をクリックします。

また、ユーザーは、ネットワークへの他社製の 802.1x サブリカントドライバの適用を許可するようにファイアウォールルールを設定する必要もあります。

p.106 の「[ファイアウォールルールの追加](#)」を参照してください。

組み込みサブリカントを使うようにクライアントを設定できます。クライアントを 802.1x 認証向けに有効にし、802.1x サブリカントとしても有効にします。

透過モードまたは組み込みサブリカントを使用するようにクライアントを設定するには

- 1 クライアントのサイドバーで、[状態]をクリックします。
- 2 [Symantec Network Access Control]の隣で、[オプション]、[設定の変更]、[802.1x の設定]の順に選択します。
- 3 [Symantec Network Access Control の設定]ダイアログボックスで、[802.1x 認証を有効にする]をクリックします。
- 4 [クライアントを 802.1x サブリカントとして使う]をクリックします。
- 5 次の処理のいずれかを実行します。
  - 透過モードを選択するには、[シマンテック透過モードを使う]にチェックマークを付けます。
  - 組み込みサブリカントを設定するために、[認証プロトコルを選択できます]をクリックします。  
次に、ネットワーク接続用の認証プロトコルを選択する必要があります。
- 6 [OK]をクリックします。

#### 認証プロトコルを選択するには

- 1 クライアントコンピュータで、[スタート]、[コントロールパネル]、[ネットワーク接続]の順に選択し、[ローカルエリア接続]をクリックします。
- 2 [ローカルエリア接続の状態]ダイアログボックスで、[プロパティ]をクリックします。
- 3 [ローカルエリア接続のプロパティ]ダイアログボックスで、[認証]タブをクリックします。
- 4 [認証]タブで、[EPAの種類]ドロップダウンリストをクリックし、次のいずれかの認証プロトコルを選択します。
  - スマートカードまたはその他の証明書
  - 保護された EAP (PEAP)
  - シマンテック NAC 透過モード

[このネットワークで IEEE 802.1X を有効にする]チェックボックスにチェックマークが付いていることを確認します。
- 5 [OK]をクリックします。
- 6 [閉じる]をクリックします。

## コンピュータの再認証

ホストインテグリティ検査に成功したコンピュータをエンフォーサが遮断している場合、そのコンピュータの再認証が必要な場合があります。通常の場合、ユーザーがコンピュータを再認証する必要はありません。

次のいずれかのイベントが発生すると、エンフォーサがコンピュータを遮断することがあります。

- ユーザー名またはパスワードの入力が正しくないために、クライアントコンピュータがユーザー認証に失敗した場合
- クライアントコンピュータが誤った VLAN に入っている場合
- クライアントコンピュータがネットワーク接続を確立しない場合。ネットワーク接続が確立されない主な原因は、クライアントコンピュータと LAN エンフォーサとの間のスイッチがユーザー名とパスワードを認証しなかったことです。
- 前のユーザーを認証したクライアントコンピュータにログオンする必要がある場合
- クライアントコンピュータがコンプライアンス検査に失敗した場合。

ユーザーまたは管理者が組み込みサブリカントを使用してコンピュータを設定した場合にのみ、コンピュータを再認証できます。

---

**メモ:** 管理者が、再認証コマンドを表示しないようにクライアントを設定していることがあります。

---

#### コンピュータを再認証するには

- 1 通知領域アイコンを右クリックします。
- 2 [再認証]をクリックします。
- 3 [再認証]ダイアログボックスで、ユーザー名とパスワードを入力します。
- 4 [OK]をクリックします。



# 4

## 監視とログ記録

- [第8章 ログの使用と管理](#)



# ログの使用と管理

この章では以下の項目について説明しています。

- ログについて
- ログサイズの管理
- リスクログと脅威ログからのリスクと脅威の検疫
- ネットワーク脅威防止ログとクライアント管理ログの使用
- ログデータのエクスポート

## ログについて

ログにはクライアント設定の変更、セキュリティに関する活動、エラーについての情報が含まれています。これらの記録はイベントと呼ばれます。ログには、これらのイベントと追加の関連情報が表示されます。

セキュリティに関する活動にはウイルス検出、コンピュータ状態、コンピュータから送受信されるトラフィックについての情報が含まれています。管理下クライアントを使用する場合は、ログが定期的に管理サーバーにアップロードされます。管理者はこれらのデータを使用して、ネットワーク全体のセキュリティ状態を分析することができます。

ログは、コンピュータの活動や、他のコンピュータやネットワークとの通信を追跡するための重要な手段です。ログに記録された情報を使用して、ウイルス、セキュリティリスク、コンピュータに対する攻撃に関する傾向を追跡できます。複数のユーザーが同じコンピュータを使用する場合、誰がリスクを持ち込んだかを識別し、そのユーザーに予防措置を取らせることができます。

ログについて詳しくは、F1 キーを押してそのログのヘルプを表示できます。

表 8-1 に各ログが表示するイベントの種類を記述します。

表 8-1 クライアントログ

ログ	説明
スキャンログ	期間内にコンピュータで実行したスキャンに関するエントリが含まれます。
リスクログ	コンピュータに感染したウイルスとセキュリティリスク(アドウェアやスパイウェアなど)に関するエントリが含まれます。セキュリティリスクには、詳細情報を提供するシマンテックセキュリティレスポンス <b>Web</b> ページへのリンクが含まれます。
ウイルス対策とスパイウェア対策のシステムログ	ウイルスとセキュリティリスクに関連するコンピュータシステムの活動に関する情報が含まれます。この情報には、設定の変更、エラー、定義ファイルの情報が含まれます。
脅威ログ	<b>TruScan</b> プロアクティブ脅威スキャンがコンピュータで検出した脅威に関する情報が含まれます。これらには、悪質な目的で使用される可能性のある商用アプリケーションが含まれます。例として、トロイの木馬、ワーム、キーロガー、大量メール送信型ワーム、スクリプトベースの脅威などがあります。
プロアクティブ脅威防止のシステムログ	<b>TruScan</b> プロアクティブ脅威スキャンに関連するコンピュータシステムの活動に関する情報が含まれます。
トラフィックログ	ファイアウォールのトラフィックと侵入防止攻撃にかかわるイベントが含まれます。ログにはコンピュータがネットワークを通じて行った接続に関する情報が含まれます。  ネットワーク脅威防止のログでは、ポートスキャンなどの脅威となる可能性のある活動を検出できます。また、トラフィックの送信元を突きとめるために使用することもできます。ネットワーク脅威防止のログを使用して、接続に関する問題を解決したり、ネットワーク攻撃の可能性を検出することもできます。ログから、コンピュータがいつネットワークから遮断されたかを確認したり、アクセスが遮断された理由を判断することができます。
パケットログ	コンピュータのポートを通過するデータのパケットに関する情報が含まれます。  デフォルトでは、パケットログは無効になります。管理下クライアントでは、パケットログを有効にできません。管理外クライアントでは、パケットログを有効にできます。
制御ログ	制御ログには、アプリケーションがアクセスする <b>Windows</b> レジストリキー、ファイル、 <b>DLL</b> に関する情報や、コンピュータが実行するアプリケーションに関する情報が含まれます。

ログ	説明
セキュリティログ	コンピュータに対して行われた潜在的に脅威を与えることがある活動に関する情報が含まれます。活動の例として、サービス拒否攻撃、ポートスキャン、実行可能ファイルの改変などがあります。
クライアント管理のシステムログ	コンピュータで起きたすべての操作上の変更に関する情報が含まれます。たとえばサービスが開始または停止したとき、コンピュータがネットワークアプリケーションを検出したとき、ソフトウェアが設定されたとき、グループ更新プロバイダ (GUP) として動作するクライアントの状態などの活動があります。
改変対策ログ	コンピュータのシマンテック製アプリケーションを改変する試みに関するエントリが含まれます。これらのエントリには、改変対策が検出した試み、または検出および阻止した試みに関する情報が含まれます。
デバッグログ	トラブルシューティングを行うためのクライアント、スキャン、ファイアウォールに関する情報が含まれます。管理者はログを有効または設定してからエクスポートするように要求することがあります。

## ログサイズの管理

ログにエントリを保存する期間を設定できます。古いエントリを削除することで、ログに使用されるディスク領域を節約できます。ネットワーク脅威防止ログとクライアント管理ログについては、使用する領域も設定できます。

### ウイルス対策とスパイウェア対策ログのエントリの保持期間の設定

ウイルス対策とスパイウェア対策ログのエントリの保持期間を設定するには

- 1 クライアントで、[状態]ページの[ウイルス対策とスパイウェア対策]の隣にある[オプション]をクリックし、[設定の変更]をクリックします。
- 2 [全般]タブで、これらのログにエントリを保持する期間を示す数値と時間の単位を設定します。ここで設定した値よりも古いエントリは削除されます。
- 3 [OK]をクリックします。

### ネットワーク脅威防止ログとクライアント管理ログのサイズの設定

ネットワーク脅威防止ログとクライアント管理ログのそれぞれについてログのサイズを設定できます。

#### ログのサイズを変更するには

- 1 クライアントで、[状態]ページの[ネットワーク脅威防止]の右側にある[オプション]をクリックし、次に[設定の変更]をクリックします。
- 2 [ネットワーク脅威防止の設定]ダイアログボックスの[ログ]タブで、[最大ログファイルサイズ]テキストフィールドにログファイルの最大サイズを KB 単位で入力します。  
コンピュータで使用できる領域は限られているため、ログファイルのサイズは小さくしておく必要があります。制御ログとバケットログを除き、すべてのログのデフォルトサイズは 512 KB です。制御ログとバケットログのデフォルトサイズは 1024 KB です。
- 3 [OK]をクリックします。

## ネットワーク脅威防止ログエントリとクライアント管理ログエントリの保持日数の設定

各ログにエントリが保存される日数を指定できます。最大日数に到達した後は、最も古いエントリが置換されます。領域を節約するにはエントリを削除し、コンピュータのセキュリティを見直すにはエントリを保持すると便利です。

#### ログエントリを保持する日数を設定するには

- 1 クライアントで、[状態]ページの[ネットワーク脅威防止]の右側にある[オプション]をクリックし、次に[設定の変更]をクリックします。
- 2 [ネットワーク脅威防止の設定]ダイアログボックスの[ログ]タブで、[ログエントリを保存する期間]テキストフィールドに、ログエントリを保存する最大日数を入力します。
- 3 [OK]をクリックします。

## ウイルス対策とスパイウェア対策のシステムログの内容の削除について

ユーザーインターフェースを使用して、システムログからイベントの記録を永続的に削除することはできません。

## ネットワーク脅威防止ログとクライアント管理ログの内容の削除

管理者が許可した場合は、ネットワーク脅威防止ログとクライアント管理ログの内容を消去できます。ログを消去した後、各ログはすぐにエントリの保存を再開します。

---

**メモ:** [消去]オプションが利用できない場合は、ログの内容を削除する権限がありません。権限がある場合は、ログの内容をログの[ファイル]メニューから消去することもできます。

---

ログの内容を削除するには

- 1 クライアントで、[状態]ページの[ネットワーク脅威防止]の右側にある[オプション]をクリックし、次に[設定の変更]をクリックします。
- 2 [ネットワーク脅威防止の設定]ダイアログボックスで、削除するログの隣にある[ログ]タブをクリックし、[ログの消去]をクリックします。
- 3 確認のメッセージが表示されたら、[はい]をクリックします。
- 4 [OK]をクリックします。

## リスクログと脅威ログからのリスクと脅威の検疫

プロアクティブ脅威防止の脅威ログに記録されている脅威を検疫できます。ウイルス対策とスパイウェア対策のリスクログから、リスクを検疫できます。また、ウイルス対策とスパイウェア対策のリスクログから、リスクをクリーニングして削除することもできます。

リスクまたは脅威を検疫するには

- 1 クライアントのサイドバーで、[ログの表示]をクリックします。
- 2 [ウイルス対策とスパイウェア対策]または[プロアクティブ脅威防止]の隣にある[ログの表示]をクリックし、目的のログの名前をクリックします。
- 3 リスクまたは脅威を選択して、[検疫]をクリックします。

選択した処理を Symantec Endpoint Protection が実行できるかどうかは、リスク検出に対して事前設定した処理に基づきます。脅威またはリスクが検疫に送られると、成功のメッセージが表示されます。このリスクまたは脅威からコンピュータを保護するために、これ以上の処理を行う必要はありません。リスク検出のために検疫されたファイルは、検疫に残すことも削除することもできます。これらのファイルは、コンピュータのアプリケーションが機能を失っていないことが確認できるまでは検疫に置いたままにしてください。

p.79 の「[検疫にある感染ファイルについて](#)」を参照してください。

Symantec Endpoint Protection がリスクまたは脅威を検疫に送ることができない場合は、エラーメッセージが表示されます。この場合は管理者に連絡してください。

リスクと脅威をクリーニングして削除したり、必要に応じてログから処理を元に戻したりすることもできます。

p.16 の「[感染ファイルへの対応](#)」を参照してください。

## ネットワーク脅威防止ログとクライアント管理ログの使用

ネットワーク脅威防止ログとクライアント管理ログを利用すると、コンピュータの活動や、他のコンピュータやネットワークとの通信を追跡できます。これらのログには、ネットワーク接

続を使ってコンピュータと送受信しようとするトラフィックに関する情報が記録されます。さらに、クライアントに適用されているファイアウォールポリシーの結果に関する情報も記録されます。

ネットワーク脅威防止クライアントログとクライアント管理クライアントログは集中的に管理できます。セキュリティログ、トラフィックログ、パケットログを利用すると、一部のデータを送信元まで追跡できます。追跡では、ICMP を使ってユーザーのコンピュータと別のコンピュータ上の侵入者との間にあるホップがすべて特定されます。

---

**メモ:** 管理者がクライアントに設定した制御の種類に基づき、これらのログの一部のオプションは利用できない場合があります。

---

## ネットワーク脅威防止ログとクライアント管理ログの更新

ログを更新するには

- 1 クライアントのサイドバーで、[ログの表示]をクリックします。
- 2 [ネットワーク脅威防止]または[クライアント管理]の右側にある[ログの表示]をクリックし、更新するログの名前をクリックします。
- 3 [表示]メニューで、[更新]をクリックします。

## パケットログの有効化

ネットワーク脅威防止ログとクライアント管理ログは、パケットログを除き、デフォルトで有効です。管理者が許可している場合は、パケットログを有効または無効にすることができます。

パケットログを有効にするには

- 1 クライアントで、[状態]ページの[ネットワーク脅威防止]の右側にある[オプション]をクリックし、次に[設定の変更]をクリックします。
- 2 [ネットワーク脅威防止の設定]ダイアログボックスで、[ログ]をクリックします。
- 3 [パケットログを有効にする]にチェックマークを付けます。
- 4 [OK]をクリックします。

## アクティブレスポンスの停止

クライアントで検出された侵入は、アクティブレスポンスをトリガします。アクティブレスポンスは、既知の侵入者の IP アドレスを一定時間、自動的に遮断します。管理者が許可する場合は、セキュリティログログでアクティブレスポンスを停止できます。

p.120 の「[攻撃側コンピュータの遮断と遮断解除](#)」を参照してください。

## ログに記録されたイベントの送信元の追跡

ログに記録された一部のイベントをさかのぼって、データの送信元を突きとめることができます。犯罪の現場で犯人の足取りをたどる刑事のように、着信トラフィックの正確な足跡（ホップ）を明らかにします。ホップは、パケットがインターネットでコンピュータからコンピュータに移動するときに通る、ルーターなどの通過点です。データがコンピュータに届くまでにどのルーターを利用したかを明らかにすることで、データパケットを逆方向に追跡します。

一部のログエントリでは、攻撃の試みに使用されたデータパケットを追跡できます。データパケットが通過した各ルーターには、IP アドレスが割り当てられています。この IP アドレスとその他の情報を確認できます。表示される情報が、本当のハッカーを示しているとは限りません。最終的なホップの IP アドレスは、ハッカーが接続したルーターの所有者のリストを示し、この人物がハッカー自身であるとは限りません。

セキュリティログやトラフィックログに記録された一部のイベントを追跡できます。

### ログに記録されたイベントを追跡するには

- 1 クライアントのサイドバーで、[ログの表示]をクリックします。
- 2 [ネットワーク脅威防止]または[クライアント管理]の右側にある[ログの表示]をクリックします。次に、追跡するエントリを含むログをクリックします。
- 3 ログ表示ウィンドウで、追跡するエントリの行を選択します。
- 4 [処理]をクリックし、次に[バックトレース]をクリックします。
- 5 [バックトレース情報]ダイアログボックスで、[Who is >>]をクリックし、各ホップの詳細情報を表示します。  
  
ドロップパネルに、トラフィックイベントが発生した IP アドレスの所有者に関する詳細な情報が表示されます。Ctrl+C と Ctrl+V を使用してパネルの情報をコピーし、管理者への電子メールメッセージに貼り付けることができます。
- 6 [Who is <<] をもう一度クリックして、情報を非表示にします。
- 7 確認が終わったら、[OK]をクリックします。

## Symantec Network Access Control でのクライアント管理ログの使用

Symantec Network Access Control をインストールすると、セキュリティログとシステムログの[処理]メニューから次のタスクが実行できます。

- ポリシーの更新  
p.28 の「[ポリシーファイルを手動で更新](#)」を参照してください。
- ホストインテグリティ検査  
p.125 の「[ホストインテグリティ検査の実行](#)」を参照してください。

## ログデータのエクスポート

ログの情報を、カンマ区切りの値 (.csv) または Access データベース (\*.mdb) 形式でエクスポートすることができます。.csv 形式は、多くのスプレッドシートプログラムやデータベースプログラムで、データをインポートするために使用される一般的なファイル形式です。データを別のプログラムにインポートすると、データを使用してプレゼンテーションやグラフを作成したり、他の情報と組み合わせることができます。ネットワーク脅威防止ログやクライアント管理ログの情報は、タブ区切りのテキストファイルにエクスポートできます。

---

**メモ:** Windows Server 2008 Server Core でクライアントソフトウェアを実行する場合には、ログデータを .mdb ファイルにエクスポートできません。.mdb 形式には Server Core で利用できない Microsoft アプリケーションが必要です。

---

次のログを .csv または .mdb ファイルにエクスポートできます。

- ウイルス対策とスパイウェア対策のシステムログ
- ウイルス対策とスパイウェア対策のリスクログ
- ウイルス対策とスパイウェア対策のスキャンログ
- プロアクティブ脅威防止のシステムログ
- プロアクティブ脅威防止の脅威ログ
- 改変対策ログ

---

**メモ:** ログデータをフィルタ処理してからエクスポートすると、現在フィルタ処理されているデータだけがエクスポートされます。この条件は、タブ区切りのテキストファイルにエクスポートするログには適用されません。これらのログでは、すべてのデータがエクスポートされます。

---

次のログをタブ区切りの .txt ファイルにエクスポートできます。

- クライアント管理の制御ログ
- ネットワーク脅威防止のパケットログ
- クライアント管理のセキュリティログ
- クライアント管理のシステムログ
- ネットワーク脅威防止のトラフィックログ

---

**メモ:** タブ区切りのテキストファイルに加え、パケットログのデータを Network Monitor 形式または NetXray 形式でエクスポートすることもできます。

---

Windows Server 2008 の Server Core のインストールでは、ユーザーインターフェースのダイアログボックスが、以下の手順で説明するものと異なることがあります。

#### データを .csv ファイルにエクスポートするには

- 1 クライアントのサイドバーで、[ログの表示]をクリックします。
- 2 [ウイルス対策とスパイウェア対策]または[プロアクティブ脅威防止]のいずれかの隣にある[ログの表示]をクリックします。
- 3 エクスポートするログの名前をクリックします。
- 4 ログウィンドウで、保存するデータが表示されていることを確認し、[エクスポート]をクリックします。
- 5 [保存する場所]ドロップダウンリストで、ファイルの保存先ディレクトリを参照します。
- 6 [ファイル名]テキストボックスで、ファイルの名前を入力します。
- 7 [保存]をクリックします。
- 8 [OK]をクリックします。

#### ネットワーク脅威防止ログデータまたはクライアント管理ログデータをテキストファイルに保存するには

- 1 クライアントのサイドバーで、[ログの表示]をクリックします。
- 2 [ネットワーク脅威防止]または[クライアント管理]の右側にある[ログの表示]をクリックします。
- 3 データをエクスポートするログの名前をクリックします。
- 4 [ファイル]をクリックし、次に[エクスポート]をクリックします。  
パケットログを選択した場合は、[Network Monitor 形式にエクスポート]または[Netxray 形式にエクスポート]をクリックできます。
- 5 [保存する場所]ドロップダウンリストで、ファイルの保存先ディレクトリを参照します。
- 6 [ファイル名]テキストボックスで、ファイルの名前を入力します。
- 7 [保存]をクリックします。
- 8 [ファイル]、[終了]の順に選択します。



## 記号

- 64 ビットコンピュータ 30
- 802.1x 認証
  - 概要 127
  - 設定 129

## A

### Auto-Protect

- Lotus Notes 用 54
- Microsoft Exchange クライアント用 54
- 暗号化電子メール接続 55
- インターネット電子メール用 54
- 拡張子によるスキャン 51
- グループウェア電子メールクライアント 54
- 使用 53
- スキャン統計の表示 56
- セキュリティリスク 53
- セキュリティリスクスキャンの無効化 57
- ネットワークキャッシュ 59
- ネットワークスキャンの設定 58
- ファイルの種類の特定 57
- 有効化または無効化 31、33
- リスクリストの表示 56
- リモートバージョンの信頼 59

## I

### IPS

- 概要 98
- 定義の更新 26

## L

### LiveUpdate

- 概要 26
- すぐに実行 27
- スケジュールの作成 27

## M

- MAC 詐称対策
  - 有効化 110

## N

- NetBIOS の保護
  - 有効化 110

## S

- Symantec Network Access Control
  - 通知 21

## T

### TruScan プロアクティブ脅威スキャン

- 概要 87～88
- 感度レベル 93
- 管理 91
- 検出 89
- 検出するプロセスの種類 94
- 誤認 90
- 情報の提出 95
- 商用アプリケーション 92
- 処理 93
- 通知 94
- 頻度 91
- 例外 96
- ログ 136

## U

- UDP 接続
  - 概要 104

## W

- Windows セキュリティセンター
  - ウイルス対策状態の確認 85
  - ファイアウォール状態の確認 86

## あ

- アイコン
  - 錠前 25
  - シールド 39
- アクティブスキャン
  - 実行 63

アクティブレスポンス

概要 120

アダプタ

定義済み 103

アドウェア 47

アプリケーション

許可または遮断 106、114

スキャンからの除外 77

定義済み 103

ウイルス

概要 46

クライアントの応答 49

クライアントの検出 61

検出オプション 74

検出されたときの処理 52

修復オプション 74

処理の設定 69

第2の処理の割り当て 72

通知の設定 74

認識されない 84

ファイルの損傷 17

ウイルス対策とスパイウェア対策

概要 12、50

システムログ 136

無効化 31、33

ウイルス定義

概要 61

更新 26～27

オプション

利用不能 24

オンデマンドスキャン

拡張子によるスキャン 51

作成 65

実行 29

## か

改変対策

概要 35

設定 36

有効化と無効化 36

改変対策ログ 137

拡張子

スキャンの対象 51

カスタムスキャン

実行 63

完全スキャン

実行 63

感染ファイル

対応 16

管理外クライアント。「自己管理クライアント」を参照  
管理下クライアント。「集中管理下クライアント」を参照  
起動時スキャン

拡張子によるスキャン 51

作成 65

編集と削除 66

脅威ログ 136

クライアント

概要 11

集中管理と自己管理 24

操作 15

保護の無効化 31

検疫 79

感染ファイルの扱い方 79

感染ファイルの表示 79

管理 80

シマンテックセキュリティレスポンスへのファイルの提出 84

手動によるファイルの再スキャン 82

手動によるファイルの削除 83

セキュリティリスクに感染したファイルの扱い方 80

バックアップファイルの削除 82

ファイルの移動 79

ファイルの解放 82

ファイルの削除 80、83

ファイルの自動再スキャン 81

ファイルの詳細の表示 81

検出率

シマンテック社への情報の送信 84

攻撃側コンピュータの遮断 120

攻撃側コンピュータの遮断解除 120

更新

定義 26～27

コンピュータ

保護の更新 26

コンピュータのテスト 37

## さ

再認証 130

サーバー

管理下クライアント 24

接続先 39

自己管理クライアント

概要 24

集中管理 24

システムトレイアイコン 39

システムログ

ウイルス対策とスパイウェア対策 136

エントリの削除 138

クライアント管理 137  
 プロアクティブ脅威防止 136

実施  
 概要 127

シマンテックセキュリティレスポンス  
 ファイルの提出 84

集中管理下クライアント  
 自己管理クライアント 24

集中例外  
 TruScan プロアクティブ脅威スキャンの検出に対す  
 る 96  
 概要 77  
 作成 77

手動スキャン。「オンデマンドスキャン」を参照

錠前アイコン 25

処理  
 ウイルスに対する第 2 の処理の割り当て 72  
 セキュリティリスクに対する第 2 の処理を割り当てる  
 ためのヒント 73

シールドアイコン 39

侵入防止。「IPS」を参照  
 応答 21  
 概要 117  
 通知 119  
 有効化または無効化 119

スキャン。「ウイルス対策とスパイウェア対策」を参照

TruScan プロアクティブ脅威スキャンからの除外 96  
 圧縮ファイル 62  
 一時停止 30  
 オンデマンドと起動 65  
 拡張子によるファイルのスキャン 51  
 休止オプション 30  
 結果の解釈 67  
 実行 29  
 スキャンするコンポーネント 60  
 すべてのファイルの種類 52  
 遅延 30  
 定時 62  
 動作 60  
 ファイル 50  
 ファイルとフォルダの除外 77

スキャン例外。「集中例外」を参照

スキャンログ 136

スタンドアロンクライアント。「自己管理クライアント」を参照

ステートフルインスペクション  
 概要 104  
 トラフィックのルールの作成 104

ステルスモードの Web 参照  
 有効化 110

スパイウェア  
 概要 48

スマート DHCP 110

スマート DNS 110

スマート WINS 110

スマートトラフィックフィルタ  
 定義済み 109  
 有効化 110

制御ログ 136

セキュリティリスク  
 オプション 74  
 概要 47  
 クライアントの応答 49  
 クライアントの検出 61  
 検出されたときの処理 52  
 修復オプション 74  
 処理の設定 69  
 スキャンからの除外 77  
 第 2 の処理を割り当てるためのヒント 73  
 ダウンロードを続行するプロセス 53  
 通知の設定 74

セキュリティリスクスキャン  
 Auto-Protect での無効化 57

セキュリティログ 137

設定  
 侵入防止 119  
 設定のロックとロック解除 25  
 ゼロデイ攻撃防止 87

## た

通知  
 応答 18  
 概要 15  
 侵入防止 119  
 ネットワークアクセス制御 21  
 ユーザー操作 67

通知領域アイコン  
 概要 39  
 非表示と表示 40

定義  
 概要 61  
 更新 26~27

定義ファイル 62

定時スキャン  
 拡張子によるスキャン 51  
 作成 62  
 複数 63  
 編集と削除 66

デバッグログ 137

## 電子メール

暗号化接続 55

検疫から添付ファイルを解放 82

受信ボックスファイルをスキャンから除外 50

電子メールスキャン。「Auto-Protect」を参照

トークンリングトラフィック

有効化 110

ドライブレベルの保護

有効化 110

トラフィック

許可または遮断 114

遮断 113

トラフィックとステルスの設定 110

定義済み 109

トラフィックの許可 114

ファイアウォールルール 106

トラフィックの遮断 113～114

ファイアウォールルール 106

トラフィックログ 99、136

トロイの木馬

概要 47

## な

ネットワークアクセス制御

概要 14、123

コンピュータの修復 125

実施 127

ネットワークキャッチ

Auto-Protect 設定 59

ネットワーク脅威防止

概要 14、98

管理 98

有効化または無効化 32、34

ログ 136

ネットワークスキャン

Auto-Protect 設定 58

## は

パケットログ 136

有効化 140

場所

概要 38

変更 38

ハッキングツール 48

バックアップ項目フォルダ

消去 82

ファイアウォール

管理 98

定義済み 98

有効化または無効化 34

ファイアウォールルール

インポート中 108

エクスポート 108

概要 101～102

順序の変更 105、107

スケジュール設定 102

追加 106

有効化と無効化 108

ログへの記録 102

ファイル

共有 111

検疫からファイルを解放 82

検疫にあるファイルの自動再スキャン 81

検疫にあるファイルの手動再スキャン 82

シマンテックセキュリティレスポンスへの提出 84

修復後の場所 82

スキャン 50

スキャンからの除外 77

バックアップ 82

ファイルシステム Auto-Protect

有効化または無効化 33

ファイルとプリンタの共有 111

プリンタの共有 111

プロアクティブ脅威スキャン。「TruScan プロアクティブ脅

威スキャン」を参照

プロアクティブ脅威防止

概要 13

有効化または無効化 32、35

プロトコル

定義済み 103

保護

更新 26～27

種類 11

有効化または無効化 31

ホスト

定義済み 103

ホストインテグリティ検査

実行中 125

ポリシー

概要 28

更新 28

## ま

マクロウイルス感染

防止 52

無効化

Auto-Protect 31、33

ウイルス対策とスパイウェア対策 31

ネットワーク脅威防止 32、34

プロアクティブ脅威防止 32、35

メッセージ

応答 18

侵入防止 119

## や

有効化

Auto-Protect 33

ネットワーク脅威防止 34

プロアクティブ脅威防止 35

ユーザー定義スキャン

編集と削除 66

## ら

リスク。「セキュリティリスク」を参照

リスクの影響評価 73

リスクログ 136

例外

TruScan プロアクティブ脅威スキャン 77、96

変更対策 77

概要 77

スキャンへの追加 77

ログ

エクスポート形式 142

エントリの追跡 141

エントリを保存する期間の設定 137～138

概要 135

クライアント管理 139

更新 140

サイズの制限 137

サイズの設定 137

削除 138

データのエクスポート 142

ネットワークアクセス制御 126

ネットワーク脅威防止 139

バケットログの有効化 140

フィルタ処理したログエントリのエクスポート 142

リスクと脅威の検疫 139

## わ

ワーム 47