

シマンテック中央検疫実装ガイド

シマンテック中央検疫実装ガイド

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。

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 の規定によって商業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。

| | | |
|--------------|---|----|
| 第 1 章 | シマンテック中央検疫の紹介 | 5 |
| | シマンテック中央検疫について | 5 |
| | 中央検疫のコンポーネントについて | 6 |
| | 中央検疫の動作 | 6 |
| | ウイルスの識別と検疫について | 7 |
| | ウイルスの分析について | 7 |
| | 中央検疫でできること | 8 |
| | 中央検疫についての詳しい情報を入手するには | 8 |
| 第 2 章 | 中央検疫のインストールと設定 | 11 |
| | インストール前にすること | 11 |
| | 中央検疫サーバーのシステム必要条件 | 12 |
| | 検疫コンソールのシステム必要条件 | 12 |
| | 中央検疫のインストール | 12 |
| 第 3 章 | 中央検疫の使用方法 | 15 |
| | 中央検疫について | 15 |
| | 検疫サーバーの有効化 | 16 |
| | 検疫サーバーの設定 | 16 |
| | 検疫サーバーを使用するためのウイルス対策とスパイウェア対策のポリシー の設定 | 17 |
| | 中央検疫のプロパティについて | 18 |
| | 検疫ファイルの管理 | 19 |
| | 検疫項目の表示方法 | 20 |
| | 検疫ファイルの削除 | 21 |
| | 検疫ファイルの復元 | 21 |
| | 分析用サンプルの提出 | 21 |
| | サンプルの自動提出ポリシーの設定 | 22 |
| | ファイルの手動提出 | 22 |
| | サンプル提出状態の見直し | 23 |
| | サンプル属性の表示方法 | 23 |
| | サンプルに適用される処理の見直し | 23 |
| | サンプルの提出エラーの見直し | 24 |
| | イベントと警告の設定 | 24 |

| | | |
|-----------------|---------------------------|-----------|
| | 警告のトリガになるイベントの指定 | 24 |
| 付録 A | サンプル処理リファレンス | 27 |
| | サンプル処理について | 27 |
| | サンプルの処理状態 | 27 |
| | サンプルの分析状態 | 28 |
| | 最終状態 | 28 |
| | 移行状態 | 30 |
| | 保留状態 | 30 |
| | 活動状態 | 30 |
| | サンプルエラー | 32 |
| 索引 | | 35 |

シマンテック中央検疫の紹介

この章では以下の項目について説明しています。

- [シマンテック中央検疫について](#)
- [中央検疫のコンポーネントについて](#)
- [中央検疫の動作](#)
- [中央検疫でできること](#)
- [中央検疫についての詳しい情報を入手するには](#)

シマンテック中央検疫について

Symantec Endpoint Protection は、現在のウイルス定義で修復できない感染項目を見つけた場合、その項目に対するアクセスを遮断します。その後、この項目に影響するシステムファイルおよび設定をパッケージ化し、そのパッケージをローカル検疫に移動します。ローカル検疫は、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。ウイルスなどの脅威はローカル検疫に隔離されると、コンピュータに損傷を与えたり伝染したりすることができなくなります。

Symantec Endpoint Protection では、感染ファイルとそれらの関連する副作用が格納されたパッケージをローカル検疫から中央検疫に自動的に転送できます。中央検疫は、中央リポジトリです。中央検疫は検疫サーバーとMMC (Microsoft Management Console の略) スナップインという 2 つのコンポーネントで構成されます。

Symantec Endpoint Protection クライアントは、ファイルのウイルススキャンに加えて、スパイウェア、アドウェア、ハッキングツール、ジョークプログラムなどのファイルのセキュリティリスクをスキャンします。これらの感染ファイルは中央検疫に転送することもできます。プロアクティブ脅威防止で検出して検疫した脅威は、異なるしくみで提出されます。

中央検疫のコンポーネントについて

シマンテック中央検疫のコンポーネントを表 1-1 に示します。

表 1-1 中央検疫のコンポーネント

| コンポーネント | 説明 |
|-------------------|---|
| シマンテックセキュリティレスポンス | 提出物を見直して分析し、更新済みのウイルス定義を作成して配布する自動分析センターです。 |
| ゲートウェイ | シマンテックセキュリティレスポンスと中央検疫の間の中継をします。サンプルは分析され、ゲートウェイにあるウイルス定義で修復できない場合にのみシマンテックセキュリティレスポンスに転送されます。サンプルを修復できる場合、ゲートウェイから中央検疫にウイルス定義が返送されます。 |
| 検疫コンソール | 検疫サーバーの動作の設定、ゲートウェイとの通信、ウイルス定義の更新版の管理のために使う中央検疫のユーザーインターフェースです。 |
| 検疫サーバー | サーバーやクライアントからの感染ファイルと副作用を受け入れて検疫コンソールと通信するコンポーネントです。検疫に届いた項目は検疫サーバーのウイルス定義セットでスキャンされ、修復できない場合には提出されます。検疫サーバーは IP プロトコルを特定のポートで応答準備するように設定されている必要があります。転送する側のクライアントはクライアントの転送用のプロトコルに対応するポートに転送するように設定する必要があります。 |
| 検疫エージェント | 検疫サーバーとゲートウェイの間の通信を扱い、DefCast 機構をトリガするコンポーネントです。検疫エージェントはゲートウェイから中央検疫に最新のウイルス定義セットが確実に届くようにします。 |
| 検疫スキャナ | 提出されたファイルを検疫サーバー自体のウイルス定義セットでスキャンするコンポーネントです。中央検疫に届くサンプルはスキャンしないと提出できません。 |
| DefCast | サーバーやクライアントにウイルス定義シーケンス番号を問い合わせるコンポーネントです。 |

中央検疫の動作

中央検疫は、デジタル免疫システムを使ってウイルス対策処理全体を管理します。デジタル免疫システムにより、提出と分析の処理に関係する手動タスクの多くが不要になります。ウイルスが最初に見つかってから **LiveUpdate** でその修復方法が配備されるまでの時間が自動化によって短縮します。

デジタル免疫システムは次の処理をします。

- 識別と検疫:強力なヒューリスティック検出と動作検出を使って新種の脅威を迅速に識別します。疑わしい項目を中央検疫に隔離し、サンプルを分析用にシマンテックセキュリティレスポンスに自動的に提出します。
- 分析:分析、修復、テストのためにファイルをシマンテックセキュリティレスポンスに提出します。

ウイルスの識別と検疫について

デジタル免疫システムの最も重要な目標はデスクトップ、サーバー、ゲートウェイ上で新種の脅威または未知の脅威を検出することです。シマンテック社は **Bloodhound** ヒューリスティック技術を使います。この技術は新種のウイルスまたは未知のウイルスの種類を大部分を検出するために設計された技術です。

疑わしいファイルと副作用をローカル検疫へ自動的に送信するようにクライアントを設定できます。ローカル検疫は、デスクトップ、サーバー、ゲートウェイのいずれかの場所にあります。疑わしいファイルはローカル検疫で提出元コンピュータについての情報と一緒にパッケージ化されてから、さらに分析するためにローカル検疫から企業の中央検疫に転送されます。

中央検疫には提出元コンピュータよりも新しいウイルス定義があるかもしれないため、中央検疫はファイルのスキャンに中央検疫自体のウイルス定義セットを使います。ファイルを修復できない場合には、秘密情報を含む可能性があるデータをはく離して(そのように設定した場合)ファイルを暗号化します。次にファイルはさらに分析するためにデジタル免疫システムによってインターネット経由で **Symantec** ゲートウェイに送信されます。

管理者はデジタル免疫システムを自動的に次の処理をするように設定できます。

- 新種のウイルスや未知のウイルスを検出して検疫する
- 暗号化したサンプルをフィルタ処理して分析を依頼するために、シマンテックセキュリティレスポンスに転送するデジタル免疫システムは、秘密情報をはく離することができます。
- 新しいウイルス定義や状態の更新がないかどうかを調べる

ウイルスの分析について

検疫エージェントは中央検疫と **Symantec** ゲートウェイの間の通信を扱います。中央検疫が感染ファイルを修復できない場合、そのファイルは検疫エージェントによってゲートウェイに転送されます。次に検疫エージェントは、修復方法が存在するかどうかをゲートウェイに問い合わせます。

修復方法が存在する場合、検疫エージェントは新しいウイルス定義セットをダウンロードしてその新しい定義を中央検疫にインストールします。修復方法が存在しない場合、検疫エージェントは 60 分間隔でゲートウェイにポーリングを行います。

デジタル免疫システムは新しい提出物を受信すると次の処理をします。

- 追跡するデータベースに提出物を追加します。
- 提出物をフィルタ処理して未感染ファイル、誤認、既知のウイルスとセキュリティリスクを取り除きます。フィルタ処理はすばやく、ほとんどの提出物がフィルタ処理で解消されるためフィルタ処理する項目の応答時間は非常に高速です。
- ウイルスと副作用を分析し修復方法を生成してからテストします。ほとんどの場合、分析と修復方法の生成は自動的に行われますが、ウイルスによってはシマンテックセキュリティレスポンスの研究者の操作が必要なことがあります。
- 新しいフィンガープリントを含む新しいウイルス定義セットを構築して、その新しい定義をゲートウェイに返送します。

中央検疫でできること

以前のバージョンの中央検疫は、新たに受信したウイルス定義や脅威の定義をすべてのレガシークライアントにプッシュ型で送信します（検疫される提出物は、クライアントにより中央検疫に送信されます）。現在のバージョンの中央検疫でも、提出物をシマンテックセキュリティレスポンスに送信し、その提出物に対応する更新を受信します。ただし、現在のバージョンでは受信した定義を **Symantec Endpoint Protection** が動作するクライアントにプッシュ型で送信しません。

中央検疫ではネットワーク上のすべての検疫項目を同じ場所に配置するための単一のソースが提供されています。すべての検疫項目は、1 つのウィンドウに表示され、自動的にシマンテックセキュリティレスポンスに送信されます。このウィンドウには、脅威を捕捉したユーザーやコンピュータなどの、提出済みの脅威に関する情報も表示されます。また、提出される未知の脅威を検出するために作成される定義の状態も表示されます。

デジタル免疫システムは提出済みの脅威についての情報を **Symantec Global Intelligence Network** に送信します。**Symantec Global Intelligence Network** では、インターネットセキュリティに関する比類なき高度な分析を提供しています。**Symantec Global Intelligence Network** は、世界中に存在する 1 億 5000 万箇所以上のデスクトップウイルス対策センサー、4 万箇所の侵入検知およびファイアウォールセンサー、4300 箇所の監視および管理されたセキュリティデバイスから構成されます。この情報は、世界で最大規模になる 1 万 3000 エントリのシマンテック社の脆弱性データベースと組み合わせられます。これらのエントリは、4000 社以上の製造元からリリースされている 3 万のアプリケーションのバージョンとオペレーティングシステムに対応しています。

中央検疫についての詳しい情報を入手するには

インストール CD の **Documentation** フォルダに中央検疫についての主要なマニュアルがあります。一部のコンポーネントフォルダには、コンポーネント固有のマニュアルが含ま

れています。マニュアルの更新は、シマンテックのテクニカルサポートおよびプラチナムサポート Web サイトから入手できます。

表 1-2 に、シマンテック社の Web サイトで入手できる追加情報を示します。

表 1-2 シマンテックのテクニカルサポート Web サイト

| 情報の種類 | Web アドレス |
|--|---|
| 一般的なナレッジベース リリースと更新情報 マニュアルと文書 連絡方法 | http://www.symantec.com/business/support/index.jsp |
| ウイルスなどの脅威についての情報と更新情報 | http://www.symantec.com/region/jp/sarcj |
| 製品の最新情報と更新情報 | http://www.symantec.com/ja/jp/business/index.jsp |
| プラチナムサポート Web サイト | https://www-secure.symantec.com/platinum/login.html |

中央検疫のインストールと設定

この章では以下の項目について説明しています。

- [インストール前にすること](#)
- [中央検疫サーバーのシステム必要条件](#)
- [検疫コンソールのシステム必要条件](#)
- [中央検疫のインストール](#)

インストール前にすること

中央検疫をインストールする前に次のことを検討してください。

- 検疫コンソールと検疫サーバーをインストールするには管理者の権利が必要です。インストールする前に適切な権利があることを確認します。
- 中央検疫をインストールする前に、コンピュータにインストールされている以前のバージョンの中央検疫を必ずアンインストールします。
- 中央検疫は検疫サーバーと検疫コンソールで構成されます。検疫サーバーと検疫コンソールは同じコンピュータまたは Windows 2000/XP/2003 の別なコンピュータにインストールできます。
- 検疫コンソールは設定のためにネットワークプロトコル (TCP/IP) を検疫サーバーと共有する必要があります。
- 検疫を使う製品は TCP/IP を使ってファイルを検疫サーバーに転送できます。このネットワークプロトコルが検疫サーバーにインストールされていることを確認します。

中央検疫サーバーのシステム必要条件

システム要件の最新情報については、シマンテック社のテクニカルサポートの日本語 web サイトで確認してください。

検疫コンソールのシステム必要条件

システム要件の最新情報については、シマンテック社のテクニカルサポートの日本語 web サイトで確認してください。

中央検疫のインストール

中央検疫のインストールでは以下のタスクを実施します。

- 検疫コンソールのインストール
- 検疫サーバーのインストール

メモ: コンソールとサーバーはどちらを先にインストールしてもかまいません。

検疫コンソールをインストールするには

- 1 製品 DVD の **CentralQ¥QConsole** フォルダからインストールを開始します。
- 2 [ようこそ]ダイアログボックスで[次へ]をクリックします。
- 3 [使用許諾契約]ダイアログボックスで[使用許諾契約の条項に同意します]を選択します。
- 4 [次へ]をクリックします。
- 5 [インストール先フォルダ]ダイアログボックスで次のいずれかの操作をします。
 - デフォルトのフォルダにインストールするには[次へ]をクリックします。
 - 異なるフォルダを選択するには[変更]をクリックします。
検疫コンソールはネットワークドライブにインストールしないでください。
- 6 画面の指示に従って操作してインストールを完了します。

検疫サーバーをインストールするには

- 1 製品 DVD の **CentralQ¥QServer** フォルダからインストールを開始します。
- 2 [ようこそ]ダイアログボックスで[次へ]をクリックします。
- 3 [使用許諾契約]ダイアログボックスで[使用許諾契約の条項に同意します]を選択します。

- 4 [次へ]をクリックします。
- 5 [インストール先フォルダ]ダイアログボックスで次のいずれかの操作をします。
 - デフォルトのフォルダにインストールするには[次へ]をクリックします。
 - 異なるフォルダを選択するには[変更]をクリックします。

検疫サーバーはネットワークドライブにインストールしないでください。
- 6 [セットアップの種類]ダイアログボックスで[インターネットベース (推奨)]をクリックします。
- 7 [次へ]をクリックします。
- 8 [最大ディスク容量]ダイアログボックスでデフォルトのディスク容量の **500 MB** を受け入れるか、[ディスク容量(MB)]フィールドに新しい値(MB 単位)を入力してから[次へ]をクリックします。
- 9 [連絡先情報]ダイアログボックスに会社名、アカウント番号(利用可能な場合)、連絡先の個人名、電話番号、電子メールアドレスを入力します。
- 10 [次へ]をクリックします。
- 11 [Web通信]ダイアログボックスでデフォルトのゲートウェイアドレスを受け入れるか、[ゲートウェイ名]フィールドに別のアドレス(シマンテック社から提供されたアドレス)を入力してから、[次へ]をクリックします。
- 12 画面の指示に従って操作してインストールを完了します。

中央検疫の使用法

この章では以下の項目について説明しています。

- [中央検疫について](#)
- [検疫サーバーの有効化](#)
- [検疫サーバーの設定](#)
- [検疫サーバーを使用するためのウイルス対策とスパイウェア対策のポリシーの設定](#)
- [中央検疫のプロパティについて](#)
- [検疫ファイルの管理](#)
- [分析用サンプルの提出](#)
- [サンプル提出状態の見直し](#)
- [イベントと警告の設定](#)

中央検疫について

中央検疫は検疫サーバーと検疫コンソールの 2 つの主なコンポーネントで構成されます。検疫サーバーは感染サンプルを格納し、シマンテックセキュリティレスポンスと通信します。検疫コンソールは、**Microsoft Management Console** にスナップインとして組み込まれます。これにより、検疫サーバーを管理することができます。

中央検疫を使うには次の操作をします。

- [検疫サーバーを有効にする](#)
- [検疫サーバーを設定する](#)
- [検疫サーバーにサンプルを転送するためにクライアントを設定する](#)

検疫サーバーの有効化

ローカルコンピュータやリモートコンピュータ上の検疫サーバーを有効にできます。

ローカルコンピュータ上の検疫サーバーを有効にするには

- 1 シマンテック中央検疫コンソールの左ペインで[Symantec 中央検疫]を右クリックして[サーバーに接続]をクリックします。
- 2 [コンピュータの選択]ダイアログボックスで[このコンピュータ]を選択して[OK]をクリックします。

リモートコンピュータ上の検疫サーバーを有効にするには

- 1 シマンテック中央検疫コンソールの左ペインで[Symantec 中央検疫]を右クリックして[サーバーに接続]をクリックします。
- 2 [検疫サーバーに接続]ダイアログボックスでサーバー名を入力します。
- 3 サーバーに接続するためのユーザー名とパスワードを入力します。
- 4 サーバーがドメインの一部であればドメイン名も入力します。

検疫サーバーの設定

次の情報を使って検疫サーバーを設定します。

- 検疫サーバー上のファイルを格納するフォルダの場所
- プロトコルと応答準備ポート

検疫サーバーの設定後にクライアントのローカル検疫にあるファイルの複製を送信するためにクライアントを設定できます。

メモ: 検疫コンソールのユーザーインターフェースでは、IP または SPX プロトコルのどちらかを選択できます。また、設定するポート番号も指定できます。IP プロトコルを選択した場合のポート番号は、TCP の応答準備ポートになります。SPX は選択しないでください。ここで入力した TCP ポート番号は、`netstat -a` のようなツールで表示される番号と異なります。たとえば、ポート番号に 33 と入力する場合でも、`netstat -a` では TCP のポートは 8448 と表示されます。これは、16 進数から 10 進数への変換が適切でないためです。詳しくは、http://service1.symantec.com/support/inter/entsecurityjapanesekb.nsf/jp_docid/20020426165626949?Open&dtype=corp を参照してください。

検疫サーバーを設定するには

- 1 シマンテック中央検疫コンソールの左ペインで[Symantec 中央検疫]を右クリックして[プロパティ]をクリックします。
- 2 [Symantec中央検疫のプロパティ]ダイアログボックスの[一般]タブで中央検疫フォルダの場所を指定します。
- 3 [最大許容サイズ]で検疫の最大サイズを指定します。
- 4 [プロトコル]で、[IP で受信準備] (TCP/IP)にチェックマークを付けます。
[SPX で受信準備]にチェックマークを付けないでください。
- 5 [ポート]フィールドで応答準備するポート番号を入力します。
デフォルトのポート番号は 33 です。
- 6 [OK]をクリックします。

検疫サーバーを使用するためのウイルス対策とスパイウェア対策のポリシーの設定

グループまたはグループの場所にある Symantec Endpoint Protection クライアントでは、検疫サンプルを検疫サーバーに転送するウイルス対策とスパイウェア対策のポリシーを使う必要があります。ポリシーでは、検疫サーバーの完全修飾ドメイン名 (推奨) または IP アドレスを入力する必要があります。また、検疫サーバーの応答準備ポートで指定したプロトコルとポート番号も入力する必要があります。

検疫サーバーを使用するためのウイルス対策とスパイウェア対策のポリシーを設定するには

- 1 Symantec Endpoint Protection Manager コンソールで[ポリシー]をクリックします。
- 2 [ポリシーの表示]で[ウイルス対策とスパイウェア対策のポリシー]をクリックします。
- 3 [タスク]で[ウイルス対策とスパイウェア対策のポリシーの追加]をクリックします。
既存のポリシーを編集することもできます。
- 4 ポリシーのページで[提出]をクリックします。
- 5 [検疫項目]で[クライアントコンピュータが検疫項目を検疫サーバーに自動的に提出するのを許可する]にチェックマークを付けます。
- 6 [サーバー名]フィールドに検疫サーバーの完全修飾ドメイン名または IP アドレスを入力します。
- 7 [ポート]フィールドで、デフォルトのポート番号を受け入れるかまたは変更します。

- 8 [再試行]フィールドで、クライアントから検疫サーバーへの通信に失敗したときの再試行間隔のデフォルト値を受け入れるか、またはその値を変更します。
- 9 [OK]をクリックします。

中央検疫のプロパティについて

[プロパティ]ダイアログボックスを使って中央検疫のさまざまなオプションを設定できます。

メモ: 詳細に設定しなくても中央検疫のデフォルト設定はインストール中に指定された情報でコンピュータを総合的に保護します。いずれの設定も変更する必要はありません。

表 3-1 中央検疫のプロパティ

| プロパティ | 説明 |
|----------|---|
| 一般 | このプロパティでは検疫フォルダの場所のような、主な検疫設定を指定できます。また、フォルダの最大サイズ、クライアントとの通信用の応答準備プロトコル、コンソールの自動更新間隔の設定も指定できます。 |
| Web 通信 | このプロパティでは Symantec ゲートウェイのコンピュータ名と次のセキュリティ設定を含む通信設定を指定できます。 <ul style="list-style-type: none">■ [提出物を保全する]: SSL (Secure Socket Layer) の略を使ってウイルスサンプルをシマンテック社に送信します。■ [ダウンロードを保全する]: SSL を使ってシマンテック社からウイルス定義の最新版を受信します。■ [Symantec免疫システムゲートウェイ]: シマンテックセキュリティレスポンスと通信するゲートウェイコンピュータを指定します。 |
| ファイアウォール | このプロパティではプロキシファイアウォールと通信する方法を指定できます(ネットワークがプロキシファイアウォールを使っている場合)。 <ul style="list-style-type: none">■ [ファイアウォール名]: ファイアウォールの IP アドレスまたは名前です。■ [ファイアウォールポート]: ファイアウォールと通信するポートです。■ [ファイアウォールのユーザー名]: ファイアウォールと通信するためのユーザー名です。■ [ファイアウォールのパスワード]: ファイアウォールと通信するためのパスワードです。 |

| プロパティ | 説明 |
|------------|--|
| サンプルポリシー | <p>このプロパティではサンプルの提出方法と処理方法を指定できます。</p> <ul style="list-style-type: none">■ [サンプルの自動提出]: ウイルスサンプルを分析用のキューに自動的に登録します。■ [キューを調べる間隔]: 検疫が新しい項目の有無を調べる頻度です。■ [サンプルからユーザーデータをはく離する]: サンプル提出物から秘密情報を含む可能性があるデータを削除してセキュリティを維持します。■ [状態問合せの間隔]: 提出済みサンプルについて状態の変化をゲートウェイがポーリングする頻度です。 |
| ウイルス定義ポリシー | <p>このプロパティではウイルス対策とスパイウェア対策定義の処理方法を指定できます。</p> <ul style="list-style-type: none">■ [アクティブシーケンス番号]: 検疫サーバーに現在インストールしてあるウイルス定義のシーケンス番号です。シーケンス番号はシマンテック製ウイルス対策製品にのみ使われる番号で、シグネチャセットに順次割り当てられます。この番号は常に累積して大きくなる番号です。シーケンス番号が大きいシグネチャセットの方がシーケンス番号の小さいシグネチャセットよりも優先されます。■ [認証済みウイルス定義の時間間隔]: 認証済みウイルス定義の更新版をダウンロードするためにゲートウェイをポーリングする分単位の頻度です。デフォルト設定は 480 分に 1 回です。 |
| お客様情報 | <p>このプロパティではインストール中に入力したお客様情報を編集できます。すべてのフィールドへの入力が必要になります。</p> |
| 警告 | <p>このプロパティでは特定イベントの警告を設定できます。</p> |
| 一般エラー | <p>このプロパティでは検疫サーバーエラーの履歴のリストを表示します。</p> |

検疫ファイルの管理

デフォルトでは、Symantec Endpoint Protection クライアントは現在のウイルス定義セットで修復できない感染項目を隔離します。これらの感染ファイルとその副作用を転送するように設定したクライアントは中央検疫サーバーに自動的に複製を送信します。

検疫項目の表示方法

感染項目を中央検疫サーバーに転送するようにクライアントコンピュータを設定すると、ファイルが検疫サーバーに追加されます。

表 3-2 検疫ファイル情報

| プロパティ | 説明 |
|---|-------------------------------------|
| ファイル名 | 感染項目の名前です。 |
| ユーザー名 | 感染ファイルを所有していたユーザーです。 |
| コンピュータ | 感染項目が発見されたコンピュータです。 |
| 分析済み | サンプルが分析済みかどうかが表示されます。 |
| 経過時間 | サンプルが検疫された日付です。 |
| サンプルの分析状態 p.28の「 サンプルの分析状態 」を参照してください。 | サンプルの現在の状態です。 |
| 必要なウイルス定義 | ウイルスを解消するために必要なウイルス定義セットのシーケンス番号です。 |
| 状態 p.27の「 サンプルの処理状態 」を参照してください。 | サンプルの処理状態です。 |
| ウイルス | 識別されたウイルスの名前です。 |
| エラー p.32の「 サンプルエラー 」を参照してください。 | サンプル処理エラーです。 |

検疫項目を表示するには

- シマンテック中央検疫コンソールの左ペインで[Symantec 中央検疫]をクリックします。
右ペインに検疫項目のリストが表示されます。
- 右ペインで検疫項目を右クリックして[プロパティ]を選択します。

検査ファイルの削除

中央検査のいずれの項目も削除できますが、このオプションは不要なファイル用にとっておきます。更新済みのウイルス定義でウイルスが検出および除去されたことを確認し終わったら検査項目を削除しても安全です。

検査ファイルを削除するには

- 1 シマンテック中央検査コンソールの左ペインで[Symantec 中央検査]をクリックします。
- 2 右ペインで1つ以上のファイルを右クリックして[削除]をクリックします。

検査ファイルの復元

ファイルの復元を選択しても Symantec AntiVirus はその修復を試みません。システムのウイルス感染のリスクを避けるために、このオプションは慎重に使ってください。たとえば、提出したファイルが未感染だったという通知がシマンテックセキュリティレスポンスからあった場合にのみファイルを復元してください。感染した可能性のあるファイルを復元することは安全ではありません。復元されたファイルは指定した場所のフォルダにコピーされます。

検査ファイルを復元するには

- 1 シマンテック中央検査コンソールの左ペインで[Symantec 中央検査]をクリックします。
- 2 右ペインで1つ以上のファイルを右クリックして[すべてのタスク]、[項目の復元]の順に選択します。
- 3 そのファイルが復元したいファイルである場合には[はい]をクリックします。
- 4 [フォルダの参照]ダイアログボックスでファイルの復元先の場所を指定して[OK]をクリックします。

分析用サンプルの提出

サンプルポリシーの設定ではウイルスサンプルがゲートウェイに自動的に提出されるかどうかを決定します。サンプルの自動提出オプションを選択していない場合、検査にある各サンプルは手動でゲートウェイに解放する必要があります。

サンプルの自動提出に対するポリシーの設定は変更できます。通常、サンプルは提出エラーまたは選択したサンプルのキュー優先度に変更があったときにのみ(提出したい場合に)手動で提出されます。

サンプルの自動提出ポリシーの設定

サンプルポリシーの設定ではウイルスサンプルがゲートウェイに自動的に提出されるかどうかを決定します。サンプルの自動提出オプションを選択していない場合、検疫に入っているサンプルは個別にゲートウェイに解放する必要があります。

セキュリティを強化するために、提出前にユーザーのデータをサンプルからはく離するように指定できます。

メモ: 提出ポリシーの設定は検疫で項目を選択して[処理]タブを表示すれば項目単位で変更できます。

サンプルの自動提出ポリシーを設定するには

- 1 シマンテック中央検疫コンソールの左ペインで[Symantec 中央検疫]を右クリックして[プロパティ]をクリックします。
- 2 [Symantec 中央検疫のプロパティ]ダイアログボックスの[サンプルポリシー]タブでサンプルポリシーを設定します。

ファイルの手動提出

疑わしいファイルは手動で提出すればウイルス分析を依頼できます。検疫サーバー上またはゲートウェイ上にあるウイルス定義で修復できるサンプルはシマンテックセキュリティレスポンスには送信されません。

手動で提出が可能なサンプルの条件は次のとおりです。

- すでに自動提出が可能なサンプルではない(X-Sample-Priority が 0 である)こと
- すでに自動提出済みのサンプルではない(X-Date-Submitted が 0 である)こと
- すでに分析済みのサンプルではない(X-Date-Finished が 0 である)こと

ファイルを手動で提出するにはその前にサンプルの優先度を設定する必要があります。

サンプルの優先度を手動で設定するには

- 1 シマンテック中央検疫コンソールの左ペインで[Symantec 中央検疫]をクリックします。
- 2 右ペインで項目を右クリックして[プロパティ]をクリックします。
- 3 [Symantec 中央検疫のプロパティ]ダイアログボックスの[処理]タブで提出優先度を設定します。

項目を手動で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 シマンテック中央検疫コンソールの左ペインで[Symantec 中央検疫]をクリックします。
- 2 右ペインで1つ以上のファイルを右クリックして[すべてのタスク]、[項目を自動分析用のキューに登録]の順に選択します。

サンプル提出状態の見直し

サンプルの状態は検疫サーバーとゲートウェイの通信中に設定された処理と属性を見直すことによって判断できます。

サンプル属性の表示方法

クライアントとサーバーの間で交換される要求と応答のメッセージには、サンプルとその状態を完全に記述するための多数の属性が入っています。これらの属性は常に X- という文字で始まります。

サンプルの属性を表示するには

- 1 シマンテック中央検疫コンソールの左ペインで[Symantec 中央検疫]を右クリックします。
- 2 右ペインで項目を右クリックして[プロパティ]をクリックします。
- 3 [プロパティ]ダイアログボックスの[サンプル属性]タブで表示される属性をダブルクリックすると属性の簡潔な定義が表示されます。

サンプルに適用される処理の見直し

サンプルに適用される処理には、選択したサンプルの提出と、ウイルス定義ファイル配布状態の表示の2つがあります。

選択したサンプルに対応するデフォルトのサンプル提出ポリシーの設定は変更することができます。サンプルを手動でシマンテックセキュリティレスポンスに提出するためのキューに登録したり、選択したサンプルの更新済みウイルス定義ファイルがあるかどうかを問い合わせたりすることができます。

サンプルの処理を見直すには

- 1 シマンテック中央検疫コンソールの左ペインで[Symantec 中央検疫]をクリックします。
- 2 右ペインで項目を右クリックして[プロパティ]をクリックします。
- 3 [プロパティ]ダイアログボックスの[処理]タブでサンプルに適用される処理を見直します。

サンプルの提出エラーの見直し

提出エラーが起きるとサンプルごとに報告されます。エントリを見直すことでサンプルに対して必要な処理を判断できます。

サンプルの提出エラーを見直すには

- 1 シマンテック中央検疫コンソールの左ペインで[Symantec 中央検疫]を右クリックします。
- 2 右ペインで項目を右クリックして[プロパティ]をクリックします。
- 3 [プロパティ]ダイアログボックスの[エラー]タブで提出エラーを見直します。

イベントと警告の設定

情報を得る必要があるイベントを指定できます。イベント情報はNT イベントログに送信できます。

警告のトリガになるイベントの指定

さまざまな種類のイベントをNT イベントログに送信できます。

表 3-3 警告のトリガになるイベント

| イベント | 説明 |
|------------------------------|---|
| ゲートウェイに接続できません | 検疫エージェントがデジタル免疫システムゲートウェイに接続できません。 |
| DefCastエラー | DefCast は新しいウイルス定義を検疫サーバーから配布先コンピュータに配布するサービスです。 |
| 配布先コンピュータにウイルス定義をインストールできません | 新しいウイルス定義を配布できませんでした。この警告は管理外クライアント用のウイルス定義が利用可能であることも示します。 |
| ウイルス定義ディレクトリにアクセスできません | 検疫サーバーがウイルス定義ディレクトリを見つけれません。 |
| 検疫スキャナサービスに接続できません | サンプルは検疫でスキャンできなかったためゲートウェイに転送されません。 |
| 検疫エージェントサービスが停止しました | 検疫がゲートウェイと通信できません。 |
| 必要なウイルス定義を待っています | ウイルス定義がまだゲートウェイから届いていません。 |

| イベント | 説明 |
|--------------------------------|--|
| 新しい認証済みウイルス定義が届きました | 検疫サーバー上に新しい認証済みウイルス定義が届きました。 |
| 新しい未認証のウイルス定義が届きました | サンプル提出に対する応答として検疫サーバー上に新しい未認証のウイルス定義が届きました。 |
| ディスク割り当て分の残りが検疫フォルダに対して不足です | 検疫フォルダがいっぱいになりそうです。 |
| 空きディスク容量が検疫の最大サイズ未満です | 検疫フォルダの最大サイズの設定が空きディスク容量よりも大きいサイズになっています。 |
| サンプル:修復していません | サンプルは修復されなかったか、修復が必要ではありませんでした。 |
| サンプル:ウイルス定義をインストールできません | 新しいウイルス定義をインストールできませんでした。通常の原因はウイルス定義セットの破損です。 |
| サンプル:処理エラー | このサンプルの処理中にエラーが発生しました。 |
| サンプル:テクニカルサポートからの指示が必要です | サンプルを自動的に処理できませんでした。テクニカルサポートにサンプルを提示して助言してもらってください。 |
| サンプル:手動提出用の保留状態です | サンプルは自動提出されずに検疫サーバー上で保留状態になっています。 |
| サンプル:新しいウイルス定義の未インストール状態が長すぎます | 新しいウイルス定義をインストールしたはず(状態は配布)ですが、インストールされていません。 |
| サンプル:配布済み状態が長すぎます | 新しいウイルス定義がゲートウェイから届きましたが、クライアント上でインストールされたという確認を検疫がまだ受信していません。 |
| サンプル:定義必要状態が長すぎます | ゲートウェイからまだウイルス定義を取り込んでいません。 |
| サンプル:解放済み状態が長すぎます | ゲートウェイがまだ応答していません。 |
| サンプル:提出済み状態が長すぎます | ゲートウェイがまだサンプルを受信していません。 |
| サンプル:検疫済み状態が長すぎます | 検疫でまだサンプルをスキャンしていません。 |
| サンプル:新しいウイルス定義は配信用の保留状態です | 新しいウイルス定義は配信される代わりに検疫サーバーで保留状態になっています。 |

警告のトリガになるイベントを指定するには

- 1 シマンテック中央検疫コンソールの左ペインで[Symantec 中央検疫]を右クリックして[プロパティ]をクリックします。
- 2 [Symantec 中央検疫のプロパティ]ダイアログボックスの[警告]タブで[NT イベントログ]にチェックマークを付けます。
- 3 [イベント通知の設定]で次のいずれかまたは両方を行います。
 - 情報を得る必要があるイベントにチェックマークを付けます。
 - 情報を得る必要がないイベントのチェックマークをはずします。
- 4 [OK]をクリックします。

サンプル処理リファレンス

この付録では以下の項目について説明しています。

- サンプル処理について
- サンプルの処理状態
- サンプルの分析状態
- サンプルエラー

サンプル処理について

デジタル免疫システムはシステムの内部にある任意のサンプルについてのリアルタイム情報（提出済みサンプルの処理状態や分析状態）を表示します。

サンプルの処理状態

サンプルの処理状態を表 A-1 に示します。サンプルの処理状態はデジタル免疫システムの内部にあるサンプルの処理状態です。

表 A-1 サンプルの処理状態

| 状態 | 説明 |
|------|--|
| 注意 | サンプルにはテクニカルサポートによる介入が必要です。 |
| 利用可能 | 新しいウイルス定義を提出元コンピュータへの配信用に保留にしました。 |
| 配布 | 新しいウイルス定義を提出元コンピュータに配信するためのキューに登録しました。 |
| 配布済み | 新しいウイルス定義を提出元コンピュータに配信しました。 |

| 状態 | 説明 |
|----------|------------------------------------|
| エラー | 処理エラーが起きました。 |
| 保留 | サンプルの提出を見合わせました。 |
| インストール済み | 新しいウイルス定義を提出元コンピュータにインストールしました。 |
| 必要 | サンプルに新しいウイルス定義が必要です。 |
| 未インストール | ウイルス定義を提出元コンピュータにインストールできませんでした。 |
| 検疫 | 中央検疫がサンプルを受信しました。 |
| 解放 | サンプルを分析用のキューに登録しました。 |
| 再開 | サンプル処理を再び開始します。 |
| 提出済み | サンプルを分析用にシマンテックセキュリティレスポンスに提出しました。 |
| 不要 | サンプルに新しいウイルス定義は必要ありません。 |

サンプルの分析状態

サンプルの分析状態はデジタル免疫システムの内部における提出済みサンプルの分析状態です。分析状態が示すのはサンプルが見つかったネットワーク階層、分析パイプラインのどの段階が現在サンプルに働いているか、またはその最終的な処理です。

メモ: サンプルがクライアントコンピュータに戻されたことを示す状態はサポートされません。

最終状態

分析が終了したサンプルは最終状態のいずれか 1 つの状態になります。デジタル免疫システムのすべてのノードは終了状態になります。終了状態になったサンプルの状態は二度と変わりません。X-Date-Analyzed 属性はサンプルが終了状態になると設定されます。この属性の存在は X-Analysis-State の値が最終状態であることを意味します。

表 A-2 最終状態

| 状態 | 説明 |
|-------|---|
| abort | 内部的なプログラミングエラーが起きてサンプルを転送または分析できませんでした。 |

| 状態 | 説明 |
|--------|---|
| 注意 | サンプルにはテクニカルサポートによる介入が必要です。 |
| broken | サンプルはウイルスに感染していますが BackOffice のウイルス定義生成サービスがエラーを報告します。利用可能なウイルス定義ファイルがありません。 |
| 拒否 | サンプルは受け入れ不能で拒否されました。 |
| エラー | 処理エラーが起きました。 |
| 感染 | サンプルはウイルスに感染していて利用可能なウイルス定義ファイルで修復可能です。 |
| 誤認 | サンプルを分析しました。感染が検出されたにもかかわらずウイルスは見つかりませんでした。誤って感染が検出された原因は以前のウイルス定義ファイルにあった誤りが新しいウイルス定義ファイルで訂正されたためです。 |
| 検出なし | サンプルを分析していませんが、明らかな疑わしいコードは入っていません。 |
| 修復なし | サンプルはウイルスに感染していますが、利用可能なウイルス定義ファイルで修復できませんでした。削除してください。 |
| 感染不能 | サンプルには実行可能コードが入っていないのでウイルスに感染することはありません。サンプルには実行可能コードを格納するサイズ的な余地がないか、またはグラフィックイメージか音声クリップなどのデータのみが入っています。 |
| 未感染 | サンプルを分析しました。ウイルスは見つかりませんでした。 |
| 提出不能 | サンプルには既知の悪質なソフトウェア (ワームまたはトロイの木馬など) が入っています。削除してください。 |
| 暗号化 | 暗号化またはパスワード保護されているため中央検査がこのサンプルをスキャンできません。再提出する前に解読するかパスワード保護を解除する必要があります。 |
| 削除 | 悪質なコードによって作成されたファイルまたは悪質なコードが入っているファイルです。このようなファイルに適用できる処理は削除のみです。 |
| 復元 | クリーニングできないファイルです。このようなファイルは誤ってまたはウイルスによって改変されたか、中に壊れたウイルスのコードが入っている可能性があります。改変されているためファイルを保持することができないか、またはファイルを保持することが危険な状態です。バックアップファイルから復元してください。 |

移行状態

シマンテックセキュリティレスポンスに到達していないサンプルは移行状態のいずれか 1 つの状態になります。シマンテックセキュリティレスポンスの外部にあるコンポーネントのみが移行状態を使います。サンプルは別の状態に移る前に不確定な保留状態のままになることがあります。

表 A-3 移行状態

| 状態 | 説明 |
|--------|---|
| 受け入れ済み | ゲートウェイがサンプルを受信しました。ただし、そのサンプルはまだシマンテックセキュリティレスポンスにインポートされていません。 |
| インポート中 | シマンテックセキュリティレスポンスがサンプルをインポートしました。 |
| 受信済 | ゲートウェイがサンプルを受信しました。 |

保留状態

シマンテックセキュリティレスポンスの内部で分析を待つサンプルは保留状態のいずれか 1 つの状態になります。シマンテックセキュリティレスポンスの内部にあるコンポーネントのみが保留状態を使います。サンプルは別の状態に移る前に不確定な保留状態のままになることがあります。

表 A-4 保留状態

| 状態 | 説明 |
|---------|---|
| 依頼済 | サンプルは自動的に分析できなかったため専門家に分析を依頼中です。 |
| 依頼済 | サンプルは自動的に分析できなかったため専門家に分析を依頼中です。 |
| 依頼中 | サンプルは自動的に分析できなかったため専門家に分析を依頼中です。 |
| インポート済み | サンプルはシマンテックセキュリティレスポンスにインポートされましたが、まだ分析されていません。 |
| 再スキャン | シマンテックセキュリティレスポンスの内部で新しいウイルス定義ファイルが利用可能になったのでサンプルを再スキャンする必要があります。 |

活動状態

シマンテックセキュリティレスポンスの内部で分析したサンプルは活動状態のいずれか 1 つの状態になります。シマンテックセキュリティレスポンスの内部にあるコンポーネントの

みが活動状態を使います。サンプルは別の状態に移る前に 2 分か 3 分、または長ければ何十分か活動状態のままになることがあります。

表 A-5 活動状態

| 状態 | 説明 |
|----------|--|
| アーカイブ | サンプルは自動分析ファイルのアーカイブを待っています。 |
| アーカイブ中 | サンプルは自動分析ファイルのアーカイブ中です。 |
| バイナリ | サンプルはバイナリプログラムとして分類され、バイナリコントローラを待っています。 |
| バイナリ制御中 | バイナリコントローラがバイナリ複製の開始条件を決定中です。 |
| バイナリ複製中 | サンプルはバイナリ複製エンジンによって実行中です。 |
| バイナリ採点中 | サンプルは他のバイナリプログラムに感染しています。バイナリスコアエンジンがウイルスを検出して修復するためのシグネチャを選択しています。 |
| バイナリ待機 | サンプルはバイナリ複製エンジンが利用可能になるのを待っています。 |
| 分類中 | サンプルはデータ型を決定するために分類中です。 |
| 完全構築中 | 新種のウイルス用に選択したシグネチャを組み入れて新しいウイルス定義ファイルのセットを構築しています。 |
| 完全単体テスト中 | 完全ウイルス定義ファイルを単体テストしています。 |
| 増分構築中 | 新種のウイルス用に選択したシグネチャを現在のウイルス定義ファイルに追加しています。 |
| 増分単体テスト中 | 増分ウイルス定義ファイルを単体テストしています。 |
| ロック中 | BackOffice のウイルス定義生成サービスに対する排他的アクセスを取得しています。 |
| マクロ | サンプルは実行可能マクロが入っているデータファイル(ワープロ文書または表計算ワークシートなど)として分類され、マクロコントローラを待っています。 |
| マクロ制御中 | マクロコントローラがマクロ複製の開始条件を決定中です。 |
| マクロ複製中 | サンプルはマクロ複製エンジンによって実行中です。 |
| マクロ採点中 | サンプルは他のデータファイル(ワープロ文書または表計算ワークシートなど)に感染しています。マクロスコアエンジンがウイルスを検出して修復するためのシグネチャを選択しています。 |

| 状態 | 説明 |
|--------|--|
| マクロ待機 | サンプルはマクロ複製エンジンが利用可能になるのを待っています。 |
| シグネチャ | サンプルは新種のウイルスに感染しています。ウイルスを検出して修復するためのシグネチャが選択され、サンプルは構築処理が利用可能になるのを待っています。 |
| ロック解除中 | ウイルス定義生成サービスに対する排他的アクセスを解放しています。 |

サンプルエラー

サンプル処理エラーには次の表に示すようなエラーがあります。

表 A-6 サンプルエラー

| エラー | 説明 |
|--------|--|
| 破棄 | シグネチャシーケンス番号が破棄されました。通常、これは対応するウイルス定義セットが単体テストで不合格であったことが原因です。 |
| 内容 | サンプルの内容チェックサムがその内容と一致しません。 |
| 未割り当て | サンプルを追跡する Cookie をゲートウェイが割り当てていません。 |
| 拒否 | 分析用に提出したサンプルをゲートウェイが拒否しました。テクニカルサポートに連絡して助言してもらってください。 |
| 内部 | サンプルの処理中に内部エラーが起きました。 |
| サンプル消失 | ネットワークエラーのためサンプルは完全に受信されませんでした。 |
| 形式不良 | サンプルの重要な属性の形式が誤っていました。 |
| 属性消失 | サンプルの重要な属性が見つかりません。 |
| オーバーラン | このサンプルの内容が予想の長さを超えています。このオーバーランは転送ネットワークの伝送エラーが原因で起きる可能性があります。 |
| サンプル | サンプルのサンプルチェックサムがその内容と一致しません。 |
| 上書き | このシグネチャシーケンス番号はより新しい認証済みウイルス定義に置き換わり、サーバーからは利用できなくなります。クライアントは以前のウイルス定義の代わりに現在の認証済みウイルス定義をダウンロードする必要があります。 |
| 種類 | サンプルの種類がサポート外です。 |
| 利用不能 | シグネチャシーケンス番号がまだ発行されていません。 |

| エラー | 説明 |
|---------|-----------------------------|
| アンダーラン | サンプルの予想の長さがその内容を超えています。 |
| パッケージ解除 | サンプルまたはシグネチャをバック解除できませんでした。 |
| 未発行 | シグネチャセットを発行できませんでした。 |

記号

サンプル
処理 27

D

DefCast 6

N

NT イベントログ 24

S

Symantec 免疫システムゲートウェイ 18

W

Web 通信
ウィンドウ 13
プロパティ 18

X

X- 文字 23

あ

イベント
警告のトリガになる 24
設定 24

インストール
検疫コンソール 12
検疫サーバー 12
中央検疫 12

ウイルス定義と認証済みウイルス定義の時間間隔 19

エラー
一般 19
提出 21
提出の見直し 24
トリガするイベント 24

お客様情報

ウィンドウ 13
プロパティ 19

か

感染ファイルの復元 21
キューを調べる間隔 19
ゲートウェイ

Symantec 免疫システムゲートウェイ 18

概要 6
コンピュータ名 18
接続できない 24
定義済み 6
デフォルトのアドレス 13
ファイルの提出 7
ポーリング 7、19
未知の脅威の検出 7

検疫

一般プロパティ 18
デフォルト設定 18
表示 20
ファイルの削除 21
ローカル 5

検疫エージェント 6

検疫コンソール

インストール 12
概要 6
中央検疫のコンポーネント 15

検疫サーバー

インストール 12
概要 6
設定
インターネットベースのスキャンと配信 16～17
中央検疫のコンポーネント 15
有効化
別のコンピュータ 16
ローカルコンピュータ 16

検疫スキヤナ 6、24

検疫ファイル 21
復元 21

さ

最大ディスク容量ウィンドウ 13
サンプル
エラー 32

- 活動状態 30
- 最終状態 28
- 自動提出 21
- 状態 23、27～28
- 処理の確認 23
- 処理の見直し 23
- 属性
 - 表示 23
- 提出状態の見直し 23
- ポリシー 21
 - サンプルの自動提出 19
 - 設定 21～22
 - プロパティ 19
- 保留状態 30
- サンプルの活動状態 30
- サンプルの最終状態 28
- サンプルの保留状態 30
- シーケンス番号 19
- システム必要条件 12
- シマンテックセキュリティレスポンス 6、15
- 状態
 - 活動 30
 - 最終 28
 - サンプル 28
 - 保留 30
- 状態問合せの間隔 19

た

- 中央検疫
 - インストール 12
 - プロパティ 18
- 提出
 - エラーの見直し 24
 - 属性の解釈 23
- デジタル免疫システム
 - 概要 6
 - コンポーネント 6
 - サンプル処理 27
 - 自動化 6
 - 分析 7

な

- 認証済みウイルス定義 19、25

は

- [ファイアウォール]タブ
 - 名前 18
 - パスワード 18

- ポート 18
- ユーザー名 18
- ファイルの提出 7
- プロトコル
 - TCP/IP 11
 - 検疫コンソールと検疫サーバーでの共有 11
 - ネットワーク 16
- ポートとネットワークプロトコル 16
- ポリシー
 - サンプルの自動提出ポリシーの設定 22
 - サンプル用の設定 22
 - 定義 19

ま

- 未認証のウイルス定義 25