

ウイルス対策&クライアントセキュリティ試験対策コース

▼ 講習日数: 3日間

▼ コースの概要

この Symantec Client Security 3.x コースは、Symantec Client Security 3.x のサポート、インストール、設定、および管理に携わるユーザーを対象としています。Symantec Client Security は、ウイルス対策、不正侵入防止、およびファイアウォールセキュリティの機能を提供します。

Symantec Client Security 3.x コースは 18 のユニットに分かれており、要望に応じて、各ユニットを他のユニットから独立して説明できるようにモジュール化されています。インストラクターの講義の後には、講義で身に付けた知識を実践するための実習を行います。

▼ コースの履修目標 (以下の項目ができるようになります)

- ・ Symantec Client Security の基礎的な概念とアーキテクチャ
- ・ Symantec Client Security のサーバー、クライアント、および管理コンポーネントの計画とインストール
- ・ Symantec Client Security または他のシマンテック製品から Symantec Client Security の最新バージョンへの移行
- ・ Symantec Client Security 製品のライセンスに関する知識
- ・ 製品機能と一般的な設定と管理について
- ・ 安全な通信に関する知識
- ・ Symantec Client Security の管理と設定
- ・ Symantec Client Security を使用したウイルスや他の脅威のスキャン
- ・ 新しいウイルススキャン機能の詳しい技術情報
- ・ ウイルス定義ファイルの更新、ウイルスアウトブレイクへの対応、両方のシナリオで起こりうる問題のトラブルシューティング

▼ 前提知識

- ・ Microsoft Windows のネットワークと管理に関する知識
- ・ コンピュータセキュリティの実施とソフトウェアに関する実践的な知識
- ・ トレーニングや経験によって得られた TCP/IP ネットワーク概念に関する基礎知識

使用 OS: Windows 2000 Server / Professional

▼ カリキュラム詳細

Unit 1 Symantec Client Security の概要

- ・ ネットワーク接続されたコンピュータの脆弱性
- ・ Symantec Client Security を使用する理由
- ・ Symantec Client Security の概要
- ・ Symantec Client Security の動作方法
- ・ Symantec Client Security を使用してできること
- ・ Symantec Client Security の構造コンポーネント
- ・ Symantec Client Security コンポーネント
- ・ Symantec Client Security の階層コンポーネント
- ・ ウイルス定義ファイルの更新の方法
- ・ Symantec Client Security クライアントの管理
- ・ このリリースの新機能
- ・ 問題

Unit 2 インストールの計画

- ・ Symantec Client Security のネットワークアーキテクチャの計画
- ・ 管理者権限と msi ファイル
- ・ システム要件
- ・ システム時間の要件

- ・ Windows XP ファイアウォールの無効化
- ・ Windows XP ファイアウォールの使用について
- ・ Windows XP コンピュータへのリモートソフトウェアのインストール許可
- ・ 他のセキュリティリスク防止プログラムの無効化

Unit 3 Symantec Client Security 管理コンポーネントのインストール

- ・ 管理コンポーネント
- ・ Symantec System Center のインストール
- ・ Symantec Client Firewall Administrator のインストール
- ・ 他の管理コンポーネントのインストール
- ・ Lab 3 - 1: Symantec System Center のインストール
- ・ Lab 3 - 2: Symantec Client Firewall Administrator のインストール

Unit 4 Symantec Client Security サーバーのインストール

- ・ インストール時の検討事項
- ・ サーバーのインストール方法
- ・ サーバーインストールの準備
- ・ Symantec Client Security サーバーの Netware サーバーへのインストール
- ・ サーバーインストールの実行
- ・ Lab 4 - 1: Symantec AntiVirus サーバーのインストール
- ・ Lab 4 - 2: Symantec System Center コンソールのない Symantec AntiVirus Server の設定

Unit 5 Symantec Client Security クライアントのインストール

- ・ クライアントインストールの準備
- ・ クライアントのインストール方法
- ・ それぞれの方法のメリットとデメリット
- ・ インストール後のクライアントのタスク
- ・ Lab 5 - 1: ClientRemote インストールツールを使用したクライアントのインストール
- ・ Lab 5 - 2: Web ベースの配備によるクライアントのインストール
- ・ Lab 5 - 3: コマンドラインからのクライアントのインストール

Unit 6 Symantec Client Security の現行バージョンへの移行

- ・ 移行準備
- ・ サーバーおよびクライアントが移行に対応しているかいないか
- ・ Symantec System Center のアップグレード
- ・ 管理サーバーの移行
- ・ クライアントソフトウェアの移行
- ・ Lab 6 - 1: サポート対象の移行方法の特定

Unit 7 Symantec Client Security の管理

- ・ Symantec System Center を使用したネットワーク階層の管理
- ・ クライアント管理
- ・ セキュリティ管理
- ・ イベントログと履歴ログの管理
- ・ Lab 7 - 1: ユーザーアカウント、サーバーグループ、およびクライアントグループの管理
- ・ Lab 7 - 2: コンピュータの検索と監査
- ・ Lab 7 - 3: クライアントログデータの管理

Unit 8 ウイルス定義ファイルの更新

- ・ ウイルス定義ファイルの更新の重要性
- ・ ウイルス定義ファイルの更新方法
- ・ クライアントからの LiveUpdate の実行
- ・ 社内 LiveUpdate サーバーの計画
- ・ LiveUpdate 管理ユーティリティの概要
- ・ 更新パッケージの取得
- ・ 社内 LiveUpdate サーバーを使用するためのサーバーとクライアントの設定

- ・ 共通する LiveUpdate の設定タスク
- ・ Virus Definition Transport Method (VDTM)
- ・ VDTM がウイルス定義ファイルを配布する方法
- ・ ウイルス定義ファイルの管理
- ・ Lab 8 - 1: LiveUpdate を使用した更新ファイル取得のためのサーバーとクライアントの設定
- ・ Lab 8 - 2: 社内 LiveUpdate サーバーのインストールと設定

Unit 9 ウイルススキャン設定

- ・ SAVCE が防御する脅威
- ・ ウイルススキャンの概要
- ・ スキャン技術
- ・ ウイルス駆除
- ・ 手動スキャン
- ・ 定時スキャン
- ・ 検出した脅威に対する処理の割り当て
- ・ スキャン動作の設定
- ・ セキュリティリスクのカテゴリ
- ・ 圧縮ファイルのスキャン
- ・ ユーザーによる操作の制御
- ・ Auto-Protect の設定
- ・ 電子メールスキャン
- ・ ネットワーク上のウイルスアウトブレイクの対処方法
- ・ Lab 9 - 1: 定時スキャンの設定
- ・ Lab 9 - 2: クライアントオプションの変更
- ・ Lab 9 - 3: スパイウェア/ アドウェアのスキャン

Unit 10 中央検疫の管理

- ・ 中央検疫について
- ・ デジタル免疫システム
- ・ 中央検疫のコンポーネント
- ・ 中央検疫サーバーとデジタル免疫システムとの連携動作方法
- ・ インストール要件
- ・ 中央検疫コンポーネントのインストール
- ・ インターネットベースのスキャンと配信の使用
- ・ 中央検疫プロパティの設定
- ・ インターネットベースのクライアント転送の設定
- ・ 中央検疫サーバーからのウイルス定義ファイル更新の設定
- ・ サンプル提出状態の調査
- ・ Lab 10 - 1: 中央検疫コンポーネントのインストール
- ・ Lab 10 - 2: 中央検疫のセットアップと設定
- ・ Lab 10 - 3: 中央検疫のテスト

Unit 11 安全な通信

- ・ SSL を使用する理由
- ・ 暗号化キーとアルゴリズム
- ・ 一方向ハッシュとデジタル署名
- ・ デジタル証明書と PKI (Public Key Infrastructure)
- ・ SSL について
- ・ 証明書が信頼の連鎖を設定する方法
- ・ 認証の経路と方法
- ・ 証明書ストアのフォルダ
- ・ ファイル命名規則
- ・ ベストプラクティス
- ・ レガシー通信と安全な通信

Unit 12 クライアントローミング

- ・ クライアントローミングサポート

Unit 13 Symantec Client Firewall の概要

- ・ Symantec Client Firewall を使用してできること
- ・ Symantec Client Firewall の機能の概要
- ・ ステートフルインスペクションファイアウォール
- ・ プロトコルフィルタ処理
- ・ ファイアウォールルール
- ・ 場所
- ・ ネットワークゾーン
- ・ Symantec Client Firewall の扱い方
- ・ 設定マネージャからのポリシーファイルのエクスポートとインポート
- ・ Symantec Client Firewall の一時的な無効化
- ・ LiveUpdate による新種のウイルスへの対応
- ・ Symantec Client Firewall の管理
- ・ Symantec Client Firewall の新機能

Unit 14 Symantec Client Firewall の警告に対する応答

- ・ 警告の種類
- ・ よく表示される警告
- ・ 警告の低減

Unit 15 ファイアウォールポリシーの管理

- ・ ポリシー管理ツール
- ・ ポリシーのコンポーネント
- ・ ポリシーと更新版の設定
- ・ ポリシーと更新版のインポートとエクスポート
- ・ ポリシーファイル内のルールと pRule のマージ
- ・ ポリシーの配布
- ・ レガシークライアント用のポリシーのサポート

Unit 16 ルールと pRule の設定

- ・ ファイアウォールルール
- ・ ルールの操作
- ・ pRule
- ・ pRule の設定
- ・ セキュアポートの使用
- ・ ファイアウォールルールおよび設定のテスト
- ・ Lab 16 - 1: ファイアウォールルールの作成と配布
- ・ Lab 16 - 2: pRule の作成

Unit 17 不正侵入防止のカスタマイズ

- ・ 不正侵入防止システム
- ・ 遮断対象からの攻撃シグネチャの除外
- ・ AutoBlock の設定
- ・ IPS 除外のロック
- ・ Lab 17 - 1: 不正侵入防止システムのカスタマイズ

Unit 18 クライアント設定と Web コンテンツ設定の作成

- ・ クライアント設定
- ・ 一般のクライアント設定
- ・ 警告の設定
- ・ [その他の通知]
- ・ [パーミッション]
- ・ プロトコルフィルタ

- ・ Web コンテンツ設定
- ・ Lab 18 - 1: Java アプレット設定の作成
- ・ Lab 18 - 2: プライバシー制御の設定
- ・ Lab 18 - 3: Cookie 遮断の設定
- ・ Lab 18 - 4: ユーザーによる操作のカスタマイズ

Appendix A Windows インストーラ(msi) のコマンドライン参照

- ・ コマンドラインパラメータを使用した Symantec Client Security のインストール
- ・ Windows インストーラコマンド
- ・ サーバーインストールのプロパティと機能
- ・ クライアントインストールのプロパティと機能
- ・ ログファイルを使用したエラーチェック
- ・ コマンドラインの例

Appendix B Windows XP/2000 サービス

- ・ Symantec Client Security サービス
- ・ Symantec System Center サービス

Appendix C SAV が X 分ごとに行う処理

Appendix D コンテンツライセンス登録

- ・ コンテンツライセンス登録について
- ・ コンテンツライセンスファイルの要求
- ・ 管理クライアントでのライセンス登録
- ・ 管理外クライアントでのライセンス登録

▼ 試験対策について

ウイルス対策&クライアントセキュリティソリューション試験
対象範囲は、下記製品になります。

- ・ Symantec Antivirus for Handhelds
- ・ Symantec Client Security
- ・ Symantec Mail Security
- ・ Symantec Web Security
- ・ Symantec AntiVirus Scan Engine
- ・ Symantec AntiVirus Enterprise Edition