McAfee Network Data Loss Prevention の管理

研修サービス / インストラクターによるトレーニング
このコースを終了すると最大 32 の CPE を獲得します

McAfee の研修サービス「McAfee Network Data Loss Prevention の管理」コースでは、Network Data Loss Prevention の集中管理と展開のメリットを詳細に習得することができます。管理者がセキュリティソリューションの機能を十分に理解することで、構成ミスのリスクを軽減するだけでなく、組織が製品の機能を最大限に利用し、保護できるようになります。このコースでは、Network DLP 製品の機能を理解し、Network DLP Manager、DLP Prevent、DLP Discover、DLP Monitor を導入および設定をおこない、運用環境での DLP Monitor またはポリシーをカスタマイズ、レポートを生成するといった情報漏洩防止対策を最適化する方法についても学習します。

アジェンダの概要

1 日目

- コースについて
- McAfee DLP の概要
- McAfee Network DLP 製品の提供
- McAfee DLP 共通要素
- ケーススタディ
- McAfee DLP インストール
- McAfee DLP マネージャ
- McAfee DLP ユーザーとグループ

2 日目

- McAfee DLP ポリシー
- McAfee DLP ルール
- ルールのコンテンツ
- ルールのコンテキスト
- 他の McAfee DLP ルール要素
- アクションルール
- McAfee DLP Monitor
- McAfee DLP ポリシー

対象者

このコースは、ネットワークとシステムのセキュリティに関わるシステム管理者、セキュリティ担当者、監査担当者、コンサルタントを対象としています。

アジェンダの概要

3 日目

- McAfee DLP Discover
- McAfee DLP Discover ポリシー
- McAfee DLP Email Prevent
- McAfee DLP Email Prevent ポリシー
- McAfee DLP Web Prevent
- McAfee DLP Web Prevent ポリシー

4 日目

- インシデント管理
- ダッシュボードとレポート
- ルールチューニングとベストプラクティス
- ケーススタディレビュー

推奨する事前知識

Microsoft Windows の管理、システム管理の概念、コンピュータセキュリティの基本的な概念、ウイルスとウイルス対策技術の一般的な理解に関する実践的な知識があることを推奨します。

コースの概要

モジュール 1：Network DLP の管理コースについて

- コース概要
- 施設紹介
- 研修サービス
- 製品トレーニング
- セキュリティ教育
- テクニカルサポート
- セキュリティコンテンツのリリースノート
- 製品改善リクエスト
- McAfee コミュニティ
- 役に立つリンク
- 教室での演習のセットアップ
- 演習ガイドの使用

モジュール 2：DLP の概要、Network DLP の管理

- 境界のないビジネス環境
- データ侵害のニュース記事
- すべての組織がデータ侵害の対象
- 特に重要なデータ
- 情報漏えいに関連するコスト
- McAfee DLP ソリューションの主な要件
- データ漏えいのベクトル
- 「誰もが原因になりうる」
- McAfee のアプローチ
- データに対する懸念事項
- 製品に関するドキュメントのソース

モジュール 3：NDLP 製品の内容

- DLP ソリューション製品

- McAfee DLP 製品
- Network DLP (NDLP) のポート
- サポートされているシステム
- 互換性のある McAfee 製品
- サポートされているリポジトリ
- サポートされているブラウザ
- サポートされている言語
- NDLP Manager
- NDLP Monitor
- データのキャプチャ
- ミラーポートとネットワークタップ
- NDLP Discover
- NDLP Prevent
- NDLP Prevent（電子メール）
- NDLP Prevent（Web）
- 配備のチェックリスト
- 接続の要件と制限事項
- 実装プロセスのチェックリスト

モジュール 4：DLP の共通要素

- ポリシーとルールのチェック
- ポリシー
- ポリシーの設定
- NDLP キャプチャデータベース
- ケース管理
- NDLP のケースワークフロー
- ダッシュボードとレポート
- ダッシュボード
- 検索リスト - 結果
- ラボ演習

モジュール 5：ケーススタディ

- 配備シナリオ
- 医療分野での DLP 推進の主な要因
- 医療分野のユースケース
- 保護対象の医療情報
- メディカル情報を保護
- 製造業での DLP 推進の主な要因
- 化学品製造会社のケース
- 保護対象の化学情報
- 金融業での DLP 推進の主な要因
- データ侵害 - 大規模な組織
- 金融業のケース
- 保護対象の金融取引情報

モジュール 6：DLP のインストール

- DLP のハードウェア
- NDLP の物理アプライアンス
- NDLP サーバーのイーサネットポート
- VMware
- NDLP のイメージ
- ソフトウェアのインストール / アップグレード
- DLP ソフトウェアのインストール手順
- アプライアンスの初期スイッチング
- NDLP Manager の初期設定
- NDLP の設定
- インストールのトラブルシューティング
- 実装プロセスのチェックリスト

モジュール 7：DLP Manager

- NDLP Manager とは何か
- NDLP Manager の主な機能
- NDLP Manager のベストプラクティス
- ファイアウォールの設定（ポート情報）
- Network DLP Manager の UI
  - HOME
  - INCIDENTS
  - SEARCH
  - POLICIES
  - CLASSIFY
  - SYSTEM
  - 新しいデバイスの追加
- NDLP の災害復旧機能
- ラボ演習

モジュール 8：DLP のユーザーとグループ

- DLP ユーザーとグループ
- ユーザーとグループの管理
- フェールオーバーアカウント
- ユーザー
- 新規ローカルユーザーの追加
- グループ
- グループとビジネスユニット
- NDLP のグループのプロパティ
- Task Permissions
- Policy Permissions
- NDLP LDAP ユーザー
- ディレクトリサーバーの作成
- LDAP ユーザーの追加
- LDAP ユーザーでのログイン
- ディレクトリサーバーの問題のトラブルシューティング
- McAfee Login Collector（MLC）
- McAfee Login Collector の作成
- ラボ演習

モジュール 9：DLP ポリシー

- NDLP ポリシー
- ポリシーの設定
- ポリシー定義
- 地域別のポリシーの選択
- ポリシーのアクション
- ポリシーのアクティブ化 / 非アクティブ化
- ポリシーの作成 - [Add Policy] 画面
- ポリシーの作成 - [Edit Policy] 画面
- ポリシーの所有権
- ポリシーとルール
- 検索
- ポリシーの詳細設定
- ラボ演習

モジュール 10：DLP ルール

- ルールのチェック
- ルール定義
- ルール関連のタブ
- 検索からのルールの追加（作成）
- ルールの作成
- ルールの管理

- 定義
- アクション
- 例外
- データー致の制限

モジュール 11：ルールのコンテンツ

- ルールのコンテンツ
- テンプレート
- キーワード
- キーワードとステム
- コンテンツタイプ
- 複数の定義の組み合わせ
- テンプレートの使用
- 式
- よく使用される式
- NDLP コンセプトでの \k と \K の使用目的
- 式の例
- 式の使用
- コンセプト
- コンセプト画面
- コンセプトの追加
- コンセプトのアルゴリズム
- コンセプトの管理
- コンセプトの複製

モジュール 12：ルールのコンテキスト

- コンテキスト
- コンテキストをコンセプトに追加する
- カウント
- 一致率
- 位置
- 近接性 - 距離
- 近接性の照合順序
- コンセプトの例
- コンテキストの例
- ラボ演習

モジュール 13：DLP ルールのその他の要素

- その他のルール要素
- Source/Destination
- 電子メールアドレス
- IP アドレス
- URL の参照
- GeoIP 位置
- ファイル情報
- 文書プロパティ
- 文書プロパティの追加
- プロトコル / ポート
- 検出
- 日付 / 時刻
- ラボ演習

モジュール 14：アクションルール

- アクションルール
- 新しいアクションルールの追加
- 電子メールオプション
- Syslog
- インシデントレビューアー

- インシデントのステータス
- アクションルール
- NDLP ルールのアクション
- ラボ演習

モジュール 15：DLP Monitor

- NDLP Monitor とは？
- NDLP Monitor
- 複数のモニターの使用
- モニターのアーキテクチャ
- ミラーポート / ネットワークタップ
- キャプチャフィルタ
- ネットワークフィルタとコンテンツフィルタ
- ネットワークフィルタのアクションタイプ
- ネットワークキャプチャフィルタのサンプル
- RFC 1918
- コンテンツフィルタのアクションタイプ
- コンテンツキャプチャフィルタのサンプル
- 検索タスクに必要な権限
- Basic Search（基本検索）– 例
- Advanced Search（詳細検索）– 例
- Search List（検索リスト）– Details（詳細）
- Search List（検索リスト）– Results（結果）
- 検索タスク
- NDLP アプライアンスのインストール
- クイックスタートウィザード
- NLDP アプライアンスの登録
- ラボ演習

モジュール 16：Monitor ポリシー

- 移動中のデータのポリシー
- 移動中のデータのアクションルール
- 移動中のデータのポリシー
- DiM 検索結果
- RFS ディスク領域のチェック
- ディスク使用率
- トラブルシューティング
  - データがキャプチャされていない
  - ポート設定の確認
  - ネットワーク
  - フィルタの確認
  - まとめ
- ラボ演習

モジュール 17：DLP Discover

- スキャン
- DLP Discover
- サポート対象リポジトリ
- サポート対象データベース
- DLP Discover のアーキテクチャ
- スキャンのタイプ
- 4つのタイプ
- 同時スキャンタスクとクロールレート
- インベントリスキャン
- ファイアウォール設定（ポート情報）
- 分類スキャン
- 登録スキャン
- データの登録

- シグネチャについて
- Signatures（署名）について
- 署名タイプの説明
- 検出スキャン
- 検出スキャンによる修復
- スキャンの設定前に
- DLP Manager への Discover の追加
- ラボ演習

モジュール 18：Discover ポリシー

- NDLP Discover のスキャン
- Schedules（スケジュール）
- Credentials（資格情報）
- Export Locations（エクスポート場所）
- SSL 対応のデータベースクローリング
- スキャンアクション
- スキャンの状態
- シナリオ – PII（個人情報）のスキャンを作成
- インベントリスキャン
- Node Definition（ノード定義）
- Single IP（単一 IP）の資格情報のチェック
- ノード定義のフィルタリング
- フィルタ
- Advanced Options（詳細オプション）
- Advanced Options（詳細オプション）
  - レート制限
- スキャンの実行
- スキャン結果
- 分類スキャン
- データ分類
- Data Classification（データ分類）
- 分類スキャン - データ分類
- 定義済みビュー - OLAP ナビゲータ
- 検出スキャン
- 検出スキャンのポリシー
- 検出スキャンによる修復
- アクションルールによる修復
- インシデントの修復
- 登録スキャン
- ラボ演習

モジュール 19：Email Prevent

- NDLP Email Prevent とは？
- アーキテクチャ：Prevent-Email
- NDLP Prevent の冗長化
- 導入ガイドライン – Prevent Email
- ファイアウォールの設定（ポート情報）
- Prevent のネットワーク / コンテンツフィルタ
- MEG と DLP Prevent の統合手順
- MEG ポリシー – NDLP Prevent にダイレクト
- MEG ポリシー – カスタムヘッダー辞書
- MEG ポリシー – ポスト NDLP Prevent ポリシー
- MEG コンプライアンスルール
- NDLP Prevent の MTA アクセス
- ラボ演習

モジュール 20：Email Prevent ポリシー

- NDLP Email Prevent
- NDLP Email Prevent のアクション
- NDLP Email Prevent に許可されているアクション
- NDLP Email Prevent ポリシーのフロー
- NDLP ポリシーの設定
- アプライアンスによる NDLP アクション
- NDLP Prevent ポリシー
- NDLP Prevent のトラブルシューティング
- Tcpdump
- mailq
- maillog
- ラボ演習

モジュール 21：Web Prevent

- NDLP Web Prevent とは？
- データフロー
- NDLP Prevent の冗長化
- 導入ガイドライン – PreventWeb
- ファイアウォールの設定（ポート情報）
- MWG と DLP Prevent の統合手順
- ライブラリルールの追加
- ルールセットの位置
- [Data Loss Prevention With ICAP] ルール
- Req Mod 設定

モジュール 22：Web Prevent ポリシー

- NDLP Prevent（Web）ポリシー
- NDLP Prevent（Web）ブロックページ
- www.csm-testcenter.org
- NDLP Prevent のトラブルシューティング
- Tcpdump
- ラボ演習

モジュール 23：インシデント管理

- ケース管理
- DLP インシデント管理
- サポートされるインシデントのタイプ
- インシデント管理 - 管理対象アプライアンス
- Manager でのインシデント管理
- インシデントダッシュボード – インシデントタイプ
- インシデントの表示形式
- さまざまな形式でのインシデントの表示
- インシデントアクション
- インシデントダッシュボードのオプション
- インシデントのビューとレポートのスケジュール
- インシデントのポリシー権限
- インシデント修正ワークフロー
- ケースとインシデント管理
- ケースの作成
- インシデントからケースの作成
- 既存のケースへのインシデントの追加
- Customize Case Config（ケース設定のカスタマイズ）オプション
- Customize Case Config（ケース設定のカスタマイズ）ページ
- Case Attachment（ケースの添付ファイル）
- ケース管理の権限

- ケースレベルの権限
- ケースのグループタスクの権限
- ケースの権限 - まとめ
- NDLP のケースワークフロー
- ケース管理のベストプラクティス
- ケース管理ワークフローの例
- ラボ演習

モジュール 24：ダッシュボードとレポート

- ダッシュボードとレポート
- 事前定義済みの表とチャート
- リスク分析グラフ
- ホームページとチャートのカスタマイズ
- Network Statistics（ネットワーク統計情報）
- エクスポート可能なインシデント
- エクスポート可能なケース
- エクスポート可能な検索
- エクスポートデータのカスタマイズ
- ラボ演習

モジュール 25：ルールの調整とベストプラクティス

- 誤検出
- 誤検出の低減
- ネットワークフィルタ
- コンテンツフィルタ
- ポリシー – インシデントの抑制
- ポリシー抑制インシデントルールの変更
- ルールの修正
- ルールの調整
- ルールの調整 - Proximity（近接）
- ルールのベストプラクティス

モジュール 26：ケーススタディのレビュー

- 導入シナリオのレビュー
- 導入シナリオのレビュー
- McAfee Medical Services
- 医療 - ファイルの統合
- 医療 – ファイル転送の制限
- McAfee Chemical Corporation
- 化学薬品会社 – IP（知的財産）検出の通知
- 化学薬品会社 - PI 転送を許可
- McAfee Federal
- 銀行 - ルール感度
- 銀行 - インシデント / ケース管理

マカフィー株式会社　www.mcafee.com/jp

東 京 本 社　〒 150-0043　東京都渋谷区道玄坂 1-12-1　渋谷マークシティウエスト 20F　TEL：03-5428-1100（代）　FAX：03-5428-1480
西日本支店　〒 530-0003　大阪府大阪市北区堂島 2-2-2　近鉄堂島ビル 18F　TEL：06-6344-1511（代）　FAX：06-6344-1517