製品ガイド

McAfee Endpoint Security for Linux 脅威対策 10.2.0

目次

スタンドアロンの Linux システムの保護

管理対象の Linux システムの保護

目次

まえがき

このガイドでは、McAfee 製品の操作に必要な情報を提供します。

目次

このガイドについて

ここでは、このガイドの対象読者、表記規則とアイコン、構成について説明します。

対象読者

McAfee では、対象読者を限定してマニュアルを作成しています。

このガイドの情報は、主に以下の読者を対象としています。

- **管理者** — 企業のセキュリティ プログラムを実装し、施行する担当者。
- **ユーザー** — このソフトウェアが実行されているコンピューターを使用し、ソフトウェアの一部またはすべての機能にアクセスできるユーザー。

表記法則

このガイドでは、以下の表記規則とアイコンを使用しています。

イタリック	マニュアル、章またはトピックのタイトル、新しい用語、語句の強調を表します。
太字	特に強調するテキストを表します。
モノスペース	コマンド、ユーザーが入力するテキスト、コードのサンプル、画面に表示されるメッセージを表します。
[やや狭い太字]	オプション、メニュー、ボタン、ダイアログ ボックスなど、製品インターフェースのテキストを表します。
青色のハイパーテキスト	トピックまたは外部サイトへのリンクを表します。
	**注:** 読み手に注意を促す場合や、別の操作手順を提示する場合に使用します。
	**ヒント:** ベストプラクティスの情報を表します。
	**重要/注意:** コンピューター システム、ソフトウェア、ネットワーク、ビジネス、データの保護に役立つ情報を表します。
	**警告:** ハードウェア製品を使用する場合に、身体的危害を回避するための重要な注意事項を表します。

製品マニュアルの検索

[ServicePortal] では、リリースされた製品の情報 (製品マニュアル、技術情報など) を入手できます。

タスク

1 [ServicePortal] (https://support.mcafee.com) に移動して、[Knowledge Center] タブをクリックします。

2 [Knowledge Base] ペインの [コンテンツのソース] で [製品マニュアル] をクリックします。

3 製品とバージョンを選択して [検索] をクリックします。マニュアルの一覧が表示されます。

1 概要

McAfee® Endpoint Security for Linux 脅威対策は、脅威と不審なソフトウェアを検出し、設定に基づいて環境を保護します。

ソフトウェアはスタンドアロンのシステムと管理対象システムで使用できます。

- **スタンドアロン システムの場合** — ユーザーまたはシステム管理者がソフトウェアをインストールし、設定を行うことができます。
- **管理対象システムの場合** — システム管理者がこれらのサーバーを使用してセキュリティ ポリシーのセットアップと設定を行います。
  - McAfee® ePolicy Orchestrator® (McAfee ePO™)
  - McAfee® ePolicy Orchestrator® Cloud (McAfee ePO™ Cloud)

McAfee Endpoint Security for Linux 脅威対策は、McAfee® VirusScan® Enterprise for Linux に続く Linux システムの新しいマルウェア対策です。 McAfee VirusScan Enterprise for Linux から McAfee Endpoint Security for Linux に移行すると、使用されているオペレーティング システムに関係なく、環境内のすべてのシステムのセキュリティを 1 つの拡張ファイルで一元管理できます。 McAfee® Endpoint Security 拡張ファイルを使用すると、Windows、Mac、Linux システムを管理できます。

目次

脅威対策によるシステムの保護

McAfee Endpoint Security for Linux 脅威対策は、インストール後すぐに Linux システムの保護を開始します。

脅威対策は、マルウェアや不審な項目を検出すると事前定義のアクションを実行し、マルウェアから Linux システムを保護します。

有効にすると、脅威対策はスキャンを実行してウイルス、トロイの木馬、不審なプログラムなどの脅威を検出します。ユーザーが項目へのアクセスや項目の作成を行うたびに、ローカル上のファイルやフォルダー、ネットワーク上のボリューム、リムーバブル メディアのスキャンが実行されます。 オンデマンドでスキャンを実行することもできます。

このソフトウェアは最新のマルウェア対策エンジンを使用して以下を実行します。

- マルウェア定義ファイル (DAT) を使用して複雑な解析を実行する。
- ユーザーがアクセスする項目の内容をデコードする。
- デコードした内容を DAT ファイルに保存されている既知の署名と比較してマルウェアを特定する。

オンアクセス スキャンとオンデマンド スキャンのアクションを設定したり、スキャンからファイルやパスを除外するには、脅威対策のオプションを使用します。

製品の機能

次の機能により、Linux システムで脅威の防止と検出、保護対策の調整と管理を行います。

防止 — 脅威の回避

- **製品更新** クライアント タスク — McAfee ダウンロード サイトに接続して、エンジンとコンテンツ ファイルを自動的に更新します。
- **5800 エンジンのサポート** — 最新の 5800 エンジンが搭載され、検出機能が強化されています。
- **Extra.DAT** — ウイルスのアウトブレークを阻止するため **Extra.DAT** ファイルをダウンロードし、インストールします。

検出 — 脅威の検出

- **オンアクセス スキャン** — ユーザーがファイルやディレクトリにアクセスする際、これらをスキャンして脅威を検出します。
- **オンデマンド スキャン** — ファイルやディレクトリのスキャンを特定の時刻にスケジュール設定します。 各オンデマンド スキャンにはそれぞれのポリシー設定が含まれています。 また、管理対象システムでフル スキャンやクイック スキャンも実行できます。
- **ポリシー別のオンデマンド スキャン クライアント タスク** — McAfee ePO からクライアントでクイック スキャンまたはフル スキャンを実行します。 オンデマンド スキャンのポリシー設定でスキャンの動作を設定します。

対応 — 脅威の処理

製品のログ ファイル、自動アクション、他の通知機能を使用して、検出の処理に最適な方法を決定します。

- **アクション** — 脅威の検出時に実行するアクションを設定します。

調整 — 保護状況の監視、分析、調整

システムのパフォーマンスを改善し、ウイルス対策を強化するため、設定を監視して分析します。 次のツールと機能を使用します。

- **クエリー、ダッシュボード、サーバー タスク McAfee ePO** () — アクティビティと検出を監視します。
- **ログ ファイル (McAfee® Endpoint Security for Linux 脅威対策クライアント)** — 検出項目の履歴を表示します。 この情報を分析することで、保護を強化する必要性や、設定を変更してシステム パフォーマンスを改善する必要性を判断できる場合があります。
- **スケジュール タスク** — クライアント タスク (製品更新など) やスキャン時間を変更し、ピーク時以外にタスクを実行してパフォーマンスを改善します。
- **スキャン ポリシー** — パフォーマンスを改善し、ウイルス対策を強化するため、ログ ファイルまたはクエリーを分析し、ポリシーを変更します。 たとえば、除外対象を設定してパフォーマンスを改善します。
- **スキャンからファイルとディレクトリを除外する** — ファイルの種類、拡張子、ワイルドカードなどの条件を使用して、オンアクセス スキャンやオンデマンド スキャンから特定のファイルやディレクトリを除外します。
- **ネットワーク ボリュームと圧縮ファイルをスキャンするオプション** — マウントされているネットワーク ボリュームと圧縮ファイルをスキャンの対象にするかどうか設定します。
- **クライアント サイドの除外を保持するオプション** — 管理対象の環境で、オンアクセス スキャンのクライアント除外リストを上書きまたは保持します。
- **Windows、Macintosh、Linux システムを管理する共通の拡張ファイル** — McAfee® Endpoint Security 拡張ファイルを Windows、Macintosh、Linux システムのポリシーを管理する共通の拡張ファイルとして使用します。

- **共通の McAfee ePO ePO ダッシュボードとクエリー** −McAfee ePO ダッシュボードを使用して、管理対象システムのステータスを表示します。
- **McAfee® ePolicy Orchestrator® Cloud (McAfee ePO™ Cloud) のサポート** − McAfee ePO Cloud でシステムのポリシーを管理できます。
- **クライアント システムからのデバッグ ロギングの有効化** − コマンドラインを使用して、クライアント システムからデバッグ ロギングを有効にします。

スタンドアロンの Linux システムの保護

ソフトウェアをインストールして 脅威対策を設定し、スタンドアロンの Linux システムを保護します。

2 スタンドアロンの Linux システムへのソフトウェアのインストール

RPM または Ubuntu ベースのスタンドアロン システムにソフトウェアをインストールします。

目次

システム要件

インストールに成功するには、システムが要件を満たしている必要があります。

コンポーネント	要件
プロセッサー	• Intel Extended Memory 64 テクノロジ (Intel EM64T) をサポートする Intel x86_64 アーキテクチャ ベースのプロセッサー • AMD 64 ビット テクノロジを搭載した AMD x86_64 アーキテクチャ ベースのプロセッサー
メモリー	最小: 2 GB RAM 推奨: 4 GB RAM

コンポーネント	要件
ディスクの空き容量	最小: 1 GB

オペレーティング システム (64 ビット)	• オペレーティング システム (64 ビット)
	  • SUSE Linux Enterprise Server/Desktop 11.x SP2 以降、12.x.
	  • Red Hat Enterprise Linux 6.x、7.x
	  • Ubuntu 12.04、14.04、15.x、16.04
	  • Amazon Linux AMI 2014 以降
	  • CentOS 6.x、7.x
	  • Amazon Elastic Compute Cloud (Amazon EC2) 上で稼働する SUSE および Ubuntu
	  • Red Hat Enterprise Linux 7 — Amazon Elastic Compute Cloud (Amazon EC2)
	  • Novell Open Enterprise Server 11 SP1
	  • Oracle Enterprise Linux 6.x、7.x — Red Hat および UEK 6.7.
	  この製品は、32 ビット プラットフォームで使用できません。
	• 仮想プラットフォーム
	  • VMware
	  • Citrix Xen
	  • Xen
	  • KVM
	  • Virtual box
	• 準仮想化環境 — Xen Hypervisor 上のゲスト OS

RPM ベース システムで署名を確認する

ソフトウェアをインストールする前に、署名を検証して正規のソフトウェアかどうか確認します。

タスク

1 root ユーザーとしてシステムにログオンします。

2 ソフトウェア ダウンロード サイトからパブリック キー (GPG) を取得します。

3 次のコマンドを実行して、パブリック キーを RPM DB にインポートします。

```
rpm --import <パブリック キー名>
```

このコマンドでパブリック キーをインポートしないと、インストールの実行中に次の警告メッセージが表示されます。

```
/tmp/tmp.FdcQqEpF3i/ISecTP-<バージョン番号>-<ビルド番号>.x86_64.rpm: Header V4 RSA/SHA1 Signature, key ID <キー番号>: NOKEY
```

4 署名を確認します。

```
rpm -K ISecESP-<バージョン番号>-<ビルド番号>_x86_64.rpm
rpm -K ISecRT-<バージョン番号>-<ビルド番号>_x86_64.rpm
rpm -K ISecTP-<バージョン番号>-<ビルド番号>_x86_64.rpm
rpm -K ISecESPFileAccess-<バージョン番号>-<ビルド番号>_x86_64.rpm
```

`ISecESP-<バージョン番号>-<ビルド番号>.x86_64.rpm: rsa sha1 (md5) pgp md5 OK` に類似したメッセージが表示されます。

Ubuntu システムで署名を確認する

Ubuntu データベースの GPG を更新し、正規のソフトウェアがインストールされていることを確認します。

タスク

1 root ユーザーとしてシステムにログオンします。

2 ソフトウェア ダウンロード サイトからパブリック キー (GPG) を取得します。

3 パブリック キーをインポートします。

```
gpg —import <パブリック キー>
```

4 署名を確認します。

```
dpkg-sig -verify ISecESP-<バージョン番号>-<ビルド番号>_64.deb
dpkg-sig -verify ISecRT-<バージョン番号>.<ビルド番号>_64.deb
dpkg-sig -verify ISecTP-<バージョン番号>.<ビルド番号>_64.deb
dpkg-sig -verify ISecESPFileAccess-<バージョン番号>-<ビルド番号>_64.deb
```

`Processing ISecTP-<バージョン番号>-<ビルド番号>_64.deb... GOODSIG _gpgbuilder 284E8BE753AE45DFF8D82748DDDF2F4CE732A79A 1414371553` に類似したメッセージが表示されます。

スタンドアロンの Linux システムにソフトウェアをインストールする

コマンドラインを使用して、RPM または Ubuntu ベースのシステムにソフトウェアをインストールします。

開始する前に

ソフトウェアをインストールするシステムに McAfee Agent がインストールされている必要があります。 ソフトウェアのインストール方法については、ご使用のバージョンの『McAfee Agent 製品ガイド』を参照してください。

競合するソフトウェアをシステムから削除します。 競合するソフトウェアがシステム上に存在する場合、McAfee Endpoint Security for Linux は使用できません。

タスク

1 root ユーザーとしてシステムにログオンします。

2 コンピューターの一時ディレクトリに `ISecTP-<バージョン番号>-<ビルド番号>-Release-standalone.tar.gz` をダウンロードします。

3 パッケージを展開します。

```
tar -zxvf ISecTP-<バージョン番号>-<ビルド番号>-Release-standalone.tar.gz
```

4 ソフトウェアを展開したディレクトリからインストール スクリプトを実行します。

```
sudo ./install-isectp.sh
```

5 [使用許諾条件] の内容を確認して `q` と入力して次に進みます。

6 同意する を入力して **Enter** を押します。

McAfee Endpoint Security for Linux では、**nails.options** ファイルを使用できません。

インストール スクリプト (`install-isectp.sh`) を使用してソフトウェアをインストールすると、オンアクセス スキャン オプションがデフォルトで有効になります。 オンアクセス スキャンを有効にする必要がある場合には、コマンドラインからいつでも有効にできます。

オンアクセス スキャンを無効にしてソフトウェアをインストールするには、次のコマンドを実行します。

ソフトウェアを展開したディレクトリから `sudo ./install-isectp.sh oasoff` を実行します。

コマンドラインからオンアクセス スキャンを有効にする方法については、『オンアクセス スキャンを有効または無効にする』または manpage のヘルプを参照してください。

パッケージ管理ツールでソフトウェアをインストールする

Yellowdog Updater Modified (YUM)、**Advanced Packaging Tool (APT)** または **Zypper** パッケージ管理ツールを使用して、ソフトウェアをインストールします。

YUM、**APT**、**Zypper** リポジトリから McAfee Endpoint Security for Linux 脅威対策をインストールすると、オンアクセス スキャンはデフォルトで無効になります。 インストール後にオンアクセス スキャンを有効にするには、コマンドラインを使用します。 コマンドラインからオンアクセス スキャンを有効にする方法については、『オンアクセス スキャンを有効または無効にする』または **manpage** のヘルプを参照してください。

タスク

- 19 ページの「*YUM リポジトリからソフトウェアをインストールする*」
  リポジトリからソフトウェアをインストールします。
- 19 ページの「*Zypper リポジトリからソフトウェアをインストールする*」
  Zypper リポジトリからソフトウェアをインストールします。
- 19 ページの「*Advanced Packaging Tool (APT) リポジトリからソフトウェアをインストールする*」
  APT リポジトリからソフトウェアをインストールする

YUM リポジトリからソフトウェアをインストールする

リポジトリからソフトウェアをインストールします。

開始する前に

次の RPM ファイルが YUM リポジトリに追加されていることを確認してください。

- ISecESP-<バージョン番号>-<ビルド番号>_x86_64.rpm
- ISecRT-<バージョン番号>-<ビルド番号>_x86_64.rpm
- ISecTP-<バージョン番号>-<ビルド番号>_x86_64.rpm
- ISecESPFileAccess-<バージョン番号>-<ビルド番号>_x86_64.rpm

タスク

- ソフトウェアをインストールします。

```
yum install ISecTP
```

Zypper リポジトリからソフトウェアをインストールする

Zypper リポジトリからソフトウェアをインストールします。

開始する前に

次の RPM ファイルが Zypper リポジトリに追加されていることを確認してください。

- ISecESP-<バージョン番号>-<ビルド番号>_x86_64.rpm
- ISecRT-<バージョン番号>-<ビルド番号>_x86_64.rpm
- ISecTP-<バージョン番号>-<ビルド番号>_x86_64.rpm
- ISecESPFileAccess-<バージョン番号>-<ビルド番号>_x86_64.rpm

タスク

- ソフトウェアをインストールします。

```
zypper install ISecTP
```

Advanced Packaging Tool (APT) リポジトリからソフトウェアをインストールする

APT リポジトリからソフトウェアをインストールする

開始する前に

次のファイルが APT リポジトリに追加されていることを確認してください。

- ISecESP-<バージョン番号>-<ビルド番号>_64.deb
- ISecRT-<バージョン番号>-<ビルド番号>_64.deb
- ISecTP-<バージョン番号>-<ビルド番号>_64.deb
- ISecESPFileAccess-<バージョン番号>-<ビルド番号>_64.deb

タスク

- ソフトウェアをインストールします。

```
apt-get install ISecTP
```

ソフトウェアのアップグレード

ソフトウェアをアップグレードして、McAfee VirusScan Enterprise for Linux から設定を移行できます。

サポートされるアップグレード方法

McAfee Endpoint Security for Linux 脅威対策では、インストール済みのバージョンからソフトウェアをアップグレードし、スキャン設定を移行できます。

次のソフトウェアのアップグレードが可能です。

- McAfee VirusScan Enterprise for Linux 1.9.2
- McAfee VirusScan Enterprise for Linux 2.x

ソフトウェアをアップグレードすると、マルウェア対策の環境設定が脅威対策の設定に移行されます。

非対応のバージョンがインストールされている場合には、ソフトウェアを対応バージョンにアップグレードしてから McAfee Endpoint Security for Linux 脅威対策にアップグレードしてください。

スタンドアロンの Linux システムのソフトウェアをアップグレードする

McAfee VirusScan Enterprise for Linux 1.9.2 または 2.x からソフトウェアをアップグレードします。

開始する前に

システムでアップグレード可能な対応バージョンが実行されていることを確認してください。

タスク

1 root ユーザーとしてシステムにログオンします。

2 コンピューターの一時ディレクトリに `ISecTP-<`バージョン番号`>-<`ビルド番号`>-Release-standalone.tar.gz` をダウンロードします。

3 パッケージを展開します。

```
tar -zxvf ISecTP-<バージョン番号>-<ビルド番号>-Release-standalone.tar.gz
```

4 ソフトウェアをダウンロードしたディレクトリからコマンドを実行します。

```
./install-isectp.sh
```

前のバージョンからアップグレードするには、`./install-isectp.sh` スクリプトを使用します。 McAfee VirusScan Enterprise for Linux 1.9.2 からアップグレードしたら、システムを再起動します。

デフォルトの設定を表示する

ソフトウェアのインストールが完了したら、デフォルトの設定を表示し、ビジネス要件に合わせて設定を調整します。

タスク

1 root ユーザーとしてシステムにログオンします。

2 次のディレクトリに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 次のコマンドを実行します。

- 製品バージョンを表示します。
  ```
  ./isecav --version
  ```
- オンアクセス スキャンの状態と設定を表示します。
  ```
  ./isecav --getoasconfig --summary
  ```
- 標準プロセスのデフォルトの設定を表示します。
  ```
  ./isecav --getoasprofileconfig standard
  ```
- 危険度高プロセスのデフォルトの設定を表示します。
  ```
  ./isecav --getoasprofileconfig highrisk
  ```
- 危険度低プロセスのデフォルトの設定を表示します。
  ```
  ./isecav --getoasprofileconfig lowrisk
  ```
- 危険度高と危険度低に設定されたプロセスを表示されます。
  ```
  ./isecav --getoasconfig --processlist
  ```
- 標準プロセスで除外リストに追加されたファイルを表示します。
  ```
  ./isecav --getoasconfig --exclusionlist --profile standard
  ```
- 危険度高プロセスで除外リストに追加されたファイルを表示します。
  ```
  ./isecav --getoasconfig --exclusionlist --profile highrisk
  ```
- 危険度低プロセスで除外リストに追加されたファイルを表示します。
  ```
  ./isecav --getoasconfig --exclusionlist --profile lowrisk
  ```
- デフォルト タスクのリストを表示します。
  ```
  ./isecav --listtasks
  ```

インストールをテストする

ソフトウェアが適切にインストールされ、システムを保護できることを確認するため、ソフトウェアのテストを行います。

開始する前に
オンアクセス スキャンが有効になっている必要があります。

EICAR 標準ウイルス対策テスト ファイルにアクセスして、脅威対策の機能をテストします。 このファイルは、ウイルス対策ソフトウェアを検証するために使用できる、ウイルス対策ソフトウェアのメーカーが共同で開発した標準規格です。

タスク

1 root ユーザーとしてシステムにログオンします。

2 EICAR テスト ファイルをダウンロードします。
```
wget www.eicar.org/download/eicar.com.txt
```

3 ログ ファイルで検出結果を確認します。

デフォルトのログ ファイルは、`/opt/isec/ens/threatprevention/var/isecoasmgr.log` です。

スタンドアロンの Linux システムからのソフトウェアの削除

コマンド ラインを使用してスタンドアロン システムからソフトウェアを削除します。

タスク

1 root ユーザーとしてシステムにログオンします。

2 次のディレクトリに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 次のコマンドを実行します。

```
./uninstall-isectp.sh
```

4 プロンプトが表示されたら、`yes` と入力します。

3 McAfee Endpoint Security for Linux の管理

ソフトウェアの設定を定義したり、変更します。また、ソフトウェアに関する情報を表示します。

目次

isecav コマンドライン ヘルプ

isecav は、タスクの実行や McAfee Endpoint Security for Linux 脅威対策の設定を行うコマンドライン ツールです。

isecav コマンドは、スタンドアロンのシステムだけでなく、管理対象システムでも使用できます。 管理対象システムの場合、コマンドラインから行った設定がポリシー施行時に上書きされます。

コマンドライン ヘルプにアクセスする前に、ヘルプで使用されている基本的な用語について理解しておくことをお勧めします。

プロセスの種類

脅威対策では、すべてのプロセスに 1 つのオンアクセス スキャン設定を定義することも、プロセスの種類 (標準、危険度高、危険度低など) ごとに異なる設定を定義することもできます。

プロセス

脅威対策は、ファイルにアクセスするプロセス (プログラム) の危険度を判断します。 ファイルにアクセスすると、脅威対策はファイルにアクセスしたプロセスを識別し、プロセスに定義された危険度を確認して、プロセスの種類に応じて設定を適用します。 プロセスを危険度高または危険度低として定義できます。 プロセスがいずれのカテゴリにも定義されていない場合、プロセスの種類は標準に設定されます。 プロセスの種類が [すべてのプロセスに標準設定を使用する] に設定されている場合、すべてのプロセスは標準プロセスとして処理されます。

たとえば、組織によっては、Web サイト経由で未知のファイルにアクセスしたときに、システムに脅威をもたらす行為と見なされる場合があります。 このような脅威からシステムを保護するには、Chrome を危険度高プロセスに追加し、設定を指定します。

必要であれば、コマンドラインを使用すると、危険度のカテゴリにプロセスを追加、編集または削除できます。 プロセス カテゴリにプロセスを追加、変更、削除する方法については、『プロセスの設定を定義する』を参照してください。

インデックス

インデックスは、**isecav** がリストのタスクまたはプロセスの識別に使用する固有の番号です。

複数のオンデマンド スキャン タスクを作成すると、タスクは順序番号に従って表示されます。 スキャン タスクは、インデックスという固有の番号で区別できます。

```
 ---------------------------------------------------------------------------------------------------
| No Task Name                                Task Type        Task Status      Last Run            |
 ---------------------------------------------------------------------------------------------------
|  1 test2__task                              ODS              Not Started                          |
|  2 KTods                                    ODS              Completed                            |
 ---------------------------------------------------------------------------------------------------
```

たとえば、次のリストには 2 つのオンデマンド スキャン スケジュールが指定されています。 オンデマンド スキャのタスク (`KTods`) を実行するには、`/opt/isec/ens/threatprevention/bin` ディレクトリから次のコマンドを実行します。

```
./isecav --runtask --index 2.
```

IsecTP ヘルプにアクセスする

コマンドラインから **IsecTP** ヘルプにアクセスして、設定を表示したり、タスクを実行します。

タスク

1. root ユーザーとしてシステムにログオンします。
2. 次のディレクトリに移動します。

   ```
   /opt/isec/ens/threatprevention/bin
   ```

3. 次のコマンドを実行します。

   ```
   isecav --help
   ```

プロセスのリスク カテゴリを定義する

リスク カテゴリにプロセスを追加したり、プロセスのリスク カテゴリを変更できます。カテゴリからプロセスを削除することもできます。

タスク

- 25 ページの「*カテゴリにプロセスを追加する*」
  コマンドラインからプロセス カテゴリ (危険度高、危険度低または標準) にプロセスを追加します。
- 25 ページの「*プロセスの危険度を変更する*」
  コマンドラインからプロセスのリスク カテゴリを変更します。
- 25 ページの「*リスク カテゴリからプロセスを削除する*」
  不要になったプロセスをリスク カテゴリから削除します。

カテゴリにプロセスを追加する

コマンドラインからプロセス カテゴリ (危険度高、危険度低または標準) にプロセスを追加します。

タスク

1 root ユーザーとしてシステムにログオンします。

2 次のディレクトリに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 次のコマンドを実行します。

```
./isecav --addprocess --profile_type process_name
```

例: Chrome プロセスを危険度高カテゴリに追加する

Chrome は Web サイトの閲覧に使用するブラウザーです。 閲覧中に書き込み操作を行い、ページの保存やファイルのダウンロードを実行できます。 また、閲覧中にブラウザーが Cookie ファイルをユーザーの `/tmp` ディレクトリに追加する場合があります。 Chrome を危険度高カテゴリに追加して [書き込み時にスキャン] オプションを有効にすると、Chrome プロセスから書き込み操作が実行された場合にのみスキャンを実行することができます。

Chrome を危険度高カテゴリに追加するには、次のコマンドを実行します。

```
./isecav --addprocess --highrisk /usr/bin/google-chrome
```

プロセスの危険度を変更する

コマンドラインからプロセスのリスク カテゴリを変更します。

タスク

1 root ユーザーとしてシステムにログオンします。

2 次のディレクトリに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 次のコマンドを実行します。

```
./isecav --setprocess --profile_type process_name
```

例: Chrome プロセスのリスク カテゴリを危険度高から危険度低に変更する

Chrome プロセスのリスク カテゴリを危険度高から危険度低に変更するには、次のコマンドを実行します。

```
./isecav --setprocess --lowrisk /usr/bin/google-chrome
```

リスク カテゴリからプロセスを削除する

不要になったプロセスをリスク カテゴリから削除します。

タスク

1 root ユーザーとしてシステムにログオンします。

2 次のディレクトリに移動します。

```
/opt/isec/ens/threatprevention/bin
```

3 次のコマンドを実行します。

```
./isecav --delprocess --index <インデックス番号>
```

例: Chrome を危険度高カテゴリから削除する

危険度高カテゴリから Chrome を削除するには、Chrome プロセスのインデックス番号が必要です。

1 すべてのプロセスを表示するには、`./isecav --getoasconfig --processlist` コマンドを実行します。

```
-------------------------------------------------------------------------------
|No    Process Name                                                Process Type    |
-------------------------------------------------------------------------------
|1     /usr/bin/google-chrome                                      High Risk       |
-------------------------------------------------------------------------------
```

このリストでは、Chrome プロセスのインデックス番号が 1 になっています。

2 `./isecav --delprocess --index 1` コマンドを実行します。

オンアクセス スキャンを管理する

オンアクセス スキャンはバックグラウンドで実行されます。アクセスの発生時にコンピューターをスキャンし、ウイルスなどの脅威を検出します。 オンアクセス スキャンのオプションは組織レベルまたはプロファイル レベルで設定できます。

タスク

- 26 ページの「*オンアクセス スキャンの状態を確認する*」
  オンアクセス スキャンが有効かどうか確認します。
- 27 ページの「*オンアクセス スキャンを有効または無効にする*」
  必要に応じて、オンアクセス スキャンを有効または無効にします。
- 27 ページの「*標準プロセスのオンアクセス スキャンを設定する*」
  コマンドラインから標準プロセスのオンアクセス スキャンを設定します。
- 28 ページの「*オンアクセス スキャンからファイルを除外する*」
  オンアクセス スキャンのプロファイルを設定して、除外対象を追加します。

オンアクセス スキャンの状態を確認する

オンアクセス スキャンが有効かどうか確認します。

タスク

1 root ユーザーとして Linux システムにログオンします。

2 ソフトウェアの /bin フォルダーに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 オンアクセス スキャン タスクの設定を表示します。

```
./isecav --getoasconfig --summary
```

4 コマンドの出力結果から On-Access Scan の値 (Enabled または Disabled) を確認します。

オンアクセス スキャンを有効または無効にする

必要に応じて、オンアクセス スキャンを有効または無効にします。

タスク

1 root ユーザーとしてシステムにログオンします。

2 /bin ディレクトリに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 スキャンを有効または無効にします。

- オンアクセス スキャンを有効にする: `./isecav --setoasglobalconfig --oas on`
- オンアクセス スキャンを無効にする: `./isecav --setoasglobalconfig --oas off`

標準プロセスのオンアクセス スキャンを設定する

コマンドラインから標準プロセスのオンアクセス スキャンを設定します。

タスク

1 root ユーザーとして Linux システムにログオンします。

2 /bin ディレクトリに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 標準プロセスの現在の設定を確認します。

```
./isecav --getoasprofileconfig standard
```

4 標準プロセスの設定を定義します。

```
./isecav --setoasprofileconfig --profile standard [オプション]
```

例: オンアクセス スキャンを設定する (標準プロセス)

```
./isecav --setoasprofileconfig --profile standard --setmode
sor --filetypestoscan all --onscanerror deny --onscantimeout deny --networkscan
enable --scanarchive disable --scanmime enable --scanunknownprograms
enable --scanunknownmacros disable --primaryaction clean --secondaryaction
delete --primaryactionpup clean --secondaryactionpup delete
```

このコマンドを実行すると、標準プロセスに次の設定が定義されます。

- スキャンのタイミング ― 読み取り時
- スキャン対象 ― すべてのファイル
- スキャン エラー時 ― ファイルに対するアクセスを拒否
- スキャン タイムアウト ― ファイルに対するアクセスを拒否
- ネットワーク ボリュームのスキャン ― 有効
- アーカイブ ファイルのスキャン ― 無効
- MIME ファイルのスキャン ― 有効
- 不審なプログラムの検出 ― 有効
- 未知のマクロ脅威の検出 ― 無効
- 脅威を検出した場合の最初の対応 ― 駆除
- 最初の対応が失敗した場合 ― ファイルの削除
- 不審なプログラムを検出した場合の最初の対応 ― 駆除
- 最初の対応が失敗した場合 ― 削除

オンアクセス スキャンからファイルを除外する

オンアクセス スキャンのプロファイルを設定して、除外対象を追加します。

タスク

1 root ユーザーとして Linux システムにログオンします。

2 ソフトウェアの /bin フォルダーに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 次の構文のコマンドを実行します。

```
./isecav --setoasprofileconfig --profile [standard | highrisk | lowrisk] [除外オプション]
```

ファイルを除外するプロファイルの危険度 (`standard`、`highrisk` または `lowrisk`) を指定します。

危険度高と危険度低のプロセスは、`--procsettings` を `riskbased` に設定した場合のみ施行されます。 `--procsettings` を `standard` に設定すると、すべてのプロセスが標準プロセスとして定義されます。 ソフトウェアのヘルプを参照するには、`isecav --help` コマンドを実行します。

[除外オプション] には次のオプションを指定します。

- 次のいずれかのオプションを使用して、ファイルまたはディレクトリを除外する条件を指定します。

オプション	定義
`--addexclusionread`	読み取り操作時にオンアクセス スキャンから除外する対象を追加します。
`--addexclusionwrite`	書き込み操作時にオンアクセス スキャンから除外する対象を追加します。
`--addexclusionrw`	読み取り操作と書き込み操作時にオンアクセス スキャンから除外する対象を追加します。

- 次のオプションを使用して、除外するファイルまたはディレクトリを指定します。

オプション	定義
`--excludepaths`	指定したファイルまたはディレクトリがスキャン対象から除外されます。 次のガイドラインに従って、絶対ファイル名、ファイル名のみ、ディレクトリの絶対名を指定します。 • 値の一部としてワイルドカード [*、?] を使用できます。 • ファイルまたはディレクトリの絶対名は、[/] で始める必要があります。 • ディレクトリ名は、スラッシュ [/] で終わる必要があります。 • 複数の値をカンマで区切って指定できます。 • スペースを含む値を指定する場合には、値を二重引用符 ("") で囲んでください。
`--excludefiletype`	除外対象を指定します。 次のガイドラインに従って拡張子を指定します。 • 値の一部としてワイルドカード [?] を使用できます。 • 複数の値をカンマで区切って指定できます。 • スペースを含む値を指定する場合には、値を二重引用符 ("") で囲んでください。
`--excludesubfolder`	特定のディレクトリ内で除外するサブフォルダーを指定します。

例: `--addexclusionread --excludepaths "/home/user1/,/home/user/file1" --excludefiletype "txt,doc,pdf" --excludesubfolder`

このコマンドにより、読み取り時に次のファイルがスキャンの対象外になります。

- /home/user1/ ディレクトリにあるすべてのファイル
- /home/user/file1
- 任意のファイル システムにあるすべての .txt、.doc または .pdf ファイル。

また、`--excludesubfolder` 属性を使用すると、指定したディレクトリのサブフォルダーもスキップされます。

オンデマンド スキャンを管理する

オンデマンド スキャン タスクを作成して設定し、スケジュールを設定します。

タスク

- 29 ページの「*オンデマンド スキャン タスクを作成する*」
  カスタム設定をスキャンを設定するには、オンデマンド タスクを作成します。
- 35 ページの「*オンデマンド スキャン タスクを実行する*」
  作成したオンデマンド タスクを実行します。
- 35 ページの「*オンデマンド スキャンの状態を確認する*」
  オンデマンド スキャンが有効になっているかどうかを確認します。
- 35 ページの「*オンデマンド スキャン タスクを削除する*」
  不要になったオンデマンド スキャン タスクを削除します。

オンデマンド スキャン タスクを作成する

カスタム設定をスキャンを設定するには、オンデマンド タスクを作成します。

タスク

1 root ユーザーとして Linux システムにログオンします。

2 ソフトウェアの /bin フォルダーに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 次の構文のコマンドを実行します。

```
./isecav --addodstask --name [タスク名] [追加オプション]
```

[タスク名] には、設定する名前を指定します。 タスク名は必須で、固有の値を指定する必要があります。

設定の異なる複数のタスクを設定することもできます。

[追加オプション] には、必要な設定を指定します。

オプション	値	説明	メモ
--scanarchive	enable (デフォルト) disable	.jar ファイルなどのアーカイブ ファイル (圧縮ファイル) 内のコンテンツをスキャンします。 アーカイブをスキャンすると、大量のリソースが消費されるため、パフォーマンスに影響を及ぼします。	
--scanmime	enable disable (デフォルト)	MIME (Multipurpose Internet Mail Extensions) 形式のファイルを検出し、デコードしてスキャンします。	
--scanpups	enable (デフォルト) disable	不審なプログラムを検出、デコード、スキャンします。	
--scanunknownprograms	enable (デフォルト) disable	未知のプログラム ファイルを検出、デコード、スキャンします。	
--scanunknownmacros	enable (デフォルト) disable	未知のマクロ ウイルスを検出、デコード、スキャンします。	
--scanlocaldrives	enable disable	ローカルにマウントされたファイル システムで通常のファイルをすべてスキャンします。	オンデマンド タスクが、設定されたファイルとディレクトリにスキャンを実行します。 以下のいずれかのオプションを使用して、スキャン パスを設定する必要があります。 --scanlocaldrives enable --scantmpfolders enable --scannetworkdrives enable --scanpaths [パス]

オプション	値	説明	メモ
`--scanpaths`	次のガイドラインに従って、絶対ファイル名、ファイル名のみ、ディレクトリの絶対名を指定します。 • ファイルまたはディレクトリの絶対名は、スラッシュ [/] で始める必要があります。 • ディレクトリ名は、スラッシュ [/] で終わる必要があります。 • 複数の値をカンマで区切って指定できます。 • スペースを含む値を指定する場合には、値を二重引用符 ("") で囲んでください。	指定したファイルまたはディレクトリがスキャン対象に追加されます。	
`--scantmpfolders`	`enable` `disable`	システムの次のディレクトリにあるすべてのファイルをスキャンします。 /tmp /usr/local/tmp /var/tmp	
`--scannetworkdrives`	`enable` `disable`	システムのすべてのネットワーク マウント ポイントをスキャンします。 システムにマウントされた NFS と CIFS 共有に制限されます。	

`--scansubfolders`	`enable`
	`disable`
		指定したフォルダーをスキャンします。	次のオプションを指定した場合にのみ使用できます。
			`scanlocaldrives`
			`scanpaths`
			`scantmpfolders`
			`scannetworkdrives`

オプション	値	説明	メモ
`--filetypestoscan`	• `all` (デフォルトの推奨) ー すべてのファイルをスキャンします。 • `defaultandspecified` ー デフォルトのファイルと指定した拡張子のファイルがスキャンされます。 • `onlyspecified` ー ユーザーが指定したファイルだけをスキャンします。`addfiletype` を使用して、1 つ以上のファイル タイプを指定します。	スキャンするファイルの種類を指定します。	
`--scanmacros`	`enable` `disable`	デフォルトのリストにある既知のマクロ脅威と指定したファイルをスキャンします。	`filetypestoscan` と一緒に使用する必要があります。
`--addfiletype`	拡張子 ー ファイルの種類を拡張子で指定します。ワイルドカード [?] も使用できます。 重複する項目は自動的に削除されます。	ファイルの種類をデフォルトのリストまたは指定したユーザー定義リストに追加します。	
`--delfiletype [拡張子]`	拡張子 ー 削除する項目を指定します。	ユーザー定義のファイル リストからファイルの種類を削除します。	
`--noextension`	`enable` `disable`	拡張子を付けずに、スキャンするファイルを指定します。	

オプション	値	説明	メモ
`--excludepaths`	次のガイドラインに従って、絶対ファイル名、ファイル名のみ、ディレクトリの絶対名を指定します。 • ワイルドカード [*、?] を使用できます。 • 複数の値をカンマで区切って指定できます。 • ファイルまたはディレクトリの絶対名は、スラッシュ [/] で始める必要があります。 • スペースを含む値を指定する場合には、値を二重引用符 ("") で囲んでください。 • ディレクトリ名は、スラッシュ [/] で終わる必要があります。	指定したファイルまたはディレクトリがスキャン対象から除外されます。	
`--excludefiletype`	拡張子。次のガイドラインに従って指定してください。 • ワイルドカード [?] を使用できます。 • 複数の値をカンマで区切って指定できます。 • スペースを含む値を指定する場合には、値を二重引用符 ("") で囲んでください。	除外対象の拡張子を指定します。	
`--excludesubfolder`	除外パスに指定したディレクトリのサブディレクトリを対象外にします。		`excludepaths` に指定したディレクトリにのみ適用されます。
`--usescancache`	`enable` `disable`	このタスクでファイルをスキャンするときに、オンアクセス スキャンのキャッシュを参照します。	

オプション	値	説明	メモ
--primaryaction	• continue — イベントは記録されますが、アクションは実行されません。 • clean (デフォルト) — 可能であれば、検出されたファイルから脅威を駆除します。 デフォルトでは、元のファイルは隔離されます。 • delete — 感染の可能性があるファイルを削除します。 デフォルトでは、元のファイルは隔離されます。	脅威検出に対する最初のスキャン アクションを設定します。 最初のアクションが失敗すると、次のアクションが実行されます。	
--secondaryaction	• continue — イベントは記録されますが、アクションは実行されません。 • delete (デフォルト) — 感染の可能性があるファイルを削除します。 デフォルトでは、元のファイルは隔離されます。	最初のアクションに失敗した場合に、このアクションが実行されます。	このオプションを使用するには、primaryaction に "clean" を指定する必要があります。 最初のアクションが「削除」の場合、2 番目のアクションに指定できるのは「続行」だけです。
--primaryactionpup	• continue — イベントは記録されますが、アクションは実行されません。 • clean (デフォルト) — 可能であれば、検出されたファイルから脅威を駆除します。 デフォルトでは、元のファイルは隔離されます。 • delete — 感染の可能性があるファイルを削除します。 デフォルトでは、元のファイルは隔離されます。	不審なプログラムに対する最初のスキャン アクションを設定します。 最初のアクションが失敗すると、次のアクションが実行されます。	
--secondaryactionpup	• continue — イベントは記録されますが、アクションは実行されません。 • delete (デフォルト) — 感染の可能性があるファイルを削除します。 デフォルトでは、元のファイルは隔離されます。	不審なプログラムに対する最初のアクションに失敗した場合に、このアクションが実行されます。	このオプションを使用するには、primaryaction に "clean" を指定する必要があります。

例: `./isecav --addodstask --name odstask --scanlocaldrives enable`

このコマンドにより、odstask という名前のオンデマンド タスクが追加されます。このタスクは、システムのローカル ドライブのみをスキャンします。

オンデマンド スキャン タスクを実行する

作成したオンデマンド タスクを実行します。

タスク

1 root ユーザーとして Linux システムにログオンします。

2 ソフトウェアの /bin フォルダーに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 次の構文のコマンドを実行します。

```
./isecav --runtask --index [インデックス番号]
```

[インデックス番号] には、実行するタスクのインデックス番号を指定します。 タスクの実行中は、このコマンドは実行されません。

オンデマンド スキャンの状態を確認する

オンデマンド スキャンが有効になっているかどうかを確認します。

タスク

1 root ユーザーとして Linux システムにログオンします。

2 ソフトウェアの /bin フォルダーに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 すべてのオンデマンド スキャン タスクの詳細を表示します。

```
./isecav --listtasks
```

4 コマンドの出力結果からオンデマンド スキャンの状態を確認します。

- Not Started — タスクはまだ実行していません。
- Running — タスクの実行中です。
- Stopped — 前回の実行がユーザーによって停止されています。
- Aborted — エラーのため、前回の実行がキャンセルされています。
- Completed — 前回の実行が正常に完了しています。

オンデマンド スキャン タスクを削除する

不要になったオンデマンド スキャン タスクを削除します。

タスク

1 root ユーザーとして Linux システムにログオンします。

2 ソフトウェアの /bin フォルダーに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 次の構文のコマンドを実行します。

```
./isecav --deltask --index [インデックス番号]
```

[インデックス番号] には、削除するタスクのインデックス番号を指定します。

DAT の更新スケジュールを設定する

DAT 更新タスクの実行方法 (すぐに実行、指定した時間、特定の間隔) を設定します。

更新タスクは次のタイミングで実行できます。

- [毎日] ー 毎日、指定した時間に更新を実行します。
- [毎週] ー 特定の曜日にタスクを実行します。 このオプションを指定する場合、曜日オプションを指定する必要があります。 複数の曜日を追加する場合には、カンマで区切って指定します。
- [毎月] ー 毎月、特定の日付にタスクを実行します。 このオプションを指定する場合、日付オプションを指定する必要があります。 複数の日付を追加する場合には、カンマで区切って指定します。
- [未指定] ー タスクのスケジュールを無効にします。
- [開始時間] ー 指定した時間にタスクを実行します。 時間は 24 時間形式で指定する必要があります。 たとえば、18:45 と入力します。

タスク

- 36 ページの「*DAT 更新タスクを作成する*」
  コマンドラインから DAT 更新タスクを作成します。
- 37 ページの「*DAT 更新タスクを実行する*」
  DAT の更新タスクをすぐに実行します。
- 37 ページの「*DAT 更新タスクのスケジュールを設定する*」
  指定した時間または特定の間隔で DAT 更新タスクを実行します。

DAT 更新タスクを作成する

コマンドラインから DAT 更新タスクを作成します。

タスク

1 root ユーザーとしてシステムにログオンします。

2 次のディレクトリに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 DAT 更新タスクを作成します。

```
./isecav --addupdatetask --name <タスク名> --updatetype --<更新の種類>
```

4 タスク リストを表示して、DAT 更新タスクが作成されていることを確認します。

```
./isecav --listtasks
```

例: DAT 更新タスクを作成する

```
./isecav --addupdate task --name datupdate --updatetype dat
```

`/opt/isec/ens/threatprevention/bin` ディレクトリからコマンドを実行すると、DAT 更新タスクが作成されます。

DAT 更新タスクを実行する

DAT の更新タスクをすぐに実行します。

タスク

1 root ユーザーとしてシステムにログオンします。

2 次のディレクトリに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 タスク リストで、DAT 更新タスクのインデックス番号を確認します。

```
./isecav --listtasks
```

4 DAT 更新タスクを実行します。

```
./isecav --runtask --index <インデックス番号>.
```

例: DAT 更新タスクを実行する

DAT 更新タスクのインデックス番号が 3 の場合、次のコマンドを実行します。

```
./isecav --runtask --index 3
```

DAT 更新タスクのスケジュールを設定する

指定した時間または特定の間隔で DAT 更新タスクを実行します。

開始する前に

DAT 更新タスクが作成されている必要があります。

タスク

1 root ユーザーとしてシステムにログオンします。

2 次のディレクトリに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 タスク リストを表示して、DAT 更新タスクが作成されていることを確認します。

```
./isecav --listtasks
```

4 タスクのスケジュールを設定します。

```
./isecav --scheduletask --index <インデックス番号> --daily --starttime <HH:MM>
```

例: 毎日 12.45 に DAT 更新タスクを実行するようにスケジュールを設定する

```
./isecav --scheduletask --index 3 --daily --starttime 12:45
```

`/opt/isec/ens/threatprevention/bin` ディレクトリからコマンドを実行すると、DAT 更新タスクが毎日 12:45 に実行されます。

製品ログを設定する

製品ログを有効または無効にします。ログ ファイルの最大サイズを定義します。

製品ログ ファイルには、すべてのイベントとアクティビティの詳細が時間付きで記録されます。 製品ログを有効にすると、製品の動作を詳しく確認できます。製品の問題を解決するときに役立ちます。

タスク

- 38 ページの「*製品ロギングを有効または無効にする*」
  必要に応じて、製品ロギングを有効または無効にします。
- 38 ページの「*製品ログ ファイルのサイズを設定する*」
  製品ログ ファイルの最大サイズを MB 単位で設定します。

製品ロギングを有効または無効にする

必要に応じて、製品ロギングを有効または無効にします。

タスク

1 root ユーザーとしてシステムにログオンします。

2 次のディレクトリに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 必要に応じて、次のコマンドを実行します。

- `./isecav --productlog enable` ー 製品ログを有効にします。
- `./isecav --productlog disable` ー 製品ログを無効にします。

製品ログ ファイルのサイズを設定する

製品ログ ファイルの最大サイズを MB 単位で設定します。

タスク

1 root ユーザーとしてシステムにログオンします。

2 次のディレクトリに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 次のコマンドを実行します。

```
./isecav --setmaxproductlogsize <数字>
```

1 MB ～ 999 MB の範囲でログ ファイルのサイズを指定できます。 デフォルト値は 10 MB です。

例: 製品ログ ファイルのサイズを 25 MB に設定する

次のコマンドを実行すると、製品ログ ファイルの最大サイズが 25 MB に設定されます。

```
./isecav --setmaxproductlogsize 25
```

イベントを Syslog に送信するようにソフトウェアを設定する

製品ログだけでなく、Syslog にも情報を記録するようにソフトウェアを設定します。

タスク

1 root ユーザーとして Linux システムにログオンします。

2 `/bin` ディレクトリに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 次のコマンドを実行します。

```
./isecav --usesyslog enable.
```

隔離ディレクトリを設定する

隔離項目を保存するディレクトリを指定します。

タスク

1 root ユーザーとして Linux システムにログオンします。

2 `/bin` ディレクトリに移動します。

```
cd /opt/isec/ens/threatprevention/bin
```

3 次のコマンドを実行します。

```
./isecav --setquarantinefolder /directory_path.
```

ディレクトリの絶対パスを指定する必要があります。

管理対象の Linux システムの保護

管理対象の Linux システムを脅威から保護するには、McAfee® Endpoint Security の拡張ファイルをインストールして、セキュリティ方針を配布します。

4 McAfee ePO で管理されているシステムへのソフトウェアのインストール

McAfee ePO で管理されているシステムにソフトウェアをインストールして管理します。

McAfee ePO は、セキュリティ製品とこれらの製品がインストールされたシステムのポリシーを一元的に管理し、施行できる拡張性に優れた管理プラットフォームです。

包括的なレポートの作成や製品の配備も一元的に管理できます。 ネットワーク内の管理対象システムにセキュリティ製品、パッチ、サービス パックを配備できます。

目次

システム要件

システム環境が次の要件を満たし、管理者権限があることを確認してください。

ソフトウェア	要件
McAfee Agent	McAfee Agent 5.0.3 以降
McAfee ePolicy Orchestrator	5.1.1 以降

McAfee ePO サーバーにパッケージをチェックインする

ソフトウェア マネージャーを使用するか手動でパッケージをチェックインすると、パッケージをチェックインできます。

タスク

- 44 ページの「*ソフトウェア マネージャーでパッケージをチェックインする*」
  ソフトウェア マネージャーを使用して、McAfee Endpoint Security for Linux をチェックインします。

- 44 ページの「*パッケージを手動でチェックインする*」
  McAfee Endpoint Security for Linux 配備パッケージを McAfee ePO マスター リポジトリに手動でチェックインし、ソフトウェアを管理します。

ソフトウェア マネージャーでパッケージをチェックインする

ソフトウェア マネージャーを使用して、McAfee Endpoint Security for Linux をチェックインします。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 McAfee ePO サーバーに管理者としてログオンします。

2 [メニュー] 、 [ソフトウェア] 、 [ソフトウェア マネージャー] を選択します。

3 [ソフトウェア (ラベル別)] の [製品カテゴリ] リストから [McAfee Endpoint Security for Linux 脅威対策 <バージョン番号> <ビルド番号>] を選択してパッケージ ファイルを選択し、[すべてチェックイン] をクリックします。

4 サマリー ページで [McAfee 使用許諾条件] を承認し、[OK] をクリックします。

パッケージを手動でチェックインする

McAfee Endpoint Security for Linux 配備パッケージを McAfee ePO マスター リポジトリに手動でチェックインし、ソフトウェアを管理します。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 McAfee ダウンロード サイトから .zip ファイルをダウンロードし、McAfee ePO サーバー上の任意の場所に保存します。

2 McAfee ePO サーバーに管理者としてログオンします。

3 [メニュー] 、 [ソフトウェア] 、 [マスター リポジトリ] 、 [パッケージのチェックイン] を選択します。

   a [パッケージ タイプ] で [製品または更新 (.zip)] を選択します。

   b [ファイルの選択] をクリックして ISecTP-<バージョン>-<ビルド番号>-Release-ePO.zip を選択し、[選択] をクリックして [次へ] をクリックします。

   c [最新バージョン] ブランチを選択します。

4 [保存] をクリックします。

McAfee ePO サーバーに拡張ファイルをインストールする

McAfee ePO サーバーに拡張ファイルをインストールし、管理対象システムのポリシーを設定、配備します。

製品の機能を有効にするには、拡張ファイルを次の順番でインストールする必要があります。

- Endpoint Security for Linux ライセンス — Endpoint Security for Linux ライセンス拡張ファイル。オペレーティング システム固有のタグをポリシーとタスク オプションに表示します。
- Endpoint Security プラットフォーム — Endpoint Security 共通設定ポリシーの拡張ファイル。
- Endpoint Security 脅威対策 — Endpoint Security 脅威対策ポリシーの拡張ファイル。
- ecn_help — Endpoint Security 共通設定ポリシーのヘルプ拡張ファイル。
- etp_help — Endpoint Security 脅威対策ポリシーのヘルプ拡張ファイル。

拡張ファイルをインストールした後で、McAfee Endpoint Security 移行アシスタントの拡張ファイルをインストールして、McAfee VirusScan for Linux 1.9 and 2.x のポリシーとタスクを移行できます。 Endpoint Security 移行アシスタントのインストールと使用方法については、『McAfee Endpoint Security 10.2.0 移行ガイド』を参照してください。

タスク

- 45 ページの「*ソフトウェア マネージャーを使用して拡張ファイルをインストールする*」
  ソフトウェア マネージャーを使用して拡張ファイルをインストールします。
- 45 ページの「*拡張ファイルを手動でインストールする*」
  Endpoint Security 拡張ファイルを McAfee ePO サーバーに手動でインストールします。

ソフトウェア マネージャーを使用して拡張ファイルをインストールする

ソフトウェア マネージャーを使用して拡張ファイルをインストールします。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 McAfee ePO サーバーに管理者としてログオンします。

2 [メニュー]、[ソフトウェア] の順に選択して、[ソフトウェア マネージャー]を選択します。

3 [ソフトウェア マネージャー] 、 [製品カテゴリ] 、 [ソフトウェア (ラベル別)] の順に移動して、[Endpoint Security] 、[McAfee Endpoint Security for Linux 10.2] の順に選択します。右側のペインから [すべてチェックイン] をクリックします。

拡張ファイルを手動でインストールする

Endpoint Security 拡張ファイルを McAfee ePO サーバーに手動でインストールします。

拡張ファイルをインストールして、製品の機能を有効にする必要があります。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 McAfee ePO サーバーに管理者としてログオンします。

2 [メニュー]、[ソフトウェア]、[拡張ファイル] の順に選択し、[拡張ファイルをインストール] をクリックします。

3 [ファイルの選択] をクリックして拡張ファイルを選択し、[OK] をクリックします。

次の順番で拡張ファイルをインストールする必要があります。

- `ENDPL_LIC <バージョン> build_number.zip`
- `Common.<バージョン>.<ビルド番号>_(拡張ファイル).zip`
- `Threat_Prevention.<バージョン>.<ビルド番号>.(拡張ファイル).zip`
- `help_ecn_<バージョン>.zip`
- `help_etp_<バージョン>.zip`

インストール URL を使用して管理対象システムにクライアント ソフトウェアをインストールする

McAfee ePO の管理者は、管理対象システムに McAfee Endpoint Security for Linux クライアント ソフトウェアをインストールするための URL を作成できます。

これは、管理対象システムのユーザーが自身でソフトウェアをインストールするための方法です。

タスク

- *46 ページの「インストール URL を作成する」*
  管理対象システムに McAfee Agent をインストールできるように、インストール URL を作成して送信します。
- *46 ページの「インストール URL を使用してソフトウェアを管理対象システムにインストールする」*
  管理対象システムのユーザーは、URL にアクセスしてクライアント ソフトウェアをシステムにインストールできます。

インストール URL を作成する

管理対象システムに McAfee Agent をインストールできるように、インストール URL を作成して送信します。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 McAfee ePO サーバーに管理者としてログオンします。

2 [メニュー]、[ダッシュボード] の順に選択し、ドロップダウンリストから [ePolicy Orchestrator の開始] を選択します。

3 [製品の配備] ページで [配備の開始] をクリックし、次の設定を定義して [配備] をクリックします。
- [システム ツリー グループ]
- [McAfee Agent]
- [ソフトウェアとポリシー]
- [自動更新]

4 [製品の初期配備のサマリー] ページで [OK] をクリックします。

[ダッシュボード] ページの [製品の配備] セクションにインストール URL が表示されます。

5 URL とクライアント ソフトウェアのインストール手順をメールで送信します。

インストールが正常に終わると、McAfee Agent は McAfee ePO サーバーに戻ってそのシステム グループに割り当てられたタスクを確認し、適切なソフトウェアをインストールします。

インストール URL を使用してソフトウェアを管理対象システムにインストールする

管理対象システムのユーザーは、URL にアクセスしてクライアント ソフトウェアをシステムにインストールできます。

開始する前に

管理対象システムがハードウェア要件とソフトウェア要件を満たしていることを確認します。

自身で作成したインストール URL または管理者から受信したインストール URL が必要です。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 ブラウザー ウィンドウを開いてインストール URL をアドレス バーに貼り付け、**Enter** を押します。

2 画面上の指示に従います。

3 インストールが自動的に開始しない場合は、[インストール] をクリックします。

McAfee ePO からクライアント ソフトウェアを配備する

McAfee ePO を使用して、ネットワーク内の管理対象システムにクライアント ソフトウェアを配備します。

オンアクセス スキャン オプションを無効にして McAfee ePO からソフトウェアを配備するには、McAfee Agent コマンドライン オプションを使用して、配備タスクに [oasoff] パラメーターを指定します。 コマンドライン オプションは、[クライアント タスク カタログ] ページの [製品] と [コンポーネント] セクションで使用できます。 デフォルトでは、オンアクセス スキャン オプションを有効にしてソフトウェアがインストールされます。

オンアクセス スキャンを無効にするには、[オンアクセス スキャンを有効にする] オプションを選択せずに McAfee Endpoint Security 脅威対策のオンアクセス スキャン ポリシーを設定します。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 McAfee ePO サーバーに管理者としてログオンします。

2 [メニュー]、[システム]、[システム ツリー] の順に選択して、グループまたはシステムを選択します。

3 [割り当て済みのクライアント タスク] タブで [アクション] をクリックし、[新しいクライアント タスクの割り当て] をクリックします。

4 次のオプションを設定して、[タスクの新規作成] をクリックします。

   a 製品に [McAfee Agent] を選択します。

   b タスクの種類に [製品配備] を選択します。

5 [クライアント タスク カタログ] ページで次の操作を行います。

   a タスクの名前を入力します。

   b 対象プラットフォームに [Linux] を選択します。

   c In [製品とコンポーネント], select the product McAfee Endpoint Security for Linux 脅威対策 <ビルド番号>, select [インストール] as the action, then click[保存].

   
   を使用して製品を追加できます。

6 [クライアント タスク割り当てビルダー] ページで次の操作を行います。

   a タスクを設定して、[次へ] をクリックします。

   b タスクをすぐに実行するようにスケジュールを設定します。[次へ] をクリックしてタスクのサマリーを確認し、[保存] をクリックします。

7 [システム ツリー] で、タスクを割り当てるシステムまたはグループを選択し、[エージェント ウェークアップ] をクリックします。

8 [ポリシーとタスクの更新を強制的に完了] を選択して、[OK] をクリックします。

インストールをテストする

ソフトウェアの配備後、管理対象システムにクライアント ソフトウェアが正常にインストールおよび更新されていることを確認します。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 クライアントが McAfee ePO サーバーに情報を戻すまで待機します。通常は 1 時間ほど待ちます。

2 McAfee ePO コンソールで、[メニュー]、[ダッシュボード] の順に選択し、[Endpoint Security: インストール ステータス] を選択して、管理対象システムの一覧とインストール ステータスを表示します。

移行後のポリシーと同等の設定

After migrating policies and settings from McAfee VirusScan Enterprise for Linux to McAfee Endpoint Security for Linux, you can view the migrated settings in the respective options.

全般ポリシー – [トラブルシューティング] タブと [詳細設定] タブ

ここでは、[全般ポリシー] の [トラブルシューティング] タブと [詳細設定] タブで、McAfee VirusScan Enterprise for Linux から McAfee Endpoint Security for Linux 脅威対策に移行される値について説明します。

[トラブルシューティング] タブ

McAfee VirusScan Enterprise for Linux				McAfee Endpoint Security for Linux		
カテゴリ	**タブ**	**タイトル**	**オプション**	**ポリシー カテゴリ**	**タイトル**	**オプション**
[全般ポリシー]	[トラブルシューティング]	[ログの詳細レベル]	[低] [標準] [高]	[共通設定] の [オプション]	[クライアント ロギング] の [アクティビティ ロギング]	[アクティビティ ロギングを有効にする]
		[Syslog にも記録]	[Syslog の詳細レベル]	[共通設定] の [オプション]	[アクティビティ ロギング]	[イベントを Windows イベント ログまたは Syslog に記録する]
		[ログ項目の経過日数を制限する]				[各アクティビティ ログ ファイルのサイズ制限 (MB)]
		[ログ項目の最大経過日数]	–	–	–	なし

[詳細設定] タブ

McAfee VirusScan Enterprise for Linux				McAfee Endpoint Security for Linux			
カテゴリ	タブ	タイトル	オプション	ポリシー	カテゴリ	タイトル	オプション
[全般ポリシー]	[詳細設定]	[クライアント Web UI を無効にする]		なし	–	–	–
		[SMTP 通知を無効にする]	[Syslog の詳細レベル]	なし	–	–	–

オンアクセス スキャン ポリシー – [全般] タブ

ここでは、[オンアクセス スキャン ポリシー] の [全般] タブで、McAfee VirusScan Enterprise for Linux から McAfee Endpoint Security for Linux に移行されたポリシー設定について説明します。

McAfee VirusScan Enterprise for Linux				McAfee Endpoint Security for Linux		
カテゴリ	タブ	タイトル	オプション	カテゴリ	タイトル	オプション
[オンアクセス スキャン ポリシー]	[全般]	[オンアクセス スキャン]	[オンアクセス スキャンを有効にする]	[オンアクセス スキャン]	[オンアクセス スキャン]	[オンアクセス スキャンを有効にする]
			[隔離ディレクトリ]	[共通設定]	[オプション]	[隔離フォルダー]
[オンアクセス スキャン ポリシー]	[全般]	[スキャンの最大時間]	[すべてのファイルに最大スキャン時間を強制的に適用] [スキャンの最大時間 (秒)]	[オンアクセス スキャン]	[オンアクセス スキャン]	[各ファイル スキャンの最大秒数を指定]

オンアクセス スキャン ポリシー – [検出] タブ

ここでは、[オンアクセス スキャン ポリシー] の [検出] タブで、McAfee VirusScan Enterprise for Linux から McAfee Endpoint Security for Linux に移行された設定について説明します。

McAfee VirusScan Enterprise for Linux				McAfee Endpoint Security for Linux		
カテゴリ	タブ	タイトル	オプション	カテゴリ	タイトル	オプション
[オンアクセス スキャン ポリシー]	[検出]	[ファイルのスキャン]	[ディスクへの書き込み時]	[オンアクセス スキャン]	[プロセス設定] > [スキャン][スキャンのタイミング]	[ディスクへの書き込み時]
			[ディスクからの読み取り時]	[オンアクセス スキャン]	[プロセス設定] > [スキャン][スキャンのタイミング]	[ディスクからの読み取り時]
			[マウントされたネットワーク ボリューム]		[オンアクセス スキャン] > [スキャン]	[ネットワーク ドライブ上をスキャンする]
[オンアクセス スキャン ポリシー]	[検出]	[スキャン対象]	[すべてのファイル]	[オンアクセス スキャン]	[プロセス設定] > [スキャン][スキャン対象]	[すべてのファイル]
			[デフォルトと追加のファイルの種類]	[オンアクセス スキャン]	[プロセス設定] > [スキャン][スキャン対象]	[デフォルトと指定したファイルの種類]

McAfee VirusScan Enterprise for Linux				McAfee Endpoint Security for Linux		
			[指定した拡張子]	[オンアクセス スキャン]	[プロセス設定] > [スキャン][スキャン対象]	[指定したファイルの種類のみ]
[オンアクセス スキャン ポリシー]	[検出]	[スキャンの対象外]	[ウイルス スキャンから除外するファイルとディレクトリを選択する]	[オンアクセス スキャン]	[プロセス設定] > [除外対象]	

オンアクセス スキャン ポリシー — [詳細設定] タブ

ここでは、[オンアクセス スキャン ポリシー] の [詳細設定] タブで、McAfee VirusScan Enterprise for Linux から McAfee Endpoint Security for Linux に移行された設定について説明します。

McAfee VirusScan Enterprise for Linux				McAfee Endpoint Security for Linux		
カテゴリ	**タブ**	**タイトル**	**オプション**	**カテゴリ**	**タイトル**	**オプション**
[オンアクセス スキャン ポリシー]	[詳細設定]	[ヒューリスティック]	[未知のプログラム ウイルスを検索]	[オンアクセス スキャン]	[プロセス設定] > [追加のスキャン オプション]	[未知のプログラム脅威を検出する]
			[未知のマクロ脅威を検索する]	[オンアクセス スキャン]	[プロセス設定] > [追加のスキャン オプション]	[未知のマクロ脅威を検出する]
[オンアクセス スキャン ポリシー]	[詳細設定]	[ウイルス以外]	[不審なプログラムを検出する]	[オンアクセス スキャン]	[プロセス設定] > [追加のスキャン オプション]	[不審なプログラムを検出する]
			[ジョーク プログラムを検索する]	[オンアクセス スキャン]	[プロセス設定] > [追加のスキャン オプション]	[不審なプログラムを検出する]
[オンアクセス スキャン ポリシー]	[詳細設定]	[圧縮ファイル]	[アーカイブ ファイル (.zip など) の内部をスキャン]	[オンアクセス スキャン]	[プロセス設定] > [スキャン][スキャン対象]	[圧縮されたアーカイブ ファイル]
			[MIME 形式のファイルをデコード]	[オンアクセス スキャン]	[プロセス設定] > [スキャン][スキャン対象]	[圧縮された MIME 形式のファイル]

オンアクセス スキャン ポリシー — [アクション] タブ

ここでは、[オンアクセス スキャン ポリシー] の [アクション] タブで、McAfee VirusScan Enterprise for Linux から McAfee Endpoint Security for Linux に移行された設定について説明します。

McAfee VirusScan Enterprise for Linux				McAfee Endpoint Security for Linux		
カテゴリ	**タブ**	**タイトル**	**オプション**	**カテゴリ**	**タイトル**	**オプション**
[オンアクセス スキャン ポリシー]	[アクション]	[ウイルスとトロイの木馬の検出時]	[感染ファイルに対するアクセスを拒否して続行する]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [脅威を検出した場合の最初の対応]	[ファイル アクセスを拒否する]
			[感染ファイルを隔離ディレクトリに移動 ([全般] タブで設定)]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [脅威を検出した場合の最初の対応]	

McAfee VirusScan Enterprise for Linux				McAfee Endpoint Security for Linux		
			[感染ファイルを自動的に削除する]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [脅威を検出した場合の最初の対応]	[ファイルを削除する]
			[感染ファイルを自動的に削除する]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [脅威を検出した場合の最初の対応]	
			[感染ファイルを自動的に駆除する]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [脅威を検出した場合の最初の対応]	[ファイルを駆除する]
		[上記のアクションに失敗した場合]	[このアクションに 2 次オプションはありません]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [最初の対応が失敗した場合]	
			[感染ファイルに対するアクセスを拒否して続行する]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [最初の対応が失敗した場合]	[ファイル アクセスを拒否する]
			[感染ファイルを隔離ディレクトリに移動 ([全般] タブで設定)]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [最初の対応が失敗した場合]	
			[感染ファイルを自動的に削除する]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [最初の対応が失敗した場合]	[ファイルを削除する]
			[感染ファイルを自動的に削除する]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [最初の対応が失敗した場合]	
		[プログラムまたはジョーク プログラムの検出時]	[感染ファイルに対するアクセスを拒否して続行する]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [脅威を検出した場合の最初の対応]	[ファイル アクセスを拒否する]
			[感染ファイルを隔離ディレクトリに移動 ([全般] タブで設定)]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [脅威を検出した場合の最初の対応]	
			[感染ファイルを自動的に削除する]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [脅威を検出した場合の最初の対応]	
			[感染ファイルを自動的に削除する]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [脅威を検出した場合の最初の対応]	
			[感染ファイルを自動的に駆除する]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [脅威を検出した場合の最初の対応]	
		[上記のアクションに失敗した場合]	[このアクションに 2 次オプションはありません]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [最初の対応が失敗した場合]	

McAfee VirusScan Enterprise for Linux				McAfee Endpoint Security for Linux		
			[感染ファイルに対するアクセスを拒否して続行する]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [最初の対応が失敗した場合]	[ファイル アクセスを拒否する]
			[感染ファイルを隔離ディレクトリに移動 ([全般] タブで設定)]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [最初の対応が失敗した場合]	
			[感染ファイルを自動的に削除する]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [最初の対応が失敗した場合]	
			[感染ファイルを自動的に削除する]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [最初の対応が失敗した場合]	
		[スキャンに失敗した場合]	[ファイルに対するアクセスを許可する]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [最初の対応が失敗した場合]	[ファイル アクセスを許可する]
			[ファイルに対するアクセスを拒否する]	[オンアクセス スキャン]	[プロセス設定] > [アクション]> [最初の対応が失敗した場合]	[ファイル アクセスを拒否する]
		[スキャンがタイムアウトした場合]	[ファイルに対するアクセスを許可する]	[オンアクセス スキャン]	[プロセス設定] > [アクション]	[ファイル アクセスを許可する]
			[ファイルに対するアクセスを拒否する]	[オンアクセス スキャン]	[プロセス設定] > [アクション]	[ファイル アクセスを拒否する]

管理対象システムからソフトウェアを削除する

管理対象システムからクライアント ソフトウェアを削除し、McAfee ePO サーバーから拡張ファイルを削除します。

タスク

- 52 ページの「*ソフトウェアの拡張ファイルを削除する*」
  McAfee ePO サーバーから 拡張ファイルを削除します。
- 53 ページの「*クライアント システムからソフトウェアを削除する*」
  管理対象システムから McAfee Endpoint Security for Linux を削除するには、McAfee ePO サーバーでクライアント タスクを作成します。

ソフトウェアの拡張ファイルを削除する

McAfee ePO サーバーから 拡張ファイルを削除します。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 McAfee ePO サーバーに管理者としてログオンします。

2 [メニュー] [ソフトウェア] [拡張ファイル] の順に選択します。

3 左側のペインで拡張ファイルを選択し、[削除] をクリックします。

4 [チェックまたはエラーを回避して強制的に削除します。] を選択して、[OK] をクリックします。

クライアント システムからソフトウェアを削除する

管理対象システムから McAfee Endpoint Security for Linux を削除するには、McAfee ePO サーバーでクライアント タスクを作成します。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 McAfee ePO サーバーに管理者としてログオンします。

2 [メニュー]、[システム]、[システム ツリー] の順に選択して、グループまたはシステムを選択します。

3 [割り当て済みのクライアント タスク] タブをクリックして、[新しいクライアント タスクの割り当て] をクリックします。

4 次のオプションを設定して、[タスクの新規作成] をクリックします。

   a 製品に [McAfee Agent] を選択します。

   b タスクの種類に [製品配備] を選択します。

5 [クライアント タスク カタログ] ページで次の操作を行います。

   a タスクの名前を入力します。

   b 対象プラットフォームに [Linux] を選択します。

   c [製品とコンポーネント] で製品を選択し、アクションに [削除] を選択して [保存] をクリックします。

6 [クライアント タスク割り当てビルダー] ページで次の操作を行います。

   a タスクを設定して、[次へ] をクリックします。

   b タスクをすぐに実行するようにスケジュールを設定します。[次へ] をクリックしてタスクのサマリーを確認し、[保存] をクリックします。

7 [システム ツリー] で、タスクを割り当てるシステムまたはグループを選択し、[エージェント ウェークアップ] をクリックします。

8 [ポリシーとタスクの更新を強制的に完了] を選択して、[OK] をクリックします。

5 McAfee ePO Cloud で管理されているシステムへのソフトウェアのインストール

McAfee ePO Cloud で管理されているシステムにソフトウェアをインストールして管理します。

McAfee ePO Cloud は、セキュリティ製品とこれらの製品がインストールされたシステムのポリシーを一元的に管理し、施行できる拡張性に優れた管理プラットフォームです。

包括的なレポートの作成や製品の配備も一元的に管理できます。 McAfee ePO Cloud では、ネットワーク内の管理対象システムにセキュリティ製品、パッチ、サービス パックを配備できます。

目次

McAfee ePO Cloud コンポーネント

McAfee ePO Cloud ソフトウェアは次のコンポーネントから構成されます。

- **McAfee ePO Cloud** — 管理を行う中心となる場所。 McAfee ePO Cloud は、すべての管理対象システムに対して、セキュリティ ポリシーとタスクの配信、更新の管理、イベントの処理を行います。
- **McAfee Agent** — McAfee ePO Cloud と各システム間で情報を収集して施行します。 エージェントは、管理対象システムに対して、更新の取得、タスクの実装の確認、ポリシーの施行、イベントの転送を行います。
- **マスター リポジトリ** - McAfee にあり、McAfee 製品のすべての更新と署名が格納される場所。 マスター リポジトリは、McAfee からユーザー指定の更新と署名を取得します。

McAfee ePO Cloud アカウントへのアクセス

以下は McAfee ePO Cloud アカウントをセットアップする高度なアクションです。

1. エンタープライズ管理者が McAfee ePO Cloud に対するアクセスを要求します。
2. McAfee が McAfee ePO Cloud URL とログオン情報をエンタープライズ管理者に電子メールで送信します。
3. McAfee ePO Cloud サーバーにログオンします。

インストール URL を使用して管理対象システムにクライアント ソフトウェアをインストールする

インストール URL を作成し、クライアント ソフトウェアを管理対象システムにインストールするユーザーに送信します。

タスク

- 56 ページの「*インストール URL を作成する*」
  管理対象システムにソフトウェアをインストールするためのインストール URL を作成します。
- 56 ページの「*インストール URL を使用してソフトウェアをインストールする*」
  管理対システムのユーザーは、インストール URL を使用してソフトウェアをローカル システムにインストールできます。

インストール URL を作成する

管理対象システムにソフトウェアをインストールするためのインストール URL を作成します。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 McAfee ePO Cloud に管理者としてログオンします。

2 [メニュー] 、 [はじめに] 、 [カスタマイズ] の順にクリックします。

3 [ソフトウェアのインストールをカスタマイズする] ページで次の設定を行い、[完了] をクリックします。

- [グループ名] - グループ名を入力します。
- [オペレーティング システム] – [McAfee Agent for Linux] を選択します。
- [ソフトウェアとポリシー] - 必要に応じて[McAfee Endpoint Security] ソフトウェア モジュールを選択します。
- [自動更新] - ソフトウェアの更新をダウンロードする場合はこのオプションを選択します。

デフォルトでは、モジュールのデフォルトのポリシーとタスクが選択されます。

4 [完了] をクリックします。

5 [ダッシュボード] ドロップダウン リストで、[ePolicy Orchestrator の開始] を選択します。

[はじめに] の右側のペインに作成した URL が表示されます。

6 インストール手順を含む URL を管理システムのユーザーにメールで送信します。

インストールが正常に終わると、McAfee Agent は McAfee ePO サーバーに戻ってそのシステム グループに割り当てられたタスクを確認し、適切なソフトウェアをインストールします。

インストール URL を使用してソフトウェアをインストールする

管理対システムのユーザーは、インストール URL を使用してソフトウェアをローカル システムにインストールできます。

開始する前に

- システムがハードウェア要件とソフトウェア要件を満たしていることを確認します。
- 自身で作成したインストール URL または管理者から受信したインストール URL が必要です。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 ブラウザー ウィンドウを開いてインストール URL をアドレス バーに貼り付け、**Enter** を押します。

2 画面上の指示に従います。

McAfee ePO Cloud からクライアント ソフトウェアを配備する

ネットワーク内の管理対象システムにクライアント ソフトウェアを配備します。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 McAfee ePO サーバーに管理者としてログオンします。

2 [メニュー] 、 [ソフトウェア] 、 [製品の配備] を選択します。

3 [製品の配備] ページで次の設定を定義し、[保存] をクリックします。

- [名前]
- [説明]
- [種類]
- [自動更新]
- [パッケージ]
- [言語]
- [ブランチ]
- [コマンドライン]
- [システムを選択]
- [開始時間を選択]

6 McAfee ePO および McAfee ePO Cloud を使用したソフトウェア管理

McAfee ePO または McAfee ePO Cloud によって McAfee Endpoint Security for Linux を統合し、管理します。

この 2 つの環境でポリシーを管理する場合の基本的な相違点は次のとおりです。

- McAfee ePO — オンプレミスで McAfee ePO サーバーを保守します。 ソフトウェアのチェックインとサーバーへのインストール、ポリシーの設定、配備タスクによる管理対象システムへのポリシー施行は、管理者が行います。
- McAfee ePO Cloud — McAfee またはサービス プロバイダーが、ソフトウェアのチェックインとインストールを含め、McAfee ePO サーバーを保守します。 McAfee または他のサービス プロバイダーのクラウド アカウントをセットアップした後、ローカル管理者はポリシーを作成し、これらを配備タスクを使用して管理対象システムに施行します。

McAfee ePO と McAfee Agent のセットアップ手順と使用方法については、お使いのバージョンの製品ガイドを参照してください。

目次

共通の拡張ファイルとしての Endpoint Security 拡張ファイルの使用

最新の Endpoint Security の拡張ファイルを共通の拡張ファイルとして使用し、Microsoft Windows、Macintosh、Linux システムの 脅威対策ポリシーとタスクを管理します。

Endpoint Security 拡張ファイルを使用して、Windows、Macintosh、Linux のポリシーを設定し、配備できます。各ポリシー ページでは、特定のオペレーティング システムにのみ適用されるポリシーにタグが付いています。 例:

- [Windows のみ] — Windows システムにのみ適用されます。
- [Linux のみ] — Linux システムにのみ適用されます。
- [Windows と Mac のみ] — Windows システムと Macintosh システムにのみ適用されます。
- [Windows と Linux のみ] — Windows システムと Linux システムにのみ適用されます。

タグが付いていないポリシー オプションは、Windows、Mac、Linux のシステムに適用されます。

これらのタグをポリシーとタスクのオプションで表示するには、McAfee ePO サーバーにライセンス拡張ファイルをインストールしておく必要があります。

各オペレーティング システムでサポートされる機能の一覧については、McAfee KnowledgeBase の記事 KB84410 を参照してください。

ポリシーの管理

McAfee Endpoint Security for Linux ポリシーを使用すると、管理対象システムで機能の設定や管理を行ったり、詳細情報を記録できます。

[製品] の下の [ポリシー カタログ] ページでこれらのポリシーを参照できます。

- [Endpoint Security 脅威対策]
- [Endpoint Security 共通設定]

これらのポリシーを環境設定で設定し、管理対象システムのグループに割り当てます。 ポリシーの全般的な情報については、ご使用の McAfee ePO のバージョンに対応する製品ガイドを参照してください。

ポリシーを作成または変更する

[システム ツリー] の特定のグループにポリシーを作成したり、編集することができます。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 McAfee ePO サーバーに管理者としてログオンします。

2 [ポリシー カタログ] から [製品] と [カテゴリ] を選択します。

3 次の手順に従って、ポリシーを作成または変更します。

ポリシーを作成する	ポリシーを変更する
1 [新規ポリシー] をクリックします。 2 [ポリシー名] にポリシー名を入力します。 3 [OK] をクリックします。 4 設定を行います。	1 変更するポリシーをクリックします。 2 設定を変更します。

4 [保存] をクリックします。

ポリシーを割り当てる

作成または変更したポリシーは、McAfee ePO で管理されているシステムまたはグループに割り当てます。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 McAfee ePO サーバーに管理者としてログオンします。

2 [システム ツリー] に移動してグループまたはシステムを選択し、[割り当て済みのポリシー] タブをクリックします。

3 製品リストから製品を選択し、ポリシーを選択して [割り当てを編集] をクリックします。

4 割り当てるポリシーを選択し、必要な継承オプションを選択して [保存] をクリックします。

共通ポリシー

共通ポリシー オプションを使用して、管理対象システムの保護設定を行います。

[共通ポリシー] で、以下の設定を行います。

- デバッグ ロギングの環境設定を行う。
- イベント ロギングの環境設定を行う。
- ログ ファイルの場所を指定する。
- 製品のアクティビティ ロギングを設定する。
- アクティビティ ログ ファイルのサイズを設定する。

クライアント インターフェース アクセスの設定

ユーザー グループを分類し、必要なアクセス レベルを決定します。

[Endpoint Security 共通設定]のポリシーでは、次の操作を行うことができます。

- [フル アクセス] – 管理対象システムのユーザーがローカル システムのパスワード認証情報を使用してすべての機能設定を表示または変更できるよう許可します。 操作の制限を設けないユーザーには [フル アクセス] を付与できます。

管理対象システムのユーザーがローカルで保護に関する設定を変更すると、その後のポリシー施行では変更が上書きされます。

デバッグ ロギングの設定

管理者はインストールされたモジュールのデバッグ ロギングを有効または無効にできます。

モジュールのデバッグ ロギングを有効にすると、モジュールのすべてのコンポーネントのイベントが保存されます。

たとえば、Threat Prevention のデバッグ ロギングを有効にした場合、オンアクセス スキャンのイベント、およびユーザー レベルと**次の**レベルのオンデマンド スキャンのイベントが保存されます。

アクティビティとイベントのロギング

アクティビティ ログとイベント ログには、脅威対策のすべてのアクティビティの詳細が記録されます。

クライアントで記録されたすべてのイベントは McAfee ePO に送信されます。

アクティビティ ログ

アクティビティ ログには、McAfee Endpoint Security for Linux 脅威対策のすべてのアクティビティが記録されます。 1 MB ～ 999 MB の範囲でログ ファイルのサイズを定義できます。 デフォルトは 10 MB です。 ログ ファイルがこのサイズよりも大きくなると、現在のファイルがバックアップされ、新しいファイルが作成されます。 5 つ前までのログ ファイルが維持されます。

イベント ログ

有効にすると、McAfee Endpoint Security for Linux クライアントのイベント ログにすべてのイベントが記録されます。これらのイベントは McAfee ePO に送信されます。 イベント ログに記録されたイベントは、Linux クライアントの Syslog に送信することもできます。 Syslog の場所は Linux システムで設定可能です。

共通ポリシーの設定

共通ポリシーを使用して、ログの設定を定義します。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 McAfee ePO サーバーに管理者としてログオンします。

2 [ポリシー カタログ] で、製品に [Endpoint Security 共通設定] を選択し、カテゴリに [オプション] を選択します。

3 [新規ポリシー] をクリックし、ポリシー名を入力して [OK] をクリックします。

4 [ポリシー カタログ] ページで、[詳細を表示] をクリックし、次のオプションを定義します。

セクション	カテゴリ	設定内容
[クライアント インターフェース モード]		• [フル アクセス] — 管理対象システムのユーザーがローカル システムのパスワード認証情報を使用してすべての機能設定を表示または変更できるよう許可します。

[クライアント ロギング]	[アクティビティ ロギング]	[アクティビティ ロギング]
		• [アクティビティ ロギングを有効にする] — McAfee Endpoint Security for Linux のすべてのアクティビティをログに記録します。
		• [各アクティビティ ログ ファイルのサイズ制限 (MB)] — ログ ファイルのサイズを制限します (1 MB ～ 999 MB)。 デフォルトは 10 MB です。 ログ ファイルがこのサイズよりも大きくなると、現在のファイルがバックアップされ、新しいファイルが作成されます。 5 つ前までのログ ファイルが維持されます。
		[デバッグ ロギング]
		• [脅威対策で有効にする] — 脅威対策のデバッグ ロギングを有効にします。 ログの場所は次のとおりです。
		`/opt/isec/ens/threatprevention/var/`
		[イベント ロギング]
		• [脅威対策で有効にする] — 脅威対策のデバッグ ロギングを有効にします。 ログの場所は次のとおりです。
		`/opt/isec/ens/threatprevention/var/.`
		• [McAfee ePO へのイベントの送信] — クライアントのイベント ログに記録されたすべてのイベントを McAfee ePO に送信します。
		• [イベントを Windows イベント ログまたは Syslog に記録する] — すべてのイベントを McAfee Endpoint Security for Linux クライアントの Syslog に送信します。 Syslog の場所は Linux システムで設定可能です。

5 [保存] をクリックします。

6 [システム ツリー] で、システムまたはグループを選択します。

7 右ペインで [グループの詳細] タブをクリックし、[エージェントのウェークアップ] をクリックします。

8 [強制的に更新するポリシー] で、[ポリシーとタスクの更新を強制的に完了] を選択し、[OK] をクリックします。

脅威対策ポリシー

脅威対策は、管理対象システム上の項目をスキャンすることにより、マルウェアなどの脅威を検出します。
Endpoint Security 脅威対策ポリシーを使用して、管理対象システム用のスキャン設定を構成します。

製品	カテゴリ	使用可能なオプション	
[Endpoint Security 脅威対策]	[オンアクセス スキャン]	• 管理対象システムでオンアクセス スキャンの有効と無効を切り替える。 • 各ファイルをスキャンする制限時間を指定する。 • ファイルをスキャンするタイミングを指定する。	• 特定の種類のファイルをスキャンする。 • 検出された項目と不審なプログラムに対するアクションを定義する。 • ファイルとディレクトリを除外する。
	[オンデマンド スキャン]	• 管理対象システムでフル スキャンとクイック スキャンを実行する。 • 特定のディレクトリとそのサブディレクトリをスキャンする。 • 特定の種類のファイルをスキャンする。	• 検出された項目と不審なプログラムに対するアクションを定義する。 • スキャンからファイルとディレクトリを除外する。

オンアクセス スキャン ポリシーを設定する

オンアクセス ポリシーを作成し、オンアクセス スキャンの有効化または無効化、各ファイルのスキャン制限時間の定義、除外対象の定義を行います。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 McAfee ePO サーバーに管理者としてログオンします。

2 [ポリシー カタログ] で、製品に [Endpoint Security 脅威対策] を選択し、カテゴリに [オンアクセス スキャン] を選択します。

3 [新規ポリシー] をクリックし、ポリシー名を入力して [OK] をクリックします。

4 作成したポリシーをクリックし、[詳細を表示] をクリックします。

5 [オンアクセス スキャン] セクションで、これらの設定を定義します。

セクション	設定内容
[オンアクセス スキャン]	• [オンアクセス スキャンを有効にする] — 管理対象システムでオンアクセス スキャンを有効または無効にします。 • [各ファイル スキャンの最大秒数を指定] — 各項目をスキャンするためのスキャン タイムアウト値を指定します。 このオプションの選択を解除すると、値は 45 秒に設定されます。
[プロセスの設定]	ファイルにアクセスするプロセスまたはプログラムに従って、脅威対策がプロセスを危険度高または危険度低に分類します。 プロセスがこれらのカテゴリに分類されていない場合には、標準プロセスと見なされます。 [すべてのプロセスに標準設定を使用する] — オンアクセス スキャンを実行するときに標準設定を適用します。 [危険度高と危険度低のプロセスに別の設定を使用する] — 識別したプロセスのタイプごとに異なるスキャン設定を適用します。 必要に応じて、 プロセスとそのタイプを追加、編集、削除できます。

セクション	設定内容

	[標準]、[危険度高]、[危険度低] で、次の設定を行います。
	• [スキャンのタイミング]:
	  • [ディスクへの書き込み時] ー 書き込み時にファイルをスキャンします。
	  • [ディスクからの読み取り時] ー 読み取り時にすべてのファイルをスキャンします。
	  • [McAfee が選択する] ー 書き込み時または読み取り時にファイルをスキャンします。
	• [ディスクの読み取りまたは書き込み中にスキャンしない] ー 読み取り操作または書き込み操作中にファイルをスキャンしません。 この設定は、危険度低プロセスにのみ使用できます。
	• [スキャン対象]:
	  • [すべてのファイル] ー あらゆる拡張子のファイルをスキャンします。
	  • [デフォルトの種類と指定したファイルの種類] ー ソフトウェアで定義されている拡張子のファイルと指定した拡張子のファイルをスキャンします。
	  デフォルトのファイル リストを使用して [デフォルトの種類と指定したファイルの種類] オプションを有効にする場合には、McAfee KnowledgeBase の記事 KB79626 を参照してください。
	  • [マクロのスキャン] ー すべてのファイルに含まれるマクロのスキャンを有効にします。
	  • [指定したファイルの種類のみ] ー 指定した拡張子のファイルのみスキャンします。オプションで、拡張子のないファイルをスキャンできます。
	• [ネットワーク ドライブ上をスキャンする] ー マウントされたネットワーク ボリューム上のファイルをスキャンします。
	• [圧縮されたアーカイブ ファイル] ー 圧縮されたアーカイブ ファイルのコンテンツをスキャンします。
	  圧縮されたアーカイブ ファイルのスキャンには追加の時間がかかります。
	• [圧縮された MIME 形式のファイル] ー MIME 形式のメールをスキャンします。
	• [追加のスキャン オプション]:
	  • [不審なプログラムを検出] ー スキャナーで不審なプログラムを検出します。
	• [未知のプログラム脅威を検出する] ー スキャナーを有効にして、未知のプログラム脅威を検出します。
	• [未知のマクロ脅威を検出する] ー スキャナーを有効にして、未知のマクロ脅威を検出します。

	[アクション] 、 [脅威を検出した場合の最初の対応] で、次の操作を行います。 • [ファイル アクセスを拒否する] ー 感染の可能性があるファイルに対するアクセスを拒否します。 • [ファイルを削除] ー マルウェアを含むファイルを削除します。 • [ファイルを駆除する] ー 検出したファイルから脅威を駆除します。 また、最初の対応が失敗した場合、[最初の対応が失敗した場合] オプションを使用して 2 番目の対応を設定できます。 [不審なプログラムに対する最初の対応] で、次の操作を実行します。 • [ファイルを駆除する] ー 検出したファイルから脅威を駆除します。 • [ファイルを削除する] ー 脅威を含むファイルを削除します。 • [ファイル アクセスを許可する] ー 検出されたファイルへのアクセスを許可します。 • [スキャン タイムアウトの応答] ー ファイルのスキャンがタイムアウトしたときに実行されるアクション。

セクション	設定内容
	• [ファイル アクセスを拒否する] — 感染の可能性があるファイルに対するアクセスを拒否します。 • [スキャン エラーの応答] — スキャン エラーが発生した場合に実行されるアクション。 また、最初の対応が失敗した場合、[最初の対応が失敗した場合] オプションを使用して 2 番目の対応を設定できます。 [除外対象] セクションで、以下をクリックします。 • [追加] — ファイルを除外リストに追加します。 • [編集] — 除外設定を編集します。 • [削除] — 除外リストから選択した項目を削除します。 • [すべてクリア] — 除外リストからすべての項目を削除します。 [クライアントで設定した除外対象を無効にする] を有効にして、管理対象システムのユーザーによって作成された除外リストを無効にします。 除外対象の設定の詳細については、『スキャンからファイルまたはディレクトリを除外する』を参照してください。

6 [保存] をクリックします。

オンデマンド スキャン ポリシー (フル スキャン) を設定する

管理対象システムにオンデマンド フル スキャン ポリシーを設定します。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 McAfee ePO に管理者としてログオンします。

2 [ポリシー カタログ] で、製品に [Endpoint Security 脅威対策] を選択し、カテゴリに [オンデマンド スキャン] を選択します。

3 [新規ポリシー] をクリックし、ポリシー名を入力して [OK] をクリックします。

4 作成したポリシーをクリックし、[フル スキャン] タブをクリックしてこれらの設定を定義します。

セクション	設定内容
[スキャン対象]	• [圧縮された MIME 形式のファイル] — MIME 形式のファイルを検出し、デコードしてスキャンします。 • [圧縮されたアーカイブ ファイル] — 圧縮されたアーカイブ ファイルのコンテンツをスキャンします。 圧縮されたアーカイブ ファイルのスキャンには追加の時間がかかります。
[追加のスキャン オプション]	• [不審なプログラムを検出] — スキャナーで不審なプログラムを検出します。 • [未知のプログラム脅威を検出する] — マルウェアに類似しているコードを含むファイルを検出します。 • [未知のマクロ脅威を検出する] — 未知のマクロ脅威を検出します。

セクション	設定内容

[スキャンする場所]	• [サブフォルダーをスキャン] — 次のいずれかのオプションを選択したときに、指定したボリュームのサブフォルダーをすべてスキャンします。
	  • [Home フォルダー] — Home ディレクトリをスキャンします。
	  • [一時フォルダー] — /var/tmp と /tmp ディレクトリをスキャンします。
	  • [ユーザー プロファイル フォルダー] — ユーザー プロファイルのディレクトリをスキャンします。
	  • [ファイルまたはフォルダー] — Linux 固有のパスのみをスキャンします。
	  • [すべてのローカル ドライブ] — マウントされているすべてのファイル システム (特殊なファイル システム、ネットワーク ファイル システムを除く)。
	  • [すべての固定ドライブ] — すべての固定ドライブをスキャンします。
	  • [すべてのネットワーク ドライブ] — マウントされた NFS、CIFS または SMBFS タイプのファイル システムがネットワーク ドライブになります。 このオプションを選択すると、このようなファイル システムがすべてスキャンされます。
	+ をクリックすると場所を追加できます。 スキャンから場所を削除するには − をクリックします。

[スキャンするファイルの種類]	• [すべてのファイル] — 種類に関係なく、すべてのファイルをスキャンします。
	  McAfee では、[すべてのファイル] を有効にして、管理対象システムにマルウェアの脅威が存在しないようにすることを強くお勧めします。
	• [デフォルトの種類と指定したファイルの種類] — ソフトウェアで定義されている拡張子のファイルと指定した拡張子のファイルをスキャンします。
	  デフォルトのファイル リストを使用して [デフォルトの種類と指定したファイルの種類] オプションを有効にする場合には、McAfee KnowledgeBase の記事 KB79626 を参照してください。
	• [マクロのスキャン] — すべてのファイルに含まれるマクロのスキャンを有効にします。
	• [指定したファイルの種類のみ] — 指定した拡張子のファイルのみスキャンします。 [拡張子のないファイルを含む] を選択し、拡張子のないファイルをスキャンします。

[除外対象]	[除外対象] セクションで、以下をクリックします。 • [追加] — ファイルを除外リストに追加します。 • [編集] — 除外設定を編集します。 • [削除] — 除外リストから選択した項目を削除します。 • [すべてクリア] — 除外リストからすべての項目を削除します。 除外対象の設定の詳細については、『スキャンからファイルまたはディレクトリを除外する』を参照してください。

セクション	設定内容
[アクション]	[脅威を検出した場合の最初の対応] で、次の操作を実行します。 • [スキャンを続行する] ー 脅威が検出された場合、ファイルのスキャンを続行します。 隔離領域に項目は移動しません。 • [ファイルを駆除する] ー 検出したファイルから脅威を駆除します。 • [ファイルを削除する] ー マルウェアを含むファイルを削除します。 また、最初の対応が失敗した場合、[最初の対応が失敗した場合] オプションを使用して 2 番目の対応を設定できます。 Linux の場合、アクションを [拒否] に設定しても、検出時に実行中のファイル書き込み操作は停止しません。 ただし、以降のアクションは拒否されます。 [不審なプログラムに対する最初の対応] で、次の操作を実行します。 • [スキャンを続行する] ー 脅威が検出された場合、ファイルのスキャンを続行します。 隔離領域に項目は移動しません。 • [ファイルを駆除する] ー 検出したファイルから脅威を駆除します。 • [ファイルを削除する] ー マルウェアを含むファイルを削除します。 また、最初の対応が失敗した場合、[最初の対応が失敗した場合] オプションを使用して 2 番目の対応を設定できます。 すべてのアクションが失敗すると、フォールバック アクションはアクセス拒否になります。
[パフォーマンス]	• [スキャン キャッシュを使用] ー スキャナーで既存のスキャン結果を使用します。 • [各ファイル スキャンの最大秒数を指定] ー 1 つのファイルに対するスキャン時間 (秒数) を制限します。 デフォルトは 45 秒です。このオプションはデフォルトで有効になっています。 制限時間を超えると、スキャンを停止し、メッセージをログに記録します。 • [最大スレッド数を指定] ー 同時に実行可能なオンデマンド スキャンのスレッド数を制限します。

5 [保存] をクリックします。

タスクのスケジュールの詳細については、お使いの McAfee ePO のバージョンの製品ガイドを参照してください。

McAfee Endpoint Security for Linux では、[右クリック スキャン] オプションをサポートしていません。

オンデマンド スキャン ポリシー (クイック スキャン) を設定する

管理対象システムにオンデマンド クイック スキャン ポリシーを設定します。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 McAfee ePO サーバーに管理者としてログオンします。

2 [ポリシー カタログ] で、製品に [Endpoint Security 脅威対策] を選択し、カテゴリに [オンデマンド スキャン] を選択します。

3 [新規ポリシー] をクリックし、ポリシー名を入力して [OK] をクリックします。

4 作成したポリシーをクリックして [クイック スキャン] タブをクリックし、これらの設定を定義します。

セクション	設定内容
[スキャン対象]	• [圧縮された MIME 形式のファイル] ― MIME 形式のファイルを検出し、デコードしてスキャンします。 • [圧縮されたアーカイブ ファイル] ― 圧縮されたアーカイブ ファイルのコンテンツをスキャンします。 圧縮されたアーカイブ ファイルのスキャンには追加の時間がかかります。
[追加のスキャン場所]	• [不審なプログラムを検出する] ― 不審なプログラムを検出します。 • [未知のプログラム脅威を検出する] ― マルウェアに類似しているコードを含むファイルを検出します。 • [未知のマクロ脅威を検出する] ― 未知のマクロ脅威を検出します。

[スキャンする場所]	• [サブフォルダーをスキャン] ― 次のいずれかのオプションを選択したときに、指定したボリュームのサブフォルダーをすべてスキャンします。
	  • [ホーム フォルダー]
	  • [一時フォルダー]
	  • [ファイルまたはフォルダー]
	  • [すべてのネットワーク ドライブ]
	[場所を指定] ドロップダウン リストからディレクトリを選択します。 + をクリックするとディレクトリを追加できます。 スキャンからディレクトリを削除するには − をクリックします。

[スキャンするファイルの種類]	• [すべてのファイル] ― 種類に関係なく、すべてのファイルをスキャンします。 **ベストプラクティス**: 管理対象システムにマルウェアの脅威が存在しないように、[すべてのファイル] を有効にしてください。 • [デフォルトの種類と指定したファイルの種類] ― ソフトウェアで定義されている拡張子のファイルと指定した拡張子のファイルをスキャンします。 デフォルトのファイル リストを使用して [デフォルトの種類と指定したファイルの種類] オプションを有効にする場合には、McAfee KnowledgeBase の記事 KB79626 を参照してください。 • [マクロのスキャン] ― すべてのファイルに含まれるマクロのスキャンを有効にします。 • [指定したファイルの種類のみ] ― 指定した拡張子のファイルのみスキャンします。 [拡張子のないすべてのファイル] を選択し、拡張子のないファイルをスキャンします。
[除外対象]	[除外対象] セクションで、以下をクリックします。 • [追加] ― ファイルを除外リストに追加します。 • [編集] ― 除外設定を編集します。 • [削除] ― 除外リストから選択した項目を削除します。 • [すべてクリア] ― 除外リストからすべての項目を削除します。 除外対象の設定の詳細については、『スキャンからファイルまたはディレクトリを除外する』を参照してください。

セクション	設定内容
[アクション]	[脅威を検出した場合の最初の対応] で、次の操作を実行します。 • [スキャンを続行する] — 脅威が検出された場合、ファイルのスキャンを続行します。 隔離領域に項目は移動しません。 • [ファイルを駆除する] — 検出したファイルから脅威を駆除します。 • [ファイルを削除する] — マルウェアを含むファイルを削除します。 また、最初の対応が失敗した場合、[最初の対応が失敗した場合] オプションを使用して 2 番目の対応を設定できます。 [不審なプログラムに対する最初の対応] で、次の操作を実行します。 • [スキャンを続行する] — 脅威が検出された場合、ファイルのスキャンを続行します。 隔離領域に項目は移動しません。 • [ファイルを駆除する] — 検出したファイルから脅威を駆除します。 • [ファイルを削除する] — マルウェアを含むファイルを削除します。 また、最初の対応が失敗した場合、[最初の対応が失敗した場合] オプションを使用して 2 番目の対応を設定できます。
[パフォーマンス]	• [スキャン キャッシュを使用] — スキャナーで既存のスキャン結果を使用します。 • [各ファイル スキャンの最大秒数を指定] — 1 つのファイルに対するスキャン時間 (秒数) を制限します。 デフォルトは 45 秒です。このオプションはデフォルトで有効になっています。 制限時間を超えると、スキャンを停止し、メッセージをログに記録します。 • [最大スレッド数を指定] — 同時に実行可能なオンデマンド スキャンのスレッド数を制限します。

5 [保存] をクリックします。

タスクのスケジュールの詳細については、お使いの McAfee ePO のバージョンの製品ガイドを参照してください。

McAfee Endpoint Security for Linux では、[右クリック スキャン] オプションをサポートしていません。

スキャンからファイルまたはディレクトリを除外する

オンアクセス スキャンまたはオンデマンド スキャンからファイルやディレクトリを除外します。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 管理者として McAfee ePO サーバーにログオンします。

2 [ポリシー カタログ] で、製品に [Endpoint Security 脅威対策] を選択し、必要に応じて [オンアクセス スキャン] または [オンデマンド スキャン] を選択します。

3 ポリシーをクリックし、[詳細を表示] をクリックします。

ポリシーが作成されていない場合は、[新規ポリシー] をクリックし、ポリシー名を入力して [OK] をクリックします。

4 [プロセスの設定] の [除外] 領域で、[追加] をクリックして必要な設定を定義し、[保存] をクリックします。

セクション	設定内容
[除外対象]	• [パターン (ワイルドカードとして * または ? が使用可能)] — 除外するファイル パターンを指定します。 たとえば、デスクトップ上のすべてのファイルを除外する場合には、パスに `/Users/user/Desktop/*` を指定します。 • [サブフォルダーも除外] — 指定された場所からファイルとディレクトリを除外します。 • [ファイルの種類 (ワイルドカードとして ? を使用可能)] — 拡張ファイルが含まれているファイルを除外します。 クライアント除外リストを無効にするには、[クライアントで設定した除外対象を無効にする] (オンアクセス スキャンのみ) を選択します。
[除外のタイミング]	• [読み取り時] — (オンアクセス スキャンのみ) ファイルにアクセスしたときにスキャンから除外します。 • [書き込み時] — (オンアクセス スキャンのみ) ファイルが変更されたときにスキャンから除外します。

管理対象システムでフル スキャンまたはクイック スキャンのスケジュールを設定する

管理対象システムでマルウェアの脅威を検出するため、オンデマンド スキャンのスケジュールを設定します。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 McAfee ePO サーバーに管理者としてログオンします。

2 [メニュー]、[システム]、[システム ツリー] の順にクリックして、グループまたはシステムを選択します。

3 [割り当て済みのクライアント タスク] タブをクリックし、次に [アクション]、[新しいクライアント タスクの割り当て] をクリックします。

   a [製品] に [Endpoint Security 脅威対策] を選択します。

   b [タスクの種類] に [ポリシー別のオンデマンド スキャン] を選択し、[タスク名] リストでタスクを選択して、[次へ] をクリックします。

4 次のパラメーターを定義して [次へ] をクリックします。

   - [スケジュール ステータス]
   - [スケジュールの種類]
   - [有効期間]
   - [開始時間]
   - [タスクは次に基づいて実行されます]
   - [オプション]

   McAfee Endpoint Security for Linux 脅威対策で使用できるオプションは、[毎日]、[毎週]、[毎月]、[1 回だけ]、[今すぐ実行] だけです。

5 [サマリー] ページで [保存] をクリックします。

6 [システム ツリー] で、タスクを割り当てたシステムまたはグループを選択します。

7 右ペインで [グループの詳細] タブをクリックし、[エージェントのウェークアップ] をクリックします。

8 [強制的に更新するポリシー] で、[ポリシーとタスクの更新を強制的に完了] を選択し、[OK] をクリックします。

カスタム オンデマンド スキャンをスケジュール設定する

管理対象システムで、カスタム オンデマンド スキャンをスケジュール設定します。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 管理者として McAfee ePO サーバーにログオンします。

2 [メニュー]、[クライアント タスク カタログ] の順に選択します。

3 [クライアント タスク タイプ] で [Endpoint Security 脅威対策] を展開し、[カスタム オンデマンド スキャン] を選択して [新規タスク] をクリックします。

4 [タスクの種類] ドロップダウンリストで [カスタム オンデマンド スキャン] を選択します。

5 次の設定を定義して [保存] をクリックします。

- [名前]
- [説明]
- [スキャン オプション]
- [スキャンする場所]
- [スキャンするファイルの種類]
- [除外対象]
- [アクション]
- [スケジュール スキャン オプション]

6 作成したカスタム スキャンを [クライアント タスク カタログ] ページで選択し、[割り当て] をクリックしてタスクに割り当てるグループを選択し、[OK] をクリックします。

7 各ページで設定を行い、[次へ] をクリックします。

- [タスクの選択]
- [スケジュール]

8 [サマリー] ページで設定を行い、[保存] をクリックします。

隔離項目の場所を設定する

管理対象システムで隔離項目の保存場所を設定します。

タスク

1 管理者として McAfee ePO サーバーにログオンします。

2 [ポリシー カタログ] で、製品に [Endpoint Security 脅威対策] を選択し、カテゴリに [オプション] を選択します。

3 隔離マネージャーで、[隔離フォルダー] ドロップダウンからディレクトリを選択します。 デフォルトの場所は `quarantine` です。

4 [保存] をクリックします。

DAT 更新をスケジュール設定する

コンテンツ ファイルとエンジンを最新の状態に保つための更新をスケジュール設定します。

タスク

製品の機能、使用方法、ベストプラクティスについては、[?] または [ヘルプ] をクリックしてください。

1 McAfee ePO サーバーに管理者としてログオンします。

2 [メニュー]、[システム]、[システム ツリー] の順に選択して、グループまたはシステムを選択します。

3 [割り当て済みのクライアント タスク] タブで [アクション] をクリックして、[新しいクライアント タスクの割り当て] を選択します。

   a [製品] で [McAfee Agent] を選択します。

   b タスクの種類に [製品更新] を選択します。

   c [タスクの新規作成] をクリックして、[クライアント タスク カタログ] を開きます。

   d タスクの名前を入力して、 の [シグネチャとエンジン] で [Mac エンジン][Linux エンジン] と [DAT] を選択し、[保存] をクリックします。

   タスクが [タスク名] の下に表示されます。

   e タスクを選択して [次へ] をクリックします。

4 [スケジュール] ページで、タスクのスケジュールを定義します。

   a [システム ツリー] で、タスクを割り当てるシステムまたはグループを選択します。

   b 値を設定して、[次へ] をクリックします。

   - [スケジュールのステータス]
   - [スケジュールの種類]
   - [有効期間]
   - [開始時刻]
   - [タスクは次に基づいて実行されます]
   - [オプション]

   McAfee Endpoint Security for Linux 脅威対策で使用できるオプションは、[毎日]、[毎週]、[毎月]、[1 回だけ]、[今すぐ実行] だけです。

5 [サマリー] ページで [保存] をクリックします。

6 右側のペインで [グループの詳細] を選択し、[エージェント ウェークアップ] をクリックします。

7 [強制的に更新するポリシー] で [ポリシーとタスクの完全な更新を強制的に実行] を選択して、[OK] をクリックします。

クエリーとレポート

事前定義のクエリーを実行してレポートを生成するか、これらを修正してカスタム レポートを生成します。

脅威対策のクエリー

以下は、Threat Prevention で表示またはカスタマイズ可能なクエリーの一覧です。

クエリー	表示
[Endpoint Security Threat Prevention: インストールされた HotFix]	Threat Prevention 用にインストールされている HotFix が表示されます。
[Endpoint Security Threat Prevention: オンアクセス スキャンの対応状況]	オンアクセス スキャンの対応状況が表示されます。

クエリー	表示
[Endpoint Security 脅威対策: 過去 7 日間でフル スキャンが完了するまでの期間]	過去 7 日間でフル スキャンが完了するまでの時間が表示されます。
[Endpoint Security Threat Prevention: 過去 7 日間でフル スキャンが完了していないシステム]	フル スキャンが過去 1 か月以内に実行され、過去 7 日間に完了していないシステムの数が表示されます。
[Endpoint Security Threat Prevention: 1 か月以内にフル スキャンが完了していないシステム]	1 か月以内にフル スキャンが完了していないシステムの数が表示されます。
[Endpoint Security 脅威対策: 過去 7 日間でクイック スキャンが完了するまでの期間]	過去 7 日間でクイック スキャンが完了するまでの時間が表示されます。
[Endpoint Security 脅威対策: 検出対応のサマリー]	過去 3 か月間にアクション (駆除または削除) が実行された脅威の数とアクションが実行されなかった脅威の数が表示されます。
[Endpoint Security 脅威対策: 過去 2 四半期に検出された脅威]	過去 2 四半期に検出された脅威が表示されます。
[Endpoint Security 脅威対策: 重大度別の脅威数]	過去 3 か月間のイベント数 (スライス数) とイベントの重大度 (スライス) が表示されます。
[Endpoint Security 脅威対策: 検出された脅威のトップ 10]	過去 3 か月間に検出された脅威のトップ 10 が表示されます。
[Endpoint Security 脅威対策: 脅威源のトップ 10]	過去 3 か月間に脅威の発生元となった上位 10 台のコンピューターが表示されます。
[Endpoint Security 脅威対策: 検出数が最も多いコンピューターのトップ 10]	過去 3 か月間で最も検出数の多かったコンピューターのトップ 10 が表示されます。
[Endpoint Security 脅威対策: カテゴリ別の脅威トップ 10]	過去 3 か月間に検出された脅威のトップ 10 がカテゴリ別に表示されます。最初に脅威カテゴリで分類され、次に脅威名で分類されます。
[Endpoint Security 脅威対策: 検出数が最も多いユーザーのトップ 10]	過去 3 か月間で最も検出数の多かったユーザーのトップ 10 が表示されます。

その他のクエリー

これらのクエリーを実行してレポートを生成するか、これらを修正してカスタム レポートを生成します。

クエリー	表示
[Endpoint Security: 過去 7 日間で最も感染が多いユーザー]	このリストには、過去 7 日間に最も感染が多いユーザーが表示されます。
[Endpoint Security: 過去 7 日間に確認された主な攻撃ベクトル]	このリストには、過去 7 日間に確認された主な攻撃ベクトルが表示されます。
[Endpoint Security: 過去 48 時間に最も多く検出された脅威]	このリストには、過去 48 時間に最も多く検出された脅威が表示されます。
[Endpoint Security: 過去 24 時間に最も多く検出された脅威]	過去 24 時間に生成された脅威イベントの数が表示されます。
[Endpoint Security: 過去 7 日間に検出された脅威]	過去 7 日間に生成された脅威イベントの数が表示されます。
[Endpoint Security: 過去 24 時間に検出された脅威のサマリー]	過去 24 時間に検出された脅威のサマリーが表示されます。
[Endpoint Security: 過去 7 日間に検出された脅威のサマリー]	過去 7 日間に検出された脅威のサマリーが表示されます。
[Endpoint Security: 現在有効な技術]	このリストには、各管理対象システムで現在有効になっている機能が表示されます。

クエリー	表示
[Endpoint Security: ポリシーの対応状況 (コンピューター名別)]	最新のポリシーが適用されたコンピューターと適用されていないコンピューターが別々のリストに表示されます。
[Endpoint Security: ポリシーの対応状況 (ポリシー名別)]	クライアント システムでのポリシーの更新状況を表すブール円グラフが表示されます。
[Endpoint Security プラットフォーム: インストールされた HotFix]	インストールされているソフトウェアの HotFix が表示されます。
[Endpoint Security: インストール ステータス レポート]	複数のモジュールのインストール ステータスを表す積み上げ横棒グラフです。

索引