Symantec™ Endpoint Protection for Mac クライアント ヘルプ - Japanese - Japan

December 2020

Symantec Endpoint Protection が Mac を保護する方法

Symantec Endpoint Protection は複数の保護層を組み合わせ、ウイルスとスパイウェアの攻撃や、侵入の試みからコンピュータを守ります。

「保護の種類」で保護の各レイヤーについて説明します。

Table 1: 保護の種類

保護	説明
ウイルスとスパイウェアの対策	Symantec Endpoint Protection には、定時ウイルススキャン、オンデマンドスキャンに加え、バックグラウンドで実行してウイルスを監視する Auto-Protect が含まれています。Symantec Endpoint Protection は、ウイルスが見つかると除去します。 ウイルスとスパイウェアの対策が Mac を保護する方法
ネットワーク脅威防止	Symantec Endpoint Protection はネットワークレイヤーでデータを傍受します。侵入防止はシグネチャを使い、パケットまたはパケットのストリームをスキャンします。ネットワーク攻撃またはブラウザ攻撃に対応するパターンを検索することで、各パケットを個別にスキャンします。ネットワーク脅威防止には次の機能が含まれます。 • 侵入防止は、オペレーティングシステムコンポーネントとアプリケーション層に対する攻撃を検出します。Symantec Endpoint Protection はネットワーク脅威を検出すると、その脅威を遮断します。 • ファイアウォールは、ファイアウォールポリシーとルールに基づいてネットワークトラフィックを許可または遮断します。 (バージョン 14.2 以降) ネットワーク脅威防止で Mac を保護する方法
デバイス制御	Symantec Endpoint Protection Manager 管理者はデバイス制御ポリシーを設定します。このポリシーを使って、デバイス名、デバイス製造元、デバイスモデル、シリアル番号別にデバイスを遮断または遮断解除できます。 管理下クライアントの [拡張] ページにデバイス制御の設定が表示されます。デバイス制御は管理外のクライアントに対して利用できません。 Symantec Endpoint Protection for Mac クライアントでのデバイス制御
エンドポイントの検出と応答	Symantec Endpoint Protection Manager 管理者は、疑わしいネットワーク活動を検出して公開する手段を提供する活動レコーダーポリシーを設定します。

クライアントはウイルス定義、IPS 定義、製品の更新を、コンピュータに自動的にダウンロードします。

ウイルス定義、侵入防止定義およびクライアントソフトウェアの更新

ウイルスとスパイウェアの対策が Mac を保護する方法

Symantec Endpoint Protection はウイルス定義を使って定時スキャンと手動スキャン中に既知のウイルスを検出します。自動保護はウイルス定義を使ってコンピュータの活動を常にスキャンします。

Symantec Endpoint Protection はウイルスかその他のセキュリティリスクを検出すると通知します。次のいずれかが起きるときウイルスかその他のセキュリティリスクが検出されます:

- 自動保護がコンピュータの監視中にウイルスを見つける。
- 自動保護がスケジュール設定または手動で開始したウイルススキャンでウイルスを見つける。

デフォルト設定によって、Symantec Endpoint Protection は見つけたウイルスを自動的に修復するように試みます。ファイルを修復できない場合、クライアントはファイルを安全に検疫し、コンピュータに害を与えることができないようにし

ます。通常、クライアントはユーザーによる操作なしでこれらの修復を実行します。コンピュータがウイルスを見つけた場合は、シマンテック社にウイルスに関する情報を提出できます。

ある特定の状況では、クライアントは見つけた感染ファイルを修復するか、削除するか、復元するかを選択するためのメッセージを表示します。その応答によってクライアントが感染ファイルをどう処理するのかが決まります。

感染およびリスクの検出についてのメッセージへの対応

シマンテック社へのセキュリティ情報提出のオンとオフの切り替え

ネットワーク脅威防止で Mac を保護する方法

ネットワーク脅威防止には、次の保護技術が含まれています。

- 侵入防止
- ファイアウォール

侵入防止

侵入防止はネットワーク攻撃を自動的に検出して遮断します。侵入防止はクライアントコンピュータを保護する内部防御層です。侵入防止は侵入防止システム（IPS）と呼ばれる場合もあります。

侵入防止はネットワーク層でデータを傍受します。侵入防止はシグネチャを使い、パケットまたはパケットのストリームをスキャンします。ネットワーク攻撃またはブラウザ攻撃に対応するパターンを検索することで、各パケットを個別にスキャンします。侵入防止は、オペレーティングシステムコンポーネントとアプリケーション層に対する攻撃を検出します。

侵入防止は、シグネチャを使ってクライアントコンピュータに対する攻撃を識別します。既知の攻撃の場合、侵入防止はシグネチャと一致するパケットを自動的に破棄します。

ファイアウォール

ファイアウォールは、Mac を保護するために、ネットワークトラフィックを監視して潜在的に有害なトラフィックを遮断します。Symantec Endpoint Protection ファイアウォールは、管理外クライアントでは利用できません。

Symantec Endpoint Protection ファイアウォールは、転送とインターネットの層でトラフィックを監視します。組み込みの Mac ファイアウォールは、Symantec Endpoint Protection ファイアウォールが監視した後に、上位のアプリケーション層でトラフィックを監視します。したがって、並列で実行するために両方のファイアウォールを同時に有効にできます。

ファイアウォールは次の種類のルールを使用して、ネットワークトラフィックを許可または遮断します。

- デフォルトルール
- カスタムルール
- 組み込みルール
- 保護ルール

これらのルールには、ポートスキャン検出、サービス拒否検出、MAC 詐称対策、スマート DHCP、スマート DNS が含まれます。ファイアウォールの設定は、Symantec Endpoint Protection Manager 管理者によってすべて制御されます。ユーザーがファイアウォールを有効または無効にできるのは、Mac を介したユーザークライアント制御を管理者が許可する場合のみです。

ファイアウォール保護は、バージョン 14.2 で追加されました。

侵入防止の管理

Mac クライアントのファイアウォール保護の管理

Symantec Endpoint Protection for Mac とオペレーティングシステムの互換性

Symantec Endpoint Protection for Mac では、以下のオペレーティングシステムバージョンがサポートされています。

- macOS 12
- macOS 11 （ Intel プロセッサと M1 チップの両方 ）
- macOS 10.15 ~ 10.15.7

以前の Mac オペレーティングシステムのバージョンのサポートについて詳しくは、「Endpoint Protection クライアントと Mac の互換性」を参照してください。

Symantec Endpoint Protection for macOS 10.15 以降でのシステム拡張の認証について

Endpoint Protection のすべてのバージョンのリリースノート、修正項目、システム要件

Symantec Endpoint Protection for Mac クライアントのインストール

リモートプッシュを使えない場合や、使わない場合には、Symantec Endpoint Protection クライアントを Mac コンピュータに直接インストールできます。手順は、クライアントが対象外または対象下に関係なくほぼ同じです。

管理下クライアントをインストールする唯一の方法は、Symantec Endpoint Protection Manager で作成されるパッケージを使用することです。管理外クライアントは、クライアント/サーバーの通信設定を Mac クライアントにインポートすることでいつでも管理下クライアントに変換できます。

NOTE

サードパーティ製のリモート配備ソフトウェアで使用するために Mac 用の Symantec Endpoint Protection クライアントを準備するには、以下を参照してください。

Apple Remote Desktop または Casper を使用した Symantec Endpoint Protection クライアントのエクスポートと配備

Table 2: Mac クライアントをインストールする方法

インストールファイルをダウンロードした場合。	1. Mac コンピュータでその内容をフォルダに展開し、フォルダを開きます。 2. `SEP_MAC` を開きます。 3. `Symantec Endpoint Protection.dmg` を Mac コンピュータのデスクトップにコピーします。 4. `Symantec Endpoint Protection.dmg` をダブルクリックして、仮想ディスクとしてファイルをマウントします。Symantec Endpoint Protection for Mac クライアントをインストールします。
Broadcom サポートポータルからクライアントインストールパッケージの .zip をダウンロードした場合 詳細については、以下を参照してください。 Broadcom サポート ポータル	1. ファイルを Mac コンピュータのデスクトップにコピーします。ファイルには、`Symantec Endpoint Protection.zip` または `Symantec_Endpoint_Protection_version_Mac_Client.zip` という名前が付いています。ここで、 version は製品バージョンです。 2. [開く] > [アーカイブユーティリティ] の順に右クリックして、ファイルの内容を展開します。 3. 結果のフォルダを開きます。Symantec Endpoint Protection for Mac クライアントをインストールします。

展開した仮想ディスクイメージやフォルダは、アプリケーションインストーラと Additional Resources というフォルダを含んでいます。正常にインストールするには、これらの項目が両方とも同じ場所に存在する必要があります。別の場所にインストーラをコピーする場合は、Additional Resources もコピーする必要があります。

Mac 用 Symantec Endpoint Protection クライアントをインストールするには

1. `#Symantec Endpoint Protection #######`をダブルクリックします。
2. インストールを開始するには、[インストール] をクリックします。
3. Symantec Endpoint Protection クライアントをインストールするのに必要なヘルパーツールをインストールするには、Mac の管理者ユーザー名およびパスワードを入力し、[ヘルパーのインストール] をクリックします。
4. インストール後、[続行] をクリックして、Symantec Endpoint Protection クライアントの設定を終了します。
5. Symantec Endpoint Protection クライアントを設定するには、以下の手順に従います。

Symantec Endpoint Protection システム拡張を許可します。	[セキュリティとプライバシー] ダイアログボックスの [全般] タブの「アプリケーション **"Symantec Endpoint Protection"** からのシステムソフトウェアのロードがブロックされました」で、[許可] をクリックします。 必要に応じて、ロックアイコンをクリックして変更を行います。 Symantec Endpoint Protection が完全に機能するためには、システム拡張を認証する必要があります。次のサイトを参照してください。 Symantec Endpoint Protection for macOS 10.15 以降でのシステム拡張の認証について
ディスクへのフルアクセスを許可します。	[セキュリティとプライバシー] ダイアログボックスの [プライバシー] タブで、[Symantec **System Extension**（Symantec システム拡張）] が、Mac デバイスのすべてのユーザーのデータと管理設定にアクセスできることを確認します。 必要に応じて、ロックアイコンをクリックして変更を行います。
ネットワークプロファイルへの変更を許可します。	**Symantec Endpoint Protection** でネットワークコンテンツをフィルタするかどうかを確認するメッセージが表示されたら、[許可] をクリックします。

6. [完了] をクリックします。

Symantec Endpoint Protection for macOS 10.15 以降でのシステム拡張の認証について

macOS 10.15 以降のセキュリティ機能として、システム拡張の認証が必要になります。Symantec Endpoint Protection が完全に機能するためには、システム拡張を認証する必要があります。

Symantec Endpoint Protection のシステム拡張を認証するには、Symantec Endpoint Protection クライアントの設定中に、[セキュリティとプライバシー] ダイアログボックスの [全般] タブの「アプリケーション **"Symantec Endpoint Protection"** からのシステムソフトウェアのロードがブロックされました」で、[許可] をクリックします。

詳細については、次を参照してください。

Mac 用 Symantec Endpoint Protection クライアントのインストール

Symantec Endpoint Protection for Mac クライアントのアップグレード要求

Symantec Endpoint Protection Manager 管理者は、クライアントインストールパッケージを割り当てて、クライアントインストールの設定で管理下クライアントコンピュータを自動的にアップグレードできます。

Mac にログオンしている場合は、再起動してインストールを完了するように求められる場合があります。クライアントインストール設定に応じてこの再起動を延期できる場合があります。

Mac にログオンしていない場合は、インストールによって Mac が自動的に再起動します。

Symantec Endpoint Protection クライアントを始めましょう

Symantec Endpoint Protection クライアントを開くと、[You **are Protected**（保護されています）] というメッセージがページの最上部に表示されます。問題を解決するには [修復] をクリックします。

Symantec Endpoint Protection クライアントには、実行できる主なタスクが表示されます。

Table 3: Symantec Endpoint Protection クライアントページ

オプション	説明
セキュリティ	コンピュータの保護状態を表示します。
スキャン	コンピュータをスキャンできます。クイックスキャンの実行または完全スキャンの実行を選択できます。 また、スキャンするファイルまたはフォルダを削除することもできます。 手動のスキャンの実行
LiveUpdate	Symantec Endpoint Protection の定義ファイルと製品ファイルを更新するには、LiveUpdate を実行します。 Symantec Endpoint Protection の内容の即時更新
拡張	ウイルスとスパイウェアの対策、ネットワーク脅威防止、LiveUpdate の詳細オプションを指定します。

Symantec Endpoint Protection での Mac の保護管理

Symantec Endpoint Protection のデフォルト設定で、多くの種類のマルウェアから Mac を保護します。クライアントが自動的にマルウェアを処理するか、またはユーザーがマルウェアの処理方法を選択できます。

管理者が設定したオプションに応じて、次のタスクを実行して保護を保守してください。

NOTE
管理者がこれらのタスクをユーザーが制御できないようにしている場合もあります。

Table 4: コンピュータの保護

手順	説明
ステップ 1: ウイルスとスパイウェアの対策、ネットワーク脅威防止の両方が有効であることを確認する	[セキュリティ] ページを表示します。保護がオンの場合は緑色のチェックマークと [You **are Protected**（保護されています）] というメッセージが表示されます。 ウイルスとスパイウェアの対策をオンまたはオフにする ネットワーク脅威防止のオンとオフの切り替え
ステップ 2: ソフトウェアと定義が最新であることを確認する	[セキュリティ] ページに、ウイルスとスパイウェアの対策とネットワーク脅威防止の定義を更新した最終時刻が表示されます。**LiveUpdate** に、前回の製品更新時間が表示されます。 ソフトウェアのバージョン番号を確認するには、[ヘルプ] > [バージョン情報] の順に選択します。
ステップ 3: 必要に応じてソフトウェアまたは定義を更新する	ソフトウェアと定義をすぐに更新するには、Symantec Endpoint Protection クライアントで [LiveUpdate] をクリックします。 ウイルス定義、侵入防止定義およびクライアントソフトウェアの更新
ステップ 4: スキャンを実行します。	スキャンを定期的に実行するように設定することも、スキャンをすぐに実行することもできます。 定時スキャンの設定 手動のスキャンの実行

ウイルスとスパイウェアの対策設定の管理

製品ライセンスの延長

メニューバーの Symantec Endpoint Protection クライアントアイコンの下に、Symantec Endpoint Protection のライセンスが期限切れであるというメッセージが表示されることがあります。Symantec Endpoint Protection クライアントは、ライセンスを使用して次の更新を行います。

- クライアントソフトウェア
- ウイルスとスパイウェアのスキャン、侵入防止用の保護定義ファイル

クライアントは、試用ライセンスまたは有償ライセンスを使うことがあります。どちらかのライセンスが期限切れになった場合には、クライアントは定義やクライアントソフトウェアを更新しません。

どちらの種類のライセンスの場合も、管理者に連絡してライセンスを更新するか、または再契約する必要があります。

感染およびリスクの検出についてのメッセージへの対応

Symantec Endpoint Protection for Mac クライアントでのデバイス制御の有効化または無効化

Symantec Endpoint Protection Manager 管理者は、デバイス制御ポリシーを使って管理下クライアントを設定できます。このポリシーを使って、デバイス名、デバイス製造元、デバイスモデル、シリアル番号別にデバイスを遮断または遮断解除できます。

[活動] > [Security **History** （ セキュリティ履歴 ）] をクリックすることで、 [拡張] ページにデバイス制御の活動を表示できます。

[デバイス制御] での Symantec Endpoint Protection クライアントの設定では、デバイス制御を有効または無効にできます。デバイス制御が有効な場合、デバイスが遮断または遮断解除されたときの通知を有効または無効にできます (省略可能) 。

設定を変更するには、Mac の管理者資格情報を使って認証を行う必要があります。これらの設定がグレーアウト表示の場合は、この機能を有効化または無効化できないように管理者がロックしていることを意味します。

Symantec Endpoint Protection クライアントインターフェースを使って、遮断または遮断解除するデバイスを追加または編集できません。

> **NOTE**
> Symantec Endpoint Protection Manager のデバイス制御ポリシーはデバイス制御設定を制御します。これらの設定に行った変更は、次回のハートビートで、ポリシーが指定する内容に戻されます。

デバイス制御は管理外のクライアントに対して利用できません。

Web とクラウドのアクセス保護 for the Mac クライアントについて

Web とクラウドのアクセス保護 は Symantec Web Security Service への Web トラフィックリダイレクトを自動化し、Symantec Endpoint Protection を使用する各コンピュータ上で Web トラフィックを保護します。

管理者は Web とクラウドのアクセス保護 が使用する設定を制御します。これにはプロキシの設定 URL と、オプションで Symantec Web Security Service ルート証明書が含まれます。Symantec Endpoint Protection Manager 管理者のみがこれらの設定を構成できます。これらの設定は Symantec Endpoint Protection クライアント UI には表示されません。Mac のプロキシ構成ファイルの URL は、 [プロキシ] の下の [システム環境設定] > [ネットワーク] で表示できます。クラウドサービス証明書は、 [キーチェーン] に表示されます。

Web とクラウドのアクセス保護 をサポートする Web ブラウザは、Safari、Chrome、Firefox バージョン 65 以降です。14.2 RU1 以前の Symantec Endpoint Protection バージョンでは、Safari と Chrome のみがサポートされます。

> **NOTE**
> トンネル方式は、Mac クライアント上では実行されません。

Mac 用の Symantec Endpoint Protection クライアントのアンインストール

メニューバーのクライアントアイコンを使って、Symantec Endpoint Protection for Mac クライアントをアンインストールします。Symantec Endpoint Protection for Mac クライアントのアンインストールでは管理者ユーザーの資格情報が必要です。

> **NOTE**
> Symantec Endpoint Protection クライアントをアンインストールした後、アンインストールを完了するためにクライアントコンピュータを再起動するように求めるメッセージが表示されます。開始する前に、必ず未完了のすべての作業を保存して、すべての開いているアプリケーションを閉じます。

Mac 用の Symantec Endpoint Protection クライアントをアンインストールする方法

1. Mac クライアントコンピュータで、Symantec Endpoint Protection クライアントを開き、[**Symantec Endpoint Protection**] > [**Symantec Endpoint Protection** のアンインストール] をクリックします。
2. [アンインストール] を再びクリックして、アンインストールを開始します。
3. Symantec Endpoint Protection クライアントをアンインストールするのに必要なヘルパーツールをインストールするには、Mac の管理者ユーザー名およびパスワードを入力し、[ヘルパーのインストール] をクリックします。
4. [Symantec **Endpoint Protection is trying to modify a System Extension**（Symantec **Endpoint Protection** はシステム拡張を変更しようとしています ）] ダイアログボックスで、Mac の管理者ユーザー名とパスワードを入力し、[OK] をクリックします。

   クライアントをアンインストールするためにパスワードの入力を求められる可能性もあります。このパスワードは、Mac の管理パスワードと別のパスワードである可能性があります。
5. アンインストールが完了したら、[今すぐに再起動] をクリックします。

アンインストールが失敗した場合は、別の方法を使用したアンインストールが必要になる場合があります。次のサイトを参照してください。

Symantec Endpoint Protection のアンインストール

ウイルス定義、侵入防止定義およびクライアントソフトウェアの更新

シマンテック製品は最新情報に基づいて、新しく発見された脅威からコンピュータを保護します。シマンテックでは、LiveUpdate を使ってこの情報を Symantec Endpoint Protection に提供します。LiveUpdate は、インターネット接続を使って、コンピュータの製品更新と定義の更新を入手します。

定義の更新とは、最新の脅威防止技術を使ってシマンテック製品を最新の状態に保つファイルです。LiveUpdate はシマンテック社のインターネットサイトから新しい侵入防止シグネチャまたはウイルス定義ファイルを取り込んで、古いファイルを置換します。

製品の更新とは、インストール済みクライアントの改良を意味します。一般的に、製品の更新は、オペレーティングシステムまたはハードウェアとの互換性の向上、性能問題の調整、製品エラーの修正を目的として作成されます。製品の更新は必要に応じてリリースされます。クライアントは LiveUpdate サーバーから製品の更新を直接受信します。製品の更新と定義の更新はともにコンテンツ更新と呼ばれます。

Table 5: コンピュータの内容を更新する方法

タスク	説明
内容をすぐに更新	LiveUpdate をすぐに実行できます。 Symantec Endpoint Protection の内容の即時更新
スケジュールに従って内容を更新	デフォルトでは、LiveUpdate は自動で定期的に実行されます。 スケジュールに従って Symantec Endpoint Protection の内容を更新

Symantec Endpoint Protection での Mac の保護管理

Symantec Endpoint Protection の内容の即時更新

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

- クライアントソフトウェアが最近インストールされた
- 前回のスキャンから長い時間が経過している
- ウイルスやその他のマルウェア問題の疑いがある

Symantec Endpoint Protection の内容を即時更新するには

次のいずれかの方法で LiveUpdate を起動します。

- メニューバーの Symantec Endpoint Protection アイコンを右クリックして、 [LiveUpdate] クリックします。
- Symantec Endpoint Protection クライアントを開き、 [LiveUpdate] をクリックします。

LiveUpdate は設定された LiveUpdate サーバーに接続して利用可能な更新がないか確認し、更新がある場合には、自動的に更新をダウンロードしてインストールします。ステータスバーには、ダウンロードの進行状況が示されます。

スケジュールに従って Symantec Endpoint Protection の内容を更新

ウイルス定義、侵入防止定義およびクライアントソフトウェアの更新

スケジュールに従って Symantec Endpoint Protection の内容を更新

管理下の **Mac** クライアントのスケジュール

デフォルトで、管理下の Mac クライアントは、4 時間ごとに LiveUpdate を実行する Symantec Endpoint Protection Manager からスケジュールを受信します。Symantec Endpoint Protection Manager 管理者はスケジュールを制御します。管理下クライアントは、管理者が作成したスケジュールを削除、修正、表示したり、新しいスケジュールを作成したりすることができません。

管理外の **Mac** クライアントのスケジュール

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

Symantec Endpoint Protection のコンテンツをスケジュールに従って更新するには

1. Symantec Endpoint Protection クライアントの [拡張] ページで、 [製品の設定] をクリックし、 [定時 LiveUpdate] の設定アイコンをクリックします。

   現在のスケジュールが表示されます。

2. LiveUpdate のスケジュールのドロップダウンメニューから間隔を選択してください。

   初期設定は **4** 時間ごとの実行です。時間または日時をそれぞれ選択して [日単位] または [週単位] で実行することもできます。

3. [変更の適用] をクリックします。

Symantec Endpoint Protection の内容の即時更新

ウイルス定義、侵入防止定義およびクライアントソフトウェアの更新

プロキシサーバーを経由した管理サーバーへの接続について

Symantec Endpoint Protection がユーザーのクレデンシャルを使ってプロキシ経由で管理サーバーに接続することを許可するように求められる場合があります。`smcdaemon` プロセスの資格情報へのアクセスを許可するかどうかを尋ねるメッセージを受け取ります。

メッセージをクリックして常に許可する必要があります。この設定を行わないと、クライアントが LiveUpdate サーバーと通信するたびに同じメッセージを表示し続けます。 [拒否] をクリックすると、クライアントはソフトウェアや定義の更新を受信できません。

ウイルス定義、侵入防止定義およびクライアントソフトウェアの更新

ウイルスとスパイウェア対策設定の管理

デフォルトでは、Symantec Endpoint Protection はコンピュータが起動するとすぐにネットワーク脅威などのウイルスとセキュリティのリスクを防ぎます。ウイルスとスパイウェアの対策には、プログラムの実行時にウイルスを調べる Auto-Protect が含まれます。コンピュータを監視して、ウイルスまたはセキュリティリスクの存在を示す可能性のある活動がないかも調べます。Auto-Protect の遮断はウイルスがコンピュータに感染することを防ぐので、Auto-Protect をオンにしておく必要があります。

管理下クライアントでは、これらの設定の制御権は、管理者がクライアントをどのように設定したかによって異なります。さらに、これらの設定に行った変更は、次回のハートビートで、ポリシーが指定する内容に戻される可能性があります。

「ウイルス対策とスパイウェア対策の管理」では Mac でウイルスとスパイウェアの対策を管理するためにユーザーが実行できるタスクについて説明します。

Table 6: ウイルス対策とスパイウェア対策の管理

手順	説明
ステップ 1: ウイルスとスパイウェアの対策のオンとオフの切り替え	ウイルスとスパイウェアの対策の有効と無効を簡単に切り替えることができます。シマンテック社はオンのままにすることを推奨します。 ウイルスとスパイウェアの対策をオンまたはオフにする
ステップ 2: 自動保護設定のカスタマイズ	自動保護はウイルスとスパイウェアの対策の重要な機能です。 これらのオプションは [拡張] ページで設定できます。 Auto-Protect オプションとスキャンゾーンオプションの設定
ステップ 3: コンピュータのウイルススキャン	ウイルススキャンを定期的に実行する、またはすぐに実行するように設定できます。 定時スキャンの設定 スキャンの一時停止、休止、停止 手動のスキャンの実行
ステップ 4: Symantec Endpoint Protection がウイルスを検出した場合の応答	Symantec Endpoint Protection がコンピュータをスキャンするときは、次のことを実行できます。 • 実行可能な処理について通知する • 実行された保護処理について通知する 感染およびリスクの検出についてのメッセージへの対応

ウイルスとスパイウェアの対策をオンまたはオフにする

デフォルトでは、ウイルスとスパイウェアの対策は Auto-Protect とともにオンになります。

特定のオプションの設定により、Auto-Protect をより精密に制御できます。

ウイルスとスパイウェアの対策をオフにした場合、[状態] ページに「ウイルスとスパイウェアの対策は無効です」というメッセージとともに赤い「x」が表示されます。保護を無効にした場合、できるだけ早く有効にする必要があります。

NOTE
定時スキャンは、ウイルスとスパイウェアの対策が有効か無効かに関係なく続行されます。一部の Symantec Endpoint Protection の設定へのアクセスは、システム管理者によって制限されていることがあります。これらの設定の無効化、スキャンのスケジュール、保護オプションのカスタマイズが許可されていないことがあります。これらの設定を変更するには、Mac 管理者パスワードを提供する必要がある場合があります。

ウイルスとスパイウェアの対策をオンまたはオフにするには

1. [ウイルスとスパイウェアの対策ポリシー] をオンにするには、Symantec Endpoint Protection クライアントの [拡張] ページで、 [Protect **My Mac** （ Mac を保護する ）] をクリックし、 [自動スキャン] を有効にします。
2. [ウイルスとスパイウェアの対策ポリシー] をオフにするには、Symantec Endpoint Protection クライアントの [拡張] ページで、 [Protect **My Mac** （ Mac を保護する ）] をクリックし、 [自動スキャン] を無効にします。

Auto-Protect オプションとスキャンゾーンオプションの設定

ウイルスとスパイウェアの対策設定の管理

感染およびリスクの検出についてのメッセージへの対応

Auto-Protect オプションとスキャンゾーンオプションの設定

管理下クライアントでは、管理者の許可があれば Auto-Protect がウイルスを監視し、感染ファイルを修復する方法をカスタマイズできます。

Auto-Protect 設定は、 [Protect **My Mac** （ Mac を保護する ）] にオプションとして表示されます。Auto-Protect を有効にするには、 [自動スキャン] を有効にする必要があります。

[スキャンゾーン] 設定では、スキャンに含めるファイルまたはスキャンから除外するファイルを指定できます。

Auto-Protect オプションを設定するには

1. Symantec Endpoint Protection クライアントの [拡張] ページで、 [Protect **My Mac** （ Mac を保護する ）] をクリックし、 [自動スキャン] の設定アイコンをクリックします。
2. 次のオプションのいずれかを変更します。

自動検疫	修復できないすべてのファイルを検疫に送信するかどうかを選択できます。
自動修復	Auto-Protect が検出したすべての感染ファイルを自動的に修復するように設定できます。
スキャン	[データディスク] や [他のすべてのディスク] を選択できます。
圧縮ファイルをスキャン	Auto-Protect スキャンに圧縮ファイルを含めるかどうかを選択できます。スキャンには圧縮ファイルと圧縮ファイル内のファイルが含まれます。

WARNING
[自動修復] を選択しなければ、 [自動検疫] を選択しても感染ファイルは検疫に移されません。感染ファイルを修復するかどうかを確認するメッセージが表示されます。ファイルを修復しなければ、そのファイルはコンピュータに残ります。 [自動修復] を選択し、 [自動検疫] を選択しないと感染ファイルは削除されます。

3. [完了] をクリックします。

スキャンゾーンオプションを設定するには

1. Symantec Endpoint Protection クライアントの [拡張] ページで、 [Protect **My Mac** （ Mac を保護する ）] をクリックし、 [Scan **Zone Settings** （ スキャンゾーン設定 ）] の設定アイコンをクリックします。
2. 次のオプションのいずれかを変更します。

すべての場所をスキャン	コンピュータ上のすべてのファイルとプロセスがアクセスしたときにスキャンされます。
一部の場所のみをスキャン	指定したファイルやフォルダのみがスキャンに含まれます。
スキャンしない	スキャンから除外することを指定したファイルやフォルダを除き、すべてのファイルがスキャンされます。
デフォルトを使う	このオプションを選択するとすべての場所をスキャンします。

3. [OK] をクリックします。

ウイルスとスパイウェアの対策が Mac を保護する方法

ウイルスとスパイウェアの対策をオンまたはオフにする

検疫ファイルの管理

定時スキャンの設定

Symantec Endpoint Protection は管理下クライアントがあれば自動的にデフォルトのスキャンを実行します。管理者の許可があれば、ユーザーは他の定時スキャンを設定できます。

管理外クライアントでは、独自のスキャンを実行する必要があります。できるだけ早く完全な手動スキャンを実行し、通常の定時スキャンを設定することを推奨します。定時スキャンと手動スキャンの両方を含め、すべてのスキャンは一時停止または見送ることができます。

管理下クライアントでは、自動修復が有効な状態でデフォルトのスキャンを毎日午後 8 時に実行します。

NOTE
定時スキャンを 1 日に 2 回以上実行することは推奨されません。スキャンの頻度を増やしたり、複数の定時スキャンを設定したりすると、パフォーマンスの問題が発生する可能性があります。

手動のスキャンの実行

定時スキャンを設定するには

1. Symantec Endpoint Protection クライアントの [拡張] ページで、 [Protect **My Mac** （ Mac を保護する ）] をクリックし、 [定時スキャン] の設定アイコンをクリックします。
2. ダイアログボックスで、 [定時スキャンの追加] をクリックするか、または現在の定時スキャンをクリックし、 [編集] をクリックして、その設定を調整します。
3. [スキャン項目] ページで、次のオプションを設定できます。

ドライブ	ハードディスクドライブとリムーバブルドライブをスキャンするかどうかを選択できます。
フォルダ	[ホームフォルダ (アクティブユーザー)] 、 [アプリケーション] 、 [ライブラリ] のファイルのスキャンを選択できます。 ホームフォルダの定時スキャンのときにログオンしているユーザーがいない場合、スキャンは実行しません。
スキャンオプション	選択できるオプションは次のとおりです。 • 圧縮のスキャン • 自動修復 • 自動検疫 • アイドルタイムスキャン有効化

4. [スキャンスケジュール] ページで、次のオプションを設定できます。

スキャンスケジュール	時間、日、週、月のいずれか特定の間隔で実行するようにスキャンを設定できます。新しいスキャンをスケジュール設定する場合は、デフォルトで [特定の間隔で実行] が選択されます。
実行間隔	[スキャンスケジュール] で [特定の間隔で実行] を選択した場合に設定できます。
開始日時	スキャンスケジュールで [日単位] 、 [週単位] 、 [月単位] を選択した場合に設定できます。スキャンを実行する時刻を選択できます。スキャンを実行するとコンピュータのパフォーマンスが低下する可能性があるため、通常は就業時間外の時刻を選択してください。
オン	スキャンスケジュールで [週単位] または [月単位] を選択した場合に設定できます。スキャンを実行する曜日または日にちを選択できます。スキャンを実行するとコンピュータのパフォーマンスが低下する可能性があるため、通常は就業時間外の時刻を選択することを推奨します。

5. [調整] タブでは、スキャンのパフォーマンスを最適化する方法を調整できます。
6. [OK] をクリックします。
7. [完了] をクリックします。

スキャンの一時停止、休止、停止

Symantec Endpoint Protection での Mac の保護管理

感染およびリスクの検出についてのメッセージへの対応

シマンテック社へのセキュリティ情報提出のオンとオフの切り替え

手動のスキャンの実行

一部のファイルは手動でスキャンする必要があることがあります。たとえば、Symantec Endpoint Protection がインストールされる前にコンピュータに保存されたファイルをスキャンする必要があることがあります。または、定時スキャンから除外されている一部のファイルをスキャンする必要があると判断する場合があります。

NOTE
定時スキャンと手動スキャンの両方を含め、すべてのスキャンは一時停止または見送ることができます。

手動スキャンを実行するには

Symantec Endpoint Protection クライアントの [スキャン] ページで、以下のいずれかのタスクを実行します。

- クイックスキャンを開始するには、[Quick **Scan**（クイックスキャン）] をクリックし、[Start **a Quick Scan**（クイックスキャンの開始）] をクリックします。
- 完全スキャンを開始するには、[完全スキャン] をクリックし、[Start **a Full Scan**（完全スキャンの開始）] をクリックします。
- ファイルまたはフォルダをスキャンするには、[File **Scan**（ファイルスキャン）] をクリックし、[Select **a file**（ファイルの選択）] をクリックします。Finder が開き、[隠しファイルの表示] や [圧縮ファイルのスキャン] を行うかどうかを選択できます。[自動修復] や [自動検疫] を有効にすることもできます。

スキャンの一時停止、休止、停止

定時スキャンの設定

シマンテック社へのセキュリティ情報提出のオンとオフの切り替え

スキャンの一時停止、休止、停止

一時停止機能を使うとスキャンを停止し、選択した別の期間に再開できます。スキャンはいつでも停止し、取り消すことができます。これらの機能を使うために管理者権限は必要ありません。

スキャンを再開すると、スキャンを停止した場所から開始されます。

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

休止が有効である場合、スキャンが始まる前にのみスキャンを休止することもできます。進行中のスキャンは休止できません。

実行中の定時スキャンを一時停止または停止するには

1. スキャンの進行状況ダイアログボックスで、[一時停止] をクリックします。
2. スキャンを続行するには [再開]、スキャンを停止するには [中止] をスキャンの進行状況ダイアログボックスで選択します。[完了] をクリックしてウィンドウを閉じることもできます。

実行中の手動スキャンを一時停止または停止するには

1. スキャンを一時停止するには、スキャンの進行状況ダイアログボックスで [一時停止] をクリックします。
2. 実行中の手動スキャンを停止するには [キャンセル] 、スキャンを続行するには [再開] をクリックします。

開始しようとするスキャンを休止するには

1. 休止する値 (期間) を選択するには、表示されるウィンドウでドロップダウンメニューをクリックします。最小で 15 分、最大で 1 日休止できます。
2. [OK] をクリックしてスキャンを休止します。

   予定通りスキャンを実行する場合、何もする必要はありません。

定時スキャンの設定

手動のスキャンの実行

感染およびリスクの検出についてのメッセージへの対応

コンピュータが感染しているかどうかを確認し、セキュリティを高めたり、パフォーマンスを向上させたりしたい場合は、追加タスクを実行できます。

クライアントが管理者によって管理されている場合も、管理外クライアントを実行している場合もあります。ユーザーが実行できる保護タスクは、管理者のクライアントに対する制御の程度によって異なります。

Symantec Endpoint Protection がウイルスまたはセキュリティリスクを検出した場合、リスクに対応するように求められることがあります。管理者が選択した設定に基づいて、クライアントが自動的に実行する処理について通知される場合もあります。

Table 7: 感染についてのメッセージへの対応

メッセージの内容	必要な対応
感染ファイルが修復された	なし
感染ファイルの修復の承認を要求する	修復を承認します。このオプションは Auto-Protect の環境設定によって異なります。 ウイルスとスパイウェアの対策設定の管理 自動的に感染ファイルを修復するオプションがオフにされている場合、ファイルを手動で修復する必要があります。 感染ファイルの修復
感染ファイルを修復できない	検疫にある感染を管理します。 検疫ファイルの管理

ウイルスとスパイウェアの対策が Mac を保護する方法

感染ファイルの修復

感染ファイルが自動的に修復されなかった場合や検疫に置かれなかった場合は、スキャン結果リストからファイルを修復できます。コンピュータのハードディスク上またはリムーバブルメディア上のファイルを手動で修復できます。

感染ファイルを修復するには

1. スキャン結果リストで、修復するファイルを選択し、 [修復] をクリックします。

   Mac の **Finder** または検索メニューでファイルを右クリックすることもできます。

2. 必要に応じて繰り返します。
3. 他の感染ファイルを確認する場合は、さらにスキャンを実行します。
4. 修復したファイルが正しく機能することを確認します。

ウイルスとスパイウェアの対策設定の管理

検疫ファイルの管理

検疫ファイルの管理

デフォルトでは、クライアントがファイル内のウイルスを検出するとウイルスを除去しようとします。ウイルスを除去できない場合、ファイルはコンピュータの検疫に置かれます。Symantec Endpoint Protection がファイル内のセキュリティリスクを検出すると、まず検疫にファイルを置きます。その後、リスクのすべての副作用が修復されます。

ウイルス定義を更新すると、クライアントは検疫を自動的に調べます。ユーザーは検疫にある項目を再スキャンできます。最新の定義によって、検疫されたファイルをクリーニングまたは修復できる場合があります。

検疫ファイルを管理するには

1. Symantec Endpoint Protection クライアントの [拡張] ページで、 [活動] > [Security **History** （ セキュリティ履歴 ）] > [検疫] をクリックすることで、
2. 管理するファイルを選択し、適切なオプションを選択します。

修復	検疫ファイルの修復を試みる場合はこのオプションを選択します。 ファイルが検疫された日よりウイルス定義が新しいことを確認してください。
削除	不要になったファイルを検疫から削除する場合はこのオプションを選択します。
復元	ファイルがウイルスを含んでいないことを確認したら、コンピュータの元の場所にファイルを復元できます。 このオプションは、ファイルをスキャンしたり、ファイルの修復を試みたりしません。

感染およびリスクの検出についてのメッセージへの対応

シマンテック社へのセキュリティ情報提出のオンとオフの切り替え

Symantec Endpoint Protection を使うと、検出された脅威に関する匿名情報をシマンテック社に提出できます。シマンテック社は、この情報を使って新しい脅威、対象になる脅威、変異する脅威からクライアントコンピュータを保護します。提出されるデータは、シマンテック社がコンピュータに対する脅威に対処して対策をカスタマイズするために役立ちます。

シマンテック社が遠隔測定によって収集したデータには、直接的には識別できない匿名要素が含まれている場合があります。シマンテック社は個人ユーザーを特定するために遠隔測定データの使用を必要としたり求めたりすることはありません。

デフォルトで、クライアントコンピュータはシマンテック社に検出に関する情報を送信します。シマンテック社はこの設定をオンのままにすることを推奨しますが、提出をオフにすることもできます。

このオプションはウイルス検出に関する情報のみを送信します。

NOTE
シマンテック社はこのオプションをオンのままにすることを推奨します。

シマンテック社への匿名セキュリティ情報の提出をオンまたはオフに切り替えるには

Symantec Endpoint Protection クライアントの [拡張] ページで、 [Product **Settings** （ 製品の設定 ）] をクリックし、 [Security **Info Submission** （ セキュリティ情報の提出 ）] をオンまたはオフにします。

定時スキャンの設定

手動のスキャンの実行

侵入防止の管理

侵入防止のデフォルト設定は Mac クライアントを保護します。ただし、独自の保護を管理したい場合はネットワーク脅威防止の一部として侵入防止を管理できます。

Table 8: 侵入防止の管理

手順	説明
ステップ 1: 侵入防止について学習する	侵入防止がネットワーク攻撃を検出して遮断する方法を学習します。 ネットワーク脅威防止で Mac を保護する方法
ステップ 2: 最新の IPS シグネチャのダウンロード	デフォルトでは、最新のシグネチャはクライアントにダウンロードされます。ただし、シグネチャをすぐにダウンロードする場合もあります。 Symantec Endpoint Protection の内容の即時更新
ステップ 3: 侵入防止の有効と無効を切り替える	トラブルシューティングを行う場合やクライアントコンピュータが過度の誤認を検出する場合は、侵入防止を無効にすることが必要な場合があります。通常は侵入防止を無効にしないでください。 ネットワーク脅威防止のオンとオフの切り替え
ステップ 4: 侵入防止通知を有効にするには	Symantec Endpoint Protection が攻撃を検出した場合に表示する通知を設定できます。 ネットワーク脅威防止通知のオンとオフの切り替え

Mac クライアントのファイアウォール保護の管理

Mac 用 Symantec Endpoint Protection ファイアウォールは、イベント、ポリシー、およびコマンドを含む Symantec Endpoint Protection に完全に統合されたファイアウォール保護を提供します。Symantec Endpoint Protection ファイアウォールは、管理下クライアントでのみ利用できます。

NOTE
Mac 用 Symantec Endpoint Protection ファイアウォールは、オペレーティングシステムの組み込みファイアウォールとは統合しません。そうではなく、並列で実行されます。オペレーティングシステムファイアウォールはアプリケーション層で検査しますが、Symantec Endpoint Protection ファイアウォールは下位レベル (IP と伝送) で検査します。Mac 用 Symantec Endpoint Protection ファイアウォールは、ピアツーピア遮断ルールは提供しませんが、カスタムファイアウォールルールによってこれらを部分的に作成することはできます。

Table 9: ファイアウォール保護の管理

手順	説明
ステップ 1: ファイアウォール保護の理解	ファイアウォール保護がトラフィックを監視し、一般的な攻撃ベクトルから保護する方法について説明します。 ネットワーク脅威防止で Mac を保護する方法
ステップ 2: ファイアウォールの有効と無効を切り替えるには	許可されるはずのトラフィックが遮断される場合などのトラブルシューティングを目的として、ファイアウォールを無効にすることが必要になる場合があります。通常、ファイアウォールを無効にするべきではありません。 ネットワーク脅威防止のオンとオフの切り替え

ネットワーク脅威防止のオンとオフの切り替え

通常、コンピュータでネットワーク脅威防止コンポーネントをオフにすると、コンピュータの安全性は低下します。ただし、誤認を回避するために侵入防止をオフにしたり、遮断されたトラフィックをトラブルシューティングするためにファ

イアウォールをオフにしたりすることが必要になる場合があります。侵入防止とファイアウォールはネットワーク脅威防止の一部です。

管理下クライアントでは、これらの設定の制御権は、管理者がクライアントをどのように設定したかによって異なります。さらに、これらの設定に行った変更は、次回のハートビートで、ポリシーが指定する内容に戻される可能性があります。

管理外クライアントの場合、ファイアウォールは利用できません。

ネットワーク脅威防止をオンまたはオフにするには

1. Symantec Endpoint Protection クライアントの [拡張] ページで、 [ネットワーク脅威防止] をクリックします。
2. 侵入防止を有効または無効にするには、 [侵入防止] をオンまたはオフにします。
3. ファイアウォールを有効または無効にするには、 [ファイアウォール] をオンまたはオフにします。
4. 侵入防止およびファイアウォールの通知を有効または無効にするには、 [Vulnerability **Protection** （脆弱性保護）] の設定アイコンをクリックし、ダイアログボックスで [Display **Vulnerability Protection Notifications** （脆弱性保護通知の表示）] をオンまたはオフにします。
5. [完了] をクリックします。

これらのコンポーネントをオフにした場合は、できるだけ早期に再度オンにして、コンピュータを最大限保護してください。

侵入防止の管理

Mac クライアントのファイアウォール保護の管理


Symantec
A Division of Broadcom