

# **Symantec Endpoint Protection 11.0**

## **導入時の注意及び推奨事項**

本資料に関する内容は、2009年3月現在のものとなります。製品の仕様等は、都合により予告なしに変更することがあります。本資料作成時のSEP11.0のバージョンはMR4となります。

本資料では主に Symantec Endpoint Protection (以下SEP) 導入時の推奨事項や保護コンポーネントのセキュリティポリシー作成時の指針に焦点を当てています。本資料では、SEP のインストール、ワークステーションへの導入、その他の管理に関する一般的な問題の詳細までは言及していません。これらの指針については製品マニュアルを参照してください。

ハードウェアの規模とアーキテクチャに関する推奨事項については、『Symantec Endpoint Protection アーキテクチャ、サイジング、及びパフォーマンスに関する検討事項』を参照してください。

## 【目次】

Symantec Endpoint Protection Manager(以下 SEPM)及びクライアント .....	3
SEPM 構成時の IIS 設定 .....	3
埋め込みデータベースと SQL データベース .....	3
SQL サーバーを使用する場合 .....	3
サイト(拠点)間のフェールオーバーとロードバランシング .....	3
同期 .....	4
64-bit やサーバーOS 上の制限事項 .....	4
ログの保持設定 .....	4
コンテンツ配布時の推奨事項 .....	5
SEPM .....	5
GUP .....	5
LiveUpdate Administrator と Symantec の LiveUpdate サーバー .....	6
SEPM のバックアップ .....	6
管理者アカウント .....	6
推奨するクライアント保護ポリシー .....	6
ウイルス対策とスパイウェア対策ポリシー .....	6
ファイアウォールポリシー .....	7
侵入防止 (IPS) ポリシー .....	8
アプリケーションとデバイス制御ポリシー .....	8
LiveUpdate ポリシー .....	8
集中例外ポリシー .....	9

## 導入時の注意・推奨事項

### Symantec Endpoint Protection Manager(以下SEPM)及びクライアント

SEP11.0を導入する場合、機能強化、不具合の修正、パフォーマンス調整などが多数実装されている最新バージョンの導入を推奨します。異なるバージョンでのSEPMとSEPクライアントの運用は可能ですが、SEPMのバージョンはSEPクライアントと同等もしくは、それ以上のバージョンにて運用することを推奨します。

最新のSEP11.0は下記サイトからダウンロードできます。

[https://fileconnect.symantec.com/licenselogin.jsp?localeStr=ja\\_JP](https://fileconnect.symantec.com/licenselogin.jsp?localeStr=ja_JP)

### SEPM構成時のIIS設定

SEPMをデフォルト設定で構成すると、IISの設定でTCP8014番を使用する「カスタムWebサイト」が有効になり、もう一方の「既定のWebサイト」が無効になります。「既定のWebサイト」を選択すると、「既定のWebサイト」を使う既存のアプリケーションがある場合、仮想ディレクトリの競合が発生する可能性があります。もしIISを使用する既存のアプリケーションとSEPMを共存する場合は、両方のアプリケーションを「カスタムWebサイト」で構築するか、SEPMを専用サーバー上に構築して運用することを推奨します。

### 埋め込みデータベースとSQLデータベース

埋め込みデータベースでは、5,000台未満のクライアントの管理を行えるよう設計されています。5,000台未満であっても、ログ保持期間やサイズをデフォルト値以上に設定して運用すると、データベースの容量が大きくなりますので、MicrosoftのSQLサーバーの使用をご検討下さい。埋め込みデータベース(Sybase Adaptive Server Anywhere)では格納されるデータが100万レコードを超えると、パフォーマンスの低下に繋がる可能性があります。

### SQLサーバーを使用する場合

SEPMとSQLを同じマシンにインストールすることは可能ですが、別々のマシンにインストールして運用することを推奨します。これは、ディスクのI/Oやボトルネックとなる他のリソースの消費を抑えるためです。また別々のマシンにSEPMとSQLをインストールする場合は、SEPMとデータベースは、ほぼ毎分通信している為、必ず同じLAN内に設置して下さい。

### サイト(拠点)間のフェールオーバーとロードバランシング

SQLを使用したSEPMを構築したサイト間を同期しており、サイト間を跨いだクライアントのフェールオーバーを行う場合、管理サーバーリストの設定で、各サイトのSEPMに異なる優先度を定義して下さい。同等レベルの優先度を定義したサイトを跨ぐクライアントのロードバランシングはサポートされません。

## 同期

- ・ クライアントパッケージと定義ファイル等のコンテンツは同期せず、各サイトの SEPM が LiveUpdate しコンテンツをダウンロードする設定を推奨します。
- ・ 同期に掛かる時間は、データサイズやネットワーク帯域幅等によりますが、同期処理が完了しない内に、次の同期処理が走るとデータベースのデッドロックが発生する可能性があるため、同期間隔は、最低でも 1 時間間隔に設定することを推奨します。

## 64bitやサーバーOS上の制限事項

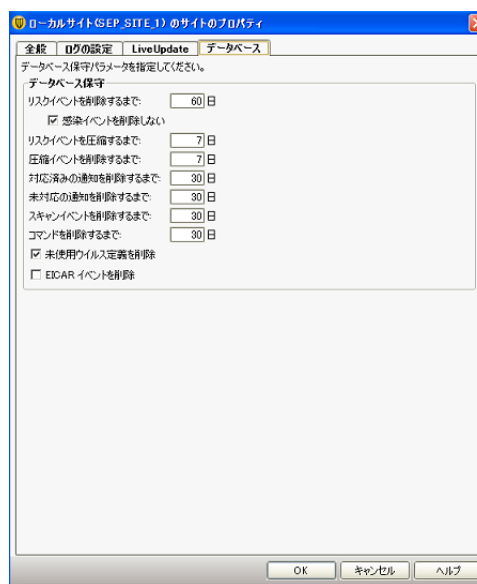
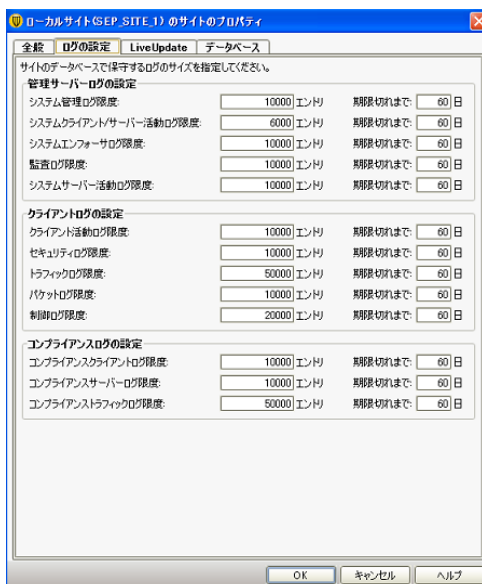
64bitやサーバーOSは、TruScan™やアプリケーションとデバイス制御機能に対応していません。詳しくは、下記のMR4リリース時点でのプラットフォーム別機能対応表をご確認下さい。現在未対応の機能はインストールしないか、無効としてお使い頂く事を推奨します。

クライアント機能	Win 2k pro	WinXP 32	WinXP 64	Vista 32	Vista 64	Win2k server	Win 2k3 32-bit	Win 2k3 64-bit	Win 2k8 32-bit	Win 2k8 64-bit
オンデマンドスキャン	○	○	○	○	○	○	○	○	○	○
ファイルシステムAuto-Protect	○	○	○	○	○	○	○	○	○	○
インターネット電子メールAuto-Protect	○	○	×	○	×	×	×	×	×	×
Lotus Notes Auto-Protect	○	○	×	○	×	○	○	×	○	×
Microsoft Outlook Auto-Protect	○	○	×	○	×	○	○	×	○	×
デバイス制御	○	○	×	○	×	○	○	×	○	×
アプリケーション制御	○	○	×	○	×	○	○	×	○	×
ファイアウォール	○	○	○	○	○	○	○	○	○	○
侵入防止 (IPS)	○	○	○	○	○	○	○	○	○	○
TruScanプロアクティブ脅威スキャン*	○	○	×	○	×	×	×	×	×	×
SNAC ホストインテグリティ	○	○	○	○	○	○	○	○	○	○
変更対策	○	○	×	○	×	○	○	×	○	×

## ログの保持設定

SEP では、大半のログは日数ベース又はサイズベースで、データを保持するように設定できます。サイズに関係なく一定期間ログを保持する場合には、次のような設定を行います。

- 1) [ログエントリ数]を 999999999 に設定し、保持する日数を設定(例: 30 日など)  
(SEPM コンソール>サーバー>サイトのプロパティ>ログの設定)
- 2) ログを保持する日数と一貫性があるように[リスクイベントを削除するまで]を設定  
(SEPM コンソール>サーバー>サイトのプロパティ>データベース)



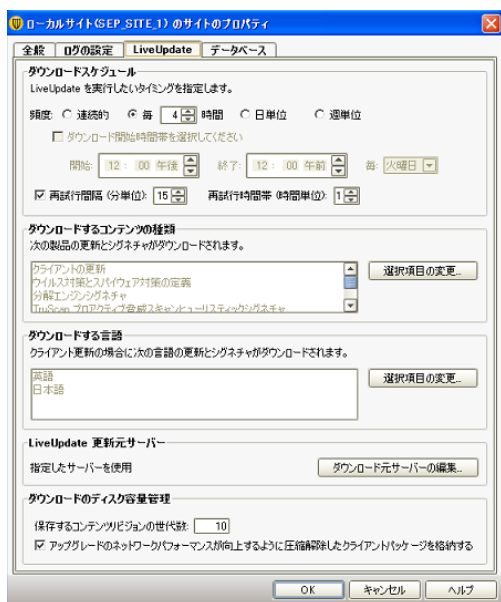
## コンテンツ配布時の推奨事項

コンテンツ配布方法は複数ありますが、本資料では SEPM、グループ更新プロバイダ(以下 GUP)、及び LiveUpdate Administrator を使用した配布について説明します。

### SEPM

デフォルトで SEPM は 4 時間ごとに Symantec の LiveUpdate サーバー に接続し、新しいコンテンツを取り込みます。ウイルス定義ファイルは、毎日 2-3 回提供されます。

メモ: SEPM の LiveUpdate スケジュールは、デフォルトの 4 時間ごとの設定を推奨します。ウイルス定義ファイルは 1 日に 2-3 回更新されますので、[連続的(15 分間隔)]に設定する必要はありません。



SEPM 上にクライアントが保持している定義と最新の定義が存在する場合、差分が生成されクライアントに配布されます。クライアントが保持している定義が SEPM がない場合、フルの定義ファイルが配布されます。差分が生成されるようにするには、管理者が SEPM に十分な世代数の定義を保持することが重要です。例えば、1 ヶ月さかのぼってクライアントが差分の定義を取得できるようにするには、[保存するコンテンツリビジョンの世代数]を 1 日 3 回定義ファイルをリリースしたと計算し、「90」世代に設定します。もしユーザーが 1 ヶ月定義ファイルを更新していない環境下においても、差分取得が可能です。SEPM に多くの世代を保持する事により、フルの定義ファイルを配布するよりもネットワーク帯域に負荷が掛かりません。

メモ: 2008 年下半期に弊社の環境で 90 世代のコンテンツを保持した結果、SEPM 上のコンテンツ総サイズは約 22GB となりました。

### GUP

1,000 台までの SEP クライアントが存在するサイト(拠点)がある場合、GUP をリモートサイト(拠点)に導入することを検討して下さい。GUP はグループ内の 1 台の SEP クライアントが代表して、SEPM の代わりにコンテンツを他の SEP クライアントに配布します。GUP を使用する事によって、2 つのサイト間の WAN をまたぐネットワークトラフィックを最小にする事が可能です。GUP が何らかの問題でダウンした場合、SEP クライアントは SEPM にフェールオーバーし、SEPM より定義ファイルを取得する事も可能です。

メモ: GUP は常に電源がオンになっている端末に設定することが望ましいです。

## LiveUpdate AdministratorとSymantecのLiveUpdateサーバー

LiveUpdate は SEPM と SEP クライアント通信とは異なるスケジュール設定が行えます。コンテンツ更新を一定の時間帯に行う場合に、クライアントは Symantec の LiveUpdate サーバーや LiveUpdate Administrator を構築した社内 LiveUpdate サーバーから、直接差分のコンテンツを取得できます。LiveUpdate を使用する例として、10 台以下のクライアントが存在するリモートサイト(拠点)に、SEPM を設置するのではなく、直接インターネット上にある Symantec の LiveUpdate サーバーへウイルス定義ファイル等のコンテンツを取得させる方法があります。その他、1,000 台以上のクライアントが存在する場合には、リモートサイト(拠点)に社内 LiveUpdate サーバーを設置し、コンテンツの配布する方法もございます。

---

メモ: LiveUpdate Administrator2.x を導入する場合、SEPM と同居せず、別々のマシンに SEPM と LiveUpdate Administrator2.x を導入して運用する事を推奨します。

---

### SEPMのバックアップ

SEPM サーバーのバックアップを定期的に行うことを推奨します。また何らかの障害で SEPM を再構築する場合には、必ずサーバー証明書のバックアップを取得しておいて下さい。詳しくは下記のナレッジベースをご参照下さい。

[http://service1.symantec.com/support/inter/entsecurityjapanesekb.nsf/jp\\_docid/20080403175122949?OpenDocument&dtype=corp](http://service1.symantec.com/support/inter/entsecurityjapanesekb.nsf/jp_docid/20080403175122949?OpenDocument&dtype=corp)

### 管理者アカウント

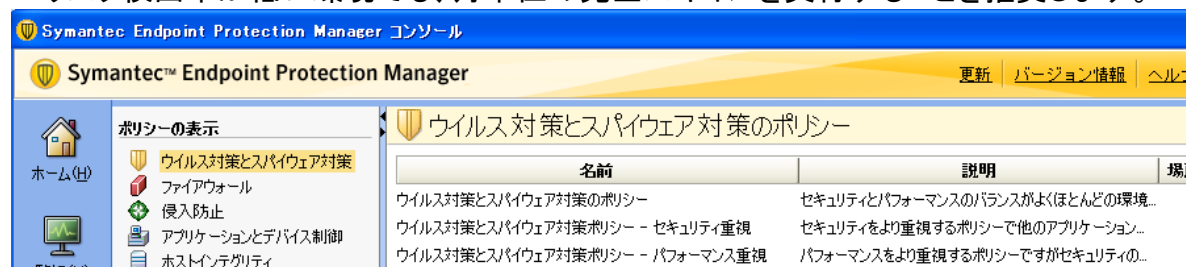
管理者が 1 名のみでも、アカウントロックアウト時に備え 2 つ以上のアカウントを作成することを推奨します。アカウントロックアウト中は、設定時間を経過するまでログイン出来なくなります。

### 推奨するクライアント保護ポリシー

以下は、Windows XP 及び Vista 上で SEP クライアントを実行する場合の推奨事項です。

#### ウイルス対策とスパイウェア対策ポリシー

必ず Auto-Protect を有効にし、週単位の完全スキャンの実行を推奨します。定時スキャンで発見されるリスクが少ない場合、スケジュールとスキャン対象ファイルを減らし運用します。リスク検出率が低い環境でも、月単位の完全スキャンを実行することを推奨します。



The screenshot shows the Symantec Endpoint Protection Manager console. The main window displays the 'Virus and Spyware Protection Policy' settings. The left sidebar shows a navigation menu with options like 'Home', 'Policy Display', and 'Host Integrity'. The main content area shows a table of policies with columns for 'Name' and 'Description'.

名前	説明	場
ウイルス対策とスパイウェア対策のポリシー	セキュリティとパフォーマンスのバランスがよくほとんどの環境...	
ウイルス対策とスパイウェア対策ポリシー - セキュリティ重視	セキュリティをより重視するポリシーで他のアプリケーション...	
ウイルス対策とスパイウェア対策ポリシー - パフォーマンス重視	パフォーマンスをより重視するポリシーですがセキュリティの...	

SEPMには ウイルス対策とスパイウェア対策ポリシー(デフォルト)、ウイルス対策とスパイウェア対策ポリシー(セキュリティ重視)、ウイルス対策とスパイウェア対策ポリシー(パフォーマンス重視)の3つのウイルス対策ポリシーが用意されています。ほとんどの場合、デフォルトウイルス対策ポリシーを適用し、低速でリソース消費が高いコンピュータやパフォーマンスに問題があるコンピュータには、パフォーマンス重視のポリシー、ミッションクリティカルなコンピュータ、検出率が高い(インターネットのウイルス対策が十分でない)コンピュータまたはユーザーには、セキュリティ重視のウイルス対策ポリシーを適用することを推奨します。

次に上記の項目以外に検討すべき設定を示します。

### 検討する追加設定

- ・ バッテリーで動作する場合、「バッテリーで動作するときに定時スキャンを遅延する」を有効にすることを推奨します。バッテリーで動作中のクライアントに定時スキャンで完全スキャンを実行すると、バッテリーを早く消耗してしまいます。
- ・ エンドユーザーにスキャンを中止する権限を与える場合、[スキャンの進行状況を表示する]と[ユーザーによるスキャンの停止を許可する]を有効にします。スキャンをユーザーが中止することが多い場合、[ユーザーによるスキャンの一時停止または休止を許可する]を有効にします。

[インターネット電子メール Auto-Protect]、[TruScan プロアクティブ脅威スキャン]、[検疫]、[提出]はデフォルト設定を推奨します

SEPは1日に2-3回ウイルス定義ファイルを更新し、1日に平均7,500ものシグネチャを追加します。毎日定義を更新しないとセキュリティレベルが低下するため、定義が古い場合は、エンドユーザーに警告メッセージを通知することを推奨します。

### ファイアウォールポリシー

ファイアウォールの導入を検討している場合は、設定ミス等で正当なアプリケーション通信が遮断されることのないよう注意して下さい。導入時は、全ての通信を許可するファイアウォールルール作成や、ファイアウォールポリシーを撤回し侵入防止(IPS)のみを有効にする状態から始め、十分な検証を行ってからファイアウォールによる通信を制御し、徐々にセキュリティを高めていくことを検討して下さい。

No	有効	名前	重大度	アプリケーション	ホスト	時間	サービス	アダプタ	スクリー...	処理
1	<input checked="" type="checkbox"/>	Allow all	5-重度	★ 任意	★ 任意	★ 任...	★ 任意	すべての...	★ 任意	🟢 許可
2	<input checked="" type="checkbox"/>	IPv6 を遮断する	10-軽度	★ 任意	★ 任意	★ 任...	Ethe...	すべての...	★ 任意	🔴 遮断
3	<input checked="" type="checkbox"/>	IPv6 over IPv4 (Tere...	10-軽度	★ 任意	★ 任意	★ 任...	UDP...	すべての...	★ 任意	🔴 遮断
4	<input checked="" type="checkbox"/>	IPv6 over IPv4 (ISA...	10-軽度	★ 任意	★ 任意	★ 任...	IP:[41]	すべての...	★ 任意	🔴 遮断
5	<input checked="" type="checkbox"/>	断片化パケットを許可...	10-軽度	★ 任意	★ 任意	★ 任...	IP:[fr...	すべての...	★ 任意	🟢 許可
6	<input checked="" type="checkbox"/>	無線 EAPOL を許可...	10-軽度	★ 任意	★ 任意	★ 任...	Ethe...	すべての...	★ 任意	🟢 許可

社内ネットワークに接続している場合は全ての通信を許可するファイアウォールを適用し、ユーザーが社内ネットワークに接続していない場合はファイアウォールの強化を検討するこ

とも有効です。また、Symantec Network Access Control で提供されるピアツーピア認証方式を使うことにより、リモートコンピュータが企業ポリシーに準拠していない場合、そのコンピュータからのすべての接続を強制的に遮断することもできます。

場所(クライアントが接続する環境)ごとに、異なるファイアウォールポリシーを定義するときには間違いやすい設定があります。社内ネットワークに繋がっていない場合にファイアウォールルールを強化し、社内ネットワークに繋がっている場合にルールを緩めるような設定をするとき、誤った場所のトリガーを設定してしまうことです。たとえば、場所のトリガーを管理サーバーに接続しているか、接続していないかのみを選択したとします。管理サーバーが停止した場合、そのサーバーに接続できないため、全てのクライアントはリモートの場所に切り替わり、クライアントは社内のネットワークに接続していても、社外用のファイアウォールルールが適用されてしまいます。

---

**メモ:** 特にサーバーOS 上では、全てのトラフィックを許可したファイアウォールルールを作成し、侵入防止 (IPS) 機能を有効にしたネットワーク脅威防止機能を導入することを推奨します。ファイルサーバーや DHCP サーバーとして稼働しているサーバーにファイアウォールを導入すると、パフォーマンスのオーバーヘッドや競合が発生する可能性があります。通信自体を制御する必要がある場合は、十分な検証を行った上で導入して下さい。

---

### 侵入防止 (IPS) ポリシー

常時、侵入防止機能を有効にすることを推奨します。組織内の管理者またはユーザーがセキュリティツールと評価ツールを実行している場合に、誤検知が発生する可能性があるため、これらのアプリケーションを侵入防止検出から除外設定することを推奨します。

### アプリケーションとデバイス制御ポリシー

アプリケーション制御とデバイス制御は、情報漏えい対策としての拡張機能です。アプリケーションとデバイス制御機能により、管理者は企業内のアプリケーションとユーザーの動作を制限できます。アプリケーション制御では、「USB メモリへの書き込み」や「すべてのリムーバブルドライブを読み取り専用」など7つのルールセットがデフォルトで用意されています。

### LiveUpdateポリシー

クライアントを更新する方法を、常に複数用意しておくことを推奨します。ポリシーを2つ作成し、一つ目のポリシーでは管理サーバーである SEPM に接続できる場合、SEPM よりコンテンツを更新するポリシーと、もう一つのポリシーでクライアントが SEPM に接続できない場合、Symantec の LiveUpdate サーバーや社内 LiveUpdate サーバーからコンテンツを更新するポリシーを用意します。SEPM がインストールされていないリモートの拠点ではグループ更新プロバイダ (GUP) を使うことや、常にユーザーが手動で LiveUpdate を実行できるようにすることを推奨します。

## 集中例外ポリシー

必要に応じてウイルススキャン等の例外(除外)を追加することが可能です。SEP では、特定のアプリケーションに対して自動的に例外を適用しますが、データベース、トランザクションログ、VMware イメージ、その他トランザクションのボリュームが大きい項目に対しては、例外を追加することを推奨します。除外設定方法については下記のシマンテック社のオンラインナレッジベースを参照してください。

### 集中例外の設定方法

[http://service1.symantec.com/support/inter/entsecurityjapanesekb.nsf/jp\\_docid/20071211111642949?OpenDocument&dtype=corp](http://service1.symantec.com/support/inter/entsecurityjapanesekb.nsf/jp_docid/20071211111642949?OpenDocument&dtype=corp)

## その他の便利なオンラインリソース

Symantec Endpoint Protection ホワイトペーパー (サイジング資料や移行ガイド等)

[http://www.symantec.com/ja/jp/business/products/whitepapers.jsp?pcid=pcat\\_info\\_risk\\_comp&pvid=endpoint\\_prot\\_1](http://www.symantec.com/ja/jp/business/products/whitepapers.jsp?pcid=pcat_info_risk_comp&pvid=endpoint_prot_1)

Symantec Endpoint Protection 11.0: サポートナレッジベース

<http://service2.symantec.co.jp/support/inter/entsecurityjapanesekb.nsf/Enterprise-HotTopics/Endpoint%20Protection%2011?OpenView>