SOPHOS

Security made simple.

Sophos Enterprise Console
ポリシー設定ガイド

製品バージョン: 5.5

目次

1 このガイドについて

このガイドでは、Sophos Enterprise Console および Sophos Endpoint Security and Control のポリシーを設定する際のガイドラインについて説明します。

注: ライセンスの種類により利用できない機能もあります。

主な内容は次のとおりです。

- 推奨するポリシーの設定方法。
- 各種類のポリシーを設定し、適用する。
- 検索オプションを使用してアイテムを検出する。
- 検索から除外するアイテムを指定する。

このガイドの対象読者は次のとおりです。

- Enterprise Consoleのユーザー。
- ポリシーの設定や適用方法を最適化したい方。

このガイドをお読みになる前に、「**Sophos Enterprise Consoleクイック スタートアップ ガイド**」をご覧ください。

Enterprise Console に関するすべてのドキュメントは、http://www.sophos.com/ja-jp/support/documentation/enterprise-console.aspx から入手可能です。

2 ポリシーの設定にあたって

Enterprise Console をインストールすると、「デフォルト」というポリシーが作成されます。デフォルトポリシーは、新たに作成するグループすべてに適用されます。デフォルトポリシーを使用するだけで、十分に保護を提供できるようになっています。なお、ネットワーク アクセス コントロール、パッチ、アプリケーション コントロール、データコントロール、デバイスコントロール、タンパー プロテクションなどの機能を使用する場合は、新たにポリシーを作成するか、デフォルトポリシーを変更する必要があります。ポリシーを設定する際は、次の点に注意してください。

- 可能な限り、ポリシー内のデフォルト設定を使用してください。
- デフォルトポリシーの設定を変更したり、新規ポリシーを作成したりする場合は、設定対象のコンピュータの役割 (クライアントマシン、サーバーなど) を考慮してください。
- ポリシーを全体で管理する場合は、Enterprise Console を使用し、可能な限り、各コンピュータ上でなく Enterprise Console でオプションを設定してください。
- コンピュータごとに一時的な設定が必要な場合や、検索の詳細設定など、全体で管理できない項目を設定する場合のみに、各コンピュータでオプションを設定してください。
- 常時、特別な設定が必要なコンピュータに対しては、専用のグループおよびポリシーを作成してください。

3 アップデートポリシーの設定

アップデートポリシーは、新しい脅威定義ファイルや、ソフォス製品の更新ファイルを各コンピュータに配布する方法を指定します。ソフトウェアのサブスクリプションは、各プラットフォームに対して、ソフォスのサーバーから定期的にダウンロードする、エンドポイント用ソフトウェアのバージョンを指定するものです。デフォルトのアップデートポリシーを使うと、「推奨バージョン」というサブスクリプションで指定されているソフトウェアをインストール、アップデートできます。アップデートポリシーを設定する際は、次の点に注意してください。

- 通常、自動的に最新の状態に保つために、各ソフトウェアの「推奨バージョン」を選択します。しかし、運用環境に展開する前に、新しいバージョンのソフトウェアを評価する場合は、評価を実施する間、固定バージョンのソフトウェアを運用環境で利用することもできます。固定バージョンの場合、脅威検出データは更新されますが、ソフトウェアは毎月リリースされる最新バージョンに更新されません。
- 1つのアップデートポリシーを使用するグループの数が、管理可能な範囲にあることを確認してください。通常、1つのアップデート元からアップデートできるコンピュータの台数は1,000台までです。最適なアップデート台数は、1つのアップデート元に対し600～700台です。

  注: 同じディレクトリからアップデートできるコンピュータの台数は、そのディレクトリのあるサーバーやネットワークの接続性によって異なります。

- デフォルトで各コンピュータは1箇所のプライマリロケーションに接続し、アップデートを実行しますが、セカンダリロケーションを設定し、常に別のアップデート元が使える状態にしておくことを推奨します。エンドポイントコンピュータがプライマリのアップデート元に接続できない場合、セカンダリのアップデート元が設定されていれば、そこからアップデートを実行します。詳細は Sophos Enterprise Consoleヘルプの「**コンピュータのアップデート** > **アップデートポリシーを設定する**」のセクションを参照してください。

- 社内に海外出張や長距離出張をするモバイルPCユーザーがいる場合は、移動先でのアップデートを許可するように、アップデートポリシーを設定する必要があります。このオプションが有効になっていると、外出先のモバイル PC は同じローカルネットワークに接続している固定マシンに問い合わせを行い、最も近いアップデートロケーションを検出し、そこからアップデートを実行するため、アップデート時間の短縮、およびネットワーク帯域の抑制につながります。複数のロケーションが検出された場合は、モバイル PC から最も近いと判断されたロケーションが使用されます。いずれのロケーションにも接続できない場合、モバイル PC に適用されているアップデートポリシーが定義するプライマリロケーション (接続できない場合はセカンダリロケーション) が使用されます。

  移動先でのアップデートの許可機能は、外出先のモバイルPC と固定エンドポイントが、同じ Enterprise Console のインスタンスによって管理され、同じソフトウェアのサブスクリプションを使用している場合だけ利用できます。他社製のファイアウォールがある場合、アップデートサーバーのロケーションのクエリや応答を許可するよう設定する必要があります。デフォルトで 51235 ポートが使用されますが、変更可能です。

詳細は、Sophos Enterprise Consoleヘルプの「**コンピュータのアップデート** > **アップデートポリシーを設定する** > **アップデートサーバーのロケーションを設定する**」のセクションを参照してください。移動先でのアップデートに関するよくある質問は、ソフォスのサポートデータベースの文章 112830 を参照してください。(http://www.sophos.com/ja-jp/support/knowledgebase/112830.aspx)

- 速度の遅いコンピュータで、パフォーマンスに与える影響を最小限に抑えるには、まず、固定バージョンのソフトウェアのダウンロードを指定し、ソフトウェアのアップデート版をインストールする準備ができた時点で、ソフトウェアのサブスクリプションを手動で変更してください。これによって、コンピュータは常に最新の脅威検出データで更新されます。また、処理速度の遅いコンピュータの場合、アップデートの頻度を減らしたり (1日に 2～3回にするなど)、通常の就業時間外 (夜間、週末など) にアップデートを行うなどの対策を取ることもできます。

⚠ **注意:** アップデート頻度を減らすと、セキュリティリスクが高まることに注意してください。

4 ウイルス対策および HIPS ポリシーの設定

4.1 設定にあたって

ウイルス対策および HIPS ポリシーは、セキュリティソフトがウイルス、トロイの木馬、ワーム、スパイウェア、アドウェア、および不要と思われるアプリケーション (PUA) を検索し、疑わしい動作やファイルを検知・検出する方法を指定します。また、コンピュータをクリーンアップする方法も指定します。ウイルス対策および HIPS ポリシーを設定する際は、次の点を考慮してください。

- デフォルトのウイルス対策および HIPS ポリシーで、コンピュータはウイルスやその他のマルウェアから保護されます。ただし、不要と思われるアプリケーションや疑わしい動作の検出を有効にする場合は、新たにポリシーを作成するか、デフォルトのポリシーを変更する必要があります。
- デフォルトで有効に設定されている Sophos Live Protection の機能を活用するには、「**サンプルファイルをソフォスに自動送信する**」オプションも選択することを推奨します。
- Malicious Traffic Detection (MTD - 悪質なトラフィックの検出) を有効にしてください。この機能は、エンドポイントコンピュータと、ボットネットやその他のマルウェア攻撃に関わっているコマンドアンドコントロールサーバー間の通信を検知します。Enterprise Console 5.3 以降を新規インストールした場合、「**悪質なトラフィックを検知する**」オプションはデフォルトで有効に設定されます。旧バージョンの Enterprise Console をアップグレードした場合、この機能を使用するにはオプションを有効に必要があります。

  注: Malicious Traffic Detection (MTD) は、現在 Windows 7 以降のみ (サーバー OS 以外) に対応しています。Sophos Live Protection が必要です。

- 疑わしい動作のみを検知するため、「**警告のみ**」オプションを指定してください。はじめに、レポートのみ受信することをポリシーで指定することで、ネットワーク全体の疑わしい動作の全容を把握することができます。このオプションはデフォルトで有効になっていますが、プログラムやファイルのブロックを指定するポリシーを適用後は、無効に設定してください。

詳細はソフォス サポートデータベースの文章 114345 を参照してください。
(http://www.sophos.com/ja-jp/support/knowledgebase/114345.aspx)

4.2 ウイルス対策および HIPS ポリシーを適用する

ウイルス対策および HIPS ポリシーは、次のように適用することを推奨します。

1. グループごとに異なるポリシーを作成します。
2. Sophos Live Protection のオプションを設定します。この機能は、ソフォスのオンライン検索サービスを使用して、不正な疑いのあるファイルが脅威であるか否かを瞬時に判断

し、ソフォス製品のソフトウェアをリアルタイムで更新します。Malicious Traffic Detection とダウンロードレピュテーション機能には、Sophos Live Protection が必要です。

- 「**オンアクセス検索での Live Protection を有効にする**」と「**オンデマンド検索での Live Protection を有効にする**」のオプションが選択されていることを確認してください。エンドポイントコンピュータのウイルス検索機能で疑わしいファイルが検出されたものの、ローカルの脅威定義ファイル (IDE ファイル) によるチェックでは、そのファイルが悪質なファイルであるか否かを判断できない場合は、ファイルの特徴 (チェックサムやその他の属性など) をソフォスに提出し、さらなる解析を行います。ソフォスのオンライン検索サービスでは、疑わしいファイルが瞬時に SophosLabs のデータベースに照会されます。ファイルが未感染または悪質であると判断された場合、結果がローカルコンピュータに返信され、ファイルのステータスが自動的に更新されます。
- 「**サンプルファイルをソフォスに自動送信する**」オプションを選択します。悪意のあるファイルと想定されるものの、ファイルの特徴だけからでは悪質なファイルと判断できない場合、Sophos Live Protection で、ソフォスへのサンプルファイルの提出が要求されます。Live Protection が有効で「サンプルファイルをソフォスに自動送信する」オプションが有効になっている場合、ソフォスに当該のファイルのサンプルがなければ、ファイルが自動的にソフォスに送信されます。ソフォスは、このようなファイルのサンプルの送信を通じて、誤検出のリスクを抑えたマルウェア検出率の継続的な向上に取り組んでいます。

重要: 使用している Web フィルタで、ファイルの送信先であるソフォスのドメインを信頼済みサイトとして設定する必要があります。詳細はソフォスサポートデータベースの文章 62637 を参照してください。(http://www.sophos.com/ja-jp/support/knowledgebase/62637.aspx)WS1000 Web Appliance などのソフォス Web フィルタリング ソリューションを使用している場合、何も操作は必要ありません。ソフォスのドメインは信頼できるドメインに既に指定されています。

3. ウイルス/スパイウェアを検索します。
   a) ウイルス/スパイウェアを検索するには、オンアクセス検索を有効にするか、または「スケジュール検索」でシステムのフル検索を設定します。デフォルトでオンアクセス検索は有効になっています。詳細は、オンアクセス検索の使用 (p. 36) または スケジュール検索の使用 (p. 37) を参照してください。
   b) ウイルス/スパイウェアのクリーンアップのオプションを設定します。
4. 疑わしいファイルを検索します。

   疑わしいファイルとは、マルウェアに共通の特質を持つものの、新種のマルウェアとして検出されるには至らないファイルを指します。

   a) 疑わしいファイルを検索するには、オンアクセス検索を有効にするか、「スケジュール検索」でシステムのフル検索を設定します。
   b) 検索の設定で「**疑わしいファイル**」オプションを選択します。
   c) 疑わしいファイルのクリーンアップのオプションを設定します。
   d) 必要に応じて、実行を許可するファイルをすべて認証します。
5. 悪意のあるファイル、疑わしい動作、バッファオーバーフロー、および悪質なトラフィックを検知します (動作監視機能)。

これらのオプションは、実行中のプロセスを常に監視し、プログラムに悪質または疑わしい動作が見られないかを判定します。この機能は脆弱性対策に有効です。

a) オンアクセス検索に対する動作監視が有効になっていることを確認します。このオプションはデフォルトで有効になっています。

b) 「**悪質なトラフィックを検知する**」オプションが選択されていることを確認します。

c) 「**警告のみ**」オプションを指定して、疑わしい動作およびバッファオーバーフローの検知のみを行います。このオプションはデフォルトで有効になっています。

d) 今後も継続して使用するプログラムやファイルすべてを認証します。

e) 「**警告のみ**」オプションを選択から外して、検出されたプログラムやファイルをブロックするようポリシーを設定します。

この方法により、ユーザーが必要なプログラムおよびファイルがブロックされないようになります。詳細はソフォス サポートデータベースの文章 50160 を参照してください。(http://www.sophos.com/ja-jp/support/knowledgebase/50160.aspx)

6. アドウェアや不要と思われるアプリケーションを検索します。

はじめてアドウェアや不要と思われるアプリケーションを検索すると、ネットワーク上で既に起動しているアプリケーションに対する大量の警告が発生することがあります。最初にスケジュール検索を実行することで、ユーザーの作業環境に影響を与えることなく、ネットワークで既に起動しているアプリケーションに対処することができます。

a) すべてのアドウェアや不要と思われるアプリケーションを検索するために、「スケジュール検索」でシステムのフル検索を設定します。

b) 検索によって検出されたアプリケーションを認証またはアンインストールします。

c) 「**アドウェアや不要と思われるアプリケーション**」オンアクセス検索オプションを選択して、今後、他のアドウェアや不要と思われるアプリケーションが検出されるようにします。

詳細はソフォス サポートデータベースの文章 13815 を参照してください。(http://www.sophos.com/ja-jp/support/knowledgebase/13815.aspx)

7. Web ページ内の脅威を検索します。

次のオプションを指定して、マルウェア感染サイトへのアクセスをブロックし、悪質なコンテンツがダウンロードされないよう検索します。

a) 「**悪意のある Web サイトへのアクセスブロック**」オプションが「**有効**」になっていることを確認し、悪意のある Web サイトへのアクセスをブロックします。このオプションはデフォルトで有効になっています。

b) 「**コンテンツスキャン**」オプションを「**有効**」または「**オンアクセス検索の設定と同じ**」に指定して、悪意のあるダウンロードデータを検索し、ブロックします。デフォルトで設定されている「**オンアクセス検索の設定と同じ**」を選択した場合、オンアクセス検索が有効になっている場合のみ、ダウンロードスキャンが実行されます。

c) 必要に応じて、アクセスを許可する Web サイトをすべて認証します。

d) レピュテーションチェックが有効に設定されていることを確認します。

注: さらに、Web コントロール ポリシーを使用して、不適切とされる上位 14種類のサイトカテゴリに基づいて Web サイトをフィルタリングし、ユーザーの Web サイト閲覧

を管理することができます。Web コントロール ポリシーの設定方法については、Web コントロールポリシーの設定 (p. 30) を参照してください。

ウイルス対策および HIPS ポリシーの設定について、詳細は Sophos Enterprise Console ヘルプを参照してください。

5 ファイアウォール ポリシーの設定

5.1 ファイアウォールポリシーについて

ファイアウォールポリシーでは、どのような方法でファイアウォールがコンピュータを保護するかを設定します。ここで指定するアプリケーションやアプリケーションのクラスだけに、社内ネットワークやインターネットへの接続が許可されます。

注: Sophos Client Firewall は、サーバー OS では利用できません。本製品のシステム要件は、ソフォスの Web サイトの「システム要件」を参照してください。(http://www.sophos.com/ja-jp/products/all-system-requirements)

注意: ファイアウォールポリシーは、製品を使用する前に必ず構成してください。未変更のデフォルトポリシーを Enterprise Console からコンピュータのグループに適用すると、ネットワークの通信障害が発生します。

デフォルトのファイアウォールポリシーは、そのままの状態で適用することを目的に構成されていないため、通常の環境での使用には適していません。ポリシーをカスタマイズする際のテンプレートとして使用してください。

ファイアウォールはデフォルトで有効になっているため、必須のネットワークトラフィック以外はすべてブロックされます。デフォルトのポリシーは必要不可欠な接続以外をすべてブロックするため、ほとんどの場合、基礎ネットワーク以外 (メールソフト、Web ブラウザ、ネットワーク上のデータベース接続など) の接続はすべて正常に動作しません。したがって、必ず、使用するトラフィック、アプリケーション、およびプロセスを許可するように設定し、テストを行った上で、すべてのコンピュータにファイアウォールをインストール・実行してください。

5.2 ファイアウォールポリシーの設定を準備する

ファイアウォールのルール (グローバル ルール、アプリケーション ルールなど) を作成/編集する前に、ポリシーの作成について計画を立て、導入の目的を明確にしてください。

ファイアウォールのポリシーを作成する際は次の点を考慮してください。

- どのコンピュータに Sophos Client Firewall をインストールするか。
- コンピュータはデスクトップとモバイル PC のどちらであるか。「2種類の設定 (モバイル PC 用)」は、モバイル PC に適しています。
- 接続先の検出方法は、「DNS 参照を使用する」、「ゲートウェイの MAC アドレスを使用する」のどちらにするか。
- ネットワーク上のシステムおよびプロトコル。
- リモート接続。

各ユーザーグループで必要なアプリケーションやネットワークのアクセス権に基づいて、作成するファイアウォール ポリシーの数を決めます。これらのポリシーでは、さまざまなア

プリケーションを設定し、制限の程度も異なります。複数のポリシーを作成するには、複数の Enterprise Console のグループが必要となることに注意してください。

- 1つのSophos Client Firewall ポリシーのみを使用しないでください。ポリシーが 1つしかない場合、たとえば、1～2台のコンピュータ (管理者用ワークステーションなど) のみに対して特定のルールを追加すると、追加したルールがネットワーク全体に対して存在することになります。この状態はセキュリティリスクとなります。
- また、反対にポリシーを作成しすぎてもシステム監視やメンテナンスの負荷が高くなります。

ネットワーク上のシステムおよびプロトコル

社内ネットワークの根幹となるサービスを考慮します。例:

- DHCP
- DNS
- RIP
- NTP
- GRE

デフォルトのファイアウォール構成には、これらのサービスのほとんどを制御するルールが含まれています。ただし、許可するべきものと不要なものをよく把握してください。

コンピュータへのリモート接続

コンピュータの監視や保守作業にリモート接続ソフトを使用する場合は、リモート接続を許可するルールをポリシーに追加する必要があります。

ネットワーク上のコンピュータへの接続方法を調べます。例:

- RDP
- VPN クライアント/サーバー
- SSH/SCP
- Terminal Services
- Citrix

必要な接続の種類を確認し、それに応じてルールを作成します。

5.3 設定にあたって

ファイアウォールポリシーを設定する際は、次の点に注意してください。

- Sophos Client Firewall をインストールすると、Windows ファイアウォールは無効になります。このため、Windows ファイアウォールを使用している場合は、その設定内容をあらかじめメモし、Sophos Client Firewall に適用します。
- 「**規定で許可**」モードを指定して、トラフィック、アプリケーションおよびプロセスの検出のみを行い、ブロックは行わないようにします。はじめに、レポートのみのポリシーを定義することで、ネットワーク活動の全容を把握することができます。

- 「ファイアウォール - イベントビューア」を使用して、使用中のトラフィック、アプリケーションおよびプロセスを表示してください。イベントビューアを使用して、レポートされたトラフィック、アプリケーションおよびプロセスを許可/ブロックするルールを容易に作成することができます。イベントビューアを開くには、「**イベント** > **ファイアウォールのイベント**」をクリックします。
- イベントビューアで作成したルールの内容を確認してください。1種類のアプリケーションが原因で複数のファイアウォールのイベントが発生することもありますが (アプリケーションの各動作ごとに異なるイベントが発生します)、1つのアプリケーション ルール内で、それらの動作すべてに対応する条件を設定する必要があります。たとえば、メールクライアントがメールを送信したり、受信したりすると、2種類のイベントが発生しますが、どちらの動作も、このクライアントのアプリケーションルールで処理する必要があります。
- Webブラウザやメールの使用、およびファイルとプリンタの共有を許可してください。
- ネットワーク構築に関する専門知識がない場合は、デフォルトの ICMP 設定、グローバル ルール、およびアプリケーション ルールは変更しないことを推奨します。
- 可能な限り、グローバルルールではなくアプリケーションルールを作成することを推奨します。
- 接続先が 2カ所設定されているポリシーでは、「**対話型**」モードは使用しないでください。
- 大・中規模ネットワークやドメイン環境では、「**対話型**」モードは使用しないでください。「**対話型**」モードは、ワークグループ環境にある、非常に小規模なネットワーク (クライアント数 10台までなど) 上のスタンドアロン コンピュータでファイアウォールのルールを作成する際に使用できます。

5.4 2種類のファイアウォール接続先の設定を行う

「1種類の設定 (固定マシン用)」オプションは、デスクトップなど、常に同一のネットワークに接続されているコンピュータを対象にしています。「2種類の設定 (モバイル PC 用)」は、社内や社外など、使う場所に応じて異なるファイアウォールの設定を使い分ける場合に選択してください。「2種類の設定 (モバイル PC 用)」は、モバイル PC に適しています。

「2種類の設定 (モバイル PC 用)」を選択した場合は、プライマリロケーションとセカンダリロケーションの環境設定オプションを次のように設定することを推奨します。

- 社内ネットワークなど、管理対象ネットワークをプライマリロケーションに指定し、社外など、管理対象外の場所をセカンダリロケーションに指定します。
- プライマリロケーションへの接続はオープン性を高め、セカンダリロケーションへの接続は、より厳しく制限します。
- プライマリロケーションの検出オプションを設定する場合、大規模で複雑なネットワークに対しては DNS 参照を使用し、小規模でシンプルなネットワークに対してはゲートウェイの MAC アドレスを使用することを推奨します。DNS 参照を使用した検出には、DNSサーバーが必要となりますが、通常、ゲートウェイを使用した検出よりもメンテナンスが簡単です。ゲートウェイ検出に使用しているハードウェアで問題が発生した場合は、MACアドレスの再構成が必要となり、ハードウェアの構成に関する問題が解決するまで、セカンダリロケーションの設定内容が誤って各コンピュータに送信される恐れがあります。

- DNS 検出を使用する場合は、ご使用の DNS サーバーに、localhost の IP アドレス (別名ループバックアドレス (127.x.x.x)) に対する DNS エントリを一意の名前で追加することを推奨します。このように設定することで、接続する他のネットワークが、プライマリロケーションのネットワークとして誤って検出されることがほぼなくなります。
- 「ファイアウォールの詳細ポリシー」の「**全般**」タブの「**コンピュータの接続先と設定内容**」で、コンピュータに適用するファイアウォールの設定内容を選択します。適用する設定が、コンピュータの接続先に依存するよう設定する場合は、「**検出された場所に応じた設定内容**」オプションを選択してください。接続先に関係なく、プライマリロケーション用またはセカンダリロケーション用の設定内容を適用する場合は、該当するオプションを選択してください。

⚠ **注意:** セカンダリロケーションの設定でローカルサブネット ルールを使用する場合は、十分な注意が必要です。社外で使用するモバイル PC の場合、不明なサブネットに接続することがあります。この場合、セカンダリロケーションに対するファイアウォール ルールで、アドレスとしてローカルサブネットを使用するものがあると、不明なトラフィックが許可されてしまう恐れがあります。

5.5 ファイアウォール ポリシーを適用する

社内ネットワークを通過する、すべてのトラフィックを監視できるポリシーをエンドポイントコンピュータに展開します。トラフィックの状態はファイアウォールのイベントビューアに表示されます。この情報を利用して基本となるポリシーを設定します。

Sophos Client Firewall は段階的にネットワーク上に展開してください。つまり、1グループずつ Sophos Client Firewall をインストールしてください。そうすることで、インストールの初期段階に起こる急激なネットワークトラフィックの増加を防ぐことができます。

⚠ **注意:** 設定内容を十分に確認・テストするまで、ネットワーク全体にはインストールしないでください。

1. 社内ネットワーク上のさまざまな役割に対応する、テスト用コンピュータのグループに Sophos Client Firewall をインストールします。
2. ファイアウォールポリシーの「**規定で許可**」オプションを選択し、共通のトラフィック、アプリケーション、およびプロセスの検出のみを行い、ブロックは行わないように設定してテスト用グループに適用します。

   a) 新しいファイアウォールポリシーを作成します。Enterprise Console の「**ポリシー**」ペインで、「**ファイアウォール**」を右クリックし、「**ポリシーの作成**」を選択します。ポリシー名を入力し、ダブルクリックします。

   「**ファイアウォール ポリシー**」ウィザードが表示されます。

   b) ウィザードを使用するには「**次へ**」をクリックします。手動でポリシーを構成するには「**ファイアウォールの詳細ポリシー**」をクリックします。

   - ウィザードを使用する場合: 「**次へ**」をクリックします。「**1種類の設定**」を選択し、「**次へ**」をクリックします。「**監視する**」を選択し、「**次へ**」をクリックします。そして、もう一度「**次へ**」をクリックし、「**完了**」をクリックします。
   - 「**ファイアウォールの詳細ポリシー**」オプションを使用する場合:「**ファイアウォール ポリシー**」ダイアログボックスで、「**プライマリ ロケーション**」の横の「**環境**

設定」をクリックします。「**全般**」タブで、動作モードを「**規定で許可**」に設定します。「**OK**」をクリックし、続けてもう一度「**OK**」をクリックします。

c) テスト用グループに新しいファイアウォールのポリシーを適用します。

3. 「ファイアウォール - イベントビューア」を使用して、使用中のトラフィック、アプリケーションおよびプロセスを表示してください。イベントビューアを使用して、レポートされたトラフィック、アプリケーションおよびプロセスを許可/ブロックするルールを容易に作成することができます。イベントビューアを開くには、「**イベント** > **ファイアウォールのイベント**」をクリックします。
4. ファイアウォールのイベントを一定期間 (例: 2週間以上) 監視した後、ポリシーを作成します。

   a) イベントビューアからルールを作成します。イベントからルールを作成するには、対象のイベントを右クリックします。ファイアウォールのルールの作成について、詳細は Sophos Enterprise Console ヘルプの「**ポリシーの設定** > **ファイアウォールポリシー**」というセクションを参照してください。

   b) ポリシーにセキュリティ上の問題がないことを確認します (一部のユーザーに必要以上のアクセス権があるなど)。

   c) 異なる設定が必要な場合は、グループを分割し、それぞれ、必要なポリシーとルールを作成します。

5. イベントビューアで作成したルールの内容を確認してください。1種類のアプリケーションが原因で複数のファイアウォールのイベントが発生することもありますが (アプリケーションの各動作ごとに異なるイベントが発生します)、1つのアプリケーション ルール内で、それらの動作すべてに対応する条件を設定する必要があります。たとえば、メールクライアントがメールを送信したり、受信したりすると、2種類のイベントが発生しますが、どちらの動作も、このクライアントのアプリケーションルールで処理する必要があります。
6. 残りのネットワークを管理しやすいグループに分割します。営業用ワークステーション、IT 管理者用ワークステーションなど、ネットワークでのさまざまな役割ごとにグループとしてまとめます。
7. すべての種類のファイアウォールのイベントに対してルールを作成したら (どのルールにも一致しないファイアウォールのイベントが発生しなくなったら)、作成したルールからポリシーを作成し、必要に応じて、それらのポリシーを適用します。ネットワークに接続されているコンピュータの台数が多い場合は、1グループずつ Sophos Client Firewall をインストールしていってください。
8. ルールをテストした後は、ポリシーのモードを「**規定でブロック**」に変更します。変更しない場合、コンピュータに保護が提供されません。

ファイアウォールの設定について、詳細は Sophos Enterprise Console ヘルプの「**ポリシーの設定** > **ファイアウォールポリシー**」というセクションを参照してください。

注: きわめて小規模なネットワークや、Windows 7 以前が稼働しているスタンドアロン コンピュータの場合は、ネットワークのトラフィックを監視し、ファイアウォールのイベントビューアを使ってルールを作成する代わりに、Sophos Client Firewall をテスト用コンピュータにインストールして「**対話型**」モードで設定を行うこともできます。この場合、Web ブラウザなど、できるだけ多くのネットワーク上で使用するアプリケーションを実行します。このプロセスで確立したルールを含むファイアウォールの環境設定をインポート・編集します。詳細は、Sophos Endpoint Security and Controlヘルプを参照してください。

6 アプリケーション コントロール ポリシーの設定

6.1 設定にあたって

アプリケーションコントロールポリシーは、コンピュータでブロック/許可するアプリケーションを指定します。アプリケーション コントロール ポリシーを設定する際は、次の点に注意してください。

- 「**検出するが、実行は許可する**」オプションを指定して、管理対象アプリケーションの検出のみを行い、ブロックは行わないようにします。はじめに、レポートのみ受信することをポリシーで指定することで、ネットワーク全体のアプリケーション使用の全容を把握することができます。
- 「アプリケーション コントロール - イベントビューア」を使用して、社内のアプリケーション使用を監査します。イベントビューアを開くには、「**イベント** > **アプリケーション コントロールのイベント**」をクリックします。
- 「レポートマネージャ」を使用して、コンピュータまたはユーザーごとのアプリケーション コントロールのイベントの傾向に関するレポートを作成してください。
- 「今後ソフォスが追加するアプリケーションすべて」オプションを指定して、今後ソフォスによって追加される特定のタイプの新規アプリケーションすべての使用をブロックすることができます。これによって、ポリシーを頻繁に更新する必要がなくなります。たとえば、現在、すべてのインスタントメッセージング (IM) アプリケーションをブロックしている場合、今後追加される同タイプのアプリケーションすべてをブロックすることを指定できます。

6.2 アプリケーション コントロール ポリシーを適用する

デフォルトで、すべてのアプリケーションおよびアプリケーションのタイプは許可されています。アプリケーション コントロールは、次の手順で導入することを推奨します。

1. どのアプリケーションを管理の対象にするか決定します。
2. オンアクセス検索を有効に設定し、「**検出するが、実行は許可する**」オプションを指定して、管理対象アプリケーションの検出のみを行い、ブロックは行わないようにします。

   この時点で、社内ネットワーク全体に対して設定されているアプリケーション コントロール ポリシーは 1つです。
3. 「アプリケーション コントロール - イベントビューア」を使用して、使用中のアプリケーションを表示し、ブロックするアプリケーションやアプリケーションのタイプを決定します。イベントビューアを開くには、「**イベント** > **アプリケーション コントロールのイベント**」をクリックします。

4. コンピュータのグループごとに、アプリケーションへのアクセスを許可するには、グループごとに異なるポリシーを作成します。たとえば、社内に設置されているデスクトップコンピュータに対しては、VoIP の使用を許可せず、社外で使用するモバイルコンピュータに対しては、使用を許可することなどができます。
5. ブロックするアプリケーションやアプリケーションのタイプを決定し、「ブロック」リストに移動します。
6. 「**検出するが、実行は許可する**」オプションを選択から外して、検出された管理対象アプリケーションをブロックするようポリシーを設定します。

このように導入することで、多数の警告が発生したり、必要なアプリケーションがブロックされることを防ぎます。アプリケーション コントロール ポリシーの設定について、詳細は Sophos Enterprise Console ヘルプを参照してください。

注: パッチ評価で使用される CScript.exe をブロックするように Application Control を設定することもできます。アプリケーション コントロールとパッチ評価の両方を使用する場合は、「**プログラミング/スクリプティングツール**」カテゴリで「**Microsoft WSH CScript**」をブロックしないようにしてください。デフォルトで、プログラミング/スクリプティングツールの使用は許可されています。

7 データコントロール ポリシーの設定

7.1 データコントロール ポリシーの定義

データコントロール ポリシーを使用して、コンピュータから機密情報を誤って転送することに伴うリスクを管理することができます。

企業ごとに、機密情報として扱われるデータに違いはありますが、一般的な例は次のとおりです。

- 個人を特定できる情報を含む顧客記録。
- クレジットカード番号などの財務関連情報。
- 機密文書。

データコントロール ポリシーを有効にすると、データが転送される可能性の高いポイントでのユーザーのアクションが監視されます。

- ストレージデバイス (リムーバブル ストレージ デバイス、光学メディアドライブ、フロッピー ディスク ドライブなど) へのファイル転送。
- アプリケーション (社内標準ブラウザ、メールクライアント、インスタント メッセージング (IM) クライアントなど) へのファイルのアップロード。

データコントロールのルールは、次の 3つの要素から構成されます。

- 一致するアイテム: ファイルに含まれるデータ、ファイルタイプ、ファイル名などのオプションがあります。
- 監視するポイント: ストレージデバイスのタイプやアプリケーションなどがあります。
- 実行するアクション: 「ファイル転送を許可し、イベントをログに記録する」(監視モード)、「ユーザーの同意で転送を許可し、イベントをログに記録する」(対話型モード)、および「転送をブロックし、イベントをログに記録する」(制限モード) などがあります。

たとえば、スプレッドシートの Internet Explorer を使ったアップロードをログしたり、ユーザーの同意後、顧客住所を DVD に転送することを許可するよう、データコントロールのルールを設定できます。

データの内容に基づいて機密データを定義するのは複雑な作業です。この作業は、ソフォスが作成した機密データの定義ライブラリ (コンテンツ コントロール リスト) を利用することで簡略化されます。このライブラリは、個人情報や財務関情報の多様なデータ形式に対応しており、ソフォスによって最新の状態に保たれます。随時、カスタム コンテンツ コントロール リストを作成することもできます。

ソフォス設定の他のポリシーと同様、データコントロール ポリシーは、社内ネットワークから切り離されたコンピュータにも引き続き適用されます。

7.2 設定にあたって

データコントロール ポリシーを設定する際は、次の点に注意してください。

- 「**ファイル転送を許可し、イベントをログに記録する**」アクションを指定して、管理対象データの検出のみを行い、ブロックは行わないようにします。はじめに、レポートのみ受信することをポリシーで指定することで、ネットワーク全体のデータ使用の全容を把握することができます。
- 機密データを含む可能性のある文書を転送するリスクについて、ユーザーに警告する場合は、「**ユーザーの同意で転送を許可し、イベントをログに記録する**」アクションを指定します。この方法により、IT 部門に過大な負荷をかけることなく、データ流出リスクを削減することができます。
- 各ルールで指定されているアクション実行のしきい値となる機密情報の量は、コンテンツルールにある「データ量」で設定します。たとえば、文書内に住所が最低 1件含まれているか検索するルールは、最低50件含まれているか検索するルールより、より多くのデータコントロールのイベントを生成します。

  注: ソフォスでは、各コンテンツ コントロール リストに対して、デフォルトのデータ量を指定しています。

- 「データコントロール - イベントビューア」を使用して、イベントをフィルタですばやく抽出し、調査してください。データコントロールのイベントおよび動作状況はすべて Enterprise Console に一括ログが出力されます。イベントビューアを開くには、「**イベント** > **データコントロールのイベント**」をクリックします。
- 「レポートマネージャ」を使用して、ルール、コンピュータまたはユーザーごとのデータコントロールのイベントの傾向に関するレポートを作成してください。
- デスクトップメッセージの送信を有効にして、アクション実行時に表示するユーザー向けのメッセージを作成してください。たとえば、データセキュリティに関する社内ポリシードキュメントへのリンクを表示することができます。
- データコントロールのルールが適切であるか判断するために詳細な情報を取得する場合は、ログレベルを「詳細」に設定してください。当該のルールの評価を終了した後は、ログレベルを「通常」に設定し直してください。

  注: 「詳細」ログの設定は、各コンピュータで行う必要があります。生成されたログはすべて、各コンピュータのローカルのデータコントロールログに保存されます。ログレベルが「詳細」の場合、ルールで指定されているデータに一致する、各ファイル内の文字列すべてがログされます。ログに記録された詳細情報は、データコントロールのイベントを発生させる原因となった文章内の用語や文字列を判断するために使用することができます。

7.3 データコントロール ポリシーを適用する

デフォルトで、データコントロールは無効になっています。また、ストレージデバイスやアプリケーションへのファイル転送を監視・制限するルールも指定されていません。データコントロールは、次の手順で導入することを推奨します。

1. コンピュータにおけるデータコントロールの動作の説明を参照してください。

   - **ストレージデバイス:** データコントロール機能は、Windows エクスプローラを使って監視対象ストレージデバイスにコピーされるすべてのファイルをブロックします (Windows のデスクトップでファイルをコピーした場合も同様です)。ただし、Microsoft Word など、アプリケーションから直接ファイルを保存した場合や、コマンドプロンプトでファイルを転送した場合は、ブロックされません。

     管理対象ストレージデバイスへのファイル転送を、すべて Windows エクスプローラを使って実行させるようにするには、「ユーザーの同意で転送を許可し、イベントをログに記録する」アクション、または「転送をブロックし、イベントをログに記録する」アクションを利用します。どちらの場合でも、アプリケーションから直接ファイルを保存しようとしたり、コマンドプロンプトでファイルを転送しようとすると、データコントロール機能でブロックされます。そして、Windows エクスプローラを使ってファイル転送を行うよう、デスクトップ警告が表示されます。

     データコントロール ポリシーで、「ファイル転送を許可し、イベントをログに記録する」アクションに関するルールのみが設定されている場合は、アプリケーションで直接ファイルを保存しようとしたり、コマンドプロンプトからファイルを転送しようとしても、ファイルはブロックされません。この設定では、ユーザーが制限なしでストレージデバイスを使うことができます。しかし、Windows エクスプローラを使ってファイル転送を行ったときのみ、データコントロールのイベントが記録されます。

     注: アプリケーションの監視はこの制限の対象ではありません。

   - **アプリケーション:** データコントロール機能は、監視対象アプリケーションにアップロードされるファイルやドキュメントに対して割り込みを実行します。ユーザーが実行するファイルのアップロードだけを監視するため、一部のシステムファイルの保存先は、データコントロールによる監視の対象から除外されています。検索が実行される/されないアプリケーションの動作やコンテンツについて、詳細は、データコントロールの対象となるアプリケーション動作やコンテンツ (p. 22) を参照してください。

     注: メールクライアントを監視している場合、データコントロール機能により、すべての添付ファイルに対して検索が実行されます。ただし、メールの内容は検索されません。メールの内容に対して検索を実行する必要がある場合は、Sophos Email Security and Data Protection 製品を使用してください。

2. 検索する情報の種類を選択後、ルールを作成してください。あらかじめ用意されているサンプルルールを活用して、データコントロール ポリシーを構成してください。

   重要: コンテンツ検索には過大な負荷が伴うことがあるので、コンテンツルールを作成する際にはそのことを考慮してください。作成したコンテンツルールを多数のコンピュータに適用する前に、ネットワークへの影響をテストすることが重要です。

   注: はじめてポリシーを作成する場合は、個人を特定する情報が文書内に多数存在するか検索することを推奨します。この条件を満たすルールはあらかじめサンプルとして用意されています。

3. データコントロールを有効に設定し、ルール内で「**ファイル転送を許可し、イベントをログに記録する**」アクションを指定して、管理対象データの検出のみを行い、ブロックは行わないようにします。

   重要: 各コンピュータに適用する前に、すべてのルールでこのアクションを指定しておくことを推奨します。これによって、ユーザーの生産性に影響を与えることなく、各ルールの効果を評価することができます。

4. 作成したデータコントロールポリシーを数台のコンピュータに限って適用します。これによって、生成されるイベントの解析が容易になります。
5. 「データコントロール-イベントビューア」を使用して、使用中のデータを表示したり、テスト設定に問題点がないか確認します (条件が絞り込まれていないため、予想以上のイベント数が生成されるなど)。イベントビューアを開くには、「**イベント>データコントロールのイベント**」をクリックします。
6. ポリシーをテストした後は、適宜、設定を調整し、残りの社内コンピュータに適用します。この際、次の操作を行うこともできます。
   - 必要に応じ、一部のルールに対するアクションを「**ユーザーの同意で転送を許可し、イベントをログに記録する**」や「**転送をブロックし、イベントをログに記録する**」に変更する。
   - グループごとに異なるポリシーを作成します。たとえば、人事部のコンピュータには、個人を特定できる情報へのアクセスを許可し、それ以外の部署のコンピュータに対しては、アクセスを禁止するように設定できます。

データ コントロール ポリシーの設定について、詳細は Sophos Enterprise Console ヘルプを参照してください。

7.4 データコントロールの対象となるアプリケーション動作やコンテンツ

次の表は、データコントロール機能が対応しているアプリケーションで検索が実行される/されないコンテンツや動作の一覧です。

データコントロール機能の制限について、確認されている内容の詳細は、ソフォス サポートデータベースの文章 63016 を参照してください。
(http://www.sophos.com/ja-jp/support/knowledgebase/63016.aspx)

アプリケーション	対象となる動作・コンテンツ
Web ブラウザ	**検索を実行:** ▪ ファイルのアップロード ▪ Web メールの添付ファイル ▪ Microsoft SharePoint でのアップロード **検索を実行しない:** ▪ Web メールのメッセージ内容 ▪ ブログのエントリ

アプリケーション	対象となる動作・コンテンツ
	▪ ファイルのダウンロード **注:** 稀にファイルのダウンロード時にも検索が実行されることがあります。
メールクライアント	**検索を実行:** ▪ メールの添付ファイル **検索を実行しない:** ▪ メールのメッセージ内容 ▪ 転送した添付ファイル ▪ Windows エクスプローラや Microsoft Office などのアプリケーションのメールを「送る」オプションを使って添付されたファイル ▪ Windowsエクスプローラの「このファイルを電子メールで送信する」オプションを使って添付されたファイル ▪ 1つのメールから別のメールにコピーした添付ファイル ▪ 保存した添付ファイル **注:** 稀にファイルの保存時にも検索が実行されることもあります。
インスタントメッセンジャー (IM クライアント)	**検索を実行:** ▪ ファイルの転送 **注:** ファイルに対して二度検索が実行されることがあります。一度目は、IMクライアントにアップロードしたとき、二度目は受信者が受け取ったときです。どちらの検索も送信元のコンピュータで実行されます。 **検索を実行しない:** ▪ IM メッセージの内容 ▪ 送信したファイル

8 デバイスコントロールポリシーの設定

8.1 設定にあたって

デバイスコントロール ポリシーは、コンピュータで使用を認証するストレージデバイスやネットワーク機器を指定します。デバイスコントロール ポリシーを設定する際は、次の点に注意してください。

- 「**デバイスを検出するが、ブロックしない**」オプションを指定して、管理対象デバイスの検出のみを行い、ブロックは行わないようにします。設定するには、まず、検出する各デバイスタイプのステータスを「**ブロック**」に指定します。このように指定されていないデバイスタイプに対して検索は実行されません。はじめに、レポートのみ受信することをポリシーで指定することで、ネットワーク全体のデバイス使用の全容を把握することができます。
- 「デバイスコントロール - イベントビューア」を使用して、ブロックされたイベントをフィルタですばやく抽出し、調査してください。イベントビューアを開くには、「**イベント** > **デバイスコントロールのイベント**」をクリックします。
- 「レポートマネージャ」を使用して、コンピュータまたはユーザーごとのデバイスコントロールのイベントの傾向に関するレポートを作成してください。
- 機密情報へのアクセスが許可されているユーザーのコンピュータに対しては、より厳格なアクセスコントロールを実施することもできます。
- デバイスのブロックを指定するポリシーを適用する前に、除外対象デバイスのリストを作成します。たとえば、デザイン部門のみに対して光学メディアドライブの使用を許可することを指定できます。
- 「セキュリティ搭載リムーバブルストレージデバイス」カテゴリを使用して、多種の対応ベンダの、ハードウェア暗号化機能を持つ USB ストレージ デバイスを自動認証することができます。対応しているベンダの一覧は、ソフォスWebサイトを参照してください。サポートされているセキュリティ搭載リムーバブルストレージデバイスの一覧は、ソフォス サポートデータベースの文章 63102 を参照してください。(http://www.sophos.com/ja-jp/support/knowledgebase/63102.aspx)
- デバイスコントロールポリシーにデバイスの除外を追加する際、「**コメント**」フィールドに、デバイスを除外する理由や、除外をリクエストしたユーザーの名前を入力してください。
- デスクトップメッセージの送信を有効にして、管理対象デバイスの検出時に表示するユーザー向けのメッセージを作成してください。たとえば、デバイスの使用に関する社内ポリシードキュメントへのリンクを表示することができます。
- コンピュータをネットワークから切り離したときに、ネットワークデバイス (Wi-Fi アダプタなど) が有効になるよう設定するには、ネットワークデバイスのアクセスレベルで、「**ブリッジ接続をブロックする**」オプションを選択します。

  注: 「ブリッジ接続をブロックする」モードでは、企業ネットワークと外部ネットワーク間のブリッジ接続におけるリスクを大幅に削減できます。ワイヤレスデバイス、モデムのどちらでも、「ブリッジ接続をブロックする」モードを利用できます。この動作モー

ドは、エンドポイントが物理的なネットワーク (通常、イーサネットで接続) に接続した際に、ワイヤレスアダプタかモデムのどちらかが無効になることで作動します。エンドポイントを物理的なネットワークから切り離すと、シームレスにワイヤレスアダプタやモデムは再度有効になります。

- ポリシーを適用する前に、ブロックするデバイスの設定が適切であることを確認してください。特に、Wi-Fiやネットワークデバイスに関しては、すべての使用ケースを考慮するようにしてください。

注意: ポリシーの変更は、Enterprise Console サーバーからネットワーク経由でコンピュータに適用されます。したがって、一度ネットワークが遮断されると、それ以降サーバーから送信される設定をコンピュータで受け入れられなくなるため、Enterprise Consoleからブロックを解除することはできません。

8.2 デバイスコントロール ポリシーを適用する

デフォルトで、デバイス コントロールは無効になっています。すべてのデバイスが許可されています。デバイスコントロールは、次の要領で導入することを推奨します。

1. 管理の対象にするデバイスを決めます。
2. デバイスコントロールを有効に設定し、「**デバイスを検出するが、ブロックしない**」オプションを指定して、管理対象デバイスの検出のみを行い、ブロックは行わないようにします。設定するには、まず、検出する各デバイスタイプのステータスを「**ブロック**」に指定します。このように指定されていないデバイスタイプに対して検索は実行されません。

   この時点で、社内ネットワーク全体に対して設定されているデバイスコントロールポリシーは 1つです。
3. 「デバイスコントロール-イベントビューア」を使用して、使用中のデバイスを表示し、ブロックするデバイスのタイプを決定します。イベントビューアを開くには、「**イベント > デバイスコントロールのイベント**」をクリックします。
4. コンピュータのグループごとに異なるデバイスへのアクセスを許可するには、グループ別にポリシーを作成します。たとえば、人事や経理部門のユーザーにはリムーバブルストレージ デバイスの使用を許可せず、IT や営業部門のユーザーには許可するように設定することができます。
5. 特定のデバイスやモデルがブロックされないように除外を指定できます。たとえば、デバイスとして特定の USB キー、モデルとしてソフトバンク 3G モデムすべて、などを指定できます。
6. ブロックするデバイスを決定し、ステータスを「**ブロック**」に変更します。一部のストレージデバイスに対しては、ステータスを「読み取り専用」に指定できます。
7. 「**デバイスを検出するが、ブロックしない**」オプションを選択から外して、検出された管理対象デバイスをブロックするようポリシーを設定します。

このように導入することで、多数の警告が発生したり、必要なデバイスがブロックされることを防ぎます。デバイス コントロール ポリシーの設定について、詳細は Sophos Enterprise Console ヘルプを参照してください。

9 タンパー プロテクション ポリシーの設定

9.1 タンパー プロテクション ポリシーについて

タンパー プロテクションは、ユーザー (専門知識のないローカルアドミニストレータなど) が、ソフォスのセキュリティソフトの設定を変更したり、無効化、またはアンインストールしたりすることを防止する機能です。タンパープロテクション用のパスワードを知らないユーザーは、これらの操作を行うことができません。

注: この機能は詳しい専門知識を持つユーザーから製品を保護するものではありません。また、検出を避けるためにオペレーティングシステムの動作を妨害するマルウェアから製品を保護するものでもありません。このタイプのマルウェアは、脅威検索や疑わしい動作検索のみで検出されます。詳細は、ウイルス対策および HIPS ポリシーの設定 (p. 8) を参照してください。

タンパー プロテクションを有効にし、タンパー プロテクションのパスワードを作成すると、パスワードが与えられていない ユーザーは、Sophos Endpoint Security and Control でオンアクセス検索や疑わしい動作の検知を再設定したり、タンパー プロテクションを無効にしたり、コントロールパネルから Sophos Endpoint Security and Control のコンポーネント (Sophos Anti-Virus、Sophos Client Firewall、Sophos AutoUpdate、Sophos Remote Management System など) をアンインストールしたりすることができなくなります。

タンパー プロテクション ポリシーを設定する際は、次の点に注意してください。

- 「タンパー プロテクション - イベントビューア」を使用して、タンパー プロテクション用パスワードの使用状況をチェックしたり、社内でセキュリティソフトを改変しようとする試みがないかをどうかを監視したりしてください。タンパープロテクションの認証に成功したイベント (認証済みユーザーによるタンパー プロテクションのオーバーライド)、およびソフォスのセキュリティソフト改変の試みに失敗したイベントの両方を表示できます。イベントビューアを開くには、「**イベント** > **タンパープロテクションのイベント**」をクリックします。

9.2 タンパー プロテクション ポリシーを適用する

デフォルトで、タンパー プロテクションは無効になっています。タンパー プロテクション ポリシーは、次の要領で導入することを推奨します。

1. タンパープロテクションを有効にして、タンパープロテクションの安全なパスワードを作成します。

   このパスワードは、ソフォスのセキュリティソフトの再設定、無効化、アンインストールを、認証済みエンドポイントユーザーのみに許可します。

   注: SophosUser および SophosPowerUser グループのメンバーは、タンパー プロテクション機能による影響を受けません。タンパープロテクションを有効にした場合でも、これらのユーザーは、タンパープロテクションのパスワードを入力せずに、通常、実行を許可されているタスクすべてを実行できます。

2. タンパー プロテクションをグループごとに有効/無効にしたり、タンパー プロテクションのパスワードをグループごとに設定する場合は、各グループに対して個別のポリシーを作成してください。

タンパー プロテクション ポリシーの設定について、詳細は Sophos Enterprise Console ヘルプを参照してください。

10 パッチポリシーの設定

注: この機能はすべてのライセンスには含まれていません。利用するには追加購入が必要となります。詳細は、https://www.sophos.com/ja-jp/products/endpoint-antivirus/how-to-buy.aspx を参照してください。

10.1 パッチポリシーについて

パッチポリシーはコンピュータに最新のパッチが適用されているかどうかを確認するポリシーです。

SophosLabs が定義する緊急度から、最も深刻なセキュリティパッチがどれであるかがわかるため、緊急性の高い問題にすばやく対処できます。最新の攻撃情報をもとに算出しているため、SophosLabs が指定するパッチの緊急度は他のベンダーによる深刻度評価と異なる場合があります。

パッチポリシーを設定する際は、パッチ評価のイベントビューアで、社内ネットワーク上にパッチが適用されていないコンピュータがないかどうかをチェックしてください。セキュリティパッチやパッチ評価の結果に関する情報が表示されます。パッチの適用状況は、パッチポリシーでパッチ評価を有効にした後、コンピュータごと、グループごと、または脅威ごとに表示できます。イベントビューアを開くには、「**イベント** > **パッチコントロールのイベント**」をクリックします。

注: パッチ評価には CScript.exe が使用されますが、これはアプリケーション コントロールを使用してブロックすることができます。アプリケーション コントロールとパッチ評価の両方を使用する場合は、「**アプリケーション コントロール**」ポリシーの「**プログラミング/スクリプティングツール**」カテゴリで「**Microsoft WSH CScript**」をブロックしないようにしてください。デフォルトで、プログラミング/スクリプティングツールの使用はアプリケーション コントロールで許可されています。

10.2 パッチポリシーを適用する

はじめに、すべてのコンピュータに「デフォルト」というパッチポリシーが適用されます。パッチ評価はデフォルトのポリシーで無効に設定されています。

パッチ評価を有効化すると、コンピュータで評価が開始されます。これには数分かかることがあります。以後、ポリシーで設定されている頻度に基づいて (デフォルトで一日一回) 評価が行われます。

注: Enterprise Console がソフォスからパッチの評価データを一度もダウンロードしない状態でコンピュータの評価を実行した場合、パッチ評価のイベントビューアに結果は表示されません。ダウンロードには数時間かかることがあります。ダウンロードが完了したかどうかを確認するには、「**パッチ評価 - イベントビューア**」の「**パッチ情報**」フィールドを参照します。

パッチポリシーは、次の手順で導入することを推奨します。

1. 「コンピュータの保護ウィザード」を使用して、パッチエージェントを各コンピュータにインストールします。(ウィザードの「**機能の選択**」ページで、「**パッチ**」を選択します。)

   注: すでに Endpoint Security and Control を稼働していても、パッチエージェントがインストールされていない場合は、「コンピュータの保護 ウィザード」を実行してコンピュータを再保護する必要があります。

2. デフォルトのパッチポリシーでパッチ評価を有効にします。

   この時点で、社内ネットワーク全体に対して設定されているパッチポリシーは1つです。

3. パッチ評価のイベントビューアを使用し、パッチが未適用のコンピュータや最新のパッチがインストールされているコンピュータを表示します。イベントビューアを開くには、「**イベント** > **パッチコントロールのイベント**」をクリックします。

   注: 未適用のパッチは手動で各コンピュータにインストールする必要があります。

4. グループごとにパッチ評価を有効/無効にしたり、パッチ評価の実行間隔を設定したりする場合は、各グループに対して個別のポリシーを作成してください。

パッチポリシーの設定について、詳細は Sophos Enterprise Console ヘルプを参照してください。

11 Web コントロールポリシーの設定

注: この機能はすべてのライセンスには含まれていません。利用するには追加購入が必要となります。詳細は、https://www.sophos.com/ja-jp/products/endpoint-antivirus/how-to-buy.aspx を参照してください。

Web コントロール ポリシーはユーザーがブラウザで閲覧できる Web サイトを指定します。

デフォルトで、Web コントロールは無効になっているため、Enterprise Console の Web Protection 機能で制限されていない限り、すべての Web サイトにアクセスできます。「不適切な Web サイトのコントロール」または「高度な Web コントロール」のどちらかのポリシーを使用できます。操作方法は、この後のセクションを参照してください。

11.1 設定にあたって

Web コントロールには 2種類のポリシーがあります。1つは「不適切な Web サイトのコントロール」で、もう 1つは「高度な Web コントロール」です。推奨する設定内容は、どちらのポリシーを選択するかによって異なります。Web コントロール ポリシーを設定する際は次の点を考慮してください。

不適切な Web サイトのコントロール

- 各 Web サイトカテゴリに対するアクションを確認し、所属する組織やグループの要件に応じて調整してください。コンピュータのグループごとに、Web サイトへのアクセスを許可するには、各グループ個別のポリシーを作成します。たとえば、人事部のみに閲覧を許可することのある Facebook のような Web サイトは、これに該当します。
- ポリシーをエンドポイントコンピュータに適用する前に、除外する Web サイトの一覧を作成します。「**例外 Web サイト**」タブで、ポリシーから除外する Web サイトを手動で入力できます。たとえば、フィルタリングの必要がない複数のローカル Web アドレスや、許可するカテゴリ内の特定の Web サイトをブロックしたい場合などは、これに該当します。
- 「Web - イベントビューア」を使用して、イベントをフィルタですばやく抽出し、調査してください。イベントビューアを開くには、「**イベント** > **Web のイベント**」をクリックします。ここに表示される動作状況をもとに Web サイトのカテゴリの設定を調整します。

高度な Web コントロール

重要: 「高度な Web コントロール」を使用するには、Sophos Web Appliance または Security Management Appliance が必要です (どちらも国内未販売です)。

- アプライアンスの設定に関する全般的なガイドラインは、「Sophos Web Appliance 設定ガイド」(英語) および「Security Management Appliance 設定ガイド」(英語) を参照してください。アプライアンスのセットアップ ウィザードを使うと、組織内の環境に最も適した設定を選択できます。

- ユーザーの種類ごとに異なるポリシーを設定した方がよい場合もあります。詳細は、Web Appliance のオンライン製品ドキュメント (英語) を参照してください。

  Sophos Web Appliance のドキュメント (英語) は、次のサイトから入手可能です。
  http://wsa.sophos.com/docs/wsa/

- ポリシーをエンドポイントコンピュータに適用する前に、Web コントロール ポリシーの対象から除外する項目を確認します。たとえば、「Special Hours」機能を使用して、通常の就業時間外 (昼休みなど) における特定の Web サイトへのアクセスを一部またはすべて許可することができます。また、特定のユーザーのみに適用される「Additional Polices」を作成することもできます。このポリシーはデフォルトポリシーや「Special Hours」ポリシーの対象から除外されます。

- どのカテゴリにも該当しない Web サイトに対して Web Appliance でどのようなアクションを実行するかを検討します。デフォルトで、「**Web サイトのカテゴリを識別できない場合は、閲覧をブロックする**」チェックボックスは選択されて**いません**。つまり、カテゴリを識別できない場合、サイトの閲覧は許可されます。チェックボックスを選択すると、設定を無効に戻すまで、カテゴリを識別できない URL の閲覧がブロックされます。

詳細は、Sophos Enterprise Console および Sophos Web Appliance の製品ドキュメントを参照してください。

11.2 Web コントロール ポリシーを適用する

はじめに、どの Web フィルタを使用するかを決めます。Web フィルタには「不適切な Web サイトのコントロール」と「高度な Web コントロール」の 2種類があります。「高度な Web コントロール」を使用するには、Sophos Web Appliance または Security Management Appliance が必要です (どちらも国内未販売です)。

Web コントロール ポリシーの設定について、詳細は Sophos Enterprise Console ヘルプを参照してください。

11.2.1 「不適切な Web サイトのコントロール」ポリシーを適用する

「不適切な Web サイトのコントロール」は、Web コントロールの基本的なオプションで、14種類の基本的なカテゴリに基づいて設定を行うことができます。このオプションはユーザーの不適切な Web サイトの閲覧を防止するためのオプションです。Web コントロール ポリシーを導入する際は、次の点を考慮してください。特定の操作については、Enterprise Console のドキュメントを参照してください。

1. Web コントロール ポリシーが有効になっていることを確認します。
2. Web サイトの閲覧に関する適切な社内ポリシーがある場合は、それに応じて設定を変更し、不適切と思われるすべてのサイトの閲覧を防止します。
3. コンピュータのグループごとに異なる Web サイトへのアクセスを許可するには、グループ別にポリシーを作成します。
4. Web コントロールの対象となるグループ、および各グループのコンピュータに適用するポリシーの種類を選択します。
5. 各 Web サイトカテゴリに対するデフォルトのアクションを表示します。異なるアクションを適用する場合は、ドロップダウンリストから選択します。どのカテゴリの閲覧をブロック・許可するか、または閲覧した際に警告を表示するかを検討します。

6. フィルタリングの対象から除外する Web サイトを決めたら、「**許可する Web サイト**」リストまたは「**ブロックする Web サイト**」リストに追加します。

   注: ブロックリストと許可リストの間で重複や整合性のとれない項目がある場合は、常にブロックリストの項目が優先されます。たとえば、ブロックリストと許可リストの両方に同じ IP アドレスが指定された場合、そのWebサイトはブロックされます。さらに、ブロックリストにあるドメインのサブドメインが許可リストで指定された場合は、許可リストの設定は無視され、ドメインとそのサブドメインすべてがブロックされます。

7. Web コントロールのイベントビューアを使用し、フィルタリングの結果を確認します。イベントビューアを開くには、「**イベント > Web のイベント**」をクリックします。イベントビューアを使用し、Web のイベントを表示します。この結果に応じて設定を調整します。

詳細は、Enterprise Console の製品ドキュメントを参照してください。

11.2.2 「高度な Web コントロール」ポリシーを適用する

「高度な Web コントロール」では、すべての Web ポリシーが使用されます。全機能に対応した包括的な Web コントロール ポリシーを施行し、Web トラフィックに関する詳細なレポートを提供します。このオプションを利用するには、Sophos Web Appliance または Security Management Appliance が必要です (どちらも国内未販売です)。

1. アプライアンスのドキュメントの説明に従って、Sophos Web Appliance または Security Management Appliance を構成します。その際、「**Endpoint Web Control**」が有効になっていることを確認します。
2. Enterprise Console で Web コントロールが有効になっていることを確認します。
3. Web サイトの閲覧に関する適切な社内ポリシーがある場合は、それに応じて設定を変更し、不適切と思われるすべてのサイトの閲覧を防止します。
4. さまざまなユーザーのグループに対して異なる Web サイトへのアクセスを許可するには、ユーザーのグループごとに個別のポリシーを作成します。
5. 制御の対象となる Web サイトを選びます。ユーザーによる閲覧を防止するカテゴリ、アクセスを許可するカテゴリ、閲覧の際に警告を表示するカテゴリを決めます。
6. 制御の対象から除外する Web サイトを決め、アプライアンスの Local Site List に追加します。
7. 「高度な Web コントロール」では、任意で Sophos LiveConnect を使用できます。LiveConnect を使用するようにアプライアンスを設定すると、社内からネットワークに接続していない場合でも、ポリシーの更新内容が各ユーザーに適用され、ユーザーのコンピュータからレポートデータがアップロードされます。

詳細は、Sophos Enterprise Console および Sophos Web Appliance の製品ドキュメントを参照してください。

12 エクスプロイト対策ポリシーの設定

注: この機能はすべてのライセンスには含まれていません。利用するには追加購入が必要となります。詳細は、https://www.sophos.com/ja-jp/products/endpoint-antivirus/how-to-buy.aspx を参照してください。

エクスプロイト対策ポリシーでは、ランサムウェアや、マルウェアによるその他の形式のエクスプロイトからの防御レベルを設定します。

- ランサムウェアから文書ファイルを保護する (CryptoGuard)。
- Web ブラウザの重要な機能を保護する (セーフブラウジング)。
- エクスプロイトを防止する。Java アプリケーションなど、最もマルウェアに悪用されやすいアプリケーションを保護します。
- プロセス書き換え攻撃から防御する。
- 信頼できないフォルダから .DLL ファイルが読み込まれることを阻止する。
- CPU のブランチトレースから保護する。

12.1 推奨設定

エクスプロイト対策ポリシーでは、セキュリティソフトウェアを使用して、ランサムウェアや、マルウェアによるその他の形式のエクスプロイトからどのように防御するかを設定します。

注: デフォルトでは、すべてのエクスプロイト対策のオプションは有効になっています。

デフォルトの設定を使用することを推奨します。

12.2 エクスプロイト対策ポリシーを適用する

エクスプロイト対策ポリシーは、次のように適用することを推奨します。

1. デフォルトでは、すべてのエクスプロイト対策のオプションは有効になっています。デフォルトの設定を使用することを推奨します。設定を変更する前に、しばらくの間、エクスプロイト対策のイベントを監視する必要があります。
2. エクスプロイト対策のイベントを監視するには、エクスプロイト対策のイベントビューアを使用します。イベントビューアを開くには、「**イベント** > **エクスプロイト対策のイベント**」をクリックします。
3. 監視結果に基づいて、エクスプロイト対策ポリシーを修正します。たとえば、一部のアプリケーションをエクスプロイト防止の対象から除外することなどができます。詳細は、Sophos Enterprise Consoleヘルプの「**ポリシーの設定** > **エクスプロイト対策ポリシー**」のセクションを参照してください。

重要: 攻撃の対象になりやすいアプリケーションは、デフォルトで保護されます。エクスプロイト対策の対象からアプリケーションを除外する際は注意が必要です。除外を設定した場合でも、CryptoGuard およびセーフブラウジングによる保護は解除されません。

a) 新しいポリシーを作成するか、デフォルトのポリシーを変更します。

b) 作成したポリシーにセキュリティ上の問題がないか確認します。

c) 異なる設定が必要な場合は、グループを分割し、それぞれ必要なポリシーを作成します。

4. 必要に応じて、ポリシーを適用します。

エクスプロイト対策ポリシーの設定について、詳細は Sophos Enterprise Console ヘルプを参照してください。

13 検索の設定にあたって

次の検索オプションは「ウイルス対策および HIPS」ポリシーで設定します。検索オプションを設定する際は、次の点に注意してください。

- 可能な限り、デフォルト設定を使用してください。
- 可能な限り、個別のコンピュータではなく、Enterprise Console で検索を設定してください。
- 設定対象のコンピュータの役割 (クライアントマシン、サーバーなど）を考慮してください。

拡張子

オンアクセス検索に対する拡張子のオプションを開くには、「**ウイルス対策および HIPS ポリシー**」ダイアログボックスで、「**オンアクセス検索を有効にする**」の横の「**環境設定**」をクリックし、「**拡張子**」タブを開きます。

スケジュール検索の場合は、「**ウイルス対策および HIPS ポリシー**」ダイアログボックスの「**スケジュール検索**」の下にある「**拡張子・除外**」をクリックします。

- 通常、「**すべてのファイルを検索する**」オプションは必要ありません。また推奨もしません。代わりに、「**実行ファイルなど感染の可能性があるファイルのみを検索する**」オプションを選択します。ソフォスラボで解析済みの脅威が検索されます。すべてのファイルの検索は、テクニカルサポートのアドバイスを受けた場合のみに実行してください。

その他の検索オプション

オンアクセス検索に対する他の検索オプションを開くには、「**ウイルス対策および HIPS ポリシー**」ダイアログボックスで、「**オンアクセス検索を有効にする**」の横の「**環境設定**」をクリックします。

スケジュール検索の場合は、「**ウイルス対策および HIPS ポリシー**」ダイアログボックスの「**スケジュール検索**」の下にある検索の項目を選択し、「**編集**」をクリックします。「**スケジュール検索の設定**」ダイアログボックスで、「**環境設定**」をクリックします。

- 「**圧縮ファイル内を検索する**」オプションを選択すると検索スピードが低下しますが、この操作は通常必要ありません。圧縮ファイルのコンテンツにアクセスしようとすると、ファイルは自動的に検索されます。したがって、圧縮ファイルを頻繁に使用する場合を除き、このオプションは選択しないことを推奨します。
- コンピュータのシステムメモリの脅威スキャンを推奨します。システムメモリはオペレーティングシステムで使われます。オンアクセス検索が有効にしたまま、定期的にシステムメモリをバックグラウンド検索できます。また、スケジュール検索の一部としてシステムメモリの検索を実行することもできます。「**システムメモリを検索する**」オプションはデフォルトで有効になっています。

14 オンアクセス検索の使用

オンアクセス検索を使用する際は、次の点に注意してください。

- 可能な限り、デフォルト設定を使用してください。
- ソフトウェアを新規インストールした場合のみ、オンアクセス検索の「**読み取ったとき**」、「**書き込んだとき**」および「**ファイル名を変更したとき**」オプションは有効になっています。ソフトウェアをアップグレードした場合は、有効に設定する必要があります。
- 特定の暗号化ソフトがインストールされている場合、オンアクセス検索でウイルスが検出されないことがあります。コンピュータのスタートアッププロセスを変更し、オンアクセス検索が開始するとファイルが復号化されるように設定してください。暗号化ソフトがインストールされている環境でのウイルス対策および HIPS ポリシーの使用について、詳細はソフォスのサポートデータベースの文章 12790 を参照してください。(http://www.sophos.com/ja-jp/support/knowledgebase/12790.aspx)
- オンアクセス検索を選択しない場合は、各コンピュータでスケジュール検索を設定するようにしてください。詳細は、スケジュール検索の使用 (p. 37) を参照してください。

注意: オンアクセス検索を無効にすると、セキュリティリスクが高まることに注意してください。

15 スケジュール検索の使用

スケジュール検索を使用する際は、次の点に注意してください。

- 可能な限り、デフォルト設定を使用してください。
- スケジュール検索は、脅威のセキュリティ評価を行ったり、不要と思われるアプリケーションや管理対象アプリケーションの使用状況を評価するために使用してください。
- オンアクセス検索を選択しない場合は、各コンピュータでスケジュール検索を設定するようにしてください。このようなコンピュータを 1つのグループにまとめ、スケジュール検索を設定してください。
- スケジュール検索を設定する場合は、パフォーマンスに与える影響を考慮してください。たとえば、データベースに頻繁に読み取り、書き込みを行うサーバーを検索する場合は、パフォーマンスに与える影響を最小限に留めることのできる時間帯を選んでください。
- サーバーで実行されるタスクの種類を考慮してください。バックアップタスクがある場合は、バックアップを実行する時間帯にスケジュール検索を設定しないようにしてください。
- 定期的に検索を実行してください。午後 9時など、毎日、各コンピュータでスケジュール検索を実行するようにしてください。スケジュール検索は、すべてのコンピュータで、少なくとも毎週実行するようにしてください。
- 「**低いプライオリティで検索を実行する**」オプションを選択すると、Windows Vista 以降の OS では低いプライオリティでスケジュール検索を実行できます。このため、ユーザーが使うアプリケーションへの影響を最小限に抑えられます。このオプションは有効にすることを推奨しますが、無効にしているときに比べ、検索時間が長くなります。

16 オンデマンド検索の使用

オンデマンド検索を使用する際は、次の点に注意してください。

- オンデマンド検索は、手動で評価/クリーンアップすることが必要な場合に使用してください。

17 検索の対象から除外するアイテムの設定

検索の対象からアイテムを除外する方法は次のとおりです。

- 除外機能を使用して、特定のファイルタイプを検索の対象から除外します。
- 除外機能を使用して、ファイルやドライブなど、特定のアイテムを検索の対象から除外します。除外は、ドライブ (X: など)、ディレクトリ (X:\Program Files\Exchsrvr\ など)、またはファイル (X:\Program Files\SomeApp\SomeApp.exe など) レベルで指定できます。
- メディアドライブを頻繁に使用するユーザーに対しては、メディアドライブをオンアクセス検索から除外することを考慮してください。メディアドライブを使用すると、一時ファイルへの読み取り、書き込みが行われるため、そのたびに各ファイルが割り込み・検索され、検索スピードが低下します。
- ネットワークリソース上のリモートロケーションにあるファイルを検索しない場合は、「**リモートファイルを除外する**」オプションを指定してください。通常、すべてのコンピュータに対して、リモートファイルをアクセス時に検索することを推奨しますが、ファイルサーバー、または、サイズの大きいファイルや頻繁に変更されるファイルにリモートアクセスする場合などは、このオプションを選択してください。

注意: アイテムを検索から除外すると、セキュリティリスクが高まることに注意してください。

18 テクニカルサポート

ソフォス製品のテクニカルサポートは、次のような形でご提供しております。

- ユーザー コミュニティ サイト「Sophos Community」(英語) (community.sophos.com/) のご利用。さまざまな問題に関する情報を検索できます。
- ソフォス サポートデータベースのご利用。www.sophos.com/ja-jp/support.aspx
- 製品ドキュメントのダウンロード。 www.sophos.com/ja-jp/support/documentation.aspx
- オンラインでのお問い合わせ。 https://secure2.sophos.com/ja-jp/support/contact-support/support-query.aspx

19 利用条件

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™

commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant. Likewise, DOC software is compliant with the new US daylight savings rule passed by Congress as "The Energy Policy Act of 2005," which established new daylight savings times (DST) rules for the United States that expand DST as of March 2007. Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE™, TAO™, CIAO™, DAnCE™, CoSMIC™, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. This license grants no permission to call products or services derived from this source ACE™, TAO™, CIAO™, DAnCE™, or CoSMIC™, nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

If you have any suggestions, additions, comments, or questions, please let me know.

Douglas C. Schmidt

Apache

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License. A copy of the license agreement for any such included software can be found at http://www.apache.org/licenses/LICENSE-2.0

Boost Software License

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Common Public License

The Sophos software that is referenced in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is

distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.co.jp or via the web at https://www.sophos.com/ja-jp/support/contact-support.aspx. A copy of the license agreement for any such included software can be found at http://opensource.org/licenses/cpl1.0.php

ConvertUTF

Copyright 2001–2004 Unicode, Inc.

This source code is provided as is by Unicode, Inc. No claims are made as to fitness for any particular purpose. No warranties of any kind are expressed or implied. The recipient agrees to determine applicability of information provided. If this file has been purchased on magnetic or optical media from Unicode, Inc., the sole remedy for any claim will be exchange of defective media within 90 days of receipt.

Unicode, Inc. hereby grants the right to freely use the information supplied in this file in the creation of products supporting the Unicode Standard, and to make copies of this file in any form for internal or external distribution as long as this notice remains attached.

Loki

The MIT License (MIT)

Copyright © 2001 by Andrei Alexandrescu

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Microsoft Public License (MS-PL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

   The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

   A "contribution" is the original software, or any additions or changes to the software.

   A "contributor" is any person that distributes its contribution under this license.

   "Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

   (A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

   (B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

   (A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

   (B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

   (C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

   (D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

   (E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

A copy of the MS-PL terms can be found at https://opensource.org/licenses/MS-PL.

OpenSSL Cryptography and SSL/TLS Toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998–2016 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

   The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

WilsonORMapper

Copyright © 2007, Paul Wilson

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Windows Template Library (WTL)

Copyright © Microsoft Corporation. All rights reserved.

The use and distribution terms for this software are covered by the Common Public License. Source code for this component is available here: https://sourceforge.net/projects/wtl/files/

zlib data compression library

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu