

SOPHOS

Security made simple.

Sophos Enterprise Console アドバンススタートアッ プガイド

分散型インストール

製品バージョン: 5.5



目次

1 このガイドについて.....	4
2 インストールにあたって.....	5
2.1 Enterprise Console のインストールについて.....	5
2.2 データベースのセキュリティについて.....	7
2.3 コンピュータのグループについて.....	8
2.4 セキュリティポリシーについて.....	8
2.5 ネットワーク上のコンピュータの検出について.....	8
2.6 コンピュータの保護について.....	8
3 システム要件.....	9
3.1 ハードウェアおよび OS.....	9
3.2 マイクロソフトのシステムソフトウェア.....	9
3.3 ポート要件.....	10
4 必要なアカウント.....	11
4.1 データベース用アカウント.....	11
4.2 Update Manager アカウント.....	11
5 Enterprise Console コンポーネントのインストール先について.....	13
5.1 管理データベースを別のサーバーにインストールする方法.....	14
5.2 追加のアップデートマネージャを別のサーバーにインストールする方法.....	14
6 シナリオ 1: 管理データベースを別のサーバーにインストールする方法.....	16
6.1 インストーラのダウンロード.....	16
6.2 SEC データベースのインストール.....	16
6.3 SEC のインストール - 管理コンソール、管理サーバー、アップデートマネー ジャ.....	17
6.4 追加の SEC 管理コンソールのインストール.....	18
6.5 セキュリティソフトのダウンロード.....	19
7 シナリオ 2: 追加のアップデートマネージャを別のサーバーにインストールする方法	23
7.1 インストーラのダウンロード.....	23
7.2 SEC のインストール - すべてのコンポーネント.....	24
7.3 追加の SEC 管理コンソールのインストール.....	25
7.4 追加のアップデートマネージャのインストール.....	26
7.5 セキュリティソフトのダウンロード.....	27
8 セキュリティソフトの Web サーバーへの配置.....	35

9	コンピュータグループの作成.....	36
10	セキュリティポリシーの設定.....	37
10.1	デフォルトポリシー.....	37
10.2	ファイアウォールポリシーの設定.....	37
10.3	ポリシーの作成・編集.....	38
10.4	グループへのポリシーの適用.....	38
11	コンピュータの検出.....	39
12	コンピュータの保護の事前準備.....	40
12.1	他社製セキュリティ対策ソフトを削除する準備.....	40
12.2	ソフトウェアをインストールできるアカウントがあることの確認.....	40
12.3	ウイルス対策ソフトをインストールする準備.....	41
13	コンピュータの保護.....	42
13.1	自動での Windows コンピュータの保護.....	42
13.2	手動での Windows コンピュータや Mac の保護.....	43
13.3	Linux または UNIX コンピュータの保護.....	43
14	ネットワークのセキュリティの状態の確認.....	44
15	スタンドアロン コンピュータの保護.....	45
15.1	スタンドアロン コンピュータのユーザーへの必要な情報の送信.....	45
16	テクニカルサポート.....	46
17	利用条件.....	47

1 このガイドについて

このガイドでは、構成が複雑なネットワークや、クライアント数が 1000 台を超える大規模なネットワークに、ソフォスのセキュリティソフトを新規インストールする方法について説明します。対象となるオペレーティングシステムは、Windows および Mac です。

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。

クライアント数が 1000 台未満の小規模な Windows および Mac ネットワークへインストールする場合は、このガイドではなく、「**Sophos Enterprise Console クイック スタート アップガイド**」をご覧ください。

Linux または UNIX コンピュータにインストールするには、このガイド以外に「**Enterprise Console スタートアップガイド Linux/UNIX 版**」もご覧ください。

アップグレードを行う場合は、「**Sophos Enterprise Console アップグレードガイド**」をご覧ください。

Sophos Enterprise Console のドキュメントは次のサイトから入手可能です。
www.sophos.com/ja-jp/support/documentation/enterprise-console.aspx

2 インストールにあたって

お使いのコンピュータを保護する主なステップは次のとおりです。

1. Sophos Enterprise Console をインストールする。
2. セキュリティソフトを社内ネットワーク上のフォルダ (各クライアントマシンに一斉配信できる場所) にダウンロードする。
3. 任意で Web サーバー上にセキュリティソフトを配置する。
4. コンピュータのグループを作成する。
5. セキュリティポリシーを各グループに対して設定する。
6. ネットワーク上のコンピュータを検索し、グループに配置する。
7. コンピュータを保護する。
8. ネットワークのセキュリティの状態を確認する。
9. 社内ネットワークに常に接続していないコンピュータを保護する。

注: Active Directory をお使いの場合は、一部のステップを自動的に処理できます。

このセクションでは、上記の各項目で選択する設定内容について説明します。

2.1 Enterprise Console のインストールについて

Sophos Enterprise Console (SEC) は、各コンピュータにセキュリティ対策ソフトを集中的にインストールし、インストールしたソフトウェアを管理します。

Enterprise Console には次の 4つのコンポーネントが含まれています。

管理コンソール	コンピュータの保護や管理を行います。
管理サーバー	アップデートや通信を処理します。
データベース	ネットワーク上のコンピュータに関するデータを保存します。
アップデートマネージャ	ソフォス製品やアップデート版をソフォスのサーバーからダウンロードし、各コンピュータが接続し、アップデートする社内サーバーに取り込みます。

管理コンソール

別のサーバーに追加のリモート管理コンソールのインスタンスをインストールすると、ネットワーク上のコンピュータを効率よく管理できます。この操作は、各ロールに対して管理コンソールへの管理権限を設定したり、IT 資産をサブ管理サイトに分割する場合に関連して行うものです。

- **ロールベースの管理:** 管理コンソールへの管理権限を各ロール (役割) ごとに設定するには、まず、ロールを作成して権限を追加します。そして、Windows のユーザーやグループ

ブを作成したロールに追加します。たとえば、ヘルプデスク担当者は、コンピュータのアップデートやクリーンアップを実行できますが、ポリシー設定の権限は与えられていません。ポリシーの設定は、管理者ロールの役割です。

- **サブ管理サイト:**各コンピュータやグループに対して、ユーザーが実行できる操作に制限を設けることができます。社内のIT資産はサブ管理サイトとして分割し、管理コンソールのコンピュータのグループを追加できます。そして、Windowsのユーザーやグループをサブ管理サイトに追加し、サブ管理サイトへのアクセスをコントロールできます。「デフォルト」サブ管理サイトには、管理コンソールで作成したすべてのグループと「**グループ外のコンピュータ**」が含まれます。

このガイドでは、追加の管理コンソールをインストールする方法について説明します。ロールベースの管理とサブ管理サイトの作成について、詳細は次の文章を参照してください。
www.sophos.com/ja-jp/support/knowledgebase/63556.aspx

データベース

データベースを別のサーバーに追加インストールする場合、次のような理由があります。

- データベースの容量が足りない。
- SQL Server 専用のサーバーを使っている。
- データベース処理にかかる負荷を複数のサーバーに分散させたい。

このガイドでは、データベースを他の Enterprise Console コンポーネントと同じサーバーにインストールする方法、および別の専用のデータベースサーバーにインストールする方法について説明します。

注: データベースをスクリプトを使用して安全なサーバーにインストールしたり、クラスタ化された SQL サーバー環境にインストールしたりする必要がある場合は、次の文章を参照してください。
www.sophos.com/ja-jp/support/knowledgebase/33980.aspx

重要: ソフォス監査データベース「**SophosSecurity**」は、ソフォス監査機能を使用しない場合でも、他の Enterprise Console のデータベースと共に稼働させておく必要があります。このデータベースは、監査イベントのログ記録の他、強化されたアクセスコントロール機能のためにも必要です。

アップデートマネージャ

アップデートマネージャでは、各エンドポイントに展開するソフトウェアを配置する共有フォルダを作成できます。保護されている各コンピュータは、この共有フォルダにアクセスし自動的にアップデートを実行します。アップデートマネージャは、必ず、Enterprise Console の一部としてインストールされます。デフォルトで、エンドポイント用ソフトウェアおよびアップデート版が、SophosUpdate という UNC シェアに配置されます。なお、大規模なネットワークの場合、他のサーバーにアップデートマネージャを追加インストールし、追加の共有フォルダを作成して、ソフトウェアを複数の場所に取り込んで展開することもできます。

一般に、ネットワーク上のクライアントコンピュータ 25,000台につき、追加のアップデートマネージャ1つをインストールする必要があります。また、リモートの場所ごとに、追加のアップデートマネージャ1つをインストールすることも推奨します。これによって、リモートの場所にあるエンドポイントコンピュータも、それぞれローカルのアップデート元からアップデートすることになるので、バンド幅を節減できます。また、リモートの場所にあ

るアップデート元との接続が途絶えてアップデートが正常に終了しない、という問題も回避することができます。

UNC パスで指定したアップデート用共有フォルダは、専用のファイルサーバーにある場合を除き、最高 1,000 台のコンピュータで使用するようにしてください。一方、アップデート元として Web の場所を指定した場合は、約 10,000 台のコンピュータで使用できます。

2.2 データベースのセキュリティについて

データベースを監査する

Enterprise Console データベースに内蔵の保護機能の他に、SQL Server インスタンスに対して追加の保護レイヤーを設定し (未設定の場合)、ユーザーアクティビティや SQL Server への変更を監査することを推奨します。

たとえば、SQL Server 2008 Enterprise Edition を使用している場合は、SQL Server Audit 機能を使用できます。旧バージョンの SQL Server では、内蔵のトレース機能を使用して、ログインの監査、トリガーを使用した監査、およびイベントの監査を実行できます。

SQL Server システムでのアクティビティおよび変更を監査するために使用できる機能の詳細は、該当するバージョンの SQL Server ドキュメントを参照してください。例:

- [SQL Server Audit \(データベース エンジン\)](#)
- [監査 \(データベース エンジン\)、SQL Server 2008 R2](#)
- [SQL Server 2008 の監査機能 \(英語\)](#)
- [監査 \(データベース エンジン\)、SQL Server 2008](#)

データベースへの接続を暗号化する

クライアントと Enterprise Console データベースの接続を暗号化することを強く推奨します。詳細は、次の SQL Server のドキュメントを参照してください。

- [データベース エンジンへの暗号化接続の有効化 \(SQL Server 構成マネージャー\)](#)
- [SQL Server 2008 R2 への暗号化接続](#)
- [Microsoft 管理コンソールで SQL Server インスタンス用に SSL 暗号化を有効にする方法](#)

データベースのバックアップへのアクセスをコントロールする

データベースのバックアップやコピーにはアクセス制限を設定し、適切なアクセスが行われるようコントロールしてください。これによって、未認証のユーザーがファイルにアクセスしたり、改ざん、または誤って削除したりすることを防止できます。

注: このセクションにあるリンクのリンク先ページは第三者の Web サイトによって管理されているもので、リンクは便宜上の目的においてのみ掲載しています。ソフォスでは、リンク切れなどについて定期的に確認していますが、第三者の Web サイトによって予告なしにリンクが変更される場合があります。

2.3 コンピュータのグループについて

保護するコンピュータをどのようにグループ分けするかを決めます。このベストプラクティスについては、www.sophos.com/ja-jp/support/knowledgebase/63556.aspxを参照してください。

2.4 セキュリティポリシーについて

セキュリティポリシーとは、1つ以上のコンピュータのグループに適用できる設定の集まりです。

Enterprise Console でグループを作成すると、デフォルトのポリシーが適用されます。このガイドの説明に従って、このポリシーを編集したり、または新しいポリシーを作成することができます。推奨する設定について、詳細は「**Sophos Enterprise Console ポリシー設定ガイド**」を参照してください。

2.5 ネットワーク上のコンピュータの検出について

ネットワーク上のコンピュータにセキュリティ対策ソフトをインストールする前に、必ずインポートしたコンピュータを Enterprise Console のコンピュータのリストに追加してください。コンピュータを検出し、リストに追加する方法について、詳細は Enterprise Console ヘルプを参照してください。

2.6 コンピュータの保護について

Windows が稼働しているコンピュータには、Enterprise Console からセキュリティ対策ソフトを自動インストールできます。

注: Sophos Client Firewall は、サーバー OS が稼働しているコンピュータにはインストールできません。

ネットワーク上に他の OS を実行しているコンピュータがある場合は、手動でインストールしたり、スクリプトを使用したり、あるいは Active Directory を利用するなど他の方法でソフトウェアをインストールする必要があります。このガイドでは、次の OS で手動インストールを行う方法について説明します。

- Windows
- Mac OS X

他の OS 環境での手動インストールに関する詳細は、「**Sophos Enterprise Console スタートアップガイド Linux/UNIX 版**」を参照してください。

3 システム要件

ヒント: 今すぐインストールを開始しない場合でも、Enterprise Console のインストーラを実行して、サーバーが Enterprise Console のインストール要件を満たしているかどうかチェックすることができます。システムチェックの結果は、インストールウィザードの「**システムプロパティの確認**」ページで確認できます。結果を確認した後、「**キャンセル**」をクリックしてウィザードを閉じます。システムチェックの結果についての詳細は、次の文章を参照してください。 <http://www.sophos.com/ja-jp/support/knowledgebase/113945.aspx>

3.1 ハードウェアおよび OS

本製品のシステム要件は、ソフォス Web サイトの「システム要件」(www.sophos.com/ja-jp/products/all-system-requirements.aspx) を参照してください。

3.2 マイクロソフトのシステムソフトウェア

Enterprise Consoleのインストールには、データベースソフトなど、特定のマイクロソフトのシステムソフトウェアが必要です。

このようなシステムソフトウェアが対象のサーバーにインストールされていない場合は、Enterprise Consoleの製品インストーラが自動的にシステムソフトウェアのインストールを開始します。ただし、サーバーとシステムソフトウェアに互換性がない場合は手動によるインストールが必要です。

注: 必要なシステムソフトウェアをインストール後、コンピュータの再起動が必要となることがあります。詳細は、<https://www.sophos.com/ja-jp/support/knowledgebase/65190.aspx> を参照してください。

SQL Server のインストール

既存の SQL Server 2005 Express 以降のインスタンスを使用することを選択しない限り、インストーラは自動的に SQL Server 2012 Express Edition サービスパック 2 (SP2) のインストールを開始します。以下の点に注意してください。

- SQL Server はドメイン コントローラ以外のコンピュータにインストールすることを推奨します。
- Enterprise Consoleのデータベースを別のサーバーにインストールする場合、SQL Server インスタンスへリモートアクセスできるように設定してください。詳細は、<http://www.sophos.com/ja-jp/support/knowledgebase/118473.aspx>を参照してください。

.NET Framework のインストール

.NET Framework 4.x がインストールされていない場合は、インストーラが .NET Framework 4.5.2 のインストールを自動的に開始します。

重要: .NET Framework 4.5.2 のインストールの一環として、一部のシステムサービス (IIS Admin Service など) が再起動することがあります。

.NET Framework 4.5.2 のインストール後、コンピュータの再起動を求めるメッセージが表示されることがあります。その場合は、インストール後ただちに、またはなるべく早く再起動することを推奨します。

Microsoft メッセージキューのインストール

MSMQ (Microsoft メッセージキュー) がインストールされていない場合は、インストーラが自動的にインストールを開始します。

重要: MSMQ のインストール中、次のサービスが停止します。MSDTC、MSSQLServer、SQLSERVERAGENT。このため、デフォルトの SQL Server データベースとの接続が中断されます。インストール中、これらのサービスが停止しても問題がないことを確認してください。また、操作終了後、サービスが再開したことも確認してください。

3.3 ポート要件

Enterprise Console を使用するには、特定のポートが開放されている必要があります。詳細は、次の文章を参照してください。

www.sophos.com/ja-jp/support/knowledgebase/38385.aspx

4 必要なアカウント

ソフォス製品をインストールする前に、以下のユーザーアカウントを作成する必要があります。

- **データベース用アカウント:** Enterprise Console の管理サービスがデータベースに接続するための Windows ユーザーアカウントです。他のソフォスのサービスでも使用されません。

データベース用アカウントの名前は、**SophosManagement** とすることを推奨します。

- **Update Manager アカウント:** Enterprise Console によって製品アップデート版が配置されるフォルダに、エンドポイントコンピュータがアクセスするための Windows ユーザーアカウントです。

Update Manager アカウントの名前は、**SophosUpdateMgr** とすることを推奨します。

4.1 データベース用アカウント

データベース用アカウントが次の要件を満たしていることを確認してください。

- Sophos Management Server (Enterprise Console のコンポーネント) のインストール先コンピュータにログオンする権限がある。
- システムの一時ディレクトリ (\windows\temp\ など) に読み取り権限と書き込み権限がある。「Users」グループのメンバーには、デフォルトでこの権限があります。
- ドメインアカウントの場合は、UPN (ユーザープリンシパル名) が関連付けられている。

これ以外に必要な権限およびグループのメンバーシップは、インストール時に自動的に付与されます。

以下のようにアカウントを設定することを推奨します。

- 無期限に設定する。また、その他のログオン制限を指定しない。
- アカウントに管理者権限がない。
- インストール後、アカウントを変更しない。
- アカウント名が **SophosManagement** である。

推奨事項や設定方法については、次の文章を参照してください。

<https://www.sophos.com/ja-jp/support/knowledgebase/113954.aspx>

4.2 Update Manager アカウント

Update Manager アカウントには、Enterprise Console が製品アップデート版を配置するフォルダへの読み取り権限が必要です。デフォルトで、このフォルダは \\[サーバー名]\SophosUpdate です。

以下のようにアカウントを設定することを推奨します。

- 無期限に設定する。また、その他のログオン制限を指定しない。
- アカウントに管理者権限がない。
- ドメインアカウントの場合は、UPN(ユーザープリンシパル名)が関連付けられている。
- アカウント名が **SophosUpdateMgr** である。

推奨事項や設定方法については、次の文章を参照してください。

<https://www.sophos.com/ja-jp/support/knowledgebase/113954.aspx>

5 Enterprise Console コンポーネントのインストール先について

Sophos Enterprise Console (SEC) には次の 4種類のコンポーネントが含まれます。

管理コンソール	コンピュータの保護や管理を行います。
管理サーバー	アップデートや通信を処理します。
データベース	ネットワーク上のコンピュータに関するデータを保存します。
アップデートマネージャ	ソフォス製品やアップデート版をソフォスのサーバーからダウンロードし、各コンピュータが接続し、アップデートする社内サーバーに取り込みます。

SEC のコンポーネントを別々のサーバーにインストールする場合は、それらのサーバーすべてを同じドメインに配置することをお勧めします。

SEC データベースはドメイン コントローラ以外のコンピュータにインストールすることを推奨します。

このガイドでは 2とおりのインストールシナリオについて説明します。

- 管理データベースを別のサーバーにインストールする方法
- 追加のアップデートマネージャを別のサーバーにインストールする方法

それぞれのシナリオで、ネットワーク上の SEC のコンポーネントの配置が異なります。

5.1 管理データベースを別のサーバーにインストールする方法

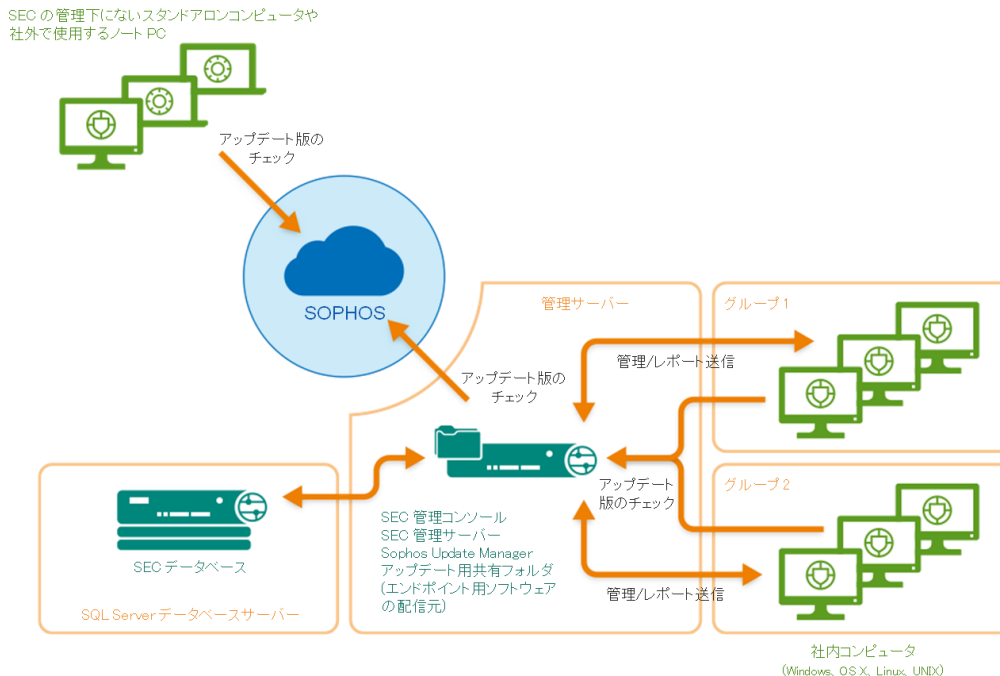


図 1: インストールシナリオの例: 管理データベースを別のサーバーにインストールする

このシナリオを使用する場合は、[シナリオ1:管理データベースを別のサーバーにインストールする方法](#) (p. 16) に進んでください。

5.2 追加のアップデートマネージャを別のサーバーにインストールする方法

このシナリオには、各アップデートマネージャのアップデート元を設定する方法が2とおりあります。

1つ目の方法は次のとおりです。

- SEC 管理コンソールと一緒にインストールされるメインのアップデートマネージャを、直接ソフォスのサーバーに接続し、アップデート版をダウンロードする。
- メインのアップデートマネージャから、追加のアップデートマネージャにアップデート版を取り込む。

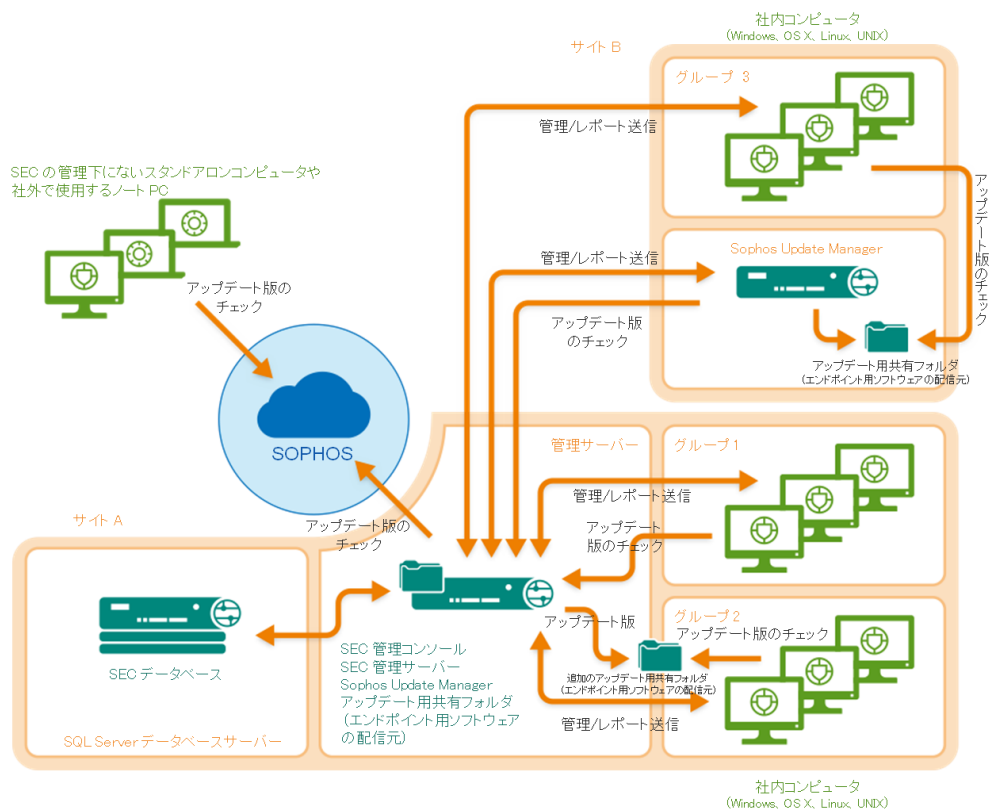


図 2: インストールシナリオの例: 追加のアップデートマネージャをメインのアップデートマネージャからアップデートする

2つ目の方法は次のとおりです。

- 追加のアップデートマネージャを、直接ソフォスのサーバーに接続し、アップデート版をダウンロードする。
- 追加のアップデートマネージャから、SEC 管理コンソールと一緒にインストールされるメインのアップデートマネージャにアップデート版を取り込む。

どちらの方法を選択する場合でも、このインストールシナリオを使用するには、[シナリオ 2: 追加のアップデートマネージャを別のサーバーにインストールする方法](#) (p. 23) に進んでください。

6 シナリオ 1: 管理データベースを別のサーバーにインストールする方法

6.1 インストーラのダウンロード

注: インストーラは任意のコンピュータにダウンロードし、その後、ソフトウェアをインストールするコンピュータにコピーすることもできます。

1. Sophos ID を使って、次のサイトにログインします。
<https://www.sophos.com/ja-jp/support/downloads.aspx>

注: Sophos ID についてご不明の点は、[ソフォスのサポートデータベースの文章 111195](#)を参照してください。

2. ダウンロードするためにログインしたことがある場合は、「**製品・アップデート版のダウンロード**」ページが表示されます。

注: はじめてログインする場合は、プロファイルが表示されます。「**Endpoint and Server Protection**」をクリックして、「**Downloads and Updates**」をクリックします。

3. 「**Console**」の下で、「**Sophos Enterprise Console**」をクリックして、インストーラをダウンロードします。

6.2 SEC データベースのインストール

注: データベースをスクリプトを使用して安全なサーバーにインストールしたり、クラスタ化された SQL サーバー環境にインストールしたりする必要がある場合は、次の文章を参照してください。www.sophos.com/ja-jp/support/knowledgebase/33980.aspx

ユーザーアカウント制御 (UAC) を有効にしている場合、無効にし、サーバーを再起動します (Windows Server 2008 以降の場合)。UAC はデータベースをインストールした後で、有効に設定し直せます。

管理者権限でログオンします。

- サーバーがドメインに属している場合は、ローカル管理者権限を持つドメインアカウントを使用してください。
- サーバーがワークグループに属している場合は、ローカル管理者権限を持つローカルアカウントを使用してください。

1. 前述の手順でダウンロードした Enterprise Console のインストーラを参照し、ダブルクリックします。
2. デフォルトのインストール先フォルダ、または任意のフォルダにインストールファイルを展開します。このサーバー上のフォルダのみ指定できます。

インストールウィザードの指示に従ってインストールを行います。以下に説明のないオプションは、デフォルトの設定をそのまま選択します。

- a) 「**コンポーネントの選択**」ページで、「**データベース**」を選択し、「**管理コンソール**」と「**管理サーバー**」の選択を外します。
- b) 「**データベースの詳細**」ページで、このサーバーと、Enterprise Console の管理サーバーをインストールするサーバーの両方にログインできるアカウントの情報を入力します。サーバーが共に**ドメイン**に属している場合は、ドメインアカウントを使用できます。サーバーが共に**ワークグループ**に属している場合は、両方のサーバーにアクセスできるローカルアカウントを使用してください。管理者アカウントは使用しないでください。

注: このデータベースアカウントは、[データベース用アカウント](#) (p. 11) で作成したものです。

Enterprise Console のウィザード完了後、プロンプト表示されたらサーバーを再起動してください。

ユーザーアカウント制御を無効にした場合は、ここで有効に設定し直してください。

6.3 SEC のインストール - 管理コンソール、管理サーバー、アップデートマネージャ

Enterprise Console の管理コンソール、管理サーバー、およびアップデートマネージャをインストールするサーバーに移動します。サーバーがインターネットに接続されていることを確認します。

このサーバーのホスト名は、アップデートマネージャをインストールする他のサーバーのホスト名とは異なっている必要があります。

ユーザーアカウント制御 (UAC) を有効にしている場合、無効にし、サーバーを再起動します (Windows Server 2008 以降の場合)。UAC は、Enterprise Console をインストールし、ソフォス アップデートに登録した後で、有効に設定することができます。

管理者権限でログオンします。

- サーバーがドメインに属している場合は、ローカル管理者権限を持つドメインアカウントを使用してください。
 - サーバーがワークグループに属している場合は、ローカル管理者権限を持つローカルアカウントを使用してください。
1. 前述の手順でダウンロードした Enterprise Console のインストーラを参照し、ダブルクリックします。
 2. デフォルトのインストール先フォルダ、または任意のフォルダにインストールファイルを展開します。このサーバー上のフォルダのみ指定できます。

インストールウィザードの指示に従ってインストールを行います。以下に説明のないオプションは、デフォルトの設定をそのまま選択します。

- a) 「**コンポーネントの選択**」ページで、「**管理コンソール**」と「**管理サーバー**」を選択し、「**データベース**」の選択を外します。
- b) 「**データベースの詳細**」ページで、別のサーバーに作成した Enterprise Console のデータベースの場所と名前を入力します。このサーバーと Enterprise Console のデータベースをインストールしたサーバーの両方にログインできるアカウントの情報を入力します。サーバーが共に**ドメイン**に属している場合は、ドメインアカウントを使用できます。サーバーが共に**ワークグループ**に属している場合は、両方のサーバーにアクセスできるローカルアカウントを使用してください。管理者アカウントは使用しないでください。

注: このデータベースアカウントは、[データベース用アカウント](#) (p. 11) で作成したものです。

インストールが完了したら、ログオフ、またはサーバーを再起動します (ウィザードの最後の画面にどちらかのオプションが表示されます)。ログインし直すと、Enterprise Console が自動的に開き、セキュリティソフトのダウンロード ウィザードが起動します。ここではウィザードをキャンセルし、このガイドの説明の順序に従い、後で起動します。

6.4 追加の SEC 管理コンソールのインストール

別のコンピュータに追加の Sophos Enterprise Console 管理コンソールのインスタンスをインストールすると、ネットワーク上のコンピュータを効率よく管理できます。必要ない場合は、このセクションは読み飛ばしてください。

重要: 管理サーバー上で実行されているのと同じバージョンの Enterprise Console をインストールする必要があります。

注: 新しく追加したコンソールは、Enterprise Console 管理サーバーをインストールしたサーバーにアクセスする必要があります。そのサーバーでファイアウォールを使用している場合、コンソールからアクセスできるようにファイアウォールの設定が必要なことがあります。リモートコンソールから管理サーバーへの DCOM トラフィックを許可するファイアウォールルールを追加する方法は、[サポートデータベースの文章 49028](#) を参照してください。

追加の管理コンソールをインストールする方法は次のとおりです。

ユーザーアカウント制御 (UAC) を有効にしている場合、無効にし、サーバーを再起動します (Windows Server 2008 以降 または Windows Vista 以降の場合)。UAC は管理コンソールをインストールした後で、有効に設定し直せます。

管理者権限でログオンします。

- コンピュータがドメインに属している場合は、ローカル管理者権限を持つドメインアカウントを使用してください。
- コンピュータがワークグループに属している場合は、ローカル管理者権限を持つローカルアカウントを使用してください。

1. ダウンロードした Enterprise Console のインストーラを参照し、ダブルクリックします。

2. デフォルトのインストール先フォルダ、または任意のフォルダにインストールファイルを展開します。このコンピュータ上のフォルダのみ指定できます。

インストールウィザードの指示に従ってインストールを行います。以下に説明のないオプションは、デフォルトの設定をそのまま選択します。

- a) 「**コンポーネントの選択**」ページで、「**管理コンソール**」を選択し、「**管理サーバー**」と「**データベース**」の選択を外します。
- b) 「**管理サーバー**」ページで、Enterprise Console 管理サーバーをインストールしたサーバーの名前を入力します。

注: 管理サーバーをインストールする際にポートを変更した場合は、必ず、このページでも同じポートを指定する必要があります。

- c) ドメイン環境の場合、Enterprise Consoleデータベースへの接続に使用するユーザーアカウントを入力します。

このアカウントはEnterprise Consoleデータベースをインストールする際に入力したアカウントです。また、Enterprise Consoleの管理サーバーをインストールしたサーバーの Sophos Management Host サービスでも同じアカウントが使用されています。

ウィザードが完了したら、ログオフ、またはコンピュータを再起動します (ウィザードの最後の画面にどちらかのオプションが表示されます)。ログインし直すと、Enterprise Console が自動的に開きます。「**セキュリティソフトのダウンロード ウィザード**」が起動した場合は、キャンセルします。

インストールの前にユーザーアカウント制御を無効にした場合は、ここで有効に設定し直してください。

追加の管理コンソールの使用を他のユーザーに許可するには、次の手順を実行してください。

- 管理サーバーをインストールしたサーバー上の **Sophos Console Administrators** グループと、**Distributed COM Users** グループに、ユーザーを追加する。
- 少なくとも1つの Enterprise Consoleロールとサブ管理サイトに、ユーザーを追加する。

6.5 セキュリティソフトのダウンロード

各クライアントマシンへ斉配信できるようにセキュリティソフトを社内のサーバーに取り込むには、インストールしたアップデートマネージャを設定する必要があります。次のどちらかまたは両方の方法で設定できます。

自動でのアップデートマネージャの設定 (p. 20) : この手順に従ってウィザードを起動します。

- サポートされる各 OS 用セキュリティソフトウェアをダウンロードできます。
- 最新の推奨バージョンのみをダウンロードできます。
- ダウンロード先は共有フォルダ **サーバー名**\SophosUpdate のサブフォルダのみです。ここで**サーバー名**は、アップデートマネージャがインストールされているサーバーの名前です。

[手動でのアップデートマネージャの設定](#) (p. 20) : この手順に従ってアップデートマネージャを直接設定します。

- サポートされる各 OS 用セキュリティソフトウェアをダウンロードできます。
- プレビューバージョンまたは以前のバージョンをダウンロードできます。
- ダウンロード先は、上記とは別の共有フォルダ (複数可) です。別のサーバー上の共有フォルダを指定することもできます。

6.5.1 自動でのアップデートマネージャの設定

1. Enterprise Console で、「**アクション**」メニューの「**セキュリティソフトのダウンロードウィザードの実行**」をクリックします。
2. 「**ソフォス ダウンロード用アカウントの詳細**」ページで、ライセンスの別表 (License Schedule) に記載されているユーザー名とパスワードを入力します。プロキシサーバー経由でインターネットにアクセスする場合は、「**プロキシサーバー経由でソフォスにアクセスする**」チェックボックスを選択します。
3. 「**OS の選択**」ページで保護するプラットフォームを選択します。
「**次へ**」をクリックすると、Enterprise Console は選択したソフトウェアのダウンロードを開始します。
4. 「**ソフトウェアをダウンロードしています**」ダイアログボックスに、ダウンロードの進行状況が表示されます。随時、「**次へ**」をクリックします。
5. Enterprise Console で既存の Active Directory のコンピュータのグループを利用する場合は、「**Active Directory からコンピュータをインポートします**」ページで、「**コンピュータグループを設定する**」チェックボックスを選択します。

注: 1つのコンピュータが複数の Active Directory のコンテナに配置されている場合、そのコンピュータと Enterprise Console との間で常にメッセージが送受信される問題が発生します。

選択したソフトウェアが共有フォルダ **サーバー名**\SophosUpdate にダウンロードされます。ここで**サーバー名**はアップデートマネージャがインストールされているサーバーです。

Enterprise Console のインストールを開始する前に、ユーザーアカウント制御を無効にした場合は、ここで有効に設定し直してください。

次に、必要に応じてアップデートマネージャを手動で設定します。次に、[セキュリティソフトの Web サーバーへの配置](#) (p. 35) へ進んでください。

6.5.2 手動でのアップデートマネージャの設定

Enterprise Console のインストールを開始する前に、ユーザーアカウント制御を無効にした場合は、ここで有効に設定し直してください。

1. Enterprise Console の「**表示**」メニューで、「**アップデートマネージャ**」をクリックします。

2. アップデートマネージャを自動的に設定していない場合は、アップデート元を「Sophos」に設定します。
 - a) 「**アップデートマネージャ**」ペインで、このサーバーにインストールされているアップデートマネージャを選択します。右クリックして「**環境設定の表示/編集**」をクリックします。
 - b) 「**アップデートマネージャの環境設定**」ダイアログボックスの「**アップデート元**」タブで、「**追加**」をクリックします。
 - c) 「**アップデート元の詳細**」ダイアログボックスの「**アドレス**」ボックスから「**Sophos**」を選択します。「**ユーザー名**」と「**パスワード**」ボックスに、ソフォスから入手したダウンロード用アカウントの詳細を入力します。
 - d) プロキシサーバー経由でアップデート元に接続する場合は、「**プロキシサーバーを使用して接続する**」チェックボックスを選択します。プロキシサーバーの「**アドレス**」と「**ポート**」番号を入力します。「**ユーザー名**」と「**パスワード**」ボックスに、プロキシサーバーに接続するためのアカウント情報を入力します。「**ユーザー名**」とドメイン名をあわせて指定する必要がある場合は、ドメイン名ユーザー名 という形式で入力してください。
 - e) 「**OK**」をクリックして「**アップデート元の詳細**」ダイアログボックスを閉じます。「**アップデートマネージャの環境設定**」ダイアログボックスの「**アップデート元**」タブの一覧に「**Sophos**」が表示されます。
 - f) 「**OK**」をクリックして「**アップデートマネージャの環境設定**」ダイアログボックスを閉じます。
3. ダウンロードするソフトウェアを登録します。
 - a) 「**ソフトウェアのサブスクリプション**」ペインで次の手順を実行します。
 - 既存のサブスクリプションを変更するにはダブルクリックします。
 - 新しいサブスクリプションを追加するには、ペイン上部の「**追加**」をクリックします。
 - b) 新しいサブスクリプションを追加する場合は、「**ソフトウェアのサブスクリプション**」ダイアログボックスの「**サブスクリプション名**」ボックスにサブスクリプション名を入力します。
 - c) プラットフォームのリストから対象のソフトウェアの横にあるチェックボックスを選択し、「**バージョン**」の一覧から適切なバージョンを選択します。

通常、ソフトウェアを自動的に最新の状態に保つために、「**Recommended**」(推奨バージョン)を選択します。利用できるその他のソフトウェアのバージョンについては、Enterprise Console ヘルプのソフトウェアのサブスクリプションの設定に関するセクションを参照してください。
 - d) 「**OK**」をクリックして「**ソフトウェアのサブスクリプション**」ダイアログボックスを閉じます。
 - e) 変更、または追加する各サブスクリプションに対して、ここでのステップを繰り返してください。

4. アップデートマネージャを設定し、これらのサブスクリプションを使用するようにします。
 - a) 「**アップデートマネージャ**」ペインで、このサーバーにインストールされているアップデートマネージャを選択します。右クリックして「**環境設定の表示/編集**」をクリックします。
 - b) 「**アップデートマネージャの環境設定**」ダイアログボックスの「**サブスクリプション**」タブの「**ダウンロードするサブスクリプション**」リストにサブスクリプションが表示されていることを確認します。表示されていない場合は、「**選択可能アイテム**」リストからサブスクリプションを選択して「>」ボタンをクリックし、「**ダウンロードするサブスクリプション**」リストに追加します。
5. **サーバー名**\SophosUpdate 以外の共有にダウンロードする場合は以下の手順を実行します。
 - a) 「**配布**」タブをクリックします。
 - b) タブ上部のリストで使用するサブスクリプションが選択されていることを確認します。
 - c) 「**追加**」をクリックします。
 - d) 「**フォルダの参照**」ダイアログボックスで共有フォルダを参照します。「**OK**」をクリックします。
 - e) 「**選択可能アイテム**」リストから共有フォルダを選択して「>」ボタンをクリックし、「**アップデート先**」リストに追加します。
 - f) 共有フォルダの説明や、書き込み用アカウントの詳細を入力するには、共有フォルダを選択し、「**環境設定**」をクリックします。「**共有マネージャ**」ダイアログボックスで、説明とアカウント情報を入力します。
 - g) 各共有フォルダに対してこの手順を繰り返します。
6. 「**OK**」をクリックして「**アップデートマネージャの環境設定**」ダイアログボックスを閉じます。

選択したソフトウェアは、指定した共有フォルダへダウンロードされます。

これで、管理ツールのインストールが完了しました。次に、[セキュリティソフトの Web サーバーへの配置](#) (p. 35) へ進みます。

7 シナリオ 2: 追加のアップデートマネージャを別のサーバーにインストールする方法

このシナリオには、各アップデートマネージャのアップデート元を設定する方法が2とおりあります。

1つ目の方法は次のとおりです。

- 管理コンソールと一緒にインストールされるメインのアップデートマネージャを、直接ソフォスのサーバーに接続し、アップデート版をダウンロードする。
- メインのアップデートマネージャから、追加のアップデートマネージャにアップデート版を取り込む。

2つ目の方法は次のとおりです。

- 追加のアップデートマネージャを、直接ソフォスのサーバーに接続し、アップデート版をダウンロードする。
- 追加のアップデートマネージャから、管理コンソールと一緒にインストールされるメインのアップデートマネージャにアップデート版を取り込む。

2つ目の方法は、メインの Enterprise Console サーバーをインターネットに接続しない場合に利用できます。

どちらの方法を選択するかによって次の点が異なります。

- インターネットへの接続が必要となるサーバーが異なります。これより後のセクションで、インストール先のサーバーをインターネットに接続するタイミングを説明します。
- 各クライアントマシンへ斉配信できるようにセキュリティソフトを社内のサーバーに取り込む方法が異なります。設定する際に該当するセクションを選択してください。
- Enterprise Console でパッチ評価機能を使用できるか、できないかが異なります。使用する場合は、1つ目の方法を選択してください。

7.1 インストーラのダウンロード

注: インストーラは任意のコンピュータにダウンロードし、その後、ソフトウェアをインストールするコンピュータにコピーすることもできます。

1. Sophos ID を使って、次のサイトにログインします。
<https://www.sophos.com/ja-jp/support/downloads.aspx>

注: Sophos ID についてご不明の点は、[ソフォスのサポートデータベースの文章 111195](#)を参照してください。

2. ダウンロードするためにログインしたことがある場合は、「製品・アップデート版のダウンロード」ページが表示されます。

注: はじめてログインする場合は、プロファイルが表示されます。「Endpoint and Server Protection」をクリックして、「Downloads and Updates」をクリックします。

3. 「Console」の下で、「Sophos Enterprise Console」をクリックして、インストーラをダウンロードします。

7.2 SEC のインストール - すべてのコンポーネント

Enterprise Console のすべてのコンポーネントをインストールするサーバーに移動します。これからインストールするアップデートマネージャを直接ソフォスのサーバーに接続し、アップデート版をダウンロードする場合は、インストール先のサーバーがインターネットに接続されていることを確認してください。

このサーバーのホスト名は、アップデートマネージャをインストールする他のサーバーのホスト名とは異なっている必要があります。

ユーザーアカウント制御 (UAC) を有効にしている場合、無効にし、サーバーを再起動します (Windows Server 2008 以降の場合)。UAC は、Enterprise Console をインストールし、ソフォス アップデートに登録した後で、有効に設定することができます。

管理者権限でログオンします。

- サーバーがドメインに属している場合は、ローカル管理者権限を持つドメインアカウントを使用してください。
- サーバーがワークグループに属している場合は、ローカル管理者権限を持つローカルアカウントを使用してください。

1. 前述の手順でダウンロードした Enterprise Console のインストーラを参照し、ダブルクリックします。
2. デフォルトのインストール先フォルダ、または任意のフォルダにインストールファイルを展開します。このサーバー上のフォルダのみ指定できます。

インストールウィザードの指示に従ってインストールを行います。以下に説明のないオプションは、デフォルトの設定をそのまま選択します。

- a) 「**コンポーネントの選択**」ページで、すべてのコンポーネントが選択されていることを確認します。
- b) 「**データベースの詳細**」ページで、このサーバーにログインできるアカウントの情報を入力します。サーバーが**ドメイン**に属している場合は、ドメインアカウントを使用できます。サーバーが**ワークグループ**に属している場合は、そのサーバーにアクセスできるローカルアカウントを使用してください。管理者アカウントは使用しないでください。

注: このデータベースアカウントは、[データベース用アカウント](#) (p. 11) で作成したものです。

インストールが完了したら、ログオフ、またはサーバーを再起動します (ウィザードの最後の画面にどちらかのオプションが表示されます)。ログインし直すと、Enterprise Console が自動的に開き、セキュリティソフトのダウンロード ウィザードが起動します。ここではウィザードをキャンセルし、このガイドの説明の順序に従い、後で起動します。

7.3 追加の SEC 管理コンソールのインストール

別のコンピュータに追加のSophos Enterprise Console管理コンソールのインスタンスをインストールすると、ネットワーク上のコンピュータを効率よく管理できます。必要ない場合は、このセクションは読み飛ばしてください。

重要: 管理サーバー上で実行されているのと同じバージョンの Enterprise Consoleをインストールする必要があります。

注: 新しく追加したコンソールは、Enterprise Console管理サーバーをインストールしたサーバーにアクセスする必要があります。そのサーバーでファイアウォールを使用している場合、コンソールからアクセスできるようにファイアウォールの設定が必要なことがあります。リモートコンソールから管理サーバーへの DCOM トラフィックを許可するファイアウォールルールを追加する方法は、[サポートデータベースの文章 49028](#) を参照してください。

追加の管理コンソールをインストールする方法は次のとおりです。

ユーザーアカウント制御 (UAC) を有効にしている場合、無効にし、サーバーを再起動します (Windows Server 2008 以降 または Windows Vista 以降の場合)。UAC は管理コンソールをインストールした後で、有効に設定し直せます。

管理者権限でログオンします。

- コンピュータがドメインに属している場合は、ローカル管理者権限を持つドメインアカウントを使用してください。
- コンピュータがワークグループに属している場合は、ローカル管理者権限を持つローカルアカウントを使用してください。

1. ダウンロードした Enterprise Consoleのインストーラを参照し、ダブルクリックします。
2. デフォルトのインストール先フォルダ、または任意のフォルダにインストールファイルを展開します。このコンピュータ上のフォルダのみ指定できます。

インストールウィザードの指示に従ってインストールを行います。以下に説明のないオプションは、デフォルトの設定をそのまま選択します。

- a) 「**コンポーネントの選択**」ページで、「**管理コンソール**」を選択し、「**管理サーバー**」と「**データベース**」の選択を外します。
- b) 「**管理サーバー**」ページで、Enterprise Console 管理サーバーをインストールしたサーバーの名前を入力します。

注: 管理サーバーをインストールする際にポートを変更した場合は、必ず、このページでも同じポートを指定する必要があります。

- c) ドメイン環境の場合、Enterprise Consoleデータベースへの接続に使用するユーザーアカウントを入力します。

このアカウントはEnterprise Consoleデータベースをインストールする際に入力したアカウントです。また、Enterprise Consoleの管理サーバーをインストールしたサーバーの Sophos Management Host サービスでも同じアカウントが使用されています。

ウィザードが完了したら、ログオフ、またはコンピュータを再起動します (ウィザードの最後の画面にどちらかのオプションが表示されます)。ログインし直すと、Enterprise Console が自動的に開きます。「**セキュリティソフトのダウンロード ウィザード**」が起動した場合は、キャンセルします。

インストールの前にユーザーアカウント制御を無効にした場合は、ここで有効に設定し直してください。

追加の管理コンソールの使用を他のユーザーに許可するには、次の手順を実行してください。

- 管理サーバーをインストールしたサーバー上の **Sophos Console Administrators** グループと、**Distributed COM Users** グループに、ユーザーを追加する。
- 少なくとも1つの Enterprise Console ロールとサブ管理サイトに、ユーザーを追加する。

7.4 追加のアップデートマネージャのインストール

重要: アップデートマネージャを追加インストールするサーバーに、SEC の管理コンソールを追加インストールする場合は、必ず最初に追加コンソールをインストールしてください。この手順の詳細は、[追加の SEC 管理コンソールのインストール](#) (p. 25) を参照してください。

追加のアップデートマネージャをインストールするサーバーに移動します。これからインストールするアップデートマネージャを直接ソフォスのサーバーに接続し、アップデート版をダウンロードする場合は、インストール先のサーバーがインターネットに接続されていることを確認してください。

このサーバーのホスト名は、アップデートマネージャをインストールする他のサーバーのホスト名とは異なっている必要があります。

ネットワーク探索機能を無効にしている場合、有効にし、サーバーを再起動します (Windows Server 2008 以降の場合)。

ユーザーアカウント制御 (UAC) を有効にしている場合、無効にし、サーバーを再起動します (Windows Server 2008 以降の場合)。UAC は、アップデートマネージャをインストールし、ソフォス アップデートに登録した後で、有効に設定することができます。

管理者権限でログオンします。

- サーバーがドメインに属している場合は、ローカル管理者権限を持つドメインアカウントを使用してください。
 - サーバーがワークグループに属している場合は、ローカル管理者権限を持つローカルアカウントを使用してください。
1. Enterprise Console をインストールしたサーバーの「SUMInstallSet」という共有フォルダを参照します。
 2. Setup.exe をダブルクリックしてインストーラを起動します。
インストールウィザードの指示に従ってインストールを行います。オプションはデフォルトの設定をそのまま選択します。

Enterprise Console で管理するアップデートマネージャがインストールされます。

7.5 セキュリティソフトのダウンロード

このシナリオには、各アップデートマネージャのアップデート元を設定する方法が2とおりあります。どちらか適切な方法を選択してください。

- [メインのアップデートマネージャによるソフォスからのアップデート版のダウンロード](#) (p. 27)
- [追加のアップデートマネージャによるソフォスからのアップデート版のダウンロード](#) (p. 31)

7.5.1 メインのアップデートマネージャによるソフォスからのアップデート版のダウンロード

メインのアップデートマネージャを設定して、ソフォスから直接アップデートするようにする

SEC 管理コンソールと一緒にインストールされるメインのアップデートマネージャを設定して、ソフォスから直接アップデートするようにしてください。次のどちらかまたは両方の方法で設定できます。

[自動でのメインのアップデートマネージャの設定](#) (p. 28) : この手順に従ってウィザードを起動します。

- すべてのサポートされるプラットフォーム版セキュリティソフトウェアをダウンロードできます。
- 最新版のみをダウンロードできます。
- ダウンロード先は共有フォルダ **サーバー名**\SophosUpdate のサブフォルダのみ。ここで**サーバー名**は、メインのアップデートマネージャがインストールされているサーバーの名前です。

[手動でのメインのアップデートマネージャの設定](#) (p. 28) : この手順に従ってメインのアップデートマネージャを直接設定します。

- サポートされる各 OS 用セキュリティソフトウェアをダウンロードできます。
- 以前のバージョンをダウンロードできます。
- ダウンロード先は、上記とは別の共有フォルダ (複数可) です。別のサーバー上の共有フォルダを指定することもできます。

利用できるその他のソフトウェアのバージョンについては、Enterprise Console ヘルプのサブスクリプションの設定に関するセクションを参照してください。

追加のアップデートマネージャを設定して、メインのアップデートマネージャからアップデートするようにする

[追加のアップデートマネージャの設定](#) (p. 30) を行うと、メインのアップデートマネージャから、追加のアップデートマネージャにアップデート版が取り込めるようになります。

7.5.1.1 自動でのメインのアップデートマネージャの設定

1. Enterprise Console で、「**アクション**」メニューの「**セキュリティソフトのダウンロードウィザードの実行**」をクリックします。
2. 「**ソフォス ダウンロード用アカウントの詳細**」ページで、ライセンスの別表 (License Schedule) に記載されているユーザー名とパスワードを入力します。プロキシサーバー経由でインターネットにアクセスする場合は、「**プロキシサーバー経由でソフォスにアクセスする**」チェックボックスを選択します。
3. 「**OS の選択**」ページで保護するプラットフォームを選択します。
「**次へ**」をクリックすると、Enterprise Console は選択したソフトウェアのダウンロードを開始します。
4. 「**ソフトウェアをダウンロードしています**」ダイアログボックスに、ダウンロードの進行状況が表示されます。随時、「**次へ**」をクリックします。
5. Enterprise Console で既存の Active Directory のコンピュータのグループを利用する場合は、「**Active Directory からコンピュータをインポートします**」ページで、「**コンピュータグループを設定する**」チェックボックスを選択します。

注: 1つのコンピュータが複数の Active Directory のコンテナに配置されている場合、そのコンピュータと Enterprise Console との間で常にメッセージが送受信される問題が発生します。

選択したソフトウェアが共有フォルダ **サーバー名**\SophosUpdate にダウンロードされます。ここで**サーバー名**はアップデートマネージャがインストールされているサーバーです。

Enterprise Console のインストールを開始する前に、ユーザーアカウント制御を無効にした場合は、ここで有効に設定し直してください。

次に、必要に応じてアップデートマネージャを手動で設定します。次に、[追加のアップデートマネージャの設定](#) (p. 30) へ進んでください。

7.5.1.2 手動でのメインのアップデートマネージャの設定

Enterprise Console のインストールを開始する前に、ユーザーアカウント制御を無効にした場合は、ここで有効に設定し直してください。

1. Enterprise Console の「**表示**」メニューで、「**アップデートマネージャ**」をクリックします。

2. アップデートマネージャを自動的に設定していない場合は、アップデート元を「Sophos」に設定します。
 - a) 「**アップデートマネージャ**」ペインで、このサーバーにインストールされているアップデートマネージャを選択します。右クリックして「**環境設定の表示/編集**」をクリックします。
 - b) 「**アップデートマネージャの環境設定**」ダイアログボックスの「**アップデート元**」タブで、「**追加**」をクリックします。
 - c) 「**アップデート元の詳細**」ダイアログボックスの「**アドレス**」ボックスから「**Sophos**」を選択します。「**ユーザー名**」と「**パスワード**」ボックスに、ソフォスから入手したダウンロード用アカウントの詳細を入力します。
 - d) プロキシサーバー経由でアップデート元に接続する場合は、「**プロキシサーバーを使用して接続する**」チェックボックスを選択します。プロキシサーバーの「**アドレス**」と「**ポート**」番号を入力します。「**ユーザー名**」と「**パスワード**」ボックスに、プロキシサーバーに接続するためのアカウント情報を入力します。「**ユーザー名**」とドメイン名をあわせて指定する必要がある場合は、ドメイン名ユーザー名 という形式で入力してください。
 - e) 「**OK**」をクリックして「**アップデート元の詳細**」ダイアログボックスを閉じます。
「**アップデートマネージャの環境設定**」ダイアログボックスの「**アップデート元**」タブの一覧に「**Sophos**」が表示されます。
 - f) 「**OK**」をクリックして「**アップデートマネージャの環境設定**」ダイアログボックスを閉じます。
3. ダウンロードするソフトウェアを登録します。
 - a) 「**ソフトウェアのサブスクリプション**」ペインで次の手順を実行します。
 - 既存のサブスクリプションを変更するにはダブルクリックします。
 - 新しいサブスクリプションを追加するには、ペイン上部の「**追加**」をクリックします。
 - b) 新しいサブスクリプションを追加する場合は、「**ソフトウェアのサブスクリプション**」ダイアログボックスの「**サブスクリプション名**」ボックスにサブスクリプション名を入力します。
 - c) プラットフォームのリストから対象のソフトウェアの横にあるチェックボックスを選択し、「**バージョン**」の一覧から適切なバージョンを選択します。
通常、ソフトウェアを自動的に最新の状態に保つために、「**Recommended**」(推奨バージョン)を選択します。利用できるその他のソフトウェアのバージョンについては、Enterprise Console ヘルプのソフトウェアのサブスクリプションの設定に関するセクションを参照してください。
 - d) 「**OK**」をクリックして「**ソフトウェアのサブスクリプション**」ダイアログボックスを閉じます。
 - e) 変更、または追加する各サブスクリプションに対して、ここでのステップを繰り返してください。

4. アップデートマネージャを設定し、これらのサブスクリプションを使用するようにします。
 - a) 「**アップデートマネージャ**」ペインで、このサーバーにインストールされているアップデートマネージャを選択します。右クリックして「**環境設定の表示/編集**」をクリックします。
 - b) 「**アップデートマネージャの環境設定**」ダイアログボックスの「**サブスクリプション**」タブの「**ダウンロードするサブスクリプション**」リストにサブスクリプションが表示されていることを確認します。表示されていない場合は、「**選択可能アイテム**」リストからサブスクリプションを選択して「>」ボタンをクリックし、「**ダウンロードするサブスクリプション**」リストに追加します。
5. 「**OK**」をクリックして「**アップデートマネージャの環境設定**」ダイアログボックスを閉じます。

選択したソフトウェアは、このサーバーにインストールしたアップデートマネージャにダウンロードされます。

7.5.1.3 追加のアップデートマネージャの設定

1. Enterprise Console の「**表示**」メニューで、「**アップデートマネージャ**」をクリックします。
2. 追加のアップデートマネージャのアップデート元にメインのアップデートマネージャを指定します。
 - a) 「**アップデートマネージャ**」ペインで、追加のアップデートマネージャを選択します。右クリックして「**環境設定の表示/編集**」をクリックします。
 - b) 「**アップデートマネージャの環境設定**」ダイアログボックスの「**アップデート元**」タブで、「**追加**」をクリックします。
 - c) 「**アップデート元の詳細**」ダイアログボックスの「**アドレス**」ボックスから、メインのアップデートマネージャがダウンロードしたソフトウェアを配置する共有フォルダを選択します。

「**ユーザー名**」と「**パスワード**」ボックスに、この共有フォルダへのアクセスに必要なアカウント情報が自動的に挿入されます。
 - d) プロキシサーバー経由でアップデート元に接続する場合は、「**プロキシサーバーを使用して接続する**」チェックボックスを選択します。プロキシサーバーの「**アドレス**」と「**ポート**」番号を入力します。「**ユーザー名**」と「**パスワード**」ボックスに、プロキシサーバーに接続するためのアカウント情報を入力します。「**ユーザー名**」とドメイン名をあわせて指定する必要がある場合は、ドメイン名\ユーザー名 という形式で入力してください。
 - e) 「**OK**」をクリックして「**アップデート元の詳細**」ダイアログボックスを閉じます。

メインのアップデートマネージャがダウンロードしたソフトウェアを配置する共有フォルダは、「**アップデートマネージャの環境設定**」ダイアログボックスの「**アップデート元**」タブに表示されます。

3. アップデートマネージャを設定して、先程設定したサブスクリプションを使用するようにします。
 - 「サブスクリプション」タブの「ダウンロードするサブスクリプション」リストにサブスクリプションが表示されていることを確認します。表示されていない場合は、「**選択可能アイテム**」リストからサブスクリプションを選択して「>」ボタンをクリックし、「**ダウンロードするサブスクリプション**」リストに追加します。
4. **サーバー名**\SophosUpdate 以外の共有にダウンロードする場合は以下の手順を実行します。
 - a) 「**配布**」タブをクリックします。
 - b) タブ上部のリストで使用するサブスクリプションが選択されていることを確認します。
 - c) 「**追加**」をクリックします。
 - d) 「**フォルダの参照**」ダイアログボックスで共有フォルダを参照します。「**OK**」をクリックします。
 - e) 「**選択可能アイテム**」リストから共有フォルダを選択して「>」ボタンをクリックし、「**アップデート先**」リストに追加します。
 - f) 共有フォルダの説明や、書き込み用アカウントの詳細を入力するには、共有フォルダを選択し、「**環境設定**」をクリックします。「**共有マネージャ**」ダイアログボックスで、説明とアカウント情報を入力します。
 - g) 各共有フォルダに対してこの手順を繰り返します。
5. 「**OK**」をクリックして「**アップデートマネージャの環境設定**」ダイアログボックスを閉じます。

選択したソフトウェアは、次回行われるスケジュールアップデート時に、指定した共有フォルダへダウンロードされます。

これで、管理ツールのインストールが完了しました。次に、[セキュリティソフトの Web サーバーへの配置](#) (p. 35) へ進みます。

7.5.2 追加のアップデートマネージャによるソフォスからのアップデート版のダウンロード

追加のアップデートマネージャを設定して、直接ソフォスのサーバーからアップデート版をダウンロードする方法は、[追加のアップデートマネージャの設定](#) (p. 32) を参照してください。

SEC 管理コンソールと一緒にインストールされるメインのアップデートマネージャを設定して、追加のアップデートマネージャからアップデートを行う方法は、[メインのアップデートマネージャの設定](#) (p. 33) を参照してください。

7.5.2.1 追加のアップデートマネージャの設定

Enterprise Console のインストールを開始する前に、ユーザーアカウント制御を無効にした場合は、ここで有効に設定し直してください。

1. Enterprise Console の「**表示**」メニューで、「**アップデートマネージャ**」をクリックします。
2. 追加のアップデートマネージャのアップデート元にソフォスを指定します。
 - a) 「**アップデートマネージャ**」ペインで、追加のアップデートマネージャを選択します。右クリックして「**環境設定の表示/編集**」をクリックします。
 - b) 「**アップデートマネージャの環境設定**」ダイアログボックスの「**アップデート元**」タブで、「**追加**」をクリックします。
 - c) 「**アップデート元の詳細**」ダイアログボックスの「**アドレス**」ボックスから「**Sophos**」を選択します。「**ユーザー名**」と「**パスワード**」ボックスに、ソフォスから入手したダウンロード用アカウントの詳細を入力します。
 - d) プロキシサーバー経由でアップデート元に接続する場合は、「**プロキシサーバーを使用して接続する**」チェックボックスを選択します。プロキシサーバーの「**アドレス**」と「**ポート**」番号を入力します。「**ユーザー名**」と「**パスワード**」ボックスに、プロキシサーバーに接続するためのアカウント情報を入力します。「**ユーザー名**」とドメイン名をあわせて指定する必要がある場合は、ドメイン名\ユーザー名 という形式で入力してください。
 - e) 「**OK**」をクリックして「**アップデート元の詳細**」ダイアログボックスを閉じます。「**アップデートマネージャの環境設定**」ダイアログボックスの「**アップデート元**」タブの一覧に「**Sophos**」が表示されます。
 - f) 「**OK**」をクリックして「**アップデートマネージャの環境設定**」ダイアログボックスを閉じます。
3. ダウンロードするソフトウェアを登録します。
 - a) 「**ソフトウェアのサブスクリプション**」ペインで次の手順を実行します。
 - 既存のサブスクリプションを変更するにはダブルクリックします。
 - 新しいサブスクリプションを追加するには、ペイン上部の「**追加**」をクリックします。
 - b) 新しいサブスクリプションを追加する場合は、「**ソフトウェアのサブスクリプション**」ダイアログボックスの「**サブスクリプション名**」ボックスにサブスクリプション名を入力します。
 - c) プラットフォームのリストから対象のソフトウェアの横にあるチェックボックスを選択し、「**バージョン**」の一覧から適切なバージョンを選択します。

通常、ソフトウェアを自動的に最新の状態に保つために、「**Recommended**」(推奨バージョン)を選択します。利用できるその他のソフトウェアのバージョンについて

は、Enterprise Console ヘルプのソフトウェアのサブスクリプションの設定に関するセクションを参照してください。

- d) 「**OK**」をクリックして「**ソフトウェアのサブスクリプション**」ダイアログボックスを閉じます。
 - e) 変更、または追加する各サブスクリプションに対して、ここでのステップを繰り返してください。
4. アップデートマネージャを設定し、これらのサブスクリプションを使用するようにします。
 - a) 「**アップデートマネージャ**」ペインで、追加のアップデートマネージャを選択します。右クリックして「**環境設定の表示/編集**」をクリックします。
 - b) 「**アップデートマネージャの環境設定**」ダイアログボックスの「**サブスクリプション**」タブの「**ダウンロードするサブスクリプション**」リストにサブスクリプションが表示されていることを確認します。表示されていない場合は、「**選択可能アイテム**」リストからサブスクリプションを選択して「>」ボタンをクリックし、「**ダウンロードするサブスクリプション**」リストに追加します。
 5. 「**OK**」をクリックして「**アップデートマネージャの環境設定**」ダイアログボックスを閉じます。

選択したソフトウェアは、追加のアップデートマネージャにダウンロードされます。

7.5.2.2 メインのアップデートマネージャの設定

1. Enterprise Console の「**表示**」メニューで、「**アップデートマネージャ**」をクリックします。
2. メインのアップデートマネージャのアップデート元に追加のアップデートマネージャを指定します。
 - a) 「**アップデートマネージャ**」ペインで、このサーバーにインストールされているアップデートマネージャを選択します。右クリックして「**環境設定の表示/編集**」をクリックします。
 - b) 「**アップデートマネージャの環境設定**」ダイアログボックスの「**アップデート元**」タブで、「**追加**」をクリックします。
 - c) 「**アップデート元の詳細**」ダイアログボックスの「**アドレス**」ボックスから、追加のアップデートマネージャがダウンロードしたソフトウェアを配置する共有フォルダを選択します。

「**ユーザー名**」と「**パスワード**」ボックスに、この共有フォルダへのアクセスに必要なアカウント情報が自動的に挿入されます。
 - d) プロキシサーバー経由でアップデート元に接続する場合は、「**プロキシサーバーを使用して接続する**」チェックボックスを選択します。プロキシサーバーの「**アドレス**」と「**ポート**」番号を入力します。「**ユーザー名**」と「**パスワード**」ボックスに、プロキシサーバーに接続するためのアカウント情報を入力します。「**ユーザー名**」とドメイン名をあわせて指定する必要がある場合は、ドメイン名<ユーザー名>という形式で入力してください。
 - e) 「**OK**」をクリックして「**アップデート元の詳細**」ダイアログボックスを閉じます。

追加のアップデートマネージャがダウンロードしたソフトウェアを配置する共有フォルダは、「**アップデートマネージャの環境設定**」ダイアログボックスの「**アップデート元**」タブに表示されます。

3. アップデートマネージャを設定して、先程設定したサブスクリプションを使用するようにします。
 - 「**サブスクリプション**」タブの「**ダウンロードするサブスクリプション**」リストにサブスクリプションが表示されていることを確認します。表示されていない場合は、「**選択可能アイテム**」リストからサブスクリプションを選択して「>」ボタンをクリックし、「**ダウンロードするサブスクリプション**」リストに追加します。
4. **サーバー名**\SophosUpdate 以外の共有にダウンロードする場合は以下の手順を実行します。
 - a) 「**配布**」タブをクリックします。
 - b) タブ上部のリストで使用するサブスクリプションが選択されていることを確認します。
 - c) 「**追加**」をクリックします。
 - d) 「**フォルダの参照**」ダイアログボックスで共有フォルダを参照します。「**OK**」をクリックします。
 - e) 「**選択可能アイテム**」リストから共有フォルダを選択して「>」ボタンをクリックし、「**アップデート先**」リストに追加します。
 - f) 共有フォルダの説明や、書き込み用アカウントの詳細を入力するには、共有フォルダを選択し、「**環境設定**」をクリックします。「**共有マネージャ**」ダイアログボックスで、説明とアカウント情報を入力します。
 - g) 各共有フォルダに対してこの手順を繰り返します。
5. 「**OK**」をクリックして「**アップデートマネージャの環境設定**」ダイアログボックスを閉じます。

選択したソフトウェアは、次回行われるスケジュールアップデート時に、指定した共有フォルダへダウンロードされます。

これで、管理ツールのインストールが完了しました。次に、[セキュリティソフトの Web サーバーへの配置](#) (p. 35) へ進みます。

8 セキュリティソフトの Web サーバーへの配置

各コンピュータから HTTP 経由でアクセスできるように、ソフォスのセキュリティソフトを Web サーバーに配置することもできます。社内ネットワークに常時接続しないコンピュータがある場合は特に有効です。

- セキュリティソフトの Web サーバーへの配置について、詳細は次の文章を参照してください。 www.sophos.com/ja-jp/support/knowledgebase/38238.aspx

9 コンピュータグループの作成

「セキュリティソフトのダウンロード」ウィザードを使用して、(Active Directory のグループを基に) コンピュータグループを設定した場合は、ここで説明する操作は必要ありません。[セキュリティポリシーの設定](#) (p. 37) に進んでください。

コンピュータを保護・管理する前に、コンピュータのグループを作成する必要があります。

1. 「**グループ**」ペイン (画面左側) が表示されていない場合は、「**表示**」メニューで、「**エンドポイント**」をクリックします。
2. 「**グループ**」ペイン内をクリックします。**グループ外のコンピュータ**グループが選択されていないことを確認します。
3. 「**グループ**」メニューで、「**グループの作成**」をクリックします。
「**新規グループ**」が左ペインに追加され、そのグループ名がハイライト表示されます。
4. 使用するグループ名を入力します。
5. トップレベルのグループを新たに作成するには、「**グループ**」ペインの最上部に表示されているサーバーを選択し、ステップ 3 ~ 4 を繰り返してください。
既存のグループのサブグループを作成するには、既存のグループを選択し、ステップ 3 ~ 4 を繰り返してください。

10 セキュリティポリシーの設定

セキュリティポリシーとは、1つ以上のコンピュータのグループに適用できる設定の集まりです。

Enterprise Console は、デフォルトポリシーをコンピュータのグループに適用します。ここで説明する内容は次のとおりです。

- デフォルトポリシーの概要とその変更について。
- ポリシーの作成・編集。
- コンピュータグループへのポリシーの適用。

10.1 デフォルトポリシー

Enterprise Console は、各種の「デフォルト」というセキュリティポリシーをコンピュータのグループに適用します。これらのデフォルトポリシーに必要な設定は以下のとおりです。これ以外の変更は任意です。

- ファイアウォールポリシーは、すぐに設定する必要があります。
- 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、パッチ、エクスプロイト対策、またはWeb コントロール機能を使用する場合は、該当する各ポリシーを編集する必要があります。この操作は、いつ行っても構いません。

ポリシーの設定の詳細は、「**Sophos Enterprise Console ポリシー設定ガイド**」を参照してください。

10.2 ファイアウォールポリシーの設定

デフォルトの設定では、ファイアウォールは重要な接続以外はすべて遮断します。したがって、各コンピュータに設定を適用して保護する前に、ファイアウォール ポリシーの設定を行う必要があります。

1. 「**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。

「**新規ポリシー**」がリストに追加され、ポリシー名がハイライト表示されます。使用するグループ名を入力します。

2. ポリシーをダブルクリックして編集します。

ウィザードが起動します。

3. 「**ファイアウォールのポリシー ウィザード**」で、次のように設定することを推奨します。
 - a) 「**ファイアウォールの環境設定**」ページで、接続場所に応じて、異なるファイアウォールの設定を使い分ける場合以外は、「**1種類の設定 (固定マシン用)**」を選択します。
 - b) 「**操作モード**」ページで、「**受信トラフィックをブロックし、送信トラフィックを許可する**」を選択します。
 - c) 「**ファイルとプリンタの共有**」ページで、「**ファイルとプリンタの共有を許可する**」を選択します。

10.3 ポリシーの作成・編集

1. Enterprise Console で、「**ポリシー**」ペイン (画面左下) が表示されていない場合は、「**表示**」メニューで、「**エンドポイント**」をクリックします。
2. 「**ポリシー**」ペインで、次のいずれかの手順を実行します。
 - 新しいポリシーを作成するには、「**アップデート**」など、作成するポリシーの種類を右クリックし、「**ポリシーの作成**」をクリックします。
 - デフォルトポリシーを編集するには、編集するポリシーの種類をダブルクリックします。次に、「**デフォルト**」を選択します。

ポリシーを作成すると、「**新規ポリシー**」がリストに追加され、ポリシー名がハイライト表示されます。使用するグループ名を入力します。

3. ポリシーをダブルクリックし、必要に応じて内容を設定してください。

ポリシーを作成した場合は、作成したポリシーをコンピュータグループに適用してください。

10.4 グループへのポリシーの適用

- 「**ポリシー**」ペインで、適用するグループに、ポリシーをドラッグします。

注: または、各グループを右クリックして、「**グループポリシーの詳細の表示/編集**」を選択します。表示されるドロップダウンメニューから、そのグループに対するポリシーを選択できます。

11 コンピュータの検出

Enterprise Console でコンピュータの保護と管理を行うには、まずネットワーク上のコンピュータを検出する必要があります。

1. 「**グループ**」ペイン (画面左側) が表示されていない場合は、「**表示**」メニューで、「**エンドポイント**」をクリックします。
2. 「**アクション**」メニューで、「**コンピュータの検出**」をクリックします。
3. コンピュータの検索方法を選択してください。
4. 適宜、アカウントの詳細を入力し、検索場所を指定します。

「**検出**」オプションのいずれかを選択すると、検出されたコンピュータは「**グループ外のコンピュータ**」フォルダに追加されます。

12 コンピュータの保護の事前準備

12.1 他社製セキュリティ対策ソフトを削除する準備

現在インストールされているセキュリティソフトをアンインストールする場合は、次の手順を実行してください。

1. 他社製のウイルス対策ソフトを実行しているコンピュータで、そのウイルス対策ソフトの GUI が閉じていることを確認します。

注: スタンドアロン製品、または Sophos Central の一機能として、HitmanPro.Alert がインストールされていることがあります。HitmanPro.Alert は、Sophos Enterprise Console からオンプレミス型の管理を適用する前に削除する必要があります。

2. 他社製のファイアウォールや HIPS 製品を実行しているコンピュータで、これらのソフトウェアを無効にするか、またはソフォス製品のインストーラの起動を許可するように設定します。

他社製のアップデートツールを実行している場合は、削除した方がよい場合があります。詳細は Enterprise Console ヘルプを参照してください。

12.2 ソフトウェアをインストールできるアカウントがあることの確認

セキュリティソフトのインストールに使用できる Windows ユーザーアカウントを入力する画面が表示されます。次の条件を満たしている必要があります。

- 保護するコンピュータへのローカル管理者権限がある。
- Enterprise Console をインストールしたコンピュータにログオンできる。
- コンピュータのアップデート元に対する読み取り許可がある。アップデート元がどこかを確認するには、「ポリシー」ペインで、「アップデート」をダブルクリックし、次に、「デフォルト」をダブルクリックします。

注: 「ポリシー」ペイン (画面左下) が表示されていない場合は、「表示」メニューで、「エンドポイント」をクリックします。

以下のようにアカウントを設定することを推奨します。

- ドメイン管理者アカウントでなく、制約付き委任が構成されている。
- Enterprise Console、追加のアップデートマネージャ、またはメッセージリレーがインストールされているコンピュータに対して、管理者権限やシステム特権がない。
- コンピュータのアップデート元に対する書き込みのアクセス許可や変更のアクセス許可がない。
- コンピュータの保護のみに使用し、一般的な管理タスクには使用していない。
- 頻繁にパスワードを変更している。

12.3 ウィルス対策ソフトをインストールする準備

ウィルス対策ソフトをインストールする前に、コンピュータの準備を行う必要があります。詳細は、ソフォス エンドポイント展開ガイド (英語) (https://docs.sophos.com/esg/enterprise-console/tools/deployment_guide/en-us/index.html) の「コンピュータへの導入の準備をする」セクションを参照してください。

保護するコンピュータでは、ファイアウォールを有効化することを推奨します。

注: 保護を完了し、そのコンピュータが Enterprise Console に「管理対象コンピュータ」として表示されたら、コンピュータへのリモートインストールを許可するために作成した、すべてのファイアウォールの例外設定を無効に設定しなおすことを検討してください。

13 コンピュータの保護

13.1 自動での Windows コンピュータの保護

ここでは Enterprise Console で Windows ベースのコンピュータを集中的に保護する方法について説明します。

任意のツールやスクリプトを使用して Windows コンピュータに保護機能をインストールすることもできます。詳細は、次の文章を参照してください。

www.sophos.com/ja-jp/support/knowledgebase/114191.aspx

注: Sophos Client Firewallをインストールする際、すべてのネットワークアダプタが一時的に切断されます。最長20秒間ネットワークに接続できなくなります。また、Microsoft Remote Desktop などのネットワークアプリケーションが切断されます。

1. Enterprise Consoleで、保護するコンピュータを選択します。
2. 次のいずれかの手順を実行してください。
 - コンピュータがグループに追加されている場合は、右クリックし「**コンピュータの保護**」を選択します。
 - コンピュータが「**グループ外のコンピュータ**」フォルダに表示されている場合は、適切なグループにドラッグします。

ウィザードの指示に従ってソフォスのセキュリティソフトをインストールします。以下に説明のないオプションは、デフォルトの設定をそのまま選択します。

- a) 「**機能の選択**」ページで、インストールする追加機能を選択します。
- b) インストール中に問題が発生した場合は、「**保護のサマリー**」ページでその詳細を確認します。詳細は、[トラブルシューティング](#) (p. 42) を参照してください。
- c) 「**アカウント情報**」ダイアログボックスで、各コンピュータへのソフトウェアのインストールに使用できるアカウントの詳細を入力します。

選択したコンピュータには、セキュリティソフトがインストールされます。インストールはすべてのコンピュータで同時に開始されないため、操作がすべて完了するまで時間がかかることがあります。一部のコンピュータでは、インストールの完了に再起動が必要となる場合があります。

インストール完了後、コンピュータのリストをもう一度確認します。「**オンアクセス**」カラムに表示される「**アクティブ**」は、コンピュータで脅威のオンアクセス検索が実行されていることを表します。

13.1.1 トラブルシューティング

Windows コンピュータの自動保護を行う際、セキュリティソフトのインストールに失敗することがありますが、考えられる原因は次のとおりです。

- 使用している OS で自動インストールを実行することができない。この場合は、手動でインストールを行います。詳細は、[手動での Windows コンピュータや Mac の保護](#) (p.

43) を参照してください。他の OS に関しては、このガイドの後半のセクションを参照してください。

- OS が認識されない。これは、コンピュータの検索を行った際に、「ドメインユーザー名」形式でユーザ名を入力しなかったことが原因の場合があります。
- セキュリティ対策ソフトを展開するために必要なアクセスが、ファイアウォールのルールによってブロックされている。
- Windows XP コンピュータ上の「簡易ファイルの共有」が無効になっていない。
- Windows Vista コンピュータ上の「共有ウィザード」が無効になっていない。
- OS でサポートされていない機能をインストールしようとした。

13.2 手動での Windows コンピュータや Mac の保護

自動保護できないコンピュータがある場合は、セキュリティソフトがダウンロードされている共有フォルダ内のインストーラを手動で実行して保護します。このフォルダの通称は「インストーラの場所」です。

保護を実施するコンピュータで管理者アカウントを使用する必要があります。

Windows コンピュータや Mac を手動で保護する方法は次のとおりです。

1. Enterprise Console の「**表示**」メニューで、「**インストーラの場所**」をクリックします。
インストーラの場所の一覧が表示されます。保護を実施する各 OS のインストーラの場所をメモします。
2. 保護を実施する各コンピュータで、インストーラの場所を参照し、次の手順を実行します。
 - Windows コンピュータの場合、`setup.exe` を見つけ、ダブルクリックします。
 - Mac の場合は、`Sophos Installer.app` インストーラファイルおよび `Sophos Installer Components` ディレクトリを任意の場所 (デスクトップなど) にコピーし、ダブルクリックします。

ウィザードの指示に従ってインストールを行います。以下に説明のないオプションは、デフォルトの設定をそのまま選択します。

- Windows コンピュータでは、「**ユーザーアカウントの詳細**」に、先に指定した Update Manager への接続用アカウントの詳細を入力します。このアカウントは、[Update Manager アカウント](#) (p. 11) で Enterprise Console をインストールしたときに設定したものです。

ヒント: どのアカウントがよくわからない場合は、「インストーラの場所」にアクセスできる、権限の低い任意のアカウントを使用します。後で、Enterprise Console によって正しいアカウントの詳細を含むアップデートポリシーが適用されます。

13.3 Linux または UNIX コンピュータの保護

Linux や UNIX コンピュータを保護する方法の詳細は、「[Enterprise Console スタートアップガイド Linux/UNIX版](#)」を参照してください。

14 ネットワークのセキュリティの状態の確認

Enterprise Console でネットワークのセキュリティの状態を確認する方法は次のとおりです。

1. Enterprise Console のダッシュボードを表示します。

既に表示されていない場合は、「**表示**」メニューで、「**ダッシュボード**」をクリックします。

ダッシュボードには次の情報が表示されます。

- 「警告を発したコンピュータ」の台数。
- 「最新版が適用されていないコンピュータ」の台数。
- 「ポリシーと異なるコンピュータ」の台数。

15 スタンドアロン コンピュータの保護

従業員が自宅で使用するコンピュータなど一部のコンピュータは、社内ネットワークに接続することがないため、管理者が簡単にアクセスできません。このようなコンピュータを保護する場合、ユーザー自身が「スタンドアロン」インストーラを使用してソフォスのセキュリティソフトをインストールする必要があります。インストールしたソフトウェアはインターネット経由で最新の状態に保たれます。方法は次の2とおりから選べます。

- ユーザーが次のサイトからソフトウェアをダウンロードする。
www.sophos.com/ja-jp/support/downloads/standalone-installers/esc-for-windows-2000-up.aspx
ユーザーは、ソフトウェアをインストールし、ソフォスからアップデート版を取得するよう設定します。
- ソフトウェアとインストール以降のアップデート版を社内の Web サイトから再配信する。ユーザーは社内の Web サイトからソフトウェアをダウンロード、インストールし、社内の Web サイトからアップデート版を取得するよう設定します。社内の Web サイトからソフォス製品のアップデート版を再配信する方法については、次の文章を参照してください。 www.sophos.com/ja-jp/support/knowledgebase/38238.aspx

15.1 スタンドアロン コンピュータのユーザーへの必要な情報の送信

社内ネットワークに接続していないユーザーには、次の情報を送信してください。

- セキュリティソフトをダウンロードする場所 (CD を配布する場合は不要)。
- **Sophos Endpoint Security and Control スタンドアロン スタートアップガイド**。
- ダウンロードに必要なユーザー名およびパスワード (ソフォス Web サイトから直接、または自社 Web サイトからダウンロードするどちらの場合でも)。

アカウント情報を送信する際は次の点にご注意ください。

- ウイルスに感染しているコンピュータにメール送信しないでください。アカウント情報が盗まれる恐れがあります。
- 必要な場合は、郵送やファックスで送付してください。

16 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>

17 利用条件

Copyright © 2009–2017 Sophos Limited. All rights reserved. この出版物の一部または全部を、電子的、機械的な方法、写真複写、録音、その他いかなる形や方法においても、使用許諾契約の条項に準じてドキュメントを複製することを許可されている、もしくは著作権所有者からの事前の書面による許可がある場合以外、無断に複製、復元できるシステムに保存、または送信することを禁じます。

Sophos、Sophos Anti-Virus および SafeGuard は、Sophos Limited、Sophos Group および Utimaco Safeware AG の登録商標です。その他記載されている会社名、製品名は、各社の登録商標または商標です。

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

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™ (henceforth referred to as "DOC software") are copyrighted by Douglas C. Schmidt and his research group at Washington University, University of California, Irvine, and Vanderbilt University, Copyright (c) 1993-2014, all rights reserved. Since DOC software is open-source, freely available software, you are free to use, modify, copy, and distribute—perpetually and irrevocably—the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with any code built using DOC software that you release. No copyright statement needs to be provided if you just ship binary executables of your software products.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not misappropriate the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, in a way that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us know so we can promote your project in the [DOC software success stories](#).

The ACE, TAO, CIAO, DAnCE, and CoSMIC web sites are maintained by the DOC Group at the Institute for Software Integrated Systems (ISIS) and the Center for Distributed Object Computing of Washington University, St. Louis for the development of open-source software as part of the open-source software community. Submissions are provided by the submitter "as is" with no warranties whatsoever, including any warranty of merchantability, noninfringement of third party intellectual property, or fitness for any particular purpose. In no event shall the submitter be liable for any direct, indirect, special, exemplary, punitive, or consequential damages, including without limitation, lost profits, even if advised of the possibility of such damages. Likewise, DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A [number of companies](#) around the world provide

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

Copyright © 1995–2013 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly jloup@gzip.org

Mark Adler madler@alumni.caltech.edu