

SOPHOS

Sophos Control Center スタートアップガイド

製品バージョン: 4.1

ドキュメント作成日: 2011年 2月



目次

1 このガイドについて.....	3
2 システム要件.....	4
3 インストール.....	5
4 ネットワーク上のコンピュータの保護.....	9
5 コンピュータ保護の確認.....	13
6 メール警告の設定.....	14
7 不要と思われるアプリケーションの検索の設定.....	16
8 ウイルスの対処.....	19
9 ファイアウォールの設定.....	20
10 テクニカルサポート.....	23
11 著作権情報.....	24

1 このガイドについて

このガイドでは、ウイルス (スパイウェアを含む)、不要と思われるアプリケーション、およびその他のセキュリティ脅威に対して、ネットワーク上のコンピュータ (Windows/Mac の両方) を保護する方法について説明します。

ネットワークに全く接続しないコンピュータの場合は、このガイドに加え、「**Sophos Endpoint Security and Control スタンドアロンスタートアップガイド**」もご覧ください。

Sophos Control Center の既存バージョンをアップグレードする場合は、「**Sophos Control Center アップグレードガイド**」をご覧ください。

このガイドでは説明していない、Sophos Control Center の環境設定オプションの全容は、Sophos Control Center ヘルプをご覧ください。

ソフォスのドキュメントは、<http://www.sophos.co.jp/support/docs/> から入手可能です。

2 システム要件

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」(<http://www.sophos.co.jp/products/all-sysreqs.html>) を参照してください。

また、製品をソフォス Web サイトからダウンロードするには、インターネットにアクセスする必要があります。

Sophos Control Center およびサーバーコンポーネントのその他の要件は次のとおりです。

- ネットワーク上の他のコンピュータとの相互アクセスが必要です。
- サーバー OS (Windows Server 2003 または Windows Small Business Server 2011 など) を使用することを推奨します。サーバー OS を使用しないと、Sophos Control Center のパフォーマンスに影響を与えるのでご注意ください。

重要: Sophos Control Center を Windows 2008 Small Business Server (SBS) にインストールする場合は、コンピュータに Windows Live OneCare がインストールされていないことを確認してください。Windows Live OneCare をアンインストールするには、Windows の「コントロールパネル」から、「アプリケーションの追加と削除」を使用してください。

ソフォス製品で既定で使用される SQL Server 2005 Express でなく、SQL Server を使用する場合は、それがインストール済みであることを確認した後、SOPHOS というインスタンスを作成してください。操作方法については、ご使用の SQL Server のドキュメントやマイクロソフトのテクニカルサポートを参照してください。

3 インストール

3.1 Sophos Control Center をインストールする前に

Sophos Control Center のインストールを開始する前に、次の操作を行ってください。

- ソフォス提供のユーザー名とパスワードがあることを確認します。
- Sophos Control Center がインストールされているコンピュータに、適宜、管理者またはドメイン管理者としてログオンします。

ヒント: ワークグループにある、任意の Windows OS 環境のコンピュータを保護する場合は、さらに、

<http://www.sophos.co.jp/support/knowledgebase/article/29728.html> に説明のある手順を行ってください。

3.2 エンドポイントコンピュータを準備する

エンドポイントコンピュータにセキュリティソフトをインストールする前に、次の操作を行ってください。

- Sophos Anti-Virus をインストールするすべてのコンピュータから、他社のウイルス対策ソフトを削除します。
- ここで説明する OS ごとの設定を行います。

3.2.1 Windows Vista 以降

Sophos Anti-Virus を Windows Vista 以降のコンピュータにインストールするには、次の追加要件を満たしている必要があります。

- 「**RemoteRegistry**」サービスが起動しており、「スタートアップの種類」が「**自動**」に設定されている。このサービスは、Windows Vista ではデフォルトで自動的に開始しません。この設定を変更するには、「**スタート-コントロールパネル-管理ツール-サービス**」を開きます。次に、サービスの一覧から「**RemoteRegistry**」サービスをダブルクリックします。「**RemoteRegistry**のプロパティ」ダイアログボックスの「**全般**」タブで、「**スタートアップの種類**」のドロップダウンリストから「**自動**」を選択して「**適用**」をクリックします。「**開始**」を選択して「**OK**」をクリックします。
- 「**ユーザーアカウント制御(UAC)**」を無効にする。この設定は、「**スタート-コントロールパネル-ユーザーアカウント-ユーザーアカウント制御**

の有効化または無効化」で変更できます。インストールが完了したら、この設定を有効にしてください。

- 「セキュリティが強化された Windows ファイアウォール」を開きます。この設定は、「スタート - コントロールパネル - 管理ツール」で変更できます。「受信の規則」を変更して次の設定を有効にします。

規則の名前	Profile
リモート管理 (NP 受信)	ドメイン
リモート管理 (NP 受信)	プライベート
リモート管理 (RPC)	ドメイン
リモート管理 (RPC)	プライベート
リモート管理 (RPC-EPMAP)	ドメイン
リモート管理 (RPC-EPMAP)	プライベート

ヒント: インストールが完了したら、これらの設定を再度無効にしてください。

3.2.2 Windows XP

Windows XP コンピュータ (サービスパック適用/未適用) で次のステップを実行してください。

- Sophos Client Firewall をインストールするすべての Windows XP コンピュータから、他社のファイアウォールソフトすべて (Windows ファイアウォールは除く) を削除する。
- 簡易ファイルの共有を無効にする。

操作方法は、<http://www.sophos.co.jp/support/knowledgebase/article/12837.html> を参照してください。

Windows XP SP 2

Windows ファイアウォールが有効で、Sophos Client Firewall をインストールしない Windows XP SP 2 コンピュータでは、次の操作を行ってください。

- 「Microsoft ネットワーク用ファイルとプリンタ共有」を有効にする。
- 次のプログラムを「例外」に追加する。

C:\Program Files\Sophos\Remote Management System\RouterNT.exe

操作方法は、<http://www.sophos.co.jp/support/knowledgebase/article/11075.html>を参照してください。

3.2.3 Windows Server 2003 SP 1

Windows ファイアウォールが有効になっている場合は、次の操作を行ってください。

- 「Microsoft ネットワーク用ファイルとプリンタ共有」を有効にする。
- 次のプログラムを「例外」に追加する。

C:\Program Files\Sophos\Remote Management System\RouterNT.exe

操作方法は、<http://www.sophos.co.jp/support/knowledgebase/article/11075.html>を参照してください。

3.2.4 Windows 2000

- Sophos Client Firewall をインストールするすべての Windows 2000 コンピュータから、他社のファイアウォールソフトすべて (Windows ファイアウォールは除く) を削除する。

3.2.5 Windows 98 SE

- 既にインストールされている Sophos Anti-Virus をすべて削除する。削除を行うには、Windows の「コントロールパネル」から、「アプリケーションの追加と削除」を使用してください。

3.3 Sophos Control Center をインストールする

まずはじめに、ウイルス対策/ファイアウォールソフトをダウンロード、デプロイ、および管理する Sophos Control Center をインストールします。

1. ソフォスの製品ダウンロードページ (<http://www.sophos.co.jp/support/updates>) で、ソフォス提供のユーザー名とパスワードを入力します。

該当するリンクをクリックして、ソフォススモールビジネスソリューションの製品インストーラをダウンロードし、実行します。

2. **Sophos Small Business Edition インストーラ**で、インストールファイルの展開先を確認します。ファイルは、Sophos Control Center をインストールするコンピュータ上に保存する必要があります。そして、「**Install**」(インストール)をクリックします。

3. 「ようこそ」 ページで、「次へ」をクリックします。

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、デフォルト設定をそのまま選択します。

4. 「セットアップタイプ」 ページで、「すべて」を選択して、プログラムの機能すべてをインストールします。

ヒント: セキュリティソフトを他のコンピュータから管理する場合は、このインストーラを管理元のコンピュータにコピーして、起動し、「**管理コンソールのみ**」を選択します。

「次へ」をクリックし、再度デフォルトのオプションを指定して、ウィザードの指示に従います。

5. インストール手順が完了したら、自動的にログオフするには、「完了」をクリックします。後でログオフするには、「今すぐログオフする」のチェックを外してから「完了」をクリックします。

ログオフするだけでなく、Windowsの再起動が必要な場合もあります。この場合、チェックボックスは表示されず、続いてWindowsを今すぐ、または後で再起動するかメッセージが表示されます。

6. 同じユーザーとして再ログオンします。「ソフォス ネットワークの保護ウィザード」が自動的に開始します。

ネットワーク上のコンピュータを保護する方法の詳細は、[ネットワーク上のコンピュータの保護](#) (p. 9) を参照してください。

4 ネットワーク上のコンピュータの保護

インストール後の初回ログオンでは、Sophos Control Centerが自動的に開き、「ソフォス ネットワークの保護 ウィザード」が開始します。このウィザードを使用して、ネットワーク上のコンピュータを保護します。

1. 「ようこそ」ページで、「次へ」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」ページに、ソフォス提供のユーザー名とパスワードを入力し、「次へ」をクリックします。

Sophos Control Center は、現在、使用しているコンピュータ上のフォルダにソフトウェアを取り込み、そこから他のコンピュータへ配信します。フォルダの場所は次のとおりです。オペレーティングシステムにより異なります。

- Windows 2000/XP/2003 の場合:
C:\Documents and Settings\All Users\Application Data\Sophos\Update Manager\Update Manager\CIDs\
- Windows Vista 以降の場合:
C:\ProgramData\Sophos\Update Manager\Update Manager\CIDs\

プロキシサーバーを使用してインターネットに接続している場合は、「**プロキシサーバー経由でソフォスにアクセスする**」を選択し、プロキシの詳細を入力します。

3. 「**OS の選択**」ページで、ご使用のコンピュータで起動している OS を選択します。
 - デフォルトで「**Windows 2000 以降用**」というオプションが選択されています。
 - Mac OS X コンピュータがある場合は、「**Mac OS X 用**」チェックボックスを選択してください。後で Mac OS X コンピュータにウイルス対策ソフトをインストールできるようになります。
4. 「**ソフトウェアをダウンロードしています**」ページで、プログレスバーが表示されます。Sophos Control Center は、ソフトウェアをダウンロードします。ダウンロード終了後、「次へ」をクリックしてください。
5. 「**Windows ユーザーアカウントの詳細**」ページに、ネットワーク上のコンピュータすべてに対して有効で、かつソフトウェアのインストールに使用可能な管理者権限を持つアカウントの詳細を入力します。このアカウントは、前の手順で使用したソフォスのアカウントとは別のものです。ほとんどの場合、インストール開始前にログオンで用いたアカウントを使用することができます。

6. 「**コンピュータの保護**」 ページで、ウィザードは、ソフトウェアを自動的にインストールできるコンピュータを検索します。

自動インストールは、Windows 98 コンピュータや Mac コンピュータに対しては実行できないため、このページのリストには Windows 2000 以降のコンピュータのみが表示されます。

デフォルトで、すべてのコンピュータに対して保護が指定されています。保護を提供しないコンピュータについては、その横にあるチェックボックスのチェックを外してください。リストのチェックボックスをすべて選択、または選択をすべて解除するには、「**保護**」カラムのヘッダにあるチェックボックスを選択、または解除します。

7. 「**機能の選択**」 ページで、インストールする機能を選択します。

- ウイルス対策 (デフォルト設定)。
- Sophos Client Firewall (ライセンスで使用が許諾されている場合)。

ヒント: Sophos Client Firewall のインストールを指定したコンピュータは、ファイアウォールを有効にするため、再起動する必要があります。

- 競合他社製品の削除ツール。

「**次へ**」をクリックします。

8. 「**手動で保護する必要があるコンピュータ**」 ページで、コンピュータのリストが表示された場合は、「**印刷**」をクリックしてリストを印刷するか、「**名前を付けて保存**」をクリックしてリストのコピーを保存するか、またはコンピュータ名をメモします。「**次へ**」をクリックしてウィザードの指示に従います。

Sophos Control Center は、ここで選択したコンピュータにソフトウェアを自動インストールします。

ウイルス対策とファイアウォール保護が各コンピュータに適用されると、Sophos Control Center は、コンピュータ名の横に青いコンピュータアイコンを、そして「**更新状況**」カラムに「**最新**」と表示します。

手動でコンピュータを保護する方法の詳細は、[手動でネットワーク上のコンピュータを保護する](#) (p. 10) を参照してください。

4.1 手動でネットワーク上のコンピュータを保護する

各コンピュータは、手動で保護することができます。

1. 印刷または保存したリストにある各コンピュータへ移動します。Sophos Control Center が、ウイルス対策/ファイアウォールソフト、およびアップデート版を配置するフォルダを参照します。デフォルトのフォルダは次のとおりです。

OS	フォルダ
Windows 2000 以降	\\[サーバー名]\sophosUpdate\CIDs\Sxxx\EECSXP
Windows 98	\\[サーバー名]\sophosUpdate\CIDs\Sxxx\ES9X
Mac OS X	smb://[サーバー名]/sophosUpdate/CIDs/Sxxx/ESCOSX

注:

[サーバー名] とは、Sophos Control Center をインストールしたコンピュータ名です。

[Sxxx] は、ダウンロード中に生成される番号 (S000 など) です。

2. setup.exe (Windows の場合) または Sophos Anti-Virus.mpkg (Mac OS X の場合) をダブルクリックしてください。

Mac OS X 10.2 以降にインストールする場合は、Sophos Anti-Virus.mpkg を対象の Mac にコピーして、そこからインストールを行う必要があります。

ネットワークに常時接続していないコンピュータを保護することもできます ([ネットワークに常時接続していないコンピュータを保護する](#) (p. 11))。

4.2 ネットワークに常時接続していないコンピュータを保護する

ネットワークに常時接続していないコンピュータ (例: 社内外で使用するモバイル PC) は、社内のネットワークに接続していない間も保護することができます。

ウイルス対策とファイアウォールソフトがインストール済みのコンピュータは、社内のネットワークに接続されていない場合でも、これらのソフトウェアのアップデート版をソフォスから直接取得するように、既に環境設定されています。

ウイルス対策、またはファイアウォールソフトがインストールされておらず、ネットワークに常時接続していないコンピュータがある場合は、次に社内ネットワークに接続した際にコンピュータの保護を行ってください。この

詳細については、Sophos Control Center ヘルプの新規コンピュータの保護に関する項を参照してください。

5 コンピュータ保護の確認

ネットワーク上のコンピュータが脅威に対して保護されているか、ダッシュボードを使って確認することができます。

ダッシュボードは、ネットワークのセキュリティステータスを一目でわかるよう表示します。ダッシュボードのしきい値を設定して、指定した値を超えると警告メッセージが送信されるようにできます。

ダッシュボードを表示/非表示するには、ツールバーにある「**ダッシュボード**」ボタンをクリックしてください。

ダッシュボードの環境設定方法、および表示されるアイコンの一覧とそのステータスに関する詳細は、Sophos Control Center ヘルプを参照してください。

6 メール警告の設定

デフォルトで、デスクトップ警告は脅威が検出されたコンピュータ上のみで表示されます。これとは別に、脅威検出時に、指定したユーザーに Sophos Control Center からメール警告を送信することも可能です。

脅威検出時に送信するメール警告を設定する方法は次のとおりです。

1. 左ペインの「**環境設定**」で、「**検索の環境設定**」をクリックします。
2. 「**検索の環境設定**」ダイアログボックスで、「**メッセージング**」をクリックします。

「**メッセージング**」ダイアログボックスが表示されます。

3. 「**メール警告**」タブをクリックし、「**メール警告を送信する**」を選択してメールによる警告の送信を有効にします。
4. 「**送信するメールの内容**」パネルで、メール警告を送信するイベントの種類を選択します。

ヒント: 「疑わしい動作の検知」、「疑わしいファイルの検出」、および「アドウェアや不要と思われるアプリケーションの検出・クリーンアップ」の設定内容は Windows 2000 以降のみに適用されます。「その他のエラー」の設定内容は、Windows コンピュータにのみに適用されます。

5. 「**受信者**」パネルで、「**追加**」または「**削除**」ボタンをクリックして、メール警告の受信者アドレスを追加・削除します。追加したメールアドレスを変更するには、「**名前の変更**」をクリックします。

ヒント: MacOSX コンピュータの場合、リスト最上部の受信者のみにメール警告が送信されます。

6. SMTP サーバーの設定内容や、メール警告で使用する言語を変更するには、「**SMTP の設定**」をクリックします。

7. 「**SMTPの設定**」ダイアログボックスで、次のように詳細を設定します。
 - 「**SMTPサーバー**」テキストボックスに、SMTPサーバーのホスト名、またはIPアドレスを入力します。テスト用メール警告を送信する場合は、「テスト」をクリックします。
 - 「**SMTP送信者アドレス**」テキストボックスに、バウンスメールや配信不能レポートの送信先アドレスを入力します。
 - 「**SMTP返信先アドレス**」テキストボックスに、このメール警告に対する返信先アドレスを入力できます。メール警告は無人の送信専用メールボックスから送信されます。

ヒント: Linux および UNIX コンピュータでは、SMTP 送信者アドレスや返信先アドレス (Reply-to) は無視され、root@<ホスト名> というアドレスが使用されます。
 - 「**言語**」パネルで、ドロップダウン矢印をクリックして、メール警告で使用する言語を選択します。

ダッシュボードで表示されるしきい値を基にした、ネットワークのステータスに関するメール警告を送信するよう、Sophos Control Center を設定することもできます。詳細は、Sophos Control Center ヘルプの「警告の管理」のセクションを参照してください。

7 不要と思われるアプリケーションの検索の設定

Sophos Anti-Virusはデフォルトで、ウイルス、トロイの木馬、スパイウェア、およびワームを検出します。また、不要と思われるアプリケーション (PUA) を検出するように環境設定することもできます。

ヒント: このオプションは、Windows 2000 以降で稼動している Sophos Anti-Virus のみが対象です。

ソフォスでは、まずスケジュール検索を使用して、不要と思われるアプリケーションを検出することをお勧めしています。これによって、ネットワークで既に稼動しているアプリケーションに確実に対処することができます。その後、オンアクセス検索を有効にすることで、将来インストールされる不要と思われるアプリケーションからコンピュータを保護できます。

7.1 コンピュータのスケジュール検索を実行する

1. 左ペインの「**環境設定**」で、「**検索の環境設定**」をクリックします。
2. 「**検索の環境設定**」ダイアログボックスの「**スケジュール検索**」パネルで、「**追加**」をクリックして新規検索を作成するか、リストから検索を選択して、「**編集**」をクリックして設定内容を編集します。
3. 「**スケジュール検索の設定**」ダイアログボックスで、画面下部の「**環境設定**」をクリックします。
4. 「**検索・クリーンアップ設定**」ダイアログボックスで、「**検索**」タブをクリックします。「**検索オプション**」パネルで、「**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**」チェックボックスを選択し、「**OK**」をクリックします。

検索実行後 Sophos Anti-Virus が不要と思われるアプリケーションの検出をレポートすることがあります。この場合は、アプリケーションを認証するか、またはコンピュータから除去することができます。

7.2 使用するアプリケーションを認証する

スケジュール検索で、アドウェアや不要と思われるアプリケーションとして検出されたアプリケーションを認証することができます。

アプリケーションの認証方法は次のとおりです。

1. 左ペインの「**環境設定**」で、「**検索の環境設定**」をクリックします。
2. 「**検索の環境設定**」ダイアログボックスで、「**認証**」をクリックします。

3. 「**認証マネージャ**」ダイアログボックスで、次のいずれかを実行します。
 - 認証するアプリケーションを選択します。「**追加**」をクリックして、「**認証済みアドウェアや不要と思われるアプリケーション**」リストに追加します。
 - 当該のアプリケーションが表示されない場合は、「**新規エントリ**」をクリックします。表示されるダイアログで、「**ソフオスアプリケーションリスト**」のリンクをクリックし、不要と思われるアプリケーションのリストを表示します。認証するアプリケーションを探し、「**名前**」フィールドにアプリケーション名を入力します。

7.3 使用しないアプリケーションをクリーンアップする

スケジュール検索で、アドウェアや不要と思われるアプリケーションとして検出されたアプリケーションをクリーンアップすることができます。

アプリケーションをクリーンアップする方法は次のとおりです。

1. 左ペインの「**アクション**」で、「**警告とエラーの対処**」をクリックします。

「**警告とエラーの対処**」ダイアログボックスが表示されます。

2. 除去する各アプリケーションのチェックボックスを選択するか、または「**すべてを選択**」をクリックして、「**クリーンアップ**」をクリックします。

これにより、選択したアプリケーションの既知のコンポーネントすべてが、選択したコンピュータから除去されます。クリーンアップには多少時間がかかる場合があります。

ヒント: なお、一部のアプリケーションについては、Sophos Control Center でクリーンアップできないものもあります。この場合は、対象のコンピュータに移動し、Sophos Anti-Virus を使用してアプリケーションをクリーンアップしてください。

複数のコンポーネントで構成される一部のアプリケーションをコンピュータから完全にクリーンアップするには、コンピュータの再起動が必要な場合もあります。この場合は、対象のコンピュータにメッセージが表示され、今すぐ、または後でコンピュータを再起動するか選択できます。クリーンアップは、コンピュータを再起動するまでは完全に終了しません。

ソフォス Web サイト上の特定のアプリケーションに関する情報を参照するには、「**警告とエラーの対処**」ダイアログボックスで、該当するアプリケーション名をクリックします。

「**消去**」をクリックすると、選択したアプリケーションがリストから消えますが、クリーンアップや認証は行われません。

7.4 アドウェアおよび不要と思われるアプリケーションのオンアクセス検索を設定する

1. 左ペインの「**環境設定**」で、「**検索の環境設定**」をクリックします。
「**検索の環境設定**」ダイアログボックスが表示されます。
2. 「**オンアクセス検索**」をクリックします。
「**オンアクセス検索の設定**」ダイアログボックスが表示されます。
3. 「**検索オプション**」パネルで、「**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**」チェックボックスを選択します。「**OK**」をクリックします。

アプリケーションの中には、ファイルを「**監視**」して、頻繁にアクセスしようとするものもあります。オンアクセス検索が有効になっている場合は、各アクセスが検出され、そのたびに警告が送信されます。

8 ウイルスの対処

ウイルスをクリーンアップする方法は次のとおりです。

1. Sophos Control Center の「ダッシュボード」で、「ウイルス/スパイウェア」リンクをクリックします。

「警告とエラーの対処」ダイアログボックスで、感染したコンピュータのリストと、ウイルスの詳細が表示されます。

2. クリーンアップするウイルスを選択し、「クリーンアップ」をクリックします。

これにより、感染しているファイルまたはブートセクタからウイルスが除去されます。ただし、ウイルスによってドキュメントに加えられた変更は、クリーンアップで修復されません。また、プログラムのクリーンアップはあくまでも暫定対策なので、後で必ず、オリジナルのディスクや感染する前に作成したバックアップを使用してクリーンアップしたプログラムを入れ替える必要があります。クリーンアップには多少時間がかかる場合があります。

なお、一部のウイルスについては、Sophos Control Center でクリーンアップできないものもあります。この場合は、対象のコンピュータに移動し、Sophos Anti-Virus を使用してウイルスをクリーンアップしてください。

複合型脅威をコンピュータから削除する前に、コンピュータに対してスケジュール設定したフル検索を実行し、複合型脅威に含まれる全コンポーネントを特定することをお勧めします。

ソフォスWebサイト上の特定のウイルスに関する情報を参照するには、「警告とエラーの対処」ダイアログボックスで、該当するウイルス名をクリックします。

9 ファイアウォールの設定

Sophos Client Firewall を新規インストールした後は、必要な送受信トラフィックを許可する設定になっています。

ヒント: Sophos Client Firewall は IPv6 には対応していません。バージョン 1 は IPv6 パケットを通過させません。バージョン 1.5 およびバージョン 2.0 では、設定に応じて、すべての IPv6 パケットがブロックまたは許可されます。

9.1 ファイアウォールを設定する

随時、トラフィックを許可/ブロックするようファイアウォールを設定できます。デフォルトで、ファイアウォールは、必要な受信トラフィックとすべての送信トラフィックを許可する設定になっています。

ファイアウォールの設定方法は次のとおりです。

1. 左ペインの「**環境設定**」で、「**ファイアウォールの環境設定**」をクリックします。
2. 「**ファイアウォールの環境設定 ウィザード**」で、「**次へ**」をクリックします。
3. 「**ファイアウォールの環境設定**」ページで、次のいずれかのオプションを選択します。

■ 1種類の設定 (固定マシン用)

デスクトップなど、常に社内ネットワークに接続されているコンピュータに対して選択します。

■ 2種類の設定 (モバイル PC 用)

社内ネットワークや社外など、コンピュータを使う場所に応じて、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ます。「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。

■ すべてのトラフィックを許可する

ファイアウォールを無効にして、すべてのトラフィックを許可する場合に選択します。

4. 前のステップで、「**2種類の設定(モバイルPC用)**」を選択した場合、「**ネットワークの識別方法**」ページで、ネットワークの識別方法として、DNS または ゲートウェイを設定します。

ヒント:「ネットワークの識別方法」ページは、「**2種類の設定(モバイルPC用)**」を選択した場合のみに表示されます。

ここで指定するネットワークに接続しているかどうかによって、Sophos Control Center で各コンピュータに異なるファイアウォールの設定が適用されます。

5. 「**操作モード**」ページで、ファイアウォールが送受信トラフィックを処理するモードを選択します。

■ 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

ご使用のコンピュータの必要な送信トラフィックに対してのみ、ネットワークとインターネットへのアクセスを許可しますが、受信トラフィックはブロックします。このモードでアプリケーションは認証されません。

■ 送受信トラフィックをブロックする

このモードを選択すると、ファイアウォールは、許可したアプリケーション以外のすべての送信トラフィックをブロックします。アプリケーションを追加するには、このオプションの右側にある「**信頼**」をクリックしてください。「**信頼**」できるアプリケーションに対しては、すべての送受信トラフィックが許可されます。

■ 監視する

設定したルールすべてをコンピュータで実行する他、不明なトラフィックすべてのネットワークとインターネットへのアクセスを許可します。ネットワークの情報がコンソールにレポート送信されます。ネットワークの情報収集を行い、それに基づいてルールを作成する場合に選択してください。

■ カスタム

カスタム設定を適用します。ファイアウォールの詳細設定を表示するには、「**詳細設定**」をクリックします。

ヒント:詳細オプションは非常に高度な設定であるため、変更内容が与える影響を理解している場合のみご使用ください。

ファイアウォールの詳細設定については、**Sophos Endpoint Security and Control ヘルプ**を参照してください。

6. ネットワーク上の他のコンピュータが、ローカルプリンタとフォルダを共有できるようにする場合は、「**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。
7. 「**2種類の設定(モバイルPC用)**」を選択した場合、セカンダリロケーション(社外で使用する場合)用に、操作モード、およびファイルとプリンタの共有(ステップ5、6を参照)を設定する必要があります。

後で設定内容を変更する場合は、このウィザードを再実行することができます。

ファイアウォールの設定を完了すると、「**ファイアウォール-イベントビューア**」で、ファイアウォールでブロックされたアプリケーションなど、ファイアウォールのイベントを表示できます。詳細は、Sophos Control Center ヘルプを参照してください。

9.2 ファイアウォールがブロックしたアイテムに対処する

Sophos Control Center は、実行対象のアプリケーションやプロセスをブロックすることがあります。その場合は、次の操作を行ってください。

1. Sophos Control Center の「**ダッシュボード**」で、「**ファイアウォール**」リンクをクリックします。
2. 「**ファイアウォール-イベントビューア**」ダイアログボックスで、許可する、または新しいルールを作成するアプリケーションのエントリを選択します。「**ルールの作成**」をクリックします。
3. 表示されるダイアログボックスで、アプリケーションを許可するか、または既存のプリセットルールを使って、アプリケーションに対してルールを作成するかを選択します。

10 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。

- 「SophosTalk」 ユーザーフォーラム (英語) (<http://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。 <http://www.sophos.co.jp/support/>
- 製品ドキュメントのダウンロード。 <http://www.sophos.co.jp/support/docs/>
- メールによるお問い合わせ。ソフォス製品のバージョン番号、OS および適用しているパッチの種類、エラーメッセージの内容などを、support@sophos.co.jp までお送りください。

11 著作権情報

Copyright © 2011 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、写真複製、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 および Sophos Anti-Virus は、Sophos Limited 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。

このドキュメントに説明のあるソフォスのソフトウェアには、一般公衆利用許諾契約書 (Common Public License、あるいは単に CPL) に基づいてユーザーの使用が許諾(またはサブライセンス)されているソフトウェア・プログラムが含まれています。または含まれている可能性があります。CPL に基づき使用が許諾され、オブジェクトコード形式で頒布されるいかなるソフトウェアも、CPL により、オブジェクトコード形式のユーザーへの、このようなソフトウェアのソースコードの開示が義務付けられています。CPL に基づくこのようなソフトウェアのソースコードの入手を希望する場合は、ソフォスに書面でお申込みいただくか、次のメールアドレスまでご連絡ください:

support@sophos.co.jp。または次のリンク先よりご連絡ください:

<http://www.sophos.co.jp/support/queries/enterprise.html>。ソフォス製品に含まれるこのようなソフトウェアの使用許諾契約書は、次のリンク先をご覧ください: <http://opensource.org/licenses/cpl1.0.php>。

ACE™, TAO™, CIAO™, and CoSMIC™

ACE¹, TAO², CIAO³, and CoSMIC⁴ (henceforth referred to as "DOC software") are copyrighted by Douglas C.Schmidt⁵ and his research group⁶ at Washington University⁷, University of California⁸, Irvine, and Vanderbilt University⁹, Copyright © 1993-2005, all rights reserved.

Since DOC software is open-source, free 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 code built using DOC software.

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 do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, 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 us¹⁰ know so we can promote your project in the DOC software success stories¹¹.

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. Moreover, 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 companies¹² 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.

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.

The ACE¹³, TAO¹⁴, CIAO¹⁵, and CoSMIC¹⁶ web sites are maintained by the DOC Group¹⁷ at the Institute for Software Integrated Systems (ISIS)¹⁸ and the Center for Distributed Object Computing of Washington University, St. Louis¹⁹ for the development of open-source software as part of the open-source software community²⁰. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, 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. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me²¹ know.

Douglas C. Schmidt²²

References

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>

3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. mailto:doc_group@cs.wustl.edu
11. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
12. <http://www.cs.wustl.edu/~schmidt/commercial-support.html>
13. <http://www.cs.wustl.edu/~schmidt/ACE.html>
14. <http://www.cs.wustl.edu/~schmidt/TAO.html>
15. <http://www.dre.vanderbilt.edu/CIAO/>
16. <http://www.dre.vanderbilt.edu/cosmic/>
17. <http://www.dre.vanderbilt.edu/>
18. <http://www.isis.vanderbilt.edu/>
19. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
20. <http://www.opensource.org/>
21. <mailto:d.schmidt@vanderbilt.edu>
22. <http://www.dre.vanderbilt.edu/~schmidt/>

iMatix SFL

This product uses parts of the iMatix SFL, Copyright © 1991-2000 iMatix Corporation
<<http://www.imatix.com>>.