

# SOPHOS

## Sophos Control Center 4.1 アップグレードガイド

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 Sophos Control Center 4 の新機能.....	4
3 システム要件.....	6
4 アップグレードにあたっての準備.....	7
5 Sophos Control Center のアップグレード.....	9
6 コンピュータ保護の確認.....	10
7 ファイアウォールの設定.....	11
8 アプリケーション コントロールの設定.....	12
9 デバイスコントロールの設定.....	14
10 テクニカルサポート.....	18
11 著作権情報.....	19

# 1 このガイドについて

この Sophos Control Center 4.1 アップグレードガイドは、次の操作方法について説明します。

- Sophos Control Center バージョン 2.0 またはバージョン 2.5 から Sophos Control Center バージョン 4.1 へのアップグレード。
- Sophos Anti-Virus および Sophos Client Firewall (ライセンスでファイアウォールの使用が許諾されている場合) から Sophos Endpoint Security and Control へのアップグレード。

Sophos PureMessage の旧バージョンをご使用で、最新バージョンの Sophos PureMessage へのアップグレードがライセンスで許諾されている場合、アップグレード方法は「**Sophos PureMessage アップグレードガイド**」をご覧ください。

- 新しいセキュリティ機能を設定する。

このガイドには説明のない、Sophos Control Center のその他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 Sophos Control Center 4 の新機能

最新版の Sophos Control Center は、次のような新機能を備えています。

### Sophos Control Center 4.1

#### OS との互換性

Sophos Control Center バージョン 4.1 は、次の OS との互換性があります。

- Windows Server 2008 R2
- Windows 7

**ヒント:** Sophos Control Center バージョン 4.0 は、これよりも前のバージョンの Windows OS に対応しています。システム要件の詳細は、[システム要件](#) (p. 6) を参照してください。

### Sophos Control Center 4.0

#### 最新版のエンドポイント セキュリティソフトに対応

最新版の Sophos Control Center は、Windows 2000 以降のエンドポイントコンピュータで、最新のウイルス対策およびファイアウォール製品を提供する Sophos Endpoint Security and Control を使用することを可能にします。

#### ダッシュボード

Sophos Control Center にはダッシュボードが追加され、ネットワークのセキュリティステータスが一目でわかるようになりました。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。ダッシュボードの設定方法の詳細は、[Sophos Control Center ヘルプ](#) を参照してください。

#### アプリケーション コントロール

Sophos Control Center では、ビジネス環境での使用は適切でないと考えられるアプリケーションを検出し、ブロックすることができます。アプリケーション コントロールに関する詳細は、[アプリケーション コントロールの設定](#) (p. 12) を参照してください。

#### デバイスコントロール

デバイスコントロール機能では、各コンピュータにおける、認証されていない外付けのハードディスク機器、リムーバブルストレージメディア、および無線接続機器の使用を防止することができます。デバイスコントロールに関する詳細は、[デバイスコントロールの設定](#) (p. 14) を参照してください。

### **Sophos PureMessage および Sophos for Microsoft SharePoint の起動**

Sophos Control Center と同じコンピュータにインストール済みの Sophos PureMessage や Sophos for Microsoft SharePoint コンソールを、Sophos Control Center コンソールから起動することができます。

### 3 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。

## 4 アップグレードにあたっての準備

ヒント:

- アップグレード開始前に、既存バージョンの Sophos Control Center のバックアップを作成することをお勧めします。
- Sophos Control Center インストールウィザードを完了後、Sophos Control Center をアップグレードしたコンピュータからログオフして再ログオンするか、またはコンピュータを再起動する必要があります。
- Sophos Client Firewall をインストールする場合は(ライセンスで使用が許諾されている場合)、インストール後、ファイアウォールを有効にするため、各コンピュータを再起動する必要があります。

Sophos Control Center 4.0 にアップグレード後、旧バージョンの Sophos Control Center で生成されたファイアウォール警告を表示することはできません。アップグレードを行う前に、すべてのファイアウォール警告に対処しておくことをお勧めします。

### 4.1 前提条件

Sophos Control Center をアップグレードし、続いてネットワーク上の管理対象コンピュータにあるソフトウェアをアップグレードするには、次の前提条件を満たしている必要があります。

- **システム要件** (p.6) に記載されているハードウェアおよびソフトウェア要件をすべて満たしている。
- Sophos Control Center をアップグレードするコンピュータに対する管理者権限がある。

#### Windows OS 環境のエンドポイントコンピュータの準備

Windows OS 環境のエンドポイントコンピュータで、次の操作を行ってください。

- すべての Windows XP コンピュータで「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。

- Sophos Client Firewall をインストールする Windows 2000 以降のコンピュータすべてから、他社製ファイアウォールソフトをすべて削除する (Windows ファイアウォールは除く)。

## **Sophos Client Firewall をインストールしないエンドポイントコンピュータの準備**

Sophos Client Firewall をインストールしない Windows XP (SP 2) クライアントマシンがあり、当該のコンピュータで 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。  
操作方法は、<http://www.sophos.co.jp/support/knowledgebase/article/11738.html>を参照してください。
- TCP ポート 8192、8193 および 8194 を開放する。
- 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。
- コンピュータを再起動して変更内容を有効にする。

## 5 Sophos Control Center のアップグレード

既存の設定を維持しつつ、Sophos Control Center をアップグレードするには、旧バージョンの 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。

1. 開いているソフォスのアプリケーションをすべて閉じます。
2. 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、Sophos Control Center のインストーラをダウンロードし、実行します。

3. **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。
4. 「**ようこそ**」ページで、「**次へ**」をクリックします。

「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、デフォルト設定をそのまま選択します。

5. アップグレード手順が完了したら、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。

Sophos Control Center のインストール完了後、エンドポイントコンピュータは、最新のエンドポイントソフトのダウンロードが完了すると、自身を自動アップデートします。

**ヒント:** Windows 98 または Mac OS X 環境のエンドポイントコンピュータでは、手動で Sophos Anti-Virus をアップグレードする必要があります。手動でコンピュータを保護する方法の詳細は、「**Sophos Control Center スタートアップガイド**」を参照してください。

## 6 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。

## 7 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、すべてのトラフィックを許可する設定になっています。その後、必要なトラフィックのみを許可/ブロックするよう設定できます。

ファイアウォールをはじめて設定する場合、操作方法は **Sophos Control Center ヘルプ** を参照してください。

**ヒント:** Sophos Client Firewall は、IPv6 に対応していません。Sophos Client Firewall バージョン 1 は IPv6 パケットを通過させます。Sophos Client Firewall 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。

## 8 アプリケーション コントロールの設定

Sophos Control Center では、アプリケーション コントロール機能で「管理対象アプリケーション」、すなわち、セキュリティ脅威はもたらさないものの、管理者が業務上の使用は不適切と判断する正規のアプリケーションを検知・ブロックすることができます。このようなアプリケーションには、インスタントメッセージング (IM) クライアント、VoIP クライアント、デジタル画像ソフト、メディアプレーヤー、ブラウザプラグインなどがあります。

**ヒント:** このオプションは、Sophos Endpoint Security and Control for Windows 2000 以降のみに適用されます。

管理対象アプリケーションのリストは、ソフォスが定期的に更新し、提供しています。お客様自身でリストに新しいアプリケーションを追加することはできません。新たな正規アプリケーションをアプリケーションコントロールの対象にする必要がある場合は、ソフォスまでご連絡ください。詳細は、ソフォス サポートデータベースの文章 35330

(<http://www.sophos.co.jp/support/knowledgebase/article/35330.html>) をご覧ください。

アプリケーション コントロールのイベントに関する詳細は、Sophos Control Center ヘルプを参照してください。

### 8.1 アプリケーション コントロールを設定する

ネットワーク上で使用をコントロールしたいアプリケーションをオンアクセス検索するように Sophos Control Center を設定することができます。

1. 左ペインの「**環境設定**」で、「**アプリケーション コントロールの環境設定**」をクリックします。

「**アプリケーション コントロールの環境設定**」ダイアログボックスが表示されます。

2. 「**検索**」タブで、オプションを次のように設定します。
  - オンアクセス検索を有効にするには、「**オンアクセス検索を有効にする**」チェックボックスを選択します。アプリケーションの検出はするものの、オンアクセスでのブロックは実行しない場合は、「**検出するが、実行は許可する**」チェックボックスを選択します。
  - オンデマンド/スケジュール検索を有効にするには、「**オンデマンド/スケジュール検索を有効にする**」チェックボックスを選択します。

**ヒント:** ウイルス対策および HIPS ポリシーの設定内容で、検索するファイルが指定されます (拡張子と除外の設定など)。

3. 「**認証**」タブをクリックし、管理の対象にするアプリケーションを選択します。

アプリケーションの選択方法の詳細は、[管理するアプリケーションを選択する](#) (p. 13) を参照してください。

## 8.2 管理するアプリケーションを選択する

デフォルトで、すべてのアプリケーションが許可されています。アプリケーションコントロール機能で、使用をコントロールするアプリケーションを選択する方法は次のとおりです。

1. 左ペインの「**環境設定**」で、「**アプリケーションコントロールの環境設定**」をクリックします。
2. 「**アプリケーションコントロールの環境設定**」ダイアログボックスで、「**認証**」タブをクリックします。
3. 「**アプリケーションの種類**」(たとえば「**ファイル交換**」など)を選択します。

選択したタイプに属するアプリケーションの一覧が「**認証済み**」リストに表示されます。

- 特定のアプリケーションをブロックするには、それを選択して、以下のような「**追加**」ボタンをクリックし、「**ブロック**」リストへ移動します。



- 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場合は、「**今後ソフォスが追加するアプリケーションすべて**」を「**ブロック**」リストに移動します。
- 特定の種類のアプリケーションすべてをブロックするには、以下のような「**すべて追加**」ボタンをクリックして、すべてのアプリケーションを「**認証済み**」リストから「**ブロック**」リストへ移動します。



管理対象アプリケーションのアンインストール方法の詳細は、Sophos Control Center ヘルプを参照してください。

## 9 デバイスコントロールの設定

**重要:** ソフォスのデバイスコントロール機能は、他社製デバイスコントロールソフトがインストール済みの環境にはインストールしないでください。

デバイスコントロール機能では、各コンピュータにおける、認証されていない外付けのハードディスク機器、リムーバブルストレージメディア、および無線接続機器の使用を防止することができます。これによって、事故などによるデータ流出リスクを大幅に削減することができ、また、ユーザーが社内ネットワークにソフトウェアを持ち込むことを制限できます。

また、リムーバブルストレージデバイス、光学ディスクドライブ、およびフロッピーディスクドライブに対して、読み取り専用の制限を設けることもできます。

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。

はじめてデバイスコントロール機能を有効にする際は、次のように設定することを推奨します。

- 使用をコントロールするデバイスの種類を選択する。
- デバイスをブロックせずに検出する。
- デバイスコントロールの警告を設定する。
- デバイスを検知・ブロックするか、またはストレージデバイスに対して読み取り専用の制限を設ける。

デバイスコントロールのイベントに関する詳細は、Sophos Control Center ヘルプを参照してください。

### 9.1 コントロールできるデバイスの種類

デバイスコントロールでブロックできるデバイスは3種類あります。ストレージデバイス、ネットワークデバイス、短距離無線通信デバイスの3つです。

#### ストレージデバイス

- リムーバブルストレージデバイス (USB フラッシュドライブ、PC カードリーダー、外付けハードディスクドライブなど)
- 光学メディアドライブ (CD-ROM/DVD ドライブ/Blu-ray ドライブ)
- フロッピーディスクドライブ

- セキュアなリムーバブルストレージドライブ (SanDisk Cruzer Enterprise、SanDisk Cruzer Enterprise FIPS Edition、Kingston Data Traveler Vault - Privacy Edition、Kingston Data Traveler BlackBox、IronKey Enterprise Basic Edition などのハードウェア暗号化対応 USB フラッシュメモリ)

セキュアなリムーバブルストレージのカテゴリを使うと、他のリムーバブルストレージデバイスをブロックしつつ、カテゴリに該当するセキュアなリムーバブルストレージデバイスの使用を簡単に許可できます。セキュアなリムーバブルストレージディスクについて、最新の対応一覧は、ソフォス Web サイト ([www.sophos.co.jp](http://www.sophos.co.jp)) をご覧ください。

## ネットワークデバイス

- モデム
- ワイヤレス機器 (Wi-Fi インターフェース、802.11 規格)

ネットワークインターフェースに対しては、「ブリッジ接続をブロックする」という追加のアクセスレベルを設定することができます。これによって、コンピュータをネットワークから切り離れたときに、ネットワークデバイス (Wi-Fi アダプタなど) は有効になります。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てください。

**ヒント:** 「ブリッジ接続をブロックする」オプションは、企業ネットワークと外部ネットワーク間などのブリッジ接続を阻止します。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。

## 短距離無線通信デバイス

- Bluetooth インターフェース
- 赤外線 (IrDA 赤外線インターフェース)

デバイスコントロールでは、内蔵型と外付け両方のデバイス/インターフェースがブロックされます。たとえば、Bluetooth インターフェースをブロックすると、次のどちらのインターフェースもブロックされます。

- コンピュータに内蔵されている Bluetooth インターフェース
- コンピュータに接続されている USB ベースの Bluetooth アダプタ

## 9.2 デバイスコントロールを設定する

ネットワーク上で使用をコントロールしたいデバイスをオンアクセス検索するように Sophos Control Center を設定することができます。

1. 左ペインの「**環境設定**」で、「**デバイスコントロールの環境設定**」をクリックします。

「**デバイスコントロールポリシー**」ダイアログボックスが表示されます。

2. 「**環境設定**」タブで、オプションを次のように設定します。

- デバイスコントロールを有効にするには、「**デバイスコントロールを有効にする**」チェックボックスを選択します。デバイスの検出はするものの、ブロックは実行しない場合は、「**デバイスを検出するが、ブロックしない**」チェックボックスを選択します。
- デバイスの種類ごとにアクセスレベルを設定するには、デバイスタイプの横にある「**ステータス**」カラムをクリックし、表示されるドロップダウン矢印をクリックします。許可するアクセスの種類を選択します。

デフォルトで、デバイスにはフルアクセスが許可されています。リムーバブルストレージデバイス、光学ディスクドライブ、およびフロッピーディスクドライブについては、「**ブロック**」または「**読み取り専用**」に変更できます。セキュアなリムーバブルストレージデバイスについては、「**ブロック**」に変更できます。

デバイスコントロール警告の設定方法は、Sophos Control Center ヘルプを参照してください。

## 9.3 デバイスを除外する

デバイスをデバイスコントロールポリシーの対象から除外することができます。

デバイスは個別に除外するか(「このデバイスのみ」)、またはモデル別に除外できます(「このモデルのデバイスすべて」)。除外の設定は、必ず、個別かモデル別か、どちらか1つのレベルで設定してください。両方設定した場合、個別のデバイスの設定が優先されてしまいます。

デバイスを除外する方法は次のとおりです。

1. 「**表示**」メニューの「**デバイスコントロールのイベント**」をクリックします。

「**デバイスコントロール-イベントビューア**」ダイアログボックスが表示されます。

2. 特定のイベントだけを表示する場合は、「**検索の条件**」ペインで、適宜フィルタを設定します。そして、「**検索**」をクリックしてイベントを表示します。
3. 除外するデバイスのエントリを選択し、「**デバイスの除外**」をクリックします。

「**デバイスの除外**」ダイアログボックスが表示されます。「**デバイスの詳細**」に、デバイスのタイプ、モデル、および ID が表示されます。

## 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](mailto: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](mailto: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™**

ACE<sup>1</sup>, TAO<sup>2</sup>, CIAO<sup>3</sup>, and CoSMIC<sup>4</sup> (henceforth referred to as "DOC software") are copyrighted by Douglas C.Schmidt<sup>5</sup> and his research group<sup>6</sup> at Washington University<sup>7</sup>, University of California<sup>8</sup>, Irvine, and Vanderbilt University<sup>9</sup>, 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 us<sup>10</sup> know so we can promote your project in the DOC software success stories<sup>11</sup>.

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 companies<sup>12</sup> 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 ACE<sup>13</sup>, TAO<sup>14</sup>, CIAO<sup>15</sup>, and CoSMIC<sup>16</sup> web sites are maintained by the DOC Group<sup>17</sup> at the Institute for Software Integrated Systems (ISIS)<sup>18</sup> and the Center for Distributed Object Computing of Washington University, St. Louis<sup>19</sup> for the development of open-source software as part of the open-source software community<sup>20</sup>. 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 me<sup>21</sup> know.

Douglas C. Schmidt<sup>22</sup>

## 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](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/>