



# Data Migration Assistant ユーザ ガイド Release 5.1(1)

---

このマニュアルでは、Data Migration Assistant (DMA) について説明し、DMA をインストールして使用する方法および関連情報を示します。

このマニュアルは、Cisco Unified CallManager バージョン 4.0(x) または 4.1(x) を実行している場合に、Cisco Unified CallManager 5.1(1) にアップグレードする準備が整った時点でお読みください。

本書の内容は、次のとおりです。

- [DMA の概要](#)
- [DMA の取得](#)
- [DMA のインストール](#)
- [DMA の削除](#)
- [始める前に](#)
- [CAR データの移行](#)
- [Cisco Unified CallManager Attendant Console データの移行](#)
- [既存の CAPF 1.0\(1\) データの移行](#)
- [4.0 サブスクリバ サーバから 4.0 パブリッシャ データベース サーバへの CAPF 1.0\(1\) データのコピー](#)
- [新しい CAPF 証明書の生成](#)
- [DMA の実行](#)
- [DMA バックアップ情報ファイル](#)
- [DMA の管理とトラブルシューティング](#)
- [技術情報の入手方法](#)
- [テクニカル サポート](#)
- [その他の資料および情報の入手方法](#)

## DMA の概要

DMA は、次の各項で説明しているように、Cisco Unified CallManager および Cisco Emergency Responder のデータを移行します。

DMA は、バージョン 4.0(x) および 4.1(x) の Cisco Unified CallManager データを、Cisco Unified CallManager 5.1(1) が読み取り可能な形式でバックアップすることで、Cisco Unified CallManager データをバージョン 4.0(x) および 4.1(x) から Cisco Unified CallManager 5.1(1) に移行する上での最初のステップを支援します。Cisco Unified CallManager 4.1(x) は Windows 環境で動作し、Cisco Unified CallManager 5.1(1) は Linux 環境で動作するため、DMA は Windows ベースのデータを、Linux がインポートできる形式にエクスポートします。Cisco Unified CallManager 5.1(1) のインストールプロセスで、Cisco Unified CallManager 5.1(1) の必要に応じて、バックアップされたデータが変換され、それによってデータ移行が完了します。

DMA は、Tape Archive (TAR; テープアーカイブ) ファイルにエクスポートしたデータを、指定された場所に保存します。

Cisco Unified CallManager 5.1(1) にアップグレードする前に、Cisco Unified CallManager パブリッシャサーバ上で DMA をインストールして実行する必要があります。DMA の実行後に Cisco Unified CallManager に設定変更を加えた場合、アップグレードするとその変更が失われます。

DMA は、Cisco Unified CallManager データをエクスポートするだけでなく、次の関連アプリケーションのデータもエクスポートします。

- Cisco Unified CallManager Attendant Console (AC)
- Cisco Extension Mobility (EM; エクステンション モビリティ)
- CDR Analysis and Reporting (CAR)
- Certificate Authority Proxy Function (CAPF; 認証局プロキシ関数)
- Certificate Trust List (CTL; 証明書信頼リスト)
- International Dial Plan (IDP)

DMA は、次の情報をエクスポートしません。

- カスタム Music on Hold (MOH; 保留音) ファイル : Cisco Unified CallManager 5.1(1) にアップグレードした後に、このファイルを再度適用する必要があります。
- TFTP 電話機ロード ファイル : Cisco Unified CallManager 5.1(1) にアップグレードした後に、このファイルを再度適用する必要があります。
- Cisco Unified CallManager サブスクリバサーバ上のファイル : サブスクリバサーバは、Cisco Unified CallManager アップグレードプロセスの一部として、必要な情報をパブリッシャサーバから取得します。

また、DMA は、Cisco Emergency Responder 1.3 をアップグレードするためにデータをエクスポートします。詳細については、『*Cisco Emergency Responder Administration Guide*』を参照してください。

## DMA の取得

ディスク上に DMA ソフトウェアが存在しない場合は、次の手順を実行して、DMA ソフトウェアを Cisco Unified CallManager パブリッシャ サーバにダウンロードします。Cisco.com の登録ユーザだけがこのソフトウェアをダウンロードできます。

### 手順

---

**ステップ 1** 次の URL にアクセスします。

<http://cco/cgi-bin/tablebuild.pl/cmva-3des>

**ステップ 2** DMA ファイルを選択します。

**ステップ 3** プロンプトに従い、必要な情報を入力して、ソフトウェアをダウンロードします。

---

## DMA のインストール

この項では、DMA のインストールおよびその手順について詳しく説明します。次のトピックについて取り上げます。

- [インストール前のガイドラインと手順 \(P.4\)](#) : DMA をインストールする前に、この情報を確認してください。
- [DMA のインストール手順 \(P.5\)](#) : この手順に従って、DMA をインストールします。

### インストール前のガイドラインと手順

DMA をインストールする前に、次のガイドラインを確認し、適切な手順を実行してください。

- DMA をサーバにインストールする前に、次のいずれかのサポート対象製品がサーバにインストールされていることを確認します。
  - Cisco Unified CallManager 4.1(x) (パブリッシャとして設定されていること)
  - Cisco Emergency Responder 1.3



**(注)** DMA インストーション ウィザードは、サポート対象製品が存在するかどうかを確認します。サーバにサポート対象製品がインストールされていない場合は、DMA をインストールできません。

- Terminal Services を使用して DMA をインストールしないでください。
- Virtual Network Computing (VNC) を使用して DMA をインストールできます。VNC の詳細については、最新バージョンの『*Using Virtual Network Computing*』を参照してください。このマニュアルは、次の URL で入手できます。  
[http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel\\_os/vnc/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/iptel_os/vnc/index.htm)
- DMA は、Cisco Unified CallManager 4.1(x) サーバの C:\ ドライブ上に 4 GB の空きディスク領域を必要とします。
- Cisco Security Agent for Unified CallManager を無効にします (有効になっている場合)。



**(注)** DMA を実行する前に Cisco Security Agent for Unified CallManager のアンインストールが必要になることがあります。問題がある場合は、詳細についてシスコのサポートにお問い合わせください。

インストールの完了後、必ず CSA を有効にしてください。

CSA を無効および有効にする方法については、『*Installing Cisco Security Agent for Unified CallManager*』を参照してください。このマニュアルは、次の URL で入手できます。

[http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_callmg/sec\\_vir/csa/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/csa/index.htm)

## DMA のインストール手順

DMA をインストールするには、次の手順を実行します。

この手順は、完了までに約 20 分かかります。

DMA をインストールする前に、P.4 の「インストール前のガイドラインと手順」の情報を確認してください。



(注)

以前のバージョンの DMA がインストールされている場合は、別のバージョンをインストールする前に、以前のバージョンを削除する必要があります。詳細については、P.7 の「DMA の削除」を参照してください。

### 手順

**ステップ 1** Windows Administrator としてサーバにログインします。

**ステップ 2** 次のいずれかの操作を実行します。

- DMA インストールディスクを持っている場合は、そのディスクを挿入します。
- ダウンロードした DMA がある場合は、DMA を保存したフォルダに移動し、**DataMigrationAssistant-5-0-4.exe** をダブルクリックします。

DMA Welcome ウィンドウが表示されます。

**ステップ 3** DMA Welcome ウィンドウで、**Next** をクリックします。

License ウィンドウが表示されます。

**ステップ 4** ライセンス契約に同意し、**Next** をクリックします。Informix Password ウィンドウが表示されます。

**ステップ 5** **Informix Password** テキスト ボックスに、Informix Database Server (IDS) のパスワードを入力します。

パスワードは、次の各文字タイプを少なくとも 1 つ使用して 8 ~ 14 文字にする必要があります。

- 大文字 (A ~ Z)
- 小文字 (a ~ z)
- 数字 (0 ~ 9)
- 特殊文字 ( { } , . < > : ? / | \ ` ~ ! @ \$ ^ & \* ( ) \_ - + )



注意

DMA のインストール後に Informix パスワードを変更しないでください。このパスワードを変更すると、DMA バックアップが失敗します。

**ステップ 6** **Confirm Password** テキスト ボックスに、パスワードを再度入力します。

Ready to Install the Program ウィンドウが表示されます。

**ステップ 7** Ready to Install ウィンドウで、**Install** をクリックします。

インストールが開始されます。Installing Data Migration Assistant ウィンドウに、インストールの進捗状況が表示されます。

約 20 分後、InstallShield Wizard Completed ウィンドウが表示されます。

**ステップ 8** InstallShield Wizard Completed ウィンドウで、**Finish** をクリックします。

サーバを再起動するように要求するプロンプトが表示されます。

**ステップ 9** **Yes** をクリックして、サーバを再起動します。

サーバが再起動すると、DMA のインストールが完了します。

---

## DMA の削除

別の DMA バージョンをインストールする前に、DMA、および DMA と共にインストールされたアプリケーションを削除する必要があります。手順については、次の各項を参照してください。

- [DMA のアンインストール \(P.7\)](#)
- [Informix Dynamic Server の削除 \(P.7\)](#)
- [Informix Client SDK のアンインストール \(P.8\)](#)

## DMA のアンインストール

DMA をアンインストールするには、次の手順を実行します。

### 手順

- 
- ステップ 1** [スタート]>[設定]>[コントロール パネル]>[アプリケーションの追加と削除]の順に選択します。
  - ステップ 2** [アプリケーションの追加と削除] ウィンドウで、**Cisco Data Migration Assistant** を選択します。
  - ステップ 3** [削除] をクリックします。
  - ステップ 4** システムをリブートします。
- 

## Informix Dynamic Server の削除

Informix Dynamic Server (IDS) を削除するには、次の手順を実行します。

- 
- ステップ 1** IDS アプリケーションをアンインストールします。
    - [スタート] > [設定] > [コントロール パネル] > [アプリケーションの追加と削除] の順に選択します。
    - [アプリケーションの追加と削除] ウィンドウで、**IDS (Informix Dynamic Server)** を選択します。
    - [削除] をクリックします。Uninstall Informix Dynamic Server ダイアログボックスが表示されます。
    - アンインストール方法 **Remove all database server files and all database information** を選択し、**OK** を選択します。Delete User Account ダイアログボックスが表示されます。
    - Yes** を選択して informix ユーザ アカウントを削除します。Informix Storage Manager (ISM) サーバを削除するかどうかの確認を求められます。
    - Yes** を選択して Informix Storage Manager (ISM) サーバを削除します。SNMP 拡張エージェントを削除するかどうかの確認を求められます。
    - Yes** を選択して SNMP 拡張エージェントを削除します。
  - ステップ 2** ハード ドライブから次のフォルダを削除します。
    - C:\informix
    - C:\ifmxdata

- C:\ciscowebs\dma\bin\IIF
- C:\tmp
- C:\preferences
- C:\DMAROOT
- C:\Program Files\Cisco\Trace\DMA
- C:\Program Files\Cisco\Trace\DBL\installdb\*
- C:\Program Files\Cisco\Trace\DBL\dbl\_INSTALLLDB\*

**ステップ 3** システムをリブートします。

---

## Informix Client SDK のアンインストール

Informix Client SDK を削除するには、次の手順を実行します。

**ステップ 1** [スタート]>[設定]>[コントロール パネル]>[アプリケーションの追加と削除]の順に選択します。

**ステップ 2** [アプリケーションの追加と削除] ウィンドウで、**IBM Informix Client-SDK** を選択します。

**ステップ 3** [削除] をクリックします。Uninstall IBM Informix Client-SDK ダイアログボックスが表示されます。

**ステップ 4** **Yes** をクリックして IBM Informix Client-SDK を削除します。

**ステップ 5** システムをリブートします。

---



## 始める前に

DMA を起動する前に、表 1 に示す手順を実行します。

**表 1 DMA の起動前に実行する必要がある手順**

手順	参照先
Cisco Unified CallManager Backup and Restore Utility を使用して、データをバックアップします。必要に応じて、BARS バックアップを使用して、現在のソフトウェアバージョンにフォールバックできます。	次の URL で、該当するバージョンの『 <i>Cisco Unified CallManager Backup and Restore Utility Administration Guide</i> 』および関連マニュアルを参照してください。 <a href="http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/voice/backup/index.htm</a>
アップグレードする前に、Cisco Unified CallManager Upgrade Utility を使用して、システムが良好な状態であることを確認することをお勧めします。	次の URL で、該当するバージョンの『 <i>Using Cisco Unified CallManager Upgrade Utility</i> 』を参照してください。 <a href="http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm">http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/index.htm</a>
CAR データをバックアップする場合は、CAR プラグインがパブリッシャ サーバにインストールされていることを確認します。	P.9 の「CAR データの移行」を参照してください。
Cisco Unified CallManager Attendant Console を使用する場合は、必要なファイルがパブリッシャ サーバ上に存在することを確認します。	P.10 の「Cisco Unified CallManager Attendant Console データの移行」を参照してください。
CAPF データをサブスクリバ サーバからパブリッシャ サーバにコピーします。	P.10 の「既存の CAPF 1.0(1) データの移行」を参照してください。
サーバに Cisco Security Agent for Unified CallManager がインストールされている場合は、DMA が正常に動作することを確認します。	P.12 の「DMA と Cisco Security Agent for Unified CallManager の互換性の確認」を参照してください。
Cisco Emergency Responder システムで DMA を実行する場合は、C:\Program Files\Cisco Systems\CiscoER\Subscriber_backup ファイルを作成し、バックアップしたすべてのサブスクリバ データをこのファイルに移動します。	詳細については、該当するバージョンの『 <i>Cisco Emergency Responder Administration Guide</i> 』を参照してください。

## CAR データの移行

Cisco CDR Analysis and Reporting (CAR) データをバックアップする前に、CAR プラグインがパブリッシャ サーバにインストールされていることを確認する必要があります。CAR プラグインがインストールされていない場合は、[アプリケーション] > [プラグイン] の順に選択し、CAR プラグインをインストールします。詳細については、『*Cisco Unified CallManager アドミニストレーションガイド*』または『*Cisco Unified CallManager Serviceability アドミニストレーションガイド*』を参照してください。



(注)

CDR レコードを Cisco Unified CallManager 5.1(1) に移行する必要がない場合は、DMA を実行する前に CDR レコードを消去することをお勧めします。

## Cisco Unified CallManager Attendant Console データの移行

Cisco Unified CallManager Attendant Console を使用する場合は、DMA を実行する前に、次のファイルがパブリッシャ サーバ上に存在することを確認します。これらのファイルがパブリッシャ サーバ上に存在しない場合は、DMA を実行する前にサブスクリバサーバからパブリッシャサーバにコピーする必要があります。

- C:\Program Files\Cisco\CallManagerAttendant\etc\acserver.properties
- C:\Program Files\Cisco\CallManagerAttendant\etc\DialRules.xml

## 既存の CAPF 1.0(1) データの移行



### 注意

この項で説明している作業を実行しないと、CAPF データが失われる可能性があります。次の情報は、P.11 の「4.0 サブスクリバサーバから 4.0 パブリッシャ データベース サーバへの CAPF 1.0(1) データのコピー」と併せてお読みください。

Cisco Unified CallManager 5.1(1) で CAPF を使用方法については、『Cisco Unified CallManager セキュリティガイド』を参照してください。

Cisco Unified CallManager 5.1(1) にアップグレードする前に、次の詳細を確認してください。

- CAPF が Cisco Unified CallManager 4.0 パブリッシャ データベース サーバにインストールされている場合の Cisco Unified CallManager 4.0 からのアップグレード：Cisco Unified CallManager 4.0 で証明書の操作を実行し、CAPF 1.0(1) がパブリッシャ データベース サーバ上で動作した場合は、最新の操作ステータスが Cisco Unified CallManager 5.1(1) データベースに移行されます。
- CAPF が Cisco Unified CallManager 4.0 サブスクリバサーバにインストールされている場合の Cisco Unified CallManager 4.0 からのアップグレード：Cisco Unified CallManager 4.0 で証明書の操作を実行し、CAPF 1.0(1) がサブスクリバサーバ上で動作した場合は、Cisco Unified CallManager 5.1(1) にアップグレードする前に、CAPF データを 4.0 パブリッシャ データベースサーバにコピーする必要があります。



### 注意

Cisco Unified CallManager 5.1(1) にアップグレードする前にデータをコピーしないと、Cisco Unified CallManager 4.x サブスクリバサーバ上の CAPF データは Cisco Unified CallManager 5.1(1) データベースに移行されないため、データが失われる可能性があります。データが失われた場合、CAPF ユーティリティ 1.0(1) で発行したローカルで有効な証明書は電話機に残りますが、その証明書は無効になるため、CAPF 5.1(1) が証明書を再発行する必要があります。

- Cisco Unified CallManager 4.1(x) の任意のリリースから Cisco Unified CallManager 5.1(1) へのアップグレード：アップグレードにより、CAPF データが自動的に移行されます。

## 4.0 サブスクリバサーバから 4.0 パブリッシャ データベース サーバへの CAPF 1.0(1) データのコピー



### 注意

Cisco Unified CallManager 4.0 サブスクリバサーバに CAPF ユーティリティ 1.0(1) をインストールした場合は、Cisco Unified CallManager 5.1(1) にアップグレードする前に、CAPF データを 4.0 パブリッシャ データベース サーバにコピーする必要があります。この作業を実行しないと、CAPF データが失われます。たとえば、C:\Program Files\Cisco\CAPF\CAPF.phone にある電話機レコードファイルが失われる可能性があります。データが失われた場合、CAPF ユーティリティ 1.0(1) で発行したローカルで有効な証明書は電話機に残りますが、その証明書は無効になるため、CAPF 5.1(1) が証明書を再発行する必要があります。

次の手順は、P.10 の「既存の CAPF 1.0(1) データの移行」を併読して実行してください。CAPF データのファイルをコピーするには、次の手順を実行します。

### 手順

- ステップ 1** 表 2 の各ファイルを、CAPF 1.0 がインストールされているマシンから、Cisco Unified CallManager 4.0 がインストールされているパブリッシャ データベース サーバにコピーします。

表 2 サーバからサーバへのコピー

コピーするファイル	CAPF 1.0 がインストールされているマシンのフォルダ(コピー元)	Cisco Unified CallManager 4.0 がインストールされているパブリッシャ データベース サーバのフォルダ (コピー先)
*.0	C:\Program Files\Cisco\CAPF	C:\Program Files\Cisco\Certificates
CAPF.phone	C:\Program Files\Cisco\CAPF	C:\Program Files\Cisco\CAPF
CAPF.config ファイル	C:\Program Files\Cisco\CAPF	C:\Program Files\Cisco\CAPF

- ステップ 2** クラスタ内の各サーバを Cisco Unified CallManager 5.1(1) にアップグレードします。
- ステップ 3** クラスタを Cisco Unified CallManager 5.1(1) にアップグレードした後、電話機を使用する前に、次の作業を実行します。
- 既存の Cisco CTL クライアントを削除します。
  - Cisco Unified CallManager の管理ページで、[アプリケーション] > [プラグイン] の順に選択して、最新の Cisco CTL クライアントをインストールします。
  - クライアントを設定し、CTL ファイルを作成または更新します。



**ヒント** Cisco CTL クライアントのインストールおよび設定については、『Cisco Unified CallManager セキュリティ ガイド』を参照してください。

Cisco CTL クライアントは、CAPF 証明書をクラスタ内のすべてのサーバにコピーします。

- ステップ 4** Cisco Unified CallManager 4.0 で使用していた CAPF ユーティリティをアンインストールします。

ステップ 5 P.12 の「新しい CAPF 証明書の生成」を参照してください。

## 新しい CAPF 証明書の生成

CAPF 証明書を再生成する必要がある場合は、Cisco Unified CallManager の証明書管理機能を使用します。手順および詳細については、『Cisco Unified Communications Operating System アドミニストレーションガイド』を参照してください。

## DMA と Cisco Security Agent for Unified CallManager の互換性の確認

Cisco Security Agent for Unified CallManager が原因で DMA バックアップが失敗することがあります。バックアップ中に、DMA が Cisco Security Agent for Unified CallManager を自動的に無効にする場合と無効にしない場合があります。このため、DMA バックアップを実行する前に Cisco Security Agent for Unified CallManager サービスを手動で無効にしなければならないこともあります（この操作を行わないと、バックアップが失敗します）。

CSA を無効および有効にする方法については、『Installing Cisco Security Agent for Unified CallManager』を参照してください。このマニュアルは、次の URL で入手できます。

[http://www.cisco.com/univercd/cc/td/doc/product/voice/c\\_callmg/sec\\_vir/csa/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/csa/index.htm)

Cisco Security Agent for Unified CallManager を手動で無効にした場合は、DMA バックアップの終了後、必ず Cisco Security Agent for Unified CallManager を有効にしてください。



(注)

DMA を実行する前に Cisco Security Agent for Unified CallManager のアンインストールが必要になることがあります。問題がある場合は、詳細についてシスコのサポートにお問い合わせください。

DMA と Cisco Security Agent for Unified CallManager 間の相互対話には、次の規則が適用されます。

- DMA バージョン 5.0(4) 以前の場合
  - バージョン 2.0(5) より前の Cisco Security Agent for Unified CallManager は、DMA バックアップ中に自動的に無効になります。
  - バージョン 2.0(5) 以降の Cisco Security Agent for Unified CallManager は、自動的に無効になりません。DMA バックアップを実行する前に、Cisco Security Agent for Unified CallManager を手動で無効にする必要があります。
- DMA バージョン 5.1(1) 以降の場合
  - バージョン 3.0(2) 以降の Cisco Security Agent for Unified CallManager は、DMA バックアップ中に有効のままにしておくことができます。
  - バージョン 3.0(2) より前の Cisco Security Agent for Unified CallManager は、DMA バックアップ中に有効のままにしておくことはできません。また、自動的には無効になりません。DMA バックアップを実行する前に、Cisco Security Agent for Unified CallManager を手動で無効にする必要があります。

## DMA の実行

Cisco Unified CallManager パブリッシャ サーバで DMA を実行するには、次の手順を実行します。  
DMA を起動する前に、P.9 の「始める前に」の情報を確認してください。

### 手順

**ステップ 1** [スタート] > [プログラム] > **Cisco DMA > DMAAdmin** の順に選択します。

**ステップ 2** プロンプトが表示されたら、Windows Administrator としてログインします。

Data Migration Assistant Home ウィンドウが表示されます。

**ステップ 3** Data Migration Assistant メニューバーで、**Backup > Storage Location** の順に選択します。

Backup Storage Location ウィンドウが表示されます。

**ステップ 4** Backup Storage Location ウィンドウで、次の操作を実行します。

a. 次のいずれかのオプション ボタンをクリックして、DMA が TAR ファイルを格納する場所を選択します。

- **Network Directory** : ネットワーク フォルダに TAR ファイルを格納します。次の各フィールドに情報を入力します。

Path Name : 目的のフォルダへのネットワーク パス

User Name : ネットワーク アクセス用のユーザ名

Password : ネットワーク アクセス用のパスワード

- **Local Directory** : DMA を実行しているサーバ上のフォルダに TAR ファイルを格納します。Path Name フィールドで、フォルダへのパスを入力するか、**Browse** をクリックしてフォルダを選択します。



**(注)** マップされたネットワーク ディレクトリを **Local Directory** に指定しないでください。指定した場合、DMA が目的のフォルダを作成できない可能性があります。

- **Tape Device** : バックアップ デバイスに TAR ファイルを格納します。プルダウン メニューから使用可能なテープ ドライブを選択します。

DMA では、目的の各ディレクトリに 2 つの TAR ファイルを保存できます。3 つ目の TAR ファイルを保存しようとする、新しい TAR ファイルが正常に作成された後、既存の TAR ファイルのうち古い方が削除されます。

b. **Update** をクリックします。

c. バックアップの保管場所として **Local Directory** を選択した場合は、次のプロンプトが表示されたら **OK** をクリックします。

Please ensure that you transfer the contents from the LOCAL path to an external device before upgrading. The files will not be readable from the local directory during the upgrade installation

**ステップ 5** Data Migration Assistant メニューバーで、**Backup > Backup Now** の順に選択します。

Migrate Data Source Server ウィンドウが表示されます。バックアップの実行に必要な時間の概算が表示されます。

**ステップ 6** Migrate Data Source Server ウィンドウで、**Start Backup Now** をクリックします。

バックアップが開始されます。

ステータス ウィンドウに、バックアップの進捗状況が表示されます。ステータス ウィンドウには、バックアップの開始時点と検証フェーズの開始時点の両方で、バックアップの完了に必要な時間の概算が表示されます。ステータス ウィンドウを閉じた場合は、Migrate Data Source Server ウィンドウで **View Latest Status** リンクをクリックすると、再びステータス ウィンドウを表示できます。

バックアップ プロセスの完了には、長い時間がかかることがあります。[スタート] > [プログラム] > Cisco DMA > Cancel Backup の順に選択し、Cancel Backup Process ダイアログボックスで **Cancel Backup Now** をクリックすることにより、いつでもこのプロセスを停止できます。バックアップ プロセスのキャンセルには、数分かかることがあります。



(注) バックアップ プロセスの実行中に DMA ウィンドウを閉じても、バックアップは続行します。ただし、DMA を再起動すると、メイン ウィンドウに **Reset Status** ボタンが表示されます。**Reset Status** ボタンをクリックすると、現在実行中のバックアップ プロセスがキャンセルされます。

バックアップが完了すると、ステータス ウィンドウに次の行が表示されます。

```
Archive built successfully
Backup information file DMABackupinfo.inf saved to D:\DMA
```



(注) データを正常に移行できるように、DMA がデータに小さな変更をいくつか加えることがあります。

**ステップ 7** ステップ 4 で指定したローカル ディレクトリに TAR ファイルを保存した場合は、アップグレードする前に、そのファイルをネットワーク サーバまたはテープ ドライブにコピーします。

TAR ファイルの名前の形式は、次のとおりです。ここで、*date* および *time* はファイルの作成日時を示します。

```
DMABackupdate#time.tar
```

このステップを実行しなければならない理由は、アップグレード プロセス中はローカル ディスクの TAR ファイルにアクセスできないため、およびアップグレード プロセスがローカル サーバ ディスクを再フォーマットするときに TAR ファイルが削除されるためです。

## バックアップデータの検証

DMA バックアップの実行後、データを検証するにはログファイル C:\CiscoWebs\DMA\bin\datavalidation.log を調べます。このログでは、データがビジネスルールに適合していることを保証するためにデータを検証できます。

このログでエラーが見つかった場合でも、DMA バックアップを使用してシステムをアップグレードできます。ただし、不良データは、アップグレードしたシステムでも不良であるため、そのデータを使用する前に修正する必要があります。アップグレードしたシステムに不良データが復元されないようにするために、Microsoft SQL を使用してデータを修正してから、DMA バックアップを再度実行できます。

バックアップ進捗ログは、ファイル C:\Program Files\Cisco\Trace\DMA\Progress\AllProgress.log で確認できます。このフォルダには、追加のログファイルも格納されます。詳細については、P.17 の「[ログファイル](#)」を参照してください。

## DMA バックアップ情報ファイル

DMA は、データをバックアップするときに、バックアップ情報ファイルを自動的に作成します。このファイルには、DMA ソフトウェア、DMA を実行したサーバ、およびバックアップしたデータのソフトウェアに関する設定データと環境データが含まれています。

バックアップ情報ファイル (DMABackupInfo.inf という名前) は、DMA を実行するサーバ上の D:\DMA フォルダに保存されます。また、このファイルは TAR ファイルの一部として保存されるため、このファイルに対しては何も操作する必要はありません。



## DMA の管理とトラブルシューティング

次の各項では、DMA の管理およびトラブルシューティングに使用できる情報を示します。

- [DMA ソフトウェアのバージョンの確認 \(P.16\)](#)
- [前回実行した DMA バックアップ手順の結果の確認 \(P.16\)](#)
- [ログ ファイル \(P.17\)](#)
- [トレース ファイル \(P.19\)](#)

### DMA ソフトウェアのバージョンの確認

サーバにインストールされている DMA のバージョンを確認するには、次の手順を実行します。

#### 手順

- 
- ステップ 1** Data Migration Assistant ウィンドウが表示されていない場合は、次のいずれかの操作を実行して、このウィンドウを表示します。
- DMA が動作している場合は、DMA メニューバーで **Backup > Home** の順に選択します。
  - DMA が動作していない場合は、[スタート] > [プログラム] > **Cisco DMA > DMAAdmin** の順に選択し、プロンプトが表示されたら Windows Administrator としてログインします。
- ステップ 2** Data Migration Assistant ウィンドウで、**Details** ボタンをクリックします。
- 

### 前回実行した DMA バックアップ手順の結果の確認

DMA で前回実行したバックアップ手順の結果を確認するには、次の手順を実行します。

#### 手順

- 
- ステップ 1** [スタート] > [プログラム] > **Cisco DMA > DMAAdmin** の順に選択します。
- ステップ 2** プロンプトが表示されたら、Windows Administrator としてログインします。
- ステップ 3** Data Migration Assistant メニューバーで、**Backup > Backup Now** の順に選択します。
- ステップ 4** Migrate Data Source Server ウィンドウで、**View Latest Status** リンクをクリックします。
- 

バックアップ手順の実行中に **View Latest Status** リンクをクリックすると、現在実行している手順のステータスが表示されます。

---



## ログ ファイル

表 3 は、DMA が作成するログ ファイルについて説明しています。必要に応じて、トラブルシューティングのサポートを受けるために、Cisco Technical Assistance Center (TAC) にログ ファイルを提供できます。

表 3 DMA ログ ファイル

ファイル タイプ	説明	ファイルの場所	ファイル名
インストール ログ ファイル	DMA インストール手順を実行するたびに作成されます。	C:\Program Files\ Common Files\Cisco\Logs	DMAInstalldate_time.log (date_time はファイルの作成日時)  DMAInstallUI.log  IDSInstall.log
バックアップ操作ログ ファイル	DMA を実行してデータをバックアップする日ごとに作成されます。同じ日に複数回バックアップ手順を実行すると、DMA はその日の既存のファイルに情報を追加します。	C:\Program Files\ Common Files\Cisco\Logs\ DMA\BACKUP	Backupdate.log (date はファイルの作成日)  このログは、 <b>View Latest Status</b> リンクをクリックしても表示されます。
データベース エクスポート操作ログ ファイル	初めて DMA を実行してデータをバックアップするときに作成されます。その後バックアップ手順を実行するたびに、DMA はこのファイルに情報を追加します。	C:\CiscoWebs\DMA\Bin	exportdb.log  このフォルダには、他にも次のデータベース エクスポート ログがあります。  <ul style="list-style-type: none"> <li>createdb.log</li> <li>dropdb.log</li> <li>dropdb_w.log</li> </ul>
ディレクトリ エクスポート操作エラー ログ ファイル	DMA を実行してデータをバックアップするたびに作成されます。このファイルが存在する場合、DMA はこのファイルを上書きします。	C:\CiscoWebs\DMA\ DirExport\logs	DirExport_Error.log
ディレクトリ エクスポート操作レポート ファイル	初めて DMA を実行してデータをバックアップするときに作成されます。その後バックアップ手順を実行するたびに、DMA はこのファイルに情報を追加します。	C:\CiscoWebs\DMA\ DirExport\logs	DirExport_Reprt.txt
ディレクトリ エクスポート操作結果ファイル	DMA を実行してデータをバックアップするたびに作成されます。このファイルが存在する場合、DMA はこのファイルを上書きします。	C:\CiscoWebs\DMA\ DirExport\logs	DirExport_Result.txt
データ検証ログ	バックアップ プロセス中、データベースおよびディレクトリのデータを確認しているときに見つかった検証エラーを格納します。	C:\CiscoWebs\DMA\Bin	datavalidation.log

表 3 DMA ログ ファイル (続き)

ファイルタイプ	説明	ファイルの場所	ファイル名
バックアップ進捗インジケータ ログ	DMA を実行するときに作成されます。バックアップおよびデータ検証の高レベルの進捗ログを格納します。	C:\Program Files\Cisco\Trace\DMA\Progress	AllProgress.log  バックアップの進行中にエラーが発生した場合は、同じフォルダに次のログファイルが作成されます。  <ul style="list-style-type: none"> <li>• CSV_Import*.*</li> <li>• ExportDB_CCM*.*</li> <li>• ExportToCSVs*.*</li> <li>• InstallDB_Full*.*</li> </ul>
Informix Dynamic Server (IDS) インストール ログ	DMA のインストール中に作成されます。IDS インストールのログを格納します。	C:\Program Files\Cisco\Logs	IDSInstall.log

## 一般的なエラー

DMA は、表 4 で説明しているエラーを返すことがあります。このエラーにより DMA の実行に失敗する場合があります。

表 4 DMA のエラー メッセージと説明

エラー メッセージ	説明
Failure- Product check; Database contains models that are no longer supported in this release.  AT, AS, and ICS gateways are not supported. Please remove unsupported models and repeat export.	このエラーは、次のいずれかの項目がデバイス テーブルに存在する場合に表示されます。  <ul style="list-style-type: none"> <li>• Cisco AT-2 Gateway PRODUCT_AT2_GATEWAY</li> <li>• Cisco AT-4 Gateway PRODUCT_AT4_GATEWAY</li> <li>• Cisco AT-8 Gateway PRODUCT_AT8_GATEWAY</li> <li>• Cisco AS-2 Gateway PRODUCT_AS2_GATEWAY</li> <li>• Cisco AS-4 Gateway PRODUCT_AS4_GATEWAY</li> <li>• Cisco AS-8 Gateway PRODUCT_AS8_GATEWAY</li> <li>• すべての ICS プラットフォーム</li> </ul>
Failure, Pre-SD CCM Migration	このエラーは、Cisco CallManager 3.x から Cisco Unified CallManager 4.1 への移行中に問題が発生したことを示します。
Failure - Sony devices exist in the database, but there is no corresponding csv file.  Please reinstall the Sony installation.	このエラーは、システムが Sony 電話機の CSV ファイルを検出できないことを示します。移行を続行する前に、デバイスを再インストールする必要があります。
Failure - Tandberg devices exist in the database, but there is no corresponding csv file.  Please reinstall the Tandberg installation.	このエラーは、システムが Tandberg 電話機の CSV ファイルを検出できないことを示します。移行を続行する前に、デバイスを再インストールする必要があります。

表 4 DMA のエラー メッセージと説明 (続き)

エラー メッセージ	説明
Failure- Invalid enum 31970 in Zimbabwe Locale csv file.  Zimbabwe network locale needs to be replaced with a newer version before upgrade.	このエラーは、無効なバージョンの Zimbabwe ロケール ファイルが存在することを示します。移行を続行する前に、Cisco.com から Zimbabwe ロケール ファイルの新しいコピーをダウンロードし、システムにインストールする必要があります。
Failure- Zimbabwe network locale needs to be replaced with a newer version before upgrade.	このエラーは、無効なバージョンの Zimbabwe ロケール ファイルが存在することを示します。移行を続行する前に、Cisco.com から Zimbabwe ロケール ファイルの新しいコピーをダウンロードし、システムにインストールする必要があります。
Failure- Tandberg.xml file is invalid and needs to be replaced before upgrade.  Please reinstall Tandberg with a newer installation.	このエラーは、無効なバージョンの Tandberg.xml ファイルが存在することを示します。移行を続行する前に、Cisco.com から Tandberg.xml ファイルの新しいコピーをダウンロードし、システムにインストールする必要があります。

## トレース ファイル

表 5 は、DMA が作成するトレース ファイルについて説明しています。必要に応じて、トラブルシューティングのサポートを受けるために、Cisco Technical Assistance Center (TAC) にトレース ファイルを提供できます。

表 5 DMA トレース ファイル

ファイル タイプ	説明	ファイルの場所	ファイル名
DMA 操作トレース ファイル	DMA を実行してデータをバックアップする日ごとに作成されます。同じ日に複数回バックアップ手順を実行すると、DMA はその日の既存のファイルに情報を追加します。	C:\Program Files\Cisco\Trace\DMA	Tracedate.log (date はファイルが作成または更新された日付)
データベース エクスポート操作トレース ファイル	DMA は、Cisco Unified CallManager データをバックアップするたびに 1 つのファイルを作成し、CAR データをバックアップするたびに 1 つのファイルを作成します。	C:\Program Files\Cisco\Trace\DBL	<ul style="list-style-type: none"> <li>エクスポート : installdbccm.log</li> <li>W1 インストール : instaldbw1.log</li> </ul>
ディレクトリ エクスポート操作トレース ファイル	初めて DMA を実行してデータをバックアップするときに作成されます。その後バックアップ手順を実行するたびに、DMA はこのファイルに情報を追加します。	C:\CiscoWebs\DMA\DirExport\logs	DirExport_Trace.log
データベース インストール セットアップ トレース ファイル	Informix セットアップ ステータスを表示します。	C:\CiscoWebs\DMA\Bin	dbcmds.log

## 技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。ここでは、シスコが提供する製品マニュアル リソースについて説明します。

### Cisco.com

次の URL から、シスコ製品の最新資料を入手することができます。

<http://www.cisco.com/techsupport>

シスコの Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com>

各国のシスコ Web サイトには、次の URL からアクセスできます。

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

<http://www.cisco.com/jp>

### Product Documentation DVD（英語版）

Product Documentation DVD は、技術情報を包含する製品マニュアルをポータブルなメディアに格納したライブラリです。この DVD を使用することにより、シスコ製の各ハードウェアやソフトウェアのインストール、コンフィギュレーション、およびコマンドに関するマニュアルにアクセスすることができます。また、この DVD を使用すると、次の URL のシスコの Web サイトに掲載されている HTML マニュアルおよび PDF ファイルにアクセスすることができます。

<http://www.cisco.com/univercd/home/home.htm>

Product Documentation DVD は定期的に作成され、リリースされます。DVD は、1 回単位で入手することも、または定期購読することもできます。Cisco.com 登録ユーザの場合、Product Documentation Store の Cisco Marketplace から Product Documentation DVD（Product Number DOC-DOCDVD= または DOC-DOCDVD=SUB）を発注できます。次の URL にアクセスしてください。

<http://www.cisco.com/go/marketplace/docstore>

### マニュアルの発注方法（英語版）

Cisco Marketplace にアクセスするには、Cisco.com 登録ユーザである必要があります。登録ユーザの場合、Product Documentation Store からシスコ製品の英文マニュアルを発注できます。次の URL にアクセスしてください。

<http://www.cisco.com/go/marketplace/docstore>

ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

<http://tools.cisco.com/RPF/register/register.do>

## シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

<http://www2.hipri.com/cisco/>

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

<http://www2.hipri.com/cisco/>

なお、技術内容に関するお問い合わせは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合わせください。

## シスコ製品のセキュリティの概要

シスコでは、オンラインの Security Vulnerability Policy ポータル（英文のみ）を無料で提供しています。URL は次のとおりです。

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

このサイトは、次の目的に利用できます。

- シスコ製品のセキュリティ脆弱性を報告する。
- シスコ製品に伴うセキュリティ事象についてサポートを受ける。
- シスコからセキュリティ情報を受け取るための登録をする。

シスコ製品に関するセキュリティ勧告、セキュリティ上の注意事項、およびセキュリティ対策の最新のリストには、次の URL からアクセスできます。

<http://www.cisco.com/go/psirt>

セキュリティ勧告、セキュリティ上の注意事項、およびセキュリティ対策がアップデートされた時点でリアルタイムに確認する場合は、次の URL から Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) フィードに登録してください。PSIRT RSS フィードへの登録方法については、次の URL を参照してください。

[http://www.cisco.com/en/US/products/products\\_psirt\\_rss\\_feed.html](http://www.cisco.com/en/US/products/products_psirt_rss_feed.html)

## シスコ製品のセキュリティ問題の報告

シスコでは、セキュアな製品を提供すべく全力を尽くしています。製品のリリース前には内部でテストを行い、すべての脆弱性を早急に修正するよう努力しています。万一、シスコ製品に脆弱性が見つかった場合は、PSIRT にご連絡ください。

- 緊急の場合のみ: [security-alert@cisco.com](mailto:security-alert@cisco.com)（英語のみ）

緊急とは、システムがアクティブな攻撃を受けている場合、または至急の対応を要する重大なセキュリティ上の脆弱性が報告されている場合を指します。これに該当しない場合はすべて、緊急でないと見なされます。

- 緊急でない場合: [psirt@cisco.com](mailto:psirt@cisco.com)（英語のみ）

緊急の場合は、電話で PSIRT に連絡することもできます。

- 1 877 228-7302（英語のみ）
- 1 408 525-6532（英語のみ）



### ヒント

シスコに機密情報をお送りいただく際には、PGP (Pretty Good Privacy) または GnuPG などの互換製品を使用して、暗号化することをお勧めします。PSIRT は、PGP バージョン 2.x から 9.x で暗号化された情報に対応しています。

無効になった暗号鍵または有効期限が切れた暗号鍵は、絶対に使用しないでください。PSIRT に連絡する際に使用する正しい公開鍵には、Security Vulnerability Policy ページの Contact Summary セクションからリンクできます。次の URL にアクセスしてください。

[http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html)

このページ上のリンクからは、現在使用されている最新の PGP 鍵の ID にアクセスできます。

PGP を持っていない、または使用していない場合は、機密情報を送信する前に PSIRT に問い合わせ、他のデータ暗号化方法を確認してください。

## Product Alerts および Field Notices

シスコ製品に対する変更やアップデートは、Cisco Product Alerts および Cisco Field Notices で発表されます。Cisco.com のプロダクト アラート ツールを使用すると、Cisco Product Alerts および Cisco Field Notices を受け取ることができます。このツールを使用すれば、プロフィールを作成して、情報を受け取る製品を選択できます。

プロダクト アラート ツールにアクセスするには、Cisco.com の登録ユーザとなる必要があります (Cisco.com にユーザ登録するには、<http://tools.cisco.com/RPF/register/register.do> にアクセスします)。登録ユーザは、<http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en> でこのツールを使用できます。

## テクニカル サポート

Cisco Technical Support では、24 時間テクニカル サポートを提供しています。Cisco.com の Cisco Technical Support & Documentation Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、シスコと正式なサービス契約を交わしているお客様には、Cisco Technical Assistance Center (TAC) のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合わせください。

### Cisco Technical Support & Documentation Web サイト

Cisco Technical Support & Documentation Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ただけのように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間、いつでも利用可能です。URL は次のとおりです。

<http://www.cisco.com/techsupport>

Cisco Technical Support & Documentation Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

<http://tools.cisco.com/RPF/register/register.do>



(注)

---

オンラインまたは電話でサービス リクエストを発行する前に、**Cisco Product Identification Tool** を使用して製品のシリアル番号を確認してください。Cisco Technical Support & Documentation Web サイトでこのツールを使用するには、**Tools & Resources** リンクをクリックし、**All Tools (A-Z)** タブをクリックした後、アルファベット順のリストから **Cisco Product Identification Tool** を選択します。このツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、**show** コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

---



ヒント

---

Cisco.com での表示および検索

ブラウザが Web ページをリフレッシュしていないと思われる場合は、Ctrl キーを押したまま F5 を押すことで強制的にブラウザに Web ページを更新させます。

技術情報を検索する場合は、Cisco.com の Web サイト全体ではなく、技術マニュアルに検索対象を絞り込みます。Cisco.com のホームページで、Search ボックスの下にある **Advanced Search** リンクをクリックし、**Technical Support & Documentation** オプション ボタンをクリックしてください。

Cisco.com の Web サイトまたは特定の技術マニュアルに関するフィードバックを送るには、Cisco.com のすべての Web ページの下部にある **Contacts & Feedback** をクリックします。

---



## Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト (<http://www.cisco.com/tac>) のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

<http://www.cisco.com/jp/go/tac>

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

<http://www.cisco.com/jp/register>

## サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます (S3: ネットワークに軽微な障害が発生した、S4: 製品情報が必要である)。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、シスコのエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

<http://www.cisco.com/techsupport/servicerequest>

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合わせください (S1: ネットワークがダウンした、S2: ネットワークの機能が著しく低下した)。S1 および S2 のサービス リクエストには、シスコのエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

電話での問い合わせ先は、次のとおりです。

Cisco TAC の連絡先については、次の URL を参照してください。

<http://www.cisco.com/techsupport/contacts>

## サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1 (S1): 既存のネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2 (S2): 既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3 (S3): ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4 (S4): シスコ製品の機能、インストラクション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

## その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Online Subscription Center は、シスコの E メール ニュースレターなどに登録できる Web サイトです。プロフィールを作成して、受け取る情報を選択できます。Cisco Online Subscription Center には、次の URL からアクセスしてください。

<http://www.cisco.com/offer/subscribe>
- 『Cisco Product Quick Reference Guide』は手軽でコンパクトな参照ツールです。チャネルパートナー経由で販売される多くのシスコ製品に関する簡単な製品概要、主要な機能、サンプル部品番号、および簡単な技術仕様を記載しています。年 2 回の更新の際には、シスコ製品の最新情報が収録されます。『Cisco Product Quick Reference Guide』の注文方法および詳細については、次の URL にアクセスしてください。

<http://www.cisco.com/go/guide>
- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、マニュアル、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

<http://www.cisco.com/go/marketplace/>
- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版物やその他の情報を調べるには、次の URL から Cisco Press にアクセスしてください。

<http://www.ciscopress.com>
- 『Internet Protocol Journal』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『Internet Protocol Journal』には、次の URL からアクセスしてください。

<http://www.cisco.com/ipj>
- シスコシステムズが提供するネットワーキング製品、および各種のカスタマー サポート サービスは、次の URL から入手できます。

<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection は対話形式の Web サイトです。このサイトでは、ネットワーキング製品やテクノロジーに関する質問、提案、および情報をネットワーキング担当者がシスコの専門家や他のネットワーキング担当者と共有できます。次の URL にアクセスしてディスカッションに参加してください。

<http://www.cisco.com/discuss/networking>
- 「What's New in Cisco Documentation」は、シスコ製品の最新のマニュアルリリースに関する情報を提供するオンライン出版物です。このオンライン出版物は毎月更新され、製品カテゴリ別に編成されているため、製品のマニュアルを簡単に検索できます。次の URL で「What's New in Cisco Documentation」の最新リリースを見ることができます。

<http://www.cisco.com/univercd/cc/td/doc/abtnucd/136957.htm>
- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

<http://www.cisco.com/en/US/learning/index.html>

CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.(0609R)

Copyright © 2006 Cisco Systems, Inc.  
All rights reserved.

お問い合わせは、購入された各代理店へご連絡ください。

シスコシステムズでは以下のURLで最新の日本語マニュアルを公開しております。  
本書とあわせてご利用ください。

**Cisco.com 日本語サイト**

[http://www.cisco.com/japanese/warp/public/3/jp/service/manual\\_j/](http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/)

日本語マニュアルの購入を希望される方は、以下のURLからお申し込みいただけます。

**シスコシステムズマニュアルセンター**

<http://www2.hipri.com/cisco/>

上記の両サイトで、日本語マニュアルの記述内容に関するご意見もお受けいたしますので、  
どうぞご利用ください。

なお、技術内容に関するご質問は、製品を購入された各代理店へお問い合わせください。



シスコシステムズ株式会社

URL:<http://www.cisco.com/jp/>

問合せ URL:<http://www.cisco.com/jp/service/contactcenter/>

〒107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館

TEL.03-5549-6500 FAX.03-5549-6501