

White Paper : (Microsoft Exchange を搭載した) Cisco Unity 4.0 のセキュリティ上のベスト プラクティス

はじめに

この White Paper では、Cisco Unity 4.0 サーバを「強化する」ために、推奨されるベスト プラクティスについて説明します。「サーバの強化」という用語は、サーバが不要なアクセスまたは不正なアクセスや、ウィルスの影響を受けにくくするためのプロセスを記述するのに使用します。

この文書は、インストール中と通常の操作時に Cisco Unity サーバを強化するため、『Cisco Unity インストレーション ガイド』とあわせて使用してください。ここでは、音声メッセージングの設定およびユニファイド メッセージングの設定に関する、Cisco Unity for Exchange について主に説明しています。また、この文書に記載されている推奨事項と設定は、定期的に見直され、必要に応じて更新されます。

以下のセクションでは、Cisco Unity サーバでの、セキュリティ上の主な考慮事項を取り上げます。

- **Cisco Unity 稼動環境の保護** Cisco Unity の稼動環境は、複数のサードパーティ製品から構成されています。これらの各製品は、製品の製造業者によって発行されたセキュリティ ガイドラインに従って、セキュリティを確保する必要があります。これらのガイドラインは、Cisco Unity に搭載されている各コンポーネントを使用するための固有の推奨事項とあわせて、このセクションで要約されており、インストール中、またはインストール後に、Cisco Unity の稼動環境を強化するために使用できます。
- **Cisco Unity アプリケーションの保護** Cisco Unity アプリケーションをインストールした後、このセクションで詳細に説明されている推奨事項に従って、セキュリティを確保できます。
- **Cisco Unity サーバセキュリティ ポリシー** このセクションでは、インストール完了後、サーバのセキュリティをさらに強化するために実装可能な、セキュリティ ポリシーについて説明します。
- **オンライン リファレンス** このセクションでは、この文書で参照されているサイトをリストします。

Cisco Unity 稼動環境の保護

Cisco Unity 稼動環境には、サービス ユーザに必要なサードパーティ製の全コンポーネントが含まれています。これらのコンポーネントは、主として Microsoft 社の製品から構成されていますが、Dialogic 社のソフトウェア (Cisco Unity サーバを従来の電話システムに接続するために、音声ボードが使用されている場合) などの、その他のサードパーティ製品も使われています。Cisco Unity 稼動環境に必須の Microsoft 社の製品は、以下のコンポーネントです。(本文書の執筆時点)

- 最新のセキュリティ パッチを適用した Windows 2000 Service Pack 3
- 最新のセキュリティ パッチを適用した Internet Information Server (IIS) 5.0
- 最新のセキュリティ パッチを適用した Internet Explorer (IE) 6.0 Service Pack 1
- Microsoft Message Queuing 2.0
- MSXML Service Pack 1
- Microsoft .NET Framework v.1.1
- SQL Server 2000 Service Pack 3 または MSDE 2000 Service Pack 3
- Exchange 2000 Service Pack 2



最新の Cisco Unity 稼働環境のコンポーネントの詳細なリストについては、http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/40_sysrq.htm に掲載されている『Cisco Unity システム要件およびサポートされるハードウェアとソフトウェア』を参照してください。

Cisco Unity 稼働環境内の各コンポーネントには、セキュリティリスクが存在します。これは、各コンポーネントに障害が発生すると、Cisco Unity が確実かつ効果的に実行できなくなる可能性があるためです。しかしデフォルトでは、ほとんどのコンポーネントが最低レベルのセキュリティでインストールされているので、セキュリティの強化を考慮した再構成が可能です。

適用可能な場合は、次のセクションに記載されているガイドラインを、『Cisco Unity インストールガイド』(http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html に掲載) とあわせて使用し、Cisco Unity の新規インストール時およびインストール後の Cisco Unity 稼働環境を強化してください。

Windows の保護

IIS サービスがスタートされると、IIS サービスのセキュリティは脆弱な状態にさらされます。この状態は、Cisco Unity サーバに Windows 2000 を脆弱性を解消した形でインストールするまで続きます。選択肢としては、Windows 2000 Service Pack 3 が適用されるまで、IIS サービスを無効にするか、インストールしないことです。ここで、Windows をインストールする場合の最も安全なアプローチは、最初から Service Pack 3 を適用した Windows 2000 の CD を作成するという、統合された方法を採用することです。手順の詳細は、Microsoft 社の Web サイトからアクセスできる「Installing and Securing a New Windows 2000 System」というセクションに説明されています。また、Windows 2000 と IIS 5.0 に関する、最新のセキュリティの強化とガイドについては、Microsoft Security のホームページを参照してください。既存の Windows 2000 インストールの脆弱性をチェックするには、まずサーバに Service Pack 3 がインストールされているかどうかを確認します。次に Microsoft TechNet Web サイトを参照して、既存の Windows 2000 システムの保護に関する最新情報を参照してください。Cisco Unity サーバにセキュリティ ポリシーを適用することは可能ですが、Cisco Unity のインストールが完了するまでは適用しないでください。セキュリティ ポリシーとその適用方法については、Microsoft 社の Web サイトまたは Windows 2000 のオンラインヘルプを参照してください。



警告 特定のセキュリティ テンプレートを適用すると、Cisco Unity が操作不能になる場合があります。セキュリティ テンプレートを適用する場合は、「[Cisco Unity サーバのセキュリティ設定の変更](#)」のセクションで概説されている、推奨されるセキュリティ設定が使用されていることを確認してください。これらの設定によって、Cisco Unity サーバは完全な機能を維持できます。

SQL Server と MSDE の保護

Cisco Unity サーバへの SQL Server または MSDE のインストールは、バック エンド データベースとして使用することを意図したものであり、それ以外の目的に使用しないでください。Cisco Unity サーバに SQL Server または MSDE をインストールする場合は、次のセキュリティ ガイドラインを使用します。

- Windows のセキュリティのみを使用して、SQL Server をインストールする。
SQL サービスを実行するために、ドメイン ユーザ アカウントまたはローカル システム アカウントを使用できますが、最善の方法は、デフォルトのローカル システム アカウントを使用することです。
- SQL Administrator (SA; SQL 管理者) アカウントにパスワードを割り当てる。
パスワードを書き留め、安全な場所に保管します。



- SQL Server へのクライアント アクセスを制限する。

SQL Server のディレクトリ、フォルダ、およびファイルのアクセスは、Cisco Unity サービス アカウント および、システム管理者による使用を想定した高位の権限アカウント のみに許可します。(詳細は、「[Cisco Unity アカウントのベスト プラクティス](#)」のセクションを参照してください)。Cisco Unity のインストール プロセスでは、ローカル サーバ管理者グループ内のメンバーシップによって、SQL Server へのアクセスが得られます。

SQL Server の追加インスタンスの保護

『Cisco Unity インストールガイド』の指示に従って Cisco Unity サーバに SQL Server または MSDE をインストールすると、W32.Slammer ワームなどのウイルスから保護されます。ただし、サードパーティ製のアプリケーション (Dell 社の OpenManage IT Assistant、Hewlett-Packard 社の Insight Manager、Hewlett-Packard 社の OpenView、VERITAS 社の Backup Exec、VERITAS 社の NetBackup など) によってインストールされた MSDE データベースには脆弱性が残る可能性があります。詳細については、http://www.cisco.com/en/US/customer/products/sw/voicesw/ps2237/products_tech_note09186a008013435f.shtml に掲載されている、Tech Note 『Cisco Unity 3.x and 4.0 Are Vulnerable to W32.Slammer Worm』の、「Detecting and Patching Additional Instances of MSDE on the Cisco Unity Server」のセクションを参照してください。

Internet Explorer の保護

Cisco Unity サーバには、最低でも IE 6.0 Service Pack 1 をインストールする必要があります。ベスト プラクティスとして、Cisco Unity サーバ上では、IE を Cisco Unity の管理専用で使用し、その他の目的には使用しないでください。次の手順を実行して、最近の Blaster ウィルスや Nachi ウィルスなどのワームに感染する可能性を減らしてください。Blaster ウィルスへの感染防止、およびウイルスからの復旧についての詳細は、Microsoft Knowledge Base (マイクロソフト サポート技術情報) 826955 のセクションを参照してください。

Microsoft 社は、Security Notification Service に加入することを推奨しています。ただし、そのためには、この文書の手順で示されている設定よりも、安全性が下がる設定を使用して、IE を設定しなければなりません。したがって、サイト内にある最低 1 台のコンピュータ (Cisco Unity サーバ以外) は、Security Notification Service に加入し、その他のワークステーションでは、次の手順を実行してください。これにより、Cisco Unity のセキュリティを大きく損なわずに、最新のホットフィックスやセキュリティ上の問題に関するアップデートを受け取ることができます。



アクティブなスクリプトを無効にする

ステップ 1 Internet Explorer を起動します。

ステップ 2 4つのセキュリティレベルのそれぞれに対して、次のサブステップを実行します。

a. [ツール]>[インターネット オプション]の順にクリックします。

b. [インターネット オプション]ダイアログ ボックスで、カスタマイズするセキュリティレベル（インターネット、イントラネット、信頼済みサイト、制限付きサイト）に適用可能なアイコンをクリックします。

c. [セキュリティ]>[レベルのカスタマイズ]の順にクリックします。

d. [スクリプト]で、[ダイアログを表示する]のチェック ボックスをオンにします。

ステップ 3 [OK] をクリックします。

ステップ 4 [OK] をクリックします。

ステップ 5 Internet Explorer を終了します。

Microsoft Message Queuing の保護

Microsoft Message Queuing (MSMQ) 2.0 は、Active Directory からの変更を読み取り、その変更を Cisco Unity のバック エンド データベースに書き込むために、Cisco Unity サービスが使用しています。Cisco Unity サーバを Active Directory に接続するためには、使用されません。ベスト プラクティスとして、MSMQ がローカル専用として設定されていることを確認してください。つまり、MSMQ によって Active Directory が使用されないように、MSMQ をインストールしなければならないということです。

IIS の保護

Cisco Unity アプリケーションをインストールする前に、Cisco Unity サーバで、IIS 5.0 の インストールのセキュリティを保護するために、次のガイドラインを使用します。また、インストールが完了した後の、追加の参考情報にも注意してください。

IIS の設定ガイドライン

IIS 5.0 用の最新の累積アップデート パッチがインストールされていることを確認してください。「Windows の保護」に記載されている方法を使用して、オペレーティング システムがインストールまたはアップデートされている場合、デフォルト設定を削除することによって、IIS 5.0 のセキュリティを保護します。また、Cisco Unity サーバで IIS を設定するには、次のガイドラインを使用してください。



警告 このセクションに記載されているガイドラインに従わなかった場合、Cisco Unity Web サーバのコネクトが操作不能になる場合があります。

- サンプル ファイル、フォルダ、および Web アプリケーションを削除する。

Microsoft TechNet Web サイトに掲載されている、詳細な IIS 5.0 セキュリティ チェックリストで指定されているガイドラインに従います。



- Cisco Unity Web コンポーネントを保護する。
Microsoft TechNet Web サイトに掲載されている、詳細な IIS 5.0 セキュリティ チェックリストで指定されているガイドラインに従います。ただし、Cisco Unity のディレクトリ、フォルダ、およびファイルに対するフルコントロールアクセスは、Cisco Unity サービス アカウントやローカル サーバ管理者グループにのみ許可する必要があります。(<ドライブ名>:\inetpub\wwwroot\ を参照)。
- デフォルトの IIS COM オブジェクトをすべて無効にする。
Microsoft TechNet Web サイトに掲載されている、詳細な IIS 5.0 セキュリティ チェックリストで指定されているガイドラインに従います。ただし、「ファイル システム オブジェクト」(FSO) は無効にしません。
- 使わないスクリプト マッピングを削除する。
Cisco Unity は、ASA と ASP スクリプト マッピングだけを使用します。他の使わないスクリプト マッピングは削除します。
- 上位パスを無効にしない。
Microsoft TechNet Web サイトの詳細な IIS 5.0 セキュリティ チェックリストで指定されている、上位パスを無効にするガイドラインには従わないでください。デフォルトでは、このオプションは有効に設定されており、Cisco Unity サーバでもそのまま使用する必要があります。

その他の IIS 参考情報

次のセキュリティ ツールは、IIS インストール後に既存の脆弱性を明らかにするために使用できます。



警告 前のセクションに記載されている IIS 設定を変更するために、これらのツールを使用しないでください (またはこの文書で言及されていない手順を実行しないでください)。これらの操作を行うと、Cisco Unity サーバが操作不能になる場合があります。

- IIS Lockdown と URLScan ツールを活用する。
Microsoft IIS Lockdown と URLScan ツールを使って、IIS サーバを強化できます。ただし、active server pages (asp; アクティブ サーバ ページ) またはスクリプト仮想ディレクトリのサポートは、無効にしないようにしてください。これらのツールのダウンロードのインストラクションと詳細な使用方法については、Microsoft TechNet Web サイトにあるセキュリティ ページを参照してください。Exchange 環境におけるこれらのツールの設定方法については、Microsoft 製品サポート サービス Web サイトのセクション #Q309508 (「XCCC:IIS Lockdown and URLScan Configurations in an Exchange Environment」) を参照してください。
- Microsoft 社のセキュリティ チェックリストに従う。
詳細なチェックリストに加え、Microsoft 社は TechNet Web サイト上で、IIS 用のベースライン セキュリティ チェックリストを提供しています。インストール後、IIS セキュリティ問題に関して最新の情報を維持する場合は、チェックリストの推奨事項 (Microsoft Security Notification Service への加入など) の多くが必須です。

Exchange の保護

Cisco Unity サーバに Exchange をインストールしたり、Cisco Unity サーバが Exchange サーバ オフボックスを指し示すように設定することができます。Exchange を使用するための要件の詳細については、

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/sysreq/40_sysrq.htm に掲載されている『Cisco Unity システム要件およびサポートされるハードウェアとソフトウェア』を参照してください。Cisco Unity サーバ上に



Exchange をインストールしていない場合、既存の Exchange サーバを保護するために、Microsoft 社が提供している推奨事項を使用してください。あるいは、ご使用の Exchange のバージョンに適用可能な、次のセキュリティガイドラインを参照してください。

Exchange 5.5 の設定

Exchange 5.5 が Cisco Unity サーバにインストールされている場合、または Cisco Unity が Exchange 5.5 サーバに接続されている場合には、LDAP ポート番号を 389（デフォルト値）以外に変更します。または、LDAP ポート番号を、使用頻度が低いポートに（2,000 番台以降のポートなど）割り当てます。Cisco Unity の設定のほとんどの場合には、Exchange Administrator のサーバ コンテナにある [プロトコル] セクションにアクセスすることで、LDAP ポート設定を変更できます。ただし Cisco Unity をユニファイド メッセージング システムとしてインストールした場合、サイト構成コンテナ内の設定の変更が必要な場合があります。登録されているポートの詳細については、Internet Engineering Task Force (IETF) Web サイト、または Microsoft TechNet Web サイトを検索してください。

Exchange 2000 の設定

Exchange 2000 が Cisco Unity サーバにインストールされている場合、あるいは Cisco Unity が Exchange 2000 サーバに接続されている場合には、Exchange 2000 サーバの強化に関する推奨事項については、Microsoft 社の Web サイトを参照してください。

Cisco Unity アプリケーションの保護

不正侵入やウイルス感染のリスクを最小限に抑えるために、Cisco Unity サーバを強化するには複数の方法があります。詳細は、以下のセクションを参照してください。

- [Cisco Unity アカウントのベスト プラクティス](#)
- [サービス クラス制限のベスト プラクティス](#)
- [音声メッセージング ユーザ アカウント作成のベスト プラクティス](#)
- [ユーザの電話アクセスのベスト プラクティス](#)
- [ユーザの Web アクセスのベスト プラクティス](#)
- [Text To Speech の使用のベスト プラクティス](#)

Cisco Unity アカウント のベスト プラクティス

Cisco Unity サービス アカウントとアクセス権の最新の要件については、http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/inst/inst403/ex/index.htm に掲載されている、『Cisco Unity インストレーションガイド、リリース 4.0(3)』を参照してください。

ベスト プラクティスとして、Cisco Unity アカウントを保護するために、次のガイドラインを使用します。

Cisco Unity へのアカウント アクセスの制限

Cisco Unity サーバへのアクセスは、Cisco Unity サービス アカウントおよび、システム管理者による使用を想定したその他の高位の権限アカウントのみに制限する必要があります。このようなアカウントは、ドメインレベルの管理機能、Cisco Unity のユーティリティ、ディレクトリ、ファイル、およびデータへのアクセス権を持つことが可能で、Cisco Unity 管理者を使用して Cisco Unity を管理する必要があります。



Cisco Unity のディレクトリ、ファイル、およびデータへのアカウント アクセスの制限

Cisco Unity アプリケーションはデフォルトで、CommServer ディレクトリにインストールされます。このディレクトリは、インストール中に選択された任意のローカルドライブに作成できます。

デフォルトでは、Cisco Unity サービス アカウントには、ローカル サーバ管理者グループ内でのメンバーシップにより、このディレクトリへのフルコントロール アクセスが割り当てられています。また、システム管理者による使用を想定した高位の権限アカウントに対しても、Cisco Unity のディレクトリ、フォルダ、ファイル、およびデータへのフルコントロール権限を与える必要があります。このようにして、管理またはトラブルシューティング関連の高度なタスクを実行するために、このアカウントを使用できます。

ベスト プラクティスとして、Cisco Unity のシステム管理者が使用するその他のドメイン アカウントは読み取り専用で制限し、Cisco Unity ユーザ、および他のすべてのドメイン アカウントとグループには、Cisco Unity サーバのディレクトリ、フォルダ、またはファイルへのアクセス権限を与えないようにする必要があります。アクセスを制限するには、Cisco Unity サーバの C:\ や他のすべてのドライブのルートに対するデフォルトのユーザ権限から System Group Everyone を除外します。その代わりに、認証されたユーザを割り当てます。また、個々のグループまたはアカウントに対して、明示的な権限が割り当てられていないことを確認します。

Cisco Unity を管理するために、Cisco Unity サービス アカウントを使用しない

Cisco Unity サービス アカウントには、ほとんどの管理タスクを実行するために、必要とするよりも多くの権限が割り当てられている場合があります。このため、Cisco Unity 管理者にアクセスする必要があるけれども、Cisco Unity サーバ自体へのアクセスを必要としないドメイン ユーザに対しては、Cisco Unity サービス アカウントを使用して Cisco Unity 管理者にアクセスすることを許可しないでください。

Cisco Unity の管理にサービス アカウントを使用する代わりに、GrantUnityAccess ユーティリティを使用して、単一の Cisco Unity ユーザアカウントに、任意の数の Windows ドメイン アカウントを関連付けることができます。GrantUnityAccess は、関連付けられた Windows ドメイン アカウントと Cisco Unity ユーザアカウントのテーブルを保持します。ユーザが Cisco Unity 管理者へのアクセスを試行する（Cisco Unity 管理者が使用した認証メカニズムにかかわらず）と、Cisco Unity はこのテーブルを参照します。このテーブルは、ユーザに Cisco Unity 管理者へのアクセスを許可するかどうかを決定するために使用します。GrantUnityAccess ユーティリティの使用については、『Cisco Unity システム アドミニストレーション ガイド』

(http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag403/ex/index.htm) に掲載) の「Cisco Unity システム管理へのアクセス」の章の「別の Cisco Unity サーバに対する管理者権限の付与」のセクションを参照してください。

GrantUnityAccess ユーティリティの使用とアクセスの制限

GrantUnityAccess ユーティリティへのアクセスと使用は、システム管理者による使用を想定した高位の権限アカウントのみに許可します。

Cisco Unity 権限ウィザードの実行

Cisco Unity 権限ウィザードは、インストール アカウント、ディレクトリ サービス アカウント、およびメッセージストア サービス アカウントに関して、ユーザ権限、グループ メンバーシップ、および Active Directory のユーザ権限を自動的に設定します。Cisco Unity 権限ウィザードについての詳細は、

http://www.ciscounitytools.com/App_PW_403.htm を参照してください。



デフォルト アカウントの保護

Cisco Unity は、デフォルトのアカウントを使用して、ユーザ用と管理者用のサンプル設定を提供します。また、コールハンドラ、配布リストなど、メッセージ処理に関連するデフォルトのエンティティをオーナーに提供して、サービスのデフォルト クラスのメンバとしてサービスを供給します。詳細については、『Cisco Unity システム アドミニストレーション ガイド』

(http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag403/ex/index.htm に掲載) の「デフォルト アカウントとメッセージの処理」の章を参照してください。


デフォルト アカウントについては、次で説明します。

サンプル管理者

EAdministrator アカウントのデフォルトの内線番号は 99999 で、その電話パスワードは 12345 です。サンプル管理者には、Exchange のメールボックスと Windows ドメイン アカウントが設定されています。Cisco Unity を不正アクセスから保護するには、インストール後、デフォルトの電話パスワードを変更し、長い (20 文字以上) かつ簡単にわからないパスワードを指定する必要があります。(Cisco Unity 管理者の [ユーザ]>[ユーザ]>[Phone Password] ページで、デフォルトの電話パスワードを変更できます)。

サンプルユーザ

ESubscriber アカウントのデフォルトの内線番号は 99990 で、その電話パスワードは 12345 です。Cisco Unity を不正アクセスから保護するには、インストール後、デフォルトの電話パスワードを変更し、長い (20 文字以上) かつ簡単にわからないパスワードを指定する必要があります。(Cisco Unity 管理者の [ユーザ]>[ユーザ]>[Phone Password] ページで、デフォルトの電話パスワードを変更できます)。このアカウントは、いつでも削除できます。

 **注** Cisco Unity バージョン 4.0(3) 以降、サンプルユーザのアカウントは、Cisco Unity のインストール時に作成されなくなりました。ただし、Cisco Unity の以前のバージョンからアップグレードした場合は、アカウントはアップグレード プロセスでは削除されないため、サンプルユーザのアカウントは設定されたままです。

サービス クラス制限のベスト プラクティス

Class of Service (COS; サービス クラス) は、ユーザによる Cisco Unity の使用方法の定義と制限を行います。COS は、各ユーザ テンプレートで指定されます。このためユーザは、ユーザアカウントの作成に使用されたテンプレートに関連付けられた COS に割り当てられます。COS システム アクセスの設定は、Cisco Unity 管理者でユーザ (他のシステム管理者を含む) が、実行可能なタスク (もし存在すれば) を指定します。Cisco Unity 管理者で [ユーザ]>[サービス クラス]>[システム アクセス] ページ上のフィールドを使用して、管理者は Cisco Unity へのアクセスをさまざまな方法でカスタマイズできます。たとえば、管理者は次の操作ができます。

- Cisco Unity 管理者へのアクセスの拒否、または Cisco Unity 管理者内の特定のページ (COS、ユーザまたは配布リスト ページ) へのアクセスの拒否。
- Cisco Unity 管理者内の特定のページに対する、読み取り、編集、追加、または削除の各権限の指定。
- ユーザアカウントのロック解除またはユーザパスワードの変更のみを目的とした、ユーザページへのアクセスの許可。



Cisco Unity では、事前に定義された次のサービス クラスが用意されており、ユーザは修正はできますが、削除はできません。

- **デフォルトユーザ** - ユーザに適用可能な設定を含むデフォルト ユーザ COS。デフォルトでは、この COS はデフォルト ユーザ テンプレートに関連付けられていて、Cisco Unity 管理者へのアクセスからは除外されています。すべてのユーザ COS 設定では、Cisco Unity 管理者へのアクセスを禁止することを推奨します。
- **デフォルト管理者** - デフォルト管理者 COS はシステムのアクセス設定を含み、ユーザが Cisco Unity 管理者で実行可能なタスク（もし存在すれば）を指定しています。（Cisco Unity のシステム管理者は、Cisco Unity 管理者にアクセスできるよう設定された、単なるユーザです）。デフォルトでは、この COS は Cisco Unity の完全な管理権限を持っていて、次の操作が可能です。
 - Cisco Unity 管理者へのアクセス。
 - サービス クラス、規制テーブル、ルーティング テーブル、コールハンドラ、スケジュールと休日、ユーザ、パブリック同報リストの作成、編集または削除。
 - ステータス モニタ、レポート、診断ツール、および技術専門機能へのアクセス。

COS 設定と割り当てを修正する場合、次のベスト プラクティスを考慮します。

- 管理者は、自分の Cisco Unity アカウントを管理するために、Cisco Personal Communications Assistant へのログインに使用するのと同じユーザ アカウントで、Cisco Unity 管理者へログインしない。
- デフォルト管理者 COS システムのアクセス設定は変更しない。その代わりに、Cisco Unity 管理者へのアクセス権限がほとんど、または、まったくない別の COS に、ユーザ アカウントを再度割り当てます。
- Cisco Unity 管理者へのアクセス権限があるすべてのアカウントは、Cisco Unity 管理者へのアクセスをほとんどまたはまったく持たない別の COS に再度割り当てない。



警告 Cisco Unity 管理者へのアクセスを提供する COS 内で、メンバーシップが付加されたドメイン アカウントを最低 1 つ持っていない場合、Cisco Unity が管理できなくなり、再インストールを要求される場合があります。ベスト プラクティスとして、デフォルト管理者 COS にアカウントが最低 1 つ割り当てられていることを確認します。COS 設定と割り当ての詳細については、『Cisco Unity システム アドミニストレーション ガイド』

(http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag403/ex/index.htm に掲載) の「サービス クラスの設定」の章を参照してください。

音声メッセージング ユーザ アカウント 作成のベスト プラクティス

それぞれの Cisco Unity ユーザは、Active Directory アカウントに関連付けられた Exchange メールボックスを所有する必要があります。Cisco Unity 管理者を使って新しいユーザ アカウントを作成した場合、Exchange メールボックス、および関連付けられている Active Directory アカウントが自動的に作成されます。Active Directory に最初に割り当てられるパスワードは、デフォルトのパスワードの複雑さに関する要件を満たす、ランダムに生成された値です。このパスワードが割り当てられるときに、どのようなパスワードにするか決定する方法はありません。その結果、システム管理者（ドメイン レベルの管理機能を持つ、高い権限のアカウントが割り当てられた管理者）は、ユーザが Cisco Personal Communications Assistant にアクセスするためにアカウントを使用できるように、パスワードをリセットしなければなりません。



ユーザの電話アクセスのベスト プラクティス

ユーザが電話を使用して Cisco Unity にログインした場合、Cisco Unity カンパセーション、または Telephone User Interface (TUI; 電話ユーザ インターフェイス) が聞こえます。ログインするには、ユーザは Cisco Unity パイロット番号（または DID を使っている場合は自分の内線番号）にダイヤルし、パスワードを入力します。

Cisco Unity 管理者のアカウントの原則の設定により、Cisco Unity にログインするためにユーザが使用する電話パスワードの特性が定義されます。また、アカウントのロックアウト設定を使用すると、誤った電話パスワードが繰り返し入力された場合、ユーザアカウントをロックできます。無効なログイン試行が指定した回数繰り返されると、そのアカウントはロックされます。一定時間経過後にロックされたアカウントを自動的にロック解除するか、システム管理者がアカウントのロックを解除しなければならないかを指定することができます。以下のセクションで説明されているように、ベスト プラクティスとして、より安全性の高いアクセスを Cisco Unity アプリケーションに提供できるように、デフォルトの電話パスワードとアカウントのロックアウト設定を変更する必要があります。

- [ユーザテンプレートのパスワード設定](#)
- [電話パスワード設定の保護](#)
- [アカウント ロックアウト設定の保護](#)
- [料金の不正を防止するための規制テーブルの設定](#)

ユーザテンプレートのパスワード設定

ユーザテンプレート設定には、ユーザのデフォルトの電話パスワード（12345）が含まれています。Cisco Unity を不正アクセスから保護するため、デフォルトの電話パスワードを変更する必要があります。デフォルトの電話パスワードを使用してユーザアカウントを作成する前に、ユーザテンプレート上でこのパスワードを変更できます。また、電話パスワードを作成した後で、Cisco Unity Bulk Import ウィザードを使用して、複数のユーザの電話パスワードを一度に変更することもできます。（詳細は、Cisco Unity Bulk Import のオンラインヘルプを参照してください）。ベスト プラクティスとして、ユーザパスワードを設定する場合は、長く（8文字以上）簡単にわからないパスワードを指定してください。ユーザが自分のパスワードを変更することを許可した場合も、同様のパスワード設定を勧めてください。

電話パスワード設定の保護

ベスト プラクティスとして、Cisco Unity 管理者でパスワードとアカウント ポリシーを設定する場合、次のフィールドを有効にしないでください。

- [パスワードを無期限にする]
- [パスワードなしを許可]
- [パスワードの履歴を記録しない]

その代わりに、次のガイドラインを使用して、Cisco Unity サーバでの電話パスワードのセキュリティを強化します。

電話パスワードの最大有効期間

[有効期間 (日)] フィールドが選択されている場合、ユーザは X 日ごとにパスワードを変更するように求められます。ここで X は隣のボックスで指定された値です。



表 1 電話パスワードの最大有効期間

デフォルト設定	より安全な設定
42	30

電話パスワードの長さ

[パスワードの最少桁数]を選択すると、ユーザは最低でも X 文字のパスワードを作成するように求められます。ここで X は隣のボックスで指定された値です。一般的に、短いパスワードは使いやすいですが、長いパスワードの方がより安全です。パスワードの最少桁数を変更すると、ユーザは次にパスワードを変更する場合、新しい桁数で入力するように求められます。

表 2 電話パスワードの長さ

デフォルト設定	より安全な設定
3 文字	8 文字

電話パスワードの独自性

[記録するパスワード数]フィールドを選択すると、Cisco Unity は、ユーザの以前のパスワードを指定された数だけ保管して、パスワード履歴を実施します。Cisco Unity は、新しいパスワードと以前のパスワードを比較して、一意性を決定します。Cisco Unity は、履歴に保存されたパスワードが新しいパスワードと一致すると、そのパスワードを拒否します。デフォルトでは、Cisco Unity はパスワード履歴を保持しないということに注意してください。ベストプラクティスとして、電話パスワードの履歴を実施するため、[記録するパスワード数]フィールドを有効にし、隣のボックスに入力する次の値を考慮する必要があります。

表 3 電話パスワードの独自性

デフォルト設定	より安全な設定	最も安全な設定
無効（または有効の場合は 1）	10 パスワード	24 パスワード

安全性のため単純なパスワードは禁止する

このチェックボックスをオンにすると、Cisco Unity は新しいパスワードが次の基準を満たすかどうかを確認します。

- パスワードが以前のパスワードと異なる
- 同じ数字が繰り返されていない（たとえば 9999）
- 数字が連続していない（たとえば 1234）
- パスワードがユーザに割り当てられた内線番号と同じでない
- パスワードがユーザの名前のスペルになっていない

ベストプラクティスとして、[安全性のため単純なパスワードは禁止する]フィールドを有効にしてください。[パスワードなしを許可]ボックスをオンにすると、[安全性のため単純なパスワードは禁止する]フィールドが自動的に無効になる点に注意してください。



関連マニュアル

電話パスワードの設定の詳細については、『Cisco Unity システム アドミニストレーション ガイド』 (http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag403/ex/index.htm に掲載) の「アカウントの原則の設定」の章にある、「電話パスワードの制限の設定」セクションを参照してください。

アカウント ロックアウト設定の保護

デフォルトでは、ログイン試行の上限に達すると、Cisco Unity ではユーザ アカウントへの電話アクセスがブロックされます。(ただし、ユーザは Cisco Personal Communications Assistant を使用してそのアカウントにアクセスし、受信ボックスからメッセージを再生できます)。有効なログインによってアカウントがアクセスされた場合、Cisco Unity はログインの試行回数を 0 にリセットします。ベスト プラクティスとして、[ロックアウトしない] フィールドは有効にしないでください。その代わりに、次のガイドラインを使用して、Cisco Unity サーバ上でのアカウントのセキュリティを強化してください。

[アカウントのロック __ 回後のログイン失敗後] フィールド

このフィールドには、ログイン試行の失敗回数を入力し、この値を越えると Cisco Unity は、ユーザ アカウントへの電話アクセスをブロックします。

表 4 表 4 [アカウントのロック __ 回後のログイン失敗後] フィールド

デフォルト設定	より安全な設定	最も安全な設定
6 回	4 回	3 回

[カウンタのリセット __ 分のロックアウト後]

このフィールドには、時間 (分) を入力し、この値を超えると Cisco Unity は、ログイン試行数をクリアします。ただし、試行上限に到達し、アカウントがロックされた場合は、この限りではありません。

表 5 表 5 [カウンタのリセット __ 分のロックアウト後]

デフォルト設定	より安全な設定	最も安全な設定
60 分	1440 分 (1 日)	無期限 (システム管理者はパスワードを変更する必要があります)

関連マニュアル

アカウントのロックアウトの設定の変更の詳細については、『Cisco Unity システム アドミニストレーション ガイド』 (http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag403/ex/index.htm に掲載) の「アカウントの原則の設定」の章にある、「アカウントのロックアウトの設定」のセクションを参照してください。

料金の不正を防止するための規制テーブルの設定

ユーザが Cisco Unity Assistant または Cisco Unity カンパセーションを使用して、メッセージの到着通知、FAX 送信またはコール転送用の電話番号を変更しようとした場合、Cisco Unity では適切な規制テーブルを適用して、入力された電話番号の変更が許可されているかどうかを確認します。管理者が Cisco Unity 管理者を使用して、メッセージの到着通知、FAX 送信、またはコール転送に使用される電話番号を変更しようとするときも、同様に確認されます。いずれの場合も、使用される規制テーブルは、番号を変更しようとしているユーザまたは管理者に関連付けられています。



規制テーブルにより、以下のためにユーザと管理者が使用可能な電話番号を制御できます。

- 着信転送
- Cisco Unity アプリケーションからの電話による記録と再生（Media Master で記録と再生用デバイスとして電話が指定されている場合）（Media Master は、Cisco Unity 管理者、Cisco Unity Assistant、Cisco Unity Inbox、および ViewMail で使用できます）
- FAX マシンへの FAX の送信
- メッセージ到着通知の送信
- AMIS メッセージの送信

たとえば、ユーザは内部の内線番号だけに通話を転送するように指定したり、FAX は国内の電話番号だけに送信されるように指定できます。規制テーブルは、ユーザや管理者の Cisco Unity へのアクセス方法にかかわらず、適用されます。

関連マニュアル

規制テーブルの設定の詳細については、『Cisco Unity システム アドミニストレーション ガイド』（http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag403/ex/index.htm に掲載）の「規制テーブル」の章を参照してください。

ユーザの Web アクセスのベスト プラクティス

それぞれのユーザ アカウントには、システム管理者が Cisco Unity 管理者を使用して管理するさまざまな設定があります。ユーザ設定の中には、Cisco Personal Communications Assistant (PCA) を使用して、ユーザ自身を変更できるものもあります。Cisco PCA は、Cisco Unity 管理者に似ている、Web ベースのインターフェイスです。Cisco PCA は、Cisco Unity Assistant および Cisco Unity Inbox に対する主要アクセス ポイントとしてサービスを提供する Web サイトです。これはライセンス提供される機能でもなければ、ユーザがアクセスのために COS 権限を必要とする機能でもありません。ただし、ユーザは Cisco Unity Assistant および Cisco Unity Inbox に対する適切な COS 権限を所有している必要があります。

デフォルトでは、ユーザ認証証は、ユーザが Cisco PCA にログインしたときに、ネットワークを介してクリアテキスト形式で送信されます。（統合型の Windows 認証方式を使用せずに）匿名認証方式を使って Cisco Unity 管理者や Status Monitor を設定する場合も、同じことが当てはまります。また、ユーザが Cisco PCA ページや Cisco Unity 管理者で入力する情報は（使用した認証方式にかかわらず）、暗号化されません。セキュリティを強化するため、Security Socket Layer (SSL) プロトコルを使用するように Cisco Unity をセットアップすることを推奨します。

SSL を使用するための Cisco Unity の設定については、

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag403/ex/index.htm に掲載されている、『Cisco Unity システム アドミニストレーション ガイド』の「SSL を使用するための Cisco Unity の設定」の章を参照してください。

Text To Speech の使用のベスト プラクティス

Text to Speech (TTS) 機能を使うと、Cisco Unity のユーザは、電話を使用して電子メールを聞くことができます。Cisco Unity は、電子メール メッセージのテキスト部分を読み取り、送信者の名前（送信者がユーザの場合）、メッセージの送信日と送信時刻などの追加情報を提供します。



ただし、ユーザへの TTS の提供には、セキュリティ上のリスクがあると考えられる場合もあります。リスクを最小限に抑えるため、適用可能なユーザ COS で TTS を無効にしたり、2 ファクタ ユーザ認証として知られている安全なログイン方式を使用するように、Cisco Unity ユーザアカウントを設定できます。Cisco Unity は、拡張電話セキュリティの方式を提供するため、RSA SecurID システムで動作します。Cisco Unity 管理者では、拡張電話セキュリティを有効にしたサービス クラスに、ユーザを割り当てることができます。

拡張されたセキュリティは、これまで Cisco Unity を使用する場合でも利用可能で、Cisco Unity にアクセスするユーザを認証するための、安全な方法を実現します。RSA ACE Server、ACE Agent、SecurID Token fob は、Cisco Unity システムに含まれていませんが、個別に購入する必要があります。Cisco Unity と RSA SecurID システム連携やセットアップの詳細については、『Cisco Unity システム アドミニストレーション ガイド』(http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity40/sag/sag403/ex/index.htm に掲載) の「拡張電話セキュリティ」の章を参照してください。

Cisco Unity サーバ セキュリティ ポリシー

このセクションでは、デフォルトの「汎用」Cisco Unity サーバの設定をさらに強化する方法について説明します。Cisco Unity のインストールが終了したら、このセクションで提案されている変更を実施することをお勧めします。このセクションで説明されている設定の変更については、Microsoft 社の Web サイトで、「セキュリティ構成ツール セットを使用するためのステップバイステップガイド」を検索してください。

次のセクションを参照してください。

- [Cisco Unity サーバのセキュリティ設定の変更](#)
- [強固なパスワードの使用](#)
- [リモート アクセスの保護](#)
- [物理ユニットの保護](#)
- [TCP ポートの保護](#)
- [RPC ダイナミック ポート 範囲の制限](#)
- [TCP/IP フィルタリングの適用](#)
- [ウイルス攻撃からの Cisco Unity の保護](#)

Cisco Unity サーバのセキュリティ 設定の変更

Cisco Unity サーバへのアクセスを制限するには、表 6 に示されているセキュリティ強化設定を使用します。サイトにセキュリティ ポリシーをすでに設定している場合は、次のポリシー設定を見直して、Cisco Unity サーバを保護するために、追加の設定が必要かどうかを判断します。これらの設定は、セキュリティ テンプレートを適用せずに、手動で行うこともできます。Cisco Unity がどのようにアクセスされているかを追跡するため、監査をオンにすることが重要です。監査が有効でない、いつだれがシステムにアクセスしたか分かりません。



表 6 ローカル ポリシー : 監査ポリシーとユーザ権限の割り当て

設定	デフォルト値	推奨値
アカウント ログイン イベントの監査	監査なし	失敗
アカウントの管理の監査	監査なし	成功、失敗
ディレクトリ サービスのアクセスの監査	監査なし	失敗
ログイン イベントの監査	失敗	失敗
オブジェクト アクセスの監査	監査なし	監査なし
ポリシーの変更の監査	監査なし	成功、失敗
特権使用の監査	失敗	失敗
システム イベントの監査	監査なし	監査なし
オペレーティング システムの一部として動作	Cisco Unity をインストールするために使用したアカウント	Cisco Unity をインストールするために使用したアカウント
ネットワーク経路でこのコンピュータへアクセス	バックアップ オペレータ、 パワー ユーザ、ユーザ、管理者、 servername\IWAM、 domainname\ISUR_servername、 Everyone	デフォルトと同じ (ただし、Everyone を含まない)
システムのシャット ダウン	バックアップ オペレータ、 パワー ユーザ、管理者	バックアップ オペレータ、管理者

強固なパスワードの使用

包括的なセキュリティ ポリシーの一部として、強固なパスワードを使用する必要があります。強固なパスワードは、Windows 2000 で実現できます。強固なパスワードは、ドメイン パスワード ポリシー設定の [パスワードは要求する複雑さを満たす] 設定を有効にすることで実施できます。

すべての Cisco Unity アカウントは、最低 8 文字以上のパスワードを使う必要があります。Cisco Unity サーバのインストール中に、インストーラ アカウントやサンプル管理者アカウントなどの Cisco Unity のエンティティには、15 文字のパスワードが指定されます。これらのパスワードは、複雑さの要件を満たすようにランダムに生成されます。これらのアカウントは、使用可能になる前に、適切な権限を持つ管理者によって、パスワードをリセットされなければなりません。詳細は、「[音声メッセージング ユーザ アカウント作成のベスト プラクティス](#)」のセクションを参照してください。

表 7 に示す設定は、Cisco Unity サーバの Windows Local Security Policy のユーティリティを使用して、変更できます。



表7 ローカル ポリシー : セキュリティ オプション

設定	デフォルト値	推奨値
匿名接続の追加の制限	なし、デフォルトの権限による	SAM アカウントと共有の列挙を許可しない
システムをシャットダウンするのにログオンを必要としない	DISABLED	DISABLED
バックアップと復元の特権の使用を監査する	DISABLED	DISABLED
システムのシャットダウン時に仮想メモリのページファイルをクリアする	DISABLED	DISABLED
常にクライアント側の通信にデジタル署名を行う	DISABLED	DISABLED
可能な場合、クライアントの通信にデジタル署名を行う	ENABLED	ENABLED
常にサーバの通信にデジタル署名を行う	DISABLED	DISABLED
可能な場合、サーバの通信にデジタル署名を行う	DISABLED	ENABLED
ログインに Ctrl+Alt+Del キーを必要としない	DISABLED	DISABLED
ログイン画面に最後のユーザ名を表示しない	DISABLED	ENABLED
LAN Manager 認証レベル	LM と NTLM 応答の送信	NTLM 応答のみ送信
ログイン時のユーザへのメッセージのテキスト	(空白)	システムが認証によってのみ使用可能なことを示す、お客様固有の情報。この情報は、不正アクセスが発生した場合の法的な保護として重要です。
ログイン時のユーザへのメッセージのタイトル	(空白)	システムが認証によってのみ使用可能なことを示す、お客様固有の情報。この情報は、不正アクセスが発生した場合の法的な保護として重要です。
以前のログインをキャッシュする数 (ドメイン コントローラが使用できない場合)	10 ログイン	5 ログイン
コンピュータ アカウント パスワードのシステム保守をしない	DISABLED	ENABLED
パスワードが無効になる前にユーザに変更を促す	14 日前	7 日前
管理者アカウント名の変更	管理者	推測が困難な値
CD-ROM へのアクセスを、ローカル ログオン ユーザだけに制限する	DISABLED	ENABLED
フロッピーへのアクセスを、ローカル ログオン ユーザだけに制限する	DISABLED	ENABLED



チャンネルの保護：常にセキュリティ チャンネルのデータをデジタル的に暗号 化または署名する	DISABLED	ENABLED
チャンネルの保護：強固な（Windows 2000 かそれ以降のバージョン） セッ ションキーを必要とする	DISABLED	ENABLED
サードパーティ製の SMB サーバへ接 続するためのパスワードを、暗号化し ないで送信する	DISABLED	DISABLED
スマート カードの取り出し時の動作	何もしない	ワークステーションをロックする
署名されていないドライバのインス トール時の動作	警告するがインストールは許可する	インストールを許可しない
署名されていないドライバ以外のイン ストール時の動作	警告なしで許可する	警告なしで許可する / 警告するがイン ストールは許可する

表 8 に示す設定は、Cisco Unity サーバの Windows Local Security Policy のユーティリティを使用して、変更でき
ます。

表 8 イベント ログ設定

設定	デフォルト値	推奨値
アプリケーション ログの最大サイズ	8192 KB	未定義
セキュリティ ログの最大サイズ	512 KB	5120 KB
システム ログの最大サイズ	512 KB	1024 KB
アプリケーション ログのゲストアクセスの制限	DISABLED	ENABLED
セキュリティ ログのゲストアクセスの制限	DISABLED	ENABLED
システム ログのゲスト アクセスの制限	DISABLED	ENABLED
システム ログの保存日数	7 日間	14 日間
アプリケーション ログの保存方法	必要に応じて	必要に応じて
セキュリティ ログの保存方法	日数	必要に応じて

表 9 に示すサービスは、Cisco Unity サーバで無効にする必要がありますが、[IPSec ポリシー エージェント] の設
定は除きます。[管理ツール] フォルダの [サービス コントロール パネル] にアクセスすることによって、これ
らのサービスを無効にできます。


表 9 サービス設定

設定	デフォルト値	推奨値
Alerter	自動	無効
Application Management	手動	手動
Automatic Updates	自動	自動
Background Intelligent Transfer Service	手動	手動



Clipboard	手動	無効
COM+ Event System	手動	手動
Computer Browser	自動	無効
CsBridgeConnector	手動	手動
DHCP Client	自動	無効
Distributed File System	自動	無効
Distributed Link Tracking Client	自動	無効
Distributed Link Tracking Server	手動	無効
Distributed Transaction Coordinator	自動	自動
DNS Client	自動	自動
DNS Server	自動	自動
Event Log	自動	自動
Fax Service	手動	無効
File Replication Service	自動	自動
IIS Admin Service	自動	自動
Indexing Service	手動	手動
Internet Connection Sharing	手動	無効
Intersite Messaging	自動	自動
IPSEC Policy Agent	自動	自動
Kerberos Key Distribution Center	自動	自動
License Logging Service	自動	自動
Logical Disk Manager	自動	自動
Logical Disk Manager Administrative Service	手動	手動
Message Queuing	自動	自動
Messenger	自動	無効
Microsoft Exchange Event	手動	手動
Microsoft Exchange IMAP4	自動	無効
Microsoft Exchange Information Store	自動	自動
Microsoft Exchange Management	自動	自動
Microsoft Exchange MTA Stacks	自動	自動
Microsoft Exchange POP3	自動	無効
Microsoft Exchange Routing Engine	自動	自動
Microsoft Exchange Site Replication Service	無効	無効
Microsoft Exchange System Attendant	自動	自動
Microsoft Search	自動	自動
MSSQLSERVER	自動	自動



MSSQLServerADHelper	手動	手動
Net Logon	自動	自動
NetMeeting Remote Desktop Sharing	手動	無効
Network Connections	手動	手動
Network DDE	手動	手動
Network DDE DSDM	手動	手動
Network News Transport Protocol (NNTP)	自動	無効
NT LM Security Support Provider	手動	手動
Performance Logs and Alerts	手動	手動
Plug and Play	自動	自動
Print Spooler	自動	無効
Protected Storage	自動	自動
QoS RSVP	手動	手動
Remote Access Auto Connection Manager	手動	無効
Remote Access Connection Manager	手動	無効
Remote Procedure Call (RPC)	自動	自動
Remote Procedure Call (RPC) Locator	自動	自動
Remote Registry Service	自動	無効
 警告 Cisco Unity をインストールし、フェールオーバーを設定するには、Remote Registry Service を有効にしてください。Cisco Unity をインストールするか、フェールオーバーを設定した直後、このサービスを再度、無効にする必要があります。		
Removable Storage	自動	自動
Routing and Remote Access	無効	無効
RunAs Service	自動	自動
Security Accounts Manager	自動	自動
Server	自動	自動
Simple Mail Transport Protocol (SMTP)	自動	自動
Smart Card	手動	手動
Smart Card Helper	手動	手動
SQLSERVERAGENT	自動	自動
System Event Notification	自動	自動
Task Scheduler	自動	自動
TCP/IP NetBIOS Helper Service	自動	自動
Telephony	手動	手動
Telnet	手動	手動



Terminal Services	自動	自動
Uninterruptible Power Supply	手動	手動
Utility Manager	手動	手動
Windows Installer	手動	手動
Windows Management Instrumentation	自動	自動
Windows Management Instrumentation Driver Extensions	手動	手動
Windows Time	自動	自動
Workstation	自動	自動
World Wide Web Publishing Service	自動	自動

リモート アクセスの保護

Cisco Unity サーバ上で Telnet アクセスを許可しないでください。また、Cisco TAC が Cisco Unity サーバをサポートする間にモデムが必要なため、ベスト プラクティスとして、モデムをオフにするか、使用しない場合は接続を解除する必要があります。

物理ユニットの保護

不正なアクセスから物理ユニットを保護するためのベスト プラクティスは、CERT Coordination Center(CERT/CC) の Web サイトで参照できます。CERT サイトの「Security Improvement Module」内にある、「Practices About Hardening and Securing Systems」のセクションを参照してください。

TCP ポートの保護


Cisco Unity を機能させるのに特定のサービスを有効にする必要があるのと同様に、特定の TCP ポートも全機能を実現するために、オープンなままにする必要があります。表 10 は、オープンなポートと、関連するプロトコルやサービスのリストです。

表 10 TCP ポートの設定

TCP ポート	プロトコル/サービス
25	SMTP
53	DNS
80	HTTP
135	MS-RPC
139	NETBIOS-SESSION
389	LDAP
443	HTTP/SSL
445	MICROSOFT-DS
636	LDAP/SSL
691	SMTP/LSA



1433	MS-SQL-S
3268	LDAP
3269	LDAP/SSL
3372	MSDTC
3389	WTS
ダイナミック	RPC-DCOM

 **注** Cisco Unity サーバにインストールされたサードパーティ製のソフトウェア（ウイルス防止やバックアップソフトウェアなど）に対処するためには、追加ポートをオープンにする必要がある場合があります。


RPC-DCOM を除き、すべてのプロトコルとサービスでは静的ポートが使用されます。したがって、TCP/IP フィルタを適用する場合の唯一の障害は、既知のポート範囲に RPC-DCOM が制限されることです。

オープンなポートの詳細については、Microsoft Knowledge Base のセクション（278339）を参照してください。

RPC ダイナミック ポート 範囲の制限

RPC ダイナミック ポート割り当てを制限するには

-
- | | |
|--------|--|
| ステップ 1 | Windows の [スタート] メニューで、[プログラム] > [管理ツール] > [コンポーネント サービス] の順にクリックします。 |
| ステップ 2 | ステップ 2 [コンポーネント サービス] と [コンピュータ] ノードを展開表示します。[マイ コンピュータ] を右クリックし、[プロパティ] をクリックします。 |
| ステップ 3 | ステップ 3 [既定のプロトコル] タブの [DCOM プロトコル] リストから、[コネクション型 TCP/IP] をクリックし、続いて [プロパティ] をクリックします。 |
| ステップ 4 | ステップ 4 [COM インターネット サービスのプロパティ] ダイアログ ボックスで、[追加] をクリックします。 |
| ステップ 5 | ステップ 5 [ポート範囲] テキスト ボックスに、ポート範囲（たとえば、5000 ~ 5020 を入力）を追加し、[OK] をクリックします。 |
-

 **注** 20 ポートより小さいポート 範囲を入力すると、いくつかのサービスが起動しなくなります。


- | | |
|--------|---|
| ステップ 6 | [ポート範囲の割り当て] オプションと、[既定のダイナミック ポート割り当て] オプションを、[インターネットの範囲] に設定します。 |
| ステップ 7 | [OK] を 3 回クリックします。 |
| ステップ 8 | Cisco Unity サーバを再起動します。 |
-

ダイナミック ポート範囲の制限についての詳細は、Microsoft Knowledge Base のセクション（300083）を参照してください。



TCP/IP フィルタリングの適用

TCP/IP フィルタリングを設定するには

-
- ステップ 1** デスクトップで [マイ ネットワーク] を右クリックし、続いて [プロパティ] をクリックします。
- ステップ 2** [ネットワークとダイヤルアップ接続] ダイアログ ボックスで、[ローカル エリア接続] を右クリックし、続いて [プロパティ] をクリックします。
- ステップ 3** [ローカル エリア接続のプロパティ] ダイアログ ボックスで、[インターネット プロトコル (TCP/IP)] をクリックし、続いて [プロパティ] をクリックします。
- ステップ 4** [インターネット プロトコル (TCP/IP) のプロパティ] ダイアログ ボックスで、[詳細設定] をクリックします。
- ステップ 5** [TCP/IP 詳細設定] ダイアログ ボックスの [オプション] タブで、[TCP/IP フィルタリング] をクリックし、続いて [プロパティ] をクリックします。
- ステップ 6** [TCP/IP フィルタリング] ダイアログ ボックスで、[TCP/IP フィルタリングを有効にする (すべてのアダプタ)] チェック ボックスをオンにし、[TCP ポートに対してのみ許可する] を選択します。
- ステップ 7** [追加] をクリックし、[フィルタの追加] ダイアログ ボックスにポート番号を入力し [OK] をクリックします。
- ステップ 8** アクセスを許可する各ポートに対して、[ステップ 7](#) を繰り返します。
推奨されるポートのリストについては、[表 10](#) を参照してください。
-
-  **注** Cisco Unity サーバにインストールされたサードパーティ製のソフトウェア（ウイルス防止やバックアップソフトウェアなど）に対処するためには、追加ポートをオープンにする必要がある場合があります。
-
- ステップ 9** [OK] を 4 回クリックし、コンピュータを再起動します。
-

ウイルス攻撃からの Cisco Unity の保護

ウイルス攻撃のリスクを最小限に抑えるため、Cisco Unity サーバにアンチウイルス ソフトウェアのパッケージをインストールします。ただしその前に、次の問題に対処する必要があります。

Cisco Unity のインストール中は、アンチウイルス ソフトウェアを無効にする

Cisco Unity をインストールした後で、アンチウイルス ソフトウェアをインストールするのが最善の方法です。Cisco Unity アプリケーションをインストールする前に、アンチウイルス ソフトウェアがすでにインストールされている場合は、処理を続行する前に、このソフトウェアを無効にします。場合によっては、いったん、アンチウイルス ソフトウェアを完全に削除し、Cisco Unity のインストール終了後に再インストールしなければならないという点に注意してください。

Exchange を保護するため、Microsoft 社の推奨事項を使用する

Exchange が Cisco Unity サーバにインストールされている場合は、ウイルス攻撃からの Exchange サーバの保護に関する最新情報について、Microsoft 社の Web サイトを参照してください。

SQL サーバと MSDE を保護するため、Microsoft 社の推奨事項を使用する

ウイルス攻撃からの SQL サーバと MSDE の保護に関する最新情報について、Microsoft 社の Web サイトを参照してください。



メッセージ スキャンを使用する場合は、注意する

ウイルスをスキャンする前に、スキャンの実行が Cisco Unity サーバのパフォーマンスに与える影響を考慮する必要があります。たとえば、完全なファイル IO スキャンを実行すると、Cisco Unity サーバのパフォーマンスにマイナスの影響を与える可能性があります。Cisco Unity サーバのパフォーマンスに劇的な影響を与えかねないメッセージ スキャンは、使用しないでください。

ハッカーの攻撃から Cisco Unity を保護する

不要なアクセスや不正アクセスからサーバを保護するには、Microsoft 社の推奨事項に従ってください。脆弱性スキャナ（Cisco Scanner、Nessus、SAINT など）を入手できます。これらの製品を使用すると、ネットワーク上のセキュリティの脆弱性が特定されます。ベスト プラクティスとして、Cisco Unity サーバにスキャナをインストールしないでください。

また、Cisco Unity を保護するように特別に設定されている Cisco Security Agent (CSA) は、Cisco.com で入手できます。Cisco Security Agent は、サーバおよびデスクトップ コンピューティング システムに、脅威からの保護を提供します。Cisco Security Agent を使用すると、ホストの不正侵入防止、分散ファイアウォール、不正モバイルコード保護、オペレーティング システムの整合性の保証、監査ログの統合が組み合わせられ、複数のセキュリティ機能が集約されます。Cisco Unity サーバに CSA をインストールすることを強く推奨します。

オンライン リファレンス

この文書で参照されているトピックの詳細については、次のサイトへアクセスしてください。

Cisco Unity の資料

Cisco Unity 4.0 の製品資料は、

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_technical_documentation.html に掲載されています。

Cisco Unity の White Paper とアプリケーション ノートは、

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_technical_reference_list.html に掲載されています。

Cisco Unity のインストール、保守、および使用に関するテクニカル ティップスは、

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_tech_notes_list.html に掲載されています。

CERT Coordination Center (CERT/CC) の Web サイト

<http://www.cert.org/>

Internet Engineering Task Force (IETF) の Web サイト

<http://ietf.org/>

Microsoft 社の Web サイト

Microsoft 社の Security Web サイト

<http://www.microsoft.com/security/default.asp>

Microsoft 社の TechNet Web サイト

<http://www.microsoft.com/techNet/>

©2003 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。
この文書で説明した商品、サービスはすべて、それぞれの所有者の商標、サービスマーク、登録商標、登録サービスマークです。
この資料に記載された仕様は予告なく変更する場合があります。



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.03-6655-4433

電話でのお問合せは、以下の時間帯で受け付けております。

平日 10:00 ~ 12:00 および 13:00 ~ 17:00

お問い合わせ先