CHAPTER 5

# Cisco Unified MeetingPlace Web Conferencing への外部アクセスの設定

ファイアウォール内のポートを開くだけで Cisco Unified MeetingPlace Web 会議への外部アクセスが可能になりますが、この方法はセキュリティが不十分であるため、お勧めしません。代わりに、Cisco Unified MeetingPlace Web Conferencing では Segmented Meeting Access 構成をサポートしています。これを使用すると、ネットワーク セキュリティを維持したまま、ユーザに外部アクセスを提供できます。

次の項を参照してください。

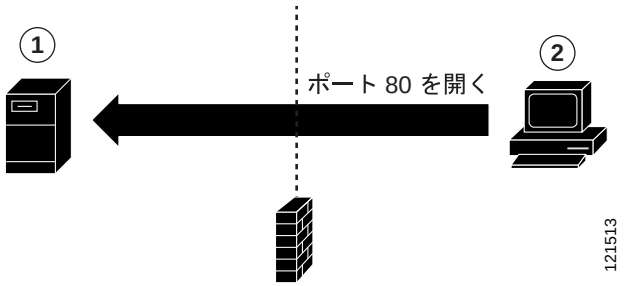
# ファイアウォールについて

## ファイアウォールの基本

ファイアウォールとは、ローカル エリア ネットワーク（LAN）を好ましくないインターネット アクセスから保護するように設定されたセキュリティ デバイスです。ただし、特定の TCP ポートを開いて共用サーバへの着信アクセスを許可することで、ネットワークの一部を保護したまま、他の部分に制限付きアクセスを提供できます。たとえば、インターネット上のユーザが企業のホーム ページに接続する場合、図 5-1 に示すように、ユーザは企業のファイアウォールの TCP ポート 80 を経由して、Web サーバにアクセスする必要があります。

したがって、他に特別な操作をしなくても、ネットワーク上のポートを開くことで、Cisco Unified MeetingPlace Web 会議への外部アクセスを許可できます。

**図 5-1　一般的なファイアウォールの設定**




| | | | |
|---|---|---|---|
| 1 | 企業のプライベート ネットワークの内部にある Cisco Unified MeetingPlace Web サーバ | 2 | 企業のプライベート ネットワークの外側にあるエンドユーザ システム |

## ファイアウォールに関するポート アクセス要件

ファイアウォールでポート 80 が Web Conferencing サーバ上の両方のホスト名または IP アドレスに対して着信方向に開いていれば、会議コンソールを使用する外部ユーザは Cisco Unified MeetingPlace Web 会議に参加できます。ただし、ポート 80 では会議コンソール接続（Web Conferencing のホスト名または IP アドレス）に対して「トンネリング」が必要なため、Web 会議の速度が低下します。したがって、Web 会議のパフォーマンスを最適に保つには、TCP ポート 80 をホーム ページのホスト名または IP アドレスに対して着信方向に開き、さらに TCP ポート 1627 を Web Conferencing のホスト名または IP アドレスに対して着信方向に開くことを強くお勧めします。

展開で SSL を使用する場合は、ファイアウォールでポート 443 が Web Conferencing サーバ上の両方のホスト名または IP アドレスに対して着信方向に開いていることを確認します。

外部参加者がファイアウォールの内側にいる場合、参加者は自分の側で同じポートを出力方向に開く必要があります。

# Secure Sockets Layer の設定方法

Secure Sockets Layer（SSL）は、ネットワークを横断するデータを暗号化することにより、Web 会議の共有情報をセキュリティで保護します。

### 制約事項

- Web Conferencing SSL を設定する前に、Cisco Unified MeetingPlace をインストールする必要があります。
- 外部 Web サーバで SSL を使用する場合、SSL 証明書上のホスト名が外部 Web サーバの IP アドレスに解決されることを確認します。
- セグメント化された DNS を使用システム上で SSL を使用する場合は、SSL 証明書上のホスト名がセグメント化された DNS 名と異なることを確認します。ホーム ページのホスト名または Web Conferencing のホスト名を変更する場合は、P.2-29 の「Web サーバの設定」を参照してください。
- ユーザがファイアウォール経由で Web Conferencing サーバにアクセスする場合は、ファイアウォールでポート 443 がサーバ上の両方のホスト名または IP アドレスに対して着信方向に開いていることを確認します。

### 作業リスト

1. SSL/TLS 設定ページを使用して、デジタル ID 証明書に適用するために認可された認証局に送信する証明書署名要求を生成します。2 つの証明書が必要です。1 つはホーム ページのホスト名用のもので、もう 1 つは Web Conferencing のホスト名用のものです。手順については、P.5-3 の「証明書署名要求を新規に作成して証明書ファイルを取得する」を参照してください。
2. 認証局から証明書を受け取ったら、証明書を Cisco Unified MeetingPlace Web Conferencing Web サイトに適用します。手順については、P.5-4 の「SSL 証明書を Cisco Unified MeetingPlace Web Conferencing Web サイトに適用する」を参照してください。
3. ［Web Server］管理ページの［Require SSL］フィールドを有効にします。手順については、P.5-5 の「SSL を有効にする」を参照してください。
4. SSL 接続をテストします。手順については、P.5-5 の「HTTPS 接続を介して Web サーバをテストする」を参照してください。

### 証明書署名要求を新規に作成して証明書ファイルを取得する

**ステップ 1**　Cisco Unified MeetingPlace Web Conferencing にサインインします。

**ステップ 2**　［ようこそ］ページで、**［Admin］**をクリックします。

**ステップ 3**　**［SSL/TLS］**をクリックします。［SSL/TLS］ページが表示されます。

**ステップ 4**　ホーム ページのホスト名に対応する**［Edit］**アイコンをクリックします。

**ステップ 5**　適切なフィールドに、会社名と、組織ユニットまたは部門を入力します。

**ステップ 6**　適切なフィールドに、市区町村および都道府県の完全な正式名称を入力します。略称は使用しないでください。

**ステップ 7**　国または地域を選択します。

**ステップ 8**　**［Generate Request］**をクリックします。下のテキスト ボックスに新しい Certificate Signing Request（CSR; 証明書署名要求）が表示されます。要求は、自動生成された秘密鍵を使用して署名されています。秘密鍵の値を表示するには、**［Private Key］**リンクをクリックします。

**ステップ 9**　CSR テキスト ボックスの内容をテキスト ファイルにコピーします。次に、このファイルを認証局に送信し、証明書ファイルを取得します。

**注意**　認証局からサーバ タイプについて尋ねられた場合は、Apache または Custom を指定します。Microsoft または IIS は指定しないでください。SSL/TLS 設定ページを使用して Microsoft または IIS 証明書をインストールし、システムをリブートしようとすると、Cisco Unified MeetingPlace Web Conferencing は再起動せずに、証明書に関するエラーを記録し、SSL を無効にします。この場合は、再起動し、問題を解決します。

**ステップ 10**　［**Back**］をクリックします。

**ステップ 11**　Web Conferencing のホスト名について、ステップ 3 からステップ 10 を繰り返します。

**ステップ 12**　認証局から .cer ファイルを受け取ったら、P.5-4 の「SSL 証明書を Cisco Unified MeetingPlace Web Conferencing Web サイトに適用する」に進みます。

### SSL 証明書を Cisco Unified MeetingPlace Web Conferencing Web サイトに適用する

**ステップ 1**　Cisco Unified MeetingPlace Web Conferencing にサインインします。

**ステップ 2**　［ようこそ］ページで、［**Admin**］をクリックします。

**ステップ 3**　［**SSL/TLS**］をクリックします。［SSL/TLS］ページが表示されます。

**ステップ 4**　ホーム ページのホスト名に対応する［**Edit**］アイコンをクリックします。

**ステップ 5**　ホーム ページのホスト名の証明書ファイルをテキスト エディタで開き、テキストをクリップボードにコピーします。

**ステップ 6**　ページの下部にあるテキスト ボックスに、このホスト名用に入手した証明書のテキストを貼り付けます。貼り付けたテキストに証明書の開始デリミタと終了デリミタが含まれていることを確認します。

**ステップ 7**　［**Install Certificate**］をクリックします。これで、ホストに証明書がセットアップされました。

**ステップ 8**　［**Back**］をクリックします。

**ステップ 9**　Web Conferencing のホスト名について、ステップ 3 からステップ 8 を繰り返します。

**ステップ 10**　P.5-5 の「SSL を有効にする」に進みます。

### SSL を有効にする

**ステップ 1**　［SSL/TLS］ページで、［**Toggle SSL**］をクリックして SSL をオンにします。

**ステップ 2**　［**Reboot Server**］をクリックします。サーバがシャットダウンしてから再起動します。

**（注）**　Web Conferencing サーバが SSL 証明書を検証できない場合、サーバはエラーを記録し、SSL をオフに切り替えます。この場合は、Web Conferencing サーバを再起動し、問題を解決してから、この手順を繰り返します。

### HTTPS 接続を介して Web サーバをテストする

**ステップ 1**　Web サーバから、Web ブラウザを使用して、Web サーバの完全修飾ドメイン名（FQDN）である https://hostname.domain.com に接続します。

Cisco Unified MeetingPlace Web Conferencing のホーム ページが表示された場合、ホーム ページのホスト名への接続は成功しています。

セキュリティ警告のダイアログボックスが表示された場合は、ダイアログボックスを表示しないように SSL を設定します。詳細については、Microsoft の Web サイトでマイクロソフト サポート技術情報 813618 および 257873 を参照してください。

**ステップ 2**　Cisco Unified MeetingPlace Web Conferencing にサインインします。

**ステップ 3**　［即時会議］をクリックします。

会議コンソールが開いた場合、Web Conferencing のホスト名への接続は成功しています。

# Segmented Meeting Access について

外部参加者を受け入れる方法として、ファイアウォール経由のポート アクセスを制御することは有効ですが、代わりに Segmented Meeting Access（SMA）構成を検討することを強くお勧めします。SMA 構成は、企業のプライベート ネットワーク上で一部の会議を分離し、外部として指定されたその他の会議をインターネットに公開します。ユーザは、スケジュール作業の中で［新しい会議］スケジューリング ページの［外部 Web 参加者を許可］パラメータを設定することで、会議を内部または外部として指定します。

（注）　Segmented Meeting Access-1 Server（SMA-1S）構成は、Cisco Unified MeetingPlace Web Conferencing Release 6.x ではサポートされなくなりました。

## SMA-2S 構成について

（注）　システム要件については、次の URL の『*Cisco Unified MeetingPlace システム要件*』を参照してください。http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html

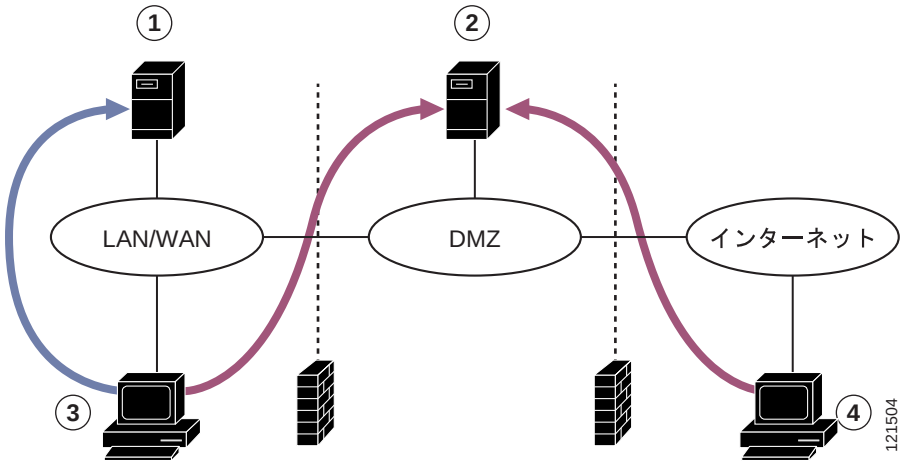
Segmented Meeting Access -2 Server（SMA-2S）構成では、Cisco Unified MeetingPlace Web Conferencing は、2 つの別個の Web サーバまたは 2 つの別個の Web サーバ クラスタで展開されます。一方は、ファイアウォールの内側にある内部ネットワークで、もう一方は、非武装地帯（DMZ）などのネットワーク セグメントです。内部サーバまたはクラスタには、ファイアウォールの内側からのみアクセスできますが、外部サーバまたはクラスタには、ファイアウォールの内側と外側の両方からアクセスできます。

内部ユーザは、フルアクセス可能な Web Conferencing ユーザ インターフェイスにアクセスできますが、外部ユーザは、外部会議への参加だけが可能な参加専用 Web ページにアクセスできます。

SMA-2S 構成は、Cisco Unified MeetingPlace Web 会議への外部アクセスを提供する場合に優先される最も安全な展開モデルです。

（注）　外部 Web サーバには Secure Sockets Layer（SSL）を使用するように設定することをお勧めします。この設定によって、セキュリティが最適な状態になり、Web 会議へのユーザの参加を妨げる可能性があるプロキシ サーバの問題が解決されます。SSL の設定方法については、P.5-3 の「Secure Sockets Layer の設定方法」を参照してください。

**図 5-2　Segmented Meeting Access -2 Server 構成**




| | | | |
|---|---|---|---|
| **1** | 内部 Cisco Unified MeetingPlace Web サーバ<br>• この Web 会議サーバは、企業のプライベート ネットワークの内部に配置されます。 | **2** | 外部 Cisco Unified MeetingPlace Web サーバ<br>• この Web 会議サーバは、DMZ などのネットワーク セグメントに配置されます。 |
| **3** | 内部ユーザ。<br>• 内部ユーザは、内部会議に参加するときは内部 Web サーバを経由します。<br>• 内部ユーザは、外部会議に参加するときは外部 Web サーバを経由します。 | **4** | 外部ユーザ。<br>• 外部ユーザは、外部会議だけに参加できます。<br>• 外部会議に参加する外部ユーザは、外部 Web サーバを経由します。 |

## SSL およびセグメント化された DNS を使用する SMA-2S 構成について

Cisco Unified MeetingPlace Web Conferencing システムには外部 Web サーバに SSL が構成され、セグメント化された DNS を使用する場合、セグメント化された DNS 名を、外部または内部マシン上の SSL 証明書名と同じ名前にすることはできません。構成のガイドラインについては、次の例を参照してください。

### 例

SMA-2S が構成されており、この構成では外部ユーザには SSL が必要ですが、内部または外部マシンにアクセスする内部ユーザには不要です。

- セグメント化された DNS 名は *meetingplace.company.com* です。
- 外部マシンの SSL 証明書名は *meetingplace1* です。
- 内部マシンからの外部マシンのホスト名は *meetingplace1* です。
- URL および参加リンクはすべて、http://*meetingplace.company.com* の形式です。

ユーザが外部ネットワークから http://*meetingplace.company.com* にアクセスすると、外部マシンによってユーザは HTTPS およびデータベースに設定されているホスト名（この場合は *meetingplace1*）に自動的にリダイレクトされます。

**（注）** すべてのユーザに SSL を強制すると、内部および外部ユーザは両方とも、外部 Web サーバにアクセスするときに、SSL を使用する必要があります。

# SMA-2S 展開の設定方法

この項では、SMA-2S 構成プロセスの概要を説明します。

### 始める前に

- P.5-6 の「SMA-2S 構成について」を参照してください。
- 複数の Web サーバをインストールする場合は、Purge パラメータを同期化していることを確認してください。詳細については、P.3-2 の「Web Conferencing のデータ ストレージについて」を参照してください。
- Cisco Unified MeetingPlace Web Conferencing を内部 Web サーバにインストールします。詳細については、次の URL の『*Cisco Unified MeetingPlace Web Conferencing インストレーション アップグレード ガイド*』を参照してください。
  http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html
- 内部 Web サーバの GUIDS を、外部 Web サーバにコピーします。詳細については、次の URL の『*Cisco Unified MeetingPlace Web Conferencing インストレーション アップグレード ガイド*』を参照してください。
  http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html
- Cisco Unified MeetingPlace Web Conferencing を外部 Web サーバにインストールします。詳細については、次の URL の『*Cisco Unified MeetingPlace Web Conferencing インストレーション アップグレード ガイド*』を参照してください。
  http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html

### SMA-2S 展開の設定の作業リスト

1. 内部 Web サーバで、外部会議のリダイレクションを設定します。手順については、P.5-8 の「外部会議のリダイレクションを設定する」を参照してください。
2. （オプション）Secure Socket Layer（SSL）をサポートするように外部 Web サーバを設定します。手順については、P.5-3 の「Secure Sockets Layer の設定方法」を参照してください。
3. 設定をテストします。手順については、P.5-9 の「内部会議をテストする」および P.5-10 の「外部会議をテストする」を参照してください。

### 外部会議のリダイレクションを設定する

外部会議は、ユーザがインターネットから会議に参加できるようにするため、外部 Web サーバ上で開催されます。すべてのユーザに特定の外部 Web サーバにログインさせるのではなく、内部 Web サーバから指定の外部 Web サーバへ、すべての外部会議を自動的にリダイレクトするよう設定します。

次の手順を実行する前に、すべての内部および外部 Web サーバに Cisco Unified MeetingPlace Web Conferencing を適切にインストールしておく必要があります。

---

**ステップ 1**　内部 Web サーバから、Cisco Unified MeetingPlace Web Conferencing にサインインします。

**ステップ 2**　［ようこそ］ページで、**［Admin］**、**［Web Server］**の順にクリックします。

**ステップ 3**　空白の［Web Server Name］フィールドに、指定した外部 Web サーバを表す新しい Web サーバの名前を入力します。

**ステップ 4**　［Hostname］に、外部 Web サーバの完全修飾ドメイン名（FQDN）、つまり *hostname.domain.com* を入力します。Web サーバが Domain Name Server（DNS; ドメイン ネーム サーバ）に登録されていない場合は、代わりに IP アドレスを入力します。

- 内部 Web サーバからこのホスト名を解決できる必要があります。

- SSL を使用する場合、SSL 証明書上のホスト名が外部 Web サーバの IP アドレスに解決されることを確認します。
- SSL とセグメント化された DNS を使用する場合は、DNS 名と SSL 証明書名が異なることを確認します。

**ステップ 5**　この Web サーバをデータベースに追加するには、**［Submit］**をクリックします。

これで、このサーバがページの下部にある Web サーバのリストに表示されます。

- 内部 Web サーバと外部 Web サーバがそれぞれ 1 つしかない場合は、P.5-9 の「内部会議をテストする」に進みます。
- 内部 Web サーバが複数ある場合は、ステップ 6 に進みます。

**ステップ 6**　メインの［Admin］ページに戻って**［Site］**をクリックします。［Site］管理ページが表示されます。

**ステップ 7**　内部 Web サーバのクラスタを表す［Site Name］をクリックします。

- WebConnect を展開した場合を除き、このページに表示されるサイトは 1 つだけです。
- ［Site Name］には、デフォルト値として、このクラスタにインストールした最初の Web サーバの NetBIOS 名が割り当てられます。

**ステップ 8**　［DMZ Web Server］には、追加した外部 Web サーバを選択します。

この結果、このクラスタの内部 Web サーバが、外部会議の場合にこの外部 Web サーバをポイントするように設定されます。

**ステップ 9**　**［Submit］**をクリックします。

**ヒント**　外部クラスタでは、追加で SQL Server データベースの設定を行う必要はありません。

**ステップ 10**　P.5-9 の「内部会議をテストする」に進みます。

### 内部会議をテストする

**ステップ 1**　Web ブラウザを起動して、内部 Cisco Unified MeetingPlace Web Conferencing Web サイトに移動します。

**ステップ 2**　システム管理者権限のある Cisco Unified MeetingPlace プロファイルを使用してサインインします。

**ステップ 3**　内部アクセスの会議をスケジュールして、2 つの添付ファイルを追加します。

**a.**　［ようこそ］ページで、**［会議スケジュールの作成］**をクリックします。

**b.**　会議の日時など、会議の詳細を設定します。

**c.**　**［外部 Web 参加者を許可］**では、**［いいえ］**をクリックします。

**d.**　**［添付 / 記録］**をクリックし、ドキュメント ファイルと Microsoft PowerPoint 添付の 2 つの添付を追加してから、**［OK］**をクリックします。

**e.**　**［スケジュール］**をクリックします。

**ステップ 4**　ステップ 3 でスケジューリングした会議に関する通知を受信したことを確認します。

**ステップ 5**　企業のプライベート ネットワークの内部から、通知の中にある内部の参加リンクが機能することを確認します。

a. 参加リンクをクリックします。
b. 以前にこの Web サーバでの会議に参加している場合は、会議コンソールにリダイレクトされます。
c. 以前にこの Web サーバでの会議に参加したことがない場合は、フルアクセス可能な Cisco Unified MeetingPlace Web Conferencing ユーザ インターフェイスが表示されます。

**ステップ 6**　インターネットから、通知の中にある内部の参加リンクが機能しないことを確認します。

**ステップ 7**　会議に参加できることを確認します。

- 以前にこの Web サーバでの会議に参加したことがある場合は、参加リンクをクリックすると、会議コンソールに直接移動します。
- 以前にこの Web サーバでの会議に参加したことがない場合は、会議 ID を入力し、Cisco Unified MeetingPlace Web Conferencing のホーム ページから［**会議に参加**］をクリックします。

**ステップ 8**　会議コンソールに自分のプロファイル名が表示されることを確認して、自分のプロファイルでログインしていることを確認します。

**ステップ 9**　P.5-10 の「外部会議をテストする」に進みます。

---

### 外部会議をテストする

次の手順を完了するには、システム管理者権限を持つ Cisco Unified MeetingPlace プロファイルが必要です。

---

**ステップ 1**　Web ブラウザを起動して、内部 Cisco Unified MeetingPlace Web Conferencing Web サイトに移動します。

**ステップ 2**　システム管理者権限のある Cisco Unified MeetingPlace プロファイルを使用してサインインします。

**ステップ 3**　外部アクセスの会議をスケジュールし、次のステップを完了して 2 つの添付ファイルを追加します。

a. ［ようこそ］ページで、［**会議スケジュールの作成**］をクリックします。
b. 会議の日時など、会議の詳細を設定します。
c. ［**外部 Web 参加者を許可**］では、［**はい**］をクリックします。
d. ［**添付 / 記録**］をクリックし、ドキュメント ファイルと Microsoft PowerPoint 添付の 2 つの添付を追加してから、［**OK**］をクリックします。
e. ［**スケジュール**］をクリックします。

**ステップ 4**　ステップ 3 でスケジューリングした会議に関する通知を受信したことを確認します。

**ステップ 5**　通知の中にある外部の参加リンクが機能することを確認します。

**a.** 参加リンクをクリックします。

**b.** 以前にこの Web サーバでの会議に参加している場合は、会議コンソールにリダイレクトされます。

**c.** 以前にこの Web サーバでの会議に参加したことがない場合は、外部参加専用の Cisco Unified MeetingPlace Web Conferencing ユーザ インターフェイスが表示されます。

**ステップ 6**　会議に参加できることを確認します。

- 以前にこの Web サーバでの会議に参加したことがある場合は、参加リンクをクリックすると、会議コンソールに直接移動します。
- 以前にこの Web サーバでの会議に参加したことがない場合は、会議 ID を入力して［**会議に参加**］をクリックします。

**ステップ 7**　会議コンソールに自分のプロファイル名が表示されることを確認して、自分のプロファイルでログインしていることを確認します。

**ステップ 8**　外部 Web サーバから添付とスライド ショーにアクセスできることを確認します。

**a.** 会議コンソールから、［添付］タブをクリックして添付を開けることを確認します。

**b.** 会議コンソールから、［スライド］タブをクリックしてスライドを表示できることを確認します。

**c.** プレゼンテーション モードに切り替えて、Web コラボレーション ウィンドウに最初のスライドが表示されることを確認します。