WebVPN の設定

次の事項について説明します。

WebVPN の準備

WebVPN によってユーザは、ブラウザを使用してセキュリティ アプライアンスへのセキュアなリモートアクセス VPN トンネルを確立できます。ソフトウェアやハードウェア クライアントは必要ありません。

WebVPN を使用することで、インターネット上のほぼすべてのコンピュータから、幅広い Web リソースおよび Web 対応アプリケーションへのセキュアで容易なアクセスが可能になります。次のようなアクセス先があります。

- 内部 Web サイト
- Web 対応アプリケーション
- NT/Active Directory ファイル共有
- POP3S、IMAP4S、および SMTPS などの電子メール プロキシ
- MS Outlook Web Access
- MAPI
- Application Access （他の TCP ベースのアプリケーションにアクセスするためのポート転送）

WebVPN は Secure Sockets Layer プロトコルおよびその後継である Transport Layer Security を使用して、リモート ユーザと、中央サイトで設定した特定のサポートされている内部リソースとの間で、セキュアな接続を提供します。セキュリティ アプライアンスはプロキシで処理する必要がある接続を認識し、HTTP サーバは認証サブシステムと対話してユーザを認証します。

ネットワーク管理者は、ユーザに対してグループ単位で WebVPN リソースへのアクセスを提供します。ユーザは、内部ネットワーク上のリソースに直接アクセスすることはできません。

次の項では、WebVPN アクセスを設定するための準備について説明します。

- WebVPN セキュリティ対策の順守
- WebVPN でサポートされていない機能の概要
- 中央サイトにアクセスするための SSL の使用
- デジタル証明書による認証
- Web VPN 用にブラウザのクッキーをイネーブルにする
- パスワードの管理
- WebVPN でのシングル サインオンの使用
- デジタル証明書による認証

WebVPN セキュリティ対策の順守

セキュリティ アプライアンス上の WebVPN 接続は、リモートアクセス IPSec 接続とはまったく異なっています。特に SSL 対応サーバとの対話方法やセキュリティ上のリスクを減らすための対策に大きな違いがあります。

WebVPN 接続では、セキュリティ アプライアンスは、エンド ユーザの Web ブラウザとターゲット Web サーバとの間のプロキシとして機能します。WebVPN ユーザが SSL 対応 Web サーバに接続すると、セキュリティ アプライアンスはセキュアな接続を確立し、SSL 証明書を検証します。エンド ユーザのブラウザは提示された SSL 証明書を受信しないため、この証明書を検証することはできません。

セキュリティ アプライアンス上の現在の WebVPN 実装では、有効期限が切れた証明書を提示するサイトとの通信は許可しません。また、セキュリティ アプライアンスは信頼できる CA 証明書の検証も実行しません。このため、WebVPN ユーザは、SSL 対応の Web サーバと通信する前に相手が提示する証明書を分析することができません。

SSL 証明書に関するリスクを最小限にするには、次のようにします。

1. WebVPN　アクセスを必要とするすべてのユーザからなるグループポリシーを設定し、そのグループポリシーに対してだけ WebVPN 機能をイネーブルにします。
2. WebVPN ユーザに対してインターネット アクセスを制限します。その方法の 1 つは、URL エントリをディセーブルにすることです。次に、WebVPN ユーザがアクセス可能なプライベート ネットワーク内の特定のターゲットへのリンクを設定します。
3. ユーザに適切な情報を提供します。SSL 対応サイトがプライベート ネットワーク内部にない場合、ユーザは WebVPN 接続を介してこのサイトにアクセスすることはできません。そのようなサイトにアクセスする場合、ユーザは別のブラウザ ウィンドウを開き、そのブラウザを使用して、提示された証明書を表示する必要があります。

WebVPN でサポートされていない機能の概要

セキュリティ アプライアンスは、WebVPN 接続では次の機能をサポートしていません。

- モジュラ ポリシー フレームワークの検査機能。コンフィギュレーション制御を検査する機能です。
- **vpn-filter** コマンドなどのフィルタ設定コマンドが持つ機能。
- NAT。グローバルに一意の IP アドレスの必要性を減らす機能です。
- PAT。複数の発信セッションが 1 つの IP アドレスから発信されているように見せることができる機能です。
- QoS。**police** コマンドと **priority-queue** コマンドを使用してレートを制限する機能です。
- 接続制限。スタティックまたはモジュラ ポリシー フレームワークの **set connection** コマンドを使用して、接続をチェックする機能です。
- **established** コマンド。このコマンドを使用すると、高セキュリティ ホストから低セキュリティ ホストへの接続が確立済みの場合に、低セキュリティ ホストから高セキュリティ ホストへのリターン接続が可能になります。

中央サイトにアクセスするための SSL の使用

WebVPN は SSL およびその後継である TLS1 を使用して、リモート ユーザと、中央サイトにある特定のサポートされている内部リソースとの間で、セキュアな接続を提供します。ここでは、次の項目について説明します。

- WebVPN セッション用 HT4TPS の使用
- 同一インターフェイス上での WebVPN と ASDM の設定
- WebVPN HTTP/HTTPS プロキシの設定
- SSL/TLS 暗号化プロトコルの設定

WebVPN セッション用 HT4TPS の使用

WebVPN セッションの確立には、次のことが必要です。

- セキュリティ アプライアンスまたはロードバランシング クラスタへのアクセスに HTTPS を使用する。Web ブラウザには、セキュリティ アプライアンスの IP アドレスを *https:// address* 形式で入力します。*address* はセキュリティ アプライアンス インターフェイスの IP アドレスまたは DNS ホスト名です。
- ユーザの接続先のセキュリティ アプライアンス インターフェイス上で WebVPN セッションをイネーブルにする。

インターフェイス上で WebVPN セッションを許可するには、次の手順を実行します。

ステップ 1　グローバル コンフィギュレーション モードで **webvpn** コマンドを入力して、webvpn モードに入ります。

ステップ 2　WebVPN セッションに使用するインターフェイス名を指定して **enable** コマンドを入力します。

たとえば、外部のインターフェイス上で WebVPN セッションをイネーブルにするには、次のように入力します。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

同一インターフェイス上での WebVPN と ASDM の設定

セキュリティ アプライアンスは、同一インターフェイスで WebVPN 接続と HTTPS 接続の両方の ASDM 管理セッションを同時にサポートできます。HTTPS と WebVPN の両方がデフォルトでポート 443 を使用します。したがって、HTTPS と WebVPN の両方を同一インターフェイス上でイネーブルにするには、HTTPS か WebVPN のいずれかに異なるポート番号を指定する必要があります。あるいは、異なるインターフェイス上で WebVPN と HTTPS を設定します。

HTTPS のポートを指定するには、**http server enable** コマンドの *port* 引数を使用します。次の例では、HTTPS ASDM セッションが外部インターフェイスでポート 444 を使用するように指定しています。WebVPN も外部インターフェイスでイネーブルになっており、デフォルト ポート（443）を使用します。このコンフィギュレーションでは、リモート ユーザは https://<outside_ip>:444 とブラウザで入力して、ASDM セッションを開始します。

```
hostname(config)# http server enable 444
hostname(config)# http 192.168.3.0 255.255.255.0 outside
hostname(config)# webvpn
hostname(config-webvpn)# enable outside
```

WebVPN のポートを指定するには、webvpn コンフィギュレーション モードから **port** コマンドを使用します。次の例では、外部インターフェイスのポート 444 で WebVPN をイネーブルにします。ASDM の HTTPS も外部インターフェイスで設定されており、デフォルト ポート（443）を使用します。このコンフィギュレーションでは、リモート ユーザは https://<outside_ip>:444 とブラウザで入力して、WebVPN セッションを開始します。

```
hostname(config)# http server enable
hostname(config)# http 192.168.3.0 255.255.255.0 outside
hostname(config)# webvpn
hostname(config-webvpn)# port 444
hostname(config-webvpn)# enable outside
```

WebVPN HTTP/HTTPS プロキシの設定

セキュリティ アプライアンスは HTTPS 接続を終了して、HTTP/HTTPS 要求を HTTP プロキシ サーバや HTTPS プロキシ サーバに転送できます。これらのサーバは、ユーザとインターネットの仲介役として機能します。すべてのインターネット アクセスが組織によって制御されているサーバを経由するように指定することで、別のフィルタリングが可能になり、セキュアなインターネット アクセスと管理制御が保証されます。

HTTP プロキシと HTTPS プロキシに対する値を設定するには、webvpn モードで **http-proxy** コマンドと **https-proxy** コマンドを使用します。これらのコマンドを使用すると、HTTP や HTTPS のプロキシ サーバとポートを指定できます。

SSL/TLS 暗号化プロトコルの設定

SSL/TLS 暗号化プロトコルを設定するときは、次のことに注意してください。

- 使用しているセキュリティ アプライアンスとブラウザが、同じ SSL/TLS 暗号化プロトコルを利用していることを確認してください。
- 電子メール プロキシを設定する場合は、セキュリティ アプライアンス SSL バージョンを TLSv1 Only に設定しないでください。
  MS Outlook と MS Outlook Express は TLS をサポートしていません。
- TCP ポート転送には、Sun Microsystems Java Runtime Environment（JRE）バージョン 1.4.x と 1.5.x が必要です。WebVPN ユーザが次の SSL バージョンで接続している場合、ポート転送は機能しません。

Negotiate SSLv3	Java がダウンロードされる
Negotiate SSLv3/TLSv1	Java がダウンロードされる
Negotiate TLSv1	Java がダウンロードされない
TLSv1Only	Java がダウンロードされない
SSLv3Only	Java がダウンロードされない

デジタル証明書による認証

SSL はデジタル証明書を使用して認証を行います。セキュリティ アプライアンスは、ブート時に自己署名の SSL サーバ証明書を作成します。または、PKI コンテキストで発行された SSL 証明書をセキュリティ アプライアンスにインストールすることもできます。HTTPS の場合、この証明書をクライアントにインストールする必要があります。証明書のインストールは、特定のセキュリティ アプライアンスから 1 度だけ行います。

デジタル証明書によるユーザ認証には、次のような制限事項があります。

- デジタル証明書を使用して認証を行う WebVPN ユーザに対して、Application Access は機能しません。JRE には、Web ブラウザ キーストアにアクセスする機能はありません。このため、JAVA はブラウザがユーザ認証に使用する証明書を使用できず、起動できません。
- 電子メールプロキシは、Netscape 7.x の電子メール クライアントの証明書認証だけをサポートします。MS Outlook、MS Outlook Express、Eudora など、他の電子メール クライアントは、証明書ストアにアクセスできません。

デジタル証明書を使用する認証と認可の詳細については、「AAA サーバとローカル データベースの設定」の「証明書とユーザ ログイン クレデンシャルの使用方法」を参照してください。

Web VPN 用にブラウザのクッキーをイネーブルにする

WebVPN が正しく動作するためには、ブラウザのクッキーが必要です。ブラウザでクッキーがディセーブルになっていると、Web ポータル ホームページからのリンクによって新しいウィンドウが開き、ユーザはもう一度ログインするように要求されます。

パスワードの管理

パスワードの期限切れが近づくとにエンド ユーザに警告するようにセキュリティ アプライアンスを設定することができます。これを設定するには、トンネルグループの一般アトリビュート モードで、**password-management** コマンドを指定します。

このコマンドを設定すると、セキュリティ アプライアンスは、リモート ユーザのログイン時に、現在のパスワードの期限切れが近づいているか、または期限が切れていることを通知します。次に、セキュリティ アプライアンスからパスワード変更の機会がユーザに提供されます。現在のパスワードの期限がまだ切れていない場合は、ユーザはこのパスワードで引き続きログインできます。このコマンドは、このような通知機能をサポートする RADIUS、RADIUS 対応 NT サーバ、LDAP サーバなどの AAA サーバで有効です。RADIUS 認証または LDAP 認証が設定されていない場合、セキュリティ アプライアンスはこのコマンドを無視します。

このコマンドは、パスワードが期限切れになるまでの日数は変更しませんが、パスワードの期限切れが近づいていることをセキュリティ アプライアンスがユーザに警告する期限切れまでの日数を指定します。デフォルト値は 14 日間です。

LDAP サーバ認証だけの場合は、キーワード ***password-expire-in-days*** を使用すると特定の日数を指定できます。***password-expire-in-days*** を使用する場合は、日数も指定する必要があります。

日数を 0 にしてこのコマンドを指定すると、このコマンドはディセーブルになります。セキュリティ アプライアンスは期限切れが迫っていることをユーザに通知しませんが、ユーザは期限切れ後にパスワードを変更することができます。

次の例は、トンネルグループ「testgroup」についてパスワードの期限切れが迫っていることをユーザに警告し始めるまでの日数を 90 日間に設定しています。

```
hostname(config)# tunnel-group testgroup type webvpn
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# password-management password-expire-in-days 90
```

WebVPN でのシングル サインオンの使用

シングル サインオン サポートは、WebVPN ユーザがパスワードを 1 回入力するだけで複数の保護されたサービスや Web サーバにアクセスできるシステムです。一般に、SSO のメカニズムは、AAA プロセスの一部として開始されるか、または AAA サーバのユーザ認証に成功した直後に開始されます。セキュリティ アプライアンス上で実行されている WebVPN サーバは、認証サーバにアクセスするユーザのプロキシとして機能します。ユーザがログインすると、WebVPN サーバは HTTPS を使用して認証サーバに SSO 認証要求を送信します。要求にはユーザ名とパスワードが含まれます。サーバは認証要求を承認した場合、SSO 認証クッキーを WebVPN サーバに返します。セキュリティ アプライアンスは、ユーザの代理としてこのクッキーを保持し、ユーザ認証でこのクッキーを使用して、SSO サーバで保護されているドメイン内部の Web サイトの安全を確保します。

この項では、WebVPN でサポートされる 3 種類の SSO 認証方法について説明します。これらの認証方法には、HTTP Basic 認証と NTLMv1（NT LAN Manager）認証、Computer Associates の eTrust SiteMinder SSO サーバ（前 Netegrity SiteMinder）による認証、および HTTP Form プロトコルによる認証があります。

この項の内容は次のとおりです。

- HTTP Basic 認証または NTLM 認証による SSO の設定
- SiteMinder による SSO 認証の設定
- HTTP Form プロトコルを使用した SSO の設定

HTTP Basic 認証または NTLM 認証による SSO の設定

この項では、HTTP Basic 認証または NTLM 認証を使用するシングル サインオンについて説明します。この方法のいずれかまたは両方を使用して SSO を実装するようにセキュリティ アプライアンスを設定することができます。**auto-signon** コマンドを使用すると、セキュリティ アプライアンスは WebVPN ユーザのログインのクレデンシャル（ユーザ名およびパスワード）を内部サーバに自動的に渡すように設定されます。**auto-signon** コマンドは 2 回以上入力することができます。コマンドを複数回入力すると、セキュリティ アプライアンスは入力順（先に入力されたコマンドを優先）にこれらを処理します。IP アドレスと IP マスク、または URI マスクのいずれかを使用してログインのクレデンシャルを受信するようにサーバに指定します。

auto-signon コマンドは、webvpn コンフィギュレーション モード、webvpn グループポリシー モード、webvpn ユーザ名モードのすべてで使用できます。ユーザ名はグループより優先され、グループはグローバルより優先されます。モードは、次のように、必要な認証の範囲に応じて選択します。

モード	範囲
Webvpn コンフィギュレーション	WebVPN ユーザ全員に対するグローバルな範囲
Webvpn グループ コンフィギュレーション	グループポリシーで定義される WebVPN ユーザのサブセット
Webvpn ユーザ名コンフィギュレーション	個々の WebVPN ユーザ

次の例では、モードと引数の組み合せが可能なさまざまなコマンドについて説明します。

すべてのユーザ、IP アドレス範囲、NTLM

NTLM 認証を使用し、10.1.1.0 から 10.1.1.255 の IP アドレス範囲に存在するサーバに対するすべての WebVPN ユーザからのアクセスに**自動サインオン**を設定するには、次のようなコマンドを入力します。

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow ip 10.1.1.1 255.255.255.0 auth-type ntlm
```

すべてのユーザ、URI 範囲、HTTP Basic

基本の HTTP 認証を使用するすべての Web VPN ユーザに対し、URI マスク https://*.example.com/* で定義されたサーバへのアクセスに**自動サインオン**を設定するには、次のようなコマンドを入力します。

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow uri https://*.example.com/* auth-type basic
```

グループ、URI 範囲、HTTP Basic および NTLM

基本認証または NTLM 認証を使用して、Web VPN ユーザの ExamplePolicy グループに対し、URI マスク https://*.example.com/* で定義されたサーバへのアクセスに**自動サインオン**を設定するには、次のコマンドを入力します。

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type
all
```

特定のユーザ、IP アドレス範囲、HTTP Basic

NTTP Basic 認証を使用し、10.1.1.0 から 10.1.1.255 の IP アドレス範囲に存在するサーバに対する Anyuser と名付けられたユーザからのアクセスに**自動サインオン**を設定するには、次のようなコマンドを入力します。

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow ip 10.1.1.1 255.255.255.0
auth-type basic
```

SiteMinder による SSO 認証の設定

ここでは、SiteMinder を使用して SSO をサポートするためのセキュリティ アプライアンスの設定について説明します。ユーザの Web サイトのセキュリティ インフラストラクチャにすでに SiteMinder を組み込んでいる場合は、SSO に SiteMinder を使用するのが普通です。この方式により、SSO 認証は AAA から切り離され、AAA プロセスが完了するとこの認証が 1 回実施されます。WebVPN ユーザまたはグループに SSO を設定する場合は、まず RADIUS サーバまたは LDAP サーバなどの AAA サーバを設定する必要があります。その後で、WebVPN の SSO サポートをセットアップできます。この項の内容は次のとおりです。

- タスクの概要：Siteminder による SSO の設定
- タスクの詳細：Siteminder による SSO の設定
- シスコの認証スキームの SiteMinder への追加

タスクの概要：Siteminder による SSO の設定

この項では、SiteMinder SSO を使用して SSO を設定するために必要なタスクの概要について説明します。必要なタスクは次のとおりです。

- SSO サーバの指定
- セキュリティ アプライアンスが SSO 認証要求を作成するための SSO サーバの URL の指定
- セキュリティ アプライアンスと SSO サーバとの間でセキュアな通信を確立するための秘密キーの指定。このキーはパスワードのようなもので、ユーザが作成および保管し、Cisco Java プラグイン認証スキームを使用してセキュリティ アプライアンスおよび SiteMinder Policy Server の両方で入力します。

これらの必須タスクに加えて、次のようなオプションの設定タスクを行うことができます。

- 認証要求のタイムアウトの設定
- 認証要求のリトライ回数の設定

設定タスクの完了後、ユーザまたはグループポリシーに SSO サーバを割り当てます。

タスクの詳細：Siteminder による SSO の設定

ここでは、CA SiteMinder による SSO 認証をサポートするためのセキュリティ アプライアンスの特定の設定手順について説明します。SiteMinder を使用して SSO を設定するには、次の手順を実行します。

ステップ 1　webvpn コンフィギュレーション モードで、次の **sso-server** コマンドと **type** オプションを入力して SSO サーバを作成します。たとえば、Example of type siteminder という名前の SSO サーバを作成するには、次のように入力します。

```
hostname(config)# webvpn
hostname(config-webvpn)# sso-server Example type siteminder
hostname(config-webvpn-sso-siteminder)#
```

（注）　現時点では、セキュリティ アプライアンスは、SSO サーバ タイプ siteminder のみサポートします。

ステップ 2　webvpn-sso-siteminder コンフィギュレーション モードで次のように **web-agent-url** コマンドを入力して SSO サーバの認証 URL を指定します。たとえば、http://www.Example.com/webvpn という URL に認証要求を送信するには、次のように入力します。

```
hostname(config-webvpn-sso-siteminder)# web-agent-url http://www.Example.com/webvpn
hostname(config-webvpn-sso-siteminder)#
```

ステップ 3　セキュリティ アプライアンスと SiteMinder との間の認証通信をセキュアにする秘密キーを webvpn-sso-siteminder コンフィギュレーション モードで **policy-server-secret** コマンドを使用して指定します。キーの長さは、標準またはシフト式英数字を使用した任意の文字長にできますが、セキュリティ アプライアンスと SSO サーバの両方で同じキーを使用する必要があります。

たとえば、AtaL8rD8! という秘密キーを作成するには、次のように入力します。

```
hostname(config-webvpn-sso-siteminder)# policy-server-secret AtaL8rD8!
hostname(config-webvpn-sso-siteminder)#
```

ステップ 4　また、オプションで、webvpn-sso-siteminder コンフィギュレーション モードから **request-timeout** コマンドを使用すると、失敗した SSO 認証がタイムアウトを試行するまでの秒数を設定することができます。デフォルトの秒数は 5 秒で、1 秒から 30 秒までの範囲で指定できます。要求がタイムアウトするまでの秒数を 8 に変更するには、次のように入力します。

```
hostname(config-webvpn-sso-siteminder)# request-timeout 8
hostname(config-webvpn-sso-siteminder)#
```

ステップ 5　また、オプションで、webvpn-sso-siteminder コンフィギュレーション モードから **max-retry-attempts** コマンドを使用すると、セキュリティ アプライアンスがタイムアウトするまでに、失敗した SSO 認証をリトライする回数を設定することができます。デフォルトのリトライ回数は 3 で、1 回から 5 回までの範囲で指定できます。たとえば、リトライの回数を 4 に設定するには、次のように入力します。

```
hostname(config-webvpn-sso-siteminder)# max-retry-attempts 4
hostname(config-webvpn-sso-siteminder)#
```

ステップ 6　SSO サーバの設定後、グループまたはユーザのいずれかに対して SSO 認証を指定する必要があります。グループに SSO を指定するには、group-policy-webvpn コンフィギュレーション モードで **sso-server value** コマンドを使用して SSO サーバをグループポリシーに割り当てます。ユーザに SSO を指定するには、同じ **sso-server value** コマンドを使用して SSO サーバをユーザに割り当てますが、この場合は username-webvpn コンフィギュレーション モードで実行します。たとえば、Example という名前の SSO サーバをユーザ名 Anyuser に割り当てるには、次のように入力します。

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# sso-server value Example
hostname(config-group-webvpn)#
```

ステップ 7　最後に、特権 EXEC モードで、**test sso-server** コマンドを使用すると SSO サーバの設定をテストできます。たとえば、Example という名前の SSO サーバをユーザ名 Anyuser でテストするには、次のように入力します。

```
hostname# test sso-server Example username Anyuser
INFO: Attempting authentication request to sso-server Example for user Anyuser
INFO: STATUS: Success
hostname#
```

シスコの認証スキームの SiteMinder への追加

SiteMinder による SSO を使用するためのセキュリティ アプライアンスの設定に加え、Java プラグインとして提供されている、シスコの認証スキームを使用するようにユーザの CA SiteMinder Policy Server を設定する必要もあります。

（注）
- SiteMinder Policy Server を正しく設定するには、SiteMinder の経験が必要です。
- この項では、手順のすべてではなく、一般的なタスクを取り上げます。
- カスタム認証スキームを追加するための完全な手順については、CA SiteMinder のマニュアルを参照してください。

ユーザの SiteMinder Policy Server にシスコの認証スキームを設定するには、次のタスクを実行します。

ステップ 1　Siteminder Administration ユーティリティを使用して、次の特定の引数を使用できるようにカスタム認証スキームを作成します。

- Library フィールドに、**smjavaapi** と入力します。
- Secret フィールドに、セキュリティ アプライアンスに設定したものと同じ秘密キーを入力します。コマンドライン インターフェイスから **policy-server-secret** コマンドを入力するか、ASDM の Add SSO Server ダイアログの Secret Key フィールドに入力するかのいずれかの方法でセキュリティ アプライアンスにこれを設定します。
- Parameter フィールドに、**CiscoAuthAPI** と入力します。

ステップ 2　Cisco.com のログインを使用して **cisco_vpn_auth.jar** ファイルを http://www.cisco.com/cgi-bin/tablebuild.pl/asa からダウンロードし、SiteMinder サーバのデフォルトのライブラリ ディレクトリにコピーします。

HTTP Form プロトコルを使用した SSO の設定

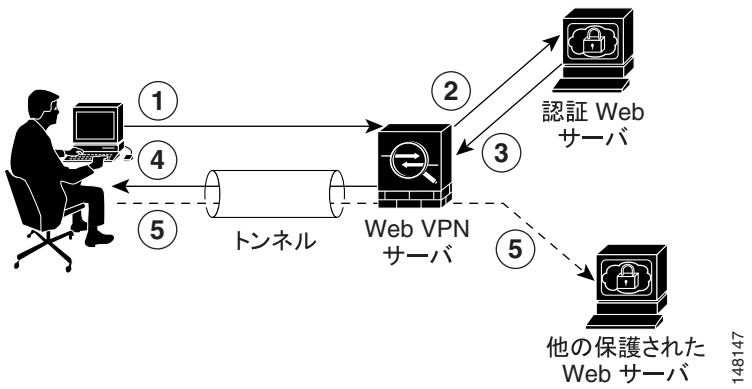
この項では、SSO における HTTP Form プロトコルの使用方法について説明します。HTTP Form プロトコルは SSO 認証を実行するための一般的な手段で、AAA 方式としても使用できます。このプロトコルは、WebVPN ユーザおよび認証を行う Web サーバの間で認証情報を交換するセキュアな方法を提供します。HTTP Form は一般的なプロトコルとして、Web サーバや Web ベースの SSO 製品との高度な互換性を持ち、RADIUS サーバや LDAP サーバなど他の AAA サーバと共に使用することができます。

（注）　HTTP プロトコルを使用して SSO を正しく設定するには、認証および HTTP プロトコル交換に関する実用的な知識が必要です。

セキュリティ アプライアンスは、ここでも認証 Web サーバに対する WebVPN ユーザのプロキシとして動作しますが、この場合は、要求に対して HTTP Form プロトコルと POST 方式を使用します。フォーム データを送受信するためにセキュリティ アプライアンスを設定する必要があります。図 37-1 は、次の SSO 認証の手順を示したものです。

1. 最初に、WebVPN ユーザは、ユーザ名とパスワードを入力してセキュリティ アプライアンス上の WebVPN サーバにログインします。
2. ユーザのプロキシとして動作する WebVPN サーバは、このフォーム データ（ユーザ名およびパスワード）を、POST 認証要求によって認証する Web サーバに転送します。
3. 認証する Web サーバがユーザのデータを承認した場合は、ユーザの代行で保管していた認証クッキーを WebVPN サーバに戻します。
4. WebVPN サーバはユーザまでのトンネル接続を確立します。
5. これでユーザは、ユーザ名やパスワードを再入力しなくても、保護された SSO 環境内の他の Web サイトにアクセスできるようになります。

図 37-1　HTTP Form による SSO 認証



セキュリティ アプライアンスでユーザ名やパスワードなどの POST データを含めるようにするフォーム パラメータを設定するときに、Web サーバが追加的に要求する非表示パラメータの中には、ユーザ側で当初認識できないものがある場合があります。認証アプリケーションによっては、ユーザ側に表示されず、ユーザが入力もしない非表示データを要求する場合があります。しかし、認証 Web サーバが要求する非表示パラメータを見つけることは可能です。これは、セキュリティ アプライアンスを仲介役のプロキシとして使用せずに、ユーザのブラウザから Web サーバに直接認証要求を出す方法で行います。HTTP ヘッダー アナライザを使用して Web サーバの応答を分析すると、非表示パラメータが次のような形式で表示されます。

```
<param name>=<URL encoded value>&<param name>=<URL encoded>
```

非表示パラメータには、必須のパラメータとオプションのパラメータとがあります。Web サーバが非表示パラメータのデータを要求した場合は、そのデータを省略するすべての認証 POST 要求を拒否します。非表示パラメータが必須かオプションかについてはヘッダー アナライザではわからないので、必須であることが判別できるまではすべての非表示パラメータを含めることを推奨します。

この項の内容は次のとおりです。

HTTP Form データの収集

この項では、必要な HTTP Form データを検出および収集する手順を示します。認証 Web サーバが要求するパラメータが何かわからない場合は、次の手順を実行して認証交換を分析するとパラメータ データを収集することができます。

（注）　これらの手順では、ブラウザと HTTP ヘッダー アナライザが必要です。

ステップ 1　ユーザのブラウザと HTTP ヘッダー アナライザを起動して、セキュリティ アプライアンスを経由せずに Web サーバのログイン ページに直接接続します。

ステップ 2　Web サーバのログイン ページがユーザのブラウザにロードされてから、ログイン シーケンスを検証して交換時にクッキーが設定されているかどうか判別します。Web サーバによってログイン ページにクッキーがロードされている場合は、このログイン ページの URL を *start-URL* として設定します。

ステップ 3　Web サーバにログインするためのユーザ名とパスワードを入力して、Enter キーを押します。この動作によって、ユーザが検証する認証 POST 要求が HTTP ヘッダー アナライザで生成されます。

次に、ホストの HTTP ヘッダーおよび本文が記載された POST 要求の例を示します。

```
POST
/emco/myemco/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000430e1-7443-125c-ac0
5-83846dc90034&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk3DRNwNjk2KcqVCFb
IrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fwww.example.com%2Femco%2F
myemco%2F HTTP/1.1
Host: www.example.com
(BODY)
SMENC=ISO-8859-1&SMLOCALE=US-EN&USERID=Anyuser&USER_PASSWORD=XXXXXX&target=https%3A%2F
%2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0
```

ステップ 4　POST 要求を検証してプロトコル、ホストをコピーし、URL を入力して、action-uri パラメータを設定します。

ステップ 5　POST 要求の本文を検証して、次の情報をコピーします。

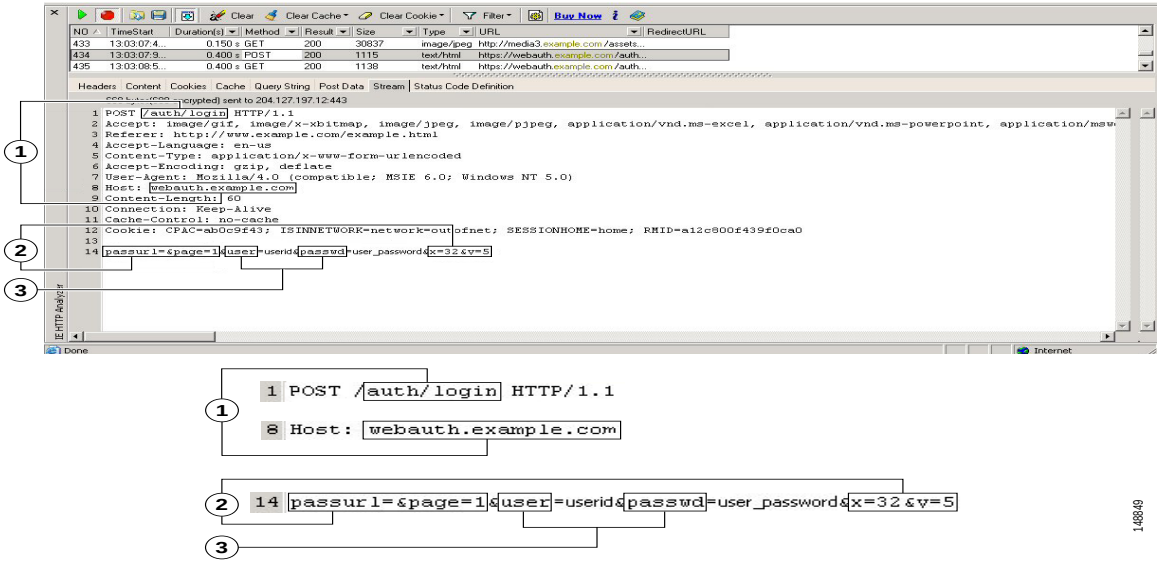
a. ユーザ名パラメータ。上記の例では、このパラメータは USERID で、値は anyuser ではありません。

b. パスワード パラメータ。上記の例では、このパラメータは USER_PASSWORD です。

c. 非表示パラメータ。このパラメータは、POST 本文からユーザ名パラメータとパスワード パラメータを除くすべてです。上記の例で言うと、非表示パラメータは、SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fmyemco%2F&smauthreason=0 の部分です。

図 37-2 に、HTTP アナライザの出力例に表示される action URI、非表示データ、ユーザ名、パスワードの各種パラメータを示します。これは一例です。出力は Web サイトによって大きく異なります。

図 37-2　action-uri、非表示、ユーザ名、パスワードの各種パラメータ



1	action URI パラメータ
2	非表示パラメータ
3	ユーザ名パラメータとパスワード パラメータ

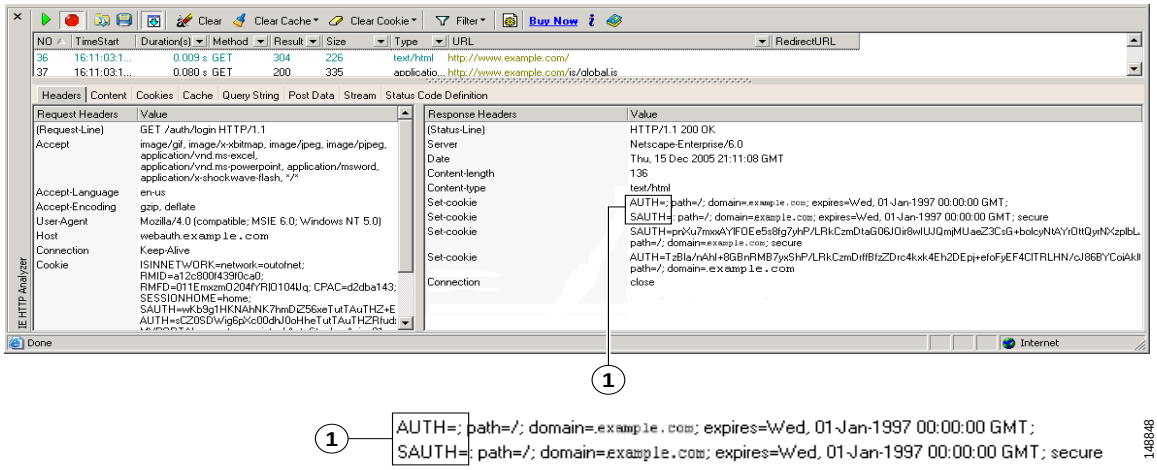
ステップ 6　Web サーバへのログインが成功したら、HTTP ヘッダー アナライザを使用して、サーバからユーザのブラウザ内に設定されているセッションのクッキー名を見つけ出すことによって、サーバの応答を検証します。ここで **auth-cookie-name** パラメータを使用します。

次のサーバ応答ヘッダーでは、SMSESSION がセッションのクッキーの名前です。必要なのはこの名前だけです。値は不要です。

```
Set-Cookie:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZPbHIHtWLD
KTa8ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0dSSOSepWvnsCb7IFxCw
+MGiw0o88uHa2t4l+SillqfJvcpuXfiIAO06D/gtDF40Ow5YKHEl2KhDEvv+yQzxwfEz2cl7Ef5iMr8LgGcDK7
qvMcvrgUqx68JQOK2+RSwtHQ15bCZmsDU5vQVCvSQWC8OMHNGwpS253XwRLvd/h6S/tM0k98QMv+i3N8oOdj1V
7flBqecH7+kVrU01F6oFzr0zM1kMyLr5HhlVDh7B0k9wp0dUFZiAzaf43jupD5f6CEkuLeudYW1xgNzsR8eqtP
K6t1gFJyOn0s7QdNQ7q9knsPJsekRAH9hrLBhWBLTU/3B1QS94wEGD2YTuiW36TiP14hYwOlCAYRj2/bY3+lYz
Vu7EmzMQ+UefYxh4cF2gYD8RZL2RwmP9JV5l48I3XBFPNUw/3V5jf7nRuLr/CdfK3OO8+Pa3V6/nNhokErSgyx
jzMd88DVzM41LxxaUDhbcmkoHT9ImzBvKzJX0J+o7FoUDFOxEdIqlAN4GNqk49cpi2sXDbIarALp6Bl3+tbB4M
lHGH+0CPscZXqoi/kon9YmGauHyRs+0m6wthdlAmCnvlJCDfDoXtn8DpabgiW6VDTrvl3SGPyQtUv7Wdahuq5S
xbUzjY2JxQnrUtwB977NCzYu2sOtN+dsEReWJ6ueyJBbMzKyzUB4L3i5uSYN50B4PCv1w5KdRKa5p3N0Nfq6RM
6dfipMEJw0Ny1sZ7ohz3fbvQ/YZ7lw/k7ods/8VbaR15ivkE8dSCzuf/AInHtCzuQ6wApzEp9CUoG8/dapWriH
jNoi4llJOgCst33wEhxFxcWy2UWxs4EZSjsI5GyBnefSQTPVfma5dc/emWor9vWr0HnTQaHP5rg5dTNqunkDEd
MIHfbeP3F90cZejVzihM6igiS6P/CEJAjE;Domain=.example.com;Path=/
```

図 37-3 に、HTTP アナライザによる認可クッキーの出力例を示します。これは一例です。出力は Web サイトによって大きく異なります。

図 37-3　HTTP アナライザの出力例に表示された認可クッキー



1	認可クッキー

ステップ 7　この場合は、認証の成否に関わらず同じクッキーがサーバによって設定される可能性があり、このようなクッキーは SSO の目的上、認められません。クッキーが異なっていることを確認するには、無効なログイン クレデンシャルを使用して、「失敗した」クッキーと「成功した」クッキーとをステップ 1 からステップ 6 を繰り返して比較します。

これで、HTTP Form プロトコルによる SSO をセキュリティ アプライアンスに設定するために必要なパラメータ データを入手できました。

タスクの概要：HTTP Form プロトコルによる SSO の設定

この項では、HTTP Form プロトコルを使用した SSO の設定の概要について説明します。HTTP によって SSO をイネーブルにするには、次のタスクを実行します。

- フォーム データ（**action-uri**）を受信および処理するために、認証 Web サーバの Uniform Resource Identifier（URI; ユニフォーム リソース識別子）を設定する。
- ユーザ名パラメータ（**user-parameter**）を設定する。
- ユーザ パスワード パラメータ（**password-parameter**）を設定する。

認証 Web サーバの要件によっては次のタスクが必要になる場合もあります。

- 認証ウェブサーバがログイン前のクッキー交換を必要とする場合は、開始 URL（**start-url**）を設定する。
- 認証 Web サーバが要求する任意の非表示認証パラメータ（**hidden-parameter**）を設定する。
- 認証 Web サーバによって設定される認証クッキーの名前（**auth-cookie-name**）を設定する。

タスクの詳細：HTTP Form プロトコルによる SSO の設定

この項では、HTTP Form プロトコルを使用した SSO を設定するために必要な詳細タスクを取り上げます。セキュリティ アプライアンスが HTTP Form プロトコルを使用した SSO を実行するように設定するには、次の手順を実行します。

ステップ 1　認証 Web サーバが要求する場合は、aaa-server-host コンフィギュレーション モードで **start-url** コマンドを入力して、認証 Web サーバから事前ログイン クッキーを取得するための URL を指定します。たとえば、http://example.com/east/Area.do?Page-Grp1 の URL 認証 Web サーバを、IP アドレス 10.0.0.2 の testgrp1 サーバ グループに指定するには、次のように入力します。

```
hostname(config)# aaa-server testgrp1 host 10.0.0.2
hostname(config-aaa-server-host)# start-url http://example.com/east/Area.do?Page-Grp1
hostname(config-aaa-server-host)#
```

ステップ 2　認証 Web サーバに認証プログラム用の URI を指定するには、aaa-server- host コンフィギュレーション モードで **action-uri** コマンドを入力します。1 つの URI を連続する複数行にわたって入力することができます。1 行あたりの最大文字数は 255 です。URI 全体の合計の最大文字数は 2048 です。action URI の出力例は次のとおりです。

http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=SM5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fauth.example.com

この action URI を指定するには、次のコマンドを入力します。

```
hostname(config-aaa-server-host)# action-uri http://www.example.com/auth/index.htm
hostname(config-aaa-server-host)# action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP
hostname(config-aaa-server-host)# action-uri 554433&REALMOID=06-000a1311-a828-1185
hostname(config-aaa-server-host)# action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON
hostname(config-aaa-server-host)# action-uri =0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk
hostname(config-aaa-server-host)# action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r
hostname(config-aaa-server-host)# action-uri B1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F
hostname(config-aaa-server-host)# action-uri %2Fauth.example.com
hostname(config-aaa-server-host)#
```

（注）　action URI には、ホスト名およびプロトコルを含めることができます。上記の例では、これらは、http://www.example.com の URI の最初に表示されます。

ステップ 3　HTTP POST 要求のユーザ名パラメータを設定するには、aaa-server-host コンフィギュレーション モードで、**user-parameter** コマンドを入力します。たとえば、次のようにコマンドを入力すると、ユーザ名パラメータ userid が設定されます。

```
hostname(config-aaa-server-host)# user-parameter userid
hostname(config-aaa-server-host)#
```

ステップ 4　HTTP POST 要求のユーザ パスワード パラメータを設定するには、aaa-server-host コンフィギュレーション モードで、**password-parameter** コマンドを入力します。たとえば、次のようにコマンドを入力すると、ユーザ パスワード パラメータ名として user_password が設定されます。

```
hostname(config-aaa-server-host)# password-parameter user_password
hostname(config-aaa-server-host)#
```

ステップ 5　認証 Web サーバと交換する非表示パラメータを指定するには、aaa-server-host コンフィギュレーション モードで、**hidden-parameter** コマンドを入力します。次に、POST 要求から抜粋した非表示パラメータの例を示します。

SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0

この非表示パラメータには、間を & で区切った 4 つの Form エントリとその値が含まれています。4 つのエントリとその値は次のとおりです。

- SMENC エントリおよび値 ISO-8859-1
- SMLOCALE エントリおよび値 US-EN
- target エントリと値 https%3A%2F%2Fwww.example.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG
- smauthreason エントリと値 0

この非表示パラメータを指定するには、次のコマンドを入力します。

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# hidden-parameter
SMENC=ISO-8859-1&SMLOCALE=US-EN&targe
hostname(config-aaa-server-host)# hidden-parameter
t=https%3A%2F%2Fwww.example.com%2Femc
hostname(config-aaa-server-host)# hidden-parameter
o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo
hostname(config-aaa-server-host)# hidden-parameter de%3DENG&smauthreason=0
hostname(config-aaa-server-host)#
```

ステップ 6　認証クッキーの名前を指定するには、aaa-server-host コンフィギュレーション モードで、**auth-cookie-name** コマンドを入力します。このコマンドをはオプションです。次に、SsoAuthCookie という名前の認証クッキーを指定する例を示します。

```
hostname(config-aaa-server-host)# auth-cookie-name SsoAuthCookie
hostname(config-aaa-server-host)#
```

デジタル証明書による認証

デジタル証明書を使用して認証を行う WebVPN ユーザは、グローバルな認証と認可の設定を使用しません。その代わり、証明書の検証が完了すると、ユーザは認可サーバを使用して認証します。デジタル証明書を使用する認証と認可の詳細については、「AAA サーバとローカル データベースの設定」の「証明書とユーザ ログイン クレデンシャルの使用方法」を参照してください。

WebVPN ポリシーの作成と適用

中央にあるリソースへのアクセスを制御する WebVPN ポリシーを作成および適用するには、次の作業を実行します。

- グローバル コンフィギュレーション モードでのポート転送、URL、およびアクセスリストの作成
- グループポリシー モードまたはユーザ モードでのグループポリシーとユーザへのリストの割り当て
- グループポリシーとユーザ用の機能のイネーブル化
- グループポリシーへのユーザの割り当て

第 30 章「トンネルグループ、グループポリシー、およびユーザの設定」では、これらのタスクについて詳細な手順で説明しています。

グローバル コンフィギュレーション モードでのポート転送、URL、およびアクセスリストの作成

転送するポートと WebVPN ユーザに提示する URL のリストを設定し、これらのアクセス レベルを設定するには、グローバル コンフィギュレーション モードで **port forward** コマンド、**url-list** コマンド、および **access-list** コマンドを使用します。

グループポリシー モードまたはユーザ モードでのグループポリシーとユーザへのリストの割り当て

ポート転送と URL リストを設定したら、webvpn グループポリシー モードまたはユーザ モードで **port forward** コマンド、**url-list** コマンド、および **filter** コマンドを使用して、グループポリシーやユーザにリストを割り当てます。

グループポリシーとユーザ用の機能のイネーブル化

グループポリシーとユーザ用の機能をイネーブルにするには、グループポリシー モードまたはユーザ コンフィギュレーション モードで **functions** コマンドを発行します。

グループポリシーへのユーザの割り当て

ユーザをグループポリシーに割り当てると、複数のユーザにポリシーを適用することで設定が容易になります。ユーザをグループポリシーに割り当てるには、内部の認証サーバまたは RADIUS サーバを使用することができます。グループポリシーを使用して設定を簡略化する説明の詳細については、第 30 章「トンネルグループ、グループポリシー、およびユーザの設定」を参照してください。

セキュリティ アプライアンス認証サーバを使用する

セキュリティ アプライアンスの内部認証サーバでユーザを認証するように設定し、これらのユーザをセキュリティ アプライアンス上でグループポリシーに割り当てることもできます。

RADIUS サーバを使用する

RADIUS サーバをユーザ認証に使用する場合は、次の手順を実行して、ユーザをグループポリシーに割り当てます。

ステップ 1　RADIUS でユーザ認証を行い、Class アトリビュートを使用してそのユーザを特定のグループポリシーに割り当てます。

ステップ 2　OU=group_name 形式で Class アトリビュートをグループポリシー名に設定します。

たとえば、WebVPN ユーザを SSL_VPN グループに割り当てるには、RADIUS Class アトリビュートを *OU=SSL_VPN;*（セミコロンは省略不可）の値に設定します。

WebVPN トンネルグループ アトリビュートの定義

表 37-1 は、WebVPN に特有のトンネルグループ アトリビュートをリストで示したものです。これらのアトリビュートに加えて、すべての VPN 接続に共通する一般的なトンネルグループ アトリビュートを設定します。トンネルグループを設定するための詳細な手順については、第 30 章「トンネルグループ、グループポリシー、およびユーザの設定」の「WebVPN トンネルグループの設定」を参照してください。

表 37-1　WebVPN トンネルグループ アトリビュート

コマンド	機能
authentication	認証方式を設定します。
customization	以前に定義した、適用対象のカスタマイゼーションの名前を指定します。
nbns-server	CIFS 名前解決用の NetBIOS ネーム サービス サーバの名前（nbns-server）を指定します。
group-alias	サーバがトンネルグループの参照に使用できる代替名を指定します。
group-url	1 つ以上のグループの URL を指定します。このアトリビュートを設定すると、指定した URL に着信するユーザはログイン時にグループを選択する必要がありません
dns-group	DNS サーバ名、ドメイン名、ネーム サーバ、リトライの回数、およびタイムアウト値を指定する DNS サーバ グループを指定します。
hic-fail-group-policy	Cisco Secure Desktop Manager を使用してグループベースのポリシー アトリビュートを「Use Failure Group-Policy」または「Use Success Group-Policy, if criteria match」に設定する場合の VPN フィーチャ ポリシーを指定します。

WebVPN グループポリシーとユーザ アトリビュートの設定

表 37-2 は、WebVPN グループポリシーとユーザ アトリビュートをリストで示したものです。グループポリシーとユーザ アトリビュートの詳細な手順については、第 30 章「トンネルグループ、グループポリシー、およびユーザの設定」の「グループポリシーの設定」と「特定ユーザのアトリビュートの設定」を参照してください。

表 37-2　WebVPN グループポリシー アトリビュートとユーザ アトリビュート

コマンド	機能
auto-signon	自動サインオンの値を設定します。設定では WebVPN への初回の接続のみユーザ名およびパスワードのクレデンシャルが必要です。
customization	カスタマイゼーション オブジェクトをグループポリシーまたはユーザに割り当てます。
deny-message	WebVPN へのログインに成功したが VPN 特権を持たないリモート ユーザに送信されるメッセージを指定します。
filter	webtype アクセスリストの名前を設定します。
functions	WebVPN 機能（自動ダウンロード、Citrix、ファイル アクセス、ファイル ブラウジング、ファイル エントリ、フィルタリング、HTTP プロキシ、URL エントリ、MAPI プロキシ、ポート転送）の一部または全部をイネーブルにします。
homepage	ログイン時に表示される Web ページの URL を設定します。
html-content-filter	このグループポリシー用の HTML からフィルタリングするコンテンツとオブジェクトを設定します。
http-comp	圧縮を設定します。
keep-alive-ignore	セッション タイマーのアップデートを無視する最大オブジェクト サイズを設定します。
port-forward	転送する WebVPN TCP ポートのリストを適用します。ユーザ インターフェイスにこのリスト上のアプリケーションが表示されます。
port-forward-name	ポート転送アプレットの名前を設定します。
sso-server	SSO サーバの名前を設定します。
svc	SSL VPN クライアントのアトリビュートを設定します。
url-list	エンド ユーザのアクセス用にユーザ インターフェイスで表示される WebVPN サーバと URL のリストを適用します。

Application Access の設定

次の各項では、Application Access の設定について説明します。

ポート転送アプレットの自動ダウンロード

WebVPN を介してリモート アプリケーションを実行するには、WebVPN ホームページの **Start Application Access** をクリックしてポート転送 Java アプレットをダウンロードし、起動します。アプリケーションのアクセスを簡略化して起動時間を短縮するには、WebVPN にユーザが最初にログインした時点で、このポート転送アプレットを自動的にダウンロードするように WebVPN を設定できます。

ポート転送アプレットの自動ダウンロードをイネーブルにするには、webvpn モードから **auto-download** オプションを使用して **functions** コマンドを入力します。

（注）　自動ダウンロード機能を設定する前に、ポート転送、Outlook/Exchange プロキシまたは HTTP プロキシなどのアプレットを使用するアプリケーションを最初にイネーブルにする必要があります。

hosts ファイル エラーを回避するための Application Access の終了

Application Access の実行の妨げになる hosts ファイル エラーを回避するために、Application Access を使用し終わったら Application Access ウィンドウを正しく閉じるようにします。終了するには、close アイコンをクリックします。

Application Access 使用時の hosts ファイル エラーの回復

Application Access ウィンドウを正しく閉じないと次のエラーが発生することがあります。

- 次に Application Access を起動しようとしたときに、Application Access がディセーブルになっていて、`Backup HOSTS File Found` エラー メッセージが表示される。
- アプリケーションをローカルで実行している場合でも、アプリケーション自体がディセーブルになっているか、または動作しない。

このようなエラーは、Application Access ウィンドウを不適切な方法で終了したことが原因です。次の例を参考にしてください。

- Application Access の使用中に、ブラウザがクラッシュした。
- Application Access の使用中に、停電またはシステム シャットダウンが発生した。
- 作業中に Application Access ウィンドウを最小化し、このウィンドウがアクティブな状態（ただし最小化されている）でコンピュータをシャットダウンした。

ここでは、次の項目について説明します。

hosts ファイルの概要

ローカル システム上の hosts ファイルは、IP アドレスをホスト名にマッピングしています。Application Access を起動すると、WebVPN は hosts ファイルを修正し、WebVPN 固有のエントリを追加します。Application Access ウィンドウを正しく閉じて Application Access を終了すると、hosts ファイルは元の状態に戻ります。

Application Access の起動前	hosts ファイルは元の状態です。
Application Access の起動時	• WebVPN は hosts ファイルを hosts.webvpn にコピーして、バックアップを作成します。 • 次に WebVPN は hosts ファイルを編集し、WebVPN 固有の情報を挿入します。
Application Access の終了時	• WebVPN はバックアップ ファイルを hosts ファイルにコピーして、hosts ファイルを元の状態に戻します。 • WebVPN は hosts.webvpn を削除します。
Application Access の終了後	hosts ファイルは元の状態です。

（注）　Microsoft アンチスパイウェア ソフトウェアは、ポート転送 JAVA アプレットによる hosts ファイルの変更をブロックします。アンチスパイウェア ソフトウェアの使用時に hosts ファイルの変更を許可する方法の詳細については、www.microsoft.com を参照してください。

不正な Application Access の終了

Application Access が正しく終了しなかった場合、hosts ファイルは WebVPN 用にカスタマイズされた状態のままになっています。ユーザが次に Application Access を起動するときに、WebVPN は hosts.webvpn ファイルを検索することで、Application Access の状態をチェックします。hosts.webvpn ファイルが検出されると、Backup HOSTS File Found エラー メッセージ（図 37-4）が表示され、Application Access が一時的にディセーブルになります。

Application Access を正しくシャットダウンしないと、リモートアクセス クライアント / サーバ アプリケーションが不安定な状態のままになります。WebVPN を使用せずにこれらのアプリケーションを起動しようとすると、正しく動作しない場合があります。通常の接続先のホストが使用できなくなる場合があります。一般にこのような状況は、自宅からリモートでアプリケーションを実行し、Application Access ウィンドウを終了せずにコンピュータをシャットダウンし、その後職場でそのアプリケーションを実行しようとした場合に発生します。

hosts ファイルの再設定

Application Access または正しく動作しないアプリケーションを再度イネーブルにするには、次の手順を実行します。

- リモートアクセス サーバに接続できる場合は、「WebVPN による hosts ファイルの自動再設定」の項で説明されている手順を実行してください。
- 現在の場所からリモートアクセス サーバに接続できない場合や、hosts ファイルをカスタム編集した場合は、「手動による hosts ファイルの再設定」で説明されている手順に従ってください。

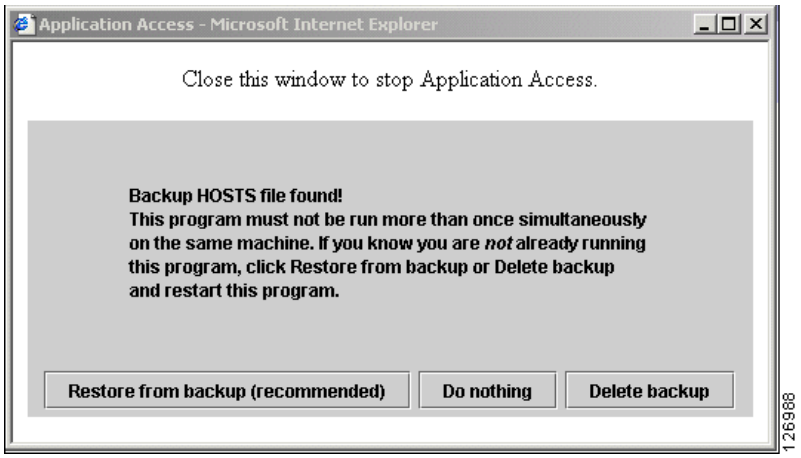
WebVPN による hosts ファイルの自動再設定

リモートアクセス サーバに接続できる場合は、hosts ファイルを再設定し、Application Access やアプリケーションを再度イネーブルにするために、次の手順を実行します。

ステップ 1　WebVPN を起動してログインします。ホームページが開きます。

ステップ 2　**Applications Access** リンクをクリックします。`Backup HOSTS File Found` メッセージが表示されます（図 37-4 を参照）。

図 37-4　Backup HOSTS File Found メッセージ



ステップ 3　次のいずれかのオプションを選択します。

- **Restore from backup** ：WebVPN は強制的に正しくシャットダウンされます。WebVPN は hosts.webvpn backup ファイルを `hosts` ファイルにコピーし、hosts ファイルを元の状態に戻してから、hosts.webvpn を削除します。その後、Application Access を再起動する必要があります。
- **Do nothing** ：Application Access は起動しません。リモートアクセスのホームページが再び表示されます。
- **Delete backup** ：WebVPN は hosts.webvpn ファイルを削除し、hosts ファイルを WebVPN 用にカスタマイズされた状態にしておきます。元の `hosts` ファイル設定は失われます。Application Access は、WebVPN 用にカスタマイズされた hosts ファイルを新しいオリジナルとして使用して起動します。このオプションは、hosts ファイル設定が失われても問題がない場合にだけ選択してください。Application Access が不適切にシャットダウンされた後に、ユーザまたはユーザが使用するプログラムによって hosts ファイルが編集された可能性がある場合は、他の 2 つのオプションのどちらかを選択するか、または hosts ファイルを手動で編集します（「手動による hosts ファイルの再設定」を参照）。

手動による hosts ファイルの再設定

現在の場所からリモートアクセス サーバに接続できない場合や、カスタマイズした hosts ファイルの編集内容を失いたくない場合は、次の手順に従って、hosts ファイルを再設定し、Application Access とアプリケーションを再度イネーブルにします。

ステップ 1　hosts ファイルを見つけて編集します。最も一般的な場所は、c:\windows\sysem32\drivers\etc\hosts です。

ステップ 2　`# added by WebVpnPortForward` という文字列が含まれている行があるかどうかをチェックします。この文字列を含む行がある場合、hosts ファイルは WebVPN 用にカスタマイズされています。hosts ファイルが WebVPN 用にカスタマイズされている場合、次の例のようになっています。

```
123.0.0.3 server1 # added by WebVpnPortForward
123.0.0.3 server1.example.com vpn3000.com # added by WebVpnPortForward
123.0.0.4 server2 # added by WebVpnPortForward
123.0.0.4 server2.example.com.vpn3000.com # added by WebVpnPortForward
123.0.0.5 server3 # added by WebVpnPortForward
123.0.0.5 server3.example.com vpn3000.com # added by WebVpnPortForward

# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     cisco.example.com          # source server
#       38.25.63.10     x.example.com              # x client host

123.0.0.1       localhost
```

ステップ 3　`# added by WebVpnPortForward` という文字列が含まれている行を削除します。

ステップ 4　hosts ファイルを保存してから閉じます。

ステップ 5　WebVPN を起動してログインします。

ホームページが開きます。

ステップ 6　Application Access リンクをクリックします。

Application Access ウィンドウが表示されます。これで Application Access がイネーブルになります。

ファイル アクセスの設定

Common Internet File System（CIFS; 共通インターネット ファイル システム）プロトコルは、ファイル、プリンタ、および他のマシン リソースへのネットワーク アクセスをユーザに提供します。Microsoft では、Windows コンピュータのネットワークで CIFS を実装しています。一方、CIFS のオープン ソース実装では、Linux、UNIX、および Mac OS X など他のオペレーティング システムを実行するサーバへのファイル アクセスも提供しています。

WebVPN は、リモート ユーザに HTTPS ポータル ページを提供しています。このページは、セキュリティ アプライアンス上で稼動するプロキシ CIFS クライアントとのインターフェイスになっています。WebVPN は、このクライアントを使用して、ユーザが認証の要件を満たしていてファイルのプロパティがアクセスを制限しない限り、ネットワーク上のファイルへのネットワーク アクセスをユーザに提供します。クライアントは透過的です。WebVPN から送信されるポータル ページでは、ファイル システムに直接アクセスしているかのように見えます。

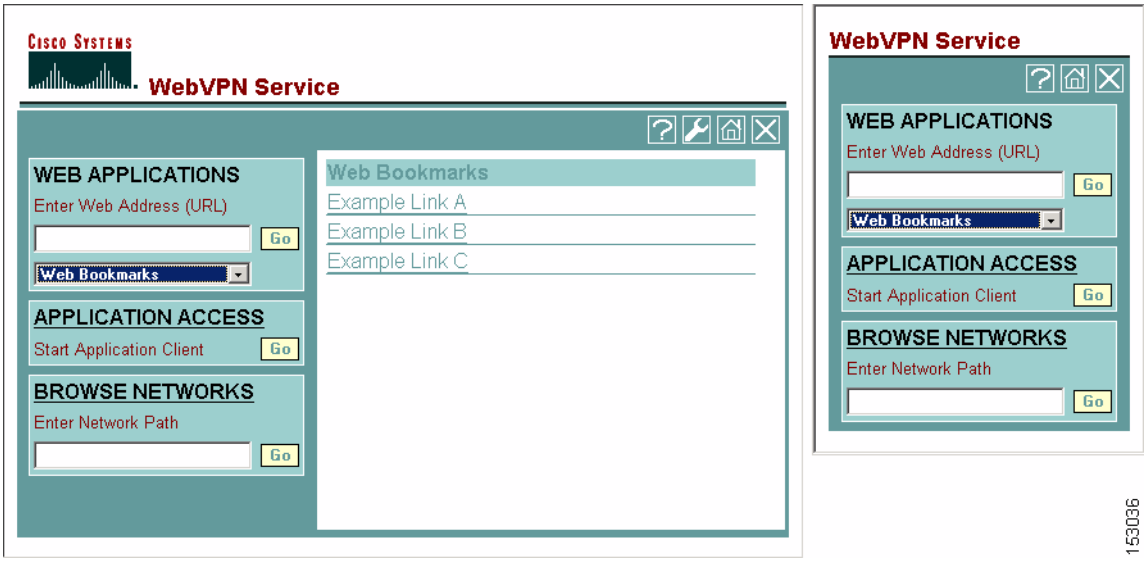
ユーザがファイルのリストを要求すると、WebVPN は、そのリストが含まれるサーバの IP アドレスをマスター ブラウザに指定されているサーバに照会します。セキュリティ アプライアンスはリストを入手してポータル ページ上のリモート ユーザに送信します。

WebVPN は、ユーザの認証要求とファイルのプロパティに応じて、ユーザが次の CIFS の機能を呼び出すことができるようにします。

- ドメインおよびワークグループへの移動とリスト、ドメインまたはワークグループ内のサーバへの移動とリスト、サーバ内部の共有、共有部分またはディレクトリ内でのファイルの共有
- ディレクトリの作成
- ファイルのダウンロード、アップロード、移動、削除

セキュリティ アプライアンスは、通常、同じネットワーク上か、またはこのネットワークからアクセス可能な場所にマスター ブラウザまたは WINS サーバが必要です。これは、リモート ユーザが WebVPN ホームページまたはツールバー上の Browse Networks をクリックしたときにサーバ リストのクエリーがネットワークに送信されるようにするためです（図 37-5）。

図 37-5　WebVPN ホームページとフローティング ツールバーのネットワークのブラウズ



マスター ブラウザには、セキュリティ アプライアンス上の CIFS クライアントと、Web VPN がリモート ユーザに提供するネットワーク リソースのリストが表示されます。マスター ブラウザに DNS サーバを使用することはできません。WebVPN は、WINS サーバを使用した Active Native Directory 環境でのファイル アクセスをサポートしますが、ダイナミック DNS サーバでのアクセスはサポートしません。

次に示す手順 1 は、マスター ブラウザと WINS サーバの指定方法について説明します。手順 1 の代わりに、グローバル コンフィギュレーション モードか、グループポリシーまたはユーザ名モードから入る webvpn モードで **url-list** コマンドを使用して、File Folder Bookmark にサーバ共有を設定することができます。次の例を参考にしてください。

url-list *listname displayname* **cifs:**//*ServerA*/*ShareX*/

この方法（共有を追加）では、マスター ブラウザまたは WINS サーバは不要ですが、Browse Networks リンクはサポートされません。このコマンドの入力時に ServerA を参照するためのホスト名または IP アドレスが使用できます。ホスト名を使用する場合、セキュリティ アプライアンスには IP アドレスを解決するための DNS サーバが必要です。

（注） ファイル アクセスを設定する前に、ユーザ アクセス用のサーバに共有を設定する必要があります。

次の手順を実行して CIFS のファイル アクセスをサポートするようにします。

ステップ 1　NetBIOS Name Server（NBNS）ごとに 1 回ずつ、トンネルグループの webvpn コンフィギュレーション モードで、**nbns-server** コマンドを使用します。

nbns-server {*IPaddress* | *hostname*} [***master***] [***timeout*** *timeout*] [***retry*** *retries*]

master は、マスター ブラウザに指定されるコンピュータです。マスター ブラウザは、コンピュータと共有リソースのリストを保持します。コマンドのマスター部分を入力せずにこのコマンドで指定する任意の NBNS サーバは、Windows Internet Naming Server（WINS）である必要があります。まずマスター ブラウザを指定してから、WINS サーバを指定してください。トンネルグループ用のマスター ブラウザを含め、サーバは最大 3 つまで指定できます。

retries は、NBNS サーバに対するクエリーのリトライ回数です。セキュリティ アプライアンスは、この回数だけサーバのリストを再利用してからエラー メッセージを送信します。デフォルト値は 2 で、範囲は 1 ～ 10 です。

timeout は、セキュリティ アプライアンスが、クエリーを再度サーバに送信する前に待機する秒数です。このとき、サーバが 1 つしかない場合は同じサーバに送信し、サーバが複数存在する場合は別のサーバに送信します。デフォルトのタイムアウトは 2 秒で、範囲は 1 ～ 30 秒です。

次に例を示します。

```
hostname(config-tunnel-webvpn)# nbns-server 192.168.1.20 master
hostname(config-tunnel-webvpn)# nbns-server 192.168.1.41
hostname(config-tunnel-webvpn)# nbns-server 192.168.1.47
```

（注） トンネルグループのコンフィギュレーションにすでに存在する NBNS サーバを表示する場合は、**tunnel-group webvpn-attributes** コマンドを使用します。

ステップ 2　（オプション）WebVPN のポータル ページをリモート ユーザに送信するために符号化する文字セットを指定する **character-encoding** コマンドを使用します。デフォルトでは、リモート ブラウザ上の符号化タイプ セットで WebVPN ポータル ページの文字セットが決定されるため、ユーザは、ブラウザで符号化を適切に実行するために必要となる場合に限り、文字の符号化を設定する必要があります。

character-encoding *charset*

Charset は、最大 40 文字からなる文字列で、http://www.iana.org/assignments/character-sets で指定されたいずれかの有効文字セットと同じです。このページのリストにある名前またはエイリアスのいずれかを使用できます。例には、iso-8859-1、shift_jis、および ibm850 が含まれています。

（注）　character-encoding 値および file-encoding 値では、ブラウザが使用するフォント ファミリを除外しません。これらの値のいずれかに対し、次の例で示すように日本語の Shift JIS 文字符号化を使用する場合は、webvpn カスタマイゼーション コマンド モードの **page style** コマンドを使用してフォント ファミリを置き換えるか、webvpn カスタマイゼーション コマンド モードで **no page style** コマンドを入力してフォント ファミリを削除することにより、設定を補う必要があります。

次に、日本語の Shift JIS 文字をサポートしてフォント ファミリを削除し、さらにデフォルトの背景色を保持するための character-encoding アトリビュートを設定する例を示します。

```
hostname(config-webvpn)# character-encoding shift_jis
hostname(config-webvpn)# customization DfltCustomization
hostname(config-webvpn-custom)# page style background-color:white
hostname(config-webvpn-custom)#
```

ステップ 3　（オプション）特定の CIFS サーバの Web VPN ポータル ページの符号化を指定する **file-encoding** コマンドを使用します。このため、これ以外の文字の符合化が必要な各 CIFS サーバに対し、異なるファイル符号化値を使用できます。

file-encoding {server-name | server-ip-address} *charset*

次の例では、IBM860 （エイリアス「CP860」）文字をサポートするために、CIFS サーバ 10.86.5.174 にファイル符号化アトリビュートを設定しています。

```
hostname(config-webvpn)# file-encoding 10.86.5.174 cp860
hostname(config-webvpn)
```

ステップ 4　ファイル アクセス、ファイルのブラウジング、およびファイル サーバ エントリをサポートするようにセキュリティ アプライアンスを設定するために、グループポリシー モードまたはユーザ名モードから入る webvpn モードで、**functions** コマンドを使用します。

functions file-access file-browsing file-entry

次の例を参考にしてください。

```
hostname(config-group-webvpn)# functions file-access file-browsing file-entry
hostname(config-group-policy)#
```

これらのコマンドの詳細については、『*Cisco Security Appliance Command Reference*』を参照してください。

Citrix MetaFrame サービスへのアクセスの設定

WebVPN ユーザは、セキュリティ アプライアンスとの接続を通じて Citrix MetaFrame サービスにアクセスすることができます。この設定では、セキュリティ アプライアンスは Citrix のセキュアなゲートウェイとして機能します。次の手順を実行して、Citrix MetaFrame サービスのサポートを設定します。

ステップ 1　セキュア ゲートウェイを使用しないモードで動作するように Citrix Web Interface ソフトウェアを設定します。

ステップ 2　リモート ユーザが接続のために Fully-Qualified Domain Name（FQDN; 完全修飾ドメイン名）を使用するセキュリティ アプライアンスのインターフェイスに SSL 証明書をインストールします。

（注）　SSL 証明書の Common Name（CN; 通常名）に IP アドレスを指定しないでください。リモート ユーザは FQDN を使用してセキュリティ アプライアンスとの通信を試みます。リモート PC は、FQDN を解決するために System32\drivers\etc\hosts ファイル内の DNS またはエントリを使用できる必要があります。

ステップ 3　Citrix サポートをイネーブルにするグループポリシーまたはユーザに対し、**functions citrix** コマンドを 1 回ずつ実行します。

次の例は、FirstGroup という名前のグループポリシーに Citrix を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup internal
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# functions citrix
hostname(config-group-webvpn)#
```

PDA での WebVPN の使用

Pocket PC または他の認定された携帯情報端末から WebVPN にアクセスすることができます。セキュリティ アプライアンスの管理者や WebVPN ユーザは、特に何もしなくても、認定された PDA で WebVPN を使用することができます。

シスコでは次の PDA プラットフォームを認定しています。

HP iPaq H4150
Pocket PC 2003
Windows CE 4.20.0、ビルド 14053
Pocket Internet Explorer (PIE)
ROM バージョン 1.10.03ENG
ROM 日付：7/16/2004

PDA のバージョンによって、WebVPN に次のような相違点があります。

- ポップアップの WebVPN ウィンドウはバナー Web ページに置き換わっている
- 標準の WebVPN フローティング ツールバーがアイコン バーに置き換わっている。このバーには、Go、Home、および Logout の各種ボタンが表示されます。
- メインの WebVPN ポータル ページに Show Toolbar アイコンがない
- WebVPN のログアウト時に、警告メッセージで PIE ブラウザを正しく閉じる手順が表示される。この手順に従わないで通常の方法でブラウザのウィンドウを閉じると、WebVPN または HTTPS を使用するすべてのセキュアな Web サイトから PIE が切断されません。
- WebVPN は OWA 2000 版および OWA 2003 版の基本認証をサポートする。OWA サーバに基本認証を設定せずに WebVPN ユーザがこのサーバにアクセスしようとするとアクセスは拒否されます。
- サポートされていない WebVPN の機能
  - Application Access （ポート転送）および他の Java 依存の各種機能
  - MAPI プロキシ
  - HTTP プロキシ
  - Cisco Secure Desktop（CSD は Microsoft Windows CE 用のサポートは限定的に提供）
  - Microsoft Outlook Web Access (OWA) 5.5
  - Citrix Metaframe 機能（PDA に対応する Citrix ICA クライアント ソフトウェアが装備されていない場合）

WebVPN を介した電子メールの使用

WebVPN は、電子メールにアクセスする方法をいくつかサポートしています。ここでは、次の方式について説明します。

- 電子メール プロキシの設定
- MAPI の設定
- Web 電子メール MS Outlook Web Access の設定

電子メール プロキシの設定

WebVPN は IMAP4S、POP3S、および SMTPS 電子メール プロキシをサポートしています。表 37-3 に、電子メール プロキシ ユーザにグローバルに適用されるアトリビュートを示します。

表 37-3　電子メール プロキシ ユーザに適用される WebVPN アトリビュート

機能	コマンド	デフォルト値
電子メール プロキシで使用するように事前に設定されているアカウンティング サーバを指定します。	**accounting-server-group**	なし
電子メール プロキシ ユーザ用の認証方式（複数可）を指定します。	**authentication**	IMAP4S：メールホスト（必須） POP3S メールホスト（必須） SMTPS：AAA
電子メール プロキシで使用するように事前に設定されている認証サーバを指定します。	**authentication-server-group**	LOCAL
WebVPN で使用するように事前に設定されている認可サーバを指定します。	**authorization-server-group**	なし
ユーザが接続するには、正常に認可される必要があります。	**authorization-required**	ディセーブル
認可のユーザ名として使用するピア証明書の DN を指定します。	**authorization-dn-attributes**	プライマリ アトリビュート：CN セカンダリ アトリビュート：OU
使用するグループポリシーの名前を指定します。	**default-group-policy**	DfltGrpPolicy
指定したインターフェイスで電子メール プロキシをイネーブルにします。	**enable**	ディセーブル
電子メールと VPN のユーザ名とパスワードとの間の区切り記号を定義します。	**name-separator**	「:」（コロン）
未処理の未承認セッションの最大数を設定します。	**outstanding**	20
電子メール プロキシがリスンするポートを設定します。	**port**	IMAP4S：993 POP3S：995 SMTPS：988[1]
デフォルトの電子メール サーバを指定します。	**server**	なし
電子メールとサーバ名との間の区切り記号を定義します。	**server-separator**	「@」

1. Eudora 電子メール クライアントでは、SMTPS 接続のデフォルトのポートが 988 の場合でも、SMTPS はポート 465 でだけ動作します。

電子メールプロキシの証明書認証

電子メール プロキシ接続の証明書認証は、Netscape 7x 電子メール クライアントで機能します。MS Outlook、MS Outlook Express、Eudora など、他の電子メール クライアントは、証明書ストアにアクセスできません。

MAPI の設定

MS Outlook Exchange プロキシとも呼ばれる MAPI には、次の要件があります。

- MS Outlook Exchange がリモート コンピュータにインストールされている必要があります。
- セキュリティ アプライアンス インターフェイス上で、MS Outlook Exchange プロキシをイネーブルにします。これには、グループポリシー webvpn コマンドの 1 つである **functions** コマンドを入力します。次の例を参考にしてください。

```
hostname(config)# group-policy group_policy_name attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# functions mapi
```

- Exchange サーバの NetBIOS 名を指定します。この Exchange サーバは、セキュリティ アプライアンス DNS サーバと同じドメイン上にあることが必要です。次の例を参考にしてください。

```
hostname(config)# domain domain_name
hostname(config)#
```

（注）　MS Outlook Exchange Mail Proxy を経由して接続されているオープンな MS Outlook クライアントは、Exchange Server 上で定期的にメール チェックを行っているため、接続がオープン状態に保たれます。Outlook がオープンである限り、接続がタイムアウトすることはありません。これは、設定には関係ありません。

Web 電子メール MS Outlook Web Access の設定

Web 電子メールとは、MS Outlook Web Access for Exchange 2000、Exchange 5.5、および Exchange 2003 のことです。中央サイトに MS Outlook Exchange Server が必要です。また、ユーザが次の作業を行う必要があります。

- WebVPN セッションで、ブラウザに電子メール サーバの URL を入力する。
- プロンプトが表示されたら、電子メール サーバのユーザ名を *domain\username* 形式で入力する。
- 電子メールのパスワードを入力する。

WebVPN のパフォーマンスの最適化

セキュリティ アプライアンスには、WebVPN のパフォーマンスと機能性を最適化するいくつかの方法があります。パフォーマンスの改善には、キャッシングと Web オブジェクトの圧縮が含まれます。機能性の調整には、コンテンツの変換およびプロキシのバイパスが含まれます。APCF は、コンテンツの変換を調整するための追加的な方法を提供します。この項では、次のトピックを取り上げます。

- キャッシングの設定
- コンテンツの変換の設定

キャッシングの設定

キャッシングを行うと WebVPN のパフォーマンスが向上します。キャッシングによって頻繁に再利用されるオブジェクトはシステム キャッシュに保存され、コンテンツを繰り返しリライトしたり圧縮する必要性を減らすことができます。また、WebVPN とリモート サーバとのトラフィックが軽減されるため、多くのアプリケーションが今までよりはるかに効率的に実行できるようになります。

デフォルトでは、キャッシングはイネーブルになっています。次のように、webvpn モードからキャッシング コマンドを入力すると、ユーザの環境に応じてキャッシング動作をカスタマイズできます。

```
hostname(config)#
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)#
```

次に、キャッシング コマンドとその機能のリストを示します。

キャッシング コマンド	機能
cache-compressed	圧縮したコンテンツをキャッシングします。
disable	キャッシングをディセーブルにします。
expiry-time	キャッシング オブジェクトの期限切れの時刻を設定します。
lmfactor	キャッシングされたオブジェクトを再検証するための用語を設定します。
max-object-size	キャッシュに入れるオブジェクトの最大サイズを設定します。
min-object-size	キャッシュに入れるオブジェクトの最小サイズを設定します。

コンテンツの変換の設定

デフォルトでは、セキュリティ アプライアンスは、コンテンツ変換およびリライト エンジンを通じ、JavaScript および Java などの高度な要素からプロキシ HTTP へのトラフィックを含む、すべての WebVPN トラフィックを処理します。このようなトラフィックでは、ユーザがアプリケーションにアクセスするのに SSL VPN デバイス内部からアクセスしているか、これらに依存せずにアクセスしているかによって、セマンティックやアクセス コントロールのルールが異なる場合があります。

Web リソースによっては高度に個別の処理が要求される場合があります。次の各項では、このような処理を提供する機能について説明します。

- リライト済み Java コンテンツに署名するための証明書の設定

- コンテンツのリライトのディセーブル化
- プロキシのバイパスの使用
- アプリケーション プロファイル カスタマイゼーション フレームワークの設定

組織や関係する Web コンテンツの要件に応じてこれらの機能のいずれかを使用する場合があります。

リライト済み Java コンテンツに署名するための証明書の設定

WebVPN が変換した Java オブジェクトは、その後、トラストポイントに関連付けられた PKCS12 デジタル証明書により署名されます。**crypto ca import** コマンドと **java-trustpoint** コマンドを組み合せて、証明書をインポートし使用します。

次のコマンド例は mytrustpoint と呼ばれるトラストポイントの作成と Java オブジェクト署名への割り当てを示しています。

```
hostname(config)# crypto ca import mytrustpoint pkcs12 mypassphrase
Enter the base 64 encoded PKCS12.
End with the word "quit" on a line by itself.
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully.
hostname(config)# webvpn
hostname(config)# java-trustpoint mytrustpoint
hostname(config)#
```

コンテンツのリライトのディセーブル化

公開 Web サイトなどの一部のアプリケーションや Web リソースによっては、セキュリティ アプライアンスを通過しない設定が求められる場合があります。このため、セキュリティ アプライアンスでは、特定のサイトやアプリケーションをセキュリティ アプライアンスを通過せずにブラウズできるリライト ルールを作成できます。これは、IPSec VPN 接続のスプリット トンネリングと同様の機能です。

webvpn モードで **rewrite** コマンドと **disable** オプションを使用して、WebVPN トンネル外部にアクセスするためのアプリケーションとリソースを指定します。

この rewrite コマンドは複数回使用できます。セキュリティ アプライアンスはリライト ルールを順序番号に従って検索するため、ルールの順序番号は重要です。このとき、最下位の番号から順に検索して行き、最初に一致したルールが適用されます。

プロキシのバイパスの使用

ユーザはプロキシ バイパスを使用するようにセキュリティ アプライアンスを設定できます。これは、プロキシ バイパスが提供する特殊なコンテンツ リライト機能を使用した方が、アプリケーションや Web リソースをより有効活用できる場合に設定します。プロキシ バイパスはコンテンツ リライトに代わる手法で、元のコンテンツへの変更を最小限にします。多くの場合、カスタム Web アプリケーションでこれを使用すると有効です。

このコマンドは複数回使用できます。エントリを設定する順序は重要ではありません。インターフェイスとパス マスク、またはインターフェイスとポートを組み合せることで、プロキシ バイパスのルールを一意に指定できます。

ネットワーク設定に応じてパス マスクではなくポートを使用してプロキシ バイパスを設定する場合、これらのポートからセキュリティ アプライアンスにアクセスできるようにファイアウォール設定を変更する必要がある場合があります。この制約を回避するにはパス マスクを使用します。ただし、このパス マスクは変更される場合があるため、複数の pathmask 文を使用して可能性を排除する必要があることに注意してください。

パスとは URL の中で .com、.org、または他のドメイン名以降に記述されているすべてを指します。たとえば、www.mycompany.com/hrbenefits という URL では、*hrbenefits* がパスになります。同様に、www.mycompany.com/hrinsurance という URL では、*hrinsurance* がパスです。すべての hr サイトでプロキシ バイパスを使用する場合は、/hr* のように * をワイルドカードとして使用すると、コマンドを何度も入力しなくてもすみます。

プロキシ バイパスを設定するには、webvpn モードで **proxy-bypass** コマンドを使用します。

アプリケーション プロファイル カスタマイゼーション フレームワークの設定

WebVPN 用の Apllication Profile Customization Framework（APCF; アプリケーション プロファイル カスタマイゼーション フレームワーク）プロファイルを使用すると、セキュリティ アプライアンスは、標準以外のアプリケーションや Web リソースを処理できるようになり、WebVPN 接続を介してこれらが正しく表示されます。APCF プロファイルには、特定のアプリケーションに送信するデータの送信時刻（処理前、処理後）、送信部分（ヘッダー、本文、要求、応答）、および送信内容を指定したスクリプトが含まれています。スクリプトは XML 形式で記述され、ストリングおよびテキストの変換では sed（ストリーム エディタ）のシンタックスが使用されます。APCF プロファイルは、セキュリティ アプライアンス上で数種類を同時に実行することができます。1 つの APCF プロファイルのスクリプト内に複数の APCF ルールを適用することができます。この場合、セキュリティ アプライアンスは、最も古いルール（設定履歴に基づいて）を最初に処理し、次に 2 番目に古いルール、その次は 3 番目という順序で処理します。

APCF プロファイルは、セキュリティ アプライアンスのフラッシュ メモリ、HTTP サーバ、HTTPS サーバ、または TFTP サーバに保存できます。webvpn モードで **apcf** コマンドを使用すると、セキュリティ アプライアンス上にロードする APCF プロファイルを指定し、検索することができます。

次の例は、フラッシュ メモリに保存されている apcf1.xml という名前の APCF プロファイルのイネーブル化を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf flash:/apcf/apcf1.xml
hostname(config-webvpn)#
```

この例では、ポート番号 1440、パスが /apcf の myserver という名前の https サーバにある APCF プロファイル apcf2.xml をイネーブルにする手順を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml
hostname(config-webvpn)#
```

APCF シンタックス

次の項では、APCF シンタックスについて説明します。

注意　APCF プロファイルの使い方を誤ると、パフォーマンスが低下したり、好ましくない表現のコンテンツになる場合があります。シスコのエンジニアリング部では、ほとんどの場合、APCF プロファイルを提供することで特定アプリケーションの表現上の問題を解決しています。

APCF プロファイルは、XML フォーマットおよび sed スクリプト シンタックスを使用します。表 37-4 に、この場合に使用する XML タグを示します。

表 37-4　APCF XML タグ

タグ	用途
<APCF>...</APCF>	すべての APCF XML ファイルを開くための必須のルート要素。
<version>1.0</version>	APCF の実装バージョンを指定する必須タグ。現在のバージョンは 1.0 だけです。
<application>...</application>	XML 記述の本文を囲む必須タグ。
<id> text </id>	この特定の APCF 機能を記述する必須タグ。
<apcf-entities>...</apcf-entities>	単一または複数の APCF エンティティを囲む必須タグ。
<js-object>…</js-object> <html-object>…</html-object> <process-request-header>...</preprocess-request-header> <process-response-header>...</preprocess-response-header> <preprocess-request-body>...</preprocess-request-body> <postprocess-request-body>...</postprocess-request-body> <preprocess-response-body>...</preprocess-response-body> <postprocess-response-body>...</postprocess-response-body>	コンテンツの種類または実施される APCF 処理の段階を指定するこれらのタグのうち 1 つは必須です。
<conditions>… </conditions>	処理前および処理後の子要素タグで、次の処理基準を指定します。 http-version （1.1, 1.0, 0.9 など） http-method （get、put、post、webdav） http-scheme （http、https、other） ("a.."z" | "A.."Z" | "0.."9" | ".-_*[]?")) を含む server-regexp 正規表現 ("a.."z" | "A.."Z" | "0.."9" | ".-_*[]?+()\{},")) を含む server-fnmatch 正規表現 user-agent-regexp user-agent-fnmatch request-uri-regexp request-uri-fnmatch 条件タグのうち 2 つ以上が存在する場合は、セキュリティ アプライアンスはすべてのタグに対して論理 AND を実行します。
<action> … </action>	指定の条件以下のコンテンツで実行する 1 つまたは複数のアクションを囲みます。つまり、これらのアクションのそれぞれを下記の <do> タグまたは <sed-script> タグで定義します。

表 37-4　APCF XML タグ （続き）

タグ	用途
<do>…</do>	次のいずれかのアクションを定義します。 <no-rewrite/> <no-toolbar/> <no-gzip/> <force-cache/> <force-no-cache/>
<sed-script> TEXT </sed-script>	アクション タグの子要素です。TEXT は有効な Sed スクリプトである必要があります。<sed-script> は、これより前に定義された <conditions> タグに適用されます。

APCF の例

APCF プロファイルの例を次に示します。

```
<APCF>
<version>1.0</version>
<application>
  <id>Do not compress content from notsogood.com</id>
  <apcf-entities>
      <process-request-header>
         <conditions>
           <server-fnmatch>*.notsogood.com</server-fnmatch>
         </conditions>
           <action>
             <do><no-gzip/></do>
           </action>
      </process-request-header>
  </apcf-entities>
</application>
</APCF>
```

WebVPN エンド ユーザ設定

この項は、エンド ユーザのために WebVPN を設定するシステム管理者を対象にしています。ここでは、エンド ユーザ インターフェイスをカスタマイズする方法について説明します。

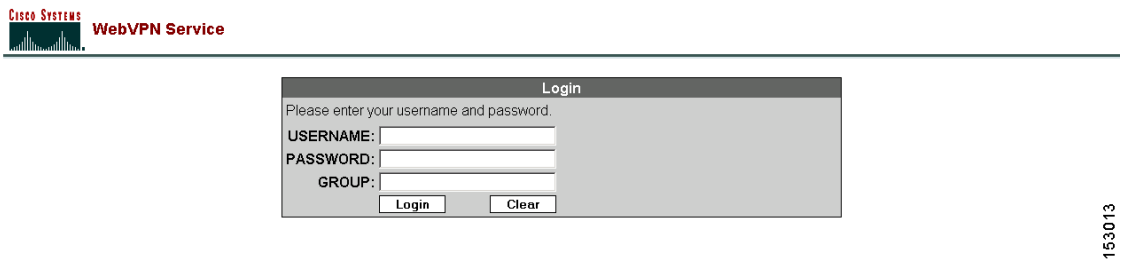
この項では、リモート システムの設定要件と作業の概要を説明します。ユーザが WebVPN の使用を開始するために、ユーザに伝える必要のある情報を明確にします。次の項目について説明します。

- エンド ユーザ インターフェイスの定義
- WebVPN ページのカスタマイズ
- ユーザ名とパスワードの要求
- セキュリティのヒントの通知
- WebVPN 機能を使用するためのリモート システムの設定

エンド ユーザ インターフェイスの定義

WebVPN エンド ユーザ インターフェイスは一連の HTML パネルで構成されます。ユーザは、セキュリティ アプライアンス インターフェイスの IP アドレスを https://*address* 形式で入力することにより、WebVPN にログインします。最初に表示されるパネルは、ログイン画面です（図 37-6）。

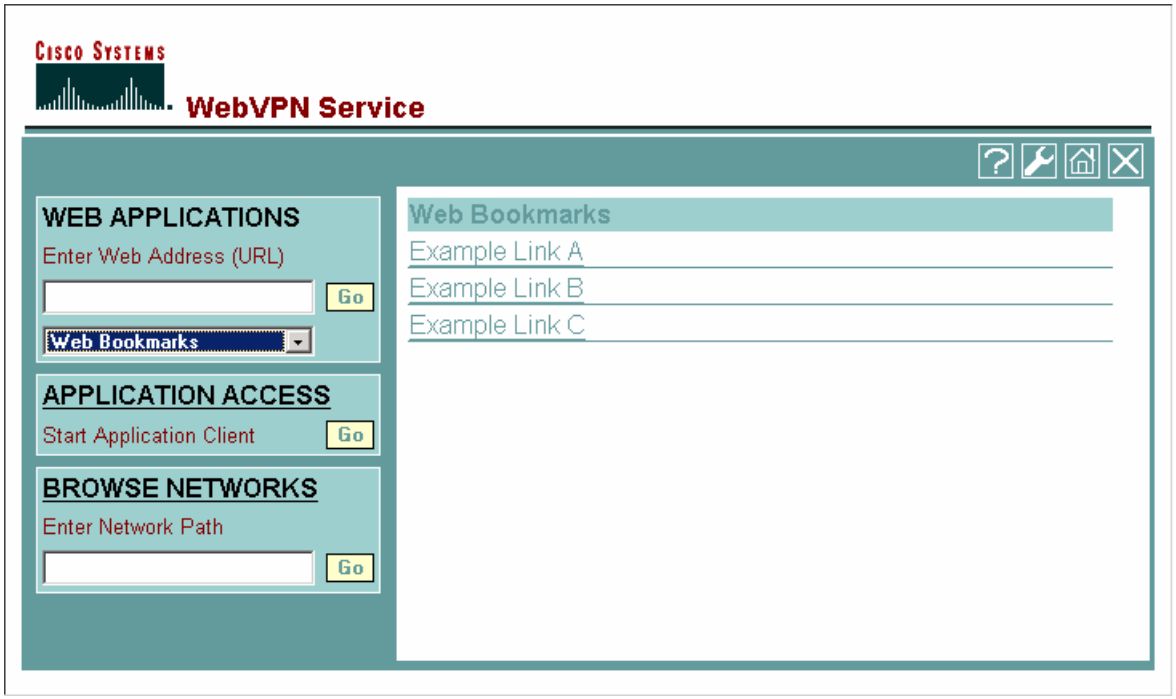
図 37-6　WebVPN の Login 画面



WebVPN ホームページの表示

ユーザがログインすると、WebVPN ホームページが開きます（図 37-7）。

図 37-7　WebVPN ホームページ

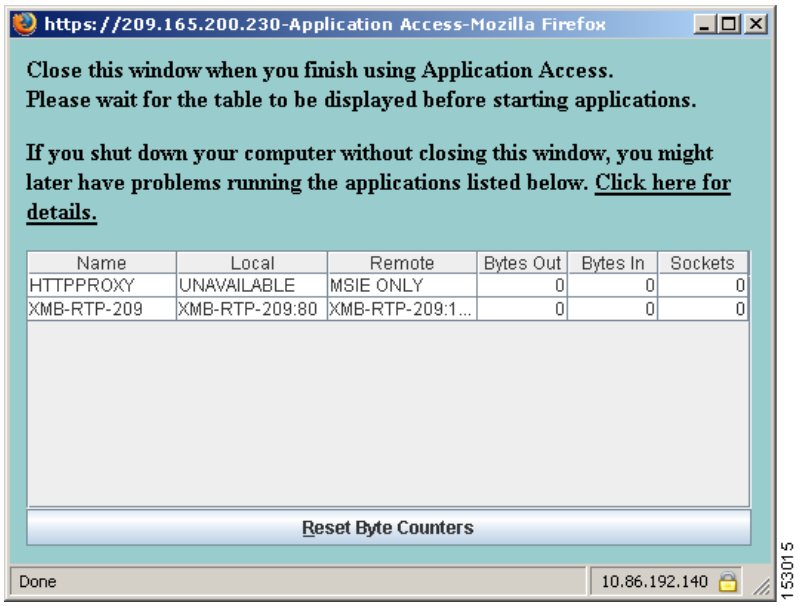


ホームページには設定済みの WebVPN 機能がすべて表示され、選択済みのロゴ、テキスト、および色が外観に反映されています。このサンプル ホームページには、特定のファイル共有の指定機能以外のすべての WebVPN 機能が表示されています。ユーザはこのホームページを使用して、ネットワークのブラウズ、URL の入力、特定の Web サイトへのアクセス、およびポート転送による TCP アプリケーションへのアクセスを実行できます。

WebVPN Application Access パネルの表示

ポート転送（アプリケーション アクセスとも呼ばれる）を開始するには、ユーザは Application Access ボックスの Go ボタンをクリックします。Application Access ウィンドウが開きます（図 37-8）。

図 37-8　WebVPN Application Access ウィンドウ



このウィンドウには、この WebVPN 接続用に設定された TCP アプリケーションが表示されます。アプリケーションを使用する場合は、このパネルを開いたまま、通常の方法でアプリケーションを起動します。

フローティング ツールバーの表示

図 37-9 に示すフローティング ツールバーは、現在の WebVPN セッションを表します。

図 37-9　WebVPN フローティング ツールバー

フローティング ツールバーの次の特性に注意してください。

- ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。
- ポップアップをブロックするようにブラウザが設定されている場合、フローティング　ツールバーは表示できません。
- ツールバーを閉じると、セキュリティ アプライアンスは WebVPN セッションの終了を確認するプロンプトを表示します。

WebVPN の使用方法については、表 37-6 を参照してください。

WebVPN ページのカスタマイズ

WebVPN ユーザに表示される WebVPN ページの外観を変えることができます。変更できる外観には、ユーザによるセキュリティ アプライアンスへの接続時に表示される Login ページ、セキュリティ アプライアンスのユーザ承認後に表示されるホームページ、ユーザによるアプリケーション起動時に表示される Application Access ウィンドウ、さらにはユーザによる Web VPN サービスのログオフ時に表示される Logout ページがあります。

WebVPN ページのカスタマイズ後は、このカスタマイズを保存して特定のトンネルグループ、グループ、ユーザに適用できます。いくつものカスタマイゼーションを作成、保存して、ユーザ個人やユーザ グループに応じて Web VPN ページの外観を変更するようにセキュリティ アプライアンスをイネーブル化できます。

ここでは、次の項目とタスクについて説明します。

- Cascading Style Sheet パラメータの使用（P.37-40）
- WebVPN Login ページのカスタマイズ（P.37-41）

Cascading Style Sheet パラメータの使用

多くの WebVPN カスタマイゼーション コマンドには、**style** オプションが含まれています。この値は、任意の有効な Cascading Style Sheet (CSS) パラメータで表されます。これらのパラメータの説明は、このマニュアルの範囲外です。CSS パラメータの詳細については、World Wide Web Consortium (W3C) の Web サイト、www.w3.org で CSS 仕様を参照してください。CSS 2.1 Specification の Appendix F には、CSS パラメータのリストがわかりやすく一覧されています。www.w3.org/TR/CSS21/propidx.html で参照できます。

次に、WebVPN ページの最も一般的な変更である、ページ色の変更についてヒントを示します。

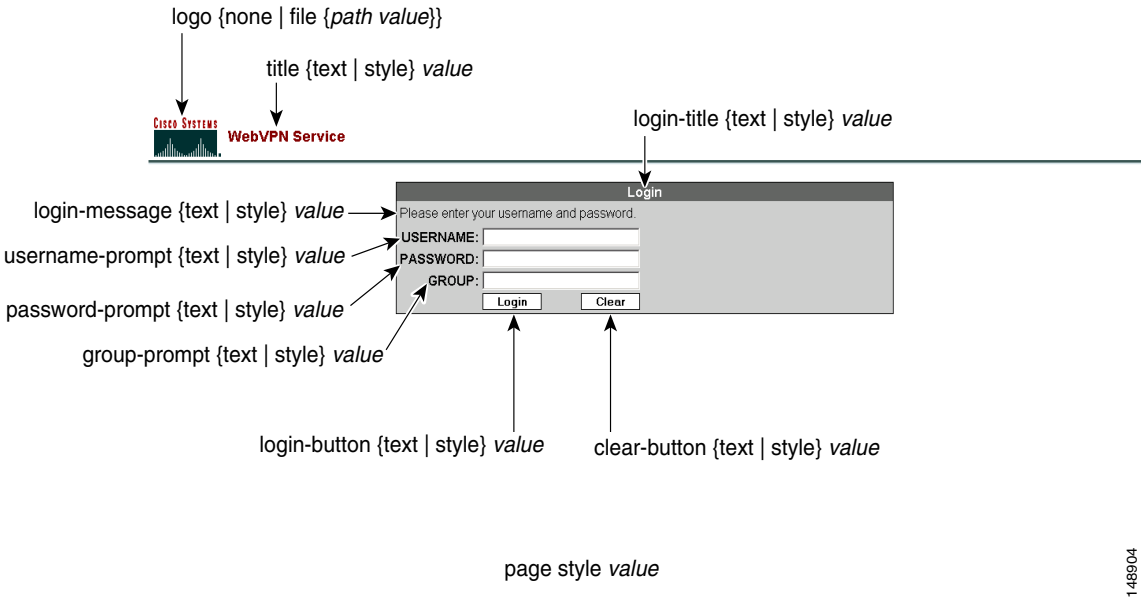
- カンマで区切った RGB 値、HTML の色値、または HTML で認識されている場合はその色の名前を使用することができます。
- RGB の形式は 0,0,0 で、赤、緑、青の各色にはそれぞれ 0 から 255 までの範囲の 10 進数を指定できます。カンマで区切ったエントリは、各色を他の色と組み合せる場合の強度を示します。
- HTML 形式は #000000 です。6 桁の 10 進数で構成され、最初と 2 番目の数字が赤、3 番目と 4 番目が緑、残りの 2 つが青をそれぞれ表します。

（注）　WebVPN ページのカスタマイズを簡略化するには ASDM を使用することをお勧めします。ASDM には、色見本などのスタイル要素の設定やプレビューなどの便利な機能があります。

WebVPN Login ページのカスタマイズ

図 37-10 に、WebVPN Login ページと、このページをカスタマイズするのに使用可能な関連する CLI コマンドを示します。

図 37-10　WebVPN Login ページと関連する CLI コマンド



次の手順に従うと、CLI コマンドを使用して WebVPN Login ページのすべての要素をカスタマイズできます。各種コマンドの使用例も示します。

ステップ 1　webvpn モードから **customization** コマンドを使用して、WebVPN カスタマイゼーション モードに入ります。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)#
```

ステップ 2　**page style** コマンドを使用して WebVPN Login ページの CSS のスタイルを変更します。

[no] page style *value*

```
hostname(config-webvpn-custom)# page style font-size:large
```

ステップ 3　**title** コマンドを使用してタイトルを変更します。

[no] title {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# title text Cisco WebVPN Service
```

ステップ 4　**logo** コマンドを使用して、ロゴをフラッシュ メモリに常駐するロゴに変えます。

[no] logo {none | file {*path value***}}**

ロゴを拒否して、ロゴが継承されないようにするには、**none** オプションを使用してヌル値を設定します。

```
hostname(config-webvpn-custom)#logo file disk0:cisco_logo.gif
```

ステップ 5　Login ボックスのタイトルを **login-title** コマンドを使用して変更します。

[**no**] **login-title** {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# login-title style background-color:
rgb(51,51,255);color: rgb(51,51,255); font-family: Algerian; font-size: 12pt;
font-style: italic; font-weight: bold
```

ステップ 6　Login ボックスのメッセージを **login-message** コマンドを使用して変更します。

[**no**] **login-message** {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# login-message text username and password
```

ステップ 7　Login ボックスに表示されるユーザ名のプロンプトを **username-prompt** コマンドを使用して変更します。

[**no**] **username-prompt** {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# username-prompt text Corporate Username:
hostname(config-webvpn-custom)# username-prompt style font-weight:bolder
```

ステップ 8　Login ボックスに表示されるパスワードのプロンプトを **password-prompt** コマンドを使用して変更します。

[**no**] **password-prompt** {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# password-prompt text Corporate Username:
hostname(config-webvpn-custom)# password-prompt style font-weight:bolder
```

ステップ 9　Login ボックスに表示されるグループ プロンプトを **group-prompt** コマンドを使用して変更します。

[**no**] **group-prompt** {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# group-prompt text Corporate Group:
hostname(config-webvpn-custom)# group-prompt style font-weight:bolder
```

ステップ 10　Login ボックスの Login ボタンの内容または外観を **login-button** コマンドを使用して変更します。

[**no**] **login-button** {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# login-button text OK
```

ステップ 11　Login ボックスの Clear ボタンの内容または外観を **clear-button** コマンドを使用して変更します。

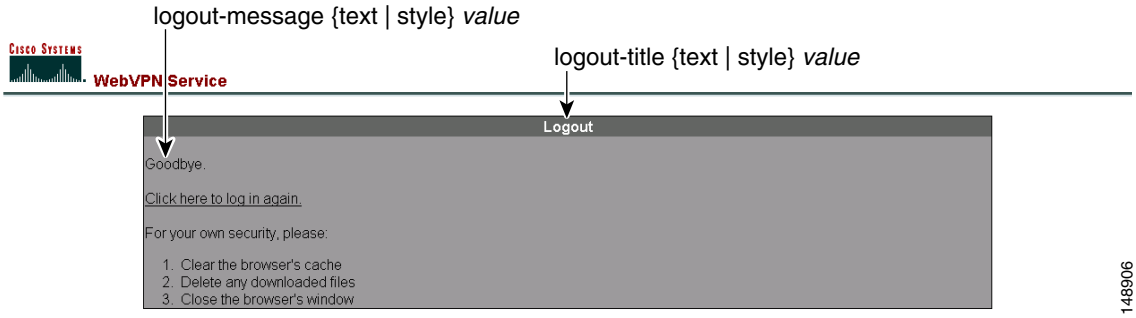
[no] clear-button {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# clear-button background-color:blue
```

WebVPN Logout ページのカスタマイズ

セキュリティ アプライアンスは、WebVPN ユーザが WebVPN のサービスをログアウトするときに WebVPN Logout ページを表示します。図 37-11 に、WebVPN Logout ページとこのページをカスタマイズするのに使用可能な関連する CLI コマンドを示します。

図 37-11　WebVPN Logout ページ



次の手順に従うと、CLI コマンドを使用して WebVPN Logout ページをカスタマイズできます。各種コマンドの使用例も示します。

ステップ 1　webvpn モードから **customization** コマンドを使用して、WebVPN カスタマイゼーション モードに入ります。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)#
```

ステップ 2　Logout ボックスのタイトルを **logout-title** コマンドを使用して変更します。

[no] logout-title {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# logout-title style background-color:
rgb(51,51,255);color: rgb(51,51,255); font-family: Algerian; font-size: 12pt;
font-style: italic; font-weight: bold
```

ステップ 3　Logout ボックスのメッセージを **logout-message** コマンドを使用して変更します。

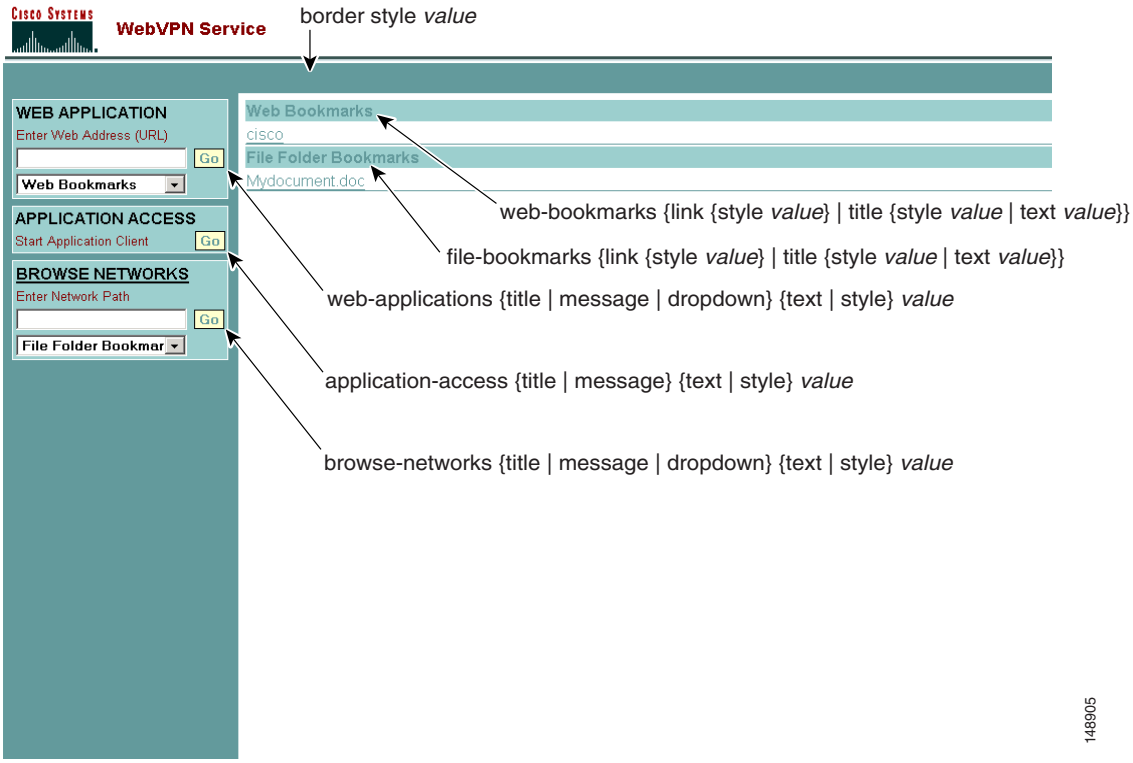
[no] logout-message {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# login-title style background-color:
rgb(51,51,255);color: rgb(51,51,255); font-family: Algerian; font-size: 12pt;
font-style: italic; font-weight: bold
```

WebVPN ホームページのカスタマイズ

セキュリティ アプライアンスが認証済み WebVPN ユーザに表示する WebVPN ホームページの外観をカスタマイズできます。図 37-12 に、WebVPN ホームページと、このページをカスタマイズするのに使用可能な関連する CLI コマンドを示します。

図 37-12　WebVPN ホームページと関連する CLI コマンド



次の手順に従うと、CLI コマンドを使用して WebVPN ホームページのすべての要素をカスタマイズできます。各種コマンドの使用例も示します。

ステップ 1　webvpn モードから **customization** コマンドを使用して、WebVPN カスタマイゼーション モードに入ります。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)#
```

ステップ 2　**border style** コマンドと CSS パラメータを使用して WebVPN ページの外枠のスタイルを変更します。

[no] border style *value*

```
hostname(config-webvpn-custom)# border style background-color:66FFFF
```

ステップ 3　**web-applications** コマンドを使用して、Web Applications ボックスの外観を変更します。

[**no**] **web-applications** {**title** | **message** | **dropdown**} {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# web-applications title text WWW Applications
hostname(config-webvpn-custom)# web-applications title style color:blue
hostname(config-webvpn-custom)# web-applications message text Enter URL
hostname(config-webvpn-custom)# web-applications message style color:blue
hostname(config-webvpn-custom)# web-applications dropdown text URLs to Browse
hostname(config-webvpn-custom)# web-applications dropdown style color:red
```

ステップ 4　**application-access** コマンドを使用して、Application Access ボックスの外観を変更します。

[**no**] **application-access** {**title** | **message**} {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# application-access title text Applications
hostname(config-webvpn-custom)# application-access title style color:blue
hostname(config-webvpn-custom)# application-access message text Start Application
hostname(config-webvpn-custom)# application-access message style color:blue
```

ステップ 5　**browse-networks** コマンドを使用して、Browse Networks ボックスの外観を変更します。

[**no**] **browse-networks** {**title** | **message** | **dropdown**} {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# browse-networks title text Corporate Nets
hostname(config-webvpn-custom)# browse-networks title style color:blue
hostname(config-webvpn-custom)# browse-networks message text Enter URL
hostname(config-webvpn-custom)# browse-networks message style color:blue
hostname(config-webvpn-custom)# browse-networks dropdown text URLs to Browse
hostname(config-webvpn-custom)# browse-networks dropdown style color:red
```

ステップ 6　**web-bookmarks** コマンドを使用して、Web Bookmarks タイトルまたはリンクを変更します。

[**no**] **web-bookmarks** {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

```
hostname(config-webvpn-custom)# web-bookmarks link style color:black
hostname(config-webvpn-custom)# web-bookmarks title style color:black
hostname(config-webvpn-custom)# web-bookmarks title text Corporate Web Bookmarks
```

ステップ 7　**file-bookmarks** コマンドを使用して、File Bookmarks タイトルまたは File Bookmarks リンクを変更します。

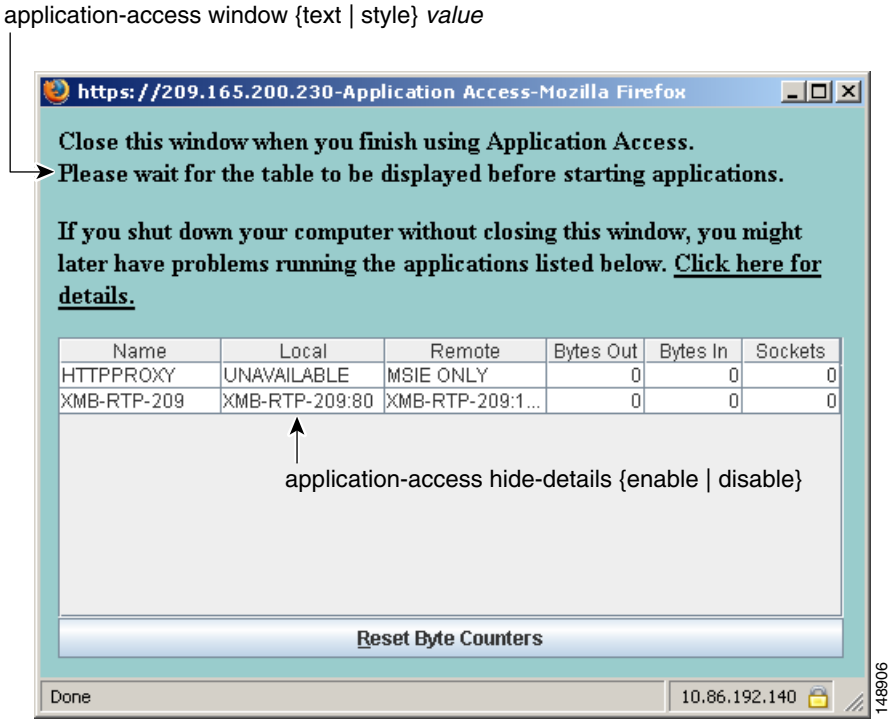
[**no**] **file-bookmarks** {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

```
hostname(config-webvpn-custom)# file-bookmarks link style color:blue
hostname(config-webvpn-custom)# file-bookmarks title style color:blue
hostname(config-webvpn-custom)# file-bookmarks title text Corporate File Bookmarks
```

Application Access ウィンドウのカスタマイズ

リモート ユーザがアプリケーションを選択すると起動される Application Access ウィンドウをカスタマイズすることができます。図 37-13 に、Application Access ウィンドウとカスタマイズで使用可能な関連する CLI コマンドを示します。

図 37-13　Application Access ウィンドウ



次の手順に従うと、CLI コマンドを使用して Application Access ウィンドウをカスタマイズできます。各種コマンドの使用例も示します。

ステップ 1　webvpn モードから **customization** コマンドを使用して、WebVPN カスタマイゼーション モードに入ります。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)#
```

ステップ 2　**application-access window** コマンドを使用して、Application Access ウィンドウを変更します。

[no] application-access window {**text** | **style**} *value*

```
hostname(config-webvpn-custom)# application-access window text URLs to Browse
hostname(config-webvpn-custom)# application-access window style color:red
```

ステップ 3　**application-access hide-details** コマンドを使用して、WebVPN Applications Access ウィンドウへのアプリケーション詳細の非表示をイネーブル化またはディセーブル化します。

[**no**] **application-access hide-details {enable | disable}**

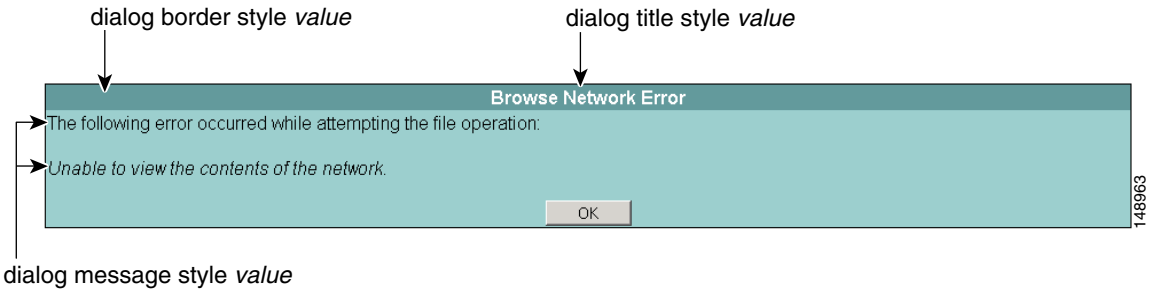
デフォルトではディセーブルになっています。アプリケーションの詳細は非表示にならず、Application Access ウィンドウに表示されます。

```
hostname(config-webvpn-custom)# application-access hide-details enable
```

プロンプト ダイアログのカスタマイズ

セキュリティ アプライアンスは、通知や警告などのさまざまなプロンプト ダイアログ メッセージを WebVPN ユーザに送信します。図 37-14 に、ダイアログ メッセージと、これらのメッセージの外観をカスタマイズするのに使用可能な関連する CLI コマンドを示します。

図 37-14　ダイアログ メッセージと関連する CLI コマンド



次の手順で、ダイアログ メッセージのすべての要素のカスタマイズと、各種コマンドの使用例を示します。

ステップ 1　webvpn モードから **customization** コマンドを使用して、WebVPN カスタマイゼーション モードに入ります。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)#
```

ステップ 2　**dialog border** コマンドを使用して、ダイアログ メッセージの外枠をカスタマイズします。

[**no**] **dialog border style** *value*

```
hostname(config-webvpn-custom)# dialog border style color:blue
```

ステップ 3　**dialog title** コマンドを使用してタイトルの外観を変更します。

[**no**] **dialog title style** *value*

```
hostname(config-webvpn-custom)# dialog title style font:bolder
```

ステップ 4　**dialog message** コマンドを使用してメッセージの外観を変更します。

[**no**] **dialog message style** *value*

```
hostname(config-webvpn-custom)# dialog message style font:italic
```

トンネルグループ、グループ、およびユーザへのカスタマイゼーションの適用

カスタマイゼーションを作成したら、このカスタマイゼーションを **customization** コマンドを使用して、トンネルグループ、グループ、またはユーザに適用することができます。このコマンドで表示されるオプションは、現在のモードの種類によって異なります。

トンネルグループ、グループポリシー、およびユーザの設定の詳細については、第 30 章「トンネルグループ、グループポリシー、およびユーザの設定」を参照してください。

トンネルグループへのカスタマイゼーションの適用

トンネルグループにカスタマイゼーションを適用するには、トンネルグループの webvpn モードで、次のように **customization** コマンドを使用します。

[**no**] **customization** *name*

name は、トンネルグループに適用するカスタマイゼーションの名前です。

コンフィギュレーションからコマンドを削除して、トンネルグループからカスタマイゼーションを削除するには、コマンドの **no** 形式を使用します。

customization コマンドの後に疑問符（?）を入力して、既存のカスタマイゼーションのリストを表示します。

次の例では、トンネルグループの webvpn モードに入ってから、トンネルグループ *cisco_telecommuters* のカスタマイゼーション *cisco* をイネーブルにしています。

```
hostname(config)# tunnel-group cisco_telecommuters webvpn-attributes
hostname(tunnel-group-webvpn)# customization cisco
```

グループおよびユーザへのカスタマイゼーションの適用

グループまたはユーザにカスタマイゼーションを適用するにはグループポリシー webvpn モードまたはユーザ名 webvpn モードで、**customization** コマンドを使用します。これらのモードには、**none** および **value** のオプションが含まれています。

[**no**] **customization** {**none** | **value** *name*}

none は、グループまたはユーザのカスタマイゼーションをディセーブルにして値が継承されないようにするオプションで、デフォルトの WebVPN ページを表示します。

value *name* は、グループまたはユーザに適用するカスタマイゼーションの名前です。

コンフィギュレーションからコマンドを削除して値が継承されるようにするには、コマンドの **no** 形式を使用します。

customization value コマンドの後に疑問符（?）を入力して、既存のカスタマイゼーションのリストを表示します。

次の例では、グループポリシーの webvpn モードに入ってから、セキュリティ アプライアンスにカスタマイゼーションのリストを照会し、グループポリシー *cisco_sales* のカスタマイゼーション *cisco* をイネーブルにしています。

```
hostname(config)# group-policy cisco_sales attributes
hostname(config-group-policy)# webvpn
hostname(config-username-webvpn)# customization value ?

config-username-webvpn mode commands/options:
Available configured customization profiles:
    DfltCustomization
    cisco
hostname(config-group-webvpn)# customization value cisco
```

次の例では、ユーザ名の webvpn モードに入ってから、ユーザ *cisco_employee* のカスタマイゼーション *cisco* をイネーブルにしています。

```
hostname(config)# username cisco_employee attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# customization value cisco
```

ユーザ名とパスワードの要求

ネットワークによっては、リモート セッション中にユーザが、コンピュータ、インターネット サービス プロバイダー、WebVPN、メール サーバ、ファイル サーバ、企業アプリケーションのうち、それらの一部またはすべてにログインする必要が生じることがあります。ユーザはさまざまなコンテキストで認証を行うために、一意のユーザ名、パスワード、PIN などさまざまな情報が要求される場合があります。

表 37-5 に、WebVPN ユーザが知っておく必要のあるユーザ名とパスワードのタイプを示します。

表 37-5　WebVPN ユーザに通知するユーザ名とパスワード

ログイン ユーザ名 / パスワード タイプ	目的	入力するタイミング
コンピュータ	コンピュータへのアクセス	コンピュータの起動
インターネット サービス プロバイダー	インターネットへのアクセス	インターネット サービス プロバイダーへの接続
WebVPN	リモート ネットワークへのアクセス	WebVPN の起動
ファイル サーバ	リモート ファイル サーバへのアクセス	WebVPN ファイル ブラウジング機能を使用して、リモート ファイル サーバにアクセスするとき
企業アプリケーションへのログイン	ファイアウォールで保護された内部サーバへのアクセス	WebVPN Web ブラウジング機能を使用して、保護されている内部 Web サイトにアクセスするとき
メール サーバ	WebVPN 経由によるリモート メール サーバへのアクセス	電子メール メッセージの送受信

セキュリティのヒントの通知

必ず WebVPN セッションからログアウトするようにユーザに通知してください（WebVPN からログアウトするには、WebVPN ツールバーの logout アイコンをクリックするか、またはブラウザを閉じます）。

WebVPN を使用してもすべてのサイトとの通信がセキュアであるとは限らないことを、ユーザに通知してください。WebVPN は、企業ネットワーク上のリモート PC やワークステーションとセキュリティ アプライアンスとの間のデータ転送のセキュリティを保証するものです。したがって、ユーザが HTTPS 以外の Web リソース（インターネット上や内部ネットワーク上にあるもの）にアクセスする場合、企業のセキュリティ アプライアンスから目的の Web サーバまでの通信はセキュアではありません。

WebVPN 機能を使用するためのリモート システムの設定

表 37-6 に、WebVPN を使用するためのリモート システムの設定に関する、次の各種情報を示します。

- WebVPN の起動
- WebVPN フローティング ツールバーの使用
- Web ブラウジング
- ネットワーク ブラウジングとファイル管理
- アプリケーションの使用（ポート転送）
- ポート転送を介した電子メールの使用
- Web アクセスを介した電子メールの使用
- 電子メール プロキシを介した電子メールの使用

また、表 37-6 には、次の項目に関する情報も記載されています。

- WebVPN の要件（機能別）
- WebVPN をサポートするアプリケーション
- クライアント アプリケーションのインストールとコンフィギュレーションの要件
- エンド ユーザに提供する必要のある情報
- エンド ユーザのためのヒントや使用上の推奨事項

ユーザ アカウントを別々に設定し、各ユーザがそれぞれ異なる WebVPN 機能を使用できるようにすることが可能です。表 37-6 には機能別の情報をまとめてあります。利用できない機能の情報についてはスキップしてください。

表 37-6　WebVPN リモート システム コンフィギュレーションとエンド ユーザの要件

作業	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
WebVPN の起動	インターネットへの接続	サポートされているインターネット接続は、次のとおりです。 • 家庭の DSL、ケーブル、ダイヤルアップ • 公共のキオスク • ホテルの回線 • 空港の無線ノード • インターネット カフェ
	WebVPN 対応のブラウザ	WebVPN には次のブラウザを推奨します。他のブラウザでは、WebVPN 機能を完全にはサポートできない場合があります。 Microsoft Windows の場合： • Internet Explorer バージョン 6.0 • Netscape バージョン 7.2 • Mozilla バージョン 1.7 以降 • Firefox 1.x Linux の場合： • Mozilla バージョン 1.7 • Netscape バージョン 7.2 • Firefox 1.x Solaris の場合： • Netscape バージョン 7.2 Macintosh OS X の場合： • Safari バージョン 1.0 • Firefox 1.x
	ブラウザでのクッキーのイネーブル化	ポート転送を介してアプリケーションにアクセスするために、ブラウザでクッキーをイネーブルにする必要があります。
	WebVPN 用の URL	https アドレスの形式は次のとおりです。 https://*address* *address* は、WebVPN がイネーブルになっているセキュリティ アプライアンスのインターフェイスの IP アドレスまたは DNS ホスト名（またはロードバランシング クラスタ）です。たとえば、https://10.89.192.163 または https://cisco.example.com のようになります。
	WebVPN のユーザ名とパスワード	
	（オプション）ローカル プリンタ	WebVPN は、Web ブラウザからネットワーク プリンタへの印刷をサポートしていません。ローカル プリンタへの印刷はサポートされています。

表 37-6　WebVPN リモート システム コンフィギュレーションとエンド ユーザの要件（続き）

作業	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
WebVPN フローティング ツールバーの使用		フローティング ツールバーを使用すると、WebVPN を簡単に使用できます。ツールバーを使用して、メインのブラウザ ウィンドウに影響を与えずに、URL の入力、ファイルの場所のブラウズ、設定済み Web 接続の選択ができます。 ポップアップをブロックするようにブラウザが設定されている場合、フローティング ツールバーは表示できません。 フローティング ツールバーは、現在の WebVPN セッションを表します。**Close** ボタンをクリックすると、セキュリティ アプライアンスは WebVPN セッションの終了を確認するプロンプトを表示します。 **ヒント**　ヒント：テキストをテキスト フィールドに貼り付けるには、Ctrl+V キーを使用します（WebVPN ツールバーでは右クリックはディセーブルになっています）。
Web ブラウジング	保護されている Web サイトのユーザ名とパスワード	WebVPN を使用しても、すべてのサイトとの通信がセキュアになるわけではありません。「セキュリティのヒントの通知」を参照してください。 WebVPN での Web ブラウジングのルックアンドフィールは、ユーザが見慣れたものではない場合があります。次の例を参考にしてください。 • WebVPN タイトル バーが各 Web ページの上部に表示される • Web サイトへのアクセス方法： 　– WebVPN ホームページ上の Enter Web Address フィールドに URL を入力する 　– WebVPN ホームページ上にある設定済みの Web サイト リンクをクリックする 　– 上記 2 つのどちらかの方法でアクセスした Web ページ上のリンクをクリックする また、特定のアカウントの設定によっては、次のようになる場合もあります。 • 一部の Web サイトがブロックされている • 使用可能な Web サイトが、WebVPN ホームページ上にリンクとして表示されるものに限られる

表 37-6　WebVPN リモート システム コンフィギュレーションとエンド ユーザの要件（続き）

作業	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
ネットワーク ブラウジングとファイル管理	共有リモートアクセス用に設定されたファイル アクセス権	WebVPN を介してアクセスできるのは、共有フォルダと共有ファイルに限られます。
	保護されているファイル サーバのサーバ名とパスワード	—
	フォルダとファイルが存在するドメイン、ワークグループ、およびサーバ名	ユーザは、組織ネットワークを介してファイルを見つける方法に慣れていない場合があります。
	—	コピー処理の進行中は、**Copy File to Server** コマンドを中断したり、別の画面に移動したりしないでください。コピー処理を中断すると、不完全なファイルがサーバに保存される可能性があります。
アプリケーションの使用 （ポート転送またはアプリケーション アクセスと呼ばれる）	**（注）** Macintosh OS X の場合、この機能をサポートしているのは Safari ブラウザだけです。	
	（注） この機能を使用するには、Sun Microsystems Java™ Runtime Environment をインストールしてローカル クライアントを設定する必要があります。これには、ローカル システムで管理者の許可が必要になるため、ユーザがパブリック リモート システムから接続した場合に、アプリケーションを使用できない可能性があります。	
	注意 ユーザは、**Close** アイコンをクリックしてアプリケーションを終了したら、必ず Application Access ウィンドウを閉じる必要があります。このウィンドウを正しく閉じないと、Application Access またはアプリケーション自体がディセーブルになる可能性があります。詳細については、「Application Access 使用時の hosts ファイル エラーの回復」を参照してください。	
	インストール済みのクライアント アプリケーション	—
	ブラウザでイネーブルにされているクッキー	—
	管理者特権	ユーザが DNS 名を使用してサーバを指定する場合、そのユーザは PC の管理者用アクセス特権を持つ必要があります。これは、hosts ファイルを修正するのにこの特権が必要なためです。

表 37-6　WebVPN リモート システム コンフィギュレーションとエンド ユーザの要件（続き）

作業	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
	インストール済みの Sun Microsystems Java Runtime Environment（JRE）バージョン 1.4.x と 1.5.x ブラウザで Javascript をイネーブルにする必要があります。デフォルトでは、イネーブルになっています。	JRE がインストールされていない場合は、ポップアップ ウィンドウが表示され、ユーザに対して使用可能なサイトが示されます。 まれに、JAVA 例外エラーで WebVPN ポート転送アプレットが失敗することがあります。このような状況が発生した場合は、次の手順を実行します。 **1.** ブラウザのキャッシュをクリアして、ブラウザを閉じます。 **2.** JAVA アイコンがコンピュータのタスク バーに表示されていないことを確認します。JAVA のインスタンスをすべて閉じます。 **3.** WebVPN セッションを確立し、ポート転送 JAVA アプレットを起動します。
	設定済みのクライアント アプリケーション（必要な場合） **（注）** Microsoft Outlook クライアントの場合、この設定手順は不要です。 Windows 以外のすべてのクライアント アプリケーションでは、設定が必要です。 Windows アプリケーションの設定が必要かどうかを確認するには、Remote Server の値をチェックします。 • Remote Server にサーバ ホスト名が含まれている場合、クライアント アプリケーションの設定は不要です。 • Remote Server フィールドに IP アドレスが含まれている場合、クライアント アプリケーションを設定する必要があります。	クライアント アプリケーションを設定するには、ローカルにマッピングされたサーバの IP アドレスとポート番号を使用します。この情報を見つけるには、次の手順を実行します。 **1.** リモート システム上で WebVPN を起動し、WebVPN ホームページの Application Access リンクをクリックします。Application Access ウィンドウが表示されます。 **2.** Name カラムで、使用するサーバ名を確認し、このサーバに対応するクライアント IP アドレスとポート番号を Local カラムで確認します。 **3.** この IP アドレスとポート番号を使用して、クライアント アプリケーションを設定します。設定手順は、クライアント アプリケーションによって異なります。
	（注） WebVPN でアプリケーションを実行している場合、アプリケーションで表示される URL（電子メール内の URL など）をクリックしても、WebVPN ではそのサイトは開きません。WebVPN でこのようなサイトを開くには、Enter WebVPN (URL) Address フィールドに URL をカット アンド ペーストします。	

表 37-6　WebVPN リモート システム コンフィギュレーションとエンド ユーザの要件（続き）

作業	リモート システムまたはエンド ユーザの要件	仕様または使用上の推奨事項
Application Access を介した電子メールの使用	Application Access の要件を満たす（「アプリケーションの使用」を参照）	電子メールを使用するには、WebVPN ホームページから Application Access を起動します。これにより、メール クライアントが使用できるようになります。
	（注） IMAP クライアントの使用中にメール サーバとの接続が中断し、新しく接続を確立できない場合は、IMAP アプリケーションを終了して WebVPN を再起動します。	
	その他のメール クライアント	Microsoft Outlook Express バージョン 5.5 および 6.0 はテスト済みです。 WebVPN は、Netscape Mail、Lotus Notes、および Eudora などの、ポート転送を介したその他の　SMTPS、POP3S、または IMAP4S 電子メール プログラムをサポートしますが、動作確認は行っていません。
Web アクセスを介した電子メールの使用	インストールされている Web ベースの電子メール製品	次の製品がサポートされています。 • Outlook Web Access 最適な結果を得るために、Internet Explorer 6.x 以上、Mozilla 1.7、または Firefox 1.x. で OWA を使用してください。 • Louts iNotes その他の Web ベースの電子メール製品も動作しますが、動作確認は行っていません。
電子メール プロキシを介した電子メールの使用	インストール済みの SSL 対応メール アプリケーション セキュリティ アプライアンス SSL バージョンを TLSv1 Only に設定しないでください。Outlook および Outlook Express は TLS をサポートしていません。	サポートされているメール アプリケーションは次のとおりです。 • Microsoft Outlook • Microsoft Outlook Express バージョン 5.5 および 6.0 • Netscape Mail バージョン 7 • Eudora 4.2 for Windows 2000 その他の SSL 対応クライアントも動作しますが、動作確認は行っていません。
	設定済みのメール アプリケーション	メール アプリケーションの使用方法と例については、「WebVPN を介した電子メールの使用」を参照してください。

WebVPN データのキャプチャ

CLI キャプチャ コマンドにより、WebVPN 接続では正しく表示されない Web サイトに関する情報を記録できます。このデータは、Cisco カスタマー サポート エンジニアによる問題のトラブルシューティングに役立ちます。次の各項では、キャプチャ コマンドの使用方法について説明します。

- キャプチャ ファイルの作成
- キャプチャ データを表示するためのブラウザの使用

（注）　WebVPN キャプチャをイネーブルにすると、セキュリティ アプライアンスのパフォーマンスに影響します。トラブルシューティングに必要なキャプチャ ファイルを生成したら、WebVPN キャプチャを必ずディセーブルにしてください。

キャプチャ ファイルの作成

次の手順を実行して WebVPN セッションに関するデータをファイルにキャプチャします。

ステップ 1　WebVPN キャプチャ ユーティリティを開始するには、特権 EXEC モードで **capture** コマンドを使用します。

capture *capture_name* **type webvpn user** *webvpn_username*

パラメータは次のとおりです。

- *capture_name* は、キャプチャに割り当てる名前です。これは、キャプチャ ファイルの名前の先頭にも付加されます。
- *webvpn_user* は、キャプチャの対象となるユーザ名です。

キャプチャ ユーティリティが開始されます。

ステップ 2　WebVPN ユーザが WebVPN セッションを開始するためにログインします。キャプチャ ユーティリティは、パケットをキャプチャしています。

コマンドの **no** バージョンを使用してキャプチャを停止します。

no capture *capture_name*

キャプチャ ユーティリティは *capture_name*.zip ファイルを作成し、このファイルはパスワード **koleso** で暗号化されます。

ステップ 3　.zip ファイルをシスコシステムズに送信するか、Cisco TAC サービス リクエストに添付します。

ステップ 4　.zip ファイルの内容を確認するには、パスワード **koleso** を使用してファイルを解凍します。

次の例では、*hr* という名前のキャプチャを作成します。これは、user2 への WebVPN トラフィックを次のようにファイルにキャプチャします。

```
hostname# capture hr type webvpn user user2
WebVPN capture started.
   capture name   hr
   user name      user2
hostname# no capture hr
```

キャプチャ データを表示するためのブラウザの使用

次の手順を実行して WebVPN セッションに関するデータをキャプチャし、これをブラウザに表示します。

ステップ 1　WebVPN キャプチャ ユーティリティを開始するには、特権 EXEC モードで **capture** コマンドを使用します。

capture *capture_name* **type webvpn user** *webvpn_username*

パラメータは次のとおりです。

- *capture_name* は、キャプチャに割り当てる名前です。これは、キャプチャ ファイルの名前の先頭にも付加されます。
- *webvpn_user* は、キャプチャの対象となるユーザ名です。

キャプチャ ユーティリティが開始されます。

ステップ 2　WebVPN ユーザが WebVPN セッションを開始するためにログインします。キャプチャ ユーティリティは、パケットをキャプチャしています。

コマンドの **no** バージョンを使用してキャプチャを停止します。

ステップ 3　ブラウザをオープンし、アドレスを指定するボックスに次のように入力します。

https://*IP_address またはセキュリティ アプライアンスのホスト名* **/webvpn_capture.html**

キャプチャされたコンテンツが sniffer 形式で表示されます。

ステップ 4　コンテンツをキャプチャし終えたら、コマンドの **no** バージョンを使用してキャプチャを停止します。