Cisco VPN 3000 シリーズ コンセントレータ リリース ノート（Release 4.1.2）

Part Number OL-5447-03

はじめに

（注） リリースされた Cisco VPN 3000 製品に関する最新の資料は、http://www.cisco.com から入手できます。これらのオンライン資料には、印刷版資料の作成後に行われた更新や変更が反映されている場合があります。

以下のリリース ノートは、Cisco VPN 3000 シリーズ コンセントレータ Release 4.1、Release 4.1.1、および Release 4.1.2 ソフトウェアを対象とします。これらのリリース ノートでは、新機能、既存機能の変更、制限および制約事項（「注意事項」）、解決済みの問題、および関連資料について説明します。また、このリリースに関して注意すべき問題点と、このリリースをロードする前に行う必要のある手順についても説明します。「使用上の注意」では、VPN 3000 シリーズ コンセントレータをインストールおよび使用する際に知っておくべきインターオペラビリティ上の考慮事項およびその他の問題点について説明します。これらのリリース ノートを熟読してから、このリリースをインストールしてください。

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

内容

リリース ノートの内容は次のとおりです。

システム要件（p.2）
Release 4.1.2 へのアップグレード（p.4）
Release 4.1 の新機能（p.9）
Release 4.1 の変更点（p.24）
使用上の注意（p.29）
VPN 3000 シリーズ コンセントレータの判明している注意事項（p.35）
Release 4.1.2 で解決された注意事項（p.47）
Release 4.1.1 で解決された注意事項（p.49）
Release 4.1 で解決された注意事項（p.50）
マニュアルの更新（p.54）
サービスおよびサポート（p.55）
マニュアルの入手方法（p.56）
テクニカル サポート（p.57）
その他の資料および情報の入手方法（p.60）

システム要件

ここでは、Release 4.1 のシステム要件について説明します。

サポートするハードウェア

Cisco VPN 3000 シリーズ コンセントレータ ソフトウェア Release 4.1 は、次のハードウェア プラットフォームをサポートします。

- Cisco VPN 3000 シリーズ コンセントレータ、モデル 3005 ～ 3080
- Altiga Networks VPN コンセントレータ、モデル C10 ～ C60
- Cisco VPN 3002 ハードウェア クライアント

次の表に、各 VPN コンセントレータ プラットフォームに必要な最小限のメモリ容量および推奨メモリ容量を示します。

（注） 推奨メモリ容量を使用しない場合、WebVPN の同時セッション数が減少します。

プラットフォーム	必要最小限のメモリ（MB）	WebVPN 用に強く推奨メモリ（MB）
3005	32	64
3015	128	256
3020	256	256
3030	128	512
3060	256	512
3080	256	512

（注） モデル 3030 ～ 3080 で、Enhanced-SEP（SEP-E）暗号化カードは従来の Scalable Encryption Processing（SEP）モジュールよりも高度なパフォーマンスを提供します。モデル 3020 では、SEP-E のみ使用できます。

プラットフォーム ファイル

Release 4.1.2 には 3 つのバイナリ ファイルがあり、それぞれ次のプラットフォームで使用します。

ファイル名の先頭部分	サポートするプラットフォーム
vpn3000	VPNコンセントレータ3015～3080プラットフォーム
vpn3005	VPN コンセントレータ 3005 プラットフォームのみ
vpn3002	VPN 3002 ハードウェア クライアントのみ

- vpn3000 で始まるファイル ― VPN コンセントレータ 3015 ～ 3080 プラットフォームをサポートします。
- vpn3005 で始まるファイル ― VPN コンセントレータ 3005 プラットフォームのみサポートします。
- vpn3002 で始まるファイル ― VPN 3002 ハードウェア クライアントのみサポートします。

注意 アップグレードするプラットフォームに対応するファイルをインストールしてください。

Release 4.1.2 へのアップグレード

ここでは、以前のリリースから Release 4.1.2 へのアップグレードについて説明します。

VPN 3000 コンセントレータのリリースをアップグレードする場合、VPN コンセントレータの管理中に新しい画面がすべて正しく表示されるように、ブラウザのキャッシュをクリアする必要があります。

（注） さらに、ログインしたあと、[Save Needed] をクリックして新しい Release 4.1.2 パラメータをコンフィギュレーション ファイルに追加する必要があります。これらの新しい Release 4.1.2 パラメータは、設定するとただちに実行コンフィギュレーションに追加されますが、VPN Concentrator Manager で [Save Needed] または [Save] アイコンをクリックしない限り、保存されたコンフィギュレーションには追加されません。

VPN 3000 コンセントレータ ソフトウェアを新バージョンにアップグレードしても、既存のコンフィギュレーション ファイルは自動的には上書きされません。新機能の設定オプション（たとえば、IKE プロポーザル）が、アップグレードによって自動的にコンフィギュレーション ファイルに保存されるわけではありません。HTML Manager では（[Save] ではなく）[Save Needed] が表示され、コンフィギュレーションを保存する必要があることが示されます。コンフィギュレーションを保存しなかった場合は、次の再起動時に新しい設定オプションが再び追加されます。コンフィギュレーション ファイルを TAC に送信する場合は、最初に実行コンフィギュレーションをコンフィギュレーション ファイルに保存してください。

作業を始める前に

このリリースにアップグレードする前に、*既存のコンフィギュレーションのバックアップ コピーをフラッシュおよび外部サーバに保存しておいてください*。これにより、必要な場合にシステムを以前のコンフィギュレーションおよびソフトウェアに戻すことができます。

アップグレードする前に、次の考慮事項に注意してください。これらの考慮事項は判明している製品の動作であり、製品をアップグレードする前に知っていると役立つものです。各項目の最後に、該当する問題について記述している注意事項の番号が付記されている場合があります。この番号を使用して特定の注意事項を探し出す方法については、VPN 3000 シリーズ コンセントレータの判明している注意事項（p.35）を参照してください。

VPN 3000 コンセントレータ ソフトウェア Release 4.1.2 には、VPN Client および VPN 3002 ハードウェア クライアント ソフトウェアの Release 4.0.x バージョンに対応する新機能と対話する機能がいくつか含まれています。このコンセントレータ リリースを最大限に活用するには、クライアント ソフトウェアを最新のリリースにアップグレードする必要があります。

（注） VPN 3000 コンセントレータ Release 4.1.2 と同時に発表される VPN Client リリースはありません。

VPN 3000 コンセントレータ ソフトウェア Release 4.1.2 は、VPN Client および VPN 3002 ハードウェア クライアントのバージョン 3.6 および 4.0 とは相互動作しません。Release 3.6 より古いバージョンの VPN 3002 または VPN Client を使用している場合は、新機能を活用するために、次のいずれかの新しいバージョンにアップグレードする必要があります。

- Release 3.0 から Release 4.1.2 にアップグレードしてグループ ルックアップ機能を使用する場合は、アップグレード後にグループ ルックアップを手動で設定する必要があります。この機能をイネーブルにするには、Configuration | System | General | Authentication の順に選択し、[Enable] チェック ボックスをオンにします（CSCdu63961）。
- VPN Client Release 3.0 以上を使用するには、VPN コンセントレータを Release 3.0 以上にアップグレードする*必要*があります。VPN Client Release 3.0 以上は、VPN 3000 コンセントレータのバージョン 2.5 以下とは相互動作*しません*。
- システムの処理負荷が高くなっているときには、VPN 3000 コンセントレータをアップデートしないでください。アップデートが失敗する可能性があります（CSCdr61206）。

次のバックアップ手順で、バックアップ用のコンフィギュレーションを確保します。

既存コンフィギュレーションのフラッシュへのバックアップ

1. Administration | File Management | Files の順に選択します。
2. コンフィギュレーション ファイルを選択し、[Copy] をクリックします。
3. バックアップ ファイルの名前（8.3 フォーマット、例 : CON412BK.TXT）を入力します。

これで、既存のコンフィギュレーションがフラッシュにコピーされました。

既存コンフィギュレーションの外部サーバへのバックアップ

サーバにもコンフィギュレーションのバックアップ コピーを作成しておく必要があります。これにはさまざまな方法がありますが、そのうちの 1 つに、Web ブラウザを使用して HTML インターフェイス（VPN コンセントレータ）からファイルをダウンロードする方法があります。

これにより、必要であれば以前のコンフィギュレーションを使用して以前のファームウェアに戻れる状態で、ソフトウェアをアップグレードできるようになりました。

注意 アップグレード後に、ブラウザのキャッシュを必ずクリアしてください。Release 4.1.2 では、機能の追加、HTML ページ レイアウトの拡張および cookie の削除が行われます。ブラウザのキャッシュをクリアすることによって、すべてが正しく表示され、新しい機能およびレイアウトを確実に使用することができます。

VPN 3000 上でのパスワード保存のイネーブル化による VPN 3002 パスワードの保存

VPN 3002 を 4.1.1 以上にアップグレードすると、VPN 3002 のユーザ パスワードが削除されます。この新機能は、VPN 3002 上でのユーザ パスワードのローカルな保存をイネーブルまたはディセーブル（デフォルト）にするオプションを提供し、パスワードの集中的な管理を可能にします。VPN 3002 にパスワードを保存するには、この時点でトンネルの VPN 3000 側のパスワード保存機能をイネーブルにする必要があります（CSCeb23742）。

VPN 3002 ハードウェア クライアントを使用して中央サイトの VPN3000 コンセントレータに接続している場合は、Release 4.1.x にアップグレードする *前*、*現在のソフトウェア リリースを実行している間に次の手順を行ってください。*

ステップ 1 2 台のデバイス間の既存のトンネルを使用して、中央サイトの VPN 3000 コンセントレータ上のパスワード保存機能をイネーブルにします。

ステップ 2 既存のトンネルをダウンにした後、トンネルを再確立します。この操作を最低でも 1 回実行してから、Release 4.1.x にアップグレードしてください。

ステップ 3 現在のイメージのバックアップ コピーを作成します。

ステップ 4 Release 4.1.x へのアップグレードを実行します。

Release 4.1.1 へのアップグレード後の HTTP/HTTPS 管理の設定

デフォルトでは、プライベート インターフェイス上で HTTP(S) 管理がイネーブルに設定されます。Release 4.1.1 以上へのアップグレード後に、パブリック / 外部インターフェイス経由で VPN 3000 コンセントレータを管理するには、Configuration | Interfaces | Ethernet # 画面の WebVPN タブの [public/external interfaces] で、HTTPS/HTTP 管理を明示的にイネーブルに設定する必要があります。

この設定は、プライベート インターフェイス経由での Telnet または HTTP(S) アクセスを使用するか、またはコンソール CLI（コマンドライン インターフェイス）を使用して行います。Configuration | Interfaces | Ethernet # 画面の WebVPN タブで、[Allow Management HTTPS sessions] パラメータを設定します（CSCec37514）。

VPN 3005 シリーズ コンセントレータ上の CompactFlash の修復

製造工程の問題によって、一部の VPN 3005 コンセントレータでファイル システムが壊れている場合があります。この不具合の結果、証明書やコンフィギュレーション ファイルを保存できない場合があります。不具合のある VPN 3005 コンセントレータは、シリアル番号 CAM0708xxxx ～ CAM0750xxxx（xxxx は各コンセントレータの一意のサフィックス）の範囲のコンセントレータです。ただし、この範囲に限定されるわけではありません（CSCed68739、CSCed72955）。

Release 4.1.1 以上では、使用する VPN 3005 コンセントレータにこの問題があれば自動的に検知されますが、Release 4.1.1 以上で稼働する VPN 3005 コンセントレータ上の壊れた CompactFlash 上でファイルを修復するには、次の手順を行う必要があります。

ステップ 1 コンフィギュレーション ファイルをローカルに保存します。

ステップ 2 必要なすべてのファイルをリモート ホストにバックアップします。

ステップ 3 CLIプロンプトから、**Administration > File Management > Reformat Filesystem** の順に選択します。

ステップ 4 プロンプトに YES と入力します。

ステップ 5 コンフィギュレーションをリロードします。

ステップ 6 各コンセントレータの certificates.suffix を再インストールします。

（注） この修復手順を実行する場合、VPN 3005コンセントレータ上のCompactFlashカードを交換する必要はありません。

Release 4.1.2 からのダウングレード

Release 4.1.2 より 前のリリ ースに戻す必要がある場合は、次の手順を行います。

ステップ 1 希望するリリースのファームウェアをリロードします（まだ再起動しないでください）。

ステップ 2 既存のコンフィギュレーション ファイルのコピーを作成し、そのコピーに新しい名前を付けます（例：CON412BK.TXT）。

ステップ 3 [CONFIG] を削除します。

ステップ 4 以前に保存しておいたバックアップ　ファイル（例：CON411BK.TXT）を [CONFIG] にコピーします。[Save] はクリックしないでください（クリックすると、元の CONFIG ファイルが実行コンフィギュレーションで上書きされます）。

ステップ 5 ソフトウェアのリセットを実行します。

以前のファームウェアおよびイメージが復元されます。

Release 4.0、4.1、4.1.1、4.1.2 のコンフィギュレーションから Release 3.6 にダウングレードした場合の LAN 間接続グループからの情報の削除

125 を超えるユーザおよびグループが組み合わされた VPN コンセントレータは、SEP がアクティブでない場合、トンネルを終端できません。これは、アクティブな SEP のない VPN コンセントレータがモデル 3015 とみなされるためです。モデル 3015 は、125 のユーザおよびグループの組み合わせしかサポートしていません。

SEP-E を搭載し、Release 4.0、4.1、4.1.1、または 4.1.2 で稼働する VPN コンセントレータを Release 3.6 にダウングレードした場合に、この状況になることがあります。Release 3.6 は SEP-E モジュールをサポートしていないため、問題が発生します。Release 3.6 コードの実行中に SEP-E カードが検出されると、SEP-E は不明のカードとみなされます。

何らかの理由によって、モデルがサポートする以上のユーザ数を含むコンフィギュレーションをロードしようとすると、再起動後のコンソールに次のイベントが表示されます。

****

3 03/20/2003 14:03:16.260 SEV=3 CONFIG/32 RPT=1

SERVE Too Many Entries Error.Delete an entry before adding a new one.

****

（CSCea51435）

Release 4.1 の新機能

ここでは、VPN 3000 シリーズ コンセントレータの Release 4.1 の新機能について説明します。ポイント リリース（4.1.x）には、新機能が含まれません。これらの機能の設定および使用方法については、『*VPN 3000 Series Concentrator Reference Volume I: Configuration*』および『*VPN 3000 Series Concentrator Reference Volume II: Administration and Management*』を参照してください。

VPN 3020 コンセントレータ

VPN 3000 コンセントレータ シリーズに VPN 3020 が追加されました。VPN 3020 の仕様は次のとおりです。

- 750 の同時リモート アクセス IPSec セッション *または* 200 の同時 WebVPN セッションのサポート（同時 IPSec セッション *および* WebVPN セッションの最大数については、「アクティブ セッションの最大数：WebVPN または IPSec、PPTP、L2TP/IPSec」[p.24] を参照してください）。
- メモリ 256 MB
- 1 つの SEP-E モジュールによるハードウェア ベースの暗号化
- 1 つの電源装置
- 拡張性：
  - 冗長性を提供するセカンダリ SEP-E モジュール
  - オプションの冗長電源装置

VPN 3020 を VPN 3030、3060、または 3080 にアップグレードすることはできません。

WebVPN

WebVPN を使用すると、ユーザは Web ブラウザを通じて VPN 3000 コンセントレータ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。ソフトウェアまたはハードウェア クライアント（IPSec または PPTP ベース）は不要です。WebVPN を使用すると、インターネットに接続して HTTP(s) サイトに到達できる任意のコンピュータから、Web リソース、Web 対応アプリケーション、NT/Active Directory（AD）ファイル シェア（Web 対応）、電子メールなどの TCP ベース アプリケーションをはじめとする、広範囲のエンタープライズ アプリケーションに簡単にアクセスすることができます。WebVPN は、Secure Socket Layer（SSL）プロトコルおよびその後継プロトコルである Transport Layer Security（SSL/TLS）を使用し、中央サイトにあるサポート対象の特定の内部リソースとリモート ユーザの間にセキュアな接続を提供します。VPN コンセントレータがプロキシを必要とする接続を認識し、HTTP サーバが認証サブシステムと対話してユーザを認証します。

（注） WebVPN をサポートするのは、VPN 3000 シリーズ コンセントレータ モデル 3005 ～ 3080 と、Altiga Networks VPN コンセントレータ モデル C10 ～ 60 のみです。VPN 3002 ハードウェア クライアントは、WebVPN をサポートしません。

ネットワーク管理者はユーザにグループ単位で WebVPN リソースへのアクセスを提供します。Release 4.1 で使用できる機能は次のとおりです。

- 電子メール プロキシ ― SSL 上の Post Office Protocol リビジョン 3（POP3S）、SSL 上の Internet Messages Access Protocol リビジョン 4（MAP4S）、および SSL 上の Simple Mail Transfer Protocol Secure（SMTPS）プロキシ経由での電子メールを可能にします。
- ポート フォワーディング（アプリケーション アクセス）― Java 1.4.1 以上が必要です。
- Windows ファイル アクセス ― 設定済みファイル サーバ上のファイルへのアクセス、またはネットワーク上のファイル閲覧を提供します。

（注） セキュリティ上の理由から、WebVPN ユーザは少なくとも WebVPN の使用を終えた時点でログアウトすることを強く推奨します。可能な場合、ブラウザ ウィンドウを閉じてください。

WebVPN の設定

WebVPN の設定方法については、『*VPN 3000 Series Concentrator Reference Volume I: Configuration*』の付録 A「Configuring WebVPN」を参照してください。

WebVPN で使用可能な最大セッション数については、このリリース ノートの「最大セッション数」（p.24）を参照してください。

WebVPN での閲覧に問題のある Web サイト

一部の社内 Web サイトまたは URL を指定して起動するアプリケーションが、WebVPN で正常に機能しない場合があります。ただし、サイトでスタティック TCP ポート番号を使用している場合は、WebVPN の TCP ポート フォワーディング（アプリケーション アクセス）機能を使用して、この問題を回避することができます。ダイナミック TCP ポートはサポートされません。

次に、TCP ポート フォワーディング パラメータを使用したサイトの設定例を示します。

名前：My_Web_Site

ローカル ポート：3456（例：http(s)://127.0.0.x:3456 または http(s)://FQDN:3456）。たとえば TCP ポート 3000 を使用する場合（例：http://FQDN または http://127.0.0.x:3000）

リモート サーバ：10.1.1.2 または Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）

リモート TCP ポート：3456（例：http(s)://127.0.0.x:3456 または http(s)://FQDN:3456）。たとえば TCP ポート 80 を使用する場合（例：http://FQDN または http://127.0.0.x:3000）

WebVPNを使用してこのWebサイトにアクセスする手順は、次のとおりです。

ステップ 1 WebVPN セッションを確立し、ポート フォワーディング（アプリケーション アクセス）アプレットを起動します。

ステップ 2 ブラウザを開き、アドレス フィールドに次のいずれかの値を入力します（値は前出の例に基づいています）。

- IPアドレスを使用する場合は、[http(s)://127.0.0.x:3000] を入力します。
- ドメイン ネーム サーバを使用する場合は、[http(s)://FQDN] を入力します。

また、正常に機能しないインターネット サイトまたは外部 Web サイトには SSL VPN（WebVPN）は使用せず、Web ブラウザを使用するという方法もあります。

Java または HTML に関して非互換の Web サイト

VPN 3000 WebVPN ソリューションは、Macromedia Flash を使用する Web サイトをサポートしていません。導入画面に Flash が使用されているだけで、WebVPN ユーザがログアウトされる場合もあります。その他のサイトでも問題が発生する可能性がありますが、限られたWebサイトしかテストしていません。

サイトによっては、JavaScript、Java、HTML、または Macromedia Flash コンテンツの現在の実装が非互換であるために動作しない場合があります（CSCeb78900、CSCec25478、CSCec49393、CSCec74334、CSCed05714）。このようなサイトの例に、次のものがあります。

www.avega.com、www.coors.com、www.hotmail.com、www.pwc.com、www.remax.com、www.windowsupdate.microsoft.com

Java アプレットによっては、そのアプレットのダウンロードに使用されたサーバが調べられ、定義済みサーバのリストと一致しないと、アプレットの実行が許可されないものがあります。このようなサイトにVPN 3000 WebVPN経由でアクセス（プロキシ）を試みても、この種のアプレットをダウンロードできません。その結果、これらのサイトは正常に表示されなかったり、情報が欠落していたりします。

アプリケーションに関する問題がある Web サイト

その他に、アプリケーションに関する問題があるサイトがあります。HTTP要求を生成する Java アプレット使用したアプリケーションは、WebVPN 上では動作しません。この理由から、たとえば CiscoSecure ACS アプリケーションにはログインできません（CSC78536）。

TCP ポート フォワーディング（アプリケーション アクセス）の Java に関する問題

（注） WebVPN ポート フォワーディング（アプリケーション アクセス）でサポートされるのは、Sun Microsystems Java のみです。Microsoft Java はサポートされません。

ポート フォワーディング（アプリケーション アクセス）に関して、次の問題があります。

- TCP ポート フォワーディング（アプリケーション アクセス）を使用するためにクライアントに必要なのは、J2SE バージョン 1.4.1 以上の Java Runtime Environment（JRE）部分だけです。

ヒント アプレットを使用して自動的にダウンロードするのではなく、java.sun.com から J2RE を手動でダウンロードすることを*強く*推奨します。

  - J2RE は、わずか 10 MB です。
  - J2SE は、90+ MB（以上）です（CSCec33444）。

- 証明書を使用してユーザ認証を実行する場合、TCP ポート フォワーディング（アプリケーション アクセス）Java アプレットは動作しません。Java は Web ブラウザのキーストアにアクセスできないので、ブラウザがユーザ認証に使用した証明書を使用できません（CSCec16732）。
- リンク（たとえば、電子メール メッセージに含まれているリンクなど）をクリックすると、そのリンクがアプリケーション アクセス Java アプレットを実行するブラウザ ウィンドウを使用しているため、ポート フォワーディング（アプリケーション アクセス）が無効になる場合があります。この動作は Internet Explorer では見られませんが、Netscape および Mozilla ブラウザにはこの問題があり、回避する方法も提供されていません（CSCec47541）。

アプリケーション アクセスの正常な停止

注意 アプリケーション アクセスの使用を終えた時点で、アプリケーション アクセス ウィンドウを閉じる（終了する）必要があります。

このウィンドウを閉じずにコンピュータをシャットダウンすると、あとでこれらのアプリケーションを実行するときに問題が発生することがあります。また、アプリケーションのホスト（メール サーバなど）にアクセスできなくなる可能性があります。アプリケーション アクセスを起動すると、ユーザの hosts ファイルが変更され、WebVPN 固有のエントリが追加されます。アプリケーション アクセス ウィンドウを閉じると、このファイルが元の状態に戻ります。詳細は、『*VPN 3000 Series Concentrator Reference Volume I: Configuration*』の付録 B「WebVPN End User Setup」を参照してください。

WebVPN での URL 閲覧用に推奨するブラウザ

現在のリリースで WebVPN を使用して URL を閲覧する場合、推奨するブラウザは次のとおりです。

オペレーティング システム	推奨するブラウザ
Windows	Internet Explorer バージョン 6.0、Service Pack 1
	Netscape バージョン 7.1
	Mozilla バージョン 1.4 および 1.5[1]
Linux	Mozilla バージョン 1.4 および 1.5[1]
	Netscape バージョン 7.1
Solaris	Netscape バージョン 7.1
Mac OS X[2]	Safari バージョン 1.0

1. Mozilla ブラウザ バージョン 1.6 では、WebVPN でアプリケーション アクセスを実行できません。Mozilla ブラウザ バージョン 1.5 および 1.4 では、アプリケーション アクセスを正常に起動して相互運用することができます（CSCed62309）。
2. Mac OS X では、Safari 1.0 だけがすべての WebVPN 機能をサポートします。

- それ以外のブラウザは、完全に適格ではありません。Opera 7.11 はサポートされません（CSCec18059）。Netscape 4.7x は推奨 *できません*。Linux プラットフォーム上の Opera Web ブラウザでは、WebVPN 経由のポートフォワーディングを使用できません。適正な 1.4.1 Java を使用しても、Linux 版の Opera は正常に動作しません（CSCeb81453）。
- Outlook Web Access（OWA）は、Internet Explorer 5.x 以下および他のブラウザでは表示および動作方式が異なります。これは WebVPN 接続とは無関係です。OWA は IE 5.x 以上でしか使用できない固有の機能を使用します（CSCec18088）。

各インターフェイスの SSL 証明書

Release 4.1 では、HTTP 管理および WebVPN のため、インターフェイスごとに 1 つの SSL 証明書が対応づけられます。インターフェイスに SSL 証明書がなければ、VPN 3000 コンセントレータの再起動時に自動的に生成されます。

さらに、ロードバランシングがイネーブルになると、ロードバランシング SSL 証明書が自動的に生成され、ディセーブルになると自動的に削除されます。

（注） セキュア HTTPS 管理または WebVPN アクセスに使用するインターフェイスに、有効な SSL 証明書があることを確認してください。

パブリックおよび外部インターフェイスでの HTTP および HTTPS のデフォルト設定（ディセーブル）

HTTP および HTTPS はデフォルトで、パブリック インターフェイスおよび外部インターフェイス上でディセーブルです。

HTTP および HTTPS をイネーブルにするには、CLI にアクセスするか、Telnet を使用するか、またはプライベート インターフェイスを使用します。両方ともイネーブルにするか、または両方ともディセーブルにするかのどちらかです。

HTML（GUI）インターフェイスで、Configuration | Interfaces の順に選択し、WebVPN タブの [Allow Management HTTPS Sessions] チェック ボックスをオンにします。

また、特定の IP アドレスからのアクセスを許可または禁止するには、Administration | Access Rights | Access Control List | Add または Modify の順に選択します（CSCec37514）。

VPN 3000 コンセントレータのグローバル設定

Web VPN が使用する認証および許可の設定は、グループ別に設定されたものではなく、グローバルな設定（ベース グループ）です。

（注） WebVPN は、有効期限付きの RADIUS *以外*のすべての認証方式（内部、RADIUS、SDI、Kerberos/Active Directory、証明書、NT ドメイン）をサポートします（CSCec38676）。

Release 4.1 の WebVPN では一般に、IPSec/PPTP で現在使用できるグループ単位の（およびベース グループ）パラメータの大部分が、WebVPN には適用できません。ただし、以下の例外があります。

- グループの WebVPN タブで使用できる WebVPN パラメータ
- Client Config タブの [Banner] は、WebVPN セッションに適用されます（CSCeb40901）。その他に [Base Group] の [Authorization/DN] フィールド パラメータ、および General タブのトンネリング プロトコルも適用されます。

WebVPN は、接続先グループの DNS 設定を使用しません。WebVPN は VPN 3000 コンセントレータのグローバルな DNS 設定に従います。

- そのため、同じグループに割り当てられたユーザであっても DNS の結果が異なる場合があり、管理者が混乱する可能性があります。コンセントレータのグローバルな DNS 設定が適切であるかどうかを確認するには、『*VPN 3000 Series Concentrator Reference Volume I: Configuration*』を参照してください（CSCed25396）。

次の表に、各種のパラメータに対する WebVPN のサポートの有無を示します。

パラメータ	グループ別	グローバル / システム全体
認証	なし	あり[1]
許可	なし	あり
アカウンティング	あり	あり[2]
DNS	なし	あり
サーバ /URL	あり[3]	あり
ポート フォワーディング	あり[3]	あり
URL エントリのイネーブル化	あり	あり

1. このリリースでは、WebVPN は有効期限付き RADIUS 認証をサポートしません（CSCec38676）。
2. グループにアカウンティング サーバが定義されていない場合は、IPSec/PPTP の場合と同様、グローバル / システム サーバが使用されます。
3. これらのポリシー設定を強制するには、RADIUS 認証が必要であり、RADIUS サーバが Class アトリビュートの値を `[OU=Group_name ;]`（セミコロンを含む）に設定して返す必要があります。

（注） WebVPN セッションの認証および許可には、リストの最上位にあるアクティブ サーバが、種類を問わず使用されます。この最上位のサーバで認証または許可が失敗した場合、リスト内で後続のサーバがこれらのタスクのために使用されることは*ありません*が、最上位のサーバが到達不可能である場合（たとえば、VPN 3000 コンセントレータがサーバへの TCP/UDP 接続を確立できない場合）は例外です。その場合に限り、リスト内で後続のサーバに接続して、認証または許可が試みられます。

WebVPN ブラウザのキャッシングおよびセキュリティに関連する注意事項

インターネット カフェやキオスクなど、パブリックまたは共有型のインターネット システムを通じて WebVPN を使用する場合は、WebVPN セッションを終了またはログアウトしたあと、セキュリティ保護のために、WebVPN セッション中に PC 上に保存したファイルをすべて削除してください。接続の切断時にこれらのファイルが自動的に削除されることはありません。*ログアウトしたあとで、ブラウザのキャッシュもクリアする必要があります*（CSCec78671）。

（注） WebVPN ではセッション中に表示した Web ページのコンテンツは保存されません。ただし、さらなるセキュリティ保護のために、ブラウザのキャッシュもクリアすることを推奨します。PC からコンテンツを削除しても、そのコンテンツが確実に回復不可能になるわけではありません。重要なデータをダウンロードするときは、このことを念頭に置いてください。

Solaris プラットフォームでの WebVPN のポートの常時待ち受け

Solaris プラットフォームで WebVPN のポート フォワーディング機能を使用したあと、WebVPN 接続を終了するか [Port Forwarding] ウィンドウを閉じても、ワークステーションは引き続きそれらのポートを待ち受けしています。また、同じブラウザで新しい WebVPN 接続を確立した場合、それらのポート経由のトラフィックは発生しません。この問題は、Solaris プラットフォームでのみ発生します。

ブラウザを閉じることによって、オープンされていたポートが完全に閉じられ、新しい WebVPN 接続でポートがトラフィックを転送できるようになります（CSCeb58582）。

WebVPN ユーザのアイドル タイムアウトの短時間設定

ブラウザが cookie をディセーブルに設定している場合、または cookie を要求されて拒否した場合、クライアント側のユーザは接続できないにも関わらず、Admin | Admin session | RAS データベースにそのユーザが追加されます。[max logins] が 1 に設定されていれば、すでに最大接続数を超過しているので、そのユーザは再びログインできません。管理者は WebVPN ユーザのアイドル タイムアウトを短く設定することを推奨します（CSCeb77581）。

WebVPN における Cookie の必要性

cookie がディセーブルに設定されていると、WebVPN は正常に動作できません。WebVPN には、cookie の使用が必須です（CSCeb58578）。

WebVPN のファイル共有におけるユーザ名およびパスワードの必要性

パスワードで保護されたシェアを使用する Windows 98 ワークグループは、共有リソースのアクセス制御がシェア レベルで設定されている場合、アクセスできません（CSCec23335）。

VPN 3000 経由のネットワーク プリンタの非サポート

WebVPN は、VPN 3000 コンセントレータの後ろ側にあるネットワーク プリンタへの印刷をサポートしません。WebVPN 上での印刷は、ホストまたは PC が WebVPN の外部で到達可能なすべてのプリンタでサポート*されます*（CSCec50393）。

Refresh アイコンによる WebVPN ページの更新およびリロード

ページを更新またはリロードするには、WebVPN ツールバーの [Refresh] アイコンを使用してください。WebVPN セッション中には、*ブラウザ*の更新 / リロード ボタンは使用しないでください。ブラウザの更新ボタンを使用すると、Internet Explorer 6.0 SP1 の場合には WebVPN セッションがホーム ページに戻され、Netscape 7.x および Mozilla 1.4 以上の場合には WebVPN セッションがログアウトされます（CSCed01739）。

一部のポップアップ / 広告防止ソフトウェアによるポート フォワーディング動作への悪影響

ある種のポップアップ / 広告防止ソフトウェア パッケージを使用した場合に、[TCP Port Forwarding] ウィンドウがポップアップしなくなることがあります。[TCP Port Forwarding] ウィンドウを選択したときにポップアップされるようにするには、このような広告防止ソフトウェアで、WebVPN のポータル ページを信頼できるサイトとして追加する必要があります（CSCeb35674）。

VPN 3000 コンセントレータのログインの変更（Release 4.1 以上）

WebVPN がイネーブルに設定されているインターフェイスを使用して VPN Concentrator Manager にログインするとき、管理者はインターフェイスの IP アドレスの後ろに [/admin] というストリングを入力する必要があります（例：192.168.1.1/admin）。

WebVPN エンド ユーザは、ログイン時に VPN 3000 コンセントレータの IP アドレスのみを入力します（例：192.168.1.1）。

MeetingMaker および SofTracker アプリケーションの非サポート

WebVPN 上では、MeetingMaker および SofTracker アプリケーションはサポートされません（CSCeb81114）。一般的に、WebVPN のポート フォワーディングでは、UDP を使用するアプリケーションはサポートされません。

ホスト名でのアンダースコア（ _ ）の使用不可

VPN 3000 コンセントレータのホスト名にアンダースコア（ _ ）が含まれていて、なおかつ Internet Explorer 6.0 SP1 Web ブラウザで VPN コンセントレータへの Web VPN 接続を確立しようとすると、その後のログインが失敗します。

FQDN にアンダースコアが含まれていても、ログイン ページにアクセスすることはできますが、ユーザ名とパスワードを入力すると、次のエラーが戻されます。

Cookies must be enabled to log in.

同じ設定でも Mozilla を使用すればログインできますが、この動作は VPN 3000 側の問題ではありません。

RFC 952 によると、これは Microsoft の問題でもなく、ホスト名にアンダースコアが不正に使用されていることが原因と考えられます。ホスト名の中でアンダースコアを使用することは認められません（CSCed34985）。

次に、この RFC の抜粋を示します。

> 「名前」（ネット、ホスト、ゲートウェイ、またはドメイン名）は、英字（A-Z）、数字（0-9）、マイナス記号（-）、およびピリオド（.）で構成される最大 24 文字のテキスト ストリングである。ピリオドは、「ドメイン スタイルの名前」でコンポーネントの区切り文字としてのみ使用できる（詳細は RFC 921「Domain Name System Implementation Schedule」を参照）。名前の一部としてブランクまたはスペース文字を使用することはできない。大文字と小文字は区別されない。最初の文字は英字でなければならない。最後の文字はマイナス記号またはピリオドであってはならない。ゲートウェイとして動作するホストは、名前の一部に「-GATEWAY」または「-GW」が使用されている必要がある。

Microsoft Knowledge Base の次のリンクも参照してください。

http://support.microsoft.com/default.aspx?scid=kb;en-us;149044

http://support.microsoft.com/default.aspx?scid=kb;en-us;294217

WebVPN キャプチャ ツール

WebVPN CLI には、WebVPN 接続で正常に表示されない Web サイトに関する情報を記録するためのキャプチャ ツールが含まれています。このツールの出力に基づいて、シスコのカスタマー サポートが問題をトラブルシューティングします。

このツールを使用するには、WebVPN でロギングをイネーブルに設定している必要があります(『*VPN 3000 Series Concentrator Reference Volume I: Configuration*』の「Monitoring | Event Log | Configure WebVPN Logging」を参照)。このツールを使用して、正常に表示されない Web サイトに関する情報を取得します。

WebVPN キャプチャ ツールの出力は、次の 2 つのファイルで構成されます。

- [mangled.001, 002...] など（Web ページのアクティビティによって異なります)。mangle ファイルは、VPN 3000 コンセントレータが WebVPN 接続を使用してこれらのページを転送するために実行した HTML アクションを記録しています。
- [original.001, 002...] など（Web ページのアクティビティによって異なります)。original ファイルは、その URL で VPN 3000 コンセントレータに送信されたファイルです。

キャプチャが終了した時点で、必ずキャプチャ ツールをオフにしてください。これらのファイルを表示するには、Administration | File Management の順に選択します。

WebVPN キャプチャ ツールの使用法については、『*VPN 3000 Series Concentrator Reference Volume I: Configuration*』の付録「Configuring the VPN Concentrator for WebVPN」を参照してください。

Lotus iNotes および Microsoft Exchange の非サポート

このリリースでは、WebVPN は Lotus iNotes および Microsoft Exchange（Outlook/Exchange プロキシ）アプリケーションをサポートしません。

Microsoft Distributed File の非サポート

WebVPN は CIFS をサポートしますが、Microsoft Distributed File はサポートしません（CSCed86246）。

traceroute

VPN コンセントレータおよび VPN 3002 で、traceroute コマンドがサポートされるようになりました。このコマンドは、パケットが宛先 IP アドレスに到達するために使用したルートを記録し、ネットワーク接続に関する問題のトラブルシューティングに役立ちます。traceroute コマンドを使用するには、Sun Microsystems の JRE バージョン 1.4.1 以上が必要です。

注意 適正なバージョンの JRE をインストールしていない場合は、traceroute を実行しないでください。JRE のない状態で traceroute を実行すると、admin セッションが終了します。

Zone Labs Integrity：障害時の接続許可 / 禁止および複数サーバのサポート

Release 4.1 では IPSec 接続に関してのみ、接続を試みる時点で Integrity サーバが使用不可能な場合に、プライベート ネットワークを開く（Fail Open）、またはトンネルを終了する（Fail Closed）、のいずれかを指定できるオプションが追加されています。従来は、ユーザが接続する際 Zone Labs Integrity サーバが使用不可能な場合、ユーザはネットワークへのアクセスが与えられました。

このリリースでは、管理者は VPN コンセントレータが接続を受け入れる最大 5 つの Integrity サーバのリストを設定できます。アクティブな Integrity サーバが使用不可能になった場合、別の Integrity サーバが接続を開始できます。そのサーバが設定済みリストに含まれていれば、コンセントレータはそのサーバでユーザを認証します。

クライアントの OS/ バージョン タイプ別のアクセス制御

WebVPN 接続以外の接続について、管理者がサポート対象のクライアント タイプおよびソフトウェア バージョン別にリモート アクセス接続を制限することができます。この制限はすべての EZ-VPN クライアントに適用されます。たとえば、Windows 2000 ユーザだけが Internet Explorer 6.0, Service Pack 1 を使用してネットワークに接続でき、他のプラットフォームまたはバージョンにはアクセスを禁止するといった設定が可能です。

ネットワーク リストの LAN 間接続拡張機能

管理者は Configuration | IPSec | LAN-to-LAN | Add または Modify ページを使用して、LAN 間接続用のネットワーク リストを作成できます。

ping の拡張機能

ping コマンドを発行すると、デフォルトで、0xABCD というパターンに設定された ICMP データを持つ 100 バイトの ICMP エコー要求が 5 つ、タイムアウト 2 秒で送信されるようになりました。Manager および CLI の両方で、ステータスとして次の文字が ICMP 要求と同じ数だけ表示されます。

! ― 正常に応答を受信できた場合

. ― ping への応答を待機してタイムアウトした場合

C ― データが一致しなかった場合

U ― ICMP unreachable を受信した場合

VPN コンセントレータは、応答までの最小、平均、および最大ラウンドトリップ時間も計算して表示します。

VPN 3002 のパスワード保存に関する拡張機能

パスワード保存の拡張機能によって、保存されたパスワードは電源をリセットすると無効になります。デバイスが元の場所から移動された場合、この機能によってセキュリティが強化されます。

Release 4.1 の変更点

ここでは、Release 4.1 機能の旧リリースからの変更点について説明します。

最大セッション数

VPN コンセントレータは、IPSec、PPTP、L2TP/IPSec、および WebVPN セッションを、単独、またはこれらの組み合わせでサポートします。同時にアクティブにできるセッション数が、VPNコンセントレータでサポート可能なセッション数よりも少なくなるように制限することができます。セッション数の制限では、IPSec、PPTP、および L2TP/IPSec セッションが 1 つのグループとして扱われます。Configuration | System | General | Sessions 画面で、[Maximum Active Sessions]パラメータが上記のセッションに適用され、[Maximum Active WebVPN Sessions] パラメータが WebVPN セッションに適用されます。

一方のタイプのセッションの最大数を下げれば、もう一方のタイプのセッションがより多くサポートされるようになると思うかもしれませんが、VPN コンセントレータはそのようには動作しません。実際には、どちらかのタイプのアクティブ セッション数を意図的に減した場合、VPN コンセントレータがサポートする両方のタイプのセッション数が減ります。次の各項で具体的な例を示します。

（注） シスコでは、これらのパラメータのデフォルト値を入念にテストして確認済みです。シスコのテクニカル サポートから指示された場合以外は、これらのデフォルト値を変更しないことを推奨します。

アクティブ セッションの最大数：WebVPN または IPSec、PPTP、L2TP/IPSec

WebVPN セッションは、他のタイプよりも VPN コンセントレータのリソース所要量が著しく大きいので、次の表では WebVPN セッションだけを別扱いにしています。WebVPN セッションと他のタイプのセキュア セッションを混在させるときは、この違いについて理解しておく必要があります。

サポートされる最大セッション数は、VPN コンセントレータ ハードウェアによって決まるので、モデルごとに異なります。次の表に、VPN コンセントレータの各モデルで同時にサポートできるアクティブ WebVPN セッション *または* IPSec、PPTP、L2TP/IPSec セッションの最大数を示します。

VPNコンセントレータモデル	メモリ（MB）	他のセッションがアクティブでない場合のWebVPNセッション数（デフォルト = 最大数）	WebVPNセッションがアクティブでない場合の IPSec、PPTP、L2TP セッションの最大数（デフォルト = 最大数）	スループット（Mbs）[1]
3005	32	10	100	1
3005	64	50	200	1
3015	128	75	100	1.5
3020、SEP-E 搭載	256	200	750	9
3020、SEP-E 搭載	512	200		9
3030、SEP-E 搭載	128	100	1,500	9
3030、SEP-E 搭載	256	200		9
3030、SEP-E 搭載	512	500		9
3060、SEP-E 搭載	256	200	5,000	10.3
3060、SEP-E 搭載	512	500		10.3
3080、SEP-E 搭載	256	200	10,000	10.3
3080、SEP-E 搭載	512	500		10.3

1. これらのスループット値は、VPN コンセントレータが大量の処理を実行する必要のある Web ページで計測したパフォーマンスを反映しています。バイナリ データ ファイル、または検証や処理をあまり必要としないファイルを使用する場合には、記載されているスループット速度の約 2 倍になります。

WebVPN に関して記載されている数字は、VPN 3000 コンセントレータが WebVPN を使用して Web ページを取得するパフォーマンスを計測するための標準的なキャパシティおよびパフォーマンス テストに基づいています。これらのパフォーマンス テストは、次の条件に基づいて実施されています。

- 1 つの WebVPN セッションは、3DES 暗号化を使用してログオンした TLS-v1 WebVPN ユーザ 1 人を表す。
- 各ユーザは最大 60 秒ごとに 1 つの Web ページを受信する。
- ユーザは 1 秒ごとに 1 人の速度でログインし、テストを実行している間、データを送受信する。
- ベンチマークによる Web ページの平均取得時間は 5 秒以下である。
- テストに使用した Web ページのコンテンツには、次のフォーマットがすべて含まれる。プレーン テキスト、.gif ファイル、.jpg ファイル、URL、および Java スクリプト ファイル。

アクティブなセッションの最大数

同時にアクティブにできる IPSec、PPTP、および LT2P/IPSec セッション数を、VPN コンセントレータで潜在的にサポート可能なセッション数よりも少なくなるように制限することができます。

[Maximum Active Sessions] フィールドに 0 を指定すると、ハードウェアがサポートする最大セッション数より下の意図的な限界はないという意味になります。言い換えると、VPN コンセントレータ 3030 の場合、このフィールドが 0（デフォルト値）であれば、最大セッション数は 1500 です。

セッション数が設定された値に達すると、VPN コンセントレータは新たなどのタイプのセッションも許可しなくなります。たとえば、VPN 3005 上の IPSec セッションの最大数を 50 に設定した場合、アクティブな IPSec セッションが 50 個になると、VPN コンセントレータは新たな WebVPN、IPSec、PPTP、または L2TP/IPSec セッションを 1 つも受け入れなくなります。

アクティブな WebVPN セッションの最大数

[Maximum Active WebVPN Sessions] フィールドは、この VPN コンセントレータ上で同時にアクティブにできる WebVPN セッションの最大数を指定します。デフォルト値を使用することを推奨します。

セッション数が設定した値に達すると、VPN コンセントレータは新たなどのタイプのセッションも許可しなくなります。たとえば、VPN 3060 上の WebVPN セッションの最大数を 95 に設定した場合、アクティブな WebVPN セッションが 95 個になると、VPN コンセントレータは IPSec または WebVPN セッションを 1 つも受け入れなくなります。

IPSec、PPTP、L2TP/IPSec セッションに対する WebVPN セッションの比率

アクティブ セッションの最大数を示した表から、各プラットフォーム上での IPSec、PPTP、L2TP/IPSec セッションに対する WebVPN セッションの比率が導き出されます。VPN の使用に関連してネットワーク プランニングおよび管理を行うとき、これらの比率を利用できます。

いずれかの [Maximum Sessions] パラメータを変更すると、VPN コンセントレータ上での WebVPN セッションの他のセッションに対する比率が変化する点に注意してください。

例として、最大容量のメモリおよび SEP-E を搭載した VPN 3030 コンセントレータでの、[Maximum Session] パラメータと [Maximum WebVPN Sessions] パラメータの相互作用を次の表に示します。

プラットフォーム	Max Active Sessions（IPSec、PPTP、L2TP）の設定	Max Active WebVPN Sessions の設定	比率（WebVPN：その他のセッション）	例（WebVPN：その他のセッション）	例（その他のセッション：WebVPN セッション）
SEP-E および 512 MB のメモリを搭載した VPN 3030	1,500（デフォルト）	500（デフォルト）	1:3	アクティブなWebVPN セッションが 50 個の場合、最大 1350 個の IPSec セッションが許可される。	アクティブな IPSec セッションが1200個の場合、最大 100 個の WebVPN セッションが許可される。
	800	100	1:8	アクティブなWebVPN セッションが 50 個の場合、最大 400 個の IPSec セッションが許可される。	アクティブな IPSec セッションが 300 個の場合、最大 62 個の WebVPN セッションが許可される。
	1,500	50	1:30	アクティブなWebVPN セッションが 10 個の場合、最大 1200 個の IPSec セッションが許可される。	アクティブな IPSec セッションが 800 個の場合、最大 23 個の WebVPN セッションが許可される。
	1,200	50	1:24	アクティブなWebVPN セッションが 48 個の場合、最大 48 個の IPSec セッションが許可される。	IPSec セッションが 800 個の場合、最大 16 個の WebVPN セッションが許可される。
	1,200	50	1:24	アクティブなWebVPN セッションが 50 個の場合、IPSec セッションは許可されない。	アクティブな IPSec セッションが1200個の場合、WebVPN セッションは許可されない。

アクティブ セッション数が設定した値に達すると、VPN コンセントレータは新たなどのタイプのセッションも許可しなくなります。

Telnet Over SSL の変更点

Release 4.1 では、VPN コンセントレータへの Telnet over SSL 接続を確立する機能が削除されました。管理セッション用には、Telnet over SSL ではなく SSH を使用することを推奨します。WebVPN ポート フォワーディングには Telnet のサポートが含まれますが、VPN コンセントレータに Telnet over SSL で接続することはできません。

64 MB メモリ搭載 VPN 3005 コンセントレータの IPSec または PPTP セッションに対する最大サポート数

Release 4.1 では、64 MB のメモリを搭載した VPN 3005 コンセントレータは、最大 200 個のリモート アクセス IPSec セッションを同時にサポートします。

この最大セッション数を達成するには、VPN Client が次のどちらかの条件を満たしている必要があります。

- 4.0 以上のソフトウェアで稼働している。
- 4.0 より前のソフトウェアで稼働している場合は、分割トンネリングを実行しない。

VPN 3002 ハードウェア クライアントでは、分割トンネリングを実行しないでください。

（注） 32 MB のメモリを搭載した VPN 3005 コンセントレータは、最大 100 個の IPSec または PPTP セッションをサポートします。

HTTPS フィルタ ルールの変更点

Release 4.1 にアップグレードすることによって、HTTPS 用の設定済みのフィルタ ルールの実施に影響が出ます。インターフェイス上で [Allow Management HTTPS sessions] または [Allow WebVPN HTTPS sessions] パラメータをイネーブルに設定すると、以前のフィルタ設定との矛盾が生じる可能性があります。

たとえば、Release 4.0 では、VPN コンセントレータのパブリック インターフェイスには、パブリック ネットワーク上の PC 1 との間で HTTPS トラフィックを送受信するための 2 つの HTTP ルール（HTTPS In/Out）があります。

Release 4.0 VPN コンセントレータは、これらのフィルタ ルールを次のように実施します。

ルール 1. PC 1 に HTTPS In/Out を許可する。

ルール 2. それ以外の HTTPS トラフィックをすべて廃棄する（デフォルトのアクション）。

Release 4.1 にアップグレードし、パブリック インターフェイス上で [Allow Management HTTPS sessions] または [Allow WebVPN HTTPS sessions] パラメータをイネーブルに設定すると、実施方式が変更されます。VPN コンセントレータは、次の順序でフィルタ ルールを実施します。

ルール 1. PC 1 に HTTPS In/Out を許可する。

ルール 2. インターフェイスを入出する HTTPS 管理セッションおよび WebVPN HTTPS セッションを許可する。

ルール 3. それ以外の HTTPS トラフィックをすべて廃棄する（デフォルトのアクション）。

ルール 2 によって、ルール 3 が実施されなくなり、パブリック ネットワーク上のすべての PC が、VPN コンセントレータとの間で HTTPS を使用できます。

Release 4.1 では、特定の PC からの HTTPS トラフィックを禁止するためのルールを明示的に定義する必要があります。次の例では、ルール 2 を定義する必要があります。

ルール 1. PC 1 に HTTPS In/Out を許可する。

ルール 2. その他の PC（0.0.0.0/255.255.255.255）をどれも禁止する。

ルール 3. インターフェイスを入出する HTTPS 管理セッションおよび WebVPN HTTPS セッションを許可する。

ルール 4. それ以外の HTTPS トラフィックをすべて廃棄する（デフォルトのアクション）（CSCec72348）。

使用上の注意

ここでは、VPN 3000 シリーズ コンセントレータ ソフトウェア Release 4.1 をインストールして使用する前に知っておく必要のある、インターオペラビリティおよびその他の考慮事項を示します。

Cisco Security Agent によるポート フォワーディングのブロック

ポート フォワーディングを使用する PC システムに Cisco Security Agent（Version 4.0、build 119）がインストールされている場合、Cisco Security Agent はポート 80 の TCP 接続へのアクセスをブロックします。Cisco Security Agent を使用する場合は、特定のポートでの 127.0.0.1 へのアクセスを許可するポリシーを作成する必要があります（CSCec06741）。

TCP ポート フォワーディングによるクライアント PC の CPU 使用率の増大

ブロードバンドおよびイーサネットのスループット速度でファイルを転送するために TCP ポート フォワーディング機能を使用する場合、ダウンロードされた Java アプレットが、リモート PC のシステム処理能力を著しく消費する可能性があります（CSCeb38638）。

SDI または NT ドメイン認証を使用する場合のグループ ロックのディセーブル化

この機能は、内部認証または RADIUS 認証を使用する場合にのみサポートされます。この機能を正しく使用する方法については、次の URL を参照してください。
http://www.cisco.com/warp/public/471/altigagroup.html

パスワード期限によるLANのユーザ プロファイルの変更不可

（IPSec ユーザにのみ）パスワード期限を使用するには、VPN クライアントで [Start Before Logon] をイネーブルにする必要があります。また、DNS サーバおよびWINS サーバが適切に設定されていることを確認しなければならない場合もあります（CSCdv7325）。

ブラウザの互換性の問題

ここでは、特定の Web ブラウザに関して判明している動作および問題点について説明します。

- 現在、VPN 3000 コンセントレータで管理用に完全にサポートされているブラウザは、Netscape、Internet Explorer、および Mozilla です。
- 上記以外のブラウザを使用すると、許容不可能な動作が発生する可能性があります。たとえば、サポートされていないブラウザを使用して VPN 3000 コンセントレータの管理を試みると、いずれかのリンクをクリックした際にログイン画面に戻る場合があります（CSCdx87630）。
- VPN 3000 コンセントレータとの対話には、サポートされている Web ブラウザを使用してください。特に、ポート フォワーディング機能を使用する場合には、Opera 以外のブラウザを使用してください。
- ファイル共有を使用している場合、ファイルを開くか保存する動作をキャンセルすると、Internet Explorer 5.5 が終了します。Internet Explorer 5.5 では、ファイルを開くか保存するためにそのファイルをクリックすると、ブラウザが閉じられる場合があります。また、ファイルを開くか保存しているときに [Cancel] をクリックしても、ブラウザが閉じられる場合があります。

  Microsoft 社は Internet Explorer 5.5 に関するこの問題を確認しています。詳細については、次のリンクにある Microsoft Knowledge Base の記事を参照してください。

  http://support.microsoft.com/default.aspx?scid=kb;en-us;275290&Product=ie

  この問題を回避するには、ファイルを右クリックし、次に [Save Target As] をクリックします（CSCec51902）。

Internet Explorer によるポート フォワーディング起動時のセキュリティ警告の表示

Internet Explorer 6.0 からポート フォワーディング（アプリケーション アクセス）を起動するたびに、[Security Information] ウィンドウで次のメッセージが表示されます。

```
This page contains both secure and nonsecure items.
Do you want to display the nonsecure items?
```

このエラーは Netscape 7.1 では発生しません（CSCed25138）。

IMAPS プロキシによる複数のメール サーバ セッションの起動

IMAP クライアントの動作方式に起因した現象として、VPN コンセントレータおよびメール サーバの管理者は、同一の送信元またはクライアントから複数のセッションが起動されるのに気づく場合があります（たとえば、メールをチェックするときやフォルダを同期化するときに IMAP セッションが開かれる場合があります）。その結果、VPN コンセントレータのセッション テーブルに同じ送信元からの 2 つの IMAPS セッションがリストされたり、メール サーバ上で VPN コンセントレータの送信元 IP アドレスおよび同じメール ユーザの 2 つの IMAP セッションがリストされる場合があります（CSCec18358）。

[Group Strip] および [Strip Realm] 設定の変更

（IPSec ユーザの）グループ ルックアップ機能に、[Group Strip] というスイッチが追加されました。このスイッチは、ユーザ名を認証するときにユーザ名からグループを削除するかどうかを指定します。デフォルトでは、グループ名が削除されます。

従来のリリースでは、内部認証では常にグループ名が削除され、外部認証はグループ デリミタ「@」を使用する [Strip Realm] の設定に依存していました（! および # グループは削除されませんでした）。

グループ ルックアップ機能を外部ユーザ認証とともに使用し、*なおかつ*ユーザ認証が（アップグレード後に）失敗するようになった場合は、[Group Strip] および [Strip Realm] の設定を確認してください（CSCec20818）。

ネイティブ Kerberos 認証

VPN 3000 シリーズ コンセントレータは Release 4.0 から、Kerberos/Active ディレクトリへの認証をサポートするようになりました。これは Windows 2000 および Windows XP のデフォルトの認証メカニズムです。[Kerberos] は信頼されないネットワークに使用する認証プロトコルです。このプロトコルは 2 段階の認証で構成されています。第 1 レベルは Key Distribution Center（KDC; 鍵発行局）であり、第 2 レベルは各クライアント / サーバ間の認証です。

この機能を設定するには、Kerberos 認証サーバをグループ単位で追加するか、またはグローバル認証サーバ リストにサーバを追加し、サーバの IP アドレス、サーバ ポート、再試行回数などのパラメータを設定します。IPSec group タブに認証タイプとして [Kerberos] が含まれ、統計情報にも Kerberos 認証の統計が表示されます。

VPN コンセントレータを使用して、Kerberos サーバを実行している Linux または Unix サーバでユーザを認証するには、次の作業を行います。

ステップ 1 認証するユーザが使用できる鍵を確認します。次のコマンドを実行します。

kadmin.local -q "getprinc *username*"

ステップ 2 使用できる鍵の中に、[DES cbc mode with RSA-MD5, Version 5] があることを確認します。[DES cbc mode with RSA-MD5, Version 5] が表示されていない場合は、kdc.conf ファイルを編集し、supported_enctypes = 行の先頭に、des-cbc-md5 の選択項目を追加または移動します。次に例を示します。

```
[realms]
MYCOMPANY.COM = {
master_key_type = des-cbc-crc
supported_enctypes = des-cbc-md5:normal des-cbc-md5:norealm
des-cbc-md5:onlyrealm
```

ステップ 3 ファイルを保存します。そのあと、krb5kdc、kadmin、および krb524 サービスを再起動します。

a. [DES cbc mode with RSA-MD5] 鍵を作成するために、ユーザ パスワードを変更します。

kadmin.local -q "cpw -pw newpassword *username*"

これで、このユーザを Linux/Unix Kerberos 5 サーバで認証できるようになります（SCea20236）。

日本語版オペレーティング システムのサポート

日本語版 Windows オペレーティング システムでは、WebVPN は次の用途をサポートしません。

- 日本語を含んだ URL のアクセス
- ファイル名またはパスに日本語が含まれる CIFS ファイル アクセス

WebVPN は、Linux、Solaris、Mac OS の日本語版に対応していません。それ以外の VPN 3000 コンセントレータ Release 4.1 の機能は、4.0 から使用可能だった機能も含めて、日本語版システムで使用できます。

ファイル共有時のシェア名の最大文字数

ファイル共有を使用する場合、シェア名の長さは最大 12 文字です。12 文字より長いシェア名は、表示されません。これは CIFS プロトコルによる制約事項です（CSCed21075）。

Windows ME で Norton アンチウィルスを使用する場合の TCP ポート フォワーディングのブロック

TCP ポート フォワーディング（アプリケーション アクセス）は、Norton Antivirus をインストールしている Windows ME PC 上では使用できません。[TCP Port Forwarding] メニューをロードしようとすると、Norton Antivirus によって、フォワーディングされる TCP ポートがオープンできないか、または PC がダウンする場合があります。これは Norton Antivirus の問題です（CSCec18162）。

$ で終わるシェア名の非表示

ファイル共有を使用する場合、シェア名の最後にドル記号（$）が使用されていると、その共有フォルダは表示されません。この共有リソースは、ユーザによる閲覧も不可能です。これは正常な動作です。Microsoft 社によると、ドル記号で終わるシェア名（share$）は非表示シェアです。ユーザはこれらの非表示シェアを閲覧できません（CSCed09634）。

ファイル共有でのドメイン / ワークグループごとの最大サーバ表示数

ファイル共有では現在、ドメインまたはワークグループごとに 2520 のサーバしか表示されません。表示されないサーバについては、Network Path エントリ ボックスにサーバ名を入力することによって閲覧できます（CSCec73349）。

VPN 3000 シリーズ コンセントレータの判明している注意事項

注意事項では、予想外の動作または Cisco ソフトウェア リリースの不具合について説明します。ユーザの便宜を考慮して、Release 4.1 固有の判明している注意事項を最初にリストします。その後で、Release 4.1 より前に判明していた注意事項をリストします。各リストは識別番号順になっています。どちらのリストでも、実行できる対処方法を併記しています。対処方法が併記されていない場合、対処方法はありません。

（注） CCO のアカウントをお持ちの場合、Bug Navigator II を使用して、リリースおよび重大度を指定して注意事項を検索できます。CCO で Bug Navigator II を使用するには、Software & Support:Online Technical Support:Software Bug Toolkit の順に選択するか、または http://www.cisco.com/pcgi-bin/Support/Bugtool/launch_bugtool.pl にアクセスします。

Release 4.1 固有の判明している注意事項

Release 4.1 で発生した新しい問題は、次のとおりです。

- CSCeb21763

  ブラウザからWebVPN機能を使用してコンセントレータにログインした後、ブラウザの [Back] ボタンを使用すると、バナー ポップアップ ボックスが 2 回以上表示されます。通常、バナーはユーザがログインした直後に 1 回しか表示されません。

Netscape 7.x および Mozilla 1.x で [Back] および [Previous] ボタンを使用すると、ブラウザのキャッシュ設定やコンセントレータから送信されたページのプロパティとは無関係に、常にキャッシュからページが取得されます。その結果、[Back] ボタンをクリックして WebVPN ホーム ポータル サイトに戻ると、バナー ポップアップが再表示されます。

対処方法 :

ホーム ポータル サイトに戻るには、[Back] ボタンではなく、WebVPN コントロール バーの [Home] ボタンを使用してください。

- CSCeb38638

  非常に高いデータ転送速度で TCP ポート フォワーディング機能を使用すると、Java アプレットが CPU 利用率 50% 以上で動作する場合があります。クライアント PC の CPU が高速であるほど、CPU 利用率に対する Java の影響は少なくなります。

- CSCeb59310

  グループに定義されている WebVPN ACL に、不正な、または DNS で解決不可能な ACL エントリが大量に（10 より多く）含まれている場合、VPN 3000 コンセントレータがこれらの ACL エントリを解析しようと試みると、CPU サイクルがすべて消費されます。その結果、他のトンネルの確立や HTTP(s) 管理セッションが拒否されます。

  対処方法 :

  WebVPN ACL 定義に使用されている URL が有効であるかどうかを確認してください。

- CSCeb86147

  RC4-128 SSL 暗号化は、WebVPN 接続でサポート されていますが、CPU 利用率が非常に高いので WebVPN 用には推奨できません。暗号化には、DES-56 または 3DES-168 を使用することを推奨します。RC4-128 はソフトウェア ベースですが、これらの暗号化方式はハードウェア ベースです。

- CSCec03101

  [Monitoring Sessions] ページで [Group] ドロップダウン タブを選択しているときに、モニタリングの更新が行われると、メインのフレームが空白になり、左または上のフレームで別のリンクを選択しても、空白のままになります。

対処方法：

次の*いずれか*の操作を行います。

– ログアウト / ログイン

– 右のフレームを右クリックし、[Refresh] を選択する

この動作は IE 6.0 でのみ発生し、IE 5.0、Netscape 4.78、または Netscape 6.2 では観察されていません。

- CSCec09317

  NBNS の [Master Browser Server] オプションが機能しません。現在、名前の変換は WINS サーバを使用する場合のみ正常に機能します。

- CSCec20414

  Outlook Web Access を使用して新しいカレンダ オブジェクトに参加者を呼ぶとき、[invite attendees] ボタンを選択するとページがリセットされる場合があります。これは、ページが完全にロードされていないために発生します。ページが完全にロードされているかどうかを確認するには、カレンダ オブジェクトの [start time] および [end time] ドロップダウンに現在の日付および時刻が表示されているかどうかをチェックします。

- CSCec24244

  ファイル共有を使用し、ファイルをコピーするとき、コピーするファイルによって既存のファイルが上書きされる場合にも、確認を求めるプロンプトが表示されません。追加（コピー）するファイルと同名のファイルが存在しないことを確認する必要があります。

- CSCec28525

  WebVPN は一連のサイトを 1 つのフレームに収容します。WebVPN はベストエフォート式でサイトをフレームに収容するよう試みますが、一部のサイトはフレームに入った状態では正常に動作しません。このようなサイトは、フレームに入っていないか、またはサイト自身のフレームがトップ レベルに位置しています。このようなサイトの例に、www.cutimes.com があります。

- CSCec30364

  Admin | File Management テーブルで、「.grp」など、ある種の Windows 拡張子の付いたファイルに [View] オプションを選択しても、これらのファイルが表示されません。

  対処方法：

  該当するファイルのコピーを別のファイル名で作成し、名前を変更した新しいファイルを表示してください。

- CSCec34817

  VPN 3002 でユーザ認証がイネーブルに設定されている場合、HTTP でリダイレクトされるインターフェイス向けの Web ブラウザ セッションを、VPN 3002 ユーザ ログイン プロンプトにリダイレクトできません。

  VPN 3002 とともに自分自身を認証する PC 上の Web ブラウザに、VPN コンセントレータのプライベート IP アドレスを入力すると、ブラウザのドロップダウン リスト上の最初の IP アドレスに、プレフィクス [https://] が追加されます。[https] があると、VPN 3002 はブラウザをログイン プロンプトに切り替えることができません。

  対処方法 :

  VPN 3002 とともに認証を試みるブラウザのアドレス バーの [https] から「s」を削除します。最終的には [https] を使用して接続が確立されますが、上記のステップで「s」を削除することによって、VPN 3002 がログイン プロンプトを表示できないという障害を回避することができます。

- CSCec36405

  WebVPN エンド ユーザの Logout 画面で、リンク [Click here to close the browser window] が、Mozilla 1.4 および Netscape 7.x では動作しません。

- CSCec37257

  Internet Explorer でファイル共有を使用する場合、ユーザが同時に実行できるダウンロードは 2 つだけです。2 つのダウンロードが進行しているときは、アイコンまたはアクション ボタンをクリックしても外見上、応答しません。どちらか 1 つのダウンロードが完了すれば、WebVPN ファイル共有は再び応答するようになります。

- CSCec38676

  WebVPN は、このリリースでは有効期限付きの RADIUS に対応しません。

- CSCec46657

  WebVPN 上で Outlook Web Access/WebDAV を使用し [Change Password] をクリックすると、接続エラーになります。これは MS Exchange Server のセキュリティ上の欠陥であると考えられ、MS は現在その使用をサポートしていません。

  対処方法 :

  Exchange Server に直接接続している状態でパスワードを変更してください。

- CSCec47541

  リンク（たとえば、電子メール メッセージに含まれているリンクなど）をクリックすると、そのリンクがアプリケーション アクセス Java アプレットを実行するブラウザ ウィンドウを使用していて、アプリケーション アクセスが無効になる場合があります。このようなウィンドウへのリダイレクトの結果、WebVPN ポート フォワーディングが終了します。

  Microsoft Internet Explorer では、この問題を防止できます。Netscape および Mozilla ブラウザにはこの問題を防止する手段は提供されていません。

- CSCec64525

  Domino Web Access を使用する場合、既存の電子メール メッセージを転送しようとすると、ユーザは WebVPN セッションからログアウトされます。

- CSCec65416

  VPN 3000 コンセントレータは、WebDAV の問題により、Microsoft Outlook Exchange 2003 の Outlook Web Access をサポートしていません。

- CSCec75742

  ファイル共有を使用する場合、名前に 2 つのドットを含むファイルをダウンロードすると、ファイル名が変更されます。たとえば、ファイル「filename.v1.zip」は、ダウンロード後は「filename[1].v1.zip」という名前になります。

  対処方法 :

  [Save As] ダイアログ ボックスを使用して手動でファイル名を変更してください。

- CSCec75765

  Release 4.1 をロードしたあと、次のエラー イベントが生成される場合があります。

  – SET validation Bad Value Error on alSessionLimit.0.

  – SERVE Bad Value Error.

  これらのイベントは無害であり、コンフィギュレーションを保存している場合、これらのメッセージは次回の再起動時からは表示されません。

- CSCec77427

  Mozilla ブラウザを使用する場合、WebVPN ユーザとしてログアウトしたあとに、ブラウザ ウィンドウを閉じるためのリンクが機能しません。

  対処方法 :

  ブラウザ ウィンドウを手動で閉じてください。

- CSCec78536

  WebVPN は、http 要求を生成する Java アプレットをサポートしません。この理由から、たとえば CiscoSecure ACS アプリケーションにはログインできません。

- CSCec82791

  ファイル共有で、[Network Path] エントリ ボックスに入力した共有フォルダが存在しない場合、認証を要求するプロンプトが表示されます。有効な証明書があっても、認証は成功しません。

  対処方法 :

  認証をキャンセルするか、または [Home] アイコンをクリックしてください。

- CSCed05714

  一部のサイトの HTTP 応答で、JavaScript コンテンツが通常の HTTP データとして不正に識別されている場合があります。そのため WebVPN をこれらのサイトと相互運用すると、WebVPN が誤動作します。

  このようなサイトの例に、www.pwc.com があります。[Site Navigation] ドロップダウン メニューからいずれかのオプションを選択すると Javascript エラーが発生し、WebVPN セッションが終了します。

- CSCed05959

  Web ページが生成する応答で、1 対の HTML タグの間にあるコンテンツが 9 キロバイトを超えている場合、WebVPN はその応答を廃棄します。その結果、Web ページが正常に表示されない場合があります。

- CSCec07602

  VPN 3000コンセントレータでPIXファイアウォールへのanswer-onlyモードの LAN 間接続セッションを実行するとき、LAN 間接続設定ページでネットワークを定義する代わりにネットワーク リストを使用している場合、エラーになる可能性があります。

- CSCed12191

  ファイル共有を使用する場合、ワークグループの閲覧時にメンバー サーバが表示されない場合があります。これは、サーバからの応答が遅いことから発生する障害です。

  対処方法 :

  サーバに到達するには、[Enter Network Path] エントリ ボックスにサーバ名を入力してください。

- CSCed14579

  シェア内のフォルダへの絶対パスを入力するとき、フォルダ名の大文字 / 小文字の区別が正しいことを確認してください。そうでないと、フォルダの内容を表示できません。たとえば、シェア内の共有フォルダがサブフォルダである場合、[Network Path] エントリ フィールドに、このフォルダへの絶対パスを次のように入力する必要があります。
  \\server\share\SharedFolder

- CSCed22336

  Netscape 4.79 でファイル共有を使用する場合、テキスト ファイルのダウンロードが失敗します。テキスト ファイルを表示することはできますが、ファイルを右クリックして [Save Target As...] を選択しても、動作が完了することはありません。

  対処方法 :

  この問題を回避するには、ダウンロードが正常に処理される Netscape の最新版にアップグレードしてください。

  現在の Netscape バージョンのままにしておく必要がある場合は、テキスト ファイルを表示したあと、[File] メニューから [Edit] を選択し、[Select All] をクリックして、メモ帳にコピー ペーストします。

- CSCed23549

  Release 3.6.7 ソフトウェアで稼働する VPN 3030 コンセントレータで、メモリ不良が発生しています。ログに次のメッセージが含まれます。

  ```
  SEV=3 SYSTEM/10 RPT=47 Freeing free memory block.
  Ptr=034ec494, CPC1=000218e8, CPC2=00025d2c, TID=00360000

  SEV=4 SYSTEM/0 RPT=185 0000:FACEDBAD 030CF9C8 031C4E40
  00010000
  ```

  このようなエラー メッセージが表示されても、VPN 3030 コンセントレータがダウンするわけではないので、crashdump ファイルはありません。

- CSCed34297

  ファイル共有を使用する場合、VPN 3005 には 64 MB のメモリが必要です。メモリがこれより少ないと、ネットワークを閲覧するときに使用可能なドメイン / ワークグループおよびサーバがすべて正常に表示されない場合があります。また、オブジェクト数が 1,000 を超える場合は、フォルダ数およびファイル数として信頼できる数字が表示されません。

- CSCed38056

  WebVPN フレームの下に、次の行が表示されます。

  Via:1.1 VPN3000 Cache-Control:no-cache Transfer-Encoding:chunked 58F

  一部のページで、WebVPN が CRLF または LF のどちらかで終了するヘッダーを必要としているにもかかわらず、これらが混在したヘッダーが返される場合があります。その結果、ページにヘッダー フィールドが不要であっても、ヘッダー フィールドが表示されます。

- CSCed45861

  Netscape 4.7 でファイル共有を使用する場合、シェア名にスペースが含まれていると、そのシェアにはアクセスできません。Netscape は共有リソースを開くことができず、このエラーが発生したという表示もありません。Netscape の最新版では、この問題は発生しません。

  対処方法 :

  Netscape 7.1 以上にアップグレードしてください。

- CSCed48738

  大量の cookie 転送が行われるサイトがあります。これらのサイトをログアウトし、再びログインすると、サイトが正常に動作しなくなる場合があります。このような問題のあるサイトに、401k.com、quicken.com、hotmail.com があります。その他にも cookie を大量に使用するサイトで、この問題が発生します。

  対処方法 :

  サイトを広範囲にわたってナビゲートしたあと、ログアウトして再びログインする場合は、WebVPN からログアウトして、再び WebVPN にログインしてください。

- CSCed49449

  Netscape で WebVPN を使用する場合、ブラウザを閉じて再び開かないと、WebVPN セッションを再確立できません。

  WebVPN は、7.1 より前の Netscape バージョンをサポートしていません。ユーザが不正な方法（たとえば、別の Web サイトに直接切り替えるなど）によって WebVPN セッションをログアウトした場合、前のセッションからの cookie が削除されず、そのために新しい WebVPN セッションの確立が阻止されます。

対処方法 :

- WebVPN セッションからのログアウトは、常に正しい方法で行ってください。
- WebVPNアドレスを扱うすべてのcookieを削除するか、またはブラウザを再起動してください。
- Netscape 7.1 にアップグレードしてください。

- CSCed50600

  Release 4.1 では、WRITE 動作（Savelog + Config）用に 1 MB のフラッシュの空きが必要です。今後のリリースではこの動作を最適化する予定ですが、その方法はフラッシュのスペースを確保するのではなく、WRITE タスクをグレースフルに終了させてHTTP(s) タスクを続行できるようにするという方法です。

- CSCed52118

  同じグループ ログインに複数のユーザが存在する場合、Administrator sessions | sessions detail をチェックすると、各グループの最初のセッションにしか、対応づけられた ACL が表示されません。

- CSCed52950

  [Fleet Bank Home Link] タブごとに、個別のウィンドウが起動されます。

- CSCed53867

  WebVPN セッション中に、PDF 文書のツールバーの [Acrobat] アイコンをクリックしたとき、「続行するとセッションがログアウトされる」という警告メッセージが表示されます。

- CSCed55624

  WebVPN セッション中に、ブラウザの cookie である webvpn（すべて小文字）を削除すると、**WebVPN** セッションがログアウトされます。

（注） cookie 名は「webvpn」であり、「WebVPN」ではありません。

- CSCed56415

  Netscape 7.1 を使用する場合、一部のサイト（例：potterybarn.com）でブラウザがハングアップします。この問題が発生した場合は、ブラウザをいったん閉じて再び開き、WebVPN セッションを再確立してください。

- CSCed58734

  SSH ホスト キーを再生成するとき、VPN 3000 コンセントレータをリセットして SSH 管理を再開しなければならない場合があります。

- CSCed58753

  VPN 3000 への WebVPN 接続を維持しながら、もう 1 つの VPN 3000 のコンフィギュレーションを保存しようとすると、javascript エラーになります。

- CSCed62309

  Mozilla ブラウザ バージョン 1.6 では、WebVPN でアプリケーション アクセスを実行できません。Mozilla ブラウザ バージョン 1.5 および 1.4 では、アプリケーション アクセスを正常に起動して相互運用することができます。

- CSCed72955

  2003 年 3 月から 2003 年 12 月までの間に製造された VPN 3005 コンセントレータは、製造工程の誤りにより、フラッシュ ファイル システムが壊れている可能性があります。該当するシリアル番号は、CAM0708xxxx ～ CAM0750xxxx です。

  症状としては、証明書の生成および保存でエラーが発生したり、ファイル システムで inconsistent volume エラーが発生することがあります。

旧リリースの判明している注意事項

以下の問題点は、Release 4.1 より前のリリースから判明しており、VPN 3000 シリーズ コンセントレータ Release4.1 で解決されていません。

- CSCds44095

  L2TP over IPSec 接続は、NAT デバイスを経由すると失敗します。接続を確立するとき、VPN クライアントと VPN 3000 コンセントレータは IP アドレスを交換します。クライアントが VPN 3000 コンセントレータのものと信じるアドレス（実際には NAT で変換されたアドレス）を送信すると、VPN 3000 コンセントレータは接続を解除します。

  原因は、インターフェイスに割り当てられているアドレスが、クライアントから着信するアドレスと一致しないことです。クライアント側にも同じ問題があります。この問題は、Windows 2000 MS クライアントが UDP カプセル化をサポートするようになるまで解決されません。

- CSCdt08303

  IOS または PIX を使用して LAN 間接続を設定する場合、キープアライブ設定を一致させること（両方とも「ON」、または両方とも「OFF」にすること）が重要です。キープアライブ設定が、VPN 3000 では OFF、IOS デバイスでは ON である場合、データを使用してトンネルが確立されます。

  VPN 3000 コンセントレータでキープアライブが OFF に設定されている場合、コンセントレータは IOS スタイルのキープアライブに応答しないので、IOS によってトンネルが切断されます。

- CSCdw36613

  Windows NT バージョン 4.0 オペレーティング システムで、VPN クライアントを接続し、ポリシーを変更して再配置し、接続をアップにしたときに、Zone Labs Integrity Agent が正常に更新されない場合があります。具体的には、[Policy] の [Firewall Security Rules] で [Block Internet Servers] を選択し、その新しいポリシーを [Deploy] した場合に、Windows NT バージョン 4.0 で稼働している PC が更新済みのポリシーを受信しても、そのポリシーの[Block Internet Servers]設定が有効にならない場合があります。

  対処方法 :

  オペレーティング システムを再起動してください。

- CSCdx47596

  Windows XP 搭載 PC は Microsoft 固有の制約により、大量の Classless Static Routes（CSR; クラスレス スタティック ルート）を受信できません。VPN 3000 コンセントレータは、DHCP INFORM メッセージ応答に挿入される CSR の数を設定によって制限することができます。

  VPN 3000 コンセントレータは、クラスに応じてルート数を 28 ～ 42 に制限します。

- CSCdx89348

  コンセントレータはVPNクライアントの接続時に次のイベントを表示する場合があります。これらのイベントは、クライアントのパケットを不正に変更したLinksys Cable/DSLルータの後ろ側にクライアントが存在することが原因であり、そのため VPN コンセントレータがパケットを受信するときにパケットの認証が失敗します。LZS 圧縮を使用した場合には、この問題がより顕著になります。

イベント：

131500 06/20/2002 17:08:34.300 SEV=4 IPSEC/4 RPT=4632

IPSec ESP Tunnel Inb:Packet authentication failed, username:gray, SPI:

4e01db67, Seq Num:0000850f.Dump of failed hash follows.

この問題については Linksys に通知済みです。

対処方法：

現時点では対処方法はありませんが、コンセントレータ上で LZS 圧縮をディセーブルにすると、イベントの発生率が減ります。コンセントレータ上で LZS 圧縮をディセーブルにするには、グループ設定の IPSec タブで [IPComp] を [none] に設定します。

- CSCdy26161

  Windows 98、Windows ME、および Windows NT 対応の Microsoft L2TP/IPSec クライアントが、VPN コンセントレータにデジタル証明書を使用して接続しません。

  対処方法：

  事前共有鍵を使用してください。

- CSCdz24882

  Microsoft Internet Explorer バージョン 5.0 を使用する場合、Monitoring | System Status | Memory Status | Detailed Memory Report の順に選択しても詳細なメモリ レポートを作成できません。file memory.txt が作成*されません*。このファイルがすでに存在していれば、レポートが作成されます。最初に CLI インターフェイスを使用して詳細レポートを作成することによって、このファイルを作成*できます*。Internet Explorer バージョン 5.5 および Netscape では、この問題はありません。

- CSCdz83332

  [html-management] ページの [interface] セクションでタブからタブへ移動する場合に、操作が失敗することがあります。

  その場合には、[interface summary] ページに戻り、そこから目的とするインターフェイスに再び移動してください。これにより、正常な状態に戻ります。

- CSCdz87108

  LDAP 認証の失敗理由は、この種のエラー コードの LDAP サーバでの実装方法によって異なります。RFC 1777-LDAP では、LDAP サーバがエラー コードを戻さない場合もあるとしています。したがって、そのような場合、VPN 3000 での障害理由は [Invalid response received from server] と表示されます。

  LDAP サーバが特定のエラー診断（たとえば、noSuchAttribute など）を*戻した*場合には、VPN 3000 では適切なストリングが障害理由として表示されます。

Release 4.1.2 で解決された注意事項

以下の問題は、Release 4.1.2 で解決されています。

- CSCeb47529

  VPN 3000 コンセントレータに、同じメジャー ネットのルートがすでに存在する場合、より固有性の高いルートを、その VPN 3000 コンセントレータに入力することはできません。

- CSCed42494

  Linksys デバイスの後ろ側にある（同じ DHCP プールを使用する）2 台の PIX501（EZ VPN クライアント）が、IKE 鍵の更新中に接続解除されます。この場合、各 PIX は public-to-public IPSec SA をアップにしようとします（その結果、もう一方の PIX を切断します）。PIX は、新しい IKE SA 上に新しい IPSec SA を確立します。このアップダウンにより、IKE が削除されます。

（注） 旧 IKE SA では、削除メッセージを受信するか、SA が期限切れになって新しい SA をアクティブ化するまで、新しい IKE SA にトンネルを転送しません。

- CSCed48380

  VPN 3000 コンセントレータのイベントである IKE/124 が、R_U_THERE 障害と誤解されるおそれがあります。VPN コンセントレータは、DPD シーケンス番号には前のシーケンス番号よりも大きい数を期待します。最初のシーケンス番号は、ランダムに生成された番号とみなされます。

  モデル 831 ハードウェア クライアントと相互運用する場合、モデル 831 ハードウェア クライアントが VPN 3000 コンセントレータへの接続を試みると、次のイベントが発生しました。

  ```
  588 01/19/2004 20:17:41.750 SEV=5 IKE/124 RPT=98 address
  Group [group]
  Received DPD sequence number 0x0 in R_U_THERE, expected 0x0
  ```

  モデル 831 ハードウェア クライアントは最初のシーケンス番号として乱数 0 を繰り返し送信し、VPN 3000 コンセントレータは正常に接続をリジェクトしていましたが、このイベント メッセージは誤解を招くおそれがあります。次のイベント メッセージが適切です。

  ```
  Received unexpected DPD sequence number %d in R_U_THERE.
  Next expected sequence number should be greater than %d.
  ```

- CSCed60514

  最大接続タイムアウトのユーザ設定（[general] タブ）を適用して保存した後に、この設定が保存されていません。同じユーザを編集した場合、前に行った設定が消去され、デフォルト（グループ設定から最大接続タイムアウトを継承する）に戻ります。

- CSCed70850

  VPN 3000 コンセントレータへの SSH リモート管理接続は、1 回しか実行できません。そのあとで SSH を使用して接続することは不可能です。この障害は、[exit] コマンドを使用して SSH セッションをクリーンに終了した場合に発生します。SSH セッションをタイムアウトさせた場合や、http 管理によって終了させた場合には、この障害は発生しません。また、SSH 統計情報には、VPN 3000 コンセントレータがダウンしたと表示されます。

Release 4.1.1 で解決された注意事項

以下の問題は、Release 4.1.1 で解決されています。

- CSCed53846

  4.0.4.B にアップグレードした後、LCP 認証方式が CHAP である場合、VPN 3002 ハードウェア クライアントの PPPoE クライアントが接続できなくなります。

- CSCed56906

  WebVPN ユーザが VPN コンセントレータを介してプライベート ネットワーク サーバに大量の TCP データを送信するとき、ターゲット サーバがトラフィックを厳密にフロー制御している場合、そのデータによって VPN コンセントレータのデータ バッファ リソースがすべて使用される可能性があります。その場合、コンセントレータは新しい WebVPN または HTTP/HTTPS 管理セッションを受け入れなくなります。既存のセッションは低速化するか、またはデータの送受信を停止します。

- CSCed59586

  Release 4.1 にアップグレードされた VPN 3002 ハードウェア クライアントは、外部インターフェイス上の HTTPS 経由で管理できなくなります。

- CSCed60615

  VPN 3000 Release 4.0.x コードでは、RADIUS サーバとして Funk を使用すると、有効期限付き RADIUS でエラーが発生します。Release 3.0.x コードには、この問題はありません。また、Funk RADIUS は MSCHAPv2 を正常にサポートします。

  対処方法 :

  VPN 3000 Release 3.0.x コードを使用してください。または RADIUS（または有効期限付き RADIUS）認証を使用しないでください。

- CSCed60860

  Release 4.0.4.B を使用する VPN 3000 は、VPN 3000 コンセントレータの再起動後、実 MAC アドレスおよび独自の IP アドレス（VRRP アドレスでもある）を使用して gratuitous ARP を送信します。

  対処方法 :

  セカンダリ VPN 3000 に接続できない場合は、2 台の VPN 3000 間でのスパニングツリーをイネーブルにするスイッチを設定して、不正な書き換えを防止してください。

- CSCed63615

  Release 4.1 にアップグレードされた VPN 3002 ハードウェア クライアントでは、PPPoE を使用するとエラーが発生します。この問題は PPPoE に限られます。

- CSCed66779

  Cisco VPN 3000 シリーズ コンセントレータを Release 4.1 にアップグレードしたあと、非常に稀に、ユーザがアクティブ コンフィギュレーションを保存できない場合があります。

  次のエラー メッセージが表示されます。

  ```
  Could not write to file, error 20
  CERTS Error 0x2003
  ```

Release 4.1 で解決された注意事項

以下の問題は、Release 4.1 で解決されています。

- CSCdy27564

  VPN 3000 コンセントレータで最初の IPSec/Phase 2 の鍵の更新が行われるまで、ネットワーク拡張モードで PIX-501 に割り当てられた IP アドレスが 0.0.0.0 と表示されます。Phase 2 の鍵の更新が完了すると、割り当てられた IP アドレスは PIX-501 のプライベート インターフェイスのネットワーク アドレスに正しく設定されます。

- CSCea29828

  HTTP ソフトウェア アップデートが失敗し、[Software Update Error] が表示されることがあります。もう一度アップデートを試みても、イメージが更新されません。

- CSCea52820

  HTML の Monitoring | System Status | Memory Details ページの Help ページのテキストが、[Memory Detail Report] を不正に参照しています。このページのラベルは、[Detailed Memory Report] です。

- CSCea52936

  SEP-E の Monitoring | System Status | SEP インライン SEP ページのヘルプが不完全です。それ以外のセクションでは、SEP-E を参照しています。

[Encryption and Decryption] バレットに [AES (SEP-E only)] を追加する必要があります。

この画面は、VPN コンセントレータの次のハードウェア ベースの暗号化機能を実行する SEP または SEP-E モジュールのステータスおよび統計情報を表示します。

- 乱数生成
- 認証のためのハッシュ変換（MD5 および SHA-1）
- 暗号化および復号化（DES および 3DES）

この画面には、最後にシステムが起動またはリセットされてからの累積的なデータが表示されます。

- CSCeb27069

  Release 4.0.1 で、RSA SecurID を使用してある種の PIN を否定しても、正常に機能しません（たとえば、英数字の PIN の否定、PIN の長さに基づくアクセスの否定など）。

- CSCeb38654

  VPN 3002-8E モデルで、パブリック インターフェイスのリンクが起動時にダウンすると、装置が連続的に再起動されます。

- CSCeb48289

  VPN 3000 コンセントレータで、不正な PPP IP 制御メッセージに起因するエラーが発生します。

- CSCeb65325

  VPN 3000 コンセントレータが、認証サーバに空白のユーザ名 / パスワードを送信します。

- CSCec02285

  VPN 3002 の CLI で、Administration | Access Rights | Administrators メニューに、モニタ ユーザではなく ISP ユーザが表示されます。ただし、GUI ではモニタ ユーザが表示されます。モニタ アカウントを使用して GUI にログオンしようとすると失敗します。ISP アカウントを使用して GUI にログオンすると成功しますが、その場合にもクイック コンフィギュレーションを使用して設定を変更することは可能です。VPN 3002 でこの問題があれば、この問題は常に発生します。VPN 3002 にこの問題がなければ、どのバージョンのコードを使用しても、この問題が発生することはありません。

- CSCec11767

  Web（または XML）インターフェイスから認証サーバのテストを実行するたびに、解放されないメモリが少しずつあります。その結果、最終的に VPN コンセントレータがダウンする可能性があります。

- CSCec16876

  VPN3k が 2 つ以上のリモート LAN へのルートを自動的に追加しません。リモート LAN ごとにスタティック ルートを VPN 3000 コンセントレータに追加する必要があります。

- CSCec61306

  3DES/SHA に対する Kerberos サポートが機能しません。

- CSCec66975

  VPN 3000 コンセントレータの FastEthernet インターフェイスの ifType（1.3.6.1.2.1.2.2.1.3）が 7 と報告されます（iso88023Csmacd）。IANA によると、ifType 7 は RFC-draft-ietf-hubmib-etherif-mib-v3 で使用しないように指示されています。代わりに ifType 6（ethernetCsmacd）を使用してください。

  （ianaiftype-mib および RFC 2665 を参照）：

  http://www.iana.org/assignments/ianaiftype-mib

  http://www.ietf.org/rfc/rfc2665.txt?number=2665

  不正な ifType を使用すると、一部の NMS システムで混乱を生じます。これらのシステムはイーサネット インターフェイスにはifType=6を想定するためです。

- CSCec73218

  一部のケーブル モデムは、ブロードバンド信号が消失した場合に、DHCP 経由で IP アドレス 192.168.1.11 を発行します。その場合、VPN 3002 がこのアドレスを受け入れると、VPN 3002 はその 192 アドレスを IKE ネゴシエーションで使用します。その結果、トンネルはトラフィックを送受信できなくなります。中央サイトのコンセントレータからは正常に機能しているように見えても、RX バイトや private-to-private SA のないトンネルになります。

- CSCec77145

  RSA/Ace 5.0.3 Agent API を使用する Cisco VPN コンセントレータの実装が、レルム間の認証で正常に機能しません。ACE/Server は、エージェントにダウングレード要求を送信します。この要求をエージェントは、v5 ヘッダーのある v2 認証要求を生成することと解釈します。Cisco VPN コンセントレータは、実際にダウングレードし、完全な v2 要求を送信します。ACE/Server はこれをプライマリ / セカンダリとして動作する必要のある v2 エージェントと解釈するので、この要求によりエラーが発生します。

- CSCed03366

  RADIUS 経由での SDI サーバへのユーザ認証に使用する新しい pin モードが正常に動作しません。この問題は、Release 4.0.3.REL から発生しました。

- CSCed09411

  VPN 3000 コンセントレータは、メモリ統計情報の表示中にダウンする場合があります。

- CSCed09496

  VPN 3000 コンセントレータは、分割トンネリングがイネーブルに設定された NEM PIX 501 接続を受け入れます。VPN コンセントレータはしばらくすると高い CPU 利用率を示しますが、最終的には dead-peer-detection（dpd）損失によって接続を廃棄します。

  PIX NEM 接続はデフォルトの dpd インターバルが短いために、他の接続よりも頻繁にこの問題に影響されます。その他の接続も稀に影響されることがあります。

- CSCed18995

  デジタル証明書を使用する場合、メイン モードの IKE 鍵の更新が行われるたびに、64 バイトのメモリ ブロックが解放されません。

- CSCed34928

  HTML からの Filter Rule Copy で、古いルールから新しいルールにネットワーク リストがコピーされません。

- CSCed40267

  ネットワーク リストおよびDHCP インターセプトがイネーブルに設定された L2TP または PPTP クライアントからの DHCP Inform メッセージを処理するとき、解放されないメモリ ブロックのために VPN 3000 コンセントレータが最終的にダウンします。解放されないブロック サイズは、ネットワーク リストのサイズによって変化します。

マニュアルの更新

Cisco VPN 3000シリーズ コンセントレータのマニュアル セットは、このリリース用に改訂されており、Cisco Connection Online（CCO）および www.cisco.com からオンラインで入手できます。ここでは、マニュアルの発行後に行われたマニュアルの変更および訂正について説明します。

マニュアルの変更点

以下のマニュアルについては、次に説明する製品変更を反映して変更が必要です。

- 『*VPN 3000 Series Concentrator Reference Volume I: Configuration*』
- 『*VPN 3000 Series Concentrator Reference Volume II: Administration and Monitoring*』

（注） VPN ハードウェア クライアントのマニュアルは、このリリースでは更新されていません。

VPN 3000 コンセントレータ マニュアルの更新

リリース ノートに加えて、次のマニュアルが Release 4.1 に対応するように更新されています。

- 『*VPN 3000 Series Concentrator Reference Volume I: Configuration*』
- 『*VPN 3000 Series Concentrator Reference Volume II: Administration and Management*』
- 『*VPN 3000 Series Concentrator Getting Started*』
- オンライン ヘルプ

関連資料

- 『*VPN Client User Guide for Windows*』
- 『*VPN Client Administrator Guide*』
- 『*VPN 3002 Hardware Client Getting Started*』
- 『*VPN 3002 Hardware Client Reference*』
- 『*VPN 3002 Hardware Client Quick Start Card*』

サービスおよびサポート

リセラーから購入した製品のサービスおよびサポートについては、リセラーにお問い合わせください。製品に添付されている『*Cisco Information Packet*』の「Service and Support」に記載された各種のサービスおよびサポート プログラムをご利用いただけます。

（注） リセラーから製品を購入された場合は、CCO にゲストとしてアクセスできます。CCO は、シスコの主要なリアルタイム サポート チャネルです。CCO サービスへの直接アクセスも含む各種プログラムについては、リセラーにお問い合わせください。

シスコシステムズから直接購入した製品のサービスおよびサポートについては、CCO をご利用ください。

マニュアルの入手方法

シスコの製品マニュアル、テクニカル サポート、およびその他のリソースは、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

WWW上の次のURLから、シスコ製品の最新資料を入手することができます。

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

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

http://www.cisco.com/jp

シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

シスコ製品のマニュアルおよびその他の資料は、製品に付属の Cisco Documentation CD-ROM パッケージでご利用いただけます。Documentation CD-ROM は定期的に更新されるので、印刷資料よりも新しい情報が得られます。この CD-ROM パッケージは、単独、年間または 3 カ月契約で入手することができます。

Cisco.com 登録ユーザの場合、Cisco Ordering ツールから Documentation CD-ROM（Customer Order Number DOC-CONDOCCD=）を単独で発注できます。次の URL にアクセスしてください。

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

また、どなたでも、オンラインの Subscription Store から毎月または 3 カ月ごとの購読契約で発注できます。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace

マニュアルの発注方法

マニュアルの発注方法については、次の URL にアクセスしてください。

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

シスコ製品のマニュアルは、次の方法でご発注いただけます。

- Cisco.com（Cisco Direct Customers）に登録されている場合、Networking Products MarketPlace からシスコ製品のマニュアルを発注できます。次の URL にアクセスしてください。

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Cisco.com に登録されていない場合、製品を購入された代理店へお問い合わせください。

テクニカル サポート

シスコシステムズでは、あらゆる技術上の支援のための窓口として、TAC Web サイトを含む Cisco.com を運営しています。お客様およびパートナーは TAC Web サイトからマニュアル、トラブルシューティングに関するヒント、およびコンフィギュレーション例を入手できます。Cisco.com にご登録済みのお客様は、各種ツール、ユーティリティなど、TAC Web サイトで提供するすべてのテクニカル サポート リソースをご利用いただけます。Cisco.com へのご登録については、製品を購入された代理店へお問い合わせください。

Cisco.com

Cisco.com は、いつでもどこからでも、シスコシステムズの情報、ネットワーキング ソリューション、サービス、プログラム、およびリソースにアクセスできる対話形式のネットワーク サービスです。

- Cisco.com は、広範囲の機能やサービスを通してお客様に次のような利点を提供します。
- 業務の円滑化と生産性の向上
- オンライン サポートによる技術上の問題の解決
- ソフトウェア パッケージのダウンロードおよびテスト
- シスコのトレーニング資料および製品の発注
- スキル査定、トレーニング、認定プログラムへのオンライン登録

また、Cisco.com に登録することにより、各ユーザに合った情報やサービスをご利用いただくことができます。Cisco.com には、次の URL からアクセスしてください。

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

TAC

シスコの製品、テクノロジー、またはソリューションについて技術的な支援が必要な場合には、TAC をご利用いただくことができます。2 種類のサポートを提供しています。TAC Web サイトと TAC Escalation Center です。問題のプライオリティおよびサービス契約の内容に応じて、適切な TAC サービスを選択してください。

テクニカル サポートへの問い合わせは、問題の緊急性に応じて分類されます。

- プライオリティ レベル 4（P4）—シスコ製品の機能、インストレーション、基本的なコンフィギュレーションについて、情報または支援が必要で、業務への影響がほとんどまたは全くない場合。
- プライオリティ レベル 3（P3）—ネットワークのパフォーマンスが低下しているが、ほとんどの業務運用が機能している場合。十分に運用できるレベルまで、通常の業務時間内にサービスの復旧を行います。
- プライオリティ レベル 2（P2）—ネットワークのパフォーマンスが著しく低下、またはシスコ製品のパフォーマンス低下により業務に重大な影響がある場合。通常の業務時間内にフルタイムで問題の解決にあたります。
- プライオリティ レベル 1（P1）—ネットワークがダウンし、業務に致命的な損害が発生する場合。24 時間体制であらゆる手段を使用して問題の解決にあたります。

TAC Web サイト

TAC Web サイトでは、オンラインで資料やツールを利用して、トラブルシューティングやシスコ製品およびテクノロジーに関する技術上の問題の解決に役立てることができます。Technical Support Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/techsupport

シスコシステムズとサービス契約を結んでいるお客様、パートナー、リセラーは、TAC Web サイトのすべてのテクニカル サポート リソースをご利用いただけます。Cisco TAC Web サイトの一部のサービスには、Cisco.com のログイン ID とパスワードが必要です。サービス契約が有効で、ログイン ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

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

Cisco.com 登録ユーザは、TAC Web サイトで技術上の問題を解決できなかった場合、次の URL から TAC Case Open ツールのオンライン サービスを利用することができます。

http://www.cisco.com/techsupport

[Open a case（service request）] を選択し、表示される指示に従ってください。

インターネットを利用する場合、P3 および P4 の問題については、状況を十分に説明し必要なファイルを添付できるよう、TAC Web サイトで Case Open ツールを利用することをお勧めします。

Japan TAC Web サイト

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

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

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

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

TAC Escalation Center

TAC Escalation Center では、P1 および P2 レベルの問題に対応しています。このレベルに分類されるのは、ネットワークの機能が著しく低下し、業務の運用に重大な影響がある場合です。TAC Escalation Center にお問い合わせいただいた P1 または P2 の問題には、TAC エンジニアが対応します。

TAC フリーダイヤルの国別電話番号は、次の URL を参照してください。

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

ご連絡に先立って、お客様が契約しているシスコ サポート サービスがどのレベルの契約となっているか（たとえば、SMARTnet、SMARTnet Onsite、または Network Supported Accounts [NSA; ネットワーク サポート アカウント] など）、お客様のネットワーク管理部門にご確認ください。また、お客様のサービス契約番号およびご使用の製品のシリアル番号をお手元にご用意ください。

その他の資料および情報の入手方法

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

- 『*Cisco Product Catalog*』には、シスコシステムズが提供するネットワーキング製品のほか、発注方法やカスタマー サポート サービスについての情報が記載されています。『*Cisco Product Catalog*』には、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press では、ネットワーク関連の出版物を幅広く発行しています。初心者から上級者まで、さまざまな読者向けの出版物があります。『*Internetworking Terms and Acronyms Dictionary*』、『*Internetworking Technology Handbook*』、『*Internetworking Troubleshooting Guide*』、『*Internetworking Design Guide*』などです。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』は、シスコシステムズが発行する季刊誌で、業界の専門家向けにネットワーク分野の最新動向、テクノロジーの進展、およびシスコの製品やソリューションに関する情報を提供し、ネットワークへの投資を最大限に活用するのに役立ちます。ネットワークの配置やトラブルシューティングのヒント、設定例、お客様の事例研究、チュートリアル、教育や認定に関する情報、および多数の詳細なオンライン リソースを紹介しています。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/go/packet

- 『*iQ Magazine*』は、シスコシステムズが発行する隔月刊誌で、ビジネスリーダーや経営幹部向けにネットワーク業界の最新情報を提供します。『*iQ Magazine*』には、次の URL からアクセスしてください。

  http://www.cisco.com/go/iqmagazine

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

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- トレーニング — シスコシステムズはネットワーク関連のトレーニングを世界各地で実施しています。トレーニングの最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/le31/learning_learning_resources_home.shtml

---

この資料は、「関連資料」に記載されている資料と併せてご利用ください。