ASA クライアントレス SSL VPN（WebVPN）トラブルシューティング テクニカル ノート

内容

概要

このドキュメントでは、ASAバージョン7.1、7.2、および8.0で採用されたクライアントレスSSL VPN(WebVPN)のトラブルシューティングテクニックを示します。これらのリリース間には、さまざまなトラブルシューティングテクニックを採用する必要がある大きな進歩があります。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、ソフトウェア バージョン 7.1 以上が稼働する Cisco 5500 シリーズ ASA に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

トラブルシューティング

ASA でのクライアントレス SSL VPN 接続（WebVPN）のトラブルシューティングの前提条件は、スクリーンショットおよび HTML キャプチャ ツールの両方を使用してクライアントの使用感についての情報を取得できること、およびその取得した情報と、アクセスしている URL またはアプリケーションに直接接続したときの情報（取得した情報と同じもの）とを比較できることです。

ASA バージョン 7.1/7.2 クライアントレス

このセクションでは、ASA バージョン 7.1/7.2、および 8.0 リリースまで（8.0 は含まない）の暫定リリースすべてのトラブルシューティング テクニックを説明します。

このリリースで Java と Javascript の複合機能に問題がある場合は、その他のオプション（アプリケーション アクセス ポート フォワーディングまたはプロキシバイパスの使用など）を検討します。これらの代替方法の詳細については、「アプリケーション アクセスの設定」および「プロキシ バイパスの使用」を参照してください。

ほとんどのシナリオでは、クライアントレス SSL VPN を使用して Internet Explorer で URL にアクセスできなかった場合、その他のブラウザでもアクセスできません。

クライアント PC またはオペレーティング システムに依存する問題ではないことを確認するために、別の場所にある他のクライアントを使用してください。IPsec または SSL VPN クライアントもテストできます。

「WebVPN 用ブラウザのクッキーのイネーブル化」の説明に従って、ASA がブラウザの Trusted Zone に含まれていることを確認し、「クッキーのイネーブル化」の説明に従って、クッキーがイネーブルになっていることを確認します。

それでもプロセスが失敗する場合は、次の手順に従って必要な情報を収集し、TAC ケースを開きます。

1. 「ブラウザ キャッシュのクリア」の説明に従って、ブラウザのキャッシュをクリアします。
2. 「Java キャッシュのクリア 」の説明に従って、Java のキャッシュをクリアします。
3. 「キャッシングの設定」の説明に従って、ASA の WebVPN キャッシュをディセーブルにします。
4. Java アプレットが存在する場合は、「Java アプレット デバッグ オプションのイネーブル化」の説明に従って、アプレット ウィンドウでデバッグ レベル 5 を使用します。
5. クライアントレス SSL VPN 経由で ASA にログインします。
6. 問題のある URL の直前の URL で、「HTML キャプチャ ツールのイネーブル化」の説明に従って、ブラウザの HTML キャプチャ ツールをイネーブルにします。

7. ここから問題のある URL までのシーケンスをキャプチャします。
8. キーボードで **Ctrl キーを押した状態で Print Screen** キーを押して、スクリーンショットをキャプチャします。
9. HTML キャプチャ ツールを停止します。
10. IPsec または SSL VPN セッションのいずれかを使用して ASA 経由で直接 URL に接続するか、または同じ LAN セグメントに直接接続して（可能な場合）ステップ 1 ~ 9 を実行し、分析用として TAC にデータを送付します。

ASA バージョン 8.0 クライアントレス

このセクションでは、ASA バージョン 8.0 およびすべての暫定版で使用するトラブルシューティング テクニックについて説明します。

このリリースで、クライアントレス SSL VPN で複合 URL またはアプリケーションに問題がある場合は、効果的な代替案として他のオプション（スマート トンネルの使用など）があります。スマート トンネルの詳細については、「スマート トンネル アクセスの設定」を参照してください。

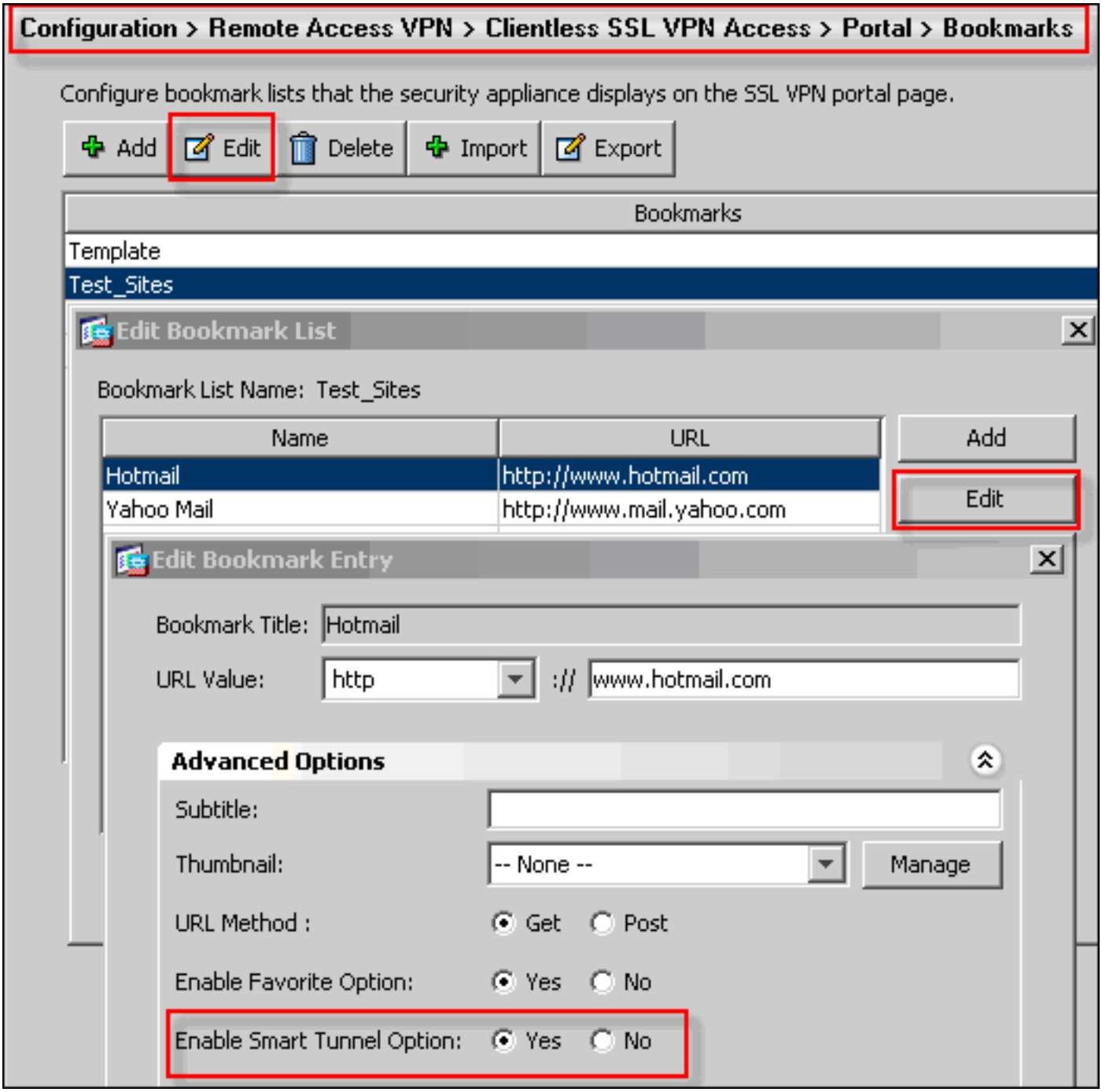
また、アプリケーション アクセス ポート フォワーディングまたはプロキシバイパスの使用を検討することもできます。これらの代替方法の詳細については、「アプリケーション アクセスの設定」および「プロキシ バイパスの使用」を参照してください。

ほとんどのシナリオでは、クライアントレス SSL VPN を使用して Internet Explorer で URL にアクセスできなかった場合、その他のブラウザでもアクセスできません。

クライアント PC またはオペレーティング システムに依存する問題ではないことを確認するために、別の場所にある他のクライアントを使用してください。IPsec または SSL VPN クライアントもテストできます。

「WebVPN 用ブラウザのクッキーのイネーブル化」の説明に従って、ASA がブラウザの Trusted Zone に含まれていることを確認し、「クッキーのイネーブル化」の説明に従って、クッキーがイネーブルになっていることを確認します。

アプリケーションでクライアントレス Content Transformation Engine（CTE/リライタ）に問題が発生した場合は、そのアプリケーションのブックマークを変更して、次の図に示すようにスマート トンネル オプションを有効にしてください



ブックマークでこのオプションをイネーブルにしても、追加の設定が必要になることはありません。ポート フォワーディングと同様に、ブックマークをクリックしてスマート トンネルを使用する新しいウィンドウを開き、アプリケーションのトラフィックを通過させて問題のリライトを避ける方法も、便利なオプションです。

TCP Winsock 32 アプリケーション（RDP など）でこの機能を使用する場合は、管理者はスマート トンネルを経由して使用されるプロセスを識別する必要があります。たとえば、RDP は mstsc.exe プロセスを使用します。このプロセス用に、簡単なスマート トンネル エントリを作成できます。

より複雑なアプリケーションでは、複数のプロセスを発生させる場合があります。[WebVPN Portal] ページで、[Application Access] パネルを選択します。ロードされると、*許可されたアプリケーション*のリストがネットワークのプライベート サイドに接続できるようになります。

それでもプロセスが失敗する場合は、次の手順に従って必要な情報を収集し、TAC ケースを開きます。

1. 「ブラウザ キャッシュのクリア」の説明に従って、ブラウザのキャッシュをクリアします。
2. 「Java キャッシュのクリア 」の説明に従って、Java のキャッシュをクリアします。
3. 「キャッシングの設定」の説明に従って、ASA の WebVPN キャッシュをディセーブルにします。
4. Java アプレットが存在する場合は、「Java アプレット デバッグ オプションのイネーブル化」の説明に従って、アプレット ウィンドウでデバッグ レベル 5 を使用します。
5. クライアントレス SSL VPN 経由で ASA にログインします。
6. 問題のある URL の直前の URL で、「HTML キャプチャ ツールのイネーブル化」の説明に従って、ブラウザの HTML キャプチャ ツールをイネーブルにします。
7. ここから問題のある URL までのシーケンスをキャプチャします。
8. キーボードで **Ctrl キーを押した状態で Print Screen** キーを押して、スクリーンショットをキャプチャします。
9. HTML キャプチャ ツールを停止します。
10. IPsec または AnyConnect SSL セッションのいずれかを使用して ASA 経由で直接 URL に接続するか、または同じ LAN セグメントに直接接続して (可能な場合) ステップ 1 ~ 9 を実行し、これらのステップを完了して、分析用として TAC にデータを送付します。

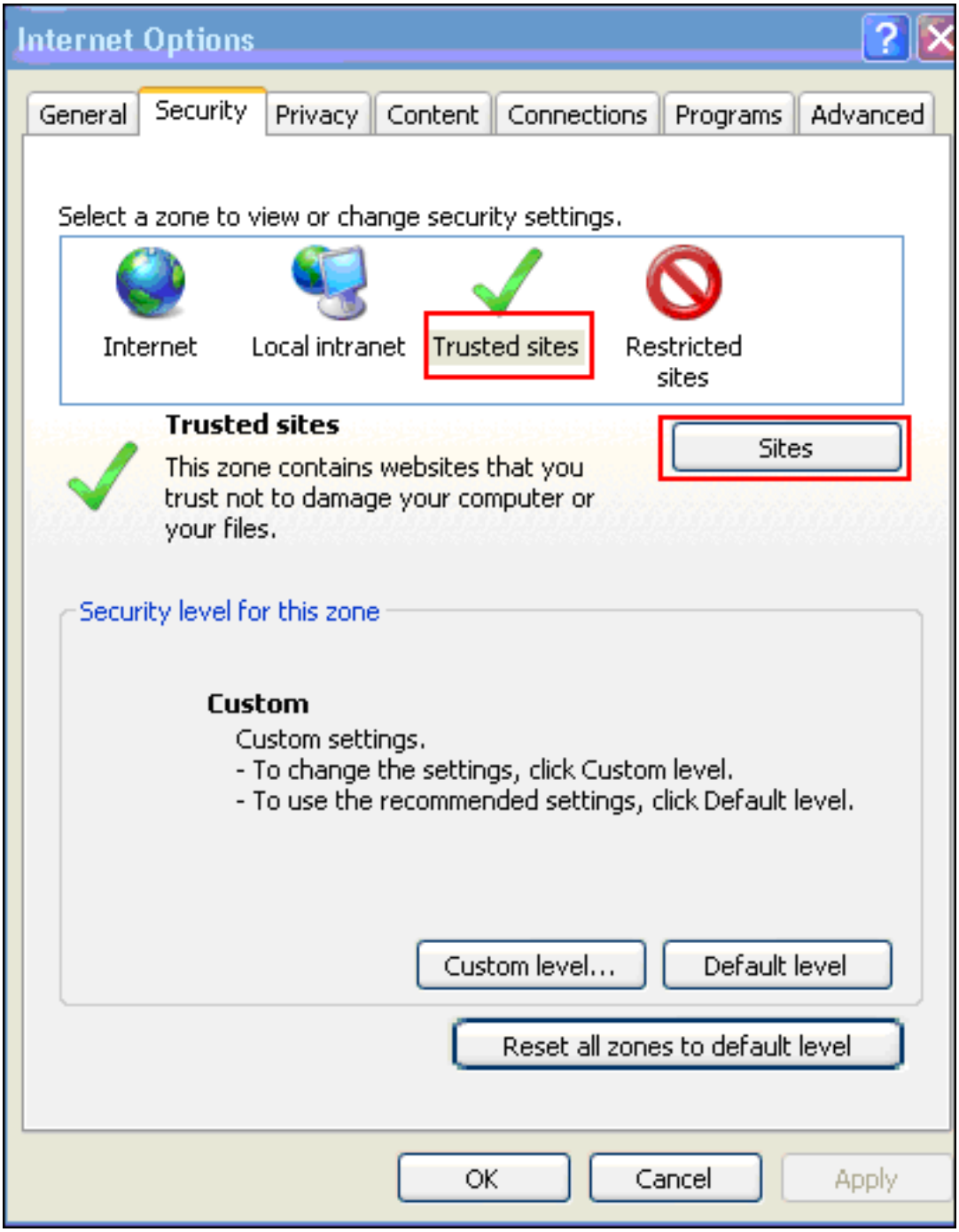
手順

信頼済みサイトとしての ASA の追加

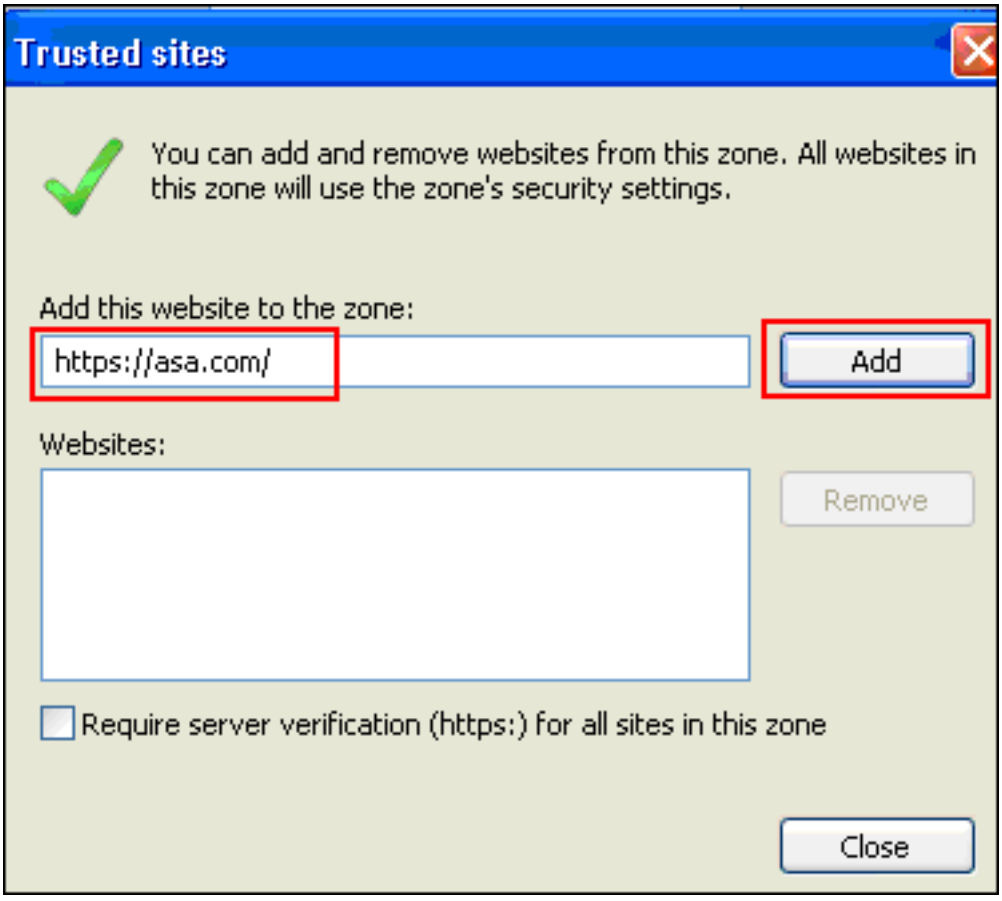
Internet Explorer で ASA にアクセスすると、サイトが信頼済みサイトに含まれていない場合は、証明書エラーが表示されます。

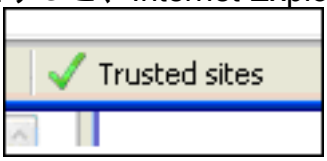
次の手順を実行して、ASA を信頼済みサイトとして追加します。

1. Interent Explorer で、[Tools] > [Internet Options] を選択します。
2. [Security] タブをクリックし、[Trused sites] を選択します。



3. [Sites] をクリックします。
4. https:// と ASA のアドレスを追加し、[Add] をクリックします。



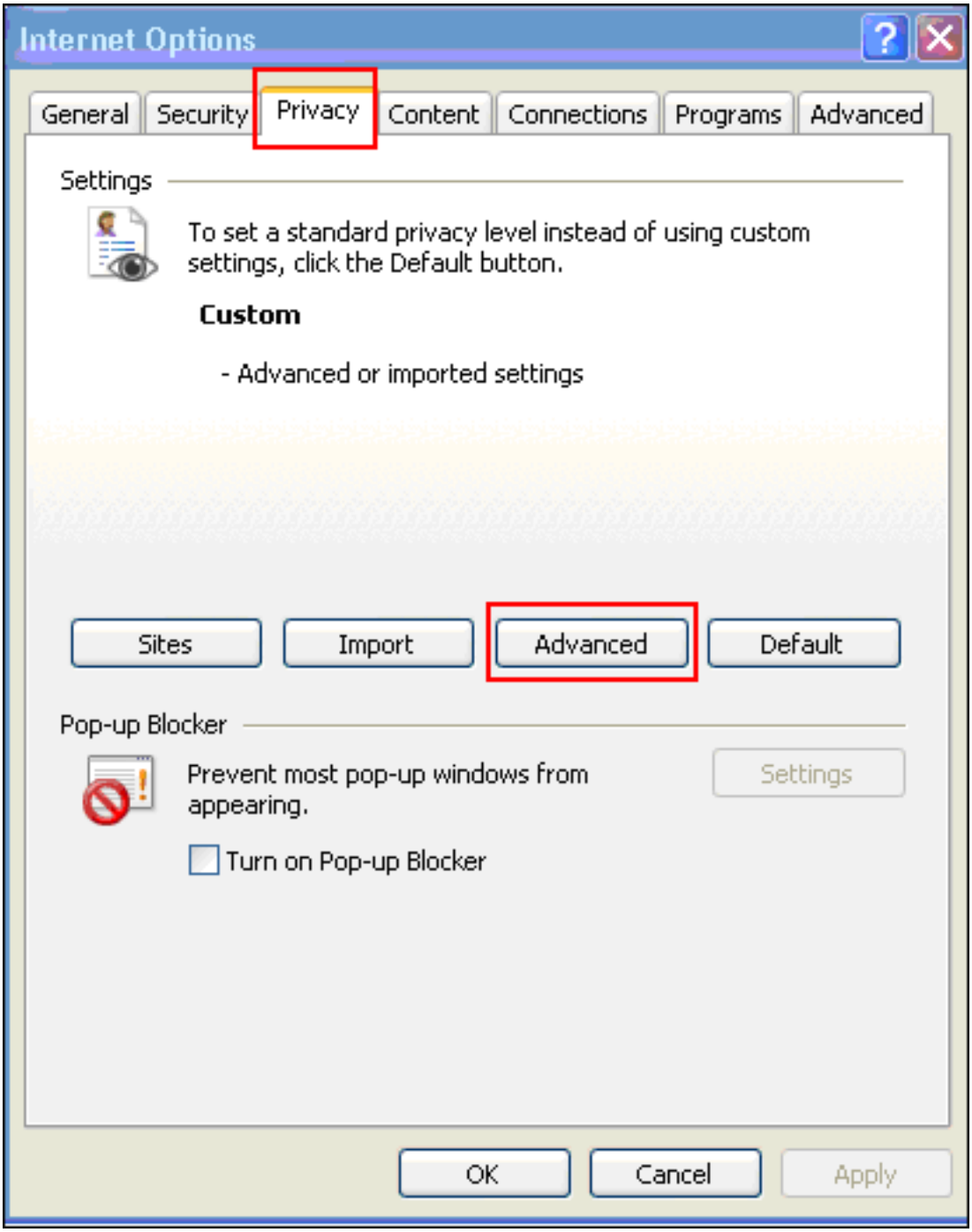
5. サイトを追加すると、Internet Explorer のステータス バーに信頼済みサイトのアイコンが表示されます。 

注：この手順の詳細については、『Internet Explorer 6セキュリティ設定の操作』を参照してください。

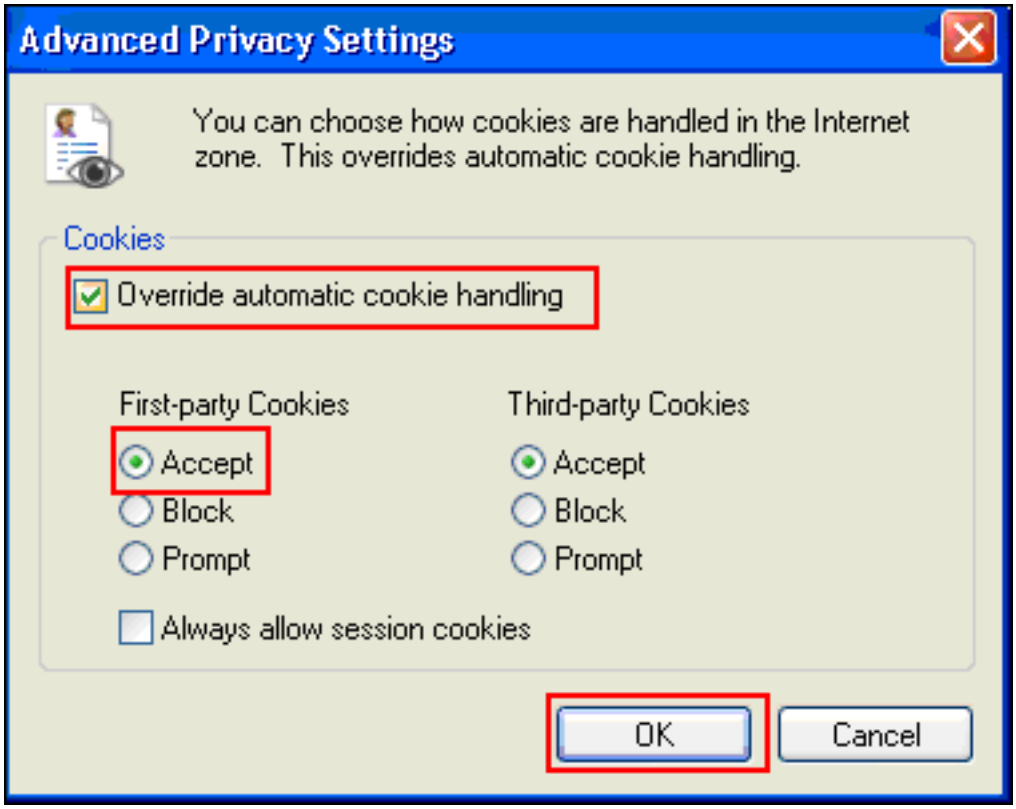
クッキーのイネーブル化

クッキーをイネーブルにするには、次の手順を実行します。

1. Internet Explorer で、[Tools] > [Internet Options] を選択します。
2. [Privacy] タブをクリックして、次に [Advanced] をクリックします。



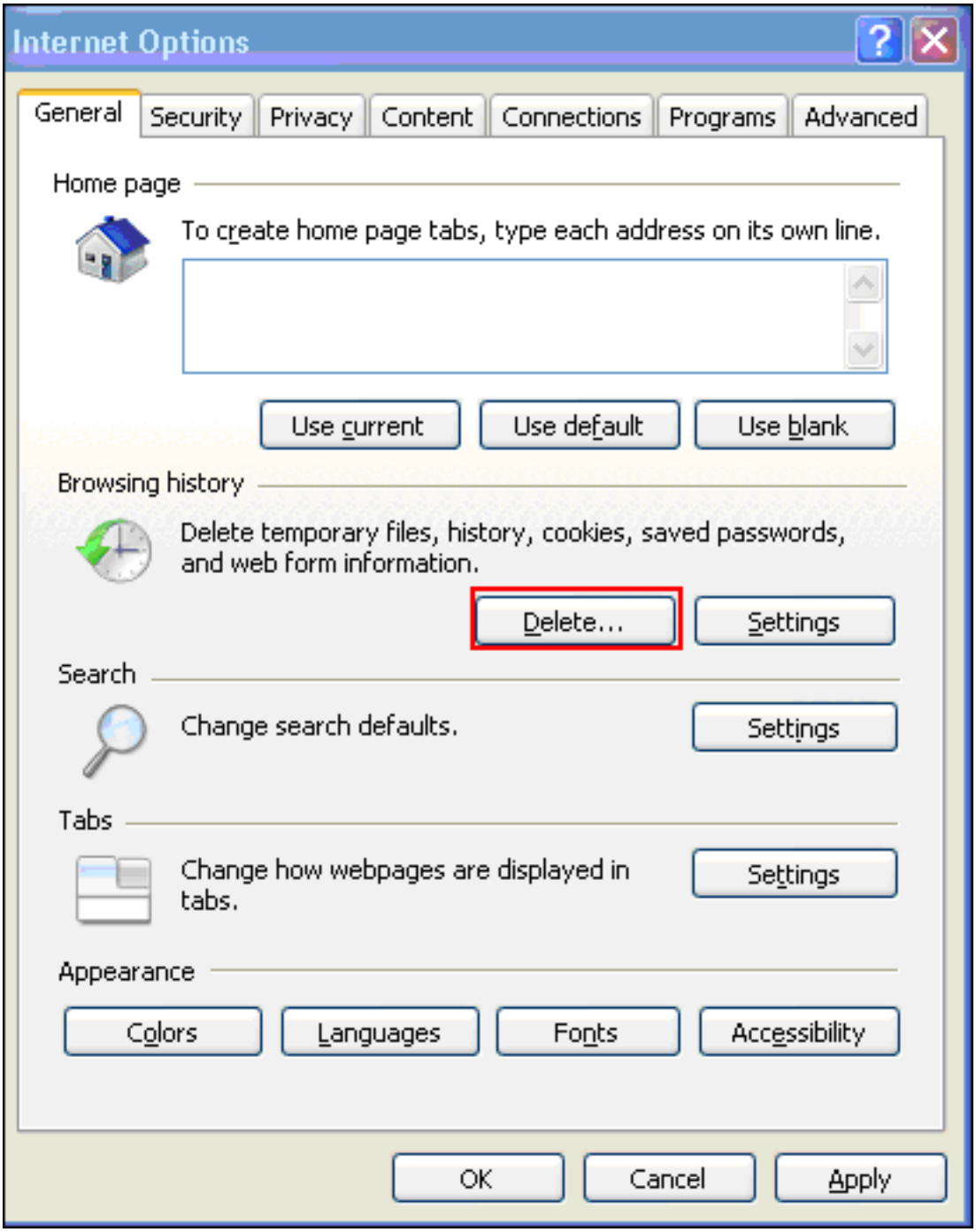
3. [Advanced Privacy Settings] ダイアログボックスで [Override automatic cookie handling] チェックボックスをオンにし、[Accept] オプション ボタンをクリックして、[OK] をクリック

します。 

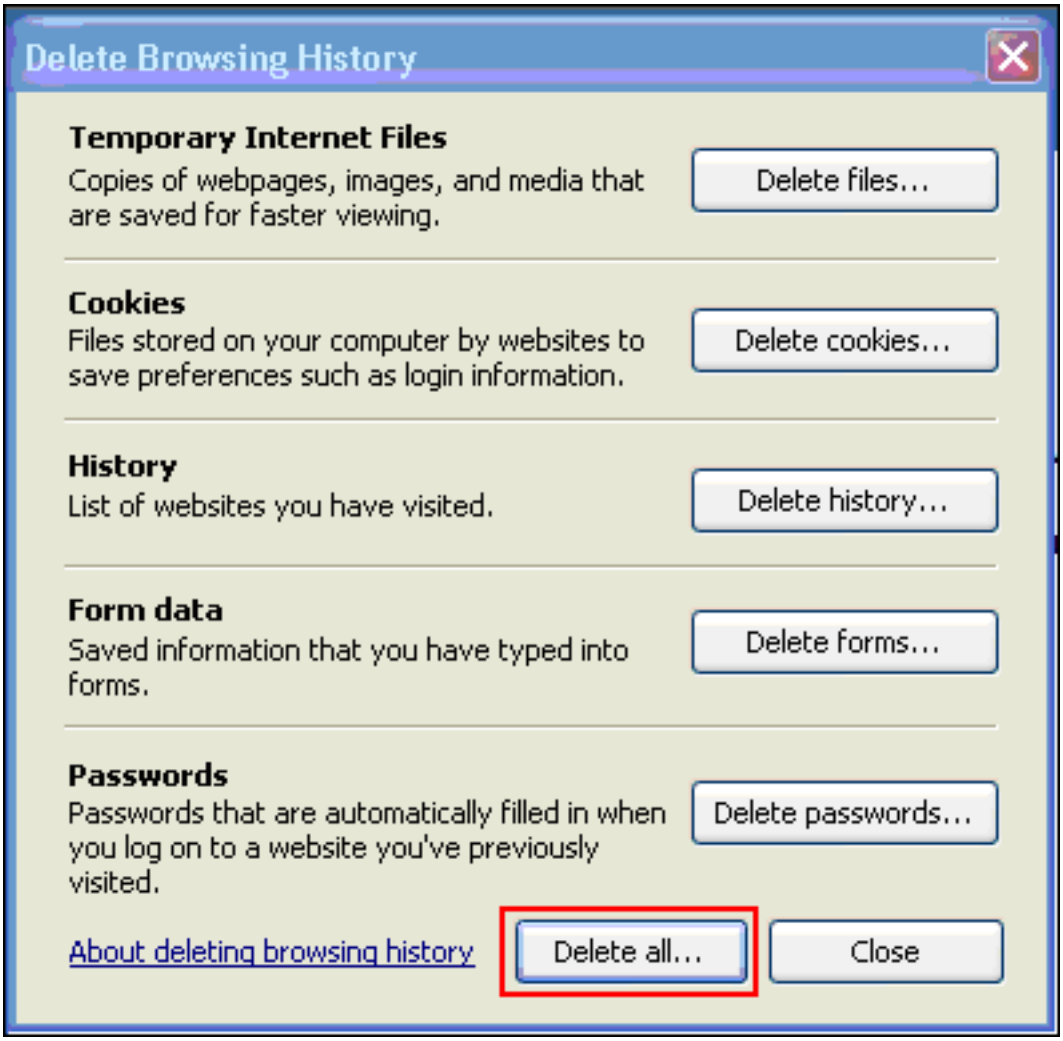
ブラウザ キャッシュのクリア

Internet Explorer のキャッシュをクリアするには、次の手順を実行します。

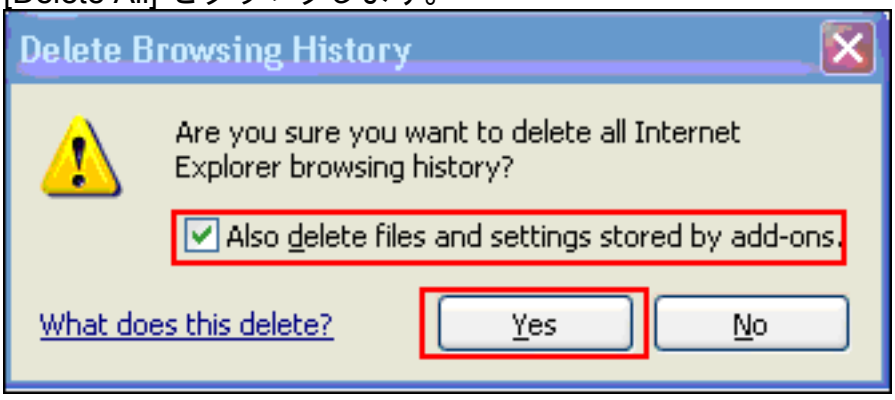
1. Internet Explorer で、[Tools] > [Internet Options] を選択します。



2. [General] タブの [Browsing history] セクションで [Delete] をクリックします。



3. [Delete All] をクリックします。



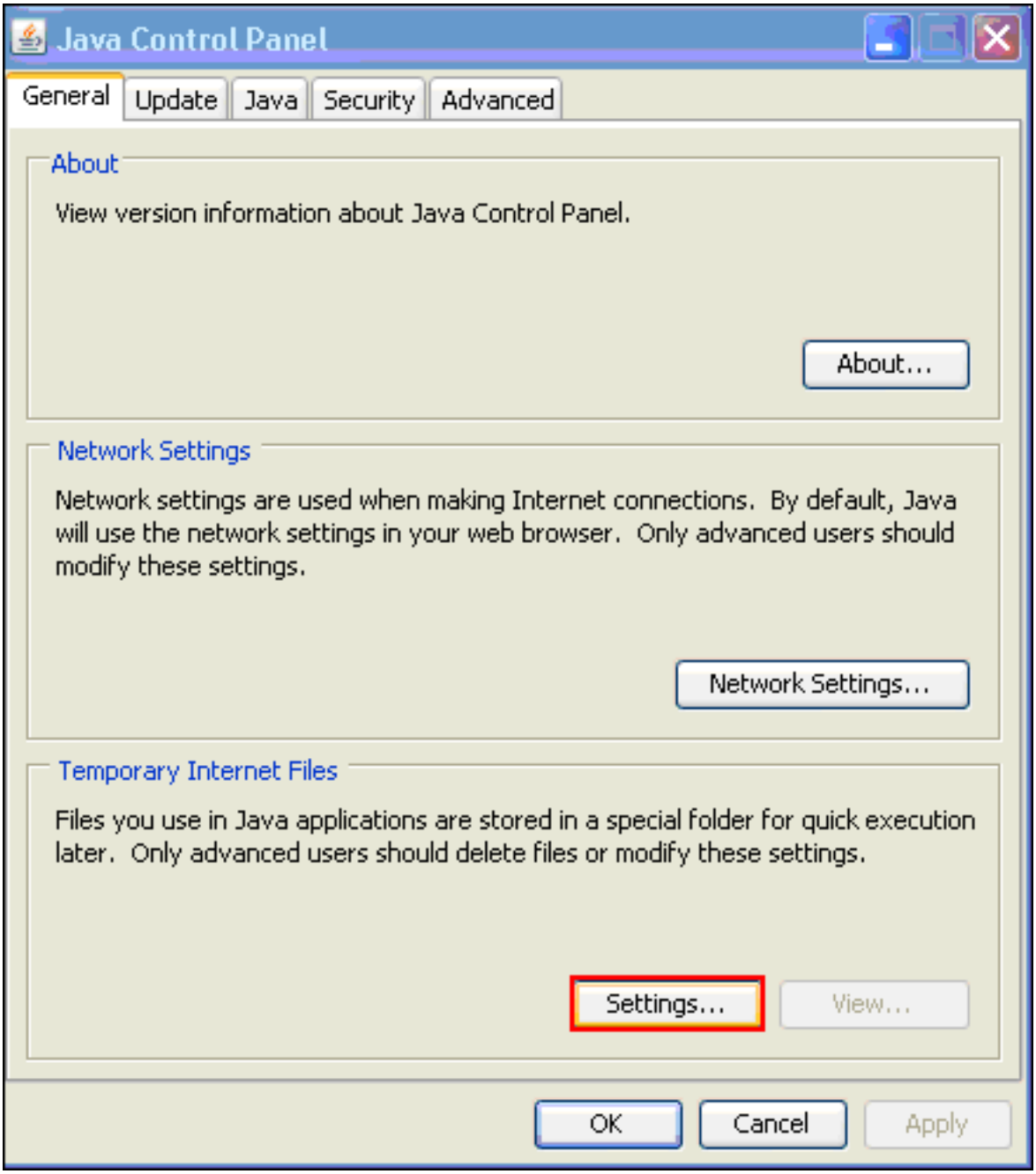
4. [Also delete files and settings stored by add-ons] チェックボックスをオンにして、[Yes] をクリックします。
5. キャッシュがクリアされたら、ブラウザのすべてのインスタンスをシャットダウンして、ブラウザを再起動します。

注：他のブラウザのキャッシュをクリアするには、「ブラウザのキャッシュをクリアする[には（パフォーマンスを向上させるために）」を参照してください。](#)

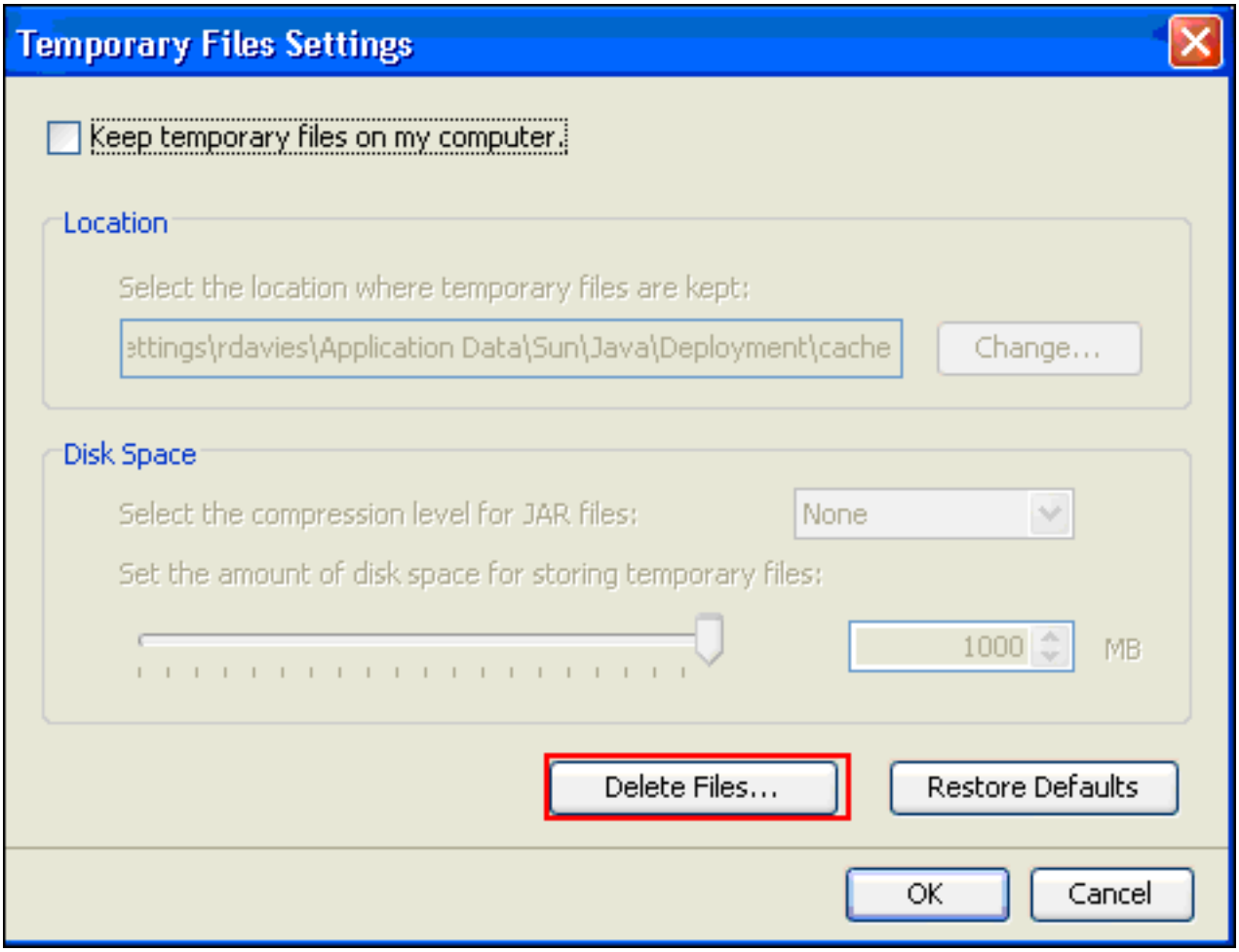
[Java キャッシュのクリア](#)

Java のキャッシュをクリアするには、次の手順を実行します。

1. Windows の [Start] メニューから [Control Panel] を選択します。
2. [Java] をダブルクリックします。



3. [Setting] をクリックします。
4. [Delete Files] をクリックします。

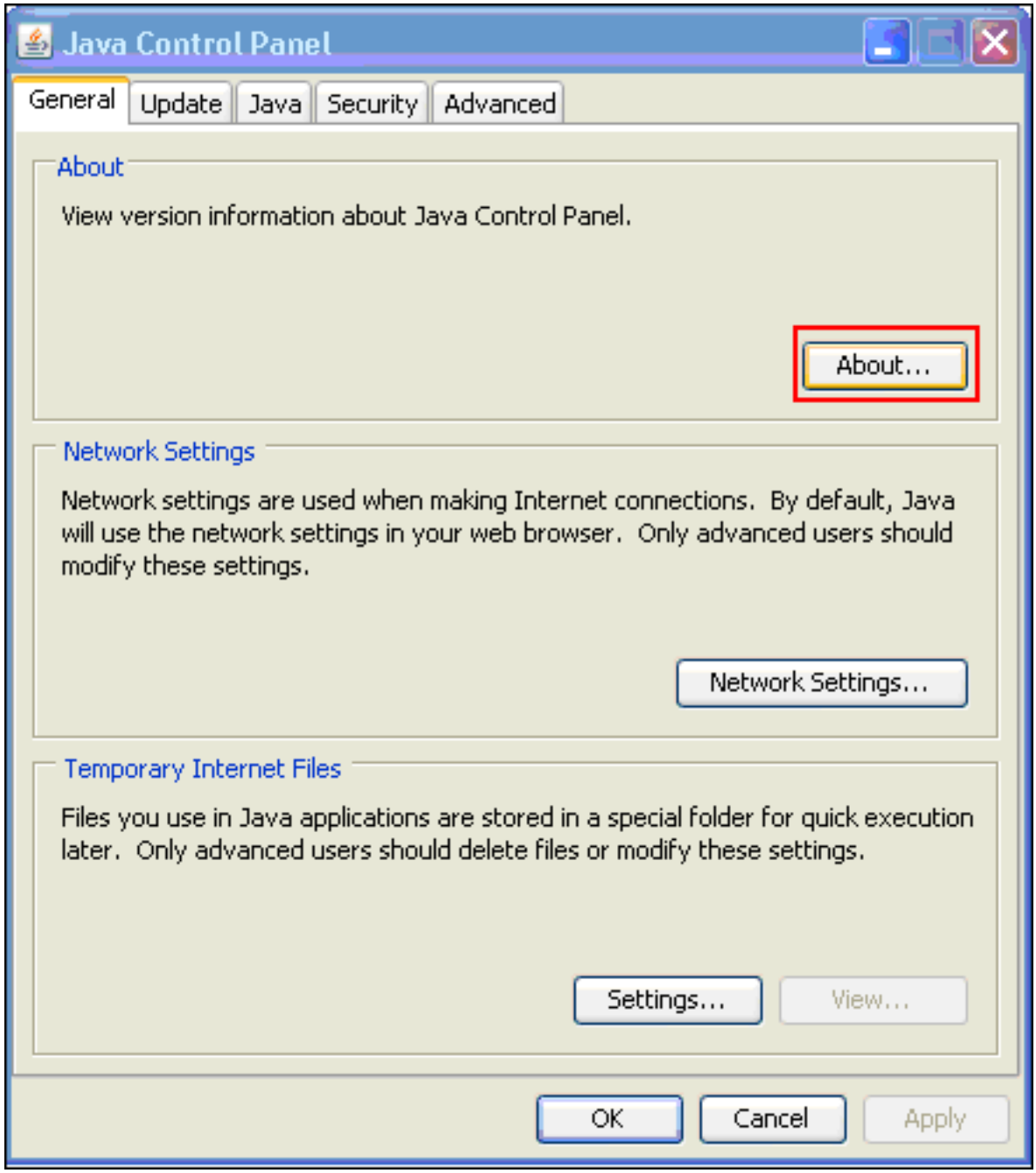


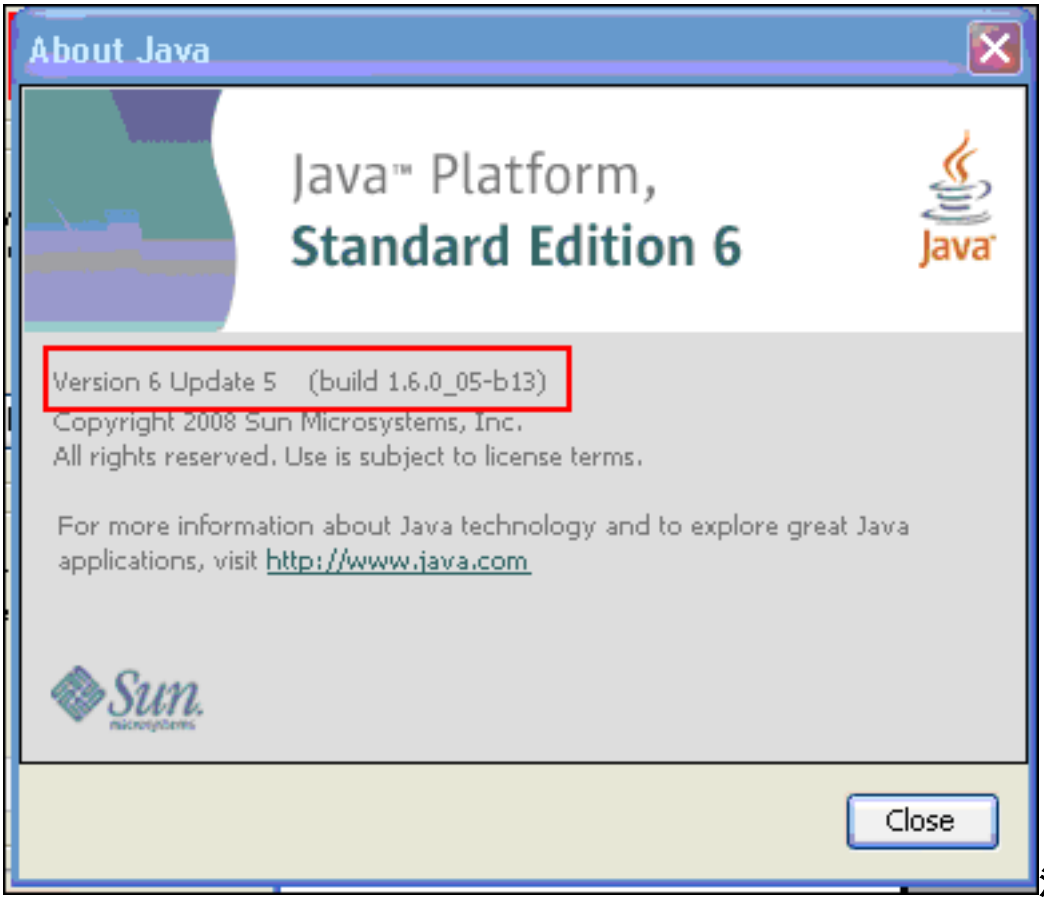
注： 「How do I clear my Java cache?」を参照してください。 を参照してください。

Java アプレット デバッグ オプションのイネーブル化

Java アプレット デバッグ オプションをイネーブルにするには、次の手順を実行します。

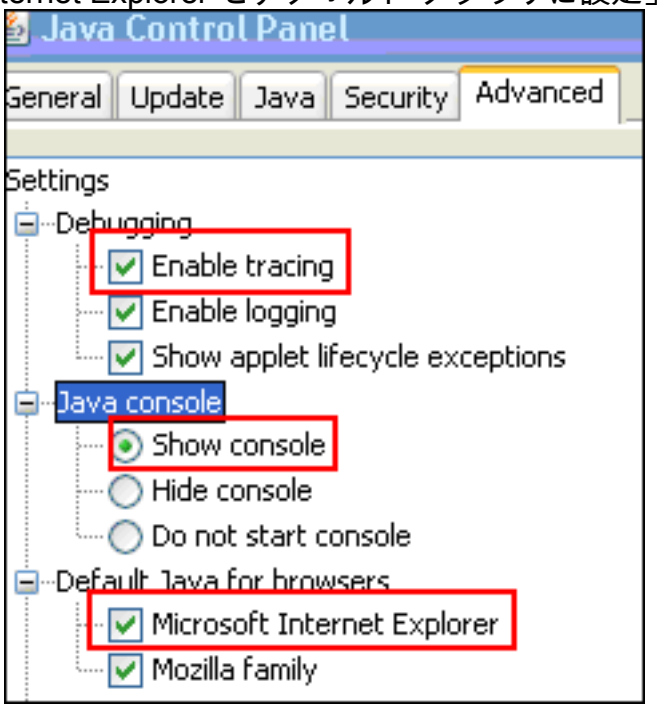
1. Java 1.4 以上がイネーブルになっていることを確認します。Windows の [Start] メニューから [Control Panel] を選択します。[Java] をダブルクリックします。[About] をクリックして、バージョン番号を確認します。


Java Control Panel
General
Update
Java
Security
Advanced
About
View version information about Java Control Panel.
About...
Network Settings
Network settings are used when making Internet connections. By default, Java will use the network settings in your web browser. Only advanced users should modify these settings.
Network Settings...
Temporary Internet Files
Files you use in Java applications are stored in a special folder for quick execution later. Only advanced users should delete files or modify these settings.
Settings...
View...
OK
Cancel
Apply

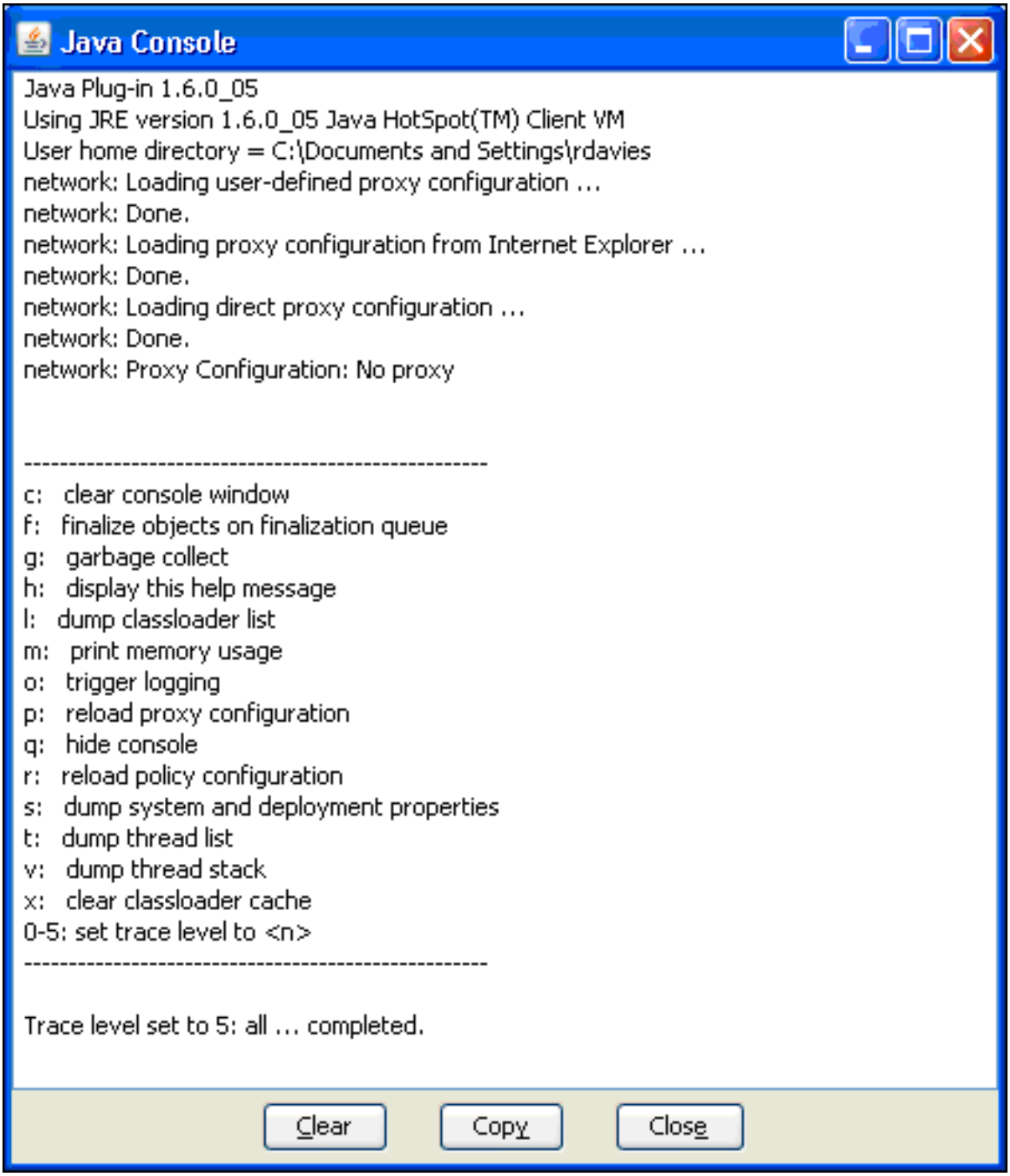


注：Javaの更新は、http://java.com/en/からダウンロードできます。

2. 次の図のように、Java が「トレースをイネーブル」、「コンソールを表示」、「Microsoft Internet Explorer をデフォルト ブラウザに設定」に設定されていることを確認してください。



3. 「Java キャッシュのクリア」の説明に従って、Java のキャッシュがクリアされていることを確認します。
4. Internet Explorer で、[Tools] > [Java Console] を選択して、Java デバッグ ウィンドウを開きます。



5. Java Console のデバッグ ウィンドウが開いたら、**5** を押してトレース レベルを設定します。Java Applet が含まれる URL にアクセスすると、そのアクティビティがこのウィンドウでキャプチャされます。
6. [Copy] をクリックして情報をコピーします。

HTML キャプチャ ツールのイネーブル化

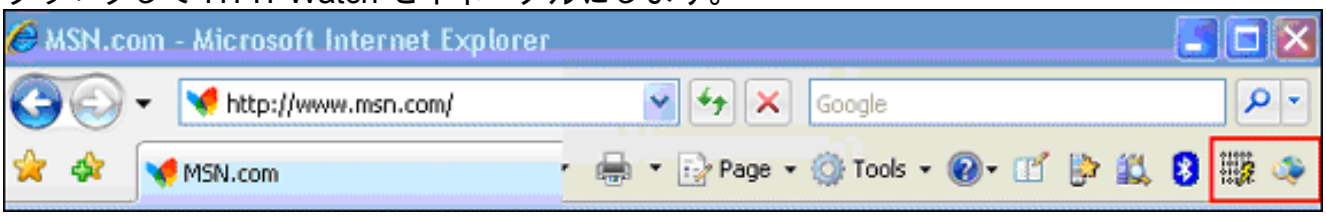
データの収集には、多くのさまざまな HTML キャプチャ ツールを使用でき、ここにリストされているものはその一部です。これらの HTML キャプチャ ツールのいずれかを、データの収集に使用するクライアント PC にインストールします。

- HTTPWatch
- IE Inspector
- Debug Proxy

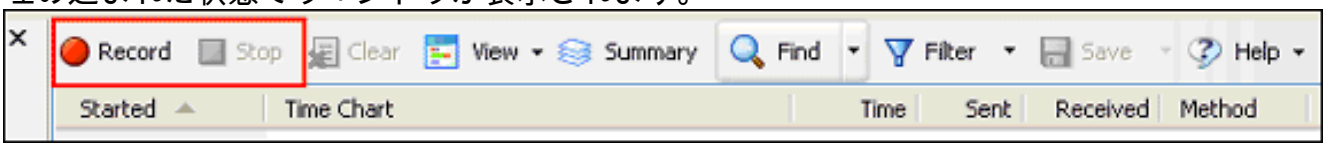
注：このプロシージャでは、HTTPWatchアプリケーションを使用します。

アプリケーションをインストールしたら、次の手順を実行します。

1. Shift キーを押した状態で P、F、2 キーを押すか、またはブラウザ ウィンドウのアイコンをクリックして HTTPWatch をイネーブルにします。



2. アプリケーションがイネーブルになると、次の図のように、ブラウザ ウィンドウの下部に埋め込まれた状態でウィンドウが表示されます。



3. [Record] をクリックしてデータを記録します。記録を停止するには、[Stop] をクリックします。

注：データを記録するには、HttpWatch 7.xを使用することをお勧めします。

関連情報

- ASA でのクライアントレス SSL VPN（WebVPN）の設定例
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- テクニカル サポートとドキュメント – Cisco Systems