URL フィルタリングソフト

InterSafe WebFilter

Technical Guide

テクニカル＆トラブルシュートガイド
認証除外について

目次

変更履歴

変更日	ページ番号	変更内容
2012/11/14	P.1	サブタイトルを変更
	全体	Ver8.0 の情報を追加
	P.16	ホスト名一覧 No.1 を追加
2013/03/15	P.12	UA 一覧 No.14 に「Microsoft Office」を追加
	P.16	ホスト名一覧 No.1 に「download.windowsupdate.com」を追加
	P.16	ホスト名一覧 No.3 を追加
2013/10/24	P.9	「ホストによる認証除外設定」に Ver8.5 での動作を記載
	P.16	ホスト名一覧 No.10 を追加
2015/05/01	P.8	「2-3.notice.log から確認する方法」を追加
	P.10	Ver8.5 SP1 以降、管理画面から認証除外設定を行う方法を追加
	P.11	「ホストによる認証除外設定」に Ver8.0 での動作を記載
	P.14	「フィルタリングバイパス設定による回避」を追加
2015/12/02	P.19	ホスト名一覧 No.1 に Windows10 での WindowsUpdate で利用されるホスト名を追加

1.はじめに

InterSafe WebFilter(以下 ISWF)で、LDAP 連携によるアカウント認証や NTLM 認証を行っている場合、クライアント PC 側で動作するアプリケーションや Windows Update などが､ISWF のアカウント認証に対応していないことが原因でリクエストに失敗し、そのアプリケーション等に不具合が生じる場合がございます。本資料で紹介する､「ユーザエージェントによる認証除外設定」（Ver5.0 以降)、あるいは､「ホストによる認証除外設定」（Ver6.5 以降）のいずれかの設定で認証除外を行うことで、不具合を解消できる場合がございます。

2.UA、ホストの確認

本項では、ユーザエージェント（UA)、ホストの確認方法について説明します。

2-1.UA、ホストをアクセスログから確認する方法

事前設定

UA を確認するには、ログの出力項目として､「ブラウザバージョン」を追加します。（ブラウザバージョンは UA を指します。）また、アクセスログで確認するには、認証に失敗しているリクエストを成功させる必要があるため、IP アドレスを登録し、IP アドレス認証にて成功した際のアクセスログを出力させます。

1) ISWF 管理画面にログインし、ログ設定画面を表示します。

●Ver8.0 以降の場合　[ログ管理] > [ログ設定]

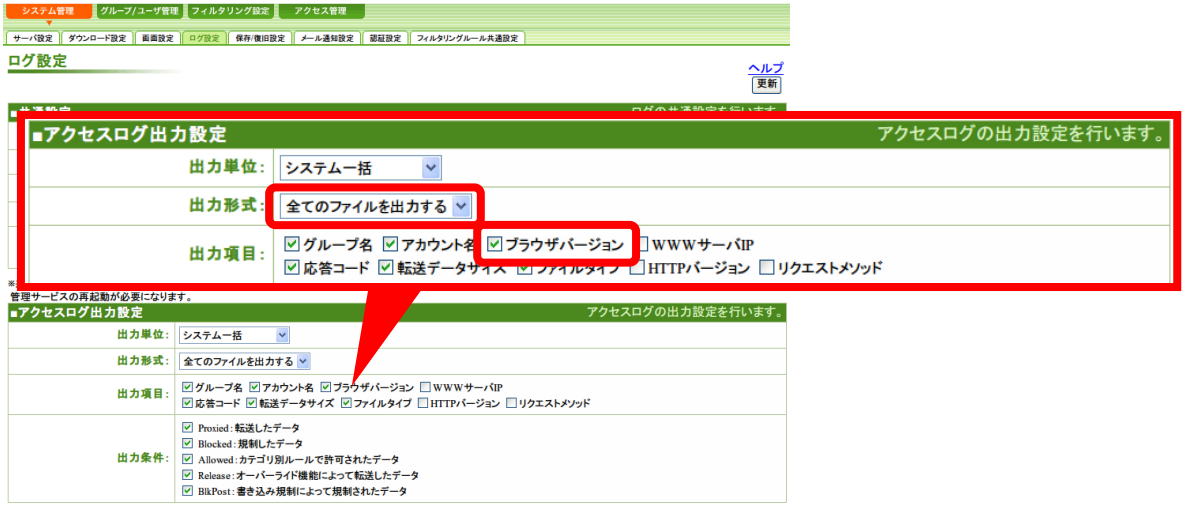
●Ver7.0 以前の場合　[システム管理] > [ログ設定]

2) 「出力項目」の 「ブラウザバージョン」にチェックが入っていることを確認します。（インストール直後は､「ブラウザバージョン」にチェックは入っていません。)「出力形式」を「全てのファイルを出力する」に変更します。

● 「出力形式」を「TEXT のみ出力する」にしていると、アクセスログが出力されず UA が確認できない場合があるため､「全てのファイルを出力する」に変更する必要があります。

図 2-1 Ver8.0 の場合

図 2-2 Ver7.0 以前の場合



4) 画面右上の[保存]（Ver7.0 以前は[更新]）ボタンをクリックし設定を保存します。

5) IP アドレス認証を設定します。

●Ver8.0 以降の場合　[グループ/ユーザ管理] > [ユーザ管理] にて、対象のユーザ（PC）が所属するグループを選択し、[IP アドレス一覧]タブの「+IP アドレスを追加」にて「開始 IP アドレス」に PC の IP アドレスを入力して、[保存]ボタンをクリックします。

●Ver7.0 以前の場合　[グループ/ユーザ管理] にて、対象のユーザ（PC）が所属するグループを選択し、IP アドレス登録画面にて、「IP アドレス（開始）」に PC の IP アドレスを入力し[登録]ボタンをクリックします。

● LDAP 連携によるアカウント認証のままですとリクエストに失敗しログが出力されません。一時的に特定の PC の IP アドレスを登録し、IP アドレス認証をおこなうことで、失敗していたリクエストが可能になります。ログ取得後は、登録した IP アドレスを削除してください。

図 2-3 Ver8.0 以降の場合

図 2-4 Ver7.0 以前の場合

アクセスの実施

リクエストできないアプリケーションにて、ISWF 経由でのアクセスを行います。アクセス後、InterSafe_http.log のログに UA が出力されているか確認します。ログファイルは下記の場所にあります。

Windows 版：<ISWF インストールフォルダ>¥log

Linux、Solaris 版：<ISWF インストールディレクトリ>/logs

例）Internet Explorer 7 の UA

Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR2.0.50727)

http ログは下記のフォーマットにて出力されます。

●Ver8.0 以降(タブ区切り)

年月日　時刻　プロトコル　クライアントアドレス　グループ名　アカウント名　ブラウザバージョン　転送状態　WWW サーバ IP　応答コード　WWW サーバ名　転送時間　送信データサイズ　受信データサイズ　ファイルタイプ　コンテンツタイプ　判定理由　判定カテゴリ　カテゴリ 1　カテゴリ 2　セキュリティカテゴリ　リクエスト URL　HTTP バージョン　リクエストメソッド　リンク元サイト

●Ver7.0 以前(カンマ区切り)

年月日,時刻,”プロトコル”,”リクエスト元 IP”,”グループ名”,”アカウント名”,”ブラウザバージョン”,”転送状態”,”WWW サーバ IP”,応答コード,”WWW サーバ名”,転送時間,転送データサイズ,”ファイルタイプ”,”カテゴリ名”,”リクエスト URL”,”HTTP バージョン”,”リクエストメソッド”

UA は〝ブラウザバージョン” に表示されます。ホスト名は、WWW サーバ名、もしくはリクエスト URL にて確認できます。

2-2.UA、ホストをパケットキャプチャから確認する方法

前項で UA、あるいはホストが確認できない場合は、パケットキャプチャを取得して UA の確認を行います。Windows 版パケットキャプチャソフト「Wireshark」を利用してパケットキャプチャの取得、確認を行います。Linux 版、Solaris 版をご利用のお客様の場合は、以下のコマンドにてパケットキャプチャの取得し、Wireshark にて確認を行います。

Linux の場合：*tcpdump -x -s 3000 -w ファイル名*

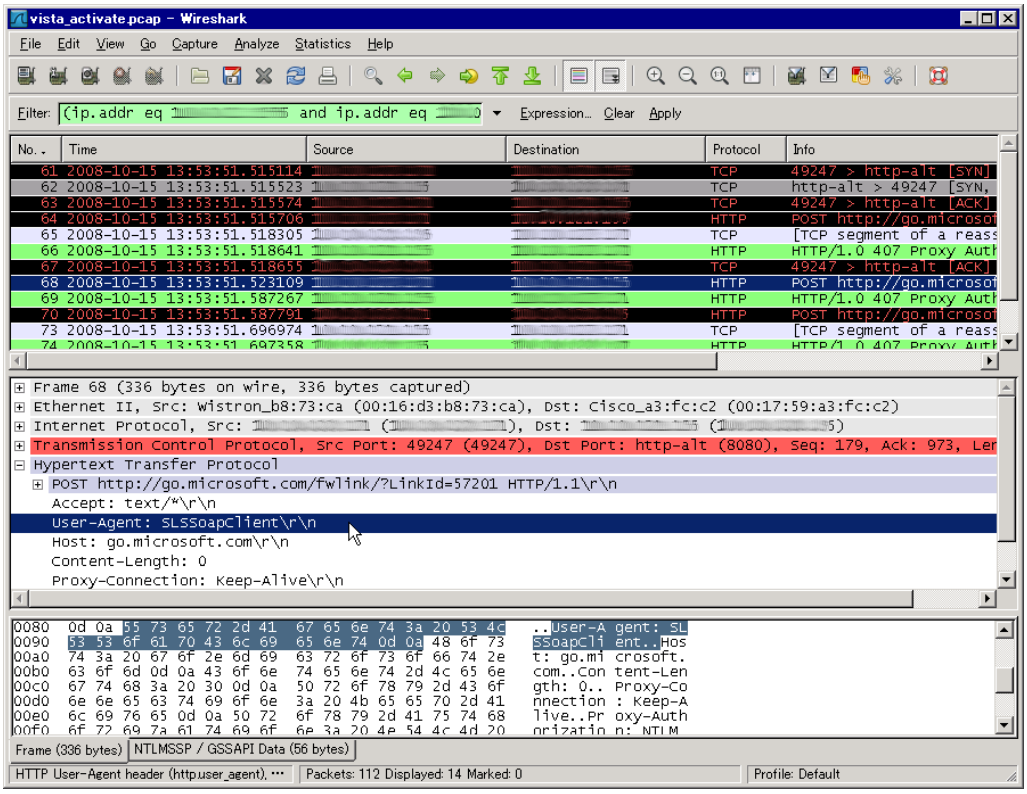
Solaris の場合：*snoop -o ファイル名*

UA は、パケットの HTTP ヘッダの一つ「User-Agent」にて確認することができます。

ホストは、HTTP ヘッダの「Host」などから確認できます。

- HTTPS の場合、User-Agent ヘッダは暗号化されているため確認ができません。下図では WireShark の 1.0.1 の画面を示しています。この例では、68 フレーム目のパケットに POST リクエストがあり、User-Agent にて"SLSSoapClient"が確認できます。"SLSSoapClient"は Vista の OS ライセンス認証時に使用される UA です。

図 2-5



2-3.notice.logから確認する方法

Ver8.5 SP1 以降では出力されるログに「InterSafe_notice.log」が追加されました。
上記ログは認証に失敗した際に出力されます。
出力されるログには以下の内容が含まれます。

・クライアント IP アドレス
・リクエストメソッド
・宛先ホスト
・User-Agent

ログ出力例
Failed to NTLM authenticate. (invalid NTLM parameter(2)) [client=192.168.1.1; method=GET;
elapsedTime=25;Host=www.alsi.co.jp; User-Agent=alsitool;]

上記ログの場合、User-Agent が alsitool のアプリケーションから「www.alsi.co.jp」というホスト宛にリクエストを送信しましたが、アプリケーションが NTLM 認証に対応していないため、認証に失敗しています。

- notice.log は管理画面にログイン後、[ログ管理] > [システムログ] より確認できます。

3.回避策

本項では、認証除外の設定方法について説明します。

3-1.認証除外の設定

前項 2 で UA が確認できた場合は、「UA による認証除外設定」をご確認ください。「UA による認証除外設定」にて、回避できなかった場合、あるいは、UA 自体が確認できない場合は、「ホストによる認証除外設定」をご確認ください。

UA による認証除外設定

■ **Proxy.inf への追加**

前項 2 で確認した UA を proxy.inf の"AUTHORIZED_USER_AGENT="に追加します。追加した UA からのリクエストは、自動的にルートグループのユーザとして認証され、ルートグループにスケジュールされているフィルタリングルールが適用されます。既存で UA が指定されていますので、末尾に追記します。追記する場合は、セパレータ文字のカンマ(,)を加えて UA を追記します。Proxy.inf は以下の場所にあります。

Windows の場合：*<ISWF インストールフォルダ>¥conf*
Linux、Solaris の場合：*<ISWF インストールディレクトリ>/conf*

例）"SLSSoapClient"を追加する場合

●追加前

AUTHORIZED_USER_AGENT=Windows-Update-Agent,Microsoft BITS,EndPointModule,Windows Installer,Microsoft-CryptoAPI,CATsecurity

●追加後

AUTHORIZED_USER_AGENT=Windows-Update-Agent,Microsoft BITS,EndPointModule,Windows Installer,Microsoft-CryptoAPI,CATsecurity,SLSSoapClient

セパレータ文字列は以下のパラメータで指定できます。

AUA_SEPARATOR=,

設定後、「3-2.認証除外の設定」の手順に従って、設定を反映させます。

アプリケーションによっては、UA にバージョン情報など可変する可能性のある文字列を含んでいるものもあります。可変する可能性のある文字列を除いて登録いただくと効果的です。

例）Internet Explorer 7 の UA の場合

Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729; MDDR; InfoPath.1; OfficeLiveConnector.1.3; OfficeLivePatch.0.0)

上記のようにバージョン情報など、可変する要素が含まれており、何らかのきっかけで UA が変わる可能性があるため、可変の可能性が少ない、"MSIE 7" を AUTHORIZED_USER_AGENT に登録することで、より変化に対応しやすくなります。

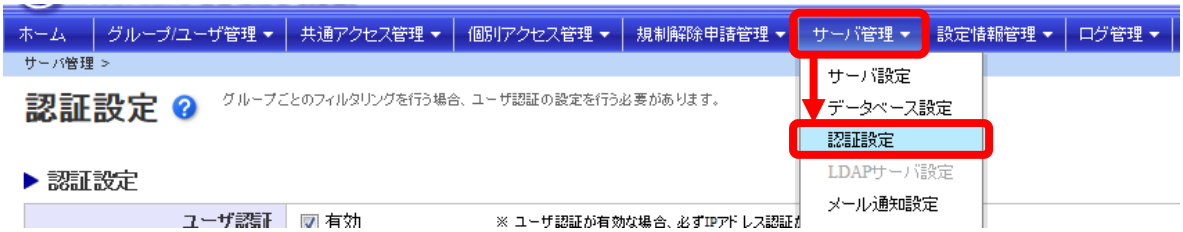
- Ver5.0、Ver6.0 にて、メモ帳で proxy.inf を編集すると、制御コード（BOM）が付加され、設定が正しく読み込まれない場合がございます。proxy.inf はメモ帳以外のテキストエディタで編集してください。
- 登録された UA は部分一致となります。「a」と登録した場合、「a」の文字を含む UA が認証除外の対象となります。
- ワイルドカード(*)などで正規表現を行うことはできません。
- 大文字小文字を判別します。

■ **管理画面から追加**

Ver8.5 SP1 以降では管理画面より認証除外する UA を追加できます。

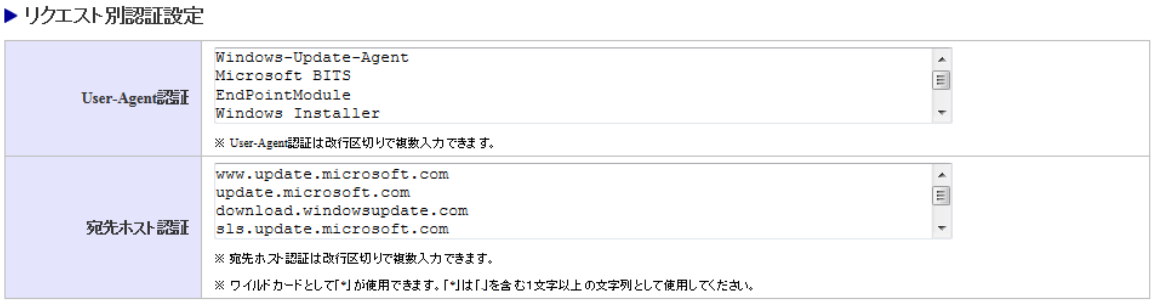
1) 管理画面にログイン後、[サーバ管理] > [認証設定] をクリックします。

図 3-1



2) 「リクエスト別認証設定」の「User-Agent 認証」に認証除外する UA を追加します。

図 3-2



3) 追加後、画面右上の[保存]ボタンをクリックし、設定を反映させます。

ホストによる認証除外設定

■ **Proxy.inf への追加**

前項 2 で確認したホストを proxy.inf の"AUTHORIZED_HOST="に追加します。追加したホストへのリクエストは、自動的にルートグループのユーザとして認証され、ルートグループにスケジュールされているフィルタリングルールが適用されます。既存でホスト名が指定されていますので、末尾に追記します。追記する場合は、セパレータ文字のカンマ(,)を加えてホスト名を追記します。

例）"activation.sls.microsoft.com", "192.168.0.1"を追加する場合

●追加前

AUTHORIZED_HOST=www.update.microsoft.com

●追加後

AUTHORIZED_HOST=www.update.microsoft.com,activation.sls.microsoft.com, 192.168.0.1

または、Ver8.5 以降では以下でも指定できます。

*AUTHORIZED_HOST=*microsoft.com, 192.168.0.1*

セパレータ文字列は以下のパラメータで指定できます。

AH_SEPARATOR=,

設定後、「3-2.認証除外の設定」の手順に従って、設定を反映させます。

- Ver5.0、Ver6.0 にて、メモ帳で proxy.inf を編集すると、制御コード（BOM）が付加され、設定が正しく読み込まれない場合がございます。proxy.inf はメモ帳以外のテキストエディタで編集してください。
- ホスト名は完全一致したものが有効になります。
- Ver8.5 以降ではワイルドカード(*)を利用できるようになりました。

- Ver8.0 以前ではワイルドカード(*)などで正規表現を行うことはできません。完全一致となります。
- Ver8.5 をご使用の場合 HTTPS サイトのホスト名を登録する場合、ポート番号は**付与せずに**登録してください。
- Ver8.0 をご使用の場合 HTTPS サイトのホスト名を登録する場合、ポート番号を**付与して**登録してください。
  例）www.alsi.co.jp:443

■ 管理画面から追加

Ver8.5 SP1 以降では管理画面より認証除外するホスト名を追加できます。

- 認証を除外するホスト名の追加手順は P.10「UA による認証除外設定」の「管理画面から追加」をご参照ください。

3-2.認証除外の設定反映

前項 3-1 での設定変更後、ISWF の設定読み込みコマンドを実行、もしくは、フィルタリングサービスの再起動を行ない、設定を反映させます。

- Ver8.5 SP1 以降で管理画面より追加した場合は、設定を反映させる以下の手順は必要ありません。

設定読み込みコマンドの実行

ISWF サーバの CLI にて、以下のコマンドを実行します。

<インストールディレクトリ>/bin/amsdata -reload

- 実行に成功すると、”Processing was completed.” のメッセージがプロンプトに表示されます。

コマンド実行後、現象が改善されているかご確認ください。

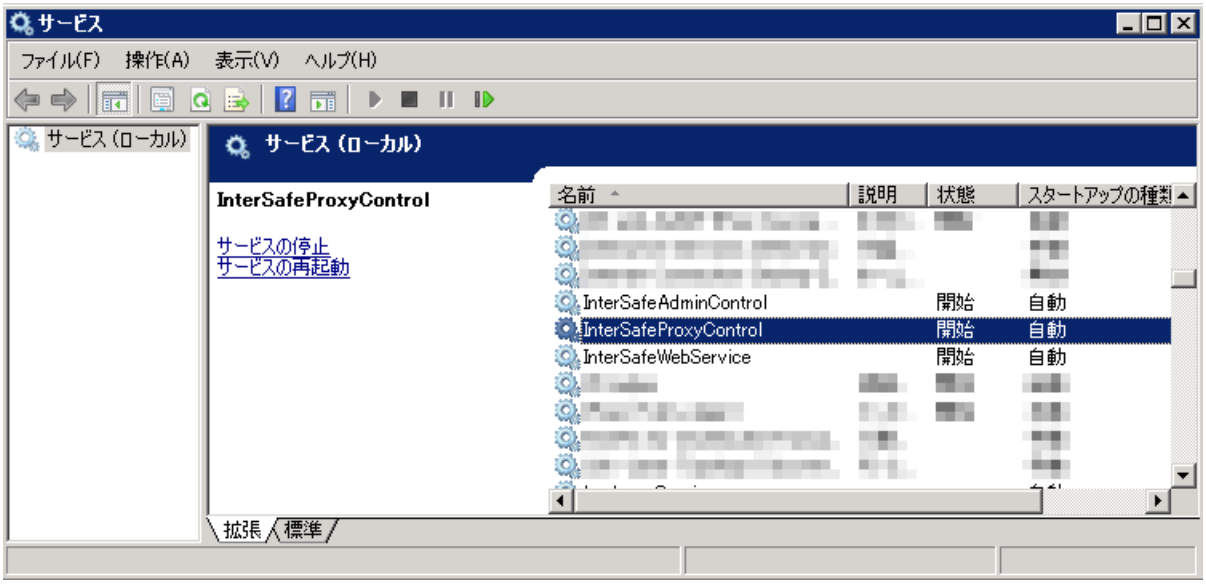
ISWF のフィルタリングサービス再起動

■Windows の場合

Windows 版でフィルタリングサービスを起動/停止するには、Windows の[コントロールパネル]の[サービス]を使用します。次の手順でフィルタリングサービスの起動と停止をします。

1) サービスの起動と停止を実行可能なユーザアカウントで Windows にログインします。
2) [スタート] ボタン→ [設定] → [コントロールパネル] → [管理ツール] の順に選択し、[サービス] をダブルクリックします。
3)「InterSafeProxyControl」(フィルタリングサービス)を右クリックして [操作] メニューの [開始] または [停止] を実行します。

図 3-3



■Solaris/Linux の場合

Solaris 版と Linux 版の ISWF のフィルタリングサービスを起動 / 停止する場合は、ターミナルで、次のコマンドを実行します。

● 起動 / 停止は root ユーザで実行してください。

フィルタリングサービスの再起動

起動：< インストールディレクトリ>/bin/amsproxy start

停止：< インストールディレクトリ>/bin/amsproxy stop

再起動後、現象が改善されているかご確認ください。

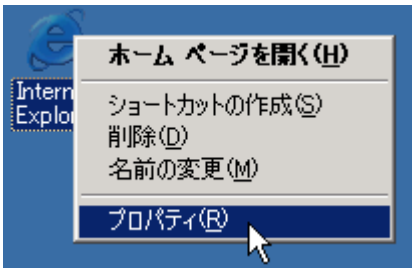
4.その他の回避策

Internet Explorer のプロキシ例外設定による回避

前述の手順で正常にアクセスできない場合には、プロキシ例外に該当のサイトを指定することで正常にアクセスが出来る場合があります。Internet Explorer の場合、下記のように設定を行います。

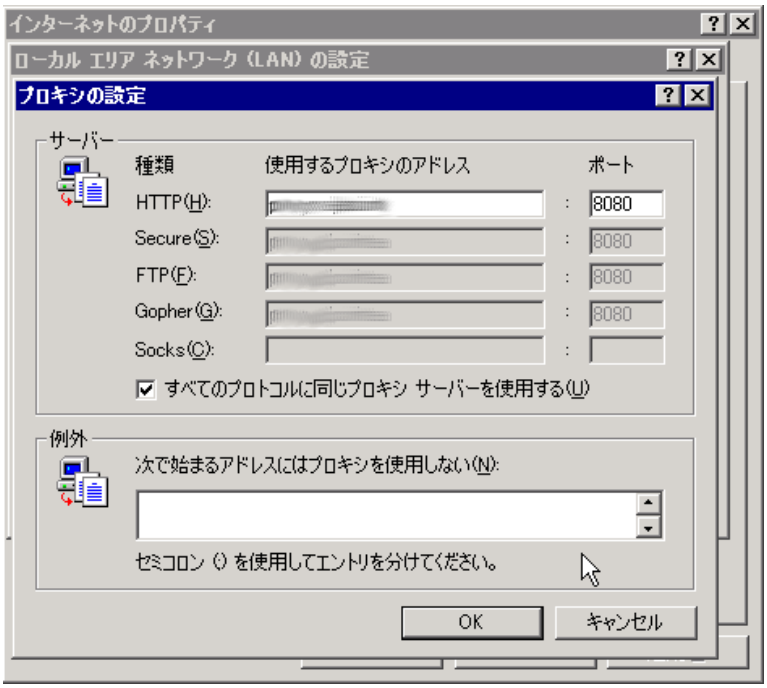
1) Internet Explorer のアイコンを右クリックしてプロパティを開きます。

図 4-1



2) 接続タブを開き、LAN の設定ボタンをクリックします。ローカルエリアネットワーク(LAN)の設定ダイアログが開くので詳細設定ボタンを開きます。下記の画面が表示されるので該当の URL、ドメイン名を例外フィールドに記述します。

図 4-2



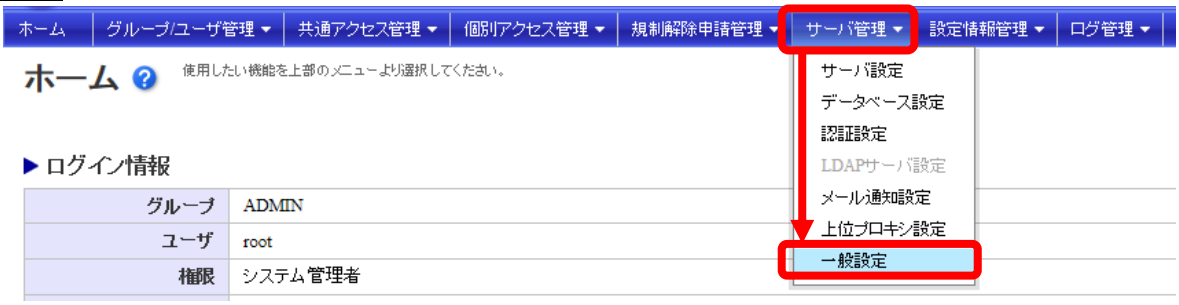
フィルタリングバイパス設定による回避

Ver8.5 SP1 以降の Proxy 版ではフィルタリングバイパス機能が追加されました。フィルタリングバイパスに設定された UA やホストへのリクエストは ISWF のフィルタリング処理の対象外となり、認証処理などすべての処理が行われません。

● フィルタリングバイパス設定に一致したリクエストはアクセスログに出力されません。

1) 管理画面にログイン後、[サーバ管理] > [一般設定] をクリックします。

図 4-3



2) 「フィルタリングバイパス設定」の「User-Agent」「宛先ホスト」に認証除外する UA/ホスト名を追加します。

図 4-4

3) 追加後、画面右上の[保存]ボタンをクリックし、設定を反映させます。

5.確認済み UA 及びホスト

UA 一覧

以下の表は、弊社サポートにて確認した UA の一覧になります。詳細が不明なものやプログラムのバージョンにより UA が異なる場合もあります。設定の際にご参考ください。

No.	UA	プログラム・サービス名	備考	ISWF による回避の可否
1	Acrobat	Acrobat 全般	Acrobat 全般	○
2	Solid Core	Adobe Flash Player インストール	UA による認証除外の設定のみでは回避不可。Ver6.5 より追加された「ホストによる認証除外設定」と「UA による認証除外設定」を両方設定することで回避可能。ホスト名一覧の No.4 を参照。	×
3	Adobe	Adobe 全般	Adobe 全般	○
4	Adobe Update Manager 6 Adobe Update Manager 5	Acrobat9 アップデータ Acrobat8 アップデータ	Acrobat アップデータ使用時。	○
5	GIZMO	Gizmo(インターネット電話)	Gizmo(インターネット電話)	○
6	tenki.rx	Goo ツールバー	Goo ツールバー	○
7	goostkver.rx	Goo ツールバー	Goo ツールバー	○
8	CATsecurity	InterSafe CATS	InterSafe CATS	○
9	Java	Java プログラム	Java プログラム	○
10	Managed VirusScan	McAfee(アンチウィルス)	McAfee(アンチウィルス)	○
11	VirusScan ASaP ConnectionCheck	McAfee(アンチウィルス)	McAfee(アンチウィルス)	○
12	dpupdchk	Microsoft IntelliPoint	Microsoft IntelliPoint	○
13	Microsoft	Microsoft 全般	Microsoft 全般	○
14	MicrosoftOffice Microsoft Office ClipOrganizer VCSoapClient CLView	MicrosoftOffice 全般	Office2007 以降の各アプリケーションの下記のような操作をすると認証 POPUP が表示される場合があること確認しております。 ①テキストを選択した後、マウスを右クリックしてコンテキストメニューを表示した場合 ②セキュリティ センターの設定を開いた場合 ③校閲を選択した場合 ④クリップアートで Web コレクションを検索する場合など ⑤オンラインでテンプレートを表示する場合 また、テンプレートが表示できない事象も確認されております。	○
15	NOD32 Update	NOD32(アンチウィルス)	NOD32(アンチウィルス)	○

16	Office Source Engine	Office Update	Office Update	○
17	Oracle Proxy Enabled SSL Socket	Oracle Client	Oracle Client	○
18	Shockwave	Shockwave	ショックウェーブ、マルチメディアのデータを再生するためのプラグイン	○
19	RwAAAAA	Symantec(アンチウィルス)	UA は可変するため、注意が必要。	可変した場合回避不可
20	SAAAAA	Symantec(アンチウィルス)	UA は可変するため、注意が必要。	可変した場合回避不可
21	LiveUpdate	Symantec ライブアップデート	シマンテック(アンチウィルス)のアップデート用プログラム	○
22	LegitCheck	Windows Genuine Advantage	正規 Windows 推奨プログラム	○
23	MS Clearing House Default Agent	Windows Genuine Advantage	正規 Windows 推奨プログラム	○
24	Windows-Media-DRM	Windows Media Player	ウィンドウズメディアプレーヤ	○
25	Windows-Media-Player	Windows Media Player	ウィンドウズメディアプレーヤ	○
26	NSPlayer	Windows Media Player(NetShow クライアント)	ウィンドウズメディアプレーヤ	○
27	SLSSoapClient	VistaOS Office2010	Vista の OS ライセンス認証 Office2010 のアクティベーション	○
28	Windows-Update-Agent Microsoft BITS Microsoft WU Client Windows Update Microsoft-CryptoAPI Windows Installer MSDW VCSoapClient	Windows Update	Windows アップデート	○
29	CryptRetriveObjectByUrl	Windows Update(Win98+IE6)	Windows アップデート、Windows98 と IE6 の組み合わせ	○
30	Industry Update Control	Windows Update(WinXP+IE6)	Windows アップデート、WindowsXP と IE6 の組み合わせ	○
31	Railupd	リアルプレイヤー	リアルプレイヤー	○
32	RealPlayer	リアルプレイヤー	リアルプレイヤー	○

33	e-Tax VersionUp Support Program	e-Tax	国税電子申告・納税システム（e-Tax）	○
34	Streaming	特定のプログラム	ユーザ独自のインターネット接続の Web カメラ用のプログラム。UA は「Streaming Sdk 1.0」、MJPEG モードのリクエストでは、UA が付加されないリクエストパターンが存在するので、全てのモードでリクエストを可能にするには IP アドレス認証が必要になります。	○
35	contype	特定のプログラム	ユーザ独自のプログラム ActiveX コントロールがこの UA の GET を送信する場合があるようです。特定のプログラムではない可能性があります。 参考 URL:http://support.microsoft.com/kb/416569/ja	○
36	anatagoyomi	特定のプログラム(あなたごよみ)	デスクトップツール(ガジェット)	○
37	SendHTTP	特定のプログラム	ユーザ独自のプログラム、詳細は不明。	○
38	Client	特定のプログラム	ユーザ独自のプログラム、詳細は不明。	○
39	fclock	特定のプログラム	データセキュリティ製品、詳細は不明。	○
40	Tcpwsd	特定のプログラム	ユーザ独自のプログラム、詳細は不明。	○
41	Vegas	特定のプログラム	ユーザ独自のプログラム、詳細は不明。	○
42	Win32	特定のプログラム	ユーザ独自のプログラム、詳細は不明。	○
43	ClipOrganizer	特定のプログラム	ユーザ独自のプログラム、詳細は不明。	○
44	IPC_Update	特定のプログラム	ユーザ独自のプログラム、詳細は不明。	○
45	jupdate	特定のプログラム	ユーザ独自のプログラム、詳細は不明。	○
46	Lotus-Notes	Lotus-Notes	Notes ブラウザ	○
47	Windows Live Messenger	Windows Live Messenger	MS メッセンジャー	○
48	Windows MSN Messenger	Windows MSN Messenger	MS メッセンジャー	○
49	Mozilla/4.0 (Windows 2000 5.0) Java/1.6.0_03	citibank（オンラインバンク）	ナビゲーションバーが表示されない	○
50	iCATs SOAP	ヤマト運輸送り状発行ソフト（B2）	NTLM だけではなくユーザ認証に対応していないとのメーカ回答（IP アドレス認証なら可能）	×
51	i-CATs DownLoad	ヤマト運輸送り状発行ソフト（B2）	NTLM だけではなくユーザ認証に対応していないとのメーカ回答（IP アドレス認証なら可能）	×

52	-	ThinkVantage System Update	特定の UA を持たないため回避ができない。	×
53	-	iPass Connect CISCO	特定の UA を持たない。	×
54	-	google パック	特定の UA を持たない。	×
55	-	Mcafee Managed Total Protection	詳細不明。	×
56	-	Logitech Desktop Messenger	詳細不明。	×
57	-	JWNET	特定の UA を持たない 認証ポップアップに正しい ID、パスワードを入力した場合は通る。	×
58	-	IT-Truck	「Biz/Browser」の UA を持っているが、 proxy.inf に登録しても回避が出来なかった。 原因は不明。	不明
59	-	iTERAN	特定の UA を持たないため回避ができない。	×
60	-	現場図書館 EX	特定の UA を持たない。	×
61	-	現場 Office	特定の UA を持たない。	×
62	urlgrabber/3.1.0	QuartusⅡ	開発ソフトウエア	○
63	its-moNavi PC	its-mo Navi	地図ソフトウエア	○
64	ZION	its-mo Navi	地図ソフトウエア	○
65	-	LeySer Services	詳細不明。	×
66	-	FedEX Ship Manager	UA 確認不可。	×
67	-	MATLAB	UA 確認不可。	×
68	Smc	Symantec Endpoint Protection	ウイルス・セキュリティ対策ソフト	○
69	CHTTP	KASHU-USB メモリのセキュリティ	USB 暗号化ソフトライセンス登録時のリクエスト時に認証失敗となるため UA 登録で回避。	○
70	-	弥生給与ソフト	ソフトアップデートのリクエストで認証失敗となる。UA 確認不可のため、ホスト名による認証除外で回避。	× ※ホスト名一覧の No.7 を参照

ホスト名一覧

以下の表は、弊社サポートにて確認したホスト名の一覧になります。詳細が不明なものやプログラムのバージョンによりホスト名が異なる場合もあります。設定の際にご参考ください。

No.	ホスト名	プログラム・サービス名	備考	ISWF による回避の可否
1	www.update.microsoft.com update.microsoft.com download.windowsupdate.com v4.download.windowsupdate.com fe3.delivery.mp.microsoft.com	Windows Update	Windows Update 時のリクエスト先	○
2	activation.sls.microsoft.com	Office2010/2013	Office2010/2013 のライセンス登録(アクティベーション)時のリクエスト先	○ ※UA 一覧の No.27 も必要。
3	office15client.microsoft.com	Office2013	Office2013によるテンプレート取得のためのバックグラウンドアクセス時のリクエスト先	○
4	get.adobe.com platformdl.adobe.com fpdownload.adobe.com fpdownload.macromedia.com dlmping.adobe.com dlmping2.adobe.com	Adobe Flash Player	Adobe Flash Player インストール時のリクエスト先	○
5	activate.adobe.com	Adobe 社製品	Adobe 社製品のライセンス認証の際のリクエスト先	○
6	www.google.com	Google Adwords Editor	Adwords Editor ソフト起動時の認証	○
7	www.yayoi-kk.co.jp info.yayoi-kk.co.jp	弥生給与ソフト	ソフトアップデートのリクエスト先	○
8	www.jprom.co.jp	JP-NET	検索サーバへ接続する際のリクエスト先	○
9	ardownload.adobe.com	Adobe Reader	Adobe Reader インストール/アップデート時のリクエスト先	○
10	odc.officeapps.live.com	Office2013	Office2013の起動時の送信されるリクエスト先	○