ALSI

[InterSafe WebFilter Ver8 Ver9]
Active Directory との連携

[Document Level 2]
ALPS SYSTEM INTEGRATION Co., LTD.
2019/02/05 version 1.0.4 Technical Support Section

目次

[InterSafe WebFilter Ver8 Ver9] ActiveDirectory との連携

変更履歴

変更日	ページ番号	変更内容
2013/5/7	P.16	「3-5-6.AD の 1000 以上のユーザを ISWF の認証で利用する場合」の手順を変更
2013/5/7	P.18	「3-5-7.複数の AD を登録する場合」
2015/9/11	P.5	Windows2012Server を追加
	P.16	「3-5-6.AD の 1000 以上のユーザを ISWF の認証で利用する場合」の条件を修正
2016/3/1	P.16	「3-5-6.AD の 1000 以上のユーザを ISWF の認証で利用する場合」の条件を修正
2019/2/5	表紙	Ver9 を追加
	P.17	「Ver8.0 Build0820 にて、IE7、IE9 で非表示にならない事象が確認されております。 この事象は以降のバージョンで修正されています。」に修正

1. はじめに

ISWFWebFilter（以下、ISWF と略します)には、LDAP サーバと連携しユーザ管理、ユーザ認証を行う機能があります。

本書では、一般的な LDAP サーバである Active Directory（以下、AD と略します）と連携する際の設定について説明します。

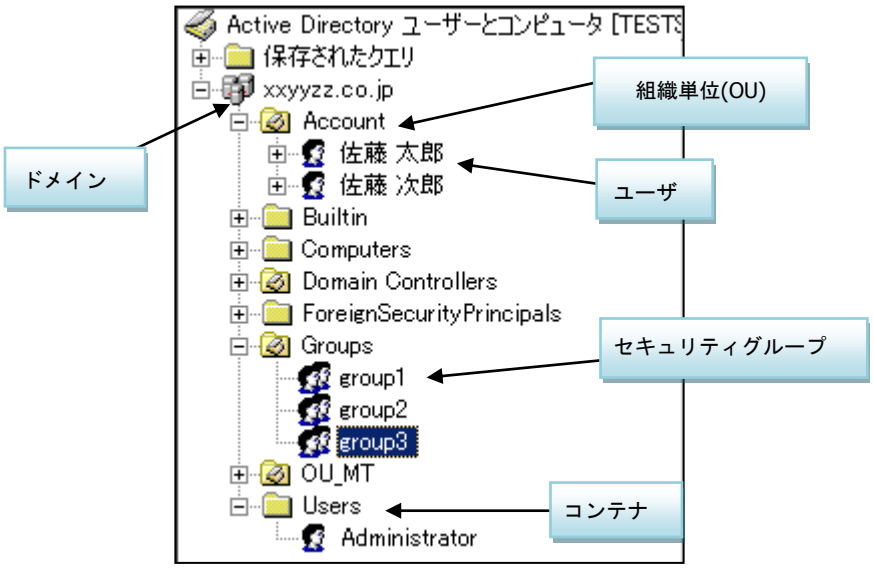
※本資料に記載されている会社名および商品名は、各社の商標もしくは登録商標です。

2. AD のオブジェクトと属性

この項では、ISWF との連携に必要な情報である、AD のオブジェクトと、その属性について説明します。

図 1 は、「Active Directory ユーザとコンピュータ」実行時のウィンドウの一部です。こちらから、AD に登録されているオブジェクトを確認できます。オブジェクトには、『ドメイン』『ユーザ』『組織単位(OU)』『コンテナ』や『セキュリティグループ』などがあります。

図 2-1



AD のオブジェクトを ISWF に取り込むためには、オブジェクトが持つ『属性』と『属性値』を条件に検索する必要があります。ISWF の「アカウント」「グループ」に対応する、AD のオブジェクトは、表 1 の通りです。

表 1

ISWF	AD のオブジェクト
アカウント	ユーザ
グループ	組織単位（OU）、セキュリティグループ、コンテナ

AD のオブジェクトが持つ主な『属性』や『属性値』については、表 2 を参照してください。なお、『属性値』が固定では無い変数を持つものは、表記しておりません。

表 2

アイコン		オブジェクト	属性	属性値
2003 Server	2008/2012 Server			
		ユーザ	CN	
			objectClass	user
			sAMAccountName	
			displayName	
		InetOrgPerson	CN	
			objectClass	InetOrgPerson
			objectClass	user
			givenName	
		連絡先	CN	
			objectClass	contact
			givenName	
		コンピュータ	CN	
			objectClass	computer
			objectClass	user
			sAMAccountName	
		組織単位（OU）	OU	
			objectClass	organizationalUnit
		コンテナ	CN	
			objectClass	builtinDomain
		グループ	CN	
			objectClass	group
			sAMAccountName	
		共有フォルダ	CN	
			objectClass	volume
			uNCName	
		共有プリンタ	CN	
			objectClass	printQueue
			uNCName	

3. ISWF と LDAP 認証の設定

ここでは、ISWF と LDAP（AD）を連携させ認証情報を利用するための設定方法について説明します。

3-1.ADと連携して認証するまでの流れ

1. 認証設定
   ISWF の認証を設定します。
   詳しくは、P.6「認証設定」を参照してください。

2. AD サーバ情報の登録
   ISWF と連携する AD サーバの情報を登録します。
   詳しくは、P.9「AD サーバ情報の設定」を参照してください。

3. ISWF のグループとの紐付け
   ISWF ではグループ単位にフィルタリングルールを設定します。そのため、ISWF のグループ情報と AD のグループ情報を紐付けする必要があります。
   詳しくは、P.12「ISWF のグループとの紐付け」を参照してください。

3-2.認証設定

最初に必要な設定は、ISWF の認証方法の選択です。設定方法は、まずユーザ認証を有効にしてから、ISWF 管理画面のメニューより[サーバ管理 > 認証設定]の[認証設定]画面において、[認証方式]にて、

- **【BASIC 認証】→【LDAP 連携を行う】**
- **【NTLM 認証】**

のどちらかを選択し、続いて[LDAP グループ特定方式]から、

- **【ユーザの DN からグループ階層を特定する】**
- **【グループ毎にユーザ抽出条件を指定する】**

の 2 種類から選択する必要があります。選択後[保存]ボタンを押下することで、[LDAP サーバ情報へ]リンクが有効になり、LDAP サーバと連携するための情報入力画面に移動する事が可能となります。

- LDAP とは、ディレクトリサービスを利用するための通信用のプロトコルです。Active Directory も LDAP の規格に従ったディレクトリサービスを提供するソフトウェアです。
- 【NTLM 認証】は Proxy 版のみの機能です。ICAP 版では表示されません。

図 3-1

■ **認証方式**

【BASIC 認証】→【LDAP 連携を行う】

Web アクセス時にユーザ名とパスワードの入力を求められ、ユーザ名とパスワードの確認がされて初めて、ユーザ毎に設定されたフィルタリングルールに沿って Web アクセスが可能になります。

LDAP サーバ連携の設定において、[LDAP サーバ情報]画面にて複数 LDAP サーバを登録した場合は、認証の優先順位を設定する必要があります。

【NTLM 認証】

シングル・サイン・オンが可能となり、Web アクセス時にユーザ名とパスワードの入力を求められません。

LDAP サーバ連携の設定においては、以下の様な違いがあります。

・[LDAP サーバ情報]画面において、【NTLM 認証】が選択された場合、[NetBIOS ドメイン名]を指定することができます。

・同じ NetBIOS ドメイン名で複数 LDAP サーバを登録した場合、[LDAP サーバ情報]画面において認証の優先順位を設定する必要はありません。

● シングル・サイン・オンとは OS へのログオン時のユーザ名とパスワードを利用することで、認証の必要なサービスの利用においてパスワードの入力を求めずに、認証が済む方式を指します。

■ **LDAP グループ特定方式**

【ユーザの DN からグループ階層を特定する】

AD の『組織単位(OU)』毎にフィルタリングルールを割り当てたい場合には、こちらを選択してください。

LDAP サーバ連携の設定においては、以下の様な違いがあります。

・[LDAP サーバ情報]画面に、項目【自動連携設定】【連携情報更新】が表示されます。

・[LDAP サーバ登録/編集]画面にて、[アカウント]と[グループ]の検索条件を設定する必要があります。

● DN とは Distinguished Name の略称であり、識別名とも言います。DN はユーザオブジェクトの属性として持っている値です。

【グループ毎にユーザ抽出条件を指定する】

AD の『セキュリティグループ』毎等、属性の値毎にフィルタリングルールを割り当てたい場合には、こちらを選択してくだ

さい。LDAP サーバ連携の設定においては、以下の様な違いがあります。

・[LDAP サーバ情報]画面に、【自動連携設定】【連携情報更新】が表示されません。

・[LDAP サーバ登録/編集]画面にて、[アカウント]のみ検索条件を設定する必要があります。

図 3-2、図 3-3 は、認証方式やグループ特定方式違いによる設定画面違いを表しています。

図 3-2 LDAP サーバ設定画面

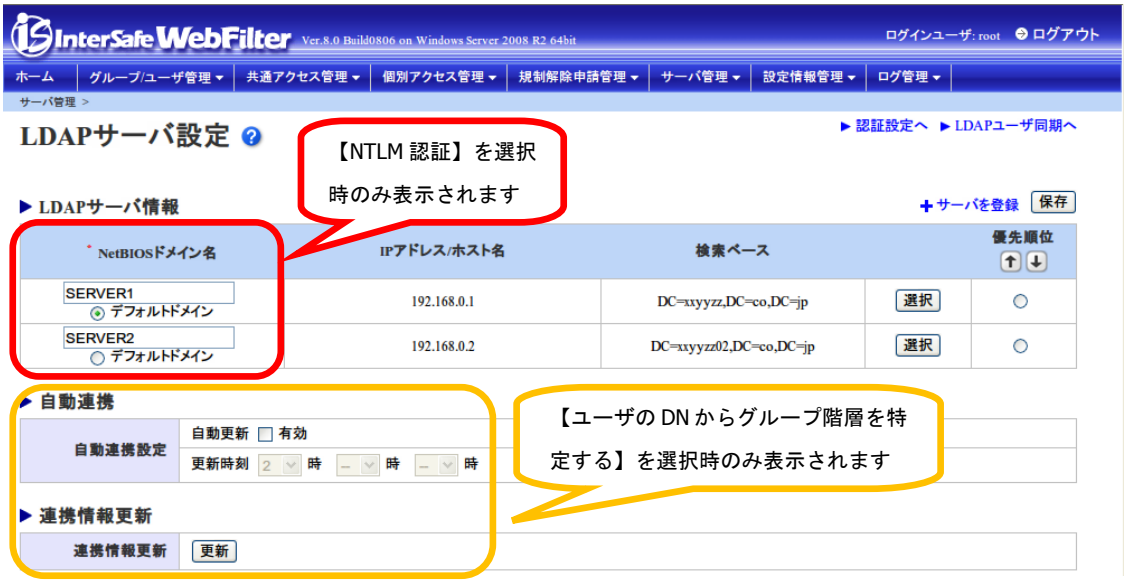


図 3-3 LDAP サーバ登録/編集画面

3-3.ADサーバ情報の設定

認証方式を選択後は、ISWF と連携する AD サーバの情報を登録する必要があります。AD サーバの情報の登録は、メニューより[サーバ管理 ＞LDAP サーバ設定](図 3-4)をクリックするか、[認証設定]画面の右上にある[LDAP サーバ設定へ]をクリックし、[LDAP サーバ設定]画面中にある[＋ サーバを登録](図 3-5)をクリックしてください。クリック後、[LDAP サーバ登録/編集]画面(図 3-3)に移ります。

図 3-4

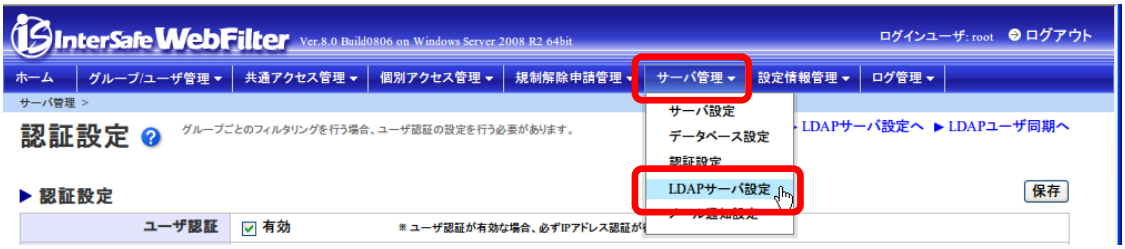


図 3-5

[LDAP サーバ登録/編集]画面(図 3-3)にて LDAP サーバと連携するための情報を入力します。各項目については、表 3 を参考にしてください。

- LDAP サーバは、最大 10 台まで登録可能です。

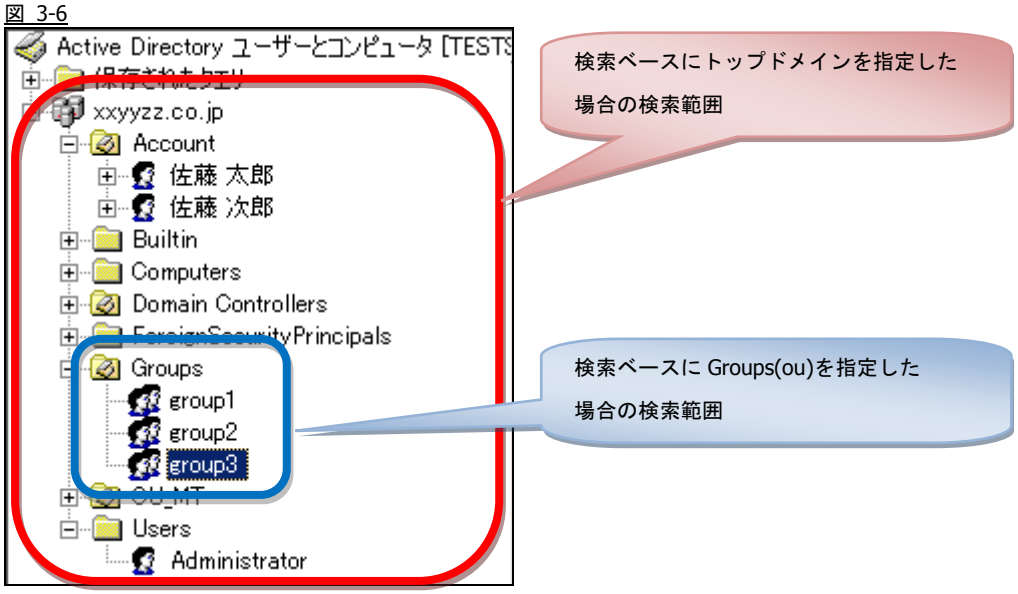
表 3

項目	内容
NetBIOS ドメイン名（NTLM 認証設定時のみ利用）	Active Directory で設定した NetBIOS ドメイン名を入力します。 新しい NetBIOS ドメインを登録する場合、[新規登録]をクリックし、NetBIOS ドメイン名を 15 文字以内の半角英数字、大文字で入力します。 登録済みドメイン名から選択する場合、[登録済み]をクリックし、プルダウンメニューからドメイン名を選択します。 ● 同じドメインの LDAP サーバを複数登録する場合は、各サーバの NetBIOS ドメイン名を、必ず、正しい名称に統一してください。
IP アドレス	LDAP サーバの IP アドレスまたはドメイン名を入力します。
ポート	LDAP サーバの接続ポート番号を入力してください。 初期値は「389」です。
検索ベース(※)	LDAP サーバの BASE 情報を DN で入力します。
管理者アカウント	LDAP サーバのアカウントを DN で入力します。
パスワード	指定した管理者アカウントのパスワードを入力します。
パスワード (確認)	パスワードの確認入力をします。

(※)検索ベースの設定について

検索ベースとは、ISWF が AD を検索するための基準となる位置です。ISWF で認証したいユーザが含まれるように設定する必要があります。

図 3-6



例えば、図 3-6 のトップドメイン（dc=xxyyzz,dc=co,dc=jp）を検索ベースに指定した場合、トップドメイン以下が全て検索の対象となります。Groups というグループ（ou=Groups,dc=xxyyzz,dc=co,dc=jp）を検索ベースに指定した場合は、Groups 以下が検索の対象となります。

以下に、入力の例を掲載します。

AD サーバの『システムのプロパティ』の情報が図 3-7 の通りとした場合、ISWF 側の設定内容は図 3-8 の通りとなります。

● 【検索ベース】【管理者アカウント】の情報については、P.4「2. AD のオブジェクトと属性」も参考にしてください。

図 3-7

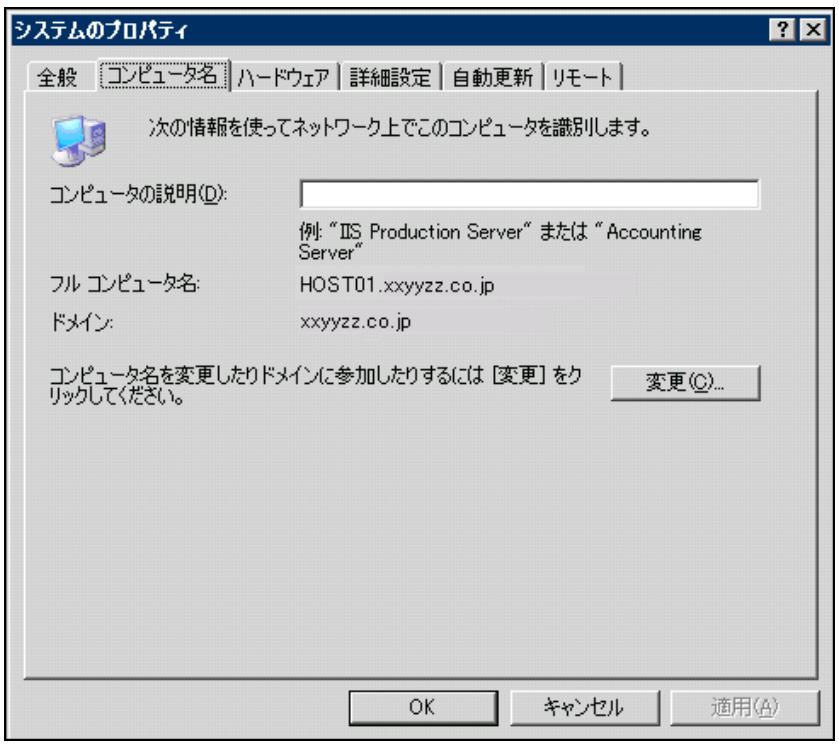


図 3-8

表 4

項目		内容
NetBIOS ドメイン名 (NTLM 認証設定時のみ表示)		HOST01
IP アドレス (またはドメイン名)		192.168.0.1 (または、HOST01.xxyyzz.co.jp)
ポート		389
検索ベース		DC=xxyyzz, DC=co, DC=jp
管理者アカウント		CN=Administrator, CN=Users, DC=xxyyzz, DC=co, DC=jp
パスワード		管理者アカウントのパスワードを入力します。
検索条件	アカウント	ユーザアカウントの検索条件とスキーマをそれぞれ設定します。
	グループ (ユーザの DN からグループ階層を特定する場合のみ表示)	グループの検索条件とスキーマをそれぞれ設定します。

3-4.ISWFのグループとの紐付け

AD サーバの登録完了後、AD に登録されているアカウントを利用して ISWF で認証を行うためには、ISWF の[グループ]と AD のグループ情報を連携する(紐付ける)必要があります。

● 紐付ける方法については図 3-1 の[LDAP グループ特定方式]の選択によって異なります。

3-4-1.LDAP グループ特定方式：【ユーザの DN からグループ階層を特定する】の場合

AD の組織単位(OU)を ISWF の[グループ]として登録します。手順は以下の通りです。

1) ISWF 管理画面のメニューより[サーバ管理 ＞ LDAP サーバ設定]をクリックします。
2) [LDAP サーバ設定]画面（図 3-2）中にある、[▶ 連携情報更新]の[更新]ボタンをクリックします。
3) ISWF 管理画面の[グループ/ユーザ管理]画面にて、新規にグループが登録されていることを確認します。

3-4-2.LDAP グループ特定方式：【グループ毎にユーザ抽出条件を指定する】の場合

AD のセキュリティグループ]所属するユーザを ISWF のアカウントとして利用するには、【グループ毎にユーザ抽出条件を指定する】を選択した上で、ISWF のグループの[LDAP グループ特定条件]に抽出条件を指定します。手順は以下の通りです。

1) ISWF 管理画面のメニューより[グループ/ユーザ管理 ＞ グループ管理]をクリックします。
2) [グループ管理]画面でセキュリティグループと連携させたいグループを選択し(グループがない場合は新規作成して)、[LDAP 設定]タブをクリックし、[編集]ボタンをクリックします。

図 3-9

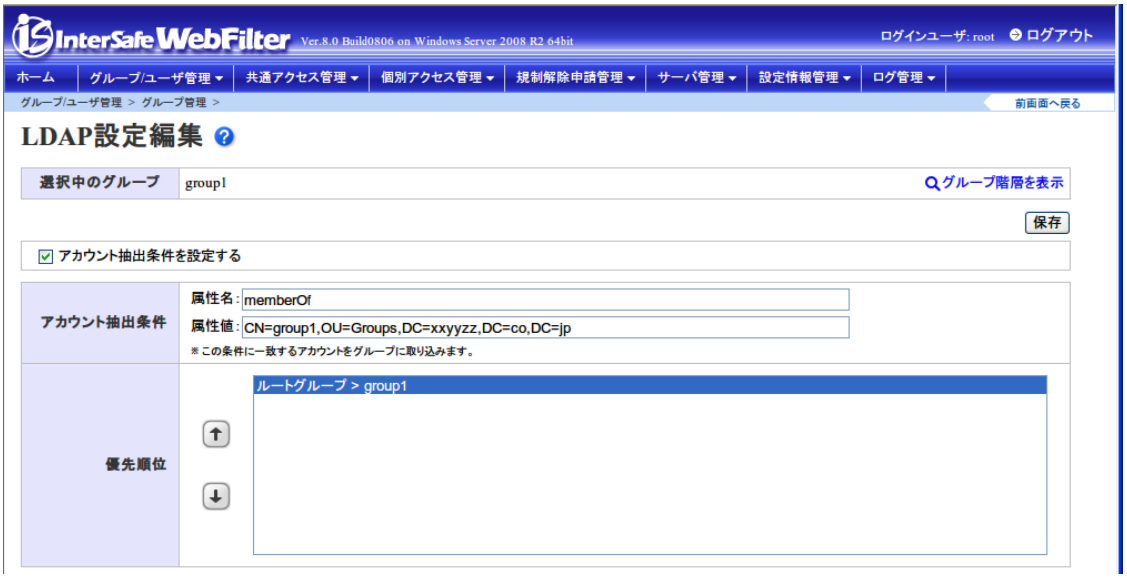
3) [LDAP 設定編集]画面にて、「アカウント抽出条件を設定する」にチェックを入れます。
4) アカウント抽出条件では「属性名」に『memberOf』を、「属性値」に該当『セキュリティグループ』の DN を記載してください。

例えば、図 2-1 にある『group1』に所属するユーザを取り込む場合、『属性値』は、以下のようになります。

CN=group1,OU=Groups,DC=xxyyzz,DC=co,DC=jp

● セキュリティグループに所属するユーザは、属性『memberOf』を持ち、その値はセキュリティグループの DN と同じになります。

図 3-10



.

5) [保存]ボタンをクリックし、設定した内容を保存します。

3-4-3.AD との連携確認

3-4-1.や 3-4-2.で設定した内容で、AD との連携が正常に行われているかどうかを確認します。

1) ISWF 管理画面の[認証設定]/[LDAP サーバ設定]画面の右上にある[LDAP ユーザ同期へ]をクリックします。(図 3-1、図 3-2 を参照)

2) [LDAP 同期設定]画面の[▸ ユーザ情報同期]にて、「未登録アカウント一覧」に AD に登録されているユーザが表示されていることを確認してください。表示されましたら、連携成功です。

図 3-11

- LDAP グループ特定方式が【ユーザの DN からグループ階層を特定する】の場合、AD の組織単位(OU)が ISWF の[グループ]となり、AD のユーザが ISWF の[アカウント]として表示されます。
- LDAP グループ特定方式が【グループ毎にユーザ抽出条件を指定する】の場合、ISWF で抽出条件付けしたグループが[グループ]となり、抽出条件にヒットした AD のユーザが ISWF の[アカウント]として表示されます。
- ISWF の検索ベース配下に所属して、かつグループの紐付けができなかったユーザで検索ベース直下に所属する AD ユーザは、ISWF の「LDAP」グループのアカウントとして表示されます。

図 3-11 のように「未登録アカウント一覧に表示されたアカウントは、「連携できていないアカウント」ではなく、「AD 上に存在していて ISWF 上に登録されていないアカウント」を示しております。

この画面での未アカウント登録は必須ではありません。

・グループ管理者のアカウントを設定したい。

・アカウントにメールアドレスを設定したい。

・OU（もしくはセキュリティグループ）の特定のユーザに限り別のフィルタリングルールを適用したい。

などの理由がある場合は、登録を行ってください。

なお、LDAP グループ特定方式が【ユーザの DN からグループ階層を特定する】の場合、AD 側の制限により、AD の 1000 以上のユーザで認証できない場合があります。1000 以上のユーザで認証する場合は、「3-5-6.AD の 1000 以上のユーザを ISWF の認証で利用する場合」を参考に設定変更を行ってください。

3-5.注意事項

3-5-1.AD の情報の変更

AD との連携において AD の情報に変更があった場合、以下のような点に注意してください。

■ **AD にてユーザの追加や削除、または別の OU やセキュリティグループにユーザを移動した場合**

・ AD から ISWF にユーザを登録している場合

AD の情報に合わせて ISWF に登録されているユーザを手動で別グループへ移行、削除する必要があります。

・ AD から ISWF にユーザを登録していない場合

特に作業は発生しません。

■ **AD にて OU やセキュリティグループが移動された場合**

・ LDAP グループ特定方式が【ユーザの DN からグループ階層を特定する】の場合

[LDAP サーバ設定]画面(図 3-2)中にある、[▶ 連携情報更新]の[更新]ボタンをクリックします。

・ LDAP グループ特定方式が【グループ毎にユーザ抽出条件を指定する】の場合

既存の ISWF のグループの抽出条件を変更する、もしくは、ISWF にグループを新規作成し抽出条件を設定します。

● 移動前のグループは ISWF に残るため、手動で削除する必要があります。

■ **AD にて OU やセキュリティグループが削除された場合**

ISWF 側も AD に合わせて手動でグループを削除する必要があります。

3-5-2.NTLM 認証時ドメイン不参加のクライアントとの共存

NTLM 認証時にネットワーク内にドメイン不参加のクライアントが存在した場合、どのように認証するかについて説明します。

■ **AD に同名のユーザが存在する場合**

Windows にログインしたユーザと同じ名前のユーザが AD に存在する場合、ドメイン不参加であっても認証が可能です。

複数の AD と連携している場合は、デフォルトドメインで指定している AD に Windows にログインしたユーザと同じユーザが存在すれば認証が可能です。

■ **未登録ユーザを利用する**

LDAP 連携時(NTLM 認証を含む)、ISWF のローカルに登録されているアカウントと AD に登録されているアカウント以外は無効なアカウントとして扱われ、未登録ユーザとして扱うことができます。また、未登録ユーザ用にフィルタリングルールを適用することが可能です。

未登録ユーザの設定方法は図 3-1 を参考に「未登録ユーザ設定」のチェックを有効にしてください。

■ **IP アドレス認証を利用する場合**

IP アドレス認証はアカウント認証より先に行われるため、ドメインに不参加であっても予め登録しておいた IP アドレスで認証され、フィルタリングルールを適用することが可能です。

IP アドレスの追加方法は、InterSafe WebFilter の管理者マニュアルの「3-4. ユーザの登録と管理」をご参照ください。

3-5-3.【NTLM 認証】を利用する場合

・ NTLM 認証時は、LDAP 連携のため検索条件で、アカウントを「sAMAccountName」に設定してください。
検索条件でアカウントを「cn」に設定している場合、正しくアカウントが検索されません。

・ 環境によっては NTLM 認証が正常に動作しない場合、ISWF の以下設定ファイルを編集して下さい。
/<ISWF インストールフォルダ>/conf/proxy.inf
[LDAP]
ENABLE_NTLM_KEEPALIVE=FALSE （この 1 行を追記して下さい）
＊追記後は ISWF のサービスを全て再起動して下さい。

3-5-4.『セキュリティグループ』を抽出条件に利用する場合

AD ユーザのプロパティにて、[所属するグループ]タブのセキュリティグループを[プライマリグループの設定]に設定すると、セキュリティグループのユーザ抽出条件である『memberOf』属性の値が削除されてしまうため、AD 側の当該ユーザは ISWF 上では「LDAP」グループのユーザとして認識されます。

3-5-5.ISWF で使用できないコマンド

LDAP 連携中、ISWF のコマンドで使用できないコマンドは以下の通りです。

・ amsaccount

3-5-6.AD の 1000 以上のユーザを ISWF の認証で利用する場合

ISWF にて Active Directory（AD）連携を行う時、AD に 1000 件以上のユーザが存在する場合には、以下のような問題が発生することがあります。
①グループ特定方式を「ユーザの DN からグループ階層を特定する」にし、連携情報更新をした際、1000 件以降のユーザの所属 OU が ISWF 側のグループとして作成されません。グループが作成されないとその OU に所属するユーザは認証に失敗します。※グループ特定方式が「グループ毎にユーザ抽出条件を指定する」の 場合は該当しません。

②管理画面の[サーバ管理]-[認証設定]-[LDAP サーバ同期へ]（※）の未登録ユーザに、1000 件分のユーザしか表示されずに InterSafe WebFilter にユーザが登録できない。
※Ver7.0 までは、[システム管理]-[認証設定]-[LDAP 同期設定へ]です。
※グループ特定方式が「ユーザの DN からグループ階層を特定する」 「グループ毎にユーザ抽出条件を指定する」のどちらでもユーザが 所属するグループが ISWF にすでにグループとして存在する場合は、 未登録ユーザに表示されていなくても認証は可能です。

それぞれの処理では、ISWF から AD に対しクエリーが実行されますが、この際 AD 側の設定（MaxPageSize）によりクエリーの最初の 1000 件のみが ISWF に返るため、上記の事象が発生します。
これらの事象を回避する方法は、下記の２つがあります。

■ その 1：ISWF の OVER_MAXPAGESIZE=TRUE を設定する。（Ver5.0 以降）(①の対処)

ISWF の以下の設定ファイルを編集して下さい。
/<ISWF インストールフォルダ>/conf/proxy.inf
[LDAP]
OVER_MAXPAGESIZE=TRUE （この 1 行を追記して下さい）
＊追記後は ISWF の全てのサービスを再起動して下さい。
＊OVER_MAXPAGESIZE=TRUE の場合、LDAP 同期設定画面は非表示になります。

● 変更により以下の影響があります。

・連携情報更新を行った際、ユーザの有無に関わらず検索ベース配下全ての OU をグループとして作成します。

（FALSE の場合は、検索ベース配下の OU の内、ユーザが所属している OU だけをグループとして作成します。）

・[サーバ管理]-[認証設定]-[LDAP サーバ同期へ]の画面が非表示（リンクが無効）になります。

（Ver8.0 Build0820 にて、IE7、IE9 で非表示にならない事象が確認されております。

この事象は以降のバージョンで修正されています。）

これらの影響を与えたくない場合は、その 2 をご検討ください。

■ その 2：AD の MaxPagesize を変更する。(①②共通の対処)

1) AD サーバにて、「ファイル名を指定して実行」より下記コマンドを実行します。

NTDSUTIL

2) 上記コマンド実行直後、ウィンドウが起動しましたら、下記 3 つのコマンドを順次入力してください。

```
C:¥WINNT¥system32¥ntdsutil.exe: LDAP policies
ldap policy: Connections
server connections: Connect to Server ホスト名
```

3) Quit コマンドを入力した後、Show Values コマンドで現在の値を確認してください。

「MaxPageSize」が一度に取得できる値です。

```
server connections: quit
ldap policy: show values
```

----------略

```
MaxActiveQueries                20
MaxPageSize                   1000
MaxQueryDuration               120
```

----------略

4) Set Maxpagesize to コマンドで、MaxPageSize の値を変更し、変更した値を反映させます。(例 8000)

```
ldap policy: Set Maxpagesize to 8000
ldap policy: Commit Changes
```

5) 値が変更されたかどうか確認します。

```
ldap policy: show values
```

----------略

```
MaxActiveQueries                20
MaxPageSize                   8000
MaxQueryDuration               120
```

----------略

3-5-7.複数の AD を登録する場合

ISWF には AD サーバの複数登録が可能ですが、冗長機能はございません。複数の AD を登録しても、必ず登録順（上から下）に問い合わせを行います。問い合わせ先の AD サーバの状態によっては、遅延が発生する場合がございます。

図 3-12 NTLM 認証で、「HOST01」という NetBIOS ドメイン名の AD サーバを 2 台登録していた場合

■ 問い合わせ先の AD がダウンしていた場合の ISWF の動作

・パターン A

問い合わせ先の AD サーバ（OS）自体は稼動しており、ポート(389,445)が LISTEN していない状態。

→即座に接続失敗と判断し、2 番目以降の AD サーバへ接続を行います。

・パターン B

問い合わせ先の AD サーバ（OS）自体は稼動しており、ポート(389,445)が LISTEN しているが、応答が無い状態。もしくは電源 OFF の状態。

→OS 側の挙動（TCP 再送など）の影響により、即座に問い合わせ失敗とは判断されません。一定時間経過後、2 番目以降の AD サーバへ接続を行います。失敗と判断する時間は OS に依存します。

● パターン B の状態となった場合は、以下の方法で復旧を行ってください。

1. ISWF の管理画面の[サーバ管理]＞[LDAP サーバ設定]にてダウンした AD サーバを削除する。

2.ISWF の全サービスの再起動を行う。

3.AD サーバが復旧した後、ISWF の管理画面の[サーバ管理]＞[LDAP サーバ設定]にて AD サーバを再登録する。

4.ICAP 版における運用例

ここでは、ICAP 版 ISWF と AD との連携方法や、AD 連携の注意点について説明します。
なお、ICAP 版では ICAP クライアント側で NTLM 認証を行う必要があり、ISWF ではその認証情報を元に BASIC 認証を行う仕様になっております。

4-1.BlueCoatを用いたシングルサインオン

ここでは、BlueCoat SG OS と ISWF for ICAP を用いて、AD と連携しシングルサインオン(SSO)を実現する方法について説明します。なお、以下の条件を満たしていることが前提となります。

1. ISWF において[サーバ管理] > [認証設定]の設定が完了していること
2. AD から ISWF にグループの取り込みが完了していること
3. ISWF においてフィルタリングルールの設定が完了していること
4. InterSafe WebFilter の管理者マニュアルの付録「C. ICAP クライアントでの NTLM 認証」の設定が完了していること
5. BlueCoat において『Network』の設定、及び、『Authentication』 > 『Console Access』の設定が完了していること

- 以下、「4-1-4.BCAAA のインストール」までの説明は ICAP クライアントについての説明になります。
- 本章で使用している BlueCoat の OS は SGOS5.4.6.1 です。SGOS5.4.6.1 より前のバージョンをご利用の場合、画面など一部違う場合がございますが、予めご了承ください。
- ICAP クライアントの設定については動作を保証するものではありません。ICAP クライアントの詳細につきましては ICAP クライアントのサポート窓口までお問い合わせください。

4-1-1.ICAP サーバの設定

認証情報を ICAP サーバに転送するため、ICAP サービス設定ダイアログ画面でオプション設定の設定を行ってください。
(ICAP サーバの設定については、InterSafe WebFilter の管理者マニュアルの「1-5. ICAP クライアントの設定」を参照し設定を行ってください。)

表 5

項目名	設定値 / 設定内容
Server URL	icap://<ISWF サーバの IP アドレス>:<ICAP ポート>/ ICAP ポートはデフォルト値(1344)の場合省略可能です。
Method supported	○request modification を選択します。
Send	□Authenticated user、□Authenticated groups にチェックを入れます。

4-1-2.認証設定

1) BlueCoat の管理画面より『Authentication』 > 『IWA』を選択し[New]ボタンをクリックします。

2) 「Realm name」「Primary server host」の項目を入力し、[OK]ボタンをクリックします。

図 4-1

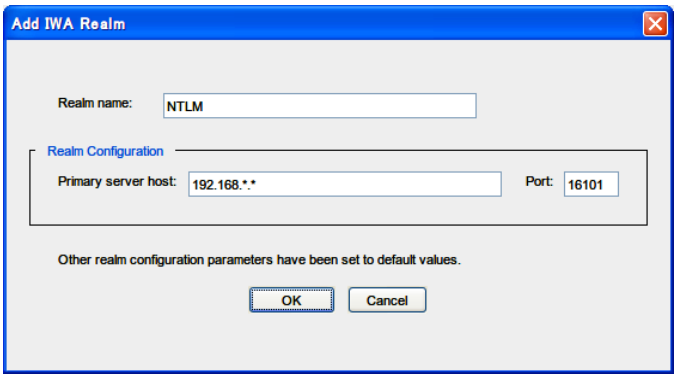
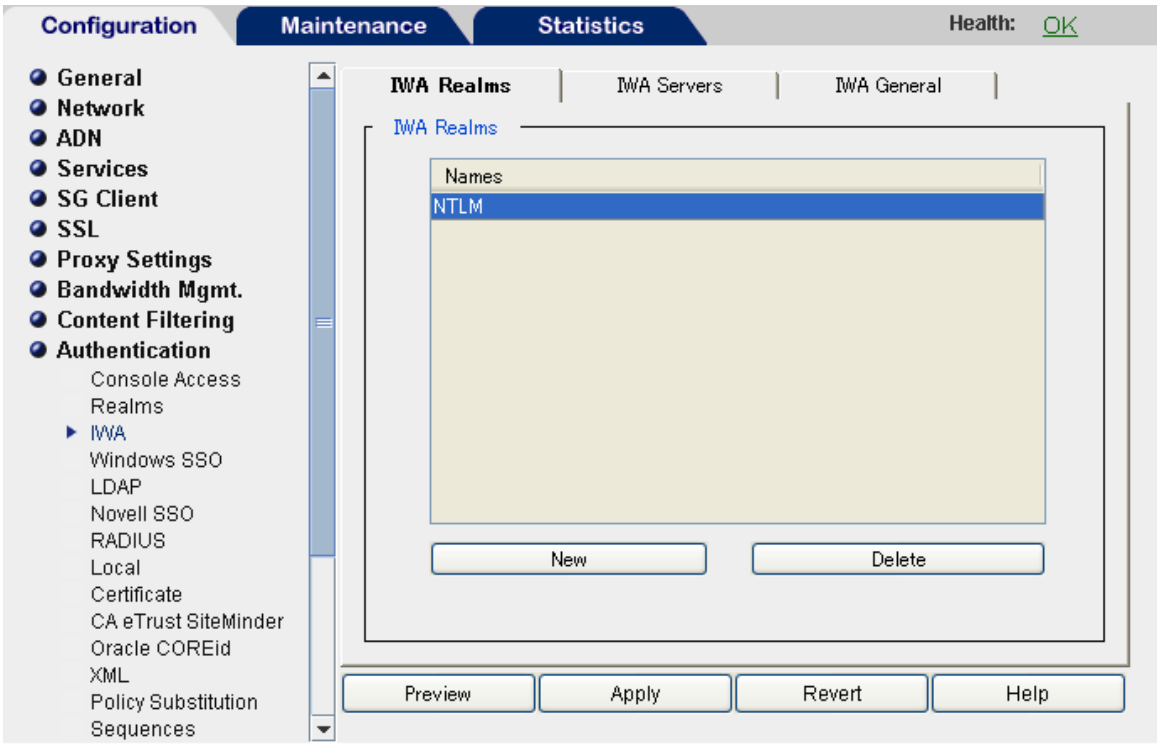


表 6

項目名	内容
Realm name	任意の名前
Primary server host	AD がインストールされているサーバの IP アドレス

3) [Apply]ボタンをクリックして、設定を反映させます。

図 4-2

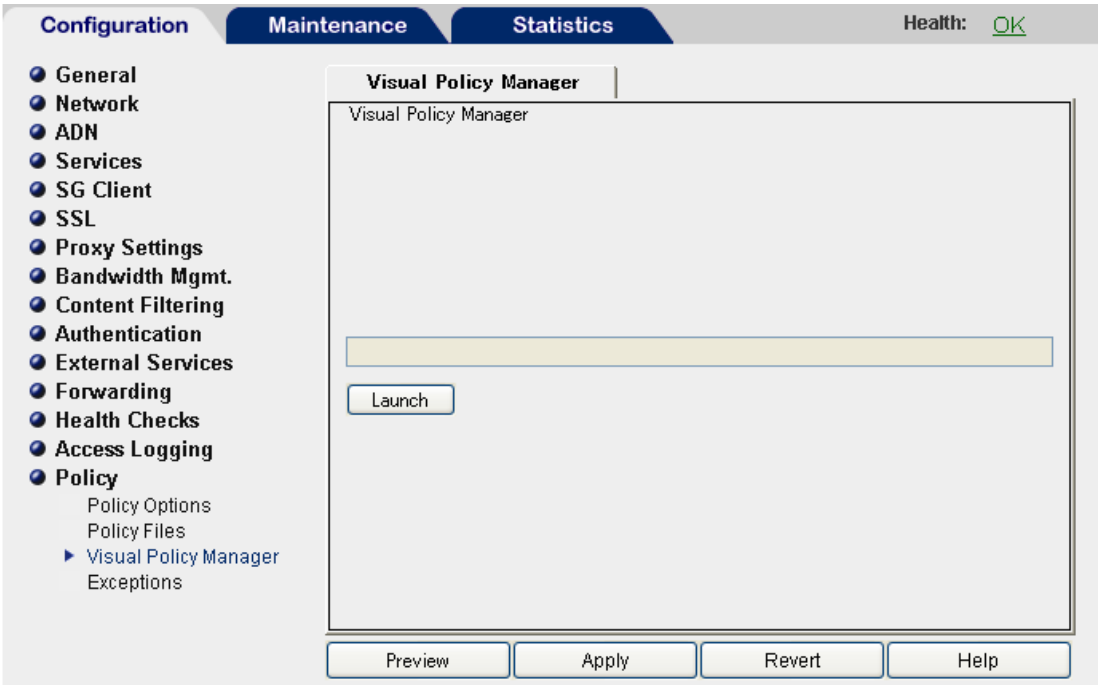


4-1-3.Policy の設定

BlueCoat の『Visual Policy Manager』（以下、VPM と略します）を利用して Policy の設定を行います。

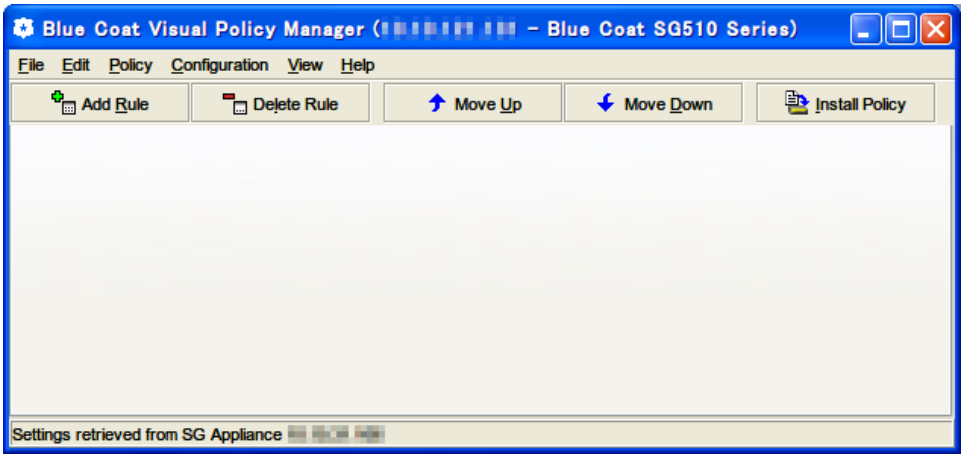
1) BlueCoat の管理画面より、『Policy』 > 『Visual Policy Manager』を選択し、[Launch]ボタンをクリックします。

図 4-3



2) VPM の設定画面が起動します。

図 4-4



■ 【Web Access Layer】の設定

ここでは BlueCoat で Web アクセスする際のルールを設定します。

1) VPM のメニューより『Policy』 > 『Add Web Access Layer』を選択します。

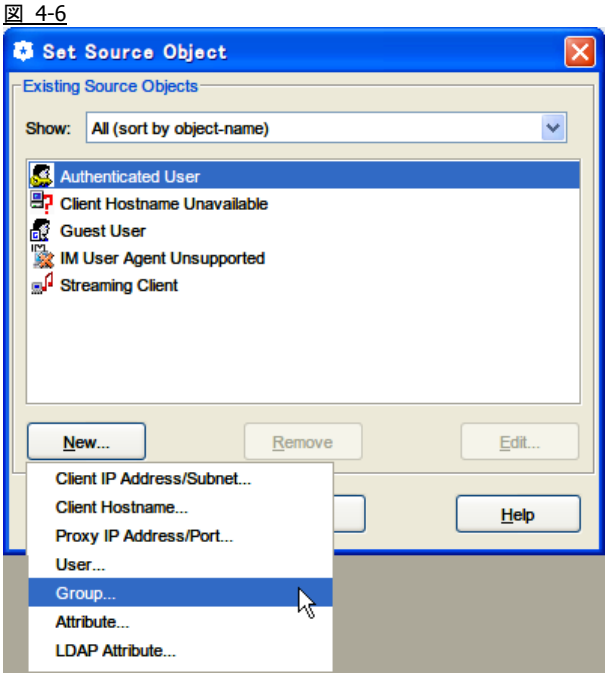
2) 『Add New Layer』で「Layer Name」を入力し[了解]ボタンをクリックします。

図 4-5

3) 作成された Layer の「Source」の項にて右クリックし、「Set」を選択します。

4) 『Set Source Object』の[New]ボタンをクリックし表示される一覧の中から Object を選択します。
この時、認証の対象が個々のユーザであれば、「User」を選択し、グループが対象であれば「Group」を選択します。
ここでは、「Group」を選択して説明します。

図 4-6



5) 『Add Group Object』にてグループの設定を行います。

図 4-7

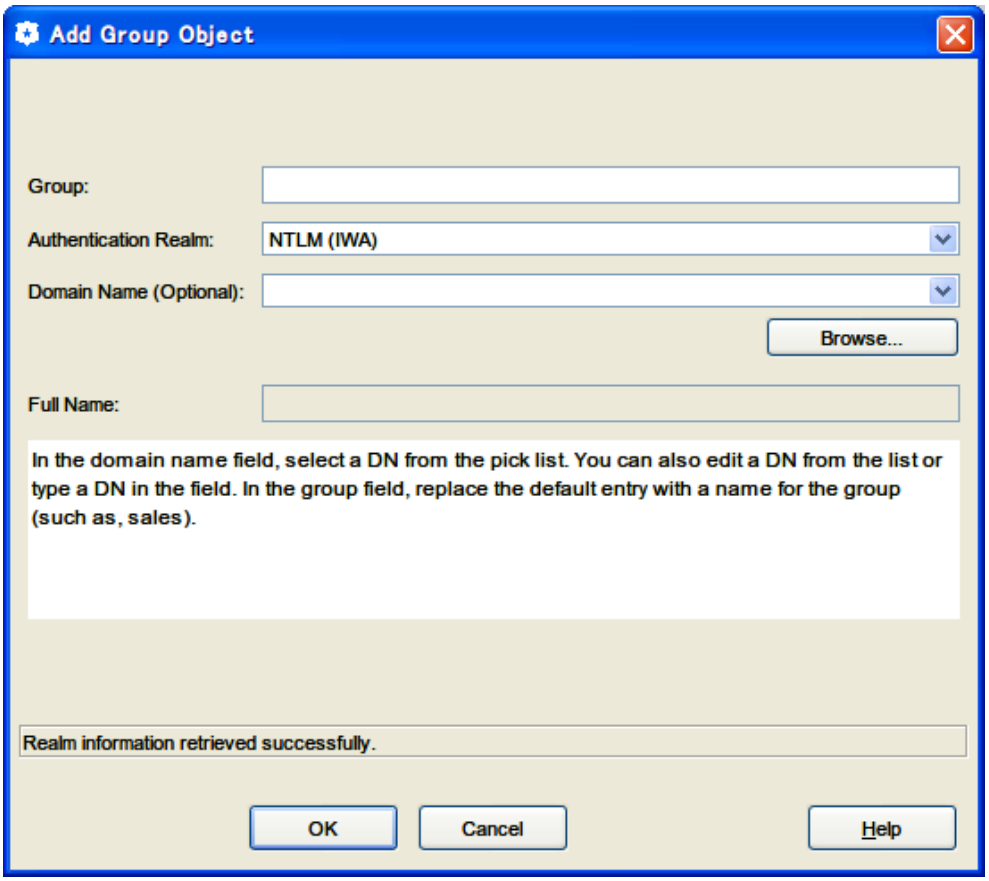


表 7

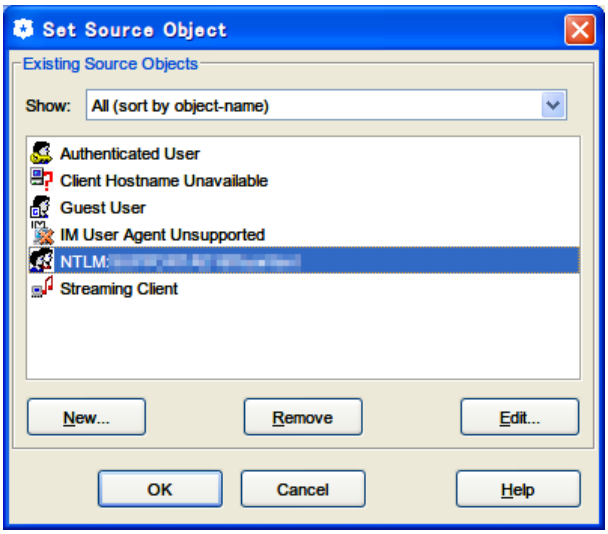
項目名	設定値
Group	Directory に登録されていて、BlueCoat にて認証の対象としたいグループ名を入力します。※1
Authentication Realm	P.20「4-1-2.認証設定」にて設定した Realm を選択します。
Domain Name (Optional)	ドメイン名を入力します。※1

- ※1 これらの項目は[Browse…]ボタンをクリックすることで、項目から選択入力することもできます。
- 対象となるグループが複数存在する場合には、VPM のメインウィンドウの上部にある[Add Rule]ボタンをクリックすると、新たなグループを登録することが可能です。

6) グループを設定後、[OK]ボタンをクリックします。

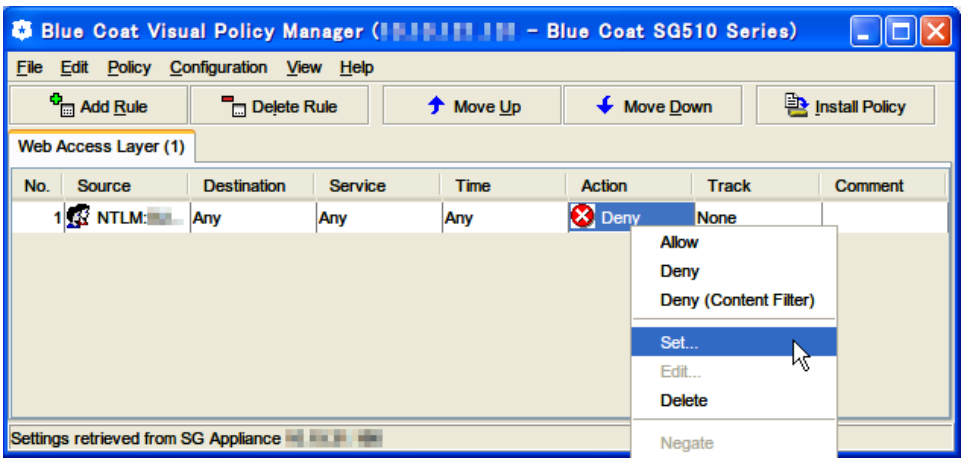
7) 『Set Source Object』の一覧に先程作成した Group Object が追加されますので、選択して[OK]ボタンをクリックします。

図 4-8



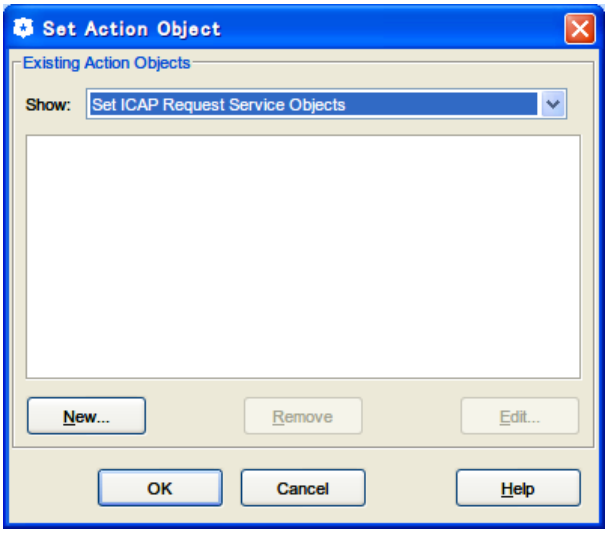
8) 次に「Action」の項にて右クリックし、「Set」を選択します。

図 4-9



9) 『Set Action Object』の『Show』で「Set ICAP Request Service Objects」を選択します。一覧の中に「ICAPRequestService」がない場合、[New]ボタンをクリックし表示される一覧の中から「Set ICAP Request Service…」を選択し新しい Object を作成します。すでに一覧に「ICAPRequestService」がある場合は、「ICAPRequestService」を選択後[Edit]ボタンをクリックします。

図 4-10



10) ICAP サーバの設定を行い、［OK］ボタンをクリックします。

図 4-11

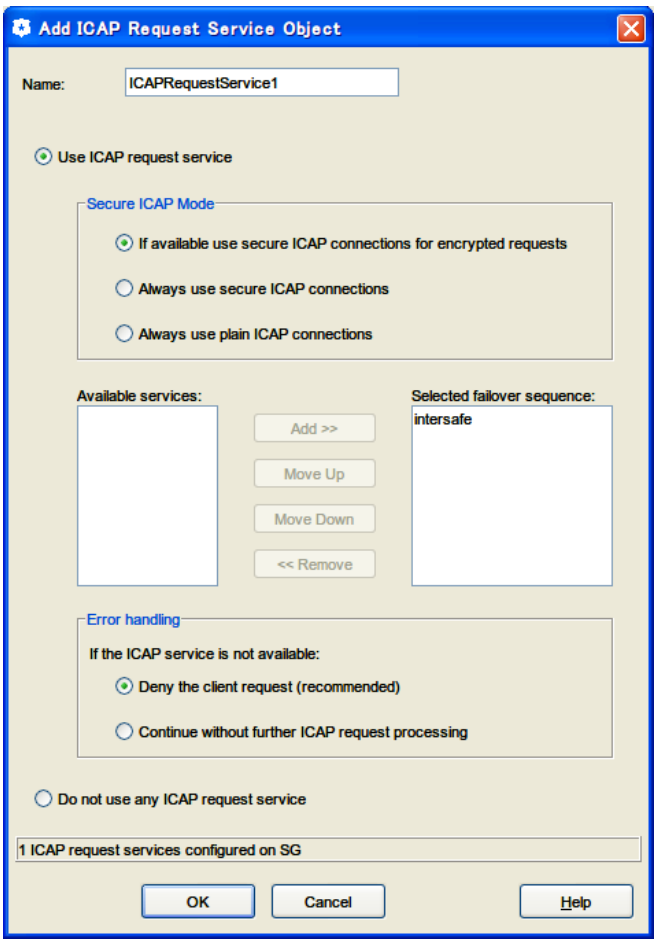
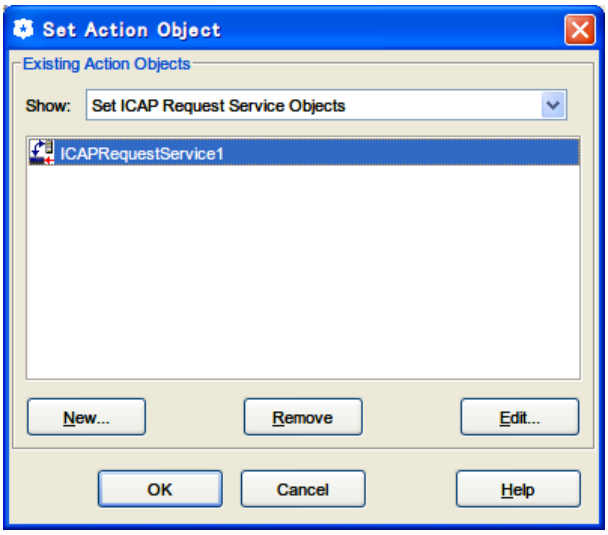


表 8

項目名	設定内容
Name	ICAP Request Service Object の名前を入力します。
Use ICAP request service	P.19「4-1-1.ICAP サーバの設定」で作成した ICAP サーバを選択し、[Add >>]ボタンをクリックします。
Error handling	ICAP Request がエラーになった場合のリクエストの処理方式を選択します。 ○Deny the client request (recommended) クライアントにエラー画面を表示し、インターネットへは接続できません。 ○Continue without further ICAP request processing ICAP サーバにリクエストを送信しないで、そのままインターネットへ接続します。 (ISWF の規制は行われません。)

11) 『Set Adtion Object』の一覧に先程作成した ICAP Request Service が追加されますので、選択して[OK]ボタンをクリックします。

図 4-12



■ **認証設定**

ここでは、認証の Policy を設定します。

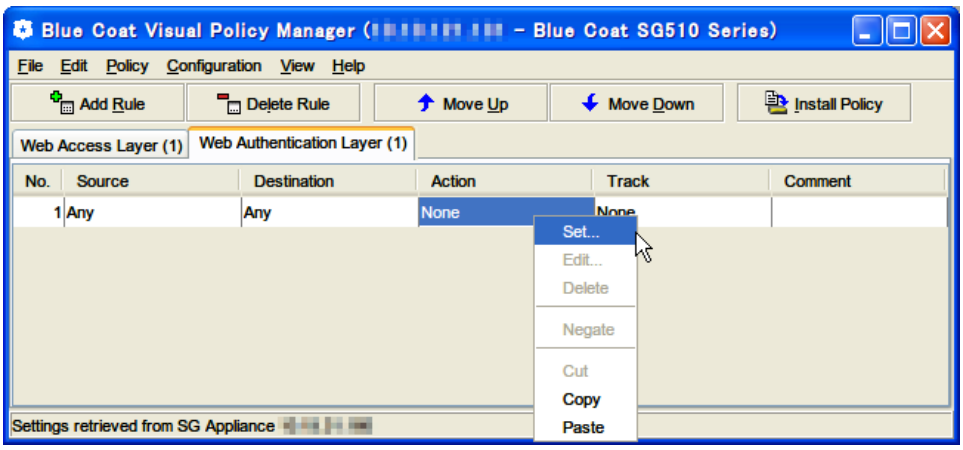
1) VPM のメニューより『Policy』 > 『Add Web Authentication Layer』を選択します。

2) 『Add New Layer』で「Layer Name」を入力し[了解]ボタンをクリックします。

図 4-13

3)　作成された Layer の「Action」の項にて右クリックし、「Set」を選択します。

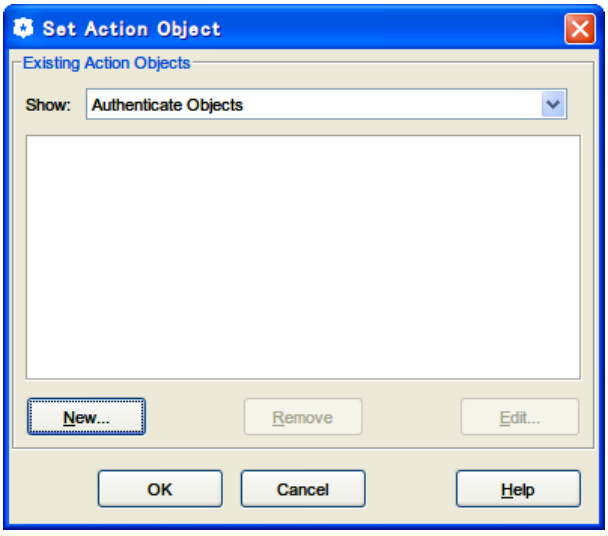
図 4-14



4)　『Set Action Object』の『Show』で「Authenticate Objects」を選択します。一覧の中に「Authenticate」がない場合、[New]ボタンをクリックし表示される一覧の中から「Authenticate」を選択し新しい Object を作成します。

すでに一覧に「Authenticate」がある場合は、「Authenticate」を選択後[Edit]ボタンをクリックします。

図 4-15



5) Authenticate Object の設定を行い、[OK]ボタンをクリックします。

図 4-16

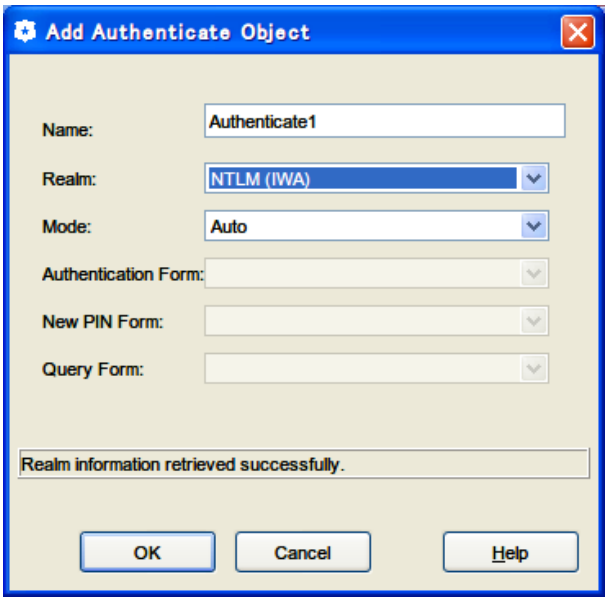
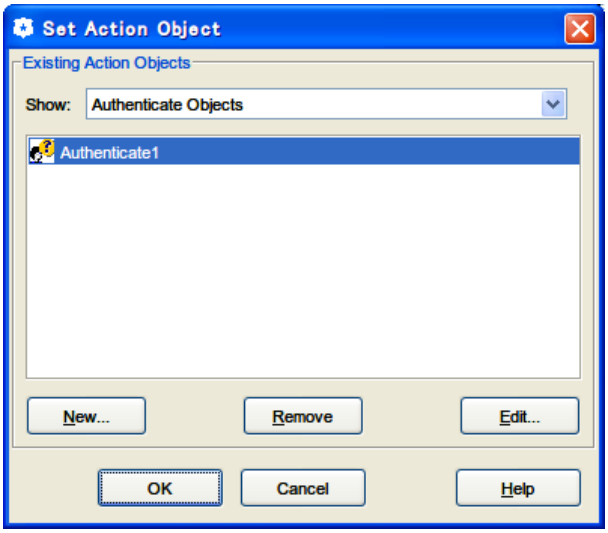


表 9

項目名	設定内容
Name	Authenticate Object の名前を入力します。
Realm	P.20「4-1-2.認証設定」で作成した NTLM 設定を選択します。

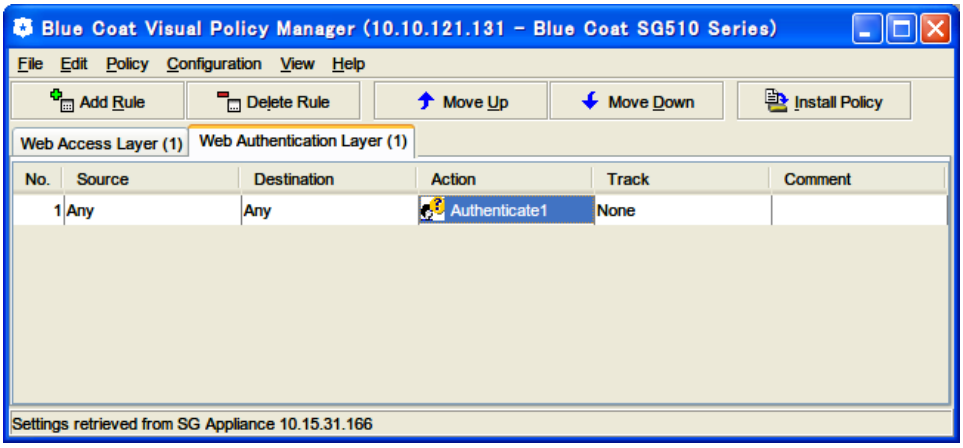
6) 『Set Adtion Object』の一覧に先程作成した Authenticate Object が追加されますので、選択して[OK]ボタンをクリックします。

図 4-17



7) VPM による設定が全て完了した後、ウィンドウを閉じる前に必ずウィンドウの右上の方にある[Install Policy]ボタンをクリックし、設定内容を反映させてください。

図 4-18



4-1-4.BCAAA のインストール

BCAAA とは「Blue Coat Authentication and Authorization Agent」の事です。NTLM 認証を実現するためには AD サーバに BCAAA をインストールする必要があります。BCAAA は BlueCoat 社より提供されています。

4-1-5.Client の設定

Client の設定（説明の対象は、Internet Explorer）は、メニューバーより「インターネットオプション」 > 「接続」 > 「LAN の設定」をクリックします。「プロキシ サーバー」の枠内にある「LAN にプロキシ サーバーを利用する」のチェックボックスにチェックを入れ「アドレス」に、BlueCoat の IP アドレスを、「ポート」に、BlueCoat で指定している HTTP の受付ポートを入力してください。

4-2.Squidを用いたシングルサインオン

ここでは、Squid と ISWF for ICAP を用いて、AD と連携しシングルサインオン(SSO)を実現する方法について説明します。なお、以下の条件を満たしていることが前提となります。

1. ISWF において[サーバ管理] > [認証設定]の設定が完了していること
2. AD から ISWF にグループの取り込みが完了していること
3. ISWF においてフィルタリングルールの設定が完了していること
4. InterSafe WebFilter の管理者マニュアルの付録「C. ICAP クライアントでの NTLM 認証」の設定が完了していること
5. Squid をインストールしているサーバが、認証で利用する AD のドメインに参加していること(Samba に実装された winbind などを利用)

- 本章で使用している Squid のバージョンは 3.1.8 です。Squid 3.1.8 より前のバージョンをご利用の場合、設定内容が違う場合がございますが、予めご了承ください。
- Squid(ICAP クライアント)に対応している ISWF for ICAP のバージョンは Ver7.0 以降です。
- Squid 及び Samba の詳細設定については、文献や Web などをご参照ください。

4-2-1.Squid のインストール

Squid で NTLM 認証機能を有効にするには、Squid インストール時の configure のオプションで"--enable-auth="ntlm"を追加してください。(Squid インストール時のオプションについては、InterSafe WebFilter の管理者マニュアルの「1-5. ICAP クライアントの設定」を参照し設定を行ってください。)

■ **Squid インストール時の実行例**

```
# ./configure --enable-icap-client □
            --enable-auth="ntlm"
# make
# make install
```

4-2-2.Squid の設定

Squid の設定ファイル(squid.conf)に認証設定と ICAP 連携の設定を記述します。

■ **squid.conf の記述例**

```
# Squid の認証設定例
auth_param ntlm program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-ntlmssp
auth_param ntlm children 5
acl AuthorizedUsers proxy_auth REQUIRED
http_access allow all AuthorizedUsers

# ICAP 連携設定例
icap_enable on
icap_service service_1 reqmod_precache 0 icap://<ISWF サーバ IP>:1344
adaptation_service_set service_set_1 service_1
adaptation_access service_set_1 allow all
icap_send_client_ip on
icap_send_client_username on
icap_client_username_header X-Authenticated-User
icap_client_username_encode on
```

4-2-3.Client の設定

Client の設定（説明の対象は、Internet Explorer）は、メニューバーより「インターネットオプション」 > 「接続」 > 「LAN の設定」のをクリックします。「プロキシ サーバー」の枠内にある「LAN にプロキシ サーバーを利用する」のチェックボックスにチェックを入れ「アドレス」に Squid の IP アドレスを、「ポート」に Squid で指定している HTTP の受付ポートを入力してください。

[InterSafe WebFilter Ver8 Ver9] Active Directory との連携

2019 年 2 月 第 5 版

作成/発行/企画　アルプスシステムインテグレーション株式会社

〒145-0067　東京都大田区雪谷大塚町 1-7