もっと豊かな情報未来へ
アルシー・ソリューション

InterSafe WebFilter Ver.9.0
バージョンアップ概要・注意事項（初版）

InterSafe WebFilter

アルプスシステムインテグレーション株式会社
セキュリティ事業部プロダクト技術部
作成日　2018年4月18日

はじめに

本資料は、

InterSafe WebFilter Ver.9.0
（以下 ISWF）へのバージョンアップを前提とした内容となっております。

プログラムの入手方法についてはサポート窓口までお問い合わせください。

■サポート窓口
メール：support@alsi.co.jp
電話　：03-5499-1331(平日10:00～12:00、13:00～17:00)

また、Ver.9.0の不具合情報については、下記リンク（FAQ）をご参照ください。

InterSafe WebFilter 障害・不具合報告
http://support.alsi.co.jp/faq_list.html?page=-1&category=38

変更履歴

新規作成

目次

1.必要条件

Ver.9.0にバージョンアップが可能なOS、製品の必要条件について説明します。

1.必要条件

本項で説明する必要条件は以下の通りです。

1-1.動作要件

● WebFilterが動作するサーバ

Windows版

[OS(32ビット)]
・日本語版Microsoft Windows Server 2008 Standard/Enterprise EditionSP2
[OS(64ビット)]
・日本語版Microsoft Windows Server 2008 Standard/Enterprise SP2
・日本語版Microsoft Windows Server 2008 R2 Standard/Enterprise SP1
・日本語版Microsoft Windows Server 2012 Standard
・日本語版Microsoft Windows Server 2012 R2 Standard
・日本語版Microsoft Windows Server 2016 Standard [CPU] Intel Pentium 4以上
[メモリ] 2GB以上
[ディスク容量] 1GB以上の空き領域(ログ使用領域を除く)

Linux版

[OS(32ビット/64ビット)]
・Red Hat Enterprise Linux 6
Linux カーネル v 2.6.32および glibc v 2.11
[OS(64ビット)]
・Red Hat Enterprise Linux 7
Linux カーネル v 3.10.0および glibc v 2.17
[CPU] Intel Pentium 4以上
[メモリ] 2GB以上
[ディスク容量] 1GB以上の空き領域(ログ使用領域を除く)

●仮想環境を使用する場合
WebFilterが対応しているOSを、ゲストOS上で動作保証している仮想環境
※仮想環境固有の問題を除いては対応可能です。

●WebFilter for ICAPを使用する場合
[ICAP クライアント]
Blue Coat Systems SGOS 5.4～5.5,6.4,6.5
Squid 3.1～3.5

1-1.動作要件

●LDAP 連携を行う場合
[LDAPサーバ]
・Active Directory:Windows Server 2008 (SP2推奨)
・Active Directory:Windows Server 2008 R2 (SP1推奨)
・Active Directory:Windows Server 2012
・Active Directory:Windows Server 2012 R2
・Active Directory:Windows Server 2016
・OpenLDAP 2.4.35
・Oracle Directory Server Enterprise Edition 11 g R2
※Windows Server 2008,Windows Server 2008 R2およびWindows Server 2012ではActive Directory ドメインサービス（AD DS）が必要です。Active Directoryライトウェイトディレクトサービス（AD LDS）には対応していません。
※NTLM認証及びKerberos認証はWindows Server 2008、Windows Server 2008R2、 Windows Server 2012、Windows Server 2012 R2 が対応しています。

●WebFilterに接続するクライアント
Windows
[ブラウザ]
・Internet Explorer 10/11 (Microsoft)
・Microsoft Edge (Microsoft)
・Firefox (Mozilla)
・Chrome (Google)
※ NTLM認証を行う場合、Internet Explorer 10/11、Firefox、Chromeの利用を推奨します。
※ iOSでNTLM認証を行なう場合は、Wi-fi接続で、InterSafe WebFilterをプロキシに指定してください。
※ Kerberos認証を行う場合は、Internet Explorer 10/11の利用を推奨します。

Macintosh
[OS]
Mac OS X (v10.10 推奨)
[ブラウザ]
Safari v9 on Mac OS (Apple)

1-1.動作要件

●WebFilterに接続するクライアント

iPhone/iPad

[OS]
iOS
[ブラウザ]
Safari v9 on iOS iPhone/iPad (Apple)
※Wi-fiプロキシにてwebFilterに接続した場合のHTTPおよびHTTPSプロトコルのみ対象

Android

[OS]
Android (6.0推奨)
[ブラウザ]
ブラウザ（com.android.browser）
Chrome for Android （com.android.chrome）
※Wi-fiプロキシにてwebFilterに接続した場合のHTTPおよびHTTPSプロトコルのみ対象

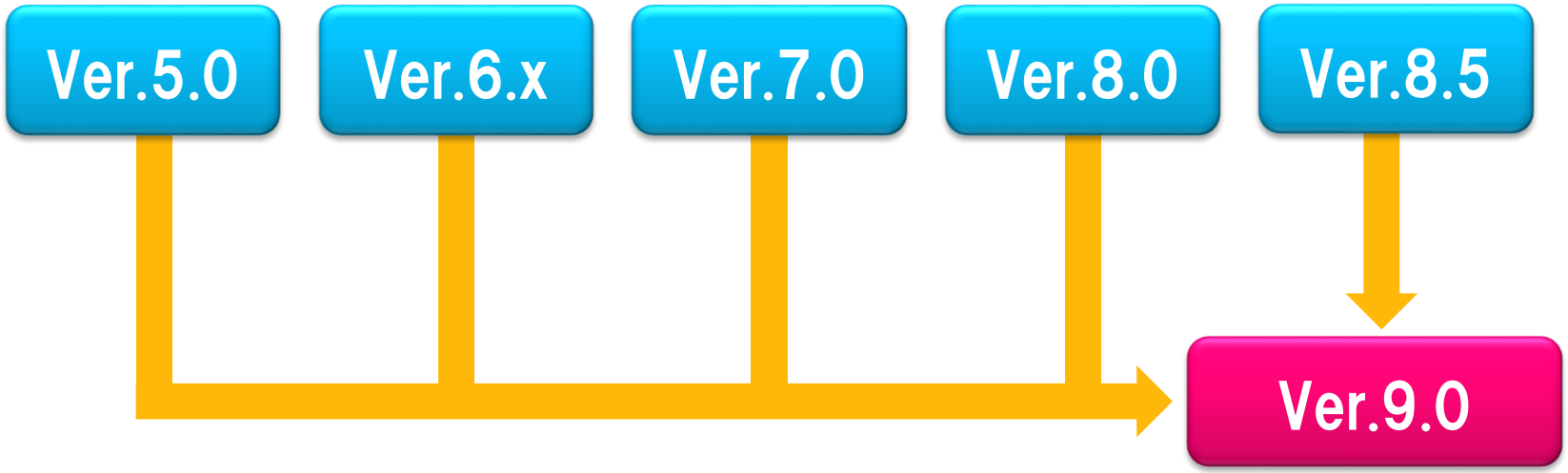
●WebFilterの管理画面操作に使用するクライアント

[ブラウザ]
・Internet Explorer 10/11 (Microsoft)
※ 互換表示を無効にしてください。
※ Windows 8.1のIE11に関しては、デスクトップ用のみ対応しております。

※ Internet Explorerは各OSがサポートする最新バージョンに対応します。

1-2.バージョン

Ver.5.0以降のバージョンをご利用のお客様は、Ver.9.0のインストールプログラムを実行することにより、Ver.9.0へ一度でバージョンアップすることができます。
(Ver.8.0までは、1つ前のバージョンからのバージョンアップのみ可能でした。)



一度でVer.9.0にバージョンアップ可能

1-3.製品タイプ

- **Proxy版（Windows / Linux / Solaris）**からのバージョンアップ **OK**
  Ver.5.0以降のProxy版をお使いのお客様は、Ver.9.0のセットアッププログラムを実行することによって、バージョンアップ前の設定は引き継がれます。
  ただし、Ver9.0はSolarisは対応OSではないため、対応OSへ変更が必要です。

- **ICAP版（Linux / Solaris）**からのバージョンアップ **OK**
  Linux ICAP版をお使いのお客様は、Ver.9.0のセットアッププログラムを実行することによって、バージョンアップ前の設定は引き継がれます。
  ただし、Ver9.0はSolarisは対応OSではないため、対応OSへ変更が必要です。

- **Squid版（Linux / Solaris）**からのバージョンアップ **OK ※要注意**
  Ver.5.0以降のSquid(Redirector)版をお使いのお客様は、Ver.9.0のセットアッププログラムを実行することによって、Ver.9.0にバージョンアップするとともに、製品が**ICAP版に変わります**。バージョンアップ前の設定は引き継がれます。
  この際、Squid側の設定は変換されません。Squid側でICAPのオプション機能が付加されていない場合は、再インストールが必要になります。（Ver.9.0 ICAP版では Squid 3.1～3.5 に対応しています。）

2.バージョンアップの流れ

Ver.9.0へのバージョンアップの流れについて説明します。

2.バージョンアップの流れ

ここではVer.7.0 →Ver.9.0適用までを例に説明します。

- 事前に設定ファイルのバックアップをしてください。
- setup.exe/setup.shの実行はVer.7.0がインストールされているマシン上で実施してください。

Ver.9.0の
setup.exe(Windows版)/
setup.sh(Linux版)を実行

上書き
インストール

バージョン
アップ完了

- ここでVer.9.0の上書きインストールが実行されます。
- 各種設定ファイルを自動的に変換（コンバート）します。

※データ量やサーバスペックによっては、コンバートに時間を要する場合がございますのでご注意ください。

3.バージョンアップ前の注意事項

Ver.9.0にバージョンアップ前の注意事項について説明します。

3.バージョンアップ前の注意事項

本項で説明する注意事項は以下の通りです。

3-1.設定情報のバックアップ

バージョンアップの前には必ず設定ファイルフォルダ（ディレクトリ）をバックアップして下さい。万が一インストール途中で障害が発生しインストールが失敗した場合においても、設定ファイルを利用することにより旧バージョンの状態へリカバリすることができます。

[バックアップしていただきたい設定ファイルフォルダ（ディレクトリ）]
バックアップは全サービスを停止した上で行って下さい。
もしくは、管理画面を操作していないことを確認した上で行ってください。

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

デフォルトのインストールフォルダ（ディレクトリ）は以下となります。
Windows: C:¥InterSafe
Linux: /usr/local/intersafe
Solaris: /opt/intersafe

3-2.keystoreファイルのバックアップ

管理画面をHTTPSで使用している場合は予め以下のバックアップを
取得してください。

Windows:<インストールフォルダ>¥tomcat配下のファイル
Linux / Solaris:<インストールディレクトリ>/tomcat配下のファイル

バージョンアップ後、同じkeystoreファイルを利用する場合は、
keystoreのバックアップを取得し、事前のインストールフォルダ
（ディレクトリ）以外に退避してください。

※バージョンアップ後、管理画面をHTTPSで利用される場合は、
　管理者マニュアルの「HTTPSプロトコルで管理画面を使用する」を
　ご参照いただき、再設定を行ってください。

3-3.ulimitの確認（Linux版のみ）

Ver.8.5以降では、ファイルディスクリプタの上限を設定ファイル（system.inf）で設定できるようになりました。

<インストールディレクトリ>*/conf/sys/system.inf*内
*[STSTEM_GLOBAL]*セクション
LIMIT_NOFILE=32768
※隠しキーのため、変更する場合は、キーを 追記して値を設定します。
変更後は、フィルタリングサービスの再起動が必要です。

この設定により、バージョンアップ後はファイルディスクリプタの上限に32768が適用されます。
バージョンアップ前に、ISWFの起動シェル内にulimitコマンドを記述してファイルディスクリプタの上限を変更されていたお客様は、上記の設定を変更してください。Ver.8.0までのファイルディスクリプタの上限の変更方法は以下FAQをご参考ください。

FAQ No.1584「ファイルディスクリプタが不足し、Webアクセス不能となってしまう。」
http://support.alsi.co.jp/faq_detail.html?id=1584&category=

例）Ver.8.0にてファイルディスクリプタの上限を40000に設定している場合

Ver.8.5以降へバージョンアップした場合、32768に減少する結果になりますので、
上記の設定を40000以上に変更します。

3-4.tomcatのポート確認

お客様によっては、ISWFの動作に必要なTomcatのポート番号8005が
同居するアプリケーションとバッティングすることを回避するため、
Tomcatのポート番号を変更されている場合がございます。
仮に変更していた場合、ISWFのバージョンアップにより、
設定が初期化されますので、バージョンアップ後は、必要に応じて
再度変更をしてください。（以下FAQページをご参考ください。）

FAQ No.2522 「Tomcatが内部で使用するポート番号を変更したい」
http://support.alsi.co.jp/faq_detail.html?id=2522&category=

3-5.カスタマイズ規制画面ファイルのバックアップ

カスタマイズした規制画面htmlファイルは、バージョンアップした際に、自動的にバックアップ対象として保存されますが、念のため、バージョンアップ前にバックアップを取得してください。

※規制画面のカスタマイズはサポート対象外となります。

▼規制画面のHTMLファイル（デフォルト）
Windows:<インストールフォルダ>¥conf¥block¥nfblock.htm
Linux / Solaris:<インストールディレクトリ>/conf/block/nfblock.htm

▼自動バックアップデータ（バージョンアップ後に生成されます）
Windows:<インストールフォルダ>¥backup¥conf_vxx_<バージョンアップ日付>
Linux / Solaris:<インストールディレクトリ>/backup/conf_vxx_<バージョンアップ日付>

補足：Ver.9.0の規制画面htmlのカスタマイズについて

●Ver.8.0からバージョンアップされるお客様
バージョンアップ時、規制画面htmlファイルは引き継がれますので、バージョンアップ後のカスタマイズは不要です。

●Ver.8.0より前のバージョンからバージョンアップされるお客様
バージョンアップ時、**規制画面htmlファイルは引き継がれません**。また、規制画面htmlファイルの内容が大幅に変わっておりますので、Ver.9.0に合わせたカスタマイズが必要です。

3-6.Ver.5.0～7.0 Squid版からのバージョンアップ

Ver.5.0～7.0 Squid版をインストールしたサーバで、Ver.9.0のセットアッププログラムを実行した場合、Ver.9.0 ICAP版としてバージョンアップされます。（Ver.5.0～7.0 Squid版の設定はコンバートされます。）

※Squid でICAP クライアント機能を有効にするには、Squidのconfigure のオプションに **“--enable-icap-client“ が追加されていることが必要ですのであらかじめご注意ください。**

ICAP連携に必要な設定については、Ver.9.0 管理者マニュアル「1-5. ICAP クライアントの設定」をご参照ください。

3-7.マスタ・スレーブ構成でのバージョンアップ

マスタ・スレーブ構成でバージョンアップを行う場合は、それぞれのサーバでバージョンアップを行ってください。
バージョンアップ作業前に管理画面でスレーブサーバを削除する必要はありません。

※異なるバージョンのマスタサーバおよびスレーブサーバが混在していると、同期に失敗する場合があります。マスタサーバとすべてのスレーブサーバが同一バージョンになるまでは、管理画面での設定変更をしないでください。

4.バージョンアップ後の作業

バージョンアップ後に設定していただく作業について説明します。

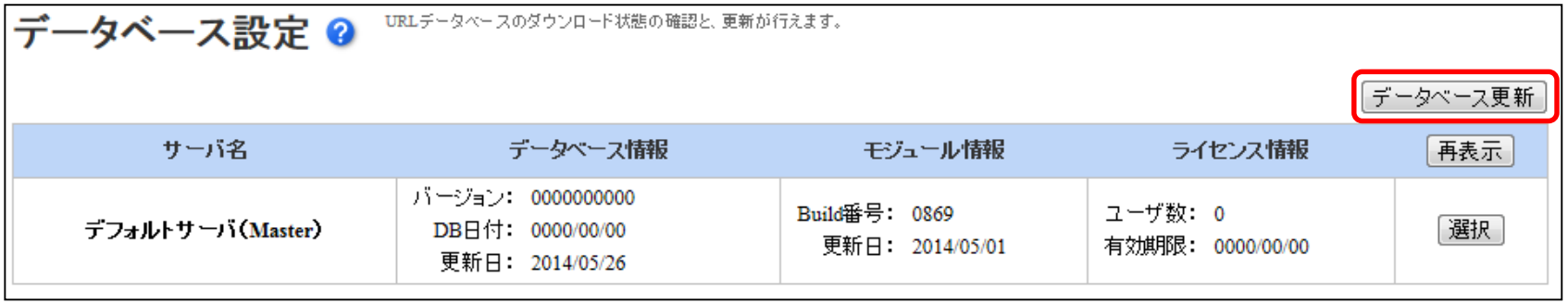
4-1.データベースのダウンロード

Ver.8.0よりも古いバージョンからバージョンアップした直後は、URLデータベースが初期化され、フィルタリングが掛からない状態になります。（自動ダウンロード後、フィルタリングが掛かるようになります。）

Ver.8.0以降からVer.9.0へバージョンアップした場合は、Ver.8.0のデータベースが継承されるため、バージョンアップ直後もフィルタリングが可能な状態となります。Ver.8.5以降で追加されたカテゴリ分のURLについては、次回URLデータベースダウンロード時に反映されます。また、管理画面上はデータベース情報の「バージョン」「DB日付」はすべて「0」になりますが、こちらも次回URLデータベースダウンロード時に反映されます。
手動でダウンロードする場合は、以下の手順で行います。
※必ず、ISWFの全てのサービス（プロセス）が起動した状態でダウンロードを実施してください。
サービスの起動確認の方法は以下FAQをご参照ください。

FAQ No.4091「Ver.9.0/8.xで起動するプロセスについて教えてください」
http://support.alsi.co.jp/faq_detail.html?id=4091&category=

●手順
管理画面の[サーバ管理] - [データベース設定]の画面にて、「データベース更新」をクリックして、確認画面で「OK」ボタンを押します。（スレーブサーバが登録されている場合は、スレーブサーバ側でも同時にダウンロードが実行されます。）



4-2.その他の作業

第3章の項目にある

3-2.keystoreファイルのバックアップ
3-3.ulimitの確認（Linux版のみ）
3-4.tomcatのポート確認
3-7.マスタ・スレーブ構成でのバージョンアップ

に該当するお客様は、各スライドの内容に従って作業を行ってください。

5.バージョンアップ後の注意事項

Ver.8.0以降ではシステム構成やグループ/ユーザ管理、フィルタリング管理の仕組みが変更になります。Ver.7.0からバージョンアップした場合のデータの変更点や、設定の移行先について説明します。

Ver.9.0の新機能については、マニュアル、Readme.txtをご参照ください。

5.バージョンアップ後の注意事項

本項で説明する注意事項は以下の通りです。

5-1.管理画面の設定用語の違い

Ver.8.0以降では、管理画面での用語を一部変更しております。

Ver.7.0	Ver.8.0以降	補足
オーバーライド	一時解除	規制画面に対して、一時的にアクセス許可を与える機能。確認ボタンのみと、事前に登録した解除パスワードを入力を求められる2種類が存在する。
システム管理	サーバ管理	サーバの設定変更が可能。 スレーブサーバの追加。 アクセスポート、プロセス数の変更が可能。
ダウンロード設定	データベース設定	ライセンスキー、障害時のエラーメールの宛先、データベースのダウンロード時間などが指定可能。
保存/復旧設定	保存/復旧/同期	設定のバックアップ及びスレーブサーバとの自動同期設定の有効無効の設定が可能
最低基準ルール	カテゴリ設定制限	下位のグループに対して、強制的にルールを適用する。
例外ユーザ	個別ルール	例外ユーザに対して個別にルールを適用する。 適用可能なルールは以下の５つ。 • カテゴリ/スケジュール設定 • ブラウザ規制設定 • 検索キーワード規制設定 • 書き込みキーワード規制設定 • 規制オプション設定

5-2.HTTPS規制画面の動作変更

Ver.8.0～Ver.8.5 Build0860までは、ICAP版でIE8以降を使用してHTTPSの規制サイトを表示した場合、規制画面は表示されますが、規制理由・一時解除ボタンは表示されません。Ver.8.5 SP1 Build0870以降で規制画面に規制理由・一時解除ボタンが表示されるようになりました。

ISWFのバージョン	規制理由表示
7.0	不可
7.0 on IPv6	設定により可能
7.0 SP1	設定により可能
8.0	不可
8.5 Build0860まで	不可
8.5 SP1以降	可能

5-3.使用するポートの追加

使用するポートが追加されます。

Ver.7.0	
管理サービス用ポート（全製品共通）	41212
データ同期用ポート（全製品共通）	41213
フィルタリングサービス制御用ポート（全製品共通）	41214
管理画面用ポート（全製品共通）	2319
HTTP ポート（Proxy版のみ）	8080
HTTPS ポート（Proxy版のみ）	8443
FTP OVER HTTP ポート（Proxy版のみ）	8021
ICAP ポート（ICAP版のみ）	1344
リダイレクタポート（Squid版のみ）	53556
HTTP規制画面出力用ポート（ICAP版/Squid版）	21128
HTTPS規制画面出力用ポート（Squid版/ICAP版）	443
管理画面停止用ポート（全製品共通）	8005

※Ver.8.0以降では、Proxy版、ICAP版ともに、フィルタリング処理を行うために、内部的にポート1344を使用する仕様に変更しております。

Ver.8.0以降	
管理サービス用ポート（全製品共通）	41212
データ同期用ポート（全製品共通）	41213
フィルタリングサービス制御用ポート（全製品共通）	41214
	41215
	41216
キャッシュデータ制御用ポート（全製品共通）	5963
管理画面用ポート(全製品共通)	2319
HTTP ポート（Proxy版のみ）	8080
HTTPS ポート（Proxy版のみ）	8443
FTP OVER HTTP ポート（Proxy版のみ）	8021
ICAP ポート（全製品共通）※	1344
Webコンテンツキャッシュ制御待受ポート(Ver8.5 SP2以降 Proxy版のみ)	41211
HTTP規制画面出力用ポート（ICAP版のみ）	21128
HTTPS規制画面出力用ポート（ICAP版のみ）	443
ARMS連携機能のコールバック待受ポート(Ver8.5 SP2以降)	8319
アクセスログエージェントポート(Ver9.0以降)	41210
集計データベースサービスポート(Ver9.0以降のマスタのみ)	41209
管理画面停止用ポート（全製品共通）	8005

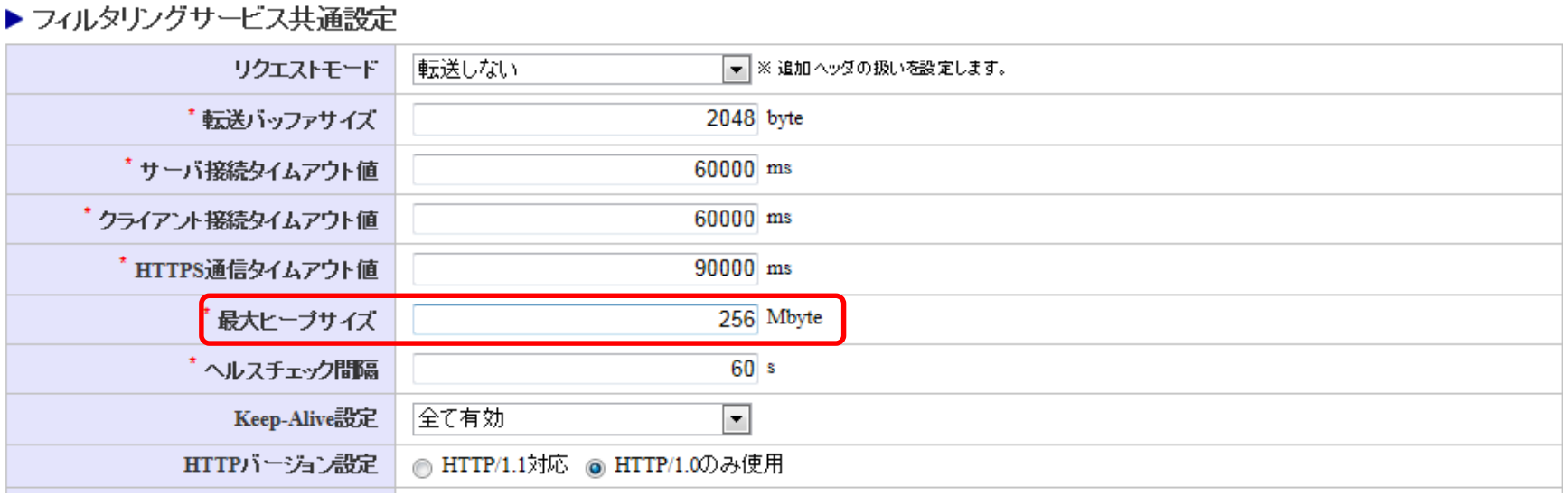
5-4.起動プロセスの変更

起動するプロセスが分割されます。
※各サービスの起動方法は、管理者マニュアルをご参照ください。

	Ver.7.0	Ver.8.0以降		
		Windows版	Linux版	備考
管理サービス	AdminControl	AdminControl	java(Admin)	
プロキシ・フィルタリングサービス	ProxyControl	ProxyControl	sbin/ams_sd	フィルタリング管理プロセス
		nsfiltering	sbin/nsfilterin (NsFiltering)	フィルタリングを行うプロセス
		nscache	sbin/nscache/nscache (NsCache)	各種データを保持するプロセス
		javaw	java (NsProxy)	プロキシを行うプロセス
管理画面サービス	WebService	WebService java	java(Tomcat)	
Geoスコープの集計用サービス(Ver9.0以降のマスタのみ)	-	DataCollector Control	java(amscollector)	

5-5.最大ヒープサイズの設定

最大ヒープサイズが 256Mbyte に変更になります。
Ver.8.5以降ではデータベースの格納領域にJAVAヒープを利用しないため、
Ver7.0以前に比べて最大ヒープサイズを256Mbyteに抑えてあります。



補足：Ver.8.0以降からバージョンアップした場合

Ver.8.0～Ver.8.5 Build0860まではヒープサイズは128Mbyteで設定されています。これらのバージョンからバージョンアップした場合は、128Mbyteが引き継がれます。
ヒープサイズ 128Mbyteは600プロセス数程度を想定した数値となっておりますので、プロセス数を600以上に増加している場合は、ヒープサイズを増加してください。(1000プロセスの場合ヒープサイズは256MBを目安としてください。)

5-6.ルールの考え方

Ver.8.0以降ではグループとルールの関係が以下のように変更になります。

Ver.7.0

グループごとに各設定を直接登録します。

営業部グループ

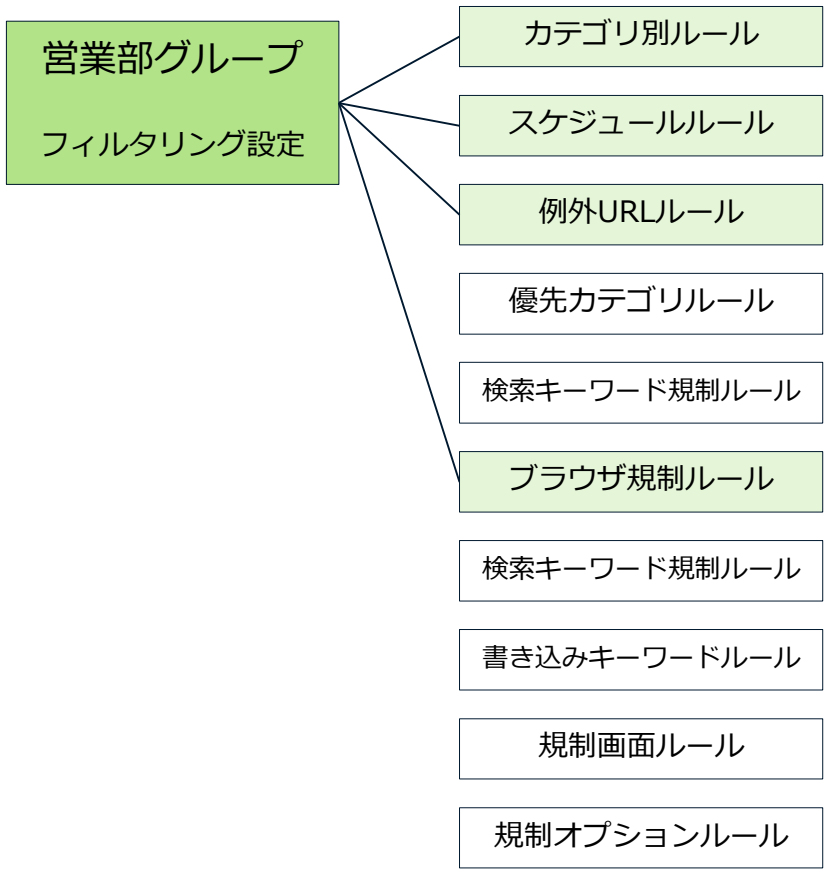
フィルタリング設定	カテゴリ別ルール
	スケジュール
	例外URL
	クライアント規制
	規制オプション

開発部グループ

フィルタリング設定	カテゴリ別ルール
	スケジュール
	例外URL
	クライアント規制
	規制オプション

Ver.8.0以降

各設定は「ルール」という単位で登録し、
必要な設定をグループに適用します。
（パーツを組み合わせるイメージ）

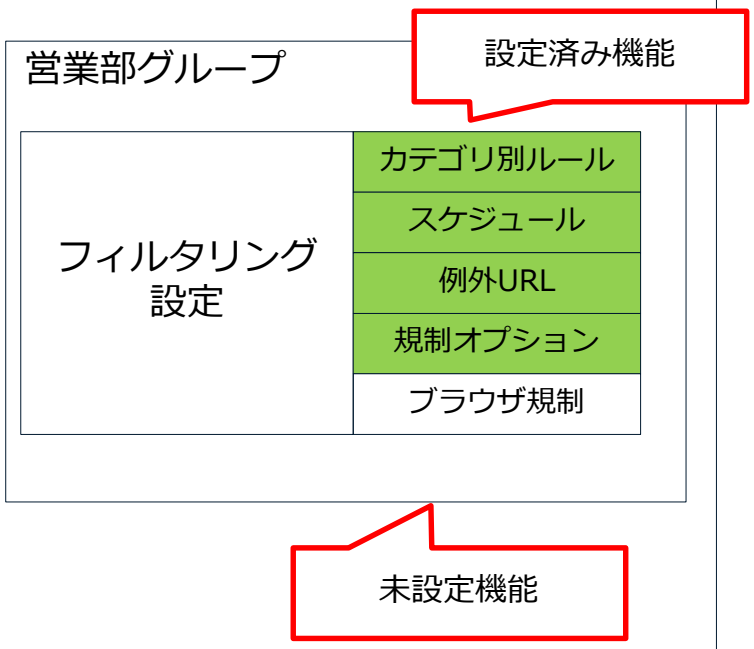


5-7.バージョンアップによるルールの適用・確認

Ver.7.0で設定が行われていた機能はルールが作成され、適用された状態でバージョンアップします。

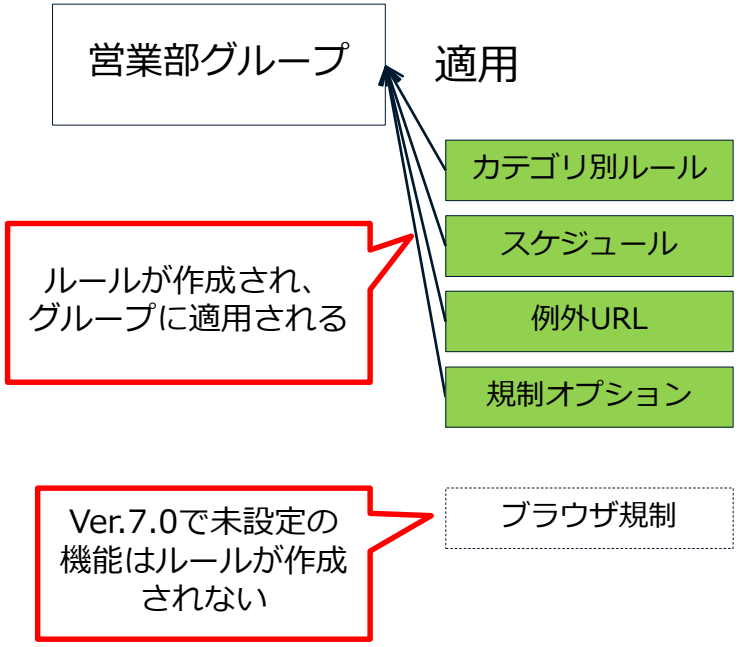
Ver.7.0

グループ毎に設定が固定で用意されています。



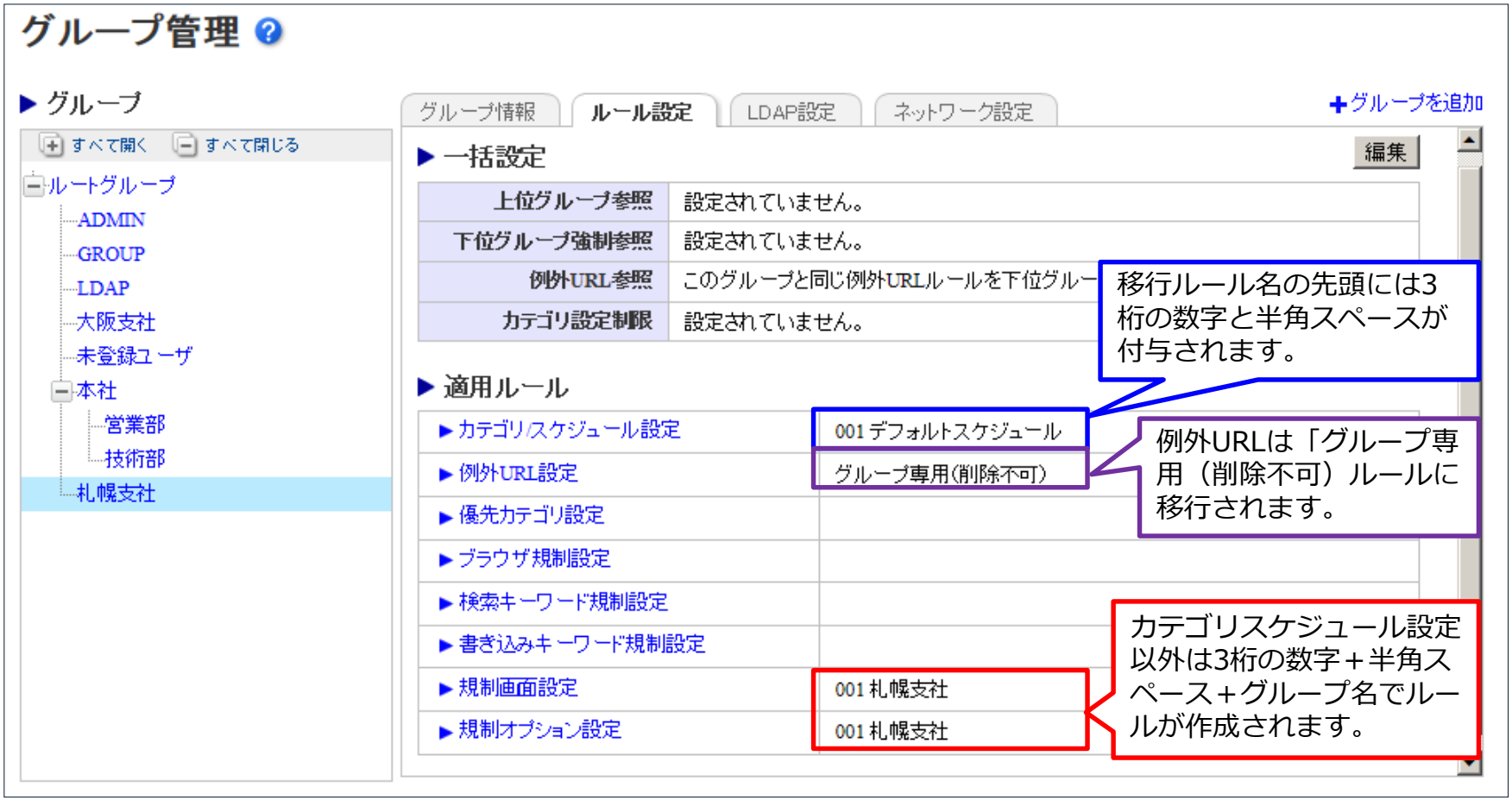
Ver.8.0以降

各設定はルールという単位で存在し、必要な設定をグループに適用します。



5-7.バージョンアップによるルールの適用・確認

[グループ/ユーザ管理] - [グループ管理]画面にて、グループに適用されるルールを確認する事が出来ます。

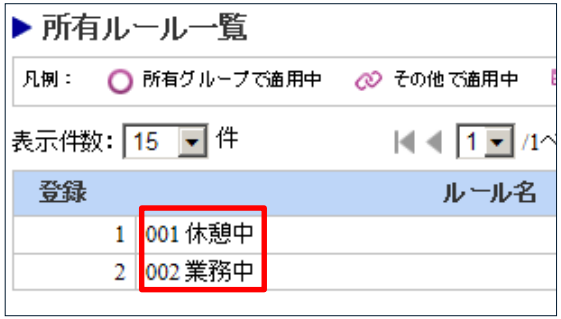


5-8.フィルタリングルールのルール名

移行後はルール名が以下の命名規則に従い変更されます。
ルール名の前に [3桁の数字] ＋ [半角スペース] が付与されます。

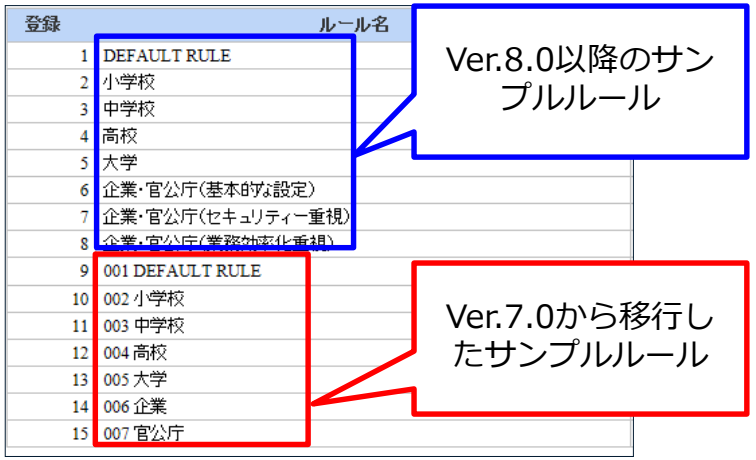
（例１）お客様が作成したルール

Ver.7.0ルール名	Ver.8.0バージョンアップ後のルール名
休憩中	001 休憩中
業務中	002 業務中



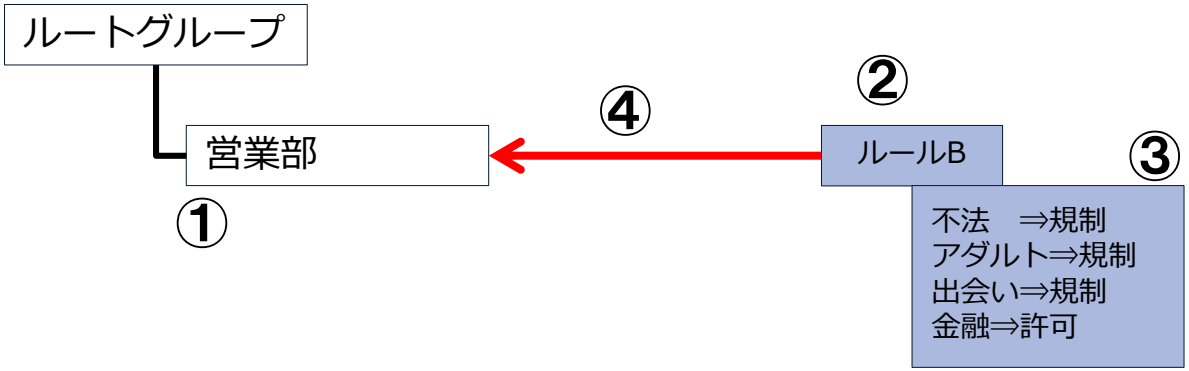
（例２）デフォルトで用意されているサンプルルール
Ver7.0からサンプルルールを移行します。別途Ver8.0以降のサンプルルールも提供されます。

Ver.7.0ルール名	Ver.8.0バージョンアップ後のルール名
DEFAULT RULE	001 DEFAULT RULE
小学校	002 小学校
中学校	003 中学校
高校	004 高校
大学	005 大学
企業	006 企業
官公庁	007 官公庁



5-9.運用中にルールを適用するまでの流れ

Ver.8.0以降での、グループの登録からフィルタリングルールの適用までの流れは以下の通りです。



●グループの登録からフィルタリングルールの適用までの流れ
①管理画面の[グループ/ユーザ管理]-[グループ管理]にてグループを作成
②管理画面の[個別アクセス管理]にて各ルールを登録
③管理画面の[個別アクセス管理]にて各ルールの設定
④管理画面の[グループ/ユーザ管理]-[グループ管理]にて各ルールを適用

※詳しい手順については、管理者マニュアルをご参照ください。

5-10.例外ユーザ

Ver.7.0の例外ユーザは一般のユーザに統合されます。
例外ユーザだったユーザは、アカウント一覧にて
「個別ルール」の欄にマークが付きます。

クリックするとユーザごとの
ルール設定画面に移動します

5-11.カテゴリ設定の移行ルール

カテゴリが新設、細分化されたことにより、これまでの閲覧結果と違いが出る場合があります。

	移行ポリシー	カテゴリ例　（カッコ内はVer.7.0のカテゴリ名）
Ver.8.0以降でも存在するカテゴリ	**既存の設定を引き継ぎます。**	違法と思われる行為、公開プロキシ、ウェブメール、迷惑メールリンク
名称を変更したカテゴリ	**既存の設定を引き継ぎます。**	クラッキング（ハッキング）、出会い（出会い・異性紹介）、ギャンブル（ギャンブル一般）、オンラインショッピング（通信販売一般）
Ver.7.0のカテゴリから分割したカテゴリ	**分割元のカテゴリの設定を引き継ぎます。**	公開プロキシ、フィルタリング回避（公開プロキシ） 銀行、ローン・決済（金融商品・サービス） SNS・ミニブログ、ブログ（SNS・ブログ）
統合したカテゴリ	**統合したうち、カテゴリ番号の上位のカテゴリの設定を引き継ぎます。**	アダルト・ポルノ（性行為、ヌード画像、性風俗、アダルト検索・リンク集）
新設カテゴリ	**許可**	クチコミ・評価・コメント、位置情報、プロバイダ、病気・医療、学校・教育、天気・災害情報
新設カテゴリ	**既存の「未分類カテゴリ」の設定を引き継ぎます。**	イメージサーバ、CDNサーバ、その他のシステムコンテンツ（Ver.8.5から新設）、ダイナミックDNS(Ver.8.5 SP2から新設)
廃止	**移行なし**	話題、同性愛 ※これらのカテゴリに登録されていたURLは内容に応じてその他のカテゴリに分類されます。
例外	**既存の設定に関わらず、必ず規制になります。**	マルウェア　（不正コード配布） DBD攻撃　（新設）

詳しくは以下のFAQページをご参照ください。
FAQ No.4090「Ver9.0 Ver.8.5 および Ver.8.0 カテゴリ一覧」
http://support.alsi.co.jp/faq_detail.html?id=4090&category=

5-12.ログファイルの変更・分割

システム系のログファイルの変更・分割が行われます。

	Ver.7.0	Ver.8.0以降	
		ログファイル名	備考
管理サービスログ	adm.log	adm.log	
		service.log	各サービスの起動状態を出力
管理画面操作ログ	ctrl.log	ctrl.log	
LogLyzerExtendPackログ	loglyzersys.log	loglyzersys.log	
Tomcatログ	catalina.log	catalina.log	tomcat/logs 以下に出力
CLI　エラーログ	amserror.log	amserror.log	
フィルタリングサービスログ	sys.log	proxy.log	プロキシログ
		filtering.log	フィルタリングログ
		cache.log	キャッシュサーバ（各設定値を保持）ログ
		cacheini.log	キャッシュサーバ初期化ログ
		matching.log	データベースマッチングログ
規制解除申請ログ	offer.log	offer.log	
ウイルスチェック連携ログ	なし	icap.log	Ver.8.5以降
注意ログ(認証に失敗した理由などが記録されます。)	なし	notice.log	Ver.8.5 SP1以降
バージョンアップログ	update.log	update.log	
Geoスコープログ	なし	geo.log	Ver9.0以降のマスタのみ

実際にはログファイル名の先頭にプレフィックス（デフォルトでは「InterSafe_」が付与されます。

5-13.ログ設定

ログ設定の内容は引き継がれます。

注意点①「出力項目」
「転送データサイズ」は「送信データサイズ」「受信データサイズ」に、
「ファイルタイプ」は「ファイルタイプ」「コンテンツタイプ」に分割
されます。

Ver.7.0まで		Ver.8.0以降		ICAP版の出力
名称	初期値	名称	バージョンアップ後の設定	
グループ名	ON	グループ名	引き継ぎ	○
アカウント名	ON	アカウント名	引き継ぎ	○
ブラウザバージョン	OFF	ブラウザバージョン	引き継ぎ	○
WWWサーバIP	OFF	WWWサーバIP	引き継ぎ	○
応答コード	ON	応答コード	引き継ぎ	×
転送データサイズ	ON	送信データサイズ	引き継ぎ	○
		受信データサイズ	引き継ぎ	×
ファイルタイプ	ON	ファイルタイプ	引き継ぎ	○
		コンテンツタイプ	引き継ぎ	×
-	-	応答カテゴリ	OFF　（新項目）	○
HTTPバージョン	OFF	HTTPバージョン	引き継ぎ	○
リクエストメソッド	OFF	リクエストメソッド	引き継ぎ	○
-	-	リンク元サイト	OFF　（新項目）	○

5-13.ログ設定

注意点②「出力条件」
出力条件にConfirm、CfmPostが追加されます。
一時解除画面(Ver.7.0ではオーバーライド)を表示した際に出力されます。

Ver.7.0まで		Ver.8.0以降	
名称	初期値	名称	バージョンアップ後の設定
Proxied：転送したデータ	ON	Proxied：転送されたリクエスト	引き継ぎ
	ー	Confirm：規制されたリクエスト（一時解除可能）	新項目 Blocked　がONの場合ON OFFの場合OFF
Blocked：規制したデータ	ON	Blocked：規制されたリクエスト	引き継ぎ
Allowed：カテゴリ別ルールで許可されたデータ	ON	Allowed：ルールで許可されたリクエスト	引き継ぎ
Release：オーバーライド機能によって転送したデータ	ON	Release：一時解除で転送されたリクエスト	引き継ぎ
ー	ー	CfmPost：書き込み規制されたリクエスト（一時解除可能）	新項目 BlkPost　がONの場合ON OFFの場合OFF
BlkPost：書き込み規制によって規制されたデータ	ON	BlkPost：書き込み規制されたリクエスト	引き継ぎ

5-14.CLI(各種設定コマンド)

コマンド名、コマンド仕様に変更があります。

	Ver.7.0	Ver.8.0以降	CSV 仕様変更
アカウント管理	amsuser	amsaccount	あり
IPアドレスユーザの管理	amsip	amsip	あり
グループ管理	amsgroup	amsgroup	あり
例外URL設定	amsurl	amsurl	あり
カテゴリ別メッセージの変更/出力	amscatemsg	amscatemsg	あり
カテゴリ別書き込み規制サイズの変更/出力	amscatepostsize	amscatepostsize	あり
ルール適用（グループ）管理の変更/出力	-	amsgruleflg	新設
ルール適用（ユーザ）管理の変更/出力	-	amsuruleflg	新設
ルール管理	amsrule	amscaterule	名称変更のみ
カテゴリ別書き込み規制サイズの変更/出力(例外ユーザ)	amucatepostsize	-	廃止
例外ユーザの管理	amsexuser	-	廃止

※赤字は名称が変更になったコマンドです。

5-15.CLI（amstuneコマンド）

Ver.8.0以降では、ISWFの処理能力向上を目的とした、Windows/Linux/Solarisのチューニングを行うamstuneコマンドを用意しております。

【操作方法】

1.サーバのパラメータ表示

<インストールディレクトリ>*/bin/amstune –s*

■実行結果（環境によって表示される値は異なります。）

Linuxの場合	Solarisの場合	Windowsの場合
Current Parameters: *ip_local_port_range=～* *tcp_fin_timeout=～*	*tcp_smallest_anon_port=～* *tcp_fin_timeout=～*	Current Parameters: MaxUserPort=～ TcpTimedWaitDelay=～

2.最適化設定

<インストールディレクトリ>*/bin/amstune -l original | medium | high | extra*

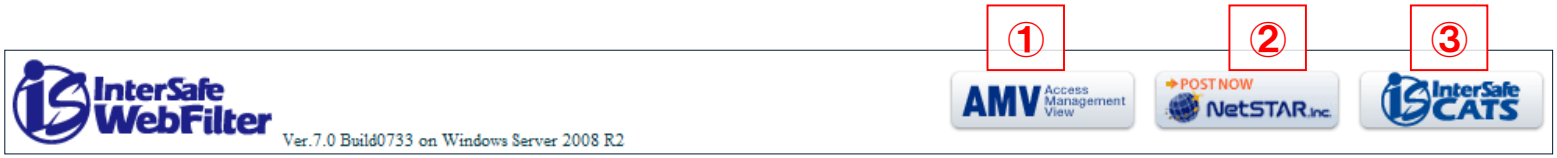
■オプションの説明

original　：コマンド初回実行時のパラメータ値に戻します。
medium　：緩やかなパフォーマンス向上を想定したパラメータチューニングを実施します。
high　　：高性能なパフォーマンスを想定したパラメータチューニングを実施します。
extra　　：さらに高性能なパフォーマンスを想定したパラメータチューニングを実施します。
（Linux 版のみ対応）

※Ver.5.0、Ver.6.x、Ver.7.0からVer.9.0へバージョンアップする場合、バージョンアップ中、OSチューニングの作業があります。この際、チューニングを実施した場合は、amstuneの「 high 」のオプションの内容でチューニングが行われます。なお、Ver.8.0以降からVer.9.0へバージョンアップした場合は、バージョンアップ中、OSチューニングの作業は含まれておりません。チューニングが必要な場合は、バージョンアップ後にamstuneコマンドでチューニングを行ってください。

5-16.管理画面ヘッダ部のリンク変更

Ver.7.0の管理画面ヘッダ部分に配置されていた各サービスへのリンク
表示が変わります。

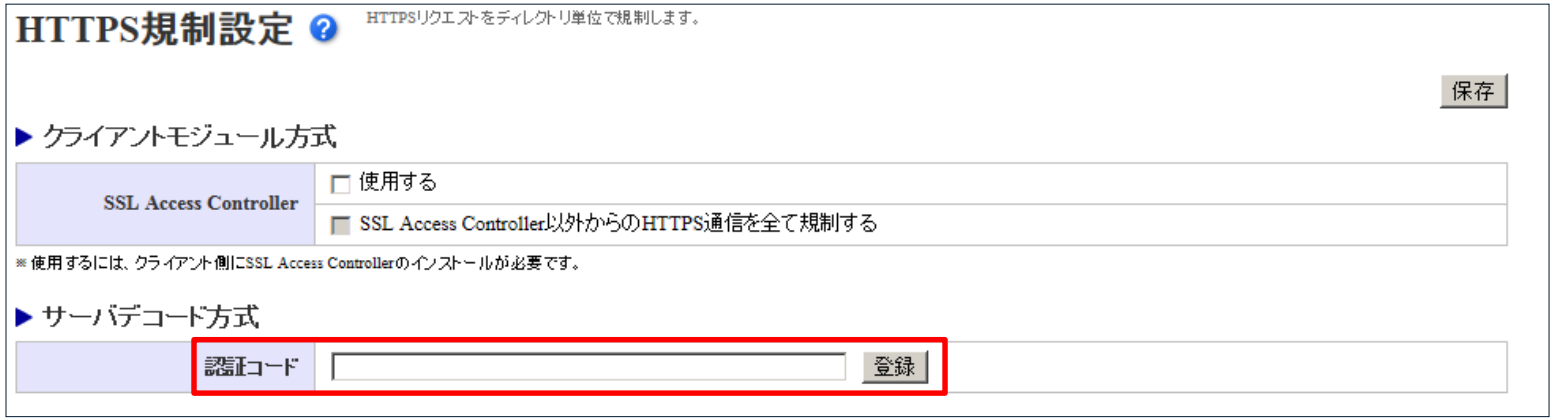


①. AMV（AccessManagementView）
　Ver.8.0以降では本機能は省略されます。
②. ネットスターリンク（カテゴリ確認システム）
　管理画面ホームの「カテゴリ確認システム」のリンクから表示できます。
③. InterSafe CATSへのリンク
　Ver.8.0以降では省略されます。

5-17.HTTPS解析のアクティベート方法

HTTPS解析機能(Ver.7.0以降の機能)を利用するためには、通常、申請(認証コードの発行）と、認証コードの登録が必要になりますが、バージョンアップ前にHTTPS解析機能をご利用のお客様は、バージョンアップ後もHTTPS解析機能が有効な状態となりますので、申請、再設定は不要です。

※Ver.8.0以降ではHTTPS解析機能（サーバデコード）のアクティベート方法が変わります。Ver.8.0以降からHTTPS解析機能を初めて利用される場合は、認証コードの発行を行い、管理画面の[共通アクセス管理]-[HTTPS規制設定]に、 発行された認証コードを登録してください。



認証コードの発行は弊社ダウンロードサイトよりお申し込みください。
弊社3営業日以内にご連絡いたします。
「ダウンロードサイト」
https://alsi-iss.jp/download/intersafe/

5-18.金融カテゴリ

※この注意事項は、バージョンアップ前まで、「金融カテゴリのサイトのトップページを登録していない専用のデータベース」をご利用のお客様が対象です。

●管理画面にて利用有無を確認する方法
[システム管理]-[ダウンロード設定]でサーバを選択し、表示された「ダウンロード先URL」のURL（ディレクトリ部）に「～**ex**」が指定されている場合、専用のデータベースをご利用です。

●Ver.7.0の設定ファイル（proxy.inf）にて利用の有無を確認する方法
<インストールディレクトリ>/conf/proxy.inf内、[SYSTEM_UPDATE]セクションの「DB_ALIAS=」に「～**ex**」が指定されている場合、専用のデータベースをご利用です。

詳細は以下FAQページをご参照ください。
FAQ No.4090 「【Ver.5.0～Ver.7.0】金融カテゴリに分類されるサイトをトップページで規制させない方法」
http://support.alsi.co.jp/faq_detail.html?id=4089&category=

5-18.金融カテゴリ

※この注意事項は、バージョンアップ前まで、「金融カテゴリのサイトのトップページを登録していない専用のデータベース」をご利用のお客様が対象です。

Ver.8.0以降では、「金融カテゴリのサイトのトップページを登録していない専用のデータベース」がございませんが、その代わりに、金融サイトのトップページを登録していないサブカテゴリをそれぞれ用意しております。専用のデータベースをご利用のお客様がバージョンアップした場合は、動作に変化を与えないよう、カテゴリを自動設定します。自動設定の内容は以下の通りです。

Ver.7.0	Ver.8.0		バージョンアップ後の設定
投資商品の購入	投資商品の購入	V7と同じ名前	規制
	証券・先物取引	新設	許可
金融商品・サービス	金融商品・サービス	V7と同じ名前	規制
	銀行	新設	許可
	ローン・決済	新設	許可
保険商品の申込	保険商品の申込	V7と同じ名前	規制
	保険	新設	許可

新設 のカテゴリは、それぞれ、**トップページ自体を登録**したカテゴリとして用意されています。V7と同じ名前 のカテゴリは、**トップページ以外のサイト**が登録されております。バージョンアップ後は、上記の通り、新設 には **許可**、V7と同じ名前 には **規制** が自動設定されます。これによって、トップページが規制されない動作となります。

5-19.認証局設定について

■Proxy版
Ver8.5 SP1 修正パッチ(Build0881)以降では、HTTPS規制画面表示や、HTTPS規制設定サーバデコード方式使用時の認証局証明書を動的に作成することが可能です。
具体的な手順については、「Proxy版 認証局設定マニュアル 」をご参照ください。

■ICAP版
Ver8.5 SP1(Build0870)以降では、HTTPS規制画面表示時の仕様が変更(※)になった影響で、HTTPS規制画面表示時にブラウザのSSL警告が表示されるようになっています。
Ver8.5 SP1 修正パッチ(Build0881)以降では、HTTPS規制画面表示時にブラウザのSSL警告画面を非表示にすることが可能です。
具体的な手順については、「ICAP版 認証局設定マニュアル 」をご参照ください。

(※)HTTPS規制画面表示時に規制理由を表示するように仕様が変更されています。

※各マニュアルの入手については、2枚目のスライドに記載のサポート窓口までご連絡ください。

5-20.HTTPSタイムアウト値について

Ver.8.5 SP1以降でHTTPS通信タイムアウト値が新規に追加されました。(Proxy版のみ)
HTTPSデコードが無効の状態で、HTTPSリクエスト転送時に参照されるタイムアウト値が変更になります。

	Ver.8.5まで	Ver.8.5 SP1以降
HTTPSデコード無効時	サーバ接続タイムアウト値 (初期値60秒)	**HTTPS通信タイムアウト値 (初期値90秒)**
HTTPSデコード有効時	サーバ接続タイムアウト値 (初期値60秒)	サーバ接続タイムアウト値 (初期値60秒)

各タイムアウト値は、管理画面の[サーバ管理]-[サーバ設定]-[フィルタリングサービス情通設定]より設定します。

5-21.Ver8.5 SP2以降のセキュリティ強化について

Ver.8.5 SP2 Proxy版では、HTTPS通信のセキュリティ強化機能がデフォルトで有効となっており、その影響でバージョンアップ後、任意のHTTPSサイトと通信できなくなる場合があります。

バージョンアップ前と同じ挙動としたい場合は、FAQNo. 4967をご参照いただき設定変更を実施してください。

5-22.認証除外設定の引継ぎについて

ホワイトリスト運用のため、リクエスト別認証設定 > 宛先ホスト認証 に何も記載せず運用している環境（空欄）で、アップデート後に下記の認証除外設定が追加されます。
「update.microsoft.com」

この場合には、手動で削除を行ってください。

6.ログレポートツール

Ver.9.0のアクセスログ・POSTログ、ICAP連携ログをレポートできるレポーティングツールについて説明します。
※ICAP連携ログは、Ver8.5より追加された、「ウィルスチェック連携」において、ICAP 連携した際の処理内容が記録されるログファイルです。
「ウィルスチェック連携」の詳細については、管理者マニュアルをご覧ください。

6.ログレポートツール

ISWF Ver.9.0 の対応レポートツールは以下の通りです。

InterSafe LogDirector 4.0.10
LogLyzer Ver.8.5

●InterSafe LogDirector(LD)をご利用のお客様

・LD Ver.3.0以前をご利用のお客様は、LD Ver.4.0へバージョンアップが必要です。
アップデートインストーラにてバージョンアップを行ってください。
・LD Ver.3.0からVer.4.0への変更は製品の再インストールになります。
・LD Ver.4.0～からVer.4.0.10へビルドアップも再インストールになります。
※アンインストール前にログデータをエクスポートいただくことで、 LD Ver.4.0へインポートが可能です。詳細はLD Ver.4.0の管理者マニュアルをご参照ください。
※ISWF Ver.8.5以降のICAP連携ログはLD Ver.4.0以降で取り込みが可能です。

●LogLyzer(LL)をご利用のお客様

・LL Ver.8.0以前をご利用のお客様は、LL Ver.8.5へバージョンアップが必要です。
現在のLLをアンインストール後、LL Ver.8.5をインストールしてください。
※アンインストール前にログデータをエクスポートいただくことで、 LL Ver.8.5へインポートが可能です。詳細はLL Ver.8.5の管理者マニュアルをご覧ください。

・ISWF Ver.7.0以前のログがLLに取り込まれた状態で、ISWF Ver.9.0のログを取り込むと、
レポートには新カテゴリと旧カテゴリが両方表示されます。

INTERNAL SECURITY SOLUTIONS

情報を守り、活用する。

アルプス システム インテグレーション株式会社

ホームページ　http://www.alsi.co.jp
FAQサイト　http://support.alsi.co.jp

●サポート窓口
メール：support@alsi.co.jp
TEL：03-5499-1331
（受付時間　平日10:00 ～ 12:00、13:00 ～ 17:00）