



InterSafe WebFilter Ver.9.1 SP1 バージョンアップ概要・注意事項(初版)

セキュリティ事業部プロダクト技術部

作成日 2020.6.1

アルプスシステムインテグレーション株式会社

© Alps System Integration Co., Ltd. All rights reserved.



はじめに 変更履歴

Chapter 1 必要条件

- 1-1.動作要件
- 1-2.製品タイプ

Chapter 2 バージョンアップの流れ

Chapter 3 注意事項(作業前)

- 3-1.設定情報のバックアップ
- 3-2.keystoreファイルのバックアップ
- 3-3.ulimitの確認(LinuxOSのみ)
- 3-4.tomcatのポート確認
- 3-5.カスタマイズ規制画面ファイルのバックアップ
- 3-6.マスタ・スレーブ構成でのバージョンアップ

Chapter 4 バージョンアップ後の作業

- 4-1.データベースのダウンロード
- 4-2.最大ヒープサイズの設定
- 4-3.その他の作業

Chapter 5 注意事項(作業後)

- 5-1.HTTPS規制画面の動作変更
- 5-2.利用ポートの確認
- 5-3.認証局設定について
- 5-4.HTTPSタイムアウト値について
- 5-5.Ver.8.5 SP2以降のセキュリティ強化について

Chapter 6 新機能について

- 6-1.最新OSへの対応
- 6-2.CLIコマンドの拡張
- 6-3.文部科学省のYouTubeについて
- 6-4.ヘッダ制御設定
- 6-5.規制画面の拡充

Chapter 7 ログレポートツール

はじめに

本資料は、

InterSafe WebFilter Ver.9.1 SP1

(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

お問い合わせフォーム https://alsifaq.dga.jp/support_form.html

また、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

變更履歷

日付	変更内容
2020/06/01	新規作成

Chapter 1 必要条件

1-1.動作要件

1-2.製品別条件

ISWFが動作するサーバについて

Windows版

[OS(64bit)]

- ・ 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
- ・ 日本語版Microsoft Windows Server 2019 Standard

[CPU] OSの動作要件を満たすこと

[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)

※ここに記載されていないエディションで不具合が生じた場合は、上記のシステム環境で再現した場合に対応します。

Linux版

[OS(64bit)]

- Red Hat Enterprise Linux 6
Linux カーネル v 2.6.32および glibc v 2.11
- Red Hat Enterprise Linux 7
Linux カーネル v 3.10.0および glibc v 2.17
- Red Hat Enterprise Linux 8
Linux カーネル v 4.18.0および glibc v 2.28

※RHEL8の環境ではWebFilterをインストールする前に「libnsl」のインストールが必要となります。

[CPU] OSの動作要件を満たすこと

[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

ISWF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。

ISWF for ICAPを使用する場合

[ICAP クライアント]

Blue Coat ProxySG SGOS 5.4~5.5/6.4~6.7

Squid 3.3~3.5、4.4

A10 Thunder CFW/SSLi ACOS 4.1

LDAP連携を行う場合

[LDAPサーバ]

- Active Directory:Windows Server 2012
- Active Directory:Windows Server 2012 R2
- Active Directory:Windows Server 2016
- Active Directory:Windows Server 2019
- OpenLDAP 2.4.35
- Oracle Directory Server Enterprise Edition 11 g R2

※Windows Server 2012、Windows Server 2012 R2 およびWindows Server 2016、Windows Server 2019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リサービス(AD LDS)には対応していません。

※NTLM認証及びKerberos認証はWindows Server 2012、Windows Server 2012 R2、Windows Server 2016、Windows Server 2019が対応しています。

ISWFに接続するクライアント

[Windows]

[ブラウザ]

- Internet Explorer 11 (Microsoft)
- Microsoft Edge (Microsoft)
- Firefox (Mozilla)
- Chrome (Google)

※NTLM認証を行う場合は、Internet Explorer 11、Firefox、Chrome の利用を推奨します。

※Kerberos認証を行う場合は、Internet Explorer 11の利用を推奨します。

[macOS]

[ブラウザ]

Safari

[Mac iOS/iPadOS]

[ブラウザ]

Safari

※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]

[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

ISWFの管理画面操作に使用するクライアント

[Windows]

[ブラウザ]

Internet Explorer 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。

Proxy版

Ver.5.0以降のProxy版からVer.9.1 SP1 Proxy版へ移行できます。

ICAP版からProxy版への移行はできません。

Ver.8.5 SP2以降はSolarisはサポート対象OSではないため、サポート対象のOSへ変更が必要です。

ICAP版

Ver.5.0以降のProxy版からVer.9.1 SP1 ICAP版へ移行できます。

Proxy版からICAP版への移行はできません。

Ver.8.5 SP2以降はSolarisはサポート対象OSではないため、サポート対象のOSへ変更が必要です。

●参考情報 Squid版

Squid版はVer.8.0以降では販売を終了しました。

Ver.7.0からVer.9.1 SP1にバージョンアップは可能ですが、ICAP版として移行されます。

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、Squidの再インストールが必要です。

Chapter 2

バージョンアップの流れ

事前準備

- 設定ファイルのバックアップを取得します
- ISWF Ver.9.1 SP1のプログラムをサーバ上にコピーしておきます

Ver.UP作業

- ISWFのサービスを停止します
- setup.exe(WindowsOS)、setup.sh(LinuxOS)を実行します

※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

完了

- ISWFのサービスを起動します

Chapter **3 注意事項(作業前)**

3-1.設定情報のバックアップ

3-2.keystoreファイルのバックアップ

3-3.ulimitの確認(LinuxOSのみ)

3-4.tomcatのポート確認

3-5.カスタマイズ規制画面ファイルのバックアップ

3-6.マスタ・スレーブ構成でのバージョンアップ

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。

●バックアップする設定情報

Windows : <ISWFインストールフォルダ>¥conf

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

※バックアップはISWFの全サービスを停止した上で行って下さい。
もしくは、ISWFの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。

●補足情報

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

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。

● バックアップする設定情報

Windows : <ISWFインストールフォルダ>¥tomca配下のファイル

Linux / Solaris : <ISWF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で利用する場合は、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」を参照して、再設定を行ってください。

● 補足情報

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

Ver.8.5以降で、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
```

※初期状態では非表示のため、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の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=

●補足情報

例えば、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.9.1 SP1へバージョンアップすると、ファイルディスクリプタが32768に減少する結果になるため、LIMIT_NOFILEの設定を40000以上に変更します。

環境によっては、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。設定手順は以下のFAQ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=

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。

※Ver.8.0以降からバージョンアップする場合、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。

●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>

●補足情報

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

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。

Chapter 4

バージョンアップ後の作業

4-1. データベースのダウンロード

4-2. 最大ヒープサイズの設定

4-3. その他の作業

Ver.8.0以降からVer.9.1 SP1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です。

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。

手動でデータベースをダウンロードする手順は、以下のFAQをご参照ください。

FAQ No.5344「手動でURLデータベースを更新する方法」

http://support.alsi.co.jp/faq_detail.html?id=5344&category=

※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のFAQをご参照ください。

FAQ No.4091「Ver.9.1/9.0/8.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=

最大ヒープサイズの初期設定が 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、最大ヒープサイズを256Mbyteに抑えてあります。

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。

Proxy版でヒープサイズ 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、プロセス数の総和を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。)
ICAP版の場合は、ヒープサイズについては256Mbyteから変更する必要はほとんどありません。

Chapter3 の下記項目に該当する場合は、スライドの内容に沿って作業を行ってください。

[3-2.keystoreファイルのバックアップ](#)

[3-3.ulimitの確認\(LinuxOSのみ\)](#)

[3-4.tomcatのポート確認](#)

Chapter **5 注意事項(作業後)**

5-1.HTTPS規制画面の動作変更

5-2.利用ポートの確認

5-3.認証局設定について

5-4.HTTPSタイムアウト値について

5-5.Ver.8.5 SP2以降のセキュリティ強化について

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。

この仕様は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変更されました。

ISWFのバージョン	規制理由・一時解除ボタン表示
8.0	不可
8.5 Build0860まで	不可
8.5 SP1 Build0870以降	可能

ISWFでは以下のポートを利用します。
 ファイアウォール等を利用している場合、以下のポートが利用できるようにしてください。

ポート名	ポート番号	ポート名	ポート番号
管理サービス用ポート(全製品共通)	41212	ICAP ポート(全製品共通)※	1344
データ同期用ポート(全製品共通)	41213	Webコンテンツキャッシュ制御待受ポート (Ver.8.5 SP2以降 Proxy版のみ)	41211
フィルタリングサービス制御用ポート (全製品共通)	41214	HTTP規制画面出力用ポート(ICAP版のみ)	21128
	41215	HTTPS規制画面出力用ポート(ICAP版のみ)	443
	41216	ARMS連携機能のコールバック待受ポート (Ver.8.5 SP2以降)	8319
	5963	アクセスログエージェントポート(Ver.9.0以降)	41210
管理画面用ポート(全製品共通)	2319	集計データベースサービスポート(Ver.9.0以降の マスタのみ)	41209
HTTP ポート(Proxy版のみ)	8080	管理画面停止用ポート(全製品共通)	8005
HTTPS ポート(Proxy版のみ)	8443		
FTP OVER HTTP ポート(Proxy版のみ)	8021		

※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。

Proxy版

Ver.8.5 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、認証局設定の「Proxy版利用マニュアル」をご参照ください。

ICAP版

Ver.8.5 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した。

Ver.8.5 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、認証局設定の「ICAP版利用マニュアル」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、[はじめに](#)に記載のサポート窓口までご連絡ください。

●補足情報

ISWFのバージョン	利用証明書
Ver.8.0～Ver.8.5	SHA-1
Ver.8.5 SP1	SHA-1 ※Build0881以降であれば、SHA-256に変更可能。
Ver8.5 SP2以降	新規インストールの場合は、SHA-256 バージョンアップの場合は過去バージョンでSHA-1を利用しているとSHA-1のまま ※SHA-256に変更可能。

また、HTTPSデコード時はWebサーバ(上位サーバ)より受け取ったサーバ証明書が信頼できる証明書か、独自の証明書リストを使用してチェックを行います。バージョンアップの場合、以前のバージョンの証明書リストを引き継ぐため、アクセスするWebサイトによっては証明書の警告画面が表示される場合があります。この動きは最新の証明書リスト情報へ更新することで、回避できる場合があります。更新手順については、以下のFAQをご参照ください。

FAQ No.5398「証明書リスト更新」

http://support.alsi.co.jp/faq_detail.html?id=5398&category=

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、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。

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、以下のFAQをご参照いただき設定変更を実施してください。

FAQ No.4967 「(WebFilter ver8.5 SP2以降)セキュリティ機能について」
http://support.alsi.co.jp/faq_detail.html?id=4967&category=

Chapter 6 新機能について

6-1.最新OSへの対応

6-2.CLIコマンドの拡張

6-3.文部科学省のYouTubeについて

6-4.ヘッダ制御設定

6-5.規制画面の拡充

Redhat Enterprise Linux8の対応を開始しました

Windows版インストールプログラムがWindows Server 2019に対応しました

これまで、Windows Server 2019 OS専用のインストールプログラムとなっていますが、通常のWindowsOS用のインストールプログラムにてWindows Server 2019にインストールできるようになりました。

ユーザ管理(amsaccount)

amsaccount に以下のオプションが追加されました。

amsaccount **-search**

-searchオプションを使用すると、登録されているユーザを検索して画面に出力します。
指定したアカウント名に部分一致したユーザについて、グループ名と併せて出力されます。

例外URL(amsurl)

amsurl に以下のオプションが追加されました。

amsurl **-add**

-addオプションを使用すると、指定されたファイルに記述されている例外URLを登録します。
※amsurl -import は上書きとなりますが、amsurl -add は追加となります。

例外URL(amsurl)

amsurl に以下のオプションが追加されました。

amsurl -clear

-clearオプションを使用すると、指定されたファイルに記述されている例外URLルールに登録された例外URLデータを一括削除します。

例外サービスに文部科学省のYouTubeに特化したメニューが追加されました。
これにより、管理画面より簡単に文部科学省の動画コンテンツを許可できます。

例外サービス登録

カテゴリを規制した状態で特定のサービスを利用する場合の

選択中のルール

ルートグループ >






▶ サービス一覧

登録したいサービスを一覧から選択します。

サービス名:

検索

サービスカテゴリ名:

Yahooキッズ	
YouTube	
YouTube_文部科学省	
ZOZOTOWN	
fromA navi	

Ver9.1 SP1より、ヘッダ制御設定が管理画面より行うことができるようになりました。



ヘッダ編集設定 ?

リクエストヘッダに追加する項目をドメイン単位で設定します。



ホーム ?

使用したい機能を

- HTTPS規制設定
- 高度分類クラウド設定
- 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
- 規制画面設定
- カテゴリ名設定
- 規制オプション設定
- ヘッダ編集設定

ログイン情報

グループ	ADMIN
ユーザ	root
権限	システム
前回ログイン日時	2020/

ドメイン別ヘッダ編集設定

保存

+ 設定を追加

1	ヘッダ編集	<input checked="" type="checkbox"/> 有効		
	* 対象ドメイン	mail.google.com		
		※ 改行区切りで複数指定できます。		
	* ヘッダ	リクエストにヘッダを追加する	+ 項目を追加	
		* ヘッダ名	ヘッダ値	削除
		X-GoogApps-Allowed-Domains	example.com	<input type="checkbox"/>

削除



- ① 規制画面内に規制したサーバ名と規制時間が表示されるようになりました
- ② 規制画面より認証局証明書のダウンロードが可能になりました

① サーバ名 デフォルトサーバ
応答日時 2020/06/01 16:08:47.503



このウェブサイトは現在管理者によって規制されています。

あなたがリクエストしたURL

<https://www.alsi.co.jp/>

規制理由(カテゴリ)

ITサービス > IT

Information Technology Service > Information Technology

② 認証局証明書のダウンロード

ダウンロード

Chapter 7 ログレポートツール

ISWF Ver.9.1 SP1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)をご利用の場合
 - ・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。
※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。
 - ・LD Ver.4.0～からVer.4.0.10へはアップデートをご利用ください。
※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。
 - ※LogLyzerは2021年6月30(水)に提供が終了します。



もっと豊かな情報未来へ
アルシー・ソリューション

www.alsi.co.jp

