

InterSafe plus

CSRF 脆弱性対応手順マニュアル

—InterSafe LogDirector—

提供元： ALPS SYSTEM INTEGRATION Co., LTD.

2024/9/9 初版

目次

はじめに	3
脆弱性対策適用手順	4

はじめに

本書では、InterSafe LogDirector におけるクロスサイトリクエストフォージェリ (CSRF) の脆弱性 (JVN#05579230) への対策として、InterSafe LogDirector 導入ディレクトリへの Tomcat 関連ファイル配置・ファイル編集での対応方法をご案内します。

<脆弱性対応適用条件>

- ・本脆弱性対応は、InterSafe LogDirector Ver. 4.0.11 以降のバージョンに適用可能です。

脆弱性対策適用手順

※InterSafe LogDirector Ver. 4.0.11 以降に適用が可能です。

※InterSafe LogDirector のインストールディレクトリは、初期値では以下の通りです。

Linux 版 : /usr/local/logdirector

Windows 版 (Tomcat) : C:\Program Files\Apache Software Foundation\Tomcat 7.0

以下、初期値でのインストールを前提に記載いたします。

<脆弱性対策適用手順>

- (1) InterSafe LogDirector サービス (Tomcat サービス) を停止します。

Linux 版: 以下コマンドで InterSafe LogDirector サービスを停止します。

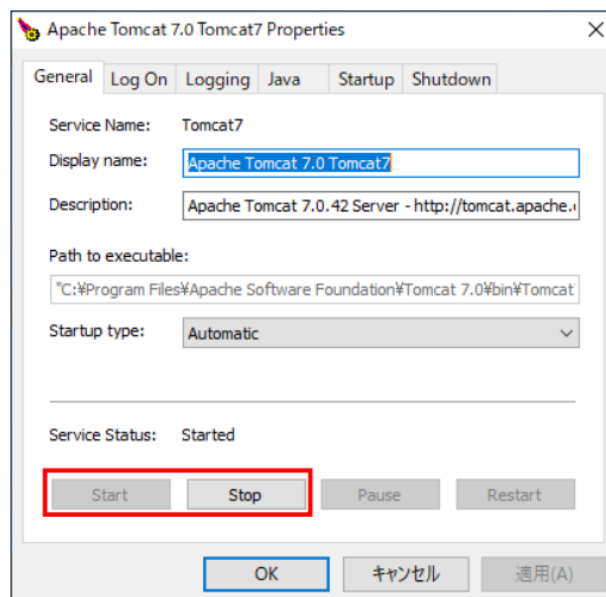
停止コマンド:

```
/usr/local/logdirector/bin/log_director_ctl.sh stop
```

Windows 版: 以下手順にて Tomcat サービスを停止します。

Tomcat サービス の停止

- 1) InterSafe LogDirector 導入サーバにログインし、
[スタート]ボタン→[Apache Tomcat 7.0 Tomcat7]→[Monitor Tomcat]を
クリックします。
「Apache Tomcat 7.0 Tomcat7 Properties」画面が表示されます。
- 2) 画面下部で[Stop]をクリックします。



(2) CSRF 脆弱性対応のフィルターを適用するため、製品ダウンロードサイトより nssvlfiltr.jar をダウンロードの上、以下のパスへ配置をお願い致します。

Windows の場合 :

C:\Program Files\Apache Software Foundation\Tomcat 7.0\lib\nssvlfiltr.jar

Linux の場合 :

/usr/local/logdirector/tomcat/lib/nssvlfiltr.jar

※注意点 : Linux の場合、ファイルの所有者はインストール時に設定したユーザに揃えていただけますようお願いいたします。

(デフォルトでは lduser となっております。)

(3) Tomcat の以下の設定ファイルを編集し、フィルターを有効化します。

Windows の場合 :

C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf\web.xml

Linux の場合 :

/usr/local/logdirector/tomcat/conf/web.xml

編集(追記)箇所は次ページ内の赤字部分となります。

※注意点 : web.xml への追記の際は、赤字部分で記載しているタグをコメントアウトタグ内に記載しないようご注意ください。

▼web.xml 記載箇所（赤字箇所を追記します。）

～省略～

```
<!-- （～省略～）
    <param-name>isVirtualWebappRelative</param-name>
    <param-value>>false</param-value>
  </init-param>
</filter>
-->
```

～追記する設定値～

```
<filter>
  <filter-name>SameSiteCookieHeaderFilter</filter-name>
  <filter-class>
    jp.netstar.servlet.filter.SameSiteCookieHeaderFilter
  </filter-class>
  <init-param>
    <param-name>strict</param-name>
    <param-value>JSESSIONID</param-value>
  </init-param>
  <init-param>
    <param-name>log</param-name>
    <param-value>>false</param-value>
  </init-param>
</filter>
```

～追記する設定値～

～省略～

```
<!--
    <filter-name>ssi</filter-name>
    <url-pattern>*.shtml</url-pattern>
  </filter-mapping>
-->
```

～追記する設定値～

```
<filter-mapping>
  <filter-name>SameSiteCookieHeaderFilter</filter-name>
  <url-pattern>/*</url-pattern>
</filter-mapping>
```

～追記する設定値～

(4) ファイル配置後は InterSafe LogDirector サービス (Tomcat サービス) を起動します。

Linux 版: 以下コマンドで InterSafe LogDirector サービスを起動します。

起動コマンド:

```
/usr/local/logdirector/bin/log_director_ctl.sh start
```

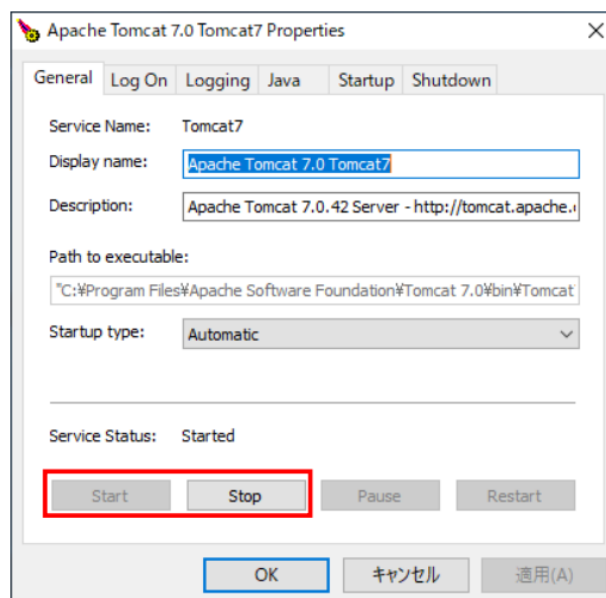
Windows 版: 以下手順にて Tomcat サービスを起動します。

Tomcat サービス の起動

2) InterSafe LogDirector 導入サーバにログインし、
[スタート]ボタン→[Apache Tomcat 7.0 Tomcat7]→[Monitor Tomcat]を
クリックします。

「Apache Tomcat 7.0 Tomcat7 Properties」画面が表示されます。

2) 画面下部で[Start]をクリックします。



以上で InterSafe LogDirector の CSRF 脆弱性対策は完了です。