CSRF 脆弱性対応手順マニュアル

ALPS SYSTEM INTEGRATION Co.,LTD.

2024/9/9 初版

目次

はじめに

本書では、InterSafe WebFilter 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 WebFilter Tomcat 関連ファイルの編集での対応方法をご案内します。

なお、本書でご案内するファイル編集での脆弱性対応はワークアラウンド対応であり、Build 表記は変更とならない点、ご了承ください。

本脆弱性への対応としましては、本書で案内するファイル編集手順以外に、修正パッチである Ver9.1 SP4 Build1653 適用での対応手順がございます。パッチ適用にて対応の場合、Build 表記も「Build1653」へ変更となります。運用方針・ご要件に応じてパッチでの適用もご検討をお願いいたします。

脆弱性対策適用手順

＜脆弱性対策適用の条件・注意事項＞
・InterSafe WebFilter Ver9.1 SP4 に適用が可能です。
・本書で案内するファイル書き換え・管理画面サービス再起動の手順は、プライマリサーバのみでの実施となります。
・本書で案内するファイル書き換えでの脆弱性対応はワークアラウンド対応であり、Build 表記は変更とならない点、ご了承ください。

＜脆弱性対策適用手順＞
CSRF 脆弱性対策として Cookie の属性設定を変更するため、
InterSafe WebFilter 設定ファイルの編集を行います。

① 以下ファイルを開きます。
Linux: ＜InterSafe WebFilter 導入ディレクトリ＞/tomcat/conf/context.xml
Windows : ＜InterSafe WebFilter 導入ディレクトリ＞¥tomcat¥conf¥context.xml

※InterSafe WebFilter 導入ディレクトリは、デフォルトでは以下の通りです。
Linux: /usr/local/intersafe
Windows: C:¥InterSafe

② context.xml をエディタで開き、ファイル内に以下タブの追記を行います。

追記するタブ：

```
<CookieProcessor className="org.apache.tomcat.util.http.Rfc6265CookieProcessor" sameSiteCookies="strict" />
```

実際の追記例は次ページに掲載しております。

▼context.xml 追記例

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<!-- The contents of this file will be loaded for each web application -->
<Context>

    <!-- Default set of monitored resources. If one of these changes, the    -->
    <!-- web application will be reloaded.                                   -->
    <WatchedResource>WEB-INF/web.xml</WatchedResource>
    <WatchedResource>WEB-INF/tomcat-web.xml</WatchedResource>
    <WatchedResource>${catalina.base}/conf/web.xml</WatchedResource>

    <!-- Uncomment this to disable session persistence across Tomcat restarts -->
    <!--
    <Manager pathname="" />
    -->

    <CookieProcessor className="org.apache.tomcat.util.http.Rfc6265CookieProcessor" sameSiteCookies="strict" />

</Context>
```

③ InterSafe WebFilter の管理画面サービス（拡張 WEB サービス）を再起動します。

標準インストール先の場合：
Linux: ＜InterSafe WebFilter 導入ディレクトリ＞/bin/amsweb restart
Windows: [コントロールパネル]-[サービス]より
拡張 WEB サービス「InterSafeWebService」を再起動します。

以上で CSRF 脆弱性対応は完了です。