SPバージョン2アップデートに関する情報

Shibboleth SPバージョン2系列の全てのバージョンに脆弱性が見付かっております。
最新のShibboleth SPへのアップデートに関してはこちらをご覧ください。⇒SPv3アップデートに関する情報

バージョン共通

CentOS等、yumコマンドによりインストールした環境では以下のコマンドで簡単に最新版にアップデートできます。

```
$ sudo yum update
```

もしくは、Shibboleth SP関連のパッケージのみをアップデートする場合は、代わりに以下のコマンドを実行してください。

```
$ sudo yum update shibboleth libsaml9 libxmltooling7 libxml-security-c17 liblog4shib1 opensaml-schemas xmltooling-schemas libxerces-c-3_1 libcurl-openssl xerces-c
（OSによっては libcurl-openssl パッケージや libxerces-c-3_1 パッケージが存在しない場合がありますが、無視されますので問題ありません）
```

アップデート後、httpdおよびshibdが再起動されていることを確認し、再起動されていなければ手動で再起動してください。

```
$ sudo /sbin/service shibd restart
$ sudo /sbin/service httpd restart
```

CentOS 7の場合コマンドが異なります。自動再起動されていない場合は以下のコマンドを用いてください。

```
$ sudo systemctl restart shibd
$ sudo systemctl restart httpd
```

※ 例えば、2.6.0から2.6.1へのアップデートは自動的に再起動する模様。2.6.1にアップデート後、libxmltooling7のみをアップデートした場合は自動再起動されない模様。2.5.1から2.5.2へのアップデートはhttpdおよびshibdを自動的に再起動する模様。2.4.3から2.5.2へのアップデートでは自動再起動されない模様。

注意点

2.5.0以降の機能ですが、デフォルトでは有効になっていない、オープンリダイレクタとならないための設定があります。特に事情がなければ以下の指示に従って設定を有効にしてください。

⇒オープンリダイレクタとなりうる問題の対処

SP 2.6.x からSP 2.6.x へのアップデートに関する情報

バージョンは変わっておりませんが、2.6.1リリース後にlibxmltooling7のセキュリティアップデートが出ていますので適宜アップデートしてください。
これのみの適用の場合は自動再起動されませんので、shibdおよびhttpdを再起動してください。

バージョンは変わっておりませんが、2.6.0リリース後にCentOS 6/7(RHEL 6/7)向けにlibcurl-openssslのアップデートが出ていますので、適宜アップデートしてください。同様に、2.6.1リリース後にlibcurl-openssslのセキュリティアップデートが出ています。
https://marc.info/?l=shibboleth-announce&m=151205545006433&w=2

> *A security advisory [1] and update to curl was released a couple of days ago, so we have updated the version included in our packages accordingly to 7.57.0.*
>
> *RPMs on affected platforms were published on Tuesday and the Windows installers have been updated this morning to 2.6.1.2. I'll update the release notes imminently.*

http://marc.info/?l=shibboleth-announce&m=147817836306162&w=2

> *As a sidenote, the RPMs supplied for libcurl on RHEL 6/7 have also been updated.*

SP 2.5.x から SP 2.6.x へアップデートする場合の注意点

2.6.0でのセキュリティフィックスはXerces-Cライブラリについてのみ。
いくつか機能追加および運用改善オプション（後述する verifyBackup="false"）あり。

ライブラリがlibsaml9およびlibxmltooling7にバージョンアップしています。不要なら以下のように以前のバージョンは削除してください。

```
$ sudo yum erase libsaml8 libxmltooling6
```

ignoreCase属性を使用している場合は以下の情報を元にcaseSensitiveを使うように設定ファイルを更新してください。
2016-07-27 [upki-fed:01064] Shibboleth SP脆弱性情報にかかる補足（Re: Shibboleth SP の脆弱性について (2016/5/6)

2016-07-13までに提供していたRPMパッケージはデフォルト設定ファイルのcipherSuitesに問題がありTLS接続でエラーになる可能性があります。デフォルト設定ファイルの問題ですので原則的にこの期間に新規インストールした方が対象となり、cipherSuites=の記述をコピーしていない限り以前のバージョンからアップデートした方は対象外です。
2.6.0-1.1をインストールしている方は2.6.0-2.1にアップデートした上で、shibboleth2.xmlに

```
    <ApplicationDefaults entityID="https://sp.example.org/shibboleth"
                         REMOTE_USER="eppn persistent-id targeted-id"
                         cipherSuites="ECDHE+AESGCM:ECDHE:!aNULL:!eNULL:!LOW:!EXPORT:!RC4:!SHA:!SSLv2">
```

のような記述があれば、cipherSuites="..."の部分を削除してください。
Shibboleth Projectからのアナウンス: http://marc.info/?l=shibboleth-announce&m=146834985418022&w=2

その他の新機能:
exportDuplicateValues
template (base64-encoded SAML <AuthnRequest> message)

XERCES_DISABLE_DTD=1

> ここに書いていた手順は機能しないことが判明しました。CentOS 7については、Red Hatが提供している標準パッケージのXerces-Cライブラリのバージョンが3.1.1である（2018年1月現在バックポートもされていない）ため、DTDを無効化するために必要なXerces-Cライブラリのバージョンが3.1.4以上であることを満たせません。**Shibboleth SPバージョン3以降向けにはShibboleth独自パッケージを提供している（下記CentOS 6と同じ状況である）ため、バージョンアップすることを強く推奨します。**
> ⇒SPv3アップデートに関する情報
>
> 一方CentOS 6については、Shibboleth SP 2.6.0以上であれば自動的にDTD無効化されるため特殊な作業は必要ありません。
>
> 誤った情報を提供しておりましたことをお詫びします。

CentOS 6では、脆弱性の温床であるDTD形式での記述を一切処理しないようにすることができます。Shibbolethおよび学認では使用しておりませんので、セキュリティ強化のため是非この手順を実施してください。

実施するには、/etc/sysconfig/shibdおよび/etc/sysconfig/httpdの末尾に以下の行を加えます。（CentOS 7での手順は後述）

```
export XERCES_DISABLE_DTD=1
```

shibdおよびhttpdの再起動後に、以下のようなコマンドを使って当該環境変数が設定されていることを確認してください。

```
$ sudo /sbin/service httpd restart
$ sudo /sbin/service shibd restart
$ sudo less /proc/`pidof -s shibd`/environ
$ sudo less /proc/`pidof -s httpd`/environ
```

CentOS 7では上記手順では反映されませんので、下記手順に従ってください。

shibdについては、以下のようにしてsystemdの設定で環境変数を追加します。最後のコマンドで当該環境変数が設定されていることを確認してください。

```
$ sudo systemctl edit shibd.service
[Service]
Environment=XERCES_DISABLE_DTD=1
$ sudo systemctl daemon-reload
$ sudo systemctl restart shibd
$ sudo less /proc/`pidof -s shibd`/environ
```

httpdのほうはexportを省いた以下の行を/etc/sysconfig/httpdの末尾に追記します。同様に最後に記載したコマンドで当該環境変数が設定されていることを確認してください。

```
XERCES_DISABLE_DTD=1
```

```
$ sudo vi /etc/sysconfig/httpd
$ sudo systemctl restart httpd
$ sudo less /proc/`pidof -s httpd`/environ
```

verifyBackup="false"

バッキングファイルが他者によって変更されないことが確実な場合はSignature MetadataFilterの末尾に verifyBackup="false" を追加してください。起動時のメタデータ読み込み時にバッキングファイルの署名検証がスキップされ起動が速くなります。

```
<MetadataFilter type="Signature" certificate="/etc/shibboleth/cert/gakunin-signer-2010.cer" verifyBackup="false"/>
```

SP 2.5.x から SP 2.5.x へのアップデートに関する情報

*はセキュリティフィックス

- 2.5.6(*) [upki-fed:01018] Shibboleth SPの脆弱性について(2016.2.26) (CVE-2016-0729)
  - 本件はXerces-Cライブラリの脆弱性ですので当該ライブラリのアップデートのみでも対処可能です。またディストリビューションのアップデート提供時期によっては当該ライブラリのアップデート提供時期が後になることが考えられます。その場合自動再起動が行われませんので、上記手順に従って再起動（もしくはOS自体の再起動）を必ず行ってください。
- 2.5.5(*) [upki-fed:00950] Shibboleth SP の脆弱性について (2015/7/21) (CVE-2015-2684)
  - MetadataProviderにてvalidate="true"がデフォルトになりました。これまでの設定ファイルは上書きされませんので、新規SPでだけ問題が発生している場合はこの影響である可能性があります。例えば、regexp属性を持たない<shibmd:Scope>要素がエラーになります。
    ちなみにIdPv3でもダウンロードしたメタデータのバリデーションを行うのがデフォルトです。
  - 初期のCentOS 7向け（systemd対応版）はリブート時に/var/run/shibboleth/が消えて起動しなくなるので2.5.5-3.1以降を使うこと。
- 2.5.4(*) [upki-fed:00923] Shibboleth SP の脆弱性について (2015/3/19) (CVE-2015-0252)
  - mod_shibのログのデフォルト出力先が /var/log/httpd/{native.log,native_warn.log} から /var/log/shibboleth-www/{native.log, native_warn.log} に変更になっています。
    既存環境で追随するにはnative.logger.distを参考にnative.loggerを修正してください。
  - /var/cache/shibboleth/以下に大量の*.jsonという名前のキャッシュが削除されず残る問題が、このバージョンで修正されています。このファイルが大量にある場合は、適宜削除してください。
  - 2.5.0での修正点に見落としがありましたので、下のほうに追記しました。当該warningが気になる人は対処してください。⇒2.5.0のshibboleth2.xml
  - このバージョン前後でOpenSSL 1.0.1系とリンクするようになり、可能な環境ではECDSA/GCMに対応します。/Shibboleth.sso/Metadataから利用可能なアルゴリズムが確認できます。

    - shibboleth2.xml:
      DiscoveryFilterが追加され、フェデレーションメタデータ中に"hide-from-discovery"と宣言されているIdPがDiscoFeedに入らなくなります。
    - attribute-map.xml:
      uidの行が追加されていますが、デフォルトでコメントアウトされています。
- 2.5.2(*) Shibboleth SP heap overflow processing InclusiveNamespace PrefixList (CVE-2013-2156)

  2.5.2において/etc/httpd/conf.d/shib.confに以下の追加が行なわれておりますが、shib.confを修正している場合は反映されません。必要に応じてshib.confを修正してください。
  なお、サイト全体にBASIC認証等で制限をかけている場合を除いてこれによる影響はないと思われます。

```
#
LoadModule mod_shib /usr/lib64/shibboleth/mod_shib_22.so

#
# Ensures handler will be accessible.
#
<Location /Shibboleth.sso>
 Satisfy Any
 Allow from all
</Location>

#
# Used for example style sheet in error templates.
#
<IfModule mod_alias.c>
 <Location /shibboleth-sp>
  Satisfy Any
  Allow from all
 </Location>
```

- 2.5.1(*)
  特になし

SP 2.4.x から SP 2.5.x へアップデートする場合の注意点

0. 事前準備

以前情報交換メーリングリストでご案内いたしましたように、rpmパッケージで導入されている場合は、shibd という非rootユーザが新たに作られその権限で起動するようになるため、昔の学認の技術ガイドに沿って設定している場合に2点問題が生じます。技術ガイドは2011年11月に修正済みです。それ以前にSPを構築された方は以下の設定を確認してください。

まず、server.key のパーミッションの問題です。rootにしか読み取り権限を与えていない場合、2.5をインストールした時点で自動再起動がかかるため、shibdがエラーで停止してしまいます。
回避方法はいくつかありますが、下記のように sp-key.pem をシンボリックリンクにしておくと、2.5インストール時に自動的に server.key のownerが修正されます。

```
$ sudo mv -i /etc/shibboleth/sp-key.pem{,.dist} && sudo ln -s cert/server.key /etc/shibboleth/sp-key.pem
```

> ⚠ この回避策は当該秘密鍵がSPのみで使用されている場合で、slapdなど他のプロセスからも参照されている場合は注意が必要です。
> 具体的に言うと、アップデート前の時点で秘密鍵ファイルのowner/グループがroot:rootでない場合が該当します。上述のようにシンボリックリンクを作成すると、2.5へのアップデートによってこれがshibd:shibdに強制変更されます。ACLを含めたパーミッションは変更されないようですので、setfacl等でACLを設定しておけば回避できます。

2点目の問題は、ダウンロードしたメタデータのバックアップファイルを置くディレクトリのパーミッションです。/etc/shibboleth/metadata/ にバックアップを置くように設定されている場合、このディレクトリはshibdユーザの権限ではファイルが置けません。

回避方法は、shibboleth2.xmlで

> *backingFilePath="/etc/shibboleth/metadata/federation-metadata.xml"*

のように絶対パスで指定している部分を

> *backingFilePath="federation-metadata.xml"*

のように相対パスに変更します。このように変更しておけば、適切にownerが設定されるディレクトリ /var/cache/shibboleth/ を使うようになります。

これを無視してアップデートすると以下のようなエラーがログに記録されるようになります。（リモートのメタデータにアクセスできている限りにおいてSP停止などの実害はありません）

```
2011-10-17 18:30:07 DEBUG OpenSAML.MetadataProvider.XML [GakuNinMetadata]: committing backup file to permanent location (/etc/shibboleth/metadata/federation-metadata.xml)
2011-10-17 18:30:07 CRIT OpenSAML.MetadataProvider.XML [GakuNinMetadata]: unable to rename metadata backup file
```

1. SPアップデート後

事前準備の後始末

事前準備で sp-key.pem をシンボリックリンクにしていた場合、それを元に戻してowner/グループを2.5対応に変更します。

```
$ sudo chown shibd:shibd /etc/shibboleth/sp-key.pem.dist && sudo rm /etc/shibboleth/sp-key.pem && sudo mv -i /etc/shibboleth/sp-key.pem{.dist,}
```

また、メタデータのバックアップファイルの移動に伴い、/etc/shibboleth/metadata/federation-metadata.xml* は使われなくなっておりますので、紛らわしくないように削除しておきましょう。

> *sudo rm /etc/shibboleth/metadata/federation-metadata.xml**

これにより /etc/shibboleth/metadata/ に1つもファイルがなくなったら、ディレクトリ自体を削除してしまってかまいません。

> *sudo rmdir /etc/shibboleth/metadata/*

もし、事前準備後shibdを再起動していたら、/var/run/shibboleth/以下にバックアップファイルが作成されています。しかしアップデート後は/var/cache/shibboleth/以下が使われているはずです。こちらも紛らわしくないように削除しておきましょう。同様に、/var/run/shibboleth/側に *.json というファイルがある場合も削除してかまいません。

> *sudo rm /var/run/shibboleth/federation-metadata.xml**
> *sudo rm /var/run/shibboleth/*.json*

不要なパッケージの削除

libsaml, libxmltooling, libxml-security-cが合わせてバージョンアップしパッケージ名が変更になっています。古いバージョンは削除されないようなので、他で使っていなければ削除してしまいましょう。

> *sudo yum erase libsaml7 libxmltooling5 libxml-security-c16*

shibboleth2.xml

静的ファイルの1つ、Shibbolethロゴが削除された影響の1つです。
以前からのshibboleth2.xmlを使っている場合は以下の行を含んでいるはずですが、当該ファイルが削除されていますので、shibboleth2.xmlのこの行も削除してください。

> *logoLocation="/shibboleth-sp/logo.jpg"*

また、以前からのshibboleth2.xmlをそのまま使っている場合は2.5.0以降では以下の警告が表示されるようになります。

```
2012-10-13 18:54:49 WARN Shibboleth.AttributeExtractor.XML : attribute mappings are reloadable; be sure to restart web server when adding new attribute IDs
```

attribute-map.xmlの読み込み部分にreloadChanges="false"を付けるとよいです。こうすることでattribute-map.xmlの修正時に反映するには再起動が必要になりますが、元々そうすべきでした（そのほうが安全です）。

```
        </MetadataProvider>

        <!-- Map to extract attributes from SAML assertions. -->
-       <AttributeExtractor type="XML" validate="true" path="attribute-map.xml"/>
+       <AttributeExtractor type="XML" validate="true" reloadChanges="false" path="attribute-map.xml"/>

        <!-- Use a SAML query if no attributes are supplied during SSO. -->
        <!--
```

詳細: Default Reloading of Attribute Mappings Disabled - NativeSPConfigurationChanges - Shibboleth Wiki

shib.conf

静的ファイルの1つ、Shibbolethロゴが削除された影響のもう1つです。
/etc/httpd/conf.d/shib.conf を修正して使っていた方は、shib.conf.rpmnew というファイルが新たに作成されていると思います。差分を確認し（下記の行は削除して問題ありません）必要があれば修正の上、shib.confを置き換えてください。

```
--- /etc/httpd/conf.d/shib.conf        2013-05-21 19:33:44.696374317 +0900
+++ /etc/httpd/conf.d/shib.conf.rpmnew        2013-01-10 04:30:48.000000000 +0900
@@ -20,7 +20,6 @@
     Allow from all
   </Location>
   Alias /shibboleth-sp/main.css /usr/share/shibboleth/main.css
-  Alias /shibboleth-sp/logo.jpg /usr/share/shibboleth/logo.jpg
 </IfModule>

 #
```

2. SP 2.5.0からの新機能

一部GakuNinShareでご紹介しています。
⇒Shibboleth SP 2.5.0からの新機能

- Webアプリケーションのログアウトフローへの Shibbolethログアウト処理の挿入
- Attribute Checker Handler
- ローカルからあたかもIdPで認証されたような状態にする機能2つ（GakuNinShare未掲載のためShibboleth Wikiへのリンク）
    - SAML Artifact Spoofing
    - External Authentication Handler
- IdPから取得した属性に対する操作がいろいろと追加されました（GakuNinShare未掲載のためShibboleth Wikiへのリンク）
    - Transform AttributeResolver
    - Template AttributeResolver
    - UpperCase AttributeResolver
    - LowerCase AttributeResolver

3. その他の情報

- PKCS#1.5使えなくなった - /etc/shibboleth/security-policy.xml
    <AlgorithmBlacklist includeDefaultBlacklist="true"/>
  新機能Metadata Attribute Extractor non-ASCIIでエラー SSPCPP-547
  _shibsession_* cookie HttpOnlyが付くようになった
  _shibstate_* 時限付き
  acl ::1入った
  helpLocation="/about.html"
  cookieProps書式変更
  handlerSSL="true"
  shibboleth2.xmlの書式エラーでhttpdが起動しなくなった？
  /var/log/httpd/native.log, native_warn.logが記録されるようになる

  > *2012-08-08 04:35:19 CRIT XMLTooling.Logging : error in file permissions or logging configuration: exception creating appender: failed to open log file (/var/log/httpd/native.log)*
  > *2012-08-08 04:35:19 CRIT Shibboleth.Config : failed to load new logging configuration from (native.logger)*

  https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPConfigurationChanges
  https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPInterestingFeatures
  requireAuthenticatedEncryption signResponse="conditional"にしないと

  >

> *opensaml::FatalProfileException at (https://HOSTNAME/Shibboleth.sso/SAML2/POST)*
> *A valid authentication statement was not found in the incoming message.*

ログには以下が記録される。

> *2012-10-14 09:26:14 ERROR Shibboleth.SSO.SAML2 [7]: failed to decrypt assertion: Unauthenticated data encryption algorithm unsupported.*

2012-10-13 18:54:49 WARN Shibboleth.PropertySet : deprecation - remapping property (relayStateLimit) to (redirectLimit)
2012-10-13 18:54:49 WARN Shibboleth.Application : empty/missing cookieProps setting, set to "https" for SSL/TLS-only usage
2012-10-13 18:54:49 WARN Shibboleth.Application : handlerSSL should be enabled for SSL/TLS-enabled web sites

以前の情報

SPアップデート手順（*はセキュリティフィックス）

- 2.4.0 情報交換ML:00300 情報交換ML:00302 情報交換ML:00306
- 2.4.1 情報交換ML:00316
- 2.4.3(*) 情報交換ML:00356 情報交換ML:00367 情報交換ML:00460