

SPv3アップデートに関する情報



Shibboleth IdPのアップデートに関してはこちらをご覧ください。⇒[IdPv4アップデートに関する情報](#)



SP 2.5.xおよびそれ以前からアップデートする場合はこちらの情報もご覧ください。⇒[SPバージョン2アップデートに関する情報](#)



以前の本手順でSPv2からSPv3にアップデートして以降、`/var/log/messages` に`mod_shib`のログが出力されなくなっている場合は、`/etc/shibboleth/native.logger` を同ディレクトリの`native.logger.dist`と比較し、必要な修正を適用してください。出力されるべき`mod_shib`のログは以下のようなフォーマットです:

```
Nov 10 22:37:54 localhost shobboleth: ...
```

- [バージョン共通](#)
 - [注意点](#)
- [Apache httpd 2.4へ移行する場合の注意点](#)
- [SP 3.2.x から SP 3.3.x へアップデートする場合の注意点](#)
- [SP 3.1.x から SP 3.2.x へアップデートする場合の注意点](#)
- [SP 3.0.x から SP 3.1.x へアップデートする場合の注意点](#)
- [SP 3.0.x から SP 3.0.x へのアップデートに関する情報](#)
- [SP 2.6.x から SP 3.0.x へアップデートする場合の注意点](#)
 - [1. 事前準備](#)
 - [2. SPアップデート後の作業](#)
 - [2.1. 不要なパッケージの削除](#)
 - [2.2. 不要なファイルの削除](#)
 - [2.3. shibboleth2.xmlの新形式への移行](#)
 - [2.4. security-policy.xmlが新形式へ移行していることの確認](#)
 - [2.5. transaction.log新フォーマットへの移行](#)
 - [3. SP 3.0からの新機能](#)
 - [4. SP 3.0からの注意事項](#)
 - [5. その他の情報](#)

バージョン共通

CentOS等、yum/dnf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 libsaml12 libxmltooling10 libxml-security-c20 liblog4shib2 opensaml-schemas xmltooling-schemas libxerces-c-3.2 libcurl-openssl  
(OSによっては libcurl-openssl 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 systemctl restart shibd  
$ sudo systemctl restart httpd
```

※ 例えば、2.6.1から3.0.1へのアップデートは自動的に再起動する模様。3.0.1にアップデート後、libxmltooling8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。

注意点

すでにNIIオープンフォーラム等でアナウンスしておりますが、Shibboleth開発元におけるメンテナンス持続性のため、Shibboleth SP次期バージョンはJavaで再実装する方向でデザインが進行しており、リリース目処は2024年もしくは2025年となっております。次期バージョンリリースまでは現行バージョンがメンテナンスされますが、それ以降も運用を続けるには大きな改修が必要になる可能性があります（利用している機能によっては提供されなくなる可能性もあります）ので予めご了承ください。

RPMパッケージ情報が取得できない場合は、本ページ末尾の説明を参照して新しいリポジトリを利用するよう設定ファイルを更新してください。

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](#)

Shibbolethプロダクトに関する次節以降記載以外のセキュリティフィックスおよび脆弱性情報は以下のページにてご覧いただけます。

⇒ Shibboleth Wiki: [SecurityAdvisories](#)

Apache httpd 2.4へ移行する場合の注意点

OSのバージョンアップ等でApache httpd 2.2およびそれ以前の環境からApache httpd 2.4の環境へ移行する場合の、Shibboleth SP周りの設定ファイルに関する注意事項です。

Apache httpd 2.2およびそれ以前からApache httpd 2.4へ移行する場合、設定ファイルのShibCompatWith24の行はコメントアウトもしくは削除してください。

2016-12-08 [\[upki-fed:01115\] Re: Proxy配下でのSP構築に関して](#)

require valid-user など、許容される構文もしくはその意味が変わっておりますので、昔の設定を引き継いで使っている方はご注意ください。

⇒ Shibboleth Wiki: [Apache Compatibility Changes](#), [Apache](#), [htaccess](#)

特に、以前の意味での"require valid-user"の使用は避け、"require shib-session"もしくは"require shib-user ..."で置き換えてください。BASIC認証等との組み合わせで問題が発生する場合は"ShibCompatValidUser On"を指定してください。

詳細: Shibboleth Wiki: [Recommended Practices for Compatibility](#)

2.4に移行するとrequireの条件を満たさない場合に表示されるエラーページが"403 Forbidden"から"401 Unauthorized"に変更されます。これに伴いshibboleth2.xmlの<Errors>要素に記述されたaccess属性（エラーページのカスタマイズ）が有効になりません。ApacheのErrorDocumentで代替してください。

なお、Apache httpd 2.4上でSPを構築した場合、なんらかの条件のもとで、シボレス認証が必要な場面で"401 Unauthorized"というエラーが発生するという情報があります。この場合は以下の方法を試してみてください（CentOS 7での手順です）。
/etc/httpd/conf.modules.d/00-shib.conf のようなファイル名で以下の内容で新規ファイルを作成し、/etc/httpd/conf.d/shib.conf の該当行を削除してください。終わりましたらhttpdを再起動してください。

```
#
# Load the Shibboleth module.
#
LoadModule mod_shib /usr/lib64/shibboleth/mod_shib_24.so
```

2016-12-09 [\[upki-fed:01121\] Re: Proxy配下でのSP構築に関して](#)

関連: <https://issues.shibboleth.net/jira/browse/SSPCPP-628>

関連: ([Shibboleth Users ML](#)) [Configuration of SP with apache and mod_shib - HTTP 401 error](#)

SP 3.2.x から SP 3.3.x へアップデートする場合の注意点

本リリースよりRPMパッケージの署名に使われるGPG鍵が変更されているために、以前のバージョンからそのままではyumコマンドによるアップデートに失敗します。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手順でアップデートしてください。

1. Shibboleth用のrepositoryファイルの更新

Shibboleth用のrepositoryファイルを下記URL先より取得できる最新のものに更新してください。

<https://shibboleth.net/downloads/service-provider/latest/RPMS/>

(CentOS 7の場合のコマンド例)

```
$ sudo curl 'https://shibboleth.net/cgi-bin/sp_repo.cgi?platform=CentOS_7' -o /etc/yum.repos.d/shibboleth.repo
```

2. GPG鍵のインポートとアップデートの完了

repositoryファイルの更新後、yumコマンドによりアップデートを実施すると、新しいGPG鍵のインポートを促されますので、表示されるフィンガープリントが以下と一致することを確認してインポートしてください。

```
Fingerprint: dcaa 1500 7bed 9de6 90cd 9523 378b 8454 0227 7962
```

その後アップデート処理が進みますので、そのまま完了してください。

SP 3.1.x から SP 3.2.x へアップデートする場合の注意点

libsaml, libxmltooling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、他で使っていないければ削除してしまいましょう。

```
$ sudo yum erase libsaml11 libxmltooling9
```

<https://www.gakunin.jp/ml-archives/upki-fed/msg01430.html>

にて説明していますが、Form SessionInitiatorでdiscoveryTemplate.htmlを使っている場合、3.2.1以降では forceAuthn, isPassive, acsIndex, authnContextClassRef, authnContextDeclRef, authnContextComparison の各パラメーターをURLのquery stringで受け渡しHTMLに反映することができなくなっておりますので、そのような機能に依存している箇所がございましたら、代替としてJavaScriptでquery stringを確認するなど別の手段を使うようにしてください。

また、3.2.1以降<Errors>関連のテンプレートについて、query stringパラメーターによる置換のデフォルトがオフになったことにより、この機能に依存している箇所に影響が出る可能性があります。JavaScriptなど別の手段でカバーすることが推奨されますが、externalParameters="true"により以前のバージョンの挙動を再現することも可能です。

SP 3.0.x から SP 3.1.x へアップデートする場合の注意点

libsaml, libxmltooling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、他で使っていないければ削除してしまいましょう。

```
$ sudo yum erase libsaml10 libxmltooling8
```

Shibboleth IdP v3における設定ファイルのフラット化と同じことがSPでも進行しており、大量のDEPRECATEDのwarningが出力されるようになっていきます。実際に支障をきたすのはv4以降ですが、attribute-policy.xml.distファイルおよびIdPフラット化の記述を参考に時間のあるときに対処しておくことを推奨します。

SP 3.0.x から SP 3.0.x へのアップデートに関する情報

3.0.4.0までの3系で、Windowsサーバ向けのIIS 7モジュールを使っていて、<Sessions>で handlerURL="/acs/Shibboleth.sso" のようにハンドラのパスを変更している場合うまく動かないという問題があります。3.0.4.1で修正されました。また、以下の記述を加えれば回避できます。

```
<ISAPI handlerPrefix="/acs/Shibboleth.sso" >
```

詳細: <https://issues.shibboleth.net/jira/browse/SSPCPP-856>

3.0.0には起動に失敗するものを含むバグが存在します。3.0.1以降にアップデートしてください。アップデート後、shibboleth2.xmlに verifyBackup= という文字列が含まれる場合は誤字ですので verifyBackup= に修正してください。

3.0.1/3.0.0にはWindows版v3の新機能である.NETハンドラがうまく動かない問題と、<SSO>要素のsigning指定が反映されないという問題があります。3.0.2以降に更新してください。

SP 2.6.x から SP 3.0.x へアップデートする場合の注意点

2.6.xで動作している設定ファイルは全て3.0.xでも動作します。下記1.の手順で確認した上で、上記手順でアップデートを行ってください。ただし、旧設定ファイルでは新機能が使えないほかいくつか不要なものがございましたので後日以下の2.の手順を実施することをお勧めします。SP 3での変更点の詳細は開発元の[ReleaseNotes](#)をご参照ください。

1. 事前準備

shibboleth2.xmlに accessError.html および syslog.logger への参照がないことを確認してください。参照している場合は、ファイルが編集されている（.distを付加したファイルと同一でない）ことを確認してください。参照されておりかつ編集されていない場合、アップデートで当該ファイルが削除され問題が発生する可能性があります。編集された状態のものは削除されませんので、コメントを挿入しておくなどして対処してください。

同様に、attribute-map.xmlが編集されていない場合、かつ属性 unscoped-affiliation (eduPersonAffiliation) を使っておりv3にバージョンアップする場合は、アップデート後にunscoped-affiliationの受け渡しに失敗するようになりますので、編集（コメントを挿入しておくなど）して対処してください。

2. SPアップデート後の作業

2.1. 不要なパッケージの削除

libsaml, libxmltooling, libxml-security-c, liblog4shib, libxerces-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。また、CentOS 7ではBaseリポジトリのxerces-cパッケージを使用していたものが独自のlibxerces-c-3.2パッケージを使用するようになっていきます。古いバージョンは削除されないようなので、他で使っていないければ削除してしまいましょう。

```
$ sudo yum erase libsaml9 libxmltooling7 libxml-security-c17 liblog4shib1 libxerces-c-3_1 xerces-c
```

2.2. 不要なファイルの削除

2.xで/var/log/shibboleth-www/以下に出力されていたログは3.0では/var/log/messagesに出力されるようになりました。既存のログファイルに有益なものはないと思いますので削除してかまいません。

```
$ sudo rm -r /var/log/shibboleth-www
```



ただし native.logger を修正している場合は自動で出力先が切り替わりませんので、/etc/shibboleth/native.logger を同ディレクトリの native.logger.dist と比較し、必要な修正を適用してください。
ちなみに /var/log/messages には多量のログが混在しており、mod_shibからの出力は以下のようなフォーマットで出力されます。

```
Nov 10 22:37:54 localhost shibboleth: WARN Shibboleth.Application : ...
```

また、2.xには不要になったDiscoFeedキャッシュの削除処理に不具合があり、当該ディレクトリに残り続けているものがある可能性があります。アップデート後1時間以上経ってから以下のようなコマンドを実行して不要なファイルを削除してください。

```
$ sudo find /var/cache/shibboleth/ -name '*.json' -type f -mmin +60 -exec rm {} \;
```

2.3. shibboleth2.xmlの新形式への移行

shibboleth2.xmlがv2とv3で唯一異なる形式を持つファイルです（次に示すsecurity-policy.xmlを除いて）。SP v3でも旧形式のファイルを読み込むことは可能ですがいずれサポートされなくなりますので新形式に移行する手順をご紹介します。



紛らわしいですがファイル名はv3でも shibboleth2.xml のままです。



新形式（3.0フォーマット）でデフォルト値が変更になった部分があり、該当機能を使っている場合は移行する際には注意が必要です。これまで判明しているところでは、<SessionCache>のcacheAssertions="false"がデフォルトになったことによりtrueを明示していない場合はWebアプリケーションがアサーションを直接取得することができなくなります。従来の値を指定するようにshibboleth2.xmlを修正してください。詳細は開発元の[ReleaseNotes](#)の3.0.0の"Changed Defaults"を参照してください。

まず、アップデート後起動するとDEPRECATEDと表示されているログが見られると思います。これは新形式で許容されない記述の指摘ですので、DEPRECATEDが表示されなくなるまで修正を繰り返します。典型的には

```
<MetadataProvider type="XML" validate="true" file="partner-metadata.xml"/>
```

のような記述の file= を path= に、 uri= を url= に修正する必要があります。

DEPRECATEDログが出なくなったら、ファイル先頭の2.0を3.0に変更（2か所）して完了です。

```
<SPConfig xmlns="urn:mace:shibboleth:3.0:native:sp:config"
  xmlns:conf="urn:mace:shibboleth:3.0:native:sp:config"
```

2.4. security-policy.xmlが新形式へ移行していることの確認

これもv2からv3で形式が変わったファイルですが、ほとんどの場合編集の必要がないため自動的に新形式に移行されているはずです。security-policy.xmlとsecurity-policy.xml.distを比較して差分がないことを確認してください。差分がある場合は必要な変更をマージしファイル先頭の名前空間指定を2.0から3.0に修正してください。

```
$ diff /etc/shibboleth/security-policy.xml{.dist,}
```

2.5. transaction.log新フォーマットへの移行

これは必須ではありませんが、SP 3から/var/log/shibboleth/transaction.logに新フォーマットが導入され従来より見やすくなっております。アップデートした場合には自動的に移行はされませんので、以下の手順で移行してください。

1アクセスが2行で表されるようになり、各行のプレフィックスを含め機械的に読みやすいように改善されています。

旧フォーマット:

```
2017-02-20 11:13:29 INFO Shibboleth-TRANSACTION [1]: New session (ID: _6f1...) with (applicationId: default) for principal from (IdP: https://idp.example.ac.jp/idp/shibboleth) at (ClientAddress: xxx.xxx.xxx.xxx) with (NameIdentifier: AAdz...vQ==) using (Protocol: urn:oasis:names:tc:SAML:2.0:protocol) from (AssertionID: _b2a...)
2017-02-20 11:13:29 INFO Shibboleth-TRANSACTION [1]: Cached the following attributes with session (ID: _6f1...) for (applicationId: default) {
2017-02-20 11:13:29 INFO Shibboleth-TRANSACTION [1]:      eppn (1 values)
2017-02-20 11:13:29 INFO Shibboleth-TRANSACTION [1]: }
```

新フォーマット (最後から2番目の項はUser Agent、最後の項はクライアントIPアドレスです) :

```
2018-08-03 15:08:07|Shibboleth-TRANSACTION.AuthnRequest|||https://idp.example.ac.jp/idp/shibboleth|||urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect||| 2018-08-03 15:08:17|Shibboleth-TRANSACTION.Login|uid@example.ac.jp|_1d7...|https://idp.example.ac.jp/idp/shibboleth|_19f...|urn:oasis:names:tc:SAML:2.0:classes:PasswordProtectedTransport|2018-08-03T15:08:14|eppn(1)|AAdz...cA==|urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST|urn:oasis:names:tc:SAML:2.0:status:Success||Mozilla/5.0 ...|xxx.xxx.xxx.xxx
```

shibboleth2.xmlの先頭 (<SPConfig>の最初の子要素として。ただしその位置に<Extensions>がある場合はその下) に以下を追加するか、すでに<OutOfProcess>要素が存在する場合にはその属性としてtranLogFormat=の部分を追加してください。

```
<OutOfProcess tranLogFormat="%u|%s|%IDP|i|%ac|%t|%attr|%n|%b|%E|%S|%SS|%L|%UA|%a" />
```

次に、shibd.loggerがshibd.logger.distと差分がある場合には、必要な変更をマージしてください。2.6.1と3.0.2の差分は以下の通りです。

```
--- 2.6.1/shibd.logger.dist      2017-11-15 09:40:50.000000000 +0900
+++ 3.0.2/shibd.logger.dist      2018-08-03 09:41:41.000000000 +0900
@@ -29,11 +29,14 @@
 # logs XML being signed or verified if set to DEBUG
 log4j.category.XMLTooling.Signature.Debugger=INFO, sig_log
 log4j.additivity.XMLTooling.Signature.Debugger=false
+log4j.ownAppenders.XMLTooling.Signature.Debugger=true

 # the tran log blocks the "default" appender(s) at runtime
 # Level should be left at INFO for this category
 log4j.category.Shibboleth-TRANSACTION=INFO, tran_log
 log4j.additivity.Shibboleth-TRANSACTION=false
+log4j.ownAppenders.Shibboleth-TRANSACTION=true
+
 # uncomment to suppress particular event types
 #log4j.category.Shibboleth-TRANSACTION.AuthnRequest=WARN
 #log4j.category.Shibboleth-TRANSACTION.Login=WARN
@@ -61,7 +64,7 @@
 log4j.appender.tran_log.maxFileSize=1000000
 log4j.appender.tran_log.maxBackupIndex=20
 log4j.appender.tran_log.layout=org.apache.log4j.PatternLayout
-log4j.appender.tran_log.layout.ConversionPattern=%d{%Y-%m-%d %H:%M:%S} %p %c %x: %m%n
+log4j.appender.tran_log.layout.ConversionPattern=%d{%Y-%m-%d %H:%M:%S} |%c|%m%n

 log4j.appender.sig_log=org.apache.log4j.FileAppender
 log4j.appender.sig_log.fileName=/var/log/shibboleth/signature.log
```

3. SP 3.0からの新機能

- Stateless Clustering
[ReleaseNotes](#)より:

A form of [session recovery](#) across clustered SP nodes using encrypted cookies is available. While making clustering much simpler, it does affect the behavior of logout in some cases, but it offers more flexibility for deployers willing to make trade-offs.

- /Shibboleth.sso/Logout/Admin
[ReleaseNotes](#)より:

An endpoint is available to programmatically remove sessions based on the SP-assigned session ID, with associated communication to an IdP via SOAP where possible (though this is rarely possible). While complex, it is possible to create a more limited shared store of revoked sessions that prevents the stateless session recovery feature from re-creating the session in some cases, without requiring a fully-shared session store.

- entityIDSelf / APPLICATIONID-override.xml
[ReleaseNotes](#)より:

A set of virtual hosts can be auto-assigned a distinct entityID without the creation of `<ApplicationOverride>` elements to do so, using the new `entityIDSelf` [content setting](#). While this does not eliminate the overhead of managing metadata for each host, it does eliminate most actual configuration overhead within the SP itself.

In addition, when overrides are still required for other purposes, it is now possible to load XML fragment files containing just the override configurations from a directory at [runtime](#), including adding additional overrides on the fly without configuration reload.

なお、CentOS 7ではXerces Cライブラリを独自提供することによりDTDを無効化するという機能強化が行われております。**攻撃耐性強化**のために、是非移行をご検討ください。

4. SP 3.0からの注意事項

- 上記「1. 事前準備」にも書きましたが、設定ファイルのデフォルト値の変更に影響を受ける場合があります。具体的にはバージョン毎に以下の属性設定が有効化されており、v2でこの範囲内の属性しか利用していない場合（設定ファイルがデフォルトのままの場合）設定ファイルが書き換えられv3のデフォルトが適用されますので `unscoped-affiliation` が利用できなくなります。問題が発生した場合、`attribute-map.xml`の該当箇所がコメントアウトされていますのでその部分だけ解除してください。

バージョン	初期設定ファイルで利用可能な属性
2.6.1	eppn, affiliation, unscoped-affiliation , entitlement, targeted-id , persistent-id
3.0.3	subject-id, pairwise-id, eppn, affiliation, entitlement, persistent-id

※ `targeted-id`はSAML1用であり以前から利用は推奨されていません

※ `subject-id`および`pairwise-id`は2019年3月現在学認では規定されていません

```
...
-->
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1" id="unscoped-affiliation">
  <AttributeDecoder xsi:type="StringAttributeDecoder" caseSensitive="false"/>
</Attribute>
<!--
...
-->
<Attribute name="urn:mace:dir:attribute-def:eduPersonAffiliation" id="unscoped-affiliation">
  <AttributeDecoder xsi:type="StringAttributeDecoder" caseSensitive="false"/>
</Attribute>
<!--
...
```

- レアケースですがSPが直接外部サーバへHTTPS接続する場合（例えばメタデータのダウンロード）、同梱の設定ファイルでは（つまりv3で新規に構築すると）TLS 1.2以上を使うように強制されます。問題がある場合は`shibboleth2.xml`の`cipherSuites`の項を修正してください。（少なくとも学認メタデータのダウンロードで問題になることはありません）
- ハッシュアルゴリズムとしてSHA-1ではなくSHA-256を使うようになっています。これが問題になることはないと思いますが、古いIdPと連携する場合はご注意ください。
- 同梱の設定ファイルからSAML 1.xサポートが削除されております。つまりSPを新規に構築した場合SAML 2.0をサポートしていないIdPと連携できません。必要があればSAML1を有効化してください。
- 同様に、SPv3同梱の設定ファイルでは、属性の取得に失敗した場合Attribute Queryリクエストを試みる機能がデフォルトでは機能しないようになっています。必要な場合はQuery AttributeResolverを有効化してください。
- Solarisがサポート外となりました。

5. その他の情報

shibbolethリポジトリが冗長化され設定ファイルが変更になっております。古いものをお使いの場合は[技術ガイド](#)の手順に従って `/etc/yum.repo.d/shibboleth.repo` ファイルを更新してください。これに伴いパッケージの更新が必要になることはありません。

SP 3へのアップデートに関する他の情報源: ([Shibboleth Wiki](#)) [UpgradingFromV2](#)