SPにおけるAES-GCM暗号対応状況

Shibboleth IdP V4より、新規インストール時のデフォルトのXML暗号化アルゴリズムの設定が従来のAES-CBCからAES-GCMに変更されています。
IdPv3からのアップグレード時には従来通りのAES-CBCが維持されます。

非Shibbolethの大部分のSPや、一部の古いShibbolethや古いOS(RHEL/CentOS 5等)/ソフトウェアを用いているSPはGCMをサポートしておらず、GCMに変更した場合はこれらのSPと連携が取れなくなるとの情報がございますので、IdPv4を新規インストールされる際はご注意ください。

また、SP運用ご担当の方におかれましては、SPがGCMをサポートしているかをご確認いただき、サポートしていないことが判明しましたら、その旨を学認事務局までご一報いただけますと幸いです。

詳細はShibboleth Wikiの下記ページをご参照ください。
https://wiki.shibboleth.net/confluence/display/IDP4/GCMEncryption

2021年7月8日時点で問題ありとの情報のあるSP（情報は随時更新していきます）：

- HeinOnline
- Emerald Insight
- Clarivate社のWeb of Science (https://sp.tshhosting.com/shibboleth)

2021年9月2日時点追加：

- HighWire

2023年2月時点再追加：

- Thieme

対応済み情報：

- Thieme 2022年2月第2週対応済み →2023年2月問題ありとの情報あり
- SpringerLink (https://fsso.springer.com)　→解消？(2021/9/2)
- Nature (https://secure.nature.com/shibboleth)　→解消？(2021/9/2)

IdPでの一時的対処方法：

> ⚠ 本記述はIdP側での一時的な対処方法であり、本質的にはSP側で対処してもらう必要があるものであり、また将来的にこの設定をそのままにしますとSPがAES-GCMをサポートした後も弱い暗号を使い続けることになりますので、ご注意ください。定期的にリストの見直しを行うことを推奨します。

metadata-providers.xmlの当該SPを読み込んでいるMetadataProviderに、MetadataFilterの1つとして以下のようにSPのentityIDを列挙してください。

```
<MetadataFilter xsi:type="Algorithm">
    <!-- CBC-only SPs. -->
    <md:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
    <Entity>https://broken.example.org/sp</Entity>
    <Entity>https://also-broken.example.org/sp</Entity>
</MetadataFilter>
```

metadata-providers.xmlを修正しましたら下記コマンドで設定内容を再読み込みさせてください。

```
$ /opt/shibboleth-idp/bin/reload-service.sh -id shibboleth.MetadataResolverService
```

詳細: https://wiki.shibboleth.net/confluence/display/IDP4/AlgorithmFilter