SameSite cookieのIdP/SPへの影響について

本問題を発生させているSameSiteは、eTLD+1（例えばnii.ac.jp）が異なるサイト間で遷移した場合に送受信されるcookieに制約を加えるものです。例えばnii.ac.jp内の2サイトでどのような遷移を行ってもcookieの挙動は従来通りです。これに鑑み「クロスサイト」の文言を「クロスドメイン」に改めました。

2020年2月4日にリリース予定のGoogle Chrome 80にて**2月17日の週から一部のChromeを皮切りに順次展開**されていく予定ですが、cookieの取り扱いに関する挙動が変更になり、この影響で特定の設定のIdP/SPにおいて期待するSSOの挙動を示さない、などの調査結果が示されました。
上記の通りですので脆弱性・セキュリティに類する問題ではありません
また、対処を誤ると古いSafariでここに書いてある以上の問題になることが示されており
ますので、対策として何か行う場合はご留意ください

目次:

Shibboleth IdPについて:

https://wiki.shibboleth.net/confluence/display/IDP30/SameSite
下記の影響が見られますのでHTML Local Storageの有効化（idp.storage.htmlLocalStorage=true）が推奨されています。

- （学認の技術ガイドに沿って構築したIdPについて）特定のSPからの認証要求でSSOが期待される場面でもログイン画面が表示されID/パスワードを要求される

学認ではShibboleth IdPのCASに関する知見が足りておりませんので、もしCASを使っていて問題が発生したという場合は事務局までお知らせください。

Shibboleth SPについて:

https://wiki.shibboleth.net/confluence/display/SP3/SameSite
学認技術ガイドに沿った構築でかつWebアプリケーションの構成が単純な場合、影響を受けない模様です。

- RelayStateにcookieを使うよう設定変更をしている場合、認証に時間がかかると本来の遷移先を忘れ認証後にサイトトップ等に遷移する
- Webアプリケーションが独自にセッションを管理しておらずShibbolethセッションに依存している場合、クロスサイトのPOSTを伴う場合にログイン状態が維持されない
- Form Recovery機能を有効にしている場合、認証に時間がかかるとこれが機能しない

これはSAMLの仕様に起因するものであるため、Shibboleth以外（simpleSAMLphp, ADFS等）のIdP/SPも影響を受ける可能性がございます。またSP側のWebアプリケーション自体に、クロスドメインでデータを受け渡すことに依存する部分があれば今回の挙動変更の影響を受ける可能性があります。

運用されている各IdP/SPでサービスの挙動に問題がないかご確認をお願いいたします。

テスト方法:

2月4日より前でも以下のブラウザ設定変更によりテストすることが可能です。

Chromeの場合、 chrome://flags#same-site-by-default-cookies の一番上にある「SameSite by default cookies」をDefaultからEnabledに変えて下に表示されるRelaunchボタンをクリックしてください。

Firefoxでも同様の状況をテストすることが可能です。about:config にて network.cookie.sameSite.laxByDefault=true にして試してください。

IdPのテストは上記のように設定を変更したブラウザで各SPへのログインを試みることが必要かと思われます。

SPのテストはIdPによるログインはもちろん、通常のサービス利用に問題がないかを確認、特にクロスドメインで情報を受け渡す仕組みがあればそれについて問題なく動作することを確認していただく必要があるかと思われます。

また、Shibboleth SPの1点目（RelayState）の問題が存在するかどうかについては、shibboleth2.xmlにrelayState="cookie"（文字列の末尾に":数字"が追加されている場合もあります）が含まれるかを確認するほか、SP→IdPもしくは逆の遷移時のRelayStateパラメーターに"cookie"の文字列が含まれるかどうかで確認することも可能です。

テストフェデレーションのIdPをテストする場合、test-sp1で試せるようにAuthnRequestをPOSTするハンドラを追加しました。以下のように（<IDPENTITYID>を自分のIdPのentityIDに変更して）お使いください。
https://test-sp1.gakunin.nii.ac.jp/Shibboleth.sso/SAMESITETEST?target=/secure/&entityID=<IDPENTITYID>

テスト時の注意点:

Chromeの場合はテスト時に限りませんがcookie設定後2分間はPOSTについて従来の挙動を示す（クロスドメインのPOSTでもcookieが送信される, Lax + POST mitigation）との情報があります。テストの際には操作ごとの間隔を空けて実施するようにしてください。Firefoxにはそのような制約はありません。

このChromeの挙動は暫定的なもので、時期は未定ながら無くなるものですので、この挙動に依存した実装は避けてください。

Chromeの上記2分間の特殊性をなくすには、`--enable-features=SameSiteDefaultChecksMethodRigorously` オプションを付けて起動してください。

問題があると指摘されているSP:

ML等でIdPからのSSOに支障があったと指摘のあったSPを以下にリストアップします。これらと接続している場合は特にご注意ください。指摘当時問題があっただけで現在は解消されている可能性もあります。

以下は上述のIdPの設定で回避できると思われます。

- box.com
- EZProxy

以下は「ログインできない」とされているのでサービス自体に問題があると考えられます。IdP側で対処のしようがないと思われます。

- ~~ServiceNow~~ (2/5解消したとの情報あり)
- Instructure Canvas (2/5一部解消したとの情報あり)
    - Chromeのみに~~SameSite~~を付与しているという情報もありますので、テストの際にはご注意ください。
- Rimeto
- University Tickets
- eShipGlobal
- Off Campus Partners
- Cornerstone (2/26追加)
    - SameSite=Noneを付与したため古いSafariで動作しなくなったという情報があります
- （LMSのLTI連携関係はダメになりそう）