IdPのホスト名変更に関する注意点

IdPのホスト名（entityID）を変更する場合にはいくつか考慮または解決すべき点があります。ホスト名を変更することによるリスクを考慮して，システム更新の際にホスト名は変更せず新しいIdPに移行する機関もあります。

まずはホスト名の切り替えについては次の点を参照の上，ご検討いただければと思います。

- a. entityIDをみて認可している電子ジャーナル等のSPへは，ホスト名（entityID）の切り替えをご連絡いただく必要があります。過去にホスト名を変更した機関からお聞きした話では，このホスト名の切り替えに苦労した（時間がかかった）ということがあったそうです。
- b. eduPersonTargetedID (ePTID) でユーザの紐づけを行っていたSPについては，IdP移行にあたりePTIDも変更となるため，移行後のアクセスが別IDとみなされます（SP側が協力していただける場合は旧ePTIDから新ePTIDへの移行も可能となる場合もあると考えられます）。ホスト名を変更しない場合でもePTID生成のsaltの値を引き継がないと，ePTIDが変わってしまいますので注意が必要です。

  eduPersonTargetedIDの仕様：eduPersonTargetedID
- c. 現行IdPと新IdPでスコープも変更する場合には，eduPersonPrincipalName (ePPN) が新旧IdPで異なることになります。ePTIDと同じですが，あるSPにてePPNをユーザの紐づけに使っている場合には移行後のそのSPへのアクセスが別IDとみなされることになります。
  eduPersonPrincipalNameの仕様：eduPersonPrincipalName
- d. 1つのホストでホスト名切り替えを行う（=既存IdPのホスト名設定を書き換える）場合，ホスト名を切り替えたという連絡がSP側に伝わりSP側での設定変更が行われるまでの間，サービスを利用できない危険が生じます。サービスを中断なくご利用いただくためには，現行IdPと新IdPの2つを並行して運用していただくことが必要になると考えられます。
- e. 現行IdPと新IdPの2つを並行運用していただく際，ディスカバリーサービス(DS)上でユーザが選択すべきIdPや，新旧の切り替えのタイミングなどユーザへの周知が必要です。これに関連して，各SPの対応状況（切り替え状況）に応じてどちらかのIdPを選択しないと認証できない，という状況があり得ます。

ホスト名を切り替えるか否かによらず，IdP移行にあたり検討が必要な項目は次の通りです。

- f. 現行IdPと新IdPが参照する統合認証基盤が異なる場合かつ現行IdPと新IdPで同一のスコープを用いる場合に考えられる問題ですが，統合認証基盤ごとにID体系も異なり，同一IDが別人に割り当てられる可能性がある場合には，ePPNを使っているSPでなりすましが発生することにつながりますので，値が重複しないようePPNの生成方法を工夫する必要があります。

以上の点を検討の上、**ホスト名を切り替える場合**についての具体的な作業を示します。

1. ホスト名（entityID）の切り替えについて，学認事務局に事前にご連絡ください。現行IdPのentityIDおよび新IdPのホスト名もご連絡いただくとスムーズに進められるかと思います。
2. 現行のIdPとは別のentityIDで新IdPを構築してください。
3. 学認申請システムで新IdPの新規申請を行ってください。申請時の注意点は次の通りです。
   - 新IdP名称は「XXX大学(新)」などのように現行のIdP名称と区別できるように異なるものを設定してください。
   - 「フェデレーションの参加機関一覧への掲載を許可する」にはチェックを入れないでください。

   ・・・新IdPの承認を待ちます。事務局のチェック後に申請書を郵送いただくため時間がかかることが想定されます。・・・
4. 新IdPが事務局より承認されましたら，新IdPの動作確認や，必要に応じてSPに新IdPへの切り替え連絡などを行っていただくことになります。
5. 新IdPの利用に問題ないことが確認でき，また旧IdPに依存するSPがなくなりましたら，学認申請システムより旧IdPの廃止申請を行ってください。
6. 旧IdPの廃止と合わせて，学認申請システムより新IdPの名称を変更してください。申請時の注意点は次の通りです。

   - 新IdP名称を「XXX大学(新)」から「XXX大学」に変更してください。（IdP名称は機関名称と同じにしていただいています）
   - 「フェデレーションの参加機関一覧への掲載を許可する」にチェックを入れてください。

ホスト名を切り替えずに新しいサーバに移行する場合は、以下の作業手順を参考にしてください。

1. 新規サーバ、あるいは運用中の既存IdPのクローンサーバを用意する
   - ホスト名は現在運用中のIdPと同一とし、IPアドレスのみ新たに割り振る
   - クローンしない場合でも旧サーバから以下の情報を引き継がなければなりません：
     entityID、スコープ、eduPersonTargetedID(ePTID)生成用のsalt、サーバ証明書
2. 新規サーバへのIdPのインストールあるいはクローンサーバのIdPアップグレード、設定等を行う
   - 旧サーバがShibboleth IdP 3.xで新サーバをShibboleth IdP 4.xとする場合は、1.で新規サーバを用意したとしてもShibboleth IdPインストールディレクトリを丸ごとコピーしてアップグレードを行うようにしてください。詳細はこちら。
3. 新IdPサーバのテストを行う（aがおすすめの方法）
   a. 試験用クライアント端末のhostsに新IdPサーバのホスト名とIPアドレスを記述してDNSに頼らずに動作確認を行う
   b. 夜間や休日などユーザの利用がない時間帯に一時的にDNSの設定を新IdPサーバに切り替えてテストする
4. 動作および各SPへの接続に問題がないことが確認できたら、DNSの設定を新IdPサーバに通信が向かうように切り替える

上記手順であれば、entityIDと使用するサーバ証明書に変更が生じないため、学認申請システムへの変更申請や各SPへの設定変更作業の依頼を行わず、IdPを切り替えることが可能です。