# 学術認証フェデレーション対応 IdP における AAL2 認証

# 評価報告書

2023 年 3 月 31日

# 目次

# 1 評価の概要

## 1.1 評価の背景と目的

昨今、クラウドサービスやモバイルデバイスの普及・活用が加速しており、様々なサービスのオンライン化が急速に進む中で、より便利に、より安全に Web サービスを利用するため、シングルサインオンや多要素認証などのセキュリティを高める機能が強く求められている時代となっている。

このような背景の中で、米国国立標準技術研究所（NIST）では電子的認証に関するガイドライン（Electronic Authentication Guideline）を公表しており、2006 年の粗飯から改定が重ねられている。これは米国の政府機関がユーザー認証(Authentication Assurance)や身元証明(Identity Assurance)を行うシステムを実装する際のガイドラインとなるものだが、米国政府機関以外にとっても参考にすべき点が多く、実際に日本をはじめとする世界各国から参考にされている基準の 1 つになっている。

ガイドラインでは、ユーザー認証、身元証明などにおいて、その手段ごとの信頼性に応じたレベル分けをしており、両者はそれぞれ IAL（Identity Assurance Level）、AAL（Authentication Assurance Level）と呼ばれる。レベル毎の要件は細かく定められているが、AAL について大雑把に言えば、AAL1 としてパスワード認証が、AAL2 として多要素認証が用いられることになる。日本では大学等が教育研究等で利用する Web サービスへのアクセスに各大学等が保有する認証システムを利用するための枠組みである学術認証フェデレーション「学認」（GakuNin）が国立情報学研究所を中心に推進されており、「学認」における AAL などの要件や活用について検討が進められている。

AAL は認証システム側（IdP）でのユーザー認証処理の結果に基づき設定、制御することになるが、IdP においてどのレベルのユーザー認証処理を行うべきかは Web サービス側(SP)が扱う情報の内容に依存することから、Web サービス側（SP）から提示したい場合も多い。そのため、SP 側から AAL を要求し、IdP 側で要求に応じたユーザー認証処理を実施、その結果を SP に応答する、という仕組みの利用が注目されている。この仕組みは SAML のフレームワークで定義されてはいるものの、その本格的な利用はこれからであり、前の記述にあるようにサービスのオンライン化が加速したことや、フィッシング被害やパスワード漏えい事故の増加などの背景もあり、今後、利用ニーズが高まるものと考える。

今回の評価では GakuNin に対応している IdP ソフトウェアを一つ例として取り上げ、「SP が求める AAL に応じた確認を IdP 側で行い、その結果を SP に応答する仕組み」に関して、どの程度の有効性があるか評価を行う。

なお、評価は「2023 年 2 月 1 日～3 月末」の期間で実施した。

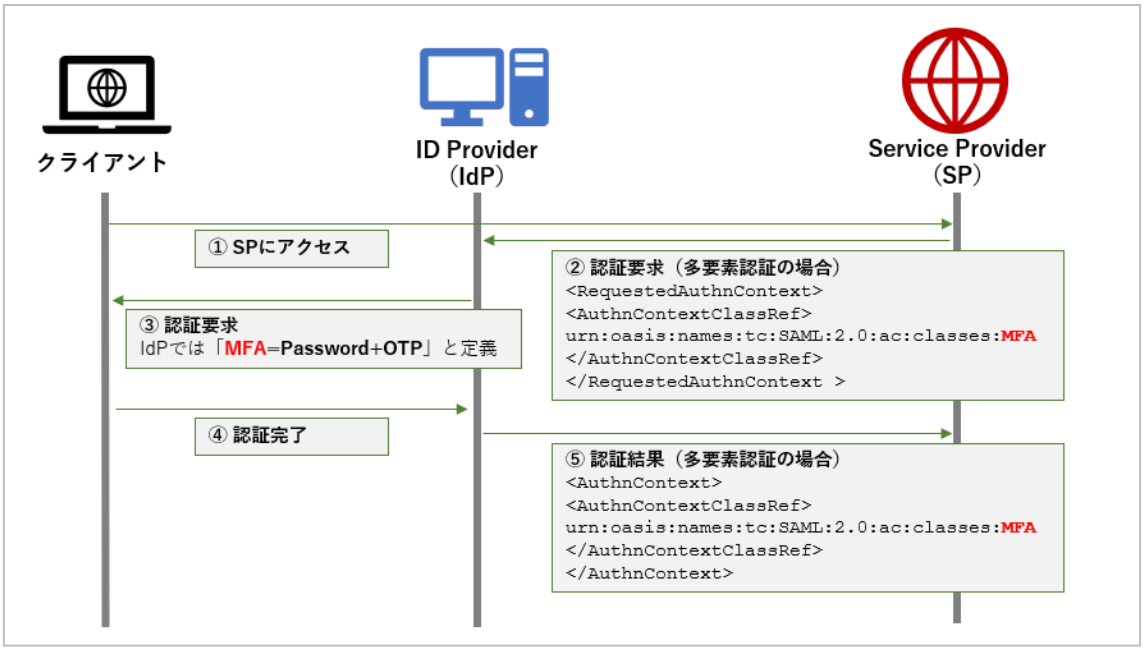
## 1.2 認証レベル要求の仕組み

SP 側から IdP 側に対して AAL を要求する仕組みは、SAML リクエスト（SP が送出）内

に含まれる「RequestedAuthnContext」要素の「AuthnContextClassRef」クラスに要求する認証方式を記載し、この値を IdP 側で解釈、ユーザー（クライアント）に対して認証を要求、認証結果を SAML レスポンス（IdP が送出）に含まれる「AuthnContext」要素の「AuthnContextClassRef」クラスに値を格納するという形で実現される。SP 側はこの認証結果の値を見ることで、要求したレベルで認証が実施されたかを確認し、最終的にサービスをユーザーに利用させるか否かを判断することができる。

なお、SP 側から要求される AAL に対して、具体的にどのような認証をユーザーに対して行えば良いかは、事前に SP 側と IdP 側との間で合意しておく必要があり、GakuNin の場合は、GakuNin がその基準を定めることとなる。本評価では、具体的な認証方式は検討の対象外であることから、AAL1 をパスワード認証、AAL2 を多要素認証という程度の区別で扱うものとする。

【認証レベル要求のシーケンス図】




① クライアントが SAML サービス（SP）にアクセス

② SP が認証システム（IdP）にリダイレクト。送出する「SAML リクエスト」に求める認証レベルや認証方式を含める。

→「RequestedAuthnContext」要素の「AuthnContextClassRef」クラスに格納

③ IdP は求められた認証レベル、認証方式（事前に IdP 側で定義ができる機能が必要）に応じてクライアントに認証を要求する。

④ クライアント側では要求された方式で認証を実施。

⑤ IdP が送出する「SAML レスポンス」に実施した認証情報を含める。

→「AuthnContext」要素の「AuthnContextClassRef」クラスに格納

### 1.3 評価環境

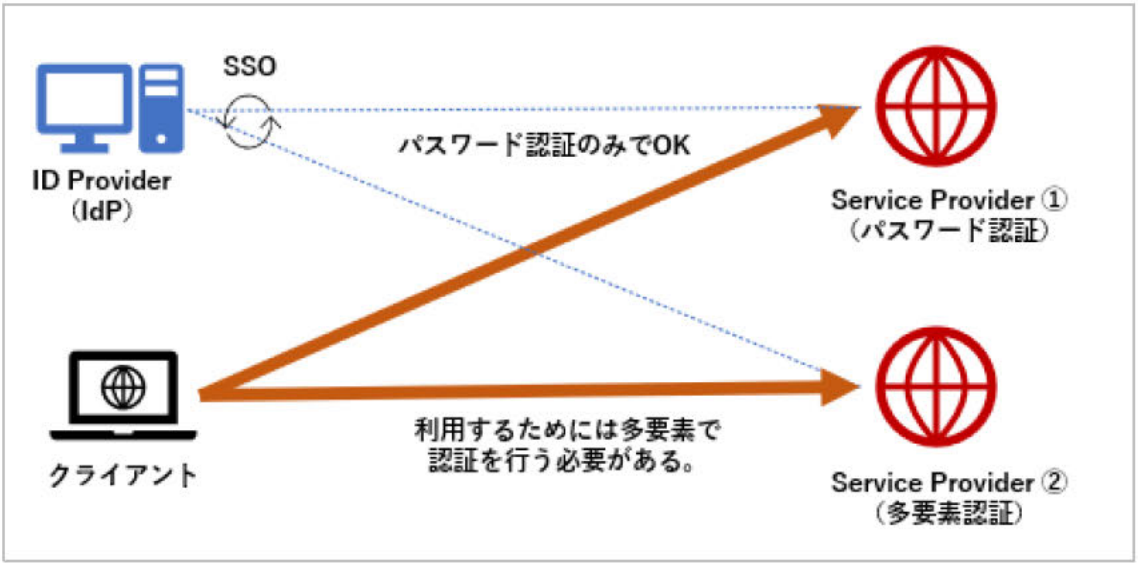
評価に利用する学認対応 IdP は株式会社セシオスが開発、販売する「Secioss Access Manager Enterprise（SAME)」を利用する。

SAME は SP 側から送出される SAML リクエスト内に含まれる認証要求レベル、認証方式を事前に定義し、その認証方式をユーザーに要求、結果を SP に返す機能を有している。

SAME のコンポーネントは認証サーバー、管理用 LDAP、ログ DB があるが、今回は全て 1 つのインスタンス（AWS 環境）に集約したものを用意する。

SAME（IdP）と連携する SAML SP は Apache を利用した Web アプリケーション（テスト用）に「Shibboleth SP」モジュールを導入、SAML 対応を行ったものを 2 つ（多要素認証を要求する SP とパスワード認証のみで OK とする SP）用意する。

【評価環境概要図】




| 役割 | 導入パッケージ |
|---|---|
| IdP | Secioss Access Manager Enterprise Ver.4.4.1 |
| | 389 Directory Server Ver. 1.4.3.30 |
| | MariaDB Ver. 10.3.35 |
| | Apache Ver. 2.4.37 |
| | PHP Ver. 7.2.24 |
| | Perl Ver. 5.26.3 |
| SAML SP (SP①/SP②) | Apache Ver. 2.4.37 |
| | Shibbolth SP Ver. 3.4.1 |
| クライアント PC | Windows 11 Pro |
| | Microsoft Edge / Google Chrome |

# 2 評価内容

## 2.1 事前定義

### 2.1.1 SAML SP の設定

今回、SAML SP 側から送出する SAML リクエストには認証レベルとして以下の値を「RequestedAuthnContext」要素の「AuthnContextClassRef」クラスに入れる。

・SP①：AAL1・・・「パスワード認証」のみで利用可。
・SP②：AAL2・・・「パスワード認証+α」の多要素認証を行った場合のみ利用可。
→「+α」の認証方式は任意とする。

```
<RequestedAuthnContext>
  <AuthnContextClassRef>
      urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2（or AAL1）
  </AuthnContextClassRef>
</RequestedAuthnContext >
```

今回の評価では「AAL1」、「AAL2」という値（文字列）を「AuthnContextClassRef」クラスに入れるが、この認証レベルを表す文字列は共通の定義として統一されている状況にはない。そのため、SP 側で設定する文字列に合わせて IdP 側でも定義できるような機能が現状では求められる。

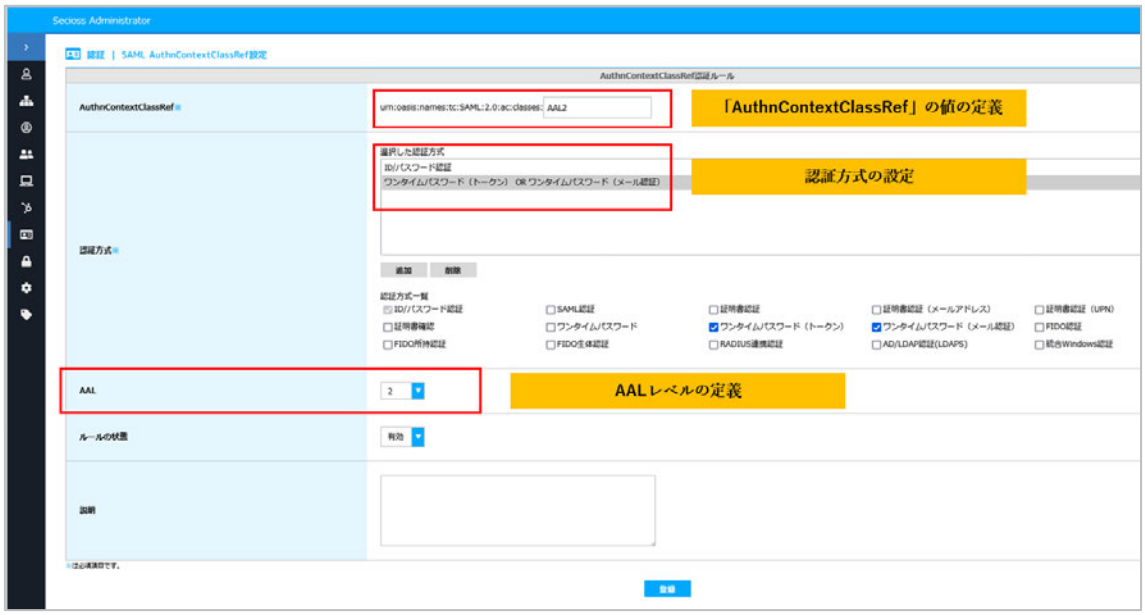
### 2.1.2 IdP の設定

SAME 側では「AuthnContextClassRef」に格納されている値（文字列）に応じた認証方式を定義する。「2.1.1」の SAML SP 側の設定を受け、認証方式を以下のように定義、設定する。また、認証レベルを要求しない SP（「AuthnContextClassRef」に値がない）が混在している状況を想定し、その場合に適用される「デフォルト」も定義する。

なお、SAME には認証方式として「パスワード認証」のほか、「ワンタイムパスワード（OTP：メールで通知/OTP アプリを利用）」、「FIDO」、「証明書認証」など幾つか機能を有しているが、今回は「OTP（アプリ方式）」を利用する。

・AAL1・・・パスワード認証
・AAL2・・・パスワード認証+ワンタイムパスワード（OTP）
・デフォルト（認証方式の指定が無い場合）・・・パスワード認証
※OTP はスマートデバイス向け「Google Authenticator」アプリを利用する。

【SAME：「AuthnContextClassRef」の文字列定義と AAL レベルの設定画面】




以上の設定を行うと、認証完了後に送出する SAML レスポンスの「AuthnContext」要素の「AuthnContextClassRef」クラスに定義した文字列（今回は AAL2 or AAL1）を入れて SP へ返却する動作となる。

```
<saml:AuthnContext>
    <saml:AuthnContextClassRef>
        urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2（or AAL1）
    </saml:AuthnContextClassRef>
</saml:AuthnContext>
```

### 2.1.3 クライアントから SP へアクセス

クライアントから SP へアクセスし、IdP へリダイレクト、ログイン画面で SP が要求するレベルに応じた認証が求められることを確認する。また認証済み状態から認証要求レベルが異なる SP へのアクセス時に追加で認証要求が求められるかなど、想定される利用パターンを確認する（具体的な評価項目は「2.2 評価項目」を参照）。

## 2.2 評価項目

以下に評価項目と評価に対して期待する結果を記載する。

| No | 種別 | 内容 |
|---|---|---|
| 1 | 評価項目 | AAL1/AAL2 に該当する認証要求の定義とその要求に対する動作についての設定機能 |
| | 詳細 | SP 側で SAML リクエストに含める認証要求レベルに合わせて、IdP 側で認証方式を定義が出来る機能を確認する。 |
| | 期待する結果 | SP が送出する認証レベルに合わせて IdP は認証方式を柔軟に定義、結果を返却できる機能を有していること。 |
| 2 | 評価項目 | AAL2 認証要求に対する基本動作 |
| | 詳細 | SP が認証レベル「AAL2」を要求した場合、IdP はそれを満たす認証方式をクライアントに要求し、認証レベルを満たした場合のみ認証を完了とする基本的な動作を確認する。 |
| | 期待する結果 | IdP は SP が要求する認証レベル「AAL2」を満たす認証方式をクライアントに要求し、認証が正常に完了した場合のみ SP の利用ができること。 |
| 3 | 評価項目 | AAL1 認証後の AAL2 認証要求における昇格動作 |
| | 詳細 | 認証レベル「AAL1」を要求していた SP が認証レベル「AAL2」に変更された場合（SP の認証レベル昇格)、次回アクセス時にはクライアントに「AAL2」を満たす認証方式を要求する動作となるか確認する。 |
| | 期待する結果 | 認証レベルが「AAL1」から「AAL2」に変更された場合でも、クライアントには認証レベルに合わせた認証を要求すること。ただし認証セッションが継続している場合には IdP へのリダイレクトが発生しないため、ログオフや SP/IdP 側で一度、認証セッションを破棄するような操作が必要になる点に留意すること。 |
| 4 | 評価項目 | 異なる SP 間での SSO における基本動作（AAL2→AAL2) |
| | 詳細 | SSO 環境下で 2 つの SP が以下の認証レベルを要求する場合、クライアントが SP 間の移動を行う際に必要に応じて追加の認証が求められる、或いは求められないことを確認する。<br>SP①の認証レベル：AAL2<br>SP②の認証レベル：AAL2 |
| | 期待する結果 | SP 間で認証レベルが同一の場合、基本的には追加で認証を求められないこと。ただし SP1 と SP2 で求める認証方式が異なる場合には実施していない認証方式が求められること。 |
| 5 | 評価項目 | 異なる SP 間での SSO における降格動作（AAL2→AAL1) |
| | 詳細 | SSO 環境下で 2 つの SP が以下の認証レベルを要求する場合、クライアントが SP 間の移動を行う際に必要に応じて追加の認証が求められる、或いは求められないことを確認する。 |

| | | |
|---|---|---|
| | | SP①の認証レベル：AAL2<br>SP②の認証レベル：AAL2 から AAL1 に降格 |
| | 期待する結果 | 認証レベルが「AAL2」から「AAL1」に降格した場合、基本的には追加で認証を求められないこと。ただし、変更されたレベルで要求される認証方式を実施していない場合、追加で認証が求められること。 |
| 6 | 評価項目 | 異なる SP 間での SSO における昇格動作（AAL1→AAL2） |
| | 詳細 | SSO 環境下で 2 つの SP が以下の認証レベルを要求する場合、クライアントが SP 間の移動を行う際に必要に応じて追加の認証が求められる、或いは求められないことを確認する。<br>SP①の認証レベル：AAL1<br>SP②の認証レベル：AAL1 から AAL2 に昇格 |
| | 期待する結果 | 認証レベルが「AAL1」から「AAL2」に昇格した場合、基本的には追加で認証を求めること。ただし、認証レベルが変更された SP が求める認証方式を他の SP の認証で既に実施済みの場合、追加で認証は求められないこと。 |
| 7 | 評価項目 | AAL1/AAL2 の両方等複数指定による認証要求時の動作 |
| | 詳細 | SP が送出する SAML リクエストに複数の認証レベル要求が含まれている場合の挙動について確認する。 |
| | 期待する結果 | 「AuthnContextClassRef」クラスが複数記載されている場合、最も高い認証レベルがクライアントに要求されること。 |
| 8 | 評価項目 | ローカル（学認外）認証連携時の動作 |
| | 詳細 | SSO 環境下で認証レベルを要求する SP と要求しない SP が含まれている場合でも動作に問題がないか確認する。 |
| | 期待する結果 | IdP で「認証レベルを要求する SP」と「認証レベルを要求しない SP」の定義を行い、定義に従った認証方式が要求されること。また、このような SP が混在している場合でも認証システム全体で矛盾や問題が発生しないこと。 |
| 9 | 評価項目 | 強制再認証時の動作 |
| | 詳細 | SP が送出する SAML リクエストに強制再認証（ForceAuthn）が含まれている場合の挙動について確認する。 |
| | 期待する結果 | IdP ですでに認証済みのセッションがあったとしても SP から「ForceAuthn」を含む SAML リクエストを受けた場合、認証を実施すること。また同時に認証レベルの要求があった場合、定義に従いクライアントに認証を要求すること。 |

# 3 評価の結果

## 3.1 評価結果

評価項目に対する評価結果は全ての項目で想定する結果となった。以下に詳細を記す。

| No | 評価項目 | 結果 |
|---|---|---|
| 1 | AAL1/AAL2 に該当する認証要求の定義とその要求に対する動作についての設定機能 | 今回利用した IdP ソフトウェア（SAME）では、SP が「AuthnContextClassRef」クラスに設定する文字列に合わせて認証方式を定義する機能を有しており、また、SP 側が設定する文字列がどんな値でも、複数 SP 間で異なる文字列でも柔軟に定義、利用できることを確認した。 |
| 2 | AAL2 認証要求に対する基本動作 | IdP は SP が要求する認証レベル「AAL2」を満たす認証方式（パスワード認証+OTP）をクライアントに要求し、認証が正常に完了した場合のみ SP の利用ができることを確認した。 |
| 3 | AAL1 認証後の AAL2 認証要求における昇格動作 | 認証レベルが「AAL1（パスワード認証）」から「AAL2（パスワード認証+OTP）」に昇格した場合、次回アクセス時には「AAL2（パスワード認証+OTP）」が要求されることを確認した。ただし、認証セッションが保持されている状況では IdP にリダイレクト要求がないため、認証レベル変更前の状態で SP の利用が継続できてしまう点は実運用で考慮すべき事項である。 |
| 4 | 異なる SP 間での SSO における基本動作（AAL2→AAL2） | 今回設定した認証レベルの定義において、SP 間で認証レベルが同一の場合、追加で認証を求められないこと。認証レベルは同一だが認証要素が別の場合、追加で認証を求められることを確認した。 |
| 5 | 異なる SP 間での SSO における降格動作（AAL2→AAL1） | 今回設定した認証レベルの定義において、認証レベルが「AAL2」から「AAL1」に降格した場合、追加で認証を求められないことを確認した。 |
| 6 | 異なる SP 間での SSO における昇格動作（AAL1→AAL2） | 今回設定した認証レベルの定義において、認証レベルが「AAL1」から「AAL2」に昇格した場合、追加で OTP の認証を求められることを確認した。 |
| 7 | AAL1/AAL2 の両方等複数指定による認証要求時の動作 | 複数の値（今回は「AAL1/AAL2」という文字列）が記載されている場合、最も高い認証レベル「AAL2」の定義が適用され、認証時、クライアントに「パスワード認証+OTP」が要求されることを確認した。 |

| | | |
|---|---|---|
| 8 | ローカル（学認外）認証連携時の動作 | 「認証レベルを要求する SP」と「認証レベルを要求しない SP」が混在している環境にて、「認証レベルを要求しない SP」へのアクセスでは「パスワード認証」を要求され、認証後に「認証レベル「AAL2」を要求する SP」へアクセスした場合は追加で「OTP」が要求されることを確認した。 |
| 9 | 強制再認証時の動作 | SP から「ForceAuthn」を含む SAML リクエストを受けた場合、IdP のセッションが有効な状態でも SP が要求するレベルの認証が要求されることを確認した。 |

# 4 考察

## 4.1 機能の有用性について

昨今のデジタル環境において、パスワード認証だけでは不十分な時代であるのは周知の事実であり、追加で認証を求める多要素認証や、生体情報を利用した認証方式の採用が強く求められる。

しかしながら Web サービスを利用するユーザーのセキュリティ知識や意識が低い場合や、認証システムを導入しているが多要素認証や安全な認証方式を採用できていない、或いは適切な運用ができていない（費用やリソースの問題もあるだろう）状況もまだまだ散見される。

このような状況において、例えば、機微な情報を扱わないサービスの場合にはパスワード認証を許容し、個人情報を扱うようなサービスは多要素認証を強制させるといったように Web サービス提供側がサービス内容に合わせて必要な認証レベルを（半ば強制的に）要求することは（ある意味、無意識に）利用者のセキュリティリスクを低減する効果があると考える。

以上のことから Web サービス（SP）の認証セキュリティにおいて、「SP 側が認証レベルを要求（強制）する」仕組みは、非常に有用な仕組みであると言える。

## 4.2 課題と今後について

今回の検証において、重要な要素は SP 側から要求する認証レベルにどのような値（文字列）を利用し IdP 側で定義するか、という点である。

SAML の標準化団体 OASIS の SAML 関連ドキュメントには「認証コンテキスト（認証方式）」として、「Password/X.509/ Kerberos」などの値は定義されているが、作成されたのは 2005 年と古く、FIDO やパスキー（パスキーは FIDO 技術を利用しているのだが）など新しい認証技術についての記載は当然のことながらない。また今回の検証で実施したように具体的な認証方式は運用者に一任し、SP は認証レベル（AAL）を要求するよう

な使い方も想定される。導入している IdP 製品によって備わっている認証機能が異なること、ユーザーに利用させたい認証方式も状況によって様々だと考えると、むしろ後者の使い方が現実的だとも考えられる。

以上のことから「SP 側から認証方式や認証レベルを要求する際、どのような値を利用するか？」という点が課題としてあげられる。

しかしながら、様々な Web サービスが提供されている状況のなか、サービス間で統一された取り決めを行うには、例えば OASIS による SAML フレームワークの改定などが必要となり、直近で足並みをそろえるのは難しいと思われる。

一方、GakuNin の場合は、GakuNin が SP/IdP が備えるべき技術、運用基準を示しているため、課題に対する解決策も提示しやすいと考える。

シングルサインオン環境における「SP 側が認証レベルを要求（強制）する」仕組みは、GakuNin の枠組みの中で検討を重ね、利用されるようになれば、普及への第一歩となると考える。

## 5 おわりに

今回の評価で、「SP 側から認証レベルを提示する仕組み」における有用性と課題を明確化することができたと考える。今後、このような認証連携技術はさらに重要となり、広く普及することが期待される。

以上

# 学術認証フェデレーション対応IdPにおけるAAL2認証

# 評価報告書

## 別添　試験記録

2023年3月31日

## 【評価レポート試験項目】

下記試験項目について、期待する結果が得られるか試験を実施する。
各試験の前提条件として、「事前準備」シートにてIdPの設定を行う。
各試験シートにて、IdP、SPの設定を試験に合わせて変更していき期待する動作となるかを確認する。
画面のキャプチャ、SAMLでの認証ではSAMLのトレースログを試験結果として記録する。

評価レポートの評価項目に対する試験を実施する。

| No | 項目 | 詳細 | 期待する結果 |
|---|---|---|---|
| 1 | AAL1/AAL2に該当する認証要求の定義とその要求に対する動作についての設定機能 | SP側でSAMLリクエストに含める認証要求レベルに合わせて、IdP側で認証方式を定義が出来る機能を確認する。 | SPが送出する認証レベルに合わせてIdPは認証方式を柔軟に定義、結果を返却できる機能を有していること。 |
| 2 | AAL2認証要求に対する基本動作 | SPが認証レベル「AAL2」を要求した場合、IdPはそれを満たす認証方式をクライアントに要求し、認証レベルを満たした場合のみ認証を完了とする基本的な動作を確認する。 | IdPはSPが要求する認証レベル「AAL2」を満たす認証方式をクライアントに要求し、認証が正常に完了した場合のみSPの利用ができること。 |
| 3 | AAL1認証後のAAL2認証要求における昇格動作 | 認証レベル「AAL1」を要求していたSPが認証レベル「AAL2」に変更された場合（SPの認証レベル昇格）、次回アクセス時にはクライアントに「AAL2」を満たす認証方式を要求する動作となるか確認する。 | 認証レベルが「AAL1」から「AAL2」に変更された場合でも、クライアントには認証レベルに合わせた認証を要求すること。ただし認証セッションが継続している場合にはIdPへのリダイレクトが発生しないため、ログオフやSP/IdP側で一度、認証セッションを破棄するような操作が必要になる点に留意すること。 |
| 4 | 異なるSP間でのSSOにおける基本動作（AAL2→AAL2） | SSO環境下で2つのSPが以下の認証レベルを要求する場合、クライアントがSP間の移動を行う際に必要に応じて追加の認証が求められる、或いは求められないことを確認する。<br>SP①の認証レベル：AAL2<br>SP②の認証レベル：AAL2 | SP間で認証レベルが同一の場合、基本的には追加で認証を求められないこと。ただしSP1とSP2で求める認証方式が異なる場合には実施していない認証方式が求められること。 |
| 5 | 異なるSP間でのSSOにおける降格動作（AAL2→AAL1） | SSO環境下で2つのSPが以下の認証レベルを要求する場合、クライアントがSP間の移動を行う際に必要に応じて追加の認証が求められる、或いは求められないことを確認する。<br>SP①の認証レベル：AAL2<br>SP②の認証レベル：AAL2からAAL1に降格 | 認証レベルが「AAL2」から「AAL1」に降格した場合、基本的には追加で認証を求められないこと。ただし、変更されたレベルで要求される認証方式を実施していない場合、追加で認証が求められること。 |
| 6 | 異なるSP間でのSSOにおける昇格動作（AAL1→AAL2） | SSO環境下で2つのSPが以下の認証レベルを要求する場合、クライアントがSP間の移動を行う際に必要に応じて追加の認証が求められる、或いは求められないことを確認する。<br><br>SP①の認証レベル：AAL1<br>SP②の認証レベル：AAL1からAAL2に昇格 | 認証レベルが「AAL1」から「AAL2」に昇格した場合、基本的には追加で認証を求めること。ただし、認証レベルが変更されたSPが求める認証方式を他のSPの認証で既に実施済みの場合、追加で認証は求められないこと。 |
| 7 | AAL1/AAL2の両方等複数指定による認証要求時の動作 | SPが送出するSAMLリクエストに複数の認証レベル要求が含まれている場合の挙動について確認する。 | 「AuthnContextClassRef」クラスが複数記載されている場合、最も高い認証レベルがクライアントに要求されること。 |
| 8 | ローカル（学認外）認証連携時の動作 | SSO環境下で認証レベルを要求するSPと要求しないSPが含まれている場合でも動作に問題がないか確認する。 | IdPで「認証レベルを要求するSP」と「認証レベルを要求しないSP」の定義を行い、定義に従った認証方式が要求されること。また、このようなSPが混在している場合でも認証システム全体で矛盾や問題が発生しないこと。 |
| 9 | 強制再認証時の動作 | SPが送出するSAMLリクエストに強制再認証（ForceAuthn）が含まれている場合の挙動について確認する。 | IdPですでに認証済みのセッションがあったとしてもSPから「ForceAuthn」を含むSAMLリクエストを受けた場合、認証を実施すること。また同時に認証レベルの要求があった場合、定義に従いクライアントに認証を要求すること。 |

## 【その他機能試験項目】

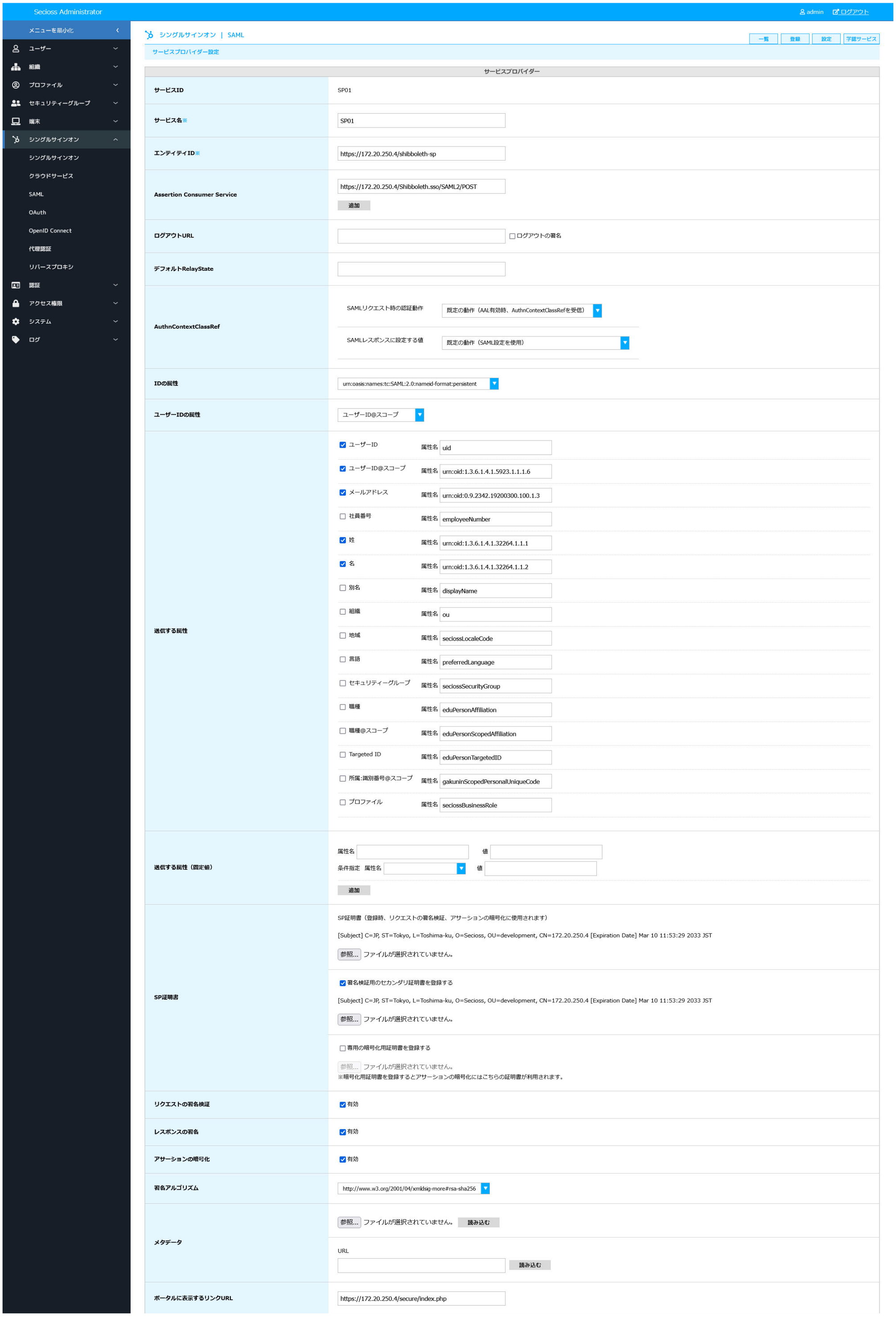
評価レポートの観点とは別にAAL2認証機能のその他機能実装に対する試験を実施する。

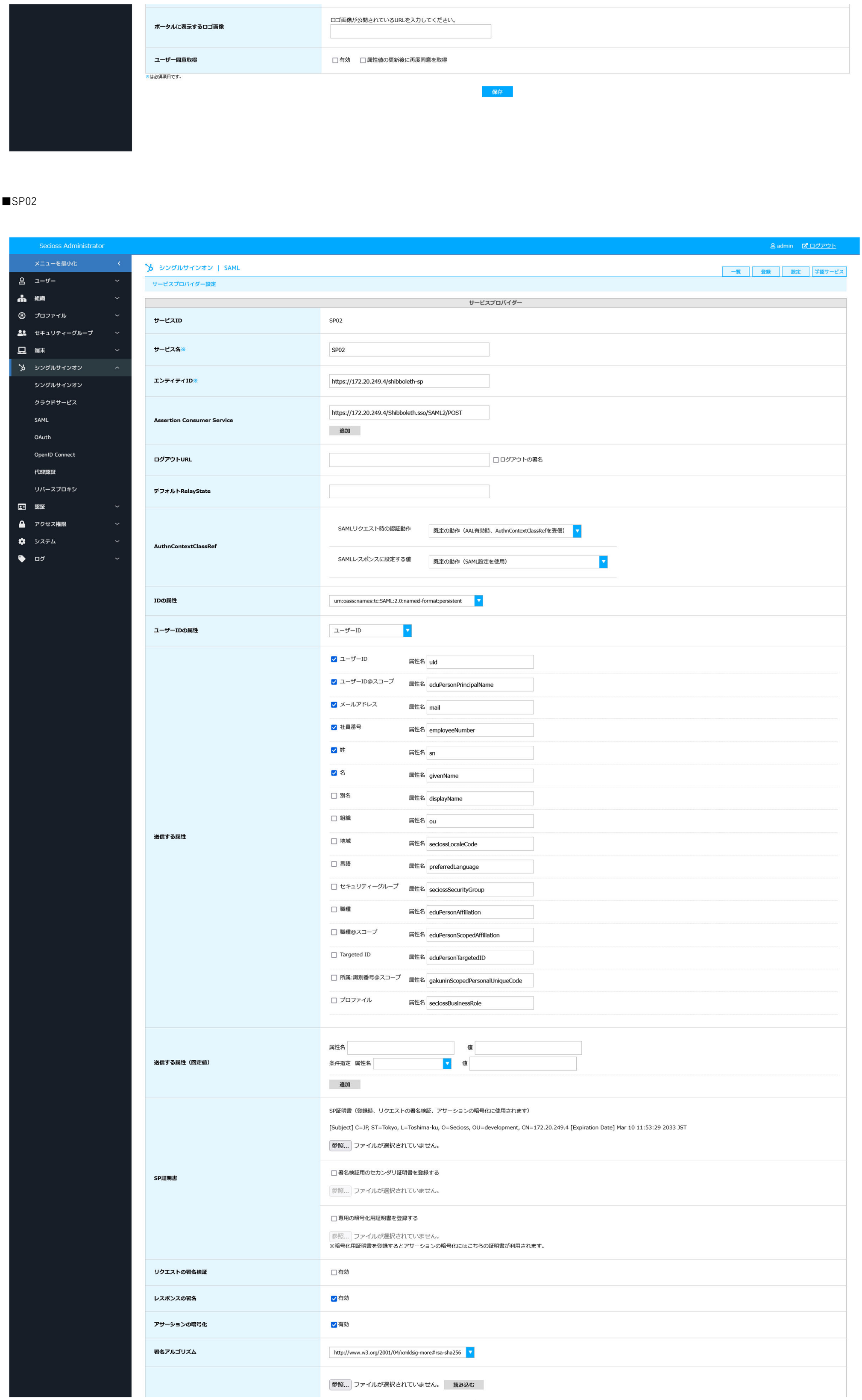
| No | 項目 | 詳細 | 期待する結果 |
|---|---|---|---|
| 1 | SPから要求されたAuthnContextClassRefが未定義時の動作 | SPから要求されたAuthnContextClassRefの認証要求がIdPで定義していないAuthnContextClassRefの場合、ユーザーにエラーを提示しSPへエラー応答を返却する | SPからAAL2の認証を求められているとき、ユーザーがワンタイムパスワード設定を行っていないとき、ユーザーにエラーを表示したのちSPにNoAuthnContextのエラーを返却する。 |
| 2 | AuthnContextClassRefの条件を満たせないときの動作 | SPから要求されたAAL2の認証要求が満たせないことが確定した場合、ユーザーにエラーを表示したのちSPにエラー応答を返す。 | SPからAAL2の認証を求められているとき、ユーザーがワンタイムパスワード設定を行っていないとき、ユーザーにエラーを表示したのちSPにNoAuthnContextのエラーを返却する。 |
| 3 | SPからの、AuthnContextClassRefを無視してIdPで任意のAuthnContextClassRefを返却する。 | SPが送出するSAMLリクエスト内のAuthnContextClassRefを無視してIdPで認証する。<br>返却する値は、SPから送出されたAuthnContextClassRefで返却を行う。または、IdPにて指定の値を送信するか送信しないかを選択する。 | SPからの、AuthnContextClassRefを無視してIdPにて設定した認証を実施する。<br>以下の順に検証し、期待する動作を得られること。<br>1. SAMLレスポンスには、SPから送出されたAuthnContextClassRefで返却する。<br>2. SAMLレスポンスには、IdPにて設定したAuthnContextClassRefで返却する。<br>3. SAMLレスポンスにAuthnContextClassRefを送出しない |

# 【事前準備】SAML SP設定

SAML SPと連携するための設定をIdPにて実施する
2つのShibboleth SPとのSAML連携を設定。

■SP01




ポータルに表示するロゴ画像
ロゴ画像が公開されているURLを入力してください。
ユーザー同意取得
有効
属性値の更新後に再度同意を取得
※は必須項目です。
保存
Secioss Administrator
admin
ログアウト
メニューを最小化
ユーザー
組織
プロファイル
セキュリティーグループ
端末
シングルサインオン
シングルサインオン
クラウドサービス
SAML
OAuth
OpenID Connect
代理認証
リバースプロキシ
認証
アクセス権限
システム
ログ
シングルサインオン | SAML
一覧
登録
設定
学認サービス
サービスプロバイダー設定
サービスプロバイダー
サービスID
SP02
サービス名※
SP02
エンティティID※
https://172.20.249.4/shibboleth-sp
Assertion Consumer Service
https://172.20.249.4/Shibboleth.sso/SAML2/POST
追加
ログアウトURL
ログアウトの署名
デフォルトRelayState
AuthnContextClassRef
SAMLリクエスト時の認証動作
既定の動作（AAL有効時、AuthnContextClassRefを受信）
SAMLレスポンスに設定する値
既定の動作（SAML設定を使用）
IDの属性
urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
ユーザーIDの属性
ユーザーID
送信する属性
ユーザーID 属性名 uid
ユーザーID@スコープ 属性名 eduPersonPrincipalName
メールアドレス 属性名 mail
社員番号 属性名 employeeNumber
姓 属性名 sn
名 属性名 givenName
別名 属性名 displayName
組織 属性名 ou
地域 属性名 seciossLocaleCode
言語 属性名 preferredLanguage
セキュリティーグループ 属性名 seciossSecurityGroup
職種 属性名 eduPersonAffiliation
職種@スコープ 属性名 eduPersonScopedAffiliation
Targeted ID 属性名 eduPersonTargetedID
所属:識別番号@スコープ 属性名 gakuninScopedPersonalUniqueCode
プロファイル 属性名 seciossBusinessRole
送信する属性（固定値）
属性名
値
条件指定 属性名
値
追加
SP証明書
SP証明書（登録時、リクエストの署名検証、アサーションの暗号化に使用されます）
[Subject] C=JP, ST=Tokyo, L=Toshima-ku, O=Secioss, OU=development, CN=172.20.249.4 [Expiration Date] Mar 10 11:53:29 2033 JST
参照... ファイルが選択されていません。
署名検証用のセカンダリ証明書を登録する
参照... ファイルが選択されていません。
専用の暗号化用証明書を登録する
参照... ファイルが選択されていません。
※暗号化用証明書を登録するとアサーションの暗号化にはこちらの証明書が利用されます。
リクエストの署名検証
有効
レスポンスの署名
有効
アサーションの暗号化
有効
署名アルゴリズム
http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
参照... ファイルが選択されていません。
読み込む

■SP02

[redacted]

| | |
|---|---|
| **メタデータ** | URL<br>読み込む |
| **ポータルに表示するリンクURL** | https://172.20.249.4/secure/index.php |
| **ポータルに表示するロゴ画像** | ロゴ画像が公開されているURLを入力してください。 |
| **ユーザー同意取得** | ☐ 有効　☐ 属性値の更新後に再度同意を取得 |

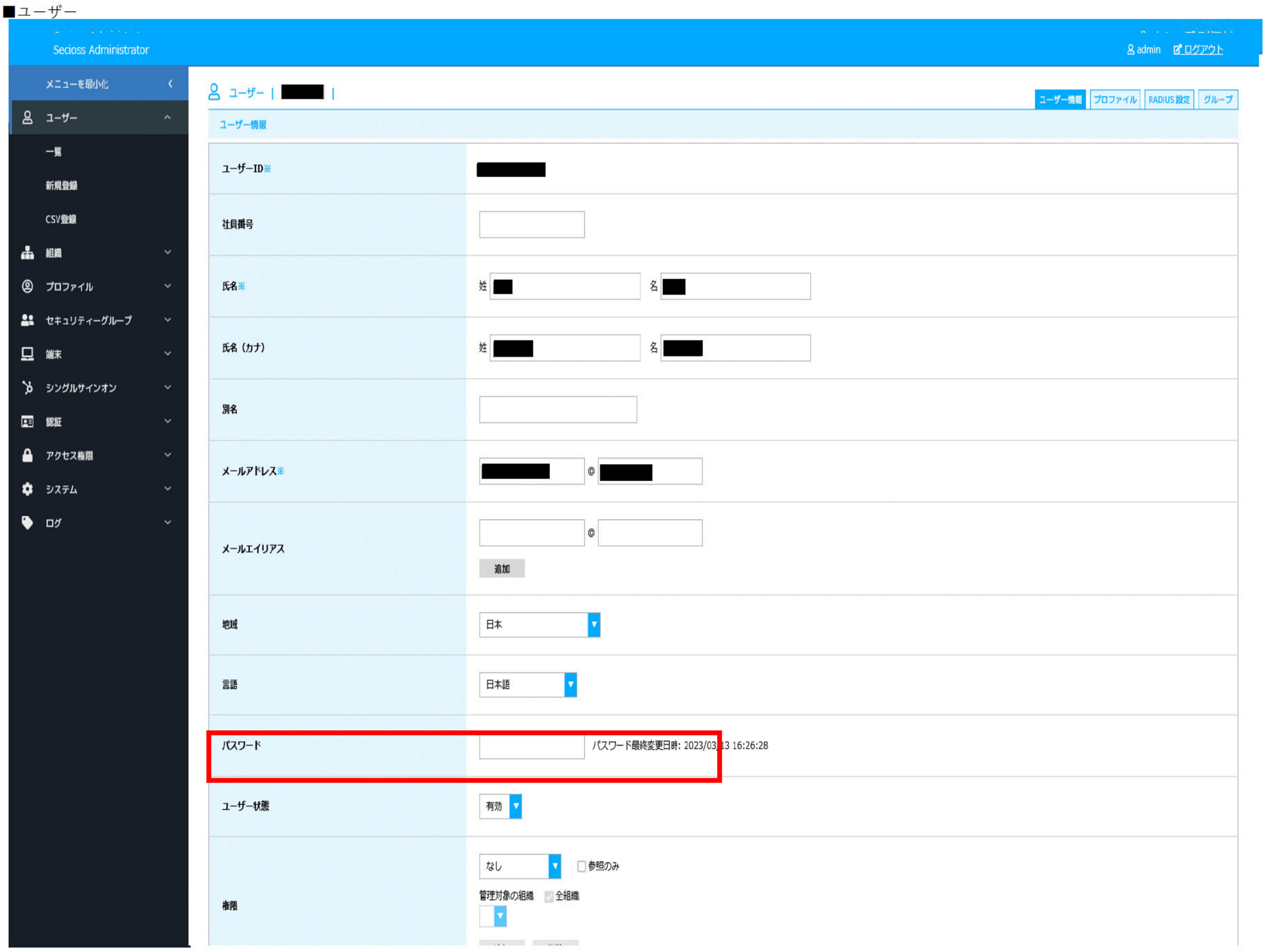
※は必須項目です。

保存

# 【事前準備】ユーザー設定

ユーザーがSP01,02にアクセスできる許可を設定。
許可するサービスに、「SP01」「SP02」を設定し保存。

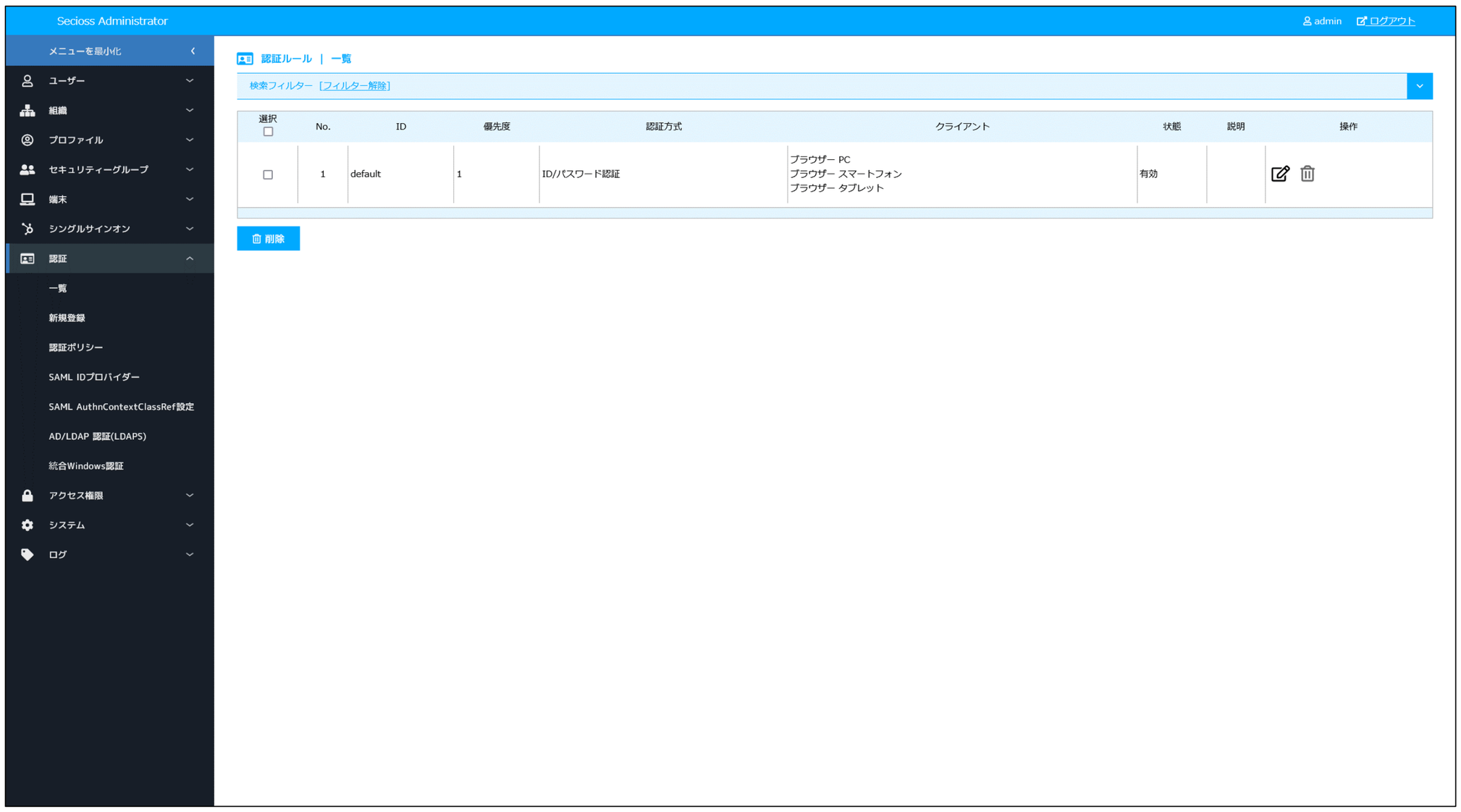
■ユーザー



# 【事前準備】認証ルール設定

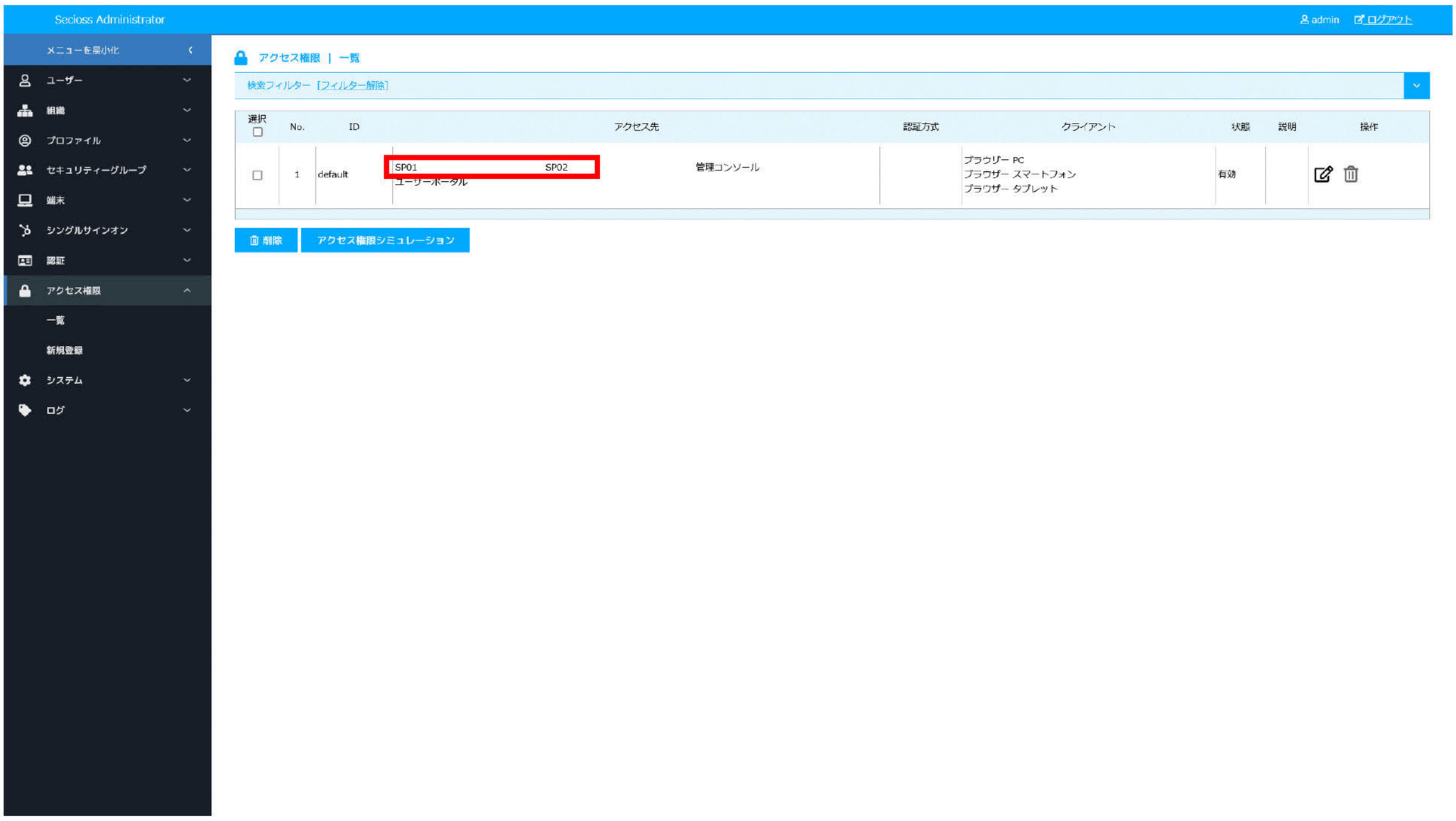
IdPやSPにログインするための認証を設定します。
defaultの認証ルールとして、「ID/パスワード認証」を指定します。
この設定は、AALに対応していないSAMLSPや代理認証を必要とするSPなど汎用的に利用する認証設定です。

■ユーザー



# 【事前準備】アクセス権限設定

IdPやSPにログインするための認証を設定します。
ネットワークやユーザーの持つプロファイルやグループ情報によりアクセス制御をかけるための設定です。
この設定は、AALに対応していないSAMLSPや代理認証を必要とするSPなど汎用的に利用する認証設定です。
アクセス権限のdefaultに「SP1」「SP2」を設定します。



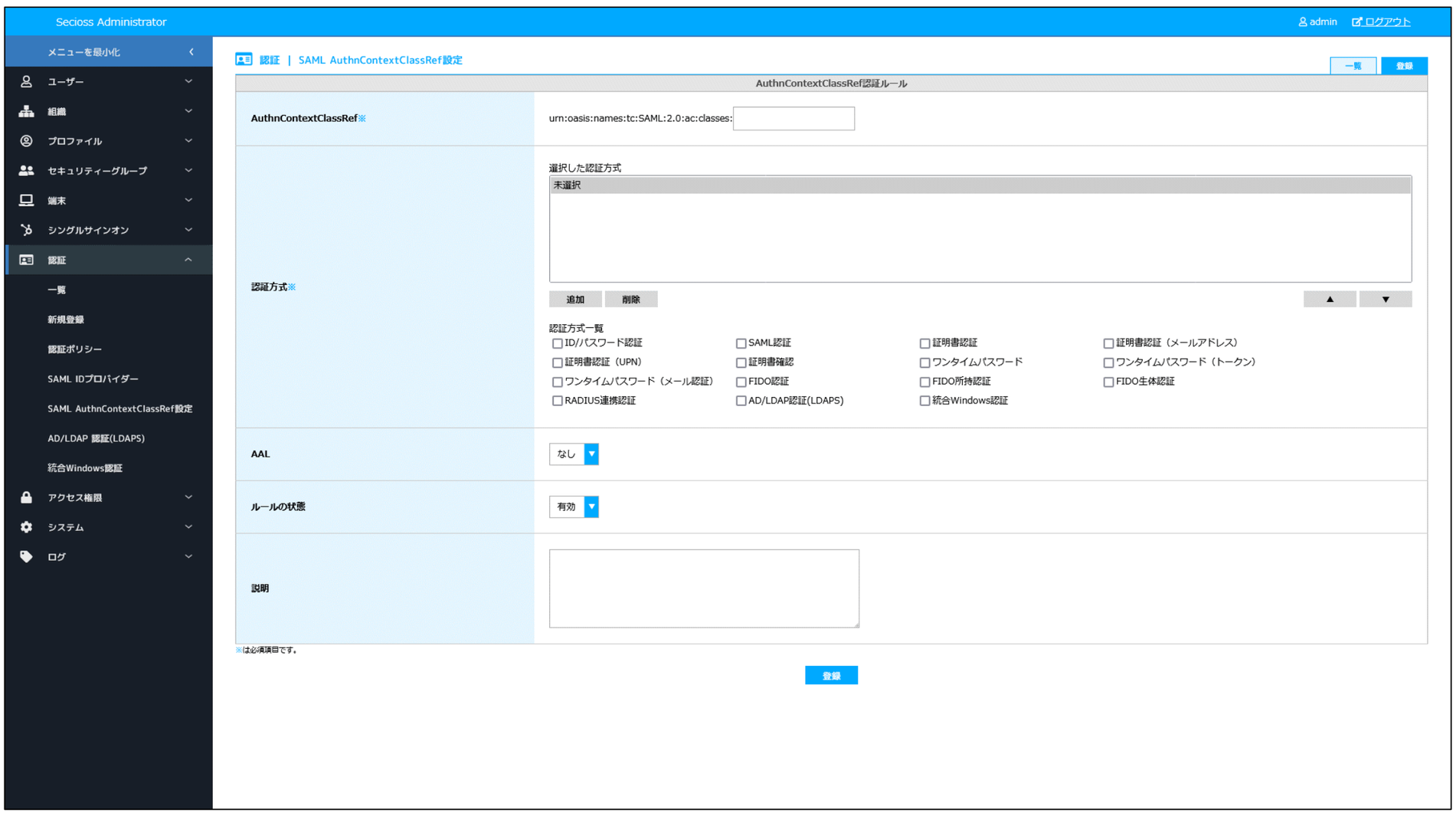
| 区分 | 評価レポート |
|---|---|
| 試験No | 1 |
| 試験項目 | AAL1/AAL2に該当する認証要求の定義とその要求に対する動作についての設定機能 |
| 詳細 | SP側でSAMLリクエストに含める認証要求レベルに合わせて、IdP側で認証方式を定義が出来る機能を確認する。 |
| 期待する結果 | SPが送出する認証レベルに合わせてIdPは認証方式を柔軟に定義、結果を返却できる機能を有していること。 |

1. IdPで受け付けるAuthnContextClassRefの定義設定画面

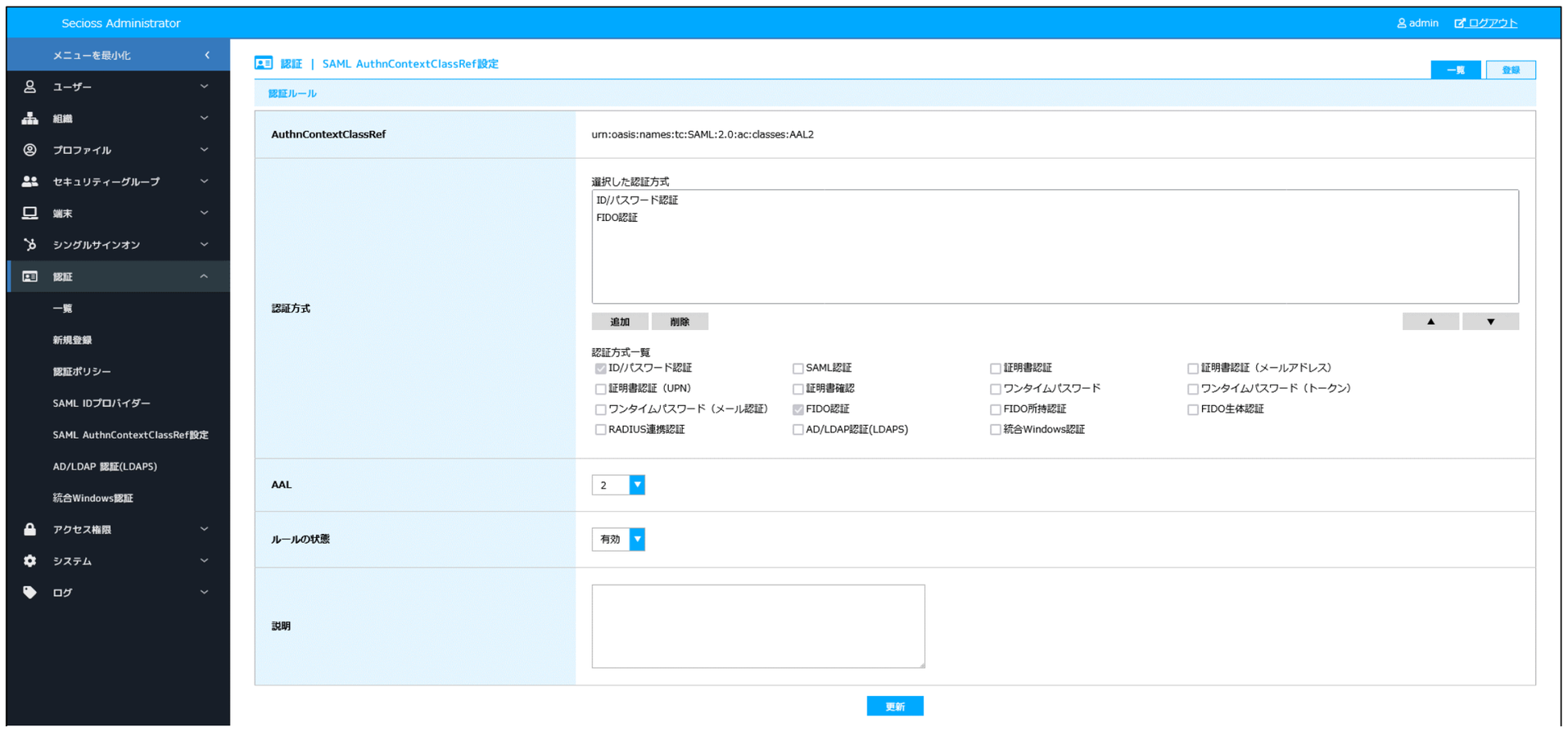
以下の設定が可能

| 画面項目 | 説明 |
|---|---|
| AuthnContextClassRef | SPからのSAMLリクエストに含まれるAuthnContextClassRefの値を設定可能 |
| 認証方式 | AuthnContextClassRef受信時に求める認証が定義可能。<br>単一の認証方式、or、andで複数設定ができ、認証の順番も指定可能 |
| AAL | 定義するAuthnContextClassRefがどのAAL（Authenticator Assurance Level）かを定義可能。<br>管理上のラベルとして利用するほか、複数のAuthnContextClassRefが定義されてリクエストされてきた場合に、AALが一番高い設定を求めるようにするために利用。 |
| ルールの状態 | 定義したAuthnContextClassRefの設定が利用できる状態か否かを設定可能。 |
| 説明 | 管理用の説明欄 |

■新規作成

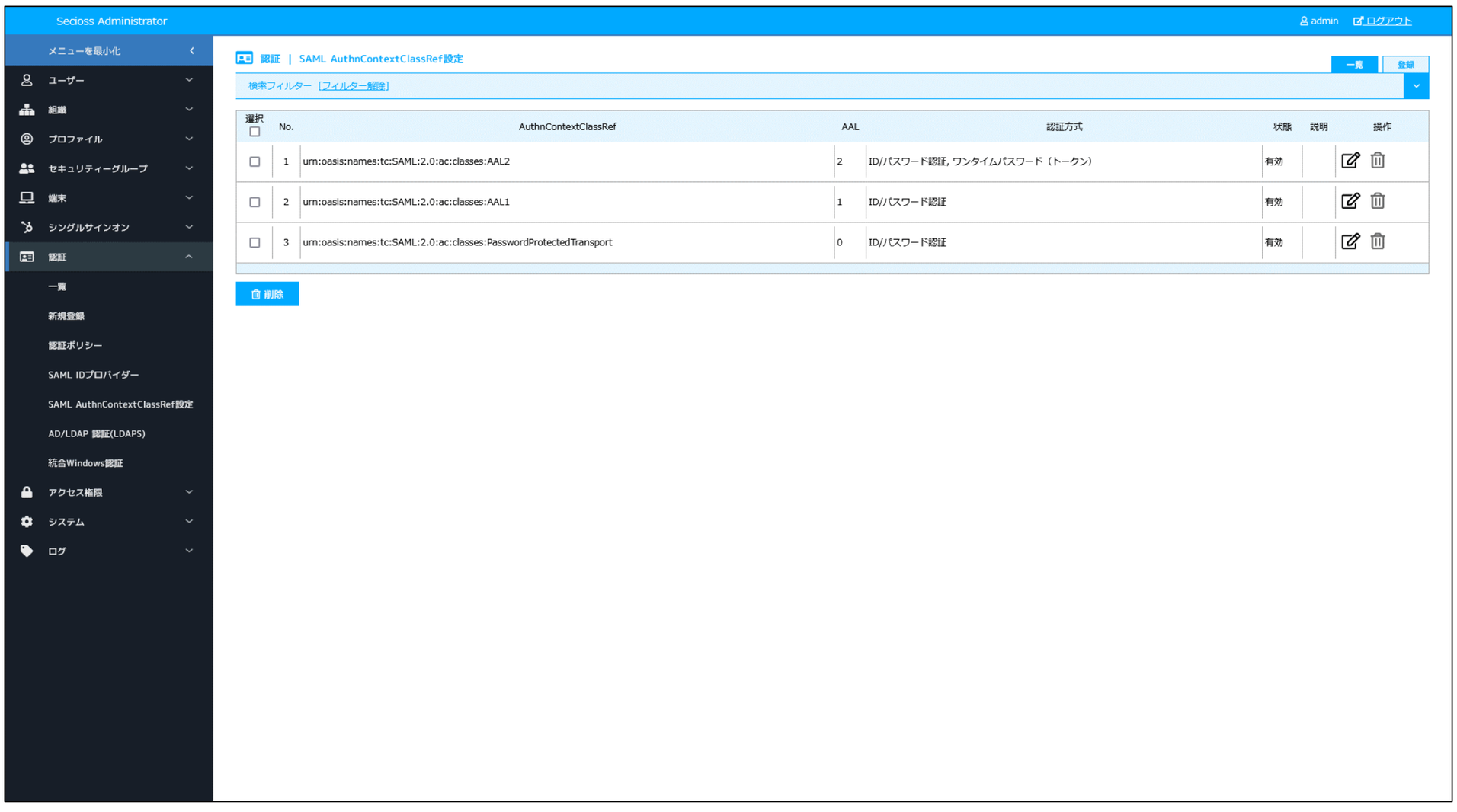



■更新



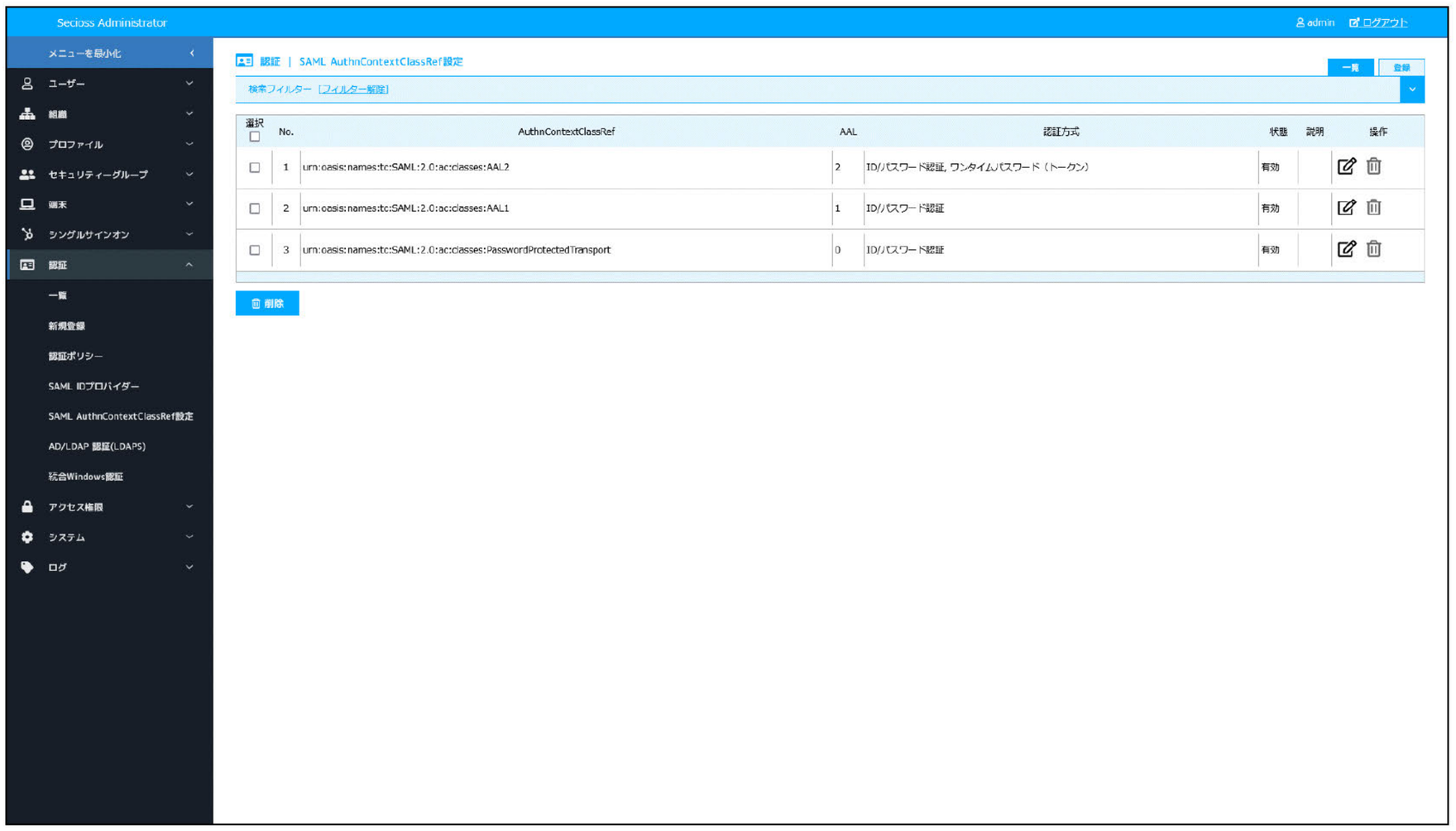
[redacted]

■一覧


Secioss Administrator
admin
ログアウト
メニューを最小化
ユーザー
組織
プロファイル
セキュリティーグループ
端末
シングルサインオン
認証
一覧
新規登録
認証ポリシー
SAML IDプロバイダー
SAML AuthnContextClassRef設定
AD/LDAP 認証(LDAPS)
統合Windows認証
アクセス権限
システム
ログ
認証 | SAML AuthnContextClassRef設定
一覧
登録
検索フィルター [フィルター解除]
選択
No.
AuthnContextClassRef
AAL
認証方式
状態
説明
操作
1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 2 ID/パスワード認証, ワンタイムパスワード（トークン） 有効
2 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 1 ID/パスワード認証 有効
3 urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport 0 ID/パスワード認証 有効
削除

| 区分 | 評価レポート |
|---|---|
| 試験No | 2 |
| 試験項目 | AAL2認証要求に対する基本動作 |
| 詳細 | SPが認証レベル「AAL2」を要求した場合、IdPはそれを満たす認証方式をクライアントに要求し、認証レベルを満たした場合のみ認証を完了とする基本的な動作を確認する。 |
| 期待する結果 | IdPはSPが要求する認証レベル「AAL2」を満たす認証方式をクライアントに要求し、認証が正常に完了した場合のみSPの利用ができること。 |

1. IdPで設定しているAuthnContextClassRefの設定




2. Shibboleth SP（SP01）で AuthnContextClassRefに”AAL2”を要求する設定

■設定追加

ファイル：/etc/httpd/conf.d/shib.conf

```
<Location /secure>
 AuthType shibboleth
 ShibRequestSetting requireSession 1

 # セキュリティレベルを追加（Secioss）
 ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
 # ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
 # ShibRequestSetting forceAuthn true
 # END セキュリティレベルを追加（Secioss）
 require shib-session
</Location>
```

設定追加

■設定反映

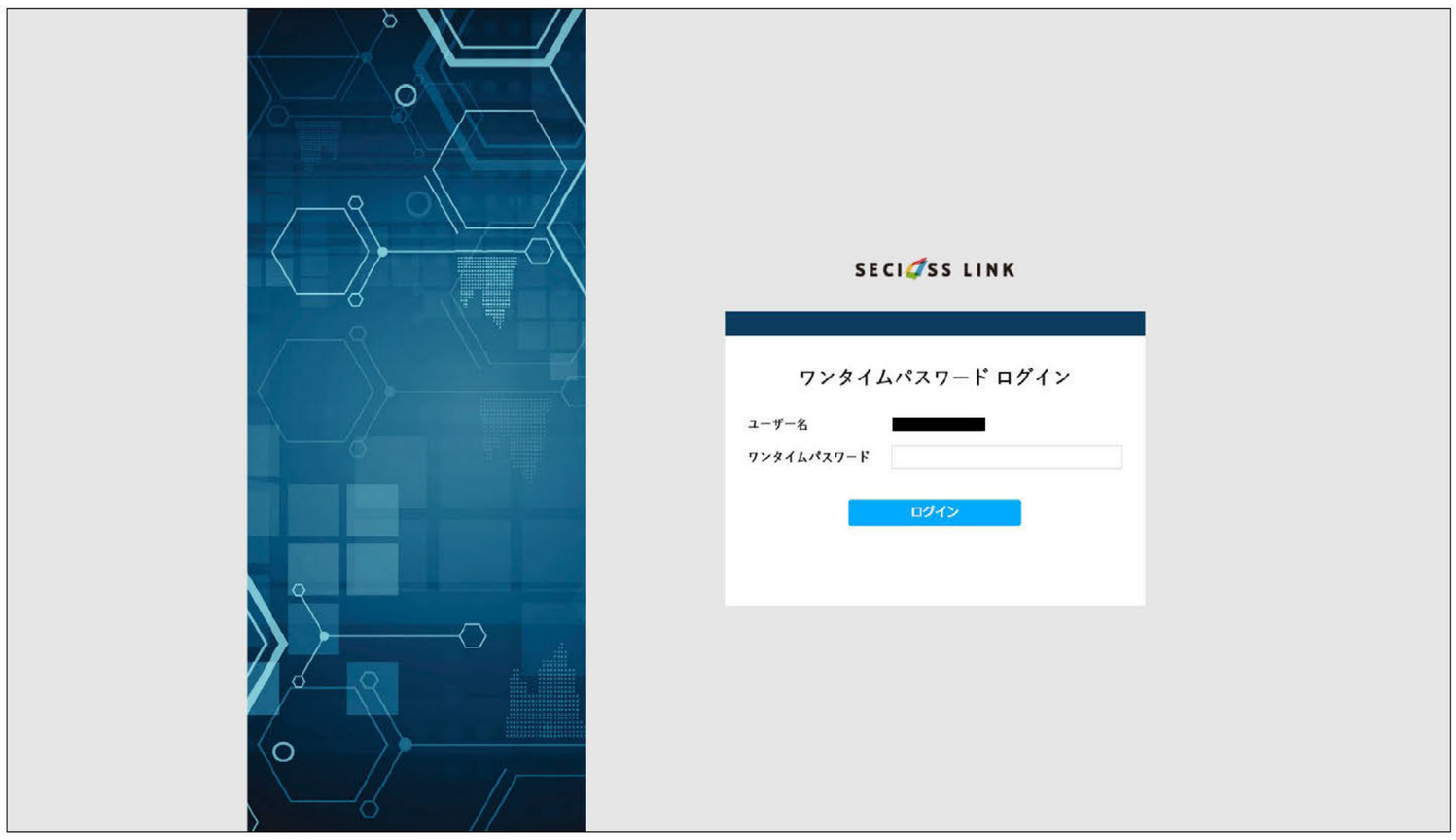
systemctl restart httpd

3. SP01にアクセスし、SAMLによるログインを行う。

IdP未認証状態で、「https://172.20.250.4/secure/index.php」 にブラウザでアクセスする。

IdPに遷移し、ID/パスワード認証認証が求められるため、認証を行う。

ID/パスワード認証後、ワンタイムパスワードが求められる。




すべての認証を成功したのち、SPへアクセスが行える。

基本情報

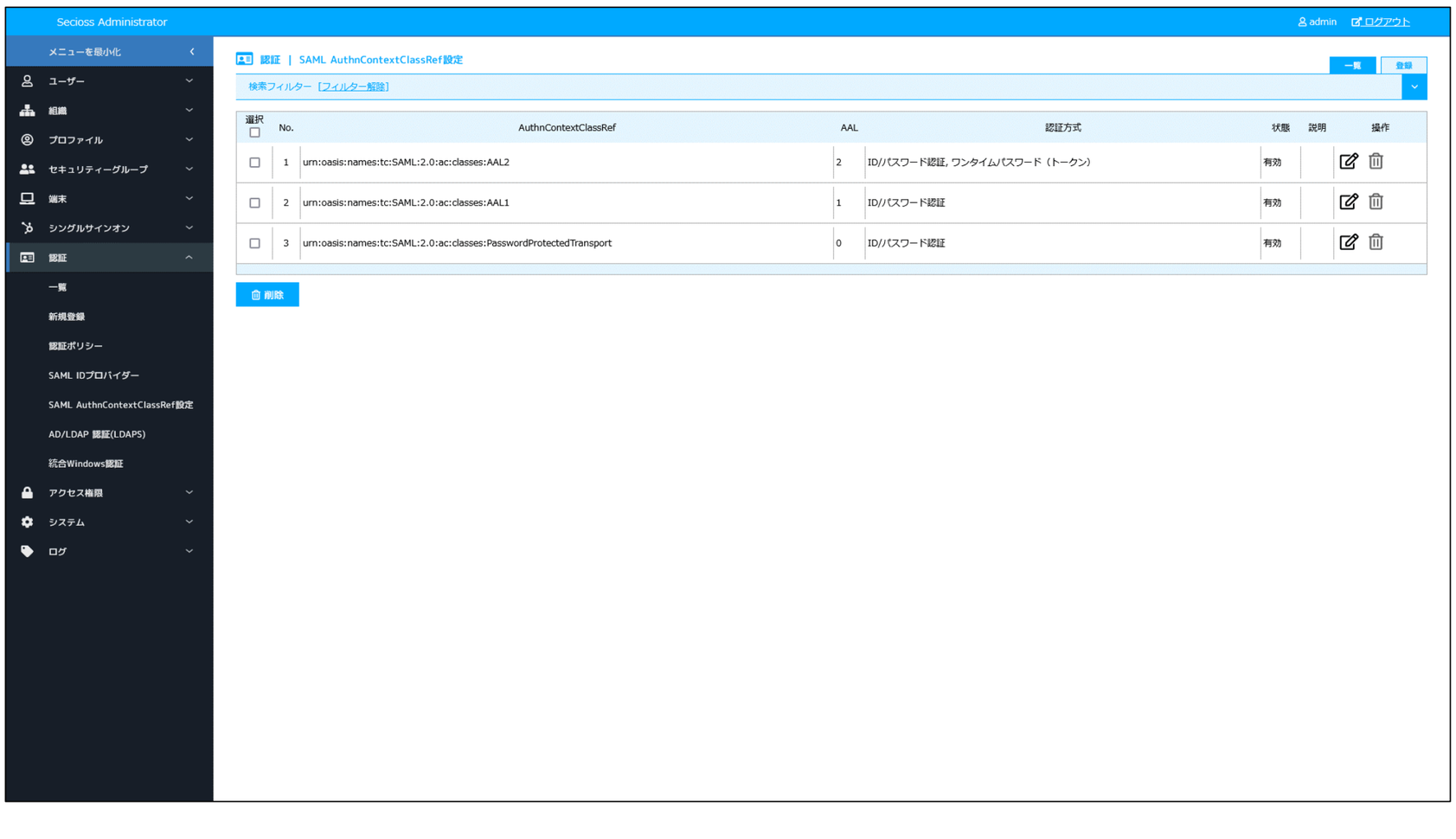
| | |
|---|---|
| SP | 172.[redacted]0.4 |
| ログインユーザー | [redacted] |
| 認証したIdP | https://authtest2.[redacted] |
| AuthnContext-Class | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Authentication-Method | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Error reporting | |

受信したSAML属性

| 属性 | 属性値 |
|---|---|
| ePPN(eduPersonPrincipalName) | NOT RECEIVED |
| eduPersonTargetedID | [redacted] |
| o(organizationName) | NOT RECEIVED |
| jao(jaOrganizationName)[日本語] | NOT RECEIVED |
| ou(organizationalUnitName) | NOT RECEIVED |
| jaou(jaOrganizationalUnitName)[日本語] | NOT RECEIVED |
| 職位(eduPersonAffiliation) | NOT RECEIVED |
| スコープ付き職位(eduPersonScopedAffiliation) | NOT RECEIVED |
| 権限(eduPersonEntitlement) | NOT RECEIVED |
| メールアドレス(mail) | [redacted] |
| 名(givenName) | NOT RECEIVED |
| 名(jaGivenName)[日本語] | [redacted] |
| 姓(sn) | NOT RECEIVED |
| 姓(jasn)[日本語] | [redacted] |
| 表示名(displayName) | NOT RECEIVED |
| 表示名(jaDisplayName)[日本語] | NOT RECEIVED |
| gakuninScopedPersonalUniqueCode | NOT RECEIVED |
| isMemberOf | NOT RECEIVED |
| eduPersonAssurance | NOT RECEIVED |
| eduPersonUniqueId | NOT RECEIVED |

| 区分 | 評価レポート |
|---|---|
| 試験No | 3 |
| 試験項目 | AAL1認証後のAAL2認証要求における昇格動作 |
| 詳細 | 認証レベル「AAL1」を要求していたSPが認証レベル「AAL2」に変更された場合（SPの認証レベル昇格）、次回アクセス時にはクライアントに「AAL2」を満たす認証方式を要求する動作となるか確認する。 |
| 期待する結果 | 認証レベルが「AAL1」から「AAL2」に変更された場合でも、クライアントには認証レベルに合わせた認証を要求すること。ただし認証セッションが継続している場合にはIdPへのリダイレクトが発生しないため、ログオフやSP/IdP側で一度、認証セッションを破棄するような操作が必要になる点に留意すること。 |

1. IdPで設定しているAuthnContextClassRefの設定




2. Shibboleth SP（SP01）で AuthnContextClassRefに”AAL1”を要求する設定

■設定追加

ファイル：/etc/httpd/conf.d/shib.conf

```
<Location /secure>
  AuthType shibboleth
  ShibRequestSetting requireSession 1

  # セキュリティレベルを追加（Secioss）
  ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1"
  # ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
  # ShibRequestSetting forceAuthn true
  # END セキュリティレベルを追加（Secioss）
  require shib-session
</Location>
```

設定追加

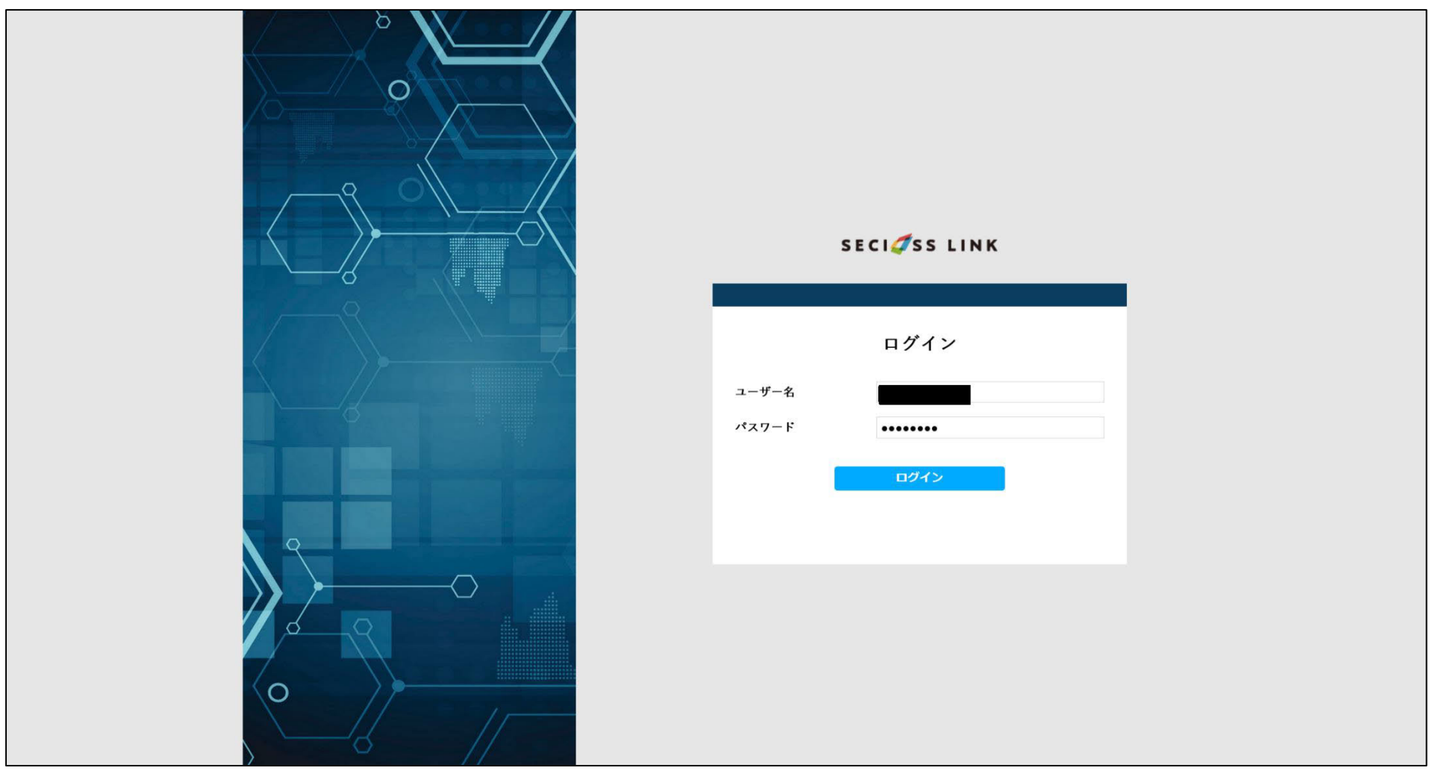
■設定反映

systemctl restart httpd

3. SP01にアクセスし、SAMLによるログインを行う。

IdP未認証状態で、「https://172.20.250.4/secure/index.php」 にブラウザでアクセスする。

IdPに遷移し、ID/パスワード認証認証が求められるため、認証を行う。




すべての認証を成功したのち、SPへアクセスが行える。

**基本情報**

| | |
|---|---|
| SP | 172.[redacted]4 |
| ログインユーザー | [redacted] |
| 認証したIdP | https://authtest2.[redacted] |
| AuthnContext-Class | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 |
| Authentication-Method | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 |
| Error reporting | |

**受信したSAML属性**

| 属性 | 属性値 |
|---|---|
| ePPN(eduPersonPrincipalName) | NOT RECEIVED |
| eduPersonTargetedID | [redacted] |
| o(organizationName) | NOT RECEIVED |
| jao(jaOrganizationName)[日本語] | NOT RECEIVED |
| ou(organizationalUnitName) | NOT RECEIVED |
| jaou(jaOrganizationalUnitName)[日本語] | NOT RECEIVED |
| 職位(eduPersonAffiliation) | NOT RECEIVED |
| スコープ付き職位(eduPersonScopedAffiliation) | NOT RECEIVED |
| 権限(eduPersonEntitlement) | NOT RECEIVED |
| メールアドレス(mail) | [redacted] |
| 名(givenName) | NOT RECEIVED |
| 名(jaGivenName)[日本語] | [redacted] |
| 姓(sn) | NOT RECEIVED |
| 姓(jasn)[日本語] | [redacted] |
| 表示名(displayName) | NOT RECEIVED |
| 表示名(jaDisplayName)[日本語] | NOT RECEIVED |
| gakuninScopedPersonalUniqueCode | NOT RECEIVED |
| isMemberOf | NOT RECEIVED |
| eduPersonAssurance | NOT RECEIVED |
| eduPersonUniqueId | NOT RECEIVED |

4. Shibboleth SP（SP01）で AuthnContextClassRefに”AAL2”を要求する設定

■設定追加

ファイル：/etc/httpd/conf.d/shib.conf

```
<Location /secure>
  AuthType shibboleth
  ShibRequestSetting requireSession 1

  # セキュリティレベルを追加（Secioss）
  ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
  # ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
  # ShibRequestSetting forceAuthn true
  # END セキュリティレベルを追加（Secioss）
  require shib-session
</Location>
```

設定追加

■設定反映

systemctl restart httpd

※この変更を行った時点では、認証済みのセッションは変更前のAAL1の認証状態でアクセスを継続できる。

5. SP01のセッション切れ後に再度アクセスし、SAMLによるログインを行う。

IdP認証済み（AAL1）の状態で、「https://172.20.250.4/secure/index.php」 にブラウザでアクセスする。

IdPに遷移し、ワンタイムパスワード認証が求められるため、認証を行う。


ワンタイムパスワード認証が成功すると、SPにアクセスする。

この時、SPへ渡ってきたAuthnContextClassRefはAAL2となる。

**基本情報**

| | |
|---|---|
| SP | 172.[redacted].4 |
| ログインユーザー | [redacted] |
| 認証したIdP | https://authtest2[redacted] |
| AuthnContext-Class | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Authentication-Method | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Error reporting | |

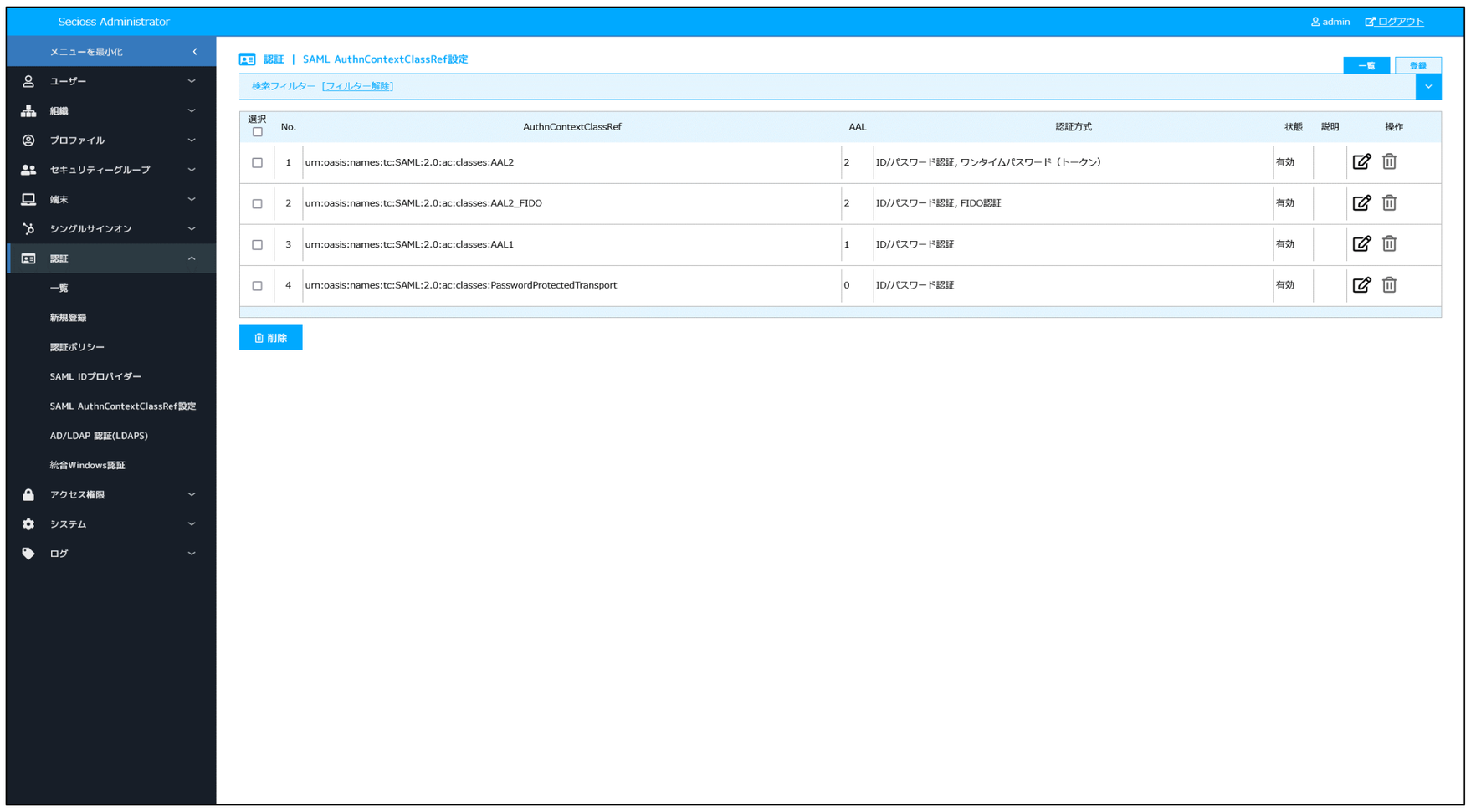
**受信したSAML属性**

| 属性 | 属性値 |
|---|---|
| ePPN(eduPersonPrincipalName) | NOT RECEIVED |
| eduPersonTargetedID | [redacted] |
| o(organizationName) | NOT RECEIVED |
| jao(jaOrganizationName)[日本語] | NOT RECEIVED |

| | |
|---|---|
| ou(organizationalUnitName) | NOT RECEIVED |
| jaou(jaOrganizationalUnitName)[日本語] | NOT RECEIVED |
| 職位(eduPersonAffiliation) | NOT RECEIVED |
| スコープ付き職位(eduPersonScopedAffiliation) | NOT RECEIVED |
| 権限(eduPersonEntitlement) | NOT RECEIVED |
| メールアドレス(mail) | [redacted] |
| 名(givenName) | NOT RECEIVED |
| 名(jaGivenName)[日本語] | [redacted] |
| 姓(sn) | NOT RECEIVED |
| 姓(jasn)[日本語] | [redacted] |
| 表示名(displayName) | NOT RECEIVED |
| 表示名(jaDisplayName)[日本語] | NOT RECEIVED |
| gakuninScopedPersonalUniqueCode | NOT RECEIVED |
| isMemberOf | NOT RECEIVED |
| eduPersonAssurance | NOT RECEIVED |
| eduPersonUniqueId | NOT RECEIVED |

| 区分 | 評価レポート |
|---|---|
| 試験No | 4 |
| 試験項目 | 異なるSP間でのSSOにおける基本動作（AAL2→AAL2） |
| 詳細 | SSO環境下で2つのSPが以下の認証レベルを要求する場合、クライアントがSP間の移動を行う際に必要に応じて追加の認証が求められる、或いは求められないことを確認する。<br>SP①の認証レベル：AAL2<br>SP②の認証レベル：AAL2 |
| 期待する結果 | SP間で認証レベルが同一の場合、基本的には追加で認証を求められないこと。ただしSP1とSP2で求める認証方式が異なる場合には実施していない認証方式が求められること。 |

1. IdPで設定しているAuthnContextClassRefの設定
   AAL2の要求として、AAL2_FIDOを追加。



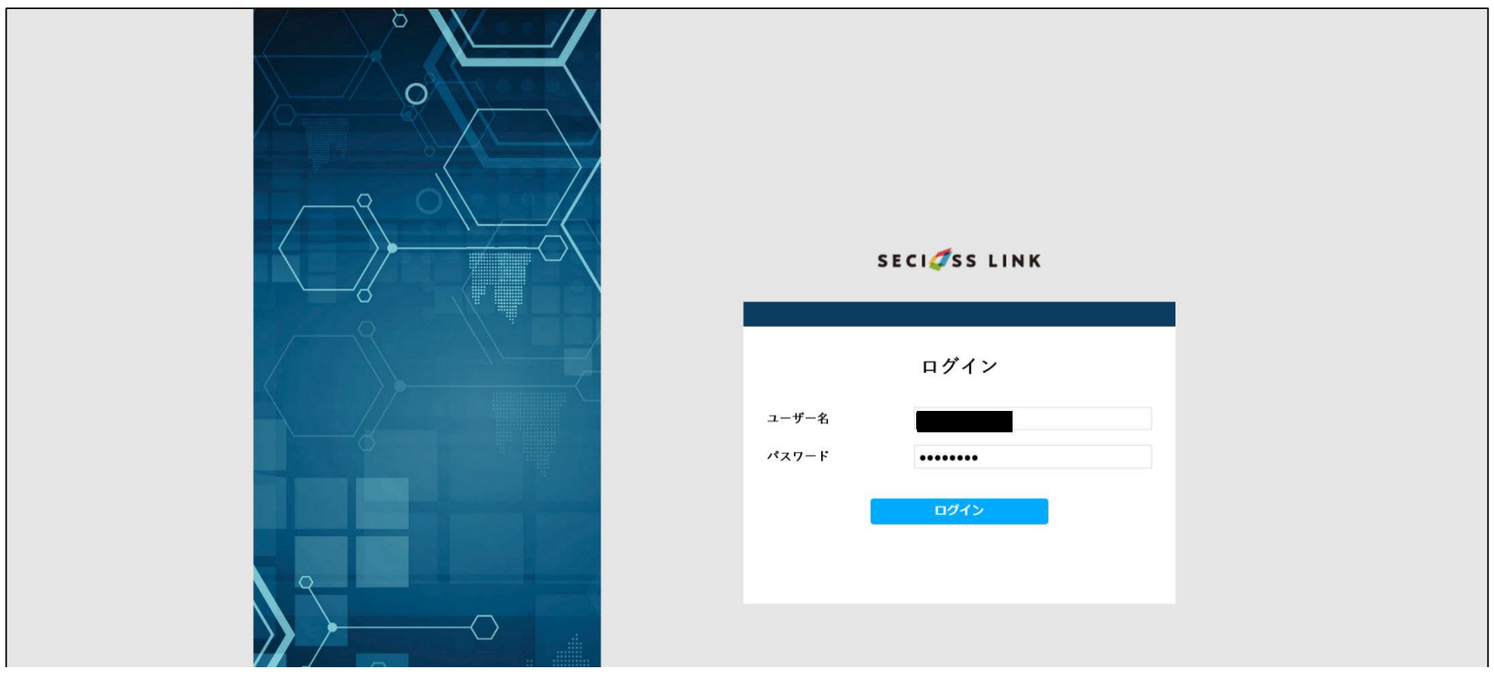

2. Shibboleth SP（SP01）で AuthnContextClassRefに”AAL2”を要求する設定
   ■設定追加
   ファイル：/etc/httpd/conf.d/shib.conf

```
<Location /secure>
 AuthType shibboleth
 ShibRequestSetting requireSession 1

 # セキュリティレベルを追加（Secioss）
 ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
 # ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
 # ShibRequestSetting forceAuthn true
 # END セキュリティレベルを追加（Secioss）
 require shib-session
</Location>
```

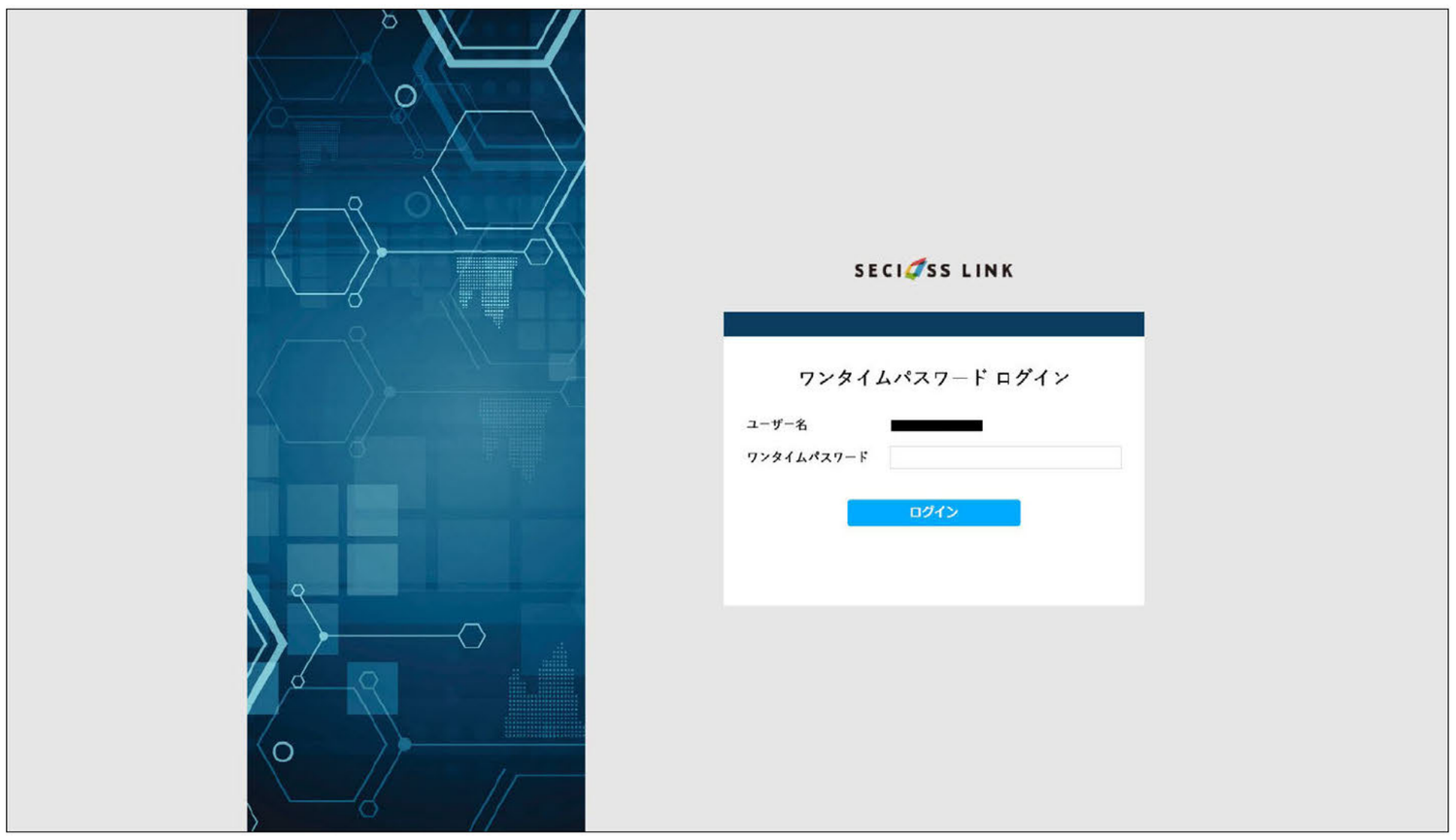
設定追加

   ■設定反映
   systemctl restart httpd

3. SP01にアクセスし、SAMLによるログインを行う。
   IdP未認証状態で、「https://172.20.250.4/secure/index.php」 にブラウザでアクセスする。
   IdPに遷移し、ID/パスワード認証認証が求められるため、認証を行う。



ID/パスワード認証後、ワンタイムパスワードが求められる。




すべての認証を成功したのち、SPへアクセスが行える。

基本情報

| | |
|---|---|
| SP | 172.20.250.4 |
| ログインユーザー | [redacted] |
| 認証したIdP | https://authtest2.[redacted] |
| AuthnContext-Class | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Authentication-Method | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Error reporting | |

受信したSAML属性

| 属性 | 属性値 |
|---|---|
| ePPN(eduPersonPrincipalName) | NOT RECEIVED |
| eduPersonTargetedID | [redacted] |
| o(organizationName) | NOT RECEIVED |
| jao(jaOrganizationName)[日本語] | NOT RECEIVED |
| ou(organizationalUnitName) | NOT RECEIVED |
| jaou(jaOrganizationalUnitName)[日本語] | NOT RECEIVED |
| 職位(eduPersonAffiliation) | NOT RECEIVED |
| スコープ付き職位(eduPersonScopedAffiliation) | NOT RECEIVED |
| 権限(eduPersonEntitlement) | NOT RECEIVED |
| メールアドレス(mail) | [redacted] |
| 名(givenName) | NOT RECEIVED |
| 名(jaGivenName)[日本語] | [redacted] |
| 姓(sn) | NOT RECEIVED |
| 姓(jasn)[日本語] | [redacted] |
| 表示名(displayName) | NOT RECEIVED |
| 表示名(jaDisplayName)[日本語] | NOT RECEIVED |
| gakuninScopedPersonalUniqueCode | NOT RECEIVED |
| isMemberOf | NOT RECEIVED |
| eduPersonAssurance | NOT RECEIVED |
| eduPersonUniqueId | NOT RECEIVED |

4. Shibboleth SP（SP02）で AuthnContextClassRefに”AAL2”を要求する設定

■設定追加

ファイル：/etc/httpd/conf.d/shib.conf

```
<Location /secure>
 AuthType shibboleth
 ShibRequestSetting requireSession 1

 # セキュリティレベルを追加（Secioss）
 ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
 # ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
 # ShibRequestSetting forceAuthn true
 # END セキュリティレベルを追加（Secioss）
 require shib-session
</Location>
```

設定追加

■設定反映

systemctl restart httpd

5. SP02にアクセスし、SAMLによるログインを行う。
   IdP認証済み（SP01アクセス時にAAL2の認証済み）の状態で、「https://172.20.249.4/secure/index.php」 にブラウザでアクセスする。
   SP01アクセス時にAAL2の認証をすでに行っているため、SP02へアクセスが行える。

基本情報

| | |
|---|---|
| SP | 172.20.249.4 |
| ログインユーザー | [redacted] |
| 認証したIdP | https://authtest2[redacted] |
| AuthnContext-Class | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Authentication-Method | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Error reporting | |

受信したSAML属性

| 属性 | 属性値 |
|---|---|
| ePPN(eduPersonPrincipalName) | NOT RECEIVED |
| eduPersonTargetedID | [redacted] |
| o(organizationName) | NOT RECEIVED |
| jao(jaOrganizationName)[日本語] | NOT RECEIVED |
| ou(organizationalUnitName) | NOT RECEIVED |
| jaou(jaOrganizationalUnitName)[日本語] | NOT RECEIVED |
| 職位(eduPersonAffiliation) | NOT RECEIVED |
| スコープ付き職位(eduPersonScopedAffiliation) | NOT RECEIVED |
| 権限(eduPersonEntitlement) | NOT RECEIVED |
| メールアドレス(mail) | NOT RECEIVED |
| 名(givenName) | NOT RECEIVED |
| 名(jaGivenName)[日本語] | NOT RECEIVED |
| 姓(sn) | NOT RECEIVED |
| 姓(jasn)[日本語] | NOT RECEIVED |
| 表示名(displayName) | NOT RECEIVED |
| 表示名(jaDisplayName)[日本語] | NOT RECEIVED |
| gakuninScopedPersonalUniqueCode | NOT RECEIVED |
| isMemberOf | NOT RECEIVED |
| eduPersonAssurance | NOT RECEIVED |
| eduPersonUniqueId | NOT RECEIVED |

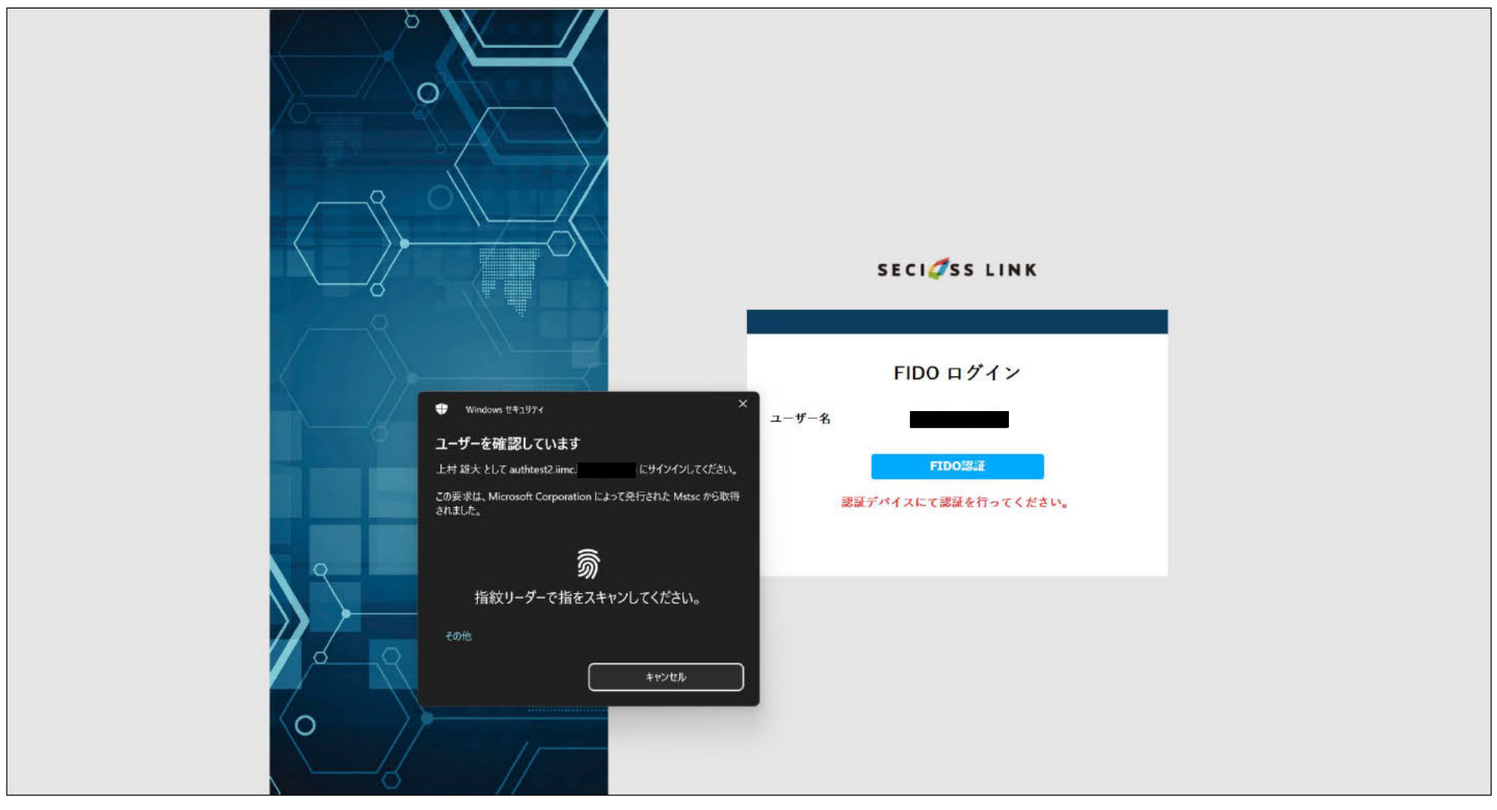
6. Shibboleth SP（SP02）で AuthnContextClassRefに”AAL2_FIDO”を要求する設定
   ■設定追加
   ファイル：/etc/httpd/conf.d/shib.conf

```
<Location /secure>
 AuthType shibboleth
 ShibRequestSetting requireSession 1

 # セキュリティレベルを追加（Secioss）
 ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2_FIDO"
 # ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
 # ShibRequestSetting forceAuthn true
 # END セキュリティレベルを追加（Secioss）
 require shib-session
</Location>
```

設定追加

   ■設定反映
   systemctl restart httpd

7. SP02で一度ログアウトを行い、再度SAMLでログインを行う
   SP02のログアウトを行う（https://172.20.249.4/Shibboleth.sso/Logout?return=https://172.20.249.4/へアクセス）
   IdP認証済み（SP01アクセス時にAAL2の認証済み）の状態で、「https://172.20.249.4/secure/index.php」 にブラウザでアクセスする。
   SP01アクセス時にAAL2の認証をすでに行っているため、ID/パスワード認証は求められず、FIDO認証が求められる。




すべての認証を成功したのち、SPへアクセスが行える。

基本情報

| | |
|---|---|
| SP | 172.20.249.4 |
| ログインユーザー | [redacted] |
| 認証したIdP | https://authtest2[redacted] |

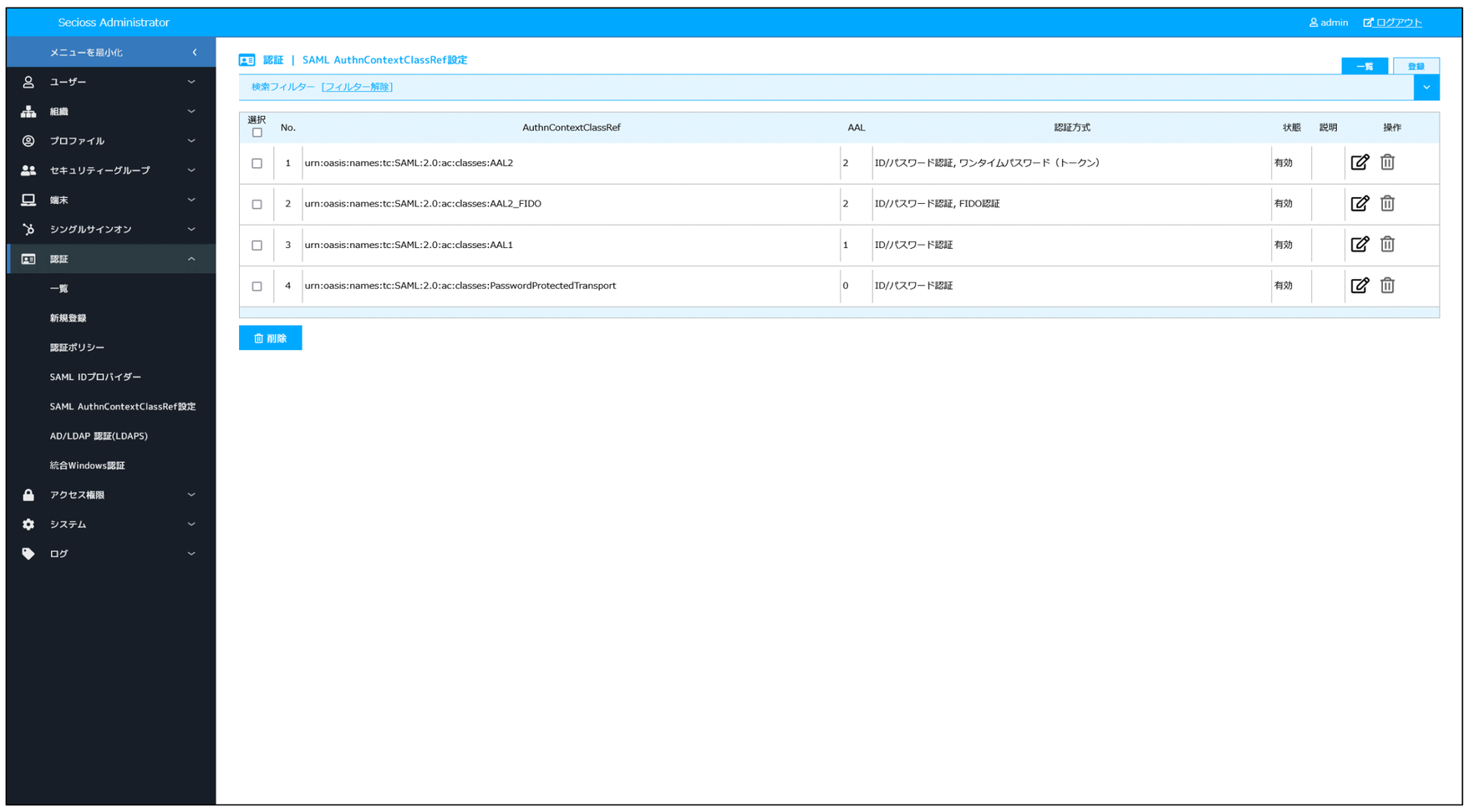
| | |
|---|---|
| AuthnContext-Class | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2_FIDO |
| Authentication-Method | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2_FIDO |
| Error reporting | |

受信したSAML属性

| 属性 | 属性値 |
|---|---|
| ePPN(eduPersonPrincipalName) | NOT RECEIVED |
| eduPersonTargetedID | [redacted] |
| o(organizationName) | NOT RECEIVED |
| jao(jaOrganizationName)[日本語] | NOT RECEIVED |
| ou(organizationalUnitName) | NOT RECEIVED |
| jaou(jaOrganizationalUnitName)[日本語] | NOT RECEIVED |
| 職位(eduPersonAffiliation) | NOT RECEIVED |
| スコープ付き職位(eduPersonScopedAffiliation) | NOT RECEIVED |
| 権限(eduPersonEntitlement) | NOT RECEIVED |
| メールアドレス(mail) | NOT RECEIVED |
| 名(givenName) | NOT RECEIVED |
| 名(jaGivenName)[日本語] | NOT RECEIVED |
| 姓(sn) | NOT RECEIVED |
| 姓(jasn)[日本語] | NOT RECEIVED |
| 表示名(displayName) | NOT RECEIVED |
| 表示名(jaDisplayName)[日本語] | NOT RECEIVED |
| gakuninScopedPersonalUniqueCode | NOT RECEIVED |
| isMemberOf | NOT RECEIVED |
| eduPersonAssurance | NOT RECEIVED |
| eduPersonUniqueId | NOT RECEIVED |

| 区分 | 評価レポート |
|---|---|
| 試験No | 5 |
| 試験項目 | 異なるSP間でのSSOにおける降格動作（AAL2→AAL1） |
| 詳細 | SSO環境下で2つのSPが以下の認証レベルを要求する場合、クライアントがSP間の移動を行う際に必要に応じて追加の認証が求められる、或いは求められないことを確認する。<br>SP①の認証レベル：AAL2<br>SP②の認証レベル：AAL2からAAL1に降格 |
| 期待する結果 | 認証レベルが「AAL2」から「AAL1」に降格した場合、基本的には追加で認証を求められないこと。ただし、変更されたレベルで要求される認証方式を実施していない場合、追加で認証が求められること。 |

1. IdPで設定しているAuthnContextClassRefの設定




2. Shibboleth SP（SP01）で AuthnContextClassRefに”AAL2”を要求する設定

■設定追加

ファイル：/etc/httpd/conf.d/shib.conf

```
<Location /secure>
  AuthType shibboleth
  ShibRequestSetting requireSession 1

  # セキュリティレベルを追加（Secioss）
  ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
  # ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
  # ShibRequestSetting forceAuthn true
  # END セキュリティレベルを追加（Secioss）
  require shib-session
</Location>
```

設定追加

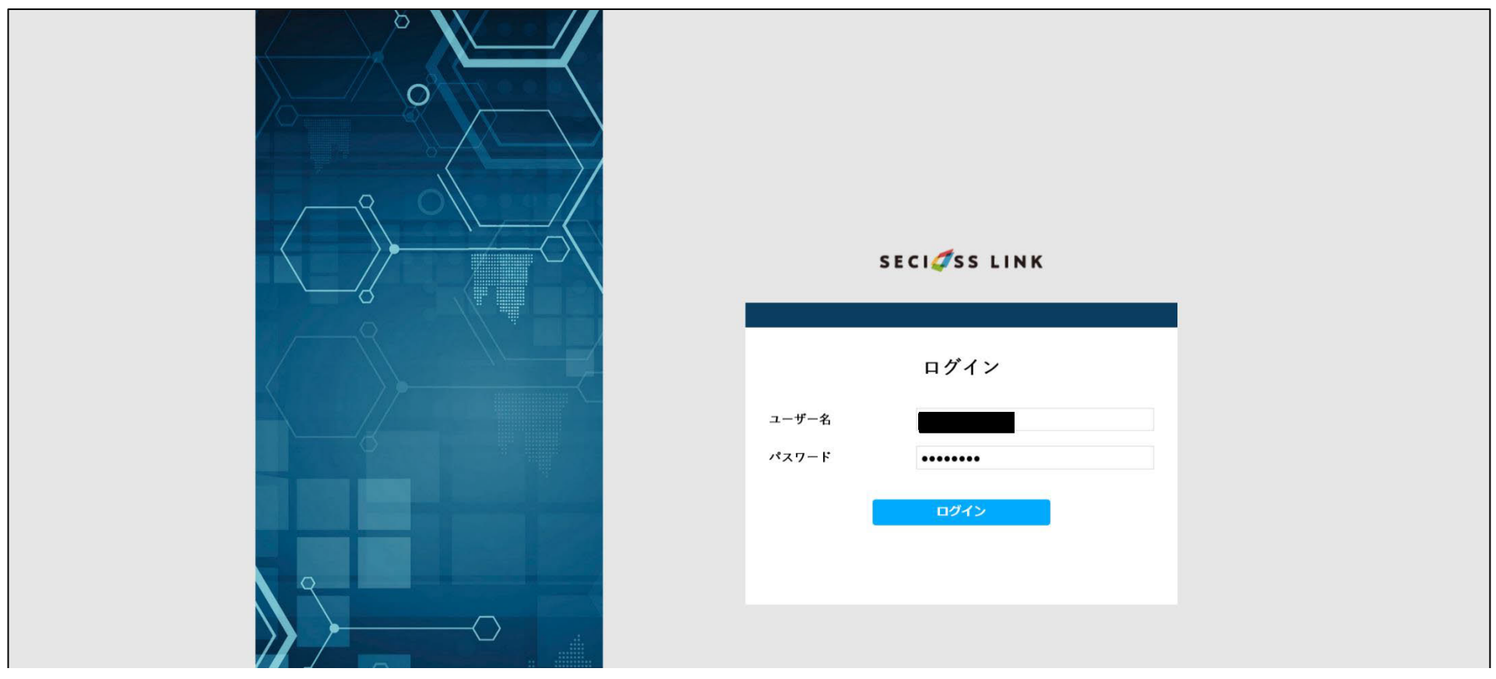
■設定反映

systemctl restart httpd

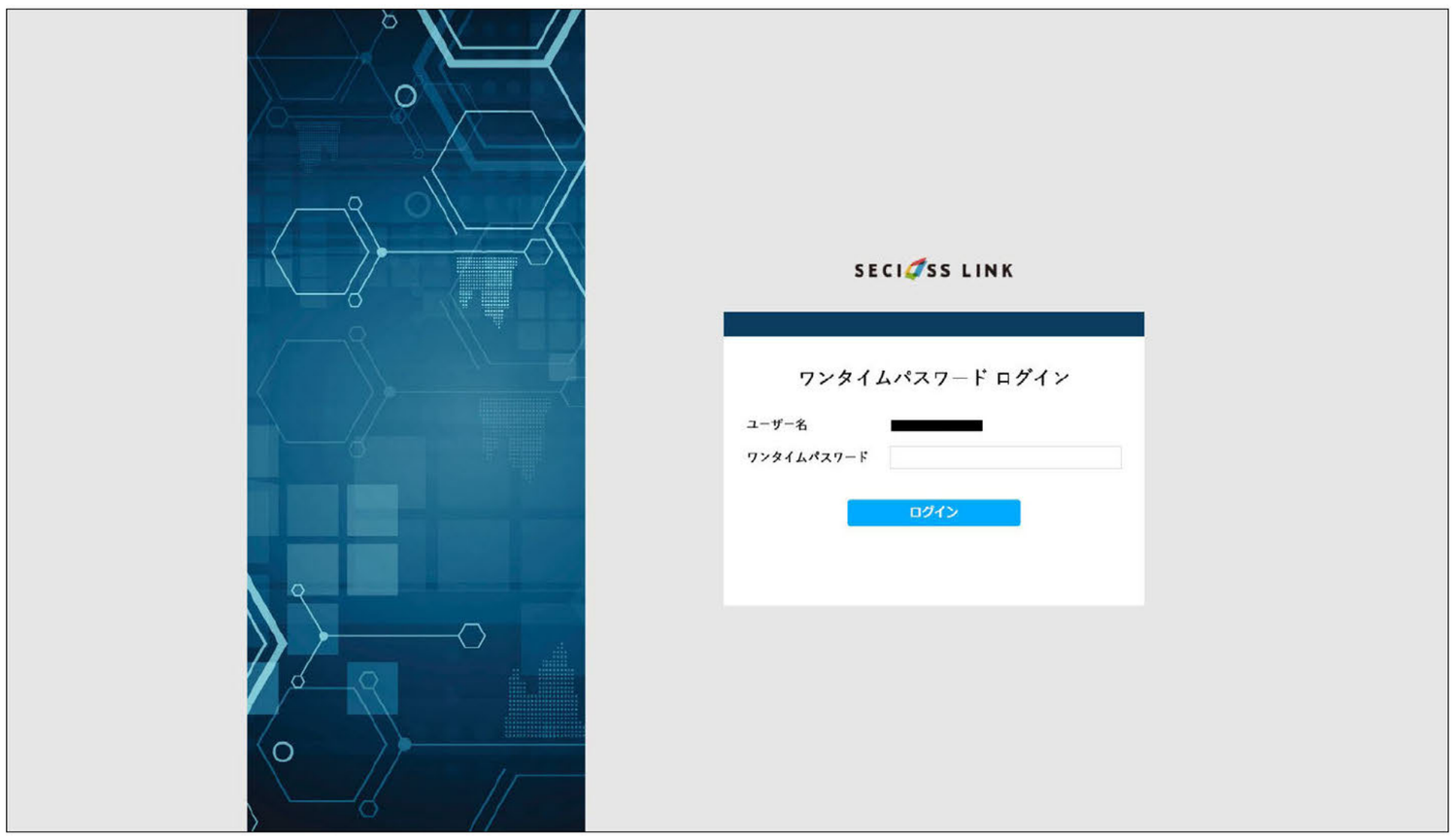
3. SP01にアクセスし、SAMLによるログインを行う。

IdP未認証状態で、「https://172.20.250.4/secure/index.php」 にブラウザでアクセスする。

IdPに遷移し、ID/パスワード認証認証が求められるため、認証を行う。



ID/パスワード認証後、ワンタイムパスワードが求められる。




すべての認証を成功したのち、SPへアクセスが行える。

基本情報

| | |
|---|---|
| SP | 172.20.250.4 |
| ログインユーザー | [redacted] |
| 認証したIdP | https://authtest2.[redacted] |
| AuthnContext-Class | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Authentication-Method | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Error reporting | |

受信したSAML属性

| 属性 | 属性値 |
|---|---|
| ePPN(eduPersonPrincipalName) | NOT RECEIVED |
| eduPersonTargetedID | [redacted] |
| o(organizationName) | NOT RECEIVED |
| jao(jaOrganizationName)[日本語] | NOT RECEIVED |
| ou(organizationalUnitName) | NOT RECEIVED |
| jaou(jaOrganizationalUnitName)[日本語] | NOT RECEIVED |
| 職位(eduPersonAffiliation) | NOT RECEIVED |
| スコープ付き職位(eduPersonScopedAffiliation) | NOT RECEIVED |
| 権限(eduPersonEntitlement) | NOT RECEIVED |
| メールアドレス(mail) | [redacted] |
| 名(givenName) | NOT RECEIVED |
| 名(jaGivenName)[日本語] | [redacted] |
| 姓(sn) | NOT RECEIVED |
| 姓(jasn)[日本語] | [redacted] |
| 表示名(displayName) | NOT RECEIVED |
| 表示名(jaDisplayName)[日本語] | NOT RECEIVED |
| gakuninScopedPersonalUniqueCode | NOT RECEIVED |
| isMemberOf | NOT RECEIVED |
| eduPersonAssurance | NOT RECEIVED |
| eduPersonUniqueId | NOT RECEIVED |

4. Shibboleth SP（SP02）で AuthnContextClassRefに”AAL2”を要求する設定

■設定追加

ファイル：/etc/httpd/conf.d/shib.conf

```
<Location /secure>
 AuthType shibboleth
 ShibRequestSetting requireSession 1

 # セキュリティレベルを追加（Secioss）
 ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
 # ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
 # ShibRequestSetting forceAuthn true
 # END セキュリティレベルを追加（Secioss）
 require shib-session
</Location>
```

設定追加

■設定反映

systemctl restart httpd

5. SP02にアクセスし、SAMLによるログインを行う。
   IdP認証済み（SP01アクセス時にAAL2の認証済み）の状態で、「https://172.20.249.4/secure/index.php」 にブラウザでアクセスする。
   SP01アクセス時にAAL2の認証をすでに行っているため、SP02へアクセスが行える。

**基本情報**

| | |
|---|---|
| SP | 172.20.249.4 |
| ログインユーザー | [redacted] |
| 認証したIdP | https://authtest2[redacted] |
| AuthnContext-Class | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Authentication-Method | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Error reporting | |

**受信したSAML属性**

| 属性 | 属性値 |
|---|---|
| ePPN(eduPersonPrincipalName) | NOT RECEIVED |
| eduPersonTargetedID | [redacted] |
| o(organizationName) | NOT RECEIVED |
| jao(jaOrganizationName)[日本語] | NOT RECEIVED |
| ou(organizationalUnitName) | NOT RECEIVED |
| jaou(jaOrganizationalUnitName)[日本語] | NOT RECEIVED |
| 職位(eduPersonAffiliation) | NOT RECEIVED |
| スコープ付き職位(eduPersonScopedAffiliation) | NOT RECEIVED |
| 権限(eduPersonEntitlement) | NOT RECEIVED |
| メールアドレス(mail) | NOT RECEIVED |
| 名(givenName) | NOT RECEIVED |
| 名(jaGivenName)[日本語] | NOT RECEIVED |
| 姓(sn) | NOT RECEIVED |
| 姓(jasn)[日本語] | NOT RECEIVED |
| 表示名(displayName) | NOT RECEIVED |
| 表示名(jaDisplayName)[日本語] | NOT RECEIVED |
| gakuninScopedPersonalUniqueCode | NOT RECEIVED |
| isMemberOf | NOT RECEIVED |
| eduPersonAssurance | NOT RECEIVED |
| eduPersonUniqueId | NOT RECEIVED |

6. Shibboleth SP（SP02）で AuthnContextClassRefに”AAL1”を要求する設定
   ■設定追加
   ファイル：/etc/httpd/conf.d/shib.conf

```
<Location /secure>
  AuthType shibboleth
  ShibRequestSetting requireSession 1

  # セキュリティレベルを追加（Secioss）
  ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1"
  # ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
  # ShibRequestSetting forceAuthn true
  # END セキュリティレベルを追加（Secioss）
  require shib-session
</Location>
```

設定追加

   ■設定反映
   systemctl restart httpd

7. SP02で一度ログアウトを行い、再度SAMLでログインを行う
   SP02のログアウトを行う（https://172.20.249.4/Shibboleth.sso/Logout?return=https://172.20.249.4/へアクセス）
   IdP認証済み（SP01,SP02アクセス時にAAL2の認証済み）の状態で、「https://172.20.249.4/secure/index.php」 にブラウザでアクセスする。
   SP02へのAAL1（ID/パスワード認証）要求に対して認証が求められず、アクセスが行える。

**基本情報**

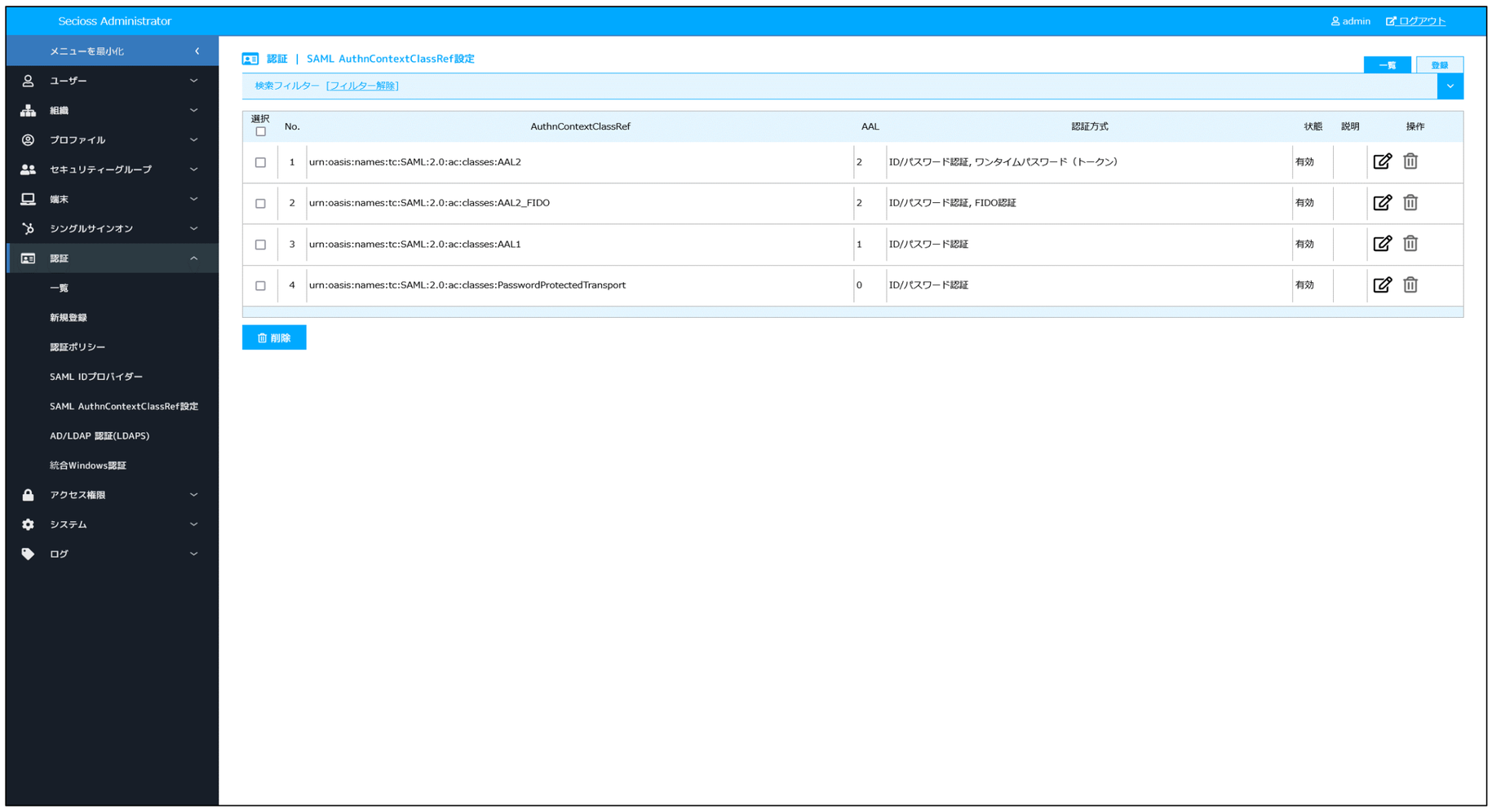
| | |
|---|---|
| SP | 172.20.249.4 |
| ログインユーザー | [redacted] |
| 認証したIdP | https://authtest2[redacted] |
| AuthnContext-Class | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 |
| Authentication-Method | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 |
| Error reporting | |

**受信したSAML属性**

| 属性 | 属性値 |
|---|---|
| ePPN(eduPersonPrincipalName) | NOT RECEIVED |
| eduPersonTargetedID | [redacted] |
| o(organizationName) | NOT RECEIVED |
| jao(jaOrganizationName)[日本語] | NOT RECEIVED |
| ou(organizationalUnitName) | NOT RECEIVED |
| jaou(jaOrganizationalUnitName)[日本語] | NOT RECEIVED |
| 職位(eduPersonAffiliation) | NOT RECEIVED |
| スコープ付き職位(eduPersonScopedAffiliation) | NOT RECEIVED |
| 権限(eduPersonEntitlement) | NOT RECEIVED |
| メールアドレス(mail) | NOT RECEIVED |
| 名(givenName) | NOT RECEIVED |
| 名(jaGivenName)[日本語] | NOT RECEIVED |
| 姓(sn) | NOT RECEIVED |
| 姓(jasn)[日本語] | NOT RECEIVED |
| 表示名(displayName) | NOT RECEIVED |
| 表示名(jaDisplayName)[日本語] | NOT RECEIVED |
| gakuninScopedPersonalUniqueCode | NOT RECEIVED |
| isMemberOf | NOT RECEIVED |
| eduPersonAssurance | NOT RECEIVED |
| eduPersonUniqueId | NOT RECEIVED |

| 区分 | 評価レポート |
|---|---|
| 試験No | 6 |
| 試験項目 | 異なるSP間でのSSOにおける昇格動作 (AAL1→AAL2) |
| 詳細 | SSO環境下で2つのSPが以下の認証レベルを要求する場合、クライアントがSP間の移動を行う際に必要に応じて追加の認証が求められる、或いは求められないことを確認する。<br><br>SP①の認証レベル：AAL1<br>SP②の認証レベル：AAL1からAAL2に昇格 |
| 期待する結果 | 認証レベルが「AAL1」から「AAL2」に昇格した場合、基本的には追加で認証を求めること。ただし、認証レベルが変更されたSPが求める認証方式を他のSPの認証で既に実施済みの場合、追加で認証は求められないこと。 |

1. IdPで設定しているAuthnContextClassRefの設定




2. Shibboleth SP（SP01）で AuthnContextClassRefに”AAL1”を要求する設定

■設定追加

ファイル：/etc/httpd/conf.d/shib.conf

```
<Location /secure>
  AuthType shibboleth
  ShibRequestSetting requireSession 1

  # セキュリティレベルを追加（Secioss）
  ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1"
  # ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
  # ShibRequestSetting forceAuthn true
  # END セキュリティレベルを追加（Secioss）
  require shib-session
</Location>
```

設定追加

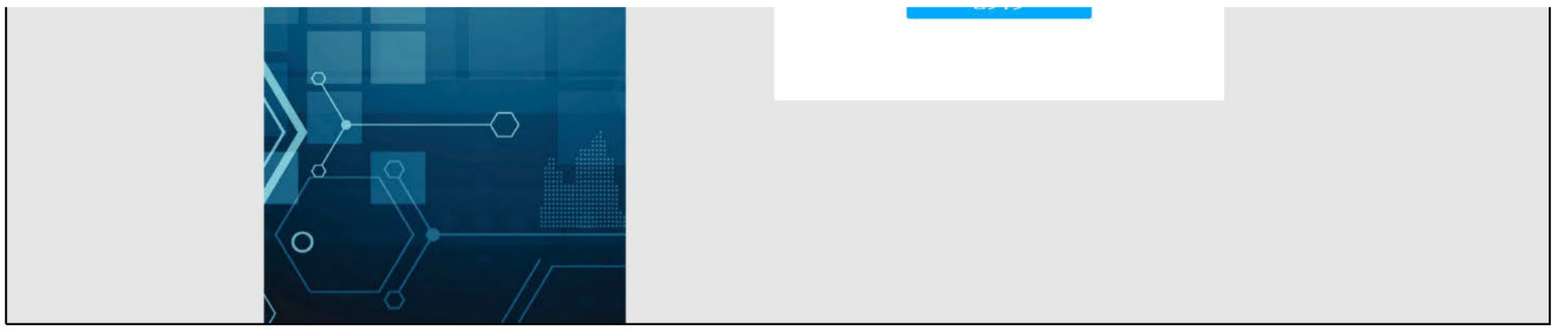
■設定反映

systemctl restart httpd

3. SP01にアクセスし、SAMLによるログインを行う。

IdP未認証状態で、「https://172.20.250.4/secure/index.php」 にブラウザでアクセスする。

IdPに遷移し、ID/パスワード認証認証が求められるため、認証を行う。



認証が成功したのち、SPへアクセスが行える。

基本情報

| | |
|---|---|
| SP | 172.20.250.4 |
| ログインユーザー | [redacted] |
| 認証したIdP | https://authtest[redacted] |
| AuthnContext-Class | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 |
| Authentication-Method | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 |
| Error reporting | |

受信したSAML属性

| 属性 | 属性他 |
|---|---|
| ePPN(eduPersonPrincipalName) | NOT RECEIVED |
| eduPersonTargetedID | [redacted] |
| o(organizationName) | NOT RECEIVED |
| jao(jaOrganizationName)[日本語] | NOT RECEIVED |
| ou(organizationalUnitName) | NOT RECEIVED |
| jaou(jaOrganizationalUnitName)[日本語] | NOT RECEIVED |
| 職位(eduPersonAffiliation) | NOT RECEIVED |
| スコープ付き職位(eduPersonScopedAffiliation) | NOT RECEIVED |
| 権限(eduPersonEntitlement) | NOT RECEIVED |
| メールアドレス(mail) | [redacted] |
| 名(givenName) | NOT RECEIVED |
| 名(jaGivenName)[日本語] | [redacted] |
| 姓(sn) | NOT RECEIVED |
| 姓(jasn)[日本語] | [redacted] |
| 表示名(displayName) | NOT RECEIVED |
| 表示名(jaDisplayName)[日本語] | NOT RECEIVED |
| gakuninScopedPersonalUniqueCode | NOT RECEIVED |
| isMemberOf | NOT RECEIVED |
| eduPersonAssurance | NOT RECEIVED |
| eduPersonUniqueId | NOT RECEIVED |

4. Shibboleth SP（SP02）で AuthnContextClassRefに”AAL1”を要求する設定

■設定追加

ファイル：/etc/httpd/conf.d/shib.conf

```
<Location /secure>
 AuthType shibboleth
 ShibRequestSetting requireSession 1

 # セキュリティレベルを追加（Secioss）
 ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1"
 # ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
 # ShibRequestSetting forceAuthn true
 # END セキュリティレベルを追加（Secioss）
 require shib-session
</Location>
```

設定追加

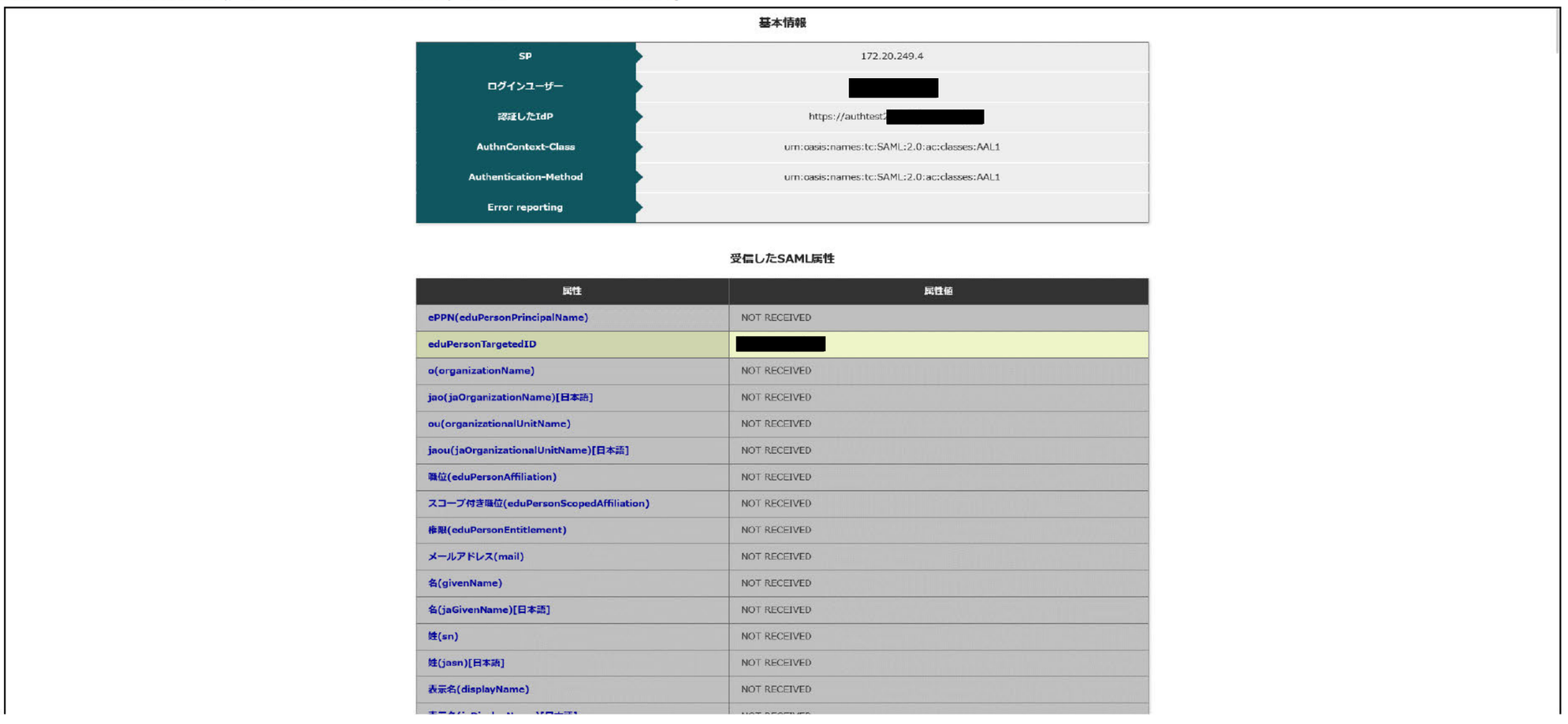
■設定反映

systemctl restart httpd

5. SP02にアクセスし、SAMLによるログインを行う。

IdP認証済み（SP01アクセス時にAAL1の認証済み）の状態で、「https://172.20.249.4/secure/index.php」 にブラウザでアクセスする。

SP01アクセス時にAAL1の認証をすでに行っているため、SP02へアクセスが行える。



基本情報

| | |
|---|---|
| SP | 172.20.249.4 |
| ログインユーザー | [redacted] |
| 認証したIdP | https://authtest2[redacted] |
| AuthnContext-Class | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 |
| Authentication-Method | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 |
| Error reporting | |

受信したSAML属性

| 属性 | 属性値 |
|---|---|
| ePPN(eduPersonPrincipalName) | NOT RECEIVED |
| eduPersonTargetedID | [redacted] |
| o(organizationName) | NOT RECEIVED |
| jao(jaOrganizationName)[日本語] | NOT RECEIVED |
| ou(organizationalUnitName) | NOT RECEIVED |
| jaou(jaOrganizationalUnitName)[日本語] | NOT RECEIVED |
| 職位(eduPersonAffiliation) | NOT RECEIVED |
| スコープ付き職位(eduPersonScopedAffiliation) | NOT RECEIVED |
| 権限(eduPersonEntitlement) | NOT RECEIVED |
| メールアドレス(mail) | NOT RECEIVED |
| 名(givenName) | NOT RECEIVED |
| 名(jaGivenName)[日本語] | NOT RECEIVED |
| 姓(sn) | NOT RECEIVED |
| 姓(jasn)[日本語] | NOT RECEIVED |
| 表示名(displayName) | NOT RECEIVED |

| | |
|---|---|
| 表示名(jaDisplayName)[日本語] | NOT RECEIVED |
| gakuninScopedPersonalUniqueCode | NOT RECEIVED |
| isMemberOf | NOT RECEIVED |
| eduPersonAssurance | NOT RECEIVED |
| eduPersonUniqueId | NOT RECEIVED |

6. Shibboleth SP（SP02）で AuthnContextClassRefに”AAL2”を要求する設定

■設定追加

ファイル：/etc/httpd/conf.d/shib.conf

```
<Location /secure>
 AuthType shibboleth
 ShibRequestSetting requireSession 1

 # セキュリティレベルを追加（Secioss）
 ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
 # ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
 # ShibRequestSetting forceAuthn true
 # END セキュリティレベルを追加（Secioss）
 require shib-session
</Location>
```

設定追加

■設定反映

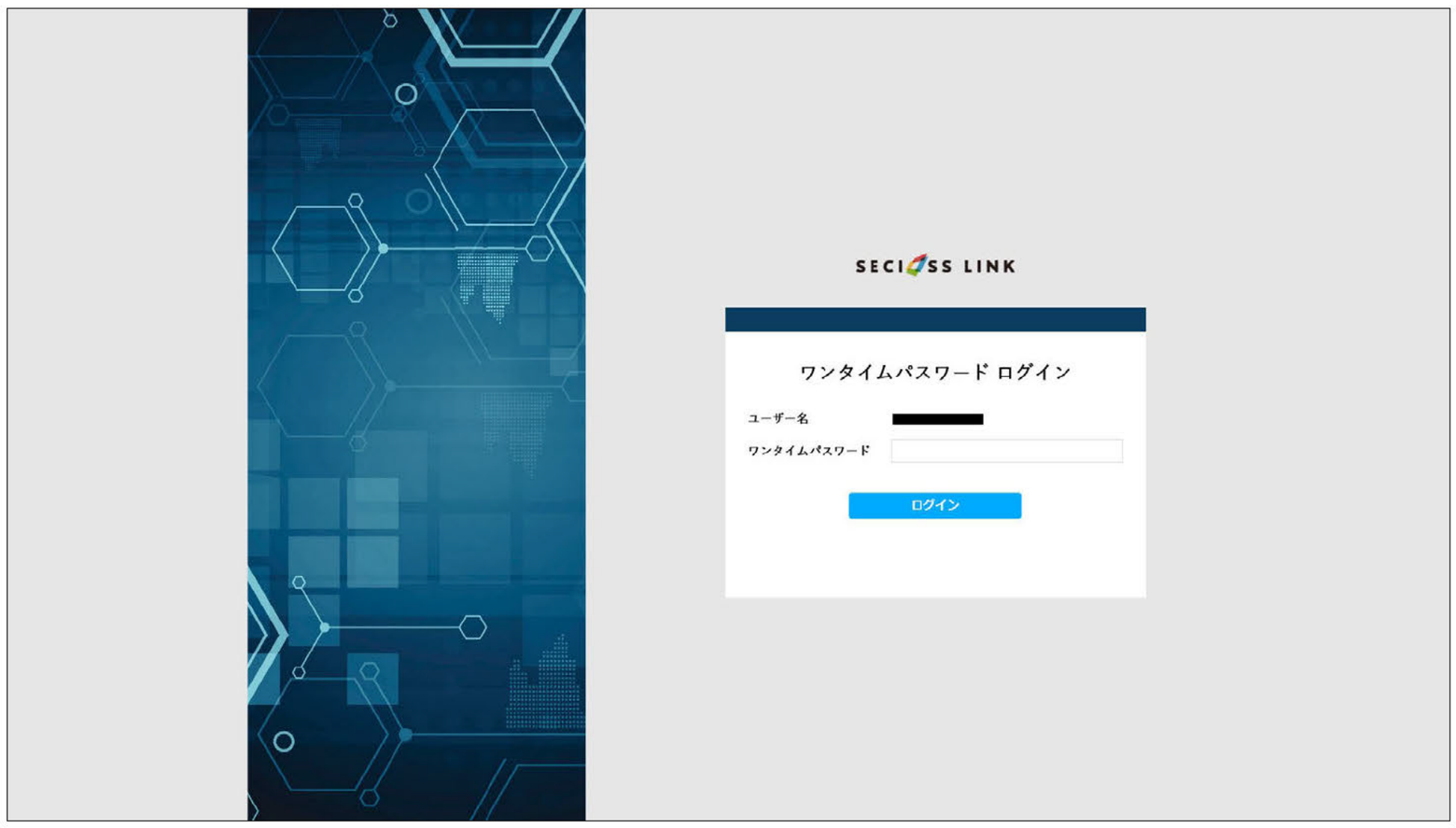
systemctl restart httpd

7. SP02で一度ログアウトを行い、再度SAMLでログインを行う

SP02のログアウトを行う（https://172.20.249.4/Shibboleth.sso/Logout?return=https://172.20.249.4/へアクセス）

IdP認証済み（SP01,SP02アクセス時にAAL1の認証済み）の状態で、「https://172.20.249.4/secure/index.php」 にブラウザでアクセスする。

SP02へのAAL2（ワンタイムパスワード認証）要求が行われる。




ワンタイムパスワード認証後、SPへアクセスが行われる。

基本情報

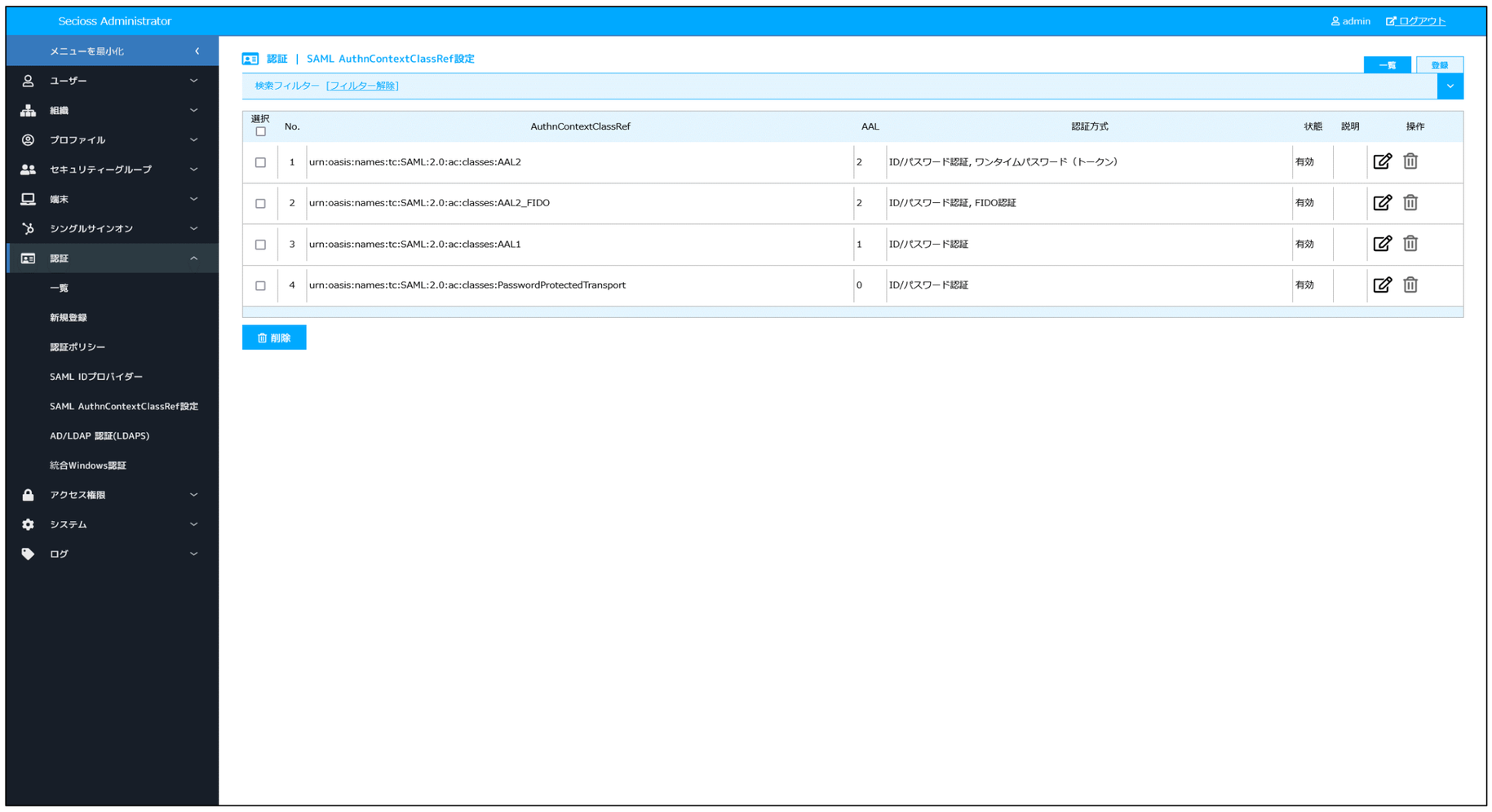
| | |
|---|---|
| SP | 172.20.249.4 |
| ログインユーザー | [redacted] |
| 認証したIdP | https://authtest2[redacted] |
| AuthnContext-Class | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Authentication-Method | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Error reporting | |

受信したSAML属性

| 属性 | 属性値 |
|---|---|
| ePPN(eduPersonPrincipalName) | NOT RECEIVED |
| eduPersonTargetedID | [redacted] |
| o(organizationName) | NOT RECEIVED |
| jao(jaOrganizationName)[日本語] | NOT RECEIVED |
| ou(organizationalUnitName) | NOT RECEIVED |
| jaou(jaOrganizationalUnitName)[日本語] | NOT RECEIVED |
| 職位(eduPersonAffiliation) | NOT RECEIVED |
| スコープ付き職位(eduPersonScopedAffiliation) | NOT RECEIVED |
| 権限(eduPersonEntitlement) | NOT RECEIVED |
| メールアドレス(mail) | NOT RECEIVED |
| 名(givenName) | NOT RECEIVED |
| 名(jaGivenName)[日本語] | NOT RECEIVED |
| 姓(sn) | NOT RECEIVED |
| 姓(jasn)[日本語] | NOT RECEIVED |
| 表示名(displayName) | NOT RECEIVED |
| 表示名(jaDisplayName)[日本語] | NOT RECEIVED |
| gakuninScopedPersonalUniqueCode | NOT RECEIVED |
| isMemberOf | NOT RECEIVED |
| eduPersonAssurance | NOT RECEIVED |
| eduPersonUniqueId | NOT RECEIVED |

| 区分 | 評価レポート |
|---|---|
| 試験No | 7 |
| 試験項目 | AAL1/AAL2の両方等複数指定による認証要求時の動作 |
| 詳細 | SPが送出するSAMLリクエストに複数の認証レベル要求が含まれている場合の挙動について確認する。 |
| 期待する結果 | 「AuthnContextClassRef」クラスが複数記載されている場合、最も高い認証レベルがクライアントに要求されること。 |

1. IdPで設定しているAuthnContextClassRefの設定




2. Shibboleth SP（SP01）で AuthnContextClassRefに”AAL1”, "AAL2"を要求する設定

■設定追加

ファイル：/etc/httpd/conf.d/shib.conf

```
<Location /secure>
  AuthType shibboleth
  ShibRequestSetting requireSession 1

  # セキュリティレベルを追加（Secioss）
  #ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1"
  ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
  # ShibRequestSetting forceAuthn true
  # END セキュリティレベルを追加（Secioss）
  require shib-session
</Location>
```

設定追加

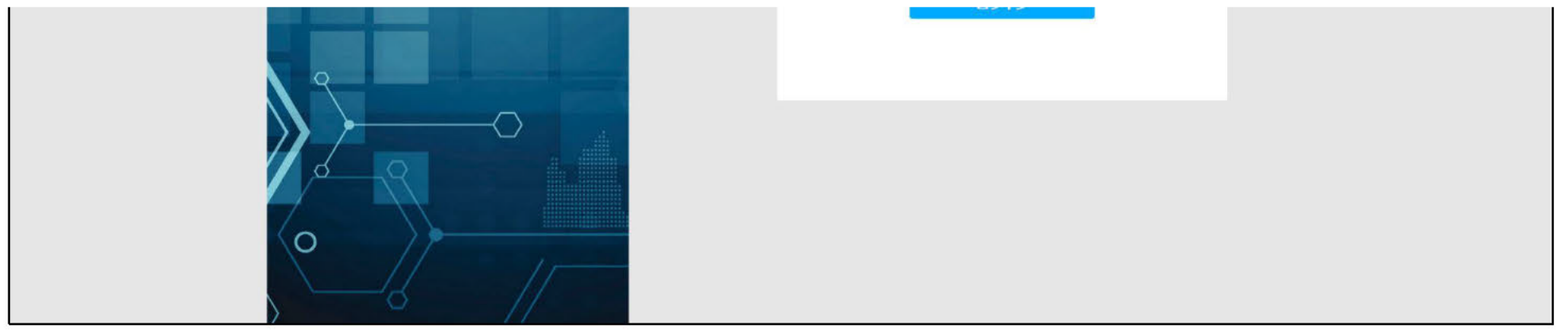
■設定反映

systemctl restart httpd

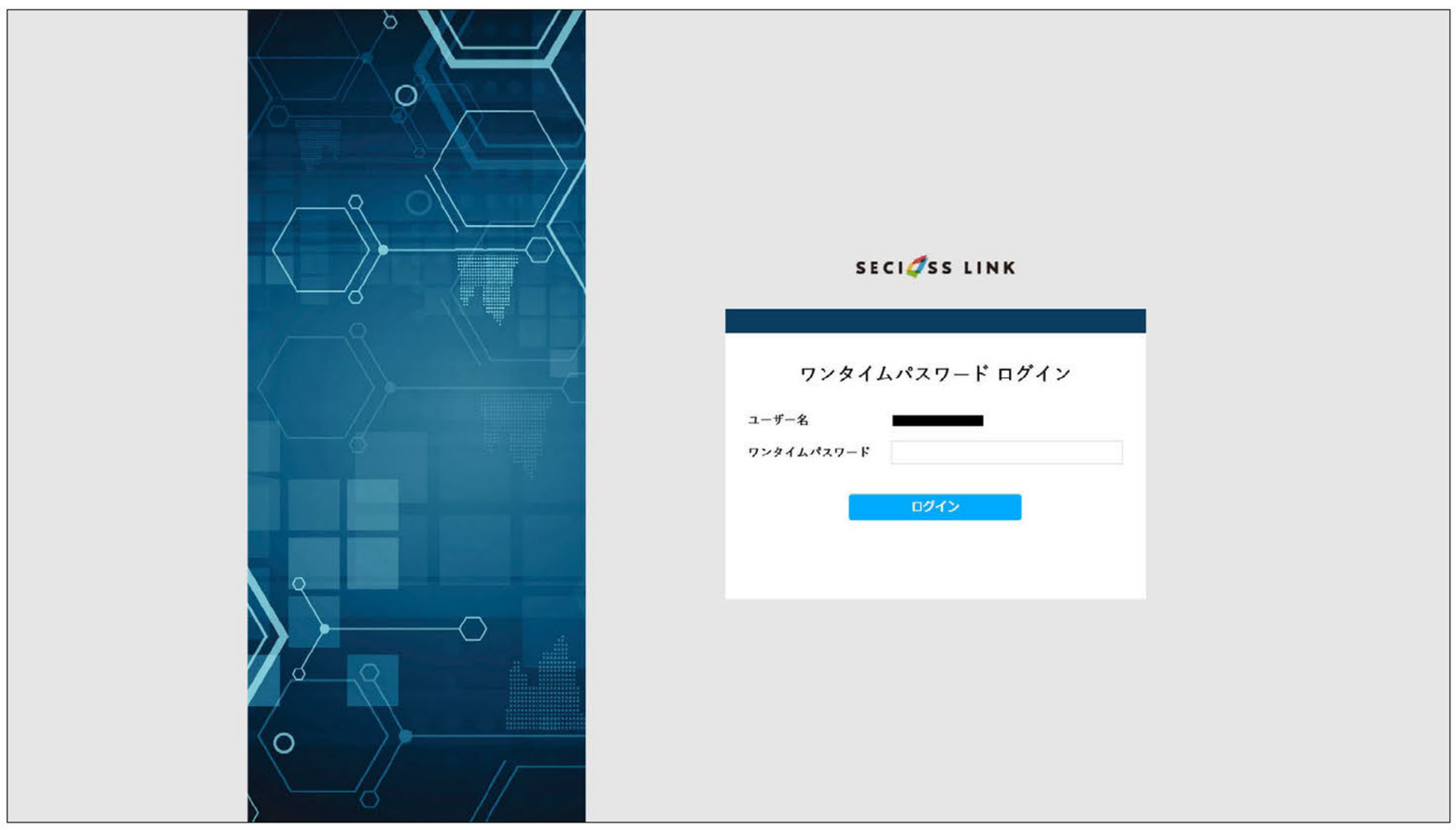
3. SP01にアクセスし、SAMLによるログインを行う。

IdP未認証状態で、「https://172.20.250.4/secure/index.php」 にブラウザでアクセスする。

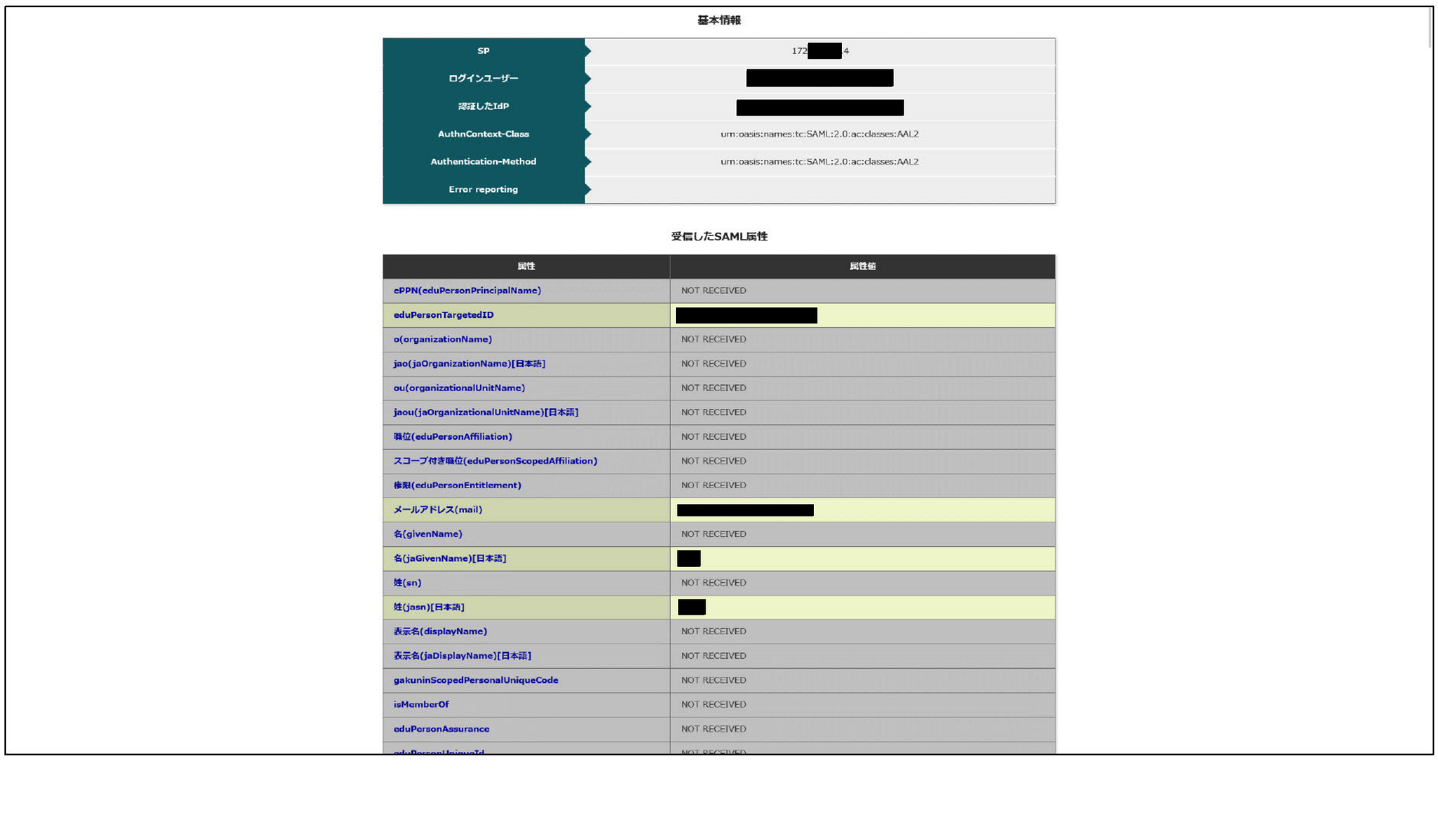
IdPに遷移し、ID/パスワード認証認証が求められるため、認証を行う。



ワンタイムパスワード認証要求が行われる為、認証を行う。




すべての認証を成功したのち、SPへアクセスが行える。



基本情報

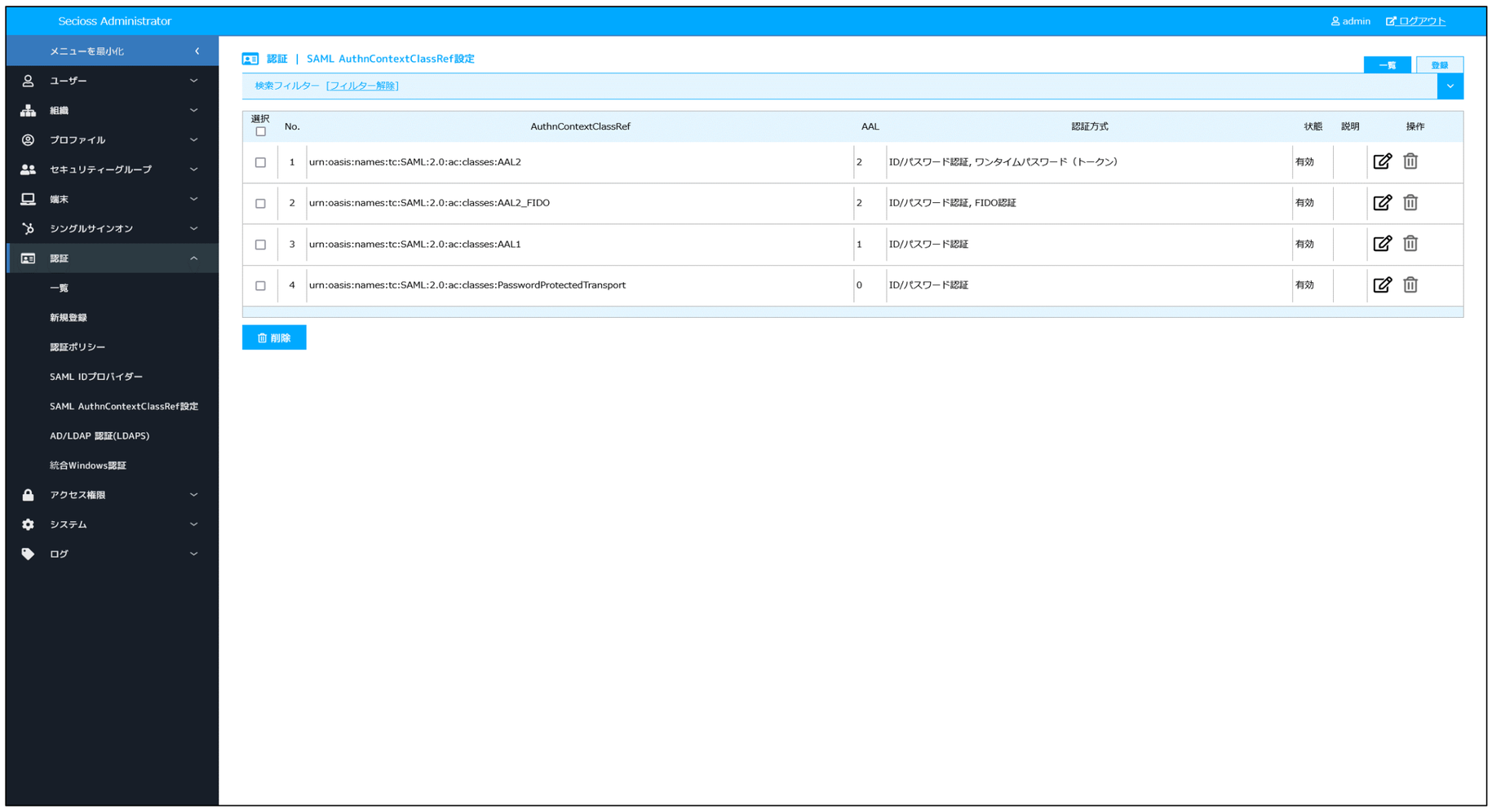
| | |
|---|---|
| SP | 172[redacted]4 |
| ログインユーザー | [redacted] |
| 認証したIdP | [redacted] |
| AuthnContext-Class | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Authentication-Method | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Error reporting | |

受信したSAML属性

| 属性 | 属性値 |
|---|---|
| ePPN(eduPersonPrincipalName) | NOT RECEIVED |
| eduPersonTargetedID | [redacted] |
| o(organizationName) | NOT RECEIVED |
| jao(jaOrganizationName)[日本語] | NOT RECEIVED |
| ou(organizationalUnitName) | NOT RECEIVED |
| jaou(jaOrganizationalUnitName)[日本語] | NOT RECEIVED |
| 職位(eduPersonAffiliation) | NOT RECEIVED |
| スコープ付き職位(eduPersonScopedAffiliation) | NOT RECEIVED |
| 権限(eduPersonEntitlement) | NOT RECEIVED |
| メールアドレス(mail) | [redacted] |
| 名(givenName) | NOT RECEIVED |
| 名(jaGivenName)[日本語] | [redacted] |
| 姓(sn) | NOT RECEIVED |
| 姓(jasn)[日本語] | [redacted] |
| 表示名(displayName) | NOT RECEIVED |
| 表示名(jaDisplayName)[日本語] | NOT RECEIVED |
| gakuninScopedPersonalUniqueCode | NOT RECEIVED |
| isMemberOf | NOT RECEIVED |
| eduPersonAssurance | NOT RECEIVED |
| eduPersonUniqueId | NOT RECEIVED |

| 区分 | 評価レポート |
|---|---|
| 試験No | 8 |
| 試験項目 | ローカル（学認外）認証連携時の動作 |
| 詳細 | SSO環境下で認証レベルを要求するSPと要求しないSPが含まれている場合でも動作に問題がないか確認する。 |
| 期待する結果 | IdPで「認証レベルを要求するSP」と「認証レベルを要求しないSP」の定義を行い、定義に従った認証方式が要求されること。また、このようなSPが混在している場合でも認証システム全体で矛盾や問題が発生しないこと。 |

1. IdPで設定しているAuthnContextClassRefの設定




2. Shibboleth SP（SP01）で AuthnContextClassRefに”AAL2"を要求する設定

■設定追加

ファイル：/etc/httpd/conf.d/shib.conf

```
<Location /secure>
  AuthType shibboleth
  ShibRequestSetting requireSession 1

  # セキュリティレベルを追加（Secioss）
  ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
  #ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
  # ShibRequestSetting forceAuthn true
  # END セキュリティレベルを追加（Secioss）
  require shib-session
</Location>
```

設定追加

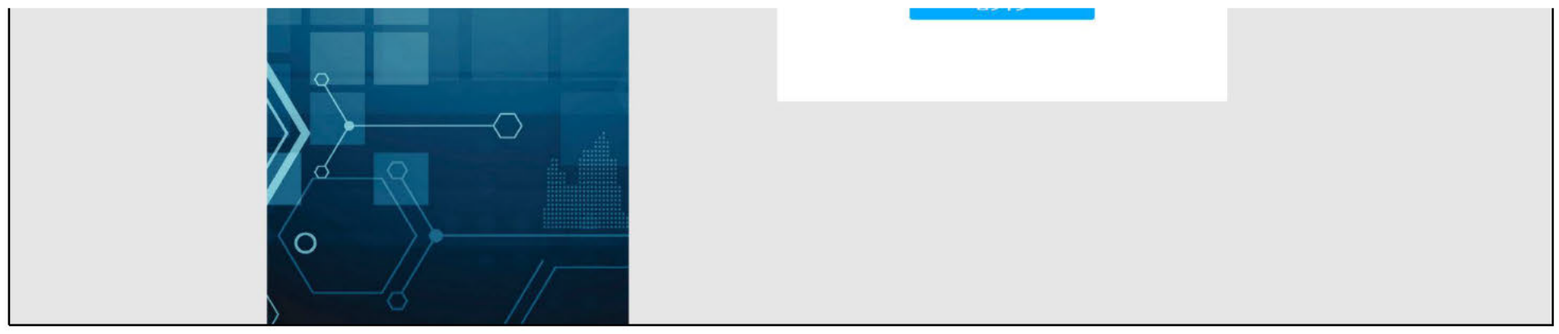
■設定反映

systemctl restart httpd

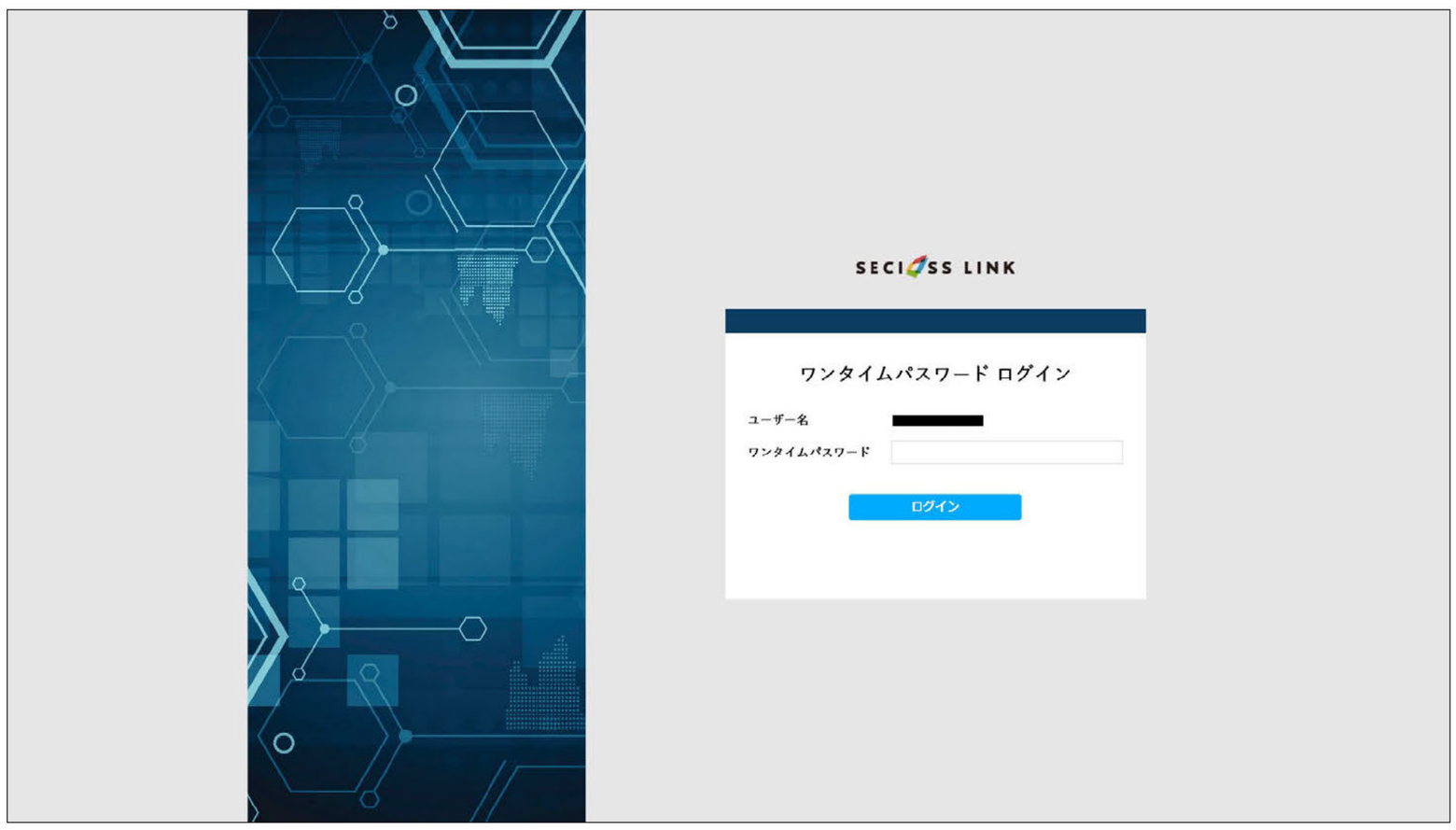
3. SP01にアクセスし、SAMLによるログインを行う。

IdP未認証状態で、「https://172.20.250.4/secure/index.php」 にブラウザでアクセスする。

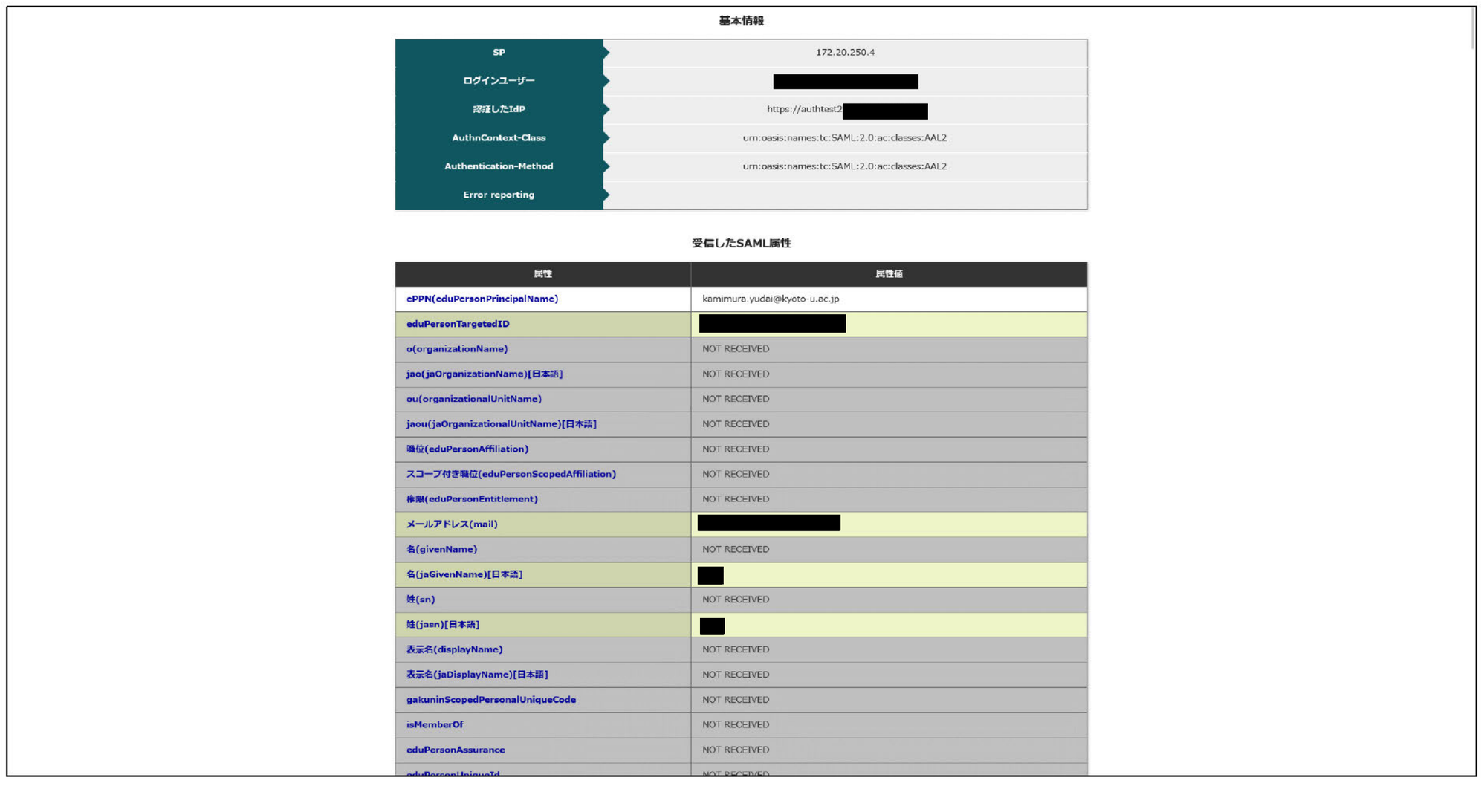
IdPに遷移し、ID/パスワード認証認証が求められるため、認証を行う。



ワンタイムパスワード認証要求が行われる為、認証を行う。




すべての認証を成功したのち、SPへアクセスが行える。



基本情報

| | |
|---|---|
| SP | 172.20.250.4 |
| ログインユーザー | [redacted] |
| 認証したIdP | https://authtest2[redacted] |
| AuthnContext-Class | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Authentication-Method | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Error reporting | |

受信したSAML属性

| 属性 | 属性値 |
|---|---|
| ePPN(eduPersonPrincipalName) | kamimura.yudai@kyoto-u.ac.jp |
| eduPersonTargetedID | [redacted] |
| o(organizationName) | NOT RECEIVED |
| jao(jaOrganizationName)[日本語] | NOT RECEIVED |
| ou(organizationalUnitName) | NOT RECEIVED |
| jaou(jaOrganizationalUnitName)[日本語] | NOT RECEIVED |
| 職位(eduPersonAffiliation) | NOT RECEIVED |
| スコープ付き職位(eduPersonScopedAffiliation) | NOT RECEIVED |
| 権限(eduPersonEntitlement) | NOT RECEIVED |
| メールアドレス(mail) | [redacted] |
| 名(givenName) | NOT RECEIVED |
| 名(jaGivenName)[日本語] | [redacted] |
| 姓(sn) | NOT RECEIVED |
| 姓(jasn)[日本語] | [redacted] |
| 表示名(displayName) | NOT RECEIVED |
| 表示名(jaDisplayName)[日本語] | NOT RECEIVED |
| gakuninScopedPersonalUniqueCode | NOT RECEIVED |
| isMemberOf | NOT RECEIVED |
| eduPersonAssurance | NOT RECEIVED |
| eduPersonUniqueId | NOT RECEIVED |

4. Shibboleth SP（SP02）で **AuthnContextClassRefを要求しないよう**に設定する。

■設定追加

ファイル：/etc/httpd/conf.d/shib.conf

```
<Location /secure>
 AuthType shibboleth
 ShibRequestSetting requireSession 1

 # セキュリティレベルを追加（Secioss）
 # ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1"
 # ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
 # ShibRequestSetting forceAuthn true
 # END セキュリティレベルを追加（Secioss）
 require shib-session
</Location>
```

設定OFF

■設定反映

systemctl restart httpd

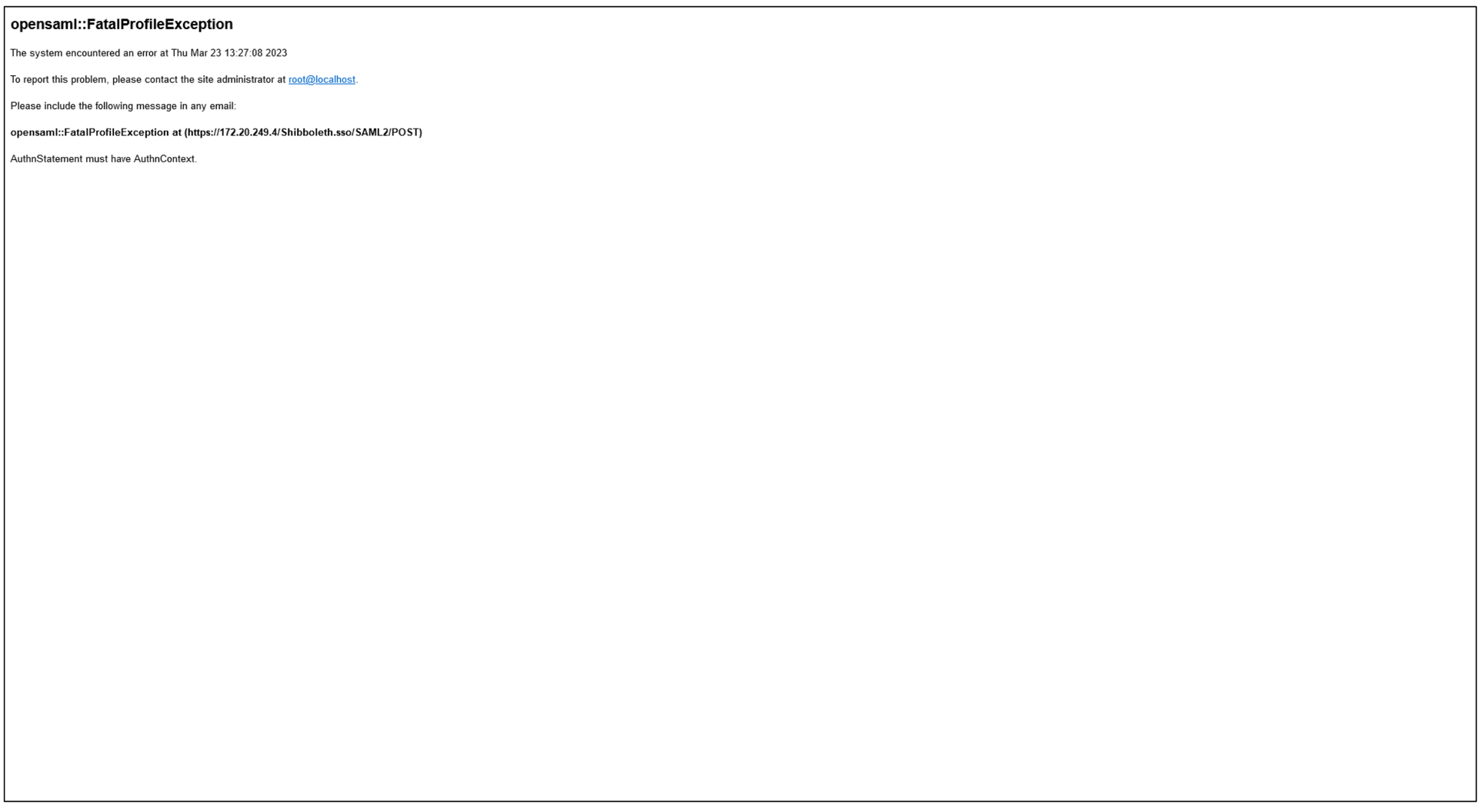
5. SP02にアクセスし、SAMLによるログインを行う。

IdP認証済み（SP01アクセス時にAAL2の認証済み）の状態で、「https://172.20.249.4/secure/index.php」 にブラウザでアクセスする。

SP01アクセス時にID/パスワード認証とワンタイムパスワード認証をすでに行っているため、SP02へアクセスが行える。

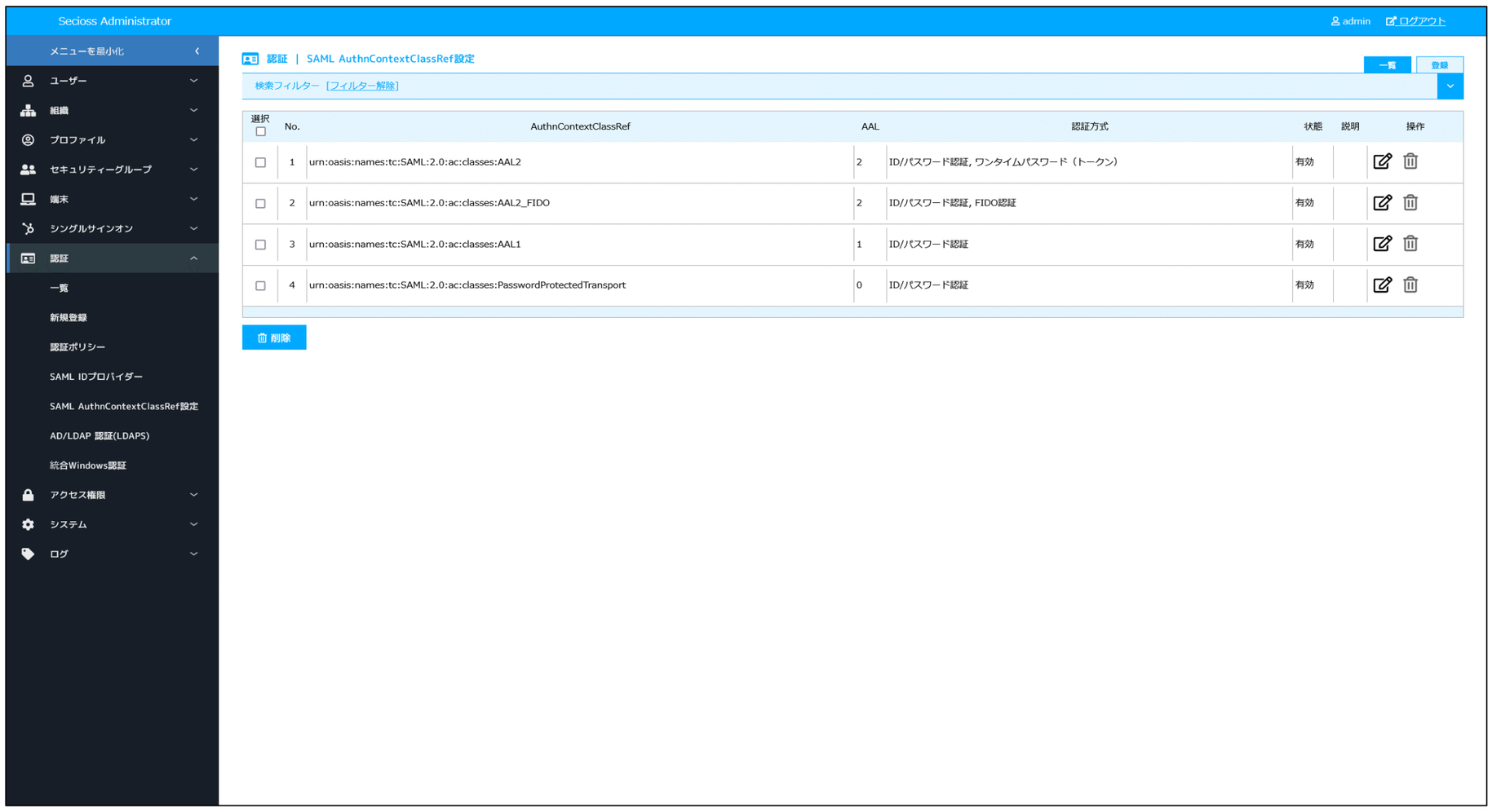
※1 SP02は認証ルールとアクセス権限で設定されている認証を行う必要があるが、この設定では、事前準備の認証ルールで「ID/パスワード認証」のみ求められる状態となっている。

※2 IdPはSPに対して、AuthnContextClassRefを送信していないため、SPでエラーとなる。



| 区分 | 評価レポート |
|---|---|
| 試験No | 9 |
| 試験項目 | 強制再認証時の動作 |
| 詳細 | SPが送出するSAMLリクエストに強制再認証（ForceAuthn）が含まれている場合の挙動について確認する。 |
| 期待する結果 | IdPですでに認証済みのセッションがあったとしてもSPから「ForceAuthn」を含むSAMLリクエストを受けた場合、認証を実施すること。また同時に認証レベルの要求があった場合、定義に従いクライアントに認証を要求すること。 |

1. IdPで設定しているAuthnContextClassRefの設定




2. Shibboleth SP（SP01）で AuthnContextClassRefに”AAL2"を要求し、強制再認証をIdPへ要求する設定

■設定追加

ファイル：/etc/httpd/conf.d/shib.conf

```
<Location /secure>
  AuthType shibboleth
  ShibRequestSetting requireSession 1

  # セキュリティレベルを追加（Secioss）
  ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
  #ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
  ShibRequestSetting forceAuthn true
  # END セキュリティレベルを追加（Secioss）
  require shib-session
</Location>
```

設定追加

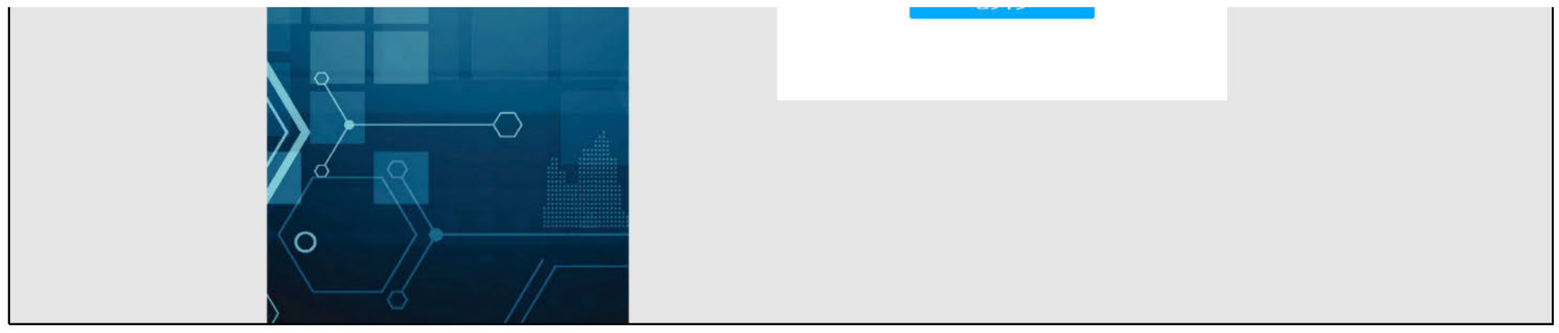
■設定反映

systemctl restart httpd

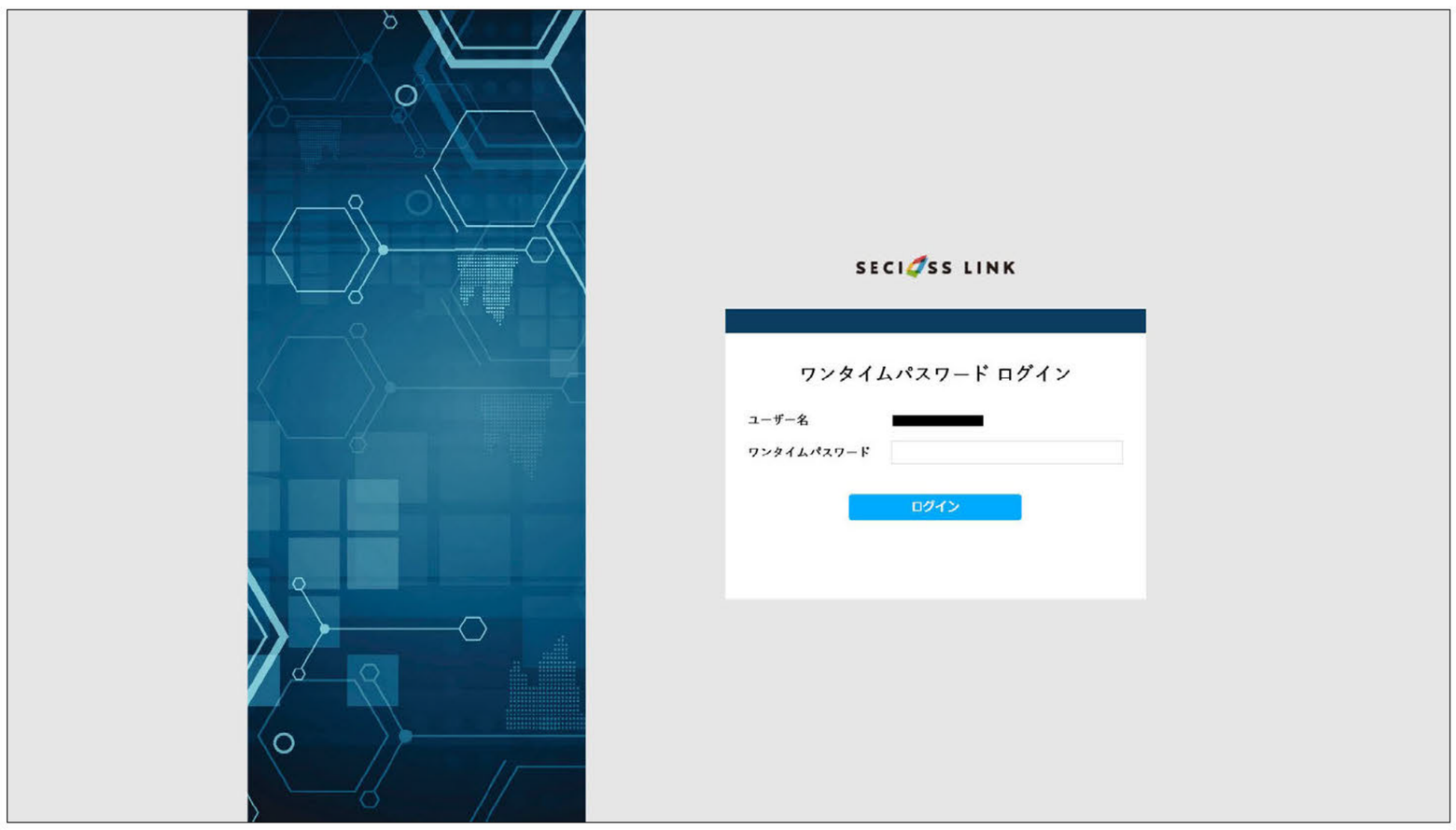
3. SP01にアクセスし、SAMLによるログインを行う。

IdP未認証状態で、「https://172.20.250.4/secure/index.php」 にブラウザでアクセスする。

IdPに遷移し、ID/パスワード認証認証が求められるため、認証を行う。



ワンタイムパスワード認証要求が行われる為、認証を行う。




すべての認証を成功したのち、SPへアクセスが行える。

基本情報

| | |
|---|---|
| SP | 172.20.250.4 |
| ログインユーザー | [redacted] |
| 認証したIdP | https://authtest[redacted] |
| AuthnContext-Class | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Authentication-Method | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Error reporting | |

受信したSAML属性

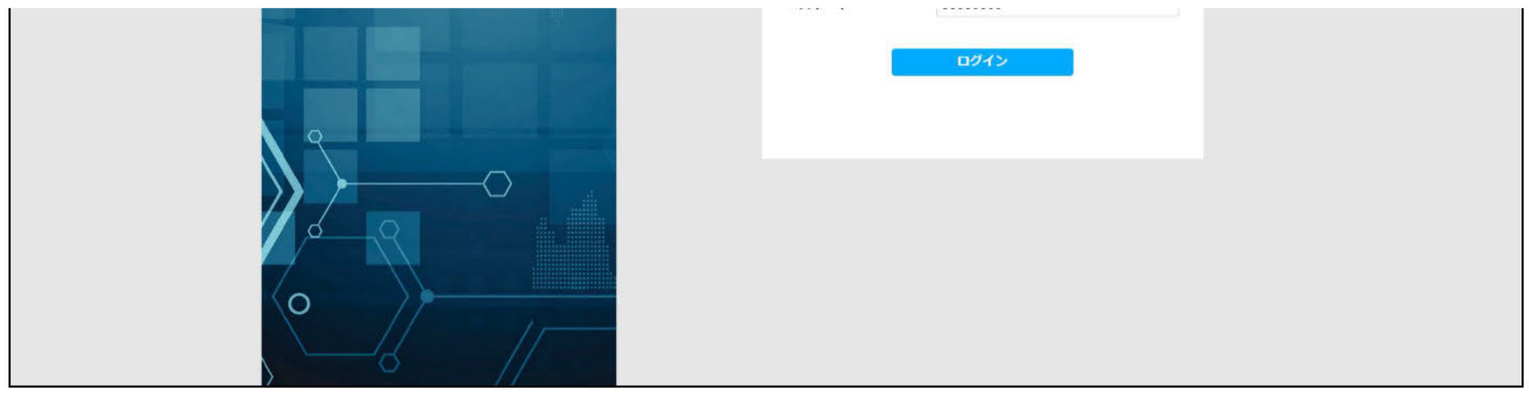
| 属性 | 属性値 |
|---|---|
| ePPN(eduPersonPrincipalName) | kamimura.yudai@kyoto-u.ac.jp |
| eduPersonTargetedID | [redacted] |
| o(organizationName) | NOT RECEIVED |
| jao(jaOrganizationName)[日本語] | NOT RECEIVED |
| ou(organizationalUnitName) | NOT RECEIVED |
| jaou(jaOrganizationalUnitName)[日本語] | NOT RECEIVED |
| 職位(eduPersonAffiliation) | NOT RECEIVED |
| スコープ付き職位(eduPersonScopedAffiliation) | NOT RECEIVED |
| 権限(eduPersonEntitlement) | NOT RECEIVED |
| メールアドレス(mail) | [redacted] |
| 名(givenName) | NOT RECEIVED |
| 名(jaGivenName)[日本語] | [redacted] |
| 姓(sn) | NOT RECEIVED |
| 姓(jasn)[日本語] | [redacted] |
| 表示名(displayName) | NOT RECEIVED |
| 表示名(jaDisplayName)[日本語] | NOT RECEIVED |
| gakuninScopedPersonalUniqueCode | NOT RECEIVED |
| isMemberOf | NOT RECEIVED |
| eduPersonAssurance | NOT RECEIVED |
| eduPersonUniqueId | NOT RECEIVED |

7. SP01で一度ログアウトを行い、再度SAMLでログインを行う

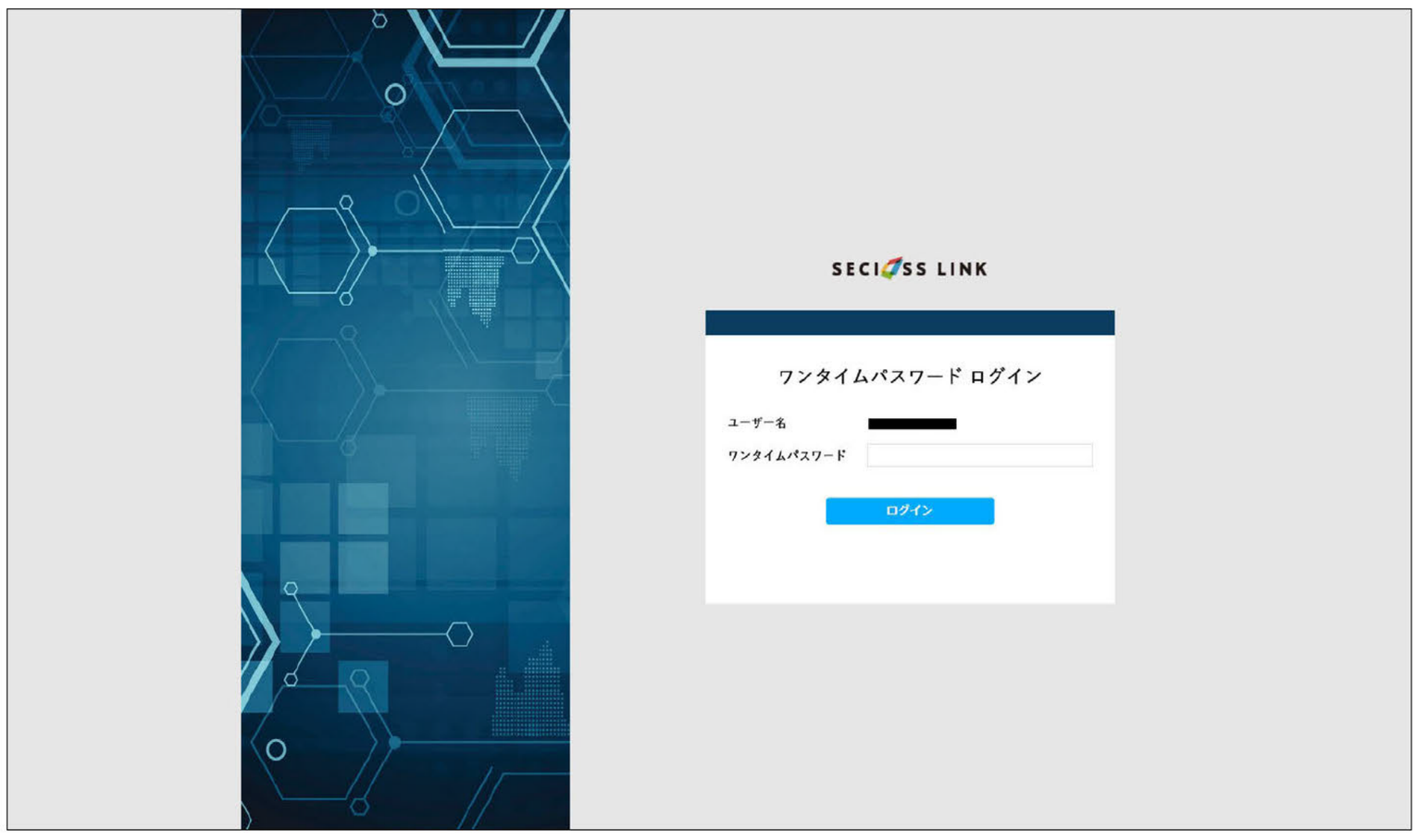
   SP01のログアウトを行う（https://172.20.250.4/Shibboleth.sso/Logout?return=https://172.20.250.4/へアクセス）

   IdP認証済み（SP01アクセス時にAAL2の認証済み）の状態で、「https://172.20.250.4/secure/index.php」 にブラウザでアクセスする。

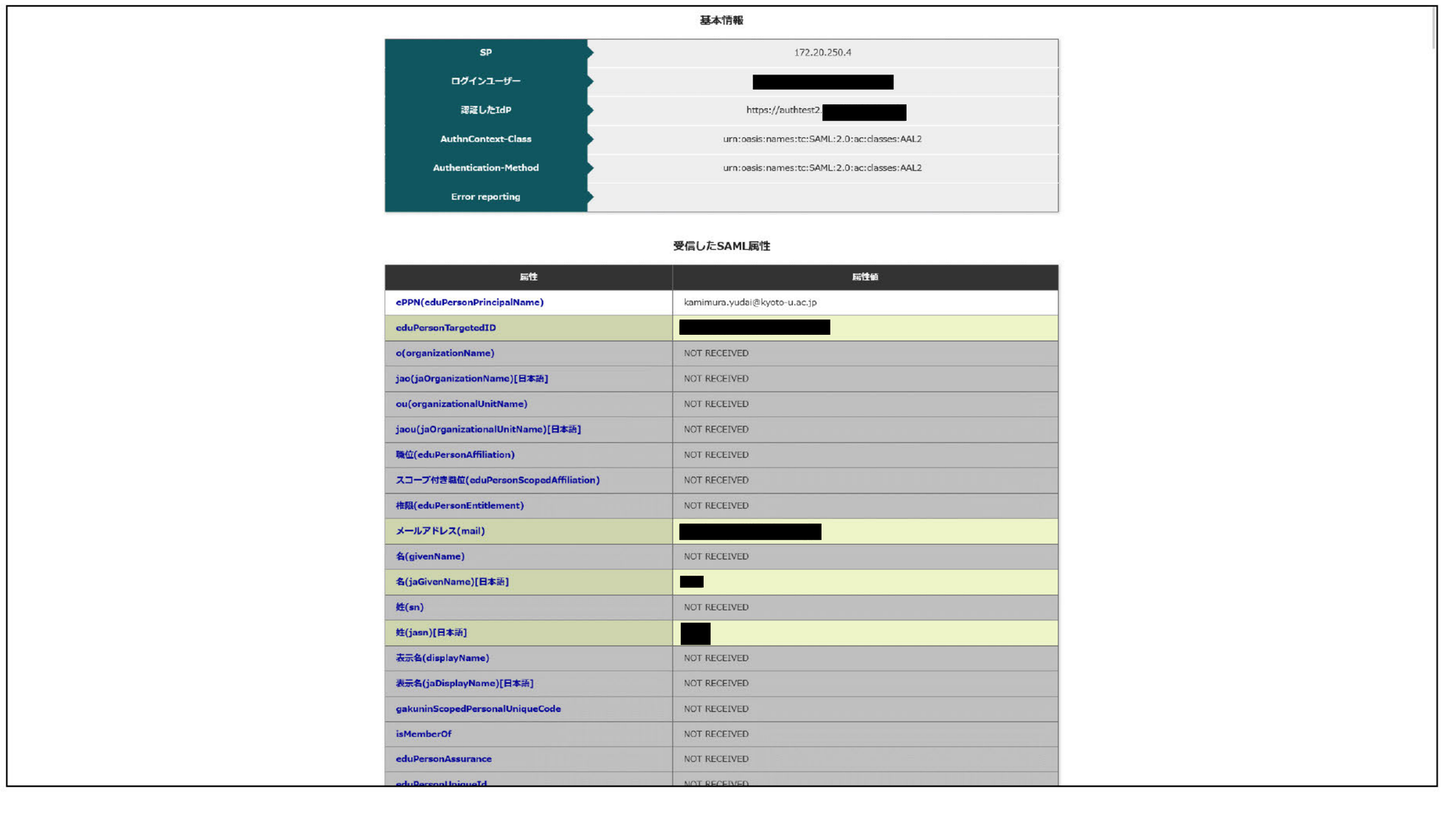
   SP01アクセス時にAAL2の認証をすでに行っているが、再度ID/パスワード認証とワンタイムパスワード認証が求められる。




ワンタイムパスワード認証要求が行われる為、認証を行う。




すべての認証を成功したのち、SPへアクセスが行える。



基本情報

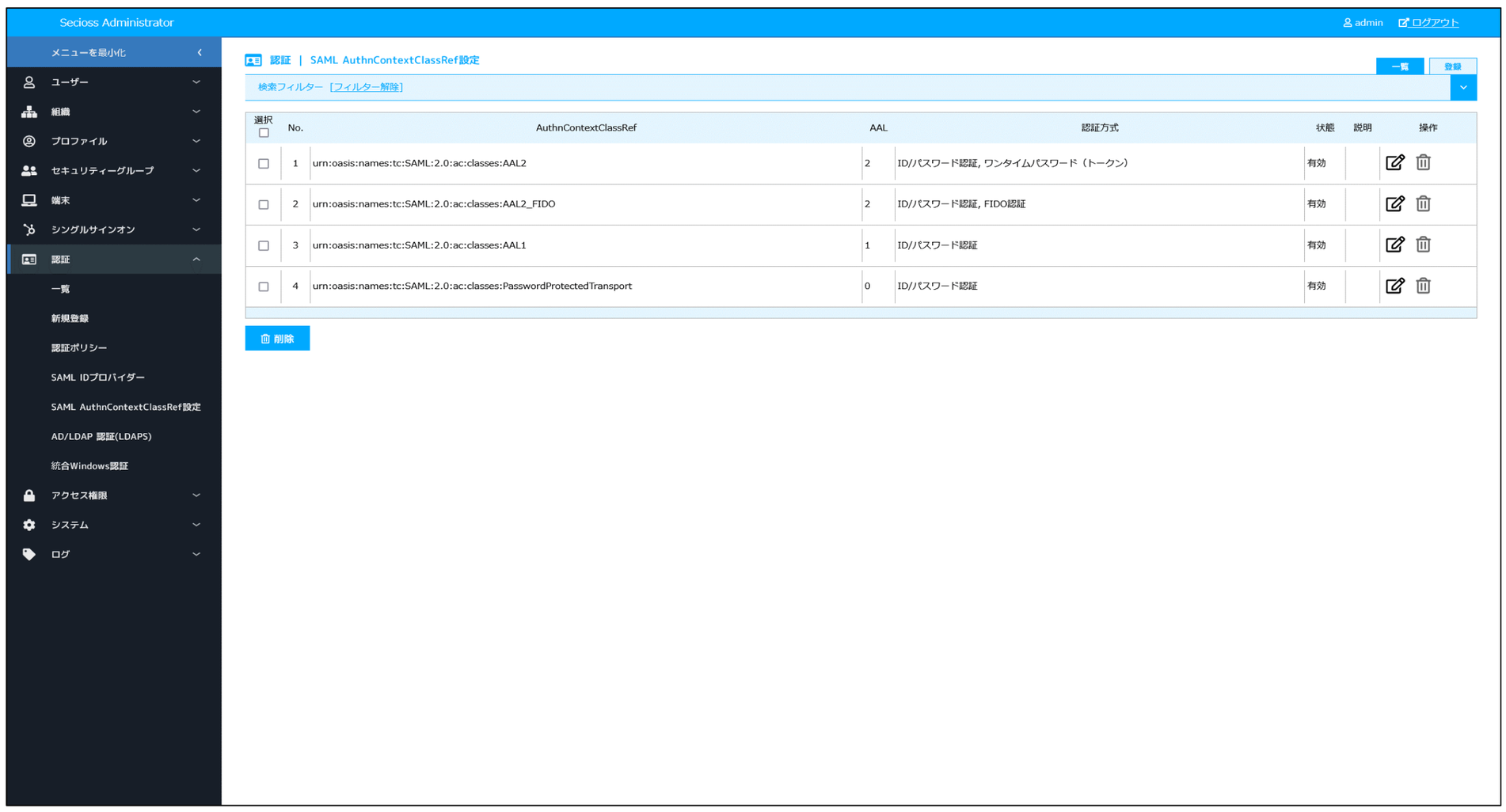
| | |
|---|---|
| SP | 172.20.250.4 |
| ログインユーザー | [redacted] |
| 認証したIdP | https://authtest2.[redacted] |
| AuthnContext-Class | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Authentication-Method | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Error reporting | |

受信したSAML属性

| 属性 | 属性値 |
|---|---|
| ePPN(eduPersonPrincipalName) | kamimura.yudai@kyoto-u.ac.jp |
| eduPersonTargetedID | [redacted] |
| o(organizationName) | NOT RECEIVED |
| jao(jaOrganizationName)[日本語] | NOT RECEIVED |
| ou(organizationalUnitName) | NOT RECEIVED |
| jaou(jaOrganizationalUnitName)[日本語] | NOT RECEIVED |
| 職位(eduPersonAffiliation) | NOT RECEIVED |
| スコープ付き職位(eduPersonScopedAffiliation) | NOT RECEIVED |
| 権限(eduPersonEntitlement) | NOT RECEIVED |
| メールアドレス(mail) | [redacted] |
| 名(givenName) | NOT RECEIVED |
| 名(jaGivenName)[日本語] | [redacted] |
| 姓(sn) | NOT RECEIVED |
| 姓(jasn)[日本語] | [redacted] |
| 表示名(displayName) | NOT RECEIVED |
| 表示名(jaDisplayName)[日本語] | NOT RECEIVED |
| gakuninScopedPersonalUniqueCode | NOT RECEIVED |
| isMemberOf | NOT RECEIVED |
| eduPersonAssurance | NOT RECEIVED |
| eduPersonUniqueId | NOT RECEIVED |

| 区分 | その他機能 |
|---|---|
| 試験No | 1 |
| 試験項目 | SPから要求されたAuthnContextClassRefが未定義時の動作 |
| 詳細 | SPから要求されたAuthnContextClassRefの認証要求がIdPで定義していない<br>AuthnContextClassRefの場合、ユーザーにエラーを提示しSPへエラー応答を返却する |
| 期待する結果 | SPからAAL2の認証を求められているとき、ユーザーがワンタイムパスワード設定を行っていないとき、ユーザーにエラーを表示したのちSPにNoAuthnContextのエラーを返却する。 |

1. IdPで設定しているAuthnContextClassRefの設定




2. Shibboleth SP（SP01）で AuthnContextClassRefに”Certificate"を要求する設定

■設定追加

ファイル：/etc/httpd/conf.d/shib.conf

```
<Location /secure>
  AuthType shibboleth
  ShibRequestSetting requireSession 1

  # セキュリティレベルを追加（Secioss）
  ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:Certificate"
  #ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
  #ShibRequestSetting forceAuthn true
  # END セキュリティレベルを追加（Secioss）
  require shib-session
</Location>
```

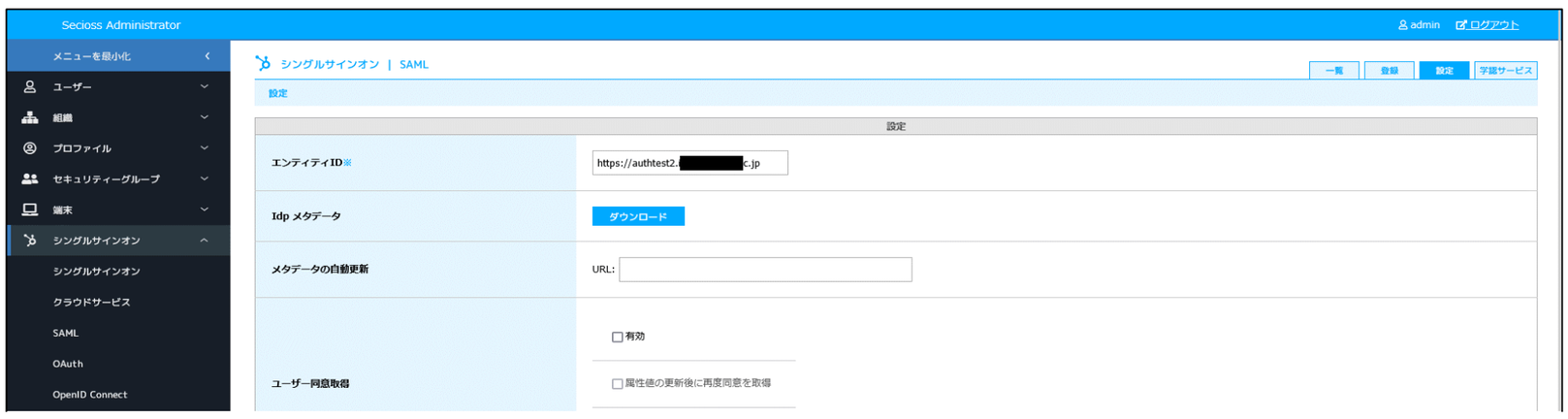
設定追加

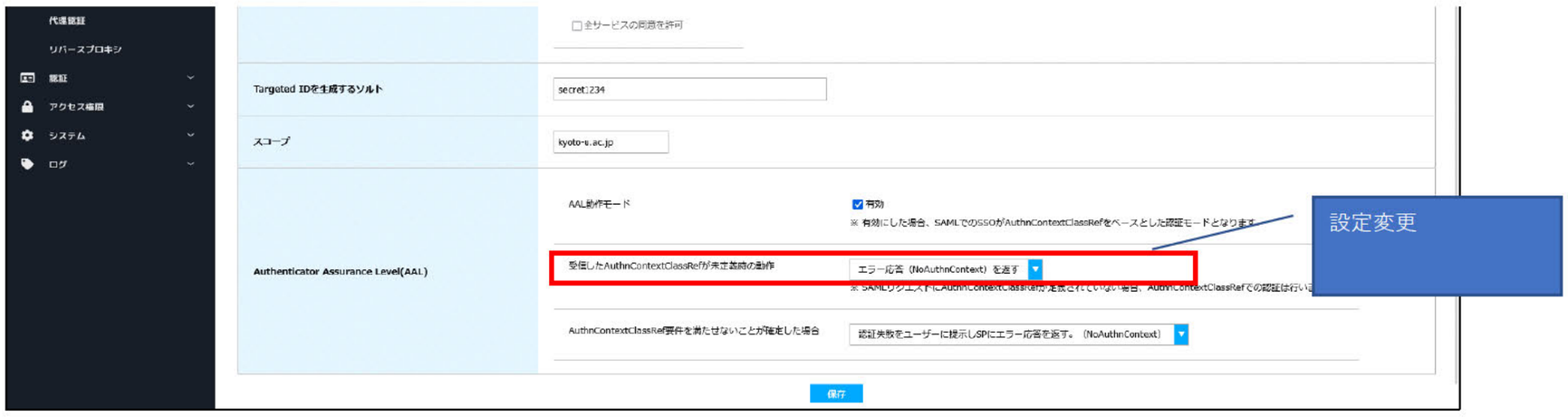
■設定反映

systemctl restart httpd

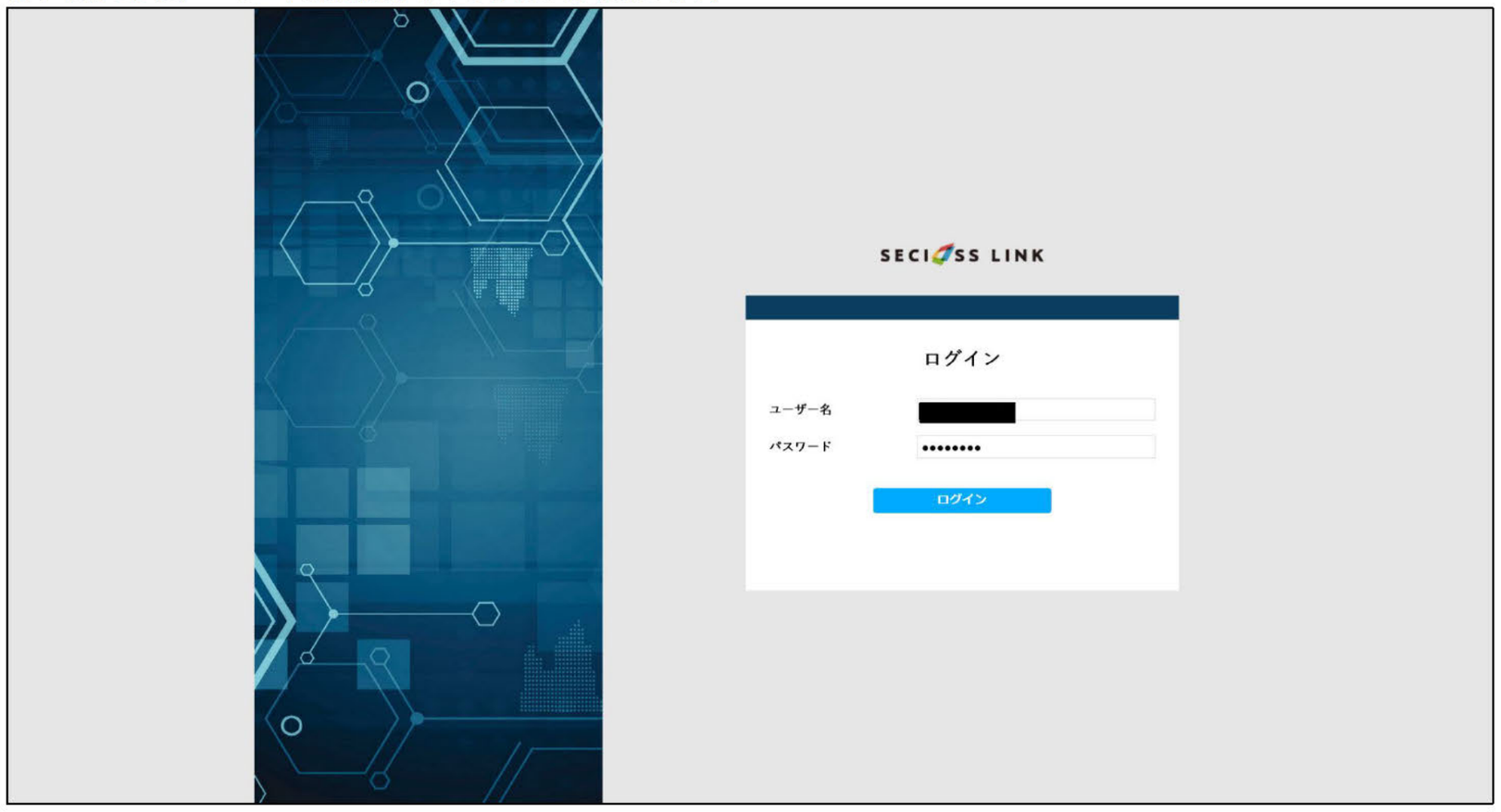
3. IdPでAuthnContextClassRef要件を満たせないことが確定した場合の動作を設定

受信したAuthnContextClassRefが未定義時の動作の値を「エラー応答を返す（NoAuthnContext）」に設定



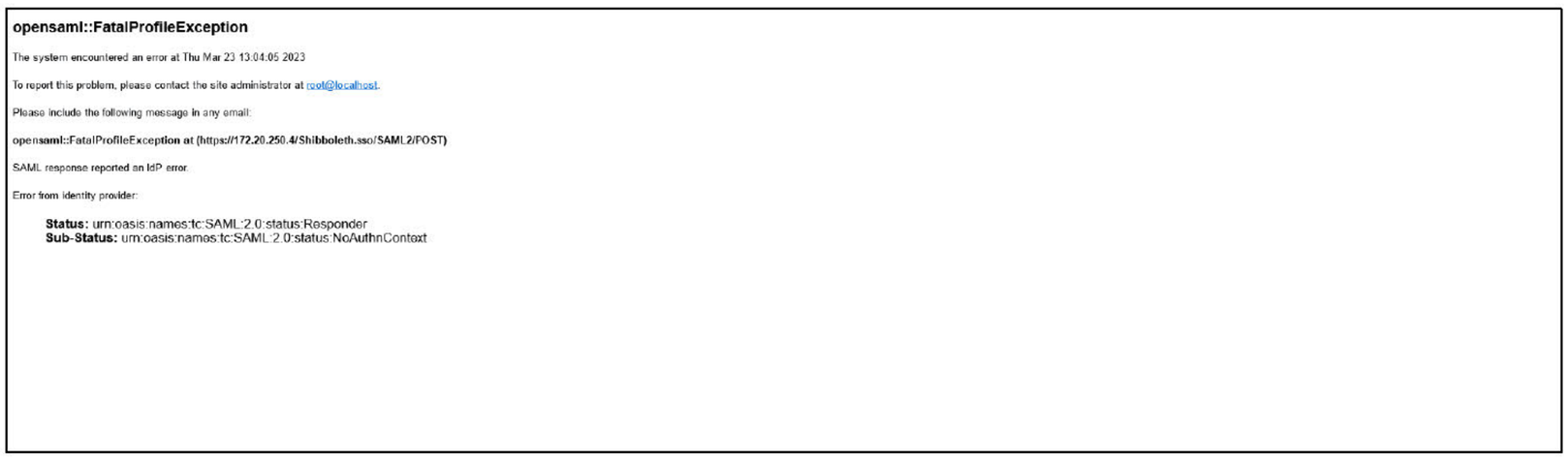



4. SP01にアクセスし、SAMLによるログインを行う。
   IdP未認証状態で、「https://172.20.250.4/secure/index.php」 にブラウザでアクセスする。
   IdPに遷移し、ID/パスワード認証認証が求められるため、認証を行う。



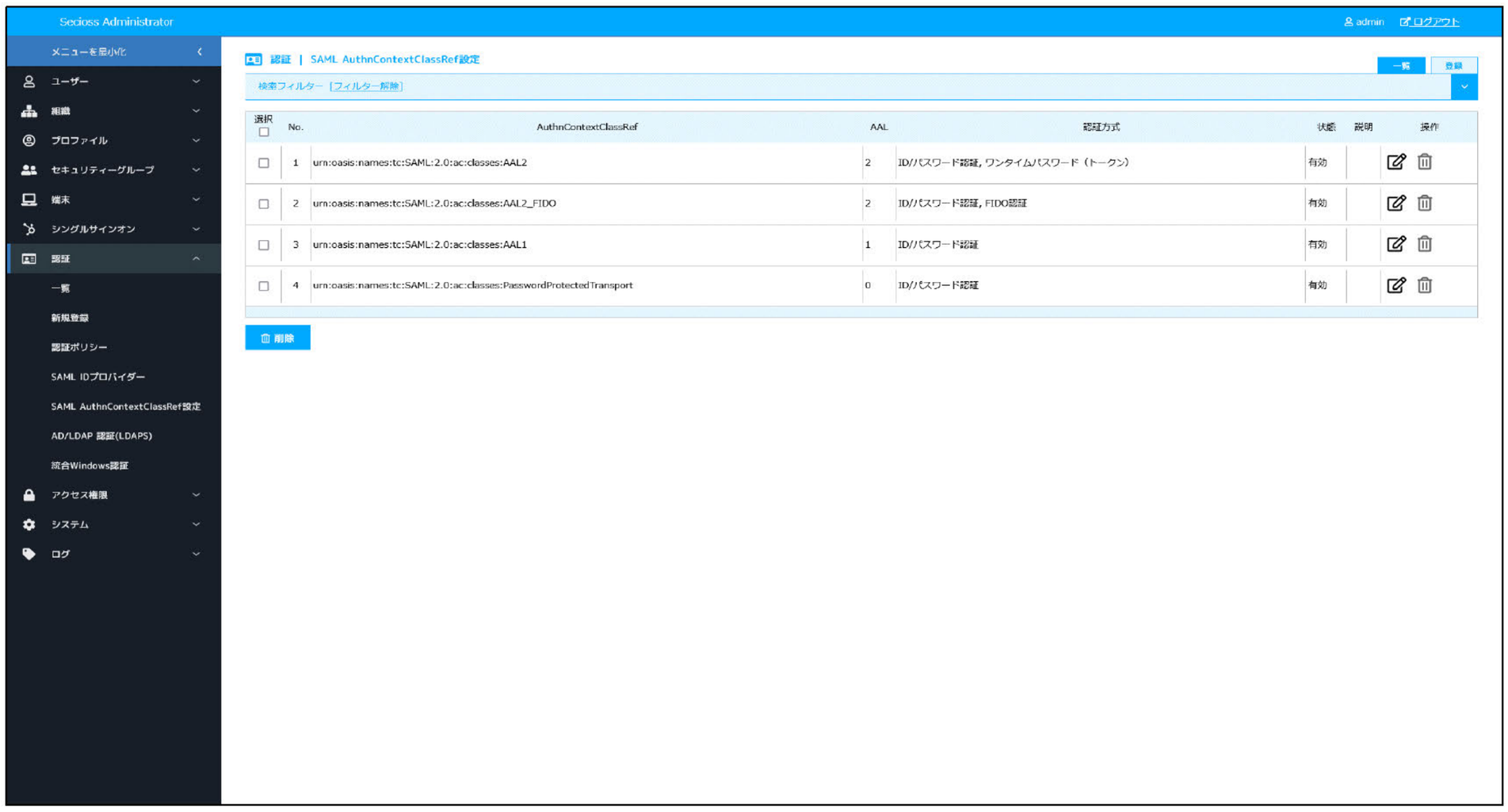

AuthnContextClassRefの認証要求がCertificateで要求されるが、IdPで未定義であるため、エラーが表示される。


エラー表示から5秒後に、SPへNoAuthnContextのエラーを送信する



| 区分 | その他機能 |
|---|---|
| 試験No | 2 |
| 試験項目 | AuthnContextClassRefの条件を満たせないときの動作 |
| 詳細 | SPから要求されたAAL2の認証要求が満たせないことが確定した場合、ユーザーにエラーを表示したのちSPにエラー応答を返す。 |
| 期待する結果 | SPからAAL2の認証を求められているとき、ユーザーがワンタイムパスワード設定を行っていないとき、ユーザーにエラーを表示したのちSPにNoAuthnContextのエラーを返却する。 |

1. IdPで設定しているAuthnContextClassRefの設定




2. Shibboleth SP（SP01）で AuthnContextClassRefに”AAL2"を要求する設定

■設定追加

ファイル：/etc/httpd/conf.d/shib.conf

```
<Location /secure>
  AuthType shibboleth
  ShibRequestSetting requireSession 1

  # セキュリティレベルを追加（Secioss）
  ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
  #ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
  #ShibRequestSetting forceAuthn true
  # END セキュリティレベルを追加（Secioss）
  require shib-session
</Location>
```

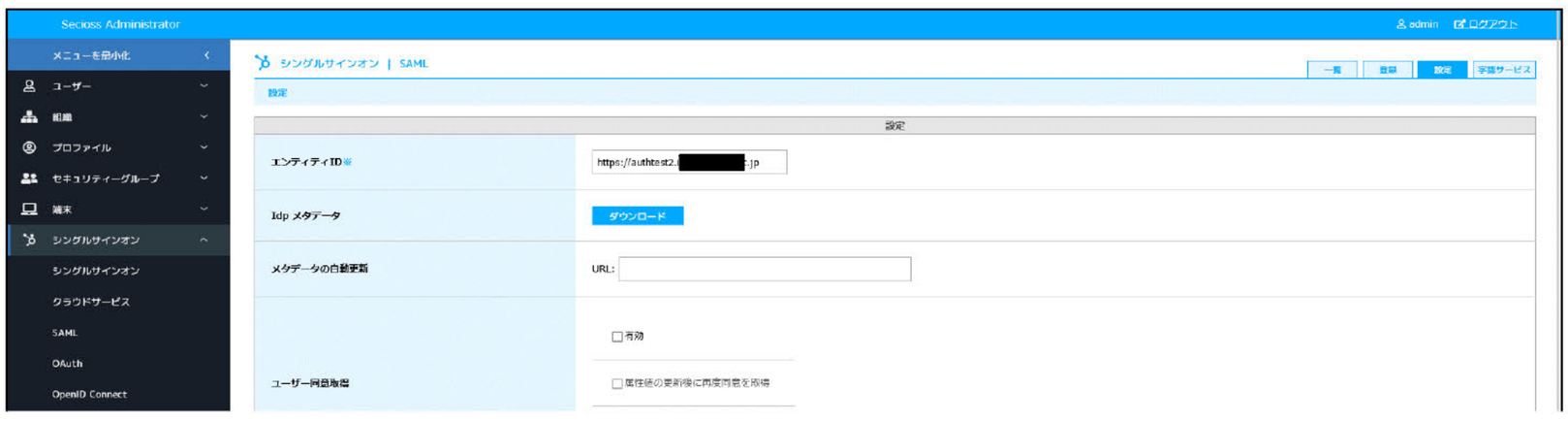
設定追加

■設定反映

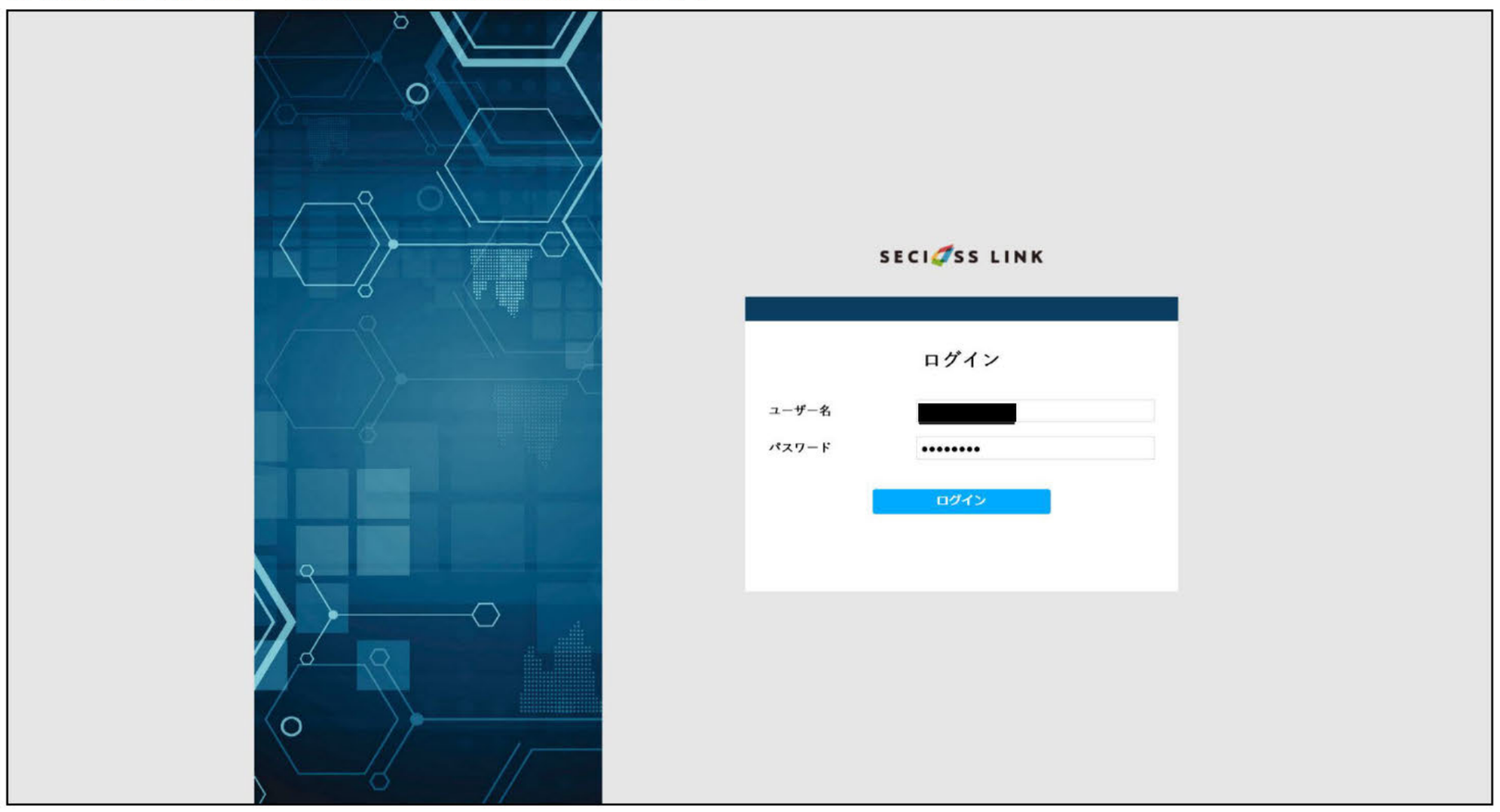
systemctl restart httpd

3. IdPでAuthnContextClassRef要件を満たせないことが確定した場合の動作を設定

AuthnContextClassRef要件を満たせないことが確定した場合の値を「認証失敗を提示しSPにエラー応答を返す（NoAuthnContext）」に設定

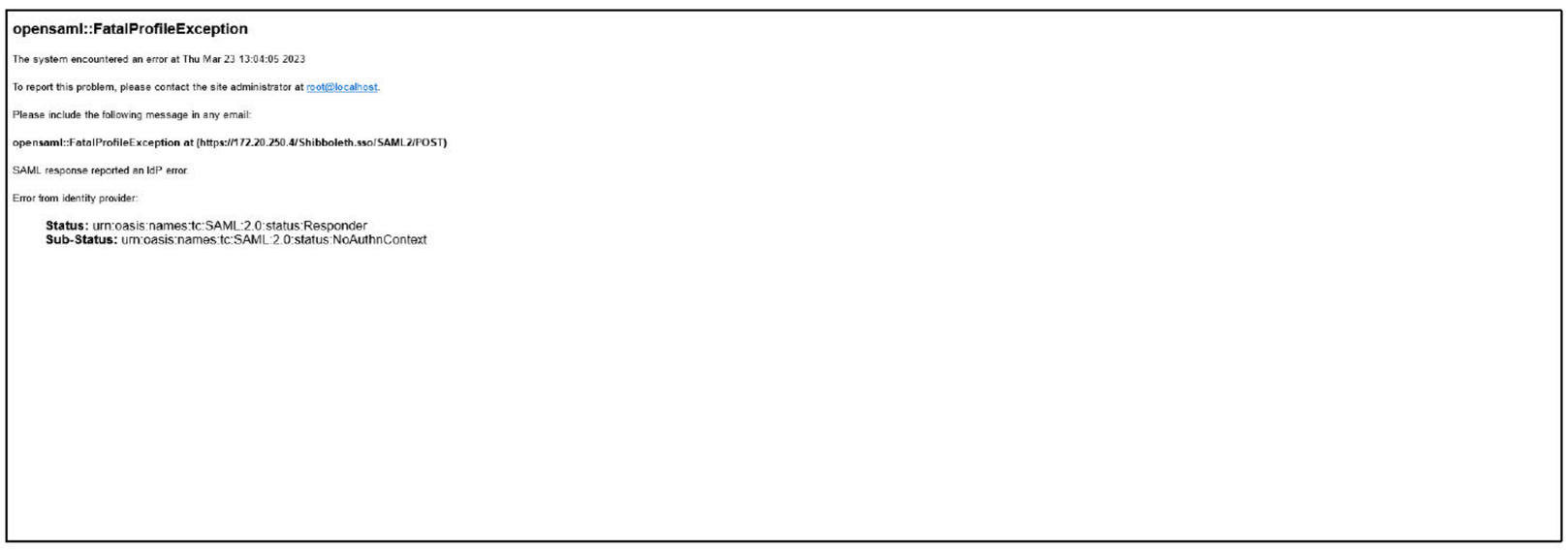



4. SP01にアクセスし、SAMLによるログインを行う。
   ログインするユーザーのワンタイムパスワードを初期化して未設定状態であること。
   IdP未認証状態で、「https://172.20.250.4/secure/index.php」 にブラウザでアクセスする。
   IdPに遷移し、ID/パスワード認証認証が求められるため、認証を行う。



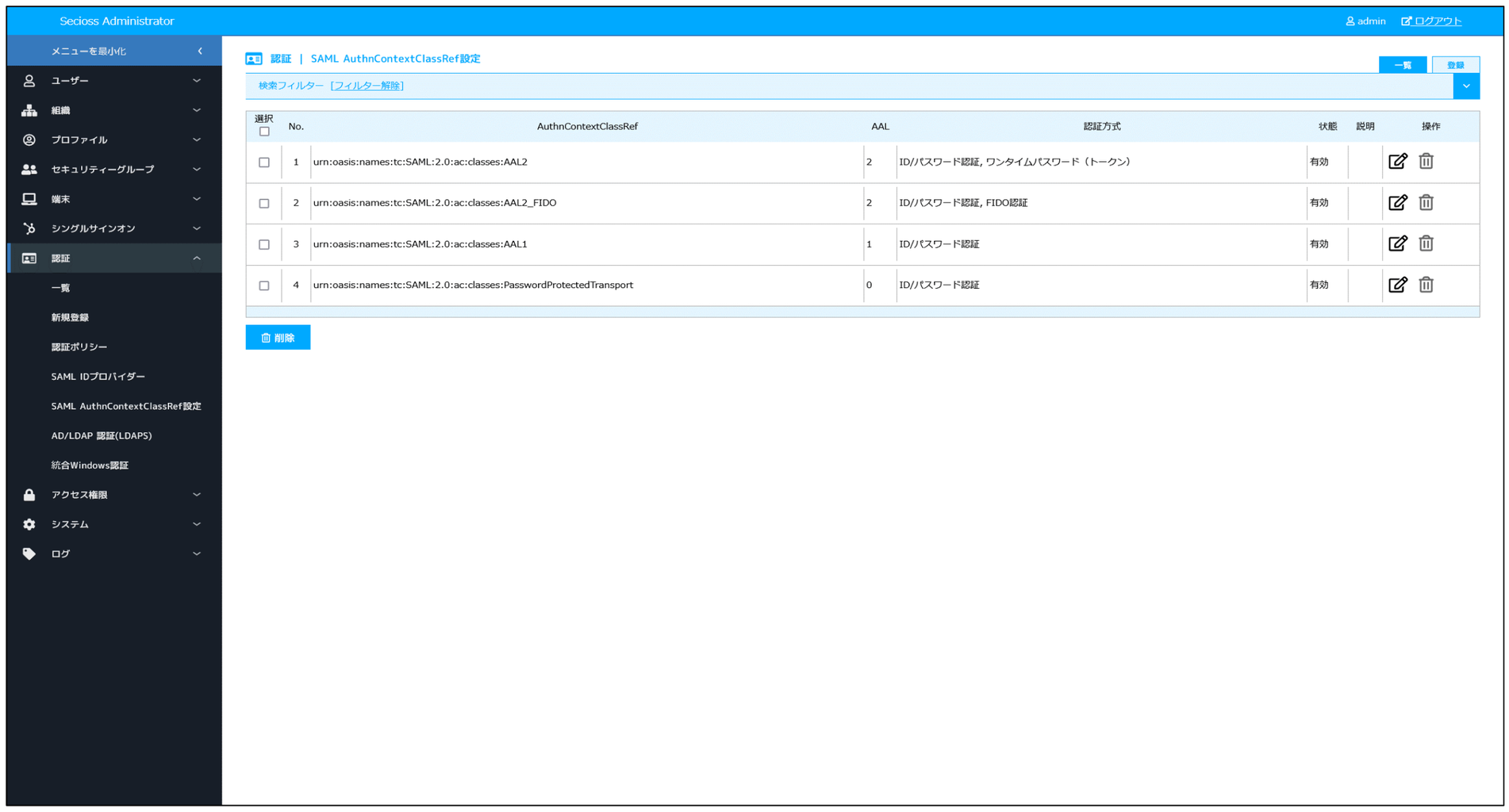

ワンタイムパスワードが未設定であるため、AAL2の認証要素を満たすことができずエラーが表示される。


エラー表示から5秒後に、SPへNoAuthnContextのエラーを送信する



| 区分 | その他機能 |
|---|---|
| 試験No | 3 |
| 試験項目 | SPからの、AuthnContextClassRefを無視してIdPで任意のAuthnContextClassRefを返却する。 |
| 詳細 | SPが送出するSAMLリクエスト内のAuthnContextClassRefを無視してIdPで認証する。<br>返却する値は、SPから送出されたAuthnContextClassRefで返却を行う。または、IdPにて指定の値を送信するか送信しないかを選択する。 |
| 期待する結果 | SPからの、AuthnContextClassRefを無視してIdPにて設定した認証を実施する。<br>以下の順に検証し、期待する動作を得られること。<br>1. SAMLレスポンスには、SPから送出されたAuthnContextClassRefで返却する。<br>2. SAMLレスポンスには、IdPにて設定したAuthnContextClassRefで返却する。<br>3. SAMLレスポンスにAuthnContextClassRefを送出しない |

1. IdPで設定しているAuthnContextClassRefの設定




2. Shibboleth SP（SP01）で AuthnContextClassRefに”AAL2"を要求する設定

■設定追加

ファイル：/etc/httpd/conf.d/shib.conf

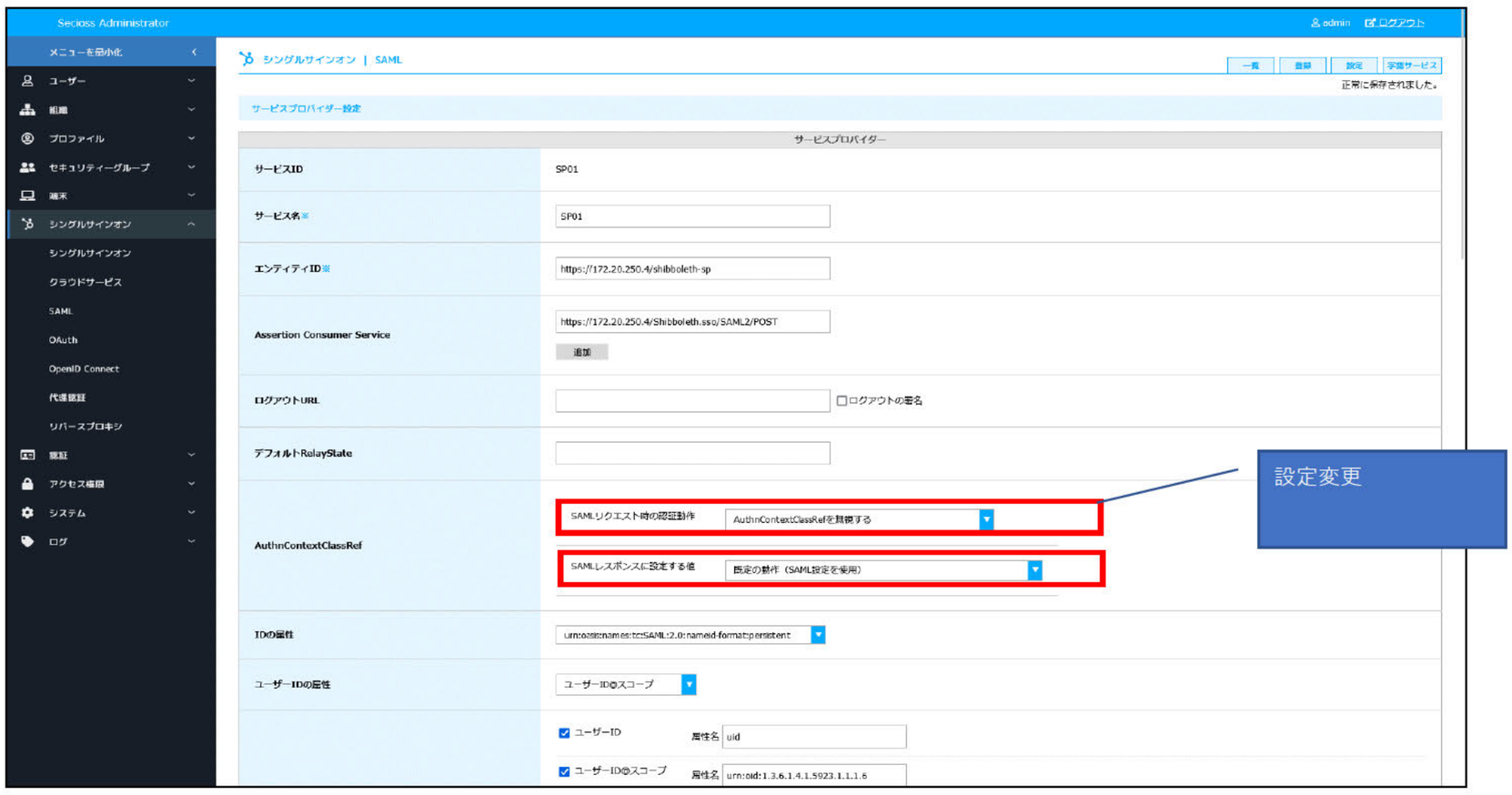
```
<Location /secure>
  AuthType shibboleth
  ShibRequestSetting requireSession 1

  # セキュリティレベルを追加（Secioss）
  ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
  #ShibRequestSetting authnContextClassRef "urn:oasis:names:tc:SAML:2.0:ac:classes:AAL1 urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2"
  #ShibRequestSetting forceAuthn true
  # END セキュリティレベルを追加（Secioss）
  require shib-session
</Location>
```

設定追加

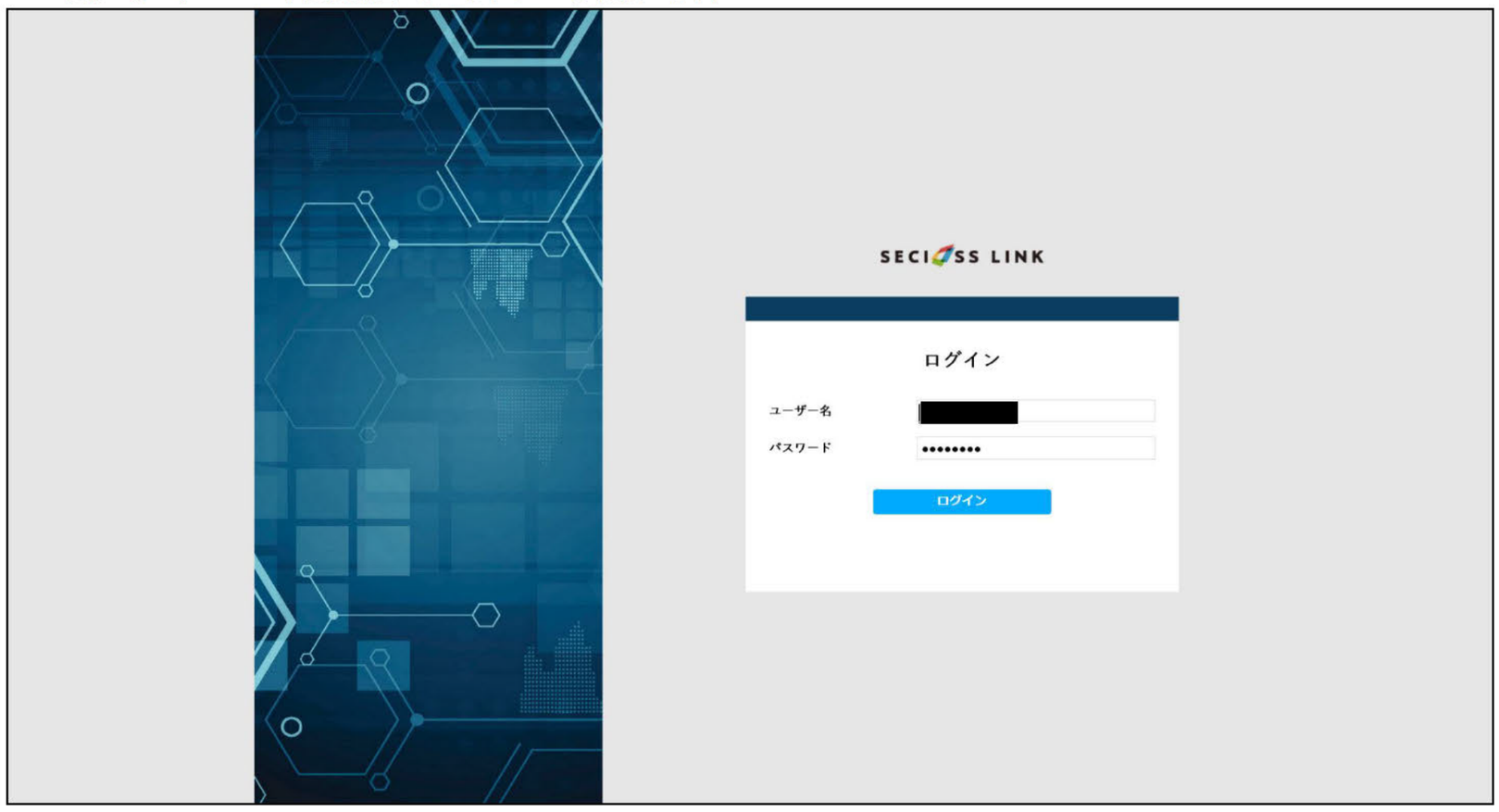
■設定反映

systemctl restart httpd

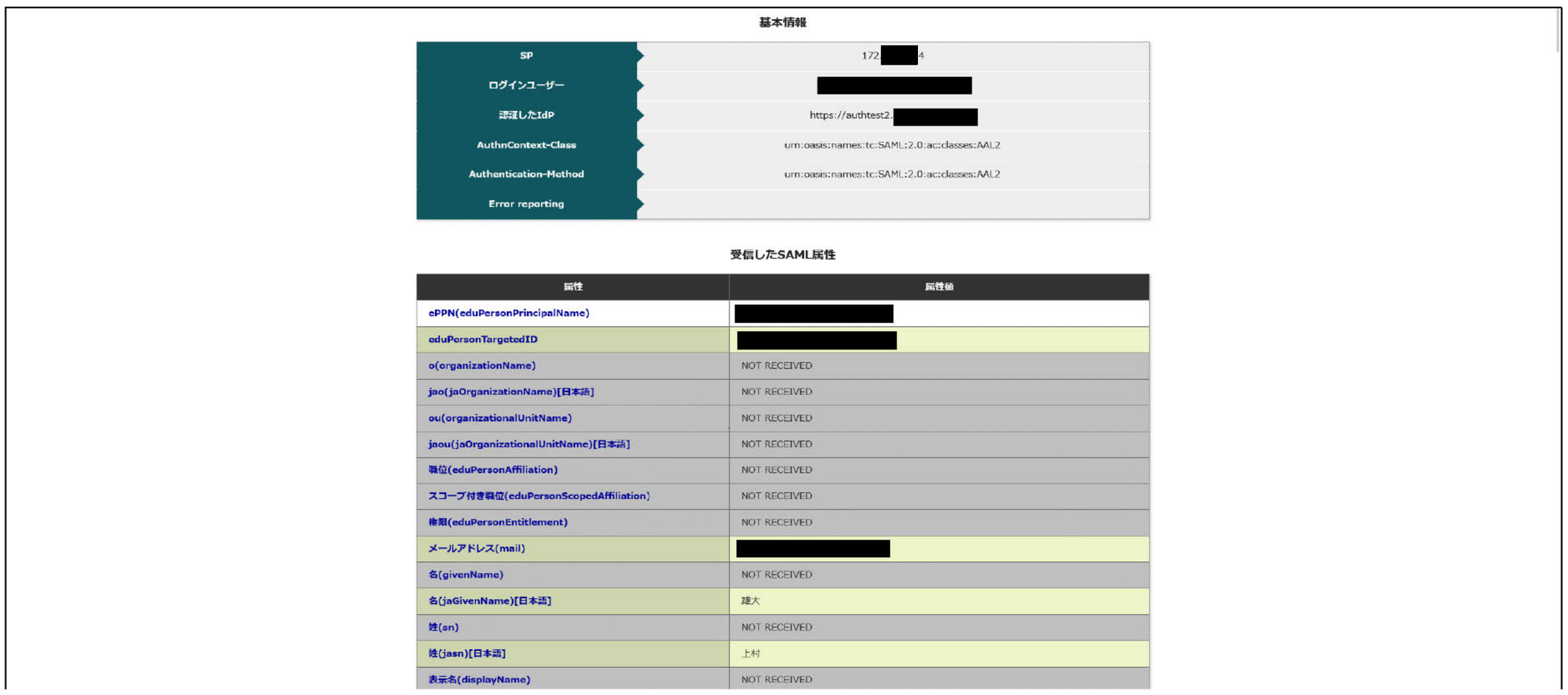
3. IdPにてSP01のSAMLリクエスト、レスポンスに含むAuthnContextClassRefに関する動作設定を行う。
   SAMLリクエスト時の認証動作を「AuthnContextClassRefを無視する」に設定。
   SAMLレスポンスに設定する値を「既定の動作」に設定。




4. SP01にアクセスし、SAMLによるログインを行う。
   IdP未認証状態で、「https://172.20.250.4/secure/index.php」 にブラウザでアクセスする。
   IdPに遷移し、ID/パスワード認証認証が求められるため、認証を行う。




すべての認証を成功したのち、SPへアクセスが行える。
AAL2を受信しているが、AuthnContextClassRefを無視する設定が入っているため、IdPの認証ルール＋アクセス権限設定の認証としてID/パスワード認証のみが求められる。
ID/パスワード認証のみ行った状態だが、SAMLレスポンスとしての動作が既定の動作であるため、受信したAuthnContextClassRefで返却している。



基本情報

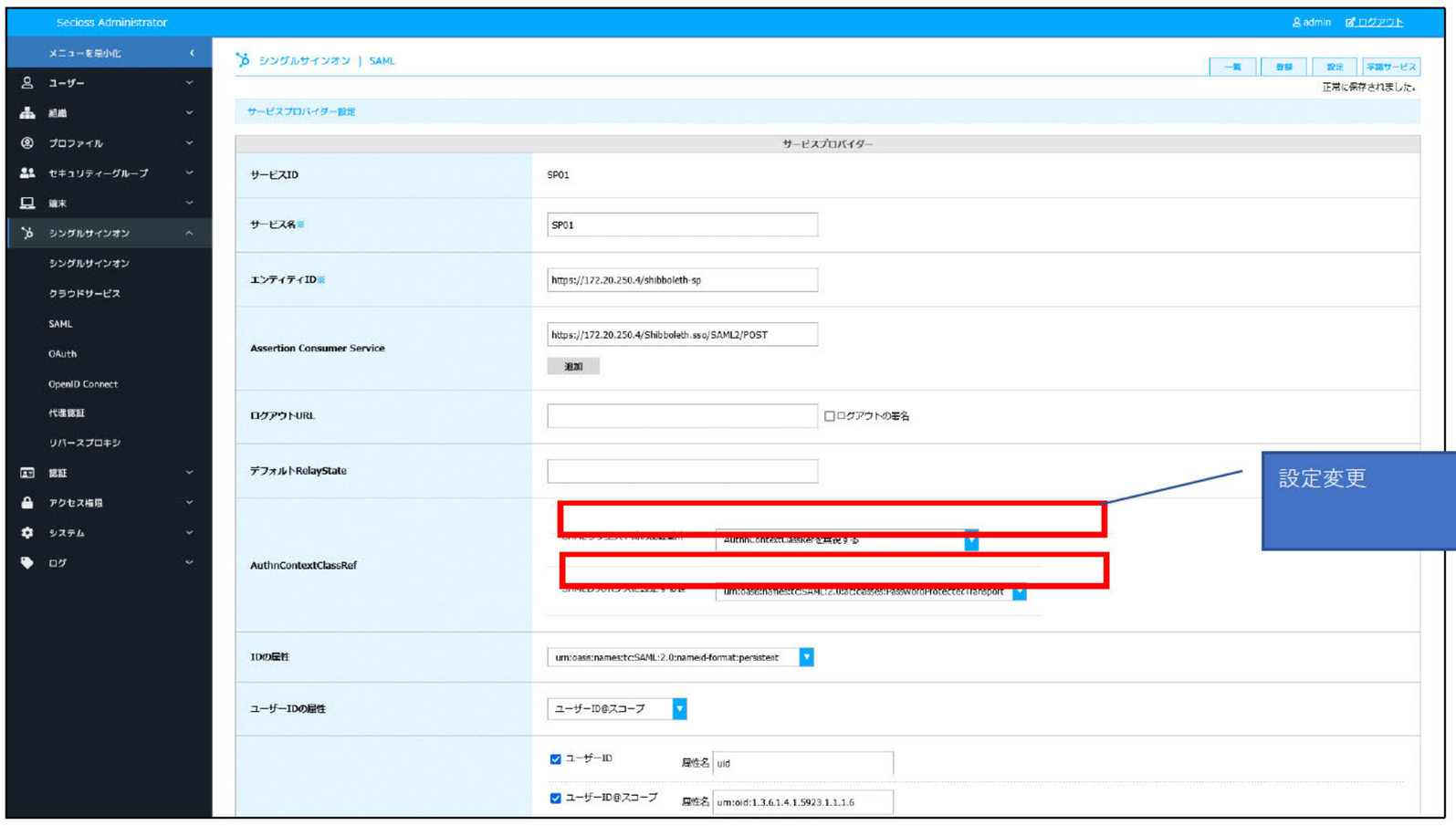
| | |
|---|---|
| SP | 172.[redacted]4 |
| ログインユーザー | [redacted] |
| 認証したIdP | https://authtest2.[redacted] |
| AuthnContext-Class | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Authentication-Method | urn:oasis:names:tc:SAML:2.0:ac:classes:AAL2 |
| Error reporting | |

受信したSAML属性

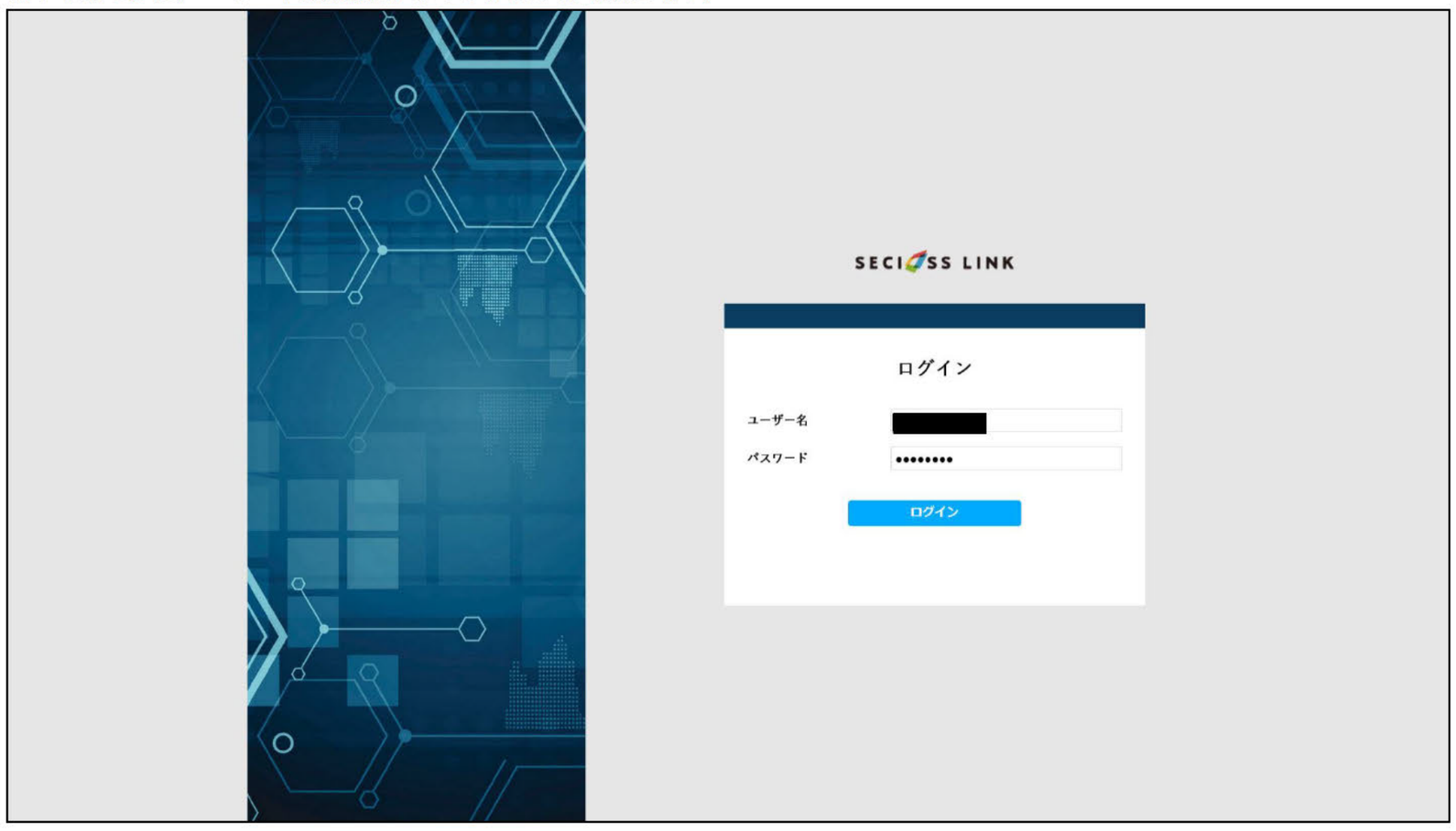
| 属性 | 属性値 |
|---|---|
| ePPN(eduPersonPrincipalName) | [redacted] |
| eduPersonTargetedID | [redacted] |
| o(organizationName) | NOT RECEIVED |
| jao(jaOrganizationName)[日本語] | NOT RECEIVED |
| ou(organizationalUnitName) | NOT RECEIVED |
| jaou(jaOrganizationalUnitName)[日本語] | NOT RECEIVED |
| 職位(eduPersonAffiliation) | NOT RECEIVED |
| スコープ付き職位(eduPersonScopedAffiliation) | NOT RECEIVED |
| 権限(eduPersonEntitlement) | NOT RECEIVED |
| メールアドレス(mail) | [redacted] |
| 名(givenName) | NOT RECEIVED |
| 名(jaGivenName)[日本語] | 雄大 |
| 姓(sn) | NOT RECEIVED |
| 姓(jasn)[日本語] | 上村 |
| 表示名(displayName) | NOT RECEIVED |

| | |
|---|---|
| 表示名(jaDisplayName)[日本語] | NOT RECEIVED |
| gakuninScopedPersonalUniqueCode | NOT RECEIVED |
| isMemberOf | NOT RECEIVED |
| eduPersonAssurance | NOT RECEIVED |
| eduPersonUniqueId | NOT RECEIVED |

5. IdPにてSP01のSAMLリクエスト、レスポンスに含むAuthnContextClassRefに関する動作設定を行う。
   SAMLリクエスト時の認証動作を「AuthnContextClassRefを無視する」に設定。
   SAMLレスポンスに設定する値を「urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport」に設定。




6. SP01にアクセスし、SAMLによるログインを行う。
   IdP未認証状態で、「https://172.20.250.4/secure/index.php」 にブラウザでアクセスする。
   IdPに遷移し、ID/パスワード認証認証が求められるため、認証を行う。




すべての認証を成功したのち、SPへアクセスが行える。
AAL2を受信しているが、AuthnContextClassRefを無視する設定が入っているため、IdPの認証ルール＋アクセス権限設定の認証としてID/パスワード認証のみが求められる。
AAL2で求められるワンタイムパスワード認証はSAMLレスポンスとしての動作が「urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport」であるため行わず、
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransportで返却している。

**基本情報**

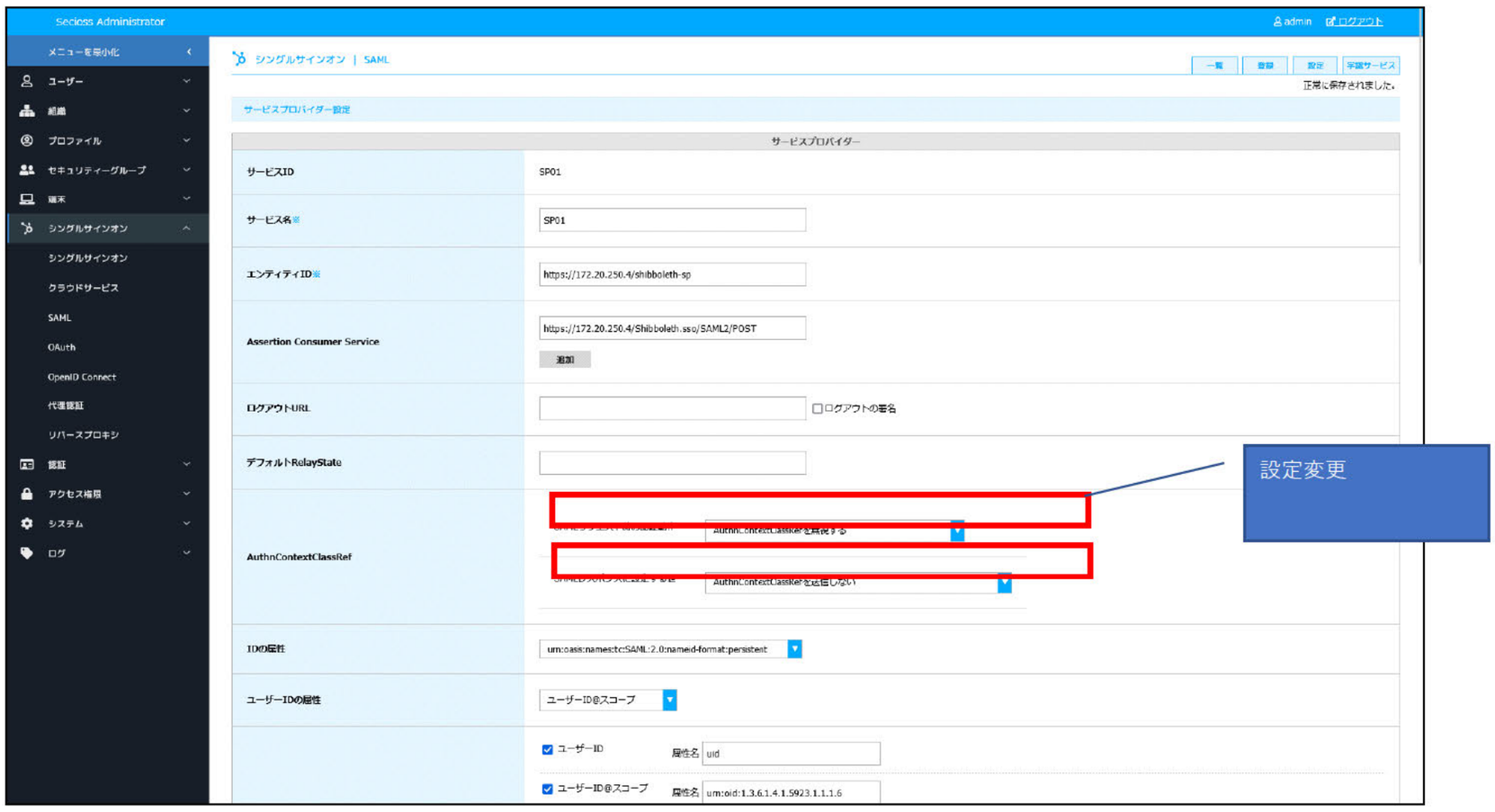
| | |
|---|---|
| SP | 172[redacted].4 |
| ログインユーザー | [redacted] |
| 認証したIdP | https://authtest2.iimc.kyoto-u.ac.jp |
| AuthnContext-Class | urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport |
| Authentication-Method | urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport |
| Error reporting | |

**受信したSAML属性**

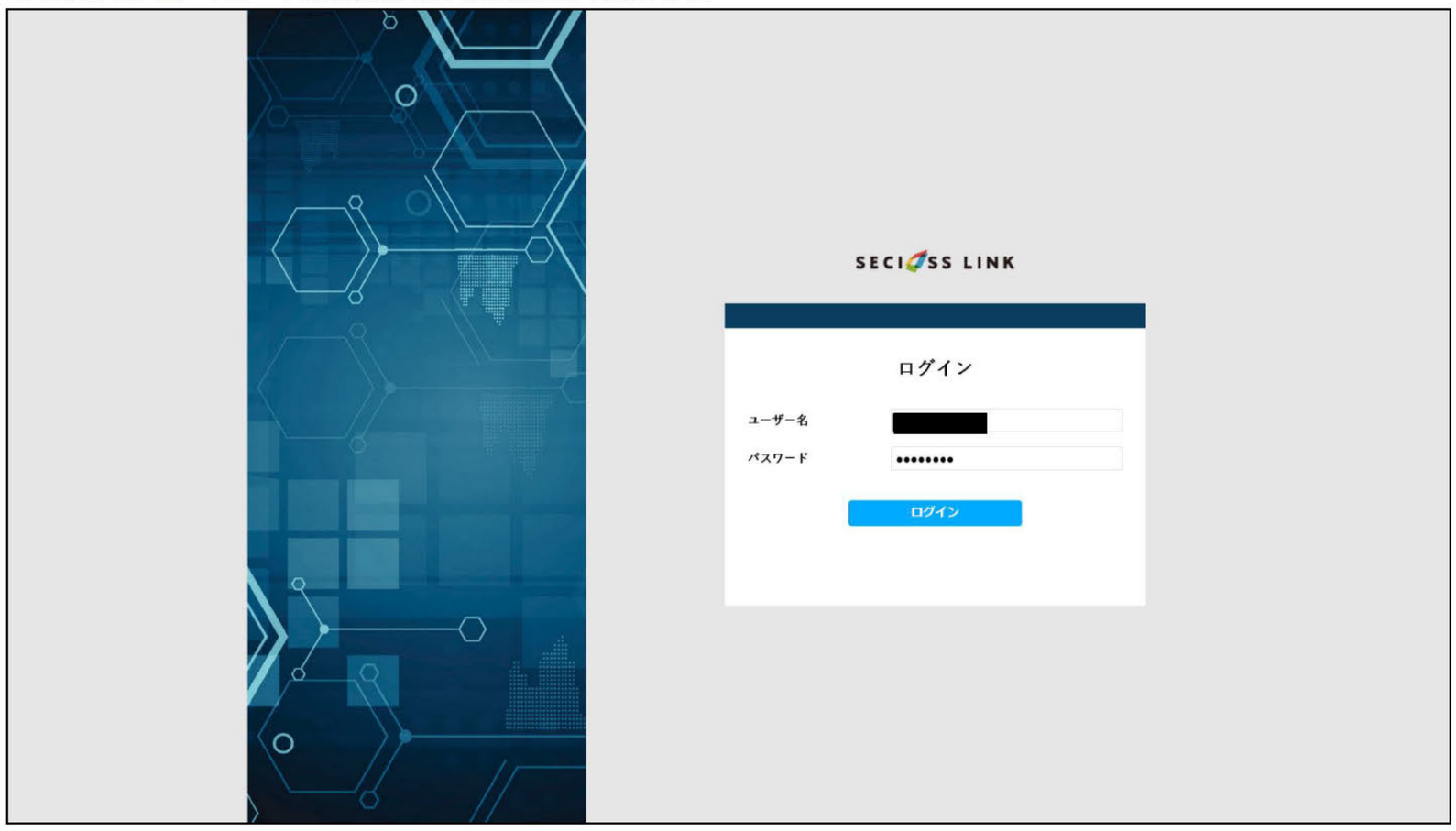
| 属性 | 属性値 |
|---|---|
| ePPN(eduPersonPrincipalName) | [redacted] |
| eduPersonTargetedID | [redacted] |
| o(organizationName) | NOT RECEIVED |
| jao(jaOrganizationName)[日本語] | NOT RECEIVED |
| ou(organizationalUnitName) | NOT RECEIVED |
| jaou(jaOrganizationalUnitName)[日本語] | NOT RECEIVED |
| 職位(eduPersonAffiliation) | NOT RECEIVED |
| スコープ付き職位(eduPersonScopedAffiliation) | NOT RECEIVED |

| | |
|---|---|
| 権限(eduPersonEntitlement) | NOT RECEIVED |
| メールアドレス(mail) | [redacted] |
| 名(givenName) | NOT RECEIVED |
| 名(jaGivenName)[日本語] | [redacted] |
| 姓(sn) | NOT RECEIVED |
| 姓(jasn)[日本語] | [redacted] |
| 表示名(displayName) | NOT RECEIVED |
| 表示名(jaDisplayName)[日本語] | NOT RECEIVED |
| gakuninScopedPersonalUniqueCode | NOT RECEIVED |
| isMemberOf | NOT RECEIVED |
| eduPersonAssurance | NOT RECEIVED |
| eduPersonUniqueId | NOT RECEIVED |

7. IdPにてSP01のSAMLリクエスト、レスポンスに含むAuthnContextClassRefに関する動作設定を行う。
   SAMLリクエスト時の認証動作を「AuthnContextClassRefを無視する」に設定。
   SAMLレスポンスに設定する値を「AuthnContextClassRefを送信しない」に設定。




6. SP01にアクセスし、SAMLによるログインを行う。
   IdP未認証状態で、「https://172.20.250.4/secure/index.php」 にブラウザでアクセスする。
   IdPに遷移し、ID/パスワード認証認証が求められるため、認証を行う。




すべての認証を成功したのち、SPへアクセスが行える。
AAL2を受信しているが、AuthnContextClassRefを無視する設定が入っているため、IdPの認証ルール＋アクセス権限設定の認証としてID/パスワード認証のみが求められる。
AAL2で求められるワンタイムパスワード認証はSAMLレスポンスとしての動作が「AuthnContextClassRefを送信しない」であるため行わず、
SAMLレスポンスにAuthnContextClassRefの定義が行われない。Shibboleth SPはAuthnContextClassRefが返却されることを期待しているため、SPでエラーとなる。

**xmltooling::ValidationException**

The system encountered an error at Thu Mar 23 12:42:41 2023

To report this problem, please contact the site administrator at root@localhost.

Please include the following message in ary email:

**xmltooling::ValidationException at (https://172.20.250.4/Shibboleth.sso/SAML2/POST)**

AuthnStatement must have AuthnContext.