OpenAM 14 アダプティブリスク認証モジュール 利用手順書

OSSTech 株式会社

更新日	2022 年 7 月 14 日
リビジョン	1.2

目次

1 はじめに

本文書は、OSSTech 版 OpenAM14 に含まれるアダプティブリスク認証モジュールの利用手順書です。

1.1 機能概要

アダプティブリスク認証モジュールの機能について説明します。

アダプティブリスク認証モジュールは、認証するユーザーの要素からリスクスコアを計算し、スコアがリスクしきい値に達した場合に認証失敗とするモジュールです。データストア認証や OpenLDAP 認証といった認証モジュールに合わせ、リスクの高いときには HOTP 認証や ForgeRock Authenticator (OATH) 認証などの追加認証を行ったり、WebAuthn（登録）認証などのモジュールの前段に配置し、リスクの高いときには登録を拒否することができます。また、リスクの高いログインが成功した際、事前に登録されたユーザーのアドレス宛てにメールを送信することも可能です。

1.2 リスク評価の種類

アダプティブリスク認証で評価できるリスクの種類を示します。

【種類】	【評価内容】
認証失敗	前回の認証時パスワードミスなどによって、ユーザーが特定された上で認証を失敗していた場合、リスクが高いと評価します。
IP アドレスレンジ	指定された IP レンジとクライアントの IP アドレスを比較し、クライアントの IP アドレスが IP レンジの範囲外である場合、リスクが高いと評価します。
IP アドレス履歴	ユーザープロファイルの指定された属性に格納されている IP アドレスの履歴リストとクライアントの IP アドレスを比較し、クライアントの IP アドレスが履歴リストに含まれていない場合、リスクが高いと評価します。属性名は任意の名前を使用でき、属性値は|(パイプ) で区切って複数の IP アドレスを定義することができます。(例：`192.168.0.1|192.168.0.2`)。

【種類】	【評価内容】
既知の Cookie	クライアントリクエストが指定された Cookie 名の Cookie を保持していない場合、またはその Cookie 値が指定された Cookie 値と一致しない場合、リスクが高いと評価します。
デバイス登録 Cookie	クライアントリクエストが指定された Cookie 名のデバイス登録識別子 Cookie を保持していない場合、リスクが高いと評価します。デバイス登録識別子 Cookie とは、User-Agent や Accept-* 系のリクエスト HTTP ヘッダー、ユーザー ID などを暗号化した値で、認証成功時に OpenAM が設定します。
最終ログインからの経過時間	指定された Cookie をもとに計算された前回ログイン時からの経過時間が指定された期限を過ぎていた場合、または Cookie がセットされていない場合、リスクが高いと評価します。ログイン成功時に暗号化されたログイン時刻が Cookie にセットされます。
プロファイル属性	指定された属性値と、指定された属性名に対応するユーザープロファイルの属性値が一致しない場合、リスクが高いと評価します。ただし、属性値の指定がされていないときには、指定された属性名の属性がユーザープロファイルに存在しない場合にリスクが高いと評価します。
位置情報	クライアントの IP アドレスから判別された国コードが、指定された有効な国コードのリストに含まれていない場合、リスクが高いと評価します。
位置情報履歴	クライアントの IP アドレスから判別された国コードが、ユーザープロファイルの指定された属性内のリストに含まれていない場合、リスクが高いと評価します。
リクエストヘッダー	指定されたリクエストヘッダーの値と、指定されたリクエストヘッダー名に対応する実際のリクエストヘッダーの値が一致しない場合、リスクが高いと評価します。ただし、リクエストヘッダーの値が指定されていないときには、指定されたリクエストヘッダー名のヘッダーが実際のリクエストヘッダーに存在しない場合にリスクが高いと評価します。

2 事前準備

認証モジュールを使用するためには、以下の事前準備が必要です。

- OpenAM の初期設定
- 追加の認証などに利用する認証モジュールの設定
- （ユーザープロファイルを参照するリスク評価をする場合のみ）アダプティブリスク認証で利用する属性の設定
- （認証失敗チェックを利用する場合のみ）アカウントロックアウトの設定
- （位置情報チェックまたは位置情報履歴チェックを利用する場合のみ）位置情報データベースの取得
- （警告メールを送信する場合のみ）電子メールサービスの設定
- （ログイン時に LDAP 属性の更新や Cookie のセットなどが必要なリスク評価をする場合のみ）認証ポストプロセスクラスの設定

上記のうち、「OpenAM の初期設定」と「追加の認証などに利用する認証モジュールの設定」、「アダプティブリスク認証で利用する属性の設定」に関しては、アダプティブリスク認証に限った特別な設定ではないため説明を省略します。

2.1 アカウントロックアウトの設定

認証失敗を評価するためには、ユーザーの認証失敗回数を記録するように設定を変更する必要があります。デフォルト設定では認証失敗回数が記録されないため、前回認証時に認証失敗していた場合も必ずリスクが低いと評価されます。認証失敗回数の記録は、アカウントロックアウト機能によって行われます。アカウントロックアウトに関する設定は、OpenAM 管理コンソールの「認証」→「設定」の「アカウントロック」タブで行います。

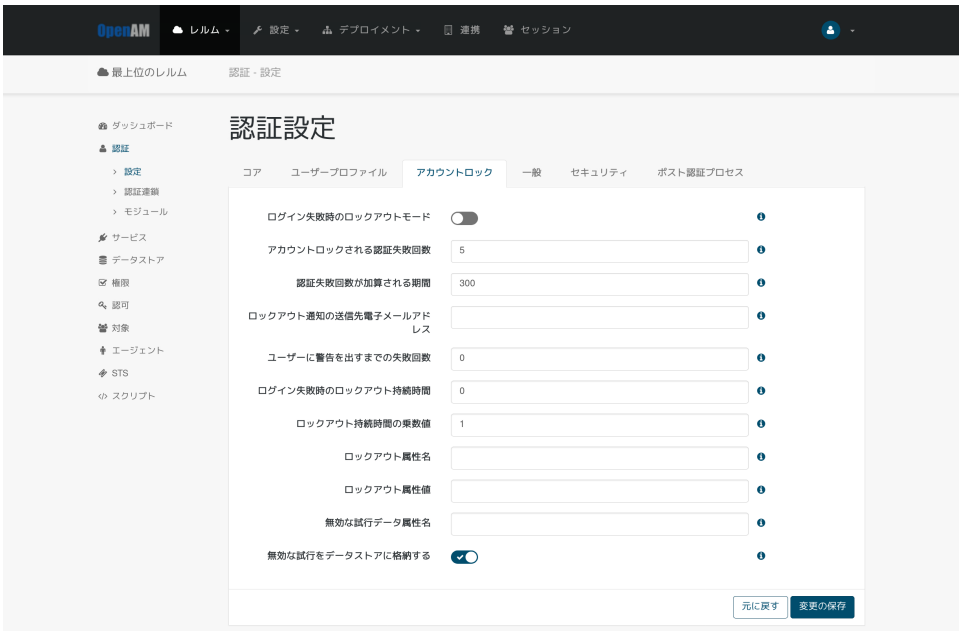

図 1　アカウントロックアウト設定

アカウントロックアウト機能を有効にするため、「ログイン失敗時のロックアウトモード」設定を「有効」にします。

アカウントロックアウトには、ロックアウト情報をメモリに保存する方式とユーザーデータストアに保存する方式があります。「無効な試行をデータストアに格納する」が有効な場合はデータストアに保存され、無効な場合はメモリに保存されます。OpenAM が複数台で構成されている場合や OpenAM を再起動した場合などに、保存方式によって認証失敗チェックの挙動が変わる可能性があります。アカウントロックについての詳細は管理者マニュアルを参照してください。

2.2 位置情報データベースの取得

位置情報データベースには MaxMind のバイナリ形式の国データベースを使用します。データベースには有償版と無償版があり、それぞれ以下から詳細を確認することができます。

- GeoIP2 Country Database（有償版） - https://www.maxmind.com/en/geoip2-country-database
- GeoLite2 Free Geolocation Data（無償版）- https://dev.maxmind.com/geoip/geoip2/geolite2/

ここでは、無償版の GeoLite2 の国データベースを使用します。有償版を使用する際は、適宜読み替えてください。

1. MaxMind にログイン後、GZIP 形式で圧縮されている GeoLite2 のバイナリ形式の国データベースを取得します。（必要であればアカウントを作成してください。）
2. データベースを展開します。

```
$ tar -xvzf GeoLite2-Country_XXXXXXXX.tar.gz
$ ls GeoLite2-Country_XXXXXXXX/
> COPYRIGHT.txt  GeoLite2-Country.mmdb  LICENSE.txt
```

3. 2. で取得したデータベースを任意のパスに配置後、OpenAM で利用できるように必要に応じてパーミッションを変更します。 以下は/opt/osstech/var/lib/openam/database 配下にデータベースを配置する場合の例です。

```
# mkdir -p /opt/osstech/var/lib/openam/database
# cp /path/to/database/GeoLite2-Country_XXXXXXXX/GeoLite2-Country.mmdb \
    /opt/osstech/var/lib/openam/database
# chown -R root:tomcat /opt/osstech/var/lib/openam/database
# chmod 750 /opt/osstech/var/lib/openam/database
# chmod 440 /opt/osstech/var/lib/openam/database/GeoLite2-Country.mmdb
```

2.3 電子メールサービスの設定

環境に合わせて設定を変更してください。

1. OpenAM の管理コンソールにログイン後、対象のレルムを選択します。
2.「サービス」を開き、「サービスの追加」を押下します。

図 2　サービス画面

3.「サービスタイプを選択」に **電子メールサービス**を設定し、「作成」を押下します。

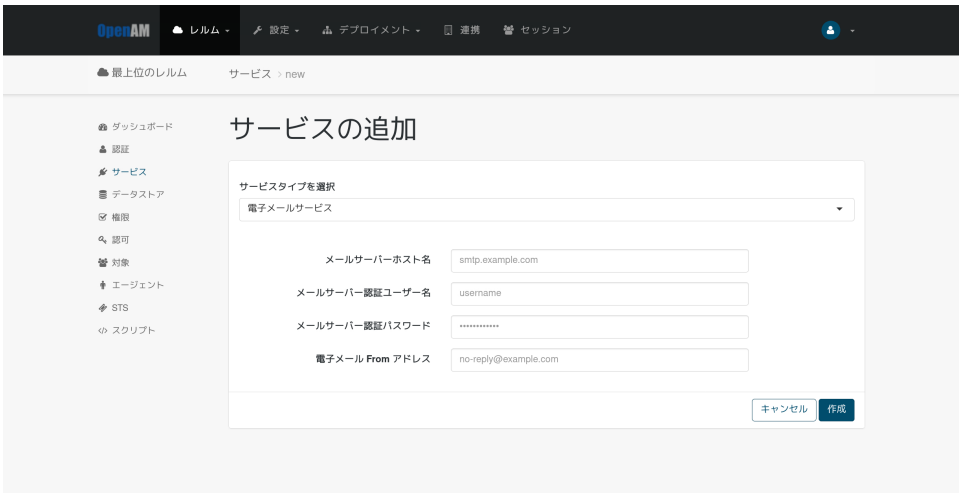

図 3　サービスの追加

4. それぞれの項目を設定します。
   なお、「電子メール From アドレス」と「電子メール属性名」はアダプティブリスク認証モジュールの設定が反映されるため、ここに設定する必要はありません。「アダプティブリスク認証モジュールの設定」の「警告メール」タブの「From アドレス」と「メールアドレス属性名」にそれぞれ設定してください。また、「電子メールの件名」と「電子メールの内容」はアダプティブリスク認証モジュールのプロパティファイルの設定が反映されるため、設定する必要はありません。警告メールの件名および本文についての設定方法は「警告メールの件名と本文の設定」を参照してください。

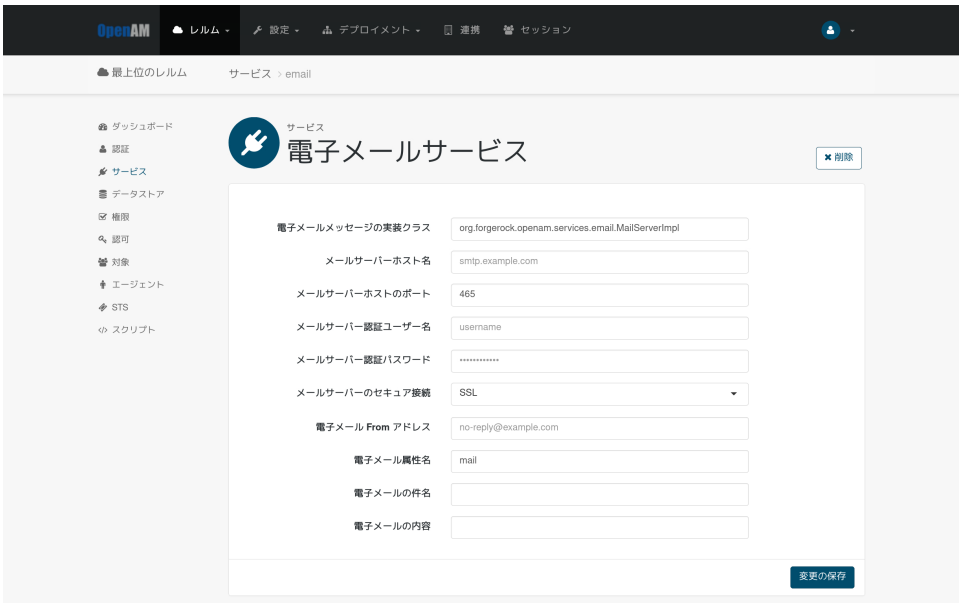

図 4　電子メールサービス設定

以下が設定例です。

【項目名】	【設定例】
電子メールメッセージの実装クラス	org.forgerock.openam.services.email.MailServerImpl
メールサーバーホスト名	localhost
メールサーバーホストのポート	25
メールサーバー認証ユーザー名	（空欄）
メールサーバー認証パスワード	（空欄）
メールサーバーのセキュア接続	Non SSL
電子メール From アドレス	（設定する必要はありません）
電子メール属性名	（設定する必要はありません）
電子メールの件名	（設定する必要はありません）
電子メールの内容	（設定する必要はありません）

5.「変更の保存」を押下します。

2.4 認証ポストプロセスクラスの設定

以下の条件で利用する場合、この設定が必要です。

- IP アドレス履歴を評価し、ログイン成功時に IP アドレスをユーザープロファイル属性に格納する。
- 既知の Cookie を評価し、ログイン成功時に指定された Cookie をクライアントへのレスポンスにセットする。
- デバイス登録識別子 Cookie を評価し、ログイン成功時にデバイス登録識別子 Cookie をクライアントへのレスポンスにセットする。
- 最終ログインからの経過時間を評価し、ログイン成功時に最終ログイン時間の Cookie をクライアントへのレスポンスにセットする。
- 位置情報履歴を評価し、ログイン成功時に国コードをユーザープロファイル属性に格納する。
- リスクの高いログイン成功時に警告メールを送信する。

設定方法は以下の通りです。

1. OpenAM の管理コンソールにログイン後、対象のレルムを選択します。
2. 「認証」→「設定」に移動し、「ポスト認証プロセス」タブを開きます。
3. 「認証ポストプロセスクラス」に `org.forgerock.openam.authentication.modules.adaptive.Adaptive` を設定し、「変更の保存」を押下します。

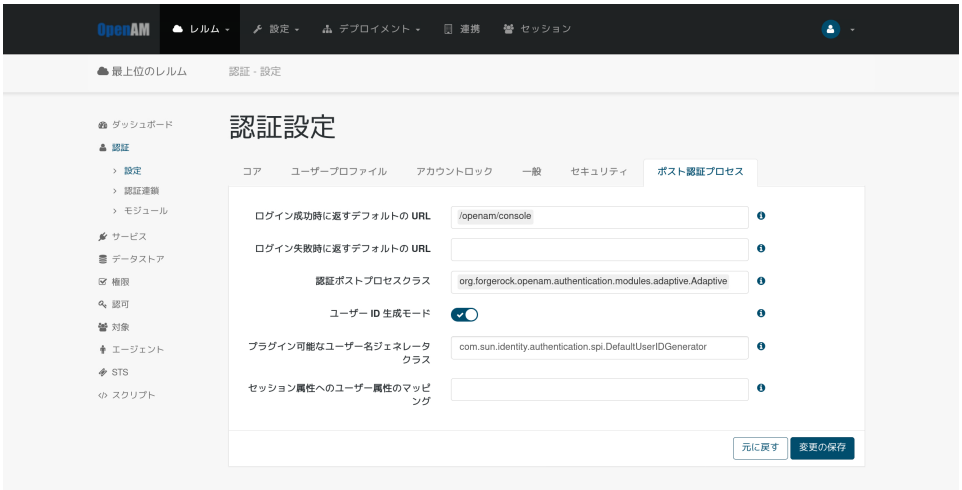

図 5　認証ポストプロセスクラスの設定

3 リスクの高いログインに対し追加認証をする

ここでは、アダプティブリスク認証モジュールでリスクが高いと評価されたときに追加の認証を求めるための設定方法を説明します。

3.1 認証モジュールと認証連鎖の設定

下図のように、アダプティブリスク認証でリスクが高いと評価され、その後ログイン成功した際に警告メールを送信する場合の設定方法を記述します。また、リスク評価は位置情報履歴チェックで行い、追加の認証は ForgeRock Authenticator (OATH) 認証をするものとします。

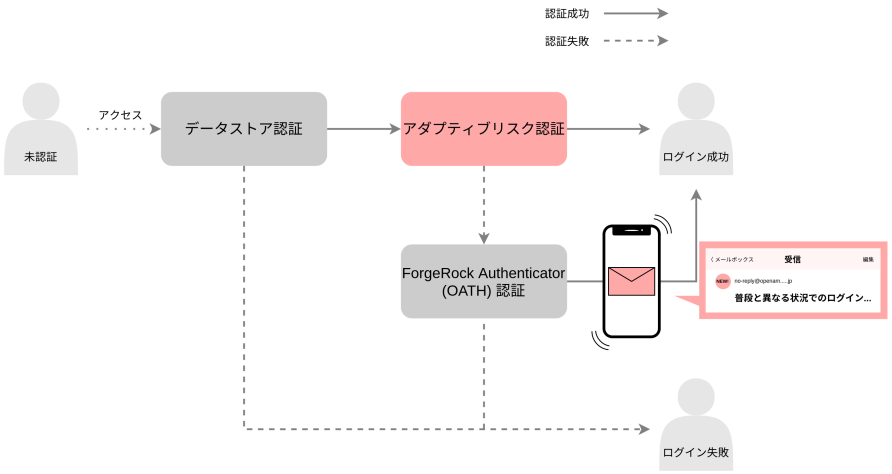

図 6　認証フロー

3.1.1 認証モジュールの追加

1. OpenAM の管理コンソールにログイン後、対象のレルムを選択します。
2. 「認証」→「モジュール」に移動し、「モジュールの追加」を押下します。
3. 「名前」に認証モジュール名 (ここでは `adaptiveRisk`) を入力し、「種類」のドロップダウンリストから**アダプティブリスク** を選択します。

図 7　アダプティブリスク認証モジュールの作成

4. 「作成」を押下し、認証モジュールの設定画面に移動します。
5. 変更する設定は「位置情報（共通）」、「位置情報履歴」、「警告メール」タブにある設定です。
   それぞれの設定の詳細は「アダプティブリスク認証モジュールの設定」を参照してください。ここでは動作確認にあたり最低限変更が必要な設定のみ記述します。

【設定場所】	【項目名】	【設定例】
位置情報（共通）	位置情報データベースの場所	/opt/osstech/var/lib/openam/database/GeoLite2-Country.mmdb
位置情報履歴	位置情報履歴チェック	有効
位置情報履歴	履歴属性名	description
位置情報履歴	成功したロケーションを保存	有効
警告メール	リスクの高いログイン成功に対して警告メールを送信する	有効

3.1.2 認証連鎖の追加

1. OpenAM の管理コンソールにログイン後、対象のレルムを選択します。
2. 「認証」→「認証連鎖」に移動し、「認証連鎖の追加」を押下します。

3.「名前」に任意の認証連鎖名（ここでは adaptiveRiskService）を入力し、「作成」を押下します。

図 8　認証連鎖の追加

4.「認証モジュールの追加」を押下し、「モジュールの選択」のドロップダウンリストから設定済みのデータストア認証モジュール (ここでは DataStore) を選択し、「基準の選択」のドロップダウンリストから Requisite を選択して「OK」を押下します。

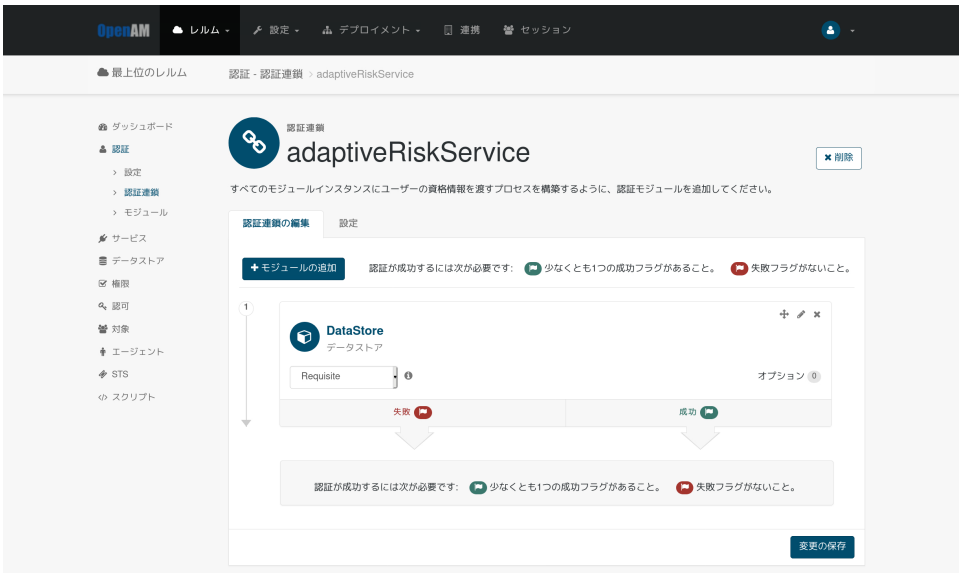

図 9　データストア認証モジュールの追加

5. 4．と同様にしてアダプティブリスク認証モジュール（ここでは adaptiveRisk）を Sufficient に設定します。

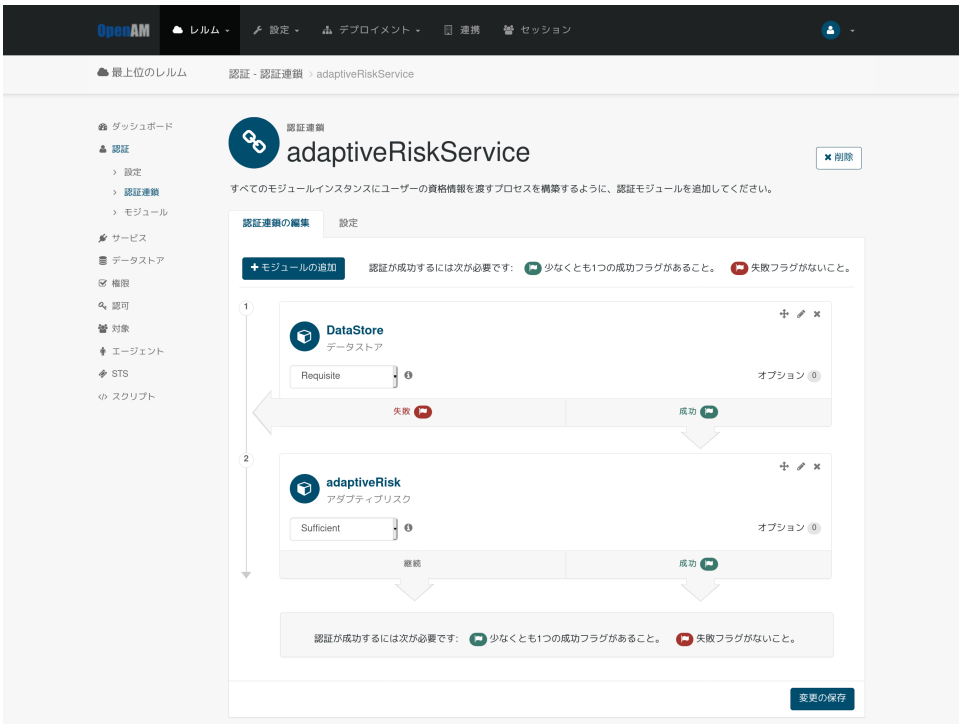

図 10　アダプティブリスク認証モジュールの追加

6. 4．と同様にして追加の認証として使用する ForgeRock Authenticator (OATH) 認証モジュール（ここでは `frOATH`）を `Required` に設定します。

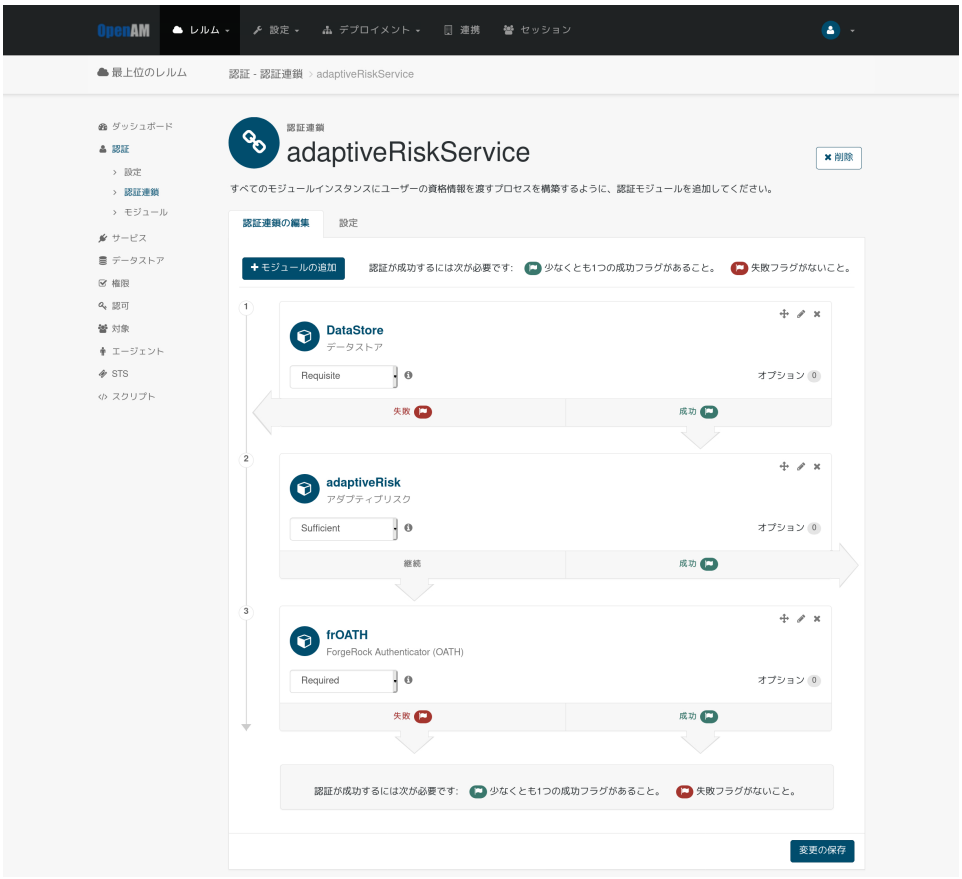

図 11　ForgeRock Authenticator (OATH) 認証モジュールの追加

7.「変更の保存」を押下します。
8.「認証」→「設定」に移動し、「組織認証設定」のドロップダウンリストから作成した認証連鎖（ここでは `adaptiveRiskService`）を選択し、「変更の保存」を押下します。

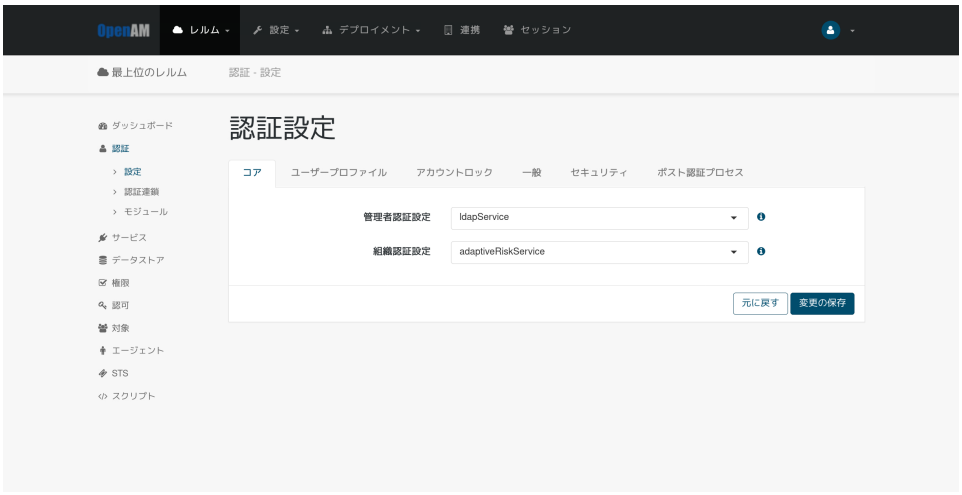

図 12　組織認証設定の変更

3.2 認証時の動作

ここでは「認証連鎖の追加」の例のように設定した場合の認証時の動作について説明します。

1. OpenAM にアクセスします。
2. 表示されたデータストア認証の画面で存在するユーザーの ID とパスワードを入力し、「ログイン」を押下します。

図 13　データストア認証

3. アダプティブリスク認証が失敗するため、ForgeRock Authenticator (OATH) 認証の画

面が表示されます。(現時点では「認証モジュールの追加」で位置情報タブの「履歴属性名」に指定した属性をユーザーが持っていないものとします。)

4. 3．で表示された画面に正しいワンタイムパスワードを入力し、「送信」を押下します。

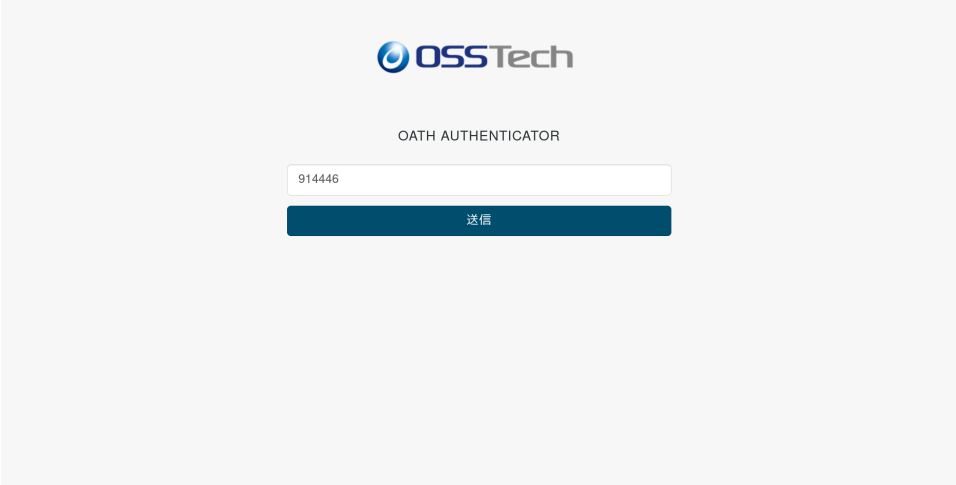

図 14　ForgeRock Authenticator (OATH) 認証

5. ログインが成功し、ユーザープロファイル画面に遷移します。

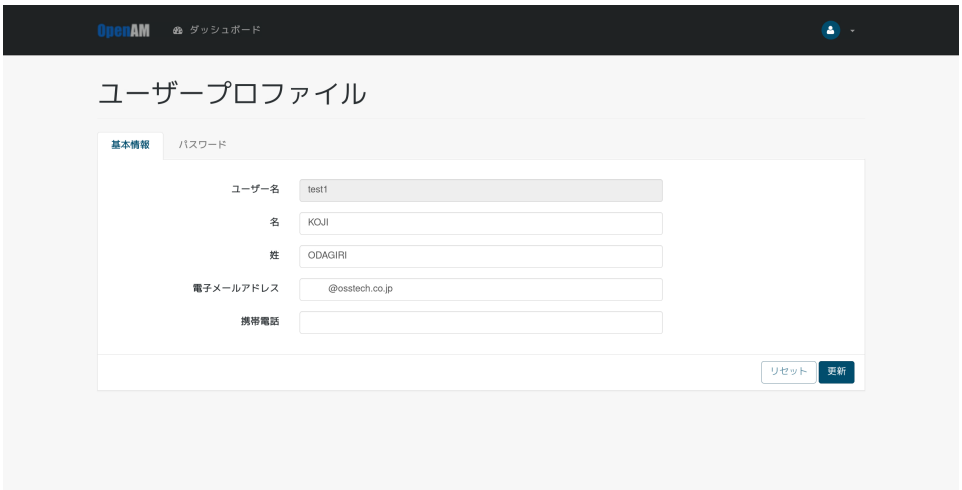

図 15　ユーザープロファイル画面

6. 3．でアダプティブリスク認証が失敗し、5．でログインが成功したため、ログインユーザーのメールアドレス宛てに警告メールが送信されます。

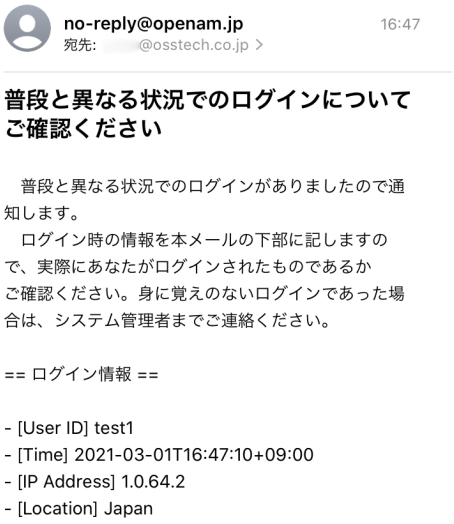

図 16　警告メール

7. 一度ログアウトし、再度 OpenAM にアクセスします。
8. 2．と同様にデータストア認証を行います。

図 17　データストア認証

9. 前回ログイン時に履歴属性が追加・更新されているためアダプティブリスク認証が成功し、ユーザープロファイル画面に遷移します。

図 18　ユーザープロファイル画面

4 モジュールの利用制限をする

アダプティブリスク認証は、WebAuthn（登録）認証モジュールなどの登録系モジュールの前段に配置して「IP アドレスレンジ」などを評価することによって登録系認証モジュールへの登録制限を行ったり、ForgeRock Authenticator (OATH) 認証モジュールなどの未登録の場合デバイス登録を促すようなモジュールの前段に配置して「プロファイル属性」を評価することによって未登録ユーザーの認証を拒否したりすることができます。

ここでは、登録系の認証モジュールの利用制限を行うための設定方法を説明します。

4.1 認証モジュールと認証連鎖の設定

下図のように、アダプティブリスク認証で IP レンジを評価し、社内ネットワークからのアクセスである（= リスクが低い）と評価した場合にのみ WebAuthn の認証デバイスを登録できるようにします。また、ユーザーの特定のため、データストア認証を利用するものとします。

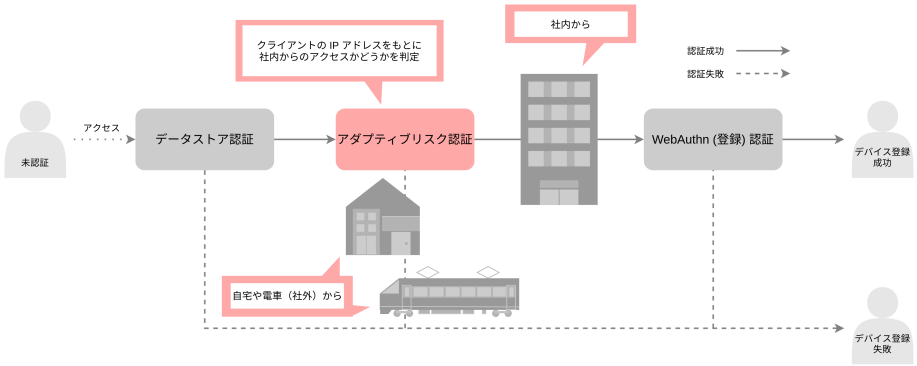

図 19　認証フロー

4.1.1 認証モジュールの追加

1. OpenAM の管理コンソールにログイン後、対象のレルムを選択します。
2. 「認証」→「モジュール」に移動し、「モジュールの追加」を押下します。
3. 「名前」に認証モジュール名（ここでは `internalNetwork`）を入力し、「種類」のドロップダウンリストから**アダプティブリスク** を選択します。

図 20　アダプティブリスク認証モジュールの作成

4. 「作成」を押下し、認証モジュールの設定画面に移動します。
5. 変更する設定は「一般」、「IP アドレスレンジ」タブにある設定です。
   それぞれの設定の詳細は「アダプティブリスク認証モジュールの設定」を参照してください。ここでは動作確認にあたり最低限変更が必要な設定のみ記述します。また、ユーザーが社内ネットワーク以外からアクセスした際に、社内ネットワークからのアクセス時のみ登録を受け付ける旨を伝えるため、「認証失敗時のエラーメッセージコードの設定」をプロパティキー「internalNetworkOnly」、プロパティ値「社内ネットワークからアクセスしてください。」で行うものとします。

【設定場所】	【項目名】	【設定例】
一般	認証失敗時のエラーメッセージコード	internalNetworkOnly
IP アドレスレンジ	IP レンジチェック	有効
IP アドレスレンジ	IP レンジ	10.0.0.0/24[*1]

4.1.2 認証連鎖の追加

1. OpenAM の管理コンソールにログイン後、対象のレルムを選択します。
2. 「認証」→「認証連鎖」に移動し、「認証連鎖の追加」を押下します。
3. 「名前」に任意の認証連鎖名（ここでは `registerService`）を入力し、「作成」を押下

[*1] 社内ネットワークからのアクセスであると判定する IP アドレスの範囲を指定します

します。

図 21　認証連鎖の追加

4. 「認証モジュールの追加」を押下し、「モジュールの選択」のドロップダウンリストから設定済みのデータストア認証モジュール (ここでは DataStore) を選択し、「基準の選択」のドロップダウンリストから Requisite を選択して「OK」を押下します。

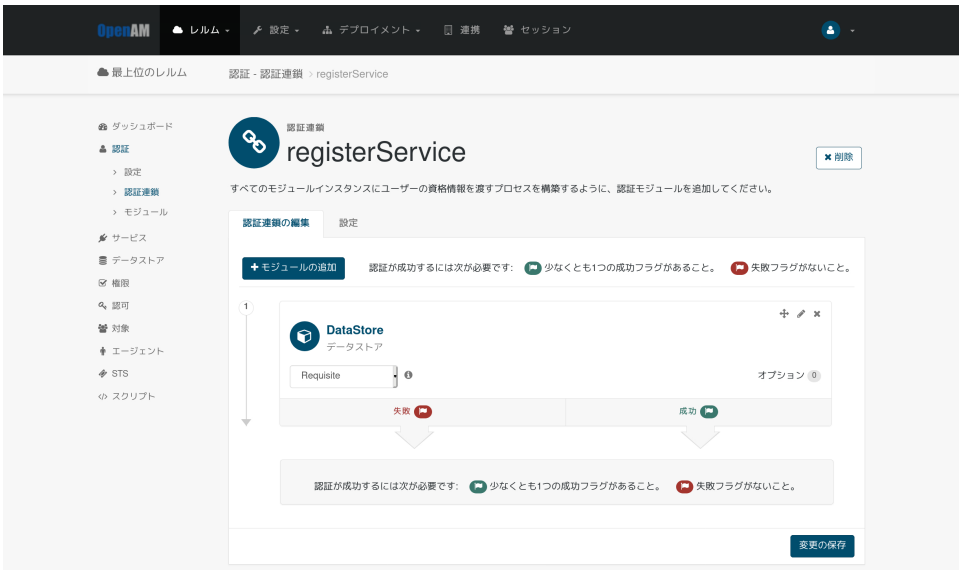

図 22　データストア認証モジュールの追加

5. 4. と同様にしてアダプティブリスク認証モジュール（ここでは internalNetwork）を Requisite に設定します。

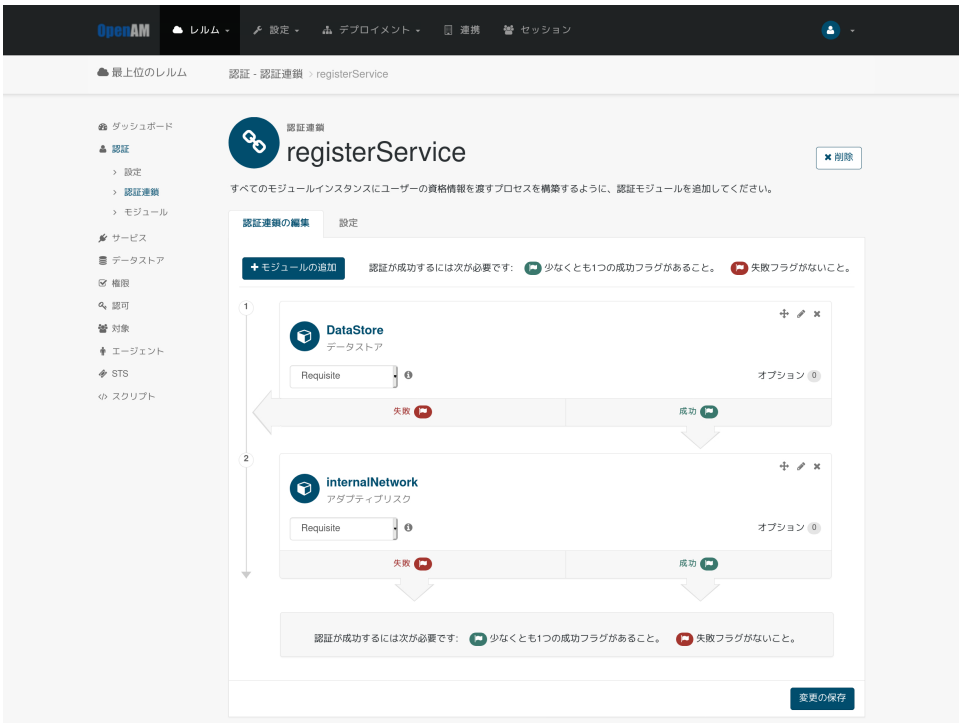

図 23　アダプティブリスク認証モジュールの追加

6. 4．と同様にして WebAuthn（登録）認証モジュール（ここでは `register`）を `Required` に設定します。

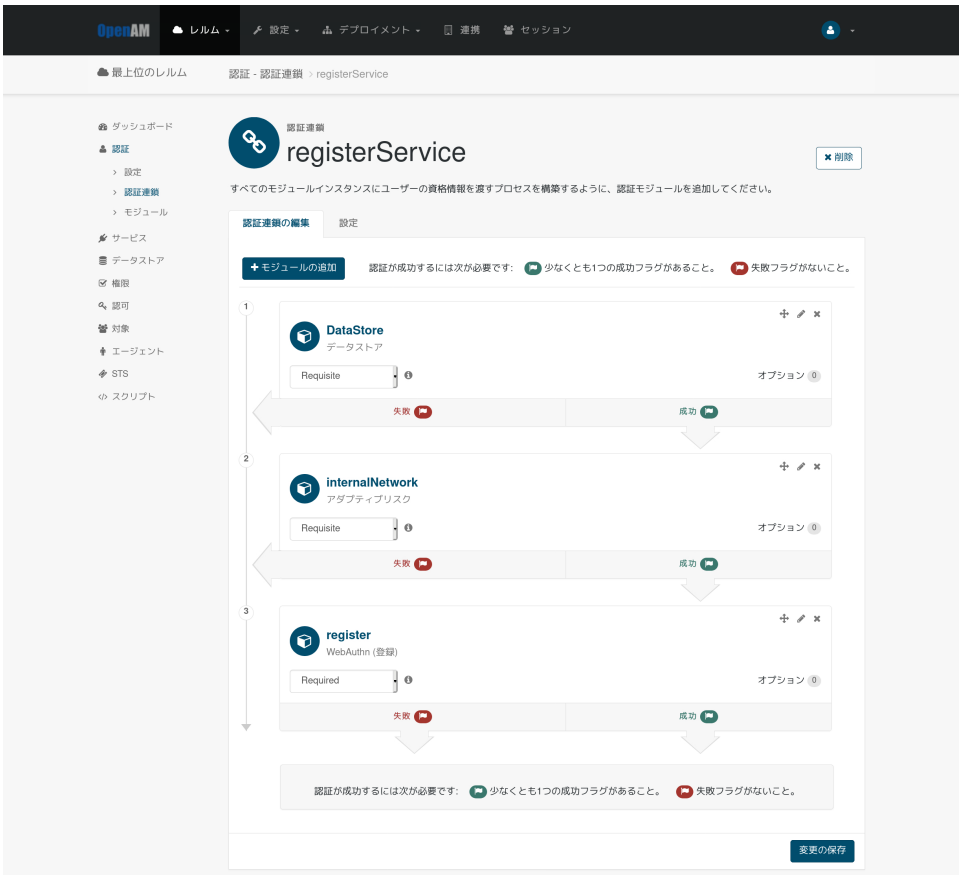

図 24　WebAuthn（登録）認証モジュールの追加

7.「変更の保存」を押下します。
8.「認証」→「設定」に移動し、「組織認証設定」のドロップダウンリストから作成した認証連鎖（ここでは `registerService`）を選択し、「変更の保存」を押下します。

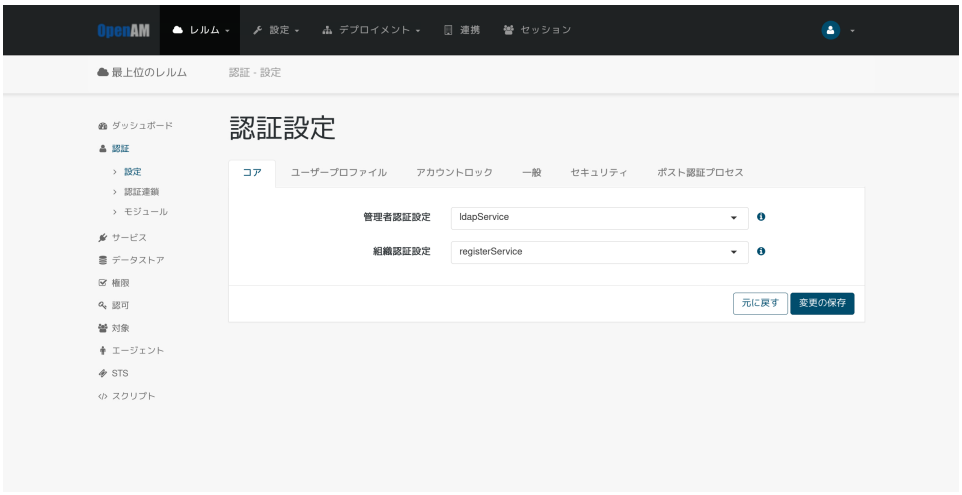

図 25　組織認証設定の変更

4.2 認証時の動作

ここでは「認証連鎖の追加」の例のように設定した場合の認証時の動作について説明します。

- 社内ネットワークからアクセスする場合
  1. OpenAM にアクセスします。
  2. 表示されたデータストア認証の画面で存在するユーザーの ID とパスワードを入力し、「ログイン」を押下します。

図 26　データストア認証

  3. アダプティブリスク認証が成功するため、WebAuthn（登録）認証の画面が表示

されます。

図 27　WebAuthn（登録）認証

4. 認証デバイスを操作して登録します。
5. ログインが成功し、ユーザープロファイル画面に遷移します。

図 28　ユーザープロファイル画面

- 社外からアクセスする場合
  1. OpenAM にアクセスします。
  2. 表示されたデータストア認証の画面で存在するユーザーの ID とパスワードを入力し、「ログイン」を押下します。

図 29　データストア認証

3. アダプティブリスク認証が失敗するため、「認証モジュールの追加」で設定したエラーメッセージが表示されます。（認証デバイスの登録はできません。）

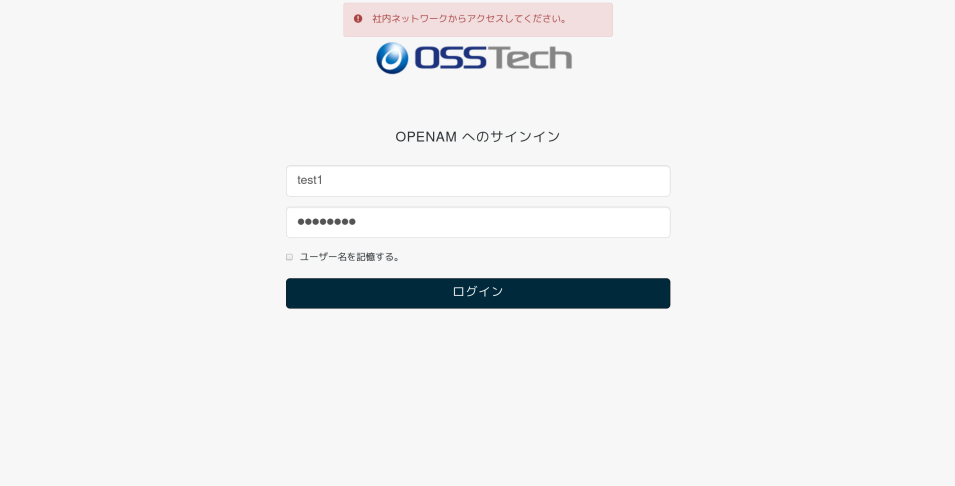

図 30　アダプティブリスク認証失敗画面

5 設定の詳細

5.1 アダプティブリスク認証モジュールの設定

ここでは、アダプティブリスク認証モジュールで設定可能な全ての設定とその内容について説明します。それぞれのタブごとに説明します。

- 一般

【設定項目】	【設定内容】
認証レベル	アダプティブリスク認証モジュールが認証成功時にセットする認証レベル
リスクしきい値	認証失敗とする最小のリスクスコア合計値
認証失敗時のエラーメッセージコード	標準のエラーメッセージから変更する場合に使用するプロパティファイルに定義された任意のプロパティキー

- 認証失敗

【設定項目】	【設定内容】
認証失敗チェック	認証失敗を評価するかどうか
スコア	認証失敗チェックでリスクが高いと評価された場合にリスクスコアに加算される値
結果の反転	認証失敗チェックでの評価を反転させるかどうか

- IP アドレスレンジ

【設定項目】	【設定内容】
IP レンジチェック	IP アドレスレンジを評価するかどうか
IP レンジ	リスクが低いと評価するクライアントの IP アドレスの範囲
スコア	IP レンジチェックでリスクが高いと評価された場合にリスクスコアに加算される値

【設定項目】	【設定内容】
結果の反転	IP レンジチェックでの評価を反転させるかどうか

- IP アドレス履歴

【設定項目】	【設定内容】
IP 履歴チェック	IP アドレス履歴を評価するかどうか
履歴のサイズ	ログイン成功時に履歴リストに格納されるクライアントの IP アドレス数
プロファイル属性名	データストアに履歴リストを格納するための属性名
成功した IP アドレスを保存	ログイン成功時に履歴リストを更新するかどうか[*2]
スコア	IP 履歴チェックでリスクが高いと評価された場合にリスクスコアに加算される値
結果の反転	IP 履歴チェックでの評価を反転させるかどうか

- 既知の Cookie

【設定項目】	【設定内容】
Cookie 値チェック	既知の Cookie を評価するかどうか
Cookie 名	クライアントリクエストから探す Cookie の名前
Cookie 値	指定された Cookie 名に対応するクライアントリクエスト内の Cookie 値
ログイン成功後に Cookie 値を保存する	ログイン成功時にクライアントへのレスポンスに Cookie をセットするかどうか
スコア	Cookie 値チェックでリスクが高いと評価された場合にリスクスコアに加算される値

[*2] 重複有りの先入れ先出し方式で更新されます

【設定項目】	【設定内容】
結果の反転	Cookie 値チェックでの評価を反転させるかどうか

- デバイス Cookie

【設定項目】	【設定内容】
デバイス登録 Cookie チェック	デバイス登録識別子 Cookie を評価するかどうか
Cookie 名	クライアントリクエストからデバイス登録識別子 Cookie として取得する Cookie の名前
ログイン成功のデバイス登録を保存する	ログイン成功時にクライアントへのレスポンスにデバイス登録識別子 Cookie をセットするかどうか
スコア	デバイス登録 Cookie チェックでリスクが高いと評価された場合にリスクスコアに加算される値
結果の反転	デバイス登録 Cookie チェックでの評価を反転させるかどうか

- 最終ログインからの経過時間

【設定項目】	【設定内容】
最終ログインからの経過時間チェック	最終ログインからの経過時間を評価するかどうか
Cookie 名	クライアントリクエストから最終ログイン時間として取得する Cookie の名前
最終ログインからの最大時間	リスクが低いと評価する最終ログインからの最大日数
ログイン成功の時間を保存する	ログイン成功時にクライアントへのレスポンスに最終ログイン時間の Cookie をセットするかどうか
スコア	最終ログインからの経過時間チェックでリスクが高いと評価された場合にリスクスコアに加算される値

【設定項目】	【設定内容】
結果の反転	最終ログインからの経過時間チェックでの評価を反転させるかどうか

- プロファイル属性

【設定項目】	【設定内容】
プロファイルのリスク属性チェック	プロファイル属性を評価するかどうか
属性名	ユーザープロファイルから取得する属性の名前
属性値	リスクが低いと評価する指定された属性名に対応する属性の値
スコア	プロファイルのリスク属性チェックでリスクが高いと評価された場合にリスクスコアに加算される値
結果の反転	プロファイルのリスク属性チェックでの評価を反転させるかどうか

- 位置情報（共通）

【設定項目】	【設定内容】
位置情報データベースの場所	「位置情報データベースの取得」でデータベースを配置した場所
IP アドレスのホワイトリスト	位置情報国コードチェックと位置情報履歴チェックにおいて、位置情報関係なしにリスクが低いと評価したい IP アドレスのリスト

- 位置情報

【設定項目】	【設定内容】
位置情報国コードチェック	位置情報の国コードを評価するかどうか
有効な国コード	リスクが低いと評価する国コードのリスト

【設定項目】	【設定内容】
スコア	位置情報国コードチェックでリスクが高いと評価された場合にリスクスコアに加算される値
結果の反転	位置情報国コードチェックでの評価を反転させるかどうか

- 位置情報履歴

【設定項目】	【設定内容】
位置情報履歴チェック	位置情報履歴を評価するかどうか
履歴のサイズ	ログイン成功時に履歴リストに格納される国コード数
履歴属性名	データストアに履歴リストを格納するための属性名
成功したロケーションを保存	ログイン成功時に履歴リストを更新するかどうか[*3]
スコア	位置情報履歴チェックでリスクが高いと評価された場合にリスクスコアに加算される値
結果の反転	位置情報履歴チェックでの評価を反転させるかどうか

- リクエストヘッダー

【設定項目】	【設定内容】
リクエストヘッダーチェック	リクエストヘッダーを評価するかどうか
リクエストヘッダー名	クライアントリクエストから取得するリクエストヘッダーの名前
リクエストヘッダーの値	リスクが低いと評価する指定されたリクエストヘッダー名に対応するリクエストヘッダーの値
スコア	リクエストヘッダーチェックでリスクが高いと評価された場合にリスクスコアに加算される値

[*3] 重複有りの先入れ先出し方式で更新されます

【設定項目】	【設定内容】
結果の反転	リクエストヘッダーチェックでの評価を反転させるかどうか

- 警告メール

【設定項目】	【設定内容】
リスクの高いログイン成功に対して警告メールを送信する	アダプティブリスク認証に失敗し、その後ログインが成功した際に警告メールを送信するかどうか
メールアドレス属性名	メールアドレスとして使用されるユーザープロファイルの属性の名前
From アドレス	警告メールの送信元アドレスとして表示される任意のアドレス
履歴の属性が保存されていない場合はメールを送信しない	IP アドレス履歴チェックと位置情報履歴チェックにおいて履歴リスト属性が存在せず、履歴の保存が有効な場合に警告メールの送信を省くかどうか

5.2 警告メールの件名と本文の設定

警告メールの件名および本文のテンプレートはプロパティファイルに定義します。アクセスユーザーがブラウザの設定言語を日本語にしている場合、参照されるプロパティファイルは amAuthAdaptive_ja.properties ファイルです。それ以外の言語にしている場合、amAuthAdaptive.properties ファイルです。OpenAM のインストールディレクトリのパス[*4]を{OPENAM_INSTALL} とすると、プロパティファイルは{OPENAM_INSTALL}/WEB-INF/lib/openam-auth-adaptive-14.x.x.jar の中にあります。テンプレートを変更する場合は、この jar ファイルを展開し、その中にあるプロパティファイルを{OPENAM_INSTALL}/WEB-INF/classes/ ディレクトリにコピーして編集します。

ここでは、日本語のプロパティファイルを変更します。

以下にインストールディレクトリがデフォルトパスの場合の展開および配置方法を示します。OpenAM のバージョンによって 14.x.x の部分を変更して実行してください。

[*4] デフォルトでは/opt/osstech/share/tomcat/webapps/openam です

```
# cd /opt/osstech/share/tomcat/webapps/openam/WEB-INF/classes/
# jar -xvf ../lib/openam-auth-adaptive-14.x.x.jar amAuthAdaptive_ja.properties
```

編集する際は Unicode エスケープされたプロパティファイル内のテキストをネイティブコードに変換し、編集後 Unicode に戻します。[*5]

```
# native2ascii -reverse amAuthAdaptive_ja.properties\
    amAuthAdaptive_ja.properties.utf8
# vi amAuthAdaptive_ja.properties.utf8
（ファイルの編集）
# native2ascii amAuthAdaptive_ja.properties.utf8 amAuthAdaptive_ja.properties
```

変更を反映するため OpenAM を再起動します。

```
# systemctl restart osstech-tomcat
```

以下がデフォルトのテンプレートです。

```
wariningMailSubject=普段と異なる状況でのログインについてご確認ください
wariningMailContent=  普段と異なる状況でのログインがありましたので通知します。\r\n\
  ログイン時の情報を本メールの下部に記しますので、実際にあなたがログインされたものであるか\r\n\
ご確認ください。身に覚えのないログインであった場合は、システム管理者までご連絡ください。
\r\n\
\r\n\
== ログイン情報 ==\r\n\
\r\n\
%UserIDInformation%\
%DateInformation%\
%IPAddressInformation%\
%CountryInformation%\
\r\n
InformationLineFormat=\ -\ [{0}] {1}\r\n
UserIDInformationTitle=User ID
DateInformationTitle=Time
IPAddressInformationTitle=IP Address
CountryInformationTitle=Location
```

[*5] この作業は ISO-8859-1 文字セットに含まれていない文字列がプロパティファイル内に存在する場合にのみ必要です

デフォルトのテンプレートでは以下のように送信されます。

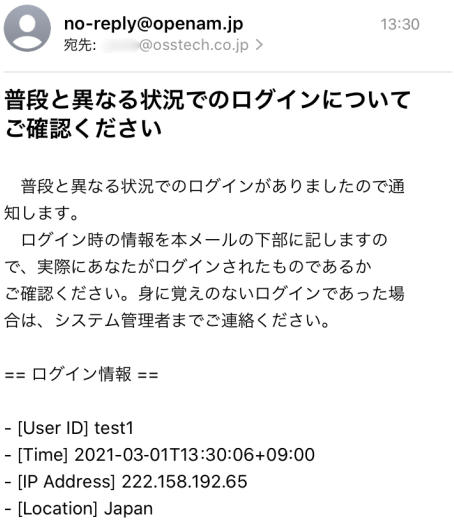

図 31　デフォルトの警告メール

5.2.1 件名の変更

件名を変更するには `wariningMailSubject` キーの値を編集します。

例えば、件名を「[OpenAM] セキュリティ通知」と変更する場合は以下のように変更します。

```
wariningMailSubject=[OpenAM] セキュリティ通知
```

5.2.2 本文の変更

本文は、`wariningMailContent` キーの値にユーザー ID などのログイン時の情報が埋め込まれて生成されます。

埋め込むことのできる情報は以下の 4 つです。

情 報	置き換えられる文字列	表示名のキー
ユーザー ID	%UserIDInformation%	UserIDInformationTitle
ログイン時刻	%DateInformation%	DateInformationTitle

情報	置き換えられる文字列	表示名のキー
IP アドレス	%IPAddressInformation%	IPAddressInformationTitle
国名	%CountryInformation%	CountryInformationTitle

「置き換えられる文字列」を wariningMailContent キー値内に記述すると、InformationLineFormat キーに定義されたフォーマットに沿って文字列がそれぞれの「表示名のキー」に対応する値と実際のログイン情報で置き換えられます。InformationLineFormat キーの値の {0} はそれぞれの情報の表示名に置き換えられ、{1} は表示名に対応するそれぞれの実際のログイン情報に置き換えられます。

「国名」のログイン情報は、「位置情報」または「位置情報履歴」を評価する場合にのみ表記されます。IP アドレスから国が特定できなかったときや、ホワイトリストに含まれる IP アドレスでログインしたときには「国名」のログイン情報は -- と表記されます。

例として以下のように変更します。

```
wariningMailContent=\ \ 普段と異なる国からの OpenAM へのログインが検出されました。ログインの詳細については以下をご確認ください。\r\n\
\r\n\
_____\r\n\
%UserIDInformation%\
%DateInformation%\
%CountryInformation%\
%IPAddressInformation%\
- - - - - - - - - - - - - - - - - - -\r\n\
\r\n\
\ \ 上記のログインに心当たりが無い場合、管理者にご連絡ください。\r\n\
\r\n\
-- \r\n\
オープンソース・ソリューション・テクノロジ株式会社\r\n
InformationLineFormat=\ \ [{0}]\r\n     {1}\r\n
UserIDInformationTitle=ユーザー ID
DateInformationTitle=ログイン時刻
IPAddressInformationTitle=IP アドレス
CountryInformationTitle=国名
```

「件名の変更」と「本文の変更」の例のように変更すると以下のように送信されます。

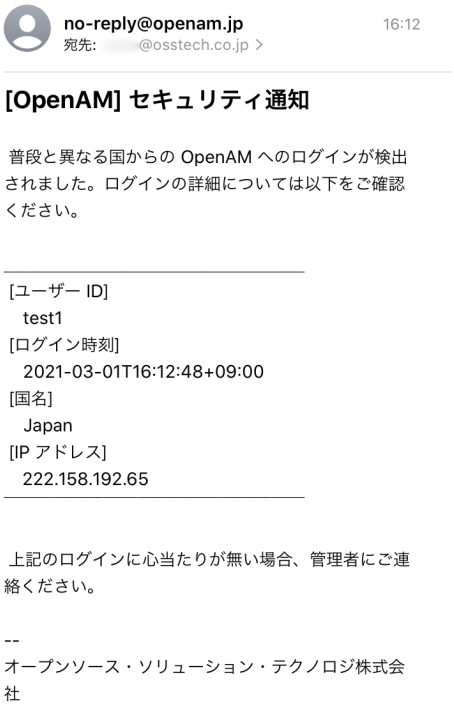

図 32　カスタマイズされた警告メール

5.3 認証失敗時のエラーメッセージコードの設定

アダプティブリスク認証を Requisite 条件で利用する場合、アダプティブリスク認証失敗時に表示されるメッセージをカスタマイズすることができます。デフォルトでは下図のように「認証に失敗しました。」と表示されます。

図 33　デフォルトのエラーメッセージ

カスタマイズするには、表示したいメッセージをプロパティファイルに定義し、「アダプティブリスク認証モジュールの設定」の「一般」タブの「認証失敗時のエラーメッセージコード」の設定を行う必要があります。

アクセスユーザーがブラウザの設定言語を日本語にしている場合、参照されるプロパティファイルは amAuthAdaptive_ja.properties ファイルです。それ以外の言語にしている場合、amAuthAdaptive.properties ファイルです。OpenAM のインストールディレクトリのパス[*6]を{OPENAM_INSTALL} とすると、プロパティファイルは{OPENAM_INSTALL}/WEB-INF/lib/openam-auth-adaptive-14.x.x.jar の中にあります。テンプレートを変更する場合は、この jar ファイルを展開し、その中にあるプロパティファイルを{OPENAM_INSTALL}/WEB-INF/classes/ ディレクトリにコピーして編集します。

ここでは、日本語のプロパティファイルを変更します。

以下にインストールディレクトリがデフォルトパスの場合の展開および配置方法を示します。OpenAM のバージョンによって 14.x.x の部分を変更して実行してください。

```
# cd /opt/osstech/share/tomcat/webapps/openam/WEB-INF/classes/
# jar -xvf ../lib/openam-auth-adaptive-14.x.x.jar amAuthAdaptive_ja.properties
```

編集する際は Unicode エスケープされたプロパティファイル内のテキストをネイティブコードに変換し、編集後 Unicode に戻します。[*7]

```
# native2ascii -reverse amAuthAdaptive_ja.properties\
    amAuthAdaptive_ja.properties.utf8
# vi amAuthAdaptive_ja.properties.utf8
（ファイルの編集）
# native2ascii amAuthAdaptive_ja.properties.utf8 amAuthAdaptive_ja.properties
```

以下がプロパティファイルに予め記述されている設定例です。

```
AdaptiveAuthError=認証に失敗しました。
```

上記のプロパティ値のみを変更するか、またはプロパティキーとプロパティ値を新しく定義します。新しくプロパティキーを定義する場合は、既に設定されている他のプロパティキーと重複しない文字列を定義してください。ここでは、例としてプロパティキーを

[*6] デフォルトでは/opt/osstech/share/tomcat/webapps/openam です

[*7] この作業は ISO-8859-1 文字セットに含まれていない文字列がプロパティファイル内に存在する場合にのみ必要です

「errorMessage」、プロパティ値を「ログインに必要な条件を満たしていません。」と定義します。

```
errorMessage=ログインに必要な条件を満たしていません。
```

新しくプロパティキーを定義した場合、amAuthAdaptive.properties ファイルにも同様のキーを定義する必要があります。amAuthAdaptive.properties ファイルを展開後、編集します。

```
# cd /opt/osstech/share/tomcat/webapps/openam/WEB-INF/classes/
# jar -xvf ../lib/openam-auth-adaptive-14.x.x.jar amAuthAdaptive.properties
# vi amAuthAdaptive.properties
```

以下のように定義します。

```
errorMessage=You do not fulfill the requirements for login.
```

変更を反映するため OpenAM を再起動します。

```
# systemctl restart osstech-tomcat
```

OpenAM 再起動後、管理コンソールの「アダプティブリスク認証モジュールの設定」の「一般」タブの「認証失敗時のエラーメッセージコード」にプロパティファイルに定義したエラーメッセージのプロパティキーを設定します。プロパティファイルに記述されていた設定例のプロパティ値のみ変更した場合は「AdaptiveAuthError」と設定し、プロパティキーとプロパティ値を新しく定義した場合はそのキー（例では「errorMessage」）を設定します。

例のように変更すると、アダプティブリスク認証失敗時に以下のように表示されます。

図 34　カスタマイズされたエラーメッセージ

6 改版履歴

- 2021 年 3 月 9 日 リビジョン 1.0
  - 初版作成
- 2021 年 3 月 12 日 リビジョン 1.1
  - 「アカウントロックアウトの設定」を追加
- 2022 年 7 月 14 日 リビジョン 1.2
  - 表紙の社名を OSSTech 株式会社に変更