OpenAM 14 reCAPTCHA v3 認証モジュール 利用手順書

OSSTech 株式会社

更新日 2022 年 10 月 28 日
リビジョン 1.0

目次

1 はじめに

本文書は、OSSTech 版 OpenAM 14 に含まれる reCAPTCHA v3 認証モジュールの利用手順書です。

1.1 機能概要

reCAPTCHA v3 認証モジュールはデータストア認証や OpenLDAP 認証などの ID・パスワード認証に reCAPTCHA v3 によるボット判定の機能を提供します。そして、ボットによるアクセスと判定した場合に追加の認証の要求や、認証を失敗させることが可能です。

図 1　データストア認証との組み合わせた場合のログイン画面

1.2 システム構成

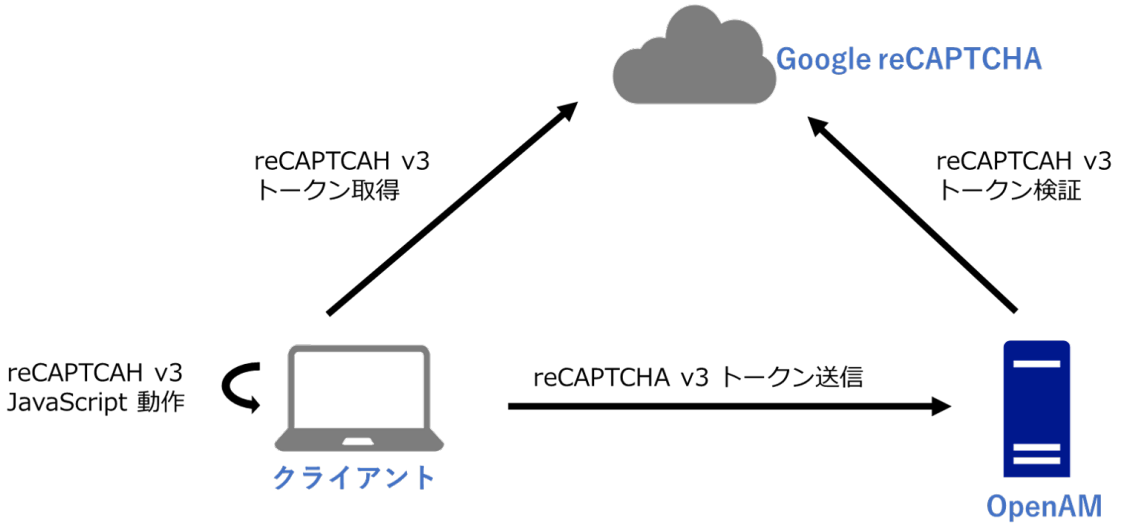

図 2　システム構成

reCAPTCHA v3 認証のログイン画面では reCAPTCHA v3 の JavaScript が動作して Google reCAPTCHA サービスからトークンを取得します。ログインボタンを押下すると、トークンは OpenAM に送信されます。OpenAM は reCAPTCHA v3 検証 API を実行してトークンを検証します。

1.3 認証モジュールの構成

reCAPTCHA v3 認証は以下の 2 つの認証モジュールで構成されています。

- reCAPTCHA v3 ラッパー
- reCAPTCHA v3 判定

これは、リスクベース認証を使った認証連鎖に reCAPTCHA v3 を当てはめる場合、データストア認証などの ID・パスワード認証とアダプティブリスク認証などのリスクベース認証が reCAPTCHA v3 認証の対象となるためです。

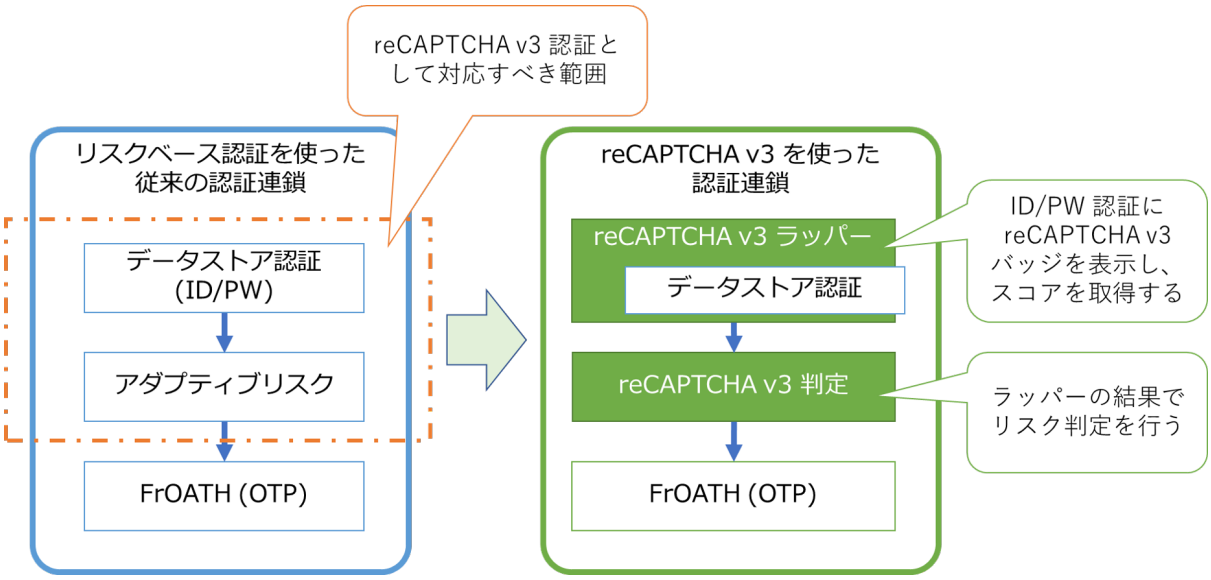

図 3　モジュール構成

1.4 ユースケース

reCAPTCHA v3 認証のユースケースを以下に示します。ユースケースによって認証連鎖の内容が異なります。

【ユースケース】	【説明】
ボットの場合に追加の認証を求める	ボットでない場合は ID・パスワード認証で認証が成功します。ボットの場合は追加の認証が求められます。
ボットの場合に認証を失敗させる	ボットでない場合は ID・パスワード認証で認証が成功します。ボットの場合は認証が失敗します。

1.5 制限事項

- reCAPTCHA v3 認証では次の認証モジュールに対してボット判定の機能を追加できます（内部認証モジュールとして指定可能）
  - データストア認証
  - OpenLDAP 認証
  - LDAP 認証
  - Active Directory 認証

  - ID 認証
- ボット判定のスコアの精度は reCAPTCHA サービスに依存します
- サポートするブラウザーは reCAPTCHA サービスに依存します
  - https://support.google.com/recaptcha/answer/6223828?hl=en
- リクエストが秒間 1000 回を超えるか、1 月で 100 万件を超える場合は Google に例外の承認を受ける必要があります
  - https://developers.google.com/recaptcha/docs/faq
- クライアント端末および OpenAM はインターネットに接続出来る必要があります
  - Google reCAPTCHA サービスと通信するために必要です。クライアント端末がインターネットに接続できない場合は reCAPTCHA v3 トークンが送られないため OpenAM はボットであると判定します。

2 事前準備

reCAPTCHA v3 認証を導入する前に、実施すべき内容を記載します。

2.1 reCAPTCHA サービスにサイトを登録する

Google アカウントでログインして、登録ページにアクセスします。

以下の項目を入力し、「reCAPTCHA 利用条件に同意する」にチェックして「送信」ボタンを押下します。

【項目】	【説明】
ラベル	サイトを識別する名称です。
reCAPTCHA タイプ	reCAPTCHA v3 を選択します。
ドメイン	OpenAM サーバーのドメインを指定します。
オーナー	Google アカウントのメールアドレスを指定します。

その後、表示されたページでサイトキーとシークレットキーをコピーしておきます（認証モジュールの設定に必要です）。シークレットキーの取扱いには注意してください。

2.2 パラメーターの検討

reCAPTCHA v3 認証モジュールでは reCAPTCHA v3 を動作させるために以下の情報が必要です。事前に設定値を検討しておきます。

【項目】	【説明】
アクション名	reCAPTCHA v3 のスクリプトを動作させる際に指定する action パラメーターの値です。reCAPTCHA が組み込まれたページを識別するために利用されます。 reCAPTCHA v3 のドキュメントにはアクション名を login としたユースケースが記載されています。
スコアの閾値	ボットかどうかを判定する閾値です。reCAPTCHA 検証 API の応答は 1.0 から 0.0 までの スコアを返却します。なお、reCAPTCHA v3 のドキュメントでは標準の閾値が 0.5 であると記載されています。

3 ボットの場合に追加の認証を求める

本章では reCAPTCHA v3 認証でボットの場合に追加の認証を求めるための手順を示します。

3.1 reCAPTCHA v3 ラッパーモジュールを設定する

reCAPTCHA v3 ラッパーモジュールのインスタンスを作成します。

1. OpenAM に管理者ユーザーでログインします。
2. 対象レルム → 「認証」 → 「モジュール」を開きます。
3. 「モジュールの追加」ボタンを押下します。
4. ここでは「名前」に “reCAPTCHAWrapper” と入力し、「タイプ」は「reCAPTCHA v3 ラッパー」を選択して、「作成」ボタンを押下します。
5. 各パラメーターを入力し、「変更の保存」を押下します。以下はパラメータの例です。

【項目名】	【設定例】
サイトキー	（reCAPTCHA サービスより取得したサイトキーを設定します）
シークレットキー	（reCAPTCHA サービスより取得したシークレットキーを設定します）
スコアの閾値	0.5
アクション名	login
ホスト名	（OpenAM サーバーにアクセスする際の FQDN）
IP アドレスチェック[*1]	無効
reCAPTCHA v3 トークン検証 URL	https://www.google.com/recaptcha/api/siteverify
reCAPTCHA v3 コネクションタイムアウト	5000
reCAPTCHA v3 リードタイムアウト	5000

[*1] reCAPTCHA v3 のトークン検証 API 実行時にクライアントの IP アドレスを含めるかを設定します。API としては IP アドレスの送信は任意 (Optional) です。IP アドレスが API 側でどのようにハンドリングされるかという情報は公開されていません。

【項目名】	【設定例】
内部認証モジュール	DataStore
ボットによるアクセスの場合は内部認証を行わない	無効
ボットによるアクセスの場合に認証失敗とする内部認証ステージ	（空）
認証レベル	0

以上で完了です。

3.2 reCAPTCHA v3 判定モジュールを設定する

reCAPTCHA v3 判定モジュールのインスタンスを作成します。

1. OpenAM に管理者ユーザーでログインします。
2. 対象レルム → 「認証」 → 「モジュール」を開きます。
3. 「モジュールの追加」ボタンを押下します。
4. ここでは「名前」に “reCAPTCHACheck” と入力し、「タイプ」は「reCAPTCHA v3 判定」を選択して、「作成」ボタンを押下します。
5. 各パラメーターを入力し、「変更の保存」を押下します。以下はパラメータの例です。

【項目名】	【設定例】
認証レベル	0

以上で完了です。

3.3 ForgeRock Authenticator (OATH) 認証モジュールを設定する

ForgeRock Authenticator (OATH) 認証モジュールのインスタンスを作成します。

1. OpenAM に管理者ユーザーでログインします。
2. 対象レルム → 「認証」 → 「モジュール」を開きます。
3. 「モジュールの追加」ボタンを押下します。

4. ここでは「名前」に “frOATH” と入力し、「タイプ」は「ForgeRock Authenticator (OATH)」を選択して、「作成」ボタンを押下します。
5. 各パラメーターを入力し、「変更の保存」を押下します。以下はパラメータの例です。

【項目名】	【設定例】
認証レベル	0
ワンタイムパスワードの長さ	6
秘密鍵の最小桁数	40
使用する OATH アルゴリズム	TOTP
HOTP ウィンドウサイズ	100
チェックサム数字の追加	False
トランケーションオフセット	-1
TOTP タイムステップ期間	30
TOTP タイムステップ数	1
最大許容クロックドリフト	1
発行者の名前	OpenAM
リカバリーコードの発行	有効

以上で完了です。

3.4 認証連鎖を設定する

1. OpenAM に管理者ユーザーでログインします。
2. 対象レルム → 「認証」 → 「認証連鎖」を開きます。
3. 「認証連鎖の追加」ボタンを押下します。
4. ここでは「認証連鎖名」に “botNeedsOTPService” と入力し、「作成」ボタンを押下します。
5. 認証連鎖の設定画面で「モジュールの追加」ボタンを押下し、「モジュールの選択」のプルダウンで reCAPTCHA v3 ラッパーモジュール（ここでは “reCAPTCHAWrapper”）を選択、「基準の選択」は「Requisite」を選択して「OK」ボタンを押下します。

6. 5 と同様にして reCAPTCHA v3 判定モジュール（ここでは “reCAPTCHACheck”）を「Sufficient」に設定します。
7. 5 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。
8. 認証連鎖の設定画面に戻ったら、「変更の保存」ボタンを押下します。

以上で完了です。

4 ボットの場合に認証を失敗させる

本章では reCAPTCHA v3 認証でボットの場合に認証を失敗させるための手順を示します。

4.1 reCAPTCHA v3 ラッパーモジュールを設定する

reCAPTCHA v3 ラッパーモジュールのインスタンスを作成します。手順及び設定内容は「3.1 reCAPTCHA v3 ラッパーモジュールを設定する」と同様です。既に実施している場合は次に進みます。

4.2 reCAPTCHA v3 判定モジュールを設定する

reCAPTCHA v3 判定モジュールのインスタンスを作成します。手順及び設定内容は「3.2 reCAPTCHA v3 判定モジュールを設定する」と同様です。既に実施している場合は次に進みます。

4.3 認証連鎖を設定する

1. OpenAM に管理者ユーザーでログインします。
2. 対象レルム → 「認証」 → 「認証連鎖」を開きます。
3. 「認証連鎖の追加」ボタンを押下します。
4. ここでは「認証連鎖名」に “botIsFailureService” と入力し、「作成」ボタンを押下します。
5. 認証連鎖の設定画面で「モジュールの追加」ボタンを押下し、「モジュールの選択」のプルダウンで reCAPTCHA v3 ラッパーモジュール（ここでは “reCAPTCHAWrapper”）を選択、「基準の選択」は「Requisite」を選択して「OK」ボタンを押下します。
6. 5 と同様にして reCAPTCHA v3 判定モジュール（ここでは “reCAPTCHACheck”）を「Required」に設定します。
7. 認証連鎖の設定画面に戻ったら、「変更の保存」ボタンを押下します。

以上で完了です。

5 スコアのログ出力

OpenAM は reCAPTCHA v3 検証 API が応答したスコアを認証ログ (authentication.csv) に出力します。authentication.csv を確認することで日々のアクセスのスコアを確認可能です。 スコアは reCAPTCHA v3 ラッパーモジュールが動作すると出力されます。

スコアは authentication.csv の entries カラムの info 内に reCaptchaV3Score という項目で出力されます。 下記にサンプルを示します。

- スコアが 0.7 の場合

```
info””:{...,””reCaptchaV3Score””:””0.7””,...}}
```

スコアは OpenAM で何らかのエラーが発生した場合や reCAPTCHA v3 検証 API から "success": false の応答があった場合は error となります。 クライアント端末から reCAPTCHA v3 トークンが送られてこなかった場合は empty-token となります。

- クライアント端末から reCAPTCHA v3 トークンが送られてこなかった場合

```
info””:{...,””reCaptchaV3Score””:””empty-token””,...}}
```

6 高度な設定

6.1 ボットによるアカウントロックを防ぐ

reCAPTCHA v3 ラッパーモジュールではボットと判定した場合でも内部認証モジュールを呼び出すしくみとなっています。そのため、OpenAM のアカウントロックや OpenLDAP の ppolicy でアカウントロックを有効にしている場合、ボットによってアカウントロックを引き起こされる恐れがあります。この場合、reCAPTCHA v3 ラッパーモジュールの「ボットによるアクセスの場合は内部認証を行わない」を「有効」にすることで、ボットによるアカウントロックを防ぐことが可能です。

6.2 ボットによるパスワード変更を防ぐ

OpenLDAP 認証には OpenLDAP の ppolicy でパスワード有効期限を設定している場合にパスワード変更画面を表示することができます。reCAPTCHA v3 ラッパーモジュールの内部認証モジュールとして OpenLDAP 認証を設定している場合、ボットによってパスワード変更ができる構成では問題があります。この場合、reCAPTCHA v3 ラッパーモジュールの「ボットによるアクセスの場合に認証失敗とする内部認証ステージ」に「OpenLDAP2」を設定することで、パスワード変更画面を表示せずに認証失敗とさせることが可能です。

7 改版履歴

- 2022 年 10 月 28 日 リビジョン 1.0
  - 初版作成