

O-PLUS
Account Protection

導入仕様書

3.3 版

2026/04/01 更新

目次

内容

はじめに	3
全体概要図	3
シーケンス図	3
JavaScript 仕様	6
API 仕様	7
JavaScript 収集データ項目	8
Cookie 仕様	10
審査結果仕様	11
非機能要件/制約	12
テスト方針	12

はじめに

本書について

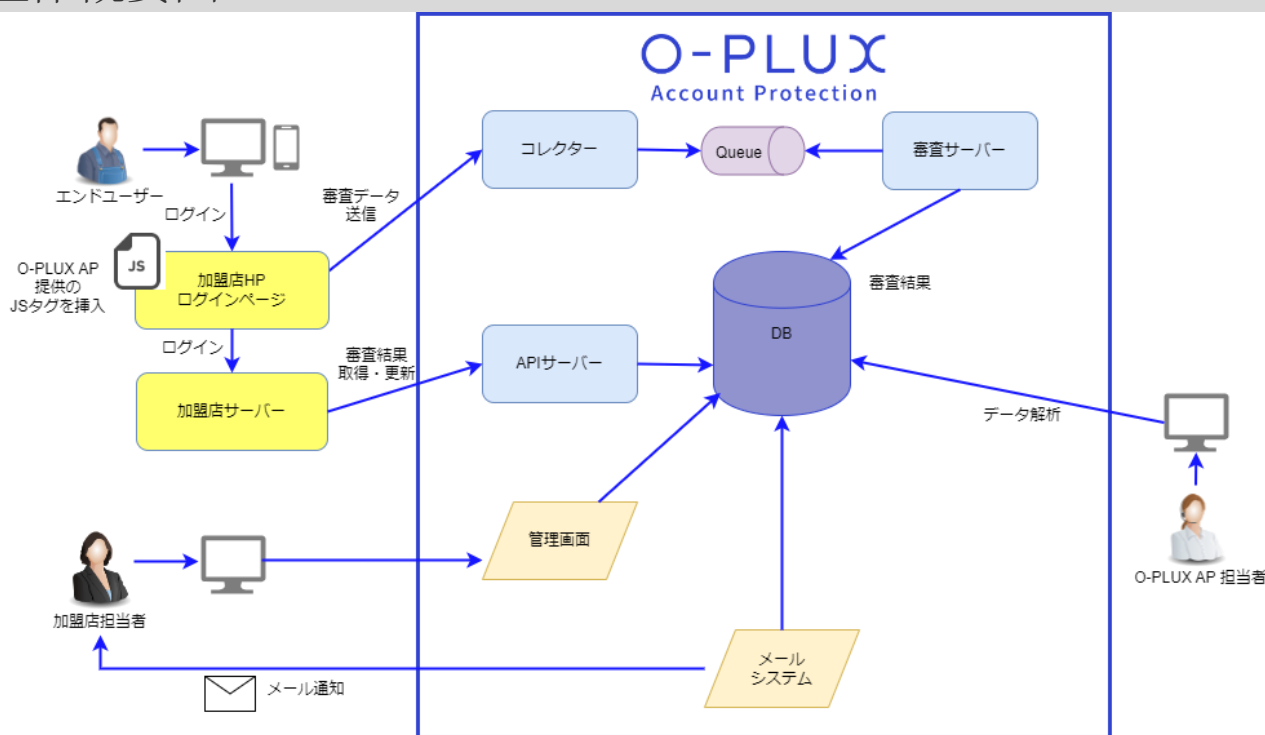
本書は、かつこ株式会社が提供する『O-PLUX Account Protection』のシステム仕様を説明することを目的として作成しており、O-PLUX Account Protection を導入いただく企業様（以下、加盟店）を対象としています。

O-PLUX Account Protection とは

O-PLUX Account Protection は、他人のなりすましを識別することによって不正アクセスから生じる不正行為（個人情報搾取・不正送金・不正ポイント交換等）を防止するソリューションです。

加盟店のWEBサイトに埋め込んでいただくタグからJavaScript を呼び出してエンドユーザーのアクセス時の操作情報やアクセスした端末情報等をリアルタイムで取得・分析し、不正の疑いがあるアクセスについては審査結果を加盟店宛てにシステム連携等で返却します。

全体概要図



シーケンス図

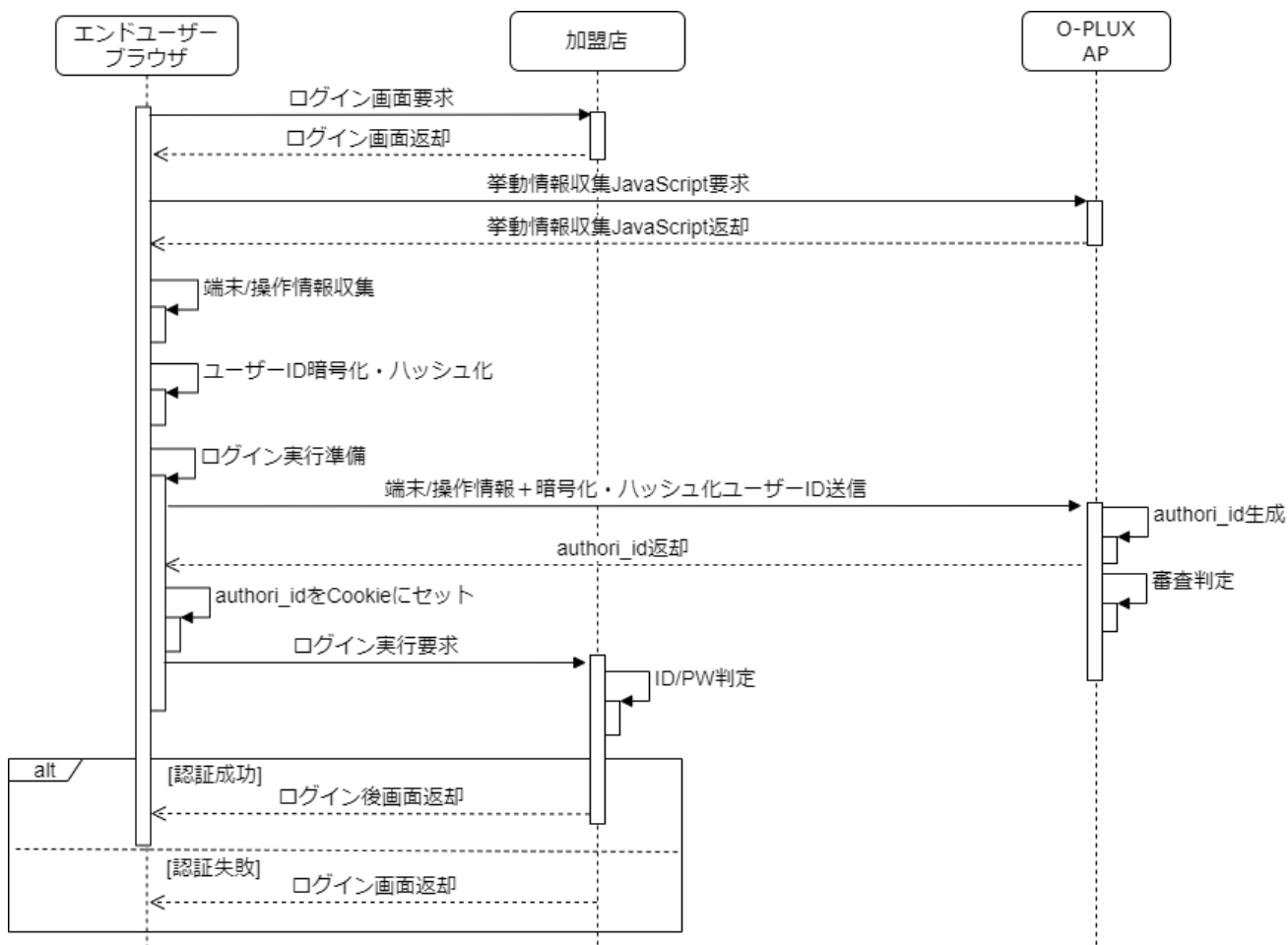
O-PLUX Account Protection のフローについて

O-PLUX Account Protection のフローは情報収集フロー、認証成否通知フロー、審査結果通知フローの3つで構成されます。

本例はログインでの利用をモデルケースとして記載しています。

情報収集フロー

エンドユーザーがログイン画面にアクセスしてからログイン判定が行われるまでのフローは下記のとおりです。



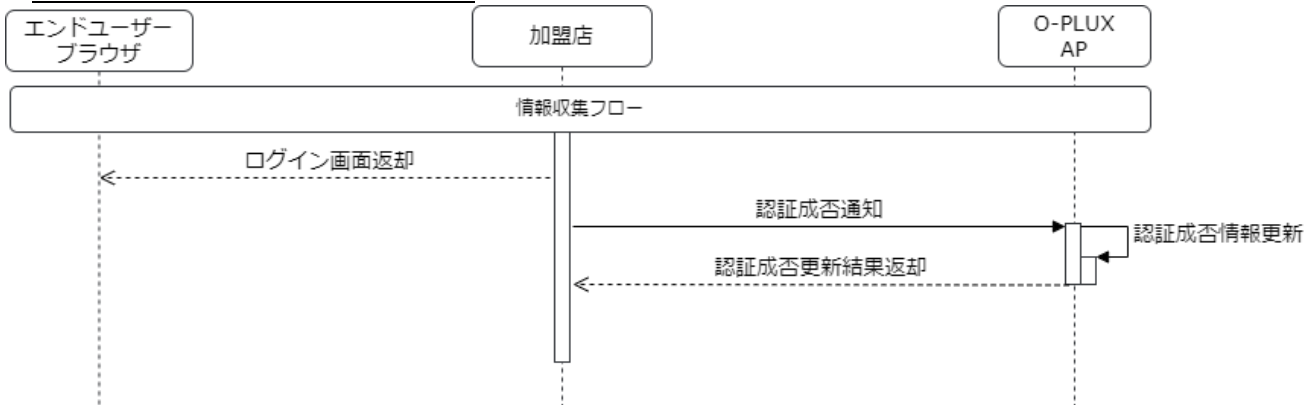
認証成否通知フロー

エンドユーザーがログイン後画面に遷移してから Web サーバーに認証成否通知が行われるまでのフローは下記のとおりです。

JavaScript で認証成否を通知する場合



API で認証成否を通知する場合



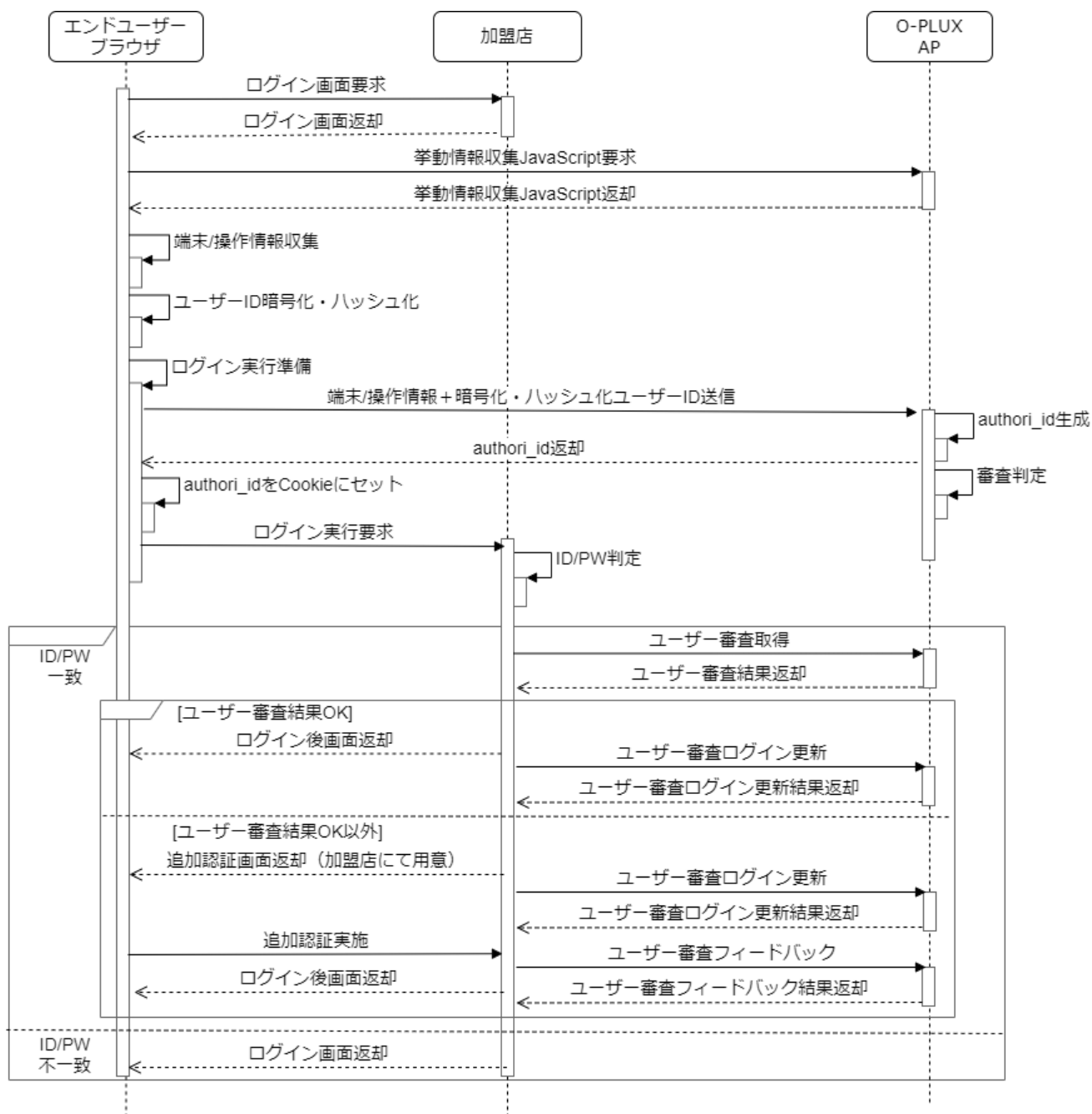
審査結果取得フロー

加盟店が審査結果を取得する際のフローは下記のとおりです。



O-PLUX Account Protection をログインと同期して使用する場合のフロー

O-PLUX Account Protection をログインと同期して使用する場合のフロー例は下記のとおりです。



JavaScript 仕様

O-PLUX Account Protection JavaScript とは

審査データ及び関連するデータの生成、収集及び送信を目的とした JavaScript です。

審査実施の対象ページにタグを埋め込むことで動作し、収集したデータはアクセス実行時に Web サーバーへ送信されます。

タグによって読み込まれる JavaScript は PC、モバイル端末(スマートフォンまたはタブレット)で動作することを前提としています。

JavaScript 種類

名称	概要	サイズ
挙動情報収集 JavaScript	挙動情報(デバイス情報及び操作情報)及び関連するデータ	200KB

	の生成、収集及び送信を行う。	
three.js	審査データを生成するために使用するライブラリ。 挙動情報収集 JavaScript によって読み込みが行われる。	490KB
認証成否通知 JavaScript	Web サーバーに認証成否の通知を行う。 認証成否通知を API で行う場合は不要。	70KB

挙動情報収集 JavaScript の詳細

実行する処理

処理	概要	参照
審査データの収集と送信	審査に用いるデータを収集し、アクセス実行時に Web サーバーへ送信する。	収集項目仕様
Cookie の生成	審査を一意にする識別子を生成し、Cookie にセットする	Cookie 仕様

送信データサイズ

環境	データサイズ
PC	20～30KB
モバイル端末	70～80KB

埋め込み手順

以下の Script タグを body タグ内に埋め込みます。

ドメイン名、JavaScript 名は加盟店 WEB サイト毎に調整となります。

body タグ内での位置は、body の終了タグ直前を推奨しております。

```
<script src="https://{ドメイン名}/assets/js/{JavaScript 名}.js"></script>
```

認証成否通知 JavaScript の詳細

実行する処理

処理	概要	参照
認証成否通知	審査を一意にする識別子を SessionStorage または Cookie から取り出し、Web サーバーへ送信する。	Cookie 仕様

送信データサイズ

環境	データサイズ
PC/モバイル端末	100B

審査後画面への埋めこみ手順

以下の Script タグを body タグ内に埋め込みます。

ドメイン名、JavaScript 名は加盟店 WEB サイト毎に調整となります。

body タグ内での位置は、body の終了タグ直前を推奨しております。

```
<script src="https://{ドメイン名}/assets/js/{JavaScript 名}.js"></script>
```

API 仕様

O-PLUX Account Protection サーバーAPI とは

O-PLUX Account Protection と加盟店システムを連携するためのサーバーAPI です。

下記 5 種類の API を用意しています。

- ・ ユーザー審査取得 API
 ログイン単位でユーザーの審査結果を取得いただけます。

- ・ ユーザー審査一覧取得 API
 ユーザーの審査結果の一覧を最新または任意の審査より前のものから最大 20 件取得いただけます。
- ・ ユーザー審査フィードバック更新 API
 ユーザーの審査に対してフィードバックをいただけます。
- ・ ユーザー審査ログイン成功更新 API
 ユーザーの審査に対して `login_success` の値を更新できます。
- ・ 端末一覧取得 API
 端末情報を最新のものから最大 20 件取得いただけます。

詳細は「O-PLUX Account Protection サーバーAPI 仕様書 (<https://docs.api.o-moti.com/>)」をご覧ください。

JavaScript 収集データ項目

個人情報の取り扱いについて

O-PLUX Account Protection では以下のような個人を特定するための情報は公開鍵方式での暗号化及びハッシュ化したうえで取得しており、加盟店以外の第三者（弊社含む）では復号できない仕様となっています。

項目	対応内容
ユーザーID(ログイン ID)	取得対象とするが、挙動情報収集 JavaScript で公開鍵方式での暗号化及びハッシュ化それぞれの対応を行った値を Web サーバーへ送信する。
パスワード	取得対象外。 キー入力情報の収集は行うが、収集データから入力内容は推測できない。

暗号化及びハッシュ化について

暗号化及びハッシュ化はデータ送信前に挙動情報収集 JavaScript を介してエンドユーザーブラウザ上で実施するため、通信上では暗号化済データ及びハッシュ済データが送信されます。

公開鍵暗号化ロジック仕様

項目	仕様
アルゴリズム	公開鍵：RSA 方式 ※秘密鍵および公開鍵生成については弊社から提供するツールを用いて加盟店にて実施いただきます。
秘密鍵パスフレーズ	加盟店にて設定
暗号化対象の正規化処理	加盟店のログイン仕様に合わせる。

ハッシュ化ロジック仕様

項目	仕様
アルゴリズム	SHA-256
ソルト値	加盟店毎に設定
ハッシュ化対象の正規化処理	加盟店のログイン仕様に合わせる。(例：ユーザーID の名寄せ)

挙動情報仕様

加盟店サイトへのアクセス時にエンドユーザーの以下のデータを収集し、JSON 形式で Web サーバーへ送信します。

収集する情報は基本情報、デバイス情報、操作情報の 3 つに分類されます。

基本情報

O-PLUX Account Protection の審査に要する情報です。ユーザーID(ハッシュ値及び暗号化値)や Cookie などが該当します。

デバイス情報

ユーザーが使用するブラウザ種別やバージョン、端末の OS バージョンや画面サイズなどの情報です。

操作情報

マウス移動やキー入力等、ユーザーの端末操作の特徴に関する情報です。

データ量が膨大になる可能性があるため、情報の取得回数に一定の制限を設けて収集します。

また、キーストローク・ペースト操作・ドラッグアンドドロップ操作・オートコンプリートは、下記の type 属性を持つ<input>要素に限定して収集します。

type 属性 : text、email、tel、password

操作情報一覧

分類	概要及びイベント仕様
マウス操作	マウス移動時の座標情報や入力方法などを一定の間隔で収集。 マウスの座標が変化した時(mouseMove)にイベントが発火。
キーストローク	キー入力時の時間や文字数、特殊キーの押下情報などを収集。 キー押下時(keyDown)とキー解放時(keyUp)にイベントが発火。
クリック操作	クリック操作時の時間やマウス座標などを収集。 クリックが開始された時(mouseDown)、クリックが終了した時(mouseUp)にイベントが発火。
スワイプ操作	スクリーンへのタッチ及びスワイプ操作時の座標などを一定の間隔で収集。 スクリーンがタッチされた時(touchStart)、スワイプ中に座標が変化した時(touchMove)、スクリーンから指が離れた時(touchEnd)にイベントが発火。
ペースト操作	ペースト操作の実行履歴を収集。 ペースト操作が行われた時(paste)にイベントが発火。
ドラッグ&ドロップ操作	ドラッグ&ドロップ操作の実行履歴を収集。 フォームへのドロップが発生した時(drop)にイベントが発火。
オートコンプリート	オートコンプリートによる入力を検知し、実行履歴を収集。 ページロード完了時(load)、フォームへの入力発生時(input)と入力内容の変化時(change)にイベントが発火。
ソフトウェアキーボード	加盟店サイトにソフトウェアキーボードが組み込まれている場合、ソフトウェアキーボードが使用されたか否かの情報を収集。 ソフトウェアキーボードを起動するための要素に対するクリック時(click)にイベントが発火。
エラー情報	挙動情報収集 JavaScript で発生したエラー情報を収集。

JSON データ参考

下記の構成にて、JSON データを難読化して取得します。

JSON データ例,json

```
{
  "userId": "0123456789abcdef0123456789abcdef",
  "accessDate": "2017-01-01 00:00:00 000",
  "sendDate": "2017-01-01 00:00:10 000",
  "cookie": "samplebank#20170101000000AbCdE",
  ...
  "device": {
    "appName": "Mozilla",
```

```

appMinorVersion: "undefined",
appName: "Netscape",
...
},
mouse: [{ ... }],
keyStroke: [{ ... }],
click: [{ ... }],
swipe: [{ ... }],
paste: [{ ... }],
dragDrop: [{ ... }],
autocomplete: [{ ... }],
softwareKeyboard: { ... },
errors: [{ ... }
}
    
```

Cookie 仕様

O-PLUX Account Protection では以下の Cookie を生成します。
 下記目的で加盟店ドメインに対応したカスタムドメインを使用し、ファーストパーティーCookie として生成します。

- クロスドメインによるエンドユーザー環境での警告表示及び O-PLUX Account Protection へのデータ未送信を防ぐ。
- 不正者に不正対策の為の JavaScript と悟られにくくする。

Cookie 一覧

名称	概要	生成タイミング	登録内容
ユーザー識別 Cookie	ユーザーを一意に識別するための 1 要素として生成する。 Web サーバーへ送信し、端末同一性判定を行うために用いる。	審査対象画面表示時	ユーザー単位で一意となる値
審査識別 Cookie	O-PLUX Account Protection への審査を一意にするために生成する。 Web サーバーへ送信し、認証成否通知を行うために用いる。 通常は SessionStorage へ書き込まれるが、SessionStorage が使用できないブラウザ、または js ビルド時の設定によって使用しない場合に Cookie へ書き込まれる。	審査完了時	審査単位で一意となる値
審査 ID 保存 Cookie	O-PLUX Account Protection への審査リクエストのレスポンスで返却される審査 ID(authori_id)を保存する。 O-PLUX Account Protection サーバーAPI の利用において、審査単位での取得・更新を行う際に用いる。	審査リクエスト実行時	O-PLUX Account Protection の審査リクエストを一意に識別する ID

属性

項目	ユーザー識別 Cookie	審査識別 Cookie	審査 ID 保存 Cookie
名称	sess_{加盟店コード}	sess_tran_{加盟店コード}	sess_auth_{加盟店コード}
値	加盟店識別名+"_"+ yyyyMMddHHmmssSSS + a-Z で長さ 5 のランダム な文字列	審査を一意に識別する値	審査を一意に識別する値
ドメイン	ルートドメインを指定	ルートドメインを指定	ルートドメインを指定
http-only	指定しない	指定しない	指定しない

生成/破棄に関する仕様

項目	ユーザー識別 Cookie	審査識別 Cookie	審査 ID 保存 Cookie
生成箇所	挙動情報収集 JavaScript	挙動情報収集 JavaScript	挙動情報収集 JavaScript
破棄箇所	破棄しない	破棄しない	破棄しない
上書き可否	以前の Cookie が残っている場合、上書きは行わない	以前の Cookie が残っている場合でも、Cookie 生成のタイミングで値を更新する	以前の Cookie が残っている場合でも、Cookie 生成のタイミングで値を更新する

審査結果仕様

審査結果とは

O-PLUX Account Protection にて審査を行った結果を指します。

審査結果は O-PLUX Account Protection からのメール通知、管理画面、API による審査結果取得のいずれかの方法で確認することができます。

審査結果は判断した理由も合わせて表示し、一部理由は審査結果を変更することも可能です。

審査結果の種類

審査結果		標準の審査理由		審査結果の変更可否
		論理名	物理名	
OK	問題ない正常なログインと判定されたものです。 OK と判定されたログインデータは、以降本人端末リストとして扱われます。	ユーザーID の端末と一致	USER_DEVICE	
		利用履歴のない端末	FIRST_USER_DEVICE	○
		利用履歴のないユーザーID	FIRST_USER	○
REVIEW	不正ログインの疑いがあると判定されたものです。	ユーザーID の端末と一致	USER_DEVICE	
		ネガティブ IP リストと一致	NEGATIVE_IP	
		異なるユーザーID の端末と重複	SAME_DEVICE	○
		Tor からのアクセス	TOR_IP_MATCH	○
		外国語設定で海外からのアクセス	FOREIGN_IP_AND_LANGUAGE	○
		海外からのアクセス	FOREIGN_IP	○
		ユーザーID の端末数が閾値を超過	FIRST_USER_DEVICE_COUNT_OVER	○

NG	不正ログインと判定されたものです。 NG と判定されたログインデータは、以降ブラックリストとして扱われます。	ユーザーID の端末と一致	USER_DEVICE	
		異なるユーザーID の不正端末と一致	NG_DEVICE	
		BOT 特徴と一致	BOT	○

非機能要件/制約

O-PLUX Account Protection の非機能要件及び制約は下記のとおりです。

項目	内容
同時接続数	最大 300rps、バーストスロット 600rps ※加盟店単位で拡張可能
レイテンシー	Web サーバー：平均 30ms、99 パーセンタイル 100ms 以内 審査サーバー：平均 50ms、99 パーセンタイル 300ms 以内 API サーバー：平均 50ms、99 パーセンタイル 300ms 以内 ※Web サーバー到達までのネットワーク遅延は含まない、サーバー内部は非同期処理のためエンドユーザーへのアクセス処理に影響なし
冗長化	地理冗長を採用
確認済みブラウザ	別表に記載
動作環境	接続方式：HTTPS SSL Protocol Version：TLSv1.1 以降 ブラウザ設定：JavaScript、Cookie が有効
IP 制限	本番環境/STG 環境問わず、Web サーバーに対する IP 制限はない
セキュリティ	第三者機関での脆弱性診断を実施 アンチウイルス、改ざん検知を導入

確認済みブラウザ一覧

下記記載の OS/ブラウザの最新版を随時動作保証環境として確認しております。

OS	ブラウザ
Windows	Microsoft Edge、Firefox、Chrome
OS X/macOS	Safari、Firefox、Chrome
Android	Chrome
iOS	Safari、Chrome

テスト方針

O-PLUX Account Protection では利用開始までに動作確認テストを実施して事前検証を行います。

動作確認テスト

目的

加盟店 WEB サイトでログインを行い、O-PLUX Account Protection の JavaScript タグが導入チェックシートの項目(ログイン入力フォーム名/ユーザーID のハッシュ/Cookie 等の名称)に則って作成されていること及び審査対象データが送信されることを検証します。

環境

対象	環境
O-PLUX Account Protection	本番環境
加盟店サイト	テスト環境

事前準備

- 加盟店に O-PLUX Account Protection の JavaScript タグが提供済みであること。
- 加盟店テスト環境にて O-PLUX Account Protection の JavaScript タグが HTML の Body タグ内の指定箇所に設置済みであること。
- 加盟店にユーザーID 復号ツールが提供済みであること。
- 加盟店から加盟店サイトのテスト環境でアクセス可能なユーザーアカウントを受領済みであること。

テスト内容

- O-PLUX Account Protection 担当者が加盟店 WEB サイトにログイン等のアクセスを行い、O-PLUX Account Protection へ正しく疎通しているか検証する。
- ログインしたユーザーアカウントのユーザーID の暗号値を加盟店担当者様に共有する。加盟店担当者様は、暗号値を復号ツールで復号し、DB 上のユーザーID と一致するか確認する。

以上