Google Cloud

# WEB からアプリまで一貫した不正アクセス対策

## reCAPTCHA Enterprise 導入のポイント、最新機能のご紹介

Google Asia Pacific　セキュリティサービス担当　齋藤桃子

Google Cloud　カスタマーエンジニア　桃井啓行

# スピーカー自己紹介

齋藤 桃子

アジア太平洋地域および日本におけるセキュリティーサービスのビジネス発展をリード。　セキュリティ部門のユーザー保護サービスに特化し、幅広いマーケットの拡大・発展に尽力。

桃井 啓行

デジタル ネイティブ エンタープライズ担当カスタマーエンジニア。Google Cloud ソリューションの紹介やアーキテクチャ設計、PoC 支援などを通してお客様のクラウドシステム構築を技術面よりサポートしています。

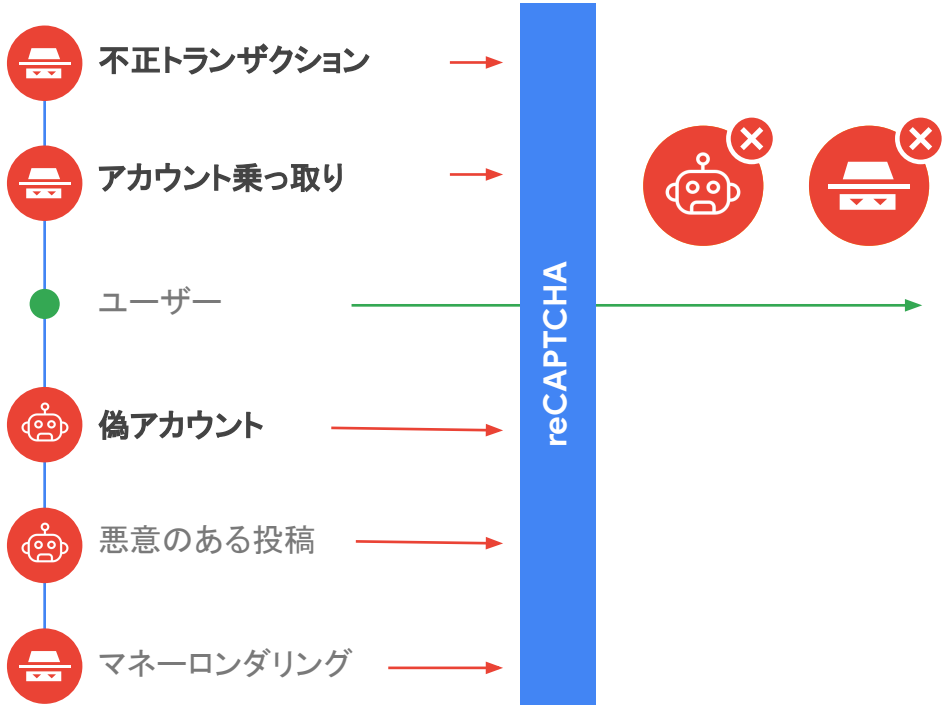
Google Cloud

## セッションの内容

- reCAPTCHA のボット検出とは？
- 各バージョンの比較
- reCPATCHA Enterprise の特徴
- reCPATHCA Enterprise の仕組みと導入ポイント
- 事例紹介

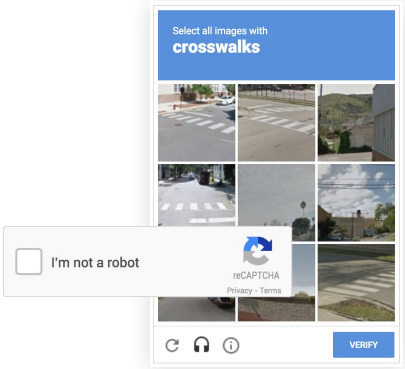
# reCAPTCHA
# ボット検出のユースケース

ボット、詐欺、自動攻撃からビジネスを守ります



# reCAPTCHAの進化


reCAPTCHA v1
(released 2007)




reCAPTCHA v2
(released 2012)

```
<script
src="https://www.google.com/recaptcha/api.js?render=r
eCAPTCHA_site_key"></script>

   <script>

   grecaptcha.ready(function() {

       grecaptcha.execute('reCAPTCHA_site_key',
{action: 'homepage'}).then(function(token) { ...});

 });  </script>
```

reCAPTCHA v3
(released 2018)

reCAPTCHA
v2 + v3

iOS

Mobile SDKs

reCAPTCHA
Enterprise
(released 2020)

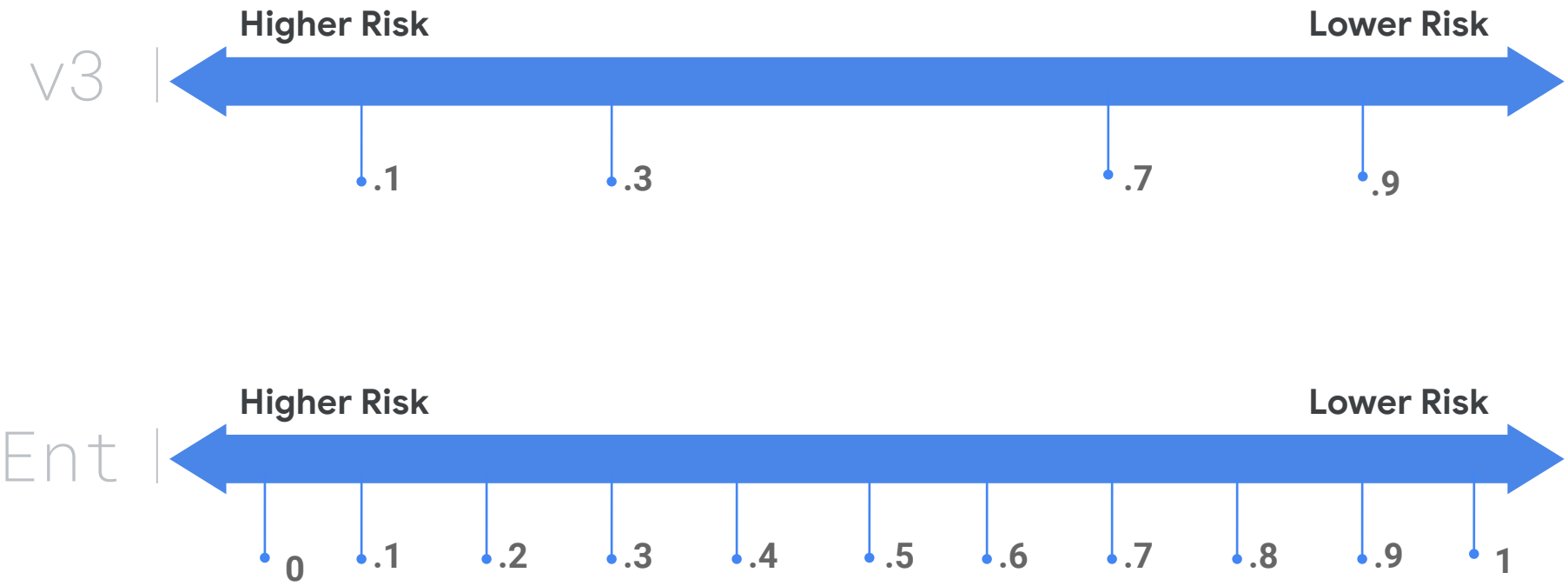
# バージョン比較

| | Enterprise | v3 | v2 |
|---|---|---|---|
| API コール | 無制限 | 月あたり 100 万コール | 月あたり 100 万コール |
| チェックボックス | 可能 | 可能 | ○ |
| チェックボックス無し | ○ | ○ | |
| リスクスコア | 11 段階 | 4 段階 | |
| 機械学習モデルカスタマイズ可 | ○ | | |
| サービスレベル契約 | ○ | | |
| Google Cloud 利用規約 | ○ | | |
| サポート | ○ | | |
| モバイル SDK | ○ | | |
| 二要素認証対応 | ○ | | |
| パスワード 漏洩確認 | ○ | | |

# reCPATCHA Enterprise の特徴

- 粒度の細かいリスク評価を提供
- Reason コードとその定義
- 機械学習モデルのカスタマイズ
- モバイル SDK (Android and iOS)
- パスワード漏洩確認 (レビュー必要)
- 2 段階認証 - SMS and Email (レビュー必要)

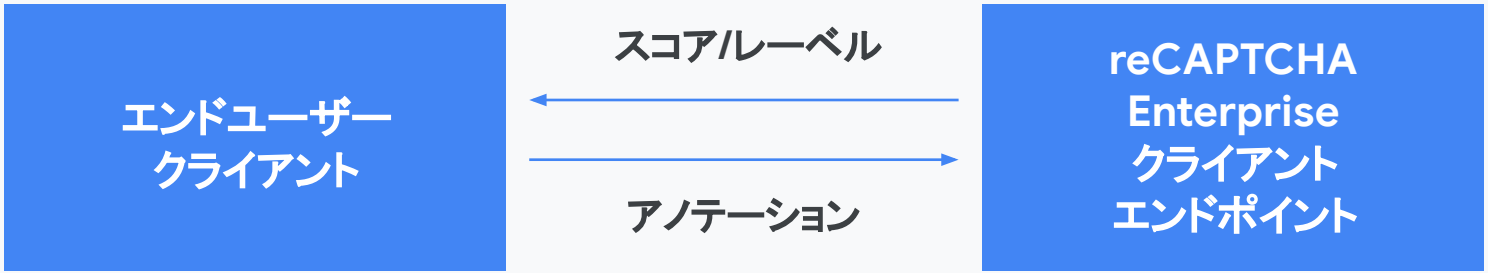
# 粒度の細かいリスクスコア



# Reasonコードとその定義

| REASON CODE | DESCRIPTION |
| --- | --- |
| AUTOMATION | インタラクションが自動化エージェントの動作と一致しています。 |
| UNEXPECTED_ENVIRONMENT | イベントの発生元が不正な環境です。 |
| UNEXPECTED_USAGE_PATTERNS | インタラクションが、想定したパターンと大きく異なっていました。 |
| TOO_MUCH_TRAFFIC | トラフィック量が通常よりも多いです。 |
| LOW_CONFIDENCE_SCORE | 質の高いリスク分析を行うにはトラフィック量が少なすぎます。 |

# 機械学習モデルのカスタマイズ



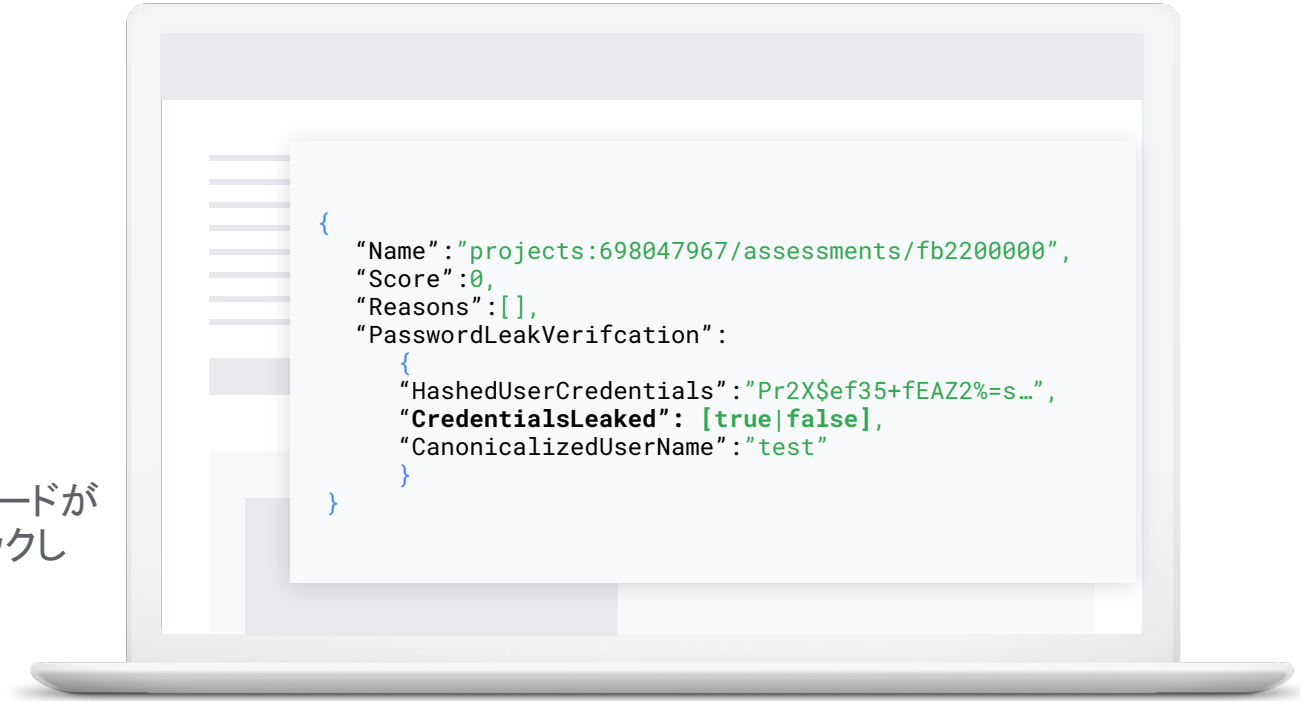
モバイル SDK

モバイルアプリも保護

iOS

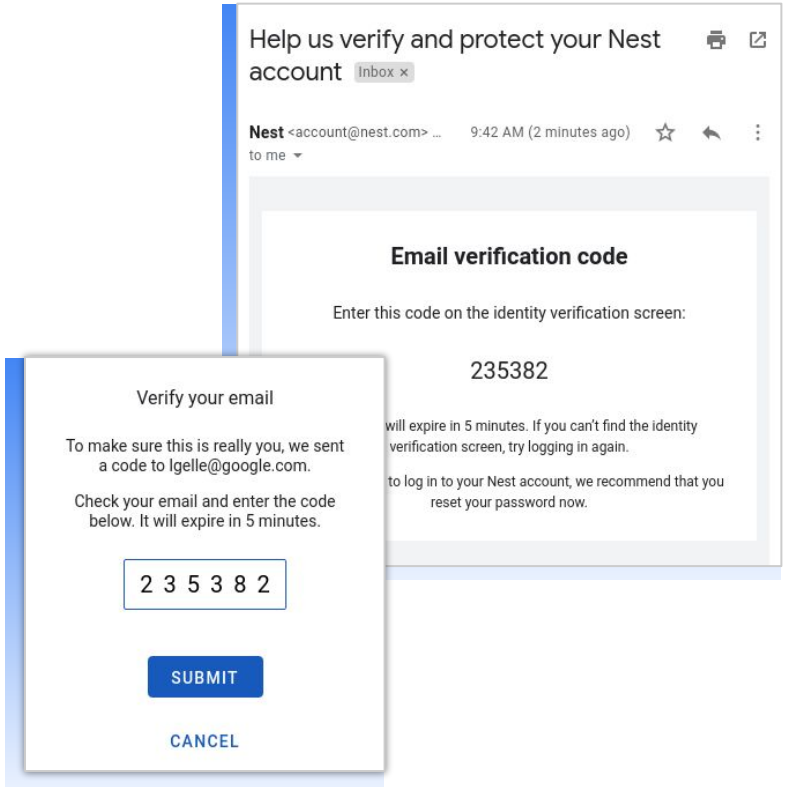
# パスワード漏洩確認

reCAPTCHA は、パスワードが漏洩していないかをチェックします



# 二要素認証

- Google のユーザーアカウント保護の経験がベース
- email と SMS による承認
- 他の手法もリリース予定



# 重大なセキュリティリスクから防御する最新機能

## 決済

- カーディングやチャージバックを防止
- 決済ページに組み込み
- reCAPTCHA スコアと類似する詐欺スコアを提供
- チャージバックデータ経由のモデルの調整
- 決済向けのインテリジェンス (将来追加予定)

## アカウント

- アカウントのハイジャック、アカウントの偽造、クレデンシャル スタッフィングを防止
- ログインページやサインアップ ページに組み込み
- 新しいユーザーデバイス特有の理由コードを提供
- ログインの成功/失敗データ経由でのモデルの調整

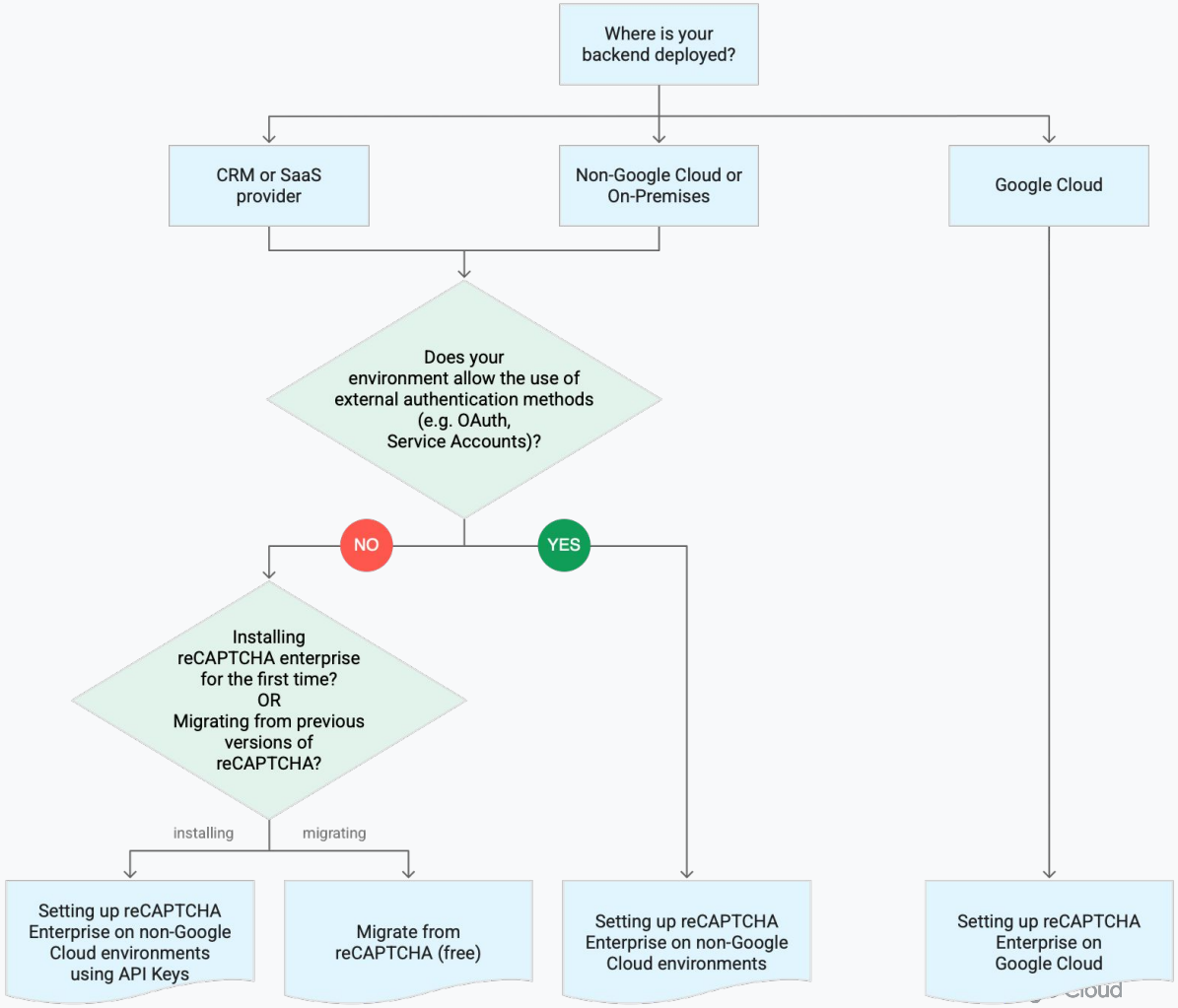
# reCPATCHA Enterprise の特徴

- 粒度の細かいリスク評価を提供
- Reason コードとその定義
- 機械学習モデルのカスタマイズ
- モバイル SDK (Android and iOS)
- パスワード漏洩確認 (レビュー必要)
- 2 段階認証 - SMS and Email (レビュー必要)

# reCAPTCHA Enterprise の仕組みと導入ポイント

# reCAPTCHA Enterprise のセットアップ方法の選択

- ✅ バックエンドのロケーション
- ✅ 認証方法
- ✅ デプロイのタイプ




[reCAPTCHA Enterprise のセットアップ方法の選択]

# reCAPTCHA Enterprise の仕組み

# reCAPTCHA Enterprise の仕組み

# reCAPTCHA インストール

👨‍💻 API を有効にする
👨‍💻 API キーを入手する
👨‍💻 コードを挿入する
📞 100 万件 / 月 もしくは
フル機能を利用するために
Google Cloud セールスに
連絡する

```
<!-- スクリプトの読み込み  -->
<head>
 <script src="https://www.google.com/recaptcha/enterprise.js?render=SITE_KEY"></script>
 ....
 </head>


<!-- たとえば LOGIN イベントに reCAPTCHA Enterprise を追加する: -->
 <script>
   function onClick(e) {
     e.preventDefault();
     grecaptcha.enterprise.ready(async () => {
       const token = await grecaptcha.enterprise.execute('SITE_KEY', {action: 'LOGIN'});
       // IMPORTANT: The 'token' that results from execute is an encrypted response sent by
       // reCAPTCHA Enterprise to the end user's browser.
       // This token must be validated by creating an assessment.
       // See https://cloud.google.com/recaptcha-enterprise/docs/create-assessment
     });
   }
  </script>


<!-- たとえば ページのロードに reCAPTCHA Enterprise を追加する: -->
<script>
 grecaptcha.enterprise.ready(function() {
     grecaptcha.enterprise.execute('SITE_KEY', {action: 'homepage'}).then(function(token) {
        // IMPORTANT: The 'token' that results from execute is an encrypted response sent by
        // reCAPTCHA Enterprise to the end user's browser.
        // This token must be validated by creating an assessment.
        // See https://cloud.google.com/recaptcha-enterprise/docs/create-assessment
     });
 });
</script>
```

# reCAPTCHA Enterprise の仕組み

# reCAPTCHA アセスメント

5. バックエンドが reCAPTCHA トークンをサーバーエンドポイントに送信

```
const { RecaptchaEnterpriseServiceClient } = require("@google-cloud/recaptcha-enterprise");

/**
* Create an assessment to analyze the risk of an UI action. Note that
* this example does set error boundaries and returns `null` for
* exceptions.
*
* projectID: GCloud Project ID
* recaptchaSiteKey: Site key obtained by registering a domain/app to use recaptcha services.
* token: The token obtained from the client on passing the recaptchaSiteKey.
* recaptchaAction: Action name corresponding to the token.
*/
async function createAssessment({
 projectID = "your-project-id",
 recaptchaSiteKey = "your-recaptcha-site-key",
 token = "action-token",
 recaptchaAction = "action-name",
}) {
 // Create the reCAPTCHA client & set the project path. There are multiple
 // ways to authenticate your client. For more information see:
 // https://cloud.google.com/docs/authentication
 // TODO: To avoid memory issues, move this client generation outside
 // of this example, and cache it (recommended) or call client.close()
 // before exiting this method.
 const client = new RecaptchaEnterpriseServiceClient();
 const projectPath = client.projectPath(projectID);

 // Build the assessment request.
 const request = {
   assessment: {
     event: {
       token: token,
       siteKey: recaptchaSiteKey,
     },
   },
   parent: projectPath,
 };

 // client.createAssessment() can return a Promise or take a Callback
 const [response] = await client.createAssessment(request);
```

# reCAPTCHA アセスメント

7. reCAPTCHA サーバー エンドポイントが、トークンから復号されたデータと、内部ソースからの他のデータを返す

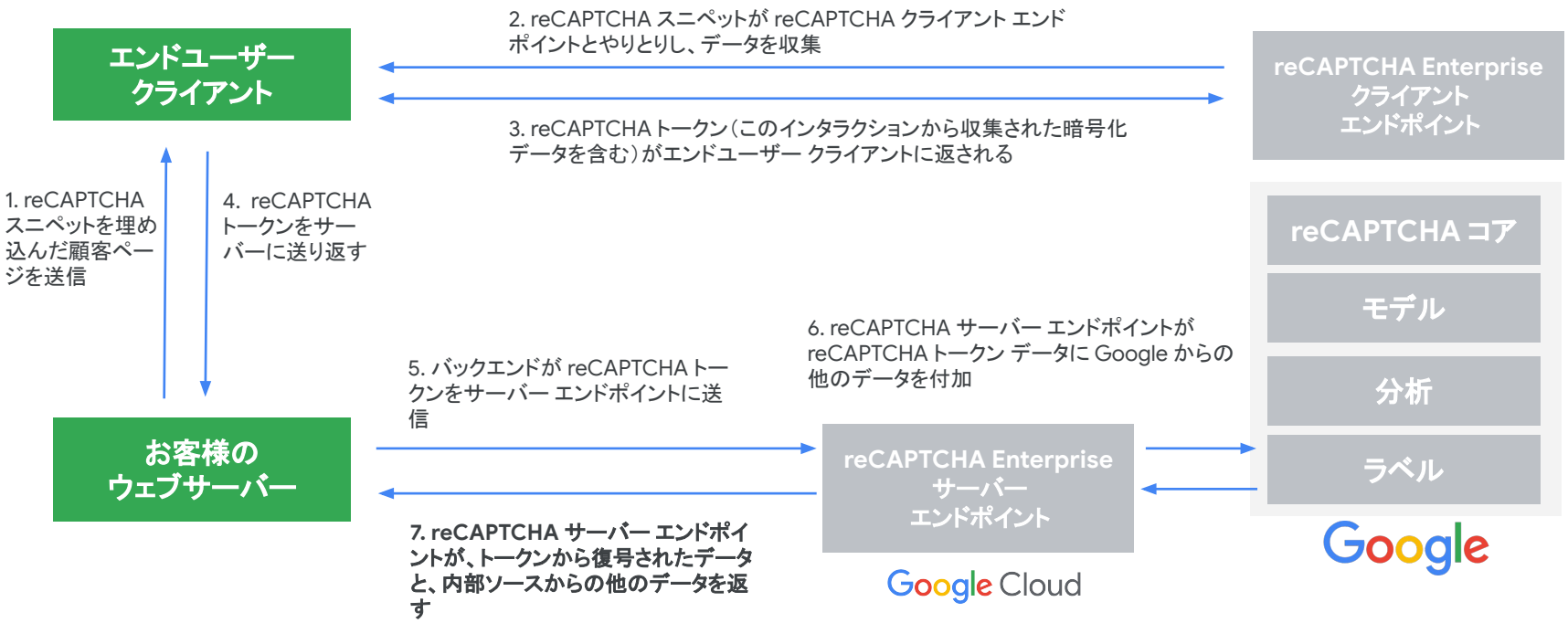
```
// Check if the token is valid.
 if (!response.tokenProperties.valid) {
   console.log(
     "The CreateAssessment call failed because the token was: " +
       response.tokenProperties.invalidReason
   );

   return null;
 }

 // Check if the expected action was executed.
 // The `action` property is set by user client in the
 // grecaptcha.enterprise.execute() method.
 if (response.tokenProperties.action === recaptchaAction) {
   // Get the risk score and the reason(s).
   // For more information on interpreting the assessment,
   // see: https://cloud.google.com/recaptcha-enterprise/docs/interpret-assessment
   console.log("The reCAPTCHA score is: " + response.riskAnalysis.score);

   response.riskAnalysis.reasons.forEach((reason) => {
     console.log(reason);
   });
   return response.riskAnalysis.score;
 } else {
   console.log(
     "The action attribute in your reCAPTCHA tag " +
       "does not match the action you are expecting to score"
   );
   return null;
 }
}
```

# reCAPTCHA Enterprise の仕組み

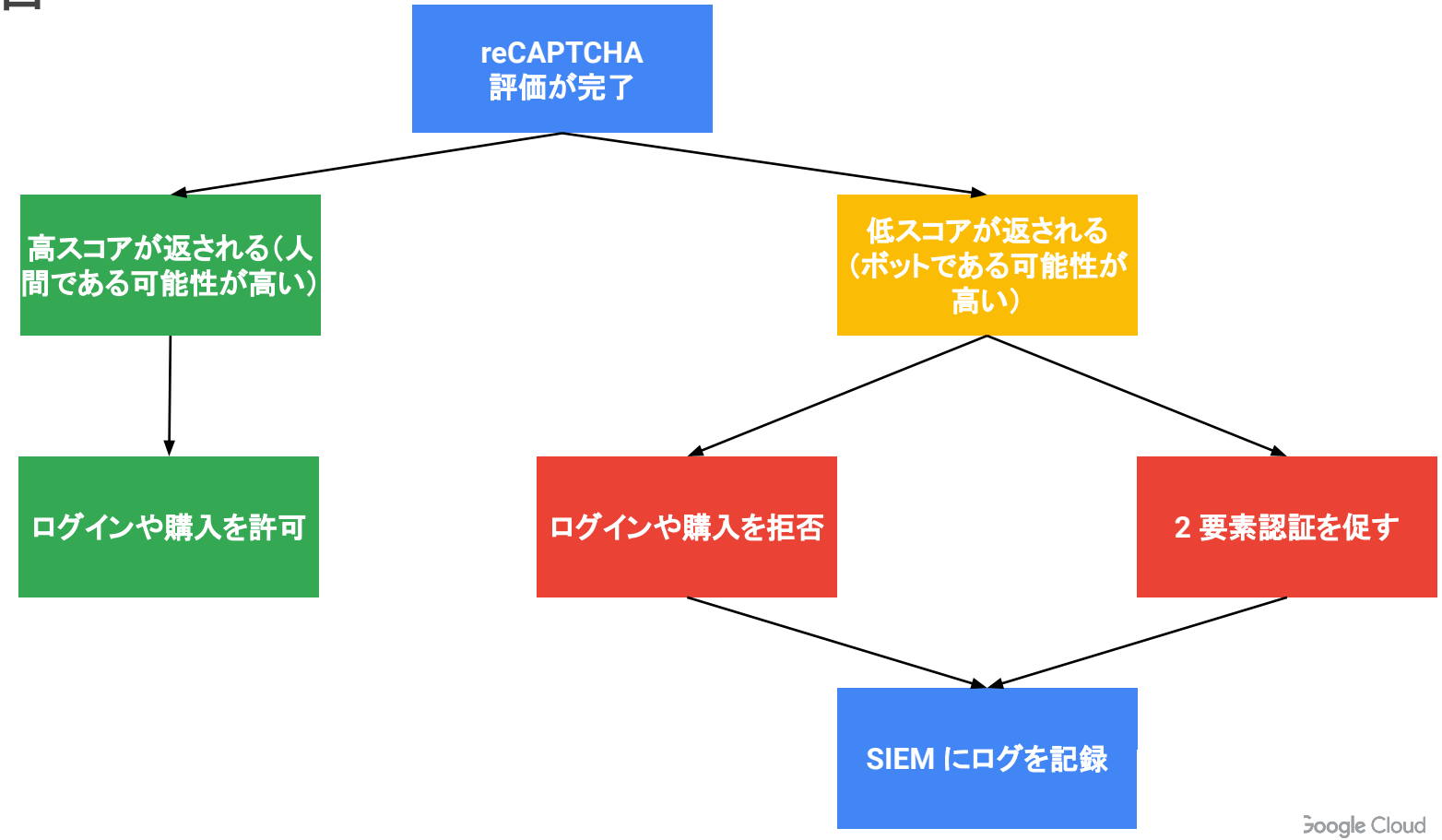


# reCAPTCHA アセスメントの解釈

レスポンスを確認してアクションを決定する

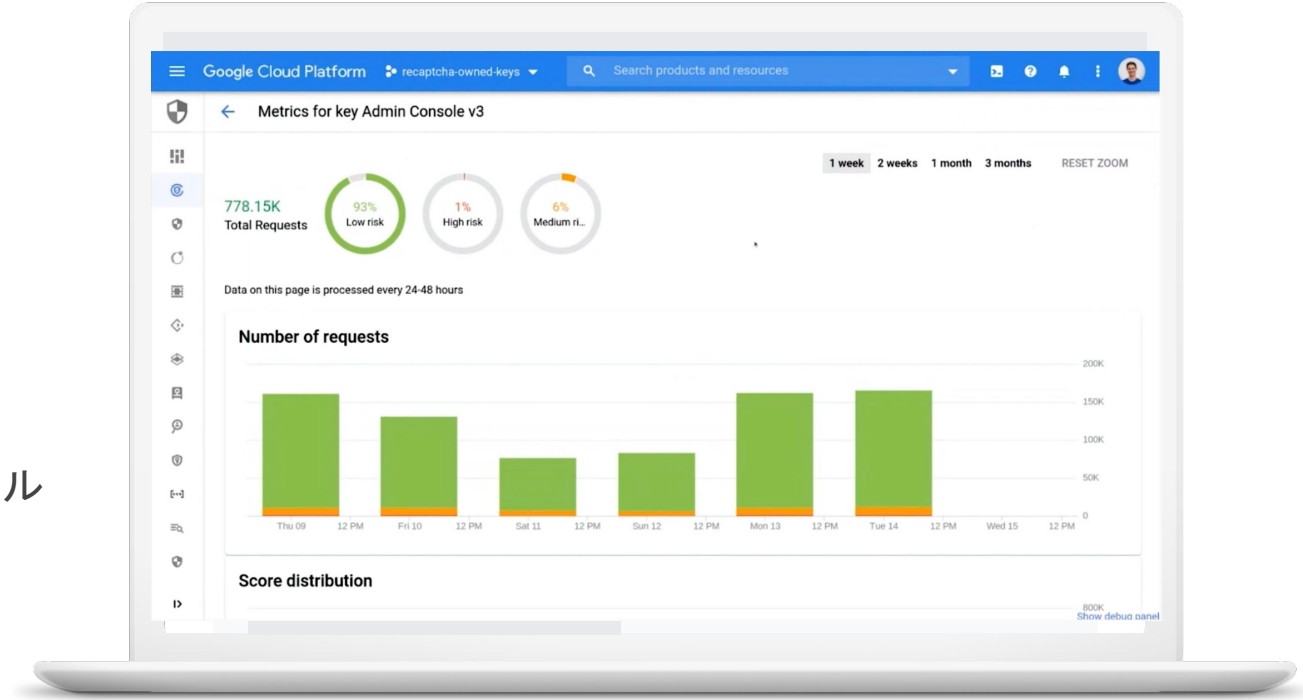
```
{
 "event": {
   "expectedAction": "EXPECTED_ACTION",
   "hashedAccountId": "ACCOUNT_ID",
   "siteKey": "SITE_KEY",
   "token": "TOKEN",
   "userAgent": "(USER-PROVIDED STRING)",
   "userIpAddress": "USER_PROVIDED_IP_ADDRESS"
 },
 "name": "ASSESSMENT_ID",
 "riskAnalysis": {
   "reasons": ['AUTOMATION'],
   "score": 0.1
 },
 "tokenProperties": {
   "action": "USER_INTERACTION",
   "createTime": "TIMESTAMP",
   "hostname": "HOSTNAME",
   "invalidReason": "(ENUM)",
   "valid": "(BOOLEAN)"
 }
}
```

# 対処フロー


reCAPTCHA
評価が完了
高スコアが返される（人間である可能性が高い）
低スコアが返される（ボットである可能性が高い）
ログインや購入を許可
ログインや購入を拒否
2 要素認証を促す
SIEM にログを記録

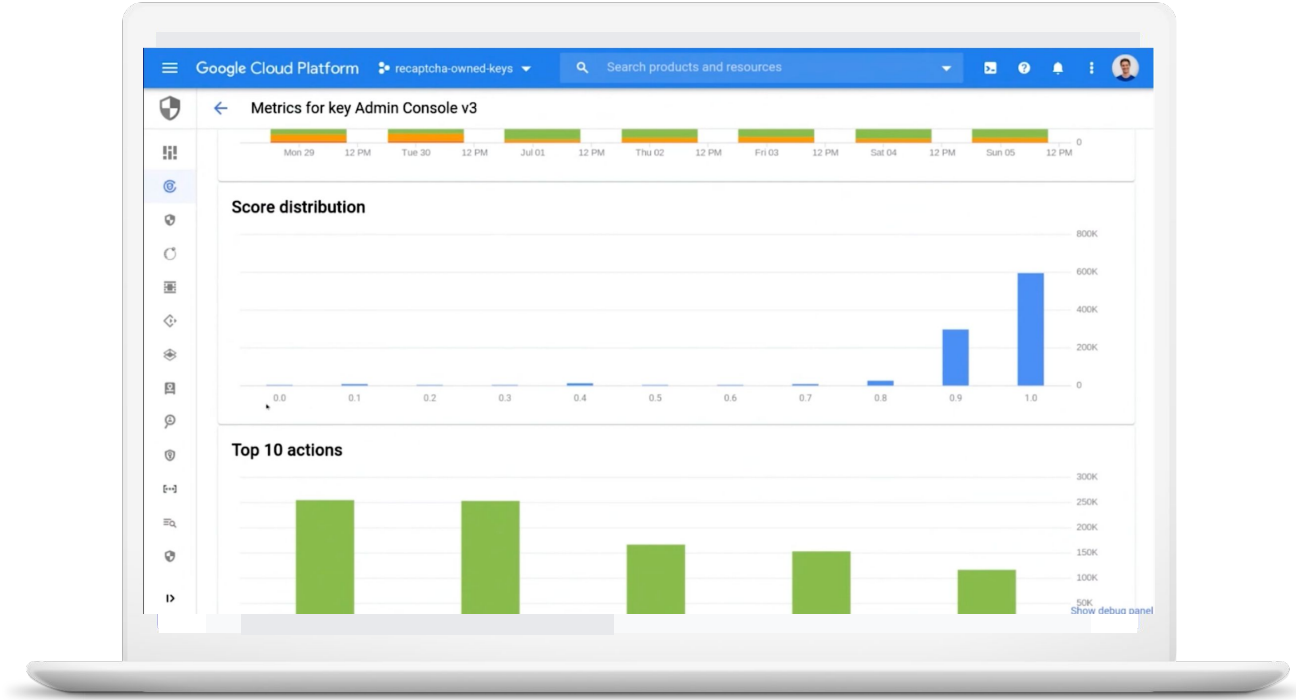
# メトリック ダッシュボード

Google Cloud コンソール ダッシュボード



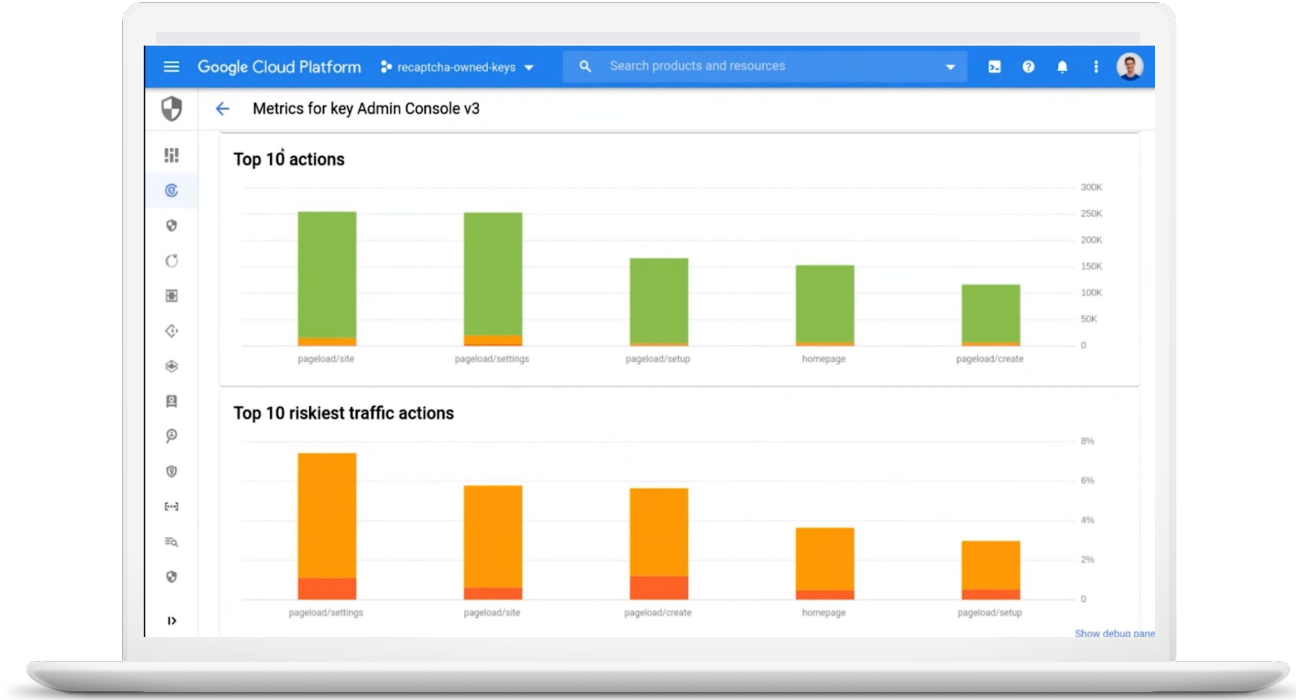
# メトリック ダッシュボード

スコア分布



# メトリック ダッシュボード

トップ 10 アクション などの統計



# 事例紹介

# ユーザー体験の維持と不正ボット対策を実現

## Etsy について

- 520 万人の販売者
- 9050 万人のアクティブな購入者
- 企業の目標は”Keep Commerce Human”

## 課題

- ボットトラフィックの増加 - クレデンシャル スタッフィング

## reCAPTCHA Enterprise の活用方法

- 柔軟性が可能とするほぼリアルタイムの情報に基づく意思決定
- ゼロ ユーザー インタラクション
- 可視化することで最もリスクが高いウェブサイト部分を把握
- 機械学習モデルによるカスタマイズ

# Thank you.

Google Cloud