エコシステムのための認証基盤と reCAPTCHA Enterprise

ピクシブ株式会社
技術開発本部インフラ部 エンジニア
小堀晋太郎

Google Cloud

About me

- 2018/04 中途入社
- pixiv運営本部 エンジニア → インフラ部 エンジニア
- プロダクトセキュリティからコーポレートセキュリティまで幅広く携わる
- 脆弱性診断、脆弱性報奨金制度の運用、開発、レビュー、...
- CSIRT設立、コーポインフラ、資産管理、...

pixiv Inc.

- 「創作活動がもっと楽しくなる場所を創る」
- イラスト・小説投稿SNS「pixiv」を始めとして、創作活動を支援する事業を展開
- SNS、Eコマース、パトロン、VR、etc...

pixiv

- イラスト・小説投稿SNS
- 6000万+ユーザー
- 9000万+作品

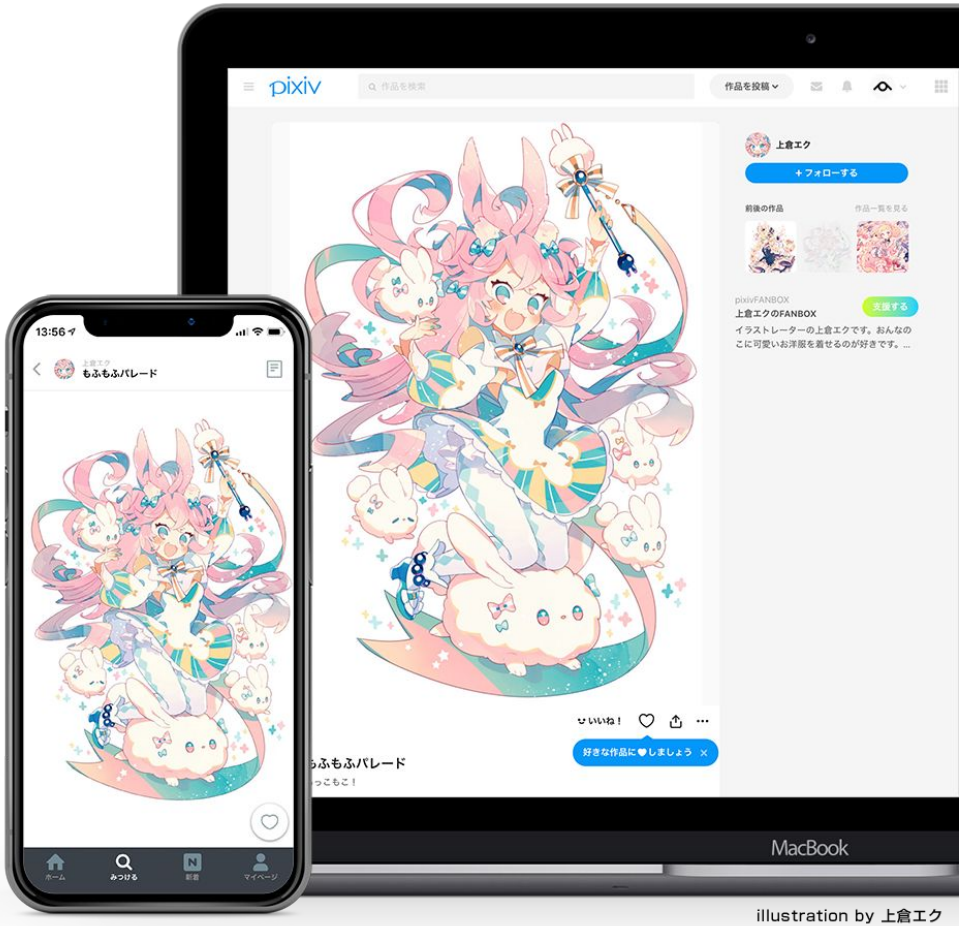


illustration by 上倉エク

Google Cloud

pixiv Inc.

Google Cloud

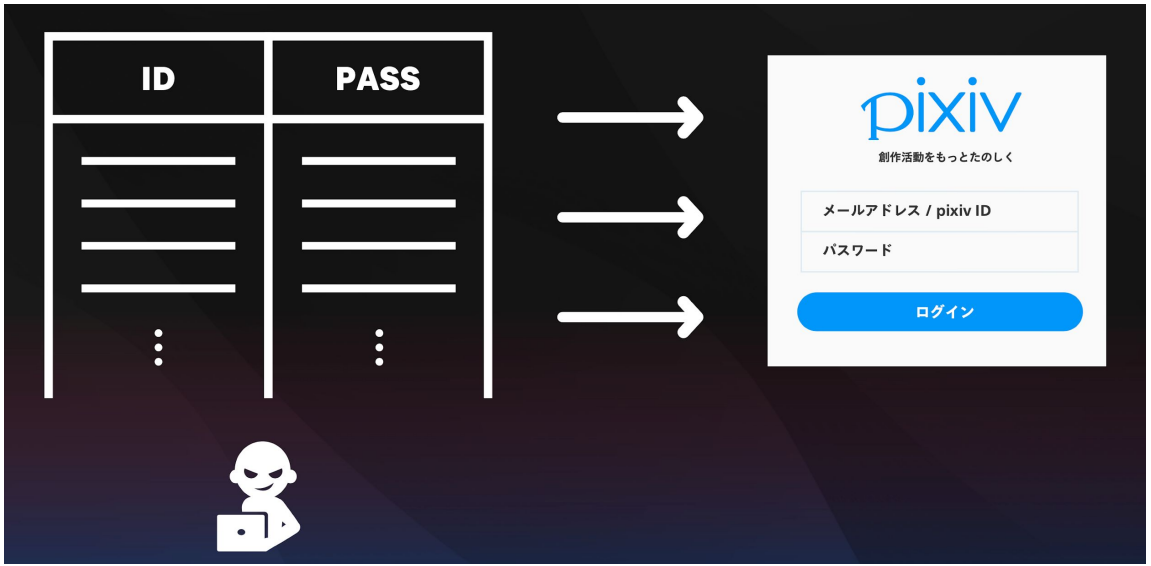
Agenda

- 認証基盤におけるBot対策の必要性
- pixivの認証基盤について
- reCAPTCHA Enterprise

認証基盤におけるBot対策の必要性

パスワードリスト型攻撃

- 様々なサイトから漏洩したID/パスワードのDBを利用して他のサイトにログインを試行する攻撃



パスワードリスト型攻撃

- 漏洩パスワードリストは誰でも簡単に入手可能
- リスト型攻撃を実施するツールも流通

14億件の平文ログインデータが漏洩、最多のパスワードは?

2017/12/15 09:45

著者：後藤大地

URLをコピー

このほど4iQに掲載された記事「1.4 Billion Clear Text Credentials Discovered in a Single Database」が、ダークWebにおいて14億件を超えるアカウントデータを含んだファイルおよびデータベースを発見したと伝えた。

これまでダークWebで発見された流出アカウントデータとしては過去最大規模で、調査の結果、流出したアカウントデータが本物であることも確認されたという。

パスワードリスト型攻撃

7pay不正アクセスの原因は「リスト型攻撃の可能性が高い」　7iDパスワードを一斉リセット

2019年07月30日 18時12分 公開　　[田中聡，ITmedia]

印刷　63　Share　B! 18

セブン&アイ・ホールディングスは、不正アクセスを受けたコード決済「7pay」のセキュリティ対策の一環で、7月30日に7iDパスワードの一斉リセットを行った。

同社によると、7payの不正アクセスの原因は、あらかじめ入手したIDとパスワードを用いて不正アクセスをする「リスト型攻撃」の可能性が高いという。そのため、パスワードとIDの情報が第三者に取得されていたとしても、パスワードをリセットすることで、リスクを最小化できると考えたとのこと。

パスワードリスト型攻撃

- パスワードリスト型攻撃でスクリーニングされたSpotifyの認証情報のリストが発見された事例 (2020/11)

https://www.vpnmentor.com/blog/report-spotify-scam/

パスワードリスト型攻撃

お知らせトップ お知らせ 2016年12月2日 のお知らせ

【重要】pixivの一部アカウントに対する「なりすましログイン」の報告とパスワード変更のお願い

2016年12月2日　　共有

pixiv事務局です。

pixivの一部のアカウントで、他社サービスより流出したID・パスワードをもとにした第三者からの「なりすましログイン」を確認いたしました。「リスト型アカウントハッキング」の手法で2016年11月29日（火）18時00分ごろから発生し、なりすましログインされたアカウント数は、3,646件となります。
該当アカウントを保有するユーザーの皆さまへは、12月2日（金）21時15分にメールとpixivのメッセージにてご案内をお送りしておりますので、大変お手数ですがご確認をお願いいたします。
なお、今回のなりすましログインによる登録情報の改ざんや、クレジットカード情報の不正利用が行われた形跡はございません。

リスト型アカウントハッキングとは
第三者が不正に取得したID・パスワードを利用し、これらのID・パスワードを様々なサイトを対象にログインを試みることで、個人情報の閲覧等を行うサイバー攻撃のこと（※）

※「リスト型アカウントハッキング」に関する総務省資料：「リスト型アカウントハッキングによる不正ログインへの対応方策について」
http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000063.html

Google Cloud

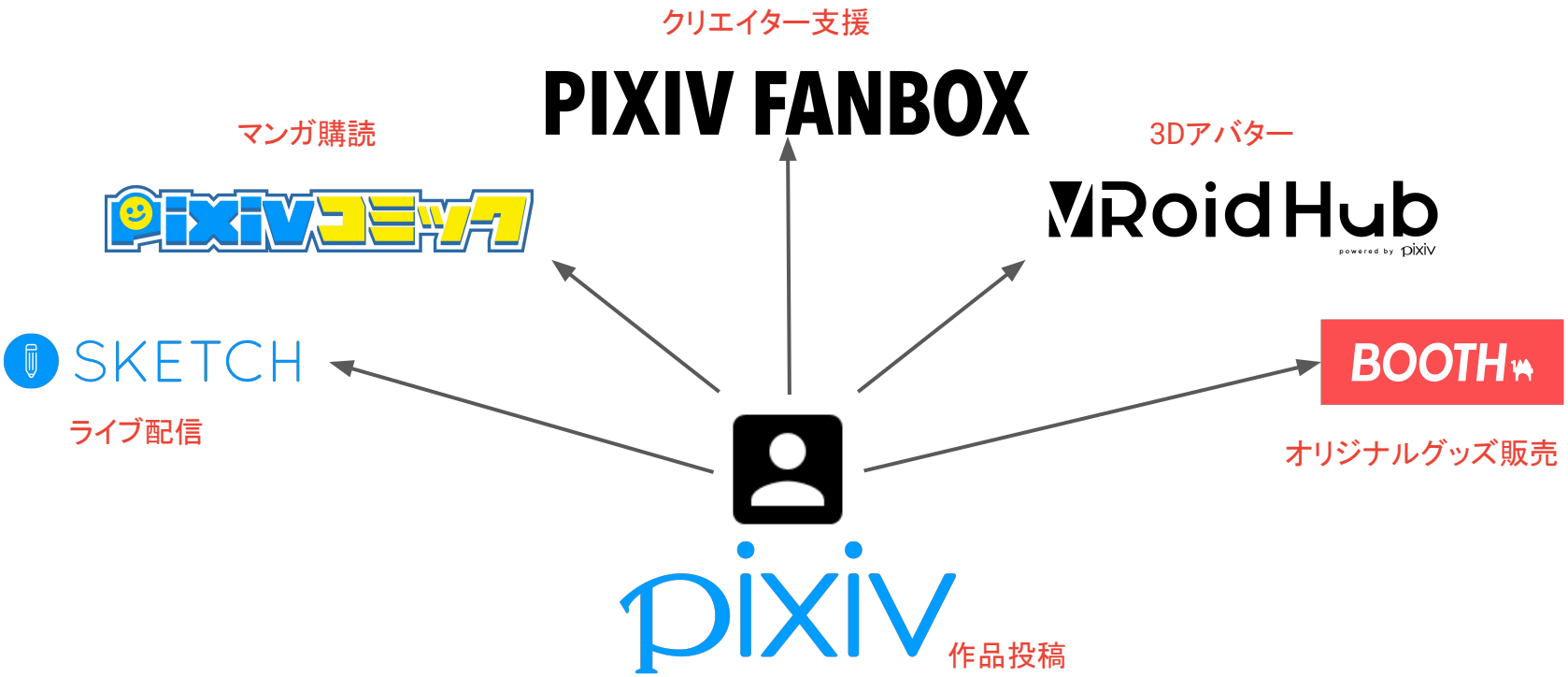
対策

- 多要素認証
  - 現在の最善策
  - ユーザに設定させる必要がある
  - 実装してもごく一部のユーザしか利用してくれない場合も
- レートリミット
  - 試行回数制限 → 単純なものでは不十分
    - 攻撃者はVPNやbotnetで大量のIPアドレスを利用可能
    - Low and slowな攻撃パターンも
  - ログイン試行を自動化できないようBot対策が必要
- and more...

pixivの認証基盤

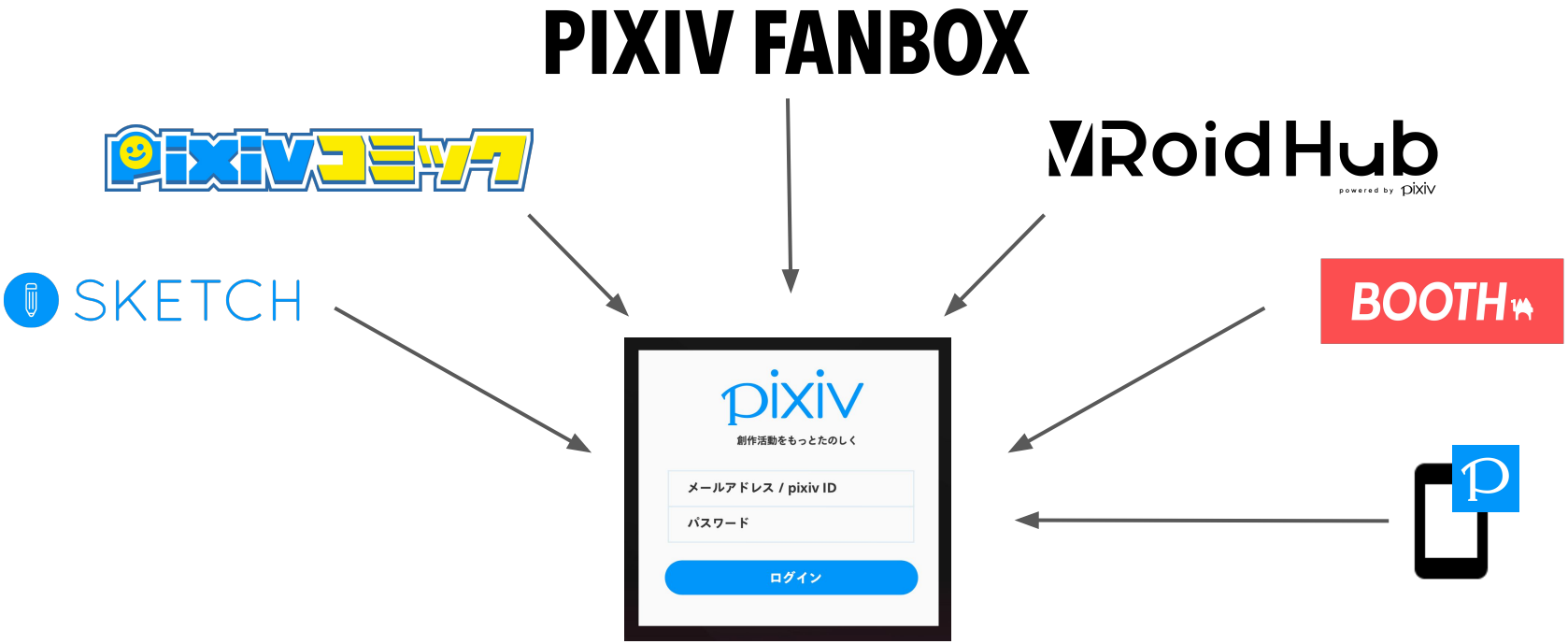
1 pixiv account

1 pixiv account

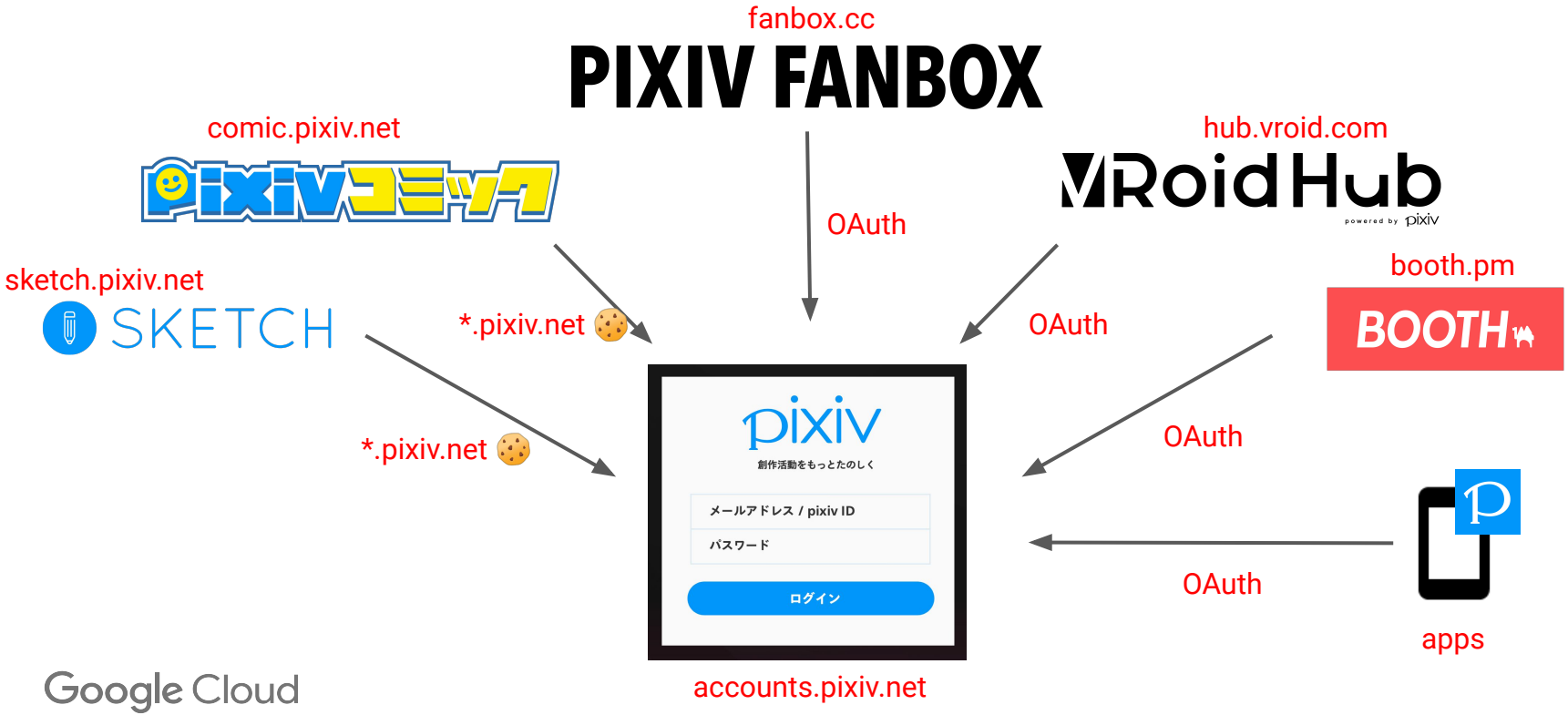


Google Cloud

1 pixiv account

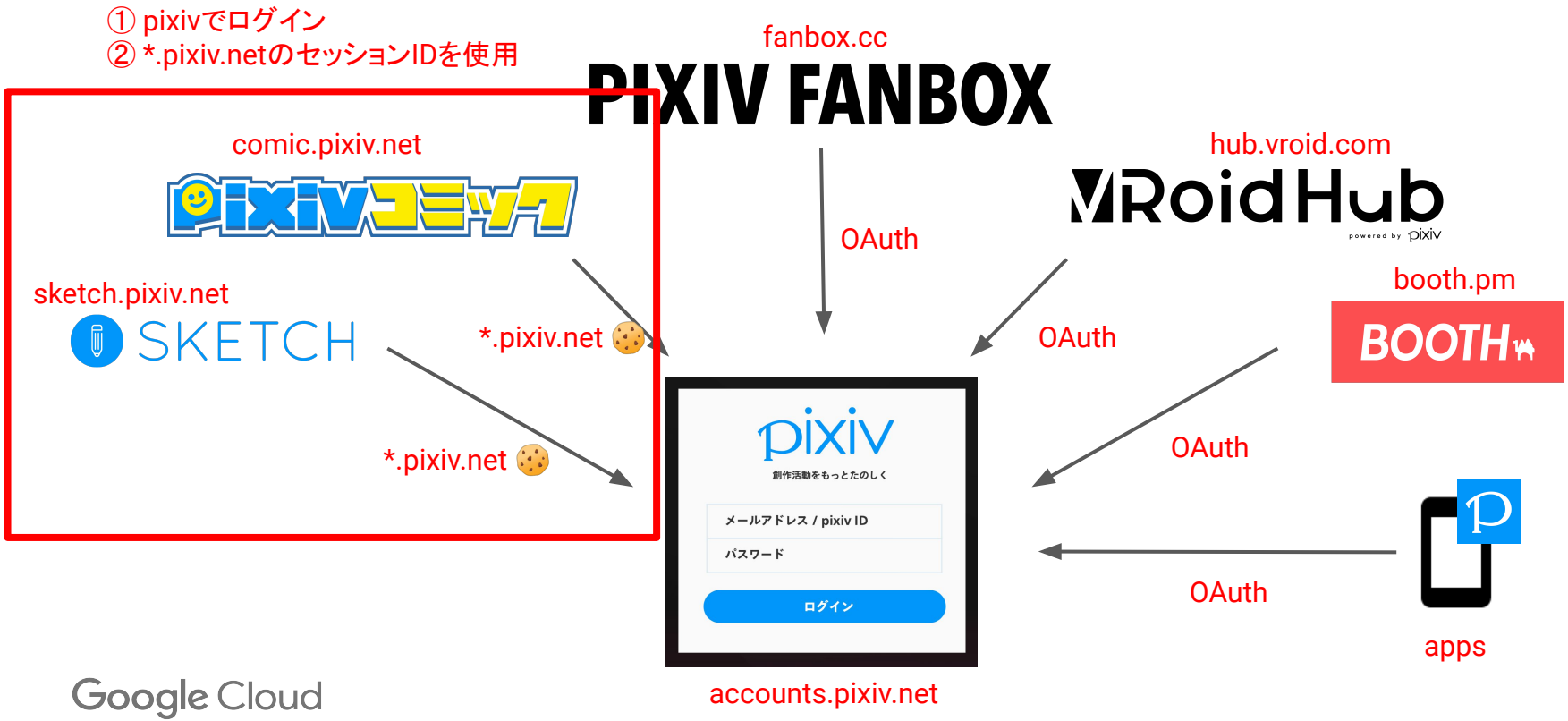


1 pixiv account



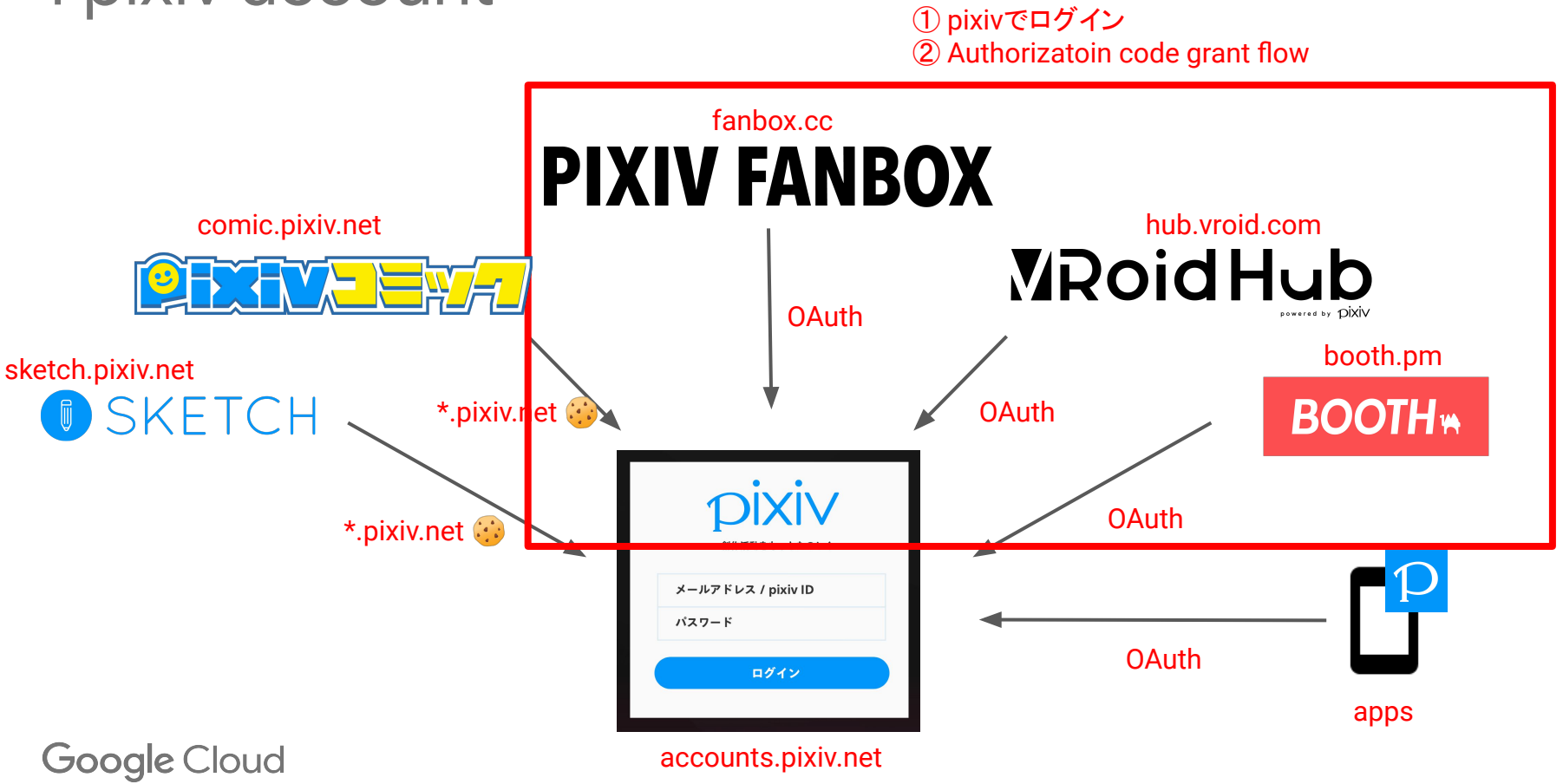
Google Cloud

1 pixiv account



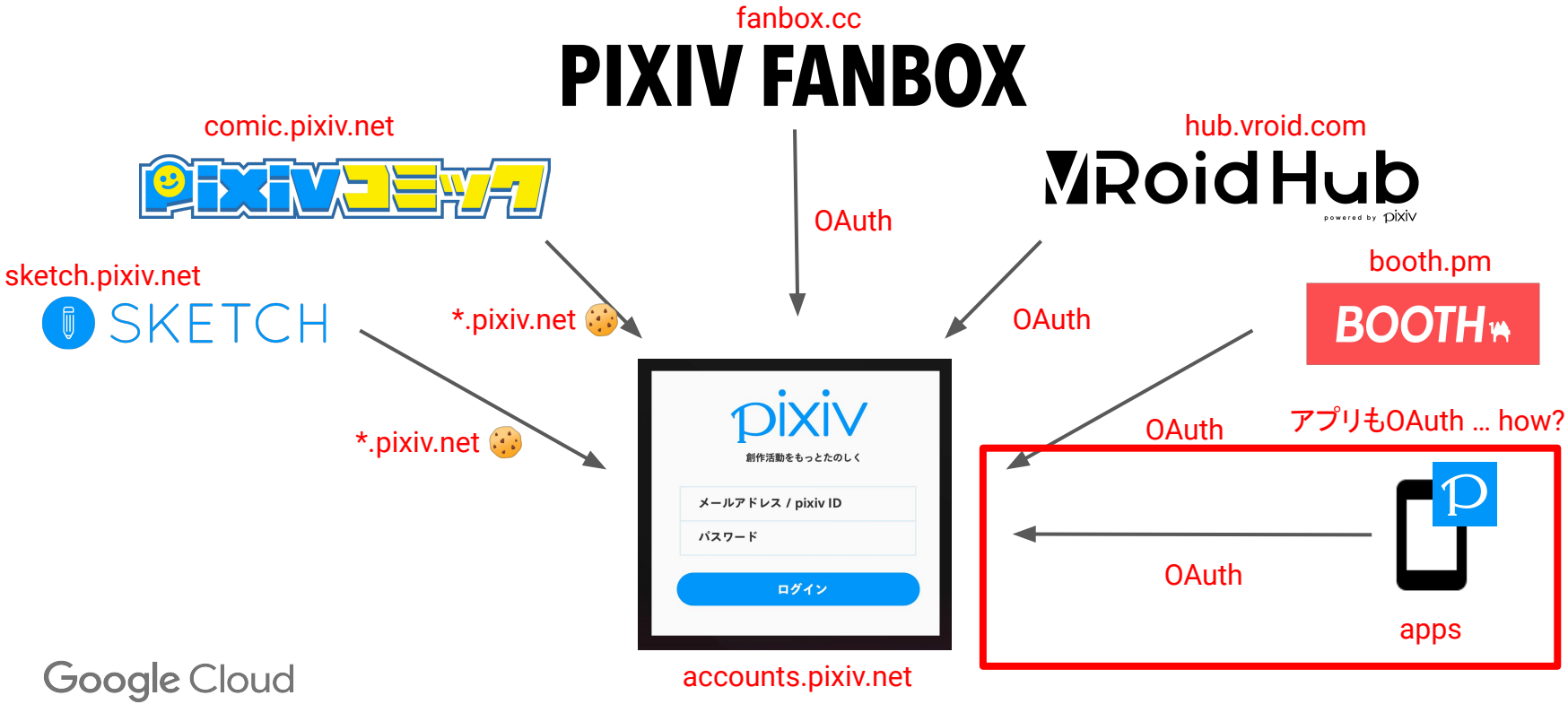
Google Cloud

1 pixiv account



Google Cloud

1 pixiv account



アプリOAuth方式

- Before: Password grant flow
  - アプリ専用の認証API
  - アプリが直接APIにID / Passwordを送信して、bearer tokenを受け取る
- After: Authorization code grant flow
  - アプリからブラウザを呼び出してPIXIV共通ログインフォームにアクセス
  - ログイン完了後、Auth. code grant flowを実行
  - ブラウザはAuth. codeをアプリに渡して終了。アプリはAuth. codeをpixivのOAuth APIに送ってbearer tokenを受け取る

アプリOAuth - Before

id=...&password=...

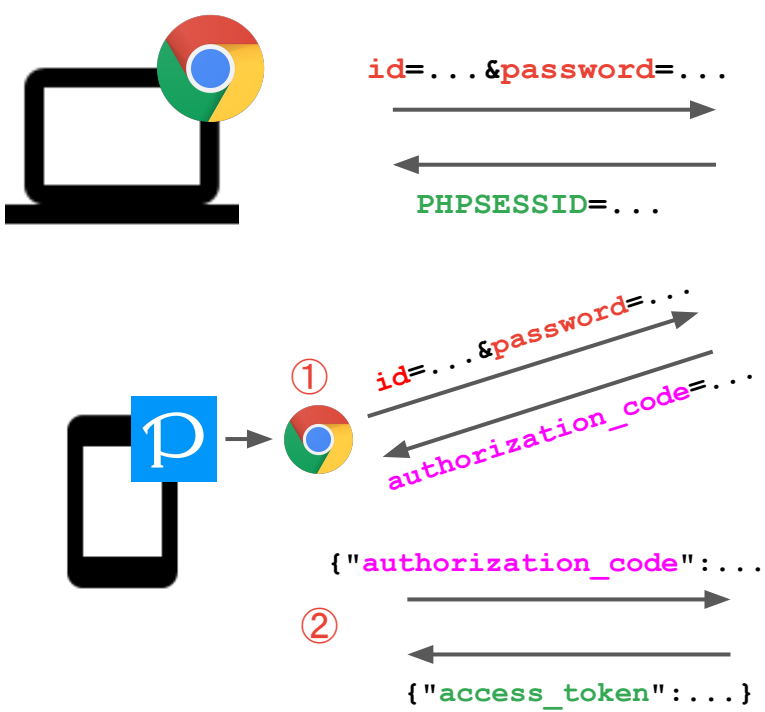
PHPSESSID=...

ID / Passwordを受け付けるAPIが複数存在

{"id":"...","password":...}

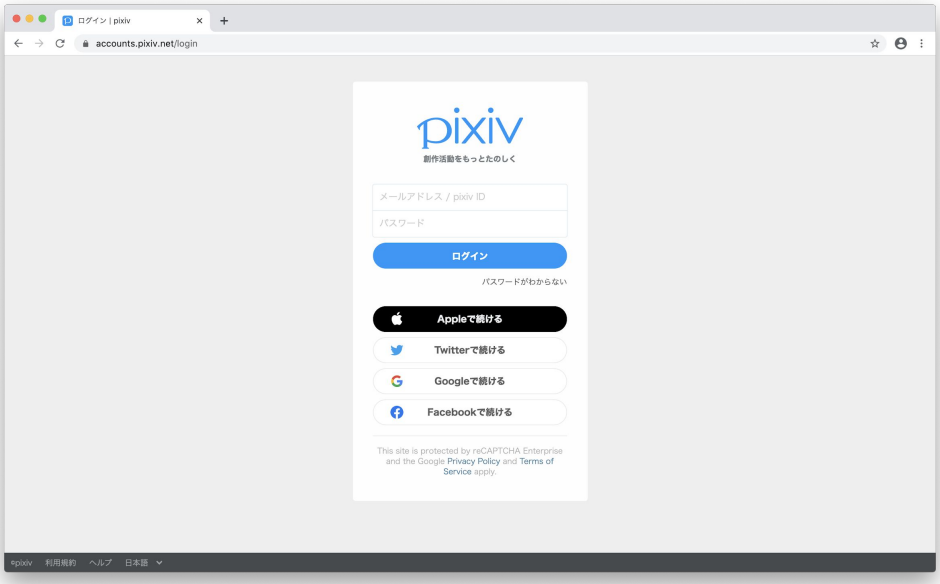
{"access_token":...}

アプリOAuth - After



ID / Passwordを受け付けるAPIは1つだけ

OAuth API



Google Cloud

RFC8252

- OAuth 2.0 for Native Apps
  - ネイティブアプリでOAuthする際のベストプラクティス
  - アプリからブラウザを呼び出してAuthorization code grant flowを実行する
  - アプリのカスタムURLスキーマを通じてauthorization codeを受け取る
  - PKCEを使用してauthorization codeを保護する
- Google系アプリ、GitHubアプリなどもこのパターン

変更前の方式の問題

- 認証エンドポイントが複数存在することになる
  - 実装の相違、メンテナンスコストが2倍、機能追加が困難
- ネイティブアプリはBot対策がしづらい
  - ID / パスワードを受け付けるAPIにはbot対策が必要
  - WAF型
    - 振る舞い検知型の高精度な検知ができない
    - 典型的にはIPアドレス、アクセス頻度のみで判断
  - SDK組み込み型
    - 導入、展開が難しい場合がある
    - PC版のログインエンドポイントと同じソリューションが使えない可能性

変更後の方式のメリット

- RFCに準拠
  - 標準に従うことで将来的な拡張性、メンテナビリティ向上
- 認証エンドポイントがウェブに統一される
  - 認証ロジックを複数実装する必要がない
  - コードが1箇所なので機能追加が容易
    - 例: Sign in with Apple
- PCと共通のウェブベースのBot対策ソリューションが使える
  - pixivの場合 reCAPTCHA

ここまでのまとめ

- PC、アプリ含む全プロダクトでウェブベースの共通の認証エンドポイントを利用するよう統一した
- そのおかげで認証のBot対策も1つの仕組み = reCAPTCHAでできた

reCAPTCHA Enterprise

reCAPTCHA Enterprise

- Bot対策ソリューションreCAPTCHAの有償版
- JavaScriptでクライアントの「Botらしさ」を判定
- reCAPTCHA (v2 / v3) の機能 + Enterprise機能
- Bot対策ソリューションの中でも、特にアカウント乗っ取り対策に特化

reCAPTCHA v2
チャレンジあり

reCAPTCHA v3
チャレンジなし

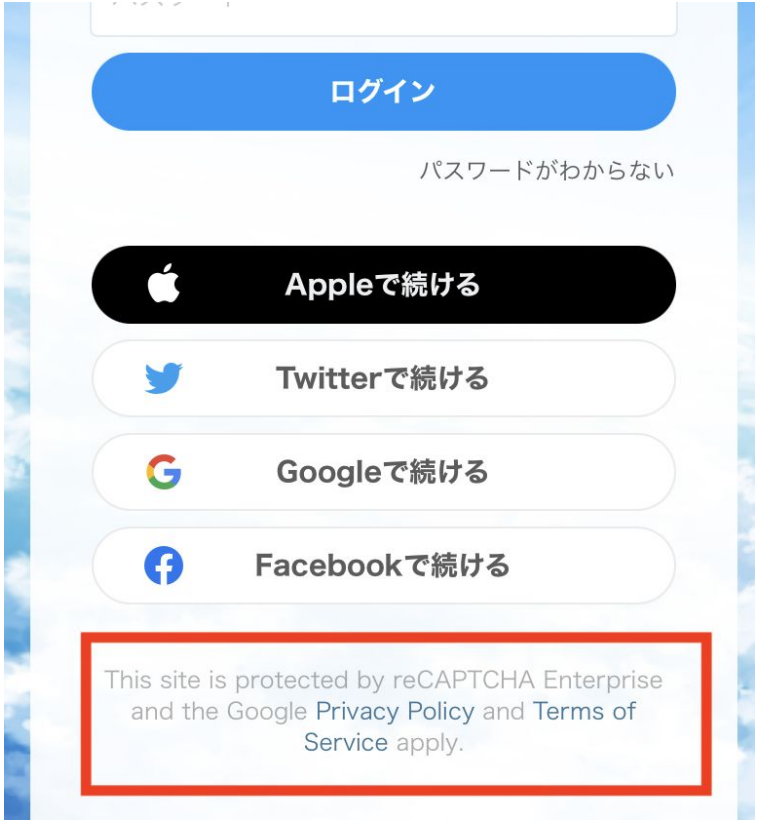
Google Cloud

reCAPTCHA (無償) との違い

	reCAPTCHA	reCAPTCHA Enterprise
CHECKBOX (v2)	✔	✔
SCORE (v3)	✔	✔
SCORE粒度	4段階	11段階
モデルチューニング	-	✔
APIコール数	100万コール/月まで	制限無し (従量課金)
Password Checkup (beta)	-	✔
Account Verification (beta)	-	✔
iOS / Android SDK (beta)	-	✔

reCAPTCHA @ pixiv

- SCOREとCHECKBOXを併用
- まずBotらしさのSCOREを計算し、人間と判断されればパス
- SCOREが低かった場合、CHECKBOX (CAPTCHA) にフォールバック
  - SCOREでロックアウトされないようにするため
- ただ、最近のドキュメントによるとこの方法は非推奨らしい……
  - 推奨はSCOREが低い場合に別の認証要素 (PINなど) を要求



reCAPTCHA @ pixiv

- アカウントのスクリーニング防止
  - スクリーニング→リスト型攻撃 阻止

Google Cloud

reCAPTCHA @ pixiv

- スパムや脆弱性スキャナによるノイズを削減

その他

漏洩パスワードDBとの照合

- インターネットに流出した漏洩パスワードのDBと照合し、脆弱なパスワードを検出
- 漏洩パスワードDBはHave I Been Pwned提供のハッシュ化されたDBを使用
- 照合はユーザがパスワードを入力した際にオンメモリで実施

ピクシブ、脆弱なパスワードを登録不可に　“漏えいリスト”と照合

2020年01月28日 14時40分 公開　[ITmedia]

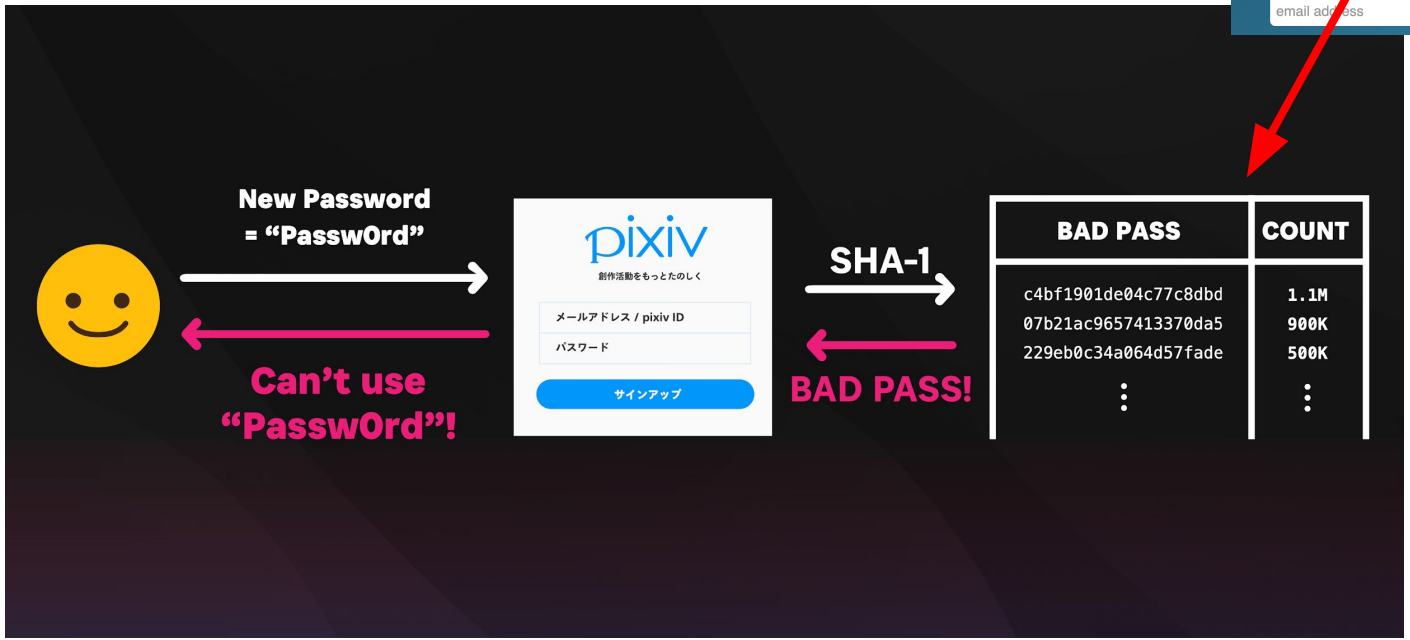
印刷　167　Share　B! 7

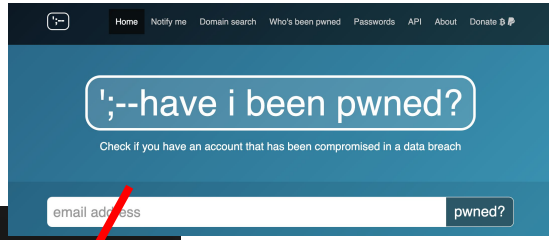
ピクシブはこのほど、イラストSNS「pixiv」で、脆弱（ぜいじゃく）なパスワードを登録できないようにしたと発表した。過去に他社サイトで漏えいしたパスワードのリストを活用。簡単なパスワードや、複数のサイトで使い回しされているパスワードを排除し、パスワードリスト型攻撃の被害を抑えるという。

ピクシブによる発表

Google Cloud

漏洩パスワードDBとの照合





HIBP vs Password Checkup (beta)

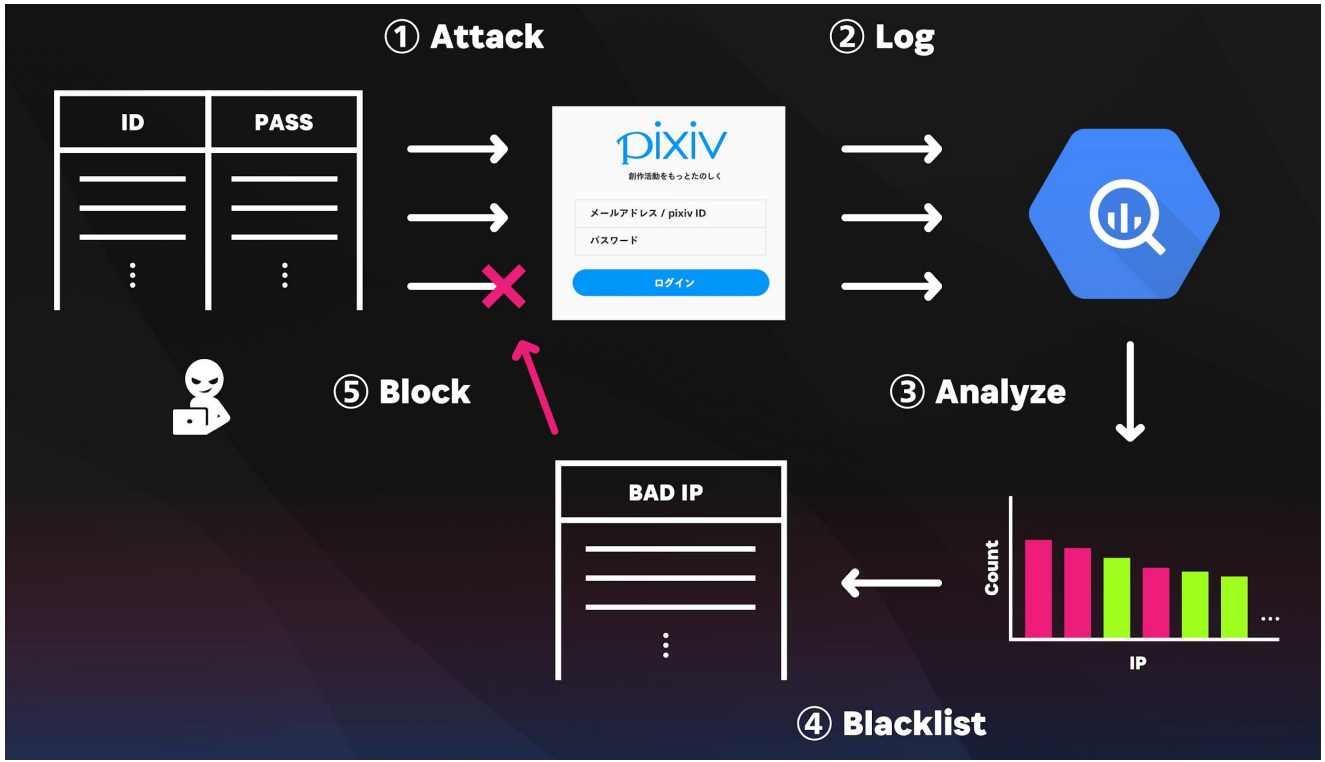
- Password Checkup = メールアドレス & パスワードハッシュを送ると、漏洩済みかどうかを返すreCAPTCHA EnterpriseのAPI
- ChromeのPassword Checkupと同じDB

	HIBP	Password Checkup (beta)
マネージド	-	✔
入っている情報	パスワードハッシュ + 漏洩回数	メールアドレス & パスワードハッシュ
漏洩ID数	100億+	40億+

ログ分析による検知 & ブロック

- Low and slowな攻撃の検知には長期的なログ分析が必要
- 長期的なログからIPアドレスごとにログイン成功率、失敗率、ユニークID比率などの指標を計算し、攻撃IPを検知
- 検知したIPアドレスのブロッキングや侵入されたアカウントの復旧まで自動化

ログ分析による検知 & ブロック



Google Cloud

まとめ

まとめ

- pixivエコシステム全体で認証エンドポイントを1つに統一した
- ウェブに統一したことで、1つのソリューション = reCAPTCHA Enterpriseでエコシステム全体を保護することができるようになった
- Bot対策、漏洩パスワードDB、ログ分析を通じてアカウント乗っ取りの対策を実施している

Thank you