Engineer

ユーザー

システムの利用を許された人や、その人のために動くプロセス

どのようなものか

ユーザーとは、システムがそのために動作する人、あるいは何らかの主体です。通常の技術文書では、この語は三つの異なる役割を持ちます。ユーザーについての混乱の多くは、それらを一つにしてしまうことから生まれます。

一つ目は人です。製品を開き、何かを成し遂げようとする人を指します。デザイナー、サポート担当者、プロダクトマネージャーが通常意味するのはこれで、システム内で決まった形を持つわけではありません。二つ目はアカウントです。再び同じ相手だと分かるよう、システムが保存する記録で、通常はログイン名、内部識別子、権限の集合、有効や停止中といった状態を持ちます。アプリケーションのコードでは、主にこちらを意味します。三つ目はOSのユーザーです。Unix系システムでは、ユーザー名と数値のユーザーIDを持つ、ユーザーデータベースの項目です。実行中のプロセスは、カーネルが権限検査に使うユーザーIDの資格情報を持ちます。

この三つが一対一に対応することは、あまりありません。一人が多くのサービスにアカウントを持てます。NISTのデジタルアイデンティティーの指針も、一人が複数のデジタルアイデンティティーを持ち、それぞれの一意性は自身のサービス内だけで成り立ち得ると明記しています。一つのアカウントを複数人で共有することもありますが、ほぼ常に誤った選択です。また、人が直接対応しないユーザーも数多くあります。Webサーバー、データベース、バックアップジョブ、デプロイスクリプトは、それぞれ専用のOSユーザーとして動き、他システムのアカウントを持つこともよくあります。そのため、NISTの定義は「個人、または個人のために動作するシステムのプロセス」となっています。

Unixホストでは、名前と番号の違いを簡単に確かめられます。

```
$ id ana
```

```
uid=1001(ana) gid=1001(ana) groups=1001(ana)
```

カーネルが扱うのは番号です。POSIXは、ユーザーごとに、ユーザー名、数値のユーザーID、初期グループID、初期作業ディレクトリー、最初に実行するプログラムを保存するユーザーデータベースを定義しています。ファイルの所有者も番号で保存し、人に表示するときだけ名前を調べます。プロセスは複数のユーザーIDを持ちます。実ユーザーIDは誰が開始したかを、実効ユーザーIDはその時点で誰の権限を使っているかを示します。

アプリケーションのアカウントも、通常は同じ区別をします。あるシステムから別のシステムへユーザーを作成・設定するためのSCIM標準は、人が見てログインに使う `userName` を必須としています。これはサービス内で一意で、大文字と小文字を区別せずに比較します。それとは別に、サービスが割り当て、変わらず、決して再割り当てしない `id` があります。 `active` フラグは、停止したアカウントと利用可能なアカウントを区別します。

概念を判断に生かす

「ユーザーとは？」を実際の判断に生かしましょう。その概念を、開発または購入するシステムに結び付けて考えるお手伝いをします。 ノートパソコン、プリンター、ログイン、メールの問題を、利用者が気後れしない平易な説明で、速やかに解決します。

サービスを見る お問い合わせ →

用語の背後にある前提を検証する

解説とリンク先の実績を参考に、プロジェクトについての質問を整理してください。ツールを選ぶ前に、前提を一緒に検討できます。 技術サポート部門を設立 — 10,000 ゼロから設立したサポート部門が対応した顧客数

技術サポート部門を設立 お問い合わせ →

なぜ重要なのか

アクセスの可否は、どれもユーザーについての判断です。誰がユーザーなのか曖昧なら、判断も曖昧になります。「この人はこの請求書を見てよいか」という問いは、コードでは「このアカウントは、この文脈で、この記録を対象とする権限を持つか」になります。その読み替えの各段階で、意図した人物と実際のアカウントがずれる可能性があります。

人とアカウントの境目は、責任を追えるかどうかの境目でもあります。ログが記録するのはアカウントです。各アカウントがちょうど一人に属していれば、ログの一行から誰が何をしたか分かります。共有アカウントでは、どの秘密情報を使ったかしか分からず、誰が入力したかは分かりません。一人のアクセスを終わらせるにも、全員分を変える必要があります。

OSユーザーは、最小権限のために長く使われてきた手段です。専用の非特権ユーザーで動くサービスは、そのユーザーの権限で制限されます。制限は、ファイルの所有関係だけで決まるわけではありません。共有の書き込み可能な資源を変更し、ネットワークリクエストを送り、利用可能な認証情報を使うことは、なお可能です。サービスごとにユーザーを分けると、侵害時の被害を減らせますが、完全な隔離にはなりません。同じサービスをスーパーユーザーで動かすと、マシン全体を危険にさらし得ます。プログラムごとに専用ユーザーを与えるのは小さな設定変更ですが、問題が起きたときに使える権限を狭めます。

最後に、人とアカウントでは寿命が異なります。人は名前、メールアドレス、勤務先を変え、アカウントは停止、統合、削除されます。メールアドレスのように変わる属性をアカウントの識別子として扱うと、いつか一人の履歴を別の人に結び付けます。

実際の活用例

海事プラットフォームでは、専門職が企業や教育機関などの組織を管理し、組織自体はログインを持ちません。リンク先のページは、人がアカウントであり、組織はその人が代理する対象だと明示しています。この仕事は、ユーザーが管理するどの組織としても動けるコンテキスト切り替えです。ブラウザーのローカルストレージに選択中の組織を保存するため、切り替えは即座に行えます。サーバー側のCookieにも同じ値を持たせ、サーバーで描画するページも同じ文脈を示します。しかし、そのどちらもアクセスの可否は決めません。サーバーはリクエストごとに認可を再確認するので、保存値を書き換えても、自分の画面の表示しか変えられません。

会社自身のホストでは、ほとんど権限を持たないOSユーザーがリリースを配備します。コンテナーの実行基盤を設けた際、デプロイと環境の準備を分離しました。rootが一度だけ配備先のパスを用意し、その後は非特権ユーザーが、一つの固定スクリプトを実行して再デプロイします。許可を限定したルールにより、そのコマンドだけを引数なしで実行できます。通常のリリースはイメージをビルドし、サービスを再起動します。そのためにrootのシェルを開く人はいません。

誰がユーザーかを把握すること自体も、報告書になります。読み取り専用のホスト報告ロール七つの一つは、稼働中のホストから、リポジトリ内のMarkdownへアクセス報告を出力します。アカウント、sudoの許可範囲、鍵のフィンガープリント、Gitフォージのユーザー、データベースのロールを並べます。七つの報告には、実行時に測った数字だけを載せるという共通ルールがあります。未確認の

箇所は、読者が信じそうなもっともらしい推測で埋めず、空欄にします。報告全体では、申告されていない待ち受けポートや、機能していないセキュリティー対策二つなど、実際の問題を見つけました。

問題が起きるところ

削除したユーザーが、別人として戻る。 アカウントを削除した後で識別子を再発行すると、新しい利用者は、古い値を参照するものを引き継ぎます。テーブルの行、一覧の項目、ディスク上のファイルなどです。Unixホストでは、削除したユーザーのファイルは数値の所有者を保ち、同じ番号で次に作ったユーザーが所有者になります。SCIMが `id` に求めるように、アカウントには再利用しない識別子を与え、削除前に、利用を終えるユーザーのデータをどう扱うか決めます。

メールアドレスをアカウントそのものとして使う。 自然なキーに見えても、本人がアドレスを変えたり、古いアドレスを使えなくなったり、雇用主が新しい社員へアドレスを渡したりすることがあります。すると、一人の履歴が別人に結び付いたり、一人が二つのアカウントを持つことになったりします。変わらない内部識別子をキーにし、アドレスは変更可能な属性として扱います。

全員が同じアカウントでログインする。 共有の管理者ログインは簡単に作れても、誰が操作したか監査できません。誰かが去ったとき、全員分の秘密情報を変えなければ、その人のアクセスは終わりません。ログに残るのも、人物ではなく役割です。一人に一つのアカウントを与え、共通の権限はグループ、ロール、許可範囲の狭いsudoルールで与えれば、ログも離脱時の扱いも実態を表します。

ブラウザーが、ユーザーに何を許すか決める。 ローカルストレージ、Cookie、フォームの隠しフィールドにあるロールは、クライアントからの申告であり、誰でも編集できます。サーバーがそれを信じるなら、書き換えが攻撃になります。クライアントは利便性のために文脈を覚えてよいですが、サーバーはリクエストごとに、自身で権限を検査しなければなりません。

簡単だからサービスをrootで動かす。 動作はしても、悪用可能な欠陥がそのサービスにあれば、ホスト全体を危険にさらし得ます。各サービスに専用の非特権ユーザーを与え、追加の権限は広く渡さず、指定した一つのコマンドに絞って与えます。

参考資料

- NIST CSRC用語集：user — NISTのセキュリティー文書で使う定義を、出典の文書とともに示しています。
- POSIX.1-2024 Base Definitions：Definitions — Unix系システムのユーザーデータベース、ユーザーID、ユーザー名の正式な意味です。
- RFC 7643：SCIM Core Schema — サービス間でアカウントを移すUser資源と、`userName`、`id`、`active`を定めています。
- NIST SP 800-63-4：Digital Identity Guidelines — 一人が複数のデジタルアイデンティティーを持つ仕組みと、申請者、加入者、申告者の役割を説明します。
- POSIX.1-2024：File Access Permissions — 所有者、グループ、その他のアクセス権の区分、代替のアクセス制御、適切な特権を扱い、所有関係だけではアクセスを限定できないことを示します。

用語集

実際の制約に合わせて選ぶ

機器やサービス、観測された症状、保持すべきデータをご説明ください。安全性を最も重視しながら、役に立つ診断の次の一手を定められます。

料金を見る お問い合わせ →

用語を実務に結び付ける

「ユーザーとは？」がお客様の組織にどう当てはまるかをご相談ください。現在のシステムの具体例が一つあれば、話を始められます。

サービスを見る

welcome@engineer.company +45 50 10 61 84 デンマーク、コペンハーゲン

このページを持ち歩く 連絡先カード

心を込めて丁寧に制作： D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

著作権 © 2025 – 現在 · Engineer ApS · すべての権利を留保します。

印刷元： https://engineer.company/ja/glossary/user/