

Protected Computing

Protected Computing は、データを処理する方法、タイミング、場所に変革をもたらし、データのプライバシーと安全性を技術的に保証します。

コンピューティングは、もはやパソコンや電話だけではなく、家や車の中、手首の上やクラウドでも行われています。ますます複雑になる環境の中で、ユーザーのプライバシーを保護しながら、パーソナライズされた便利なユーザー体験を実現することは、新たな技術的課題をもたらします。

そのため、個人データのプライバシー、安全性、セキュリティの確保を目的とした新しい技術ソリューションである Protected Computing を開発しました。

今日の Protected Computing :

- ✓ 会話のプライバシーを完全に守りながら、Android がテキスト内で次にくるフレーズを提案できるようにします。
- ✓ 画面を起動したままにするタイミングを Pixel が認識できるようにすると同時に、処理中の環境信号を継続的に削除します。
- ✓ 侵害されたパスワードを知らなくても Chrome が警告できるようにします。

Protected Computing の原則

最小化 されるデータ フットプリント

エッジ プロセッシングやエフェメリティなどのテクニックを使用して、個人を特定できるデータの量を全体的に縮小し、収集量を減らして削除量を増やしています。データが存在しなければ、ハッキングはできません。

匿名化 されるデータ

識別可能な信号のぼかしやランダム化、統計的ノイズの追加まで、さまざまな匿名化技術を使用してデータからユーザーの個人情報を取り除き、本人と関連付けられないようにします。

制限 されるデータへのアクセス

エンドツーエンドの暗号化や安全なエンクレープなどのテクノロジーを使用してアクセスを制限します。これは、Google の社員を含め、機密データにアクセスすることを技術的に不可能にするためです。

