「AXIES認証基盤部会・学認合同企画セッション」に頂いた質問と回答

講演名	質問	回答
東京大学における 認証基盤の取り組み	MFA疲れへの対策としてリスクベース認証・条件付きアクセス（怪しければMFAを強制）を使うのも一案だと思うのですが、こちらご検討などされていらっしゃるのでしょうか？	リスクベース認証などの新しい対策を期待してクラウドサービスを活用したIdP構成を採用しました。ライセンスの都合で現在はリスク評価に基づく動的な認証処理を実現できませんが、重要な課題として認識しています。
	当機構においても一部構成の違いはあるものの、同様の枠組みで認証基盤を構築しております。全学認証基盤を利用してくれるサービスについては一定レベルの対応が可能ですが、大学においては部局、研究室単位で運用されている（MFA対応が困難な）レガシーサーバ類も多いかと思います。これら独立サーバも含めた大学全体の認証セキュリティ強化の取り組みなどもしありましたらお聞かせ願えませんでしょうか。	Googleアカウントも提供しており、大学Googleアカウントでサインインしたユーザだけが閲覧できるウェブサイトやアプリを作成している事例があります。クラウドIdPの利点をうまく活用できているのではないかと考えています。
FIDO2対応Yubikeyが グローバルで選ばれる理由 とパスキーの展開	現在はスマホPush通知認証、TOTP認証が主流だと思います。パスキーの普及期はいつ頃到来すると予想されますか？（マルチデバイスとシングルデバイスで時期が異なるかな	FIDO2の実装も活発に行われつつありますが、日本で一般的（コモディティ化）となるにはまだ数年かかると思います。パスキーはFIDO2ベースなので、同じような流れです。ただ、コンシューマーの視点ではグローバル大手ITサービスベンダーがいち早く対応しているので、ユーザー側の理解が進めば、意外と早いかもしれません。