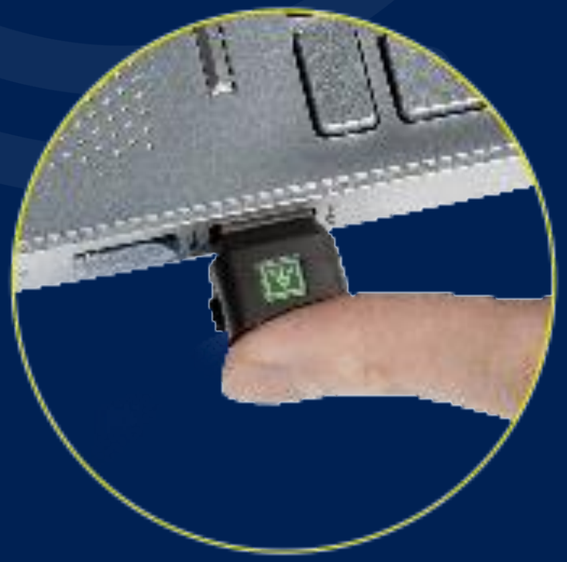
未来のカギ。ATKeyで始めるパスキーの世界
（認証器）

#FIDO　#パスキー　#生体認証 #フィッシング対策

オーセントレンドテクノロジー株式会社
塩川雄介



AUTHENTREND

被害は増加中

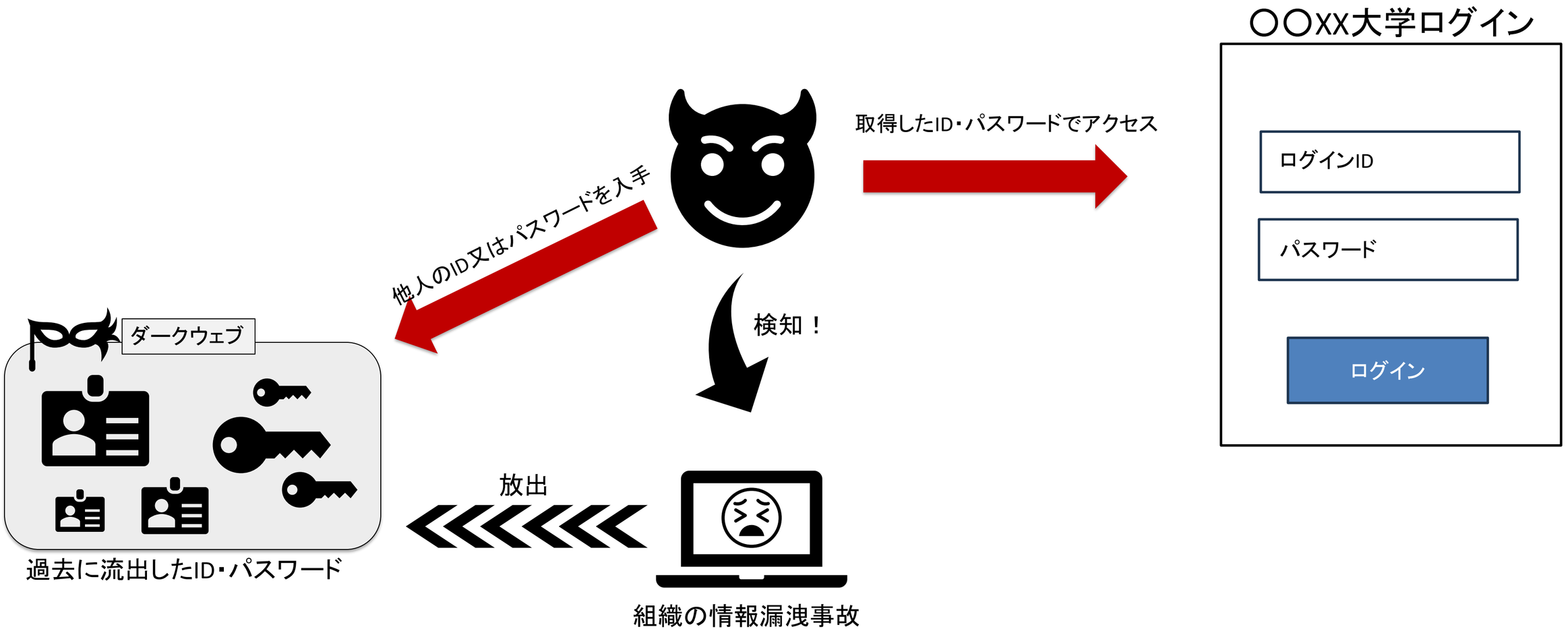
	2025年1月	2025年2月	2025年3月	2025年4月	2025年5月	合計
不正取引が発生した証券会社数	2	2	5	9	16	
不正アクセス件数	96	71	1420	5279	3556	10422
不正取引件数	39	33	687	2910	2289	5958
売却額	80,000,000円	100,000,000円	12,900,000,000円	154,000,000,000円	110,100,000,000円	277,200,000,000円
買付額	70,000,000円	60,000,000円	12,800,000,000円	134,600,000,000円	99,300,000,000円	246,800,000,000円

金融庁：インターネット取引サービスへの不正アクセス・不正取引による被害
https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

合計不正売買：約5,240億円！

従来の認証方式の問題点

パスワードの流出・不正利用



MFA技術の現在(比較)

認証方式	セキュリティ	利便性	導入・運用コスト
SMS/OTP	△	○	低～中
TOTPアプリ	○	△	中
FIDO2（セキュリティキー）	◎	◎	低
Passkey	◎	◎	低

パスワードの限界：漏洩・リスト攻撃など
FIDO2とPasskeyが今後の主流へ

各認証レベル

セキュリティレベル	弱い		まぁまぁ			まぁまぁ強い	強い	
認証方法	**電話**	**SMS**	**プッシュ通知**	**OTP** **(TOTP等)**	**OATH Token**	**Authenticator** **(MS、Google)**	**Windows Hello**	**FIDO2** **(デバイスバウンド)**
リスク	フィッシング リアルタイムフィッシング チャネルジャッキング 中間車攻撃	フィッシング リアルタイムフィッシング チャネルジャッキング 中間車攻撃	フィッシング リアルタイムフィッシング MFA疲労攻撃	フィッシング リアルタイムフィッシング	リアルタイムフィッシング	フィッシング リアルタイムフィッシング Push Bombing	**低**	**低**
依存	**パスワード** **通信・通信費**	**パスワード** **通信・通信費**	**パスワード、Wi-Fi** **OSメッセージ**	**パスワード**	**パスワード**	**Wi-Fi** **通信**	**TPM** **ローカルストレージ**	**外部認証器**
レガシーMFA						**MFA、パスワードレス**		

ATKey製品の概要と導入例

セキュアエレメント実装
耐タンパー設計
ロック・自壊

秘密鍵を格納
指紋情報を格納

指紋センサー
登録指紋 x 10

セキュアエレメント実装
耐タンパー設計
ロック・自壊

秘密鍵を格納
指紋情報を格納

指紋センサー
登録指紋 x 2

生体 or PIN + デバイスに保存された FIDO Credential = パスキー(デバイス固定パスキー)

ATKey製品の概要と導入例

製品：ATKey.CardNFC、ATKey.Pro

USBタイプ

カードタイプ

物理的なセキュリティキー：
遠隔攻撃やフィッシング等では突破できない。物理的な盗難があっても、指紋がなければ突破できない。

ローカル認証データの保護：
指紋情報はサーバーに保存されず、認証器の安全なセキュリティチップ内に保存されるので、大規模データ漏洩の影響を受けない。

1. **ローカル(ATKey内)で認証が完結**
   生体情報やパスワードをクラウドや外部には送らず、安全性が高い。

パスワードの概念

合い言葉

扉を守っている人
↓ 合い言葉の一致でドアを開ける番人

扉を開けてほしい人
↓

知ってる合い言葉：イロハニホヘト

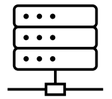
知ってる合い言葉：イロハニホヘト

=

パスワード

パスワード：イロハニホヘト

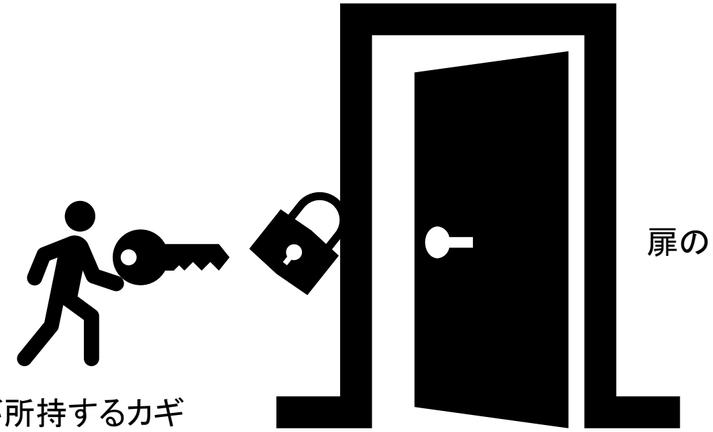
認証サーバー



パスワード：「イロハニホヘト」を暗号化

パスワードの一致でログインする

セキュリティキーのFIDO認証は？(技術的視点ではなく、利用者的視点で)

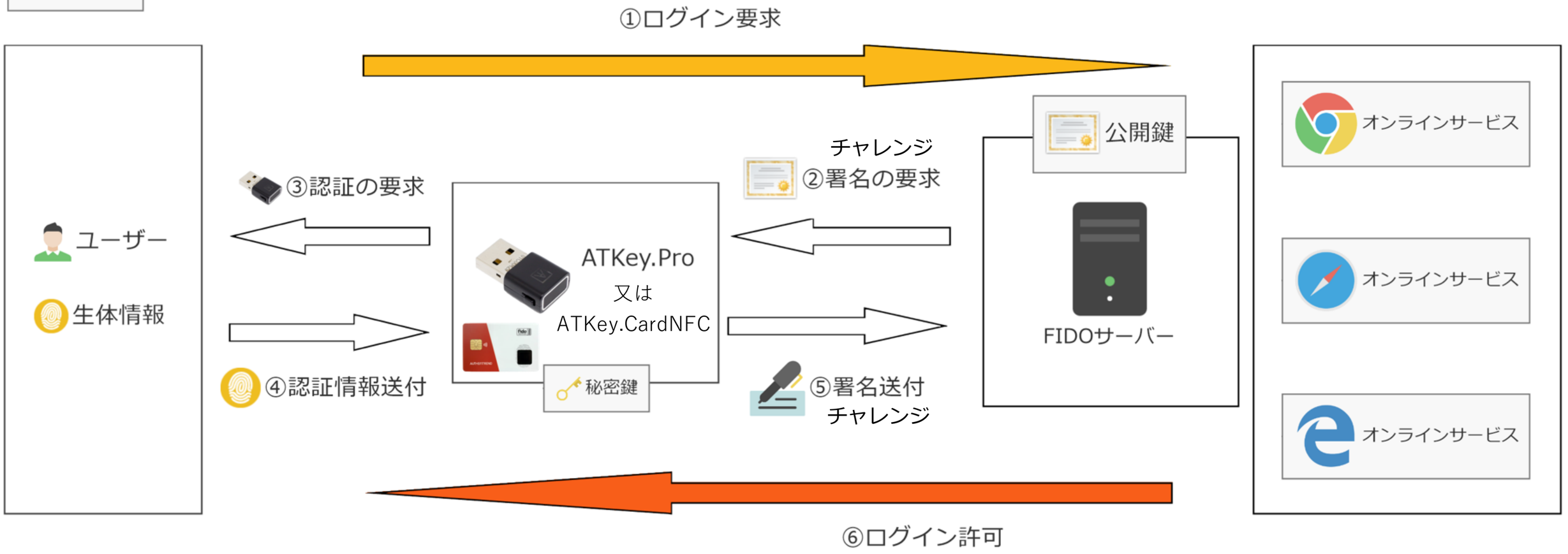


扉の向こうには誰もいない

ユーザーが所持するカギ
(スマホとかATKeyとか)

カギのシリンダーとカギが一致でドアが開く

FIDOの仕組み



FIDO認証は公開暗号方式
秘密鍵の役割：署名を行う
公開鍵の役割：秘密鍵の署名検証を行う

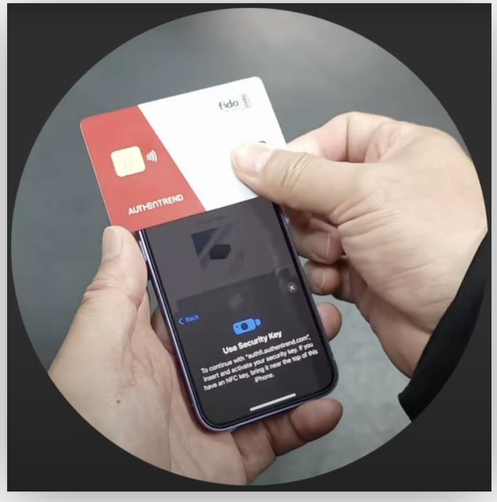
認証に必要なFIDO2セキュリティキー

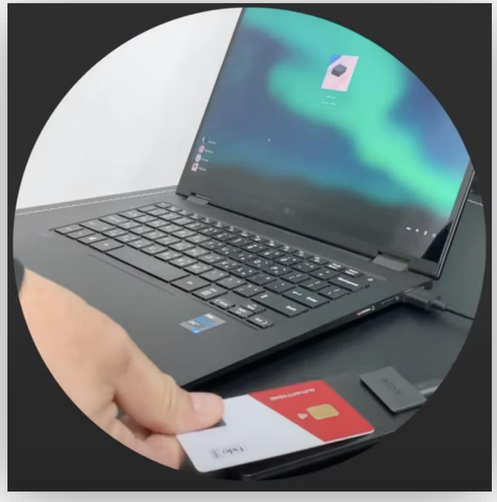
実際のログイン利用例

東京大学様　UTAS、UTOLへのログイン

USBタイプ

カードタイプ





スマホのパスキーと何が違う？！

	デバイス固定パスキー	同期パスキー
保存先	特定デバイス内の安全な領域 （例：TPM、セキュアエレメント付きセキュリティキー）	ベンダー提供のクラウド同期ストレージ （例：iCloud Keychain、Google Password Manager）
利用可能デバイス	登録された1台のデバイスのみ	同じアカウントで同期された複数のデバイス
例	ATKey、Windows Hello（TPM利用）	iPhone＋iCloud、Android＋Googleアカウント
鍵の抽出	不可能（セキュリティ的に鍵は外部に出ない）	同様に不可能（OSが鍵を抽出させない設計）

個人的には・・・

「鍵の抽出」はどちらも**論理的に不可能**に設計されていますが、**物理的に「取り出し困難」なのはデバイス固定パスキーの方が上かも。**
同期パスキーは**利便性重視（UX）コンシューマー向け**、デバイス固定パスキーはセキュリティ・制御重視（特にエンタープライズ向け）。

セキュリティキー(認証器)を使うメリット【FIDO2/パスキー】

1. 🔒 フィッシング耐性が非常に高い
- 鍵の情報は物理キーから外に出ないため、**中間者攻撃や偽ログインページに騙されるリスクがゼロ。**

2. 🔐 秘密鍵が端末から漏れない（秘密鍵非移動性）
- セキュリティキーは**秘密鍵をローカルで保持し、外に出さない**仕組み。

3. 🧠 パスワード不要＝パスワードレス
- パスワードの作成・記憶・定期変更が不要。
- パスワード流出や辞書攻撃の心配がない。

4. ⚙️ 導入メリット
- Microsoft Entra ID や Google Workspaceなどと統合可能。
- **社内のSSOやゼロトラスト運用にも適応。**
- IT部門によるアカウントリセットやパスワード管理負荷が大幅に減少。
- BYOD不要。(支給されていないスマホなど)
- 低コスト

AUTHENTREND

一緒に組織の認証やウェブサービスに
パスワードレスの導入を始めましょう

www.AuthenTrend.com

ahxiong@authentrend.com

AuthenTrend

AuthenTrend technology inc.