fakePointer: 覗き見攻撃に対しても安全な認証手法

産業技術総合研究所 情報技術研究部門 高田哲司

覗き見攻撃の脅威は今も健在


ATM の盗撮事件

Mobile/Ubiquitous 環境 -> 状況は悪化 (?)

既存の対策手法

覗き見攻撃は主体が人間から
カメラ撮影へ

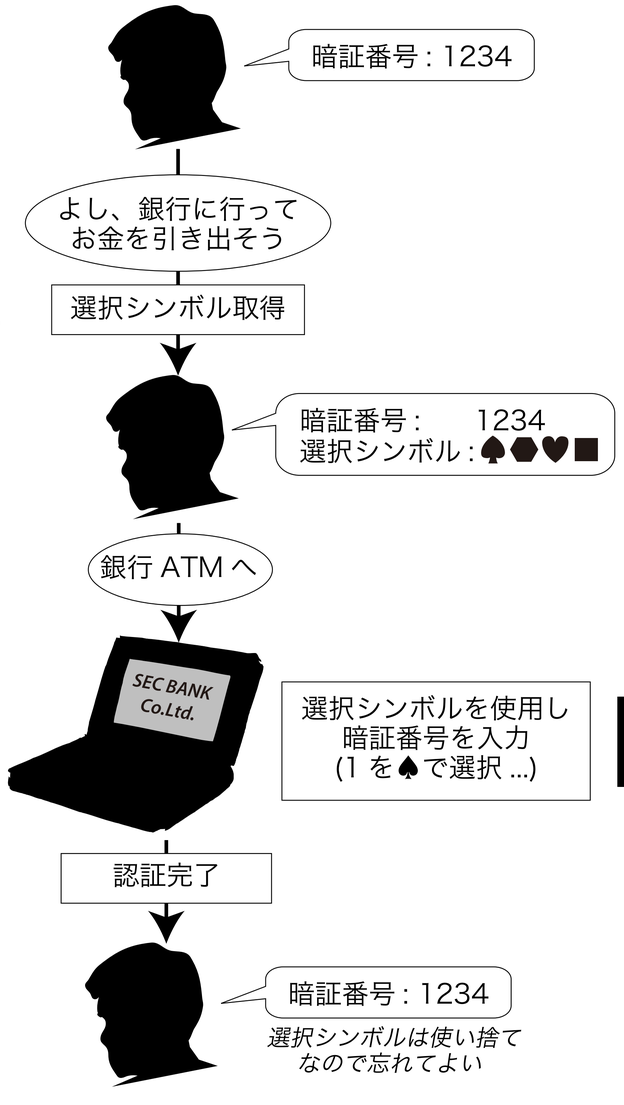
既存の対策手法が無意味に！

fakePointer の特徴

1. ランダムに発行される情報を利用して秘密情報を入力

2. 入力値が特定不能な秘密入力用ユーザインタフェース

✓ **ビデオ撮影されたとしても、ある条件が成立しない限り秘密情報の特定は困難**



利点 :

簡単操作

(画面に集中できる．携帯電話でも可)

記憶負担の増加は必要最小限

(認証時のみ選択シンボルを記憶)

認証画面