Seeds

情報工学・
人間科学系

稲葉 宏幸 教授
URL http://www.sec.is.kit.ac.jp/

お問合せ先
corc@kit.ac.jp
産学公連携推進センター

■キーワード

情報セキュリティ　個人認証　パスワード　覗き見対策

パスワードに代わる認証方式
覗き見に耐性をもつ個人認証方式

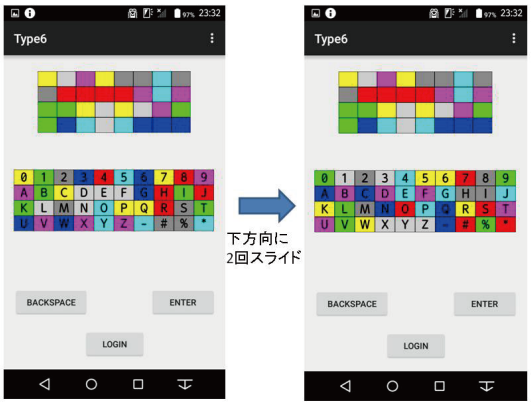
■研究の概要

スマホのロック解除や、SNS、ショッピング、オンラインバンキングなどの様々なWebサービス、あるいは銀行ATMまで、あらゆる情報システムで個人認証が必要不可欠です。個人認証は、貴重な財産やデータを保護するための重要な砦ですが、実際には簡便なパスワード(PIN)による認証方式が主流です。研究室では、覗き見や盗聴があったとしても他人がなりすますことができない個人認証方式の研究・開発を行っています。

■研究・技術のプロセス／研究事例

・背景パターンスライド認証方式

この方式は、パスワード文字の並びの背景に、色やパターンからなる背景パターンが表示されており、あらかじめ決められたルールに従って背景パターンをスライドし、パスワード文字に合わせることでパスワードの入力を行います。背景パターンは全体的にスライドするので、覗き見があったとしても、どの文字に合わせたのかは判断できません。研究室で開発した方式は、背景パターンをパスワード文字に合わせるときに、合わせる色やパターンが文字ごとにランダムに変更されるように工夫をすることで安全性の向上をはかっています。

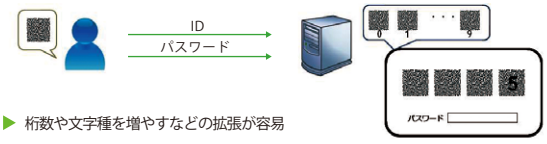


背景パターンスライド認証方式

・VSSS(Visual Secret Sharing Scheme)を用いたワンタイムパスワード方式

VSSSとは、視覚復号型秘密分散法と呼ばれる暗号技術で、一般的な暗号と異なり人間の視覚により復号を行うことができます。この認証方式では、認証画面に表示される一見ランダムなパターン上に、ユーザーが所持する透明シート上に印刷されているパターンをかざすと、視覚的な効果により文字等が浮かび上がりますので、その文字をワンタイムパスワードとして入力します。画面に表示されるランダムパターンからだけでは理論的にパスワード文字を読み取ることはできません。通常の方式では、ワンタイムパスワードを表示する小型デバイスが必要になりますが、この方式では透明シートを所持するだけでよいという特徴があるため、イベント会場への来場者や観光客などに、認証が必要なサービスを安価に提供するといった応用も考えられます。

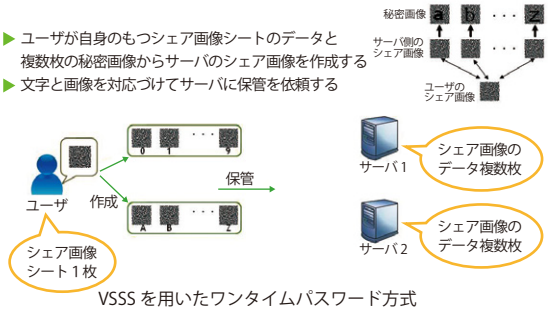
▶ 例）4 桁の数字の場合（PIN 認証）
1. ユーザ ID をサーバに送信する
2. サーバがシェア画像をランダムに表示する
3. ユーザは表示されたシェア画像に所持しているシェア画像シートを重ねていく
4. 復号された画像から文字を読み取り、パスワードとして入力する



▶ 桁数や文字種を増やすなどの拡張が容易

VSSS を用いたワンタイムパスワード認証の流れ

▶ ユーザが自身のもつシェア画像シートのデータと複数枚の秘密画像からサーバのシェア画像を作成する
▶ 文字と画像を対応づけてサーバに保管を依頼する



VSSS を用いたワンタイムパスワード方式

■セールスポイント

スマートフォンやタブレットPCの普及によって、いつでもどこでも色々なサービスを利用できるようになっていますが、駅やカフェなど公共の場でパスワード入力をする機会も多くなっています。本技術を使えば、そういった場合でも安心して認証することができます。