# ColorPassword: テンキーの背景に色を用いたパスワード覗き見防止システムの提案と試作

原田 真彰† 渡邊 恵太†

本論文では，公共の場などでの個人認証における脅威である覗き見攻撃に対して，安全性を高めることを目的とした認証方法 ColorPassword を提案する．ColorPassword は，数字と色の種類の組み合わせを任意に考え，その羅列をパスワードとして認証するシステムであり，従来のインタフェースや記憶負担量を踏襲している．ユーザは従来のデバイスと同様に入力を行うが，数字と色の入力箇所が重なっていることにより他者はユーザが数字と色どちらを目的に入力したのかを判別することが出来ない．本論文では ColorPassword の提案と実装について紹介し，その利用について議論する．

# ColorPassword: Shoulder Surfing Resistant Authentication System in Personal Identifier by Using Color and Number Password

MASAAKI HARADA† KEITA WATANABE†

***Abstract:*** In this paper, we proposed resistant authentication system “ColorPassword” against shoulder surfing attack in public place. A shoulder surfing attack is some threat for cell phone users in modern society. Our scheme ColorPassword is authentication system that use password we thought a combination of number and color, and follows former interface and user’s memory load. Therefore it enables users to input password like a former device. On the other hand, observers are not able to identify whether operator uses number or color for inputting password because our ten key uses color to background of ten key buttons. In this paper, we introduce system of ColorPassword and discuss about use of it.

## 1. はじめに

スマートフォンなどの普及により，現在我々の生活の多くの場面でタッチパネル式端末を操作，使用するという機会がある．その中で，スマートフォンのロック画面解除などを含めるタッチパネルを用いての個人認証の行為において，他者にその認証行為を見られてしまうことにより暗証番号やパスワードが知られてしまうという問題（これを覗き見攻撃と呼ぶ）がある．また，この覗き見攻撃は人間の視覚情報だけではなくカメラ録画を使用したものも存在し，カメラ録画による覗き見攻撃は人間の視覚情報のみの攻撃に比べ，複数回ユーザの認証行為を確認できる，認証行為をデータ化することにより確実に暗証番号やパスワードの解析を行うことが出来るなど，正確な認証情報の取得を行うことができると考えられる．

そこで，本研究ではタッチパネル式端末などにおける個人認証において他者による覗き見攻撃やカメラ録画による覗き見攻撃を受けたとしても，その暗証番号やパスワードの特定，解析を困難にするシステム ColorPassword を提案する．

† 明治大学総合数理学部先端メディアサイエンス学科
Department of Frontier Media Science, Faculty of Interdisciplinary Mathematic Science at Meiji University

## 2. ColorPassword

ColorPassword は，図 1 に示すように数字列のボタン背景に色を導入したインタフェースによって，色をキーにしているのか，数字をキーにしているのか，第三者からの特定を困難にし，パスワード入力の様子を覗き見られてもパスワードの流出を防止する．

具体的には，たとえばパスワードを「赤・2・青 3」というように，数字と色の組み合わせたパスワードを設定する．これを図 1 の入力画面を例に考えると，数字だけみれば 1・2・4・3 と入力しているように見える．つまり背景が赤なのは 1 で，青は 4 だからである．また，色を基準に見てみると，「赤・黄・青・緑」と入力しているように見える．これにより，第三者は入力者がそのキーを数字として入力したのか，色として入力したのかが判別が困難になる．

### 2.1 インタフェースの仕組み

インタフェースは iPhone や Android などのロック解除操作のインタフェース画面を踏襲し，数字列の並び順は等しい．また，それぞれのテンキーには 10 種類の色（赤色，黄色，緑色，青色，茶色，白色，橙色，桃色，紫色，水色）がボタンの背景色として振り分けられており，画面のタップを行う度にそれぞれのボタンに対する色がランダムに変わるようになっている．数字列の並び順はタップを行っても変化しない．なおシステムは Processing により実装され

ている．

### 2.2 認証方法

ユーザは 0~9 の数字 10 通りとテンキーに振り分けられている色（赤色，黄色，緑色，青色，茶色，白色，橙色，桃色，紫色，水色）10 通りの計 20 通りから重複を許した 4 つの順列をパスワードとして設定する．(一例として，赤色・2・白色・4 など)このとき，パスワードの組み合わせ方として 4 つすべて数字または色，3 つ数字かつ 1 つ色または 3 つ色かつ 1 つ数字，2 つ数字かつ 2 つ色となるパターンが存在し，考えられるパスワード総数は 20 の 4 乗すなわち，160,000 通りである．次に，図 1 に対してユーザは自らが設定したパスワードの順番の通りに条件となるボタン入力を行い，入力値とユーザの設定したパスワードの値が順番通りに一致した場合，認証成功となる．

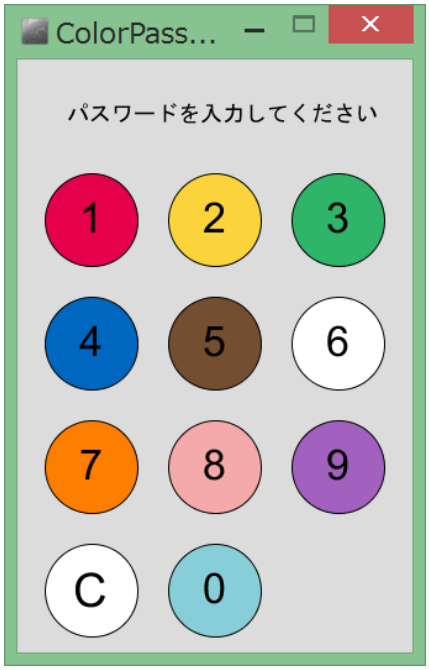


図 1　ColorPassword の認証インタフェース画面

### 2.3 利用とその考察

ColorPassword は従来の個人認証におけるインタフェースを踏襲しながらも，覗き見攻撃に対し暗証番号の特定を困難なものにすることを可能にした．提案手法の入力動作は数字と色どちらの目的でユーザはボタンを入力したのかという可能性 2 通りを計 4 回繰り返すため 16 通りの暗証番号の組み合わせが考えられる．そのため，他者は視覚情報で提案手法の入力動作により認証情報の取得，暗証番号の特定を行うことは困難であると考える．また，カメラ録画による覗き見攻撃も同様にして，数回程度の入力動作に対しては認証情報の取得，暗証番号の特定を行うことを困難なものにすると考える．

## 3. 議論

関連研究として，**CCC**：振動機能を応用した携帯端末での個人認証における覗き見攻撃対策手法の提案[1]や CursorCamouflage [2]があるが，CCC では認証時間の長さなどから，CursorCamouflag ではタッチパネル式端末への応用が困難なことなどから実用性には課題が残ると考えられる．ColorPassword は従来のインタフェースを踏襲している点は学習コストが低く，直感的に認証を行うことが出来る．

さらに，スマートフォンをはじめ，銀行 ATM などのタッチパネル式のパスワード入力インタフェースとしても置き換え可能なため，導入コストも低い．

一方で ColorPassword は色と数字という二次元の暗証番号となるため，覚えなければならない組み合わせが煩雑になる．ユーザの記憶負担については今後の課題となる．

したがって，色以外のアプローチも今後検討していく．たとえば，色の代わりに形やイラスト，記号など利用することでも同じ効果が期待できる．しかも，色の場合は色盲者など色が判別できない，あるいは困難なユーザにとっては利用できないが，たとえば fakePointer[3]のように形やイラストなどの組み合わせであれば，よりユニバーサルに利用できると考えられる．ただし，数字のテンキーに加えて背景にイラストや他の記号が提示されると，見た目上の煩雑性が増す可能性もあり，利用負荷が高まる可能性も懸念される．これらは今後，どのようなデザインがユーザにとって記憶負荷や入力負荷低いのか，検討してきたいと考えている．

## 4. おわりに

本研究では個人認証における覗き見攻撃に対し，暗証番号やパスワードの特定，解析を困難なものにするということを目指し，数字と色という二次元的なパスワードを考えることにより他者に数字と色のどちらの目的でボタン入力したのか分からせないようにするシステム ColorPassword を提案，実装した．今後は提案したパスワードの考え方自体の記憶負担や色に置き換わる要素を検討し，それに伴うユーザの認証行為の変化について考えていきたい．

## 参考文献

1) 石塚 正也，高田 哲司 CCC : 振動機能を応用した携帯端末での個人認証における覗き見攻撃対策手法の提案，インタラクション 2014 論文集，pp.501-503 (2014).
2) Keita Watanabe, Fumito Higuchi, Masahiko Inami, Takeo Igarashi CursorCamouflage: Multiple Dummy Cursors as A Defense against Shoulder Surfing, The 5th SIGGRAPH Conference and Exhibition on Computer Graphics and Interactive Techniques in Asia (Siggraph Asia 2012), Emerging Technologies, Nov. 28 - Dec. 1.
3) 高田，哲司: fakePointer:映像記録による覗き見攻撃にも安全な認証手法，情報処理学会論文誌 Vol.49, No.9, pp3051-3061,(2008).