# ユーザの入力方法に基づくパスワードの脆弱性評価に関する研究
# Password Vulnerability Assessment Based on Input Methods of Users

土屋 璃和登・ネットワーク分科会・中央大学大学院

***Abstract***: In the list of 10 Major Threats to Information Security 2022 [Personal], the threat of unauthorized login to Internet services has been on the increase in recent years, and is ranked 10th in the list. In addition to the use of passwords leaked from other services, there is another method of unauthorized login, which is to guess the passwords that the victims are likely to use by analogy. Therefore, it is desirable to set passwords that are difficult for others to guess. However, the data of the most frequently leaked passwords show that 8 out of the top 10 passwords are easy-to-type passwords. Therefore, in this paper, we define the concept of distance on the keyboard and evaluate the vulnerability of passwords using this concept

## 1:研究概要

近年の情報化社会では多くの情報がインターネットサービス上に登録されており，これらはIDとパスワードによって認証と保護が行われている．そのため強固なパスワードを設定することが求められる．しかしパスワードの強度評価についてパスワードの強度メーターには明確な基準が定まっていないことがわかっている[1]．そこで流出したパスワードからユーザの入力方法に距離の概念を考慮したパスワードの脆弱性評価を行った．

## 2:手法

キーボードの配置を図1のように定める．これをもとにネットワークグラフとして有向グラフGを作成する．エッジとしては隣接するキーをもち，エッジの属性としては，ベクトル$v$と重み$w$を持つとする．$v$と$w$を以下のように計算する．

ベクトルについて

ベクトルは任意のノード$i$から，自身に向けてのエッジのベクトルを0とし，それ以外のエッジについて以下のように定める．なお隣接するキーの中心までの角度を$\theta$とし，水平右方向を0°とする．

$$v=\begin{cases}1\ (\text{if } 0^\circ\le\theta\le 22.5^\circ \text{ or } 337.5^\circ\le\theta<360^\circ)\\ 2\ (\text{if } 22.5^\circ<\theta<67.5^\circ)\\ 3\ (\text{if } 67.5^\circ\le\theta\le 112.5^\circ)\\ 4\ (\text{if } 112.5^\circ<\theta<157.5^\circ)\\ 5\ (\text{if } 157.5^\circ\le\theta\le 202.5^\circ)\\ 6\ (\text{if } 202.5^\circ<\theta<247.5^\circ)\\ 7\ (\text{if } 247.5^\circ\le\theta\le 292.5^\circ)\\ 8\ (\text{if } 292.5^\circ<\theta<337.5^\circ)\end{cases}$$

重みについて

前述したベクトルの値によって定める．

$$w=\begin{cases}0\ (\text{if } v=0)\\ 1\ (\text{if } v=1 \text{ or } v=5)\\ 2\ (\text{if } v=3 \text{ or } v=7)\\ 3\ (\text{if } v=2 \text{ or } v=4 \text{ or } v=6 \text{ or } v=8)\end{cases}$$

図1:キーボード配置

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 0 | - | ^ | ¥ |
| q | w | e | r | t | y | u | i | o | p | @ | [ | |
| a | s | d | f | g | h | j | k | l | ; | : | ] | |
| z | x | c | v | b | n | m | , | . | / | ¥ | | |

**提案手法1:離れた入力のスコアを定数とするスコア計算**

離れたキーのスコア$s$を定数$k$とする．

ステップ (I) $V_0:=0$，スコア計算を行うパスワード$p$の文字数を$m$として$i$番目の文字を$c_i$で表す．
$i\in[1,m)$において以下の手順を行う．

ステップ (II) 有向グラフ$G$が$e_{c_{i-1}c_i}$を含むとき，$e_{c_{i-1}c_i}$の持つベクトルを$V_i$とする．
有向グラフ$G$が$e_{c_{i-1}c_i}$を含まないとき，$V_i=-1$とする．

ステップ (III) 以下の式 (4.1) を用いて，$s_i$を求める．

$$s_i=\begin{cases}k & \text{if } V_i=-1\\ 0 & \text{else if } V_{i-1}=V_i \text{ or } V_i=0\\ 1 & \text{else if } V_i=1,5\\ 2 & \text{else if } V_i=3,7\\ 3 & \text{else if } V_i=2,4,6,8\end{cases}\tag{4.1}$$

ステップ (IV) 以下の式 (4.2) より，スコア$S$を求める

$$S=\sum_{m-1}^{i=1}s_i\tag{4.2}$$

**提案手法2:離れた入力までのパスを求め計算するスコア計算**

離れたキーがあった場合，有向グラフGにおいてそのキーまでの最短路をエッジのWを用いて計算し，この経路をpathとしてスコア計算を行う．

ステップ (I) $V_0:=0$，スコア計算する$path$の長さの上限を$k$とする．スコア計算を行うパスワード$p$の文字数を$m$として$i$番目の文字を$c_i$で表す．
$i\in[1,m)$において以下の手順を行う．

ステップ (II) 有向グラフ$G$がエッジ$e_{c_{i-1}c_i}$を含むとき，$e_{c_{i-1}c_i}$の持つベクトルを$V_i$として式 (4.1) を用いて，$s_i$を求める．
有向グラフ$G$がエッジ$e_{c_{i-1}c_i}$を含まないとき，$G$上で$c_{i-1}$から$c_i$までの$W$における最短路$path$を求め，III を行う．

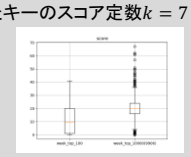
ステップ (III) $path$の長さを$l$として以下のように場合分けを行い計算する．
$l>k$のとき，$s_i=3k-2$とする．
$l\le k$のとき，$path$の$j$番目の文字を$pc_j$で表し，，$j\in[1,l)$において$e_{pc_{j-1}pc_j}$の持つベクトルを$V_j$として式 (4.3) を用いてスコア$s_i$を求める．
なお，式 (4.3) における$s_j$については式 (4.1) を用いて計算を行う．

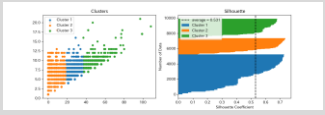
$$s_i=\sum_{j=1}^{i-1}s_j\tag{4.3}$$

ステップ (IV) 式 (4.2) を用いて，スコア$S$を求める

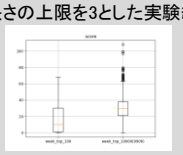
## 3:実験と結果

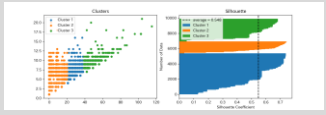
提案手法1
離れたキーのスコア定数$k=7$





提案手法2
pathの長さの上限を3とした実験結果





## 3:まとめ

提案手法1, 提案手法2ともに流出件数の多いものほど中央値が上昇することから脆弱性の高いパスワードほど本手法が効果的であることがわかる．またK-means法の長さとスコアの関係から，スコアのほうで分類が行われておりこちらからも手法が有効であることがわかる．一方でシルエット係数の数値はあまり高くないことから他にも指標が必要なことがわかる．

## 関連研究

[1]菅井琢, 金岡晃ほか. 実利用されているパスワード強度メーターの分析と検証. 研究報告マルチメディア通信と分散処理 (DPS), Vol. 2016, No. 16, pp. 1–6, 2016.