注 1：在来手法の弱点

文字パスワード･暗証番号･単純画像パスワード･パターン記憶法

- **簡単に覚えられるものは、第3者による収集･推測を防げず他人排除力に欠ける**
- **他人を排除できるものは覚えられず或いは混乱しやすく、本人も排除してしまう**
- **導入コストは低いが、質問対応･再発行コストが大きい**

リマインダー･Q&A 方式

- **質問中に答えが隠されており、反復試行には脆弱**

生体照合･バイオメトリックス（顔貌･手紋･指紋･虹彩紋･網膜紋･声紋･署名･静脈紋･骨紋･脳波形、etc）

- **原理的に本人拒否を伴うため単独では「本人を排除することなく他人のみを有効に排除する」ことが不可能**
- **本人排除を避けるための救済策を組み込むと、他人排除力は救済策を上回ることはない**
- **物理的･映像音声的･電気的に複製可能と知られた時点で他人排除力が崩壊する**
- **複製対策は際限なきイタチゴッコの泥沼化の可能性**
- **物理的計測結果を意思確認を伴うべき認証結果と同一視する無理に伴うプライバシー問題･人格尊厳毀損問題あり。（個々人の忌避感情の否定はできない。）**
- **導入コストが高い。**

所事物照合(IC カード/タグ/鍵/トークン,etc)

- **盗用に対して無力**
- **「紛失･置き忘れvs付けっ放し」のジレンマから逃れられない」**
- **導入コストが高い。**

異種複合･マルチモーダル手法（上記技術相互の組合せ）

長所の組合せとの誤解が蔓延しているが、実際には短所の組合せに帰着し、最低レベルの技術が全体のレベルを決定する。導入コストも運用コストも高い。

注 2　ニーモニックガードと在来技術の比較

A　高い数学的強度を実現できるか

在来型パスワード方式	X～△	＊1
生体照合･所持物照合	X～△　或いは評価不能	＊2、＊3
ニーモニックガード	○	＊4

B　いつでも、どこでも、パニック状態でも、ユーザにストレスを掛けず、人格の尊厳を損なわずに、本人を排除せずに他人のみを有効に排除できるか？

在来型パスワード方式	X	＊5
生体照合･所持物照合	X	＊6
ニーモニックガード	○	＊7

C　コスト（導入費用＋運用費用）は妥当か

在来型パスワード方式	△	＊8
生体照合･所持物照合	X	＊9
ニーモニックガード	○	＊10

＊1：　一般には覚えやすさ優先や混乱回避から本人固有の客観的事実を材料にするので△であるが、厳格管理の旗の下でランダム･英数字大文字小文字特殊記号混じり･6 桁以上の強制を受けると表面上は服従しつつもメモに記して端末機の周辺に（同僚･上司･部下がやっているように）秘匿するのでXとなる

＊2：　一般の実運用では本人拒否対策の救済策としてパスワードを OR 型選択式で併用するので数学的強度がパスワードの強度を上回ることはない。従って自動的にX～○となる。本人拒否対策の救済策を併用しない単独使用では、メーカー毎に算定

基準の異なる本人拒否率と他人受容率のトレードオフ関係の中で数学的強度が確定できない。つまり、評価不能である。

＊3：盗用・付けっ放しの場合の強度はゼロ。「付けっ放しvs紛失・置き忘れ」ジレンマの数学的評価は不可能。

＊4：8x8＝64 個の写真の中に秘匿された昔の愛着ある写真 10 枚を探すだけで認証を完了できるケースであれば、パニック状態でも、老若を問わず、誰でも実行でき且つまぐれ当たり確率は
10/64x9/63x8/62x7/61x6/60x5/59x4/58x3/57x2/56x1/55 = 1/(1.99463E+22) として確定する

＊5：他人排除力のあるパスワードを複数組も使いこなせる人は極めて稀である。

＊6：注意深い善意の同僚に恵まれた事務所内など特定の環境の下でしか成立しない。

＊7：全ての要件を満たす。

＊8：導入コストは極めて低いが問い合わせ・再発行など運用コストは高い。

＊9：大きなハードウェア購入コストが掛かる上に、維持コストも無視できない。

＊10：問い合わせ・再発行の運用コストが押さえられる為に、無償で導入できる文字パスワードよりもトータルコストは小さい。