各種評価軸によるニーモニックガード（クリプトニーモ）の検討

1　セキュリティ強度

A. 最初のポイントは、思い出せるものと思い出せないものを比較しても全く無意味、ということ。比較は間違いなく思い出せるもの同士の間で行われるべきものです。

B. 一般に使われているパスワード、特に、使わないかもしれないが念のために登録しておくバックアップ用パスワード（＝バックアップ用パスワードに頼る生体照合・所持物照合）の場合には、

どんなに慌てていても 3 回以上間違うことがないと自信の持てる本人関連データ登録 50 個も候補のある人はまれ、（恐らく 10 個もない人が多数）
＝　ユーザ名が判る環境では、強度はせいぜい　3〜5 ビット（＝8〜32 個）級どまり

＊　端末とシステム間のセキュリティは暗号技術によって 128 ビット級以上であっても、人と端末の間のセキュリティは 3〜5 ビット級。

C. ここで「パスワードの厳格管理」を強制すると

I.　優れた記憶力に恵まれた一部の若い人の場合には

無意味な 8 桁以上の英数字記号の丸暗記で　　50 ビット級以上可能
無意味な 4 桁の PIN の丸暗記で　　13 ビット級可能

II. ところが、記憶力に衰えを感じる中高年・高齢者、並びに
若くても多数のアカウントを持っている人の場合には

出来ないものは出来ないのでメモを端末機周辺に隠す或いは端末機と一緒の持ち歩きに追い込まれる
＝　強度は多くの場合に　　0 ビット、
工夫をしてもせいぜい　3 ビット級どまり
（工夫が過ぎると隠した場所自体を思い出せなくなる）

＊放っておくより悪くなる。これがセキュリティ・パラドックス。

上記 B と C の合算で、一部の若い人を除き、人と端末の間のセキュリティはユビキタスに 0 乃至 5 ビット。バイオメトリックスもトークン認証もバックアップ用パスワードに頼る限り同じく 0 乃至 5 ビット。これが眼前の現実です。

D.　遠い昔に愛着のあった視覚記憶を使ったニーモニックガードのパスシンボルを使うと

大昔に覚えてしまっているものを照合データにしているのだから思い出せないということはありえず、他人が採集し易い客観的文字データでなくて主観的な視覚イメージで他人の類推も困難であるから

64 個中の 8 個以上選択で（中高年でも）50 ビット級以上可能
16 個中の 4 個選択で（高齢者でも）11 乃至 16 ビット級可能

つまり、一握りの若く記憶力の良い人にしか実現できなかった 50 ビット級パスワードとか 13 ビット級暗証番号等と同じレベルのセキュリティを、ニーモニック認証であれば老若男女の誰でも、しかもアカウントの数が多少増えても、容易に実現することが可能です。現在 0 乃至 5 ビット級のセキュリティしかないところを 10 乃至 50 ビット級に向上させることが出来るのですから当然ビジネスの場で有効･有用であり、高機密性の情報を取り扱う分野こそニーモニック認証を採用して頂くべきものと考えます。

2　生物学的観点

動物は他の生命体を捕食して生存します。自分を捕食する生命体からは逃げなければなりません。他の生命体を認知し識別する能力（主には視覚記憶）は動物にとって生存の前提です。こうした視覚記憶能力は植物から動物が分化した時から、遺伝子の深いところに組込まれて綿々と受け継いできた普遍的な能力であると考えられます。これに対して抽象的な数字･文字に関わる記憶は古くても人類誕生後、新しければこの数万から数千年に獲得したものだと考えられます。しかも文字も数字も長く一部特権階層に独占されてきたもので、一般市民が親しむようになったのは先進国といわれている国々でも最近（百～数百年）のことです。また、一部の稀な職業を除いて数字･文字の確実な記憶保持の有無が生死を分けるようなことは先ずありませんでした。生命の歴史から見れば、どうでもいいと言って良いような付加的な能力でしょう。

無数の類似対象の中から守るべき我が子を速やかに見つける能力を保持している種や、或いは上空に舞う鳥が自分達を捕食する種の鳥なのか他の種を狙う鳥なのかを

識別できる種のみが長く存続してきました。孫・姪・甥の乳幼児時代の愛らしい写真、自分になついていた懐かしいペットの写真、自ら作成した画像、等を自らパスシンボルとして登録したニーモニックガードの使用者は同様の根源的識別能力に依拠しています。パニック状態に陥ってもこうした対象の識別に失敗することは考えられません。

3　技術論的観点

長所・メリットが特徴点となる一般技術と異なり、セキュリティ技術は短所・デメリットがその技術の特徴点となります。つまり、「その技術を導入すると何が得られるか？」よりも「その技術を導入すると何が失われるか？」に着目しなければなりません。

パスワードを長くランダムにすると或いは 3 回ルールを闇雲に適用すると高い数学的強度が得られるように見えて、実は「出来ないものは出来ない」とユーザのセキュリティを確保しようとする意思が失われます。

高い他人排除率を得られるように見える生体照合を導入すると、本人拒否の場合には本人には何の責任もないのに権利義務の履行機会が失われます。（そこで、権利義務の履行機会を失わないようにしようとすると、使わないかも知れないと思いつつ念の為に登録しておく最脆弱パスワードを OR 型で併用せざるを得ずセキュリティ崩壊に陥ることになります。）

高い他人排除率を得ようと所持物照合を導入すると、置き忘れの場合には権利義務の履行機会が失われます。（そこで、権利義務の履行機会を失わないようにしようとすると、付けっぱなしになって所持物照合の目的が失われます。置き忘れ VS 付けっぱなしの解決を念の為の最脆弱パスワードの OR 型併用に求めるとセキュリティ崩壊に陥ります。）

上記技術の組合せは「導入によって失うもの」の組合せになり、最も失うものの大きな技術のレベル、つまり最低レベルに落ち着くことになります。2 要素・3 要素と数を増やすと、他人排除率が向上するように見える一方で、本人であるのに業務不能に陥るケースはより頻繁に発生します。業務不能を受け入れるという方針を堅持すればセキュリティは守れますが、業務を優先して最脆弱パスワードに依存するとセキュリティ崩壊に陥ります。

ニーモニックガードを導入すると何を失うことになるでしょうか？それによって何か出来なくなるものはあるでしょうか？

4　心理学的観点

"記憶力が衰えてパスワードが思いだせない"、あるいは"記憶力が優れている"等という場合の記憶は心理学的には3つの機能 "符号化(記録)"、"保持"、"想起" から成り立っていると考えられます。

"符号化（記録）"は年齢や個人による差が著しいものです。対象情報内容にもよりますが一般には40代から低下し始め加齢と共に伸展します。これは符号化をつかさどる蛋白受容体の機能が衰え、記憶をになうシナプス結合が起こりにくくなるためと言われています。

"保持"は年齢差以上に、保持する内容や保持テクニックによる差異が大きいと考えられます。数字や意味の無い単語の羅列は保持し難く、意味や脈絡関係のある事象は保持し易いのです。またリハーサル効果と呼ばれる同じ内容を何回も想起すれば保持効率は向上します。これを人の脳のメカニズムで対応させると、情報は最初に音韻ループと呼ばれる機能をつかさどる側頭葉の一部を通過して海馬に記憶されます。この記憶容量は限度がありその保持期間はせいぜい1月とされています。これを心理学では短期記憶と言います。この期間中に再度リハーサルと呼ばれる想起や関連する事象情報との結合が行なわれるとその情報関連付けられたコード情報となり長期記憶として貯蔵されます。 この長期記憶情報で何回もリハーサル想起され新しいに関連情報が追加されたものはエピソード記憶と呼ばれ、長期にわたって強固に保持されます。このエピソード記憶能力は10歳程度から発達を始めると言われています。

"想起"能力については加齢による低下については未だ検証データがないようです。但し、能力よりもその情報内容による差異の方が大きいと思われます。すなわち数字や記号の様な単一の情報は想起し難く、逆に出来事の様な様々な情報が絡み合った複雑な情報は想起の鍵が多数あるために想起し易いのです。

以上の記憶メカニズムを理解すると、個々人の保有する個人情報の中でセキュリティのパスワードやバスシンボルとして使用に適したものは何かが見えてきます。 第一には、10歳以降40歳までの間に記憶されその間に何回もリハーサル効果を受け、

側頭葉に記憶された情報を使用する事です。第二は、その情報対象内容が単一の数字や単語の単一の記憶ではなく、多数の関連した情報として側頭葉にエピソード記憶として記憶された情報を用いる事です。

以上の選択は、少なくとも10歳以上の海馬や側頭葉に損傷を受けた人以外は誰でも適用可能な方法であり、高齢者であろうと若者であろうとそのパス情報を思い出す（符号化、保持、想起）能力はセキュリティとして使用するに全く障害とならないレベルの筈です。逆に言うと、40歳以上の人は（これには個人差あり一概にはいえませんが），セキュリティのための個々人のキーワード情報を新たに創造して記憶する様な事はバスワードであろうとパスシンボルであろうとお勧めでできません。

よくあるご質問

1．16 個の中の 4 個を選択する方式では数学的強度は 1/4（＝2 ビット）にしかならずセキュリティツールとしては余りに低レベルなのでは？

16 個の中にある 4 個の正解を過不足なく選択することと、16 個の中にある 4 個の正解のどれかを正しく選択することの違いを見失われたものだと思います。後者であればまぐれ当たり確率は 1/4 ですが、ニーモニックガードは前者であり、まぐれ当たり確率は次のように計算できます。

順序付きで同じシンボルの複数回選択も含めた場合には 1/16 の 4 乗＝1/65,536 となります。ビット数で表現すると 16 ビットです。複数回選択を含めない場合には 1/16x1/15x1/14x1/13＝1/43,680 となり、16 ビットを少し下回ります。順不同の場合には 4/16x3/15x2/14x1/13＝1/1,820 となり、11 ビット弱となります。

1/1,820 は一見すると心もとないような数字に見えますが、実際に多くの人に使われている暗証番号は殆どの人では本人固有文字データを使わざるを得ないためにユーザ名が判っている環境での強度は 1/5 乃至 1/10 程度です。この現実を前にすると 1/1,820 は低い数字ではありません。因みに、実効レベルでランダムな英数字記号 8 桁パスワードに匹敵する強度を要求するユーザの場合には、64 個以上のシンボル群から 8 個以上の愛着あるパスシンボルを選択すれば中高年・高齢者であっても同等レベルのセキュリティを容易に実現できます。

2．家族やペットの写真を使うといくら古いものでも家族には判ってしまうのだからニー

モニックガードはセキュリティツールとしては不適格では？

「濡れた猫の乾燥には使用できない旨を明記していない電子レンジは欠陥品である」に近いコメントとは思いますが、家族から秘密を守りたい場面で家族やペットの写真を使うのは明らかな運用ミスです。しかし、このような場面では家庭外に材料を探せば済むことです。同窓会、出張先で気に入った風景、子供時代に憧れたスター、など中高年・高齢者と人生経験が長く深ければそれだけ材料に不自由するようなことはないはずです。

3. 認証時に画面を覗かれるではないか？

画面縮小機能に加えてキーボード入力オプションを付けたことで解決しています。また、偏光フィルムを通してのみ画面内容を見ることの出来る画面非可視化技術を併用すると認証時のみなら入出力作業時も覗かれることを防げます。

4. ニーモニックガードは固定パスワードの弱点を抱えているのでワンタイムパスワードに劣るのでは？

端末機本体上で発生させるソフト方式のワンタイムパスワードについては、ニーモニックガードでもシンボル群のランダム表示によって同等の効果を得ることができるのでこちらは比較の対象にはなりません。

高いコストはかかりますがICカードや携帯電話など補助デバイス上で発生させたワンタイムパスワードを主デバイスである PC や PDA から入力させるハード方式のワンタイムパスワードは盗聴に対する堅牢性に優れています。ただ、補助デバイスの盗用問題や「置き忘れ VS 付けっぱなし」ジレンマ問題を抱えていますので、このジレンマ脱出に脆弱なパスワードではなくニーモニックガードを使うアイデアが登場しても不思議ではありません。

5. セキュアマトリックス或いは MCOP（同方式の NTT コミュニケーションでの呼称）と同じようなものでは？

セキュアマトリックスと MCOP は画面に表示された乱数表から特定のパターンに従っ

て複数の数字を拾ってワンタイムパスワードとするものです。ニーモニックガードもシンボルのランダム表示で同等のワンタイム性を提供でき、共に画面表示と記憶を利用するという基準では同じ範疇に属すものと言えるかも知れませんが、使い勝手も得られる効果も全く違います。

在来の画像パスワードの限界の一つは、認証失敗の不安があるとストレスに弱いユーザの多くは四隅/直線/斜線/L/N/V/Z など単純なパターンを選んでしまいがちになることです。このような単純なパターンは成りすまし志願者が最初に試みることが明らかなので、こうした単純なパターン選択に陥らないようにとの工夫を凝らす中で「愛着ある」シンボルを照合データにするというニーモニック認証が生まれた経緯があります。単純なパターン選択に依拠し、それ故に複数アカウントへの対応も難しいセキュアマトリックスや MCOP とは全く別の技術とお考え下さい。