ニーモニックガード開発の経緯

2004 年 3 月 1 日
株式会社ニーモニック セキュリティ
代表取締役　國米　仁

ニーモニックガードは欧米で開発された技術であるとの誤解が一部で流布していることを知りましたので、筆者による考案・開発の経緯をご紹介しておきたいと思います。

筆者は 2000 年初頭には２次元コードの用途開発を試みていました。例えば、先行事例については未確認ですが、金属鉛で２次元コードを構成しこれを製品の心臓部に格納してＸ線スキャニングによる経路追跡を可能にし製品横流しや盗品故買の抑止手段とする、などといったものです。ある日相談中の弁理士さんから「２次元コードは通信のセキュリティに使えないものか？」との問いかけがありました。

“ とても覚えきれないような多桁のパスワードを表した２次元コードを１枚のカードに印刷して所持し、個人認証が必要なところでその２次元コードをスキャンすれば長いパスワードを送出できる。ユーザの記憶負担はカードを失わないように気をつけるだけ。 ” というアイデアが瞬時に浮かんだものの、その２分後に“ このカードを不正取得した人物には 100%の確率で成りすましを許してしまう ” （注）と気がつきました。

その夜の寝床の中で多桁パスワードを例えば４分割して４つの２次元コードに割り振り正しい順序でスキャンして当初の多桁パスワードを復元して送出する ” というアイデアが登場しました。しかし、４分割であれば４ｘ３ｘ２ｘ１の組合せしかありませんから最大２４回の試行で破られます。１０分割もすれば３，６２８，８００通りの組合せにはなりますが復元方法の記憶が大変です。少ない記憶負担で大きな効果を得るという最初の目的に背いてしまいます。

数日後の夜明け前に９６個の囮と混在させた４個を正しく選ぶようにするとまぐれ当たりの確率を１００の４乗に近いところまで上げられることに気がつきました。これだと４個の位置と順序を記憶するだけで､通信上のセキュリティは例えば 40 桁のパスワードであれば 200 ビット相当であり、盗難時の不正取得者に対するまぐれ当たり確率は１億分の１弱となり、かなりの数学的強度を提供できます。混在させる囮の数を１０００個にすれば１０００の４乗というレベルの強度すら得られます。

実際に試作をして自ら試してみました。すると４個の位置に関して、覚えやすい位置と覚え難い位置があることが判りました。直線上に集める、４角に置く、或いはアルファベットなど簡単なパターン上に配置したものしか覚えられないのです。これでは実際には 100 の 4 乗どころではなく、恐らく１００にも届かない少数のパターンの組合せ数が上限になってしまうのでセキュリティを謳えるよう代物にはなりません（注）。

長い煩悶の時期を経て、個々の 2 次元コードに識別補助の為のイラストか写真を対応させようと考えつきました。次に、不正取得者に対する数学的強度が余りに低い状況でパスワードを無闇に長くしても無意味であると気づき、力点を不正取得者対策に置くに従って２次元コードに拘る理由がなくなってきました。２次元コードと切り離しますと、囮に混在した登録イラスト・写真を選ぶことになり旧来から研究されてきた単純画像パスワード（注）と一見同じようなも

のが出来上がりました。

しかし、在来の単純画像パスワードとは異なり、有意味なものを無意味なものに混在させるというプロセスを経て辿り着いたものですから見かけは似ていても思想は異なります。無意味なものの中から有意味なものを選ぶという考え方を更に精緻化する思考努力の中で、愛着のある視覚対象を登録データにする、とりわけ遠い昔に脳に刷り込まれた画像イメージを登録データにするという現在の長期視覚記憶活用方式に辿り着くことになりました。

その間、ある方から「どれかのシンボルを選択すると自爆するようにしておけば」とのアイデアを頂戴しました。このアイデア自体はユーザに新たな記憶負担を要求することになるので使わないことにしましたが、このことが契機となってユーザに新たな記憶負担を要求しない自爆メカニズムの模索が始まりました。ああでもないこうでもないとの試行錯誤を数週間にわたって寝床の中で繰り返す中で生まれたのが「本人でも犯すような間違い選択」と「本人なら犯すはずのない間違い選択」をパターンとして定義してソフトウェアに自動判定させるという現在の本人・他人峻別アルゴリズムです。

異常事態通報シンボルはあるセキュリティセミナーに参加している時に、この人達はシステムを守ることしか眼中になくてユーザ個々人を守るという発想に欠けていると感じた瞬間に頭に浮かんだものです。直ちにセミナー会場から弁理士さんに電話した記憶があります。

このユーザ保護の観点からは「生体照合に意思行為を加える」というアイデアも同時に浮かびました。筆者は客体としての人間を取り扱う生体計測・識別技術がそのまま意思行為の主体としての人間に関わる本人認証に応用できるとは考えていませんが、識別を生体計測で行い認証は記憶照合で行うという複合方式は有効であろうとは考えていました。例えば顔計測で本人を推定識別（認証に非ず）しておき、本人認証は本人ならば行えるであろう意思的行為（ウインクを右、右、左、顔を右向き、右向き、左向き、或いは右手上げ、右手上げ、左手上げによって 3 ビットの記憶照合）の自動認識によって行うのですが、そこにユーザがプラスαの行為を行って異常事態であることも通報しようというものです。児戯のようなものかも知れませんが特許申請には加えました。

> 注：　所持物照合、パターン記憶法、単純画像パスワード等は、ニーモニックガード開発途上で通過していることにお気づきと思います。

ともあれ、ニーモニックガードは以上のような経緯でゼロから、主に夜明け前に寝床の中で、筆者の頭の中で考案されたものです。欧米の研究成果を輸入したものではないことを明言しておきたいと存じます。

以上