改めて誤解を解く　Ｖ６

2008 年４月１８日

株式会社ニーモニックセキュリティ

＜　目次　＞

- **本人認証には「記憶照合」「所持物照合」「生体照合」の３つの範疇がある**

これまでは、本人認証については
　　記憶照合：What we know
　　所持物照合：What we have
　　生体照合： What we are
という３つの範疇がある、という認識が主流でした。

これは、『本人確認』・『個人識別』・『本人認証』という３つの概念についての明確な区別・定義が不在であり、また当人の意思の有無確認についての問題意識が欠如していたことによる不正確な認識で、その結果として『個人識別＝本人認証』といった誤った考え方の蔓延につながってきました。ただ、対面交渉が主流であった時代ではこうした不正確な認識でも実践上は特に大きな不都合はなかったようです

しかしよく考えてみると「所持物照合・生体照合」と「記憶照合」の間には、いわば非常に深くて暗い河のあることが判ります。警察が探し出した被疑者と自ら名乗り出てきた被疑者を取り調べているところを想像してみましょう。

「やったのは俺ではない。」と言い張る被疑者の主張を突き崩すのには「所持物」と「生体」が有効です。「お前はやっていないというが、現場にはお前の財布が落ちていたし、お前の指紋も残っていたぞ」。この場面では被疑者の「記憶」の出番はありません。

「俺がやりました。現場には俺の財布も指紋も残っている筈です。」との被疑者の主張を「所持物照合」と「生体照合」だけで受け入れてしまうと身代わり自首を簡単に許してしまうことになります。ここは当事者である犯人しか知り得ない情報（＝照合されるべき記憶）を被疑者から聞き出さなければなりません。この場面では「所持物」や「生体」に頼ることはできません。

つまり、「所持物・生体」と「記憶」の役割は見事に正反対あるいは凹凸と凸凹となっていることがわかります。この両者を等しく同一の範疇として扱うのは無茶というものです。「所持物」ないし「生体」の照合で実現するものは「個人識別」です。「記憶」の照合で実現するのは「本人認証」です。個人識別＝本人認証という認識が成立することはありえません。

「本人確認」は「個人識別」と「本人認証」というレベルを異にする２つの領域から成り立っている、と考えると全体がすっきりと整合します。そして、それぞれ実現するための技術要件は次のように異なります。

個人識別：　意思確認不要。所持物の照合および身体の特徴点の照合によります。

本人認証：　意思確認必須。記憶の照合によります。

＊　「本人認証手段が法理に則っているか否かは、手段の技術的優劣の議論に先行する。法理の観点からは、本人の意思が反映されないままに権利義務の主体確定のプロセスが完結してしまう本人認証なるものは存在しない。」という法的な点に注目しても「本人認証」と「個人識別」の原理的な違いは明確です。

- **メモや手帳で管理するパスワード**

「アカウント毎に異なるパスワードを使うこと。パスワードは少なくとも８桁、できれば１２桁の無意味無機質なランダム英数字とすること。望ましくは特殊記号も混ぜて。また、数ヶ月に一度は変更すること。そして、このルールはアカウント数がいくら増えても変りなし。」

全ての社員がこのような要求をメモ・手帳に頼らずに実行できていることになっている企業はギネスブックにでも申請して頂くことにして、現実的には手帳での管理を認めるか見て見ぬ振りをするところからセキュリティを考えることになります。

現実的なセキュリティポリシーとしては、「パスワード類の記載された手帳は、食事も手洗いも離席時にはいつも肌身離さずに持ちあるくこと。メモをＰＣの周囲に置いておくことは厳禁。」ということでしょうか。ユーザがＰＣから離れる時には手帳もＰＣから離れますからメモをＰＣの周囲に置き去りにしている状態より相対的にはずっと安全と言えるでしょう。

ところが運用場面にモバイル環境が入ってくると極めて悩ましくなります。端末と手帳の保管場所が同じだと端末を失う時には手帳も一緒に失うことになり、そのリスクを下げようと保管場所を違うところにすると端末を持って出たものの手帳は置き去りといったことになり仕事になりません。置忘れを一度でも経験すると多くの場合は端末と手帳はいつも同じ保管場所に入れられることに落ち着きます。紛失時にパスワードによる保護は期待できません。

他方では、手帳に頼らずに済むような覚えやすいパスワードは破られやすいことが知られています。そうするとモバイル環境で確かな利用者認証が必要な場合には文字パスワード以外で手帳に頼らずに済む本人認証手段を考えざるを得ません。本人拒否時の救済手段としてパスワードを併用せざるを得ない本人認証手段では何の解決にもならないことは言うまでもありません。

- **オフィスで使えればモバイルでも使える**

オフィス環境でもモバイル環境でも利用者認証＝本人認証の要件は同じだとの前提に立った議論が多く見かけられます。

しかし、オフィスとモバイルは次のように環境が全く異なります。

	オフィス環境	モバイル環境
・物理的警備	可	不可
・同僚の環視	可	不可
・管理者の支援	可	不可
・端末盗難・紛失リスク	小	大
・脅迫・強要リスク	小	大

モバイルで使えるものは、よりリスクの低いオフィスでも使えるとはいえます。しかしオフィスで使えるからといって、よりリスクの高いモバイルでも使えるとは言えません。

オフィス環境では、食事・会議・手洗いなど離席する時に手帳を離さずに持ち歩くようにしておけば、ユーザの不在を狙って攻撃者がＰＣに触れようとしてもパスワードの記載された手帳はそこにはありませんから『文字パスワードの手帳管理』でそれなりの安全性を確保できます。

ところがモバイル環境ではどんなに頑張っても端末と手帳はユーザの右手と左手以上に離れることはありません。離れてしまうと仕事にならず、離れなければ一緒に紛失したり盗まれる可能性が高くなります。

同じことは『携帯電話・ＩＣカード・ＵＳＢキーなどの所持物』を照合する方式でも成りたち、端末と所持物が離れてしまうと仕事にならず、離れなければ一緒に紛失したり盗まれる可能性が高くなります。（携帯電話Ａからのアクセス時には携帯電話Ｂを照合用所持物として使い、携帯電話Ｂからのアクセス時には携帯電話Ａを照合用所持物として使うといった妙案にご興味のある方は
http://www.mneme.co.jp/manga/parody/index1-14.html　をご笑覧ください。）

生体照合の場合、オフィス環境では本人拒否が起こってもセキュリティを下げない解決が可能です。一般にセキュリティ管理でユーザより上位の権限を持つシステム管理者に対応を委ねることができるからです。ところが、モバイル環境とはそうしたシステム管理者に頼ることのできない環境です。

本人拒否が起こらないような設定値（閾値）で運用すればセキュリティは確保できず、セキュリティを確保できるで設定値（閾値）で運用すれば本人拒否時にユーザ自身が裏口を開けられるようにしておかねばなりません。そこでパスワードを裏口に使うとセキュリティはパスワード単独方式よりも低下してしまいます。

「オフィスではオフィスで使える本人認証手段を使えばよく、モバイルではモバイルで使える本人認証手段を使えばよい」という結論になってもよいのですが、今やオフィスとモバイルが有機的に一体化する方向に進んでいます。同じアカウントにオフィスではオフィスのＰＣから、移動時にはモバイル端末から、自宅では自宅のＰＣからアクセスするという情景が普通のことになるでしょう。

選択肢としては

Ａ　オフィスで使っている本人認証手段をモバイルでも使い、モバイルでのセキュリティ不安には目をつぶる。

Ｂ　オフィスではオフィスで使える本人認証手段を、モバイルではモバイルで使える本人認証手段を使い、利便性の低さと高いコストには目をつぶる。

Ｃ　モバイルで使う本人認証手段をオフィスでも使い、セキュリティ・利便性・低コストの全てを実現する。

モバイル環境で信頼できるものは『他の手段に依存することなく単独で利用可能な記憶照合』しかありません。当社がモバイル分野に注力している所以です。

・生体の特徴点も印鑑も共に本人の意思を反映しない？

当社事業の出発点は、『本人確認』は社会的生活を成り立たせる根源的な要件であるが、この本人確認には異なる二つの範疇があり、一つは「この人は誰？」に答える『個人識別』であり、もう一つが「この人が真にその人か？」に答える『本人認証』である、との認識です。

私達は「この人が真にその人か？」に答える本人認証は、当該人物を何らかの権利義務の主体として確定させる社会的行為なのだから本人の意思確認なしに成立してはならない、と言い続けてきました。また、本人の意思の有無を反映しないプロセスの結果として個人が何らかの権利義務の主体として確定されてしまう本人認証なるものは民法の基本理念と如何なる整合性を持つのか、といった問題提起も行ってきました。

このテーマに関してある方から「本人の意思を反映しないという意味では生体の特徴点だけでなく印鑑もそうではないか？」という質問をお受けしました。筆者の見解は次の通りです。

いわゆる三文判ではなく実印について考えます。起きている時も寝ている時も『実印』と明記した実印を誰にも見えるようにして首からぶら下げて暮らしている人を考えれば（生体の特徴点とはそのようなもの）その通りとも考えられますが、実印をそのように扱おうという人はどの位いるでしょうか。少なくとも筆者の場合は、実印は窃盗の意図を持って拙宅に侵入した盗人でも必死に家捜しをしなければ見つからないと思われる場所に秘匿しており、実印が必要な場合には筆者は自らの記憶を頼りに意思的に実印を秘匿場所から持ち出します。押印された実印には本人の意思が反映されていると想定することが十分に可能です。

盗難あるいは欺瞞によって本人の意思が反映されないままに実印が使用されるケースでは生体の特徴点と同じではないかとの議論もありえますが、そのように考えても得られる結論は一つ、本人の意思を可能な限り明確に反映する本人認証手段が必要とされている、ということでしょう。。

尚、そこにいる管理者が、当人が不審な動作無く自発的に、意思的に行動していることを監視している、または衆人が環視しているといった恵まれた環境では、本人認証手段自体が意思を反映していなくても本人認証の主体の意思確認が行なわれていると見なすことは可能です。ただし、デジタル社会・ネットワーク社会というのはこうした管理者の監視や衆人の環視のないところで信頼できる本人認証が必要とされる社会であることを忘れるわけにはゆきません。

・本人認証製品として売られているからといってセキュリティを向上させているとは限らない

パターン記憶型マトリックス認証:　四隅とその周辺・縦横斜めの直線・Ｌ やＶなどの簡単なアルファベットは誰にでも（＝攻撃者にも）簡単に思いつくもので、こうしたもので得られるセキュリティはせいぜい数十種類、ビット数ではせいぜい５～６ビット程度でしかありません。これでセキュリティを謳うのは無茶というものです。そうすると、攻撃者には思いつかないパターンでありながら、正規のユーザには簡単に記憶でき複数のアカウントでも使いこなせるパターンが幾つ位存在できるかを考えてみる必要がありますが、ユーザも攻撃者も同時代に生きている同じような人間であることを考えると、この設定の中身自体が矛盾を含んでいます。

機械生成型ワンタイムパスワード：　機械によって生成される「ワンタイムパスワード」と呼ばれている一時乱数が証明しているのはトークンの真正性であって本人の真正性ではありません。フィッシング対策効果やスパイウェア対策効果については、トークンの真正性を証明する情報はワンタイム化されているのでフィッシャーに盗まれても影響はないといえますが、これは元来本人認証情報ではありません。即ち、本人認証情報の流出防止とは別の範疇での出来事に過ぎません。

救済用パスワードを併用する多くの生体認証製品:　ロック状態を、生体認証でもパスワードでも、どちらでも解除できる運用方式を許しているのであれば、パスワードよりも高いセキュリティを謳うことは原理的にできる筈がありません。

救済用パスワードを併用しない一部の生体認証製品：　身体や環境が多少変動しても本人拒否が起こらないのであれば、そのような閾値設定で運用されていると解釈されます。そうした場合の実際の他人排除率つまりセキュリティは、第三者機関による客観的評価のない状態では、「低いとも高いとも何とも判らない」としか言えません。

・**「扉を頑丈にすることは良いことだが鍵の強化の代替にはならない」**

１メートル厚の鋼鉄製の扉に４桁のコンビネーションロックが付いている金庫を考えると、この金庫の安全性は１メートルの鋼鉄製扉ではなく４桁のコンビネーションロックによって決まっていることは誰にでも判ります。

同じことが暗号などの情報セキュリティでも成り立ちます。どんなに強固な暗号ソフトであっても或いは秘密分散法などの他の情報秘匿手法であっても、利用者認証が４桁の暗証番号であれば、この暗号ソフトの運用上のセキュリティが４桁の暗証番号のセキュリティを上回ることなどありえません。データをより長い鍵で暗号化する或いはより強力・巧妙に分散・秘匿することは良いことには違いありません。しかし、利用者認証の強度向上が伴わなければ運用上の安全性が向上することはないのです。

・　**一番大事なことは最後にじっくりと**

最高機密の暗号化保護などの高度なソリューションについては、アクセス管理の整備などセキュリティ体制全般の見直しを行った後で時間をかけてじっくりと検討するのが望ましいといった考え方が強いようです。これは妥当なものでしょうか？

洪水の危険が迫っています。乳幼児や家宝を先ずは高いところに避難させておいてそれから家の周りに土嚢を積むことを考えますか、それとも乳幼児や家宝は一階に置きっ放しのままで先ず家の周りの土嚢積みを終わらせてしまおうと考えますか？　筆者ならば迷うことなく前者を選択します。

情報の保護も同じでしょう。外部から守秘義務を負って預かっているデータなど、この情報が流出したら、特に権限を与えてある社員に持ち出されたりでもしたら、大変なことになるといった最高度の機密情報を今手に入る最良の手段で保護して最悪の事態に対する手当てを先ずは終えておき、それからじっくりと時間をかけて全般的なセキュリティ体制の整備を進めるのが王道ではないでしょうか？

・**リモートロックがあれば暗証番号を覚えなくてもよい**

最近は携帯電話紛失時のリモートロック・リモート削除機能が大きく取り上げられていますが、こうした機能の存在を知っている攻撃者に対する効果は極めて限定的であることに触れない議論が多いことに憂慮しています。

紛失時には遠隔で停止処理を行うというのは、「リモート」という言葉を使わないだけでキャッシュカードやクレジットカードでは昔から当たり前のことでした。しかし「遠隔からの停止処理が行えるから紛失しても心配しなくても良い」などと言う銀行やカード会社はなく、カードは紛失するものとの前提で暗証番号の管理に注意を払うように呼びかけてきました。携帯電話は紛失すると直ぐに気が付くがカードの入った財布なら失っても直ぐには気が付かない、ということもないはずです。

携帯電話のリモート処理は電源が入っており電波が届いている限りにおいて有効という（カードにはなかった）制約条件もあります。リモートロック・リモート削除に頼り切るのは避けるべきで、何といっても携帯電話の所有者認証（カードの暗証番号に当たる）には十分な注意を払うべきだろうと思います。

・シンクライエント端末からの情報漏洩

シンクライエントの場合には『端末』からの情報漏洩はありえません。しかしアカウント凍結以前であれば接続先の『サーバ』からの情報漏洩がありえます。

数百件の顧客データへのアクセス権限を持つＡさんがネット非接続のモバイル端末で持ち歩く顧客データについてはその日訪問予定分のみを当日朝一番にダウンロードし前日分は消去されています。盗まれて利用者認証を通過されてしまった場合には当日訪問分の顧客データが漏洩する恐れがありますが、それ以上の被害はありません。

同じく数百件の顧客データへのアクセス権限を持つＢさんはシンクライエント端末を持ち歩いています。盗まれて利用者認証を通過されてしまった場合には『端末』からの情報漏洩はありませんが、接続先のサーバから数百件の顧客データが最も貴重なものから順に『端末』経由で漏洩する恐れがあります。アカウント凍結までの時間は、素人にはアッと言うまでの短さでも、計画的なプロには贅沢といえるほどの長さかもしれません。

「シンクライエントは安全」という命題は成り立ちません。シンクライエントであれ、リッチクライエントであれ、利用者認証の確実性が最重要課題です。

・　漏洩と改竄

先に情報漏洩に関して「シンクライアントは安全」という命題は成立しないと申し上げました。しかし管理者の観点からはリッチクライアントよりも情報の管理を行いやすいのだから間接的にはセキュリティ向上に貢献するのではとのご意見を頂戴しました。この観点に立つ限りはその通りだと思います。ところが、考えを進めてゆくうちに別の難題に突き当たりました。

ユーザがファイルサーバ上のデータに直接アクセスできる方式でユーザ認証が脆弱であった場合のリスクは情報漏洩もさることながら、更に恐ろしいのはデータの改竄です。たとえば、ファイルサーバへの加筆修正可能アクセス権を持つユーザのパスワードを入手した攻撃者がファイルサーバに直結できるシンクライアント端末を前にすれば

・機械部品の規格を微妙に変える
・与信供与先の収入・利益の数字を微妙に変える
・医療データの病名・病歴や投薬内容を微妙に変える
・開発中のソフトウェアのコードの一部を微妙に変える

といった悪質なサボタージュを行うことは極めて容易です。特に外部から預かったデータを悪意の侵入者に巧妙に且つ微妙に改竄されて気づかないケースを考えると、引き起こされるダメージは測り知れません。

リッチクライアントの場合は端末上でのデータ改竄が直ちにファイルサーバ上のオリジナルデータの改竄となるわけではなく、サボタージュが実現するためにはデータがシンクロナイズされる必要があります。つまり少なくとも一ステップの余裕があります。

シンクライアント方式はリスクが高いと言っているわけではありません。ただ、シンクライアント方式であればただそれだけで安全であるかのごとき不適切な認識が蔓延することには大きな危惧を抱かざるを得ません。シンであれリッチであれ、また情報漏洩であれ改竄であれ、特にモバイル環境も視野に入れると、安全のための最大の鍵は確かな利用者認証・本人認証であることを力説しておきたいと存じます。

・工夫次第で破られない暗証番号を覚えられる

筆者の経験をご紹介しますと、例えば「國米→黒米→くろごめ→くろふね→黒船来航」で連想できる１８５３から某縁者の生まれ年を引算した結果を右から逆に読んだ数値を暗証番号として登録する、といった手法を実践していました。必ず復元でき誰にも破られない、と自信を持っていました。

普段は問題なく使いこなせました。ところが短気で怒りっぽい大事なお客さんを待たせている場で慌てて暗算を急いだところその数字をＡＴＭが受け付けず、焦れば焦るほど最初に設定したルール自体の記憶に自信がなくなるという事態に陥りました。後で落ち着いたところではっきりと思い出しても後の祭りです。そこで悟ったのです。パニック状況でも間違いなく入力できるような数字列を多くの人が暗証番号として登録することになってしまうのは当たり前で自然なことだ、と。パニックに耐える記憶照合本人認証を目指す当社技術開発の伏線となったエピソードでもあります。

工夫を負担と思わない或いは楽しみとできるような頭脳に余裕のある人達にはどんどん工夫をして破られない暗証番号を覚えて頂けばよいと思います。ただ、我々はこうした工夫を負担と思ってしまう或いは工夫に楽しみを見出せないような人達を念頭に置いた記憶照合技術の開発を続けたいと考えています。

・文字パスワードの上位互換

文字パスワードとニーモニックガードは排他的な関係にあるものではなく、ニーモニックガードは文字パスワードに対して上位互換の関係にあるものです。

ニーモニック認証画面にイラスト・写真に加えて英数字も用意しておきますと、自然に既存の英数字パスワードを吸収することになります。携帯電話の場合であれば１０キーも十字キーによる画面選択もどちらでも入力可能とできます。

つまり文字パスワードを使っている既存の利用者に違和感を与えることなくセキュリティの強化手段を追加的に提供できるのです。また、漢字を暗証画像（パスシンボル）として使う手法もニーモニックガード誕生以来活用されています。

因みに、ニーモニックガードはパターン記憶法に対して、また単純画像パスワードに対しても上位互換です。ニーモニックガードの中でパターン記憶法をその一部として使うことは自由であり、長期記憶に関わらない単純画像パスワードを下位互換の手法として使うことも自由なのです。

つまり、ニーモニックガードはこれまで知られている記憶照合手法に対して上位互換技術であると言うことができるのです。

・２要素認証はニーモニックガードより強いか

いわゆる２要素認証はパスワードを一つの要素とし、照合すべき何らかの所持物をもう一つの要素とし、二つの要素が共に真正である場合に正規の利用者であると認証するものです。

所持物としてはＩＣカード、ＵＳＢキー、使い捨て乱数受信携帯電話、使い捨て乱数生成トークン、などが知られています。

ニーモニックガードを１要素とする２要素認証は他の要素の効力がゼロでない限り単独で運用されるニーモニックガードよりも強くなります。αもβもプラス値であるかぎりα＋β＞αですから。

ここで２要素方式一般について考えてみます。１＋１＝２＞１なのだから弱いものでも２つ合わせれば強いものになると信じたいところですが、残念ながら無条件で成り立つものではありません。子供２人でも２人は２人であり、２人は１人より強いのだから朝青龍にでも勝てる、とはなりません。２人であっても朝青龍に負けないためには２人のうちの少なくとも一人は相当に強い力士でなければなりません。

２要素認証はその中に１要素として所持物照合を含んでいますから、オフィス環境（端末は机に張り付き、所持物は人間に張り付く）ではそれなりの有効性を謳うことはできます。しかしモバイル環境（端末も所持物も同一の人間に張り付く）では事情が全く変わってしまいます。【盗用には無力な所持物】と【使いこなせない文字パスワード】とによる２要素認証のモバイル環境での信頼性については、同じ様に【盗用に無力なカード】の提示と【使いこなせない暗証番号】の入力を求めるＡＴＭ出金方式を考えてみればよいでしょう。

ところで、実際に使われている例は寡聞にして聞いていませんが、手帳を１要素とする低コストでシンプルな２要素認証もありえます。１要素は２要素認証で一般に使われている【記憶できるパスワード】、もう一つの要素を【頻繁に変更する難解パスワードを記載した手帳】とします。正規の利用者であれば記憶パスワードを入力できる上に真正な所持物（手帳）を保持していることを証明でき、逆に攻撃者はユーザの記憶と所持物（手帳）の両方を取得せねばならないわけですから、これで立派な２要素認証になります。　この【記憶できる脆弱なパスワード】を文字パスワード上位互換のニーモニックガードで置き換えることもできるのは言うまでもありません。

・パスワードを掛けたＰＣは紛失しても大丈夫

紛失したＰＣに掛けていたパスワードは何桁ですか？　１５桁以上のランダムなパスワードであれば一応大丈夫といえますが、１４桁以下であればパスワードクラッキングソフトを持っている不正取得者の手に落ちれば簡単に破られてしまう可能性大です。

こうしたクラッキングソフトはパスワードを復元できなくて困っているユーザを救うためのツールとしてネット上などで公開されていて誰でも入手できます。(逆の観点では、パスワードを復元できなくなっても困らないということを情報漏洩防止よりも優先させるのならば１４桁以下にしておけばよいとも言えます。)

筆者のグループが試したものでは１４桁のランダムパスワードが１時間程度で破られました。一番確実な防衛策は異なる照合方法が使われているといわれている１５桁以上のパスワードを登録することです。オフィスの中ならパスワードの手帳管理という手があるので３２桁までででも取り扱い可能でしょう。

しかしモバイル環境での手帳管理は不安です。だからといって１５～３２桁ものパスワードをしっかりと覚えていて慌てても焦っても思いだせるなどというのは人間業ではありません。別のアプローチが有効です。当社からは以下の対策を提供できます。

○　ニーモニックガードＰＣログオン版：　１５桁以上できれば３２桁のパスワードを登録し、このパスワードはメモに記して安全な場所に保管します。この記憶の必要のない管理コードともいえる強力なパスワードを長期視覚記憶活用のニーモニックガードで管理運用します。

○　ニーモニックガード起動型ないしクリプトニーモ搭載型ＵＳＢメモリー：　　持ち出しＰＣには大事なデータは保存しません。ニーモニックガードを通過し　なければメモリー領域にアクセスできない或いは暗号データを復号できないＵ　ＳＢメモリーに保存してＰＣと一緒に持ち出します。

・見えやすい脆弱性と見えにくい脆弱性

「見えやすい」脆弱性は「見えにくい」脆弱性よりも大きな問題のように感じてしまいがちです。本当にそうでしょうか？

「ソフトキーボードやニーモニックガードは覗き見に弱い」などは見えやすい脆弱性どころか『誰にでも見えてしまう』脆弱性の代表といえるでしょう。攻撃者も気づきますが、それ以前に使っているユーザ自身が気づいてしまうので自然に画面の遮蔽や傾斜を試みるなど覗き見されないための工夫をすることになります。

「見えにくい」脆弱性の例としては「１４桁以下の Windows パスワードは、一般ユーザには容易ではないような設定処理をしない限りパスワードクラッキングソフトの持ち主にかかると短時間で破られてしまう」ことなどが挙げられます。この「見えにくい」脆弱性に伴う問題は、殆どのユーザが知らないことを、目的意識的に迅速な情報共有を行う犯罪予備軍の人達は知っている可能性が高いことです。

「犯罪予備軍の間では知られている脆弱性を、正業を営んでいるユーザの殆どは知らない」という状況と「犯罪予備軍が知っている脆弱性は一般ユーザも広く知っている」という状況のどちらが恐ろしいと思われますか？

・できないことをやらせるのがセキュリティ

A　難解パスワードを覚えろ　→　隠れメモ依存蔓延　：　高い確率で机周辺かユーザの身の回りにメモがある。攻撃者はそのことを知っている

B　USB メモリーの持ち出しは一律に禁止する　→　私物 USB メモリーでの無断持ち出し蔓延　：　紛失しても会社に届けない。攻撃者はそのことを知っている

C　情報端末の持ち出しは一律に禁止する　→　紙媒体の持ち出し継続　：　鞄は必ず開けられる・重要書類は一目で見つかる・スキャナーで PC に取り込める・文書はデジタルデータとして売却できネット上で公開できる。攻撃者はそのことを知っている

我々の考え方は、無理難題の言いっ放しは「百害あって一利なし」なので、やれることの中での最善を尽くそうというものです。つまり、

A　難解パスワードを覚えられない人にはニーモニックガードを使うという選択肢がある（覚えられないからといって脆弱パスワードに戻るのは不可。）

B　確実な利用者認証機能のついた USB メモリー持ち出しは許可する（暗号化だけでは不可。何故ならば暗号ソフトの運用上の強度は暗号ソフト利用者認証の強度を上回ることがないから。あくまで利用者認証の強度が判断基準。）

C　確実な利用者認証のできる情報端末の持ち出しは許可する（暗号化については B と同じ。）