長期イメージ記憶と情報セキュリティ

株式会社ニーモニックセキュリティ
代表取締役　國米　仁

2008年5月1日

目次

１．　本人認証

・本人認証の意義 ---------- 3 ～ 4頁
・オフィス環境とモバイル環境 ---------- 5 ～ 6頁
・長期視覚記憶を活用する本人認証 ---------- 7 ～12頁

２．　長期視覚記憶を活用する本人認証の応用事例

・安全なモバイルビジネスを実現 ---------- 13 ～16頁
　　ノートＰＣ・スマートフォンのログオン認証
　　ＵＳＢメモリーのロック機能
　　暗号鍵をその都度作るクリプトニーモ
・暗証番号・パスワードを手元で管理 ---------- 17頁
　　携帯クリプト手帳
・有権限者も一人ではデータの持ち出し不能 ---------- 18頁
　　権限分散クリプトニーモ
・ネット取引の利用者認証 ---------- 19 ～21頁
　　フィッシング排除機能内在ウェブアクセス認証
　　トロイの木馬を無力化
・制限エリア入室管理 ---------- 22頁
　　非可視画面複合キオスクステーション
・開発中の応用製品 ---------- 23頁

３．　資料編

・本人確認における「識別」と「認証」 ---------- 25 ～28頁
・在来の認証方式 ---------- 29 ～32頁
・本人認証と法理 ---------- 33頁
・優良誤認問題 ---------- 34 ～41頁
・技術マップ ---------- 42 ～48頁

本人認証が暗号技術のセキュリティも決める

暗号技術は、情報の機密性確保など情報社会秩序維持の必須技術
　だが、有権限者は必ず望むときに平文で読めなければならないので、
運用上の安全性は、利用者認証（本人認証）の安全性を上回ることはない。

また、

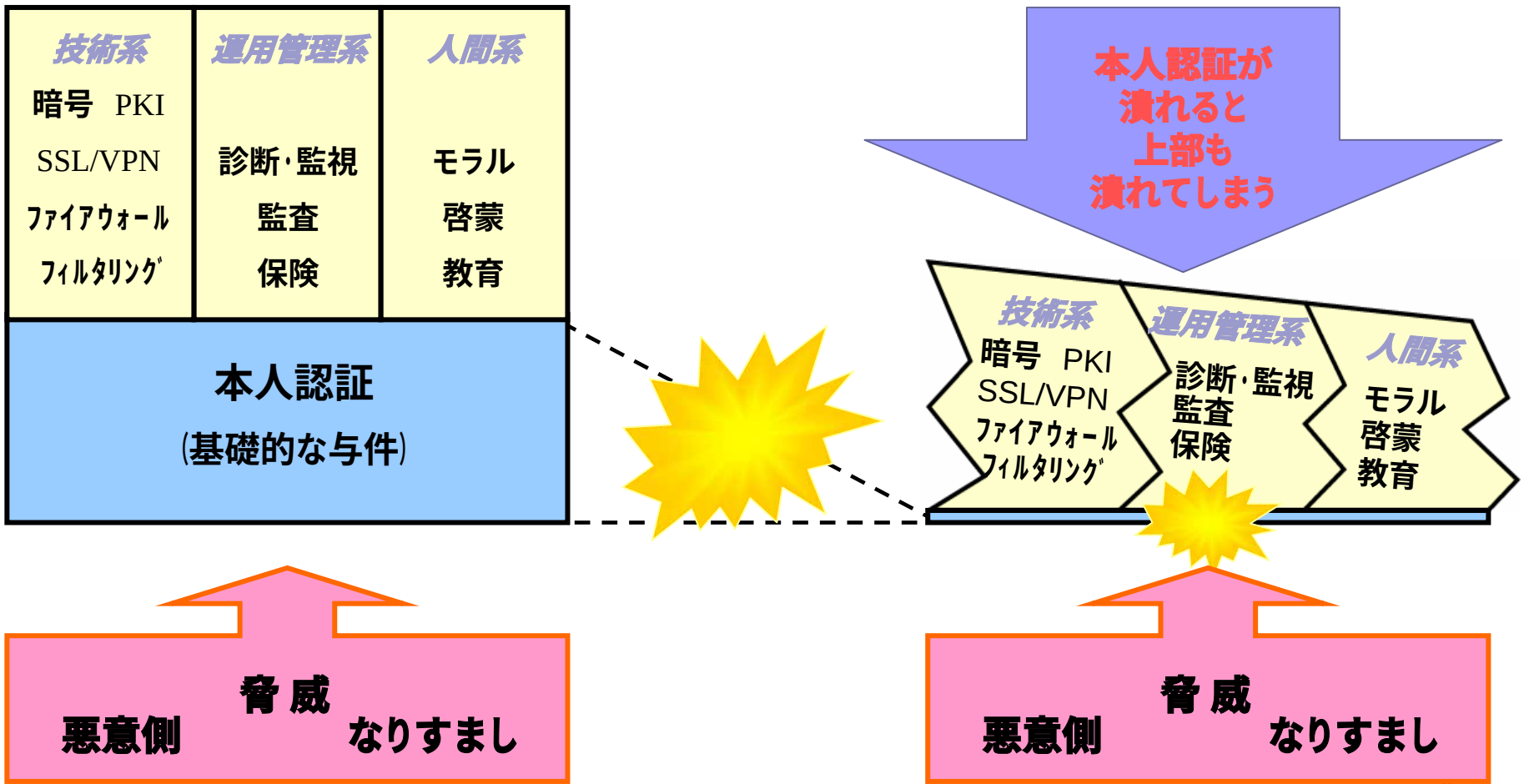
全てのログを完璧に収集していても、ログ対象のアカウントの本人認証がおざなりでは収集したログ情報を信頼できない。

シンクライアント方式でも本人認証が弱いと情報の流出を防げず、特に改竄の脅威は深刻。

更に、管理者の本人認証が脆弱だとセキュリティシステム全体が攻撃者の便利ツールに化けてしまいかねない。

本人認証はセキュリティの基礎的与件

本人認証はあらゆるセキュリティ要素技術を考慮する前に
すでに存在していなければならない基礎的な与件



オフィス環境とモバイル環境

	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言える。

しかし、オフィスで使えるからと言って、よりリスクの高いモバイルでも使えるとは言えない。

攻撃手段はどんどんと高度化し多様化する： A→B→C→D → V・W・X・Y・Z
攻撃者は最古のAから最新のZまで自由な選択と組み合せが可能
＝ 防衛側はA～Zの全てに同時に対抗しなければならない

オフィスで有効 ≠ モバイルでも有効

オフィス環境 (**端末： 机に張り付いている**)

1. 離席する時に手帳を持ち歩く → ＰＣの近くに手帳はない
   → 『難解パスワードの手帳管理』でそれなりの安全性を確保
   (携帯電話・ＩＣカード・ＵＳＢキーなどの照合用所持物でも同様)
2. 生体照合で本人拒否発生 → 上位権限者による対応でセキュリティ維持

モバイル環境・野外現場 (**端末： ユーザ個人に張り付いている**)

1. 端末と手帳・照合用所持物が
   離れてしまうと仕事にならない
   離れなければ一緒に盗まれる可能性が高くなる
2. 本人拒否時に頼れる上位権限者はいない
   救済用にパスワードを使用するとセキュリティはパスワード単独より低下
   本人拒否を起こさない閾値での運用は他人排除力なし

在来の本人認証技術はオフィスではそれなりに有効、
しかし、モバイルではとても有効とはいえない

モバイル環境で使いこなせる

ニーモニックガードとは(概要)

なつかしく愉しい長期視覚記憶を活用し、いつでも、どこでも、誰もが、ストレスなく使いこなせる、確実な「本人認証技術」です。

本人認証(暗証番号・パスワード入力)時、
数字や英文字ではなく、**思い出の写真・イラスト(記憶の映像化したもの)**
により、認証を行います。

暗証番号を思い出す必要や、新しく憶える必要はありません。

認証画面作成登録の手間は:　便益(運用時のセキュリティと利便性)とのバランスで判断

混乱・パニックの危機現場に耐える

ニーモニックガードとは(特長)

思い出の写真やイラストを数枚準備しパスシンボルとして登録。
ダミーを加えてユーザー独自の認証画面を作成。

1．正規ユーザには優しい

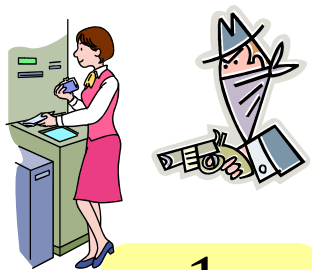
・正規ユーザにとっては思い出の写真（イラスト）を
使っているから、どんな時でも、すぐに見つけられます。

・本人を推定するエラーは何度でも許容します。

2．不正使用者には厳しい

・速やかな他人断定機能。

本人が犯すことがない（非登録シンボルを選択）
エラーを検知し不正使用者を強制排除。



3．強要脅迫に強い

・非常通報信号を発信可能。
異常事態シンボルとして登録した写真（イラスト）
を強要脅迫された際、選択することにより可

4．高いセキュリティ強度を容易に実現

・1兆×1兆分の1の強度を高齢者でも実現可能。

$$\frac{1}{2^{80}}$$

パスワード（パスシンボル）の例

幼い頃、桃子ちゃん と
犬のポチ と恵介 とで
ひまわり公園 でサッカー
をしてジュース を飲んで帰
るのが放課後の楽しみだった。

上の例は20億分の1（36の6乗分の1）

パニックにも耐える信頼性と確かな数学的強度

深い愛着のある画像をパスシンボル（暗証画像）としたニーモニックガードは、一般的なモバイル環境はもとより混乱とパニックの危機現場でも確実に使いこなすことができる。

長期記憶イメージをマトリックス上で運用する本人認証技術では、数学的強度を簡単に計算することが可能。

6ｘ6＝36個のマトリックスに埋め込まれた6個の暗証画像の順列を再認する場合では36の6乗の総当りを要求する。（実際には他人推定エラー数ないしエラー総数が設定値に達したところで処理を停止し早期に排除。）

8桁のランダム英数字列と同等の強度が要求される場合には8ｘ8＝64個のマトリックスに埋め込まれた8個の見忘れるはずのない懐かしい画像を再認すればよい

文字パスワードでは机上の空論に終わるような高い強度を、老若を問わない生身の人間が実生活の中で実現する

モバイル環境･野外現場で確実に信頼できるのは、この方式に代表される『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』のみ

ニーモニックガードの2つの運用方法

1. 文字パスワードに換えてニーモニックガードを使う

「ニーモニックガード･WM」、「クリプトニーモ」、「ウェブアクセス版」など

2. 多桁文字パスワードをニーモニックガードで管理運用する

既存のパスワード認証システムに全く手を入れずに済ますことが可能になる。

ニーモニックガードで管理運用される多桁パスワードは覚える必要のないものなので、どんなに無機質で長いものであってもかまわず、また頻繁に変更されてもユーザの負担にならない。

「ＰＣログオン版」、「パスワードロッカー･ウェブ自動ログイン」など

運用では文字パスワードの上位互換

ニーモニック認証画面にイラスト･写真に加えて文字･数字も用意しておく

↓

既存の文字パスワード･暗証番号を吸収

↓

文字パスワード･暗証番号を記憶して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強化手段を追加的に提供可能

同様に、パターン記憶法や単純画像パスワードに対しても上位互換。ニーモニックガードの中でパターン記憶法をその一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。

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全般に対して上位互換となる本人認証技術

注: 多桁パスワードをニーモニックガードで管理運用する方式では、管理される多桁パスワードを例えば100ビット級以上にしておくと、画面･キーボードからの手動攻撃はニーモニックガードが防ぐ一方で総当り自動攻撃は100ビット級という数学的強度で防ぐので、短い桁数の文字パスワード記憶であっても在来の直接入力方式に比べるとより高いセキュリティを実現する。

代表的運用事例

・安全なモバイルビジネスを実現
　　ノートPC・スマートフォンのログオン認証
　　ＵＳＢメモリーのロック機能
　　常態では暗号鍵の存在しない暗号ソフト
・暗証番号・パスワードを手元で管理
　　携帯電話上の暗号化メモ帳
・機密情報の持ち出しを防止
　　権限分散方式による暗号鍵合成
・ネット取引の利用者認証
　　フィッシング排除機能内在ウェブアクセス認証
　　盗聴・盗撮・トロイの木馬の無力化
・制限エリア入室管理
　　非可視画面複合キオスクステーション

モバイルＰＣログオン版　WindowsPCの利用者認証

ＬＭハッシュ保存問題を回避しつつ安全なモバイルコンピューティングを実現するには
３２桁までの難解パスワードを登録しメモに記して安全な場所に保管し
記憶する必要のない管理コードとしてニーモニックガードで運用する

＜　危機現場でも使いこなせるニーモニックガード＞

幼い頃に自分になついていた数匹の犬の写真を照合データ（パスシンボル）とした認証画面の例。たとい数年ぶりの認証でもすぐに判る。

正規ユーザーは…再認したパスシンボルを選択するだけで本人認証完了。本人を推定するエラーは何度でも許容されるのでストレスを感じない。

不正取得者は…
本人であれば犯す筈のないエラー（非登録シンボルのみ選択）を犯すと、例えば２回目で他人断定　→
アクセス拒否＋ID無効化
（＋退路遮断・追跡）

不正アクセスを強要されたユーザーが、懐かしい犬数匹に加えて、異常事態シンボルとして登録していた（例えば故なく吠えられた）犬１匹を選択すると、本人認証した上で（脅迫者に知られること無く）対応

認証画面は４ｘ４～８ｘ８など自由に設定できる
写真以外にイラスト・漢字・英数字も使える
暗証画像（パスシンボル）は「組み合わせ」も「順列」も登録できる

不正取得者は
１．Windows立ち上げの前にニーモニックガードの通過を要求され、他人推定エラー回数あるいは総エラー回数が事前に設定された値に達するとそれ以後の認証作業継続を拒否される。
２．自動プログラムでの総当りを試みることは可能だが、Windowsパスワードとして最大３２桁のランダム英数字記号列を登録してあれば我々の生きている間に破られる確率はゼロに近いといえる。
管理者は
ユーザが突然退職したような場合、管理簿のパスワードを使ってセーフモードでWindowsを立ち上げてニーモニックガードのアンインストールを行い、新たなユーザ用に再インストールを行えばよい。

ニーモニックガードWM　スマートフォンの利用者認証

最も危険な紙媒体の持出を抑制

営業効率向上でコストは短期間で回収

電源投入時
ロック状態解除時
アクティブシンク起動時

→

「ニーモニックガード」
による利用者認証

これまで

不安なモバイル営業のメリット　＜　端末盗難による企業情報流出リスク　＋　導入・運用コスト

「ニーモニックガード・WM（WindowsMobile）」で利用者認証を強化後

安全なモバイル営業のメリット　＞　紙媒体盗難による企業情報流出リスク　＋　導入・運用コスト

パスシンボルロッカー　ＵＳＢメモリーのロック機能

ＣＤ－ＲＯＭ領域･リムーバブル領域･秘匿領域を持つＵＳＢメモリー［ＵＤ－ＲＷ］を使用
ニーモニック認証を通過できない不正取得者はリムーバブル領域にアクセスできない！
ソフトのインストールは不要！

パスシンボルロッカー・セキュア・ストレージ

ＵＳＢメモリーを装着するとニーモニックガードが自動的に起動。ニーモニック認証を通過するとＵＳＢドライブのリムーバビルディスクの領域を見ることができる。

パスシンボルロッカー・ウェブ自動ログイン

ＵＳＢメモリーを装着するとニーモニックガードが自動起動し、通過するとＩＤ／パスワードを登録済みのウェブサイトに自動ログイン。

シンクライアント方式でも本人認証が弱いと情報の流出を防げず、特に改竄の脅威は深刻。本製品を使うと現行のパスワード認証システムに変更を加えることなくセキュリティを大きく向上。

覚える必要のない１００ビット級以上の多桁パスワードを本製品に登録しておくと、端末上での成りすまし攻撃は画面とキーボードを占拠しているニーモニックガードが防ぎ、ネット上での総当り攻撃は１００ビット以上という数学的強度で防ぐ。覚える必要のないパスワードを運用するので頻繁に変更してもユーザの負担はほとんど増えない。

クリプトニーモ　常態では暗号鍵が存在しない暗号化

「如何に強力なデータ暗号化ソフトであっても実運用上の安全性は

利用者認証の安全性と暗号鍵秘匿方法の安全性を上回ることはない」という問題を一挙に解決

暗号キー作成　＞　使用　＞　削除

個人使用の効果

- 機密情報をソフトと一緒に外部メモリーに保管すれば、どこであっても仕事を続行。
- 暗号化ファイルをPCに保存しておけば外部メモリー紛失によるデータ喪失に備え。
- 外部メモリーを閲覧・編集時にのみＰＣに接続すればネット流出リスクを極小化。

グループ使用の効果

- グループメンバーは、それぞれ異なる認証画面・パスシンボルを使いながらも同一の暗号鍵を復元。
- 暗号化ファイルはメール添付或いはFTPでのメンバーへの電送可能。

携帯クリプト手帳　暗証番号・PWを手元で管理

暗証番号やパスワードやなどの秘密個人情報を手帳に書いてしまうと紛失･盗用が心配。

手帳の中身を、クリプトニーモ技術で暗号化すれば安心

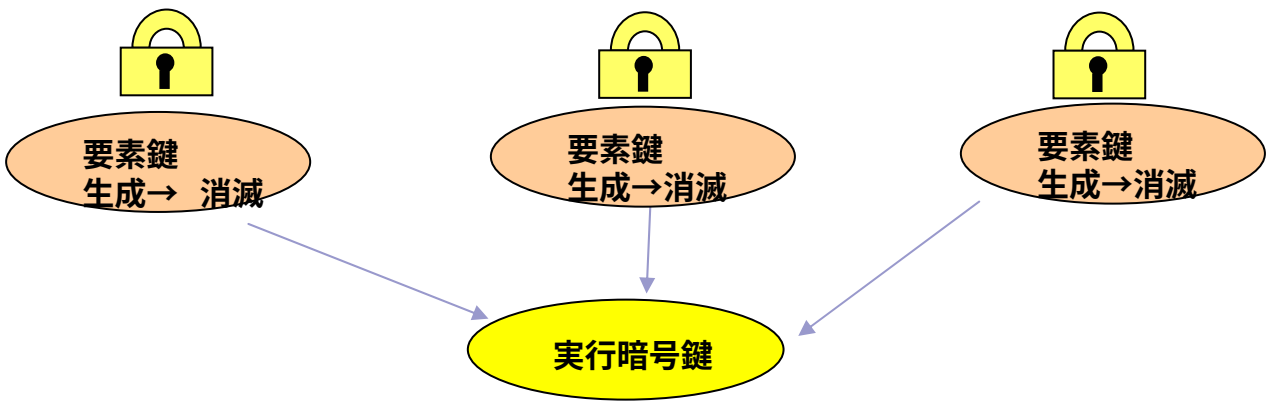
例えば、
１．ＡＴＭに近づく直前に本ソフトを起動しニーモニック認証を通過（動的に生成された暗号鍵により暗号データを復号）

２．表示された暗証番号を視認してＡＴＭを操作（本ソフト終了時に暗号鍵は消滅）

権限分散クリプトニーモ

最高機密データの漏洩防止の決定打

任意のα人中の任意の組み合わせのβ人が共同でクリプトニーモを操作すると
同一の暗号鍵が復元。　作業終了後は実行鍵も要素鍵も全て消滅。
β人が結託して共同作業しない限りデータを復号させ漏洩させることは不可能。



合成　→　暗号化･復号処理に使用　→消滅

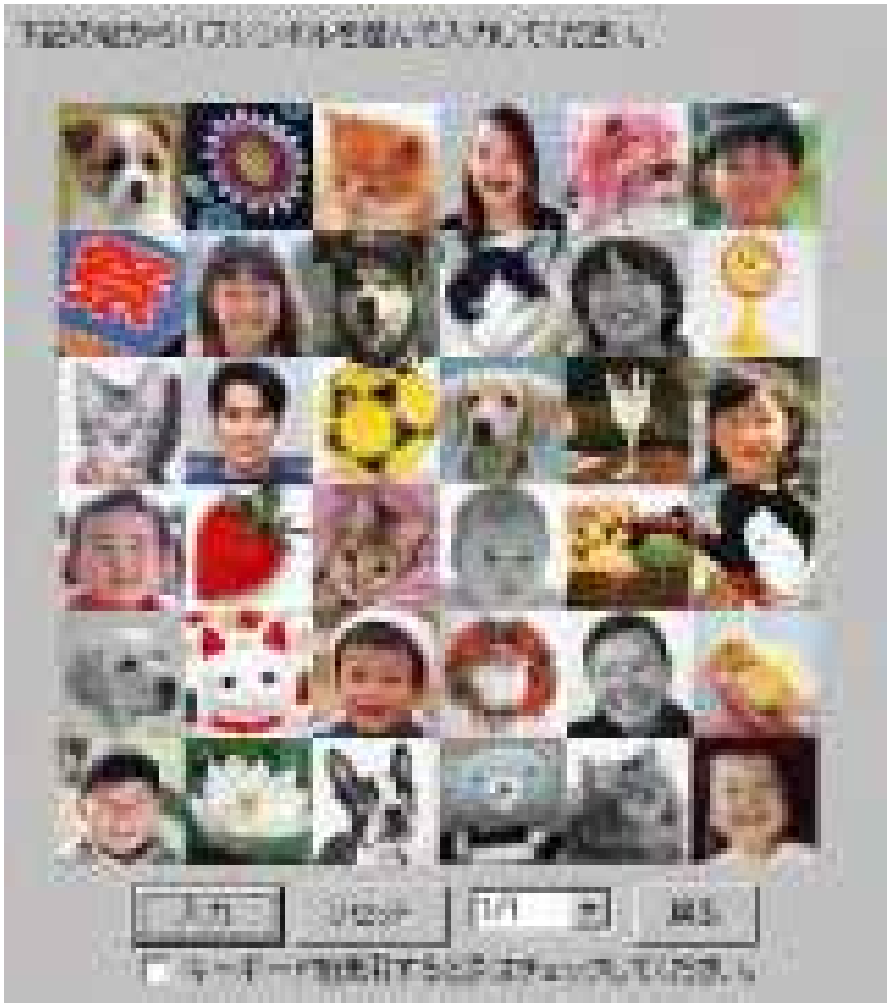
機密情報の管理者を脅威･ストレスから解放。
しっかり人間を守ると、データもしっかり守れる。

ウェブアクセスの利用者認証

1経路1端末のベーシックモデル
ＡＳＰモデルでも運用中

グローバル･シングル･サインオン仕様
「SAML 2.0」の方式と同じ原理です

ニーモニックガードのフィッシング排除機能



認証画面が個人別に違うので、一律の偽画面が作れない

偽サーバは認証データを盗むことができない

多数の認証画面を事前に用意するのは不可能ではないが費用対効果が著しく悪く、経済犯的なフィッシング犯はニーモニックガード認証に手を出せない

この偽サーバ排除機能はニーモニックガードに内在されており、
追加コストは発生しない

2経路2端末 ワンタイム･ニーモニックガード

携帯電話に表示される認証画面からワンタイム暗証番号を生成
盗聴･盗撮･フィッシング･スパイウエアを無力化

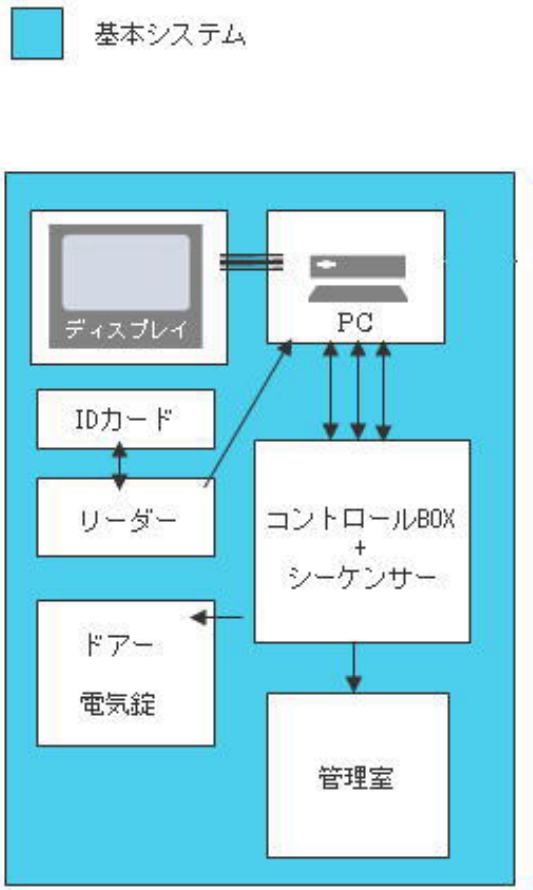
在来のワンタイム製品が窃取を防いでいるのは『デバイス認証』情報
2経路2端末ニーモニックガードで『本人認証』情報のワンタイム化を実現

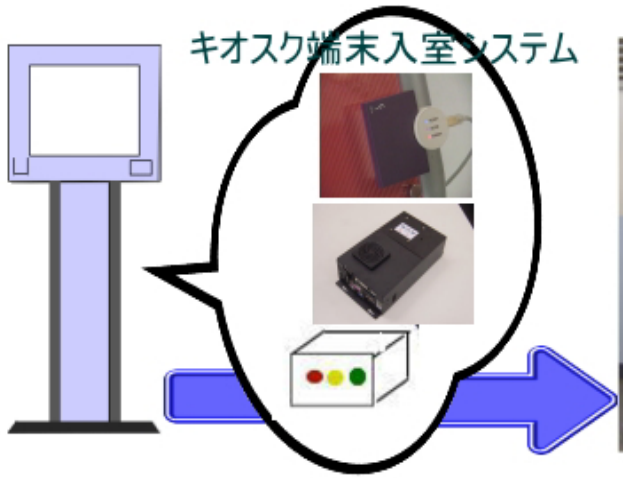
携帯電話に表示される認証画像の一つ一つに異なる英数字がランダムに割り振られる
→ パスシンボル（正解の暗証画像）は毎回異なる英数字列で表現される
＝ ＰＣから入力されるワンタイム英数字列はユーザの記憶を含む本人認証情報

ＡＴＭ、ＰＩＮ対応クレジットカード支払端末、入室管理への応用も可能

制限エリアの入退室管理

非常事態通報シンボルを使って気付かれずに共連れに対応
他人断定時には退路を断つなど果断に対処





17インチ液晶変更可能

業務用PC+コントローラ設置例

モバイル・社内システム・物理的警備の全てを同じロジックとユーザインタフェースで

開発中の応用製品

- **個人機微情報の匿名管理システム**

  IPAの受託開発としてプロトタイプを開発した個人特定情報と個人機微情報との分割管理及びネットワーク上でのIPアドレス秘匿

- **個人狙い撃ちフィッシングも排除する多段階相互認証**

  TAO（現NICT）の助成を得てプロトタイプを開発した
  多段階相互認証システム。

- **電子債権の安全な流通を実現するファイル電送システム**

  クリプトニーモ＋ による秘密鍵の厳重管理を用いた、公開鍵暗号方式ベースのファイル伝送システム

- **本人認証専用携帯デバイス**

  信頼性のない端末からでも安全にアクセスできる本人認証専用の携帯デバイス

長期イメージ記憶と情報セキュリティ

資料編

株式会社ニーモニックセキュリティ
代表取締役　國米　仁

本人認証： 過去の認識

過去の認識： 本人認証には
「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。

その背景： 本人確認・個人識別・本人認証についての明確な区別・定義が不在。 当人の意思の有無確認についての問題意識が欠如。

その影響： 個人識別＝本人認証といった不正確な認識の蔓延。

対面交渉が主流であった時代ではこうした認識でも実践上は特に不都合はなかったが、モバイル環境を統合するネットワーク社会では正しい認識が不可欠となる。

本人認証： 我々の認識

我々の認識： 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つの範疇から成り立っている。それぞれ実現するための技術要件は異なる。

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る。

本人認証： 権利義務の主体確定のプロセス。意思確認必須。記憶の照合による。

- 所持物や身体の特徴点の照合は、当人の否認（それは俺ではない）を他者が否定するには有効。しかし、当人の主張（それは俺だ）を他者が肯定するには無効（例えば替玉自首を許してしまう）。

- 記憶の照合は、当人の否認（それは俺ではない）を他者が否定するには無効。しかし、当人の主張（それは俺だ）を他者が肯定するには有効（当人しか知り得ない事実を知っている）。

被疑者と自首者

【本人確認】＝【個人識別】＋【本人認証】

誰か？

①「やったのは俺ではない。」

（主張を突き崩すには）

②「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！」

【個人識別】

意思確認不要。所持物の照合や身体の特徴点の照合による。

当事者か？

①「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。」

（身代わり自首を許さないためには）

③「お前はやったというが、当事者なら知っている筈のことを知らないではないか！」

【本人認証】

意思確認必須。記憶の照合による。

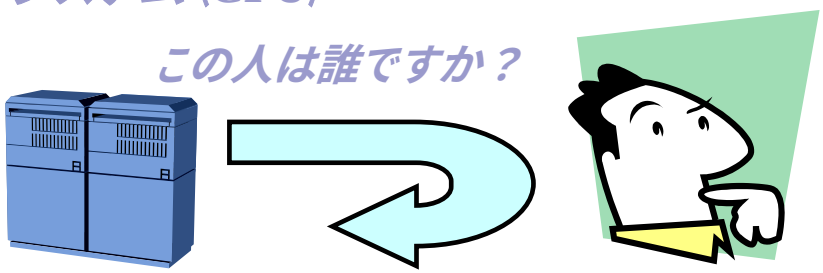
本人確認における「識別」と「認証」

【個人識別】

Who is this person ?

この人は誰ですか？

システム（CPU）



『確率90％で田中さんです』　で良い

確率

本人の意志・意識の確認不要

＜適切な適用分野＞

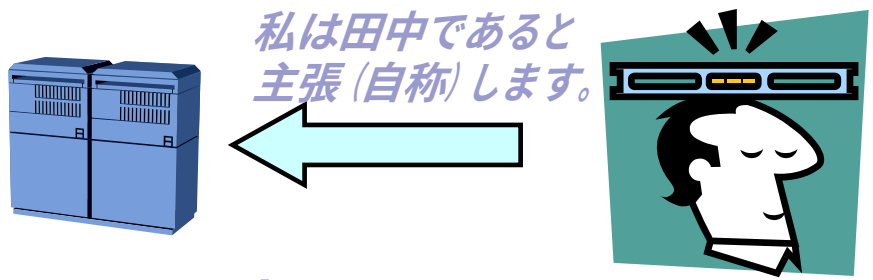
警備、鑑識、捜査 等

【本人認証】

Is he/she the person who claims to be ?

本人だと主張（自称）している彼/彼女は真に本人ですか？

システム（CPU）　　頭脳（意思・意識）



『YES / NO』　しかない

真・偽

本人の意志・意識の確認必須！

＜適切な適用分野＞

権利・義務の主体の確定に関わる分野

在来の本人認証方式－１

文字パスワード　(照合するデータは秘密情報　＝　有効な本人認証)

覚え易いものは盗まれ易く、盗まれ難いものは思い出せない。
厳格管理は隠れメモ依存を引き起こす。特にモバイル環境では不安。

パターン記憶法　(照合するデータは一応は秘密情報)

パターンに従って選択される乱数列（2次データ）はいくらでも強くできるが、誰にでも記憶できるものでありながら攻撃者には思いつかないパターン（1次データ）は多くないので高いセキュリティの実現は困難。

所持物照合　(照合データは秘密情報ではない)

誰の手中にあるかを語らない　＝　盗用には効力ゼロ。
「不所持 vs 付けっ放し」のジレンマもあり。　特にモバイル環境では不安。

生体計測技術　(照合データは秘密情報ではない)

本人拒否がゼロでない限り、本人拒否の救済策が必要。
（深刻な優良誤認問題が存在。参考情報として後述。）

在来の本人認証方式－２

記憶照合、所持物照合、生体計測技術　の組合せ

ＡＮＤ型組合せ
　長所の足し算と同時に短所の足し算も行われる
　weak + weak = less weak　(strongではない)
ＯＲ型組合せ
　個々の要素の脆弱性の総和が全体の脆弱性となる

注：　ＰＫＩ(公開鍵基盤)・使い捨て乱数発生方式などは秘密鍵ないし乱数をユーザ自身が記憶するか頭脳で生成するのでない限り、デバイスの真正性の認証方法であって直接的には本人認証技術ではない。

モバイル端末に遠隔停止機能があれば利用者認証不要との議論があるがキャッシュカード・クレジットカードには昔から遠隔停止機能が付随していても暗証番号不要論などは出ていない。

「扉」の強化は「鍵」の強化の代替にはならない。

大転換期を迎えた本人認証手段

数千年のアナログ時代の本人確認を支えてきた伝統的手段

伝統的文明社会：

印章、署名、花押

身元を保証する証明書　(勘合割符、関所手形)、

＋

本人なら知っているはずの情報の対面での共有確認

これらの伝統的手段･方法はデジタル･ネット社会では効力を喪失

デジタルコピー技術の登場：　署名も印影も容易に複製可能

対面確認不能：　相手が隣にいるのか地球の裏側にいるのか判らない

速度の要求：　瞬時に、自動的に判定する必要

モバイル環境の登場：　本人排除時に誰にも頼れない環境

恒久的な安全性を維持できる電子的本人認証手段の確立が急務

大転換期に登場すべき本人認証

電子的本人確認手段は時と場所を選ばない無制限の脅威に曝され続ける。従って、本人認証システムには、最先端のIT知識と悪知恵に長けた頭脳集団の執拗な組織的攻撃にも耐える強靭さが必要。

どんなに頭の良い攻撃者がいかに手の込んだ攻撃方法を考え出しても、個々人それぞれが長い人生の中で蓄積してきたその人固有の記憶をその人の**主観的な文脈通り**に取り出すことはできない。本人であれば簡単に主観的な文脈通りに取り出せる秘密情報、それは過去の懐かしい記憶。こうした過去の懐かしい記憶をイメージとして活用することで、人格の尊厳を損なうことなくストレスのない安心で確実な本人認証を実現することができる。

この長期視覚記憶を活用する本人認証技術は、文字パスワードが果たすものと期待されていながら果たしきれなかった秘密情報の確実な照合を、最新のデジタル技術によって果たすもので、文字パスワードの正統な後継技術とみなせるもの。

本人認証の法理

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。

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。

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かない。

虚構に侵される情報セキュリティ

「パスワードは8桁以上、出来れば１２桁のランダムな大文字小文字混じり英数字とすること」、「出来れば特殊文字･記号も用いること」、「アカウント毎に異なるものにすること」、「数ヵ月毎に変更すること」。

次に、「こうした難解パスワードを使う場合アカウント数が増えると手帳に頼らざるを得なくなるが、手帳の管理には十分に注意をすること」ならば理解可能で現世のこと。

ところが、「どんなにアカウント数が増えても手帳での管理は禁止。」になると、「老若を問わず自分の足だけで１００Ｍを１２秒で進むこと」と同じようなもので、この世のことではない。しかし、何故か情報セキュリティの世界に入る者はこの虚構を疑わず受け入れることを要求される。

情報セキュリティを学ぶ第一歩で虚構を受け入れることが当然のことになってしまうと、後からどんな虚構が出てきても抵抗無く受け入れることになり、優良誤認の横行が黙認されてしまうことになる。

セキュリティ製品の優良誤認問題

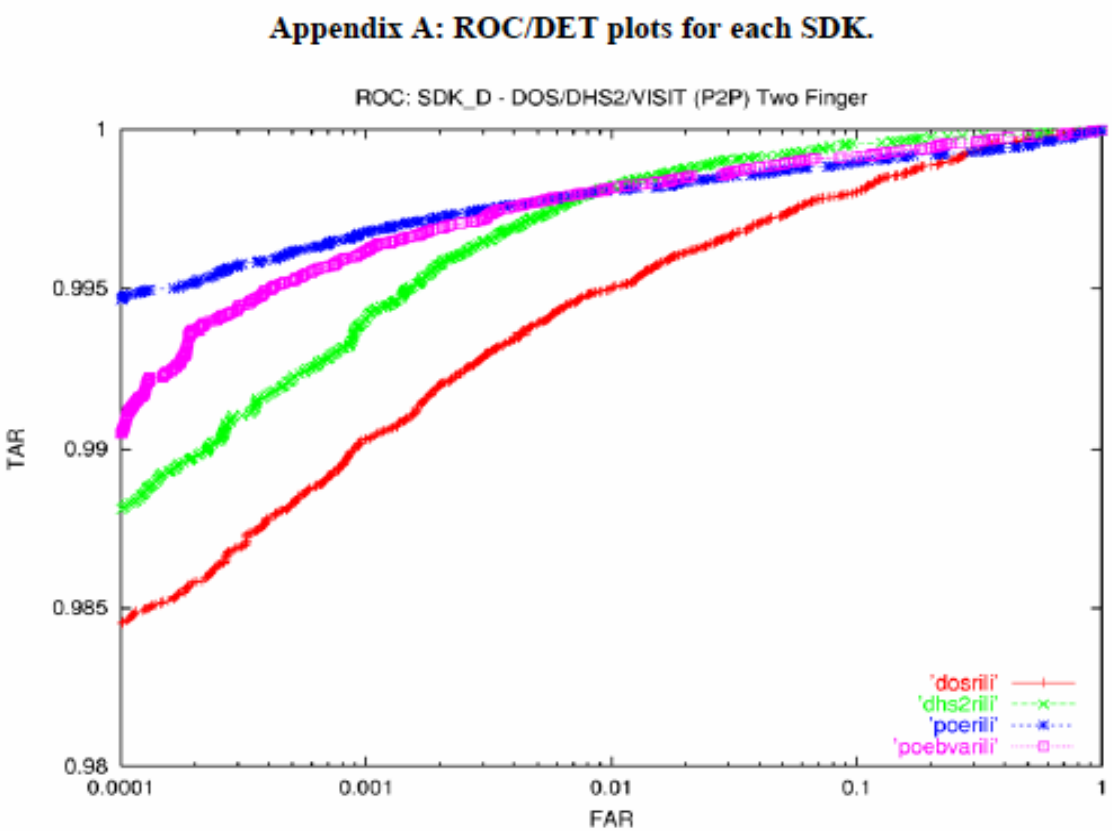
2007年6月16日に情報セキュリティ大学院大学で行われた日本セキュリティ・マネジメント学会（ＪＳＳＭ　http://www.jssm.net ）第21回全国大会で、学会有志による論文『本人を認証する製品の優良誤認を防ぐための提言』が発表された。

著者は

日本セキュアテック研究所	鵜野　幸一郎　氏
アットマーク・ベンチャー	原岡　望　氏
ＮＥＣ	力　利則　氏

主に、生体認証製品とワンタイムパスワード発生トークンがとりあげられている。

生体認証の特性



メキシコからの入国者の指紋データを使ったと言われる米国商務省NISTの指紋認証製品評価資料（ http://fpvte.nist.gov ）から

指2本登録のケースだが、本人通過率100%（本人拒否率0%）の時は全てのデータにおいて他人通過率100%（他人拒否率0%）。

最良のデータにおいて他人受容率0.01%の時の本人通過率99.4%で、本人通過率99.9%の時の他人受容率1%となっている。

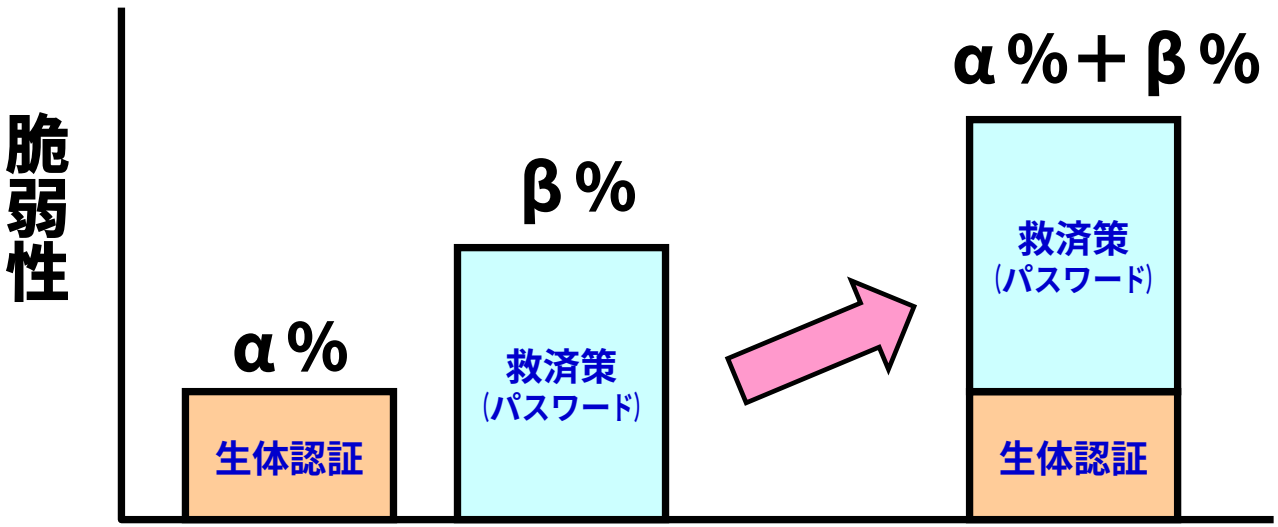
日ごろカタログ等で見かける数値とはかなり異なっている。

本人拒否ゼロ（＝他人排除ゼロ）で運用しない限りは、本人拒否救済策が不可欠。

救済用パスワードを併用する生体認証

生体認証･パスワード双方の脆弱性の合算値が全体の脆弱性（他人受容の確率）となる。

生体認証の脆弱性をα％としパスワードの脆弱性をβ％とすると、全体の脆弱性は（α＋β）％、つまりパスワードの脆弱性をβ％のままとすると、パスワード単独の脆弱性よりも大きくなる。



論文が提言する生体認証製品に関る判断基準

表示レベル	救済用パスワード併用生体認証の事例	生体照合装置の精度値の事例
A．適正表示	救済用パスワード併用生体認証では、従来と同じパスワードの管理ではセキュリティ強度が弱くなることを表記する。「パスワードによるロック状態を指紋認証で解除することができます。（注意：パスワード管理を厳密にしないとセキュリティ強度は低下します）」	第三者機関の計測値の表記。 （例）本人拒否率　0.08%、そのときの他人受容率0.01%　指紋両手4指　米国商務省NISTの2005年調査） （準適正表示）自社基準での計測データ・計測前提条件を明記し、本人拒否率と対（つい）の他人受容率を表記
B-1．不親切表示 （止むを得ない不親切表示）	指紋認証あるいはパスワードによってロック状態を解除することができます。	他人受容率は表示する。本人拒否率は他社も出していないので競争上表記しない。
B-2．不親切表示 （努力不足の不親切表示）	指紋認証ならびに従来と同じパスワードによってロック状態を解除することができます。	本人拒否率、他人受容率ともに表記しない。あるいはどこかで行った結果をそのまま基準に当てはめる。
C-1．優良誤認表示 （無知・不注意による過剰表示）	「セキュリティ」「安全性」の高い指紋認証、ならびにパスワードによるロック状態の解除ができます。	自社基準での計測結果のみ表記。（ユーザの実稼動における本人拒否率／他人受容率との大幅乖離が常態）、（例）他人許容率が0.00001%以下の時の本人拒否率は、0.08%以下
C-2．優良誤認表示 （故意の不実／誇張表示）	指紋認証が加わったのでパスワードだけの他の製品よりも格段に高いセキュリティです。	自社基準の計測データの不完全表記、他社基準の発表値借用。（例）・他人許容率が0.00001%以下だけ表示して対（つい）の本人拒否率の値を表示しない。・『何億分の1』と指写真を大写しして、おおげさな指紋照合の精度のイメージを植えつけるもの

デバイスが生成するワンタイムパスワード

たとえ盗んでも数分後には無効！

① 世間の認識

固定パスワードの限界を破るもの

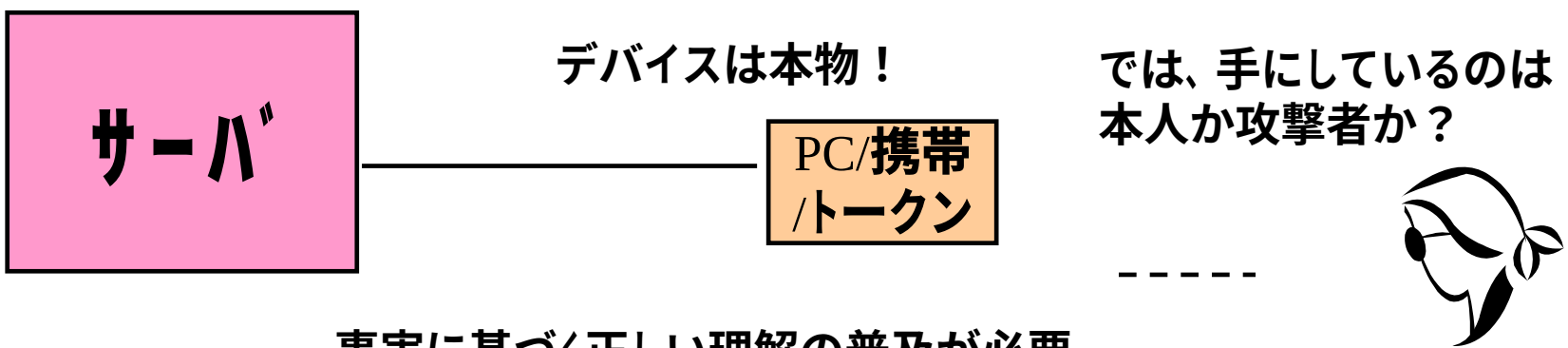
固定パスワードの上位技術

② 事実

乱数を発生したデバイスが本物であると証明しているだけ

デバイスが今誰の手中にあるかは語らない

現在そのワンタイムパスワード生成器を使っているのが正規の所有者であるかどうかを確認するための手段が別途必要



事実に基づく正しい理解の普及が必要

論文の提言する対策

- 一般ユーザがセキュリティ技術の複雑さとの内容を理解することの難しさ
- 製造･販売･サービス供給者が競争上の劣位を避けようとする
- メディアによって優良誤認を招く情報の再生産が行われている（こだま効果）

⇒啓蒙活動が必要

- 専門家･提供側の故意･不作為による優良誤認を招く情報発信もある

⇒（何らかの）社会的制裁が必要

優良誤認表示や不親切表示を排除して
セキュリティ技術の適正な表示を推進する

IPA ガイドライン

２００７年７月に（独）情報処理推進機構が『生体認証導入・運用のためのガイドライン』を発行した。

http://www.ipa.go.jp/security/fy18/reports/bio_sec/index.html

先述の生体認証に関わる優良誤認に関連するものとしては、「生体認証において、どのように閾値を定めても、誤って他人を受け入れる可能性を０にし、かつ誤って本人を拒否する可能性を０とすることはできない。」との記述があり、この記述を受けて本人拒否時における代替手段について留意すべきことが各所で言及されている。

（但し、代替手段としてパスワードが使用されながらパスワードを上回るセキュリティを提供しているかの如き印象を消費者に与えている製品が実際に市場に出回っている現実についての言及はない。）

本人認証製品　3つのカテゴリー

一口に本人認証製品といっても一種類ではなく、
大別して次の3つのカテゴリーが存在

A　利便性を志向する技術と運用
セキュリティ低下を伴うことが多い

B　心理的満足を志向する技術と運用
セキュリティも利便性も向上しない

C　セキュリティを志向する製品と運用
利便性低下を伴わない方法もある

A. 利便性志向製品

1． 救済パスワードを併用する生体認証

パスワードによるロック状態を生体認証で解除できる

生体認証の本人拒否時にはパスワードで解除できる

所有者のみならず不正アクセス者も共に、パスワードでも認証でき、また生体認証でも認証できる。つまり、パスワードの脆弱性と生体認証の脆弱性の総和が全体の脆弱性となる。 ＝ セキュリティはパスワード単独よりも低くならざるを得ない。

2． 閾値を大きく下げて本人拒否が起こらなくした生体認証

他人受容率は急上昇せざるを得ない ＝ 高いセキュリティは謳えない。

3．所定の所持物を保持している人を本人と見なす所持物照合

ICカード・USBキー・携帯電話の紛失・置忘れのない人達には便利な方法。

B. 心理的満足志向製品

１．バイパスボタン付加方式

Ａ．「○○ボタンを押すとＸＸ認証操作をしなくても暗証番号入力画面が表示されます。 」

知識のない不正取得者に対してはセキュリティは向上しているが、所有者と同じレベルの知識を持つ不正取得者に対してはセキュリティが暗証番号単独を上回ることはない。利便性の向上はない。

Ｂ．「ＸＸ認証を通過できない場合には○○ボタンを押して所定のキー　ワードを入力すると暗証番号入力画面が表示されます。」

暗証番号単独よりもセキュリティは向上しているが、キーワードＡＮＤ暗証番号方式を基準にすると、それよりもセキュリティは低下している。利便性の向上はない。

２．パターン記憶による乱数表選択方式　（後述）

３．使い捨て乱数発生デバイス利用方式　（後述）

C. セキュリティ志向製品

1. 救済用パスワードを併用せず且つ高い閾値のまま運用する生体認証

拒否時は利用者が一切の不利益を蒙らないシステムの存在が前提となる。管理者の監視や衆人の環視が保証された環境でない限り、本人の積極的な意思確認を必要とする分野での使用は不適切。

2. 長期記憶認証 (ニーモニックガードなど)

あらゆる環境で高いセキュリティを実現できる。しかし、セキュリティを欲しないユーザまでは守れないので、セキュリティ向上の動機を持たない利用者に対する管理者側での教育的或いは強制的な管理対策が必要な場合もある。

補足情報

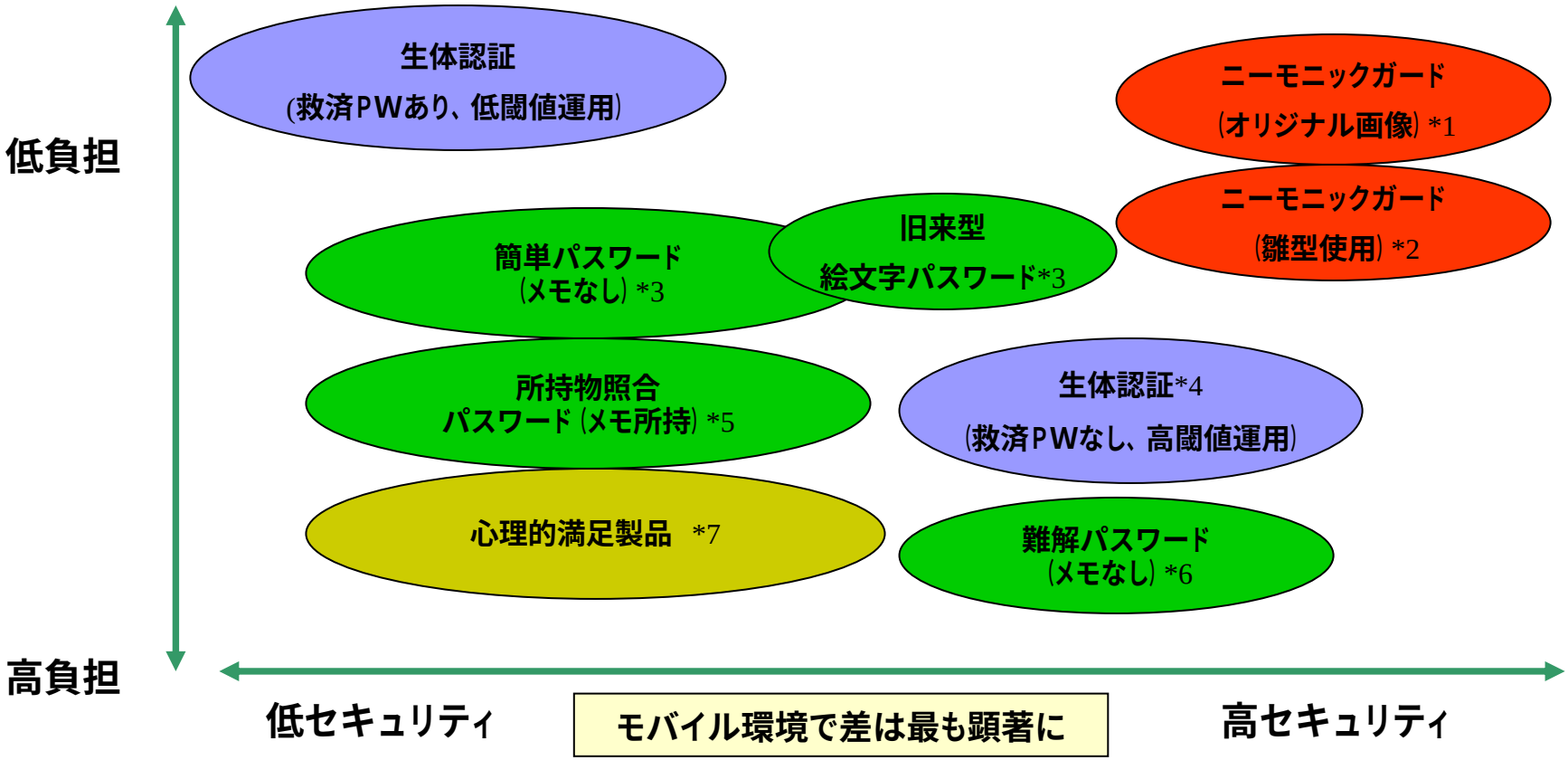
パターン記憶法： 誰にも覚えられるが攻撃者には思いつかないパターンが多数は存在しないので有効性は疑わしい。

使い捨て乱数発生デバイス： デバイスが発生する使い捨て乱数が証明しているのはデバイスが本物であるかどうかであって、それ以上ではない。所持物認証の補強手段であって本人認証手段ではなく、セキュリティを志向するならばデバイスの所有者認証が必要。

異種認証手法の組み合わせ： ＡＮＤ併用では他人排除率だけでなく本人排除・拒否率も上昇し、ＯＲ併用では個々の要素の脆弱性の総和が全体の脆弱性となり、有効性の証明不能。

データ暗号化ソフト： 暗号化はデータ防衛に有効。しかし、運用上の強度は利用者認証の強度及び暗号鍵の秘匿強度を上回ることがないことに留意する必要あり。（常態では暗号鍵を存在させずニーモニック認証によって動的に暗号鍵を復元する「**クリプトニーモ**」はこの問題に対応したもの。）

相対比較図　＃１（セキュリティとユーザの負担：　運用時）



＊１：　懐かしい画像を見つけるだけ

＊２：　体験ストーリーに添って思い出すだけ

＊３：　記憶保持･想起に小さな努力必要

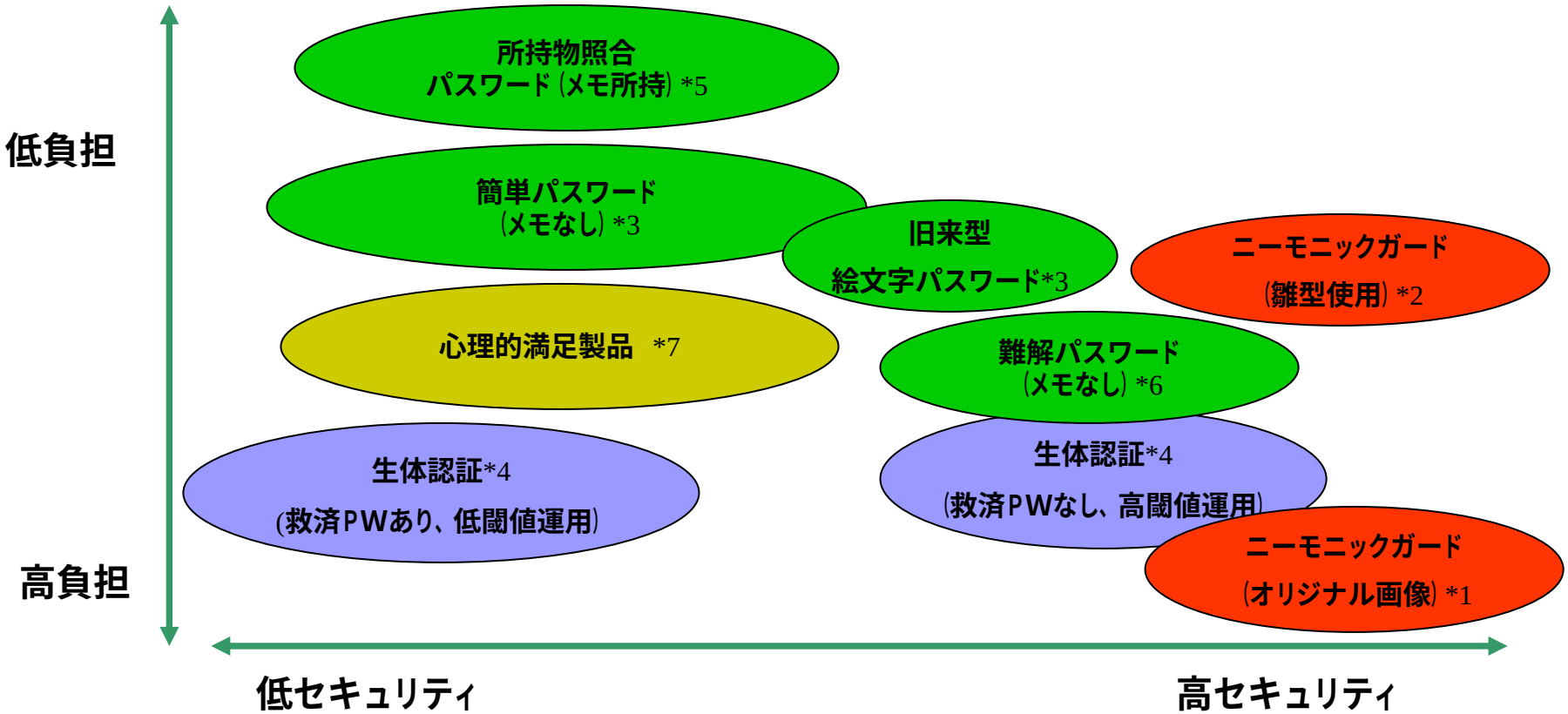
＊４：　本人拒否時業務不能予測ストレス

＊５：　常時保持の努力必要

＊６：　記憶保持･想起に大きな努力必要

＊７：　P44参照

相対比較図　＃２（セキュリティとユーザの負担：　初期設定・登録時）



＊１：　オリジナル画像の準備・登録が必要
（但し、準備過程は第三者に委託可能）

＊２：　体験ストーリーによる登録が必要

＊３：　設定・登録の負担は最小

＊４：　登録の手順が必要

＊５：　ユーザによる登録・設定は不要

＊６：　記憶形成・定着の負担

＊７：　P44参照