ニーモニックガード

確実な本人認証なくして
機密情報漏洩・改竄の抑止なし

株式会社　ニーモニックセキュリティ
代表取締役　國米　仁

2004/5/21

確実な本人認証なくして
セキュリティソリューションなし

完璧に暗号化されたデータも正規ユーザ（＝なりすまし成功者）の前には平文で掲示される

広域に分散されたデータも正規ユーザ（＝なりすまし成功者）の前には集約されて掲示される

VPNも専用線も端末の前に誰が座っているかを語らない

実は大昔からの鉄則　－　高い壁と深い濠に護られていても「城の者じゃ」の一言で敵兵が表門から出入りできる城砦の運命や如何に

続出する個人情報大量漏洩　1/2

どんなに高度な技術をいくら導入しても内部関係者による確信犯的データ持ち出しの完全防止は不可能。

顧客の個人情報を蓄積している企業は全て漏洩リスクを抱えている。

これまで発生していないところも今日明日にでも発生しても全く不思議ではない。

経営問題であると気がついている少数の経営者は眠られぬ夜を過ごし、技術問題であると誤解してシステム管理責任者に丸投げしている経営者は気がついていないだけで実は時限爆弾の上で寝ている。

社外からのリモートアクセスを許している企業では特に流出リスクが高い。

個々の企業が抑止とリスク最小化の対応策を取る以外にはない。
最大の鍵は有権限者の身元を同僚や他人に盗用されないための確実なユーザ認証技術導入。

続出する個人情報大量漏洩　2/2

完全防止は不可能でも抑止努力と被害極小化努力は可能であり必要。

信頼に足る本人認証技術を導入すれば大きな抑止効果が期待でき、また最良最善の抑止努力をしていたという事実によって流出時の被害の最小化を図ることができる。

建前だけの本人認証しか行なっていない現状を放置したままで顧客情報の流出が発生した時には天井知らずの損害賠償を要求される可能性がある。

電子的な本人確認には、“記憶を照合するもの”、“肉体の特徴点を照合するもの”、“所持物を照合するもの”に大別されそれぞれ多くの選択肢があるが、**「いつでも、どこでも、老若を問わず誰でも、本人を排除することなく他人のみを有効に排除できるか否か」**という判断軸に則って「汎用的な実用性あり」と判断できるのはニーモニックガードのみ。しかも低コスト。

ニーモニックガードはネットワーク社会のアキレス腱防衛に貢献する。

ニーモニックガード

いつでも、どこでも、老若男女の誰でも

たといパニック状態になっても

ストレスを感じることなく

人格の尊厳を損うことなく

確実に自分が自分であると意思的に証明する

長期視覚記憶を活用するユーザ本人認証技術

2004/5/21

株式会社ニーモニックセキュリティ

事業分野

情報セキュリティ、個人認証

事業理念

技術の人間的・社会的側面を重視し

全ての市民がストレスを感じることなく

人格の尊厳を損なうことなく

自己のアイデンティティを電子社会で

確実に証明する個人認証技術を世界に提供する

2004/5/21

株式会社ニーモニックセキュリティ

産学連携

今井秀樹東京大学教授（経済産業省・総務省共管「電子政府実現のための暗号技術検討会 CRYPTREC」座長）：万人向け個人認証技術として認知・支援

公的助成

プロジェクト6件、計1.3億円

(今井教授の推薦或いは共同事業)

セキュリティ崩壊に陥り難い
ニーモニックガード

忘れるはずのない愛着のあるシンボルを照合データとして囮のシンボルに混在させる

表示例は子供の頃自宅で、隣人宅で、親戚宅で自分になついていた犬（或いは同種の犬）の写真数枚を照合データ（パスシンボル）としたもの

正規ユーザーは…

なついていた犬数匹を再認して選択するだけで個人認証完了

本人を推定するエラーは何度でも許容される

セキュリティ崩壊に陥り難い
ニーモニックガード

不正使用者は…

総当りを試みる
→
非登録シンボルのみの選択
→
自動他人判定
→
管理者通報・操作不能

不正アクセスを強要されたユーザーは…
認証シンボル　＋
異常事態シンボル
→
認証した上で（脅迫者に知られることなく）異常事態対応（囮データへの誘導、管理者への通報、etc.）

Mnemonic Guard

overcome security paradox

20年程昔に撮った孫娘の写真数枚を照合データ（パスシンボル）とした高齢者用認証画面の例

パニック状態でも確実に認証可能。

昔のものだから他人には類推困難。

Mnemonic Guard

overcome security paradox

小画面では見やすくする為にポイントされているシンボルを拡大する

全ての製品に認証画面自作支援ソフトを無償でバンドル

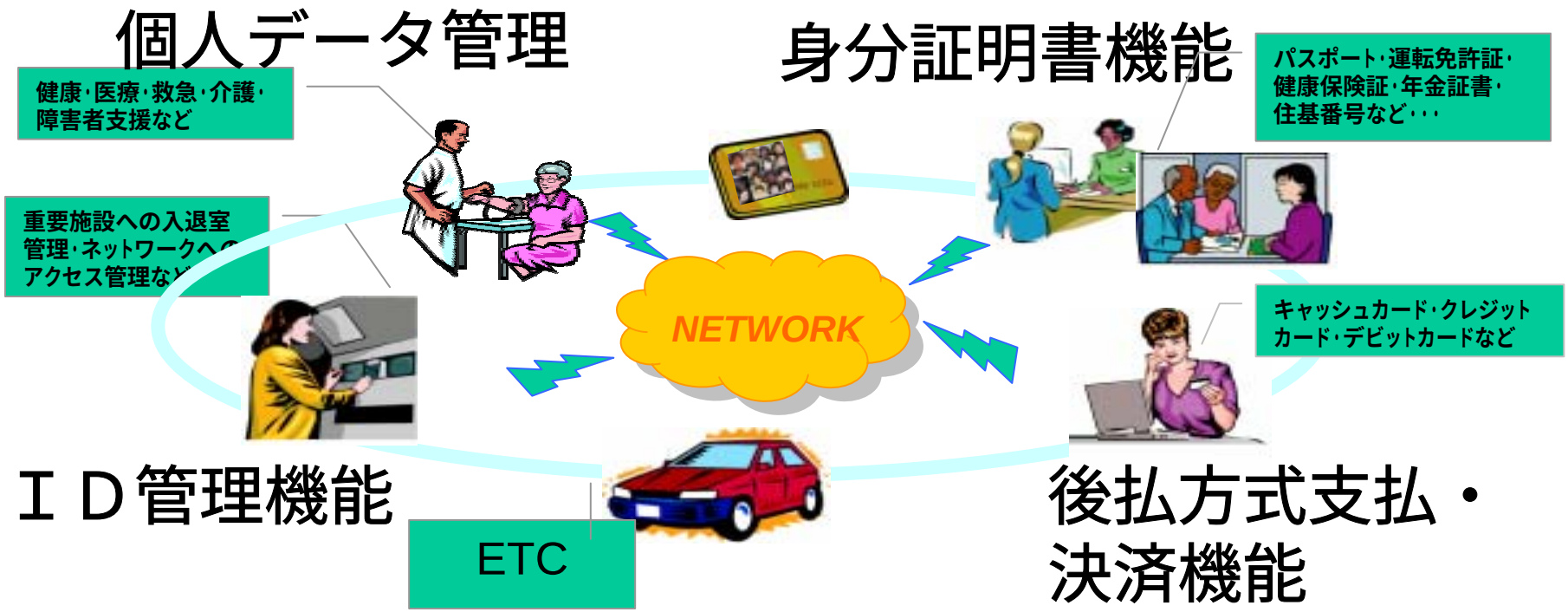
自作困難なユーザには作成代行サービスを提供

音声入力ニーモニックガード

シンボルはランダム表示･数字列は固定表示

たとえシンボルの一つが異常事態通報用であっても脅迫者には知り得ない

ニーモニックガード搭載多機能ICカード
紛失･盗難にも安心



その他、盗用･データ漏洩の不安解消に伴う新規活用分野全般

いずれは、老若男女全ての市民が所持する電子証明書の携帯媒体としてe-Japan実現に貢献

2004/5/21

ニーモニックガードの優位性　1/3

高い数学的強度を実現できるか？

在来型パスワード	X～△
生体照合・所持物照合	X～△・評価不能
ニーモニックガード	○

ニーモニックガードの優位性　2/3

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	**X**
生体照合・所持物照合	**X**
ニーモニックガード	**○**

ニーモニックガードの優位性　3/3

コスト（導入費用＋運用費用）は十分に妥当か？

在来型パスワード	△
生体照合・所持物照合	X
ニーモニックガード	○

製品紹介　1/2
販売中

ログオン認証

PC・PDA

単独使用・LAN接続

ウェブアクセス認証

PC・携帯電話

ライブラリソフト

各種アプリ組込み

製品紹介　2/2
開発中・計画中

盗用防止記録媒体

USBメモリー・SDカード

音声入力製品

カーナビ・ウェアラブル・手指障害

携帯情報金庫

携帯電話・PDA

海外市場向け製品

英語・中国語

IT社会におけるニーモニック認証

たかがパスワードの代替か？
IT社会を支える基幹技術か？

ＩＴ社会はセキュリティがなければ絵に描いた餅

確実な本人確認なくしてセキュリティなし

信頼できる電子的本人確認技術なくしてＩＴ社会の繁栄なし

↓

ニーモニック認証はセキュリティ関連技術の結節点

多くの複合化・アライアンス事業が進行中

広範なアライアンス事業

- 個人情報の保護・活用両立情報通信基盤
- ユーザ・システム相互認証システム
- 携帯情報金庫ＡＳＰ事業
- 多機能ICカード
- 音声入力によるユビキタス対応
- 国際事業「Object Management Group C4I」

実例モデルのご紹介　1/2

社内ネットワークへのログオン管理
Ｍ社（不動産）、ＮＤ社（保険）

社外からのリモートアクセス管理
ＮＤ社（保険）、Ｆ社（ERPソフト）

携帯電話決済アプリのログオン管理
ＮＳ社（クレジット）

一般ユーザからのリモートアクセス管理
ＮＣ社（通信・ＩＳＰ）

実例モデルのご紹介　2/2

ＰＣアプリケーションのログオン
　Ｐ社・Ｓ１社・Ｉ社・Ｖ社・Ｔ社・Ｓ２社
　　（暗号・通信・画像・文書）

警備システム組込み
　ＳＫＲテクノロジー：ＴＶ東京ワールドビジネスサテライト・NHK-BS1経済最前線で紹介

ヘルスケア推進コンソーシアム組込み
　　8社参加NEDOプロジェクトの一環として実証実験準備中。

事業形態

企業向け製品

Sier・代理店への卸販売

個人向け製品

オンライン販売

組込み用ライブラリ製品

ソフトウェアベンダーへの卸販売

複合製品

パートナーからの販売

ASP事業

パートナーとの共同事業

普及見通し

２００４年9月期	売上目標
２０万ユーザ	1.2億円
２００５年9月期	
２００万ユーザ	６億円
２００６年9月期	
１０００万ユーザ	２０億円
２００７年9月期	
３０００万ユーザ	３４億円

会社概要

■会社名	株式会社 ニーモニック セキュリティ (　Mnemonic Security, inc.　)
■所在地	大阪市北区曽根崎2丁目16番19号 りそな梅田ビル7階 〒530-0057　Tel : 06-6361-5311 Fax : 06-6315-5271 Mail : sales@mneme.co.jp
■主な事業内容	個人認証用ソフトウェアの開発、販売
■設立	1995年11月９日
■資本金	1,000万円（2003年9月12日現在・増資予定）
■決算期	9月30日（年1回）
■役員	代表取締役　　國米　仁 取　締　役　　桝野　隆平
■取引銀行	三井住友銀行梅田支店　りそな銀行梅田支店
■加盟団体	大阪商工会議所 モバイルコンピューティング推進コンソーシアム ホームアイランズセキュリティ協議会 e4c-village協議会
■URL	http://www.mneme.co.jp

資料

本人認証技術　比較表

	認証技術 ＼ 比較項目	他人排除力	本人を排除せずに他人のみを排除するか（最重要項目）	導入コスト	運用コスト	課題／特長
1	文字パスワード 暗証番号	×　△ 簡単に覚えられるものは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、本人も排除	◎	△	他人排除を重視すると、質問対応・再発行コスト上昇
2	生体照合	△　○ 指紋など複製可能なものは他人排除力に欠ける	× 原理的に本人拒否を伴う	×	×	パスワードAND併用は、もし有効であれば他人排除率とともに本人排除率も上昇させる
3	所持物照合	△　○ 盗用に対して無力	× 紛失、置忘れVSつけっぱなしのジレンマ	×	×	パスワードAND併用は、もし有効であれば他人排除率とともに本人排除率も上昇させる
4	生体・所持物照合 （パスワードOR 併用）	×　△ 救済用パスワードは最も脆弱で他人排除力を崩壊させる	×	×	×	異種複合化は短所の組合せになる
5	画像パスワード パターン記憶法	△　○	△　○	○	△	他人排除を重視すると質問対応・再発行コスト上昇
6	ニーモニックガード	○　◎	○　◎	○	○	いつでも、どんな場所でも、どんな環境でも、たとえパニック状態でも、誰にでも実行可能

評価マーク	×：気休めにもならない	△：気休め程度	○：実用性あり	◎：使いやすくセキュリティ強度も高い
コストマーク	×：コストが高い	△：コストがやや高い	○：コストが低い	◎：コストがきわめて低い

2004/5/21

更に詳しく 比較項目 / 認証技術		数学的強度 (ユーザの名前・身元を知られている環境)	備考
1	文字パスワード 暗証番号	覚えられる本人関連文字情報　2～5ビット相当 メモされた4～32桁文字情報　0～3ビット相当	・慌てても焦っても3乃至5回以上間違うことなく思い出せると確信できるものしか登録できない。候補が10個以上もある人は稀である。覚えられずにメモをして隠したり携帯すれば安全性は崩壊する。(例外的な記憶力の持主は対象としない)
2	生体照合	本人拒否＝ 業務不能 本人拒否を許容できない環境では　評価不能 本人拒否許容環境では　顔見知り認証など他の手法に依存	・識別技術としての有用性　≠ 認証技術としての有用性 ・本人の責任ではない本人拒否 ・複製技術とのイタチゴッコの宿命: 指紋・顔・虹彩・声紋については偽造報告あり ・プライバシー問題・人間の尊厳毀損の問題
3	所持物照合	付けっぱなし　0ビット 紛失・置き忘れ＝業務不能 本人排除を許容できない環境では　評価不能 本人排除許容環境では　顔見知り認証など他の手法に依存	・偽造防止技術の要件　≠　本人認証技術の要件
4	生体・所持物照合 (パスワードOR 併用)	併用するパスワードのレベルを上回らない　0～3ビット相当	・恐らく使わない或いは稀にしか使わないと予想して登録するバックアップ用パスワードは脆弱なパスワードの中でも最も脆弱。
5	画像パスワード パターン記憶法	文字パスワードとニーモニックガードの中間程度	・視覚記憶は情報量が膨大で文字情報よりも記憶内容が蒸発しにくい。 ・記憶の再生ではなくて対象の再認によるものではユーザの負担は非常に小さくなる。(ニーモニックガード開発の通過ポイント)
6	ニーモニックガード	64個以上の中の8個以上選択すれば　50ビット以上可能 16個の中の4個選択でも　11～16ビット相当	・長期記憶化している視覚イメージを認証データにするのだから負担はなく思い出せないこともありえない。主観的なもので且つ昔の記憶を使えば第3者による採集は極めて困難となる。 ・本人・他人峻別機能によってユーザにはストレスをかけず、他人は早期に排除できる。

・本人認証技術に求められる機能と効果は、本人を排除することなく他人を有効に排除することに尽きる。

・本人を排除しないようにすると他人を有効に排除できなくなる技術は本人認証技術としては不適格。・他人を排除するには有効だが時には本人も排除してしまう技術は (本人排除による業務不能を許容できない環境では) セキュリティ強度の崩壊を招かずに本人排除問題を解決することができないかぎり本人認証技術としては不適格。

2004/5/21

参考資料

パスワードのパラドックス

意図

パスワードの桁数を大きくする・無機化する・頻繁に変更する
セキュリティは上がるはず

一部の人には有効、
殆どの人は実行不能

メモ携帯・
貼り出し

セキュリティ崩壊へ

モバイル環境では致命的なセキュリティ崩壊
アカウントの数が増えると、この崩壊現象はさらに顕著に

意図

入力を何度か間違えると続行不能とする
まぐれ当たりによる不正行為の確率は小さくなるはず

思い出せない＝業務不能なので身近にあるデータ（電話番号、誕生日など.）を使う

ユーザー情報を得た第三者には、類推容易

セキュリティ崩壊へ

参考資料

生体照合のパラドックス

意図

本人のみが持つ生体の特徴点を照合する
セキュリティは上がるはず

突然のケガなど本人でありながら拒絶される「本人拒否」問題を原理的に伴う

「本人拒否＝業務不能」を避けようとしてパスワードをOR方式で併用

パスワードを破ればよい

更に、こうなる

恐らく使わないと予想して登録するパスワード

絶対に忘れないもの（最も類推容易な）を使うか　或いはメモ携帯・貼り出し

パスワード単独照合よりも更に低いセキュリティしか提供せず
セキュリティ崩壊へ

但し、管理者が常駐しOR型パスワード併用禁止が実行可能な場面では有効

肉体の複製は不可能だが、肉体の特徴点の複製は容易　(実証TV放映)

混乱の背景は、識別(これは誰？)　≠　認証(これが本人？)の理解欠如

2004/5/21

参考資料

所持物照合のパラドックス

意図

特定の小物の保持者以外は排除
セキュリティは上がるはず

置忘れ
＝業務不能

置忘れ
防止努力

付けっぱなし・
入れっぱなし

端末と小物の同時
盗難を避ける努力

置忘れ＝業務不能の多発

このループからの
脱却を図る

パスワードをOR
方式で併用

絶対に忘れないもの
（最も類推容易な）
を使うか或いは
メモ携帯
セキュリティ崩壊へ

但し、管理者が常駐しOR型パスワード併用禁止が実行可能な場面では有効

参考資料

組合せのパラドックス

意図

単独では弱点がある技術も、複合化すれば
セキュリティは向上するはず

AND型複合化は、
「本人拒否・紛失・置忘れ＝業務不能」問題を悪化させる

OR型導入は、最低レベルへの回帰に帰結する

AND型でもOR型でもない組合せはありえない

↓

組合せによってセキュリティが向上することはない

むしろ、誤認識の拡散　→　セキュリティ崩壊促進