暗号鍵は随時深い記憶から生成　  　鍵盗用による解読を根絶

ニーモニックガードとデータ暗号技術を統合

クリプトニーモ

データを堅固に守る暗号ソフトの運用上の泣き所は**ユーザ認証**と**鍵の保管**

忘れない暗証イメージから動的に生成される暗号鍵を使用

プログラム終了時に暗号鍵は消滅　→　鍵の盗用による解読を根絶

ニーモニック認証を通過できない限り誰であれデータ無断閲覧は不可能

広範な活躍場面 

デバイス防御：　端末・メモリー媒体の盗難によるデータ漏洩を防止します

何故なら、暗号鍵はどこにも存在しないから

盗用犯はニーモニックガードが確実に排除するから

ネットワークセキュリティ：　機密情報の流出を強力に抑止します

何故なら、ユーザの秘密鍵はどこにも存在しないから

不正アクセス犯はニーモニックガードが確実に排除するから

電子証明書：　証明書の中身を盗まれても悪用される心配はありません

何故なら、ユーザの秘密鍵はどこにも存在しないから

盗用犯はニーモニックガードが確実に排除するから

開発・販売元
株式会社　ニーモニックセキュリティ
代理店
株式会社　SKR テクノロジー

製品共通仕様

暗号鍵はユーザが必要な時にニーモニック・パスシンボルから動的に生成
プログラム終了時に暗号鍵を消滅させて盗用による解読を根絶
共通鍵は標準としてＡＥＳ、公開鍵基盤には標準としてＲＳＡ暗号を使用

簡単な操作

１．ソフトウェアを暗号化データを保存するドライブ或いはフォルダーにセットアップします。
２．エクスプローラ画面でアイコンをクリックしますとニーモニックガードの設定画面が現れます。
添付或いは自作の認証画面を使ってパスシンボルを登録してください。
３．次回以降、アイコンをクリックするとニーモニック認証画面が現れますのでパスシンボルを選択して下さい。認証が完了すると専用ビューア画面が現れます。
４．エクスプローラ画面からビューアに任意のファイルＡをドラッグ＆ドロップすると暗号化ファイルＡ.mnemとして指定ドライブ或いはフォルダーに格納されます。
５．ビューアから暗号化ファイルＡ.mnemをPC上にドラッグ＆ドロップすると平文のファイルＡが復元されます。

製品ラインアップ

メモリー媒体：　共通鍵方式
内部メモリー：　PCの中に自分だけの安全な情報金庫が出来ます
外部メモリー：　会社データを安全に社外に持ち出せます

ストレージサービス：　共通鍵方式
ユーザ本人以外にデータを復元できる人間はいません

ネットワークセキュリティ：　公開鍵基盤方式
内部犯罪を有効に抑止しつつ、１対多や多対多で暗号化データを安全に運用できます

セキュアメール：　公開鍵基盤方式
暗号化メールの安全性を更に向上します

電子証明書発行システム：　公開鍵基盤方式
中身を盗まれても心配のない電子証明書を発行します

ニーモニックガード

裏口パスワード併用によるセキュリティ崩壊を抱える在来技術と異なり、視覚長期記憶を活用し
本人認証＋他人認証機能を組込んだ、老若男女が誰でもストレスなく使いこなせるユーザ本人認証技術

20年も昔に撮った甥や姪の写真数枚を照合データ（パスシンボル）とした認証画面の例

たといパニック状態であっても認証に失敗することはない。高齢者にも簡単に実行できる。

不正取得者は…

本人であれば犯す筈のないエラーを犯す
→　例えば2回目で他人判定
→　**プログラム・データ消滅**

正規ユーザは…

再認したパスシンボルを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のでストレスを感じない。

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りますが、「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。ネットワーク社会のアキレス腱の防衛に直接的に貢献します。

１．本人認証なくしてセキュリティなし

いつでもどこでも情報セキュリティが不可欠な時代になってきましたが、セキュリティを考える上で忘れてはならないのは、完璧な侵入防止手段や暗号化も権限あるユーザへの成りすましに対しては全く無効であるという無慈悲な事実です。

個人情報・機密情報の漏洩や改竄の対策も基本は本人認証です。信頼できる本人認証技術の導入なくしてはアクセス権限の制限も、ログの保管も、データの分散も、セキュリティ教育も、全て上滑りなお題目で終わってしまうからです。

２．本人認証の決定打：長期視覚記憶活用と本人・他人峻別手法

本人認証技術には「記憶を照合するもの」、「所持物を照合するもの」、「生体の特徴点を照合するもの」があります。各分野で多くの技術・製品が発表されており、それぞれ特定の条件を満たす限定された環境ではそれなりの効用を発揮しています。しかし、在来の記憶照合では「覚えられるものは簡単に破られ、破られないものは覚えられず」、生体照合は「原理的に根絶不能な本人拒否問題と複製による他人排除力崩壊リスク問題との二重苦」で足元が定まらず、所持物照合は盗用に無力なことに加えて「紛失・置き忘れvs付けっ放しのジレンマ」から逃れられず、「いつでも、どこでも、老若男女を問わず誰でも、個人の尊厳を損なわず、ストレスをかけず、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」という包括的な判断基準を満たすものは長く存在しませんでした。

こうした閉塞状況を打開するものとして、数十年にも及ぶ長い期間を経てもなお記憶に強固に留まり続け、いつでも即時の再認が可能な視覚記憶の対象(注)を認証データ（パスシンボル）とする照合手法に加えて、「本人であっても犯し得る間違い選択」と「本人であれば犯すはずのない間違い選択」を峻別するアルゴリズムを組み込んだ個人認証手法（ニーモニックガード）が当社によって開発されました。（注：甥や姪が幼かった頃の写真、子供の頃自分になついていたペットの写真或いは新婚旅行先で伴侶と共に見た感動的な風景の写真などは何十年後になっても一瞥すれば即座に認識ができます。）

３．在来技術との比較

Ａ　高い数学的強度を実現できるか？

在来型パスワード	Ｘ～△	*1
生体照合・所持物照合	Ｘ～△・評価不能	*2、*3
ニーモニックガード	○	*4

Ｂ　いつでも、どこでも、誰でも、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	*5
生体照合・所持物照合	Ｘ	*6
ニーモニックガード	○	*7

Ｃ　コスト（導入費用＋運用費用）は妥当か？

在来型パスワード	△	*8
生体照合・所持物照合	Ｘ	*9
ニーモニックガード	○	*10

＊１：　一般には覚えやすさ優先や混乱回避から本人固有の客観的事実を材料にするので△ですが、厳格管理の旗の下でランダム・英数字大文字小文字特殊記号混じり６桁以上の強制を受けると表面上は服従しつつもメモに記して端末機の周辺に（同僚・上司・部下がやっているように）秘匿するのでＸとなります。

＊２：　本人拒否率をゼロとする閾値を取った場合の他人受容率を表示しているメーカーは存在せず、本人拒否については顧客が受忍すべきものとして生体照合以外の対策或いは救済策を取るように要求されます。一般の実運用では救済策としてパスワードをＯＲ型選択式で併用するので数学的強度がパスワードの強度を上回ることはなく、従って自動的にＸ～△となります。本人拒否時の救済策を併用しない単独使用では、メーカー毎に算定基準の異なる本人拒否率と他人受容率のトレードオフ関係の中で数学的強度が確定できず評価不能です。

＊３：　盗用・付けっ放しの場合の強度はゼロ。「付けっ放しｖｓ紛失・置き忘れ」ジレンマの数学的評価は不可能です。

＊４：　８ｘ８＝６４個の写真の中に秘匿された昔の愛着ある写真１０枚を探すだけで認証を完了できるケースであれば、パニック状態でも、老若を問わず、誰でも実行でき且つまぐれ当たり確率は 0/64x9/63x8/62x7/61x6/60x5/59x4/58x3/57x2/56x1/55=1/(1.99463　E+22) として確定します。

＊５：　他人排除力のあるパスワード複数組を使いこなせる人は極めて稀です。

＊６：　注意深い善意の同僚に恵まれた事務所内など特定の環境の下でしか成立しません。

＊７：　ニーモニックガードは全ての要件を満たします。

＊８：　導入コストは極めて低いが問い合わせ･再発行など運用コストは高いのです。

＊９：　大きなハードウェア購入コストが掛かる上に､維持コストも無視できません。

＊１０：　ニーモニックガードでは問い合わせ・再発行の運用コストが押さえられる為に、大規模運用では無償で導入できる文字パスワードよりもトータルコストは小さくなります。

４．産学連携

（株）ニーモニックセキュリティでは東京大学生産技術研究所今井研究室（今井秀樹教授は CRYPTREC（総務省・経済産業省共管「電子政府実現のための暗号技術検討会」座長･委員長）と共同で暗号等他のセキュリティ技術との複合化事業を推進しています。例として、個人情報を保護する匿名ネットワーク、ユーザ・システム相互認証、盗用不安のない多機能 IC カード、などを挙げることができます。

2004 年 4 月 27 日

〒530-0057 大阪市北区曽根崎 2 丁目 16 番 19 号

株式会社　ニーモニックセキュリティ

◇　お問い合わせ

株式会社 SKR テクノロジー

144-0044　　東京都大田区本羽田 2-12-2-304

TEL: 03-5735-7788　　FAX: 03-5735-7789

http://www.skr-tech.co.jp