クリプトニーモ
メモリーデバイス防御

V1.0

２００４年１１月６日

概要

「クリプトニーモ」は確実な本人確認で第 3 者による盗用・データ漏洩を防止する本人認証ソフト「ニーモニックガード」によって本人認証と暗号鍵の動的生成を行うデータ暗号化ソフトウェアです。画面上の写真やイラスト等のシンボルをいくつかタッチするだけで確実な所有者の本人認証とデータ防御の為の暗号鍵の生成・再生ができます。プログラム終了後には暗号鍵はどこにも存在しません。

特長

- 専用のビューアにドラッグ＆ドロップするだけでファイルが暗号化されます。
- 暗号化されたファイルは、ビューアからドラッグ＆ドロップ或いはビューア上でダブルクリックすれば復号され元の平文に戻ります。
- 専用ビューアは本人認証が終わらないと起動しません。
- 本人がおかしやすい間違いは許容されて何度でも試行錯誤を繰り返せますので不必要なストレスを感じることがありません。しかし、本人がおかす筈のないような間違い入力は第 3 者の不正と判定して早い段階でシャットアウトします。
- 自作の写真やイラストを自由に組み合わせて認証画面として使用するためのユーティリティソフトがバンドルされています。愛着を感じないものを囮（おとり）とし、愛着のあるものを認証データとして登録すれば、想い出せずに困ってしまうということはなくなります。
- 使用者本人の不注意ミスや子供等のいたずらで他人判定が起動してしまった場合の対策として擬似認証画面による冗長ループ（チャイルドロック）が用意されています。
- 最終他人判定時には本ソフトウェアは機能を停止します。

＊　PC 動作環境

	必須スペック	推奨スペック
CPU	Celeron 500MHz 以上	ー
メモリ	128MB 以上	256MB 以上
OS	Windows2000 SP4 または WindowsXP SP1	ー

＊　使用分野

多くの企業で会社データの社外持ち出しは禁止されていますが、禁止命令が遵守されているところは殆どありません。放置するとセキュリティモラルが崩壊して憂慮すべき状態に陥ります。しかし、「会社が認めた有効なデータ漏洩防止機能付きの記憶媒体やモバイル PC による社外持ち出しは許可するが、そうしたデータ漏洩防止機能のない記憶媒体や PC による社外持ち出しは厳禁で違反者は処罰する」とする命令は実行可能で現実的なものになります。

クリプトニーモを搭載した外部メモリー媒体やモバイル PC ならば紛失しても慌てる必要はありません。媒体を不正取得した第三者がデータを見ようとして中身を解析しても、媒体の中には暗号鍵がないので手の出しようがありません。メモリー媒体は Windows2000・XP 対応であれば種類は問いません。USB、SD、スティック、外付け HD 等の外部メモリーに加えて内蔵 HD 上でもお使い頂けます。

＊　多様な使い方

１．　外付けメモリーデバイスに搭載して機密データの社外持ち出しを安全に：　標準的な使い方です。１６MB 以上の容量があり Windows2000/XP 搭載の PC で使うのあればメモリーデバイスの種類は問いません。暗号データだけを持ち運ぶのではなく、認証ソフト及び暗号ソフト（暗号鍵なし）と一緒に暗号データを持ち運ぶことができますので、目的地のＰＣに専用ソフトを用意しておく必要はありません。どこであれ Windows2000/XP 搭載ＰＣがあり、そこにニーモニック認証を通過できる正しいユーザがこのメモリーデバイスを持っていれば暗号データを復号して仕事ができるのです。

注：　操作説明書を PC に移動させれば８MB の容量があれば使用可能となります。

注：　ハギワラシスコム製ＵＳＢメモリー「ＵＤ－ＲＷ」のライトプロテクトＵＤ－ＲＯＭ領域に搭載した場合には、ＵＤ－ＲＷ挿入時に本ソフトが自動的に起動します

２．　ノートＰＣ内蔵ハードディスク上に情報金庫を：　ハードディスク上に設けた専用フォルダ内に本ソフトを格納すると、そのフォルダが自分だけの安全な情報金庫となります。本ソフトのショートカットをデスクトップに置くと便利です。

注：　内蔵メモリー上で情報金庫として使う場合には、暗号化前のファイルはゴミ箱に放り込むだけでなく、ゴミ箱からも確実に削除してください。

３．　暗号鍵を共有したグループ内でデータの受け渡しを安全に：　ライセンス入力後の「クリプトニーモ」ソフトウェアをグループメンバーにコピー配布して初期パスシンボル情報も教示すれば、クリプトニーモで暗号化した重要なデータをグループメンバー間で安全に受け渡しすることができます。ソフトコピー配布後、全てのメンバーは自分だけのオリジナル認証画面・パスシンボルに変更できます。暗号化データはメールに添付して送ることも可能です。

注１：　ライセンス入力後にコピーされたソフトウェアは全て同一の暗号鍵で暗号化・復号を行うことになりますので、こうしたグループでの情報共有目的で一度使うと以後は当該ソフトを使って自分だけの秘密情報を守るということは出来なくなります。自分だけの秘密情報防御には別途購入のクリプトニーモをお使いください。
注２：　サポート対象となるのはライセンス購入者だけです。

＊　セキュリティ強度

データを堅固に守るための暗号技術の有用性については言うまでもありません。しかし、暗号ソフト製品の運用上のセキュリティ強度はその前に貼り付けるユーザ認証の強度を上回ることができないという大きな泣き所を抱えています。いくら暗号強度を 64 ビットだ 128 ビットだ、いやもっと高いと謳ってみても実効強度が数ビット級のパスワードや、そのパスワードを裏口に併用して同様に数ビット級のセキュリティしか提供しない生体照合をユーザ認証に使っていれば、全体のセキュリティ強度は数ビット級ということになってしまいます。もう一つの泣き所は暗号鍵の管理です。鍵を入手できた攻撃者の前には 64 ビットも 128 ビットもありません。何らかのデバイスに暗号鍵を格納して持ち歩く方式ではデバイスの盗難には全く無力です。

これまではこれら２つの泣き所は別個の問題でした。「クリプトニーモ」はこの２つの問題を 1 個の問題の２つの側面として一挙に解決を図ります。ユーザに負担を掛けることなく数十ビット級の認証強度を提供できるニーモニックガード認証の実行時のパスシンボルから動的に暗号鍵を生成し、作業が終わりプログラムを終了させる時にはその鍵を消滅させてしまいます。つまり暗号鍵はプログラム実行中に存在するだけで、プログラム終了後はどこにも存在しないのです。存在しないものは盗用される心配がありません。

漏洩すると甚大な被害を被る極秘情報の防御が必要な場合には８ｘ８画面上に無意味・無感動な類似画像に混ぜて１４個以上の“見れば判る愛着ある”画像を登録することをお勧めします。６４個中の１４個の順列選択の強度は８０ビットを上回りますので、盗難にあったデバイスが徹底的なリバースエンジニアリングにあってソフトウェア内部に格納してある全ての秘密情報を奪われるという万が一のケースを想定しても、貴重な暗号化データは依然として８０ビット級のセキュリティで防御されるからです。（詳細は後述「クリプトニーモの暗号鍵生成について」をお読みください。）

一般には認証画面サイズと登録個数・方法は、予測される漏洩被害の深刻さと毎回の認証時の簡便さとのバランスを考慮してユーザのご判断にお任せすることになりますが、事情が許す限りは多少の手間はかけても大きな画面でできるだけ多くの愛着画像を順列登録されるようお勧めします。

＊　クリプトニーモの暗号鍵生成について

クリプトニーモでは暗号鍵を記憶情報（パスシンボル情報から作られるユニークな値）＋記録情報（ユニークな乱数）から生成しています。記録情報は秘匿していますが徹底的なリバースエンジニアリングを行われると第三者に奪われる可能性はゼロではありません。これは秘密情報をデバイス上に秘匿するソフトウェア製品全般に共通する問題です。万一記録情報を奪われると暗号化データを守るのは記憶情報部分の強度だけになります。

一般に暗号鍵は８０ビット以上（おおよそ１兆の１兆倍）であることを求められます。８０ビット級の記憶情報を使用して動的に暗号鍵を生成する手法では、万一記録情報部分が奪われても依然として８０ビット級の記憶情報由来のセキュリティが残っていることになります。８０ビットは８ｘ８画面で１４個の愛着画面を過不足なく順列選択すれば実現できます。２０個も順列登録すれば強度は１１５ビットにもなります。因みに、高い強度を出せる長いパスワードはメモに記して持ち歩くことになり、メモに頼らなくても済む短いパスワードでは高い強度が出せません。バイオメトリックス情報では十分な容量のデータは完全な再現が不可能であり、再現可能なものではデータ量が足りません。記録情報以外の入力データから８０ビットを超える高い強度を実現するのはクリプトニーモのみが為し得ることです。

愛着あるイメージ記憶は老若男女の誰にとっても暗号鍵生成の最適の材料であり、最高の耐タンパーデバイスは人間の頭です。記憶（＝人間の頭脳の働きそのもの）と暗号技術（人間の頭脳活動の最高の産物の一つ）との一体化を果たすのがクリプトニーモです。

＊　注意

暗号化・復号処理中に何らかの事情で異常終了した場合には必ず本ソフトウェアを再起動した上で正常に終了させて下さい。（異常終了したままで記憶デバイスを取り外しますとデバイス内に平文を含んだ作業ファイルが残存している可能性を否定できません。再起動後に正常終了すれば作業ファイルは消滅します。）

本製品は、機密データを外部記憶媒体やノート PC などによって持ち出す場合のデータ防衛を主眼として開発されたものです。本ソフトウェア及び付属ファイルの破損その他予期せぬ事態の可能性を考慮して、安全な環境に保管されている原本は暗号化せずに平文のままで保存しておいて下さい。

A　セットアップ編

１．ダウンロードした「クリプトニーモ」ソフトウェアを、暗号化ファイルを保管すべきデバイスのドライブ或いはフォルダの中に保管してください。デフォルトは C ドライブのプログラムフォルダーとなっています。

２．本ソフトのアイコンをダブルクリックするとプログラムが自己解凍され、本ドライブ或いはフォルダ内にアプリケーションと専用フォルダ crmn がセットアップされます。格納フォルダの中には標準添付の認証画面雛型が入っています。また、インストールフォルダの中には認証画面作成ソフト（Symbol-Regist3cm.exe）が入っています。

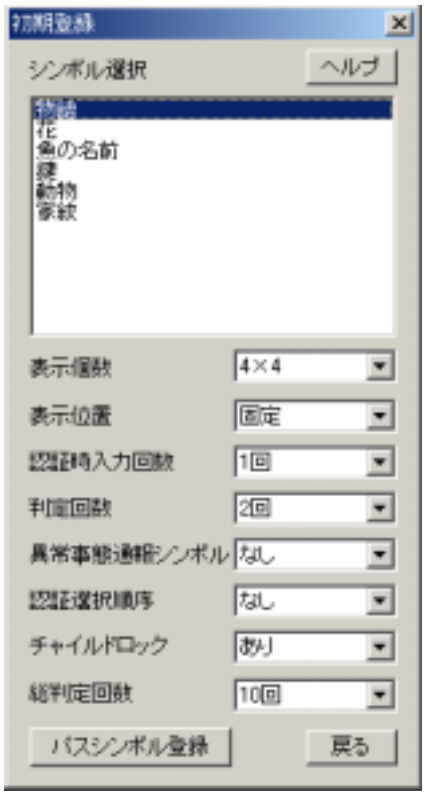
３．本操作説明書と一緒にダウンロードした認証画面作成説明書に従ってご自分だけの認証画面をご準備ください。多少の手間はかかりますが、できれば全ての画像をご自分で用意されることをお勧めします。
（とりあえず試してみたいという方は、　雛型の中で強い愛着を感じるもの或いは過去の愉しい記憶に直結するものを出来るだけ多く選んで、出来ればストーリーをつけるなどして、登録して頂く事もできます。後刻、ご自分だけの認証画面に変更することをお勧めします。）

４．ご自分の認証画面の準備が出来ましたら、ｸﾘﾌﾟﾄﾆｰﾓ.exe をダブルクリックするか「スタート」→「プログラム」からアプリケーションを起動して次の登録操作編にお進みください。

B　登録操作編

１.「初期登録画面」が現れたところで、プルダウンメニューを使って以下の選択を行ってください。いつでも変更可能ですから気軽に進んで下さい。

「シンボル選択」　（認証に使用するシンボルと画面を選択します。6 種の認証画面が標準で用意されていますが最大 100 画面まで拡張可能です。本ソフトにはオリジナルの認証画面を自作するためのユーティリティソフト「Symbol_Regist2U」が添付されています。）



認証画面の内の一つをクリックして選択

「表示個数」　（画面に表示するシンボル個数を決めます。）

「４ｘ４」或いは「６ｘ６」或いは「８ｘ８」のいずれかを選択

「表示位置」　（シンボルの画面での表示方法を決めます。）

「固定」或いは「ランダム」のどちらかを選択

固定：認証シンボルはいつも決まった位置に表示されます
ランダム：認証シンボルは毎回違った位置に表示されます

「認証時入力回数」　（認証時に 1 回の入力で照合するか、2 回同じ入力をして照合するかを決めます。）

「1 回」或いは「2 回」のどちらかを選択

「判定回数」　（本人がおかす可能性の低い間違い入力＝他人推定エラーを何度まで許容するかを決めます。2 回を選択すると 2 回目の他人推定エラー入力で不正使用判定となります。
不正使用判定となると一切の操作を不能とします。

「2 回」から「9 回」のいずれかを選択

「異常事態通報シンボル」　本ソフトでは使用しません。（所有者であることを認証した上で、脅迫状態にあることを脅迫者に知られることなくシステムに通知させるためのシンボルを登録することができる機能です。ネットワーク対応版では使用します。）

「なし」のままにしておく

「認証選択順序」　（シンボル登録に順序をつけるか、順序不問にするかを決めます。ストーリー付けの容易なシンボルの組合せに順序を付けるとセキュリティ強度を高く維持できます。順序不問ではセキュリティ強度は下がりますが認証操作は容易です。認証画面の性格に応じて使い分けて下さい。）

「あり」或いは「なし」のどちらかを選択

「あり」: 登録時の順序どおりにシンボルを選択したときに認証が完了します
「なし」: 登録時のシンボルを選択したときに、順序を問わずに認証が完了します

「チャイルドロック」　（使用者本人の不注意・ミスや子供等のいたずらで他人判定機能が働いてしまった場合に対する万一のための安全弁機能です。「あり」を選択すれば不正使用判定時に直ちに操作不能とはならず、一度複雑な手動操作[Shift キーを押しながらマウスを右クリック]を要求する擬似認証画面（冗長ループ）に入ります。擬似認証画面を抜け出た後に改めて現れる認証画面で正しい認証シンボルの選択が行われれば認証が完了し、再度不正判定が行われると、不正使用と最終判定し一切の操作が不能となります。）

「あり」或いは「なし」のどちらかを選択

「総判定回数」　（本人がおかす可能性の高い間違い入力（本人推定エラー）と本人がおかす可能性の低い間違い入力（他人推定エラー）の総計を何度まで許容するかを決めます。5 回を選択すると本人推定エラーと他人推定エラーの合計が 5 回目に達したところで不正使用判定となります。不正使用判定となると一切の操作を不能とします。）

「5 回」或いは「10 回」或いは「20 回」のいずれかを選択

定義：　本ソフトでは本人推定エラーと他人推定エラーを以下の様に定義しています。

本人推定エラー：　登録シンボルを 1 個以上含み、且つ間違いシンボル選択個数が 3 個以下
他人推定エラー：　登録シンボルを全く含まないか、間違いシンボル個数が 4 個以上

登録した後でも再変更可能ですから、先ずは「パスシンボル登録」をクリックして次に進んで下さい。

２．シンボル登録画面が現れます。

意図していた画面と違っていれば「戻る」をクリックして、初期登録画面に戻ってやり直します。

意図した通りの画面であれば認証データとして登録するべきシンボルを2個以上随意の個数クリックして、最後に「入力」をクリックします。自分の昔の楽しかった想い出などと結びつけられるシンボルを登録すると長期間使わなくても忘れることなく簡単に想い出せます。高いセキュリティを得るには８ｘ８画面を使い出来るだけ多くのパスシンボルを登録することをお勧めします。

再確認のために同じ選択をもう一度繰り返してください。間違えた時には「リセット」をクリックして、やり直して下さい。

３．正しく「再入力」が終わりますと、パーソナル ID が表示されます。後述の「ライセンス登録」手順に従って購入したライセンス ID を入力してください。ライセンス ID の入力が完了するまでは、本人認証完了後に表示される専用ビューア画面は機能せず、ファイルの暗号化・復号機能は作動しませんが、認証画面の変更などは可能です。

ライセンス ID を入力しますと認証後に表示される専用ビューアを使ってファイルの暗号化・復号が可能になります。実用編にお進みください。

C　クリプトニーモ実用編

１．本ソフト起動時に表示される「認証シンボル入力画面」で先に登録したパスシンボルをクリックして下さい。「順序あり」を選択した場合には、登録した順序でクリックして、最後に「入力」をクリックして下さい。認証が完了すると専用ビューアが表示されます。

２－１.暗号化したいファイルをエクスプローラ画面からビューア内にドラッグ＆ドロップしてください。ファイルが暗号化され、ビューアで指定したフォルダに格納されます。（初期状態では、ビューアに使用上の便宜のためフォルダ名が表示されている場合でも、ファイルは何も入っていません。）

２－２.暗号化されたファイルをビューアからエクスプローラ画面内やデスクトップにドラッグ＆ドロップすると復号され元の該当するフォルダ内或いはデスクトップに平文のファイルが復元されます。

３－１．ビューア上で暗号化されたファイルをダブルクリックすると、アプリケーションを起動してファイルが平文で画面に表示されます。

３－２．上記のファイルを閉じると元の暗号化ファイルを上書きします。平文ファイルはどこにも残りません。

４．ビューア内ではファイルの削除以外の操作はできません。該当するフォルダ内のファイルの操作はエクスプローラ上で行ってください。

＊　100ＭＢを超す大きなファイルをドラッグ＆ドロップしますとメモリー消費の影響で処理時間が相当長くかかることがあります。大きなファイルを復号する際にはダブルクリックして復号した後で希望のフォルダに格納する方法をお奨めします。

暗号化・復号処理

暗号化・復号処理は次の４種類の方法で処理を行います。

- 暗号一覧ビューア内へのドラッグ＆ドロップにより、暗号化処理を行います。
- 暗号一覧ビューアから外へのドラッグ＆ドロップにより、復号処理を行います。
- 暗号一覧ビューア内の暗号ファイルをダブルクリックもしくは暗号ファイルを選択後、Enter キーを押下することにより、復号処理を行います。
- ダブルクリックもしくは Enter キーにより復号された場合、拡張子に関連付いたアプリケーションが終了後、暗号化処理を行います。

処理	フォルダ	ファイル
暗号化	・サブフォルダ内を含む全ファイルを暗号化する(右のファイル欄参照) ・サブフォルダがない場合、フォルダを作成するか確認する (**暗号化フォルダ生成確認**参照)	・ファイルを暗号化する ・ビューアのカレントフォルダ配下に、拡張子[mnm]を追加した暗号化ファイルを作成する※1 ・暗号化処理中は、プログレスバーを表示する(**ビューア表示画面**参照) ・ファイルが既存の場合、上書き確認を呼び出す(**暗号化ファイル上書き確認**参照)
復号	・暗号化ファイルの有無に関わらず、フォルダ構成をコピーする ・サブフォルダ内を含む全ファイルを復号する(右のファイル欄参照) ・復号先のフォルダ操作は Windows へ処理を渡すものとする(**暗号化ファイル上書き確認**参照)	・ファイルを復号する ・ドラッグ＆ドロップした場合、拡張子[mnm]を除いたファイル名の復号したファイルを生成する※2 ・ダブルクリックもしくは Enter キーにより復号依頼された場合、一時ファイルを生成し、拡張子に関連付いたアプリケーションを起動する ・復号処理中は、プログレスバーを表示する(**ビューア表示画面**参照) ・ファイル操作は Windows へ処理を渡すものとする(**復号処理確認画面**参照)

※1 暗号化ファイル生成例
フォルダ・複数ファイルを指定した暗号化の場合、ファイル毎に暗号化したファイルを生成する。

暗号化対象ファイル名：「ファイル名.bmp」
↓
暗号化済みファイル名：「ファイル名.bmp.mnm」

※2 ダブルクリック、Enter キーによる一時ファイル
管理フォルダ配下に、「temp フォルダ」および「一時ファイル」を作成する。

暗号化ファイル名：「ファイル名.bmp.mnm」
↓
一時ファイル名：「mnm ファイル名.bmp」

注１：　セキュリティ優先

セキュリティ保持のために復号処理は暗号化データの格納されているフォルダ内部で行われます。通信速度の低い外部メモリーデバイスを使用している場合には処理速度にそれだけ時間がかかりますが、製品の性格上セキュリティを最優先しているためです。

注２：　本人認証

１．　認証作業中には、手が滑った、勘違いで似たものをクリックしてしまった、といった間違いは誰にでもありますが、こうした間違いは本人である可能性があるものとして次の入力を許容します。あせらず気軽に認証操作を続けて下さい。ただし、総判定回数を越えると不正使用になりますので余り油断はしないでください。

定義：　本ソフトでは本人推定エラーと他人推定エラーを以下の様に定義しています。

本人推定エラー：　登録シンボルを１個以上含み、且つ間違いシンボル選択個数が 3 個以下
他人推定エラー：　登録シンボルを全く含まないか、間違いシンボル個数が 4 個以上

２．不正使用を試みる者が電源を入れても同じ認証画面を見ることになります。他人が簡単に入手できる所有者固有データ（誕生日・電話番号等）は何の手がかりにもなりませんから、先ずは総当りを試みる以外にはありません。登録シンボルを一つも含まない選択の上に「入力」をクリックされた時には、本人である可能性の低い他人推定エラーとして判定回数に数えます。登録時に 2 回が選択されていれば、2 回目の他人推定エラー入力で不正使用と判定され、一切の操作が不能となり不正拾得者の盗用・データ漏洩を防止します。「判定回数」登録時に、例えば 3 回と指定されていれば、2 回の誤り入力は許し 3 回目で不正と判定されることになります。登録シンボルを含む選択をしても、総判定回数を越えると、不正使用と判定されます。

３．ミス・悪戯に対する安全弁としての「チャイルドロック」を選択していれば不正判定時に前の画面に戻ります。再度先に進むと改めて認証画面が現れますが、これは擬似画面で一切の入力を受け付けません。“**Shift キーを押しながらマウスの右ボタンを同時に押す**”特殊キー操作を行って下さい。ポカミスでこうした複雑な行為をしてしまうことは考えられません。この説明書を読んでいない悪戯っ子もこの過程で排除されます。

こうした複雑な操作を通過できた所有者には改めて正規の認証画面が表示されます。今回はポカミスをしないように注意して登録シンボルをクリックして下さい。不正使用を試みる者はここで最終的に排除されます。

注３：　不正使用について

不正使用判定となった場合、クリプトニーモ環境ファイルを削除し、インストール直後の初期状態に戻ります。こうしてデータ復号を不可能としてデータ漏洩を防ぎます。

注４：　複数のクリプトニーモの並行運用について

同一フォルダ内での二重起動はできませんが、フォルダの異なる複数のクリプトニーモの並行運用は可能です。２本目は、1 本目とは異なるフォルダに手動でセットアップを行って下さい。

D　認証シンボル等変更編

１．認証画面と登録データを新たなものに変更したい時の手順は以下の通りです。

添付の認証画面作成ソフト(Symbol-regist3cm)を使って新しい認証画面を用意しておきます。手順は認証シンボル・画面作成ソフト操作説明書に説明してあります。

→　クリプトニーモアイコンをクリックして本ソフトを起動し認証を通過し「初期設定」ボタンを押して下さい

→　「B　登録操作編」に従って、認証シンボルや表示個数等を登録し直していきます。

→　「再入力」ボタンを押すと新しいパスシンボルが登録されます。

- ✧　パスシンボル登録済みのユーザがクリプトニーモ実行中のシンボル画面を「シンボル登録」を用いて登録・削除することはできません。
- ✧　「シンボル登録」を用いてシンボル画面を登録し直すと、パスシンボル登録済みのユーザがそのシンボル画面を使用していた場合、「ユーザ選択」画面から「認証シンボル入力」画面へ遷移できなくなりますので、その場合ユーザは初期登録をし直す必要があります。

同じ認証画面を使って登録データだけを変更することは避けて下さい。記憶の混乱を招くことがあります。

登録データを変更する時には必ず新しい認証画面を使用して下さい。記憶の混乱は起こりません。

F　アンインストール編

本ソフト及び暗号化データが不要になった場合はエクスプローラ画面で削除して頂けます。更にゴミ箱からも削除してください。

G　ライセンス番号取得編

本ソフトをセットアップしパスシンボルを登録した直後に行った最初の認証に引き続き表示されたパーソナル番号を記憶させるかメモをしておいて下さい。

当社ウエブサイトにアクセスして「クリプトニーモ　ライセンス購入」をクリックし表示される購入画面のガイダンスに従って、先程コピーしたパーソナル No. を貼り付けて下さい。次に鍵コードの送り先となるメールアドレスを入力して下さい。メールアドレスをお間違えになると鍵コードをお届けできませんので慎重に入力をお願いします。

次に、「送信」をクリックして下さい。後刻当社より、お客様の入力されたメールアドレス宛に「クリプトニーモ購入申し込み受付メール」を送信いたします。この「購入申し込み受付メール」に支払先（三井住友の PAYWEB サイト）のご案内が出ておりますので、同サイトにアクセスし、画面のご案内に従って支払手続きを行って下さい。支払方法は、クレジットカード、コンビニ支払、銀行振込、郵便振替がご利用になれます。三井住友の PAYWEB サイトに入力されたお客様の個人情報は当社には通知されません。当社ではお客様のメールアドレスと入力されたパーソナル No. のみを登録いたします。

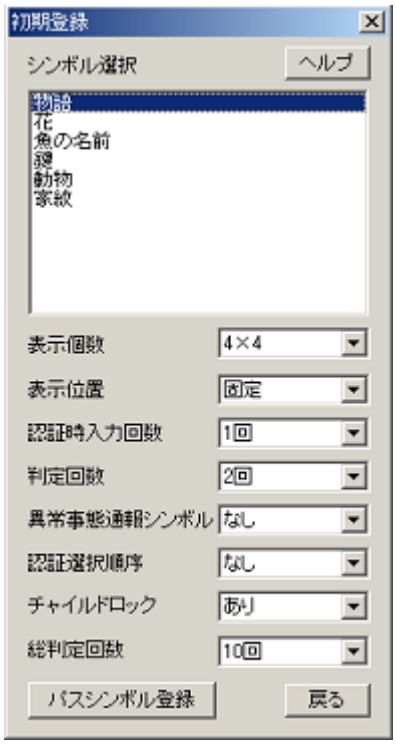
三井住友の PAYWEB から入金が当社に通知されますと（通常は入金日の翌営業日）、お客様のメールアドレスにパーソナル No と合致するライセンス番号をメールにてご通知いたします。本ソフトを起動し認証を終えたところで表示されるライセンスＩＤ入力画面上で通知されたライセンス番号を入力してください。ビューア上での暗号化と復号が始まります。

＊　その他の一般の操作につきましては、Windows2000/XP の説明書をご参照下さい。

ご質問は　http://www.mneme.co.jp　FAQ コーナー　＆　お問い合わせコーナー　へどうぞ

付録　　主要画面の詳細説明

初期登録画面



ニーモニック認証の認証方法等について以下の設定項目の設定を行います。

「シンボル選択」
認証画面とタイトル文字を割当て、プルダウンにて選択する。
認証画面は、最大１００画面分まで登録できます。
初期値は（花、家紋、魚の名前、鍵、動物、物語）です。

「表示個数」
認証画面のシンボル表示の個数「4X4,6X6,8X8」の切り替えをプルダウンにて選択します。シンボル選択で選択したタイトルで登録してあるシンボル数が足りないような表示個数は選択できません。

「表示位置」
認証画面内のシンボル表示を「固定、ランダム」からプルダウンで選択します。固定とした場合には、シンボルを固定位置に表示し、ランダムとした場合には、シンボル表示位置を毎回変更します。

「認証時入力回数」
認証画面の回数を「１回、２回」からプルダウンにて選択します。２回とした場合には、同じ選択を２度繰り返した場合に照合プロセスに進みます。

「判定回数」
認証画面での他人判定回数で、「２回～９回」からプルダウンにて選択します。全てのシンボルが一致しないパスシンボル指定を、本回数だけ行うと他人による不正な試みと判定します。

「異常事態通報シンボル」（クリプトニーモ　メモリーデバイス防御では使用していません）
認証画面で異常事態通知を「なし、あり」からプルダウンにて選択します。「あり」とした場合は、通常の認証用シンボルの登録に加えて、異常事態通報シンボルを２回の操作で登録します。異常事態通報とは、脅迫されて認証しようとした場合に脅迫されていることをシステム管理者等に通知するための機能であり、何らのメッセージも表示せず脅迫者に知られることなく異常事態通知を実行し、正常にログオンします。
試用版、製品版とも「ニーモニックガード」はドメインユーザに限り、サーバへ通知する機能があり、サーバのツールの設定により、管理者へメールが送信されます。

「認証選択順序」
シンボルの選択順序を「なし、あり」からプルダウンにて選択します。「あり」とした場合には、シンボルの選択順序を問う方式となります。

「チャイルドロック」
使用者本人の不注意・ミスや子供等のいたずらで他人判定機能が働いてしまった場合に対する万一のための安全弁機能です。

「あり」或いは「なし」のいずれかが選択できます。

あり ： 不正使用判定時に、一度意思的で複雑な手動操作を要求する擬似認証画面（冗長ループ）に入ります。擬似認証画面を抜け出た後に改めて現れる認証画面で正しい認証シンボルの選択が行われれば認証が成功します。ロックの解除は Shift キーを押しながらマウスを右クリックします。再度不正判定が行われると、不正使用と最終判定し一切の操作が不能となります。

なし ： 不正使用判定時に直ちに操作不能になります。

「総判定回数」
認証画面での本人推定判定回数で、「５回、１０回、２０回」からプルダウンにて選択します。本人推定・他人推定を問わず、エラーの総数が本回数に達すると他人による不正な試みと判定します。

「**戻る**」ボタンを押下すると、ログイン時は「ユーザ選択」画面、ロック時は「オプション」画面に戻ります。
「パスシンボル登録」で「シンボル登録」画面に遷移します。

一度初期登録を行っても、再登録時には前回の登録状態は初期登録画面に表示されません。これは、不正なユーザに設定状態を確認されないようにするためです。

キーボード入力機能

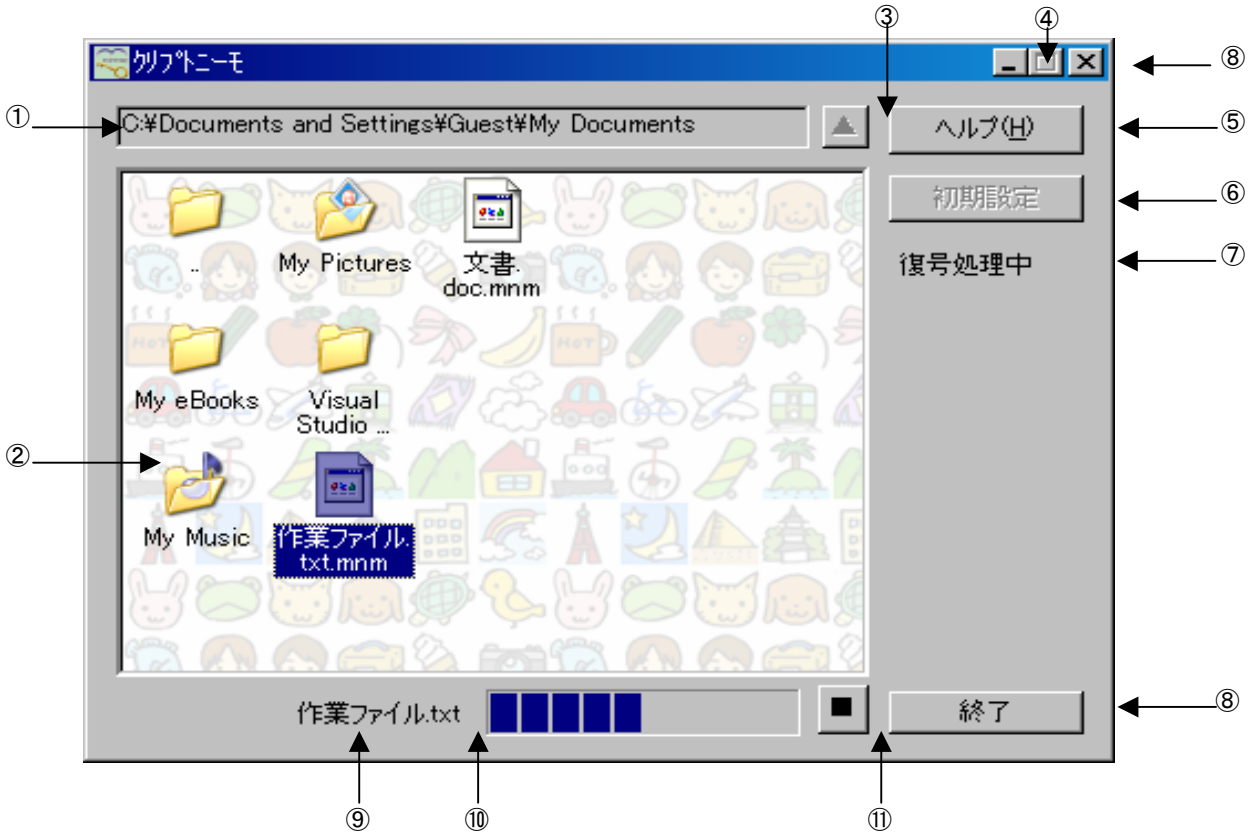
入力操作を覗き見され易い環境でマウスでのクリックのかわりにキーボードによる入力をするための機能です。認証画面の下の方に「□キーボードを使用するときはチェックしてください。」というチェックボックスがあります。

「☑キーボードを使用するときはチェックしてください。」のようにチェックすると以下のような画面になります。

選択するシンボル左下のアルファベット２文字のキーを順次入力するとマウスクリックしたのと同じ状態になります。
最後に入力ボタンをマウスクリックする必要があります。
上図でウサギと鉛筆がシンボルパスワードの場合は「qtap」とキーボード入力し、最後に入力ボタンをマウスクリックします。

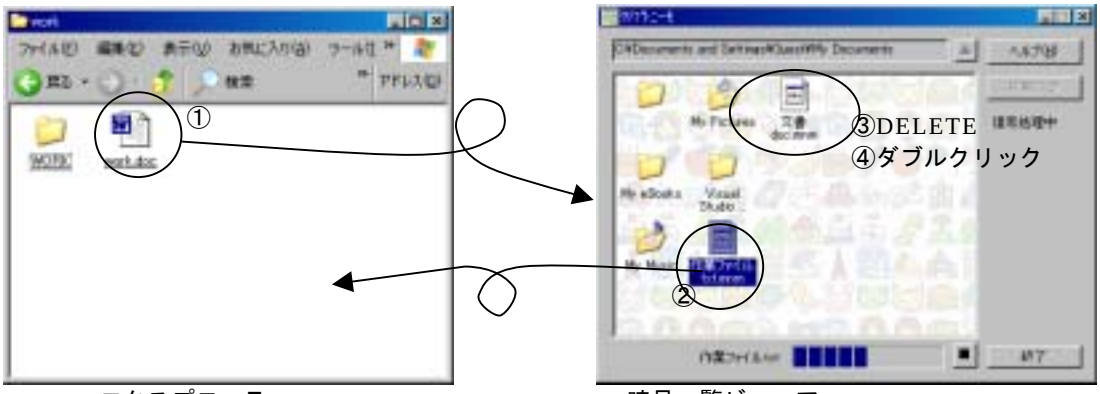
ビューア表示画面

アプリケーションを起動したドライブのフォルダと暗号化したファイルを表示します。



項番	項目名	属性	処理
①	カレントフォルダ名	Edit Control	カレントのフォルダ名を表示する ・入力不可
②	暗号化ファイルビュー	Control	カレントフォルダ配下のフォルダと本アプリケーションで暗号化されたファイルを表示する
③	フォルダ移動ボタン	Button	上位フォルダへ移動する ・最上位は、ドライブのルートフォルダになる
④	最小化ボタン	Button	ウィンドウを最小化する
⑤	ヘルプボタン	Button	ヘルプを表示する
⑥	初期設定ボタン	Button	初期登録更画面を表示する
⑦	状況	Static Text	処理状況を表示する ・固定文字：「ライセンス未登録」 「暗号化処理中」 「復号処理中」 上記以外のときは表示しない。
⑧	終了ボタン	Button	暗号一覧ビューアを終了する
⑨	処理ファイル名	Static Text	処理中のファイルを表示する ・最大 20 文字まで表示する
⑩	プログレスバー	Progress Control	暗号化または復号処理の状況を表示する ・各ファイルに対して、100KB 処理する毎にバーを進める
⑪	中断ボタン	Button	暗号化または復号処理を中断する ・処理中の暗号・復号ファイルは残さないが、対象ファイルを複数選択していた場合、処理済のファイルは残す

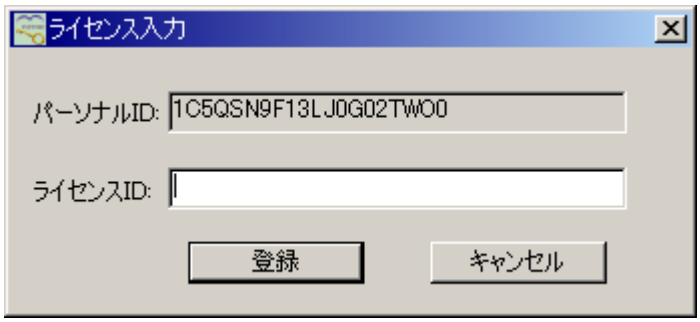
ビューア画面　暗号化・復号操作



エクスプローラ　　暗号一覧ビューア

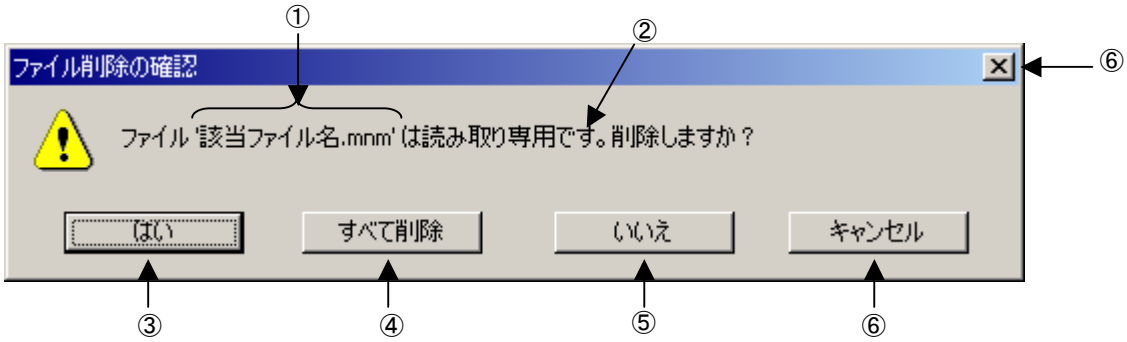
項番	操作	説明
①	エクスプローラから暗号化ファイルビュー内へドラッグ＆ドロップ	暗号化処理 ・ファイル、フォルダともに対象になる ・複数のファイル、フォルダが指定可能である
②	暗号化ファイルビュー内からエクスプローラへドラッグ＆ドロップ	復号処理 ・ファイル、フォルダともに対象になる ・複数のファイル、フォルダが指定可能である
③	暗号化ファイル選択後、 Delete キー押下	暗号化ファイルを削除する
④	暗号化ファイル選択後、 マウスの左ボタンをダブルクリック、もしくは Enter キーを押下	復号して、関連するアプリケーションを起動する (**暗号化・復号処理**参照)
	フォルダ選択後、 マウスの左ボタンをダブルクリック、もしくは Enter キーを押下	・カレントフォルダを移動する ・フォルダが移動できない場合、エラーを表示する。(アクセスエラーメッセージ画面参照)

パーソナル ID 表示画面



ファイル削除メッセージ画面

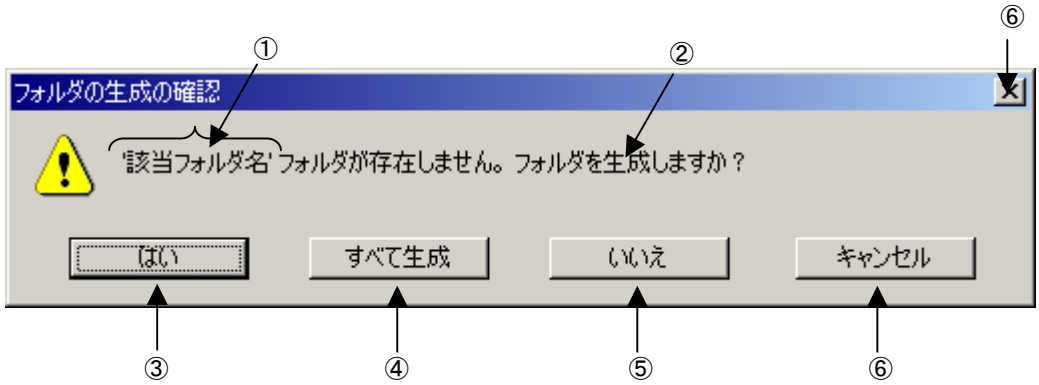
「はい」押下時：OK、対象のファイルを削除します。
「すべて削除」押下時　：ALLOK、以降読取り属性ファイルがある場合、すべて削します。
「いいえ」押下時：NG、対象の読取り属性ファイルはすべて削除対象から外します。
「キャンセル」押下時：CANCEL、削除処理を中断します。



項番	項目名	属性	説明
①	フォルダ名	Static Text	該当するフォルダ名を表示する ・最大 20 文字まで表示する
②	確認メッセージ	Static Text	確認メッセージを表示する
③	はいボタン	Button	対象フォルダを削除する
④	すべて削除ボタン	Button	以降読取り属性ファイルがある場合、本ダイアログを表示せず、すべて削除する
⑤	いいえボタン	Button	対象ファイルを削除対象から外す
⑥	キャンセル	Button	すべてのファイルの削除を中断する

暗号化フォルダ生成確認

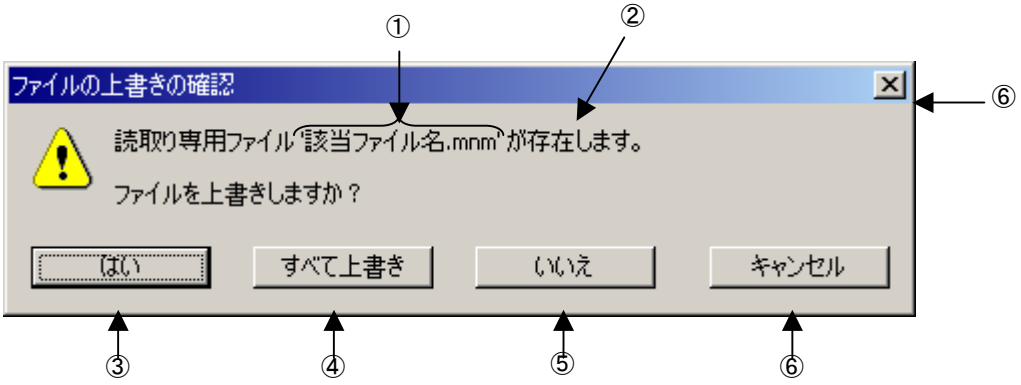
暗号化先のフォルダが存在しない場合に表示されます。
「はい」押下時：OK、対象のサブフォルダを生成して処理を継続します。
「すべて生成」押下時　：ALLOK、以降サブフォルダがない場合、すべて生成しながら処理を継続します。
「いいえ」押下時：NG、対象のサブフォルダ配下はすべて暗号化対象から外します。
「キャンセル」押下時：CANCEL、暗号化処理を中断します。



項番	項目名	属性	説明
①	フォルダ名	Static Text	該当するフォルダ名を表示する ・最大 20 文字まで表示する
②	確認メッセージ	Static Text	確認メッセージを表示する
③	はいボタン	Button	対象フォルダを生成する
④	すべて生成ボタン	Button	以降サブフォルダがない場合、本ダイアログを表示せず、すべて生成しながら処理を継続する
⑤	いいえボタン	Button	対象のサブフォルダ配下はすべて暗号・復号対象から外して、処理を継続する
⑥	キャンセル	Button	すべての暗号・復号処理を中断する

暗号化ファイル上書き確認

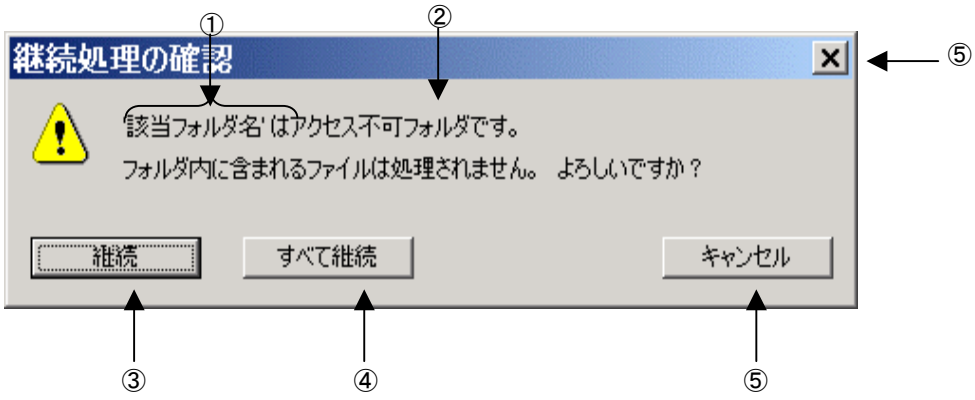
暗号化先のフォルダに同名ファイルが存在する場合に表示されます。
「はい」押下時：OK、対象ファイルを上書きして処理を継続します。
「すべて上書き」押下時　：ALLOK、以降対象ファイルをすべて上書きして処理を継続します。
「いいえ」押下時：NG、対象ファイルは処理対象から外して、処理を継続します
「キャンセル」押下時：CANCEL、暗号化処理を中断します。



項番	項目名	属性	説明
①	ファイル名	Static Text	該当するファイル名を表示する ・最大 20 文字まで表示する
②	確認メッセージ	Static Text	確認メッセージ画面を表示する 「読み取り専用ファイル***が存在します。ファイルを上書きしますか？」 「*** ファイルが存在します。ファイルを上書きしますか？」
③	はいボタン	Button	対象ファイルを上書きする
④	すべて上書きボタン	Button	以降同じファイル名がある場合、本ダイアログを表示せず上書き処理を行う
⑤	いいえボタン	Button	対象ファイルを上書きしない
⑥	キャンセルボタン	Button	処理を中断する

暗号化処理確認画面

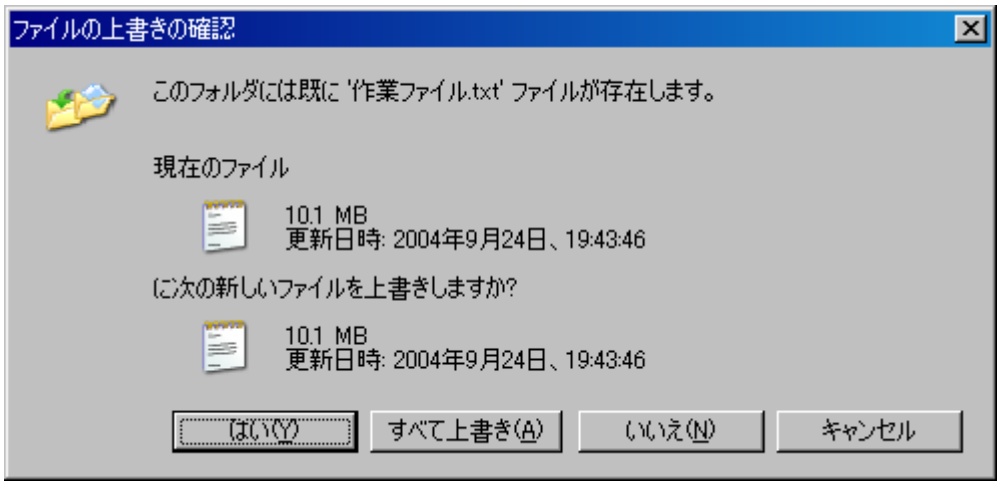
暗号化処理で読取り専用のためアクセス不可のフォルダが含まれる場合に表示されます。
「継続」押下時：OK、対象フォルダ配下のファイルは暗号処理せず、他のフォルダの処理を継続します。
「すべて継続」押下時　：ALLOK、以降、読取りフォルダに対してはすべて暗号処理をせず、他のフォルダの処理を継続します。
「キャンセル」押下時：CANCEL、暗号化処理を中断します。



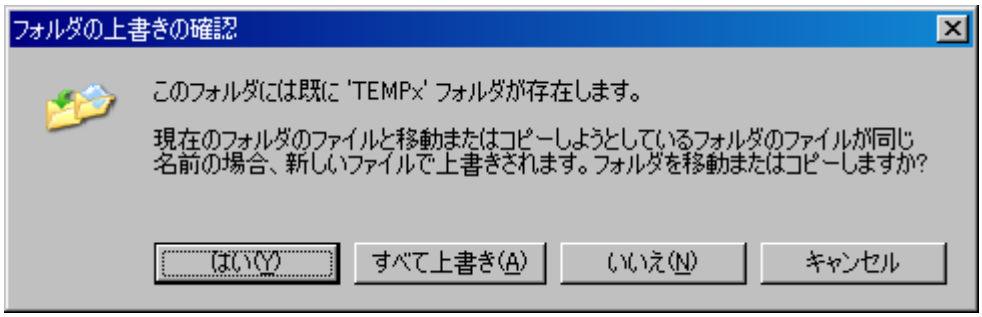
項番	項目名	属性	説明
①	フォルダ名	Static Text	該当するフォルダ名を表示する ・最大 20 文字まで表示する
②	確認メッセージ	Static Text	確認メッセージを表示する
③	継続ボタン	Button	処理を継続する
④	すべて継続ボタン	Button	以降、同じ処理がある場合、本ダイアログを表示せず処理を継続する
⑤	キャンセルボタン	Button	暗号化処理を中断する

復号処理確認画面

復号先のフォルダに同名ファイルが存在する場合に表示されます。



復号先に同名フォルダが存在する場合に表示されます。

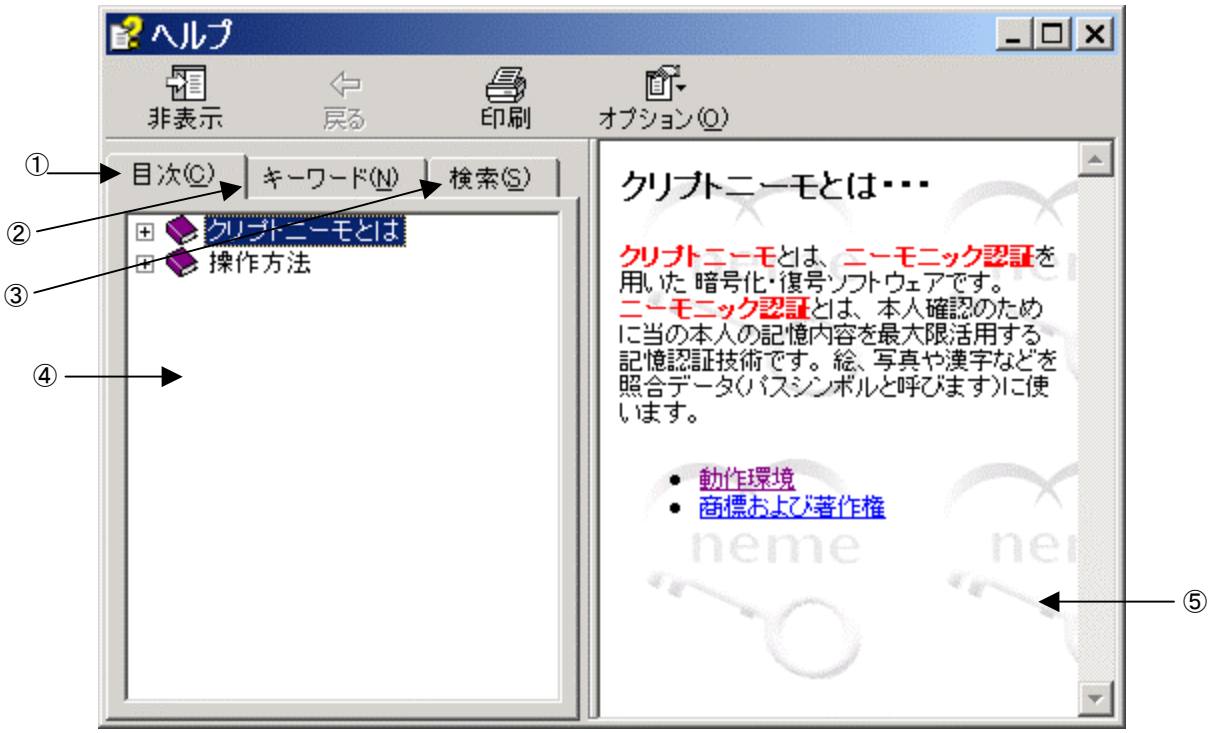


暗号・復号処理エラーメッセージ画面

暗号・復号処理中に、一般的なファイルアクセスエラーが発生した場合に表示します。

ヘルプ画面

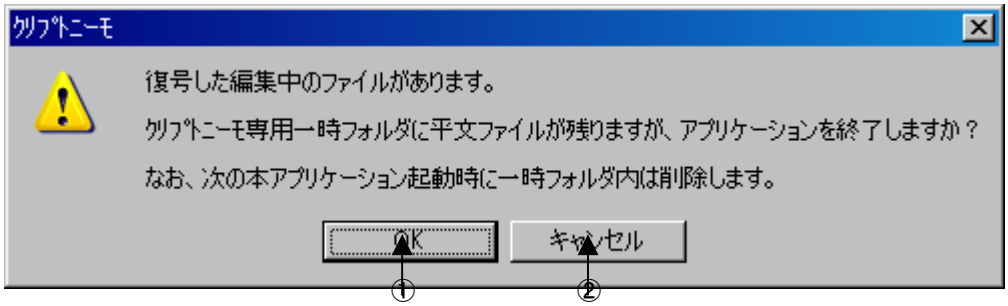
暗号一覧ビューア画面でヘルプボタンをクリックするか、F1 キーを押した場合に呼び出されます。



項番	項目名	属性	説明
①④	目次	—	目次を④の部分に表示する
②④	キーワード	—	キーワード一覧を④の部分に表示する
③④	検索	—	検索のキーワード入力を④の部分に表示する
④	本文	—	目次およびキーワードおよび検索キーワードに合わせた本文を表示する

終了確認処理

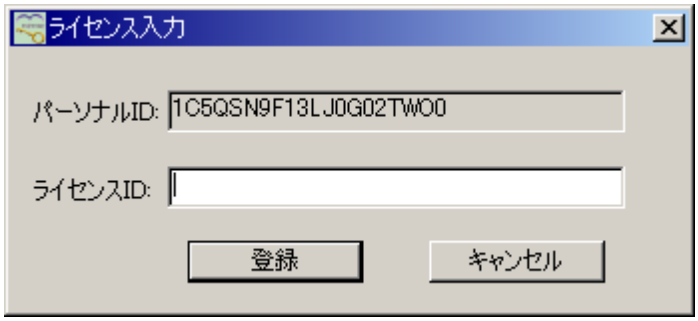
ダブルクリック、Enter キーで復号したファイルを編集中のアプリケーションが終了していない時に表示されます。尚、temp フォルダー内のファイルは、次に本アプリケーションを起動した時に削除されます。



項番	項目名	属性	説明
①	OK ボタン	Button	復号されたファイルを一時フォルダに残し、アプリケーションを終了する
②	キャンセルボタン	Button	アプリケーションの終了を中止し、ビューア画面に戻る

ライセンス登録処理

ライセンスビューア表示画面の登録ボタンを押下したときに表示されます。
ライセンス登録成功時：OK、ライセンス成功を示します。
ライセンス登録失敗時：NG、ライセンス失敗を示します。



アクセスエラーメッセージ画面

アクセス権がないフォルダを開こうとした場合に表示されます。

環境エラーメッセージ画面

環境確認処理でエラーが発生したとき表示します。本ソフトが使用不能となっていることを示します。

実行 AES モジュールに関する記載

Issue Date: 29/07/2002

以上