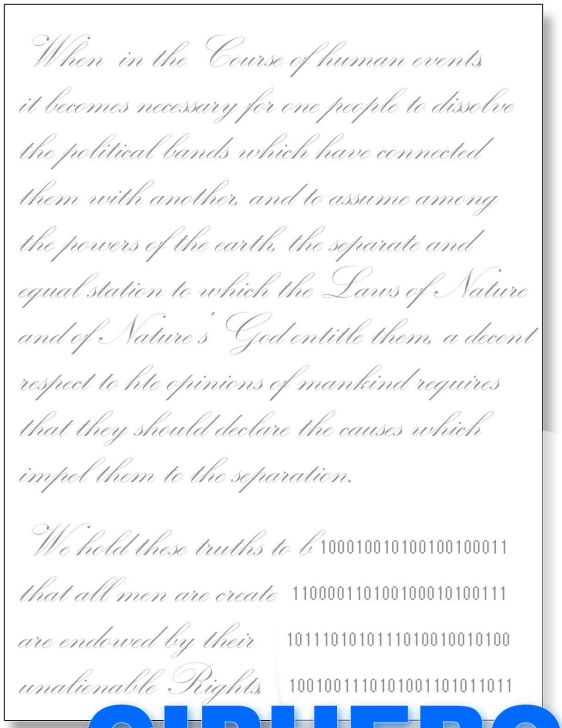


CIPHERON Standard® X Edition

ユーザーズマニュアル(Windows®版)

ChaosWare Inc.

MAN-CSTDX-V20-20080304

はじめに

『CIPHERON Standard X Edition』とは

『CIPHERON Standard X Edition』(サイファロン　スタンダード X エディション)は、いつでも、どこでも、誰とでも、安心して機密性のあるデータを、ユーザーフレンドリーに交換することを実現するファイル暗号化ソフトです。

『CIPHERON Standard X Edition』には VSC(Vector Stream Cipher:ベクトル型ストリーム暗号)という暗号化エンジンが搭載されています。VSC は、世界で初めて任意の次元のランダムなベクトルを発生するアルゴリズム(カオス写像ベクトル)を用いて、非常に軽量かつ高速でデータの暗号化・復号化を可能にしました。また、現在最も普及している公開鍵暗号方式 RSA を併用し、他者との暗号のやりとりをする際のセキュリティを高めています。

『CIPHERON Standard X Edition』は、暗号化／復号化に用いる鍵ファイルを USB メモリなどに保存することで、これを物理的な“鍵”とすることができます。“鍵”をコンピュータに挿しこむことでファイルの暗号化／復号化をすることができるようになります。

2005 年 4 月 1 日より、個人情報保護法が施行され、民間企業においても個人の情報を管理する義務が課せられました。『CIPHERON Standard X Edition』はまさに個人の情報を管理するのに適したツールです。また、個人の情報だけでなく、企業や研究機関における機密情報などもしっかりと保護することができます。

目 次

はじめに

目次

第１章　CIPHERON Standard X Edition の特徴と暗号化のしくみ　5

１－１ 暗号化とは ―― 5
１－２ 『CIPHERON Standard X Edition』の特徴 ―― 10
１－３ 『CIPHERON Standard X Edition』ご利用の例 ―― 12
１－４ 他の『CIPHERON』製品との互換について ―― 12

第２章　ソフトのインストールと初期設定 ―― 13

２－１ 動作環境 ―― 13
２－２ インストールの手順 ―― 13
２－３ 初回起動と初期設定 ―― 15

第３章　自分しか開けないファイルを作る ―― 18

３－１ 自分宛てにファイルを暗号化する ―― 18
３－２ 暗号化ファイルを復号化する ―― 19
３－３ 特定フォルダを自動的に暗号化／復号化する ―― 20

第４章　他人とのやりとり―宛先の登録 ―― 24

４－１ 宛先登録の手順 ―― 24
４－２ あなたが暗号化する側の場合 ―― 25
４－３ あなたが復号化する側の場合 ―― 27
４－４ 宛先リストの編集 ―― 28

第５章　他人とのやりとり―暗号化と復号化 ―― 33

５－１ 他人宛てにファイルを暗号化する ―― 33
５－２ 暗号化ファイルを復号化する ―― 35

第6章　他人とのサイズの大きいファイルのやりとり ―――― 41

6－1 暗号便の概要 ―――― 41
6－2 サイズの大きいファイルの送信する（CIPHERON で暗号化） ―――― 42
6－3 サイズの大きいファイルの送信する（暗号便で暗号化） ―――― 48
6－4 サイズの大きいファイルを受信する ―――― 53

第7章　アドバンストメニューを使う ―――― 58

7－1 アドバンストメニューを使う ―――― 58
7－2 アドバンストメニューの機能 ―――― 59
7－3 暗号化／復号化 ―――― 59
7－4 暗号化ファイルの履歴表示／転送 ―――― 65
7－5 ファイルの抹消 ―――― 68
7－6 鍵セットの生成 ―――― 69

第8章　拡張機能 ―――― 70

8－1 公開鍵の認証 ―――― 70
8－2 認証鍵の登録 ―――― 71
8－3 暗号化の詳細設定 ―――― 72
8－4 宛先リストからの暗号化 ―――― 74
8－5 一時復号化 ―――― 75
8－6 右クリックメニュー ―――― 76
8－7 鍵の選択 ―――― 79

第9章　環境設定 ―――― 80

9－1 オプション設定 ―――― 80
9－2 言語の選択 ―――― 82
9－3 ソフトのアンインストール ―――― 82

第10章　その他 ―――― 83

10－1 鍵の管理は USB メモリで ―――― 83
10－2 メールソフトについて ―――― 84

鍵のバックアップについて ——— 85

Q&A ——— 87

トラブルシューティング ——— 91

索引

カオスウェアについて

第1章　CIPHERON Standard X Edition の特徴と暗号化のしくみ

この章では『CIPHERON Standard X Edition』の特徴を説明し、暗号化のしくみについて解説します。

１－１　暗号化とは

『CIPHERON Standard X Edition』は、ファイルの暗号化／復号化を行うソフトです。暗号化とは、他人に内容がわからないように、データの内容を隠すことです。決められた人しかデータを元に戻すことはできません。暗号化されたデータを元に戻すことを復号化といいます。

一般的に、暗号化のやりとりは安全性を高めるためにやや複雑な手順を踏む必要がありますので、わかりやすく図で説明していきます。


『Ｃｉｐｈｅｒｏｎ』
はパスワード
のかわりに
その鍵で暗号化
するのよ
パスワード
じゃなくて、
鍵で…
ですか？
そうよ。正確には
鍵と錠前だけどね
施錠＝暗号化
開錠＝復号化
簡単に言うと錠前を
かけることを暗号化と
言って、鍵を開けること
を復号化と言うのよ
実際にやって
みましょうか
え？

これが公開鍵ファイルです

これが秘密鍵ファイルです

Check ！！

他人との暗号化については

→4章 p.24-

5章 p.33-

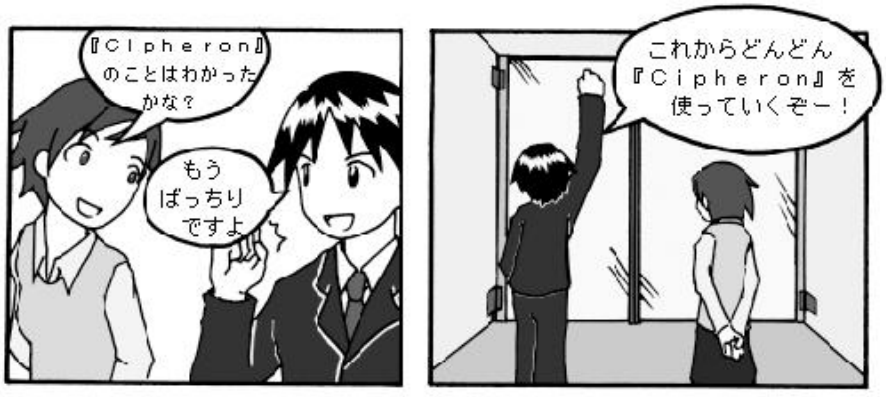

そしてこの箱の中には
ファイルの他に…
A.name
A.name
私の公開鍵と
私のサインの入った
カードが入っています
あなたがこれを
受け取って
自分の秘密鍵
で開錠して
サインを確認
することで
A.name
差出人が
私だと
わかるでしょ
そして
さらに
そこにあなた(B)の
サインを書き込むと…

一度暗号化のやりとりをした相手との間にできる専用鍵のことを、“認証鍵”と呼びます。その相手と二回目以降にやりとりをする場合は、公開鍵ではなくこちらの認証鍵で暗号化します

anata))aite-auth.vpub
CIPHERON公開鍵
1 KB

これが認証鍵です

署名～認証鍵の作成は、暗号化ファイルのやりとりをする上で、行われます
詳しくは
→5－2 p.35-



１－２ 『CIPHERON Standard X Edition』の特徴

（1）すぐれたセキュリティ機能

『CIPHERON Standard X Edition』はカオスウェア社が独自に開発した秘密鍵暗号方式VSC(Vector Stream Cipher)と、公開鍵暗号方式RSAを用いた二重のセキュリティシステムでデータを暗号化するため、極めて強固な暗号化ファイルを作成することが可能です。

（2）パスワードを用いない鍵と重要データの完全分離の実現

一般的な暗号化ソフトでは、パスワードにより復号化を行っています。しかし、多くの場合、パスワードは本人が覚えられるような単純なフレーズであるため、ワードアタックなどの手段によって看破されてしまうことも少なくありません。また、複雑なパスワードでは、本人がそれを忘れてしまうこともあります。忘れないように何かに書き留めておくとしたら、そちらのほうが危険といえます。
『CIPHERON Standard X Edition』は、パスワードによる復号化ではなく、“鍵ファイル”をパスワードの代わりに用いています。そのため、この“鍵ファイル”を保持していればパスワードを覚える必要もなく、また、パスワードを看破されることもありません。“鍵ファイル”を USBメモリなどの外部記憶装置に保存することで、USBメモリを“鍵”のようにすることができます。鍵となるUSBメモリをコンピュータに接続していない状態ではソフトの使用ができず、ファイルの暗号化／復号化もできなくなります。

（3）特定フォルダの自動暗号化／復号化

『CIPHERON Standard X Edition』は、オプション設定でソフトの終了時、または“鍵”(USBメモリ等)をコンピュータから抜いた際に、特定のフォルダを自動的に暗号化することができます。そのフォルダに入っているファイルは、“鍵”が挿さっていない限り常に暗号化されているため、万が一コンピュータを盗難されても、そのフォルダ内のデータが流出することはありません。機密ファイルの保管に適しています。

Check ！！

暗号化ファイルの履歴管理・転送については

→7－4 p.65-

（4）暗号化ファイルの履歴管理

暗号化したファイルに、誰が、いつ、どのような操作をしたか(閲覧、更新、復号化など)という履歴情報をつけることが可能です。そのため、履歴情報を確認することで、より強固な暗号化ファイル管理をすることが可能です。そのため、特定のグループでファイルを共有しながら、しっかりとした情報管理をすることができます。

（5）1 対多の同時暗号化が可能

『CIPHERON Standard X Edition』は、1対1の暗号化・相互認証に加え、1対多の暗号化・相互認証を可能にしています。つまり、1 人の送信者は、特定の 1 人もしくは複数の受信者のみが復号化できるように指定し、暗号化のやりとりをすることができます。また、暗号化ファイルの転送機能により、より多数の人とのやりとりがスムーズに行えます。

（6）宛先リストによるグループ管理が可能

Check ！！

宛先リストについては

→4－4 p.28-

『CIPHERON Standard X Edition』では、暗号化の相手をリスト管理することができるため、暗号化の相手をグループに分けての管理が容易です。宛先リストを有効活用することで、部署単位や取引先単位など、1 対多数の暗号化のやりとりに、さらに柔軟性を持たせることが可能です。

（7）暗号化ファイルの復号化有効期限の設定

Check ！！

復号化できる期限をつける

→8－3 p.72-

暗号化時に復号化有効期限を設定することができます。このため、ファイルを暗号化した時に、設定した復号化有効期限を過ぎていた場合、そのファイルを復号化することはできません。そのため、納品書などの危急を要するファイルに復号化有効期限を設定することで、そのファイルを確実に先方に見ていただくことができます。

（8）電子シュレッダー機能

不要になったファイルを電子シュレッダーにかけることができます。電子シュレッダーにかけられたファイルはランダムに暗号化され、二度と復号化できないような形にしてから削除されます。通常のファイルはもちろん、個人情報などが含まれているファイルや、コンピュータの廃棄の際の、ハードディスク初期化などにお使いいただけます。

１－３ 『CIPHERON Standard X Edition』ご利用の例

（1）企業・その他研究機関でのご利用の例

顧客情報や社外秘、人事データ、カルテなど個人や企業の情報も、『CIPHERON Standard X Edition』を利用することによって安全に管理することができます。

（2）教育機関でのご利用の例

教育機関において、学級の児童・生徒に一斉に重要なファイルを送信することができます。その際、無償の『CIPHERON Initiative』を併用することにより、児童・生徒の家庭に経済的な負担をかけずにご利用いただけます。

（3）本人以外が閲覧することのできないファイルを作成する

Check ！！

自分しか開けないファイルを作る

→3章 p.18-

『CIPHERON Standard X Edition』は他者とのやりとりにおける暗号化だけではなく、自分自身しか開けないファイルを作ることも可能です。これにより、コンピュータを奪われることがあっても重要な情報の流出を防ぐことができます。また、特定フォルダの自動暗号／復号機能を使うことで、より安全なデータの管理が可能です。

１－４ 他の『CIPHERON』製品との互換について

『CIPHERON Standard X Edition』は、他のすべての『CIPHERON』製品、および姉妹製品である『VSC-P2P』と暗号化ファイルを交換することができます。また、『CIPHERON』製品を持っていない相手に暗号化ファイルを送りたい場合に、無償の『CIPHERON Initiative』をダウンロードしていただき、相手に負担をかけずにファイルのやりとりをすることができます。

また、弊社のファイル暗号化ソフト『VSC-P2P』とも互換性があるので、鍵および暗号化ファイルの交換が可能です。

なお、無償の『CIPHERON Initiative』は弊社のホームページからダウンロードできます（http://www.chaosware.com/）。

第2章　ソフトのインストールと初期設定

この章では『CIPHERON Standard X Edition』のインストールと初期設定について説明します。

自動的に CD-ROM が起動されない場合は、「マイコンピュータ」から直接起動してください

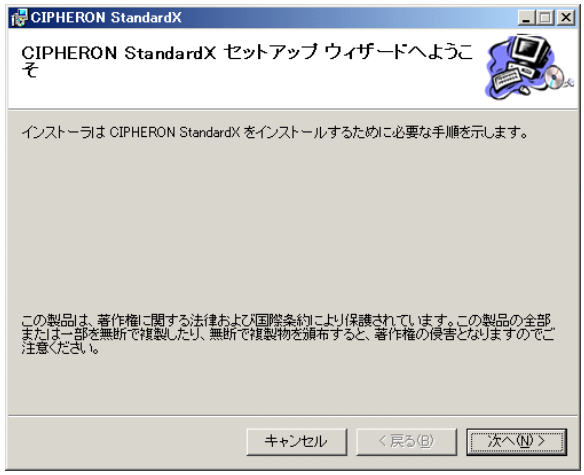
2－1　動作環境

『CIPHERON Standard X Edition』は、「Windows2000(SP4 以降)」および「Windows XP」上で動作します。2MB 以上のハードディスクの空き容量、128Mbyte 以上のメモリが必要です。

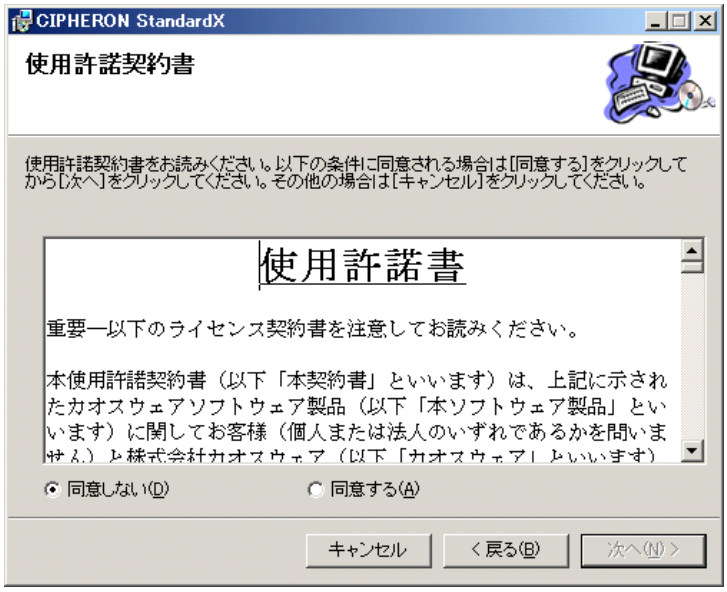
『CIPHERON Standard X Edition』をインストールするには、**CD-ROMドライブ**が必要です。また初回起動時のみ、ソフトウェアのライセンス登録を行うためにインターネットへの接続が必要です。

2－2　インストールの手順

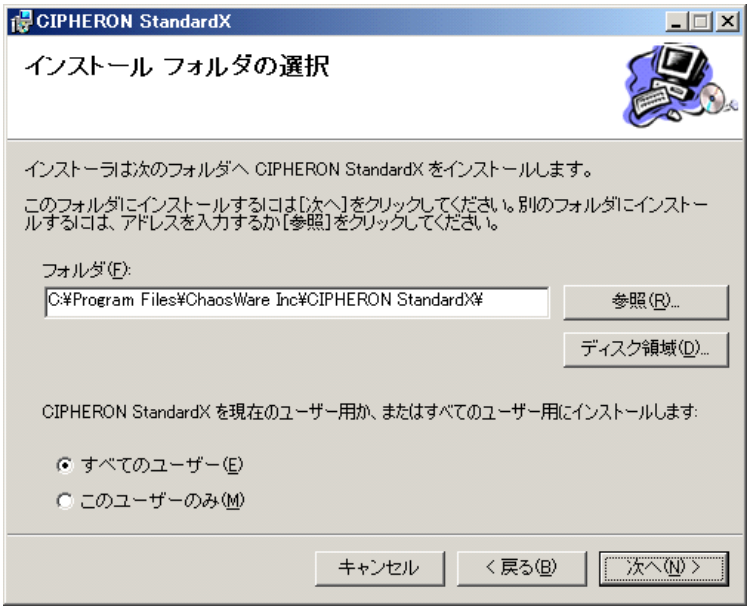
『CIPHERON Standard X Edition』の CD-ROM をドライブにセットすると、次の画面が表示されます。**[次へ]**をクリックしてください。



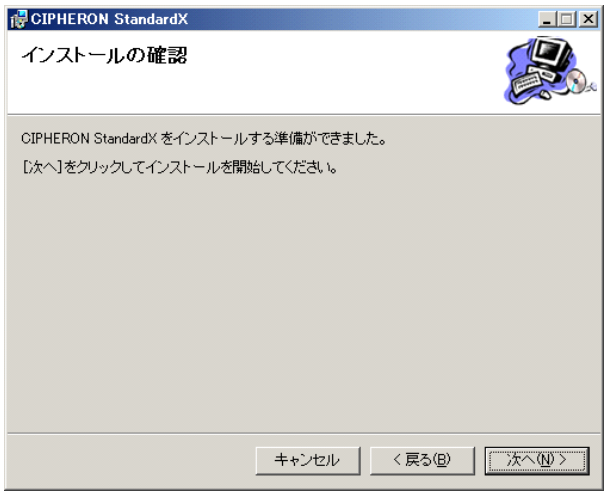
次に、プログラムをインストールするにあたっての使用許諾書が表示されます。
内容をご確認いただいた上、同意いただける場合は[同意する]へチェックを入れた後、[次へ]をクリックしてください。



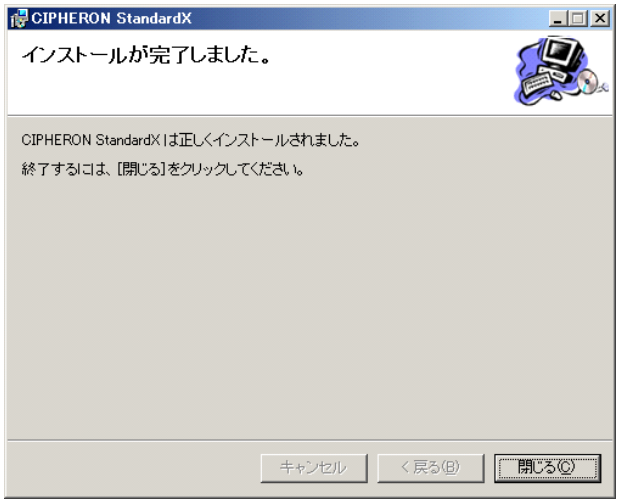
次に、プログラムをインストールする場所を指定します。特に指定する必要がなければそのまま**[次へ]**をクリックしてください。



次に、インストールの開始の確認を求められますので、特に問題がなければそのまま[**次へ**]をクリックしてください。

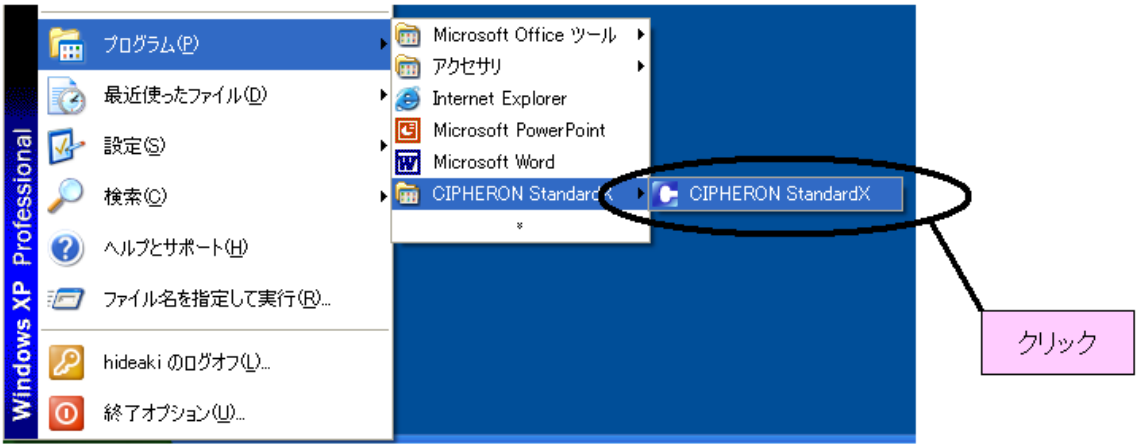


一通りのファイルのインストールが完了すると以下のダイアログが表示されます。
表示が行われたら[**閉じる**]をクリックして、インストールを終了します。



２－３　初回起動と初期設定

アプリケーションの起動はスタートメニューから行います。



初回起動時は“**シリアル番号**”と“**パスワード**”が要求されますので、同封されている“**シリアル番号**”と“**パスワード**”を記入します。

ソフトウェアライセンスの登録にはインターネットへの接続が必要です。

Check ！！

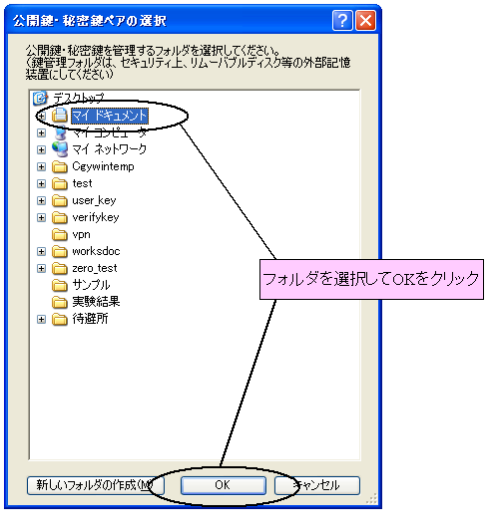
CIPHERON はインターネットへの接続を Internet Explorer の設定を参照して行います。

Check ！！

鍵管理フォルダは USB メモリ等の外部記憶装置におこなうことをお勧めします

→10－1 p.83-

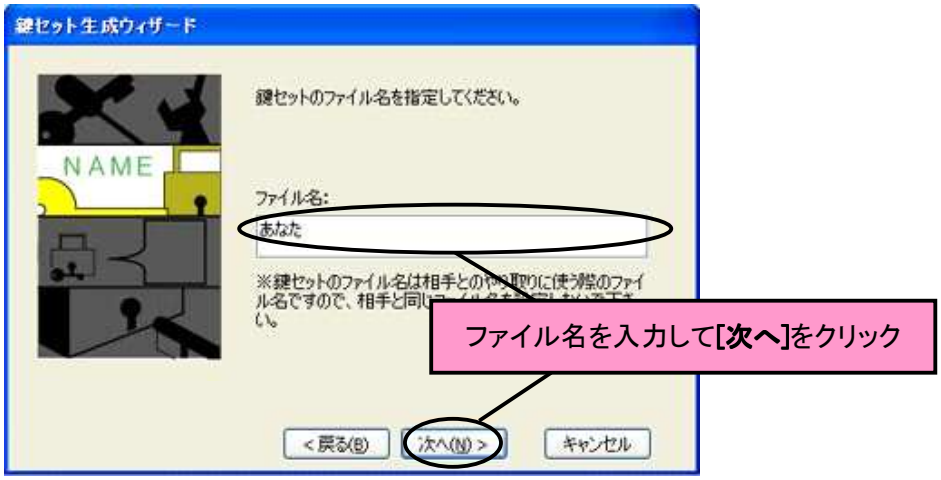
“シリアル番号”と**“パスワード”** を入力して[OK]をクリックすると、鍵管理を行うフォルダの選択ダイアログが表示されます。



以下のような暗号化／復号化に使う鍵セットの生成画面に移行します。ダイアログをよく読み、**[次へ]**をクリックしてください。

鍵ファイル名は、一度設定したら変更できません。またエクスプローラ上で鍵ファイル名を変更すると、復号化できなくなるので、おやめください

鍵のファイル名をつけます。ここでつけた名前が、エクスプローラ上の鍵の名前になります。名前を入力したら**[次へ]**をクリックしてください。



次に、鍵セットの持ち主の情報を登録します。あなたの名前と E メールアドレスを入力して[次へ]をクリックしてください。

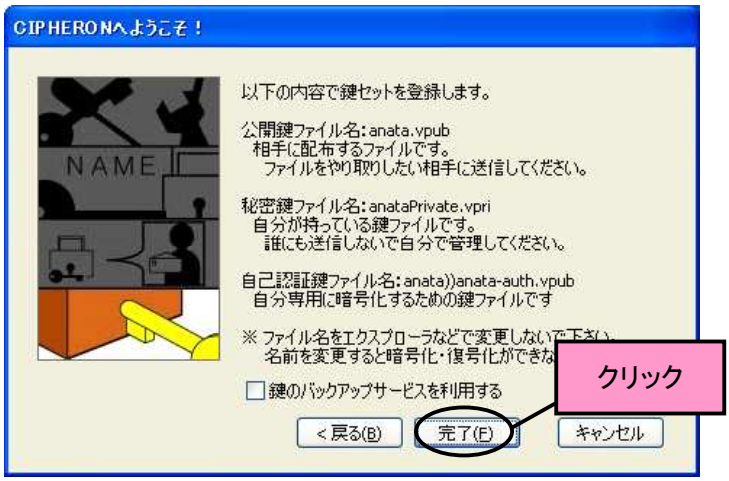
持ち主の名前と E メールアドレスは入力しなくても構いません

Check ！！

鍵の持ち主の情報と E メールアドレスはオプションで変更できます。

→9－1　p.80−

以下のような画面が表示されますので、内容をよく読み、[完了]をクリックすれば鍵の生成は終了し、初期設定も完了です。



Check ！！

なお、新しい鍵セットを生成したい場合は

→7－6　p.69−

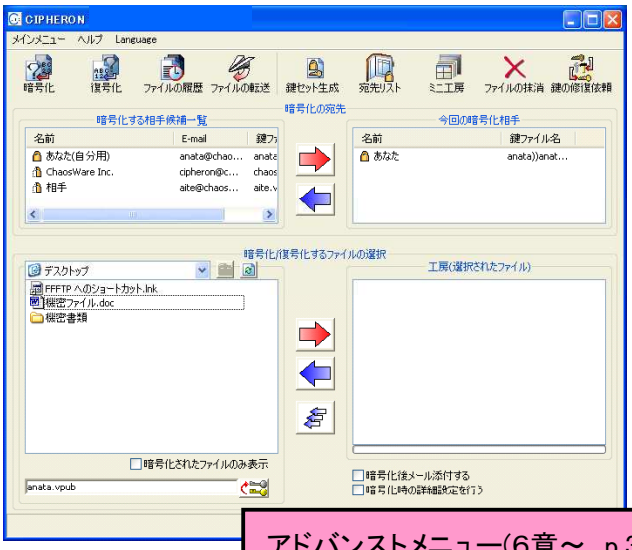
Check ！！

バックアップサービスについては

→p.85−

初期設定が完了すれば、すぐにアプリケーションをお使いいただくことができます。

ミニ工房(3章～　p.17−)



アドバンストメニュー(6章～　p.39−)

第3章　自分しか開けないファイルを作る

この章では自分専用の暗号化ファイルの作り方を説明します。

3－1　自分宛てにファイルを暗号化する

“自分宛て”とは、自分だけが復号化できるような暗号化ファイルを作ることです。
大きく分けて二つの手順があります。

(1)暗号化したいファイルをドラッグする
(2)暗号化を実行する

(1)暗号化したいファイルをドラッグする

暗号化したいファイルを選択し、ミニ工房にドラッグしてください。

(2)暗号化する

ファイルをドラッグすると、以下のようなダイアログが表示されます。暗号化するファイルの出力先を指定したり、復号化できる期限をつけるなどの詳細設定をする必要がなければ、そのまま**[暗号化保存]**をクリックしてください。

以下のようなダイアログが表示されれば、暗号化は終了です。

Check ！！

暗号化ファイルの出力先を特に指定したい場合は

→8－3 p.72-

特に暗号化ファイルの出力先を指定していなければ、暗号化ファイルは元のファイルと同じ場所に保存されます。

3－2 暗号化ファイルを復号化する

“復号化”とは、暗号化ファイルを元のファイルに戻すことです。復号化したいファイルをミニ工房にドラッグしてください。

以下のようなダイアログが表示され、復号化は終了です。復号化元のファイルがあった場所にファイルが出力されます。

３－３　特定フォルダを自動的に暗号化／復号化する

『CIPHERON Standard X Edition』起動時や終了時に、指定したフォルダを自動的に暗号化／復号化することができます。指定したフォルダに重要なファイルを保存しておくことで、『CIPHERON Standard X Edition』が起動していないとき、あるいは鍵管理している USB メモリなどの外部記憶装置が接続されていないときは、常に暗号化されている状態を保っています。

自動暗号化／復号化が開始される条件は、以下の通りです。

☆自動暗号化

ソフトが起動しているときに、鍵が入っている USB メモリが抜かれた

ソフトを終了した

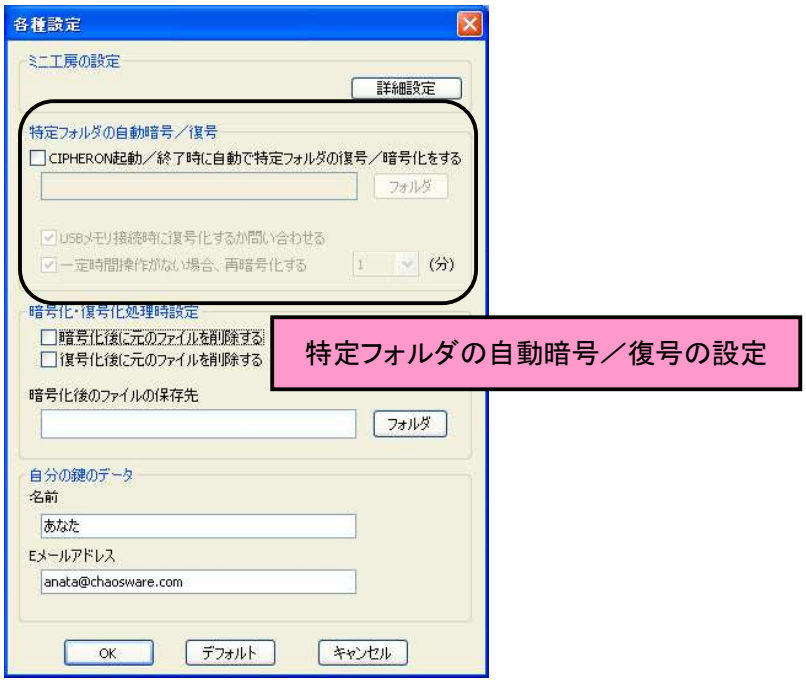
一定時間コンピュータの操作が行われなかった

☆自動復号化

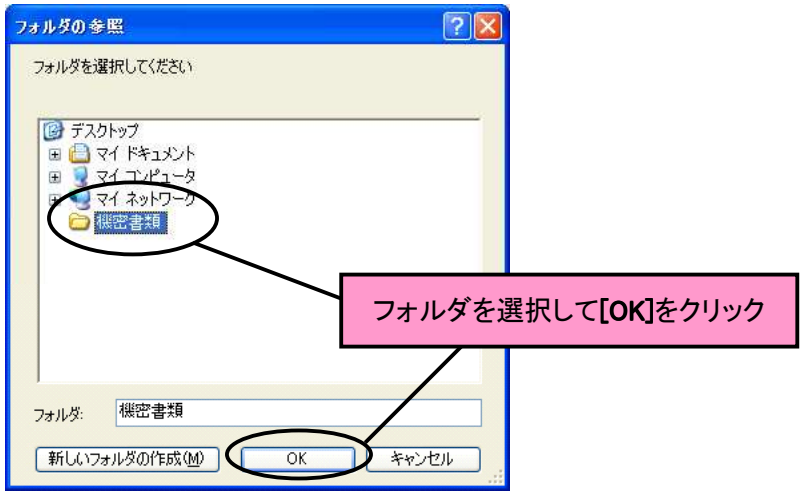
ソフトが起動しているときに、鍵が入っている USB メモリが接続された

鍵が入っている USB メモリが接続された状態でソフトを起動した

特定フォルダの自動暗号化／復号化はオプションの各種設定で設定します。



“特定フォルダの自動暗号／復号”にチェックを入れます。次に[**フォルダ**]をクリックして、自動的に暗号化／復号化したいフォルダを選択します。



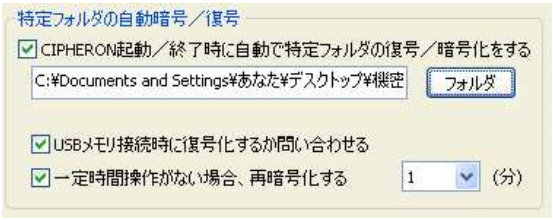
選択をしたら[OK]をクリックしてください。

次に、“USB メモリ接続時に復号化するか問い合わせる”、“一定時間操作がない場合、再暗号化する”の設定を行います。

フォルダ内のファイル数が多い場合、復号化に時間がかかることがあるので、場合に応じて選んでください

“USB メモリ接続時に復号化するか問い合わせる”にチェックを入れると、USB メモリ接続時に、以下のようなダイアログが表示されるようになります。[**はい**]をクリックすると、フォルダの自動復号が開始されます。[**いいえ**]をクリックすると、フォルダは自動的には復号化されません。初期設定では、この機能はオンです。

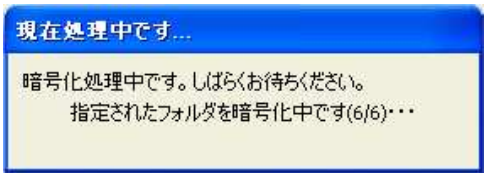
“一定時間操作がない場合、再暗号化する”にチェックを入れると、一定時間コンピュータを操作しなかった場合に、指定したフォルダが自動的に暗号化され、ソフトが終了します。もし指定されたフォルダ内のファイルを他のアプリケーションで編集中だった場合は、そのファイル以外がすべて暗号化されますが、編集中のファイルは暗号化されません。初期設定では、この機能はオンで、設定された時間は 1 分です。



すべての設定が終了したら、[OK]をクリックして設定を有効にしてください。

＜自動暗号化＞

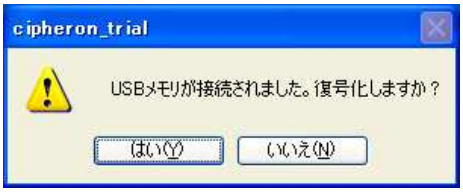
ソフトを起動中に、鍵管理フォルダのある USB メモリをコンピュータから抜く、ソフトを終了する、あるいは設定した時間以上コンピュータの操作を行わなかった場合、画面の右下に、以下のようなダイアログが表示され、指定したフォルダの暗号化が開始されます。



このダイアログが画面から消えた時点で暗号化はすべて完了です。指定したフォルダ内のファイルがすべて暗号化されているか確認してください。

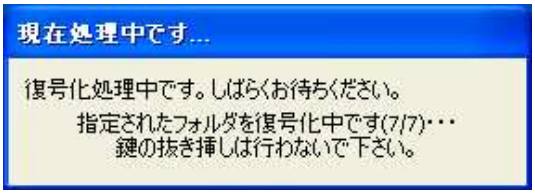
＜自動復号化＞

ソフトを起動したとき、あるいはソフトが起動しているときに鍵管理フォルダのある USB メモリをコンピュータに挿入すると、復号化を行うかどうかのダイアログが表示されます。



“USB メモリ接続時に復号化するか問い合わせる”にチェックがない場合は、このダイアログは表示されず、ただちに復号化が開始されます

[はい]をクリックすると、以下のようなダイアログが表示され、指定したフォルダの自動復号化が開始されます。



復号化中は、絶対に USB メモリを抜かないでください。メモリやファイルが壊れる可能性があります

このダイアログが消えて、『CIPHERON Standard X Edition』の起動画面が表示された時点で復号化は終了です。指定したフォルダ内のファイルがすべて復号化されていることを確認してください。

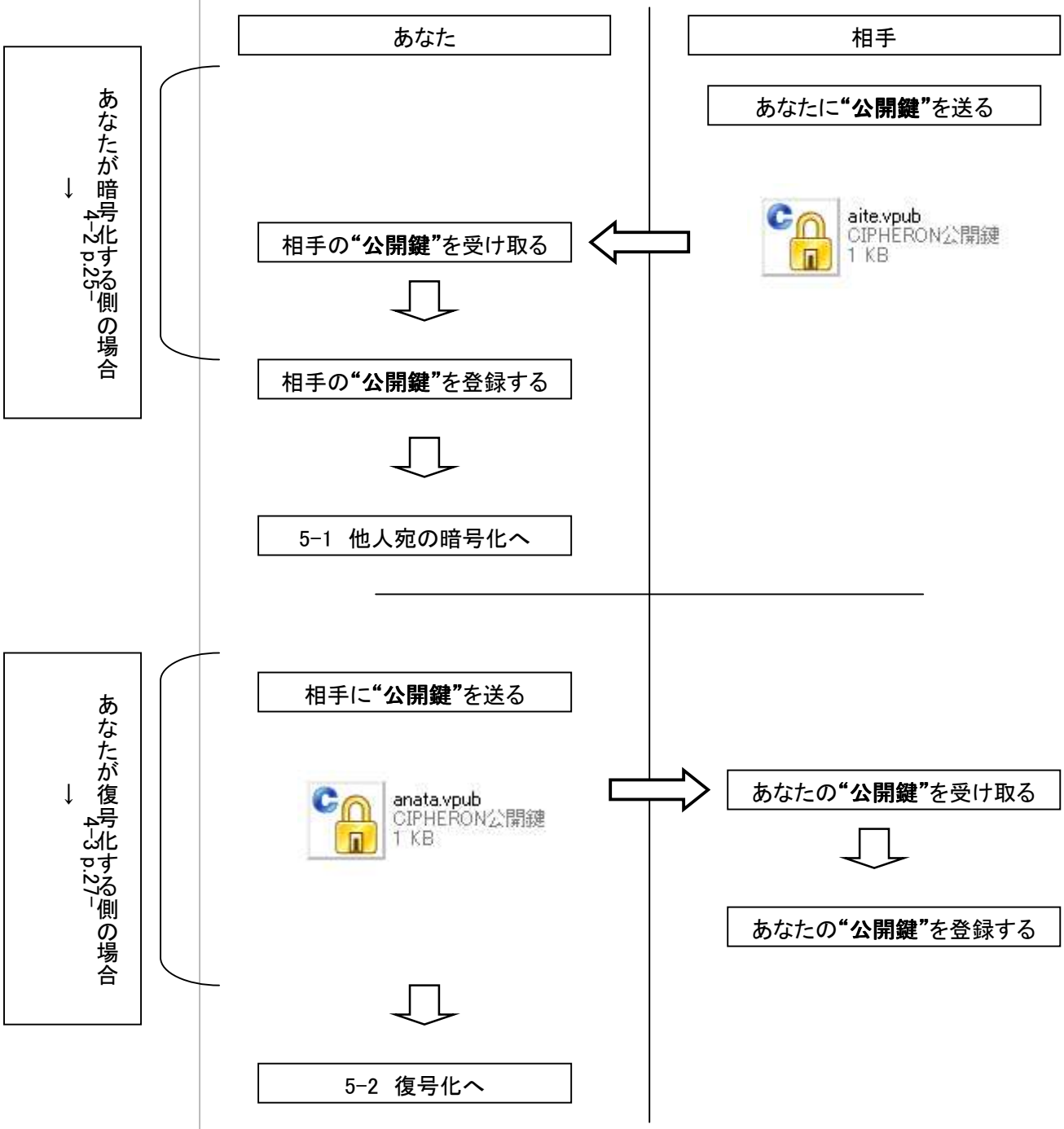
復号化を行うかどうかのダイアログで**[いいえ]**をクリックすると、復号化は行われません

第4章　他人とのやりとり―宛先の登録

この章では他人と暗号化ファイルをやりとりする際の、最初の手順の説明をします。

４－１　宛先登録の手順

他人と暗号化ファイルのやりとりをする場合、相手の宛先をまず登録しなくてはなりません。宛先登録の手順は以下の図の通りです。なお、すでに登録されている相手とやりとりをする場合は、これらの手順を行う必要はありません。



４－２　あなたが暗号化する側の場合

あなたが暗号化ファイルを誰かに送るときには、まず相手の”公開鍵”を宛先に登録します。公開鍵の登録は大きく分けて二つの手順があります。

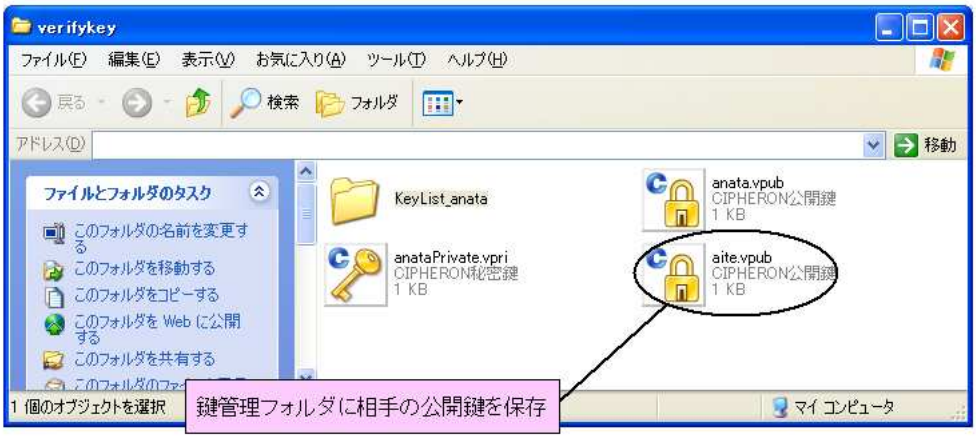
（1）相手の公開鍵を受け取る

（2）受け取った公開鍵を「宛先リスト」に登録する

このアイコンが公開鍵ファイルです

（1）相手の公開鍵を受け取る

まず、暗号化する相手の公開鍵を受け取らなくてはなりません。メールで受け取るなどをして、相手の公開鍵を鍵管理フォルダに保存します。



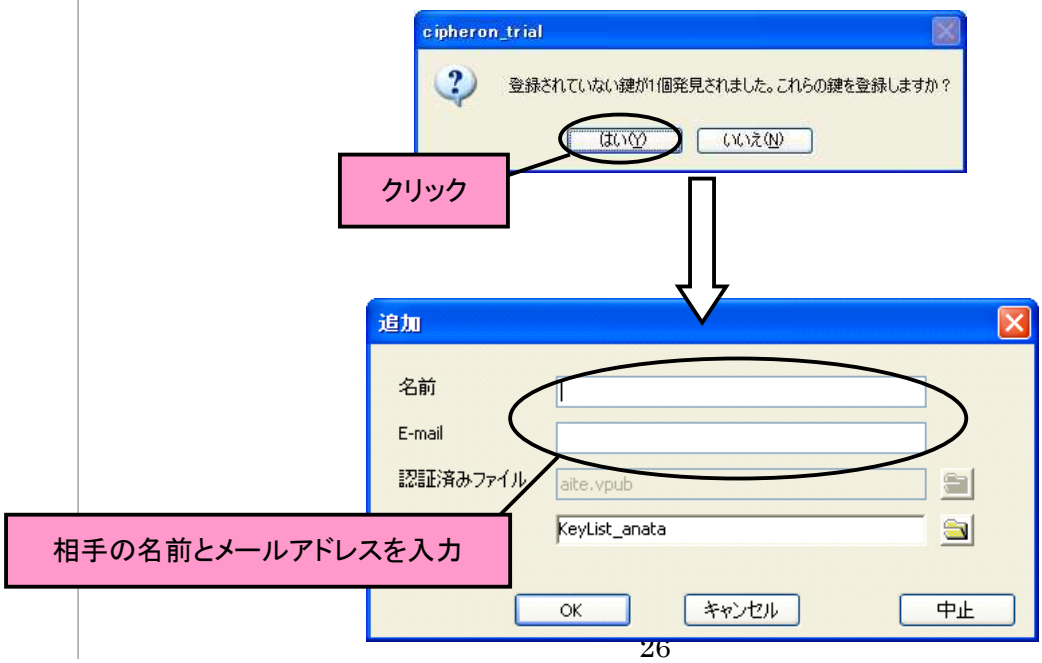
Check　！！

手動で宛先リストに登録する場合は

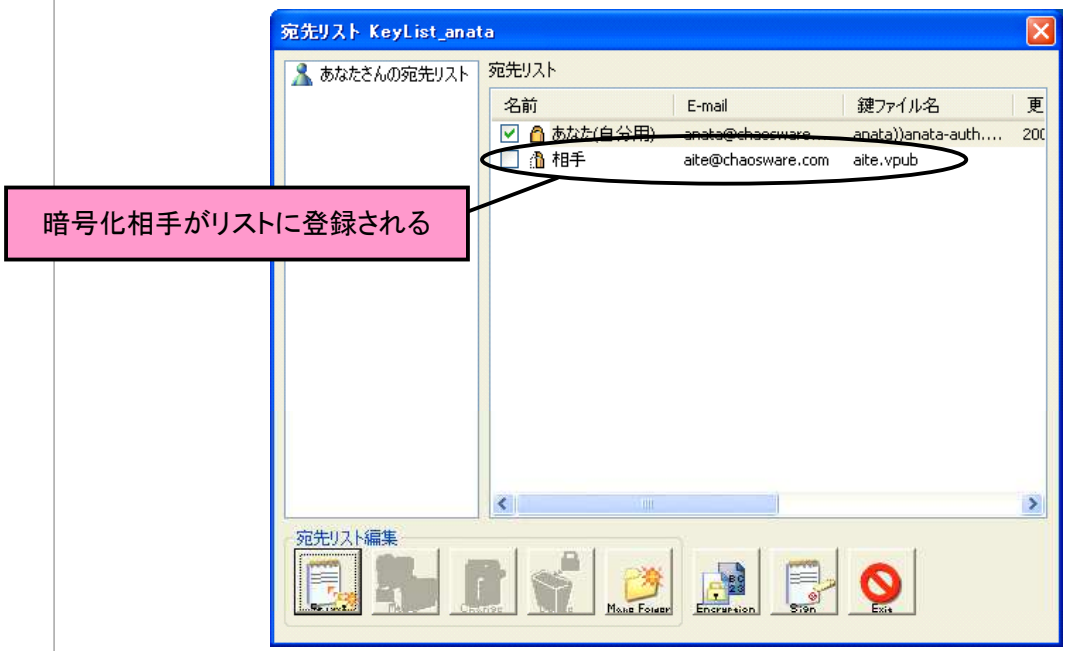
→4－4　p.28-

(2)受け取った公開鍵を「宛先リスト」に登録する

鍵管理フォルダに受け取った公開鍵があることを確認し、ソフトを起動してください。以下のようなダイアログが表示されますので、鍵の持ち主(相手)の名前と E メールアドレスを入力し、[はい]をクリックしてください。



以下のようなダイアログが表示されれば、登録完了です。宛先リストに登録されているかを確認してください。登録されていれば、暗号化ファイルを送信することができます。**「５－１ 他人宛てにファイルを暗号化する」**(p.33-)へ進んでください。



４－３　あなたが復号化する側の場合

相手から暗号化ファイルを受け取るときには、あなたの“公開鍵”を相手に登録してもらわなくてはなりません。
公開鍵の送付には、メールソフトを起動し、あなたの公開鍵ファイルをメールに添付して送信してください。

絶対に秘密鍵(このアイコン)は送信しないでください

４－４　宛先リストの編集

Check　！！

自分用の宛先は宛先リストから変更することはできません。変更したい場合はオプションから行ってください

→９－１　p.80-

新しい宛先の手動による追加や、すでに登録されている宛先の登録内容を変更したいときは、宛先リストから行います。

宛先リストでは以下のことができます。

（1）宛先の新規登録

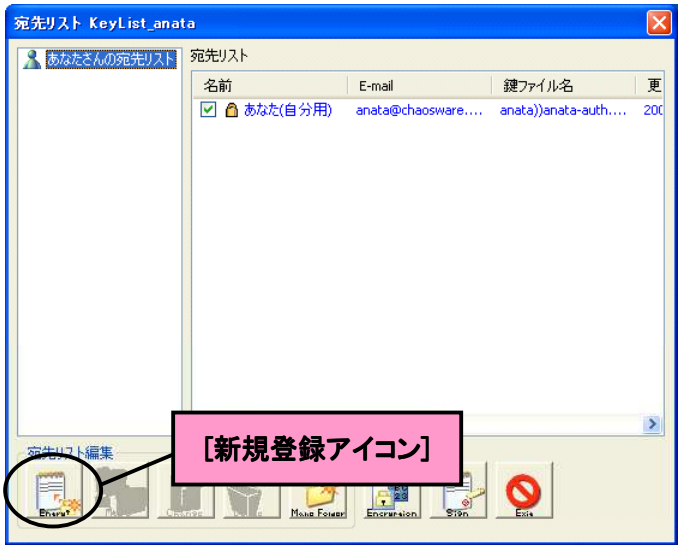
（2）登録内容の変更

（3）宛先のグループ分け

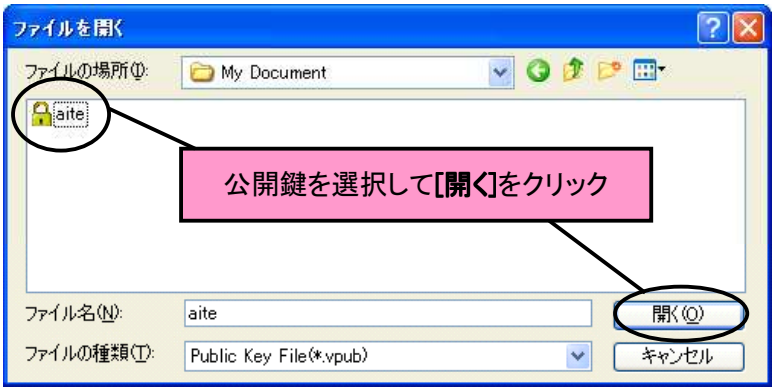
（4）宛先の削除

（1）宛先の新規登録

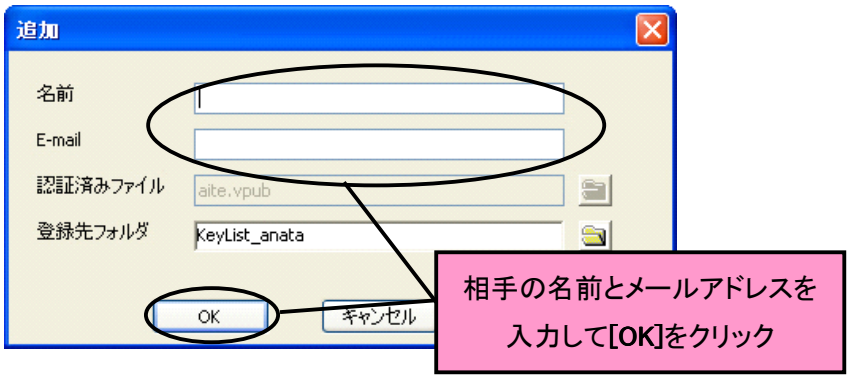
鍵管理フォルダに相手から送られた公開鍵がない場合は、手動で宛先リストに登録する必要があります。**[新規登録アイコン]**をクリックしてください。



[新規登録アイコン]をクリックすると、以下のような画面が表示されます。登録したい公開鍵を選択し、**[開く]**をクリックしてください。

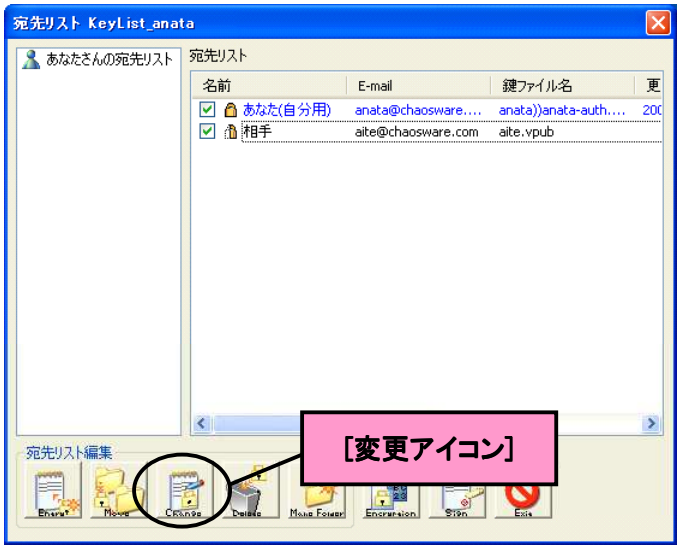


[開く]をクリックすると、登録内容が表示されます。鍵の持ち主(相手)の名前やＥメールアドレスを入力し、[OK]をクリックしてください。登録は完了です。



(2) 登録内容の変更

登録されている宛先の名前や Ｅ メールアドレスを変更します。変更したい宛先のチェックボックスにチェックを入れ、[**変更アイコン**]をクリックしてください。

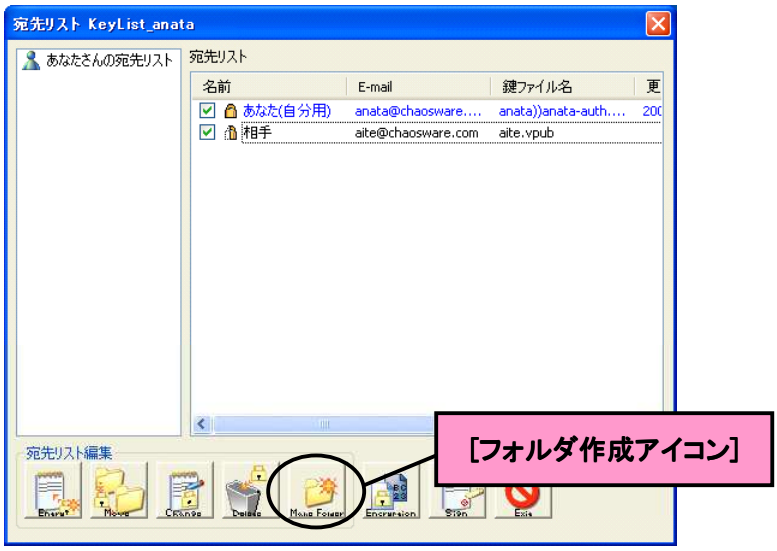


[**変更アイコン**]をクリックすると、以下のような画面が表示されます。登録内容の変更が終了したら、[OK]をクリックしてください。登録内容が更新されます。

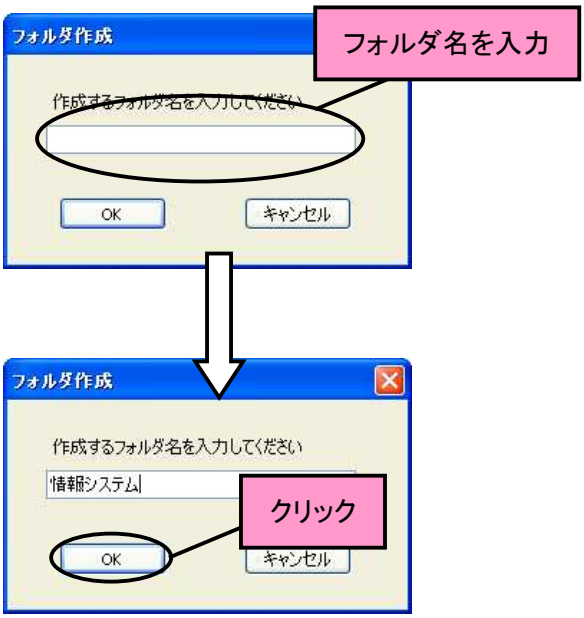
(3)宛先のグループ分け

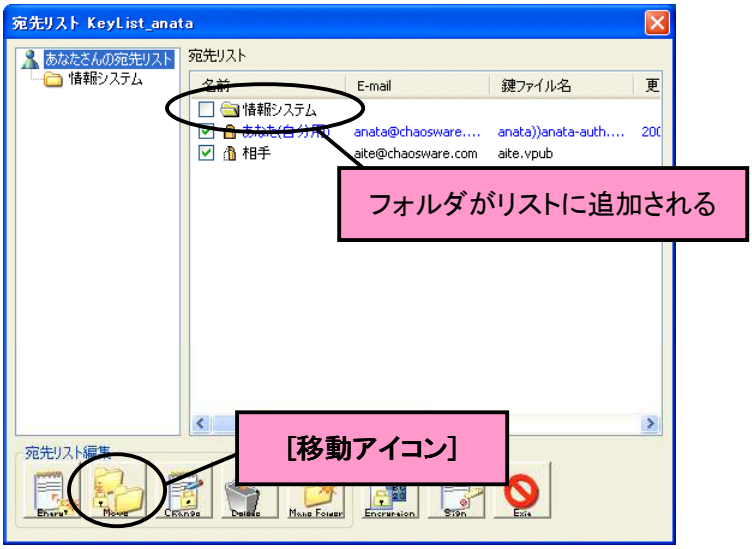
暗号化の相手が増えると、暗号化する相手のグループ分けをする方が便利です。

まず、暗号化相手のグループのフォルダを作成します。[**フォルダ作成アイコン**]をクリックしてください。



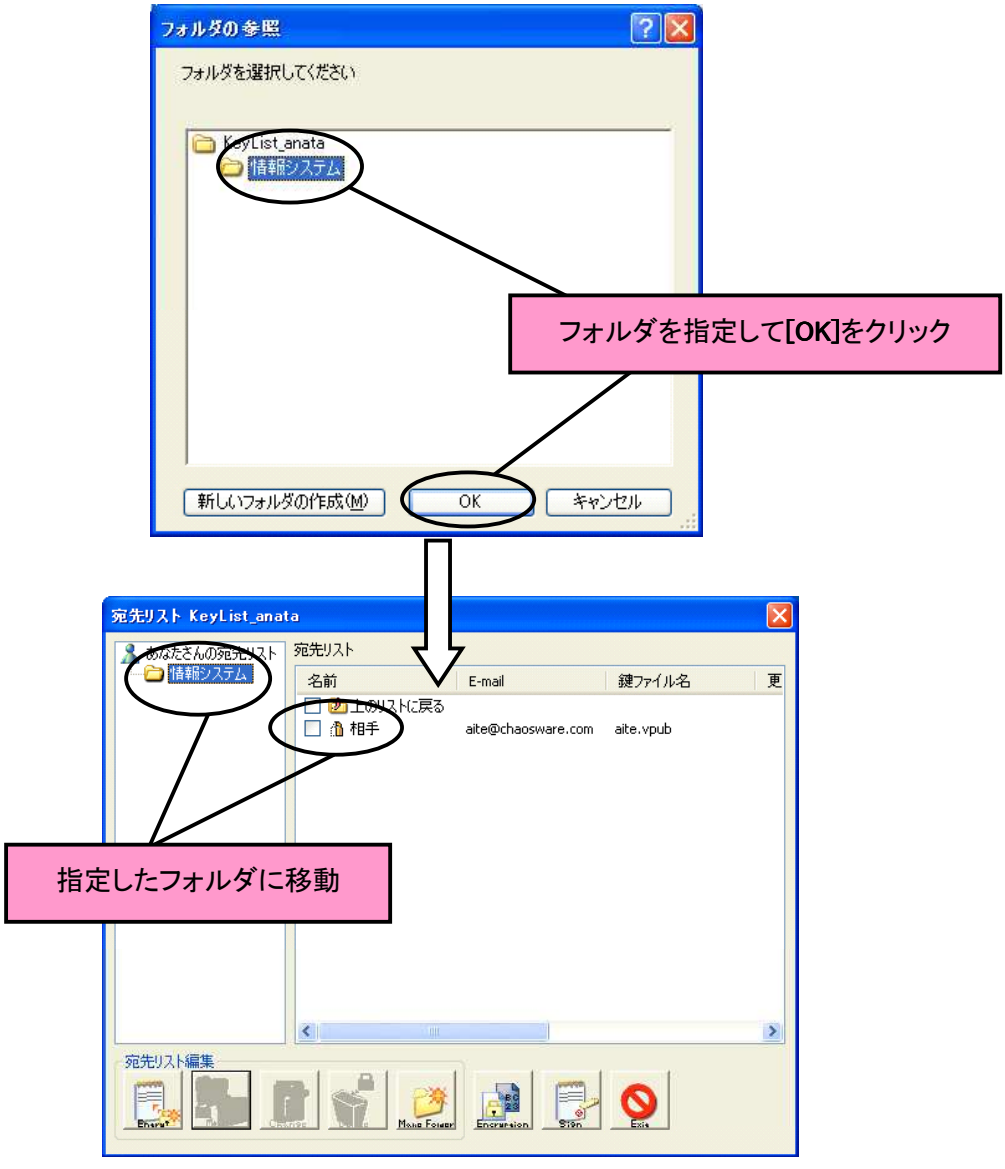
次のようなダイアログが表示されるので、フォルダの名前を入力して[OK]をクリックしてください。





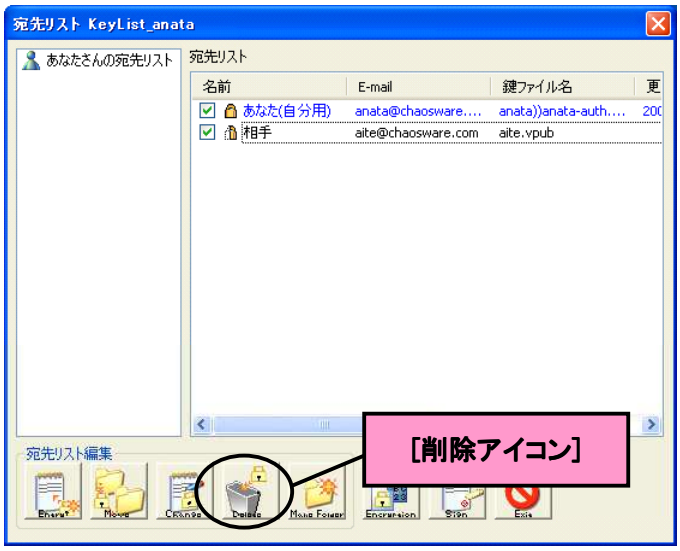
リストに作成したフォルダが追加されます。次に、作成されたフォルダに宛先を移動します。移動したい宛先のチェックボックスにチェックを入れ、**[移動アイコン]**をクリックしてください。

[移動アイコン]をクリックすると、以下のような画面が表示されます。移動先のフォルダを選択し、[OK]をクリックしてください。選択された宛先が、指定したフォルダに移動します。

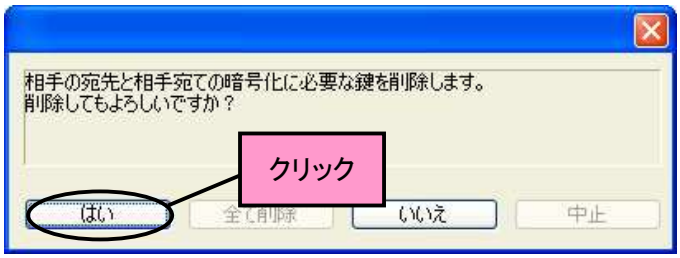


(4)宛先の削除

不必要になった宛先を削除することができます。削除したい宛先にチェックを入れて、**[削除アイコン]**をクリックしてください。



次のようなダイアログが表示されるので、**[はい]**をクリックしてください。選択された宛先が削除されます。



一度削除した宛先を元に戻すことはできません。公開鍵の登録からやりなおす必要があります

第5章　他人とのやりとり―暗号化と復号化

この章では、4章に引き続き、他人と暗号化ファイルのやりとりをする作業について説明します。宛先の登録を行っていないと、他人との暗号化のやりとりをすることはできないので注意してください

5－1　他人宛てにファイルを暗号化する

“他人宛て”とは、相手が復号化できるような暗号化ファイルを作成することです。
大きく分けて手順は三つです。

(1)暗号化するファイルをドラッグする
(2)暗号化する相手を選択する
(3)暗号化する

Check ！！
暗号化の詳細設定については
→8－3　p.72-

(1)暗号化するファイルをドラッグする

暗号化したいファイルを選択し、ミニ工房にドラッグしてください。

(2)暗号化する相手を選択する

暗号化したいファイルをドラッグ＆ドロップすると、次のような画面が表示されます。暗号化の相手を選択し、[→]をクリックして右のボックスに入れます。

すでに右のボックスに入っている宛先を除きたい場合は、その宛先を選択し、[←]をクリックしてください

Check ！！

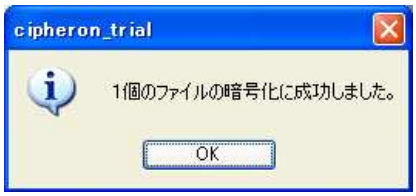
暗号化の詳細設定については

→8－3 p.72-

(3)暗号化する

暗号化するファイルの出力先を特に指定したり、復号化できる期限をつけるなどの暗号化の詳細設定をする必要がなければ、そのまま[**暗号化後保存**]をクリックします。

以下のようなダイアログが表示されれば、暗号化は終了です。



特に暗号化ファイルの出力先を指定していなければ、暗号化ファイルは元のファイルと同じ場所に保存されます。

！

暗号化したファイルを相手にすぐに送信したい場合は、[暗号化後メール添付]をクリックしてください

５－２　暗号化ファイルを復号化する

ファイルの復号化は、自分宛て暗号化ファイルの復号化と手順は同一です。ただし、暗号化のやりとりをする相手により、暗号化ファイルを復号化するときには、鍵の登録作業が途中で行われることがあります。

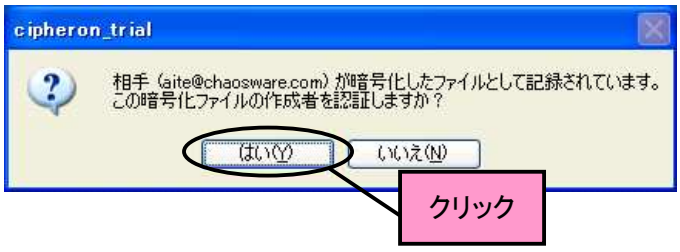
(1)公開鍵が登録されていない相手からの暗号化ファイルを復号化する
(2)公開鍵が登録されている相手からの暗号化ファイルを復号化する
(3)すでに何回かやりとりをしている相手からの暗号化ファイルを復号化する

このうち、(1)と(2)のときに、復号化中に鍵の登録作業があります。

Check ！！
ここで登録される鍵は、その相手宛てに暗号化するときの専用鍵(認証鍵)です
認証鍵については
→1－1　p.5-

(1)公開鍵が登録されていない相手からの暗号化ファイルを復号化する
相手からの公開鍵を宛先に登録していない場合の手順です。
復号化したいファイルをミニ工房にドラッグしてください。

ドラッグすると、一度ファイルの中身が表示されます。内容を確認して、暗号化ファイルを送ってきた相手が、本当に本人かどうか(誰かが相手になりすましていないか)を判断してください。ファイルを閉じると、次のようなダイアログが表示されます。本人であると判断した場合は[**はい**]をクリックしてください。



[はい]をクリックすると、鍵の登録ダイアログが表示されます。鍵の持ち主の名前やメールアドレスを確認し、[OK]をクリックしてください。

[OK]をクリック後、以下のようなダイアログが表示されたら鍵の登録は完了です。

鍵のファイル名が重複するのを避けるため、ファイル名には英数字が自動的に割り当てられます

鍵の登録が終了し、以下のようなダイアログが表示されたら復号化は完了です。復号化元のファイルと同じ場所にファイルが出力されます。

Check ！！

ここで登録される鍵は、その相手と暗号化するときの専用鍵（認証鍵）です。認証鍵については

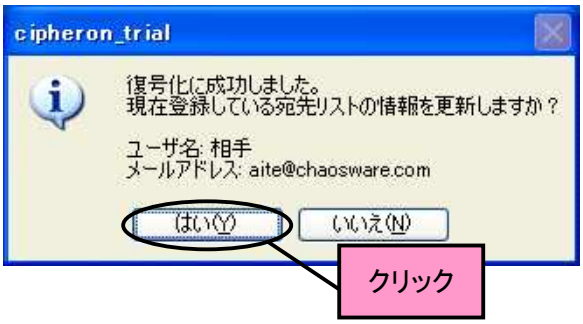
→1－1 p.5-

(2)公開鍵が登録されている相手からの暗号化ファイルを復号化する

相手の公開鍵が登録されている状態で、相手からの暗号化ファイルを復号化する場合の手順です。

復号化したいファイルをミニ工房にドラッグしてください。

次のようなダイアログが表示されます。[はい]をクリックしてください。



[はい]をクリックすると、鍵の登録ダイアログが表示されます。鍵の持ち主の名前やメールアドレスを確認し、[OK]をクリックしてください。

[OK]をクリック後、以下のようなダイアログが表示されたら鍵の登録は完了です。

鍵の登録が終了し、以下のようなダイアログが表示されたら復号化は完了です。復号化元のファイルと同じ場所にファイルが出力されます。

(3)すでに何回かやりとりをしている相手からの暗号化ファイルを復号化する

自分宛ての暗号化ファイルを復号化するのと同じ手順で行います。

復号化したいファイルをミニ工房にドラッグします。

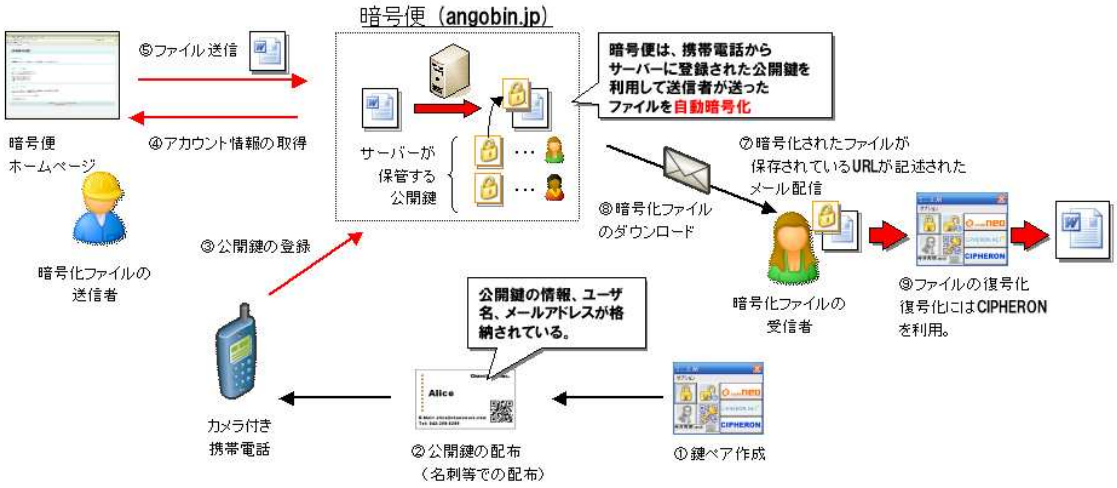
以下のようなダイアログが表示されれば、復号化は終了です。復号化元のファイルと同じ場所にファイルが出力されます。

第6章　他人とのサイズの大きいファイルのやりとり

この章では、暗号便(http://angobin.jp/) を利用して、メールで添付して送信ができない様な非常に大きなサイズのファイルをやりとりする方法を説明します。

６－１　暗号便の概要

暗号便(http://angobin.jp/) とは、株式会社カオスウェアが提供するメールに添付できない様なサイズのファイルを暗号化し、相手へ届けることができるサービスです。
例えば、動画ファイルや、高解像度の静止画映像のファイル等の非常にサイズの大きいファイルでも安全に且つ、確実に送付することができます。
暗号便では、ファイルの暗号化はサーバー上で行われ、暗号化された状態で保管されます。
ファイルを受け取った人は CIPHERON を使って復号化をすることで、暗号化された情報を受け取ることができます。
また、前章までのやり方で作成された暗号化ファイルをアップロードすることで、送信者から受信者まで全ての経路において送信するファイルのデータを保護することもできます。



次節以降では、以下の場合に分けて説明を行います。
サイズの大きいファイル受信したいケースと送信したいケースとで手順が異なります。
また、サイズの大きいファイルを送信したい場合、2 通りのやり方が存在します。

サイズの大きいファイルを送信したい場合
- → 暗号化を手元で行う場合→６－２節
- → 暗号化をサーバーで行う場合→６－３節

サイズの大きいファイルを受信したい場合 → ６－４節へ

６－２ サイズの大きいファイルの送信する（CIPHERON で暗号化）

ここでは CIPHERON StandardX をご利用中のユーザが、4章「他人とのやりとり―宛先の登録」(→ p.24) で宛先として既に登録されている相手に対して作成した暗号化ファイルを暗号便で送信する方法を説明します。

1. CIPHERON StandardX でファイルを暗号化する

まず、送信したいサイズの大きいファイルを CIPHERON StandardX で暗号化します。
暗号化は、５－1節「他人宛てにファイルを暗号化」(→ p.33)に書かれているやり方で行います。

2. 暗号便で暗号化されたファイルを送信する

送りたいサイズの大きいファイルの暗号化が完了した後、暗号便でファイルを送信します。暗号便では、暗号便に登録された公開鍵を用いて暗号化を行いファイルを送信する方法と、一時的な鍵で暗号化を行い送信する方法の二通りありますが、今回は CIPHERON StandardX を用いて暗号化が行われているため、後者の方法で送信を行います。
暗号化されたファイルの送信は以下の手順で行います。

（1） 暗号便に接続する
（2） 送信するファイルを選択する
（3） 送信先となるメールアドレスを入力する
（4） メッセージを設定する
（5） 送信する

(1) 暗号便に接続する

Web ブラウザから暗号便のページを開きます。

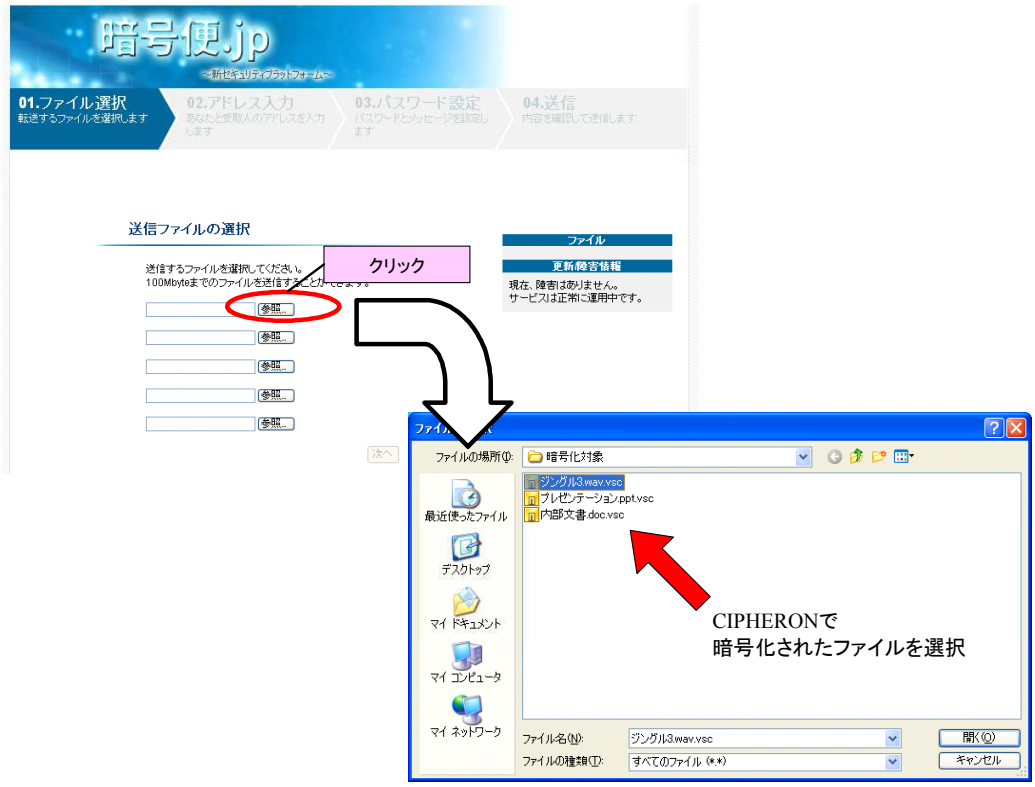
暗号便は以下の URL からアクセスすることができます。

暗号便の URL
http://angobin.jp/

暗号便に接続すると以下の様なページが表示されますので、**「いますぐファイル転送」**をクリックします。

(2) 送信するファイルを選択する

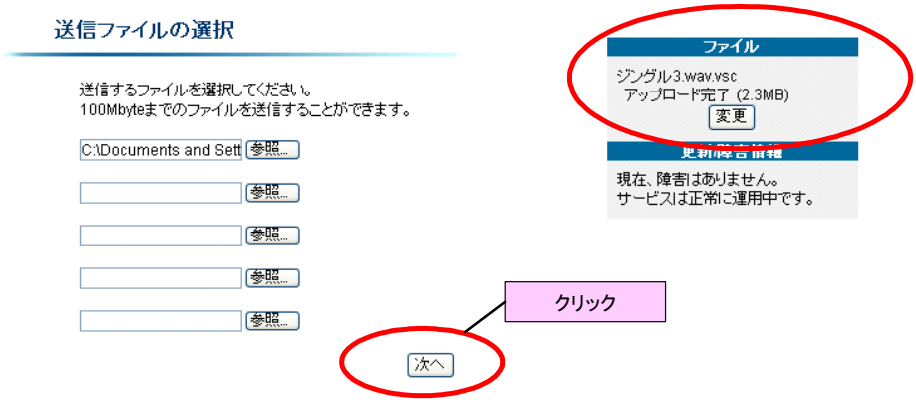
暗号便のトップページから「いますぐファイル転送」をクリックすると下の様な画面に切り替わります。
ここでは、まず送信するファイルを選択します。
画面内にある「参照」のボタンをクリックして、CIPHERON StandardX で暗号化したファイルを選択します。



Check ！！

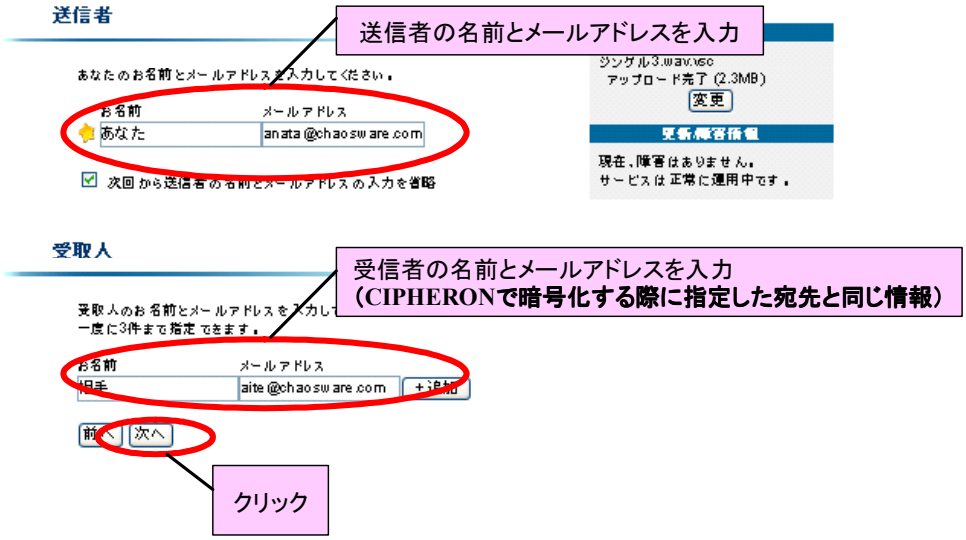
送信ファイルの選択が完了した後、すぐにアップロードが行われますが、アップロードが完了するのを待つ必要はありません。

ファイルの選択を行うと、すぐにファイルのアップロードが開始されます。
画面下の次へをクリックします。



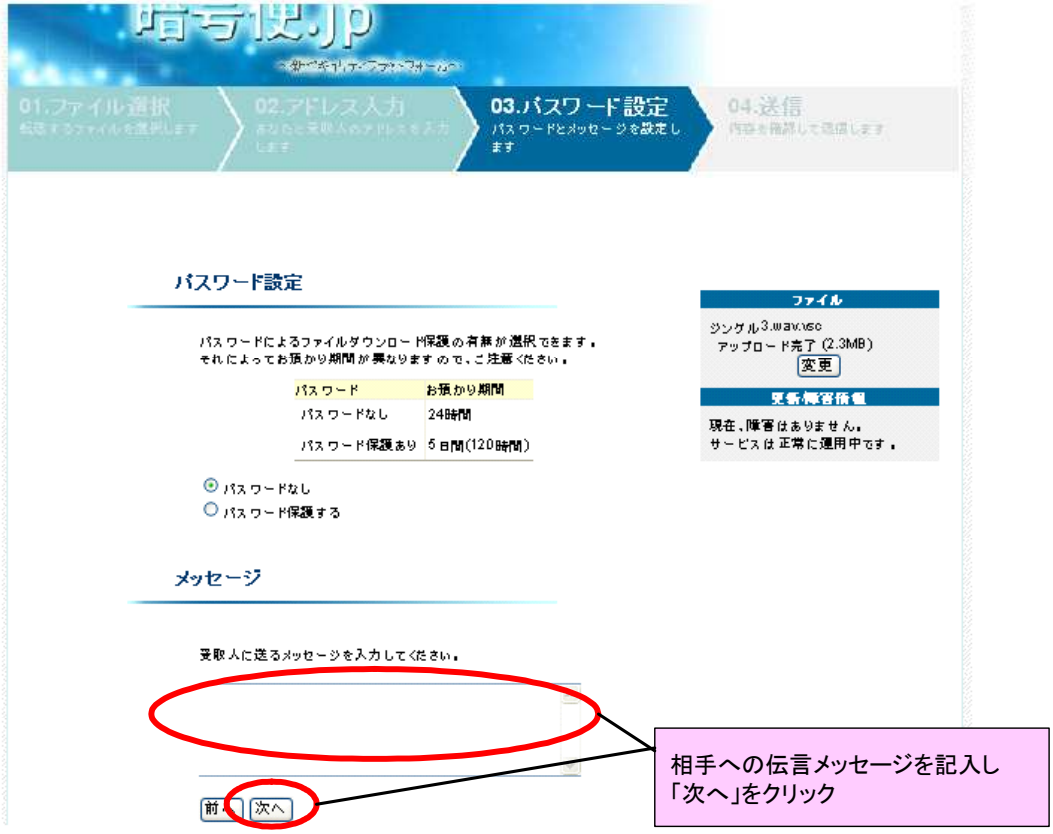
(3) 送信先となるメールアドレスを入力する

次に送信先を指定します。
送信先は CIPHERON StandardX で暗号化された大きいサイズのファイルの受信者となるため、CIPHERON StandardX で設定した宛先と同じメールアドレスを指定します。



(4) メッセージを設定する

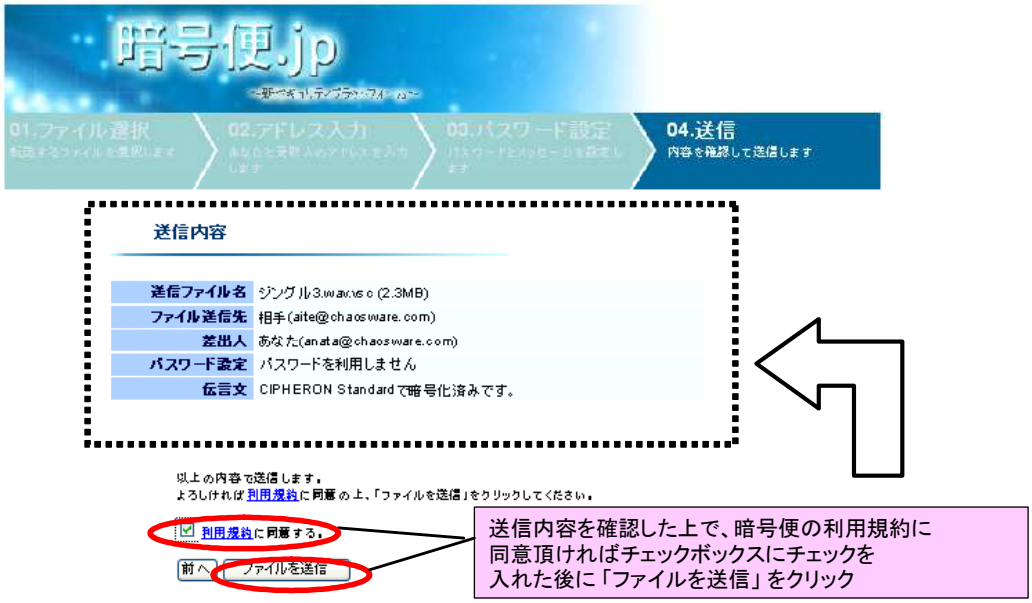
次に受信者への伝言メッセージを入力します。なお、メッセージの入力は任意です。
メッセージの入力が完了したら、「次へ」をクリックします。



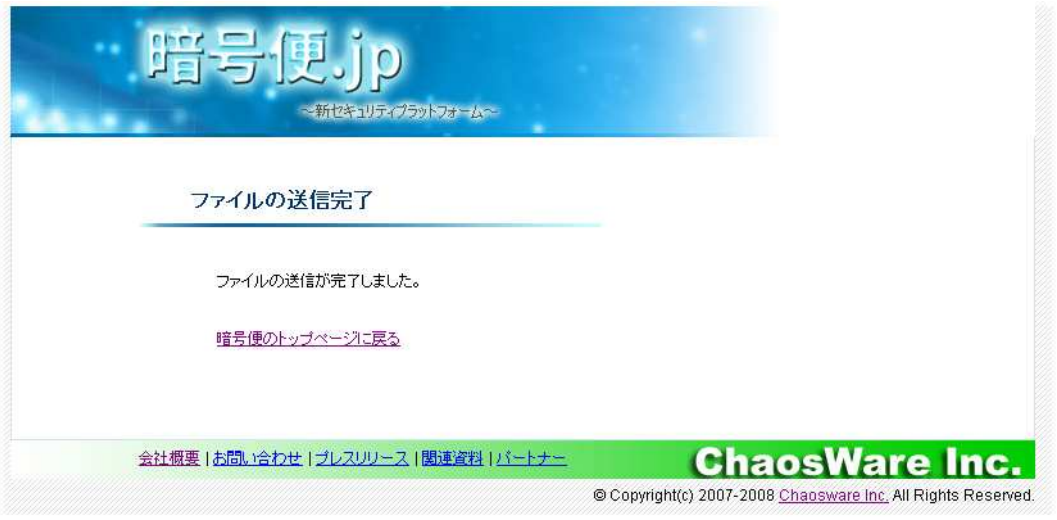
パスワードの設定項目がありますが、今回は CIPHERON StandardX で暗号化が既に行われているため、特に設定しなくても問題ありません。

(5) 送信する

次に設定内容を確認するための画面が表示されます。
送信内容として表示されている、送信ファイル名、ファイル送信先、差出人のメールアドレス及び、名前、メッセージ等に誤りがないことを確認します。
送信内容に問題がなければ、暗号便の利用規約に同意の上、「**利用規約に同意する**」のチェックボックスにチェックを入れた後に、「**ファイルを送信**」をクリックします。



「ファイルを送信」を押すと送信が実行され、次の様な画面が表示され、サイズの大きいファイルが送信されました。

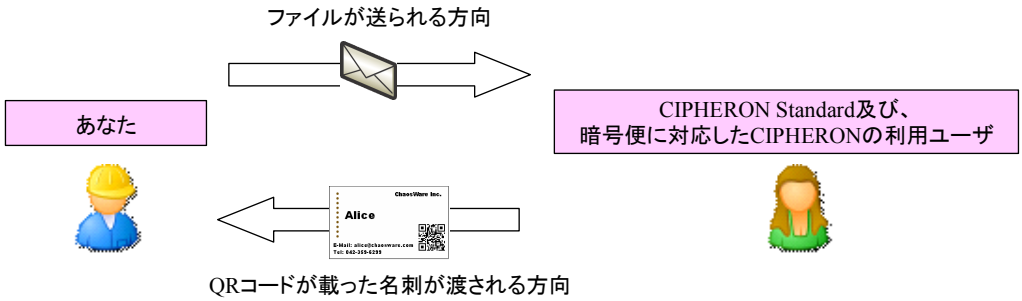


Check ！！

ファイル選択(p.44-)で非常にサイズの大きいファイルを送った場合等でファイルのアップロードが完了していなかった場合、アップロード中であることを示す画面が表示されることがあります。

６－３　サイズの大きいファイルの送信する（暗号便で暗号化）

ここでは自分以外の CIPHERON StandardX 及び、暗号便に対応した他の CIPHERON シリーズをご利用中のユーザから QR コードで暗号化を行うための公開鍵を受け取り、暗号便を利用して暗号化とファイルの送信を行う方法を説明します。



（ファイルの送信者）　　（ファイルの受信者）

この方法でファイルを暗号化して送信する場合、ファイルの送信者側には CIPHERON Standard は必須ではありませんが、ファイルの受信者が CIPHERON StandardX 及び、暗号便に対応した CIPHERON を利用している必要があります。

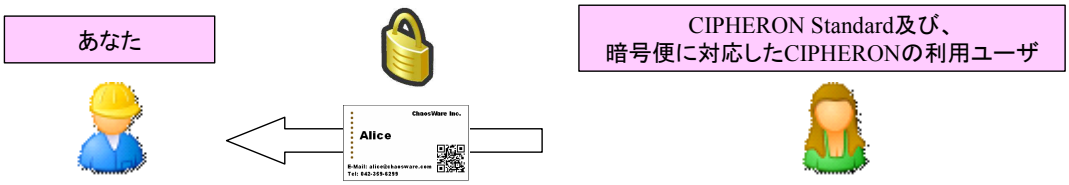
サイズの大きいファイルを暗号便で暗号化した上で送信するには以下の手順で操作を行います。

(1) ファイルを送信する相手から QR コードで印刷された公開鍵を受け取る
(2) 暗号便のアカウントを作成する
(3) 受け取った QR コード公開鍵を登録する
(4) ファイルを送信する

(1)ファイルを送信する相手から QR コードで印刷された公開鍵を受け取る

暗号便のサーバー側で暗号化も行う場合、あらかじめ受信者の公開鍵を暗号便へ登録しておく必要があります。

まず、受信者となる CIPHERON StandardX 及び、暗号便に対応した CIPHERON シリーズを利用しているユーザから QR コードで印刷された公開鍵を受け取ります。受け取った QR コードには公開鍵情報が含まれており、暗号便ではこの公開鍵を利用してファイルの受信者へファイルを暗号化して送信します。



（ファイルの送信者）　　（ファイルの受信者）

(2)暗号便のアカウントを作成する

次に受け取った公開鍵を暗号便へ登録します。

公開鍵の登録を行うには暗号便へアカウントを作成しておく必要があります。既にアカウントをお持ちの方は「(3)受け取った QR コード公開鍵を登録する」へ進んでください。

以下の URL にアクセスをするとアカウント開設のためのページが準備されています。

ページの内容に従って、必要事項を記入していただくことでアカウントの開設を行うことができます。

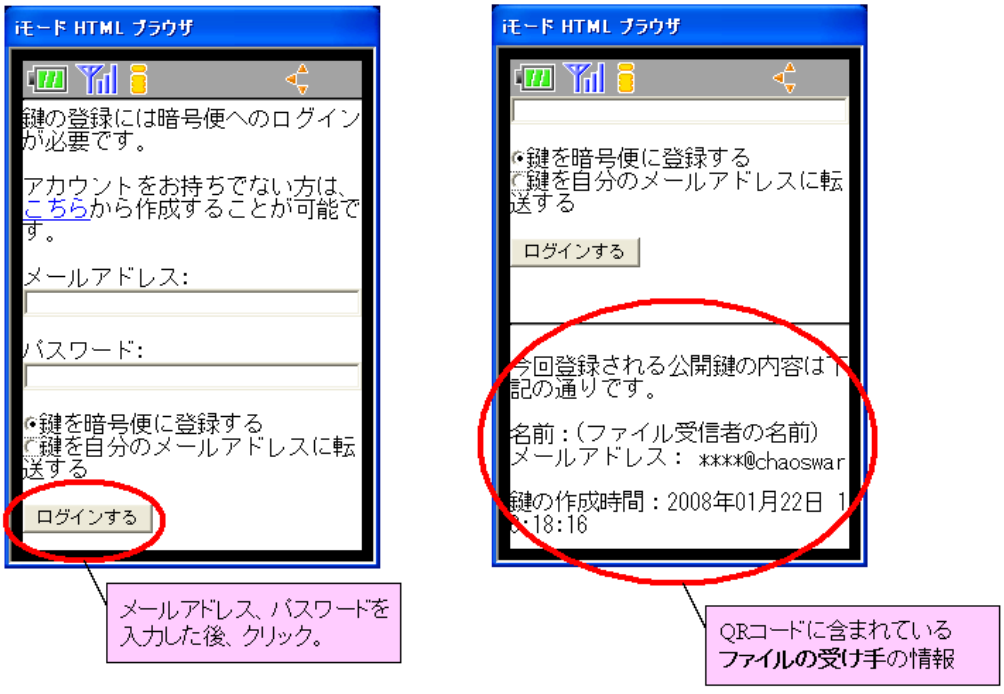
暗号便アカウント開設用 URL

http://angobin.jp/id/

(3)受け取った QR コード公開鍵を登録する

アカウントが登録された後、次にファイルの受け手から渡された QR コードを携帯電話で読み取ります。読み取りが完了し、表示される URL に従って携帯電話から暗号便へ接続を行うと次の画面が表示されます。
(2)で作成した暗号便のアカウント作成時に設定したメールアドレス及び、パスワードを入力し、「ログインする」ボタンをクリックします。
入力したメールアドレス及び、パスワードが正しければログインが行われ、QR コードに記載されていた公開鍵が暗号便に登録されます。

なお、更に画面をスクロールさせると QR コードに含まれているファイル受信者の名前、メールアドレスを確認することができます。

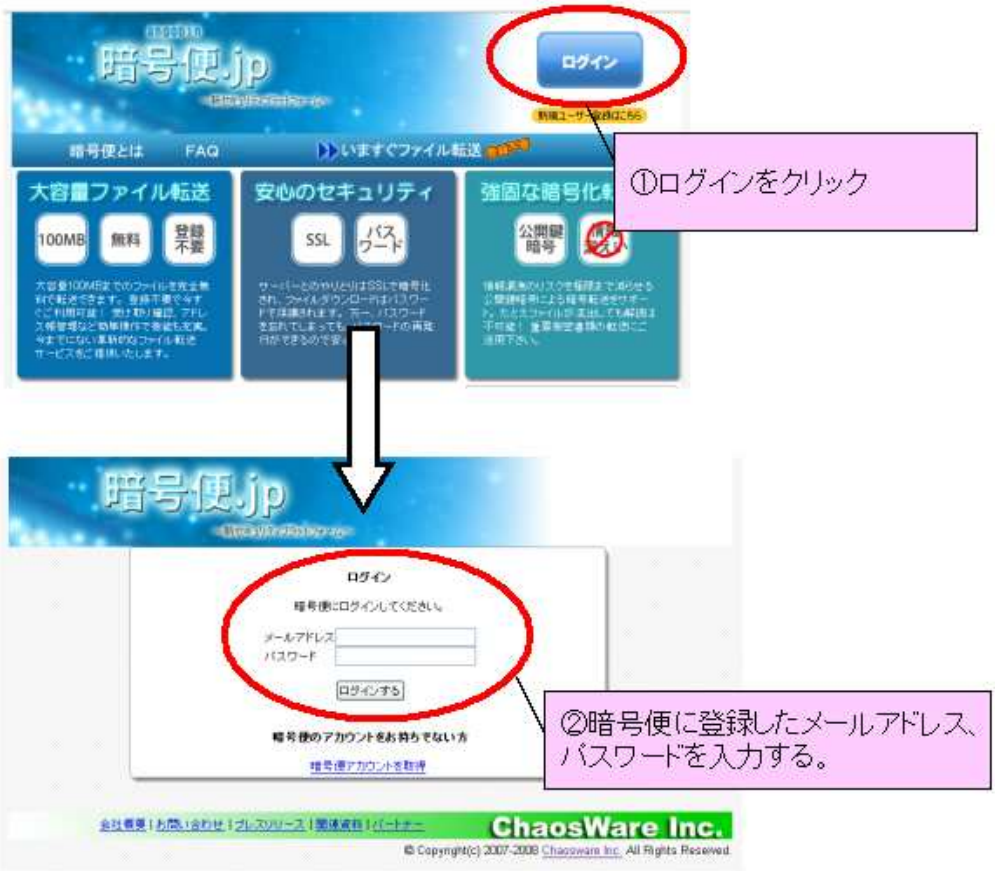


(4)ファイルを送信する

6－3において、ファイルの受け手の公開鍵を登録しました。ここまででファイルを送る準備が整いました。
次に Web ブラウザから実際にファイルの受け手の方へファイルを送信します。
暗号便へログインします。

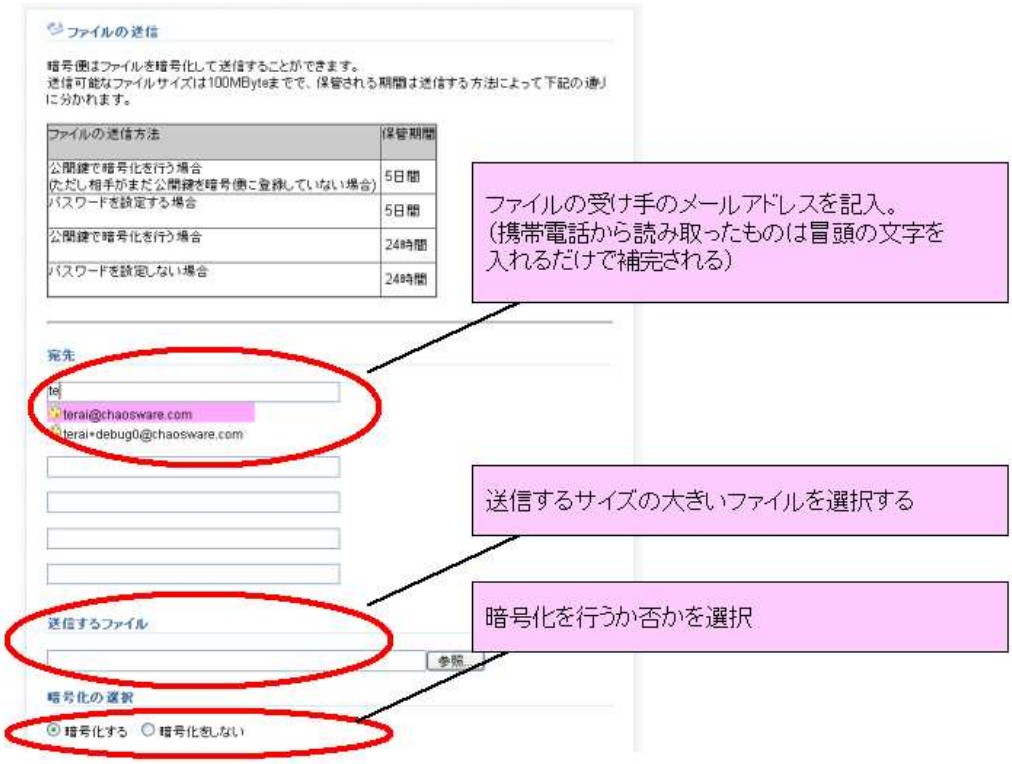
暗号便トップページ URL

http://angobin.jp/



ログインが完了すると、次の様なアカウント所有者用のトップページが表示されます。
ファイルを送信するために「ファイルの送信」をクリックします。

ファイルの送信を選択すると以下の様な画面が表示されますので、ファイルの受け手のメールアドレス(宛先)、送信するファイル等を選択します。ファイルは100Mbyteまでのファイルを送信することができます。
ページの末尾にある「ファイルを送信」ボタンをクリックすれば、ファイルの転送が開始されます。



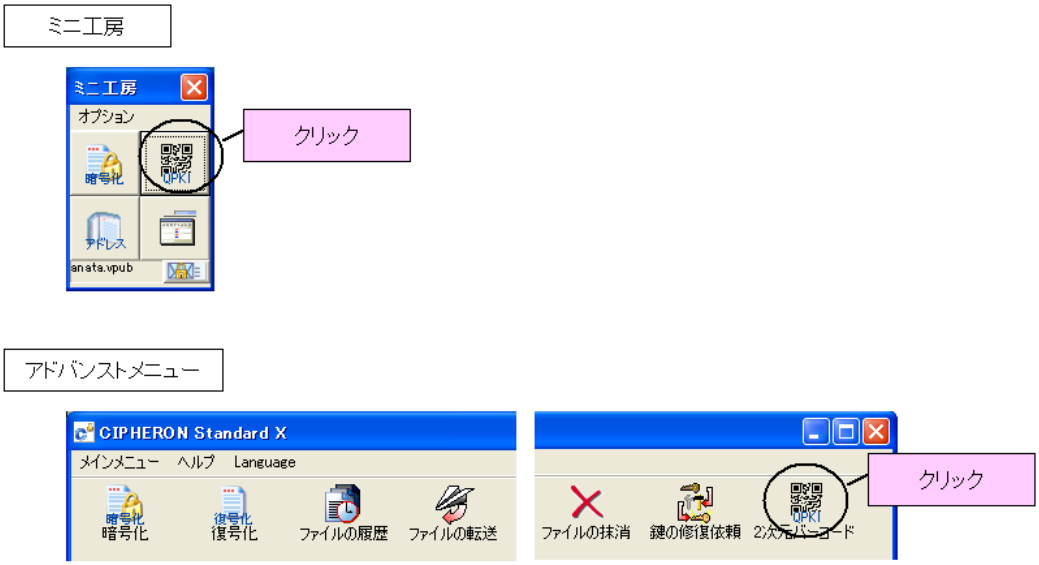
６－４　サイズの大きいファイルを受信する

　ここでは、暗号便を利用して大きいファイルを受け取りたい場合の方法について説明します。

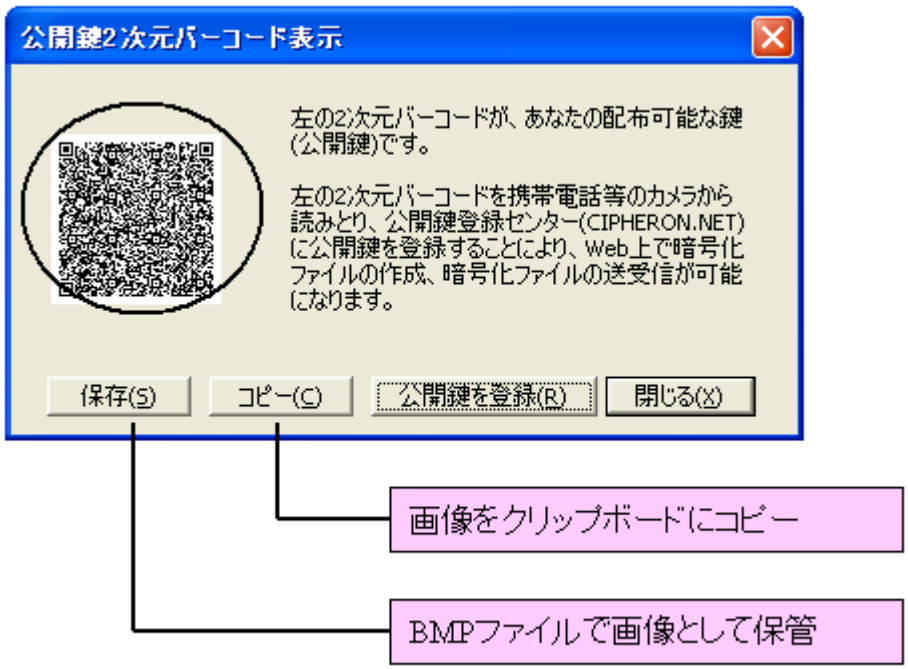
1．ファイルのやり取りまでの準備

ファイルの受け手となる側は、暗号便を利用して大きいサイズのファイルをやりとりするまでにファイルの送り手に公開鍵を渡しておく必要があります。
CIPHERON StandardX では、以下の手順で自分が現在利用している公開鍵の情報を QR コードにすることができます。

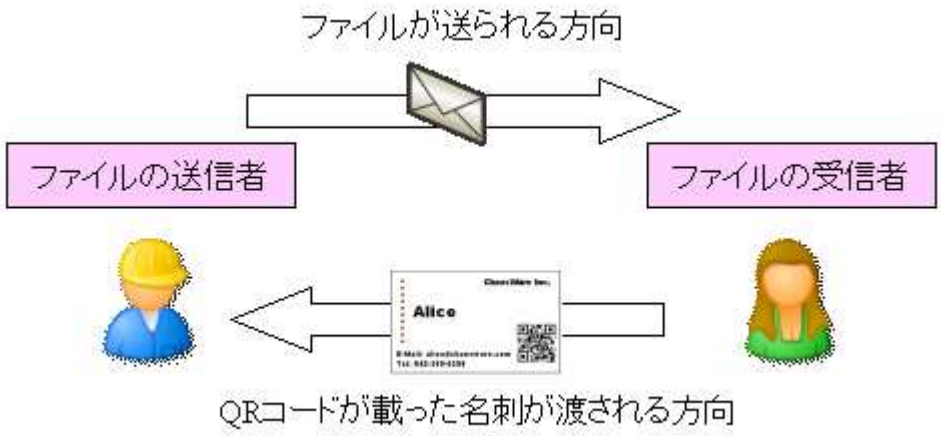
（1）ミニ工房及び、アドバンストメニューから該当のアイコンをクリックします。



（2）QR コードが表示されますので、「保存(S)」または、「コピー(C)」をクリックします。
保存(S)を選択した場合には、作成された QR コードを BMP ファイルとして保存することが可能です。
コピー(C)を選択した場合には、クリップボードに QR コードがコピーされています。

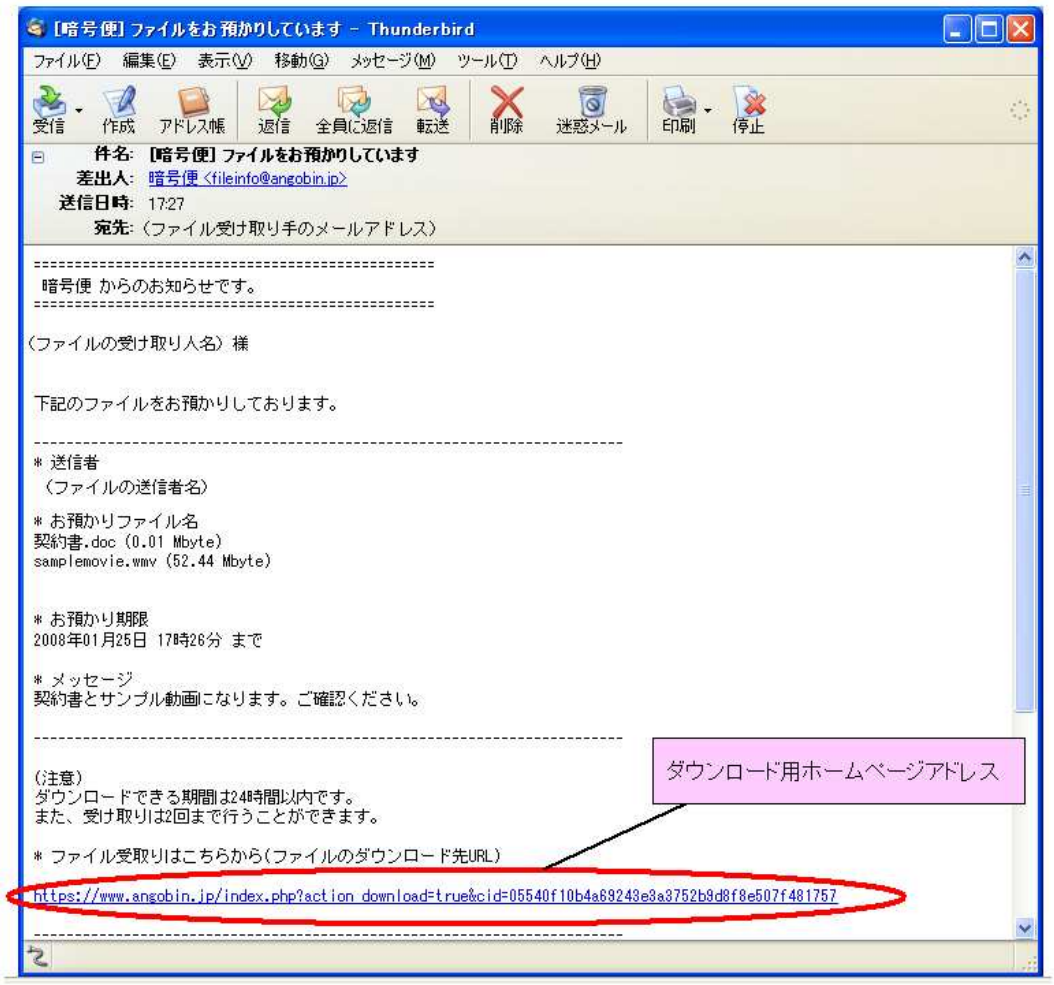


（3）QR コードをファイルの送り手へ渡します。
ファイルとして保存及び、クリップボードにコピーされた QR コードを名刺等への印刷を行い、ファイルの送り手へ渡します。
これで、受け手の公開鍵の情報を、ファイルの送り手へ渡すことができました。
ファイルの受け手側の準備は以上です。実際のファイルの受け取りは6－5からの手順をご確認ください。



2.　暗号化されたファイルの受け取り

ファイルが暗号便を経由して送付された場合、ファイルの受け手の方には次の様なメールが暗号便から送付されます。
メールには、送信者の方の情報とメッセージ、併せて保管期間や預かり中のファイル名が記載されています。
メール末尾にファイルをダウンロードするための URL が掲載されていますので、クリックをしてホームページを開きます。



ダウンロード用のページを開くと次の様な画面が表示されますので、されたファイルをダウンロードします。
ダウンロードしたファイルは暗号便によって暗号化が行われていますので、前章までと同様に CIPHERON へドラッグ＆ドロップを行い復号化を行います。

以下のようなダイアログが表示されれば、復号化は終了です。復号化元のファイルと同じ場所にファイルが出力されます。

第7章　アドバンストメニューを使う

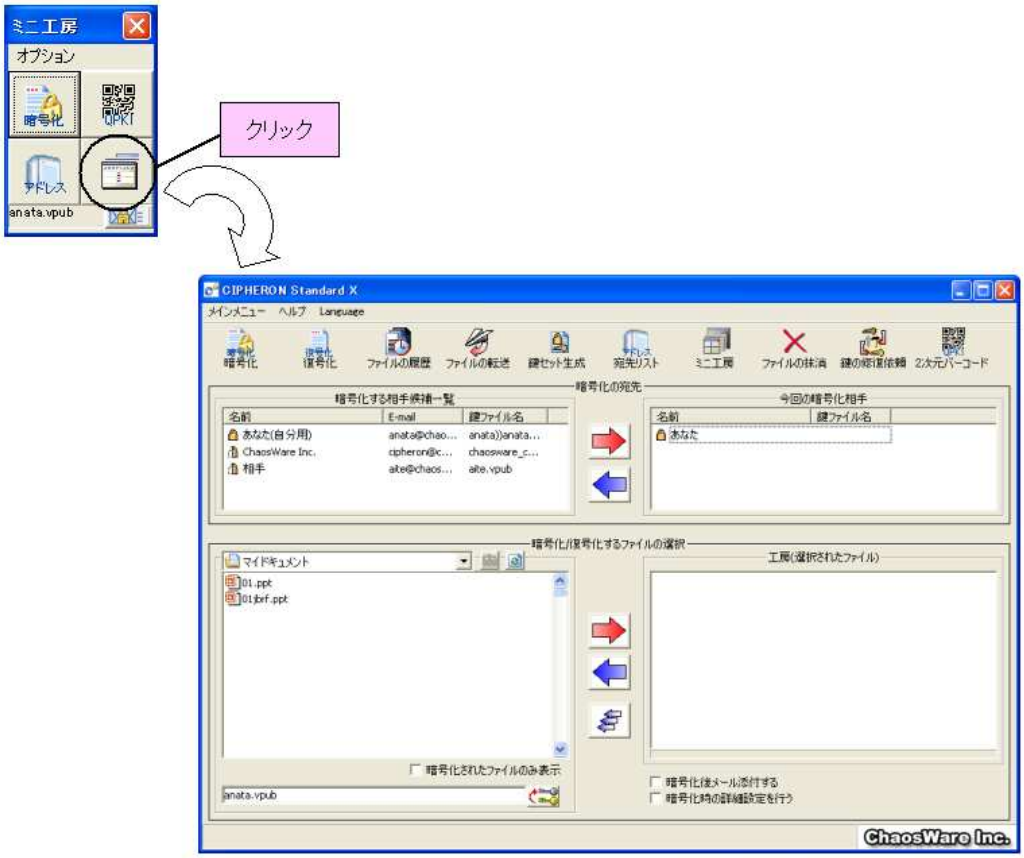
この章では、ミニ工房ではなく、『CIPHERON Standard X Edition』の機能がすべてそろっているアドバンストメニューの使い方を説明します。

7－1　アドバンストメニューを使う

暗号化・復号化や宛先登録の機能はミニ工房から行うことができますが、暗号化ファイルの履歴表示を行ったり、ディレクトリの階層が異なる複数のファイルを一括して暗号化を行いたいときなどは、アドバンストメニューを使用する方が便利です。

アドバンストメニューを使用する場合は、[**アドバンストメニューへの切り替え**]アイコンをクリックしてください。

アイコンをクリックすると、アドバンストメニューが表示されます。



７－２　アドバンストメニューの機能

アドバンストメニューの機能は大まかに 10 あります。

（1）ファイルの暗号化
（2）ファイルの復号化　　６－３ p.40-

（3）暗号化ファイルの履歴表示
（4）暗号化ファイルの転送　　６－４ p.46-

（5）ファイルの抹消　　６－５ p.49-

（6）宛先リストの編集
（7）公開鍵の送付

（8）鍵セット生成　　６－６ p.50-

（9）鍵の選択
（10）鍵のバックアップ依頼

このうち、“（6）宛先リストの編集”と“（7）公開鍵の送付”は、ミニ工房で行う場合と同じですので、４－3および4－4をご覧ください。また、（9）鍵の選択、（10）鍵のバックアップおよび復元依頼については、それぞれ**「８－７　鍵の選択(p.79-)」**、**「鍵のバックアップについて(p.85-)」**をご覧ください。

７－３　ファイルの暗号化／復号化

（1）ファイルの暗号化

ミニ工房からの暗号化とは手順が少し異なります。

大きく分けて手順は三つあります。

①暗号化したいファイルを工房に入れる
②暗号化する相手を選択する
③暗号化する

なお、①と②は順不同です。どちらの操作から行っても構いません。

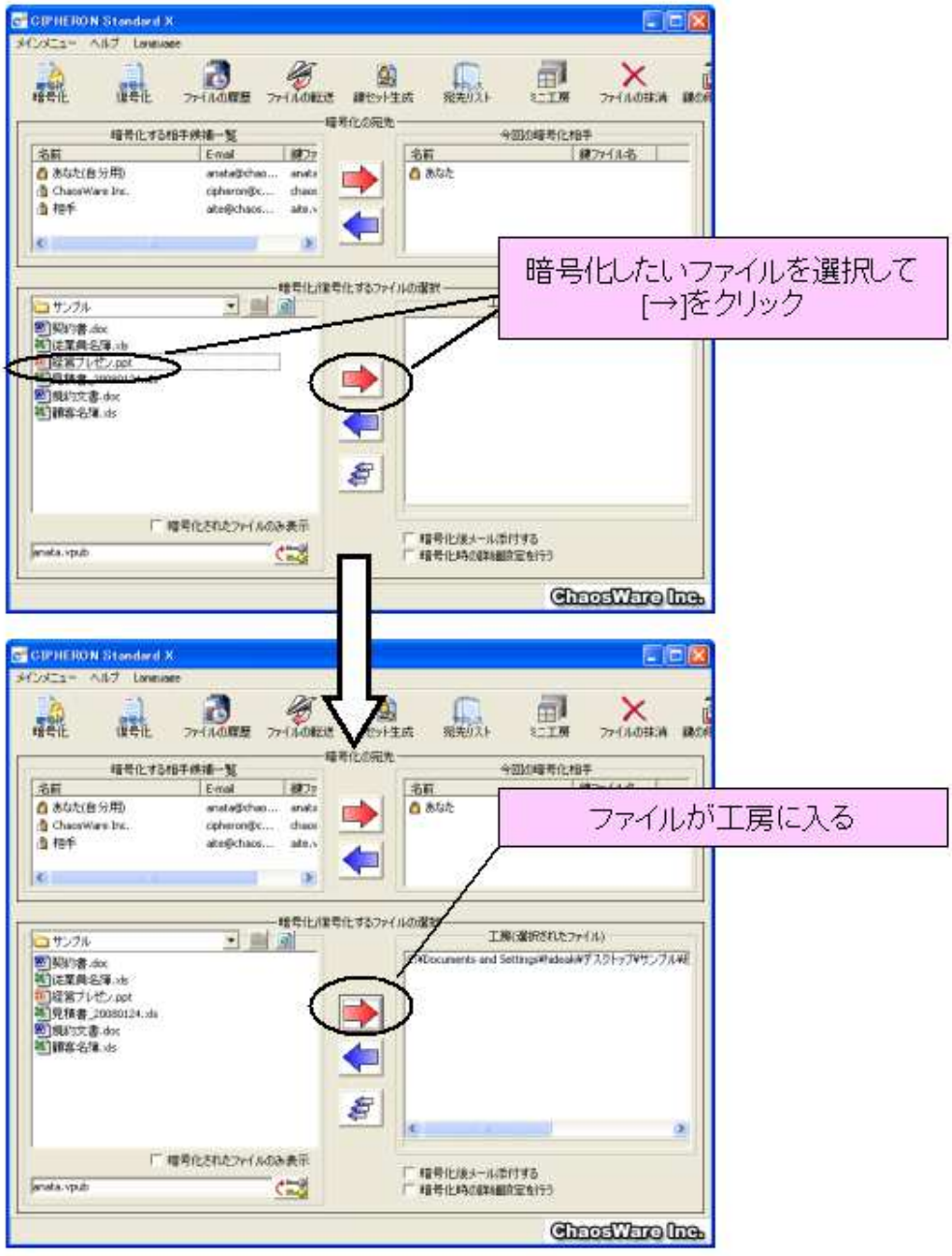
一度選択したファイルや宛先を削除したいときは、削除したいファイルをクリックしてから、[←]をクリックしてください

暗号化したファイルを相手にすぐに送信したい場合は、[暗号化後メール添付する]にチェックを入れてください

①暗号化したいファイルを工房に入れる

左下のボックスに、ファイル一覧が表示されます。

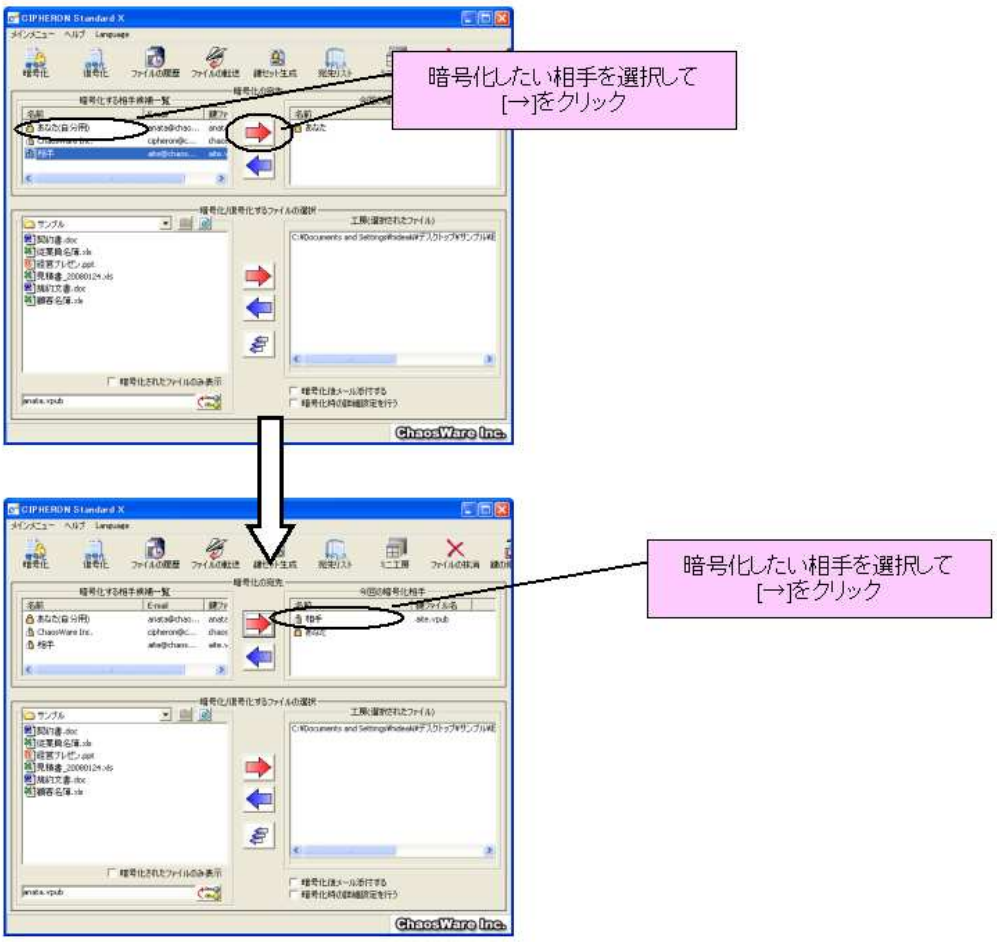
ファイル一覧より、暗号化したいファイルを選択して[→]をクリックしてください。ファイルが工房に入ります。



②暗号化する相手を選択する

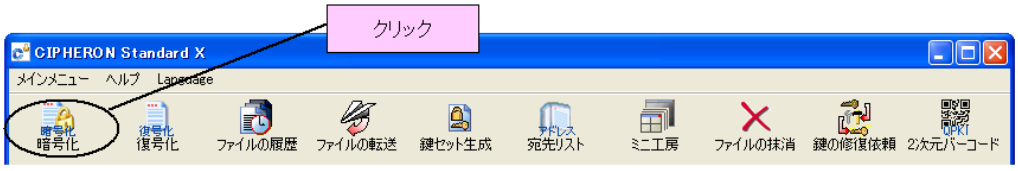
左上のボックスには、暗号化のやりとりが可能な相手の一覧が表示されています。

暗号化の相手を選択し、[→]をクリックして右のボックスに入れます。

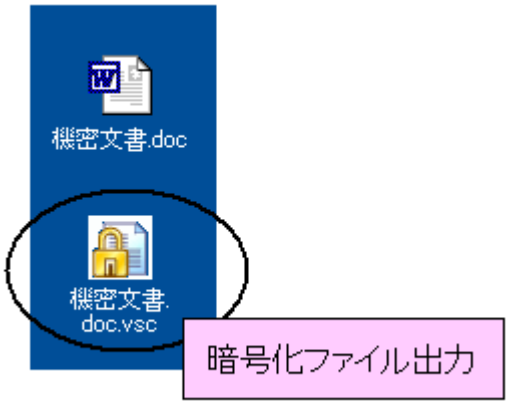


③暗号化する

[暗号化]をクリックします。



以下のようなダイアログが表示されれば暗号化は終了です。暗号化されたファイルは、暗号化元のファイルと同じ場所に保存されます。



Check ！！

暗号化されたファイルの出力先を変更するなどの暗号化の詳細設定をしたい場合は

→8－3 p.72-

(2)ファイルの復号化

これもミニ工房からの復号化と手順が異なります。大きく分けて手順は二つです。

①復号化したいファイルを工房に入れる

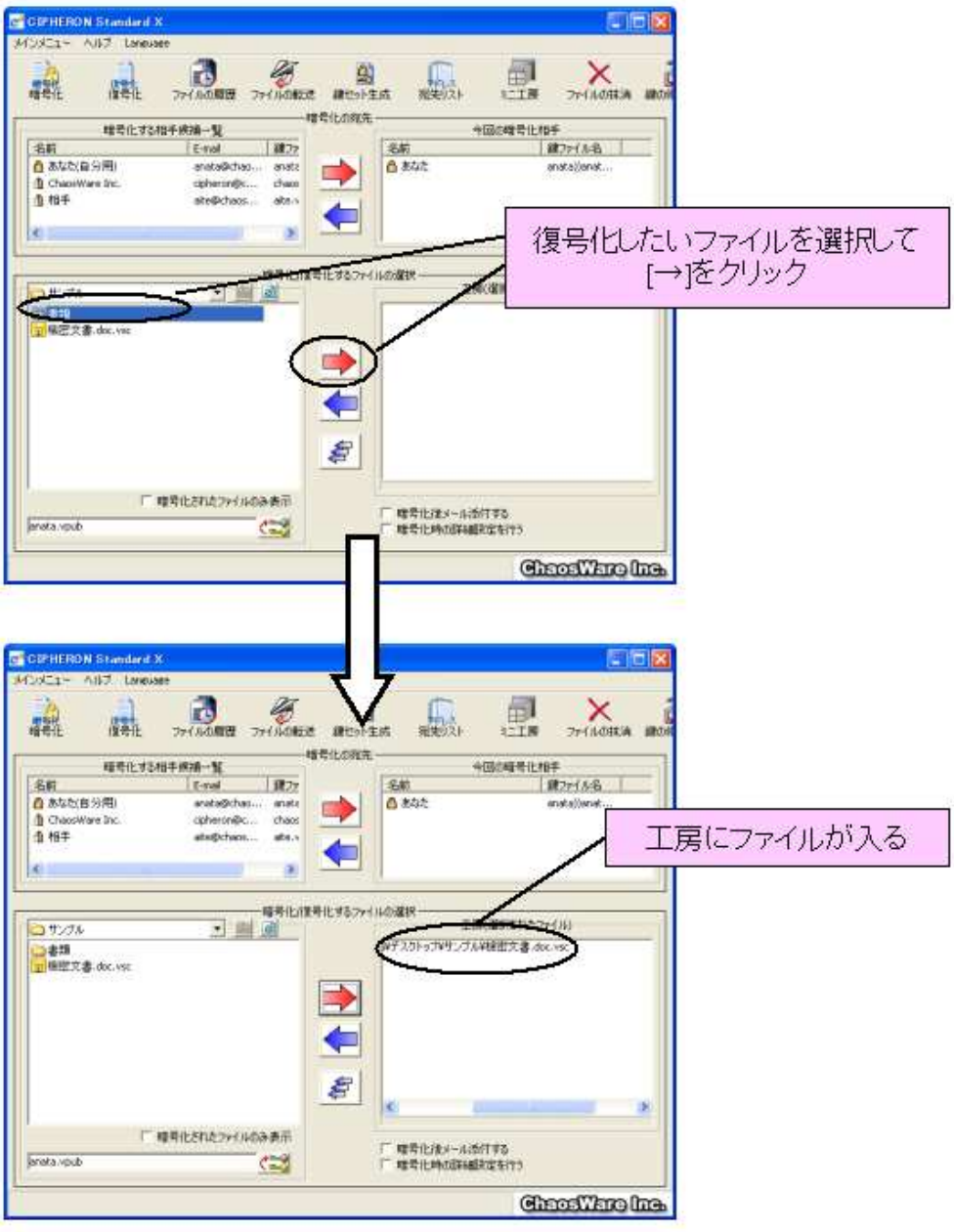
②ファイルの出力先を選択する

①復号化したいファイルを工房に入れる

左下のボックスにファイル一覧が表示されます。

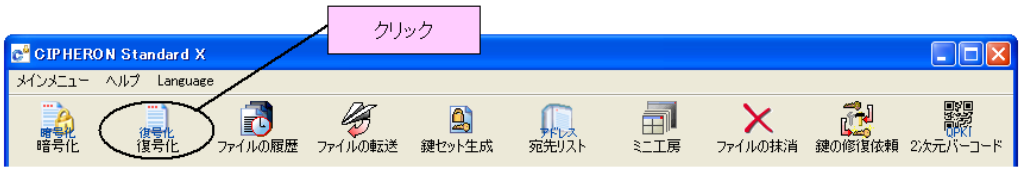
ファイル一覧より、復号化したい暗号化ファイルをクリックしてください。

復号化したいファイルを工房に入れます。[→]をクリックしてください。ファイルが工房に入ります。

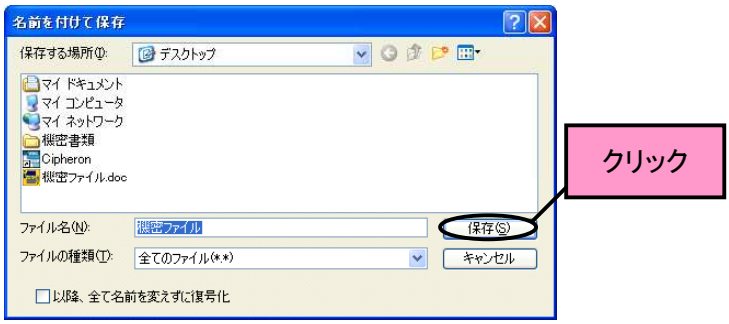


②ファイルの出力先を選択する

[**復号化**]をクリックします。



[**復号化**]をクリックすると、次のような画面が表示されます。復号化するファイルの保存先を選択して[**保存**]をクリックしてください。この例では、デスクトップに保存します。



これで復号化は終了です。指定した場所にファイルが保存されているか確認してください。

7－4　暗号化ファイルの履歴表示／転送

Check　！！

履歴が更新されるのは、一時復号化および復号化の時です。一時復号化については

→8－5　p.75-

暗号化ファイルには誰がどのような操作をしたかという履歴管理をつけることができます。また、履歴を利用してファイルを転送することもできます。履歴の詳細については、(1)の②で解説します。

(1)暗号化ファイルの履歴表示

暗号化ファイルに記録されている履歴を表示します。大きく分けて手順は二つです。

①履歴を表示したい暗号化ファイルを工房に入れる

②履歴表示する

なお、履歴管理されていない暗号化ファイルおよび復号化権限のない暗号化ファイルは履歴を表示することはできません。

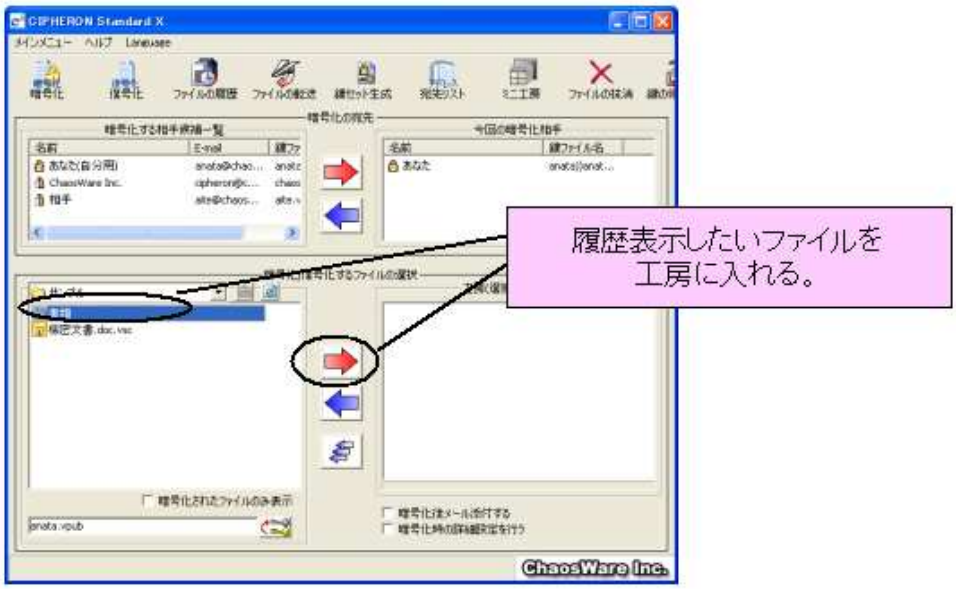
Check　！！

エクスプローラ上から右クリックで履歴表示をする方法については

→8－6　p.76-

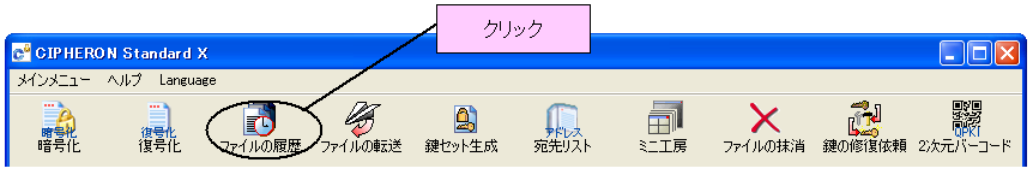
①履歴を表示したい暗号化ファイルを選択

ファイル一覧から、履歴表示したい暗号化ファイルを工房に入れます。ファイルを選択し、[→]をクリックしてください。

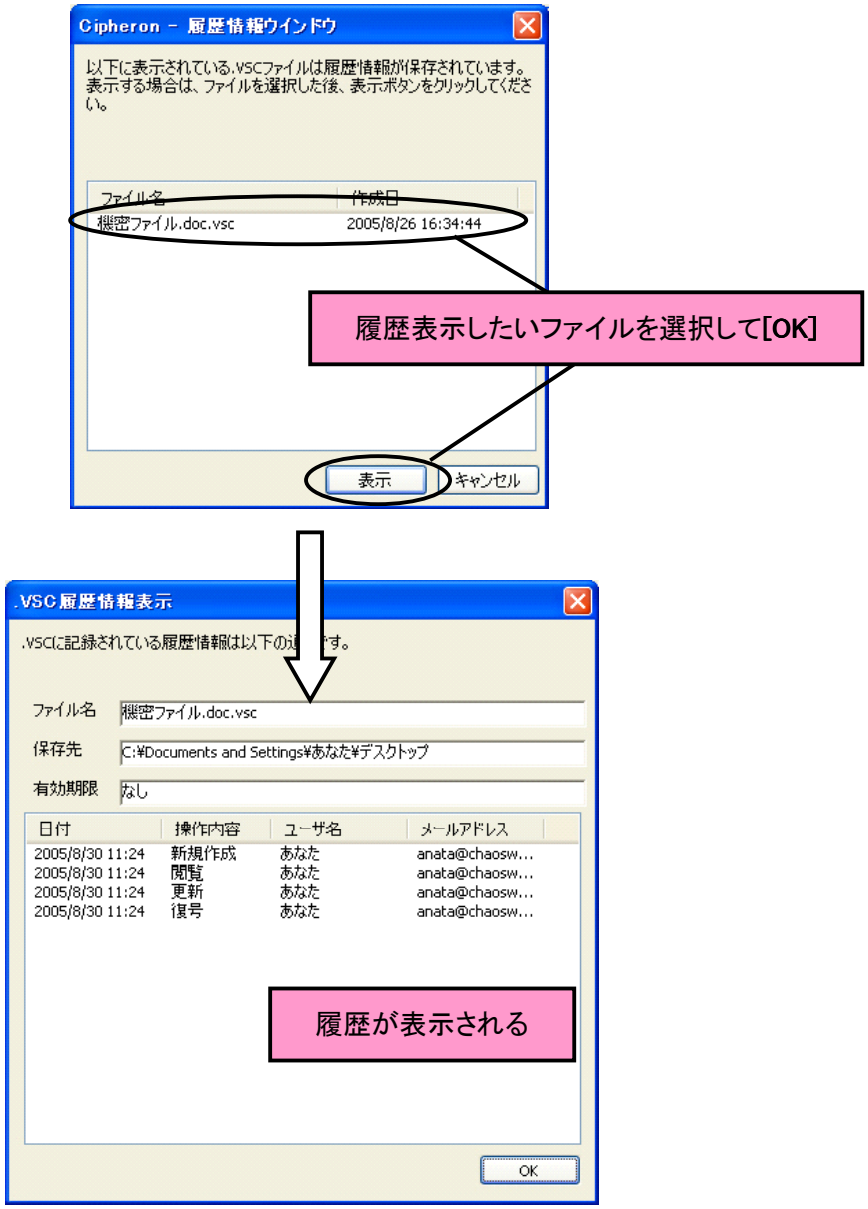


②履歴表示する

[**ファイルの履歴**]をクリックします。



[**ファイルの履歴**]をクリックすると、以下のような画面が表示されます。履歴表示したいファイルを選択し、[**表示**]をクリックしてください。履歴が表示されます。



操作内容の説明

新規作成:暗号化ファイルが作成された時点を意味します

閲覧:暗号化ファイルが一時復号化され、内容の変更がなかったことを意味します

更新:暗号化ファイルが一時復号化され、そこで内容が変更されたことを意味します

復号:暗号化ファイルが復号化されたことを意味します

履歴管理を行っていないファイルおよび、復号化権限のない暗号化ファイルの場合は、履歴表示・転送することができません

(2)暗号化ファイルの転送

履歴管理されている暗号化ファイルは、ファイルを復号化できる相手に転送することができます。

大きく分けて二つの手順があります。

①転送したい暗号化ファイルを工房に入れる

②相手を選択して転送する

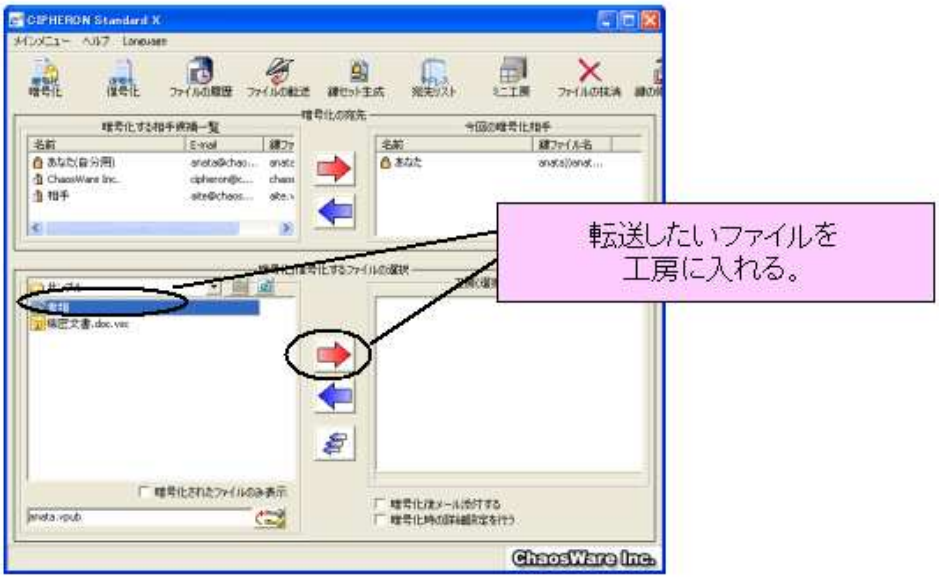
Check ！！

エクスプローラ上から右クリックでファイルの転送をする方法については

→8－6 p.76-

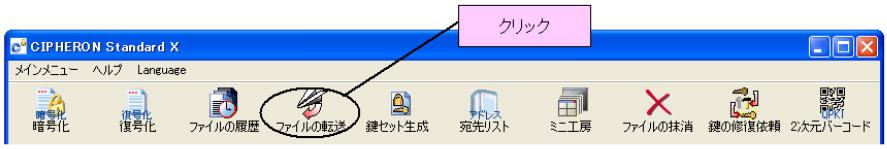
①転送したい暗号化ファイルを選択する

ファイル一覧から、転送したい暗号化ファイルを工房に入れてください。

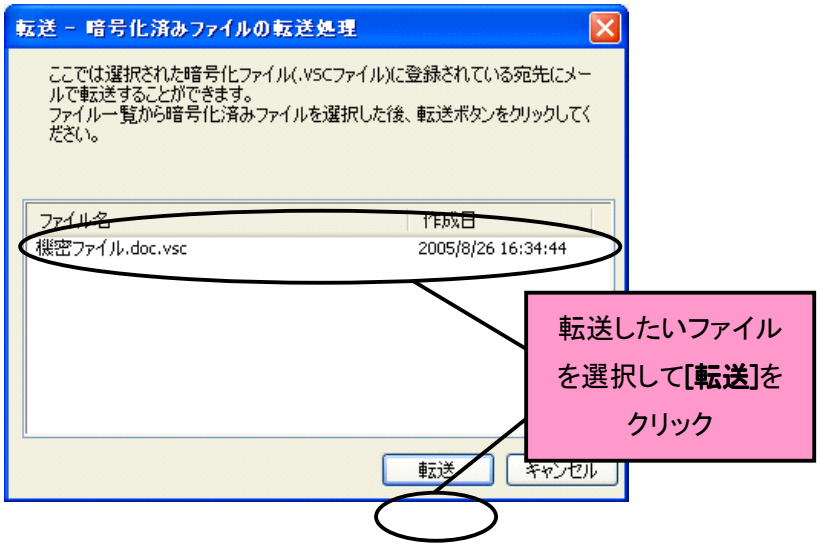


②相手を選択して転送する

[**ファイルの転送**]をクリックします。



以下のような画面が表示されますので、転送したいファイルを選択し、[**転送**]をクリックしてください。

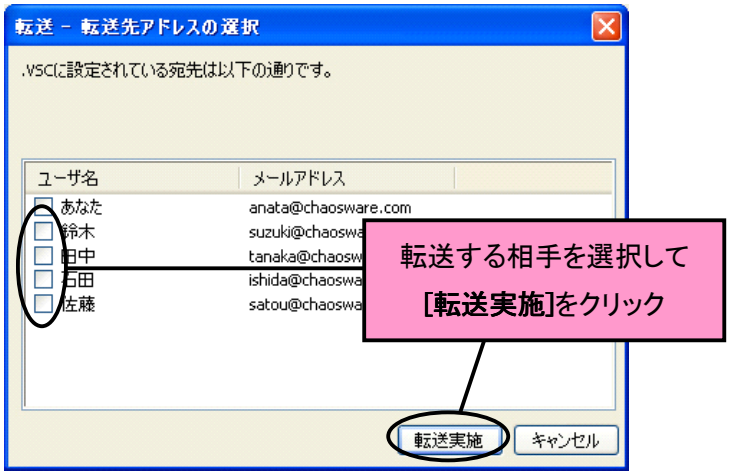


Check ！！

メールソフトが起動しない場合は

→10－2 p.84-

[転送]をクリックすると、以下のような画面が表示されますので、転送したい相手にチェックを入れ、[転送実施]をクリックします。すぐにメールソフトが起動しますので、本文を入力してメールを送信してください。



7－5 ファイルの抹消

アドバンストメニューでは、不要になったファイルの完全削除を行うことができます。
ファイル抹消の手順は大きく分けて二つです。

①抹消したいファイルを工房に入れる
②抹消を実行する

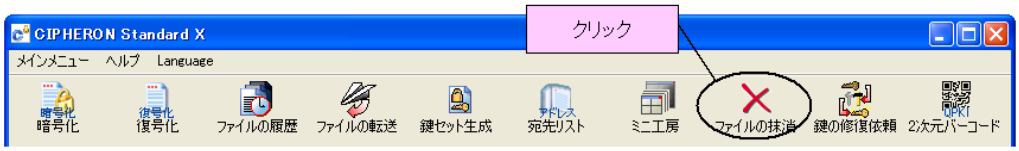
このコマンドで削除したファイルは、ランダムに暗号化されてから消去されるので、ファイル復元ソフトなどを使用しても元に戻すことはできません

①抹消したいファイルを工房に入れる

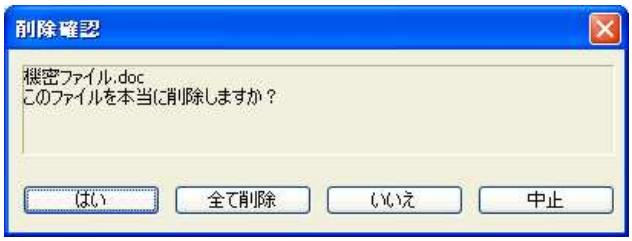
ファイル一覧から、抹消したいファイルを工房に入れます。ファイルを選択し、[→]をクリックしてください。

②抹消を実行する

[**ファイルの抹消**]をクリックします。



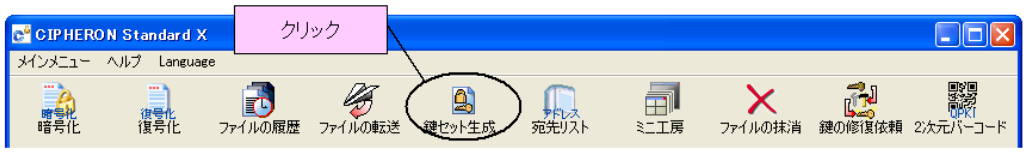
本当にファイルを抹消するかどうかのダイアログが表示されるので、抹消するならば[**はい**]か[**全て削除**]を、キャンセルするならば[**いいえ**]か[**中止**]をクリックしてください。



[**はい**]または[**全て削除**]をクリックすれば、ファイルの抹消は完了です。

7－6　鍵セットの生成

『CIPHERON Standard X Edition』をお使いの際に、複数の鍵が必要となった場合に実行します。[**鍵セット生成**]アイコンをクリックすると、鍵セット生成ウィザードが表示されます。操作内容は『CIPHERON Standard X Edition』初回起動時に行う鍵セット生成と同じですので、「**2－3　初回起動と初期設定**(p.15-)」をご覧ください。また、鍵を複数作成した場合、鍵の選択が必要になることがあります。鍵の選択については「**8－7　鍵の選択**(p.79-)」をご覧ください。



第8章　拡張機能

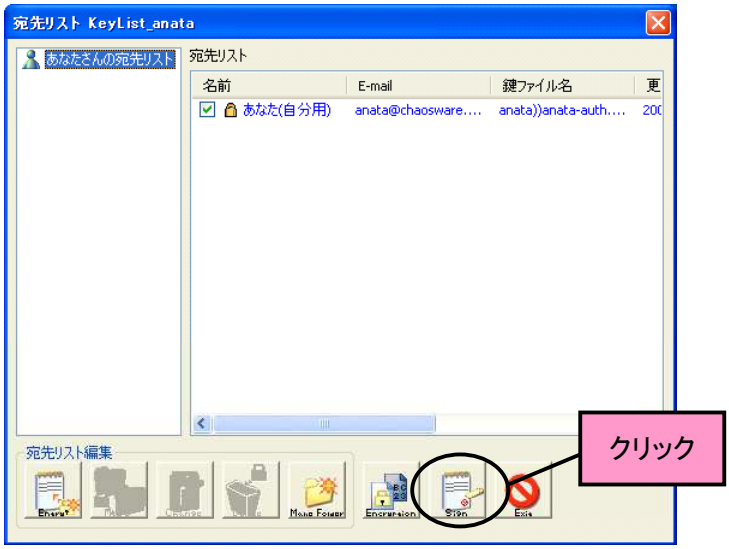
この章では、第6章までのオーソドックスな操作法ではなく、より細かい暗号化設定や右クリックメニューを用いた操作法を説明します。

8－1　公開鍵の認証

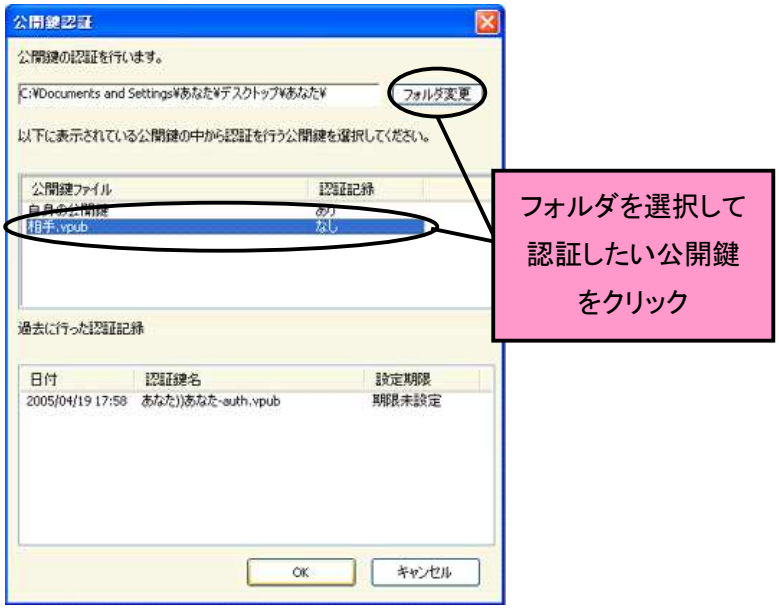
公開鍵の認証を行う必要がある場合は、『VSC-P2P ver 1.03』以前のバージョンとやりとりをする場合です

弊社の暗号化ソフト『VSC-P2P』と暗号化ファイルのやりとりをする場合、“公開鍵の認証”手続きを手動でする必要があります。
あなたが相手から暗号化ファイルを受信するときに、公開鍵の認証作業が必要となります。

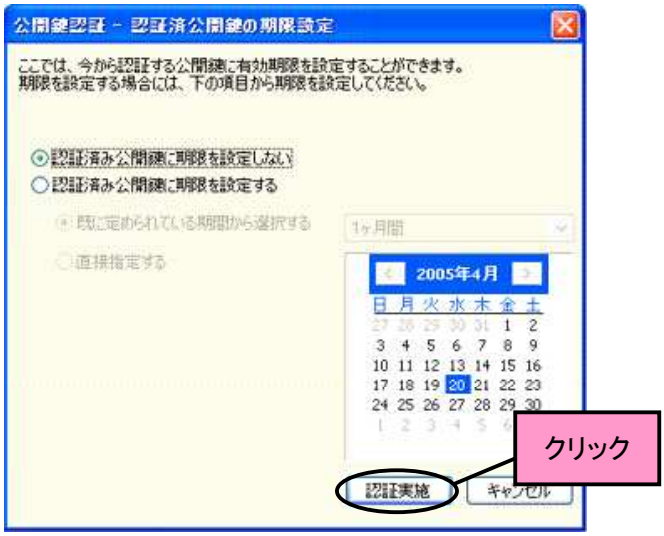
まず宛先リストを開き、[**公開鍵の認証アイコン**]をクリックします。



以下のような画面が表示されるので、相手の公開鍵のあるフォルダを指定します。

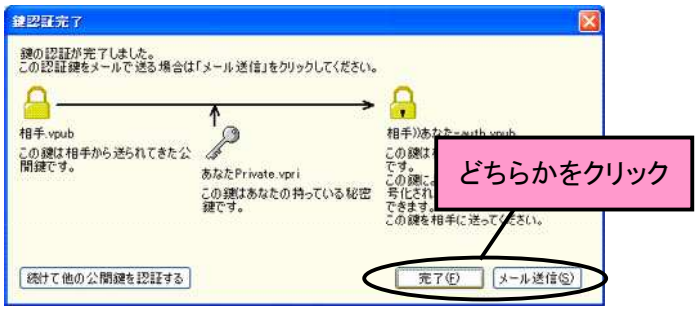


[OK]をクリックすると、認証の有効期限をつけるダイアログが表示されます。通常は“認証期限をつけない”にチェックして、[**認証実施**]をクリックします。



以下のようなダイアログが表示され、公開鍵の認証は終了して認証鍵が作成されます。作成された認証鍵をメールに添付して、相手に送信してください。[**メール送信**]をクリックすると、メールソフトが起動して、鍵が添付された状態になります。相手のメールアドレスを入力して、メールを送信してください。

メールソフトが自動的に起動しない場合や、後で相手に送信したい場合は[**完了**]をクリックし、手動でメールソフトを起動して鍵を添付してください。



８－２　認証鍵の登録

Check　！！

認証鍵については

→１－１　p.5-

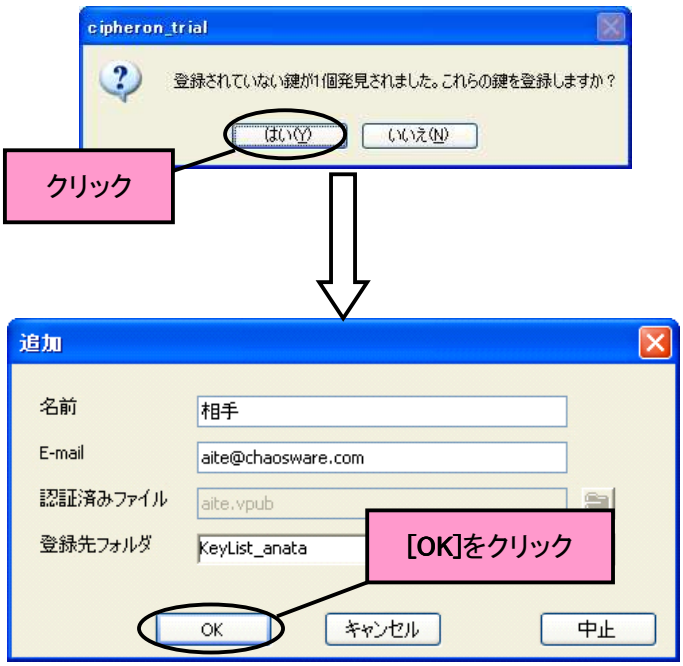
ver 1.03 以前のバージョンの『VSC-P2P』をお使いいただいている相手に暗号化ファイルを送りたい場合は、まずあなたの公開鍵を相手に送信する必要があります。現在ご利用中の公開鍵をメールに添付して(**４－３　p.27-**)、相手に公開鍵を送信してください。

Check ！！

宛先リストについては

→4－4 p.28-

公開鍵を送ると、相手から認証鍵が送信されてくるので、認証鍵を鍵管理フォルダに保存してください。その状態でソフトを起動すると、以下のようなダイアログが表示されます。相手の名前や E メールアドレスを確認または変更し、[OK]をクリックしてください。宛先に登録されます。

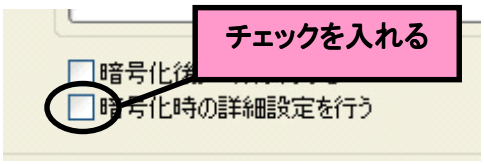


8－3 暗号化の詳細設定

『CIPHERON Standard X Edition』では、暗号化をする際に、細かい設定が可能です。詳細設定では、4つのことが設定できます。

(1)ファイルの履歴管理のオン／オフ
(2)暗号化元ファイルの完全削除
(3)暗号化ファイルの出力先指定
(4)復号化有効期限の設定

アドバンストメニュー使用時に暗号化時の詳細設定を行いたい場合は、画面右下の「暗号化時の詳細設定を行う」にチェックを入れてから[**暗号化**]をクリックしてください。ミニ工房を使用している場合は、このような操作は必要ありません。

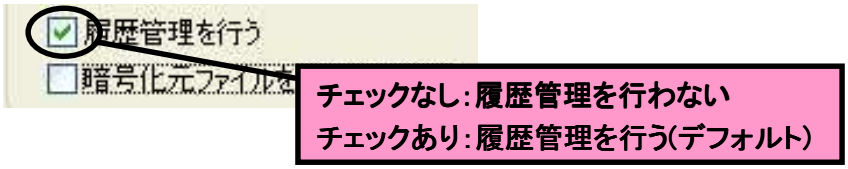


履歴管理をしていない場合、ファイルの履歴表示・ファイルの転送をすることはできません

Ver 1.03 以前の『VSC-P2P』をお使いいただいている相手に暗号化ファイルを送信する場合は、必ず履歴管理をオフにしてください。

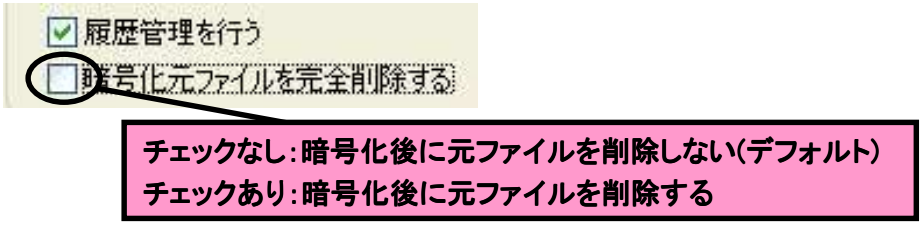
(1)ファイルの履歴管理のオン／オフ

「暗号化時の詳細設定を行う」にチェックがある場合、**[暗号化]**をクリックすると、暗号化の詳細設定ダイアログが表示されます。ここで暗号化ファイルの履歴管理のオン／オフを設定します。履歴管理がオフの場合は、ファイルの履歴表示およびファイルの転送はできません。初期設定ではオンです。



(2)暗号化元ファイルの完全削除

履歴管理のオン／オフと同じように、暗号化の詳細設定ダイアログで、暗号化が終了した後で、暗号化の元になったファイルを削除するかどうかを設定します。初期設定ではオフです。



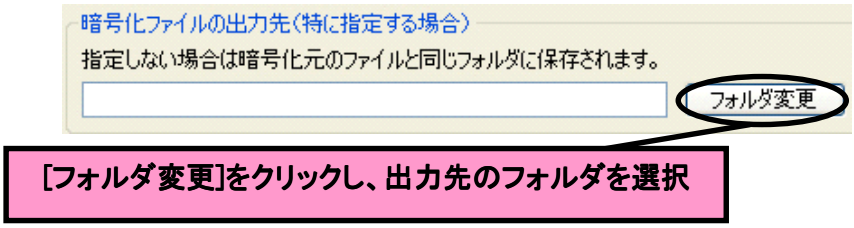
(3)暗号化ファイルの出力先指定

暗号化ファイルは特に指定しない場合、暗号化元のファイルと同じ場所に出力されますが、出力先を指定することができます。初期設定では出力先は指定されていません。

Check ！！

オプションで出力先を指定している場合は、そのディレクトリが表示されています

→9－1 p.80-



(4)復号化有効期限の設定

暗号化するファイルには、復号化有効期限を設定することができます。有効期限を過ぎている暗号化ファイルは復号化ができなくなり、強制削除されます。初期設定では復号化有効期限は設定されていません。

「暗号化を行った時点からの有効期限設定」

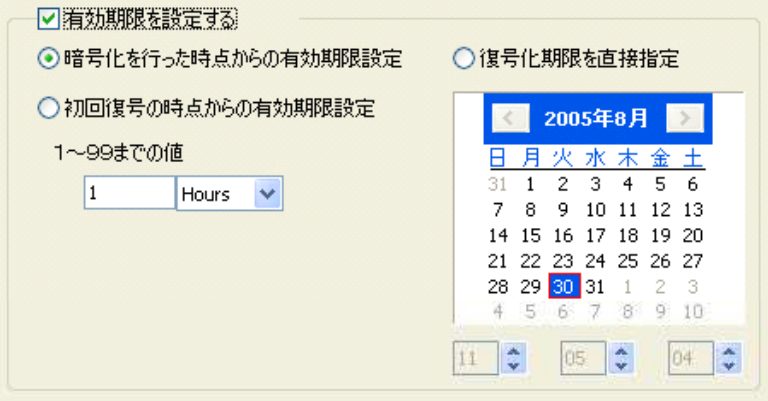
暗号化を行った時点からの復号化有効期限を設定します。1から99までの値を入力し、単位を指定してください。

「初回復号の時点からの有効期限設定」

初めてファイルが復号化された時点からの有効期限を設定します。1から 99 までの値を入力し、単位を指定してください。

「復号化期限を直接指定」

復号化できる期限を直接指定します。カレンダーで日付を選択し、時間を指定してください。



8－4　宛先リストからの暗号化

Check ！！

ミニ工房から暗号化したい場合は

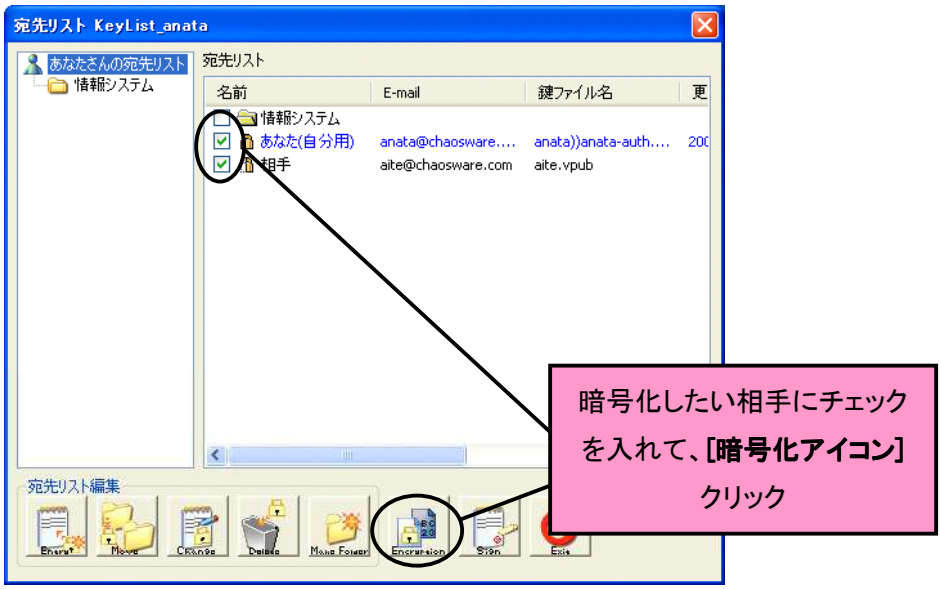
→3－1　p.18-

5－1　p.33-

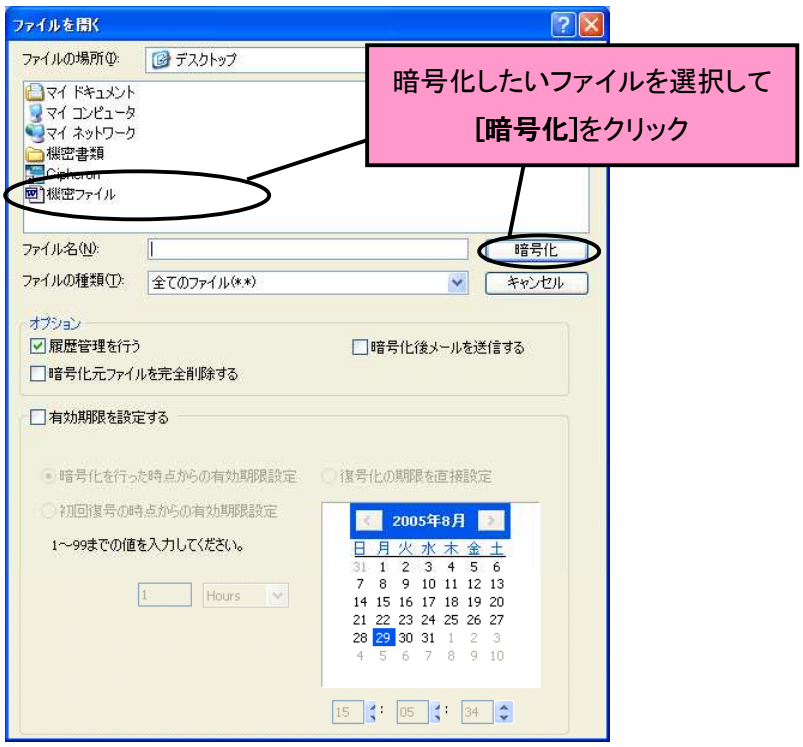
アドバンストメニューから暗号化したい場合は

→6－3　p.48-

ファイルの暗号化は宛先リストからも行えます。暗号化したい相手にチェックを入れてください。フォルダにチェックを入れると、そのフォルダ内のすべてにチェックが入ります。相手を選択し終わったら、**[暗号化アイコン]**をクリックしてください。



暗号化するファイルの選択および暗号化の詳細設定の画面が表示されるので、暗号化するファイル、復号化有効期限などを設定し、**[暗号化]**をクリックしてください。



8－5　一時復号化

Check　！！

暗号化ファイルの履歴表示については

→6－4　p.53-

『CIPHERON Standard X Edition』は暗号化ファイルの一時復号化ができます。この機能により、暗号化ファイルの中身を確認したり修正したいときに、ファイルを復号化し、修正を加え、また暗号化するという面倒なプロセスを省くことができます。

また、履歴管理を行っている暗号化ファイルの場合は、一時復号化による暗号化ファイルへの操作が履歴に記録され、**“暗号化ファイルの履歴表示”**によって確かめることができます。

一時復号化をしたい暗号化ファイルをダブルクリックしてください。関連するアプリケーションが起動し、閲覧や更新をすることができます。

８－６　右クリックメニュー

右クリックメニューを活用することによって、『CIPHERON Standard X Edition』を起動することなく暗号化などを行うことができます。

右クリックメニューでは以下の5つのことが可能です。

（1）ファイルの暗号化

（2）ファイルの復号化

（3）ファイルの履歴表示

（4）ファイルの転送

（5）ファイルの抹消

Check　！！

ミニエ房からの暗号化については

→３－１　p.18－

５－１　p.33－

アドバンストメニューからの暗号化については

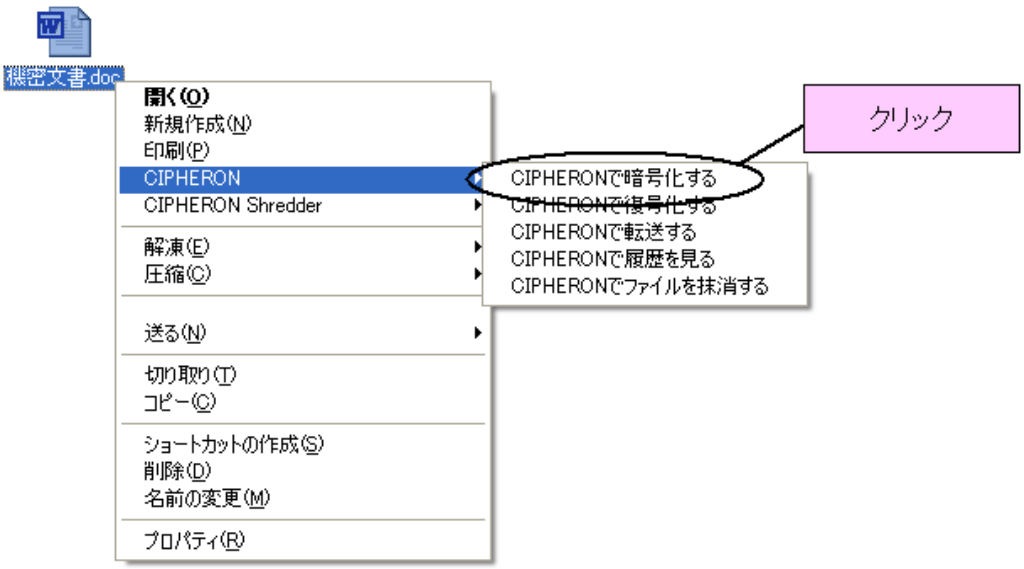
→７－３　p.59→

宛先リストからの暗号化については

→８－４　p.74－

（1）ファイルの暗号化

暗号化したいファイルを選択し、右クリックをして[CIPHERON で暗号化する]をクリックしてください。



[CIPHERON で暗号化する]をクリックすると、暗号化のメニューが表示されるので、暗号化の相手や暗号化の詳細設定を行い、[暗号化後保存]または[暗号化後メール添付]をクリックしてください。

Check ！！

ミニ工房からの復号化については

→3－2 p.19-

5－2 p.35-

アドバンストメニューからの復号化については

→7－3 p.59-

(2)ファイルの復号化

復号化したい暗号化ファイルを選択し、右クリックをして[CIPHERON で復号化する]をクリックしてください。

[CIPHERON で復号化する]をクリックすると、復号化するファイルの保存先を指定するダイアログが表示されるので、保存したい場所を指定し、[復号実施]をクリックしてください。

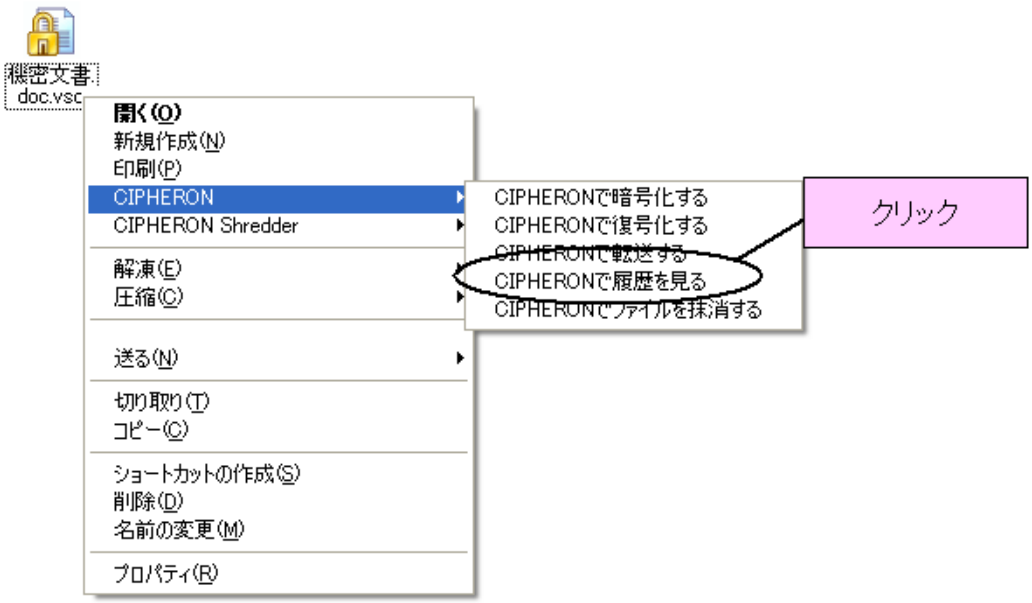
(3)ファイルの履歴表示

履歴表示したい暗号化ファイルを選択し、右クリックをして[CIPHERON で履歴表示する]をクリックしてください。

Check ！！

履歴については

→7－4 p.65-



[CIPHERON で履歴表示する]をクリックすると、ファイルの履歴が表示されます。

Check ！！

ファイルの転送については

→7－4 p.65-

(4)ファイルの転送

転送したい暗号化ファイルを選択し、右クリックをして[CIPHERON で転送する]をクリックしてください。

[CIPHERON で転送する]をクリックすると、転送相手の選択になります。転送したい相手にチェックを入れ、[転送実施]をクリックしてください。

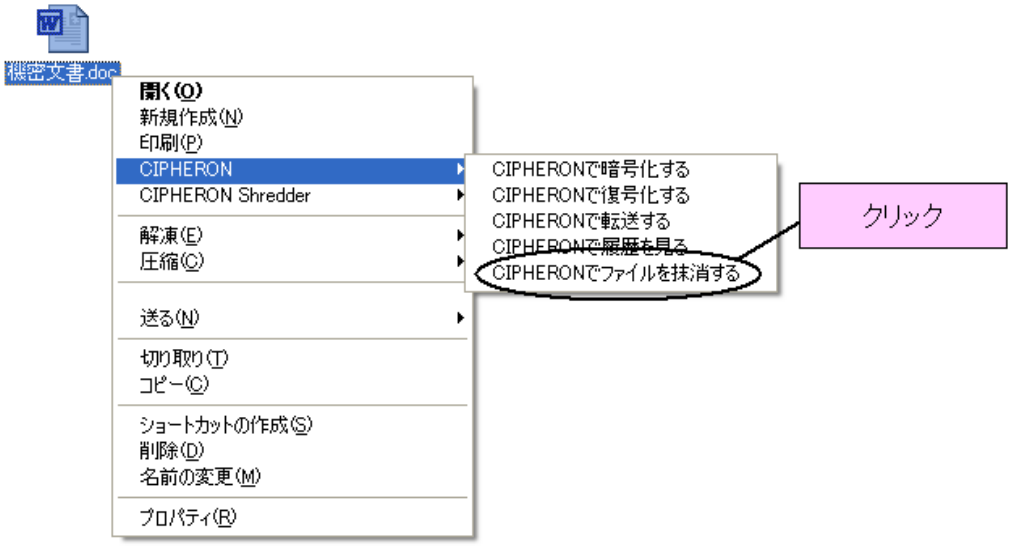
(5)ファイルの抹消

抹消したいファイルを選択し、右クリックをして[CIPHERON で抹消する]をクリックしてください。

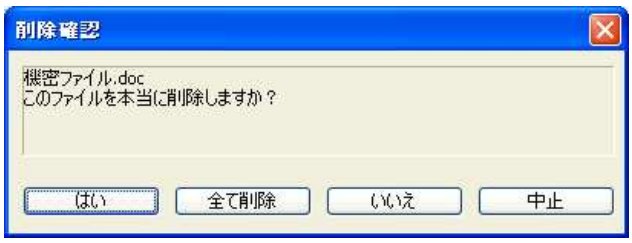
Check ！！

ファイルの抹消については

→7－5 p.68-

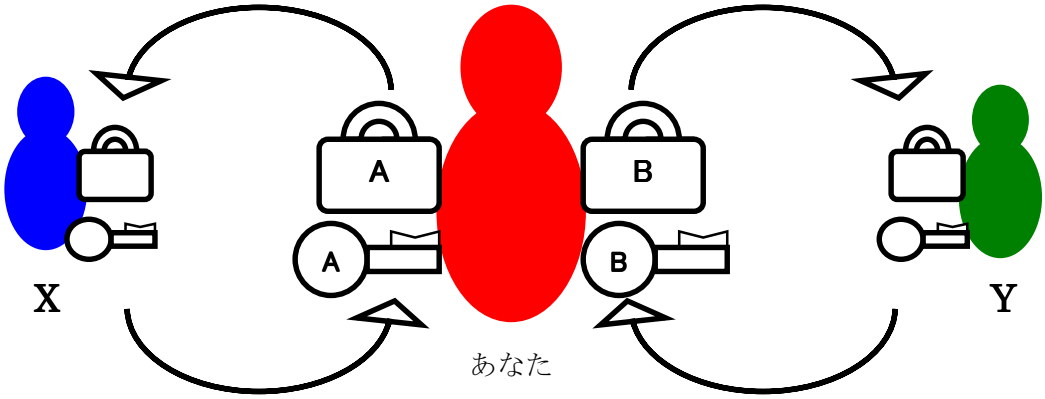


クリックすると、以下のようなダイアログが表示されます。本当にファイルを抹消するならば[**はい**]か[**すべて削除**]を、キャンセルするならば[**いいえ**]か[**中止**]をクリックしてください。



8－7　鍵の選択

鍵セットの生成を行うことにより、複数の鍵を管理しなくてはならないことがあります。
以下の図を見てください。



このような場合、X さんとは“A”という鍵セットを介して暗号化のやりとりをし、Y さんとは“B”という鍵を介して暗号化のやりとりをしています。そのため、X さんとは“B”の鍵を用いて暗号化のやりとりをすることはできませんし、Y さんとは“A”の鍵を用いて暗号化のやりとりをすることはできません。そこで、相手に合わせて鍵を選択しなければなりません。

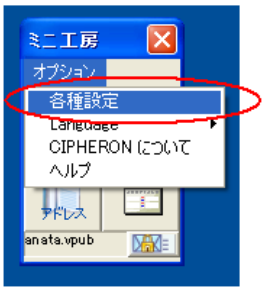
鍵の選択は、ミニ工房からもアドバンストメニューからも行うことができます。

第9章　環境設定

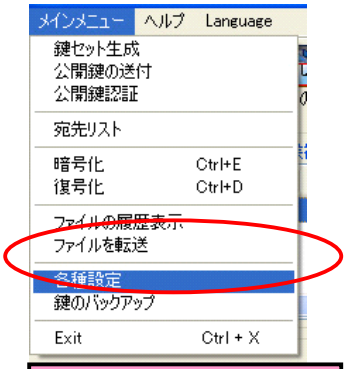
この章では、オプションを用いた『CIPHERON Standard X Edition』の環境設定について解説します。

9－1　オプション設定

オプション設定は、ミニ工房からもアドバンストメニューからも行うことができます。



ミニ工房



アドバンストメニュー

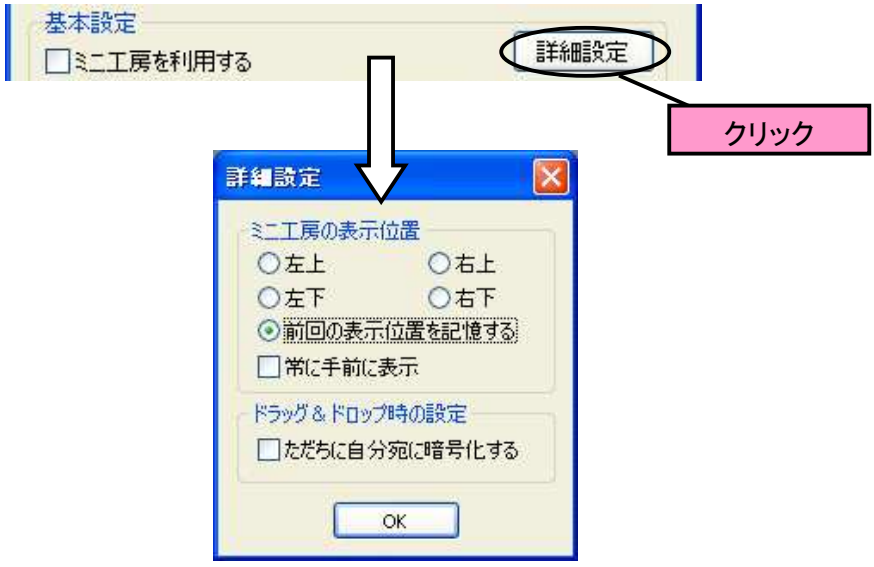
オプションでは以下の環境を設定することができます。

(1)ミニ工房の詳細設定
(2)特定フォルダの自動暗号化／復号化
(3)暗号化・復号化処理時の設定
(4)自分の宛先データの変更

(2)に関しては**「3－3　特定フォルダを自動的に暗号化／復号化をする(p.20-)」**を参照してください。

(1)ミニ工房の詳細設定

ミニ工房の詳細設定を行います。**[詳細設定]**をクリックしてください。



「ミニ工房の表示位置」

『CIPHERON Standard X Edition』を起動したときのミニ工房の表示位置です。「前回の表示位置を記憶する」にした場合は、最後にミニ工房のあった位置に表示されます。初期設定では「右下」です。

「常に手前に表示」

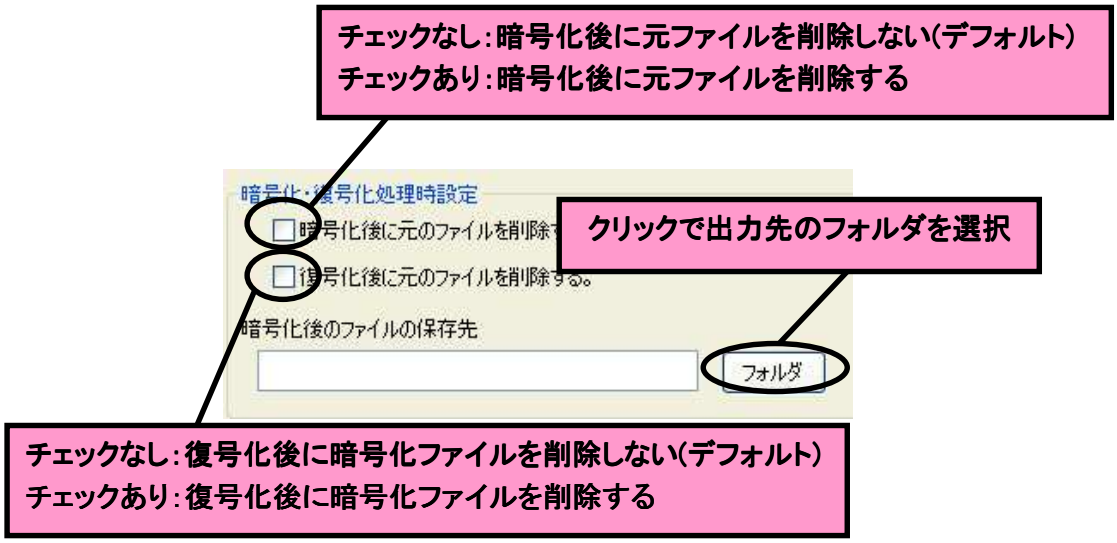
チェックを入れると、別のファイルやアプリケーションを開いていても、常にミニ工房が画面の手前に表示されます。初期設定ではチェックはオンです。アドバンストメニューには適用されません。

「ただちに自分宛に暗号化する」

チェックを入れると、ミニ工房にファイルをドラッグ＆ドロップしたときに、暗号化の詳細設定が省略され、すぐに自分宛ての暗号化ファイルが作られます。初期設定ではオフです。

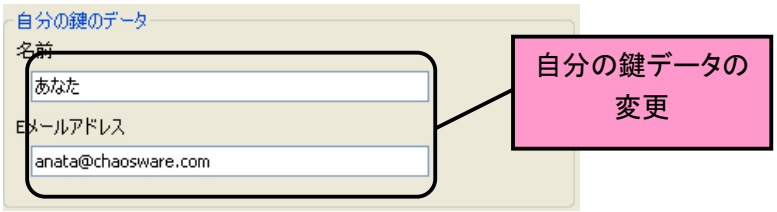
(3)暗号化・復号化処理時の設定

暗号化・復号化処理時に元のファイルを削除するかどうか、暗号化ファイルの出力先を設定することができます。



(4)自分の宛先データの変更

(自分用)となっている宛先データの名前とＥメールアドレスの変更ができます。



Check ！！

宛先リストについては

→4－4 p.28-

９－２　言語の選択

『CIPHERON Standard X Edition』は日本語と英語の言語の選択ができます。ご使用の環境に合わせて設定してください。

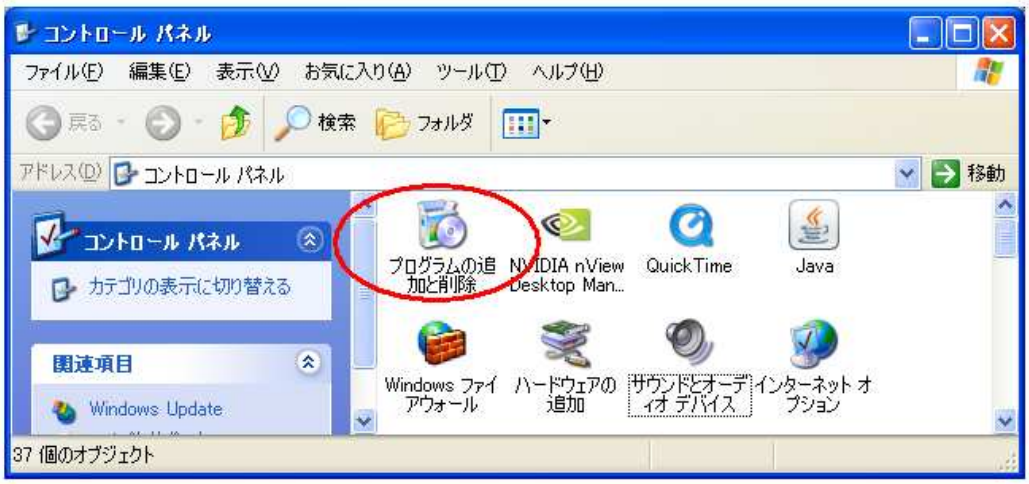
ミニ工房

アドバンストメニュー

９－３　ソフトのアンインストール

ソフトを削除すると、暗号化ファイルを復号化できなくなるので、削除の前にすべての暗号化ファイルを復号化してください

『CIPHERON Standard X Edition』のアンインストールはコントロールパネルから行います。コントロールパネル内のメニュー[**プログラムの追加と削除**]をクリックしてください。



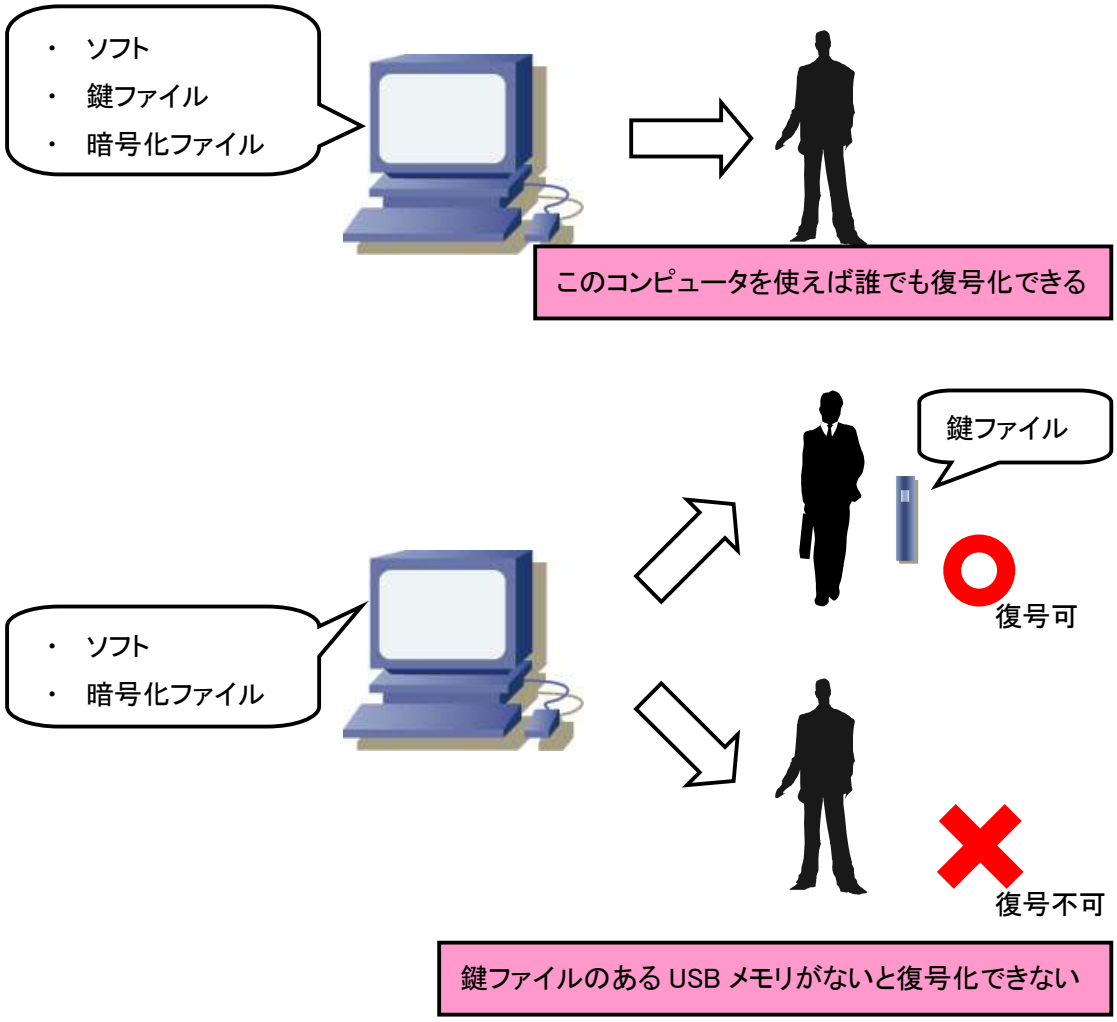
プログラムの追加と削除中のメニュー内の”CIPHERON StandardX”に関する欄には「変更」及び、「削除」というボタンありますので [**削除**]をクリックすると、お使いのコンピュータからソフトが削除されます。なお、鍵管理フォルダはアンインストールで削除されないので、こちらはエクスプローラ上からの削除を行ってください。

第10章　その他

この章では、『CIPHERON Standard X Edition』を使用するにあたって、互換性のあるメールソフトや、より安全にやり取りを行うための方法を紹介します。

10－1　鍵の管理は USB メモリで

暗号化されたデータは、ソフト・鍵ファイルがそろうことで復号化されます。そのため、暗号化ファイルとソフト、鍵ファイルが同じコンピュータ上にすると、そのコンピュータを使う全ての人間が暗号化ファイルを復号化できてしまいます。もしコンピュータ自体を盗まれてしまった場合、たとえデータを暗号化していても、簡単に復号化されてしまいます。そのため、鍵の管理は USB メモリで行ってください。



鍵ファイルなどを入れた USB を紛失・破壊してしまうと、復号化できなくなるため、鍵ファイルはバックアップを取ることをお勧めします
弊社で行っているバックアップサービスについては
→p.85−

１０－２　メールソフトについて

『CIPHERON Standard X Edition』では、下記の作業時、メール等で情報を送る必要があります。これらの作業時に、『CIPHERON Standard X Edition』は**自動的に現在お使いのメールソフトを起動させ**、所定のファイルを自動的に添付する機能を備えています。

Hotmail などの web メーラや Notes などのグループウェアを使用している場合は自動添付はされませんので、作業を行うときは手動でメーラを起動し、必要ファイルを添付してください

- “公開鍵”の送付のとき⇒４－３ p.27-
- 暗号化ファイルの転送のとき⇒７－４ p.65-
- 暗号化ファイルの送信のとき⇒５－１ p.33-
- “認証済み公開鍵”の送信のとき⇒８－１ p.70-
- 鍵のバックアップサービスのとき⇒p.85

自動的に添付が行えるのは**MAPI 対応メールソフト**と呼ばれるメールソフトのみとなります。**MAPI 対応メールソフト**の代表例として、下記のソフトウェアが挙げられます。

メールソフト横の(*)は、当社で動作確認を行ったメールソフトです

- Microsoft Outlook (*)
- Microsoft Outlook Express (*)
- Mozilla Mail
- Mozilla Thunderbird (*)
- Netscape Mail (*)
- Eudora Version6 (*)
- Becky!
- Shuriken

他の MAPI 対応メールソフトでも正常に添付されないことがあります

下記メールソフトにおいては、添付ファイルが正常に添付されないことが確認されています。

- Eudora Ver4.3
- Eudora Ver5.0

鍵のバックアップについて

『CIPHERON Standard X Edition』の鍵のバックアップについて説明します。

鍵の復元サービスは有料(¥3,150-)です。

鍵の復元サービスの概要

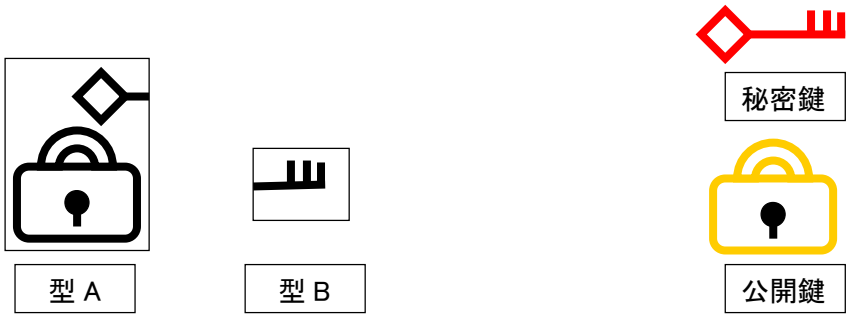
○秘密分散法を用いた半鍵管理によるバックアップ

弊社では秘密鍵・公開鍵の紛失や破損時に、鍵の復元サービスを行っております。事前に鍵の型を弊社に登録しておくことでご利用になれます。

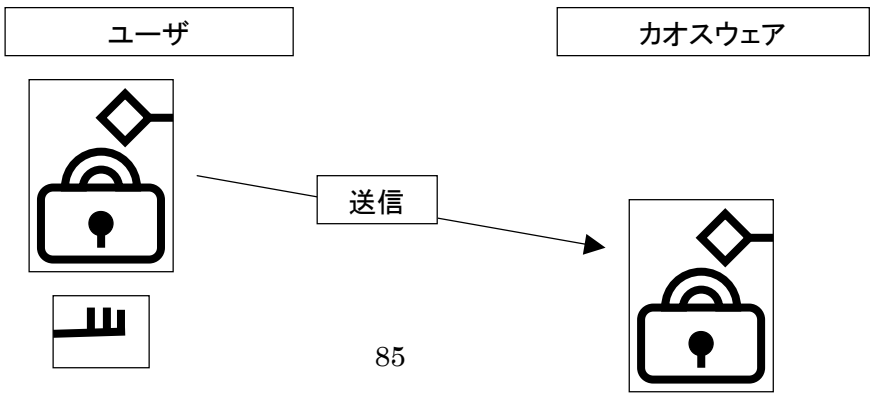
鍵セット生成時に、[**バックアップサービスを利用する**]にチェックを入れる、あるいはアドバンストメニュー上のメインメニューから[**鍵のバックアップ**]をクリックしていただきますと、鍵の復元用の型Aと型Bが作成されます。型の作成と同時にメールソフトが起動し、型Aが添付されますので、そのままメールを弊社に送信してください。送信された型 A は弊社に登録されますが、型Aだけでは鍵全体を復元することはできません。

次に、実際にお使いの鍵を紛失あるいは破損してしまった場合に、アドバンストメニュー上のツールバーから[**鍵の修復依頼**]アイコンをクリックします。[**鍵の修復依頼**]アイコンをクリックすると、メールソフトが起動し、型 B が添付されますので、メールを弊社に送信してください。弊社では送信された型Aと型Bを合成し、鍵を復元して CD-ROM で返送いたします。送っていただいた型Bは破棄されるので、弊社が完成した復元用の型および、復元された鍵を保持することはありません。

＜[**鍵のバックアップ**]クリック時に作成されるファイル＞

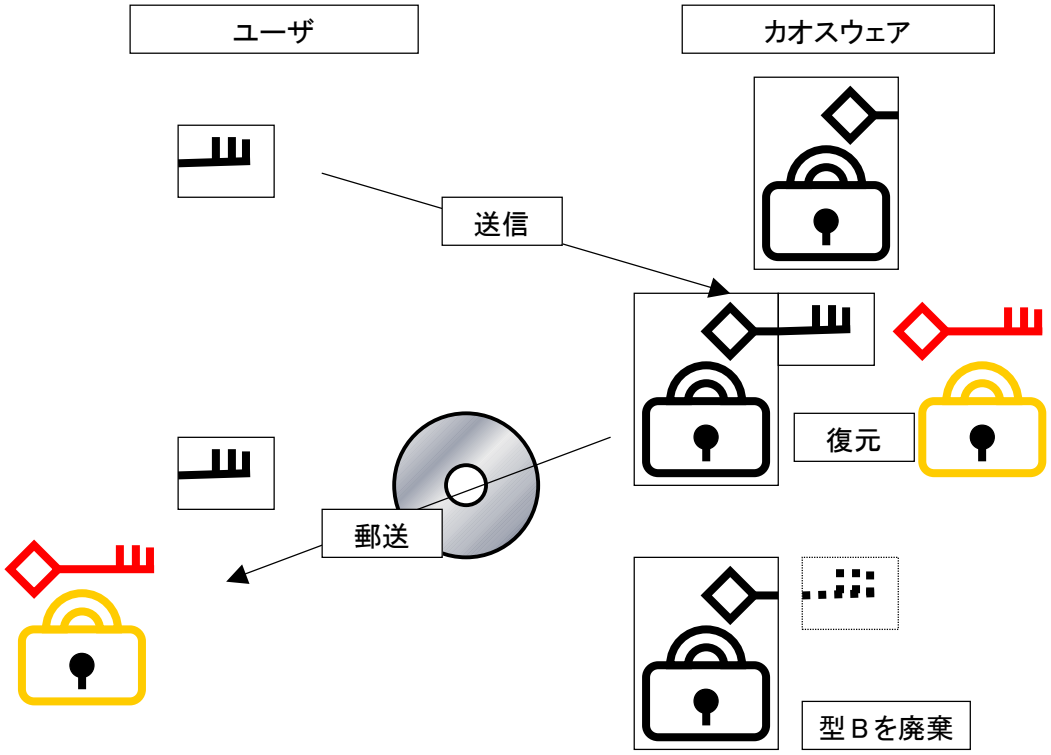


＜鍵のバックアップファイル送信＞



鍵を復元した後、送信していただいた型は廃棄いたしますので、弊社がお客様の秘密鍵を保持することはありません

＜[鍵の復元依頼]クリック時＞



もしメールソフトが自動的に起動しない場合は、手動でメールに復元用の型を添付してください。『CIPHERON Standard X Edition』実行ファイルのあるフォルダに保存されているOOOO_cw.vbky.vsc というファイルが型 A、OOOO_user.vbky というファイルが型 B(それぞれの OOOO には鍵ファイル名が入ります)です。送信先メールアドレスは key@chaosware.com です。

○鍵の復元

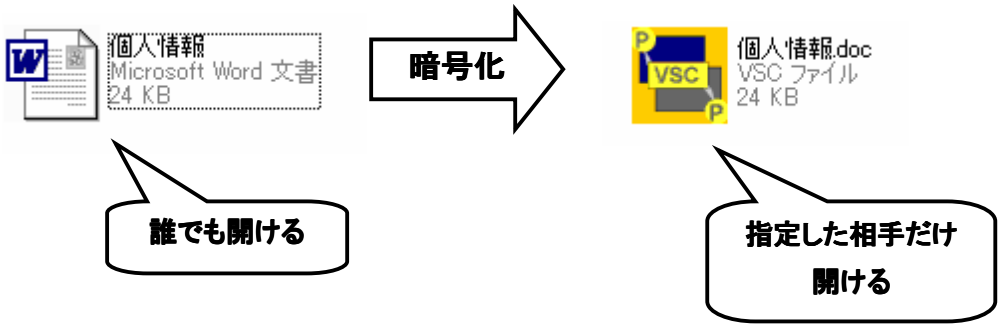
鍵の復元依頼をお受け次第、弊社で鍵を復元し、復元された鍵および、鍵の再登録用のツールを CD-ROM に保存して郵送いたします。鍵の再登録用のツールをダブルクリックし、ツールの指示通りに操作を行ってください。

Q&A

この章では『CIPHERON Standard X Edition』をご使用の際の、よくある質問をとりあげます。

Q1. このソフトはいったい何をするソフトなのですか？

A.　このソフトは、重要なファイルや第三者に知られたくないデータなどを暗号化するためのソフトです。



Q2. 復号化できません。

この問題のよくある原因として、2つ挙げられます。

①暗号化の宛先が異なっている

②ver1.03 以前のバージョンの『VSC-P2P』で暗号化されたファイルを『CIPHERON Standard X Edition』で復号化した

次ページから対処法を解説します。

＜考えられる原因と解決策①＞

暗号化の際に、暗号化の相手が間違っていた、もしくは復号化する鍵が間違っている可能性があります。

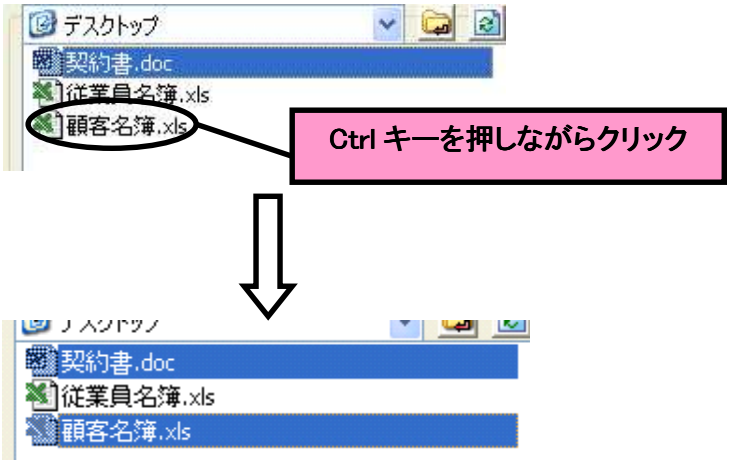
上のように暗号化相手が選択されて暗号化が行われていた場合、太郎・次郎・三郎しかその暗号化ファイルを復号化ができません。一度暗号化し直したファイルを取得して復号化を行ってみてください。

＜考えられる原因と解決策②＞

『CIPHERON Standard X Edition』は姉妹製品である『VSC-P2P』と互換性がありますが、ver1.03 以前のバージョンの『VSC-P2P』とは**“暗号化ファイルの履歴管理”**の互換ができません。そのため、『CIPHERON Standard X Edition』で暗号化し、1.03 以前のバージョンの『VSC-P2P』で復号化する際は、**“暗号化ファイルの履歴管理”**のチェックを外して暗号化をしてください。

Q3. 宛先やファイルを複数一括して選択したいのですが、どうすればよいですか？

A.　宛先やファイルを選択する際に、Ctrl キーを押しながら選択してください。



また、暗号化の宛先を選択するときに、宛先の入っているフォルダごと選択すると、フォルダ内の全ての宛先が選択されます。

Q4. 暗号化するとファイルのサイズが大きくなったのですが、どうしてですか？

A.　暗号化を行った際の情報が加えられているため、暗号化を行うと数 byte だけファイルサイズが大きくなります。

Q5. ［暗号化ファイルをメールに添付する］を押しても、メールソフトが起動しないのですが、なぜですか？

A. 自動起動対応は MAPI 対応のメールソフトのみとなっています。そのため、Hotmail などの web メールや、Notes などのグループウェアではこの機能は使用できません。手動でメールソフトを起動してください。メールソフトについては１０－２ p.84-をご覧ください。

Q6. エクスプローラ上でマウスの右ボタンをクリックした際に表示されるメニュー（「CIPHERON で暗号化する」 etc.）が表示されないのですが、どうしてですか？

A. 登録にはアドミニストレータ権限が必要です。

Q7. エクスプローラ上でマウスの右ボタンをクリックした際に表示されるメニュー（「CIPHERON で暗号化する」 etc.）が消せません。

A. ソフトをアンインストールすることで削除されます。

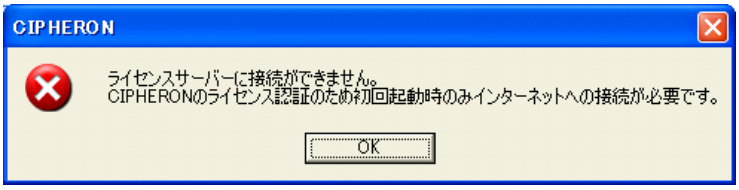
Q8. 暗号化ファイルを圧縮できません。

A. 暗号化ファイルは、ソフトによっては圧縮することはできませんが、暗号化ファイルを圧縮してもファイルサイズは小さくなりません。また、ファイルが壊れることがあるので暗号化ファイルの圧縮はしないでください。ファイルサイズを小さくしたい場合は、先に圧縮をかけてから暗号化を行ってください。

第11章　トラブルシューティング

この章では『CIPHERON Standard X Edition』ご使用の際のトラブルの原因と対処法について簡単に解説します。

＜インストール＞



原因：

以下の原因が考えられます。

① インターネットに接続されていない

② ご利用の PC へ導入されているファイアーウォールが CIPHERON のネットワーク接続を許可していない。

③ HTTP, HTTPS 接続のためのプロキシ設定を InternetExplorer 以外のソフトウェアで設定している

④ ご利用中のネットワークのポリシーにより、規定で定められたソフトウェア以外ネットワーク接続が禁止されている

対処：

以下の方法で解決できます。

① CIPHERON 初回起動時のみ、ライセンス認証のためにネットワークへの接続が必要です。オフィス内の LAN 等を利用した上でインターネットに接続してください。

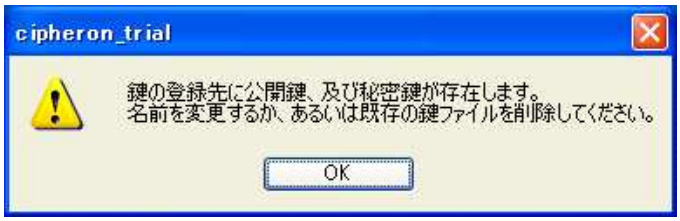
② ファイアーウォールのホワイトリストに CIPHERON を加えてください。ファイアーウォールの設定につきましては、各ソフトウェアのヘルプ及び、システム管理者へ御問い合わせください。

③ CIPHERON では InternetExplorer の設定を参照する形でネットワーク設定を行っております。InternetExplorer 以外のソフトウェアで行われている設定を InternetExplorer へ反映させてください。

④ CIPHERON からの外部ネットワークへの接続、及び、弊社サイトへの接続禁止解除が必要です。システム管理者へ御問い合わせください。

＜鍵の設定＞

原因:鍵の名前に¥ / : * ? " < > | が含まれていた
対処:鍵の名前に、上記の禁止文字を使わないでください



原因:過去に作成した鍵セットと同じ名前の鍵を設定しようとした
対処:別の名前をつけてください

＜暗号化＞

原因:オプションで暗号化ファイルの出力先を外部記憶装置などに指定し、その外部記憶装置がない状態で暗号化を実行した
対処:オプションで暗号化ファイルの出力先を変更するか、暗号化時の詳細設定でファイルの出力先を変更してから暗号化を実行してください

原因：他のアプリケーションで編集中のファイルを暗号化した
対処：編集中のファイルを閉じてから暗号化を実行してください

＜復号化＞

原因：復号化権限のない暗号化ファイルを復号化した
対処：復号化権限のない暗号化ファイルは復号化できません

原因：復号化有効期限の過ぎた暗号化ファイルを復号化した
対処：復号化有効期限の過ぎた暗号化ファイルは復号化できません

＜履歴表示＞

原因:復号化権限のない暗号化ファイルの履歴を表示しようとした
対処:復号化権限のない暗号化ファイルの履歴は表示できません

原因:履歴管理を行っていない暗号化ファイルあるいは暗号化されていないファイルの履歴を表示しようとした
対処:履歴管理を行っていない暗号化ファイルあるいは暗号化されていないファイルの履歴を表示することはできません

＜転送＞

原因:履歴管理を行っていない暗号化ファイルあるいは暗号化されていないファイルを転送しようとした
対処:履歴管理を行っていない暗号化ファイルあるいは暗号化されていないファイルを転送することはできません

その他のトラブルシューティングについてはオンラインヘルプをご覧ください。

索 引

M

MAPI 対応メールソフト.....84

Q

QR コード.....48, 49, 50, 53, 54

R

RSA 1, 10

U

USB メモリ 1, 3, 10, 21, 22, 23, 24, 83

あ

アカウント開設.....49

アドバンストメニュー3, 53, 58, 59, 68, 72, 79, 80, 81, 85

暗号化1, 2, 3, 5, 10, 11, 12, 17, 19, 20, 21, 22, 23, 25, 26, 27, 28, 31, 34, 35, 36, 38, 39, 58, 59, 60, 61, 62, 63, 65, 66, 67, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 83, 84, 87, 88, 89, 90, 92, 93, 94

暗号化後保存.....35, 76

暗号化の相手.....11, 34, 76, 88

暗号化の詳細設定.....35, 73, 75, 76

暗号便3, 41, 42, 43, 44, 47, 48, 49, 50, 51, 53, 55, 56

い

一時復号化.....3, 66, 75

インストール2, 3, 13, 14, 15, 82, 90, 91

え

閲覧.....10, 12, 66, 75

お

オプション 3, 10, 21, 80, 92

か

外部記憶装置 10, 21, 92

鍵セット. 3, 17, 18, 59, 69, 79, 85, 92

こ

公開鍵1, 3, 10, 26, 28, 29, 36, 38, 59, 70, 71, 72, 84, 85

公開鍵の認証 3, 70, 71

工房 60, 63, 65, 67, 68

し

自動暗号化 10, 21, 23, 80

自動復号化 21, 24

自分宛て 2, 19, 36, 39, 81

シリアル番号 16, 17

新規作成 66

た

ダウンロード 12

他人宛て 2, 27, 34

て

転送3, 11, 59, 65, 67, 68, 73, 76, 78, 84, 94

と

動作環境 2, 13

に

認証 11, 71, 72, 84

は

パスワード 10, 16, 17

バックアップ 4, 59, 84, 85

ひ

秘密鍵 10, 85

ふ

復号化1, 2, 3, 5, 10, 11, 17, 19, 20, 21, 22, 23, 24, 28, 34, 35, 36, 37, 38, 39, 40, 58, 59, 63, 64, 65, 66, 67, 72, 73, 74, 75, 76, 77, 80, 81, 83, 87, 88, 93, 94

復号化有効期限 11, 73

み

右クリックメニュー 3, 76

ミニ工房19, 20, 34, 36, 38, 39, 53, 58, 59, 63, 72, 79, 80, 81

ら

ライセンス認証 91

り

履歴管理10, 65, 67, 72, 73, 75, 88, 94

履歴表示3, 58, 59, 65, 66, 73, 75, 76, 77, 94

ろ

ログイン. 50, 51, 52

カオスウェアについて

カオスウェアは、独立行政法人情報通信研究機構(NICT)プレベンチャー制度及び、科学技術振興機構(JST)プレベンチャー制度により誕生した NICT 発第１号のベンチャー企業です。
研究機構内で培ってきた多くの技術、開発の特許や経験を生かし、皆様に私たちの製品を通し、ユビキタス社会のための次世代情報通信インフラの新しいコンセプトを提案していきたいと思っております。

- 開発元： 株式会社カオスウェア
  (http://www.chaosware.com/)
  ○住所：東京都小金井市貫井北町４－２－１
  独立行政法人情報通信研究機構内　産学官研究交流棟２Ｆ
  ○TEL：042-359-6299
  ○FAX：042-359-6339

- お客様お問合せ先: cipheron@chaosware.com

- VSC(Vector Stream Cipher)は、独立行政法人情報通信研究機構(http://www.nict.go.jp/)とその他の共有する日本国特許第 3030341 号、特許第 3455748 号、及び米国特許第 6,668,265 号で保護されている独自暗号アルゴリズムのストリーム暗号です。

法律上の注意

CIPHERON Standard X Edition(R) ユーザーズマニュアル(Windows(R) 版)

本マニュアルおよびその中に記載されているソフトウェアは、エンドユーザ使用許諾契約書にもとづいて提供されるものであり、当該エンドユーザ使用許諾契約書の契約条件に従ってのみ、使用または複製することが可能となるものです。本マニュアルに記載される内容は、あくまでも参照用としてのみ使用されること、また、なんら予告なしに変更されることを条件として、提供されるものであり、従って、当該情報が、ChaosWare Incorporated(カオスウェア社)の責務として解釈されることがあってはなりません。カオスウェア社は、本マニュアルにおけるいかなる誤謬または不正確な記述に対しても、なんら責を負うものではありません。当該エンドユーザ使用許諾契約書により許可されている場合を除き、本マニュアルのいかなる部分といえども、カオスウェア社の書面による事前の許可なしに、電子的、機械的、録音、その他いかなる形式・手段であれ、複製、検索システムへの保存、または伝送を行うことはできません。
例として使用されている会社名・人名等は、実在の会社・人物を示すものではありません。

Microsoft、およびWindows、およびWindows NT は、マイクロソフト社の米国および各国での商標または登録商標です。Pentium はIntel Corporation の登録商標です。その他すべての商標は、それぞれの権利帰属者の所有物です。
