

ファイル暗号パッケージ

# セキュアセブンV1.20のご紹介



株式会社イノス

2009年9月

# 目次

- セキュアセブンとは
- セキュアセブンの機能と特徴
  - － セキュアセブンの機能
  - － セキュアセブンの特徴
    - カオス理論とは
    - 高速暗号エンジンC4Customの実力
    - 暗号 / 復号のバッチ処理が可能
- セキュアセブンの制限事項と注意事項
- ご利用事例集
  - － 1. 現在のバックアップを暗号バックアップに変え、バックアップ媒体の盗難・データの漏洩に備える
  - － 2. 本社・支社間でのデータのやり取りを暗号化し、輸送経路上の盗難・紛失に備える
  - － 3. サーバー上の大切なデータや資料を暗号化しておき、許可された人のみが復号し、参照できるようにする
- 参考資料
  - － セキュアセブンの暗号処理速度
- 対応OS
- 価格及び保守について

# セキュアセブンは

個人情報保護法の施行や情報漏洩の事故のニュースが絶えない中、企業の重要な情報をいかに守っていくか、早急な対応が必要とされています。

- ◆ 情報を保護するためには、以下のようなポイントで総合的に対策をとる必要があります。
  - 組織的安全措置(管理体制の整備など)
  - 人的安全措置(社員への教育など)
  - 物理的安全措置(建物や部屋の入退出管理など)
  - 技術的安全措置(ファイアウォール、ウイルス対策、**暗号化**など)

セキュアセブンはデータを暗号化するツールです。  
情報保護、情報漏洩対策の1つとして活用することで、万が一事故が起こったとしても被害を最小限にとどめることができます。

# セキュアセブンの機能と特徴

## < 機能 >

セキュアセブンは7つの機能で、大切なデータを守ります。

- ◆ ファイル/フォルダの暗号化ができます。
- ◆ ファイル/フォルダの復号化ができます。
- ◆ 暗号時に圧縮も可能です。
- ◆ 暗号/復号処理のバッチ処理が可能です。
- ◆ 実行ログによって、実行結果管理が可能です。
- ◆ 環境設定で暗号キーを設定しておくことができます。
- ◆ バッチ実行時のエラーをエラー報告書としてプリンター出力できます。

# セキュアセブンの機能と特徴

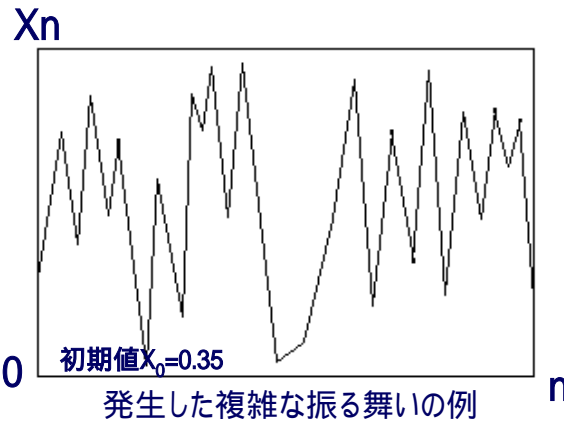
## <特徴>

セキュアセブンは‘カオス理論’を用いた暗号エンジン: C4Custom™を採用した、安全・高速な暗号ツールです。(C4Custom™は株式会社シーフォーテクノロジーの商標です。)

カオス関数の特徴の1つに‘初期値のごくわずかな違いが、その結果に膨大な差を生み出す’というものがあります。これによって与えた暗号キーの違いによってデータが不規則に暗号化されることとなります。規則性がないことは第三者からの解読を困難にします。

またカオス関数は‘比較的簡単な数式’で表現されるので、暗号化が高速に処理できます。‘暗号キーが長くなっても処理速度があまり落ちない’ことも特徴の1つです。長いキーが使用できることは、鍵総当りによる解読も難しいこととなります。

## ～カオス理論とは～ 比較的簡単な規則に支配された不規則振動

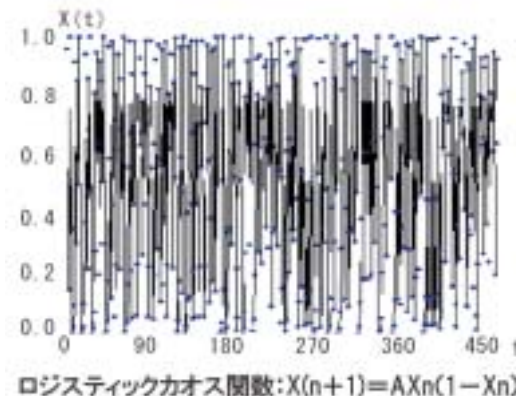


(特徴)

単純な関数形であるが、複雑な信号を発生  
初期値に敏感に反応  
一方向性を有する

一見不規則な値をとる数列 $\{X_n\}$ のグラフ。  
実は下記のようなロジックで出力されている。

$$X_{n+1} = 4 X_n (1 - X_n)$$

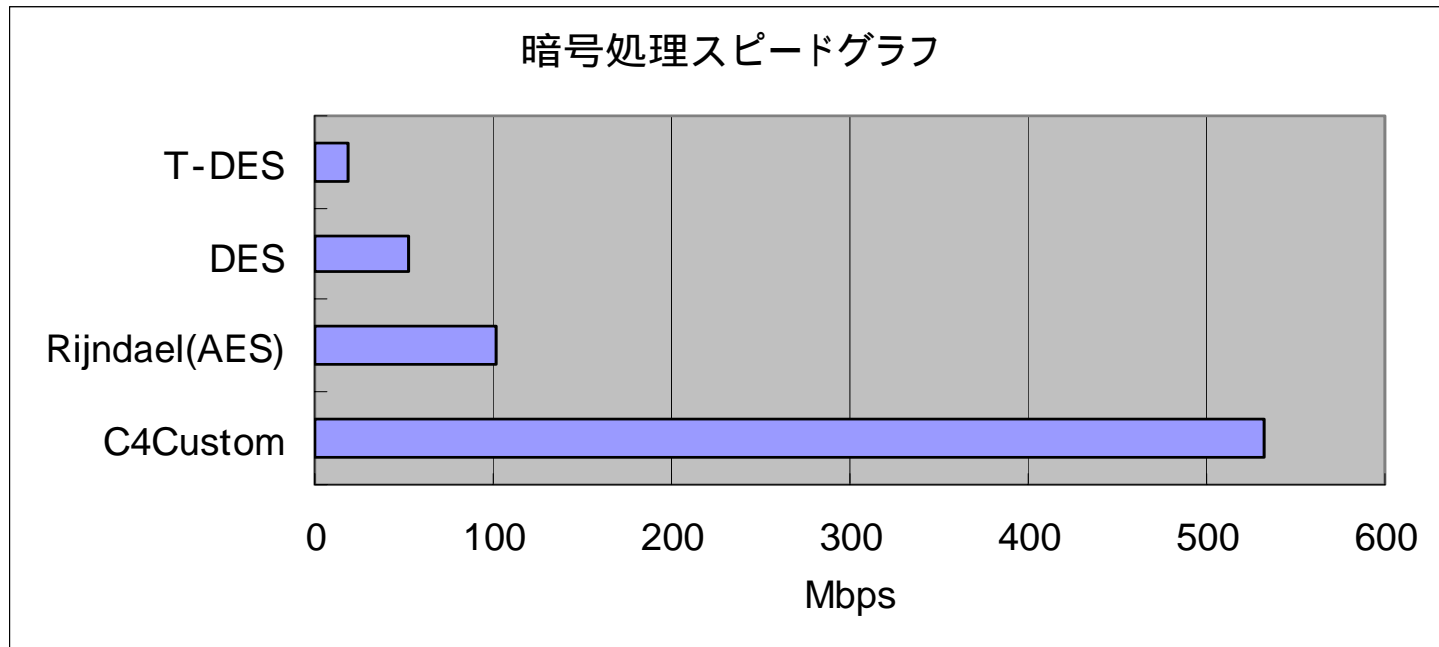


# セキュアセブンの機能と特徴

## < 特徴 >

### 高速暗号エンジン: C4Custom™ の実力

Pentium® 598MHz Key 256bitの環境下で、500Mbps以上の処理速度を実現しました。



Intel® Pentium®III/Celeron® Coppermine Processor with MMX 598MHz  
Windows® 2000 Service Pack 4 (測定環境により、測定結果が異なる場合がございます。)

# セキュアセブンの機能と特徴

## < 特徴 >

### 暗号 / 復号のバッチ処理が可能

◆バッチ実行可能なので、処理の自動化が可能です。システム管理者やシステム担当者が不在の時間にスケジューリングできます。(スケジューリングにはWindows®のタスク機能など別ソフトが必要です。)

◆実行コマンドをバッチファイルにしておけば、毎回同じ処理を画面からオペレーションする必要はありません。

◆市販のバックアップソフト「Backup Exec®」や「ARC serve®」と組み合わせることで、夜間バックアップを暗号バックアップにすることが可能です。

# セキュアセブンの制限事項と注意事項

## < 制限事項 - 1 >

セキュアセブンでは以下の制限事項があります。

- ◆ セキュアセブンでは「セキュアセブンがインストールされたフォルダ」と「トレース出力フォルダ」、「ネットワーク共有名」について、処理を行うことができません。
- ◆ ファイル名が256バイトを超える場合は処理できません。出力後256バイトを超える場合も同様にエラーとなります。
- ◆ マルチユーザには対応していません。
- ◆ 1つの端末内で、同時に起動できません。
- ◆ 復号時には暗号前のファイルの情報(サイズ / 属性 / 作成日時 / 更新日時)は引継ぎますが、セキュリティの情報は引継ぎません。出力先フォルダのセキュリティと同等となります。

# セキュアセブンの制限事項と注意事項

## < 制限事項 - 2 >

セキュアセブンでは以下の制限事項があります。

- ◆ FAT及びFAT32ファイルシステムでフォーマットされたドライブでは、フォルダを指定して暗号化 / 復号化を行う場合、暗号結果または復号結果の出力先に元フォルダと同じフォルダを指定すると、同じファイルを複数回処理してしまう誤作動を起こすことがあります。FAT及びFAT32ファイルシステムの場合、処理対象フォルダとは別のフォルダを出力先に指定してください。FDドライブはFATファイルシステムですので、ご注意ください。また、MOについては、フォーマット時にNTFSファイルシステムでフォーマットした媒体を使用するようにしてください。

例) 暗号化対象フォルダ	A:¥test1	出力先フォルダ	A:¥test2	正常処理
暗号化対象フォルダ	A:¥test1	出力先フォルダ	A:¥test1	異常処理

# セキュアセブンの制限事項と注意事項

## < 注意事項 - 1 >

セキュアセブンでは以下の注意事項があります。

- ◆ 「環境設定」に設定されたフォルダ配下に以下のファイルが出力されます。

「Tran\_log.txt」 (処理ログ)

「Err\_log.txt」 (エラーログ)

「環境設定」に設定された最大サイズを超過した場合、今まで作成したログファイルはバックアップとして残り、新しいファイルが作成されます。

尚、バックアップファイルは1世代のみ残る為、ログファイルでディスク空き容量を圧迫することはありません。

- ◆ ネットワーク上のファイルやフォルダを暗号(または復号)したり、暗号先(または復号先)をネットワーク上のフォルダに指定した場合、ネットワークの接続方法や接続先OS、環境によっては正常に動作しないことがあります。
- ◆ 設定キー、手入力キーの内容を確認することはできません。暗号時に使用したキーが分からなくなってしまうと、そのファイルを復号することは弊社サポートでも不可能ですのでご注意ください。

# セキュアセブンの制限事項と注意事項

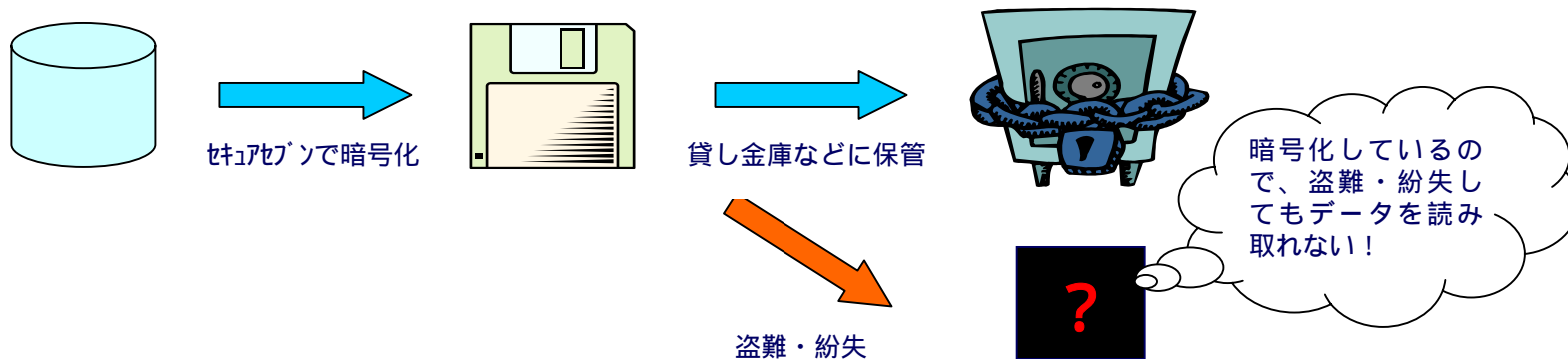
## < 注意事項 - 2 >

セキュアセブンでは以下の注意事項があります。

- ◆ 暗号時に圧縮処理を指定した場合、本ソフトウェアは最初に圧縮処理を行った後に暗号処理を行います。圧縮処理を行ったファイルはワークエリアに一時的に作成され、暗号処理が完了すると削除されます。このワークエリアが本ソフトウェアをインストールしたフォルダに必要になります。(4GBのファイルを圧縮して3GBになるとすると、一時的に3GBのワークエリアが必要です。)
- ◆ 暗号化 / 復号化の処理は他のアプリケーションが使用中のファイル / フォルダには行わないようにしてください。アプリケーションによっては、サービスを一旦停止しないと暗号化 / 復号化ができなかったり、アプリケーションが正常に動作しなくなる場合があります。特に暗号化後、「元ファイルを削除する」という設定にする場合は、ご注意ください。他のアプリケーションへの影響が出た場合でも、その損害等について弊社では補償いたしかねます。

# ご利用事例集

## 1. 現在のバックアップを暗号バックアップに変え、バックアップ媒体の盗難・データの漏洩に備える。



### Point!

#### < 暗号キーの管理・運用方法 >

暗号キーは定期的に変更することでより安全性が高くなります。ただし、定期的な変更はキーの管理者にとっては、大変なことです。

セキュアセブンは手入力キーと設定キーの2種類があります。設定キーを使用すればキーを忘れてしまっても復号できないということもありません。

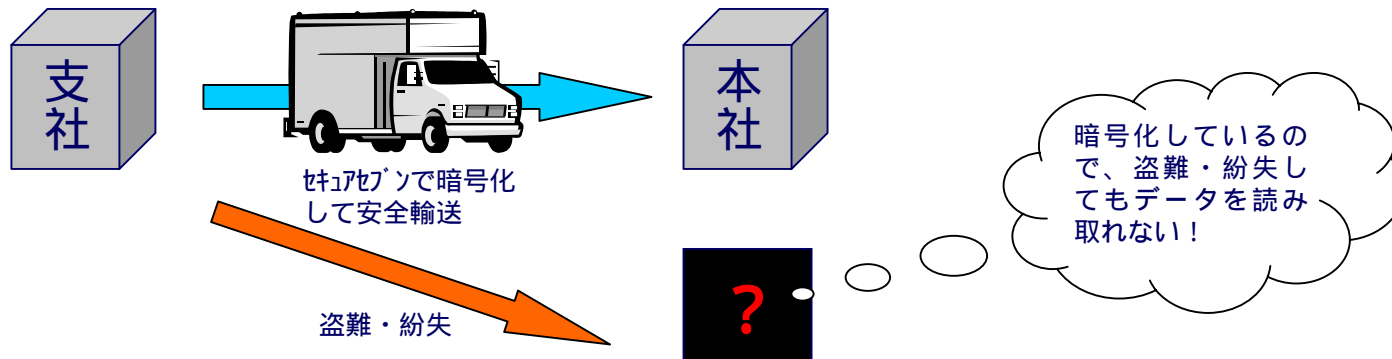
暗号化をバッチ実行する場合には設定キーを使用します。設定キーは最大99まで設定可能です。曜日ごと、月ごとに暗号キーを設定することが可能です。設定キー自体を変更する際には、暗号化しているデータが復号できなくなるように、暗号キーを別管理することも検討してください。

暗号キーを忘れてしまうとデータを復号することは弊社でも不可能です。管理者は1名でなく、2名～3名としておくと良いでしょう。暗号キーの変更時に管理者全員に新しいキーを知らせておくと、管理者の不慮の事故時にも対応できます。

暗号キーの作成ルールを作っておくことも、キーを忘れないための工夫です。例えば、会社名+管理者名+年月+曜日というルールを作成しておけば、キーを忘れてしまってもルールから再度設定できます。(キーには全角文字は使用できません。半角英数字で設定します。)

# ご利用事例集

## 2. 本社・支社間でのデータのやり取りを暗号化し、輸送経路上の盗難・紛失に備える。



### Point!

#### < 復号キーの伝え方 >

暗号したデータ送って送り先で復号化したい場合には、相手に復号キーを伝えて復号してもらう必要があります。このキーが一致していないと決して復号できません。

せっかく暗号化して安全に輸送できても、復号キーと一緒に送ってしまったら、盗難・紛失時にそのキーで復号されてしまう恐れがあります。復号キーは暗号化されたデータとは別に送らなければいけません。

復号キーを相手に送る例をご紹介します。

例1) テキストファイルに復号キーを記入し、そのファイルを最初に取り決めた暗号キー (例えば会社名) で暗号化してメール添付して送ります。受取った側は取り決められた暗号キーでテキストファイルを復号し、その内容をデータの復号キーとして使用します。

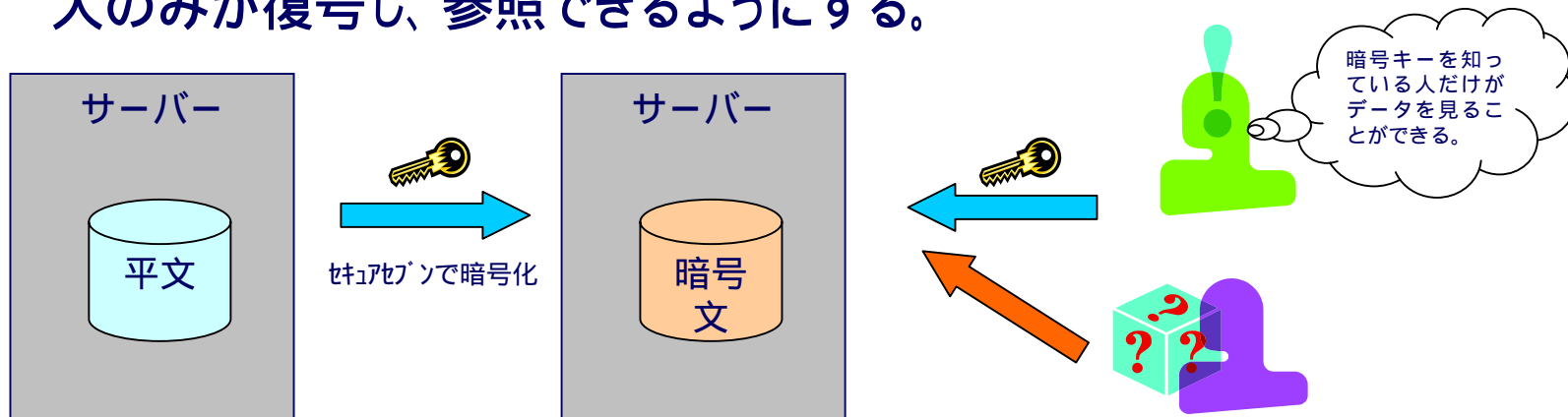
例2) 暗号キーの作成ルールを取り決めておきます。事例1と同様に暗号キーのルールを取り決めておけば、復号キーを相手に送る必要もありません。例えば支社名 + ファイル名 + 年月などとしておけば、支社事にキーが変わることになります。

暗号データを送る先を間違ってしまったとしても、相手は復号できません。

作業担当者と暗号キー管理者が異なる場合でも、管理者が暗号キー / 復号キーを設定キーとして設定しておけば、作業担当者に暗号キーを知らせることなく安全に運用可能です。

# ご利用事例集

## 3. サーバー上の大切なデータや資料を暗号化しておき、許可された人のみが復号し、参照できるようにする。



### Point!

#### < 共通サーバーの管理 >

共通サーバーのアクセス管理の方法としてフォルダごとにアクセス権限を設定する方法が良くとられます。内部の人間がデータを盗み見たり、データをコピーすることを防ぐ方法の1つです。

この方法でも、フォルダのアクセス権限自体を操作できるシステム管理者や、ハッカーのような存在であれば簡単にそのフォルダにアクセスできてしまいます。

そこで、さらにそのフォルダ内のファイルを暗号化しておく方法があります。暗号化しておけば、フォルダアクセスされてもデータをコピーされてもデータの中身を見ることはできません。このときに、暗号キーは設定キーを使用しないほうがいいでしょう。設定キーで暗号化していると、設定キーで復号化できてしまいます。

セキュアセブンでは復号時に設定キーを使用できないように環境設定することも可能です。環境設定の画面を開くためのパスワード設定も可能です。誰でも環境設定を変更することが出来ないようにパスワード設定することが重要です。もし、暗号時に設定キーを使用する場合は、復号時にキーを手入力されるように設定するほうが安全です。

# 参考資料

## セキュアセブンの暗号処理時間

(測定環境)

OS: Windows® Server 2003      CPU: Xeon® 3GHz      メモリ: 3GB

OS: Windows® Server 2008(64bit)      CPU: Celeron® 1.8GHz × 2CPU      メモリ: 2GB

OS: Windows® Server 2008(32bit)      CPU: Celeron® 1.8GHz × 2CPU      メモリ: 2GB

全て暗号時に圧縮も指定しています。

測定環境	サイズ	フォルダ数	ファイル数	圧縮暗号後のサイズ	圧縮率	処理時間
	32.40GB	12,800	164,619	13.60GB	58%	1時間51分16秒
	25.97GB	8,245	46,814	14.98GB	42%	1時間02分24秒
	24.16GB	7,910	46,250	13.84GB	43%	58分00秒

# 対応OS

以下のOSについて動作検証を行っております。

- ・Windows NT®4.0
- ・Windows® 2000
- ・Windows® Server 2003
- ・Windows® XP
- ・Windows® Server 2008

# 価格及び保守について

**【製品価格】 ￥157,500 (税込)**

**【年間保守料金】 ￥15,750 (税込)**

購入後1年間は無償保守期間です。無償保守期間終了の月に保守の更新手続きを行なうと、そのまま継続して保守サービスが受けられます。保守を一旦解約し再契約する場合、解約期間に応じて追加料金が発生する場合がございます。

## < 保守内容 >

- ・製品に関するQ / A対応  
メールやFAXにてセキュアセブンの仕様や利用方法などのご質問にお答えします。
- ・ライセンス証明書の再発効  
ライセンス証明書を紛失された場合に、再発効いたします。
- ・製品バージョンUP時のメディアの無料配布  
セキュアセブンの機能追加や対応OSの追加などのバージョンUP時に無料でメディアをお届けします。
- ・製品不具合時の修正プログラムの無料配布  
セキュアセブンのプログラムで不具合が見つかった場合、修正プログラムを無料でお届けします。