C4U　～ファイル暗号化アプリケーション～(2)

Focus Systems, Corp

C4U 機能

■ **自動暗号・復号**

あらかじめ指定したフォルダ内のファイル全て(サブフォルダを含む)を、C4Uキーの抜き挿しのタイミングで暗号／復号(暗号の解除)します。

■ **手動暗号・復号**

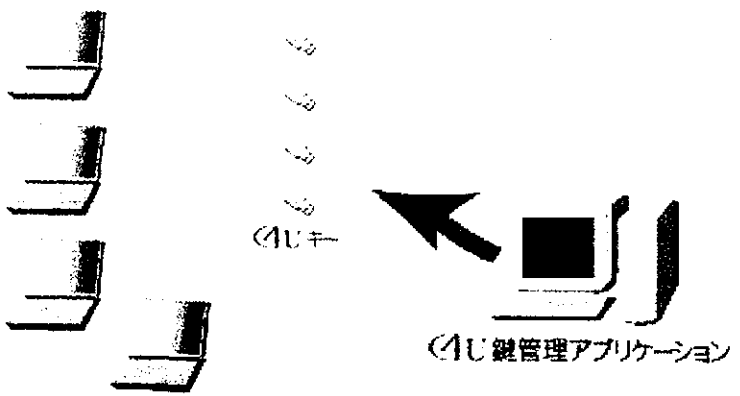
ファイルの右クリックメニューから「C4U暗号(C4U復号)」を選択することで、ファイルを個別に暗号(復号)します。複数ファイルも指定可能です。

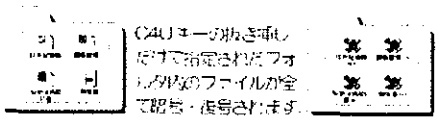
■ **C4Uログオン**

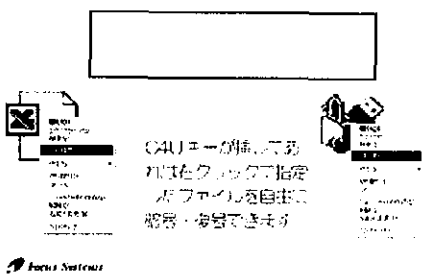
C4UキーにPCへのログオンIDとパスワードを登録すれば、PC起動時にC4Uキーを挿すだけで、Windowsにログオンすることができます。C4Uキーを抜くとログオフします。

■ **改ざんチェック**

暗号ファイルの復号時に、悪意の第三者によって不正に書き換えられていないかを自動的にチェックします。メールへの添付ファイルに対して利用することで、添付ファイルの正当性を検証することが可能です。





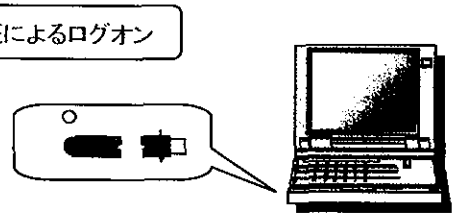


3-7 **C4-Fingered ～指紋認証+ファイル暗号化～**

Focus Systems,Corp

C4-Fingered

バイオメトリクスでも普及度・認知度の高い指紋認証とC4暗号を組合わせたセキュリティツールです。
USB端末接続型の小型デバイスで、持ち運びも簡単。PC利用者の本人認証およびデータの暗号化により、第三者によるPCの不正利用や盗難等による情報漏洩を防ぎ、大切なデータを守ります。



C4-Fingeredの優れた特徴

●指紋による本人認証

パスワードやIDを覚えることなく、また高認証率でストレスなく、指一本で簡単にPCへのログインが可能です。バイオメトリクスによる確実な本人認証で、PC盗難・パスワード漏洩やパスワードクラッキングツールを使用したPCの不正利用を防ぎます。

●小型デバイス

C4-Fingeredは小型デバイスで場所を取らず、持ち運びにも便利です。
USB端末に接続して使用するので、導入・取り付けも簡単です。

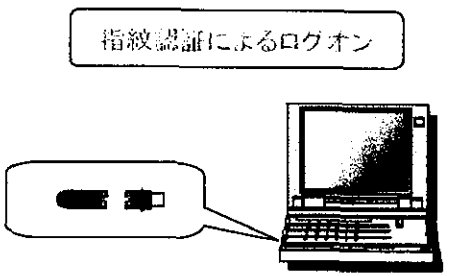
C4-Fingered　～指紋認証+ファイル暗号化～(2)

Focus Systems, Corp

機能

■ 指紋認証によるログオン

本人のみが持つ指紋で認証を行い、PCへのログオンを行います。パスワードを忘れることや、ICカード等の紛失・盗難の心配をすることなく、確実な本人認証で高いセキュリティを確保します。



■ 指紋認証によるスクリーンロック・スクリーンセーバーロック解除

スクリーンロックまたはスクリーンセーバーロック解除を指紋認証で行います。
ちょっとした離席の際も、第三者によるPCの不正利用を防ぎます。

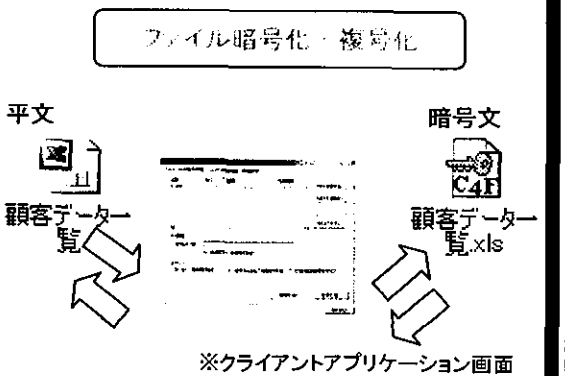
■ ファイルプロテクト

・フォルダやファイルの暗号化

簡単操作でデータを暗号化・復号化処理でき、重要な情報を守ります。

・暗号書庫

データを圧縮して暗号化し、異なるドライブのフォルダやファイルも同一書庫へ格納し管理できます。



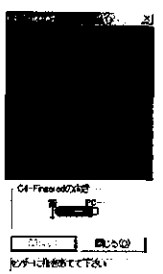
※クライアントアプリケーション画面

■ シュレッダー削除

復元ソフトを使用しても、データを二度と復元することができないように削除します。

■ 指紋認証による管理アプリケーション（C4-Fingered）の起動

C4-Fingeredの発行や設定変更を行う「管理アプリケーション」の起動には、管理者の指紋認証が必要になるため、管理者以外の人物にむやみに設定変更されることがなく、高いセキュリティレベルを維持できます。


※指紋認証画面

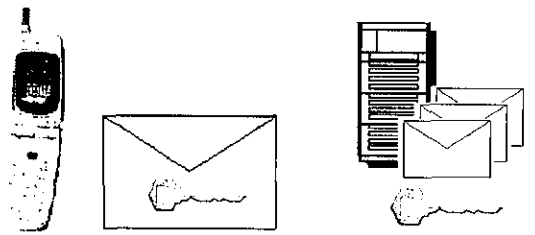
3-8

C4 i ～携帯電話メール暗号化ソリューション～

Focus Systems, Corp

C4i

NTTドコモのiアプリ対応の携帯電話にて動作可能な携帯暗号メールシステムです。携帯電話だけでなく、PCと携帯電話との暗号メール送受も実現しました。機密情報をやり取りするビジネスにおいても、携帯電話でのメールの送受信を安全なものにし、重要な情報を守ります。



C4iの優れた特徴

●暗号メール

事前に決めていた秘密の鍵で、手元で暗号化／復号化を行います。(鍵は毎回変更可能)

暗号メールの着信を通常のメールアドレスに通知する着信通知機能もあります。

●新世代の「カオス理論」応用の高速暗号技術「C4S」

データ秘匿には、暗号化処理**511Mbps**を誇る高速カオス暗号「C4S」を搭載しています。

エンジン自体が軽量であるため、C4iはiアプリでの実装を可能にしました。※約2.9kbyte

●サーバに保管されているメッセージも暗号化

データがサーバに暗号化されて保管されているため、ハッキングされた場合でもデータを安全に守ります。携帯電話紛失の際も、データ流出の心配はありません。

Focus Systems
Bring Computer Solutions into Focus

C4S、C4Kに関するお問い合わせ

株式会社フォーカスシステムズ

新規事業推進室：C4担当

E-Mail　prom@focus-s.com

〒141-0022　東京都品川区東五反田1-23-1

フォーカス五反田第２ビル

TEL 03-5420-3659　FAX 03-5420-3634

URL　http://www.focus-s.com

開発元：株式会社シーフォーテクノロジー

（フォーカスシステムズグループ）

＿＿＿＿＿＿＿＿＿＿＿＿殿

C4暗号理論及び強度評価について

平成16年　7月

株式会社フォーカスシステムズ
新規事業推進室

現代暗号技術の区分（共通鍵暗号と公開鍵暗号）

- 共通鍵暗号と公開鍵暗号の比較

	共通鍵暗号	公開鍵暗号
鍵の関係	暗号鍵＝復号鍵	暗号鍵≠復号鍵
利点	処理速度が速い	鍵の管理が容易 デジタル署名が可能
欠点	鍵の管理が困難 （暗号化の鍵の機密を守りつつ配布するのが困難）	処理速度が遅い （大容量の暗号処理にはパフォーマンスの面で不向き）
利用方法	文書などのデータ量が大きいものを暗号化	暗号化に使う鍵の暗号化 デジタル署名の利用

※　共通鍵と公開鍵の利点と欠点はちょうど反対の関係になる。

特に速度の問題は、コンピュータで暗号処理を行なうとき処理内容が、共通鍵方式ではビット演算などのハードウェアが得意な命令の組み合わせ、公開鍵方式では算術的に複雑な命令の組み合わせが多いという傾向のためにおこる。

また両者の用途を比べると、公開鍵はその仕組みを利用した認証系のセキュリティ（PKI）に用いられ、共通鍵は情報秘匿のセキュリティに用いられるという役割傾向にある。

共通鍵暗号の区分(ブロック型とストリーム型)

- ブロック暗号とストリーム暗号の比較

	ブロック暗号	ストリーム暗号
処理単位	平文の複数ビット(数十ビット以上)を1ブロックとして、その単位に暗号処理を施す	平文を1ビットまたは数ビット単位で暗号処理を施す。
暗号基本構造	鍵スケジュールとデータランダム化の処理構成でデータ攪拌をおこなう。	ビットデータに擬似乱数を付加してデータの攪拌を行なう。
安全度のポイント	データランダム化の処理回数 転換、置換ロジックの複雑さ (非線形の処理構造を持つ)	使用する擬似乱数が暗号学的に安全であること(データバランス、乱数同士の無相関性など)
特　徴	①計算量が多いためにストリーム系に比べての処理系が重い傾向 ②暗号強度は鍵長／ブロック長／計算量の増強で比較的に簡単に向上が可能	①暗号に使用する擬似乱数の生成が難しい。 ②ブロック型に比べ処理系が軽い傾向

現代暗号技術で顕在化している問題点

現代暗号ではこのような問題が顕在化しています。

1　強度性

これまで一般的に使用されていたDESは、1999年には約22時間で解読されました。また、鍵長1024bitのRSAは2010年ごろには解読されるだろうと言われています。

2　処理速度

一般に、暗号化に用いる鍵が長いほど安全です。ところが、最近の暗号でさえも高々128bit、256bitの鍵長しか用いていないのは、一般に鍵長が長くなるほど暗号化（復号）処理にあたえます。

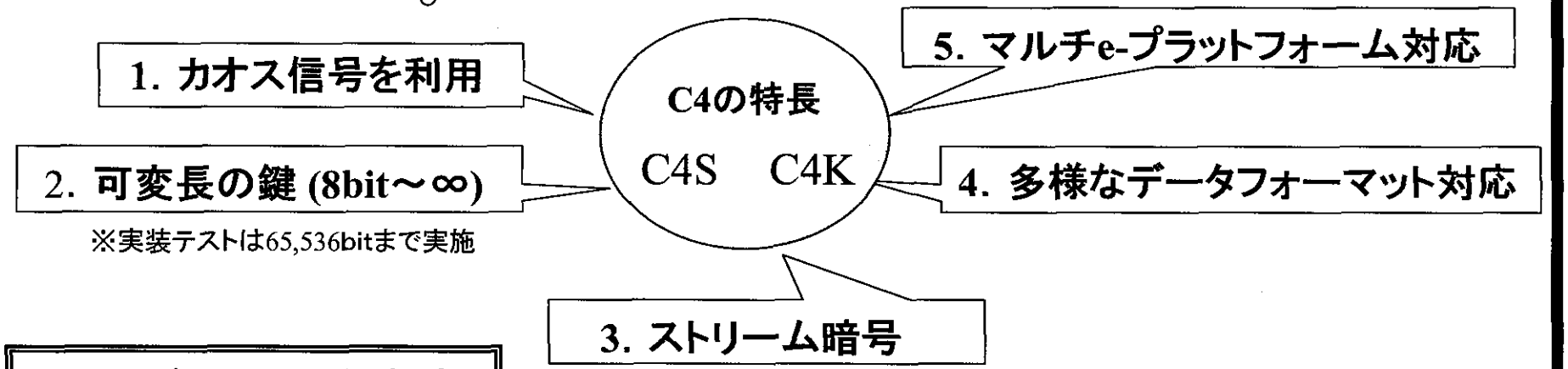
3　使用機種（OS）が限定される

これまでの暗号処理は、限られた計算機での処理が中心でしたので、様々なプラットフォームでの相互換性の対応は低いものでした。しかしクロスプラットフォームでのセキュリティニーズが増すなかでのマルチプラットフォーム化は少ないものでした。

C4シリーズ

Focus Systems, Corp

C4暗号5つの特徴



暗号モジュール評価対応

独立行政法人情報処理推進機構（IPA）では、国際標準化の流れを視野に入れて、国内における暗号モジュール評価制度の整備が進められています。
暗号アルゴリズムだけでなく、暗号技術の実装レベルでの安全性が問われ、暗号モジュール評価の必要性が高まってきています。

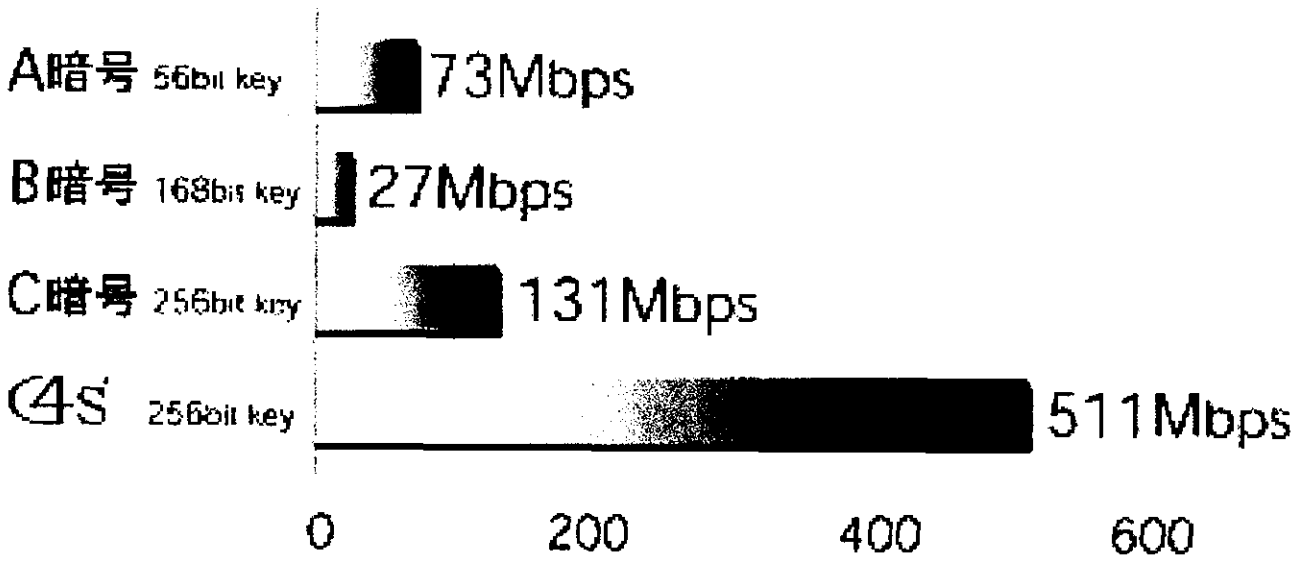
C4製品（C4CS※1）も、米国（NIST）とカナダ（CSE）が行う暗号モジュール評価プログラム（CMVP）において、評価テストを受けている段階にあり、**9月頃には認定される予定**となっております。

※1　C4CS　：　C4Custom暗号エンジンに加え、NIST(*1)が規定したAESなど複数のアルゴリズムを含む製品で、様々なセキュリティニーズへの柔軟な対応が可能となります。

C4Sの速度 － (1)

Focus Systems,Corp

暗号化処理スピードグラフ



Pentium® III 733MHz Windows2000 Professional **当社調べ**
（測定環境により、測定結果が異なる場合がございます）

＜快適さを誇るスピード＞

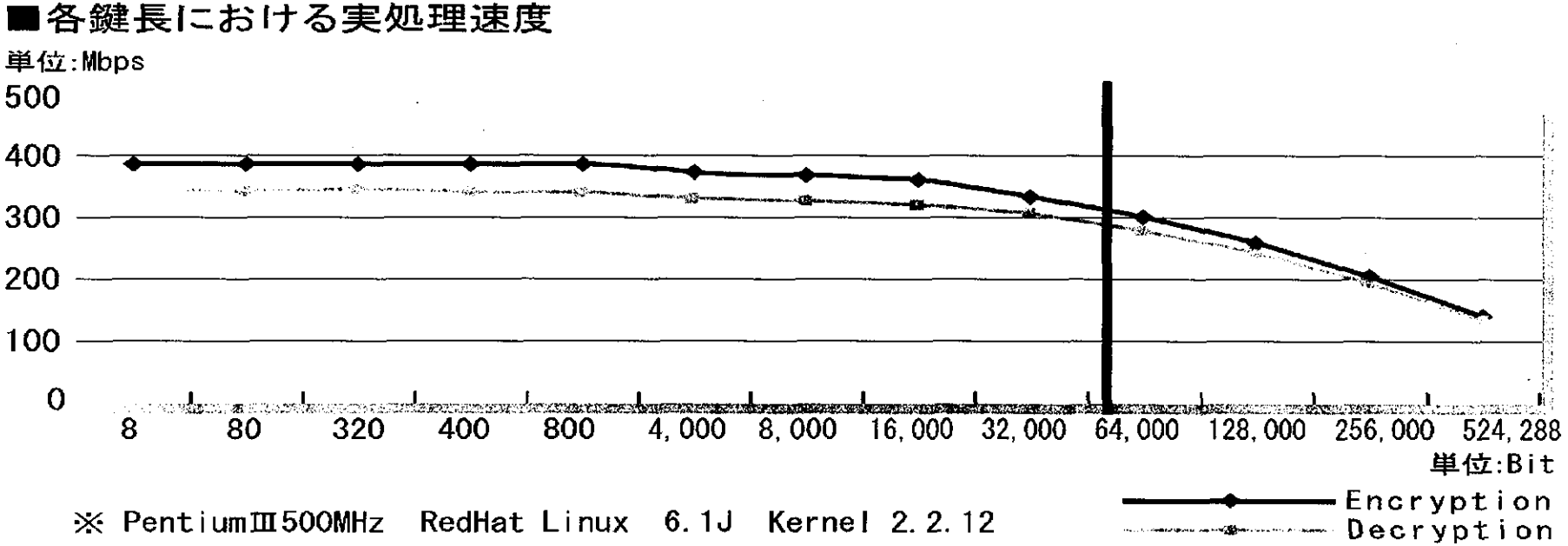
PentiumⅢ 733MHz Key 256bitの環境下で、511Mbpsの処理速度を実現。

次世代標準暗号として利用が広まっている「AES」の約4倍の処理スピードを誇ります。

C4Sの速度 - (2)

Focus Systems, Corp

■各鍵長における実処理速度



※ PentiumⅢ500MHz　RedHat Linux　6.1J　Kernel 2.2.12

＜セキュリティバランス＞

安全性を高める長い鍵、ストレスを感じることのない高速な処理。

その両方を実現させ、強度・速度ともに優れたブロードバンド時代に

最適な暗号化を可能にしました。

ストリーム暗号技術「C4」の特徴

- C4暗号の特徴

（1）カオスの性質を利用した安全な擬似乱数

暗号鍵要素を初期値として複雑なカオス系列を出力して擬似乱数を生成

（2）擬似乱数生成器とストリーム暗号の構造の特徴で実現した処理の高速性

①擬似乱数の要素となるカオス信号は、シンプルな非線形関数から生成。

②非常に軽微なストリーム暗号処理構造を利用

（3）多種プラットフォームでの実装性の高さを実現

ストリーム暗号技術の安全性

●擬似乱数の安全性が暗号強度●

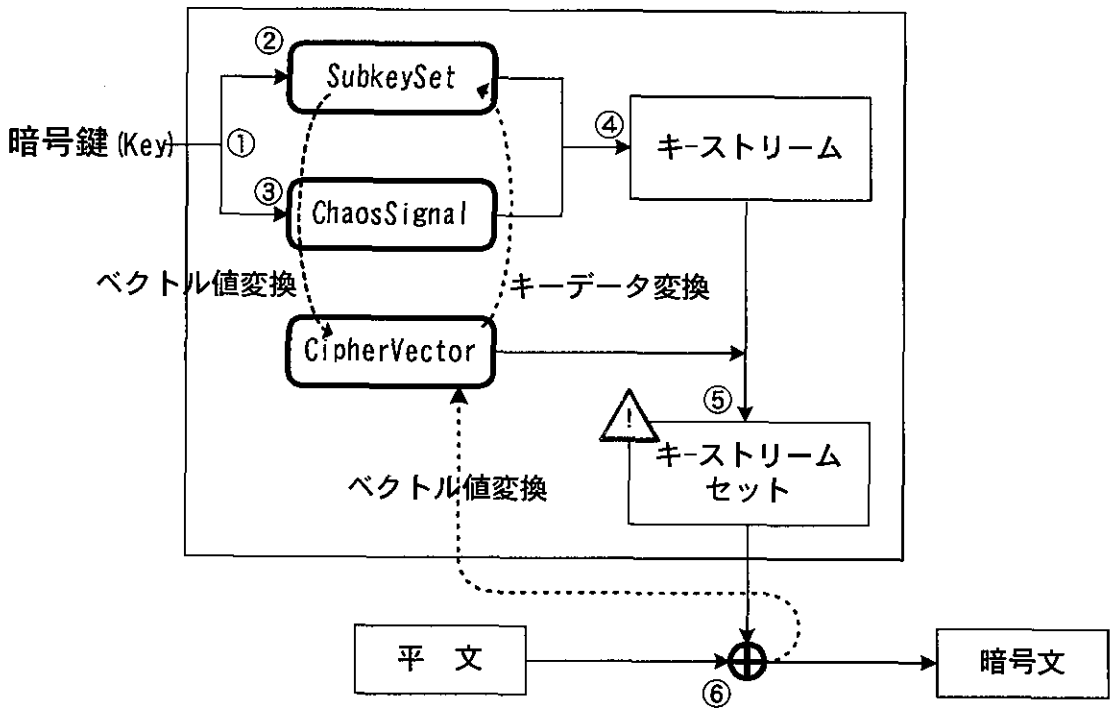
ストリーム暗号において暗号学的に安全な乱数が生成されるとその暗号系は安全であるとされる。

暗号学的に安全な乱数の条件

(1)0,1の等頻度性(バランス性)
出力される乱数列の総ビット0,1の配分が等頻度であること(統計的性質が現れない)
(2)長周期性
乱数列として生成する数列の(1)、(3)、(4)の条件が長い周期で継続
(3)無相関性
乱数列の個々の数値が他の数値に依存していないこと。乱数発生のための入力と出力データの間に相関が無いことなど
(4)非線形性
暗号器の出力が線形フィードバックシフトレジスタ(LFSR)の出力そのものではない。

これを必要条件として満たす擬似乱数で暗号化を実現

C4S暗号処理構造



★ 入力された暗号鍵を初期値として「非線形デジタルカオス信号」を発生

★「非線形デジタルカオス信号」と暗号鍵から、キーストリームを合成

★ キーストリームを暗号ベクトルで置換していく擬似乱数生成器（キーストリームセット構造）　で平文を暗号化

✧ 鍵要素、カオス信号、内部暗号ベクトルの有機的な合成により、より強固な仕組みとなっています。

キーストリームセットの各機能の役割

- SubkeySet:
  鍵変換処理でベクトル値を反映した変換鍵データを入力

- ChaosSignal:
  暗号鍵から複数のデジタルカオス信号を生成、その上でそのカオス信号群を合成したひとつのデータ列を発生

- CipherVector:
  鍵変換処理、キーストリーム攪拌、置換など、C4暗号で発生する様々なデータ列に対して影響を及ぼし、また逆に影響を及ぼされながら変化していく参照データ値

安全性の担保としてのカオスの性質

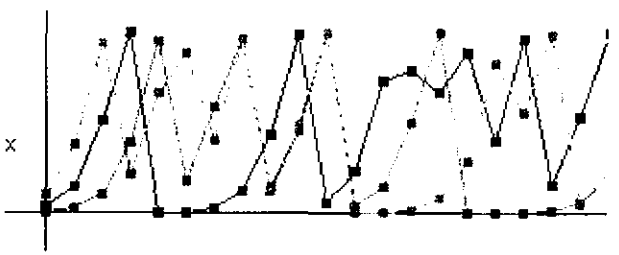
■デジタルカオス信号を要素とした擬似乱数生成■

カオス的性質と呼ばれるカオス関数の下記の性質を利用して、非常に高い擬似乱数性の条件を満たします。

①初期条件に敏感な依存

②一方向性

③複雑な線形（軌道）を描く



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

暗号学的に安全な乱数の必要条件を満たす

0,1の等頻度性／長周期性／無相関性／非線形性

擬似乱数生成器についての強度評価

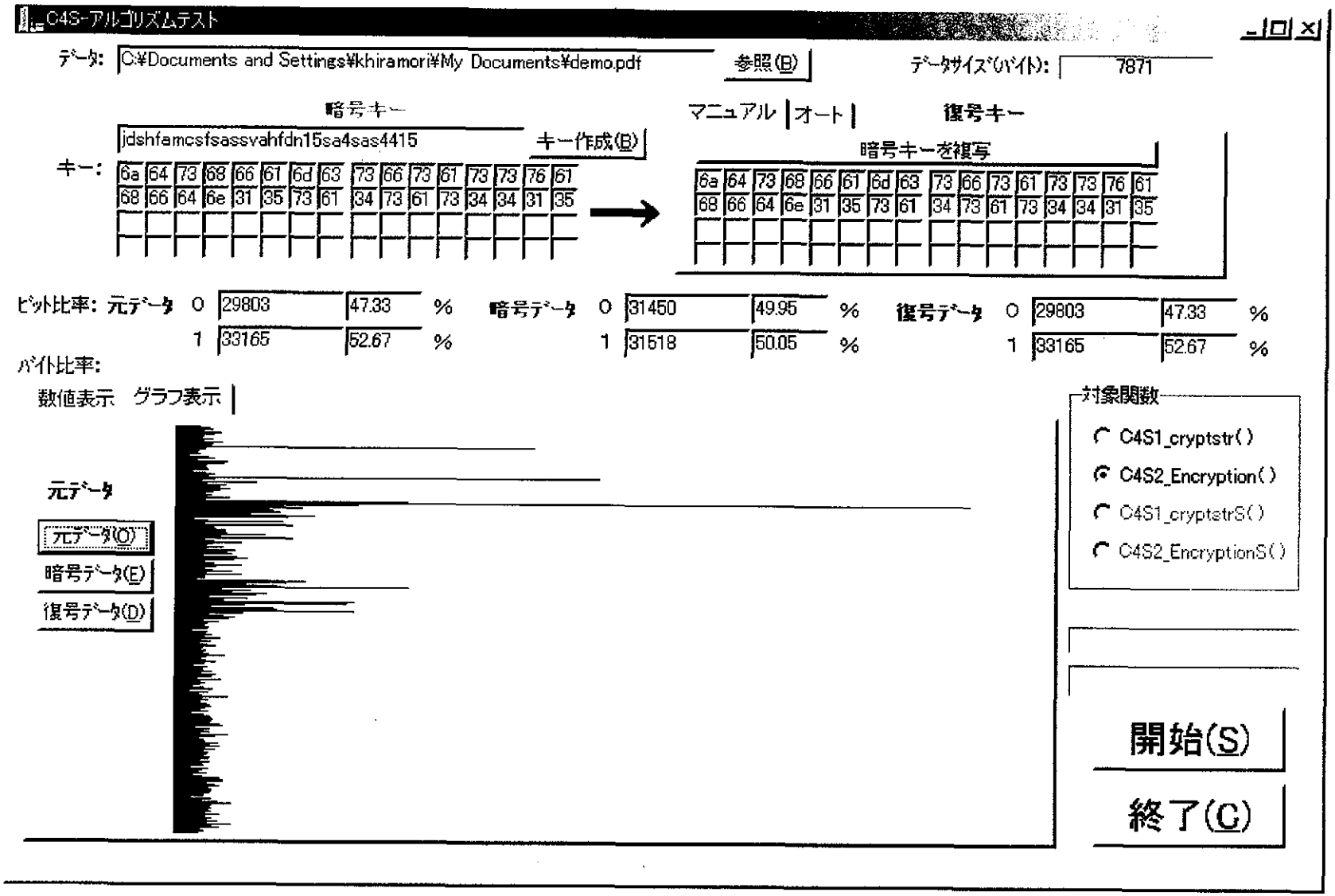
- 擬似乱数を用いたストリーム暗号の強度は、擬似乱数自身の安全性が最大のポイントです。その擬似乱数の強度を評価するのに用いられることの多い基準は以下の2つがあります。

- （1）FIPS　PUB140-1（最新は140-2、乱数評価部分は変わらず）
  ①モノビットテスト・・・擬似乱数データの全体としての01比率
  ②ポーカーテスト・・・4ビットで区切ったデータでの16進表示の出現回数の比率の乖離性
  ③ランテスト・・・0または1が連続する場合の連続回数のカウント
  ④ロングランテスト・・・0または1が26個以上続く場合の出現カウント

- （2）NIST　SP800-22
  評価項目は全16項目

上記は、ともに米国（NIST）が規定している指標で、暗号技術調達の要件としての必要条件を記しているものです。

参考資料1 ： 01分布(平文)



参考資料2 ： 01分布(暗号文)