3-3 C4Custom ～暗号化機能コンポーネント～

Focus Systems,Corp

C4Custom C4Custom

マルチプラットフォームをコンセプトに、安全性とスピードを高度に両立させたC4S暗号。そんなC4S暗号をベースにし、各プラットフォームに合わせてパフォーマンスを最適化し、より処理速度を上げることができました。

C4Customの優れた特徴

●共通鍵暗号モジュールの新シリーズ

C4Sをベースに、プログラムレベルの改良(CPU固有の命令セットの利用やメモリアクセスの最適化等)を行い、各プラットフォームごとに最適化しています。

●C4S比で2倍以上の暗号化速度を実現

C4Sの強みであった高速性な暗号処理を一層高め、Java環境においてはC4Sと比べ2倍強と、さらなる高速化を実現しました。

●C4Sの特徴を継承

C4Sと理論が同じであるため、共通鍵暗号方式、ストリーム暗号方式、暗号鍵が可変長等、C4Sの特徴を継承しています。※ただし、プログラムの大幅な変更により、C4Sとの互換性はありません。

3-4 C4VPN ～高速暗号通信ソリューション ～ (1)

Focus Systems,Corp

C4VPN C4VPN

インターネットを介した企業間通信、企業内部の特定部署等との通信のセキュリティを実現します。

C4VPNの優れた特徴

●IP通信の業界標準セキュリティ規格の採用

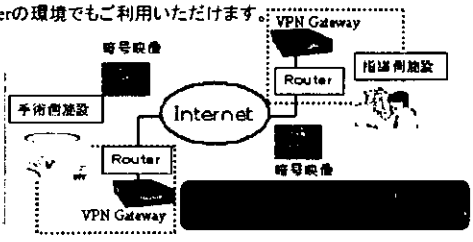
TCP/IP通信にセキュリティを実装するためのIPsec規格に準拠しています。

●ファイアウォール機能・・・パケットフィルタリング機能のファイアウォールを標準搭載。

●無線・有線イーサネット対応・・・無線LAN(802.11a、11b、11g)や、FastEther/ギガビットEtherの環境でもご利用いただけます。

＜遠隔医療共同研究で採用＞

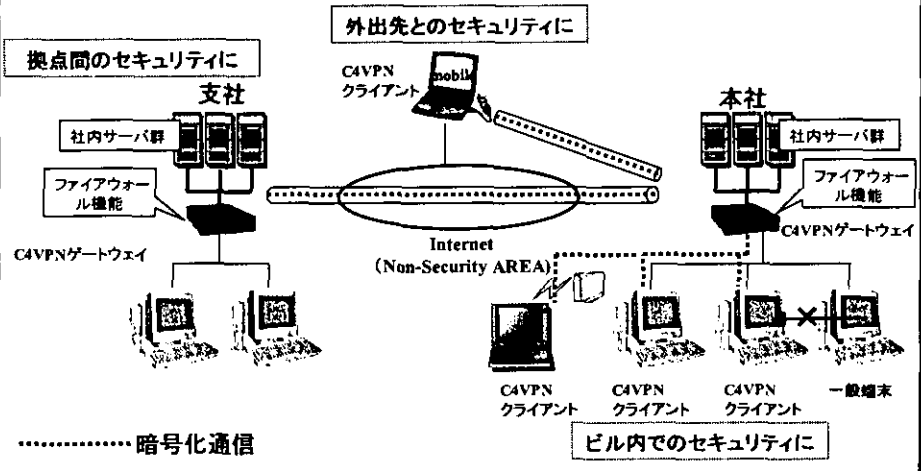
指導医側病院(慶應義塾大学病院)と手術側病院(東京医療センター)とをインターネット回線でつなぎデータをやり取りする遠隔医療研究において、セキュリティ確保の為にC4VPNを利用しています。



C4VPN　～高速暗号通信ソリューション～ (2)

Focus Systems,Corp

C4VPN　C4VPNのセキュリティ構成図



3-5

C⁴ FILE PROTECTOR

～情報漏洩対策ソリューション～ (1)

Focus Systems,Corp

C⁴ FILE PROTECTOR

企業のPC内のデータは重要な情報であふれています。そんな大切な資産をぞんざいに扱っていませんか？予期せぬ紛失、盗難であなたの大切な情報が他者に漏洩することを防ぎます。

C⁴ FILE PROTECTORの優れた特徴

●簡単なファイル操作でも高いセキュリティ対策

エクスプローラから、クリックメニューから、ユーティリティからと、ユーザー操作の選択肢の豊富さや、シャットダウンの際に暗号化操作を忘れないための自動暗号化など、ユーザーフレンドリーな機能が満載です。

●暗号化に加え、情報漏洩・保護対策機能の充実

ファイルの完全削除、ファイルのセキュリティバックアップなど、ユーティリティツールとしての高い情報メインテナンスを実現しています。

C⁴ FILE PROTECTOR

～情報漏洩対策ソリューション～(2)

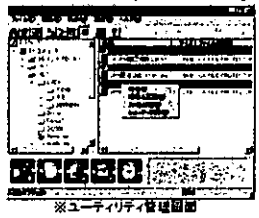
Focus Systems, Corp

機能

■ ファイル暗号
簡易操作でPC内のファイルやフォルダを暗号化

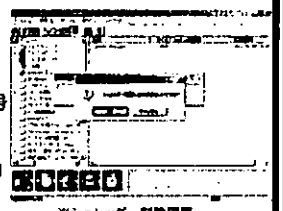
★右クリックで暗号 → ユーティリティ、エクスプローラ、デスクトップなどで、直接ファイルを右クリックしての簡単な 暗号、復号を実現します。

★直感的な操作イメージ → アイコンへのドラッグ＆ドロップでも各種機能が実行されます。


※ユーティリティ管理画面

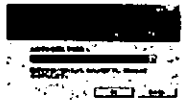
■ ファイル分割暗号
大きなファイルを一定の指定サイズまたはメディアの容量に合わせて分割暗号

■ 暗号圧縮
複数のファイルやフォルダをまとめて圧縮して暗号化し、同一暗号書庫に格納


※シュレッダー削除画面

■ シュレッダー削除
データを二度と復元できない形にして削除

■ セキュアシャットダウン
シャットダウンとともに設定ファイル・フォルダを自動暗号化処理


セキュアシャットダウン画面

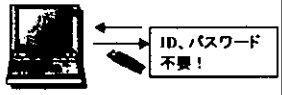
3-6 C4U ～ファイル暗号化アプリケーション～(1)

Focus Systems, Corp

C4U

企業内PCの重要なデータを情報漏洩から守るため、暗号化処理はしたい。しかし、「パソコン初心者で扱い方が分からない」、「IDやパスワードの入力を手間だと感じる」、または「忘れてしまう」、そういった方でも簡単な操作でファイル暗号化ができるファイル暗号化アプリケーションです。

C4Uの優れた特徴



●簡易操作

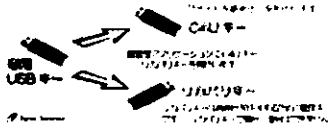
初回の暗号化フォルダ設定以後は、C4Uキー(USBキー)の抜き差しのみの操作です。

キーを抜いた状態が暗号化、キーの挿入で復号化と、わずらわしいIDやパスワードなどが不要です。

●耐タンパ性

C4Uキーは耐タンパ性を備えた制御チップを搭載しており、不正にキー情報を読み取ろうとすると、中の情報が壊れ、読み取れないようになっています。

また、キーの再発行には複数個のリカバリーキーを揃えてはじめて可能となる新しいシステムを搭載しています。



C4U ～ファイル暗号化アプリケーション～(2)

Focus Systems,Corp

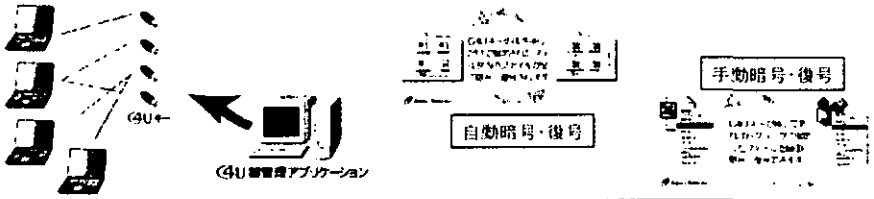
C4U 機能

■ **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。

■ **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。

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

＿＿＿＿＿＿＿＿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 <u>強度性</u>

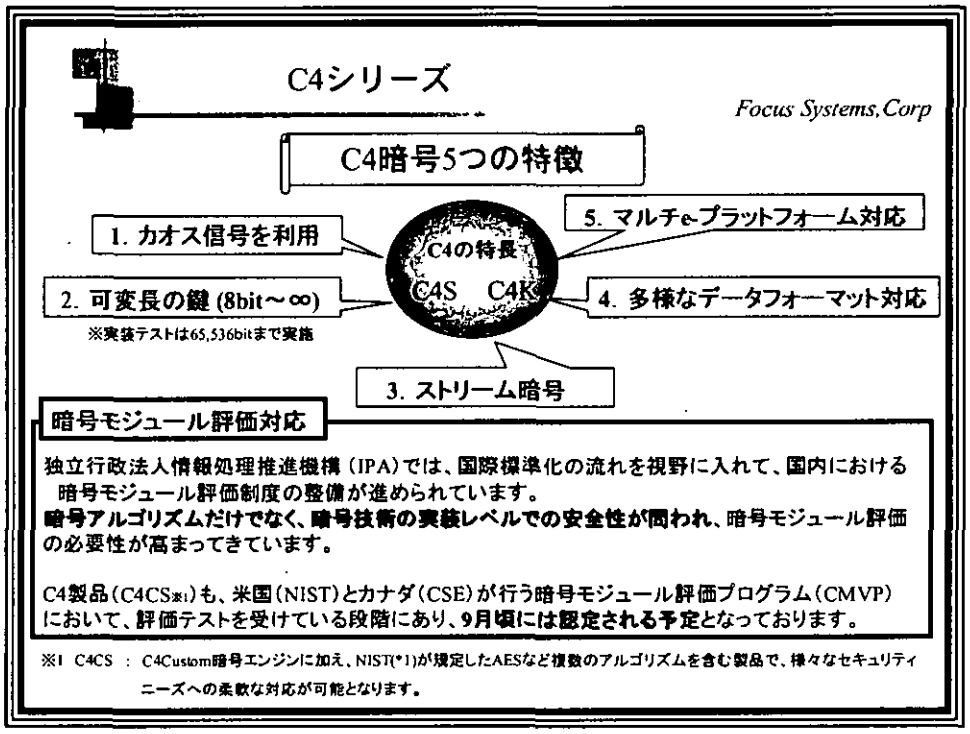
これまで一般的に使用されていたDESは、1999年には約22時間で解読されました。また、鍵長1024bitのRSAは2010年ごろには解読されるだろうと言われています。

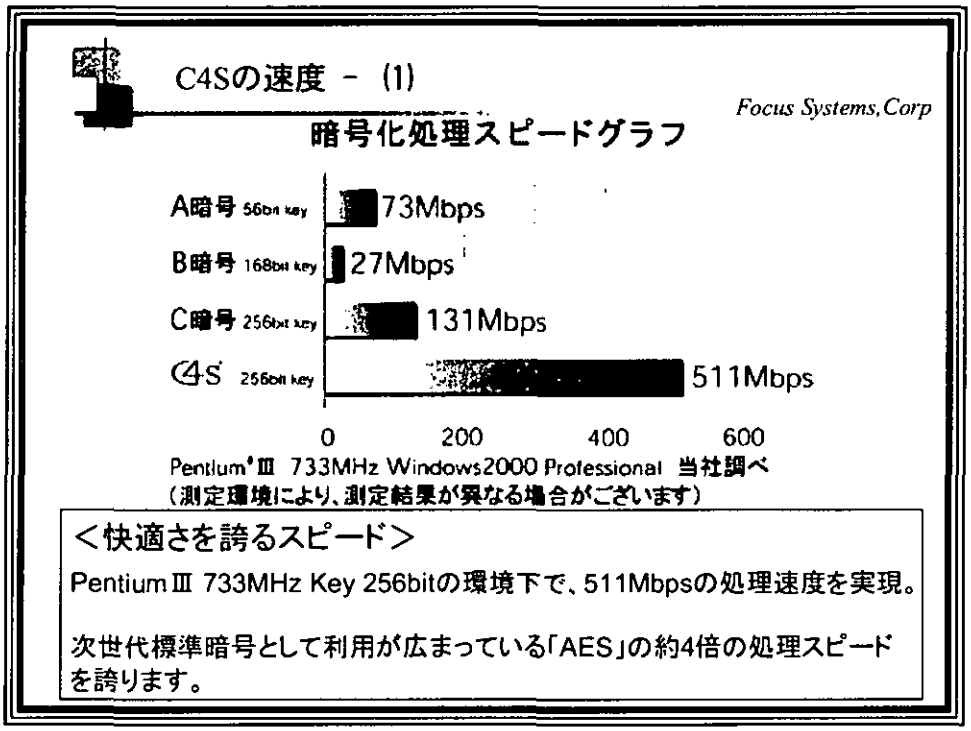
2 <u>処理速度</u>

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 <u>使用機種(OS)が限定される</u>

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。

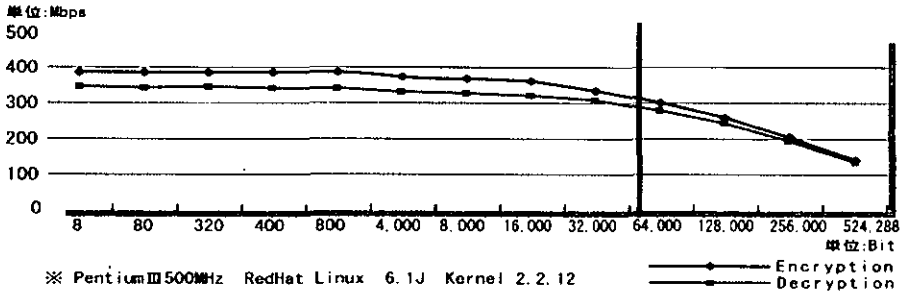

C4シリーズ
Focus Systems,Corp
C4暗号5つの特徴
1. カオス信号を利用
2. 可変長の鍵 (8bit～∞)
※実装テストは65,536bitまで実施
C4の特長
C4S C4K
5. マルチe-プラットフォーム対応
4. 多様なデータフォーマット対応
3. ストリーム暗号
暗号モジュール評価対応
独立行政法人情報処理推進機構（IPA）では、国際標準化の流れを視野に入れて、国内における暗号モジュール評価制度の整備が進められています。
暗号アルゴリズムだけでなく、暗号技術の実装レベルでの安全性が問われ、暗号モジュール評価の必要性が高まってきています。
C4製品（C4CS※1）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
A暗号 56bit key
73Mbps
B暗号 168bit key
27Mbps
C暗号 256bit key
131Mbps
C4S 256bit key
511Mbps
0
200
400
600
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＞
Pentium III 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●

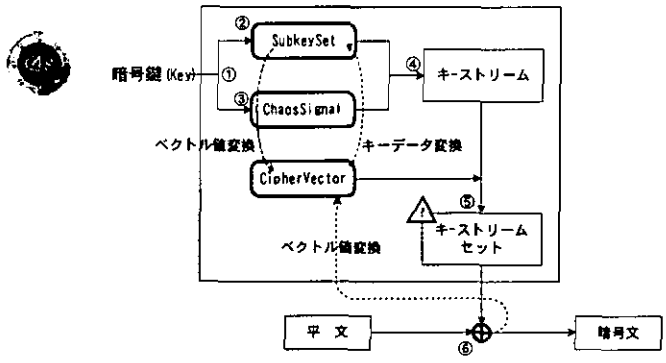
ストリーム暗号において暗号学的に安全な乱数が生成されるとその暗号系は安全であるとされる。

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

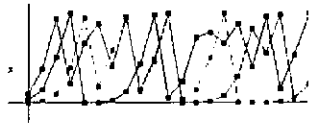
- SubkeySet:
  鍵変換処理でベクトル値を反映した変換鍵データを入力
- ChaosSignal:
  暗号鍵から複数のデジタルカオス信号を生成、その上でそのカオス信号群を合成したひとつのデータ列を発生
- CipherVector:
  鍵変換処理、キーストリーム攪拌、置換など、C4暗号で発生する様々なデータ列に対して影響を及ぼし、また逆に影響を及ぼされながら変化していく参照データ値

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

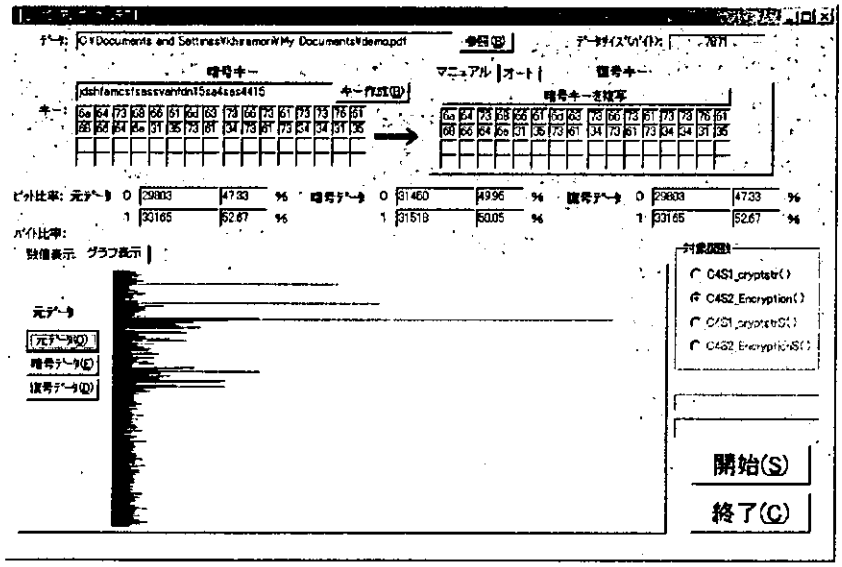
- 擬似乱数を用いたストリーム暗号の強度は、擬似乱数自身の安全性が最大のポイントです。その擬似乱数の強度を評価するのに用いられることの多い基準は以下の2つがあります。

- （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

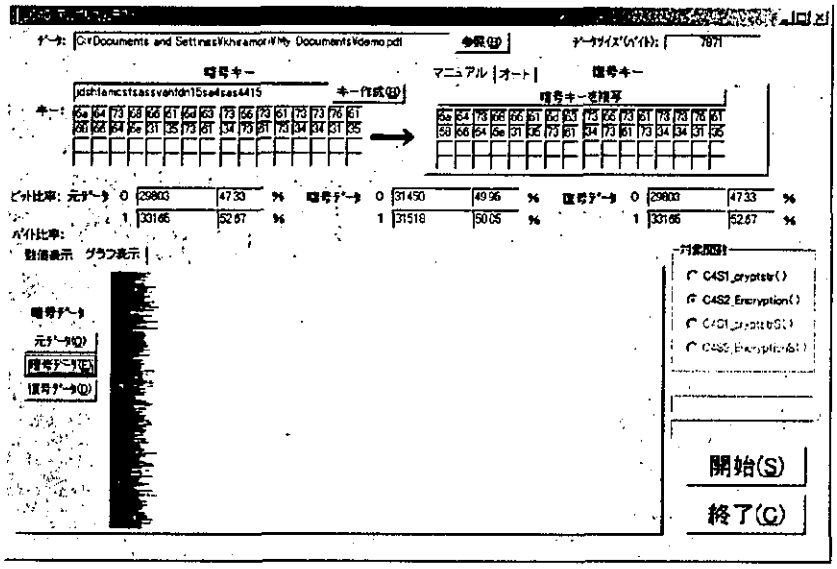
- （2）NIST SP800-22
  - 評価項目は全16項目

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)



参考資料3 ： FIPSテスト結果

FIPS PUB 140-1

①試験暗号データ量 10Mbyte

②ランダム抽出したnビット番目から固定長「20000bit」の範囲でのデータ分布に関する試験

FIPS PUB 140-1 test #1

//1-20,000bit

The monobit test	X=	9,916	pass	(pass if 9,654 <X <10,346)
The poker test	X=	26.304	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2,436	2,477	pass	(pass if 2,267 <X <2,733)
2	1,263	1,250	pass	(pass if 1,079 <X <1,421)
3	655	659	pass	(pass if 502 <X <748)
4	315	315	pass	(pass if 223 <X <402)
5	154	124	pass	(pass if 90 <X <223)
6+	159	156	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

FIPS PUB 140-1 test #2

//20,000,001-20,020,000bit

The monobit test	X=	10,053	pass	(pass if 9,654 <X <10,346)
The poker test	X=	6.2016	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2,467	2,469	pass	(pass if 2,267 <X <2,733)
2	1,248	1,251	pass	(pass if 1,079 <X <1,421)
3	659	641	pass	(pass if 502 <X <748)
4	329	317	pass	(pass if 223 <X <402)
5	155	162	pass	(pass if 90 <X <223)
6+	131	150	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

FIPS PUB 140-1 test #3

//40,000,001-40,020,000bit

The monobit test	X=	10,118	pass	(pass if 9,654 <X <10,346)
The poker test	X=	9.7984	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2,531	2,487	pass	(pass if 2,267 <X <2,733)
2	1,268	1,253	pass	(pass if 1,079 <X <1,421)
3	613	614	pass	(pass if 502 <X <748)
4	320	348	pass	(pass if 223 <X <402)
5	155	153	pass	(pass if 90 <X <223)
6+	134	165	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

FIPS PUB 140-1 test #4

//60,000,001-60,020,000bit

The monobit test	X=	10,079	pass	(pass if 9,654 <X <10,346)
The poker test	X=	9.2032	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2,495	2,536	pass	(pass if 2,267 <X <2,733)
2	1,300	1,243	pass	(pass if 1,079 <X <1,421)
3	636	608	pass	(pass if 502 <X <748)
4	306	309	pass	(pass if 223 <X <402)
5	157	164	pass	(pass if 90 <X <223)
6+	130	164	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

FIPS PUB 140-1 test #5

//79,980,001-80,000,000bit

The monobit test	X=	9,968	pass	(pass if 9,654 <X <10,346)
The poker test	X=	13.9648	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2,577	2,520	pass	(pass if 2,267 <X <2,733)
2	1,225	1,306	pass	(pass if 1,079 <X <1,421)
3	604	618	pass	(pass if 502 <X <748)
4	323	306	pass	(pass if 223 <X <402)
5	144	144	pass	(pass if 90 <X <223)
6+	171	150	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

参考資料:

eToken R2 のタンパー機能について

(株)アラジンジャパン

1. はじめに

eToken R2

eToken R2 は、内部のメモリに構成した秘密領域を極めて堅牢に保護し、悪意あるアタックや解析から強固にプロテクトするセキュリティ・デバイスです。

eToken が備えているこの機能のように、ある領域に格納した秘密情報（たとえばアプリケーションで使用する暗号キー、PKI における秘密鍵など、機密を要するデータ）をプロテクトする機能をタンパー機能と言います。本資料では、eToken R2 がこのクラスで最高のタンパー機能をどのように実現しているかについて、いくつかの観点からその概要を説明します。

2. タンパー性に関係するハードウェアの基本機能

2.1 内臓暗号処理機能

eToken R2 は、DES-X（120bit キー）対称アルゴリズムを搭載しています。この機能は、eToken R2 内部で、すべての秘密データの暗号化、およびユーザ認証プロトコルにおけるチャレンジレスポンスの仕組みに使用しています。またこの機能は、PC 上の情報を保護するための暗号化/復号化エンジンとしても使用することができます。

2.2 RNG ベースのチャレンジレスポンス機能

eToken R2 はランダム・シードをベースにした擬似乱数発生機構を内臓しています。これと上の DES-X 機能により、ログイン制御を行います。つまりパスワードを検証するときは、eToken R2 内でランダムなチャレンジ値を発生させ、PC に送ります。レスポンス値は格納しているパスワードと比較されます。これにより、eToken は二因子認証による確実なユーザ認証を行います。

3. 秘密情報に対するプロテクション

eToken R2 のタンパー性は上のハードウェア基本機能をベースにしていますが、以下に主要な観点からどのように秘密領域をプロテクトしているかを説明します。

3.1 チップに対するプロテクション

eToken R2 は、物理的にはセキュア化されたマイクロコントローラと EEPROM で構成されています。EEPROM にはすべてのデータが格納されますが、ユーザ・データや暗号鍵など、秘密領域の内容はマイクロコントローラに格納されたキーにより、DES-X で暗号化されて EEPROM に格納されます。これらのキー(120bit 長)は、如何なる方法によっても、読み出したりアクセスしたりすることはできません。

3.2 USB データ・トラフィックに対するプロテクション

eToken R2 へのログインが成功することによってのみ、秘密領域へのアクセスが可能になることに加え、そのデータのトラフィックは常に暗号化されます。トラフィックの暗号化はログイン時に乱数発生機構で生成される 120bit 長のセッションキーを使用して DES-X アルゴリズムで行われます。

したがって、USB 信号ラインをスニッファー装置で解析しようとしても、またハウジングをはずしメモリからUSB に至る回路上を同様の装置で解析しようとしてもできません。

3.3 アクセスに対するプロテクション

eToken R2 内の秘密データの書き込みと使用は、eToken へログインすることによりのみ、可能になります。ログインは、きわめて高度なセキュリティレベルが確保できるチャレンジレスポンス方式によってのみ可能であり、加えてチャレンジ値は上記のように乱数発生機構により発生させています。このように、レスポンス値は毎回ランダムに変化することに加え、DES-X で暗号化していますので、ハウジングを破壊して開けてもパスワードが判明することはありません。

3.4 制御に対するプロテクション

eToken R2 のマイクロコントローラで使用するファームウェアは、アクセスしたり取り出したりすることができません。このため、ハウジングを破壊して開け、直接マイクロコントローラ・チップになんらかの機器を接続して解析し、悪意あるものに書き換えて動作そのものを変えようとしても不可能です。

3.5 タンパー・エビデント

タンパー・エビデントとは、"改ざんした、あるいは改ざんを試みた痕跡が物理的に残る作りになっていること" を指します。悪意から未然に防ぐ意味で、セキュリティ・デバイスでは重要な要求事項の一つになっています。

eToken R2 は、改ざんや解析のため内部にアクセスするには、ハウジングを破壊しない限り行うことができず、また一旦破壊すると復元することはできません。 なおプラスチック製のハウジングにはガラス繊維が混入されており、頑丈なだけでなく痕跡を残させることにも役立っております。

さらには、このような構造なのでタンパー性に加え、IP X8-IEC 529 の防水規格をも満たしており、持ち歩くことによる水との接触の可能性に対しても考慮が払われております。

FPS PUB 140-1 Test Result Details

Results of FIPS 140-1 Specified Tests on sample3

data: c4s(1Mbyte)

//1-20000

The monobit test	X=	10105	pass	(pass if 9654 <X <10346)
The poker test	X=	18.0224	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2539	2479	pass	(pass if 2267 <X <2733)
2	1246	1249	pass	(pass if 1079 <X <1421)
3	625	639	pass	(pass if 502 <X <748)
4	302	316	pass	(pass if 223 <X <402)
5	154	166	pass	(pass if 90 <X <223)
6+	144	160	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//1000001-1020000

The monobit test	X=	9914	pass	(pass if 9654 <X <10346)
The poker test	X=	11.0336	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2417	2483	pass	(pass if 2267 <X <2733)
2	1285	1277	pass	(pass if 1079 <X <1421)
3	657	616	pass	(pass if 502 <X <748)
4	304	313	pass	(pass if 223 <X <402)
5	181	145	pass	(pass if 90 <X <223)
6+	159	150	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//2000001-2020000

The monobit test	X=	9938	pass	(pass if 9654 <X <10346)
The poker test	X=	10.752	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2518	2480	pass	(pass if 2267 <X <2733)
2	1232	1314	pass	(pass if 1079 <X <1421)
3	630	612	pass	(pass if 502 <X <748)
4	311	300	pass	(pass if 223 <X <402)
5	156	165	pass	(pass if 90 <X <223)
6+	166	142	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//3000001-3020000

The monobit test	X=	9946	pass	(pass if 9654 <X <10346)
The poker test	X=	14.4192	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2479	2492	pass	(pass if 2267 <X <2733)
2	1208	1246	pass	(pass if 1079 <X <1421)
3	628	606	pass	(pass if 502 <X <748)
4	307	303	pass	(pass if 223 <X <402)
5	169	150	pass	(pass if 90 <X <223)
6+	170	165	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//4000001-4020000

The monobit test	X=	9991	pass	(pass if 9654 <X <10346)
The poker test	X=	17.7728	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2476	2467	pass	(pass if 2267 <X <2733)
2	1235	1249	pass	(pass if 1079 <X <1421)
3	604	600	pass	(pass if 502 <X <748)
4	316	309	pass	(pass if 223 <X <402)
5	150	164	pass	(pass if 90 <X <223)
6+	173	166	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

FIPS PUB 140-1 Test Result Details

Results of FIPS 140-1 Specified Tests on sample1

data: c4s(1Mbyte)

//1-20000

The monobit test	X=	9973	pass	(pass if 9654 <X <10346)
The poker test	X=	12.864	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2455	2579	pass	(pass if 2267 <X <2733)
2	1279	1158	pass	(pass if 1079 <X <1421)
3	636	621	pass	(pass if 502 <X <748)
4	326	306	pass	(pass if 223 <X <402)
5	166	188	pass	(pass if 90 <X <223)
6+	139	151	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//1000001-1020000

The monobit test	X=	10050	pass	(pass if 9654 <X <10346)
The poker test	X=	11.5264	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2554	2550	pass	(pass if 2267 <X <2733)
2	1283	1301	pass	(pass if 1079 <X <1421)
3	651	617	pass	(pass if 502 <X <748)
4	312	294	pass	(pass if 223 <X <402)
5	127	167	pass	(pass if 90 <X <223)
6+	145	142	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//2000001-2020000

The monobit test	X=	9987	pass	(pass if 9654 <X <10346)
The poker test	X=	20.5952	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2501	2509	pass	(pass if 2267 <X <2733)
2	1239	1216	pass	(pass if 1079 <X <1421)
3	615	640	pass	(pass if 502 <X <748)
4	336	337	pass	(pass if 223 <X <402)
5	160	165	pass	(pass if 90 <X <223)
6+	151	135	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//3000001-3020000

The monobit test	X=	9869	pass	(pass if 9654 <X <10346)
The poker test	X=	15.3856	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2481	2521	pass	(pass if 2267 <X <2733)
2	1227	1251	pass	(pass if 1079 <X <1421)
3	647	636	pass	(pass if 502 <X <748)
4	332	297	pass	(pass if 223 <X <402)
5	160	155	pass	(pass if 90 <X <223)
6+	157	144	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//4000001-4020000

The monobit test	X=	10048	pass	(pass if 9654 <X <10346)
The poker test	X=	17.0176	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2511	2462	pass	(pass if 2267 <X <2733)
2	1219	1242	pass	(pass if 1079 <X <1421)
3	612	624	pass	(pass if 502 <X <748)
4	316	335	pass	(pass if 223 <X <402)
5	172	143	pass	(pass if 90 <X <223)
6+	150	173	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

FIPS PUB 140-1 Test Result Details

Results of FIPS 140-1 Specified Tests on sample4

data: c4s(2Mbyte)

//1-20000

The monobit test	X=	10105	pass	(pass if 9654 <X <10346)
The poker test	X=	18.0224	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2539	2479	pass	(pass if 2267 <X <2733)
2	1246	1249	pass	(pass if 1079 <X <1421)
3	625	639	pass	(pass if 502 <X <748)
4	302	316	pass	(pass if 223 <X <402)
5	154	166	pass	(pass if 90 <X <223)
6+	144	160	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//2000001-2020000

The monobit test	X=	9938	pass	(pass if 9654 <X <10346)
The poker test	X=	10.752	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2518	2480	pass	(pass if 2267 <X <2733)
2	1232	1314	pass	(pass if 1079 <X <1421)
3	630	612	pass	(pass if 502 <X <748)
4	311	300	pass	(pass if 223 <X <402)
5	156	165	pass	(pass if 90 <X <223)
6+	166	142	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//4000001-4020000

The monobit test	X=	9991	pass	(pass if 9654 <X <10346)
The poker test	X=	17.7728	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2476	2467	pass	(pass if 2267 <X <2733)
2	1236	1249	pass	(pass if 1079 <X <1421)
3	604	600	pass	(pass if 502 <X <748)
4	316	309	pass	(pass if 223 <X <402)
5	150	164	pass	(pass if 90 <X <223)
6+	173	166	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//6000001-6020000

The monobit test	X=	10003	pass	(pass if 9654 <X <10346)
The poker test	X=	17.3696	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2371	2408	pass	(pass if 2267 <X <2733)
2	1291	1263	pass	(pass if 1079 <X <1421)
3	635	622	pass	(pass if 502 <X <748)
4	302	299	pass	(pass if 223 <X <402)
5	165	159	pass	(pass if 90 <X <223)
6+	159	173	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)

//8000001-8020000

The monobit test	X=	9929	pass	(pass if 9654 <X <10346)
The poker test	X=	12.4672	pass	(pass if 1.03 <X <57.4)
The runs test				
Run length	Zeros	Ones		
1	2559	2571	pass	(pass if 2267 <X <2733)
2	1248	1316	pass	(pass if 1079 <X <1421)
3	617	587	pass	(pass if 502 <X <748)
4	323	287	pass	(pass if 223 <X <402)
5	179	152	pass	(pass if 90 <X <223)
6+	140	152	pass	(pass if 90 <X <223)
			pass	(pass if all twelve counts pass)
The long runs test			pass	(pass if no long run)