ENCRYPTION Software

“無限乱数式ソフトウェア”

ソリトンランダムジェネレーター

「SRG-SDK」

Smart Security Innovation

Powered by
Smart Security Innovation, Inc.

ENCRYPTION Software

“無限乱数式ソフトウェア” ソリトンランダムジェネレーター

「SRG-SDK」

index

Smart Security Innovation

Powered by
Smart Security Innovation, Inc.

“無限乱数式ソフトウェア”
SRG-SDK ソリトンランダムジェネレーター

はじめに ｜ 発明、開発の背景

ICT（当初は**IT**が通称）が日々の生活において、常識的な時代がきっと来る。そんな時代のテクノロジーでもっとも大切なこと、それは“**ITを安全に使えること**”だ、との想いから通信技術に着目。すなわち、傍受、盗聴されないようにするためには通信が暗号化できることと考え、暗号＝乱数の研究、開発を手掛けることになりました。

また一方で、様々な角度からの視方で乱数を追究する中、「コンピューターも、もっと進化する」とも考え、その進化に追随するのではなく、コンピューターよりも卓越した乱数技術でなければならない、そんな研究から生まれたのが、今日の量子コンピューターでも解読が不可能なソリトン式無限乱数「ソリトンランダムジェネレーター “**SRG-SDK**”」です。

株式会社スマートセキュリティイノベーション（以下、**SSI**または弊社という）の代表者で、開発者である**Dr.**由井氏は乱数開発の発想の原点、それは水溜りにそそぐ雨によって起こる波紋の現象から「波を重畳させれば乱数ができるのでは…」と、その着眼点を語っている。（※重畳（チョウジョウ）＝幾重にも重なる様）

SRG［Soliton Random Generator］
ソリトン・ランダム・ジェネレーター
「擬似乱数発生装置、擬似乱数発生プログラム及び擬似乱数発生プログラムを記録した媒体」
日本特許　特許第**4351741**号
米国特許　特許番号**US 8,510,359 B2**

米国標準とされる**AES**［**Advanced Encryption Standard**］は**DES**に代わる**128**ビットブロック暗号が一般的ですが、当社**SSI**では圧倒的な処理性能、強度の優位性があるストリーム暗号＋無限乱数式（ワンタイムパッド）を採用した**SRG**［**Soliton Random Generator**］暗号化技術の特許を取得、**NIST**（アメリカ国立標準技術研究所）の評価基準を遥に超えるものです。

SRGの乱数は**10**の**27000**乗という超長周期を備える高品質な乱数発生であり、量子コンピューターでも解読が不可能とされる世界最高峰の無限乱数方式です。

※資料の内容は専門的な表現や説明、専門用語の取扱いについて、極力控えて作成すること、また乱数の具体的なロジック、アルゴリズム等についての記述は特許の取得に伴い、差控えておりますので、ご容赦ください。

Smart Security Innovation

Powered by
Smart Security Innovation, Inc.

“無限乱数式ソフトウェア”

SRG-SDK ソリトンランダムジェネレーター

乱数とは何でしょう？ ｜ソリトン式無限乱数の開発について

乱数とは簡単に言えば無作為に抽出された数字やアルファベットのランダムな値列。すなわち、その選択される数字やその数列、その順序が予測できないものを乱数と言います。ちなみに身近なものではプリンタの自然な発色は乱数（※乱数性能が悪いと国旗の写真のようにモアレが発生）で実現していたり、携帯電話は電波を乱数に変化させ、高性能な通話が軍事通信として実現しています。また**1992**年、米国で最後の核実験が行われましたが、これは核コードが解明され、コンピュータ内部で核反応のシミュレーションができるようになったためです。

このような乱数生成に近似するアルゴリズムとして、ソリトン式を採用した擬似乱数発生装置および擬似乱数発生プログラムの開発に成功しました。

擬似乱数とは乱数のように見えるが、実際には確定的な方法で求められた数字やその数列の値が生成されたものです。
したがって、上記で述べた乱数は規則性や再現性などが確定的な方法で計算できない、予測が不可能なものに対して、どれだけ近似する値を生成できるかが、擬似乱数の生成の完成度になります。

真性乱数の代表例はサイコロ。そのサイコロを振る出目で例えると、サイコロを振った出た目に対して、次に出る目を予測することは不可能であり、出た目が予想通りであっても、確率による出目であって偶然にすぎません。この繰り返し回数が増えれば増えるほど、言うまでもなく予測できない出目であり、すなわちこれが乱数です。一方、擬似乱数では確定的な方法で求められる出目という結果を理論的には予測可能なものであって、出目を生成する方法、値が問われるのが擬似乱数になります。

（※ソリトン（**soliton**）＝非線形方程式に従う孤立波で、「慣性の法則」による複数の波が衝突した後でも安定に存在するパルス状の波動のこと。）

では乱数は何に使うもの？｜ 乱数技術から日々の恩恵を受けていること

乱数（擬似乱数）は大別して、データ通信やデータ管理を行う場合に盗聴、改ざんなどをさせないために“暗号化する”方法に、また膨大なデータの“シミュレーションをする”方法として技術を有効活用することができます。

暗号と言えば、スパイ映画で表現されるような現実離れした印象を持たれるかも知れませんが、**ICT**が日常化した今日において、スマホやタブレット、**PC**を使ってサービスを受ける場合に個人を特定したり、認証を受ける大切なプライバシー情報の通信に個人が意識することなく、暗号化技術が使われています。

Smart Security Innovation

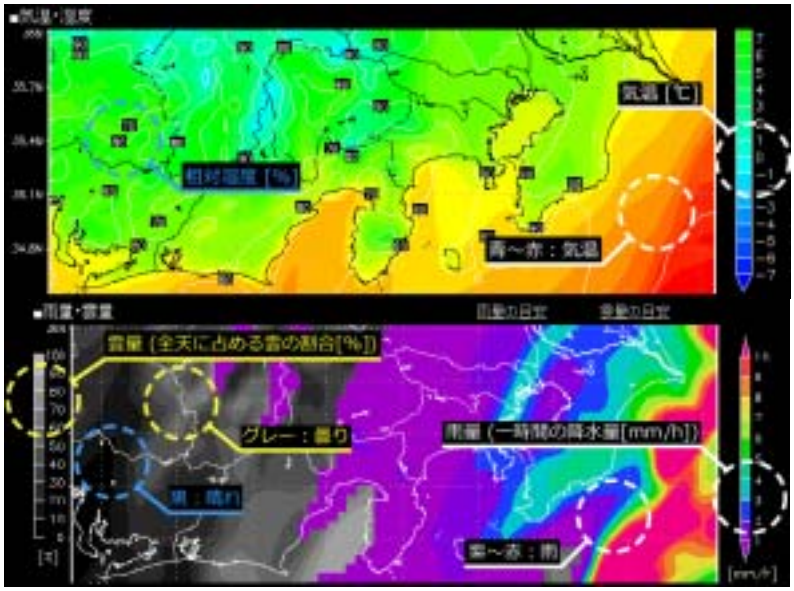
Powered by
Smart Security Innovation, Inc.

“無限乱数式ソフトウェア”

SRG-SDK ソリトンランダムジェネレーター

そのサービスを提供する企業は受信したその個人の情報資産がハッキングで脅かされ、情報漏えいや改ざん、情報が乗っ取られるようなことが発生すれば個人の不利益となり、企業はブランドイメージが失墜し、倒産に追い込まれることも少なくありません。

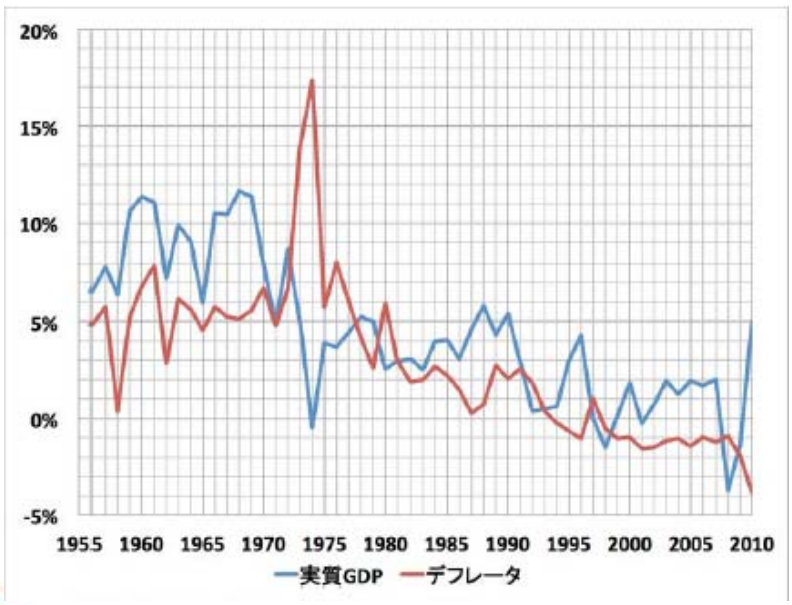
またシミュレーションと言えば、こちらも日常的に恩恵を受けているのは天気予報。
「**GPV**」気象予報や天気予報サイト「**SCW**」などがありますが、



地域エリアと広域における雨量･雲量、気圧･風速、気温･湿度、低気圧･台風進路、沿岸波浪予報（波高･波向･周期)などの様々なパラメーターと、刻々と変化、変動する大気動向の分子をスーパーコンピューターで解析できるように擬似乱数技術を活用しています。

この解析精度を向上するためにはビッグデータの処理能力を改善することがポイントになります。
したがって、いくらスーパーコンピューターの性能が高くても、コンピューターの処理能力以上に擬似乱数の生成精度に影響され、乱数生成にバラツキや偏りが発生すると正確な解析結果を求められないものになります。

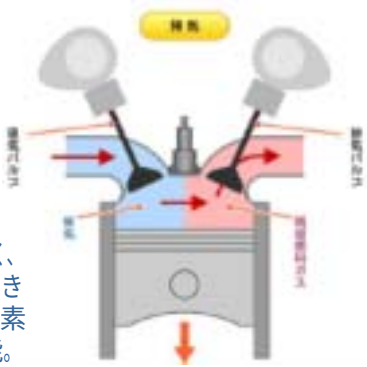
擬似乱数の生成は流体力学の範疇に属する流動解析が可能ですので、統計（**GDP**デフレーター）やエンジン燃焼などのシミュレーターなど、数多くの応用技術として活用することが可能になります。



エンジン燃焼室設計の応用

燃焼室の性能をシミュレーションで解析。

解析スピードが速く、高精度な解析ができれば、より多くの要素技術の検証が可能。



Smart Security Innovation

Powered by
Smart Security Innovation, Inc.

“無限乱数式ソフトウェア”

SRG-SDK ソリトンランダムジェネレーター

乱数の性能は何で決まる？ ｜乱数の品質の重要な3要素

乱数の性能は“高速性（乱数生成速度）”“乱数性（精度）”“周期性”の3要素が重要であり、この総合評価が品質になります。

1. 高速性（乱数生成速度）

乱数の生成速度が遅いと、暗号化によるデータ通信の速度、暗号化されたデータの再生データの生成などが遅くなり、また流動解析によるシミュレーションのデータ出力の結果も同様に遅くなることで、求められるサービスや情報が得られない状況に陥ります。

2. 乱数性（精度）

乱数の生成精度が低いと、イカサマサイコロのように出目の頻度に偏りがあったり、同じような出目ばかり出やすいのでは乱数に値しません。乱数性はバラツキや偏りが少なく、より長い周期性のあることが精度の高いものと評価できます。

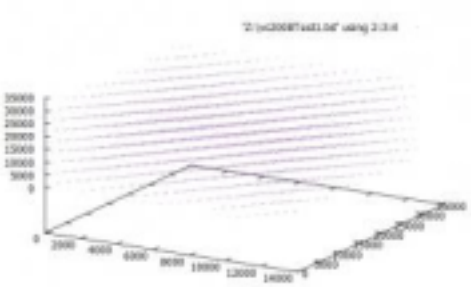
3. 周期性（安全度）

乱数の生成の周期が短いと、暗号化技術においては暗号化される数字の桁数が少ない組合せで構成される乱数と理解され、容易に解読できるものとして、暗号が見破られしまいます。例えば、周期が6桁の乱数は 10÷7＝1.42857「142857」という数式で乱数が生成されます。一般的に電子機器で使用する乱数は10の70乗前後と言われており、乗数が多くなるほど周期性が長く、無限乱数に近づき、解読が不可能なものになります。

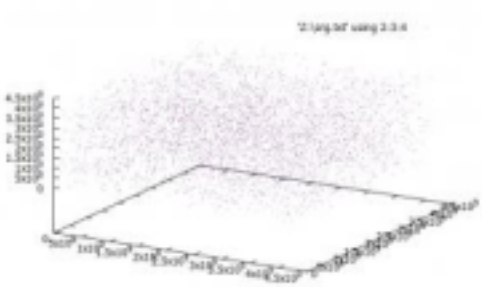
乱数の性能評価 ｜SRG（ソリトンランダムジェネレーター）の評価と優位性

米国国立標準技術研究所（NIST）はDESに代わる暗号として認証したブロック暗号の「AES」がもっとも採用されている現状があり、このAES暗号とストリーム暗号の「SRG（ソリトンランダムジェネレーター）」を比較し、その評価について、独立行政法人情報通信研究機構/カオスウェアの検査結果、NISTの評価基準の検査結果を提示して、説明します。

■一般的な乱数の生成分布図



■SRGの作る乱数の生成分布図



左図は擬似乱数による空気の分布を解析したもので、SRGは均一な分布が確認できるが、一般的乱数では乱数の性能が悪いため、線状のムラが発生するので、品質が一目瞭然です。この乱数生成の分布でSRGはシミュレーションに適応できることが確認できます。

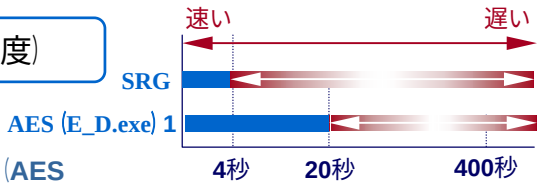
Smart Security Innovation

Powered by
Smart Security Innovation, Inc.

“無限乱数式ソフトウェア”
SRG-SDK ソリトンランダムジェネレーター

乱数の性能評価
NIST／NICT/カオスウェア検証

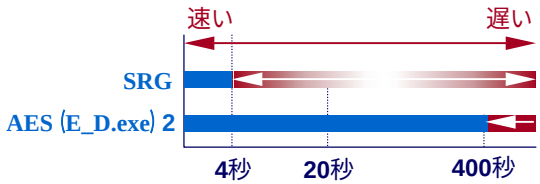
1.スピード（速度）



右図の検証ではE_D.exe（AES 128をチューニングされたもの）のフリーソフトが1、サンプルコードをコンパイルしたものが2で、これらを検証したもの。

テスト環境：インテル Core i7+Windows7+ 16GBのRAM-DISK /電机本舗

検証 1



追加検証：インテル Core i7+Windows7+ 16GBのRAM-DISK /電机本舗

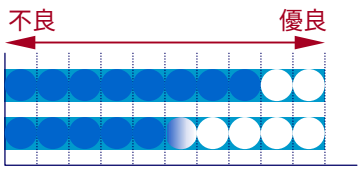
検証 2

結果

秒速1Gbpsの検証において、検証1）で、SRGは4秒と高速で、AES（E_D.exe）1に対して5倍の速さ（※フリーソフトの提供元でAESを独自にチューニングしたものと推測）を確認できます。
ただし、検証2）で、AES（E_D.exe）2（※サンプルコードをコンパイルしたもの）は400秒かかっており、結果、AES（E_D.exe）2 に対して、SRG は100倍以上の速さの優位性が確認されています。

2.バラツキ（精度）

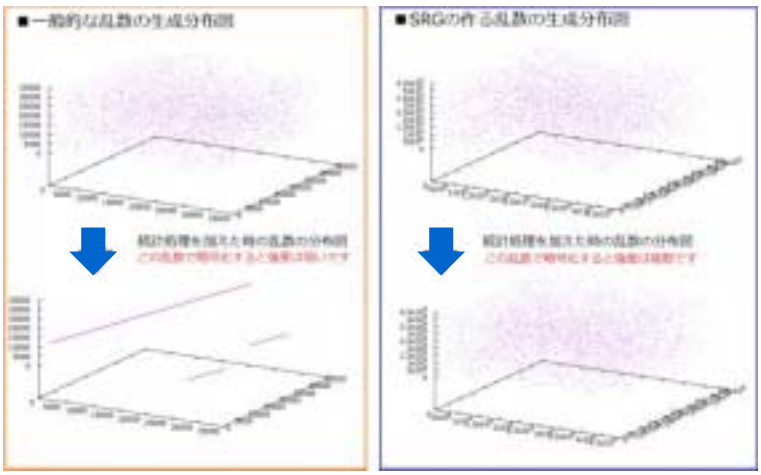
NIST「SP800-22」によるファイルテスト10本の検定連続3回



検証 1

NIST「SP800-22」STS2.1.2×100によるファイルテスト100本の単独連続検定

検証 2



結果

検証1）の「SP800-22」10本のファイル検定テスト連続3回でSRGは常に8ファイルがクリアしたことに対して、AESは6ファイルがクリアとなったが、5ファイルの場合も発生するなど、不安定さが確認されています。また検証2）では「SP800-22」の最新版STS2.1.2の機能強化版「NIST SP800-22 STS2.1.2×100」（※100本のファイルを連続検定テストができるよう機能を強化したもの）でSRGを単独検証。
結果、SRGは100のファイルサンプルに対して、90の乱数ファイルが合格、NISTの基準をクリアするものです。

※NISTでは「SP800-22」にて乱数ファイル10本を検定して、8本以上の合格を指針としています。※

※機能強化版「NIST SP800-22 STS2.1.2×100」乱数100ファイルの一括自動検定機能ソフトとしてリメイクしたものを無料配布中。

Smart Security Innovation

Powered by
Smart Security Innovation, Inc.

“無限乱数式ソフトウェア”
SRG-SDK ソリトンランダムジェネレーター

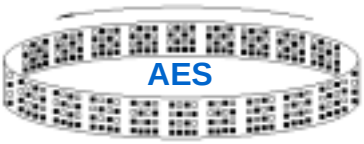
乱数の性能評価
NIST／NICT/カオスウェア検証

3.周期の長さ（安全度）

※周期性は前記の乱数性（精度）と併せて検証しています。

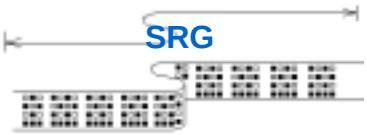
結果

本検定の補足になりますが、**AES暗号の周期性は10の77乗（10の80乗前後）と推測**できます。
詳しく観ると小さな周期が**59、81、87、27、2**バイト間隔で繰り返しがありそうです。コンピューター内部でメモリの桁数を増やせば増やすほど周期を長くすることができますが、複雑な処理をすることによって遅くなります。**AES暗号はすでに処理速度が遅く、これ以上の複雑な暗号処理ができない状況**であることが確認できます。（※コンピューターのリソース（メモリ）が有限であるため、数字の組合せ、順列で取り得るパターンが出尽くせば振り出しに戻って、同じ結果を繰り返します。）



有限乱数方式

一方、**SRGは乱数精度が高く、周期性も10の27000乗と長いだけでなく、ワンタイムパッド（1度限りの使い捨て暗号）方式を採用**しており、その乱数は規則性の無い乱数列で、**1**度使った乱数表を使用しない、圧倒的な優位性があるもので、暗号として高い性能、安全性を備えていることが判ります。



無限乱数方式

※外務省では、最高機密は「無限乱数式暗号」の使用を推奨しています。※

4.SRG周期の特長

※**SRG**が暗号化する周期の特長について補足説明します。

SRGの周期は、**2**つの乱数生成ボックスからランダムにピックアップされた数字の組合せによって、規則性のない無限乱数を生成しています。その乱数生成の条件について、簡単に説明します。
※ここでは**2**つのボックスを「素数カードボックス」と「乱数セルボックス」と呼称します。

■ 素数カードボックス

1. 素数を保存したボックスになります。**1**つひとつのセルに異なる素数を持ち、このボックスに取り得る組合せは階乗に従います。（※階乗（カイジョウ）＝**1** から **n** までのすべての整数の積）

3	5	7	11	19	23

・・・ **6**個のセルがある場合、この素数カードボックスの組合せは**720**通り。

2. **6**個のセルの並びを選択する確率を決めます。最初のセルは**1/6**の確率で選択できます。

3	3	5	7	11	19	23

Smart Security Innovation

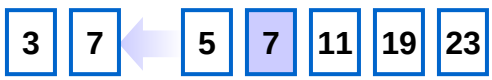
Powered by
Smart Security Innovation, Inc.

“無限乱数式ソフトウェア”
SRG-SDK ソリトンランダムジェネレーター

乱数の性能評価
NIST／NICT/カオスウェア検証

■ 素数カードボックス

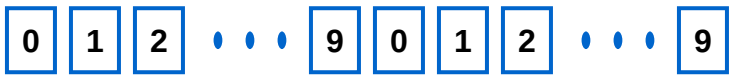
3. 次のセルは既に1枚引いていますので、1/5の確率で選択できます。



4. 次のセルは既に2枚引いていますので、1/4の確率で選択できます。
このように6×5×4×3×2×1の組合せの存在が判ります。

■ 乱数セルボックス

実際にはコンピューターと相性の良い16進法で使用しますが、ここでは判りやすく10進法で説明します。
10進法の場合、0～9までの10枚1組のセルを n セット用意します。（※ n は任意の数です。）
n が大きいほど周期は長くなります。



SRGではこの乱数セルの数字を素数カードボックスの数字と入れ替えて、乱数生成します。乱数生成時にこのボックスの取り得る組合せはセルの階乗となります。セルを100用意した場合、100の階乗で10の157乗になります。単にこの組合せであってもAESの周期を超えることを理解できるものです。

結果

5.乱数の総合評価

※SRGの評価は「独立行政法人情報通信研究機構/カオスウェア」、米国国立標準技術研究所（NIST）の検定の合格基準に基づいています。

「SRG-SDK」の性能は鍵の長さは1,200ビット以上、指定可能で、生成する乱数の周期は10の27000乗であり、その作業負荷はたったの8KBと超高速。20KB程度のメモリで十分に稼動する。また周期、速度と併せて、乱数性、周期性、偏りが少ない安定性の高いものとして、世界最高品質の暗号と評価された。

アルゴリズム	速度（Mバイト/秒）	精度（検定合格率 %）	周期（10の指数）
SRG（ソリトン式）	268	80	27000
AES（ブロック式）	53	50	77

SRG（ソリトン式）	高速性（乱数生成速度）	“15Gbps /sec”	世界最高の速度
	乱数性（精度）	“周期性、偏りが少ない”	世界最高の精度
	周期性（安全度）	“10の27000乗”	世界最高の周期

Smart Security Innovation

Powered by
Smart Security Innovation, Inc.

“無限乱数式ソフトウェア”

SRG-SDK ソリトンランダムジェネレーター

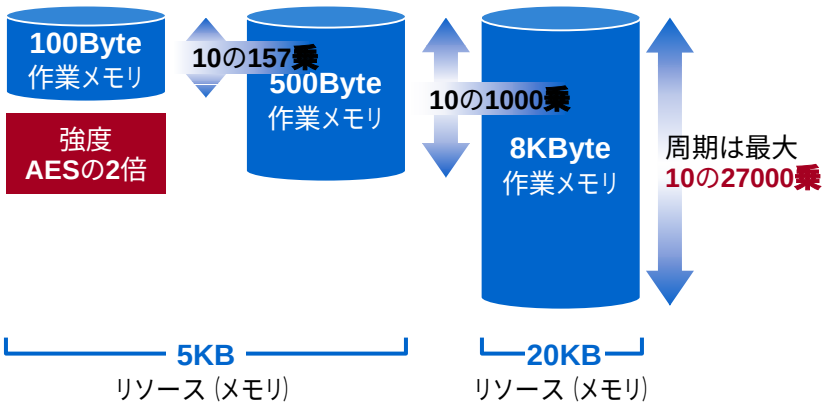
「SRG-SDK」の稼動スペック ｜プラットフォームを選ばないポテンシャル

SRGの性能は検査結果から確認できるように“世界最高品質”と評価され、ブロックチェーンなどの高度なセキュリティに対応した暗号強度であることは前述から理解いただけるものですが、更に驚く特長として、鍵の長さ、周期、リソース（コンピューターのメモリ）から選択することが可能で、例えば、鍵長の周期が**10の157乗**（※**AES**の約**80**乗倍/約**2**倍の周期）程度で良ければ、**4**ビットの**CPU**上で稼動することも可能であることから、プラットフォームを選ばない拡張性があること、また汎用性も容易であり、組込み**CPU**でも高速稼動を実現します。

防犯･監視カメラ、キーレスロックなどやドローンの遠隔操作の盗聴対策など、小型の**CPU**にも組込みが可能で、常識的に稼動、実装を提供します。

SRGの適用範囲

SRGの稼動スペック



作業メモリとは別にプログラム領域のリソース（メモリ）が必要となります。**10**の**1000**乗程度までならプログラム本体を含めて、**5KB**程度のリソース（メモリ）で稼動します。

なお、**AES**の**2**倍の強度で作業メモリ**100Byte**程度で稼動、**4bitCPU**の上で高速稼動が可能です。

Smart Security Innovation

Powered by
Smart Security Innovation, Inc.

“無限乱数式ソフトウェア”
SRG-SDK ソリトンランダムジェネレーター

SRGの事業ベクトル/アジェンダ ｜解析技術/暗号化技術によるソリューション

弊社では急務なサイバーセキュリティ対策から近未来のICT×IoTのイノベーションまで安全を担保する技術を提供することをミッションとして、幅広い事業セグメントにチャレンジマインドで邁進します。

- ソリトン式
  - 1.HW事業
    - 1-1.USBメモリ
      - 1-1-1.AutoLockU
    - 1-2.組込製品
      - 1-2-1.スマホ･携帯デバイス向け
      - 1-2-2.ネットワーク機器
        - 1-2-2-1.VPN機器
        - 1-2-2-2.DMZ機器
        - 1-2-2-3.WiFi機器
      - 1-2-3.仮想通貨/スマート決済
      - 1-2-4.クレジット決済機器
      - 1-2-5.防犯カメラ･防犯システム
      - 1-2-6.ドライブレコーダー
      - 1-2-7.db暗号化モジュール
      - 1-2-8.HDD用ホットシュレッド
    - 1-3.ドローン通信制御
  - 2.SW事業
    - 2-1.SDK提供
      - 2-1-1.WWWサーバ
      - 2-1-2.メール･各種サーバ
      - 2-1-3.CAD/CAE 各種サーバ
    - 2-2.アプリケーション開発
      - 2-2-1.PC向け総合セキュリティ
      - 2-2-2.PC向けHDD暗号化ツール
      - 2-2-3.DBサーバ/エンジン
        - 2-2-3-1.MySQL
        - 2-2-3-2.Oracle
        - 2-2-3-3.EMPRESS
    - 2-3.スパコン用乱数発生装置
    - 2-4.OS用セキュリティモジュール
  - 3.特殊フレームワーク事業
    - 3-1.金融･ブロックチェーンの暗号化
  - 4.シミュレーション関連事業

Smart Security Innovation

Powered by
Smart Security Innovation, Inc.

“無限乱数式ソフトウェア”
SRG-SDK ソリトンランダムジェネレーター

弊社では**Windows、Linux、Mac**をプラットホームとした**C/C++**言語、アセンブラを使用したソフトウェア、セキュリティソフトウェアの開発、デバイス、ドライバーの開発および各種ソリューション、**OEM**供給、ビジネスアライアンスなど、様々なビジネスニーズにお応えできるよう、ご検討いたしますので、お気軽にお問い合わせください。

社名	株式会社 スマートセキュリティイノベーション
英字名称	**Smart Security Innovation, Inc.**
代表取締役	由井 清人
所在地	東京都港区高輪 **1-2-16-6A**
TEL	**03-6688-9181**
FAX	**03-3447-2775**
MAIL	**Info@ssi.ac**

Powered by
Smart Security Innovation, Inc.