# 解読は“不可能”な
# エンクリプション（暗号化）で
# 創造する頼れるパートナー。

**Powered by**

スマートセキュリティイノベーション

Smart Security Innovation



## 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。

## はじめに　サービスを開始するに当たって

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）は昨今のサイバー攻撃による被害状況を鑑みて、弊社が貢献できるサイバーセキュリティ対策の実現に向けて、より身近な窓口として事業化をスタートしました。

**SSI設立の前身、**本事業化のポテンシャルとなる電机本舗は**SSI**の発足を機に、多岐にわたる課題解決に挑戦する研究、開発に特化した「**Dr.**由井研究所（**Dr.YUI Lab.**）※仮称」として事業領域を拡大しつつ、弊社の監修にも勤め、一方、**SSI**ではその**30**年間の膨大なノウハウ、開発実績の集大成として、世界最高峰の暗号化技術によるセキュリティのソリューション、ノベーションに注力、日本国内のサイバーセキュリティを高度化すること、**ICT**（**Information and Communication Technology**）×**IoT**（**Internet of Things**）の基幹産業への貢献をすべく、その事業ミッションのコア技術としてご提案するものです。

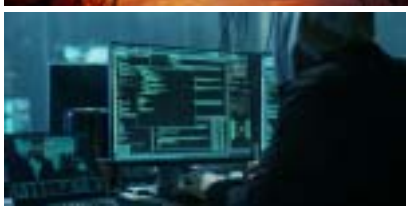
※資料の内容は専門的な表現や説明、専門用語の取扱いについて、極力控えて作成することで、幅広い事業セグメントの様々な立場の方々にご理解をいただくことを主旨としてご提示し、お役に立てればと考えております※。

## 現況の課題　サイバー攻撃に対する課題認識

近年のサイバー攻撃は様々な形態で巧妙化する傾向にあって、その被害は世界的に爆発的な猛威を振るっており、攻撃に対する防御策をいくら実施しても、更なる攻撃手法で対策をすり抜ける、そんな現況が周知のところではないでしょうか。

国内では社会問題として報道されたウィルス「**Wanna Cry**」のランサムウェア。**PC**機能を乗っ取り、復旧するための金銭を恐喝する標的攻撃型マルウェアが記憶に新しいところに、耳を疑うような仮想通貨の流出問題が発生。こちらは従来のマルウェアを使わない「非マルウェア攻撃」と推測され、単なるセキュリティの甘さ！？では片付けられない事象。

また米国ではセキュリティ専門家のウェブサイトが、ジャックされた**100**万台もの防犯カメラ、ビデオレコーダーなどから攻撃を受けてダウンする事件や送電網システムがハッキングされ、実際に電力供給が遮断される事件も発生している。



**2018**年、全世界での被害総額は**90**億米ドル超になるというレポートも出ていますが、これから日進月歩で進化する近未来の**ICT**、**IoT**において、インターネットと接続するスマート家電を始め、医療機器、医療システムを含めた**IoT**機器がハッカーに乗っ取られると人体に被害を与え、場合によっては人命を危険にさらしてしまう可能性があるという深刻な問題であり、もはや**PC**などの情報端末等の数で終始しない被害の増大が想定される、セキュリティターゲットが拡大している現状にある。

## 高まる危機感と問題

サイバーセキュリティ対策

米国では国土安全保障省が「**IoT**のセキュリティを担保する戦略的原則」を公表、政府が「設計段階でセキュリティ機能を組み込むこと」を怠る企業に対し、訴訟を起こせるよう提言。更に様々な分野のテクノロジーに関する産業基準を定める米国国立標準技術研究所（**NIST**）機関は「より防御力が高く攻撃耐性の強いネット接続型システムを開発するための業界向け“自主的ガイドライン”を策定」した。


経済産業省

日本でも情報処理推進機構（**IPA**）をはじめとする公的機関から、**IoT**のセキュリティ対策についてのガイドラインが公開、経済産業省も「サイバーセキュリティ経営ガイドライン」を策定し、経営者が認識する必要がある**3**原則、**CISO**（情報セキュリティ管理最高責任者）等に指示すべき重要**10**項目に“自社のみならず、系列企業やサプライチェーンのビジネスパートナー等を含めたセキュア対策が必要”と明示している。

一般的なセキュア対策として、官公庁および多くの民間企業は、堅牢なルーター、ネットワークファイアウォール、ウェブアプリケーションファイアーウォール（**WAF**）などのサイバーセキュリティ機器をデータセンターに展開し、ウェブベースの情報資産を防御しています。これらのデバイスにより、ウェブセキュリティが提供されますが、防御手段としては重大な弱点があります。

### サイバーセキュリティ対策の弱点

1. これらのデバイスは着信トラフィックを検査およびフィルタリングするものであるため、サイバー攻撃者が標的とするパフォーマンス低下ポイントや**SPOF**（**Single Point of Failure** /単一障害点）になりやすく、システム全体が障害となること。
2. デバイスはデータセンター内にあるため、データセンターと電気通信事業者を結ぶインターネット回線をブロックしようとする攻撃を防ぐことができない。
3. オンプレミスの機器およびソフトウェアは、サイバーセキュリティとして継続的な運用や頻度の高いメンテナンスの必要があり、またコストパフォーマンスも悪い。
4. ネットワーク環境外に重要データを管理し、これらのデバイスを介して何らかのエンドポイントからデータ転送または移動する手法において情報漏えい対策はできるが、データ転送または移動時の感染で情報の改ざん、もしくは情報の破壊につながる危険性がある。
5. ネットワーク環境下にあるデバイスに接続するエンドポイントによる不正処理、情報端末の盗難による情報流出等の対策が必須となる。

このようにセキュア対策の弱点を踏まえると圧倒的な攻撃者優位の実態が続くものと考えられ、完全にサイバー攻撃を防ぐことは困難であり、ゼロリスクでないことを前提とした対策をする必要性があることは間違いない。ただ、ここでの提言はゼロリスクでないことを念頭に置きつつも、被害が起こってからの対応策（インシデントレスポンスやデジタルフォレンジックなど）ではなく、なぜ水際で防いで内部ネットワークに入れないようにできないのか、エンドポイントセキュリティで感染を防ぐことができないのか、などについて、その問題点を提言したい。

## なぜ防げないのか？ | セキュリティ技術の問題点と対策手法

前記のセキュア対策と同様のインフラとしても、サイバーセキュリティを高度化できる手法があり、抜本的な違いがあるのは、そのデバイスからデータ通信する経路上の盗聴対策であり、すなわち暗号化技術にある。

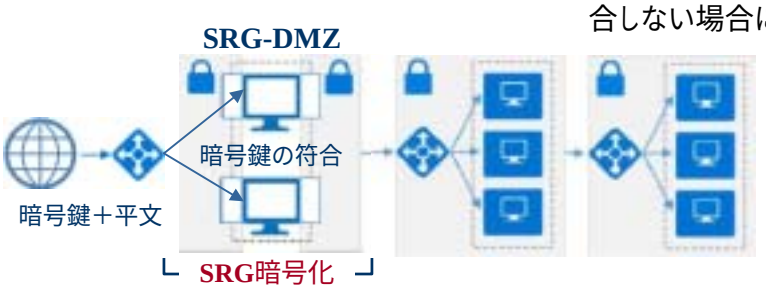
通信経路からのデータ漏えいを防止するには、一般にSSL（Sec-ure Sockets Layer）やVPN（Virtual Private Network /仮想閉域網）など通信経路の暗号化技術を使用する。またより安全性を高めるために、アプリケーション間でデータを暗号化して受け渡す技術を導入している場合も多く、「Point-to-Point Encryption（P2PE）」と呼ぶ暗号化手法になる。だか一般的なSSLやVPNだけでは不十分とする論調が米国のセキュリティ専門家の間で常識になりつつある。

その理由は現在、SSL/TLS（Transport Layer Security）やVPNを始めとする通信経路に使用されている暗号化のほとんどがAES暗号であり、量子コンピューターなどのコンピューター技術の発展、進化によって解読されてしまうということを認識されていない問題がある。（※米国国立標準技術研究所（NIST）はDESに代わる暗号としてAESを認証したが、既にNISTにも課題認識があり、前記に述べたようなガイドラインの策定に至っている。）

すなわち、サイバーセキュリティのコア技術となる暗号が見破られてしまうのなら、いくら対策を実施してもいたちごっこ、もぐら叩きということになり、対策には至らない。

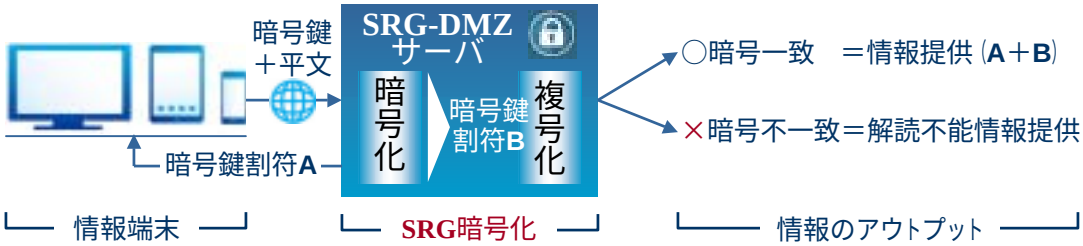
そこで弊社はたとえ量子コンピューターであっても解読は不可能な“無限乱数式ソフトウェア”　ソリトンランダムジェネレータ「SRG-SDK」を活用した暗号化技術の提供でゼロリスクを目指すサイバーセキュリティ対策にチャレンジマインドをもって提言するものです。（※NISTの評価基準を遥に超えるものです。）

弊社が提言する1つ目のサイバーセキュリティ対策として、インタネットなどの外部ネットワークと社内ネットワークの中間につくられるネットワーク上のセグメント（区域）＝DMZ（DeMilitarized Zone /「非武装地帯」※軍事用語）にサーバ（ファイアーウォール機能を含む）を設置、SRG暗号エンジンを付加するものによって、不正アクセスによる社内ネットワークへの進入を防御するだけでなく、情報端末からDMZサーバへの情報請求に対して、双方の暗号が符合しない場合にはDMZサーバ内の暗号も符合せず、解読不能な情報を吐き出す。



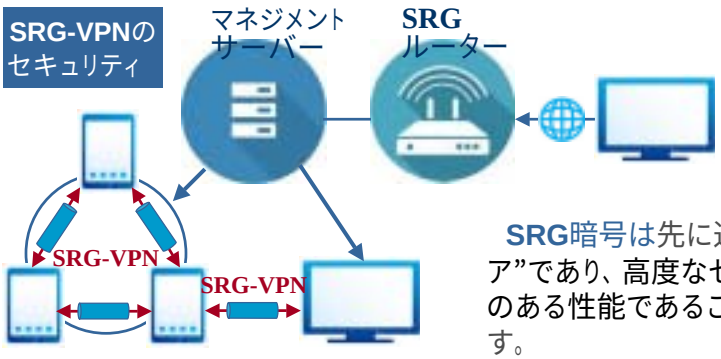

このようにサーバ内の情報をSRG暗号化することは不正アクセスに対するサーバ処理の負荷も軽減できる。また他のサーバにも同様に展開が可能であり、連係複合化することで、より強固なセキュア対策が可能となります。

## SRG-DMZサーバによるサイバーセキュリティ対策




**2つ目のポイントは**アタックと言われる複数のソースから大量のトラフィックを送り、ウェブサイトやオンラインサービスをユーザーが利用できないようにする**DDos**攻撃（**Distributed Denial of Service Attack** /分散型サービス妨害攻撃）の対策には**SRG**ルーターの設置＋アプリケーションセキュリティ対策が望ましく、大規模なウェブトラフィックを処理できる拡張性を備え、**UDP**（**User Datagram Protocol**）や**SYN**フラッド（**SYN Flood Attack**）などのネットワークレイヤーへの**DDoS**攻撃を回避、**HTTP**や**POST**フラッドなどの**DDoS**攻撃をネットワークのエッジで対処するなど、アプリケーションのオリジンに到達することを防御できます。

## SRG-VPNのセキュリティ




**また3つ目のポイントとして、**エンドポイントからの情報端末のアクセスを**SRG-VPN**（**SRG**暗号化プライベートネットワーク）にアップグレードすることで、暗号の強度が向上する専用回線となり、より効果的なサイバーセキュリティ対策が実現できます。

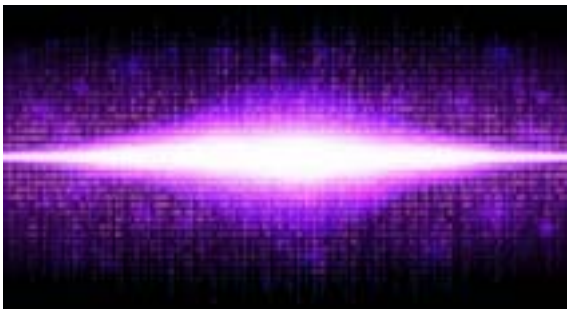
**SRG暗号は**先に述べましたように解読が不可能な“無限乱数式ソフトウェア”であり、高度なセキュリティのインフラに対応できる拡張性、暗号化強度のある性能であることから、過度な設備が必要なく、セキュア対策が可能です。

**「SRG-SDK」の暗号化技術は**電子記録媒体のソリューションとして、個人認証と情報漏えい対策を備えた暗号化エンジン付デバイスとして「**SRG**暗号エンジン＋指紋認証付セキュア**USB**」を開発。官公庁、大手警備保障会社、大手通信会社、大手通信機器販売会社ほか数十社に提供、またネットワークディスクの暗号化による教育システムを高等学校に、社内の**SRG**セキュリティシステム＋外出先の利用約款に対応したセキュリティソリューションを大手自動車メーカー向けに開発、提供するなど、約**10**年間の社会実装の実績があります。

**また「SRG-SDK」を活用した**セキュリティソフトウェアとして、離席管理で簡単セキュリティ「**PeopleLogOn**（ピープルログオン）」、ディスク丸ごと暗号化セキュリティ「**Peo-pleLock4**（ピープルロック）」、不正コピー防止暗号化セキュリティ「簡単**DRM**プロテクションマネージャ」などのパッケージソフトをリリース、販売しており、フリーウェアの暗号化ソフトも多数、ご提供しています。

## 暗号化技術の優位性

## 「SRG-SDK」はココが凄い！



暗号、乱数に関する詳しい説明につきましては別途、専門資料としてご案内しておりますので、そちらをご確認いただくこととして、ここでは解読は不可能な“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「**SRG-SDK**」の性能などのポテンシャルについて、知ってもらいたい旨、ご案内します。

まず、**AES**ブロック暗号は、鍵長やブロック長が可変の共通鍵方式。パラメーターとしては、鍵長は**3**種類あり、**128**ビット、**192**ビット、**256**ビットのいずれかで、ブロック長は**1**種類、**128**ビットのみ。そのため、鍵長によって「**AES-128**」「**AES-192**」「**AES-256**」という**3**種類から選択。ただし、鍵長が多いほど安全性が高まるものの、それだけ処理速度などが低下するため、「**AES-256**」は敬遠され、セキュリティが概ねしっかりしているとされる「**AES-128**」が最もよく利用されているのが現状。「**AES-256**」の鍵長の周期は**10**の**77**乗程度であり、メモリの桁数を増加すれば周期性が向上するものの、汎用性が低く、また処理速度も低下する弱点があることから、「**AES-128**」を採用されているが、簡単に解読されてしまう有限乱数式に値するものに間違いない。

それに対して「**SRG-SDK**」の性能が大きく異なるポイントは ストリーム暗号＋“無限乱数式（ワンタイムパッド＝**1**回限り暗号）”であること。
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、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。
（※**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」）

### 暗号（アルゴリズム）別の比較検査実績

| アルゴリズム | 速度（**M**バイト/秒） | 品質（検定合格率 **%**） | 周期（**10**の指数） |
|---|---|---|---|
| **SRG**（ソリトン式） | **268** | **80** | **27000** |
| **AES**（**SHA-1**） | 53 | 50 | 77 |
| メルセンヌ・ツイスター | **550** | 30 | 6000 |
| **BlumBlumShub512** | 0.066 | **N/A**（評価不能） | **N/A**（不明） |

※品質において、評価機関が過去に検査評価した中で、最も高い評価、数値を確認したもの。
※テスト環境は　インテル **Core i7+Windows7+16GB**の**RAM-DISK**

### 「SRG-SDK」の3つの性能／暗号強度

| | | |
|---|---|---|
| **SRG**（ソリトン式） | 周期 | “**10**の**27000**乗” 世界最高の周期 |
| | 速度 | “**15Gbps /sec**” 世界最高の速度 |
| | 精度 | “周期性、偏りが少ない” 世界最高の品質 |

※米国国立標準技術研究所（**NIST**）の**STS2.1.2**は**2014**年**7**月版となる**SP800-22**の最新版乱数検定ソフト、**NISTSP800-22**の最新版で検証。（※**SRG**の評価は基準値を遥にクリアするもの　/　※検証レポートは別途、ご確認ください。）
※**STS2.1.2**の強化版「**NIST SP800-22 STS2.1.2×100**」無料配布中

またSRGの特長として、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と考えますが、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ることで組込みCPUでも高速稼動を実現します。

## SRG活用による提案

## これからのICT×IoT

近未来のライフスタイルでは私たちが世界中の「何処にいても」国、場所に関係なく、時差やサービスの営業時間などの「時間帯にとらわれることもなく」ひとりで、大切な家族やパートナーと、大勢の仲間みんなで、「コミュニティーで繋がる」、「使いたいサービスで繋がる」、「やりたいビジネスで繋がる」など、もっと快適で、楽しく、そして大切なことは“安全に”。これからのICT×IoTはそんな制約や制限の突破に挑戦し、私たちの創造を超える未来へ導いてくれるものになると確信しています。

そんな明るい未来像を創るイノベーションに欠かせないのは“安全”であること。未来の安全を担保するコア技術として「SRG-SDK」で貢献したいと考えています。

ICT×IoTの創造は、それぞれの分野のイノベーションにおいて共通することは最先端テクノロジー＋データ、情報通信テクノロジーのベストマッチングにあり、通信のほとんどが無線、電波を介して実現するイノベーションになります。
「無線認証」、「無人監視」、「遠隔操作」、そして「無人走行」など操縦、操作や機密などに係る重要な情報通信が不正なアクセスによって、盗聴される、改ざんされる、乗っ取られる、などが絶対に発生してはならない、重要な安全を脅かすファクターであり、成功へのピースとして「SRG-SDK」の活用シーンをご提案します。

サイバーセキュリティ対策のセンテンスでは主にサービスを提供する企業や社内ネットワーク側のインフラ、プラットフォームに関係するコア技術として、「SRG-SDK」による改善策を述べましたが、ここではユーザー側（クライアント）に視点を置いて、そのサービスを取り巻く「SRG-SDK」の必要性、改善策についてご案内することとします。

まずはクライアントのセキュリティ対策では私たちの生活でなくてはならないものとなったスマホなどのエンドポイント。インターネットの普及により、PCはもとより、携帯電話、スマホやタブレットなどの情報端末の発展、目覚しい進化により、そのエンドポイントは限定的なネットワーク端末ではなくなり、多種多様な利用方法、特定しない場所から公衆無線LANなどを介して、情報の送受信が可能となっている。

無線認証からネットショッピングをして決済をしたり、銀行に出向くことなく送金ができたり、電話をすることなく予約をするなどのサービスを受けたり、また帰社せずに外出先からリモートアクセスを使って社内**LAN**に接続すれば、外部から社内のアプリケーションを使用できたり、社外ユーザーからエクストラネット（イントラネットに接続するネットワークシステム）を活用して取引をしたり、エンドポイントのサービス範囲も拡大している。

現段階で判断できることは上記の述べた**“特定しない場所からの公衆無線LAN”を介するエンドポイントの情報端末そのもののセキュリティを観ると無防備な状態に晒されており、具体策がないのが現状。**ただし、セキュリティ技術の問題点と対策手法のところの**3**つ目で述べましたように“エンドポイントからの情報端末のアクセスを**SRG-VPN**にアップグレードする”の対策は可能であるが、特定のサービスを提供する企業に繋ぐ場合に限った対策案に過ぎない。

― 従ってクライアントを守るための**改善ポイントは公衆無線LAN**。
**2020年**の東京オリンピック開催や訪日外国人の増加に伴って公衆無線**LAN**のサービススポットは拡充されており、日本人にとってもその利便性は飛躍的に高まっていますが、安全性には疑問があり、こちらも「**SRG-SDK**」によるアップグレードが必須となります。
もちろん、**家庭用の無線LANのWi-Fiルーター、ターミナルも同様**です。不正アクセスの対策のみならず、スマホやタブレット、**PC**などのエンドポイントセキュリティを実現するために**OS**の統合にも着目し、改善策を検討していきます。

次にクライアントの安全を見守るセーフティテクノロジー、つまり盗難、盗聴、盗撮などを無人監視する防犯カメラ、監視カメラとビデオレコーダーを始め、入退出時のセキュリティパスや、スマホ、タブレットを使ったキーレスロック、外出先からでも確認できる防犯監視モニターなどの自己防衛を支援するサービスも数多く、目新しいものでは不審者を判定するディフェンダーシステムと連動する解析システムなど、防犯意識の高まりとともに、様々なニーズの対応策や防犯対策のシーンと警備、その体制に至るチェック＆アクションでシステム化されている。

この監視情報のデータ通信も固定回線でなく無線、インターネットを介した場合は盗聴が可能であり、無線**LAN**と同様で通信回線の暗号化が必要になります。

最後に数ある遠隔操作の中から物流を始め、産業用ロボット、警備・防災偵察機、軍用兵器など、その活躍に大きな期待を集めるドローン。既に放送メディアを通じて、私たちが体感したことことがない上空からの映像が観られたり、福島第一原発事故における汚染区域でドローンに搭載された**GPS**による位置情報と空間線量のリンク測定で活躍するなど、その認知度が高まる中、**2018年3月16日**に「ドローンの商用化へ政府が動き出す。今夏に離島や山間部で荷物を運べるようにするほか、国土交通省は**2020**年以降の都市部での本格解禁をめざし検討に入る」と日本経済新聞が報じた。またこの報道を先取りしたかたちで、（株）**NTT**ドコモはドローンを活用したビジネスを支援する「ドローンプラットフォーム **docomo sky**」を開発。ソーラーパネル自動点検・解析サービスとしてトライアル版の提供を開始した。

ドローンの飛行は大別して遠隔操作と自律飛行で、一般ユーザーが操縦するのはラジコン式の側面が強い遠隔操作だが、産業界から期待されるのはドローンの自律飛行という自動運転が実用化することにある。（飛行機では自律航法とオートパイロットが主流であり、既に実現されている。）

これが実用化すれば物流業界のイノベーションであり、様々なソリューションが起こることに違いない。

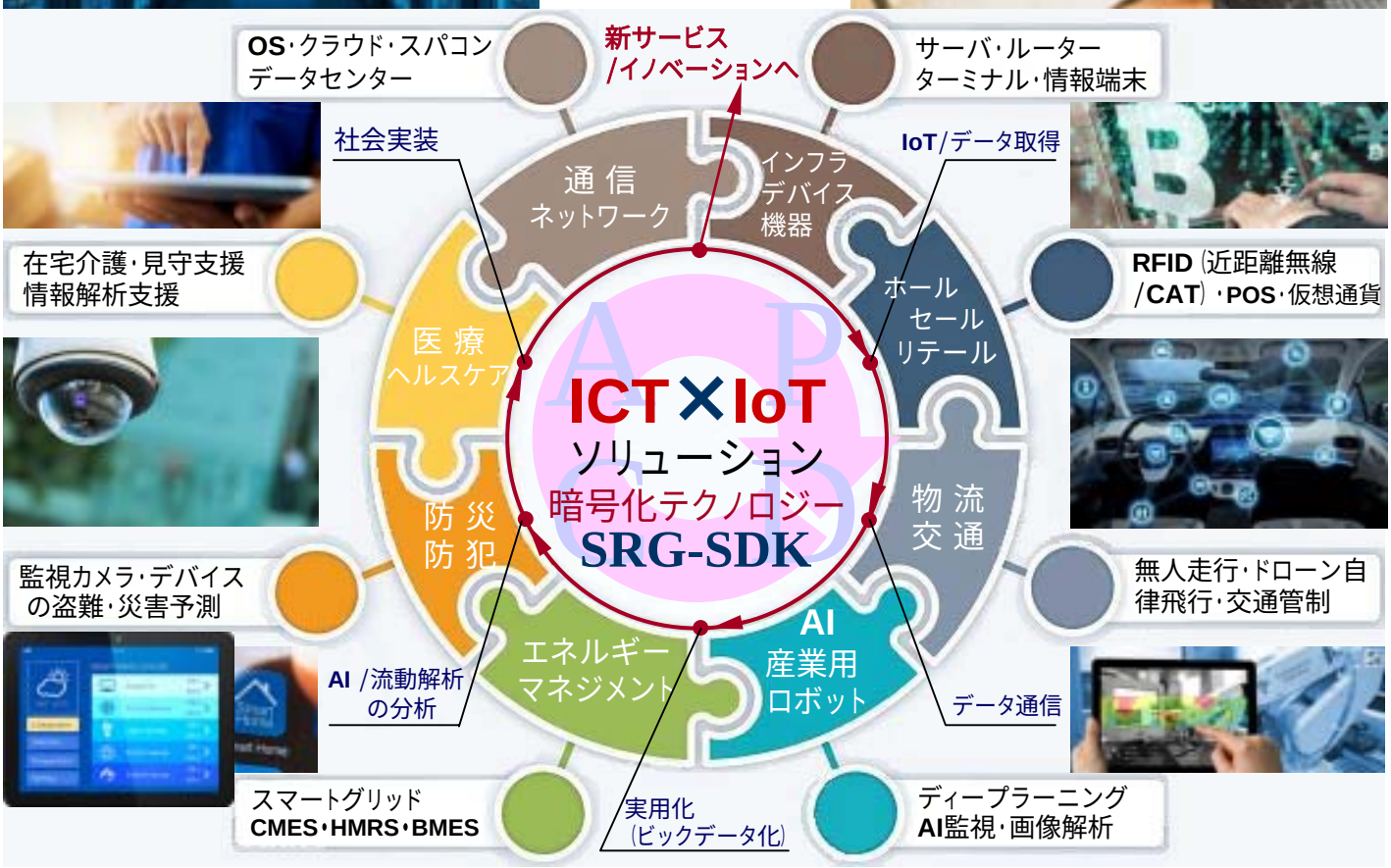
ドローンの操縦のいずれの方法においても、リモートコントローラー側に小型の**SRG-CPU**、ドローン側に**SRG**受信機を搭載、またドローンからのデータ通信、受信側のレコーダーに**SRG-SDK**が必要となり、ドローンの操縦が乗っ取られない、ドローンが取得したデータを送信時に盗聴されないことで、安全飛行によるミッション遂行が達成されるでしょう。

ドローンの自動運転が実用化することは直ぐそこまで近づいた実感がありますが、同じような**GPS**レーダーが用いられる自動車の無人走行という自動運転が実現することは様々なハードルがあり、「限定走行が**2020**年にも、」と少し先になりそうだが、**SSI**が提供する世界最高峰の無限乱数式ソフトウェアであるソリトンランダムジェネレーター「**SGK-SDK**」が活躍することになりそう。（※レポート**vol.2**でご案内します）

## 注目したいICT×IoT

「SRG-SDK」の活用を様々な事業セグメントで

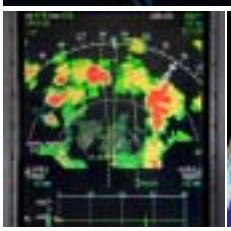
近未来のICT×IoTは情報端末などのデバイス、通信ネットワークのインフラなどのイノベーションによって、飛躍的な更なる成長を遂げようとしています。しかし、日本国内において抱える課題はエネルギー問題を始め、少子化、超高齢化時代、地域経済格差、そして人財不足など、多岐にわたるものであり、その解決は容易ではありません。
弊社として、**ICT×IoT**をもっと快適に、未来の安全が担保できるように、未然に解決を図る。そんな**1**つひとつの取組みで課題解決に貢献すべき、大別する**8**つの事業セグメントに着目し、パートナーシップで実現を目指します。

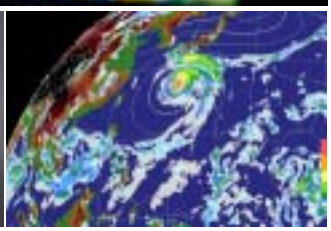



安全を約束するセキュリティピースとして「**SRG-SDK**」が**8**つの事業セグメントで貢献し、**ICT×IoT**を安全に創造できるスタンダードテクノロジーを目指します。ソリューションのプロセスは［**IoT** /データ取得］→［データ通信］→［実用化（ビッグデータ化）］→［**AI** /流動解析の分析］→［社会実装］→新サービスの開始 の**PDCA**サイクルを精力的なアクションで対応します。また「**SRG-SDK**」は“解析支援”として活用できるポテンシャルがありますので、応用技術として次項でご案内します。

## SRGによる流動解析 | 応用技術のポテンシャルについて

**SRG**［ソリトンランダムジェネレーター］はソリトン式のアルゴリズムを採用した暗号化技術、すなわち乱数の擬似発生装置、擬似発生プログラムであり、流体力学の範疇に属する流動解析が可能なものになります。





例えば刻々と変化、変動する大気動向に対して、乱数生成の処理を連続実行、流動解析した結果、天気予報として情報提供を受けています。この流動解析に**SRG**を採用することで、ビッグデータの処理能力（※特に処理スピードアップ）が向上、より高精度な解析情報を得ることが可能です。処理能力が改善されることによって、スパコンの負荷、コストの低減はもとより、火山噴火や地震予知、津波予測、大気汚染（黄砂、**PM2.5**、花粉飛散等）の警報など、未然に災害を防止できる可能性が高まります。

従いまして、**SRG**のもう**1**つの強みとして、擬似乱数発生装置による流動解析の応用により、スパコンの能力に依存せずに統計（**GDP**デフレーター）、エンジン燃焼などのシミュレーターや空洞実験（高速で走行する列車等で高速時の空力特性を検証するもの）、原子核反応実験などの解析も可能であり、幅広い分野で**SRG**の可能性が期待できるものになります。（※エンターテイメントではバーチャルシミュレーター、アミューズメントではカジノゲーム機全般、オンラインゲームなど。防衛ではサイバーレンジ対策に。）　※レポート**vol.2**以降で様々な角度から技術の可能性を掘り下げます。

## 会社情報 | お問い合わせ

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** |