リアルシス（株）の秘密分散法関連の製品・サービスのご紹介

リアルシス(株)は、ソフトウェア開発、コンサルティング等のサービス事業を中核に据え、その他、情報セキュリティソリューション、SaaS ソリューション、Smart Phone ソリューションを提供するベンチャー企業です。本ニュースレターでは、リアルシス(株)の秘密分散法関連の製品・サービスを紹介します。
秘密分散法は、暗号鍵を使わない暗号方式であり、情報の秘匿方式の一種です。暗号方式とは異なる特徴を有し、様々な応用の可能性を秘めています。リアルシス(株)では AONT 秘密分散方式の実装を行い、そのライブラリ形式での提供、応用したバックアップシステムや文書保管・閲覧システムのサービスの提供、それらのシステムを構成するソフトウェアそのものの提供を、実施中です。現時点で提供中のライブラリ、サービス、ソフトウェアは以下の通りです。

① ライブラリ

＊ 対応 OS：Windows、Linux、iOS

＊ 対応言語：C/C++

なお、Android 対応および JAVA 版は開発中です。

また、リアルシス(株)では、各社の応用システム・製品・サービスへの組込み業務も、請け負っています。

② サービス

＊ TRUSTAS（秘密分散技術を利用した安全な分散バックアップサービス）

特徴は以下の通り。

- バックアップデータの自動取得
- バックアップデータのハッシュ値による改ざん検知
- 秘密分散処理による情報漏洩対策
- データの分散化による安全管理
- データの情報管理と保管状態管理によるデータの長期保管への対応
- 災害・人災によるデータ消失への対応
- 大災害と局地的災害への対応

＊ TRUSTAS フレーム（秘密分散技術を利用した安全な文書保管・閲覧サービス）

特徴は以下の通り

- オフイススペースの有効利用促進（収納場所に関わるコスト削減）
- 文書閲覧時間の短縮（キーワード検索、分散拠点からの利用）
- 不正アクセスへの安全性確保
- 災害発生時の事業継続性確保

③ ソフトウェア

＊ TRUSTAS および TRUSTAS フレームを構成するソフトウェア群

提供されたソフトウェアを利用し新たなシステムの構築、既存システムとの統合が可能で、構築されたシステムによる事業展開も可能です。

また、リアルシス(株)では、システム構築業務も請け負っています。

秘密分散法の実用的実装であるリアルシス(株)の秘密分散ライブラリやその応用サービス、ソフトウェアは、今後幅広い分野で活用されることが期待されますし、新たなサービスやソフトウェアの開発時にも、差別化機能として組み込まれ活用されることが期待されます。

リアルシス(株)が提供中の秘密分散技術ライブラリ、その応用サービス、応用ソフトウェアや、リアルシス(株)が展開中のソフトウェア開発業務受託等にご関心をお持ちの方は、当社までご連絡ください。

(株)IT 企画　Mail：info@advanced-it.co.jp

電話：090-2310-8920

URL：http://www.advanced-it.co.jp/

＜リアルシス(株)の秘密分散方式とは＞

秘密分散法とは、RSA 暗号生みの親の一人であるシャミア博士が 1979 年に考案した、公開鍵暗号方式の「秘密鍵」を安全に保管するために考えられた「鍵を使わない暗号方式」です。一定数以上の分散化されたデータを用いない限り、元のデータに関する一切の情報を得ることができない方式です。この方式は、電子認証局の秘密鍵バックアップのような秘匿性の高い用途に使われてきましたが、分散化されたデータの総量が元のデータの数倍になり、ファイルなどの大きなデータへの適用には課題がありました。

この欠点を克服した方式が、AONT (All-or-Nothing Translation) と呼ばれる方式で、RSA 暗号のもう一人の生みの親であるリベスト博士が概念を考案したデータの変換方式です。AONT の適用により、元のデータはほぼ同じ大きさのデータに変換され、変換されたデータを複数のデータに分割し分散化すると、分散化されたデータが全てそろわないと元のデータを復元できないという性質を持っています。これが基本 AONT 秘密分散法です。

なお、災害や障害により一定範囲の分散化されたデータを喪失した場合でも、残りの分散化されたデータで元のデータを復元可能な方式も実現可能で、これが耐障害性 AONT 秘密分散法です。

トラステッドソリューションズ(株)では、セキュリティレベルを落とすことなく AONT の実装に成功しました。リアルシス(株)では、その成果を引き継ぎ、発展させつつ、その実用化を展開しています。なお、本技術の一部は、花岡悟一郎氏（博士(工学)、産業技術総合研究所情報セキュリティ研究センター研究員）の指導をうけて開発がなされました。

以上