

「創造の芽」

研究シーズ情報



株式会社アドテックシステムサイエンス カオス・ニューラルネットワークを利用した、 世界最高レベルの堅牢性と高速性を持つ セキュリティ保護装置の開発

1. はじめに

株式会社アドテックシステムサイエンスは、花巻市に工場と研究開発のための R&D センターを置く、コンピュータ関連機器の開発・製造・販売を行っている会社です。

この装置は、岩手大学・吉田等明先生、中西貴裕先生、石巻専修大学・川村暁先生の持つ暗号化技術をベースに、当社が製品化を行ったものです。（平成 12 年度の RSP 事業育成試験、平成 16 年度の夢県土いわて戦略的研究推進事業を活用）

本装置は、当社製 CF カードリーダーライタ（AMI-410CF）に暗号化エンジンを搭載したものです。データ書き込みの際に暗号化を行いますので、万が一カードを紛失した際にも第三者にその内容を読み取られる（解読）ことはありません。

カードの内容を読み込む際は、暗号化されたデータを元に戻す復号化を行います。その際には SD カード等記憶媒体によるパスワード照合や指紋等による生体認証（オプション）による確認を行います。

2. 装置の概要

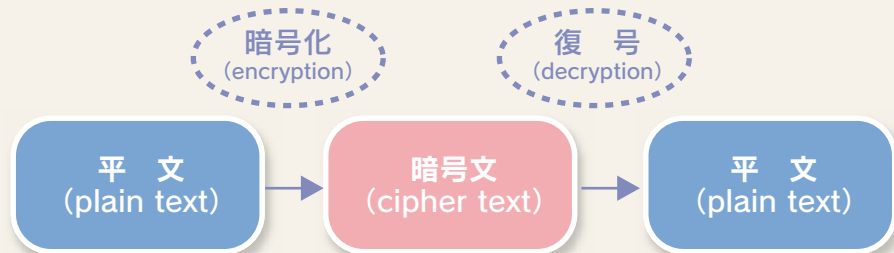
近年情報通信技術の発達により、企業の機密情報や個人情報漏洩するリスクが高まっており、この情報漏洩を防ぐ手法の 1 つがデータの暗号化です。

キーとなる暗号化技術には、世界最高レベルの堅牢性と高速性を持つ、カオス・ニューラルネットワーク（CNN）を利用した独自の暗号化エンジンを採用し、業界標準の DES や RIJNDAEL を凌ぐ高い信頼性を持っています。



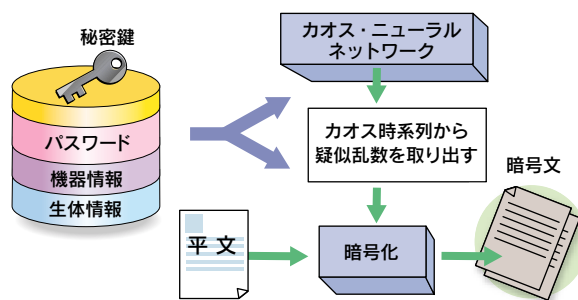
AMI-410CF

暗 号
暗 号：情報の意味が当事者以外にはわからないように情報を変換すること

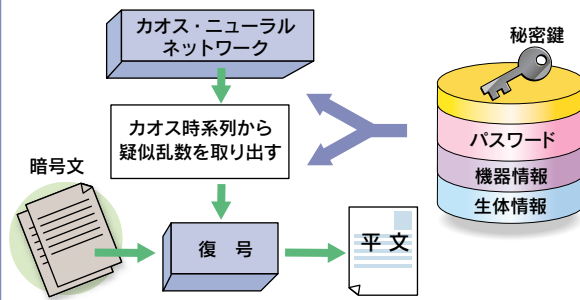


・データ秘匿には、この例では共通鍵暗号（暗号化鍵・復号鍵が同一）が用いられる。

暗号化の仕組み



復号の仕組み



暗号強度評価の結果（例）

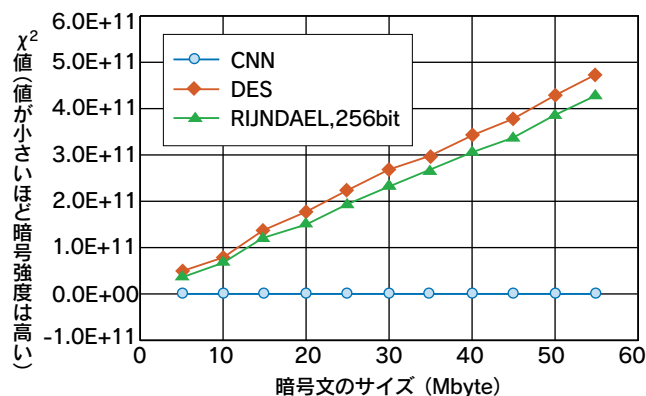
累加 χ^2 乗の法則とは、暗号文中の文字出現頻度にどれだけ暗号系特有の偏りがあるかを検定するものである。暗号文に偏りがあると、その情報を元に解読される危険性がある。

「累加 χ^2 乗の法則が成立しないカオス・ニューラルネットワークを用いた暗号系（CNN Cipher）は、最も安全性が高い」

〈実験環境〉

CPU: Alpha 21164A

OS : Red Hat Linux 5.2



本装置は記憶媒体として一般的な CF カードを使用しているため、PDA 等携帯端末の連携を意識しており、PDA で暗号化したデータをリーダー側で復号する、またはリーダーで暗号化したデータを PDA 側で復号する等も可能です。

3. 今後の展望

本開発で得られた暗号化エンジンは、さまざまなプラットフォームへの移植が可能であるため、パソコン上で

のファイル暗号化ソフトや、デバイス化して装置への搭載等も考えられ、さまざまな製品への応用が期待されます。

●お問い合わせ先

株式会社アドテックシステムサイエンス

本社所在地 神奈川県横浜市保土ヶ谷区神戸町 134

YBP ウェストタワー 8F

TEL.045-331-7575

花 巻 工 場 岩手県花巻市二枚橋 1-145-1

TEL.0198-27-4711

URL <http://www.adtek.co.jp/>