報道発表

- NICT発ベンチャー企業が本格的活動を開始
- 平成16年4月5日

独立行政法人情報通信研究機構（以下、NICT。理事長 長尾 真）の情報通信部門主任研究員 梅野健は、４月１日付けでNICTを休職して、平成１５年８月に設立したCRL[注]発ベンチャー第１号である株式会社カオスウェアの代表取締役社長に就任し、ベンチャー企業の経営・研究開発に専念することとなりました。

注：独立行政法人通信総合研究所（CRL）は、平成16年4月1日に放送・通信機構と統合し、新たにNICTが発足した。

梅野健（情報通信部門超高速フォトニックネットワークグループ主任研究員）は、平成１５年８月に、研究成果の実用化・普及を図るため所内ベンチャー起業支援制度(プレベンチャー制度)を活用したCRL発ベンチャー第１号である株式会社カオスウェアを所内に設立、取締役副社長に就任し研究成果活用事業に取り組んできました。
今回、市場の拡大が予想される有線・無線・コンテンツにおけるセキュリティ分野において、より積極的に新規事業を展開し、ベンチャー企業として更なる発展を図るため、休職して（人事院規則１４－１８に基づく無給の研究成果活用型役員兼業休職）、同社の代表取締役社長に就任し、ベンチャー企業の経営・研究開発に専念することとなりました。

このように、独立行政法人の研究者がベンチャー企業の経営に専念するために役員兼業から切り替えて休職して社長に就任するのは本例が初めてです。（他機関の例では、大多数は兼業のまま。過去に、休職して社長に就任したケースが１例あるが（他機関）、現在は他に例が無い。）

＜プレベンチャー制度における主な研究実施成果＞

1. 世界初のカオス暗号チップを開発し、14.85Gbpsという世界最高の暗号化・伝送・復号化スピードにより世界初のHDTV映像のリアルタイム暗号化に成功。

2. 世界最高速ストリーム暗号型カオス暗号VSC(ブイ・エス・シー)を、カオス暗号で初めて仕様公開し、その安全性を世界標準のランダム性評価テストであるNIST800-22の２つの誤りを修正した上で検証し、更に安全性の外部評価を行った。

3. 世界初のカオスCDMAの無線通信実験に成功。

＜連絡先＞

総合企画部　知財・産学連携室
澤田　史武
Tel：042-327-7464
Fax：042-327-6659

<補足資料>

1. 世界最高速カオス暗号VSCの仕様の公開と今後の展開

医療データ等を含む個人情報の保護が大きな社会問題となっている中、データベースシステムの加入者数・データ量に対してスケーラブルなセキュリティ・システムが現在必要とされております。カオス暗号VSCは、その様な大規模データを高速に暗号化することができる技術で、今まで、1秒間に25.6Gbit/secという世界最高速の暗号処理を達成し、世界初のデジタルハイビジョン映像のカオス暗号VSC(ベクター・ストリーム・サイファー)を開発してきました。今般、NICT発ベンチャー企業の株式会社カオスウェアにて、このVSC暗号の更なる普及と標準化を推進するため、128ビット長の鍵を持つVSCの仕様を同社ホームページにて公開し、プレベンチャープロジェクトで行われてたランダム性評価を含む安全性評価を引き継ぐ形で、継続的にメンテナンスすることとなりました。同社は、VSCを活用した製品(VSCシリーズ)を開発中であり、その販売は5月以降を予定しています。今後は、VSC暗号の安全性評価を実施済みのソフトバンク・テクノロジー株式会社(代表取締役:石川憲和)、既にVSCの製品化実績を持つジャパン・インフォメーション・テクノロジー株式会社(代表取締役:石崎利和)、更に他企業にも協力を呼びかけて、VSC公開仕様の安全性に係る継続的な検証を行うと同時に、緊急に対応が必要な個人情報保護システムの大量データ紛失に耐え得るスケーラブルなセキュリティシステムの早期実現を目指していきます。

リンク先:

1. 株式会社カオスウェアホームページ
   http://www.chaosware.com/

2. 128ビットVSC暗号の仕様公開とランダム性評価実施結果
   http://www.chaosware.com/vsc128.pdf

3. AES選定評価及びCRYPTREC評価に用いられてたランダム性評価
   テストNIST SP800-22の2つの誤りの指摘とその修正
   http://xxx.lanl.gov/PS_cache/nlin/pdf/0401/0401040.pdf

4. 世界初デジタルハイビジョン映像(CRL(NICTの前身)の広報ビデオ)のリアルタイム暗号化のデモビデオ(無料ダウンロード可)
   http://www.chaosware.com/HDTVencryption.wmv

2.世界初のカオスCDMA無線通信実験

カオス暗号VSCとは別の事業で、カオスウェアが力を入れているのは、無線LAN、携帯電話等で必要となっている無線通信システムのセキュリティです。その実現のために、現在第三世代移動体通信システムで標準化されたCDMA(符号分割多元接続通信)の方式を更に発展させたカオスCDMAを提案し、開発してきました。このカオスCDMAは、無線通信システムのセキュリティの向上が望めると同時に、第4世代移動体通信で必要な100Mbpsという高速なデータ伝送を実現し、更に既存システムと比較して加入者数を増やすことができるというメリットを有しています。このカオスCDMAに関して、今まで理論的な提案・シミュレーションは行われてきましたが、実際に無線での実験というのは今まで成功したことはなく、その実用性そのものが問題となってきました。
今般、プレベンチャー制度において、世界で初めてカオスCDMAの無線通信実験に成功しました(図2－図4)。

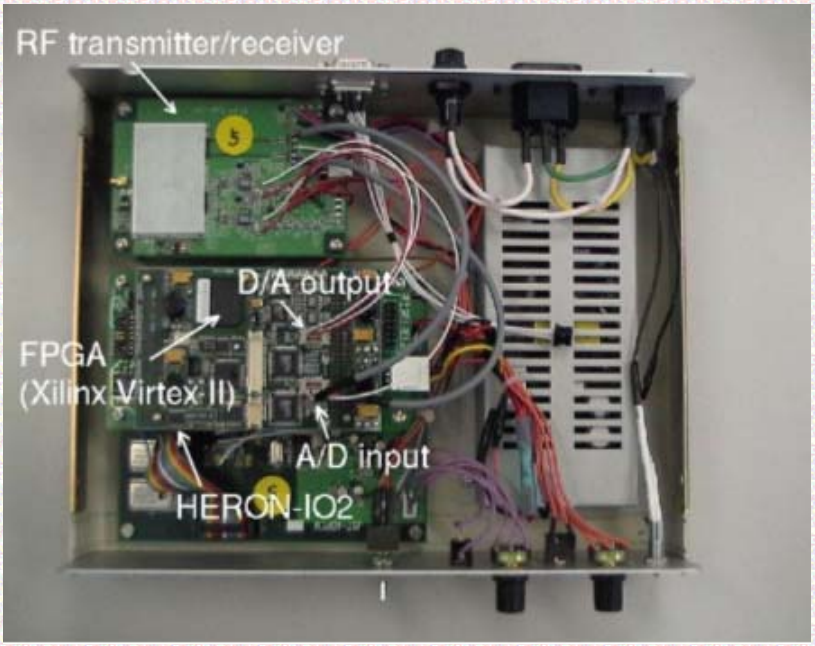

図1. カオスCDMA送受信装置

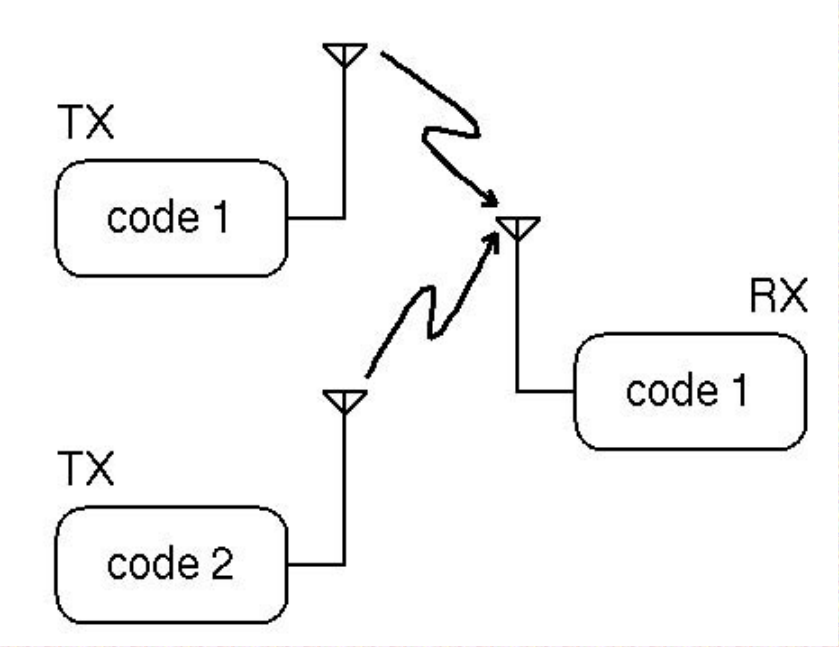

図2. カオスCDMA無線通信実験の概要

図3. カオスCDMAの無線通信実験成功の様子。
様々な外部ノイズがある実環境下での実験。
（NICTにある㈱カオスウェアの研究室内）

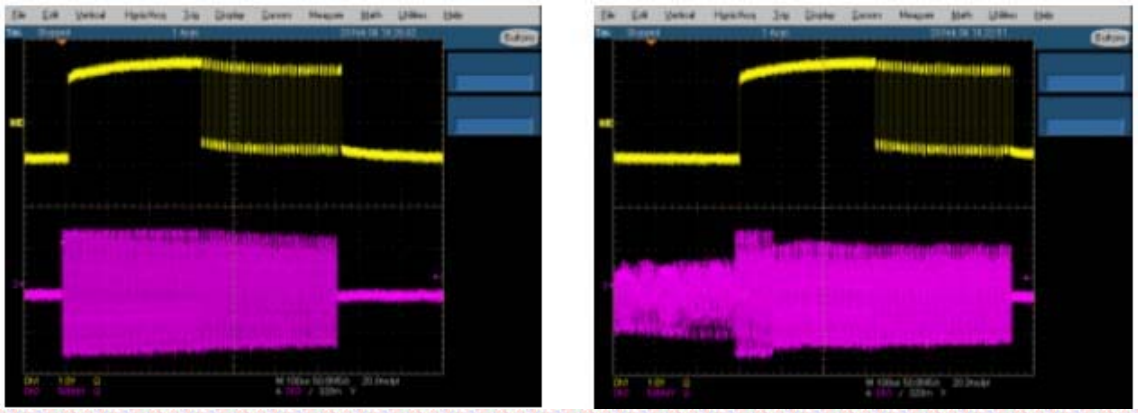

図4. 1ユーザーの時、及び2ユーザーの時の受信信号。各図の上部の信号が同期をとる上で必要な相関値信号と復号されたデータ信号であり、下部の信号が、相関検波する前のカオス拡散により拡散されたベースバンド信号。

なお、本カオスCDMA送受信装置のプロトタイプ試作及びそのカオスウェアでの事業化については、独立行政法人科学技術振興機構(JST)の成果育成プログラムC（カオスCDMAチップ）からも支援を受けました。
今後、カオスウェアにて、カオスCDMAの実用化を進めるのと同時に、カオスCDMAの普及・標準化に力を入れていく予定です。

リンク先：カオスCDMAの多重化技術とセキュリティ技術への展開
http://www.nict.go.jp/kk/e414/101kenpatsu/ronbun/umeno.pdf