報道発表

- **日本-インドネシア間でカオス暗号を用いた長距離衛星通信実験に成功**
- **平成15年11月27日**

通信総合研究所（以下、CRL。理事長 飯田尚志）の所内ベンチャー起業支援制度(プレベンチャー制度)で、実用化を進めているカオス暗号VSC(ブイ・エス・シー。補足資料の関連資料(3)を参照)を使用して、10月27日、CRL、バンドン工科大学（インドネシア）間で、マルチキャスト衛星通信の暗号化・復号化実験に成功しました。

これまでのカオス暗号通信実験が実験室内のものであったのに対し、今回の実験は、既存の衛星通信回線を用いており、カオス暗号による衛星通信の暗号化として世界初、かつ地球上の2局間のカオス暗号通信実験としても世界最長となります。

＜背景＞
ディジタル放送、eラーニングなどの映像コンテンツの配信・流通においては、暗号化による著作権管理とマルチキャストの2つの機能を両立する必要があります。今回の実験は、日本－インドネシア間の衛星回線を用い、ビデオ映像信号の暗号化通信を行いました。更に将来のマルチキャストコンテンツ配信に向け、日本からビデオ映像を暗号化し、衛星に送信して日本、インドネシアの2局で同時受信、及び復号化実験を行いました。

＜本実験の意義＞
CRLでは、カオス暗号VSCのLSIチップ化の研究開発を行い、TV信号のリアルタイム暗号化、デジタルハイビジョン信号のリアルタイム暗号化に成功してきました。このたび、長距離衛星回線用のカオス暗号化ボックスを製作し、総務省のポストパートナーズ・プロジェクトで整備された衛星通信設備を用い、（社）電波産業会の協力のもとに、10月27日、CRL、バンドン工科大学（インドネシア）間で衛星暗号化ユニットを配備し、通信実験を行ったところ、5,000km以上離れた2国間でマルチキャスト衛星通信の暗号化・復号化実験に成功しました。

これは、地球上の2局間のカオス暗号通信実験としては世界最長となります。本実証実験の結果により、衛星回線を利用した長距離VPN（バーチャル・プライベートネットワーク）を今回開発した小型の暗号ボックスを配備することにより容易に実現できることを実証しました。

＜今後の展開＞
来年2月に再び、インドネシアとの日本との間で降雨下でのビット誤り率測定等の更なる精密実験を行い、暗号化による長距離通信の品質への影響を詳細に調べていき、さらに衛星通信用暗号化ユニットの信頼性を高めます。

なお、CRLからVSC暗号の特許ライセンスを受けたCRL発ベンチャー企業、（株）カオスウェア(補足資料の関連資料(2)を参照)にて一般衛星回線用の暗号化ユニットの商品化（製品名：「VSC-SAT」）を今後進め、一般衛星回線用暗号化ボックスVSC-SATとして、同社を販売元、東京エレクトロンデバイス㈱（取締役社長 砂川 俊昭）を代理店として、販売することにより、CRLは、CRL発ベンチャー企業を活用する技術移転を積極的に進めていきます。

＜連絡先＞
企画部研究連携室
五十嵐　喜良　Tel:042-327-7478
澤田　史武　　Tel:042-327-7464
FAX：042-327-6659

＜補足資料＞

＜関連資料＞

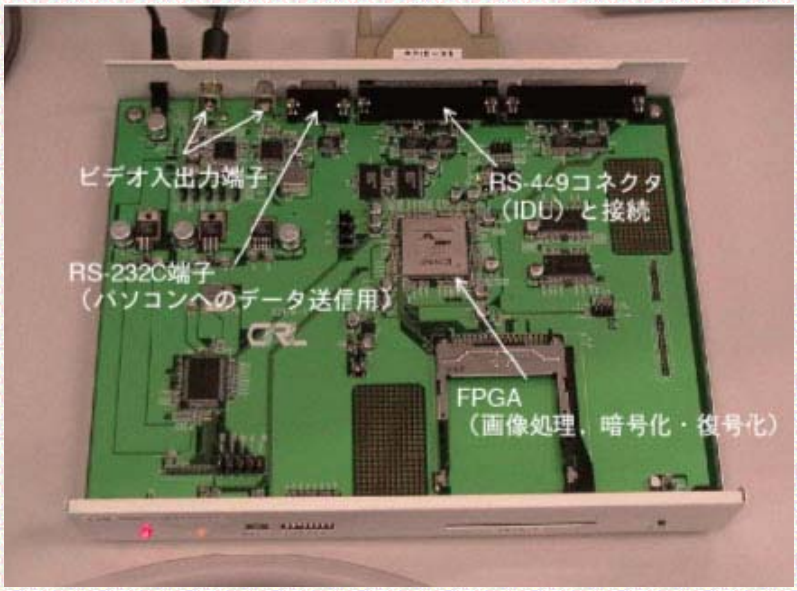
1. 所内ベンチャー支援制度に係る資料
   http://www2.crl.go.jp/kk/e412/CRL_News/0204/frame/002_flame.html

2. CRL発ベンチャー企業（株）カオスウェアに係る資料
   http://www2.crl.go.jp/pub/whatsnew/press/030827/030827.html

3. カオス暗号VSCに係る資料
   http://www2.crl.go.jp/pub/whatsnew/press/030415-1/030415-1.html

＜実験の概要＞

- 実験実施期間：2003年10月27日～29日。
- 東京～ジャカルタ間の距離：約5,800km。
- 実験で用いたユニットの鍵長：56bit（鍵長は可変であり、例えば480bit等に長くすることができる）。
- 今回の実験の衛星回線データレート：全て1,536kbps。
- 暗号鍵と復号鍵が違う場合について：ユニット内に1bitだけ違う鍵を2つ用意し、鍵を切り替えて送受信実験を行い、鍵が違うと正常に復号化できないことを確認した。
- 実験計画の参加施設（予定を含む）
  - 日本：通信総合研究所（CRL），放送教育開発センター（NIME）
  - インドネシア：バンドン工科大学（ITB）
  - フィジー：南太平洋大学（USP）
  - フィリピン：アテネオ・ド・マニラ大学（AdMU）
  - タイ：チェンマイ大学（CMU），キングモンクット工科大学（KMITL）
  - マレーシア：マレーシア科学大学（USM）
- 衛星暗号ユニット：送信、受信とも同じユニットを用い、FPGA内の回路を書き換えることで暗号化／復号化に対応する。A4サイズであり、持ち運びが容易な構造となっている。



＜衛星暗号ユニットについて＞

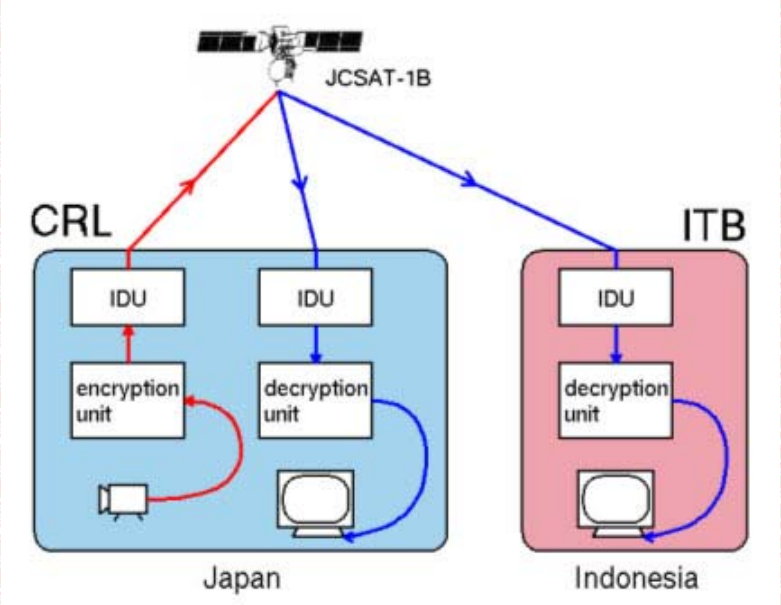
本ユニットは、ビデオ入力信号（NTSC）を暗号化し、衛星回線にて送信を行い、受信側では受信したデータを復号化してモニタに出力する装置です。送信局側では、入力されたビデオ信号をディジタル化し、FPGAチップにてVSC暗号（鍵長＝56bitとしています。）による暗号化を行います。

非圧縮のビデオ信号のデータ量は約200Mbpsですが、今回使用した衛星回線のデータレートは最大で2,048kbpsのため、衛星回線の通信速度に合わせてフレームを削除し、送信するデータ量を減らします（1,536kbpsで送信の場合、約4～5秒に1フレーム送信されます）。データ量を減らした後の暗号化されたデータをRS-449/422ポートを介してIDU注に送り、衛星回線を通じて受信局に送信されます。受信局側では、受信した暗号化されたデータをIDUよりRS-449/422ポートを介して受信し、FPGAにて復号化を行います。復号化されたデータは送信の際にフレームが落とされているため、同じ映像を流し続けることで不足のフレームを加え、ビデオ出力から出力します。

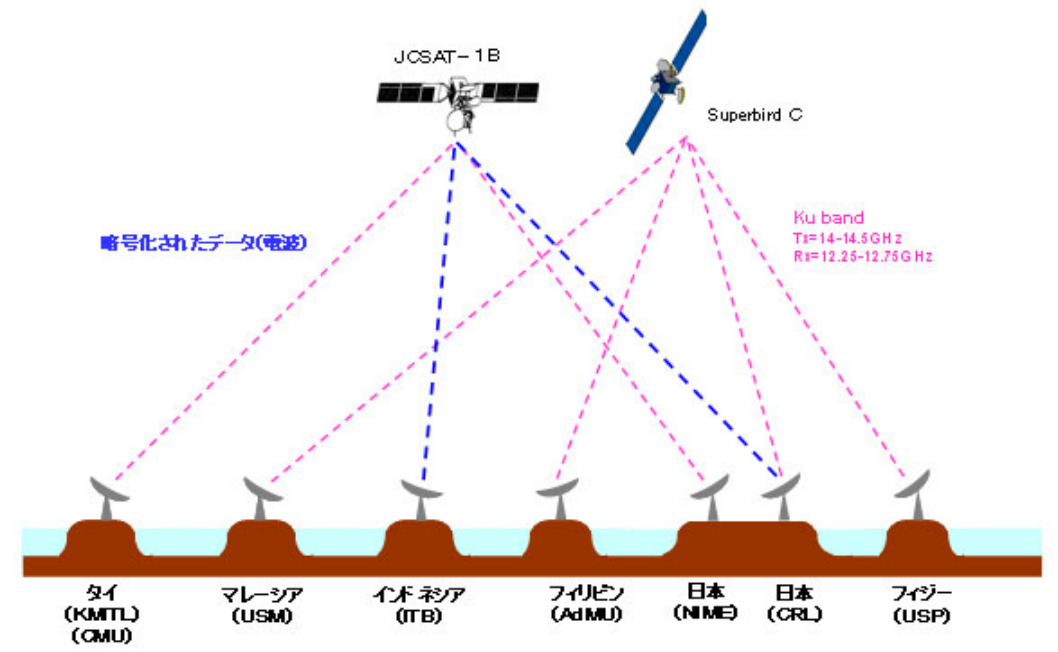
なお、本ユニットは、東京エレクトロンデバイス株式会社の協力により製作されました。

注　IDU：
In-Door Unit の略。地球局はパラボラアンテナ、屋外装置（ODU：Out-Door Unit）、屋内装置（IDU）で構成されている。テレビ会議システム装置や、データ送受信のためのルータなどをIDUに接続して利用する。

- CRLで暗号化し衛星回線にて送信したデータをCRLおよびITBにて受信／復号化を行う実験の概略図。

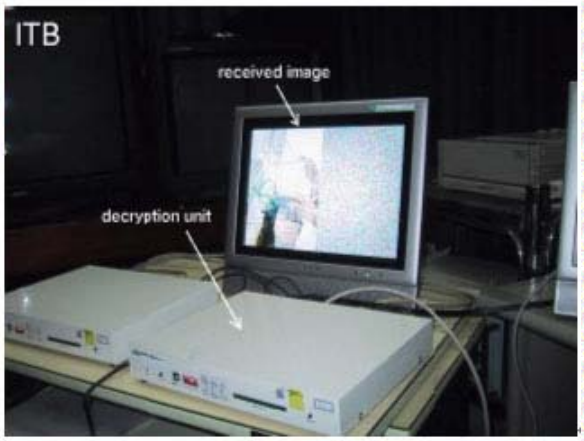


- 国際共同実験ネットワークと今回暗号化実験に使われた回線（青）。



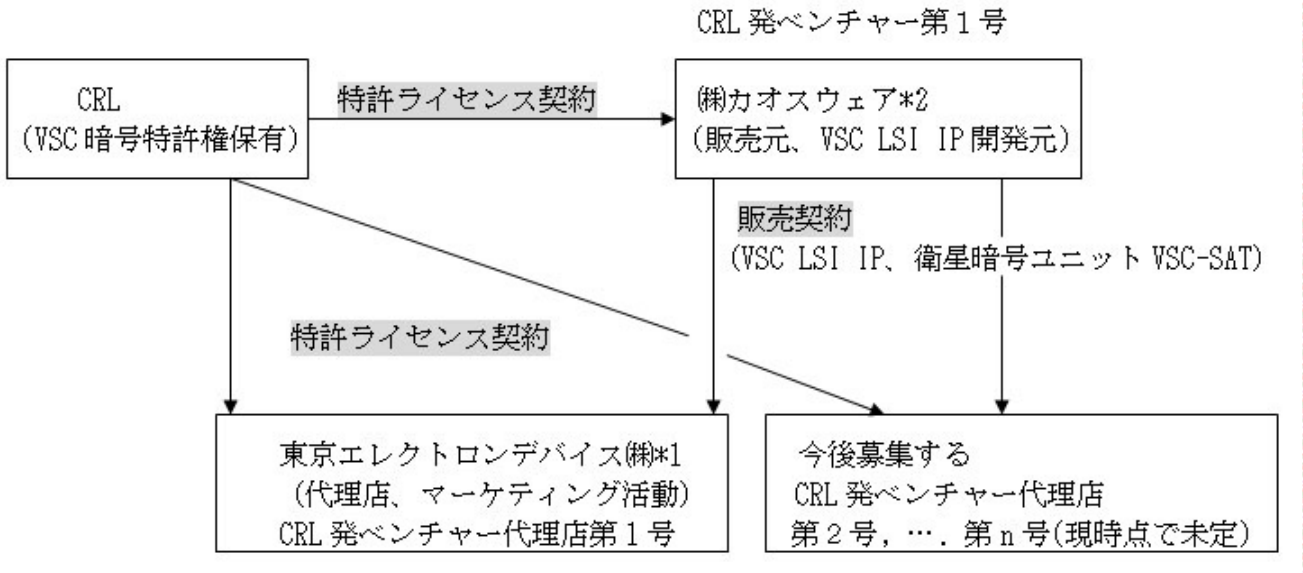
- CRLからCRLとITBへの送受信実験。

  左図はCRL側での様子で、右側のユニットで画面の右半分のみを暗号化しIDUを介して衛星に送信している。右側のモニタは暗号化された状態を映している。衛星より受信した暗号化されたデータはIDUから右側のユニットに送られ、復号化されモニタに出力される。写真では復号化せずに、暗号化された状態そのままを左側のモニタに出力している。CRLから送られた信号は、ITBでも同時に受信されている（右図）。



- CRLにて暗号化し送信し、ITBにて受信した映像。左は暗号化された状態。右は復号化した状態。

●今後の衛星暗号ユニットのCRL発ベンチャーを活用した技術移転の進め方について



注 *1
東京エレクトロン デバイス(株)
横浜市都筑区東方町1番地
取締役社長 砂川 俊昭
＜連絡先＞
総務部 秋永 裕之
Tel:045-474-7000

注 *2
(株)カオスウェア
＜連絡先＞
広報担当係
Tel:042-359-6299
Fax:042-359-6339