

ストリーム暗号 *Enocoro-128v2*

---

## テストベクトル生成ソースコード仕様書

株式会社 日立製作所

2010 年 2 月 2 日

## 目次

1	はじめに	3
2	関数仕様	3
2.1	提供関数 . . . . .	3
2.2	インターフェース . . . . .	3
3	ファイル一覧	4

## 1 はじめに

本ドキュメントは、ストリーム暗号 *Enocoro-128v2* のテストベクトルを生成するためのソースコードの仕様書である。

## 2 関数仕様

### 2.1 提供関数

本プログラムで提供する関数を表 1 に示す。

表 1 提供関数

#	関数名称	機能概要
1	main()	あらかじめ設定された秘密鍵と IV を使って、 <i>Enocoro-128v2</i> のテストベクトルを生成する。

### 2.2 インターフェース

本プログラムで提供する関数のインターフェースを以下に示す。

- (1) 名称 main()
- (2) 機能概要 本関数には、あらかじめテストベクトル生成用の秘密鍵と初期ベクトルが 10 個設定されている。本関数は *Enocoro-128v2* モジュールを呼び出し、テストベクトルを生成する。
- (3) 引数 なし
- (4) 戻り値 なし
- (5) 特記事項 テストベクトルの表示は、標準出力とする。

### 3 ファイル一覧

本プログラムのファイルを表 2 に示す。

表 2 ファイル一覧

#	ファイルタイプ	ファイル名	内容
1	C ソースファイル	test_main.c	テストベクトル生成