# CRYPTRECワークショップ
# ランプセッション用
# プレゼンテーション


ジェーシーエヌ株式会社
2002年1月28日

# TAO　TIME　認知アルゴリズムにおけるPRN生成手順

STEP<1>

**独自の論理クロック採用**

**送受信イベント値のユニークコード化**

**任意の乱数発生装置を利用**
eg；RAND()関数 or Others

STEP<2>

TAO　TIME　**独自のPRN生成**
（**ネット上に露出するTAOデータ情報**…cS、V_STIME、X_cR、X）
※PRN生成パラメータとして使用

STEP<3>

**識別子としてのPRN**
**C(n)とS(n-1)**

**判断子としてのPRN**
**仮C(n)と仮S(n-1)**

# C(n)＆S(n-1)と仮C(n)＆仮S(n-1)の生成式

Client識別子・・・・・・・・・Client側で生成してServerに送信。

$$C(n) = S(n-1) - \{cS(n-1) - cR(n-2)\}$$

※正規クライアント以外は、S(n-1)とcS(n-1)とcR(n-2)の値を推測しなければならない。
そのためには、RANDによって生成される、a(n-1)とX(n-2)、もしくはa(n-2)の値を推測しなければならない。

Client判断子・・・・・・・・・Server側で生成してC(n)と照合して認知

$$仮C(n) = \langle C(n-1) + \{ sR(n-1) - sR(n-2) \} \rangle - \{cS(n-1) - cR(n-2)\}$$

※サーバの側には、a( )の値を生成するための、いかなる暗号生成テーブルも存在しない、
また、Seed値はアクセスごとに毎回、変化し、Seed値の共有化もなされない。

Server識別子・・・・・・・・・Server側で生成してClientに送信。

$$S(n-1) = C(n-1) + \{sR(n-1) - sR(n-2)\}$$

Server判断子・・・・・・・・・Client側で生成してS(n-1)と照合して認知。

$$仮S(n-1) = C(n) + \{ cS(n-1) - cR(n-2) \}$$

# CRYPTREC委員会の皆様への要望

1．着目点a(n)に対する認識の相違について。

・TAO　TIME認知アルゴリズムにおける評価対象PRNの
着目点を、C(n)＆S(n-1)と、仮C(n)＆仮S(n-1)にして頂きたい。

＜理由　1＞

・仮C(n)＆仮S(n-1) をサーバ側で生成するためには、
クライアント側で生成されるa(n-2)とa(n-1)の値が必要となる。

・a(n-2)と、a(n-1)の値を割り出すためには、クライアント側で生成された、
過去2世代に渡ってのcS(n-2)＆cR(n-2)とcS(n-1)＆cR(n-1)の値を、
クライアントの認知許諾の元に入手しなければならない。

＜理由　2＞

・サーバ側には、いかなるa( )を生成するための共通暗号テーブルも、
Seed値も存在しない。

2．従って、「安全性にも問題がある」という記述個所については、
客観的な根拠を提示していただきたい。