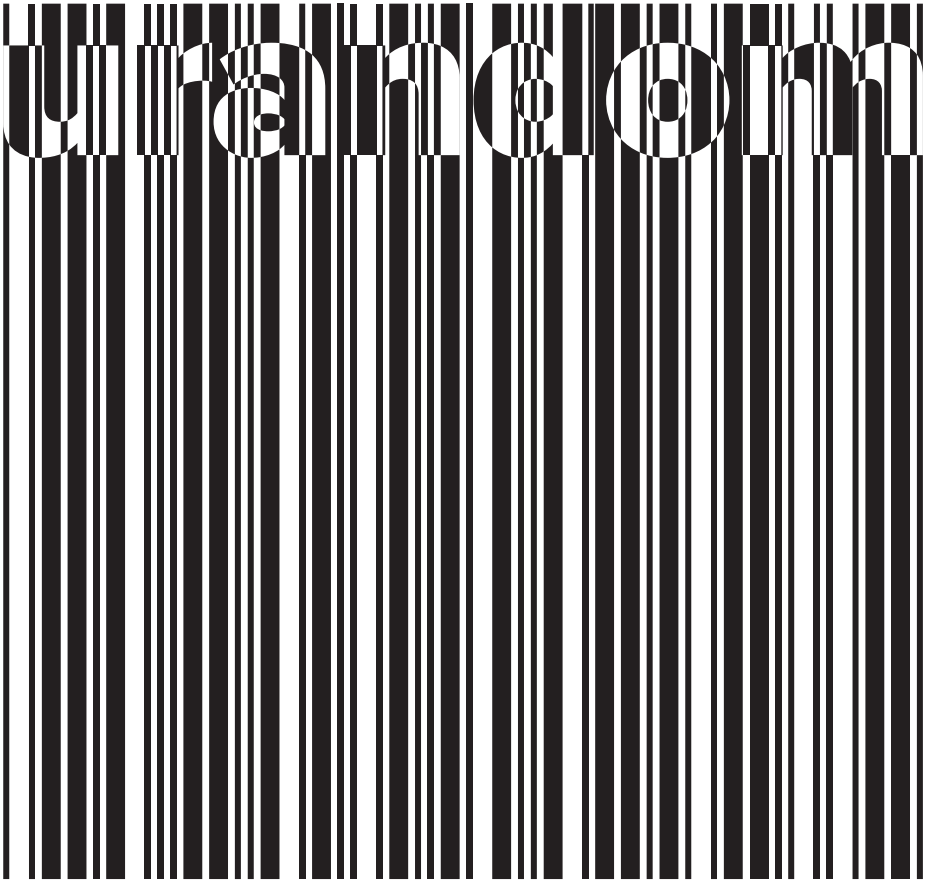

urandom vol.2

バイナリの調べ方 – *op*

Mental Game! – *yyu*

目次

1
バイナリの調べ方

1　はじめに

CTF、フォレンジック、あるいはリバースエンジニアリングの作業中に、正体不明のバイナリデータが時たま出土します。正体不明のバイナリとは、具体的にはメモリダンプや二次記憶から回収したデータ断片あるいは組み込み機器のファームウェアイメージ等で、フォーマットが明らかでないものを意図しています。そのような作業の最終目的は回収したバイナリから何かしらの情報を読み取ることですが、その為にはまず目の前のバイナリが「何のフォーマット」になっていて、その中に「何が」格納されているのかを知らなくてはなりません。ヘッダーやメタデータから素性が明らかになればいいのですが、そのバイナリが独自フォーマットや暗号文の場合にはそうもいきません。そのような場合、詳細な解析に入る前にまずバイナリについての「手がかり」を見つけるステップが必要になります。本稿ではこの最初の「手がかりをバイナリに見出す」ステップについて、暗号文、画像、音声、また機械語コードを取り上げて筆者なりにまとめたものを記します。

2　解析の前に

解析対象のバイナリが既によく知られているフォーマットのファイルならば、わざわざ時間をかけて手がかりを探す必要はありません。既存の知識に乗っかれるからで

図 6: 音声 1 のビットマップ表示 (一部切り出し、Width 128、8bit color)

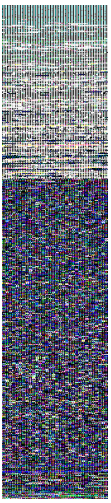

図 7: 音声 2 のビットマップ表示 (一部切り出し、Width 128、8bit color)

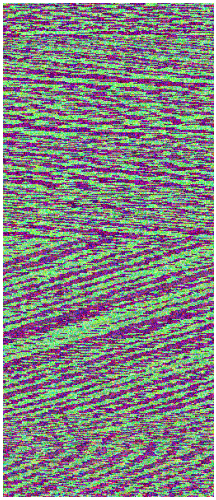

図 8: 音声 1 のビットマップ表示 (一部切り出し、Width 256、32bit color)

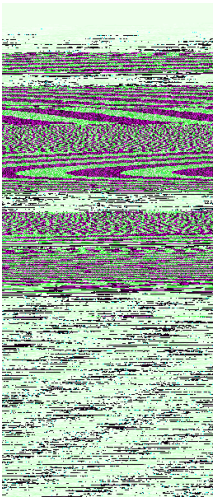

図 9: 音声 2 のビットマップ表示 (一部切り出し、Width 256、32bit color)

2
Mental Game！

1　はじめに

巷では NEW GAME ！というマンガ・アニメが流行っています。ゲーム会社に新卒で入社した主人公の涼風青葉（すずかぜあおば）くんが、他の社員と共にゲームを制作する日々などを描いた作品です。しかし、彼女たちが一体どのような理論に基づくゲームを作っているのか、という疑問に答えられるでしょうか。実は、彼女たちは本稿で紹介する伝統的でかつ画期的である *“Mental Game”* という理論に基いたゲームを制作しているのです。Mental Game とは一体どのようなものなのか、本稿ではそれを紹介します。

2　従来のゲームの課題

Mental Game とは何かを紹介する前に、まずは従来のゲームにある課題を共有しましょう。ゲームはさまざまな分類ができますが、その分類の一つとして次のような分類があります。

- 完全情報ゲーム
- 不完全情報ゲーム

この二つの違いについてはすでに知っている方も多いと思いますが、前者の完全情報ゲームとはゲームのすべての意思決定点において、これまでにとられた行動や実現

となると涼風くんたちは完全情報ゲームを作っているのでしょうか。いえ、彼女たちは暗号理論に基づく非常に洗練された手段——Mental Game を用いて、不完全情報ゲームから審判を排除し、かつそれでゲームの公平性を保つことに成功しているのです。

3 直感的な Mental Game

それでは Mental Game とはどのようなものなのでしょうか。Mental Game は 1979 年に Adi Shamir、Ronald L. Rivest そして Leonard M. Adleman により発表された “Mental Poker” が基礎となっています。コンピューターについて詳しい方は、この三人に見覚えがあるのではないでしょうか。この三人は現代で広く用いられている公開鍵暗号 RSA[*3]を開発した三人です。彼らの開発した Mental Poker とは「電話越しに公平なポーカーゲームができるのか？」という問いに答えるものでした。電話越しですから、不誠実なプレイヤーは山札から自分にとって都合のよいカードをドローしたことにするかもしれません。しかし、彼らの Mental Poker は審判を使わずにこのような不誠実な行為を防止できます。

本稿では、Mental Game を次のように定義します。

> “ Mental Game とは、あるゲームから公平な審判を取り除いても、なお公平性を保ち続けるゲームのことである。 ”

つまり、Mental Game とは Mental Poker をポーカー以外にも適用したものを指します。ですが、いきなり Mental Game の説明をするのはやや困難なので、まずは直感的な説明をします。簡単のため、ここではまず鞄と南京錠を使って説明します。

鞄について説明します。ここで言う鞄とは次のような特徴を持つ入れものです。

- 外側からある鞄と他の鞄を区別できない
- 鞄には任意の数の南京錠を取り付けることができる

外側から鞄を区別できないとは、一旦鞄に入れてしまえば中身に何が入っているのかを外から認識できないという特徴です。また、通常の鞄であれば鞄の物理的な制約から取り付けられる南京錠の数に限界がありますが、ここでは簡単のため任意の数の南京錠を取り付けられるものとします。

次に南京錠についておさらいしておきましょう。ここで言う南京錠は鞄に取り付けて使うもので、次のような特徴があります。

[*3] この記事では RSA 暗号の知識は必要ありません。

urandom vol.2

発行者	urandom
表紙デザイン	polamjag
発行日	2016 年 8 月 14 日
バージョン	1.00（2016-07-19 16:47:48+09:00）
連絡先	https://urandom-ctf.github.io/
印刷所	株式会社栄光