

FPGAでパスワードクラックしてみた

2010年度
ソフトウェアセキュリティ組

ψ (プサイ)



A doll with blonde hair and large blue eyes is wearing a green fuzzy hat with two large, round, white eyes with black pupils. She is wearing a light blue and yellow patterned dress. To her right is a yellow wicker basket with a white lace trim. To her left is a book with Japanese text on the cover. The background is a plain, light-colored surface.

じょ しょうかい

A doll with a green fuzzy hat and a yellow basket. The doll has blonde hair and is wearing a blue and yellow patterned dress. The hat has two large, round, white eyes with black pupils. The basket is yellow and has a white lace trim. The background is dark.

2010年 ソフトウェア セキュリティ

@tikal
ledyba.org



A doll with long blonde hair, wearing a blue and yellow patterned dress, sits next to a yellow wicker basket with a white lace trim. The doll wears a green fuzzy hat with two large, round, white eyes. The background is dark. A semi-transparent white box contains the text.

理学部
天文学科
の
はずだった

わあしい



幼 田年

おひなまつり
ひな人形



あかみ



幼 田年

おひなまつり
ひな人形



大好き

大好き





プログラマーが
書けるよ！

やったね
たえちゃん！



A doll with a green fuzzy hat and a floral dress is sitting next to a yellow basket. The doll has large, round eyes and is wearing a blue and yellow floral dress. The basket is made of yellow straw and has a white lace trim. The background is dark. The text is overlaid on a semi-transparent white box.

言語処理系
作ってました



メインペ

<http://saccubus.sourceforge.jp/>

「さきゅばす」公式サイトへようこそ！

案内

メインページ

最近の出来事

ダウンロード

使い方

変換サンプル

コミュニティ・ポータル

ねこまた (ニワン語)

メインページ

開発者向け

開発者ポータル

ソースコード

ビルド方法

ソースの歩き方

さきゅばす関連ページ

ライセンス表示

SourceForge

バグ報告



さきゅばすは、ニコニコ動画の動画を、コメント付きの動画として保存するソフトです。

画面キャプチャソフトなどでは高いスペックのコンピュータが必要で、フレームレートも低く
となく、スムーズに変換する事ができます。

変換にはffmpegを用いており、iPodやPSP向けの動画を作成することも可能です。

最新リリース

投稿者コメントに正式対応し、ニワン語にも一部対応したバージョン2.0β2を公開中です。ダウ

A doll with a green fuzzy hat and a floral dress is sitting next to a yellow basket. The doll has large blue eyes and is wearing a blue and yellow floral dress. The basket is yellow with a white lace trim. The background is dark. The text is overlaid on a semi-transparent white box.

で
本題のはなし
します

A doll with blonde hair and blue eyes is wearing a green fuzzy hat with two large, round, white eyes. She is sitting next to a yellow wicker basket with a white lace trim. In the background, there is a book with Japanese text on the cover. The text on the book includes 'プログラミング' (Programming) and 'システム' (System).

プログラミング キャンプ なので

プログラミング
しました




FPGA

= Field Programmable
Gate Array



A doll with a green fuzzy hat and a yellow basket. The doll has large blue eyes and is wearing a blue and yellow patterned dress. The basket is yellow and woven. The background is dark.


論理回路を
テキストで
記述できる！

A doll with long blonde hair, wearing a light blue and yellow patterned dress, is sitting next to a yellow wicker basket with a white lace trim. The doll is wearing a large, fluffy green hat with two large, round, white eyes. The background is dark. The text is overlaid on a semi-transparent white rectangle.

おうちに
クリーンハウス
が無い君も

A doll with long blonde hair, wearing a green fuzzy hat with three large eyes and a blue and yellow patterned dress, is sitting next to a yellow wicker basket with a white lace trim. The background is dark. A semi-transparent white box is overlaid on the image, containing the text.

C++とか
分からない
君も

A doll with a green fuzzy hat featuring two large, round, blue eyes. The doll has blonde hair and is wearing a blue and yellow patterned dress. To the right of the doll is a yellow woven basket with a white lace trim. The background is dark. The text is overlaid on a semi-transparent white rectangle.

機械で！
自動で！
計算できる！



で

ホームページ ビルダー



A doll with a green fuzzy hat and a floral dress is sitting next to a yellow basket. The doll has large blue eyes and is wearing a light blue and yellow floral dress. The basket is yellow with a white lace trim. The background is dark. The text is overlaid on a semi-transparent white box.

「パスワード付き ページ」

ブルートフォース アタック





```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html lang="ja">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=Shift_JIS">
<meta http-equiv="Content-Style-Type" content="text/css">
<title>パスワードリンクの例</title>
<script language="JavaScript" charset="Shift_JIS" src="CheckPassword80.js"></script></head>
<body>
<p><a href="http://google.co.jp" onclick="return _HpbPwdWnd(this, 'ciY`JWeqUV[bEXC`_');">次のページ</a>を見るにはパスワードを入力してください。
</div>
<script type="text/javascript"><!--
var _JustAnalyticsConfig = {
  'siteid': '1373',
  'domain': 'hpbuilder.net',
  'path': '/'
};
// -->
</script><script type="text/javascript" src="http://tracker.kantan-access.com/js/ja.js"></script><noscript><img alt="Google Analytics tracking code" data-bbox="10 680 100 710" style="display:none" />
</html>
```



```
return _HpbPwdWnd(this, 'ciY`JWeqUV[bEXC`_');"
```



ciY`JWeqUV[bEXC`_

を、所定の
アルゴリズムで復号



A doll with a green fuzzy hat and a floral dress is sitting next to a yellow basket. The doll has large blue eyes and is wearing a light blue and yellow floral dress. The basket is yellow and has a white lace trim. The background is dark.

ciY`JWeqUV[bEXC`_



usushio.htmlakari

A doll with a green fuzzy hat and a yellow basket. The doll has blonde hair and is wearing a blue and yellow patterned dress. The basket is yellow and has a white lace trim. The background is dark.

復号先の文字同士で
依存性が無い



並列で復号可能

ciY`JWegqUVIpbEXC`_

一文字分の復号

一文字分の復号器

一文字分の復号器

一文字分の復号器

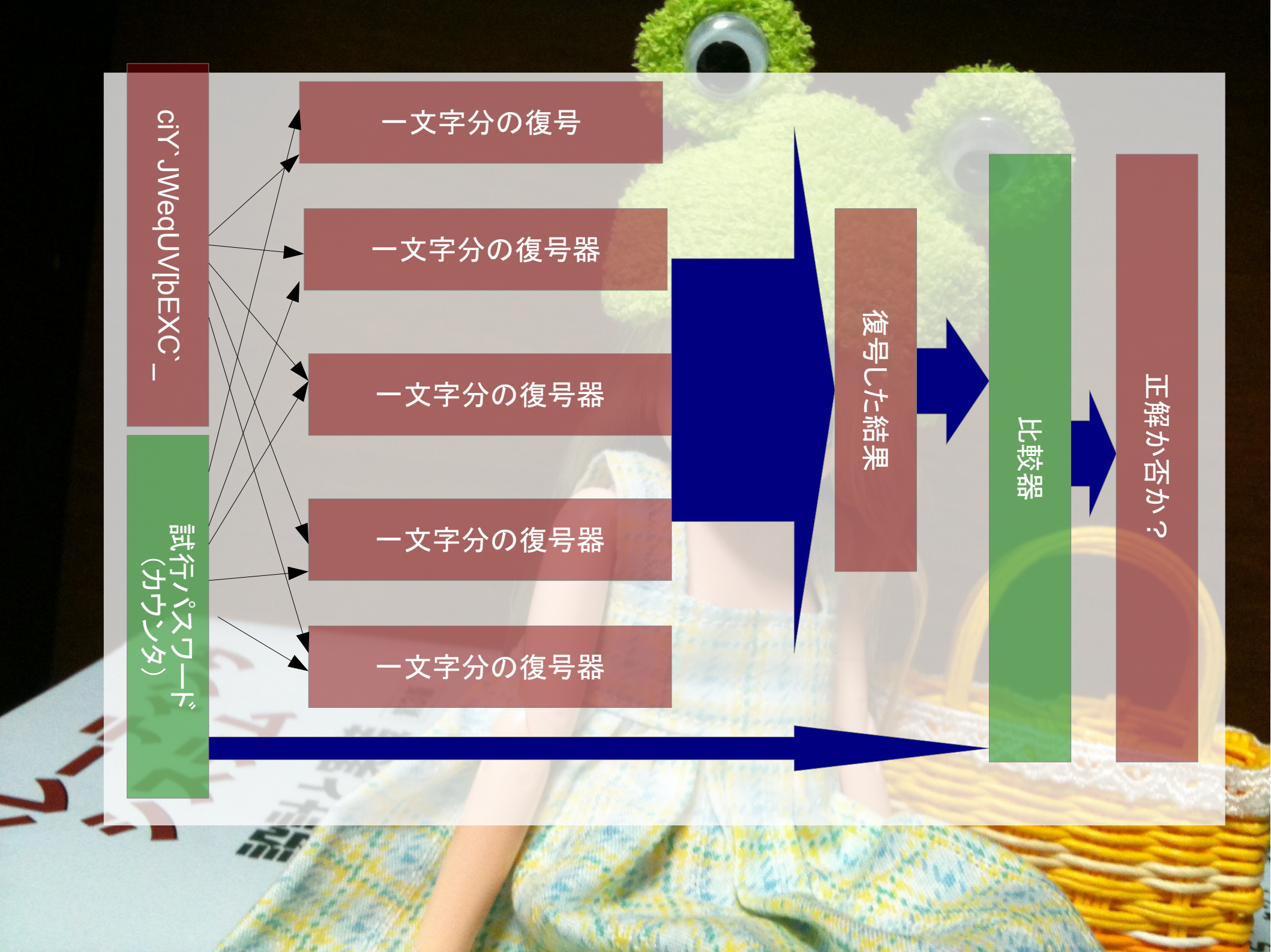
一文字分の復号器

試行パスワード
(カウンタ)

復号した結果

比較器

正解か否か?



A doll with large blue eyes and a green fuzzy hat with two large eyes on top. The doll is wearing a blue and yellow patterned dress and is sitting next to a yellow wicker basket. The background is dark. The text is overlaid on a semi-transparent white box.

試行文字列

クロック信号で
一つ繰り上がる

1 パスワード あたり



A doll with a large, fluffy green hat featuring two large, round, white eyes. The doll has blonde hair and is wearing a light blue and yellow floral dress. It is sitting next to a yellow woven basket with a white lace trim. The background is a plain, light-colored surface.

1 クロックで
探索可能

A doll with a green fuzzy hat featuring two large eyes, wearing a blue and yellow floral dress, is sitting next to a yellow wicker basket with a white lace trim. The doll is positioned in the center of the frame. The background is dark, and the doll is sitting on a light-colored surface with some text visible.

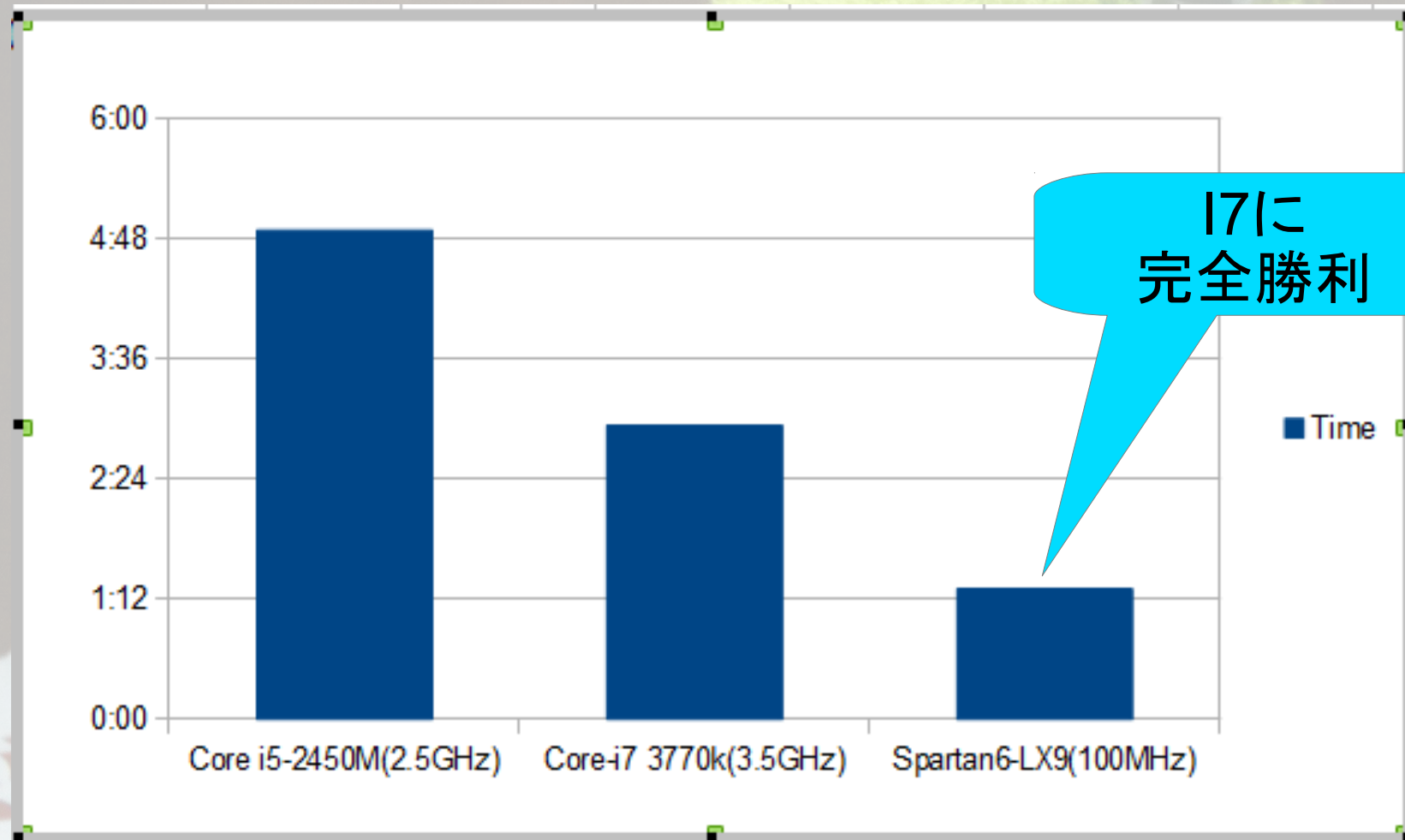
— 人 人 人 人 人 —
> 嬉しい <
— ^ Y ^ Y ^ Y ^ —

A doll with a green fuzzy hat and a floral dress is sitting next to a yellow basket. The doll has large blue eyes and long blonde hair. The hat has three large, round, white eyes. The dress is light blue with yellow and green floral patterns. The basket is yellow with a white lace trim. The background is a plain, light-colored surface.

ぱほーまんす 測定

単純に時間



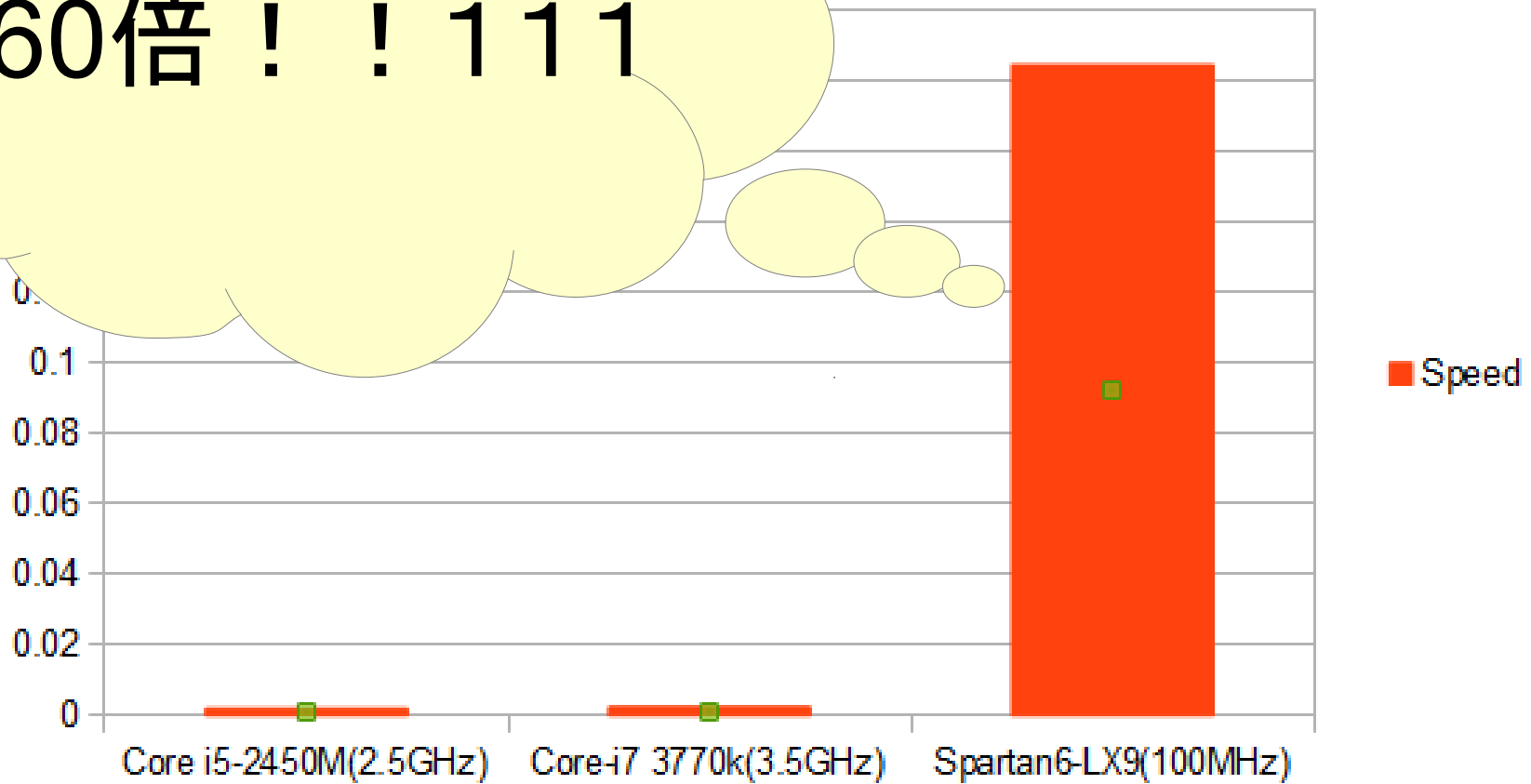


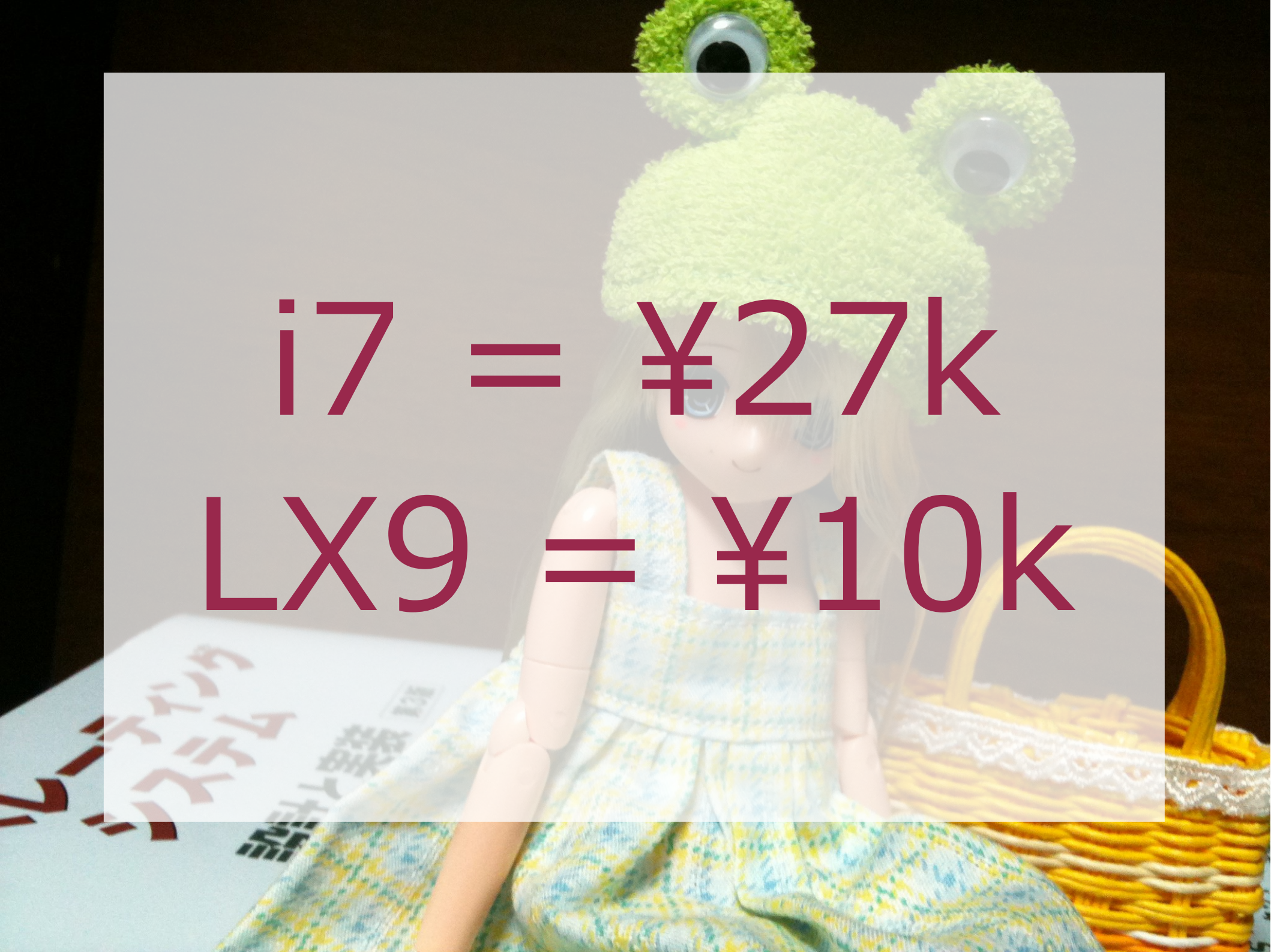
17に
完全勝利

クロック数あたり



60倍！！111



A doll with a green fuzzy hat and a floral dress is sitting next to a yellow basket. The doll has large blue eyes and is wearing a blue and yellow floral dress. The basket is yellow with a white lace trim. The background is dark.

i7 = ¥27k
LX9 = ¥10k


A doll with a large, fluffy green hat featuring two large, round, white eyes with black pupils. The doll has blonde hair and is wearing a light blue and yellow floral dress. It is sitting next to a yellow wicker basket with a white lace trim. The background is a plain, light-colored surface.

コスパ =
約180倍

消費電力

i7 => 77w

LX9 => 0.15w

A doll with a green fuzzy hat and a yellow basket. The doll is wearing a blue and yellow patterned dress. The background is dark. The text is overlaid on a semi-transparent white box.

しかもまだまだ
回路規模に
余裕がある

でも調べてみたら

グランド
システム
雑誌



A doll with long blonde hair, wearing a blue and yellow patterned dress, sits next to a yellow wicker basket with a white lace trim. The doll's hat is a large, fuzzy green shape with two large, round, blue eyes. The background is dark. A semi-transparent white box with Japanese text is overlaid on the image.

akari
だけでなく
akaqj
も通る

A doll with a green fuzzy hat and a yellow basket. The doll has large blue eyes and is wearing a blue and yellow patterned dress. The basket is yellow and woven. The background is dark.

「正解」数

95[^][パスワード
文字/2]

A doll with a green fuzzy hat and a yellow basket. The doll is wearing a blue and yellow patterned dress. The basket is yellow and has a white lace trim. The background is dark.

今回5文字

$95^{[5/2]}$

= 95²個

A doll with a green fuzzy hat and a yellow basket. The doll is wearing a blue and yellow patterned dress. The hat has three large, round, white eyes with black pupils. The basket is yellow and has a white lace trim. The background is dark.

あんまり
意味が無かった
／（^o^）＼

A doll with long blonde hair and blue eyes, wearing a light blue and yellow patterned dress, sits next to a yellow wicker basket with a white lace trim. The doll is wearing a large, green, fuzzy hat with three large, round, white eyes. The background is dark. A semi-transparent white box with red text is overlaid on the image.

処理を早くする前に
アルゴリズム！

A doll with a green fuzzy hat and a yellow basket. The doll has large blue eyes and is wearing a blue and yellow patterned dress. The basket is yellow and woven. The background is dark.

Githubに Verilogあるぽよ

<https://github.com/ledyba/CheckPassword80>