

【洋風及び和風】 キャップ・トリップ

そして、それらの

種類・歴史・算出方式・算法 一覧

フレッド・ブレンナン
(★コピー)

*†

二〇二二年六月二五日
新ジャージー州 大西洋岸都†

注意：CC表示・改変禁止（BY・ND）4.0国際ライセンスの下で利用可能です。

* メール：<copypaste@kittens.ph>

※ コンピュータ組版、デジタル字体、フォント・フォーマット（OTFとTTF専）などの国際的な専門家

※ 匿名巨大掲示板（和・際・米）ネット文化などの国際的専門家

※ 日本語、エスペラント語、スペイン語、タガログ語、英語を喋れる人

※ 最終に、8ちゃんねる創設者

† もう頑なにならずウィキで僕の名前を正しく表記してくれよ

‡ 見つからないの場合は、勇気のない人は「Atlantic City」と「アトランティック・シティ」を書いている。そんな人たちは違って、糸の玉はおおきい。

目次

一	2ちゃんねるトリップ【◆・◇】	2
1	洋風トリップとは何？	2
2	2ちゃんねる風トリップ	3
a	★FOXのパール・スク립ト	3
1	★コピーの（一行一行）注釈付き版	3
b	技術分析	6
二	2ちゃんねる風キャップ【★】	7
3	2ちゃんねるキャップとは何？	7
三	次世代和風トリップ【◆】	8
4	2ちゃんねるSC風トリップ【#&】、12桁トリップ【&】、生キー【##】など	9
四	国際風キャップ	10
五	洋風トリップ【#】	10
5	いわゆる「セキュア」（安全な）トリップ【##】	10
六	付録等	12
A	NPO法人CC・BY・NDライセンスについて	12

一 2ちゃんねるトリップ【◆・◇】

1 洋風トリップとは何？

洋風トリップ（替名…トリップ（1）・トリップコード（2）米国風トリップ／国際風トリップ・トリップコード）とは、4chan（4ちゃん、四つ葉ちゃんねる）や 8chan（8ch、8ちゃんねる、ワトキンズ組盗品名…8君・8^{kun}）などの匿名巨大掲示板に於いて、投稿（すなわちカキコ）時にユーザー名横に表示される文字列と数字のこと。

この文字列の生成方法には様々なものがあり、生成方法は利用者と管理者の双方に微妙な影響を与えます。

ここでは、主なトリップコードの生成方法について簡単にお話しします。

- (1) 英語 trip
- (2) 英語 tripcode

2 2ちゃんねる風トリップ

洋風のトリップを説明する前に、「和風」トリップ⁽³⁾の機能を再確認しておく必要があります。
現在でも国際的に最も広く使われているトリップ生成の方法は、**2ちゃんねる**の初期のプログラマー、**★FOX** なかにょしひろ (中尾佳宏) が書いた次のスクリプトに基づいています。

a ★FOXの^{P_e_r_l}パール・スクリプト

```
$tripkey = "#istrip"; # トリップキー文字列 (#付き)
$tripkey = substr $tripkey, 1;
$salt = substr $tripkey . "H.", 1, 2;
$salt =~ s/[^\.-z]/\./g;
$salt =~ tr/::<=>?@[\\]~/A-Ga-f/;
$trip = crypt $tripkey, $salt;
$trip = substr $trip, -10;
$trip = "◆" . $trip;
print $trip, "\n";
# $
```

3

もし、★FOXのコードを説明する欲しい人があ、以下の一行一行を注釈付きのパール・スクリプトを⁽³⁾覧ください。

1 ★コピペの(一行一行)注釈付き版

```
#!/usr/bin/perl
# 2ちゃんねる掲示板風トリップ取得 (★コピペの注釈付き版) .pl
# (2ch_tripcode_annotated_ja.pl)
#
# © 2020年〜2022年 フレドリック R ブレンナン
#
# ★FOX (中尾嘉宏) の公開ドメインコードを基にしています。
# これも公開ドメインコードである。
```

```
# トリップキーを標準入力から取得する
$tripkey = <STDIN>;
chomp $tripkey;
```

(3) トリップの元祖にはかなり無粋な言葉なので、減多に本書では曖昧さをなくすためにのみ使用。減多にするべき言葉。

```

if (substr($stripkey, 0, 1) ne "#") {
    print STDERR "トリップキーは#で始まる必要があります" && exit 1
};
# 「#」削除
$stripkey = substr $stripkey, 1;

#### ソルト生成 ####
# パスワードから2文字目と3文字目をソルトとして使用する。
# 例:「salt」から「st」を生成。
$salt = substr $stripkey . "H.", 1, 2;
# パスキー範囲外の文字をすべてOX2E（ピリオド）に変換する。
$salt =~ s/[\.\-z]/\./g;
# 2つの文字や ABCDEFGabcdef に置き換える。
# :;<=>?@[_]`_`
# 例えば`#strip`の場合に salt が"st"のもちである。しかし、#:.`の場合に salt が"ef"になる。
$salt =~ tr/::;<=>?@[_]`_`/A-Ga-f/;

```

4

```

print STDERR "注: ソルトが $salt\n";

```

```

#### トリップコードを生成する ####

```

`crypt()`を実行する。これはDESベースの一方方向ハッシュである。
 # このパール版では、トリップキーの最初の8文字（!）のみを考慮する。
 \$strip = crypt \$stripkey, \$salt;

```

if (length($stripkey) > 8) {
    my $extra = substr $stripkey, 8;
    my $err = "警告: パスワードは長すぎ。$extra は無視された、ハッシュ結果でない。 \n";
    print STDERR $err;
}

```

```

# ハッシュの最後の10文字を取得する
$strip = substr $strip, -10;

```

```

# 先頭に◆を付ける。4chanでは!が使われる。

```

```

$strip = "◆" . $strip;

# 標準出力に出力する
print STDOUT "トリップ: ", $strip, "\n";

exit 0

```

出力の例え:

```

fred@apache# perl 2ちゃんねる掲示板風トリップ取得 (★コピペの注釈付き版) .pl
#istrip
注: ソルトは st
トリップ: ◆/WG5qp963c
fred@apache# perl 2ちゃんねる掲示板風トリップ取得 (★コピペの注釈付き版) .pl
#: _
注: ソルトは ef
トリップ: ◆rZgPfAs/mo
fred@apache# perl 2ちゃんねる掲示板風トリップ取得 (★コピペの注釈付き版) .pl
#wakuwaku
注: ソルトは ak
トリップ: ◆tSdCM0v21w
fred@apache# perl 2ちゃんねる掲示板風トリップ取得 (★コピペの注釈付き版) .pl
#wakuwaku``
注: ソルトは ak
警告: パスワードは長すぎ。: は無視された、ハッシュ結果でない。
トリップ: ◆tSdCM0v21w

```

b 技術分析

前節の★FOXの形式は約20年前のものであり、現代のコンピュータはそのトリップを容易に破れる。さらに、トリップの最初の8文字だけが重要で、パールではそれがすべての暗号とみなされるため、さらなる欠陥がある。

一般消費者向けパソコンに搭載されている現代のGPUでは、2ちゃんねる形式のトリップコードは数日で解読できてしまいます。8君のロン・ワトキンスでさえ、これを認めています。

そのため、欧米では2ちゃんねるの枠を超えた、より強力なハッシュようにが求められる。そこから、いわゆる「洋風トリップ」の旅が始まった。

しかし、その旅に出る前に、キャンプの話をしなければなりません。

二 2ちゃんねる風キャップ【★】

3 2ちゃんねるキャップとは何？

元々はトリップコードが解読されやすく、2ちゃんねるのスタッフになりました荒らしが発生したことから考案された暗号の一種。

しかし、これみたいのキャップ型トリップは、「ボランティア」⁽⁴⁾やニュー速板の「レポーター」など、運営とは関係のないユーザーにもどんどん拡大されていった。

掲示板は、たとえ巨大ウェブ掲示板であっても、専用ブラウザ⁽⁵⁾の存在により、技術的にはほとんど変化しないことは、技術志向の高い日本人なら誰でも知っていることである。

ただ、これは欧米ではありえないことだ。欧米では、文字掲示板であれ画像掲示板であれ、掲示板はその利用者向け窓口（フロントエンド）を完全に管理している。まれに非公認の携帯アプリやパソコンアプリが登場すると、急に（非文献化）APIが変更させる。ここには「dat」形式ファイルは存在しないし、4ちゃんと8君のように異なる掲示板間の交換を期待することもできない。

また、氾濫、破壊、荒らしに使われるような「bbs・cgi」も存在しない。

なぜbbs・cgiにそんなことを言うのか？なぜなら、欧米にはBBXやBBQ⁽⁶⁾もないからだ。2016年に2ちゃんねるのテクニカルディレクターになったとき、社内システムのアマリの違いに衝撃を受け、なぜ2ちゃんねるが安全で使えるのかさえ理解するのに時間がかかりました。

その理由を知りたくありませんか？

理由は**人種差別**である。

2ちゃんねるは外国人ユーザーを全て排除しています。

つまり、日本に割り当てられている（比較的）小さなIPアドレス空間のみに関心を持てばよいのです。欧米の掲示板より問題が簡単ことは、残念ながら2ちゃんねるでは、社内手続きやITセキュリティが客観的に悪くなることにつながります。そして、こうした手順の悪化は、より強いハッシュのある新トリップ種類を作るのではなく、管理者以外の人にキャップが渡されることに繋がったのです。

(4) 2ちゃんねるの所謂「ボランティア」は、現実には、スタッフ。少なくとも²⁰¹⁵年時点では全員有給。追伸 所謂「★スライム」の実名は恵菅原。

(5) すなわち、専ブラ

(6) 2つのブラックリスト。

疑問…「人種差別から、キャップ」は本当じゃなくて本当は「外国人荒らしから、キャップ」んだ

いや。賢女★みつをの引用を読もう←

「荒らしだから規制」

これが毎回、ただの運営の都合で規制する時の言い訳。1番の荒らしは運営が飼ってるK5・F9だし」

歴史的に、ひろゆきの管理下でも、つまり²⁰¹⁴年以前でも、大部分の米SPを禁止されている。

初期の2ちゃんねるには、海外の荒らしが書き込んでいたことは間違いないでしょう。自分の記憶では【ニップを荒らす】とは**/b/**のゲームを出った。いわゆるゲームの目的は、2ちゃんねる又はふたば☆ちゃんねるに行っていた、荒らした。ですけども、そのスレの種類では多くの外国人（僕を含め）達が、所謂「ゲーム提案」に嫌悪感を抱いていたことを思い出します。

「2ちゃんねるの管理者達に外国人全員を追放するの口実をやるな！馬鹿」と投稿した。⁽⁷⁾ 仮に荒らしが起きたとしても、差別的な政策であることに変わりはない。最終的にはテック問題が簡単になりすぎてたので、2ちゃんねるのITインフラ・セキュリティに不備が出るようになりました。理由はどうであれれば紛れもない歴史的事実なのだ。

8

三 次世代和風トリップ【◆】

続きの前に、ある問題进行处理しなければならない。トリップコードの分岐の歴史を書いている以上、前に書いた文章はすべて事実であるが、あくまで²⁰¹⁰年時点の話である。

※²⁰¹⁰年頃（日本語版ウィキペディアでは²⁰⁰⁹年とされているが、私には疑うべき理由が残っている）、2ちゃんねるに「12桁トリップコード」と呼ばれる一種のトリップコードが出現した。

※²⁰⁰³年の4ちゃんねる開設から²⁰¹⁰年までの7年間で、欧米がどのように乖離したかについては、すぐに説明するが、簡単に言えば、「12桁トリップコード」、そして、ひろゆきの真2ちゃんねろ⁽⁸⁾トリップコードが、どのように違うかについて説明すればよいだろう。

(7) 結局無駄だったけどね
(8) すなわち、sc、2ch.sc

4 2ちゃんねるSC風トリップ【#\\$】、12桁トリップ【\\$】、生キー【##】など

次世代和風トリップの技術的な詳細を一つ一つ本文で列挙することはず、表で示す←(9)


名前	元サイト	年(約)	ハッシュ方法	入力	出力
生キー	2ちゃんねる	不明	DES	16 桁の十六進数	10 桁の base64
12 桁トリップ	2ちゃんねる	2010	SHA1	≥ 12 桁の SJIS	12 桁の base64
15 桁トリップ	2ちゃんねる.sc	2014	SHA1	≥ 11 桁の SJIS	15 桁の base64
カタカナトリップ(##\$。)	2ちゃんねる.sc	2014	SHA1	≥ 11 桁の SJIS	15 桁の半角カタカナ

(9) SCのトリップは、全ハッシュを使用しない。19ビット目から108ビット目までの90ビットのみ使用。モナトリップ(ジム2ちゃんねるのトリップ)は、先頭64ビットのみ使用。

技術的な詳細は、^{Rust crate}ラスト・クレート [tripcodes](#) を参照してください。

四 国際風キャップ

国際的には、キャップは決まった外観を持たず、掲示板によって異なる。しかし、和風キャップに比べると非常に華やかなものが多いようです。

例えば、8 君のキャップは色を変えます。4 ちゃんでは、ロゴがキャップの目印として使われます (例:  Administrator)。

以前の 8 君では、キャップされた投稿は自動的に GnuPG 署名されたものでありました。ロン ([10](#)) の暗号文旨を考えると、この必要な機能が引退したのは当然です。

海外の掲示板では、巨大掲示板では管理者の投稿は珍しく、熱心なユーザーしか見ることができないことを考えると、色を変えたり、小さなロゴを入れたりといった気を引く機能があることも納得がいきます。したがって「特別なイベント」であるため、気が散るのはこのためだとも言えるでしょう。

五 洋風トリップ【#】

すべての事前情報が説明されたところで、洋風トリップ式の扱いに入ります。通常の洋風トリップは元の 2 ちゃんねると同じなので、再解説はしない。その代わり、日本には存在しない最初のトリップから説明する。

5 いわゆる「セキユア」(安全な)トリップ【##】

スタッフ以外のキャップがないために、トリップコードユーザーのなりすましの問題に直面したとき、それは恐ろしいことだと思われた。

当時、日本ではこのテック問題の進展が見られないため、トリ漏れを逃げるために、4 ちゃんの管理人であるクリストファー・プール氏は、「##」という接頭語を共有しながらも、日本にはない新しいシステムを考案したのである。

セキユア・トリップがいつ導入されたかは不明である。∞ の主要な専門機関 (ビップ・アノン ([11](#)) または彼の大名無し図書館 ([12](#)), ルーミア名無し ([13](#)), よつば史研究会 ([14](#))) はいずれも年表で

(10) 所謂^{CM}

(11) すなわち^{CM} bibanon。意味: 司書アノン

(12) 英語: Bibliotheca Anonoma

(13) 英語: Nameless Rūmia

(14) 英語: Yotsuba Society

その導入について触れていない。

ですけど、絶対にセキュア・トリップは古いことです。2008年で、誰かがこの投稿を書き込んだ…

「A secure tripcode can be generated by placing two octothorpes in the [Name] field, as opposed to one as with a normal tripcode (ex. “User#password”). Secure tripcodes use a secret key file on the server to help obscure their password. The previous example would display “User!iOo43raDVH61” after being posted.^a」

^a 出所：ですアーカイブ、4ちゃん、アニメ板、スレ号 11157921

「通常のトリップが一回に#に対し「セキュア」トリップの方に、【名前】フィールドに2回に#（例：「User#password」）を入力することで生成される。セキュア・トリップは、サーバー上の秘密鍵ファイルを使用して、パスワードをほとんど解読不可能になる。先ほどの例では投稿後に「User!iOo43raDVH61」と表示される。」

つまり、いわゆる安全なトリップは誤用であり、セキュリティはもはやトリップではなく、サーバー、秘密の暗号ソルト、ハッシュ関数にあるのである。

11

これには様々な影響があります。これはいわゆる「Qアノン」で使われているタイプのトリップコードで、私は何年も前にロン・ワトキンスに乗っ取られたと固く信じています。安全なトリップの仕組みにより、少なくとも2022年時点では彼が乗っ取ったという事実が今判明しているのです。なぜわかるのでしょうか？この種のトリップコードの弱点は、たとえば一つのウェブサイトであっても、それが無常であることです。

同じ入力で他のセキュア・トリップコードが変更された場合、すべてのセキュア・トリップコードが無効になり、変更します。

秘密暗号ソルトのトリップは、和風トリップとは異なり、（秘密のソルトは本質的に秘密であるために）セキュア・トリップを検証不可能にするためソルト更新によって掲示板全体のトリップが無効になった後に古いセキュア・トリップが投稿されたことに注目することが改ざんを証明する唯一の方法となる。

六 付録等

本書の転載などライセンスについて

A NPO法人CC・BY・ND ライセンスについて

注意 ※NPO 法人クリエイティブ・コモンズ (CC) 表示 (BY) 改変 (ND) 禁止 4.0 国際ライセンスの下で利用可能です。ライセンス全文の日本語訳は [こちら](#) をご覧ください。以下は、NPO 法人クリエイティブ・コモンズによる法的拘束力のない簡単な要約です。

共有どのようなメディアやフォーマットでも資料を複製したり、再配布できます。

- ・営利目的も含め、どのような目的でも。
- ・あなたがライセンスの条件に従っている限り、許諾者がこれらの自由を取り消すことはできません。

12

あなたの従うべき条件は以下の通りです。

・表示

あなたは適切なクレジットを表示し、ライセンスへのリンクを提供し、変更があったらその旨を示さなければなりません。これらは合理的であればどのような方法で行っても構いませんが、許諾者があなたやあなたの利用行為を支持していると示唆するような方法は除きます。

・改変禁止

あなたがこの資料をリミックスし、改変し、あるいはこの資料をベースに新しい作品を作った場合、あなたは改変された資料を頒布してはなりません。

・追加的な制約は課せません

あなたは、このライセンスが他の者に許諾することを法的に制限するようないかなる法的規定も技術的手段も適用してはなりません。

未所属表明

著者は ※NPO 法人クリエイティブ・コモンズとは一切関係ありません。

印刷物を御覧へ

印刷物の配布・販売などは行っていないですが、ライセンスの全文を取得するためにコンピュータには以下のURLを手動で入力して貰います。⁽¹⁵⁾

⁽¹⁵⁾ <<https://creativecommons.org/licenses/by-nd/4.0/deed.ja>>