Vol.2012-CSEC-57 No.19
Vol.2012-IOT17 No.19
2012/5/11

日本語文字と熟語及び英数字を用いた CAPTCHA に関する提案

金森一樹† 児玉英一郎† 王家宏† 高田豊雄†

近年，フリーの Web メールをはじめとする Web 上のサービスに対し，BOT を用いて大量のアカウントを不正に取得する等の DoS 攻撃が定常的に発生している．これに対処するため，画面上に文字が描かれた画像を人間が読み取るといった CAPTCHA を利用したシステムが広く用いられる．しかし，BOT による OCR を排除する率を向上させると同時に人間にとっても読みづらいものになってしまう．このような問題に対し本研究では，日本語文字と漢字熟語および英数字を用いた CAPTCHA を提案し，評価実験の結果，漢字熟語の導入が可用性の向上に有効であることを示した．

A Proposal of a CAPTCHA Using a Japanese Character, a Set of Kanji and an Alphanumeric Character

KAZUKI KANAMORI† EIICHIRO KODAMA†
JIAHONG WANG† TOYOO TAKATA†

Recently, on free Web mail services and other kinds of service on Web, such DoS attacks as creating numerous accounts illegally using BOT have been occurring on a regular basis. For solving the problem, CAPTCHA systems, which require users to read and input some alphanumeric characters hiding in images shown on screens, have been widely used. The problem is that, however, alphanumeric characters have become more and more difficult to understand since modern CAPTCHA systems have to use more sophisticated images to avoid the BOT-based OCR. In this paper, we propose a new CAPTCHA that uses Japanese characters, Japanese compound words, and alphanumeric characters to solve the problem. Experimental results of a performance study shown that, introducing the Japanese compound words could really improve the availability of CAPTCHAs.

1. はじめに

近年，フリーの Web メールをはじめとする Web 上のサービスに対し，BOT を用いて大量のアカウントを不正に取得したり，大量の不正なサービス要求を行うなどの DoS 攻撃が定常的に発生している．例えば，米セキュリティ会社の Websense 社によると，米 Microsoft 社が提供するサービスである Windows Live Mail[1]用のアカウントを自動取得しているとされる[2]．Windows Live Mail は MSN Hotmail の後継として発表された無料の Web メールサービスで，世界中に数百万人以上のユーザがいるためブラックリストに載せられることが少ない．こうして不正な手段で手に入れられたアカウントはスパムメールの送信やソーシャルエンジニアリングなどといった攻撃に悪用されることになる．このような問題に対処するため，コンピュータ上の悪意ある自動プログラムからのリクエストであるか，人間からのリクエストであるかを判別するための CAPTCHA を利用したシステムが用いられるようになってきた．これは，もともとは BOT が検索エンジンに自動で URL を追加するのを防ぐために開発されたものである．多くの CAPTCHA を用いたシステムでは，画面上に文字が描かれた画像を提示し，それを読み取る手法が用いられている．この文字が書かれた画像には，機械による OCR（光学式文字認識）が困難になるように，形が歪められていたり関係のないノイズが加えられた文字列が描かれた画像が自動で人の手を介さず生成され，コンテンツの中で提示される．これに解答できれば，ユーザは人間，つまり正当なサービスを受けるべきユーザでありスパムでは無いと判断できる．

一方，オンラインゲームに代表される，日本国内で提供されているサービスの中には，詐欺防止や未成年者保護，リアルマネートレーディングといった不正な行為を阻止し正常なサービスを展開するため，という点から海外からの接続が規約で禁止されているものがあり[3][4]，これらのサービスを提供するサーバでは，海外からのアクセスが遮断されている．しかし実際には，中継サーバなどを用いることで回避されてしまうといった問題により，すべてのアクセスを排除しきれていないとされる[5][6]．以上から，本研究では，前述のような問題に対し，日本語を構成する文字の複雑性と，ネイティブスピーカーによる日本語文章の読解能力に着目して，日本語文字と漢字熟語，および英数字を混合した CAPTCHA の提案を行う．この提案手法では，既存の多くの英数字を用いた手法に対し，使用する文字種が多くなる分既存の CAPTCHA に対し突破成功率を抑えることが期待できる．欠点としては，使用する文字種の増加によりユーザビリティが損なわれる可能性があることが挙

†岩手県立大学大学院
Graduate School of Iwate Prefectural University

げられるが，入力に最も手間が掛かる漢字の入力が容易になるように熟語を用いることで，それを抑えることができる．

2. 既存手法と問題点

2.1 文字読み取り方式について

文字読み取り方式の CAPTCHA は，その名の通り，画面上に表示された文字を読み取り、入力する方式の CAPTCHA である．図 1 に具体例を示す．

図 1　既存の文字読み取り方式の CAPTCHA の認証画面の一例[7]

このように，画面上には歪みや内容とは関係の無い線などのノイズを含む文字列が画像として表示される．サービスを利用しようとする正規ユーザは画像に書かれた文字を読み取り，正しい解答を入力しなければならない．この文字読み取り方式には，大きく分けて 3 つの問題点がある．

2.1.1 自動プログラムによる不正な自動解答

第一に，自動プログラムによる不正な自動解答が挙げられる．本来 CAPTCHA は，コンピュータ上の悪意ある自動プログラムからのリクエストであるか，人間からのリクエストであるかを判別するために作られたものである．しかし，昨今の OCR（光学式文字認識）技術の発展により，ノイズが加えられていない，あるいはノイズが少ない画像については，高確率で OCR に成功し，CAPTCHA としての意味を成していないとされている．具体例として，PWNtcha[8]というプロジェクトでは，実際に 12 種類の CAPTCHA について，高確率での突破が成功したと報告されている他，OCR では読み取ることが困難と思われるノイズを付与した CAPTCHA のひとつである EZ-Gimpy も，非常に高い確率での解析に成功し，さらに高度なノイズを加えた Gimpy も，解読に成功し突破が可能となった[9]という報告もあり，何千ものリクエストを要求することができる BOT にとっては障壁となりえないことが示された．

2.1.2 人海戦術による不正な解答

第二に，CAPTCHA が多くの人々による人海戦術で機械的に解かれているという問題がある．この問題では，偽物のウェブサイトを用いてユーザを誘い，騙して CAPTCHA を解かせるという手法の他，発展途上国を拠点とし安い賃金で大量の人員を雇い CAPTCHA を解かせる，いわゆるバングラディシュアタックと呼ばれる手法がある[10]．また，人海戦術とツールが連携した，CAPTCHA を突破する有償のオンラインサービスといったものの存在も確認されており，人海戦術への対策が困難なものとなっている[11][12]．

2.1.3 ユーザビリティの問題

第三にユーザビリティの問題が挙げられる．CAPTCHA は本来，自動プログラムによる不正なリクエストを排除するために生まれた技術であるが，時には自動プログラムに対してだけではなく，サービスを受けるべき正規ユーザに対しても，サービス享受の障壁となっているという問題がある．CAPTCHA を解答するという行為は，サービスを受けるにあたって不要なものであり，正規ユーザにとっては煩わしいものである．簡単な問題であれば煩わしさは小さいが，自動プログラムによる突破が容易となる．逆に読み取ることが困難なほどにノイズを付与した CAPTCHA 認証画像を提示することで，自動プログラムによる解答が困難になるが，正規ユーザの煩わしさも大きくなってしまう．行き過ぎたサービスでは，明らかに多数の正規ユーザが読み取ることができないと思われる CAPTCHA が提示されることもある[13]．また，ニューラルネットワークによる文字の認識率の高さを人間と比較した研究があり，人間よりもコンピュータの方が高い認識率を持つという本来の CAPTCHA の想定と相反する結果が報告されており，文字そのものの難読化が利点になっていないということが明らかにされている[14]．図 2 は，利用規約上で日本国外からの接続行為を禁止しているサービスを利用する際に求められる CAPTCHA の一例である．この CAPTCHA は，認証に平仮名や片仮名，漢字を用いる事で出現する文字種数を増やし，BOT による突破を困難なものにしている．しかし，この CAPTCHA の認証画像に現れる漢字には意味的な規則性が無いため，画数が多く形の複雑な漢字は，字体がノイズによって潰れた場合，読解することが困難となる可能性が高い．

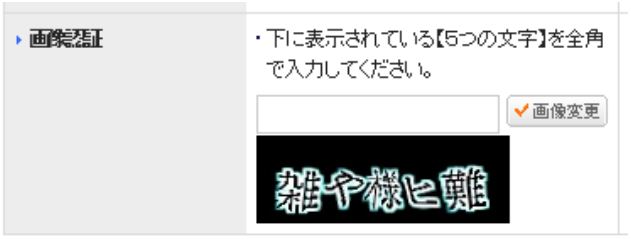

図 2　既存の日本語文字を用いた CAPTCHA の認証画面の一例[15]

2.2 画像を用いる方式

2.1 節で述べたように，文字列を読み取れるかどうかを試す CAPTCHA の一部は既に容易に突破されている．そこで，人間の持つ認知処理機能を利用し CAPTCHA をより強固なものにする方法が検討されてきた[16]．そのひとつに、Asirra がある[17]．Asirra は 10 枚の犬と猫が混ざった画像

を画面上に提示し，ユーザに全ての猫の画像を選ばせるという方法で認証を行う．Asirra の認証画面を図 3 に示す．提示される犬と猫の画像はペットの里親探しサイト Petfinder.com のものが使われている．しかしこの Asirra も，画面上に表示される画像が猫であるかどうかを約 83%の正解率で識別するプログラムが登場[18]し，新しい強固な CAPTCHA が求められている．

図 3　Asirra の認証画面の一例

3. 提案手法

3.1 英数字と日本語文字および熟語を用いた CAPTCHA の提案

本研究では，前述のような問題に対し，日本語文字と熟語，および英数字を混合した CAPTCHA の提案を行う．日本語文字は平仮名と片仮名および漢字を含めると，義務教育で学ぶ範囲で 2000 字を越え，英数字の文字数とは比較にならない数になっており，英数字に比べ OCR が比較的困難になると考えられる．また，アキを狭めることで，OCR は困難になる一方で人にとってはそれほど困難ではない認証画像を生成することで正答率や入力性といったユーザビリティの向上と，攻撃耐性の向上を図る．

3.1.1 使用する文字種

使用する文字種は，平仮名，片仮名，漢字，アルファベット，数字，記号からなる．文字種数を表 1 に，熟語種数を表 2 に示す．ここで用いる記号は，@（アットマーク），＃（シャープ），＄（ドル），％（パーセント），＆（アンパサンド），？（クエスチョンマーク）の 6 種を用いるものとする．平仮名と片仮名については，歴史的仮名遣い文字（ゐ，ゑ，ヰ，ヱ）を用いないものとする．また，ここで用いる漢字は，文部科学省文化審議会国語分科会が定めた常用漢字からなる単漢字および熟語の中から，中学校の 3 年次までに学習する漢字を選別した範囲（約 30 万項目[19]）から 5 文字以下の熟語を用いるものとする．日本語文字を用いた CAPTCHA は既に提案・実用化されているが，認証文字列に漢字熟語を混入させることで，読み取りと入力の両方の面でユーザにかかる負荷が軽減することが期待できる．

表 1　文字種数 一覧

文字種	文字種数
漢字	1,845
平仮名	46
片仮名	46
記号	6
英数字	38

表 2　熟語数 一覧

構成字数	熟語数
1	1,845
2	62,250
3	64,011
4	105,078
5	50,129

3.1.2 使用するフォント

単一フォントによる認証画像の生成はパターンマッチによる突破が考えられる．実際，既存の多くの文字認証型の CAPTCHA ではフォントを多数用いている．本提案では合計 82 種用意し，生成毎にランダムに用いるものとする．

3.1.3 認証文字列生成手順

まず，上述の辞書[19]より，熟語の選択を行う．熟語は認証画像生成毎にランダムに選択する．ここで，選択した熟語が 2 文字以下であればもう 1 つの 2 文字以下の熟語を選択する．熟語を生成した後，熟語の各漢字を配置する文字位置を，熟語を構成する漢字の順序を維持しつつ熟語同士がまたがない範囲で無作為に指定し，残りの文字位置には漢字以外のすべての文字を無作為に指定するものとする．また，認証文字列は 8 文字で固定される．

3.2 プロトタイプシステムの実装

前述の提案手法の有効性について評価するため，認証システムのプロトタイプの構築を行った．システムの開発・実験環境を表 3 と図 4 に示す．本システムは，生成ボタンを押すことで認証画像を生成し，ボタン下のテキストボックスに認証文字列を入力し，解答ボタンを押すと正解か不正解かが表示される仕様となっている．本システムの実行画面を図 5 に示す．

Vol.2012-CSEC-57 No.19
Vol.2012-IOT17 No.19
2012/5/11

表 3　実験環境 諸元一覧表

開発言語	Visual C#
OS	Windows 7
キーボード	SK-5400
インプットメソッド	MS-IME v10
モニター解像度	1280x1024px
認証画像解像度	800 x 100px

図 4　プロトタイプシステム実験環境

図 5　実行画面の一例

4. 予備評価実験

4.1 実験の目的

提案手法と既存手法を比較するため，ノイズの生成アルゴリズムを共通としたうえで「英数字のみを用いた場合（英数字方式）」,「日本語文字と記号を用い熟語を用いない場合（日本語方式）」,「熟語と日本語文字と記号を用いた場合（熟語方式）」それぞれについて，20 問を正答するまでに要する時間と試行回数を測定し，被験者からの意見・感想およびプロトタイプシステムのプログラム上の問題点を収集する．

4.2 所要正答時間の定義

ここでは，所要正答時間について説明する．所要正答時間は，「解答するまでに要した時間を正答率で割ったもの」とする．すなわち，計算式は「所要正答時間＝解答時間の平均/正答率」となる．ここでの「解答時間の平均」は，解答時間の総和を解答回数で割ったものとし，また「正答率」は，正答数（ここでは 20 回で固定）を解答数で割ったものとする．例えば，1 問あたりの解答時間が平均 35 秒で，解答回数が 30 回（正答率 0.67）ならば，35 秒/0.67＝約 52.24 秒となる．

4.3 評価結果

被験者 3 名に対して行った予備評価実験で得られた，各被験者の所要正答時間を表 4 に，試行回数を表 5 に示す．まず，英数字版の所要正答時間と試行回数に注目する．英数字版は単漢字版および熟語版と比べ，所要正答時間が圧倒的に短いことがわかる．これは，使用文字種の少なさから生まれる，読み取り性の高さと入力の容易性の高さが原因として考えられる．次に単漢字版と熟語版に注目すると，熟語版は単漢字版に比べ，試行回数が少なく所要正答時間も短い傾向にあることがわかる．これは当初の予想通り，熟語を用いることで，読み取り性と入力の容易性が向上しているためと考えられる．一方で，所要正答時間や試行回数に大きな個人差が生まれた．タイピング速度が一因として考えられるが，英数字版で所要正答時間が 2 番目に短いユーザ 3 が単漢字版および熟語版で 3 ユーザ中もっとも長い所要正答時間となっていることから，他にも原因があると考えられる．一方，日本語と英数字を交互に入力する際に全角文字と半角文字が入り混じる事があることがわかったほか，片仮名のイと以を似と誤認するなど，文字数を間違える事があることが判明した．最後に被験者からの指摘として，誤認されやすい文字がある，と指摘を受けた．具体的には，アルファベット大文字のO（オー）と 0（ゼロ），アルファベット大文字の I （アイ）とアルファベット小文字の l （エル）などである．

表 4　予備評価実験 所要正答時間

単位:秒	英数字	単漢字	熟語
ユーザ 1	15.6	35.6	27.9
ユーザ 2	21.3	55.7	35.5
ユーザ 3	16.7	60.7	41.4

表 5　予備評価実験 試行回数

単位:回	英数字	単漢字	熟語
ユーザ 1	29	25	26
ユーザ 2	43	44	34
ユーザ 3	34	45	44

4.4 予備評価時からの仕様変更点

上述の形成的評価で判明した問題点を，総括的評価に向けて修正することとした．

- 誤認されやすい文字（アルファベット大文字のO（オー）と 0（ゼロ），アルファベット大文字の I （アイ）とアルファベット小文字の l （エル））を区別しない

ものとした．

- 半角文字と全角文字を区別しないものとした．
- 文字数を間違えないように，「文字数は 8 文字で固定する」と明示することとした．
- プログラム上の問題（バグ）が指摘されたため，プログラムを修正した．

5. 総括的評価

5.1 予備評価時からの評価手順変更点

実験の概要は，4.4 節で述べた変更点を適用した点以外は，4 節で行った実験と同様である．

5.2 評価結果

被験者 10 名に対して行った評価の結果のうち，所要正答時間についてを図 6 に，試行回数を図 7 に示す．

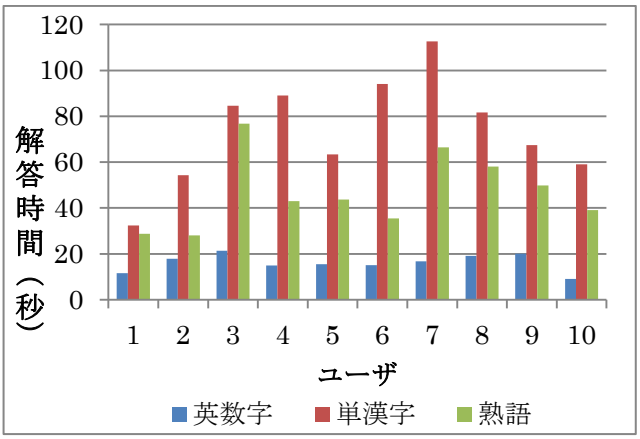

図 6　所要正答時間

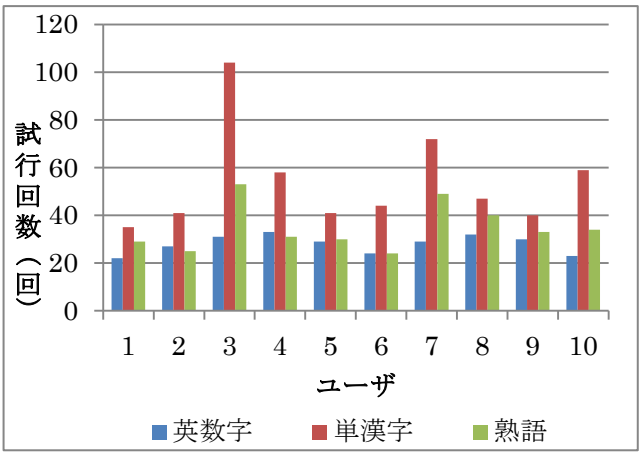

図 7　試行回数

まず，英数字版の所要正答時間と試行回数に注目すると，所要正答時間が 16.1 秒と，英数字版は予備評価時と同じく単漢字版および熟語版に比べ，所要正答時間が圧倒的に短いことがわかった．また，試行回数も少ない傾向にあり，ほとんどの被験者が 30 回前後以下で，正答率が 65%以上あることがわかる．理由としては，やはり使用文字種が少ないことから読み取り性と入力の容易性が高くなっていることが原因として挙げられる．次に単漢字版に注目すると，他 2 方式と比較して所要正答時間が圧倒的に長くなっており，また試行回数も多くなっていることがわかる．これは単漢字版が読み取り，入力ともに他 2 方式と比べ困難であることを示している．最後に熟語版に注目すると，単漢字版と比較して所要正答時間が全体的に短くなっており，また試行回数も少なくなっていることがわかる．これは単漢字版に熟語という要素を織り込むことで読み取り，入力がともに容易になっていることが原因として挙げられる．

6. 考察

6.1 類似文字の誤認について

前述の英数字の間違われやすい文字のほか，日本語文字間でも間違われやすい文字があることがわかった．まず，片仮名と漢字の間での誤認である．具体的には，片仮名の‘エ’，‘カ’と，漢字の‘工’，‘力’などである．この問題は，解答として両方を許容するか，あるいは出題から除外することで対処が可能である．次に，漢字を違う漢字と誤認する事例である．具体的には，骨と滑，折と祈，箱と籍などである．この誤認は，主に単漢字版で多く発生することがわかった．熟語版ではこの種の誤認は少ない傾向にあるが，同音異義かつ熟語を構成する漢字の一部が一致する場合で、誤認あるいは入力ミスが起きることがあった．具体的には，公園と公演のような場合である．

6.2 被験者からの意見と感想

まず，ほぼ全ての被験者から熟語を歓迎する感想を受けた．その多くはノイズが酷くとも熟語からの推測で文字を入力できるというものである．一方で，ネガティブな意見としては，まず文字同士が重なりすぎると読めないというものがあった．原因としては、フォントごとのアキの調整が不完全であることが挙げられるが，熟語版と単漢字版で条件は平等となっている．次に，似た文字の判別が困難であるとの意見があったが，前述のように一部文字は解答として両方を許容するか，あるいは除外することで対処が可能である．また，熟語を意識しすぎて逆に混乱してしまうという意見もあった．

6.3 生成文字列のパターン空間の広さ

英数字版，単漢字版，熟語版をそれぞれ 8 文字とした場合のパターン空間の広さと，単漢字版と熟語版それぞれが 8 文字の時にパターン空間の広さが英数字何文字に相当するかを換算したものを表 6 に示す．熟語版は単漢字版のものより 10 の 6 乗分の 1 ほど小さいものとなっているが，英数字版 13～14 文字相当となることから，十分に大きな広さを持っていると考えられる．

Vol.2012-CSEC-57 No.19
Vol.2012-IOT17 No.19
2012/5/11

表 6　8 文字の場合の文字列の生成パターン空間の広さ

	空間の広さ	英数字換算
英数字版	4.3E+12	8 文字
単漢字版	2.3E+26	16～17 文字
熟語版	8.6E+20	13～14 文字

7. まとめ

本研究では，日本語文字と漢字熟語，および英数字を混合した CAPTCHA を提案した．そして，プロトタイプの実装と評価実験を行い，熟語を用いる本提案手法の CAPTCHA システムは熟語を用いない CAPTCHA システムに比べて，人間に対しては高い認証成功率が得られ，解答に要する時間が短縮されることを確認した．今後の課題として，まず個人差を小さくすることが挙げられる．本研究の目的のひとつとして，全ての正規ユーザにとって解答が容易な CAPTCHA を実現することが挙げられるが，本提案手法の評価実験においては解答時間に大きな個人差が生まれた．ユーザごとのタイピング速度の違いが，個人差が生まれる一因であると考えられるが，タイピング速度以外にも原因がある可能性があるため，これについて調査および検討することは非常に重要である．また，6.1 節で述べた通り，熟語版であっても少なからず文字の誤認があることがわかった．この誤認をどのように少なくしていくかについて，考案する必要がある．

参考文献

1) Windows Live Hotmail
http://explore.live.com/hotmail
2) 「Windows Live Mail」アカウント取得時の CAPTCHA を大量処理
http://itpro.nikkeibp.co.jp/article/COLUMN/20080226/294681/
3) Gamechu 利用規約- Gamechu
http://api.gamechu.jp/register/agree
4) HanbitStation 利用規約 - HanbitStation
http://www.hanbitstation.jp/support/page_m3_1.asp
5) MMO 総合研究所
http://www.mmoinfo.net/news/ziken/
6) 人気ゲーム不正アクセスで逮捕者- AllAbout
http://allabout.co.jp/gm/gc/216004/2/
7) reCAPTCHA
http://www.google.com/recaptcha
8) PWNtcha - CAPTCHA DECODER
http://caca.zoy.org/wiki/PWNtcha
9) J.Yan,A.S.E.Ahmad: Breaking Visual CAPTCHAs with Naive Pattern Recognition Algorithms, 2007 Computer Security Applications Conference, pp.279-291, 2007.
10) Spammers Pay Others to Answer Security Tests
http://www.nytimes.com/2010/04/26/technology/26captcha.html
11) 人海戦術で CAPTCHA を解読する犯罪者向けサービス、RSA セキュリティが報告
http://it.impressbm.co.jp/e/2009/12/17/1641
12) DEATH BY CAPTCHA
http://deathbycaptcha.com/
13) Top 10 Worst Captchas
http://www.johnmwillis.com/other/top-10-worst-captchas/
14) K.Chellapilla, P.Simard,: Using Machine Learning to Break Visual Human Interaction Proofs (HIPs)
Neural Information Processing Systems(NIPS) 2007.
15) Gamechu
http://www.gamechu.jp/
16) K.Chellapilla, K.Larson, P.Simard, M.Czerwinski: Computers Beat Humans at Single Character Recognition in Reading-based Human Interaction Proofs(HIPs), 2nd Conference on Email and Anti-Spam (CEAS), 2005.
17) Asirra Project Microsoft Research
http://research.microsoft.com/en-us/um/redmond/projects/asirra/
18) P.Golle: Machine Learning Attacks against the Asirra CAPTCHA, CCS '08 Proceedings of the 15th ACM Conference on Computer and Communications Security, pp.535-542, 2008.
19) GigaDict 日本語教育漢字熟語大字典
http://gigadict.com/