

技術ノート

ツール, ライブラリ, 処理環境

Copyright © 2017-2018, Katsunori Nakamura

中村勝則

2020年3月24日

免責事項

本書の内容は参考資料であり、掲載したプログラムリストは全て試作品である。本書の使用に伴って発生した不利益、損害の一切の責任を筆者は負わない。

目次

| | |
|--|-----------|
| 1 ツール群 | 1 |
| 1.1 文字コード／改行コード変換 | 1 |
| 1.1.1 iconv | 1 |
| 1.1.2 NKF (Network Kanji Filter) | 1 |
| 1.1.2.1 MIME 関連の機能 | 3 |
| 1.1.2.2 若干の注意点 | 3 |
| 1.2 MeCab(和布蕪)：日本語形態素解析 | 4 |
| 1.2.1 NEologd のインストール | 5 |
| 1.3 CaboCha(南瓜)：日本語係り受け解析 | 7 |
| 1.4 JUMAN：日本語形態素解析 | 10 |
| 1.5 KNP：日本語係り受け解析 | 10 |
| 1.6 Open JTalk：テキスト読み上げ | 12 |
| 1.6.1 処理の例 | 12 |
| 1.7 Julius：音声認識 | 13 |
| 1.7.1 動作テスト | 14 |
| 1.7.2 WAV 形式音声ファイルの認識 | 15 |
| 1.8 OpenSSL：暗号化，復号，電子署名 | 18 |
| 1.8.1 公開鍵暗号方式による暗号化の方法 | 18 |
| 1.8.1.1 公開鍵と秘密鍵の生成 | 18 |
| 1.8.1.2 公開鍵による暗号化 | 19 |
| 1.8.1.3 秘密鍵による復号 | 19 |
| 1.8.2 公開鍵暗号方式による電子署名の作成 | 19 |
| 2 ライブラリ | 21 |
| 2.1 GMP/MPFR：任意多倍長演算 | 21 |
| 2.1.1 GMP | 21 |
| 2.1.1.1 GMP で利用できる関数 (一部) | 22 |
| 2.1.1.2 サンプルプログラム | 24 |
| 2.1.1.3 プログラムの実行に際して | 24 |
| 2.1.2 MPFR | 26 |
| 2.1.2.1 サンプルプログラム | 27 |
| 2.1.2.2 プログラムの実行に際して | 28 |
| 2.1.3 MPFR で利用できる数学関数 (一部) | 28 |
| 3 処理環境 | 30 |
| 3.1 Microsoft Visual Studio / Visual C++ | 30 |
| 3.1.1 Visual C++ | 30 |
| 3.1.1.1 コマンドツールとしてのコンパイラ | 30 |
| 3.1.2 Visual Studio | 32 |
| 3.2 MinGW / MSYS2 | 33 |
| 3.2.1 導入とパッケージ管理の方法 | 33 |
| 3.2.1.1 pacman によるパッケージ管理 | 33 |

| | |
|---|-----------|
| 4 Python での応用例 | 35 |
| 4.1 MeCab との連携 | 35 |
| 4.1.1 mecab-python3/mecab-python-windows | 35 |
| 4.1.2 MeCab の解析結果の取り扱いについて | 36 |
| 4.2 日本語テキストの読み上げ (Open JTalk と PyAudio の応用) | 38 |
| 4.3 Python と SWI-Prolog の連携 | 40 |
| 4.3.1 基本的な使用方法 | 40 |

1 ツール群

1.1 文字コード／改行コード変換

1.1.1 iconv

iconv はテキストデータの文字コードを変換するツールとライブラリであり、POSIX 規格で標準化されている。このため iconv は多くの UNIX 系 OS で利用可能な場合が多く、Windows 環境でも POSIX 系ツール群を導入している場合は利用可能なことが多い。ここではコマンドツールとしての iconv の使用方法について説明する。

■ 使い方

iconv コマンドには、変換元のファイルの文字コードと、変換先の文字コードを起動時のオプションとして与える。

コマンド書式: `iconv -f 変換元の文字コード -t 変換先の文字コード 変換元ファイル名`

変換元のデータは iconv の標準入力に与えることもできる。変換先のデータは標準出力に出力される。

コマンドオプションに指定できる文字コードは '-l' オプションで起動することで確認できる。

例. iconv で扱うことのできる文字コードの確認 (bash でのコマンド操作の例)

```
$ iconv -l  ←コマンドの投入
ANSI_X3.4-1968 ANSI_X3.4-1986 ASCII CP367 IBM367 ... ←指定できる文字コードが表示される
UTF-8
      ⋮
      (途中省略)
      ⋮
CP949 UHC
CP1361 JOHAB
ISO-2022-KR CSISO2022KR
```

1.1.2 NKF (Network Kanji Filter)

NKF¹ はテキストデータの文字コードを変換するだけでなく、改行コードの変換など様々な機能を備えている。コマンド名は `nkf` で、`-help` オプションを与えて起動すると基本的な使用方法が表示される。

例. `nkf` のヘルプ表示 (bash でのコマンド操作の例)

```
$ nkf --help  ←コマンドの投入
Usage: nkf [-flags] [--] [in file] .. [out file for -o flag] ←ヘルプ表示が始まる
j/s/e/w Specify output encoding ISO-2022-JP, Shift_JIS, EUC-JP
UTF options is -w[8[0],16,32[B,L[0]]]
      ⋮
      (途中省略)
      ⋮
Network Kanji Filter Version 2.1.4 (2015-12-12)
Copyright (C) 1987, FUJITSU LTD. (I.Ichikawa).
Copyright (C) 1996-2015, The nkf Project.
```

変換元のテキストデータは `nkf` コマンドの標準入力から与えることができる。また、ファイルとして保存されているテキストデータを変換対象とする場合は、`nkf` のコマンド引数にそのファイル名を記述する。変換結果は標準出力に出力される。

¹1987年に富士通が開発。現在は OSDN のインターネットサイト (<https://ja.osdn.net/projects/nkf/>) で保守されている。

例. ファイル text1.txt の文字コードを変換して text2.txt を作成する例 (bash でのコマンド操作の例)

```
$ nkf -w text1.txt > text2.txt
```

この例では、'-w' オプションを与えることで、UTF-8 の文字コードに変換している。変換先の文字コードの指定など、出力データに関するオプションとして重要なものを表 1 に挙げる。

表 1: 出力に関するオプション (一部)

| オプション | 解説 |
|--------------|--|
| -j | JIS コードで出力 (デフォルト) |
| -e | EUC コードで出力 |
| -s | シフト JIS コードで出力 |
| -w, -w80 | UTF-8 コードで出力 (BOM なし) |
| -w8 | UTF-8 コードで出力する (BOM あり) |
| -w16, -w16B0 | UTF-16 コードで出力 (ビッグエンディアン / BOM なし) |
| -w16B | UTF-16 コードで出力 (ビッグエンディアン / BOM あり) |
| -w16L | UTF-16 コードで出力 (リトルエンディアン / BOM あり) |
| -w16L0 | UTF-16 コードを出力する (リトルエンディアン / BOM なし) |
| -l | ISO-2022-JP 以外の漢字コードを「 ■ 」(げた記号) に変換 |
| -d, -Lu | 改行を LF に変換 (UNIX 系) |
| -c, -Lw | 改行を CRLF に変換 (Windows 系) |
| -Lm | 改行を CR に変換 (古い Macintosh) |
| -X | 半角カナ (JIS X 0201 片仮名) を全角カナ (JIS X 0208 片仮名) に変換 (デフォルト) |
| -x | 半角カナを維持する |
| -Z, -Z0 | 全角を半角に変換 (JIS X 0208 英数字といくつかの記号を ASCII に変換) |
| -Z1 | JIS X 0208 和字間隔を ASCII スペース 1 つに変換 |
| -Z2 | JIS X 0208 和字間隔を ASCII スペース 2 つに変換 |
| -Z3 | 「>」「<」「”」「&」をそれぞれ「>」「<」「"」「&」に変換 |
| --hiragana | カタカナをひらがなに変換 |
| --katakana | ひらがなをカタカナに変換 |
| --overwrite | ファイルを変換して上書きする |

改行コードに関するオプションをつけない場合は改行コードは変換しない

NKF は変換元のテキストデータの文字コードと改行コードを自動的に判別するが、明にオプション (表 2) として指定することもできる。

表 2: 入力に関するオプション (一部)

| オプション | 解説 |
|---------|--|
| -J | 入力を ISO-2022-JP とみなす |
| -E | 入力を日本語 EUC とみなす |
| -S | 入力をシフト JIS とみなす。半角カナ (JIS X 0201 片仮名) も受け入れる |
| -W, -W8 | 入力を UTF-8 とみなす |
| -W16 | 入力を UTF-16 (リトルエンディアン) とみなす |
| -W16B | 入力を UTF-16 (ビッグエンディアン) とみなす |
| --guess | 対象ファイルの文字コードと改行コードを調べる |

1.1.2.1 MIME 関連の機能

nkf は MIME² に関する変換機能を備えている。そのためのオプションを表 3 に示す。

表 3: MIME に関するオプション (一部)

| オプション | 解説 |
|-------|--|
| -m | MIME を解読。「-mS」と同じ (デフォルト) |
| -mB | base64 stream を解読 |
| -mQ | Quoted stream を解読 |
| -mS | MIME のチェックの厳格化 (他のオプションと組み合わせ可) |
| -mN | MIME のチェックを緩く (他のオプションと組み合わせ可) |
| -m0 | MIME を解読しない |
| -M | MIME に変換 (JIS に変換してから base64 ヘッダ形式に変換) |
| -MB | base64 stream に変換 |
| -MQ | Quoted stream に変換 |

1.1.2.2 若干の注意点

iconv と NKF は共に文字コードの変換機能を有するが、両者の処理結果は完全には一致しないことに注意すること。

²MIME (Multipurpose Internet Mail Extensions): RFC 2045, RFC 2046, RFC 2047, RFC 4288, RFC 4289, RFC 2049

1.2 MeCab(和布蕪)：日本語形態素解析

MeCab は、京都大学情報学研究科—日本電信電話株式会社コミュニケーション科学基礎研究所共同研究ユニットプロジェクトを通じて開発されたオープンソースの形態素解析エンジンである。³

MeCab を用いることで日本語の文章を解析して、文章の要素データを生成することができる。基本的に MeCab はコマンドラインツールであり、日本語文章のテキストを標準入力やテキストファイルから入力することで、標準出力やテキストファイルに文章の要素データを出力することができる。

次に示す test11.txt のようなテキストファイルを MeCab に与える例を示す。

サンプルテキスト：test11.txt

```
1 (フリー百科事典「ウィキペディア」より)
2
3 コードを単純化して可読性を高め、読みやすく、また書きやすくしてプログラムの
4 作業性とコードの信頼性を高めることを重視してデザインされた、汎用の高水準言語
5 である。反面、実行速度はCなどの低級言語に比べて犠牲にされている。
6
7 核となる文法（シンタックス）および意味（セマンティクス）は必要最小限に抑え
8 られている。その反面、豊富で大規模な文書（document）や、さまざまな領域に
9 対応する大規模な標準ライブラリやサードパーティ製のライブラリが提供されている。
10 またPythonは多くのハードウェアとOS（プラットフォーム）に対応しており、複数の
11 プログラミングパラダイムに対応している。Pythonはオブジェクト指向、命令型、
12 手続き型、関数型などの形式でプログラムを書くことができる。動的型付け言語であり、
13 参照カウントベースの自動メモリ管理（ガベージコレクタ）を持つ。
14
15 これらの特性により、PythonはWebアプリケーションやデスクトップアプリケーション
16 などの開発はもとより、システム用の記述（script）や、各種の自動処理、理工学や
17 統計・解析など、幅広い領域における支持を得る、有力なプログラム言語となった。
18 プログラミング作業が容易で能率的であることは、ソフトウェア企業にとっては
19 投入人員の節約、開発時間の短縮、ひいてはコスト削減に有益であることから、
20 産業分野でも広く利用されている。Googleなど主要言語に採用している企業も多い。
```

■ MeCab の実行

コマンドの書式： `mecab test11.txt`

この結果、次のような文章の要素データが標準出力に出力される。

出力例

```
( 記号, 括弧開, *, *, *, *, (, (, (
フリー 名詞, 一般, *, *, *, *, フリー, フリー, フリー
百科 名詞, 一般, *, *, *, *, 百科, ヒヤッカ, ヒヤッカ
事典 名詞, 一般, *, *, *, *, 事典, ジテン, ジテン
「 記号, 括弧開, *, *, *, *, 「, 「, 「
ウィキペディア 名詞, 固有名詞, 一般, *, *, *, *
」 記号, 括弧閉, *, *, *, *, 」, 」, 」
事典 名詞, 一般, *, *, *, *, 事典, ジテン, ジテン
:
(途中省略)
:
EOS
コード 名詞, 一般, *, *, *, *, コード, コード, コード
を 助詞, 格助詞, 一般, *, *, *, *, を, を, を
:
(以下省略)
:
```

この例にあるように、1行の解析毎にEOSという行が出力される。

入力ファイルを指定せずに MeCab を起動すると、標準入力から文章の入力を受け付ける。

MeCab の出力の形式は次の通りである。

³この紹介文は MeCab のインターネットサイト <http://taku910.github.io/mecab/> からの引用を元に行っている。

表層形 (タブ) 品詞, 品詞細分類 1, 品詞細分類 2, 品詞細分類 3, 活用例, 活用形, 原形, 読み, 発音

MeCab は起動時に、出力先や出力の形式を変更するためのオプションを与えることができる。

出力に関するオプション (一部)

- O wakati 表層形のデータのみをスペースで区切った形 (分かち書き形式) で出力する。
- o 出力ファイル名 出力ファイル名に指定したファイルに出力する。

分かち書き出力の例

```
mecab -O wakati test11.txt
```

この結果次のような出力となる。

分かち書きの出力例

(フリー百科事典「ウィキペディア」より)
コードを単純化して可読性を高め、読みやすく、また書きやすくしてプログラムの作業性とコードの信頼性を高めることを重視してデザインされた、汎用の高水準言語である。
:
(以下省略)
:

1.2.1 NEologd のインストール

NEologd は MeCab の辞書を拡張するもの (ユーザ辞書) であり、Web コンテンツや SNS への投稿記事から採取された比較的新しい語彙を提供するものである。NEologd の最新の辞書データは公式インターネットサイト

<https://github.com/neologd/mecab-ipadic-neologd>

から得られる。

■ 辞書の元になるデータ (seed ファイル) の取得

辞書データの元になる CSV 形式ファイル (seed ファイル) をダウンロードする。本書執筆時点では

```
mecab-user-dict-seed.20200315.csv.xz
```

というファイルが最新のものである。拡張子「~.xz」は 7zip による圧縮ファイルであり、展開することで CSV 形式ファイル「mecab-user-dict-seed.20200315.csv」が得られる。

■ 辞書データの作成

上で得られた seed ファイルから MeCab 用の辞書ファイルを作成するには mecab-dict-index コマンドを使用する。これは MeCab のシステムに含まれるものであり、MeCab 関連のコマンドが使用できるようにコマンドサーチパスを適切に設定しておく必要がある。

例. Windows 版 MeCab 関連コマンドのディレクトリ

```
C:\Program Files (x86)\MeCab\bin
```

このようなディレクトリのパスをコマンドサーチパスに設定した状態で mecab-dict-index コマンドを実行する。

《コマンドの書式》

```
mecab-dict-index -d 辞書設定ファイルがあるディレクトリ -u 作成する辞書ファイル  
-f seed ファイルのエンコーディング  
-t 作成する辞書ファイルのエンコーディング seed ファイル
```

「-d 辞書設定ファイルがあるディレクトリ」には、MeCab の辞書設定を記述したファイル dicrc のディレクトリを指定する。「-u 作成する辞書ファイル」には実際に MeCab が使用するユーザ辞書の名前を指定する。ここには任意のファイル名が指定できる。

例. Windows 環境での作業 (UTF-8 の辞書を作成)

```
mecab-dict-index -d "C:¥Program Files (x86)¥MeCab¥dic¥ipadic"  
-u NEologd.20200315-u.dic -f utf-8 -t utf-8 mecab-user-dict-seed.20200315.csv
```

この例では seed ファイル ‘mecab-user-dict-seed.20200315.csv’ から MeCab 辞書 ‘NEologd.20200315-u.dic’ を作成している。

作成した辞書ファイルは適切なディレクトリに配置する。例えば Windows 環境の場合は

```
‘C:¥Program Files (x86)¥MeCab¥dic’
```

の下に ‘neologd’ といったディレクトリを作成してその中に配置すると良い。

■ MeCab 設定ファイルの編集

作成した辞書ファイルが使用できるように、MeCab の設定ファイルを編集する。例えば Windows 環境の場合は MeCab の設定ファイルは

```
C:¥Program Files (x86)¥MeCab¥etc¥mecabrc
```

であり、この中に

```
userdic="C:¥Program Files (x86)¥MeCab¥dic¥neologd¥NEologd.20200315-u.dic"
```

などと記述する。

1.3 CaboCha(南瓜)：日本語係り受け解析

CaboCha(南瓜)は、MeCabの形態素解析の結果を用いて、日本語の文の係り受け構造を解析するツールである。CaboChaに関する詳しい情報は、公式インターネットサイト <https://taku910.github.io/cabocha/> から得られる。

CaboChaは基本的にはコマンドツールであり、OSのコマンドシェルにて cabocha コマンドを投入することで起動する。例えば jtext-u.txt のようなテキストファイルの係り受け構造の解析について考える。

サンプルテキスト：jtext-u.txt

- ```
1 | この文のような複雑な係り受け構造を持つ文を解析することができる
 | と人工知能プログラムのためのヒューマンインター
 | フェースを開発するのに役立ちます。
```

このテキストファイルを次のようなコマンドで処理をする。

```
cabocha jtext-u.txt
```

これにより、次のような結果（木構造）が標準出力に出力される。

```
この-D
文のような-----D
 複雑な-D |
 係り受け---D |
 構造を-D |
 持つ-D |
 文を-D |
 解析する-D |
 ことが-D |
 できると-----D
 人工知能プログラムの-D |
 ための-D |
 ヒューマンインターフェースを-D
 開発するの-D |
 役に立ちます。EOS
```

また、cabocha コマンドに '-f1' オプションを付けて実行する (cabocha -f1 jtext-u.txt) と次のような出力となり、機械可読な解析結果が得られる。

出力結果：

```
1 | * 0 1D 0/0 0.047241
2 | この 連体詞,*,*,*,*,*,この,コノ,コノ
3 | * 1 6D 2/3 1.151904
4 | 文 名詞,一般,*,*,*,*,文,ブン,ブン
5 | の 助詞,連体化,*,*,*,*,の,ノ,ノ
6 | よう 名詞,非自立,助動詞語幹,*,*,*,よう,ヨウ,ヨー
7 | な 助動詞,*,*,*,特殊・ダ,体言接続,だ,ナ,ナ
8 | * 2 3D 0/1 0.705414
9 | 複雑 名詞,形容動詞語幹,*,*,*,*,複雑,フクザツ,フクザツ
10 | な 助動詞,*,*,*,特殊・ダ,体言接続,だ,ナ,ナ
11 | * 3 5D 1/1 0.694835
12 | 係り 名詞,一般,*,*,*,*,係り,カカリ,カカリ
13 | 受け 動詞,自立,*,*,一段,連用形,受ける,ウケ,ウケ
14 | * 4 5D 0/1 2.508135
15 | 構造 名詞,一般,*,*,*,*,構造,コウゾウ,コーゾー
16 | を 助詞,格助詞,一般,*,*,*,を,ヲ,ヲ
17 | * 5 6D 0/0 1.335883
18 | 持つ 動詞,自立,*,*,五段・タ行,基本形,持つ,モツ,モツ
19 | * 6 7D 0/1 2.262625
20 | 文 名詞,一般,*,*,*,*,文,ブン,ブン
21 | を 助詞,格助詞,一般,*,*,*,を,ヲ,ヲ
22 | * 7 8D 1/1 1.993750
23 | 解析 名詞,サ変接続,*,*,*,*,解析,カイセキ,カイセキ
24 | する 動詞,自立,*,*,サ変・スル,基本形,する,スル,スル
25 | * 8 9D 0/1 1.854513
```

26 | こと 名詞,非自立,一般,\*,\*,\*,こと,コト,コト  
 27 | が 助詞,格助詞,一般,\*,\*,\*,が,ガ,ガ  
 28 | \* 9 13D 0/1 0.124090  
 29 | できる 動詞,自立,\*,\*,一段,基本形,できる,デキル,デキル  
 30 | と 助詞,接続助詞,\*,\*,\*,と,ト,ト  
 31 | \* 10 11D 2/3 1.869991  
 32 | 人工 名詞,一般,\*,\*,\*,人工,ジンコウ,ジンコー  
 33 | 知能 名詞,一般,\*,\*,\*,知能,チノウ,チノー  
 34 | プログラム 名詞,サ変接続,\*,\*,\*,プログラム,プログラム,プログラム  
 35 | の 助詞,連体化,\*,\*,\*,の,ノ,ノ  
 36 | \* 11 12D 0/1 2.088981  
 37 | ため 名詞,非自立,副詞可能,\*,\*,\*,ため,タメ,タメ  
 38 | の 助詞,連体化,\*,\*,\*,の,ノ,ノ  
 39 | \* 12 13D 1/2 1.876101  
 40 | ヒューマン 名詞,一般,\*,\*,\*,ヒューマン,ヒューマン,ヒューマン  
 41 | インターフェース 名詞,一般,\*,\*,\*,インターフェース,インターフェース,インターフェース  
 42 | を 助詞,格助詞,一般,\*,\*,\*,を,ヲ,ヲ  
 43 | \* 13 14D 2/3 0.124090  
 44 | 開発 名詞,サ変接続,\*,\*,\*,開発,カイハツ,カイハツ  
 45 | する 動詞,自立,\*,\*,サ変・スル,基本形,する,スル,スル  
 46 | の 名詞,非自立,一般,\*,\*,\*,の,ノ,ノ  
 47 | に 助詞,格助詞,一般,\*,\*,\*,に,ニ,ニ  
 48 | \* 14 -1D 0/1 0.000000  
 49 | 役立ち 動詞,自立,\*,\*,五段・タ行,連用形,役立つ,ヤクダチ,ヤクダチ  
 50 | ます 助動詞,\*,\*,\*,特殊・マス,基本形,ます,マス,マス  
 51 | . 記号,句点,\*,\*,\*,.,.,.  
 52 | EOS

上記出力結果の書式に関しては cabocha の公式インターネットサイトなどを参照のこと。

CaboCha では実行時のコマンドオプションとして '-f3' を与えると、解析結果を XML 形式で出力することもできる。出力例を次に示す。

出力結果：

```

1 <sentence>
2 <chunk id="0" link="1" rel="D" score="0.047241" head="0" func="0">
3 <tok id="0" feature="連体詞,*,*,*,*,この,コノ,コノ">この</tok>
4 </chunk>
5 <chunk id="1" link="6" rel="D" score="1.151904" head="3" func="4">
6 <tok id="1" feature="名詞,一般,*,*,*,文,ブン,ブン">文</tok>
7 <tok id="2" feature="助詞,連体化,*,*,*,の,ノ,ノ">の</tok>
8 <tok id="3" feature="名詞,非自立,助動詞語幹,*,*,*,よう,ヨウ,ヨー">よう</tok>
9 <tok id="4" feature="助動詞,*,*,*,特殊・ダ,体言接続,だ,ナ,ナ">な</tok>
10 </chunk>
11 <chunk id="2" link="3" rel="D" score="0.705414" head="5" func="6">
12 <tok id="5" feature="名詞,形容動詞語幹,*,*,*,複雑,フクザツ,フクザツ">複雑</tok>
13 <tok id="6" feature="助動詞,*,*,*,特殊・ダ,体言接続,だ,ナ,ナ">な</tok>
14 </chunk>
15 <chunk id="3" link="5" rel="D" score="0.694835" head="8" func="8">
16 <tok id="7" feature="名詞,一般,*,*,*,係り,カカリ,カカリ">係り</tok>
17 <tok id="8" feature="動詞,自立,*,*,一段,連用形,受ける,ウケ,ウケ">受け</tok>
18 </chunk>
19 <chunk id="4" link="5" rel="D" score="2.508135" head="9" func="10">
20 <tok id="9" feature="名詞,一般,*,*,*,構造,コウゾウ,コーゾー">構造</tok>
21 <tok id="10" feature="助詞,格助詞,一般,*,*,*,を,ヲ,ヲ">を</tok>
22 </chunk>
23 <chunk id="5" link="6" rel="D" score="1.335883" head="11" func="11">
24 <tok id="11" feature="動詞,自立,*,*,五段・タ行,基本形,持つ,モツ,モツ">持つ</tok>
25 </chunk>
26 <chunk id="6" link="7" rel="D" score="2.262625" head="12" func="13">
27 <tok id="12" feature="名詞,一般,*,*,*,文,ブン,ブン">文</tok>
28 <tok id="13" feature="助詞,格助詞,一般,*,*,*,を,ヲ,ヲ">を</tok>
29 </chunk>
30 <chunk id="7" link="8" rel="D" score="1.993750" head="15" func="15">
31 <tok id="14" feature="名詞,サ変接続,*,*,*,解析,カイセキ,カイセキ">解析</tok>
32 <tok id="15" feature="動詞,自立,*,*,サ変・スル,基本形,する,スル,スル">する</tok>

```

```

33 </chunk>
34 <chunk id="8" link="9" rel="D" score="1.854513" head="16" func="17">
35 <tok id="16" feature="名詞,非自立,一般,*,*,*,こと,コト,コト">こと</tok>
36 <tok id="17" feature="助詞,格助詞,一般,*,*,*,が,ガ,ガ">が</tok>
37 </chunk>
38 <chunk id="9" link="13" rel="D" score="0.124090" head="18" func="19">
39 <tok id="18" feature="動詞,自立,*,*,一段,基本形,できる,デキル,デキル">できる</tok>
40 >
41 <tok id="19" feature="助詞,接続助詞,*,*,*,と,ト,ト">と</tok>
42 </chunk>
43 <chunk id="10" link="11" rel="D" score="1.869991" head="22" func="23">
44 <tok id="20" feature="名詞,一般,*,*,*,人工,ジンコウ,ジンコー">人工</tok>
45 <tok id="21" feature="名詞,一般,*,*,*,知能,チノウ,チノー">知能</tok>
46 <tok id="22" feature="名詞,サ変接続,*,*,*,プログラム,プログラム,プログラム">プ
47 ログラム</tok>
48 <tok id="23" feature="助詞,連体化,*,*,*,の,ノ,ノ">の</tok>
49 </chunk>
50 <chunk id="11" link="12" rel="D" score="2.088981" head="24" func="25">
51 <tok id="24" feature="名詞,非自立,副詞可能,*,*,*,ため,タメ,タメ">ため</tok>
52 <tok id="25" feature="助詞,連体化,*,*,*,の,ノ,ノ">の</tok>
53 </chunk>
54 <chunk id="12" link="13" rel="D" score="1.876101" head="27" func="28">
55 <tok id="26" feature="名詞,一般,*,*,*,ヒューマン,ヒューマン,ヒューマン">ヒュー
56 マン</tok>
57 <tok id="27" feature="名詞,一般,*,*,*,インターフェース,インターフェース,インタ
58 ーフェース">インターフェース</tok>
59 <tok id="28" feature="助詞,格助詞,一般,*,*,*,を,ヲ,ヲ">を</tok>
60 </chunk>
61 <chunk id="13" link="14" rel="D" score="0.124090" head="31" func="32">
62 <tok id="29" feature="名詞,サ変接続,*,*,*,開発,カイハツ,カイハツ">開発</tok>
63 <tok id="30" feature="動詞,自立,*,*,サ変・スル,基本形,する,スル,スル">する</tok>
64 <tok id="31" feature="名詞,非自立,一般,*,*,*,の,ノ,ノ">の</tok>
65 <tok id="32" feature="助詞,格助詞,一般,*,*,*,に,ニ,ニ">に</tok>
66 </chunk>
67 <chunk id="14" link="-1" rel="D" score="0.000000" head="33" func="34">
68 <tok id="33" feature="動詞,自立,*,*,五段・タ行,連用形,役立つ,ヤクダチ,ヤクダチ">
69 役立つ</tok>
70 <tok id="34" feature="助動詞,*,*,*,特殊・マス,基本形,ます,マス,マス">ます</tok>
71 <tok id="35" feature="記号,句点,*,*,*,. . . ">.</tok>
72 </chunk>
73 </sentence>

```

上記出力結果の書式に関しては cabocha の公式インターネットサイトなどを参照のこと。

## 1.4 JUMAN：日本語形態素解析

JUMAN は、京都大学大学院情報学研究科で開発<sup>4</sup>された日本語形態素解析プログラムである。JUMAN に関する情報はインターネットサイト

<http://nlp.ist.i.kyoto-u.ac.jp/index.php?JUMAN>

で公開されている。

JUMAN を用いることで日本語の文章を解析して、文章の要素データを生成することができる。基本的に JUMAN はコマンドラインツールであり、日本語文章のテキストを標準入力から入力することで、文章の要素データを出力することができる。(次の例参照)

### ■ JUMAN の実行例

コマンドの書式： `juman`

この後、標準入力からの文書の入力が受け付けられ、処理の結果次のような文章の要素データが標準出力に出力される。

例. `juman` の実行

```
C: ¥Users ¥katsu>juman ← juman コマンドの投入
これは日本語の文です. ←日本語文の投入
これ これ これ 指示詞 7 名詞形態指示詞 1 * 0 * 0 NIL ←解析結果の表示
は は は 助詞 9 副助詞 2 * 0 * 0 NIL
日本 にほん 日本 名詞 6 地名 4 * 0 * 0 "代表表記:日本/にほん 地名:国"
@ 日本 につぼん 日本 名詞 6 地名 4 * 0 * 0 "代表表記:日本/にほん 地名:国"
語 ご 語 名詞 6 普通名詞 1 * 0 * 0 "代表表記:語/ご 漢字読み:音 カテゴリ:抽象物"
の の の 助詞 9 接続助詞 3 * 0 * 0 NIL
文 ぶん 文 名詞 6 普通名詞 1 * 0 * 0 "代表表記:文/ぶん 漢字読み:音 カテゴリ:抽象物"
です です だ 判定詞 4 * 0 判定詞 25 デス列基本形 27 NIL
. . . 特殊 1 句点 1 * 0 * 0 NIL
EOS
```

このように、文の構成要素（語）に切り離されて1行毎に出力される。各行の形式は空白区切りで、

表記 読み 原型 品詞 品詞細分類 活用例 活用例 意味情報

の順となっている。(詳しくは先のインターネットサイトを参照のこと)

JUMAN は標準入力からの読み込みがファイルの終端 (EOF) となった時点で終了する。OS のシェルから標準入力に対してファイルの終端を入力するには `CTRL+Z` と入力する。この操作で JUMAN が終了する。

## 1.5 KNP：日本語係り受け解析

KNP は、JUMAN による日本語文の形態素解析の結果を用いて、文の係り受け構造を解析するツールである。(開発元は JUMAN と同じである)

KNP はコマンドツールであり、標準入力から受け付けた JUMAN からの入力を解析して結果を標準出力に出力する。

次に示す `jtext-s.txt` のようなテキストファイルを JUMAN と KNP を用いて解析する例を示す。

サンプルテキスト：`jtext-s.txt`

```
1 | この文のような複雑な係り受け構造を持つ文を解析できると人工知能プログラムのためのヒューマンインターフェイスを開発するのに役立ちます。
```

このテキストファイルを次のようなコマンドで処理をする。

<sup>4</sup>知能情報学専攻 知能メディア講座 言語メディア分野 (工学部電気電子工学科) 黒橋・河原研究室



## 1.6 Open JTalk：テキスト読み上げ

Open JTalk は名古屋工業大学で開発された音声合成ソフトウェア<sup>5</sup>である。このソフトウェアは同大学が開発した hts\_engine API を用いて構築されており、与えられた辞書と音響モデルに従って、日本語のテキストデータを読み上げた音声データ（WAV 形式データ）を生成する。このソフトウェアを計算機環境にインストールすると、OS のコマンド open\_jtalk として実行できる。

Open JTalk のソースコード、日本語辞書、音響モデルなどがインターネットサイト

<http://open-jtalk.sourceforge.net/>

で公開されており入手できる。

### ■ open\_jtalk コマンドの基本的な使い方

```
open_jtalk -x 辞書ディレクトリ -m 音響モデル -s サンプリング周波数 -r 読み上げ速度の比率
 -ow 出力ファイル 入力用テキストファイル
```

「辞書ディレクトリ」には辞書関連データを収めたディレクトリのパスを、「音響モデル」にはモデルデータのファイルのパスを指定する。「サンプリング周波数」には Hz 単位の数値を指定する。「読み上げ速度の比率」には、システムが標準としている読み上げ速度に対する比率を数値（小数点付き）で指定する。「入力用テキストファイル」は読み上げ対象のテキストデータのファイルのパスを指定するが、これは標準入力から与えることもできる。

処理が正常に終了すると「出力ファイル」に指定したパスに WAV 形式のデータがファイルとして生成される。出力ファイルのファイル名の末尾には拡張子 '.wav' を付けておくべきである。

### 1.6.1 処理の例

#### 【Windows での例】

日本語文書が記述された入力ファイル jtest1.txt から、それを読み上げた結果の WAV 形式ファイル jtest1.wav を生成する方法の例を示す。Open JTalk のコマンドや辞書、音響モデルのファイルが次のようなディレクトリ階層に配置されているとする。

```
C:\OpJTalk
├── dic_utf.8 ←辞書関連のディレクトリ
│ ├── char.bin
│ ├── left-id.def
│ ├── matrix.bin
│ ├── pos-id.def
│ ├── rewrite.def
│ ├── right-id.def
│ ├── sys.dic
│ └── unk.dic
├── mei_angry.htsvoice ←音響モデルファイル
├── mei_bashful.htsvoice ←音響モデルファイル
├── mei_happy.htsvoice ←音響モデルファイル
├── mei_normal.htsvoice ←音響モデルファイル
├── mei_sad.htsvoice ←音響モデルファイル
└── open_jtalk.exe ← Open JTalk 本体
```

この環境で音響モデル mei\_normal.htsvoice に従って OpenJTalk コマンドを実行するには次のようなコマンドを投入する。

```
C:\OpJTalk\open_jtalk -x C:\OpJTalk\dic_utf.8 -m C:\OpJTalk\mei_normal.htsvoice
 -s 44100 -r 1.0 -ow jtest1.wav jtest1.txt
```

<sup>5</sup><http://software.web.nitech.ac.jp/>「研究室のソフトウェア」（名古屋工業大学 産学官連携センター）

## 1.7 Julius：音声認識

Julius は音声入力デバイスや音声データファイルから入力された音声を認識するためのソフトウェアである。Julius は国内の大学<sup>6</sup> や IPA<sup>7</sup> によって開発、保守されており、関連情報（ソフトウェア本体、ドキュメント等）は OSDN サイトの Julius ページ <http://julius.osdn.jp/> から入手できる。

Julius の機能は、各種プログラミング言語用の API という形（ライブラリという形）で利用することができる。また Julius は OS のコマンドとして実行することもでき、標準入出力やファイル、あるいは TCP/IP の通信を介して他のソフトウェアと連携させることができる。本書ではコマンドの基本的な使用方法を紹介し、音声入力デバイス（マイクからの入力）と音声データファイル（WAV 形式ファイル）から入力された音声を認識してテキストデータとして出力する過程を例示する。

### ■ 入手するパッケージ

先に挙げたインターネットサイトからディクテーションキットをダウンロード<sup>8</sup> して展開する。（図 1）

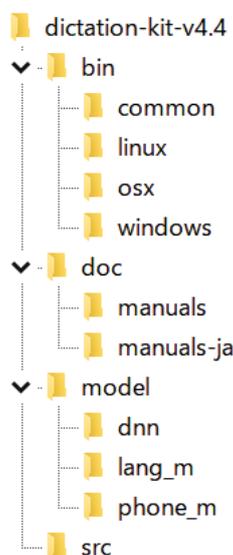


図 1: ディクテーションキットの中身（Ver.4.4）

このパッケージには Julius 本体をはじめ、音声認識に必要なとなるデータ（音響モデル、単語辞書、言語モデル）が含まれている。展開して出来上がったディレクトリ（図 1 の例では「dictation-kit-v4.4」フォルダ）はディスクの適切なディレクトリに配置しておく。

図 1 の例では「bin」フォルダ配下に Julius 関連の実行可能なプログラムファイル（各種 OS 用）が収められているので、使用する OS に合わせてコマンドサーチパスの設定をしておくのが良い。

以下、Ver.4.4 のディクテーションキットを前提として解説する。

### ■ Julius を利用するための基礎知識

Julius の動作を正しく理解して有効に利用するためには音声認識に関する基礎知識を有することが望ましいが、本書では Julius を最低限の範囲で動作させるために必要となる最小限の解説にとどめる。

Julius では HMM（隠れマルコフモデル）で状態遷移をモデル化する手法に基いて音声認識を行う。HMM としては GMM-HMM（Gaussian Mixture Model）と DNN-HMM（深層ニューラルネットワークモデル）の 2 種類のモデルから選択して利用することができ、Julius の起動時に必要となるモデルデータを指定する。これら 2 種類のモデルの違いとしては概ね次の通りである。

<sup>6</sup>京都大学 河原研究室、奈良先端科学技術大学院大学 鹿野研究室、名古屋工業大学 Julius 開発チーム

<sup>7</sup>独立行政法人情報処理推進機構（経済産業省所管）

<sup>8</sup>Ver.4.4 の場合、ZIP アーカイブ形式で 407MB、展開すると 830MB のサイズになることを予め留意すること。

## 1) GMM

認識精度はやや低いが発行時の CPU への負荷が低い。

## 2) DNN

CPU への負荷は大きいが発行精度が高い。

どちらのモデルを使用するかは、Julius を利用する計算機環境と処理の目的から判断する。

### 1.7.1 動作テスト

ディクテーションキットに含まれるファイルを使用して Julius の動作をテストする方法を紹介する。パッケージのフォルダにはテスト実行用のバッチファイル<sup>9</sup>などが含まれており、それらを利用して音声認識のテスト（デモンストレーション）を行うことができる。

#### 【Windows で動作テストを実行する例】

Windows 用の起動バッチファイルとして下記のようなファイルがパッケージに含まれている。

- 1) run-win-dnn.bat : DNN による音声認識
- 2) run-win-dnncli.bat : DNN による音声認識（クライアントモードで実行）
- 3) run-win-gmm.bat : GMM による音声認識

この内、1) のバッチファイルを起動する例を示す。

音声認識処理に先立って、マイクを計算機環境に接続して音声入力が機能することを確認する。この後、コマンドプロンプトウィンドウを開いてカレントディレクトリをディクテーションキットのディレクトリに移動してバッチファイルを起動する。

例.

```
run-win-dnn [Enter] ←バッチの起動
```

起動直後に Julius からのメッセージが多数表示された後、次のような表示となる。

```
Notice for feature extraction (01).

* Cepstral mean and variance norm. for real-time decoding: *
* initial mean loaded from file, updating per utterance. *
* static variance loaded from file, apply it constantly. *
* NOTICE: The first input may not be recognized, since *
* cepstral mean is unstable on startup. *

Stat: adin_portaudio: audio cycle buffer length = 256000 bytes
Stat: adin_portaudio: sound capture devices:
1 [MME: Microsoft サウンド マッパー - Input]
2 [MME: マイク (2- USB PnP Audio Device)]
3 [MME: マイク (Realtek High Definition)]
6 [Windows DirectSound: プライマリ サウンド キャプチャ ドライバー]
7 [Windows DirectSound: マイク (2- USB PnP Audio Device)]
8 [Windows DirectSound: マイク (Realtek High Definition Audio)]
Stat: adin_portaudio: APIs: DirectSound MME
Stat: adin_portaudio: -- DirectSound selected
Stat: adin_portaudio: [Windows DirectSound: プライマリ サウンド キャプチャ ドライバー]
Stat: adin_portaudio: (you can specify device by "PORTAUDIO_DEV_NUM=number")
Stat: adin_portaudio: try to set default low latency from portaudio: 0 msec
Stat: adin_portaudio: latency was set to 0.000000 msec
pass1_best: <input rejected by short input>
<<< please speak >>>
```

図 2: run-win-dnn 起動直後の表示

ウィンドウの最下行に “<<< please speak >>>” と表示されたら音声入力が受け付けられるので、マイクに向かって短く（10 秒程度）発話してみる。ここで、

「音声認識のテストをしています」

と発話した場合の認識例（コマンドプロンプトウィンドウの表示内容）を示す。

<sup>9</sup>処理を実行するために必要な各種設定を記述したファイル。

```
pass1.best: < input rejected by short input >
pass1.best: 温泉 認識 の、 テスト して います
sentence1: 音声 認識 の、 テスト を して います。
<<< please speak >>>
```

音声認識の結果が表示されている。

### バッチファイルの内容について

ここで使用したバッチファイル run-win-dnn.bat の内容は次のようなものである。

```
. %bin%windows%julius.exe -C main.jconf -C am-dnn.jconf -demo
 -charconv utf-8 sjis -dnnconf julius.dnnconf
```

Julius 本体を起動するには多くのオプションを指定する必要があり、このバッチファイルではそのための処理が記述されている。バッチファイルの中で、次に示す記述は各種のオプション指定を記述するファイルであり、更に詳細なオプションが記述されている。

```
main.jconf
am-dnn.jconf
julius.dnnconf
```

参考) これらのファイルの内容を調べることで、オプション指定の方法に関するヒントが得られる。オプションの指定に関する詳細については公式のドキュメントを参照のこと。

### 1.7.2 WAV 形式音声ファイルの認識

WAV 形式の音声データファイルを入力として音声認識を行う例を示す。次に示すような筆者が読み上げた音声のデータを認識する過程を取り上げて説明する。

#### 使用する音声データ

```
snd01.wav : 「音声認識のテストをしています」
snd02.wav : 「結果はどうでしょうか」
```

処理はディクテーションキットのディレクトリで行うことを前提とし、コマンドプロンプトウィンドウでバッチ処理を行う際のカレントディレクトリもディクテーションキットのディレクトリであることを前提とする。また OS は Windows を前提とする。

#### 手順1：バッチファイルの作成

先の動作テストで使用したバッチファイルを参考にして次のような内容のバッチファイル to-file.bat を作成する。

```
. %bin%windows%julius.exe -C myconf.jconf -C am-dnn.2.jconf
 -dnnconf julius.dnnconf -charconv utf-8 sjis
```

#### 手順2：設定ファイルの作成

バッチファイル to-file.bat にある myconf.jconf はディクテーションキットに含まれる設定ファイル main.jconf を参考にして次のように作成する。

## 設定ファイル：myconf.jconf

```
1 ## ログファイルの設定など
2 -logfile log.txt
3 -quiet
4
5 ## 入力ファイルの設定など
6 -input rawfile
7 -filelist flist.txt
8 -spsegment
9
10 ## 認識結果のファイル出力
11 -outfile
12
13 ## 単語2-gram,3-gramファイル
14 -d model/lang_m/bccwj.60k.bigram
15
16 ## 単語辞書ファイル
17 -v model/lang_m/bccwj.60k.htkdic
18
19 ##### 探索パラメータ #####
20 -b 1500
21 -b2 100
22 -s 500
23 -m 10000
24 -n 30
25 -output 1 # 第2パスで見つかった文のうち出力する数（文数）
26 -zmeanframe # フレーム単位のDC成分除去を行う（HTKと同処理）
27
28 ##### 短時間瞬時入力の棄却 #####
29 -rejectshort 800 # 指定ミリ秒以下の長さの入力を棄却する
```

ファイルからの音声データ入力に関する設定で重要な記述が 6, 7, 11 行目である。-input rawfile というオプションを与えることで WAV 形式ファイルからの入力となる。また -filelist **入力ファイル名リストのファイル名** という記述によって、入力用の WAV 形式ファイルのファイル名 Julius に与えることができる。

### 手順3：入力ファイル名リストの作成

今回は「入力ファイル名リスト」のファイル名は flist.txt（設定ファイル7行目）で、内容は次のようなものである。

```
snd01.wav
snd02.wav
```

設定ファイルの 11 行目にある -outfile という記述は、認識結果をテキストファイルとして出力することを指定する。この際の実出力ファイルの名前は、入力ファイルと同じファイル名で、拡張子が '.out' となったものである。従って今回の場合は出力ファイルは、

```
snd01.out
snd02.out
```

の2つとなる。

### 手順4：バッチファイルの実行

実行用のバッチファイル to-file.bat をコマンドプロンプトのウィンドウで実行する。

以上の処理が正常に終了すると、snd01.out、snd02.out に認識結果が出力される。実行結果の例を次に示す。

### 認識結果 1 : snd01.out

```
1 sentence1: 音声 認識 の、 テスト を して います。
2 wseq1: <s> 音声+名詞 認識+名詞 の+助詞、 +補助記号 テスト+名詞 を+助詞 し+動詞 て+
 助詞 い+動詞 ます+助動詞 </s>
3 phseq1: sp_S | o_B N_I s_I e:_E | n_B i_I N_I sh_I i_I k_I i_E | n_B o_E | sp_S |
 t_B e_I s_I u_I t_I o_E | o_S | sh_B i_E | t_B e_E | i_S | m_B a_I s_I u_E |
 sp_S
4 cmscore1: 0.902 0.844 0.894 0.312 0.790 0.992 0.215 0.988 0.995 0.543 0.769 1.000
5 score1: 421.860229 (AM: 716.412537 LM: -294.552307)
```

### 認識結果 2 : snd02.out

```
1 sentence1: 結果 は、 どう でしょう か。
2 wseq1: <s> 結果+名詞 は+助詞、 +補助記号 どう+副詞 でしょう+助動詞 か+助詞 </s>
3 phseq1: sp_S | k_B e_I q_I k_I a_E | w_B a_E | sp_S | d_B o:_E | d_B e_I sh_I o:_E
 | k_B a_E | sp_S
4 cmscore1: 0.591 0.972 0.925 0.425 0.848 0.980 0.733 1.000
5 score1: 509.048126 (AM: 665.216736 LM: -156.168594)
```

各出力ファイルにおいて、行頭が 'sentence1:' となる行が認識結果で、行頭が 'wseq1:' となる行が解析結果である。

## ■ その他

本書で紹介した内容は Julius の機能の部分的な紹介に過ぎない。利用者が作成したプログラムと Julius のプログラムを連携させるための方法の詳細に関しては、公式ドキュメントをはじめとする各種ドキュメントを参照のこと。

## 1.8 OpenSSL：暗号化，復号，電子署名

OpenSSL は通信の暗号化やメッセージの暗号化，ハッシュ生成のための関数ライブラリある．またそれらを用いた機能を実行するためのコマンド `openssl` も提供している．OpenSSL に関する情報はインターネットサイト

<https://www.openssl.org/>

で公開されている．OpenSSL がサポートする暗号化通信プロトコルは，

SSL 2.0, 3.0          TLS 1.0, 1.1, 1.2          DTLS 1.0, 1.2

である．また，文書を暗号化する際のアルゴリズムは，

Blowfish, Camellia, DES, RC2, RC4, RC5, SEED, IDEA, AES

が，ハッシュアルゴリズムとしては，

MD5, MD2, SHA-1, SHA-2, MDC-2

が利用できる．OpenSSL は公開鍵暗号方式の暗号化機能も提供しており，アルゴリズムとして，

RSA 暗号, DSA, Diffie-Hellman 鍵共有

が利用できる．

### 1.8.1 公開鍵暗号方式による暗号化の方法

公開鍵暗号方式は，メッセージ（ファイル）の暗号化と復号にそれぞれ異なる鍵を使用する暗号化方式であり，この形態から**非対称鍵暗号方式**とも呼ばれる．公開鍵暗号方式には**鍵の所有者**の存在が前提とされている．すなわち，暗号化処理を利用する者は，暗号化に使用する鍵である**公開鍵**と，復号のために使用する鍵である**秘密鍵**を作成して用意する．そして公開鍵を第三者に渡しておき，その第三者から鍵の所有者にメッセージやデータを送信する際に公開鍵を用いて暗号化してもらう．これによって，第三者から鍵の所有者に向けてのデータ送信の秘匿化が実現する．暗号化されたメッセージやデータを受け取った鍵の所有者は，秘密鍵を用いてそれを復号する．**秘密鍵**はその名が示すとおり，鍵の所有者のみが保持するものであり，決して第三者に開示してはならない．

OpenSSL には公開鍵，秘密鍵を生成するための機能と，それらを用いて暗号化と復号を行う機能が提供されており，`openssl` コマンドによりそれらの機能が利用できる．ここでは，RSA 暗号アルゴリズムを用いた公開鍵暗号方式の使用方法について説明する．

#### 1.8.1.1 公開鍵と秘密鍵の生成

`openssl` コマンドに引数 `genrsa` を与えることで秘密鍵を生成することができる．

例．秘密鍵の生成

```
openssl genrsa > secret.key
```

この結果，秘密鍵がファイル `secret.key` として作成される．鍵を生成する際に**鍵の長さ**（ビット長）を指定することができる．鍵は長い程安全である．

例．ビット長を指定した秘密鍵の生成

```
openssl genrsa 2048 > secret.key
```

この結果，2048 ビットの秘密鍵がファイル `secret.key` として作成される．

第三者に開示する**公開鍵**は秘密鍵を元にして作成する．

例．秘密鍵 `secret.key` から公開鍵 `public.key` を作成する

```
openssl rsa -pubout < secret.key > public.key
```

このように openssl コマンドの引数に `rsa` と、オプション `-pubout` を与えて実行する。

### 1.8.1.2 公開鍵による暗号化

先の例に引き続き、作成した公開鍵 `public.key` を使用してメッセージデータ `original.dat` を暗号化して暗号データ `encrypted.dat` を生成する例を示す。

例. 公開鍵を用いた暗号化

```
openssl rsautl -encrypt -pubin -inkey public.key < original.dat > encrypted.dat
```

このように openssl コマンドの引数に `rsautl` と、オプション `-encrypt`, `-pubin`, `-inkey` を与えて実行する。オプション `-inkey` の後ろには公開鍵のファイル名を指定する。作成された暗号データ `encrypted.dat` の内容は可読性の無いものになっている。

### 1.8.1.3 秘密鍵による復号

先の例に引き続き、作成した秘密鍵 `secret.key` を使用して暗号データ `encrypted.dat` を復号して `decrypted.dat` を生成する例を示す。

例. 秘密鍵を用いた復号

```
openssl rsautl -decrypt -inkey secret.key < encrypted.dat > decrypted.dat
```

このように openssl コマンドの引数に `rsautl` と、オプション `-decrypt`, `-inkey` を与えて実行する。オプション `-inkey` の後ろには秘密鍵のファイル名を指定する。作成されたデータ `decrypted.dat` の内容は暗号化前のデータと同じ内容となっている。

## 1.8.2 公開鍵暗号方式による電子署名の作成

公開鍵暗号方式による暗号化は、第三者から鍵の所有者に向けてのデータの送信を秘匿化することが目的である。これとは別に、鍵の所有者が第三者に向けてデータを配信する場合に、配信者が鍵の所有者であることを保証し、かつ、配信されたデータが改竄されていないこと（真正性）を保証するための方法として電子署名の利用がある。

電子署名は、鍵の所有者が**配信するデータ**と**自身の秘密鍵**から作成するものであり、当該データを配信する際に添付するものである。

電子署名の利用の手順は次の通りである。

1. 鍵の所有者が秘密鍵を使って、配信対象のデータのための電子署名を作成する。

`original.dat` の真正性を保証するために電子署名 `sign.dat` を作成するには、openssl コマンドを用いて次のように処理する。

```
openssl dgst -sha1 -sign secret.key < original.dat > sign.dat
```

これで、`original.dat` の真正性を保証する電子署名 `sign.dat` が作成される。この例では、`secret.key` は秘密鍵である。

2. データと電子署名の両方を第三者に配信する。

3. 電子署名を用いてデータの真正性を検査する。（受信した第三者の作業）

openssl コマンドを用いて次のように処理する。

```
openssl dgst -sha1 -verify public.key -signature sign.dat < original.dat
```

この例では `public.key` は公開鍵である。データの真正性が確認できた場合は、

```
Verified OK
```

と表示され、そうでない場合は、

## Verification Failure

と表示される.

この例のように、電子署名の生成やデータの真正性の検査をする際には openssl コマンドの引数には dgst を与える。また電子署名生成に用いるハッシュアルゴリズムを指定することができ、-sha1 の他にも -md5, -sha256, -sha512 などが指定できる。

## 2 ライブラリ

### 2.1 GMP/MPFR：任意多倍長演算

C や Java で標準的に扱える数値の型はビット長が固定されており、整数として扱える数値の桁数や、浮動小数点数として扱える数値の有効桁数（精度）には限界がある。従って、それを超える桁数の数値を扱う<sup>10</sup>には、特別なデータ構造を定義して、それを扱うための関数やメソッドを実装する必要がある。ここで紹介する GMP（GNU Multi-Precision Library）と MPFR は、任意精度の数値演算を実行するためのライブラリであり、C 言語と C++ 言語で利用できるが、それ以外の各種言語で利用するためのラッパーも用意されている。

GMP は任意精度の整数、有理数、浮動小数点数を扱うためのライブラリであり、インターネットサイト

<https://gmplib.org/>

でソースコードやドキュメントが公開されている。GMP 自体には各種の数学関数の値を求める機能は提供されておらず、GMP を用いて開発されたライブラリ MPFR として各種の数学関数が提供されている。MPFR に関しては、インターネットサイト <http://www.mpfr.org/> でソースコードやドキュメントが公開されている。

GMP と MPFR は別々のライブラリであり、C/C++ 言語で利用する際にもインクルードするヘッダファイルやリンクするライブラリは別のものとして扱われる。本書ではこれらライブラリの使用方法を導入的に紹介する。詳しくは各ライブラリのドキュメントを参照のこと。

#### 2.1.1 GMP

GMP には任意精度の整数、有理数、浮動小数点数の値を保持するオブジェクトのデータ型としてそれぞれ `mpz_t`、`mpq_t`、`mpf_t` がある。<sup>11</sup>

GMP を用いて行うことは概ね次の 3 種類の処理である。

1. オブジェクトの宣言と初期化  
`mpz_t`、`mpq_t`、`mpf_t` といった GMP のオブジェクトは宣言した後、初期化する必要がある。
2. データの変換  
C の各種データ（`long`、`double`、`char*` など）と GMP のオブジェクトの値を相互に変換する機能。
3. 算術演算など  
加減乗除、開平をはじめとする基本的な演算処理。
4. オブジェクトの開放  
不要になったオブジェクトの記憶域を開放する。

オブジェクトの初期化と値の変換に関する処理について重要なものを表 4~5 に挙げる。

表 4: オブジェクトの初期化

| 対象の型               | 書き方                                                                         | 説明                                                                                                                                 |
|--------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <code>mpz_t</code> | <code>mpz_init(x)</code><br><code>mpz_inits(x1, x2, ..., (mpz_t *)0)</code> | <code>mpz_t</code> 型の <code>x</code> を初期化する。<br><code>mpz_t</code> 型の <code>x1, x2, ...</code> を初期化する。<br>初期値は 0 となる。              |
| <code>mpq_t</code> | <code>mpq_init(x)</code><br><code>mpq_inits(x1, x2, ..., (mpq_t *)0)</code> | <code>mpq_t</code> 型の <code>x</code> を初期化する。<br><code>mpq_t</code> 型の <code>x1, x2, ...</code> を初期化する。<br>初期値は 0/1 となる。            |
| <code>mpf_t</code> | <code>mpf_init2(x, p)</code>                                                | <code>mpf_t</code> 型の <code>x</code> を <code>p</code> ビット長の精度で初期化する。<br>初期値は 0 となる。（ <code>p</code> の型は <code>mp_bitcnt_t</code> ） |

<sup>10</sup>情報セキュリティ関連の処理（暗号化や復号など）や、数理科学系分野における力学系の高精度シミュレーションなどを行う際に必須の機能である。

<sup>11</sup>`mpz_t` は整数を表す  $\mathbb{Z}$  を、`mpq_t` は有理数を表す  $\mathbb{Q}$  を命名の由来とする。

表 5: 値の変換

| 変換前の<br>オブジェクト | mpz_t 型の x へ              | mpq_t 型の x へ                                      | mpf_t 型の x へ              |
|----------------|---------------------------|---------------------------------------------------|---------------------------|
| long n         | mpz_set_si( x, n )        | mpq_set_si( x, n, d )<br>x ← n / (unsigned long)d | mpf_set_si( x, n )        |
| double n       | mpz_set_d( x, n )         | mpq_set_d( x, n )                                 | mpf_set_d( x, n )         |
| mpz_t n        | mpz_set( x, n )           | mpq_set_z( x, n )                                 | mpf_set_z( x, n )         |
| mpq_t n        | mpz_set_q( x, n )         | mpq_set( x, n )                                   | mpf_set_q( x, n )         |
| mpf_t n        | mpz_set_f( x, n )         | mpq_set_f( x, n )                                 | mpf_set( x, n )           |
| (char *)n      | mpz_set_str( x, n, Base ) | mpq_set_str( x, n, Base )                         | mpf_set_str( x, n, Base ) |

※ Base には int 型の整数で基数を指定する。

表 6: GMP の型から文字列 (char \*)s への変換

| 変換前の<br>オブジェクト | 書き方                                  |
|----------------|--------------------------------------|
| mpz_t n        | mpz_get_str( s, Base, n )            |
| mpq_t n        | mpq_get_str( s, Base, n )            |
| mpf_t n        | mpf_get_str( s, &E, Base, Digit, n ) |

#### [表 5,6 の補足]

Base は基数を指定する整数で, int 型で与える。E は mp\_exp\_t 型の変数で, 処理の結果得られた文字列の小数点の位置を表す数値 (整数) が取得される。引数には E のアドレスを渡す。

Digit は size\_t 型の整数値で, 文字列として取得する数値の桁数を指定する。Digit の値として 0 を指定すると, 最も正確な値が取られる最大の桁数が自動的に設定される。

#### ■ mpz\_t オブジェクトの精度と初期化について

mpz\_t オブジェクトを初期化するに当たって, 精度を暗黙値として設定する方法がある。具体的には関数 mpf\_set\_default\_prec を使って,

```
mpf_set_default_prec(精度)
```

とすることで初期化のための精度を事前に設定しておくことができる。(精度の型は mp\_bitcnt\_t) この関数呼び出しの後, 複数の mpf\_t オブジェクト a, b, c, ... に対して mpf\_inits 関数を使って

```
mpf_inits(a, b, c, ..., (mpf_t *)0)
```

として一括して初期化することができる。

#### 2.1.1.1 GMP で利用できる関数 (一部)

##### ■ 加算

###### • mpz\_t の加算

```
mpz_add_ui(y, x, n) : (mpz_t)y ← (mpz_t)x + (unsigned long)n
mpz_add(y, x, n) : (mpz_t)y ← (mpz_t)x + (mpz_t)n
```

###### • mpq\_t の加算

```
mpq_add(y, x, n) : (mpq_t)y ← (mpq_t)x + (mpq_t)n
```

###### • mpf\_t の加算

```
mpf_add_ui(y, x, n) : (mpf_t)y ← (mpf_t)x + (unsigned long)n
mpf_add(y, x, n) : (mpf_t)y ← (mpf_t)x + (mpf_t)n
```

## ■ 減算

### • mpz\_t の減算

$\text{mpz\_sub\_ui}(y, x, n) : (\text{mpz\_t})y \leftarrow (\text{mpz\_t})x - (\text{unsigned long})n$   
 $\text{mpz\_ui\_sub}(y, x, n) : (\text{mpz\_t})y \leftarrow (\text{unsigned long})x - (\text{mpz\_t})n$   
 $\text{mpz\_sub}(y, x, n) : (\text{mpz\_t})y \leftarrow (\text{mpz\_t})x - (\text{mpz\_t})n$

### • mpq\_t の減算

$\text{mpq\_sub}(y, x, n) : (\text{mpq\_t})y \leftarrow (\text{mpq\_t})x - (\text{mpq\_t})n$

### • mpf\_t の減算

$\text{mpf\_sub\_ui}(y, x, n) : (\text{mpf\_t})y \leftarrow (\text{mpf\_t})x - (\text{unsigned long})n$   
 $\text{mpf\_ui\_sub}(y, x, n) : (\text{mpf\_t})y \leftarrow (\text{unsigned long})x - (\text{mpf\_t})n$   
 $\text{mpf\_sub}(y, x, n) : (\text{mpf\_t})y \leftarrow (\text{mpf\_t})x - (\text{mpf\_t})n$

## ■ 乗算

### • mpz\_t の乗算

$\text{mpz\_mul\_si}(y, x, n) : (\text{mpz\_t})y \leftarrow (\text{mpz\_t})x * (\text{long})n$   
 $\text{mpz\_mul}(y, x, n) : (\text{mpz\_t})y \leftarrow (\text{mpz\_t})x * (\text{mpz\_t})n$

### • mpq\_t の乗算

$\text{mpq\_mul}(y, x, n) : (\text{mpq\_t})y \leftarrow (\text{mpq\_t})x * (\text{mpq\_t})n$

### • mpf\_t の乗算

$\text{mpf\_mul\_ui}(y, x, n) : (\text{mpf\_t})y \leftarrow (\text{mpf\_t})x * (\text{unsigned long})n$   
 $\text{mpf\_mul}(y, x, n) : (\text{mpf\_t})y \leftarrow (\text{mpf\_t})x * (\text{mpf\_t})n$

## ■ 除算

### • mpq\_t の除算

$\text{mpq\_div}(y, x, n) : (\text{mpq\_t})y \leftarrow (\text{mpq\_t})x / (\text{mpq\_t})n$

### • mpf\_t の除算

$\text{mpf\_div\_ui}(y, x, n) : (\text{mpf\_t})y \leftarrow (\text{mpf\_t})x / (\text{unsigned long})n$   
 $\text{mpf\_ui\_div}(y, x, n) : (\text{mpf\_t})y \leftarrow (\text{unsigned long})x / (\text{mpf\_t})n$   
 $\text{mpf\_div}(y, x, n) : (\text{mpf\_t})y \leftarrow (\text{mpf\_t})x / (\text{mpf\_t})n$

## ■ 比較

表 7 に値の大きさを比較する関数の一部を挙げる。

表 7: 値の比較:  $x_i n \rightarrow$  正の整数,  $x=n \rightarrow 0$ ,  $x_j n \rightarrow$  負の整数

| x の型    | long n                             | double n        | mp*_t n<br>(n は x と同じ型) |
|---------|------------------------------------|-----------------|-------------------------|
| mpz_t x | mpz_cmp_si(x, n)                   | mpz_cmp_d(x, n) | mpz_cmp(x, n)           |
| mpq_t x | mpq_cmp_si(x, n, d)<br>(n/d との比較※) |                 | mpq_cmp(x, n)           |
| mpf_t x | mpf_cmp_si(x, n)                   | mpf_cmp_d(x, n) | mpf_cmp(x, n)           |

※ d は unsigned long

## ■ その他

表 8 にその他の関数 (一部) を挙げる。

表 8: その他の関数

| 対象の型       | 正負判定<br>正:1, 零:0, 負:-1 | 正負反転<br>$y = -x$ | 絶対値<br>$y =  x $ |
|------------|------------------------|------------------|------------------|
| mpz_t x, y | int mpz_sgn( x )       | mpz_neg( y, x )  | mpz_abs( y, x )  |
| mpq_t x, y | int mpq_sgn( x )       | mpq_neg( y, x )  | mpq_abs( y, x )  |
| mpf_t x, y | int mpf_sgn( x )       | mpf_neg( y, x )  | mpf_abs( y, x )  |

※ 正負判定は関数の戻り値を見る

表 9: オブジェクトの記憶域を開放する関数

| 関数                                                          | 説明                                                  |
|-------------------------------------------------------------|-----------------------------------------------------|
| mpz_clear( mpz_t n )<br>mpz_clears( a, b, ..., (mpz_t *)0 ) | mpz_t n の記憶域を開放する。<br>mpz_t 型の a, b, ... の記憶域を開放する。 |
| mpq_clear( mpq_t n )<br>mpq_clears( a, b, ..., (mpq_t *)0 ) | mpq_t n の記憶域を開放する。<br>mpq_t 型の a, b, ... の記憶域を開放する。 |
| mpf_clear( mpf_t n )<br>mpf_clears( a, b, ..., (mpf_t *)0 ) | mpf_t n の記憶域を開放する。<br>mpf_t 型の a, b, ... の記憶域を開放する。 |

## ■ オブジェクトの開放

不要になったオブジェクトは表 9 に挙げるような関数を使用して記憶域を開放する。

ここで紹介するもの以外の関数も多数あるため、公式のドキュメントを参照のこと。

### 2.1.1.2 サンプルプログラム

#### ■ 任意桁数の整数の計算

100 の階乗 (100!) を求めるプログラムを bn\_gmp01.c に示す。

プログラム: bn\_gmp01.c

```

1 #include <stdio.h>
2 #include <gmp.h>
3
4 int main()
5 {
6 int i;
7 char s[1024];
8 mpz_t n; /* 任意精度整数の宣言 */
9
10 mpz_init(n); /* 初期化 */
11 mpz_set_si(n, 1); /* 1 をセット */
12 for (i = 2; i < 100; i++) {
13 mpz_mul_si(n, n, i); /* n = n * i の計算 */
14 }
15 mpz_get_str(s, 10, n); /* 文字列に変換 */
16 printf("100!=%s\n", s); /* 文字列の表示 */
17
18 mpz_clear(n); /* 記憶域の開放 */
19 }

```

### 2.1.1.3 プログラムの実行に際して

GMP を利用するアプリケーションプログラムを作成するに当たって、ヘッダファイル gmp.h を読み込む必要がある。具体的にはソースプログラムの冒頭に、

```
#include <gmp.h>
```

と記述する必要がある。また、ソースプログラムを翻訳、結合する際には、GMP のライブラリの結合をコンパイラ



ていることを意味している。

## 2.1.2 MPFR

MPFR は GMP を用いて構築されたライブラリであり、GMP が提供していない高度な数学関数が多数実装されている。MPFR の扱い方は基本的には GMP に倣ったものとなっており、ライブラリの利用は概ね次の 3 種類の処理に分類することができる。

### 1. オブジェクトの宣言と初期化

MPFR のデータ型 `mpfr_t` のオブジェクトを宣言した後、それらを初期化する。

### 2. データの変換

C の各種データ (`long`, `double`, `char*` など) や GMP の各種オブジェクトと値を相互に変換する。

### 3. 演算処理

算術演算, 数学関数などの演算。

## ■ `mpfr_t` オブジェクトの初期化

`mpfr_t` のオブジェクト `x` がある場合、これを 512 ビット長の精度を持つものとして初期化するには `mpfr_init2` 関数を用いて、

```
mpfr_init2(x, 512)
```

とする。第 2 引数には整数で精度を与えるが、より正確には `mpfr_prec_t` 型の値として与える。

複数の `mpfr_t` のオブジェクト `m1`, `m2`,... を一度に初期化するには `mpfr_inits2` 関数を用いて、

```
mpfr_inits2(512, m1, m2, ..., (mpfr_ptr)0)
```

とする。この関数は最初の引数に精度を指定し、最後の引数に `(mpfr_ptr)0` を与える。

## ■ 値の変換

`mpfr_t` のオブジェクトと、他の型のオブジェクトや変数との間で値を変換する関数の一部を表 10 に挙げる。

表 10: 各種の型の値 `n` と `mpfr_t` `x` の間で変換を行う関数 (一部)

| 変換元                        | <code>x ← n</code>                           | <code>n ← x</code>                                          |
|----------------------------|----------------------------------------------|-------------------------------------------------------------|
| <code>long n</code>        | <code>mpfr_set_si( x, n, Rnd )</code>        | <code>n = mpfr_get_si( x, Rnd )</code>                      |
| <code>double n</code>      | <code>mpfr_set_d( x, n, Rnd )</code>         | <code>n = mpfr_get_d( x, Rnd )</code>                       |
| <code>long double n</code> | <code>mpfr_set_ld( x, n, Rnd )</code>        | <code>n = mpfr_get_ld( x, Rnd )</code>                      |
| <code>mpz_t n</code>       | <code>mpfr_set_z( x, n, Rnd )</code>         | <code>mpfr_get_z( n, x, Rnd )</code>                        |
| <code>mpq_t n</code>       | <code>mpfr_set_q( x, n, Rnd )</code>         |                                                             |
| <code>mpf_t n</code>       | <code>mpfr_set_f( x, n, Rnd )</code>         | <code>mpfr_get_f( n, x, Rnd )</code>                        |
| <code>char *n</code>       | <code>mpfr_set_str( x, n, Base, Rnd )</code> | <code>mpfr_get_str( n, &amp;E, Base, Digit, x, Rnd )</code> |

### [表 10 の補足]

`Base` は基数を指定する整数で、`int` 型で与える。`E` は `mpfr_exp_t` 型の変数で、処理の結果得られた文字列の小数点の位置を表す数値 (整数) が取得される。引数には `E` のアドレスを渡す。`Digit` は `size_t` 型の数値で、文字列として取得する数値の桁数を指定する。`Digit` に 0 を与えると、信頼できる範囲の最大限の桁数で文字列データが得られる。

`Rnd` には `mpfr_rnd_t` 型の値で丸め (Rounding Mode) を指定する。具体的には表 11 のようなものが定義されており、それを指定する。

表 11: 丸め (Rounding Mode)

| Mode      | 説明                                              |
|-----------|-------------------------------------------------|
| MPFR_RNDN | 最近接丸め. (推奨)                                     |
| MPFR_RNDA | 最近接丸め. 0 から遠い方向に丸める.                            |
| MPFR_RNDZ | 0 に近い方向に丸める. (切り捨て: truncation)                 |
| MPFR_RNDU | $+\infty$ の方向に丸める. (切り上げ: rounding up, ceiling) |
| MPFR_RNDD | $-\infty$ の方向に丸める. (切り下げ: rounding down, floor) |

(IEEE-754 2008 準拠)

表 12: オブジェクトの記憶域を開放する関数 (MPFR)

| 関数                                      | 説明                             |
|-----------------------------------------|--------------------------------|
| mpfr_clear( mpfr_t n )                  | mpfr_t n の記憶域を開放する.            |
| mpfr_clears( a, b, ..., (mpfr_ptr *)0 ) | mpfr_t 型の a, b, ... の記憶域を開放する. |

## ■ オブジェクトの開放

不要になったオブジェクトは表 12 に挙げるような関数を使用して記憶域を開放する.

ここで紹介するもの以外の関数も多数あるため, 公式のドキュメントを参照のこと.

### 2.1.2.1 サンプルプログラム

$\pi$  から  $\frac{\pi}{6}$  を求め, 更に  $\sin\left(\frac{\pi}{6}\right)$  と  $\cos\left(\frac{\pi}{6}\right)$  を求め, それを用いて  $\sqrt{\sin^2\left(\frac{\pi}{6}\right) + \cos^2\left(\frac{\pi}{6}\right)}$  を求める

プログラム bn\_mpfr01.c を示す.

プログラム: bn\_mpfr01.c

```

1 #include <stdio.h>
2 #include <mpfr.h>
3
4 int main()
5 {
6 char st[2048];
7 mpfr_t s, c, p, p6, s2, c2, l, norm;
8 mpfr_exp_t e;
9
10 mpfr_init2(p, 512);
11 mpfr_inits2(512, p6, s, c, s2, c2,
12 1, norm, (mpfr_ptr)0);
13
14 mpfr_const_pi(p, MPFR_RNDN);
15 mpfr_div_si(p6, p, 6, MPFR_RNDN);
16
17 mpfr_get_str(st, &e, 10, (size_t)0, p, MPFR_RNDN);
18 printf("Pi=%s(point:%d)\n\n",st,e);
19
20 mpfr_sin(s, p6, MPFR_RNDN);
21 mpfr_get_str(st, &e, 10, (size_t)0, s, MPFR_RNDN);
22 printf("sin(Pi/6)=%s(point:%d)\n\n",st,e);
23
24 mpfr_cos(c, p6, MPFR_RNDN);
25 mpfr_get_str(st, &e, 10, (size_t)0, c, MPFR_RNDN);
26 printf("cos(Pi/6)=%s(point:%d)\n\n",st,e);
27
28 mpfr_sqr(s2, s, MPFR_RNDN);
29 mpfr_sqr(c2, c, MPFR_RNDN);
30 mpfr_add(l, s2, c2, MPFR_RNDN);

```



表 13: MPFR の数学関数 (一部)

| 関数                           | 書き方                                   | 関数                           | 書き方                                            |
|------------------------------|---------------------------------------|------------------------------|------------------------------------------------|
| $y = \sqrt{x}$               | mpfr_sqrt( mpfr_t y, mpfr_t x, Rnd )  | $y = x^n$                    | mpfr_sqrt( mpfr_t y, mpfr_t x, mpfr_t n, Rnd ) |
| $y = \log_e(x)$              | mpfr_log( mpfr_t y, mpfr_t x, Rnd )   | $y = \log_2(x)$              | mpfr_log2( mpfr_t y, mpfr_t x, Rnd )           |
| $y = \log_{10}(x)$           | mpfr_log10( mpfr_t y, mpfr_t x, Rnd ) | $y = e^x$                    | mpfr_exp( mpfr_t y, mpfr_t x, Rnd )            |
| $y = 2^x$                    | mpfr_exp2( mpfr_t y, mpfr_t x, Rnd )  | $y = 10^x$                   | mpfr_exp10( mpfr_t y, mpfr_t x, Rnd )          |
| $y = \sin(x)$                | mpfr_sin( mpfr_t y, mpfr_t x, Rnd )   | $y = \cos(x)$                | mpfr_cos( mpfr_t y, mpfr_t x, Rnd )            |
| $y = \tan(x)$                | mpfr_tan( mpfr_t y, mpfr_t x, Rnd )   | $y = \sec(x)$                | mpfr_sec( mpfr_t y, mpfr_t x, Rnd )            |
| $y = \csc(x)$                | mpfr_csc( mpfr_t y, mpfr_t x, Rnd )   | $y = \cot(x)$                | mpfr_cot( mpfr_t y, mpfr_t x, Rnd )            |
| $y = \sin^{-1}(x)$           | mpfr_asin( mpfr_t y, mpfr_t x, Rnd )  | $y = \cos^{-1}(x)$           | mpfr_acos( mpfr_t y, mpfr_t x, Rnd )           |
| $y = \tan^{-1}(x)$           | mpfr_atan( mpfr_t y, mpfr_t x, Rnd )  |                              |                                                |
| $y = \sinh(x)$               | mpfr_sinh( mpfr_t y, mpfr_t x, Rnd )  | $y = \cosh(x)$               | mpfr_cosh( mpfr_t y, mpfr_t x, Rnd )           |
| $y = \tanh(x)$               | mpfr_tanh( mpfr_t y, mpfr_t x, Rnd )  | $y = \operatorname{sech}(x)$ | mpfr_sech( mpfr_t y, mpfr_t x, Rnd )           |
| $y = \operatorname{csch}(x)$ | mpfr_csch( mpfr_t y, mpfr_t x, Rnd )  | $y = \operatorname{coth}(x)$ | mpfr_coth( mpfr_t y, mpfr_t x, Rnd )           |
| $y = \sinh^{-1}(x)$          | mpfr_asinh( mpfr_t y, mpfr_t x, Rnd ) | $y = \cosh^{-1}(x)$          | mpfr_acosh( mpfr_t y, mpfr_t x, Rnd )          |
| $y = \tanh^{-1}(x)$          | mpfr_atanh( mpfr_t y, mpfr_t x, Rnd ) |                              |                                                |
| $y = \Gamma(x)$              | mpfr_gamma( mpfr_t y, mpfr_t x, Rnd ) | $y = \zeta(x)$               | mpfr_zeta( mpfr_t y, mpfr_t x, Rnd )           |
| $y = \pi$                    | mpfr_const_pi( mpfr_t y, Rnd )        |                              |                                                |

## 3 処理環境

### 3.1 Microsoft Visual Studio / Visual C++

Microsoft Visual Studio (以後 VS と略す) は Microsoft 社が開発している統合開発環境 (IDE) である。VS 下では C/C++/C#, Visual Basic, Python をはじめとする各種のプログラミング言語でソフトウェア製品を開発できる。これら言語の内, C++ としては, 同社が開発する Visual C++ (以後 VC と略す) を使うことができる。VC は最適化性能の高い C 言語処理系であり, Windows 環境下の標準的な C/C++ コンパイラである。

VS / VC は Microsoft 社のインターネットサイトから入手することができる。具体的には, Visual Studio のインストールパッケージを入手して起動し, インストーラの指示に従って作業すると VS と VC の両方が計算機環境にインストールされる。本書では Visual Studio Community 2017 の版に基づいて使用方法などを解説する。

#### 3.1.1 Visual C++

C 言語処理系は基本的にコンパイラ, ライブラリ, インクルードファイルといったファイル群から成る。コンパイラは翻訳処理の際にインクルードファイルを読み込み, 結合処理の際にライブラリ内の関数などを読み込む。(動的リンクライブラリ / DLL は実行時に結合される) 従って, ライブラリやインクルードファイルのディレクトリを環境変数に設定しておき, 翻訳と結合の際にコンパイラが参照できるようにしておく必要があるが, それら設定作業はインストール時に行われる。

##### 3.1.1.1 コマンドツールとしてのコンパイラ

VS / VC をインストールすると開発者コマンドプロンプトが使える。これは Windows 標準のコマンドプロンプトに VC 用の環境設定を施したものである。例えば, Visual Studio 2017 で開発者コマンドプロンプトを起動するバッチファイルは下記のパスである。

例. VS2017 での開発者コマンドプロンプト起動バッチファイル

```
C:¥Program Files (x86)¥Microsoft Visual Studio¥2017¥
Community¥Common7¥Tools¥VsDevCmd.bat
```

このバッチファイルを用いてコマンドプロンプトを起動すると, コンパイラ利用のための環境設定が施される。

開発者コマンドプロンプトを起動した例を次に示す。

例. 開発者コマンドプロンプトの起動

```

** Visual Studio 2017 Developer Command Prompt v15.7.1
** Copyright (c) 2017 Microsoft Corporation

C:¥Program Files (x86)¥Microsoft Visual Studio¥2017¥Community>
```

この後, コンパイラのコマンド cl.exe を使うことができる。

#### ■ 翻訳と実行の例

次のような C 言語のプログラム test00.c を翻訳して実行する例を示す。

プログラム: test00.c

```
1 #include <stdio.h>
2
3 int main()
4 {
5 int a = 1, b = 2, c;
6 c = a + b;
7 printf("%d + %d = %d\n", a, b, c);
8 }
```

開発者コマンドプロンプトで次のようにして翻訳処理を行う。

例. 翻訳処理

```
C:¥Users¥katsu> cl test00.c ←翻訳と結合の処理
Microsoft(R) C/C++ Optimizing Compiler Version 19.14.26433 for x86
Copyright (C) Microsoft Corporation. All rights reserved.

test00.c

Microsoft (R) Incremental Linker Version 14.14.26433.0
Copyright (C) Microsoft Corporation. All rights reserved.

/out:test00.exe
test00.obj
```

これで、オブジェクトファイル（結合前のファイル）test00.obj と実行形式ファイル test00.exe が生成された。test00.exe を実行する例を次に示す。

例. 実行

```
C:¥Users¥katsu> test00 ←実行
1 + 2 = 3 ←結果表示
```

■ cl.exe の使用方法

cl.exe はオプション '/?' を付けて起動すると各種オプションの使用方法（ヘルプ）を表示する。

例. ヘルプの表示

```
C:¥Users¥katsu>cl /? ←ヘルプの表示
Copyright (C) Microsoft Corporation. All rights reserved.

C/C++ COMPILER OPTIONS

-最適化-

/01 最大限の最適化（スペースを優先） /02 最大限の最適化（速度を優先）
/Ob<n> インライン展開（既定値 n=0） /Od 最適化を無効にする（既定）
/Og グローバルな最適化を有効にする /Oi [-] 組み込み関数を有効にする
⋮
(以下省略)
⋮
```

### 3.1.2 Visual Studio

Visual Studio は統合開発環境（IDE）であり、構築対象のソフトウェアのためのファイル群をプロジェクトという単位で管理する。Visual Studio 2017 を起動した例を図 3 に示す。

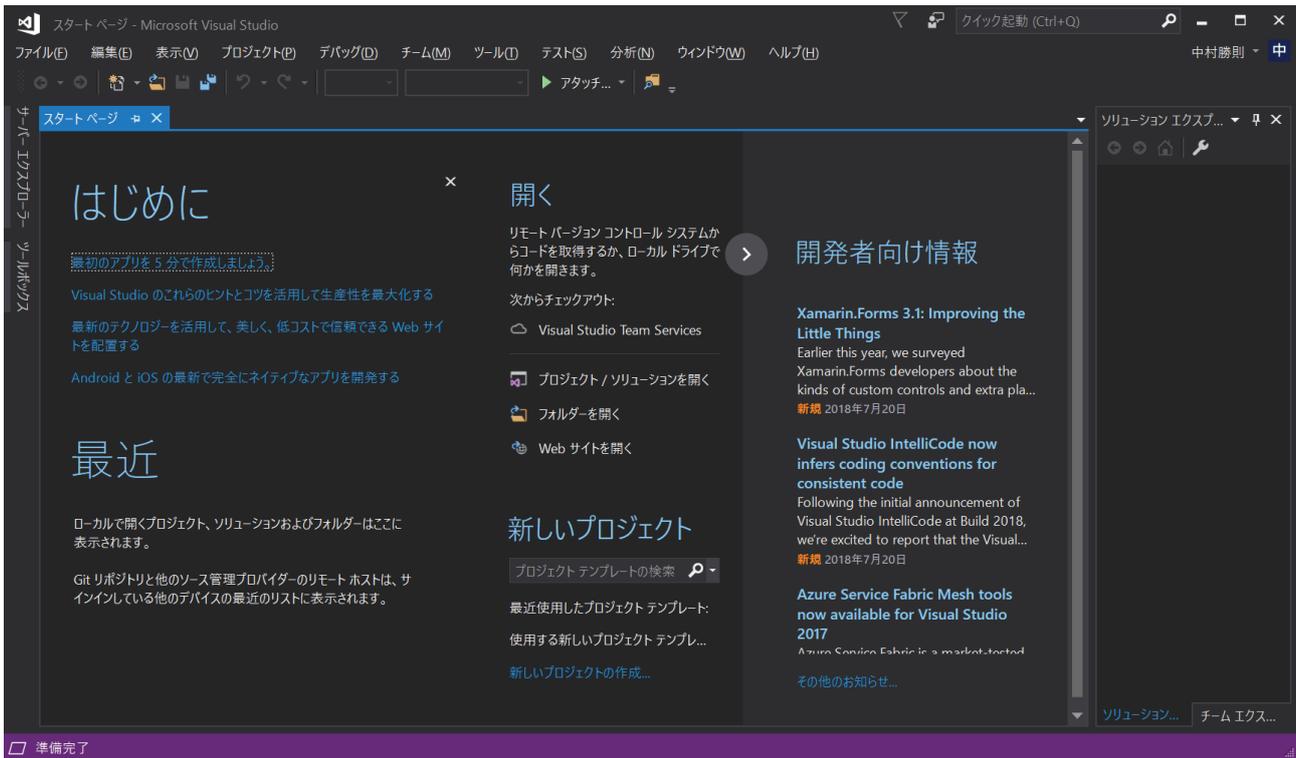


図 3: Visual Studio のウィンドウ

## 3.2 MinGW / MSYS2

MinGW (Minimalist GNU for Windows) は GNU の GCC <sup>12</sup> をはじめとするソフトウェアツール群を Windows 環境に移植したものである。また、MSYS (Minimal SYSTEM) は UNIX の基本的なコマンドツール群を Windows 環境に移植したものである。Windows 環境で UNIX (POSIX) に準拠した開発ツール群を利用する場合、MinGW と MSYS の両方をインストールすると良い。

MinGW, MSYS は共に Cygwin <sup>13</sup> から派生したツールセットであり、公式サイトは下記の通りである。

| ツールセット | 公式サイト URL                                                 |
|--------|-----------------------------------------------------------|
| MinGW  | <a href="http://www.mingw.org/">http://www.mingw.org/</a> |
| MSYS   | <a href="http://www.msys2.org/">http://www.msys2.org/</a> |

### 3.2.1 導入とパッケージ管理の方法

MSYS にはパッケージ管理のための機能が備わっており、それによって MSYS 導入後に MinGW を導入することができる。MSYS の公式インターネットサイトからインストーラ (図 4) を入手する。



図 4: MSYS のインストーラ

これを起動して導入作業を行う。インストーラの指示に従って作業を進めるが、MSYS のインストール先のディレクトリを選択できる。標準的なインストール作業ではインストール先はデフォルトで「C:¥msys64」となる。

インストール作業が終了すると MSYS のシェルである bash が利用できる。シェルを起動するためのアイコンが Windows のスタートメニューに登録されているのでそれによってシェルを起動する。パッケージ管理などは MSYS 標準の bash で、MinGW のツール群を使用する場合は MinGW32 (もしくは 64) の bash を使用する。

#### 3.2.1.1 pacman によるパッケージ管理

MSYS は pacman というツール (コマンド) でパッケージを管理する。このコマンドの起動時にオプションを付けることで、様々な管理操作ができる。

■ インストールされているパッケージの確認: `pacman -Q`

例.

```
$ pacman -Q ←コマンドの発行
bash 4.4.019-3
bash-completion 2.8-1
bsdcpio 3.3.2-1
bsdtar 3.3.2-1
bzip2 1.0.6-2
⋮
(以下省略)
⋮
```

<sup>12</sup>各種プログラミング言語のコンパイラ・コレクションとして有名である。

<sup>13</sup>Windows 上に実現する UNIX (POSIX) API 互換レイヤーである。公式インターネットサイトは <https://www.cygwin.com/>

■ パッケージのインストール: `pacman -S パッケージ1 パッケージ2 ...`

MSYS用の各種パッケージはリポジトリとして公開されており、オンラインでパッケージを入手してインストールすることができる。始めてMSYSを導入する際は、リポジトリから基本的な開発ツールを導入する。この作業は下記のコマンド操作による。

```
pacman -S base-devel msys2-devel
```

このコマンドを発行した後、未インストールのものを確認してインストールする。(処理が終了するまでしばらく待つ)次に、MinGWのツール群をインストールするために下記のコマンド操作を行う。

```
pacman -S mingw-w64-x86_64-toolchain
```

先と同様に、処理が終了するまでしばらく待つ。

これらが終われば、後は個別にツール(例えば vim, cmake, winpty など)をインストールする。

■ パッケージをリポジトリから検索: `pacman -Ss キーワード`

指定したキーワードを含むパッケージをリポジトリから検索する。例えば GUI のライブラリである wxWidgets の存在を検索するには次のようにする。

例. リポジトリから wxWidgets を検索

```
$ pacman -Ss wxwidgets ←検索開始
mingw32/mingw-w64-i686-wxPython 3.0.2.0-7
 A wxWidgets GUI toolkit for Python (mingw-w64)
mingw32/mingw-w64-i686-wxWidgets 3.0.4-1
 A C++ library that lets developers create applications for Windows, Linux
 and UNIX (mingw-w64)
mingw64/mingw-w64-x86_64-wxPython 3.0.2.0-7
 A wxWidgets GUI toolkit for Python (mingw-w64)
mingw64/mingw-w64-x86_64-wxWidgets 3.0.4-1
 A C++ library that lets developers create applications for Windows, Linux
 and UNIX (mingw-w64)
```

■ パッケージデータベースの更新: `pacman -Sy`

■ インストール済みパッケージの更新: `pacman -Su`

まとめて `pacman -Syu` として実行しても良い。

■ 指定したパッケージの削除: `pacman -R パッケージ`

依存関係も含めて削除するには「`pacman -Rs パッケージ`」とする。

## 4 Pythonでの応用例

### 4.1 MeCab との連携

natto-py パッケージを導入することで Python から MeCab を呼び出して日本語文章の形態素解析ができる。natto-py パッケージについての情報はインターネットサイト

<https://github.com/buruzaemon/natto-py>

<https://pypi.python.org/pypi/natto-py>

を参照のこと。また、natto-py とは別に mecab-python3, mecab-python-windows (Windows 用) というパッケージもあり、下記のインターネットサイトから入手することができる。

<https://pypi.org/project/mecab-python3/>

<https://pypi.org/project/mecab-python-windows/>

ここでは mecab-python3, mecab-python-windows の使用方法を紹介する。

#### 4.1.1 mecab-python3/mecab-python-windows

このモジュールは Python 処理系から MeCab を呼出して文章の形態素解析を行う。使用に際しては、次のようにしてモジュールを読み込む。

```
import MeCab
```

次に形態素解析のために Tagger クラスのオブジェクトを生成する。(下記参照)

例. モジュールの読み込みと Tagger オブジェクトの生成

```
>>> import MeCab ←モジュールの読み込み
```

```
>>> m = MeCab.Tagger() ←Tagger オブジェクト m を生成
```

この例では Tagger クラスのインスタンス m が生成されている。この m に対して parse メソッドを実行することで解析結果が得られる。

例. “私は大阪府に住んでいます。”の解析

```
>>> r = m.parse('私は大阪府に住んでいます。') ←文章解析
```

```
>>> print(r) ←結果の表示
```

```
私 名詞, 代名詞, 一般, *, *, *, 私, ワタシ, ワタシ
は 助詞, 係助詞, *, *, *, *, は, ハ, ワ
大阪 名詞, 固有名詞, 地域, 一般, *, *, 大阪, オオサカ, オーサカ
府 名詞, 接尾, 地域, *, *, *, 府, フ, フ
に 助詞, 格助詞, 一般, *, *, *, に, ニ, ニ
住ん 動詞, 自立, *, *, 五段・マ行, 連用タ接続, 住む, スン, スン
で 助詞, 接続助詞, *, *, *, *, で, デ, デ
い 動詞, 非自立, *, *, 一段, 連用形, いる, イ, イ
ます 助動詞, *, *, *, 特殊・マス, 基本形, ます, マス, マス
. 記号, 句点, *, *, *, *, ., ., ..
EOS
```

この例のように、parse メソッドの引数に解析対象の文章の文字列を与える。parse メソッドは解析結果を文字列で返す。この文字列は ‘¥n’ で区切られたレコードの形式であり、各行のフォーマットは

```
単語 ¥t 属性 1, 属性 2, …¥n
```

である。また ‘EOS’ は解析の終端を意味する。(「1.2 MeCab(和布蕪)：テキスト形態素解析」を参照のこと)

#### 4.1.2 MeCab の解析結果の取り扱いについて

MeCab の解析結果は文字列で得られるが、実際の形態素解析処理においては使いやすいデータ構造の形に変換する方が良い。

次のプログラム MeCabEx.py は、MeCab モジュールの機能を応用して、形態素解析の結果をリストとして取得するものである。

プログラム：MeCabEx.py

```
1 # coding: utf-8
2 import MeCab
3
4 #####
5 # mecab-python 準拠の機能
6 #####
7 class Tagger():
8 # コンストラクタ
9 def __init__(self):
10 self.M = MeCab.Tagger()
11
12 # 文章解析
13 def parse(self,s):
14 self.R = self.M.parse(s)
15 s1 = self.R.split('\n')
16 s2 = []
17 for m in s1:
18 s3 = m.split('\t')
19 if s3[0] == 'EOS':
20 break
21 else:
22 s4 = [s3[0]]
23 for n in s3[1].split(','):
24 s4.append(n)
25 s2.append(s4)
26 self.A = s2
27 return(self.R)
28
29 # 解析結果表示
30 def show(self):
31 for m in self.A:
32 msg = m[0]+'\\t'+', '.join(m[1:])
33 print(msg)
34
35 # 列の取り出し
36 def col(self,n):
37 r = []
38 for m in self.A:
39 if len(m) <= n:
40 r.append('')
41 else:
42 r.append(m[n])
43 return(r)
44
45 #####
46 # モジュールの実行テスト
47 #####
48 if __name__ == '__main__':
49 m = Tagger()
50 s = '私は大阪府に住んでいます。'
51 print(' (元の文章) ',s,'\n')
52 m.parse('私は大阪府に住んでいます。')
53 print(' (解析結果) ')
54 m.show()
55 print('\n(単語リスト)')
56 w = m.col(0)
57 print(w)
58 print('\n (再構成) ',', '.join(w))
```

## MeCabEx モジュールの使用方法

MeCabEx モジュールは、MeCab モジュールと同様の方法で使用することができ、解析結果をリストとして得ることもできる。解析処理の例を次に示す。

### 例. モジュールの読み込みと Tagger オブジェクトの生成

```
>>> import MeCabEx ←モジュールの読み込み
>>> m = MeCabEx.Tagger() ←Tagger オブジェクト m を生成
```

MeCab モジュールの場合と同様の処理ができる。(下記参照)

### 例. 文書の形態素解析 (1)

```
>>> r = m.parse(' 私は大阪府に住んでいます。 ') ←文章解析
>>> print(r) ←結果の表示

私 名詞, 代名詞, 一般, *, *, *, 私, ワタシ, ワタシ
は 助詞, 係助詞, *, *, *, *, は, ハ, ワ
大阪 名詞, 固有名詞, 地域, 一般, *, *, 大阪, オオサカ, オーサカ
府 名詞, 接尾, 地域, *, *, *, 府, フ, フ
に 助詞, 格助詞, 一般, *, *, *, に, ニ, ニ
住ん 動詞, 自立, *, *, 五段・マ行, 連用タ接続, 住む, スン, スン
で 助詞, 接続助詞, *, *, *, *, で, デ, デ
い 動詞, 非自立, *, *, 一段, 連用形, いる, イ, イ
ます 助動詞, *, *, *, 特殊・マス, 基本形, ます, マス, マス
. 記号, 句点, *, *, *, *, ., ., .
EOS
```

これに加えて、解析結果をリストの形として得ることができる。(下記参照)

### 例. 文書の形態素解析 (2)

```
>>> m.col(0) ←0 番目の列 (単語列) の取得
[' 私', ' は', ' 大阪', ' 府', ' に', ' 住ん', ' で', ' い', ' ます', ' . '] ←結果表示
>>> m.col(1) ←1 番目の列 (品詞列) の取得
[' 名詞', ' 助詞', ' 名詞', ' 名詞', ' 助詞', ' 動詞', ' 助詞', ' 動詞', ' 助動詞', ' 記号'] ←結果表示
```

このように col メソッドを使用して、MeCab からの出力の特定の列を取り出すことができる。col メソッドの引数には列のインデックスを与える。

このプログラムでは、parse メソッドを実行すると解析結果を Tagger オブジェクト内に保持しており、show メソッドを使用することで再度表示することができる。解析結果は次の parse メソッドの実行まで保持され、その間 show、col メソッドは同じ処理結果となる。解析結果は Tagger オブジェクトの A プロパティに保持されている。

### 例. Tagger オブジェクトの A プロパティ

```
>>> m.A ←A プロパティの参照
[[' 私', ' 名詞', ' 代名詞', ' 一般', '*', '*', '*', '私', ' ワタシ', ' ワタシ'],
 [' は', ' 助詞', ' 係助詞', '*', '*', '*', '*', 'は', ' ハ', ' ワ'],
 [' 大阪', ' 名詞', ' 固有名詞', ' 地域', ' 一般', '*', '*', '大阪', ' オオサカ', ' オーサカ'],
 [' 府', ' 名詞', ' 接尾', ' 地域', '*', '*', '*', '府', ' フ', ' フ'],
 [' に', ' 助詞', ' 格助詞', ' 一般', '*', '*', '*', 'に', ' ニ', ' ニ'],
 [' 住ん', ' 動詞', ' 自立', '*', '*', '五段・マ行', '連用タ接続', '住む', ' スン', ' スン'],
 [' で', ' 助詞', ' 接続助詞', '*', '*', '*', '*', 'で', ' デ', ' デ'],
 [' い', ' 動詞', ' 非自立', '*', '*', '一段', '連用形', 'いる', ' イ', ' イ'],
 [' ます', ' 助動詞', '*', '*', '*', '特殊・マス', '基本形', 'ます', ' マス', ' マス'],
 [' .', ' 記号', ' 句点', '*', '*', '*', '*', '.', '.', '. ']]
```

## 4.2 日本語テキストの読み上げ (Open JTalk と PyAudio の応用)

Open JTalk と PyAudio モジュールを併用することで、テキスト読み上げの機能を実現することができる。ここではプログラムの1例を示す。

### ■ 実装の概要

サンプルプログラム `kspeech.py` は、与えたテキスト (文字列型データ) を読み上げる関数 `speak` を実装するものである。このプログラムはモジュールとして他の Python プログラムに読み込んで使用することができる。他のプログラムから利用する場合はこの `kspeech.py` を

```
import kspeech
```

として読み込んで、

```
kspeech.speak(文字列データ)
```

と記述することで与えた文字列を読み上げることができる。

このプログラム (`speak` 関数) は、与えた文字列データを一旦テキストファイル `kspeech_tmp.txt` として保存した後に `open_jtalk` コマンドを起動してそれを WAV 形式ファイル `kspeech_tmp.wav` に変換する。更にその WAV 形式ファイルを PyAudio モジュールを使用して再生する。

プログラム: `kspeech.py`

```
1 # coding: utf-8
2 #####
3 # kspeech.py #
4 # 0.5版 2017/08/13 #
5 #####
6 # 必要なモジュール
7 import subprocess
8 import wave
9 import pyaudio
10
11 # 作業ファイル
12 ftxt = 'kspeech_tmp.txt' # 読み上げ作業ファイル
13 fout = 'kspeech_tmp.wav' # 作業用音声ファイル
14 #####
15 # PyAudioによる再生 #
16 #####
17 # WAVファイルの再生
18 def playwave():
19 # 再生用コールバック関数
20 def sndplay(in_data, frame_count, time_info, status):
21 buf = wf.readframes(frame_count)
22 return(buf, pyaudio.paContinue)
23 # 音声ファイルのオープン
24 wf = wave.open(fout, 'rb')
25 # 属性情報の取得
26 ch = wf.getnchannels() # チャンネル数
27 qb = wf.getsampwidth() # 量子化ビット数 (バイト数)
28 fq = wf.getframerate() # サンプリング周波数
29 # PyAudioオブジェクトの生成
30 p = pyaudio.PyAudio()
31 # ストリームの生成
32 stm = p.open(format=p.get_format_from_width(qb),
33 channels=ch, rate=fq, output=True,
34 stream_callback=sndplay)
35 # コールバック関数による再生を開始
36 stm.start_stream()
37
38 #####
39 # open_jtalkコマンドによる読み上げ #
40 #####
41 #----- open_jtalkコマンド -----
42 cmd0 = 'C:\0pJTalk\open_jtalk' # コマンド本体
```

```

43 cmd1 = '-x C:\0pJTalk\dic_utf_8' # 辞書ディレクトリ
44 cmd2 = '-m C:\0pJTalk\mei_normal.htsvoice' # 音響モデル
45 cmd3 = '-s 44100 -r 1.0 -ow ' # サンプリング周波数と読み上げ速度など
46 # 実行用コマンド
47 cmd = cmd0+' '+cmd1+' '+cmd2+' '+cmd3+' '+fout+' '+ftxt
48
49 #----- 読み上げ -----
50 def speak(s):
51 # 読み上げ作業ファイル作成
52 f = open(ftxt,'w',encoding='sjis')
53 f.write(s)
54 f.close()
55 # open_jtalkのプロセス生成
56 sp = subprocess.Popen(cmd,shell=False,
57 stdin=None, stdout=None, stderr=None)
58 # プロセス実行
59 sp.wait() # open_jtalk終了待ち
60 playwave() # 再生
61
62 #=====
63 # kspeech.pyパッケージ実行テスト #
64 #=====
65 if __name__ == '__main__':
66 print('--- kspeech.py: begin ---')
67 while True:
68 s = input('テキスト入力: (終了は\'exit\') ')
69 if s == 'exit':
70 print('終了します...')
71 break
72 else:
73 speak(s)
74 print('--- kspeech.py: end ---')

```

このプログラムはPythonインタプリタで直接実行することもでき、その場合は、65行目以降の部分が実行され、キーボードから入力された文字列を読み上げる。

### 4.3 Python と SWI-Prolog の連携

PySwip モジュールの利用により、Python と SWI-Prolog を連携することができる。PySwip に関する情報はインターネットサイト

<https://github.com/yuce/pyswip>

から得ることができる。

#### 4.3.1 基本的な使用方法

PySwip モジュールが提供する Prolog クラスのオブジェクトを生成すると、それに対応する SWI-Prolog 処理系が 1 つ起動して連携が始まる。

例. Prolog オブジェクトの生成

```
>>> from pyswip import Prolog ← Prolog クラスの読み込み
>>> pr = Prolog() ← Prolog オブジェクト pr の生成
```

この例では、Prolog クラスの pr オブジェクトを生成している。この処理により SWI-Prolog 処理系が起動し、pr オブジェクトを介して SWI-Prolog 処理系に各種の処理を依頼することができる。

例. 述語の SWI-Prolog 処理系への登録

```
>>> pr.assertz('human(taro)')
>>> pr.assertz('human(jiro)')
>>> pr.assertz('human(hanako)')
```

この例では、assertz メソッドを用いて pr に 3 つの述語を登録している。SWI-Prolog への問い合わせ（節の単一化）には query メソッドを使用する。

例. SWI-Prolog 処理系への問い合わせ

```
>>> q = pr.query('human(X)') ←問い合わせ処理
>>> list(q) ←単一化の結果をリストに変換
[{'X': 'taro'}, {'X': 'jiro'}, {'X': 'hanako'}] ←単一化の結果
```

query メソッド実行により、単一化の結果が返される。この例では結果をリストに変換している。この処理により Prolog の変数 への単一化が辞書オブジェクトとして得られる。単一化の全ての変数の組み合わせが、それぞれの辞書オブジェクトを要素とするリストとして得られる。

SWI-Prolog 処理系に Prolog プログラムのソースを読み込ませるには consult メソッドを使用する。Prolog のプログラム test02.pl を読み込む例を示す。

Prolog のプログラム：test02.pl

```
1 human(taro).
2 human(hanako).
3
4 dog(pochi).
5 dog(nana).
6
7 deceased(nana).
8
9 cat(ruru).
10 cat(tama).
11
12 animal(A) :- human(A).
13 animal(A) :- dog(A).
14 animal(A) :- cat(A).
15
16 mortal(A) :- animal(A), not(deceased(A)).
```

例. Prolog のプログラム test02.pl の読み込みと問い合わせ

```
>>> from pyswip import Prolog ← Prolog クラスの読み込み
>>> pr = Prolog() ← Prolog オブジェクト pr の生成
>>> pr.consult('test02.pl') ← Prolog プログラムの読み込み
>>> q = list(pr.query('cat(A)')) ←問い合わせ処理 (?- cat(A))
>>> q ←結果の確認
[{'A': 'ruru'}, {'A': 'tama'}]
>>> q = list(pr.query('mortal(A)')) ←問い合わせ処理 (?- mortal(A))
>>> q ←結果の確認
[{'A': 'taro'}, {'A': 'hanako'}, {'A': 'pochi'}, {'A': 'ruru'}, {'A': 'tama'}]
```

# 索引

CaboCha, 7

DLL, 30

GCC, 33

GMP, 21

GNU, 33

iconv, 1

IDE, 30, 32

Julius, 13

JUMAN, 10

KNP, 10

MeCab, 4

MIME, 3

MinGW, 33

mpf\_clear, 24

mpf\_clears, 24

mpf\_t, 21

MPFR, 21, 26

mpfr\_clear, 27

mpfr\_clears, 27

mpfr\_init2, 26

mpq\_clear, 24

mpq\_clears, 24

mpq\_t, 21

mpz\_clear, 24

mpz\_clears, 24

mpz\_t, 21

MSYS, 33

natto-py, 35

NEologd, 5

nkf, 1

Open JTalk, 12

open\_jtalk, 12

OpenSSL, 18

openssl, 18

pacman, 33

PySwip, 40

RSA 暗号, 18

SWI-Prolog, 40

Visual C++, 30

Visual Studio, 30, 32

XML, 8

暗号化, 19

音声認識, 13

改行コード変換, 1

開発者コマンドプロンプト, 30

鍵の所有者, 18

鍵の生成, 18

鍵の長さ, 18

公開鍵, 18

公開鍵暗号方式, 18

電子署名, 19

統合開発環境, 30, 32

動的リンクライブラリ, 30

日本語係り受け解析, 7, 10

日本語形態素解析, 4, 10

任意精度の数値演算, 21

非対称鍵暗号方式, 18

秘密鍵, 18

復号, 19

プロジェクト, 32

文字コード変換, 1