知能と複雑系　129－7
(2002. 7. 26)

携帯型端末を利用した手書きサブリミナルチャネルの構築

瀬川 典久　村山 優子　宮崎 正俊
岩手県立大学ソフトウェア情報学部
〒020-0193 岩手県滝沢村滝沢字巣子152-52
TEL:019-694-2674 E-MAIL:sega@acm.org

概要

近年，セキュリティの技術の一つとしてサブリミナルチャネルが着目されている．サブリミナルチャネルとは，プライバシーを守りたい情報を，多量に流通する情報の中に紛れ込ませ(情報隠蔽)，特定の利用者だけがその情報を取り出せる手法である．研究グループでは，手書きによって書かれた筆跡情報でサブリミナルチャネルを行う手法を提案してきた．手書きによって書かれた筆跡を筆跡情報として符号化し，その符号化された情報に特定の人だけがわかるように情報を埋め込み，その情報をその人達で交換する．その筆跡情報を，第3者が見ても情報が埋め込まれている事実には気づかない．よって，安全に情報を交換することができる．

本稿では，携帯型端末を利用した手書きサブリミナルチャネルの構築について報告する．メモリが非常に少なくCPUの力が弱い携帯型端末において，手書きサブリミナルチャネルを構築する手法について報告し，その手法にしたがって構築したプロトタイプシステムについて報告する．

キーワード

ステガノグラフィ・手書き・Java(waba)・携帯型端末

The Construction of a Handwriting Subliminal Channel with a Personal Digital Assistant (PDA)

Norihisa Segawa Yuko Murayama Masatoshi Miyazaki
Faculty of Software and Information Science, Iwate Prefectural University
152-52, Sugo, Takizawa, Iwate, 020-0193
TEL: +81-19-694-2674 E-mail:sega@acm.org

Abstract

In recent years, its attention is paid to the subliminal channel as one of the technology of security. A subliminal channel is the technique from which the information which wants to protect privacy is made lost into the information which circulates so much, and only a specific user can take out the information. We have proposed the technique of performing a subliminal channel for handwriting information.

This paper reports the construction of a handwriting subliminal channel with a personal digital assistant (PDA). In a PDA with the weak power of CPU with very few memories, the technique of building a handwriting subliminal channel is reported, and the prototype system built according to the technique is reported.

Keyword

steganography, handwriting, Java (waba), personal digital assistant (PDA)

1 はじめに

ネットワークの普及・拡大と個人利用の増加にともない，コンピュータネットワークはコミュニケーションのためのシステムとして利用されるようになってきている．

また，近年の携帯電話，PDAの開発の進歩により，コミュニケーションシステムで扱う情報は，文字だけではなく，図，絵等さまざまな種類を扱えるようになってきている[1].

特に，手書きによる筆跡は，(1)短い文章を素早く書ける(2)文字だけではなく図等も扱うことが出来る(3)キーボード入力に比べ初心者の利用が行いやすい等の特徴がある(図1)[2].

それらのコミュニケーションにおいて，重要な点の一つとして，コミュニケーションのプライバシーの保持が挙げられる．そして，そのコミュニケーションのプライバシーを保護するためによく利用される手法としては，コミュニケーションの内容を暗号化して送受信する手法である．ただし，この手法では，悪意を持った第3者は，暗号化された情報の存在に気づく．そのために，その暗号化された情報を入手したとしたら，もしかすると第3者によって復号化され，情報の中身を知られてしまう恐れがある．

そこで，悪意をもった第3者から情報の交換の秘密を守るために考えられた手法の一つとして，サブリミナルチャネルという手法が提案された[3].サブリミナルチャネルでは，プライバシーを守りたい情報を，多量に流通する情報の中に紛れ込ませ(情報隠蔽)，特定の利用者だけがその情報を取り出せる手法である．第3者には，情報隠蔽の事実そのものがわからないので，プライバシー情報が盗まれる恐れはない．

この情報隠蔽を実現するには，(1)特定の利用者間でしかわからないメッセージの交換，なおかつ(2)一般の利用者には，特定の利用者間でのメッセージの交換の事実を気づかれない事が重要である．

我々の研究グループは，サブリミナルチャネルのための筆跡情報を用いた情報隠蔽について提案を行ってきた[4]．これは，誰でも見れる筆跡情報に，特定の利用者のみにしかわからない情報を付加することである．例えば，共有型ホワイトボードシステムのようなコミュニケーションにおいて，全ての参加者が，筆跡情報が見える状況下で，特定の参加者だけで，情報が交換できるシステムを構築するのに利用できる．

本稿では，従来のPCで利用するのではなく，携帯型端末で情報隠蔽を行う手法について提案，および携帯型端末にプロトタイプシステムを構築について述べる．

以下，2章で，筆跡情報について特定の人だけが理解できる情報を埋め込む手法について述べる．3章で，携帯型端末での情報隠蔽の実現手法について述べ，4章でまとめを行う．

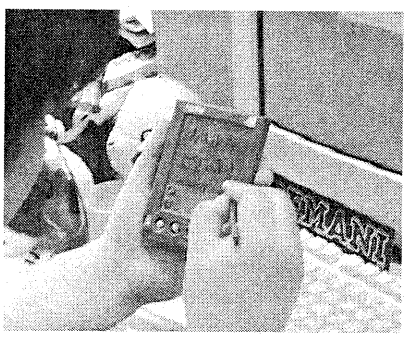


図1携帯型端末の利用

2拡張された筆跡情報における情報隠蔽

2.1概要

筆跡情報を用いた，情報隠蔽を構築するには，(1)特定の利用者間でしかわからないメッセージの交換，なおかつ(2)一般の利用者には，特定の利用者間でのメッセージの交換の事実を気づかれない事が重要である．

そのために，本研究では次の手法を考えた．

(1)手書きの筆跡を，vector drawingとしてとらえ，符号化を行う．

(2)符号化された情報に対して，第3者には気づかれないような情報を付加する．つまり，特定の利用者間のみに理解でき，なおかつ一般の利用者には普通の手書きと見えるような特殊な手書き情報の交換を行えるようにすることである．

2.2 vector drawing

今回扱う筆跡情報は一般にvector drawaingと呼ばれる点と直線の集合として管理されている．

利用者の手書きによって作られた筆跡に対して，一定時間毎にサンプリングを行い，(1)複数の座標点と(2)その複数の座標点をつなぐ図形を取り出す．その複数の座標点と，座標点をつなぐ図形情報が，符号化される．符号化されたデータが，本研究で扱う筆跡情報になる．

2.3 筆跡情報

本研究では，手書きにおける一画が，1行の筆跡情報として表される．1行の筆跡情報は，(A)データの形式(B)色(C)線の太さ(D)点の座標情報（X,Yの組みの集合）が含まれている（図2）．

写真などの画像を格納するのによく利用されるbitmapデータより，vector drawingの方がデータ量が小さくなる事が多い．しかし，手書きのような自由

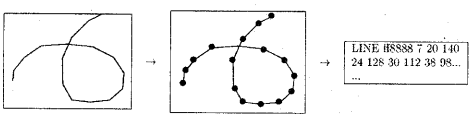


図2 描画情報（符号化）

曲線を扱うのには，サンプリングする点の数を多くしないと，不自然な筆跡になる．

2.4 筆跡情報のに対する情報の埋込

図3に，誰もが読める筆跡情報に，特定の利用者間のみで共有される情報を埋め込む手法を示す．基本的な考え方は，本来かかれる線分に複数の点をとり，その複数の点を，埋め込む情報にしたがって移動させ，線を引き直すということである．その際に，元の図形と著しく異ならないようにする事が重要なことである．

まず，送信者が手書きを行ない，筆跡情報を生成する．生成された筆跡情報は，複数の点と線からなる．点(X1,Y1),点(X2,Y2)が本来の点である．

(1)点A,点Bをn等分する．（この例では3等分）

(2)ある点に対して移動させる量の最大値を決定する．移動する量の最大値を，x軸はM，y軸はNとする．

(3)この組み合わせに対して，コードブックを作成する．例えばアルファベットとの1対1対応を決めておく．

コードブックの大きさは，次のように決めることができる．

$$\left|\frac{M}{x}\right| \cdot \left|\frac{N}{y}\right|$$

一つの点の最大移動量 X軸:M Y軸:N
一つの点の最小移動単位:X軸:x Y軸:y

(4)埋め込む情報から，各点の移動量を決定し，点を移動させる．そして，移動した点に対して，線を引き直す．

埋め込める情報の最大量は，次のように計算できる．

$$Z = A \cdot (P-1) \cdot \left(\left|\frac{M}{x}\right| \cdot \left|\frac{N}{y}\right|\right)$$

埋込に利用する線分の数:A
一つの線分を分割する数:P
一つの点の最大移動量 X軸:M Y軸:N
一つの点の最小移動単位:X軸:x Y軸:y
ただし，分割数P,移動量M，Nが大きくなってしまうと，本来かかれるはずの情報からおおきくはみ出てしまい，第3者に情報が埋め込まれていることがわかってしまう恐れがあるので，P,M,Nを調整することによって回避する．

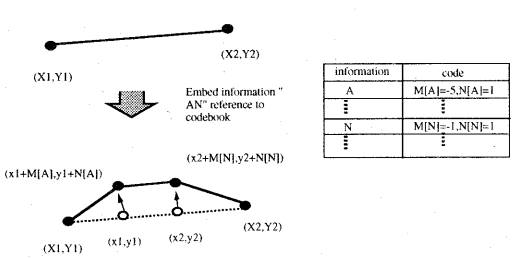


図3 情報の埋込手法

2.5 情報の復元

埋め込まれた情報を取り出すためには，次のことを行なう(図4)．

(1)情報を埋め込んだ人から，次の情報を鍵として安全な手法を用いあらかじめ受け取っておく．

(A)埋込に利用する線分の集合
(B)線分の分割数
(C)コードブック

(2)筆跡情報から，情報が埋め込まれた点，本来ある点に分類する．(A),(B)の情報を利用して，分類を行なう．

(3) 情報が埋め込まれた点を使い，埋め込まれた情報を取り出す．取り出しかたは，埋め込むときと逆になり，本来ある点に引かれた線分からの変化量が，埋め込まれた情報に対応する．

2.6 情報の埋込の実現

2.5まで述べた情報の埋込手法を用い，実際の筆跡情報に，情報を埋め込んでみた．

図5の上は，情報を埋め込む際の元になった手書きである．画数は，３１画で，１９０の点と１５９本の直線で構成されている．

図5の上に，"NORIHISA SEGAWA"というアルファベット文字列を埋め込んでみた．

次の手法で行なっている．

(1)情報を埋め込む位置，埋め込む情報とコードの関係を決める．

(A)利用する線分：各画における一番目の線分
(B)分割数：2
(C)コードブック

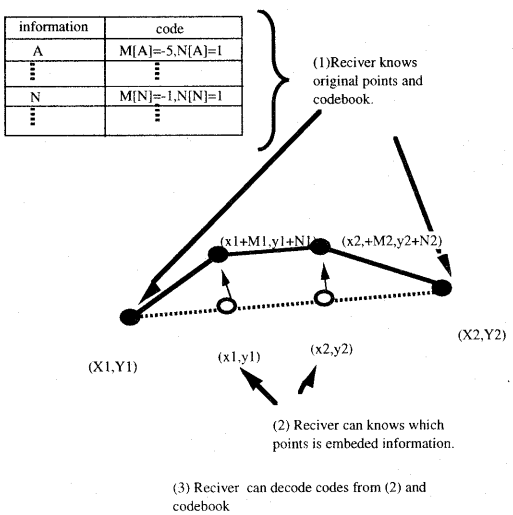
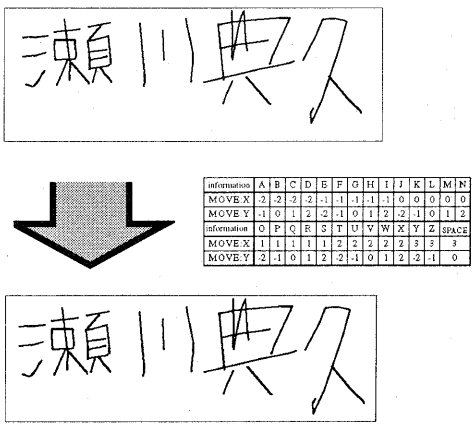


図4 情報の復元手法



information	A	B	C	D	E	F	G	H	I	J	K	L	M	N
MOVE X	-2	-2	-2	-2	-1	-1	-1	-1	-1	0	0	0	0	0
MOVE Y	-1	0	1	2	-2	-1	0	1	2	-2	-1	0	1	2

information	O	P	Q	R	S	T	U	V	W	X	Y	Z	SPACE
MOVE X	1	1	1	1	1	2	2	2	2	2	3	3	3
MOVE Y	-2	-1	0	1	2	-2	-1	0	1	2	-2	-1	0

図5 実際の情報の埋込

(2) (1) の情報に従い，情報を埋め込んでいく．まず，各画における1番目の点と2番目の点の中間点を求める．その中間点に対して，アルファベットに対応した移動量だけその中間点を移動する．

(3)1番目の点から，移動された中間点経由して，2番目の点に線を引き直す．

実行結果は，図5の下になる．

3 携帯型端末を利用したサブリミナルチャネルの構築

2章において，筆跡情報において情報隠蔽が構築できることを示した．

本章では，2章での手法を携帯型端末で利用する手法を述べる．

3.1携帯型端末の概要

近年，電子部品が小型化，また省電力化されたために，さまざまな携帯型端末が開発されている．また，Java搭載の携帯電話に代表されるように，従来の携帯電話に小型のコンピュータが搭載され，情報を扱う端末としても利用できるようになっている．

これらの携帯型端末は，次のような特徴を持っている．

(1)非常に小型である

常に，ユーザが携帯できるように，ユーザが利用するのに困らない範囲で端末を小型化している．特に，近年は小型でなおかつ薄型の物が開発されている．

携帯型端末は，従来型のキーボード，マウスを搭載していない．一般的には，小型キーボード，ペン入力，スティックポインター等，携帯するのに困らない入力インタフェースを搭載している．

(2)電池によって長時間駆動できる

携帯型端末は，一般的には充電池によって駆動する．一回の充電によって，短い物で約１２時間，長い物では１カ月間駆動することが可能である．

(3)移動体通信機能と組み合わせることが出来る

携帯型端末本体に内蔵されている移動体通信機能を利用，もしくはアダプターなどを利用して携帯電話，PHS，無線LANに接続を行い，外部ネットワークと通信を行うことが出来る．そのために，ユーザは，通信回線さえ確保できれば，どこでもネットワークを利用することが可能である．

(4)メモリの容量が小さい

現在のパーソナルコンピュータ(PC)は，メモリが512MBを越えている場合も少なくない．しかし，携帯型端末は，多くて32MB，少ない物は16KBしか搭載されていない．ただ，それらのメモリの多くが内臓電池で保護されているもしくはフラッシュメモリを利用しているので，一度導入したプログラムは，ユーザが消さない限り保持されている．

(5)専用OSで動作する

現在のPCに搭載されている，Windows2000, Windows XP, Linux, FreeBSD等のOSは，多量のメモリー，ハードディスクを利用することを前提として設計されている．さらに，多量のプロセスを処理することも要求されている．

携帯型端末は，原則ハードディスクが搭載されていない，搭載されているメモリの容量が小さい．また，携帯電話のように作業中に電話を受ける場合には，確実に実時間で応答しなければならない等の制限がある．さらに，各携帯型端末で装着している入出力装置が異なる．

そのために，携帯型端末では，専用のＯＳを設計し搭載している．携帯型端末のOSの特徴としては，容量の小さいメモリーで動作するようにカーネルのサイズ出来る限り小さくしている．また，多量のプロセスを動作させることよりも，応答時間保証に重点をおいてOSが設計されている．また，PCの用に標準の入出力装置がないため，各端末に応じて独自の改良がOSに加えられている．

3.2 携帯型端末でのシステムの構築

3.1で述べたように，携帯型端末はPCと異なり，ハードディスクが搭載されておらず，非常に少ないメモリーで動作させなければならない．また，キーボードを利用することを前提としたソフトウェアの設計は避けなければならない．

また，それぞれの携帯型端末は専用OSで動作しているので，それぞれの携帯型端末用にシステムを構築すると他の携帯型端末に移植するのが難しくなる．

そこで，本研究では，Javaを利用して実装を行う．ただし，従来のJavaは携帯型端末では動作しないので，携帯型端末用のJavaを利用する．

携帯型端末用のJavaは，従来利用されているJava 2 Standard Edtion(J2SE)ではなく，そのサブセットになる．

以下に，携帯型端末用Javaもしくはその準拠品を示す[5].

(1) Java 2 Micro Edtion (J2ME)
(2) ChaiVM
(3) KaffeVM
(4) Waba

(1)が純正のJavaであるが，本研究では，(4)のWabaを利用して開発を行った．Wabaは，wabasoft [6][7]が開発した言語で，ライセンスフリーとして利用することができる．Wabaは，Java言語の文法の

完全なサブセットとして設計されており，クラスファイル，バイトコードもJavaのサブセットとして設計されている．よって，既存のJavaの開発環境がそのまま利用できる．

またwabaは，J2MEに比べて仮想マシンのサイズが小さい，従来のJavaで動かすための仕組みも提供されている，小型デバイスで動作させるためのクラスが存在するなどの特徴を持つ．よって，wabaを利用することによって，今回開発するシステムをさまざまな携帯型端末に移植することが容易に行えると考えられる．

3.3 携帯型端末でのサブリミナルチャネルの構築

2章で説明した情報隠蔽の手法をもちいて，携帯型端末上にプロトタイプシステムをwabaを用いて実装した．

構築したプロトタイプシステムは，以下のとおりである（図6).

(1)送信者は，まず手書きメモを作成する．

(2)送信者は，筆跡に対して隠蔽したい情報を入力し，手書きの筆跡に情報を隠蔽する．

(3)ネットワーク（無線PHSと無線:LAN)を利用し，送信者が受信者に情報を隠蔽した手書きメモを送信する．

(4)受信者は，送信者から送られてきた手書きメモから隠蔽されている情報を取り出す．

開発は，windowsマシン上で従来のJavaの開発環境を利用して行った．具体的な開発環境のスペックを表１に示す．

送信者，受信者が利用する実行環境は，PalmOSが稼働する携帯型端末である（図１)．Palmは，ペン入力を基本とするシステムである．具体的なスペックを，表2に示す．

今回作成するシステムは，wabaのAppletとして実装される．このAppletには，ユーザが手書きメモを書く機能，情報を隠蔽する機能（送信者，受信者間で共有するコードブックも含む），手書きメモを送受信する機能が含まれている．Appletのサイズは，約10KBである．

また，あらかじめ筆跡を格納するためのデータ領域を確保する必要が有り，今回は1000点(2KB)を確保した．

実装したAppletは，図7である．また，その実装したAppletをPalmVx上で実行した物が図8になる．

利用者は，この画面上で自由に手書きメモを書くことができる．

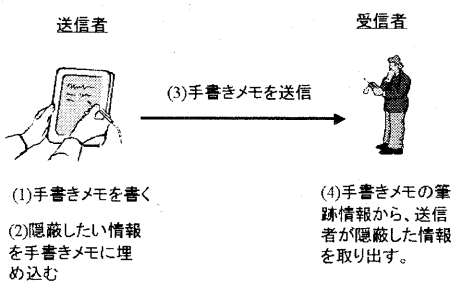


図6 本システムの概要

表1 開発環境

CPU	Celelon 300A
RAM	256MB
OS	Windows 2000
開発環境	Jbuilder 4
ターゲットコード	waba Ver 1.0

表2 送信者，受信者の実行環境

機種名	Palm Vx
CPU	Motorola DragonBall-EZ 20MHz
RAM	8MB
LCD	縦160 dot, 横160dot
通信機能	PHS 無線通信
重さ	113g
入力方法	ペン入力方式
OS	Palm OS 3.5 日本語版
実行環境	waba 1.0

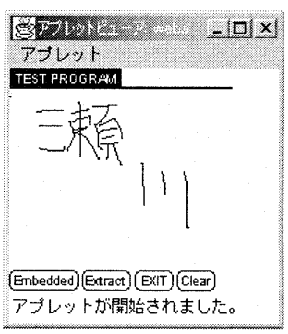


図7 Appletの実行例(windows開発環境で実行)

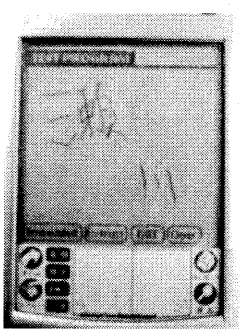


図8 AppletのPalmVx上での動作

手書きメモを書き終えた後，送信者が図7の左下にある[embedded]ボタンを押すと，埋め込みたい情報（現在はアルファベットのみ）をペンで入力し，第2章で示した手法で，手書きメモに情報が隠蔽される．隠蔽された情報は，受信者に送信される．

受信者は，送信者から送られた手書きメモを表示した後に，図7の左から2番目にある[extract]ボタンを押すと，隠蔽されていた情報が表れる．

3.4 考察

図9は，このAppletを利用して"SEGAWA"という文字列を図9の左側の筆跡に埋め込んだ物である．図9の左側は，約600本の線から構成される．図9の左側の筆跡の1, 11, 21, 31, 41,51本目の線に"S", "E", "G", "A", "W", "A"の6文字を埋め込んだ．埋込後の筆跡は，図9の右側である．

図9からわかるように，埋め込んだ前後で筆跡はほとんど変化していない．第3者には，情報が埋め込まれた事実を判別することは困難だと考えられる．よって，このプロトタイプシステムを用いてサブリミナルチャネルの構築が可能であると考えられる．

また，PalmVxでこのプログラムは実時間で動作した．PalmのCPUは，現在のPCで用いられているCPUに比べて100倍以上遅い．そのために，従来のPCで用いていた手法が携帯型端末で利用できるか調べる必要があった．今回の実装により，実行速度を確かめることが出来，なおかつ実時間で動作することがわかり，本手法が携帯型端末にも利用できることがわかった．本手法の計算量がほぼO(n)であるので，携帯型端末でも問題なく動作したと考えられる．

本システムのAppletのサイズは，約10KBであった．このサイズは現在のPCの環境からすると非常に小さいサイズであるが，携帯型端末の環境からすると非常に大きなサイズである．現在のAppletでは，一部の携帯型端末では動作しない．このサイズになった理由は，従来のPC上での開発手法を取ったために，メモリ使用量の節約を行わなかったためである．今後開発する場合には，データ領域のデータの圧縮作業などを利用してメモリ使用量の減少を行う必要がある．

4 まとめ

本稿では，携帯型端末を利用した手書きサブリミナルチャネルの構築を示した．具体的には，手書きをvector drawingの筆跡情報ととらえ，その筆跡情報に情報隠蔽を行う手法を示した．この，情報隠蔽の手法を利用し，携帯型端末上にwabaを用いて実装を行った．また，実装したシステムが動作することを確認した．

今後の課題は以下の通りである．

(1)Appletのメモリ使用量の節約

現在構築したAppletは，メモリ使用量について工夫をいっさい行っていない．今後は，さまざまな携帯型端末で動作させるためにメモリ使用量の節約を行う．

(2)他のJavaの環境への移植

今回は，wabaを用いてシステムを構築した．ただし，携帯電話などwabaそのものが動かない携帯型端末も存在する．

今回構築したシステムを，さまざまな携帯型端末のJavaに移植を行い，さまざまな端末間で動作させる．

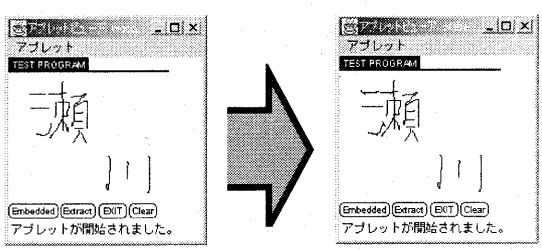


図9 Appletをもちいた情報隠蔽の実現
(windows開発環境で実行)

参考文献

[1]松下 温, 岡田謙一編著:コラボレーションとコミュニケーション,分散協調メディアシリーズ,共立出版(1995)

[2]瀬川 典久, 村山 優子, 権藤 広海, 中本 泰然, 宮崎正俊:WWW上の戸口伝言板における手書きの評価,第60回情報処理学会全国大会講演CD-ROM, 4W-02 (2000)

[3]G.J. Simmons : "The Prisones' Problem and the Subliminal Channel," in Advances in Cryptology, Proceedings of CRYPTO '83, pp.51-67,(1984)

[4]Norihisa Segawa, Yuko Murayama, Masatoshi Miyazaki: Information Hiding with a Handwritten Message in Vector-drawing Codes, Proceedings of the 35th Hawaii International Conference on System Sciences- 2002, CD-ROM Proceedings, (2002)

[5]眞壁 幸一:Javaは組み込み分野で本当に使えるのか!?- 組み込みJavaの現状と将来-,Interface 2000年12月号(CQ出版),p.68-72,(2000)

[6] wabasoft:http://www.wabasoft.com/ ,(2002年7月現在)

[7]Waba World:http://www.cc.yamaguchi-u.ac.jp/~shingo/WabaWorld/, (2002年7月現在)