KOGEI東京工芸大学 TOKYO POLYTECHNIC UNIVERSITY

情報ビジネスNO11

eビジネスに使われる技術

2013年12月10日

後　保範

1

KOGEI東京工芸大学 TOKYO POLYTECHNIC UNIVERSITY

1. 検索技術

- 検索サイトは下記の2種類に大別される

(1) ロボット型（カテゴリ検索）

ネットのWeb文書を定期的に巡回して情報を集め検索インデクスを作成。

(2) ディレクトリ型（Web検索）

人が登録申請されたサイトやネットを見て、手動で検索インデクスを作成。

有料登録のリスティング広告（検索連動型広告)はディレクトリ型

2

KOGEI東京工芸大学 TOKYO POLYTECHNIC UNIVERSITY

1.1 ロボット型検索エンジン

- Web検索に使用されるロボット型検索エンジンには「Google」とYahoo!の「YST」を使用するグループとマイクロソフトの「Bing」がある。
- ポイントは検索キーワードに対し、どれだけ良い品質の検索結果及び順位を表示できるか
- 検索品質の向上やSEO防止対策のためアルゴリズムの変更がよく行われる
- 検索インデックスの登録は早い

3

KOGEI東京工芸大学 TOKYO POLYTECHNIC UNIVERSITY

1.2 ディレクトリ型検索エンジン

- 手動でデータベースに登録するため、登録数は少なく、時間がかかる。
- 人がキーワードや登録内容の確認を行うので、検索したときにサイトの内容が適切で分かり易いことが多い。
- 代表的なサイトは「Yahoo!」
- ロボット型に比較し、登録数が少ないため減少傾向 → Yahoo!ジャパンがGoogleと提携

4

KOGEI東京工芸大学 TOKYO POLYTECHNIC UNIVERSITY

1.3 検索エンジンの動向

以前、日本では「goo」「エキサイト」「インフォシーク」「ライコス」「フレッシュアイ」など各社、独自の検索エンジンを持っていました。その後、日本に「Google」が上陸するとその人気に押され、「Yahoo!」のページ検索をはじめ、ほとんどの検索エンジンが「Google」を採用するようになりました。
そして検索連動型広告が大きなビジネスになることから、「Yahoo!」がYST、「MSN」がLive Serchを開発。「Google」キラーと呼ばれる新興検索エンジンも登場しましたが、ふたたび淘汰の時代へと向かいます。
2009年6月にマイクロソフトが次世代の検索エンジン「Bing」を投入。米YahooとマイクロソフトのBingにより、米YahooもYSTからBingに変更されることとなりした。しかしYahoo!ジャパンは2010年7月にGoogleを導入を発表し、日米による「ネジレ現象」が起こることになりました。またWEB検索で以前にGoogle陣営からYST陣営に移動した、インフォシークやニフティを含む大手ポータルサイトの動向も気になるところです。

「http://plaza.harmonix.ne.jp/~ma0011/engin.htm」より引用

5

KOGEI東京工芸大学 TOKYO POLYTECHNIC UNIVERSITY

1.4 代表的な検索エンジン(1/3)

検索エンジン	WEB検索	カテゴリ検索	画像検索	ブログ検索	その他	備考
YAHOO! JAPAN	YST	独自	独自	独自	動画 地図 商品(B)	日本ではNo.1検索エンジン。WEB検索はYSTだがGoogleに変更予定。
Google	Google	DMOZ	独自	独自(B)	動画 ニュース 地図(B)	世界最大の検索エンジン。WEB検索の制度には定評があり、多くの検索エンジンのサイトに利用されている。
msn	Bing	無し	独自	無し	動画 ニュース 地図	2009年6月にエンジンを「Live Serch」から「Bing」に変更。
goo	Google	クロス・リスティング	独自	独自	動画 電話帳 地図	WEBはGoogleの検索結果にgooのサービスを繋ぎ込んで表示。ブログ、画像、動画、音楽は独自のエンジン。
infoseek	YST	独自	有り	Yahoo!	動画 辞書	独自の検索エンジンは2007年7月で廃止。さらにWEB検索は2008年9月にGoogleからYSTに変更。カテゴリはあるが登録申請はできない。

「http://plaza.harmonix.ne.jp/~ma0011/engin.htm」より

6

KOGEI東京工芸大学 TOKYO POLYTECHNIC UNIVERSITY

1.4 代表的な検索エンジン(2/3)

検索エンジン	WEB検索	カテゴリ検索	画像検索	ブログ検索	その他	備考
excite	YST	クロス・リスティング	有り	無し	ニュース 買い物 辞書	WEB検索はYSTを使用。
Fresh eye	YST	J-リスティング	無し		ニュース 買い物 ウィキペディア	WEB検索はYSTJの検索結果からウィキペディアの項目を削除して表示。
OCN	Google	クロス・リスティング	無し	有り		
BIGLOBE	Google	クロス・リスティング	Google	無し	動画 買い物 電話帳	
@nifty	YST	クロス・リスティング	有り	Goo	動画 ニュース 商品	WEB検索は2009年8月1日からGoogleよりYSTJへ変更。動画検索はfoooooo、商品検索はアラジン、ニュースは自社。
livedoor	NAVER	J-リスティング	NAVER	NAVER	動画 まとめ 商品	画像検索は2010年6月から、WEB検索も2010年9月からNAVERへ変更。

「http://plaza.harmonix.ne.jp/~ma0011/engin.htm」より

KOGEI東京工芸大学 TOKYO POLYTECHNIC UNIVERSITY

1.4 代表的な検索エンジン(3/3)

検索エンジン	WEB検索	カテゴリ検索	画像検索	ブログ検索	その他	備考
Baidu 百度	Baidu	無し	独自	独自	動画	中国でNo.1の検索エンジン。2008年1月28日から日本で正式にサービス開始。
NAVER	YetiBot	無し	有り	有り	動画 クチコミ テーマ	韓国でNo.1の検索エンジン。2009年6月15日から日本でのサービスを再開。
MARS FLAG	独自	J-リスティング	無し	有り	無し	「画像主体」の独自の検索エンジンを使用。ただし画像の専用検索は無い。
SAGOOL	独自	無し	無し	無し	動画	人の主観・興味を反映した検索結果がコンセプトの独自の検索エンジンを使用。
mooter	YST	無し	無し	無し	無し	ソフトウェアがユーザーを予測するという概念に基づき開発したといいながら、表示内容はYahoo!と同じ。
All About Japan	YST	独自	無し	無し	無し	「ガイド」と呼ばれるその分野に詳しい人が、サイトを選定して登録。サイト内検索にYahoo!を使用。
Ask	独自	無し	無し	無し	無し	2009年6月で一旦終了したが11月から再開。

「http://plaza.harmonix.ne.jp/~ma0011/engin.htm」より

KOGEI東京工芸大学 TOKYO POLYTECHNIC UNIVERSITY

1.5 Googleの検索テクノロジー

- Google の検索テクノロジーを支えているのは、一連の計算を数分の一秒で同時に行うソフトウェア。
- 従来型の検索エンジンは、単語が 一つのWeb ページに何回出てくるかに重点を置いてる。
- Google の PageRank™ テクノロジーはWebのリンク構造全体を調べ、どのページが最も重要かを判断する。
- その後、ハイパーテキスト一致分析を通じて、現在行っている検索に関連のあるページを特定する。
- Google は、全体の重要度と検索クエリの関連性を組み合わせ、最も関連性の高い、信頼の置ける結果を提供している。

http://www.google.comのHPより

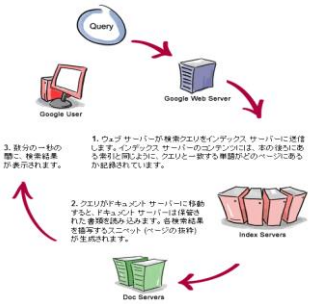
KOGEI東京工芸大学 TOKYO POLYTECHNIC UNIVERSITY

1.5 GoogleのWebページの評価法

- GoogleはWebページの重要性の評価方法として、リンクされていることは投票されている、とみなすページランクのアルゴリズムの検索技術を採用
- 単に、被リンクの数からページランクを決めるのではなく、リンク元のサイトの格付けをしている。
- これで、リンクファーム（何百ものリンクを並べただけの無意味なサイト）によって意図的にページランクを高めるSEO手法が使えなくなるようにしている。
- 検索エンジンスパムをはじくため、あまりに多くのキーワードが出るページのランクを低くしてる。

KOGEI東京工芸大学 TOKYO POLYTECHNIC UNIVERSITY

1.5 Googleの検索概念図



http://www.google.comのHPより

KOGEI東京工芸大学 TOKYO POLYTECHNIC UNIVERSITY

2. パーソナライゼーション

- パーソナライゼーションとは、ネットショップやポータルで、顧客ごとの画面表示を行う技術
- 利用者にとって便利な機能で、かつリピータとなることで、ネットショップの売り上げ増につながる。
- ログインして利用者を知った上で行う場合と、Cookie (Webサイトの利用者が、Webブラウザを通じて訪問者のコンピュータに一時的に書き込んだメモ)を用いる場合がある
- 例えばアマゾンにおいて、「あなたにおすすめの商品」という形で表示されるものがこれである

2.1 パーソナライゼーションの好循環

- 顧客がショップサイトを訪問
→ ショップサイトが顧客について学習し、顧客ニーズについてナレッジを蓄積
→ そのナレッジを用いて価値のあるサービスを提供
→ 顧客がそのサービスに満足
→ ロイヤリティを獲得。リピータになる。

13

3. ASP(Application Service Provider)

- ASPとは、ユーザにシステムを販売するのではなく、使用契約でアプリケーションの使用を提供する。
- アプリケーションはユーザ側にインストールしないで、センター側に設置するサーバにインストールする。
- ASPでは主としてパッケージソフトをインターネットやVPNなどのWANを通して提供する。
- ユーザはアプリケーションを「所有」するのではなく、「利用」する。
- ASPは利用するユーザは、サーバもアプリケーションも持たず、社内に運用担当者がいなくてすむため、コストを削減できる。

14

3.1 ASPのユーザのプラスとマイナス

- ユーザ企業側のプラス面
(1) ITの初期投資が少なくて済む
(2) 最新のサービスを利用できる
(3) 運用の手間が省ける
- ユーザ企業側のマイナス面
(1) 自由にシステムの機能が変えられない
(2) サービスの品質の問題がつきまとう

15

4. Webサービス

- WedサービスとはXML,HTTP,SOAPなどのインターンネットと標準技術を使用して、異なるプラットホーム上のアプリケーションとも統合することが可能なソフトウェアの総称
- 機能を部品化することで、初期投資を少なくすることができ、加えて柔軟なシステムを構築することができる。
- 汎用サービスの部品化が可能になることで、外部からそのサービスを使うことでビジネスの差別化に利用できる。

16

4.1 Web2.0

- Web2.0とは、情報の送り手と受け手が固定され送り手から受け手への一方的な流れであった状態(web1.0)が、送り手と受け手が流動化し誰でもがウェブを通して情報を発信できるように変化したwebの利用状態のこと。
- Web 2.0の本質を「ネット上の不特定多数の人々（や企業）を、受動的なサービス享受者ではなく能動的な表現者と認めて積極的に巻き込んでいくための技術やサービス開発姿勢」としている。

17

4.2 Web2.0の特徴

- 一般のソフト並みに操作性が高いネットサービス
Google Mapsの地図スクロールなど。
- 造語階層分類学ではなく、ユーザが自由に分類
- 利用者参加型サービス
Wikipedia(利用者が自由に読み書きできるネット上の百科事典)や、はてなキーワードなど。
- ロングテール
- Webサービスの利用による外部サービスの利用

18

KOGEI 東京工芸大学 TOKYO POLYTECHNIC UNIVERSITY

5. セキュリティ技術

- ネットでは、セキュリティ対策として、PKI(Public Key Infrastructure、公開鍵基盤)を用いた暗号化やディジタル署名が利用されている。
- セキュリティ技術では、公開鍵基盤を利用した技術が重要である。
- 共通鍵方式は、秘密の通信を多くの相手と行う場合は不向きである。
- 公開鍵方式として、RSA暗号方式が使用されている。
- RSA暗号は大きな数の素因数分解の困難性を利用

KOGEI 東京工芸大学 TOKYO POLYTECHNIC UNIVERSITY

5.1 情報を安全に送るには何が必要か

(1) 盗み見の防止は不可能
インターネット で情報を送る限りは、情報の盗み見 を完全に防ぐことは不可能

(2) 読むことができないようにする
情報を「暗号化 」して送信する
送信者: 情報を暗号化 する
受信者: 復号化 して情報に復元する

KOGEI 東京工芸大学 TOKYO POLYTECHNIC UNIVERSITY

5. 2 使用されている暗号を調べる

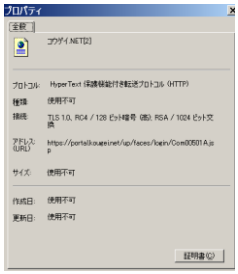
(1) 暗号化されたWeb
http : 暗号化されていないWeb
https : 暗号化されたWeb (s: security)

(2) 使用されている暗号を調べる
httpsのWebページを右クリック → プロパティ
(a) 接続: SSL 3.0、RC4/128 ビット暗号 (高);
RSA / 1024 ビット交換
(b) 接続: TLS 1.0、AES/128 ビット暗号 (高);
RSA / 1024 ビット交換

KOGEI 東京工芸大学 TOKYO POLYTECHNIC UNIVERSITY

5.2 インターネットの暗号調査例

東京工芸大HP(http)



工芸ネット(https)

KOGEI 東京工芸大学 TOKYO POLYTECHNIC UNIVERSITY

5.3 暗号化通信システム

(1) SSL (Security Session Layer)
SSL は、Netscape 社によって開発された通信路を暗号化する仕組み。
プライバシーに関わる情報やクレジットカード番号、
企業秘密などを安全に送受信することができる。
RSA暗号で鍵を送付し、データ自体は共通鍵暗号
で暗号化して送信する、ハイブリッド方式

(2) TLC (Transport Layer Security)
SSLを標準化団体IETFで標準化したもの

KOGEI 東京工芸大学 TOKYO POLYTECHNIC UNIVERSITY

5.4 共通鍵暗号と公開鍵暗号

(1) 共通鍵暗号
暗号化と復号化で共通の鍵を使用
利点: 高速に処理できる
欠点: 鍵の送信が必要である

(2) 公開鍵暗号
暗号化した鍵では復号化できない
利点: 鍵の送信が不要(公開鍵で暗号化)
欠点: 共通鍵暗号に比べ処理が遅い

5.5 共通鍵暗号方式

(1) 紀元前50年にシーザーが使用
英字を指定数ずらす。(a,b,c,.. → d,e,f,..)

(2) 暗号化処理
ビットの転置、シフト、加算(桁上げなし)の 組み合わせ。暗号化強度はビット数に依存。

(3) 代表的な暗号
(a) DES（Data Encryption Standard）： 1977年に米国標準
(b) AES (Advanced Encryption Standard)：2002年DESの後継
(c) RC4： RSA暗号を開発したR.L.Rivestの開発した暗号

5.5 公開鍵暗号方式

(1) 1976年に公開鍵暗号を発表
共通鍵暗号の鍵の「配送問題」を解決する手段として開発。暗号化と復号化に別の鍵を用いる。

(2) 1978年にRSA暗号を発表
R.L.Rivest, A.Shamir, L.M.Adlemanの3名が開発したのでRSA暗号と言われる。
多数桁の因数分解の困難性を利用した暗号方式。
現在の公開鍵暗号は全てRSA/1024である。

5.6 RSA暗号の仕組み

- RSA暗号鍵の作成(数学的な方法)
  (1) 素数p, qを選ぶ。
  (2) $n = p \times q$及び$f = (p-1) \times (q-1)$を計算
  (3) 素数eを選ぶ。
  (4) $d = 1/e \bmod (f)$となるdを計算する。

- (e,n)が公開暗号化鍵、(d,n)が復号鍵となる。

5.6 RSA暗号化と復号化

- RSA暗号化
  (1) 文をn以下の数Mに変換（公開方法)
  (2) $C=M^e \bmod (n)$で暗号Cを作成

- RSA復号化
  (1) $M=C^d \bmod (n)$で元の数Mに復号
  (2) 数Mを文に変換（公開方法)

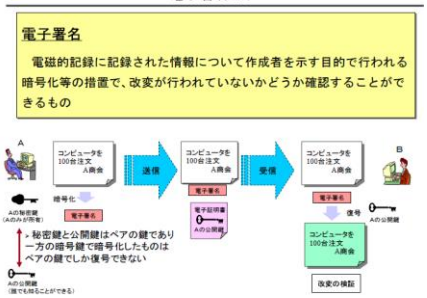
5.6 RSA暗号の復号化の数学理論

n=p×qのp,qが素数なら $M^{(p-1)(q-1)}=1 \bmod (n)$
なるオイラーの定理を使用

$$C^d \bmod (n) = (M^e)^d \bmod (n) = M^{\alpha f+1} \bmod (n)$$
$$= (M^{(p-1)(q-1)})^{\alpha} \times M \bmod (n)$$
$$= M \bmod (n) = M$$

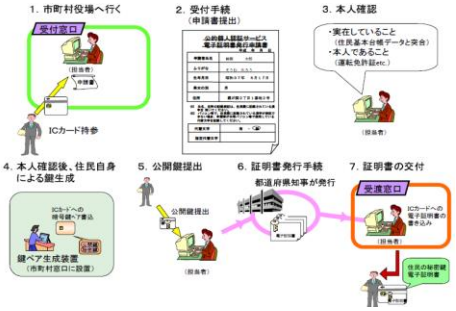
$ed = 1 \bmod (f)$で $ed=\alpha f+1$ (αは整数)を利用

5.7 電子署名



http://www.soumu.go.jp/のHPより

5.7 電子証明書発行のイメージ



http://www.soumu.go.jp/のHPより