京都大学大学院文学研究科 21 世紀 COE プログラム
「グローバル化時代の多元的人文学の拠点形成」

現代科学・技術・芸術と多元性の問題

Plurality and Science, Technology, Art

PaSTA

Newsletter

No.2

2003/02/07

活動報告

第 2 回 PaSTA 研究会は以下のように盛況に開催されました。

日時： 1 月 24 日（金）午後 3 ： 00-6 ： 00
会場：京都大学文学部東館 4 階（北東角） COE 研究室

電子暗号 1 -公開鍵暗号
伊藤　和行（文学研究科助教授）

デスクトップメタファーはどのようにして生まれたのか
喜多　千草（文学研究科博士課程修了）

報告要旨

●電子暗号 1-公開鍵暗号とは何か

伊藤　和行（文学研究科助教授）

現代ほど暗号が一般人の日常生活に関わっている時代はかつてなかった．従来，暗号は軍事・外交の手段として一般人からは遠い世界のものだったのであり，暗号がもっとも脚光を浴びたのは戦争時だった．それに対して今日のインターネットでは，商品を購入する際に暗号化通信が日常的に用いられている．暗号が経済的活動で用いられるようになった背景には，1960 年代にコンピュータを企業が利用するようになったことがあった．各企業は，遠隔地のコンピュータ間のデータを電話回線等で伝達する際に第三者からデータを守らねばならなかったのである．最初の商業用暗号として，1971 年に，IBM は"Lucifer"という暗号を開発している．さらに開発コストを下げ，異なる企業間での暗号通信を可能にするために，米国国立標準局（後の連邦標準技術局）は，電子商用暗号の標準化を行い，1973 年に「データ暗号化規格」（DES: Data Encryption Standard）を制定した．　商業活動で暗号が広く用いられるにつれて重要な問題となったのは，鍵の受け渡しにかかるコストだった．多くの受信者に鍵をどのようにして渡すかという問題を解決するために考案されたのが，公開鍵暗号（Public key encryption）という考えである．これは，暗号化の際と複合化の際に異なる鍵を用いるというもので，その核心は暗号化鍵によっては，復号化（解読）できない点である．暗号を送る際の手順は次のようになる．　1 受信者　自分の暗号化鍵（公開鍵）を公開　2 送信者　受信者の公開鍵を用いて送りたい情報を暗合化　3 受信者　もう一つの復号化鍵（秘密鍵）を用いて元の情報に変換復号化鍵は公開されず，受信者以外の者は暗号化鍵しか持っていないので，暗号を解読することはできないのである．この公開鍵暗号の考えは「暗号学の革命」と呼ばれるが，それを最初に考案したのは，W. Diffie と M. Hellman である（1976 年）．彼らは公開鍵暗号の考えを述べつつも，そのようなアルゴリズムを発見できなかった．しかし従来の暗号（暗号化と複合化に同じ鍵を用いるので共通鍵暗号と呼ばれる）の鍵を，誰かに盗聴される可能性のある通信手段において共有する方法（Diffie-Hellman 鍵交換方式）を提案している．これは，剰余体での累乗計算の一方向性を利用したもので，インターネットにおいて共通鍵暗号を用いるために広く利用されている．　Diffie と Hellman の論文に刺激を受け，L. Rivest，A. Shamir，L. Adleman は，1977 年に最初の公開鍵暗号のアルゴリズムを考案した．彼らのシステムは 整数論を巧みに利用してもので，非常に大きな自然数の素因数分解が困難な利用していた．さらにそのシステムを逆にすることによって，発信者を特定する署名の確認（デジタル署名）も可能なことを示した．彼らの暗号は RSA 公開鍵暗号と呼ばれ，最初に実用化公開鍵暗号だったが，それは 1980 年代後半になってからだった．　RSA 公開鍵暗号以後，公開鍵暗号のアルゴリズムはみな整数論を利用しており，その結果，それまで応用とはまったく関係なかった整数論という純粋数学の分野が重要な応用分野になったのである．

●デスクトップメタファーはどのようにして生まれたのか

喜多　千草（文学研究科博士課程修了）

今日、人々の生活に広く普及しているパーソナルコンピュータには、「デスクトップメタファ」と呼ばれる、コンピュータ画面を机上空間と見立てるインターフェイスデザインが施されている。ファイルやフォルダー、ゴミ箱といったアイコンと呼ばれるちいさな画

像を選ぶことで、机上での事務的な作業を行うというメタファによる、コンピュータのユーザ環境のことである。このような画像によるコンピュータ利用のためのインターフェイスを、グラフィカルユーザインターフェイス（Graphical User Interface, GUI）と呼ぶ。 そもそもコンピュータに画像表示装置が入出力装置として接続されること自体、デジタルコンピュータが生まれたときからなされてきたわけではない。画像表示装置がコンピュータにつけられたという記録は、1950 年ごろから見られるが、当時はまだ非常に珍しいものだったとされている。今では当たり前の、人間がコンピュータを直接利用するための入出力装置がつながれるようになった、デジタルコンピュータが生まれてから 10 年ほどたってからのことであった。例えば、マサチューセッツ工科大学で最初に Whirlwind というコンピュータにキーボードが接続されたのは 1956 年だったと言われる。しかし、徐々に画像表示装置を介したコンピュータの直接利用形態が洗練され、人間がコンピュータシステムをオンラインで利用することが定着していった。

やがて、大型汎用機のダウンサイジングという経済的要因からオンライン利用が一般人（事務員）にまで普及するとの予測が現実味を帯び始めた 1970 年代初頭に、ゼロックス社パロアルト研究所では、非プログラマのオンライン利用環境の研究開発が先鋭的に進められた。当時は、科学計算利用では、しばしば大型汎用機を時分割処理（タイムシェアリング）して多くの端末をつなぎ、同時に大勢の人々が利用する方式が広がっていたが、パロアルト研究所では、端末に独自の処理能力とメモリをおく、個人用コンピュータを端末にしたネットワークシステムへと移行する準備が進められた。こうして端末用のネットワークコンピュータとして生まれたのが Alto と呼ばれるコンピュータである。この Alto は、将来事務員でも簡単に使えるコンピュータを目指してデザインされたため、ハードウエア的に画像表示装置の利用を重視していた。そしてソフトウエア的にも、画面を紙とみなして、指示装置によって普段事務処理をしている感覚に近い使い勝手で文書作成などができるアプリケーションが開発されていった。このとき、指示装置にマウスが採用された。

パロアルト研究所では、二系統に分かれて実験的オンライン利用環境の構築が行われた。一系統は、Alto そのものをデザインしたグループによるもので、事務員のための環境をめざしたが、もう一系統は、さらに子どもでも使えるコンピューティング環境を目指していた。この二系統の環境構築により、GUI の基本ができあがっていった。やがて 1970 年代半ば以降、その二系統の環境が商用機へと統合される段階で、統合的インターフェイスデザインとして「デスクトップメタファ」が採用された。このメタファを提案したのは、アイコンを使ったプログラミングという新しい試みに取り組んでいた、デイブ・スミスというコンピュータ科学者であった。ゼロックス社内の文書によれば、1976 年末には、スミスによって、初期のデスクトップデザイン案が提出されており、これが、1981 年に発表されたゼロックス社による Alto システムの商用バージョンに搭載された。

以後、このゼロックス社のメタファが、まずアップル社に移植され、さらにマイクロソフト社にも移植されたため、ゼロックス社で生まれた、事務員のためのコンピュータ環境をデザインした「デスクトップメタファ」が、すべての人々のパーソナルコンピュータ利用環境として普及した。

こうしたメタファの存在を表層とした階層構造であるコンピュータシステム自体が多層的、あるいは多元的とも言えるかもしれないが、むしろ、デスクトップメタファがデファクトスタンダードとなることによって限定されたコンピューティングの本来持ち得たはずの多元性へ目を向けることもできるだろう。

今後の予定

●第 3 回「現代科学・技術・芸術と多元性の問題」PaSTA 研究会

日時：2 月 28 日（金）午後 3 ： 00-6 ： 00

会場：京都大学文学部東館 4 階（北東角） COE 研究室

〈演題未定〉

網谷　祐一（文学研究科博士課程）

〈演題未定〉

水谷　雅彦（文学研究科助教授）

●第 4 回「現代科学・技術・芸術と多元性の問題」PaSTA 研究会

科学哲学科学史研究室創立 10 周年記念行事

アインシュタインの思考をたどる
特殊相対性から一般相対性へ

日時：3 月 16 日（日）午後 1 時-5 時

場所：芝蘭会館（京大医学部北側）

あいさつ　伊藤　邦武（文学研究科教授）

司会　　伊藤　和行（文学研究科助教授）

講演（一）相対的時空と等価原理

講演（二）重力と曲がった時空

内井　惣七(文学研究科教授)

コメンテイター

石垣　寿郎（北海道大学大学院理学研究科教授）

菅野　礼司（大阪市立大学理学部名誉教授）

※PASTA 研究会の電子メール通知をご希望の方は事務局までご連絡下さい。

■PaSTA 事務局

〒606-8501　京都市左京区吉田本町　京都大学大学院文学研究科

現代文化学共同研究室（瀬戸口） TEL: 075-753-2792

E-mail: pasta-hmn@bun.kyoto-u.ac.jp

Webpage: http://www.hmn.bun.kyoto-u.ac.jp/pasta/