情報技術論

ノイマン型コンピュータ（von Neumann-type computer）

ノイマン型コンピュータはプログラムとデータを記憶装置に格納し、逐次制御により動作するコンピュータで、米プリンストン高等研究所のジョン・フォン・ノイマン(John von Neumann)により1946年に提唱された。現在の一般的なコンピュータはほぼ全てノイマン型である。ノイマン型は**プログラム内蔵方式**とも呼ばれ、プログラムを記憶装置に格納し、記憶装置から命令を一つずつ取り出して逐次実行を行う。当時のコンピュータは計算の指示を物理的な配線や真空管の差し替えにより行っていたが、ノイマン型ではこれをプログラムとして分離し、ハードウェアに汎用性を持たせることを可能にした。

ノイマン型コンピュータは5つの基本装置、すなわち、①CPUの内部にあり算術・論理演算を行う演算装置、②同CPUの内部にあり記憶装置上の命令に従って各装置の統制と制御を行う制御装置、③プログラムやデータを格納する記憶装置、④プログラムやデータを記憶装置に読み込む入力装置、⑤演算結果を表示・記録する出力装置から構成される。記憶装置はさらに当面の演算に必要な少量のデータやプログラムを格納し読み書きが高速な主記憶装置と、大量のデータやプログラムを長期的に保存し比較的安価に大容量化が可能な補助記憶装置から成る。

世界初のノイマン型コンピュータは1949年に英ケンブリッジ大学のモーリス・ウィルクス(Maulice Wilkes) により開発されたEDSACである。ノイマンは自身でもこれを実現するためのEDVACの開発に携わっていたが、こちらは開発が遅れ稼働の開始は1951年になった。

ノイマン型でないコンピュータ（非ノイマン型コンピュータ）としてはニューロコンピュータ（neuro computer）やバイオコンピュータ（bio computer）などがある。

デジタル化（digitize）

連続的に変化する音声や画像などの物理的なアナログデータを離散値のデジタル信号へ変換することをデジタル化という。デジタル化の処理は基本的に、アナログデータが記録された座標系を時間軸や平面領域において一定の間隔で分割する**標本化**(sampling)と、標本化された単位区間（領域）ごとに信号の大きさを離散値で置き換える**量子化**(quantization)の2つの操作で構成される。離散値になった信号を2進数に対応させる符号化を行うことでデジタル信号へ変換される。デジタル化されたデータはその性質上もとのアナログデータの近似値となり、標本化と量子化においてどのような“粗さ”で分割し、離散値に置き換えたかに依存して近似の精度が決まることになる。例えば、画像データで標本化を粗くする（単位領域を大きく取る）と画像内の細部の情報は失われザラつきの目立つ画像とな

る。また、音声データで量子化を粗く取ると、音質の低下した電話通話やAMラジオ放送のような音声になる。一方、デジタル化したデータの量もこれらの2操作に依存し、粗さをより細かくとると元のアナログデータをよりよく近似する高品質の画像や音声が得られる反面、作成されたデジタルデータのサイズもそれに比例して増大する。

デジタル化されたデータは劣化しにくい特性を持つ。データ伝送などにより混入したノイズは許容する閾値内であればすべて除去し完全に復元できることから、もとのデータと全く同じ複製の作成や、劣化による通信エラーを排除したデータ通信などが可能となる。

CPU（central processing unit）

CPU（中央処理装置）は算術・論理演算や各装置の制御を行う装置で、コンピュータの動作において中心的な役割を果たす。CPUの内部は主に、プログラムに記された命令に従って演算を実行するALU(arithmetic logic unit: 算術論理演算装置)、動作の基準となるクロック周波数に基づいて各装置に制御信号を送る制御装置、演算に必要なプログラムやデータを一時的に格納し高速に読み書きを行うレジスタ (register)、CPU内でこれらの要素をつなぐための信号線を束ねたバス(bus)等で構成される。

ノイマン型コンピュータでは主記憶装置にプログラムとして格納された機械語(マシン語)の命令をCPUが1つずつ取り出し解釈して計算を行う。命令はコンピュータへ与える指示の基本単位で、命令コードとオペランド (operand)から成り、命令コードは演算、条件分岐、データ転送などの動作指示の内容であり、CPUの種類ごとに異なる命令コードのセットが規定されている。オペランドは命令コードの処理対象を表し、対象データが格納されているメモリ上のアドレスやレジスタが参照先として指定される。実際の動作は、①制御装置が1つの命令を主記憶装置から取り出しレジスタに置き、②ALUが命令に従い演算を実行し、③結果がレジスタや主記憶装置に書き戻される、といったサイクルの繰り返しによりプログラムが実行されてゆく。

パソコンなどの小型コンピュータではCPUの機能が１つのLSI（large scale integration:大規模集積回路）に集積されたMPU(micro processing unit)が用いられる。また、バスの信号線数（バス幅）はCPUの動作単位である1クロックあたりに処理できるデータの量を表しCPU全体の処理能力に大きく影響するため、パソコンのCPUの性能を表す指標として8bit、16bit、32bit、64bitなどのバス幅がしばしば使用される。

キャッシュメモリ（cache memory）

キャッシュメモリはCPUと主記憶装置との速度差を補うため、主記憶装置よりも高速な記憶装置を媒介させ、一度使用したデータを再び読み込む際は高速な記憶装置から読み取ることで、パフォーマンスを向上させようとする技術である。最近のCPUでは、小容量で高速な1次キャッシュに加え、ある程度の容量を持ちやや高速に動作する2次キャッシュの2種類を併せ持つものがある。一般的に記憶装置は動作速度を高めようとするとビット

単価（単位容量当たりのコスト）が高価になり大容量化が難しくなるため、このような技術が広く利用されるようになった。キャッシュメモリは同じデータを2回以上読む際に効果を発揮するため、少量のデータを対象とした繰り返し処理などにおいては大幅なパフォーマンスの向上が期待できる。一方、大量のデータを一度だけ読み続け処理を行うような場合には向上効果は得られない。

頻繁に使用するデータをキャッシュに置くことで高速化をねらった同様の手法としては、磁気ディスク（ハードディスク）と主記憶装置の間で動作するディスクキャッシュ(disk cache) や、Webブラウザで一度表示したページのデータを格納しておくキャッシュファイル (cache file) などがある。また、主記憶装置からのデータの読み込みを高速化する他の技術としては、主記憶装置を複数のバンクに分けデータを分散記憶し、各バンクに対し同時に読み書きの動作を行うことでアクセスを高速化するメモリインタリーブ (memory interleave) などの手法がある。

プログラミング言語（programming language）

コンピュータに実行させる一連の指示内容を記したプログラムを記述するための人工言語で、コンピュータ（CPU）は理解しやすいが人には分かりづらい低水準言語と、人が理解しやすい高水準言語とに大別される。低水準言語にはCPUが直接理解できCPU毎に異なる命令セットが規定される機械語（マシン語）や、機械語の命令に対して1対1に単純な単語を対応させたアセンブラ言語(ニーモニック)がある。機械語は数値の列であり、アセンブラ言語は単純な単語や略語の並びとなるため、通常、人がこれらを直接に読み書きするのは困難である。低水準言語ではCPUやハードウェアを直接に制御できるため、それらの機能や性能を最大限に利用した効率のよいプログラムの作成が可能となるが、人にとっての判読の難しさから、大規模なソフトウェアの開発には向かない。一方、高水準言語はある程度日常の言語に近い単語の組み合わせによりプログラムを作成できるため、人が目的の処理を記述する際に処理内容をプログラムに置き換える作業（コーディング）が大幅に効率化される。高水準言語は利用目的に応じ種々のものが開発されてきた。主な言語として、科学技術計算用のFortran、事務処理用のCOBOL、構造化プログラミング向けのPascal、システム記述に適した汎用性の高いC言語、C言語をオブジェクト指向用に拡張したC++、コンピュータの機種やOSなどの実行環境（プラットフォーム）に依存しないプログラムが作成可能なオブジェクト指向言語であるJavaなどがある。これらの高水準言語は汎用プログラミング言語とも呼ばれるが、この分類以外にも、機能は多くないが小規模なプログラムを手軽に作成できるスクリプト言語（PerlやJavaScript等）や、文書中にタグなどのマークを挿入して文章構造や文字修飾を記述するマークアップ言語（HTML、XML等）などの分類があり,様々なプログラミング言語が開発されている。

無線LAN（むせんらん）

アクセスポイントから発信される電波の範囲内で無線により通信を行うLAN方式のネットワークで、アクセスポイントから接続するコンピュータまでの間が無線となる。パソコンの低価格化とノートパソコンの普及に伴い、家庭内で所持する複数のコンピュータから煩雑な物理配線なしにネットワークへ接続したいというニーズが高まり、また,空港ロビーやファーストフード店内などの公共空間でノートパソコンからインターネットが利用できるサービスが提供され、さらに企業や大学などにおいてもLANの無線化が進む等の経緯で普及してきた。無線LANの規格は、IEEE（米国電気電子学会)の802委員会によるIEEE802.11系列の諸規格が一般に利用されている。最初に普及したのは1999年に策定されたIEEE802.11bで、周波数帯域として2.4GHzを使用し通信速度は11Mbpsであった。IEEE802.11aは11bと同時期に策定されたもので、こちらは5.2GHzの帯域を使用し、通信速度は54Mbpsに高速化されている。現在はこの11aと、2003年に策定されたIEEE802.11gが普及している。11gは11aと同様に54Mbpsでの通信が可能であるが、帯域が異なり2.4GHzを使用している。

無線LANを利用する際はその性質上、アクセスポイントの不正利用や無線の盗聴などに対処するセキュリティ技術が必須となる。不正利用への基本的な対策としてはアクセスポイント側で接続できるコンピュータをMACアドレスにより制限したり、誰でも利用可とするANY設定を不許可とするなどの方法がある。盗聴への対処としては暗号化が有効であるが、暗号化の方式としては、初期に規格化された64bitや128bitのキーを使用するWEP(Wired Equivalent Privacy)や、WEPへの脆弱性の指摘を受け、より強度を高めたWPA (Wi-Fi Protected Access)などが策定されている。

公開鍵暗号（こうかいかぎあんごう）

もとの平文を暗号文に変換する暗号化に使用する鍵と、暗号文をもとに戻す復号化に使用する鍵に異なるものを使用し、片方の鍵を一般に公開できるようにした暗号化方式で、その理論は1976年に米スタンフォード大学のウィットフィールド・デフィー (Whitfield Diffie)とマーティン・ヘルマン(Martin Hellman)により公表された。現在のネットワーク通信においてはこの理論を基礎とした暗号化が広く利用されている。暗号化した文書をやり取りする場合、暗号文の受信者は文書を復号化するための鍵を入手する必要があるが、多くの暗号化方式ではこの鍵は安全な方法で送信者から別途入手しておく必要がある。しかしながら、送受信者の双方にとってこれは手間のかかる作業である。公開鍵暗号では、暗号化と復号化に使用する鍵は一つの対として作成し、他で作成された鍵との組み合わせは意味を持たない仕組みにしておく。生成した一方の鍵を本人のみが持つ秘密鍵とし、もう一方は一般に公開し誰でも入手可能な公開鍵とする。このような条件のもとで、例えばA氏が自分の秘密鍵で暗号化した文書をB氏に送信した場合、文書を受け取ったB氏はA氏の公開鍵でこれを復号化することになるが、A氏の公開鍵は容易に入手可能なため、別途手間のかか

る方法で復号化の鍵を入手する必要はない。実際の鍵の生成は数理的な理論に基づいたアルゴリズムにより行われ、上記のような性質を持つ1対の鍵が文字や数字の列として作成される。公開鍵はWebページや電子メールなどで通知される。公開鍵暗号の典型的な実装例としては素因数分解問題の困難さを利用したRSA暗号方式がある。また、この仕組みを応用することで、印鑑や自筆による署名と同等の意味を電子的なデータに持たせることを可能とする**デジタル署名**や、関連して鍵やデジタル署名の正当性を保証する認証局などの技術や仕組みが開発されてきている。

画像ファイル形式（がぞうふぁいるけいしき）

スキャナでデジタル化した写真や、画像作成アプリケーションを使用して描いた画像など、コンピュータで扱われる様々な画像は、それぞれ特定のデータ表現に従ってファイル化されディスク等に保存されることになるが、画像データの内部表現は、画像を画素（pixel）の集合体として表現するラスタ（ビットマップ）形式と、点と線で幾何学的に輪郭を描いた複数の部品を重ね合わせて全体画像を構成するベクトル形式に大別することができる。ラスタ形式は画素単位で微細な表現が可能であるが、画素数と色数に依存して保存の際にファイルのデータ量が膨大になる傾向があり、ファイル化の際には圧縮技術の併用が重要になる。例えば、白と黒の2色からなる2値画像の1画素を表現するには1 bitで十分であるが、一般的なフルカラー画像の1画素を表現するには光の三原色を構成する R（赤）、G（緑）、B（青）の各々に対して256階調の濃度の割り当てを行うと24 bitが必要となり、ファイル化の際にはさらにこれに画素数を乗じたサイズとなる。一方、ベクトル形式は基本的に比較的簡素な部品の組み合わせになるため絵画的な表現には向かないが、部品単位での変形や移動などが容易で、保存の際のデータ量もラスタ形式に比べ飛躍的に減少させることができる。実際に広く使用されている画像形式としては例えば、米Compuserve社により開発された色数の比較的少ないイラスト向けでラスタ形式に圧縮されたGIF（graphics interchange format）形式や、主に色数の多い写真向けで圧縮率の指定により画像品質を制御可能なJPEG（joint photographic experts group）形式、DTP（desk top publishing）などの分野で利用され高品質な印刷を目的としベクトル形式でデータを保持するEPS（encapsulated postscript）形式などがあるが、その他にも種々の目的で開発された多種多様な形式が存在し利用されている。

ユビキタスコンピューティング（ubiquitous computing）

ユビキタス（ubiquitous）とは、“至る所にある”ことを意味し、ユビキタスコンピューティングはコンピュータが生活や社会の中に偏在し、あらゆる場面で直接・間接的に人の生活をサポートする情報環境である。携帯電話やノートパソコンを利用して職場や家庭にとどまらず外出先からもシームレス（seamless: 複数のソフトやサービスが違和感なく同様の

操作で統合的に利用できること）にネットワークの利用が可能なモバイルコンピューティング(mobile computing)が実現されつつあるが、それに加え冷蔵庫やエアコンなどの家電や自動販売機や自動車などに組み込まれたコンピュータが連携するなどして様々な支援をし、人がそれらを意識することなく利用できる環境の実現を目指すものである。

歴史的には,ユビキタスコンピューティングは1991年に米ゼロックス社のパロアルト研究所により提唱された概念であるが、携帯電話などの情報端末やインターネットの普及などにより実現の可能性が身近なものとなり注目されるようになった。ユビキタスの概念のもとで開発された技術としては、コンピュータを着て歩くウェアラブルコンピュータ (wearable computer)などがある。また、日本では1984年に東京大学の坂村健教授により発足したTRONプロジェクトの中でユビキタスに近いものとして電脳社会の構想が提案されている。