■14 群（歴史・年表・資料）－ 1 編（電子情報通信技術史）

4 章 情報技術

■概要■

【本章の構成】

■14 群 － 1 編 － 4 章

4-1 コンピュータ

（執筆者：佐藤直樹）［2009 年 3 月 受領］

本節では，主に電子的な論理回路の組合せで構成されたディジタル計算機の歴史について述べる．

4-1-1 コンピュータの主要構成要素

コンピュータは，演算装置，制御装置，記憶装置，入力装置，出力装置を主要な 5 機能として構成される．これらはバスなどにより相互接続され動作する．なお，初期のコンピュータにおいては，これら 5 機能をすべて装備していないものもある．

(1) 演算装置と制御装置

演算装置（ALU : Arithmetic Logic Unit）は，コンピュータにおいて四則演算（加算，減算，乗算，除算），論理演算（AND，OR，NOT，XOR），ビットシフト操作などの処理を行う装置である．制御装置は，後述の主記憶装置に格納されている命令を取り出し解析し，演算装置や入力装置，出力装置などを制御し命令を実行する装置である．一つの命令の実行が終了すると次の命令の実行に移るという制御を行う．演算装置と制御装置を合わせて中央演算装置（CPU : Central Processing Unit）と呼ぶ．

1940 年代から 1950 年代にかけ，演算装置，制御装置には真空管，リレー，パラメトロンなどが使用され，1950 年代から 1960 年代にかけ，トランジスタ製が主流となった．1970 年代からは集積回路（IC）に演算装置と制御装置をまとめたマイクロプロセッサとなった．

(2) 記憶装置

記憶装置は，主に主記憶装置（メインメモリ）と補助記憶装置（外部記憶装置）で構成される．主記憶装置はプロセッサが直接アクセスできる記憶装置であり，1940 年代まで水銀遅延線，ウィリアムス管（ブラウン管）などが使用された．その後，1960 年代まで磁気ドラムメモリや磁気コアメモリが使用され，1970 年代初めから現在にかけて半導体メモリが主に使用されている．

補助記憶装置はプロセッサが直接アクセスできない記憶装置であり，主記憶装置と比較し大容量でありデータやプログラムなどの情報を永続的に保存するために使用される．補助記憶装置は多様であり，紙媒体（紙テープ，パンチカードなど），磁気テープ（オープンリール，DDS など），磁気ディスク（フロッピーディクス，ハードディスクなど），光ディスク（CD，DVD など），光磁気ディスク（MO など），メモリカードなどがある．

(3) 入力装置

入力装置は，コンピュータに対してデータを入力するための装置である．コンピュータ黎明期には，スイッチやコンピュータ出現以前から使用されていた紙テープリーダ，パンチカードリーダが入力装置として使用された．その後，入力装置は多様化し，文字や記号を入力するためのキーボード，位置情報を入力するためのポインティングデバイス（マウス，タッチ

パネル，トラックボールなど），イメージを入力するためのディジタルカメラやイメージスキャナ，サウンドを入力するためのマイクなどが使用されている．

(4) 出力装置

出力装置は，コンピュータからデータを出力するための装置である．コンピュータの黎明期には出力装置（ユーザーインタフェース）として紙テープせん孔装置，カードせん孔装置などが使用された．現在までにディスプレイ（CRT や液晶など），プリンタ（ラインプリンタ，ドットインパクトプリンタ，レーザープリンタなど），サウンドを出力するスピーカなど，多様な出力装置が使用されている．

4-1-2 コンピュータの歴史

(1) 1940 年代

1939 年から 1942 年にかけてアイオワ州立大学で開発された ABC マシンが世界最初のコンピュータとされている．約 280 本の真空管，回転式ドラムの表面に装着された 1500 個のコンデンサでデータを記憶するメモリ，入出力装置にはパンチカードリーダ，カードせん孔装置を使用していた．

1946 年，ペンシルバニア大学で ENIAC が公開された．ENIAC は約 17500 本の真空管，70000 個の抵抗器，10000 個のコンデンサなどで構成され，補助記憶装置は備えていない．十進法での計算を採用し毎秒 5000 回の加算，14 回の乗算が可能であった．プログラムはメモリ上にプログラムを配置するストアドプログラム方式とは異なり，配線により行う方式であった．

1948 年，マンチェスタ大学で SSEM が開発された．世界で始めてストアドプログラム方式を採用したコンピュータであるといわれている．SSEM の記憶容量は 32 ワードと少ないものであった．

1949 年，ケンブリッジ大学で EDSAC が開発された．世界初の実用的なストアドプログラム方式をとった電子計算機であるとされる．主記憶装置には水銀遅延線を使い，1 ワード 17 ビットで 1024 ワード記憶可能であった．

(2) 1950 年代

1950 年に UNIBAC I が完成，世界初の商用コンピュータといわれている．5200 本の真空管，10000 本のダイオードを使用し，メモリには 100 本の水銀遅延線を使用していた．入力装置として磁気テープを搭載．ストアドプログラム方式により，1 秒間に 100000 回の加算を行うことができた．

1952 年にはストアドプログラム方式の大型コンピュータ IBM 701 が IBM 初の商用コンピュータとして発表された．演算装置は真空管式で，メモリにはウィリアムス管が使用された．1 秒間に 21000 回の計算が可能であったとされる．入力装置としてパンチカードが使用された．

IBM は更に 1954 年に IBM 704 を発表．メモリには磁気コアメモリが使用された．

1956 年には富士フィルムが日本で初めての電子式コンピュータ FUJIC を開発した．真空管約 1700 本，水銀遅延線によるメインメモリ，入出力装置としてカードリーダと電動タイプライタを装備していた．

1959 年，IBM は IBM 7090 を発表．初の全トランジスタ式であり，主記憶装置には磁気コアメモリを使用しアドレス空間は 32 キロワードであった．

(3) 1960 年代

1960 年に DEC が PDP-1 の出荷を開始．最初のミニコンピュータといわれており，主記憶装置として磁気コアメモリを使用していた．

1964 年，初の汎用コンピュータである System/360 を IBM が発売した．それまでのコンピュータは業務ごとの専用機であったが，System/360 はプログラムの入れ替えにより多様な業務に適用できることが特徴であった．

またこの頃には，コンピュータを計算だけではなく機器の制御に利用する組込みシステムが出てきた．コンピュータがまだ非常に高価であったため，プラントの制御や航空管制システムなど高価な機器の制御が主であった．

(4) 1970 年代

1970 年に IBM が System/370 を発表，商用では初めての仮想記憶を搭載していた．

また, 1970 年代に入ると, コンピュータの中核機能を LSI として実装したマイクロプロセッサが開発された．インテルが 1971 年に世界初の 4 ビットマイクロプロセッサである i4004 を開発，搭載されたトランジスタ数は 2300，クロック周波数は 108 kHz であった．1974 年には i8080 を開発，搭載されたトランジスタ数は 6000，クロック周波数は 2 MHz であった．

1970 年代半ばになると，8 ビットのマイクロプロセッサを利用し，限定された機能ながら個人で購入可能な価格帯のパーソナルコンピュータが作られるようになった．初期のボード型パーソナルコンピュータの入出力装置には，16 進キーボードと LED 表示機などが使用されていた．1970 年代後半に入ると，フルキーボードやディスプレイを入出力装置として装備するパーソナルコンピュータも現れた．

スーパーコンピュータ分野では，1976 年に Cray 社がベクトル型プロセッサを搭載した Cray-1 を初出荷した. これ以後しばらくの間, スーパーコンピュータではベクトル型プロセッサを搭載した機種が主流となった．

また，マイクロプロセッサの登場により，特定の機能を実現するために機器や機械にコンピュータを使用する組込みシステムが多様化していった．この頃の組込みシステムでは，汎用の CPU などの LSI を使用し，目的の機能を実現していた．

(5) 1980 年代

1980 年代に入ると，パーソナルコンピュータに搭載されるマイクロプロセッサは 16 ビットへと移っていった．またこの時期，ユーザーインタフェース，表示能力，ネットワークなどでパーソナルコンピュータよりも高い能力をもつワークステーションも出現した．また，これまでの CISC（Complex Instruction Set Computer）以上の性能を狙った RISC（Reduced Instruction Set Computer）アーキテクチャによるマイクロプロセッサが発表された．

1980 年代前半には，32 ビットのマイクロプロセッサが登場し，ワークステーションなどで使用された. RISC アーキテクチャによるマイクロプロセッサもワークステーションで使用された．

この時期のスーパーコンピュータ分野では，高速計算に特化したシステム専用のベクトル型プロセッサを各メーカーが開発し，システムに使用していた．1982 年から 1983 年にかけて日本のメーカーもスーパーコンピュータの開発を発表している．

また，マイクロプロセッサの低価格化が進むにつれ，組込みシステムの多様化も更に進み，家電製品などの民生機器にもコンピュータが使用されるようになった．この頃の組込みシステムで使用されていたのは，4 ビットプロセッサ，8 ビットプロセッサなど処理能力が低いものが主であった．

(6) 1990 年代

1990 年代に入ると，64 ビットのマイクロプロセッサが登場し，主にワークステーションで利用される一方，パーソナルコンピュータにおいても 16 ビットプロセッサから 32 ビットプロセッサへの移行が進んだ．

この時期，スーパーコンピュータ分野では，ベクトル型プロセッサを用いたシステムと並び，汎用のプロセッサをベースとしたシステムが利用され始めた．

1990 年代後半には，パーソナルコンピュータの急激な性能向上によってワークステーションとの性能差が小さくなり，価格優位性をもつパーソナルコンピュータが市場の主流となっていった．

スーパーコンピュータ分野では一部のハイエンド機を除いて，汎用マイクロプロセッサを利用するようになった．汎用マイクロプロセッサを多数プロセッサ搭載することで高いスループットを狙ったシステムはコンピュータクラスタと呼ばれる．

一方，組込みシステムの分野では，1990 年代半ばには高性能なマイクロプロセッサが低いコストで利用できるようになり，高機能化，多機能化が進んだ．AV 機器や携帯電話などの家電機器においても 16 ビット，32 ビットのマイクロプロセッサが使用されるようになった．

(7) 2000 年代

2000 年代前半，マイクロプロセッサのクロック周波数が 1 GHz に到達．速度の向上も続いたが，パーソナルコンピュータ向け，サーバ向け，組込み機器向けなど目的ごとに細分化されたマイクロコンピュータが提供されるようになった．また，2000 年代半ばにはマイクロプロセッサ単体での周波数向上が物理的，電気的な限界に近づき，消費電力当たりの性能で優位性のあるマルチコアプロセッサが広がり始めた．

スーパーコンピュータの分野では，ハイエンド機においても更に汎用マイクロプロセッサの利用が進み，多数のマイクロプロセッサを利用することによる並列度も向上していった．

今後は，マルチコアプロセッサ上でいかに実行効率を高め，高い性能を達成するか，あるいは，複数のプロセッサをネットワーク接続した高並列システムにおいて，いかに高い性能を達成するか，が大きな課題になると予想される．

■参考文献

1) 大駒誠一，“コンピュータ開発史 －歴史の誤りを正す「最初の計算機」をたずねる旅ー，” 共立出版，2005.
2) デイビッド・A・パターソン，ジョン・L・ヘネシー，“コンピュータの構成と設計 (第 3 版) <別冊>歴

史展望,” 日経 BP 社, 2007.
3) “Computer History Museum,” http://www.computerhistory.org/
4) “The ENIAC Museum Online,” http://www.seas.upenn.edu/~museum/index.html
5) 文部科学省, “科学技術白書,” http://www.mext.go.jp/b_menu/hakusho/hakusho.htm#gijyutu
6) 社団法人情報処理学会, “コンピュータ博物館,” http://museum.ipsj.or.jp/index.html
7) “IBM Archives: Valuable resources on IBM’s history,” http://www-03.ibm.com/ibm/history/index.html
8) “Intel Computer Archives,” http://www.intel.com/museum/archives/index.htm
9) “Cay History,” http://www.cray.com/About/History.aspx

■14 群 － 1 編 － 4 章

4-2 基本ソフトウェア

（執筆者：菅原智義・副島賢司・島村　栄・小西弘一）［2009 年 3 月 受領］

基本ソフトウェアは，多くのアプリケーションプログラムに共通に必要とされる機能を提供するプログラムである．最初期には，その多くはハードウェア資源の操作や分配に関わるものであったが，特定のアプリケーション分野の発展につれて，トランザクション処理やサービス指向アーキテクチャ実現のための機能をも担うようになった．また，IT システムの運用管理のためのソフトウェアも，広い意味では，基本ソフトウェアに含まれると見ることもできる．このように，基本ソフトウェアに当たるものは幅広いが，本節では，おおもとの意味にあたる，ハードウェアを制御するプログラムとしての OS を中心に説明し，その他についてはアプリケーションサーバを概観するにとどめる．

4-2-1 オペレーティングシステム（OS）

(1)　汎用機用 OS の誕生（1960 年代）

OS の機能は 1950 年代のコンピュータから，プログラムをロード・実行や入出力のためのデバイスドライバなどの形で存在していたが，最初の本格的な OS と呼べるのは 1964 年に登場した IBM の OS/360 といわれている．OS/360 は，従来のシステムが機種ごとに別の制御ソフトウェアを必要としていたのに対し，1 種類の OS で様々な機種や応用プログラムに対応できるという今日の OS の概念を確立したといえる．

OS/360 と同時期に登場し，後の OS に大きな影響を与えたのが Multics である．Multics は，1964 年に始まった，MIT，AT&T ベル研究所及びゼネラルエレクトリック（GE）社の共同プロジェクトで作成された．Multics は，タイムシェアリングシステム，単一レベル記憶，動的リンク，階層型ファイルシステムなど，現在の OS の根幹をなす機能を既に実現していた．しかし，商業的にはあまり成功せず，後継である UNIX に取って代わられた．

(2)　UNIX の誕生（1970 年代）

1970 年代に入ると，DEC の VMS（Virtual Memory System）など汎用機用の OS は更に発展を遂げた．それと同時期に誕生したのが UNIX であった．

UNIX は，Multics と同じ AT&T ベル研究所で開発された OS であるが，Multics が複雑過ぎて失敗した点を省みて，シンプルさを重視して設計された．当初，UNIX はケン・トンプソンにより PDP-7 上にアセンブラで実装されたが，その後，デニス・リッチにより，C 言語が開発され，UNIX は，PDP-11 上に C 言語で実装された．UNIX は，マルチユーザー，マルチタスク，ファイルシステムなどを備え，現在の OS の原型となっている．その後，UNIX は BSD（Berkeley Software Distribution）系と System V 系に分かれて発展した．それ以外にも，UNIX の派生となる OS は数多く，代表的なものとして，SunOS（後の Solaris），AIX，HP-UX，Windows NT などがある．

(3)　パーソナル OS の発展（1980 年代）

CP-M（Control Program for Microcomputer）は，ディジタルリサーチ社により開発されたパー

ソナルコンピュータ（PC）用の OS である．8 ビットの PC 用 OS としては最も代表的な存在であり，インテルの 8080 プロセッサ上で動作した．CP/M はフロッピーディスクから起動する OS であり，また，CCP（Console Command Processor），BDOS（Basic Disk Operating System），BIOS（Basic Input and Output System）で構成される点など，後の MS-DOS に大きな影響を与えた．

1980 年代に入ると PC が一般家庭や大学などに普及し始めた．その PC 上で動作する OS を総称してパーソナル OS と呼ぶ．パーソナル OS の代表的なものが，マイクロソフトが開発・販売した MS-DOS である．MS-DOS は CP/M と類似した機能をもっていたが，当時普及し始めた 16 ビットコンピュータを対象としていたため，CP/M より市場で優位に立ち，その後，累計 1 億本を販売するに至った．なお，IBM-PC 用のものは，PC-DOS と呼ばれる．

(4) グラフィカルユーザーインタフェースの発展（1980～1990 年代）

PC の発展は同時に，グラフィカルユーザーインタフェース（GUI）の発展の歴史であった．GUI の歴史は PARC の Alto に始まるといわれているが，1980 年代に入ると，PC に GUI が搭載され，大きな進歩を遂げた．1983 年に発売された Apple の PC，Lisa に搭載されていた Lisa Office System は，PC で初めての GUI 環境の OS であった．その後，1984 年に発売された Apple の Macintosh では，ビットマップディスプレイ，マウスでの操作，オーバーラップするマルチウインドウなど現在の GUI 環境にほぼ近いものができあがった．

1990 年代に入り，Microsoft が本格的な GUI を搭載した Windows 3.0 を発売し，その後，Windows 3.1，Windows 95 と大ヒットし，PC 用 OS の不動の地位を確立した．その後，サーバ用 OS として開発された Windows NT と統合されて，Windows 2000，Windows XP，Windows Vista へと続いている．2009 年には Windows 7 が発売された．

(5) マイクロカーネルの誕生（1990 年代）

1990 年代を代表する OS 研究の動きは，マイクロカーネルである．マイクロカーネルとは，OS の機能のうち，必要最小限のみをカーネル（OS の中核部分）に残し，残りの機能をユーザーレベルで実現するという OS の設計思想である．マイクロカーネルの代表といえるのが，Mach である．実際には，1989 年にリリースされた Mach 3.0 からマイクロカーネル化された．

Mach では，タスクとスレッドという 2 段階の CPU 抽象化，ユーザーが変更可能な仮想記憶，ポートとメッセージにより実現される高度なタスク間通信機能など，革新的な OS 設計の見直しが行われた．マイクロカーネルの設計思想は，その後，商用 OS にも影響を与えた．

(6) Linux の誕生と発展（1990～2000 年代）

1900 年代に起きたもうひとつの大きな OS の動きは，Linux である．Linux は，1991 年に当時フィンランドの大学生であったリーナス・トーバルズが個人で開発を開始した．当初の Linux は，商用 UNIX や BSD 系 UNIX に比べてはるかに機能が劣っていたが，GPL（GNU Public License）で公開され，誰でも改造可能であったため，世界中の開発協力者の力を得て，急速に進歩した．Linux の発展により大きく注目を浴びるようになった，このオープンソースソフトウェア（OSS）の誕生は，その後のソフトウェアの開発形態を大きく変えた．現在，商用 OS の一部もかつては非公開だったカーネルのソースコードを OSS として公開しており，

また，データベース，アプリケーションサーバ，Web ブラウザなど多くのアプリケーション，ミドルウェアが OSS として開発・利用されている．

4-2-2 仮想マシンモニタ

仮想マシンモニタ（VMM）は，仮想化技術を提供する基本ソフトウェアであり，ハイパーバイザとも呼ばれる．VMM の歴史は，汎用機用 OS の歴史の原点である OS/360 の誕生と，ほぼ同時期に始まった．1967 年に開発された IBM の CP-40/CMS が，最初の VMM である．

VMM は，1990 年代後半から，大きな発展を遂げる．その発端となったのが，1998 年に発売された VMware である．VMware は，仮想化が難しいとされる，x86 アーキテクチャに対応したことにより，VMM の利用者層を大きく広げた．その後，x86 アーキテクチャに対応するオープンソースソフトウェアの VMM である，Xen が登場し，商用だけでなく研究の面でも，VMM は急速に発展した．Xen では，準仮想化という，ゲスト OS と VMM が連携する技術が導入されており，これによりゲスト OS の性能を大幅に向上した．準仮想化による高速化は，今では商用の VMM でも利用されている．また，x86 アーキテクチャ用の VMM の発展は，Intel VT や AMD-V などのハードウェアによる仮想化支援機能というハードウェアの進歩をもたらした．

4-2-3 アプリケーションサーバ

1990 年代半ばから，Web システムによる業務機能の提供が一気に増加した．これに先立って始まっていた，クライアント／サーバシステムに代わる新たなアーキテクチャの模索が Web システムに答えを見出した．これにより Web 3 層アーキテクチャが成立し，現在もメインストリームに位置している．このアーキテクチャの普及により，ブラウザ，アプリケーションサーバ，データベースというプロダクトラインが形成され，多くのベンダーが新しい領域であるアプリケーションサーバ（**図 4･1**）の開発に乗り出した．

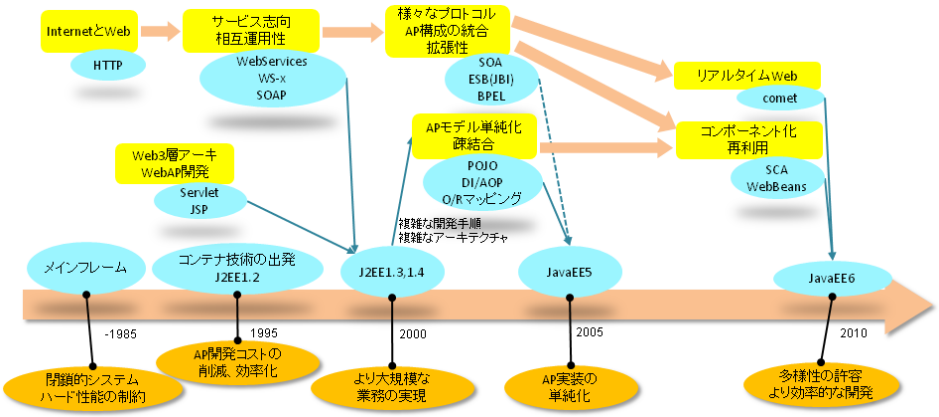

図 4･1　アプリケーションサーバの発展

(1) アプリケーションサーバ以前

1980 年代前半までのメインフレームの時代には，企業基幹システムの多くがメインフレームを利用したシステムであった．超高信頼なハードウェアやミドルウェアが保証する安定性がこの形態の存在意義を支えていた．

その後，ミニコンやワークステーションの出現に伴い，クライアント／サーバシステムの時代がやってきた．これは機能豊富なリッチクライアントと，比較的単純なサーバの組合せで構成された．メインフレームに比べ，安価なハードウェアを使うことでシステムのコストは下がったが，クライアントは複数の機器に点在するため，業務処理の更新時に多大なコストがかかっていた．

(2) アプリケーションサーバの出現と発展

クライアント／サーバシステムの欠点を解決するアーキテクチャとして，Web 3 層システムが 1990 年代半ばに成立した．ビューとビジネスロジックとデータを分離することで，それぞれを個別に開発し組み合わせて構成できる．これにより，基本ソフトウェアの進化のスピードが上がるなかで，頻繁に必要になったシステムの移行の際に，その影響範囲を限定できるようになった．

これに先立って，ブラウザと Web サーバの出現により，汎用のブラウザをクライアントとして，Web サーバがサーバ側でビューの詳細を定めるという仕組みが出現していた．Web 3 層システムは，これを取り込むことでクライアントの機能を業務によらない軽量なソフトウェア（ブラウザ）に限定し，業務処理の更新時にクライアントソフトウェアを更新することを原則として不要にした．

アプリケーションサーバの形態を方向付けたのは，Sun Microsystems が 1999 年から 2003 年にかけて発表した Java 2 Platform, Enterprise Edition（J2EE 1.2～1.4）である．エンタープライズアプリケーション向けの機能を追加した Java リリースであり，後述する Java EE 5 との対比において，第 1 世代のエンタープライズ Java と位置づけられる．主な機能には，アプリケーションの部品化を担う Enterprise Java Beans（EJB），Web サービス対応機能群，AP 間接続 JMS，トランザクション管理 JTA，アプリ開発の簡略化を狙った Java Servlet，Java Server Pages などがある．J2EE は機能仕様群であり，これを実装したソフトウェアは様々なベンダーや，オープンソースコミュニティによって提供されている．

(3) Web サービス

2000 年代に入り，あらゆるサービスを Web ベースの技術で提供するというコンセプトが支持され始め，2000 年 5 月には SOAP 1.1 が発表されて，システム間をつなぐ基本スキームとして SOAP を使うことで多くのベンダーが合意した．これは標準化団体 OASIS において，システム間結合に関する標準技術体系に発展し，Web サービス標準と呼ばれるようになった．Web サービス標準は膨大な機能を含んでいる．主なものをあげると，セキュリティ（アクセス制御，属性管理・伝播，ID 伝播，ID プロビジョニング，暗号化），ビジネスプロセス（業務手順の定型化と自動化），付加価値トランスポート（高信頼通信），システム管理（サーバ，データベース，ネットワークなどのリソース管理），などを含む．その後，SOAP に対抗するシンプルなアーキテクチャとして REST が，また，膨大な仕様の複雑さをプラットフォーム

に吸収させるための Enterprise Service Bus などのトランスポート抽象化技術が生まれた.

(4) DI コンテナ

J2EE は大きな発展を遂げたが，あまりに複雑な設計や API 構造のために，開発者には高いスキルが要求された．API が要求する決まりごとが多く，単純な機能を実現するためにも多数のコードを書く必要があった. そこで, 複雑性を排除し, モジュール間の依存関係をロジックと切り離したデザインパターンが考案され，主にオープンソースコミュニティの努力によって，J2EE と並行して発達した．主な技術的特徴である，Dependency Injection というデザインパターンから, DI コンテナと呼ばれる. DI コンテナのさきがけとして代表的なものに, オープンソースの Spring Framework がある. また後には, J2EE の流れを汲む Java EE5 / EJB 3.0 にも DI コンテナが取り入れられた.

■参考文献

1) 電子情報通信学会ハンドブック委員会, “エンサイクロペディア 電子情報通信ハンドブック,” オーム社, 1998.
2) A. S. タネンバウム, “OS の基礎と応用,” トッパン, 1995.
3) “An Introduction to the Java EE 5 Platform”
   http://java.sun.com/developer/technicalArticles/J2EE/intro_ee5/
4) “The Java History Timeline”
   http://java.com/en/javahistory/timeline.jsp
5) “OASIS Standards and Other Approved Work”
   http://www.oasis-open.org/specs/
6) “Spring Source COMMUNITY”
   http://www.springsource.org/

■14 群 － 1 編 － 4 章

4-3 分散コンピューティング

（執筆者：小山和也）［2009 年 3 月 受領］

4-3-1 概　要

近年，コンピュータシステムはネットワークに接続されることが当たり前になっている．特に，異なるシステムの間でデータを転送するだけではなく，一つの目的を達成するシステムを，ネットワークで接続された複数のコンピュータを用いて実現する分散コンピューティングは，インターネットの普及と相まって，コンピュータのあり方に大きな影響を与えてきた．ここではこの分散コンピューティングの技術の進展の一遍を述べる．

4-3-2 コンピュータネットワークへの萌芽（1970 年代前半）

1960 年代後半から 1970 年代前半にかけて，コンピュータの中心は，センターにある大型計算機を遠隔の端末から利用者が自由に使う，TSS（Time Sharing System）であった．1963 年に MIT（Massachusetts Institute of Technology）により CTSS が開発され，その後 1964 年から 1969 年にかけて UNIX を生み出すきっかけとなった Multics が開発された．

このような TSS に対して，1970 年代，Xerox 社のパロアルト研究センター（Palo Alto Research Center）において，現在の LAN 分散システムの発端となる，ワークステーション Alto と関連する分散システムが研究開発された．その狙いは，利用者に対するユーザーインタフェースの改善を重視するために，TSS のような大型計算機の利用ではなく，利用者にパーソナルコンピュータ提供すべきというものであった．そしてそれらを高速なネットワークで接続し，更に TSS の大型計算機が提供していた機能を分散してサーバとして配置する．1972 年に Alto が，1973 年にイーサネットが開発され，その後 1977 年にはファイルサーバである Xerox DFS が開発されている．これら技術は Xerox 社の製品として商用化され，広く普及するには至らなかったものの，その後の技術開発に大きな影響を与えた．

一方，1969 年，米国の大学や研究機関のもつ TSS システムを相互接続した学術用ネットワーク ARPANET が稼働し，コンピュータの大規模な相互接続が始まった．更に，Multics に対し，先進的であったが複雑すぎたとの反省から，よりコンパクトな OS である UNIX が 1970 年代にベル研究所によって開発され，米国の大学や研究機関に普及し始めた．

4-3-3 ネットワークアーキテクチャの発達（1970 年代後半）

1970 年代後半は，企業各社による独自ネットワークアーキテクチャの出現と充実が進んだ．1974 年に，IBM 社は SNA（System Network Architecture）として，独自仕様のネットワークアーキテクチャを発表した．これは，TSS で主流であった TSS の端末-センター間の接続に加えて，センター同士を結ぶネットワークが必要になってきたという背景があった．更に IBM 社は 1974 年に新 SNA を発表，1976 年に UNIVAC 社が DCA を発表し，更に他社も次々に独自ネットワークアーキテクチャを打ち出した．このような複数の異種ネットワークアーキテクチャの登場と，相互接続の必要性から，1977 年には，ISO において標準アーキテクチャの検討が開始された．

4-3-4 LAN 分散システムの実用化（1980 年代前半）

1980 年代前半になると，LAN 分散システムが実用期に入り，TCP/IP やその上のアプリケーションのプロトコルなど，現在も広く使われる LAN 分散システムの基盤が形作られた．

1980 年には Sun Microsystems 社の Sun Workstation や，Apollo 社の Apollo Domain，1983 年には Novel 社の NetWare など，商用の LAN 分散システムが開発された．

また，Xerox パロアルト研究センターが開発したイーサネットは，1990 年に Ethernet 1.0 として IEEE で標準化され，その後 1982 年に現在使用されているイーサネットのベースとなる Ethernet 2.0 も公開された．1983 年には ARPANET が TCP/IP に全面移行し，TCP/IP 上での各種プロトコルも，1980 年にはファイル転送プロトコル FTP が，1982 年には電子メールのプロトコル SMTP が，1983 年には名前解決サービスの DNS が IETF の RFC として公開された．また 1985 年には Sun Microsystems 社の NFS（Network File System）が初めて発表された．

分散コンピューティングの基盤である RPC（Remote Procedure Call）も併せて実用化された．RPC 自体は 1970 年代には既に存在していた概念であったが，1981 年にはその初の商用実装として Xerox 社の Courier が開発され，1984 年には NFS の一部として現在も広く利用されている ONC（Open Network Computing）RPC も開発された．また 1982 年には，UNIX でのプロセス間通信用 API のデファクトとなるソケット（Berkeley sockets）も開発された．

一方，1977 年に開始された ISO による標準ネットワークアーキテクチャの成果として，1984 年に開放型システム間相互接続（OSI）の参照モデルが完成し，その後，実システムでの利用は TCP/IP がデファクト標準となるものの，階層型モデルの概念の普及に大いに寄与した．

また研究レベルでは，アプリケーションにネットワークによるサーバの分散を意識させない分散 OS が研究され，1982 年には Stanford 大学により V System が，1983 年には Vriji 大学により Amoeba が開発された．

4-3-5 LAN 分散システムの普及（1980 年代後半）

1980 年代後半に入ると，UNIX による LAN 分散システムは急速に普及し，関連技術も発展を遂げた．1988 年には機器の監視・制御のための SNMP が，1989 年には NFS v2 が RFC として公開された．また 1988 年には Carnegie Mellon 大学の分散ファイルシステムの AFS も開発された．

この時期は，企業内システムを従来のメインフレームなどの大型計算機から LAN 分散システムに置き換える「ダウンサイジング」が流行し始める一方で，UNIX のベンダー間で「UNIX 戦争」などと評される標準規格を巡る争いが起きた時期でもあり，1988 年には OSF（Open Software Foundation）や UI（UNIX International）の二つのオープンな UNIX 標準を決める団体が結成されるなど，この争いは 1990 年代前半まで続いた．

一方，この時期は分散 OS の開発も進み，実用性を目指した UNIX 互換の分散 OS が開発された．1986 年には，Carnegie Mellon 大学により Mach が開発され，その後 Mach は OSF の最初の OS である OSF/1 のベースとして採用された．また 1988 年には INRIA で研究発されてきた Chorus が Chorus Systems 社から商用製品化された．

4-3-6 クライアントサーバ型システムの普及（1990 年代前半）

1990 年代前半は，UNIX が規格争いを続ける一方，PC のハードウェアの性能向上や低価格

化が進み，更に 1990 年の Microsoft の Windows 3.0 の発売などを通し，PC の重要性が飛躍的に高まった．この結果，1990 年代前半は，企業システムにおいて「クライアントサーバ型システム」と呼ばれる形態が急速に普及した．これは分散システムのソフトウェアモデルである広義クライアントサーバではなく，PC 上に UI とビジネスロジックを含んだクライアントアプリケーションをインストールし，サーバ上にデータベースを置いて通信させる 2 層アーキテクチャのシステム構築方法のことであり，従来の TSS による端末-センター型の企業システム構築と比較して，システム構築や運用コストを大きく低減させるものであった．しかしながらこの方式は，クライアントアプリケーションの管理が極めて煩雑になるという課題も含んでいた．

また，分散コンピューティング基盤として，従来の RPC の概念をオブジェクト指向に適用する分散オブジェクトを実用化しようとする動きが産業界全体で起こり，1991 年，OMG（Object Management Group）により，プラットフォームやプログラミング言語に依存せずに分散オブジェクトを実現する標準仕様の CORBA 1.1 が公開された．

一方，1992 年には，CERN により WWW（World Wide Web）が開発された．当初の WWW はハイパーテキストを分散化した分散ドキュメントシステムであったが，その後，様々な分散コンピューティング基盤として発展を遂げることとなる．

4-3-7 WWW の普及と分散オブジェクト指向の普及（1990 年代後半）

1990 年代中盤になると，WWW が一般ユーザー向けに爆発的に普及し始めた．同時に，当初は固定的な文書中心であったページの内容が，プログラムによって動的にされるようになり，様々なアプリケーションの GUI として利用され始めた．これは，WWW が，WWW ブラウザさえ用意しておけば PC にはクライアントアプリケーションのインストールが不要となることで，従来のクライアントサーバ型システムで問題であったクライアントアプリケーションの管理コストを低減させられたことによる．すなわち，この頃から WWW はシンクライアント型の分散コンピューティング基盤になったといえる．

WWW が分散コンピューティング基盤と見なされるのと同時に，WWW の GUI はクライアントアプリケーションに比べて操作性が劣るという問題が指摘され，それを解決するための RIA（Rich Internet Application）技術が登場した．1995 年には，Sun Microsystems 社からプログラム言語 Java が発表された．当初の Java は実行コードの可搬性を特徴とし，アプリケーションの実行コードを WWW コンテンツの一部として PC に読み込み，実行することで RIA を実現する用途がアピールされた．しかし，その後は広くネットワークでの利用に有利なオブジェクト指向言語として強化され，1997 年には WWW のサーバ側で利用する Servlet の仕様も公開され，アプリケーションサーバとして Web アプリケーションの構築に用いられるようになった．

この時期は同時に，分散オブジェクトの普及が進んだ．1995 年には相互接続性が強化された CORBA 2.0 が発表された．加えて Java が分散オブジェクトを取り入れ，まず 1995 年に産業技術総合研究所から Horb が発表され，1996 年には Sun Microsystems 社から Java RMI（Remote Method Invocation）が，更に 1997 年には CORBA サポートが追加され，アプリケーションサーバを中心に利用され始めた．1996 年には，Microsoft 社からコンポーネント技術 COM（Component Object Model）を分散対応した DCOM が発表された．

4-3-8 Web サービスへの挑戦（2000 年代前半）

1990 年代後半から産業界を中心に，普及した WWW と分散オブジェクトの技術を融合，発展させた分散コンピューティング基盤として，Web サービスへの取り組みが始まった．Web サービスは RPC や分散オブジェクトの仕組みを，WWW の標準的技術である HTTP や XML のみを用いて実現するもので，RPC 相当として 1998 年に XML-RPC が，1999 年に SOAP が発表された．また 2000 年には，インタフェース記述言語の WSDL と，レジストリサービス仕様の UDDI も発表された．

Web サービスは，人間に対する GUI のみの WWW の世界をコンピュータ間通信にも拡大しようとする狙いと，CORBA で実現した異種システム間での分散オブジェクトを，通信インフラ化した WWW を利用してより疎結合に，WAN 上で利用可能にしようとする狙いがあり，新たな分散コンピューティング基盤として多くのベンダーから注目を集めた．その結果，登場まもなくベンダー間での通信プロトコルの激しい標準化競争が発生し，メッセージの暗号・署名規格である WS-Security 1.0 の標準化が 2004 年になるなど，標準化が遅れた．加えて XML の処理負荷による通信性能の問題も加わり，企業システムへの普及は伸び悩むこととなった．

一方，目的は同じながら，より単純に WWW 技術を利用してコンピュータ間通信を実現しようとする動きが，一般ユーザー向けサービスで始まっていた．代表的なものは WWW のサイトの更新情報を XML で配信する RSS で，1999 年に最初の仕様である RSS 0.9 が開発されて以降，WWW でのウェブログ（Blog）サービスの流行と相まって広く普及した．

4-3-9 サービス化の進展（2000 年後半）

当初の Web サービスは，RPC やメッセージングなど，従来からある通信方式の代替物と見なされることが多かったが，2000 年代の中盤から，Web サービスを使用した分散システムのアーキテクチャとして SOA（Service Oriented Architecture）という概念が普及し始めた．SOA は，従来のコンポーネント指向の延長として，全く別の目的に第三者によって構築された一つのアプリケーションシステムをコンポーネントとして扱い，それらを組み合わせて新しいアプリケーションを構築しようとするものであり，アプリケーションの構築方法に変化をもたらした．

この考えは，特に一般ユーザー向けサービスにおいてマッシュアップという言葉で広く普及した．2006 年に Google が地図サービス上に自由にデータを追加表示できる Google Maps API サービスを開始すると，ほかの様々な既存サービスから位置情報を取得し，それを Google Maps 上に表示させるというマッシュアップサービスが多数構築された．

4-3-10 おわりに

2000 年後半にサービス化が進展した結果，インターネットと WWW によって構築された世界は，全体で巨大な分散コンピューティング基盤となりつつあるといえる．現在はまだインターネット上のサービスに閉じているが，今後は携帯電話やセンサなどを通し，物理的な世界との関連も強まっていくことが予想される．一方で，セキュリティ，信頼性，性能，データ統合など，今後解決していかなければならない課題も多数あり，今後もこの分野の発展が期待されている．

■参考文献

1) G. Coulouris, J. Dollimore, and T. Kindberg, “分散システム コンセプトとデザイン,” 電気書院, 1991.
2) A. S. Tanenbaum, “分散オペレーティングシステム,” プレンティスホール出版, 1996.
3) 坂下善彦, 井手口哲夫, 滝沢 誠, 水野忠則, “分散システム入門”, 近代科学社, 1993.
4) 河込和宏, 中村秀男, 大野邦夫, 飯島 正, “分散オブジェクトコンピューティング”, 共立出版, 1999.

■14 群 － 1 編 － 4 章

4-4 情報システム

（執筆者：田淵仁浩）［2009 年 3 月 受領］

本節では，情報システムを「組織体（または社会・個人）の活動に必要な情報の収集・蓄積・処理・伝達・利用にかかわる仕組みを，コンピュータを中心とする機械的機構を用いて実現したシステム」と定義し，その発展の歴史について述べる．

4-4-1 EDP (Electronic Data Processing) システム

当初，科学技術計算を目的に発展したコンピュータは，1950 年代から 1960 年代にかけて，企業における事務処理の効率化・省力化を図るために用いられるようになっていった．大量の事務処理データを記録し，計算することが可能なデータ処理技術を実装したメインフレームコンピュータの登場により，これを用いた EDP（Electronic Data Processing）システムは，主に大企業で，例えば，給与計算，売上計算，会計処理などに使われるようになった．

4-4-2 オンラインリアルタイムシステム

1960 年から 1970 年代には，通信技術，トランザクション処理技術，データベース技術が発達し，メインフレームコンピュータと入出力端末とを専用の通信回線で接続したオンラインリアルタイムシステムが実用化されるようになった．例えば，鉄道会社や航空会社の座席予約システムでは，地域的に分散したサービス拠点の入出力端末から通信回線を介して，メインフレームコンピュータに座席予約の要求情報を送信し，座席予約を確定するトランザクション処理の結果を，再び，サービス拠点の入出力端末にリアルタイムに返すことができるようになった．オンラインリアルタイムシステムの実用化により，企業が提供するサービスを地域的に離れた場所でも，即座に受けられるようになり，銀行など金融機関の勘定系システムや ATM 網などの発展の基礎となっている．

4-4-3 経営情報システム (Management Information System)

EDP システムで大量データ処理技術やオンラインリアルタイムシステムでオンライントランザクション処理技術が実用化されてきた 1970 年代には，企業においては，従来の経験に頼っていた経営をコンピュータ利用によって効率化する目的で，経営情報システム（Management Information System）が導入されるようになった．経営情報システムは大量のデータを集計して経営の各層に瞬時に提供することを目的としていたので，オンライントランザクション処理やデータベース技術が用いられた．経営者が業務上の判断を行う際に必要な情報を，必要なときに提供するシステムを目指したが，満足な性能を達成できず広く普及しなかった．当時のコンピュータ技術では，過去から現在に至る大量の売り上げデータを多角的に分析したり，分析結果をわかりやすく要約して提供したりする機能を，意思決定者が必要なときに得られるような性能を達成できなかったためである．しかし，コンピュータシステムを利用して，経営者の意思決定に有効な情報を提供する考え方は，その後の企業向け情報システムに大きな影響を与えた．

4-4-4 意思決定支援システム（Decision Support System：DSS）

1970 年代から 1980 年代には，コンピュータの処理性能の向上や扱えるデータ量の増大に加えて，TSS（Time Sharing System）技術や対話型コンピュータ技術の進展を背景に，経営者がコンピュータを対話的に直接操作することを想定した意思決定支援システム（Decision Support System：DSS）が導入されるようになった．意思決定支援システムは，企業活動における意思決定に必要とされる知的資源を提供するための情報提供を支援するシステムである．企業活動にかかわる様々な経営情報を蓄積し，意思決定者（経営者）自身が対話的に検索・分析・加工・シミュレーションを行える点に特長がある．意思決定者が能動的に経営情報を検索・分析・加工・シミュレーションすることで，企業の経営状態を俯瞰的に把握して，意思決定の質や有効性の向上を図る目的で，情報システムを利用する考え方に基づいている．

4-4-5 オフィスオートメーション（Office Automation）

1970 年代から 1980 年代には，オフィスコンピュータ（オフコン）やパーソナルコンピュータ（パソコン）などコンピュータのダウンサイジング技術，コンピュータネットワーク技術の進展に伴い，オフィスにおける事務作業を各種の電子機器を用いて効率化することを目的としたオフィスオートメーションシステムが導入されるようになった．具体的には，従来は手作業で行われていた事務作業を，オフコン，パソコン，ワードプロセッサなどの OA 機器と，表計算やデータベースなどのデータ管理ソフトウェア，文書処理ソフトウェア，及び LAN（Local Area Network）などを使って，できる限り合理化・省力化することで業務を改善することを目的としていた．コンピュータのダウンサイジングが急速に進展し，パソコンの低価格化・高性能化が進むと，情報システムは一部の専門家のみで管理統制するものから，一般従業員も開発・運用の一部を担うものへと大きく変わっていった．例えば，表計算ソフトを使って部門固有のシステムを，情報システムの非専門家であるエンドユーザー部門で開発・運用するようになり，いわゆるエンドユーザーコンピューティング（EUC：End User Computing）が広く普及する契機となっていった．

4-4-6 戦略情報システム（Strategic Information System：SIS）

コンピュータの性能向上やネットワークの進展に加えて，大量データ処理技術が進展することにより 1980 年代には，情報システムを経営戦略・事業戦略を実現するうえでの資源として活用し，競争優位を獲得する手段に用いる戦略情報システムの考え方が登場してきた．戦略情報システムは，競合他社に打ち勝つための企業戦略を推進・実践するための手段として活用する目的で実現した情報システムと考えられる．例えば，ある航空会社は他社の航空会社の座席やホテルなど，その他の付帯サービスの予約購入を可能とするように，自社の座席予約システムを開発し，旅行代理店に開放することで，旅行代理店の囲い込みに成功し，シェアの向上に寄与している．一般に，企業にとって情報システムは重要な経営資源の一つだが，自社の情報システムにパートナー企業のシステムをネットワーク技術によって接続することで，競合他社に対して競争優位を確立する手段として情報システムを活用する例として捉えることができる．

4-4-7 企業資源統合計画（Enterprise Resource Planning：ERP）システム

1990 年代に入ると，コンピュータのダウンサイジングが一層進展するとともに，企業内のネットワークも普及した結果，企業内の業務処理をすべてカバーする情報システムを導入することが可能になってきた．一方で，従来の情報システムが，会計や人事／給与，販売，購買，在庫管理などの業務に合わせて，部門ごとに導入されてきたために，企業経営の視点から，業務全体を通した経営状況のリアルタイムな把握などに課題が認識されていた．

企業資源計画（ERP）システムは，生産や販売，在庫，購買，物流，会計，人事／給与などの企業内の経営資源（ヒト・モノ・カネ）を有効活用する目的で，経営資源を統合に管理し，最適に配置・配分する計画を立てられるようにすることにより，効率的な経営活動を行う経営手法を支援する情報システムである．ERP システムを導入すると，生産や販売，在庫，購買，物流，会計，人事／給与などの基幹業務全般の情報インフラを整備できるので，日常業務で発生するデータの収集・一元管理を実現し，各部門で共有できるようになる．その結果，経営者だけでなく，各種の部門の管理者も，意思決定や経営判断を迅速に行える．

従来の企業向け情報システムと比較して，ERP システムに特長的な機能は，以下があげられる．

(1) 経営状況のリアルタイムマネージメント

基幹業務におけるマスタデータ（製品や取引先情報など）やトランザクションデータ（会計伝票や受注伝票）をデータベース上で統合することにより，関連した業務とデータが一元的に管理できるようにしている．また，モノの動きに連動してカネの情報も同時に更新される仕組みを提供することにより，業務処理の実行と同時に関連するデータがすべて更新されるので，常に最新の経営情報にアクセスできるようにしている．その結果，経営トップから一般社員に至るまでリアルタイムに経営状況や業務内容を把握できるようになる．

(2) 業務の統合化

部門ごとに業務遂行を独立して行うことが前提となっている従来の情報システムを部門別に導入している場合には，全社レベルでは業務プロセスを分断し，部門間を横断した業務プロセスの一貫性を維持することが困難であった．ERP システムでは，販売管理，在庫管理，生産管理，購買管理など複数の業務分野をまたがる「処理フロー」を提供し，各業務のデータ間の整合性を維持することで，部門間を横断した統合業務プロセスを実現できるようになる．一般的なデータベース = RDBMS（リレーショナルデータベース管理システム）の排他制御だけでは，ロックがレコード単位だったり，テーブル単位でしかロックがかけられなかったりするため，統合業務プロセスの処理フローの実現には不十分であった．しかし，ERP システムでは，関連するデータをひとまとめにして一度に排他制御をかける仕組みを用意することで，課題を解決している．

4-4-8 2000 年代以降の情報システム

2000 年代になると，企業経営における業務革新・事業改革・経営資源の有効活用を目的とした多くのシステムが実用化されてきている．以下では，代表的な情報システムの技術動向について紹介する．

(1) Business Process Re-engineering (BPR)

BPR は，高度に専門化され，プロセスが分断された既存の分業型組織や分業型の業務ルールを抜本的に見直し，“ビジネスプロセス”（業務の流れ）の視点で職務，業務フロー，管理機構，情報システムを再設計（リエンジニアリング）するという経営的な対応法，及び，それを実現するシステムである．前述の ERP システムなどを用いた情報システムとして実現され，複数の業務プロセスや業務システムを統合・制御・自動化し，業務フロー全体を最適化する技術やツールとして実用化されている．

また，ビジネスプロセスに「分析」「設計」「実行」「モニタリング」「改善・再構築」というマネジメントサイクルを適用し，継続的な BPR を遂行する経営・業務改善コンセプトを意味する Business Process Management と合わせて論じられることが多い．

(2) Sales Force Automation (SFA)

SFA は，パソコンやインターネットなどの情報通信技術を活用して，企業の営業部門を効率化するための情報システムである．販売要員と呼ばれる契約社員が多く離職率が高い米国企業の営業部隊において，営業プロセスを確立・管理することで，人員に変動があっても営業活動の品質を一定にする目的で実用化された情報システムである．

営業プロセスを標準化するために，営業日報機能などによる商談の進捗管理機能（コンタクト管理，行動管理，評価・実績管理），グループウェアや顧客データベースによる営業部内の情報共有機能などが提供され，個人の営業員支援，及び営業部門マネージャが営業担当者を管理するシステムとして導入された．SFA システムで一元管理された顧客データベースを利用し，顧客リストを分析して見込み客や優良顧客を抽出するという，データベースマーケティングやキャンペーンマネジメントなどの要素が付け加わった結果，後述の CRM の一環として扱われることもある．

また，データベースに顧客情報のほか，コンタクト履歴や商談のプロセス，営業スケジュールを蓄積し，営業案件の進ちょく状況や案件成立の見込みを営業チーム内で共有することにより，従来は個人プレーだった営業活動を営業部門全体で戦略的に行えるようになった．

更に，各部門から集められた見込み客情報や販売情報などが営業担当者に提供する機能や営業エリア情報，営業資料を参照する機能などを盛り込んだシステムや，在庫情報などを扱う基幹システムと連動させることで，外出先からモバイル端末や携帯電話を使い，在庫状況や見積もりなどを取得し，素早い顧客対応を実現するシステムもある．

(3) Customer Relationship Management (CRM)

CRM は，企業が提供する商品やサービスを介して，顧客との間に「親密な信頼関係」（リレーションシップ）を長期的・継続的に構築することで，顧客にとっての価値と企業の収益の向上を目指した総合的な経営手法，及び，その手法の効率的な実現を支援する情報システムである．例えば，詳細な顧客データベースを元に，商品の売買から保守サービス，問い合わせやクレームへの対応など，個々の顧客とのすべてのやり取りを一貫して管理することにより，「親密な信頼関係」を実現する．

例えば，CTI（Computer Telephony Integration）による「コールセンターソリューション」を CRM システムとして導入する場合，CTI と顧客データベースを連動させることによって，

コールセンターへ着信と同時にオペレータ席のコンピュータ画面に顧客データが自動的に表示され，顧客は的確な対応を受けることが可能となる．結果として，顧客満足向上とコールセンターオペレーションの効率化が達成できる．

また，顧客のニーズにきめ細かく対応することで，顧客の利便性と満足度を高め，顧客を常連客として囲い込んで収益率の極大化をはかることを目的としたシステムも登場している．

(4) Supply Chain Management (SCM)

SCM は，ビジネスプロセスの全体最適を目指す戦略的な経営手法を実現する情報システムである．主に製造業や流通業で，原材料や部品の調達から製造，流通，販売という，生産から最終需要（消費）にいたる商品供給の流れを「供給の鎖」（サプライチェーン）と捉え，それに参加する部門・企業の間で情報を相互に共有・管理する．取引先との間の受発注，資材の調達から在庫管理，製品の配送まで，事業活動の川上から川下までをコンピュータを使って総合的に管理することにより，余分な在庫などを削減し，コストを引き下げる効果がある．

SCM システムは，販売実績情報から需要を予測し，予測をベースに生産計画・在庫計画・販売計画及び補充計画を同期・最適化することで，計画に沿った生産や物流を行えるように支援する．そのために，原材料や部品の供給者は，できる限りリアルタイムに近く，精度の高いデータを相互にやり取りする仕組みを構築する必要がある．

■参考文献

1) 倉沢良明, “情報システムにとっての SOA の役割,” 情報処理, vol.46, no.3, 情報処理学会, 2005.
2) Michael Hammer, “Reengineering Work: Don't Automate, Obliterate,” Harvard Business Review 1990 Jul.-Aug.
3) マイケル・ハマー, “情報技術を活用した業務再構築の 6 原則,” DIAMOND ハーバード・ビジネス・レビュー 1994 年 1 月号.（“Reengineering Work: Don’t Automate, Obliterate”の邦訳）.
4) マイケル・ハマー, ジェイムズ・チャンピー, (野中郁次郎監訳), “リエンジニアリング革命－企業を根本から変える業務革新,” 日本経済新聞社, 1993 年 11 月.（“Reengineering the Corporation: A Manifesto for Business Revolution”の邦訳）.
5) D. J. Power, “A Brief History of Decision Support Systems,” DSSResources.COM, World Wide Web, http://DSSResources.COM/history/dsshistory.html, ver.2.8, May 2003.
6) 高橋　茂, “日本のコンピュータメーカーと 7 人の小人(1),” 情報処理, vol.44, no.8, 情報処理学会, 2003.
7) 高橋　茂, “日本のコンピュータメーカーと 7 人の小人(2),” 情報処理, vol.44, no.9, 情報処理学会, 2003.
8) 文部科学省, “科学技術白書,” http://www.mext.go.jp/b_menu/hakusho/hakusho.htm#gijyutu
9) 社団法人情報処理学会, “コンピュータ博物館,” http://museum.ipsj.or.jp/index.html
10) “IBM Archives: Valuable resources on IBM’s history,” http://www-03.ibm.com/ibm/history/index.html
11) “Intel Computer Archives,” http://www.intel.com/museum/archives/index.htm
12) 鈴木弘幸, “実践 SIS 入門－企業と情報戦略,” 工業調査会, 1990.
13) チャールズ・ワイズマン (土屋守章, 辻　新六 訳), “戦略的情報システム－競争戦略の武器としての情報技術,” ダイヤモンド社, 1989.（“Strategic Information System” の邦訳版）.

■14 群 － 1 編 － 4 章

4-5 情報セキュリティ

（執筆者：側高幸治）［2009 年 3 月 受領］

情報セキュリティの技術史は，主に暗号技術の発展が中心であると考えることができる．暗号技術は古くは紀元前から用いられており，最古の暗号は古代エジプトで書かれた象形文字であるといわれている．それ以降，時代の変化に伴い暗号技術も変化していったが，第一次世界大戦及び第二次世界大戦においては暗号の重要性が大きくなり，暗号を解読できるか否かが戦争の勝敗を決するといっても過言ではなかった．また，コンピュータの出現により暗号は複雑になり解読が困難なものになり，更にインターネットの誕生により，暗号技術は広く企業活動並びに個人の生活と密接な関係をもつようになった．

それにより暗号技術は情報セキュリティ技術として，情報資産の機密性，完全性及び可用性を維持するための技術や，真正性，責任追跡性，否認防止及び信頼性のような特性を維持する技術として組み込まれ，今日に至るまで発展を続けている．

4-5-1 DES

戦時中までに使用されていた暗号は，鍵のみならず暗号アルゴリズムが当事者間で秘密にされていた．これらの暗号の用途は軍事及び外交であったため，鍵と暗号アルゴリズムを秘密にすることにより暗号文の解読を防止していた．しかし，戦後の世の中において不特定多数の間で暗号通信を行う必要性から，米国商務省標準局は米国政府の標準暗号方式を公募し，1977 年に DES（Data Encryption Standard）を制定した．DES が戦時中まで使用されていた暗号と大きく異なる点は，暗号アルゴリズムが公開されている点であり，DES の誕生以降の暗号は現代暗号と呼ばれている．

暗号アルゴリズムを公開するメリットとしては，（鍵の共有は必要であるが）不特定多数との通信が行える点に加えて，暗号アルゴリズムが安全で確かであることを第三者が確認できる点があげられる．DES は制定以来，長年にわたって米国のみならず世界の標準暗号となったが，1993 年に鍵の総当り攻撃よりも効率的な解読方法（線形解読法）が示され，1990 年代後半にはコンピュータの進化により総当り攻撃を用いて完全に解読されることが明らかになり，その使命を次第に終えつつある．

4-5-2 ディフィー・ヘルマン（Diffie-Hellman）鍵共有

戦時中までに使用されていた暗号方式は，暗号文の送信者と受信者の間で暗号化及び復号に使用する鍵を共有する方式（共通鍵暗号方式）が常であり，どのように鍵を安全に共有するかが課題となっていた．1976 年にディフィー（Diffie）とヘルマン（Hellman）は共通鍵暗号方式において使用する鍵（共通鍵）の受け渡しを安全に行うために，公開鍵暗号方式の始まりとなるディフィー・ヘルマン（Diffie-Hellman）鍵共有プロトコルを提案した．

本プロトコルは送信者と受信者がそれぞれ公開鍵と秘密鍵を用意し，公開鍵のみをお互いに公開する．自分のみが知っている秘密鍵を用いて共通鍵を作成する方式である．それまでの暗号＝共通鍵暗号方式では，鍵を秘密にするすることが安全性を確保する手段であったため，鍵を公開するという公開鍵暗号方式のアイディアは非常に斬新であったと考えられる．

4-5-3 RSA 暗号

ディフィー（Diffie）とヘルマン（Hellman）によって発表された公開鍵暗号方式の概念を受けて，1977 年にはリベスト（Rivest），シャミア（Shamir），エーデルマン（Adleman）により公開鍵暗号方式の概念の満たす数値上の変換方式を発表し，発明者の頭文字を取り RSA 暗号と呼ばれるようになった．RSA 暗号は公開鍵を用いた暗号化と秘密鍵を用いた復号（秘匿），及び秘密鍵を用いた署名と公開鍵を用いた検証（認証）として使用できることが特徴である．

RSA 暗号は，今日においても広く使用されている技術であり，秘匿は共通鍵暗号方式の共通鍵を暗号化する用途，認証は電子署名の用途で使用されている．

4-5-4 公開鍵基盤（PKI）

公開鍵暗号方式の利用において，なりすましなどの脅威に対抗するために，公開鍵と秘密鍵の鍵ペアを保持していることを確認する手段が必要となる．その手段として 1988 年に ITU-T により公開鍵基盤（Public Key Infrastructure，以下 PKI）の規格である X.509 が制定された．X.509 では公開鍵証明書の形式や，公開鍵証明書の検証アルゴリズムなどを定めており，現在では，1997 年に制定された公開鍵証明書の形式が使用されている．

PKI は公開鍵証明書を発行する認証局を信頼の基盤とすることで成立するモデルであり，IETF PKIX（Public Key Infrastructure working group）において，PKI を実現するために必要な公開鍵証明書の設定項目や，公開鍵証明書を利用したプロトコル及び認証局運用規程などの運用面について標準化が進められている．また公開鍵暗号方式として RSA 暗号を使用している例が多く，SSL，電子署名，認証など多くの場面で使用されている．特に SSL については多くのインターネットブラウザでサポートされており，PKI の代表的な利用例となっている．また，PKI は各国の政府機関において多く使用されていることも特徴の一つである．

4-5-5 AES

DES は登場以来，20 年以上にわたって世界の標準暗号であったが，コンピュータの進化に伴い DES の信頼性は次第に低下していき，総当り攻撃で解読されるようになった（本章 5-5-1 項参照）．これを受けて米国国立標準技術研究所（NIST）は 1997 年に DES の後継暗号として AES（Advanced Encryption Standard）として共通鍵ブロック暗号アルゴリズムの公募を実施し，選定プロセスを経た後に 2001 年にダーメン（Daemen）とライメン（Rijmen）による Rijndael が採用された．今日では，AES は DES に代わって世界の標準暗号となっており，様々な製品や規格に採用されている．

4-5-6 ファイアウォール

1990 年代後半から，自社の Web サイトをインターネットに接続する企業が急激に増加し，それに伴い Web サイトの不正改ざんなどの事件が多く発生した．また，企業間取引にインターネットを利用することが当たり前となり，これに伴い組織内のネットワークへ第三者の侵入を防ぐ必要性からファイアウォールの導入が広まった．また，ファイアウォールはソフトウェアとしての提供のみではなく，ハードウェアに組み込まれて提供されることも多いため，導入が広まった背景の一つとして考えられている．

ファイアウォールは，基本的にはネットワークを通過するパケットやアプリケーションを

監視することで，許可されたパケット及びアプリケーションのみを通過させる方式を採用しているため，監視する方針（セキュリティポリシー）の設定が重要となる．また，ファイアウォールではセキュリティポリシーで許可されたアクセス手段を利用した攻撃を防御することができないことから，不正侵入を検出するための侵入検知システム（Intrusion Detection System：IDS）を組み合わせて利用されることが多い．

4-5-7 ディジタル著作権管理（DRM）

インターネットの普及に伴い，楽曲や映像を中心としたコンテンツがディジタル化され，ネットワーク上でこれらのデータ交換や配信が可能となり，2000 年代後半にはコンテンツ配信サービスがビジネスとしても成立するようになっていった．ディジタル化されたデータは品質が劣化することなく誰でも容易に複製できることから，コンテンツの権利者を保護するために，コンテンツに対してコピー制御及び視聴制限を行う技術としてディジタル著作権管理（Digital Rights Management，以下 DRM）技術が注目を浴びるようになった．

DRM 技術には様々な方式があるが，基本的にはコンテンツを暗号化し，利用者が対価を支払った場合にのみコピーや視聴を許可する方式である．DRM 技術は，コンテンツ権利者を保護すべきという主張と，利用者の利便性を損なうものであるという主張が衝突することが多く，両者の主張をすべて満たすような技術は存在していない．また，利用者の主張が次第に大きくなっていること，及び，いくつかの DRM 技術については制限を解除する手法が発見されていることもあり，近年では DRM 技術を施さずに別の方式でコンテンツを保護する方式も検討されている．

4-5-8 無線 LAN

2000 年代に入ると，ノート型パソコンとブロードバンドネットワークの普及に伴い，無線 LAN が設置の容易さから急速に普及した．無線 LAN はアクセスポイント（親機）とパソコンなどの子機の間で無線通信を行うものであり，オフィスや家庭内での使用のみでなく，アクセスポイントを広く公衆に開放する公衆無線 LAN サービスもサービスエリアの拡大に伴い利用者を増やしている．また，子機としてはパソコンに限定せず，携帯型ゲーム機などでも使用されている．無線 LAN はその特性から，第三者に通信内容を傍受される可能性があるため，不正利用及び盗聴に対するセキュリティ対策が重要となっている．

無線 LAN は IEEE の 802.11 シリーズにおいて規格が制定されており，また Wi-Fi alliance によってもセキュリティ仕様が制定されている．これらの規格及び仕様では，通信を暗号化する方式やアクセスポイントが端末を認証する方式が制定されているが，無線 LAN は利用者の利便性を高めるという性質から，機器の基本設定はセキュリティレベルが低く設定されていることが多い．例えば，暗号化方式の基本設定として採用されていることの多い WEP は，2000 年代後半には暗号の解読が誰でも容易に行えることが判明している．

4-5-9 セキュリティ技術の評価

多くのベンダーからセキュリティ技術を実装した製品が出荷されるようになり，セキュリティシステムを構築する際には，その製品におけるセキュリティ機能の実装の確かさや，セキュリティ機能の信頼度に対する指針が求められるようになった．

米国では 1985 年に国防総省がコンピュータ製品評価基準（Trusted Computer System Evaluation Criteria：TCSEC）を制定したことを始めとして，欧州では ITSEC（Information Technology Security Evaluation Criteria），カナダでは CTCPEC（Canadian Trusted Computer Product Evaluation Criteria）が相次いで制定された．1996 年には，TCSEC，ITSEC，CTCPEC を国際的に統一するために CC（Common Criteria）評価基準が制定され，その後 CC 第二版をベースに 1999 年に ISO/IEC 15408 が国際規格として制定されている．ISO/IEC 15408 は，セキュリティ機能を備える IT 製品やシステムに対して，そのセキュリティ機能が適切に設計され，その設計が正しく実装されているかを第三者が客観的に評価する制度である．

また，米国では暗号アルゴリズムを実装した暗号モジュールが正しく実装され，鍵やパスワードなどの重要情報を適切に保護しているかを第三者が認証する制度として CMVP（Cryptographic Module Validation Program）を導入し，政府調達時には CMVP 認証製品であることを必須としている．暗号モジュールが満たすべき機能要件として，2001 年に FIPS 140-2 が制定されており，2006 年には FIPS 140-2 をベースに ISO/IEC 19790 が国際規格として制定されている．また，日本においては電子政府推奨暗号リストに掲載されている暗号アルゴリズムを中心とした暗号モジュールの評価認証制度として，2007 年より IPA により暗号モジュール試験及び認証制度（Japan Cryptographic Module Validation Program：JCMVP）が運営されている．

■参考文献

1) “Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher,” NIST Special Publication 800-67, 2008.
2) W. Diffe and M. Hellman, “New Directions in Cryptography,” IEEE Transactions on Information Theory, vol.IT-22, no.6, pp.644-654, 1976.
3) R. L. Rivest, A. Shamir and L. Adleman, “Medhod for Obtaining Digital Signature and Public-key Cryptosystems,” MIT Laboratory for Computer Science, Thechnical Memo LCS/TM82, 1997.
4) “Information technology -Open Systems Interconnection- The Directory: Public-key and attribute certificate frameworks,” ITU-T Recommendation X.509, 2000.
5) “Public-Key Infrastructure (X.509) (pkix), http://www.ietf.org/html.charters/pkix-charter.html
6) “Announcing the ADVANCED ENCRYPTION STANDARD (AES),” Federal Information Processing Standards Publication 197, 2001
7) “IEEE 802.11, The Working Group Setting the Standards for Wireless LANs, ” http://www.ieee802.org/11/
8) “Wi-Fi alliance,” http://wi-fi.org
9) “ IT セキュリティ評価及び認証制度（JISEC）,” IPA, http://www.ipa.go.jp/security/jisec/index.html
10) “暗号モジュール試験及び認証制度（JCVMP）,” IPA http://www.ipa.go.jp/security/jcvmp/