暗号技術に関する特許出願技術動向調査報告

平成１５年５月２２日
特許庁総務部技術調査課

第1章 はじめに

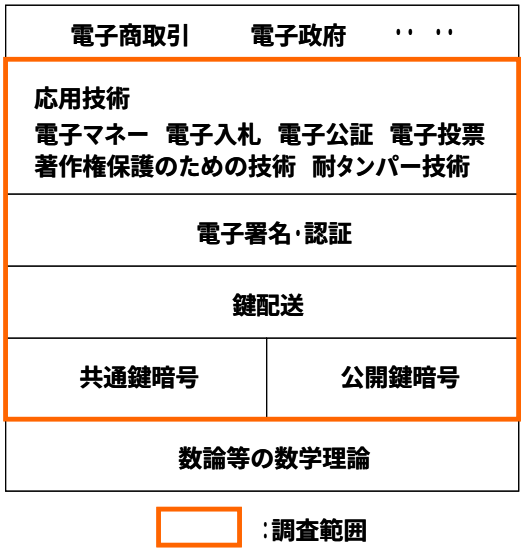
古代より、暗号技術とは、重要な情報を、第三者に知られずに、関係者の間で伝達しあう技術として認識されてきた。実際、暗号技術は軍事・外交などに閉じて用いられてきた。しかし、インターネットで一般企業・大衆が様々な情報を伝達しあうようになり、暗号技術は急速にその用途を広げてきている。例えば、電子商取引、電子政府、デジタルコンテンツ配信等において、暗号技術が欠かせない基盤技術となっている。このような用途の拡大に伴って、米国、欧州、日本など各国政府では、政府自身が利用する暗号アルゴリズムの標準化に取り組んでいる。

本調査では、このような状況を踏まえ、研究開発動向、特許出願・取得状況、市場動向、政策・標準化動向など様々な観点からの調査分析を通じて、現時点における暗号技術の全体像の把握に努め、最後に、暗号技術における今後の日本の目指すべき方向性を検討する。

第1節 本調査の対象

本調査の調査範囲を図 1-1 に示す。暗号技術の理論的基礎である数学理論や、暗号技術が陽に見えない製品・サービスは、本調査の対象としない。主要な調査対象は、基礎的な暗号方式（暗号プリミティブ）、それを直接用いた電子認証サービス（PKI サービス）、さらに暗号技術が要となる著作権保護、電子マネーなどの主要な応用を調査するものとする。

図 1-1 暗号技術と本調査の範囲

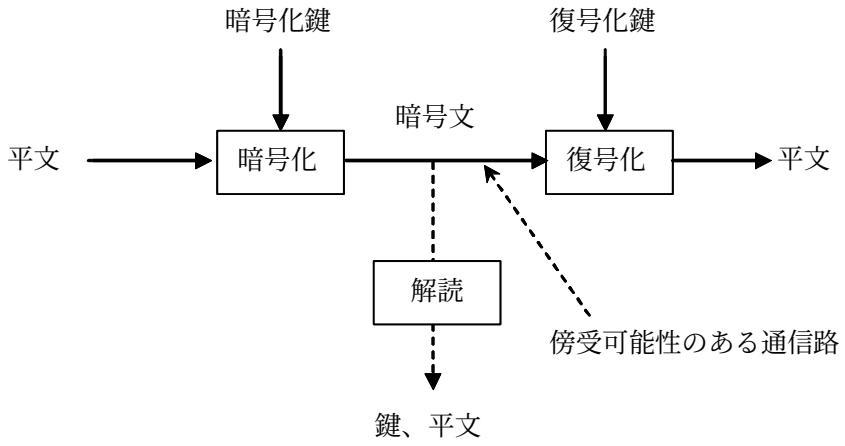


第2節 暗号技術の発展の歴史と現在

暗号技術は、基本的には文書など生のデータ（平文）を、一定の規則によって、判読不能なデータ（暗号文）に変換し、それを元の平文に戻す技術である。暗号文を通信したり、保存したりすることにより、第三者に情報の内容を知られないようにすることができる。暗号は、ローマのカエサルが戦争において用いたという記録があるなど起源は古い。第二次世界大戦では、英米がドイツと日本の暗号を解読したことが、戦いを有利に進めるために極めて重要な役割を果たしたと言われている。

暗号系は図 1-2 のように表わすことができる。暗号化鍵と平文を入力として暗号文を出力する処理を暗号化と言い、復号化鍵と暗号文を入力として平文を出力する処理を復号化と言い、暗号化・復号化の規則を暗号アルゴリズムと言う。暗号化鍵と復号化鍵が同一である暗号を共通鍵暗号と呼ぶ。

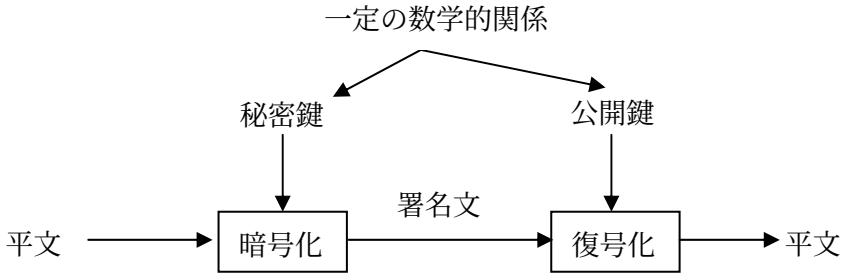
図 1-2 暗号系



コンピュータが発明され、やがて企業や行政の情報システムが構築され、そこで非公開情報が扱われるようになると、コンピュータに使われる非軍事分野の暗号が必要になってきた。米国では、1970 年代に連邦政府機関で用いる暗号の標準化がなされた（連邦情報処理標準 FIPS-46、1977 年）。これが現在まで使われている共通鍵ブロック暗号 DES である。

同時期に、公開鍵暗号という画期的な暗号方式が考案された。公開鍵暗号は、暗号化鍵と復号化鍵の一方を公開し（公開鍵）、他方を秘密にする（秘密鍵）暗号である。公開鍵暗号はデータの秘匿だけでなく、個人に秘密鍵を割り当てることによるデジタル署名（図 1-3）や安全な鍵交換など、新たな用途を開いた。さらに、公開鍵暗号と共通鍵暗号を巧みに組み合わせ、電子公証、電子マネー、電子投票、著作権保護などの多くが安全に電子的手段で実現できることが示され、実用化されている。

図 1-3 デジタル署名

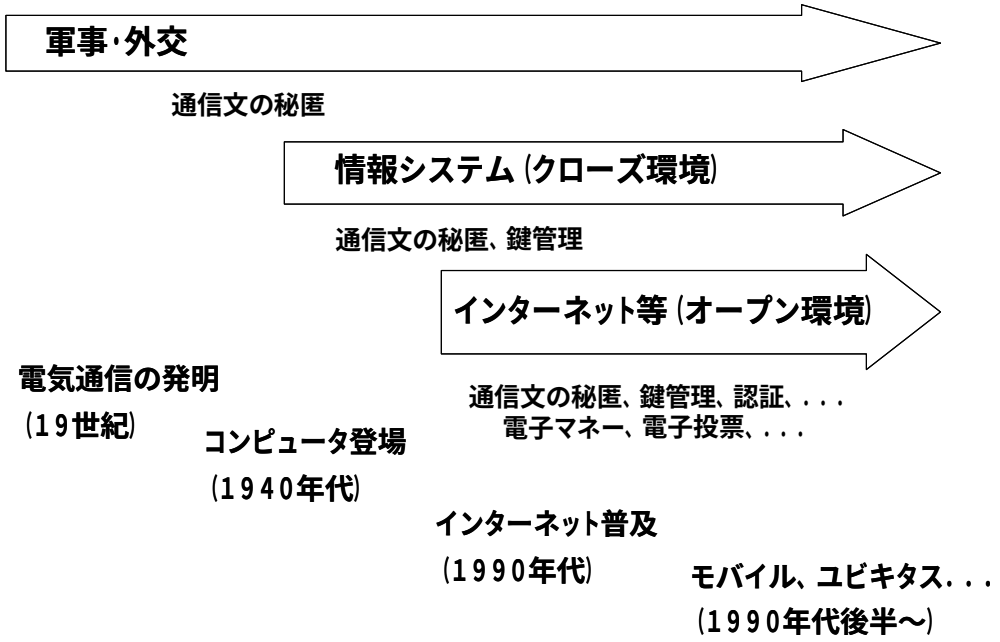


当人しか知り得ない秘密鍵で署名をしたものは、秘密鍵とともに生成される公開鍵を第三者が取得して復号化することにより、当人の署名であることが保証される。

1990 年代のインターネットの一般への普及によって多種多様な情報がネットワークでやり取りされるようになったが、オープンなインターネット上で秘密にしたい情報を伝達するために暗号技術の利用が飛躍的に拡大した。

暗号アルゴリズムは慎重に設計しても、解読方法が発見されることがあり、専門家による精密な検証が必要である。暗号技術の用途拡大に伴い、一般に利用される暗号に関しては、暗号アルゴリズムを公開し、開かれた暗号研究者のコミュニティで安全性を検証することが定着している。また、そのようにして安全性の検証された暗号技術を標準化し、普及させて行こうとする取り組みの一般化が近年の特徴である。

図 1-4 暗号技術の用途の拡大



第2章 暗号技術の研究開発動向

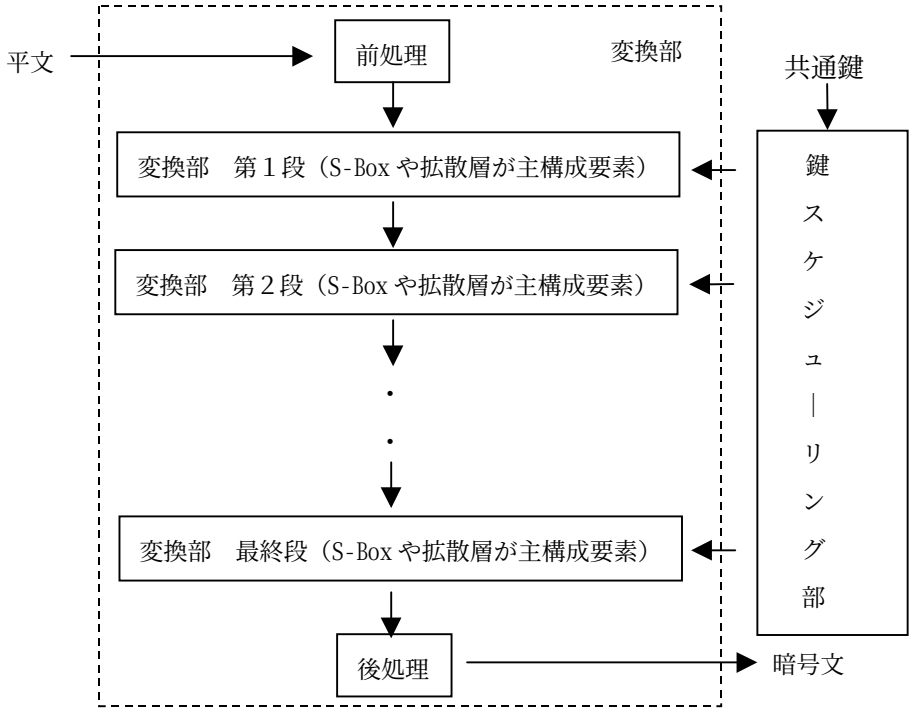
第1節 主要技術の変遷

1. 共通鍵暗号

共通鍵暗号には、平文を一定サイズ（64 ビット、128 ビットなど）のブロックに区切り、ブロック単位で暗号化する共通鍵ブロック暗号（以下、「ブロック暗号」という）と、平文をビット列として暗号化する共通鍵ストリーム暗号（以下、「ストリーム暗号」という）とがある。

1970 年代、米国連邦政府機関内で使用できる強力な政府標準暗号制定の必要性が生じ、IBM から提案された Lucifer という名前の暗号アルゴリズムに手を加えた後に、米国政府標準暗号として制定されたのが DES である。米国の暗号政策に従って、政府内のみならず広く金融界等でも使用されることを意図されていた DES はそのアルゴリズムが公開された。Lucifer 暗号の骨格である Feistel 構造は、その後のブロック暗号アルゴリズムのベースとなった(図 2-1 にブロック暗号の基本構成を示す)。

図 2-1 共通鍵ブロック暗号の基本的な構成



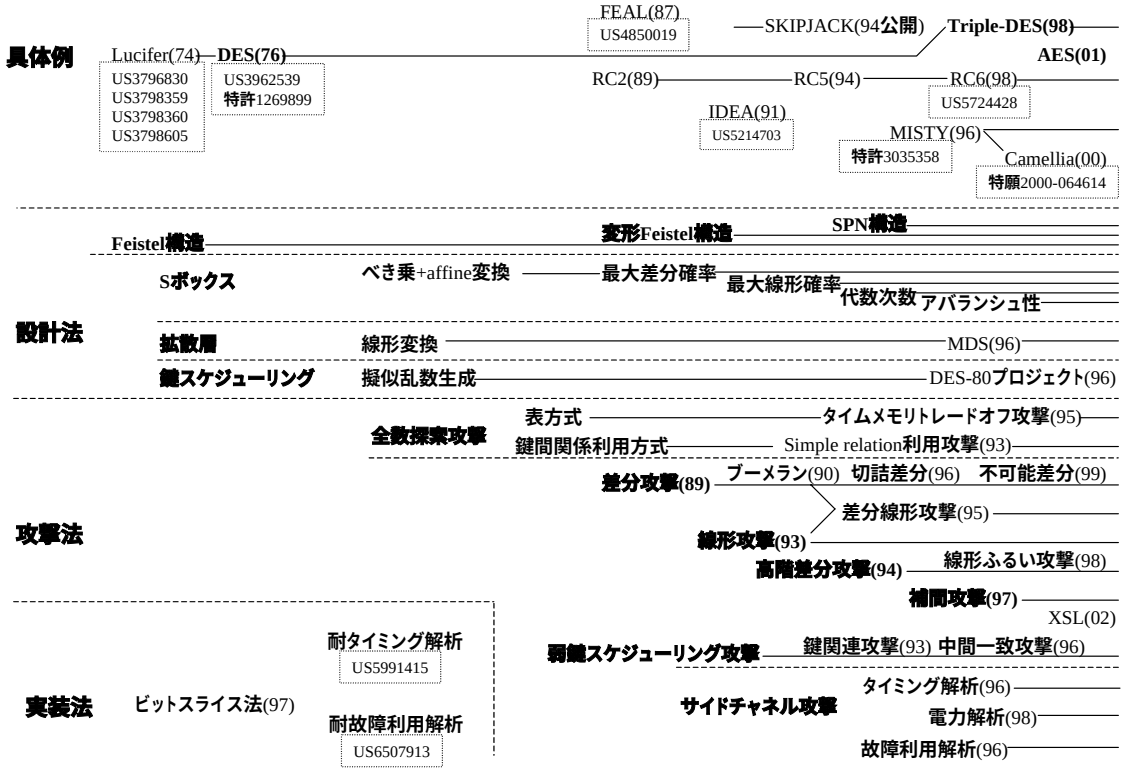
鍵スケジューリング部は共通鍵を入力として変換部各段への鍵を生成。変換部各段は基本的に同じ変換部構造を持ち、主に S-box や拡散層と呼ばれるデータ変換から構成される。各ブロック暗号はこの変換部構造や次段への処理データの渡し方により種類が分かれる。復号は上の暗号化の処理を逆方向に行う。

これら以外にも主な民間企業でブロック暗号の研究が進められている（図 2-2）。日本では、電信電話公社（現在 NTT）の FEAL（1987 年）や、三菱電機の MISTY 暗号（1996 年）がある。今後最も普及すると見込まれているのは、DES の改良版である Triple-DES、および、最近、次期米国政府標準暗号として制定された AES である。

1989 年にブロック暗号に対する攻撃法として差分攻撃法が提案された。この攻撃法は当時最も広く使用されていた DES の安全性を揺るがす事態を起こし、暗号研究全体に多大な影響を与えた。ブロック暗号に対する攻撃法の研究、ひいてはブロック暗号の研究全体はこの差分攻撃法を契機として一気に活発になったと言ってよい。さらに、1993 年に線形攻撃法が考案された（三菱電機・松井氏）。差分攻撃法と線形攻撃法は最も重要な攻撃法であり、ブロック暗号には最低限これら攻撃法に対する耐性を持つことが要求される。差分攻撃法と線形攻撃法からは、ブロック暗号のアルゴリズムの弱点を突く様々な攻撃法が派生し、またそれらに耐性を持つような新たなブロック暗号アルゴリズムの設計が進んだが、現在では、このような動きは 1990 年代に比べ下火となっている。

その一方で、現在、問題になっているのは、ブロック暗号の実装に関する弱点である。すなわち、ブロック暗号の実装が暗号化または復号化時に出す電力変化等を観測して鍵等を特定するというサイドチャネル攻撃法と呼ばれる攻撃法が 1990 年代後半から重要視され、それに対する実装の安全性の研究が大きな課題となっている。

図 2-2 共通鍵ブロック暗号の技術変遷図

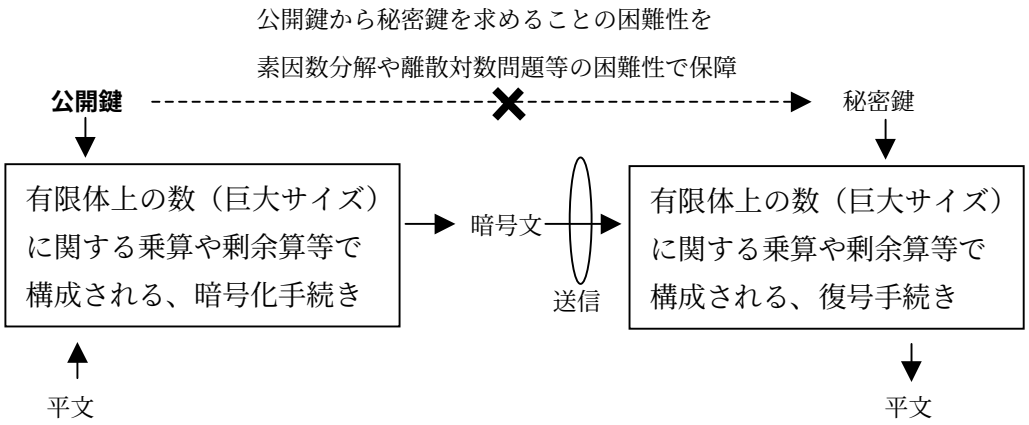


ストリーム暗号としては、バーナム暗号（使い捨て鍵暗号）が古くから使われていた。現在では、ブロック鍵暗号の S-box 等を流用する方式がストリーム暗号として広く使われている。ストリーム暗号の一種としてカオス暗号の提案が近年目立つが、その安全性や効率は十分には確認されていない。

2．公開鍵暗号

公開鍵暗号は、解読する（公開鍵から秘密鍵を求める）ためには非現実的な膨大な計算を要するという数学的な問題（計算量的に困難な問題）に基づいている（図 2-3）。公開鍵暗号は Diffie-Hellman によってその概念が示された。その後、公開鍵暗号は、大きく分けて素因数分解の難しさに基づくもの、離散対数問題の難しさに基づくもの、組み合わせ問題の難しさに基づくもの、この３種に分かれて研究が進んでいった。

図 2-3 公開鍵暗号の仕組み



現在、公開鍵暗号としてデファクトスタンダードになっている RSA 暗号は、素因数分解の難しさに基づく暗号であり、1978 年に発表されて以来、これまでに決定的な攻撃法は発見されていない。不適切な秘密鍵の研究など、その安全性に関して多くの研究が進み、1993 年に RSA の標準である RSA-PKCS#1 という形にまとめられた。また、計算機能力の向上を考慮して、1996 年には鍵長が 1024 ビットに改定された。RSA 暗号からは、多くの暗号が派生している。

離散対数問題の難しさに基づく公開鍵暗号としては ElGamal 暗号が代表的であり、楕円曲線を利用する公開鍵暗号としては楕円 ElGamal 暗号が代表的である。

組み合わせ問題の難しさに基づく公開鍵暗号は 1980 年代前半まで活発に研究された。この時期の代表的な暗号としてナップサック問題に基づく Merkle-Hellman の暗号があるが、Shamir によって効果的な攻撃法が提示された。これまでに提案された、組み合わせ問題の難しさに基づく公開鍵暗号の多くに対して効果的な攻撃法が見つかっている。

1996 年に Shor が、量子計算機[1]によって素因数分解問題を効率的に解く方法を示した。量子計算の実用化は未だ見えないとはいえ、RSA が依拠する素因数分解の難しさに問題が生じたことになる。これを受け、Ajtai-Dwork 暗号を代表とする、格子暗号と呼ばれる、量子計算機による解読に耐性のあるとされる暗号が注目されている。

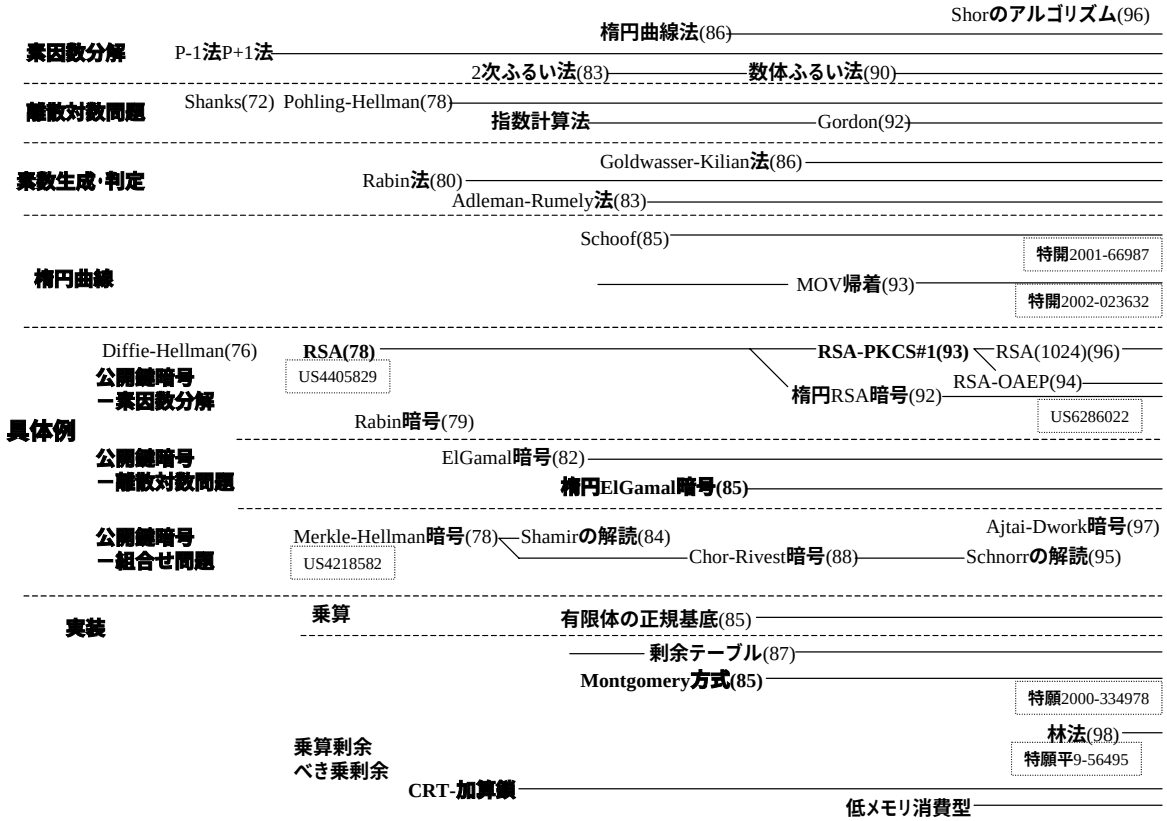
このような量子計算によって安全性が揺らぐ、あるいは計算機パワーの増大に合わせて鍵長の変更が必要になるという事態は、今までの公開鍵暗号が計算量的困難さに依存したもの

[1] **量子計算機とは、状態の重なり合いを無限に許す量子力学の原理を高度に利用して、膨大な数の選択肢を同時に計算することのできる計算機。基本的な動作原理が実証されているが、実用化までに 10 年ないし 20 年程度を要すると予想されている。**

であったからだという認識に立って、安全性を情報量の観点から数学的に証明できるようなアルゴリズムを希求する動きが出てきている。また、公開鍵暗号においてもブロック暗号と同様に実装の安全性も課題になっている。

以上の変遷を図 2-4 にまとめる。

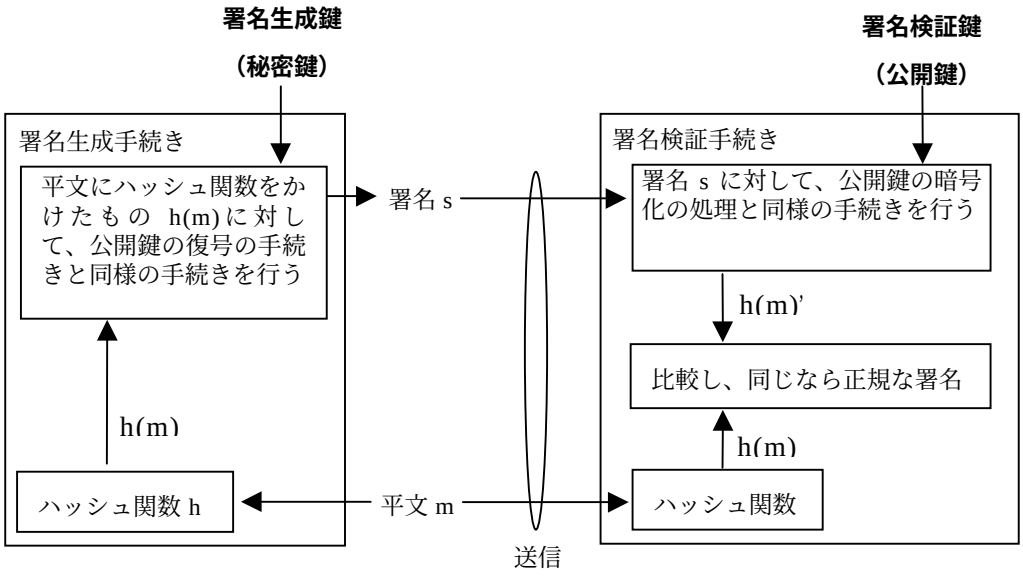
図 2-4 主要技術変遷図：公開鍵暗号



3. 鍵配送・電子署名・電子認証

電子署名には様々な方法があるが、代表的なものは公開鍵暗号に基づいたデジタル署名である（図 2-5)。デジタル署名としては、平文から署名を生成鍵（秘密鍵）で生成して検証鍵（公開鍵）で検証するという単純なデジタル署名と、そのような単純なデジタル署名に加え種々の要求仕様を満たすためのデジタル署名がある。公開鍵暗号のアルゴリズムを変形させたものとしては、RSA 署名がある。1993 年には PKCS#7 として標準化され、現在のデジタル署名のデファクトスタンダードになっている。ElGamal 暗号に対応して ElGamal 署名が提案され、後に米国政府標準である DSA へと発展した。後者のデジタル署名としては、否認不可署名、ブラインド署名、故障停止署名など、種々の要求を満足するための多様なデジタル署名が開発されつつある。

図 2-5 デジタル署名の基本的な仕組み



暗号技術を用いた認証としては、公開鍵暗号を用いて３回以上の交信を行うプロトコルという形態を取る方式が一般的であり（3 交信プロトコルと呼ばれる)、Fiat-Shamir による方式が代表的である。また、信頼できる第三者である TTP (Third Trusted Party)を用いる認証方式もよく使われ、代表例として Schnorr 認証がある。

鍵配送（鍵配布または鍵共有と呼ばれることもある）は、１対１で鍵を交換するための方法と、第三者(TTP)が介在する方法に大きく分かれる。１対１で鍵を交換するする画期的な方法は Diffie-Hellman によって提示された。以降、この形態での鍵交換は Diffie-Hellman を基本としている。TTP が鍵の作成・配布に介在する方式としては、Kerberos が代表的である。

鍵配送・電子署名・電子認証においてもブロック暗号と同様に実装の安全性が課題になっている。アルゴリズムの点からは、鍵配送・電子署名・電子認証の特徴として、ブロック暗号や公開鍵暗号に比べて、方式が要求仕様に従って細分化され、多様なプロトコルとして存在するため、個々の方式の安全性をどう評価し保証するかという課題がある。

4. 応用技術

今まで挙げた、共通鍵暗号、公開鍵暗号、署名・認証・鍵配送といったプリミティブな暗号技術は様々に応用されて実用システムに組み込まれている。これら暗号技術の応用が最も進んでいる技術としては、電子投票、電子公証、電子入札といった電子政府の一部を成す技術や、電子マネーがある。また、著作権保護のための応用も進んでいる。しかし、これら応用技術については、それぞれの方式が、様々な使用場面や要求仕様に従って様々に設計されており、従って、応用技術の全体は、暗号プリミティブを組み込んだ、多様なプロトコルの集団を成す。よって、明確な変遷というものは示しにくい。また、この多様化したプロトコルの個々の安全性をどう評価するかという課題が存在するのは、鍵配送・電子署名・電子認証と同様である。

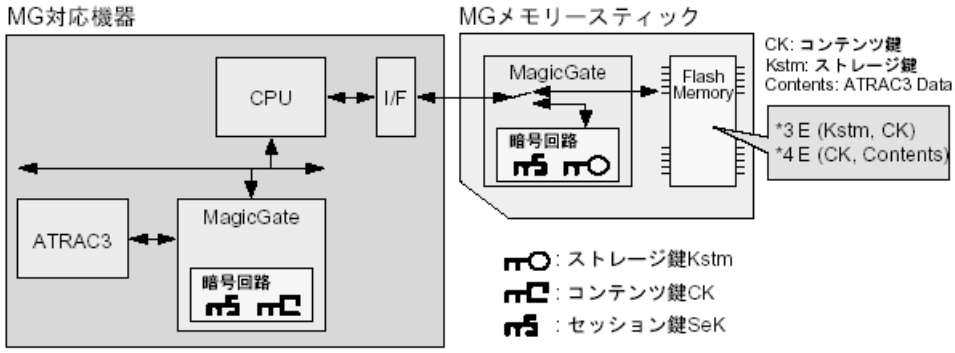
応用技術の一例として、著作権保護において、どのような要求仕様があり、それらを満たすために暗号技術がどのように使われているかという対応関係の基本的構図を示す。

表 2-1 著作権管理における、要求仕様を実現する暗号技術

要求仕様	暗号技術
コンテンツへの著作権･利用者情報の埋め込み	インフォメーションハイディング
コンテンツ自体の暗号化	ブロック暗号（ストリーム暗号）
認証（機器・エンティティ）	デジタル署名、公開鍵暗号、ハッシュ関数
配信経路・メディアの暗号化・スクランブル	ブロック暗号、ストリーム暗号、スクランブル
課金	電子マネー
鍵や利用情報の暗号化	ブロック暗号

具体的な著作権管理システムの一例に、ソニーによる MagicGate™ がある。 MagicGate™ は、メモリースティックウォークマンなどの MagicGate™ 対応機器 (MG 対応機器) と MagicGate™ メモリースティック (MG メモリースティック) の間での音楽データ等著作権保護に用いられる。MagicGate™ では、コンテンツの暗号化、機器認証、鍵交換（鍵や利用情報の暗号化）、などに暗号技術が適用されている。

図 2-6 MagicGate™ の概要



（出典）ソニー、商品情報、[online]2003.1.7 **検索、**
http://www.sony.co.jp/Products/SC-HP/CXPAL/CXPAL-44/PDF/tw.pdf

第2節 暗号技術の主要研究課題

前節において、主要技術の変遷を述べる中で、各技術において現在課題となっていることを述べた。これを改めて纏める。暗号技術において今後重要になる課題としては実装の安全性に関する研究開発とアルゴリズムの安全性の確立に関する研究開発に２分される。

1．実装に関する研究開発

- 高速化・小型化技術の研究開発

  高速化、ICカード、携帯機器等向けの小型実装・省電力化など。

- サイドチャネル攻撃法等のデータ取得手段に対抗し得る耐タンパー性評価･耐タンパー化技術の研究開発

  タイミング解析、電力消費解析、故障利用解析等サイドチャネル解析による攻撃法が著しく発展しており、それら攻撃法に耐えうる実装技術の開発が求められている。ハードウェア実装やソフトウェア実装の脆弱性を用いてデータを取得する攻撃法などに対する耐タンパー性が実装の安全性を図る上で重要である。

2．アルゴリズムの安全性に関する研究開発

- 計算量的困難さに依存しない暗号アルゴリズムの研究開発

  現在広く利用されている暗号・認証方式は、計算量的困難さに依拠したものであるが、計算機の能力向上により安全性が損なわれる危険性がある。情報量的安全性に基づく暗号技術が提案されている。

- 多様なプロトコルの安全性評価手法の研究開発

  暗号技術の応用が進むにつれ、個別の応用に特化した、より多様で複雑なプロトコルの研究開発が多くなっていくと予想される。多様なプロトコルの安全性を評価するより統一的な方法論が今後重要になる。

第3節 主要学会での発表動向に見る日本の技術競争力

研究活動の量を測定することは難しいが、暗号技術における学会として最も重要なCRYPTOでの発表者の国別内訳を調べたのが図2-7および図2-8である。

図2-7 CRYPTOにおける国別の著者数（1984年～2002年）

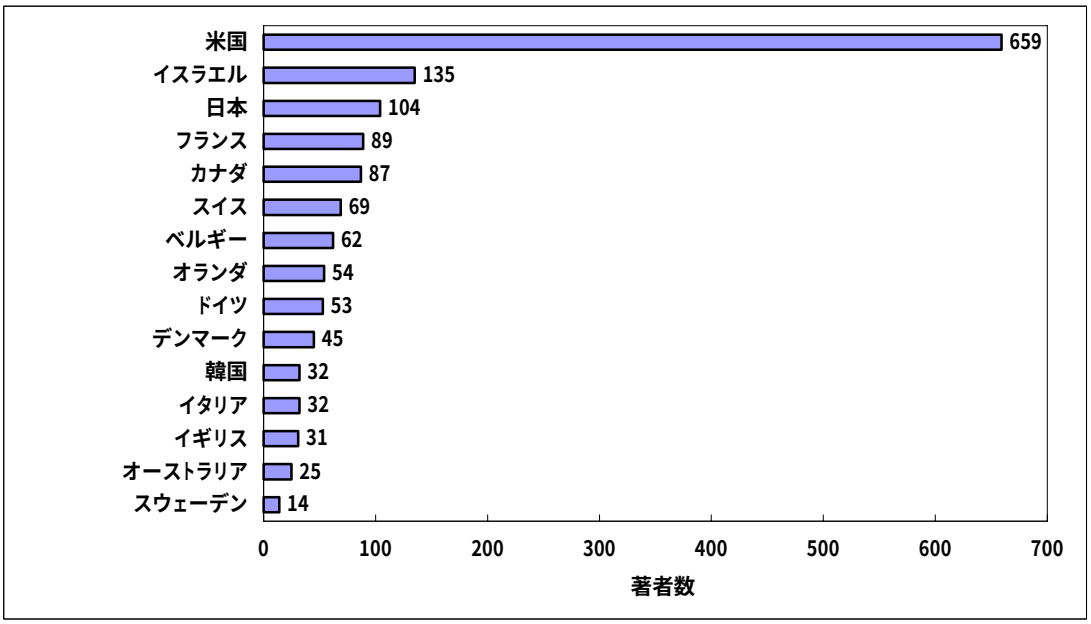
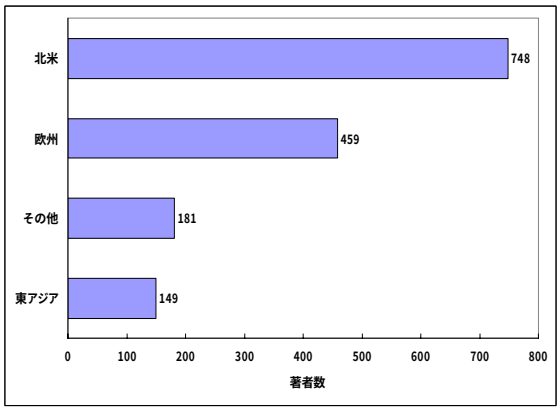
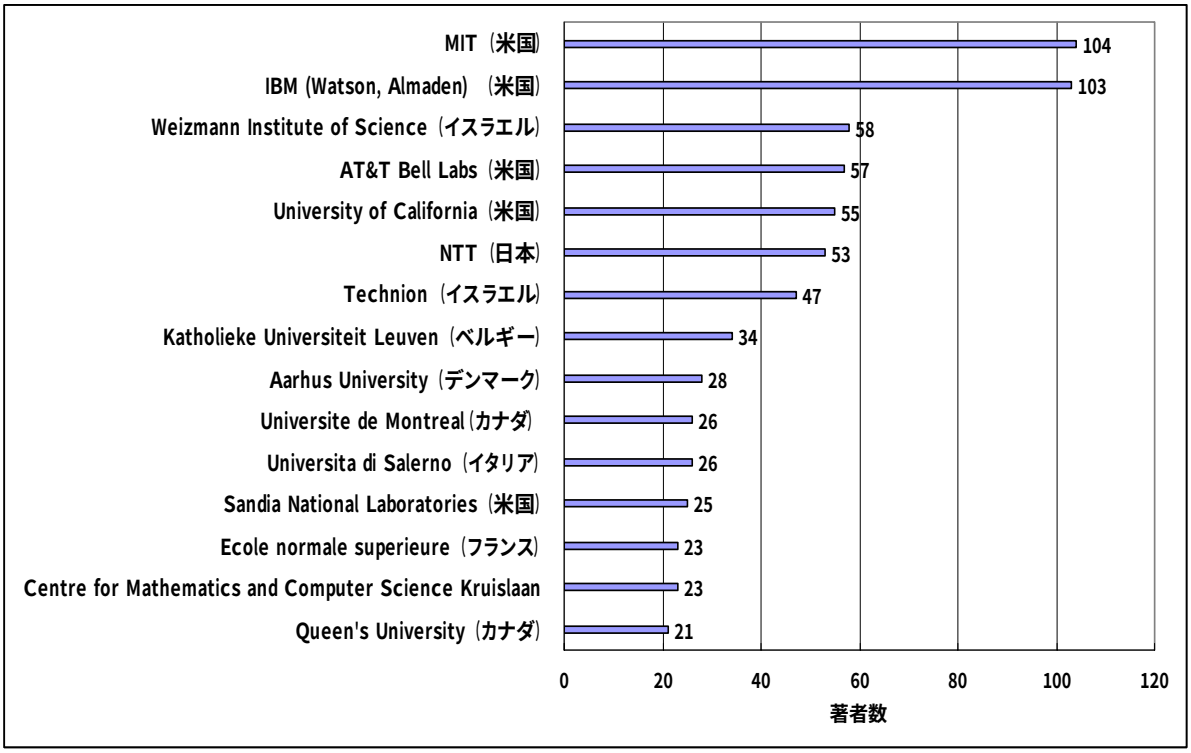


図2-8 CRYPTOにおける地域別著者数（1984年～2002年）



米国の著者数が圧倒的に多いが、CRYPTOの開催地であることの反映でもある。伝統的に暗号技術研究に強いイスラエルの著者が多いことも特徴的である。日本は欧州の国を押さえて３位となっている。ただし、地域別に見ると、日本を含む東アジアは北米、欧州のそれぞれ５分の１、３分の１となる。図2-9に著者数の多い機関のランキングを示した。大学が多く、少数の民間企業と国立研究機関が上位にランクされている。IBM、ベル研究所、NTTなどを除けば、特許出願上位企業（第3章第2節）の多くは、CRYPTOでの論文発表をそれほど盛んに行っていないことが分かる。

図 2-9 CRYPTO における著者数の多い機関（1984 年～2002 年）



なお、従来は、CRYPTO が暗号の学会を代表しているとほぼ言えたが、近年、FSE（Fast Software Encryption）など、より専門的な学会が生まれている。したがって、上記はあくまで CRYPTO における状況として理解すべきことに注意して頂きたい。

第3章 暗号技術の特許出願動向

第1節 特許出願件数および登録件数

特許を技術内容に応じて分類するためのコード体系がいくつか存在する。IPC（International Patent Classification）は世界でもっとも広く用いられている技術コード体系であり、その名のとおり世界で定義が共通しているのが特徴である。IPC をさらに詳細に展開したものとして日本国特許庁は FI 記号を独自に定めている。同様に米国特許庁では、US Class を、欧州特許庁では EC Class をそれぞれ独自に定義し特許文献に付与している。

三極間の比較などの特許機関をこえた分析を行なう場合、特許集合の決定に際しては、可能な限り定義が共通している IPC を用いるのが望ましい。ただし、一般に各特許機関が独自に設定した特許分類コードが IPC よりもきめ細かくかつ適切であるため、本調査では可能な限り IPC（第 7 版）を利用することとするが、IPC だけでは集合を特定できない場合は、各特許機関が定義する分類コードを利用することとした。

1．暗号技術全体の特許出願状況

1980 年以降の、日本国特許庁、米国特許商標庁、欧州特許庁への暗号技術全体の出願人国籍別出願件数の推移を図 3-1～図 3-3 に示す。[2]同様に、登録特許を出願年毎に集計したものを図 3-4～図 3-6 に示す。日米欧とも出願件数が 1980 年代を通して漸増しているが、米国で 1992 年頃から、日本で 1995 年頃から特に増加が見られる。日本と欧州では 1990 年代半ば以降の出願件数の増加に対応する登録件数の増加が見られないが、同時期の特許出願の多くが審査請求前ないし審査中であるためと考えられる。米国においても、1998 年以降の出願の多くは審査中のため登録件数が少なくなっている[3]。

日本への出願の大半は日本国内からである。一方、米国では３分の１程度は国外からの出願であり、欧州では半数以上が域外からの出願である。

---

[2] **米国は 2000 年 11 月まで公開制度がなかったため、登録された特許を出願年毎にまとめた。すなわち、X 年の件数が Y 件というのは、X 年における特許出願で登録されたものが Y 件ということである。図 3-2 と図 3-5 は同じグラフである。**

また、出願人国籍が EPC 加盟国であるものを欧州からの出願とした。

[3] **日本では特許出願後３年以内（2001 年 9 月 30 日以前の出願は７年以内）に審査請求することにより、審査が行われる。米国では全ての特許出願が審査される。**

図 3-1 出願人国籍別出願件数（出願先：日本国特許庁）

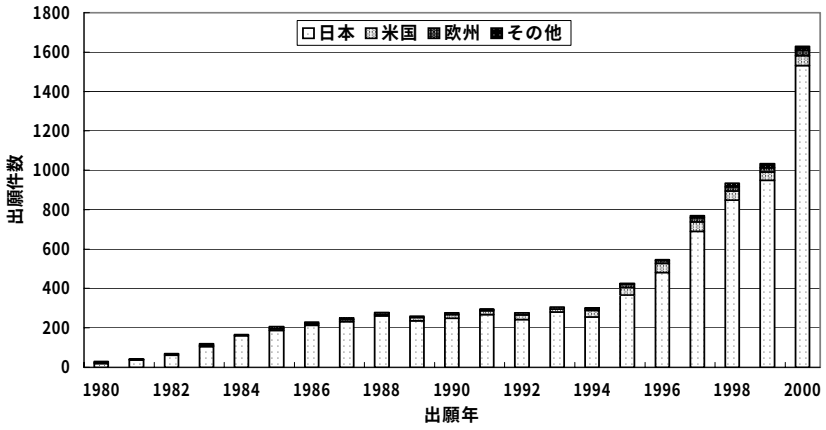


図 3-2 出願人国籍別出願件数（出願先：米国特許商標庁）

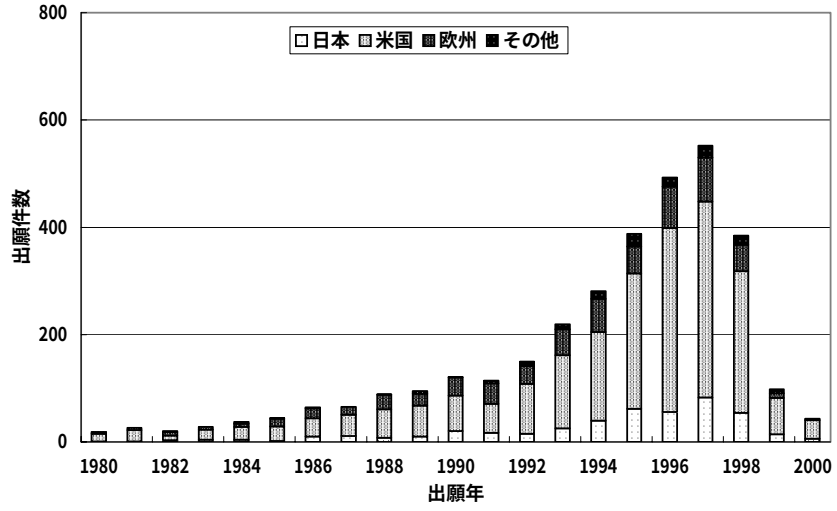


図 3-3 出願人国籍別出願件数（出願先：欧州特許庁）

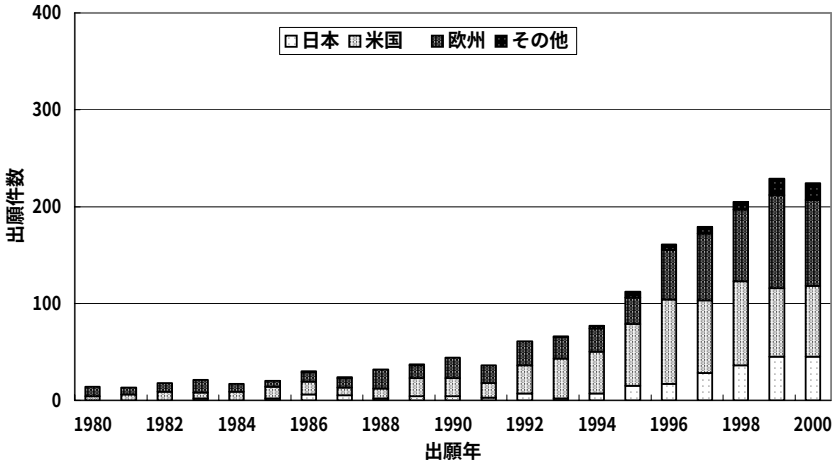


図 3-4 出願人国籍別出願件数（登録特許、出願先：日本国特許庁）

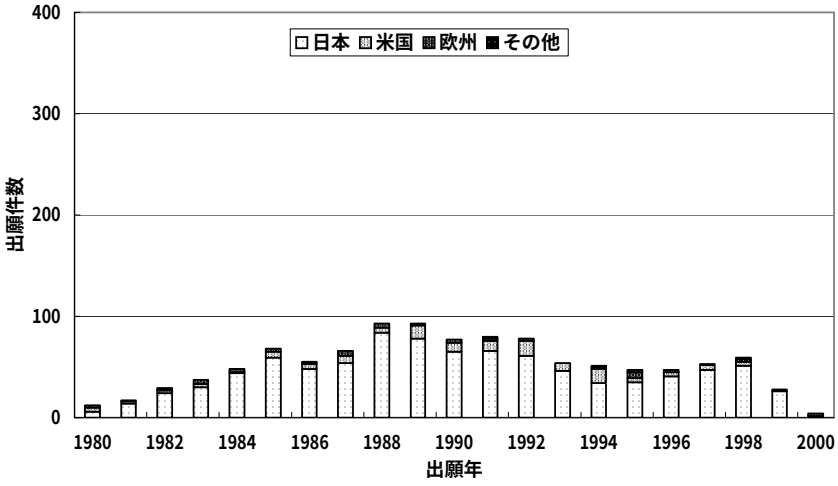


図 3-5 出願人国籍別出願件数（登録特許、出願先：米国特許商標庁）

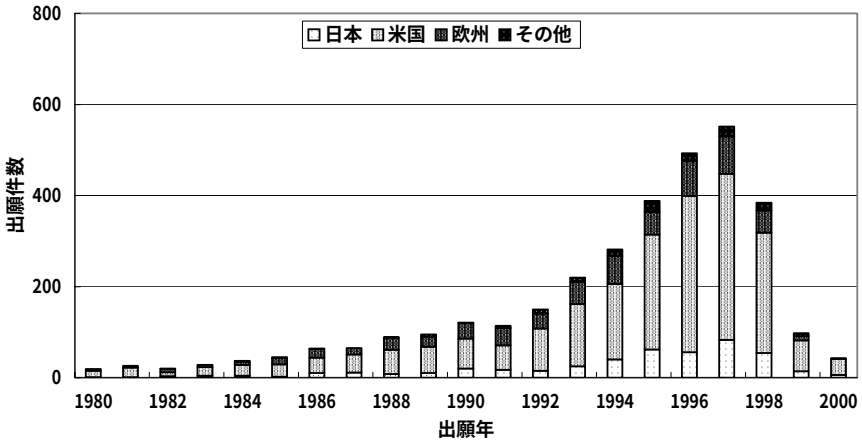
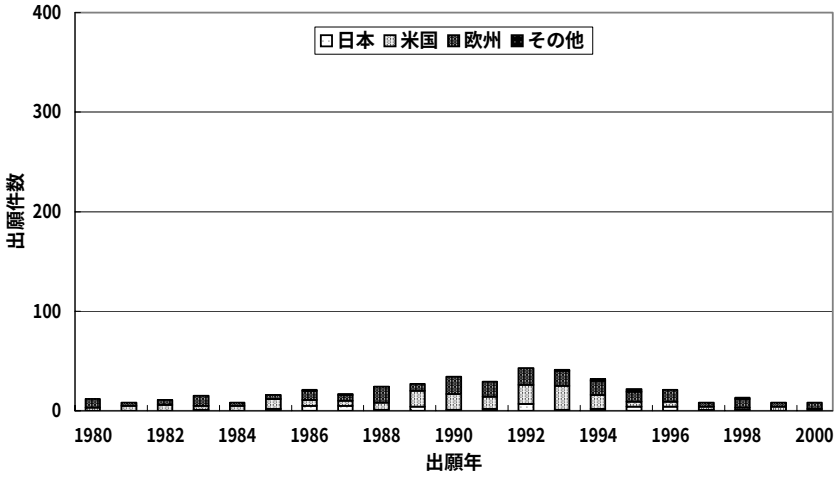


図 3-6 出願人国籍別出願件数（登録特許、出願先：欧州特許庁）

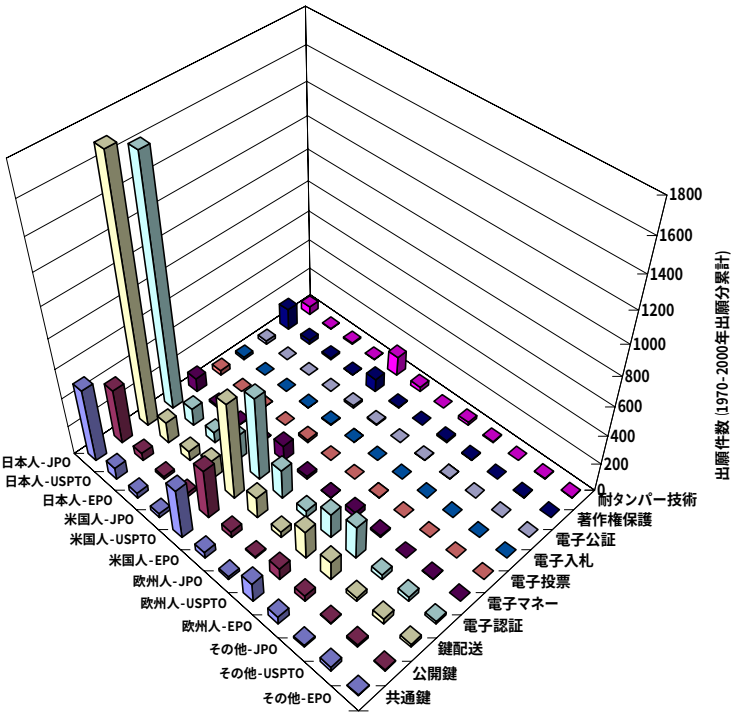


2．技術区分毎の特許出願状況

日本国特許庁、米国特許商標庁、欧州特許庁への出願人国籍別技術区分毎の累積特許出願件数（1970～2000 年出願分）を図に示す。図中の「日本人－JP0」は出願人が日本人、出願先が日本国特許庁(JP0)であることを示す。他も同様であり、USPT0 は米国特許商標庁、EP0 は欧州特許庁を表している。

三極に共通した特徴として鍵配送、電子認証の特許出願件数が他に比較して大きいことをあげることができる。

図 3-7 技術区分別三極出願件数（1970～2000 年出願分累計）



次に三極の各特許庁への技術区分別の出願数の推移を図 3-8～図 3-10 に示す。三極に共通して、鍵配送および電子署名・電子認証の出願が 1995 年ころから急激に増加している。鍵配送および電子認証の件数の大きさついては、数学の理論的要素が大きい暗号プリミティブに比べ、処理手順、システム構成等、多様な考案が可能であり、また製品、サービスにより結びつきやすいためであると考えることができる。また 1995 年頃からの急速な出願の増加はインターネットの普及により、安全性確保の重要性が高まり、これらの技術の将来性が広く認識されはじめたことを示している。

米国、欧州と比較すると日本国特許庁への出願では、特に鍵配送および電子認証・電子署名の出願が他の技術分野に比較して大きな比率を占めている。逆に米国では暗号プリミティブの比率が日本に比較して大きい。

図 3-8 技術区分別出願数 (出願先：日本国特許庁)

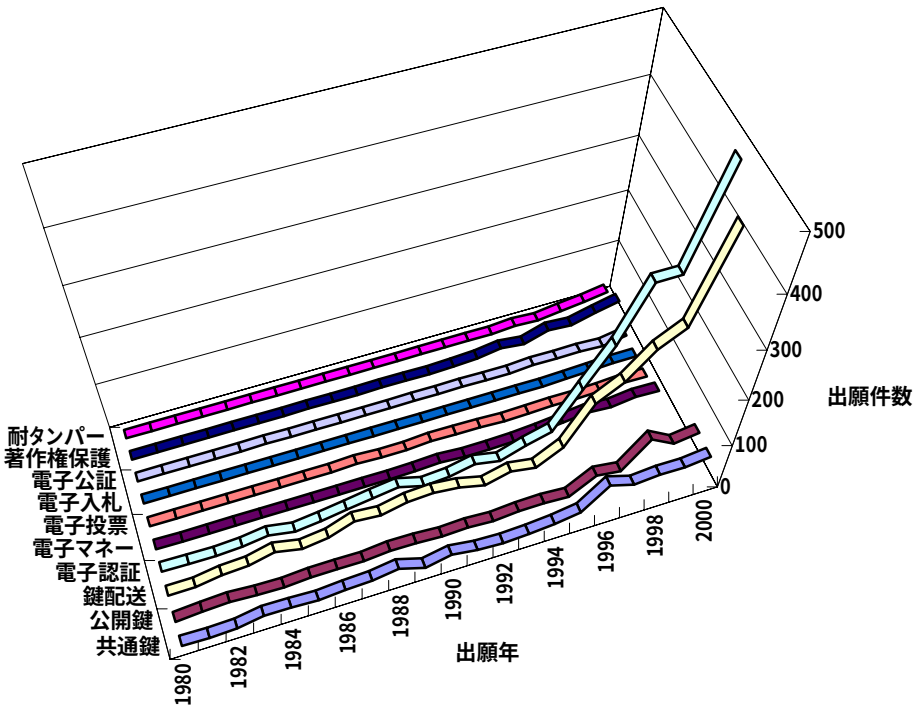


図 3-9 技術区分別出願数 (出願先：米国特許商標庁)

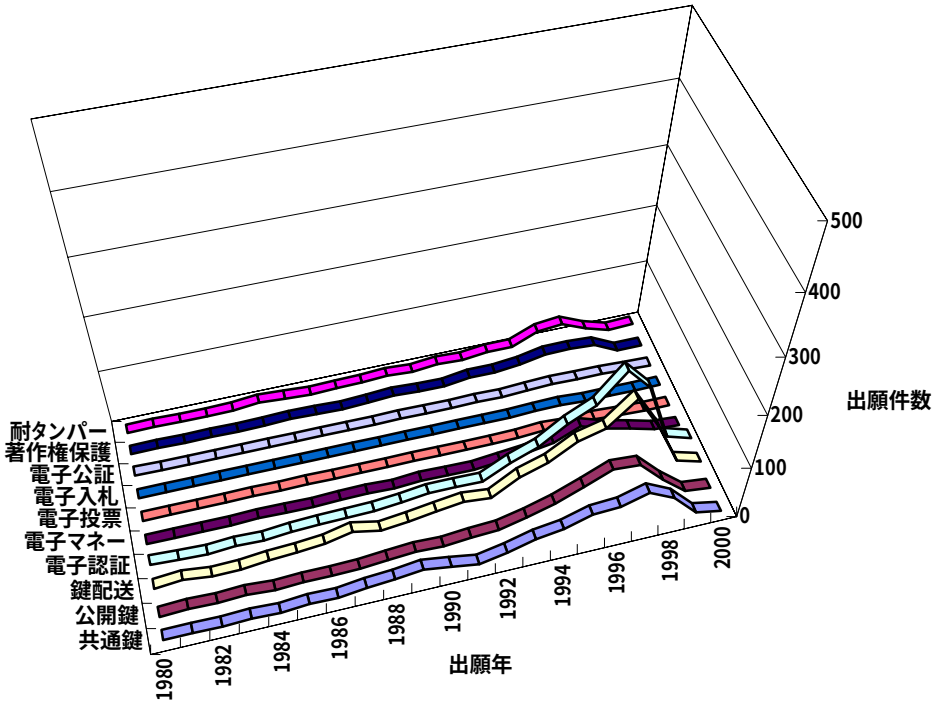
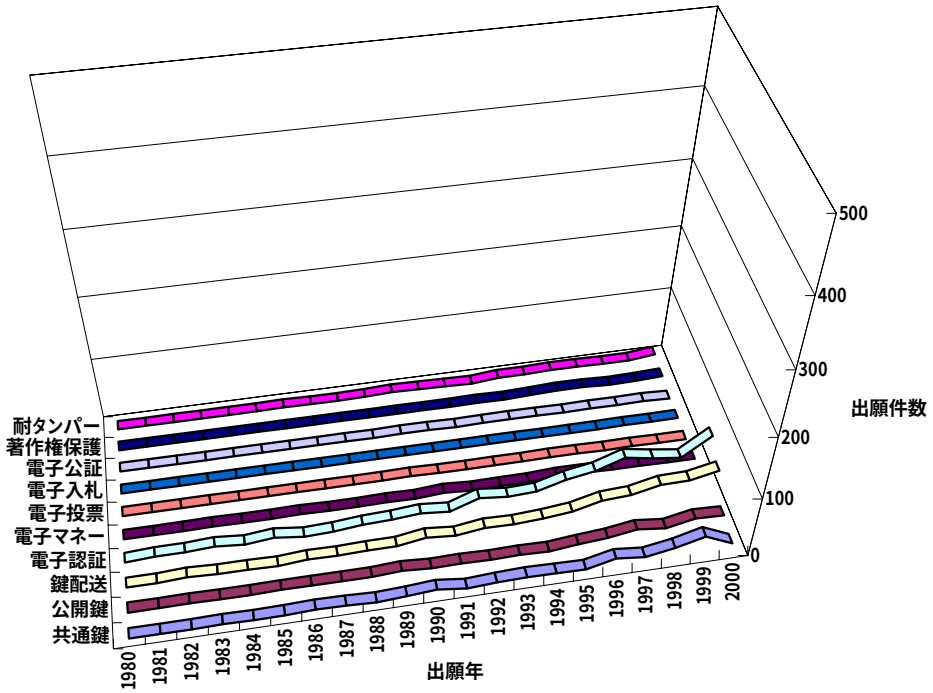


図 3-10 技術区分別出願数 (出願先：欧州特許庁)



共通鍵暗号に関する特許出願件数を図 3-11～図 3-13 に、公開鍵暗号に関する特許出願件数を図 3-14～図 3-16 に示す。

共通鍵暗号は 1970 年代から実用に供されており、特許が出願されている。DES が FIPS 標準となった 1977 年以降は僅かな増加傾向が続いたが、1990 年代初めに出願件数が減少した。これは 1989 年に差分攻撃法が発表され、攻撃法への対策が模索されたことが一つの要因であると推測される。その後も線形攻撃法(1993 年)など様々な攻撃法が研究され、MISTY（1996 年）など、それら攻撃法を前提として設計された共通鍵暗号が開発されている。公開鍵暗号は 1970 年代後半に提唱されたが、計算処理が重かったため、実用化が本格化したのは 1990 年代に入ってからである。これは出願件数推移にも現れている。

図 3-11 出願人国籍別出願数 (技術区分：共通鍵暗号、出願先：日本国特許庁)

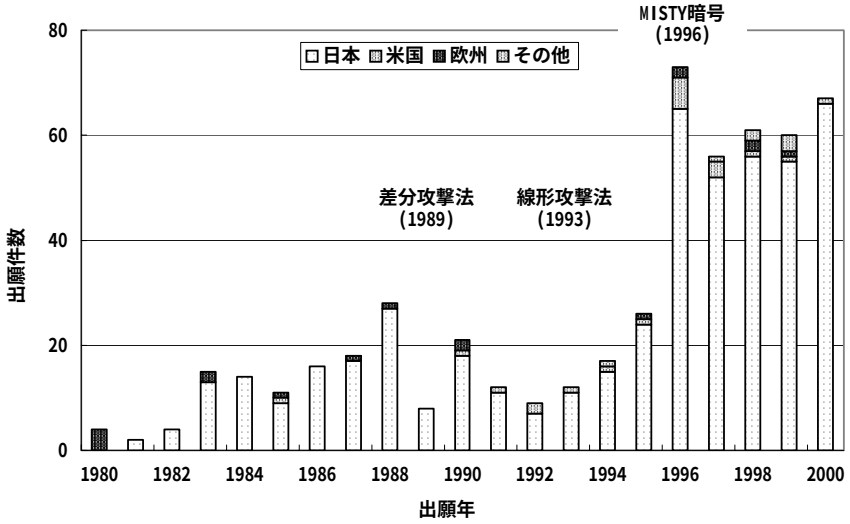


図 3-12 出願人国籍別出願数 (技術区分：共通鍵暗号、出願先：米国特許商標庁)

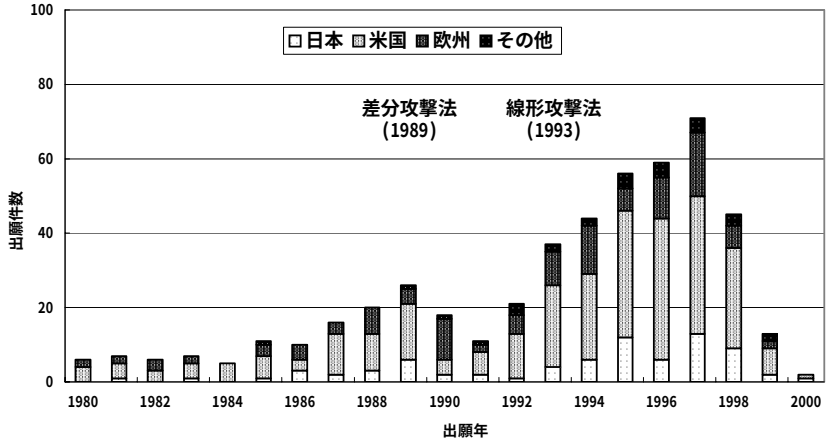


図 3-13 出願人国籍別出願数 (技術区分：共通鍵暗号、出願先：欧州特許庁)

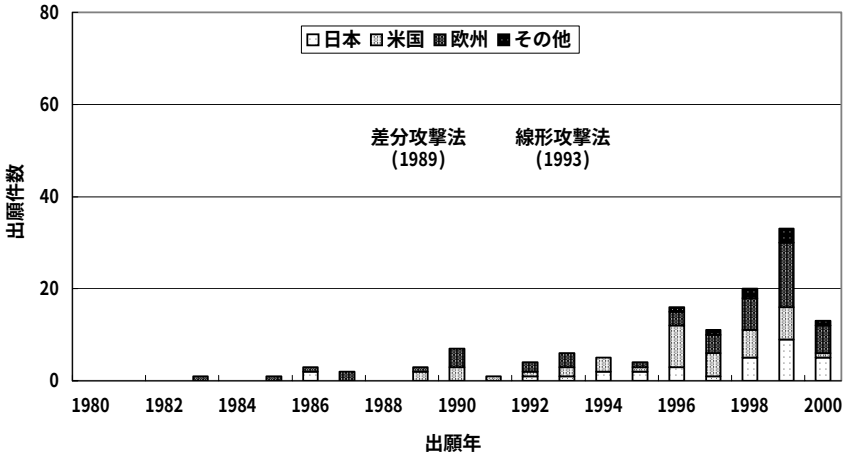


図 3-14 出願人国籍別出願数 (技術区分：公開鍵暗号、出願先：日本国特許庁)

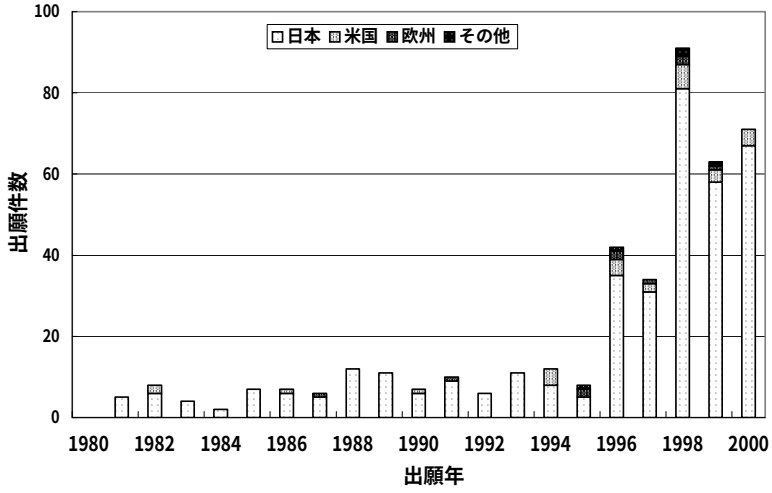


図 3-15 出願人国籍別出願数 (技術区分：公開鍵暗号、出願先：米国特許商標庁)

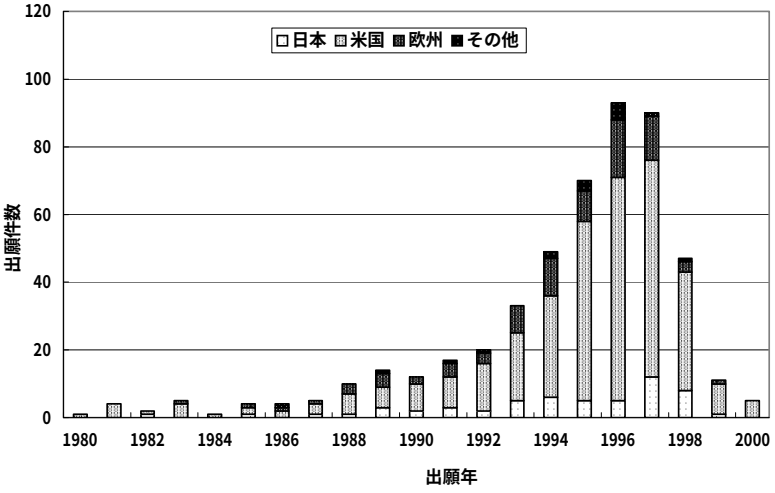
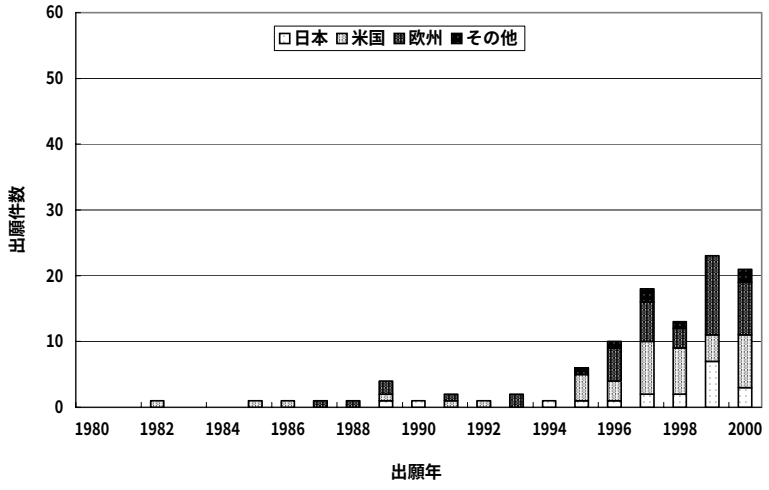


図 3-16 出願人国籍別出願数 (技術区分：公開鍵暗号、出願先：欧州特許庁)

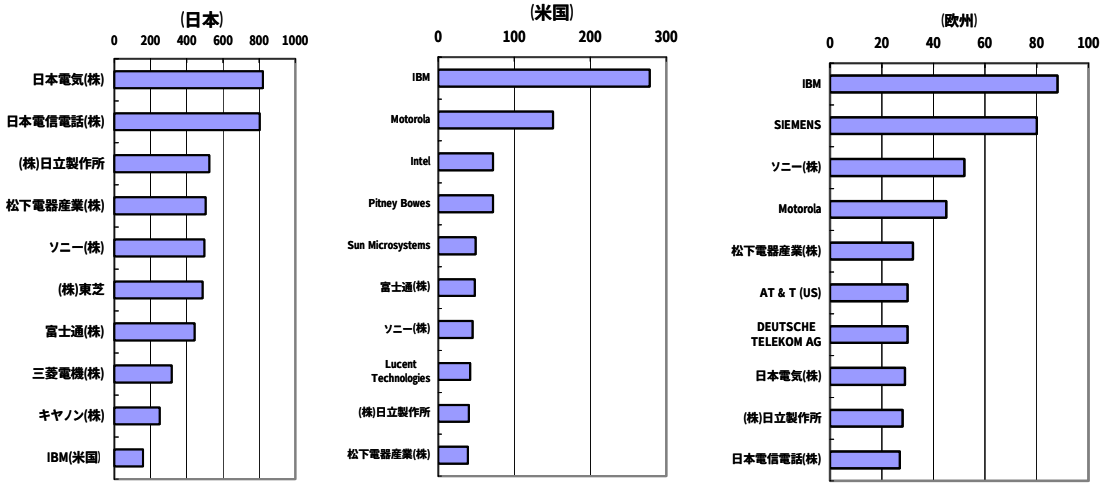


第2節 上位特許出願人

1. 全般的動向

日本国特許庁、米国特許商標庁、欧州特許庁への上位出願人 10 社を図 3-17 に示す。日本国特許庁への出願では、NTT および大手計算機メーカ、家電メーカが上位を占めている。米国特許庁への出願では、IBM 社が２位を大きく引き離して最も多く、以下米国企業と日本企業が上位である。欧州特許庁へは、ドイツ SIEMENS 社を除けば、欧州企業よりもむしろ米国、日本企業が多く出願している。

図 3-17 日米欧各特許機関における上位出願人 (暗号技術全体、1970 年～2000 年出願累計)

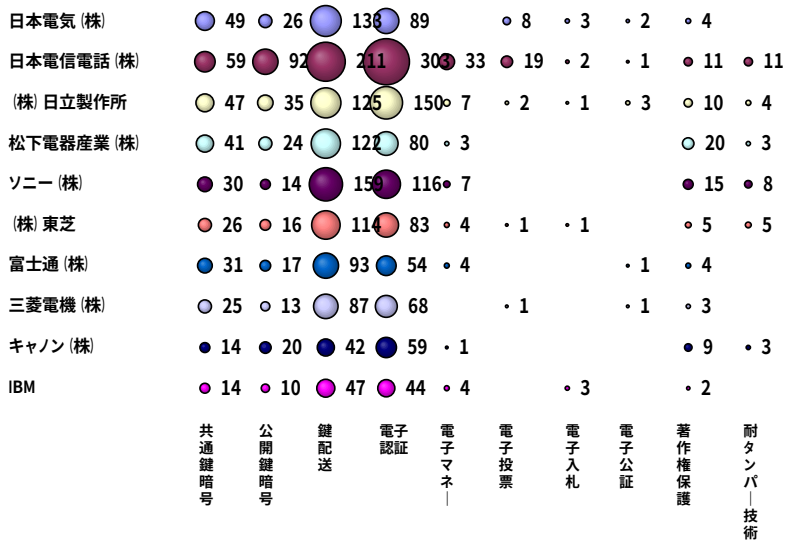


日本国特許庁への出願数で海外企業に比較して日本企業が圧倒的な規模であることは、国内市場での日本企業の優位を示しているとみることもできるが、一方特許出願に際しての言語の問題、あるいは費用の負担等、海外企業にとって出願の障壁が国内企業に比較して大きいことが、出願件数の差として現れているとも考えられる。

2. 技術区分別の動向

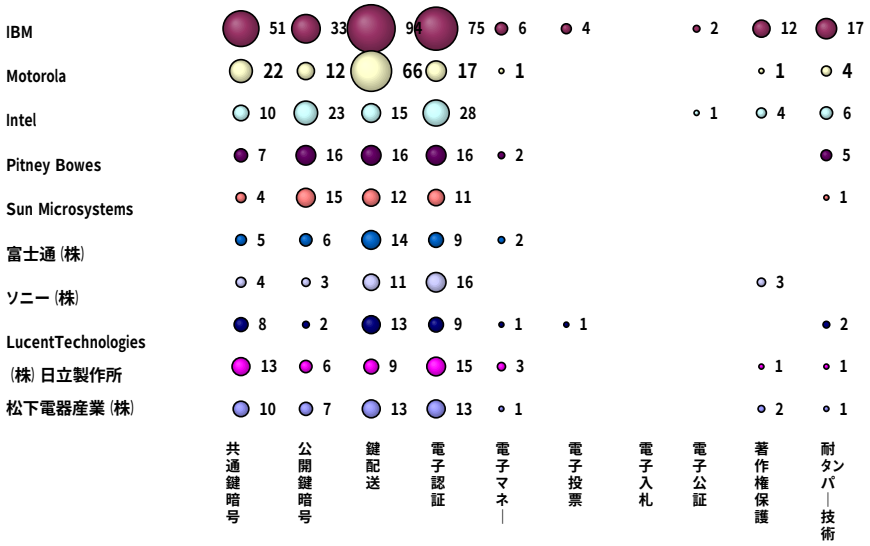
図 3-18～図 3-20 に日本国特許庁、米国特許商標庁、欧州特許庁への出願上位 10 社の技術区分別の出願件数を示す。図中円の面積が出願件数を表している。日本では日本電信電話(株)の出願に若干の特徴を認めることができる。同社は他の上位出願者に比較して、共通鍵暗号、公開鍵暗号の出願比率が高くなっている。また電子マネー、電子入札についても、わずかではあるが、他に比べて多くなっている。このような暗号基盤技術から応用までを広くカバーする出願傾向は、同社の通信事業者としての性格を反映しているということができよう。これと対照をなすのはソニー（株）である。同社は近年急激に出願件数を伸ばしており、2000 年では出願件数で１位となっている。ソニー（株）の出願に占める鍵配送、電子認証の比率は、上位出願人の中でももっとも高くなっている。その出願内容を見ると、過半数が記録媒体に関する内容であり、同社が映像および音声の記録分野における暗号技術の適用に取組んでいることを垣間見ることができる。

図 3-18 上位出願人の技術区分別出願状況(出願先：日本特許庁、1970〜2000 年出願累計)



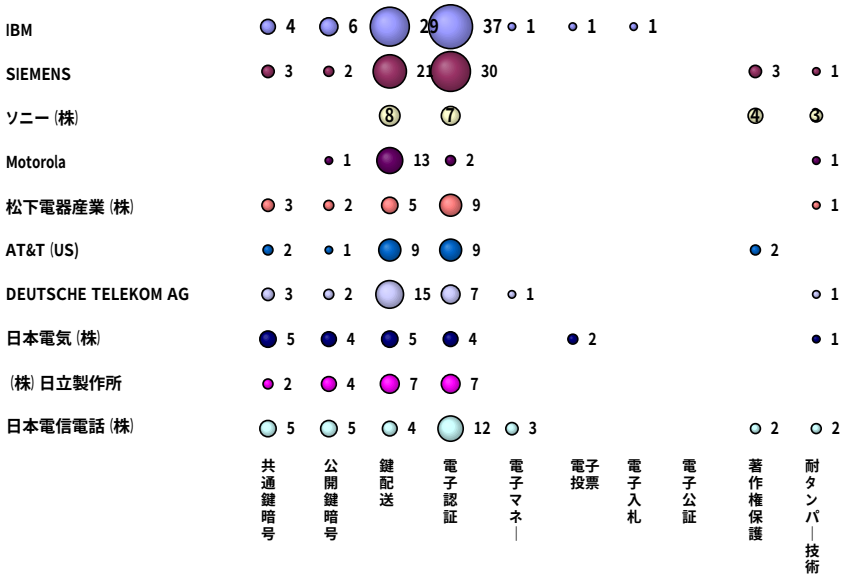
この図には表れていないが、米国の上位出願人で特徴的なのは個人出願の多さである（特許文書において出願人（Assignee）の欄がないものを個人出願とみなした場合)。1970 年から 2000 年の期間中でもっとも多く個人出願をしているのは米国の Silvio Micali 氏である（同氏は現在 MIT 教授であるが､1995 年以降の出願は出願人として大学名を記載していないため、個人出願として扱った)。個人出願の特徴は、共通鍵暗号、公開鍵暗闘といった暗号プリミティブ領域の割合が高いことである。この要因について一概に論ずることはできないが、ひとつに Silvio 氏のように大学教授等の出願のため、プリミティブ領域の出願比率が高くなっていることをあげることができよう。

図 3-19 上位出願人の技術区分別出願状況(出願先：米国特許商標庁、1970～2000 年出願累計)



欧州の特徴は、出願件数が日本では 30 位以下、米国では 15 位の SIEMENS 社が 2 位になっていることである。同社はドイツに本拠をおく総合電気・電子メーカであり、出願の内容は通信用途が中心である。ソニー（株）は出願件数累計で第 3 位であるが、欧州への出願では 10 の技術区分に属さない出願が多くを占めている。その内容は情報の記録と再生にかかわるものであり、出願年は 1996 年以降である。

図 3-20 上位出願人の技術区分別出願状況(出願先：欧州特許庁、1970～2000 年出願累計)



参考のため、上位出願人の日米欧三極特許庁への技術区分別登録数の合計を表 3-1 に示した（各技術区分における上位 5 社の欄を網掛けした)。

表 3-1 上位出願人の技術区分別登録状況

	全体		共通鍵暗号		公開鍵暗号		鍵配送		電子署名・電子認証	
	件数	順位	件数	順位	件数	順位	件数	順位	件数	順位
IBM	415	1	57	1	40	1	146	1	111	1
日本電気(株)	266	2	43	2	25	3	68	3	35	3
Motorola	169	3	21	3	12		70	2	18	
日本電信電話(株)	160	4	21	3	37	2	38	4	64	2
富士通(株)	108	5	11		7		30	5	15	
松下電器産業(株)	90	6	18		13		26		24	
Pitney Bowes	77	7	7		16	5	17		18	
(株)日立製作所	74	8	19	5	8		11		25	5
Intel	72	9	9		23	4	15		28	4
SIEMENS	65	10	15		5		19		19	
ソニー(株)	64	11	3		3		14		16	
AT&T	51	12	7		4		11		21	
三菱電機(株)	51	13	10		1		16		11	
Sun Microsystems	49	14	4		15		12		11	
キヤノン(株)	46	15	9		9		12		10	
General Instrument	44	16	6		1		16		12	
Lucent Technologies	43	17	8		2		13		9	
(株)東芝	38	18	4		3		12		3	
Microsoft	36	19	2		9		15		16	
Digital Equipment	30	20	6		7		8		2	
BRITISH TELECOMM	25	21	5		0		12		2	
FRANCE TELECOM	23	22	3		6		7		13	
沖電気工業(株)	23	23	6		1		6		3	
ALCATEL STK AS	21	24	3		1		7		3	
Bell Communications Research	21	25	3		13		8		12	
(株)高度移動通信セキュリティ技術研究所	20	26	2		5		14		5	
Northern Telecom	20	27	7		4		5		4	
Scientific Atlanta	19	28	3		0		5		6	
Compaq Computer	18	29	1		0		2		1	
KDD(株)	18	30	2		1		12		8	

電子マネー、電子投票、電子入札、電子公証、著作権保護、耐タンパー技術については、件数が少なく、順位のバラツキが多い。すなわち、技術を区分しない場合は下位であっても、特定の技術分野では上位である例が多くなっている。これは、これらの技術区分は応用的要素が強く、特定のビジネスに結びつきやすい傾向があるためと考えられる。例として、電子マネーにおける Microsoft 社、著作権保護におけるソニー (株)、耐タンパーにおける Bell Communications Research Inc. などを挙げることができる。

第3節 三極間の特許出願状況

特許出願における日米欧三極間の出願構造を示したのが図 3-21 である（米国は 2000 年 11 月出願まで公開制度がなかったため、登録件数を示す）。日本特許庁への出願 8,563 件のうち国内からの出願が 7,754 件と約 90%を占めている。これに対し米国の国内率は 65%、欧州の域内率は 38%である。また、三極以外からの出願の割合は日本国特許庁 1.1%、米国特許商標庁 4.1%、欧州特許庁 4.1%と日本のみがやや低い値となっている。三極以外は具体的にはオーストラリア、韓国、台湾、インド等である。

図 3-21 日米欧 三極間の特許出願・登録構造（期間：1970 年～2000 年）

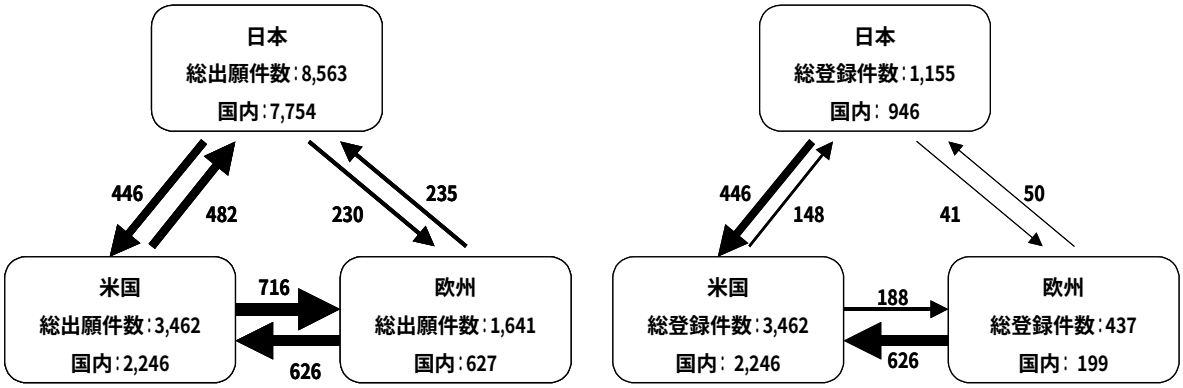


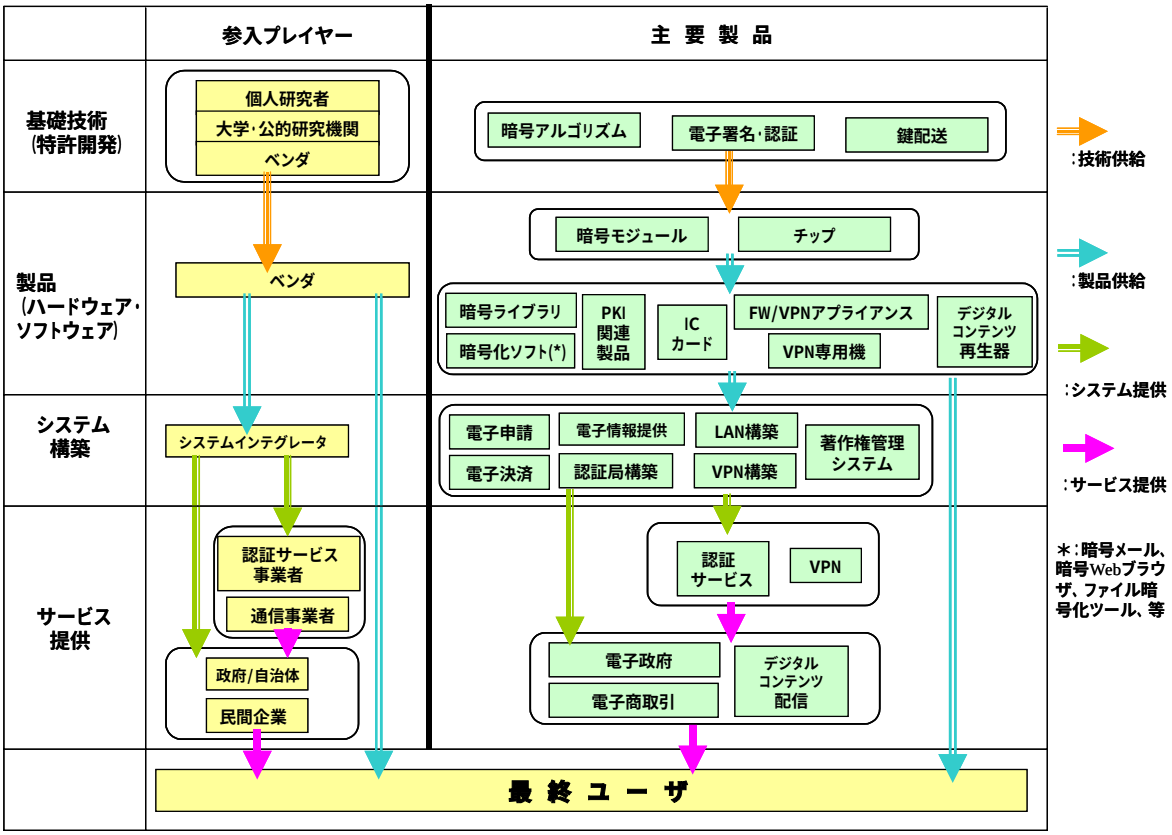
図 3-21 を見ると、日米・日欧・米欧二極間の特許出願件数の出入り、すなわち特許から推定される技術力はほぼ均衡していることがわかる。ただし、第３国を含めた場合は事情がことなり、米国に対する出願を日欧で比較すると、欧州は日本の 1.4 倍、欧州に対する出願を日米で比較すると米国は日本の３倍の件数となっている。

第4章 暗号技術の市場環境

第1節 暗号技術の市場構造

暗号技術関連市場は、暗号関連製品（ハードウェア/ソフトウェア）、システム構築、サービス提供の 3 つの領域に大きく区分して考えることができる。共通鍵暗号、公開鍵暗号、鍵配送、電子署名・認証といった暗号の基礎技術は暗号関連製品として提供され、電子マネー、電子入札、電子公証、電子投票といった応用技術はシステム構築として提供される。暗号技術関連市場の全体構造を図 4-1 に示す。企業の事業範囲の違いはあっても、全体的な構造は日米欧で共通している。

図 4-1　暗号技術市場の全体構造



（注1）　主要製品として挙げられている暗号モジュールと暗号ライブラリの違いは微妙であるが、ここでは暗号モジュールはある暗号アルゴリズムを実装したものであり、暗号ライブラリは、それらの暗号モジュールを複数組み合わせて製品化したものと区別している。たとえば三菱電機の PowerMISTY においては共通鍵/公開鍵暗号の他、デジタル署名やメッセージ認証、鍵交換などの機能を含めた形で暗号ライブラリとして提供している。

（注2）　FW/VPN アプライアンスとは、ファイアウォールに VPN 機能が付加された製品である。VPN 機能は VPN 専用機として提供されてきたが、2001 年頃からファイアウォールの機能の一部として提供される製品が増えてきている。

（注3）　最終ユーザに提供されるサービスとして、電子政府、電子商取引、デジタルコンテンツ配信などがあるが、最終ユーザ向けの最終段階のサービスにおいて暗号技術は表立って見えない形で含まれている。このため、市場規模の分析などにおいてこれらは含めないものとする。

暗号技術関連市場は、暗号技術の民間利用が開始された 1970 年以降に徐々に立ち上がった市場であり、インターネットの普及やそれに伴うセキュリティ確保の重要性の認識向上に伴い、ここ数年間で拡大している。ユーザからのニーズに対応した暗号技術を採用した新たな製品、サービスが市場に続々と投入されており、製品、サービスは分化しつつある。

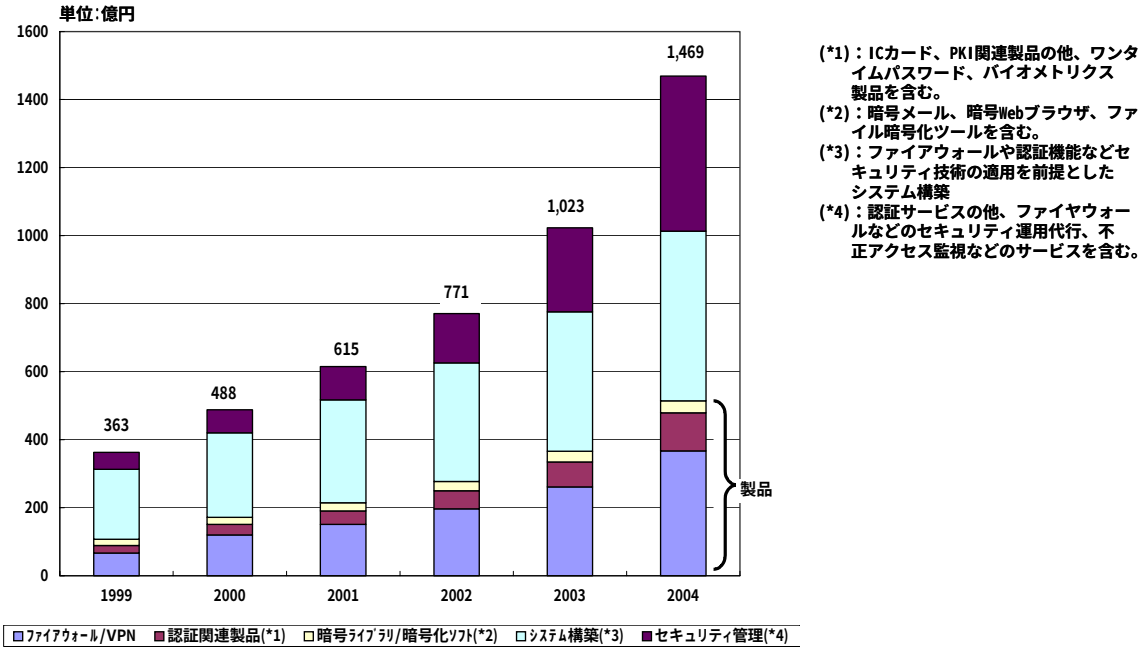
第2節 暗号技術関連市場の市場規模

暗号技術関連の市場の規模を純粋に捉えた市場調査データは無いため、セキュリティビジネスおよびセキュリティソフトウェアの市場規模を見ることにより、動向を把握することとする。

1. 市場規模の日米比較

図 4-2 および図 4-3 にセキュリティビジネス市場の日米の市場規模と予想を示す。暗号技術は、暗号ライブラリ／暗号化ソフトに含まれる他、認証関連製品等のジャンルの要素技術としても含まれている。

図 4-2 セキュリティビジネスの国内市場規模の推移

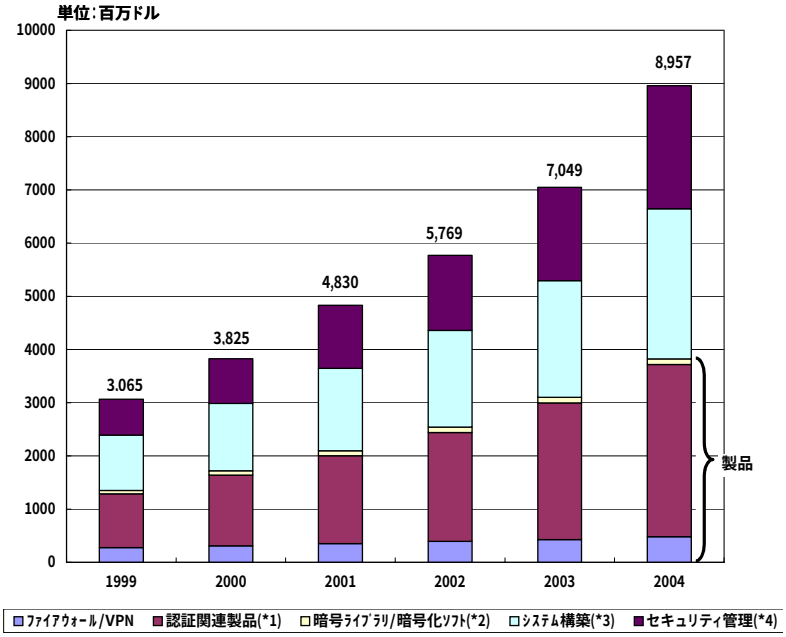


（注 1）1999 年は実績値、2000 年から 2004 年は 1999 年の実績値をベースとする予測値

（注 2）ファイアウォール/VPN、認証関連製品、暗号ライブラリ/暗号化ソフトは市場構造図（図 4-1）の製品に、システム構築はシステム構築に、セキュリティ管理はサービス提供に対応する。

（出典）情報処理振興事業協会、2001 年 3 月、「情報セキュリティビジネスに関する調査報告書」

図 4-3 セキュリティビジネスの米国市場規模の推移



(*1)：ICカード、PKI関連製品の他、ワンタイムパスワード、バイオメトリクス製品を含む。
(*2)：暗号メール、暗号Webブラウザ、ファイル暗号化ツールを含む。
(*3)：ファイアウォールや認証機能などセキュリティ技術の適用を前提としたシステム構築
(*4)：認証サービスの他、ファイヤウォールなどのセキュリティ運用代行、不正アクセス監視などのサービスを含む。

（注 1）1999 年は実績値、2000 年から 2004 年は 1999 年の実績値をベースとする予測値
（注 2）ファイアウォール/VPN、認証関連製品、暗号ライブラリ/暗号化ソフトは市場構造図（図 4-1）の製品に、システム構築はシステム構築に、セキュリティ管理はサービス提供に対応する。
（出典）情報処理振興事業協会、2001 年 3 月、「情報セキュリティビジネスに関する調査報告書」

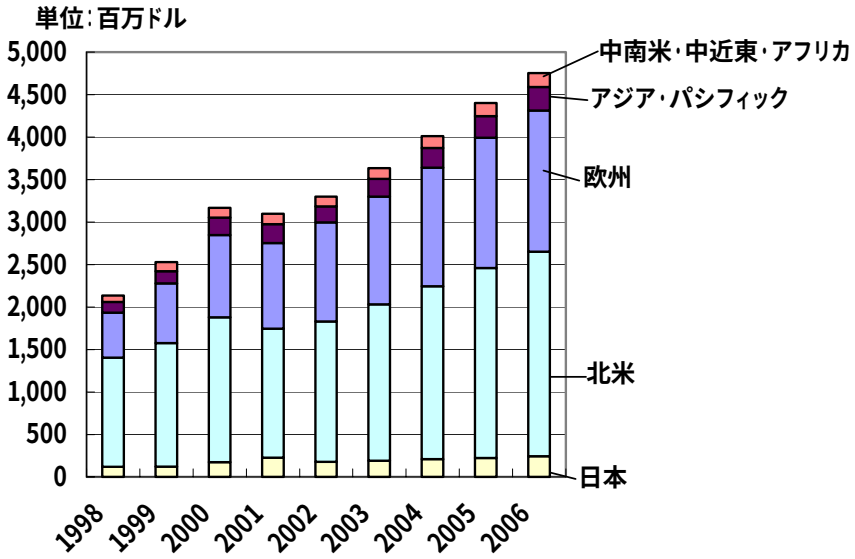
セキュリティビジネスの市場規模は、1999 年の実績において、日本の 363 億円に対し米国は 3,371 億円（1＄＝110 円で換算。以下同様）となっており、米国の市場規模は日本の 10 倍弱となっている。この差の主要因としては、EC ビジネスの市場規模の差およびセキュリティ対策の必要性に対する認識の差であると思われる。例えば、2000 年の日米の EC 市場を比較すると B to C 市場では、日本の 8,240 億円に対し米国の 8.79 兆円（10 倍）、B to B 市場では日本の 21.6 兆円に対し米国の 63.6 兆円（3 倍）となっている（2001 年経済産業省等調査）。

2． 市場規模の三極比較

日本/北米/欧州のセキュリティソフトウェア[4]の市場規模は、2001 年において欧州 10 億ドル、北米 15 億 2 千万ドル、日本 2 億 3 千万ドルとなっている（図 4-4）。

[4] **ここで、セキュリティソフトウェアは、暗号化、アンチウィルス、侵入検知システム（IDS）、その他のソフトウェアを含んでおり、その割合は暗号化が 10%、アンチウィルスソフトが 35%、IDS が 5%、その他 50%となっている（2001 年）。暗号ソフトウェアは主に PKI 関連製品やファイアウォールや VPN 製品に利用されているソフトウェアが含まれている（出典：ガートナー データクエスト、2002 年 11 月、GJ03108）。**

図 4-4 世界セキュリティソフトウェア市場規模の推移（地域別）



（出典）ガートナー データクエスト、2002 年 11 月、 GJ03107

セキュリティソフトウェア市場規模は、日本、北米、欧州ともに 2002 年以降は拡大が予想されている。2002 年までについては、製品価格のディスカウントの影響により北米は 2001 年に、日本は 2002 年に市場規模が縮小しているのに対し、欧州では 1998 年以降伸び率は小さいながらも拡大が続いている。2002 年以降の予測値を見ると、日本、北米、欧州ともほぼ同じ水準（年率約 1.1 倍）の拡大が予想されている。セキュリティソフトウェア市場における北米の市場規模は日本の約 10 倍であり（欧州は約 5 倍～7 倍）、セキュリティビジネス市場と同様の傾向が見られる。

第3節　　市場シェアの状況

1．主要製品・サービス別の市場シェア

暗号技術関連市場における主要製品・サービス別の市場シェアを表 4-1 に示す（暗号ソフトウェア以外は日本国内市場におけるシェア）。

日本国内市場において、海外企業（国外に本拠地を置く企業）の市場シェアが、暗号ライブラリ：81%、PKI 関連製品：82%、ファイウォール/VPN アプライアンス：73%、VPN 専用機：72%となっており、国内市場の 7 割以上を占めている。これらの海外企業の多くが日本法人を設立し、国内での製品の販売、サービスの提供にあたっている。

システム構築サービスにおいては、日本の大手システムインテグレータが市場シェアの上位を占めている。システム構築にあたっては、各システムインテグレータの提供する自社製品が採用されるケースが多いと考えられるが、その部分の市場規模は製品の市場規模として明確に把握することは難しい。

表 4-1 暗号技術関連市場におけるトップシェア企業

製品/サービス	企業名 （）内は日本法人	本社国籍	シェア(%) (金額ベース)
暗号ライブラリ（国内市場）			
	RSA Security（RSA セキュリティ）	米国	81.3 (*1)
	その他		
PKI 関連製品（国内市場）			
	Baltimore Technologies（日本ボルチモアテクノロジーズ）	アイルランド	47.1 (*1)
	Entrust Technologies（エントラストジャパン）	米国	35.3 (*1)
	その他		17.6 (*1)
ファイウォール/VPN アプライアンス（国内市場）			
	Nokia（ノキア・ジャパン）	フィンランド	27.0 (*1)
	Cisco Systems（シスコシステムズ）	米国	21.6 (*1)
	SonicWall	米国	12.6 (*1)
	NetScreen Technologies（ネットスクリーンテクノロジーズ）	米国	11.9 (*1)
	富士通（株）	日本	7.2 (*1)
	その他		19.8 (*1)
VPN 専用機（国内市場）			
	Cisco Systems（シスコシステムズ）	米国	27.8 (*1)
	Nortel Networks（ノーテルネットワークス）	カナダ	27.8 (*1)
	Alcatel（日本アルカテル）	フランス	16.7 (*1)
	その他		27.8 (*1)
暗号ソフトウェア（世界市場）			
	Check Point Software	イスラエル	39.9 (*2)
	RSA Security	米国	17.5 (*2)
	Entrust Technologies	米国	12.9 (*2)
	Baltimore Technologies	アイルランド	9.6 (*2)
	その他		20.1 (*2)
システム構築（国内市場）(*3)			
	富士通（株）	日本	-
	（株）日立製作所	日本	-
	日本電気	日本	-
認証サービス（国内市場）			
	日本ベリサイン	日本	75.0
	その他		

(*1)：**国内市場における市場シェア。富士キメラ総研「**2002　**ネットワークセキュリティビジネス調査総覧」**2001 **年実績値**

(*2)：**世界市場における市場シェア。**2001 **年実績値。**
出典：Gartner Dataquest "2001 Security Software Market Share" 24 October 2002, GJ03113
ここでいう「暗号ソフトウェア」は、VPN **関連製品、**PKI **関連、モバイル関連で利用される暗号ソフトウェア等を含む。**

(*3)：2000 **年度国内** IT **サービスベンダーの売り上げ順位。**
出典：atmarkit、2001.6.16、NewsInsight、[online] 2002.11.15 **検索、**
http://www.atmarkit.co.jp/news/200106/16/idc.html
ここでいう「IT **サービス」は、システムインテグレーション、ソフト/ハードの保守、コンサルティング等を含む。**

暗号技術関連製品の輸出入状況を直接的に示す統計情報は発見できなかったが、暗号技術関連の主要製品・サービスの市場シェア結果から分かるとおり、海外ベンダ製品が圧倒的市場シェアを占めている。暗号ソフトウェアの世界市場においても市場シェアの 75%は欧米の企業に独占されている。こういった事実から、現状の日本における暗号技術関連製品は大幅な輸入超過となっていると推定される。「ソフトウェアの輸出入統計調査（2000 年度）」（電

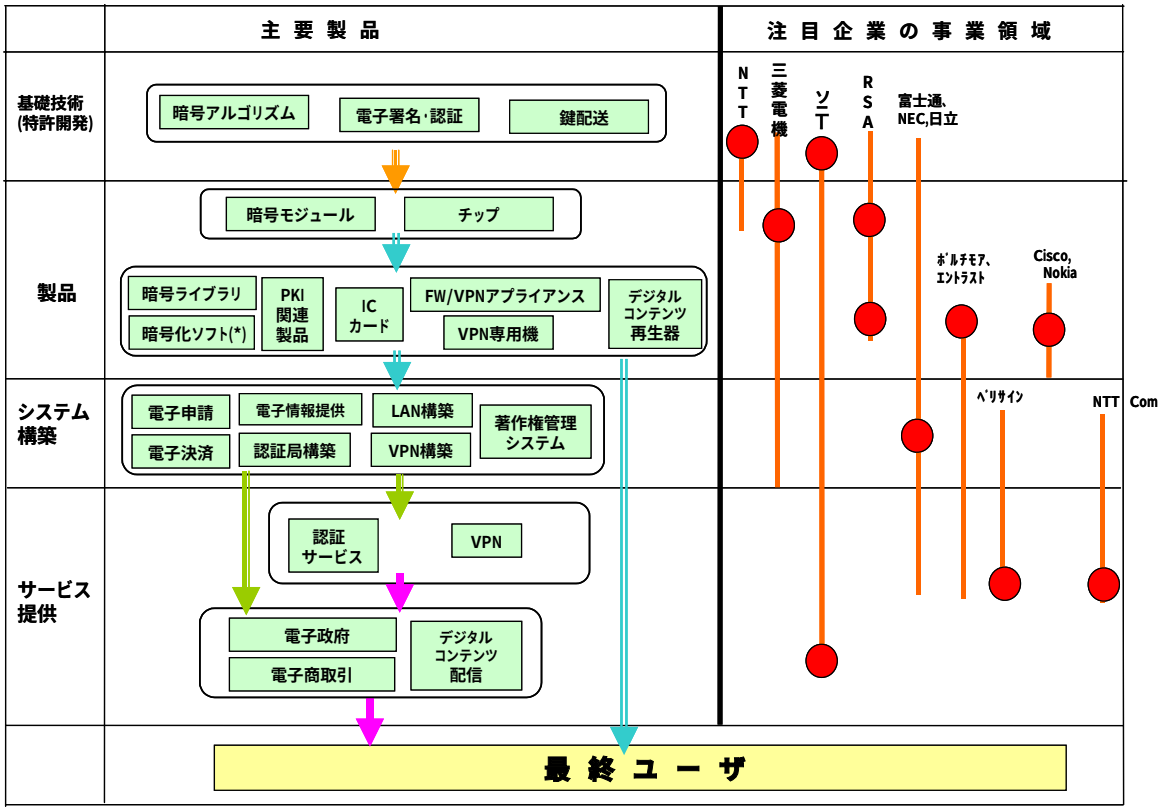
子情報技術産業協会）によると、ソフトウェア全般の輸出入の割合は 100：1 となっており、輸入超過は暗号技術関連製品に特有の現象でないことが分かる。

暗号製品の市場シェアを海外企業に押さえられている最大の理由は、デファクトスタンダードとなる技術・製品を日本が保有していないためであろう。このような状況の中、2000 年 1 月に 3GPP（3rd Generation Partnership Project）において、三菱電機の開発した MISTY に基づいた KASUMI 暗号が、次世代移動通信システムの国際セキュリティ暗号標準に採用されたこと、また、欧州の NESSE プロジェクトの決定した 12 の推奨暗号の中に、日本で開発された 3 つのアルゴリズムが選ばれたこと（第 5 章第 3 節）も、今後の普及の契機として特筆に値しよう。

第4節 暗号技術関連市場における注目企業の事業領域

注目企業の事業領域を、先に示した暗号技術関連市場の市場構造にマッピングしたものを図 4-5 に示す。縦線で各企業の事業領域の範囲を、丸で重点領域を示している。

図 4-5　暗号技術関連市場における注目企業の事業領域



（注）RSA：RSA セキュリティ、NEC：日本電気、日立：日立製作所、
ボルチモア：日本ボルチモアテクノロジーズ、エントラスト：エントラスト･ジャパン、
ベリサイン：日本ベリサイン、Cisco：シスコシステムズ、Nokia：ノキア・ジャパン、
NTT Com：NTT コミュニケーションズ

第5節 注目企業のビジネス戦略における暗号技術および特許の位置付け

RSA Security、NTT、三菱電機など、競合他社に先行して暗号アルゴリズムといった基礎技術を開発または提供し、安全性に関する実績を築いている企業においては、自社で保有する暗号の基本特許を無償化することにより、技術適用範囲の拡大を目指している。

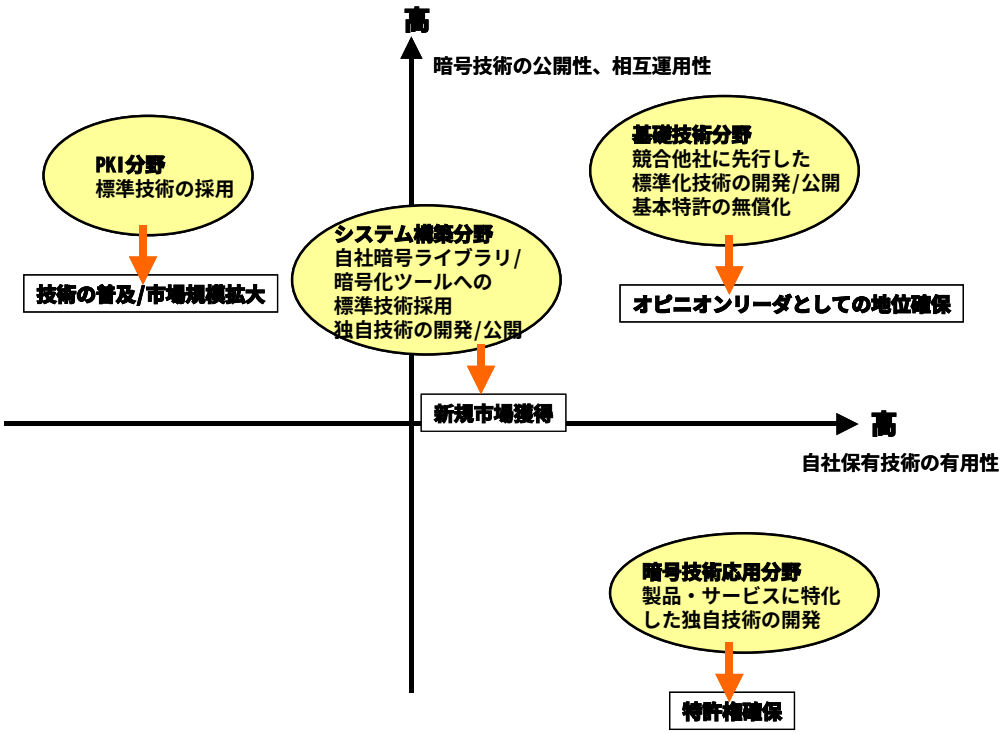
PKI 分野は、認証機関の相互認証性、安全性への信頼性に対するニーズが大きい分野である。そのため、ボルチモアテクノロジーズ、エントラスト、ベリサインといった公開鍵認証基盤である PKI 関連製品ベンダや認証サービス事業者においては、デファクトスタンダードな暗号プリミティブを採用し、その上で PKI 製品の機能を高める技術を開発して、競争優位性の獲得を図っている。

電子政府システム等のシステム構築分野では、ユーザに提供されるシステムの安全性機能の一部として暗号技術が利用されることが多い。ここにおいても、自社開発製品であれ、外部からの調達であれ、標準暗号またはデファクトスタンダードを採用することにより、ユーザの信頼性、相互運用性を確保している。

デジタルコンテンツの著作権保護技術は、民生市場向け製品に搭載されるため、コストセンシティブであり、実現できる安全性の水準はコストとのバランス上決定されざるを得ない（ただし、DeCSS の例のように、コピープロテクションを破るソフトが開発されて Web 上で公開される例もあり、今後は安全性強化の方向に進むと予想される）。また、他社製品との相互運用性は余り重視されない。

ビジネス戦略における暗号技術および特許の位置付けは、暗号技術の公開性・相互運用性と自社保有技術の有用性といった 2 つの軸で捉えることができる。図 4-6 に上記 4 つの事業分野の位置付けを示す。

図 4-6 ビジネス戦略における暗号技術および特許の位置付け



第5章 暗号技術の政策動向

暗号技術に関する政策の変遷と近年の状況は以下の通りである。

1. 暗号技術の利用の一般化に伴う規制緩和

従来、暗号技術の利用は軍事目的の利用が中心であった。しかし、1970 年代から 1980 年代に金融業界を中心に暗号利用が広まり、1990 年代のインターネットの普及とともに一般大衆の暗号利用も進んだ。こうした流れに伴い、暗号の輸出および利用に関する規制は大幅に緩和されている。

2. 規制緩和と治安維持対策

現在において、暗号政策は、通信の秘密の確保および産業振興のための規制緩和と、治安維持対策のための（鍵預託等の）法執行の両面がある。したがって、暗号政策立案に当たっては、企業や一般市民の暗号利用による社会発展に伴う利益享受と、国家安全保障上および治安上のバランスに立つことが世界的な潮流であり、わが国においても、こうした視野に立脚した議論を行う必要がある。なお、2001 年 9 月に米国で発生した同時多発テロ以後、各国で通信傍受を是認する動きがあるが、暗号の輸出規制や利用規制への直接の影響は明白ではない。

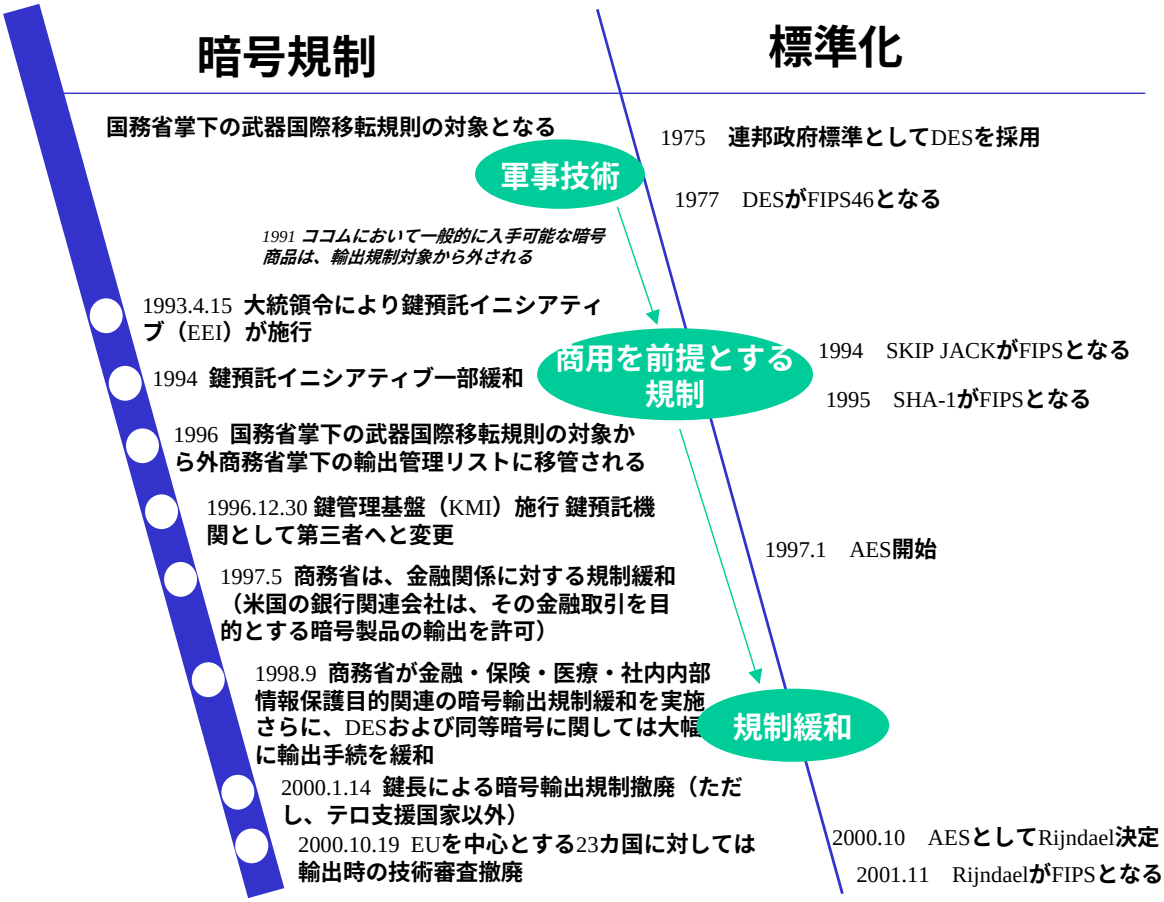
3. 政府自身による暗号の利用の拡大

従来、政府部内における暗号の利用は、防衛・外務等の国家機密に係わる利用が中心であったが、近年は各国において電子政府の構築が盛んになっており、電子申請等を中心とする民間とのインタフェース部分や政府職員の通常業務においても暗号の利用が一般化されている。この結果、従来全く接点を持っていなかった公的部門における暗号利用と民間部門における暗号利用が、接点を持つことになり、公的部門と民間部門の協調による標準暗号の検討や暗号製品の選定等の暗号政策に対するニーズが高まっている。さらには、インターネットにより世界中の多くのシステムが接続されている。そのため、暗号利用に際しても、海外との相互運用性を重視することが一般的となっている。

第1節 米国

米国における暗号技術に関する産業政策、規制政策の推移に関して、特に暗号規制と標準化を中心に図 5-1 に示す。

図 5-1 米国における暗号政策の推移



第二次大戦後、暗号製品は国務省掌下の武器国際移転規則の対象となった。これは、米国において暗号製品全体が武器とみなされていたことを示すものである。

1970 年代にはいり、オンラインシステムの発展に伴い金融業界を中心に暗号利用のニーズが増した。そのため、NBS（National Bureau of Standards、NIST の前身）が中心となり、暗号アルゴリズムの公募を行い、最終的に、IBM の提案した Lucifer に手を加えた DES を連邦情報処理標準 FIPS46 として制定した（1977 年）。DES は米国内で広く使われ、コストの低減や、安全性に問題のある暗号の淘汰という、制定当初に目的とされた効果を十分もたらした。また、米国外においても金融界を中心に DES 利用の浸透が進み、DES は事実上の国際標準暗号として機能するようになった。さらには、1990 年代に入り、インターネットの爆発的な普及、PGP と呼ばれるフリーの公開鍵暗号ソフトウェアの登場等により、暗号の利用は、産業界のみならず一般市民へと大幅に拡大した。

こうした動きに対し、1993 年に米国政府は暗号利用の大衆化に対して歯止めをかけるべく、鍵預託制度を発表した。これは、クリッパー・チップという政府設計による暗号通信用のチップを用いた鍵預託方式の採用により、国民の電話通信上の安全とプライバシーを確保しつつ、法執行の合法的な必要性にも応えようとしたものである。しかしながら、鍵預託制度には、多くの批判が浴びせられ、何度も形を変え、結局はその後撤回されている。

輸出規制に関しては、1996 年に、暗号製品は国務省掌下から、商務省掌下へと移管され、民生品としての位置付けを与えられ、2000 年には、テロリズム支援国家以外に対する鍵長に

よる暗号輸出規制撤廃、および EU を中心とする 23 カ国に対する輸出時の技術審査撤廃が相次いで実施され、実質的な暗号の輸出規制はほぼなくなった。

1990 年代に入ってから DES の安全性等に関する問題点が意識され始めたため、1997 年に次世代暗号である AES の公募が開始された。選定の主な基準は次の通りであった。安全性の問題が小さいブロック暗号であること。アルゴリズムは完全に公開され、オープンな場で議論し評価すること。実装も含めて知的財産権上の制限がなく、世界中で royalty-free で使えること。実装時に処理速度やメモリ使用量といったコストが低い暗号であること。様々な使用形態に対応できること。最終的に、ベルギーの研究者から提案された Rijndeal が AES として選定され、FIPS197 として公布された（2001 年 11 月）。

米国における暗号技術関連の研究開発は、多くの省庁で行われている。全体像は捉えにくいが、DARPA、NSF において研究開発が行われている。NIST は研究機関ではないが、非軍事目的の連邦政府機関向け暗号技術の標準化を行っており、結果を FIPS として公表している。NSA（National Security Agency）は、国家安全目的の通信傍受・暗号の専門機関であるが、その活動内容は非公開である。

第2節 日本における暗号技術に関する産業政策、規制政策等

日本における暗号規制は、旧ココムおよび現ワッセナーアレンジメントの枠組みでなされてきた。現状、この枠組みでは、暗号利用および暗号製品輸入に関しては規制が無く、暗号製品輸出に関しては規制が設けられている。

ワッセナーアレンジメントは、33 の参加国より構成されており、事務局はウィーンにある。目的は、武器とその関連汎用品及び技術の移転と過剰な蓄積を防止することによって、地域紛争を予防しようとするものである。各参加国が遵守する輸出管理品目リストを協議の上作成しており、各々の国における輸出管理制度によって輸出規制が行われている。同管理品目において、暗号製品も対象として挙げられている。1999 年に暗号関連製品については大幅な規制緩和がなされ、続いて 2000 年にも大幅な規制緩和が行われた。

日本においては、長い間、政府が利用する標準暗号は定められていなかったが、電子政府構築の機運の高まりとともに、2000 年 6 月より当時の通商産業省と郵政省が主体となって、CRYPTREC（CRYPTography Research & Evaluation Committee:暗号技術評価委員会）が発足し、電子政府推奨暗号リストの策定を開始した。電子政府推奨暗号リストは、共通鍵暗号、公開鍵暗号、その他の技術分類毎に設定されており、2 度の電子政府推奨暗号の公募を経て、2002 年 3 月には評価報告書が発表された。2002 年 11 月には、総務省と経済産業省が電子政府推奨暗号リスト案を発表し、2002 年 12 月 25 日までの意見招請を経て、2003 年 2 月 20 日に電子政府推奨暗号リストが決定された。なお、電子政府推奨暗号とは、総務省および経済産業省が、電子政府において利用する推奨暗号を規定するものであり、他省庁等に対して強制力を持つものではない。

暗号技術の研究開発に関しては、経済産業省（主として情報処理振興事業協会を通じて）、総務省（主として通信・放送機構を通じて）、防衛庁で行われていることが公表されている。

第3節 欧州・その他における暗号技術に関する産業政策、規制政策等

1. ヨーロッパ

イギリスは、ワッセナーアレンジメントと EU の規制リストの堅持のため、暗号の輸出規制を維持している。利用に関する規制は無いが、従来より、キーエスクローを推進している米国を最も強く支持してきたが、1999 年 3 月、産業界からの要請を受ける形で大幅な規制緩和がなされた。一方、1999 年の「電子商取引の促進：貿易産業委員会の報告に対する政府の回答及び法案草案に関する解説」という協議文書において、当局の暗号鍵の開示を要求する権限を宣言している。また、2000 年の捜査権限規制法により、暗号化された通信における当局の傍受の予防措置規定が明示されている。

フランスは、従来から、暗号規制の厳しい国である。1990 年の法律は、情報の秘匿を目的とする暗号使用については事前の許可申請を要することを定めていた。しかし、インターネットの普及とともに暗号の使用が広まり、1999 年には、鍵長 128 ビットまでの暗号については、利用が自由化され、128 ビット以上の鍵については、預託の義務化は撤廃された。代わりに、法律執行機関の要求に応じて、暗号化文書の平文を司法局に提出するよう人々に要求できるしくみが設けられた。

ドイツは、従来から暗号の利用規制に反対の立場をとっており、ワッセナーアレンジメントにおいてキーエスクローが規定されることを防いだとも言われている。

標準化関連では、NESSIE (New European Schemes for Signature, Integrity, and Encryption) プロジェクトが実施されている。これは、欧州における安全な暗号技術の普及促進を図るために、EU の情報社会プログラムの一環として、推奨暗号を選定するものであり、2000 年に開始された。共通鍵暗号、公開鍵暗号、電子署名アルゴリズム等の７つのカテゴリの公募に世界から 42 のアルゴリズムが提案された。選定の基準は、安全性、性能、および知的財産権（フリーであるか、安価・平等にライセンス）であり、2003 年 2 月に 12 のアルゴリズムが最終的に選定された。共通鍵暗号アルゴリズム４つのうちの２つ（MISTY1（三菱電機）、Camellia（NTT、三菱電機の共同））、公開鍵暗号アルゴリズム３つのうちの１つ（PSEC-KEM（NTT））が日本企業からの提案アルゴリズムである。

2. その他

OECD は、1997 年３月に「暗号政策に関するガイドライン(Guidelines for Cryptography Policy)」を公表した。ガイドラインでは、市場主導による暗号手法の開発、暗号手法に関する諸標準（暗号技術に関する技術的諸標準、諸基準及びプロトコルは、国内及び国際レベルで開発され、公表されるべきである）、プライバシー及び個人データの保護、合法的アクセス（国家の暗号政策は、他の原則を尊重しつつ、暗号化されたデータの平文又は暗号鍵の合法的なアクセスを認めることができる）、国際的協力（暗号政策の調整・協力、貿易障壁の除去）などを原則として掲げている。ガイドラインは、その後の加盟国の暗号規制政策の基調となった。

第6章 まとめ

第1節 現状のまとめ

従来、軍事技術であった暗号技術はコンピュータによる情報システムが構築され始めた1960年代から非軍事分野で需要が生じ、1970年代の米国における連邦政府の調達時における標準暗号アルゴリズムとしてDESが制定されたことにより、非軍事の政府機関や金融業界での使用が広がった。1990年代になると、インターネットの普及によって、一般における暗号の利用が始まった（暗号化メールPGP、電子商取引におけるSSLの利用など）。公開鍵暗号が実用的に用いられるようになったのも1990年代になってからである。同時に、1990年代は、暗号評価手法の研究が進み、計算機性能の向上とも相まって、DESが安全と言えなくなってきた。そこで、様々な用途において安心して使用できる次世代暗号の策定が必要となり、米国でAESが公募され、透明性の高い評価プロセスの結果、AESが正式に標準化された。日本でも暗号技術検討委員会が電子政府推奨暗号リストを策定し、また、ヨーロッパでもEUのNESSIEプロジェクトにおいて信頼できる暗号プリミティブのセットが作成された。今や、暗号技術は一般国民が普通に使える「コモディティ」になったと言えよう。

特許出願件数は1970年代から漸増していたが、1990年台から急増加している。

現状、暗号製品・サービスの市場においては、欧米の少数の企業の市場競争力が強力である。高度な安全性が要求されるシステム構築の分野では、システム構築に強い企業が自社ないし他社の暗号製品を用いている（暗号関連部分は表面には現れない）。応用分野では、デジタルコンテンツ流通において著作権保護技術が実用に供されている。電子マネー等の応用は、技術的には準備が出来ており、今後、期待される分野である。

暗号技術が軍事技術から民生技術になるに従い、米国において輸出に関する規制緩和が進み、世界に波及している。規制緩和に慎重な政府が、社会や市場の力に押されたという面がある。暗号技術の普及・相互運用性の保障において、政府標準暗号の制定は大きな意味を持った。

第2節 将来の展望

各国において標準暗号・推奨暗号が整備されつつある現在、それらの具体的普及が当然の次なる課題となる。これらの暗号プリミティブは、研究コミュニティによる評価を経ており、アルゴリズムの安全性は当面確保されていると考えてよい。そこで、実装上の安全性が当面の技術的課題と言える。暗号モジュール（ハードウェア、ソフトウェア）の性能向上も、重要課題であり、特に、ローエンドの機器（携帯端末等のハイパフォーマンスの出ない機器）において暗号が使用可能であるための条件となる。性能向上の要素として、低価格化、高速化、小型化（小さなメモリでの実装、など）などがある。

研究開発においては、標準暗号・推奨暗号が整備された後も、より優れた暗号アルゴリズムの研究と攻撃法の研究は、基礎研究テーマとして残る。特に、標準暗号・推奨暗号への攻撃法や、新たな攻撃法への耐性のある暗号アルゴリズムの研究は、来たるべき次世代の暗号アルゴリズムにつながるものとして必須のものであろう。

例えば、量子コンピュータにより全数探索が可能となった場合、現在の主流の暗号アルゴリズムは実用時間で解読されることになり、1970年代後半以降の暗号技術のパラダイムが崩れてしまう。量子コンピュータによる解読計算法が見つかっていないものとして、格子暗号

がある。また、計算量的安全性でなく情報量的安全性に基づく暗号や、盗聴があったことを検知できる量子暗号も既に実証されており、物理的な制約により、使用範囲は限定されるが、絶対的な機密の要求される分野での実用は早まる可能性がある。

暗号の応用技術（電子公証、電子投票、電子マネー、著作権保護、等）においては、暗号プリミティブが部品的に用いられ、一定の手順（プロトコル）に従って、機能が実現される。このような技術においては、使われている暗号プリミティブが安全であっても、プロトコルに欠陥があると安全性が保証されない。暗号プロトコルの安全性の検証手法の研究も重要である。

暗号技術に関わる政策については、規制緩和（産業政策、プライバシー保護）と治安維持とのバランスが常に課題と言える。

市場的には、将来、市場的に必要となるであろう機能要件を先見して、先行開発してゆくことがポイントである。例えば、近年の標準暗号ではICカード、携帯端末等の小型ハードウェア上に実装可能であることが一つの条件となっており、RijndaelがAESとして選定された最大の理由は、ハードウェア上の性能が優れていたことだと言われている。ユビキタス社会への大きな動きの一部として、暗号技術の用途のフロンティアが拡大して行く中で、対応する技術への需要が現実化に合わせてタイムリーに完成度の高い製品を提供できるような技術開発が求められる。例えば、Webサービスでの安全性やモバイルPKIが現実のニーズとして現れてきている。

第3節 日本の研究開発水準、産業競争力

これまでの調査結果から、暗号技術分野における日本の競争力についてまとめる。

暗号技術分野の特許出願件数は1990年代に入ってから大幅に増えているが、米国特許商標庁では1992年頃から伸びているのに対し、日本国特許庁への出願は、若干遅れて1996年頃から伸びている。また、共通鍵暗号の例では、米国における共通鍵暗号DESの制定（1977年）に対して、日本における共通鍵暗号FEALの開発(1987年)に10年程度の開きがある。米国で開発されたDES、RSAなどの暗号アルゴリズムがデファクトスタンダードとなっている。

市場について見ると、セキュリティビジネス市場規模において米国と10倍程度の差、欧州と5倍程度の差がある。暗号製品・サービスにおける市場シェアでは、現状、欧米企業が圧倒的なシェアを握っている。

しかしながら、1990年代後半の特許出願件数の伸びによって、特許出願件数において、急速にキャッチアップしている。三極間の特許出願・登録構造を見ても、米国・欧州からの出願件数と日本から米国・欧州への出願件数は、同程度になっている。

また、線形攻撃法の考案（1993年 三菱電機・松井）や既知の攻撃法に対応した暗号アルゴリズムの研究開発（MISTY：1996年 三菱電機、Camellia：2000年 NTT・三菱電機）、などに見られるように、研究レベルにおいて、日本では欧米と肩を並べる事例が生まれている。主要国際学会（CRYPTO）における論文著者数で、米国、イスラエルに次ぐ第3位であることは、ハイレベルの研究者の一定の層が日本にあることを示している。国内学会の規模も年々増大している。このように、1990年代に入って、日本の研究開発力が欧米に相当程度追いついてきたと言える。

これら研究開発の積み上げは、3GPPにおける標準暗号に、MISTYをベースにした暗号が採用されたこと（2000年）や欧州のNESSIEにおいて日本で開発された3つの暗号アルゴリズムが推奨暗号の中に選ばれたこと（2003年）など、成果として結実しているところである。今後、国際的

に認知されたことによる信頼性の向上を生かし、基本技術を広くライセンスし、実装技術でリードすること等による市場的な成功の可能性も広がっている。

一般消費者市場向けでは、ソニーが著作権保護である MagicGate™技術を早期に製品化し、他社にライセンスするなど活発な展開をしているという例がある。

第4節 日本が目指すべき研究開発の方向性、取り組むべき課題

このような状況にあって、日本が今後目指すべき研究開発の方向性（主に民間企業)、取り組むべき課題や仕組み作り（主に政府）について述べる。

1. 研究開発の方向性

今後の研究開発・製品開発は、第 2 章で記した研究開発の現状や、研究開発課題を踏まえた上で、次の２つの視点から進めるのが望ましいと思われる。

(1) 拡大する用途（＝市場）の先取り

インターネットの普及により暗号技術の用途は拡大しており、今後、携帯機器のインターネット接続（主にワイアレス接続)、無線タグによる物品のインターネット接続など、ユビキタス社会が徐々に実現して行くのに対応して、様々な場面・用途で安全性が求められるようになろう。そのような、新たなニーズに対応して、早期から製品・サービスを開発することが、将来の市場における有利な位置の確保につながる。その際、従来ないし現状と違った特性を持つ暗号技術が求められる可能性があり、そこに研究開発の方向性が見出されるであろう。

(2) 用途の高度化を実現する新技術の研究開発

用途の拡大（水平方向）と同時に、用途の高度化（縦方向）が生じて行くと予想される。インターネット上のよりクリティカルなトランザクション、電子文書による紙文書の置き換え、などである。ここにおいては、暗号技術を中心としつつ、求められる機能を実現するためのシステム化技術の設計が重要になるであろう。

潜在的には、現在、事業分野において暗号技術を利用していない企業であっても、今後の事業分野における製品・サービスの差別化の一つの手段に、暗号技術はなり得る。

2. 取り組むべき課題

政府において取り組むと良いと思われる課題を挙げる。一つは、暗号技術の重要な需要セクターとしてのものであり、もう一つは、研究開発の支援セクターとしてのものである。

(1) 政府における暗号技術の位置付けの強化

電子政府システム等の政府調達におけるセキュリティ基準の強化、政府推奨暗号に基づいた製品認定制度、暗号専門機関（政府推奨暗号の管理機関）の設置など。

これらは、電子政府における安全性確保のためなど、それ自体重要であるばかりでなく､暗号技術という産業分野における需要条件の整備･高度化に資するものでもある。

(2) 基礎から応用までのバランスに配慮した研究開発

暗号分野の研究は、暗号アルゴリズム研究に代表される基礎研究、実装技術に代表される応用研究等に分けられる。米国においては、基礎研究から応用研究をバランスよく行うことにより、シーズ醸成とデファクトスタンダード獲得の両面に寄与している。今後は、わが国においても、将来のデファクトスタンダード獲得の礎となるシーズ醸成が必要であり、自由な発想による研究開発に関して、国が積極的に支援することが重要である。

【お問い合わせ先】特許庁 総務部 技術調査課 技術動向班
TEL：03-3581-1101（内 2155）　FAX：03-3580-5741
E-mail：PA0930@jpo.go.jp