特集「情報セキュリティ」の編集にあたって

小　山　謙　二†

電子送金，電子郵便，オフィスオートメーションが広く社会に普及し，ビデオテックス，テレテックス，衛星通信などのニューメディアを利用したINS（高度情報通信システム）やVAN（高付加価値通信網）が順調な発展を遂げ，活況を呈している．

一方，こうした高価値な情報を扱うシステムが社会に浸透すればするほど，システムの信頼性（リライアビリティ）と安全性（セキュリティ）を確保することが重要になってきた．特に，最近のコンピュータ犯罪の急増に伴い，セキュリティに対する関心と要求が高まっている．

高信頼化技術はシステムの故障，エラー，ミスによる異常を検出・回復，あるいは，回避する技術であり，情報セキュリティ技術とは，システムへの意図的な不正行為，例えば，盗聴，無断コピー，ニセデータ入力，無許可データへのアクセス，改ざん，偽装などを防止する技術である．

高信頼化技術については，本誌で，2年前に特集号（Vol. 23, No. 4）が刊行されたが，セキュリティに関しては，いくつかの単発の解説記事が掲載されただけであった．暗号に関する解説（Vol. 22, No. 1）も3年前のことであり，その後我が国においても暗号の研究と開発が進展した．

こうした状況のなかで「情報セキュリティ」の特集号が企画された．本特集は，情報セキュリティを確保するための技術的対策を中心に解説したものである．その3本柱は暗号とアクセス制御と個人識別である．

本特集は次の10編から構成されている．

まず，第1編では，情報セキュリティの全般的な対策として，設備，運用，制度（保険，システム監査）の要点と我が国の実施状況を示すとともに，「セキュリティ核」モデルを解説している．第2編では，内外のコンピュータ犯罪の統計と事例研究を示し，そこから得られる教訓をもとにセキュリティ対策への指針を解説している．

第3編から第6編は通信情報の盗聴と改ざんを防ぐ技術的な対策として脚光を浴びている暗号に関するものである．特に，暗号解読の計算上の困難さに関する理論的研究の最新の成果，ディジタル署名への暗号の応用，暗号鍵管理法の実際，ISOでの暗号方式の標準化動向，および，暗号処理ハードウェアの開発状況について解説している．

第7編と第8編は蓄積情報のセキュリティを確保する主要技術であるアクセス制御に関するものである．特に，オペレーティングシステムにおけるセキュリティ制御の考え方，実現機構，具体的なシステム例と，データベース・マネジメントシステムにおけるアクセス制御，フロー制御，推論制御，および，ファイルの暗号化について解説している．

第9編と第10編は，個人の所有物や記憶内容でなく，個人の特性を利用した個人識別技術に関するものである．特に，声紋と筆跡，および，指紋と掌紋による個人識別技術を解説している．

ところで，今年の2月，多数の研究者，技術者が参加して，「暗号と情報セキュリティ技術研究会(CIS研究会)」が発足した．今後，ますます「情報セキュリティ」の研究と実用化が進むと思われる．本特集がこの分野の発展のために少しでも役立てば望外の喜びである．

最後にご多忙の中を，快く執筆を引受けてくださった執筆者の方々，ならびに，編集，査読にご協力いただいた方々に深く感謝いたします．

（昭和59年4月4日）

† 日本電信電話公社武蔵野電気通信研究所