特集「情報セキュリティの理論と応用」の編集にあたって

土　居　範　久†

1998 年に設立されたコンピュータセキュリティ研究会（CSEC）は，セキュリティ対策が重要性を増すなか，研究会，シンポジウムなどの活動を活発に行い，順調に会員数を増やしてきた．CSEC が主催し，1999 年 10 月に実施したコンピュータセキュリティシンポジウム（CSS'99）では，145 名の参加者があり，47 件の発表があった．

本号は CSEC が中心になり企画した最初の特集号である．32 件の投稿があり，内 23 件を採録とした．その内訳は，ネットワークセキュリティ関係が 5 件，暗号関係が 4 件，電子商取引関係が 3 件，認証関係が 3 件，匿名性関係が 3 件，アクセス制御関係が 3 件，情報隠蔽（いんぺい）関係が 1 件，プロトコル検証関係が 1 件であった．

全体として見た場合に，要素技術だけでなく，システム技術も扱われ，理論だけでなく応用も扱われているのが大きな特徴である．実際のセキュリティ対策の場で使われているシステムに関するものもある．これらは，CSEC の設立の段階から目指していたものであり，今後も目指すべきものであろう．今後は，ウイルス対策や，セキュリティポリシー，セキュリティ教育などに関する論文も期待したい．

最近の暗号や電子透かしなどのセキュリティ技術を用いた応用システムの増大や，不正アクセスやコンピュータウイルスによるセキュリティ被害の増加などにより，セキュリティ技術は社会にとってますます重要なものとなっていくだろう．セキュリティ研究に早い段階から携わっているものから見ると，セキュリティ技術者の数は，昔に比べてずいぶん多くなってきたと思う．しかし，その重要性から見てセキュリティ技術者人口のますますの増大が待たれる．情報処理学会にも関連のある技術分野は多く，いろいろな分野からの参加を期待している．

そのようななかで，日本のセキュリティ研究の黎明期から活躍され，名著「現代暗号理論」の著者でもある NTT の小山謙二氏がなくなられた．謹んで冥福をお祈りしたい．

最後になったが，限られた時間のなかで，多様な論文の査読を行い，出版にまでこぎつけることができたのは，査読者や編集委員，学会の担当者といった方々のご努力のおかげである．特に，村山優子編集委員（岩手県立大学）には取りまとめの中心になっていろいろな作業を行っていただいた．これら関係者の方々に深く感謝申し上げる．

[情報セキュリティの理論と応用] 特集編集委員会

- 編集長
  土居　範久（慶應義塾大学）
- 編集委員（50 音順）
  岩村　恵市（キヤノン）
  岡本　栄司（ウイスコンシン州立大学・東邦大学）
  菊池　浩明（東海大学）
  才所　敏明（東芝）
  櫻井　幸一（九州大学）
  坂本　弘章（ NTT データ）
  佐々木良一（日立製作所）
  寺田　真敏（日立製作所）
  中野　秀男（大阪市立大学）
  宮内　　宏（日本電気）

† 慶應義塾大学