A special issue of “Usable Security” has just been published. On behalf of the Editorial Board, I would like to express our gratitude.

This special issue was planned in the first half of 2019. The editorial board of 26 members was formed. The call for papers was opened in October of the same year. 19 submissions were received after 5 months of the submission period, and 14 papers (including 3 in English) were finally accepted after 6 months of review and referral period. The acceptance rate was 74%.

The special issue on “Usable Security” was also planned and published last year. We can consider that the usable security research in Japan has reached a certain maturity level because of the high quality of the papers submitted in the previous issue. Considering the thrusts of increasing sophistication and society’s growing demands, this special issue is named after the same title, “Usable Security.”

We call for papers on usable security technology and privacy protection technology considering human use in this special issue. The security is based on information security and also includes privacy protection.

The research group on Security Psychology and Trust (SPT), the parent organization of this special issue, has been continuously presenting research papers and holding workshops on usable security since 2017. In this special issue, the call for papers’ scope is flexible because we do not consider usable security as a fixed field, but as something that will be established by the authors, the readers, and future researchers. The scope of the call for papers includes research that analyzes and improves convenience and efficiency in the fields of network security, computer security, and data privacy; research on operational research; research on cyber-attack methods that take advantage of human use and countermeasures; research on error occurrence; and research on ethics and obtaining user consent. In this special issue, in addition to research papers, we have organized the so-called Systematization of Knowledge (SoK) papers to evaluate and systematize existing research, provide new insights, and reappraisals into existing research areas and new taxonomies, as well as research methods and evaluation methods in our field. SoK papers were evaluated according to a different peer-review policy than the usual research papers.

In the peer-review process, we emphasized our policy of “Do not throw away gems even if you can pick up stones (Do not reject good papers even if you can pick up bad papers)” and spent much time in the editorial committee to discuss carefully to expand the base of research on security and privacy in the first review. On the other hand, in the second review, we adopted an editorial policy to ensure the quality of the accepted papers. We appreciate the reviewers’ hard work, and we believe that their hard work has resulted in an acceptance rate of 74%.

Among the papers accepted, four papers that analyze user behavior and attitudes in detail and clarify their characteristics were the most common characteristics of this special issue. The research areas covered by each of the papers include machine learning, system analysis, system design, authentication, and malware classification. It reflects the importance of the connection between human use and security technology and its base’s breadth. This special issue is having the effect that this feature aimed for. We also note that one SoK paper, which was a new trial, was also accepted.

The deadline for the submission was before the significant impact of COVID-19 in Japan. The behavioral characteristics of users change in response to changes in the social background. These behavioral characteristics are essential from the perspective of human usage, which is essential for usable security. The papers in this special issue may have different meanings in the new society affected by COVID-19 and the new society that has to coexist with it, as the papers in this special issue reflect the pre-COVID-19 era. It is vital to make use of this research as an opportunity to investigate further whether these user perspectives are acceptable without changing. There will be a societal demand for continued research to bridge the gap between human use and security and privacy technologies.

Finally, we would like to thank the members of the Editorial Board of IPSJ Transactions and SPT Research Group for the opportunity to present this issue of the journal, the editorial board members for their sincere discussions on the journal and their careful reviewing, and the reviewers for their support of the authors. We sincerely hope that this special issue will improve the security technology of computer systems in society and bridge the gap between human use and security and privacy technologies.

The Editorial Committee

- **Editor in-Chief:**
  Akira Kanaoka (Toho University)

- **Editorial Board Members:**
  Masaki Shimaoka (SECOM)
  Sachiko Kanamori (National Institute of Information and Communications Technology)
Editorial Committee Members:
Masatsugu Ichino (University of Electro-Communications)
Atsuo Inomata (Osaka University)
Midori Inaba (Institute of Information Security)
Tetsutaro Uehara (Ritsumeikan University)
Satoshi Ozahata (University of Electro-Communications)
Ayako Komatsu (University of Nagasaki)
Hidehito Gomi (Yahoo Japan)
Yuichi Komano (Toshiba)
Takahiro Sakamoto (DataSign)
Masue Shiba (Toshiba)
Yoshiaki Shiraishi (Kobe University)
Tetsuji Takada (University of Electro-Communications)
Katsumi Takahashi (NTT Secure Platform Laboratories)
Kenji Tanaka (University of Electro-Communications)
Yukiyasu Tsunoo (Tokyo Online University)
Masato Terada (Hitachi)
Masakatsu Nishigaki (Shizuoka University)
Takashi Hatashima (NTT Secure Platform Laboratories)
Kanta Matsuura (The University of Tokyo)
Daisuke Miyamoto (The University of Tokyo)
Yuko Murayama (Tsuda College)
Koichi Mouri (Ritsumeikan University)
Akira Yamada (KDDI Research)