

はじめに

情報メディアセンター所長 松井 吉光

情報メディアセンター紀要COMの第42号をお届けいたします。寄稿していただいた皆様にお礼を申し上げますとともに、より多くの方々にお読みいただけることを希望いたします。今号は幸いにして、締め切りの段階で6本の寄稿の申し込みがあり、追加募集することもなく発行することができました。3号連続して、寄稿の申し込みが少ない状態でしたので、紀要の存続が危ぶまれましたが、これで一安心といったところですが、今後もこういった状況が続くことを期待しています。

さて、今号の巻頭においても前号と同様、ICT環境、サイバー空間におけるトラブルについて触れさせていただきます。サイバー戦争の時代といわれ、従来のいわゆるハッカー集団だけでなく国家が積極的に関与し、主に国家機関やインフラ企業、軍事企業などのコンピュータが日常的攻撃に晒されている状況になっています。また、その一方で、近年、IoT(Internet of Things)技術即ち、少し前はユビキタスと言っていたと記憶していますが、コンピュータやスマートフォンのような情報機器だけでなく、あらゆる電化製品をネットワークつないで利用する技術が注目され、実用化されつつあります。この二つの事項が一見関係なさそうに見えるかも知れませんが、実はとても密接関連していて、パーソナルコンピュータや家庭用のルーターだけでなく、IoT技術が使われているテレビやビデオまでもが、DDoS(Distributed Denial of Service attack, 分散型サービス妨害攻撃)の踏み台として利用され、サイバー戦争に一役を買っているといます。これまでコンピュータやスマートフォンなどのセキュリティ対策ばかりいわれていましたが、これからはインターネットに接続する機器すべてについてのセキュリティ対策が欠かせなくなってくると言えます。

もちろん、これまで以上にコンピュータやスマートフォンのセキュリティ対策を強化していくことも不可欠です。サイバー戦争の踏み台もしくは、情報の不正取得に関わるマルウェアは、感染しても表だった行動はせず、バックグラウンドで静かに活動をします。これを防ぐもしくは、感染に気づくにはセキュリティ対策ソフトの導入は欠かせません。しかし、絶えず進化するマルウェアに対してはそれだけでは十分とは言えない状況になってきています。これからは、LANからインターネットへの出口にも、ネットワークを監視する機器を設置し、怪しい通信がないか絶えず監視すること、また後からログを見ることでどれだけの情報が漏れたかが分かるようにしておくこと

も必要になってきているのではないかと思います。

最後になりましたが、皆様のおかげをもちまして、2016年9月30日以後メディアセンター所長の第1期目の任期を無事終えることができました。至らないことなど色々あったかと思いますが、ご容赦いただきたく存じます。引き続き、2016年10月1日以降もメディアセンター所長の任を務めさせていただくことになりました。1期目の反省を活かしながら、ICT委員会の皆さんと事務スタッフの皆さんの協力を得ながら任務を果たしていきたいと思っています。どうぞよろしく願いいたします。