

特集にあたって

片岡 靖詞 (防衛大学校)

平成の30年間は大規模な災害が多かった。その度に「ライフライン」という言葉を耳にした。元々は、電気・ガス・水道を意味したが、現代社会において「情報」もまた人々が安心して暮らしていくために必要不可欠なライフラインと言えよう。しかも、情報というライフラインは受手専用ではない。今や手のひらに収まるスマホから、誰もが情報を発信することも可能である。しかも、その範囲は水源地・発電所から家庭間ではなく、世界全体である。

しかしながら、世界とつながるといことは便利さをもたらすだけではない。ネットワークを通じて、世界の見知らぬところから、どのコンピュータにもアクセスが可能で、悪意があればシステムを破壊したり、重要な秘密を盗んだりすることも可能である。さらに厄介なことには、情報は分子式などで表されるような物質と違い、重さや形もない。そして形跡が残らない破壊、モノがなくならない窃盗、変化に気づかない改ざん…この得体の知れぬ魔物が「まもる」対象である。

今回の特集は、「社会を『まもる』」であるが、守ると言えば防衛…こじつけ感もするが、筆頭著者は全員が防衛大学校情報工学科の教官陣である。お互いに毎日、廊下でもトイレでも、何度も顔を見る同僚たちである。こんな片寄った執筆陣で許さるのかという気がするが、この特集にとってはうってつけの執筆陣であろう。

まずは、田中秀磨氏の「混合整数計画法を用いた暗号の安全性評価」では、ブロック暗号のIntegral攻撃に対する安全性評価を明確にし、そこに整数計画法を適用することでより正確な評価を達成した話をしていただいた。次の渡辺宏太郎氏らの「ボトムアップ型視覚暗号の数理計画法による構成」であるが、視覚暗号とは秘密情報を画像として分散化する手法である。その画像構成に数理計画を用いる手法について解説していただいた。

この2編のテーマは暗号の評価や開発であるが、手法として数理計画ソルバを用いていることが本誌読者としては興味深いのではなからうか。これまでの研究発表会における数理計画絡みのセッションでは、このような研究題材はあまり見られないが、これらの記事

が数理計画法の新たな適用分野を広げる端緒となってもらえるとありがたい。

余談であるが、筆者自身も最近は誤り訂正符号の復号に数理計画技法を適用する研究に浸っている。なかなか通信分野と最適化分野の両方に精通している人が少ないのが残念ではあるが、両分野にとって刺激的な未開拓の研究題材が多々あるのではないかと思っている。

続いて、三村守氏の「サイバー攻撃のアトリビューションのための統計学的アプローチ」であるが、この方は元自衛官であり、自衛隊の現場におけるサーバー攻撃などを何度も見てきており、その調査・追跡を手がけてきた経験抱負な方である。最新の防衛計画の大綱(30大綱)でも「宇宙・サイバー・電磁波などの新たな領域への対応施策」が強調されており、まさに(情報における)安全保障の最新対応施策について解説いただいた。

最後の2編は、実態があり目に見える物理的な攻撃や災害に対して「まもる・助ける」研究紹介である。宝崎隆祐氏の「警備ゲームの動向」では、警備ゲームを単にネットワーク上でのモデルではなく、テロ犯の性格や特徴までもモデルに組み込もうとしている。先の三村氏の記事にもプロファイリングなどの刑事ドラマで聞く用語も出てくるが、やはり「まもる」ためには「せめる」側の特徴も重要な考慮要因である。

岩切宗利氏は、阪神・淡路大震災のときには伊丹駐屯地から災害派遣に駆けつけた経験ももっており、情報の錯綜による救助の困難さを、文字どおり身体でわかっている。「撮影時点の異なる空撮画像の差分による災害状況推」であるが、空撮資料だけから建物の倒壊状況の大小を抽出する手法とその重要性は、災害派遣・救助経験者ならではの説得力を感じる。

出典は忘れたが、世界最速の乗り物を開発するためには、その陰で高性能なブレーキの開発が必須であるという趣旨の文章を読んだことがある。花形である動力の研究と違い、ブレーキの研究は素朴に映るかもしれない。だが、その素朴で万が一のための研究が、ますます便利になっていく社会においてわれわれを「まもり」、平和で安全な暮らしを支えているのだと思う。