特 集

増加する社会インフラを標的としたサイバー攻撃

編集にあたって

松本　尭　（株）三菱総合研究所
松崎和賢　技術研究組合制御システムセキュリティセンター

社会インフラを構成する産業制御システムや情報システムへのサイバー攻撃が世界各地で急増している．2010 年に発覚したイランのウラン濃縮施設へのサイバー攻撃では，ウラン濃縮に使われる遠心分離機が稼働不能になった．2013 年 3 月には隣国韓国でも大規模なサイバー攻撃が発生し，銀行の ATM や決済がサイバー攻撃により一時停止するなどの事態に陥っている．サイバー攻撃というと，官公庁や大手企業の Web サイトの改ざんやサーバダウン，企業の持つ機密情報や個人情報の漏えいといったことを思い浮かべるかもしれない．しかしながら，水道が止まる，鉄道が止まる，ATM が止まる，といった人々の生活や経済活動に重大な支障をきたすようなサイバー攻撃の脅威が高まりつつある．

そのような状況下，社会インフラの安全・安心を確保するためのサイバーセキュリティ技術の研究開発やサイバーセキュリティにかかわる人材育成・普及啓発活動が注目されつつあり，2012 年には技術研究組合制御システムセキュリティセンター（CSSC）[☆1] が民間企業や官公庁，大学の参加により立ち上げられるなど，産学官一体となって取り組みが進められている．

そこで，本特集では，国民の生活を支える社会インフラへのサイバー攻撃の現状，さらにサイバー攻撃に対応するための研究開発や評価認証等の取り組みについて，各分野の第一線で活躍されている皆様に執筆をお願いした．

まず，「**1．社会インフラへのサイバー攻撃に対する課題と取り組み（新）**」で，社会インフラへのサイバー攻撃が起こり得るようになった背景と，その対策をするにあたっての基本的な考え方について解説いただいた．

さらに，それでもまだ社会インフラへのサイバー

☆1　組合員数は 23 社（2014 年 4 月現在）．

攻撃の現実性について実感が湧かない読者に向けて，「**2．産業制御システムへのサイバー攻撃手法の特徴と対策（原）**」では，実際にどのような攻撃が行われているのか，どれくらい危険があるのか，という点について，実態調査の結果を紹介していただき，具体的な対策のポイントについて論じていただいた．

背景と現状に続いて，以降の 3 記事では，研究開発，評価認証・標準化，人材育成・普及啓発の 3 つの観点から，社会インフラへのサイバー攻撃に対する取り組みについて解説していただいた．

研究開発という観点では，「**3．社会インフラの安心・安全を確保するためのセキュリティ技術の研究開発（鍛）**」で，社会インフラを構成するシステムの開発・保守，運用の各フェーズに対して，必要とされる技術と課題について解説いただき，課題に対してどのような研究開発が行われているか，ご紹介いただいた．

セキュリティ対策の推進を目的として，評価認証制度の確立や規格の策定も進められており，「**4．制御システムのセキュリティを対象とした評価・検証技術と標準化動向（小林）**」では，評価認証・標準化という観点から，取り組みと動向について解説いただいた．

「**5．サイバー攻撃に備えた実践的演習（江連）**」では，普及啓発・人材育成という観点で，米国や日本で行われているサイバー攻撃に備えるための実践的な演習についてご紹介いただいた．セキュリティ対策では，人的な要因も大きく，サイバー攻撃を模擬的に実施し，その際の対応を確認する演習が有効である．

最後に，「**6．自動車や医療機器を対象とした新たなサイバー攻撃の脅威（中野）**」で，今後顕在し得る脅威として想定される，自動車や医療機器等へのサイバー攻撃とその対策について解説いただいた．スマートシティやあらゆるもののネットワーク化の進展に伴い，社会インフラの基盤のみでなく，自動車や医療機器といった社会インフラに繋がり得る機器にまで，その脅威は広がっていくと考えられる．

2020 年には東京五輪が開催される．ロンドン五輪もサイバー攻撃の標的とされていたことが後から判明しており，2020 年に向けて，多くの企業や大学，政府などが連携し，社会インフラへのサイバー攻撃対策について，取り組みを加速させていく必要がある．本特集が，その一助となれば幸いである．最後に，本特集の企画にご協力いただいた方々，記事執筆者の方々に深く感謝する．（2014 年 4 月 15 日）