情報セキュリティ　特集号

「情報セキュリティ」特集にあたって

後藤厚宏†

我々の日常生活や経済活動は，通信・放送，エネルギ，交通など，様々な社会インフラによって支えられており，その機能，サービス等を実現するために多数の情報通信システムが運用されている．例えば，利用者に社会インフラサービスの利便性を提供するために，サービス状況の通知など，インターネットを活用した様々な付加サービスが提供されるようになってきた．さらに，全国をカバーする大規模な社会インフラから，工場内の生産設備まで，それらを構成する機器・設備は，制御用のネットワークを介して運用・監視センタ―等に接続され，効率的な運用・保守が実現されている．

一方，インターネットの普及は，人々の生活や産業界に大きなメリットをもたらしたが，同時にサイバー攻撃という新たな脅威の出現を招き，今や我々の社会経済を支えるインフラシステムへのサイバー攻撃の脅威が現実のものとなっている．インターネットに接続している業務ネットワークだけでなく，通常，インターネットとの接続を持たない制御用のネットワークであっても，サイバー攻撃の脅威は高まっている．なぜならインフラシステムの遠隔保守やオンサイト保守における内部犯行のリスクまで想定すると，制御ネットワークも完全な閉域環境とはなりえないためである．

今や個人情報の漏えい，Web サイトの改ざん，大規模な業務妨害など，サイバー攻撃の実例は枚挙にいとまがない．また，最近では，特定の組織が保有する機密情報や資産に狙いを定め，巧妙な手口により執拗に攻撃を繰り返す標的型攻撃が増えている．さらには，社会インフラを構成する組み込み機器や制御システムが利便性・保守性向上などの目的でネットワーク化される傾向にあり，ひとたびそのネットワークに攻撃者が侵入すれば，大規模かつ深刻な事態を招くことが容易に想像できる．

このように，社会インフラシステムの情報セキュリティ対策は我が国のみならず全世界的に急務と言える．特に，2020 年東京オリンピック・パラリンピック競技大会を迎える我が国にとって，強固な情報セキュリティの確保による世界で最も安全・安心な社会基盤の確立は最重要課題と言えよう．

本特集では，安全な社会インフラシステムの実現にとって必須となった情報セキュリティ*の確保に向けて，現状の課題を技術的要素，人間的要素，社会経済的要素から幅広く議論する．

最初に，現代社会の「社会インフラにおけるサイバーセキュリティ課題の全体像（総論として）」，「電力・交通網へのサイバー攻撃」，「サイバーインシデントの最新動向」で我が国が直面するサイバーセキュリティ課題について概観する．続いて，プラント等の制御システム，自動車，医療の各分野におけるセキュリティ脅威と対策について詳説する．

次に，技術的観点から，システムの設計・開発における，安全とセキュリティへの取組みと標準化動向について制御システムとスマートメータ，組込み機器，要求工学の観点から論じたのち，技術的要素と人間的要素の関わりについて，セキュリティと使いやすさ，および，インターネットブラウザの安全表示について解説する．続いて，情報セキュリティの社会科学的側面から分析し，「安全」を脅かす企業不正について考察する．

対象を拡大し変化を続けるサイバー攻撃に対応し，被害の防止や最小化を図るには，相応のスキルを身につけた多数のセキュリティ人材が必要となる．本特集では，大学連携によるセキュリティ人材の取組（enPiT-Security）について紹介し，本特集の最後として，我が国のサイバーセキュリティ戦略について概説する．

今後，自動走行などの将来型交通システムや広域医療システムにおいて注目される IoT（Internet of Things）システムを活用して経済の活力を向上させようとする時代を迎え，社会インフラシステムにおいても，これまでにない多種多様な機器等がネットワークで接続されることが予想される．本特集が，情報セキュリティの確保の観点で，我々の社会生活や経済活動の「安全」に向けて役立つことを期待する．

† 情報セキュリティ大学院大学 情報セキュリティ研究科：
〒 221-0835 神奈川県横浜市神奈川区鶴屋町 2-14-1
E-mail：goto@iisec.ac.jp

＊ 本特集では，情報セキュリティとサイバーセキュリティをほぼ同義で用いることとする．