特集
Special Feature

新たなモビリティ時代のサイバーセキュリティ
―セキュリティによるジャパン・ブランドの向上に向けて―

編集にあたって

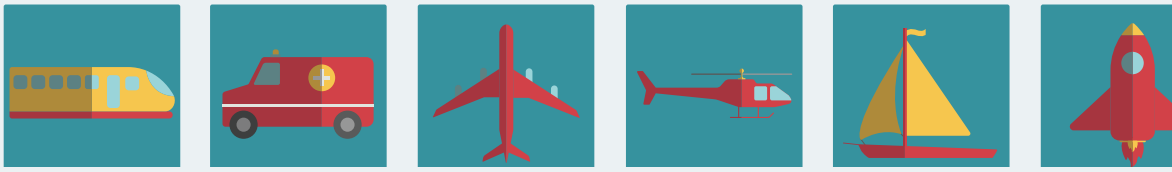
石黒正揮 (株) 三菱総合研究所　新　誠一 電気通信大学
佐々木貴之 日本電気 (株)

ディジタル化とネットワーク化の波が自動車，鉄道などのモビリティ分野にも大きな変革をもたらしている．自動車分野では，自動運転，コネクテッドサービス，シェアリングサービス，電動化など，100年に一度と言われる変革（CASE革命）が進行し産業構造が激変している．鉄道分野においては，無線式列車制御システム等により列車の位置や状態をリアルタイムで把握・予測することで安全性の確保やダイヤの乱れを迅速に回復するシステムが開発されている．このようなモビリティ分野の変革の一方で，システムが攻撃を受けた場合，生命・身体の安全にかかわる重大な事故につながる可能性があり，危機感が高まっている．実際，自動車，鉄道，航空などの分野で，セキュリティ事故や脆弱性の問題が顕在化している．このようなことから各分野では，セキュリティ基準やガイドラインの策定が急速に進められている．モビリティ分野は，安全性を前提として成り立つ分野であるためセキュリティに対する信頼は，企業の競争力やビジネスに直結する重要な課題である．日本は，自動車の品質，新幹線をはじめとした鉄道の安全性など国際的に高い技術力を確保しているが，新たなセキュリティ脅威に対して，従来産業とIT・セキュリティ産業が連携することでセキュリティを強化し，国際的な説明責任を向上させることができれば，これまでの日本の強みに加えて，ジャパン・ブランドを一層向上させることができる．このような視点から本特集では，各分野のセキュリティ脅威とその対策に関する動向および将来の課題展望についてまとめることを目的とした．サイバーセキュリティは産官学の連携による包括的な取り組みが不可欠であることから，本特集では，産官学の協力を得て，モビリティ分野のセキュリティについて知見の深い専門家によりまとめた．

本特集の構成は以下のようになっている．

(1) 自動車セキュリティの国際標準等の動向と今後の課題

「編集にあたって」のとりまとめを担当した三菱総合研究所 石黒正揮が，自動車のサイバーセキュリティに関する国際標準，政策動向等に基づく今後の取り組み課題について解説した．自動車分野の



CASE 革命に伴い，セキュリティ脅威が高まっており，国連機関 WP29 によるサイバーセキュリティ基準（案）および ISO/SAE21434 サイバーセキュリティ国際標準の策定が進められている．これらの国際基準等は，各国の強制基準である型式認証に反映されることが見込まれるため，関連企業にとって影響が大きい．自動運転にかかわるセキュリティ・フレームワーク等にいち早く対応しセキュリティ・ブランドを向上させることで，国際競争力の高い自動車産業のジャパン・ブランドをさらに強化することが期待される．

(2) 自動車分野の CASE 革命とサイバーセキュリティ

名古屋大学名古屋大学大学院情報学研究科 松原豊氏，倉地　亮氏，高田広章氏によりコネクテッド，自動運転，シェアリング，EV ごとに技術トレンドとセキュリティの脅威についてまとめ，それらに対する取り組みと今後の展望について解説した．新たな脅威が見つかることを前提に運用・保守を含むライフサイクル全体のディペンダビリティを維持する考え方の重要性を指摘している．

(3) 鉄道における列車の運行制御用情報ネットワークとサイバーセキュリティ

運輸総合研究所 信号・情報技術研究部 川崎邦弘氏，祇園昭宏氏が，鉄道分野の ICT 活用の状況を概観したのち，安全かつ安定した列車運行の実現に向けて不可欠となるサイバーセキュリティについて，鉄道関連の規格等の現状と考慮すべき事項等について概説している．また，今後の重要課題として，安全を最優先に確保しつつ，サービスレベルの低下を最低限にする（＝できるだけ運行し続ける）ための仕組み・対策の構築を挙げている．

(4) 航空分野のサイバーセキュリティ

情報セキュリティ大学院大学 大久保隆夫氏が航空分野のセキュリティ事故事例や航空システムの構成に基づき潜在的な脅威を洗い出し，それを踏まえて，航空分野等のセキュリティ人材育成にフォーカスした取り組みと今後の課題をまとめていただいた．今後，航空分野においては，セキュリティ情報の共有を行う組織の整備・活用により，運用だけでなく安全な航空システムの構築を含めた対策・人材育成を課題に挙げている．

(5) 海事産業におけるサイバーセキュリティ対策動向

東京大学大学院新領域創成科学研究科 稗方和夫氏が，造船・海運業を中心としたステークホルダの概略と情報通信技術導入の現状について触れ，国際機関や業界団体からのサイバーセキュリティ対策ガイドラインの公表の状況，今後の動向やサイバーセキュリティの産業実装の見通しについて，国際および国内の動向をまとめた．今後の海事産業においては，新造船の特に OT 要素がサイバーレジリアント（設計においてサイバーセキュリティ耐性を実現）であることを要求されることが予想され，その対応はシステムインテグレータとしての造船所が担う範囲になる．

(6) ドローンのセキュリティ

セキュアドローン協議会 春原久徳氏，田上利博氏が，ドローンの活用分野とセキュリティに関する脅威と対策に関する取り組み動向，課題についてまとめている．規制緩和により 5G 搭載ドローンの可能性が開かれ，直接クラウドと連携することで新たな応用が広がるとともに，リスクの変化にも対応できるセキュリティの重要性を指摘している．

自動車，鉄道，航空機などさまざまな交通手段をシームレスに連携させてサービスとして移動手段を提供する MaaS（Mobility as a Services）については，2020 年から 2030 年までの 10 年間に 30 倍の市場になると言われるが，本特集であまり取り上げることはできなかった．MaaS についてはサイバーセキュリティに関する取り組みが進展した時点で特集したい．

本特集で紹介したサイバーセキュリティに関する産官学の包括的な取り組み課題が，日本の産業競争力をさらに強化しブランド力を向上させることに寄与することを期待したい．

（2020 年 1 月 27 日）