

デジタルエコノミー時代の サイバーセキュリティ —デジタルトランスフォーメーション 促進の基盤確立に向けて—

編集にあたって

石黒正揮 | (株) 三菱総合研究所 細野 繁 | 日本電気 (株) 手塚 悟 | 慶應義塾大学

産業、経済、社会のさまざまな領域で進展するデジタル化によるビジネスモデルの変革（デジタルトランスフォーメーション）は新たな価値を生み出す一方で、新たなセキュリティの脅威や問題をもたらしている。

今日のデジタル化の潮流は、ビジネス構造の変革を伴うもので、数十年前から始まった従来のIT化の流れとは一線を画している。実世界の機器などからなるフィジカル空間と情報システムやインターネットなどからなるサイバー空間がデータ連携により融合し、異なる分野の組合せによるイノベーションを誘発している。また、業界の枠内でのデジタル化にとどまらず、ベンチャーや他業界など従来の業界の枠を越えた連携・協業によるサプライチェーン・エコシステムの拡大が進んでいる。

さまざまな機器がネットワークに繋がることでシステム的な攻撃ポイントが増えるとともに、サプライチェーン・エコシステムの拡大に伴い組織的に脆弱なポイントが増え、システムと組織の両面でセキュリティのリスクが高まっている。

このようなことから、本特集では、サイバーとフィジカルが融合する新しいデジタルエコノミーの進

展に伴い、従来のサイバーセキュリティでは対応できない脅威や課題について取り上げ、それらに対する取り組みや今後の方向性について展望する。

本特集内の「サイバーセキュリティ経済学—インセンティブの適正化を通じたサイバーセキュリティの確保—」でも示す通り、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、インダストリ（産）、ガバメント（官）、アカデミア（学）のステークホルダの協力を得てとりまとめることとした。

本特集の構成は以下のようにになっている。

(1) デジタル化とデータ活用により進化する社会インフラセキュリティ

宮尾健氏、谷本順一氏により、データ活用にかかわる社会インフラ（インフラストラクチャ）の脅威とセキュリティ対策の方向性を取り上げていただいた。製造機器や情報システムが繋がることで進化するサイバーフィジカルシステムにおける脅威に対して、サイバーBCP（事業継続性計画）のうち技術面に焦点を当て、アセット管理とデジタルエビデンスと呼ばれる対策を挙げ、サプライチェーンを構成する組織群や社会全体のニーズと課題を整理している。

(2) 国際連携を踏まえたトラストサービスとトラスト基盤

手塚悟により、超スマート社会 (Society 5.0) における信頼の連鎖の確保について取り上げた。サプライチェーンにおいて生まれるさまざまなサービスの安全性を保証するための技術として、「トラストサービス」と「トラスト基盤」の重要性を挙げている。また、米国、EUにおける関連する取り組みを概観し、国際連携の重要性を示している。

(3) サプライチェーンサイバーセキュリティの強化に向けて—サイバー・フィジカル・セキュリティ対策フレームワークの策定—

奥家敏和氏にサイバーフィジカルセキュリティ対策フレームワークについて解説いただいた。異分野間のシステム連携・協調が進む中で、製品・サービスを生み出す工程 (サプライチェーン) の変化と脅威について取り上げ、「企業間のつながり」を捉える第1層、「フィジカル空間とサイバー空間のつながり」を捉える第2層、そして「サイバー空間におけるつながり」を捉える第3層という3つの層に分けたフレームワークとしてセキュリティ対策の指針を示している。

(4) IoT 機器の普及とサイバーセキュリティ政策

谷脇康彦氏にIoT機器にかかわるサイバーセキュリティ政策について執筆いただいた。データがリアル空間とサイバー空間を循環しながら社会課題の解決につなげていくデータ主導社会において、リアル空間において急激に増加する多様なIoT機器のセキュリティ水準を引き上げるボトムアップアプローチや機器間でリスクが波及するリスクの連鎖を回避する仕組みについての政策を解説いただいた。

(5) フィンテックのセキュリティ

岩下直行氏にフィンテックにかかわるセキュリ

ティの問題認識についてまとめていただいた。従来の伝統的金融の枠組みを越えて進展するフィンテックのうち、仮想通貨のセキュリティ事故を経て、金融機関のシステムとセキュリティに対するスタンスと管理体制について問題を提起している。

(6) AI をセキュリティリスクから守るために—AI へのサイバー攻撃とその対策—

古澤一憲氏にAIにかかわるセキュリティの新たな課題と対策の方向性についてまとめていただいた。AIの有用性が示される一方で、悪意を持った攻撃を受けた場合には一転して大きな危険にさらされる可能性がある。AIのリスクに関する内外の議論を紹介するとともに、AI特有のサイバー攻撃手法を分類し、それらに対する対策の考え方やアプローチについてまとめている。

(7) サイバーセキュリティ経済学—インセンティブの適正化を通じたサイバーセキュリティの確保—

石黒正揮が、サイバーセキュリティ対策投資にかかわる問題と取り組みアプローチについて解説した。サイバーセキュリティ分野においては、技術だけでは解決できない、インセンティブにかかわる本質的な問題がある。その問題に対するアプローチとして、経済メカニズム、人の行動モデルなどの観点から問題の解決を目指すサイバーセキュリティ経済学について解説し、今後の展望を示す。

本特集で紹介したサイバーセキュリティに関する包括的な取り組みが、サイバー空間とリアル空間が融合する異業種連携におけるセキュリティと安全性を確保し、デジタルトランスフォーメーションを促進することを期待したい。

(2018年9月24日)