サイバーセキュリティー

NIS指令でセキュリティー強化を促す

ジェトロ海外調査部欧州ロシアCIS課　　我妻　真

欧州委員会（以下、欧州委）は2016年7月6日、「ネットワークと情報システムのセキュリティーに関する指令」（NIS指令）を採択し、同年8月8日に発効させた。18年5月25日に迫ったEUの一般データ保護規則（GDPR）適用開始に備えて、EU加盟国は同年5月9日までにNIS指令の国内法制化も求められている。

デジタルサービス提供者も対象に

欧州委は、サイバーセキュリティー（本誌p.40を参照）に対する初の取り組みとして、2013年2月に「EUサイバーセキュリティー戦略」を発表した。「開放され、安全で、保護されたサイバー空間」が欧州の自由と民主主義の価値をさらに高め、デジタル経済を安全に成長させるとしている。サイバー妨害や攻撃への対応についての取り組みを定めたものだ。

この戦略をさらに詳細にし、加盟国に具体的な行動を求めるのがNIS指令だ。同指令の要旨は下記の3点にある。①加盟国のNIS機関や情報セキュリティー・インシデント・チーム（CSIRT）などを通じたサイバーセキュリティーの能力の向上、②加盟国間の戦略的協力と情報交換体制の整備、③経済や社会に重要なサービス（エネルギー、交通、水、金融、医療など）提供者と、検索エンジン、クラウドコンピューティング、電子商取引などのデジタルサービス提供者（DSP）に適切なセキュリティー対策を講じさせ、サービスに重大な影響を与えるインシデント（情報セキュリティーが脅かされ重大事故につながる恐れがあった事例）の報告を義務付けること。

同指令は、EU域内に本社を構えるDSPのみならず、域外から域内にサービスを提供するDSPも対象とする。加盟国単位では、サイバーセキュリティーの国家戦略を策定し、指令適用状況の監視のための所管当局を設立すること、国家レベルのCSIRTを持つこと、が求められる。さらに、加盟国間のCSIRTのネットワークを構築することも明記されている。

NIS指令採択の発表の席で欧州委のギュンター・エッティンガー委員（デジタル経済・社会担当、当時）は、サイバーセキュリティー関連産業における官民パートナーシップ（PPP）事業に18億ユーロの投資をすることを発表した。官民プレーヤーの国境を越えた研究開発協力を促進するためだ。

IoTの急成長がリスク増大を招く

過去20年でインターネット、広義のサイバー空間は、社会のあらゆる分野に非常に大きな影響をもたらすようになり、欧州の市民や企業はデジタル社会におけるセキュリティーに関する課題に直面している。

欧州では、情報通信技術（ICT）関連のセキュリティー製品の規格やサービスの提供方法が国や地域によって異なる。このため、セキュリティー関連企業、特に中小企業は、欧州でも世界でも競争することが困難な状況となっている。

また、サイバーセキュリティーの専門家の不足も指摘される。欧州委の報告書によると、サイバーセキュリティー関連の労働力需要は19年には世界で600万人が見込まれ、100万～150万人不足するとみられている。この状況はEU域内でも同様であり、人材の育成も必要だ。

社会のITソリューションへの依存度の高まりや、現在のインフラと将来のインフラ（例えば、スマートシティー、スマートカー、スマートグリッド）の相互依存性が増加することで、デジタル社会の脆弱（ぜいじゃく）性が増幅されている。加えて、IoT（モノのインターネット）の発展により、インターネットに接続される機器が増え、脅威や混乱が引き起こされる可能性が広がっている。つまりサイバーセキュリティーの脅威が増しているのだ。リスクを軽減する取り組みは、欧州のみならず各国で急務となっている。