G7 財務大臣・中央銀行総裁
プレスリリース（仮訳）

ワシントン D.C.
2017 年 10 月

サイバーインシデントはますます規模が拡大し巧妙化している。このため、金融セクターにおけるサイバーセキュリティの改善は、G7 諸国の重要な課題である。G7 サイバー・エキスパート・グループ（CEG）は、メンバー間の協調を促進し、金融セクターにおけるサイバーセキュリティに関する G7 のベストプラクティスの策定を続けている。昨年、CEG は「金融セクターのサイバーセキュリティに関する基礎的要素」を公表した。これは、金融セクターの民間・公的主体のサイバーセキュリティにおける効果的なプラクティスを包含するノンバインディングな要素である。

本日、「金融セクターのサイバーセキュリティの効果的な評価に関する基礎的要素」を公表する。本「基礎的要素」では、サイバーセキュリティのグッドプラクティスによりもたらされる特徴（Outcomes）を示している。具体的には、組織的な意思決定にサイバーセキュリティの視点が組込まれていること、技術的な disruption が発生し得るものであるということが認識されていること、絶えず変化するサイバーリスクに柔軟に対応すること、サイバーセキュリティの良好な組織文化があることが含まれる。

また、本「基礎的要素」では、各組織が自身のサイバーセキュリティを評価する際に用いるための、子細（prescriptive）ではなく俯瞰的な 5 つの評価要素についても説明している。具体的には、（1）明確なサイバー評価目的の設定、（2）測定可能な期待値の設定、（3）多様なツールの活用、（4）明確な結果報告・改善措置、（5）評価の信頼性・公平性の確保が含まれる。

本「基礎的要素」は、法的拘束力はないが、サイバーセキュリティの評価のための有効なプラクティスがどのようなものかについて、G7 としての見方を明確に示しており、金融機関にも当局にも適用可能である。また、本「基礎的要素」は、様々な国で対応できるよう、また規模や対策レベルの異なる企業にも対応できるように設計されている。

2017 年 5 月のバーリ・コミュニケにもあるとおり、CEG は、サードパーティーリスクおよびセクターをまたぐ協調に関する作業を継続する。加えて、脅威に基づくペネトレーションテスト（threat-led penetration testing）に関する基礎的要素の策定、および G7 の金融当局を対象にしたクロスボーダーのサイバー模擬演習にかかる提案を行う予定である。