G7 財務大臣・中央銀行総裁
国際的な金融セクターのサイバーレジリエンス強化に向けた次のステップ
背景説明（仮訳）
2018 年 10 月

金融セクターにおけるサイバーレジリエンス（サイバー攻撃への耐性やダメージからの回復）の改善は、引き続き G7 諸国の優先事項である。G7 サイバー・エキスパート・グループ（CEG）は、G7 財務大臣・中央銀行総裁によるメンバー間の協調の促進および金融セクターにおけるサイバーレジリエンス向上のための有効なプラクティスについての G7 の見解の策定に向けた取り組みを継続的に支援している。

昨年、G7 財務大臣・中央銀行総裁は、「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」を公表した。これは、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）を提供するとともに、子細にわたるものではなく（non-prescriptive）、法的拘束力もない、各組織が自身のサイバーセキュリティを評価する際に活用するための俯瞰的な要素を提供している。これらの基礎的要素は、脅威ベースのペネトレーションテストや金融セクターにおけるサードパーティのサイバーリスクマネジメントの有効なプラクティスを検討する際に、公的・民間金融機関にとって有益である。

本日、「脅威ベースのペネトレーションテストに関する基礎的要素」および「金融セクターにおけるサードパーティのサイバーリスクマネジメントに関する基礎的要素」を公表する。

「脅威ベースのペネトレーションテストに関する基礎的要素」は、疑似的な攻撃を活用することにより組織がサイバーインシデントに対するレジリエンスを評価するための指針を提供する。「脅威ベースのペネトレーションテストに関する基礎的要素」は、金融機関や当局がそのようなテストを企画、導入、管理する際に活用するための６つの中心的な要素を示している。これらには、(1) スコープ設定とリスクマネジメント、(2) リソース確保、(3) 脅威情報、(4) ペネトレーションテスト、(5) 完了および改善、(6) 類型化したデータが含まれる。

「サードパーティのサイバーリスクマネジメントに関する基礎的要素」は、サードパーティによって金融セクターにおける民間・公的金融機関にもたらされるサイバーリスクを管理するためのベストプラクティスを提供する。また、同「基礎的要素」は、組織がサードパーティのサイバーリスクマネジメントのプラクティスの一環として活用できる俯瞰的な要素を提示する。同「基礎的要素」は、金融機関や当局がサードパーティのサイバーリスクを管理するための６つの中心的な要素を示している。これらには、(1) ガバナンス、(2) サードパーティのサイバーリスクに対するリスクマネジメントプロセス、(3) インシデント対応、(4) コンティンジェンシープラン、(5) 潜在的なシステミックリスクのモニタリング、(6) セクターを跨る協調が含まれる。

将来を見据え、CEG は、金融セクターにおけるサイバーレジリエンスを促進する活動を担うことにより、G7 財務大臣・中央銀行総裁を引き続き支援する。これには、G7 の金融当局が参加するクロスボーダー演習を通じたサイバーインシデント対応や G7 金融当局と民間関係者の連携強化に向けて、状況認識力と協調を強化するためのさらなる取組みが含まれる。