EUで義務化されたTLPT（脅威ベースのペネトレーションテスト）

EUではDORA施行を契機として、大手金融機関による「脅威ベースのペネトレーションテスト（TLPT）」の実施が義務化された。金融機関はTLPT実施に向けて、情報統制体制の構築や信頼できる外部テスターの選定をはじめとする準備を進めていくことが求められた。

大手金融機関にサイバー攻撃への対応力評価を義務化

2025年1月にEUで施行されたデジタル・オペレーショナル・レジリエンス法（DORA）を機に、EUの大手金融機関は「脅威ベースのペネトレーションテスト（Threat Led Penetration Test, TLPT）」を3年ごとに実施することが義務化された。TLPTとは現実世界で実際に起きているサイバー攻撃をテスターが動的にシミュレーションし、防御側である金融機関が防御、検知、対応を行い、金融機関のサイバー攻撃対応態勢を評価し対応能力を高めることを目的としたテストである。脆弱性診断のようにシステム面を評価するだけでなく、組織体制や脆弱性への対応プロセスも評価する。

これまでEUにおけるTLPTは、一部の金融機関による自主的な取り組みにとどまっていた。その背景としてリソース面の課題がある。TLPTは脅威インテリジェンス策定からテスター選定まで、長期的な準備を要する。また、TLPTは本番環境での実施が原則のため、不測の事態が生じた際の顧客への影響を想定したリスク管理体制も必要だ。加えてテスト品質面の課題もある[1)]。

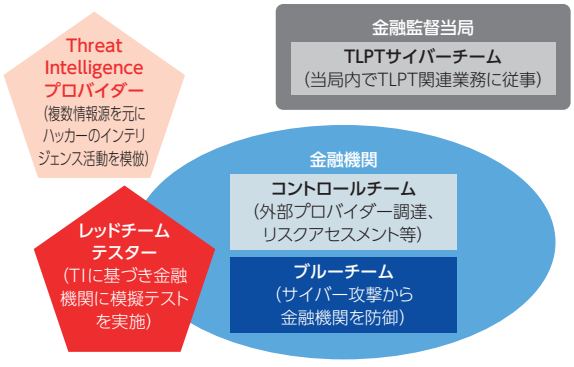
DORAを機に改訂されたTIBER-EUフレームワーク

DORAにおけるTLPTの規制技術標準との整合性をとる形で、TLPTのフレームワーク「TIBER-EU」が2025年2月に改訂された[2)]。当該フレームワークは2018年に欧州中央銀行が公表したもので、一部金融機関によって自主的に活用されてきた。TIBER-EUでは、当局のTLPT専門チームが監督的な立場で金融機関のTLPT実施に関与する[3)]。当局から通知を受けた金融機関は指定された期限内にTLPTの準備を開始する必要がある。

TIBER-EUのステークホルダーは、監督当局（TLPTサイバーチーム）、金融機関（コントロールチーム、ブルーチーム）、テスター（脅威インテリジェンスプロバイダー、レッドチームテスター）に大別される（図表1）。特に重要な役割を果たすのが金融機関のコントロールチームで当局とのコミュニケーションからテスターの選定、社内の情報制御までTLPTの全体管理を担う。

TIBER-EUでは準備、テスト、クロージャーまで1年以上を要する（図表2）。準備段階では、金融機関にとってクリティカルで重要な機能を特定した上でテスト範囲を定めることが求められる[4)]。レッドチームテストでは12週間にわたり複数シナリオのもとで金融機関の重要なシステムへの攻撃が試みられる。クロージャー段階では「パープルチーミング」が新たに義務化された。パープルチーミングとは、レッドチームとブルーチームがパープルチームを結成し、セキュリティ対策、技術等の共同検証などを行うもので、テストから得られた教訓

図表1　TIBER-EUの主なステークホルダー

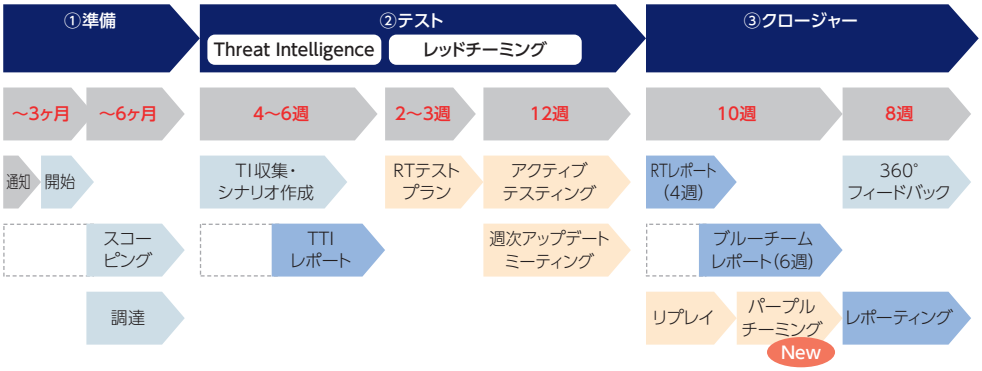


（出所）Draft Regulatory Technical Standards specifying elements related to threat led penetration tests under Article 26(11) of Regulation (EU) 2022/2554を基に野村総合研究所作成

NOTE

1) イングランド銀行によって開発されたフレームワーク「CBEST」では、テスターは、非営利団体「CREST」によって認証を受けることが必須となっている。
2) European Central Bank "TIBER-EU Framework updated to align with DORA" (2025年2月11日)
3) 欧州やアジアの一部地域では、2010年代後半から金融監督当局が主導してTLPTのフレームワークを開発してきた。代表的なものとしてイングランド銀行による「CBEST」、欧州中央銀行による「TIBER-EU」、香港金融管理局による「iCAST」等が挙げられる。
4) テスト対象となる金融機関は、クリティカルで重要な機能 (Critical Important Function, CIF)、各CIFを支えるシステムおよびサービス、各システムで収集するフラグを列挙したTIBER-EUスコープ仕様書を完了する必要がある。出所) European Central Bank "TIBER-EU Scope Specification Document Guidance" (2025年1月)
5) レッドチームテストで内部テスターを活用する場合、当該社員は1年以上の勤務経験が求められる。
6) European Central Bank "TIBER-EU Guidance for Service Provider Procurement" (2025年1月)
7) レッドチームテスターが時間的制約や金融機関のセキュリティ対策によって次の段階に進めない場合、金融機関は必要に応じてレッドチームテスターに追加的な情報を提供する等により、システムや内部ネットワークなどへのアクセスを許可し、テストを継続して次の段階に効率的に進めることができる。
8) 本邦では、金融庁が2018年に公表した「金融分野におけるサイバーセキュリティ強化に向けた取り組み方針」第二版で「(略) 脅威ベースのペネトレーションテスト」等の高度な評価手法の活用を促すことにより、対応能力の一層の高度化を図る」として、金融機関のTLPT実施を促してきた。

図表2　TIBER-EUに基づくTLPTの全体感



(出所) European Central Bank "TIBER-EU FRAMEWORK　How to implement the European framework for Threat Intelligence-Based Ethical Red teaming (2025年1月)" を基に野村総合研究所作成

を次に生かすことを企図している。

またテスト品質を担保するため、TIBER-EUでは内部テスターの利用に制限を設けている。レッドチームテストにおいて内部テスターを採用する場合は当局による承認が必要なほか[5]、3回に1度は外部テスターの利用を必須とする。また、外部テスターの品質を担保するため「サービスプロバイダー調達ガイダンス[6]」を策定し、組織要件（認証取得や実績等）や個人要件を規定している。

TLPT高度化に向けた取り組み

TIBER-EUをベースに自主的にTLPTを実施してきたEUの金融機関へのヒアリングによると、TLPTを通じてサイバー攻撃への実効性が高まってきたようだ。準備段階では、経営層レベルの理解促進やリスク管理の強化を図るため、コントロールチームのトップにCISOやCIOをアサインし、組織横断でTLPTを推進している。CISOやCIOには、組織内の信頼や体制を維持しつつ、ブルーチームへ情報を漏らすことなく当局やレッドチームとテストを進めるバランス感覚や、エスカレーションコントロールなどのスキルが求められる。また情報制御の観点からコントロールチームの人員を絞る工夫もみられる。テスト段階では、レッドチームが攻撃の糸口を見つけられず、当初想定していたテスト計画が初期段階で停滞してしまう場合がある。コントロールチームはレッドチームとコミュニケーションを密にし、段階に応じてエンドポイントセキュリティの調整を検討するなど効率的にテストを進めることが重要だ[7]。加えて本番環境下で不測の事態が起きた際には、コントロールチーム主導でテストを即時に中断できる体制を構築するとともに、事業中断保険への加入等のリスク管理策もとられている。

本邦におけるTLPT高度化およびサイバーセキュリティ強化の上で、EUにおけるTLPTの活用は参考となる[8]。金融機関はTLPT実施に向けて、自社の重要な機能の特定や社内の情報統制体制の構築を進めるとともに、信頼できる外部テスターを選定することが肝要である。

Writer's Profile

小野 亜樹 Aki Ono
金融イノベーション研究部
エキスパートコンサルタント
専門はリテール金融
focus@nri.co.jp