金融庁
Financial Services Agency

Discussion Paper Series

国際動向を踏まえた金融機関における実効性のある TLPT に関する考察

北原　幸彦

DP 2025-2

2025 年7月

金融庁金融研究センター
Financial Research Center (FSA Institute)
Financial Services Agency
Government of Japan

＜金融庁金融研究センター　ディスカッションペーパー DP2025-2（2025 年７月）＞

国際動向を踏まえた金融機関における実効性のある TLPT に関する考察

北原　幸彦*

概　　要

昨今、金融機関を狙ったサイバー攻撃の脅威が増加しており、また、攻撃手法も日々高度化・巧妙化を続けている。金融機関においては、このような巧妙化し続けるサイバー攻撃に対応すべく、日ごろから自機関におけるサイバー攻撃リスクを把握するとともに、そのようなサイバー攻撃に対して単にシステム面での対策を行うだけでなく、攻撃に対する人の動きや対応プロセスの整備も含めて強化していくことが重要である。

こうした背景の中、現実に起こりうるサイバー攻撃に対して金融機関の対応態勢がどの程度有効に機能するかを検証し、その改善と、更なる高度化に向けた教訓を得るためのアプローチとして、脅威ベースのペネトレーションテスト（Threat-Led Penetration Testing、以下、「TLPT」）の有効性の評価が高まっている。日本国内においては、特に大手金融機関を中心に TLPT の実施が増えてきている一方で、海外では、欧米を中心に先行して TLPT の取組みが進められているとともに、関連した法制度や各種フレームワークの整備などが進んでいる。

本稿では、こうした諸外国の金融機関における TLPT の取組みに関連した動向や、法令・各種フレームワーク等の整備状況をまとめるとともに、そうした諸外国の動向を踏まえ、日本の金融機関が TLPT を実施するにあたって、そのあるべき姿や留意すべきポイントなどについて考察する。

キーワード：サイバー攻撃、サイバーセキュリティ、TLPT、脅威ベースのペネトレーションテスト

* 金融庁金融研究センター研究官
本稿の執筆に当たっては、金融庁総合政策局リスク分析総括課 IT サイバー・経済安全保障監理官室の三浦調整官をはじめ、多くの庁内外の有識者に多大なる御支援をいただいた。この場を借りて感謝を申し上げたい。なお、本稿に示されている内容と意見は筆者個人に属するものであり、金融庁及び金融研究センターの公式見解を示すものではない。

１．はじめに

近年のサイバー攻撃は、国家の関与が疑われる大規模かつ巧妙で執拗な攻撃手法が相次いで発生するなど、サイバー攻撃の脅威は益々増加の一途をたどっている。一方で国内外における金融情報システムは、グローバル化の進展とともに外部ネットワークと接続するシステムが広がりをみせる中、今後もサイバー攻撃の脅威はさらに高まっていくものと考えられる。

こうした脅威に対処するため、金融機関は、サイバー攻撃の脅威を把握・分析したうえで必要な防御策を講じ、かつ、その有効性を検証する等の対策を講じる必要がある。ところが現実には、多くの金融機関は、増大し続けるサイバーリスクに対して対策が不十分であり、潜在的なリスクが高まっている状況にある。こうした中、より能動的なサイバー防御の取組みとして、現実に起こりうる脅威情報の分析（脅威インテリジェンス）を行うとともに、金融機関において実際に起こりうる攻撃手法に照らしたテストを行うことによって、そのサイバー攻撃への対応能力を検証するための手段として、TLPT（Threat-Led Penetration Testing）を実施することは金融機関におけるサイバーレジリエンスの強化にとって有効な手段となっている。

筆者は、2022 年より当庁の研究官として勤める傍ら、金融証券検査官として主に金融機関のサイバーセキュリティ対策におけるモニタリングを業務として行う中で、金融機関における TLPT の取組みやその在り方について、TLPT を実施する金融機関と直接対話を行ってきた。また、金融庁では、サイバーレジリエンス強化の政策として、2023 事務年度に開始した金融機関における TLPT に関する事例還元や、2024 事務年度には地域金融機関等に対する TLPT 実証事業といった取組みなど、金融機関におけるサイバーレジリエンス強化のための TLPT の実効性向上の政策を推進しており、筆者自身もこれらの政策に携わってきた。このような政策においても、日本の金融機関が実施する TLPT においては改善の余地がある事例が確認されている。

他方、海外の動向に目を向けると、かねてから特に英国における CBEST（Critical National Infrastructure Banking Supervision and Evaluation Testing）や、欧州における TIBER-EU（European Red Team Testing Framework）など、TLPT を実施するためのフレームワークの策定が欧州やアジアを中心として各国で進められてきている。直近では 2025 年 1 月に欧州でデジタル・オペレーショナル・レジリエンス法（Digital Operational Resilience Act 、以下「DORA」）が適用され、これにより対象となる金融機関では TLPT を実施することが実質的に義務化されている。このように、国際的な流れとして、金融機関が実効性のある TLPT の実施に取り組む諸外国での動向は日本よりも先行しており、こうした国際的な動きが日本の金融機関における TLPT の実効性向上において教訓となる点があると考えられる。

こうした点を踏まえ、本稿では、第 2 節で TLPT の概要と日本における取組みについて述べ、第 3 節では諸外国における動向として TLPT に関連する規制・ガイドラインの整備

の動きについてまとめる。続く第 4 節では、TLPT に関連するいくつかの切り口において、海外の規制・ガイドラインで対応が求められる内容を分析するとともに、日本の金融機関が、こうした海外動向を踏まえて TLPT で留意すべき点について考察する。

２．日本の金融分野における TLPT の取組み

２．１　サイバーセキュリティレジリエンステストとしての TLPT

２．１．１　サイバーセキュリティにおけるテスト・評価手法

組織がサイバー攻撃の脅威に晒されている状況においては、サイバーセキュリティ対策の実効性についてテスト・検証を実施し、組織が潜在的に抱えている脆弱性を特定し、攻撃者による侵害を未然に防ぐために必要な対策を行うとともに、インシデント対応を含めたサイバーレジリエンスを評価・向上することが極めて重要である。

一般的に、サイバーセキュリティにおけるテストは、机上でのテスト[1]と実機でのテストに分類される。このうち実機でのテストとしては、さらに「脆弱性診断」、「ペネトレーションテスト」、「TLPT」の３つに分類されることが一般的である。

脆弱性診断は、システムやネットワーク、アプリケーションなどに対して疑似的な攻撃の通信やリクエストを行うことにより、脆弱性の存在有無を検証する手法である。ペネトレーションテストは、攻撃者視点で攻撃試行を行い、システムを侵害しうるかを検証することで、システムにおける攻撃耐性を評価するテストである。そして TLPT は、現実的に起こりうる脅威をもとに疑似的な攻撃による検証を行い、システムにおける脆弱性に加えて、人・組織・プロセスにおいてどのような脆弱性、課題があるのか検証するテスト手法である。TLPT は、この３つのテスト手法のうち、一般的には最も難易度が高く、かつ高コストとなる。

２．１．２　TLPT の定義

G7 サイバー・エキスパート・グループが 2018 年に公表した「脅威ベースのペネトレーションテストに関する G7 の基礎的要素」では、TLPT は「（金融機関の）コントロール下において、実在の攻撃者の戦術、テクニック、手順をまねることにより、金融機関のサイバーレジリエンスを侵害しようとする、攻撃の試行である。これは、特定の脅威情報（threat intelligence）に基づき攻撃を試行するものであり、予備知識と、業務への影響を最小限に抑えつつ、金融機関の職員、プロセス、テクノロジーに焦点を当てた攻撃を試行するものである。」と定義している。

TLPT は、日々進化し、高度化し続けるサイバー攻撃の脅威に対し、現実的に起こりうる攻撃に対する耐性を評価する、サイバーレジリエンスの強化を目的とした高度なセキュリティテスト手法である。実際の攻撃を想定して攻撃耐性を検証するため、テストは実機を

[1] 例としてはチェックリストやヒアリングを用いたリスク評価、ドキュメントレビュー、テーブルトップエクササイズなどが考えられる。

用いて本番環境に対して実施することが必要とされている。また TLPT では、疑似攻撃テストを担うグループである「レッドチーム」、その疑似攻撃に対して防御、検知、対応を行うグループである「ブルーチーム」、そしてテスト全体の管理、調整を担当する「ホワイトチーム」[2]と呼ばれるチーム構成に分かれてテストを実施する。レッドチームが疑似的なサイバー攻撃を対象システムやネットワークに対して行うことで攻撃目標の達成を試みる一方、ブルーチームはその攻撃を検知し、対処することで、サイバー攻撃に対する防御能力の実効性を検証する。したがって、原則としてブルーチームには事前に予告されることなくテストを実施することが望ましいとされている。

このようにして、一般的な脆弱性診断やペネトレーションテストがシステム面における脆弱性を検出することを目的として実施される一方で、TLPT は、システム面での観点での評価だけでなく、「人」や「組織」、「対応プロセス」の観点に焦点を当てたサイバー攻撃耐性を評価する手法であることが特徴とされている。そうした点も踏まえ、TLPT では、現実に起こりうる攻撃を軸としてテストを計画・実施し、 レッドチームの知見の蓄積をもとにスコープやゴールを設定し、テストで実際に有効な攻撃を検証することが求められる。

２．２　国内における TLPT の取組み

２．２．１　当局の取組み

金融庁では、金融機関におけるサイバーセキュリティ対応能力強化のための、高度で実効性のある評価手法として、TLPT の実施を推進する政策を進めてきている。

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組方針」の第 2 版の改訂では、『大手金融機関について（中略）海外大手金融機関のベストプラクティスや国際的な動向を踏まえ、「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、大手金融機関を中心に TLPT の実施を促進してきた。また、2022 年に公表した同取組方針の第 3 版の改訂においては、「サイバーインシデントからの復旧・回復のための対応能力の強化のため、TLPT の実効性の向上や、大規模サイバーインシデントを見据えた対応等の取組み」をサイバーレジリエンスの強化の例として挙げている。そうした方針に加え、2018 年には諸外国の動向を把握するため、諸外国の TLPT の手法や金融機関の活用状況等について『諸外国の「脅威ベースのペネトレーションテスト(TLPT)」に関する報告書』[3]を公表し、金融機関に対して TLPT の活用を促してきた。

近年の具体的な政策としては、2023 事務年度、金融庁では TLPT を実施した実績のある一部の銀行からその事例を収集して分析し、主要な課題や好事例を還元する取組みを実施

[2] 後述する EU のデジタル・オペレーショナル・レジリエンス法（DORA）や TIBER-EU では「コントロールチーム」としている。

[3] https://www.fsa.go.jp/common/about/research/20180516.html

している[4]。こうした事例を金融機関が効果的に活用し、TLPT の実効性を高めることで、サイバーセキュリティ態勢の強化を推進している。さらに金融庁では、2024 事務年度、同様の事例還元の取組みを保険業に対して実施している。

また、地域金融機関等に対する TLPT 実証事業として、2024 事務年度、金融庁は地域金融機関等のうち複数の機関に対して TLPT を実施し、その有用性を実証するとともに、TLPT の前提となる脅威インテリジェンスについて地域金融機関に共通するものを抽出して地域金融機関に還元することで TLPT 実施の障壁を下げ、また、TLPT の結果判明した脆弱性について、よく認められるものを地域金融機関に還元することで、地域金融機関全体のサイバーセキュリティの強化を図っている。

２．２．２　国内の規制・ガイドライン

筆者がこのディスカッションペーパーを執筆している 2025 年現在において、日本国内には TLPT の実施を義務付けるような規制は存在しない。ガイドラインや手引書の位置付けとしては、公益財団法人金融情報システムセンター（FISC）が、2019 年に「金融機関等における TLPT 実施にあたっての手引書」（以下、「FISC 手引書」という）を発行している。この FISC 手引書は、TLPT を実施しようとする金融機関等の参考に資することを念頭に、TLPT を円滑に進めるための考慮事項を、プロセスごとに記載している。この FISC 手引書の策定にあたっては、海外のガイドラインをベースにしつつも、「国内金融機関等への TLPT の実施状況のヒアリング結果も参考にして、日本の現状に合うよう策定した」としており、国内金融機関が TLPT を実施するにあたって、そのプロセスを理解するうえでは参考になると考えられる。しかしながら 2019 年以降更新が行われておらず、CBEST や TIBER-EU など何年もの経験を踏まえてアップデートを重ねている諸外国での TLPT のフレームワークが求めている水準と比較すると、攻撃対象とするシステム環境や関係者への事前の情報開示の範囲の面において金融機関に判断を委ねており、本番環境での実施がどの程度推奨されるかが読み取れないことが金融機関側での判断を難しくしていることも考えられるなど、必ずしも十分とは言えない。

金融庁では、2024 年 10 月に、「金融分野におけるサイバーセキュリティに関するガイドライン」を公開し、サイバーセキュリティの観点から見たガバナンス、特定、防御、検知、対応、復旧、サードパーティリスク管理に関する着眼点について規定し、それぞれについて金融機関等において「基本的な対応事項」及び「対応が望ましい事項」を明確化している。TLPT に関しては、「対応が望ましい事項」として、以下のとおり規定している。

[4] 概要については、金融庁が 2024 年 6 月に公開した「金融機関のシステム障害に関する分析レポート」にコラムとして掲載している。（https://www.fsa.go.jp/news/r5/sonota/20240626/20240626.html）

2.2.4. 脆弱性診断及びペネトレーションテスト

【対応が望ましい事項】

b. 定期的に脅威ベースのペネトレーションテスト（TLPT）を実施すること。実施する際には、以下の点に留意すること。

・ 必要な経験及びスキルを持つ業者を選定すること（テスターの資格や経歴の確認等のバックグラウンドチェックを含む）。
・ 脅威インテリジェンスを踏まえ、実際の攻撃者が行う水準のテクニックを用いたテストを行うこと。
・ 関係主体等に対するサービスの提供に影響を及ぼしうる、深刻だが現実に起こりうる脅威シナリオをテスト計画において考慮すること。
・ テストでは、防御側の担当者（ブルーチーム）によるインシデント対応能力の評価（防御・検知・報告・封じ込め等）を行うこと。
・ テストは、本番環境を利用し、防御側の担当者（ブルーチーム）に予告することなく、実施すること。
・ 判明した課題を経営陣に報告し、改善活動を行うこと。

（資料）金融庁「金融分野におけるサイバーセキュリティに関するガイドライン」

なお、このガイドラインで規定する内容は一律の対応が求められるものではなく、金融機関等が「リスクベース・アプローチ」を採ることが必要である。TLPT に関して規定している事項は、後述する海外でのガイドライン、フレームワークと共通する点もあることから、金融機関等には、関係法令、監督指針等及び本ガイドライン等の趣旨を踏まえ、実質的かつ効果的な対応を行うことが求められている。

２．２．３　国内金融機関における TLPT を実施する上での課題

このように、日本国内においても金融機関に対して TLPT の実施を促す当局の取組みや、参考となるガイドラインの整備が進む中、国内金融機関における TLPT の実施はまだ大手金融機関を中心とした一部の金融機関に限られており、また、実施している金融機関においても、その実施内容は TLPT としては品質的に不十分であるケースも少なくない。前述した 2023 事務年度の TLPT 事例還元の取組みでは、例えば、「脅威インテリジェンスが一般的な脅威情報の分析にとどまっている」、「TLPT の計画を事前にブルーチームに伝えてブルーチームは疑似攻撃が発生することを把握している」、「TLPT の趣旨・目的に沿った十分な予算が確保されておらず、脅威インテリジェンスやブルーチームの評価が省かれ、結果として TLPT としては不十分なテストとなっている」などといった事例が確認されている。

TLPTの好事例及び課題

	望ましい事例	不十分な事例
脅威インテリジェンス	・自組織に特有の脅威インテリジェンスを導出し、シナリオ選定している。	・脅威インテリジェンスが一般的な脅威情報の分析にとどまっている。
評価	・ブルーチームに対して事前予告せずにTLPTを実施し、その検知・対応能力を評価している。 ・SOC*3における検知・対応能力だけでなく、フィッシングメールを起点とした職員からCSIRTへのエスカレーションと、CSIRT*4の対応状況も評価している。	・TLPTの計画を事前にブルーチームに伝え、ブルーチームが、疑似攻撃が発生することを把握しているため、その検知・対応能力が適正に評価されていないおそれがある。 ・攻撃者が考え得る複数の経路からの侵入や迂回攻撃を試みていないため、事前に想定した攻撃手法・経路で検証対象の脆弱性を検証する脆弱性診断と実質的に異ならないものにとどまっている。
経営陣への報告経営陣の対応	・サイバーセキュリティ担当部署は、TLPTの結果から判明した全社的な影響を生じさせ得るリスクを経営陣に報告している。 ・経営陣は、TLPTの結果報告を受け、課題への対応を指示するだけではなく、テスト範囲の拡大や事前に予告せずにテストを実施することを通じて、TLPTの高度化を図るように指示している。	・業務や顧客に重大な影響を及ぼし得る類似の課題が繰り返し検出されており、対策が十分ではなく、重要なリスクが残存している可能性を推測すべきであるにもかかわらず、過去の発見事項と類似していることをもってサイバーセキュリティ担当部署が経営陣への報告を省略している。 ・TLPTによって検出された課題のうち、金融機関の経営に重要な影響を及ぼし得るものについて経営陣に報告したり、具体的なリスクについて報告したりせず、単に「良好な結果であった」と報告している。
発見事項の活用	・サイバーセキュリティ担当部署は、TLPTで検出された課題と同様の課題がTLPTの対象でなかったシステムにおいても認められないかどうかを確認し、報告するよう、社内の他のシステム担当者及びグループ会社のシステム担当者に対して指示している。	・TLPTで検出された課題が他のシステムでも認められないかどうかを確認していない。その結果、それ以降、他のシステムに対して実施したTLPTでも類似した課題が検出されている。
その他	・犯罪集団、国家が関与する主体、内部犯行者などの様々な主体の攻撃が生じさせる脅威に応じ、複数のシナリオを設定し、TLPTを実施している。	・TLPTの趣旨・目的に沿った十分な予算が確保されておらず、脅威インテリジェンスやブルーチームの評価が省かれ、結果として、TLPTとしては不十分なテストとなっている。

図１　TLPT の好事例及び課題

（出所）金融庁「金融機関のシステム障害に関する分析レポート」（2024 年 6 月）

こうしたテストであっても、サイバーセキュリティ強化に資する面はあると考えられることから、テストの実施自体が否定されるものではないが、TLPT の目的や期待される効果を考慮すると、品質としては不十分であると言える。金融機関によってリスクプロファイルは異なり、またリソースの面において制約がある中、すべての金融機関が初回から望ましい TLPT を実施できる環境にあるとはいえないものの、形式的な TLPT を実施して満足するのではなく、望ましい TLPT が本来どうあるべきかを認識し、望ましい TLPT ではないことを経営陣に適切に報告する対応、不足する部分を補う対応が必要になるであろう。望ましい TLPT を実施する上でリソース面が制約となる場合は、経営陣に対して実効性のある TLPT の意義を伝え、予算増額等により十分なリソースを確保するなど、経営陣との適切なコミュニケーションが求められる。

こうした金融機関が実施する TLPT が実質的に不十分な品質になってしまうという課題の根本にある原因としては、「コスト」と「リスク」の側面があると考えられる。

コストの面においては、一般的なペネトレーションテストと比較すると、TLPT では脅威インテリジェンスの導出やブルーチーム評価のフェーズが加わることとなり、コストや期間の増大につながる。特に規模の小さな金融機関においては、脅威インテリジェンスの導出を綿密に行うことが、費用対効果面を踏まえると果たして必要なのかは議論の余地があろう。2024 事務年度に金融庁において実施した TLPT 実証事業では、脅威インテリジェンスを活用し、同業種の金融機関に共通する脅威情報の還元を行っているが、こうした共通の枠組みによる簡略化で TLPT の障壁は下がるであろう。こうした考え方は、4.6 節

で詳述する。

もう一方のリスクの面においては、特に本番環境でブルーチームに事前に告知せずに本番さながらの疑似攻撃を仕掛けることで、システム停止などが本番環境に影響を及ぼす事態が発生してしまうリスクを懸念する点が考えられる。金融機関におけるホワイトチームがまだ TLPT を実施した経験が浅く、TLPT の管理・運営にあたって不安があることがその根本原因として考えられる。そうした場合は、金融庁が推奨する望ましい TLPT とは異なることについて経営の理解を得たうえで、本番環境でテストを実施する前に、まずは試行的に開発環境などの本番環境への影響の不安が少ない環境でテストを行うことで、TLPT の計画やテスト段階で管理・運営を行う能力を段階的に向上させるという方法も考えられる。

こうした課題に対する筆者としての対応の考え方は、第 4 章で述べる。

３．諸外国における TLPT の動向

欧州を中心とした諸外国では、各国独自に金融機関を対象とした TLPT の推進を政策として進めている。ここでは、金融規制当局が主導する TLPT に関するフレームワークや実施手順について、特に本稿を執筆する 2025 年時点を中心に述べる。当局がどのような背景に基づき、どのような TLPT のフレームワークと手順を整備しているのか。また、テストの範囲や対象となる金融機関について、どのような条件や基準が存在するのかなどを述べる。 加えて、当局がテストにどのように関与し、テストの結果がどう扱われるのかについても触れる。

３．１　「デジタル・オペレーショナル・レジリエンス法」（DORA）

金融分野においては、欧州連合（EU）の規制であるデジタル・オペレーショナル・レジリエンス法（DORA）が注目されている。DORA は 2023 年 1 月 16 日に公布された EU の規制であり、2025 年 1 月 17 日から適用されている。

この DORA では、包括的な枠組みとして、「1. ICT リスク管理とガバナンス」、「2. インシデント報告」、「3. デジタル・オペレーショナル・レジリエンス・テスト」、「4. 第三者リスク管理」、「5. 情報共有」という 5 つの柱で構成されている。このうち、「3. デジタル・オペレーショナル・レジリエンス・テスト」では、組織の ICT 関連のインシデントに対する備えを評価し、脆弱性を検出し、是正措置を実施することを目的としたレジリエンステストに関する基本要件を定めている。これは、実質的には適用対象となる金融機関に対して TLPT の実施を義務付ける規制であり、EU 各国当局は、その国の適用対象となる金融機関における TLPT の実施状況を指導・管理することが求められている。したがって、2025 年の DORA の施行に伴い、TLPT の実施が金融機関全体に広く普及していくことが予想される。

この DORA では、その具体的な要件や運用方法を定めた技術基準である RTS（Regulatory

Technical Standards：規制技術基準）が策定されている。デジタル・オペレーショナル・レジリエンス・テストにおける RTS として、「RTS on threat-led penetration testing」が策定されており、金融機関がサイバー脅威に対する耐性を強化するための、TLPT の実施における具体的な要件や手順が詳細に定められている。具体的には、G-SIIs（国際的にシステム上重要な保険会社）および O-SIIs（その他のシステム上重要な機関）として指定された銀行など[5]、一定の基準に該当し、RTS の対象となる金融機関に対して、少なくとも 3 年に 1 度の頻度で TLPT を実施することや、その TLPT におけるアクティブなレッドチームのテストフェーズの期間を少なくとも 12 週間以上とすることを義務化するなど、具体的で厳格な要件が定められている。こうした要件は、EU 域内のみならず、EU 域内に拠点を置く諸外国の金融機関においても認識する必要があることから、今後の金融機関における TLPT の在り方として、重要な位置づけとなる可能性が考えられる。

３．２　当局主導の TLPT のフレームワーク

これまで、英国をはじめとした欧州を中心に、諸外国の大手金融機関を対象とした当局が関与する TLPT のフレームワークの開発が進められてきており、その流れはアジア等の欧州以外の諸国にも広く普及している。こうしたフレームワークは、英国における CBEST や、EU における TIBER-EU をベースとして、各国における状況等を踏まえて見直されている。そのため、日本の金融機関においても、こうした CBEST や TIBER-EU などの諸外国で開発されたフレームワークから、TLPT の在り方として教訓が得られる示唆が含まれている。なお、2018 年 5 月以前に開発された、CBEST をはじめとする諸外国の当局が主導する TLPT のフレームワークついては、2.2.1 節でも触れた『諸外国の「脅威ベースのペネトレーションテスト(TLPT)」に関する報告書』にも詳述されているので、フレームワークの内容を知るうえではあわせて参照されたい。

３．２．１　英国銀行による CBEST

各国当局の先駆けとして、2014 年に英国のイングランド銀行（Bank of England）と、情報セキュリティ市場におけるサービスの技術的専門性を保証する非営利団体である CREST（Council for Registered Ethical Security Testers）が共同で開発し、導入された金融機関における TLPT のフレームワークが CBEST である。

CBEST の主な目的は、金融機関が直面する現実的なサイバー脅威をシミュレーションし、システムや業務プロセスの防御能力を評価、強化することである。これにより、金融機関がサイバー攻撃に対する耐性やサイバーレジリエンスを向上させることが期待されている。

---

[5] 「RTS on threat-led penetration testing」では、適用対象となる金融機関の基準が“Article2　Identification of financial entities required to perform TLPT”に具体的に規定されている。
https://www.dora-info.eu/rts-tlpt/article-2/

CBEST は、実施するテスターが CREST によって認証を受けた専門機関より選定されるため、テストの質と信頼性が保証されているところに特徴がある。CBEST は規制当局によって示された TLPT における最初のフレームワークであり、その後に開発されている諸外国におけるフレームワークにおいても、その開発や改定においてベストプラクティスとして参照されており、現在の金融機関における TLPT の各種ガイドライン・フレームワークのデファクトスタンダードともいえるものである。

この CBEST では、そのテスト実施に関連する主要なフェーズ、活動、成果物、および相互作用について説明する Implementation Guide for CBEST participants（CBEST 実施ガイド）が公開されている。このガイドは 2024 年に改訂が行われており、これまで 9 か月であった典型的なプロジェクト期間を 9～12 か月とした「タイムラインの見直し」、ホワイトチームの役割である CG（コントロールグループ）がプロジェクト計画や技術テストにおける重大な懸念を直ちに規制当局に報告する責任を定めた「CG の責任強化」、CG が CBEST の全フェーズでの技術的および運用上の管理下に維持することを確実にするリスク評価の実施を規定した「リスク管理の強化」の３点が主な改訂のポイントとされている。いずれも、従来の CBEST をさらに高度化したフレームワークへと進化させる意図がうかがえる。

３．２．２　欧州中央銀行による「TIBER-EU」

欧州中央銀行において、欧州中央銀行制度を採用する 27 ヶ国の金融分野で利用可能な TLPT のフレームワークとして 2018 年 5 月に発行されたのが、TIBER-EU である。このフレームワークは、実際の攻撃者の戦術（Tactics）、技術（Techniques）、手順（Procedures）を模倣したサイバー攻撃を通じて、組織の防御能力を評価・向上することを目的としている。

TIBER-EU は、CBEST など、既に他国の当局が公表しているフレームワークを参考にしているが、他方で CBEST の実績から得られた教訓などを踏まえ改良している。

先述した DORA が 2025 年 1 月から EU 域内で適用されたことに伴い、「RTS on threat-led penetration testing」における TLPT と整合させることを目的として、TIBER-EU は 2025 年 2 月に改訂されている。この改訂においては DORA との一貫性を確保することを目的に用語の統一などを行うほか、DORA RTS で求められているパープルチーミングの義務化などが規定されている。

なお、この TIBER-EU では、フレームワークを補完するガイダンスを数多く提供している。例えば TIBER-EU for the Blue Team Test Report では、ブルーチーム評価を実施した際に、評価レポートを作成するにあたっての考慮事項について規定するなど、TLPT を実施する上で参考となると考えられることから、必要に応じて参照されたい。

表 1　TIBER-EU で提供しているガイド等

名称	説明
TIBER-EU Framework	フレームワーク
TIBER-EU Control Team Guidance	コントロールチームガイド
TIBER-EU Initiation Documents Guidance	開始文書ガイド
TIBER-EU Guidance for Service Provider Procurement	サービスプロバイダー調達ガイド
TIBER-EU Scope Specification Document Guidance	適用範囲仕様書の指針
Targeted Threat Intelligence Report Guidance	脅威インテリジェンスレポートガイド
TIBER-EU Red Team Test Plan Guidance	レッドチームテスト計画ガイド
TIBER-EU Red Team Test Report Guidance	レッドチームテストレポートガイド
TIBER-EU for the Blue Team Test Report	ブルーチームテスト計画ガイド
TIBER-EU Purple Teaming Best Practices	パープルチーミングの優良事例
TIBER-EU Test Summary Report Guidance	要約レポートのガイド
TIBER-EU Remediation Plan Guidance	改善計画のガイド
TIBER-EU Attestation Template	証明書のテンプレート

（資料）European Central Bank(https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html)

３．２．３　その他の諸外国における当局主導の TLPT のフレームワーク

2014 年の CBEST や 2017 年の TIBER-EU の開発以降、他の世界各国でも当局主導での TLPT のプログラムの開発が進められている。

香港では、香港金融管理局（HKMA）により「Intelligence-led Cyber Attack Simulation Testing（iCAST）」が 2016 年 12 月に策定されている。HKMA による固有リスク評価により、固有リスクが「high」または「medium」であった場合に iCAST を受験しなければならないということが、この iCAST の特徴である。

シンガポールでは、2018 年に「Adversarial Attack Simulation Exercise Guidelines for the Financial Industry in Singapore（AASE）」が公表されている。シンガポールの金融業界がレッドチーム(RT)演習を実施するためのガイドラインを提供するものであり、組織がそのような演習を計画、実施、報告する際に役立つガイドラインとベストプラクティスが含まれている。この AASE は 2024 年 9 月に第 2 版に改訂されており、4.6 節にて後述するパープルチーミングに関する内容が新たに追加されるなどの更新が行われている。

サウジアラビアでは、2019 年、サウジアラビア中央銀行（Saudi Arabian Monetary Authority（SAMA））により「Financial Entities Ethical Red-Teaming Framework（FEER）」を公表している。レッドチーム、ブルーチーム、ホワイトチームに加えて、SAMA の IT 金融セクターのリスク監督部門を「グリーンチーム」として定義し、TLPT を監督する役割としているこ

とが特徴的である。

オーストラリアでは、2020 年にオーストラリアの金融規制評議会によって「Cyber Operational Resilience Intelligence-led Exercises (CORIE)」を公表している。オーストラリアの金融機関向けの TLPT のプログラムガイドであり、2022 年 7 月に第 2 版に改訂されている。この CORIE では、金融機関の上級管理職がゴールドチームとして参加し、テーブルトップエクササイズを実施することにより、サイバーインシデントの管理や危機対応プロセスを評価することを規定していることが特徴である。

EU 加盟国においては、TIBER-EU を基礎として、例えばスウェーデンでは TIBER-SE、アイスランドでは TIBER-IS など、各国での状況にあわせた TIBER の策定が進められている。この各国の TIBER プログラムは、2025 年の TIBER-EU の改訂に伴い、DORA の要件と整合させて実施手順を更新させることが期待されている。

CBEST が開発されて 10 年経過した直近の 2024 年では、当局が主導する TLPT のフレームワークとして 2 つのフレームワークが公開されている。 1 つは CREST の STAR-FS、もう 1 つはオランダ中央銀行が策定した ART である。

2024 年 3 月に公開された CREST の STAR-FS（Simulated Targeted Attack & Response for the Finance Sector）は、規制当局に同じレベルの厳格さが適用されるようにしながら、規制当局へのリソースの影響を軽減しつつも、規制当局のニーズを満たすように開発されたフレームワークである。これによって、CBEST よりも広範な金融機関が利用可能であるとしている。

2024 年 4 月にオランダ中央銀行によって公開された ART（Advanced Red Teaming Framework）は、オランダの金融機関向けの高レベルの脅威情報によって推進される高度なレッドチーミングテストを実施するための包括的なフレームワークである。TIBER を発展させたものであるが、完全な TIBER テストの準備ができていない、又は DORA/TLPT の対象となっていない金融機関にも焦点を当てている点を特徴としている。DORA や TIBER の対象となるような大規模金融機関でなくとも、レッドチーミングを行うにあたって参照可能なフレームワークといえる。

近年では、金融サービスとして特に重要な位置付けを持つ大規模金融機関にとっては、DORA のように、TLPT の実施に対する規制がより強化されているとともに、CREST の STAR-FS やオランダの ART のように、高水準な TLPT を実施することが難しい金融機関に対しても適用可能なフレームワークの開発が進んでいる状況にあるということがいえる。

３．３　その他のガイドライン、フレームワーク

前節では、当局が主導する TLPT のフレームワークをいくつか取り上げて紹介したが、本節ではそれ以外のガイドラインとして、「TLPT の G7 の基礎的要素」と GFMA のフレームワークについて述べる。

2018 年、G7 サイバー・エキスパート・グループによって公表され、2.1.2 節でも紹介したのが「脅威ベースのペネトレーションテストに関する G7 の基礎的要素（G7 Fundamental Elements for Threat-Led Penetration Testing（以下、「TLPT の G7 基礎的要素」）」[6]である。この TLPT の G7 基礎的要素は、「シミュレーションを通じて悪意のある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（guide）を金融機関に提供するとともに、当局がそれぞれの国において脅威ベースのペネトレーションテスト（TLPT）の活用を検討するための指針を提供する」ことを目的としている。この TLPT の G7 基礎的要素は、当庁のホームページに仮訳として公開しているが、2.2.2 節の中で紹介した FISC 手引書と並んで、数少ない日本語でのガイダンスが入手可能であることから、TLPT の実施を検討する日本の金融機関は、参照されることが望まれる。なお、この TLPT の G7 基礎的要素は 6 つの要素から構成されるが、6 つ目の要素である「類型化したデータ」では、当局の役割として、「類型化したデータとして、セクターに共通する発見事項や脆弱性を特定し、（中略）当局と金融機関の間で共有することが、金融セクターのサイバーレジリエンスの改善に貢献することである」としており、これを踏まえて、日本においても金融庁が 2023 年に金融機関で実施した TLPT の事例を収集し、好事例や課題を類型化したデータとして還元する取組みを行っている。

2019 年、GFMA（Global Financial Markets Association）は、業界団体としてグローバルに標準化された TLPT に関するフレームワーク[7]を策定し、2020 年に第 2 版として改訂して公開している。規制当局及び金融サービス会社が、監督上の要件及び金融機関自身が課した要件の双方を満たすために効果的なテストを実施するための、合意されたアプローチを構築することを目的とする。また、TLPT を実施する際の規制当局と企業との間の相互作用に主に焦点を当てており、テストプロセスの詳細な技術的詳細を提供することを意図したものではないとしている。3.2 節で取り上げた多くの当局主導の TLPT のフレームワークが当局の視点であるのに対して、この GFMA のフレームワークは業界団体が策定したものであり、業界の視点である点が興味深い。例えば DORA や TIBER-EU など、当局主導のフレームワークではその多くが TLPT を本番環境で実施することを求めている一方で、この GFMA のフレームワークでは、リスクの高い活動は本番以外のシステムに対してテストを実施することがあることも想定したものとなっている。

４．国内金融機関における実効性のある TLPT に関する考察

ここまで、第 2 章では日本における当局の TLPT に関する取組みについて、第 3 章では諸外国の TLPT に関する規制やフレームワーク、ガイドラインについて述べてきた。グロ

[6] https://www.fsa.go.jp/inter/etc/20181015/20181015.html

[7] A Framework for Threat-Led Penetration Testing in the Financial Services Industry（https://www.gfma.org/correspondence/updated-gfma-framework-for-the-regulatory-use-of-penetration-testing-in-the-financial-services-industry/）

ーバルに進出する金融機関においては､海外の規制やガイドラインへの対応は必然であり、また中小の金融機関においても、国境のないサイバー攻撃リスクへの対応として、海外の金融機関が参照しているガイドラインは大いに参考になるはずである。本章では、日本国内での TLPT への取組みの実態に加え、諸外国のフレームワークやガイドラインを踏まえて、日本の金融機関が留意すべき TLPT の在り方について考察する。

４．１　テスト実施者

金融機関が TLPT を実施するうえでは、テスト実施者の選定が大きなポイントとなる。グローバル規模で事業展開しているような海外の金融機関では、内製化した独自のレッドチームを組成してテストを実施するような事例もみられるが、日本の多くの金融機関においては、外部のセキュリティベンダーなどのサービスプロバイダーに委託することを選択するケースがほとんどであろう。TLPT では、現実に起こりうるような、国家が関与する犯罪集団による巧妙な攻撃手法を含む疑似テストを実施することが期待されるため、それを実現するためには業者選定にあたってサービスプロバイダーの持つスキルの見極めが極めて重要となる。

諸外国のフレームワークとしては、CBEST では TLPT を実施するサービスプロバイダーは、経験値などの一定の条件を満たし、CREST による資格認定を受けることが必要とされている。その認定を受けるためには、定められた期間以上の経験値が必要とされる。また、DORA では第 27 条で TLPT 実施のためのテスト実施者に対する要件を規定しており、TIBER-EU でも、サービスプロバイダー調達ガイダンス（Guidance for Service Provider Procurement）を策定しており、2025 年 1 月に DORA に整合した形で改訂されている。

テスト実施者には、その組織や個人としての信頼性（Credibility）が重要な要素である。DORA では本文の第 27 条で TLPT のテスト実施者である組織として求められる要件について規定している。そこではテスト実施者としての高い適性や評判、加盟国の認定機関による認証取得または正式な行動規範または倫理的枠組みの遵守といった要件が定められている。また、DORA の RTS においては、テスト実施者を構成する個人の要件として、レッドチームテストで 5 年以上の経験を有する少なくとも 1 人のマネージャーと、2 年以上の経験を有する少なくとも 2 人の追加のテスターで構成されるなどといった要件が定められている。このように、実効性のある TLPT を実施するためには、テスト実施者の組織として求められる要件と、そのチームを構成する個人、特にそのチームのプロジェクトマネージャーに求められる要件を明確にして、その要件に適合するテスト実施者を選定することが重要である。

誤ったテスト実施者の選定は、リスクの過小評価やテスト品質の低下、コンプライアンス違反といった結果を招きかねない。単に複数のベンダーの見積りの中から最安値のベンダーに委託するといった安易な選択をすることなく、テスト実施者として相応しい信頼性を兼ね備えているか、しっかりと見極めることが重要である。

なお、このテスターの要件については、日本国内の文献としては FISC 手引書において「第３編プロバイダー選定にあたっての留意事項」にプロバイダーを選定する際の評価の視点等について具体的に示されている。国内金融機関がサービスプロバイダーを選定するにあたっては、参考になると思われる。

日本国内には CREST のようなサービスプロバイダーを認定するような制度はないため、客観的にテスト実施者の技術力を評価することは難しいと思われるが、サービスプロバイダーの選定に関しては上述のとおり、国内外で数多くのガイダンスが示されているため、そのようなドキュメントを参考として、過去の実績（経験年数やプロジェクトの内容を含む）や、効果的かつ高品質なサービスの提供を実現できることの裏付け（保有資格等を含む）などの情報をもとに、高スキルなサービスプロバイダーを選定することが求められる。

また、テスト実施者の内製化については、以前から開発されている CBEST や TIBER-EU（2018 年版）では、そもそもテストを内製化して実施することは想定されていなかったが、近年公表されている DORA や TIBER-EU（2025 年改訂版）、オランダの ART などにおいては、テスト実施者を一部内製化することも想定して定められた内容となっている。しかしながら DORA では、内製化にあたっては当局等からの承認や利益相反の回避などが要求事項として規定されているほか、TIBER-EU では、”In TIBER-EU, it is mandatory to use an external TIP and strongly encouraged to use external RTT”（脅威インテリジェンスは外部の利用が必須、レッドチームテストも外部の利用を強く推奨）とされており、テストの内製化に対する制約が規定されている。システムの脆弱性を検出することを目的としたいわゆる脆弱性診断やペネトレーションテストなど、比較的簡易なテストは内製化することでテストの効率化や費用対効果の面でメリットがあると思われるが、テスト実施者に高度な技術力や第三者的な視点が要求される TLPT を実施するにあたっては、内製のテスト実施者には制約を設けることが必要になるなど、外部のサービスプロバイダーによるテストと、内製によるテストとの使い分けが重要である。

４．２　対象環境

TLPT を実施する際、テスト対象を本番環境とするか、あるいは非本番環境（開発環境やステージング環境など）とするかは、重要な論点である。本番環境と非本番環境は必ずしも同一のセキュリティレベルにあるとはいえず、また、ブルーチーム評価を実施するにあたっても、本番環境と同水準での評価が行われるとはいえない。一方、テストが本番環境で行われる場合、特定の攻撃シミュレーションにリスクの高いアクティビティが含まれる場合があり、攻撃耐性が十分でない金融機関で万が一障害が発生してしまった場合、影響が甚大となり、テストで得られるメリットよりも大きな損害が発生する可能性がある。したがって、金融機関等においては、スコープ設定の段階でリスク分析を実施したうえで、テストを本番環境で実施することが適切であるか、十分な評価を行うことが必要である。

テストを実施する対象環境について、各種ガイドラインではどのように求められるかに

ついて整理する。まずDORAにおいては、第26条第2項において、“Each threat-led penetration test shall cover several or all critical or important functions of a financial entity, and shall be performed on live production systems supporting such functions”（それぞれのTLPTは、金融機関のいくつかまたはすべての重要な機能をカバーし、かつそれらの機能をサポートする本番システム上で実行されるものとする。）と規定されている。つまり、条文にてTLPTを本番環境で実施することが求められていることを意味する。また、CBESTやTIBER-EUなど以前から欧州で用いられているフレームワークにおいても同様に、原則として本番環境で実施することが要求されている。

このように、DORAやCBESTのような高度なTLPTの実施が求められる当局主導のフレームワークでは本番環境での実施を原則としているが、2.2.3節で述べたとおり、現実的なリスクを考慮すると、たとえ、提案書上で実績の豊富なレッドチームを擁するベンダーと契約を締結したとしても、本番環境でテストを行うことに躊躇してしまう金融機関も多いと考えられる。これは、ホワイトチームの経験不足であったり、レッドチームとの信頼関係がなくスキルに不安があったりすることが背景として考えられる。ホワイトチームが準備段階でリスクの発生を防ぐようしっかりプランニング[8]を行うとともに、レッドチームのスキルを見極める必要がある。このような観点で、金融庁の推奨する形とは異なるものの、経験値を高めるためにまずは開発環境やステージング環境でTLPTを実施してホワイトチームやレッドチームのスキルを十分に検証して成熟度を高めるというプロセスを踏むことは、アプローチの仕方の一つとしては理解できる。しかしながら、開発環境でテストをした結果、問題なかったと判断してしまうことは、「人」、「組織」、「プロセス」を評価するうえでは決して十分であるとはいえない。TLPTの目的を踏まえ、その結果を実効性のあるものにするためには、最終的には本番環境で実施することが必要である。その際、実際に稼動している環境に対してTLPTを実施する以上は、一定の業務リスクがありうることを踏まえ、その未然防止や、発生時の対応方法を取り決めるなどの対応が必要である。

４．３　テストのアプローチ

TLPTでは一般的に、ブラックボックステスト、グレイボックステスト、ホワイトボックステストというアプローチがある。

ブラックボックステストは、テスト実施者に対して事前にテスト対象に関する一切の情報を与えずにテストを実施する方法である。TLPTが現実に起こりうるサイバー攻撃を疑似的にテストすることであることを踏まえると、その目的には極めて近い形であるものの、事前情報が少ないため、リスクを特定するのに時間がかかったり、場合によっては本番環境に重大な影響を与えたりしてしまうというデメリットが考えられる。

[8] テストの進め方における具体的なプラクティスとしては、管理者権限を奪取されたことを以て侵害が成功したことと見做し、その管理者権限を利用してシステムの侵害までは行わないことなどが考えられる。

一方、グレイボックステストはテスト実施者に必要最低限の情報を与えてテストを実施する方法、ホワイトボックステストは、テストに必要な情報をすべてテスト実施者に与えてテストを実施する方法である。これらの方式は、情報の開示範囲が広がるほど時間とコストの観点で効率化できる一方、よりリアルな評価が難しくなるというデメリットがある。グレイボックステストは、時間をかけて調査する工程や、攻撃による情報取得の工程を時間短縮するうえで有効である一方、レッドチームに攻撃に必要な情報を与えてしまうことで、攻撃が現実のサイバー攻撃を想定した流れとならない懸念があるという点を踏まえる必要がある。いずれにせよ、グレイボックスを選択する場合、テスト実施者に与える情報は必要最低限とすることが重要である。

この点について、CBEST や TLPT の G7 の基礎的要素では、脅威インテリジェンスにあたって対象の金融機関が一定の情報を事前にテスト実施者に提供することとしており、必ずしも完全なブラックボックステストを前提とはしていない。また、TIBER-EU（2025 年改訂版）においては、効果的かつ効率的なテストを促進するために、追加情報をテスト実施者に提供する場合があるとしており、グレイボックスを選択しうることとしている。このように、諸外国のフレームワークにおいて、実践的な攻撃を想定するという観点においても、必ずしもブラックボックステストが求められているわけではないことがわかる。

以上から、まずはブラックボックスを前提としてテストを開始し、攻撃の成否の状況やテスト全体のスケジュールにあわせて部分的に情報を開示するなど、状況に応じて柔軟にグレイボックスへと移行していくアプローチも考えられる。ただし、これを実施するにあたっては、レッドチームの高度なスキルと、ホワイトチームとレッドチームとの適切な連携が必要となる。また、コスト削減の観点からテストを効果的、効率的に実施し、かつ本番環境への影響を留めるうえでも、グレイボックスを選択することもアプローチの一つと考えられる。ただし、レッドチームによる攻撃が成功した場合に、テストでは事前に非公開情報をレッドチームに提供していたことをもって判明した課題を過小評価するような姿勢では、多額の費用をかけて実施する TLPT は無駄になってしまうであろう。

４．４　ホワイトチーム（コントロールチーム）

TLPT を実施するにあたり、ホワイトチームがテスト全体の管理、調整において重要な役割を担う。従来、レッドチームやブルーチームとの区別でホワイトチームと呼称されていたが、CBEST ではコントロールグループ（Control Group）、また TIBER-EU や DORA ではコントロールチーム（Control team）としており、欧州を中心にこうしたホワイトチームの役割に即した呼び方が一般的となっている。

TIBER-EU では、このホワイトチームを組成するにあたっての要求事項について規定した TIBER-EU Control Team Guidance を公表している。この中でホワイトチームの役割として、テスト計画の策定、外部のテスト実行者の選定と管理、リスク評価、テストの安全性の確保、関係者との調整、テスト実施中の監視、問題発生時の対応、テスト実施後の評価・

報告など、実効性のある TLPT を実施するにあたって重要性の高い多くの役割を規定している。このようにホワイトチームは、TLPT において中心的な役割を担い、テストが安全かつ効率的に行われ、リスクをコントロールしつつ実践的な学びを得るために非常に重要な役割を担う。したがって、リスク管理スキルやプロジェクト管理スキル、コミュニケーション能力などの必要なスキルセットを持ったテスト実施責任者と、必要に応じて外部のセキュリティ専門家などが共同でこのホワイトチームの役割を担うことが求められる。

一方で、このホワイトチームがサイバー攻撃に関する理解やリスク管理スキル、コミュニケーション能力が不十分である場合、適切な状況判断が行われなかったり、ステークホルダーへの報告が遅れたりなど、テスト品質の低下につながるとともに、場合によっては 4.2 節でも述べたとおり、不十分なプランニングや状況判断により、本番環境に影響を及ぼすなどの大きな損害にもつながりかねない。このためホワイトチームは、十分なスキルセットを持ったメンバーによって必要な役割を果たせるよう、慎重に組成することが必要となる。

４．５　脅威インテリジェンス

TLPT は一般的に、脅威インテリジェンスフェーズとペネトレーションテスト（レッドチームテスト）フェーズに分類される。TLPT と一般的なペネトレーションテストとの違いのひとつとして、TLPT では、事前に脅威インテリジェンスフェーズを設けることで、現実的に起こりうるサイバー攻撃の脅威を分析し、その分析結果に基づくテストを実施するというプロセスが含まれるということがいえる。したがって、ペネトレーションテストから TLPT へとステップアップするにあたり、この脅威インテリジェンスフェーズは極めて重要となる。

一方、2.2.3 節でも触れたとおり、金融機関にとってはこの脅威インテリジェンスフェーズはコストの観点で足枷になることが想定される。特に、中小の金融機関にとっては、個社が独自にターゲットとなりうるような脅威が存在するかは不確かであり、その分析にコストをかけるメリットが感じられにくいと思われる。脅威インテリジェンスの結果が、どうシナリオに反映されるのかも、想像することも難しいかもしれない。TLPT を実施するにあたり、予算上の制約がある場合に、実施を断念する可能性が考えられるのもこの脅威インテリジェンスフェーズではないかと考えられる。

この点に関して、当局が主導する TLPT フレームワークの多くが、サービスプロバイダーが脅威インテリジェンスを実施する前提としているなか、業界団体が策定した GFMA の TLPT フレームワークでは、”It is recommended that industry and regulators jointly identify and prioritize the threats in order to develop test scenarios at the financial sector level”（金融セクターレベルでテストシナリオを開発するために、業界と規制当局が共同で脅威を特定し、優先順位を付けることが推奨される）としている点が興味深い。業界団体や規制当局が脅威情報を特定し、セクターに共有することで、コストを抑えつつ必要な情報が享受できるのは

合理的な考え方であるといえる。

CBEST や STAR-FS、TLPT の G7 の基礎的要素などでは、Intelligence フェーズを Threat intelligence と Targeting とに分類した考え方を用いている。このうち Threat intelligence は、攻撃者の攻撃手法を分析し、現実的な攻撃シナリオを作成することを目的としており、Targeting は、特定の攻撃対象を選定し、実際の攻撃方法を特定することを目的としている。ここでいう Threat intelligence は、業種や業態によって差はあるものと考えられるが、個社単位ではそれほどの違いは考えにくい。この Threat intelligence に関しては、業界団体や当局が主導して実施することで、全体としてコストを抑えた脅威インテリジェンスの実施が考えられる。金融庁が 2024 事務年度に実施している実証実験では、地域金融機関における脅威インテリジェンスをもとに、共通する脅威情報を業態全体に還元することを施策の目的のひとつとしている。まさにこういった動きが行われることにより、金融機関においても TLPT を実施する組織の裾野が広がるのではないかと考えられる。

こうした点を踏まえると、脅威インテリジェンスプロバイダーの技術を利用して、自組織における脅威情報を分析し、それをもとに TLPT を実施することが TLPT としてのあるべき姿ではあるが、個社特有の脅威が特定されにくいような中小の金融機関については、Threat intelligence がうまく共有されるスキームを確立し、脅威インテリジェンスの導出からシナリオ作成までを共通の枠組みで簡略化することができれば、TLPT の障壁が下がることが考えられる。一方で、コストや期間を抑える観点から脅威インテリジェンスの導出を行わず、テスト対象を予め特定のシステムに限定したり、一般的な脅威情報を元に攻撃手法を予め決めてテストを行ったりすること[9]は、その組織が潜在的に抱えている脅威が踏まえられておらず、実効性のある TLPT としては不十分である。

４．６　レッドチームテスト

脅威インテリジェンスフェーズを経て構築されたシナリオをベースとして、レッドチームテストが実施される。一般的には、組織的な攻撃者によるサイバー攻撃が、フィッシングなどのソーシャルエンジニアリングや、システムの脆弱性を突くような巧妙な手口によってインターネット経由で組織内部のネットワークに侵入し、侵害を試みるような攻撃シナリオが考えられるが、より高度な手法としては、内部不正や、物理的な建物への侵入を起点とした攻撃シナリオも考えられる。

この侵入テストフェーズに関しては、諸外国のフレームワークで規定されているタイムフレームに着目したい。DORA の RTS や、その DORA に基づく TIBER-EU では、アクティブなレッドチームのテストフェーズの期間は、少なくとも 12 週間と規定している。また、CBEST では例示として 14 週間、STAR-FS では 4～6 週間、業界団体が策定した GFMA

[9] 例えば、標的型メールの脅威が高まっているとの判断のもと、不自然な日本語表記のメールや、アンチウイルスソフトのパターンマッチで容易に検出できるような添付ファイルのメールを送付するなど、実際に生じている攻撃者のテクニックの水準に合わない形式的なテストをすることなどが考えられる。

のフレームワークでは、TLPT の開始から終了までで 10～12 週間としている。

表 2　代表的な諸外国のフレームワークにおけるタイムライン

	TIBER-EU	CBEST
テストの総期間	9～12 か月	9～12 か月
準備フェーズ	～6 か月	～6 週間
脅威インテリジェンス	4～6 週間	～10 週間
レッドチームテスト	最低 12 週間	～14 週間
終了フェーズ	～18 週間	～4 週間

（資料）TIBER-EU FRAMEWORK（https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html）、Implementation Guide for CBEST participants（https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf）

DORA に準拠する必要性がなければ、必ずしも最低 12 週とすることが必要であるとは言えないが、長期潜伏や執拗な攻撃などの現実に起こりうるサイバー攻撃手法を想定した TLPT を実施する場合、このペネトレーションテストフェーズには相応の期間を要するということがいえる。金融機関が実際に TLPT を実施する際、テストが数日から 1 週間程度で終わるような場合は、実態としては脆弱性診断やペネトレーションテストのように、予めテストスコープが特定のシステムに限定されていたり、特定の脆弱性を検出することを目的とした手法によって検査が行なわれていたりするケースが多く、TLPT の品質としてみた場合には不十分であることが想定される。この点については、脆弱性診断や一般的なペネトレーションテストと TLPT は区別して考える必要がある。

特定のシステムに対して、予め定義された検査手法に基づく脆弱性の有無や侵入可否を検証することは、脆弱性診断や一般的なペネトレーションテストとしては有効ではあるが、状況に応じて柔軟に攻撃手法を変えてくるような、現実的に起こりうる脅威を想定した疑似的な攻撃による検証であるとは言えず、実効性のある TLPT としては不十分である。結果的にそうした脆弱性診断や一般的なペネトレーションテストのような簡易なテストの実施を TLPT と称して、TLPT を実施して特に問題はなかったことと結論付けることは、経営の意思決定の誤りにつながるものであり、TLPT の実施に当たってはこのレッドチームテストの品質にも留意してテスト実施者を選定する必要がある。

４．７　ブルーチーム評価

TLPT を実施するにあたって重要なポイントのひとつとして、ブルーチーム評価がある。これに関しては「４．２　対象環境」で述べた、実施環境を本番環境とするか否かともあ

わせて検討する必要がある。TLPT の目的、主旨からして、人や対応プロセスの成熟度を評価するうえでは、ブルーチームには事前に予告することなく本番環境にてテストを行い、検知・対応能力の評価が行われることが望ましい。

DORA や TIBER-EU では、ブルーチームへの事前予告なしに TLPT を実施することが明確に規定されている。また、G7 の基礎的要素においても、ブルーチームに事前に知らせることなく実施されることを前提としている。

前述のとおり、TLPT の目的、主旨に照らし合わせると、ブルーチームに予告なしに実施することが必要である。ブルーチームの成熟度が十分なレベルにまで達する過程においては、ブルーチームに予告して実施する、あるいは一部の情報（テスト実施タイミングや攻撃者のアドレス情報など）のみを与えて実施するなど、いくつかの選択肢を以てまずは現状の対応能力の成熟度を評価するというステップを踏むことは有効であると考えられるが、最終的には事前予告なしでテストを実施することで、より高度かつ実効性のあるブルーチーム評価につながると考えられる。

なお、DORA や TIBER-EU では、レッドチームとブルーチームとの協力による組織のサイバー攻撃対応態勢の強化を目的としたパープルチーミングの実施が必須要件として明記されている。このパープルチーミングは、レッドチームテストが終わった後、クロージングフェーズでのテスト結果の振り返りとしてレッドチームとブルーチームが協力して攻撃の詳細、検知状況、ギャップなどを確認しあうプロセスである。これにより、双方の知見を共有してブルーチームの防御力を評価し、その強化を図るとともに、効果的なセキュリティ対策を講じることを目的としている。TLPT の実効性を向上させ、金融機関におけるサイバー攻撃対応態勢の成熟度を向上させるためにも、このパープルチーミングの実施が有効である[10]。

４．８　当局の関与

日本と特に欧州との TLPT の取組みの大きな違いの一つとして、当局の関与という観点がある。日本においては、2.2.1 節で述べてきたように、金融庁では 2023 事務年度、金融機関が実施した TLPT の事例を収集し、好事例や課題を類型化したデータとして還元する取組みや、2024 事務年度には地域金融機関等に対する TLPT 実証事業として、地域金融機関等のうち複数の組織に対して TLPT を実施し、その有用性を実証するという取組みを実施している。また、2.2.2 節で述べたとおり、2024 年に公開した「金融分野におけるサイバーセキュリティに関するガイドライン」では、TLPT を実施するにあたって求められる観点を提示している。

一方で、欧州で先進的に行われているような、当局主導でのフレームワークを整備し、

[10] DORA や TIBER-EU では、テストフェーズでの例外的な措置として、重大なリスク（サービス停止、データ破損、金融セクターへの影響など）を回避する必要がある事態が発生した場合に限定的に行う Limited Purple Teaming についても規定されている。

金融機関が実施する TLPT に対して監督的な立場で関与するというアプローチは採用していない。これはサイバーセキュリティ先進国である米国なども同様であるが、TLPT 実施においては金融機関の自律的な対応を促すとともに、必要な情報の提供等を行う形で当局が支援する形態をとっていると整理できる。

日本の金融機関、特に大手金融機関や地域を代表するような金融機関には、「金融分野におけるサイバーセキュリティに関するガイドライン」の主旨を踏まえ、あるべき姿での TLPT 実施を見据えた対応が求められる。また、当局としても、金融機関が TLPT を実施するにあたって有用な情報の提供などの継続した対応が、国内金融機関における実効性のある TLPT の実施にあたって有効であると考えられる。

５．おわりに

最後に、４章において述べてきた諸外国でのフレームワークやガイドラインを踏まえた考察に加えて、筆者がこれまで TLPT を実施してきた多くの金融機関との対話などを通じて、TLPT を実施するにあたって重要だと考えられるポイントについて 2 点、私見を述べさせていただきたい。

まず 1 点目は「経営層の関与」である。これはサイバーセキュリティ全般にいえることであるが、経営層がサイバーセキュリティをコストではなく投資として捉え、必要かつ十分な経営資源を割り当てて、そのリスクを抑えることが極めて重要である。そのため、現場のセキュリティ担当者は、経営層との間でしっかりと TLPT の意義や必要性について議論し、経営層の関与の下で TLPT を進める必要がある。また、経営層側も自ら積極的に TLPT の実施状況や結果に対してしっかり関与する姿勢を持つことが重要である。さらに、経営層は、TLPT で課題が発見された場合に躊躇なく現場から報告が上がってくる組織文化を築くとともに、現場と経営層との間でコミュニケーションをしっかりとってリスクを共有し、その対策についても必要なコストやリソースを割り当てて経営層主導の下で改善活動を進め、サイバーセキュリティ管理態勢の向上につなげることが極めて重要である。

特に、不十分な品質で実施した TLPT の結果をあるべき TLPT の結果として経営層に報告してしまうと、経営の意思決定を誤る可能性があるため、問題である。例えば、ブルーチームに事前に予告したうえでテストを実施したにも関わらず、そのことを伝えずにただテスト実施者による報告として検知・対応能力の評価が高かったという点だけ伝えることは、サイバー攻撃対応態勢の強化にあたって誤った経営判断が行われる可能性が考えられる。TLPT の実施にあたって制約などがあった場合は、その点もあわせて経営層に報告されるべきである。

なお、この経営層の関与に関して、DORA や TIBER-EU などの主要な海外の規制、フレームワークでは具体的に規定されてはいないが、オランダの ART では、取締役会のメンバーがホワイトチームの一員に含まれることや、脅威、テスト結果および改善計画についての報告並びに、改善計画の実施における関与、支援および説明責任などについて規定して

いる。

2 点目として、「検出事項の横展開」である。TLPT では、例年実施していても毎年同様の課題が検出されてしまうというケースが起こりうる。これは、TLPT を実施している対象システムで検出された課題について、その対象システムの範囲だけで改善を行っても、翌年に別のシステムが対象となって TLPT を実施した場合に同様の課題が検出されてしまうことに起因する。このような事態を防ぐため、特にリスクが高いと評価された検出事項や、他のシステムでも同様の課題が内在しうるような課題（例えば、必要のない高権限の付与や脆弱なパスワード設定、認証情報の不適切な管理など）が TLPT で検出された場合に、その対象システムで改善対応するだけにとどまらず、他のシステムでも同様の課題がないか点検して報告させることで、組織全体としてのリスクを低減させる取り組みを実施することが望ましい。また、単にチェックリストを用いて確認を行い、その結果の報告を求めるだけでなく、ツール等を用いて技術的な検証を他のシステムに横展開することも、より高い実効性が期待できる。TLPT は一般的に高コストであるため実施頻度にも制約が考えられることを踏まえると、TLPT の実施によって得られた教訓は効果的に活用したい。

ここまで述べてきたとおり、TLPT の在り方については各国で様々な見方がある。サイバーセキュリティ管理態勢の成熟度が総じて高いと考えられる大手金融機関、特にグローバルに進出する金融機関においては、DORA や CBEST の対象ともなりうることから、これらの規制を理解し、遵守することが求められるであろう。一方の中小金融機関で、必ずしもサイバーセキュリティ管理態勢の成熟度が十分ではなく、脆弱性診断やペネトレーションテストにおいても高いリスクの検出が数多く発見されるような場合に、いきなり TLPT を実施したとしてもその意義は薄いと考えられる。まずは脆弱性への対応をしっかりと行ってシステムの堅牢性を高めるとともに、成熟したインシデント対応態勢を整備したうえで、最終的には実効性の高い TLPT を実施することで、サイバー攻撃に対する防御態勢のさらなる高度化を目指していくことが望まれる。

本稿では、諸外国の TLPT のフレームワークを参照し、日本の金融機関が TLPT を実施するにあたって留意すべきポイントについて考察してきた。国内金融機関が実効性のある TLPT を実施するにあたって、本稿が役立てば幸いである。

付　表

表 3　本稿で掲載した TLPT に関する規制、フレームワーク等（発行、改訂年順）

名称	国/地域	発行/ 最終改訂年
iCAST (Intelligence-led Cyber Attack Simulation Testing)	香港	2016 年
G7 Fundamental Elements for Threat-Led Penetration Testing	G7	2018 年
FEER（Financial Entities Ethical Red-Teaming Framework）	沙国	2019 年
金融機関等における TLPT 実施にあたっての手引書	日本	2019 年
A Framework for Threat-Led Penetration Testing in the Financial Services Industry	GFMA (業界団体)	2020 年
CORIE（Cyber Operational Resilience Intelligence-led Exercises）	豪州	2022 年
STAR-FS（Simulated Targeted Attack & Response for the Finance Sector）	英国	2024 年
ART（Advanced Red Teaming Framework）	蘭国	2024 年
AASE（Adversarial Attack Simulation Exercise Guidelines for the Financial Industry in Singapore）	星国	2024 年
金融分野におけるサイバーセキュリティに関するガイドライン	日本	2024 年
CBEST（Critical National Infrastructure Banking Supervision and Evaluation Testing）	英国	2024 年
DORA（Digital Operational Resilience Act）	EU	2025 年
TIBER-EU （European Red Team Testing Framework）	EU	2025 年

参考文献

金融情報システムセンター (2019),「金融機関等における TLPT 実施にあたっての手引書」
（https://www.fisc.or.jp/publication/book/004197.php）
金融庁 (2018),「脅威ベースのペネトレーションテストに関する G7 の基礎的要素」
（https://www.fsa.go.jp/inter/etc/20181015/02.pdf）
金融庁 (2024),「金融機関のシステム障害に関する分析レポート」
（https://www.fsa.go.jp/news/r5/sonota/20240626/20240626.html）
金融庁 (2018),「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組方針 Ver.2.0」
（https://www.fsa.go.jp/news/30/20181019-cyber.html）
金融庁 (2022),「同 Ver.3.0」
（https://www.fsa.go.jp/news/r3/cyber/torikumi2022.html）
金融庁 (2024),「金融分野におけるサイバーセキュリティに関するガイドライン」
（https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf）
金融庁 (2018),「諸外国の「脅威ベースのペネトレーションテスト（TLPT）」に関する報告書」
（https://www.fsa.go.jp/common/about/research/20180516/TLPT.pdf）

The Association of Banks in Singapore (2024), “Adversarial Attack Simulation Exercises 2.0”
（https://www.abs.org.sg/docs/library/abs-red-team-adversarial-attack-simulation-exercises-guidelines----september-2024.pdf）
Bank of England, “CBEST Threat Intelligence-Led Assessments”
（https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide）
Bank of England, “Implementation Guide for CBEST participants”
（https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf）
Bank of England (2024), “STAR-FS UK Implementation Guide”
（https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/star-fs-implementation-guide-march-2024.pdf）
Council of Financial Regulators, Australia (2022), “Cyber Operational Resilience Intelligence-led Exercises (CORIE) Framework Ver.2.0”
（https://www.cfr.gov.au/publications/policy-statements-and-other-reports/2022/revised-corie-framework-rollout/pdf/corie-framework.pdf）

European Central Bank, “TIBER-EU FRAMEWORK”
（https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html）
European Insurance and Occupational Pensions Authority, “Digital Operational Resilience Act (DORA)”
（https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en）
Global Financial Markets Association (2020), “A Framework for Threat-Led Penetration Testing in the Financial Services Industry”
（https://www.gfma.org/wp-content/uploads/2020/12/gfma-penetration-testing-guidance-for-regulators-and-financial-firms-version-2-december-2020.pdf）
Hong Kong Monetary Authority, “Intelligence-led Cyber Attack Simulation Testing (iCAST)”
（https://www.hkma.gov.hk/eng/data-publications-and-research/guide-to-monetary-banking-and-financial-terms/iCAST/）
De Nederland Bank (2024), “Advanced Red Teaming (ART) Framework”
（https://www.dnb.nl/media/cxjjcc4b/art-framework-april-2024.pdf）
Saudi Arabian Monetary Authority (2019), “Financial Entities Ethical Red-Teaming”
（http://sama.gov.sa/en-US/Laws/BankingRules/Financial%20Entities%20Ethical%20Red%20Teaming%20Framework.pdf）

金融庁金融研究センター

〒100-8967　東京都千代田区霞ヶ関 3-2-1
中央合同庁舎 7 号館　金融庁

TEL：03-3506-6000

URL：https://www.fsa.go.jp/frtc/index.html