TLPT（レッドチーム演習）
ビジネストレンド・事例分析レポート

Librus株式会社
コンサルティングサービス事業部

エグゼクティブサマリー

TLPT（Threat-Led Penetration Testing）は、金融機関のサイバーレジリエンス強化における重要な施策として、欧州DORA規制の導入により2025年から本格的な義務化が開始される。市場規模は2024年の4,042百万ドルから2031年には9,145百万ドルへと拡大が予測される一方、専門人材不足と高い実装コストが業界課題となっている。アジア太平洋地域では日本、シンガポール、香港、オーストラリアが独自の枠組みを構築し、グローバルな標準化と相互認証の推進が進んでいる。

1. TLPTの定義と概要

1.1 TLPTの基本概念

TLPT（Threat-Led Penetration Testing）は、実際の攻撃者の戦術、技術、手順（TTP：Tactics, Techniques, and Procedures）を模倣し、金融機関の重要なライブ本番システムに対して制御された形でのレッドチーム演習を実施する高度なサイバーセキュリティテスト手法である。従来のペネトレーションテストとは異なり、脅威インテリジェンスに基づいた現実的な攻撃シナリオを用いて、組織の「人・プロセス・技術」の全領域にわたる耐性を評価する。

1.2 従来のセキュリティテストとの差異

TLPTの特徴は以下の通りである：

- 脅威インテリジェンスに基づく現実的な攻撃シナリオの採用
- 本番環境でのテスト実施による実際の運用影響の評価
- 物理的侵入、ソーシャルエンジニアリング、サイバー攻撃の複合的アプローチ
- ブルーチーム（防御側）への事前通知なしでの実施
- パープルチーミング（攻撃・防御側の合同検証）による改善プロセス

2. 規制動向とDORA要件

2.1 DORA規制の概要

EU デジタル運用レジリエンス法（DORA）は2025年1月17日に施行され、EU域内の金融機関に対してICTリスク管理、インシデント報告、デジタル運用レジリエンスのテスト、ICTサードパーティリスク管理、情報共有の5つの柱からなる包括的な要件を課している。その中でTLPTは最も高度なテスト要件として位置づけられている。

2.2 TLPT適用対象機関

DORA規制技術基準（RTS）により、以下の金融機関がデフォルトでTLPT実施義務を負う：

- グローバルシステム上重要銀行（G-SII）・国内システム上重要銀行（O-SII）認定信用機関
- 年間1,500億ユーロ超の決済取引を処理する決済機関
- 年間1,500億ユーロ超の決済取引または400億ユーロ超の電子マネー発行を行う電子マネー機関
- 中央証券保管機関（CSD）
- 中央清算機関（CCP）
- 市場シェア基準を満たす取引会場
- 総保険料5億ユーロ超等の基準を満たす保険・再保険会社

2.3 実装要件と実施頻度

主要要件

- 最低3年に1回の実施義務（監督当局判断で頻度調整可能）
- 3回に1回は外部テスター必須使用
- 最低12週間のアクティブレッドチーミング期間
- 本番環境での実施
- 脅威インテリジェンスプロバイダーは外部必須
- パープルチーミングの実施義務

3. 市場動向と成長予測

3.1 グローバル市場規模

TLPTサービス市場は急速な成長を示している。2024年の市場規模は4,042百万ドルから、2031年には9,145百万ドルに達すると予測されている。年平均成長率（CAGR）は約12.6%と高い成長率を維持している。この成長の主要因は以下の通りである：

- DORA等の規制要件によるTLPT義務化の拡大
- サイバー攻撃の高度化・複雑化への対応需要
- 金融機関における実践的セキュリティテストの重要性認識の高まり
- デジタル変革とクラウド移行に伴うリスク評価ニーズの拡大

3.2 市場の課題

急速な市場成長の一方で、重要な構造的課題が存在している:

3.2.1 専門人材不足

TLPTの実施には高度な専門性が求められるが、欧州監督機関（ESA）の調査によると、「TLPTやレッドチーミングは比較的新しい産業分野であり、既に小規模な市場がさらなる要件により縮小されている」状況である。具体的には

- 外部テスターには5年以上の経験を持つマネージャーと2年以上の経験を持つ2名以上のチームメンバーが必要
- 過去5件以上のTLPT類似案件の実績が要求される
- 脅威インテリジェンス専門家の絶対数が不足

3.2.2 実装コストの上昇

専門人材不足により、TLPTサービスの価格は上昇傾向にある。特に以下の要因がコスト押し上げに寄与している

- 高度な専門性を持つ人材への高額報酬
- 本番環境でのテスト実施に伴う高リスクプレミアム
- 複雑な調整・管理プロセスによる工数増加
- 最低12週間という長期間の実施要件

4. アジア太平洋地域の取組み

4.1 日本の動向

4.1.1 金融庁の取組み

日本では2018年以降、金融庁が「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」の下で大手金融機関にTLPTの実施を要求している。2023年度には165の金融機関が参加する「金融業界横断的なサイバーセキュリティ演習（Delta Wall VIII）」を実施し、実践的な対応能力の向上を図っている。

4.1.2 実装状況と課題

KPMGの調査によると、日本の金融機関の8割以上がTLPTを実施済みまたは実施予定である一方、地域金融機関では「コスト負担増やシステムへの影響を懸念して予算化のメドが立たない」状況が課題となっている。

4.2 シンガポールの枠組み

4.2.1 ABS-AASE Framework

シンガポール銀行協会（ABS）は2018年に「Red Team: Adversarial Attack Simulation Exercise Guidelines」を策定し、金融機関向けの包括的なレッドチーム演習ガイドラインを提供している。2024年9月には最新版が発行され、より実践的な要件が整備されている。

4.2.2 MAS規制との連携

シンガポール金融管理庁（MAS）のTechnology Risk Management Guidelinesと連携し、銀行・保険・投資会社に対する段階的なサイバーレジリエンス要件を設定している。

4.3 香港の取組み

4.3.1 Cybersecurity Fortification Initiative (CFI)

香港金融管理局（HKMA）は2016年12月にCFIを開始し、2020年にはCFI 2.0にアップグレードしている。同イニシアチブには以下の要素が含まれる：

- Intelligence-Led Cyber Attack Simulation Testing (iCAST)
- Professional Development Programme
- Cyber Resilience Assessment Framework
- Cybersecurity Information Sharing Platform

4.4 オーストラリアの規制

4.4.1 APRA CPS 230

オーストラリア健全性規制庁（APRA）は2025年7月から適用されるCPS 230「Operational Risk Management」において、規制対象機関に対する定期的なペネトレーションテストと第三者リスク管理を義務化している。年次ベースでのテスト実施と重要なシステム変更後の追加テストが要求されている。

5. 実装事例と成功要因

5.1 欧州大手銀行の事例

5.1.1 実装アプローチ

欧州の大手銀行では、DORA施行に先立ちTIBER-EU フレームワークに基づくTLPTを実施している。成功要因として以下が挙げられる：

- 経営層の強いコミットメントと予算確保
- 専任のControl Team（ホワイトチーム）の設置
- 外部専門プロバイダーとの長期パートナーシップ構築
- 段階的なスコープ拡大による経験蓄積

5.2 アジア太平洋地域の先進事例

5.2.1 三菱UFJ銀行のケース

三菱UFJ銀行は2024年にCrowdStrikeのレッドチーム演習を採用し、顧客環境や問題に合わせたカスタマイズされたテストを実施している。複数のセキュリティベンダーの提案を評価した結果、実効性の高いアプローチを選択している。

6. 技術・運用上の課題と対策

6.1 主要課題の分析

TLPTの実装において、以下の技術・運用課題が共通して確認されている

分類	課題	主な対策
ガバナンス	セキュリティ部門の立場が弱く、施策実施が停滞	セキュリティ戦略の検討・実装・振り返りサイクルの組織文化醸成
識別	CSIRTがネットワーク・システム全体像を把握不足	インシデント対応を見据えた全容把握に向けた情報整理の施策化
防御	クラウド利用・ゼロトラスト化による外部抜け道の発生	セキュリティ観点での設計見直し、要件定義段階からの専門家関与
検知	疑似攻撃に対してアラートが期待通りに上がらない	TLPT等の効果測定推進、多層的検知態勢構築
対応	正常性バイアスによるアラート看過、初動遅れ	TLPT等の実践的訓練による危機感醸成、重要スキル者への人事制度措置

6.2 リスク管理要件

本番環境でのTLPT実施には固有のリスクが伴うため、厳格なリスク管理が要求される：

- テスト実施前のリスク評価と継続的監視
- 緊急停止手順（Kill Switch）の整備
- 業務継続性への影響最小化措置
- データ保護・機密性確保の徹底
- インシデント発生時の迅速な復旧体制

7. 市場機会と将来展望

7.1 新興市場機会

7.1.1 中小金融機関市場

現在はコスト面で導入が困難な中小金融機関向けに、簡易版TLPTやクラウドベースソリューションの需要が高まっている。コンソーシアム型の共同実施や標準化されたテストパッケージの開発が市場機会として期待される。

7.1.2 業界横断的展開

金融業界で蓄積されたTLPTのノウハウは、他の重要インフラ業界（エネルギー、通信、交通）への横展開が予想される。特に供給連鎖リスクの観点から、業界を超えた連携テストの需要が拡大している。

7.2 技術革新の影響

7.2.1 AIと自動化

人工知能技術の活用により、以下の領域での革新が進んでいる

- 脅威インテリジェンスの自動収集・分析
- 攻撃シナリオの自動生成
- テスト結果の自動評価・レポート生成
- 継続的セキュリティ評価プラットフォーム

7.2.2 クラウドネイティブTLPT

クラウド環境に特化したTLPTツールとサービスの開発が加速している。コンテナ化された攻撃ツール、オンデマンドテスト環境、クラウドセキュリティポスチャ管理（CSPM）との連携が主要な技術トレンドとなっている。

7.3 グローバル標準化の進展

TIBER-EU、CBEST（英国）、TIBER-NL（オランダ）等の地域フレームワークの相互認証と標準化が進展している。ISO/IEC 27001、NIST Cybersecurity Frameworkとの整合性確保により、多国籍金融機関での効率的なTLPT実施が可能になっている。

8. 結論と提言

8.1 主要所見

TLPTは金融業界のサイバーセキュリティ対策において、従来の守りのセキュリティから攻めのセキュリティへのパラダイムシフトを象徴する取組みである。DORA規制により欧州で本格化するTLPT義務化は、グローバルな金融機関のサイバーレジリエンス向上に重要な役割を果たすことが期待される。

一方で、専門人材不足、高コスト、技術的複雑性といった課題は短期的には解決が困難であり、段階的なアプローチと産業界全体での能力構築が必要である。

8.2 金融機関への提言

1. 早期準備の開始:TLPT義務化を待たず、内部体制整備と外部パートナー選定を早期に開始すべきである。
2. 段階的スコープ拡大:重要度の高いシステムから順次TLPT対象を拡大し、組織の習熟度を高めるアプローチが効果的である。
3. 業界協力の推進:コンソーシアム型共同実施や知見共有により、コスト削減と品質向上を同時に実現すべきである。
4. 継続的改善体制の構築:TLPTを一過性のイベントとせず、継続的なサイバーレジリエンス向上のプロセスに組み込むべきである。

8.3 今後の展望

TLPTは2025年以降、金融機関の標準的なサイバーセキュリティ対策として定着することが予想される。技術革新と市場成熟により、より効率的で実効性の高いTLPTソリューションが登場し、中小金融機関への普及も進むと考えられる。また、国際的な標準化と相互認証の進展により、グローバル金融システム全体のサイバーレジリエンス向上に寄与することが期待される。

主要参考資料*:*

- *European Banking Authority, "Final Report - Draft Regulatory Technical Standards on TLPT", July 2024*
- *Deloitte, "Threat-Led Penetration Testing: A proactive approach to cybersecurity", 2024*
- *KPMG Japan, "*金融機関における脅威ベースのペネトレーションテストの動向*", October 2024*
- *Association of Banks in Singapore, "Red Team: Adversarial Attack Simulation Exercises Guidelines", September 2024*
- *Market Monitor Global, "Threat Led Penetration Testing Service Market Global Outlook", 2024*
- 金融庁, "金融業界横断的なサイバーセキュリティ演習(*Delta Wall* Ⅸ)", *2024*

監修者:
鎌田光一郎:青山学院大学法学部卒業。SMBC日興証券株式会社にて証券営業、経営管理業務に従事したのちPwCコンサルティンク゛合同会社に転籍。金融機関に対するコンサルティンク゛業務に従事。その後、Librus株式会社を設立、代表取締役に就任。

お問い合わせ先
Librus株式会社(代表取締役 鎌田光一郎)
105-0004東京都港区新橋6丁目13-12 VORT新橋Ⅱ 4F
03-6772-8015
お問い合わせフォーム
https://librus.co.jp/contact