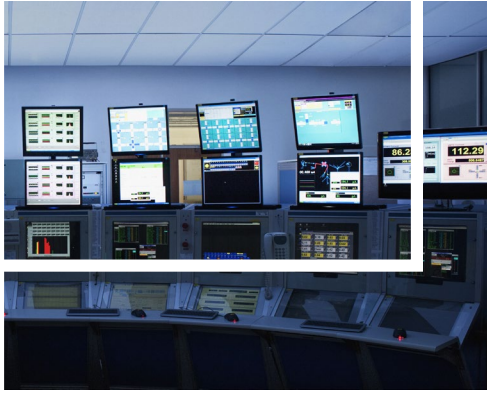
脅威ベースのペネトレーションテスト（TLPT）実践からの示唆

新たな段階に入った金融機関のTLPTの実践



PwCあらた有限責任監査法人　シニアマネージャー 小林 由昌

TLPT普及までを振り返る

G7のサイバー・エキスパート・グループが「Fundamental Elements for Threat-Led Penetration Testing（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）」*1を公表してから2年が経とうとしています。日本の金融分野において「TLPT」という言葉はもはや珍しいものではなく、広く認知された言葉となりました。

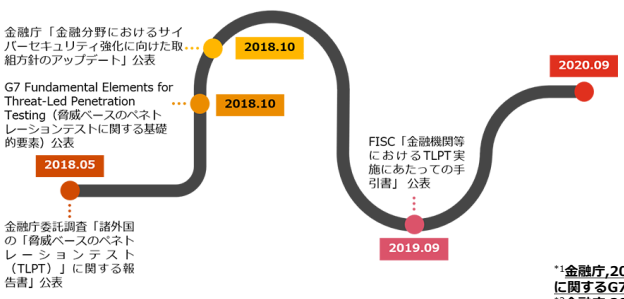
最初にこのキーワードが我が国で利用されたのは、2018年5月に金融庁が公表した「諸外国の『脅威ベースのペネトレーションテスト（TLPT）』に関する報告書」だと言われています。当報告書の作成は、金融庁から委託を受けたPwCあらた有限責任監査法人（以下、PwCあらた）が担当しました。*2

当該報告書が公表された直後は、聞き慣れない言葉であることや本番システムにサイバー攻撃を仕掛けるテストという刺激的な内容であったことから、金融機関のセキュリティ担当者からは驚きの声と共に、TLPTのコンセプトや海外金融機関での活動実態、活用効果などについて数多くの問い合わせをいただきました。

しかしながら、同年10月には、上述のG7の基礎的要素が金融庁および日本銀行を通じて公表され、TLPTが国際的なコンセンサスを得た、サイバーレジリエンス向上のために有効である手法であることが示されました。

また、同時に金融庁が公表した「『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』のアップデートについて」*3でもTLPTの有効性が評価され、大手金融機関に対し、サイバーセキュリティの高度な評価手法として活用を促していく旨が示されました。

図1：国内金融分野におけるTLPT普及までの流れ



こうした一連の動きが後押しとなってTLPTは浸透し、活用が広がっていきています。図1に普及までの流れをまとめました。

FISCによるTLPT実施の手引書の公表

上述した動きと共に、大手金融機関ではTLPTの活用が広がり始めました（図2にTLPTの特徴と主な効果をまとめています）。しかし、2019年9月に金融情報システムセンター（FISC）が「金融機関等におけるTLPT実施にあたっての手引書*4」（以下「TLTP実施の手引書」）を公表するまで、国内にはTLPTの具体的な実施手順や基準を体系的かつ実践的に示した文書はありませんでした。したがって、多くの金融機関はコンサルティング会社からの情報や英国中央銀行のCBEST*5、欧州中央銀行のTIBER-EU*6などのフレームワークを参考にしながらTLPTを実施していきました。

ただし、これらのフレームワークは金融当局主導で整備されていることから当局連携が強く意識されているほか、我が国の金融機関からするとTLPT実施に関する周辺の環境整備状況や企業の組織文化の違いもあり、そのまま適用することや実施に際して経営陣の理解を得ることが難しい面も多々ありました。

その点、FISC公表のTLTP実施の手引書は、我が国の金融機関での活用が前提となっており、例えば、情報システムの外部委託が多いことを踏まえた留意点や、金融機関のバイブルとも言えるFISCの安全対策基準との関係性が示されています。またTLPTにおける経営陣の役割を明確に示すなどし、大手金融機関はもとより、中小地域金融機関やその他多様な金融機関がTLPTの活用に一歩を踏み出すよい材料と契機になったものと考えています。

加えて当該手引書の策定においては、PwCあらたを含めたいくつかのプロバイダー企業が策定のための検討部会に参画し、FISCや金融業界と共同で作り上げたため、テストプロバイダー市場の育成・拡大の観点あるいは適切な品質と価値を提供できるTLPTプロバイダーを選定することの重要性などにも触れられており、結果としてテストプロバイダー市場の拡大にも寄与しています。

*1 金融庁,2018年10月15日,「『脅威ベースのペネトレーションテスト』及び『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G7の基礎的要素の公表について」
*2 金融庁,2018年5月16日,「諸外国の『脅威ベースのペネトレーションテスト（TLPT）』に関する報告書の公表について」
*3 金融庁,2018年10月19日,「『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』のアップデートについて」

サイバー脅威の増大によりすそ野が広がる金融機関のTLPT

このようなTLPTの実践環境の整備と期待の高まりに加えて、①金融サービスのアンバンドリングに代表されるモバイル決済やオープンエコノミー市場の拡大、②新型コロナウイルス感染症（COVID-19）に伴うリモートアクセスの増加、などに伴うサイバー脅威の増大によって、金融分野ではTLPT活用のすそ野が大きく広がる傾向にあります。

例えば、TLPTの実施を毎年のPDCA活動に組み込む金融機関や、TLPTに欠かせないレッドチーム部隊を内製化する検討を始めた金融機関も出てきています。また、グループ子会社で横断的にTLPTを実施するなど、金融持株会社のグループサイバーガバナンスの発揮の手段としてTLPTを採用している事例も見られます。

これらは大手金融機関の事例ですが、それ以外にもインターネット経由の金融サービスを主戦場とするオンライン銀行や証券、カード会社あるいは資金移動業者などでもTLPTの活用が始まっています。2019年11月、PwC Japanグループが開催したPwC's Digital Trust Forum 2019では、TLPTを活用して効果を実感されたGMOクリック証券様にご登壇いただきました。

多様化するサイバーリスクに対処するには、従来型のリスクマネジメントのみでは、サイバーの脅威や脆弱性に対処することが難しくなっています。こうした多くの金融機関の活用事例は、TLPTの価値が広く金融分野で認知された証であり、今後は中小地域金融機関や暗号資産交換業者などを含め、さらに活用のすそ野も広がっていくことが予想されます。

本質的で効果的なTLPTでなければ価値がない

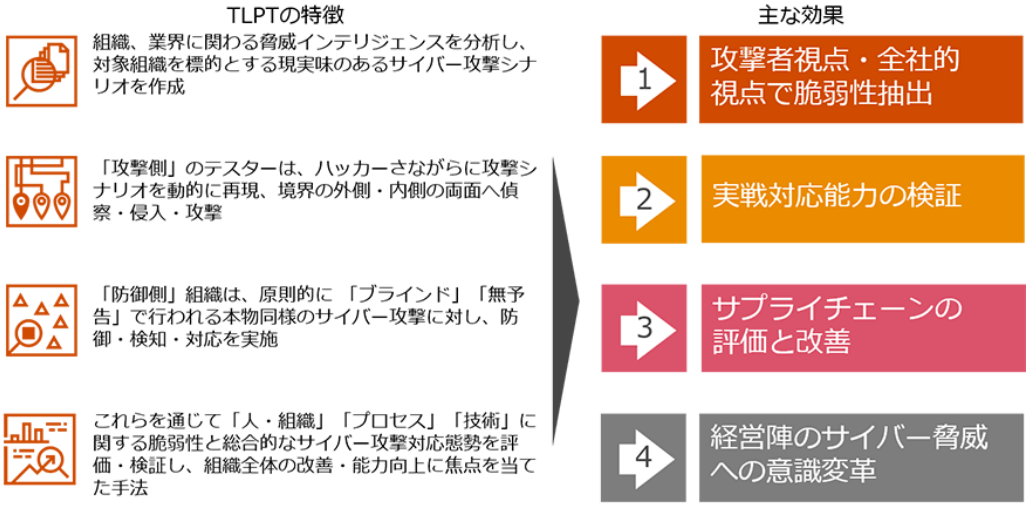
「TLPTを実施したい」。そうした声を聞く機会が増えていますが、実施にあたっては、その目的や期待する効果をしっかりと検討することが必要です。FISC公表の「TLTP実施の手引書」ではCBESTやTIBER-EU同様、当局連携にも言及していますが、その内容は極めて限定的です。TLPTの実施について金融当局が深く関与することは想定されていません。これは、当局報告のためのTLPTの実施では意味がなく、本質を捉えた効果的なTLPTの実施が金融機関に期待されていることに他なりません。言い換えれば、TLPTの活用を通じて金融機関は「人・組織」「プロセス」「技術」におけるセキュリティの価値を高め、企業体のレジリエンスの向上につなげること、ひいてはこうしたセキュリティ活動を企業文化の一部に定着させていくことが今後の金融機関には求められています。

こうしたアジェンダに対応するためも、金融機関にとっては、効果的で価値あるTLPTをいかに実現するかを十分に検討した上で実施することが重要となります。PwCは数多くのTLPT実施経験と、前述の金融庁向け調査報告業務などを通じたTLPTの知見や洞察を有しています。今後の連載の中でそうしたポイントを取り上げ、紹介していきたいと思います。

次回は、攻撃シナリオ策定のカギを握るスレットインテリジェンスの活用について取り上げる予定です。

*4金融情報システムセンター,2019年,「金融機関等におけるTLPT実施にあたっての手引書【PDF版】」
*5BANK OF ENGLAND, 'Financial sector continuity（2020年8月20日閲覧）
*6EUPEAN CENTRAL BANK, 'What is TIBER-EU?（2020年8月20日閲覧）

図2：TLPTの特徴と主な効果



お問い合わせ

PwC Japanグループ
〒100-6921　東京都千代田区丸の内2-6-1 丸の内パークビルディング
Tel：03-6250-1200（代表）　Mail：jp_cyber_inquiry@pwc.com