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

2018 年(平成 30)年 1 月 31 日

■目次

■ 1. 調査の概要

1.1. 調査の背景

近年のテクノロジーの急速な進展とデジタル化に伴い、サイバー攻撃が多様化、巧妙化するとともに、執拗さも増しており、潜在的なサイバー攻撃の脅威は急速に進展している。インターネットを介して世界がつながっている現在、サイバーセキュリティの強化に向けたたゆまぬ努力が必要なことは言うまでもない。

このような外部環境の変化を受けて、金融機関は様々なセキュリティ強化に向けた対策、取り組みを行っており、本調査である「脅威ベースペネトレーションテスト」も今後普及していく取り組みの一つと考えられる。

ペネトレーションテストとは、一般的には、Web インターフェースを有するシステムへの擬似的な攻撃により、主に技術的な脆弱性の有無を調査するためのテストであり、従来から金融機関を含む多くの企業で広く活用されている。最近では、さらに高度な手法として、対象企業が抱える脅威やリスクを個別具体的に分析したうえで、ハッカーが採用する戦術、手法を再現して擬似的な攻撃を仕掛けることで、侵入・改ざんの可否や検知の可否、対応の迅速性・適切性を検証する、より実戦的なテストが行われている。

こうしたテストは「脅威ベースペネトレーションテスト」と呼ばれており、サイバー攻撃に対する有効な評価手法の一つになってきている。英中央銀行で導入された CBEST を始め、欧州（欧州中央銀行）や香港でも、当局が主導する形でこのテストのフレームワークを構築する動きがある。

2017 年 5 月にイタリア・バーリで開催された G7 財務大臣・中央銀行総裁会議の共同声明においても、ペネトレーションテストの活用については、次のような言及がなされている。[1]

「急速に進展するサイバー脅威の性質を踏まえ、サイバーセキュリティの評価を効果的なものとするためには、現在の評価手法を、定期的なサイバー演習やシミュレーション、最も効果的にペネトレーションテストを活用する方法の検討も含め、サイバーの強靱性向上に即した慣行によって強化、補完することが求められる。」

他方、このテストは、原則として本番環境に擬似攻撃を行い、無予告で実施する実戦形式であることから、情報管理や稼働中のシステムへの影響等のおそれが指摘されている。

金融庁では、2016 年より机上演習の金融業界横断的な演習「DeltaWall」を実施しているが、世界的に、当局主導で脅威ベースペネトレーションテストのフレームワークが導入されていることに鑑み、今後の取り組みの参考として、諸外国の動向や先行事例を把握しておく必要がある。

[1] https://www.mof.go.jp/international_policy/convention/g7/cy2017/g7_170513.htm

1.2. 調査の目的

本調査の目的は、諸外国の金融当局、金融機関等における「脅威ベースペネトレーションテスト」の活用に関する取り組みから、今後の日本の金融分野における当該テストの活用に向けた参考となる情報を得るとともに、日本において、仮に金融当局が関与する形で「脅威ベースペネトレーションテスト」のフレームワークを検討する場合に、考慮すべき点を海外の先行事例を通じて把握することである。中でも英国においては、当局が主導する形で「CBEST フレームワーク」が導入されており、「脅威ベースペネトレーションテスト」が浸透している。そのため、英国をはじめとする当局、金融機関、テストプロバイダー等に直接インタビューを実施し、参考となる事例や、その効果あるいは諸課題を収集することにより、その取り組みの実態を把握する。

1.3. 調査期間

2017 年(平成 29 年)11 月 27 日(月)～2018 年(平成 30 年)1 月 30 日(火)

1.4. 調査の対象

海外(米国、英国、ECB、シンガポール、香港)における金融当局、関係事業者

1.5. 調査項目

本調査では、以下の項目について調査を行った。

1) 海外(米国、英国、ECB、シンガポール、香港)で提供されているペネトレーションテストの概要(実施主体、テストの詳細、費用、金融機関の活用状況)

2) 調査対象国のうち、当局が関与している脅威ベースペネトレーションテストに関するフレームワーク、実施手順(実施根拠、実施期間、テスト実施者(英国においては実施者の設定基準)、テスト範囲、対象となる金融機関の基準、実施環境、テスト結果のフィードバック、テスト結果の活用状況)

3) ペネトレーションテストに関して指摘されている課題(テスターの確保、情報管理、システムへの影響や事務負担)とそれに対する対応策

1.6. 調査手法

本調査では、公表されている文献(インターネットサイトに掲載された情報を含む)の調査のほか、金融当局、関係事業者へのヒアリングやアンケートを実施し、これらの結果を PwC あらた有限責任監査法人が取りまとめ、報告書を作成した。

なお、主なヒアリングおよびアンケートの対象先は以下のとおり。

- 海外の金融当局
- 米国に本部を置く大手金融機関
- 英国に本部を置く大手金融機関
- サービスプロバイダーに対し資格認定制度を提供している機関
- 米国、英国、香港、シンガポールのサービスプロバイダー

1.7. 調査の前提条件

本調査、および本報告書は、金融庁と PwC あらた有限責任監査法人との間で締結した平成 29 年 11 月 22 日付のアドバイザリー・サービス契約書に基づき実施、作成されたものであり、また、委託元である金融庁担当職員の指示のもとで実施、作成されている。

本報告書は、調査を通じて得られた情報をもとに作成されている。本調査は上記「1.6.調査の方法」に記載したとおり、公表されている文献、記事等の閲覧、および本調査テーマに関連のある機関や関係者へのヒアリングおよびアンケートを通じて実施した。そのため報告書には、調査対象とした文献の作成者や、ヒアリングやアンケートの対象先である個人および組織による私見や経験に基づく内容が含まれている。また、報告書には、本調査を通じて得られた情報をもとに、報告書の作成を担当した当法人執筆者による見解および考察が含まれている。

当法人は、本報告書内に記載されたそれらの内容について如何なる意見表明や証明を行うものではなく、保証を行うものでもない。また、本報告書は上述した調査期間に収集した情報をもとに作成されており、報告書の内容に将来の事象が含まれている場合には、その将来の事象の実現可能性や信頼性を保証するものではない。

■ 2. 脅威ベースペネトレーションテストについて

2.1. 概要

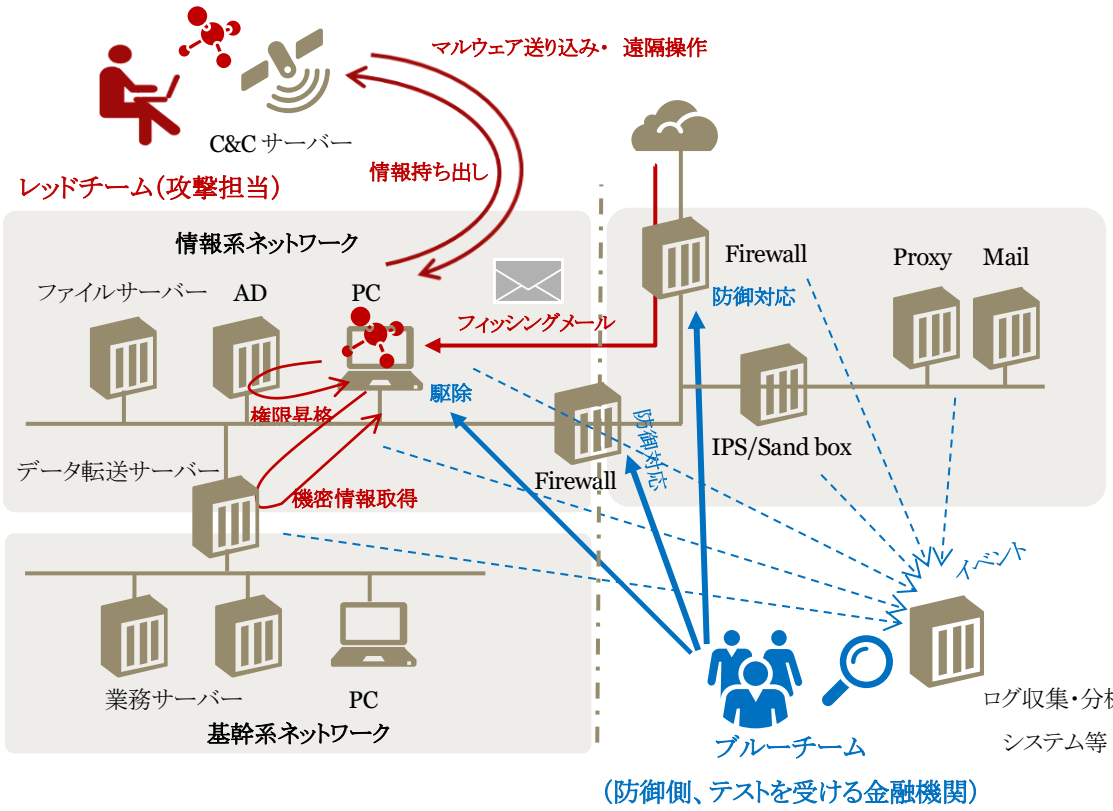
「脅威ベースペネトレーションテスト」は、従来から活用されている一般的なペネトレーションテストや脆弱性スキャンと大きく異なる性質を持っている。そこで本章では、「脅威ベースペネトレーションテスト」には、どのような特徴があり、従来の手法と何が異なるかなど、本報告書の前提として、「脅威ベースペネトレーションテスト」について述べる。

2.2. 脅威ベースペネトレーションテストとは

2.2.1. テスト概要

「脅威ベースペネトレーションテスト」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、対応を行う。それを通じて金融機関のサイバー攻撃対応態勢を評価し、対応能力を高めていくことに焦点をあてたテストである。以下がイメージ図である。

図 2-1 脅威ベースペネトレーションテストのイメージ



なお、脅威ベースペネトレーションテストは、英語では「Threat-Led Penetration Test」「Threat Intelligence-led Penetration Test」「Threat-based Penetration Test」「Threat Intelligence-based Penetration Test」等と記載されることがあるが、本報告書では「TLPT（Threat-Led Penetration Test）」とする。

2.2.2. テスト実施に関わるステークホルダー

TLPT には、一般的に以下のようなステークホルダーが存在する。

a）テスト対象組織

TLPT を実際に受ける銀行等の金融機関である。なお、金融機関の情報システムにかかる運用管理業務や SOC（Security Operation Center）業務等は外部委託されているケースもあり、そのような場合は、外部委託先もテスト対象組織に含まれる。

b）サービスプロバイダー

TLPT を実施する場合、テスト対象組織は、脅威インテリジェンスプロバイダー（Threat Intelligence Provider、以下「TI」）とペネトレーションテストプロバイダー（Penetration Test Provider、以下「PT」）を活用する。これらのサービスは、サイバーセキュリティ関連企業やコンサルティングファームによって提供されているケースが多いが、両サービスをワンストップで提供している企業もある。

1） 脅威インテリジェンスプロバイダー（TI）

TI は、テスト対象組織あるいは組織が属する業界が潜在的にどのようなサイバー攻撃の脅威にさらされているかについて情報収集・分析を行い、レポートを作成する（詳細は 3.3 章にて述べる）。当レポートはテスト対象組織がテストで利用する脅威シナリオを検討する際の基礎となる。脅威インテリジェンスにはテスト対象組織からの情報も含まれるが、多くはオープンソースから収集された情報を基に、攻撃者の目線で分析することが必要となる。そのため、TI には最新の脅威動向に関する情報を広く収集し分析、評価する経験と専門性が必要となる。

2） ペネトレーションテストプロバイダー（PT）

PT は、TI が作成した脅威インテリジェンスレポート等を基に、脅威シナリオを作成し、テスト対象組織に擬似攻撃を仕掛ける。防御システムを突破し、検知されることなくシステム内部へ侵入するための俊敏性や技術力が必要になるとともに、対象組織が潜在的に有する脆弱性や問題点を適切に識別するための洞察力が必要となるため、こちらも専門的な能力が必要となる。

c）その他ステークホルダー

TLPT を当局が主導する場合は、上記に加え、当局がステークホルダーとなる。詳細は 4 章で述べる。

2.2.3. TLPT の特徴

TLPT には、明確な定義はないが、2017 年 11 月に金融庁より公表された「金融行政方針」[2]では、TLPT（脅威ベースペネトレーションテスト）について以下のように解説されている。

「テスト対象企業ごとに脅威の分析を行い、個別にカスタマイズしたシナリオに基づく実践的な侵入テスト」

また、当該テストが比較的普及している米英では、以下のような特徴がある。

- TLPT は、現実世界で実際に起きている攻撃を動的にシミュレーションし、サイバー攻撃による侵害に対処するための攻撃対応能力を高めることに焦点をあてたテストである。従って、テストでは実機を用い、原則として本番環境で実施される。
- 具体的には、レッドチームと呼ばれる攻撃側（＝PT）が、脅威シナリオをベースに対象組織に攻撃を仕掛ける。レッドチームはハッカーさながらに洗練した攻撃技術を駆使し、境界防御の内側に侵入、潜伏し続けながら、検知されることなく攻撃目的を達成する。一方、ブルーチームと呼ばれる防御側（＝テスト対象組織）は、レッドチームが仕掛けるサイバー攻撃に対して現実のサイバー攻撃同様に、防御、検知、対応を攻撃内容に応じて実施する。この一連の攻防をシミュレーションすることで、サイバーキルチェーンの各段階でどのような攻撃を許してしまうおそれがあるかを明らかにする。
- 脅威シナリオは、オープンソース等から収集・分析された脅威インテリジェンスをもとに作成される。個々の企業や業界の特性を踏まえ、現実に直面するおそれのあるサイバー攻撃を分析（攻撃者はどのような集団か、攻撃目的は何か、どのような技術や手法を使用するか）し、具体的なシナリオが用意される。
- テスト実施後は、レッドチームの様々なサイバー攻撃に対してブルーチームがどのような方法やタイミングで防御、検知、対応できたのか、また、技術面の脆弱性のみならず、人・組織、プロセスにおいてどのような脆弱性、課題があったのかを検証し、今後の改善につなげていく。

2.2.4. レッドチームテスト

TLPT と同様に使われる用語としてレッドチームテストやレッドチーム演習（以下「レッドチームテスト」）があるが、一般的には TLPT と同様の意味合いで用いられることが多く、本調査においても同一のものとしている。

ただし、レッドチームテストにおいても、TLPT 同様にシナリオベースのテストなのか、当該シナリオが対象組織や業態に対する昨今の脅威動向を踏まえたものなのか等によって、同義と捉えられる程度が異なる。

オランダ中央銀行が作成、公表しているレッドチームテストのフレームワーク「TIBER-NL」や、EU が現在開発中の「TIBER-EU」は、いずれも「TIBER（Threat Intelligence Based Ethical Red teaming）」とされており、同じく脅威インテリジェンスを活用したレッドチームテストであり、TLPT である。

[2] https://www.fsa.go.jp/news/29/2017StrategicDirection.pdf

2.2.5. 一般的なペネトレーションテスト、脆弱性スキャン

TLPT は、従来から普及しているペネトレーションテストや脆弱性スキャンとは大きく異なる。

従来のペネトレーションテストは、インターネットに面したシステムや外部にさらされている特定の IP アドレスを対象にテストする。いわゆる境界の外側の防御能力に焦点が当てられ、スコープも限定的である。また、同テストでは、侵入を潜在的に可能としてしまう脆弱性があるかを静的に検証することに焦点があてられている。

脆弱性スキャンも、通常プラットフォームや Web アプリケーションにおける既知の脆弱性の有無を機械的に検証するための手法として捉えられている。

こうした基本的な脆弱性対策が重要であることは言うまでもなく、むしろこのような取り組みが確実に実施できていなければ、そもそも TLPT を実施する意味が薄れてしまうと考えられる。

■ 3. 金融機関における TLPT の活用

3.1. 概要

本章では、諸外国において金融機関が TLPT を活用するに至った背景や、TLPT の実施プロセス、活用状況について述べる。

3.2. TLPT の普及

諸外国の金融機関では、TLPT に対する評価が高まっており、足元ではそのニーズが高まっている。しかしながら、TLPT の普及の程度は国により異なる。

本調査では、米国が最も普及しており、2012 年頃には、グローバルにサービスを展開する大手金融機関が TLPT の活用を始めていた。最も普及した理由の1つは、APT（Advanced Persistent Threat）攻撃による境界防御の限界である。米国では 2010 年頃に、大手金融機関を標的とした国家が関与するサイバー攻撃が多数起きており、これらの攻撃は民間金融機関が想定する脅威をはるかに上回るレベルであった。国家が関与するサイバー攻撃は、明確な攻撃目的をもち、極めて高度で巧妙、執拗に行われるため、標的とされた場合、インターネットとの境界で完全に防御することは不可能となる。そのため、大手金融機関では、境界での防御力に加えて、内部に侵入された場合の検知、対応能力の高度化を図ることが急務となり、その結果として TLPT が普及していったと言われている。

米国に次いで普及しているのが英国である。とりわけ英国の場合は、2014 年に英中央銀行が導入した CBEST の影響が大きい。これにより、英国に拠点を置く大手金融機関で広く TLPT が活用されることとなった。CBEST をきっかけに TLPT の効果を認識した大手金融機関は、その後、自社の取り組みとして CBEST と同様のテストを行っている。

香港では、これまで TLPT は必ずしも一般的ではなく、認知度も低かった。大手金融機関では、グローバルレベルでの対応として TLPT が活用されていたものの、ローカルな金融機関ではほとんど認知されていなかった。しかしながら、2016 年末に香港金融管理局（HKMA）が TLPT フレームワークである「Intelligence-led Cyber Attack Simulation Testing（iCAST）」を策定、公表。これをきっかけに民間での活用が増えてきている。

他方、シンガポールでは、本調査時点で TLPT はほとんど普及していなかった。シンガポールに拠点を置く金融機関の多くは、欧米に本社を置くグローバルな金融機関である。そのため、シンガポールでの TLPT の活用の動きは限定的だが、本社主導で TLPT の活用が進められていると考えられる。

なお、当局が主導する TLPT の代表例である CBEST や iCAST については、4 章で述べる。

3.3. 金融機関にサービスプロバイダーが提供する TLPT

米英の大手金融機関では、既に TLPT が広く活用されており、TLPT を提供するサービスプロバイダー市場も醸成されている。米英の大手金融機関向けにサービスプロバイダーが提供している TLPT の一般的なアプローチは、下図のとおりである。

なお、大手金融機関では、サービスプロバイダーを活用せず、自ら内製化して TLPT を実施するケースも出てきている。

図 3-1 サービスプロバイダーが提供する TLPT のアプローチ例

Phase	主な実施事項
Phase1 計画立案・スコープ定義	● 対象組織においてリスクの高い領域（業務、機能）を識別 ● 防御すべき重要なビジネス上の資産を定義 ● 全体的なテスト戦略とスケジュールの策定　等
Phase2 脅威分析・シナリオ作成	● 脅威インテリジェンスを収集・分析し、想定する攻撃者と攻撃目標を定義 ● 対象組織の環境を調査した上で、攻撃に使用する技術や手法を整理 ● SNS 等を活用し攻撃対象者を設定　等
Phase3 テストツール開発・準備	● ソーシャルエンジニアリングを実施する環境や攻撃ツールの開発・評価 ● リスク管理フレームワークの作成・合意 ● テスト実施について対象組織へ最終通知　等
Phase4 テスト実施（攻撃・侵入）	● 攻撃対象とするシステムおよび弱点等を識別するための偵察活動を実施 ● 侵入したシステムを通じてアクセス経路の確立 ● 特権昇格を行い、機密データや複数システムにアクセス　等
Phase5 評価・報告	● 各攻撃シナリオに対して対象組織が実施した対応の証跡を収集 ● 識別された問題点がビジネスへどのような影響をもたらすか評価 ● 問題点の詳細とリスク、改善事項含め報告書を作成

3.3.1. 計画立案・スコープ定義フェーズ

金融機関側から TLPT のプロジェクトマネージャーやブルーチームリーダー等が参画し、サービスプロバイダーとともに、対象となる業務範囲やシステムの特定、実施スケジュール等を検討する。また、当該フェーズには、CRO や CISO も参加する。一般的なペネトレーションテストでは、テスト計画の検討に CRO や CISO が関与するケースは多くないが、TLPT の場合は、金融機関全体のサイバーレジリエンスの観点から、組織にとってリスクの高い領域にフォーカスしてテストを実施することや、経営層あるいは経営層に近い立場の問題意識や課題をインプットし、目的やスコープに反映することが重要となるからである。

なお、TLPT はサービスプロバイダーに事前にどこまでの情報を提供するかによって、テスト方式は下図の 3 パターンに分類される。金融機関がどのような目的で実施するかによるが、ブラックボックステストに比べ、グレーボックステスト、ホワイトボックステストが採用されるケースが多いと言われている。

例えば、明確な攻撃意図をもった ATP 攻撃の場合、攻撃者はインサイダー情報の収集も含め、攻撃に必要な対象組織の情報を入手した上で攻撃シナリオを検討し攻撃を仕掛ける。また、サービスプロバイダーが有する事前の情報が少ないため、テストが非効率になることや、意図しない影響を本番システムに与えるおそれがある。このような理由から、相対的にグレーボックステストやホワイトボックステストが選好されていると考えられる。

図 3-2 TLPT のテスト方式(情報開示の程度)

テスト方式	金融機関からサービスプロバイダーへ事前に開示される情報量	特　徴
ブラックボックステスト	情報は提供されない	対象システムや環境に関する事前情報をサービスプロバイダーに与えずテストすることによって、現実の攻撃者は、何が実施可能なのか確認できる
グレーボックステスト	限定された情報(例:システムに関するログイン認証情報等)のみ提供される	対象システムへのアクセスが許可されているユーザがどこまで、何を実施可能なのかを理解するとともに、一定の情報と知識を有するインサイダー攻撃や外部からの攻撃によって想定される被害を把握できる
ホワイトボックステスト	十分な情報(例:ネットワーク構成図や開発担当者から入手できる情報等)が提供される	多様な脆弱性や攻撃ベクトルを想定しておくことが必要なシステムに対し、集中的なテストが可能となる

※CREST A guide for running an effective Penetration Testing programme[3]を参考に、PwC あらた作成

他方、防御側であるブルーチームに対しては、無予告でテストが行われるのが一般的である。テストの具体的な内容は、TLPT の企画、設計やリスク管理に関わる金融機関の中の一部のメンバー(いわゆる「ホワイトチーム」)に限定される。従って、テストに関する情報を共有するメンバーの範囲も計画の一部として定義することが重要である。

3.3.2. 脅威分析・シナリオ作成フェーズ

一般的には下図のプロセスにそって脅威シナリオが作成される。各プロセスの内容を以下で述べる。

図 3-3　脅威シナリオ作成までの一般的なプロセス

[3] http://www.crest-approved.org/wp-content/uploads/CREST-Penetration-Testing-Guide.pdf

a) 方針決定

サービスプロバイダーは、金融機関との間で TLPT の目的やテストの前提、テストの対象となる業務、機能を確認し、相互の認識を共有する。

b) 情報収集

サービスプロバイダーは、方針に基づき、対象となる業務、機能に関連するシステムのリストや、インターネット上に公開されているドメイン名、Web サイトの情報を金融機関から入手する。さらに、それらに関連する IoCs（Indicators of Compromise）、OSINT（Open Source Intelligence）、外部専門家が有する地政学的脅威に関する情報を収集する。OSINT は、金融分野に関するメディアやインターネット上の情報に加えて、SNS の投稿やダークウェブなど、様々なオープンソースから収集され、対象金融機関あるいは所属職員に関する情報が含まれる。収集範囲が広いため自動化ツールを活用しているほか、他の脅威インテリジェンス提供会社から情報を入手するケースもある。

c) 分析、評価

サービスプロバイダーは、収集活動で得た多数の情報をもとに、どのような脅威アクターが金融機関をターゲットとして狙っているのか、各脅威アクターは、近年どのような攻撃技術や手法を使っており、攻撃能力の程度や技術の洗練度はどの程度か、攻撃の目的は何か、といった点について金融分野全体あるいはテスト対象金融機関に対する脅威トレンドを分析し、その上で想定される脅威アクターごとの脅威の程度を評価する。なお、一般的な脅威アクターとしては、以下が挙げられる。

- 破壊や混乱を与える行為を行う国家等
- スパイ行為を行う国家等
- 金銭目的のサイバー犯罪グループ
- ハクティビスト
- インサイダー

d) シナリオの報告と決定

サービスプロバイダーは、分析、評価を通じて得られた、脅威アクターごとの脅威の大きさ、および想定される攻撃技術・手法を金融機関へレポートとして報告し、金融機関のニーズやテストの目的を踏まえ、双方で採用する脅威シナリオに合意する。

3.3.3. テストツール開発・準備フェーズ

サービスプロバイダーは、攻撃の実行に必要となる環境やツール（例えば、C&C サーバー、Web サイト、フィッシングメール、マルウェア等）を開発し、稼動を検証する。検証においては、正常稼動を確認するだけではなく、ネットワークトラフィックやメモリ使用による金融機関の環境に与える負荷も確認し、本番サービスへの影響を最小化するよう工夫される。

また、金融機関は、サービスプロバイダーとともに、テスト実施中にリスクが顕在化した場合、どのように対処するかを定めたリスク管理フレームワークを作成、合意する。TLPT は本番環境で実施するため、最悪の場合には障害につながる。従って、リスク管理フレームワークをテスト実施前に関係者間で合意しておくことが、極めて重要である。その合意には、レッドチームおよびブルーチームのリーダーや金融機関のセキュリティ管理者だけではなく、双方のプロジェクトマネージャーや金融機関側の業務担当部門やリスク管理部門等も関与する。リスク管理フレームワークには、攻撃を行うレッドチームに許容される活動や行為、リスク顕在化時のテストの中止基準や責任者の意思決定、脆弱性が発見された場合や想定外の事象が発生した場合の責任者へのエスカレーションルートの確立などが含まれる。

3.3.4. テスト実施フェーズ

金融機関は、テスト実施フェーズの間、テスト管理チームを組成する。テスト管理チームは、レッドチームと緊密なコミュニケーションをとり、詳細なテスト計画や進捗状況を把握することにより、本番システムに悪影響が出ないようモニタリング・コントロールを行う。

レッドチームは、あらかじめ合意された脅威シナリオに沿って、外部からの偵察や侵入を行った上で、通信経路の確保や感染の拡大、情報収集を行う。このため、実際の攻撃さながらに、ブルーチームに検知されないよう侵入、潜伏するスキルが重要となる。一方、ブルーチームは、日々行っている監視を実施し、レッドチームの攻撃に対する防御、検知、対応を行う。このような一連の攻防をシミュレーションすることにより、サイバーキルチェーンの各段階で、どのような攻撃を許してしまう可能性があるかを明らかにしていく。

なお、テストを進めていく過程では、以下の事例のように、事前の計画と異なる事象が発生し、都度の判断が必要となる場合がある。このような状況はテスト管理チームとレッドチーム双方の負担となり、テスト期間の長期化を招くことになるため、リスク管理フレームワークの事前準備とともに、両チームの間の緊密な連携が重要となる。

テスト実施の妨げとなる事例

- レッドチームの能力不足や事前の情報不足により内部に侵入できない
- システム構成が事前に入手した設計書と異なるためテストプランを変更する必要がある
- 1つのシナリオに想定以上に時間を要したため後続のシナリオのテスト期間を短縮する必要がある
- テストによって本番システムへ悪影響が発生したため対処が必要である

また、サービスプロバイダーには、テスト実施中に認識した技術的な脆弱性を、速やか金融機関側に提供することが求められる。脆弱性は、テスト実施中といえども放置すれば実際のサイバー攻撃に悪用されるおそれがあるため、サービスプロバイダーは、3.3.5 章で述べる報告書の作成とは別に、脆弱性を記録した速報メモを都度提供することや、日次でのテスト管理チームとのミーティングを通じた情報共有により、金融機関が早期に是正を行えるための連携を図る必要がある。

3.3.5. 評価・報告フェーズ

レッドチームは、各攻撃シナリオに対してブルーチームが実施した対応の証跡を収集、検証した上で、防御、検知、対応の各段階において、ブルーチームにおいて何ができて、何ができなかったのか、タイミングは

妥当であったか、対応能力は十分であったか等を検証する。また、その中で認識された脆弱性や問題が技術、人・組織、プロセスのいずれに関係するのか、根本的な原因は何か、仮に是正されない場合はビジネスにどの程度の悪影響をもたらすのか等を評価する。なお、評価の過程では、レッドチームはブルーチームへのインタビュー等を実施し、できる限り正確に現場の対応を把握し、見解を確認した上で評価結果に反映させる。

整理された全ての脆弱性や問題については、金融機関におけるサイバー対応の成熟度やビジネスへの影響の程度を踏まえた上で、推奨される改善策やその優先度が示され、報告書として金融機関に提出される。

3.4. 金融機関における TLPT の活用状況

3.4.1. TLPT を活用している金融機関の規模、業態

米英の大手金融機関では、業態を問わず TLPT が広く活用されており、大手の銀行に加えて、大手の保険会社、証券会社、クレジットカード会社でも活用されている。また、英国では、CBEST の導入もあり、大手の資産運用管理会社や年金供給会社でも TLPT が活用されている。

米国では、サイバー攻撃に対する監視、検知、その関連プロセスと態勢が整備されている等、サイバー攻撃対応態勢が進んでいる金融機関が活用している。また、このような金融機関は、一般的なペネトレーションテストや脆弱性スキャンを従来から高い頻度で繰り返し実施してきており、いわば境界防御の対策を適切に講じている金融機関である。従って、TLPT は組織の規模というよりは、対応態勢の進展度合いによって活用されている。

香港では、大手銀行、証券会社、アジア広域でビジネスを展開する保険会社で活用されているほか、いくつかのローカル銀行でも TLPT が活用されている。ただし、ローカル銀行のケースは、RAT（リモートアクセスを可能とするマルウェア）を用いたインサイダーの脅威を想定したシナリオベーステストであるものの、テスト範囲を制限するなど限定的なものであった。

3.4.2. スコープ

米国、英国、香港では、通常 Windows ドメインや取引先情報や顧客情報等を取扱う業務アプケーションシステムやデーターベースがテストのスコープとなるケースが多い。しかしながら、TLPT では、脅威アクターの目的を再現すること、例えば、攻撃者にとって最も価値のあるものは何かに焦点を当てるため、脅威シナリオによって様々な IT および IT 以外の資産がテストのスコープとなり得る。

こうしたことから、以下のようなシステムをテストスコープとしている事例も見られた。

- インサイダーが関与した ATM システム
- ここ数年被害が多発している SWIFT システム
- VoIP（Voice over Internet Protocol）を使った IP 電話や監視カメラシステム（経営陣の会話や行動が漏えいするリスクに対処する目的）

3.4.3. 脅威シナリオ

米英で脅威シナリオとして設定される主な脅威アクターは、経済目的の犯罪集団、国家等による攻撃者、スパイ行為者、インサイダーである。なかでも米国は、金融機関の機密情報の窃取を狙った国家等によるスパイ行為のシナリオを相対的に多く用いている。香港では、脅威インテリジェンスの収集・分析が行われるケースは少なく、共通シナリオとして、スパイ行為グループ、インサイダーが用いられるケースが多い。

攻撃手法は、ソーシャルエンジニアリングやスピアフィッシングを用いて RAT 等をシステム内に送り込むケースが大半であった。その他にも、偽サイトによる水飲み場攻撃を活用するほか、RAT モジュールを保存した USB デバイスを職員の気付きやすい場所に放置し、それを標的である端末に挿入させるよう仕向ける、いわばソーシャルエンジニアリングと物理セキュリティの問題を炙り出す手法を組み合わせるケースも見られた。

3.4.4. コスト・期間

サービスプロバイダーによる TLPT の提供実績を調べ、平均的な TLPT サービスのコストと期間を算出した。ただし、コストと期間は、テストの目的やスコープ、採用するシナリオ数、実施方法、成果物等様々な条件・組み合わせによって決まるため一概に比較できないことに留意する必要がある。

図 3-4 サービスプロバイダーを活用して実施する TLPT の平均的なコストと期間

対象	コスト概算（※1）	期間（※2）
英国	90,000～120,000 ポンド （1 ポンド=155 円の場合、約 14,000,000～18,600,000 円）	4～5 か月程度
米国	100,000 ～130,000 米ドル （1 米ドル=109 円の場合、約 10,900,000～14,200,000 円）	4 か月程度
香港（※3）	500,000～1,100,000 香港ドル （1 香港ドル=14 円の場合、7,000,000～15,400,000 円）	3 週間～2 ヶ月程度

※1 上記（）内の金額は、2018 年 1 月 30 日時点の為替レートを用いた概算値

※2 テストの実施期間のみではなく、計画から報告完了までの期間（サービスプロバイダーの選定、調達にかかる期間は含まれない）

※3 香港は脅威インテリジェンスの収集・分析を行わず汎用的な脅威シナリオで実施する事例や、3.4.1 章で記載した範囲を限定した実施事例も含んだ金額と期間

3.4.5. 実施周期

TLPT の活用が進んでいる米英の大手金融機関では、サービスプロバイダーを活用した TLPT を定期的に実施している。米国では年次で実施しているほか、大規模なインフラの変更や移行があった場合には、頻度を高めて実施している事例も見られた。英国では、非公式ながら大手金融機関に対して少なくとも 2 年に 1 度、CBEST と同様の TLPT の実施を当局が推奨している。

香港については、本調査時点では、頻度についての具体的な情報は得られなかったが、当局主導で導入された TLPT のフレームワークである iCAST に対する今後の評価、当局のスタンスに依存すると考えられる。

このように、TLPT の実施頻度にはばらつきがあるが、大手金融機関がサービスプロバイダーを活用する場合は、以下のような点を踏まえて実施頻度を検討している。

実施頻度を検討する際の主な観点

- ビジネスの特性、システムの複雑性
- 直面している脅威、脆弱性の程度
- グローバル全体で見た場合のシステム環境やセキュリティ対策の標準化、集約化の程度
- レッドチームを内製化し TLPT を行っている場合、それによるカバレッジと効果の程度
- 当局の規制あるいは規制ではないものの推奨されている水準

3.4.6. 内製化

2.2.1 に記載したとおり、TLPT を実施する場合、TI、PT が必要となる。TI、PT は同一である必要はなく、異なるプロバイダーを採用する場合もある。また、昨今では、米英の大手金融グループを中心に TLPT の内製化が進んできており、サービスプロバイダーに依存しない形で取り組んでいる。

a) TI 、PT 機能の両方を内製化

TI、PT の機能を内製化し、TLPT を柔軟に活用している。外部のサービスプロバイダーを活用して TLPT を実施する場合、事前に合意した期間やコスト面で制約があるほか、プロバイダーの経験や能力によって、期待通りの効果が得られない場合がある。

また、TI、PT を行う者は、専門性が高い上に組織のセンシティブ情報や重要システムに触れる結果、組織の脆弱性を詳細に知る立場になるが、この点、内製化できれば、外部にセンシティブ情報が漏えいするリスクは低減される。大手の金融機関の中には、グローバル全体をカバーするテストチームを自社内に組成し、組織全体の脅威動向を分析した上で、TLPT を企画、立案し、様々な拠点やサービスに対して年間を通じて TLPT を実施しているところもある。

他方、内製化するためには、以下のような課題をクリアしていくことが必要となる。

- TI、PT を代替するスキルセットを有する人材は市場で不足しているため、人材の確保、継続雇用のための処遇
- 信用できる人材（ホワイトハッカー）の確証を得るための十分なバックグラウンドチェック
- 攻撃技術やその組み合わせが日々高度化、複雑化していくため、ハッカーと同等の専門知識や技術の維持、向上のためのトレーニング　など

なお、内製化した場合でも、TLPT の透明性を確保する観点から、内製チームで実施したテストが効果的でかつ十分な品質となっているかを、外部の専門家を活用し評価しているケースや、内製チームとサービスプロバイダーを併用しているケースがある。

b) TI 機能のみ内製化

本調査の結果、TI 機能のみを内製化している事例があった。脅威インテリジェンスの収集・分析は、TLPT の実施以外にも活用可能なことから、日常的なプロセスとして導入しているケースは多い。また、自組織の特性、脅威の分析という点では、自組織をよく熟知した者が実施することが望ましく、その点では人材確保も含め、体制が整備できれば外部に依存する必要性は少なくなると考えられる。

なお、TI 機能のみを内製化している大手金融機関において、PT 機能を内製化しない理由は、まさに上記 a)で述べた課題への対応である。特に、専門知識や技術力の継続維持は重要な前提条件であり、実現できない場合は、TLPT の品質に影響を与えることから、コスト面を含め総合的な判断として TI 機能のみを内製化するアプローチを採用していると考えられる。

■ 4. 金融当局が主導する TLPT

4.1. 概要

本章では、金融当局が主導する TLPT に関するフレームワークや実施手順について述べる。具体的には、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や実施環境について、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。

なお、本調査では、当局が主導する TLPT のフレームワークが、米国には存在しないため、本章の対象外としている。しかしながら、米国では、金融機関が自身のリスク評価を行う際に、自ら TLPT を主体的に活用し、態勢強化を図っている。[4]こうした金融機関の中には、レッドチームを内製化し、自社内で脅威分析を行った上でシナリオを複数作成し TLPT を行っている先進的なところもある。このように、米国では当局が主導しなくても、金融機関自らがこうしたツールを積極的に活用する企業文化が従前より根付いている。また、このように米国では金融機関のセキュリティに対する意識が高いこともあり、こうしたツールやテストを提供するサービスプロバイダーの専門性・能力も高いと言われている。

4.2. 英国による取り組み（CBEST）

英国の金融当局が推進する CBEST[5]による TLPT の取り組みについて、英中央銀行（Bank of England、以下「BoE」）が公表している「CBEST Intelligence-Led Testing -CBEST Implementation Guide-」[6]を中心に述べる。

4.2.1. CBEST

a) 導入の背景

2013 年、英金融安定政策委員会は、英財務省（HM Treasury）に対し、同省と英国の主要な金融システムや金融インフラの金融当局に対して、洗練されたサイバー攻撃へのレジリエンスを評価、強化するためのプ

[4]サイバーセキュリティの成熟度レベルの評価ツールである米国 FFIEC Cybersecurity Assessment Tool（2015 年公表）では、先進的な成熟度（Advanced）と評価する指標の 1 つとして、「Penetration tests include cyber attack simulations and/or real-world tactics and techniques such as red team testing to detect control gaps in employee behavior, security defenses, policies, and resources.」と記載されており、TLPT の実施に言及している。

[5] https://www.bankofengland.co.uk/financial-stability/financial-sector-continuity

[6] https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf?la=en&hash=1BFF85C8F9E6C0E8BE478BB22B422EDDA5E00DC0

ログラムの導入を求めている。これに基づき、2014 年に英財務省、BoE、金融行為監督機構（FCA）により導入されたツールが CBEST である。

金融サービス分野において、従来のペネトレーションテストは既知の脆弱性に対するテストとして、その有効性は理解されていた。しかしながら、従来のペネトレーションテストでは洗練された攻撃へのレジリエンスを評価するには十分ではなかった。これには 2 つの理由が考えられる。

1 つは、重要資産に対して疑似攻撃を行うテストには高いリスクが伴うため、金融機関が躊躇していたことである。

もう 1 つは、ペネトレーションテストプロバイダーが、対象組織や業界に特化した脅威情報を十分に活用できていなかったことである。[7]

こうした課題に対応するため、英国は CBEST を採用した。また、CBEST は、BoE と関連監督当局との緊密な連携が中核となっており、国の重要インフラを形成する組織に対するレジリエンスを評価するためにテストを実施する場合は、GCHQ（Government Communications Headquarter）[8]とも連携を図る。

b）概要

BoE は、2017 年 6 月時点で 31 の金融機関や金融市場インフラに対する CBEST の評価を終了している[9]。2014 年から実施されている CBEST の第 1 フェーズには、英国の重要な金融システムを構成する金融機関や金融市場インフラ（以下「Firm/FMI」）である 34 先が当局によって選定された。なお、CBEST の実施は任意であるが、実態としては選定先のほとんどが CBEST を実施している。

1） ステークホルダー

- Firm/FMI
- BoE サイバーセクターチーム（SCT）
- 監督当局
  - 健全性規制機構（PRA）
  - Financial Market Infrastructure Directorate（FMID）
  - 金融行為規制機構（FCA）
- 脅威インテリジェンスプロバイダー（TI）
- ペネトレーションテストプロバイダー（PT）

CBEST は、①開始フェーズ（Initiation Phase）、②脅威インテリジェンスフェーズ（Threat Intelligence Phase）、③ペネトレーションテストフェーズ（Penetration Testing Phase）、④完了フェーズ（Closure Phase）の 4 つのフェーズから構成される。また、評価を効果的に行うため、評価プロセス全体を通じ全てのステークホルダーが協調してプロジェクトマネジメントすることが求められている。

[7] http://www.crest-approved.org/wp-content/uploads/2014/05/CBEST-OVERVIEW.pdf

[8] GCHQ（政府通信本部）：英国政府直属の諜報機関

[9] https://www.bankofengland.co.uk/financial-stability-report/2017/june-2017

評価プロジェクト全体の責任は、Firm/FMI が負い、Firm/FMI 内の CBEST プロジェクトチームが、TI、PT とのミーティングを含むすべての活動に関与し調整を図る。TI、PT は、それぞれ担当する各フェーズの計画を Firm/FMI へ提示し、Firm/FMI はそれを全体計画に組込むことでプロジェクト全体を管理する。

図 4-1 は各フェーズとその概算期間を示している。平均的にはテスト開始から完了まで 6～7 ヶ月を想定しているが、各金融機関の意思決定プロセスのスピードやサービスプロバイダーの選定、テスト後の改善計画の内容により期間は異なってくる。

図 4-1 CBEST フレームワークのプロセスとステークホルダー

※「CBEST Intelligence-Led Testing -CBEST Implementation Guide-」を参考に、PwC あらた作成

2) リスク管理

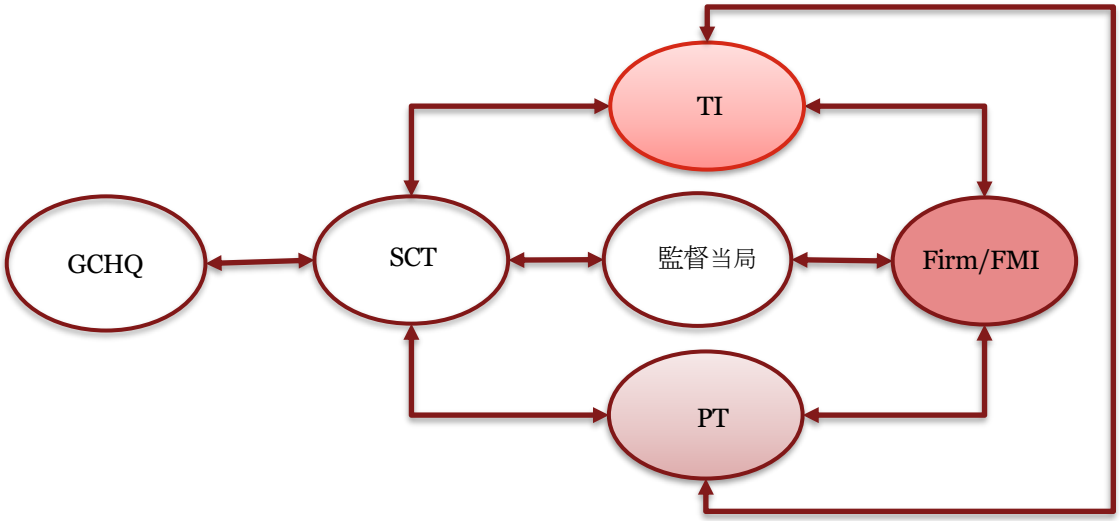
CBEST では、実際の攻撃に近い手法を再現するため、Firm/FMI においても図 4-3 に示されたメンバー以外には原則知らされることなく秘密裡に準備される、「ステルス方式」でテストが実施される。また、テストは本番環境で実施される。しかしながら、テストの対象となるシステムおよび関連する者やプロセスは、英国の

金融システム上重要な機能を担うインフラであることから、テストを行うこと自体にリスクを伴う。そのため、これらリスクを軽減するため CBEST には、以下のコントロールが組込まれている。

- 全てのステークホルダーが評価スコープ、制限事項、連絡先、実施内容および責任の所在(該当する場合は保険も含む)を明確にするため、これらが明記された同意書に全ステークホルダーが署名。
- サービスプロバイダーの一定以上の専門性や技術を担保し、テストによる本番システムへの影響を軽減するため、テスト実施者は、CREST(Council for Registered Ethical Security Testers)の付与する資格が必要(詳細は 4.2.2 章を参照)。
- Firm/FMI 内のコントロールグループの設置とエスカレーション手順の事前整備
- 定期的なリスク評価、軽減策の PDCA サイクルによる継続的な実施(推奨)

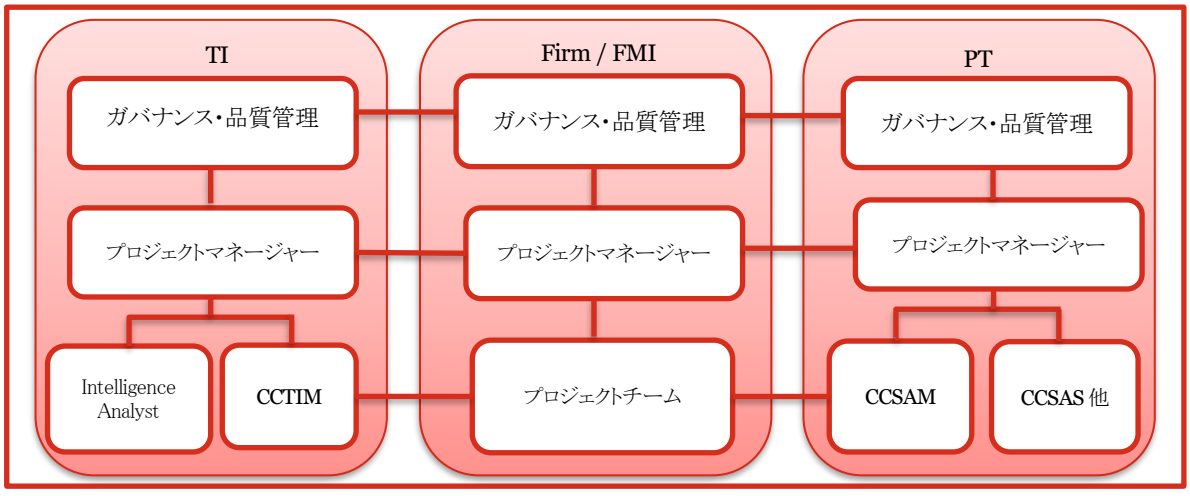
なお、テスト実施中にシステム障害(またはそのおそれ)が懸念される場合、Firm/FMI はいつでもテストの一時的な停止を指示することができる。

図 4-2 ステークホルダーと情報フロー



※「CBEST Intelligence-Led Testing -CBEST Implementation Guide-」を参考に、PwC あらた作成

図 4-3 プロジェクトチームの構成と関係性



※「CBEST Intelligence-Led Testing -CBEST Implementation Guide-」を参考に、PwC あらた作成

c) 実施プロセス

上述のとおり、CBEST は 4 つのフェーズから構成されているが、各フェーズはさらに 4 つのプロセスに分かれている。下記では、各プロセスにおける活動、アウトプットについて述べる。

1) 開始フェーズ(Initiation Phase)

開始フェーズは、主にスコープの決定、TI、PT の調達を行う。TI、PT の調達に要する期間によるが、概ね当該フェーズは 4～6 週間で終了。

図 4-4 脅威インテリジェンスフェーズのプロセス

1.1) 開始(Launch)

監督当局が CBEST による評価が必要であることを決定し、SCT に通知した時点から CBEST による評価プロセスが開始される。SCT は監督当局に対して、評価プロセス、文書、役割・責任の説明を行う。

＜アウトプット＞

- 監督当局による記録(Note for Record)

1.2) エンゲージメント(Engagement)

SCT、監督当局は、Firm/FMI に対し以下を説明し協議。

- 評価プロセス
- ステークホルダーの役割・責任
- セキュリティプロトコル
- 契約に関する事項
- プロジェクトスケジュール

SCT は面会に先立ち、CBEST の関連文書一式を Firm/FMI に送付する。この文書の中には、SCT が作成した契約書類が含まれており、それにはスムーズで効果的な評価の実現と、関係者間の透明性の確保を考慮した契約条項のテンプレートが含まれる。Firm/FMI が当該条項を TI、PT との契約に用いるため、契約にかかる時間が短縮される。また、契約条項には、SCT、監督当局から求められた場合、TI、PT が作成した文書、関連情報を、SCT、監督当局に提供しなければならないことが明記されている。

＜アウトプット＞

- 監督当局による記録(Note for Record)

1.3) スコープの決定（Scoping）

SCT、監督当局および Firm/FMI はスコープの協議を行い、Firm/FMI は CBEST スコープ定義書（CBEST Scope Specification）のドラフトを作成する。CBEST スコープ定義書の意義は、評価スコープを定義する上で、Firm/FMI に関する重要機能（Critical Function）を明確化することにある。

CBEST では、「重要機能」を、以下のように定義している。

「妨害された場合に英国の金融の安定、Firm/FMI の安全性や安定性、顧客基盤、マーケットコンダクトに有害な影響を与え得るサービスを提供する上で必要な者、プロセス、技術」

CBEST スコープ定義書には、これら重要機能だけでなく、重要機能を支えるシステムやサービスの一覧も含まれる。これらは、攻撃者が対象の Firm/FMI を侵害する場合に狙うべきポイントであるため、後続のテストシナリオを作成する際に参照される。

また、上記 b)概要で述べたが、連携ミスやテストに関する情報の漏えいを防ぐためのコントロールグループの設立は、本プロセスで行う。コントロールグループは、テスト対象となる各システムのエスカレーションフローの頂点に位置し、メンバーは一握りの上級管理者（senior individuals）で構成される。ペネトレーションテストの開始時や CBEST により攻撃が検知された場合には、事前に定めたプロセスに沿ってコントロールグループに報告される。

同時に Firm/FMI は、プロジェクト開始文書（Project Initiation Document）を作成する。プロジェクト開始文書は、Firm/FMI とステークホルダーとの打合わせ内容を記載する内部資料であるため、SCT、監督当局への提示は不要である。また、評価スコープに国の重要インフラが含まれる場合は、GCHQ との連携が必要となるため、Firm/FMI はインターネット資産登録フォーム（Internet Asset Register Form）を作成し、監督当局に提出する。監督当局はその写しを GCHQ へ提出する。

＜アウトプット＞

- CBEST スコープ定義書のドラフト
- プロジェクト開始文書のドラフト
- インターネット資産登録フォーム（Internet Asset Register Form）（必要な場合）

1.4) ベンダーの選定と契約（Procurement）

本プロセスでは、Firm/FMI は以下を実施する。

- CBEST 認定の TI/PT の調達と SCT の作成した契約条項ドラフトの内容を含めた契約の締結
- SCT、監督当局と評価スコープを合意し CBEST スコープ定義書を完成させる
- Firm/FMI、SCT、監督当局、GCHQ（必要な場合）との打合わせ日程を決定し、プロジェクト開始文書を完成させる

BoE は、各 Firm/FMI が TI、PT を選定する際のガイドラインを発行している。 特に、脅威インテリジェンスは比較的新しい領域であり、市場における成熟度も低いことから、Firm/FMI が正しく評価、選定することは困難である。そのため、当該ガイドラインでは、TI、PT の選定に役立つ評価指標を提供している。

＜アウトプット＞

- CBEST スコープ定義書の最終版
- プロジェクト開始文書の最終版

2) 脅威インテリジェンスフェーズ（Threat Intelligence Phase）

脅威インテリジェンスフェーズでは、TI 主導の下で現実的な脅威シナリオを作成する上でベースとなる情報収集を行う。TI は、Firm/FMI からスコープの説明を受け、脅威情報の収集、分析、発信、レビューを行う。並行して、PT は TI の支援の下、ペネトレーションテスト計画書（Penetration Test Plan）の作成に向けて、脅威シナリオを作成する。脅威インテリジェンスの成果物のレビューは、全てのステークホルダーが参加するレビューを経て最終化され、TI から PT へ引継がれる。また SCT は、本フェーズの最後に Firm/FMI と TI の脅威インテリジェンス能力を評価する。

TI や GCHQ（必要な場合）のアベイラビリティにもよるが、概ね当該フェーズは 10 週間程度で終了する。

ペネトレーションテストに比べて脅威インテリジェンスは比較的新しい領域であるため、BoE は「CBEST Intelligence-Led Testing Understanding Cyber Threat Intelligence Operations」[10]という、CBEST における脅威インテリジェンスに関するガイドラインを発行している。当該ガイドラインでは、「脅威（Threat）」、「サイバースペース（Cyberspace）」、「インテリジェンス（Intelligence）」等の用語の定義や脅威インテリジェンスのプロセスや組織のベストプラクティス、脅威インテリジェンスの成熟度モデル等が TI 向けに記載されている。

図 4-5 脅威インテリジェンスフェーズのプロセス

2.1) サービスプロバイダーへの情報共有（Direction）

Firm/FMI は、開始フェーズで作成した CBEST スコープ定義書の Section 2、3 を TI に提供する。Section 2、3 には、スコープに含まれる重要機能や関連するシステムにかかる情報が記載されている。また、PT ができる限り早くペネトレーションテストの計画を立てられるよう、Firm/FMI は PT に CBEST スコープ定義書の Section 4 を連携することが推奨されている。Section 4 には、重要機能に関連する各システムにとって何が侵害行為となるかが記載されている。

本プロセスは、実際に攻撃を仕掛ける PT が、Firm/FMI が直面している現実的な脅威を想定した上でシナリオを作成できるように設計されている。脅威シナリオは、実際の脅威アクターに関するエビデンスを

[10] https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf?la=en&hash=4B42B0382D1D33402689478433E2E1E0FFA93055

オープンソースで取得し、さらに Firm/FMI に関連するインテリジェンスや重要機能に関する知識を組み合わせて作成する。

TI が時間やリソースの制限の中で効率的に情報収集を行うとともに、CBEST のスコープや Firm/FMI のビジネスにとって適切な情報を分析できるよう、以下の情報が Firm/FMI から TI に提供される。すなわち、CBEST の脅威インテリジェンスは、グレーボックステストのアプローチを採用している。

- スコープに含まれる重要機能および関連システムのビジネスや技術的な内容
- 最新の脅威に対する評価
- 直近の攻撃事例

＜アウトプット＞

- 脅威インテリジェンス計画書（Threat Intelligence Plan）

2.2) インテリジェンス（Intelligence）

本プロセスは、さらに 3 つのサブプロセスから構成されている。TI は、まずは以下の 2 つの観点から重要機能に関連する情報の収集、分析、配信を行う。

- Targeting：Firm/FMI の組織全体で攻撃される可能性
- Threat Intelligence ：関連性のある脅威アクターおよび想定される脅威シナリオ

続いて、上記で得られた脅威シナリオをもとに、PT はペネトレーションテスト計画書の作成を開始する。CBEST では、脅威インテリジェンスの分析過程で、スコープ内の重要機能やその他のビジネスの侵害につながり得る脆弱性や切迫した脅威を特定した場合には、TI はただちに Firm/FMI に報告しなければならない。特定された脆弱性に関しては、Firm/FMI が改善措置を講じてもよいことになっているが、ペネトレーションテスト実施時に、Firm/FMI は PT に、本件対処に関する情報を提供する必要がある。また、どの脆弱性に対応したかは SCT、監督当局にも報告する必要がある。

2.2.1) 攻撃対象の特定（Targeting）

本サブプロセスの目的は、Firm/FMI を攻撃する立場から、広く情報収集を行い、Firm/FMI の全体像を把握することである。脅威アクターの最終的なゴールは重要機能の侵害であるが、通常重要機能は Firm/FMI の内部に位置しているため、攻撃者はまず内部への侵入方法を探る。そのため、本サブプロセスでは、Firm/FMI の脆弱性を見つけるため広い視野で Firm/FMI に関する情報収集を行う。

本サブプロセスのアウトプットとして、TI は、テスト対象機関に関する報告書（Targeting Report）を作成する。

2.2.2) 脅威インテリジェンス（Threat Intelligence）

本サブプロセスの目的は、エビデンスの裏付けがある脅威情報を基に、Firm/FMI のビジネス環境に特化した、説得力のある脅威の概観を示すことである。そのために TI は、関連性のある脅威アクターや想定される脅威シナリオに関する情報を収集、分析、配信する。

脅威インテリジェンス は攻撃対象の特定で収集した情報をもとに分析される。例えば、侵入する上で適当な資産が特定された場合（セキュアでないサーバーが露呈している等）、これをシナリオに組込むことで脅威アクターは侵入できる。

本サブプロセスのアウトプットとして、TI は、脅威インテリジェンス報告書（Threat Intelligence Report）を作成する。

2.2.3） シナリオの開発（Scenario Development）

本サブプロセスは、TI から PT への引継ぎ地点となる。PT は、脅威インテリジェンス報告書に含まれる脅威シナリオと CBEST スコープ定義書の Section 4 を基に、ペネトレーションテスト計画書の作成を開始する。

ペネトレーションテスト計画書のドラフトが完成したら、Firm/FMI、TI、PT でレビューし、TI は脅威シナリオ、PT はペネトレーションテスト計画書を説明する。

＜アウトプット＞

- テスト対象機関に関する報告書のドラフト
- 脅威インテリジェンス報告書のドラフト
- ペネトレーションテスト計画書のドラフト

2.3） 検証（Validation）（必要な場合）

本プロセスでは、GCHQ がテスト対象機関に関する報告書およびと脅威インテリジェンス報告書のドラフトのレビューを行う。その後、Firm/FMI、GCHQ、SCT、監督当局、TI、PT でレビューする。当該レビューでは、TI によるテスト対象機関に関する報告書や脅威インテリジェンス報告書の説明、GCHQ による最新の脅威インテリジェンス情報の共有、PT によるペネトレーションテスト計画書の共有が行われる。

TI はレビュー後、テスト対象機関に関する報告書と脅威インテリジェンス報告書を完成させ、Firm/FMI へ提出する。Firm/FMI は、SCT、監督当局、PT にこれら報告書を提供する。

＜アウトプット＞

- テスト対象機関に関する報告書の最終版
- 脅威インテリジェンス報告書の最終版
- ペネトレーションテスト計画書のドラフト
- 監督当局による記録（Note for Record）

2.4） 評価（Assessment）

本プロセスでは、以下の 2 つの評価を実施する。

- TI による Firm/FMI の内部インテリジェンス能力の評価
- SCT による TI の脅威インテリジェンスサービス提供能力の評価（SCT が実施）

＜アウトプット＞

- インテリジェンスの評価結果（Intelligence Assessment）

3) ペネトレーションテストフェーズ（Penetration Testing Phase）

図 4-6 ペネトレーションテストフェーズのプロセス

3.1) 計画（Planning）

PT は、脅威インテリジェンスフェーズで作成されたペネトレーションテスト計画書を完成させる。

スコープ内の各重要機能に関連するシステム侵害について記載した CBEST スコープ定義書の Section 4 に加え、テスト対象機関に関する報告書と脅威インテリジェンス報告書をレビューし、ペネトレーションテスト計画書の妥当性を確認する上でのエビデンスとして使用する。

脅威インテリジェンス報告書の中でも、特に下記の 3 つのアウトプットは、ペネトレーションテスト計画書を作成する上で関連性が高い。

- 脅威シナリオ
- 脅威アクターのゴール
- 検証されたエビデンス

テストチームは、各脅威アクターのゴールと実際のテストの整合性を保つため、脅威シナリオを再現するための攻撃手法を練る必要がある。

どのようなペネトレーションテストであっても、対象システムや関連する情報に対しては一定のリスクが伴う。このため、Firm/FMI のリスクを最小限に抑えるために、PT は、適切な管理計画を作成する必要がある。

＜アウトプット＞

- ペネトレーションテスト計画書の最終版
- リスク管理計画書（Risk Management Plan）

3.2) 実施（Execution）

PT は、スコープ策定時に特定した対象システムに対して、脅威ベースペネトレーションテストを実施する。テストを実施する上で、PT は、TI 同様に、倫理的、道徳的、法的な制約に加え、時間やリソースの制約がある。そのため、限られた時間で最大の利益を得るために、Firm/FMI からの支援が必要となる。

PT は、テスト実施後にペネトレーションテスト報告書（Penetration Test Report）を作成する。これには、スコープで定義されている各コンポーネントに関して、各脅威シナリオの段階におけるテストの経過を記載する。

＜アウトプット＞

- ペネトレーションテスト報告書のドラフト

3.3) レビュー（Review）

本プロセスでは、ペネトレーションテスト報告書のドラフトのレビューを実施するために、Firm/FMI、SCT、監督当局、PT でレビューする。当該レビューでは、以下を議論する。

- テストの実施内容
- 特定された脆弱性
- リスク軽減策
- 改善方法

＜アウトプット＞

- ペネトレーションテスト報告書の最終版
- 改善計画書（Remediation Plan）のドラフト
- 監督当局による記録（Note For Record）

3.4) 評価（Assessment）

本プロセスでは、以下の 2 つの評価を実施する。

- PT による Firm/FMI の検知、対応能力の評価
- SCT による PT のテスト能力の評価

＜アウトプット＞

- 検知、対応の評価（Detection and Response Assessment）

4) 完了フェーズ（Closure Phase）

図 4-7 完了フェーズのプロセス

4.1) 講評（Evaluation）

本プロセスでは、TI が作成したインテリジェンスの評価（Intelligence Assessment）と、PT が作成した検知・対応の評価（Detection and Response Assessment）の内容について SCT が評価し、インテリジェンス・検知・対応に関する報告書（Intelligence, Detection and Response Report）を作成する。SCT は、インテリジ

ェンス・検知・対応に関する報告書を監督当局に提出し、監督当局から Firm/FMI に当報告書の写しが提供される。当報告書は、後続の改善(Remediation)プロセスで議論される。

＜アウトプット＞

- インテリジェンス・検知・対応に関する報告書

4.2) 改善(Remediation)

本プロセスでは、Firm/FMI、SCT、監督当局が対面で、SCT が作成したインテリジェンス・検知・対応に関する報告書をもとに評価結果をレビューする。CBEST では、合格／不合格の判定は行わないが、SCT、監督当局は、評価の過程で特定された脆弱性をレビューし、Firm/FMI にフィードバックする。Firm/FMI は、フィードバックを踏まえ、改善計画書を修正し、完成させる。

＜アウトプット＞

- 改善計画書の最終版
- 監督当局による記録(Note For Record)

4.3) 最終報告(Debrief)

本プロセスでは、TI、PT が SCT と最終報告会を実施し、以下の観点でレビューを行う。

- 適切に対応できたアクティビティ、成果物
- 改善の余地があるアクティビティ、成果物
- CBEST プロセスにおいてよく機能した点
- CBEST プロセスにおいて改善の余地がある点

その後、TI/PT は自身のパフォーマンスのフィードバックを受ける。また、SCT は、CBEST プロセスにおける改善点を把握できる機会となることから、今後の改善につなげていく。

＜アウトプット＞

- 最終報告会の記録(Debrief Log)

4.4) 監督(Supervision)

CBEST の評価終了後、監督当局は、Firm/FMI の改善計画書に基づき、改善状況をモニタリングする。改善計画書の内容により、当該プロセスの期間は異なるが、1年以上になることもある。

＜アウトプット＞

- 監督当局による記録(Note For Record)

4.2.2. CREST[11]

CBEST で TLPT を実施するサービスプロバイダーは、CREST（Council for Registered Ethical Security Testers）による資格認定を受けなければならない。CREST は、情報セキュリティ市場で提供されるサービスの技術的な専門性を保証するために設立された非営利団体であり、BoE と協力して、CBEST サービスプロバイダーの認定を行っている。

CREST は、組織に対する認定に加え、個人に対する資格付与も行っている。CBEST のサービスプロバイダーとして認定されるためには、CREST STAR（Simulated Targeted Attack and Response）のサービスプロバイダーの要件に加え、CBEST 認定の追加要件を満たす必要がある。CREST STAR は CREST が認定を行っているが、CBEST サービスプロバイダーは、SCT が直接各サービスプロバイダーの申請内容を精査し、認定の可否を判断している。

a）サービスプロバイダーとして認定

1） CREST STAR サービスプロバイダーの認定要件[12]

- CREST のメンバーシップとしての要件を満たすこと
- CREST 認定資格を保持する従業員が最低 1 名所属していること
  - TI の場合、CCTIM（CREST Certified Threat Intelligence Manager）が所属していること
  - PT の場合、CCSAS（CREST Certified Simulated Attack Specialist）と CCSAM（CREST Certified Simulated Attack Manager）の両方が所属していること

2） CBEST サービスプロバイダー認定の追加要件

- 各資格を保持する従業員が以下の経験を有することが必要（経験を裏付ける参照資料（サービス提供先の一覧と連絡先）の提示を求められる）
  - TI の場合、所属する CCTIM が 7,000 時間以上の金融分野における経験を有すること
  - PT の場合、CCSAS/CCSAM が 4,000 時間以上の金融分野のペネトレーションテストおよび 14,000 時間以上の一般的なペネトレーションテストの経験が必要

b）個人に対する資格の認定[13]

下図は、CREST が認定する脅威インテリジェンスとペネトレーションテストに関する主な個人資格と各試験（実技、筆記）を示している。資格ランクは大きく 3 段階（Practitioner /Registered/Certified）に分かれており、Certified に行くにつれ、より高度な知識や経験が求められている。資格によっては、下位の資格を保持していることが必須要件となっているものがあり、例えば CCSAS の試験を受けるには、CCT の資格が必要となる。CREST STAR と CBEST のサービスプロバイダーとして組織が認定を受けるためには、最高位の資格である Certified の資格を持つ従業員が組織に属していることが必須となる。

[11] http://www.crest-approved.org/index.html

[12] http://www.crest-approved.org/join/index.html

[13] http://www.crest-approved.org/examinations/index.html

なお、これら資格の有効期間は 3 年であり、資格を維持するためには 3 年ごとに再受験し、改めて CREST の認証を得る必要がある。

図 4-8 CREST 認定資格および試験

<table>
<tr><th>Type</th><th>Practitioner</th><th>Registered</th><th colspan="2">Certified</th></tr>
<tr><td>Threat Intelligence</td><td>N/A
（現在準備中）</td><td>CRTIA
（Registered Threat Intelligence Analyst）
筆記</td><td colspan="2">CCTIM
筆記</td></tr>
<tr><td rowspan="2">Penetration Tester</td><td rowspan="2">CPSA
（Practitioner Security Analyst）
筆記</td><td rowspan="2">CRT（Registered Penetration Tester）
筆記＋実技</td><td rowspan="2">CCT（Certified Penetration Tester）
筆記＋実技</td><td>CCSAS
筆記＋実技</td></tr>
<tr><td>CCSAM
筆記</td></tr>
</table>

4.2.3. CBEST の運用実態と今後

a) 対象金融機関

英国の金融システム上重要な Firm/FMI が CBEST の対象に選定されている。BoE が公表している情報によれば、2017 年 6 月時点で CBEST の第 1 フェーズの対象として 34 の Firm/FMI が選定されている。対象には、リテール銀行、投資銀行に加え、決済システム運営会社や取引所、大手保険会社が含まれている。

b) コスト

Firm/FMI がサービスプロバイダーに支払う金額は、£150,000 前後といわれており、そのうち、TI に £50,000 前後、PT に£100,000 前後であった。

c) 期間

本調査でヒアリングした金融機関では、CBEST に要した期間は、CBEST の開始フェーズから最終報告まで概ね1年程度であった。外部のサービスプロバイダーが脅威インテリジェンスやペネトレーションテストを実施する期間は、それぞれ 3～4 週間、4～6 週間と CBEST で想定されている期間から大きなずれはないが、多くの金融機関はオペレーショナルリスクを軽減するための事前準備に重点を置いており、長い場合には開始フェーズに 6 カ月も要したところがあった。具体的には、スコープの決定プロセスで実施するコントロールグループの設立の際に、詳細なエスカレーションフローや運用ルールを定めることに時間を要していたところや、テスターの経験やバックグランドの調査を詳細に行うなど、プロバイダーの選定に時間をかけていたところがあった。

d) スコープや手法

テストの対象システムや範囲は、脅威インテリジェンス分析の結果を踏まえて決定されるが、英国の金融システム上重要な機能を担う重要システムに加え、2 つの重要なシステム、例えば英国の銀行システムや

ATM システムが SCT により推奨されている。ただし、この点について、他のシステムを選定してテストした金融機関も散見された。

また、システムへの侵入方法としては、メール等によるスピアフィッシングを採用するケースが多く、フィッシングメールも複数使用している。なお、テスターは実際のハッカーと異なり、法令遵守やあらかじめ計画された期間内で侵入を試みるため、中には侵入が困難な場合もある。その場合は、内部へのアクセス権をテスターに与え、侵入した前提でテストを継続させるアプローチを採っている。このような柔軟な対応により、境界防御における対応だけではなく、侵入された後の検知、インシデント対応といった多層的な観点で、その対応態勢を評価できるようにしている。

e) 今後の動向

BoE は、第 1 フェーズで対象とした金融システム上重要な Firm/FMI に対し、今後も定期的に当局主導の CBEST を実施することを予定している。周期は、各 Firm/FMI の重要性に依る。また、今後は対象を拡大していくことも検討されている。具体的な実現方法について、本調査時点では正式に公表されていないが、同様のフレームワークを多くの金融機関に適用することはハードルが高いため、対象の Firm/FMI を 3 つの層に分けて導入する構想がある。第 1 層は、現状の CBEST の対象となっている Firm/FMI で同様のテストを継続、第 2 層は金融分野における共通の脅威プロファイルやシナリオをベースとしたテスト、第 3 層は脅威インテリジェンスの要素をどの程度とりいれるか、である。

現状の CBEST は、各フェーズにおいて SCT が主体的に関与し、GHCQ がシナリオのレビューを行うため、プロジェクト全体が長期化し、Firm/FMI の負担が増えているとの指摘がある。新しい構想では、一度 CBEST を実施している Firm/FMI には SCT の関与を限定的にし、第 2 層以下では共通のシナリオを利用することにより、ステークホルダーの負担を軽減させながら、金融分野全体のサイバー攻撃へのレジリエンスを高めるフレームワークを維持していくことが検討されている。

なお、CBEST によりもたらされた利点と課題については、5.3 章で述べる。

4.3. 欧州中央銀行による取り組み（TIBER-EU）

欧州中央銀行（以下「ECB」）では、現在、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 のフレームワークの開発を進めている。[14]

そこで、本章では、ECB が開発中の「European Red Team Testing Framework （以下「TIBER-EU」）」[15]について、その背景や目的、概要について述べる。

なお、TIBER-EU は、CBEST を参考にしながら 2017 年前半より開発が始まったばかりである。従って、記載された内容は、本調査時点で把握できた情報に基づくものである。

4.3.1. TIBER-EU

a) フレームワーク策定が検討されている背景

ECB 理事会は、2016 年 6 月に CPMI-IOSCO[16]が公表した「Guidance on cyber resilience for financial market infrastructures（金融市場インフラのためのサイバーレジリエンスに関するガイダンス）」[17]を踏まえ、2017 年 3 月、「ユーロシステム[18]のためのサイバーレジリエンス戦略」を策定している。この戦略は以下の 3 つの柱で構成されており、当局や金融市場がサイバーセキュリティ強化に向けた取り組みを拡大し、欧州金融システムのサイバーレジリエンス強化を目指している。

＜サイバーレジリエンス戦略の 3 本柱＞

- 金融市場インフラとの協力の下、サイバー防衛能力を確立し、サイバーセキュリティの成熟度を向上
- 当局間の相互連携、情報共有、脅威インテリジェンスの向上、欧州の法執行機関との緊密な連携、市場横断的な演習、サードパーティー・サプライチェーンに関する深い理解
- 金融業界と当局との戦略的な対話を確立し、共同での取り組みを加速し効果的な解決策を検討

また、欧州中央銀行制度には 27 ヶ国が参加しており、各国に中央銀行、金融当局が存在する。しかしながら、各国の中央銀行、金融当局が国境を越えて業務を展開する金融市場インフラに対し、個別の対策や

[14] https://www.ecb.europa.eu/paym/intro/news/shared/2017-11-21_cyber_security_regulation.pdf

[15] 公表されている文献では「European Red Team Testing Framework」と紹介されているが、ECB へのインタビューの結果、通常は「TIBER-EU」と表現されているため、本報告書では「TIBER-EU」と記載する

[16] CPMI は、決済・市場インフラ委員会。中央銀行が支払・決済の仕組みやクロスボーダーまたは多通貨決済スキームの動向についてモニタリングおよび分析を行うためのフォーラム。IOSCO は、証券監督者国際機構。証券監督当局のための国際政策フォーラムであり国際的な証券・先物取引に関する主要な規制上の課題を検討し、実務的な対応を調整することを目的としている。CPMI と IOSCO は FSB により承認された国際基準設定主体

[17] https://www.bis.org/cpmi/publ/d146.pdf

[18] ユーロシステムとは、27 の EU 諸国のうち、欧州中央銀行（ECB）と 19 の中央銀行で構成されており、ECB の指示の下、統一的な金融政策を実施する仕組み

規制を要求することは効率的ではない。そのため、当戦略には、各国の協調した取り組みの必要性が言及されている。

ユーロシステムは、第 1 の柱のもと、金融市場インフラがレジリエンスを高めるために有用ないくつかのツールの開発を進めており、そのツールの1つが、TIBER-EU である。

ECB は、TIBER-EU の開発以前に、ユーロシステムで利用されている全ての決済システムに対し、約 30 項目からなるレジリエンスに関するアンケート調査を実施しており、このアンケートにより決済システムのサイバー攻撃対応態勢を把握でき有益であったとしている。とりわけこの調査で強調されているのが、ガバナンス、企業文化、ビジネスプロセスの重要性である。すなわち、多くの決済システムが、防御、検知に関連する技術的対策に重点を置き、人やプロセスの整備、高度化に重点を置いていないことが明らかになったのである。またこれと同時に、それぞれの金融市場インフラが演習を通じて、サイバーへの意識向上を図ることの重要性を強調している。

各国当局や国際機関が金融市場インフラに対し、サイバーセキュリティに関する多くの規制を課す中で、ECB は、金融市場インフラが技術的な対策に加え、人、プロセスの対策もあわせた強化、また EU 全体の協調した取り組みの必要性を強調している。

このような問題意識の下、EU 全体で利用可能な TLPT のフレームワークの開発に着手している。

b) コンセプト

TIBER-EU は、以下のようなコンセプトで開発が進められている。

- EU には、複数の国で決済・金融サービスを提供する金融市場インフラが存在することを踏まえ、EU 全体として利用可能なフレームワークとすること。そのため、TIBER-EU を採用する複数の国の当局が連携して1つの金融市場インフラのテストに関与するケースも想定されている
- 国ごとに異なる規制がある中において、各国当局が利用可能なフレームワークとすること。すなわち各国当局が当該フレームワークを規制として導入するのか、あるいは任意で利用するかも含め各国でその取扱いを選択できる
- TIBER-EU を提供するテスター、プロバイダーの能力、信頼性は、サービスを受ける金融市場インフラ自身が評価、判断すること
- テストにおいては、法律、規制を確実に遵守すること
- フレームワークが金融分野全体のレジリエンスに寄与するよう、金融市場インフラのみならず、銀行、保険など複数の業態でも利用可能とすること
- テストは本番環境で実施すること

c) フレームワークの概要

TIBER-EU は、CBEST など、既に他国の金融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ため、いくつか異なるアプローチが含まれている。

特に、「EU 全体として利用可能とすること」や「フレームワークの取扱いを各国の選択に委ねること」といった点は重要なコンセプトである。従って、より具体的なテスト実施プロセスにおいては、こうした点が、色濃く反映されたフレームワークになると考えられる。

1) 体制の確立

当局とテスト対象となる金融市場インフラの間で、テストを実施するための体制が組成される。テストを効果的、安全に実施するため、対象機関には高度な専門知識を有する少人数(3～4 名)のホワイトチームが設置され、当チームがテストを全行程にわたって管理する。当局と当該金融市場インフラの間でテストのプロセス・コンセプト、ステークホルダーの役割・責任を確認、共有するとともに、対象機関はテストを安全に実施するためのセキュリティコントロール計画およびプロジェクト計画を作成する。

2) テスト範囲の決定

対象機関が保有する EU の金融システム上重要な機能を特定するとともに、それに基づきテスト範囲を決定する。テストの範囲の決定は、テストプロセスの中で重要であるため、対象機関によっては本プロセスに複数の当局が関与する場合がある。

3) プロバイダーの調達

現在のところ、TIBER-EU では、サービスプロバイダー市場が成熟していないため、CBEST のようなプロバイダーに対する資格認定制度は当面導入されない予定である。そのため、プロバイダーの選定は各金融市場インフラがリスクマネジメントの一環として自ら評価し、判断することとなる。

4) 金融分野共通の脅威インテリジェンスをベースしたシナリオの策定

CBEST との大きな相違として、TIBER-EU の場合は、金融分野における共通の脅威インテリジェンスレポートがあらかじめ定期的に ECB から提供される予定である。そのため、サービスプロバイダーは当該レポートを踏まえ、テスト対象機関に関する情報を収集・分析するとともに、対象機関の特性を考慮した上で、シナリオを作成する。

これは、個社ごとの脅威インテリジェンスレポートが必ずしも有益ではなかったという CBEST の教訓を踏まえ、共通の脅威インテリジェンスレポートの作成により、金融市場インフラの負担を軽減させるとともに、フレームワークを効率的なものとし、EU 全体での普及を目指しているものと考えられる。

5) 実施

レッドチームとなるサービスプロバイダーがシナリオに基づきテストを実施し、テスト対象機関は本番さながらのサイバー攻撃に対処する。原則ステルス方式で実施されるため、ホワイトチームには事前にテスト内容等が開示されるものの、ブルーチームとなる SOC やインシデント対応チームには開示されない。テストは法令を遵守し、ホワイトチームの管理下で障害が発生しないよう安全に実施される。

6) 振返りと改善計画の策定

サービスプロバイダーは、テストを通じて特定した脆弱性や課題をとりまとめ、テスト対象機関に報告書を提供する。報告書に基づき、当局、サービスプロバイダー、ホワイトチーム、ブルーチームの4者が合同でシナリオごとの振返りを行う。具体的には、検知・対応について何ができて何ができなかったか、対応の良し悪しはどうだったかなどを評価し、改善事項を整理する。すなわちテスト対象機関は、当局と連携しながら改善計画を作成するのである。

7） 結果の共有

テスト結果は、所管した当局に提出されるとともに、当該テスト対象機関に関係する他の EU 域内の当局にも共有される場合がある。例えば、ある国の当局がテストを企画する際に、他の国の当局がシナリオ策定に関与する場合には、関与した当局にもテスト結果が共有される。これには1つの機関が複数の当局からテストを要求されてしまう規制上の重複を避ける狙いがある。EU 全体として利用可能なフレームワークという点で重要である。

d）TIBER-EU の適用時期

本調査時点では、TIBER-EU が開発途上であったため、適用開始のタイミングは不明であるが、2018 年春には大枠の開発作業を終了し、その後 EU 各国等との必要な調整手続きを経た上で、早ければ同年後半には、TIBER-EU を活用した取り組みが開始される見込みである。

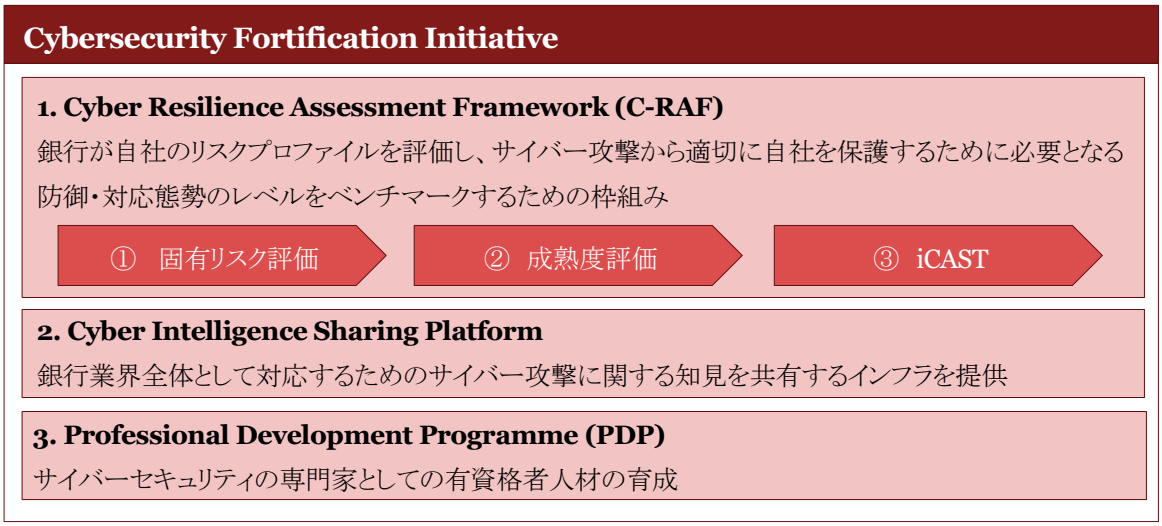
4.4. 香港による取り組み（iCAST）

香港金融管理局（Hong Kong Monetary Authority、以下「HKMA」）は、TLPT フレームワークである「Intelligence-led Cyber Attack Simulation Testing（以下「iCAST」）」を策定、公表（2016 年 12 月）し、2017 年より所管する銀行に適用している。iCAST は HKMA による銀行業界のサイバーセキュリティ強化のための各種取り組みの一部である。従って、本章では、HKMA の取り組みの全体像を紹介した上で、iCAST の策定の背景や、その内容、活用状況について述べる。

4.4.1. Cybersecurity Fortification Initiative[19]

HKMA は、2016 年 5 月に「Cybersecurity Fortification Initiative（以下「CFI」）」を公表している。これは、香港におけるサイバー脅威の増大を背景に、銀行業界のサイバーセキュリティへの取り組みを強化するための総合的な施策である。CFI は下図のとおり 3 つの柱で構成されており、iCAST は、「Cyber Resilience Assessment Framework（以下「C-RAF」）」の一部である。

図 4-9 Cybersecurity Fortification Initiative の全体イメージ



4.4.2. Cyber Resilience Assessment Framework (C-RAF)[20]

C-RAF は、銀行のサイバーレジリエンスを評価するツールであり、上図のとおり、3 段階で実施される。

a) 固有リスク評価

固有リスク評価では、HKMA が用意した評価マトリックスを用いて、銀行自身が接続しているインターネットサービスプロバイダーの数や、支店の数、クラウドコンピューティングの利用状況などを機械的に評価する。

[19] http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20160524e1.pdf および http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161221e1.pdf

[20] Cyber Resilience Assessment Framework（2016 年 12 月 HKMA）、当文書は公表されていない

銀行は、評価マトリックスで示された評価項目ごとの基準と自社の状況を照らし合わせ固有リスクレベルを 3 段階（High、Medium、Low）で確認できる。また、固有リスクレベルは、HKMA が期待するサイバーレジリエンスの成熟度レベル（baseline/intermediate/advanced）にマッピングされる。従って、固有リスクを識別することで当該銀行に期待される成熟度レベルが判定される。

b）成熟度レベル評価

成熟度レベル評価では、HKMA が用意した評価表を用いて、銀行の現在の成熟度レベルを 3 段階（baseline/intermediate/advanced）で評価する。評価表は、7 つの領域（ガバナンス、認識、防御、検知、対応と復旧、状況認識、外部委託管理）で構成されている。

現状の成熟度を評価することで、固有リスク評価から導き出された期待される成熟度レベルとのギャップを確認することができ、ギャップがある場合は、改善計画を策定する。

c）iCAST

固有リスクが「high」または「medium」であった銀行は、脅威ベースペネトレーションテストである iCAST を受検し、自身のレジリエンスを評価しなければならない。

d）C-RAF の実施者

固有リスク評価や成熟度評価を担当する Assessor と、iCAST の脅威インテリジェンス分析や実際のテストを担当するテスターは、下図のとおり、役割に応じた資格の保持が求められる。HKMA は Hong Kong Institute of Bankers（HKIB）、Hong Kong Applied Science and Technology Research Institute（ASTRI）と協力し、サイバーセキュリティのプロフェッショナル育成プログラム（Professional Development Programme）を構築した。また、資格認定機関である CREST の支援を受けて当該プログラムを設計している。当該プログラムに基づきトレーニングを受け、資格を取得したサイバーセキュリティの専門家は、Assessor やテスターを実施するに足る十分な専門性があると認められる。また、その他同等の資格を有する者にも、Assessor やテスターを担うことが認められている。ただし、同等の資格と判断する基準や方法が明確でないため、HKMA は現在、その点の整備を進めている。

各資格は個人で取得し、組織としての認定や資格は求められていない。また、HKMA は銀行が自ら評価を実施すべきか、または第三者に委託すべきか明示しておらず、銀行に判断を委ねている。

図 4-10 C-RAF の評価者と求められる資格要件

役割	資格
Assessor（固有リスク評価、成熟度評価を担当）	
Assessor	● Certified Information Systems Auditor (CISA), ● Certified Information Systems Security Professional (CISSP) または同等の資格
テスター（iCASTを担当）	
iCAST マネージャー （プロジェクトマネジメント）	● CCASP - Certified Simulated Attack Manager または同等の資格
iCAST スペシャリスト （脅威インテリジェンス＆ペネトレーションテスト）	● CCASP - Certified Simulated Attack Specialist または同等の資格
iCAST テスター （iCASTスペシャリストのアシスタント）	● CCASP - Certified Infrastructure Tester ● CCASP - Certified Web Application Tester または同等の資格

4.4.3. iCAST について

a) 導入の背景

第 2 章で述べたとおり、一般的なペネトレーションテストでは、特定の環境内で起こる技術的な脆弱性への詳細な評価は可能だが、銀行を対象とした攻撃シナリオを完全にカバーすることはできない。また、同テストでは、銀行のサイバー攻撃対応能力を評価したり、銀行のサイバーレジリエンスの有効性を評価するための指標や KPI を提供できない場合が多い。加えて、重要な情報資産（情報システムやデータなど）が技術的に高度で執拗な攻撃から保護されるという適切なレベルの保証を得るためには、テストを強化する必要があり、テスト実施者には最新の攻撃能力と脅威情報の活用が求められる。

これらのニーズと課題に対応するため、HKMA は BoE の CBEST を参考とするなどし、iCAST を開発、導入した。

b) ステークホルダー

iCAST に携わる担当者には、以下の 3 つの役割がある。各役割に求められる資格は図 4-10 のとおりである。

1) iCAST マネージャー

プロジェクト管理の観点からシミュレーションテストを管理する。iCAST マネージャーは、シミュレーションテストのすべての分野に関する幅広い知識を有し、インシデント対応、ペネトレーションテスト、およびシミュレーションテストの実績が求められる。

2) iCAST スペシャリスト

脅威インテリジェンスとペネトレーションテストの両方を実施する。脅威インテリジェンスの収集・分析を行い、脅威インテリジェンスレポートを作成するとともに、これに基づきテストシナリオを設計する。

また、様々なチャネル（フィッシング詐欺メール、ソーシャルエンジニアリング等）を通じてテストを実施し、最終的なゴールの達成を目指す。テストは iCAST スペシャリストが中心となって実施し、必要に応じて iCAST テスターがサポートする。iCAST スペシャリストには、ペネトレーションテストとシミュレーションテストの実績が求められる。

3) iCAST テスター

収集されたデータの分析や調査結果、評価レポートの作成など、iCAST スペシャリストのサポートを行う。

c) テスト実施環境

iCAST では、実際の攻撃に近い手法を再現するため、本番環境で実施することが想定されているが、本番のオペレーションに影響が懸念される場合、UAT 環境等の本番に近い環境で実施することもある。

d) リスクコントロール

実施環境の決定は、本番への影響を考慮しコントロールグループが行う。コントロールグループはテスト対象のシステムに関わる者から通常 1 人ずつ選出され、重要な情報資産やシステム、および当該資産やシステムに関連する実務上の機能を理解している必要がある。また、コントロールグループのメンバーは、テスト実施に伴うリスクや、サイバーインシデントが発生した場合のエスカレーションを理解しているなど、テストによる影響をコントロールできる者であることが求められる。

e) 実施プロセス

iCAST を実施する際の 5 つのフェーズは、以下のとおり。

1) スコープの決定（Scoping）

スコープを明確にするために、銀行は以下の点を検討し決定する。

- 主要な機能（Key Function）の特定
  銀行は、ビジネスにおけるすべての主要な機能と、それを支える機能を特定し、これら全てをスコープに含める。
- 重要なサーバー・システムの特定
  上記で特定された主要な機能をもとに関連する重要なサーバー・システムを特定する
- 各テスト目的に応じた脅威の決定
  重要なサーバー・システムを特定した後、脅威カテゴリー（機密性、完全性、可用性）を判断し、テストのゴールを定める。

2) 脅威インテリジェンスの分析（Developing threat intelligence analysis）

脅威インテリジェンスの分析を行い、レポートを作成する。レポートには、主な脅威の概要、リスクの高い脅威プロファイル、脅威アクターが銀行を攻撃する場合に想定されるシナリオが含まれる。また、iCAST では、固有リスクのレベルに応じて求められる脅威インテリジェンスレポートが異なる。

- 固有リスクが「Medium」の場合
  香港銀行業界の脅威状況をカバーする一般的な脅威インテリジェンスレポートが求められる。
- 固有リスクが「High」の場合
  対象の銀行をターゲットとする脅威情報に基づき、個社ごとにカスタマイズし作成された脅威インテリジェンスレポートが求められる。

3) テストシナリオの作成（Developing testing scenarios）

脅威インテリジェンスレポートを基に、テストシナリオを作成する。各シナリオには、以下の項目が含まれる。

- テストゴール
  各テストシナリオに関する最終ゴールを示すものであり、テスターが金融機関に攻撃を行う際の根拠となる。
- テストの開始方法
  攻撃の開始時に使われる攻撃チャネル・技術に関する情報。
- タスクチェーン
  テストの開始から合意されたゴールに達するまでの段階の流れ。
- マイルストーン
  内部システム、サービス、コンピューターリソースへのアクセス・コントロールを取得する等、テストの中間ゴール。
- タイムライン
  各タスクを完了するために必要な時間を設定する。もしタスクが時間内に完了できなかった場合は、攻撃に対する防御に成功した、または攻撃を検知したとみなされる。テスト結果には、攻撃の成功、失敗が KPI として最終レポートに記載される。
- テストの中止・継続の条件
  テスターがテストを中止・継続するために、銀行からサポートを受ける必要がある場合の条件を事前に定める。

4) 実施（Test）

作成されたシナリオをもとに、テストが実施される。テスト中は、コントロールグループに少なくとも週次で状況が報告され、テストの進捗、遭遇した障害、テストを継続すべきかの判断などを共有する。

5) 報告（Reporting）

テスト終了後、以下のレポートを作成する。

- iCAST シミュレーションテストの概要（iCAST simulation test summary）
  銀行がテスターの支援のもとで作成する。銀行の経営陣は、テスト結果をレビューし承認する。
- 脅威インテリジェンスレポート（Threat intelligence report）
  本レポートは、脅威インテリジェンス分析の要約を含めて作成される。
- シミュレーションテストレポート（Simulation testing report）
  本レポートには、テストのアプローチ、テスト結果、考察、また必要に応じて改善点が含められる。改善点は、ガバナンス、ポリシー、手続、技術的な統制、教育、啓発の観点から記載される。なお、テストが銀行の内部リソースにより実施された場合には、経営陣がレポートをレビューし承認する。

4.4.4. 運用実態と今後

HKMA は、C-RAF による評価を 2 つのフェーズに分けて実施しており、第 1 フェーズでは、全ての主要なリテール銀行と少数のグローバル規模の銀行・中小銀行の計 30 銀行を対象としている。

第 1 フェーズでは、固有リスク評価および成熟度評価を 2017 年 9 月末、iCAST を 2018 年 6 月までに完了することとしている。[21]なお、第 1 フェーズで iCAST の対象となった銀行は、20 程度と見込まれている。また第 2 フェーズは、残りの全ての銀行が C-RAF の対象となり、固有リスク評価と成熟度評価を 2018 年末までに完了する予定である。なお、iCAST の完了予定期限は公表されておらず不明である。

テスターについて

以下の理由により、iCAST のテスターには、CBEST やそれと同様のテスト実施経験を有するグローバルファームや海外のプロバイダーが選定されているケースが多い。

- iCAST フレームワークは、CBEST フレームワークと比較すると、テストの各フェーズで実施すべき作業内容や作成する成果物に関する説明が少なく、詳細が明確でない。そのため、CBEST 等の経験がないサービスプロバイダーがテストを行うことが困難となっている
- CBEST と比較すると、iCAST フレームワークを導入する前の、銀行、サービスプロバイダー、当局の間の事前協議が十分に実施されていない
- 銀行内部の人材をテストで活用することも認められているが、テスターに要求される資格、専門性を有する人材が銀行にはほとんどいない

今後の動向

iCAST を今後定期的に実施する必要があるかは明確ではないが、C-RAF の成熟度レベル評価の項目には、統制原則（Control Principle）として、「脅威インテリジェンスを活用したテストシナリオの作成と iCAST の実施」が含まれている。そのため、銀行には今後も iCAST を定期的に実施することが期待されているものと考えられる。

[21] http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20161221e1.pdf

4.5. シンガポールによる取り組み

シンガポールについては、シンガポール通貨監督局（Monetary Authority of Singapore、以下「MAS」）およびシンガポール銀行協会（Association of Banks in Singapore、以下「ABS」）が、一般的なペネトレーションテストに関するガイドラインをすでに策定している。本調査時点では、当局が主導する TLPT のフレームワークは存在していないものの、足元では、同フレームワークの策定に向けた動きがある。

本章では、これまでに当局が公表している主なガイドラインの概要を紹介するとともに、足元で検討が進められている同 TLPT フレームワークに関する動きを述べる。

4.5.1. 一般的なペネトレーションテスト等に関する当局のスタンス

a) TECHNOLOGY RISK MANAGEMENT GUIDELINES[22]

これは 2013 年 6 月に MAS が公表したガイドラインであり、規制対象金融機関に対し、適切なテクノロジーリスク管理のフレームワークを構築することや、システムのセキュリティ、信頼性、耐障害性を備えること、また、これらのシステムで取扱う顧客データや取引データ保護のための強固な認証の適用を求めている。

ガイドラインの中にでは、脆弱性評価やペネトレーションテストの実施に関する項目があり、その中には、金融機関は、インターネットに面したシステムについて少なくとも年次でペネトレーションテストを実施すべきとの記述がある。

b) SYSTEM VULNERABILITY ASSESSMENTS AND PENETRATION TESTING (Circular No. SRD TR 01/2014)[23]

これは 2014 年 5 月に MAS が金融機関に発出した通知文書である。上述したガイドラインの内容と比較しても特段の目新しい内容は示されていないが、金融分野に対するサイバー脅威の高まりを受け、ガイドラインで示している脆弱性評価やペネトレーションテストの意義を改めて周知したものと考えられる。

c) Penetration Testing Guidelines for the Financial Industry in Singapore[24]

2015 年 6 月に ABS が MAS と連携して公表した、インターネットからアクセス可能な金融機関のオンラインシステムに対して、ペネトレーションテストを実施する場合のガイドラインである。しかしながら、金融機関に対する脅威インテリジェンスを活用してシナリオを策定するものではなく、一般的なペネトレーションテストである。

なお、同ガイドラインの活用は金融機関の任意であるものの、銀行のみならず様々な業態の金融機関に広く浸透しており、金融機関がペネトレーションテストを行う際には積極的に活用されているようである。

---

[22] http://www.mas.gov.sg/~/media/MAS/Regulations%20and%20Financial%20Stability/Regulatory%20and%20Supervisory%20Framework/Risk%20Management/TRM%20Guidelines%20%2021%20June%202013.pdf

[23] http://www.mas.gov.sg/Regulations-and-Financial-Stability/Regulations-Guidance-and-Licensing/Merchant-Banks/Circulars/2014/SRD-TR-01-2014-System-Vulnerability-Assessments-and-Penetration-Testing.aspx

[24] https://abs.org.sg/industry-guidelines/cyber-security

4.5.2. 当局主導による TLPT フレームワーク策定に向けた動き

シンガポール当局へのインタビューの結果、現在、MAS と ABS が連携して、TLPT フレームワークの策定に向けた取り組みを推進していることが確認された。

ただし、TLPT のフレームワークの策定は進行中であり、以下の内容は、本調査時点で把握できた情報である。

a) TLPT フレームワークの検討主体

現在、ABS に「サイバーセキュリティに関する常任委員会（Standing Committee on Cyber Security、以下「SCCS」）」が設置され、検討が進められている模様である。SCCS は、これまでも MAS と緊密に連携しており、その代表的なものが上記で記載した「c) Penetration Testing Guidelines For the Financial Industry in Singapore」の策定である。今回の TLPT フレームワークの策定も類似の取り組みであるため、主体は ABS であるが、MAS が関与して推進していると考えられる。

b) 公表時期

公表時期はアナウンスされていないが、2018 年 12 月末までには公表される可能性が高いと言われている。なお、当該フレームワークの公表にあたり、パブリックコメントが実施されるかは不明である。

c) 適用方法と範囲

フレームワークの適用方法や範囲は明らかにされていないが、上述のペネトレーションテストのガイドラインの適用が任意であることから、TLPT のフレームワークの適用も同様に任意になるものと考えられる。また対象範囲についても、銀行に限らず広く金融機関での活用が期待されているものと考えられる。

■ 5. TLPT の活用に伴う利点と課題

5.1. 概要

諸外国の金融分野における TLPT の活用状況、および当局が主導する TLPT の取り組み状況を述べてきたが、本章では、全体を通して確認できた TLPT の利点や課題について述べる。

また、当局主導で TLPT を推進する場合の留意点について、昨年「Global Financial Markets Association（以下「GFMA」）」[25]から提言が出されており、この点もあわせて述べる。

5.2. TLPT の一般的な利点と課題

5.2.1. TLPT の利点

a）攻撃者視点

TLPT の大きな特徴の 1 つが、脅威インテリジェンスの活用である。これは、個々の金融機関あるいは業界の IT やビジネス特性、さらには地政学的リスクといった点も踏まえ、金融機関が実際に直面するおそれのあるサイバー攻撃を分析し、そこから導かれる脅威シナリオを作成してテストするものである。脅威アクターの種類や攻撃目的・手法を想定しテストをシミュレートすることは、今後起こり得る被害の未然防止あるいは影響を最小化することにつながり、金融機関にとっては、効果的なアプローチである。

もちろん、TLPT は限られた期間あるいはコンプライアンスの下で実施するため、偵察行為に膨大な時間とコストをかけ、法律や倫理観等を一切無視して攻撃する本物の脅威アクターとは異なる。しかしながら、個々の金融機関の置かれているビジネス環境やシステムの構成には、それぞれ特徴があり、攻撃者の立場からすれば当然そのような特徴をくまなく調べ、その中から弱点を見つけて攻撃を仕掛けてくることが想定される。従って、攻撃者の視点、すなわち脅威インテリジェンス分析に基づくシナリオを用いて攻防をシミュレートすることは、自組織のサイバー攻撃対応態勢の実効性を高める上で有効である。

b）実戦的な能力の評価

金融機関は、情報連携や意思決定プロセスを確認するための机上演習、専門機関が提供する技術的な演習などに参加することにより、インシデント対応の向上に努めている。もちろんこれらも重要な取り組みであるが、TLPT はいわばこれらをミックスした上で、実際の攻撃さながらに自社の本番環境で行われる。また、ステルス方式で実施されることから、事前準備が出来ない中で臨機応変な対応が試され、実戦力を高めることが可能な手法である。

[25]世界の主要な 3 つの金融業界団体（AFME（欧州）、ASIFMA（アジア）、SIFMA（北米））を包括し、グローバルな規制上の問題提起、政策提言活動の協調を促進する組織

ヒヤリハットや実際の攻撃被害を経験した金融機関は、その後、サイバーセキュリティ強化の取り組みが更に進むという傾向がある。これは真の意味で、対策の不十分さや危機感を経営陣も含めて体験したことがきっかけとなっている。TLPT は、シミュレーションではあるものの、類似の効果が期待できる。

また、職員が仮にインサイダーとしてサイバー攻撃に加担した場合は、攻撃者に簡単に侵入を許し被害がより大きくなるおそれがあるが、こうしたシナリオを現実に意識し、被害を想定することは机上では難しい。TLPT ではインサイダーシナリオを検証することで、起こりうる被害を体験することが可能となる。

TLPT の活用によって、金融機関は自らの能力を正しく理解することが可能となる。

c) 全社的な取り組み

TLPT は従来のペネトレーションテストとは異なり、単に「技術的側面」だけではなく、「人・組織面」や「プロセス面」における脆弱性や問題点を洗いだすことが可能なアプローチであり、このような組織全体へのアプローチが TLPT の優位性である。また、単に人・組織の問題といっても、それが感染源となる端末等のエンドユーザーのリテラシーに起因するのか、SOC チームの監視、検知能力不足なのか、あるいはインシデント対応を担う CSIRT メンバーの技術力不足なのか等、原因は様々考えられる。TLPT では、人・組織、プロセス、技術の各側面について、サイバーキルチェーンの段階ごとに、どのような脆弱性や問題が潜在的に存在するのかを体系的に評価することができるため、多層防御における弱点を把握しやすくなる。

サイバーセキュリティは経営目線で考えるべきであるといわれて久しいが、このようなアプローチは、組織全体を俯瞰した上で問題の所在を明らかにすることができるため、改善のための経営判断を促すインプットに活用できる。

d) サプライチェーンを含めた評価

金融機関の事務やシステム保守、あるいはサイバーセキュリティ機能の一部である SOC 機能等は、しばしば外部の専門業者に委託されている。しかしながら、過去のサイバー攻撃事案では、サプライチェーン上の弱点が狙われ、委託先で扱われている重要情報が窃取される事例が起きている。外部委託された業務に重要性がある場合は、TLPT のスコープに委託先の業務を含めることにより、当該金融機関のサプライチェーンを含めた評価が可能となる。

また、金融機関は、SOC を外部委託しているケースが多い一方、サイバーセキュリティの専門知識が不足しており、委託先によって提供されている機能の実効性や課題の有無を十分に評価できていない状況である。そのため、委託先が提供しているサイバーセキュリティサービスの能力や、委託先と自社との間の連携プロセスを評価する意味においても、TLPT は有効である。

5.2.2. TLPT の課題

このような利点がある反面、以下のような課題があると言われている。

a) テスターに対する信頼性

テスターは金融機関のシステム内部に侵入するが、高い専門的技術を有していることから、金融機関の防御や検知機能をかいくぐることが可能な場合も多い。従って、悪意あるテスターを利用した場合、情報窃取やスパイ行為につながるおそれがある。

このような懸念へ対応するためには、金融機関として、信用できるサービスプロバイダーやテスターを選定することが重要である。一例としては、CREST 認定プロバイダーやテスターを選定すること等が考えられる。またサービスプロバイダーが、自社に所属するテスターの信用調査や犯罪履歴調査を実施し問題のないことを確認しているかなど、サービスプロバイダー側のチェックプロセスを通じて、テスターが信頼できる人物かを適切に判断することが重要である。

なお、サービスプロバイダーにおいても、この点は重要視しており、諸外国では CREST 等の認定を積極的に取得し、テスターは正社員のみで構成する等の取り組みがなされている。

b) 本番業務への悪影響

TLPT は原則として本番環境で行うため、顧客サービスの停止など、金融機関の日常業務に悪影響を与え、場合によっては金融システムに悪影響を及ぼすおそれもある。このような影響を懸念する声は、ヒアリングした大手金融機関およびサービスプロバイダーから聞かれている。その主な原因は、①テスターの技術力の不足、②テスターと金融機関との間の事前準備不足などである。

①のテスターの技術力が不足している場合は、テスターが誤った操作をしたり、事前に準備した擬似攻撃ツール(RAT や C&C サーバー等)の品質が悪く、想定外の挙動をすること等が考えられる。このような懸念への対応として金融機関では、テスターが CREST などの専門資格を有していることや、金融機関に対するテスト経験が十分であるか等を確認することが重要となる。

一方、②のテスターと金融機関との間の事前準備不足による本番業務への悪影響については、双方の経験不足や信頼関係に起因する部分が大きい。そのため、サービスプロバイダーの選定も大事であるが、適切な TLPT のフレームワークを確立し、緊密なコミュニケーションを図ることや、金融機関の情報資産へのダメージや金融分野の重要なサービスに障害が生じないよう、テスト関係者による責任あるリスク管理フレームワークの構築が重要となる。

5.3. 当局主導の TLPT から見えてきた利点と課題

当局主導の TLPT のうち、本調査時点で十分な実績があるのは、CBEST のみであることから、ここでは CBEST の利点と課題を述べる。

a) CBEST の利点

1) 取締役や経営レベルにおけるサイバー脅威に対する認識の向上

CBEST を実施した効果として顕著であった点は、経営トップのサイバーの脅威に対する認識の向上である。これは、ヒアリングした金融機関全てから聞かれた。BoE が CBEST をスタートした当初、既に様々なサイバーセキュリティ対策を実装し防護力を高めていると自負のあった大手金融機関の経営陣は、障害を伴うおそれのある本番環境で TLPT を実施する意義を見出せずにいた。しかしながら、BoE と経営陣との間で TLPT の必要性について十分な時間をかけて相互理解が図られ、また、テスト結果については、経営レベルが関与する形で BoE や当局がレビューすることを通じて、金融機関がさらされているサイバーリスクとそのリスク対応としての TLPT の重要性を経営レベルで認識するに至った。その結果、これら金融機関では、サイバーセキュリティが経営上の重大なリスクと認識され、必要な投資が行われるようになっている。

また、CBEST を通じて経営陣は、TLPT を標準的なリスク評価手法の一つと認識し、自主的に CBEST と同様のテストを行うよう求めるとともに、TI 機能や PT 機能を内製化するなどの取り組みを進めている。このようにサイバーセキュリティ対策が脅威ベースすなわち洗練された現実の脅威を意識したものに変化してきている。これは、サイバーセキュリティは決められた対策を網羅するだけでは十分ではなく、絶えず変化する脅威に対し継続的に対処していく必要性を取締役レベルが認識できるようになったからである。

2) サービスプロバイダーの品質確保と市場形成

CBEST を実施するサービスプロバイダーは、4.2.2 章で述べたとおり CREST と BoE の認定が必要である。BoE は、テストを受ける金融機関のリスクを可能な限りコントロールするために、時間をかけてサービスプロバイダーの認定の仕組みを整備した。TI については課題があるものの、金融機関にとって、認定制度はサービスプロバイダーの品質確保に寄与していると考えられる。受検した金融機関において、本番業務に影響があったなどの事例はヒアリングした金融機関からは聞かれていない。このような BoE を中心とした取り組みが、英国のサービスプロバイダー市場の質・量をともに向上させ、TLPT が普及する要因になったと考えられる。

3) PDCA サイクルの定着

TLPT の目的は、金融機関にサイバーセキュリティ上の問題がないことを証明することではなく、内外の環境変化や高度化・巧妙化するサイバーの脅威から生じる新たな課題を適切に認識し、改善していくことにある。CBEST もその観点から PDCA サイクルの考え方を基礎としたプロセス設計がなされ、さらに当局が関与することによって実効的な PDCA をサポートするフレームワークとなっている。そのため、CBEST を経験した金融機関の多くは、自主的に同様の TLPT を実施することを自組織のセキュリティ評価プログラムに導入し、継続的な改善と高度化を図るサイクルを定着させている。

4) 大手金融機関の脆弱性に対する当局の知見の向上

CBEST を通じて、英国金融システムに大きな影響を及ぼすおそれのある大手金融機関のサイバー攻撃対応態勢上の脆弱性・課題を把握できるようになり、当局の知見が向上したとしている。

b) CBEST の課題

1) 脅威インテリジェンスフェーズの効果が限定的

CBEST では、認定資格を有する TI を活用することになっているが、開始当初は、脅威インテリジェンス自身が比較的新しい領域であったため業界共通のフレームワークが十分確立されていなかったことや、TI の選択肢が限られていたことから、一部の TI が策定した脅威レポートは、金融機関ごとに作成されていたにもかかわらず、内容に大きな差異はなく業態共通的な内容になっていた。

また、CBEST の対象となったグローバルにビジネスを展開する大手金融機関の中には、自社内に成熟した脅威インテリジェンス機能を有するところもあった。そのため、自社で得られた情報と TI の提供する情報に大きな差異がなかった。

2) 機密性の高い情報の取扱い

CBEST では、テスト結果報告書が当局に提出されるが、報告書には、TLPT で特定された脆弱性に関して、技術面に関する詳細な内容が含まれている。従って、一部の金融機関は、当局への提出とはいえ、機密性の高い情報が漏えいするおそれがある点に懸念をもっていた。

3) 英国に偏った評価スコープ

CBEST の対象となった大半の金融機関はグローバルにビジネスを展開する大手金融機関であり、彼らの重要システムはグローバル共通で使われている場合が多い。その一方で、CBEST は、英国当局の権限で実施されるため、英国における金融システム上の重要機能が評価スコープとして定義されている。従って、テストが英国拠点に偏ってしまう傾向があり、グローバルの視点が不足しているのではないかと言われている。

5.4. GFMA による提言

CBEST は、他の金融当局からも注目を集め、香港、EU、シンガポール、オランダも、CBEST と類似した TLPT フレームワークの整備や検討を行っている。

こうした動きは、各国金融分野におけるサイバーセキュリティの強化に資する一方、各国当局が調整をせず各々取り組みを進めていることへの懸念がある。例えば、2017 年 12 月に GFMA が公表した「Key Principles for a Commonly Accepted Penetration Testing Framework」[26]（以下「提言」）では、TLPT がサイバーセキュリティを確保する上で有益かつ効果的なツールであるとする一方、TLPT に当局が関与することによる懸念とそれを解決するための意見を表明している。

提言の内容は、今後、各国の当局が TLPT を主導する上で参考となる可能性があるため、以下、その内容について述べる。

a）懸念の背景と概要

- ペネトレーションテストは、金融機関の強固なセキュリティプログラムを実現するための最も重要なツールの 1 つであり、このようなツールの活用により金融機関は自身のシステムや防御能力を評価でき、結果として脆弱性の特定、修復が可能となる。これはサイバーの脅威に直面する金融インフラを強化することにつながる。
- 一方、世界中の当局の関心の高まりによって、当局が主導するペネトレーションテストに関し、多くの取り組みが行われている。ペネトレーションテストのメリットは大きいものの、当局の関与の度合の高まりは、意図せず様々なリスクを増幅させるかもしれない。
- 例えば、テストで明らかになった金融機関の脆弱性など機密性の高い情報が複数の関係者に共有されてしまうことや、当局の規制が金融機関の採用するテストの選択肢を狭めてしまうおそれがあること、テスト対応チームは規制の増加によりその遵守に多くの時間が割かれ効率性を阻害されること、規制上のフレームワークが複数存在することにより整合性のとれないテストが実施されること、等が挙げられている。とりわけ、グローバルにビジネスを展開する金融機関は、こうした懸念に直面している。
- そのため、GFMA は、金融機関・金融インフラのサイバー防御能力をテストする際に、リスクを最小限に抑えたい金融機関のニーズを満たしつつ、当局が金融機関のサイバーセキュリティ対応態勢を評価できる、実現可能なアプローチが必要であると主張している。

[26] http://gfma.org/uploadedFiles/News/GFMA_in_the_News/2017/GFMA-Penetration-Testing-Principles.pdf

b）共通フレームワークの原則

GFMA は、金融業界と当局の双方のニーズに対応した、グローバルの TLPT フレームワークの開発の必要性を主張している。こうしたフレームワークを活用していくことこそが、結果として世界の金融市場と経済の持続的な信頼、成長を可能にすると述べている。

その上で、以下の原則に基づく、一般的に受入れ可能な TLPT のフレームワークを確立することによって、金融機関に対するリスクを最小限に抑えながら、業界、当局が TLPT のメリットを最大限に享受できると主張している。

GFMA が主張する共通フレームワークの原則

- 金融機関は、TLPT プログラムを自ら主導できる能力を金融当局に提供すべきである。また、TLPT プログラムは、①最新の脅威インテリジェンス、②共通のリスクベースシナリオを使用することを通じ、監督目的を満たすこと、③テストは、合意されたテストスケジュール・スコープで行うこと、に基づくべきである。
- 金融機関は、想定する脅威アクターを適切に再現するために、洗練された技術・ツールを有する、訓練を積み認定を受けた者による TLPT を実施し、当局に対してその信頼性の高さを提供すべきである。
- 金融機関は、テストによって把握された弱点に適切に対処できるというガバナンスプロセスの透明性を当局に提供すべきである。
- 金融機関は、オペレーショナルリスクを最小限に抑える手法でテストを実施すべきである。
- 金融機関は、情報が極めてセンシティブである性質を踏まえ、テスト結果データを厳格なプロトコルで処理するなど、データセキュリティを確保すべきである。

■ 6. わが国金融分野における TLPT の活用にむけて

6.1. 概要

本調査を通じて、諸外国では、大手金融機関を中心に自主的な取り組みとして TLPT が積極的に活用されていること、並びに英国や EU、香港、シンガポールにおいて、当局主導による TLPT フレームワークの策定や活用の動きが確認できた。もちろん、TLPT を活用する際の課題があるものの、それ以上に利点も確認された。そのため、諸外国では官民いずれの主導かによらず積極的に TLPT が活用されている。

他方、わが国金融分野における TLPT は現状普及しているとは言えない。

そこで、本章では、今後、わが国金融分野において TLPT を活用していくためのポイントを示し、本報告書を締めくくりたい。

6.2. TLPT の活用に向けて

6.2.1. TLPT の認知度の向上

本調査の結果、ここ数年の間に TLPT は、金融機関の自主的な取り組み、当局主導の取り組みに関わらず、諸外国の金融機関において、サイバーセキュリティの効果的な評価手法として認知度が高まり、広く活用されている。

したがって、まずはこのような評価手法を、わが国の金融分野においても広く認知させていくことが重要である。この点については金融庁も、平成 29 事務年度金融行政方針[27]の中で、サイバーセキュリティ対応能力をもう一段引き上げるための高度な評価手法の一つとして TLPT を挙げている。

今後、さらなる活用を促進するためにも、金融庁あるいは金融 ISAC 等の関係団体が、TLPT の手法やそのメリットを広く金融機関に紹介し認知度を高めていくことが重要である。

また、本調査では、個社ごとの固有の脅威インテリジェンス分析は行わず、金融分野共通の汎用的な脅威シナリオを基礎として TLPT を行う事例が見られた。TIBER-EU でも、EU 圏の様々な金融機関が TLPT を活用することを念頭に、汎用的な脅威インテリジェンスレポートを採用する予定である。このような効率的な方法も参考に、大手金融機関だけではなく地域金融機関などにも順次活用を促していくことが重要である。

TLPT を普及させていく段階では、その活用に懸念の声が出てくることも想定される。CBEST 導入初期のように、リスクのある本番環境で TLPT を実施する意義を見出せない先も出てくると思われる。このような懸念を払拭するには、経営陣の正しい理解が必要である。従って、金融庁は、経営陣に対して、TLPT の利点や活用する場合に対処すべき課題を丁寧に伝え、効果的な評価ツールとしての理解・認識を共有し、活用を促していくことが重要である。

[27] https://www.fsa.go.jp/news/29/2017StrategicDirection.pdf

6.2.2. 活用段階における当局の関与

TLPT は、当局の検査・監督ツールとしても活用できる有効な手法と考えられる。これまで述べてきたとおり、複数の国において、当局が主導し TLPT を活用している。そのため、わが国においても類似のアプローチは選択肢の一つとなり得ると考えられる。しかしながら、その場合は当局側にも相応のリソースや専門性が必要となるほか、金融機関に過度な負担を強いる可能性があるなど、克服すべき課題は多い。

従って、TLPT が普及していないわが国の現段階においては、拙速に当局が TLPT を主導するのではなく、例えば、金融行政方針や監督指針などを通じて、TLPT の活用に関する当局の考え方を示し、まずは金融機関に自主的な活用を促していくことが先決である。

TLPT の実施が目的ではなく手段であることを踏まえれば、本質的には金融機関がリスクに応じて自主的にサイバーセキュリティ対策を推進する中で、TLPT が活用され、結果として、効果的な評価や自律的なサイバーセキュリティの強化・改善といった PDCA サイクルを機能させることが重要である。

他方、自主的な取り組みに任せる場合に留意すべきことは、当局の期待と異なる運用がなされ効果を生まないなど、金融機関における TLPT の活用が形骸化してしまうことである。TLPT を実施する目的は、金融機関にサイバーセキュリティ上の問題がないことを証明することではなく、刻一刻と変化し巧妙化していくサイバーの脅威に応じて、新たに生じる課題あるいは高度化すべき点を金融機関が適切に把握・改善していくことにある。よって、その目的を確保するためにも、金融機関が自主的に実施する TLPT において、当局が、その活用状況やテストの結果、改善計画を適切に把握するなど、一定程度関与しモニタリングしていくことが期待される。

6.2.3. サービスプロバイダーの品質と信頼性

サービスプロバイダーの品質や信頼性の確保、またそれらに起因するオペレーショナルリスクを最小限に抑えた TLPT の実施は、金融機関の大きな関心事の 1 つである。しかしながら、TLPT の活用が限定的なわが国においては、TLPT のテスターやサービスプロバイダーの資格を認定する制度はなく、TLPT の経験を有するサービスプロバイダーは限られており、品質や経験にバラつきがある。このような点に関する根本的な解決は短期的には難しく、実際 TIBER-EU においても、欧州のサービスプロバイダー市場が未成熟であることを理由に認定制度は当面導入せず、金融機関の選択に委ねるとしている。従って、わが国で TLPT を活用する場合も、金融機関は外部委託先管理と同様にサービスプロバイダーの品質・信頼性を適切に評価・選択することが必要である。

他方、TLPT の普及とサービスプロバイダー市場の充実は、にわとりと卵の関係にある。今後 TLPT の活用が民間においてどこまで普及していくのか、あるいは当局が TLPT の活用をどこまで促進していくのかに依る部分もあるが、一定の品質と信頼性を確保するという点においては、供給側であるサービスプロバイダーやテスターの品質と信頼性を客観的に評価できる認定制度の整備が、中長期的には望まれる。CREST のような資格認定機関の設立や、官民連携コンソーシアムを通じた枠組みも含め、将来の TLPT の活用拡大を見据えた適切な資格認定制度の枠組みの検討は一考に値する。

6.3. おわりに

サイバー攻撃は急速に高度化・巧妙化しており、サイバーセキュリティが脅かされるリスクは、より一層高まっている。このような状況において、サイバーセキュリティの確保は、金融システム全体の安定性の実現、あるいは顧客利便、顧客保護を実現するための喫緊の課題である。

わが国の金融機関は、このような認識の下、ここ数年サイバーセキュリティの確保に向けた取り組みを進めている。例えば、技術面においては、多層防御システムや統合ログ監視システムの導入などである。また、人・組織、プロセス面においても、サイバー人材の育成や採用、CSIRT の設置、情報共有、インシデント対応計画の整備など、多面的にサイバーセキュリティを強化してきている。

ただし、このような取り組みは形式的に整備されるだけではなく、現実の脅威に直面した際に有効に機能してこそ真の価値がある。

海外に目を向ければ、ATM や SWIFT、IoT 等が悪用されているように、多様かつ洗練された攻撃が次々と発生している。また国内では、デジタルイノベーションに伴い金融ビジネスやインフラがオープン化の方向に変化してきており、そこには新たなリスクが伴う。加えて、わが国が国際的なイベントを控えている現状や地政学的なリスクを踏まえれば、金融分野における脅威はますます高まっていく。

このような状況においては、高度な攻撃を形式的な取り組みで防護することは困難であり、金融機関の経営者には、自組織の「実戦力」を適切に評価し、真の価値を把握することが求められている。現実的な脅威シナリオを踏まえた効果的な評価手法を活用し、刻々と変化するサイバーの脅威を踏まえた適切なリスク評価や実戦経験を通じて、洗いだされた自組織の弱点を迅速に改善し、サイバー攻撃対応態勢を向上させていくことが、何よりも重要である。その際、TLPT は有力な評価手法の一つの選択肢となり得ると考えられる。

これまで実施してきた様々な取り組みが、効果を生むかわからない単なる「コスト」に終わってしまうのか、あるいは、リターン、すなわち真の価値を生む「投資」になるのかは、組織の「実戦力」に左右される。「仏作って魂入れず」とならないよう、TLPT を効果的に活用し、「技術面」のみならず、「人・組織」、「プロセス」における問題を特定し改善につなげていくことが、金融機関には期待されている。

本報告書が TLPT の普及に役立ち、わが国金融分野のサイバーセキュリティ向上につながれば幸いである。

ご注意

本報告書内に記載されたインターネット上の URL は 2018 年（平成 30 年）1 月現在のものであり、URL およびその内容は、その後、変更、移動、削除される場合がある。

2017 年（平成 29 年）度　金融庁委託調査

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

PwC あらた有限責任監査法人
2018 年（平成 30 年）1 月 31 日　発行