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（仮訳）

要旨

サイバー攻撃の巧妙さや執拗さが増大し、グローバルに相互接続された金融システムに混乱を生じさせるおそれがある中、G7は2016年の「金融セクターのサイバーセキュリティに関するG7の基礎的要素(G7基礎的要素)」の公表以降、金融システム上、重要な金融機関のサイバーレジリエンス（サイバー攻撃への耐性やダメージからの回復）対策の強化に向けて、公的・民間部門の取組みを一層強めるためのフレームワーク策定を促している。

これらの取り組みには、2017年に公表された「金融セクターのサイバーセキュリティの効果的な評価に関するG7の基礎的要素（評価のG7基礎的要素)」によって強調されているように、確実な評価のもと、サイバーレジリエンス対策の強靭性を確保するためのステップが含まれる。「評価のG7基礎的要素」には、サイバーレジリエンスを評価するフレームワークを策定する際に、検討され取り入れられるべき要素が含まれる。

「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（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。「TLPTのG7基礎的要素」は、サイバーレジリエンスの幅広い評価ツールを補完することを意図しており、唯一の手法とみなされることを意図していない。

「TLPTのG7基礎的要素」の中心的な目的は、以下により、金融機関や、より一般的には金融セクターのサイバーレジリエンスを強化および評価することである。

- G7各国で共通したTLPTを実施するための中心的な要素や手法を提供する。「TLPTのG7基礎的要素」は、各国におけるTLPTの手法の互換性の確保を容易にすることを目指すとともに、各国独自の市場や規制への柔軟性や地域適合性の確保を促すこと
- TLPTの活用を検討する各国当局に指針を提供すること
- 金融機関にTLPTによる自己評価の実施に関する指針を提供すること
- 当局間の相互連携および多国籍で活動する金融機関のクロスボーダーのTLPTを支援し、テスト結果の相互認証を容易にすること

「TLPT の G7 基礎的要素」はさまざまな TLPT の手法の互換性を高めることを目指すものであり、既存のフレームワークを無効化したり、変化する脅威状況へ継続的に適応することを妨げるものではない。

TLPT とは？

TLPT[1]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。***

TLPT の目的は？

TLPT の目的は、現実世界をまねたサイバーインシデントに対する、金融機関のレジリエンス能力を評価し、気付きを与えることにある。TLPT は、決められたスコープ内で実施され、金融機関へのリスクを最小限に抑えるテストとなるよう、確実にコントロールされたリスク管理プロセスを取り入れるべきである。

TLPT の G7 基礎的要素は誰のため？

「TLPT の G7 基礎的要素」は、以下の主体に指針を提供することを意図している。

(1) それぞれの国において TLPT の設計、実施、運営に向けて TLPT の活用を検討している当局
(2) TLPT を実施する金融機関
(3) サイバー脅威情報のサービスを提供する組織（「脅威情報プロバイダ」）
(4) ペネトレーションテストのサービスを提供する組織（「ペネトレーションテストプロバイダ」）
(5) 認証・資格付与（accreditation and certification）プロバイダ[2]

「TLPT の G7 基礎的要素」の適用はノンバインディングである。しかしながら、当局は特定の金融機関のサイバーレジリエンスを評価する際に、とりわけ以下の要素を考慮して TLPT を取り入れてもよい。

---

[1] 「Ethical Red Teaming」と呼ぶ国もある。
[2] 認証・資格付与プロバイダは、脅威情報およびペネトレーションテストのサービスを提供するためのベンダーの基本的な技量を確認している。

- 金融の安定性および市場の公正性の観点からみた、サイバーレジリエンスの優先度
- 金融セクターにおいて重要な機能やサービスを提供する金融機関の重要性
- サイバーレジリエンスをテストする他のリスク評価のツールやテクニックの利用（不）可能性

また、当局は、対象となる金融機関の業種、規模、複雑性、成熟度、リスクプロファイルから、TLPT を適用する度合いについて考慮してもよい。

多国籍で活動する金融機関の場合、異なる国の当局は、タイミング、スコープの決定および実施に関して最適な結果を得ることができるよう、計画、協力、調整してテストを実施すべきである。

効果的な TLPT は、評価のプロセス全体を通じて多様な関係者の強い関与を必要とする。クロスボーダーの評価に関与する金融機関は、必要に応じて、TLPT の実施に先立って、関連当局のリストを明確にすべきである。これは、クロスボーダーの評価をサポートし、多国籍で活動する金融機関の TLPT の結果の国境を越えた相互認証に関する議論を促進し、TLPT による評価の成果物を共有するためのプロトコルを策定することを目的とする。

情報共有とデータ保護

金融機関は、すべての関連当局の要求に従い、TLPT による評価を実施し、成果物を共有する責任を有する。関連当局は、必要に応じて、データ保護やクロスボーダーの情報共有の規範と整合的に、情報共有の協力を希望する可能性がある。

TLPT の活動に関連するすべての詳細情報が保護されるための、効果的なコントロールを設けるべきである。コントロールは情報の機微性（センシティビティ）を反映すべきである。情報は関係者に限定して提供されるべきである。

TLPT の基礎的要素

TLPT の全体的な目標を達成するため、「TLPT の G7 基礎的要素」は、TLPT の策定および実施を検討する当局や金融機関のために６つの基礎的要素を示し、各フェーズにおける異なる関係者の責任を明確化している。一般的に TLPT は、スコープ設定・リスクマネジメント、脅威情報、ペネトレーションテストおよび

完了のフェーズから構成される。

要素１：スコープ設定とリスクマネジメント

すべての関係者にとって、TLPT には潜在的な固有リスクがある。こうした潜在的リスクを踏まえて、「TLPT の G7 基礎的要素」は、評価全体を通じてテストのスコープを明確に定めるとともに、効果的なリスク管理措置（risk management control）を適用することを重要視している。

役割と責任

ホワイトチーム[3]は、適切なリスク管理措置を確実に機能させ、関係者からテストのスコープについて合意を得る責任を有する。テストは、レッドチーム[4]が金融機関のレジリエンス能力を効果的に評価するために、ブルーチーム[5]に事前に知らせることなく実施されることから、ホワイトチームはスコープ設定とリスクマネジメントのフェーズを含む評価のプロセスを通して、プロジェクトマネジメントの役割を果たすことが奨励される。

スコープ

第一に、テストのスコープは金融機関の重要な役割およびサービスの評価に基づき決定されるべきであり、それが次にテスト期間やパラメータの採用・不採用の決定につながる。金融機関は、サードパーティプロバイダ（IT サービスプロバイダ、サプライチェーン関係者など）を含む重要な役割やサービスを担う人々、プロセス、技術を特定すべきである。テストがサードパーティプロバイダをスコープに含めることを要求する場合には、サードパーティプロバイダに連絡し参加させることは金融機関の責任である。

金融機関は、関連する国の当局によるスコープ設定の要求を理解すべきであり、それぞれの要求を分析することが奨励される。これは、金融機関が他国の当局からの TLPT の要求を満たすために結果の利用を希望する場合に特に重要となる。そのような場合には、金融機関は最初のスコープ設定のフェーズにおいて、テストのスコープに関するガイダンスを金融機関に提示する可能性があるすべての関連当局を巻き込み連絡すべきである。

---

[3]ホワイトチームは、攻撃者に扮するレッドチームと、金融機関の情報システム利用の実際の防御者であるブルーチームの関与を調整する責任を有する。テストにおいて、ホワイトチームはルールの実効性を確保し、テストの実施を監視し、起こりうる問題を解決し、すべての情報要求や質問を受け付け、意図された方法でテストが確実に実行されるようにする。

[4]レッドチームは、テスト実施者のグループであり、金融機関のセキュリティ状況に対して、攻撃者の可能性のある攻撃や侵入能力をまねる権限が与えられ、組織されている。

[5]ブルーチームは、攻撃者に扮したグループ（すなわちレッドチーム）に対して、金融機関のセキュリティ状況を維持することにより情報システムの利用を防御する責任を有するグループである。

テストのライフサイクルにおいて、スコープおよび期間は脅威情報およびペネトレーションテストのプロバイダが実施する作業の相互作用の結果、変化しうる。当局の要求に注意を払いつつ、関係者（金融機関、脅威情報およびペネトレーションテストのプロバイダ、当局など）の間でスコープの修正について合意しておくべきである。

リスクマネジメント

金融機関は、関係者と協議し、金融機関のデータへの起こりうる影響、金融機関の資産への損害、金融機関や金融セクターにおける重要なサービスや業務の中断のリスクを減らすため、効果的なリスク管理措置を適用すべきである。リスクマネジメントの一環として、ホワイトチームは、テストの継続が金融機関にとって許容できないリスクを引き起こすと考える場合には、あらゆる時点でテストを中断することができる。

テストの完全性を守るため、金融機関内でのコミュニケーションは最小限に抑えるべきである一方、金融機関は、すべての関係者に対し適切なリスク管理措置が伝えられ、理解されたことを確認すべきである。

発見事項の分類

スコープ設定のフェーズにおいて、ペネトレーションテストプロバイダを含む関係者は、テストにおいて発見された脆弱性の分類の概念および金融機関への侵入成功を示す指標について合意しておくべきである。分類の概念は、金融機関のリスクマネジメントのフレームワークと整合的な形で、発見された脆弱性の重要性や対応の優先度を示すことを目的としている。

スコープ設定の成果物は、重要なサービスをテストするための脅威ベースのシナリオ策定を支援するため、脅威情報のプロバイダに提供されるべきである。

要素２：リソース確保

金融機関は、脅威情報およびペネトレーションテストのプロバイダを調達する責任を有する。TLPT のセンシティブな性質のため、金融機関は専門知識の水準、倫理規定、保証の十分性（例：損害賠償保険）といった要素に基づき、脅威情報およびペネトレーションテストのプロバイダを慎重に選定すべきである。認証・資格付与（accreditation and certification）は、このようなプロバイダの専門知識を確認する一つの手法となりうる。

外部の脅威情報およびペネトレーションテストのプロバイダは、一般的に独立した立場を示すが、その利用はそれぞれの国の要求による。金融機関は、スコープ設定のフェーズにおいて、手法が対象国の要求を満たすことを確認すべきである。例えば、いくつかの国では、外部の脅威情報およびペネトレーションテストのプロバイダの利用や、認証・資格付与機関によるプロバイダの専門知識の確認を義務づけていることもありうる。

要素３：脅威情報

脅威情報は、TLPT のプロセス全体の中心的なフェーズである。脅威情報のプロバイダは、テストの活動のスコープ設定にとって重要となる、実際のサイバー攻撃者を模倣した説得力のある脅威プロファイルを創り出すために、金融機関に焦点を当てた脅威情報や予備調査を活用する。脅威プロファイルは、レッドチームがペネトレーションテストのフェーズにおいて使用するテスト計画を策定するのに役立つ、脅威シナリオを含む。

役割と責任

脅威情報プロバイダは、通常、以下の責任を有する。

（1） 金融機関の指示に従い、テストのスコープに合わせて、脅威情報についての成果物を作成する
（2） 脅威情報についての成果物の妥当性の根拠を示す
（3） ホワイトチームに対し脅威情報についての成果物を周知する
（4） 必要に応じて、レッドチームを支援する。支援には、脅威シナリオの策定を助けるとともに、ペネトレーションテストのフェーズの進行に伴い発生する新たな脅威情報の必要性を満たすことを含む

金融機関は、以下を提供すべきである。

（1） 脅威情報のプロバイダに対するスコープ内の機能やシステムに関する指示
（2） 脅威情報のプロバイダによる適時かつ効果的な脅威プロファイルの策定を支援するための追加的な背景情報
（3） ペネトレーションテストプロバイダや適切な関係者、必要に応じ当局に対し、脅威情報についての成果物

脅威情報のプロバイダの適格性

効果的な脅威情報のプロバイダは、通常、以下の最低限の能力を示す。

- 金融機関、金融セクターおよび地理的な地域に適合したサイバー攻撃者像を描く能力
- 選択した攻撃者の手法を再現した攻撃シナリオを作成する能力
- 人・プロセス・テクノロジーに焦点を当てて、金融機関の脆弱性攻撃の対象となりうる領域について、正確かつ最新の状況を明らかにするためのさまざまな手法や、公開情報からの情報収集・分析（OSINT）や業界に関連したセキュリティ侵害の痕跡（IoCs）といった多様な情報や情報源の利用
- 多言語の情報収集能力

脅威情報の成果物

それぞれのTLPTの契約ごとに脅威情報プロバイダは以下のような情報を含む成果物を作成すべきである。

- 脅威情報レポート(TIR) -TIRには、金融機関に対し想定される脅威を示す、サイバー攻撃者のプロファイルが含まれるべきである。対象金融機関に関連するレポートが利用可能でない場合には、関連するセクターや地域における過去にあった既知の攻撃に基づき攻撃者を選定しうる。それぞれの攻撃者のプロファイルには、攻撃者によって利用される手法やツールを最大限強調した脅威シナリオを含むべきである。脅威シナリオは、ペネトレーションテストプロバイダが効果的なテスト計画を練り上げるために必要となるすべての関連する手法や情報を提供できるくらい十分に詳細なものとすべきである。
- ターゲティングレポート(TR) - TRは、スコープに従い、人・プロセス・テクノロジーに関連する脆弱攻撃にさらされた領域を強調した、金融機関のプロファイルを提供すべきである。レポートは、ペネトレーションテストプロバイダに対し、対象となる金融機関への可能性のある脅威の経路を提供することを目指すべきである。

ペネトレーションテストの計画に組み入れる前に、関係者が脅威情報の成果物に意見を述べるとともに、スコープ内のシステムへの合意された攻撃シナリオを描くことができるような協調的アプローチが展開されるべきである。一般的に金融機関によってとりまとめられるこうした協調により、レッドチームがテストの主要な目的と整合的で、より焦点を絞ったペネトレーションテスト計画を策定することが可能となる。

このプロセスを通じて、またペネトレーションテストのフェーズにおいて、

脅威情報のプロバイダは、必要に応じて適時に、専門知識を継続的に提供すべきである。金融機関がさまざまな国においてサービスを提供している場合には、異なる関係者は、情報の機微性（センシティビティ）と機密性を踏まえつつ、国を跨いで成果物を共有することを考慮すべきである。

要素４：ペネトレーションテスト

脅威情報のフェーズの完了後、レッドチームはスコープとして決定されたとおり、対象となるシステムやサービスに対するテストを計画し実行すべきである。レッドチームがスコープに基づき、脅威シナリオに沿った実践的なテストを実施することを可能にするために、ペネトレーションテストのフェーズには十分な時間が割り当てられることが奨励される。

役割と責任

レッドチームは、通常、以下の責任を有する。

（1） スコープとリスクマネジメントプロセスに合わせて、テストで従うシナリオを明示したペネトレーションテスト計画を作成する
（2） 脅威情報のプロバイダの成果物から作成された脅威シナリオに従いテストを実施する
（3） 金融機関に対し最終的なペネトレーションテストレポートを作成し発行する

ホワイトチームは、以下の責任を有する。

（1） テストの活動を調整し、推進する
（2） レッドチームと継続的な対話を実施し、必要に応じて追加的な支援を提供する
（3） ブルーチームを監視・監督する
（4） 効果的なリスク管理措置を適用する（必要と考えられる場合のあらゆる時点でのテストの中断を含む）

関連当局は、ホワイトチームとともにテストにオブザーバーとして立ち会うことができる。

テストの手法、アプローチおよび成果物

金融機関は、テストの受諾を求めることを希望する関連当局の要求に従ってTLPTの評価を実施すべきである。

レッドチームは、ペネトレーションテスト計画の一環として、対象金融機関へのテストシナリオを策定するため、脅威情報の成果物を利用すべきである。金融機関は、テストを適切に実施するために十分な時間をレッドチームに確実に与えるようにすべきである。

リスク管理措置に従い、対象システムへのリスクを最小限に抑えるため、ホワイトチームは全体を通してテストの実施を監督すべきである。

テスト対象とする環境の要件を定めている国もありうるので、金融機関は、テスト要件が本番環境か非本番環境か、対象を理解しておくべきである。

テストの最後に、レッドチームはペネトレーションテストレポートを作成すべきである。このレポートは、テストで採用されたアプローチの詳細やテストからの発見事項や所見を含むべきである。レポートでは、リスクや現状のコントロールについて評価し、必要に応じて改善すべき分野に関する助言を提供すべきである。

要素５：完了および改善

ペネトレーションテストのフェーズ終了後、TLPT は完了フェーズに移行する。完了フェーズでは、すべての関係者がテスト結果を分析し、テスト結果に対応してテストを受けた金融機関のサイバーレジリエンスをさらに強化するための改善策を作ることが目的となる。

ペネトレーションテストプロバイダは、通常、金融機関へのテスト結果のプレゼンテーションを含む、テスト後のワークショップを支援する責任を有する。

金融機関は、以下に責任を有する。

（1） 合意された安全な送付手段を用いて、適切な関係者に発見事項を送付する
（2） 発見事項について議論し、リスク軽減策を特定するため、関係者とのテスト後のワークショップを準備する
（3） 不足のない改善計画を作成し実行する

関連当局は、金融機関への監督活動を通じ、改善計画を承認する責任がある。また、金融機関への通常の監督活動の一環として、改善計画の実行をフォローアップする責任を有する。

要素６：類型化したデータ

「TLPT の G7 基礎的要素」の中心的な目的の一つは、金融機関、より一般的には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。これを達成するための重要な手段は、類型化したデータを作成し当局と金融機関の間で共有することである。

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すべきである。すべての類型化した結果は、個別金融機関の特定ができないようにしなければならない。TLPT 実施後の分類を作成する基礎として、独自のフレームワークを活用するかは当局の裁量に委ねられており、TLPT の実施に関連する類型化したデータの作成は関連当局の責任である。当局は、必要に応じて、データ保護やクロスボーダーの情報共有の規範と整合的な形で、多様な情報共有の手法を考慮することができる。