PwC's Cyber Security Insights 2021

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

pwc

www.pwc.com/jp

はじめに

デジタルトランスフォーメーションの推進が叫ばれる中、さまざまな金融サービスシステムにおけるインシデントが絶えず発生し、被害が報告されています。テクノロジーの進化と普及に伴いシステムの利便性が向上する一方で、そうしたシステムを狙う攻撃者の存在を看過することはできません。

近年攻撃者は、サイバー犯罪グループとして組織化され、攻撃対象の入念な事前調査、攻撃対象に特化した攻撃実施、組織内への侵入・潜伏・偵察、セキュリティ対策の回避・迂回といった高度な攻撃を仕掛けてきます。

こうした脅威に対抗するためは、企業は自組織のセキュリティ対応態勢を適切に評価・把握し、対策に取り組むことが求められます。

従来、FFIEC CAT（Cybersecurity Assessment Tool）などに代表されるセキュリティ基準に基づいたリスクアセスメントや脆弱性診断と呼ばれるシステムの欠陥を特定し、修正する取り組みが行われておきました。しかし、こうした取り組みは、日々新たな脆弱性や攻撃手法が発見される進化の早いIT環境において、攻撃者に追従することが難しいという課題があります。また、単に欠陥の有無を評価するだけでは、その結果を利用した攻撃が実際に成立するのか、攻撃が成立した際にそれを迅速に検知・対処する態勢があるのかを把握することはできません。

脅威ベースのペネトレーションテスト（Threat-led Penetraion Test）は、こうした課題を受けて、G7のサイバー・エキスパート・グループにより「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）」として策定された取り組みです。

TLPTを活用することで企業は、自組織に想定されるリアルな攻撃と自組織の対応態勢を把握し、対策の取り組みを推進することができます。既に、上記のガイドラインが公表されてから2年が経ち、国内での活用が進んでおり、今後さらなる普及と定着化が予想されます。本レポートは、TLPTの実践から見えてきた示唆を解説することで、より効果的な実践の一助になることを目的としています。

Agenda

1 新たな段階に入った金融機関のTLPTの実践

1. 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る。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った。

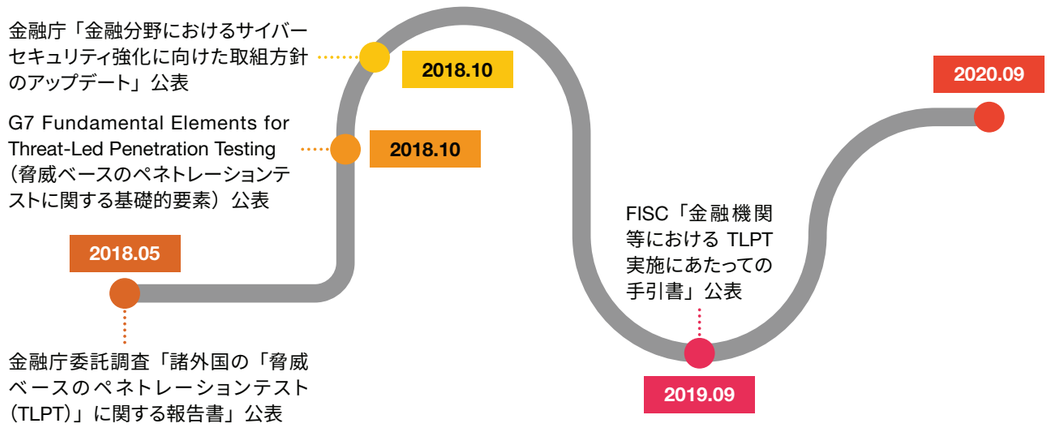
最初にこのキーワードがわが国で利用されたのは、2018年5月に金融庁が公表した「諸外国の『脅威ベースのペネトレーションテスト（TLPT）』に関する報告書」だと言われている。当報告書の作成は、金融庁から委託を受けたPwCあらた有限責任監査法人（以下、PwCあらた）が担当した[2]。

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いた。

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た。

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

図表1：国内金融分野におけるTLPT普及までの流れ



2. 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た（図2にTLPTの特徴と主な効果をまとめている）。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なかった。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を実施していった。

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、わ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った。

その点、FISC公表のTLTP実施の手引書は、わ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る。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る。

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る。

図表2：TLPTの特徴と主な効果

3. 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る。

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る。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る。

これらは大手金融機関の事例であるが、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る。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いた。

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る。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しであり、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る。

4. 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るが、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ある。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るが、その内容は極めて限定的である。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ない。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らない。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る。

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る。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る。

2 TLPTにおけるスレットインテリジェンスの活用

1. TLPTにおけるスレットインテリジェンスの位置づけ

TLPT（Threat Led Penetration Test）は、実際に想定されるサイバー攻撃の脅威に基づいて実施されるペネトレーションテストである。テスト実施者は被対象組織を闇雲に攻撃するわけではなく、初めにスレットインテリジェンスに基づいた攻撃シナリオの策定を行う。その後、策定した攻撃シナリオをどのように実施するかをテスト計画として策定し、計画に基づいてテストを実施する。スレットインテリジェンスとは一般的に、自組織のサイバーセキュリティ対策向上を目的にサイバーセキュリティ脅威に関する情報（インフォメーション）を分析する取り組みや、それを提供するサービスを指す。こうした分析は、企業や組織の意思決定を左右する知見にもなり得る。スレットインテリジェンスの活用はTLPTの特徴の一つであり、一連のプロセスは、国内では2019年9月、公益財団法人金融情報システムセンター（FISC）から公開された「金融機関等におけるTLPT実施にあたっての手引書[7]」によってまとめられている。

一方、TLPTの実施が先行している英国では、イングランド銀行によってTLPTを実施するフレームワークとしてCBEST[8]が定義されている。また、CREST（the Council for Registered Ethical Security Testers）[9]と呼ばれる資格団体がCBESTに基づいたフレーワームを定義しており、セキュリティベンダーの認証を実施している。CRESTによる認証はサービスごとに細分化されており、スレットインテリジェンスについては「Simulated Target Attack（STAR）Threat Intelligence services」として提供されている。

昨今のサイバーセキュリティを検討する上で欠かすことができないスレットインテリジェンスをTLPTでどのように活用するか、その目的と方法を考える。

2. TLPTにおけるスレットインテリジェンスの目的

前述の通り、スレットインテリジェンスは意思決定のための知見と考えることができる。あらかじめ脅威の内容を把握し、どのように対処するべきかを考えておくことは、迅速かつ的確な対応を行う上で非常に有効となる。企業や組織の重要な決断のもととなるため「何のために分析するのか」という目的設定が非常に重要となる。分析の目的によって必要となる情報や知見が異なるため、そこが明確でないと、単なる情報に留まり知見に至らない、自組織に役に立たない知見しか得られない可能性がある。TLPTにおいては「自組織（被対象組織）で実際に想定される脅威を明らかにする」ことが目的となる。

TLPTにおいてスレットインテリジェンスをどう活用するかを考える前に、どのような情報がスレットインテリジェンスになり得るのかを考えてみよう。いくつかの考え方をもとに明確にすることができるが、ここでは5W1Hを活用した例を紹介する。誰が（Who）、どこから（Where）、何を（What）、なぜ（Why）、いつ（When）攻撃しているのかを明らかにし、その手法を防御側の知見とするというものである。

例えば、実際のハッキングで多用されるハッキングツールのハッシュ値はスレットインテリジェンスと言えるであろうか。この情報から分かることは、1）ハッキングツールの存在、2）そのハッキングツールが世の中のサイバー攻撃で多用されていること、3）そのハッキングツールのハッシュ値である。そのため、誰が使っているのか（Who）、どの業種・企業、システムを攻撃し、（Where、What）、なぜ攻撃しているのか（Why）、どのように使われるのか（How）、いつ攻撃されるのか（When）などを説明しきれておらず、「実際に想定される脅威を明らかにする」という目的を十分に果たしているとは言えない。

より攻撃者像に着目してその意図、能力、機会で捉えることもできる。これを5W1Hと掛け合わせることで攻撃者の実態がより浮き彫りになり、取るべき対策の検討に役立てられると考えられる。なお攻撃者の意図に関しては、「日本企業に対するインシデント解説 サイバー攻撃者は何を目的に攻撃するか」を併せてご覧いただきたい。

図表3：攻撃者像の具体化と5W1Hを活用したスレットインテリジェンスの導き方（例）

3. 攻撃シナリオに落とし込むためのスレットインテリジェンス

スレットインテリジェンスは大きくストラテジック型、OSINT（Open Source Intelligence）型、テクニカル型に分類することができる。このうち、TLPTでより必要となるのはテクニカル型である。スレットインテリジェンスの結果に基づいて攻撃シナリオの策定を行う必要があるため、より実用的な同型が求められるのである。そのため、TLPTにおけるスレットインテリジェンス活用のアプローチとしては、大きく分けて以下の2つが考えられる。

1. 事例情報に基づいた攻撃者像の分析

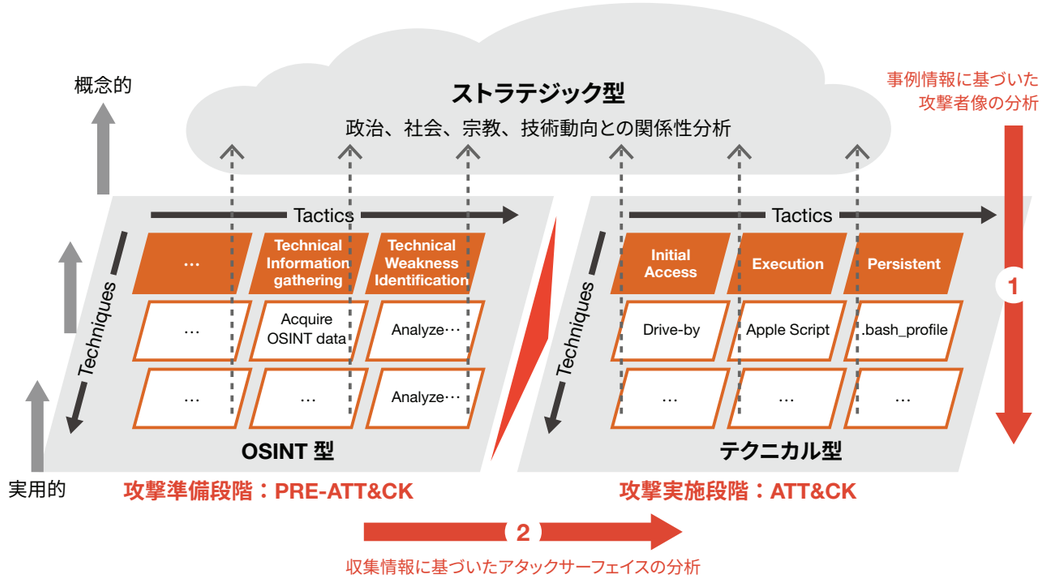
テレワーク・リモートワークの普及に伴うインシデントなど、世の中の動向に連動したインシデント事例、同業他社のインシデント事例および自組織内で過去に発生したインシデント事例に基づいて攻撃者像の分析を行うアプローチである。特に他社事例などでインシデントの詳細が判明・公開されているケース、自社事例で分析が実施されているケースでは、攻撃グループ名、戦術、攻撃手法、利用されたツールなどのいずれかをキーにMITRE ATT&CK[10]と照合することで、想定される攻撃の全体像を洗い出すことができる。こうした情報はMITRE ATT&CKのウェブサイト上でまとめられており、例えばAPT41と呼ばれる攻撃者グループの情報[11]を確認することで、同グループが用いる攻撃手法、利用するツールなどの情報を把握することができる。

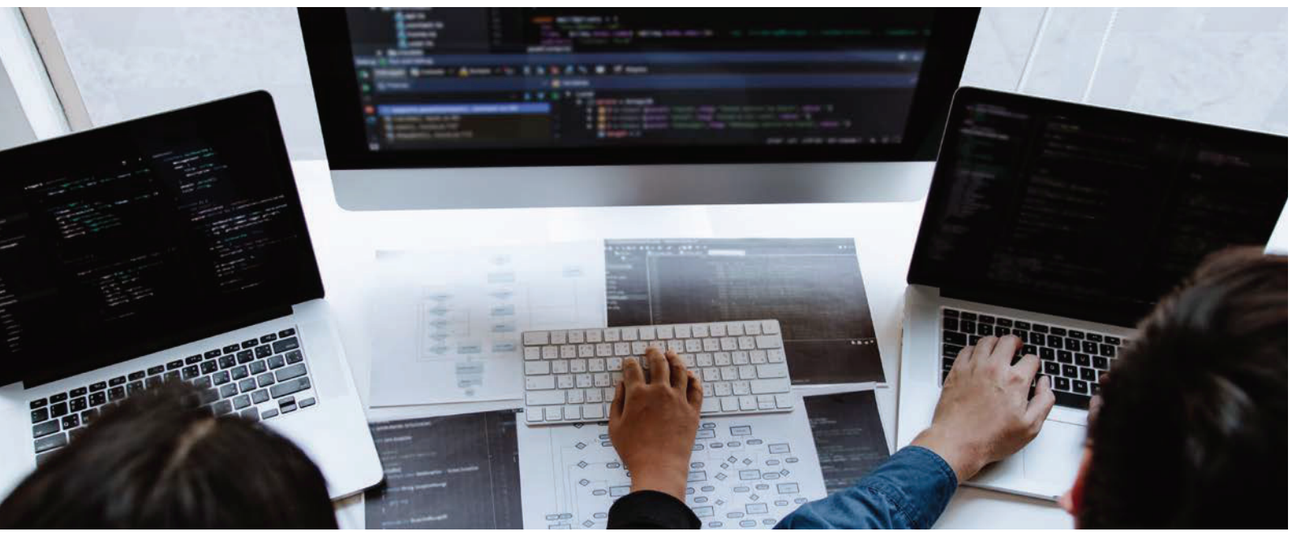
2. 収集情報に基づいたアタックサーフェイスの分析

主にOSINTにより収集されたオープン情報を攻撃者視点で見た場合に、どのような攻撃が考えられるかの分析を行うアプローチである。これは、ダークウェブなどで流通し売買されている社員のメールアドレス・パスワードなどの漏えい情報、自社が展開しているサービスのアカウント販売情報、IoT検索エンジンなどにより検出される、インターネットに接続された自社のShadow ITに関する情報が含まれる。例えば、自社で過去にサイバー攻撃による情報漏えいが発生しており、当該情報がダークウェブ上で流出していることが確認された場合、このような情報を悪用した攻撃が考えられる。具体的には、漏えいしているメールアドレスに対するスピアフィッシング攻撃や、漏えいした認証情報を悪用したサービスへの不正利用などである。

こうして収集・分析された結果と自組織が置かれた環境や情勢を複合的に分析することで、実際に起こり得る攻撃を描き、攻撃シナリオを策定する。

図表4：スレットインテリジェンスの全体像





3 攻撃シナリオに基づいたペネトレーションテストとは

これまでに脅威ベースのペネトレーションテスト（TLPT）においてスレットインテリジェンスを活用する目的として、テスト対象の組織にとっての「脅威」を明らかにすることであると述べた。また、スレットインテリジェンスを活用して攻撃シナリオを作成するアプローチとして、「事例情報に基づいた攻撃者像の分析」と「収集情報に基づいたアタックサーフェイスの分析」の2つを説明した。これらのアプローチから得た結果と自組織が置かれた環境や情勢に鑑みて分析を行うことで、現実に起こり得る攻撃を想定した攻撃シナリオを策定することができるようになる。本章では、策定された攻撃シナリオに基づいて実際にどのようにペネトレーションテストを実施するかを紹介する。

1. TLPTにはサイバーキルチェーンの活用を

TLPTでは、スレットインテリジェンスを活用して自組織にとっての脅威を明らかにした上で、その脅威によって現実世界で自組織に対して行われる攻撃を想定・シミュレーションし、ペネトレーションテストを実施する。本題に入る前に、これを行う上で有効となるフレームワークを紹介する。

米国の大手製造企業によって、標的型攻撃の一連の行動を7つの段階に構造化したサイバーキルチェーン（図表5）が提唱されている。TLPTは、これらの各段階における技術、人・組織、プロセスのサイバーレジリエンスを評価することを目的としている。つまり、現実に起こり得る攻撃のシナリオを策定し、自組織にとって脅威となり得る一連の攻防を実際に行ってみることで、サイバーキルチェーンの各段階において組織が導入しているセキュリティ装置・サービスなどのテクノロジーの有効性に限らず、人・組織、インシデントへの対応プロセスの課題を洗い出すことが可能となるのである。

図表5：サイバーキルチェーン

出所：‘Cyber Kill Chain®’（https:///lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html）の情報をもとにPwCが作成

2. スレットインテリジェンスによる攻撃シナリオの策定の仕方

スレットインテリジェンスの調査とネットワーク環境などに関するヒアリング、リスクアセスメント資料の分析をもとに、その環境に対して現実に起きる可能性がある攻撃のプロセスを、攻撃シナリオとして策定する。攻撃シナリオの検討にあたっては、初めに攻撃の目標（クラウンジュエル）と目的を決める。攻撃の目的の例としては、機密情報や個人情報の窃取と外部への持ち出し、システムの不正制御や破壊といったものがある。

次に、その目的を達成するために、どのような過程を経て攻撃が実施されるかを検討する。具体的には、想定される攻撃グループが、どのような攻撃経路を、どのような手法（Tactics, TTPs:Techniques and Procedures）で、どのようなツールを使用して攻撃の目的を達成し得るかを分析し、サイバーキルチェーンの各段階における攻撃内容へ反映しながら、攻撃シナリオを策定する。

3. 攻撃シナリオに基づいたペネトレーションテストの実施

ではここからは、攻撃シナリオに基づいたペネトレーションテストの流れを紹介する。同テストは、攻撃シナリオの策定を終えて、シナリオの内容について評価対象の組織と合意した上で開始する。ペネトレーションテストは、基本的に外部からの侵入試行から始まり、侵入後に端末を乗っ取り、C&C（C2）サーバー経由で内部での感染拡大を行った後、指定したサーバーやシステムに不正アクセスし、目的を達成するために、攻撃シナリオの各段階における攻撃試行を実施する。

各段階において、防御の可否や攻撃時の検知、攻撃への対応を評価しながらテストを実施するが、ある段階で攻撃が成功しない（防御が成功した）場合、演習の中では攻撃が成功した前提で、次の段階へ進む。こうすることにより、攻撃が失敗し次の段階への経路が断続された場合でも、テストを中止せずに一連の攻防のシミュレーションを継続して行う。これは、実際の攻撃において、演習用に作成した攻撃シナリオ以外の手法で段階が進んだ場合に備えて、それ以降の段階の態勢評価を行うことを目的としている。PwCの場合、多くのTLPTにおいて、安全かつ高度な標的型攻撃を再現するため、独自で開発した擬似リモートアドミニストレーションツール（RAT）やC2サーバーを用いて、攻撃シナリオに沿ってペネトレーションテストを実施する。

4. 攻撃シナリオの例（標的型メール攻撃・内部犯行・物理攻撃）

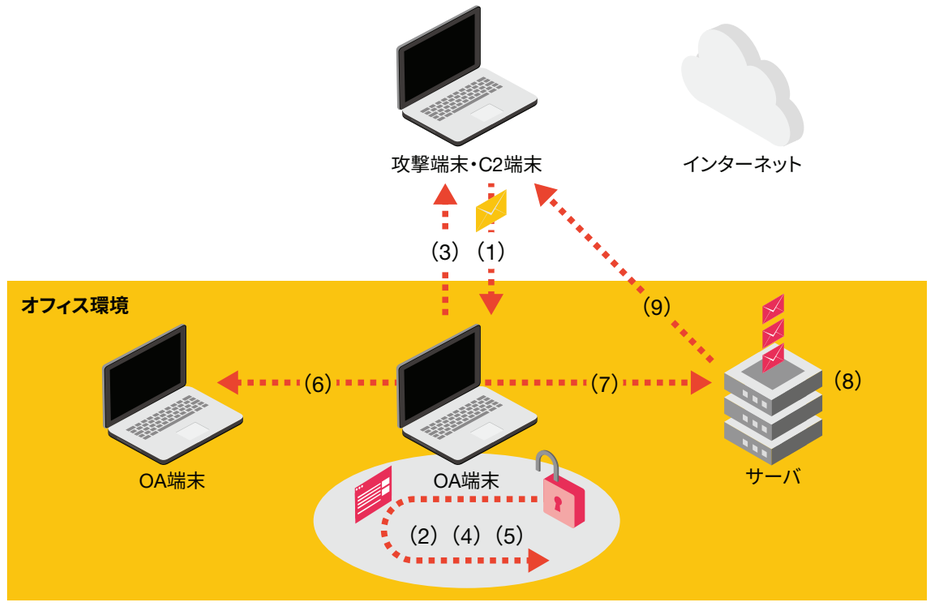
代表的なTLPTの攻撃シナリオとしては、APT（Advanced Persistent Threat：高度で継続的な脅威）グループによる標的型メール攻撃が挙げられる。この攻撃シナリオをサイバーキルチェーンに沿って策定する場合、攻撃者は、まず攻撃対象の調査を行い（探索）、攻撃に用いるマルウェアを作成し（武器化）、外部からマルウェアを添付した攻撃メールを送付することが想定される（デリバリー）。さらに、OA端末の感染を試み（エクスプロイト、インストール）、C2サーバーにより端末の遠隔操作を行うと考えられる（指令と制御）。そして、内部での感染拡大を試み、設定した攻撃の目標・目的に到達するまで攻撃試行を続ける（目的実行）――。こうして基本的な攻撃シナリオを作成することができる。

さらに、この攻撃シナリオを図表6のように（1）～（9）の詳細なプロセスまで落とし込み、より標準的なシナリオに発展させることで、攻撃の具体像をより詳細に把握することができる。攻撃は必ずしも外部からのみとは限らない。組織によっては、内部犯行による情報漏えいが最大の脅威となるため、組織内から攻撃が始まるケースも想定しておくべきであろう。または、オフィスやデータセンターへ人が物理的に不正侵入を行い、情報が格納されているサーバーやOA（Office Automation）端末などの機器に対して物理的な攻撃を行うという攻撃シナリオも考えられるであろう。

（1）メール経由でマルウェアを配布
（2）OA端末内でマルウェアを実行
（3）C2端末へ接続し、外部通信を開始
（4）脆弱性を悪用し、特権ユーザーへ権限を昇格
（5）ユーザーアカウントの認証情報を窃取
（6）窃取した認証情報を使用し、他のOA端末へ感染を拡大
（7）サーバーに対してリモートコードを実行し、攻撃を拡大
（8）サーバーから顧客情報や機密情報を収集
（9）収集した情報をC2端末に移し、外部に漏えい

このようにTLPTでは、スレットインテリジェンスで得た分析結果や組織環境の調査などにより策定した攻撃シナリオに基づいて、ペネトレーションテストを実施する。そして、適切な精度と期日で防御・検知、調査、報告などができたかを評価し、サイバーレジリエンスに対する課題を洗い出す。

図表6：標準的な標的型メール攻撃のシナリオ



4 TLPTにおけるブルーチームの態勢評価とは

1. ブルーチームとは

疑似攻撃を仕掛ける「攻め」のレッドチームに対し、ブルーチームは「守り」のチームとして検知、影響・被害の特定・低減、経営層に対する報告、社内外の関係者に対する報告・連絡などの役割を担う組織を指す。

一般的に、SIRT（Security Incident Response Team。CSIRT、PSIRT以外に、制御系システムやサービスを対象とする新たなSIRTも登場している）、SOC（Security Operation Center）が該当する。

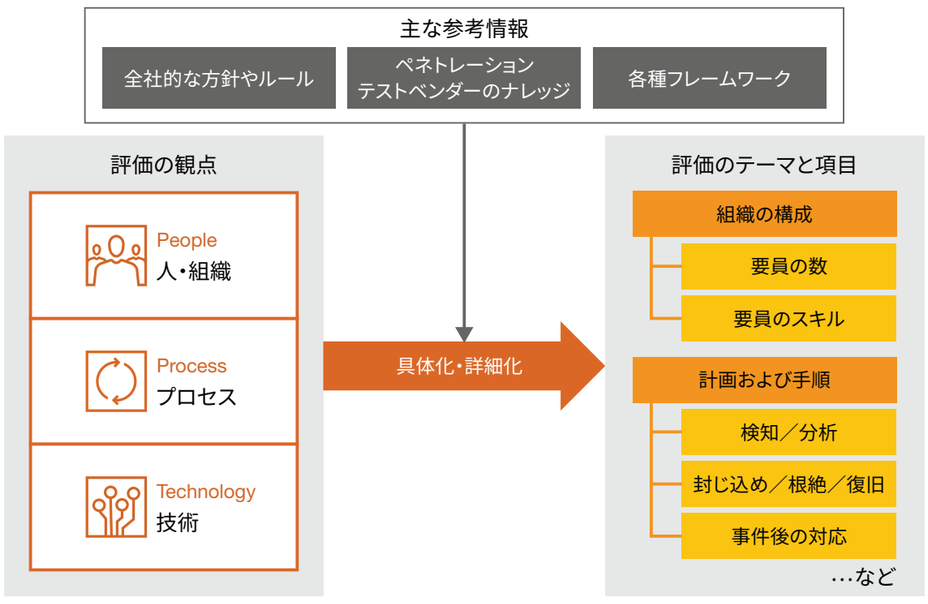
多様化、巧妙化が進むサイバー攻撃を防ぎきることは企業にとって困難であることから、「技術的な対策が施されていること」以上に、「インシデント発生時にブルーチームであるSIRTやSOCの実効性が確保されていること」が大きな意味を持つ。

2. 態勢評価の進め方

ペネトレーションテストにおける評価は、主に人・組織、プロセス、技術の観点で構成される。そして、これらの観点ごとに、インシデント対応状況の全般について社内外の各関係者にインタビューを実施し、態勢を評価する。

インタビューの内容は、当該企業におけるインシデント対応の全社的な方針やルール、ペネトレーションテストベンダーのナレッジ、各種フレームワークなどを参考に決定する。

図表7：ブルーチームの態勢評価の進め方



評価の参考になる、インシデント対応の代表的なフレームワークは下記の通りである。

【NIST SP 800-61 Computer Security Incident Handling Guide[12]】

日本でも広く知られているガイドラインである。組織の構成とインシデント対応機能という観点で文書が構成されており、影響評価、復旧評価、ツールなどに関する具体的な説明がある点が特徴である。
和訳版（rev1）が公開されており[13]、評価テーマとして利用しやすい一方、成熟度の観点が無いため、CMMI（Capability Maturity Model Integration）などのフレームワークで補う必要がある。

■主な内容
インシデント対応組織の構成と能力：6節（方針・計画・手順などの策定、組織の構成など）
インシデント対応：6節（検知と分析、封じ込めと駆除と復旧など）
情報共有と連携：4節（情報共有体制、情報共有手法など）

【SIM3（Security Incident Management Maturity Model）[14]】

欧州を中心に活用され、日本でも最近注目されているフレームワークである。4種類のテーマで構成されており、それぞれの成熟度を5段階で評価する。成熟度は各レベルの定義のみならず、次レベルとの差異も説明されている点が特徴である。

■主な内容
組織：11項目（権限移譲、継続性、責任、サービス定義など）
人：7項目（ルール、人材の健全性、スキルセット、訓練など）
ツール：10項目（資産管理、脆弱性管理、防御策、検知策など）
プロセス：17個（経営層・広報・法務などへの報告プロセス、検知・復旧などの対応プロセスなど）

■成熟度
0：利用できない／定義していない／認識していない
1：認識されているが、文書化されていない
2：文書化されているが、権威性が無い
3：文書化されており、CSIRT責任者の権限で権威付けされている
4：文書化されており、ガバナンスレベルの権限で権威付けされている

なお、欧州のネットワーク・情報セキュリティ機関から、SIM3に関するウェブベースのチェックツールやレポートが公開されている[15]。

3. 態勢評価後の取り組み

態勢評価から、ブルーチームの要員不足や知識不足といった人・組織に関する問題点、インシデント対応手順の不足といったプロセスに関する問題点など、さまざまな問題点を抽出することができるであろう。これらが対応の遅延、影響範囲の拡大といった事業被害を誘発する要因となることから、その解消が、以降の重要な取り組みとなる。

【態勢評価によって抽出される問題点の一例】

- CSIRTの要員不足により、インシデント対応が実行できない
- SOCの知識不足により、ログやアラートの分析方法が分からない
- 役割が認知・共有されていないため、誰が何をすればよいかが分からない
- インシデント対応手順が不足している、または、無い
- サービス停止が生じた際に、取るべき対応を判断できない
- インシデント発生時に連携すべき関係者に漏れがある、または、分からない
- インシデントの封じ込めや応急処置の実施に踏み切ることができない

4. 態勢評価や態勢評価後の取り組みが上手く進まない場合

入念な準備を経てペネトレーションテストを実施したものの、「TLPTの態勢評価が上手く進まない」、「TLPT実施後の問題点解消の取り組みが頓挫する」といった話をよく耳にする。ここからは、こうした事態に陥らないための対応策を紹介する。

【態勢評価を滞りなく進めるために：インタビューの段取り】

態勢評価において上手く進まないことの一つとして、インタビューが挙げられる。インタビューで聞く内容が定まらず、結果的に想定より多くの期間を費やしてしまうといったケースが少なくない。これを円滑に遅滞なく進めるためには、その内容について、インタビュー開始直前ではなく、プロジェクト開始時にテストベンダーと内容を摺り合わせ、設計すること（何を参照文書とするのか、文書上のどの内容を用いるのかなど）を推奨する。

これにより、テスト開始前にインタビューの対象者を洗い出すことができ、テスト実施に伴う調整と併せて、インタビューの内容の説明とスケジュールの確保ができる。

一般的に、情報システム部門のみならず、外部委託先、リスク管理部門、総務部門などもインタビュー対象となることが多く、最低でも1カ月程度はインタビュー期間を設けると安心である。

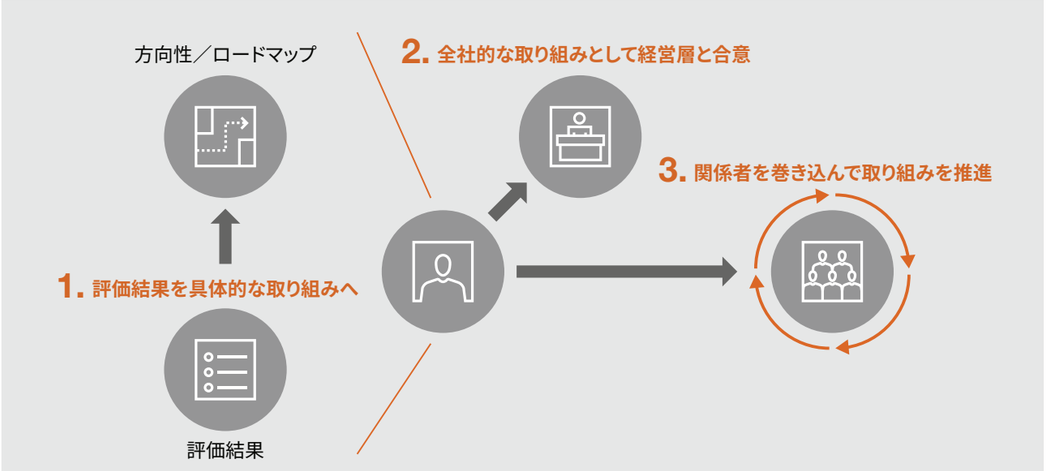
【態勢評価後の取り組みを予定通り進めるために：ロードマップの策定と経営層・関係者からの合意の取り付け】

態勢評価後の取り組みが進まない主な理由として、スケジュールの見積もりが甘い、関係者から適切なサポートを得られていない、などが考えられる。

このような状態を引き起こさないためには、問題点の因果関係を分析して、有効かつ効率的な進め方を検討およびロードマップ化することで、経営層に対して重要性を訴求し、TLPTを全社的な取り組みと位置付けた上で、関係者からその目的や内容、スケジュールに関する理解を得ることが必要である。

なお、評価の説得性を増すために、ベンチマークを活用することも推奨される。

図表8：態勢評価後の取り組みを推進するための具体策



TLPTは技術的な対策の評価に留まらず、態勢を含め幅広く評価することができる。前述の通り、TLPTの目的は、企業の重大な被害につながるインシデント発生時に、今まで投資してきた人・組織、プロセス、技術に関する対策がそれぞれ有効にムダなく機能するかを検証し、その結果から、さらなるセキュリティ強化やコスト削減を効率的に推進するための道筋を見出すことである。一連のプロセスから導き出されるブルーチームの態勢評価は言ってみればTLPTの総仕上げであり、プロジェクト成功に向けた重要なカギと言えるであろう。

おわりに

ここまでの章では、TLPTの成り立ちから実施の各フェーズにおける取り組みとその示唆を解説しました。TLPTは、単なる「ペネトレーションテスト」ではなく、攻撃者目線で企業を分析し、疑似攻撃を行い、対応態勢を評価を行うセキュリティ対策の総合評価と言えます。

そのためTLPTをより効果的な取り組みとするためには前章までに解説した示唆は勿論ですが、TLPTの企画・推進を行うホワイトチームの積極的な関与を欠かすことができません。

ホワイトチームは、攻撃を担当するレッドチーム、防御を担当するブルーチームの両方に関与することで「どこまで事前情報をレッドチームに提供するのか」、「ブルチームにテストを事前告知するのか」、「テスト時の検知イベントをどこまで本番同様に対処するのか」といった一筋縄ではいかない判断を行う必要があります。こうした問いに定型的な答えはありませんが、以下の性質を考慮して決定することが重要です。

レッドチームへの事前情報の提供
- 情報提供が多いほどスレットインテリジェンス、テスト実施のタイムパフォーマンスが向上する。
- 情報提供が少ないほど実際の攻撃者目線での評価となり、スレットインテリジェンス、テスト実施は実評価者の能力に依存する。

ブルーチームへの事前告知
- テストについてより具体的、広範囲に告知、実施内容を共有するほどテストによる意図しない障害などのビジネスインパクトを低減することができる。また、検知時の対処が迅速化する一方で、実態的な対処能力の評価が難しくなる。
- 告知、実施内容の共有を限定するほどビジネスインパクトの低減および不測の事態への事前準備が難しくなる。一方で、実態的な対処能力の評価を行いやすくなる。

テスト時の検知イベントへの対処
- 検知イベントへの対処をより早い段階で止める（テストであるため本番相当の対処不要とする）ほどブルーチームの対処工数が削減される。一方で、後続の対処能力の評価が難しくなる。

上記のようにホワイトチームは、TLPTの効果とリスクを見極めて組織内のステークホルダーと入念な調整を行う必要があります。国内においてTLPTは今後さらに普及し、実施が定着化することが予想されます。そのため、TLPTの実施に当たっては自社のセキュリティ対策の成熟度を踏まえて上記の要素を設定、実施ごとに見直すなどの工夫も考えられます。

「はじめに」でも述べたようにテクノロジーの進化に合わせて攻撃者も手口を変え、より高度な攻撃を仕掛けてきます。サイバーセキュリティ対策はいたちごっこであり、攻撃側に対して防御側は後追いになることが避けられません。そのためこうした実践的な取り組みを企業のレベルに合わせて継続的に実施していくことが重要です。

参考資料

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」
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】」
5 BANK OF ENGLAND, ‘Financial sector continuity（2020年8月20日閲覧）
6 EUPEAN CENTRAL BANK, ‘What is TIBER-EU?’（2020年8月20日閲覧）
7 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】」
8 BANK OF ENGLAND, ‘Financial sector continuity’（2020年9月2日閲覧）
9 CREST（2020年9月2日閲覧）
10 サイバー攻撃に関する戦術、テクニックをまとめたフレームワーク。実際に発生したインシデントの分析に基づいて戦術、テクニックと攻撃グループや利用されたツールなどの情報の紐づけも行われている。
11 MITRE, 2019. ‘APT41’（2020年9月2日閲覧）
12 National Institute of Standards and Technology, ‘Computer Security Incident Handling Guide’
13 独立行政法人情報処理推進機構,「 セキュリティ関連NIST文書」
14 Open CSIRT Foundation, ‘SIM3 Model & References’
15 European Union Agency For Cybersecurity, ‘CSIRT Maturity assessment’

お問い合わせ先

PwC Japanグループ
https://www.pwc.com/jp/ja/contact.html

【監修】

林 和洋
PwCコンサルティング合同会社 パートナー

【執筆者】

村上 純一
PwCコンサルティング合同会社 ディレクター

浜田 譲治
PwCコンサルティング合同会社 シニアマネージャー

小林 由昌
PwCあらた有限責任監査法人　シニアマネージャー

茂山 高宏
PwCコンサルティング合同会社 マネージャー

www.pwc.com/jp

発刊年月：2021年1月　　管理番号：I202010-08