# 金融分野のシステム障害分析レポート（概要）

- 金融庁では、監督指針等に基づき、金融機関から報告を受けているシステム障害（サイバー攻撃を含む）の分析結果をまとめ、2019年以降、毎年、「金融機関のシステム障害に関する分析レポート」として公表している。
- 本レポートは、過去の事例も含め、障害の端緒に着目して障害事例を分類し、原因と課題を分析している（次頁参照）。また、ITレジリエンス強化の参考となるよう、ATM停止時の円滑な顧客対応や、コンティンジェンシープランに則った円滑なシステム復旧などの障害対応の好事例も記載している。加えて、今般のレポートにおいては、「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（TLPT）の好事例及び課題」及び「オペレーショナル・レジリエンスに係る金融機関との対話等の概要」のコラムも掲載している。
- 金融機関においては、本レポートに加え、サイバーセキュリティを含むシステムリスク管理に関する各種標準、ガイドライン等を参照し、自組織の体制及び対策について見直し、求められるITセキュリティ又はITレジリエンスとの差異を特定し、解消することが望ましい。

# システム障害の傾向及び課題等の概要

| 発生の端緒 | 障害傾向 | 課題・対応 |
|---|---|---|
| (1)サイバー攻撃、不正アクセス等の意図的なもの | ①マルウェア感染<br>②DDoS攻撃 | ・脆弱性に係る最新情報の把握、パッチ適用の徹底<br>・マルウェア対策整備、重要な外部委託先のサイバーセキュリティ管理態勢のリスク評価実施や強化<br>・DDoS攻撃の軽減対策強化、DDoS攻撃の早期検知・復旧のための態勢整備 |
| (2)システム統合・更改や機能追加に伴い発生 | ①外部委託管理不十分<br>②BCP・大規模障害時の危機管理体制の整備が不十分 | ・外部委託先管理の強化<br>・プロジェクトの固有のリスクを踏まえたBCPの整備<br>・大規模障害を想定した危機管理体制の整備<br>・訓練等による実効性の確保<br>・課題解決のためのIT人材の確保、第三者目線によるチェック強化 |
| (3)日常の運用・保守等の過程の中で発生 | ①冗長構成*が機能しない | ・冗長構成が意図どおりに機能するよう実効性の確保<br>・冗長構成が機能不全を起こす不具合へのパッチに関する適切な管理 |
| | ②障害時の復旧に関する不芳事案 | ・障害原因を早期特定するための必要な情報把握と情報取得手段の確保 |
| | ③記憶領域の確保不足による障害 | ・記憶領域の確保に係る設定内容の十分な確認、検証の強化<br>・記憶領域の使用状況を把握、適時対策を実施するための監視強化 |
| | ④取引量増加に起因する障害 | ・顧客の利用量増加を踏まえたシステムの処理能力設計に係る品質強化<br>・システムの処理能力の事前検証による実効性の確保 |
| (4)プログラム更新、普段と異なる特殊作業等から発生 | ①設定ミス・作業の誤り | ・（本番システムに影響する作業を行うことよるリスクを軽視することなく）作業手順書の確認強化、作業実施体制の強化 |

*システム障害に備えて設備や装置を複数用意しておき、一部障害が発生しても運用が継続できるようにしたシステム構成

# コラム：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（TLPT）の好事例及び課題

## 1. 国内金融機関におけるTLPT *1の現状

- サイバー攻撃の脅威が高まる中、技術的な対策だけではなく、人及びプロセスも含めた対応が必要であり、TLPTはその対応態勢の実効性を検証する有効な手法。近年、我が国の金融機関において、TLPTの活用が増えており、好事例も認められるものの、TLPTの内容や活用方法に改善の余地がある事例も認められる
- 金融庁では、銀行等におけるTLPTの実施事例を収集し、主な好事例及び課題を整理し、匿名化・一般化したうえで、その結果を銀行と共有した

## 2. 分析結果概要

- TLPTの重要な要素：
  - ✓ 一般的な脅威だけではなく、自組織に特有の脅威を分析し、現実の攻撃を模した攻撃を実施する（具体的には、脅威インテリジェンスの導出結果を踏まえ、自組織を標的とし得る攻撃者、及び、それらの攻撃者が現実に用いている攻撃手法を想定し、テスト計画へ反映する等）
  - ✓ システム、IT資産、技術的な対策のほか、人、対応プロセスも評価する（例えば、導入されているセキュリティ製品の有効性にとどまらず、インシデント対応を担うブルーチーム*2の能力も評価する）
- 本調査で銀行等から提供された事例を分析した結果認められたTLPTとして望ましい事例と不十分な事例の概要は次頁のとおり
  - ✓ なお、TLPTとしては不十分であっても、なおサイバーセキュリティの強化に資する側面があると考えられるため、そうした金融機関の取組そのものが否定されるものではない

## 3. 金融機関に求められる対応

- 金融機関は、TLPTに重要な要素、望ましい事例及び不十分な事例を参考としてTLPTを実施することが望ましい
- 経営陣は、攻撃者の目線から、組織的な態勢と技術的対策を検証し、抽出された課題への対策を講じることにより、経営上のリスクを低減させるというTLPTの意義を踏まえたうえで、TLPTで重要な課題が検出されれば、躊躇なく現場から報告がなされるような組織文化を築くべき。また、経営陣は、現場とのコミュニケーションを厚くすることなどを通じ、TLPTによって判明した課題の経営上の重要性及び緊急性、課題の根本原因、課題の解決に必要なリソース及び時間などを含め、課題の全体像を把握したうえでその解決に臨むべきである

*1 Threat-Led Penetration Testingの略　*2 模擬的な攻撃者グループに対してセキュリティ態勢を維持することにより、組織の情報システムにおけるセキュリティを確保する責任を負うグループを指す。

# TLPTの好事例及び課題

| | 望ましい事例 | 不十分な事例 |
|---|---|---|
| **脅威インテリジェンス** | • 自組織に特有の脅威インテリジェンスを導出し、シナリオ選定している。 | • 脅威インテリジェンスが一般的な脅威情報の分析にとどまっている。 |
| **評価** | • ブルーチームに対して事前予告せずにTLPTを実施し、その検知・対応能力を評価している。<br>• SOC[*3]における検知・対応能力だけでなく、フィッシングメールを起点とした職員からCSIRTへのエスカレーションと、CSIRT[*4]の対応状況も評価している。 | • TLPTの計画を事前にブルーチームに伝え、ブルーチームが、疑似攻撃が発生することを把握しているため、その検知・対応能力が適正に評価されていないおそれがある。<br>• 攻撃者が考え得る複数の経路からの侵入や迂回攻撃を試みていないため、事前に想定した攻撃手法・経路で検証対象の脆弱性を検証する脆弱性診断と実質的に異ならないものにとどまっている。 |
| **経営陣への報告<br>経営陣の対応** | • サイバーセキュリティ担当部署は、TLPTの結果から判明した全社的な影響を生じさせ得るリスクを経営陣に報告している。<br>• 経営陣は、TLPTの結果報告を受け、課題への対応を指示するだけではなく、テスト範囲の拡大や事前に予告せずにテストを実施することを通じて、TLPTの高度化を図るように指示している。 | • 業務や顧客に重大な影響を及ぼし得る類似の課題が繰り返し検出されており、対策が十分ではなく、重要なリスクが残存している可能性を推測すべきであるにもかかわらず、過去の発見事項と類似していることをもってサイバーセキュリティ担当部署が経営陣への報告を省略している。<br>• TLPTによって検出された課題のうち、金融機関の経営に重要な影響を及ぼし得るものついて経営陣に報告したり、具体的なリスクについて報告したりせず、単に「良好な結果であった」と報告している。 |
| **発見事項の活用** | • サイバーセキュリティ担当部署は、TLPTで検出された課題と同様の課題がTLPTの対象でなかったシステムにおいても認められないかどうかを確認し、報告するよう、社内の他のシステム担当者及びグループ会社のシステム担当者に対して指示している。 | • TLPTで検出された課題が他のシステムでも認められないかどうかを確認していない。その結果、それ以降、他のシステムに対して実施したTLPTでも類似した課題が検出されている。 |
| **その他** | • 犯罪集団、国家が関与する主体、内部犯行者などの様々な主体の攻撃が生じさせる脅威に応じ、複数のシナリオを設定し、TLPTを実施している。 | • TLPTの趣旨・目的に沿った十分な予算が確保されておらず、脅威インテリジェンスやブルーチームの評価が省かれ、結果として、TLPTとしては不十分なテストとなっている。 |

*3 Security Operation Centerの略。　*4 Computer Security Incident Response Teamの略。

# コラム：オペレーショナル・レジリエンスに係る金融機関との対話等の概要

金融庁では、2023年４月に公表した「オペレーショナル・レジリエンス確保に向けた基本的な考え方」（オペレーショナル・レジリエンスに関するディスカッション・ペーパー）及び同ディスカッション・ペーパーの趣旨を踏まえて同年６月に改正した主要行等向けの総合的な監督指針に規定する基本動作及び主な着眼点等について、主要行等及び国際統一基準金融機関を対象にアンケートを実施した上で一部の金融機関と対話を行った。その結果の概要は、以下のとおり。

（なお、本コラムの内容はアンケートやヒアリングの結果をまとめたものであって、これをもって当庁が各金融機関におけるオペレジの確保が完了したと認識していることを必ずしも意味するものではない。）

| 基本動作 | 取組事例 |
|---|---|
| **①「重要な業務」の特定** | • 重要な業務の選定にあたっては、既存のBCP（事業継続計画）の対象業務を選定することを検討しつつも、新たな基準を設けて、重要業務の範囲を見直している先が多くあった。<br>• 具体的には、顧客目線に立った業務中断時の影響を重視するとともに、業務が中断した場合の自行への影響（取引数・取引額などの観点からなど）、業務の特性（取引時限があるか否かなど）等も加味しながら選定を行っている傾向が認められた。 |
| **②「耐性度」の設定** | • 既存のBCPのRTO（目標復旧時間）を活用して耐性度を設定するとしている先が多くあった。<br>• 一部の金融機関においては、影響を受ける取引数、取引額及び利用者数に加え、苦情数を考慮している事例、業務特性に応じた時限を考慮している事例、RTOにRLO（目標復旧レベル）を組み合わせている事例が認められた。 |
| **③相互連関性のマッピング・必要な経営資源の確保** | • 重要業務の遂行に必要な経営資源として、人員、システム、施設、サードパーティなどの関連性・依存度をマッピングしている先が多くあった。<br>• マッピングにおいて重要業務単位でフローチャートを用いて経営資源（人員、システム、施設など）を可視化している事例が認められた。 |
| **④適切性の検証・追加対応** | • 重要な業務の特定、耐性度の設定、必要な経営資源の配分などが適切であることを検証するシナリオとして、システム停止が長期化するなどのストレスシナリオの検証を行っている事例、業務停止の原因を問わず、システム、要員などの経営資源が棄損したという結果事象を想定したシナリオによる検証を進めている事例が認められた。 |

- **金融機関においては、利用者目線に立った重要業務の早期復旧や影響範囲の最小化のため、経営陣のコミットメントの下、ロードマップを立て、オペレジの確保を計画的に進めることが望ましい。**