金融分野におけるITレジリエンスに関する分析レポートの概要（2025年6月）

- 金融庁では、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」を公表してきた。昨今の地政学リスク、サイバーリスク等の高まりを背景に、金融業界に対して一層のレジリエンスの強化が求められていることを踏まえ、サイバーセキュリティ、オペレーショナル・レジリエンスの観点も含め、 2024年度においては、「金融分野におけるITレジリエンスに関する分析レポート」として再構成した

- 本レポートの構成：

（１）システム障害の分析（第2編）
  - 標的型ソーシャルエンジニアリングを用いたサイバー攻撃による顧客暗号資産の不正流出事案
  - 金融機関の委託先である電子帳票等の発送業者から顧客情報が漏えいした事案
  - 金融機関に対するDDoS攻撃事案
  - 金融機関が利用しているセキュリティソフトのアップデート不具合によるインシデント
  - 証券会社等の顧客口座への不正アクセスによる不正売買事案　等

（２）サイバーセキュリティ（第3編）
  - 金融分野におけるサイバーセキュリティに関するガイドライン
  - 脅威ベースのペネトレーションテスト（TLPT）

（３）クラウド（第4編）

（４）オペレーショナル・レジリエンス（第5編）

（補論）システム障害事例集、耐量子計算機暗号への移行

- 本レポートのメッセージ：

✓ ITの複雑化とITへの依存度の増大により、ITリスク・サイバーリスクは金融機関の経営ひいては金融システムを揺るがしかねないリスクを内包

✓ 金融機関はインシデントの発生を前提としてITレジリエンスを強化する必要がある

✓ 金融機関の経営層は、ITリスク・サイバーリスクをトップリスクとして認識し、内外の事例に照らし、自組織のガバナンス、体制、投資、人材育成について不断に見直す必要がある

✓ 当庁としては、金融機関の自助、金融業界の共助を促進するとともに、検査・モニタリングに加え、対話、情報共有、ガイダンスの提供、サイバーセキュリティ演習等の公助の取組みを強化していく

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 標的型ソーシャルエンジニアリングによる暗号資産の不正流出 ② マルウェア感染（外部委託先） ③ 脆弱性（外部委託先（海外拠点）） ④ DDoS攻撃（継続的攻撃、攻撃量増加） ⑤ 不正アクセス（証券取引等）	• 多要素認証の導入等、注意喚起等を参照した多層的なセキュリティ対策の実施 • システム機器の脆弱性への対応強化（最新情報の把握、パッチ適用の徹底等）、マルウェア対策整備、サイバーセキュリティ・個人情報管理等の観点を含めた外部委託先管理の実効性確保（外部委託先の重要度見直し・リスク評価態勢強化等） • 外部委託先（クラウド利用）の重要度見直し、海外拠点のサイバーセキュリティ管理態勢強化 • DDoS攻撃の軽減対策強化（プロバイダとの連携による態勢強化等）、DDoS攻撃の早期検知・復旧のための態勢整備、業務継続のための態勢整備に関する不断の取組み • 多要素認証等のセキュリティ対策強化、ウェブサイト及びメールの偽装対策の強化、不審な取引等の検知の強化、取引上限の設定、手口や対策に関する金融機関間の情報共有の強化、顧客への注意喚起の強化などの対策
(2)システム統合・更改や機能追加に伴い発生	① ATM仕様差異・ATM稼働設定内容差異の理解不足	• （実績あるプロジェクトのATM仕様等の流用における）仕様差異等に関する影響調査プロセス及びレビュー等におけるレビューアとしての有識者（金融機関、委託先等の関係者）の適切な配置によるレビュー体制の整備
(3)日常の運用・保守等の過程の中で発生	① サードパーティ（製品）の障害による影響 ② 冗長構成が機能しない等の障害 ③ システム障害発生時の復旧不芳	• 特定の製品・サービスに依存することのリスクを再認識し、（継続して）顧客対応を含む業務継続ための態勢整備 • 冗長構成の設定に関するマニュアル整備、冗長構成が意図どおりに機能するよう実効性の確保、冗長構成が機能しなかった際の業務継続のための態勢整備 • 重要なシステム停止等の不測の事態を踏まえ、障害発生時の業務継続に係る代替手段の整備、障害を想定した復旧手順の整備
(4)プログラム更新、普段と異なる特殊作業等から発生	① 作業手順の誤り	• システム変更作業の影響範囲に関する設計書の整備、システム変更作業の作業手順に関するレビューアとしての有識者の適切な配置によるレビュー体制の強化

金融分野におけるサイバーセキュリティに関するガイドライン（2024年10月公表）

（ガイドラインの構成）

１．基本的考え方

1.1. サイバーセキュリティに係る基本的考え方
1.2. 金融機関等に求められる取組み
1.3. 業界団体や中央機関等の役割
1.4. 本ガイドラインの適用対象等

２．サイバーセキュリティ管理態勢

2.1. サイバーセキュリティ管理態勢の構築
2.2. サイバーセキュリティリスクの特定
2.3. サイバー攻撃の防御
2.4. サイバー攻撃の検知
2.5. サイバーインシデント対応及び復旧
2.6. サードパーティリスク管理

３．金融庁と関係機関の連携強化

3.1. 情報共有・情報分析の強化
3.2. 捜査当局等との連携
3.3. 国際連携の深化
3.4. 官民連携

（金融庁ウェブサイト）https://www.fsa.go.jp/news/r6/sonota/20241004/20241004.html

- 近年の脅威動向及び国内外の情勢
- これまでの実態把握、建設的対話、検査・モニタリングの結果
- 金融機関が直面するリスクと求められるリスク管理態勢の差が拡大

- 脅威動向及びリスク環境、並びに、検査・モニタリングの目線を盛り込み、明確化
  - サイバーリスクは企業経営に重大な影響を与えるトップリスクのひとつ。サイバーセキュリティについて経営上プライオリティを置いて考慮しないことは金融機関にとって大きなリスクに
  - 外部（内部）の脅威に対抗するため、官民連携が重要
  - 極力これまでに明らかになったリスクや検査・モニタリング上の教訓を盛り込み明確化
  - 金融機関によってリスクプロファイルが異なるため、詳細で一律のチェックリスト方式は馴染まない。リスクベースアプローチ、自助・共助・公助（及び官民連携）を組み合わせて駆使する必要

サイバーセキュリティ管理態勢

基本的な対応事項

- いわゆるサイバーハイジーンと呼ばれる事項その他の金融機関等が一般的に実施する必要のある基礎的な事項

対応が望ましい事項

- 金融機関等の規模・特性等を踏まえると、インシデント発生時に、地域社会・経済等に大きな影響を及ぼしうる先において実践することが望ましいと考えられる取組み
- 他国の当局又は金融機関等との対話等によって把握した先進的な取組み等の大手金融機関及び主要な清算・振替機関等が参照すべき優良事例

TLPTに関する金融庁の取組み

- **脅威ベースのペネトレーションテスト（TLPT）**
  - 現実の攻撃に対して自組織の体制・対策の有効性や見落とされている点を検証し、自組織のリスクを客観的に可視化し、金融機関が効果的に改善を図るために有効な手段
- **地域金融機関に対するTLPT実証事業**
  - ✓ 地域金融機関の実態を把握するため、幾つかの金融機関に対してTLPTを実施
  - ✓ 判明した脆弱性について、よく認められるものを地域金融機関に還元
  - ✓ TLPTを実施するにあたっての推奨事項を「金融分野におけるITレジリエンスに関する分析レポート」において還元
- **脅威ベースのペネトレーションテスト（TLPT）に関する事例還元**
  - ✓ 金融機関におけるTLPTの実施事例を収集し、主な好事例及び課題を整理
  - ✓ 整理した結果を、匿名化・一般化したうえで、その結果を業態全体に還元
  - ✓ 2023事務年度に銀行を対象に実施したことに引き続き、2024事務年度は保険業を対象に実施

各社の規模やレベルに応じたTLPT等の実践的なテストの実施を推奨

Threat Led Penetration Test：脅威ベースのペネトレーションテスト

（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

出典：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）https://www.fsa.go.jp/inter/etc/20181015/02.pdf

TLPT実施にあたっての推奨方針

① テスト目的の認識合わせ

TLPTの最終的な目的は、自組織におけるリスクを可視化し、必要な対策を講じ、サイバー攻撃に備えることである。制限を設けずにテストを実施すること等を通じ、自社のリスクを可視化したうえで、次に、検知力・対応力の評価を行うべきである

② スコープの設定とテスト内容

TLPTは、脆弱性診断やペネトレーションテストと異なり、特定のシステム単体にスコープを絞らず、組織全体をスコープとすることが望ましい。また、技術的な側面だけではなく、フィッシングメールへの対応や物理侵入への対応といった「人」や「プロセス」の脆弱性を確認することも重要であるため、本番環境においてテストを実施する事を推奨する

③ 経営層の関与

TLPTの実施には部門横断的な調整が求められることなどから、経営陣が主導してTLPTの実施を決定し、推進することが重要である。テスト後においても、判明したリスクに対応するための追加的なリソースの投入や施策の推進をサポートする姿勢を経営陣が持っていることが重要である

④ 関係者との連携・通知

ブルーチームには、非通知でテストを実施することが望ましい。一方、不測の事態に備え、テスト実施に関する事前の通知をしておいた方が良い関係者としては、経営層、情報システム部門の責任者、広報部門の責任者などが挙げられる

⑤ ホワイトチームの対応

TLPT実施中にホワイトチームに求められる主な対応としては、TLPTとサイバー攻撃によって発生するアラート等を切り分けること、関係者等からの各種照会に対応すること、一度成功した攻撃の再実行を省略する等の効率的なテスト推進を検討することなどが挙げられる

⑥ 共同利用システムへのテスト

複数の金融機関で共同利用しているシステムにおいても、重要なシステムについては、テストの対象とするように調整することが望ましい

脅威ベースのペネトレーションテスト（TLPT）に関する事例還元

１．背景･目的

- 近年、金融機関においてTLPTの実施が増える一方、テスト内容や活用方法に改善の余地が認められている
- 金融庁では、TLPTを実施した経験のある一部の銀行から事例を収集して分析し、主要な課題や好事例について還元した

２．結果概要

＜好事例＞
- 一般的な脅威インテリジェンスだけではなく、自社固有の脅威インテリジェンスを導出し、それを踏まえてテストシナリオを設定している
- ブルーチーム（テスト対象となる防御側のチーム）に事前予告せずにTLPTを実施している（ブルーチームの対応を適切に評価するため）
- テスト結果に基づき、重要なリスクについて適切に経営陣に報告している

＜よく見られる課題、特筆すべき課題＞
- テストの前提となる脅威インテリジェンスの導出が、一般的な脅威情報の分析に止まっており、個社固有の脅威インテリジェンスをテストにおいて勘案していない
- ブルーチームにテストについて事前予告しており、ブルーチームの対応を正しく評価できていない
- テスト結果のうち、重要なリスクについて、経営陣に適切に報告していない

クラウドサービス事業者との対話

- ８割を超える金融機関でクラウドサービスが利用され、基幹系システムへのクラウドサービスの採用や検討も進んでいる状況を踏まえ、金融庁では、クラウドサービス事業者との対話を行っている
- 対話を通じ、パブリッククラウドサービスの利用について、障害対応上、金融機関、クラウドサービス事業者及びクラウドサービスを利用して金融機関にサービスを提供する事業者が留意すべき点は以下のとおり

留意事項

1. 金融機関はクラウドサービスを外部委託として管理する必要がある。また、クラウドサービスの特性に由来するリスクを考慮した対策を講じる必要がある
2. パブリッククラウドサービスを利用する場合、金融機関は、障害対応に必要な情報を、オンプレミスの場合と同程度に迅速に取得し、かつ、十分な情報を取扱い可能かについて、予め確認する
3. そのリスク評価のため、パブリッククラウドサービスに起因する障害として、想定以上に深刻なもので、起こり得るシナリオを具体的に設定し、金融機関とクラウドサービス事業者がともに机上演習等を行い、実態を把握することが有効である。また、こうした取組みを同一のパブリッククラウドサービスを利用する複数の金融機関が共同で実施することも有効である
4. 上記を通じ、パブリッククラウドサービスに起因する障害時に適切に対応可能かを金融機関において検証し、インシデント対応計画やコンティンジェンシープランを整備し、必要に応じて更新する

- 当庁としては、クラウドサービスに限らず、ITレジリエンスの向上の観点から、関係者が共同で行う取組みに、必要に応じて協力していく

金融機関におけるオペレーショナル・レジリエンス

- 金融庁では、2023事務年度から一部の金融機関を対象にオペレジに関するモニタリングを実施している
- モニタリングを通じて把握した基本動作ごとの取組事例や課題事例を下記に整理している。金融機関においては、これらの事例を参考として、オペレジ対応における課題の解決やそれぞれの規模・特性を踏まえたベストプラクティスの探求を行うことが望ましい

	① 「重要な業務」の特定	② 「耐性度」の設定	③ 相互連関性マッピング 必要な経営資源の確保	④ 適切性の検証 追加対応
取組事例	• 「公共的使命」「金融市場」「自社の健全性」の観点で各業務を評価した上で選定している • BIA（ビジネスインパクト分析）を行い、資産の損失、対外関係の損失、社会的影響等の観点で評価し、重要な業務を特定している • 「代替可能性」「市場シェア・利用者数」について他項目より重み付けを大きくし、より利用者目線に沿うような選定方法を検討している	• 耐性度として、既存のBCPにおけるRTO（目標復旧時間）を利用することを検討している • 業務の特性に合わせて最大停止許容時間や取引時限等の指標を選択して耐性度を設定している • 耐性度については、「時間（いつまでに）」と「復旧水準（どの程度まで）」を基準に設定している	• 商品・サービスを顧客接点から終了までの各工程と関係者を可視化した業務フロー図をベースとして、不足している経営資源を追加している • 業務フローにて特定した経営資源について、業務遂行において何名の人員が必要か、関連システムは何かなどの粒度でマッピングを実施している • マッピングは、サマリーシートと詳細版シートで構成。サマリーシートを作成することで、経営陣が業務を俯瞰できるようにしている	• 極端だが起こり得るシナリオを想定して、耐性度までに復旧できるのかについて複数のストレスケースを用いて定量的に検証を実施している • 経営資源ごとに極端だが起こり得るシナリオが発生した場合の耐性度の充足度を検証し、リスクを評価している • 検証の観点として、「①耐性度までにサービス復旧できるか」「②代替手段開始までの時間は妥当か」などを予定している
課題事例	• 評価対象業務の洗い出しにおける網羅性確保の難度が高い	• 耐性度の設定にあたっては、考慮すべき条件が多岐にわたり、条件次第で耐性度が変わるため、条件の設定に苦慮している	• 現段階で具体的なマッピング手法は未定となっている • 業務所管部の主導で、社内外の経営資源を端から端まで特定し、マッピングできるかが課題と認識している	• 極端だが起こり得るシナリオとして大規模震災を設定しているが、他のシナリオを含めるなどのブラッシュアップが必要と認識している • 「自然災害」「システム障害」という特定シナリオからのアプローチだけでなく、経営資源が毀損した場合を想定したアプローチでの検証が必要と認識している

これらの事例は、アンケートやヒアリングの結果に基づいた一般的な傾向や金融機関にとって参考となると考えられる事例をまとめたものであり、金融庁として個別の金融機関及び業界全体の進展度について認定するものではない点や、ここで紹介する取組事例を実施することでオペレジの確保が完了することを担保するものではない点に留意が必要である

耐量子計算機暗号（PQC）への移行対応

経緯	• 実用的な量子コンピュータ（量子計算機）の実現と普及は、**社会に恩恵をもたらす一方で、攻撃者が、量子コンピュータを既存の暗号化技術の解読（危殆化）のために使用するおそれ** • 耐量子計算機暗号（PQC：Post-Quantum Cryptography）への移行に向けた早期の準備が必要
概要	金融庁において、2024年7月から10月にかけて、「**預金取扱金融機関の耐量子計算機暗号への対応に関する検討会**」を開催（計3回）
目的	金融機関においてPQCへの移行を検討する際の**推奨事項、課題及び留意事項**について、**幅広い関係者と議論**を深めるため
参加者	預金取扱金融機関に係る**各業界団体の代表者や有識者**が参加 構成メンバー：3メガバンク、全銀協、地銀協、第二地銀協、全信協、全信中協、労金協、農林中金、日銀金融研究所、日本ネットワークセキュリティ協会の代表者 オブザーバー：金融ISAC、CRYPTREC事務局、FISC、日銀金融機構局、NISC
成果物（報告書）	• 金融機関の**経営層がリスクを正しく認識し、リスク低減策を適切に推進**できるようにすることを目的として、本検討会の議論を踏まえた**報告書を公表**（2024年11月） • 預金取扱金融機関のみならず、あらゆる業態の金融機関に参考となる

PQC検討会による報告書の主要メッセージ

量子コンピュータの実用化によって現在の暗号技術が破られることになれば、インターネットバンキングをはじめとする金融情報システムの安全性が根底から覆される。すべての金融機関は顧客や自身の情報・財産を守るため、規模・特性にかかわらず、直ちに耐量子計算機暗号（PQC）への移行に着手しなければならない

報告書の主要メッセージ

① 金融機関はまず、自らの情報資産を網羅的に把握した上で、それぞれの情報資産の重要性を評価し、どのような暗号が用いられているかをリスト化したインベントリー（台帳・目録）を作成すること

② その際、自らが運用するシステムだけではなく、サードパーティーに運用を委託している重要システムの情報資産と暗号に関するインベントリーも作成すること

③ インベントリーの作成作業にはかなりの労力を要するので、早い段階からITベンダーの協力を得ること

④ インベントリーに基づき、量子コンピューターが実現すると脆弱性にさらされる情報資産のうち、影響が大きいシステムから順にPQCへの移行を進めること

⑤ 検討の開始から移行までの一連の作業に関して、ロードマップを作成すること

⑥ 実務的には大規模システム更改などに合わせてPQCへの移行を進めることを踏まえると、量子コンピューターの実用化（2030年代半ば）までに残された時間は少ないため、速やかに移行への対応を開始すること

⑦ PQC自体も脆弱性が明らかとなる恐れがあるため、特定の暗号に固定することを前提とするのではなく、それが脆弱になった場合に暗号を差し替えやすいシステムにしておく、いわゆるクリプト・アジリティーを確保しておくこと

⑧ 移行には長い期間と多くの経営資源の投入が必要であるため、経営陣の強いコミットメントが求められること