国内金融機関における
サイバーセキュリティの論点

金融機関では、デジタルトランスフォーメーション（DX）の進展、新型コロナウイルス感染症（COVID-19）の世界的流行や、働き方改革への対応によるニューノーマル（新常態）社会への移行など、サイバーセキュリティを取り巻く環境が大きく変化しています。本稿では、変化する環境のなかで発生している事案や、規制当局の動向を踏まえ、今後金融機関が意識するべきサイバーセキュリティ対策の論点について考察します。

1. 金融機関を取り巻く環境の変化

2020年6月に、金融庁から「金融分野のサイバーセキュリティレポート」が公表されました。レポートでは各金融機関に対し、サイバーセキュリティの強化と、経営陣主導のもと組織の防衛力強化につながるさまざまな取組みを着実に推進することを求めています。

金融機関では、従前からクラウドサービスやAI活用を進めており、昨今のオンライン取引の増加や金融サービスの電子化、政府主導のキャッシュレス決済の推進など、DXの加速度的な進展を踏まえた対応と併せて、さらなるサイバーセキュリティへの対応が必要となっています。また、基本的なサイバーセキュリティ対策に加えて、今後はニューノーマル社会に即した取組みも求められます。

2. 国内金融機関におけるサイバーセキュリティ事案と当局動向

外部環境が変化するなか、金融機関を標的としたサイバー攻撃の高度化・複雑化によるサイバーセキュリティリスクの高まりに対応するべく、金融庁はガバナンスやリスク管理の高度化を求めています。そのなかには、サイバーセキュリティ対策の高度化の論点も多く含まれています（図表1参照）。

【図表1】

高度化・複雑化するサイバーセキュリティ事案	サイバーセキュリティに関連する当局の要請事項
キャッシュレス決済における不正利用	口座振替を行うプロセスの脆弱性を確認する
	決済における認証手続（多要素認証の導入など）等のセキュリティ強化
サードパーティリスクの増加	グループ・グローバルベースの高度なリスク管理
	セキュリティモデルの転換
リモートワーク環境を狙った攻撃の増加	インシデント対応能力の高度化
	脅威ベースのペネトレーションテスト（TLPT）を通じたサイバーセキュリティ態勢の実効性向上

I. キャッシュレス決済における不正利用

金融機関と連携する資金移動業者の決済サービスがサイバー攻撃を受け、当該サービスと関係のない消費者にも被害が発生する事案が生じたため、当局では預金取扱金融機関および資金移動業者に向けて、以下を要請する事態となりました。

- 預金取扱金融機関および資金移動業者に対し、預金取扱金融機関と資金移動業者が連携して口座振替を行うプロセスに脆弱性がないか確認すること
- 決済手続における認証手続の強化（多要素認証の導入など）を含むセキュリティを強化すること

II. サードパーティリスクの増加

新型コロナ感染拡大による業務のデジタル化やビジネスモデルの変革に伴い、定型業務のアウトソースがさらに進むことが予想されます。金融機関のサードパーティとしては、クラウド事業者やAPI提供者などが挙げられますが、その契約形態や委託業務は多岐にわたります。そのため、サードパーティごとのリスクを見極め、組織における態勢整備と技術的対策の双方を実行することが必要です。前述の「金融分野のサイバーセキュリティレポート」でも推進される取組みとして、グループ・グローバルベースの高度なリスク管理とセキュリティモデルの転換が挙げられています。前者では、自社のサイバーセキュリティ態勢の枠組みにグループ企業やサードパーティを含め一元的に管理することが求められ、リスクに応じた方針の策定や評価、モニタリング

方法等を整備することが考えられます。後者については、ゼロトラストの考え方を適用した対策として、認証の強化やアクセス権限の設定等により外部から内部への侵入リスクを低減することが挙げられます。

III.　リモートワーク環境を狙った攻撃の増加

緊急事態宣言の解除後も多くの企業が在宅勤務を継続しており、オフィスに比べて脆弱なリモートワーク環境を狙ったサイバー攻撃が増加しています。ビジネスメール詐欺やウェブ会議サービスを利用した情報の窃取等が報告されているほか、VPN接続時に認証情報が漏洩する事案も発生しています（図表2参照）。不正アクセスやウイルスなどに対する基本的な対策に加えて、インシデント対応能力を高度化することが必要です。特に大手金融機関では、2018年10月の金融庁による「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」のアップデート以来、脅威ベースのペネトレーションテスト（TLPT）を通じて、サイバーセキュリティ態勢の実効性を向上させることが期待されています。リモートワーク環境を前提として想定し得る脅威をTLPTのシナリオに組み込むことや、インシデント対応能力を評価することが必要な対応として考えられます。

【図表2】

サービス	ツール	報告された脆弱性
ウェブ会議サービス	Zoom	ユーザのWindowsアカウントの認証情報が窃取される
	Microsoft Teams	アカウントの乗っ取り
	Cisco Webex Meetings	細工したリクエストでユーザ権限を取得し、不正にアクセスする
VPN	BIG-IP	認証されていない遠隔の第三者が任意のコードを実行できる
	パルスセキュア	認証情報の漏洩

出典：『Zoomの脆弱性対策について』（独立行政法人情報処理推進機構）
https://www.ipa.go.jp/security/ciadr/vul/alert20200403.html

『緊急情報を確認する』（一般社団法人JPCERTコーディネーションセンター）
https://www.jpcert.or.jp/menu_alertsandadvisories.html

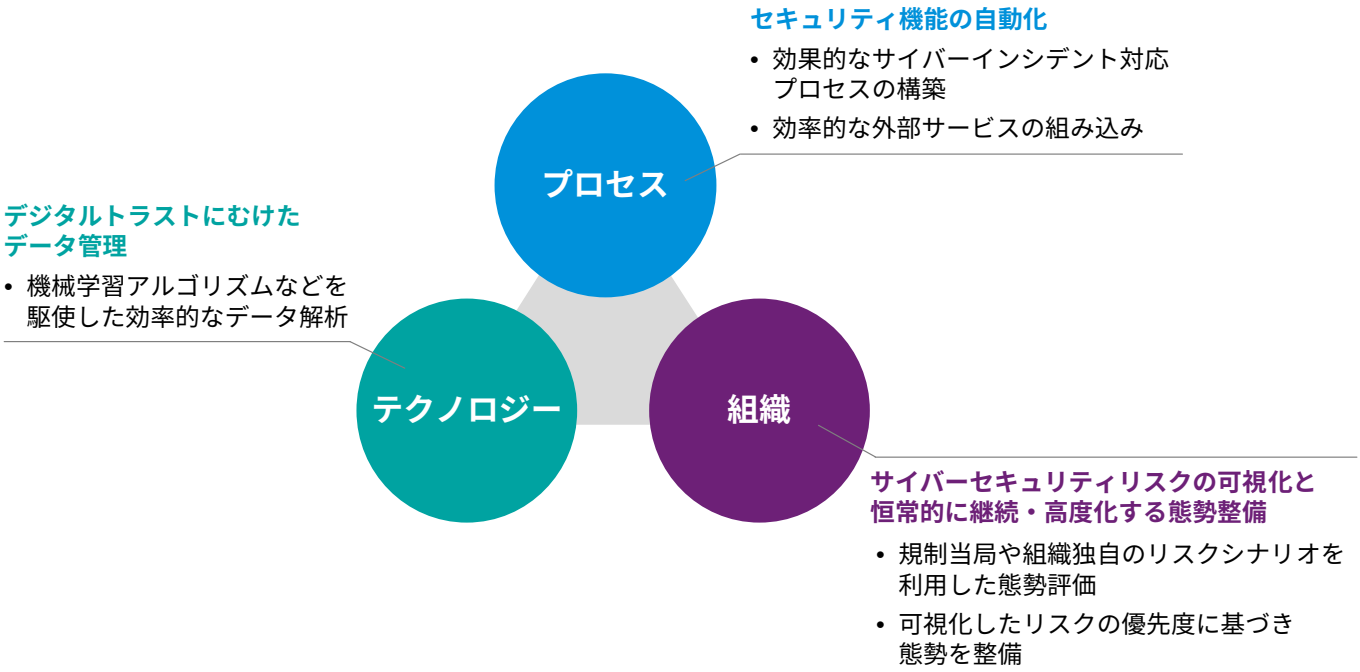
上記を基にKPMG作成

3. 今後のサイバーセキュリティの論点

外部環境の加速度的な変化に伴い、サイバー攻撃は高度化・複雑化の一途を辿っていると考えられます。そのため、サイバーセキュリティを取り巻く環境においては、これまで以上に効率的かつ迅速な対応が必要です。また、自組織だけに留まらず、サードパーティを含む金融システム全体で包括的にサイバーセキュリティリスクを捉えた対応が求められています。

そのような状況下で、今後のサイバーセキュリティの論点となる事項を「テクノロジー」、「プロセス」、「組織」の3つの観点から考察します（図表3参照）。

【図表3】



I.　テクノロジー＜デジタルトラストにむけたデータ管理＞

顧客は、取引が最も簡単かつ信頼・安全できるサービスを利用すると考えられます。そのため、金融機関は特に顧客に安全な環境を提供することが前提となります。前述のとおり、DXの推進に伴うデジタル時代において、信頼（トラスト）を構築することが今後の金融機関に求められる要件であると言えます。

信頼を得るためには、データの利用方法を理解し、それに対処することが必要です。例えば、規則に則ったシナリオに基づき取引モニタリングを実施している場合、高度なサイバー攻撃のリスク要因が想定できていない可能性があります。従来のシナリオに即した攻撃パターンへの対処だけでなく、機械学習アルゴリズムを有したツールを導入するなど、最新の「テクノロジー」を駆使し、効率的なデータ解析によってリスクの高い取引や顧客などを特定するといった、異常検知プロセスの高度化が不可欠になると考えられます。

II.　プロセス＜セキュリティ機能の自動化＞

サイバーセキュリティ事案に対して、レジリエンス（回復力）を高めるための「プロセス」の構築が論点になると考えられます。「インシデントが発生した場合に迅速に対応し、被害を最小限に抑え、重要業務を継続する」というオペレーショナルレジリエンスの考え方は、米国の金融安定理事会（FSB）の「サイバー事象の初動・回復対応の効果的な実務」や欧州銀行監督機構（EBA）の「監督上の検証・評価プロセス（SREP）」など、各国当局においても重要性が示されています。サイバー攻撃はその内容も高度化・複雑化しており、ウイルス対策ソフトの導入やアクセス権管理などの予防的対策に加え、攻撃を前提としてインシデントを封じ込めることがますます重要となると予想されます。

レジリエンスの考え方に基づいた、より効果的なサイバーインシデント対応プロセスの例として、セキュリティ対策の自動化が挙げられます。インシデントの検知や情報収集、分析から対処までの一連の対応には膨大な労力がかかりますが、それらを自動化することで効率的な対処が可能です。AIや機械学習を活用した不正アクセスの兆候検知や監視、本人確認機能の強化など外部サービスを適宜組み合わせた対応が選択肢となると考えられます。

III.　組織＜サイバーセキュリティリスクの可視化と恒常的に継続・高度化する態勢整備＞

従来から提唱されているリスク管理態勢の高度化を持続的に図ることができる「組織」の構築が、引き続き論点になります。組織として最優先すべき対応事項は、サイバーセキュリティリスクの可視化です。例えば、規制当局が公表するガイドライン、組織で独自に作成するリスクシナリオを利用した態勢評価やTLPTによる技術・インシデント対応両面の評価を通じて、現時点のリスクを把握します。その際に、外部環境の変化（リモートワーク環境での攻撃やサードパーティリスクの増加等）を踏まえ、チェック項目やシナリオを見直し、適宜追加することが効果的なリスクの可視化につながると考えられます。また、中長期的な取組みとしては、可視化したリスクに対して優先度を決めて態勢を整備すること、定期的なリスクの見直しを通じてリスク管理態勢を高度化することが挙げられます。金融機関においても従前から実施されている対応ですが、直近の事案も踏まえて改めて組織としてサイバーセキュリティ事案に対するリスク管理態勢を再評価することが重要だと考えられます。

4. おわりに

サイバー犯罪の手口は、昨今の環境変化を経て、ますます高度化・巧妙化の一途を辿るものと考えられます。営業秘密や個人情報の窃取・漏洩、基幹システムの停止など、その脅威は金融機関にとって、企業としての業績や事業継続上、深刻なダメージを引き起こします。これらの脅威を完全に排除することは非常に難しいため、サイバー攻撃や侵入を前提とした考え方にシフトする必要があります。つまり、サイバーセキュリティの本質はリスク管理であると認識しています。サイバー攻撃から壊滅的な打撃を受けることなく、サービスを継続できる環境を構築するには、日増しに進化する新たな手口に対して、継続的なリスク管理態勢を日々の業務運営に反映させることが重要です。

※本文中に記載されている会社名・製品名は各社の登録商標または商標です。

KPMGコンサルティング株式会社
シニアマネジャー　大津留 一郎
シニアコンサルタント　山崎 亮
シニアコンサルタント　栗原 麻衣

KPMGコンサルティング株式会社

03-3548-5111
kc@jp.kpmg.com

home.kpmg/jp/kc