KPMG
cutting through complexity

銀行規制の進化

パート3

データとテクノロジー：
規制上、事業上の課題

2015年10月

kpmg.com

KPMG INTERNATIONAL

目次

銀行規制の進化―パート1およびパート2

本レポートは、2015年「銀行規制の進化」シリーズのパート3です。本レポートでは、データ、テクノロジーおよびサイバー・セキュリティについて銀行が直面する課題を掘り下げます。

パート1では、**銀行に対する規制圧力**について概説しました。パート2では、銀行の事業構造について、さらには規制圧力および商業的圧力にビジネスモデルの変革を促される世界において、**多くの銀行が実行可能かつ持続可能な未来を模索している現状**について取り上げました。

今後発行予定の「銀行規制の進化」シリーズでは、コンダクト（事業行為）や文化、ガバナンスについて取り上げる予定です。

エグゼクティブ・サマリー

本レポートは、2015年「銀行規制の進化」シリーズのパート3です。パート1では、金融危機以降の規制改革の設計段階から施行段階までの道のりを取り上げました。パート2では、銀行の事業構造と、銀行が実行可能かつ持続可能なビジネスモデルを模索している現状に焦点を当てました。

銀行が直面しているデータおよびテクノロジー上の課題が、これらのテーマの延長線上にあるのは自然なことです。事実、**高品質なデータと効果的なテクノロジーは、収益力があり持続可能な銀行の中核となるべきなのです。**

規制

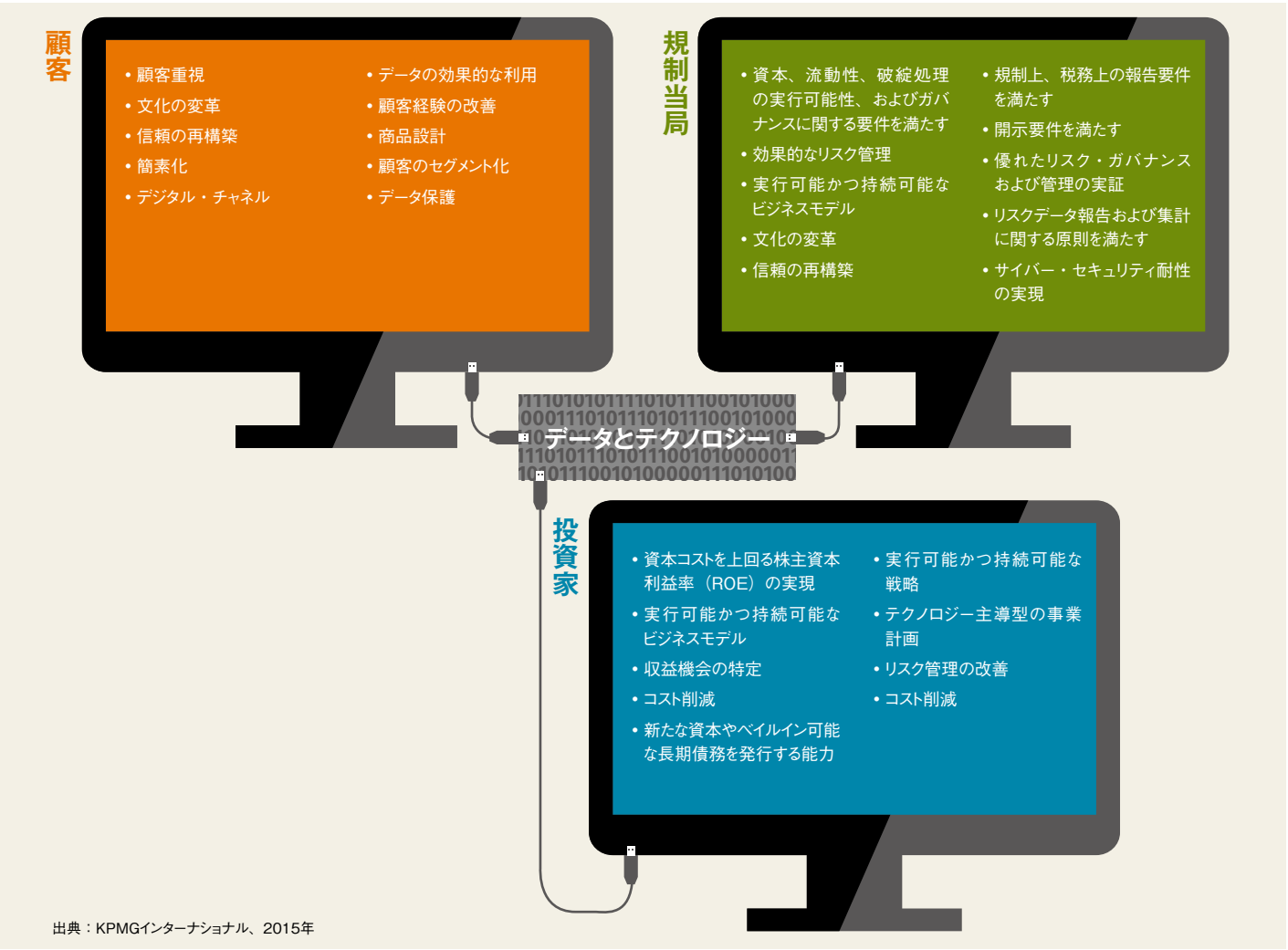
規制報告に対する銀行の負担はここ数年で格段に増加し、今後数年でさらに増えることが決まっています。規制要件が増え、監視が強化されたことにより、規制当局の間にはとどまることを知らないようなデータへの欲求が生まれました。その目的は、規制要件遵守の監視、ストレステストの支援、単発的な情報要請への対応、再生・破綻処理計画の策定に向けた素材の提供、銀行以外の融資チャネルにも目を向けること、そしてマクロ健全性方針の目的においてシステム全体のデータにアクセスすることにあります。

さらに、規制当局の焦点は、比較可能性、市場規律、市場トレーディングおよび価格形成を強化するための**情報公開、銀行内でのリスクデータ集計およびリスク報告**、さらにはよりリスクベースで外部の信用格付けへの依存度を引き下げた、**信用リスクおよび市場リスクに対する改定後の標準的手法**を支援するための代替のデータソースに向けられています。

最終的に、規制項目の下で、**本人確認、行政処分、税務、データ保護、リテール及びホールセール両方の顧客の取扱い**に関するさまざまな規制イニシアチブのすべてが、データとテクノロジーに重要な影響をもたらします。一方で、**リスクのオフショア化、サイバー・セキュリティおよび耐性**に一層厳しい目が向けられているため、いずれはデータやテクノロジーに対するさらなる規制要件に形を変えていくことに間違いはないでしょう。

この規制介入により、**銀行の上級経営陣が銀行経営に活用しているはずのデータとテクノロジーについて、根本的な疑問が生じます。**規制要件を満たすために必要となるシステムやデータ・アーキテクチャが銀行に存在するのかという疑問がその1つです。さらには、現在多くの銀行が資本計画策定、価格設定およびリスク管理に利用している内部モデルと、銀行経営の在り方についての新たな規制上の考え方との間にある隔たりが拡大しているという問題もあります。新たな規制上の考え方には、リスクウェイトの算出における内部モデルの利用制限が含まれます。

ステークホルダーから求められる銀行の対応



出典：KPMGインターナショナル、2015年

データ

顧客のニーズに応え、商業的価値を引き出し、優れたリスク・ガバナンスを支援するためのカギを握るのが、高品質なデータとデータ分析です。

商品やサービスの設計においてデータをうまく活用することで顧客体験を改善し、顧客のニーズをより効果的に特定して、それに応えることは、多くの銀行で可能であり、またそうする必要があります。しかし、ここにも規制上の問題が潜んでいます。銀行に対して認められる、顧客に特化した「ビッグデータ」の収集、保管および分析の範囲が、不適正販売やデータ機密、サイバー・セキュリティに対する懸念を理由として、規制当局に制限されることはないでしょうか。

データやデータ分析によっても、商業的価値を切り開くことは可能です。銀行は、実行可能性、持続可能性、破綻処理の実行可能性という観点から、自行の事業活動の相対的な能力に対する理解を高め、新しい戦略やビジネスモデルを策定する必要があります。

効果的なリスク・ガバナンスにとっても、データは非常に重要です。銀行は、高品質なデータや有意義な経営情報の上部への報告なしに、リスクを効果的に特定し監視することはできません。

これらのデータ利用のすべてにおいて、正確かつ適時のデータ記録、データ利用に向けた効果的な処理、データおよびデータ処理に対する明確なガバナンスとオーナーシップが求められます。

テクノロジー

デジタル・チャネルからの商品やサービスへのアクセスを求める顧客の要望に応え、コストを削減し、経営上の耐性を維持および改善し、優れたデータ管理およびリスク管理を下支えするにあたっては、効率的かつ効果的なテクノロジーがそのカギを握ります。

銀行の顧客は、銀行以外の金融機関（ノンバンク）による優れたデジタル・チャネルにも劣らないようなデジタル・サービスを、ますます期待するようになっています。このようなサービスを提供するテクノロジー能力がある銀行は、明確な競争優位性を獲得できます。

テクノロジーはまた、コスト削減の実現、または少なくとも経営上の耐性が低いことから生じるコストを回避するにあたって非常に重要な要素です。銀行は、個人預金や払戻し、決済システムなど、なくてはならない経済機能の提供における全般的な耐性に焦点を当てる必要があります。

複数の分散したITシステムを持ち、特にこれらを外部委託してきた銀行は、大きく取り残され、実行可能かつ持続可能な未来を確保できないリスクにさらされています。

したがってこれらの銀行では、明確な戦略的ビジョンを策定し、テクノロジーによって顧客サービスとリスク管理の改善をどのように進めていけるのか、（事業活動や法的構造および事業構造の簡素化とともに）テクノロジーによってどのようにコスト削減を進めていけるのか、ガバナンスの枠組みとIT戦略により、高水準なサービス提供、ITインフラ、経営の継続性およびサイバー・セキュリティを通して、経営上の耐性をどのように達成できるのかについて、明確なロードマップを描く必要があります。

銀行は、必要とされる変革の実施において、リーダーシップ、専門性、そして自信の欠如を克服しなければなりません。利益率が低い状態が続く中にあっても、何もしないことによるコストは、将来に対する投資コストを次第に上回るようになるでしょう。

銀行が受ける影響

銀行は、データとテクノロジーに関する規制圧力および商業的圧力に対応するにあたり、多額のコストを要する数々の重要課題に直面しています。これらの課題は、次の5つの分野に大別できます。

データの取込み、品質および一貫性

最も基本的なこととして、多くの銀行はデータの品質と整合性の改善において、さらに前進する必要があります。顧客体験、内部リスク管理、そして内外への報告を改善するために必要となるデータが単に整っていないか、または正確ではないという、非常に基本的ですが、到底無視できない問題に直面しているのです。

現在、多くの銀行では、縦割りでデータを保有および管理し、この縦割りの中からデータを報告しています。現状では、複数のシステム間、複数の事業活動間、複数の営業地域間、複数の法人間、事業部門と第2の防衛線（リスクおよびコンプライアンス）間、さらには規制報告と財務諸表との間でのデータの整合が困難である場合があります。これによって、重複、内外への報告書作成の遅延、不一致や間違いが生じ、さらには手作業や急場しのぎに頼らざるを得ない状況にもつながります。

こうした状況によって、これらの銀行では、すべてのリスクタイプ、事業活動、営業地域にわたるリスクデータの迅速かつ正確な集計ができなくなっています。その結果、質の高いリスク特定、測定と監視、上級経営陣および取締役会レベルでの質の高い意思決定に必要な情報として利用できる、高品質な管理情報の生成と利用に課題を抱えています。

銀行は、現存する報告要件および今後発生するであろう報告要件を満たし、内外からの単発的な情報要請に対応するための、持続可能で強固なデータ・インフラを必要としています。そのためには、定義や様式を共通化するなど、銀行グループ全体で保有するデータの標準化に注力しなければなりません。そうすれば、データの「単一ビュー」の作成や、オーナーシップ、統制および保存の面でのデータの集約、さらにはさまざまな目的での集計がより容易にできるようになります。

データ分析

多くの銀行では、データ分析能力の改善も必要になります。自行のデータから、より高い価値を抽出することにより、顧客ニーズのより深い理解と、より効果的、効率的かつ収益力のある方法でのサービス提供を通して、顧客重視の姿勢を高める必要があります。また、他行や銀行業界に、すでに出現しているか今後出現する可能性のある新規参入企業に対する競争力を維持しなければなりません。さらに、出現しつつあるトレンドや課題をより効果的に特定し、ストレステスト実施能力を高め、トレーダーの行動を監視して不正な取引やその他の疑わしい活動を発見していくことも必要になります。

データ・ガバナンス

多くの銀行で、取締役会や上級経営陣レベルでのデータ・ガバナンスの優先順位が高まっています。ここには、規制圧力と商業的圧力の両方が反映されています。この領域での課題としては、銀行のデータのオーナーシップおよび統制、リスクデータの集計および報告に関するガバナンス、データ管理および分析のためのIT能力、さらには、データおよび報告の正確性や、規制要件遵守に対する保証および認証プロセスなどが挙げられます。

一部の銀行は、最高情報責任者の職責を高めることでこれに対応しましたが、今度はそれによって上級経営陣の個人的な責任をより重視する規制当局の姿勢につながっている可能性があります。実際にイングランド銀行はその上級管理職規則（Senior Manager Regime）に、サイバー・セキュリティに対する説明責任を盛り込む予定であることを示唆しています。

多くの銀行でデータの品質、管理、報告およびガバナンスのさまざまな側面に関するプロジェクトが始まっていますが、それによってデータ品質がどのように改善されるのか、データ・ガバナンスおよびデータ管理作業をどのように両立するのか、コストのかかるプロジェクトから日常業務にどのように移行していくのか、どのような状態を目標にするのか、リスクデータ集計とリスク報告に関するバーゼル委員会の諸原則をどのように遵守するのかといった点については、説明できていません。

データ保護とセキュリティ

多くの銀行では、データのセキュリティを改善し、サイバー攻撃耐性を高める必要があります。データ保護とサイバー・セキュリティに関するさまざまな規制要件に準拠するためだけでなく、自行の利益のためにも、顧客データを保護し、サイバー攻撃から身を守るための強固な基準の導入および維持について考えなければなりません。

このセキュリティという側面で重要なのは、顧客が他のサービス提供業者よりも銀行を高く評価している数少ない領域の1つがデータ保護であるという点です。銀行セクターの評判が一般的に低く、デジタル・チャネルを通じたサービス提供がより一層求められる時代において、セキュリティは、銀行が信頼と評判を回復する重要な架け橋になるかもしれません。

テクノロジー

多くの銀行では、テクノロジーの改善に向けて思い切った策を講じる必要があります。データに欠陥があることに加え、多くの銀行では以下を実施するためのテクノロジーが欠如しています。

- 効果的かつ効率的なデータ管理。データ項目の数は急速に増加しており、これらのデータの内外への報告能力および分析能力の重要性も高まっている。
- リスク管理の改善。
- 合理化および効率化によるコストの削減。
- 従来の銀行、新規参入銀行およびテクノロジーを主体とした銀行以外の金融機関（ノンバンク）からの挑戦への対応。これらの企業はすべて、銀行サービスの提供にテクノロジーをより効率的かつ効果的に利用することによる収益機会の開拓を目指している。

多くの銀行は、内容や性質が一様でないうえに断片的に存在する、老朽化して信頼性も低下したITシステムやITインフラに依然としてしばられています。何年もの間、旧態依然としたシステムをいくつもつなぎ合わせ、行内や海外でのテクノロジー開発と外部委託による開発を混合し、増設や急場しのぎ、手作業による介入を続けた結果、銀行は競争という面では、事実上劣勢に立たされています。

必要とされる改善の計画策定と実施には、新しいITインフラを導入するための大規模かつ費用のかさむプロジェクトが必要になる場合があります。利用できるリソースや時間に制約がある場合もあり、その他の規制圧力や商業的圧力に応えるための投資も必要であることから、こうしたプロジェクトについては優先順位を慎重に判断する必要があります。

銀行に対する規制圧力

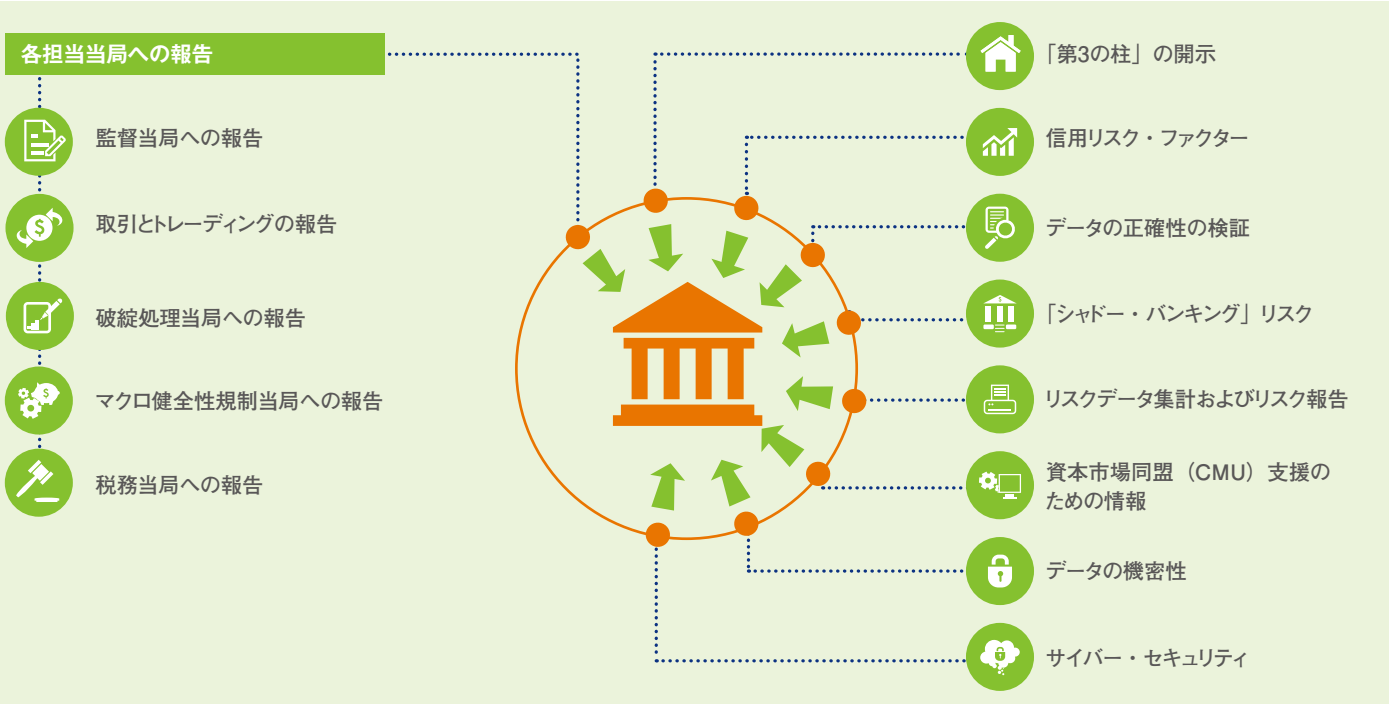
データ関連規制における銀行側の負担は、もはや各国の監督当局へのデータ報告に限られたものではなくなりました。データ面の規制圧力はここ数年で大きく高まりましたが、さらに以下が追加されます。

- 欧州中央銀行（ECB）、欧州監督機構（ESA: European Supervisory Authorities）、各国およびEUの銀行同盟決議およびマクロ健全性規制当局などの新たな監督・規制当局のすべてが、銀行に対するデータやその他の情報の要件を各自で策定している。
- 「第3の柱」の開示によるこれまで以上の情報公開と、ホールセール市場におけるトレーディングおよび証券金融取引（SFT）の報告が求められている。
- 信用リスクの計測に用いられる標準的手法の改定案では、リスクウェイトを判断する「リスク・ファクター」に関するデータの照合と活用が、すべての銀行に求められる見込みである。
- リスクデータの集計とリスク報告の改善に向けた銀行への圧力は高まっており、銀行の内部リスク・ガバナンスに対する監督機関評価の主要な要素になりつつある。
- EU内の銀行は、資本市場同盟（CMU）構築の一環として、より単純な証券化商品や中小企業（SME）についてもデータを照合し公表することが求められる可能性がある。
- 銀行の顧客によるマネーロンダリング、テロ資金供与、脱税に対する防止対策の支援として、データの利用や記録管理の改善に向けた圧力が高まり続けている。
- データの機密性、データ保存、サイバー・セキュリティ、さらには商品やサービスの抱き合わせ販売（特に個人顧客に対して）におけるデータの利用についても、今後、銀行の足かせとなりかねないアプローチがさまざまな関係当局で策定されている。

銀行に必要とされる対応：

- これらのイニシアチブと、それらがデータ報告要件に与える可能性のある影響を予測する。
- 個々のイニシアチブによる影響だけでなく、これらのイニシアチブが組み合わさった場合、特に、すでに導入されている金融危機後のデータ報告要件と組み合わさった場合の影響を評価する。
- 報告ミスを減らすために導入すべきシステムと品質管理を検討する。
- データ報告上のプロセス関連および技術的な課題が、バーゼル委員会によるリスクデータ集計およびリスク報告原則におけるデータおよびシステム要件と重複する箇所を認識する。こういったプロジェクトにおいては早い段階で互いに整合性を持たせ、技術的な重複だけでなく、利用可能なリソースやIT能力といった組織的な課題を考慮することが、銀行にとって有用である。
- 上級経営陣が銀行経営においてデータをどのように活用したいかと、規制当局からのデータ要請への対応とをできる限り整合させる。
- 規制当局からの単発的な要請にも対応できるような、一貫性があり柔軟なデータソースの開発を継続する。

銀行のデータやテクノロジーに対する規制圧力



規制報告

昨年の「銀行規制の進化」では、銀行に対する規制報告要件の分量と詳細度が飛躍的に高まっていることを取り上げました。新たな規制の1つひとつ、そして新たな監督イニシアチブの1つひとつによって、報告要件が追加されています。この報告要件への対応に必要となる人員、データの取込み、管理およびガバナンス、ITシステム、そして品質保証プロセスが、銀行の重荷となっています。

昨年を振り返ると

昨年は規制報告要件が大幅に増加した年でした。欧州・中東・アフリカ地域の銀行に対するデータ要求の中で最も重要なものには、以下があります。

EUでは2014年に**共通報告フレームワーク(COREP)と財務報告フレームワーク(FINREP)**が導入されました。銀行はより広範になった報告要件に概ね対応できましたが、一部の小規模な銀行は提出期限の遵守に頭を悩まされました。報告データについての監督当局からの質問は予想したほど多くなかったとのコメントが一部の銀行から出されており、監督当局自身も増大した報告量を消化・分析するのに手間取っていることがうかがえます。一方で、COREPとFINREPは確定したものではないことを認識することが重要です。融資の条件変更、資産に付帯する負債、レバレッジ比率などの分野で報告範囲が拡大されつつあります。

ECBによる包括的審査では、EUの銀行同盟に参加する主要銀行に対して資産査定(AQR)のための膨大なデータの生成と分析が求められ、EU全体の主要銀行に対しては、欧州銀行監督機構(EBA)が2014年に実施したストレステストの一環として詳細なデータの報告が求められました。さらに、ECBによる資産査定では、一部の銀行のデータ・システムに構造的な弱点が判明しました。ECBではすでに、2015年に銀行と追求すべきテーマとしてデータの一貫性を掲げています。

2015年1月には**EUの銀行再生・破綻処理指令**が施行され、自行の再生計画に関する詳細な情報と、破綻処理当局が破綻処理計画を策定する際に必要となる膨大な情報ベースの規制当局への提供が、ますます求められることになります。

今年の「銀行規制の進化」パート2で概説したように、**業務分離**に関する国内法の施行と、構造的施策に関するEU規制案の進展により、トレーディング活動に関する詳細なデータを提供し、規制によって課された境界線を超えないようにするための最善策を検討することが、一部の国の大手銀行に求められています。

また、今年の「銀行規制の進化」パート1で概説したように、**マクロ健全性規制当局**が創設されたことにより、これらの規制当局が金融の安定性に対するリスクを分析できるようにするための情報の提供が一層求められています。これには、他行やその他の金融機関(「シャドー・バンキング」セクターを含む)との間の相互連関性に関するデータのほか、住宅ローンに関連したローン担保価値や借り手の返済能力の比率に関するデータが含まれます。

自己資本指令4(CRD4)に基づく、**国別の利益および従業員数データの第1回報告**は終了しました。さらに、経済協力開発機構(OECD)は、税源浸食および利益移転(BEPS: Base Erosion and Profit Shifting)イニシアチブの下で各種の報告要件を規定しており、税務目的での報告の大幅な追加が予想されます。

今後に目を向けると

広範な規制イニシアチブにより、銀行にはさらなるデータ報告が求められることが予想され、すでに確定している要件を実行しつつ、これらのイニシアチブにも対応するように圧力が強まっています。

> 「また、今年の「銀行規制の進化」パート1で概説したように、マクロ健全性規制当局が創設されたことにより、これらの規制当局が金融の安定性に対するリスクを分析できるようにするための情報の提供が一層求められています。」

大手銀行による規制報告

グローバルなシステム上重要な銀行(G-SIB)19行を対象にしたKPMGの調査では、以下が明らかになりました[1]。

- プロセスがこれほどまでにデータ集約型であるにもかかわらず、驚くべきことに、規制報告において75%超を自動生成している銀行は40%のみで、自動生成の割合が50%を切っている銀行が全体の4分の1に上った。
- さらなる自動化においては、リソースの割当てと優先順位の競合が制約になっており、これらの銀行の多くでは報告ミスや規制報告遅延のリスクがある。
- 調査対象銀行のほぼ80%が、過去3年の間にリスク・アセット(RWA)の算出について規制当局からのレビューまたは調査を受けており、自己資本の算出については94%に達した。
- 対応として、調査対象銀行の64%では、RWAおよび資本の算出に関して内部での検証プロセスを導入した。
- しかしながら、「第1の防衛線」における報告統制が十分に文書化され評価されていると答えた銀行は56%にとどまった。
- 規制報告に対する取締役会による監視は、財務諸表に対する監視の徹底ぶりには遠く及ばない状況が続いている。

1 G-SIFIベンチマーキング調査、2015年、KPMG

> バーゼルの「第3の柱」では、銀行のリスク・エクスポージャーや規制資本の全体的な十分性についての透明性および信頼性を高め、市場規律を推進することを目的としています。

国際基準とイニシアチブ

(i)「第3の柱」の開示

バーゼル委員会は2015年1月、銀行による「第3の柱」の開示に対するレビューのフェーズ1を終了しました。バーゼルの「第3の柱」では、銀行のリスク・エクスポージャーや規制資本の全体的な十分性についての透明性および信頼性を高め、市場規律を推進することを目的としています。

2016年後半からは、銀行に以下の開示を求める一連の標準テンプレートが強化され、さらには裁量度のより高い様式でその他の情報の開示も求められます。

- リスク・アセット全体の推移
- 規制当局への提出書類と財務諸表との間の関連性
- 信用リスク。信用リスクの軽減、標準的手法で計測された信用リスクと内部格付け手法で計測された信用リスク、カウンターパーティの信用リスクを含む
- 証券化
- 市場リスク

これによって、銀行に求められる「第3の柱」の開示の分量と詳細度が高まり、場合によっては、開示頻度が増える（四半期毎）ことになります。

一方で、バーゼル委員会によるレビューのフェーズ2では、以下が検討されます。

- すでに実施されている「第3の柱」の枠組みで網羅されたその他の領域における報告の強化。オペレーショナル・リスクや銀行勘定における金利リスクが含まれる。
- 金融危機後の新しいバーゼル委員会基準に関連した「第3の柱」の下での既存の報告要件と報告要件案のすべてを統合する最善の方法。これには、報酬、資本構成、レバレッジ比率、流動性カバレッジ比率および安定調達比率、グローバルなシステム上重要な銀行（G-SIB）に対する、より高い損失吸収力要件が含まれる。
- 困難の早期警鐘となりうる耐性測定基準の標準化。2013年7月にバーゼル委員会が公表したリスク・センシティビティ、簡素化および比較可能性のバランスに関するディスカッション・ペーパーの中で提案された指標に基づく。
- 信用リスクの計測に内部の格付け手法を利用する銀行に対して、新しい標準的手法案（以下参照）に従った仮定上の資本要件の開示を求めるかどうか。
- 金融安定理事会が推進する民間部門のイニシアチブであり、銀行のリスク開示を改善するために設立された開示強化タスクフォース（EDTF）からの提言を実施するための最善策。

(ii) 標準的手法の改定

信用リスク、市場リスク、オペレーショナル・リスクを計測するための標準的手法、および「バーゼル1」資本フロアに代わる新たな資本フロアを計測するための標準的手法の改定案（今年の「銀行規制の進化」パート1で概説）により、必要資本の算出に内部モデルを利用する銀行を含むすべての銀行に、これらの新しい標準的手法に基づいた必要資本の算出が求められます。特に信用リスクにおいては、さまざまな信用リスクに対して提案されている新「リスク・ファクター」に関するデータを収集し、適用しなければなりません。これには、法人融資先の収益とレバレッジ比率、住宅ローンに関連したローン担保価値比率と返済能力比率、銀行のカウンターパーティにおける資本の十分性と資産内容に関する比率が含まれます。

(iii) 予想信用損失会計

予想信用損失会計に関するIFRS第9号の実施により、信用リスクに関するデータの収集、分析および監視において新たな要件が課されることになります。

バーゼル委員会は、銀行に対するデータおよびシステム要件を含む、予想信用損失会計に関連した信用リスク管理原則の改定について、コンサルテーション・ペーパーを公表しました。

(iv) ストレステストの実施

欧州銀行監督機構（EBA）や各国当局によるストレステストによって、大手銀行へのデータの要求量はすでに増加しており、また、重要な事業活動とリスクのすべてを反映した各行独自のストレス・シナリオを策定して適用する能力を実証することが求められています。ストレステストがより多くの銀行で実施されるにつれて、さらには、新興国市場リスクのほか、ソブリン債、資金調達および流動性に関するリスクなど、ストレステストの焦点が拡大されるにつれて、こういった要請は増加するでしょう。

例えば、2015年に実施予定のストレステストについてのイングランド銀行による発表には、焦点の推移が如実に表れています。この発表によれば、国内での動揺ではなくグローバルなリスク（中国やユーロ圏の景気減速）に、インフレ・ショックではなくデフレに、英国内においては個人ではなく法人に対するリスクに、より焦点を当てたストレス・シナリオを用いるとしています。イングランド銀行はさらに、信用スプレッドと株価に与える影響だけでなく、市場の流動性のさらなる低下やカウンターパーティの倒産による影響など、より厳格で複雑なトレーディング・リスク・シナリオを適用するとしています。

(v) 流動性

銀行の資金調達と流動性、各行特有のストレスや市場全体のストレスに対する感応度について、監督当局は銀行による詳細なデータを求めています。これは、ストレステストにおける資金調達と流動性の重要性の高まり、2015年1月に導入された流動性カバレッジ比率、2018年1月に導入予定の安定調達比率、「第2の柱」の評価における監督当局の流動性重視の姿勢からくるものです。

(vi) 破綻処理

破綻処理当局が破綻処理計画を策定する際に必要となる銀行の重要な機能、重要な共同利用サービス、法的構造および事業構造についての広範な情報の要請に加え、一部の破綻処理当局では、破綻処理開始時点での破綻銀行の価値を評価できることの必要性をより重視するようになっています。これによって銀行には、破綻時に利用可能な価値評価手法を策定し適用することによって破綻への備えを高めることが求められる可能性があります。

(vii) 融資の代替チャネル

マクロ健全性規制当局やその他の当局が「シャドー・バンキング」への監視体制を整えるにつれ、融資の代替チャネルに対するリスクに関するデータ報告要請が増えることが考えられます。

(viii) 税務

税務面では、外国口座税務コンプライアンス法（FATCA）を遵守するため、大量の顧客データを米内国歳入庁に報告しなければなりません（第1回目の報告期限は2015年5月31日）。さらには税務当局間でより多くの情報を共有することを目的とした共通報告基準（12ページの囲み記事参照）の規定により、ますます多くの非居住者顧客情報を各国の税務当局に報告することが求められます。これは、マネーロンダリング防止（AML）およびテロ資金供与防止に関連した「本人確認」情報の保管および報告が一層求められていることに加えての追加措置となります。

共通報告基準

50を超える国々が、金融口座情報の自動的交換の基盤となる、報告およびデューデリジェンス基準が盛り込まれた「共通報告およびデューデリジェンス基準（CRS）」に調印しました。

CRSにおいて銀行その他の金融機関は、税務上非居住者である顧客に関する金融データを自国の税務当局に報告することが求められます。各国の税務当局はそのデータを当該非居住者の居住国の税務当局に送付し、居住国の税務当局は、当該顧客の金融資産から発生した所得が正しく課税されているかどうかを確認できるようになります。

特定の種類の年金ファンドなど、一部例外があるものの、ほとんどの顧客の金融口座および取引が対象となります。報告対象となる口座には、個人および法人が保有する口座が含まれます（信託や財団を含む。CRSでは資産運用による所得を主とする受動的事業体を調査し、当該事業体を最終的に支配する個人について報告することが求められる）。CRSにはさらに、報告可能な口座を特定するために金融機関が従わなければならないデューデリジェンス手続が規定されています。

報告可能な金融口座に関して報告されるべき金融情報にはあらゆる種類の投資利益（金利、配当金、特定の保険契約による利益、その他同種の利益など）が含まれ、口座残高や金融資産の売却代金も対象となります。

したがって、銀行は以下を実施する必要があります。

- 新規顧客については税務上の居住国を確認し（多くの国では2016年1月から）、既存顧客については既保有情報から税務上の居住国を特定することで、対象となる顧客を特定する。
- 信託その他の同様の契約によって利益を得る報告対象顧客を特定する。
- 対象となる口座を特定する。
- 必要なデータを所定の様式に基づいて各国の税務当局に報告する。

情報の自動交換－共通報告基準
Automatic Exchange of Information –The Common Reporting Standard

EUの基準とイニシアチブ

(i) トレーディングおよび取引報告

2017年1月から欧州金融商品市場規制（MiFIR）と第2次金融商品市場指令（MiFID2）が施行され、銀行に対するトレーディングおよび取引の報告要件が格段に増加します。大枠としてMiFIRでは、以前の第1次金融商品市場指令（MiFID1）の範囲を拡大し、以下を網羅します。

- ほぼすべての金融商品（MiFID1で定められた株式および証券取引所で取引される一部デリバティブからの拡大）
- 取引場所の拡大（MiFID1を拡大し、各種の組織的取引施設も含める）
- EU企業がEU域外に設置している支店
- 各取引についてデータ・フィールドを3倍に増加（MiFID1を拡大し、法人の識別子、クライアントおよびエンド・クライアント両方の本人確認情報、取引成立時刻、投資を決定し実施したトレーダーおよびアルゴリズム、空売り、コモディティ・デリバティブ、権利放棄を示す報告フラグ、も含める）
- データ保管要件（MiFID1を拡大し、取引だけでなく発注を網羅）

一方でMiFIRでは、報告とデータ様式を標準化することにより、事業者による総合的なデータ・テープの作成をより容易にすることが模索されています。

欧州証券市場監督機構（ESMA）は、MiFIRの下での技術的基準の策定を続けています。しかしながら、欧州委員会とESMAが、MiFIR内に存在する重複や不一致、MiFIRとその他の一連の要件との間にある重複や不一致のすべてを解決できるかどうかは不透明なままです。

その他の一連の要件には、欧州市場基盤規制（EMIR）に規定されたデリバティブ取引の報告、証券金融取引（SFT）の報告（以下参照）、卸エネルギー市場の健全性と透明性に関するEU規則（REMIT）に規定された卸エネルギー取引に関する報告などがあります。

英国で実施された取引報告では、銀行にとって正確な報告が困難であることが示唆され、結果として数々の執行措置が取られました。取引報告ミスに対する英国での課徴金の最高額は、2015年4月にメリルリンチ・インターナショナルに課された1,330万英ポンドで、2007年から2014年までの間の12万1,000件の取引報告漏れと3,500万件の不正確な報告に対するものでした。ESMAは、ミスの減少につながると考えられる取引報告のテンプレートおよびプロトコルを策定する意向を示しています。

(ii) 証券金融取引

証券金融取引（SFT）の報告に関するEU規則案では、取引のカウンターパーティに対し、取引翌日までに当該取引をESMAに登録された取引情報貯蓄機関に報告し、少なくとも取引後10年はSFTの記録を保管することが求められます。カウンターパーティには、EU内で設立された金融機関、当該金融機関の世界中のすべての支店、EU以外で設立された金融機関（SFTをEU域内の支店を通して実行する場合）が含まれます。

(iii) 監督評価

EBAは複数の領域で銀行による追加の規制報告を求めています。これには、監督レビューおよび評価プロセスに関するEBAのガイドラインに記載された、各リスク領域に関連する四半期毎の指標が含まれます。

(iv) 外部保証

監督機関は規制報告の正確性や信頼性に懸念を抱き続けており、これが何らかの形での外部保証をさらに重視する姿勢につながっています。ドイツ、オランダ、スペイン、スイスなどでは、外部保証に関する要件がすでに存在します。英国では、健全性規制機構がイングランド・ウェールズ勅許会計士協会（ICAEW）を通して、さらなる外部保証の選択肢を検討するよう会計専門家に依頼しました。この分野では多くの銀行がさらなる措置の必要性を認めており、現在は規制報告を完成させるために複数のシステムや手作業による調整に依存し過ぎていることを認識しています。しかし、現状を踏まえたうえでの最も適切な方法については、外部保証、内部監査、上級経営陣による保証など、見解が分かれています。

(v) 資本市場同盟

EUにおける資本市場同盟（CMU）の設立により、銀行には新たなデータや報告が求められることになるでしょう。これには、シンプルで質の高い証券化商品を裏付けるためのデータの収集、集計および報告や、他行や銀行以外の融資チャネルからの中小企業による資金調達を支援することを目的とした、中小企業に関するデータの収集および提供が含まれます。

ECBイニシアチブ

(i) 財務報告

欧州中央銀行（ECB）は、銀行同盟に参加するすべての銀行および銀行グループのための比較可能な財務報告システムを開発しています。これは、IFRS連結財務諸表を作成する親会社に求められる財務報告フレームワーク（FINREP）に基づく報告による財務情報の提供要件を、さらに幅広いグループや大規模な個別銀行に拡大することによって達成されるものです。さらに、規模の小さい銀行や銀行グループには、簡素化されたFINREPの報告が求められ、これによってFINREPの何らかのバージョンが、銀行同盟に参加するすべての銀行（ECBが直接監督する銀行だけでなく）に拡大適用されることになります（共通報告フレームワーク（COREP）に基づく報告が免除されている銀行を除く）。一部の銀行にとっては、これによって財務報告要件が格段に増加することになります。

IFRSが適用されない主要グループに対するFINREPの完全報告の拡大は2015年末から開始されます。簡素化されたFINREPの導入は、規模が小さく「重要性の高い」グループおよび個別行に対しては2016年6月から、「重要性の低い」グループおよび個別行に対しては2017年6月から実施されます。

(ii) 融資データ

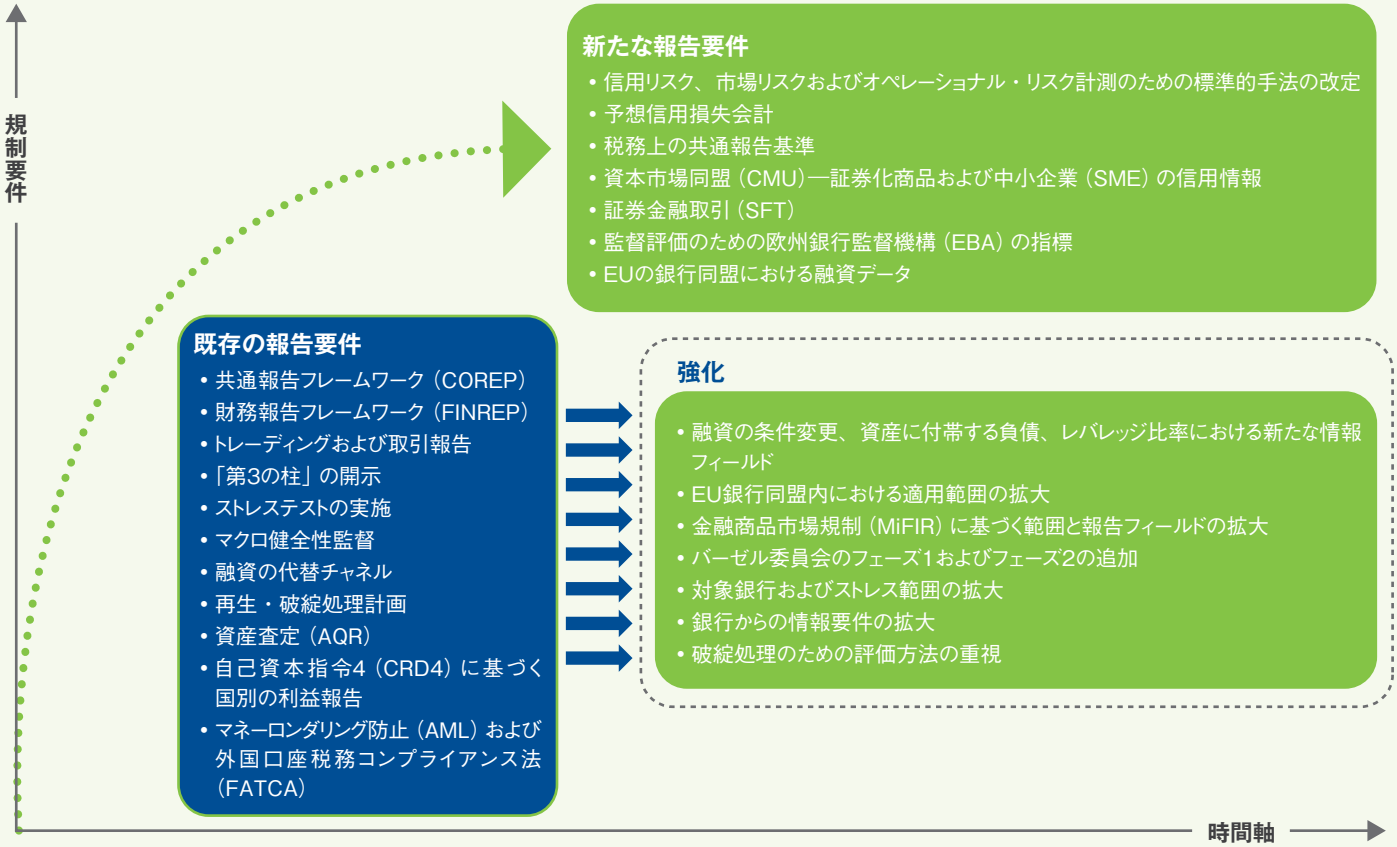
欧州中央銀行（ECB）はさらに、銀行同盟に参加する銀行から、詳細な融資情報を収集し分析することを計画しています。個々の融資について、約100の属性を網羅する精度の高い情報が収集され、報告の対象外となる融資を判断する基準値は低く設定されることが予想されています。その目指すところは、各国の信用データベースをこれらの情報で置き換えることで、2017年から段階的に実施される見込みです。

ECBではこれらの融資データの処理および分析のため、複雑なインフラである「アナクレジット（AnaCredit:Analytical Credit Dataset）」に投資しており、分析結果をECBの全体的な統計データ、個別行に対するミクロレベルでの監督、金融の安定を脅かすリスクに対するマクロ健全性分析に役立てようとしています。

ミクロレベルでは、このデータによって銀行の透明性を高め、より包括的な分析と一貫性チェックが可能になり、昨年の資産査定（AQR）で実施された分析を補足および拡充することになります。またこのデータによって、銀行のビジネスモデルや中小企業（SME）に対する融資承認の確認といった分野での、より詳細な分析が可能になります。

> 欧州中央銀行（ECB）はさらに、銀行同盟に参加する銀行から、詳細な融資情報を収集し分析することを計画しています。

規制報告



出典：KPMGインターナショナル、2015年

リスクデータ集計およびリスク報告

内部目的においても、監督当局からの情報要件を満たす目的においても、大手銀行が規制対象法人およびグループレベルでリスクを迅速かつ正確に集計できないことに対する銀行監督当局の苛立ちが、リスクデータ集計およびリスク報告に関するバーゼル委員会原則の策定（2013年1月）につながりました。

これらの原則は以下の内容を網羅しています。

取締役会および上級経営陣が、銀行のリスクデータ集計能力、リスク報告実務、IT能力に対して強力なガバナンスを発揮することの重要性。

- こうした能力およびプロセスの文書化、検証、強靭性
- 平常時とストレス時の両方におけるリスクデータの集計能力とリスク報告実務をサポートする、データ・アーキテクチャおよびITインフラの設計、構築および保守

集計されたリスクデータの正確性、一貫性、完全性、適時性、適合性。

- リスクデータの生成および集計を行うシステムおよび統制の適切性
- 主なリスクおよび規制要件の変化に素早く適応する能力

リスク管理報告書（取締役会や上級経営陣向けを含む）の正確性、包括性、明確性、有益性、発行頻度および配布。

- データの正確性やモデルの信頼性を監視するための手続
- 将来を見据えたリスク評価の有効活用
- 上級経営陣および取締役会向けのリスク管理報告書の有益性のレビュー（特に、適切な情報に基づいてリスクやビジネス上の意思決定をするための情報として）

銀行によるこれらの原則の遵守を監督当局がレビューおよび評価し、必要であれば是正措置を講じ、本国および受入国の監督当局と協力する必要性。

グローバルなシステム上重要な銀行（G-SIB）は2016年までにこの原則を満たすことが期待されています。また、国内のシステム上重要な銀行（D-SIB）は、D-SIBに指定された年から3年以内に満たさなければなりません（この指定は各国の監督当局に任されています）。監督当局は他の銀行に対しても、規模に合わせてこの原則を適用することができます。すでにドイツとイタリアでは、すべての銀行のリスク管理の最低基準に関する法的要件や、年末監査の一部として見なされる領域に、これらの原則が組み込まれています。

一方でG-SIBは、これらの**原則に照らし合わせて自己評価する**という課題に直面しています。バーゼル委員会は、過去2回の自己評価の結果について報告書を公表しています（2013年12月と2015年1月）。**2回目の自己評価報告では、ほぼ半数のG-SIBが、2016年の期限までに諸原則を完全に遵守することはできないだろうと報告しています。**確かに、2013年と2014年の自己評価において諸原則全体での平均評価はわずかしか改善されていません。この理由の一部としては、一部の銀行で大規模なITインフラ・プロジェクトの開始または実施が遅れたことが挙げられます。これによって、諸原則の遵守を優先することに対するG-SIBへの監督圧力が必然的に高まることになります。

データ集計に関して最も遵守率が低いと報告された原則は、データ・アーキテクチャとITインフラ、データの正確性と一貫性、および適合性の3つでした。半数近くのG-SIBがこれらの原則の重大な不遵守を報告しているほか、多くが強固なデータ集計プロセスの確立に苦労しており、それゆえ、膨大な手作業で急場をしのぐといった手段に頼らざるを得なかったと報告しています。銀行はさらに、自行のITインフラは平常時には適切だが、ストレス下では適切でなくなる可能性があるとも回答しました。

データ・ガバナンスに関して銀行によって特定された弱点のうち最も共通していたのは、銀行全体でガバナンスの枠組みを改善する必要性、そしてリスクデータ集計およびリスク報告に関連した複数の大規模なプロジェクトを管理する必要性に関するものでした。

一方、遵守率が最も高いと銀行が自己評価したのは、**リスクデータの報告**に関する原則、すなわち、報告書の配布および報告書の包括性、明確性、有益性でした。しかしながらバーゼル委員会では、リスク報告書に盛り込まれたデータや作成プロセスに重大な欠陥がある場合、その報告書にどれほどの信頼性と有益性があるのかという点に疑問を呈しました。

バーゼル委員会は、銀行は特に以下の事項を実施する必要があると結論付けました。

- **リスク関連のITシステムおよびガバナンス体制を大幅に改善する。**特に、正式かつ文書化されたリスクデータ集計の枠組み、全グループ企業が一貫して使用する包括的なデータ辞書、データ品質統制を管理する包括的な方針、データライフサイクルの各段階における統制に重点を置く。
- 手作業への依存度を下げ、リスクデータの品質チェックを、会計データを裏付けるチェックと同様に強固なものにすることにより、**リスクデータの正確性、完全性、適時性、適合性**を改善する。
- 内外のリスク報告要件の変化に対応するため、関連データを**適時**に生成する。

さらにバーゼル委員会は、諸原則の完全遵守に近付くためのG-SIBの進捗について**綿密な監督を継続する**意向を表明しました。これには、この課題に関して監督当局が銀行の上級経営陣、取締役会および内部監査に、より密に関与し、ITアーキテクチャ・プロジェクトの進行、手作業に依存したシステムの利用の低減および品質管理に関する銀行の進捗をより慎重に監視する必要性が含まれます。

バーゼル委員会は、2016年の期限に向けたG-SIBの進捗の監視を継続することになります。

銀行に対する商業的圧力

銀行への圧力は、規制改革のみによって生じるのではありません。「銀行規制の進化パート2」で述べたように、銀行は、現在および将来の景気動向、銀行業界における過剰能力、新規参入銀行の出現、収益性の高い銀行事業活動分野への参入を模索する銀行以外の金融機関（ノンバンク）などからの、数々の商業的圧力に直面しています。

実行可能かつ持続可能な戦略やビジネスモデルを構築しようとする銀行の試みにとって、データとテクノロジーは必要不可欠な重要要素になりました。これには以下の6つの主要要素が存在します。

- **顧客経験の改善**
- **テクノロジーの進歩の活用**
- **「デジタル・ディスラプター（デジタル化による創造的破壊者）」を含む競合他社への備え**
- **リスク管理能力の強化**
- **コストベースの引き下げ**
- **サイバー犯罪リスクへの対応**

データをより効果的に活用する

銀行がリテール市場とホールセール市場の両方において信用と信頼を再構築し、収益や利益を高めていこうとするうえで、顧客経験の改善は重要な要素です。ここでは、データ、データ分析、テクノロジーのすべてが重要な役割を担います。

銀行は**膨大な量のデータ**を持っていますが、そうしたデータは通常、相互にまたは中央データ処理センターと効果的に情報交換されていない複数の場所に、さまざまな形式で保管されています。データセットに互換性や一貫性がなければ、データ集計や照合に一層の時間と労力を要します。その結果、多くの銀行では、顧客データを集約して活用し、強固で効果的なオペレーション・システムに基づいて顧客を一元的に見ることが難しくなっています。

そのため、こうした銀行では、顧客と効果的につながることや、収益性の高いビジネス領域を特定すること、簡素化を促進することが難しくなる可能性があります。

実際、銀行と顧客の距離は開きつつあるようです。他業界での企業体験により、顧客の期待値が高まっていることを考えると、その開きは特に顕著です。他業界では、技術的進歩を有効活用して、銀行よりも顧客に関する理解を深め、顧客との効果的なコミュニケーションを実施しています。

データが完全にアクセス可能になれば、銀行は以下において分析ツールを利用できる

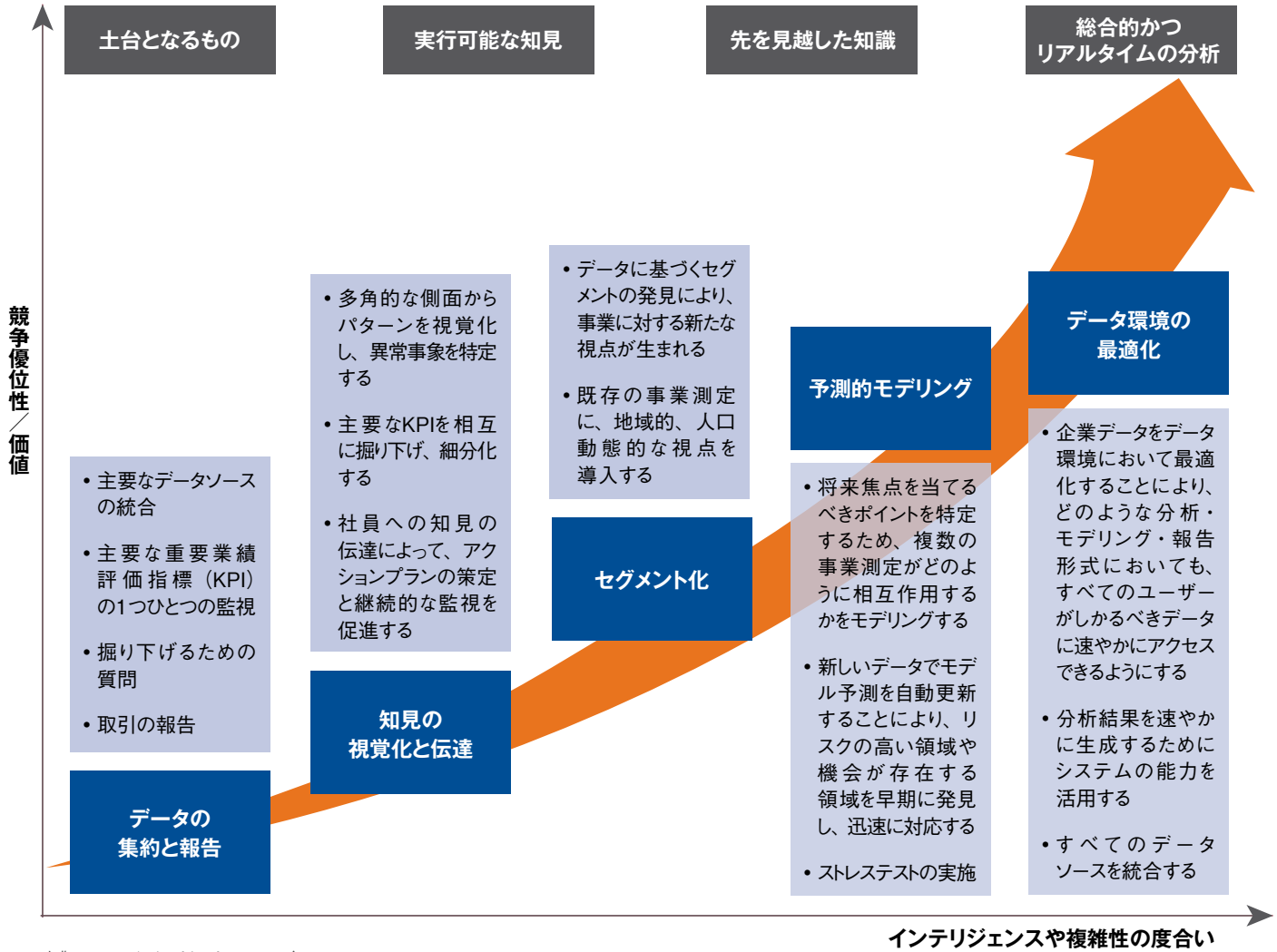
- 顧客のニーズを理解する
- 顧客の行動をモデル化する
- 商品やサービスを充実させ、顧客のニーズに合わせてカスタマイズする
- 顧客基盤をセグメント化する（例えば、購買パターン、収益性、人口動態、リスクに対する姿勢に基づいて）
- 顧客に合った商品の提案を行う
- 営業手法をカスタマイズする
- 顧客、商品、法人、営業地域、部門全体における収益機会を特定する
- 出現しつつあるトレンドや課題を特定する
- ストレステストの実施能力を強化する
- トレーダーの行動を監視して、不正な取引その他の疑わしい活動を発見する
- 重要業績評価指標（KPI）やその他の管理情報を改善する
- データの取込みおよび報告方法における異常事象を特定する

この領域での銀行による解決策の1つに、**データ分析**をより効果的に活用することが挙げられます。銀行は、自行のデータからより高い価値を引き出すことで、顧客重視の姿勢を高め、他の銀行や、銀行市場にすでに出現しているか、今後出現する可能性のある新規参入企業に対する競争力を維持する必要があります。ここでの真の競争優位性は、顧客や市場についてのすべてのデータソースをうまく統合し分析することから生まれます。

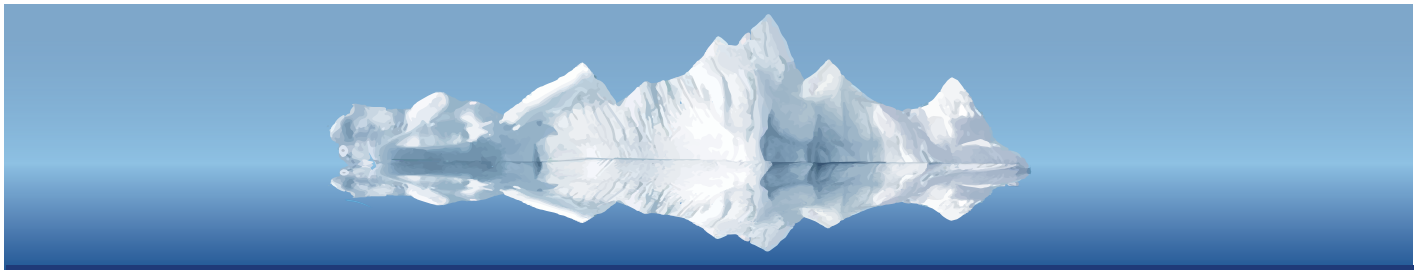
さらに銀行は、銀行経営において、どのようなデータを利用しているべきかを検討する必要があります。銀行と規制当局の双方ともに、リスク・ガバナンスの改善を重視しているにもかかわらず、資本、流動性計画およびリスク管理における内部モデルに基づいたアプローチと、改定後の標準的手法、レバレッジ比率およびストレステストの結果に基づいた規制当局からの要求との間の隔たりは、規制によって大きくなっています。

資本、流動性計画およびリスク管理における内部モデルに基づいたアプローチと、改定後の標準的手法、レバレッジ比率およびストレステストの結果に基づいた規制当局からの要求との間の隔たりは、規制によって大きくなっています。

データ分析の成熟度カーブ



出典：KPMGインターナショナル、2015年



貴行のIT氷山の下に、どれほどのものが隠されているでしょうか?

IT氷山とは?

パッチワーク状のIT
旧態依然とした
ITシステムと賛否両論
のあるシステム更新

古いプログラミング
何十年にもわたって
書き加えられてきた数々の
プログラミング規則の積み重ね

自動的なITシステム
人的な介入や監視を
必要とせずに取引を処理し、
取引明細書を発行する

「企業記憶」の喪失
IT開発担当者の退職後は、
コーディングを変更したり、新しい
システムとの互換性を持たせたりする
ための方法を知る者がいない

KPMGがIT氷山を主な課題とする理由

最近のKPMGによる分析[2]では、**旧態依然としたITシステム**を原因とした問題が、金融サービス業界においてパターン化していることが示された

金融機関はこの問題を認識しているが、「分析マヒ」に陥っていて、解決方法が分からない

この状態が貴行に与え得る影響とは?

成功
テクノロジーが
将来における
事業の成功を
導く

競争
柔軟性がなく、
データ・インテリジェンスを
競争優位性として
活用していない

評判
評判の失墜

罰則
将来の罰金
および監視リスク

顧客
顧客の信頼を失うことが、
大規模な払戻しなどの
業界におけるより大きな
影響につながる

過去を捨て去りましょう

ITシステムの改善

将来のビジネスモデル
慣行に備える

データ分析とインテリジェンスに
基づいた意思決定を
可能にする

課題にとらわれていた時代と
将来の罰金の可能性に
けりをつける

リスクの軽減をやめ、
その代わりに将来の成長と優れた
経済性に向けた投資を行う

古い課題を過去のものとする

出典:KPMG英国、2015年 http://www.kpmg.com/uk/en/issuesandinsights/articlespublications/pages/what-is-hidden-beneath-your-it-iceberg.aspx

2 KPMG英国、2015年

データおよびデータ処理が高品質であることによって、銀行には**リスク管理を改善する機会**も生まれます。

- リスクデータ集計およびリスク報告に対するバーゼル委員会の焦点は、主に銀行の資本と流動性に対する健全性リスクに当てられてきたが、ビジネス・コンダクト（事業行為）に関しても同様の課題が生じている。類似する商品の販売や取引に関するデータが、銀行の各所に異なる形式で保管されている場合、銀行は不適正販売やその他のコンダクト上の不手際を効果的に特定および対処できない可能性がある。
- データおよび管理情報によって、事業実績やリスク管理に関する個人の説明責任を支援できる。これは、個人の責任に関連する結果をはっきりと区別できるからである。
- 自動化された高性能システムを導入することで、マネーロンダリング防止（AML）、租税、取引に関する多数の懸念に対し、少なくとも部分的なソリューションを提供できるほか、コンプライアンス監視を変革する余地が生まれる可能性がある。

テクノロジー：断片化から次世代へ

たとえ銀行がデータをより重視し、データ分析への投資を増やし始めたとしても、多くの銀行は**自行のITシステムやインフラにしばられ**続けるでしょう。こういったシステムやインフラは通常、内容や性質が一様でないうえに断片的に存在しており、老朽化して信頼性も低下しています。急速な拡大、M&A、新規事業への参入というかつての時代に、まったくバラバラの旧型システムをつなぎ合わせてきたことや、複数の開発元（行内開発、海外開発、外部委託）、度重なる増設、急場しのぎ、手作業による介入が反映されていることが原因です。

銀行はこれまでデータやITシステムに多額の資金を投じて維持してきました。複数のシステムを取り除く作業に進展も見られますが、道のりはいまだ長く残っています。上級経営陣の多くは、自行のデータおよびシステムによる制約を受けるために、組織内で柔軟性が失われ、変革ペースが遅れてしまうことに対し、引き続き苛立ちを覚えています。

多くの銀行ではITインフラが完全に持続不可能になる前に、早急かつ多額の投資を伴う対策が必要です。自動化と革新を促進できるようにすることは言うまでもなく、銀行がターゲットとする販売チャネルを効果的にサポートし、データやテクノロジーを競争上の主要な差別化要因として活用でき、効果的なサイバー・セキュリティ耐性を達成できなければなりません。

したがって多くの銀行では、**ITシステムやインフラを根本的に見直し**、単にテクノロジーによって支えられた銀行ではなく、テクノロジーを主体とした銀行になるにはどのようにすべきかをしっかりと考える必要があります。旧態依然としたシステムは、**単一のストラクチャおよびオペレーティングモデル**で置き換えなければなりません。その際は、内部データ管理、外部報告、革新および自動化を促進し、機動的かつ堅牢で耐性を備え、払戻し・顧客・融資・リスクといったすべてのチャネルにおいて、明確かつ一貫性のある方法で利用される中核的なプラットフォームとなる、標準化されたシンプルなアプローチを重視しなければなりません。

> 規制報告およびリスク管理要件が、すでにその他のテクノロジーやデータプロジェクトを締め出しつつあります。

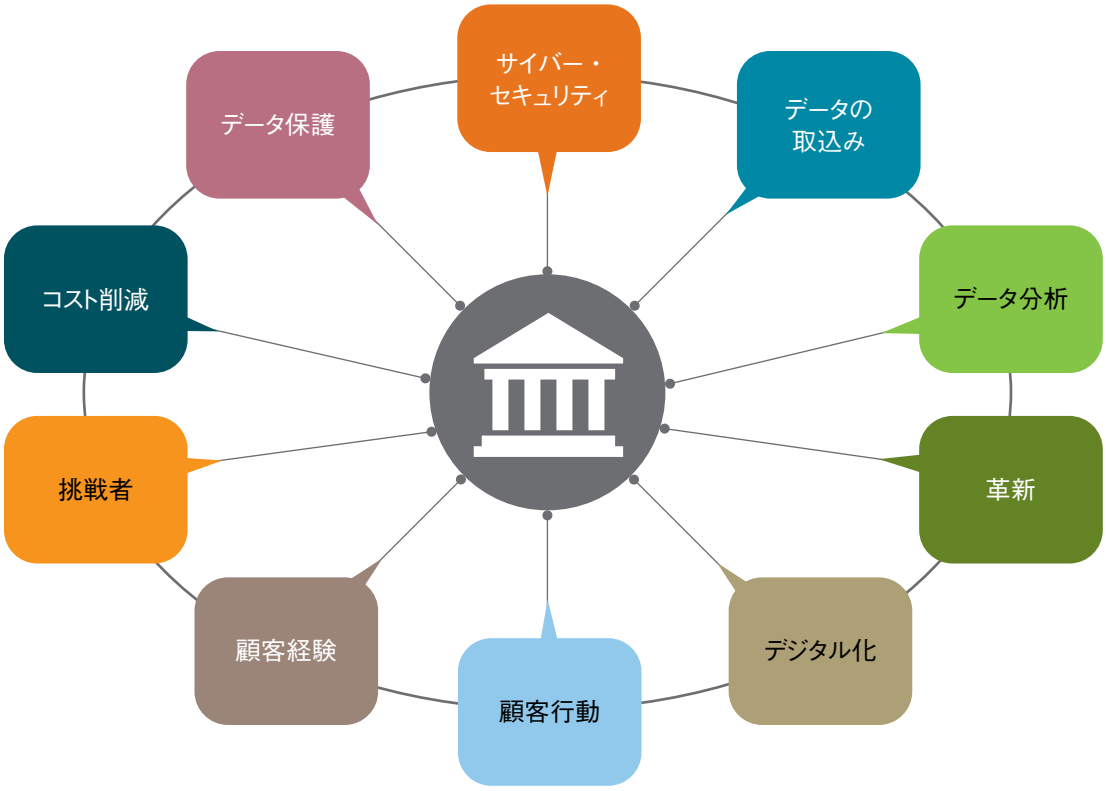
一方で、テクノロジーの進歩を利用することで、銀行は以下のように**コストを削減**できる可能性があります。

- オペレーションを合理化し、経費を削減し、効率性を高める。テクノロジーやデータ管理をスケールアップし、事業活動や事業基盤全体に拡大できる場合は、特に効果が期待できる。
- オペレーションの簡素化、標準化および統合を目的としてプロセスの組織化を進めることにより、複雑さを軽減し、顧客サービスを強化する。
- 粗悪なデータおよびITシステムから最終的に生じる財務上、規制上および評判上のコストを削減する。これは特に、粗悪なデータおよびITシステムが、稚拙な意思決定や不適切な行動を引き起こすためである。

しかしここで銀行は、以下のような**困難な選択を迫られます**。

- 銀行の収益性が低下し、コスト削減圧力が強い時期に、こうしたテクノロジー・プロジェクトの先行費用が生じる。
- その他の規制イニシアチブ（欧州の大規模な銀行グループに対する規制要件、法人の合理化、中間持株会社を設立し、包括的資本分析（CCAR）に参加するという米国での要件達成を含む）を満たすためのコストや実務に加え、規制報告およびリスク管理要件が、すでにその他のテクノロジーやデータプロジェクトを締め出しつつある。
- 銀行は、どの程度の変更を実施し、どの程度の欠陥に対処すべきかを決定する必要があるが、完璧を求めるとコストが便益を上回る恐れもある。

銀行のデータやテクノロジーに対する商業的圧力



課題：新たなチャネルと新たな競争相手

銀行の顧客の行動は変化しつつあります。銀行の支店などの既存の物理的なチャネルやインターネット・バンキングといったすでにあるデジタル・チャネルの継続した利用に並行して、多様な新しいデジタル・チャネルやアプリケーションの利用が増えています。新しい決済チャネルや、さらにはビットコインといった新しい通貨でさえも利用されているのです。

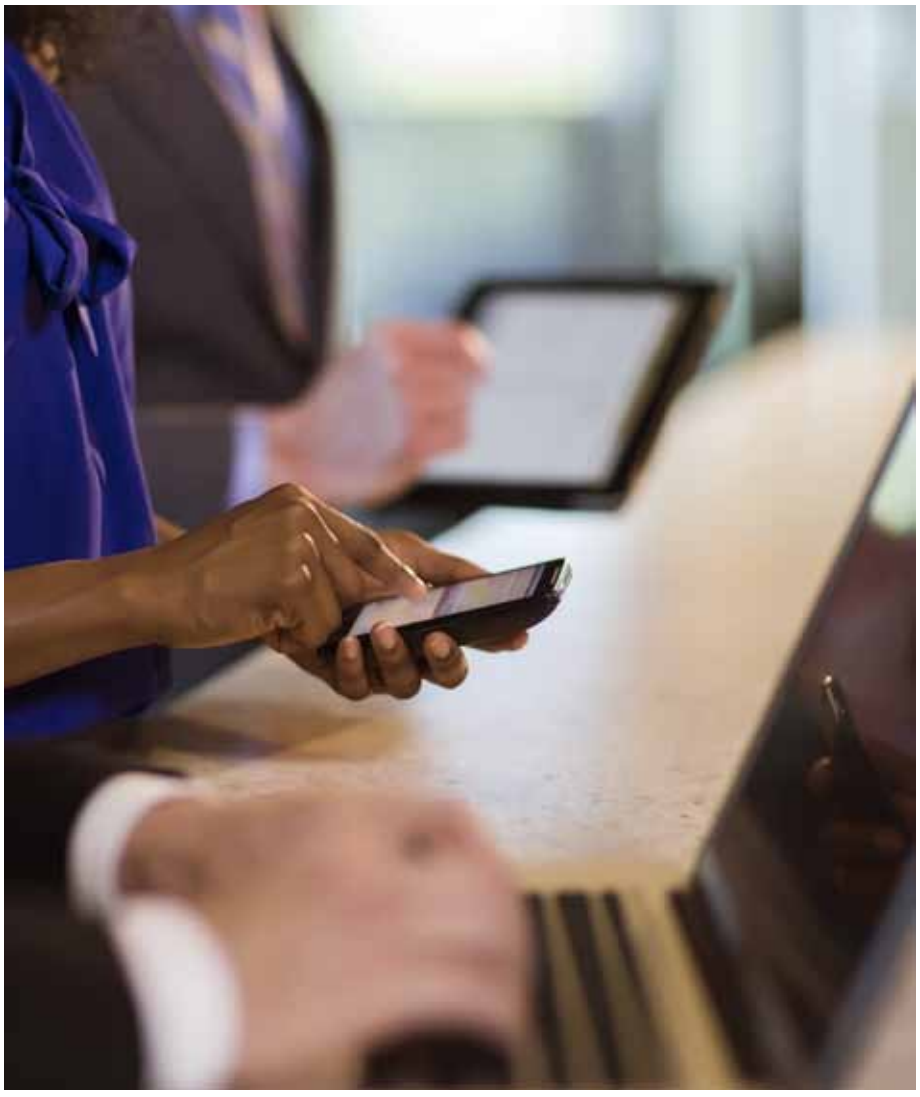
銀行は、この動きへの対応を選択する必要があります。顧客との対面でのやり取りという面で、支店にはいまだ潜在的な価値があることを認識したうえで、支店とデジタル・チャネルのバランスをどうするか、また、デジタル環境においては、利用可能なすべてのチャネルを通して顧客サービスを提供するか、またはより狭い範囲に特化するかという選択肢があります。

しかし、銀行がこの領域のどこに身を置いても、顧客の要望は、銀行との接触方法に関わらず、シームレスに統合された同一のサービスを受けることにあります。顧客は、これらの新たなチャネルが、銀行以外の金融機関（ノンバンク）の優れたデジタル・チャネルと同じように、迅速で効率的、かつ途切れることなく作動することを期待しています。

銀行は、多くの既存銀行が抱える厄介な「過去の遺産」を持たない**新規参入銀行からの挑戦**、さらにはさまざまなチャネルを通じて高水準の顧客サービスを提供する一部の従来の銀行からの挑戦に直面しています。これらの挑戦者は、データやテクノロジーの効果的な利用に裏打ちされた、より顧客重視のアプローチによって競争していこうと模索しています。

さらに銀行は、よりシンプルかつ標準化された（知識集約型ではない）金融サービスで市場への参入を模索する、**テクノロジーを主体とした銀行以外のサービス提供企業からの挑戦**にも直面しています。この市場には、既存の銀行が高い利益を上げているか、比較的非効率である部分、または十分に高水準な顧客サービスを提供していない部分に、テクノロジーやデータ処理を活用する機会があります。これはしばしば「デジタル・ディスラプション（デジタル化による創造的破壊）」と呼ばれ、実際はこうした挑戦のすべてがデジタルを主体としたものではありませんが、革新に向けた新たな動きであることは紛れもない事実です。こういったよりシンプルかつ標準化されたサービスには、以下のようなものがあります。

- デジタル決済ソリューション―現金やカードを必要としない、携帯電話やその他の電子財布による決済など
- デジタル・インフォメーション・サービス
- 決済処理―顧客取引手数料、加盟店手数料および金利負担のない預り金によって巨額の利益を生み出し、顧客による購買や送金に関する価値ある情報ソースとなり得る、巨大な産業
- 自動融資―中小企業に対するP2P融資（ソーシャル・レンディング）などで、個人だけでなく機関投資家からの投資が増えている
- デジタル通貨
- 自動推奨サービスや自動証券取引サービス



銀行はまた、既存の強固な顧客関係、顧客に関する詳細なデータ、総合的な商品およびサービスの提供の活用を模索することも可能です。

これらの挑戦は、まず一部の事業活動の収益性を少しずつ侵食することにより、さらには一部のサービスの主要提供企業として銀行に取って代わる可能性があることにより、既存の銀行にとっては明らかに脅威となります。

しかしここでも、**既存の銀行にとっての機会が存在します**。銀行は、テクノロジーの変化において先駆者となる必要はありません。成功を収めている新テクノロジーを真似したり、アレンジしたりすることもできます。

例えば銀行は、銀行業務を提供するだけでなく、ソーシャルメディアなどの新しいチャネルを利用して、既存顧客や新規の顧客とのつながりを改善できます。また、イノベーションやテクノロジーの進歩を活用して、顧客サービスを強化できます。多くの銀行ではすでにデジタル・サービスを改善し、複数のチャネルにわたって、より途切れることのない顧客体験を提供しています。声や生体認証に基づく顧客認証や、クレジットカードおよびデビットカードの顧客管理の向上、代替となるデジタル口座やデジタル通貨の提供において初期段階にある銀行もあります。また、例えばプライベートバンキングや資産管理におけるデジタル・チャネルを通じて、より幅広い顧客にデジタル化による各種メリットを提供しようと模索している銀行もあります。

さらに銀行は、顧客満足度、信頼およびロイヤリティの再構築プロセスの一環として、新しいデジタル・チャネルを活用できる可能性があります。銀行は一般に、セキュリティ侵害に関する分野では、決済サービスにおける主要な競合企業の一部よりも競争優位性を有しています。確かに、銀行に対する信頼が全般に欠如し、データに対するオーナーシップ、セキュリティおよび機密性に対して顧客が懸念を抱いているにもかかわらず、個人客はデジタル・サービスの提供に関して、銀行以外の金融機関（ノンバンク）よりも銀行を信頼しているように見受けられます。

銀行はまた、既存の強固な顧客関係、顧客に関する詳細なデータ、総合的な商品およびサービスの提供を活用することも可能です。新規参入銀行は、事業をニッチな領域に限定していることが少なくありません。銀行以外の新規参入企業の多くは、銀行として規制される可能性のある商品やサービスを取り扱わないことにこだわります。銀行は、銀行独自の「マーケットプレイス・レンディング」プラットフォームを構築し、融資先候補についてのソーシャル・ネットワークその他のデジタル情報ソースを、既存の信用リスク評価プロセスに統合させることができます。

変わりつつあるマネーの世界
The changing world of money

ゲーム・チェンジャー―変革者
The game changers

顧客体験：驚くべき結果

金融セクター（銀行、生命保険、損害保険、公益、eリテール企業）に属する5ヵ国160の企業における顧客経験について、消費者5,000人を対象としてKPMGインターナショナルが2013年後半に実施した調査では、以下が明らかになりました。

- 顧客体験のスコアが最も高いのはeリテール企業。
- 銀行は顧客満足度で2位となり、損害保険、生命保険、公益を上回った。銀行は、顧客の期待に応えるという点で、業務上の卓越性、セキュリティ、テクノロジーに投資してきており、この点で最高の得点を上げた。銀行の中でも、オーストラリアとドイツの銀行の得点が高かった一方で、英国の銀行は米国や中国を下回り、一番低い得点となった。
- 銀行の顧客が最も重視していたのは、費用対効果（預金や貯蓄の低利回り時に調査したことがその理由の一部であると考えられる）や、誠実かつ信頼できるスタッフとのやり取りだった。ここからは、銀行は顧客体験の改善に向けて、テクノロジーやデジタル・サービスのみに投資を限定すべきではないことがうかがえる。
- 費用対効果とスタッフの2点を最も重要であるとした銀行顧客の評価と、この2つの領域における銀行の現実には大きな隔たりがあった。

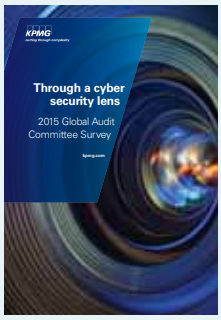
顧客体験のバロメーター
Customer Experience Barometer

一方で、**規制当局には規制当局の懸念があり**、それが銀行の戦略的選択を複雑なものにしています。

決済サービス企業やP2P融資（ソーシャル・レンディング）企業など、銀行業界への新規参入企業に対する規制上の分類において、各国の規制当局のアプローチはすでに異なっており、一部の国ではこれらの新規参入企業を、電子マネー取扱機関や融資プラットフォームではなく、銀行として規制しようとしています。新規参入企業が規制の対象となれば、既存の銀行にする競争優位性の少なくとも一部が損なわれることになります。

銀行がデータやテクノロジーを利用して商品やサービスの不適切な抱き合わせ販売や営業をする可能性に対する懸念（適切な商品やサービスによって顧客に適切にサービスを提供していると規制当局が考えるものではなく）、顧客データのセキュリティや機密性に対する懸念、銀行のデータ・システムやデータ・モデリングの適切性に対する懸念にも、各国の規制当局によって違いがあるようです。

各国の規制当局はまた、口座へのアクセスや本人確認目的でのデジタル認証、個人や企業についての信用調査情報のオンライン入手可能性の是非に対する各自のアプローチを通して、競争環境に影響を与えることになるでしょう。



サイバー・セキュリティの視点から
Through a cyber security lens

サイバー・セキュリティ

企業が取り組むべき課題において、サイバー・セキュリティ攻撃がもたらすリスクの優先順位は急速に上昇し、特に銀行その他の金融機関ではその重要度が増しています。取締役会、リスク委員会および監査委員会では、より多くの時間をサイバー・セキュリティ・リスクに費やしています。

KPMGによる2015年グローバル監査委員会調査では、調査対象となった世界1,500社のうち16%で、サイバー・セキュリティが3大リスクの1つにランクインしました。監査委員会のメンバーの40%が、サイバー・セキュリティにもっと時間を費やすべきだと回答し、41%がサイバー・セキュリティについて入手する情報を改善する必要があるとの懸念を表明しました。

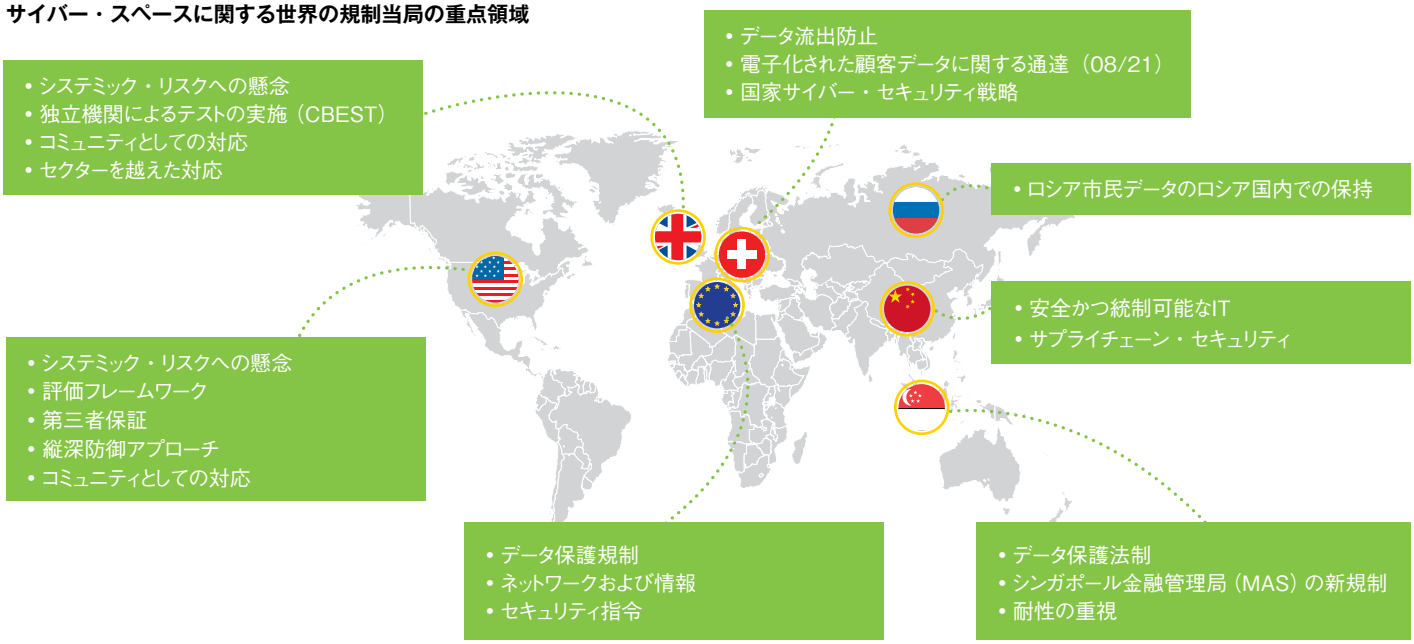
支払や決済システムで銀行が果たす役割の重要さ、慎重に扱うべき顧客情報の保有量、銀行サービスの円滑な機能を妨げることによる悪影響の大きさを考えると、銀行はサイバー攻撃の魅力的なターゲットです。

銀行に対するサイバー攻撃は増加しつつあります。以下は、その一部です。

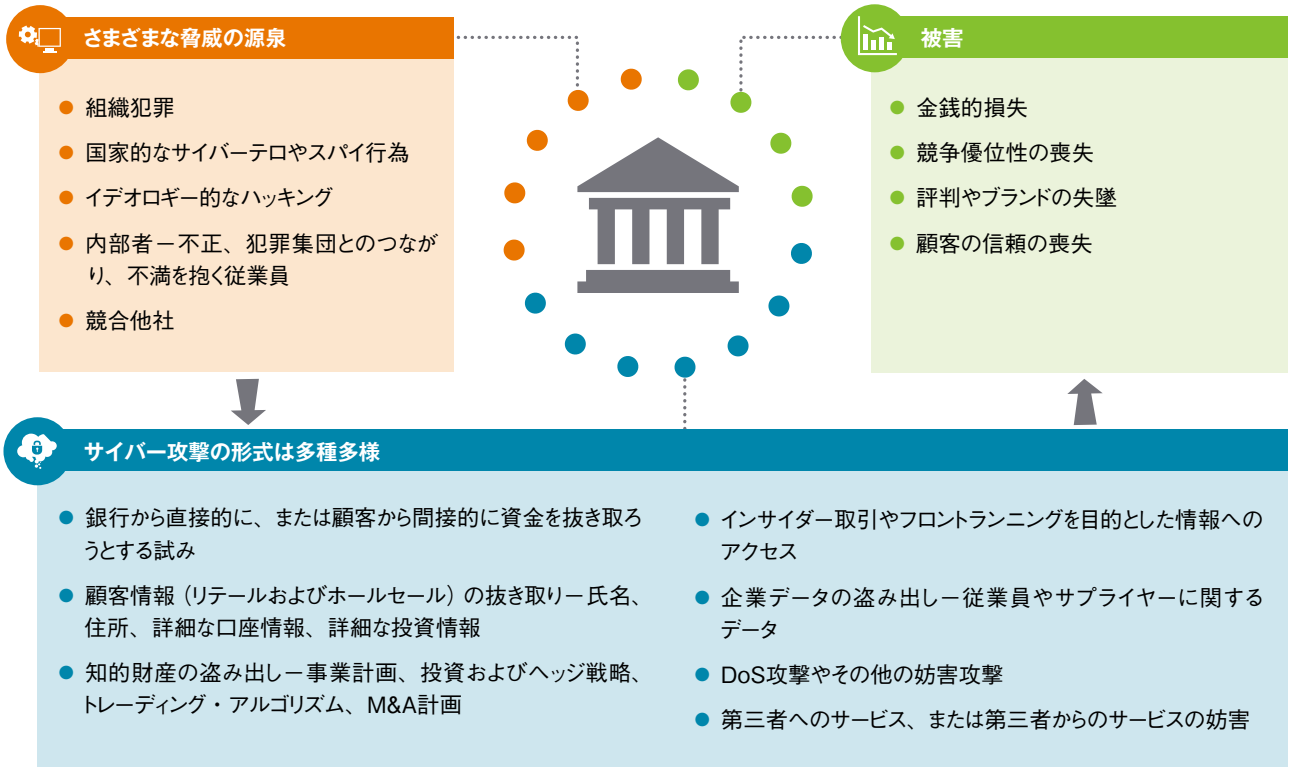
- サービス妨害攻撃（DoS攻撃）。2007年4～5月にエストニアの銀行に対して行われたほか、2012年9月に米国の複数の大手銀行、2012年10月に英国の複数の銀行に対しても行われた。
- 2013～2014年に、銀行の内部システムや統制を対象としてサイバー犯罪集団「カーバナック」が仕掛けた、不正な資金移動を目的とした標的型攻撃。
- 銀行の法人顧客を標的とした「ダイアウルフ」と呼ばれるフィッシング攻撃。
- 2014年8月に米国の大手銀行の1行が、7,600万件の個人データと700万件の小規模企業データがサイバー攻撃によって流出したと発表。顧客の資金に被害は及ばなかったが、一部の口座情報にまでアクセスが及んだ。

一方で、銀行はその効率性と有効性を高めることを目的とした取組みにより、自らをより高いサイバー・セキュリティ・リスクにさらしています。銀行は、コスト削減を目的としてテクノロジーの活用度を高め、顧客サービス改善の一環としてより幅広いアクセス・ルートに自行のITシステムを開放し、顧客についてより多くの情報

サイバー・スペースに関する世界の規制当局の重点領域



銀行に対する脅威の性質



を保有しています（どんどん複雑になる「本人確認」関連の規制要件への対応がその理由の一部）。また、IT分野の開発やITサービス、顧客データ処理および保管、さらには各種内部システム（給与支払い、事務所管理、セキュリティなど）を外部委託するようにもなっています。

サイバー・セキュリティは、規制上の課題、政府の課題としてもその優先度が上がっています。サイバー攻撃発生時の銀行や重要なマーケット・インフラの耐性をテストするための市場全体を対象としたシミュレーション・テストが米国と英国で実施されました。欧州中央銀行（ECB）は、銀行のサイバー・セキュリティへの脅威や予防策に対するテーマ別レビューを実施しています（まずは事実調査を目的として）。各国政府は、自国の利益と、公益企業、銀行およびその他の企業が担っている重要な経済機能の両方に対する脅威について懸念を深めています。

サイバー・セキュリティ―銀行が受ける影響

データやテクノロジーに関するその他の側面と同様、サイバー・セキュリティ対策をうまく進めることによって、銀行はステークホルダーの信用と信頼を維持、改善し、テクノロジーやデータを効率的かつ効果的に管理することが可能になり、競争優位性を得ることができます。

銀行は、主に次の4つの方法で、サイバー・セキュリティ・リスクを軽減させる必要があります。

まず第1に、**サイバー・セキュリティは単にテクノロジーの問題ではない**ことを認識しなければなりません。その他のハイレベルな主要リスクと同様、銀行の取締役会、リスク委員会、監査委員会、そして上級経営陣は、事業リスク管理の観点から、また、事業目的によって銀行

がサイバー・セキュリティへの脅威にどの程度さらされているかの評価、サイバー・セキュリティ・リスクが適切に測定され、適切に管理されていることの確認、脅威に関する情報の特定と収集、サイバー・セキュリティに対処するための既存のシステムや統制の能力評価、脅威に立ち向かうための戦略的・戦術的措置といった観点から、サイバー・セキュリティを優先課題とする必要があります。

第2に、**銀行はサイバー攻撃耐性を高める**必要があります。そのためには、以下の複数の領域に対する投資が必要になります。これは比較的基本的な事項であるように思われますが、効果的な実施が困難かつ複雑である場合があります。

テクノロジー―ファイアウォールやその他のセキュリティ特性を構築し、サイバー攻撃やセキュリティ侵害を監視および発見する。

人材―銀行スタッフのセキュリティに対する自覚（研修と理解）、データやシステムへのアクセスに関するセキュリティ方針、これらの方針の実務上の有効性に関するテストの実施、比較的入手が難しい重要なスキルの確保。

内部プロセス―主な内部プロセスに組み込まれたセキュリティ要件。新市場への参入や新商品およびサービスの開発、新しいテクノロジー（トレーディング・プラットフォーム、インターネット・バンキング、データ・ウェアハウスなど）の活用によってサイバー・セキュリティ・リスクが追加される可能性。

第三者の脆弱性―第三者との契約においては、サプライヤーが講じるセキュリティに対する契約前デューデリジェンスだけでなく、契約後のセキュリティ監査も盛り込むべきである。「サプライチェーン」のすべての箇所において、データの利用、保管および安全面でのセキュリティに問題点がある。銀行はサプライヤーが誰であるかを理解し、サプライヤーが保有しているデータやアクセスしたことのあるデータを把握する必要がある。第三者のサプライヤー、ジョイントベンチャーおよび銀行の顧客も、銀行のデータやシステムにある程度アクセスできることを考えると、周辺を保護するだけでは十分ではない。

脅威情報―サイバー・セキュリティの脅威が日々進化していることに合わせ、最新の情報を入手する。一部の銀行では、これらの脅威の評価、内外でのテストの実施、実施可能な予防的措置の特定を自行内で行えるよう、大規模な投資をしている。

反応度―サイバー・セキュリティ侵害が実際に発生した時の対応のスピードおよび機敏性、教訓からの事後学習とシステムおよび統制の適応、評判維持上の問題への対処。

銀行はすでにサイバー・セキュリティに多額の投資をしています。この投資は、最近までは、重要なインフラ企業による総合的なサイバー・セキュリティ・プログラムの構築に利用するために米国国立標準技術研究所（NIST）が設計した自主基準である、サイバー・セキュリティ・フレームワークを利用した評価に基づいて実施されてきました。

しかしごく最近、このNISTのフレームワークが米国連邦金融機関検査協議会（FFIEC）のサイバー・セキュリティ評価ツールに組み込まれました。この評価ツールは、以下の2つで構成されています。

固有リスク・プロファイルの評価ー企業のテクノロジー、第三者との接続、販売チャネル、商品、組織構造および外部の脅威から生じる固有リスク。

サイバー・セキュリティ成熟度の評価ー企業の慣行、プロセスおよび行動が、以下の5つの領域においてサイバー・セキュリティへの備えをどの程度サポートしているか。

01 サイバー・リスクの管理および監視

ガバナンス、リスク管理、リソース、研修、文化の品質および有効性。

02 脅威情報と協調

脅威情報を監視・分析し、情報を共有する。

03 サイバー・セキュリティ統制

予防、発見および是正における統制、プロセスおよび手続の有効性。

04 外部への依存

第三者との接続の性質、監視および関係管理。

05 サイバー・インシデント管理および耐性

インシデントに対する計画立案および戦略。発見、対応および軽減に向けたプロセスと手続。上申と報告。

第3に、銀行は**リスクベースのアプローチを取り**、リスクが最も大きい箇所、保護を最も必要としている主要なクリティカル・システム、情報およびデータ資産はどれか、企業価値を守るためにどのような措置を取る必要があるかを評価する必要があります。

第4に、銀行は、他の企業や政府、政府機関とともに、サイバー・セキュリティのさまざまな側面に対して、**包括的で調整の取れたグローバルなアプローチを取る**必要があります。情報を共有し、サイバー・セキュリティへの脅威に共に立ち向かわなければなりません。最近実施されたサイバー耐性演習である、英国の「ウェイキング・シャークII」と米国の「クアンタム・ドーン2」では、その両方で前回の演習以降さまざまな側面での進歩が見られるものの、サイバー攻撃が銀行固有のものか、または、よりシステミックな性質を有するかの判断、攻撃発生時のコミュニケーションを管理する単一の調整機関の業界での創設、国内外の規制当局および政府との調整の改善といった分野に改善の余地があると結論付けました。

しかし、このような調整は困難を伴います。銀行は情報の共有に消極的である可能性がある一方で、各国政府や規制当局はサイバー・セキュリティに対して異なるアプローチを取っています。サイバー犯罪への取組み、サイバー攻撃に対する自国の耐性の強化、サイバー・セキュリティへの包括的アプローチを支援するための知識、スキルおよび能力の活用、重要な経済機能としての銀行業務の位置付けについての政府主導による戦略は、その性質や範囲が国によって異なります。

耐性基準の向上に向けて保険会社が果たす役割もあるかもしれませんが、サイバー・リスクに対する保険は、今のところ比較的低水準にとどまっています。

サイバー・セキュリティ規制および監督

サイバー・セキュリティに対する規制や監督には、他の金融規制分野に見られる多くの特徴と同じ特徴が見られます。例えば、国によってバラバラな規制アプローチ、法律や規制ルールを適用する際の「ローカリゼーション」と域外適用の両方に対する圧力などです。さらには、個別行の安全性と健全性を高めることを目的としたミクロ健全性措置、「サイバー・エコシステム」に固有のシステミック・リスクに対する保護を目的としたマクロ健全性措置、データ保護措置の3つの間にいくぶん不安定なバランスが見られることも同様に特徴の1つです。

この領域では、主として以下の5つの動きが存在します。

第1に、**包括的な弾力性演習と企業独自の弾力性演習**です。上述の米国と英国で実施されたシステム全体での耐性演習に加え、英国は「倫理的ハッキング」で他国を主導しています。倫理的ハッキングは、サイバー攻撃に対する個別行の耐性を実際の環境でテストすることを目的として、規制当局に代わって専門家グループが実施するものです。このサイバー・セキュリティの直接的なテスト（銀行によるサイバー攻撃の発見および対応能力を含む）は、銀行の統制の枠組みのレビューにおいて、従来のアプローチから大きく前進しました。他国もこれに追随する可能性があります。

第2に、規制当局は、銀行のサイバー攻撃耐性を高めることを目的とした**ルールやガイダンス策定**の初期段階にあります。これまでこうした規則やガイダンスは、適切なシステムや統制の整備を銀行に要請することによって高度に網羅されてきましたが、一部の規制当局は、サイバー・セキュリティに特化した具体的なルールやガイダンスを追加することで、これを補足することを検討しています。

EUでは2013年に、欧州委員会が以下を目的としたネットワーク情報セキュリティ指令案を公表しました。

- より強固なリスク管理文化を構築し、非常に重要なセクターで業務を運営する企業や行政機関では、ネットワークおよび情報のセキュリティを確保するための適切な措置を講じる。
- ネットワークおよび情報セキュリティを担当する国の所轄官庁を設立する。
- EUレベルでの調整の取れた情報交換、発見および対応。

この指令案は、2015年内の合意と2017年の施行が見込まれています。

第3は、**開示要件**における動きです。一部の国では、規制当局に対するサイバー攻撃の報告要件や、データの機密保持違反が発生した際の関係顧客への報告要件が、より厳しくなりました。

第4に、**監督強化**です。新たなルールや規制が導入されていない分野でも、監督当局は銀行のサイバー・リスク方針への関心を高めています。当局が関心を寄せている分野には、取締役会および上級経営陣によるサイバー・リスクに対する自覚、理解および管理の程度、銀行による違反の発見、報告および対応能力、銀行のシステムやデータに第三者がアクセスすることでもたらされるリスクに対する銀行の認識などが挙げられます。

第5は、**データ保護**です。データ保護に関して国際的に合意された基準はなく、米国とEUに国や地域独自の基準の策定が任されている状態です。EUでは、新たなデータ保護規制および指令の導入に向けた長期の試みが続いていますが、この試みではとりわけ、現存する指令（1995年に制定）を改定し、紙ベースの情報の時代からインターネットやオンラインでのデータ収集・保管の時代に移ったことで、収集・保管される個人情報も大幅に増えたことを反映することが、大きなテーマとなっています。

欧州委員会からの提案（最初の提案は2012年1月）は、企業（および政府）による個人情報の記録、保管および配布を制限することについて、EU内でのアプローチを全般により厳しくすることを基本としています。これには以下が含まれます。

- 国による解釈の余地を狭める目的での、EU全体でのより一貫したルール（規則の利用を通して）。
- 各国当局間の紛争を解決することを目的とした、EU全体での新たな監督当局。
- 自分の個人データにアクセスして内容を修正し、データ・セキュリティ違反発生時に通知を受けることに対する個人の権利の強化。
- データを所有する企業と、データを処理する企業または保管施設の両方に対する、個人データ保護を目的とした義務。個人データに対する適切なセキュリティ面の保護を含む。
- データ機密要件違反に対する処分の厳格化。
- 強固なデータ保護基準が実施されていないEU域外地域でのデータ保管に対する制限。これによって、EU域外の企業がEU内の顧客データを自国に転送できなくなったり、グローバル企業に複数のデータセンターの運営が求められたりする可能性がある。

KPMGの提携・買収企業

サイバー・セキュリティ、データ、そして分析という複雑かつダイナミックな領域におけるクライアントのニーズに応え、優れたサービスを提供するため、KPMGメンバーファームは世界中の数々の一流企業と戦略的な提携関係を構築してきました。以下は、提携関係にある一流企業の一例です。

英国

McLaren（マクラーレン）

KPMGはマクラーレン・テクノロジー・グループとの提携により、クライアントによるパフォーマンスの飛躍的な改善に貢献しています。KPMGが有する高度な業界知識および業務経験と、マクラーレンの予測分析、シミュレーションおよび高度な意思決定サポートとを組み合わせることで、業務上の複雑な課題への独自の対応が可能になりました。共同開発によるテクノロジー、協調的な業務アプローチ、継続的な改善に向けた姿勢はさまざまな形で応用でき、例えば、地理的に分散したスタッフの効率の30%向上、製造業務における生産性の50%向上、顧客体験の改善に向けたサプライチェーンの抜本的強化などが可能です。

Nunwood（ナンウッド）

顧客体験に関するコンサルタント業務を手掛けるナンウッドを買収することにより、詳細な顧客体験管理プログラムをKPMGは入手しました。ナンウッドは有名なブランド・ベンチマーキング調査を年次で実施し、カスタマー・エクスペリエンス・エクセレンス・センター（Customer experience excellence Centre）を構えています。また、顧客との相互関係を測定し、企業によるリアルタイムでの顧客データ対応を可能にする、「フィズ（Fizz）」と呼ばれる独自のテクノロジー・ソリューションを有しています。

スペイン

ADN

KPMGスペインは、スペインの大手デジタル戦略アドバイザリー企業であるADNを買収し、KPMGスペインのマネジメント・コンサルティング部門に統合することで、KPMGのストラテジー、トランスフォーメーション、データ&アナリティクス部門を強化しました。

Zink Security（ジンク・セキュリティ）

KPMGスペインは、情報セキュリティと倫理的ハッキング・サービスに特化したテクノロジー企業であるジンク・セキュリティを買収しました。この買収によってKPMGでは、ソーシャル・ネットワーク、フォーラム、ブログ、ニュースサイトおよびディープ・ウェブから入手可能な情報を通して、個人、グループ、企業などの間の各種の出来事や情報漏洩、関係性を調査および監視し、日々生成される大量の情報を企業が監視、分析および管理するためのサポートが可能になりました。

グローバル

Cynergy（シナジー）

KPMGのデジタル体験設計部門を主導しているのがKPMGシナジーです。元は米国を拠点としていた企業で、革新的な顧客／企業体験ソリューションを提供しており、モチベーションを上げる独自の設計手法と機敏性のある協調的アプローチを用いて、テクノロジーやプラットフォームにとらわれないデジタル・ソリューションを提供しています。

用語集

AML	Anti-Money Laundering	マネーロンダリング防止
AQR	Asset Quality Review	資産査定
CCAR	Comprehensive Capital Analysis and Review	包括的資本分析（米国）
CMU	Capital Markets Union	資本市場同盟
COREP	Common Reporting	共通報告フレームワーク
CRD4	Fourth Capital Requirements Directive	自己資本指令4
CRS	Common Reporting and Due Diligence Standard	共通報告およびデューデリジェンス基準
D-SIB	Domestic Systemically Important Bank	国内のシステム上重要な銀行
EBA	European Banking Authority	欧州銀行監督機構
ECB	European Central Bank	欧州中央銀行
EDTF	Enhanced Disclosure Task Force	開示強化タスクフォース
EMA	Europe, Middle East and Africa	ヨーロッパ、中近東、アフリカ
EMIR	European Market Infrastructure Regulation	欧州市場基盤規制
ESMA	European Securities and Markets Authority	欧州証券市場監督機構
EU	European Union	欧州連合
FATCA	Foreign Account Tax Compliance Act	外国口座税務コンプライアンス法
FFIEC	Federal Financial Institutions Examination Council	連邦金融機関検査協議会（米国）
FINREP	Financial Reporting	財務報告フレームワーク
G-SIB	Global Systemically Important Bank	グローバルなシステム上重要な銀行
ICAEW	Institute of Chartered Accountants in England and Wales	イングランド・ウェールズ勅許会計士協会
IFRS	International Financial Reporting Standards	国際財務報告基準
KPI	Key Performance Indicator	重要業績評価指標
MAS	Monetary Authority of Singapore	シンガポール金融管理局
MiFID	Markets in Financial Instruments Directive	金融商品市場指令
MiFIR	Markets in Financial Instruments Regulation	金融商品市場規制
NIST	National Institute of Standards and Technology	国立標準技術研究所（米国）
OECD	Organisation for Economic Co-operation and Development	経済協力開発機構
REMIT	Regulation on Wholesale Energy Market Integrity and Transparency	卸エネルギー市場の健全性と透明性に関する規則
RWA	Risk Weighted Asset	リスク・アセット
SFT	Securities Financing Transaction	証券金融取引
SME	Small and Medium Enterprises	中小企業

Contact us

Jeremy Anderson
Chairman Global Financial Services
KPMG
T: +44 20 7311 5800
E: jeremy.anderson@kpmg.co.uk

Bill Michael
EMA Head of Financial Services
KPMG in the UK
T: + 44 20 7311 5292
E: bill.michael@kpmg.co.uk

Giles Williams
Partner, Financial Services
Regulatory Center of Excellence
EMA region
T: +44 20 7311 5354
E: giles.williams@kpmg.co.uk

Clive Briault
Senior Adviser, Financial Services
Regulatory Centre of Excellence
EMA region
T: + 44 20 7694 8399
E: clive.briault@kpmg.co.uk

Andrew Davidson
Director, Regulatory Centre of Excellence
EMA region
KPMG in the UK
T: +44 20 7694 2242
E: andrew.davidson@kpmg.co.uk

George Quigley
Partner, Information Protection and Business Resilience
KPMG in the UK
T: +44 (0) 20 7311 5603
E: george.quigley@kpmg.co.uk

Simon Topping
Principal, Financial Services
Regulatory Center of Excellence
ASPAC region
KPMG China
T: +852 2826 7283
E: simon.topping@kpmg.com

Seiji Kamiya
Partner, Financial Services
KPMG in Japan
T: +81 3 3548 5100
E: seiji.kamiya@jp.kpmg.com

fsregulation@kpmg.co.uk

www.kpmg.com/regulatorychallenges

kpmg.com/socialmedia

kpmg.com/app

Available on the App Store

本レポートは、KPMGインターナショナルが2015年10月に発行した“Evolving Banking Regulation Part Three Data and technology: The regulatory and business challenges”を翻訳したものです。翻訳と英語原文間に齟齬がある場合は、当該英語原文が優先するものとします。

Designed by Evalueserve.
Publication name: Evolving Banking Regulation – Part three: Data and technology: The regulatory and business challenges
Publication number: 132588-G