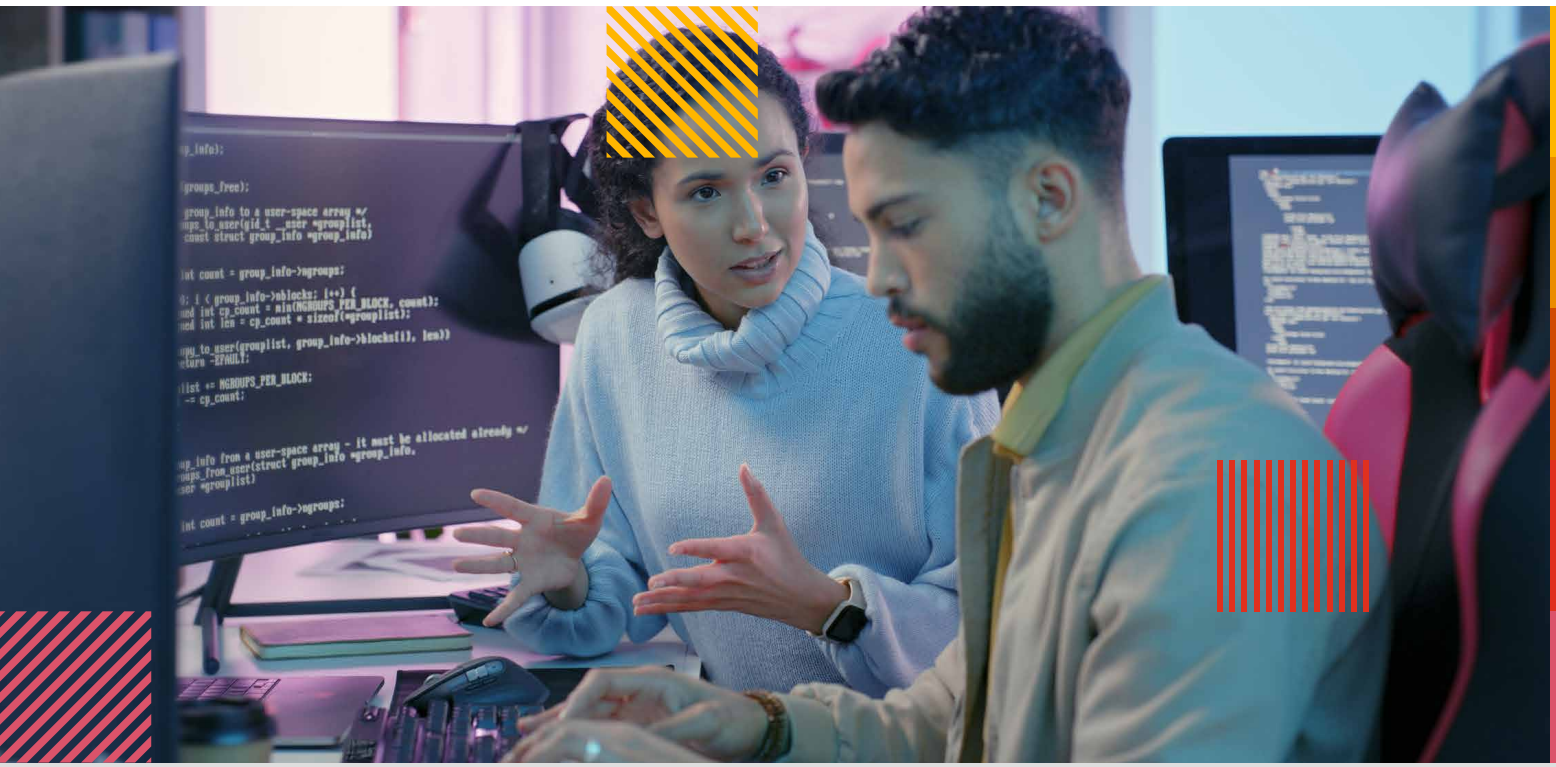
世界のサイバー規制の概要：金融サービス

pwc

www.pwc.com/jp



内容

サイバーセキュリティおよびデータ保護については、金融機関も規制当局もどちらも多くのことを考慮しています。これには、巧妙化が続くサイバー攻撃、金融犯罪への関与を強める国家レベルの悪質な脅威アクター、重大なデータ侵害、および消費者が求める自身のデータの詳細管理なども含まれます。

これらの傾向の影響を軽減するために、規制当局と政策立案者は、以下の領域で企業の防御、管理、ポリシーの改善に注力してきました。

1 | **オペレーショナルレジリエンス**

2 | **データ保護**

3 | **インシデント報告**

4 | **不正防止と責任**

5 | **サードパーティリスク管理**

6 | **人工知能**

66%

軽減すべきリスクの最上位にサイバーリスクを挙げたのは、技術担当幹部が66%に対して、経営幹部は48%

出所：PwC 2025 Global Digital Trust Insights

オペレーショナルレジリエンス

サイバー攻撃やその他の事象がサービスや事業の継続に与える影響を最小限に抑えつつ、迅速に復旧する能力を**オペレーショナルレジリエンス**と言います。現在の規制動向において極めて重要なテーマとなっています。下記に主要な動きをまとめました。

- **英国**の金融サービス（FS）セクターのオペレーショナルレジリエンスに関する標準が、2022年3月に施行されました。これらの標準では、企業は、重要な活動を定義し、影響の許容範囲を設定し、テストを実施し、オペレーショナルレジリエンスの機能に対するガバナンスを確立することが求められています。
- **欧州連合（EU）**では、デジタル・オペレーショナル・レジリエンス法（DORA）と呼ばれる金融サービスセクターのオペレーショナルレジリエンスに関する非常に広範な規制があり、デジタルリスク管理、レジリエンステスト、サードパーティリスク管理、および情報共有をカバーしています。
- **中東**にはさまざまなフレームワークがあり、サウジアラビアの2017年事業継続マネジメントフレームワークでは、ガバナンスに取り組み、災害復旧の訓練を毎年行うことを義務付けています。

データ保護

世界各国の法域では、消費者に自身のデータに対する高度な管理権限を付与する動きが広がっています。情報漏えいやサイバー攻撃によって、個人データが危険にさらされる可能性を低減するためです。以下に、主な動向を示します。

- **北米**には、金融サービスセクターのデータプライバシーとセキュリティに関するさまざまな法規制があります。米国の場合、これらにはグラム・リーチ・ブライリー法（GLBA）、公正信用報告法（FCRA）、およびカリフォルニア州消費者プライバシー法（CCPA）などが該当します。カナダでは、個人情報保護および電子文書法（PIPEDA）で、個人情報の公正な取り扱いに関する原則が定められています。

- **EU**の一般データ保護規則（GDPR）は消費者に対して、自身のデータへのアクセス、修正、削除、処理の制限、他サービスへのデータ移行（ポータビリティ）、および特定の処理活動への異議申し立ての権利を認めています。また、データの管理者および処理者にも、サイバーセキュリティやインシデント報告の要件などの義務を課しています。
- **英国**のデータ保護法では、EUのGDPRと同様の要件が含まれています。
- **アジア太平洋諸国**は、データ保護に関してさまざまなアプローチや取り組みを行っています。**中国**では、データセキュリティと国境を越えたデータ転送に関して厳しい規則があり、データの処理と共有に影響を及ぼしています。**シンガポール、香港、インド**では、GDPRとほぼ同様の要件があります。

インシデント報告

世界中の規制当局（場合によって単一の法域に複数の規制当局がある）は、さまざまな**インシデント報告**の基準や時間枠を求めています。

- **北米**では、さまざまな規制当局が金融サービス企業に対し、サイバーインシデントの発生時には当局および顧客への迅速な報告・開示を義務付けています。例えば、米国証券取引委員会（SEC）は、重大なインシデントであると判断された時点から4日以内の報告を求めているほか、ニューヨーク州金融サービス局（NYDFS）は、ランサムウェアへの支払いを行った場合、24時間以内の通知を義務付けています。
- **EU**のデジタルオペレーショナルレジリエンス法（DORA）では、金融サービス企業に対し、業務、サービス、顧客、または金融システムに重大な影響を及ぼすインシデントが発生した場合、最初の通知の提出から72時間以内に、関係当局および欧州監督当局に中間報告を提出することを義務付けています。
- **中東**にはサイバーインシデントの報告に関する統一的な規制はありませんが、**サウジアラビア**や**アラブ首長国連邦（UAE）**など一部の国では、サイバーおよびデータ保護のフレームワークを発行しており、金融サービス企業に対してサイバーインシデントをサウジアラビア通貨庁（SAMA）や電気通信規制局（TRA）などの関係当局に報告することを義務付けています。報告の要件は、国、セクター、およびインシデントの種類によって異なります。
- **アジア太平洋地域**の各国では、サイバーインシデントの報告に関するアプローチや重点領域が異なります。例えば**中国**では、「ネットワークセキュリティインシデント」が発生した場合、企業は中国国家インターネット情報弁公室（CAC）および影響を受けた個人に対して報告する義務があり、重大度に応じて72時間以内の報告期限が定められています。**シンガポール**では、重大な損害をもたらすインシデントや、500人以上の個人に影響を及ぼすインシデントについて、企業は個人情報保護委員会（PDPC）に対し、遅くとも3営業日以内に報告する必要があります。

不正防止と責任

攻撃が増加し続ける中、規制当局も**不正行為**に対処するための対策を講じていますが、銀行や消費者が、損失に対してどの範囲まで責任を負うべきかについては意見が割れています。

- **北米**では、米国の規制当局で、企業が処理する不正な支払いに対して責任を問うケースが増えており、パラダイムシフトが進行しています。
- **EU**の決済サービス指令（PSD2）には、決済のセキュリティと認証に関する厳格な規則が含まれています。また、特定の種類の詐欺や不正行為の被害を受けた顧客に対して、企業の返金対応が義務付けられています。

42%

経営幹部の42%が、最も懸念されるサイバー脅威としてクラウド関連の脅威を挙げています

出所：PwC 2025 Global Digital Trust Insights

- **中東**では、金融サービス企業や顧客に対する不正行為の試みの増加が見られます。**サウジアラビア**は、不正対策フレームワークを発行し、金融サービス企業に対して、不正対策の導入、毎年の不正リスク評価、および不正行為の特定方法と回避方法を顧客に教育することを義務付けています。

サードパーティリスク管理

規制当局は、ベンダーへの依存度が高いことによる集中リスクや、ベンダー関連のセキュリティ侵害の増加について懸念を表明しており、**サードパーティリスク管理**（TPRM）は引き続き重要な焦点領域となっています。

- **北米**では、米国内のさまざまな機関が、サードパーティリスク管理（TPRM）に関する期待事項をリリースしており、例えば、2023年にリリースされた機関間ガイダンスなどが挙げられます。**カナダ**では、金融機関監督局（OSFI）が同様のガイドラインを発行しています。
- **英国**では、健全性規制機構（PRA）が、アウトソーシングおよびサードパーティリスク管理（TPRM）に関する期待事項に重点を置いた監督声明を発表しました。
- **EU**では、デジタル・オペレーショナル・レジリエンス法（DORA）でサードパーティリスク管理をカバーしており、金融機関に対してICTリスクの管理、脅威インテリジェンスに基づく倫理的なペネトレーションテストの実施、ベンダー契約への標準的なサイバーセキュリティ条項の挿入を求めています。
- **中東**では、サウジアラビア通貨庁（SAMA）がサードパーティリスク管理フレームワークを策定中です。
- **アジア太平洋**の観点から、シンガポール通貨金融庁（MAS）は、アウトソーシングされたサービスに関連するリスクを管理するための要件を更新しました。**日本**の規制当局は、オンボーディング前から契約終了後まで、ベンダーのデューデリジェンスを強化するよう求めています。

人工知能

最後に、世界中で**人工知能（AI）**の導入が急速に進む中、政府や規制当局は、金融サービス機関全体に対してAIの安全な利用に関する期待事項を定めています。

- **北米**のAI規制は現在、多くの既存の標準や期待事項の範囲に含まれていますが、政策立案者は別の管轄が必要かどうか検討しています。**カナダ**では、安全で責任ある倫理的なAIの利用を促進するための指針を定める「人工知能およびデータ法案」が提案されています。
- **英国**には、倫理的かつ責任あるAIの開発と使用を促進するための取り組みやガイドラインがいくつかあります。これらには、英国AIセクターディール、データ倫理・イノベーションセンター（CDEI）、AIオフィス、アラン・チューリング研究所、およびAIカウンシルなどが含まれます。
- **EU**では、2024年5月に承認された人工知能法により、AIの使用に関する規制および法的枠組みが策定されています。
- **アジア太平洋諸国**は、AI規制に関してさまざまなアプローチや取り組みを行っています。**中国**では、データセキュリティと国境を越えたデータ転送に関して厳しい規則があり、AIアプリケーションに影響を及ぼしています。**シンガポール**と**日本**は、倫理的で信頼できるAIに関するガイドラインと原則を発行しました。

組織は、オペレーショナルレジリエンスに対する監督の強化に対応するために、重要サービスを定義し、これらのサービスに関係する主な脆弱性と依存関係を特定し、影響の許容度を設定し、定期的なテストを実施する必要があります。

分断されている世界各地の規制当局がこれらの領域を超えて基準を引き上げ続けているため、世界中のあらゆる地域の動向を常に把握し、**状況に応じてガバナンスやコントロールをプロアクティブに強化**することが不可欠になっています。

例えば、組織は、オペレーショナルレジリエンスに対する監督の強化に対応するために、重要サービスを定義し、これらのサービスに関係する主な脆弱性と依存関係を特定し、影響の許容度を設定し、定期的なテストを実施する必要があります。サイバーインシデントの透明性を高めるためのグローバルな規制が急増する中、組織は、インシデントの重要性の定義方法や、統治機関に開示する適切な情報量の理解など、インシデント報告プロセスと準備状況を評価する必要に迫られています。

プロアクティブなアプローチで、規制の期待事項を特定し遵守することで、企業は、避けられない破壊的なイベントによる損害を軽減し、顧客との信頼関係を強化し、金融、テクノロジー、および評判のリスクを最小限に抑えることができます。

関心のある地域の詳細については、以下のセクションに移動してください。各セクションでは、最新の規制の動向と**その背後にある考え方（概要）**を探り、**対応方法（要点）**に念頭を置きながら未来の傾向を予測し、**各地域における関係する規則（詳細）**について詳述します。

- 北米
- 英国
- 欧州連合（EU）
- 中東
- アジア太平洋（APAC）、特に中国、シンガポール、香港、日本
- インド

北米

概要：規制の現状

米国またはカナダで自社の銀行がサイバー攻撃を受けた場合、最初に誰に連絡すべきでしょうか？　この問いに明確に答えるのは容易ではありません。

多くの場合、複数の関係機関への報告が必要になります。国家による侵害の試みの増加、ランサムウェアの被害拡大、高度化する攻撃手法、そして金融システム内の相互依存性の強まりを背景に、北米ではサイバーインシデント発生時に規制当局への報告を義務付ける要件が増加しています。

一部の新しい規制や保留中の規制としては、米国証券取引委員会（SEC）による最近の開示規則、ニューヨーク州金融サービス局（NYDFS）のサイバーセキュリティ規則の新たな改定、およびカナダのC-26法案などが挙げられます。

一方で、インシデントの報告や開示は、北米のサイバー規制の一部に過ぎません。

重点領域には、オペレーショナルレジリエンス（事業継続マネジメントを含む）、サードパーティサービスプロバイダーのセキュリティ、データプライバシー、ITガバナンスも含まれます。米国では、米国証券取引委員会（SEC）、ニューヨーク州金融サービス局（NYDFS）、連邦預金保険公社（FDIC）、連邦準備制度理事会（FRB）、および全米保険監督官協会（NAIC）は全て、これらの問題に関する期待事項やガイダンスをリリースしています。カナダでは、金融機関監督局（OSFI）が同様のガイドラインを発行しています。

96%

組織の96%が、サイバーセキュリティ規制に迫られて、過去12カ月にサイバー投資が増加したと報告しています

出所：PwC 2025 Global Digital Trust Insights

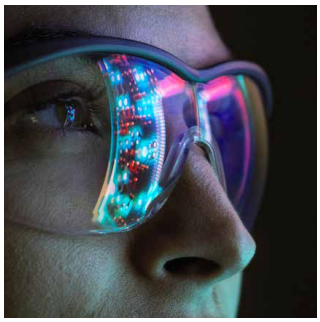
その結果、金融サービス企業は、統一性のない多数の法律、基準、フレームワークへの対応を迫られています。これらは、サイバーセキュリティ、リスク管理、プライバシー保護といった各専門部門が個別に対処しなければならない課題です。

他の州や準州の規則も加えることで、北米でセキュリティを規制する組織の完全なリストが完成します。各組織には独自の関心領域と法域もあるため、特に大規模な企業においては、こうした断片化された状況がクライアントの混乱を一層深める要因となっています。

要点：今後の見通し

- **人工知能（AI）は北米で規制の対象となる**

  米国の複数の州では、AIに関連する法的措置の検討が進められています。また、カナダが提案している人工知能およびデータ法が承認されれば、安全で責任ある倫理的なAIの使用に関するガイドラインが規定されることになります。



  これらの規制はいずれも金融サービスセクターに直接適用されるものではありませんが、銀行、保険会社、資産運用会社、フィンテック企業などの各社にとって、その要件を注視することは極めて重要です。融資、信用情報の報告、引受業務などの活動はすでに公平性の観点から厳しく監視されており、意思決定が自動化されたシステムによって行われる場合、その公平性が損なわれる可能性が懸念されています。

  言い換えれば、技術そのものが規制の対象となっていない場合でも、活動自体は既存の規制の枠組みに従う必要があるということです。AIのような新技術を導入したとしても、既存の基準への準拠が免除されるわけではありません。むしろこの強力な技術がもたらすリスクに関する議論の進展に伴い、基準そのものが見直される可能性もあります。

- 国家によるサイバー攻撃が激化する中、金融サービス業界およびその他の重要インフラに対する**セキュリティ要件の強化が求められる**可能性があります。また、地政学的な緊張の高まりは、政府機関および重要インフラシステムに対する脅威を増大させかねません。ハッキングが諜報活動や破壊工作の手段として利用されるようになっていることから、これらのシステムは一層のリスクにさらされています。

  カナダでは、規制対象の金融サービス企業は、ポリシーと手順を策定して、外国からの介入対策を含めシステムとデータの完全性を保護する必要がある、と金融機関監督局（OSFI）の監督官が示唆を出しています。

- 特に新しいテクノロジーの出現に伴い、**脅威の性質は変化し続けています。**

  米国の3つの連邦機関―連邦捜査局（FBI）、国家安全保障局（NSA）、およびサイバーセキュリティ・インフラセキュリティ庁（CISA）―は、2023年9月12日、実在の人物を模倣するコンピューター生成の映像・音声「**ディープフェイク**」の増加に関する警告と指針を発表しました。口座保有者の音声などの認証情報を模倣するために極めて精巧な偽装技術が用いられることで、口座への不正アクセスや各種詐欺行為に金融サービスが悪用される恐れがあります。

PwCによる詳細はこちら：

政策立案者、全ての人のために生成AIの安全強化に注力

78%

組織の78%が、過去12カ月に生成AIへの投資を増やしました

出所：PwC 2025 Global Digital Trust Insights

詳細：注目すべき規制

サイバーセキュリティリスク管理、戦略、ガバナンス、およびインシデントの開示（17 CFR Parts 229、232、239、240、249）

規制当局：米国証券取引委員会（SEC）

状況：2023年9月5日（2023年12月15日以降に発行される年次報告書に適用）

対象：1934年証券取引法に基づき報告義務を負うすべての登録企業（外国の民間発行体にも同様の要件が適用）

この規則では、重大なサイバーセキュリティインシデントの迅速な開示と、サイバーセキュリティのリスク管理、戦略、ガバナンスに関する年次開示が求められます。この規則では、企業は、年次報告書であるForm 10-Kの提出で、サイバープログラムの詳細を記載することが義務付けられています。また、重大なサイバーセキュリティインシデントについては、インシデントが重大であると判断されてから4日以内に迅速に報告するよう義務付けられています。

PwCによる詳細はこちら：

SECの新しいサイバー開示規則：新たな時代の情報開示の透明性に対応するには

23 NYCRR Part 500の第2次修正、金融サービス企業に対するサイバーセキュリティ要件

規制当局：ニューヨーク州金融サービス局（NYDFS）

状況：インシデント報告要件は2024年12月1日より施行されており、その他の移行期間は2025年11月まで段階的に設定されています。

対象：銀行、保険会社、その他ニューヨーク州の規制下にある金融サービス機関（「対象事業体」）。具体的には、銀行法、保険法、または金融サービス法に基づき、ライセンス、登録、認可、証明書、許可、認定、または同様の権限の下で運営することが求められるすべての事業体が該当します。

この改正により、23 NYCRR Part 500（ニューヨーク州サイバーセキュリティ規則）は以下のような追加のサイバーセキュリティインシデントを対象に拡張されます：

- 対象事業体の情報システムの重要部分にランサムウェアが展開された場合
- 関連会社または第三者サービス提供者において発生し、対象事業体に影響を及ぼすインシデント

また、対象事業体は、ニューヨーク州金融サービス局（NYDFS）が求めるサイバーセキュリティイベントの調査に関する情報を提供・更新する義務を負います。さらに、ランサムウェアによる身代金支払いを行った場合には、支払いから24時間以内にNYDFSへ通知する必要があります。対象事業体は、30日以内にNYDFSに対し、（1）支払いが必要であると判断した理由、（2）検討した支払いの代替手段と、支払いの代替手段を見つけるために試みた方法、（3）適用される規則や規制のコンプライアンスを確保するために講じた措置についても報告する必要があります。

78%

組織の78%は、規制がサイバーセキュリティ態勢の挑戦、改善、強化に役立ったと考えています

出所：PwC 2025 Global Digital Trust Insights

Guideline B-13、テクノロジーおよびサイバーリスク管理

規制当局：金融機関監督局（OSFI）

状態：2024年1月1日より施行

対象：連邦政府の規制下にあるカナダの金融機関

このガイドラインは、連邦政府が規制する金融機関に求められる、データ侵害やテクノロジー障害などのテクノロジーおよびサイバーリスクの管理方法に関する金融機関監督局（OSFI）の期待事項を定めています。

この原則に基づくガイドラインは、（1）ガバナンスおよびリスク管理、（2）テクノロジー運用およびレジリエンス、（3）サイバーセキュリティ、という3つの領域に分類されています。このガイドラインで定められている標準には、戦略的テクノロジーおよびサイバー計画、テクノロジーおよびサイバーリスク管理フレームワーク、テクノロジー資産管理プログラム、災害復旧、サイバーリスク管理、脅威インテリジェンス、セキュリティ・バイ・デザイン、多

層セキュリティ、IDおよびアクセス管理、ソフトウェア開発ライフサイクル管理、およびインシデント対応などが含まれます。

PwCによる詳細はこちら：

OSFIの最終のB-13ガイドラインのリリースにより、テクノロジーとサイバーリスク管理の優先度が上昇

ガイドラインB-10（改訂版） サードパーティリスク管理

規制当局：金融機関監督局（OSFI）

状況：2024年5月より施行

対象：カナダ連邦規制下の金融機関

このガイドラインは、上記のB-13の補足として策定されたものであり、金融サービス企業に対し、金融機関監督局（OSFI）からの要請に応じて、第三者との業務および戦略的な取り決め、リスク管理、統制環境に関する情報を提供し、監督上のモニタリングおよびレビューワークを支援することを求めています。第三者との提携が重要な業務に重大な影響を及ぼす場合には、速やかにOSFIへ通知することが義務付けられています。

また、明確なガバナンスと説明責任の確保、包括的なリスク管理戦略およびフレームワークの整備、第三者リスクの評価・管理・軽減、第三者の業務評価およびモニタリング、リスクやインシデントへの積極的な対応、第三者との関係の継続的な管理、そして第三者による技術およびサイバー業務の透明性・信頼性・安全性の確保が求められています。

Intelligence-led Cyber Resilience Testing（I-CRT）Framework（I-CRT）

規制当局：金融機関監督局（OSFI）

状況：現在有効

対象：カナダのシステム上重要な銀行（SIBs）および国際的に活動する保険グループ（IAIGs）

このフレームワークは、重要なビジネス機能に対するインテリジェンス主導型のテストを通じて、金融サービス企業のレジリエンスを向上させるためのガイダンスおよび監督について規定しています。本ガイドラインでは、各SIBおよびIAIGが少なくとも3年に1回、脅威インテリジェンスに基づいたペネトレーションテストを実施し、現実的に想定される脅威をシミュレーションすることが推奨されています。

PwCによる詳細はこちら：

適切なインサイトを通じてレジリエンスを構築する：金融機関がOSFIのI-CRTフレームワークを活用してサイバー防御を強化する方法

英国

概要：規制の現状

英国は地理的には島国ですが、同国の金融機関は決して孤立しているわけではありません。多くの企業は、大西洋をまたいでさまざまな国でビジネスを行っており、それらの現地の規制にも従う必要があります。

英国はBREXIT後、相互依存性を認識し、EUの一般データ保護規則（GDPR）とほぼ同じバージョンの規則を採用しており、サイバーセキュリティに対処するEU法であるネットワークおよび情報システムに関する指令（NIS2）のバージョンも制定されることが期待されています。

また、英国の金融サービス企業は、遵守する必要がある数多くのEU規則を継承しながら、米国で規定された要件にも対応しています。

その結果、特に国のサイバーセキュリティ法がない状況で、把握する必要がある複数のポリシーや要件が混在していることが問題となっています。

要点：今後の見通し

- 以前は、銀行やウェルスマネジメント会社が規制当局の監視の矢面に立っていましたが、現在は、**保険会社**がそのような状況になっています。
- 金融サービス企業については、特に懸念される決済処理業者やクラウドサービスプロバイダーなどの**サードパーティサービスプロバイダー**に対する審査と監視を強化する圧力が高まっています。この分野では、規則やガイダンスがさらに増えることが予想されます。

詳細：注目すべき規制

レジリエンスの強化

健全性監督機構（PRA）SS1/21：オペレーショナルレジリエンス：重要なビジネスサービスへの影響許容範囲／**金融行為規制機構（FCA）PS21/3：**オペレーショナルレジリエンスの構築：CP19/32および最終規則へのフィードバック

規制当局：イングランド銀行（BoE）、健全性監督機構（PRA）、金融行為規制機構（FCA）

状況：有効。企業は移行期間内である2025年3月31日までに遵守する必要があります。

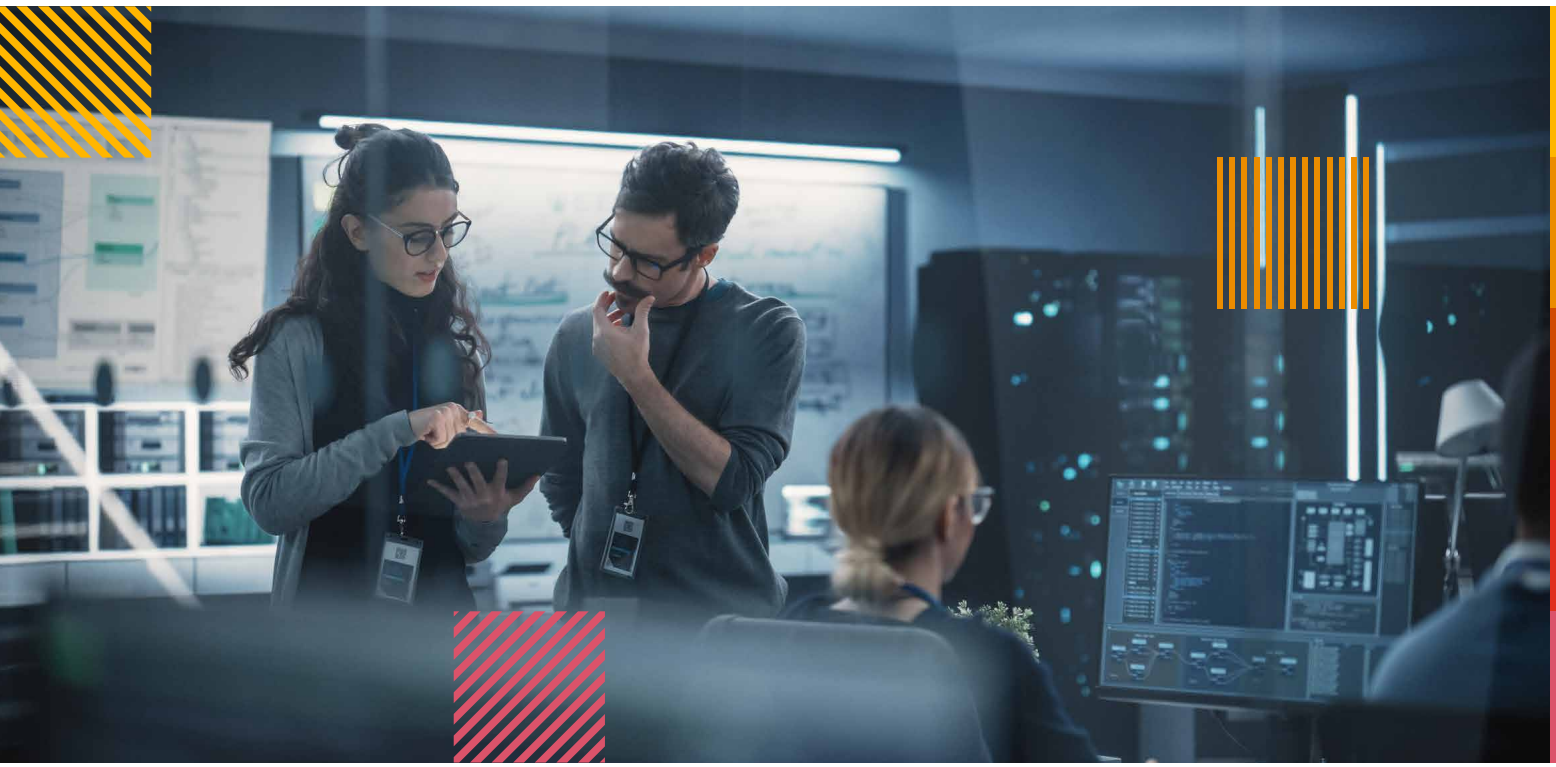
対象：健全性監督機構（PRA）：英国の銀行、住宅金融組合、PRA指定投資会社（以下、銀行）、資本要件規制（CRR）の連結企業体、および英国ソルベンシーII企業、ロイズ協会およびその経営代理店（保険会社）。金融行動監視機構（FCA）：英国の銀行、住宅金融組合、保険会社、投資取引所、決済会社、その他の大手金融サービス会社

この規制では、重要なビジネスサービスの特定から、影響許容限度内での回復を実現するためのシナリオテストまで、オペレーショナルレジリエンスを向上させるための手順が規定されています。ただし、この規制は、望ましい結果を達成する方法に関する模範的な手順を提供するものではなく、一般的な期待事項と包括的なアプローチに重点を置いており、企業が遵守を目指す際の課題を提起します。

デジタルオペレーショナルレジリエンス法（DORA）：このEUのオペレーショナルレジリエンスのフレームワークは、英国の組織、および世界中の他の国にも影響を与えています。DORAの詳細な分析については、このホワイトペーパーの「欧州連合（EU）」のセクションをご覧ください。

PwCによる詳細はこちら：

DORA、および英国の金融機関およびICTサービスプロバイダーに対するDORAの影響



サイバーセキュリティ能力のテスト

脅威ベースのペネトレーションテスト、またはレッドチーム演習は、英国の金融サービス業界のサイバー規制ツールキットの重要な一部であり、企業に対して、2つのレジリエンステストスキームを提供しています。

これらのインテリジェンス主導型のレジリエンステストフレームワークとして、ティア1機関を対象としたCBEST（Critical National Infrastructure Banking Supervision and Evaluation Testing）、および幅広い金融サービスでの使用を対象に設計されたSTAR-FS（Simulated Target Attack and Response for the Financial Services）があり、組織のサイバー攻撃の検出、防御、および対応能力をテストします。この取り組みは、組織が破壊的なイベントに耐え、そこから回復する能力に焦点を当てているオペレーショナルレジリエンスとは異なります。

英国当局は2014年にCBESTを使用して、この種のレジリエンステストを世界で初めて開始しました。現在、米国を含む主要なほとんどの金融サービスの法域で、このテストまたは類似のテストを使用しています。

CBESTテストとSTAR-FSテストはどちらも任意であり、金融サービス企業は、自身のサイバーセキュリティプログラムが強力であること、およびサイバー予算を賢く使って最大のリターンを得ていることを確認することができます。

サードパーティリスク管理

PRA PS16/24：オペレーショナルレジリエンス：英国の金融セクターの重要サードパーティ。

規制当局：イングランド銀行（BoE）、健全性規制機構（PRA）

状況：2024年11月12日に発行。

対象：英国財務省が指定する、英国の金融サービス企業に重要なビジネスサービスを提供しているサードパーティ。

この政策声明（PS）では、金融サービス企業の重要サードパーティ（CTP）プロバイダーに対する最低限のレジリエンス基準を定めています。これらの基準では、重要サードパーティ（CTP）に対して、サービスが中断した場合にシステムに影響を与える可能性があるサービスを特定し、そのようなサービスに対する重大なリスクを評価し、これらのリスクを軽減するための適切なコントロールを導入し、テストを実施することを求めています。また、事業継続性とレポート作成の基準も定められています。

規制当局はまた、市場の集中化が進む中、金融機関がクラウドサービスプロバイダーなどのサードパーティに依存する集中リスクについても懸念しています。

PRA SS2/21：アウトソーシングとサードパーティリスクの管理

規制当局：イングランド銀行（BoE）、健全性監督機構（PRA）

状況：有効

対象：英国の幅広いさまざまな金融サービス機関。一部の要件では、信用組合や指令対象外会社も含まれる。

この規則は、企業がアウトソーシングおよびサードパーティリスク管理に関する規制や期待事項への遵守に必要な方法について、PRAの期待事項を定めています。

規制当局はまた、市場の集中化が進む中、金融機関がクラウドサービスプロバイダーなどのサードパーティに依存する集中リスクについても懸念しています。

PRA SS2/21は、上記のPRA SS1/21を補完するものです。

PwCによる詳細はこちら：

規制当局は重要サードパーティのレジリエンス対策を提案

データ保護

英国GDPR／データ保護法（DPA）

規制当局：英国情報コミッショナー事務局

状況：有効

対象：個人データを収集する英国の組織と、英国居住者の個人データを収集する国外の組織。

英国政府は2020年にEUを離脱した直後、世界で最も厳格なデータプライバシー保護法であるGDPRとほぼ同じ独自のバージョンを可決しました。

EU版と同様に、英国GDPRは消費者の保護を目的としており、英国居住者から収集したデータを管理する際に企業が従わなければならない7つの原則を定めています。また、この規則では、企業が収集するデータを保有する消費者に対して8つの権利を割り当てており、これには、データの収集、処理、保管に対する同意や撤回の権利、および自動化された意思決定およびプロファイリングに関する特定の権利などが含まれます。また、違反した場合には厳しい罰則が科せられます。

英国GDPRは施行されてから2年以上経過し、EU版は2018年に施行されていますが、多くの機関が依然として準拠に苦労しているのが見られます。主な課題は、システムが収集する大量のデータの識別、分類、および追跡です。

サイバーセキュリティ能力の強化

EU全体における高い共通レベルのサイバーセキュリティ対策に関する指令（NIS2）

起源： EU。英国が独自のバージョンを採択する可能性もある

状況： 2023年に制定され、EU加盟国の各国の議会は2024年10月16日までにこれを国内法に施行するよう指示されている。

対象： EUで「重要サービス」を運営する英国企業。この分類は金融サービス企業に適用されることが多い。

NIS2指令の目的は、EUにおける重要サービス事業者（OES）のサイバーセキュリティ慣行を改善することで、以前のバージョンはNIS（ネットワークおよび情報システム規則）です。この指令は、金融サービスを含むOES組織に対して義務的なサイバーセキュリティ慣行を規定するもので、インシデント報告の義務付け、およびEU加盟国に対してセキュリティインシデントへの対応に備えるための具体的な対策を講じることを義務付ける規定などが含まれています。

欧州連合（EU）

概要：規制の現状

デジタルオペレーショナルレジリエンス法（DORA）は、多くの企業の運営およびリスク管理の方法を根本的に変え、金融サービスやEUを超えて広がる可能性があります。

DORAの背後にある主な目的は、障害の影響が相互に接続された複数の機関や他のセクターに拡大する「ブラックスワン」のような事象による経済的災害を回避することです。そのため、この法律は金融サービスセクターだけでなく、関連セクターにも適用されます。

DORAは、オペレーショナルレジリエンスをプロセスに組み込むことで、サイバーセキュリティの運用方法を確実に変えるもので、専門家が長年にわたり重要だと訴えてきた実践を義務付けています。

その名称が示すようにDORAはレジリエンスの強化を目的とした規制ですが、その規制措置は従来のレジリエンス対策の枠を超え、リスク管理、サイバーセキュリティ、そしてインシデント報告までを包含しています。

これらのトピックはそれ自体が広範囲ですが、DORAは、サードパーティリスク管理、データセキュリティ、脆弱性と変更管理、ペネトレーションテスト、情報共有、コンティンジェンシープラン、アウトソーシング契約などにも対応しています。

また、DORAは従来オペレーショナルレジリエンスに関連付けられてきた対応も求めています。その中には、重要なビジネスサービスの特定やマッピングといった、どの組織にとっても困難な作業が含まれます。

各金融サービス機関は、業務停止によって事業、顧客、あるいは経済に被害が生じるまでに耐えられる許容限度を設定する必要があります。DORAでは、組織が設定した限度内で復旧できること確認するために、シナリオベースのレジリエンステストの実施を義務付けています。

不明点は依然として残ってはいるものの、DORAは非常に具体的な指針を含む内容であるため、コンプライアンス担当者が困惑することは少ないでしょう。レベル2の標準仕様では、サードパーティリスク管理やテスト、再委託などの分野において詳細な技術仕様を規定しています。

DORAは、すでに高度に規制された金融サービスなどの業界に対して、長らく推奨されてきた対策の実施を強制することで、DORAは他業界に対してもより厳格なレジリエンス規制を促す可能性があり、GDPRと同様に他国にも影響が波及すると見込まれます。

コンプライアンス上の課題が山積み

大規模な組織であれば、DORAに準拠するのはそれほど難しくないはずです。大規模な組織の場合すでに多くの要件を満たしている可能性がありますが、サードパーティサプライヤの規則で苦労するかもしれません。このような企業の場合、数万ものベンダーと連携していることも珍しくありません。これら全ての企業を審査および監視し、そのコンプライアンスを確認することは、確かに困難だと思われます。

小規模な企業や大半の保険会社にとって、コンプライアンス遵守の道のりは長くなる可能性があります。これらの会社はサードパーティとの連携は少ないですが、大手銀行に比べてリソースが少なく、法規制を調査する経験も少ない傾向にあるためです。しかしながら、DORAは、規模に関係なく全面的に適用されます。

また、ベンダーを問いません。金融サービス企業に商品やサービスを提供する全ての企業は、EU経済の中心にある巨大な金融エコシステムと相互に結び付いているため、間接的にDORAに準拠する必要があります。

要点：今後の見通し

- 細かい部分に落とし穴が隠れています。DORAのレベル2の詳細な技術仕様は2024年7月に最終決定されました。テクノロジーの出現や変化に伴い、規制がさらに追加されることが予想されます。
- DORAの規定に準拠し、企業のコンプライアンスをサポートできると思われる**「DORA対応」ソフトウェアやサービス**を提供する情報通信技術（ICT）サプライヤーを見つける必要があります。
- DORAが義務づけるリスク評価のチェックリストに適合できない**サードパーティの金融サービスベンダー**は、銀行やその他の金融機関にサービスを提供する資格を失う可能性があります。その結果、金融サービス機関は必要なサービスの確保に奔走することになったり、承認されたサプライヤーの数が減ることで有利な契約条件の交渉が難航したりする可能性もあります。

詳細：注目すべきEU規制

2023年デジタルオペレーショナルレジリエンス法（DORA）

対象： EUの全ての金融サービス機関とそのサードパーティの情報通信技術（ICT）サービスプロバイダー

施行： 2022年12月に発行され、2023年1月に施行されました。組織は、2025年1月17日までに準拠する必要があります。

DORAにより、EUの金融セクター全体のデジタルオペレーショナルレジリエンス、リスク管理、セキュリティ、およびインシデント報告が調和します。

この規制は、デジタルリスク管理、ICT関連インシデント、デジタルオペレーショナルレジリエンステスト、サードパーティリスク管理、情報共有の5つの分野で要件が定められています。

DORAはEUの金融セクター全体のデジタルオペレーショナルレジリエンス、リスク管理、セキュリティ、インシデント報告を調和させる規制です。

DORAは、ICTリスクを管理するためのガバナンスとコントロールのフレームワークを構築および使用することを企業に義務付けており、例えば、TIBER-EUなどの脅威インテリジェンスベースの倫理的なペネトレーションテストを実施したり、サードパーティとの契約内に標準化された条項を挿入してサイバーセキュリティの強力なエビデンスを要求したり、サードパーティのICTリスクを継続的に監視する必要があります。

DORAの比例原則では、金融サービス機関は、組織の規模、活動、およびリスクレベルに応じて、比例的にDORAの要件を適用できると規定されています。

DORAの違反に対する罰則には、EU加盟国の現地の法律や規制に基づく制裁が含まれる場合があります。重要サードパーティは、コンプライアンスに違反した場合、罰則が科せられ、金融サービス機関との連携が困難になる可能性があります。

EUにおけるその他の金融サービス規則に関する注記

- EUのクライアントの間で注目を集めているのはDORAだけではありません。**EU全体における高い共通レベルのサイバーセキュリティ対策に関する指令である**NIS2も、盛んに議論されているトピックです。なお、金融サービスクライアントにとっては、NIS2について過度に心配する必要はないでしょう。なぜなら、NIS2の規定はDORAにより置き換えることができるからです。
- **TIBER-EU**は、脅威インテリジェンスベースのEthical Red Teaming（倫理的なレッドチーム演習。つまり、実際の攻撃者の手法を模倣しながらも、倫理的かつ制御された方法で組織のサイバー耐性を評価するペネトレーションテスト）のフレームワークで、制御されたサイバー攻撃を協力して実施してレジリエンスをテストするための、当局、金融サービス機関、脅威インテリジェンスの専門家、およびレッドチームプロバイダー向けのガイダンスです。DORAでは、TIBER-EUまたはそれと同等のペネトレーションテストスキームの使用を義務付けています。

DORAコンプライアンスへのアプローチ方法

DORAはチェックリスト型の規制ではありません。DORAは、サイバーセキュリティとレジリエンスに対する包括的なアプローチであり、IT部門やサイバー部門だけでなく、ビジネス部門も注目する必要があります。

最も重要な業務領域を特定してマッピングするには、全社的な取り組みが必要になります。経営層（C-suite）を含む全てのレベルで、重大なランサムウェア攻撃を受けて業務が停止した場合に何が起こるかを考える必要があります。「財務や事業、そして地域・国内・EU全体の金融セクターへの影響は？」

こうした問いに答えるには、最悪の事態を想定し、今すぐそれに対する計画を立てる必要があります。DORAのレベル2は広範囲で詳細な仕様のため、金融サービス機関は、コンプライアンスに対してリスクベースのアプローチの採用を検討するべきです。

- 企業全体のサイバーリスクとレジリエンスリスクについて、サードパーティベンダーによってもたらされるリスクも含めて評価します。
- ダウンタイムと取引損失の許容限度、およびその件数や金額について議論を始めます。
- 脅威インテリジェンスに基づく倫理的なレッドチーム演習（TIBER-EU）のペネトレーションテストについて十分に理解します。

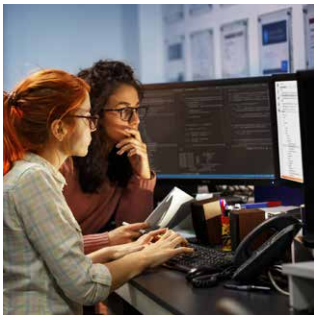
DORAを戦略的プロジェクトとして捉えるほか、サイバーセキュリティプログラムを包括的に強化する機会として考えることで、これまでとは異なるアプローチを検討してください。

セキュリティ監視およびセキュリティオペレーションセンターは、効率的かつ効果的に対応できるように適切に設定されていますか？　攻撃やその他の障害に対して長期的な被害を最小限に抑えられる自信が得られるまで、テストや再テストを繰り返すことが重要です。

また、他の企業と連携して相互にテストを行うことも検討してください。実際、EUの主要銀行11行は、特定の攻撃が銀行システム全体に与える影響を理解するためのワーキンググループを結成しています。この取り組みが成果を出すには時間がかかるかもしれませんが、非常に有望なスタートとなります。

PwCによる詳細はこちら：

デジタルオペレーショナルレジリエンス法（DORA）：金融機関が今守るべきこと



攻撃やその他の障害に対して長期的な損害がほとんどまたは全くなく対処できるという完全な自信が得られるまで、テストや再テストを繰り返します。

中東

概要：規制の現状

中東諸国は最近、サイバー犯罪だけでなく世界標準に追いつきたいという願望を背景に、数多くのサイバーフレームワークやデータ保護フレームワークを採用しています。

「フレームワーク」という言葉に惑わされないでください。少なくともサウジアラビア王国（KSA）では、フレームワークの文書はガイダンスの範囲を超えています。これらのフレームワークは、サウジアラビア中央銀行（サウジアラビア通貨庁：SAMAとも呼ばれる）によって厳格に適用される義務事項であり、違反した場合は厳しい罰則が科せられます。

制定された規制リストは長く、クラウドコンピューティング、IoT（モノのインターネット）、暗号化、暗号通貨、電子決済、アウトソーシングなどのトピックをカバーしています。また、カタール、アラブ首長国連邦（UAE）、バーレーン、エジプト、オマーンなどの中東諸国の中では、サウジアラビア王国（KSA）が先駆的です。サウジアラビアの規制当局は現在、データプライバシー／保護と不正行為という2つの課題に焦点を当てています。

プライバシー規則を推進する理由は何でしょうか？　他の多くの国と同様、EUの加盟国や組織とビジネスを行いたいという願望も一部にあります。一方で、サウジアラビア政府は、外国企業投資やその他の資源に対する同王国の魅力を高めたいとも考えています。

48%

経営幹部の48%が、データ保護およびデータ信頼性を今後1年間のサイバー投資最優先事項に掲げています。

出所：PwC 2025 Global Digital Trust Insights

サウジアラビアは、強力なセキュリティ対策によって達成される徹底的なデジタルトランスフォーメーションを含むVision 2030プログラムに沿って最新化を進めており、同国の金融サービス企業にも同様のことを求めています。2023年9月に施行されたサウジアラビアの個人データ保護法は、EUのGDPRに厳密に準拠していますが、コンプライアンス違反の場合、懲役刑を含むより厳しい罰則が科せられます。

不正行為の撲滅

サウジアラビアでは、不正行為に対する懸念が高まっています。誰もが知り合いに、銀行口座やクレジットカード番号、その他の認証情報の入手を試みる不正行為者からの音声フィッシング（「ビッシング」）の電話を1回以上受けた人がいると思われます。サウジアラビアの金融ニュースサイトの「Argaam」によると、サウジアラビア中央銀行（SAMA）の報告では、2021年にサウジアラビア国内で適切な本人確認なしにリモートで開設されたアカウントが約484万件あり、これはリモートで開設されたアカウント全体の半数以上に相当します。サウジアラビア中央銀行（SAMA）のレポートによると、金融サービス企業のコントロールに数多くの欠陥が特定され、不正行為の蔓延に寄与していると考えられます。

フィッシング詐欺も、ログイン情報やその他の情報を取得するために設計された偽のWebサイトと同様に、よく使われる手法です。

非常に多くのケースで、消費者は、アカウントにアクセスして金銭を盗むために必要な情報をこれらの詐欺師に提供しています。銀行はこれらの損失を補填しない傾向があり、顧客がその損失を負担する必要があります。一方で、サウジアラビア中央銀行（SAMA）は不正行為の特定方法や回避方法について、アカウント所有者を教育する責任は企業側にあると定めています。

多くの銀行では、主にソーシャルメディアを通じて、顧客を対象とした不正防止啓発キャンペーンを実施し、顧客の質問や懸念に答えられるように銀行職員を訓練しています。一方で、サウジアラビアで最近施行された不正対策フレームワーク（CFF）では、金融サービス企業に対して、不正対策の導入、および毎年の不正リスク評価を義務付けています。

コラボレーションの文化

金融機関のセキュリティを確保することは決して簡単なタスクではありません。詐欺師やハッカーは金銭を盗もうと考えていますが、国家レベルの脅威アクターの場合、経済全体に損害を与えようとしている可能性があります。サウジアラビア中央銀行（SAMA）のサイバー不正対策フレームワークは2022年10月に制定されましたが、組織は2023年7月1日までに成熟度レベル3を達成する必要があり、この新しい規則に準拠するまでの時間枠が極めて短期間であったことも加わり、サウジアラビアのCISO（最高情報セキュリティ責任者）らは、互いに支援を求め合っていることも無理はありません。

サウジアラビア全体の金融サービスのCISOらは、競合他社と毎週ミーティングを行い、サイバー問題とテクノロジーについて話し合い、何が効果的で何が効果的でないかについて共有しています。サウジアラビアが世界標準に追いつくために取り組む中、同国の金融サービスのCISOらは、コラボレーションが実際にどのように機能するかを外部の私たちに示しています。

要点：今後の見通し

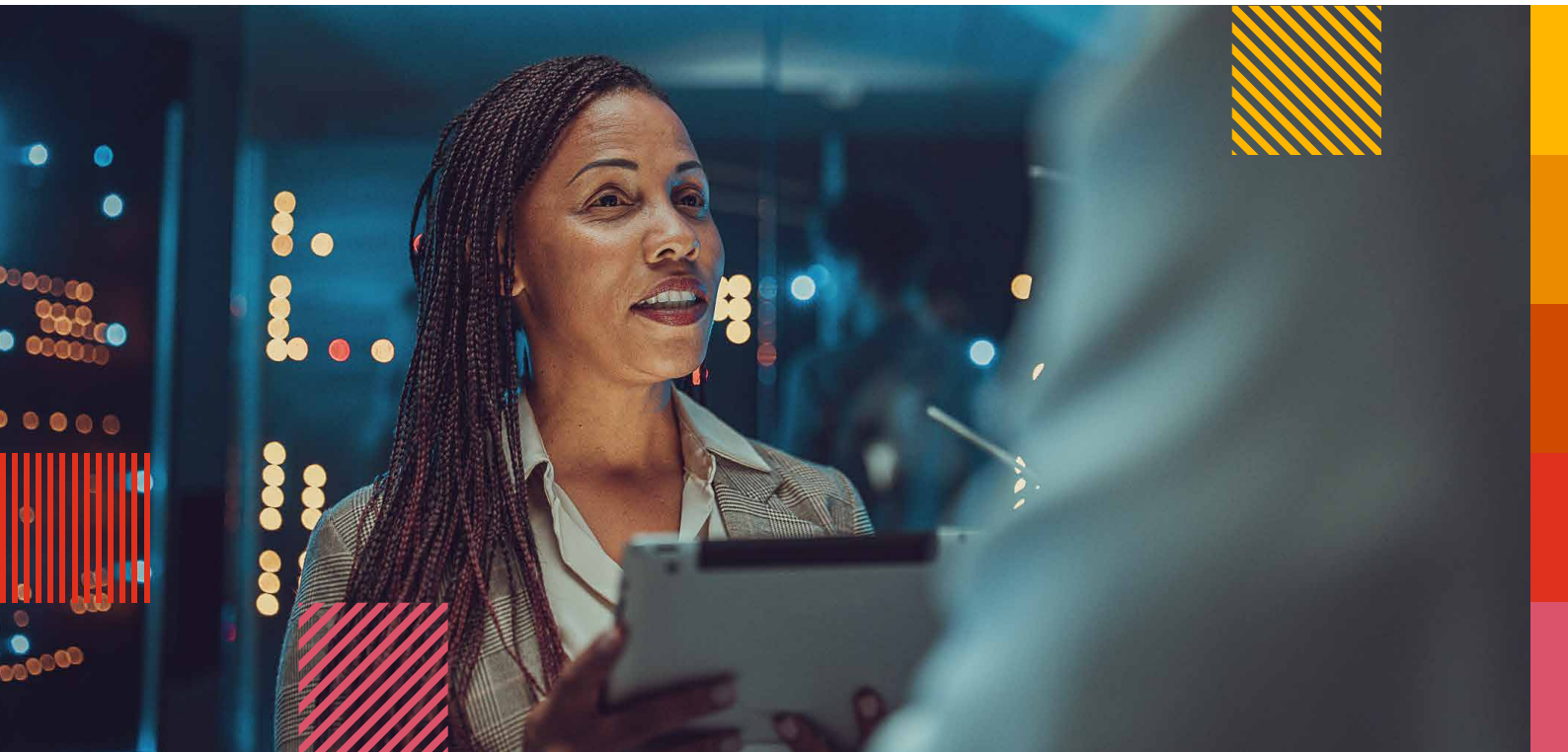
中東は、サイバーセキュリティの基準を引き上げるために前進を続け、世界的な動向に注視しながら、金融サービス機関に対する要求を増やすと思われます。

- **デジタルバンキング。**世界的にデジタル専業銀行の人気が高まるのに伴い、サウジアラビアはデジタル専業銀行の実現とセキュリティ確保に注力することは確実です。同政府は国境を越えたデータ転送に反対のスタンスであり、大半の組織に対してサウジアラビア内にホストされているクラウドプロバイダーのみ使用するよう要求しており、このことが課題となっています。近い将来、サウジアラビア中央銀行（SAMA）は、デジタルバンキングを促進できるように、データフローとデータ共有のセキュリティとプライバシー管理に焦点を当てる可能性があります。

- **レジリエンス。**サウジアラビア中央銀行（SAMA）は、金融サービス企業に対して、2017年までさかのぼって、主にガバナンス関連のコントロールに焦点を当てて、事業継続マネジメントフレームワークに準拠するよう求めています。また、銀行に対して、災害復旧の演習を毎年実施して、混乱後の回復能力をテストするよう義務付けています。

  一方で、サウジアラビアやその他の中東諸国では、EUのデジタルオペレーショナルエクセレンス法（DORA）のような、デジタルやオペレーショナルレジリエンスに特化したフレームワークや規制がありません。世界的なトレンドへの追随を強めるサウジアラビアの傾向を踏まえると、サウジアラビア中央銀行（SAMA）や他のサウジアラビア政府機関が、今後数年の間にレジリエンスの枠組みを作り出しても驚くことはありません。

- **サードパーティリスク管理。**銀行は、ITおよびセキュリティサービスをアウトソーシングする傾向があるため、関連するリスクの管理は必須となります。しかし、多くの銀行はこれをうまく行えていません。サウジアラビア中央銀行（SAMA）では、サードパーティリスク管理の枠組みを準備しています。



詳細：注目すべき金融サービス規制

個人データ保護法（PDPL）

規制当局：サウジ・データAI庁（SDAIA）

状態：2023年9月から有効。コンプライアンスの適用は2024年9月から開始。

対象：サウジアラビアの居住者の個人データを処理する公的機関または民間組織（これらの組織が存在する場所は問わない）。

サウジアラビア初の消費者データプライバシー法は、居住者のデータのプライバシーを保護し、データの共有方法と共有相手を規制することが目的です。個人データ保護法（PDPL）は、EUの一般データ保護規則（GDPR）に厳密に準拠しており、データの収集と使用に消費者の同意を求め、データの最小化を義務付け、データ管理者の責任を設定し、データ主体の権利を規定し、違反に対する罰則を設定しています。

個人データ保護法（PDPL）はGDPRとは異なり、ほとんどの場合、サウジアラビア内で個人データを保管し処理することを管理者に義務付けています。UAEにも同様の規制があります。

重要なポイント：個人データ保護法（PDPL）の全ての要件を満たしながら組織の顧客体験の品質を維持するには、多くの場合、データ管理責任者が監督するデータプライバシーチームを設立する必要があります。

この取り組みは簡単でも安価でもありません。私たちは、今すぐ個人データ保護法（PDPL）のコンプライアンスの整備に着手するか、すでに開始している場合は、個人データ保護法に伴う現実的な見解を確認することをお勧めします。

不正対策フレームワーク

規制当局：サウジアラビア中央銀行（SAMA）

状態：有効

対象：サウジアラビアで事業を行っている全ての金融サービス企業

このフレームワークには3つの目標が明記されています。具体的には、1）リスクに対処するための共通のアプローチを作成すること、2）不正対策の適切な成熟度レベルを達成すること、3）不正行為リスクが適切に管理されることを保証することです。

また、不正行為の検出、不正行為の防止、対応と修復、ガバナンスの4つの領域のコントロールが規定されています。サウジアラビア中央銀行（SAMA）はこのフレームワークを使用して、金融サービス会社の成熟度レベルを判断し、不正対策を評価します。このフレームワークでは、規制対象事業体に対して、下記を行って、2023年7月1日までに成熟度レベル3（最高は6）を達成することを求めています。

- 不正対策のコントロールが定義、承認、実装されている
- 不正行為検出システム
- これらのコントロールのパフォーマンスの監視と報告

重要サイバーセキュリティコントロール（ECC-1：2018）

規制当局：国家サイバーセキュリティ庁（NCA）

状態：有効

対象：サウジアラビアの全ての政府組織、および金融サービス企業を含む重要な国家インフラ組織

この包括的なサイバーセキュリティ規制は、サイバーコントロールの機密性、可用性、および完全性を確保することを目的としています。また、5つのドメイン（ガバナンス、防御、レジリエンス、サードパーティとクラウド、および産業用制御システム）と29のサブドメインの中に114のコントロールが規定されています。これらは全て国内法、国際法、および各規制に関連付けられています。

PwCによる詳細はこちら：

サウジアラビア王国のサイバーセキュリティコンプライアンスハンドブック

アジア太平洋

私たちは金融サービス業界のCISOに対し、競争を意識するのではなく、協力する姿勢を持つようにと助言することがよくあります。その規範を探している方は、アジア太平洋（APAC）地域で優れたモデルを見つけることができるでしょう。

コラボレーションのメリットは非常に強大です。同僚が対処している脅威に気付いていれば、自社のシステムやネットワークで何を探せばよいか事前に分かります。

サイバー侵害の試みを検知・対応する上で効果的だったことや効果的でなかったことを同僚から聞いておけば、攻撃者から自分の組織を狙われても、優位に立つことができます。他のCISOと対話すれば、規制遵守の準備が整うほか、規則が策定される過程でその形成に貢献することもできます。

このような協力モデルは、金融サービス企業が攻撃の集中砲火に対処しているアジア太平洋地域（APAC）でうまくいっています。シンガポール、香港、日本では、CISOたちは同僚や規制当局と定期的に会合を開いています。彼らが集まるのは、新たな脅威や現在の脅威、脅威の主体とその戦術、攻撃を発見・阻止するソフトウェアやテクノロジー、コンプライアンスの詳細などについて話し合うためです。

こうした協力にもかかわらず、APAC地域の規制の特性は管轄によって異なります。この地域では「画一的な」規制の概要ではうまくいかないでしょう。

中国はデータのセキュリティに注目し、データを国内に留めることを重視しています。香港とシンガポールでは、オペレーショナルレジリエンスが規制当局の間で重要な焦点となっています。日本は、増加する詐欺攻撃と闘うことに注力しながら、サードパーティリスク管理にも照準を合わせています。

規制のアプローチも異なります。中国は、違反すれば重い罰則を伴う厳格な規則を課しています。シンガポールの規制当局も厳しい傾向にあり、例えば銀行のデジタルサービスについては、ユーザーに過失があっても、ユーザーを詐欺から守る責任を銀行に責任を負わせます。

香港と日本の規制当局は、監督対象の企業をより信用する傾向があります。両国の金融サービスサイバーガイドラインは、必須でありながら規定よりも原則を明確にしています。それらのガイドラインでは、ビジョンを定め、企業に対してデータ、システム、ネットワーク、アカウントのセキュリティを確保するよう指示しますが、そのビジョンをどのように実現するかという個別の判断はほとんど企業に委ねます。

概要：規制の現状

中国で事業を展開する多国籍金融サービス企業は、3つの重要なデータプライバシー指令が自社にどのような影響を及ぼすか分からない状況にあり、不確実性に包まれています。

現在、中国では2つの規制（1つはすでに施行済み、もう1つは草案段階）があり、企業に対してデータセキュリティ監査の実施を求める可能性があります。

また、外国資本の企業に対しては、システムや顧客データを処理する人材を中国国内に置くことが求められ、中国で生成されたデータは中国国内に留めるよう義務付けられる可能性もあります。

他方、外国銀行は、中国の顧客データを処理やその他の目的で引き続き国外に送信できるかどうかについて、**中国国家インターネット情報弁公室**（CAC）の決定をいまだに待っています。

外国銀行は世界第2位の経済大国で存在感を維持したいと考えていますが、特に景気減速の中で彼らの利益は圧迫されています。CACが越境データ移転（CBDT）申請を拒否した場合、外国銀行はジレンマに陥る可能性があります。以下に示す中国の個人情報保護法のCBDT条項、サイバーセキュリティ法、およびデータセキュリティ法により、年間100万人以上の中国国民の個人データを取り扱う組織がそのデータを国外に送信するには、2023年3月1日までに許可を申請する必要ありました。CACは各申請者が提出した資料を審査し、45日以内に決定を下すと述べました。

CACが発表した情報によると、2023年8月までに1,000社を超える企業がCBDT評価を申請し、15社が最終回答を受け取りました。その中に外国銀行は入っていません。

他の分野では、CBDTの取り決めの変更を求められている申請者もいます。その結果、一部の大手外国銀行は、自社も中国での事業や業務に関するデータをホスティングする戦略や準備の変更あるいは調整が求められるのではないかと懸念しています。

これらの企業は、中国では概してわずかな利益しか上げていないため、自社のデータ処理業務全般を中国に移転するために必要なリソース（人材、プロセス、テクノロジー）の投入を躊躇するかもしれません。

要点：今後の見通し

- **「中国人民銀行の業務分野におけるデータセキュリティ管理弁法」**と**「個人情報保護コンプライアンス監査管理弁法」**が採択・確定されると、中国でよくあるように、銀行が**遵守するまでの猶予期間が1年未満**となる可能性があります。企業は、近いうちに監査が必要になると想定しておくのが賢明でしょう。したがって、企業は法案で提案されている範囲をよく理解し、自己評価、ギャップの埋め合わせ、その他の予備手段によって今から準備を始めるべきです。
- CBDTに関しては、2024年3月22日に発表されたPIPL修正条項に基づき、1万人未満の個人のデータをエクスポートする銀行には救済措置が講じられます。**越境データフローの規制および促進に関する規定**により、これらの銀行はCBDTシナリオの一部が免除されています。

詳細：今注目すべき規制

越境データ移転、個人情報保護法（PIPL）

規制当局：CAC

状況：有効

対象：中国の個人情報の処理、管理、越境移転を行う全ての企業

中国国外にある中国国民の個人情報を処理、管理、移転する全ての企業は、特定の移転について中国政府の承認を得る必要があります。この規制にはコンプライアンスの基準が定められており、その基準を下回る企業はセキュリティ評価なしで承認を申請できます。修正案では、年間1万人未満の個人データをエクスポートする組織は、CACの承認や行政申請が免除されます。

中国人民銀行（PBOC）管轄下の業務分野におけるデータセキュリティ管理措置

規制当局：中国人民銀行

状況：2025年6月30日施行

対象：中国の金融サービスデータ処理業者

この措置により、中国の金融サービスデータ処理業者は、自社のデータ資産の目録作成と分類を行うこと、重要データのカタログを中国人民銀行に提出すること、その重要データに関連するリスクを毎年評価すること、そのセキュリティを監視するとともに、脅威インテリジェンスを利用してそのデータに対する脅威を監視すること、独自のデータセキュリティ、データライフサイクルの運用と管理について毎年監査を受けることが義務付けられます。

個人情報保護コンプライアンス監査管理弁法

規制当局：CAC

状況：2025年5月1日施行

対象：中国の個人情報処理業者

この規制案は、個人情報処理者に対し、法律および規制の要件に照らして自社の個人情報処理活動のコンプライアンス監査を定期的に行うことを求める個人情報保護法第54条および第64条を明確にし、専門機関が監査を実施しなければならないと定めています。同案では、1,000万人以上の個人情報を取り扱う事業者には2年に1回の監査、その他の事業者には定期的な監査が義務付けられています。監査は12の分野を対象とし、規制当局は指定された専門組織に監査の実施を要求する裁量権を有します。

PwCの詳細記事はこちら：

中国の新しいデータ移転指令が多国籍企業に迫る市場戦略の見直し

シンガポール

概要：規制の現状

シンガポールの金融サービスセクターでは、オペレーショナルレジリエンスが大きく進展しています。シンガポール金融管理局（MAS）は、このコンセプトを規制の重点分野の1つに位置付けています。

ある銀行のシステム、データ、アプリケーションの全てを単一のクラウドプロバイダーがホストしている場合、そのプロバイダーが攻撃されると、その銀行のサービスは停止してしまう恐れがあります。

MASの事業継続マネジメント（BCM）ガイドライン2022は、金融サービス機関に対し、サイバーセキュリティを超えて、自社のクリティカルビジネスプロセスが何であるか、そしてそれらが全社的にどのように連結しているかを真に理解することを求めています。同ガイドラインが導入を求めるさまざまなセキュリティ対策には、脅威の検出と対応、サードパーティのリスク管理、システムとアカウントの安全なバックアップの維持などがあります。

「集中リスク」も重要な懸念事項です。多くの企業は、テクノロジーサービスの大部分を単一のサードパーティから調達しています。ある銀行のシステム、データ、アプリケーションの全てを単一のクラウドプロバイダーがホストしている場合、そのプロバイダーが攻撃されると、その銀行のサービスは停止してしまう恐れがあります。

MASは、金融サービス企業とシンガポール経済全体のつながりを認識し、外注サービスに関するリスクを管理するための要件をアップデートしています。

顧客を詐欺から守ることも、シンガポール当局が重視する分野です。2022年、MASとシンガポール銀行協会（ABS）は共同で、金融サービス企業に対して、一定の詐欺防止策を実施し、詐欺を見分けて回避する方法について顧客に教えることを求める要件を発行しました。

銀行は、安全でないアプリが搭載されたデバイス上で消費者が自社のバンキングアプリを使用できないようにすることで、自社と顧客を保護しています。

要点：今後の見通し

- **詐欺師**が金融サービスの顧客から口座情報を騙し取ろうと攻勢を強める中、詐欺は今後もMASとABSの監視下に置かれるでしょう。顧客口座の不正利用防止と保護のために当局が適切と考える措置を講じていない銀行に対し、MASはすでに多額の罰金を科しています。

  重要なポイント：詐欺行為を阻止するためにできることを全て行っていることをMASに示すことができれば、詐欺師が顧客口座に侵入することに成功した場合でも、貴社は多額の罰金を回避することができます。私たちは現在、ある大手銀行の包括的な啓発キャンペーンにおいて、印刷物やソーシャルメディア、その他のアウトリーチにより、口座保有者が詐欺を認識して回避できるように支援しています。

- シンガポールの金融サービスシステム全体に影響を及ぼす機能停止を防ぐ取り組みとして、**集中リスク**がより厳格なサードパーティのリスク管理要件をもたらす可能性もあります。

  重要なポイント：サービスプロバイダーについて、その契約内容も含めて、精査を強化してください。例えば、ITサービスを全て1つのクラウド／決済サービスプロバイダーにまとめるのではなく、複数のプロバイダーを使用するなど、集中リスクを軽減する方法を検討してください。

詳細：今注目すべきFSサイバー規制

事業継続マネジメントガイドライン

発行者：MAS

状況：2022年1月現在有効

対象：MAS規制対象の全ての金融機関

これらの必須ガイドラインでは、全てのクリティカルビジネスサービスの依存関係を特定してマッピングすること、クリティカルサービスごとの復旧時間目標を設定すること、集中リスクの軽減策を講じること、脅威の監視、定期的なレジリエンステスト、定期監査など、さまざまな対策が求められています。

貴社のクリティカルビジネスサービスを相互にマッピングし、またそれらの全ての依存関係にマッピングすることは、オペレーショナルレジリエンスプログラムの中で最も複雑かつ困難な部分になる可能性があります。

重要なポイント：貴社のクリティカルビジネスサービスを相互にマッピングし、またそれらの全ての依存関係にマッピングすることは、オペレーショナルレジリエンスプログラムの中で最も複雑かつ困難な部分になる可能性があります。怖がらないでください。一度に1つの領域に忍耐強く取り組んでください。きっと驚きの発見があるでしょう。

外部委託に関するガイドライン

発行者：MAS

状況：有効

対象：MAS規制対象の幅広い金融機関（リテール銀行、ホールセール銀行、保険会社、再保険会社、金融アドバイザー、信託会社、クレジットカード利用者、決済システム運営者など）

同ガイドラインでは、金融機関は少なくとも年に一度、サードパーティのサービスプロバイダーの登録簿をMASに提出することが義務付けられています。リスク評価、サービスプロバイダーの評価、ベンダー契約における特定条項、セキュリティ監視、適切なBCM対策の証拠の取得、サードパーティのセキュリティプログラムの定期的なレビューと監査のためのフレームワークを確立する必要があります。

MASは2022年の情報文書「オペレーショナルリスク管理-外部委託および第三者委託の管理」において、サードパーティの監視とガバナンスの強化、および契約期間全体にわたるコンプライアンスの監視と測定に関するより詳細なガイダンスを提供しています。

PwCによる詳細はこちら：

PwC 最新動向の解説-MAS外部委託に関するガイドライン

デジタルバンキングのセキュリティ強化策

発行者：MASとABS

状況：2022年8月現在有効

対象：全ての金融機関

2022年8月に発表されたこの措置は、シンガポールの金融機関に影響を与える詐欺事件の増加に対処するものです。企業に対し、セキュリティを強化して顧客口座を保護するための措置（消費者教育を含む）を講じるよう求め、詐欺を検出して回避するためのアドバイスを顧客に提供しています。

概要：規制の現状

香港の金融サービスサイバー規制当局にとって、レジリエンスは一番の懸念事項です。

EUのデジタルオペレーショナルレジリエンス法（DORA）のような包括的なレジリエンス法がないため、規制当局は一連の指令を通じて、その多くの原則（サードパーティリスク、事業継続性、サイバーガバナンス）に対応しています。

要点：今後の見通し

- 香港保険業監管局（HKIA）の「サイバーセキュリティに関するガイドライン」は改訂され、2025年1月1日より施行されました。このガイドラインは、キャプティブ保険会社および海上相互保険会社を除く、HKIAの規制対象となるすべての保険会社に適用されます。

  このガイドラインは、香港金融管理局（HKMA）の「サイバー・レジリエンス評価フレームワーク（CRAF）」および米国国立標準技術研究所（NIST）のサイバーセキュリティ基準と類似しており、次の7つの主要領域を網羅しています：ガバナンス、リスクの識別、評価と管理、継続的な監視、対応と復旧、情報共有、トレーニング。

  HKIAは、業界全体を対象とした意見募集を経て提案された改訂内容を反映し、本ガイドラインを更新しました。改訂には、固有リスクおよび成熟度の評価に関する要件が含まれており、固有リスクが中～高水準と判断された保険会社に対しては、脅威インテリジェンスに基づく攻撃シミュレーション（TIBAS）の実施が規制要件として義務付けられています。これらの要件は、HKMAのCRAFにおける要件と非常に近い内容となっています。

  重要なポイント：保険会社は、評価およびギャップの是正に向けた準備を今すぐ開始すべきです。遵守までの猶予期間は、6～9カ月程度と見込まれています。

詳細：今注目すべきFSサイバー規制

サイバー強化イニシアチブ（CFI）2.0英語版

規制当局：香港金融管理局（HKMA）

状況：2020年に更新、段階的な導入アプローチ

対象：HKMA認可機関（AI）

2016年のサイバー強化イニシアチブの今回の更新内容

- **サイバーレジリエンス評価フレームワーク（C-RAF）。**AIが各自のサイバーレジリエンスをより深く理解、評価、強化し、継続的に改善するために役立つ、リスクベースのサイバーセキュリティ成熟度評価フレームワークです。

  C-RAFは、固有リスク評価、成熟度評価、インテリジェンス主導型サイバー攻撃シミュレーションテスト（iCAST）という3つの評価フレームワークで構成されています。

  C-RAFは、全ての銀行およびストアドバリューファシリティ（SVF）決済サービス会社に、固有リスクと成熟度の評価を行うことを義務付けています。当該企業は、C-RAF評価基準に基づいて高程度または中程度の固有リスクがあると判断された場合、iCASTテストも行う必要があります。

- **サイバーセキュリティ情報共有プラットフォーム。**これによってAIは、迅速な防御と措置に役立つサイバー脅威インテリジェンスを交換することができます。

- **専門能力開発プログラム。**C-RAF評価とiCASTの実行に必要なサイバーセキュリティのトレーニングと認証について定めたものです。

バージョン2.0（2020年11月リリース）は、サイバーリスク管理がシステムとオペレーションの重要な部分であることを保証するため、取締役会と上級管理職に責任を持たせることに重点を置いています。

アップデートの中でも特に求められているのは、サイバーセキュリティに対する階層化された多層防御アプローチ、継続的な検出と対応、エンドポイントの行動検出、クラウドセキュリティなどのより高度なサイバーセキュリティツールの使用、ソフトウェア開発ライフサイクル（SDLC）、アジャイル、DevOpsに関する開発要件の導入、サイバーインシデント対応と復旧の要件の強化、サードパーティのサイバーリスク管理です。

重要なポイント：このアップデートは数年前に発効しましたが、金融サービス企業のコンプライアンスは十分でないと思われます。成熟度の自己評価は、例えばエンドポイントや侵入の試みを検出する企業の能力に関して、iCASTテストの結果を反映しない場合があります。

PwCによる詳細はこちら：

HKMAサイバーセキュリティ強化イニシアチブ2.0

セキュアな3次データバックアップ（STDB）

規制当局：香港銀行協会

状態：2021年制定

対象：高リスク銀行

システムを機能不全に陥らせるランサムウェア攻撃の増加も、香港銀行協会がHKMAの承認を得てこれらの高レベルの原則に基づく要件を発行した動機の1つです。

システムを機能不全に陥らせるランサムウェア攻撃の増加も、香港銀行協会がHKMAの承認を得てこれらの高レベルの原則に基づく要件を発行した動機の1つです。この通達の解釈に銀行は今なお苦慮しており、一次および二次のリポジトリが侵害されたりアクセス不能になったりした場合に備え、特定の情報の「第三のコピー」を保持することが求められています。対象となる機関にはすでに通知が行われており、現在は「何を」「いつ」バックアップすべきかを判断する段階にあります。

重要なポイント：毎年実施している業務影響分析（Business Impact Analysis）の結果を出発点として、STDB（Secondary to Tertiary Data Backup）戦略を策定しましょう。自社の業務にとって重要なシステムとデータを特定し、それらを確実にバックアップしてください。また、第三のバックアップから迅速に復旧できるかどうかをテストし、顧客サービスの中断を最小限に抑えられるよう備えておくことが重要です。

サイバーセキュリティのガイドラインと通達

規制当局：証券先物委員会（SFC）

状況：有効

対象：証券会社、仲介会社、資産運用会社

インターネット取引に伴うハッキングリスク軽減ガイドライン

認可法人向け通達：インターネット取引におけるサイバーセキュリティのレビュー（2020年9月23日）

認可法人向け通達：オンラインの証券仲介、販売、助言サービスのレビュー（2022年8月31日）

主な重点分野には、サイバーセキュリティのガバナンスと監督、インフラのセキュリティ管理、そして2要素認証（2FA）、監視および監視統制、取引執行に関する顧客への迅速な通知による顧客のインターネット取引口座の保護などがあります。

この通達には、原則に基づくガイドラインの遵守に関する詳細な解説と最新情報が記載されています。全て必須です。

監督方針マニュアル：電子バンキングのリスク管理

規制当局：香港金融管理局（HKMA）

状況：有効

対象：全ての認可機関（AI）

HKMAは、電子バンキングには固有のリスクが伴うものと認識してリスクベースのアプローチでリスク管理を行い、ガバナンスの説明責任を定め、新規サービスまたは大幅に変更した既存サービスの開始前の侵入テストと評価、顧客の認証、通知、保護、教育、システムおよびネットワークのセキュリティと制御、詐欺およびインシデントの管理、事業継続性、レジリエンスなどに関するガイダンスを提供しています。

電子バンキングサービスのセキュリティ強化

規制当局：香港金融管理局

状況：有効

対象：全ての認可機関（AI）

2023年10月31日に発出された本通達は、電子バンキングサービスのセキュリティ強化に向けた新たな措置を義務付けています。これには、動的な不正監視、疑わしい電子バンキング活動が検知された際の「アンブッシュ（奇襲型）認証」、および高リスクと判断された取引に対する追加の顧客確認が含まれます。

概要：規制の現状

20%

サイバーセキュリティ規制は、技術革新と変革の取り組みで安全策を確立する組織の20%に役立っています。

出所：PwC 2025 Global Digital Trust Insights

金融サービス企業が自社のITサービスを外部企業に著しく依存している日本では、サプライチェーン攻撃が規制当局の焦点となっています。規制当局はこれに注目し、オンボーディング前から契約終了後まで、徹底したデューデリジェンスを求めています。

日本の規制環境は主に原則に基づいています。規制当局は一般に、組織は規則に従うものと信じており、通常、特に金融サービス（FS）分野において組織はサイバー、情報セキュリティ、プライバシーに関する規則に従います。

しかし、FSのサイバーセキュリティを規制する国内法がある数少ない国の1つです。これは原則に基づいていますが、日本の財務省が設立した非営利団体である金融情報システムセンター（FISC）の付属ガイドラインには、より詳細で規範的なガイダンスが記載されています。

日本では2003年から個人情報保護法も一部施行されています。この法律は3年ごとに改正され、直近では2023年に改正されました。改正内容は、欧州連合（EU）の一般データ保護規則（GDPR）などの世界的なデータ保護規制とほぼ一致しています。

また、日本においては、金融庁が主導となり、金融分野におけるサイバーセキュリティ対策の強化が進められています。

2024年10月6日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に関するガイドライン」では、監督指針などにおいて概要的な記載であったサイバーセキュリティに関する内容が具体化・明確化されました。

このガイドラインにおいてはサイバーセキュリティの観点から見たガバナンス、特定、防御、検知、対応、復旧、サードパーティリスク管理に関する事項が記載されています。これらは米国の非営利団体であるCRI（Cyber Risk Institute）が公表した新たなサイバーセキュリティ評価ツールである“CRI Profile”のFunctionと対応しており、金融庁はCRI Profileとの整合性を意識していると考えられます。

『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』の構成	米国“CRI Profile”における7つのFunction
2.1 サイバーセキュリティ管理態勢の構築	ガバナンス（GOVERN）
2.2 サイバーセキュリティリスクの特定	特定（IDENTIFY）
2.3 サイバー攻撃の防御	防御（PROTECT）
2.4 サイバー攻撃の検知	検知（DETECT）
2.5 サイバーインシデント対応及び復旧	対応（RESPOND）
	復旧（RECOVER）
2.6 サードパーティリスク管理	拡張（EXTEND）

- 本ガイドラインは、金融庁がこれまで金融機関に対して実施してきた、サイバーセキュリティ検査・モニタリングの結果、金融セクター内外の状況変化を踏まえて策定されています。策定の背景には以下のような状況があります。
  - 金融市場のグローバル化によるグローバルガバナンスの重要性の高まり
  - 海外当局サイバーセキュリティ関連規制やガイドラインへの対応の複雑化
  - 従来の監督指針やモニタリング手法によるサイバーセキュリティ強化の限界
- 特に1点目・2点目に関して、海外展開を行う日本の金融機関は各国における規制やガイドラインを順守する必要があります。CRI Profileは各国の金融当局のサイバーセキュリティ規制・ガイドラインとのマッピングも提供しており、各海外当局の考え方も踏まえた構成となっています。金融庁はこれを参考とすることで、日本の金融機関がこのガイドラインを通じ、海外規制まで把握できるようにすることを1つの狙いとしていると考えられます。

要点：今後の見通し

- 金融分野におけるサイバーセキュリティ対策を強化する方針（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（Ver. 3.0））が発表された結果、金融庁による**監督監視活動および演習の強化。**
  - 金融庁は、特に日本のメガバンク3社を対象に、リスクベースのアプローチを用いて検査と監視を行うでしょう。彼らは、銀行が脅威の変化にどう対応しているか、また他の金融サービス機関で特定されたサイバーベストプラクティスをうまく採り入れているかを調査します。さらに金融サービス機関が自社の成熟度を評価し、自社のサイバーセキュリティ態勢を自律的に改善する場合に役立つサイバー自己評価ツール（CSSA）を開発しました。

先日行われた金融庁の「金融業界横断的なサイバーセキュリティ演習（Delta Wall VIII）」では、165の金融機関や企業がテレワーク環境に対する攻撃への対応を改善する方法を学びました。金融庁はDelta Wallを年1回実施し、2022年の演習の**概要と結果**を公表しています。

■ 日本の金融サービス分野では、**サードパーティリスク管理（TPRM）**が規制当局の注目を集めています。

2022年5月に成立した「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）」は、「国家安全保障に関連する経済的取り組みを推進する」ことを目的としています。起草段階にある条項もありますが、TPRMとサプライチェーンのリスク管理に対応する「重要製品の安定供給を確保するためのシステム」条項は2024年5月に施行されました。

この法律は「特定社会基盤事業者」、いわゆる重要インフラに適用されます。これらの企業は、特定の重要なITシステムを開発したり、ITシステムの運用を外部委託したりする場合、開発や外部委託に関わるサプライチェーンのサイバーセキュリティリスクを低減するために適用するセキュリティ管理策を記載した計画を作成し、関係当局に提出して承認を得る必要があります。

また、第三者と契約変更の交渉をする必要もあり、場合によっては別の第三者の管理と監視を要求することも必要です。の管理と監視を要求することも必要です。

PwCによる詳細はこちら：

海外金融機関におけるサプライチェーンサイバーリスク管理の最新動向 | PwC Japanグループ

- 日本の金融機関ではオペレーショナルレジリエンスへの対応が進められています。金融庁は2023年4月に「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」に関するディスカッションペーパーを発行しました。

  オペレーショナルレジリエンスとは、既存のリスク管理やBCPなどの未然防止策を尽くしてもなお、業務中断は必ず起こることを前提に、利用者目線で代替手段等を通じた早期復旧や影響範囲の軽減を担保する枠組みを指します。2021年3月にバーゼル銀行監督委員会が国際原則を策定したことを皮切りに、日本の各金融機関においても対応が進められています。

  金融機関はまず重要な業務を特定し、その業務が維持すべき水準（耐性度）を設定した後、その耐性度を実現するためのリソースを確保することが求められます。この際に重要となるのが、「顧客」「自行」「社会・市場」の3つの観点です。オペレジにおいてはこの3つの観点から、顧客の生活・自行の金融システム・市場経済等へのサービスの提供途絶の影響を極力一定の範囲内に収めることが重要であるとされています。なお、オペレーショナルレジリエンスにおいては耐性度を実現する方法として、システムの早期復旧だけでなく、代替手段を用いた対応も視野に入れる必要があります。

- 金融庁は、耐量子計算機暗号（Post-Quantum Cryptography、PQC）への移行に向けた検討会を開催し、その報告書（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報告書）を公表しています。本報告書では、PQCへの移行を検討する際の推奨事項、課題および留意事項について取りまとめており、海外の動向についても調査しています。日本では、PQCへの移行スケジュールがまだ公表されていませんが、本報告書では各国の動向を踏まえてPQCの使用開始時期は2030年代半ばが妥当であるとしており、準備期間は10年を切っています。また本報告書では耐量子計算機暗号に向けた課題として、経営層のリーダーシップや関係者の役割・責任の明確化が重要であること、かつ外部委託先・業界団体・当局との連携が必要であること、さらにはグローバルビジネスを展開している場合、海外の法令・規制を継続的に注視する必要があることを指摘しています。技術面・運用面では、IT資産のインベントリ管理の一部であるクリプトインベントリ（暗号情報の一覧）を整備し、暗号機能の移行を容易にするクリプトアジリティを実現することが重要です。さらに金融分野は重要インフラであるため、PQCに係るリスクなどに関して政府による重要インフラ分野横断的な議論が期待されています。なお、報告書には、預金取扱金融機関とありますが、すべての金融機関に参考となる情報です。

- 金融庁は2025年5月に保険業法の改正を行い、損害保険代理店に対する体制整備義務の強化などに関する事項を追加しました。保険代理店を巡っては、2023年頃から保険金の不正請求や不適切な保険募集など不祥事が相次いでおり、特に代理店に対して十分な監督が実施できていなかったことへ批判が集まっています。金融庁はこうした状況に対し、保険代理店の監督・検査に特化した「保険代理店モニタリング室（仮称）」を設置することを公表しており、保険代理店業務に関する法令順守体制が強化されます。

詳細：今注目すべきFSサイバー規制

金融庁の「金融業界横断的なサイバーセキュリティ演習（Delta Wall IX）」が、2024年10月9日 ～21日 に実施されました。約170の金融機関や企業がテレワーク環境下での対応も含めたインシデント対応能力を改善する方法を学びました。金融庁はDelta Wallを年1回実施し、2024年の演習の概要を公表しています。

総合的な監督指針

発行者／規制当局：金融庁

状態：有効

適用対象：さまざまな金融サービス企業。業態独自のガイドラインがあります。

このガイドラインは、サイバーセキュリティやリスクを含むさまざまな分野で金融庁が金融機関に要求する事項を規定しています。477ページに及ぶ「主要行等向けの総合的な監督指針」（2025年6月）には、オペレーショナルレジリエンスの鍵とされるBCM、電子決済サービスにおけるITシステムリスク、詐欺補償、個人データ保護、非金融銀行のセキュリティなどの項目について記載されています。

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

発行者／規制当局：金融庁

状態：有効、公表日2024年10月4日

適用対象：金融機関など

このガイドラインは、前述の「総合的な監督指針」を補完する内容です。監督指針より具体的な対応事項を記載しています。

金融機関などが一般的に実施する必要のある基礎的事項の「基本的な対応事項」と、インシデント発生に地域社会・経済に大きな影響を及ぼし得る機関などにおいて実践することが望ましい取り組みや、金融庁が把握した先進的な取り組みなどの優良事例を指す「対応が望ましい事項」から構成されています。これらは一律に対応を求めるものではなく、金融機関などが自らを取り巻く事業環境や経営戦略、リスクの許容度等を踏まえた上でサイバーセキュリティリスクを特定・評価し「リスクベース・アプローチ」で取り組むべきであるとしています。

金融機関等コンピュータシステムの安全対策基準・解説書

発行者／金融情報システムセンター（FISC）

状態：有効、2025年3月更新

適用対象：銀行および関連金融機関

金融庁の総合的指針の補足として作成されたこれらの非常に規範的なガイドラインは、金融機関のビジネスの種類と重要性に応じたITセキュリティ対策を詳細に説明しています。金融庁は、日本の金融サービス企業が各社のIT管理プログラムでこれを活用することを期待しています。また、「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」の内容、「特定社会基盤事業者」の対応、オペレーショナルレジリエンスの考え方を反映し、さらに、AIの利用における安全対策を追加しています。

2025年6月に金融庁が公表した「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」「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」の章で、「金融庁の取組み」「TLPTを実施するにあたっての推奨事項」を6項目、さらに「TLPT として望ましい事例、不十分な事例」を記載して、金融機関がTLPTに取り組みやすいように構成されています。さらに「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」の「脆弱性診断及びペネトレーションテスト」の項目で、TLPTの実施が望ましい事項であるとしています。TLPTの詳細については、脅威ベースのペネトレーションテスト「TLPT（Threat-Led Penetration Testing）」をご参照ください。

経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（経済安全保障推進法）（令和4年法律第43号）第3章 特定社会基盤役務の安定的な提供の確保に関する制度

発行者／規制当局：内閣官房

状態：有効、施行日2023年11月17日

適用対象：特定社会基盤事業者など（金融庁指定の金融機関などを含む）

この法律は、4つの制度で構成されており、制度ごとに段階的に施行されています。金融機関などに強く関係がある制度は第3章の特定社会基盤役務の安定的な提供の確保に関する制度です。この制度では、（1）特定重要設備の導入、（2）特定重要設備の維持管理等の委託、に関して金融庁への事前届出が定められています。（1）の特定重要設備に関しては、その設備の供給者と構成設備の供給者からの情報提供が必要であり、（2）の維持管理等の委託では、委託先・再委託先の事前審査への協力が必要です。この制度は、2024年5月17日に制度運用が開始（届出義務の適用開始）されており、事前届出においてベンダー・委託先などの協力が不可欠です。なお、金融庁が、「金融分野における経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度の解説」を公表しており、また「基幹インフラ制度に関する相談窓口」を設置しています。

重要経済安保情報の保護及び活用に関する法律（重要経済安保情報保護活用法）（令和6年法律第27号）

発行者／規制当局：内閣官房

状態：有効、施行日2025年5月16日

適用対象：特定社会基盤事業者等など（金融庁指定の金融機関などを含む）

この法律は、重要度が増している経済・技術分野の経済安全保障における、いわゆるセキュリティ・クリアランス制度の根拠となる法律です。また、既にある特定秘密保護法（特定秘密の保護に関する法律）のセキュリティ・クリアランス制度でカバーする防衛、外交、特定有害活動（スパイ行為など）の防止、テロリズムの防止の4領域に追加する運用となります。この法律で定められる「重要経済基盤」は、「重要経済安保情報保護活用法の運用基準」の中で、「経済安全保障推進法」の「特定社会基盤事業」が例として示されています。そのため、金融機関などもこの法律の対象に含まれます。セキュリティ・クリアランス制度を活用するには、まず、適合事業者としての行政機関からの認定を受ける必要があります。認定は、事業者に対する認定と職員・従業員に対する認定の2種類あり両方の認定が必要です。最初に適合事業者としての認定を受けます。次に、行政機関から重要経済安保情報の提供を受けるために契約を締結します。その次に、行政機関から受領する情報の取り扱いが見込まれる従業者に対して適正評価を実施します。

なお、この法律には、情報漏えいや不正取得に関しての罰則規定があります。

重要電子計算機に対する不正な行為による被害の防止に関する法律及び重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（サイバー対処能力強化法及び同整備法）

発行者／規制当局：内閣官房

状態：有効、施行日2025年5月23日

適用対象：日本国内の基幹インフラ事業者（金融庁指定の金融機関などを含む）

この法律は、サイバー対処能力強化法及び同整備法と呼ばれており、いわゆる「能動的サイバー防御」として広く知られているものです。この法律のポイントは、（1）官民連携の強化、（2）通信情報の利用、（3）攻撃サーバの無害化の3点です。重要インフラ事業者は、特定重要電子計算機の届け出義務があり、それがサイバー攻撃を受けた際に、政府への報告義務があります。この報告を元に、政府が総合的にサイバー攻撃の内容を分析し、幅広い組織に分析結果をフィードバックします。また、分析結果により、通信事業者と連携を行い、攻撃サーバの特定などを実施します。サイバー攻撃により重大な被害が発生する蓋然性が極めて高い場合には、攻撃サーバの無害化を慎重に検討します。なお、整備法は、強化法に適合するように関連法令を整備する法律です。

個人情報の保護に関する法律

発行者／規制当局：個人情報保護委員会（PPC）

状態：有効、施行日2023年4月1日

適用対象：日本国内のすべての組織（金融庁指定の金融機関などを含む）

この法律は、違反に気付いた事業体がPPCに通知すること、日本の個人データの仮名化（マスキング）、個人データを第三者と共有する前にデータ主体の同意を得ること、個人データを国外に送信する場合はデータ主体に通知することを義務付け、データ違反に対する罰則を定めています。補足的ガイドライン（金融分野における個人情報保護に関するガイドライン）には、金融サービスに固有の要件が追記されています。

インド

概要：規制の現状

世界で最も人口の多い国であるインドは、今や世界最大級の相互運用可能なデジタル決済システムを有していると言われています。その一因は携帯電話ユーザーの急増にあり、その数は2017年から3倍以上に増加し、2023年には10億人を超えると予想されています。

しかし、急速な成長には成長痛が伴うことが多く、インドも例外ではありません。インドの金融サービスやその他の重要インフラに対するサイバー攻撃の増加は加速しており、報道によると、インドはサイバー攻撃の標的国家リストの上位にあります。

しかし、インドはサイバー犯罪との戦いで後れをとっていません。議会は2000年にインド初のサイバーセキュリティ法である情報技術法（IT法）を制定しました。

現在、インドの最も重要な金融サービスサイバー規制は、サイバーセキュリティ／レジリエンス、デジタル決済、ITセキュリティガバナンス、IT外部委託リスクという4つの主要分野でサイバー問題に対応しています。また、2023年7月にはデジタル個人データ保護法（DPDP法）が成立し、すでに発効されています。本法に関する詳細な運用ガイドラインも間もなく発表される予定です。

数多の法律と1つの目的

インドの金融サービスサイバー規制アジェンダは、一定範囲の事業体を指導・統治するさまざまな規制当局が関与していますが、焦点は1つに絞られています。それが目的としているのは、新しいテクノロジーの利用を実現・奨励しながら、オペレーショナルレジリエンスとデジタルレジリエンスを促進することです。

サイバーは「チームスポーツ」ですが、実際にそれを実践している金融サービス企業はどれくらいあるでしょうか。企業全体に影響を及ぼすビジネス上の必須事項としてサイバーリスクとレジリエンスに対処するため、クライアントのIT、情報セキュリティ（IS）、事業、経営層、取締役会の各部門が連携してチームを編成するケースはあまり見られません。

インドの新たなサイバー規制は、当初から全ての人を結びつけることを目的としています。ITとISの両部門がセキュリティとレジリエンスの責任を負うという規定がある一方、経営層と取締役会が協力してこれらの問題に取り組むことを求める規定もあります。インドの規制当局は、企業のサイバーガバナンスとポリシーに対する最終的な責任を取締役会に負わせることで、この包括的なアプローチを引き続き奨励しています。

要点：今後の見通し

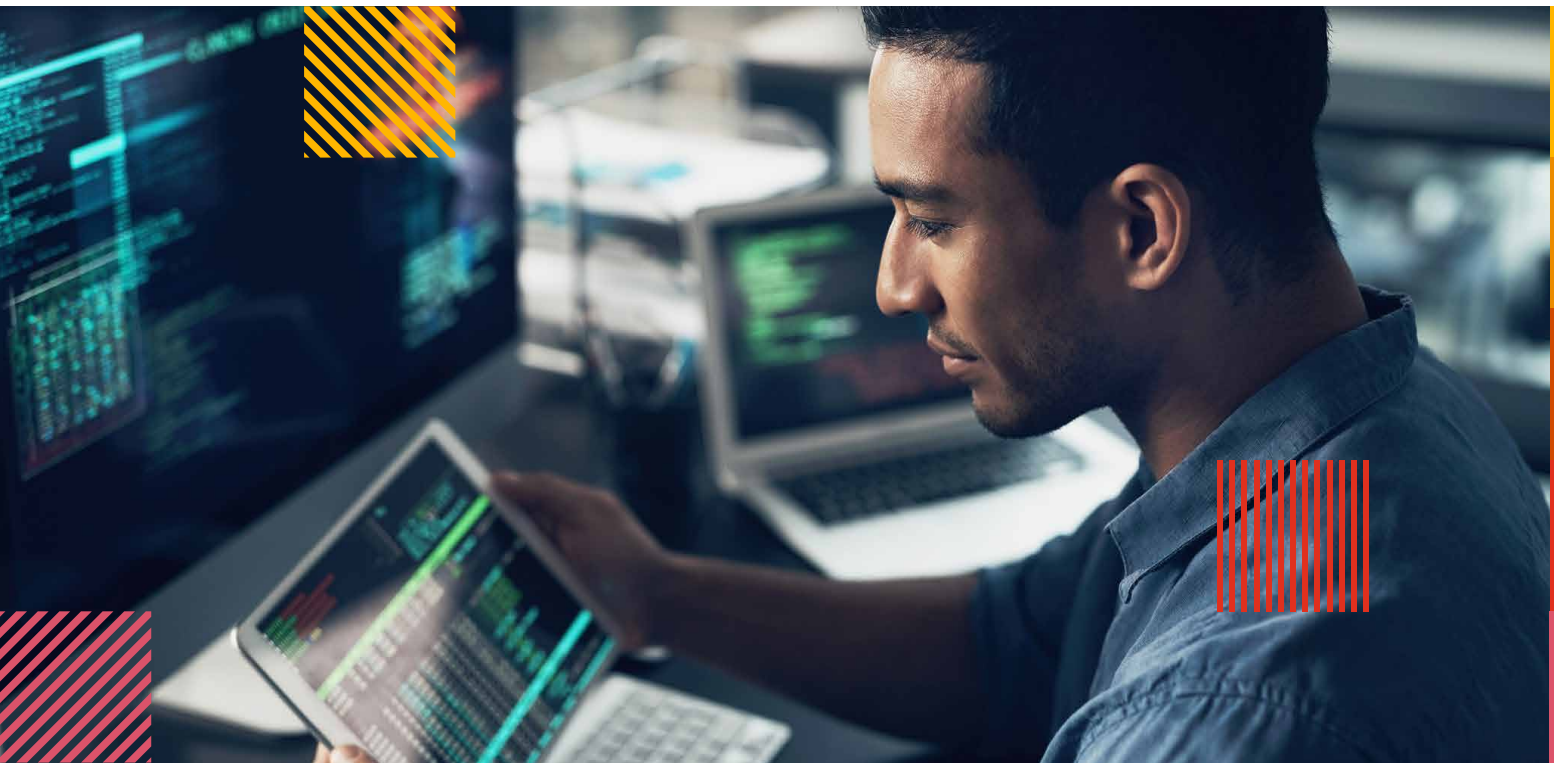
インドの金融サービスサイバー規制アジェンダは、焦点が1つに絞られています。それが目的としているのは、新しいテクノロジーの利用を実現・奨励しながら、オペレーショナルレジリエンスとデジタルレジリエンスを促進することです。

- **インシデント報告**は、世界の他の地域で注目される分野になりつつあり、金融サービスのような重要かつ／または相互連関性のある業界では特に注視されています。インドの規制当局は、データベースや他の情報共有手段の構築に注意を向け、脅威アクターやその手法、インシデント対応など、サイバー攻撃に関する警告をより発信するようになると予想されます。
- **データプライバシー**も、今後さらに厳しく精査されると思われる分野です。デジタル個人データ保護法（DPDP法）は個人データの収集と処理を保護していますが、信用情報機関や保険会社などの企業は、例えばソーシャルメディアのアカウントから情報を収集したり、銀行が提供する資金管理アプリから顧客のライフスタイルに関する洞察を得たりするなど、規則の範囲を超えた活動に従事する場合もあります。

  消費者擁護団体はこうした活動に対して懸念を表明しています。このような情報の収集や使用に歯止めをかける規制ができるかもしれません。
- **デジタル通貨**も、規制当局から目を付けられることはほぼ間違いないでしょう。インド準備銀行（RBI）、インド銀行協会、政府機関が立ち上げたイニシアチブ「e-RUPI」は、商品やサービスの購入に使用できるプリペイドのデジタルバウチャーを提供しています。近い将来、関連するセキュリティおよびデータプライバシー保護規制が制定されると予想されます。
- **クラウド導入**はインドの金融サービス企業の間で急速に広がっています。この背景には、人口知能、ブロックチェーン、エッジコンピューティングなど、テクノロジーの活用における競争があります。この傾向に続いて、クラウドセキュリティとクラウド内のデータセキュリティの強化を目的とした規制ができることはほぼ確実です。2023年3月に発行されたインド証券取引委員会（SEBI）規制対象事業体（RE）によるクラウドサービス導入のフレームワークには、REが使用を認められているクラウドプロバイダーとその他の管理策が定められていますが、今後は銀行や保険会社にも影響を与える詳細な規制が導入されるものと予想されます。

PwCの詳細記事はこちら：

サイバーセキュリティ規制の比較：インド



詳細：今注目すべきインドのFS規制

2023年デジタル個人データ保護法

状態：2023年10月1日現在有効。組織は本法律と規則を順守するにあたり、12～18カ月の猶予期間を与えられると想定されます。

対象：インド国内外でインド居住者のデジタル個人データを収集、処理、保存し、それが商品やサービスの提供に関連している全ての組織。

DPDP法は、国の総合的なサイバーセキュリティ法である情報技術法第43A条に取って代わるものです。その目的は、企業が顧客の個人データを処理する必要性と個人が各自のデータを守る権利とのバランスを取ることにあります。個人情報、機密情報、重要データは区別なく、全て同様に扱われます。他のデータプライバシーおよび保護に関する指令と同様に、下記の項目が定められています。

- **データ収集**
  - 収集目的を明記し、データ主体（データサブジェクト）（DPDP法では「データ主体（データプリンシパル）」）の明示的な同意を得ることを義務付ける
- **処理**
  - データ主体に、データの使用に関する同意の確認や訂正、取消の権利を与える
  - 事業体が個人データをいつ、どのような目的で処理できるかを定める
  - 違反があった場合の通知要件を定める

■ **データの保存と移転**

- 消費者に消去権を与える
- セキュリティとデータ保持に関するルールを定める

■ **透明性／説明責任**

- インドデータ保護委員会を通じて苦情処理のプラットフォームを提供する
- データ受託者または収集者に対し、他の条項の中でも特にデータプライバシー影響評価と監査を義務付ける

■ **データ受託者およびデータ主体の権利と義務**

- データ受託者およびデータ主体の権利と義務、違反した場合の罰金を定める

重要なポイント：この法律の要件を満たしているかどうかを判断するには、データプライバシーとデータ保護の慣行を評価することをお勧めします。必要に応じて管理体制を強化し、コンプライアンスにとどまらず、顧客の個人情報のセキュリティが確保されるよう、できる限りのことを実施してください。

PwCによる詳細はこちら：

2023年デジタル個人データ保護法

決済システム事業者（PSO）向けサイバーレジリエンスおよびデジタル決済セキュリティ管理に関する主な指針

規制当局：インド準備銀行（RBI）

状態：最終文書は2024年7月に発表

対象：カード決済ネットワークや他の非銀行系PSO（決済アグリゲーターやPPI発行体など）を含む決済システム事業者

RBIは、PSOが決済処理を非銀行系テクノロジー企業に外部委託することが多いことに留意して、非銀行系PSOとそのサードパーティが安全かつレジリエンスが担保されていることを保証するため、これらのガイドラインを起草しました。

同ガイドラインは、ガバナンスを含むデジタル決済セキュリティの管理体制を定め、PSOに基本的なITセキュリティ対策および統制を義務付けています。また、その他の対策として、PSOの取締役会と上級管理職が協力してセキュリティとレジリエンスを監督すること、ID管理の統制要件を定めること、アクセスおよびトランザクションの多要素認証を推奨すること、顧客のデバイスのセキュリティを重視すること、セキュリティテクノロジーを勧告すること、「セキュリティ・バイ・デザイン」を重視した設計フレームワークの採用を提唱することを求めています。

重要なポイント：貴社はPSOとして、取締役会と経営陣がITエコシステムのセキュリティとレジリエンスに関して協力していますか。していないなら、今こそ始めるべき時です。まもなく発効する本書の指令をよく理解し、確実に実装するようにしてください。貴社がPSOであれば、規制対象の金融サービス企業との契約を失わないために、できるだけ早急にコンプライアンス対策を開始してください。

パンデミックによって、私たちがサプライチェーンの混乱を懸念すべき理由が明らかになりました。そして、最近のセキュリティ侵害によって明らかになってきたのは、ソフトウェアのサプライチェーンも脆弱になりうるということです。

情報技術サービスの外部委託に関する主な指針

規制当局：インド準備銀行（RBI）

状態：2023年10月1日に発効。2023年10月1日より前に更新される外部委託契約は、2024年4月9日までに準拠する必要があります。2023年10月1日以後に更新される外部委託契約は、2026年4月までに準拠する必要があります。

対象：全ての銀行会社、一次協同組合銀行、信用情報会社、インドに支店を展開する外国銀行。

クラウド、データ分析、AIなど：金融サービス企業は全てを自社で行うことはできないため、外部に委託しますが、外部の事業体との協力には、特有のリスクが伴います。

本書は、ネットワークおよびセキュリティソリューション、アプリケーション開発、アプリケーションサービス、データセンター運用、クラウドサービス、マネージドセキュリティサービス、決済システム事業者など、多数に及ぶ一般的なITインフラのサードパーティを取り上げています。計画段階から契約終了・オフボーディングに至るまでのサードパーティリスクに対処しています。

重要なポイント：RBIはサードパーティリスク管理により厳格になりつつありますが、この背景には十分な理由があります。パンデミックによって、私たちがサプライチェーンの混乱を懸念すべき理由が明らかになりました。そして、最近のセキュリティ侵害によってソフトウェアのサプライチェーンも脆弱になり得ることが分かってきました。銀行は、詐欺や個人情報の窃盗、そしてビジネスパートナーを介したものも含め、金融システムに侵入しようとするサイバー犯罪者の絶え間ない攻撃にも対処する必要があります。

今こそ、サードパーティのテクノロジープロバイダー（貴社が使用しているアプリケーション、クラウドサービスプロバイダー、データ分析会社）を厳格に見直し、少なくともRBIが貴社のサービスについてテストしようとしているのと同じくらい綿密に、サードパーティが提供するサービスのレジリエンスをテストする時です。

情報技術のガバナンス、リスク、統制、保証慣行に関する主な指針

規制当局：インド準備銀行（RBI）

状態：有効

対象：指定商業銀行（地方農村銀行を除く）、小規模金融銀行、決済銀行、ノンバンク金融会社、信用情報会社、その他全てのインドの金融機関

RBIの主な指針は、複数のガバナンス関連ガイドラインを1セットのガイドラインに統合したものです。

同ガイドラインは、規制対象の事業体に対して、取締役会、役員レベルの委員会、現地管理委員会（インドで支店を運営する外国銀行の場合）、および上級管理職の役割、権限、責任を定める、ITガバナンスフレームワークを義務付けています。

同ガイドラインでは、リスク管理の監督が求められ、フレームワークは戦略的な整合、価値の提供、リスク管理、リソース管理、パフォーマンス管理、情報システム監査、および事業継続性・災害復旧管理に重点を置く必要があると記載されています。また、今日の多くのIT運用とセキュリティプロセスは混在しているという認識から、これらの機能を担当するチームが連携して取り組むことも求められています。

重要なポイント：この指令は新しいものですが、その要求事項は金融サービス企業にとって馴染み深いものとなるでしょう。そのセキュリティガイドラインは、ISO/ISMS 27001およびISO/BCMS 22301という規格の枠組みの中に含まれています。情報技術に関する方向性は、ITILやISO 20000などの既存のフレームワークに似ています。

統合されたサイバーセキュリティおよびサイバーレジリエンスのフレームワークに関するコンサルテーションペーパー

規制当局：インド証券取引委員会（SEBI）

状態：有効

対象：証券取引所、清算機関、預託機関参加者、証券会社、投資信託、本人確認登録機関、認定発行登録機関および株式名義書換代理人、SEBIに登録された全ての仲介業者

このペーパーは現在のところ指令ではありませんが、いずれ指令となる可能性があります。現時点では、ガイダンスとしてサイバー成熟度に対する段階的なアプローチを提案しています。

同ペーパーは、サイバープログラムの統一性を目指して、資産管理、ガバナンス、リスク管理、サプライチェーンリスク管理、ID管理、認証およびアクセス制御、意識向上とトレーニング、データセキュリティ、情報保護、保守、防御技術とレジリエンス、監視、検出、分析、対応と復旧など、18の分野でサイバーセキュリティの実践、データセキュリティ、監査と報告のフレームワークを定めています。

重要なポイント：このペーパーは株式市場環境に向けたものですが、全ての金融サービスセクターのセキュリティとレジリエンスに関するガイダンスの宝庫でもあります。

情報およびサイバーセキュリティガイドライン2023

規制当局：インド保険規制開発庁（IRDAI）

状態：有効

対象：全ての保険仲介者

この必須ガイドラインは、米国国立標準技術研究所のサイバーセキュリティフレームワーク（NIST CSF）を基盤としています。NIST CSFはセキュリティとレジリエンスの向上を目的に設計された、348の管理策を備えた一般的フレームワークです。

重要なポイント：このアプローチはすでに成功しています。NIST CSFの管理策を含む統合サイバーフレームワークを開発する企業は、増加するサイバー攻撃から顧客を守り、度重なる規制当局からの要求を満たす上で有利な立場を得ることになります。

PwCグローバルネットワーク

国際&米国	ショーン・ジョイス	グローバルサイバーセキュリティ&プライバシーリーダー	sean.joyce@pwc.com
	マット・ファルコナー	グローバルFSリーダー	mat.falconer@pwc.com
	アマンディープ・ランバ	グローバルFSサイバーセキュリティリーダー	amandeep.lamba@pwc.com
	ジョセフ・ノセラ	グローバルFSサイバーセキュリティリーダー	joseph.nocera@pwc.com

リージョナルFSサイバーセキュリティリーダー

カナダ	ナレン・カリャナラマン	naren.x.kalyanaraman@pwc.com
英国	アレックス・ペツポウロス	alex.petsopoulos@pwc.com
EU	パオロ・カルカーノ	paolo.carcano@pwc.com
中東	モナ・マーマー	mona.m.maamer@pwc.com
中国	チュン・イン・チャン	chun.yin.cheung@cn.pwc.com
シンガポール	ジェイミー・メトカーフ	jayme.ph.metcalfe@pwc.com
香港	ケネス・ウォン	kenneth.ks.wong@hk.pwc.com
日本	ショーン・キング	sean.king@pwc.com
インド	アモル・バット	amol.bhat@pwc.com

寄稿者

クリスチャン・アーント、カルロス・イグナシオ・モンタルボ・レブエルタ、ジャン＝ベルナール・ランボー、リズワン・ナジル、ダンカン・スコット、ポール・コッハー、ヴァネッサ・タフネル、ダニー・チャミングス、シド・ファルザディ、プリヤ・ソーカレ、フィリップ・シュルツ、ロベルト・ロドリゲス、ローレン・パーカー、プラティク・シャー

pwc

日本のお問い合わせ先

PwC Japanグループ

https://www.pwc.com/jp/ja/contact.html

www.pwc.com/jp

PwC Japanグループは、日本におけるPwCグローバルネットワークのメンバーファームおよびそれらの関連会社（PwC Japan有限責任監査法人、PwCコンサルティング合同会社、PwCアドバイザリー合同会社、PwC税理士法人、PwC弁護士法人を含む）の総称です。各法人は独立した別法人として事業を行っています。
複雑化・多様化する企業の経営課題に対し、PwC Japanグループでは、監査およびブローダーアシュアランスサービス、コンサルティング、ディールアドバイザリー、税務、そして法務における卓越した専門性を結集し、それらを有機的に協働させる体制を整えています。また、公認会計士、税理士、弁護士、その他専門スタッフ約13,500人を擁するプロフェッショナル・サービス・ネットワークとして、クライアントニーズにより的確に対応したサービスの提供に努めています。
PwCは、クライアントが複雑性を競争優位性へと転換できるよう、信頼の構築と変革を支援します。私たちは、テクノロジーを駆使し、人材を重視したネットワークとして、世界149カ国に370,000人以上のスタッフを擁しています。監査・保証、税務・法務、アドバイザリーサービスなど、多岐にわたる分野で、クライアントが変革の推進力を生み出し、加速し、維持できるよう支援します。

本報告書は、PwCメンバーファームが2025年6月に発行した『Global Cyber Regulations Roundup: Financial Services』を翻訳し日本企業へ向けた示唆を追記したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。
オリジナル（英語版）はこちらからダウンロードできます。 https://explore.pwc.com/global-cyber-regulations-roundup-fs

日本語版発刊年月：2025年10月　　管理番号：I202506-02