# オペレーショナルレジリエンスに関する欧米監督当局の期待事項の比較

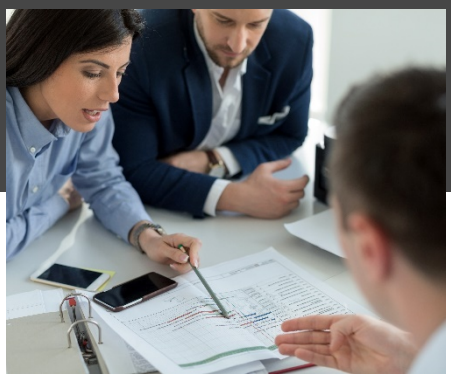
2021年5月

pwc

# 背景

**オペレーショナルレジリエンスの規制化が世界で加速度的に進んでいる。バーゼル銀行監督委員会（BCBS）、欧州委員会および米国の連邦銀行監督当局は、このテーマに関するそれぞれの視点を提供している。**

本書は、本テーマに関する主要監督当局の視点を取りまとめており、企業がグローバルで一貫したアプローチを構築する際のガイドとなる。英国の健全性監督機構（PRA）、欧州中央銀行および米国連邦準備制度理事会（FRB）による2020年12月の発表など、監督当局が協調して監督を推進していく旨を公表していることを踏まえると、このような一貫したアプローチを構築していくことは今後ますます重要となってくるであろう。



本書には、英国、欧州委員会、バーゼル銀行監督委員会（BCBS）および米国が策定したオペレーショナルレジリエンスの規制に関する文書が概説されている。これらの文書は、オペレーショナルレジリエンスの広範なトピックを取り扱った最も重要なものであると考える。

また、シンガポール、オーストラリア、カナダなど、他にも多くの国・地域が、テクノロジーリスク、業務継続管理、外部委託といったオペレーショナルレジリエンスの特定の要素に関して監督上または政策上の文書を公表していることも注目に値する。

# オペレーショナルレジリエンスに関する規制・基準

## 英国

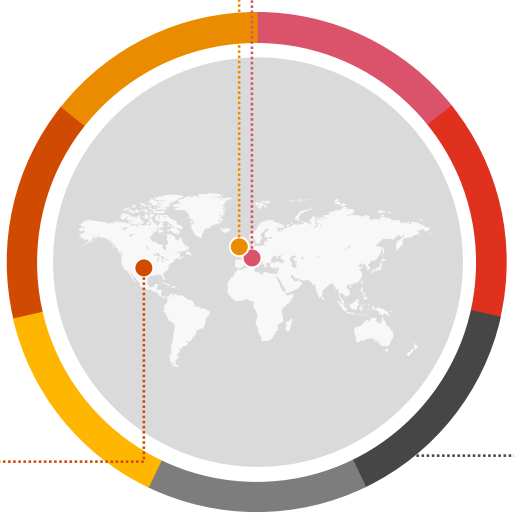
英国では、企業のみならず、顧客や市場の視点から、レジリエンスの在り方の改革を推進している。重要なビジネスサービスの特定、当該サービス提供のエンド・ツー・エンドでのプロセスのマッピング、インパクトトレランス内で収めることができるかの検証はすべて、企業のレジリエンスを構築するための投資を行うにあたって役立つ。

**今後のステップ**：2021年3月に、オペレーショナルレジリエンスに関する最終文書が公表された。政策枠組み導入のための1年間の導入期間のほか、企業がインパクトトレランス内に収めるために最長3年間の追加の移行期間が定められている。

## 欧州

2020年に、欧州委員会は、デジタル・オペレーショナル・レジリエンスに関する規則案を公表した。同規則案は、テクノロジー（および、それに関連するデータ）ならびにサードパーティリスクに重点を置いている。また、資産およびサプライヤーならびに関連する業務のリスク管理に焦点を当てており、他のオペレーショナルレジリエンスに関する文書で見られるような機能・サービスからの視点では捉えていない。

**今後のステップ**：現在、同規則案に対する修正案が検討されており、加盟国による協議が継続している。最終規則の確定は2022年までもつれこむ可能性もある。



## 米国

2020年に当局による共同文書が公表された。同文書には、既存の規制、ガイダンスおよびステートメントに基づいたオペレーショナルレジリエンスの健全なプラクティスが定められている。

**今後のステップ**：スケジュールは確定していないが、当局のアプローチの強化につながるように、企業との対話を続けていくことを約束している。

## BCBS基準

バーゼル銀行監督委員会（BCBS）は、世界各国の銀行を対象としたオペレーショナルレジリエンスに関するハイレベルの原則を公表した。同原則は、「健全なオペレーショナル・リスク管理のための諸原則」（Principles for the Sound Management of Operational Risk）の改訂と共に公表された。

**今後のステップ**：最終原則が、2021年3月に公表された。

# 英国：重要なビジネスサービスのインパクトトレランス

**英国におけるオペレーショナルレジリエンスに関する対話は、2018年7月公表のディスカッション・ペーパーを皮切りに開始し、それ以降継続して行われている。英国では、従来業務継続の領域に重点が置かれていたレジリエンスを、企業が企業だけでなく顧客および市場の視点から検討する方法について積極的に変革を進めている。**

## 対象

**「オペレーショナルレジリエンスは、業務の途絶を防止し、業務の途絶に適応・対応し、業務の途絶から回復・学習する企業・FMI・金融業界全体の能力である」**

対象は以下に限定されている。

約1,050の銀行、住宅金融組合、PRAが指定する投資会社、ソルベンシーII対象機関、公認投資取引所（Recognised Investment Exchanges）、シニアマネージャーレジーム（Senior Managers and Certification Regime）の拡大された対象企業

「2017年決済サービスに関する規則（Payments Services Regulations 2017）」または「2011年電子マネーに関する規則（Electronic Money Regulations）」において承認または登録された約1,100の事業体

中央清算機関、公認決済システム事業者（Recognised Payment System Operators）および特定サービスプロバイダー（Specified Service Providers）、証券集中保管機関（Central Securities Depositories）

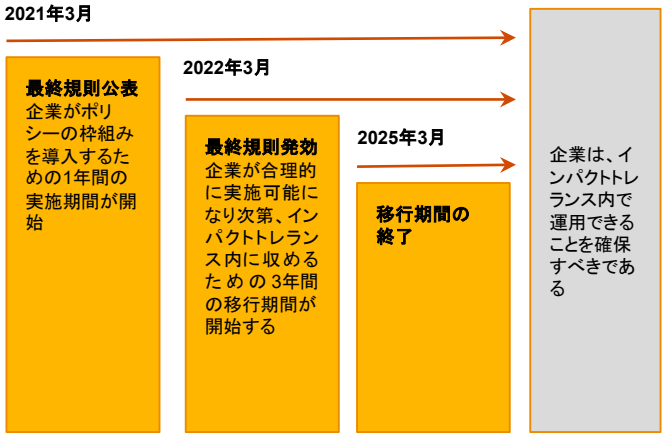
## 主要なテーマ

企業が以下の条件に該当している場合に、オペレーショナルレジリエンスを備えていると判断される。

- **重要な事項を優先させている**—エンドユーザーに対するサービスのうち、いずれが最も重要であるかを把握し、それらがどのように提供されているかを理解している。
- **レジリエンスの基準を設定している**—これらのサービスの途絶のトレランス（インパクトトレランスと呼ばれる）の上限を定めている。これは、具体的な結果・測定指標に基づき表される。
- **レジリエンス構築のために投資する**—インパクトトレランス内で収めることができるかを検証し、対応が必要な脆弱性を特定するとともに、レジリエンスを構築するための投資に備える。

上記すべてについて、**自己評価文書**において実証しなければならない。

## スケジュール




## キーポイント

- 重要なビジネスサービスはポリシー案に記載されているその他すべてのアクティビティに影響があるため、正しい方向に進むためには、重要なビジネスサービスの決定が最も重要である。
- 最も質問が多いのは、インパクトトレランスに関連するものである。企業は、「途絶の最大トレランス」を決定し、十分なエビデンスをもってその妥当性を示すことは難しいと感じている。このことは、途絶が顧客に不利益をもたらす場合や、（許容可能な）損害または許容不可能な損害をもたらす場合に、企業がそれを解決しようとする場合に特に当てはまる。
- テクノロジー、データ、サードパーティ、人材または施設を問わず、個々の資産を関連付けることが複雑であるため、重要なビジネスサービスのエンド・ツー・エンド・プロセスのマッピングは、最もリソースを要する要素であると広く認識されている。
- 監督当局が最も重要視する要素は、検証段階である。これによって各企業が業務途絶に耐え、業務途絶から回復する準備態勢の水準を実証することができるためである。
- 当局が12カ月の実施期間における期待事項の水準をわずかに緩和し、企業に対して2022年3月31日までに全面的なマッピングおよび検証の完全実施までは要求しなかったのは、上記の点を考慮したものと推察される。
- オペレーショナルレジリエンスに関する市中協議を補完するものとして、PRAは「企業の外部委託・サードパーティリスク管理に関するポリシーステートメントおよび監督上のステートメント」を公表した。これは、欧州銀行監督局（EBA）および欧州保険・企業年金監督局（EIOPA）による外部委託および情報通信技術（ICT）・セキュリティリスク管理に関するガイドラインを考慮している。金融行為規制機構（FCA）は、現時点では外部委託に対するアプローチを変更していない。

# BCBS：オペレーショナルレジリエンスのための諸原則

**BCBSおよび英国のアプローチはいずれも、これまでに実施されてきた一連のアクティビティを推進するものである。すなわち、会社がレジリエントになるための重要な業務を特定し、それらがどのように提供されているかを把握し、レジリエンスの基準を設定し、当該基準に照らして検証する。しかし、規制制度間での用語・定義の差異（例えば英国においては「重要なビジネスサービス（important business service）」、BCBSにおいては「重要な業務（critical operation）」）を含め、いくつかの大きな差異も存在する。**

## 対象

**「オペレーショナルレジリエンスとは、銀行が途絶時に重要な業務を提供する能力のことである。この能力により、銀行は、脅威や潜在的な障害を特定し、それらから自身を守り、途絶による重要な業務の提供への影響を最小限に抑えるために、途絶事象に対応・適応するとともに、その事象から回復・学習することができる」**

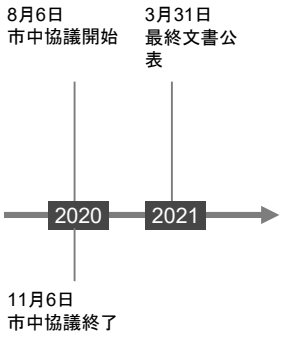
諸原則は、銀行にのみ直接関連するものである。しかし、BCBSは基準設定主体としての影響力が大きく、世界各国の規制当局が調和した制度を導入しようとするため、これらの諸原則がより広範に適用される可能性がある。イングランド銀行はBCBSのオペレーショナル・レジリエンス・ワーキング・グループにおいて重要な役割を担っており、PwCは今回の調和の動きを予期していた。

## 主要なテーマ

諸原則では、以下の7つの原則が提示されている。

- ガバナンス
- オペレーショナルリスク管理
- 業務継続計画とテスト
- 重要な業務の相互連関性と相互依存度のマッピング
- サードパーティー依存度の管理
- インシデント管理
- サイバーセキュリティを含む頑健なICT

## スケジュール




## キーポイント

- BCBSの諸原則は、リスク管理、業務継続、サードパーティリスク管理や、再建・破綻処理制度などの実務をつなげる包括的な諸原則を定めている。BCBSは、オペレーショナルリスクの規律に従うことによって、インシデントの防止を目的とした活動と、対応を重視した活動とのバランスをとることの重要性を伝えている。
- 「重要な業務」の定義については、英国当局が提言するようには明示的に顧客を考慮していないという点で重要な差異があるように思われる。例えば、PRA文書CP29/19には、「多くの企業にとって、（新しいアプローチは）個々のシステムやリソースのレジリエンスのみを検討することから、ユーザーに提供されるサービスを検討する方向へシフトすることを意味する」と記載されている。
- BCBSは、「インパクトトレランス」という概念は用いず、代わりに既存のリスクアペタイトに対して「途絶に対する許容度（tolerance for disruption）」を調整して用いることを期待している。最終原則では、これを重要な業務について適用すべきであることを明確化している。
- BCBS は、「国際的に活動する銀行（internationally active bank）」に対し、重要な業務を定義するうえで再建・破綻処理計画（RRP）を活用し、自行のオペレーショナルレジリエンスにかかる取り組みが再建・破綻処理計画と適切に調和しているかを検討することを提案している。
- 同時に、BCBSは、健全なオペレーショナル・リスク管理のための諸原則に係る一連の改訂を公表した。オペレーショナルリスク管理の規律とオペレーショナルレジリエンスの成果には、強いつながりがある。

# 米国：オペレーショナルレジリエンスを強化するための健全なプラクティス

**米国当局は、オペレーショナルレジリエンスに関する文書が新しい規則を導入するものではなく、規模が最大で、複雑性が高い銀行のために既存の規則を明確化するものであり、安全性、健全性、市場の安定性の確保に焦点を当てていると述べている（英国のPRAと同様）。しかし、新たな期待事項が盛り込まれており、企業はこれに対応する必要がある。米国は引き続き、政策立案よりも監督を通じてレジリエンスを推進している。**

## 対象

「オペレーショナルレジリエンスは、 ハザードによって生じた途絶時においても重要な業務やコア・ビジネス・ラインを含む業務を提供する能力のことである。それは、途絶に備え、適応し、耐え、途絶から回復するために、実効的なオペレーショナルリスク管理を十分な財源とオペレーション資源と組み合わせて実施した成果である」

諸原則は、国法銀行、FRB加盟銀行である州法銀行、FRB加盟銀行でない州法銀行、貯蓄金融機関（savings associations）、米国の銀行持株会社、貯蓄金融機関持株会社（savings and loan holding companies）のうち、（a）2,500億米ドル以上の平均連結総資産を保有する、または（b）1,000億米ドル以上の平均連結総資産を保有し、かつ、法域を越えた活動の平均、短期ホールセール資金調達の加重平均、ノンバンク資産の平均またはオフバランスシート・エクスポージャーの平均が750億米ドル以上であるものを対象とする。

## 主要なテーマ

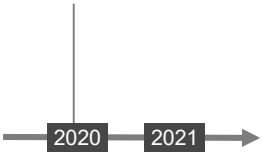
この文書では、以下の7つの原則が提示されている。

- ガバナンス
- オペレーショナルリスク管理
- 業務継続管理
- サードパーティリスク管理
- シナリオ分析
- 安全で頑健な情報システム管理
- 監視および報告
- 上記に加え、「サイバーリスク管理のための健全なプラクティス」に関する付属文書

（注）このペーパーは、BCBSの諸原則が取り扱っているマッピングやインシデント管理に係る原則は取り扱っていない。

## スケジュール

10月30日
当局による共同文書公表




今後の公表に関するスケジュールは確定していないが、このテーマを今後さらに取り上げることを企業に示唆している。この点に関して、以下の通り述べている。

「企業との対話を継続することによって、企業のオペレーショナルレジリエンスをサポートするための当局のアプローチを改善していきたい」

## キーポイント

- 健全なプラクティスは、オペレーショナルリスク管理、業務継続管理、サードパーティリスク管理、サイバーセキュリティリスク管理、再建・破綻処理計画を取り扱った既存の規則、ガイダンスおよびステートメント、ならびに共通の業界基準に基づいている。ただし、この健全なプラクティスは、当局の既存の規則・ガイダンスを修正、拡大または変更するものではない。
- これらは、米国の再建・破綻処理計画に係る取り組みと整合した、重要な業務（米国の金融安定性に影響を与える可能性があるもの）およびコア・ビジネス・ライン（収益、利益またはフランチャイズ価値に重大な損失をもたらす可能性があるもの）に重点を置いており、英国の「重要なビジネスサービス」よりも対象範囲が広い（ただし、破綻処理時の業務継続に関する制度の対象範囲を拡大するという英国の計画と整合する）。
- シナリオ分析を実施する際には、（業務の）マッピングが必要である。
- 企業は、リスクアペタイトに合わせて（企業レベルで）「途絶に対する許容度（tolerance for disruption）」を設定すべきである。
- 最終的には、企業は、 重要なビジネスサービス とインパクトトレランス（英国）を重要な業務と（企業全体の）途絶に対する許容度までに引き上げることによって、英国と米国の視 点 を一致させるような、グローバルに一貫したアプローチを維持することができるはずである。
- 固有のリスク特性を有する重要な業務とコア・ビジネス・ラインを実施するための代替的な場所・リモートワーク体制、および途絶からの回復を助けるためのスタッフのバックアップ機能の利用を義務づけている。
- 企業には、途絶に対する許容度内にとどまることができるように、公共のまたはクリティカルなインフラ（エネルギー、通信など）の途絶を管理するプロセスを整備しておくことが期待されている。なお、英国であれば、これらは、少なくとも短期間であれば、企業がインパクトトレランスを上回ることが許容される違反に該当する場合がある。

# 欧州：デジタル・オペレーショナル・レジリエンス法（DORA）

**DORAでは、ICTリスクの管理、脅威に関する情報の共有、ICT関連インシデントの報告、ICTサードパーティの管理・監督に重点が置かれている。ただし、欧州委員会と加盟国との間で細かい内容について今後協議を行って対応すべきことが多くある。テクニカルスタンダードに定める要件の検討に要する時間を踏まえると、導入までの道のりはまだ長い。**

## 対象

「デジタル・オペレーショナル・レジリエンスは、金融機関が利用し、金融サービスの提供とその品質の継続を支えるネットワーク・情報システムのセキュリティに対応するために必要な、ICTに関連するあらゆる能力を、直接的にまたはICTサードパーティプロバイダーのサービスの利用を通じて間接的に確保することによって、金融機関が技術的な視点から自社のオペレーショナルインテグリティを構築、保証、レビューする能力を意味する」

この規則は、22,000社程度に適用されると推計される。欧州におけるより広範なデジタル・ファイナンス制度の一部であるとともに、サイバーセキュリティに関する欧州の施策およびデータに関する欧州の戦略とも関連する。外部委託リスク管理やICT・セキュリティリスク管理に関するEBA[1]の既存のガイドラインと強く結び付いていることを踏まえると、作業プログラムの進捗が遅れているESMAやEIOPAの監督下にある企業にとっては、DORAはより大きな変化をもたらす規制であるといえる。

## 主な要件

DORAでは、以下の分野の頑健性を向上させるよう提案がされている。

- ガバナンス（ICTリスク）
- ICTリスク管理
- ICT関連インシデントの報告
- デジタル・オペレーショナル・レジリエンスのテスト
- 情報共有
- ICTサードパーティリスク管理

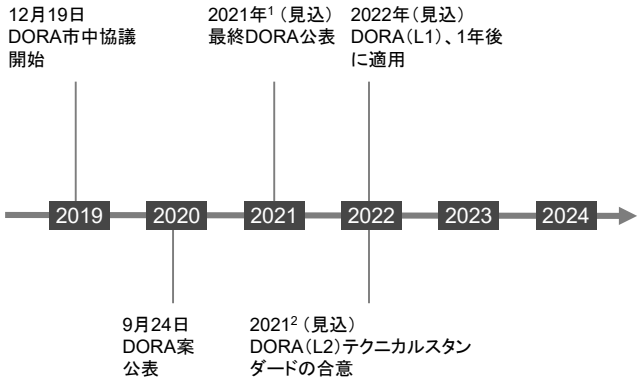
新規則は、すべての金融機関を対象としているが、金融機関の実際の規模とリスクプロファイルに応じてある程度の調整が行われることが想定される。

## キーポイント

加盟国との主な協議分野として、以下の事項が含まれると考えられる。

1. 比例原則ーなお、提案されているような「マイクロエンタープライズ」と他のすべての企業との間の階層化が、多くの金融機関にとって相応の対応とはならないと考える
2. クリティカルなサードパーティプロバイダー（TPP）の指定および監督上の枠組み
3. 他の規則やガイドラインと相互に関連するエリア（NIS指令、PSD2など）
4. 既存の制度との重複を考慮した報告要件の簡素化
5. 要件を満たす方法を金融機関に伝えるために定めるべき内容の程度
6. グループではなく、個々の企業に求められる要件に焦点を当てている
7. ESAおよび欧州各国の監督当局の役割・責任

## スケジュール




**レベル1の規制以降は、レベル2のテクニカルスタンダードにおいて詳細な内容が規定される。**

**1年後**に公表予定のテクニカルスタンダード案：

- ICTリスク管理のツール、方法、プロセス、方針
- インシデントの分類
- 報告内容・ひな形
- ICTサードパーティ情報レジスタ
- 再委託先の評価
- 重要なICT TPPについては、関係当局による合同審査チームのメンバーの指名
- 重要なICTサードパーティの監督を可能にする条件

**3年後**に公表予定のテクニカルスタンダード案：

- 単一のEUハブを通じた報告の一元化
- 高度なテスト

[1] 欧州銀行監督機構（EBA）、欧州証券市場監督機構（ESMA）、および欧州保険・企業年金監督局（EIOPA）。3機関を合わせて欧州監督機構（ESA）と呼ぶ。

[2] この法の重要性に関するメッセージが公表されたことを踏まえ、最終化までの標準的な期間である18カ月よりも早い時期に基づいている。

# EU DORAの要件の整理

**EBA監督下の企業にとって、外部委託とICT・セキュリティリスク管理に関する既存のガイドラインには多くの類似点がある。主要な条項で取り扱われている要件を以下の通り整理した。**

**ICTガバナンスと組織（第4条）**

ICTリスクの管理、ICT関連機能の明確な役割・責任の設定、ICTリスクの適切なリスク許容度の決定に係る最終的な責任など、経営体の役割を規定している。

1

**ICTリスク管理（第5～14条）**

デジタルレジリエンス戦略など、ICTリスク管理フレームワークの要件を規定している。当該フレームワークには、ICTリスクのリスク許容度とICTに係る途絶によるインパクトトレランス、主要な依存関係を示した個々の企業の包括的なICTマルチベンダー戦略（存在する場合）、オペレーショナルレジリエンスのテストの実施などが含まれるべきである。

2

**ICT関連のインシデント管理・報告（第15～20条）**

プロセスの整備という基本的な要件に加えて、公表された基準に基づくICT関連インシデントの分類に関する要件が規定されている。主要なICT関連インシデントについては、最初の通知（当日）、中間報告（1週間以内）、最終報告が求められている。欧州監督機構（ESA）は、企業間で整合した報告が行われるよう、標準となる様式、ひな形、手続きを公表する予定である。また、ESAは、主要なICT関連インシデント報告のための単一のEUハブの利用を検討する予定である。

3

**デジタル・オペレーショナル・レジリエンスのテスト（第21～24条）**

独立した立場の者が実施するテストについては、リスクベースのアプローチの適用が求められている。重要なICTシステムとアプリケーションはすべて、少なくとも年に1度テストを実施しなければならない。ESAは、少なくとも3年ごとに脅威に基づくペネトレーションテストを活用した、高度なテストを実施することが期待される「重要な金融機関（significant financial entities）」を特定する予定である。

4

**ICTサードパーティリスク管理（第25～27条）**

ICT関連の依存関係および契約上の取り決めから生じるリスクの規模・複雑性・重要性に基づいた、ICTサードパーティリスクの比例的な管理を規定している。情報レジスタは、ICTサードパーティプロバイダーによって提供されるすべての契約上の取り決めについて保管しなければならない。企業は、少なくとも年に1度、ICTサービスの新たな取り決めに関する情報を規制当局に報告しなければならない。

契約上の取り決めを終了させることが予想されるような状況が提示されており、企業は出口戦略・計画を策定することが求められている。また、すべてのICTサービスについて最低限定めるべき契約条項が設定されている。

再委託する場合（特に第三国のプロバイダーを利用する場合）を含め、潜在的な集中リスクの分析を実施することが要求されている。

なお、欧州委員会がクラウドコンピューティングのために策定した標準的な契約条項の使用については、任意である。

5

**情報共有（第40条）**

企業が、機密情報を保護する方法を用いて、信頼できるコミュニティ内でサイバー脅威に関する情報を交換する取り決めに参加する場合には、関係当局に通知することが期待されている。

6

# EU DORA：ICTサードパーティープロバイダーに対する影響

**欧州のオペレーショナルレジリエンスに関する文書は、非金融サービス企業、すなわち、ICTサードパーティプロバイダー（TPP）に対する特定の要件を導入しているという点で独特である。現時点での規則案の期待事項を以下の通り整理する。**

## すべてのICTサードパーティープロバイダー ― 主要な契約条項

- サービス・レベル・アグリーメントを含む契約書全体を、1つの文書にまとめるべきである（ただし、実務上の理由から対応できない場合はある）。
- 期待されている最低限の契約条項は、重要な外部委託契約に関するEBAガイドラインとおおむね一致しているが、ICTインシデントが発生した場合に追加のコストが発生しないか、あるいは事前にコストが定められているケースについては、支援を提供するというICTサードパーティ・サービス・プロバイダーの義務などの新たな項目が含まれている。
- 企業とICTサードパーティは、特定のサービス向けに策定された（任意の）標準的な契約条項の使用を検討することが期待されている。

## クリティカルなICTサードパーティープロバイダーのみ ― 監督当局による監督フレームワーク

### 指定（第28条）

ICTサードパーティ・サービス・プロバイダー（TPP）は、以下の条件に照らして、重要とみなされる。

- TPPによる大規模なオペレーション上の障害発生時のシステミックな影響
- TPPに依存するグローバルな、およびその他のシステム上重要な機関の数およびそれらの相互依存関係
- 同じTPPへの集中リスク
- 代替可能性の程度
- TPPがサービスを提供する加盟国数
- TPPを利用している企業が活動している加盟国数

TPPが監督フレームワークへの参加を任意に選択できるようにすべきである。

クリティカルなTPPには、収益に応じて、監督コストをカバーするための手数料が課せられる。

### 監督評価（第30条）

クリティカルなTPPが、企業にもたらす可能性のあるICTリスクを管理するための包括的、健全かつ実効的な規程、手続き、メカニズム、取り決めを整備しているかの評価。評価には以下の項目が含まれる。

- サービスの安全性、利用可能性、持続可能性、スケーラビリティ、品質を確保する能力、ならびにデータの安全性、機密性、完全性に係る基準を維持する能力
- リスク管理プロセス
- ガバナンスの取り決め
- 解約権の実効的な行使を確保するための仕組み（データおよびアプリケーションのポータビリティ）
- ICTシステム・インフラ・統制のテスト

### リード監督者の権限（第31～35条）

- すべての関連情報・文書を要請する。
- 全般的な調査・検査を実施する。
- 監督活動の実施後に、講じられた措置を明記した報告書を要請する。
- 例えばシステミックな影響を最小限に抑えるための条件の適用などに関する勧告に対応する。
- 重要なTPPに対し上記への協力を強制するために、定期的に罰金[1]を課す。
- 重要なTPPが検査を受け入れない場合には、関連企業との契約取り決めを終了する。

これはEUの監督フレームワークに沿ったものであり、ESAの1つがリード監督者（Lead Overseer）に指名され、新しい監督フォーラム（Oversight Forum）が設置される。

[1] 罰金は、コンプライアンスが達成されるまで、日次ベースで、クリティカルなICT TPPへの通知から最長6カ月間課せられる。罰金額は、重要なICT TPPの前年度のグローバルベースでの1日平均収益の1%である。

**辻田　弘志**
**パートナー**

電話：090-1424-3247
Eメール： hiroshi.tsujita@pwc.com

**村永　淳**
**パートナー**

電話：080-1347-2227
Eメール：jun.muranaga@pwc.com