金融行政の課題
～ITガバナンス、サイバーセキュリティ、エマージングテクノロジーに関する金融庁の取組について～

2024年12月4日

FISC創立40周年記念講演会

金融庁長官

井藤　英樹

はじめに

- サイバーセキュリティのように、競争ではなく協調が求められる領域が増えている
- こうした領域では、金融機関自らの努力による「自助」、金融業界の協力による「共助」、当局の支援による「公助」を組み合わせ、官民連携で知見とリソースを結集することにより、金融業界全体で課題に取り組むことが重要
- FISCの果たされてきた役割の例
  - FISC「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」は、1985年の発刊以来、民間部門の主要な実務指針となってきた
- 当庁とFISCは様々な連携を行ってきた。サイバーリスクなどの諸課題に対し、今後もFISCと連携を深め、ともに対応してまいりたい

本日のアジェンダ

１．ITガバナンス

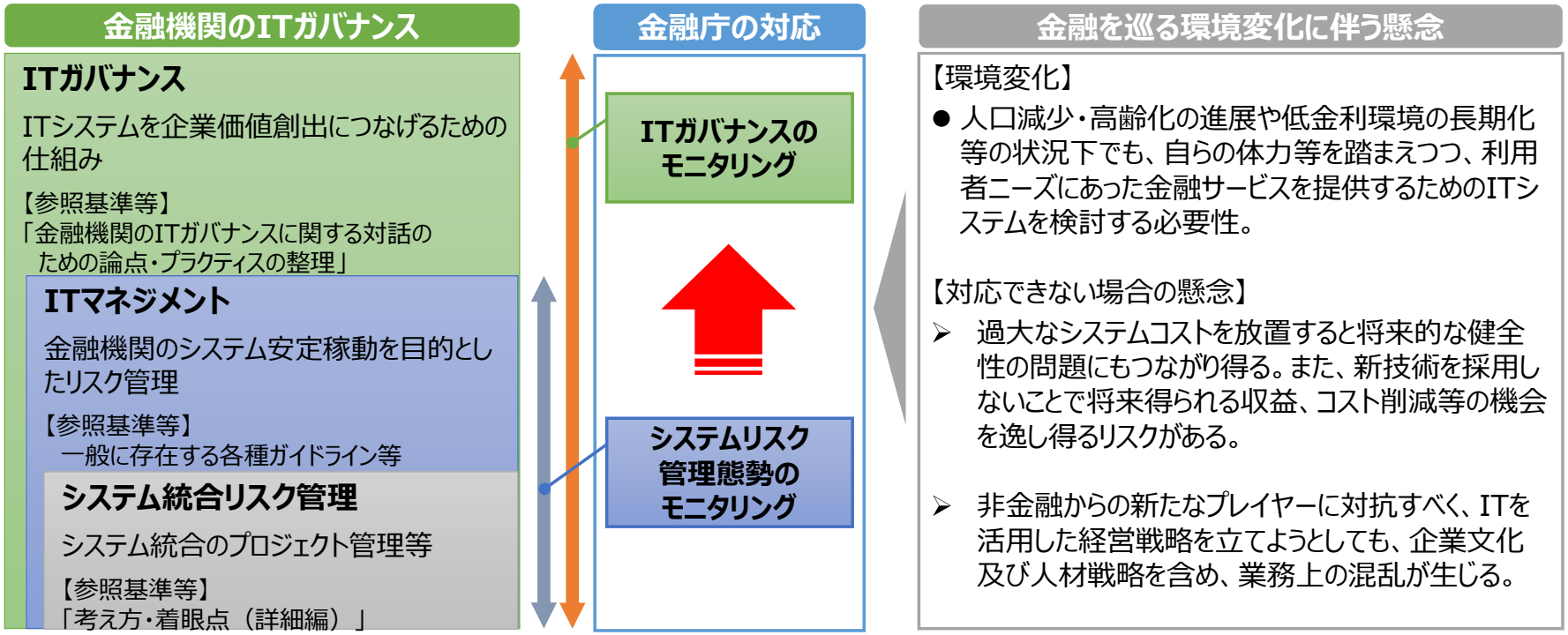
２．サイバーセキュリティ

３．エマージングテクノロジー

１．ITガバナンス

「金融機関のITガバナンスに関する対話のための論点・プラクティス」の策定

- 金融庁は、従来の検査・監督のあり方を見直し、検査マニュアルを廃止し、「検査・監督基本方針」を公表（2018年６月）した。同方針に基づくIT分野のモニタリングの考え方と進め方について、「金融機関のITガバナンスに関する対話のための論点・プラクティス」の初版を2019年６月に公表した（2023年６月に改訂）。具体的には、
  - 近年の金融セクターを巡る環境の変化を踏まえ、ITと経営戦略を連携させ、企業価値の創出を実現させるための仕組みである「ITガバナンス」の状況について、金融機関と対話を行う。
  - ITマネジメントのモニタリングについては、一般の基準等を活用する。システム統合リスク管理のモニタリングについては、従来の「チェックリスト（2002年12月）」に代わる「考え方・着眼点」を公表した。

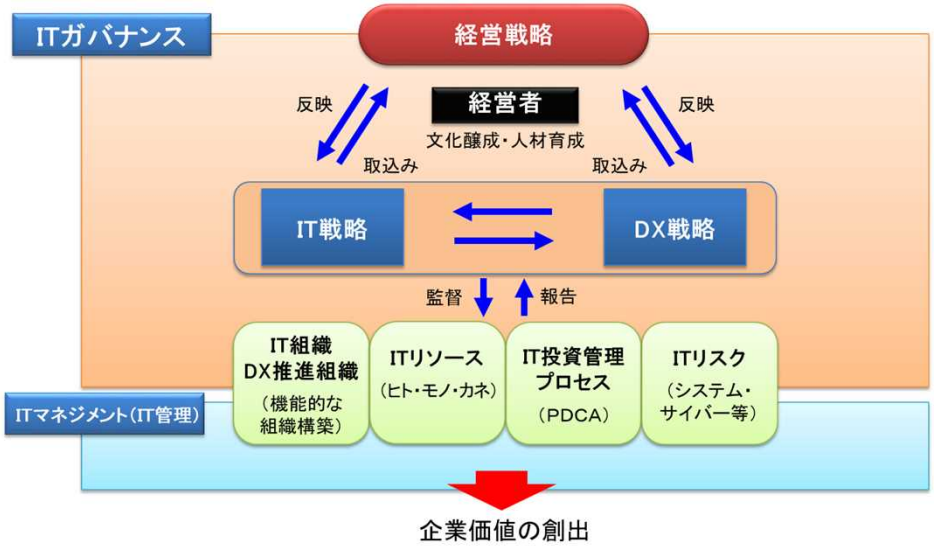


（金融庁ウェブサイト）https://www.fsa.go.jp/news/r4/sonota/20230630/20230630.html

ITガバナンスの概念

ITガバナンスの定義・要素

- ITガバナンスとは、**経営者がITシステムと経営戦略を連携させ、企業価値を創出するための仕組み**。ITガバナンスには、内部統制のみならず、ビジネスの収益を向上させるための成長戦略の実現も含まれる。
- IT組織・DX推進組織 、ITリソース、IT投資管理プロセス、ITリスクは、金融機関がIT戦略とDX戦略を実現する上で共通する要素である。

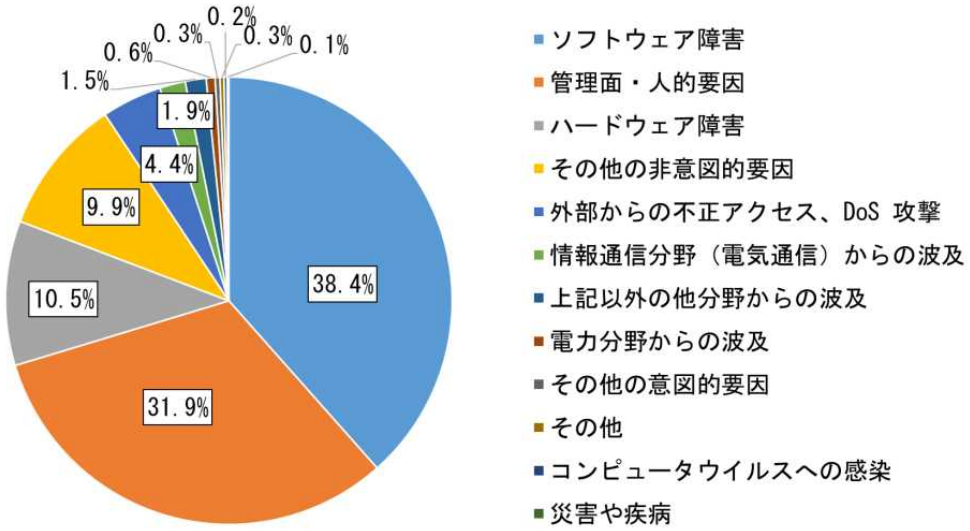


ITガバナンスに関する金融庁の考え方や着眼点

- **経営陣がリーダーシップを発揮し**、例えば情報発信を続けることで、ステークホルダーの信頼と共感を得ながら、**戦略の実現に向けた機運やモチベーションを高める**ことが重要。
- 経営陣は、デジタル活用の恩恵を享受する上での**前提となるセキュリティをどのように確保するのか、ITリスク（サイバーリスクを含む）をどのように管理するのか**等について、バランスを考えながら創造力を働かせて議論を行い、目指す将来像を明らかにしていく必要がある。
- DX戦略では、収益性の向上やビジネスモデル変革に向けて、**業務革新、顧客接点拡大、新規事業開発といった戦略領域を定め、中長期的なロードマップを策定する**ことが重要。

金融分野のシステム障害分析レポート（概要）

- 金融庁では、監督指針等に基づき、金融機関から報告を受けているシステム障害（サイバー攻撃を含む）の分析結果をまとめ、2019年以降、毎年、「金融機関のシステム障害に関する分析レポート」として公表している。
- 本レポートは、過去の事例も含め、障害の端緒に着目して障害事例を分類し、原因と課題を分析している。また、ITレジリエンス強化の参考となるよう、ATM停止時の円滑な顧客対応や、コンティンジェンシープランに則った円滑なシステム復旧などの障害対応の好事例も記載している。加えて、今般のレポートにおいては、「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（TLPT）の好事例及び課題」及び「オペレーショナル・レジリエンスに係る金融機関との対話等の概要」のコラムも掲載している。
- 金融機関においては、本レポートに加え、サイバーセキュリティを含むシステムリスク管理に関する各種標準、ガイドライン等を参照し、自組織の体制及び対策について見直し、求められるITセキュリティ又はITレジリエンスとの差異を特定し、解消することが望ましい。

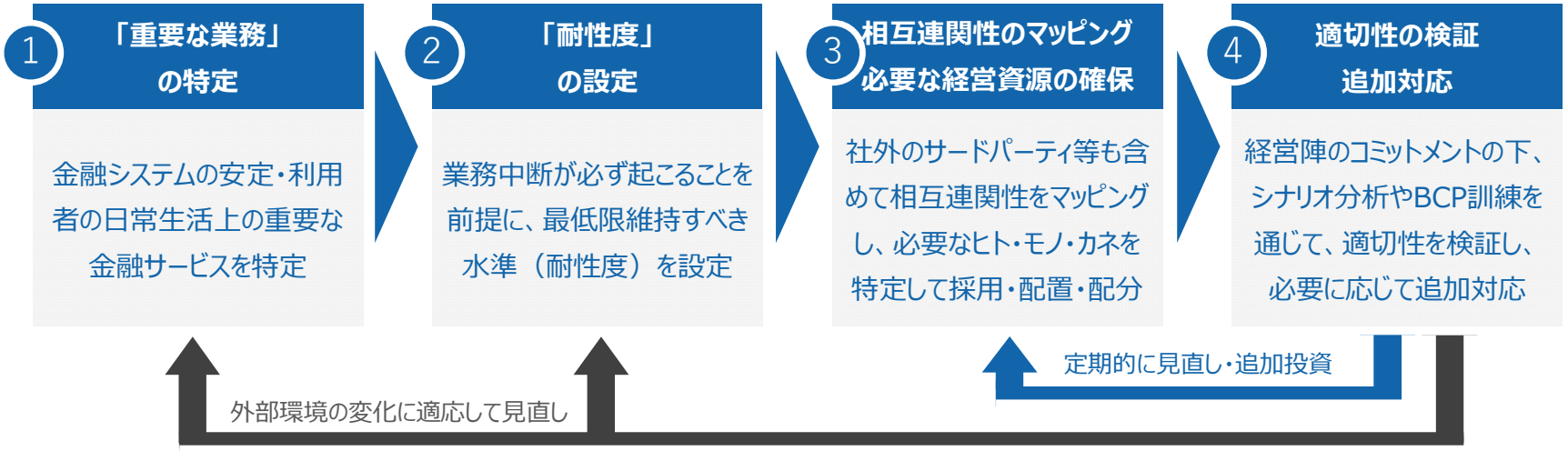


（参照）金融庁「「金融機関のシステム障害に関する分析レポート」の公表について」（2024年６月26日）
https://www.fsa.go.jp/news/r5/sonota/20240626/20240626.html

オペレーショナル・レジリエンス

- オペレジ（業務の強靭性）とは、システム障害、サイバー攻撃、自然災害等が発生しても、重要な業務を、最低限維持すべき水準において、提供し続ける能力をいう。
- 既存のリスク管理（未然防止策）や、BCP（地震などの特定のリスク事象を想定した対応計画）は重要だが、想定外の事象が生じた場合に、金融システム安定上の重要な業務を提供できなくなるおそれ。**未然防止策を尽くしてもなお、業務中断が生じることを前提に、利用者目線で早期復旧・影響範囲の軽減を確保する枠組み**として国際的に議論されている。
- 2022年12月、各金融機関のより良い実務の構築に向けて、論点・課題を整理したディスカッション・ペーパーを公表・パブコメ募集。2023年4月に最終化。主要行・国際統一基準金融機関を対象に監督指針を改正。

オペレジの基本動作



２．サイバーセキュリティ

我が国を取り巻くサイバー脅威（国家安全保障戦略より抜粋）

現在の情勢

- サイバー空間、海洋、宇宙空間、電磁波領域等において、自由なアクセスやその活用を妨げるリスクが深刻化している。特に、相対的に露見するリスクが低く、攻撃者側が優位にあるサイバー攻撃の脅威は急速に高まっている。
- サイバー攻撃による重要インフラの機能停止や破壊、他国の選挙への干渉、身代金の要求、機微情報の窃取等は、国家を背景とした形でも平素から行われている。そして、武力攻撃の前から偽情報の拡散等を通じた情報戦が展開されるなど、軍事目的遂行のために軍事的な手段と非軍事的な手段を組み合わせるハイブリッド戦が、今後更に洗練された形で実施される可能性が高い。

出所：内閣官房 https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo/dai1/siryou3.pdf

サイバーセキュリティに関する金融庁の取組み

- **ガイダンスの提供**
  - ✓ 監督指針、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 https://www.fsa.go.jp/news/r6/sonota/20241004/20241004.html
  - ✓ 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 https://www.fsa.go.jp/news/r3/cyber/torikumi2022.html
  - ✓ 金融行政方針 https://www.fsa.go.jp/news/r6/20240830/20240830.html
  - ✓ 脆弱性に関する注意喚起
  - ✓ 要請（体制整備、脆弱性診断、演習・訓練、監視・分析の強化、フィッシング対策など）
  - ✓ G7サイバーエキスパートグループ https://home.treasury.gov/policy-issues/international/g-7-and-g-20/g7-cyber-expert-group
  - ✓ 業界との意見交換会、各種講演
- **モニタリング**
  - ✓ 実態把握、オン・オフの検査・モニタリング、障害対応
- **公助の取組み**
  - ✓ 演習（Delta Wall） https://www.fsa.go.jp/news/r6/sonota/20241008/deltawall.html
  - ✓ サイバーセキュリティセルフアセスメント（CSSA） https://www.fsa.go.jp/news/r5/cyber/20240423.html
  - ✓ TLPT（※）事例還元 （※Threat-led penetration testingの略。脅威ベースのペネトレーションテスト） https://www.fsa.go.jp/news/r5/sonota/20240626/20240626.html
  - ✓ 地域金融機関向けTLPT実証事業（2023年度補正予算1.5億円に基づく）

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

（ガイドラインの構成）

1．基本的考え方

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

2．サイバーセキュリティ管理態勢

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

3．金融庁と関係機関の連携強化

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

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

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

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

サイバーセキュリティ管理態勢

基本的な対応事項

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

対応が望ましい事項

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

金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅸ）

金融分野のサイバーセキュリティを巡る状況

- 世界各国において、大規模なサイバー攻撃が発生しており、我が国においても、サイバー攻撃による重要情報の窃取、金銭被害等が発生
- こうしたサイバー攻撃の脅威は、金融システムの安定に影響を及ぼしかねない大きなリスクとなっており、金融業界全体のインシデント対応能力の更なる向上が不可欠

金融業界横断的なサイバーセキュリティ演習（Delta Wall Ⅸ）

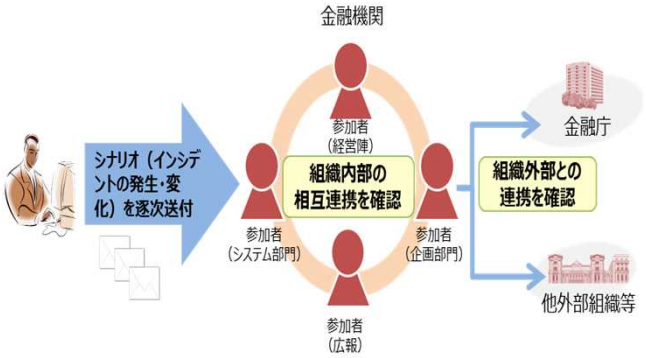
- 2024年10月、**金融庁主催による９回目の「金融業界横断的なサイバーセキュリティ演習」（Delta Wall Ⅸ（注））を実施**

  （注）Delta Wall: サイバーセキュリティ対策のカギとなる「自助」、「共助」、「公助」の３つの視点（Delta）＋防御（Wall）
- 中小規模の重要インフラ事業者の参加率向上の観点から、**170先が参加予定**（昨年度から5先増）
- シナリオについてはサイバー攻撃が同時多発的に発生し、複合的なインシデント対応を求めることで演習の高度化を図る
- 昨年度に引き続き、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の向上を図るため、**参加金融機関は自職場やテレワーク環境下で演習に参加**

演習の特徴

- ✓ インシデント発生時における**初動対応、攻撃内容の調査・分析、顧客対応、復旧対応等の業務継続**を確認
- ✓ 参加金融機関がPDCAサイクルを回しつつ、対応能力の向上を図れるよう、具体的な改善策や優良事例を示すなど、**事後評価に力点**
- ✓ 本演習の結果は、参加金融機関以外にも**業界全体にフィードバック**

演習スキーム



【演習シナリオの概要】

- **銀行、信金・信組・労金**
  - ✓ （ブラインド方式のため非開示）
- **証券**
  - ✓ 業務システムやオンラインサービスの停止等が発生
- **生命保険会社・損害保険会社**
  - ✓ 業務システムの停止等が発生
- **資金移動業者・前払式支払手段発行者・暗号資産交換業者**
  - ✓ 業務システムの停止等が発生

サイバーセキュリティセルフアセスメント（CSSA）の概要（2024事務年度）

経緯

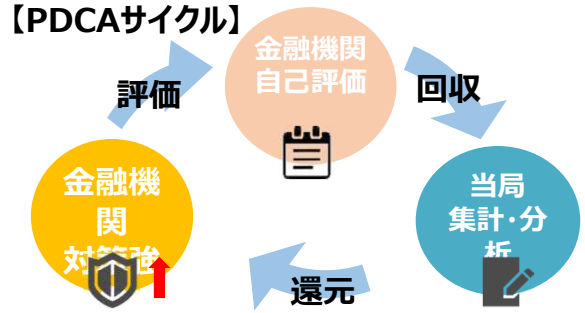
- サイバーセキュリティ成熟度評価にあたり、大手金融機関は国際的なフレームワーク（FFIEC CATなど）を活用している一方、**中小金融機関にとっては体力的に活用できるフレームワークが存在してこなかった**
- そこで、2021事務年度に、**金融庁、日本銀行及びFISCは、合同で中小金融機関向けのサイバーセキュリティに関する自己点検票を開発**
- 2022事務年度（第1回）には、**地域金融機関、新形態銀行**（ネット銀行等）に対して自己評価の実施を求め、結果を還元する取組を実施
- 2023事務年度（第2回）には、**証券会社、保険会社、信託銀行**にも対象を拡大
- 2024事務年度（第3回）には、**3メガバンク以外の主要行、労働金庫等**にも対象を拡大

狙い

①金融機関のサイバーセキュリティの強化・底上げ

・公助の一環として、ツールの提供と自己評価の実施を要請することで、自助（自律的な改善）の機会を提供する
・業態内で自組織の位置付けを可視化し、自律的な改善を促す

②金融当局等の施策への活用



金融機関に望まれる対応のポイント

経営陣の責務：リスクの認識と全社横断的な視点からの対応

- 経営上のリスク（サイバーインシデントによるビジネスの中断、投資・事業への影響、レピュテーションリスクの発生）を踏まえたセキュリティへの投資、平時と危機発生時の対応態勢構築とリーダーシップの発揮
- 変化への追随と対策の実装：ビジネスとセキュリティはセット（Security by Design）
- ベテラン・専門家の離職、企業継続のためのIT・セキュリティ人材の育成
- 事業戦略を踏まえたIT構築・セキュリティ戦略（守りやすくビジネスを展開しやすいITアーキテクチャ）
- 経営陣とセキュリティ部署間のリスクコミュニケーションの確保、外部（第三者）評価の活用

同業他社との比較、外部情報の把握

- 同業他社との比較：　サイバーセキュリティセルフアセスメント（CSSA）の活用
- 外部情報の把握：　脅威動向、対策・対応のトレンド、規制・当局動向

共助の活用

- 金融ISAC等の共助機関の活用（技術的対応、グッドプラクティス、最新動向、実践的な演習の実施等）
- 中央機関等による業務補完・支援の活用、業態内の相互扶助の充実

３．エマージングテクノロジー

デジタル技術を用いた金融サービスの変革への対応

■ AIやブロックチェーン等、デジタル技術を用いた金融サービス・取引に対応し、個人や企業の利便性向上等を図るため、**利用者保護やシステムの安全性を確保しつつ、金融機関による特色ある金融サービスの提供**を促す。

サービス利用者の安全性・適切なAML/CFT・金融システムの安定の確保

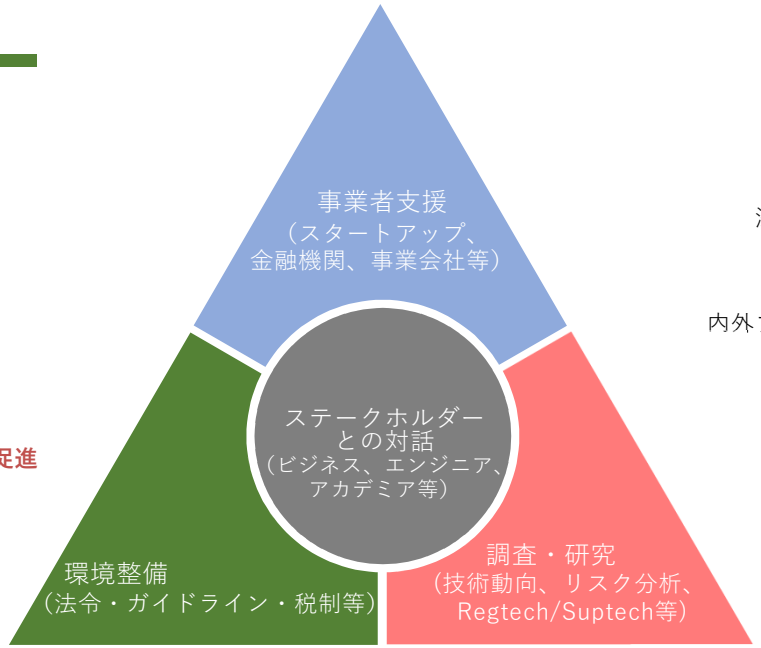
Web3.0等のイノベーションを金融面から支援

埋込型金融等の発展に向けた検討
– 金融サービス仲介法制の活用も促進

決済インフラの高度化（資金移動業者の全銀システムへの参加資格拡大、多頻度小口決済等）

公平な規制環境の実現に向けた国際的な働きかけ

金融機関における健全かつ効果的なAI利活用を促進するため、ディスカッション・ペーパーを策定



FinTechサポートデスク

FinTech実証実験ハブ

法令照会対応（グレーゾーン解消制度等）

日系フィンテック事業者と海外VC等との連携強化支援（海外展開支援）

内外フィンテック事業者と国内金融機関等との連携強化支援

金融機関システム・フロントランナー・サポートデスク

デジタル・分散型金融への対応のあり方等に関する研究会

調査研究プロジェクト
（ブロックチェーン国際共同研究プロジェクト等）

海外ネットワークの構築・活用

関係省庁・自治体等との連携
（デジタル庁、経産省等）

国際機関等との連携・協力
（FSB, FATF, OECD等）

■FIN/SUMを中心としたJapan Fintech Weekの開催
■国内外ミートアップ　■庁外拠点（FINOLAB等）の活用
■世界に向けた体外発信の強化　■ Blockchain Roundtable
■BGIN（Blockchain Governance Initiative Network）

資金決済制度等に関するワーキング・グループにおける主な検討課題

■ 送金・決済・与信サービスの利用者・利用形態の広がりや、新たな金融サービスの登場がみられる中、ビジネスの健全な発展に資する規制のあり方について検討を行う必要

資金決済制度関係＜送金分野＞

資金移動業者の破綻時には、供託手続を通じて国が各利用者に対して還付手続を実施することとされており、利用者への資金の還付に最低約170日の期間を要する。

- **利用者資金の還付手続きをより迅速に進めていく**観点からどのような制度整備が考えられるか

様々な目的で国境を越えた送金を行う**クロスボーダーの収納代行サービス**が登場している。

- こうしたサービスと、**資金移動業者による送金サービスとの規制の衡平**をどのように考えるか

資金決済制度関係＜暗号資産等分野＞

暗号資産交換業者の国際的な破綻事例が発生した。

- グローバルに活動する暗号資産交換業者が破綻した場合等に、**国内の利用者財産の返還**を担保する仕組みが考えられないか

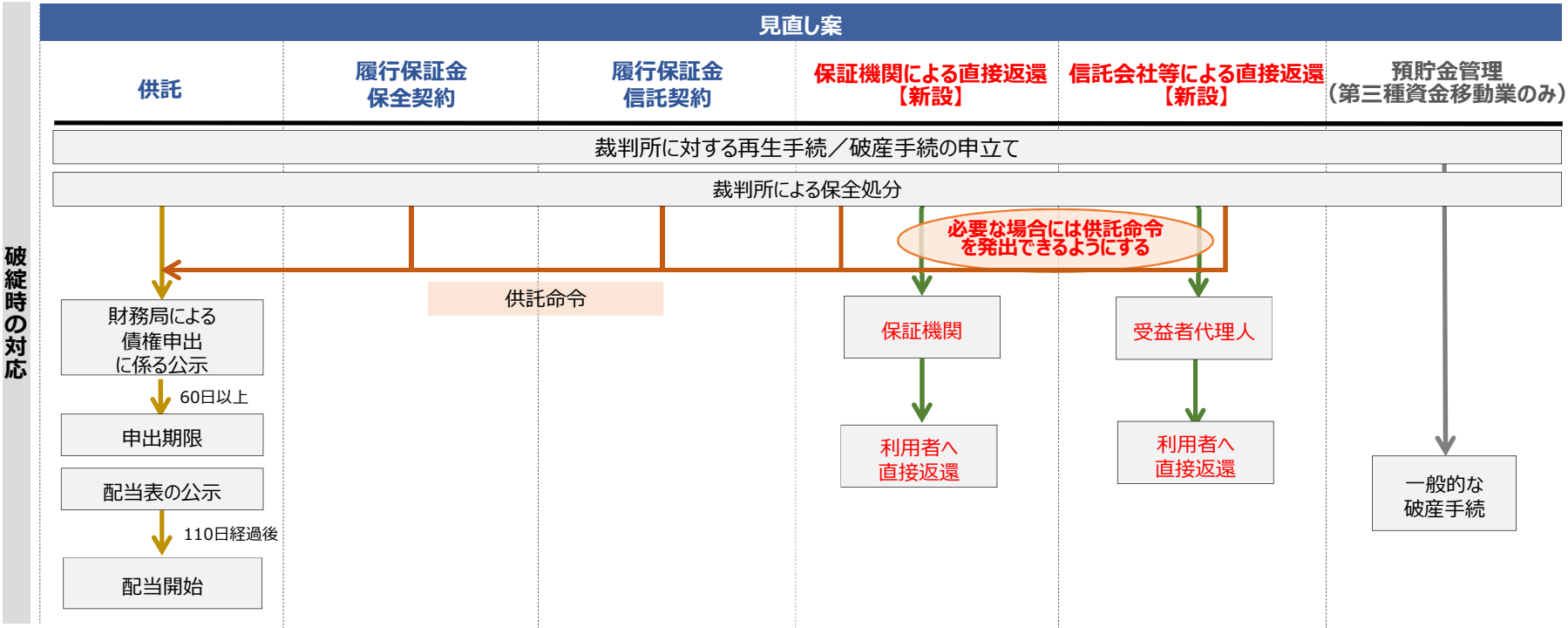
特定信託受益権の発行見合い金について、全額を預貯金で管理することが求められている。

- 電子決済手段としての価格安定性、流動性、償還確実性を確保しつつ、**管理・運用方法を柔軟化**することについてどう考えるか

※ 金融審議会総会（2024年８月26日）における金融担当大臣の諮問を受け、同年９月25日、第一回資金決済制度等に関するワーキング・グループを開催し検討を開始

資金移動業者の資産保全規制の見直し

- 資金決済法においては、資金移動業者に対して、利用者から受け入れた資金の全額を供託、銀行保証又は信託により保全することを求めた上で、破綻時には、保全された資金は、供託手続を通じて国が各利用者に対して還付手続を実施することとし、利用者への資金の還付に最低約170日という期間を要する制度となっている。
- 利用者の利便性確保及び資金移動業者による選択肢を増やす観点から、供託による返還手続や供託命令は残しつつ、保証機関や信託会社等から直接返還する方法についても認めることについてどのように考えるか。

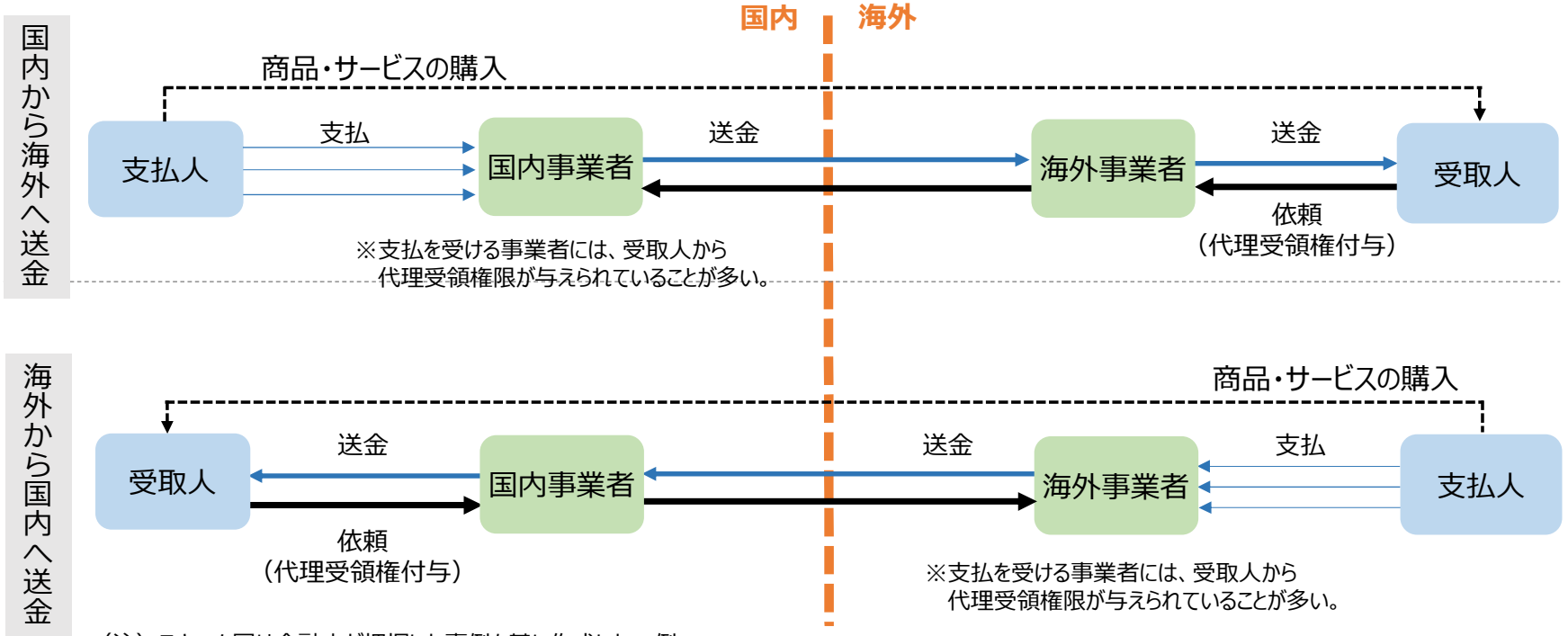


クロスボーダー収納代行

■ クロスボーダー収納代行とは、収納代行（注）のうち、国内と国外との間で資金移動が行われるものを想定。

■ クロスボーダー収納代行においては、①支払人の二重支払のリスク、②資金決済の遅延等リスク、③利用者情報保護上のリスク、④詐欺やマネー・ローンダリング等の不正利用リスクが考えられるところ、我が国においては、クロスボーダー収納代行業者に対して金融規制が必ずしも課されているわけではない。

（注）収納代行とは、代金引換を含め、①金銭債権を有する債権者から委託又は債権譲渡を受けて債務者から資金を収受し、②当該資金を直接輸送することなく債権者に移転させる行為が典型的なものと考えられる。



（注）スキーム図は金融庁が把握した事例を基に作成した一例

特定信託受益権の発行見合い金の管理・運用のあり方

- 特定信託受益権型のステーブルコイン（信託会社等により発行される、電子決済手段の一類型）は、発行見合い金の全額について、同じ通貨建ての要求払いの預貯金での管理が求められている。
- 海外では、ステーブルコインの裏付け資産について、一定の条件を課した上で預金以外の資産での運用を認めている例もある。

保護法域	規制（案）
米国（NY州）[1]	ステーブルコインの発行者に対して、満期まで３か月以内の米国債等の安全資産での運用を認めている。
欧州[2]	電子マネートークンの発行者に対して、発行見合い金の30%以上（大規模な顧客基盤、高い時価総額、多数の取引等の一定の基準を満たすことでEBAにより重要（significant）と判断されたトークンの場合は60%以上）を一定の格付以上の信用機関に対する預貯金で運用するよう求め、残りは高い流動性を持つ金融商品に対して、最小限の市場・信用・集中リスクにおいて運用することを認めている。
英国[3]	ステーブルコインの裏付け資産として認められるものは、短期現金預金及び１年以内に満期を迎える国債。 システミックな決済手段として利用されるステーブルコインの場合、裏付け資産として認められるものは、発行見合い金と同額での中央銀行への預金。
シンガポール[4]	ステーブルコインの裏付け資産は、以下の２要件を満たすように構成することとしている。 ⑴ステーブルコインがペッグされている通貨建ての ⑵現金　又は 現金同等物　又は 満期が３か月以内の債券で、 ①ペッグされている通貨の政府若しくは中央銀行　又は ②信用格付が「AA-」以上の国際政府組織 により発行されること。

（出典）

[1] ニューヨーク州Department of Financial Services「Virtual Currency Guidance」（米ドル担保ステーブルコインの発行体向けのガイダンス、2022年６月公表）を参照。

[2] EBA「Final Report Draft Regulatory Technical Standards to further specify the liquidity requirements of the reserve of assets under Article 36(4) of Regulation (EU) 2023/1114」（EU暗号資産市場規制（MiCA、2024年６月施行）第36条４項の規制技術基準に関する最終報告書、2024年6月公表）を参照。

[3] FCA「DP23/4: Regulating cryptoassets Phase 1: Stablecoins」（ステーブルコイン規制に関するディスカッションペーパー、2023年11月公表）を参照。システミックな決済手段として使用されるステーブルコインについては、Bank of England「Discussion paper Regulatory regime for systemic payment systems using stablecoins and related service providers」（ステーブルコイン及び関連事業者向けのシステミックな決済システムに関する規制枠組みをまとめたディスカッションペーパー、2023年11月公表）を参照。

[4] MAS「CONSULTATION PAPER Proposed Regulatory Approach for Stablecoin-Related Activities」（ステーブルコインの規制方針に対する市中協議文書、2022年10月）を参照。なお、市中協議結果である「Response to Public Consultation on Proposed Regulatory Approach for Stablecoin-related Activities」（2023年８月）でも規制概要に変更はなかった。

金融セクターにおけるAIのユースケースの広がり

生成AIの登場で広がる活用事例

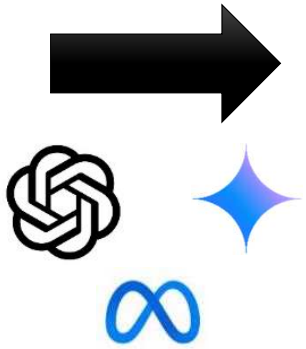
✓ 不正検知や市場予測、マーケティング等で主に活用されてきたAIが、テキスト等の生成を強みとするLLM（大規模言語モデル）／生成AIの登場により、業務の更なる効率化・高度化や新たな金融サービスの提供に繋がるユースケースが登場しつつある。

現在

セキュリティに関する業務を中心にML（機械学習）などを主に活用

- ✓ 不正検知
- ✓ ポートフォリオの最適化
- ✓ アルゴリズムを活用した取引
- ✓ リスク分析
- ✓ 顧客体験向上
  （パーソナライズドサービス等）

生成AIの進展



今後の見通し

更なる業務効率化や新しい価値創造を目的とした**生成AIの活用**の進展

- ✓ ドキュメント作成（稟議書、議事録等）
- ✓ 顧客体験の更なる向上
  （コールセンター業務支援、マーケティング高度化等）
- ✓ データ分析の高度化（合成データの生成等）

参考：“State of AI in Financial Services: 2024 trends” NVIDIA, 2024

金融セクターにおける生成AIの事例（ユースケース）

国内で模索されている事例

業務効率化

営業資料の効率的な作成などの個別業務の効率化への活用に加え、既存業務プロセス全体の効率化を図る事例が模索されている。

足元の取組

個別業務の効率化

- ✓ **ドキュメント作成等**：
  メール文や稟議書、議事録等の作成、調査、要約、翻訳、ソースコードの生成などに活用。
- ✓ **社内研修の高度化**：
  営業のロールプレイングに、AIアバターをマニュアルや講師の代わりに顧客として活用。
- ✓ **社内FAQ**：
  「マニュアル・規約」から、質問と回答の同時生成を試行。該当資料を読み込ませるだけで、自動的に「質問と回答」のセットを自動で生成。

将来

業務プロセス全体の最適化

- ✓ **営業活動の高度化**：
  CRMに蓄積されたデータを活用した、営業のネクストアクションの提案等。
- ✓ **ローン催促最適化：**
  ローン借入者に適切なタイミングを検知し、通知を行い、必要な支払金額を事前に通知し延滞を防ぐ。

CX（顧客体験）の向上

顧客から受けた問い合わせを、生成AIを活用することでより効率的に回答。人の目を通すことを前提とした出力が現在活用されている。

足元の取組

人の判断を前提とした活用

- ✓ **チャットボットでの活用**：
  チャットに質問した場合に、左側に回答案とともに右側に質問との類似性の高い「質問・回答」の上位3セットを表示。複数の「質問・回答」を跨いだ回答を自動生成。
- ✓ **コールセンターでの対応**：
  問い合わせを受け、生成AIで作成された回答文案を推敲、最終確認したうえでオペレーターから回答。

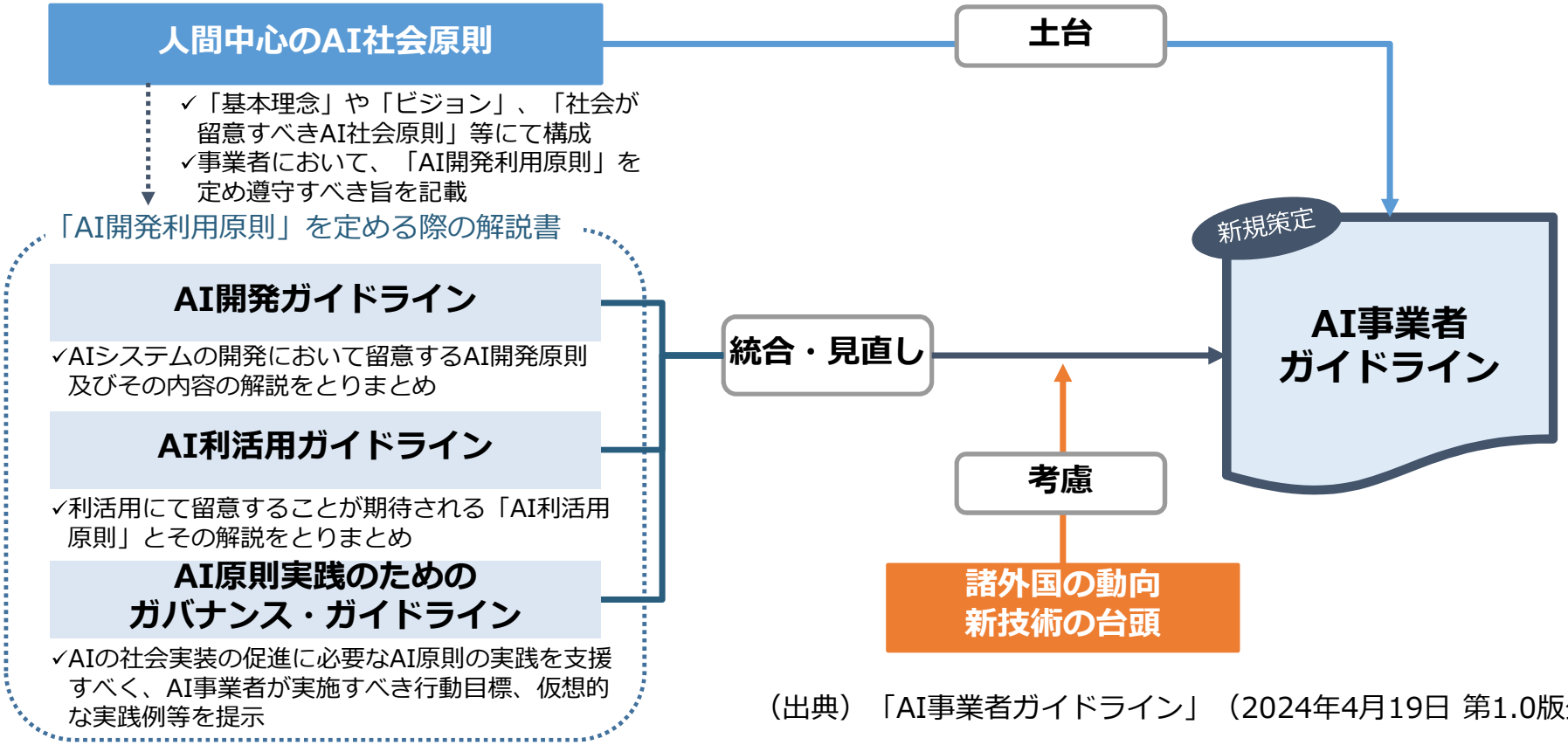
将来

出力結果を直接顧客に提示

- ✓ **ATMの高度化**：
  「ATMの照会はATMが回答」を目指し、問い合わせへの回答を自動で生成するだけでなく、話し始めた顧客の言語に応じて言語を変更する等。人との対話へ近似、回答精度（正確性）と回答性能（速度）等が課題。

「AI事業者ガイドライン」の策定（2024年4月19日 第1.0版公表、経済産業省・総務省）

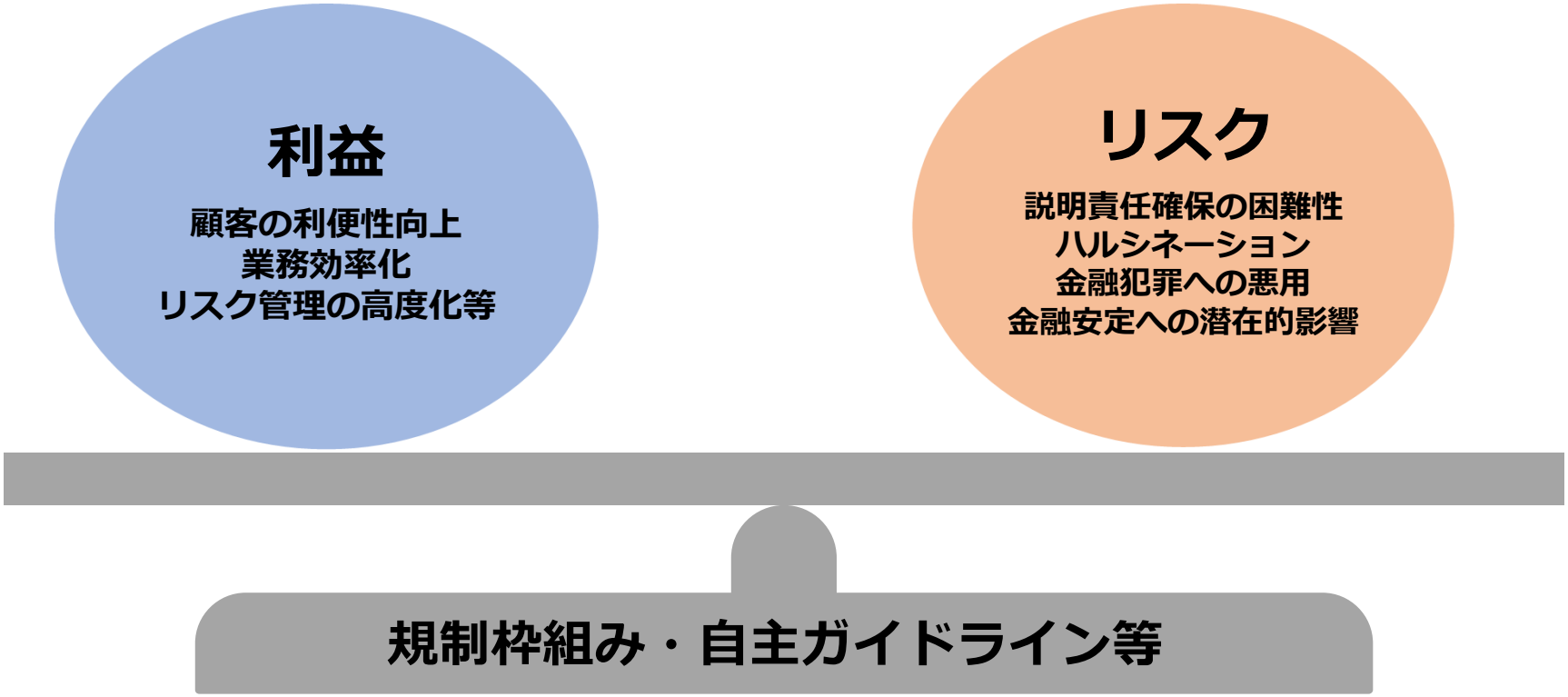
- 「AI事業者ガイドライン」は、「人間中心のAI社会原則」 を土台としつつ、我が国における3つのガイドラインを統合し、諸外国の動向や新技術の台頭を考慮して策定する。
- これまでのガイドラインとの整合性を担保することで、事業活動を支えるAIガバナンスの仕組みとして、連続性がある発展を遂げていくことが期待される。



（出典）「AI事業者ガイドライン」（2024年4月19日 第1.0版公表）

リスク低減とイノベーションに配慮した取組みの必要性

- ✓ AI/ML等の活用によって得られる**利益と、潜在的リスクへの対応とのバランス**を取ることが求められる。
- ✓ **チャレンジしないリスク**も認識すべき。
- ✓ 金融庁としては、金融セクターにおける**適切なリスクのコントロールが行われつつ、持続可能なユースケースが発展することが重要と考えており、様々な形の支援を行っていく。**



ご清聴ありがとうございました。

金融庁公式X（旧Twitter）のご紹介

- ◆ 金融庁では、ウェブサイトだけでなく金融庁日英公式X（旧Twitter）においてもタイムリーな情報発信を行っています。
- ◆ 是非フォローいただき、最新の情報をご確認ください。

日本語公式アカウント

https://x.com/fsa_JAPAN

英語公式アカウント

https://x.com/JFSA_en