ChatGPT

AIミュトス官民会議の深掘り調査報告

Executive Summary

本件の本質は、AI一般論ではなく、「高度なサイバー能力を持つ招待制AIモデルが、金融システムに対する脆弱性発見・悪用の速度と規模を変えうる」という、きわめて具体的な危機管理課題に、日本[1]の金融当局と業界中枢が初めて官民で向き合った点にある。4月22日の片山会見では、金融庁・日銀・3メガバンク・取引所による会合開催が事前告知され、4月24日の会議後には作業部会の立ち上げと「事案が発生した時の備え」の重要性が共有された。FNNは片山氏がこれを「今そこにある危機」と表現したと報じている。[2]

ただし、これはゼロから始まった議論ではない。金融庁は2025年6月から12月にかけてAI官民フォーラムを開催し、その知見を反映したAIディスカッションペーパー1.1版を2026年3月に公表した。日本銀行[3]も2025年9月時点で、約5割の金融機関が生成AIを利用済み、試行中を含めると7割強、将来的な試行・利用検討まで含めると9割強に達すると整理している一方、モニタリング、サードパーティ管理、サイバー対策にはなお改善余地が大きいと示している。[4]

本報告では、Mythosを固有名詞としてはアンソロピック[5]の「Claude Mythos Preview」と捉えつつ、分析概念としての「AI神話」を「AIはまだ遠い将来の話だという過小評価」と「防御用AIを導入すれば解決するという過大期待」の双方を指すものとして定義する。公式資料が示す実像はその中間であり、AIは防御能力を引き上げる一方で、ゼロデイ探索、データ漏えい、プロンプトインジェクション、第三者依存の集中、専門人材不足を同時に悪化させうる。[6]

短期的には、金融システム全体に直ちに資本・流動性不安が生じる蓋然性は高くない。実際、日銀は2026年4月時点で、わが国金融システムは「全体として安定性を維持している」と評価している。しかし中期以降は、顧客接点、コード生成、不正検知、運用補助、決済・市場インフラ補助へとAI利用が深く入るほど、AIサービス、クラウド、委託先への集中が単一障害点としてシステミック・リスク化しやすくなる。結論として必要なのは、会議の継続開催ではなく、日本版Project Glasswingに相当する常設の官民運用体制である。[7]

記事と会議のファクト整理

朝日新聞記事の全文は会員限定のため本調査では取得できず、以下の要約は検索スニペットと、それを補強する公式発言・当日報道の突合に基づく。確認できる記事の骨子は、①片山金融相がAIミュトスを「今そこにある危機」と位置づけたこと、②金融庁・日銀・主要金融機関による初の官民会議が開催されたこと、③日本版Project Glasswingに相当する作業部会構想が前面に出たこと、である。検索スニペットには政府によるモデル利用権購入の検討も示唆されるが、この点は本調査で確認した一次資料では裏づけを得られなかったため、未指定と扱う。[8]

区分	参加者	当時の肩書	会議での役割	確認根拠
招集者	**片山さつき**[9]	財務大臣兼内閣府特命担当大臣（金融）	会合招集、危機認識の共有、作業部会設置の表明	[10]

区分	参加者	当時の肩書	会議での役割	確認根拠
当局	**金融庁** [11]	金融行政当局	「私たちのチーム」として主管、事務レベル作業部会の母体	[12]
中央銀行	**植田和男** [13]	日銀総裁	中央銀行側の参加者として出席確認	[14]
銀行業界	**全国銀行協会** [15] / **加藤勝彦** [16] / **みずほ銀行** [17]	全銀協会長・みずほ銀行頭取	銀行業界代表。みずほ側の代表を兼ねる形で確認	[18]
メガバンク	**三菱UFJ銀行** [19] / **大沢正和** [20]	頭取	メガバンク代表として出席確認	[18]
メガバンク	**三井住友銀行** [21] / **福留朗裕** [22]	頭取	メガバンク代表として出席確認	[18]
市場インフラ	**日本取引所グループ** [23] / **山道裕己** [24]	CEO	市場インフラ代表として出席確認	[18]

現時点で確認できる公式発言の要点は明確だ。4月22日の片山会見では、会議の目的を「状況の認識とか意見交換」とし、「国際金融社会であちこちで問題が指摘され始めていることについて話し合いたい」と述べた。4月24日の会議後には、金融システムは相互接続性が高くリアルタイム処理ゆえに「市場への影響や信用不安にまで波及し得る」と説明し、事務レベルの作業部会を立ち上げたと明らかにした。ロイターはこの会議で「インシデントが発生した時の備えが、これまで以上に重要」との認識が共有されたと報じている。会議の正式名称については、ブルームバーグが「AI脅威に対する金融分野のサイバーセキュリティ対策強化に関する官民連携会議」と伝えている。なお、議事次第、配布資料、議事要旨、完全な出席者名簿は本調査では取得できず、未指定とする。 [25]

本件は単発の反応ではなく、海外での制度整備と国内の先行議論の延長線上にある。米国では2月に財務省が金融セクター向けAIリスク管理の公民成果物を公表し、4月7日にAnthropicがProject Glasswingを発表した。国内では4月20日に政党レベルの先行議論があり、4月22日に片山会見で会合開催が明言され、4月24日に官民連携会議と作業部会設置へ至っている。 [26]

```
timeline
    title AIミュトス問題を巡る主な流れ
    2025-06 : 金融庁AI官民フォーラム開始
    2025-09 : 日銀が生成AI利用状況調査を公表
    2025-10 : FSBがAI監視レポートを公表
    2026-02 : 米財務省がAIEOG成果物を段階公表
    2026-04-07 : AnthropicがMythos PreviewとProject Glasswingを発表
    2026-04-20 : 自民党合同会議で日本版Glasswingを提起
    2026-04-22 : 片山会見で4月24日の会合開催を明言
    2026-04-24 : 官民連携会議開催、作業部会設置
```

4月20日の政党合同会議は前史として重要である。そこでは、自由民主党 [27] の合同会議で、平将明 [28] が「人間の力では見つけられなかった脆弱性を見つけられる一方、攻撃にも使える」と述べ、日本版Project Glasswingの必要性を訴えた。会議は伊藤達也 [29] が会長を務める金融調査会との合同開催で、Mythos問題は政党論点から行政・金融システム論点へと急速に移行したと読める。 [30]

AIミュトスの定義と懸念

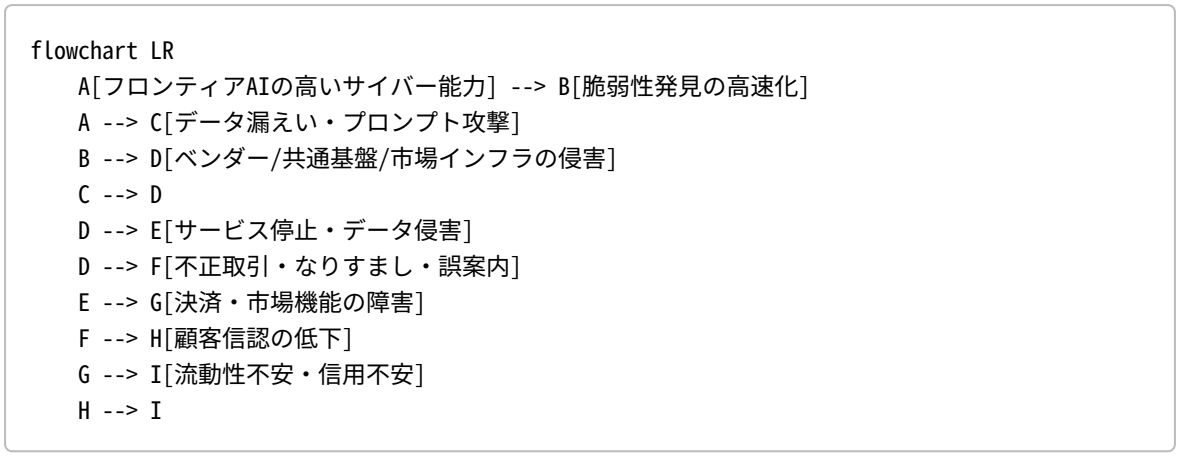
一次ソースで確認できる「AIミュトス」の公式定義は、Anthropicの未公開フロンティア・モデル「Claude Mythos Preview」である。Anthropicはこれを「汎用の言語モデル」だが「コンピューターセキュリティ作業で際立って高い能力を示す」と位置づけ、防御的サイバーセキュリティ・ワークフロー向けの招待制リサーチプレビューとして限定提供している。Project Glasswingは、その能力を「世界の最重要ソフトウェアの防御」に使うための公民連携枠組みであり、アクセスは招待制で、セルフサービス登録はない。 31

重要なのは、公式資料がMythosを「未来の抽象的脅威」とは書いていない点である。Anthropicは、同モデルが主要OSと主要ブラウザのすべてでゼロデイ脆弱性を特定し悪用できたと説明し、既に数千件の高重大度脆弱性を発見したとしている。だからこそProject Glasswingは、「いつか必要になる」施策ではなく、「今から防御に先行投入する」ための施策として設計されている。 32

他方で、「AI神話」という日本語表現は、少なくとも本件の公式資料には定義語として存在しない。そこで本報告では、分析上の定義として「AI神話」を、第一に「まだ金融システムを実質的に脅かさない」という過小評価、第二に「防御用AIを導入すれば十分」という過大期待、の双方を含む過信と定義する。この定義の妥当性は、G7サイバー専門家グループがAIを防御と攻撃の両面から捉え、FSBがAI導入の脆弱性として第三者依存、相関、サイバー、モデル・ガバナンスを並列に挙げていることによって支えられる。 33

懸念点	何が問題か	金融業固有の増幅要因
ゼロデイ探索・悪用の高速化	AnthropicはMythosが主要OS・ブラウザでゼロデイを発見・悪用できたと説明している。これは脆弱性探索コストを攻撃側にも防御側にも大きく下げる。	金融機関は共通ソフトウェア、共通ベンダー、共通委託先、共通認証基盤を多用しており、同一脆弱性が多数先へ同時波及しやすい。 34
第三者依存・集中	FSBとG7は、AIサービス提供者や関連クラウドへの集中が、単一障害点やシステム横断の波及経路になり得ると整理している。	金融ではアウトソース先停止が即時に決済、取引、顧客接点へ影響しやすい。DORAが第三者リスク管理と重要ICT提供者監督を中核に置くのはこのためである。 35
AIそのものへの攻撃	G7は、データポイズニング、データ漏えい、プロンプトインジェクションを明示的に挙げる。	金融機関のモデルには顧客情報、内部手順、AML/CFTルール、運用ルールが接続されやすく、漏えい・誘導の被害が大きい。 36
顧客接点・不正検知の逆用	EBAはEU銀行の92%がAIを導入済み、55%がGPAIまたはagentic AIを消費者向けプロセスで用いているとする。	顧客対応、本人確認、不正検知、FAQ、自動案内など、攻撃者が外部から刺激できる面が増える。説明責任と人間の介入設計も必要になる。 37
人材・監督の非対称	G7はAI literacy不足をリスクとして挙げ、日銀調査ではモニタリングやサードパーティ・サイバー対策に改善余地がある先が5割程度だった。	金融では制度・法務・IT・サイバー・事業が分断されやすく、横断人材の不足が初動遅延と誤判断につながりやすい。 38

金融システムへの伝播は、単一の「AIリスク」ではなく、既存の運用リスク、サイバーリスク、委託先リスク、モデルリスクがAIで増幅される複合経路として理解する方が正確である。Katayama発言の「相互接続性が高くリアルタイムで処理される」という点は、その伝播構造を簡潔に言い表している。 39



リスク分析

日本の現行対策は、ゼロではなく相応に厚い。金融庁のサイバーガイドラインは、金融サービス利用者保護と金融システム安定の観点からサイバーセキュリティ強化を不可欠と位置づけ、監督指針・事務ガイドラインで個社の管理態勢を求めている。さらに、CSSA、ASM、TPCRM調査、AIディスカッションペーパー、AI官民フォーラムが存在する。問題は「土台がない」ことではなく、「フロンティアAIを前提とした運用層の詰め」がまだ十分ではないことにある。 40

以下の評価は、公開資料に基づく筆者判断である。発生確率は今後12〜24カ月、影響は単一機関被害ではなく、金融システム全体への波及可能性を基準に置いた。 41

類型	リスク内容	典型的な事例・伝播経路	発生確率	影響	既存対策の有効性	総合評価
技術的	外部脆弱性の探索・悪用の高速化	共通ミドルウェア、認証、ブラウザ、OS起点の侵害が、複数金融機関や委託先へ同時波及	高	極大	ASMや脆弱性管理は有効だが、攻撃速度上昇に対しては部分的	最優先で強化が必要 42
技術的	プロンプトインジェクション、データ漏えい、訓練・参照データ汚染	社内ナレッジ接続型AIや顧客向けAIからの情報漏えい、誤応答、誘導	高	大	利用ルール整備は進むが、日銀調査では見直し・モニタリングに課題	高リスクだが管理でかなり低減可能 38
運用的	第三者依存・集中	クラウド、AI API、外部開発基盤、SOC、KYC/AMLベンダー等の停止や侵害	中高	極大	FSAのTPCRM調査、DORA型の考え方は有効。ただし日本はまだ制度・監督運用の厚みを増す段階	システミック性が高い 43

類型	リスク内容	典型的な事例・伝播経路	発生確率	影響	既存対策の有効性	総合評価
運用的	初動・復旧・人材の不足	CISO/CRO/法務/事業部の役割不明確、生成AI事故用プレイブック未整備、専門人材不足	高	大	個社のSOC/CIRTや訓練は有効だが、セクター横断演習は不足	かなり現実的な弱点 [44]
規制的・法務的	顧客接点AI・agentic AIの説明責任、適合性、責任帰属	誤案内、差別的出力、誤作動、顧客損失、苦情・訴訟・行政対応	中	大	AI DPは論点整理として有効だが、拘束力ある統一運用ルールはまだ形成途上	近い将来に重要度上昇 [45]
システム的	AI支援の不正、誤情報、相関・群集行動	AI生成の詐欺、偽情報、取引判断の相関上昇、市場機能のゆがみ	中	大〜極大	既存の市場監視・不正検知で一部対応可能だが、AI特有の速度・規模に課題	中長期で重くなる [46]

既存対策の有効性を厳密にみると、第一に、金融庁ガイドラインやCSSAは「最低限の統制と対話の共通言語」として有効である。第二に、ASMやリスクスコアリングは、外部に露出した資産や第三者リスクの把握には効果が高いが、FSA委託調査が指摘するとおり、False Positiveが多く、チューニングや解釈能力が要る。第三に、AI DPや官民フォーラムはガバナンス論点を前進させたが、防御的ユースケースをセクター全体で共同運用する仕組みにはまだ至っていない。つまり、現在の統制は「基礎工事」としては相応だが、Mythos級の能力を前提とした「共同防御の運用設計」は未完成である。 [47]

個社開示でも危機認識は一致している。みずほ銀行 [17] グループは「サイバー攻撃」をトップリスクに挙げ、AIの急速な普及や第三者管理不足が顧客情報流出やサービス中断を招きうると明記している。三菱UFJ銀行 [19] グループも、サイバー攻撃に関するITリスクをトップリスクの一つと位置づけ、Cyber Security DivisionがAIなど新技術の企画・設計段階から参画するとしている。これは、官民会議が突然の政治イベントではなく、個社の既存トップリスク認識をマクロ化したものだと示唆する。 [48]

インパクト予測とシナリオ

出発点として押さえるべきなのは、2026年4月の日銀評価である。日銀は、わが国金融システムは全体として安定性を維持しており、極端なストレスにも耐えうる資本基盤と資金調達基盤を有すると整理している。したがって、Mythos問題の短期インパクトは、直ちに金融危機へ直結するというより、サイバー・オペレーショナル・レジリエンスの前倒し強化として現れる公算が大きい。 [49]

時間軸	主要インパクト	中心チャネル	監視すべきシグナル
短期	サイバー防御投資の増加、ASM/脆弱性管理の前倒し、作業部会運営、委託先調査の強化	脆弱性管理、委託先監査、経営会議のアジェンダ昇格	官民作業部会の設計、共同演習有無、重要ベンダー棚卸し、生成AIの社内利用制御の見直し [50]

時間軸	主要インパクト	中心チャネル	監視すべきシグナル
中期	顧客接点AI、コード生成AI、agentic AIの浸透に伴う運用リスク上昇と生産性向上の併存	第三者依存、説明責任、モデル監視、AI固有の事故対応	生成AIの顧客向け利用拡大、55%のEU銀行にみられるagentic/GPAI活用の日本版波及、監督対話の高度化 [51]
長期	特定AI/クラウド基盤への集中、相関上昇、AI起因の市場慣行変化、規制の再設計	重要第三者監督、金融市場での群集行動、決済・市場インフラのAI依存	DORA型監督の国内実装議論、FSB/ESRBが示す集中・相関・システミック性の指標整備、制度改正議論 [52]

シナリオは、2026〜2029年を念頭に置くと、次のように整理できる。確率は公開資料に基づく筆者の主観評価であり、将来を断定するものではない。 [53]

シナリオ	主観確率	発火条件	金融システムへの帰結
ベスト	20〜30%	日本版Glasswing相当の常設体制が早期に整備され、金融機関・ベンダー・当局が共同で防御的評価・修正を回す	大規模障害は回避され、AIは不正検知・監視・復旧補助の面で純便益が先行。コスト増はあるが、信認は維持される。 [54]
ベース	50〜60%	近い将来に軽微〜中規模のAI関連インシデントやニアミスが散発し、規制・監督・実務が追い付いていく	個社・委託先レベルの障害や漏えいは発生しうるが、システム全体には波及せず、結果として監督強化・監査負荷増・委託先再編が進む。 [55]
ワースト	15〜25%	高度モデルの能力が悪意ある主体へ流出・模倣され、未修正脆弱性が決済・基幹系・市場インフラで同時多発的に突かれる	サービス停止、データ侵害、不正送金、市場インフラ障害が併発し、Katayama発言どおり市場影響と信用不安へ波及。流動性支援や市場安定化措置を伴う危機対応が必要になる。 [56]

より重要なのは、AI起因の金融危機は「AIが銀行を置き換える」形ではなく、「既存のサイバー・委託先・オペレーション・市場相関リスクが、AIによって時間圧縮され同時多発化する」形で現れやすい点である。この意味で、今の最大論点はAI規制単体ではなく、金融安定政策、サイバー政策、委託先監督、決済・市場インフラ政策の接続である。 [57]

海外比較

海外比較から見えるのは、先進当局のアプローチが「AIそのものの包括規制」よりも、金融システムに直結する部分での運用・監督・第三者管理の強化へ収斂しつつあることだ。米国 [58] は実務ツール中心、英国 [59] は監督対話とマクロプルーデンス中心、欧州連合 [60] はDORAを軸とした制度・監督連動型、という差がある。 [61]

地域	最新動向	中心文書・枠組み	長所	日本への示唆
米国	米財務省 [62] はAIEOGを通じて、AI Lexicon、金融向けAI RMF、サイバー・リスク管理の公民成果物を2026年2月に段階公表した。2024年報告でも国際協調、既存枠組みの補強、金融特化の情報共有を提言している。	Treasury AI RFI報告、AIEOG成果物、金融向けAI RMF、公民サイバー取組み [63]	実装可能なレキシコンとRMFを先に用意し、中小機関でも使える形に落としている。	日本でも金融庁主導で、AI用語集、金融向けAIリスク管理フレーム、事故分類・報告テンプレートを共通化すべき。
英国	イングランド銀行 [64] とFCA [65] はAI Consortium、AI Live Testing、監督優先事項を通じて継続監視を強化。BoEはFPCの4重点領域として、コア意思決定、金融市場、AIサービス提供者の運用リスク、外部サイバー脅威を監視すると明示した。	BoEのTSC報告応答、AI Consortium、FCA AI Live Testing [66]	監督対話、実地テスト、マクロプルーデンスを接続している。	日本でも、会議体だけでなく継続的なサーベイ、監督対話、限定的な安全な実運用テストの仕組みが必要。
EU	欧州銀行監督機構 [67] は92%のEU銀行がAI導入済み、55%が顧客向け工程でGPAI/agentic AIを活用と示した。DORAは2025年1月に適用開始され、ICTリスク管理、第三者管理、レジリエンステスト、重大インシデント報告、重要第三者監督を網羅する。欧州中央銀行 [68] と欧州システミック・リスク理事会 [69] は、AIをガバナンスとシステミック・リスクの観点から継続監視している。	EBA factsheet、DORA、ECB講演、ESRB報告 [70]	AIと無関係に見える運用レジリエンス規制を、AI時代の土台として機能させている。	日本もAI単独法議論だけでなく、第三者管理、レジリエンステスト、重大インシデント報告を金融横断で実務的に積み増すべき。

この比較に、金融安定理事会 [71] とG7の議論を重ねると、共通の論点はさらに鮮明になる。すなわち、AI関連の金融安定論点は、第三者依存・集中、サイバー、モデルリスク、データ品質・ガバナンス、そして当局による継続モニタリング能力の不足に集約される。日本がいま最も学ぶべきは、個別機関の自助努力よりも、業界横断で共通指標・共通演習・共通事故分類を持つことの重要性である。 [72]

実務提言

提言の基本方針は明快である。第一に「未知のAIを規制する」より先に、「既知の金融レジリエンス手法をAI前提で再設計する」べきである。第二に、個社統制だけでは不十分で、官民共同の防御運用が必要である。第三に、AI導入促進策とAIリスク抑制策を別々に管理せず、同じガバナンスの下で扱うべきである。 [73]

対象	優先度	具体アクション	期限感	主な根拠
金融機関	最優先	インターネット露出資産、共通ソフトウェア、委託先、AI API接続先を一体で棚卸しし、ASM、SBOM、脆弱性修正SLA、代替調達手順まで含む「AI時代版重要資産台帳」を整備する。	直ちに	FSAのASM監視方針、TPCRM調査、G7の第三者・供給網リスク整理。[74]
金融機関	最優先	生成AI・agentic AIを含む事故シナリオをBCPとサイバー演習に組み込み、顧客向けAI停止、コード生成停止、委託先切替、決済代替運用までを試験する。	3〜6カ月	日銀の業務継続・生成AI調査、MizuhoのSOC/CIRT体制、BoEの運用リスク重視。[75]
規制当局	最優先	金融庁ガイドラインをAI固有リスクへ拡張し、プロンプト管理、データ境界、モデル変更管理、AI事故報告、重要AI第三者管理を明文化する。	6〜12カ月	FSAガイドライン、AI DP 1.1、U.S. Treasury FS AI RMF、DORA。[76]
規制当局・中央銀行	高	官民作業部会を常設化し、業界横断の共通KPI、共通演習、共通インシデント分類、脅威情報共有の定例運用へ移行する。	直ちに開始	4月24日作業部会設置、FSBのモニタリング重視、G7の公私対話推奨。[77]
政府	最優先	日本版Project Glasswingを制度化し、厳格な管理下で防御目的のフロンティアAIアクセス、秘密保持付き脆弱性検証、重要ソフトウェアの共同点検を行う。	直ちに設計	Anthropicの枠組み、国内作業部会構想、政党レベルでのGlasswing提起。[78]
政府	高	国家サイバー政策と金融安定政策を接続し、重要金融インフラを対象にした法的セーフハーバー付き共同防御・共同演習の制度基盤を整える。	6〜12カ月	DORA、G7文書、FSA/BoJの連携実績。[79]
研究者	高	日本語環境・金融ドメイン特化で、ゼロデイ探索能力、プロンプト漏えい、agentic AIの暴走、顧客説明可能性を測る評価ベンチマークを整備する。	6〜18カ月	FSBの指標整備、BoEの追加調査要請、IMFのpayments/agentic AI問題提起。[80]
研究者	中	金融分野向けに、可観測性、ロギング、因果追跡、説明可能性、監査証跡を備えた「検証可能AI」研究へ資源を振り向ける。	継続	BISのデータ・ガバナンス論点、ECB/ESRBのガバナンス重視。[81]

優先順位を一言でいえば、いま必要なのは「新しい巨大な法律」よりも、「共同防御を可能にする共通運用」である。具体的には、金融機関は資産棚卸しと演習、当局は共通ルールとモニタリング、政府は安全な共同評価基盤、研究者は測定と検証可能性の整備に集中するのが最も費用対効果が高い。[82]

参考資料

本調査で未取得・未指定の事項は二つある。第一に、朝日新聞記事本文の全文。第二に、4月24日官民会議の正式な議事次第、配布資料、議事要旨、完全な出席者名簿である。したがって以下の参考資料一覧では、一次ソースを優先しつつ、会議当日の事実関係は公式会見要旨と複数報道の一致部分で補っている。[8]

国内の主要一次資料

1. 財務省「片山財務大臣兼内閣府特命担当大臣記者会見の概要（令和8年4月22日）」— 4月24日会合の目的、参加枠、問題認識の事前説明。 83
2. 金融庁「AIディスカッションペーパー（第1.1版）」— 2025年AI官民フォーラムの知見を反映した金融分野AIガバナンスの基礎文書。 84
3. 金融庁「金融機関のサードパーティ・サイバーセキュリティリスク管理強化に関する調査」— 米英EU大手金融機関のTPCRM/ASM実務を整理。 85
4. 日本銀行「金融機関における生成AIの利用状況とリスク管理」— 国内金融機関の生成AI利用実態と改善余地を示す。 86
5. 日本銀行「金融システムレポート（2026年4月号）」— 現時点の金融システム安定性とストレス耐性の評価。 49
6. 金融庁「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」— 金融分野サイバー監督の基礎文書。 87
7. 自民党「高度自律型AIの対策強化を最新AI『ミトス』巡り議論」— 官民会議に先行した政党レベルの問題提起。 30
8. みずほFG「Governance / Cybersecurity」およびMUFG「Risk Management」— 個社のトップリスク・CISO/SOC/CIRT体制の公開情報。 88

海外の主要一次資料

1. Anthropic「Assessing Claude Mythos Preview’s cybersecurity capabilities」— Mythosのサイバー能力評価。 89
2. Anthropic「Project Glasswing」— 防御目的の公民連携構想。 90
3. U.S. Treasury「Treasury Announces Public-Private Initiative to Strengthen Cybersecurity and Risk Management for AI」および「Treasury Releases Two New Resources to Guide AI Use in the Financial Sector」— AIEOGと金融向けAI RMFの公式説明。 91
4. U.S. Treasury「Treasury Releases Report on the Uses, Opportunities, and Risks of Artificial Intelligence in Financial Services」— 金融分野AI利用の包括整理。 92
5. G7 Cyber Expert Group Statement on AI and Cybersecurity — AI由来サイバーリスクの金融分野整理。 36
6. Bank of England「Response to TSC report on AI in financial services」— 英国のAI監督・マクロプルーデンスの最新整理。 93
7. EBA「Rising application of AI in EU banking and payments sector」— EU銀行のAI導入度と利用領域。 37
8. DORA解説ページ — ICTリスク管理、第三者管理、レジリエンステスト、重要第三者監督の枠組み。 94
9. ECB/ESRB/FSBのAI関連文書 — ガバナンス、集中、相関、システミック・リスクの観点。 95
10. BIS・IMFの分析資料 — AIが金融安定、データ・ガバナンス、paymentsに与える中長期波及。 96

会議当日の補助資料・報道

1. 朝日新聞記事検索スニペット — 片山発言と会議の骨子。本文未取得。
2. ブルームバーグ（Yahoo!ファイナンス転載）— 会議名、参加者、作業部会の設置。 18
3. ロイター — 「備え」の重要性に関する共有認識。 97
4. FNNプライムオンライン — 「今そこにある危機」という表現の報道。 98

---

1 52 79 94 https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

2 3 8 10 12 25 65 71 83 https://www.mof.go.jp/public_relations/conference/my20260422.html
https://www.mof.go.jp/public_relations/conference/my20260422.html

4 45 84 https://www.fsa.go.jp/news/r7/sonota/20260303/aidp_version1.1_revised.pdf
https://www.fsa.go.jp/news/r7/sonota/20260303/aidp_version1.1_revised.pdf

5 15 26 60 61 63 82 91 https://home.treasury.gov/news/press-releases/sb0395
https://home.treasury.gov/news/press-releases/sb0395

6 9 16 20 31 32 34 41 42 89 https://red.anthropic.com/2026/mythos-preview/
https://red.anthropic.com/2026/mythos-preview/

7 23 49 https://www.boj.or.jp/research/brp/fsr/fsr260421.htm
https://www.boj.or.jp/research/brp/fsr/fsr260421.htm

11 43 85 https://www.fsa.go.jp/common/about/research/20260403/20260403.html
https://www.fsa.go.jp/common/about/research/20260403/20260403.html

13 30 https://www.jimin.jp/news/information/213064.html
https://www.jimin.jp/news/information/213064.html

14 17 18 21 24 27 28 39 50 56 77 https://finance.yahoo.co.jp/news/detail/c8a9ea365104537fd14396e0aca80ab4646490d1
https://finance.yahoo.co.jp/news/detail/c8a9ea365104537fd14396e0aca80ab4646490d1

19 29 44 48 88 https://www.mizuhogroup.com/who-we-are/governance?tab=cybersecurity
https://www.mizuhogroup.com/who-we-are/governance?tab=cybersecurity

22 67 98 https://www.fnn.jp/articles/-/1035741
https://www.fnn.jp/articles/-/1035741

33 36 38 58 68 69 https://home.treasury.gov/system/files/136/G7-Cyber-Expert-Group-Statement-AI-and-Cybersecurity-2025.pdf
https://home.treasury.gov/system/files/136/G7-Cyber-Expert-Group-Statement-AI-and-Cybersecurity-2025.pdf

35 46 57 80 https://www.fsb.org/uploads/P101025.pdf
https://www.fsb.org/uploads/P101025.pdf

37 64 70 https://www.eba.europa.eu/sites/default/files/2025-09/146b3558-d026-47bf-a872-f05e93ed30d2/Rising%20application%20of%20AI%20in%20EU%20banking%20and%20payments%20sector.pdf
https://www.eba.europa.eu/sites/default/files/2025-09/146b3558-d026-47bf-a872-f05e93ed30d2/Rising%20application%20of%20AI%20in%20EU%20banking%20and%20payments%20sector.pdf

40 62 76 87 https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf
https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf

47 https://www.fsa.go.jp/common/about/research/20260403/02.pdf
https://www.fsa.go.jp/common/about/research/20260403/02.pdf

51 55 75 86 https://www.boj.or.jp/research/brp/fsr/fsrb250930.htm
https://www.boj.or.jp/research/brp/fsr/fsrb250930.htm

53 54 59 78 90 https://www.anthropic.com/glasswing
https://www.anthropic.com/glasswing

66 93 https://www.bankofengland.co.uk/-/media/boe/files/letter/2026/response-to-tsc-inquiry-report-on-ai-in-financial-services
https://www.bankofengland.co.uk/-/media/boe/files/letter/2026/response-to-tsc-inquiry-report-on-ai-in-financial-services

72 https://www.fsb.org/2025/10/monitoring-adoption-of-artificial-intelligence-and-related-vulnerabilities-in-the-financial-sector/
https://www.fsb.org/2025/10/monitoring-adoption-of-artificial-intelligence-and-related-vulnerabilities-in-the-financial-sector/

73 https://home.treasury.gov/news/press-releases/sb0401
https://home.treasury.gov/news/press-releases/sb0401

74 https://www.fsa.go.jp/common/ronten/202601/03.pdf
https://www.fsa.go.jp/common/ronten/202601/03.pdf

81 https://www.bis.org/fsi/publ/insights73.pdf
https://www.bis.org/fsi/publ/insights73.pdf

92 https://home.treasury.gov/news/press-releases/jy2760
https://home.treasury.gov/news/press-releases/jy2760

95 https://www.bankingsupervision.europa.eu/press/speeches/date/2026/html/ssm.sp260224~6c5b64a77a.en.html
https://www.bankingsupervision.europa.eu/press/speeches/date/2026/html/ssm.sp260224~6c5b64a77a.en.html

96 https://www.bis.org/publ/work1194.pdf
https://www.bis.org/publ/work1194.pdf

97 https://www.newsweekjapan.jp/articles/-/320632?display=b
https://www.newsweekjapan.jp/articles/-/320632?display=b