2026 年 11 月

フロンティア AI による脅威変化を踏まえた

金融機関・フィンテック事業者間のセキュリティ対応に関する論点案

〔2026 年 11 月〕

一般社団法人 Fintech 協会（Fintech Association of Japan, FAJ）

(C) 2026 Fintech Association of Japan

1．はじめに

当協会は、フロンティア AI による脅威環境の変化を踏まえ、金融機関とフィンテック事業者の間でセキュリティ対応をどのように進めるべきかについて、2026 年 7 月から検討を重ねてきた。2026 年 9 月 11 日には、金融庁及び日本銀行にオブザーバーとして参加いただき、金融機関、フィンテック事業者、監査法人等による検討会合を開催した。本書は、その検討の第一弾として、現時点で見えている論点を案として示すものである。

金融庁及び日本銀行は、2026 年 5 月 22 日、「フロンティア AI による脅威変化を踏まえた金融機関等の短期的な対応」に係る要請を発出した（金総政第 3245 号、金企市第 498 号、金監督第 1384 号。以下「上記要請」）。上記要請は脆弱性及び修正プログラムが短期間に集中して発見・提供される可能性に備え、9 項目にわたる短期的な対応を求めるものである。

本書は上記要請の存在を前提とし、上記要請に示された事項は重ねて記載しないこととしている。本書の対象は、金融機関を念頭に置いた上記要請を、オープン API 等により接続する事業者等との間で実施する際に、さらに具体化を要する部分である。

本書は当協会として結論を確定したものではなく、金融機関に新たな義務を課すものでも、フィンテック事業者に一律の水準を求めるものでもない。また、本書に記載した事項を満たさないことが、直ちに不備を意味するものでもない。各項目に付した当協会の考えは、今後の検討の方向性の案を示すものであり、関係各所からの意見を踏まえて、更に具体化・詳細化を進めることを意図している。

なお、攻撃側の能力は短い期間で変化し強力化することが想定されるため、本書も版と改訂日を付し、継続して改訂することを前提としている。

補足：9 月 11 日の会合はチャタムハウス・ルールによったため、本書に発言者は記載していない。

2．本書が扱う範囲と論点

本書は表題に「フロンティア AI による脅威変化」を掲げているが、検討を重ねる過程で、当初の想定より論点が広がっているため、性質の異なる事項の混在と、求められる対策が過剰になることを避ける目的で、論点を次の四つに区分した。

論点 1　フロンティア AI により脆弱性及び修正プログラムが短期間に集中して発見・提供されることへの対応

検討の起点であり、同上記要請が短期的な対応として直接に扱っているのもこの論点である。本書においても中心となる論点であり、第 4 章から第 8 章がこれに該当する。

論点 2　フロンティア AI が攻撃に悪用されることへの対応

公表を経ない脆弱性の悪用や、攻撃の高速化への備えである。上記要請は、短期的な対応を応急的措置と位置づけ、中長期的には脆弱性対応の自動化等への移行に取り組むことが必要であるとしている。論点 1 と連続するが対応の時間軸が異なっており、第 3 章と第 9 章(3)で扱う。

論点 3　委託先・接続先が利用する AI と、そのデータの所在

委託先や接続先が、自らのサービスの中で、又は利用する SaaS 等を通じて、どのような AI を、どのような形で用いているか、当該 AI の処理機構や処理対象データがどこに置かれているかに関する論点である。同上記要請は明示的に言及しておらず、直接にサイバーセキュリティの問題に限られない論点でもある。第 7 章及び第 8 章で一部を扱い、第 9 章(1)で論点の所在を示す。

論点 4　AI エージェントによるアクセスの認証・認可と、AI エージェントを用いた取引

顧客側のエージェントが関与する取引における利用者本人及びエージェントの確認、利用者の意図の確認、更に事業者側がエージェントを提供する場合の相互の認証や意図確認に係る設計に関する論点であり、エージェンティックコマースや決済関連取引の監視にも波及しうる内容である。同上記要請が言及していない課題であるため、本書では論点の所在を示すにとどめ、第 9 章(2)で述べる。

論点 3 と論点 4 は、当初の起点であった論点 1 及び論点 2 とは別に、検討の過程で追加的に現れたものである。いずれも検討が必要な項目であるが、これらを論点 1 と同じ比重で扱うと対策の焦点が不明瞭になるおそれがあるため、本書では、論点 1 を相応に整理したうえで、論点 2 から論点 4 については論点を示すにとどめる。

本書は金融機関とフィンテック事業者の双方に向けたものであることを追記しておく。第 4 章は双方に関わり、濃淡を決めるのは主に確認する側（金融機関）、範囲の限定とその維持を示すのは確認を受ける側（フィンテック事業者）である。第 5 章は、上記要請が金融機関に求める事項を接続関係において具体化するものであり、求める側は金融機関、対応する側はフィンテック事業者である。第 6 章と第 7 章は、主にフィンテック事業者の側の状況に基

づき記載している。ただし、第 7 章の第六（提出を受けた情報の管理）は確認する側の論点である。第 8 章は双方の論点である。

3．環境変化の捉え方

近時の脅威環境の変化の本質は特定のモデルが登場したことではなく、攻撃の手法を考案し、かつ実行するための費用が劇的に低下したことにある。この点は、検討を通じておおむね共通の理解となっている。

検討の過程で議論となったのは、脆弱性の管理をどの単位で行うかについてであった。上記要請⑥は、CVSS スコアが高くない脆弱性であっても実際の攻撃に利用されている実態を指摘し、自組織への影響と攻撃が成立する蓋然性を踏まえた評価を求めている。検討ではこの考え方をさらに進め、深刻度が中程度の脆弱性であっても、組み合わせれば攻撃が成立しうる、しかもそれは複数のシステムにまたがって起こり得るという指摘があった。システムを一つずつ見て個別にリスクを測る方法に限定していると、全体を見誤りかねない点に着目する必要性が認識された。

また、脆弱性の発見に要する費用が下がれば、公表を経ずに悪用される脆弱性も増加するため、パッチの適用に加え、多層防御と検知の仕組みを併せて設計する必要性も指摘された。

他方で、同じ技術は防御側でも活用できるため、近時の脅威変化は防御側にとって一方的な不利ではないことも指摘された。ただし継続して利用可能かどうかは別の課題であり、この点については第 9 章で述べる。

4．相手方との関係の区分

(1)既存の区分整理の活用

金融機関が接続・取引する相手方には、外部委託先、共同運営形態の運営主体、契約に基づく接続先、更に外部委託先からの再委託先や接続先からの連鎖接続先等（更にそれらの先の接続・取引する相手方も考えられる）がある。これらの相手方に求められる対応の水準も適用される規律も、この区分によって異なることが想定される。

この区分は、当協会が新たに立てるものではなく、全国銀行協会「オープン API のあり方に関する検討会報告書」（2017 年 7 月 13 日）などにおいて、接続先を一律に外部委託先として扱わない整理は、既に示されている。上記報告書ではその 1.2 節において、API の接続先企業等が銀行の銀行代理業者または外部委託先に該当しない場合について記載したものである旨を明らかにし、脚注において、これらに該当する場合には同報告書に優先して銀行法にもとづく各種の利用者保護規定が適用されることに留意すべき旨を付している。ただし、当該記述は同報告書自身の適用範囲を画定するものであって、接続先が外部委託先に当たらないと定義するものではなく、当協会としても規範的な定義としては引用しないこととする。

上記要請も、共同運営形態やクラウド事業者により提供される IT システムについて、責任分担の明確化（②）、パッチ適用時の SLA・SLO の確認（⑤）、停止の判断（⑧）に言及し

ており、特に共同運営形態については、この整理を出発点とすることが適当であると考えられる。

(2) 関係とリスクに応じた対応水準の設定

同じ相手方であっても、関係の深さによってリスクの性質は異なる。更新系の API を用い債権債務の消込まで含む相手方と、参照系の API のみで連携する API 接続先とでは、扱う情報も障害時の影響も異なっている。すべてを最も重い外部委託先の水準で扱えば、対応が形式的なものになる可能性があり、リスクベースでの対応水準の設定が求められると考えられる。

リスクベースでの対応水準を検討する際には、単純に事業者の規模や業種業態、契約の形態だけを基準に置くことは適当でない。連携先にサイバー攻撃を受ける経路がある場合、近時の攻撃者の能力拡大に鑑みれば、相手方の規模が小さいので不十分な対応でも許容されるという整理は成り立ちにくいと考えられる。

対応水準の検討時には、どのような接続をしているか、その接続がどの範囲に限定されているかの確認が重要である。情報へのアクセス範囲や相手方が採りうる行為の範囲が限定され、その限定が維持されていることを保証できるのであれば、求める水準を軽くする理由がある。逆に上記の限定が困難な場合は、相手方の規模の大小にかかわらず相応の水準が求められる。

対応水準を決める要素としては、次の三つが考えられる。

第一要素：相手方での機密性の高い情報の保持の有無

第二要素：相手方の業務の停止や遅延による、自社の業務の停止や遅延への影響の有無

第三要素：相手方との接続を通じた、自社のシステムへの侵害可能性の有無

なお、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」（2024 年 10 月 4 日）も、サードパーティについて、重要な情報の取扱いの有無や組織内システムへの接続状況などを踏まえたリスク評価を求めており、第三の要素は、上記要請⑦が挙げるネットワーク分離の実施や内部侵入後の横展開への対策と同種のものである。

上記要素の適用を例で示すと、次のようになる。

・参照系の API のみで接続し、預かる情報が限られる関係では、第一と第二の要素が小さいと考えられる。相手方での保持情報の範囲や、相手方業務の停止・遅延が自社業務に与える影響が限定されていることを示せれば、確認の水準を軽くする理由がある。また、銀行の入出金明細等の参照系 API であれば、第三の要素の観点からも、侵害の経路になりにくい構造となっている。評価の一例として詳述すると、電子決済等代行業者（電代業者）は、銀行が外部向けに設けた API の窓口にサーバー間で接続するだけで、銀行の内部ネットワークに入るわけではない。接続を通じて行えるのも、あらかじめ定められた範囲の残高・明細の照会に限られる。仮に電代業者のシステムが侵害され、トークンが盗まれたとしても、攻撃者に

与えられるのはこの限られた照会の権限だけであり、銀行内部のシステムに入り込んで横展開する足がかりにはならない。加えて、上記の全国銀行協会での検討以降、金融情報システムセンター（FISC）による「API 接続チェックリスト」などの業界共通の枠組みのもとで、接続元の限定やクライアント認証、不正を検知したときのトークン無効化といった対策が整えられてきた。このため、参照系 API による接続は、上記要請⑦が求めるネットワーク分離が接続の仕組みとしてすでに備わった形態であり、内部侵入後の横展開のリスクは小さいと評価できる。

・なお、更新系の API を用い、債権債務の消込まで含む関係では、第一から第三のいずれの要素も大きくなりうるため、相応の水準対応が必要になると考えられる。

・情報連携先がクラウドサービス等であり、そこからの接続元（金融機関）へのアクセスが想定されない関係（第三の要素の考慮が不要の場合）では、主に第一の要素、すなわち機密性の高い情報を当該クラウドサービス等で扱うか否かによって、対応の水準を決めることが考えられる。なお、業務の停止や遅延につながりうる情報連携先とは、確認の方法も評価の観点も異なりうる（第二の要素の観点）。

外部委託先と接続先の間で対応の水準に典型的に差が生じうる点は次のとおりである。ただしこれは典型的な違いを示すものであり、個々の関係における水準は上記の要素によって精査が必要であり、両者ともに契約によりその水準が明確化されていることが望ましい。

金融機関が 相手方に求める事項	外部委託先	契約に基づく接続先 （連携第三者）
可用性の水準	業務の内容により求めることがありうる。ただし合理的な範囲にとどめる	一般に高い水準を求める必要はなく、限定的で足りる
パッチ適用等の対応期限	契約上の定めに基づき求める	自社基準を定めて金融機関に提示し、対応期限の根拠を明らかにする
能動的な停止	事前の合意に基づき対応	影響の受領と左記に伴う金融機関の自社顧客への対応
システム構成等の確認の対象範囲	委託した業務に係る範囲	当該接続に係る業務のシステムを基本とする

表 1：金融機関が相手方に求める事項の水準に関する比較
（典型例であり個別には調整が必要）

なお、上記の整理に際して個別の検討を進めた場合、外部委託先については既存の蓄積があるためそちらが先行して、接続先（連携第三者）も含めた事実上の標準となるおそれがある。外部委託先と接続先への対応を一体として整理し、その中で段階を設けていくことが適切であると考えられる。

(3) 機関間での役割重複や連鎖的関係

同一の事業者が、ある相手方との関係では委託先であり、別の相手方との関係では接続先である、という例は少なくない。例えばリスクへの対応状況について、立場ごとに別の確認様

式で相手方から確認を求められれば、当該事業者は一部が重複する内容を個別に作成することになる。金融機関においては自社用の確認様式と、委託先・接続先用の確認様式との対応関係を示しておく必要がある（第 8 章）。

また、連鎖的関係は相手方のさらに先へ、再委託先や連鎖接続先といった形態で続くことも生じている。連鎖的関係をどこまで追跡して把握すべきかについては現状では目安がなく、上記の対応水準検討時の三要素などに鑑み、重要度に応じて追跡する深度を変えていくほかないと考えられる。なお、連鎖的関係を把握する場合にも、どの範囲についてどの程度の情報を求めるのかを、あらかじめ示しておくことが望ましい。

5．上記要請の中で接続関係等において具体化を要する事項

(1) 脆弱性対応の優先順位や対応期限

上記要請⑥が求める脆弱性対応は、金融機関の自組織のシステムを念頭に置いている。これを接続関係にある事業者との間で用いるには、いくつかの具体化を要することとなる。

例えば金融機関が自社で定めた脆弱性への対応期限をそのまま相手方に求めることが適切とは限らない。相手方のシステム構成や態勢によって対応できる速度は異なるため、期限内の対応を求める場合には、それが契約上の定めによるのか事実上の要請によるのかを明らかにしておくことが望ましい。

また、期限内に対応できない場合の扱いも、あらかじめ定めておく必要がある。代替措置を求める、生じ得るリスクを受容する、機能の一時的な停止を要請するなどが考えられる。誰が判断するのかも含めて事前に決めておかなければ、実際に脆弱性対応の必要性が生じたときに対応が困難となる。攻撃の状況が変われば対応期限の考え方も変わる可能性があるため、再評価を行う場合の契機も定めておく必要がある。

(2) 維持保守契約における役割分担

上記要請⑤は、パッチ適用作業が維持保守契約に含まれること及び役割分担が明確であることの確認を求め、複数の金融機関において同時に大量の適用作業が発生する場合を想定したリソース確保の確認も求めている。

接続関係において具体化を要するのは、契約の類型による違いを踏まえた実施主体の明確化である。請負によるもの、準委任によるもの、サービスの利用に含まれるものとでは、どの主体が何を実施するのかが異なってくる。脆弱性情報の収集、通知、評価、適用のそれぞれについて、実施する主体を定めておくことが求められる。

あわせて、技術的な評価と業務上の判断の分界を明らかにしておく必要がある。技術的な評価は相手方（例えば外部委託先）が主導しうるが、業務影響の判断、適用の可否、優先順位付け、リスクの受容などは、委託元の責任として残ることとなる。

また、複数の相手方が関与する場合には、全体の影響評価を単一の相手方に委ねることはできないため、どの主体が全体の調整や評価を実施するのかを定めておくことが望ましい。

(3) 可用性とパッチ適用速度

上記要請⑤は、パッチ適用対象の一層の絞り込みや、パッチ適用の遅延に係るリスク受容等のプロセスを整備することも求めている。

このプロセスは、相手方の類型に応じて具体化することが考えられる。パッチの適用時には、作業のためにサービスを止める必要が生じる場合がある。委託関係においては、金融機関側がサービスの停止を許容しないために、パッチの適用そのものが後回しになる例が現に生じていた。当該サービスの停止を認めない状況下でのパッチ適用の早期化は両立し得ない。

接続先（連携第三者）に対しては、一般に高い可用性を求める必要がないと考えられ、求める水準は限定的で足りると考えられる。また、外部委託先に対しては、業務の内容によって可用性を求めることがありうるが、その場合も合理的な範囲にとどめ、パッチ適用のための停止と両立する形で定めることが望ましい（上記表１）。

いずれの場合でも、求める可用性の水準と求める対応の速さは、両者を併せて定める必要がある。パッチ適用時のサービス停止の判断も、相互の理解に基づき、共同でリスクを判定して行うことが重要である。具体的には、予防的なサービス停止等の基準作り、顧客や取引先へのスタンス表明などを、共同で行うことが考えられる。

この点については、金融機関の側においても、どこまでの停止を許容するのかもあらかじめ相手方に対して明らかにしておくことが求められる。パッチの適用を急ぐことと、サービスを止めないこととは同時には満たせずトレードオフがある以上、どちらをどこまで優先するのかを示さなければ、相手方も判断や行動ができない。個社ごとに最適を求めるだけでは解が得られない場面もあり、その場合は社会全体としての費用を勘案し、全体としての最適を探っていくことも求められると考えられる。

(4) 能動的なサービス停止時の相手方への連絡

上記要請⑧は、優先的に対応すべきサービス・IT システムを能動的に停止させざるを得ない場合について、経営トップがあらかじめ選択肢として検討しておくべきであるとし、判断基準及び手順を自組織内で明確にしておくことを求めている。

接続関係においては、これに加えて自社（例：接続先）の業務の停止が相手方（例：金融機関）の業務継続に影響を与える場合には、連絡の順序と方法を定めておく必要がある。共同運営形態においては、業務の停止や復旧の判断が事業者側で行われる場合もある。いずれの場合においても、関与の可否と方法、接続の切断と再開の基準を、あらかじめ整理しておくことが求められる。

(5) 求める報告の粒度と頻度

上記要請④及び⑤は、パッチ適用体制と評価体制のリソース確保を求めている。他方で、接続先等が求められる報告の業務そのものが、パッチ適用などの対応に充てるべき時間を圧迫するという問題がある。

金融機関によっては、脆弱性の残存の有無、対応した脆弱性とその対応日、重大な脆弱性を検知した際の共有を求める例がある。定期の更新報告と、判明した都度の即時共有とでも接続先等の負荷が大きく異なり、同じ報告要請の中にも、報告内容の粒度や報告頻度において、複数の水準が混在している。

金融機関は接続先等における報告の負荷を加味して報告の期限を設定するとともに、個別の報告を要しない範囲をあらかじめ定めておき、接続先等にも共有しておくことが考えられる。報告に時間を要することで本来の対応に支障が生じる場合、報告を求める側が結果としてリスクを増大させうることには留意が必用である。

6．接続先・委託先の側でこそ実施可能な対応

要請への対応の際には、金融機関が接続先等に一定の対応水準を求めるという一方向の構図で語られやすい。しかし実際には、レガシーシステムの制約や既存の管理体制のもとでは短期では着手できないことでも、比較的新しいシステム構成を採用している接続先等の事業者であれば実施可能な場合がある。実施可能な主体において先んじて措置を行うことが、全体としての底上げにもつながると考えられる。

例として、防御における生成 AI の活用（脆弱性診断の継続化、ログの分析、対応時の調査の支援）、パッチ適用及びテストの自動化、構成情報を機械で照合できる形で把握し、影響範囲を即座に判定すること、などが挙げられる。

認証方式の更新も同様であり、フィッシング耐性のある方式への移行は、顧客接点を多く持つ事業者において先行しうる。なお、上記移行の途上における代替手段の確保と、その周知の方法は併せて整理しておく必要がある。

納品物の検査もこの類型に属すると考えられる。開発を委託した場合、納品されたコードに不正な処理が含まれていないかを正確に検査することは、委託した側に要員と十分な知見がなければ困難である。とりわけ資産を管理する形態のサービスでは、不正の実行と同時に資産の棄損や喪失が生じうるため、契約による事後の救済が働きにくく、事前に精緻な検査を行うことの意味が他の形態より大きいと考えられる。中立的な視点を持つ AI を用いて検査する方法は、委託した側の負担を抑えつつ、この経路を塞ぐ手段になりうる。

7．確認・報告・対応に係る負担の適正化とリスク管理の実効性確保

上記要請では言及されていないが、接続先等における対応能力等は適切に考慮する必要がある。確認・報告の実効性を確保するには、相手方の対応力や把握可能な情報を踏まえ、求める内容・水準・対象範囲等を適切に設定する必要がある。あわせて、責任の所在、契約範囲を超える対応の条件、受領情報の管理等を明確化することで、確認・報告が本来必要な対応を妨げず、全体としてのリスク低減につながる運用とすることが重要である

(1) 確認・報告業務の重複

脆弱性や新たなシステム構成等の確認は、その作業自体に相応の時間が必要となる。同種の質問が相手方ごとに繰り返される場合、担当者が一人ないし二人という事業者では、確認作業に加えて回答の作成もその他の業務を圧迫する。５.(5)で述べたとおり、求められる報告についても同様である。

(2) 把握困難な事項の存在

第二に、確認を求められた側でも把握が困難な事項が存在する。利用中のサービスに後から追加された AI 機能が、主体的に選択したものではないにもかかわらず確認の対象となる場合がある。利用するサービスが数十に及ぶ場合、どのサービスにいつ確認対象となる機能が追加されたかを追跡すること自体が負担となる。利用するサービスの裏側で用いられている AI のモデルや処理やデータの所在地が判別できない場合もある。委託・接続の連鎖の先についても、どこまで追跡して把握すべきかの目安もない状況である。

これらについては、機能追加の際の事前の通知、既定で有効となる場合の取扱い、基盤となる AI モデルの提供者及び処理の所在地の開示などについて、事前に確認事項として整理することが考えられる。その際、所在地等が開示されないことをもって直ちに不可とはせず、代替となる措置の有無等により判断することも考えられる。委託や接続の連鎖がある場合には、重要度に応じて追跡して把握する深度を変えていくことも必要である。事業者の側においても、利用するサービスとその所在地を即座に示せる体制を持つことは、確認作業の円滑化に有効である。

(3) 事業者の態勢に応じた要求水準設定と責任の明確化

第三に、接続先等の態勢の規模に対して、求められる対応の水準が釣り合わない場合も想定される。情報システム担当部門を置いていない段階の事業者に対し、大規模組織を前提とした確認が要請されれば、現在の要員では対応不可能と受け止められ、着手そのものが見送られる可能性もある。まずは対応範囲を提示する際、提示した事項を満たさないことが直ちに不備を意味するものではないことを、あわせて示すことが望ましい。他方で、小規模事業者の実態に配慮する場合にも、委託元は事態が生じた際の責任の所在を明確にし、自らの顧客への説明責任を果たすことが求められるため、接続先等の事業規模に応じた対応水準の設定と責任の明確化の、両立を図ることが重要である。

(4) 非金融業務関連領域の取扱

接続先等が金融機能以外のサービスを併せて営む場合、確認等の対象範囲をどの様に確定するのかが課題となる。電子決済等代行業者を例にとれば、①当該金融業務そのものを担うシステム、②情報処理等用の直接的には当該金融業務に関連しないシステム、③情報連携先という分類が可能である。金融機関からの確認等の対象範囲は①に絞ることを基本とし、②③を含める場合には求める側がその理由を示す、という整理が考えられる。ただし、ネットワーク上の接点があれば、契約上はスコープの範囲外であっても、サイバーセキュリティの観点では確認等の対象と考えるべきケースは生じうる。対象範囲の限定と、契約上のスコープをまたいだ侵害の防止の担保は、対にして整理しなければならない。

(5) 契約範囲を超えた緊急時対応

極めて切迫した緊急時には、契約に定めた役務の範囲を超える対応を求められる場合がある。追加の対応を求めるのであれば、対応のための期間及び費用についても、適切なタイミングで協議されるべきである。

(6) 受領した情報の適切な管理

報告等により提出を受けた対応状況やシステム構成に関する情報は、個々の脆弱性が軽微な場合でも、近時の攻撃能力の増大に鑑みると、組み合わされることで極めて機微な、攻撃が可能な経路が見出され得る情報ともなる場合がある。当該情報の管理については、情報を受領する側においても一定の取扱いを定めるなど、従来以上に厳重な情報の管理が求められる。

8．確認業務の効率化

(1) 何を先に整理するか

金融機関と接続先等との確認に関するやり取りで生じる工数を全体として削減するためには、既存の確認項目との対応関係の整理と、新たな確認項目の標準化とを、他に先立って行う必要がある。実施済みの確認結果をそのまま他所にも提供できれば、二重での作成を避けられ、情報の正確性の向上も期待できる。あわせて、同一の事業者が委託先と接続先の双方の立場を兼ねる場合も少なくないため、両者の様式の対応関係も示すことが望ましい（4.(3)参照）。

(2) 用語や確認事項の定義

確認項目として「AI の学習に利用するか」といった、正確な定義などが確認されないまま回答が行われている場合も多い。利用の有無のみを問い、どのモデルに、どのような形で情報を渡しているかまでは問わない例も見受けられる。定義が一致しないままで回答を共通化しても、比較用としては意味をなさないため、推論のみか学習に用いるのか、生の情報を渡すか、処理の所在地はどこかなど、質問項目の立て方と併せて定義を揃えることが重要である。なお、業界ごとにガイドラインが策定されていることから、業界によって、例えば「学習」の定義が異なり、同一サービス内の類似機能であっても、その機能が準拠すべき規律が異なる可能性があることに留意が必要である。

(3) 回答の機械可読形式化

確認への回答の作成は、既に相当程度が AI によって処理されていると思われるが、重要事項でもあるため最終的な内容の確認は人手に頼らざるを得ない。表計算ソフトの形式は機械での処理に向いておらず、AI にそのまま渡せる形式の方が扱いやすい。

また、年に一度の更新時などに毎回形式を変更することもなるべく避け、同じ形式を継続して用いることができれば、リスクが判明したときに双方が速やかに対応が可能となる、共通認識の土台ともできる。

(4) 第三者確認・保証・認証の活用と適用可能性

第三者による確認により、その結果の信頼性を確保するための手段には幾つかの段階があり、一般的には自己申告を除くと、合意された手続（いわゆる AUP: Agreed Upon Procedures）による確認、保証、認証などが挙げられる。

合意された手続による確認は、第三者が依頼者と合意して実施した確認手続とその結果を報告するものであり、結論として適切性などについての意見を述べるものではないが、確認作業を効率化する手段としても用いられる場合が多い（下記(5)参照）。認証は、定められた要求事項への適合性について判断を示すものであるが、対象事項の範囲外についての確認や判断は行われない。保証は一般的には監査法人等による適切性が担保された意見が得られ、対象事項の範囲も柔軟に設定可能であるが、事業規模の小さな接続先等における実施の際には費用面が課題となる場合がある。

また、第三者を活用する確認の実務上は「確認の実施時点」「確認対象範囲」「例外事項の有無」に留意する必要があり、確認内容に照らして上記が適切に設定されているかを事前に精査する必要がある。確認結果の報告書の要約だけに判断を依拠すると、上記三点が適切に設定されていないことを見落とす可能性があるため、注意が必要である。

(5) 標準化の必要性

複数の相手方から確認を受ける事業者の対応水準は、最も厳しい相手方の要請の水準に収斂しやすい傾向がある。個々の要請がそれぞれ合理的であっても、それらを合算した負担が膨大となり、対応の実施を妨げることがあるため、確認内容の標準化は重要である。なお、当該標準化は対応水準を下げる目的のために行うのではなく、同じ水準をより少ない手数で確認可能とするために実施するものである。

標準化は、確認結果の共有と組み合わせることで、よりその効果が拡大することが期待できる。項目が標準化された上で、一度確認した結果を複数の金融機関に共有することができれば、確認に対応する側の手数も減らすことができ、全体としての効率化にも繋がる。この効果は合意された手続において特に顕著である。また、標準化された項目があれば、追加で確認を要する部分のみへの対応を個別に調整することも行いやすい。

なお、確認項目の標準化については、関係する業界の枠組みにおいても議論が進められているため、当協会としてはそれらの議論との重複を避け、議論の範囲を確認しながら進めることとする。その際、確認を受ける側の状況を踏まえて、設計の際に適切に項目に反映することが重要である。2017 年の全国銀行協会のオープン API に関する検討会での整理が、その後の確認項目の土台を構成した経緯があり、その際も金融機関の側で検討を進めつつ、接続先等の事業者側からも意見を伝える形での検討が行われた。確認項目の標準化についても、同様の進め方が考えられる。

9．引き続き検討を要する事項

以下は、本書では論点の所在を示すにとどめ、次回以降の版において整理する。

(1) 論点 3　委託先・接続先が利用する AI と、そのデータの所在

委託先や接続先が、自らのサービスの中で、又は利用する SaaS 等を通じて、どのような AI を、どのような形で用いているか、当該 AI の処理機構や処理対象データがどこに置かれているかに関する論点である。これらを把握しなければ、委託元からは把握されていない AI の利用を許容しているということになる。

整理の方向としては、利用するサービスとその提供者、処理機構や処理対象データの所在地、格納するデータの種類等を一覧にして提示可能な形とすることが考えられる。確認を受ける側があらかじめ用意しておく形の方が、双方の手数が少なくなると考えられる。

なお、本論点は確認を行う側の関心が高まっている一方、金融機関の間でも論点として認識をしているところとそうではないところの差が見受けられる。当協会としては、本論点の重要性を指摘しておきたい。

(2) 論点 4　AI エージェントによるアクセスの認証・認可と、AI エージェントを用いた取引

顧客側のエージェントが関与する金銭取引が現実化しつつあり、利用者本人及びエージェントの確認が論点となる。更に事業者側がエージェントを提供する場合には、利用者側エージェントとの間で意図しない相互作用も生じることが考えられる。自然人の権限をそのままエージェントに付与すれば過剰な権限となるため、権限範囲の限定や、代理人としての資格情報の有効期間の短縮といった設計が必要となる。

国際的な規格・枠組みは現在形成途上にあり、多数の提案や取組みが並行して存在・稼働している。これらのすべてを追うことは適切ではないので、参照するものを限定して示すこととし、参照先の特定は、当該分野に知見のある者の意見を聴いたうえで行うこととする。新たな決済手段の普及に伴い、この論点は取引の監視の問題とも重なる部分がある。

(3) 論点 1 及び論点 2 のうち、なお整理を要する事項

防御側での AI の利用　第 6 章で接続先等における防御への AI 活用に言及しているが、当該活用の継続可能性についても検討が必要である。AI 機能の供給の停止・機能内容の変更や、地域による活用の制限、権限を与えて動かす場合の統制機構、不正な処理や脆弱性の検出精度の確保などが課題として考えられる。上記要請⑧が求めるサービス停止への備えの項目として、AI 機能の供給が停止した場合を含めることも検討に値する。

どのモデルの利用が許容されるのかも論点となりうる。脆弱性を検証する場面では、能力の高いクローズドモデルはアクセス等の管理が厳格であり、攻撃者が実際に用いるモデルとは異なる可能性がある。そのため、攻撃側が用いると想定されるオープンモデルで検証を行うことには一定の合理性がある、との見方も示されている。他方、モデルの選択は、その供給の安定性、情報の所在、統制の及ぶ範囲などが絡む複合的な問題であり、特定のモデルの提供者に依存しないことが、結果として適切なリスク管理になる場合もあり得る。モデルの選定にあたっての留意点や、上記の懸念を抑制可能な条件を整理しておくことが必要である。

対応力の差と、運用の共同化　費用と人員の負担の増加により、各種の対応が可能な事業者とそうでない事業者の差が広がりうると考えられる。また、非対面のチャネルで事業を継続すること自体も難しくなる状況が、金融機関にも接続先等にも生じる可能性がある。上記要請②は、既存の IT 部門のリソースを短期的に大幅に拡充することは現実的ではないとの認識に立っており、それらを踏まえると確認項目の標準化にとどまらず、運用の共同化まで含めて検討する必要があると考えられる。共同化の際に対象とする機能、運営の主体、参加条件をなどを具体的に整理することが、次の課題となる。

経営とガバナンス　サイバー対応の費用は経営戦略に関わるとの認識は広がりつつあるが、IT ガバナンス及びレジリエンスの観点からの議論はなお乏しい状況である。自組織にどのようなシステムがあるかを洗い出せない機関も現実には存在し、現場の判断を経営層が検証できないという課題も指摘されている。AI の活用により対応の負担を下げられることは、必要な要員を減らして良いことを意味しているものではない。上記要請④が人的リソースの追加を求めていることも踏まえ、経営資源の配分の見直しを含めて検討すべきである。

また、直近は現在の投資配分を維持する場合であっても、今後の脆弱性対応においては、突発的な深夜対応、計画の変更、脆弱性情報過多など、従業員のストレスの強度が高まることに配慮し、有事における交代制の導入など、チーム編成や働き方の見直しを行うことも重要である。

10. 今後の進め方

本書は最初の論点を示すものであり、次回以降の版において、論点 1 を中心に整理を進めていくこととする。あわせて、委託先と接続先を一体として整理し、その中に求められる対応の水準について、段階を設ける作業を行うこととする。論点 2 から論点 4 は、その後に展開する。

当協会は、確認事項の一覧、共通して用いうる回答の様式、既存の確認項目との対応表を順次整備する予定である。第一弾として示す確認事項は 20 項目程度を想定し、既存の規範に根拠があること、相手方の規模を問わず実施しうること、実施の有無を証跡により確認できること、を選定の基準とする。

当協会は、民間の実務者の側からプラクティスを提案していく立場にあり、制度や枠組みが定まるのを待つのではなく、実務で現に利用可能な内容を公開された形で先行して示していきたい。金融機関と事業者の双方が参加する場であることを活かし、何が実施可能で、何が過大な負担になるかについての知見も形式知化していきたい。

なお、金融機関から確認を受ける側にとって、最低限の求められる対応が明らかであることは、金融機関との取引を始められる前提でもある。情報の管理や AI の利用に際して対応すべき事項が不明確な場合は、取引そのものが難しくなると考えられる。同時に、接続先等の事業者の側に向けた整理も併せて進めることとする。

上記要請が「現時点における状況を前提とするものであり、今後の AI を巡る動向の変化を踏まえ、必要な対策を不断かつ機動的に見直し、適切に講じていくことが重要である」としているとおり、本書も継続して改訂する。

（注）本書は一般的な実務上の整理であり、個別の取引・事案に関する法的助言ではない。9 月 11 日の会合における発言は、必ずしも各参加者の所属組織を代表するものではない。