FINTECH ASSOCIATION OF JAPAN

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

説明資料　―　要請の具体化と論点の全体像

一般社団法人Fintech協会

(C) 2026 Fintech Association of Japan

FINTECH ASSOCIATION OF JAPAN

接続等の関係における「要請」対応を具体化

金融庁・日本銀行のセキュリティ対策「要請」は金融機関の自組織を念頭に置いており、接続先等との関係で実施する際には、さらに具体化が必要な部分がある。本書は、その部分を論点ごとに区分し、論点1を中心に整理する。

1　背景
フロンティアAIで攻撃の費用が低下。脆弱性とパッチが短期間に集中して発見・提供される可能性

→

2　「要請」
金融庁・日本銀行が2026年5月22日に短期的な対応を要請（9項目）。金融機関の自組織が念頭

→

3　具体化を要する部分
オープンAPI等で接続する事業者との間で実施する際には、さらに具体化が必要な部分がある

→

4　本書の整理
論点を四つに区分し、論点1を中心に整理。論点2〜4は論点の所在を示す

論点	内容	要請での扱い	本書での扱い
論点1 脆弱性・修正プログラムの集中	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	短期的な対応として直接に扱っている	中心的に整理 第4〜8章
論点2 AIの攻撃への悪用	フロンティアAIが攻撃に悪用されることへの対応（公表前の悪用、攻撃の高速化）	応急的措置と位置づけ。中長期は自動化等へ	論点を示す 第3章・第9章(3)
論点3 委託先・接続先のAIとデータ所在	委託先・接続先が利用するAIと、そのデータの所在	明示的な言及なし	論点を示す 第7・8章(一部)・第9章(1)
論点4 AIエージェントの認証・取引	AIエージェントによるアクセスの認証・認可と、エージェントを用いた取引	言及なし	論点を示す 第9章(2)

(C) 2026 Fintech Association of Japan

文書構成の全体マップ

1章　はじめに

2章　範囲と論点
- 論点1　脆弱性・パッチの集中
- 論点2　AIの攻撃への悪用
- 論点3　AI・データの所在
- 論点4　AIエージェントの扱い

3章　環境変化の捉え方
- 脆弱性を全体で捉える
- 防御側でのAI利用の可能性

4章　相手方との関係の区分（「相手方」の捉え方）
- (1) 既存の区分整理の活用
- (2) 関係とリスクに応じた対応水準の設定
  - 水準を決める三要素（情報の機微度、自社事業への影響、侵害可能性）
  - 外部委託先と接続先の対応水準の比較
- (3) 機関間での役割重複や連鎖的関係
  （委託先かつ接続先、再委託先や連鎖接続先の存在）

5章　具体化を要する事項
- (1) 脆弱性対応等の対応期限
- (2) 役割分担
- (3) 可用性とパッチ適用速度（過度な可用性追求→パッチ適用が困難に）
- (4) サービス停止時の相手方への連絡
- (5) 報告の粒度と頻度（過度な報告要求→対応時間を削ぐ）

6章　接続先・委託先で実施可能な対応
- 防御へのAI利用
- 納品検査でのAI利用

7章　負担の適正化
- (1) 確認・報告依頼の重複
- (2) 把握困難事項（海外製AIの所在等）
- (3) 相手方の態勢、状況の考慮
- (4) 非金融システムの扱い
- (5) 契約範囲を超えた対応（切迫した緊急時など）
- (6) 情報管理（攻撃高度化→軽微な脆弱性情報も管理高度化要）

8章　確認業務効率化
- (1) 確認項目の整理（優先事項として対応→10章）
- (2) 確認対象の定義の問題
- (3) 回答の機械可読形式化
- (4) 第三者確認等の活用
- (5) 標準化

9章　要検討事項
- (1) 論点3　AI・データの所在
- (2) 論点4　AIエージェントの扱い
- (3) 論点1、2の要整理事項
  - 防御側AIの「継続」的な活用
  - 共同運用の課題
  - 経営とガバナンス

10章　今後の進め方
- 論点1を先行して検討
- 確認事項の一覧、対応表を準備中

凡例
橙赤の文字：補足・理由の注記
青の太字：優先して対応する事項
中央の4〜8章：論点1の中心

(C) 2026 Fintech Association of Japan

FINTECH ASSOCIATION OF JAPAN

ポイント①対応水準を決める三要素

金融機関が接続先等に求める対応水準は、規模や契約形態ではなく、三つの要素（機密性の高い情報の保持、業務停止の影響、侵害可能性）の大きさで決める。要素が小さければ水準を軽くし、大きければ相応の水準を求める。

具体例 接続の形態ごとに、三要素の大きさと対応水準を示す	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、自社の業務への影響の有無	第三要素 相手方との接続を通じた自社システムへの侵害可能性の有無 要請⑦（ネットワーク分離・横展開対策）と同種	対応水準 三要素の大きさに応じて、相手方に求める対応の度合い
参照系APIのみで接続し、預かる情報が限られる	小	小	小	軽くする理由あり
更新系APIで、債権債務の消込まで含む	大	大	大	相応の水準が必要
情報連携先がクラウド等で、金融機関側へのアクセスが想定されない	（主たる判断要素）	個別に判断	不要	第一要素で主に決める

参照系APIのみの接続では、侵害されてトークンが盗まれても与えられるのは限られた照会の権限だけで、内部システムへの足がかりになりにくい（電子決済等代行業者の例）。

(C) 2026 Fintech Association of Japan

ポイント②委託先と接続先の違い

外部委託先と接続先では、金融機関が求める事項の水準に差異が生じ得る。ここに示すのは典型的な違いであり、個々の関係の水準は三つの要素で精査する。

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、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

典型的な違いにすぎない

個々の関係の水準は、三つの要素で精査する

契約で水準を明確化

委託先・接続先のどちらも、契約により水準が明確化されていることが望ましい

一体で整理し、段階を設ける

委託先の既存の蓄積が、接続先を含む事実上の標準になるおそれがあるため

(C) 2026 Fintech Association of Japan

ポイント③「要請」対応として具体化すべき内容

金融庁・日本銀行の「要請」の各項目は、金融機関の自組織を念頭に置いている。接続先等との関係で実施する際に具体化が必要な事項を、要請の項目ごとに五つに整理した。

要請（金融機関の自組織が念頭）	接続関係で具体化を要する事項
要請⑥ 脆弱性の評価と対応	(1) 優先順位と対応期限 自組織の脆弱性対応期限をそのまま相手方に求めることが適切と限らない。契約か事実上の要請かを明示しつつ、期限内に対応できない場合の扱い・判断者・再評価の契機を決める
要請⑤ 維持保守契約・役割分担の確認	(2) 維持保守契約の役割分担 相手方との関係で、請負・準委任・サービス利用で実施主体が異なる。技術的な評価と業務上の判断の分界、複数の相手方がいる場合の全体調整者を定める
要請⑤ パッチ適用対象の絞込み、遅延のリスク受容	(3) 可用性とパッチ適用速度 相手方のシステム停止を認めないとパッチ適用が後回しになる。可用性の水準と対応の速さを併せて定め、停止の判断についてはは共同でリスクを判定する
要請⑧ 能動的な停止の判断基準・手順（自組織内）	(4) 停止時の相手方への連絡 自組織の停止が相手方の業務継続に影響する場合の連絡の順序と方法、接続の切断・再開の基準をあらかじめ整理する
要請④⑤ パッチ適用・評価体制のリソース確保	(5) 報告の粒度と頻度 報告の負荷が対応の時間を圧迫しうる。報告負荷を加味し、個別報告が不要な範囲を事前に定めて共有する

(C) 2026 Fintech Association of Japan

ポイント④負担の適正化で、確認の実効性を担保

金融機関が接続先等に求める確認・報告については、本来必要な対応を妨げず、かつ全体としてのリスク低減に繋がる運用にする。そのため、内容・水準・対象範囲を適切に設定し、責任の所在、契約範囲を超える対応の条件、受領情報の管理を明確化する。

1	確認・報告の重複	同種の質問が相手ごとに繰り返され、少人数の事業者では他業務を圧迫する
2	把握困難な事項	後付けのAI機能、基盤モデルや処理データの所在地、連鎖等で接続していく先の情報は把握が困難な場合がある。事前の確認事項として整理する
3	態勢に応じた水準と責任	規模や態勢に合わない要求は着手の見送りも招く。水準設定と責任の明確化を両立させる
4	非金融業務関連領域	対象は金融業務のシステムが基本。確認対象範囲の限定と、契約上のスコープをまたいだ侵害防止は対で整理する
5	契約範囲を超えた緊急対応	金融機関側が追加の対応を求める場合、期間と費用を適切なタイミングで協議する
6	受領した情報の管理	確認する側が受領した情報は、全体で組み合わせると攻撃経路になり得る情報でもあるため、従来以上に厳重に管理する

(C) 2026 Fintech Association of Japan

FINTECH ASSOCIATION OF JAPAN

ポイント⑤確認業務の効率化

金融機関が接続先等に求める確認業務の負担を減らすため、確認項目の整理から始め、定義の統一、機械可読な形式、第三者確認の活用を経て、標準化と結果の共有に進める。

1	確認項目の整理 優先事項として対応→第10章	既存の確認項目との対応関係の整理と、新たな項目の標準化を先行して実施。
2	用語や確認事項の定義	「AIの学習に利用するか」等が定義を確認されずに回答される例が多い。推論のみか学習か、生の情報を渡すか、処理の所在地はどこかなど用語や定義を揃える
3	回答の機械可読形式化	回答作成は既にAIが相当程度処理。表計算形式は機械処理に不向きで、AIが理解しやすい形式が望ましい。毎回形式を変えず共通認識の土台にする
4	第三者確認・保証・認証	合意された手続、保証、認証など段階がある。確認の実施時点・対象範囲・例外事項の三点に留意する（次頁）
5	標準化と結果の共有	複数の相手方から確認を受けると最も厳しい要請に収斂しやすい。標準化と共有で負荷を低減するが、対応水準を下げることが目的ではない

(C) 2026 Fintech Association of Japan

ポイント⑥第三者による確認の類型

接続先等から金融機関への報告時に、第三者確認が有益な場合がある。確認には、合意された手続（AUP）、認証、保証などの類型がある。それぞれ提示可能な内容と適用限界が異なるため、確認の実施時点・対象範囲・例外事項を事前に精査する。

合意された手続（AUP）

何を示すか

第三者が依頼者と合意した確認手続と、その結果を報告する

限界・留意

適切性などの意見は述べない

ほか

確認作業を効率化する手段として用いられることが多い。標準化と結果共有の効果が特に顕著

認証

何を示すか

定められた要求事項への適合性について判断を示す

限界・留意

対象事項の範囲外は確認・判断されない

保証

何を示すか

監査法人等による、適切性が担保された意見が得られる

限界・留意

事業規模の小さな接続先等では費用が課題になりうる

ほか

対象事項の範囲を柔軟に設定できる

実務で事前に精査する三点

- 確認の実施時点
- 確認対象範囲
- 例外事項の有無

確認結果の報告書の要約だけで判断すると、この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

(C) 2026 Fintech Association of Japan

今後：確認事項の一覧等を公表予定

今回は論点を示す第一弾として本書を示した。次版以降で論点1を中心に整理し、確認事項の一覧、共通の回答様式、既存項目との対応表を整備して公表する予定。論点2〜4はその後に展開する。

今回（第一弾） 論点を示す	次版以降 論点1を中心に整理	その後 論点2〜4を展開
• 四つの論点（論点1〜4）に区分して提示 • 論点1の考え方と具体化事項を整理	論点1　脆弱性・修正プログラムの集中 • 委託先と接続先を一体で整理し、水準に段階を設ける	論点2　AIの攻撃への悪用 論点3　委託先・接続先のAIとデータ所在 論点4　AIエージェントの認証・取引

次版以降に整備

第一弾の確認事項（20項目程度）

確認事項の一覧、共通の回答様式、既存項目との対応表を整備

確認事項の選定基準（補足）　既存の規範に根拠がある／相手方の規模を問わず実施できる／実施の有無を証跡で確認できる

当協会の姿勢　民間の実務者の側から、制度や枠組みが定まるのを待たずにプラクティスを公開して先行して提示する。実施可能な対応や過大な負担に関する知見も形式知化する。事業者側に向けた整理も併せて進め、本書も継続して改訂する

(C) 2026 Fintech Association of Japan