2026 年●月●日

●● 御中

●●銀行

「フロンティア AI」による脅威変化を踏まえたサイバーセキュリティ管理態勢の確認・確保について

近年、いわゆる「フロンティア AI」の発展に伴い、サイバー攻撃に用いられる脆弱性の発見および攻撃コード生成の速度が向上し、従来は発見が困難であった脆弱性が短期間に大量に発見され得ることや、脆弱性の発見から攻撃に至るまでの期間が大幅に短縮され得ることが指摘されています。

こうした中、金融機関のサイバーセキュリティ対策を実効的なものとするためには金融機関自身の取組みに加え、金融機関にサービスを提供する関係事業者における対応も重要となります。

つきましては、金融機関にサービスを提供する関連事業者におかれましても、フロンティア AI による脅威変化を踏まえた IT・サイバーセキュリティ管理態勢の速やかな確認・確保をお願い申しあげます。

１．金融機関にサービスを提供する関係事業者等に求められる短期的対応例
（大量の脆弱性への対応）

以下に掲げる短期的な対応例を参考に、リスク特性や IT・サイバーセキュリティ管理態勢を踏まえ、必要な対応の主体的な検討・実施をお願い申しあげます。

① フロンティア AI による脅威変化を踏まえ、脆弱性対応や重要サービスの継続確保を経営課題として扱う
② 優先的に対応すべきサービス／IT システムを特定する
③ 特定した資産について、未適用パッチ、サポート切れ製品、不要な外部公開サービス、不要なアカウント・権限等の技術的負債を確認・是正する
④ パッチ適用や影響調査に必要な人的リソース、外部委託先の支援体制、緊急時の対応要員を確認する
⑤ 自社が利用するベンダー、保守事業者、委託先・再委託先等との維持保守契約、役割分担、緊急時の連絡・対応体制を確認する
⑥ 重要サービスへの影響度、脆弱性の深刻度、悪用可能性等を踏まえ、パッチ適用の優先順位を判断する
⑦ パッチ適用が困難な場合に備え、アクセス制御、監視強化、ウェブアプリケーション防御機能（WAF: Web Application Firewall）等による防御、機能停止、ネットワーク分離等の代替的なリスク低減策を検討する

⑧ 優先サービス／IT システムの停止、機能制限、外部接続遮断等に備え、事業継続計画（BCP）、緊急時対応体制、サービス停止判断プロセス、復旧手順を確認する

⑨ 金融機関、保守ベンダー、委託先、再委託先、業界団体、セキュリティ関係機関等との連絡・情報共有体制を確認する

２．金融機関への連絡について

金融機関に提供するサービスに影響を及ぼし得る重大な脆弱性、サイバー攻撃被害、攻撃兆候、サービス停止リスク等を認識した場合において、金融機関向けサービスへの影響が合理的に懸念されるときは、その影響範囲が確定していない段階であっても、関係する金融機関へ速やかにご連絡くださいますようお願い申しあげます。

３．ご参考

・金融庁『「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」に係る要請について』
URL：https://www.fsa.go.jp/news/r7/sonota/20260522-5/20260522.html

・日本銀行『「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」に係る要請について』
URL：https://www.boj.or.jp/finsys/release/frel260522a.htm

以　上