金総政第 3245 号
金企市第 498 号
金監督第 1384 号
令和８年５月 22 日

関係事業者代表者　殿

金融庁総合政策局長　堀本　善雄
金融庁企画市場局長　井上　俊剛
金融庁監督局長　石田　晋也
金融庁総括審議官　柳瀬　護
日本銀行理事　神山　一成

「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

AI 技術が急速に進展する中、サイバー攻撃に AI が活用されることで、攻撃のスピード・規模が劇的に加速・拡大する等、サイバーセキュリティを巡る脅威が高まっている。特に、いわゆる「フロンティア AI」により、脆弱性の発見・修正等のサイバーセキュリティ性能の急速な向上が見込まれることを踏まえ、これに対応する取組が必要不可欠である。

こうした中、金融庁は４月 24 日に「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」を開催した。その議論を踏まえ、金融業界と IT 事業者、政府・日本銀行等が AI 技術の進展による脅威について共通の理解を持ち、対応を検討していくため、実務者レベルの作業部会（第１回）を５月 14 日に実施した。

当該作業部会において、短期的に脆弱性や修正プログラム（パッチ）が集中的に発見・提供される可能性を踏まえ、「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ついて」（別添）を取りまとめた。

各金融機関等に対して、経営トップを含めた経営層の直接関与の下、別添に記載されている短期的な対応に取り組むよう要請する。なお、本要請は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。

金融庁も、５月 18 日に国家サイバー統括室が公表した、政府全体の対応パッ

ケージである「AI 性能の高度化を踏まえたサイバーセキュリティ対策の強化について～Project YATA-Shield～」[1]に沿って、金融分野の特性を踏まえつつ対応を進めていく。

[1] https://www.cyber.go.jp/pdf/press/20260518_AI_CS_Package.pdf

別添

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ついて

1. 背景

近年、いわゆる「フロンティア AI」の発展に伴い、高度なサイバー攻撃の増加が懸念されている。フロンティア AI は脆弱性の発見や高度な攻撃コードの生成に優れており、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に加え、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る。さらに、スキルの低い攻撃者がフロンティア AI を悪用することで、高度なサイバー攻撃が増加することが懸念されている。

こうした中、脆弱性が大量に発見され、これに伴い修正プログラム（パッチ）が短期間に多数提供される可能性がある。このため、金融機関等においては、こうした事態に備え、資産管理、脆弱性管理、パッチ適用、監視対応、レジリエンス等について、迅速かつ適切に対応できる態勢が整備されているかを至急点検し、必要な強化を図ることが求められる。経営トップは、リーダーシップを発揮してこれらの対応を主導するとともに、必要なリソース配分を含めた意思決定を行う必要がある。CIO、CISO をはじめとする経営層は、各種対応の実施にあたり直接関与する必要がある。

これらの脅威は、自組織で開発したシステムに限らず、オープンソースソフトウェアを含むサードパーティのソフトウェアやサービスにおいても、同様に及び得ることに留意する必要がある。

一方で、英国 AISI（AI 安全性評価機関）の報告書[2]によれば、現時点ではフロンティア AI は、十分に防御された IT システムに対しては、攻撃を達成できるとは言えないと報告されている。これを踏まえれば、金融庁の「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」に基づく基本的な対策をより迅速かつ着実に実行していくことが引き続き重要である。

2. 金融機関等に求められる短期的対応（大量の脆弱性への対応）

金融機関等においては、短期的には以下に掲げる対応を速やかに講じる必要が

[2] AI Security Institute (AISI), Our evaluation of Claude Mythos Preview's cyber capabilities, https://www.aisi.gov.uk/blog/our-evaluation-of-claude-mythos-previews-cyber-capabilities

ある[3]。ただし、これらはあくまでも応急的措置であり、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。また、大量の脆弱性への対応は、本文書に掲げる対応に限定されるものではなく、各金融機関等において、自組織のリスク特性やIT・サイバーセキュリティ管理態勢を踏まえ、必要な対応を主体的に検討・実施することが求められる。

加えて、これらの対応はIT・サイバーセキュリティ担当部署のみで完結するものではなく、経営トップがフロンティアAIに対する正確な理解と危機意識を持ち、必要なリソース（予算・人員）を確保することが不可欠である。

① フロンティアAIへの対応を経営課題として扱う

フロンティアAIがもたらす脅威の変化は、IT・サイバーセキュリティ部門にとどまらない課題であるため、経営トップは全社的な経営課題として扱う必要がある。各業務所管部門、リスク管理部門、IT・サイバーセキュリティ部門、財務部門等関係部門が横断的に連携して対応できるよう、経営トップとしてのコミットメントが不可欠である。

また、経営トップのリーダーシップの下で、CIO、CISOをはじめとする経営層が直接関与し、対応方針の策定、対応状況の把握及び課題への対処等を継続的に実施することが不可欠である。

② 優先的に対応すべきサービス／ITシステムを特定する

大量の脆弱性発見により、パッチ適用作業の対応負荷が著しく増大することが想定されるが、既存のIT部門のリソースを短期的に大幅拡充することは現実的ではない。このため、優先的に対応すべきサービス／ITシステムを特定し、リソースを重点的に配分する等、リスクベースで対応する必要がある。

特に、インターネットバンキング等の重要業務を支える外部公開ITシステムについては、最優先で対応することが考えられる。なお、当該システムが共同運営形態で提供される場合には、あらかじめ利用側と提供側双方において十分な認識の共有を図るとともに、責任分担を明確化しておく必要がある。

---

[3] 金融機関等においては、AIモデル開発企業の活動状況も踏まえ、概ね1ヶ月程度を目途に、対応を進めることが期待される。

③ 特定した資産の技術負債を解消しておく

②で特定した優先的に対応すべきサービス／IT システムにおいて、そのソフトウェア構成及びネットワーク構成等を再確認し、脆弱性発見時にパッチ適用対象を即時に特定できる状態を確保しておく必要がある。加えて、不要なネットワークポートの閉塞、特権 ID の削除、未対応のパッチの適用等により技術負債を極力解消し、防御力を高めるとともに、迅速なパッチ適用が可能な状態にしておくことが重要である。特にサポートが終了している製品についてはメーカーによるパッチ提供が行われないことから、速やかにサポート対象バージョンへ更新する必要がある。

④ パッチ適用に係る人的リソースを追加する

今後増加が見込まれる脆弱性への対応力を向上させるため、優先的に対応すべきサービス／IT システムに関連する実施計画を見直すとともに、他の IT システム部門からの支援等により、人的リソースの追加を検討すべきである。あわせて、実際のパッチ適用作業を担うベンダーにおいても、脆弱性対応の増加に対して十分なリソースが確保されることを事前に確認することが重要である。

さらに、脆弱性の優先度判断に係る評価体制についても、大量の脆弱性発見に対応できるようリソースを確保する必要がある。これをベンダーと共同で実施している場合には、ベンダー側においても必要なリソースが確保されていることを確認することが求められる。

⑤ ベンダーとの維持保守契約の内容を確認する

本邦金融機関等においては、自組織が所管する IT システムの維持保守をベンダーに委託しているケースが多く見られる。こうした状況を踏まえ、パッチ適用作業が現行の維持保守契約に含まれていること及び役割分担が明確であることを確認する必要がある。また、緊急にパッチ適用作業が必要な場合に、夜間・休日等も含めて適時に対応可能な契約内容となっていることを確認することが重要である。さらに、複数金融機関等において大量の脆弱性へのパッチ適用作業が同時に発生する場合であっても、契約で定められたサービス水準に関する合意（SLA）及び目標（SLO）[4]を遵守したパッチ適用作業が実施できるよう、ベンダー側におけるリソース確保状況を確認する必要がある。併せて、脆弱性対応がベンダー側に集中し、ベンダー側のリソースがひっ迫することも想定し、金融機関

[4] SLA（サービスレベルアグリーメント）は、金融機関等とベンダーとのサービス品質保証に関する契約であり、SLO（サービスレベルオブジェクト）は、SLA を達成するための組織内部の目標を指す。

等においては、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しておくことが求められる。

共同運営形態やクラウド事業者により提供される IT システムについては、パッチ適用に関する SLA 及び SLO の内容、適用対象及び適用状況等について金融機関等に適切に報告される契約内容となっていることを確認する必要がある。

⑥ パッチ適用プロセスをリスクベースにする

②で特定した優先的に対応すべきサービス／IT システムにおいて大量に脆弱性が発見された場合、すべての脆弱性への対応は困難となることが想定される。多くの金融機関等では共通脆弱性評価指標（CVSS）[5]スコアや攻撃コードの有無等に基づきパッチ適用の優先順位を決定していると考えられるが、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があり、こうした傾向は、フロンティア AI により、今後さらに加速することも想定される。また、脆弱性発見・パッチ提供の後、直ちに攻撃コードが出現する可能性もある。このため、金融機関等においては、発見された脆弱性が自組織のサービス／IT システムに及ぼし得る影響を適切に把握するとともに、攻撃が成立する蓋然性も踏まえた評価を行うことが重要である。その上で、リスクベースで優先順位付けを行い、よりリスクの高い脆弱性から迅速かつ着実に対応すべきである。

また、パッチ適用作業に係る事前のテストについては、テスト不足に起因するシステム障害リスクと、パッチ未適用に伴うサイバー攻撃のリスクを総合的に勘案し、テスト実施内容の合理的な縮小等の対応についても検討することが望ましい。

⑦ パッチ適用以外の対策も強化する

②で特定した優先的に対応すべきサービス／IT システムにおいて、パッチ適用そのものが困難である場合や、パッチ適用に要する期間の短縮が困難である場合には、早期に効果が期待できるクラウド型のウェブアプリケーション防御機能（WAF：Web Application Firewall）等を用いた仮想パッチ[6]の適用やボット対

---

[5] CVSS は、FIRST（Forum of Incident Response and Security Teams）が公開している脆弱性評価の枠組みであり、脆弱性そのものの技術的な深刻度を評価する基本評価基準（Base Metrics）に加え、攻撃コードの出現状況や対象のシステム環境において想定される脅威に基づき、0.0～10.0 までのスコアで脆弱性の深刻度を評価する指標である。
政府情報システムにおける 脆弱性診断導入ガイドライン：デジタル社会推進実践ガイドブック　DS-221

[6] ソフトウェアベンダーが提供する本来のセキュリティパッチをサーバー等に早急に適用することが難しい場合の暫定的なソリューションである。個々の脆弱性に対応した侵入防御ルール（仮想パッチ）を備えた機器をネットワーク経路上に設置し、当該脆弱性を悪用する攻撃通信をブロックするものである。これが設置されたネットワーク経路からの攻撃しか防御できないことや、攻撃コードの亜種が出た際に仮想パッチが追い付かないリスクがあること等、恒久的な対応ではないことに留意すべきである。

策の導入等、多層防御の強化を図る必要がある。また、ネットワーク分離の実施、特権 ID への多要素認証の導入、端末における不正検知・対応機能（EDR：Endpoint Detection and Response）等による防御能力の強化や内部侵入後の横展開への対策等についても可能な限り推進することが重要である。

なお、これらの対策はあくまでもリスク低減策であることから、パッチが適用できないことによる残存リスクを評価した上で、パッチ適用に要する期間を踏まえた適切なリスク受容手続を講じる必要がある。

⑧ 優先サービス／IT システムの停止に備える

各種対策を徹底してもサイバー攻撃を防御できない可能性を前提に、サイバー攻撃により IT システムが停止する場合を想定するとともに、②で特定した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も経営トップはあらかじめ選択肢として検討しておくべきである。

こうした事態に備えて、事業継続計画（BCP）の有効性や、顧客等ステークホルダへの対応手順の十分性、緊急時の連絡体制等を点検するとともに、サイバー攻撃のリスクが高まった場合の能動的なサービス／IT システム停止の判断基準及び手順についても自組織内で明確にしておくことが重要である。この点は、共同運営形態やクラウド事業者により提供される IT システムについても同様である。

また、⑥のとおりテスト実施内容を縮小してパッチ適用に要する期間を短縮する等した場合に、テスト不足等による IT システム障害の発生頻度が増加し得ることについても経営トップは認識しておくべきである。

更には、自組織が開発し維持保守する IT システムに限らず、サードパーティが提供するソフトウェアやサービスにおいて深刻な脆弱性が発見された場合、当該ソフトウェアの利用停止やサービス停止が生じ得ることにも備えておくべきである。

⑨ 外部との連携を維持・強化する

フロンティア AI に関する情報は短期間に多数公開されることから、自組織のみでの網羅的な把握等は困難と想定される。このため、金融 ISAC や各業界団体・コミュニティ、当局等からの情報に積極的にアクセスし、必要な情報の収集に努めるべきである。

また、フロンティア AI への対応について、自組織の取組を金融 ISAC 等の共助

のためのコミュニティで積極的に共有し、金融分野全体の強靭性の向上に努めることが望ましい。