金融分野の取組状況

- 金融庁では、 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」及びその作業部会を5月14日に開催し、金融業界とIT業界、政府・日本銀行等の官民の連携強化を図っている。
- また、5月22日には「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」に係る要請文を発出。その後、要請文に関する補助文書等を複数回にわたり発出したほか、要請事項に対する事業者の対応状況の実態把握を実施。

○要請文の概要

① フロンティアAIへの対応を経営課題として扱う

- 経営トップは、フロンティアAIへの対応を**IT部門にとどまらない全社的な経営課題**として扱い、**関係部門が横断的に連携**して対応できるようにする。
- **経営トップのリーダーシップの下、CIO、CISOをはじめとする経営層が直接関与**する。

② 優先的に対応すべきサービス／ITシステムを特定する

- **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。(例：インターネットバンキング)
- 当該システムが共同運営形態で提供される場合、**利用側・提供側双方での十分な認識共有、責任分担の明確化が必要**である。

③ 特定した資産の技術負債を解消しておく

- 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**を確保する。
- 特権ID削除や未対応パッチの適用等により**技術負債を極力解消**することで、迅速なパッチ適用が可能な状態を確保する。特にサポートが終了している製品は、**サポート対象のバージョンへ更新**する。

④ パッチ適用に係る人的リソースを追加する

- 金融機関等やベンダーにおいてパッチ適用に係る**人的リソース追加を検討**する。
- 脆弱性の優先度判断に係る評価体制についても、上記同様に人的リソースを確保する。

⑤ ベンダーとの維持保守契約の内容を確認する

- ①**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**、②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。
- ベンダー側で必要なリソース確保状況を確認しつつ、リソースがひっ迫すること等も想定し、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。

⑥ パッチ適用プロセスをリスクベースにする

- 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**影響と攻撃が成立する蓋然性も踏まえた評価**に基づき、**よりリスクの高い脆弱性から対応**する。
- パッチ適用作業に係る事前のテストについて、想定される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も検討する。

⑦ パッチ適用以外の対策も強化する

- パッチ適用そのものが困難である場合等は、仮想パッチの適用やボット対策の導入等により、**多層防御の強化**を図る。
- ネットワーク分離の実施、特権IDへの多要素認証の導入等による**防御能力の強化や内部侵入後の横展開への対策**等を講じる。
- **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。

⑧ 優先サービス／ITシステムの停止に備える

- **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。**システムを能動的に停止させざるを得ない場合もあらかじめ選択肢として検討**する。
- **BCPの有効性や顧客等への対応手順、緊急時の連絡体制等を点検**する。
- **能動的なサービス／ITシステム停止の判断基準及び手順を明確**にしておく。
- サードパーティが提供するソフトウェアやサービスの停止に備える。

⑨ 外部との連携を維持・強化する

- 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、必要な情報収集をする。
- 自組織での取組を金融ISAC等の共助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。