NEWS RELEASE

2026 年 6 月 5 日
株式会社ブロードバンドセキュリティ

「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」（金融庁及び日本銀行から公表）に対応する支援サービスを提供開始

～金融機関等に求められる緊急対応と中長期強化を包括支援～

情報セキュリティコンサルティングなどセキュリティに特化したサービスを提供する株式会社ブロードバンドセキュリティ（本社：東京都新宿区、代表取締役社長：滝澤 貴志、以下 BBSec）は、金融庁および日本銀行が公表した「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」に係る通達に対し、金融機関等に求められる短期的なセキュリティ対策から継続的な態勢強化までを支援するサービスパッケージの提供を開始します。

【提供開始の背景】
近年、生成 AI をはじめとする AI 技術の急速な進展により、サイバー攻撃の高度化・高速化が進んでいます。AI の進化は企業活動の高度化や生産性向上に寄与する一方、サイバー攻撃の手法やスピードにも変化をもたらしており、企業には AI 時代を前提としたセキュリティ態勢の整備が求められています。
特にフロンティア AI は、脆弱性の発見や高度な攻撃コードの生成に活用される可能性があります。これにより、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たり、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たりすることが懸念されています。

こうした状況を踏まえ、金融庁および日本銀行は 2026 年 5 月 22 日、金融機関等に対し、経営トップを含む経営層の直接関与の下、資産管理、脆弱性管理、パッチ適用、監視対応、レジリエンスなどについて、迅速かつ適切に対応できる態勢を至急点検し、必要な強化を図るよう要請しました。

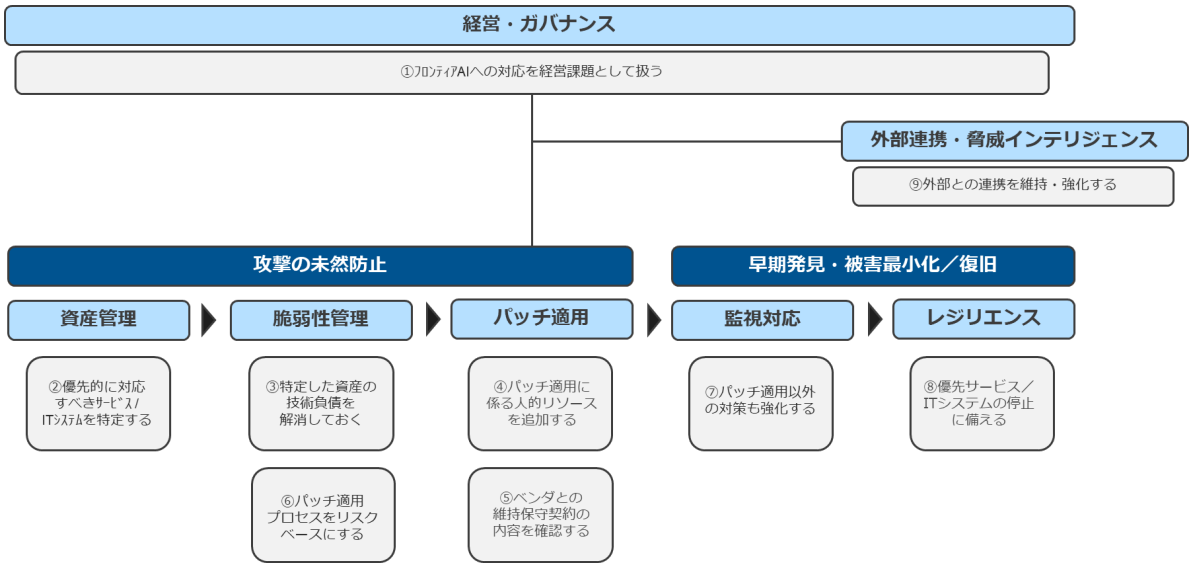

図 1：金融庁要請を実現するためのセキュリティ運用モデル

金融機関等においては、インターネットバンキングをはじめとする重要サービスの継続性確保、顧客影響の最小化、外部委託先や共同運営先を含めた対応態勢の整備、規制・ガイドラインを踏まえた説明責任が求められます。

BBSec は、本要請の公表を受け、金融機関等が短期的な対応を速やかに具体化できるよう、既存の各種セキュリティサービスを今回の要請事項に沿って体系化し、脆弱性診断、アタックサーフェス調査、セキュリティ監視、CSIRT 構築・運用支援、インシデント対応、金融庁ガイドライン対応支援などを組み合わせた支援パッケージとして提供を開始します。

運用モデル	要求事項	要約	BBSec対応ソリューション	（参考） 金融庁ガイドライン分類
経営・ガバナンス	**① フロンティアAIへの対応を経営課題として扱う**	・IT課題ではなく経営課題 ・経営トップ主導が不可欠 ・CIO/CISO等の直接関与が必要	**・セキュリティアセスメント ・アドバイザリサービス ・CISO支援サービス**	サイバーセキュリティ管理態勢の構築
資産管理	**② 優先的に対応すべきサービス／ITシステムを特定する**	・優先システムを特定しリスクベースで対応 ・特に外部公開系は最優先とする ・共同運営の場合は責任分担を明確化する	**・IT資産管理 ・ASM（Attack Surface Management）**	サイバーセキュリティリスクの特定
脆弱性管理	**③ 特定した資産の技術負債を解消しておく**	・パッチ適用対象を即時特定できる状態を確保 ・構成の可視化と技術負債の解消 ・EOL製品の更新	**・脆弱性管理 ・脆弱性診断・設定診断 ・ペネトレーションテスト**	サイバーセキュリティリスクの特定
脆弱性管理	**⑥ パッチ適用プロセスをリスクベースにする**	・影響度と攻撃成立可能性を踏まえ優先順位付け ・高リスクから迅速に対応 ・テスト内容の合理化も検討	**・脆弱性管理 ・アドバイザリサービス**	サイバーセキュリティリスクの特定
パッチ適用	**④ パッチ適用に係る人的リソースを追加する**	・優先システムの対応体制を見直す ・内部およびベンダ双方で人的リソースを確保・強化 ・大量の脆弱性に対応できる体制を整備	**・要員支援 ・アドバイザリサービス**	サイバーセキュリティ管理態勢の構築
パッチ適用	**⑤ ベンダとの維持保守契約の内容を確認する**	・役割分担や緊急対応可否を確認 ・SLA/SLOやリソース確保状況を確認 ・遅延リスク受容プロセスを整備	**・金融庁ガイドライン準拠対応支援 ・アドバイザリーサービス**	サードパーティ管理
監視対応	**⑦ パッチ適用以外の対策も強化する**	・WAF等の仮想パッチによる防御 ・MFA、EDR、ネットワーク分離による侵入・横展開対策 ・多層防御の強化 ・外部ドメイン脆弱性の監視	**・MSSサービス（WAF・IPS・UTM・EDR） ・G-MDR（XDR） ・マイクロセグメンテーション ・特権ID保護・MFA ・外部スクリプトURL監視サービス**	サイバー攻撃の防御
レジリエンス	**⑧ 優先サービス／ITシステムの停止に備える**	・IT停止を前提とした備え・BCP、顧客対応、連絡体制整備 ・停止判断基準の整備	**・IT-BCP策定支援 ・コンテンジェンシープラン策定支援**	サイバーインシデント対応及び復旧
外部連携・ 脅威インテリジェンス	**⑨ 外部との連携を維持・強化する**	・金融ISAC等から情報収集・脆弱性情報、攻撃情報を継続的に取得・業界全体で脅威情報を共有	**・アドバイザリサービス**	金融庁と関係機関の連携強化

図 2：金融庁要請に対する BBSec 対応ソリューション一覧

【BBSec が支援する主な領域】

- **経営・ガバナンス**
  フロンティア AI による脅威変化を IT 部門のみの課題ではなく経営課題として捉え、経営層の意思決定、リスク把握、対応方針の策定を支援します。
- **資産管理**
  優先的に対応すべきサービスや IT システムを特定するため、外部公開資産や IT 資産の可視化を支援します。特に、インターネットバンキングなど重要業務を支える外部公開システムについて、リスクベースで優先順位を付けた対応を可能にします。
- **脆弱性管理**
  資産情報と脆弱性情報を突き合わせ、影響度や攻撃成立可能性を踏まえた優先順位付けを支援します。脆弱性の大量発見やパッチ提供の集中を想定し、継続的かつ統制の取れた脆弱性管理態勢の構築を支援します。
- **パッチ適用体制の整備**
  大量の脆弱性発見に伴うパッチ適用負荷の増大を想定し、人的リソースの確保、ベンダーとの役割分担、維持保守契約の確認、SLA・SLO を踏まえた運用体制の整備を支援します。
- **監視対応・多層防御**
  パッチ適用が困難な場合や、攻撃の早期検知・被害最小化が必要となる場合に備え、WAF、IPS、UTM、EDR、XDR などを活用した多層防御とセキュリティ監視を支援します。
- **レジリエンス強化**
  サイバー攻撃による重要サービスや IT システムの停止を想定し、事業継続、復旧、顧客対応、連絡体制などの整備を支援します。
- **外部連携・脅威インテリジェンス**
  金融 ISAC など外部コミュニティとの連携や、脆弱性情報・攻撃情報の継続的な収集・活用を支援し、組織単独では把握しにくい脅威変化への対応力向上に貢献します。

【今後の展望】

フロンティア AI 時代においては、脆弱性の発見や攻撃のスピードが高まることを前提に、「攻撃の未然防止」と「侵入・被害発生を前提とした早期発見・被害最小化／復旧」の両面から態勢を整備することが重要です。BBSec は、セキュリティに特化した専門知見と幅広いサービスを組み合わせ、お客様のサイバーレジリエンス向上に貢献してまいります。

【BBSec について】

BBSec は、2000 年創業のトータルセキュリティ・サービスプロバイダーです。現状の可視化や診断から事故発生時の対応、24 時間/365 日体制での運用まで、フルラインアップのサービスを提供しています。高い技術力と豊富な経験、幅広い情報収集力を生かし、「サプライチェーンを狙った攻撃」「社会インフラを狙った攻撃」「AI 時代のセキュリティ」を解決すべき社会課題ととらえ、より多くのお客様を悪意ある攻撃者から守ることで、「便利で安全なネットワーク社会を創造する」というビジョンを実現します。

【本リリースに関するお問い合わせ】
株式会社ブロードバンドセキュリティ 経営企画部
TEL：03-5338-7430　E-mail：press@bbsec.co.jp

【本サービスに関するお問い合わせ】
株式会社ブロードバンドセキュリティ　営業本部
TEL：03-5338-7425　E-mail：sales@bbsec.co.jp