報道関係者各位

PRESS RELEASE

2026 年 5 月 28 日

株式会社サイバーセキュリティクラウド

サイバーセキュリティクラウド、フロンティア AI 時代の脆弱性管理・多層防御支援方針を表明

クラウド型 WAF による仮想パッチを軸に、急増する脆弱性対応を支援

グローバルセキュリティメーカーの株式会社サイバーセキュリティクラウド（本社：東京都品川区、代表取締役社長 兼 CEO：小池 敏弘、以下「当社」）は、2026 年 5 月 22 日に金融庁および日本銀行より公表された「『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』に係る要請について」（※1）を受け、当該要請が示す構造的課題は金融機関に限らず、全業界の事業者にも共通するとの認識のもと、当社およびグループ会社が提供する脆弱性管理サービス、技術者リソース、WAF（Web Application Firewall）製品群により、業界を問わずお客様の短期的対応を全面的に支援することを表明いたします。

■金融庁・日本銀行による要請の概要

金融庁および日本銀行は、高度な能力を持つ最先端の汎用 AI モデル、いわゆる「フロンティア AI」の発展に伴い、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、短期間に大量の脆弱性および修正プログラム（パッチ）が提供される可能性を指摘しています。これを受け、金融機関等に対し、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、経営トップを含めた経営層の直接関与のもと、迅速かつ適切に対応できる態勢の整備が要請されました。

要請に掲げられた短期的対応のうち、技術的な対応の中核となるのは以下の領域です。

- 優先的に対応すべきサービス／IT システムの特定と技術負債の解消（要請②・③）
- パッチ適用に係る人的リソースの追加（要請④）
- パッチ適用プロセスのリスクベース化（要請⑥）
- パッチ適用が困難な場合の仮想パッチ（WAF）等を用いた多層防御の強化（要請⑦）

■金融機関以外の業界にも共通する「同じ構造課題」

本要請は金融機関等を名宛人としていますが、その背景にある「フロンティア AI による脆弱性大量化・攻撃高速化」という事象は、業界を問わず Web システムを運用するすべての事業者に等しく到来しています。

事実、当社が日々お客様の環境で観測する攻撃トラフィックにおいても、業界を問わず新規脆弱性の悪用までのリードタイムは継続的に短縮しています。

金融庁・日本銀行の要請は、こうした「業界横断の構造課題」がいち早く金融セクターに対する規制当局メッセージとして言語化された先行事例と位置づけることができます。他の業界の事業者にとっても、本要請に示された 4 つの技術対応領域（資産特定・人的リソース・リスクベース運用・仮想パッチ）は、そのまま自社の短期対応計画のチェックリストとして有効です。

■仮想パッチ（WAF）による「時間を稼ぐ」現実解について

業界を問わず、短期的対応期間において現場で最大の制約となるのは、脆弱性の根本解消に要する時間です。資産棚卸、影響範囲調査、検証環境でのパッチ適用テスト、本番反映のためのメンテナンス調整などは、現場担当者の努力では短縮しきれない構造的なリードタイムを伴います。

一方で、AI の発展により、脆弱性公開から攻撃発生までの時間は短縮し続けています。根本対応を待つ間も、攻撃は継続的に到達します。

金融庁・日本銀行の要請⑦が仮想パッチを明記している背景には、この構造的なギャップを埋める現実的な手段が、現時点で仮想パッチによる多層防御以外に存在しないためです。クラウド型 WAF は、脆弱性の根本解消に先立って攻撃を遮断し、現場が落ち着いて根本対応を進めるための「時間を稼ぐ」役割を担います。

当社は、攻撃遮断くんおよび WafCharm により、オンプレミス・クラウド双方の環境に対し、仮想パッチ提供を可能とする体制を整えています。

■当社グループの対応方針

当社は、国内シェアNo.1（※2）のクラウド型WAF「攻撃遮断くん」をはじめとする豊富な実績を有するサイバーセキュリティ専業メーカーとして、本要請に示された対応領域を、業界・環境を問わずグループ製品・サービス群により全面的に支援いたします。

具体的には、「脆弱性管理」「人的リソースの追加」「仮想パッチ（WAF）」を、オンプレミス・クラウド双方の環境において一気通貫で提供できる体制を活かし、金融機関等はもとより、他の業界のお客様の短期的対応も広くご支援いたします。

■グループ製品・サービスによる対応カバレッジ

当社グループでは、金融庁・日本銀行の要請で示された「脆弱性管理」「人的リソースの確保」「仮想パッチによる多層防御」といった対応領域に対し、オンプレミス・クラウド双方の環境において、以下の製品・サービス群を提供しています。

- 脆弱性管理（要請②・③・⑥に相当）
  【オンプレミス環境】SIDfm（https://sid-fm.com/）
  【クラウド環境】CloudFastener（https://cloud-fastener.com/）
- 人的リソースの追加（要請④に相当）
  【オンプレミス環境】株式会社ジェネレーティブテクノロジー（https://gen-tech.co.jp/）
  【クラウド環境】CloudFastener（https://cloud-fastener.com/）
- 仮想パッチ／WAF（要請⑦に相当）
  【オンプレミス環境】攻撃遮断くん（https://www.shadan-kun.com/）
  【クラウド環境】WafCharm（https://www.wafcharm.com/jp/）

◇ 脆弱性管理ソリューション

脆弱性情報収集・管理ツール『SIDfm』

脆弱性情報収集・管理ツール『SIDfm』は、脆弱性対応の運用を効率化するツールです。OS・アプリケーション・ネットワーク製品の脆弱性情報を世界中から自動で収集・蓄積します。自

社に必要な情報だけをすぐに特定できる機能により対策すべき脆弱性とその対策内容が一目でわかります。さらに、脆弱性の対処進捗の記録・管理まで行うことができます。

フルマネージドセキュリティサービス『CloudFastener（クラウドファスナー）』

AWS、Azure、Google Cloud に対応したフルマネージドセキュリティサービス『CloudFastener』は、クラウドネイティブのセキュリティサービスを活用し、お客様のクラウド環境のリソースやアラートの包括的な管理と、セキュリティ専門家によるお客様に最適化された支援をご提供します。CloudFastener は脅威検知、脆弱性管理、データ保護、証跡監査、コンプライアンス対応などの支援を、お客様の環境構成、組織体制などに合わせた形で柔軟に提供し、ガバナンス・ポリシーの策定から復旧・修正対応にいたるまで、クラウドセキュリティの運用全体をワンストップで包括的に対応します。また、『CloudFastener』は高度な専門的知識と経験を持つチームがお客様をインソース型で支援するモデルを採用しています。そのため、専任のセキュリティチームが不在の企業や組織でも、クラウド環境のセキュリティ対策を迅速かつ効果的に進めることが可能となります。

◇ 人的リソース追加ソリューション

株式会社ジェネレーティブテクノロジー（当社グループ会社）

IT インフラ・セキュリティ領域の技術者派遣および受託開発を手掛けるグループ会社です。フロンティア AI 起因の脆弱性大量化局面において、お客様の既存運用体制を補完する技術者を機動的にアサインいたします。検証環境構築、パッチ適用作業、適用後の動作確認まで、現場運用に直結する人的支援をグループ横断で提供します。

◇ 仮想パッチ／WAF ソリューション

クラウド型 WAF『攻撃遮断くん』

クラウド型 WAF『攻撃遮断くん』は、情報漏えいやサービス停止などを引き起こす外部からのサイバー攻撃を検知・遮断し、Web サーバや Web サイトを保護するクラウド型の Web セキュリティサービスです。累計数兆件におよぶビッグデータの解析に基づいた独自の高精度検知ルールにより、多種多様なサイバー攻撃をリアルタイムで防ぎます。さらに、最新の脆弱性に対しても自社のセキュリティエンジニアが迅速に防御シグネチャを更新するほか、万が一誤検

知発生した場合でもテクニカルサポートが柔軟に対応し、安全かつ安定したサイト運営を支援します。

WAF 自動運用サービス『WafCharm（ワフチャーム）』

WAF 自動運用サービス『WafCharm』は、パブリッククラウドで提供される WAF を自動で運用できるサービスです。AWS、Azure、Google Cloud に対応しています。『WafCharm』の最大メリットは、煩雑かつ重要な WAF 運用業務を自動化できる点です。ルールの自動適用や IP ブロックリストの自動追加など豊富な機能により、WAF ルールの作成・更新作業や IP ブロックリストの追加などを手作業で行う必要がなく、『WafCharm』に任せることができます。

■ 経営層関与のもとでの現場支援

本要請では、CIO・CISO をはじめとする経営層の直接関与が不可欠であるとされていますが、これも金融機関に限った話ではありません。サイバーリスクが直接経営マターとなる時代において、現場担当者と経営層の連携は業界を問わず喫緊の課題です。

当社は、現場担当者の皆様が経営層への報告・稟議を円滑に進められるよう、経営層向け説明資料の提供、緊急時の優先対応、24 時間 365 日の日本語サポート体制等を通じて、現場対応と経営判断の双方を支援してまいります。

※1：「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

※2：出典：デロイト トーマツ ミック経済研究所「外部脅威対策ソリューション市場の現状と将来展望 2025 年度」

株式会社サイバーセキュリティクラウド（https://www.cscloud.co.jp）
所在地　：〒141-0021　東京都品川区上大崎 3-1-1 JR 東急目黒ビル 13 階
代表者　：代表取締役社長 兼 CEO 小池 敏弘
設　立　：2010 年 8 月

「世界中の人々が安心安全に使えるサイバー空間を創造する」をミッションに掲げ、世界有数のサイバー脅威インテリジェンスを駆使した Web アプリケーションのセキュリティサービスを軸に、脆弱性情報収集・管理ツールやクラウド環境のフルマネージドセキュリティサービスを提供している日本発のセキ

ュリティメーカーです。私たちはサイバーセキュリティにおけるグローバルカンパニーの 1 つとして、サイバーセキュリティに関する社会課題を解決し、社会への付加価値提供に貢献してまいります。

【報道関係者各位の問い合わせ先】
株式会社サイバーセキュリティクラウド 広報担当：井野部さりー
Mobile：080-4486-0029（いのべ　さりー）,E-Mail：pr@cscloud.co.jp