2026年11月27日

親会社GMOインターネットグループ株式会社とのガバナンス検証・高度化タスクフォースの共同設置に関するお知らせ

GMOインターネット株式会社
GMO インターネットグループ株式会社

当社および当社の親会社であるGMOインターネットグループ株式会社（証券コード：9449・東証プライム、以下、親会社といい、当社と親会社をあわせて、以下、両社といいます。）は、当社が提供する「お名前.com デスクトップクラウド」への第三者による不正アクセスおよびこれに起因する各種インシデント（あわせて以下、本件）ならびにこれらへの両社の対応について、お客様、お取引先様、株主・投資家の皆様をはじめ、関係する皆様に多大なるご心配とご迷惑をおかけしておりますことを、改めて深くお詫び申し上げます。

両社は、本件への対応を経営上の最重要課題と位置付け、被害を受けられたお客様への対応を最優先に取り組んでおります。また、システムの安全性確保に向けた措置を講じるとともに、さらなる再発防止策の実施および適切な情報開示に努めております。

また今般、本件の対応過程において課題があったことを認識しており、緊急時の対応に関する意思決定の客観性・専門性・実効性を一層高めるとともに、両社のガバナンスを検証し高度化する必要があると考えております。

つきましては、本日、親会社および当社の両取締役会においてそれぞれ審議・決議の上、両社共同で社外取締役を中心とし、外部専門家をアドバイザーに加えた「ガバナンス検証・高度化タスクフォース」（以下、本タスクフォース）を設置することといたしましたので、お知らせいたします。

１．　本タスクフォース設置の目的

両社は、これまで当社の代表取締役および担当役員を中心とする緊急対応体制の下、社外取締役および外部専門家からの助言・監督を受けながら、本件への対応を進めてまいりました。本件への対応は、被害を受けられたお客様への対応、技術的な安全性の確保、再発防止、対外的な説明など、多岐にわたっております。

こうした状況を踏まえ、従来の緊急対応体制をさらに強化し、親会社および当社の社外取締役による監督機能と、グループ内の経営資源および外部専門家の知見を組織的に活用するため、本タスクフォースを共同で設置することといたしました。あわせて、本タスクフォースは、本件への対応を踏まえて両社におけるガバナンスを検証し、その高度化を図るとともに、今後有事における緊急対応をより適切なものとすることを目的とします。

２．　本タスクフォースの構成

本タスクフォースは、以下の6名をメンバーとして構成いたします。

以下、敬称略

役職	構成	人数
リーダー	増田 要（親会社社外取締役監査等委員/弁護士）	1名
サブリーダー	鮎川 拓弥（当社社外取締役監査等委員/弁護士）	1名
メンバー	小武守 純子（親会社社外取締役監査等委員/公認会計士）	4名

	岩濱 みゆき（当社社外取締役監査等委員/公認会計士/公認情報システム監査人） 安田 昌史（親会社取締役 グループ副社長執行役員・CFO） 西山 裕之（親会社取締役 グループ副社長執行役員・COO）	
合計		6名

本タスクフォースは、親会社および当社の社外取締役であるリーダー、サブリーダーおよびメンバーの計4名を中心として運営し、その他のメンバーを含むグループ内の経営資源を活用しながら、下記3.記載の事項について審議いたします。

加えて、専門性と機動性を確保するため、本タスクフォースの外部アドバイザーとして、危機管理の専門家である白井邦芳氏、西村あさひ法律事務所・外国法共同事業および八雲法律事務所にご協力いただくほか、サイバーセキュリティに関する調査・検証および今後の態勢整備にあたり、当社グループ外の専門的な視点を取り入れるため、株式会社ラックから、本件に関する技術的な調査・検証、対応の妥当性の評価ならびにサイバーセキュリティ態勢の整備・高度化に向けた助言等の支援を受けることとします。なお、事実認定、対応方針の決定および施策の実施は、両社および本タスクフォースがそれぞれの権限と責任に基づき行います。　また、検証の充実を図るとともに、グループ全体の態勢高度化につなげるため、グループ会社からも関連する知見を有する役員以上の者をオブザーバーとして招聘し、より実効性のある提言に努めてまいります。

3.　本タスクフォースの役割および権限

本タスクフォースは、以下の事項について審議し、対応方針の策定および両社取締役会への提言・報告を行います。

（1）　本件についてのお客様対応を含む事後対応：被害状況の把握、被害を受けられたお客様への対応、補償方針その他必要な救済措置、ならびに攻撃者への対応方針（身代金の不払いおよび懸賞金の設置等）に関する事項

（2）　技術的な安全性の確保および再発防止：本件に関する外部専門家を中心とした技術面における検証の実施、システムの安全性確保、再発防止策の策定および実施状況の確認、ならびに本件の発生原因および発生に至る経緯の検証に関する事項

（3）　対外的な説明および情報開示：本件に関する対外公表、その他重要な情報発信の内容および実施方針に関する事項およびこれらを踏まえた株主・投資家をはじめとするステークホルダーとの今後の対話のあり方に関する事項

（4）　リスク・危機管理体制およびガバナンスの高度化：本件への対応を踏まえた平時および有事における社内・グループ内の報告体制、適切な情報共有・意思決定プロセス、リスク・危機管理体制および再発防止に向けた社内・グループ内における組織的な対応の整備・運用状況の検証に関する事項

（5）その他：グループにおける企業風土の検証、その他本タスクフォースが必要と認める事項

また、本タスクフォースは、必要に応じて両社および関係するグループ会社の役職員に対して説明または資料の提出を求めることができるものとします。

法令および社内規程上、親会社、当社その他関係するグループ会社の取締役会その他の機関による決定を要する事項については、本タスクフォースの審議を踏まえ、それぞれ権限を有する機関において決定いたします。

４．　代表取締役との役割分担

本タスクフォースの設置に伴い、本件に関する今後の重要な対応方針および対外的な説明については、本タスクフォースの審議を経る体制といたします。

緊急の技術的対応その他被害拡大の防止に必要な措置については、迅速な対応を優先し、事後速やかに本タスクフォースへ報告するものとします。

両社の代表取締役は、引き続きそれぞれの会社における通常の事業運営および経営戦略の推進を担うとともに、本タスクフォースによる審議および各社取締役会の決定を踏まえ、本件への対応に必要な業務執行を行います。

これにより、両社は、通常の事業運営の継続性を確保しつつ、本件に関する緊急対応について、本タスクフォースを通じて両社横断的な監督と専門的な判断を一層強化いたします。

５．　本タスクフォースの客観性および公正性の確保

本タスクフォースは、審議および判断の客観性・公正性を確保するため、適切な利益相反管理を行います。

（1）メンバー個人の利益相反への対応

メンバーについて、個別の審議事項に関する利益相反のおそれが認められる場合には、当該メンバーを当該事項の審議・判断から除外するなど、適切な措置を講じるものとします。

リーダーについて利益相反のおそれが認められる場合には、サブリーダーが当該事項の審議を主導するものとします。

また、サブリーダーについても利益相反のおそれが認められる場合には、利害関係のない他の社外取締役が審議を主導するなど、適切な対応を行います。

（2）親会社および当社との間の利益相反への対応

本タスクフォースは、親会社と当社との間で利害が対立する可能性のある事項についても、適切な利益相反管理を行います。

特に、補償費用の負担、グループ内の責任分担、資金支援その他両社の利害が異なり得る事項については、それぞれの会社の利益および少数株主の利益に適切に配慮し、公正な意思決定手続を確保いたします。

このような事項については、必要に応じて、利害関係のあるメンバーを当該事項の審議・判断から除外するとともに、各社の取締役会その他権限を有する機関において、それぞれ適切な手続により判断を行います。

（3）外部専門家の活用

上記の利益相反への対応に当たっては、必要に応じて、外部専門家による助言を受けるものとします。

これらの措置を通じて、本タスクフォースにおける判断の客観性および公正性を確保してまいります。

６．　外部専門家による技術的確認および助言

両社は、本件の技術的な原因、影響範囲、復旧措置および再発防止策の有効性について、外部のサイバーセキュリティ専門機関から技術的な確認・整理および専門的知見に基づく助言を受けるものとします。

本タスクフォースは、当該外部専門機関から技術的な確認内容および助言について報告を受け、これらを参考として、必要な改善措置の検討および対応を行います。

なお、本件に関する公表については、本タスクフォースの判断のもと、情報セキュリティ上の機密性および関係者の権利利益に配慮したうえで、内容および時期を判断するものとします。

７．　本タスクフォースの設置期間および活動状況の報告

本タスクフォースの設置期間は、当初90日間を予定しております。ただし、本件への対応状況その他必要な事情を踏まえ、両社の取締役会における必要な決議を経て、その期間を短縮・延長することがあります。

本タスクフォースは、活動状況および主要な対応事項の進捗について、定期的に両社の取締役会に報告いたします。

今後もグループ全体のセキュリティ管理体制、リスク・危機管理体制および経営ガバナンスの一層の強化・高度化に努めてまいります。

以上