

2026 年 10 月 24 日

各 位

住所	東京都渋谷区桜丘町 26 番 1 号
会社名	GMO インターネットグループ株式会社
代表者	代表取締役グループ代表 会長兼社長執行役員・CEO 兼グループ AI 変革最高責任者・CAIO 熊谷 正寿 (コード番号 9449 東証プライム)
問い合わせ先	取締役 グループ副社長執行役員・CFO グループ代表補佐 安田 昌史
TEL	03-5456-2555 (代)
URL	https://group.gmo

連結子会社 GMO インターネット株式会社における 不正アクセスに伴うお客様へのお見舞金のお支払いおよび不正取引による損失の補償に関するお知らせ

当社の連結子会社である GMO インターネット株式会社(証券コード:4784・東証プライム、以下、同社)が提供する「お名前.com デスクトップクラウド」(以下、本サービス)への第三者による不正アクセスについて、同社が 2026 年 10 月 24 日に公表した、お客様へのお見舞金のお支払いおよび不正取引による損失の補償等の対応方針について、下記のとおりお知らせいたします。

お客様および関係者の皆様に多大なるご迷惑とご心配をおかけしておりますことを、深くお詫び申し上げます。

1. 概要

同社は、これまでの調査により、本サービスのシステムにセキュリティ上の問題が存在し、本サービスの環境に対する不正なアクセスと、お客様の情報が外部に持ち出された事実を確認しています。また、一部のお客様から、お取引口座における身に覚えのない取引の報告を受けています。

同社は、多くのお客様に支えていただいていたインターネットインフラ事業者として、本事態を極めて重く受け止めており、お客様の保護を最優先とする観点から、特別措置として下記の対応を進めます。

2. 同社の対応方針

(1) お見舞金のお支払い

本サービスを現在ご利用されているすべてのお客様に対し、金銭的被害の有無にかかわらず、お見舞金として一律 5,000 円をお支払いします。このお見舞金は、本件によりお客様にご迷惑とご不安をおかけしたことに対するものであり、下記(3)に記載する不正取引による損失の補償とは別にお支払いします。対象となるお客様への連絡方法、受け取りの手続き、お支払い時期については、2026 年 10 月 30 日(金)23:59 までに登録のメールアドレス宛にお知らせします。

(2) 代替サービスのご提供と6か月間の無償化

同社は、お客様の安全を最優先とする観点から、不正アクセスを受けた現行のシステム基盤をそのまま再開することせず、抜本的なセキュリティアーキテクチャの刷新を行う判断をしました。これに伴い、本サービスをご契約中のお客様で、引き続き Windows デスクトップ環境の利用を希望するすべてのお客様には、独立したクラウド基盤上で運用されている代替サービスへの乗り換えを案内します。乗り換え後は、6か月間無償で利用できます。

代替サービスの提供にあたっては、安全性の確認を行うとともに、機能・利用方法の違い、移行に伴う注意事項、無料提供の対象範囲、無料期間終了後の料金・契約条件等を、お申し込み前に確認できるよう案内します。お客様の同意なく、代替サービスへの移行を行うことはありません。提供開始時期、申込方法、および移行を希望しないお客様の契約・利用料金の取り扱いについては、2026年10月30日(金)23:59までに電子メールにてお知らせします。

(3) お客様の取引口座における不正取引による損失の補償

本件の不正アクセスに起因して、お客様の意思によらない取引(以下、不正取引)が行われ、お客様の取引口座に発生した実現損失を補償します。補償の対象は、同社が調査の結果、不正取引であると認めた取引により生じた実現損失(取引の差損および手数料等)で、市場の変動による損失、取引で得られたはずの利益、その他の間接的な損害は対象に含まれません。対象かどうかは、同社が取引の記録、アクセスの記録、その他の資料をもとに確認します。確認にあたり、お客様に追加の資料の提出をお願いすることがあります。確認の結果については、お客様に個別にお知らせします。

お客様の意思によらない不正な取引被害が発生している場合は、①被害事実が確認できる情報(対象取引の日時、内容および損失額が客観的に確認できる情報)の提出、②取引所等に対し、対象取引が第三者の不正アクセスによるものである事情を説明し、取引の取消しおよび返金等を相談することを、お客様にお願いします。

①の提出にあたっては、ご本人様確認書類のご提出や、同社が直接取引履歴を確認するための専用パスワード(MT4/MT5ほかの閲覧専用パスワード等※1)のご提示を含め、具体的な提出手順の詳細を、別途案内します。

取引所等から返金があった場合は、その金額を差し引いた残額を同社が支払います。取引所等が返金に応じない場合も、同社が上記の補償の対象となる損失を支払います。お客様が、取引所等から返金を受けたにもかかわらず同社からも同じ損失の補償を受けた場合、およびその他の事実と異なる申請があった場合は、その金額の返還をお願いすることがあります。

申請方法、必要書類、受付期間、およびお支払い時期は、11月6日(金)までに、同社公式サイトおよび登録のメールアドレス宛に案内します。お客様の個人情報、取引情報は、本件の確認および補償の目的のためにのみ使用します。

同社が、補償の手続きに関して、お客様のパスワード(※1を除く)や暗証番号をお尋ねすることはありません。お心当たりのない連絡には、ご注意ください。

(4) 攻撃者からの悪質な脅迫行為に対する方針と防御措置について

同社は、本件の攻撃者とみられる者から金銭の要求を受けています。あわせて、要求に応じない場合には、同社およびお客様に関する情報を公開する等の行為に及ぶ旨の連絡を受けています。その内容は次のとおりです。

① 国内外の70を超える証券会社・FX会社等に開設されたお客様の取引口座に対する不正操作(不正な注文による口座残高の毀損)の継続

② 本サービスおよび本サービスに接続したお客様の PC に関する情報の不正公開と、ランサムウェア攻撃の実行

③ 同社のシステムや運用体制等に関する情報の不正公開

同社は、お客様の大切な資産および情報を標的とするこのような犯罪行為に対し、以下のとおり対応します。

同社は、攻撃者からの要求には応じません。要求に応じても、取得された情報の削除や不正利用の防止が保証されるものではないためです。本件については警察等の関係機関に相談しており、連携して対応を進めています。

本件脅迫行為については、通信記録等の全証拠を警察当局(サイバー犯罪対策部門)へ提出し、刑事事件として厳正な捜査を要請しています。なお、今後、攻撃者が同社やお客様に関する情報と称するものを公開する可能性があります。その中には事実と異なる内容が含まれるおそれがあります。同社からの正式なお知らせは同社ウェブサイト等を通じて行いますので、不確かな情報にはご注意ください。

お客様の資産・情報を守るための緊急防衛措置として、同社は、以下の措置を最優先で講じています。

不正取引の遮断: 主要な取引所・証券各社に対し、本サービス経由のアクセス遮断、全アクティブセッションの強制切断、および不正取引の緊急監視・抑止措置を要請・連携しています。

通信の遮断: 影響を受けたシステムに関し、ネットワーク接続を停止し、外部からの不正アクセスの経路を遮断しています。

(5) 政府・捜査機関等との連携

同社は、警察および所管官庁への初報を行っており、引き続き、関係機関への情報提供および捜査への協力を進めます。また、被害の拡大防止および同種の攻撃の防止に向け、能動的サイバー防御に関する措置の実施を含め、政府の関係機関への要請を進めます。

3. 当社の連結業績への影響

同社によるお見舞金のお支払いおよび損失の補償等が、当社の連結業績に与える影響については、現時点では算定できておりません。詳細が判明し次第、追加でお知らせいたします。

4. 経緯

同社は、2026 年 10 月 19 日にお客様からの問い合わせを受けて調査を開始し、10 月 20 日、本サービスの一部のお客様のサーバー環境に、第三者による不正なプログラムが設置されていることを確認しました。

同日、新規申し込みおよびコントロールパネルを停止、10 月 21 日午前 4 時から、被害拡大防止のため全プランのサーバーを順次停止しました。

10 月 21 日以降、同社はお客様から取引口座における身に覚えのない操作等の報告を受け付け、関係事業者へ状況を共有するとともに、お客様へのご案内等を通じて安全策実施への協力を依頼しております。また、10 月 22 日に警察に相談しております。

同社は、10 月 21 日、22 日および 23 日に本件の状況を公表しており、10 月 24 日に、上記 2 の対応方針を公表しました。

国民の資産保護に向けた「能動的サイバー防御」の適用に関する政府への具申について

1. 能動的サイバー防御 (Active Cyber Defense) について

能動的サイバー防御とは、サイバー空間における重大な脅威に対し、被害が深刻化する前に国や関係機関が主導して攻撃者のインフラや侵入経路を特定・無力化(無害化)し、被害の未然防止・拡大防止を図るセキュリティ枠組みです。従来の各事業者が個別に防御する枠組みを超え、サイバー攻撃者に対して国家レベルで先手を打って対処する安全保障上の重要施策として位置付けられています。政府における議論および関連施策の詳細は、内閣官房公式資料(サイバー安全保障に関する取組: https://www.cas.go.jp/jp/seisaku/cyber_anzen_hosyo_torikumi/index.html)をご参照ください。

2. 政府関係機関に対する「発動第1号」としての緊急具申

本件サイバー攻撃は、単なる一民間サービスのシステム障害にとどまらず、暗号化や情報窃取にとどまらない「一般国民の取引口座(金融資産)を標的とした不正操作・資産毀損」という極めて悪質かつ前例のない手口が用いられています。民間事業者単独の防御・事後対応のみでは、国境を越えて暗躍する高度なサイバー犯罪集団による国民資産の略奪を根絶することは困難です。

同社は、インターネットインフラを担う事業者としての社会的責任と危機感に基づき、本件を「国民の財産とサイバー空間の信頼を守るための能動的サイバー防御の『発動第1号』事案」として位置付け、国主導による攻撃基盤の追跡・遮断および無力化に向けた実効的な措置を講じていただくよう、政府関係機関へ強く具申(緊急要請)しました。同社は今後も、政府および捜査機関に対し、保有する全ログおよび侵害情報の提供を惜しまず、国と連携してサイバー犯罪の撲滅に全力を尽くします。

5. 今後の情報提供およびお問い合わせ先

同社は、今後、情報が判明次第、同社ウェブサイト等を通じて随時お知らせする方針です。当社も、新たに開示すべき事実が判明した場合は、速やかにお知らせいたします。

●本サービスに関するご相談窓口(GMO インターネット株式会社):

お問い合わせフォーム: <https://help.onamae.com/contact/>

電話: 03-5456-2560(土日・祝日を含め 24 時間受付)

(ご参考)既公表資料

- ・2026 年 10 月 21 日公表 <https://internet.gmo/news/article/246/>
- ・2026 年 10 月 22 日公表(同日 16 時 59 分時点) <https://group.gmo/info/alert/20261022/>
- ・2026 年 10 月 23 日公表(同日 16 時 10 分時点) <https://group.gmo/info/alert/20261023/>
- ・2026 年 10 月 24 日公表(同日 11 時 50 分時点) <https://group.gmo/info/alert/20261024/>

以上