

今回の GMO 事件について思うこと

2026 年 10 月 28 日午前時点

今回の GMO 事件で重く受け止めるべきことは、クラウドサービスへの不正アクセスが、情報流出にとどまらず、取引口座の不正利用や個人情報の公開を材料とした脅迫に波及し得る点である。今後、AI や攻撃用ツールの普及によって、攻撃の速度、規模、個人への圧力が増すおそれがある。今回の特殊性を認識しつつ、同様の被害が起こり得る条件を見直す必要がある。

GMO の 10 月 24 日付発表によれば、対象は「お名前.com デスクトップクラウド」であり、システム上のセキュリティ問題、不正アクセス、利用者情報の外部への持ち出しが確認されている。一部利用者からは、取引口座で身に覚えのない取引の報告も寄せられた。27 日には、攻撃者とみられる者が顧客情報などと称する情報を公開したことを同社が確認した。ただし、公開内容の真偽は調査中であり、同日 13 時 55 分時点ではランサムウェア攻撃の実行は確認されていない。予告と実行、流出の確認と公開情報の真偽は区別すべきである。

10 月 28 日朝のテレビ解説では、深刻なシステム上の問題と監視・防御の不足などが重なった珍しい事例との見方が示された。ただし、解説には犯人側の主張を前提とする部分もある。利用者の手元のパソコンから何が、どの経路で取得されたか、AI による分析が行われたかは、今回確認した公式発表からは確定できない。犯人の属性や技術水準についても、捜査・解析結果を待つ必要がある。

情報の公開を恐喝に使う手口自体は、既に広く確認されている。警視庁の公表では、2026 年上半期のランサムウェア被害報告は 123 件で、2020 年下半期以降の半期集計で最多となった。暗号化と情報公開の脅迫を組み合わせた「二重恐喝」が大半を占め、暗号化せず、盗んだ情報だけで金銭を要求する手口も確認されている。した

がって、バックアップがあっても、情報を盗まれた後の公開や悪用への備えは別途必要となる。

今後の深刻化については、公的な裏付けがある。英国 NCSC は、AI が脆弱性の探索、だましの手口、盗取データの処理などを効率化し、2027 年に向けて攻撃の頻度と影響を増すと評価している。2026 年 10 月 26 日公表の豪州 ASD の年次報告も、AI が攻撃の大規模化を助けると指摘している。これらを踏まえると、盗んだ情報を短時間で整理し、個人に合わせた詐欺や脅迫に使う動きが強まる可能性がある。ただし、今回の GMO 事件で AI が使用されたことを示す確認済みの事実とは区別する必要がある。

企業各社において、顧客資料や調査対象者の情報を必要以上に端末や外部サービスへ残さず、業務上必要な範囲でアクセスを認める運用が求められている。侵入の予防に加え、情報流出、口座の不正利用、信用毀損へ被害が連鎖することを抑える備えが、今後の経営課題となる。