

2026 年 10 月 29 日
iBank マーケティング株式会社

【第二報】

外部事業者への不正アクセスによるお客さま情報の漏洩に関するお詫びとお知らせ

iBank マーケティング株式会社（以下「当社」）が提供するアプリ「Wallet+（ウォレットプラス）」等の関連サービスでは、利用者向けメール配信に外部サービス「Cuenote FC」を利用しています。このたび、同サービスの提供元であるユミルリンク株式会社（以下「ユミルリンク社」）から、同社システムへの第三者による不正アクセスにより、Wallet+をご利用のお客さまのメールアドレスが漏洩した旨の報告を受けました。

お客さまをはじめ関係者の皆さまに多大なご心配とご迷惑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. 漏洩した情報および対象件数について

ユミルリンク社からの調査報告により、漏洩した情報および対象件数は以下のとおりです。なお、対象のお客さまには、Wallet+アプリ内等で個別にお知らせいたします。

- 漏洩した情報：メールアドレス

※漏洩した情報に、氏名・銀行口座情報・パスワード・取引履歴などは含まれておりません。

- 対象件数：合計 261,855 件

（対象のお客さまの Wallet+登録口座の内訳）

- ・ 十八親和銀行：37,737 件
- ・ 八十二長野銀行：88,107 件
- ・ 福岡銀行：136,011 件

2. お客さまへのお願い

本件に関連し、当社や関係会社を装った不審な電子メール等には十分ご注意ください。

また、Wallet+とは全く関係のない他社サービスを装った不審なメール等が届く可能性もございます。

当社が電子メールや SMS 等で、お客さまのパスワード、暗証番号等をお伺いすることはありません。不審な連絡を受けた場合は、メールに記載されたリンクへのアクセスや個人情報報告の入力を行わないようお願いいたします。

3. 今後の対応

当社は本件を重く受け止め、関係当局への報告を行いました。今後も必要に応じて関係機関と連携し、適切に対応してまいります。

当社では、ユミルリンク社とともに、引き続き原因究明を進め、再発防止に向けたセキュリティ対策の強化に取り組んでまいります。

4. 本件に関する Q&A

Q：Wallet+への不正アクセスがあったのですか？原因は何ですか？

A：Wallet+のアプリやシステム自体への不正アクセスは確認されておりません。ユミルリンク社のシステムに対する第三者による不正アクセスによるものです。

Q：ユミルリンク社ではどのような対策が取られていますか？今後も漏洩する可能性はありますか？

A：ユミルリンク社では、不正アクセスに利用された脆弱性の修正、不正プログラムの監視体制の整備、不正に利用された認証情報の削除、接続元 IP アドレスの制限などの対策を実施しています。現時点で新たな不正アクセスは確認されておりませんが、引き続き詳細な調査と再発防止策の強化が進められています。

Q：メールアドレス以外に、パスワードや口座残高なども漏洩しましたか？

A：いいえ、メールアドレス以外の情報は漏洩しておりません。パスワードや暗証番号、口座情報、お名前、ご住所などの情報は、当該の外部サービスには登録・保管されておりません。Wallet+のアプリも引き続き通常どおりご利用いただけます。

Q：今後、どのような被害が考えられますか？

A：本件に関連し、漏洩した情報を利用して、「Wallet+」または関係会社等を装った不審なメール等が送信される可能性があります。また、Wallet+とは全く関係のない他社サービスを装った不審なメール等が届く可能性もございます。実際に、ユミルリンク社の公表によれば、他社サービスを装ったメールが確認されております。不審なメール等を受信された場合には、記載された URL へのアクセスや添付ファイルの開封を行わないよう、十分にご注意ください。

5. 本件に関するお問い合わせ先

本件に関するお客さま専用のお問い合わせ窓口は、以下のとおりです。

お問い合わせメールアドレス：support@ibank.co.jp

以 上