



2026 年 10 月 26 日

各 位

会 社 名 ユミルリンク株式会社
代 表 者 名 代表取締役社長 清 水 亘
(コード番号：4372 東証グロース)
問 合 せ 先 常務取締役 小 林 幹 彦
(TEL. 03-6820-0514)

当社システムへの不正なアクセスに関するご報告（第二報）

2026 年 10 月 19 日にお知らせした内容に、その後の調査で判明した事項と当社の対応を加え、報告を更新いたします。

今般、このような事態となり、みなさまに多大なご迷惑とご心配をおかけしますことを心より深くお詫び申し上げます。

記

1. 本件事案の概要

2026 年 10 月 16 日(金)に当社担当者が一部システムにおいて不正アクセスが生じていることを確認いたしました。当該システムのアクセス記録を確認したところ、**I. プログラムの脆弱性**により、**II. 当社サポート・品質管理担当者のサービスへの認証情報を取得**していること、**III. 不正プログラムを設置しデータベースからデータを出力**していること、**IV. 当社サポート・品質管理担当者の認証情報を用い、他のシステムへの認証を試み**ていることを確認いたしました。

その後の不正プログラム、システムログの解析により、新たに 45 システム（第 1 報以降に流出を確認した Cuenote FC 44 システム、Cuenote BASE 1 システム）において、**V. 不正プログラムを介して他のシステムのデータを参照**していること、**VI. システムログイン時のセッション情報を取得し不正ログイン**していることを確認いたしました。

当社は、これを受けて不正アクセスを確認したサーバを直ちにネットワークより切り離すとともに、脆弱性修正プログラムの作成、適用、他システムからの当社サポート・品質管理担当者情報の削除、不正プログラム検知体制の整備など必要な被害拡大防止対策を実施いたしました。

【当社サービス一覧と不正アクセス・情報漏洩の有無】

サービス名	サービス概要	不正アクセス、情報漏洩の有無	件数：流出した情報
Cuenote FC	メール配信サービス（一斉送信）	ライブラリの脆弱性により、 <u>49 システムで</u> 情報漏洩が発生	51,628,280 件 (延べ件数)
Cuenote BASE	当社の顧客管理システム	プログラム脆弱性により、当社サービスの契約者情報が閲覧可	190 件

サービス名	サービス概要	不正アクセス、情報漏洩の有無 能な状態でありました	件数：流出した情報 企業名、氏名、電話、 メールアドレス
Cuenote SR-S	メール配信サービス(個別送信)	情報漏洩など影響はありません	
Cuenote SMS	ショートメッセージ配信サービス	情報漏洩など影響はありません	
Cuenote Auth	認証サービス	情報漏洩など影響はありません	
Cuenote Survey	フォーム・アンケートサービス	情報漏洩など影響はありません	
Cuenote Push	ブラウザ PUSH サービス	情報漏洩など影響はありません	
安否確認サービス	安否確認サービス	情報漏洩など影響はありません	
【Cuenote FC の一部サーバに対する不正アクセス、情報漏洩の概要】			
不正アクセスが試行 されたシステム数	システムの種別	内、情報漏洩の痕跡を 確認したシステム数	漏洩の恐れがある 件数（延べ件数）
3 システム	複数企業様でご利用いただくシステム	0 システム	0 件
78 システム	単一の企業様でご利用いただくシステム	49 システム	51, 628, 280 件

不正アクセスの末、メールアドレスなどの出力が確認されたシステムは計 49 システムであることを確認しております。現時点で漏洩件数の調査中であるシステムが 16 システム存在しており、今後の調査によって延べ件数は増加する可能性がございます。

Cuenote FC では、次のような情報が登録、記録されます。[アドレス帳]につきましてはご利用企業様毎に登録情報が異なるため、調査が完了し次第ご報告いたします。

[アドレス帳]

配信先メールアドレスおよびメールへの差込みや抽出のための氏名や都道府県、生年月日などの付属情報、サービスを利用される企業様毎に登録される付属情報が異なります。

[配信記録]

一斉送信単位で記録される通信先サーバとの通信記録、メールアドレスが含まれます。

[Web アクセス記録]

メールマガジンなどの申し込みページからの登録記録やマイページ機能を活用したユーザーの更新記録。

[サービス利用者情報]

本サービスを利用する企業担当者様の情報（氏名、メールアドレス、住所、電話番号）。

2. 本事案の経緯

年月日	時刻	対応等
2026/10/16	06:49	当社担当者が「システム 01」上の自身のアカウント異常に気付き、調査を開始
2026/10/16	07:12	「システム 01」に不正アクセスの恐れがあると判断し調査を開始
2026/10/16	10:10	ライブラリの脆弱性による攻撃である事を特定、不審な IP からのアクセスを遮断
2026/10/16	12:00	「不正アクセス対策本部」を発足、全社最優先体制へ移行
2026/10/16	20:10	Cuenote BASE にて脆弱性を他のユーザー情報の閲覧記録を確認、システムを停止
2026/10/16	20:46	脆弱性対策プログラムの適用を完了（I. VIへの対処）
2026/10/17	04:43	「システム 02」に対する不正プログラム設置を確認、システムを停止

年月日	時刻	対応等
2026/10/17	10:00	不正プログラムの解析による影響調査を開始
2026/10/17	12:58	攻撃手法を特定
2026/10/17	14:00	全システムに対する不正プログラムの設置有無の確認を開始
2026/10/17	14:00	外部セキュリティコンサルティング会社に協力を要請
2026/10/18	11:19	「システム 03、04、05」に不正プログラムが設置されていることを確認し、システムを停止
2026/10/18	12:47	「システム 04」に当社サポート・QA アカウントによる不正ログインがあることを確認し、システムを停止
2026/10/18	13:00	<u>サポート・QA アカウントの削除を開始（Ⅱ、Ⅳへの対処）</u>
2026/10/18	14:15	不正アクセスが特定データセンターで生じていることから、予防措置として同データセンターの全システムを停止、対象顧客に連絡
2026/10/18	16:24	不正アクセスが海外 IP であることから、海外からのアクセスを遮断
2026/10/18	17:00	<u>操作画面、API に対し IP 制限がなされていない環境への IP 制限（Ⅳ、Ⅴ、Ⅵへの対処）</u>
2026/10/18	17:08	海外 IP の接続制御を解除
2026/10/18	20:20	<u>不正プログラム設置の常時監視体制を確立（Ⅲ、Ⅴへの対処）</u>
2026/10/18	20:25	「システム 07」に対し不正プログラムが設置されたことを検知、システムを停止
2026/10/19	09:00	不正プログラムの解析による影響調査を継続
2026/10/19	09:00	警視庁サイバー事案通報窓口への届出
2026/10/19	19:00	個人情報保護委員会への届出
2026/10/20	01:00	予防措置として停止していた他システムを順次再開
2026/10/20	10:00	JIPDEC への届出（Cuenote FC）
2026/10/20	12:00	JIPDEC への届出（Cuenote BASE）
2026/10/20	21:29	不正プログラム解析により「システム 03」経由で「システム 08」に不正アクセスがあったことを確認
2026/10/21	15:30	予防措置として IP 制限が未設定の Cuenote SR-S サーバに IP 制限を実施
2026/10/22	09:00	全てのシステムのログイン、操作記録の遡及調査を開始
2026/10/25	21:45	新たに 42 システムに不正アクセス、データ出力記録があることを確認
2026/10/25	22:55	データ出力記録のあったシステムに対する影響範囲調査を開始
2026/10/26	12:30	新たに影響が確認された 42 システム（42 社様）にご連絡

3. データが漏洩したお客様へのご連絡状況

個人情報の漏洩の対象となる可能性のあるお客様に対しては、10 月 19 日の外部公表後、当社担当者から直接、本件のお詫びと今後の対応に関する連絡を個別に行っております。また、19 日以降新たに確認した情報漏洩の対象となる可能性のあるお客様に対しては、10 月 26 日 12 時 30 分までにご連絡を差し上げております。

4. 現時点で確認されている影響

現時点において、漏洩した個人情報が多数に公開された事実及び本事案に起因する個人情報の不正利用等の事実は確認されておりません。

他方、当社ドメインを利用し、第三者を騙った迷惑メールが複数確認されております。これらのメールは、当社及び第三者が送信指示したものと一切関係がなく、詐欺の可能性がありますので、十分にご注意ください。以下は、現時点において確認されている迷惑メールの一例です。

【迷惑メールの一例】

- ・ 件名 : 「ご利用確認のお願い」、「利用内容確認のご依頼」
- ・ 送信元アドレス : セゾンカード<info@cuenote.jp>、SAISON<info@cuenote.jp>

5. 当社の対応

現時点において、Ⅰ. VI. 脆弱性のあるプログラムの修正対応、Ⅱ. 及びⅣ. 当社サポート・品質管理担当者の認証情報の削除、Ⅲ. 不正プログラムの検知体制の整備、Ⅴ. 認証画面・API への接続元 IP 制限など再発防止策を講じるとともに、捜査機関への届出を行っております。

当社では本件を重く受け止め、外部専門家の協力のもと詳細調査を進め、情報セキュリティ体制のさらなる強化に努めてまいります。

6. 公的機関への報告状況

当社は、本事案の発覚を受け、サイバー犯罪の可能性が生じたため管轄の警視庁へ通報を行っており、今後の捜査に全面的に協力してまいります。また、個人情報保護法および関係法令に基づき、個人情報保護委員会へ速やかに本事案に係る個人情報の漏洩について報告を行いました。一般社団法人日本情報経済社会推進協会（JIPDEC）へも、同会の定める規約に基づき、本事案に係る個人情報の漏洩について報告を行いました。なお、独立行政法人情報処理推進機構（IPA）に対しては、経済産業省の告示（「コンピュータウイルス対策基準」及び「コンピュータ不正アクセス対策基準」）に基づき、全容の解明と原因の特定が完了次第、届け出を行う予定です。

7. お客様へのお願い

今回漏洩した情報が悪用され、当社や関係先などを装った不審なメールや SMS（ショートメッセージ）がお客様のもとに届く可能性がございます。二次被害を防ぐため、お客様におかれましては、大変お手数をおかけいたしますが、以下の点にご協力をお願い申し上げます。

(1) 当社アカウントのパスワード変更について

お客様のアカウントの安全性を確保するため、当社サービスのログインパスワードをご変更いただけますよう推奨いたします。

また、他社サービスにおいて同一のパスワードを使い回されている場合は、二次被害を防止するため、そちらのパスワードもあわせてご変更いただけますようお願いいたします。可能であれば、アカウント保護のために二段階認証の設定もご利用ください。

(2) 不審なメール等へのご注意

本件のインシデントに便乗した偽メールや SMS にご注意ください。当社や関係先を装い、偽の Web サイトに誘導して個人情報やアカウント情報を入力させるような不審な連絡が届く可能性がございます。

身に覚えのない連絡に記載された URL へのアクセスや添付ファイルの開封は絶対に行わず、不審な Web サイトに個人情報やパスワード等を入力しないようご注意ください。

なお、当社からメールや SMS、お電話等において、お客様のパスワード、認証コード、およびクレジットカード情報等の個人情報を直接お尋ねすることは一切ございません。

8. 今後の見通し

本件が2026年12月期の業績に与える影響については、現在精査中です。今後、開示すべき事項が生じた場合には、速やかにお伝えいたします。

みなさまに多大なご迷惑とご心配をおかけしますことを重ねて深くお詫び申し上げます。新たな事実が判明しました時点で、改めてご報告申し上げますので、ご理解賜りますよう、宜しく願い申し上げます。

<本件に関するお問い合わせ先>

ユミルリンク株式会社 不正アクセス専用お問い合わせ窓口

- ・電話番号 : 03-6820-0088 (受付時間: 平日09時00分～20時00分)
- ・電子メール : support@cuenote.ne.jp

※メールでのお問い合わせは24時間受け付けておりますが、ご返信につきましては平日9:00～19:00の間で順次ご回答させていただきますこと、ご了承くださいますようお願いいたします。

以上