2026年11月11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（第三報）

2026年10月19日（第一報）および10月26日（第二報）にてお知らせいたしました、当社が運営するメール配信サービス「Cuenote FC」等に対する外部からの不正アクセス事案（以下、「本事案」といいます。）につきまして、その後の詳細調査、関係するサーバ基盤を対象としたログ解析、および外部セキュリティ専門機関との連携検証の進捗を踏まえ、現時点までに判明した事実、漏洩件数、攻撃手法、および再発防止策を取りまとめ、報告を更新いたします。

今般、このような事態を招き、お客様ならびに関係各位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、改めて心より深くお詫び申し上げます。

記

## １．本事案の被害の概要および漏洩件数

システムに対する当社内でのフォレンジック調査およびデータ突合の結果、不正アクセスを受けた対象システムおよび外部への持ち出しが確認された個人情報の件数は以下の通りです。

| 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） | 現在の状況 |
|---|---|---|---|---|
| Cuenote FC | メール配信サービス（一斉送信） | プログラム脆弱性等を突かれ、49システム（専用ASPの一部）で情報漏洩が発生 | 配信先情報：延べ47,864,147件（メールアドレス、氏名等の属性情報） | 安全対策を完了、第三者によるフォレンジック調査対象システムを除き正常稼働中 |
| Cuenote BASE | 当社顧客管理システム | プログラム脆弱性により、契約者情報が閲覧可能な状態 | 190件（契約企業名、氏名、電話番号、メールアドレス） | 対応済であるが稼働を保留中（他システムにて運営） |
| Cuenote SR-S | メール配信エンジン | 不正アクセス・情報漏洩なし | 0件 | 正常稼働中 |
| Cuenote SMS | ショートメッセージ配信サービス | 不正アクセス・情報漏洩なし | 0件 | 正常稼働中 |

| サービス名 | サービス概要 | 不正アクセス・<br>情報漏洩の有無 | 件数<br>(流出した情報) | 現在の状況 |
|---|---|---|---|---|
| Cuenote Auth | 認証サービス | 不正アクセス・情報漏洩なし | 0件 | 正常稼働中 |
| Cuenote Survey | フォーム・アンケートサービス | 不正アクセス・情報漏洩なし | 0件 | 正常稼働中 |
| Cuenote Push | ブラウザPUSHサービス | 不正アクセス・情報漏洩なし | 0件 | 正常稼働中 |
| 安否確認サービス | 安否確認サービス | 不正アクセス・情報漏洩なし | 0件 | 正常稼働中 |

**【漏洩件数および対象データの確認に関する注記】**

※第二報では調査中であったシステムを含め、最大試算値（延べ約5,162万件）を公表しておりましたが、その後のログ突合およびデータベース解析により、実際の出力対象レコードを厳密に特定・除外し、重複して計上していたレコードを除外するなどして、配信先情報「延べ約4,786万件（47,864,147件）」であることを確認いたしました。

(Cuenote FCにおける対象データ別の延べ漏洩件数)

| 対象データ | メール<br>アドレス | 会員ID | 氏名 | 性別 | 生年月日 | 電話番号 | 郵便番号 |
|---|---|---|---|---|---|---|---|
| 漏洩件数 | 47,864,147件 | 30,500,167件 | 6,665,055件 | 2,059,658件 | 949,217件 | 412,794件 | 1,823,551件 |
| 対象データ | 都道府県 | 住所 | パスワード<br>(ハッシュ化) | 会社名 | 学校名 | 顧客が運用するサービスの認証情報<br>(2026年2月サービス閉鎖) | |
| 漏洩件数 | 1,212,868件 | 152,868件 | 226,158件 | 98,381件 | 10,608件 | 420,419件 | |

(Cuenote BASEにおける対象データの漏洩件数)

190件（企業名、氏名、電話番号、メールアドレス）

※流出したデータ項目の詳細は引き続き確認中であり、今後分かり次第公表する予定です。なお、クレジットカード情報等の決済情報の流出は現時点では確認されておりません。

## 2．第一報から第二報にかけて漏洩対象システムが増加した理由

・第一報（5システム）

本事案初動において、システムに対する直接的な実行命令や不正プログラムの設置、データベースへの直接接続といった「システム内部への重大な直接侵害」が確認されたシステムを特定・停止し、公表いたしました。

・第二報（新たに45システム追加、計49システム）

外部専門機関と連携し、当社全システムを対象とするWebアクセスログ・認証ログの遡及監査（第2次詳細調査）を実施いたしました。その結果、攻撃者が初期侵害拠点から窃取した有効なセッション情報を悪用し、Web管理画面の正規CSV出力機能を経由してデータをダウンロードしていた事象（後

述の攻撃手法２）を新たに特定いたしました。

この手法は不正プログラムの設置やデータベースへの直接侵入を伴わず、一見すると正規の管理者操作に見えるものであったため、詳細なセッション情報の解析完了をもって判明し、第二報として公表・個別通知を行うに至りました。

## ３．確認された攻撃の２つの手法と当社の対策

本事案において確認された攻撃手法は、大きく分けて以下の 2 系統です。

【攻撃手法１】不正プログラムの設置と内部侵入（直接侵入・横展開型）

プログラムの脆弱性をついて、サーバ内部に不正プログラムを使って、システムの中枢のデータベースへ直接侵入してデータを出力する手法です。さらに、管理用の内部ネットワークを伝って別のサーバへも侵入を拡大させました。（第１報の対象）

【攻撃手法２】ログイン情報の盗用となりすまし（正規機能の悪用型）

プログラムの脆弱性をついて、当時ログイン中だった正規利用者の一時的なセッション情報を盗み取り、正規の利用者になりすまして管理画面へ入る手法です。その後、画面に元から備わっている通常のデータ出力機能（CSV ダウンロード）をそのまま悪用してデータを持ち出しました。（第２報の対象）

## ４．本事案の経緯・対応時系列

攻撃の覚知から初動対応、外部専門機関の参画、各公表、および現在に至る時系列は以下の通りです。

| 年月日 | 時刻 | 事象および当社の対応 |
|---|---|---|
| 2026/10/16 | 06:49 | 当社担当者が運用管理システム上の自身のアカウントの異常を検知、調査を開始 |
| 2026/10/16 | 10:10 | 脆弱性を突いた攻撃元 IP を特定し、ネットワーク境界にてアクセス遮断 |
| 2026/10/16 | 12:00 | 全社「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 | 20:46 | 侵入の起点となったプログラムの脆弱性修正パッチを開発、全基盤へ適用 |
| 2026/10/17 | 04:43 | 不正プログラムが設置されたサーバを特定し、停止・隔離 |
| 2026/10/17 | 14:00 | 外部専門セキュリティ機関と連携し、全サーバを対象とした不正プログラムのスキャンを開始 |
| 2026/10/18 | 13:00 | 横展開の原因となった共通保守・QA アカウントの全基盤からの削除を開始 |
| 2026/10/18 | 17:00 | 全サービスの操作画面・API に対し、接続元 IP アドレス制限を適用 |
| 2026/10/18 | 20:20 | 不正プログラム設置を常時監視する体制を配備・稼働 |
| 2026/10/19 | 09:00 | 警視庁サイバー事案通報窓口への通報／個人情報保護委員会への報告 |
| 2026/10/19 | 15:00 | 当社システムへの不正なアクセスに関するご報告（第一報）を公表 |
| 2026/10/20 | 01:00 | 予防措置として停止していた他システムを安全確認のうえ順次再開 |
| 2026/10/22 | 09:00 | 全システムのログインおよび操作ログに対する遡及調査（セッション悪用監査）を開始 |
| 2026/10/25 | 21:45 | ログ全件解析により、セッション悪用によるデータ出力（42 システム）を新たに特定 |
| 2026/10/26 | 12:30 | 新たに影響が確認されたお客様への個別ご連絡を実施 |
| 2026/10/26 | 17:00 | 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）を公表 |

| 年月日 | 時刻 | 事象および当社の対応 |
|---|---|---|
| 本日 | － | **当社システムへの不正なアクセスに関するご報告（第三報）を公表** |
| 今後 | － | **外部専門機関による最終フォレンジック調査結果の受領・最終報告の公表** |

## ５．現在におけるサービス稼働状況および安全性の確認結果

当社では、本事案の判明後、すべてのサービス基盤を対象として、侵入経路の遮断、不正プログラムの排除、アクセス権限の見直し、およびシステムログの詳細調査を実施してまいりました。これらの調査・対策を踏まえ、今回確認された攻撃手法に対する必要な安全対策を実施し、サービスの稼働再開に必要な安全性の確認を完了しております。

現在、外部専門機関によるフォレンジック調査のため稼働を停止している Cuenote FC 専用 ASP の一部システムおよび Cuenote BASE を除き、各サービスは正常に稼働しており、お客様におかれては通常通り安全にご利用いただける状態です。

① 不正プログラムの排除

全サーバを対象としたスキャンにより、不正プログラムが存在しないことを確認済みです。

② 侵入経路の遮断

起点となった脆弱性修正プログラムの適用、ならびに接続元 IP 制限の適用を完了しております。

③ 影響のない環境の安全性確認

今回被害が確認されなかった専用環境および共用サービス環境については、攻撃の成立条件を満たしておらず、かつ詳細なログ監査により不正アクセスや情報漏洩の痕跡がないことを確認済みです。

## ６．再発防止策

当社では、被害拡大防止策にとどまらず、アーキテクチャおよび組織運用の根本的見直しを行い、以下の再発防止策を実施していきます。

① セキュアコーディングおよび脆弱性管理の抜本的強化

ファイルアクセス処理等における厳格な入力値検証の実装、および設計・レビュー規程の改訂を徹底するとともに、AI を活用したソースコードレビューや潜在的脆弱性の自動検知体制を導入し、さらに外部専門機関による定期的な第三者脆弱性診断を導入していきます。

② 特権アクセス管理および保守運用のゼロトラスト化

運用保守における作業即応性を維持しつつ侵害リスクを排除するため、システム内に恒常配置された共有管理者権限を撤廃し、多要素認証を前提としたセキュアゲートウェイ経由で、タスク実行時のみ最小権限を確立・運用します。

③ 多層防御による 24 時間 365 日の監視・インシデント即応体制の確立

全サーバ環境を対象に異常を監視するシステムを配備し、不審なファイル配置に対してアラート発報するとともに、専任監視体制による 24 時間 365 日の常時チェック、脅威の発生と同時に対応

する運用を行います。

## ７．公的機関への報告状況

当社は、管轄警察署への被害届の提出および捜査への協力を継続しております。また、個人情報保護委員会および一般社団法人日本情報経済社会推進協会（JIPDEC）への報告を行っております。なお、独立行政法人情報処理推進機構（IPA）に対しても所定の手続きを進めております。

## ８．今後の見通しおよび最終報告について

本件が 2026 年 12 月期の業績に与える影響につきましては、現在精査中であり、今後開示すべき事項が生じた場合には速やかに公表いたします。

現在、不正プログラムが設置された対象システムについて外部専門セキュリティ機関に委託しておりますフォレンジック調査の最終解析作業が進められております。同機関による調査結果報告書を受領した段階で、調査結果の総括として「最終報」を改めて公表させていただく予定です。

改めまして、貴社ならびに関係各位、そして対象となったお客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、重ねて深くお詫び申し上げます。

以上