

物語コーポレーション「焼肉きんぐ」公式アプリへの不正アクセス EC・会員システムを持つ中小企業が確認すべき5つの項目

公式発表（2026年10月5日・10月20日）をもとに整理した、顧客データを持つシステムの自己点検ガイド

2026年10月5日、物語コーポレーション株式会社は「焼肉きんぐ」公式アプリの会員管理システムへの不正アクセスによる個人情報漏洩（約1,079万件）を公表しました。顧客アプリ・ECサイト・会員管理システムを持つ中小企業も、同様の顧客データを保有しています。この資料では、公式発表の範囲で事実を整理し、今日から自社で確認できる5項目とセキュリティを考慮した開発の進め方をまとめます。

1. 何が起きたか（公式発表の範囲）

- 2026年10月2日：「焼肉きんぐ」公式アプリの会員管理システムへの不正アクセスを確認。通信遮断・防御措置を実施
- 10月3日：会員情報の漏洩を把握
- 10月5日：公表。個人情報保護委員会への報告を実施
- 漏洩件数：約1,078万8,963件
- 漏洩情報：会員番号・氏名（アプリ登録名）・メールアドレス・電話番号
- 非漏洩：パスワード・生年月日・性別・郵便番号・利用履歴・決済情報
- 10月20日続報：追加セキュリティ対策・監視体制強化、グループ11アプリで保持個人情報の最小化方針を発表

2. 中小企業に共通する3つの課題

課題1：顧客の個人情報を保有している

予約システム・ECサイト・ポイント管理・会員登録フォームを持つ中小企業は、顧客の氏名・メールアドレス・電話番号を保有しています。2022年の個人情報保護法改正により、一定要件を満たす漏洩は個人情報保護委員会への報告と本人通知が義務です（企業規模問わず）。

課題2：外部に公開されているシステムがある

顧客がアクセスできるシステムは外部から直接アクセスできる「入口」を持ちます。APIエンドポイント・Web予約システム・EC管理画面などの認証・認可が不十分な場合、企業規模を問わず悪用される経路になります。

課題3：「使っていない情報」を保有し続けている

物語コーポレーションが「保有情報の最小化」を方針として打ち出したように、取得したが使っていない情報を削除・取得停止することはリスクを根本から下げる手段です。「取得しない情報は漏洩しない」という発想が重要です。

3. 今日から確認できる5つの項目

#	確認項目	確認のポイント
①	保有情報の棚卸し	どのシステムにどの個人情報が入っているか把握できているか。取得している項目は業務上本当に必要か。
②	外部システムの認証状況	外部から利用されるAPIやWebシステムに適切な認証が設定されているか。長期間変更されていない認証情報がないか。
③	管理画面のアクセス制御	管理者権限アカウントは最小限か。退職者・業務委託終了者のアカウントが残っていないか。二要素認証・IP制限はあるか。
④	アクセスログの保存と確認	誰がいつ顧客DBにアクセスしたかのログが残っているか。異常アクセスを検知する仕組みがあるか。
⑤	漏洩発覚時の対応フロー	不正アクセス発見時に誰が何をするか決まっているか。個人情報保護委員会への報告・顧客への通知フローが整備されているか。

4. 開発・改修での進め方（3ステップ）

1. **現行システムの棚卸しと優先度付け**：外部公開システムを優先リストに挙げ、保有情報・アクセス権限の状況を確認する
2. **設定・認証の見直し**：管理画面の二要素認証設定・不要アカウントの削除・ログ保存の有効化など、コード変更なしで対応できる項目から着手
3. **設計段階でのセキュリティ要件の明文化**：新規開発・改修時は要件定義で「取得情報の最小化」「認証方式」「ログの保存期間」を明記。発注仕様書に含めることで開発会社との認識のズレを防ぐ

株式会社DnDにできること

業務システム・Webシステム・アプリの受託開発と、既存システムの点検（ソースコードの確認。対象システムの権利者からのご依頼に限ります）をご支援しています。「自社のシステムのリスクを把握したい」「セキュリティを考慮した新しいシステムを作りたい」という段階からご相談ください。

ご相談・お見積りは無料：<https://dnd-inc.jp/contact.html>