

これは説明用のサンプルです。架空の企業「株式会社サンプル」を題材にした見本で、**実在の企業・実在の調査結果ではありません**。実際のレポートは、お申し込みいただいた御社について同じ形式で作成します。

◆ NGRAPH CYBER DRILL

セキュリティ調査レポート

攻撃者の視点で、外から見える御社の状態を調べました（STEP 1・外から見える入口の洗い出し）

対象 **株式会社サンプル** 法人番号 **00000000000000** 調査日 **2026-10-16** 版 **サンプル**

総合評価（今回の調査範囲）

外から見える範囲は、おおむね良好です

外から見える資産は少なめですが、**早めに確認したい項目が2件**（旧通販の管理画面＝サポート終了の EC-CUBE 2.13／WordPress採用サイトのログイン・API露出）と、メール運用の見直しがあります。

※「実際に侵入できるか」や「社員が偽メールを踏むか（フィッシング）」は、この部分では**未検証**です。中小企業が実際に被害に遭うのは多くがこの“人の層”で、そこはSTEP 1の後半（訓練メール）で確かめます。



結論（まず3点）

- 1 外から見える資産は少なめ。ただし旧CMSの管理画面/APIが2か所、外に開いています。**
旧通販（EC-CUBE）とWordPress採用サイト。ここは早めに確認・対処を。
- 2 むしろ気をつけるのは「人のミス」。**偽の請求書・振込先変更やフィッシングなど。これらはこの部分では**未検証**で、STEP 1の後半（訓練メール）で確かめます。中小企業の実被害はここが多い。
- 3 万一侵害されても、事業を止めない備えが肝。**バックアップ・復旧の仕組み（外からは見えないため要確認）。

早めに手を打ちたいのは**2件**：外から開いている**旧EC-CUBE 2.13の管理画面**と、**WordPress採用サイト**のログイン/API露出を、閉じる・固める。

2 確認を優先したい
旧EC-CUBE・WordPress採用サイト

1 設定で改善できる
メールのなりすまし対策

1 社内で確認したい
業務メールの運用

4 参考情報
採用・類似ドメイン 等

手法＝公開情報の参照・通常のHTTP/DNS照会（認証の試行や攻撃は未実施。侵入可能性は未検証）。一部は**既存の取引資料でも確認**し、出所を分けて記載。各項目は深刻度の断定ではなく**確認の優先度**で区分しています。

● 点検した項目（全体像）

公開情報の範囲で、次の項目を点検しました（○＝問題の兆候なし／△＝設定で改善／△＝要確認／情報・確認事項）。詳細は以下の各セクションに記載します。

点検した項目	結果
公開ドメインの棚卸し（忘れられた公開環境がないか）	○ 問題の兆候なし
メールのなりすまし耐性（SPF・DKIM・DMARC）	△ 設定で改善
外から見える管理画面・ログイン口の露出	△ 要確認（2件）
CMS・ECの既知リスク（バージョン等）	△ 要確認
Web基本設定（TLS・各種セキュリティヘッダー）	○／情報
類似文字列のドメイン	情報・監視候補
侵入されても致命傷にしない備え（回復力）	確認事項（外からは見えない）

● 確認を優先したい点

旧通販サイトの管理画面ログインが公開（EC-CUBE 2.13・サポート終了版）

確認優先

観測事実	sample-shop.example.jp/manage/ を取得したところ、EC-CUBE 2.13 の管理画面ログインページでした（タイトル「管理機能」・ログインフォーム・ECSESSIDクッキー）。EC-CUBE 2.13 はサポートが終了した古いバージョンです。※ログインは試みておらず、認証を突破できるかは未確認です。
なぜ優先	サポート終了版は既知の弱点が直されないまま残り、管理画面のログインが外から到達できる＝総当たりや既知の脆弱性の標的になり得ます。旧通販の注文データ（顧客情報）が残っている可能性もあります。
確認・対処	応答本文・最終URL・用途を確認。使っていなければ閉鎖、残すなら社内IP制限や認証で外部到達を止める（必要に応じてソフトの更新も）。
根拠	2026-10-16・GET sample-shop.example.jp/manage/ → 200・タイトル「管理機能」・「EC-CUBE管理画面」表記・2.13系（「2.14で削除予定」の注記）・Cookie ECSESSID

採用サイトがWordPress（管理画面・REST APIが外から到達可能）

確認優先

観測事実	sample-recruit.example.jp はWordPress（7.1.3）。ログイン画面 wp-login.php が応答し、REST API（wp-json）が公開（200）、生成元メタにバージョンが表示されています。※ログイン試行・ユーザー列挙の実行はしていません。
なぜ優先	WordPressは最も狙われるCMSです。ログイン画面の公開＝総当たり・パスワードリストの標的、REST API公開＝ユーザー名（ログインID）の列挙が既定では可能なことが多く、バージョン表示＝既知の脆弱性の突き合わせが容易。プラグイン・テーマの既知脆弱性も主要な侵入経路です。
確認・対処	本体・プラグイン・テーマを最新化、ログイン試行の制限（回数制限・管理画面のIP制限）、REST APIのユーザー列挙を無効化、バージョン表示の抑制。可能ならWAFの導入。
根拠	2026-10-16・GET sample-recruit.example.jp : wp-content/wp-includes/wp-json 多数・generator「WordPress 7.1.3」・wp-login.php 応答・wp-json 200。ユーザー列挙の実行可否は、書面で許可された範囲でSTEP 1の後半に確認。

● 改善が見込まれる点

メールのなりすまし対策（DMARC・DKIM・SPF）

改善事項

観測事実	DMARCレコードは照会で確認できず。DKIMは照会したセレクト（google等）では鍵を確認できず（全体の設定状況は未確認）。SPFは存在し、`mx`（＝MXホスト）とレンタルサーバ系を許可。受信MXはGoogleでした。実際の送信経路とSPF/DKIMの整合性は未確認です。
想定リスク	自社ドメインを詐称するメールへの対策が弱いと、取引先が偽の請求書・振込先変更を見分けにくくなります（※DMARCは、似た別ドメイン・表示名の偽装・正規アカウント乗っ取りは防ぎません）。
推奨	実際の送信元を棚卸し→SPFを送信元に合わせる（Google利用なら`include:_spf.google.com`等）→DKIM署名→DMARCを監視から開始。正規メールへの影響を確認しながら段階的に（レンタルサーバの許可は安易に削除しない）。なお急ぎではなく、@sample-foods.example.jpを送信にあまり使っていなければ重要度はさらに下がります。実害（偽の振込先）の防止は、下記「振込先の変更は電話で確認」の運用の方が効きます。
根拠	2026-10-16・DNS照会。_dmarc=なし/google._domainkey=なし/MX=SMTP.GOOGLE.COM/SPF=「v=spf1 +a:svXXXX.example-host.jp +a:sample-foods.example.jp +mx include:spf.example-host.jp ~all」

● 内部統制の確認事項

業務メールにフリーメールを使用（代表＝Yahoo／経理・担当＝Gmail）

確認事項

観測事実	代表者＝Yahooの個人アカウント、経理・担当＝Gmailを業務に使用し、印刷費などの請求書もこの経路でやり取りしています。（この項目は公開情報ではなく、既存の取引資料で確認）
想定リスク	アカウントの管理権限・2段階認証・退職時の失効・振込先変更時の確認／承認手順が未確認です。手順が無いと、似たアドレスからの依頼やアカウント侵害で誤送金につながる可能性があります（独自ドメインでも同種の詐欺は起こり得ます）。
推奨	会社管理のアカウント＋2段階認証、振込先変更は既知の番号へ折り返し確認・複数人承認。独自ドメインへの統一も選択肢。※具体のアドレスは必要時のみ別紙で限定共有。
根拠	取引資料で確認（※本サンプルのため内容は架空）

● 情報・運用上の助言

採用サイトで社員情報を公開

情報・助言

観測事実	採用サイトに社員の実名・顔・役職つきの紹介があります（正当な採用広報です）。
助言	公開情報はなりすましメールの材料に使われ得ます。掲載の同意・更新責任・不審な依頼は別経路で確認する運用を。退職者の掲載が残っていないかも定期点検。

類似文字列のドメイン

情報・助言

観測事実	sample-foods.jp・sample-foods.comが名前解決します（管理主体・用途・なりすまし利用は未確認）。sample-foods-co.jp等は照会で解決せず（登録の有無はWHOIS/RDAP未確認）。
助言	各ドメインの所有者を確認し、自社で使うべきものは取得、紛らわしいものは監視候補に。

コーポレートサイトの仮ドメイン残存（情報品質）

情報・助言

観測事実	本文に制作時の例示用ドメイン（example等）の置換漏れが見られました。
助言	該当箇所を正しい値に修正（表示文言か、フォーム送信先・外部参照先かで影響が変わるため、箇所を特定して対応）。

Webのセキュリティヘッダー

情報・助言

- 観測事実** トップ等でCSP・HSTS・クリックジャッキング対策などの応答ヘッダーを確認できませんでした（対象URL・既存の防御の有無は要確認）。
- 助言** 管理・決済など操作を伴う画面を優先して、応答ヘッダーの付与を検討。

● 確認できた（問題の兆候がなかった）事実

- ✓ 通信の暗号化（TLS）は有効（コーポレート・採用とも、照会時点）
- ✓ 公式サイトの会社名・所在地が登記と一致（偽サイト判別の参考。セキュリティ評価ではありません）
- ✓ 証明書ログの照会範囲では、意図しない公開名の痕跡は見当たらず（検索サービス・期間・取得名の範囲内）

● 侵入されても“致命傷”にしないための備え（確認事項）

ここは外からは見えません。欠陥とは断定しませんが、万一のとき「事故」で済むか「事業が止まる」かを分けます（STEP 2・現場で確認）。

- ☐ **重要データのバックアップ**
顧客・受発注・会計。オフライン／書き換え不可で保管し、復元テストまで行っているか。
- ☐ **アカウント復旧**
メール・BASE・SNS を乗っ取られても取り戻せるか（2段階認証・回復用連絡先）。
- ☐ **検知**
不正ログインに気づけるか（通知・記録）。
- ☐ **初動**
誰に連絡し何を止めるか、手順が決まっているか。
- ☐ **管理責任・委託先**
ドメイン/DNS/SaaS の管理者・退職時の失効、保守の委託責任、ソフトのサポート期限。
- ☐ **現場の分離**
POS・決済・店舗Wi-Fi が業務系と分かれているか。
- ☐ **復旧目標（RTO/RPO）**
どれだけの時間で、どこまで戻せれば事業が続くか。

● 用語ミニ解説（メールのなりすまし対策）

「メールは差出人を誰でも名乗れる」ため、受け取り側が“本物か”を確かめる3つの仕組みです。

SPF 差出人の住所録

「うちのメールはこのサーバーから出す」という宣言。受け取り側が、名乗り通りの正規サーバーから来たか照合します。

DKIM 本物の電子署名（実印）

メール1通ごとに、ドメインの持ち主だけが作れる電子署名を付与。途中で改ざんされていないかを確認できます。

DMARC ニセモノの扱い+通報

SPF／DKIMの確認に失敗したメールをどうするか（素通し／迷惑メール／拒否）を宣言し、なりすましの報告も受け取れます。

→ 3つ揃うと「@sample-foods.example.jp」を名乗る偽メールが取引先に届きにくくなります。※似た別ドメイン・表示名だけの偽装・正規アカウントの乗っ取りは、これらでは防げません（別の対策が必要）。

● 調査の方法と根拠

▼ 何を・どう調べたか／未確認の点（クリックで開閉）

調査日	2026-10-16 以降に状態が変わる可能性あり
手法	DNS 照会（DoH）／HTTP 応答ヘッダーの取得（HEAD）／ 証明書透明性ログ（crt.sh）／法人・インボイスの公表情報 （gBizINFO・国税庁）／Web検索。 認証試行・脆弱性攻撃・ 辞書的パス探索は未実施 対象サーバーへの通常の通信は発生（＝「一切触れていない」 ではありません）
公開Web資産	sample-foods.example.jp（自作PHP・WordPressではない）／ sample-recruit.example.jp（ WordPress 7.1.3 ・wp- login/REST API公開）／sample-shop.base.shop（BASE）／sample- shop.example.jp（BASEへ転送、ただし /manage/ は EC-CUBE 2.13 の 管理画面ログインが公開） 実測・リダイレクト追跡
外部掲載	各種グルメサイト・求人媒体・企業情報の集約サイト・SNS に 店舗/会社情報 Web検索。なりすまし・口コミ改ざん・情報集約の面（欠陥ではなく 一般的な露出）
主な未確認事項	/manage/ の応答内容・製品/バージョン・認証方式／DKIM全体の設定 ／SPFと実送信経路の整合／類似ドメインの管理主体・登録状況／ サブドメインが同一IPに解決する理由（個別かワイルドカードか）／ 各ヘッダーの対象URL 侵入可能性は、書面で許可された範囲で STEP 1 の後半に確認
参考情報（会社の实在確認）	商号 株式会社サンプル／法人番号 00000000000000／インボイス T00000000000000。 セキュリティ評価ではなく实在確認の参考 gBizINFO・国税庁

● 次のステップ

STEP 1 の後半：書面でのご許可（対象・手法・実施時間・負荷上限・中止条件を明記）をいただいた範囲で、上の確認事項を実際に確かめ、**社員への訓練メール**を行います。結果は、この報告書に追記してお渡しします。**外部サービス（BASE 等）は、お客様の許可だけでは及ばない範囲があり、その事業者の許可が別途必要です。**

STEP 2（ご希望の場合）：報告をもとに、合意した対策（設定・権限・バックアップ・手順など）を現場で一緒に進め、同じやり方でもう一度確かめます。

本レポートの性質と範囲：STEP 1 のうち、公開情報の参照と通常のHTTP/DNS照会にもとづく「外から見える入口の洗い出し」の部分の報告で、侵入可能性（実際に侵入できるか）の検証は含みません。記載は観測した事実と、追加確認が必要な項目を分けて示したものです。危険の断定や課題の創作はせず、調べていない点は「未確認」と記しています。一部の項目（業務メールの運用）は公開情報ではなく既存の取引資料で確認したもので、出所を分けています。公開情報であっても個人情報に該当し得るため、利用目的・保管・共有範囲を管理します。
作成：NGraph（エヌグラフ）／Cyber Drill・2026-10-16・STEP 1 レポート（サンプル・架空企業・説明用）