

セキュリティ基本点検

見本レポート

架空の事例・見本

非侵入型の基本点検で何が分かり、何を先に見直すかをお伝えする報告書の見本です。公開ページで見えることと、設定資料がなければ分からないことを分けて整理します。

すべての所見・証拠・状況は説明用の仮定です。実サイトへの点検、スキャン、管理画面へのアクセスは実施していません。実際の漏えいや被害を示すものでもありません。

この見本の対象

対象サイト サンプル事業者の案内サイト example.com

想定範囲 トップページ、お問い合わせ案内、公開された管理者向け導線と、機密を伏せた設定資料。対象は相談で合意する想定です。

example.com は例示用の予約ドメインです。この資料の作成ではアクセスしていません。作成日 2026 年 10 月 24 日

確認結果の見本と次の行動

項目	見本の内容	確認の状態	優先順位
01	旧資料へのリンクの公開意図	表示のみ確認した想定	先に確認
02	HTTPS の接続表示と証明書	一部確認した想定	継続確認
03	管理者の MFA と権限	資料不足で未確認	先に確認
04	CMS や PHP の更新状況	資料不足で未確認	計画して確認
05	バックアップと復元記録	設定のみ確認した想定	計画して確認

優先順位は、この架空例で次に確認する順番です。脆弱性の深刻度や攻撃の成功率を採点したものではありません。未確認というだけで「危険」とは判定しません。

本例では公開範囲と管理者権限を先に整理し、更新と復旧の確認計画につなげます。実案件では、扱う情報、事業への影響、証拠の確かさに応じて調整します。

報告書の読み方

「観測事実」は確認した表示や資料の内容、「未確認」は証拠が足りないこと、「考えられる影響」は条件付きのリスク推測です。この見本では観測事実もすべて架空です。証拠例 E01～E05 は記録の説明で、実際の画面や資料の添付はありません。

公開ページで確認できる範囲

実際の点検では、合意した公開ページを通常どおり閲覧し、そのとき見えた表示や接続情報を記録します。見えない URL の探索、ファイル名の総当たり、攻撃用の操作は行いません。

01 旧資料へのリンクの公開意図を確認する

観測事実の例 公開ページに「旧資料」というリンクが表示されている、という仮定です。リンク先のファイルは開いていません。

確認方法と証拠例 合意したページの通常閲覧。証拠 E01 はリンク表示の位置が分かる画面の記録です。実案件では対象ページ、確認日時、確認方法も記載します。

未確認 リンク先が実際に閲覧できるか、公開が意図されたものか、内容に秘密情報があるかは未確認です。

考えられる影響 公開不要な資料にアクセスでき、秘密情報が含まれていた場合は、意図しない閲覧につながるおそれがあります。この表示だけでは情報漏えいを断定できません。

次の行動 先に確認。所有者へ公開意図を確認し、必要なら権限のある担当者が保管先と公開範囲を見直します。削除や設定変更は別途合意・承認してから行います。

不要ファイルは考え方を示す例です。内容の取得、推測したパスへのアクセス、秘密情報の収集は行いません。

02 HTTPS の接続状態を記録する

観測事実の例 合意した公開ページを HTTPS で開き、ブラウザーの証明書表示で対象名と有効期間を確認できた、という仮定です。証拠 E02 はその表示の記録です。

未確認 別ページや外部サービスの状態、すべての TLS 設定、将来の証明書更新は未確認です。HTTP ヘッダーや DNS も、合意した範囲で観測できた項目だけを記録します。

考えられる影響 HTTPS の確認だけで、サイト全体の安全性や保存データの保護を判断することはできません。

次の行動 継続確認。証明書の更新担当と確認方法を整理します。表示が正常という例であり、全体の安全を保証する判定ではありません。

設定資料で確認する範囲

管理画面や非公開設定を確認するには、事前承認と適切な権限が必要です。まずは機密を伏せた設定資料で確認します。公開ページの見た目だけで、次の設定を断定しません。

03 管理者の MFA と権限は未確認

観測事実の例 公開されたログイン画面への導線はあるが、認証・権限の設定資料はない、という仮定です。証拠 E03 は公開導線の記録と、必要資料が未提出の確認メモです。

未確認 MFA（パスワードに加える本人確認）、接続元制限、管理者権限の範囲、退職者等のアカウント整理状況は未確認です。

考えられる影響 保護が不十分な場合は、認証情報の悪用や不要な権限の残存による影響が大きくなるおそれがあります。ログイン画面が見えること自体は脆弱性の証拠ではありません。

次の行動 先に確認。権限のある担当者から、秘密情報を隠した認証設定と権限の説明を受けて判断します。パスワード試行や認証突破は行いません。

04 CMS と PHP の更新状況は未確認

観測事実の例 CMS・プラグイン・PHP の版数と更新管理の資料がない、という仮定です。証拠 E04 は必要資料の確認メモです。外部から版数を確定したものではありません。

未確認と影響 利用中の版数、サポート状況、更新担当が不明です。サポート終了や必要な更新の未適用があれば、既知の問題が残るおそれがありますが、本例では断定できません。

次の行動 計画して確認。機密を伏せた環境情報を受け取り、該当する公式サポート情報と照合します。更新作業や動作検証は別途範囲を確認します。

05 バックアップ設定と復元の実績を分ける

観測事実の例 「毎日」の取得設定が分かる架空資料はあるが、実行結果や復元記録はない、という仮定です。証拠 E05 は秘密情報を隠した設定画面の記録です。

未確認と影響 実際の取得成功、対象データ、保管先の保護、復元可否は未確認です。設定だけで復旧できるとは言えず、不足があれば障害時の復旧に支障が出るおそれがあります。

次の行動 計画して確認。取得結果、対象範囲、保管方法、過去の復元記録を確認します。実データや丸ごとのバックアップの送付は求めず、復元作業も実施しません。

点検の範囲と相談の進め方

この点検に含まれないこと

侵入テスト、認証突破、パスワード試行、脆弱性の悪用、負荷試験、自動・網羅的スキャン、ソースコードレビューは対象外です。

フォレンジック調査、漏えいの有無の断定、マルウェア除去、緊急復旧、継続監視、バックアップの復元も含みません。すべての脆弱性の検出、不正アクセスの完全な防止、安全性や認証取得を保証するものではありません。

報告書に改善案があっても、修正や設定変更を自動的に行うことはありません。作業可能な環境と対応可否を確認し、別途見積もりと事前承認のうえで範囲を決めます。

相談から報告まで

1 まず相談 所有者または許可を得た管理者から、対象 URL、気になる点、分かる範囲の利用環境をお知らせください。

2 範囲を合意 1 サイトの対象ページ・項目・必要資料・権限を確認します。受付前に料金と納期に合意し、資料の保存・削除方針も確認します。

3 合意した範囲を点検 通常閲覧と機密を伏せた設定資料で、事実・根拠・未確認・優先順位を整理します。確認できない項目は未確認のまま残します。

4 報告案を確認 現行の案内では正式納品前の質問は1回・最大3項目、補足回答は1回です。最終の PDF 報告書で内容を確認します。

最初の相談に、パスワード、API キー、個人情報、データベース全体、丸ごとのバックアップを添付しないでください。外部 AI へ資料を送る必要がある場合は、送信先・データ・目的について個別の事前同意が必要です。

公式の案内と相談窓口

点検の範囲と最新条件は、公式の点検ページをご確認ください。同ページの「点検できる範囲を相談する」から相談フォームへ進めます。

Web サイトのセキュリティ基本点検

<https://webtasuke.com/security-check/>

公開済み記事 個人情報の流出と二次被害への備え

<https://webtasuke.com/articles/personal-data-leak-secondary-harm/>

Web たすけ公式サイト

<https://webtasuke.com/>

上記の公開案内を 2026 年 10 月 24 日に確認しました。この見本は個別案件の受付・料金・納期を確約するものではありません。各案件で合意した条件が適用されます。