【見本】会社名・ドメイン・診断結果はすべて架空です。実際のレポートも、この形で毎月お届けします。

見本ウェブ制作（架空）

架空商事 様　サイバー健診 診断レポート（2026-12）

対象ドメイン：example.co.jp　診断日時：2026年12月1日 9:00（日本時間）

D

総合評価（59点）

評価を下げている項目：DMARC のポリシーの強さが要対応（重要度 中）、HTTPS の強制（HSTS）が要対応（重要度 中）、既知の脆弱性との照合が要確認（重要度 中）　ほか4項目

なりすましメール対策：**B**　SSL/TLS 証明書と通信の暗号化：**A**　Webサイトの安全設定：**B**

外部から見える入口：**A**

評価は当社の自動診断の結果を、決まった計算式で表したものです（100点から、対応が必要な項目ごとに重要度に応じて減点。重要度「高」の要対応項目が1件でもあればC以下）。公的機関による認定や評価ではありません。

要対応・要確認	新規	前回から解消	継続
7	**6**	**1**	**1**

最初に確認する項目

DMARC のポリシーの強さ（example.co.jp）

レポートでなりすましがないことを確認したうえで p=quarantine に、最終的に p=reject に変更してください

新たに検出された項目

重要度	診断項目	対象	検出内容	推奨対応	SCS★3

△中	**管理画面・リモート接続の入口**	vpn.example.co.jp	リモート接続・メールの入口と思われるホスト名（証明書の発行 2026-09-01、DNS 登録あり）	使用していない場合は DNS レコードを削除してください。使用中の場合は、アクセスできる接続元を制限し、多要素認証の設定と更新状況をご確認ください	4-5-1（ごく一部の手がかり：ホスト名からの推測）
△中	**既知の脆弱性との照合**	www.example.co.jp	WordPress 5.8.1（generator）：該当する可能性がある公開の脆弱性 18件（うち CVSS 7.0 以上 6件。例：CVE-2022-21661（7.5）、CVE-2022-21664（7.4））	サポート対象の最新版に更新してください。OS のパッケージで提供されている場合は、修正が取り込み済み（バックポート）のこともあるため、提供元の更新状況をご確認ください	4-4-4（手がかり：公開サーバーのバージョン表示）
×中	**DMARC のポリシーの強さ**	example.co.jp	p=none	レポートでなりすましがないことを確認したうえで p=quarantine に、最終的に p=reject に変更してください	
△中	**DMARC レポートの集計**	example.co.jp	直近30日に受信側（google.com、Outlook.com など）が報告した自社名義のメール 4,210通のうち、認証に成功 3,980通（94.5%）	認証に失敗している送信元を、下の一覧でご確認ください。自社で利用しているサービスであれば、SPF・DKIM の設定に追加してください	
△中	**認証に失敗した送信元**	example.co.jp	認証に失敗した送信元：203.0.113.25（逆引き：example-mailer.net）から 214通	自社で利用しているサービス（メール配信・請求書の送付など）であれば、SPF と DKIM の設定に追加してください。心当たりがなければ、なりすましの可能性があります	
△低	**ソフトウェアのバージョン表示**	www.example.co.jp	generator: WordPress 5.8.1	バージョン情報の表示を無効にし、実際のバージョンがサポート対象で最新かを管理画面でご確認ください	4-4-4（手がかり：公開サーバーのバージョン表示）

前回から継続している項目

重要度	診断項目	対象	検出内容	推奨対応	SCS★3
×中	**HTTPS の強制（HSTS）**	www.example.co.jp	未設定	Strict-Transport-Security ヘッダーを設定してください	

前回から解消された項目

重要度	診断項目	対象	検出内容
○	**SPF の末尾の指定**	example.co.jp	-all

自社名義で送られたメール（DMARC レポートの集計・直近30日）

受信側（google.com、Outlook.com、Yahoo）の報告によると、自社名義のメール 4,210通のうち 3,980通（94.5%）が認証に成功しました。認証に失敗した送信元が自社で利用しているサービスでなければ、なりすましの可能性があります。

送信元の IP	逆引き	通数	成功	失敗
198.51.100.10	**google.com**	3,610	3,602	8
198.51.100.77	**amazonses.com**	386	378	8
203.0.113.25	**example-mailer.net**	214	0	214

毎日の確認でお知らせした内容（直近30日）

日付	内容	詳細
2026年11月13日	**SSL/TLS 証明書の有効期限まで残り14日です**	shop.example.co.jp：有効期限 2026-11-27
2026年11月16日	**解消：SSL/TLS 証明書の有効期限まで残り14日です**	shop.example.co.jp：有効期限 2027-02-13
2026年11月22日	**なりすましの可能性があるメールを検知しました**	2026-11-21：203.0.113.25（逆引き：example-mailer.net）から、認証に失敗した自社名義のメールが 96通

SCS評価制度★3 の要求事項に関係する手がかり

要求事項	内容	本診断から分かる手がかり	今回の状況
2-1-1	**取引先とのシステム上の関係の把握**	利用している外部サービス（メール・DNS・送信サービス）の一覧	未確認（フルプランで診断）
3-1-2	**ネットワークに関する情報の把握**	外部に公開しているサブドメインの一覧	未確認（フルプランで診断）
3-1-3	**外部情報サービスの管理**	利用している外部サービスの一覧	未確認（フルプランで診断）
4-4-4	**セキュリティパッチ・アップデートの手続**	公開サーバーのバージョン表示と、該当する可能性がある既知の脆弱性	要確認の項目あり
4-5-1	**ネットワーク境界防護**	外部から見える管理画面・リモート接続の入口（ごく一部）	要確認の項目あり

SCS評価制度★3の要求事項（Ver.1.1、26項目）のうち、本診断の結果が手がかりになりうるのは上の5項目の一部です。IPA の自己評価等ガイド（SCS-410）と解説書（SCS-620）（2026-10-28 付）には、外部からの診断の結果を自己評価の証跡として使えるかの記載がありません。本診断は★3の証跡・取得・要求事項の充足を示すものではありません。残りの項目（社内ルール、ID・パスワード管理、教育、バックアップ、端末の対策、手順など）は外部からは確認できません。

全診断項目

結果	診断項目	対象	検出内容
○	**SPF（送信元の認証）**	example.co.jp	v=spf1 include:_spf.google.com -all
○	**SPF の末尾の指定**	example.co.jp	-all
×	**DMARC のポリシーの強さ**	example.co.jp	p=none
○	**DKIM（電子署名）**	example.co.jp	google
○	**SSL/TLS 証明書の検証**	www.example.co.jp	TLSv1.3 / Let's Encrypt
○	**証明書の有効期限**	www.example.co.jp	2027-02-01（残り62日）
×	**HTTPS の強制（HSTS）**	www.example.co.jp	未設定

△	**ソフトウェアのバージョン表示**	www.example.co.jp	generator: WordPress 5.8.1
△	**既知の脆弱性との照合**	www.example.co.jp	WordPress 5.8.1（generator）：該当する可能性がある公開の脆弱性 18件（うち CVSS 7.0 以上 6件。例：CVE-2022-21661（7.5）、CVE-2022-21664（7.4））
△	**DMARC レポートの集計**	example.co.jp	直近30日に受信側（google.com、Outlook.com など）が報告した自社名義のメール 4,210通のうち、認証に成功 3,980通（94.5%）
△	**認証に失敗した送信元**	example.co.jp	認証に失敗した送信元：203.0.113.25（逆引き：example-mailer.net）から 214通
△	**管理画面・リモート接続の入口**	vpn.example.co.jp	リモート接続・メールの入口と思われるホスト名（証明書の発行 2026-09-01、DNS 登録あり）

本レポートは自動診断により作成しています。

本レポートは、外部から確認できる範囲（公開されている DNS レコード、証明書の透明性ログ、Webサイトへの通常の HTTP・HTTPS の接続と古い暗号化方式を受け付けるかの確認）と、DMARC の集計レポート（rua に当社の宛先を加えて受信側のメールサービスから届いたもの、またはアップロードいただいたもの）のみを対象とした診断結果です。ポートスキャン、脆弱性を突く検査、ログインの試行は行っていません。「×」「△」がない場合でも、安全性を保証するものではありません。また、公的機関による認定や評価ではありません。

「SCS★3」欄は、経済産業省・IPA の SCS評価制度（★3）の要求事項のうち、本診断の結果が手がかりになりうる項目の番号です。IPA の自己評価等ガイド（SCS-410）と解説書（SCS-620）（2026-10-28 付）には、外部からの診断の結果を自己評価の証跡として使えるかの記載がありません。本レポートは★3の証跡・取得・要求事項への適合を示すものではありません。

既知の脆弱性との照合には、米国 NIST の脆弱性データベース（NVD）の公開データを使用しています。This product uses the NVD API but is not endorsed or certified by the NVD.

内容に関するご質問や配信停止のご希望は、見本ウェブ制作（架空）（support@vendor.example）までご連絡ください。