ELC SERVER HEALTH LAB ／ 高精度チェック（無料）

サーバー診断票 外から見える範囲の読み取り専用確認

株式会社ホシノ精機 御中

SERVER CHECK SHEET ／ 票番号 SC-2026-0000-SAMPLE-001 ／ 確認実施日 2026年9月12日 ／ お渡し日 2026年9月16日

SAMPLE ／ 見本

受診者	**株式会社ホシノ精機**（架空） 精密部品製造・従業員45名・大阪府
IT体制	専任のIT担当なし。総務2名が兼任し、外部の保守業者に随時依頼
対象	外から見える4か所（右表）。サーバーの中身・社内の機器は対象外
確認方法	インターネット側から「見える・応答する」ものだけを記録。侵入・負荷・設定変更は一切なし
担当	ELC SERVER HEALTH LAB 技術担当（30分のオンライン説明つき）

NDA締結日	2026年9月10日（秘密保持契約）
書面承諾日	2026年9月11日（確認作業への書面承諾）
確認実施日	2026年9月12日（単日・読み取り専用・約2時間）
お渡し日	2026年9月16日
次回のおすすめ	対策後の再確認（無料）／半年に1回の定期確認

総合判定

C ／A〜D

今すぐ手を打ちましょう

受発注データベースとECサイトの管理画面が、世界中の誰からでも届く場所にあります。

外から見えるものだけを確認した結果、8項目のうち**「危険」が2件・「注意」が3件**ありました。どちらの危険も、攻める側が特別な技術を必要としない「入口が開いている」状態です。ただし、暗号化・不要な入口・メールのなりすまし対策の3点は良好で、土台の設計は悪くありません。**まず2件の危険を閉じるだけで、判定はBに上がる見込み**です。

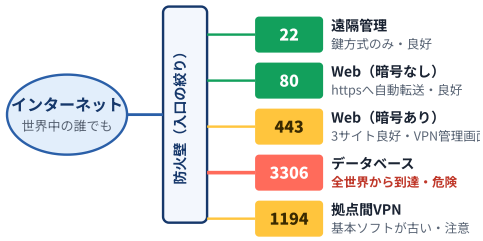
危険（今すぐ） 2件　注意（1か月以内） 3件　良好（維持） 3件

判定の目安　A：このまま維持　／　B：計画的に改善　／　**C：今すぐ手を打ちましょう（危険1件以上）**　／　D：営業に影響する事故が起きうる（危険3件以上）

01 8項目の判定一覧 SUMMARY OF 8 ITEMS

No	項目	判定	ひとことで言うと	優先度
①	データベースの入口（受発注ポータル）	危険	顧客・注文の保管庫の扉が、道路に面して開いている（203.0.113.21・3306番）	**最優先**
②	ECサイトの管理画面（WordPress）	危険	管理画面が全世界に公開され、パスワード当ての自動アクセスが実際に観測できる	**最優先**
③	ECサイトの版の古さ	注意	本体は2025年春の版。追加機能（プラグイン）に公開済みの弱点あり	高
④	拠点VPNルーター	注意	基本ソフトが2023年版のまま。管理画面がインターネット側から応答する	高
⑤	ログインの守り（ロック・二段階認証）	注意	失敗しても何度でも試せる。スマホ確認などの二段階認証なし	中
⑥	通信の暗号化（https）	良好	3サイトとも鍵マークつき。証明書は自動更新されている	維持
⑦	不要なサービスの露出	良好	外に開いている入口は5つだけで、用途不明のものはない	維持
⑧	メールのなりすまし対策	良好	送信元を証明する3つの設定（SPF・DKIM・DMARC）が入っている	維持

02 外から見えている入口 WHAT THE INTERNET CAN REACH



緑＝良好　黄＝注意　赤＝危険。数字は「入口の番号（ポート）」です。

8項目の内訳（3段階）

危険 2　注意 3　良好 3

■ ①データベースの入口　②ECの管理画面
■ ③ECの版の古さ　④VPNルーター　⑤ログインの守り
■ ⑥通信の暗号化　⑦不要な入口なし　⑧メール対策

危険を2件とも閉じると、この帯の赤が消えて判定Bになります。

入口	用途	見えた場所（文書用IP）	見えたもの	判定
22	遠隔管理（SSH）	203.0.113.20 / .21	鍵方式のみ受付。パスワードでの入室は拒否	良好
80	Web（暗号なし）	203.0.113.20 / .21 / .22	すべて暗号ありの入口へ自動で転送	良好
443	Web（暗号あり）	203.0.113.20 / .21 / .22 / .10	証明書は有効・自動更新。ただし.10はVPNルーターの管理画面が応答（④）	注意
3306	データベース	203.0.113.21（portal）	接続の呼びかけに応答。中には入っていない（①）	危険
1194	拠点間VPN	203.0.113.10（ルーター）	VPNの応答あり。基本ソフトは2023年版と推定（④）	注意

対象：shop.hoshino-seiki.example.jp（EC・WordPress＝.20）／portal.hoshino-seiki.example.jp（受発注ポータル・Laravel＝.21）／intra.hoshino-seiki.example.jp（社内ポータル＝.22）／拠点VPNルーター 203.0.113.10。IPは文書用アドレスに置き換えています。

この診断票の読み方　「危険」＝入口が開いていて、特別な技術がなくても狙える状態。「注意」＝すぐには入られないが、放置すると危険に変わる状態。「良好」＝今のまま維持すればよい状態。2ページ目に危険・注意の5件を「何が見えたか／放っておくと／何をすれば／誰がやるか／目安時間」の順で書いています。専門用語はできるだけ避け、必要なものは（　）内に添えました。

03 所見の詳細 — 危険2件・注意3件 FINDINGS IN PLAIN WORDS

各項目は「外から見えたこと」だけを根拠にしています。サーバーの中の設定やパスワードの強さは確認していないため、実際の危険度が上下する可能性があります。「誰がやるか」は、総務担当が手順どおりに進められるものを「自社でできる」、設定ミスが業務停止につながるものを「業者に頼む」としました。

① 危険 データベースの入口が、外から誰でも届く場所に開いている

受発注ポータル 203.0.113.21 ／ 入口 3306番

何が見えたか
受発注ポータルのサーバーで、データベース（顧客・注文・単価の保管庫）の入口がインターネット全体に向けて開いており、接続の呼びかけに「受け付けます」と応答しました。中に入る操作はしていないため、パスワードの強さは未確認です。本来この入口は、同じサーバーの中か社内からしか見えないのが普通です。

放っておくとどうなるか
保管庫の扉が道路に面している状態です。世界中の自動プログラムが毎日パスワードを試し、既知の欠陥を探しに来ます。突破されると**取引先の注文・単価・連絡先が丸ごと持ち出され**、取引先への通知と謝罪、取引停止、損害賠償が現実になります。製造業では「見積単価の流出」が最も痛い損失になりがちです。

何をすればよいか
①この入口を外から閉じ、同じサーバー内（またはVPN内）からだけ受け付ける設定にする。②データベースのパスワードを新しいものに変える。③これまで誰が接続してきたかの記録を確認し、不審な接続があれば別途ご相談ください。閉じても受発注ポータルの動作は変わりません。

誰がやるか・目安
業者に頼む
クラウド事業者の管理画面の「ファイアウォール」で閉じられる場合は、自社でも可能です。
目安 **1〜2時間**
業務停止なし

② 危険 ECサイトの管理画面が全世界に公開、パスワード当てが観測できる

shop.hoshino-seiki.example.jp ／ /wp-login.php・xmlrpc.php

何が見えたか
ECサイト（WordPress）の管理画面の入口（/wp-login.php）が誰でも開ける状態です。ログイン失敗時の応答の違いから「そのユーザー名が存在するか」を外から判別でき、管理者名も推測できました。さらに自動操作用の入口（xmlrpc.php）が有効で、**1回の通信で数百通りのパスワードを試せる仕組み**が使える状態です。確認当日も海外からの試行が続いていました。

放っておくとどうなるか
今この瞬間も、自動プログラムが24時間パスワードを試し続けています。突破されると商品ページの改ざん、偽の決済ページへの誘導、顧客情報の抜き取りが起こり、**サイトの停止と信用の失墜**につながります。復旧には通常数日、加えてカード会社や顧客への説明が必要になります。

何をすればよいか
①管理画面を社内・VPNからだけ開けるようにする（接続元の制限）。②自動操作用の入口（xmlrpc.php）を止める。③管理者全員にスマホ確認（二段階認証）を入れる。④ログイン失敗の回数制限を入れる。①〜④はいずれも無料の追加機能で対応できます。

誰がやるか・目安
自社でできる（一部業者）
②〜④は追加機能の導入と設定で自社対応可。①の接続元制限は保守業者に依頼を推奨。
目安 **半日**
停止なし・要動作確認

③ 注意 ECサイトの本体と追加機能（プラグイン）が古い

shop.hoshino-seiki.example.jp ／ WordPress

何が見えたか
外から見える版情報から、WordPress本体は「2025年春の版」、追加機能のうち3つは1年以上更新されていない版と推定されます。そのうち2つには**公開済みの弱点**（直し方も公開されている欠陥）があります。デザインテーマも同時期の版です。

放っておくとどうなるか
公開済みの弱点は「攻め方の手順書が出回っている」状態です。手順書どおりに自動で狙われるため、技術のない相手にも突破されます。②の管理画面公開と組み合わさると、突破は時間の問題になります。

何をすればよいか
①サイト全体のバックアップを取る。②本体・追加機能・テーマを最新版に更新する。③使っていない追加機能は無効化ではなく削除する。④以後は自動更新を有効にし、月1回は管理画面の「更新」欄を見る。

誰がやるか・目安
自社でできる
更新後に「商品検索・カート・決済」の3か所を必ず自分で操作して確認します。
目安 **2〜3時間**
確認作業を含む

④ 注意 拠点VPNルーターの基本ソフトが2023年版のまま、管理画面が外から応答する

拠点VPNルーター 203.0.113.10 ／ 入口 443・1194番

何が見えたか
拠点VPNルーターの管理画面（設定を変える画面）がインターネット側の443番で応答し、応答内容から2023年に配布された基本ソフト（ファームウェア）と推定されます。その後に公開された修正が当たっていない可能性が高い状態です。VPN自体（1194番）は正常に応答しています。

放っておくとどうなるか
VPNルーターは「社内網への正面玄関」です。ここが破られると社内ポータルや共有フォルダまで一気に到達されます。2024年以降、**修正されていないルーター類の弱点を狙う侵入が国内の中小企業でも多発**しており、ランサムウェア被害の入口になった例が目立ちます。

何をすればよいか
①管理画面を社内側からだけ開ける設定に変える（外からは応答しないように）。②基本ソフトを最新版に更新する。③管理者パスワードを新しいものに変える。④機器の保守期限（メーカーの修正提供期間）を確認し、切れていれば買い替えを検討する。

誰がやるか・目安
業者に頼む
機器メーカーの保守窓口でも対応可。再起動を伴うため業務時間外に実施します。
目安 **1時間**
VPNが5分ほど止まる

⑤ 注意 ログイン失敗が何度でも試せる（ロックなし・二段階認証なし）

受発注ポータル・社内ポータル・ECの管理画面

何が見えたか
3つのログイン画面すべてで、失敗を続けても一時停止（ロック）や待ち時間が入らず、スマホ確認などの二段階認証もありません。※実際の突破は試していません。誤ったパスワードを数回入力し、応答が変わらないことだけを確認しました。

放っておくとどうなるか
従業員や取引先の1人でも「他所と同じパスワード」を使っていれば、すでに流出している組み合わせ表で入られます。受発注ポータルは注文の改ざん・取引先情報の閲覧に直結し、**被害に気づくのは取引先からの問い合わせが最初**になりがちです。

何をすればよいか
①失敗5回で15分ロックする設定にする。②管理者・経理担当は二段階認証を必須にする。③全員に「他所と同じパスワードを使わない」よう周知し、次回ログイン時に変更を求める。④退職者・取引終了先のアカウントを棚卸しして止める。

誰がやるか・目安
自社でできる（一部業者）
③④は総務で完了できます。受発注ポータルのロック設定は開発した業者に依頼します。
目安 **半日〜1日**
周知期間を別途

補足：順番の考え方　①と②は「入口を閉じる」だけで効果が出るため、費用も時間も小さい割に効き目が最大です。③④は「古いものを新しくする」作業で、バックアップと業務時間外の実施が必要です。⑤は仕組みの追加に加えて社内周知が要るため、1か月の猶予をみています。5件すべてを終えた時点で、判定はA〜Bに達する見込みです。

04 良好だった3項目と維持のコツ WHAT IS WORKING — KEEP IT

良好 ⑥ 通信の暗号化（https）

3つのサイトすべてで通信が暗号化され、ブラウザに鍵マークが出ます。証明書（暗号化の身分証）は自動更新の仕組みが入っており、次回の更新予定は2026年11月です。暗号化なしの入口（80番）に来た通信も、自動で暗号ありへ転送されていました。

維持のコツ

証明書の期限切れ通知メールを総務の共有アドレスでも受け取る設定にし、年1回は3サイトの鍵マークを目視で確認します。期限切れは「サイトが警告画面になる」形で突然表面化します。

良好 ⑦ 不要なサービスは外に出ていない

外に開いている入口は 22・80・443・3306・1194 の5つだけで、用途がわからないものや、テスト用に開けたまま忘れられた入口はありませんでした。中小企業では「昔の業者が開けた入口が残っている」例が多く、この点は評価できます。

維持のコツ

新しいソフトや機器を入れたときは「外から見える入口が増えていないか」を業者に一言確認します。①の3306番を閉じれば、残る入口は4つになります。

良好 ⑧ メールのなりすまし対策

「hoshino-seiki.example.jp を名乗るメールは本物か」を受け取り側が確かめられる3つの設定（SPF・DKIM・DMARC）が入っています。取引先に御社を装った請求書メールが届く事故を防ぐ土台です。ただしDMARCは「様子見（監視のみ）」の段階でした。

維持のコツ

新しいメール配信サービス（一斉送信など）を使い始めるときは、先に設定へ追加します。半年ほど監視結果を見て、偽物を「隔離」する段階へ進めるのがおすすめです。

05 やることの順番 ACTION PLAN — 3 STEPS

今すぐ　1週間以内

- ① データベースの入口（3306番）を外から閉じる
- ② ECの管理画面を社内・VPNからのみに制限し、自動操作用の入口を止める
- ④ VPNルーターの管理画面を外から閉じる（更新は次段階）
- データベース・ルーター・EC管理者のパスワードを新しくする
- ECサイトのバックアップを取り、復元できるか確かめる

ここまでで「危険」2件が消え、判定はBに上がる見込み

1か月以内　計画して実施

- ③ WordPress本体・追加機能・テーマを更新し、不要な追加機能を削除
- ④ VPNルーターの基本ソフトを最新版へ（業務時間外）
- ⑤ 失敗5回でロック、管理者に二段階認証を導入
- ⑤ 全員のパスワード変更と使い回し禁止の周知、退職者アカウントの停止
- 対策後の再確認（無料）を申し込む

「注意」3件が消え、判定はAに達する見込み

3か月以内　仕組みにする

- ⑧ DMARCを「様子見」から「隔離」へ進める
- 月1回の点検チェックリスト（更新・バックアップ・入口・アカウント）を総務の定例に組み込む
- 「ソフト・機器の更新は月内に当てる」ルールを保守業者と決める
- 受発注ポータルのアカウント棚卸しを取引先ごとに実施
- 半年に1回の定期確認（無料）を予定に入れる

担当者が替わっても回る「習慣」にする

06 この診断でやらなかったこと OUT OF SCOPE

やらなかったこと	内容	それでも知りたい場合
侵入テスト	実際に突破を試す行為（パスワード当て・弱点を突く操作）は行っていません。「入口が開いている」までの確認です。	有料レポート（1か月コース）で別途合意のうえ実施可
負荷試験	大量のアクセスを送ってサイトが耐えるかを試す行為は行っていません。営業中のサイトに影響を与えないためです。	有料レポート（1か月コース）で時間帯を決めて実施可
設定変更	サーバー・ルーター・サイトの設定は一切変えていません。本票の内容は、御社が対策を実施するまで変わりません。	対策の実施は保守業者、または当社の伴走支援で
サーバー内部の確認	記録（ログ）・設定ファイル・バックアップの実態・パスワードの強さ・社内ネットワークは見ていません。外からの単日スナップショットです。	有料レポート（1週間コース以上）で内部を確認

07 次の段階 — サーバーに実際に入って調べる（有料） NEXT STEP

1週間コース　10,000円（税別）

- 主要サーバー3台（EC・受発注・社内）の中に入り、設定・更新状況・バックアップの実態・記録（ログ）を読み取り専用で確認
- 本票の①〜⑤について「実際にどこまで入られていたか」の痕跡を確認
- 成果物：サーバー健康診断レポート（8ページ・当社SHL形式）＋オンライン説明60分

1か月コース　100,000円（税別）

- 1週間コースの内容に加え、1か月間の観測（アクセス・エラー・更新）と改善作業の伴走
- 合意のうえで侵入テスト・負荷試験を時間帯を決めて実施し、対策後に再確認
- 成果物：健康診断レポート＋月次運用分析レポート＋点検チェックリスト（御社仕様）

※ どちらも読み取り専用が原則で、設定変更は御社の書面承諾がある項目のみ行います。無料の高精度チェックだけで終えていただいても構いません。対策後の再確認（無料）はこの票の番号でお申し込みください。

08 免責・本書の性質 DISCLAIMER

1. **外から見える範囲の単日スナップショットです。** 2026年9月12日時点でインターネット側から観測できたものだけを記録しており、翌日以降の変化や、内部にある問題は反映されません。
2. **サーバー内部・社内ネットワーク・実際の突破可否は対象外です。** 「危険」は入口が開いていることを示し、侵入された事実を意味しません。逆に「良好」は、内部に問題がないことを保証するものではありません。
3. **本票による判断・対策の実施は受診者の責任で行ってください。** 当社は本票の記載を根拠に生じた損害について、故意または重過失がある場合を除き責任を負いません。対策の実施前には必ずバックアップを取ってください。
4. **本書は様式サンプルです。** 受診者「株式会社ホシノ精機」は架空の企業であり、記載のホスト名・IP（文書用アドレス 203.0.113.x）・所見・判定はすべて例示です。実在の企業・団体・システムとは関係ありません。

発 行

株式会社Game　ELC SERVER HEALTH LAB 技術担当　／　票番号 SC-2026-0000-SAMPLE-001　／　お渡し日 2026年9月16日

取 扱 い

秘密保持契約（2026年9月10日締結）に基づく秘密情報です。受診者の社内および受診者が指定する保守業者以外への提供はお控えください。