ELC SERVER HEALTH LAB

サーバー健康診断レポート

INFRASTRUCTURE HEALTH ASSESSMENT REPORT

SAMPLE ／ 見本

株式会社ホシノ精機 御中

全 6 ホスト横断・読み取り専用精査 ／ 報告書番号 SHL-2026-0000-SAMPLE-001 ／ 検査実施日 2026年9月2日 ／ 報告日 2026年9月9日

総合健康スコア
62 / 100 点
判定 C
要注意 ― 経過観察および生活習慣（運用習慣）の是正

侵害の痕跡
0 件
Web シェル・不正ユーザー・マイニング・不審な永続化はいずれも全 6 ホストで検出なし。

要是正の所見
24 件
HIGH 3 件・MEDIUM 12 件・LOW 9 件。HIGH は全て 2 週間以内に着手可能。

業界内順位
7 位 / 12社
同業種・同規模の母集団中央値 63.5。偏差値 49.2 で「平均のやや下」。

是正後の見込み
86 点 / A
処方箋 Rx-01〜10（総工数 約 43 時間）を 90 日で完遂した場合の到達見込み。

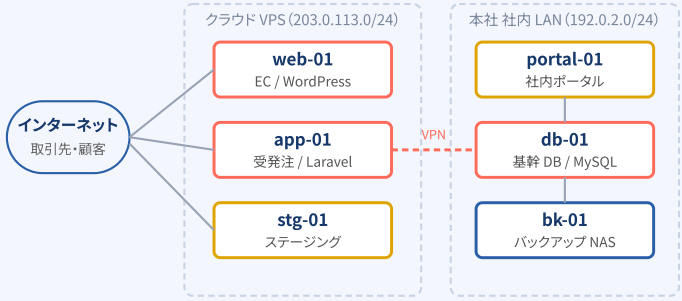
01 / SUBJECT PROFILE

受診者情報

診断対象組織の基礎情報。事業構造と IT 体制は、そのまま「守るべき資産の広がり」と「守る側の人手」に対応します。

受診者	**株式会社ホシノ精機**（架空）
業種	精密部品製造（切削・研削加工／自動車・産業機器向け）
所在地	大阪府（本社工場 1 拠点）
従業員	45 名（製造 32・営業 6・総務 4・その他 3）
IT 体制	専任担当なし。総務 2 名が兼任、外部の保守業者に随時依頼
主要システム	基幹（生産管理）／EC サイト／受発注ポータル／社内ポータル
診断対象	サーバー 6 ホスト（クラウド VPS 3・社内サーバー 3）＋参考 1（拠点 VPN ルーター）
検査実施日	2026年9月2日（単日・読み取り専用）
報告日	2026年9月9日
次回推奨	2026年12月上旬（四半期定期・是正後の再判定）

システム構成の概観



枠線の色は本診断でのホスト評点（赤 D・黄 C・青 B）。IP は文書用アドレスを使用しています。

診断上の含意。45 名の組織が、顧客の個人情報・取引先の単価情報・生産計画を扱う本番系 6 ホストを、専任担当なしで運用しています。1 人あたりの受け持ちが広く、注意力に依存した対策は必ず摩耗します。したがって本診断の処方は、「人が気をつける」ではなく**「構成で担保する」**方向に寄せています。

所見の要約（医師所見に相当）

急性所見なし。侵入・改ざん・情報持ち出しの痕跡は 6 ホスト全てで検出されませんでした。今すぐ止血が必要な状態ではありません。

慢性所見あり。秘密情報の保全（48点／D）と監査・追跡性（50点／D）が基準を大きく下回ります。いずれも「今すぐ被害が出る」ものではなく、他の攻撃が 1 段成功したときに被害を最大化する因子です。

入口の開きすぎ。EC サイトの管理画面が全世界に公開され、基幹 DB が VPN 越しに到達可能です。攻撃者が「試せる回数」が多すぎる状態で、総当たりや既知脆弱性の自動探索に晒されています。

検査体制そのものの不足。ログイン履歴が 7 日で消え、改ざん検知が未導入です。現状は「異常があっても気づけない」ため、スコア以上に実質リスクは高いと評価します。

直ちに着手すべき HIGH 所見（3 件）

ID	所見	ホスト	処方
A-02	EC 管理画面が全世界公開・MFA なし	web-01	Rx-01
P-01	退職者が使った共通 ID「admin」が有効	app-01 / portal-01	Rx-02
A-01	基幹 DB が VPN 越しに到達可能（*:3306）	db-01	Rx-03

3 件の合計工数 9 時間。いずれも設定変更のみで、サービス停止を伴いません。

本書の構成

※ 本書は報告様式のサンプルです。受診者「株式会社ホシノ精機」は架空の企業であり、記載の所見・数値・ベンチマーク母集団は様式提示のための例示値です（第 8 章 脚注参照）。計測は全て読み取り専用で行い、設定変更・サービス停止を伴う操作は一切行いません。秘密の値そのものは本書に記載せず、存在と所在のみを記します。

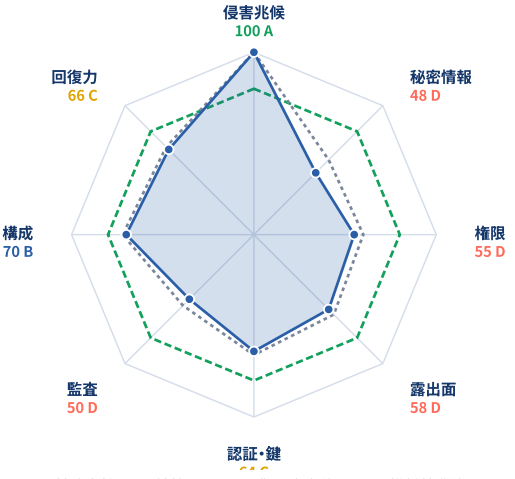
02 / OVERALL FINDINGS

総合所見

総合スコアは 8 カテゴリの加重平均です。健康診断と同じく、「病気があるか」（侵害の痕跡）と「病気になりやすい生活習慣か」（設定・運用の逸脱）を分けて評価しています。

侵害の痕跡	総合スコア	要是正の所見	是正後の見込み
0 件	**62** / 100	**24** 件	**86** 点
Web シェル・不正ユーザー・マイニング・不審な永続化・素性不明の鍵、いずれも全ホストで検出なし。	判定 C（要注意）。前回推計 58 から +4。母集団中央値 63.5 をわずかに下回る。	うち HIGH 3 件（管理画面公開・共通 ID・DB 露出）。CRITICAL は 0 件。	処方箋 Rx-01〜10 を 90 日で完遂した場合の到達見込み（判定 A 圏）。

カテゴリ別プロファイル



所見の要約（医師所見に相当）

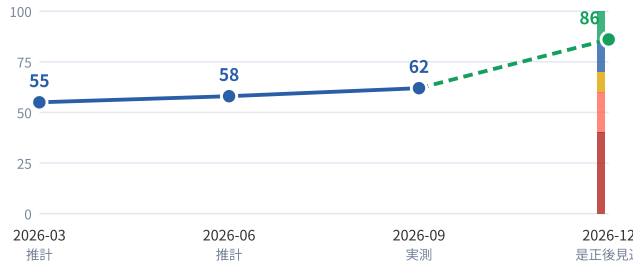
急性所見なし。侵入・改ざん・情報持ち出しの痕跡は 6 ホスト全てで検出されませんでした。侵害兆候カテゴリは満点で、これは「今は病気ではない」ことを意味します。

慢性所見あり。秘密情報の保全（48点／D）・監査・追跡性（50点／D）・権限（55点／D）・露出面（58点／D）の 4 カテゴリが D 判定です。健康診断でいえば血圧・血糖・脂質が同時に基準を外れている状態で、単独では発症しないが、合併すると重症化する構造です。

「入口」と「気づく力」の両方が弱い。露出面（管理画面の全公開・DB の到達可能性）と監査（ログ 7 日・改ざん検知なし）が同時に低いため、「侵入されやすく、かつ侵入に気づけない」組み合わせになっています。本診断で最も重く見る点です。

基礎体力はある。OS の自動更新・日次バックアップ・TLS は適正で、構成（70点／B）は母集団並みです。処方の大半は「新しい仕組みを入れる」ではなく「今ある設定を締める」もので、総工数 約 43 時間で到達できます。

総合スコアの推移



2026-03・06 は今回の検査結果と当時の変更履歴から遡って推計した値。12 月は Rx 完遂時の見込み（破線）。右端の色帯は判定グレード。

深刻度別 所見件数（全 24 件）

HIGH 3	MEDIUM 12	LOW 9

HIGH	**3 件** — CMS 管理画面の全公開（A-02）／退職者が使った共通 ID（P-01）／基幹 DB の外部到達（A-01）。いずれも侵害シナリオの起点。
MEDIUM	**12 件** — 設定ファイル権限・本番データ残置・パスワード使い回し・ログ保持・改ざん検知・VPN 機器更新など、連鎖時に被害を拡大する因子。
LOW	**9 件** — ハードニング項目。次回診断までの是正で足りる。

CRITICAL（侵害の痕跡、実鍵の公開露出）は 0 件。

カテゴリ	前回（2026-06 推計）	今回	差	変化の主因	是正後見込	主な処方
侵害兆候	100 A	100 A	±0	変化なし。IoC 6 観点すべて陰性	100 A	–
秘密情報の保全	44 D	48 D	+4	本番ダンプ 1 件が増加（2026-07）。設定ファイル権限は据え置き	84 B	Rx-05 / Rx-08
権限・アクセス制御	52 D	55 D	+3	退職者 ID 1 件削除で微増。共通 ID は残存	86 A	Rx-02 / Rx-03
ネットワーク露出面	58 D	58 D	±0	変化なし。管理画面公開・DB 待受は当初から	88 A	Rx-01 / Rx-03 / Rx-04
認証・鍵管理	60 C	64 C	+4	SSH 鍵を 1 名分追加発行で改善。使い回しは残存	86 A	Rx-06 / Rx-01
監査・追跡性	50 D	50 D	±0	変化なし。ログ保持は既定値のまま	80 B	Rx-07
構成・更新管理	66 C	70 B	+4	OS 自動更新の有効化で改善。プラグインは停滞	84 B	Rx-04 / Rx-10
回復力・保全	62 C	66 C	+4	日次バックアップの世代保持を導入し改善	82 B	Rx-09

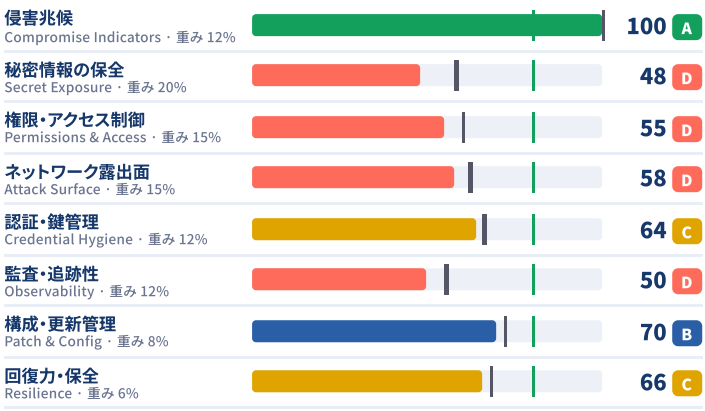
検査項目	対象ホスト	人手照合	検査方式
36 項目	**6** ＋参考 1	**3** 件	**読取専用**
8 カテゴリ・10 観点	VPS 3・社内 3・網機器 1	H-01〜03（第 8 章付記）	設定変更・再起動なし

03 / CATEGORY SCORES

カテゴリ別スコアと算定方法

8 カテゴリそれぞれの点数・判定と、総合点への重み。帯の色は判定グレード（A 緑 → E 赤）、黒線は同業種中央値、緑の破線は推奨基準値 80 を示します。

カテゴリ別スコアと判定



黒線＝同業種 中央値（12 社）／緑破線＝推奨基準値 80。カテゴリ点は各検査項目の判定分布（A=100・B=80・C=60・D=40・E=0）を重要度で加重して算出。

カテゴリ別 点数を下げている主因

カテゴリ	最も点数を下げた項目	判定	影響
侵害兆候	（逸脱なし）	—	—
秘密情報	S-01 .env / wp-config.php が 644	D	−28
権限	P-01 共通 ID「admin」（退職者利用歴）	D	−22
露出面	A-02 CMS 管理画面の全世界公開	D	−20
認証・鍵	K-02 管理者パスワードの使い回し	D	−18
監査	O-02 ログの外部集約なし	D	−20
構成	C-03 VPN ルーターの FW 更新停止	D	−16
回復力	B-03 復旧テスト未実施	D	−18

「影響」は当該項目が A 判定だった場合に回復するカテゴリ点の概算。

スコアの算定方法

総合スコアは 8 カテゴリの加重平均です。重みは「そこが破られたときに、被害がどこまで広がるか」で決めており、検査項目の数ではありません。

カテゴリ	重み	重み付けの根拠
侵害兆候	12%	実害の有無。検出時は他カテゴリに関係なく E 判定へ直行する「失格条項」として扱う
秘密情報の保全	20%	漏れた瞬間に金銭被害・個人情報事故へ直結する。最大の重み
権限・アクセス制御	15%	単独では被害にならないが、他の攻撃の成功率と被害範囲を決める増幅因子
ネットワーク露出面	15%	攻撃者が最初に触れる面。露出が多いほど「試される回数」が増える
認証・鍵管理	12%	横移動の可否を決める。1 つの資格情報が複数ホストに通ると重みが効く
監査・追跡性	12%	被害を止めるまでの時間を決める。予防ではなく損害の上限を決める要素
構成・更新管理	8%	土台の健全性。既知の脆弱性を放置しないための基礎体力
回復力・保全	6%	低くても即座の危険はないが、復旧局面で被害額を左右する

計算例：100×0.12 + 48×0.20 + 55×0.15 + 58×0.15 + 64×0.12 + 50×0.12 + 70×0.08 + 66×0.06 = 61.8 → **62 点**

判定グレードの読み方

A	85〜100	良好 — 現行の運用を維持する。
B	70〜84	おおむね良好 — 軽微な逸脱。次回診断までに是正すれば足りる。
C	60〜69	要注意 — 実害には至っていないが、条件が揃えば侵害の起点になりうる。期限を切って是正。
D	40〜59	要改善 — 既知の攻撃経路が成立する状態。90 日以内に是正。
E	0〜39	要精密検査 — 直ちに対処。侵害の痕跡が 1 件でもあれば総合点に関係なく E。

カテゴリ × 深刻度 所見件数

カテゴリ	HIGH	MEDIUM	LOW	計	主な所見
IOC 侵害兆候	·	·	·	·	—（全項目 A）
SEC 秘密情報の保全	·	2	2	4	設定ファイル 644／本番ダンプ残置
PRM 権限・アクセス制御	1	2	1	4	共通 ID・退職者 ID・root@%
ATK ネットワーク露出面	2	1	2	5	管理画面全公開／DB 待受／SSH パスワード認証
KEY 認証・鍵管理	·	1	2	3	パスワード使い回し／MFA 未導入
OBS 監査・追跡性	·	3	1	4	ログ 7 日／外部集約なし／改ざん検知なし
CFG 構成・更新管理	·	2	·	2	プラグイン未更新／VPN 機器 FW 停止
BCP 回復力・保全	·	1	1	2	復旧テスト未実施／同一拠点保管
合計	3	12	9	24	

健康診断のメタファーで読む

侵害兆候＝「病気があるか」。今回は陰性。ただし検査は単日のスナップショットで、ログが 7 日しか無い環境では過去の侵入を検出する手段がありません（第 8 章）。

D 判定 4 カテゴリ＝「生活習慣病の合併」。秘密情報・権限・露出面・監査はそれぞれ単独では発症しませんが、露出面から入られ、権限で広がり、秘密情報で金銭被害になり、監査不在で長期化する — という順序で合併します（第 5 章）。

処方箋＝「食事・運動より先に、薬で数値を下げる」。Rx-01〜04 は設定変更だけで露出面と権限を 2 週間で引き上げます。運用習慣の改善（Rx-09・10）はその後で構いません。

再診断＝「3 ヶ月後の再検査」。是正の効果は、同じ 36 項目を同じ基準で測り直して初めて確定します。推計値ではなく実測値の推移を残すことが、取引先監査への回答にもそのまま使えます。

04 / SCOPE & BENCHMARK

診断対象ホストと同業種ベンチマーク

対象は、クラウド VPS 3 台と本社設置の社内サーバー 3 台の計 6 ホスト。機密度は、そのホストが扱う情報の性質（個人情報・取引先の単価・生産計画）で判定しています。

ホスト	IP（文書用）	区分	基盤	用途	公開範囲	機密度	評点	主要所見
web-01	203.0.113.10	本番	クラウド VPS	EC サイト（WordPress）	HTTPS 全公開	高	54 D	wp-login.php が全世界公開・MFA なし。wp-config.php が 644。プラグイン 6 件が 90 日超未更新。
app-01	203.0.113.11	本番	クラウド VPS	受発注ポータル（Laravel）	HTTPS 公開（取引先 ID）	高	58 D	.env が 644。共通 ID「admin」に退職者の利用歴。開発用 Node が 0.0.0.0:3000 で待受。
db-01	192.0.2.20	本番	社内サーバー	基幹システム DB（生産管理・MySQL）	社内 LAN（VPN 経由で到達可）	高	52 D	MySQL が *:3306 で待受。root@% が有効。DB パスワードが bash_history に平文 3 件。
portal-01	192.0.2.30	本番	社内サーバー	社内ポータル（グループウェア）	社内 LAN	中	63 C	退職者アカウント 3 件残存（最終ログイン 2026-02）。ログイン履歴保持 7 日。
stg-01	203.0.113.12	検証	クラウド VPS	ステージング（EC・ポータル検証）	Basic 認証	中	61 C	本番 DB のダンプ 2 件が残置。noindex 未適用。SSH パスワード認証が有効。
bk-01	192.0.2.40	保全	社内 NAS	バックアップ保管（日次）	社内 LAN	高	72 B	日次取得は良好。同一拠点・同一 LAN 内の保管のみで、復旧テストは未実施。
（参考）拠点 VPN ルーター	203.0.113.1	網機器	本社設置	拠点間 VPN／外部からの保守接続	WAN 側管理画面 公開	—	対象外	ファームウェアが 2023 年版で停止。SSH 対象外のため評点なし。所見 C-03 として計上。

ホスト × カテゴリ 判定マップ

ホスト	侵害兆候	秘密情報	権限	露出面	認証・鍵	監査	構成	回復力	評点
web-01	A	D	C	D	D	D	C	C	54
app-01	A	D	D	C	C	D	B	C	58
db-01	A	C	D	D	C	D	B	C	52
portal-01	A	B	D	B	C	D	B	C	63
stg-01	A	D	C	C	C	D	B	B	61
bk-01	A	C	B	A	B	C	B	C	72

縦に赤が並ぶ列＝全ホスト共通の弱点（監査・秘密情報）。横に赤が並ぶ行＝そのホスト固有の問題（web-01・db-01）。処方はまず「列」を潰す方が費用対効果が高い。

読み取り

本番 3 ホストが揃って D。web-01（54）・app-01（58）・db-01（52）は顧客・取引先データを直接扱う本番系で、機密度「高」にもかかわらず評点が最も低い組み合わせです。

bk-01 は良好だが「同じ部屋」にある。日次バックアップは取れていますが、同一拠点・同一 LAN のため、ランサムウェアや火災・水害で本体と同時に失われます。

stg-01 は本番のコピーを持っている。検証環境として守りが薄い一方で、本番 DB のダンプが残置されており、実質的に本番と同じ機密等級で扱う必要があります。

同業種ベンチマークとランキング（母集団 12 社）

同規模・同業態（製造業、従業員 150 名以下、EC または取引先ポータルを自社運用）の 12 社を母集団として相対評価しました。絶対点だけでは「これで十分なのか」が判断できないため、同じ条件の会社と比べて、どこが強く・どこが弱いかを示します。

#	社名	業態・規模	スコア	判定
1	A社 ★	金属加工・120名	88	A
2	B社 ★	電子部品・85名	81	B
3	C社	樹脂成形・60名	76	B
4	D社	機械部品・38名	72	B
5	E社 ★	食品機械・52名	69	C
6	F社	精密板金・30名	65	C
7	**株式会社ホシノ精機**	**精密部品・45名**	62	C
8	G社	治具製作・22名	58	D
9	H社	ばね製造・41名	54	D
10	I社	鋳造・33名	49	D
11	J社	工具製造・18名	45	D
12	K社	部品加工・25名	38	E

★ = ISMS / P マーク取得済（A 社・B 社・E 社）。母集団はいずれも匿名化されたサンプル値です。受診者は網掛けの行。

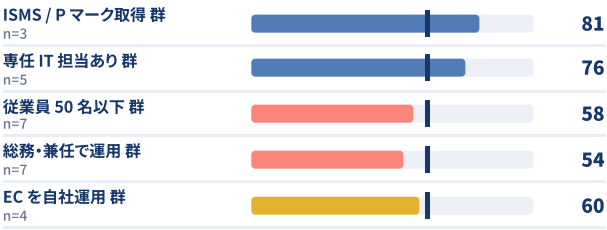
順位
7 / 12社
上位 58.3%（パーセンタイル 41.7）

偏差値
49.2
母集団平均 63.1 / 標準偏差 14.4

母集団比 優位
1 / 8
侵害兆候で中央値と同点。構成・回復力はほぼ並び

母集団比 劣位
5 / 8
秘密情報 −10／権限 −5／露出面 −4／監査 −5／認証 −2

セグメント別 中央値との比較



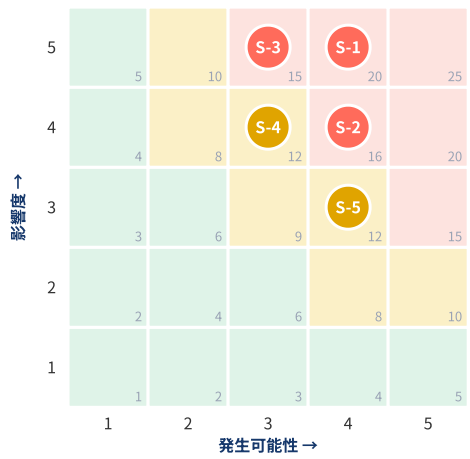
紺の縦線＝受診者 62 点。「総務・兼任で運用」群（中央値 54）の中では上位ですが、「専任 IT 担当あり」群とは 14 点の差。差の大半は監査と秘密情報の 2 カテゴリで生じています。

05 / THREAT SCENARIOS

予測される侵害シナリオ

検出された所見を単独の指摘としてではなく、「実際に攻撃者がどう繋げるか」という連鎖として提示します。個々は軽微に見える所見でも、繋がった瞬間に致命傷になる ― その筋道を可視化するのが本章の目的です。

リスクマトリクス（発生可能性 × 影響度）



ID	シナリオ	可能性	影響	リスク値	起点となる所見
S-1	WordPress 管理画面への総当たり → EC 注文データの流出 対象 web-01	4	5	20	A-02 / K-02 / S-01
S-2	退職者が使っていた共通アカウントの残存 → 受発注ポータルへの不正ログイン 対象 app-01 / portal-01	4	4	16	P-01 / P-02 / O-01
S-3	外部から到達可能な基幹 DB への直接侵入 → 生産・受注データ全件流出 対象 db-01	3	5	15	A-01 / P-03 / S-04
S-4	更新停止の VPN 機器の既知脆弱性 → 社内 LAN への侵入 対象 拠点 VPN ルーター → portal-01 / db-01	3	4	12	C-03 / O-02
S-5	ログ不在による侵害の長期滞留 対象 全ホスト横断	4	3	12	O-01 / O-02 / O-03

S-1 は仮定ではありません。WordPress 管理画面への総当たりは、公開直後から自動化ツールによって継続的に行われる「常態」です。本診断で web-01 の管理画面が無制限に公開され、かつ管理者パスワードが 3 ホストで共通であることを確認した事実が、S-1 の発生可能性を「高」と置く根拠です。

S-1 WordPress 管理画面への総当たり → EC 注文データの流出

対象 **web-01**　発生可能性 **高**　影響度 **極高**　検知容易性 **低**　**リスク値 20/25**

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5
wp-login.php が全世界公開・MFA なし・xmlrpc.php 有効。辞書攻撃が自動化ツールから継続的に到達する	管理者パスワードが 3 ホストで共通（K-02）。1 回の成功で管理者権限を取得	プラグイン改変またはファイルマネージャ経由で Web シェルを設置	wp-config.php（644）から DB 接続情報を読み、注文・顧客テーブルを全件取得	アクセスログ保持 14 日のため、発覚時には初回侵入の記録が消失

なぜこの経路が成立するのか
「管理画面の URL を知られていない」は防御にならない。WordPress の管理画面は URL が固定で、常時スキャンの対象になっている。

予兆として現れるもの
wp-login.php への深夜帯の連続 POST、見覚えのない管理者ユーザー、プラグイン一覧の変化。

想定損失（試算）
個人情報 約 8,000 件の漏えい通知・対応費 300〜800 万円／EC 停止による機会損失

紐づく予防策
Rx-01　Rx-05　Rx-07

S-2 退職者が使っていた共通アカウントの残存 → 受発注ポータルへの不正ログイン

対象 **app-01 / portal-01**　発生可能性 **高**　影響度 **高**　検知容易性 **低**　**リスク値 16/25**

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5
退職者 3 名が在職中に使っていた共通 ID「admin」のパスワードが、退職後も変更されていない	その資格情報が私物 PC のブラウザやメモに残存、または他サービスの流出リストと一致	受発注ポータルへ正規ログインとして到達。ログ上は「admin」の通常操作と区別できない	取引先の単価・発注数量・図面データを閲覧し、持ち出す	ログイン履歴が 7 日で消えるため、時期の特定が不能

なぜこの経路が成立するのか
共通アカウントは「誰が使ったか」が消える設計。退職手続きに「共通 ID のパスワード変更」が含まれていない限り、退職者は永続的に入れる。

予兆として現れるもの
業務時間外の admin ログイン、普段見ない取引先データへの連続アクセス。

想定損失（試算）
取引先との信頼失墜・見積情報の競合流出／契約上の損害賠償（金額化困難）

紐づく予防策
Rx-02　Rx-06　Rx-07

S-3 外部から到達可能な基幹 DB への直接侵入 → 生産・受注データ全件流出

対象 **db-01**　発生可能性 **中**　影響度 **極高**　検知容易性 **中**　**リスク値 15/25**

STEP 1	STEP 2	STEP 3	STEP 4
db-01 の MySQL が全インターフェース待受（*:3306）。VPN 接続端末なら誰でも到達できる	root@% が有効。VPN 内のいずれか 1 台（S-4 経由を含む）から接続できれば全権限	パスワードは bash_history に平文で残存（S-04）。app-01 侵害時にそのまま流用可能	生産計画・原価・取引先マスタを一括ダンプ、または改ざん

なぜこの経路が成立するのか
「社内 LAN の中だから安全」は、VPN 機器が社内 PC 1 台でも突破されると崩れる前提。DB 自身が接続元を制限していないことが根本原因。

予兆として現れるもの
業務時間外の 3306 接続、通常より大きい SELECT／ダンプ、不明ホストからの接続。

想定損失（試算）
基幹停止・再構築 500〜1,500 万円／取引先情報の流出責任

紐づく予防策
Rx-03　Rx-05　Rx-07

S-4 更新停止の VPN 機器の既知脆弱性 → 社内 LAN への侵入

対象 **拠点 VPN ルーター → portal-01 / db-01**　発生可能性 **中**　影響度 **高**　検知容易性 **中**　**リスク値 12/25**

STEP 1	STEP 2	STEP 3	STEP 4
拠点ルーターのファームウェアが 2023 年版で停止。以降に公表された認証迂回の脆弱性が未修正	インターネット側から管理画面が到達可能（HTTPS:443）	脆弱性を突いて VPN の資格情報を取得、または管理者権限で設定を変更	社内 LAN へ VPN 接続し、portal-01 / db-01 へ内部からアクセス

なぜこの経路が成立するのか
ネットワーク機器は「設置したら終わり」になりやすく、更新の担当が誰にもいない。攻撃者は公開されている脆弱性一覧から自動で探す。

予兆として現れるもの
ルーターの設定変更履歴、見覚えのない VPN ユーザー、海外 IP からの VPN 接続。

想定損失（試算）
内部ネットワーク全域の再点検 100〜300 万円／S-3 への連鎖

紐づく予防策
Rx-04　Rx-07　Rx-10

S-5 ログ不在による侵害の長期滞留

対象 **全ホスト横断**　発生可能性 **高**　影響度 **中**　検知容易性 **極低**　**リスク値 12/25**

STEP 1	STEP 2	STEP 3	STEP 4	STEP 5
いずれかの経路で初期侵入が成立する	改ざん検知が未導入で、ファイル改変が記録されない	ログイン履歴 7 日・アクセスログ 14 日で消え、侵入時刻が特定できない	数ヶ月静かに滞留し、取引先からの通報や不正請求で発覚	証跡が無く影響範囲を確定できず、全システムの予防的再構築を迫られる

なぜこの経路が成立するのか
これは「侵入される確率」ではなく「侵入されたとき、いつ気づけるか」の問題。今の構成では、気づく手段そのものが欠けている。

予兆として現れるもの
（現状では検知手段が無いことが所見そのもの）

想定損失（試算）
滞留日数に比例して増大／初動調査費 200 万円〜

紐づく予防策
Rx-07　Rx-09　Rx-10

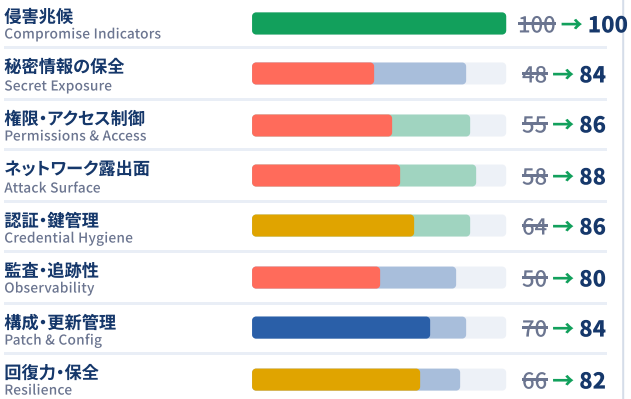
06 / PRESCRIPTION

予防策・処方箋

所見と侵害シナリオに対応する是正策を、優先度・工数・期限つきで提示します。総工数は約 43 時間（うち最優先 4 件で 12 時間）。最優先 4 件を 2 週間で完了させるだけで、リスク値の高いシナリオ S-1〜S-4 の起点が同時に潰れます。

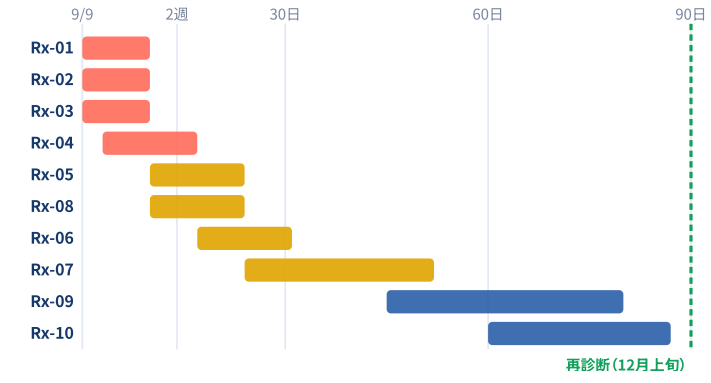
ID	優先度	処方内容	対象	工数	期限	改善見込	対応シナリオ
Rx-01	最優先	**WordPress 管理画面のアクセス制限と多要素認証** wp-login.php / xmlrpc.php を社内・VPN の IP に限定し、管理者に MFA を必須化。ログイン試行の制限を有効化	web-01	3h	2026-09-19	露出面 +14 / 認証 +6	S-1
Rx-02	最優先	**共通アカウントの廃止と退職者アカウントの棚卸し** 共通 ID「admin」を無効化し個人 ID へ分離。退職者 3 件を削除。退職手続きに ID 停止の項目を追加	app-01 / portal-01	4h	2026-09-19	権限 +16	S-2
Rx-03	最優先	**基幹 DB の待受を内部専用へ限定・root@% の廃止** bind-address を app サーバー向け内部 IP に限定。root@% を削除し、アプリ用ユーザーを接続元 IP 付きで再作成	db-01	2h	2026-09-19	露出面 +12 / 権限 +6	S-3
Rx-04	最優先	**拠点 VPN ルーターのファームウェア更新と管理画面の外部非公開** 最新版へ更新し、WAN 側の管理画面を停止。VPN ユーザーを棚卸しし、不明アカウントを削除	拠点ルーター	3h	2026-09-26	構成 +8	S-4
Rx-05	優先	**設定ファイル（.env / wp-config.php）の権限厳格化と実行ユーザー分離** 644 → 600（実行ユーザー専有）。root で動く開発用 Node を停止し、一般ユーザーで再構成	web-01 / app-01	3h	2026-10-03	秘密情報 +20	S-1 / S-3
Rx-06	優先	**SSH の鍵認証化・パスワード認証停止・接続元制限** 全ホストで PasswordAuthentication no。管理者ごとの鍵を発行し、from= で接続元を限定。同一パスワードの使い回しを解消	全ホスト	4h	2026-10-10	認証 +12	S-2
Rx-07	優先	**ログの外部集約・90 日保持・ログイン監査の開始** ログイン／Web／DB 接続ログを bk-01 とは別系統へ転送し 90 日保持。改ざん検知を導入し日次で差分通知	全ホスト	8h	2026-10-31	監査 +26	S-1〜S-5
Rx-08	優先	**ステージングからの本番データ除去と検索避け** 残置ダンプ 2 件を削除し、検証には匿名化データを使用。noindex を適用	stg-01	2h	2026-10-03	秘密情報 +12	S-5
Rx-09	計画	**バックアップの別系統・別拠点保管と復旧テスト** 日次バックアップをクラウドストレージへ暗号化コピー。四半期に 1 回、復旧テストを実施し手順書化	bk-01	10h	2026-11-28	回復力 +16	S-5
Rx-10	計画	**更新管理台帳の整備と四半期診断の定例化** OS・CMS・プラグイン・ネットワーク機器の更新状況を台帳化。四半期ごとに本診断を再実施し推移を記録	全ホスト	4h	2026-12-05	構成 +6	S-4 / S-5

是正後の到達見込み（カテゴリ別）



総合 62 点 → 86 点（判定 A 圏）。母集団順位は 7 位 → 2 位相当。薄い帯が Rx 完遂後、濃い帯が現状。

実施計画（90 日）



最優先 4 件	総工数	再診断
12 h	**43** h	**12** 月上旬
2 週間以内。S-1〜S-4 の起点を遮断	外部保守業者への依頼分を含む概算	86 点到達を客観確認

この処方の設計思想

「人が気をつける」を処方に含めない。総務 2 名が兼任で 6 ホストを運用する体制では、注意力に依存した対策は必ず摩耗します。権限・待受・鍵の分離は、いずれも一度設定すれば維持されるものだけを選定しました。

検知への投資を後回しにしない。Rx-07（ログ集約と改ざん検知）は最も工数がかかりますが、これが無い限り「侵害されていないこと」を今後も証明できません。次回診断の前提条件でもあります。

安い順ではなく、連鎖を切る順に並べる。Rx-01〜04 は工数の合計こそ 12 時間ですが、S-1〜S-4 という影響度 4〜5 のシナリオの起点を同時に潰します。費用対効果はここに集中しています。

診断そのものを仕組みに変える。Rx-10 で四半期診断を定例化し、本レポートを継続的な健康記録として運用します。スコアの推移が、対策が効いているかの唯一の客観指標になります。

07 / DETAILED FINDINGS

検査項目別 詳細所見

全 36 項目の検査結果（健康診断の検査値一覧に相当）。判定は A〜E の 5 段階、深刻度は要是正 24 件にのみ付与。

検査ID	検査項目	基準値	測定結果	判定	評価	深刻度	対象ホスト
IOC — 侵害兆候							
I-01	Web シェル・不審 PHP の設置	検出 0	検出 0（全 6 ホスト）	A	良好	—	全ホスト
I-02	不正に追加されたローカルユーザー	検出 0	検出 0	A	良好	—	全ホスト
I-03	暗号資産マイニング・不審プロセス	検出 0	検出 0	A	良好	—	全ホスト
I-04	不審な永続化（cron / systemd / rc.local）・外向き不審通信	検出 0	検出 0	A	良好	—	全ホスト
SEC — 秘密情報の保全							
S-01	アプリ設定ファイルの権限（.env / wp-config.php）	600	.env 644 / wp-config.php 644	D	要改善	MEDIUM	web-01 / app-01
S-02	本番データのステージング残置	0 件	本番 DB ダンプ 2 件（2026-05 / 2026-07）	D	要改善	MEDIUM	stg-01
S-03	git 追跡ファイルへの実鍵混入	0 件	0 件（履歴含む）	A	良好	—	app-01
S-04	コマンド履歴への平文パスワード	0 件	bash_history に DB パスワード平文 3 件	C	要注意	LOW	app-01 / db-01
S-05	バックアップの暗号化	暗号化	平文（アクセス制御のみ）	C	要注意	LOW	bk-01
PRM — 権限・アクセス制御							
P-01	共通アカウントの有無	0 件	共通 ID「admin」2 件（退職者の利用歴あり）	D	要改善	HIGH	app-01 / portal-01
P-02	退職者アカウントの残存	0 件	3 件（最終ログイン 2026-02）	D	要改善	MEDIUM	portal-01
P-03	DB ユーザーの接続元制限	localhost 限定	root@% が有効	D	要改善	MEDIUM	db-01
P-04	アプリ実行ユーザーの権限分離	非 root	開発用 Node が root で実行	C	要注意	LOW	app-01
P-05	sudo 設定の逸脱（NOPASSWD 濫用）・SUID 異常	最小	逸脱なし	A	良好	—	全ホスト
ATK — ネットワーク露出面							
A-01	データベースの待受インターフェース	127.0.0.1	*:3306（VPN 経由で拠点外から到達可）	D	要改善	HIGH	db-01
A-02	CMS 管理画面の公開範囲	IP 制限 + MFA	全世界公開・MFA なし・xmlrpc 有効	D	要改善	HIGH	web-01
A-03	開発用ポートの露出	なし	0.0.0.0:3000（Node）／:8080	C	要注意	LOW	app-01 / stg-01
A-04	SSH の公開範囲と認証方式	鍵のみ・from 制限	パスワード認証が有効（3 ホスト）	D	要改善	MEDIUM	web-01 / app-01 / stg-01
A-05	TLS 証明書の有効性と設定	有効・TLS1.2+	有効（自動更新）。TLS1.0 が残存	B	おおむね良好	—	web-01 / app-01
A-06	検証サイトの検索避け	noindex	未適用（Basic 認証のみ）	C	要注意	LOW	stg-01
KEY — 認証・鍵管理							
K-01	SSH 鍵の棚卸し	全て所有者特定	1 件が所有者不明（要人手照合 H-01）	C	要注意	LOW	app-01
K-02	管理者パスワードの使い回し	なし	3 ホストで同一（ハッシュ一致）	D	要改善	MEDIUM	web-01 / app-01 / stg-01
K-03	多要素認証	管理系に必須	未導入	C	要注意	LOW	全ホスト
K-04	パスワードポリシー・API キーの更新	12 文字以上・年 1 回	8 文字・期限なし（運用で補完）	B	おおむね良好	—	portal-01 / web-01
OBS — 監査・追跡性							
O-01	ログイン履歴の保全期間	90 日	7 日（logrotate 既定値）	D	要改善	MEDIUM	全ホスト
O-02	ログの外部集約	別系統へ集約	未実施（ホスト内のみ）	D	要改善	MEDIUM	全ホスト
O-03	改ざん検知（ファイル整合性監視）	稼働	未導入	D	要改善	MEDIUM	全ホスト
O-04	Web アクセスログの保持	90 日	14 日	C	要注意	LOW	web-01 / app-01
CFG — 構成・更新管理							
C-01	OS セキュリティ更新の追随	30 日以内	適用済（自動更新 有効）	A	良好	—	全ホスト
C-02	CMS・プラグインの更新	30 日以内	プラグイン 6 件が 90 日超未更新	C	要注意	MEDIUM	web-01
C-03	ネットワーク機器のファームウェア	最新版	拠点 VPN ルーターが 2023 年版のまま	D	要改善	MEDIUM	拠点ルーター
C-04	Web サーバー設定（セキュリティヘッダ等）	堅牢	適正（一部ヘッダ不足）	B	おおむね良好	—	web-01 / app-01
BCP — 回復力・保全							
B-01	バックアップの取得	定期取得	日次（bk-01 へ世代保持）	A	良好	—	bk-01
B-02	バックアップの隔離保管	別拠点・別系統	同一拠点・同一 LAN	C	要注意	LOW	bk-01
B-03	復旧テストの実施	年 1 回以上	未実施	D	要改善	MEDIUM	全ホスト
B-04	復旧手順の文書化	文書化済	一部のみ（手順書は口伝が主）	B	おおむね良好	—	全ホスト

判定基準　A 良好＝基準を満たす／B おおむね良好＝軽微な逸脱（所見件数に含めない）／C 要注意＝条件が揃えば侵害の起点になりうる／D 要改善＝既知の攻撃経路が成立する状態、期限を切って是正／E 要精密検査＝直ちに対処（本診断では該当なし）。人手による照合が必要な事項（H-01〜03）は第 8 章付記に掲載。

08 / OUTLOOK & METHODOLOGY

今後の展望・診断方法と免責

是正の実行計画に加えて、事業の成長に伴って必要になる備えを時間軸で示します。受発注ポータルの取引先拡大（2027 年予定）は、扱う取引先データと認証境界を確実に増やします。診断はその前に済ませておくほど安く付きます。

PHASE 1 ・ ～30日
止血

- Rx-01～04 の完遂（最優先 4 件）
- EC 管理画面の IP 制限と MFA
- 共通 ID の廃止・退職者 ID 削除
- 基幹 DB の待受を内部専用へ
- VPN ルーターの更新と管理画面非公開
- 人手照合 H-01～03 の確定

PHASE 2 ・ ～90日
構造の是正

- Rx-05～08 の完遂
- 設定ファイル 600 化・実行ユーザー分離
- SSH の鍵認証化とパスワード使い回し解消
- ログ外部集約・90 日保持・改ざん検知
- ステージングの本番データ除去
- 再診断でスコア 86 点の到達を確認

PHASE 3 ・ ～180日
仕組みへの移行

- Rx-09～10 の完遂
- バックアップの別拠点・暗号化保管
- 復旧テストの初回実施と手順書化
- 更新管理台帳の整備（OS・CMS・網機器）
- 四半期診断の定例化とスコア推移の記録

PHASE 4 ・ ～12ヶ月
事業成長への備え

- 取引先拡大に向けた受発注ポータルの認証再設計（取引先ごとの ID・MFA）
- 個人データ取扱いの棚卸しと保存期間ポリシー整備
- 取引先からのセキュリティチェックシートへの回答体制
- インシデント対応訓練の実施（本レポートの S-1 を教材化）

事業側の前提（診断への影響）

取引先ポータルの拡大	取引先 ID が 20 社 → 60 社規模に増える予定。共通 ID の廃止（Rx-02）と取引先ごとの認証設計が先行して必要。増えてからの是正は工数が 3 倍になる。
大手取引先の監査	2027 年に主要取引先からのセキュリティ監査（チェックシート）が見込まれる。ログ保持 90 日・MFA・バックアップ隔離は、ほぼ確実に問われる項目。
基幹システムの更新	生産管理システムの更新（クラウド化）を検討中。移行前に db-01 の接続元制限と権限整理を済ませておくと、移行時の棚卸しがそのまま使える。

診断方法と免責 METHODOLOGY & DISCLAIMER

実施方法

実施日	2026年9月2日（単日）
対象	SSH で到達可能な全 6 ホスト（参考：拠点 VPN ルーターは外形確認のみ）
手法	ホストへの SSH 接続による読み取り専用の構成精査。認証情報露出 8 観点、侵害兆候（IoC）6 観点
非実施	脆弱性の実証（Exploit）、負荷試験、設定変更、サービス再起動、ペネトレーションテスト
記録方針	秘密の値は一切記載せず、存在と所在のみを記録
スコア算定	8 カテゴリの加重平均（重みは第 3 章）。カテゴリ点は検査項目の判定分布から算出
検査観点	認証情報の露出／git 追跡・履歴への秘密混入／ファイル権限／ネットワーク待受と公開範囲／SSH 鍵と認証方式／Web シェル・不正ユーザー・マイニング・不審な永続化の有無／改ざん検知とログの取得状況／バックアップと復旧体制／OS・ミドルウェアの更新追随／TLS と公開設定

本診断の限界（明記事項）

単日のスナップショットです。診断時点で痕跡が無いことは、過去に侵害が無かったことを保証しません。特に改ざん検知とログが欠けているホストでは、過去の侵害を検出する手段が存在しません。

アプリケーション層は対象外です。SQL インジェクション、認可の欠陥、XSS 等のコードレベルの脆弱性は本診断の範囲に含まれません。別途、コード診断が必要です。

到達できないホストは評価していません。SSH で到達できなかった環境、および外部委託先が管理する環境は対象外です。拠点 VPN ルーターは外形からの確認のみで、内部設定は未検証です。

スコアは相対指標です。絶対的な安全性の証明ではなく、同条件の母集団内での位置と、前回からの変化を読むための指標として設計されています。

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・IP（文書用アドレス）・所見・数値・ベンチマーク母集団（A 社～K 社）はすべて様式提示のための例示値です。外部の認証機関による認証・適合証明ではありません。

付記 A ― 人手による照合が必要な事項

機械的な検査では「正当か不正か」を判定できず、関係者の確認を要する項目です。いずれも現時点で不正と判断する材料はありませんが、確認されるまでは未確定として扱います。

H-01	app-01 の authorized_keys にある所有者不明の SSH 公開鍵 1 件が、過去の保守業者のものであること（不明なら失効）
H-02	portal-01 への外部ログイン元 IP（2 件）が、既知の担当者の自宅または VPN であること
H-03	stg-01 に残置された本番 DB ダンプ 2 件の作成目的と、削除してよいことの確認

付記 B ― 再診断（12 月上旬）で確認する指標

指標	今回	目標	確認方法
総合スコア	62 / C	**86 / A**	同一 36 項目の再測定
HIGH 所見	3 件	**0 件**	A-01 / A-02 / P-01 の再判定
ログイン履歴の保持	7 日	**90 日**	集約先での実保持期間
管理系 MFA	未導入	**全管理者**	CMS・ポータル・VPN の設定
復旧テスト	未実施	**1 回完了**	手順書と所要時間の記録

付記 C ― 用語解説

MFA	多要素認証。パスワードに加えてスマートフォン等の第 2 要素を要求し、パスワード漏えい単独でのログインを防ぐ。	改ざん検知	ファイル整合性監視。重要ファイルのハッシュを定期比較し、想定外の変更を通知する仕組み。
*:3306 待受	DB が全ネットワークインターフェースで接続を受け付ける状態。127.0.0.1 限定が基本。	root@%	DB の最高権限ユーザーが「どこからでも」接続できる設定。接続元をホスト単位で限定するのが原則。
xmlrpc.php	WordPress の遠隔操作用インターフェース。総当たり攻撃の増幅に悪用されるため、不要なら無効化する。	IoC	侵害の痕跡（Indicator of Compromise）。Web シェル・不正ユーザー・不審な通信など、既に侵入されたことを示す証拠。
noindex	検索エンジンに収録させない指示。検証環境が検索結果に露出し攻撃対象として発見されることを防ぐ。	偏差値	母集団平均を 50、標準偏差を 10 として換算した相対位置。50 が平均、60 で上位約 16%。

発行：株式会社Game ／ ELC SERVER HEALTH LAB　診断チーム　報告書番号 SHL-2026-0000-SAMPLE-001

SAMPLE / 見本