KnownFor
2026/10/20

mihon.example.jp ホームページ点検報告書

このまま放っておくと、AI 経由の見込み客を逃し続け、御社のサイトや名前を使った被害が起きるおそれがあります。

売上の機会

見込み客が AI に聞く10問のうち 7問で、御社は候補に出ていません。

比べる・値段を調べる段階の質問で名前が出ない。いちばん先の原因は「トップページに製品の名前がない」

被害のリスク

外から見える範囲のセキュリティに重大な問題があり、実際のセキュリティ・インシデントと同じ状態が 2つあります。

前回の点検から、直ったものは 0件です。

—

GEO 成熟度（レベル1〜5）

GEO 成熟度のレベル1「読まれる」の手前です。基本のセキュリティ項目に重大な問題があるため、レベル1に届いていません。

レベルは、公開している GEO 成熟度の5段です。条件を満たした段までを「届いた」とします。

SAMPLE

読む人ごとの案内

経営者・役員

表紙・1枚の要約・01 実際に起きたこと・04 決めてほしいこと（決裁欄）。5分ほどで、何を決めればよいかが分かります。

情報システム・発注の担当

03 リスクの評価と対応の計画・付録。作業指示書（別冊）で、委託の範囲と作業時間の目安が分かります。予算と契約の材料に。

Web の担当・制作会社

02 いまの現在地・05 直すときと直したあと・作業指示書（別冊）。何を、どこで、どう直し、どう確認するかが1件ずつ書いてあります。

受け取った日
年　月　日

次の点検の目安
2026/10/27

作成
KnownFor の AI ガイド

KnownFor の AI ガイドは AI エージェントで、人の担当者ではありません。外から見える範囲の点検で、「安全」を保証するものではありません。御社の判断の材料としてお使いください。

1枚で全体が分かる要約

2026/10/20

GEO 成熟度	警戒レベル（セキュリティ）	AI の候補に出た質問	同じ業種の中で
レベル1の手前	5 ／5段	3 ／10問 根拠にされたのは 0問	2 位／上位2社 AI の候補に出る割合の順

うまくいっていること

- セキュリティ19項目のうち 12項目は問題なし
- 「工場のとき、どんなエアコンの節電用品がありますか」のような質問では、AI が御社の名前を挙げています

いちばん大きな課題

- 比べる・値段を調べる段階の質問で名前が出ない。いちばん先の原因は「トップページに製品の名前がない」
- 外から見える範囲のセキュリティに重大な問題があり、実際のセキュリティ・インシデントと同じ状態が 2つあります。

売上への影響	AI で比べて選ぶ見込み客に、御社が候補として出ません。選ばれる前に、他社に決まってしまうおそれがあります。
被害のリスク	外から見える範囲のセキュリティに重大な問題があり、実際のセキュリティ・インシデントと同じ状態が 2つあります。（01）
信用	起きた場合、サイトの停止・説明・お詫びに追われます（01 のセキュリティ・インシデントの結末）。

今すぐ対応する範囲を超えたリスク 4件（R1 情報の漏えい・R2 改ざん・偽サイトへの誘導・R3 なりすまし・詐欺・R4 売上の機会損失。03 のヒートマップ）

	決めてほしいこと	だれが・作業時間の目安	期限
1	R1 送信を暗号化する	制作会社・半日〜2日	2026/10/27
2	R2・R3 古いソフトを更新し、バージョン番号を見せない／セキュリティヘッダーを設定する／名前をかたるメールを止める設定を入れる	制作会社・5〜13日	2026/11/19
3	R4 製品名と、比べるための説明を書く	社内・3〜11日	2026/10/27

> この点検で調べていないこと：法令の適合（著作権・景品表示法・薬機法など）、会員の画面の中、侵入テスト。必要なら専門家にご相談ください。

SAMPLE

01 同じ状態のサイトで、実際に起きたこと

主に読む人：経営者・役員

御社で見つかった状態と、ほかの組織で実際に起きたセキュリティ・インシデント（出典のあるものだけ）を突き合わせました。御社で同じことが起きている、または必ず起きる、という意味ではありません。

セキュリティ・インシデント 1　新潟医療福祉大学（2023年）

御社にも同じ状態

何が起きたか

サイトの管理のしくみ（CMS）の脆弱性を使われて書き換えられ、訪れた人が別の悪意あるサイトへ自動で送られる状態になりました。サイトを止めて調べました。

御社では

同じ状態が見つかりました。ソフトのバージョン番号が外から見える

止め方　バージョン番号を外に出さない設定にします。

出典：ScanNetSecurity（2023年4月7日）

セキュリティ・インシデント 2　総務省・警察庁・経済産業省の要請（日本・2023年）

御社にも同じ状態

何が起きたか

クレジットカード会社などを名乗るメールで偽サイトに誘い、カード番号などをだまし取るフィッシングが多く起きているとして、総務省・警察庁・経済産業省がカード会社などに対策の強化を求めました。フィッシングメールはドメイン名をなりすまして送られることが多いとして、メールを送らないものを含む全てのドメインに DMARC を入れ、なりすましメールを受け取らせない方針（拒否）で使うよう求めています。

御社では

同じ状態が見つかりました。なりすましメール対策の設定（DMARC）がない

止め方　DNS に DMARC を足します（まず監視のみの設定から）。

出典：総務省（2023年2月1日）

セキュリティ・インシデント 3　大阪市（2026年）

御社に近い状態

何が起きたか

市が委託した事業のイベント申込フォームで、委託先が閲覧の設定をまちがえたため、申し込んだ人がほかの申込者の入力内容を見られる状態になりました。40名分の氏名・学年・電話番号・ファックス番号・メールアドレス・応募の動機が対象です。10月14日に申込者からの連絡で分かり、委託先が同じ日に設定を直しました。

原因は暗号化（https）ではありませんが、フォームに入力した内容がほかの人に見られた例です。

御社では

近い状態があります。暗号化されていない（http の）送信先のフォーム

止め方　フォームの送り先を https にします。

出典：大阪市 報道発表（2026年10月15日）

SAMPLE

02 いまの現在地と、成果を阻んでいる原因

主に読む人：Web の担当・制作会社

GEO 成熟度	警戒レベル	AI の候補に出た	根拠にされた
── レベル1の手前	5 ／5段 いちばん急ぐことを直すと 3 に下がる	3 ／10問	0 ／10問

見込み客の質問の段階ごとに、御社の名前が出たか

質問の段階	質問（例）	名前が出た
探す	工場のとき、どんなエアコンの節電用品がありますか	3／6
比べる	エアコンの節電用品の保守体制はどう比較すればよいですか	0／2
値段を調べる	エアコンの節電用品の納期と価格の目安を教えてください	0／2

AI の答えで見つかったこと（2件）

- AI がサイトを根拠にしない
- 分野の言葉がサイトにない

成果を阻んでいる最大の原因：トップページに製品の名前がない

比べる・値段を調べるの段階の質問で、御社の名前が出ていません。製品を探して来た人が、トップページで何の会社か分からず帰ってしまうことがあります。AI も、御社と製品を結びつけにくくなります。

GEO 成熟度（AI に正しく案内される度合い）

1 読まれる	2 正しく読まれる	3 案内される	4 根拠にされる	5 行動につながる

GEO 成熟度のレベル1「読まれる」の手前です。基本のセキュリティ項目に重大な問題があるため、レベル1に届いていません。枠で囲んだのが、いま取り組むレベルです。

前回の点検と比べて

直ったもの	そのまま残っているもの	新しく見つかった・悪くなったもの
0 件	20 件	2 件

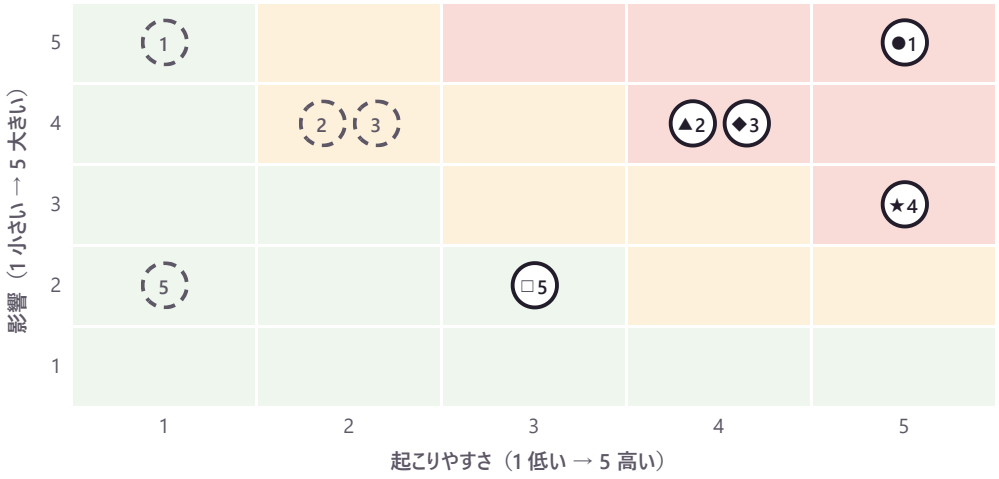
比べるのは御社の前回とだけです。

SAMPLE

03 リスクの評価と、対応の計画

主に読む人：情報システム・発注の担当

見つかった 20件を、事業のリスク 5件にまとめ、「起こりやすさ」と「影響」で評価しました。右上ほどリスクが大きく、赤い区画（15点以上）が今すぐ対応する範囲です。



印の形（リスクの種類）

- ● 情報の漏えい
- ▲ 改ざん・偽サイトへの誘導
- ◆ なりすまし・詐欺
- ★ 売上の機会損失
- □ 信用の低下
- 1 直したあとに残る位置

我慢できる範囲（点＝起こりやすさ×影響）

- 15〜25：今すぐ対応
- 8〜14：計画して対応
- 1〜7：受け入れて見張る

リスク	原因（見つかったこと）	点	対応の方針	だれが・期限・作業時間	直したあと
R1 ●	**お客様の入力が読まれる（個人情報の漏えい）** 暗号化されていない（http の）送信先のフォーム	5×5＝25	低減：送信を暗号化する	制作会社・10/27・半日〜2日	1×5＝5
R2 ▲	**ページが書き換えられ、お客様が偽サイトへ誘導される** ソフトのバージョン番号が外から見える・古い JavaScript ライブラリ・セキュリティヘッダーが不足しているほか1件	4×4＝16	低減：古いソフトを更新し、バージョン番号を見せない／セキュリティヘッダーを設定する	制作会社・11/19・5〜11日	2×4＝8
R3 ◆	**会社の名前をかたる偽メールで、取引先が被害にあう** なりすましメール対策の設定（DMARC）がない	4×4＝16	低減：名前をかたるメールを止める設定を入れる	制作会社・11/19・半日〜2日	2×4＝8
R4 ★	**AI 経由の見込み客を取り逃がす** AI の候補に出ない（10問中7問）・トップページに製品の名前がない・製品のページに説明の文章がほとんどないほか6件	5×3＝15	低減：製品名と、比べるための説明を書く	社内・10/27・3〜11日	28日後に同じ質問で測る
R5 □	**作りかけに見えて、信用を落とす** ダミーテキストのまま公開されている・メニューの名前と行き先の名前がちがう・ロゴをクリックするとトップページ以外に行く	3×2＝6	受け入れて見張る（手が空いたら直す）	社内・10/27・6時間〜3日	1×2＝2

SAMPLE

点の物差し（起こりやすさと影響の1〜5の定義）は、この章の最後に載せています。直したあとの位置は決まった規則で出したもので、効果の予測ではありません。

道筋：だれが、いつまでに 作業時間は、作業指示書の工数（小＝1〜2時間・中＝半日〜2日・大＝3〜5日）を足した目安です。金額は出しません。

時期	主なこと	社内	制作会社	KnownFor の AI ガイド
今週	暗号化されていない（http の）送信先のフォーム・トップページに製品の名前がない ほか1件	2件・2〜4時間	1件・半日〜2日	—
30日まで	製品のページに説明の文章がほとんどない・メニューの名前と行き先の名前がちがう ほか9件	5件・2〜7日	6件・6〜15日	—
60日まで	h1 見出しが画像だけ・製品のページに製品の構造化データ（Product）がない ほか2件	1件・1〜2時間	2件・5時間〜3日	1件（下書き）

時期	主なこと	社内	制作会社	KnownFor の AI ガイド
次の点検のあと	購入は別のサイトへ行く・llms.txt（AI への案内）がない	1件・1〜2時間	—	1件（下書き）

起こりやすさ
5：悪用が確認された脆弱性が見える・いま起きている
4：実際のセキュリティ・インシデントと同じ状態
3：外から機械で見つけられる・AI の答えに実際に誤りが出た
2：ほかの不備と重なると起きる
1：理論上

影響
5：個人情報の漏えい・金銭の被害
4：改ざん・停止・取引先の被害
3：誤った案内・見込み客を大きく逃す
2：信用の低下
1：軽微

SAMPLE

04 決めてほしいこと

主に読む人：経営者・役員

我慢できる範囲を超えたリスクへの、対応の方針を決めてください。選んだものに印を付け、決めた方の名前と日付を書いてください。画面でも記録でき、次の報告書で照らし合わせます。

1 R1 送信を暗号化する 被害のリスク

期限 2026/10/27

決めないと何が残るか	直すと	だれが・作業時間
R1（25点）がそのまま残ります：お客様の入力が読まれる（個人情報の漏えい）	点が下がります：R1 25→5点	制作会社 1件・半日〜2日

☐ 直す　☐ 期限を決めて見送る（理由：　　）　☐ 詳しい人に相談する

決めた人	日付	制作会社への依頼日

2 R2・R3 古いソフトを更新し、バージョン番号を見せない／セキュリティヘッダーを設定する／名前をかたるメールを止める設定を入れる 被害のリスク

期限 2026/11/19

決めないと何が残るか	直すと	だれが・作業時間
R2（16点）・R3（16点）がそのまま残ります：ページが書き換えられ、お客様が偽サイトへ誘導される／会社の名前をかたる偽メールで、取引先が被害にあう	点が下がります：R2 16→8点・R3 16→8点	制作会社 5件・5〜13日

☐ 直す　☐ 期限を決めて見送る（理由：　　）　☐ 詳しい人に相談する

決めた人	日付	制作会社への依頼日

3 R4 製品名と、比べるための説明を書く 売上の機会

期限 2026/10/27

決めないと何が残るか	直すと	だれが・作業時間
R4（15点）がそのまま残ります：AI 経由の見込み客を取り逃がす	AI に案内される根拠ができます。直した日から28日後に、同じ質問で測ります。	社内 6件・3〜11日

☐ 担当を決めて進める　☐ 期限を決めて見送る（理由：　　）　☐ 詳しい人に相談する

決めた人・担当	日付	書き上げる日

知ったあとのこと：新しい義務が増えるわけではありません。個人情報を扱う会社には、個人情報保護法の安全管理措置（第23条）がすでに求められています。受け取った日と決めた内容を残すと、「知ってから何をしたか」を説明できます（法的な助言ではありません）。

SAMPLE

05 直すときと、直したあと

主に読む人：Web の担当・制作会社

作業指示書（別冊）
1件ずつ、直し方・完了の条件・確認の方法が書いてあります。制作会社の見積もりに要る作業の範囲も、この中で分かります。

直したあと
直したあとに同じ規則で確認するには、もう1回の点検か、継続のプランをお使いください。継続のプランでは毎週自動で点検し、次の点検報告書で、04 で決めたことと照らし合わせ、リスクの点がどう変わったかを示します。

一度直しても、ふだんの作業で元に戻りやすいところがあります

見つかったことの多くは、サーバーの更新・委託先の交代・新しいページの公開といった、ふだんの作業のときに、また起こりやすいものです。直すことと同じくらい、「その作業のときに確認する決まり」を作ると、同じ問題が起きにくくなります。

元に戻りやすい作業	だれの作業か	戻りやすいとき	いまの状態
サーバー設定の変更	制作会社	設定を変えたとき	4件
公開・リニューアルの手順	制作会社	設定を変えたとき	4件
ページを作る決まり	自分たち	ページを作るとき・担当が替わるとき	11件
期限の管理（証明書・ドメイン）	制作会社	期限の日付が来たとき	期限 2026/12/1
ソフトの更新	制作会社	期限の日付が来たとき	2件
メールの送信設定	制作会社	設定を変えたとき	1件

決まりの例：サーバーの移行・委託先の変更のときに、確認する項目の表を渡す／設定を変えたあとに、もう一度点検する

SAMPLE

A 付録 ・ ページの一覧

読んだ公開ページ 10ページのうち、見つかったことのあるページ 10ページを載せています（右の番号は作業指示書の番号）。

ページ	トップページからのクリック数	作業指示書
見本株式会社 | 総合的なビジネスパートナー トップページ	0	P-02 P-15
サービス内容 | 見本株式会社 /services	1	P-07 P-11 P-15
商材 | 見本株式会社 /products	1	P-05 P-07 P-15
お客様の声 | 見本株式会社 /voice	1	P-03 P-07 P-15
採用情報 | 見本株式会社 /recruit	1	P-15
会社概要 | 見本株式会社 /company	1	P-15
Fold-M210S | 見本株式会社 /products/fold-m210s	2	P-04 P-07 P-15 P-16 P-19
クリアミナモ | 見本株式会社 /products/クリアミナモ	2	P-04 P-07 P-15
thank | 見本株式会社 /thank	行けない	P-15 P-17
お問い合わせ | 見本株式会社 /contact	行けない	P-06 P-15

B 付録 ・ AI に聞いた質問

クリアミナモ

問	質問	名前	根拠
1	“工場のとき、どんなエアコンの節電用品がありますか”	✓	×
2	“事務所の工程で電気代の削減を改善するには、どんな設備が使われますか”	×	×
3	“エアコンの節電用品を選ぶとき、納期で比べるとどのメーカーが候補になりますか”	✓	×
4	“エアコンの節電用品の納期と価格の目安を教えてください”	×	×
5	“エアコンの節電用品の保守体制はどう比較すればよいですか”	×	×

Fold-M210S

問	質問	名前	根拠
1	“工場のとき、どんなエアコンの節電用品がありますか”	✓	×
2	“事務所の工程で電気代の削減を改善するには、どんな設備が使われますか”	×	×

SAMPLE

問	質問	名前	根拠
3	“エアコンの節電用品を選ぶとき、納期で比べるとどのメーカーが候補になりますか”	×	×
4	“エアコンの節電用品の納期と価格の目安を教えてください”	×	×
5	“エアコンの節電用品の保守体制はどう比較すればよいですか”	×	×

答えの全文は、KnownFor の画面で確認できます。

C 付録 ・ 設定例

一般的な設定の見本です。ご自身のサイトに合うか、制作会社に確認してから反映してください。作業指示書の付録 C と同じものです。

Apache（.htaccess）：セキュリティヘッダー P-12

```
# .htaccess (Apache) - add after the https redirect
<IfModule mod_headers.c>
  Header always set Strict-Transport-Security "max-age=31536000"
  Header always set Content-Security-Policy "frame-ancestors 'self'"
  Header always set X-Content-Type-Options "nosniff"
</IfModule>
```

WordPress（子テーマの functions.php）：セキュリティヘッダー P-12

```
// WordPress (child theme functions.php)
add_action('send_headers', function () {
  header('Strict-Transport-Security: max-age=31536000');
  header("Content-Security-Policy: frame-ancestors 'self'");
  header('X-Content-Type-Options: nosniff');
});
```

Apache：バージョン番号の表示を隠す P-09

```
# httpd.conf / apache2.conf
ServerTokens Prod
ServerSignature Off
```

PHP：バージョン番号の表示を隠す P-09

```
; php.ini
expose_php = Off
```

WordPress：generator のバージョンを隠す P-09

```
// WordPress (child theme functions.php)
remove_action('wp_head', 'wp_generator');
add_filter('the_generator', '__return_empty_string');
```

DNS：DMARC（まず監視のみ） P-13

```
; DNS TXT record - review the reports first, then tighten step by step
_dmarc.example.jp.  TXT  "v=DMARC1; p=none; rua=mailto:dmarc@example.jp"
```

D 付録 ・ 調べた方法と調べていないこと

いまは、人が御社のサイトを開く前に、AI がページを読んで答えを作ります。同じページを、サイバー攻撃者も自動スキャンで外から見ています。この報告書は、外から見える範囲のセキュリティを土台に、AI の答えの中でどこまで育っているかを、GEO 成熟度という1本の線で点検した結果です。

SAMPLE

対象	御社のウェブサイト（mihon.example.jp）の公開ページ。大事なページから順に 10ページを読みました。サイト全体はこれより大きいことがあります。会員の画面などログインの奥は読んでいません。
AI の答え	買い手が実際に聞きそうな質問を、商品・サービスごとに AI（Gemini）へ聞きました（社名を入れない質問・合わせて 10問）。名前が出たか、御社のサイトが根拠にされたかを確認しました。
聞き方	Gemini（gemini-3.6-flash）に、ウェブ検索ありで、2026/10/20 12:00ごろ、各問 1回ずつ聞きました。AI の答えは聞くたびに変わることがあり、この結果はその時の1回分です。次の点検で、同じ質問・同じ AI で聞き直して比べます。
外から見える範囲のセキュリティ	外部から誰でも確認できる公開情報を 19項目 点検しました（通信の暗号化・証明書の期限・ブラウザのセキュリティの設定・外から見えるソフトのバージョン番号・送信ドメイン認証など）。判定は決まった規則だけで行い、AI は使っていません。サイトが同じ状態なら、だれが行っても同じ結果になります。
GEO 成熟度	判定の基準（GEO 成熟度モデル）は www.knownfor.jp/maturity/ で公開しています。点検で分かるのは、セキュリティ・検索と AI の読み取りの設定・AI の答えの数字までです。AI のクローラーの来訪（Cloudflare）・Google のインデックス（Search Console）・AI から来た訪問と問い合わせ（GA4）は、点検では分からないため「記録なし」としました。

問題が見つからなかった点検（12項目）。次のことは見つかりませんでした：http から https への転送がない／https のページが http のものを読み込む／クッキーのセキュリティの設定がない／偽メール対策（DMARC）が監視のみの設定／メールの送信元を確認する設定（SPF）がない／送信元の設定（SPF）に制限がない／証明書の期限が近い（または切れている）／サーバーのソフト（PHP など）の、公表された脆弱性があるバージョンが見える／PHP で動いていて、脆弱性の修正を外から確認できない／悪用が確認された脆弱性の対象のバージョンが見える／外部から読み込むスクリプトに、改ざんを検知する仕組み（SRI）がない／改ざんの兆候（業種と無関係なスパム語の集まり）が見える

調べていないこと

- サーバーの中・管理画面・会員の画面など、外から見えない場所
- 暗号の強さの設定、プラグインごとの脆弱性（バージョンが外から見えるものだけ確認しました）
- ほかのサブドメイン・外部のリンク先、robots.txt（クローラーに読ませない指定）で止めているページ
- 今回聞いた AI のほかの AI での答え、答えの中身がすべて正しいかどうか
- 侵入テストやセキュリティ診断の代わりにはなりません。深い点検が必要な場合は、専門の診断会社に別途ご依頼ください。

SAMPLE

読み方

重大
放っておくと被害が起こるおそれのある状態（機械で確認できたものだけ）

注意
いますぐの被害ではないが、攻撃や誤った案内の足がかりになる

軽微
整えておくこと。急ぎではない。GEO 成熟度の「記録なし」も灰で示します

問題なし
点検した範囲で見つからなかった

> 「見つからなかった」は「安全」「問題がない」という意味ではありません。点検した項目の範囲で見つからなかった、という意味です。AI の答えは、ホームページを直さなくても日によって変わります。数字は、同じ質問・同じ AI・同じ時期でそろえて比べます。

E 付録 ・ 用語と出典

GEO 成熟度	ホームページが生成 AI の答えにどの程度取り上げられているかを、外から見える範囲のセキュリティから人の行動まで1本の線で表す5つのレベル（読まれる・正しく読まれる・案内される・根拠にされる・行動につながる）。
警戒レベル	外から見える範囲のセキュリティの危険度（5段）。5がもっとも危険で、国の避難情報の警戒レベルと同じ向き。GEO 成熟度のレベルとは向きが逆。
検証期間	修正の効果を判断するために、修正のあとに待つ期間（28日）。

記録なし	材料が無く、合格とも未達とも言えない状態。推測で埋めない。
根拠にされる	AI の答えが、そのサイトを出どころ（リンク）として使うこと。
HSTS	「このサイトはいつも https で開いて」とブラウザに伝える設定。
SPF・DMARC	メールの送信元が本物かを、受け取る側が確認するための設定。DMARC には「監視のみ」「隔離」「拒否」の段階がある。
説明文（meta description）	検索や AI がページを紹介するときに使う、1〜2文の説明。
llms.txt	AI にサイトの概要と大事なページを伝えるテキストファイル（任意の取り組み）。
作業指示書	制作会社にそのまま渡せる、見つかったことごとの手順・完了の条件・報告してほしいことを書いた書類（別冊）。

新潟医療福祉大学（2023年）	ScanNetSecurity（2023年4月7日） https://scan.netsecurity.ne.jp/article/2023/04/07/49179.html
サイバー攻撃者の数字	警察庁「令和8年上半期におけるサイバー空間をめぐる脅威の情勢等について」（2026年9月）p.5 NICT「NICTER 観測レポート 2025」（2026年2月）／警察庁「令和7年におけるサイバー空間をめぐる脅威の情勢等について」p.19 警察庁令和8年上半期 p.9・p.10 IPA「情報セキュリティ 10大脅威 2026」［組織］

この報告書は、外から見える範囲の点検の結果です。「見つからなかった」は「安全」という意味ではありません。作成：KnownFor（株式会社アーグマックス） www.knownfor.jp

SAMPLE