サンプル市公式ホームページ点検報告書

このまま放っておくと、住民に正しい案内が届かず、貴市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。

住民への案内

住民が AI に聞く18問のうち 4問で、公式サイトが答えの根拠になっていません。

公式サイトが答えの根拠になりにくい。いちばん先の原因は「ダミーテキストのまま公開されている」

被害のリスク

実際の事件と同じ状態が 3つあります。

前回の点検から、直ったものは 0件です。

E

総合評価（A〜E の5段）

GEO 成熟度のレベル1「読まれる」の手前です。（判定に必要な記録がそろっていない項目があります）

A〜E は GEO 成熟度の読み替えです（レベル1に届かない＝E・レベル1＝D・2＝C・3＝B・4〜5＝A）。

SAMPLE

読む人ごとの案内

首長・幹部

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。

情報政策課（調達）

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。

広報・各課（直す人）

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
2026/11/19

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。貴市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

サンプル市・2026/10/20

総合評価	警戒レベル（セキュリティ）	公式サイトが根拠の答え
E ／A〜E	3 ／5段	14 ／18問

うまくいっていること

- セキュリティ19項目のうち 15項目は問題なし
- 18問のうち 14問は、公式サイトを根拠に案内されています

いちばん大きな課題

- 公式サイトが答えの根拠になりにくい。いちばん先の原因は「ダミーテキストのまま公開されている」
- 実際の事件と同じ状態が 3つあります。

住民への影響	AI に聞いた住民に、公式の正しい案内が届きにくいままです。
被害のリスク	実際の事件と同じ状態が 3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 の事件の結末）。

今すぐ対応する範囲を超えたリスク 1件（R1 改ざん・偽サイトへの誘導。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 古いソフトを更新し、版を見せない	委託先・1〜4日	2026/11/19

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：首長・幹部

貴市で見つかった状態と、ほかの組織で実際に起きた事件（出典のあるものだけ）を突き合わせました。貴市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。

事件 1　山梨大学（2026年）

貴市にも同じ状態

何が起きたか

大学が契約するレンタルサーバーで、1つのサイトが使っていた Joomla の拡張機能「JCE」のぜい弱性が6月上旬に使われ、サーバーを外から操る不正なプログラム（ウェブシェル）が置かれました。7月下旬までに同じサーバーのほかのサイトにも広がったとみられ、不正なアカウントや検索結果を汚すスパムが見つかりました。大学は同じサーバーの複数のサイトの公開を止めました。

貴市では

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：山梨大学 お知らせ（2026年8月27日）・ScanNetSecurity（2026年9月17日）

事件 2　Virgin Media O2（英国・2026年）

貴市にも同じ状態

何が起きたか

英国の通信会社 Virgin Media O2 が、検索や AI ツールで偽の窓口の電話番号が示されることに注意を呼びかけました。同社の調べでは、英国の人の 13%（約8人に1人）が検索や AI ツールで偽の窓口の番号を示されたことがあり、10% は AI ツールが出した番号を頼りにしています。同社は、こうした番号にかけて詐欺にあったお客様の例に対応してきたとしています。番号は会社の公式サイト・アプリ・請求書に載っているものだけを使うよう勧めています。

貴市では

同じ状態が見つかりました。AI の答えの電話番号がサイトとちがう

出典：Virgin Media O2（2026年4月24日）・ISPreview（2026年4月24日）

事件 3　名古屋市（2026年3月更新のお知らせ）

貴市にも同じ状態

何が起きたか

閉じた市のサイトのドメインのうち 5件が第三者に取られたとして、一覧を公表しました。「市とは無関係」「危険なサイトへ誘導されるおそれ」「興味本位で開かない」と呼びかけ、リンクを残している先に外すよう求めています。

貴市では

同じ状態が見つかりました。AI が公式ではないアドレスを案内

出典：名古屋市「第三者に取得された廃止ドメインへのアクセスにはご注意ください！」

SAMPLE

02 いまの現在地と、成果を阻んでいる原因

主に読む人：広報・各課（直す人）

総合評価	警戒レベル	公式が根拠
E ／A〜E	3 ／5段 いちばん急ぐことを直すと 2 に下がる	14 ／18問

AI の答えで見つかったこと（3件）

- AI の答えの電話番号がサイトとちがう
- AI が公式ではないアドレスを案内
- AI が案内する公式のページが開かない

> **成果を阻んでいる最大の原因：ダミーテキストのまま公開されている**
>
> 作りかけのサイトに見え、自治体の信用を下げるおそれがあります。

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

貴市はレベル1の手前です。セキュリティの基本項目に重大な問題があるあいだは、AI の数字が良くても、レベル1に届きません。

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	8 件	2 件

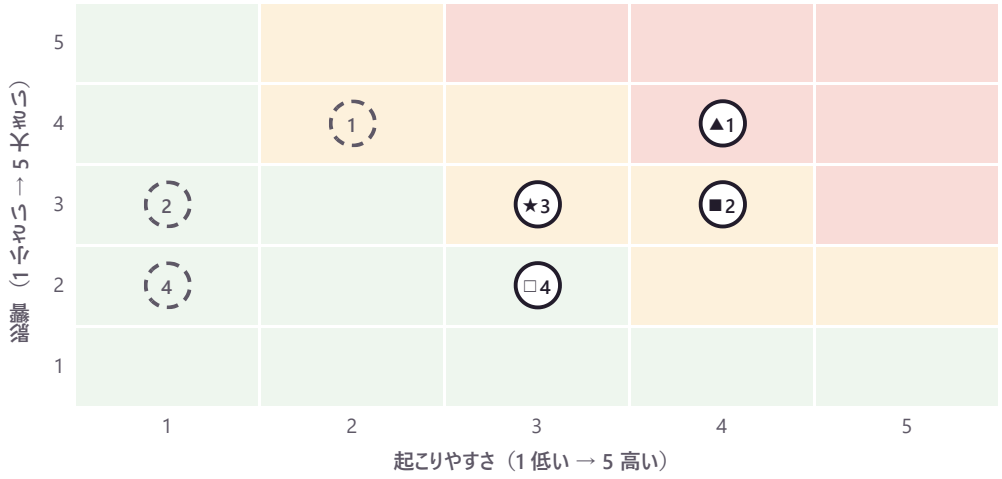
比べるのは貴市の前回とだけです。

SAMPLE

03 リスクの評価と、対応の計画

主に読む人：情報政策課（調達）

見つかった 7件を、事業のリスク 4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）

- ▲ 改ざん・偽サイトへの誘導
- ■ 案内の誤り
- ★ 公式の案内が届かない（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 ▲	**ページが書き換えられ、住民が偽の案内へ誘導される** ソフトのバージョン番号が外から見える・セキュリティヘッダーが不足している	4×4＝16	低減：古いソフトを更新し、版を見せない	委託先・11/19・1〜4日	2×4＝8
R2 ■	**AI が住民に誤った窓口や行き先を案内する** AI の答えの電話番号がサイトとちがう・AI が公式ではないアドレスを案内・AI が案内する公式のページが開かない	4×3＝12	低減：電話番号と案内を、公式の1つにそろえる	—	1×3＝3
R3 ★	**住民に公式の正しい案内が届かない** 公式サイトが答えの根拠にならない（18問中4問）・ページの説明文（meta description）がない	3×3＝9	低減：公式の案内のページを、AI が根拠にできる形に書く	庁内・11/19・半日〜2日	28日後に同じ質問で測る
R4 □	**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	3×2＝6	受け入れて見張る（手が空いたら直す）	庁内・10/27・1〜2時間	1×2＝2

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	庁内	委託先	KnownFor の AI ガイド
今週	ダミーテキストのまま公開されている	1件・1〜2時間	—	—
30日まで	ページの説明文（meta description）がない・ソフトのバージョン番号が外から見える ほか1件	1件・半日〜2日	2件・1〜4日	—
60日まで	セキュリティの連絡先（security.txt）が公開されていない・偽メール対策（DMARC）が監視のみの設定	—	2件・2〜4時間	—
次の点検のあと	llms.txt（AI への案内）がない	—	—	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：実際の事件と同じ状態
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・住民に公式の案内が届かない
2：信用の低下
1：軽微

SAMPLE

04 決めてほしいこと

主に読む人：首長・幹部

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 古いソフトを更新し、版を見せない 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
R1（16点）がそのまま残ります：ページが書き換えられ、住民が偽の案内へ誘導される	点が下がります：R1 16→8点	委託先 2件・1〜4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	制作の委託先への依頼日

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。受け取った日と決めた内容を行政文書として残すと、「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：広報・各課（直す人）

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。委託先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	制作の委託先	設定を変えたとき	3件
ソフトの更新	制作の委託先	期限の日付が来たとき	期限 2026/12/31
期限の管理（証明書・ドメイン）	制作の委託先	期限の日付が来たとき	期限 2027/1/15
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	1件
メールの送信設定	制作の委託先	設定を変えたとき	1件
公開・リニューアルの手順	制作の委託先	設定を変えたとき	2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

貴自治体でご確認いただきたいこと（2件）

自動では判定できなかったことです。貴自治体の方がいちばんよくご存じです。。

1. **この番号（000-011-0000）は、貴自治体の窓口の番号ですか。**
   貴自治体の番号なら、その番号を載せたページを公式サイトに置くと、AI が確認しやすくなります。ちがう番号なら、AI がまちがった番号を案内しています。

2. **bousai-matome.example は、貴自治体の施設・関連団体などのサイトですか。**
   関係先なら、そのままでよいです。関係のないサイトなら、AI が住民をそこへ案内していることになります。

SAMPLE

A 付録 ・ ページの一覧

読んだ公開ページ 9ページのうち、見つかったことのあるページ 4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
くらし・手続き ｜ サンプル市 /kurashi	1	P-02
子育て・教育 ｜ サンプル市 /kosodate	1	P-01 P-02
ごみ・リサイクル ｜ サンプル市 /gomi	1	P-02
お知らせ ｜ サンプル市 /news	1	P-02

B 付録 ・ AI に聞いた質問

問	質問	根拠にしたサイト	答えの確認
1	“サンプル市の指定避難所はどこですか。近くの避難所の調べ方も教えてください。”	✓ www.city.sample.example.jp、bousai-matome.example	施設・窓口の名前：公式で確認 2
2	“サンプル市で災害が起きたときの問い合わせ先の電話番号を教えてください。”	✓ www.city.sample.example.jp	窓口の番号：公式サイトと一致
3	“サンプル市の避難指示や防災情報は、どこで受け取れますか（防災メール・アプリ・防災無線など）。”	✓ www.city.sample.example.jp、bousai-matome.example	—
4	“サンプル市の洪水・浸水のハザードマップはどこで見られますか。”	✓ www.city.sample.example.jp	—
5	“サンプル市で断水したとき、給水を受けられる場所はどこですか。”	✓ www.city.sample.example.jp	施設・窓口の名前：公式で確認 2
6	“サンプル市で大きな地震のときに帰れなくなったら、一時滞在施設はどこですか。”	× kitaku-shien.example	—
7	“サンプル市の福祉避難所や、避難に助けが要る人の登録はどうすればいいですか。”	✓ www.city.sample.example.jp	窓口の番号：公式サイトと一致
8	“サンプル市で罹災証明書を申請するには、どこに何を出せばいいですか。”	✓ www.city.sample.example.jp	施設・窓口の名前：公式で確認 1
9	“サンプル市の被災者支援や義援金の、公式の受付先はどこですか。”	✓ www.city.sample.example.jp	—
10	“休日や夜間に子どもが急に熱を出したら、サンプル市ではどこに相談すればいいですか。”	× kodomo-iryo.example	—
11	“サンプル市で暑さを避けられる施設（クーリングシェルター）はどこですか。”	× heat-guide.example	施設・窓口の名前：公式で確認 1
12	“サンプル市で児童虐待やDVの相談は、どこにすればいいですか。”	✓ www.city.sample.example.jp	—

SAMPLE

問	質問	根拠にしたサイト	答えの確認
13	“サンプル市で、こころの悩みを相談できる窓口はどこですか。”	✓ www.city.sample.example.jp	—
14	“サンプル市の公式ホームページのアドレスはどれですか。”	✓ www.city.sample.example.jp	—
15	“サンプル市役所を名乗る電話やメールが来ました。本物かどうか確認するには、どこに連絡すればいいですか。”	× sagi-taisaku.example	窓口の番号：公式サイトで確認できず 公式サイトに無い番号 1件（国・都道府県・民間の窓口のこともあります）
16	“サンプル市の給付金や還付金をかたる詐欺について、注意の呼びかけはありますか。”	✓ www.city.sample.example.jp	—
17	“サンプル市の公式SNSのアカウントはどれですか。”	✓ www.city.sample.example.jp	—
18	“サンプル市のホームページが見られないとき、どこで情報を確認すればいいですか。”	✓ www.city.sample.example.jp	—

✓＝自治体の公式サイト　△＝ほかの公的機関　×＝それ以外。施設・窓口の名前は、公式サイトに同じ名前があるかで確認しました（確認できなかった名前は、国・都道府県・民間の施設のこともあります）。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、制作の委託先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-04

```
# .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>
```

Apache：バージョン番号の表示を隠す P-03

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

PHP：バージョン番号の表示を隠す P-03

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

DNS：DMARC（監視のみから隔離へ） P-06

```
; DNS TXT record - after reviewing the reports, move from monitoring (p=none) to quarantine
; keep your current rua= address
_dmarc.city.sample.example.jp.  TXT  "v=DMARC1; p=quarantine; rua=mailto:dmarc@city.sample.example.jp"
```

D 付録 ・ 調べた方法と調べていないこと

いまは、人が市のホームページを開く前に、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	サンプル市公式ホームページ（www.city.sample.example.jp）の公開ページ。大事なページから順に 9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	住民が実際に聞きそうな、命と暮らしにかかわる質問 18問（避難所・災害の窓口・給水・ハザードマップ・相談の窓口など）を AI へ聞きました。答えが根拠にしたサイトを「自治体の公式」「ほかの公的機関（国・都道府県など）」「それ以外」に分け、答えに出た窓口の電話番号と施設の名前を、公式サイトで確認しました。答えの中身がすべて正しいかまでは確認していません。
聞き方	Gemini（gemini-3.6-flash）に、ウェブ検索ありで、2026/10/20 10:10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（15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／暗号化されない送り先へ入力を送るフォーム／サポートが終わったバージョンのソフトが見える／古い JavaScript ライブラリ／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／なりすましメール対策の設定（DMARC）がない／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（分野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、専門の診断事業者に別途ご依頼ください。

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。

> この報告書の数字を、ほかの自治体と並べて公表することはありません（自治体名が分からない全国の傾向の統計にだけ使います）。比べるのは、市自身の前回の点検とだけです。

SAMPLE

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	制作の委託先にそのまま渡せる、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）。

滋賀県立図書館（2025年）	滋賀県教育委員会「県立図書館ホームページの再開について」 https://www.pref.shiga.lg.jp/edu/hodo/oshirase/344978.html 滋賀県教育委員会「県立図書館ホームページの一時閉鎖について」 https://www.pref.shiga.lg.jp/edu/hodo/oshirase/344358.html
名古屋市（2026年3月更新のお知らせ）	名古屋市「第三者に取得された廃止ドメインへのアクセスにはご注意ください！」 https://www.city.nagoya.jp/about/1048296.html
岡山県（2023年）	ScanNetSecurity（2023年10月23日） https://scan.netsecurity.ne.jp/article/2023/10/23/50128.html
総務省の注意の呼びかけ（2026年5月）	INTERNET Watch（総務省の注意の呼びかけ） https://internet.watch.impress.co.jp/docs/news/2107396.html GMO ブランドセキュリティ調査（2026年3月） https://group.gmo/pdf/news/gmo_news_9942.pdf
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。数字をほかの自治体と並べて公表することはありません（自治体名の分からない全国の統計にだけ使い、5自治体未満の単位では出しません）。作成：KnownFor（株式会社アーグマックス） www.knownfor.jp

SAMPLE