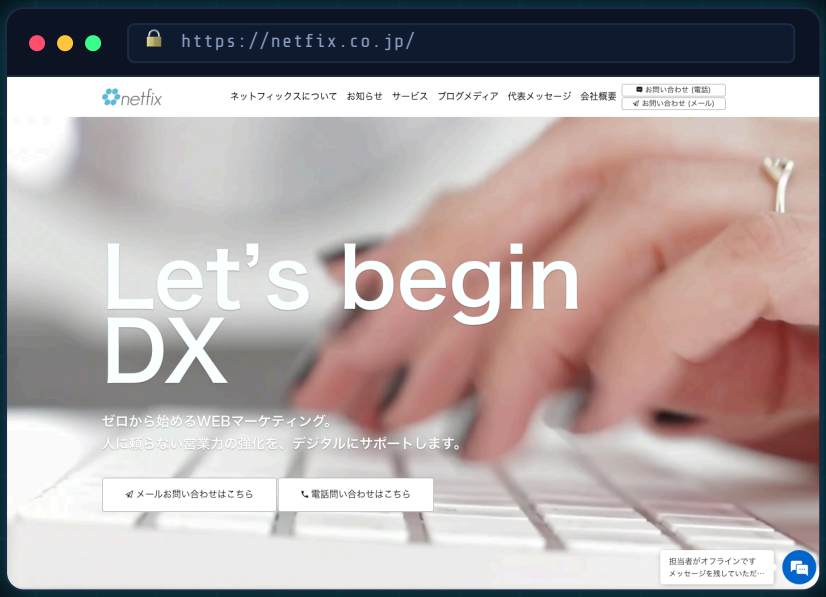
EXTERNAL ATTACK SURFACE ASSESSMENT // PASSIVE MODE

# 外部セキュリティ診断 レポート

TARGET netfix.co.jp · DATE 2026-11-10




CAPTURED 2026-11-10 · トップページの外観（診断時点）

93 / 100
RANK A

| 0 | 5 |
|---|---|
| 重大 | 要改善 |
| 10 | 17 |
| 参考 | 良好 |

VERDICT

**外部から見える範囲では良好です。内部対策の確認に進める段階です。**

最優先: Content-Security-Policy ／ 公開サブドメイン ／ クリックジャッキング防止

CLIENT

## 株式会社ネットフィックス

https://netfix.co.jp/

本レポートは、公開情報（DNS・証明書・公開Webページ・公開データベース）だけを参照する**受動的な外部調査**の結果です。侵入・負荷・攻撃的な操作は一切行っていません。点数は「外部から観測できる範囲」の評価であり、安全の保証ではありません。


READ FIRST
P.2 この1枚で判断できます

FOR EXECUTIVES
P.3〜 放置すると、こうなります

ACTION
P.5 優先順位と費用の目安



ISSUED BY

**株式会社ネットフィックス**

セキュリティ診断サービス

REPORT ID NETFIX-CO-JP-20261110

32 CHECKS · 18.8s · PASSIVE

# この1枚で判断できます

netfix.co.jp

## いま最も危ない3点

WARNING

### 1. Content-Security-Policy（スクリプト差し込み防止）

未設定。

放置すると: 改ざんされた際に不正スクリプトが素通りします。カード情報を抜くWebスキミングの防波堤です。

対策 CSPヘッダを段階導入（Report-Only→本番）　工数 15〜30分　業者相場 〜1万円

WARNING

### 2. 公開サブドメイン（証明書履歴から）

13件。管理系・開発系と思われる名前: test.netfix.co.jp

放置すると: 開発環境・管理画面は本番より守りが弱く、侵入の入口になりがちです。

対策 不要なものは停止、必要なものはIP制限/認証　工数 半日　業者相場 3〜10万円

WARNING

### 3. クリックジャッキング防止（X-Frame-Options）

未設定。

放置すると: 御社サイトを透明な枠に入れて、利用者に別の操作をさせる手口に使えます。

対策 X-Frame-Options: SAMEORIGIN　工数 15分　業者相場 〜1万円

## 分野別スコア

| # | 分野 | 達成度 | 配点 | 得点 | 重大/要改善 |
|---|---|---|---|---|---|
| 01 | メールなりすまし対策 | | 20 | 20.0 | 0 / 0 |
| 02 | 通信の暗号化 | | 15 | 13.9 | 0 / 1 |
| 03 | 公開されている入口 | | 15 | 13.2 | 0 / 1 |
| 04 | ソフトウェアの古さ | | 15 | 15.0 | 0 / 0 |
| 05 | 漏えい・ブラックリスト | | 10 | 10.0 | 0 / 0 |
| 06 | Web防御ヘッダ | | 10 | 5.5 | 0 / 3 |
| 07 | DNS・ドメイン管理 | | 10 | 10.0 | 0 / 0 |
| 08 | 情報露出・その他 | | 5 | 5.0 | 0 / 0 |

RECOMMENDED BUDGET

指摘の是正にかかる一般的な費用感（業者依頼時）

**5〜14 万円**

一時費用の合計。月額・年額の継続費は P.5 に別掲。社内で対応する場合は工数欄を参照。

NEXT 30 DAYS

1. Content-Security-Policy（スクリプト差し込み防止）（30日以内）
2. 公開サブドメイン（証明書履歴から）（30日以内）
3. クリックジャッキング防止（X-Frame-Options）（30日以内）
4. 外部から見えない項目の確認（内部ヒアリング10項目・P.10）

# 放置すると、こうなります



この章は技術の説明ではありません。「誰が・何をして・最悪どうなるか」だけを、専門用語を使わずに書いています。経営判断にはこの章と P.2 だけで足ります。

## 要改善 サイトに不正な仕掛けを差し込まれても、ブラウザが止めてくれない状態

診断項目: Content-Security-Policy（スクリプト差し込み防止）

**たとえるなら**

店内に見知らぬ人が機械を設置しても、誰も止めない状態。

**どうやって狙われるか**

犯人がサイトの一部を改ざんして『入力内容を自分に送る仕掛け』を埋めたとき、本来はブラウザ側で止められます。その指示が出ていないため、仕掛けはそのまま動きます。

**最悪、こうなる**

フォームに入力された個人情報・カード情報が盗まれます。改ざんは見た目に出ないため、発覚はカード会社からの連絡で、数か月後です。

**実際にあった話**

国内通販サイトの情報流出の典型的な手口で、この防御があれば被害を大幅に減らせたと事後調査で指摘される事例が多数あります。

## 要改善 管理用・テスト用のページが、外から見える場所に残っている状態

診断項目: 公開サブドメイン（証明書履歴から）

**たとえるなら**

本社ビルの通用口や工事用の仮設入口が、看板付きで表通りに面している状態。

**どうやって狙われるか**

犯人はまず『この会社にどんな入口があるか』を調べます。管理画面や開発中のページは本番より守りが甘いことが多く、そこから侵入して本番に横移動します。

**最悪、こうなる**

忘れられたテストサイトから侵入され、本番サイトの改ざん・顧客データの持ち出しに至ります。『そんなページがあったことすら誰も知らなかった』が典型です。

**実際にあった話**

2023年以降の国内の侵入事故の多くは、本番ではなく『使っていない古いシステム』が入口でした。

## 要改善 御社サイトを『透明なシート』の下に敷いて、利用者をだます手口が使える状態

診断項目: クリックジャッキング防止（X-Frame-Options）

**たとえるなら**

本物の窓口の上に透明な板を置き、客に別の書類に判を押させる手口。

**どうやって狙われるか**

犯人は自分のサイトの中に御社サイトを透明にして重ね、利用者には『プレゼントに応募』と見せながら、実際には御社サイト上のボタン（設定変更・送信など）を押させます。

**最悪、こうなる**

利用者が意図しない操作をさせられ、『御社サイトで勝手に手続きされた』という苦情になります。ログインが必要なサービスほど被害が大きくなります。

**実際にあった話**

SNSや通販サイトで『いいね』や購入を勝手に押させる手口として広く知られ、対策は15分程度の設定です。

# 放置すると、こうなります



### 要改善 最初の一回だけ、暗号化なしで接続される隙がある状態

診断項目: HSTS（常時https強制）

**たとえるなら**

玄関は施錠しているが、来客が毎回いったん裏口を試してから玄関に回る状態。

**どうやって狙われるか**

犯人は利用者が最初に接続する一瞬を狙って通信を横取りし、本物そっくりの偽サイトに誘導します。利用者は気づかずパスワードを入力します。

**最悪、こうなる**

お客様や社員のログイン情報が盗まれ、そこから社内システムへ侵入されます。

**実際にあった話**

公共Wi-Fiでのこの手口は実演動画が多数公開されており、専用の機器は数千円で買えます。

### 要改善 ブラウザがファイルの種類を『勘で判断』してしまう状態

診断項目: X-Content-Type-Options

**たとえるなら**

中身を確認せず『たぶん書類だろう』と封筒を開けてしまう状態。

**どうやって狙われるか**

犯人が画像や文書のふりをした不正プログラムを置くと、ブラウザがそれをプログラムとして実行してしまいます。

**最悪、こうなる**

利用者のパソコンで不正な処理が動き、御社サイト経由の被害になります。

**実際にあった話**

単体で大事故になることは少ないですが、他の弱点を『実際の被害』に変える役割を果たします。設定は15分です。

03 / ACTION PLAN

# 対策の優先順位と費用の目安

5 ITEMS

| # | 項目 | 深刻度 | 期限 | 直し方 | 社内工数 | 業者相場 |
|---|---|---|---|---|---|---|
| 01 | **Content-Security-Policy（スクリプト差し込み防止）** | 中 | 30日以内 | CSPヘッダを段階導入（Report-Only→本番） | 15〜30分 | 〜1万円 |
| 02 | **公開サブドメイン（証明書履歴から）** | 中 | 30日以内 | 不要なものは停止、必要なものはIP制限/認証 | 半日 | 3〜10万円 |
| 03 | **クリックジャッキング防止（X-Frame-Options）** | 中 | 30日以内 | X-Frame-Options: SAMEORIGIN | 15分 | 〜1万円 |
| 04 | **HSTS（常時https強制）** | 中 | 30日以内 | レスポンスヘッダに Strict-Transport-Security を追加 | 15分 | 〜1万円 |
| 05 | **X-Content-Type-Options** | 中 | 30日以内 | nosniff を追加 | 15〜30分 | 〜1万円 |

**相場の読み方**

「業者相場」は国内のWeb制作会社・ITベンダーに個別依頼した場合の一般的な価格帯です（当社調べ・2026年11月時点）。「社内工数」は、サーバやDNSの管理画面に入れる担当者が自力で行う場合の目安です。複数項目を一括で依頼すると、個別合計より3〜5割安くなるのが通例です。

04.1 / MAIL

## メールなりすまし対策

100%
配点 20 / 得点 20.0

参考 **MTA-STS / TLS-RPT（メール経路の暗号化強制）**

未設定（大企業でも未設定が多い発展項目）。メール経路の盗聴・改ざん耐性を上げられます。

▶ 直し方: MTA-STSポリシー公開＋TLS-RPT（2時間）

参考 **BIMI（受信箱にロゴ表示）**

未設定。DMARC reject 達成後に導入すると受信箱にロゴが出て、偽メールと一目で区別されます。

▶ 直し方: VMC証明書＋BIMIレコード

良好 **DMARC（なりすまし拒否ポリシー）**

p=quarantine。偽メールは迷惑メールへ。reject化が最終形です。

```
v=DMARC1; p=quarantine; rua=mailto:postmaster@netfix.co.jp
```

良好 **SPF（送信元の正当性宣言）**

設定済み（-all で厳格）。

```
v=spf1 a:sv8029.xserver.jp include:_spf.google.com -all
```

良好 **DKIM（電子署名）**

署名鍵を確認（セレクタ: google）。

良好 **メール受信サーバ（MX）**

5件（Google Workspace）。

```
alt1.aspmx.l.google.com, alt2.aspmx.l.google.com, aspmx.l.google.com, aspmx2.googlemail.com, aspmx3.googlemail.com
```

04.2 / TLS

## 通信の暗号化

92%
配点 15 / 得点 13.9

要改善 **HSTS（常時https強制）**

未設定。

▲ なぜ危ないか: 初回アクセス時の http 接続を横取りされる余地があります。

▶ 直し方: レスポンスヘッダに Strict-Transport-Security を追加（15分）

良好 **SSL証明書の有効性**

有効（発行: Let's Encrypt、残り52日、TLSv1.3）。

良好 **古い暗号方式（TLS1.0/1.1）の残存**

無効（TLS1.2以上のみ）。

良好 **http→https の強制**

http で来た訪問者を https へ転送しています。

04.3 / EXPOSURE

## 公開されている入口

88%
配点 15 / 得点 13.2

要改善 **公開サブドメイン（証明書履歴から）**

13件。管理系・開発系と思われる名前: test.netfix.co.jp

▲ なぜ危ないか: 開発環境・管理画面は本番より守りが弱く、侵入の入口になりがちです。

▶ 直し方: 不要なものは停止、必要なものはIP制限/認証（半日）

blog.netfix.co.jp, c.netfix.co.jp, ichinen.netfix.co.jp, jcn.netfix.co.jp, lp.netfix.co.jp, m.netfix.co.jp, s.netfix.co.jp, shop.netfix.co.jp, support.netfix.co.jp, test.netfix.co.jp, u.netfix.co.jp, wine.netfix.co.jp, www.netfix.co.jp

良好 **インターネットに開いているポート（公開DB参照）**

Web（80/443）とメール以外の入口は記録されていません。

良好 **サーバの既知脆弱性（CVE・公開DB照合）**

公開DB上で紐付くCVEはありません。

04.4 / SOFTWARE

## ソフトウェアの古さ

100%
配点 15 / 得点 15.0

良好 **ソフトウェア名・版数の公開**

サーバ・CMSの版数は隠されています。

良好 **JavaScriptライブラリの既知脆弱性**

版数の判別できる外部ライブラリなし。

04.5 / BREACH

## 漏えい・ブラックリスト

100%
配点 10 / 得点 10.0

参考 **セキュリティ各社の評価（VirusTotal）**

未照会（APIキー未設定）。

良好 **過去の漏えい事故（公開DB）**

Have I Been Pwned にこのドメイン発の漏えい登録はありません。

良好 **迷惑メール・不正ドメインリスト（Spamhaus DBL）**

掲載なし。

04.6 / HEADERS

# Web防御ヘッダ

55%
配点 10 / 得点 5.5

要改善 **Content-Security-Policy（スクリプト差し込み防止）**

未設定。

▲ なぜ危ないか: 改ざんされた際に不正スクリプトが素通りします。カード情報を抜くWebスキミングの防波堤です。

▶ 直し方: CSPヘッダを段階導入（Report-Only→本番）（15〜30分）

要改善 **クリックジャッキング防止（X-Frame-Options）**

未設定。

▲ なぜ危ないか: 御社サイトを透明な枠に入れて、利用者に別の操作をさせる手口に使えます。

▶ 直し方: X-Frame-Options: SAMEORIGIN（15分）

要改善 **X-Content-Type-Options**

未設定。

▲ なぜ危ないか: ファイル種別の誤解釈を使った攻撃を許します。

▶ 直し方: nosniff を追加（15〜30分）

参考 **Referrer-Policy（遷移先への情報漏れ防止）**

未設定。

▲ なぜ危ないか: 外部リンク先に御社サイトのURL（会員ページ等）が渡ります。

▶ 直し方: strict-origin-when-cross-origin（15〜30分）

参考 **Permissions-Policy（カメラ・位置情報等の制限）**

未設定。

▶ 直し方: 必要最小限に制限（15〜30分）

04.7 / DNS

## DNS・ドメイン管理

100%
配点 10 / 得点 10.0

参考 **DNSSEC（DNS応答の改ざん防止）**

未設定（日本の企業サイトの9割以上が未設定。導入は任意）。

▶ 直し方: レジストラでDNSSEC有効化（1時間）

参考 **CAA（証明書の勝手な発行防止）**

未設定。第三者が別の認証局で御社名の証明書を取る余地が残ります。

▶ 直し方: CAAレコード追加（15分）

参考 **類似ドメインの第三者取得状況**

御社名に似たドメインが稼働中: netfix.com, netfix.net（メール受信可）, netfix.co, netfix.xyz, netfix.site（メール受信可）（自社保有分を除いて要確認）

▲ なぜ危ないか: 似たドメインからの請求書メールは、取引先が見分けられません。

▶ 直し方: 主要TLDの防衛的取得＋監視（30分）

良好 **放置された転送先（サブドメイン乗っ取りリスク）**

存在しない先を指すレコードはありません。

良好 **ドメインの有効期限**

2027-05-31（残り201日）。

良好 **DNSサーバの冗長性**

4台。

04.8 / MISC

## 情報露出・その他

100%
配点 5 / 得点 5.0

参考 **WAF/CDN（Web攻撃の防波堤）**

WAF/CDNの兆候なし。攻撃がサーバに直接届きます。

▶ 直し方: Cloudflare（無料〜）等の導入（2時間）

参考 **security.txt（脆弱性の連絡先公開）**

未公開。善意の研究者が脆弱性を知らせる窓口がありません。

▶ 直し方: /.well-known/security.txt を置く（15分）

良好 **プライバシーポリシーの掲示**

トップページから到達できます。

05 / BEYOND THE PERIMETER

# 外部からは見えない、本当に大事な10項目

本診断で見えるのは「外から見える表面」です。実際の被害（ランサムウェア・情報漏えい）の大半は、**社内の端末・アカウント・バックアップ**の運用から起きます。会議で以下を確認してください。経済産業省「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS）」★3の自己評価でも求められる領域です（対応付けは当社整理）。

| # | 確認事項 | Yesなら | 確認 |
|---|---|---|---|
| 01 | 全PCにウイルス対策（EDR）が入り、管理画面で全台の状態が見えているか | 端末の乗っ取りを早期検知できる | ☐ |
| 02 | メール・クラウドのログインに2要素認証（MFA）が全員・例外なしで設定されているか | アスクル事例（MFA例外アカウントが突破口）の再発防止 | ☐ |
| 03 | バックアップが『社内ネットから切り離された場所』にあり、復元テストを年1回以上しているか | ランサムウェアに暗号化されても復旧できる | ☐ |
| 04 | 退職者・業務委託のアカウントが当日中に止まる手順があるか | 放置アカウント経由の侵入を防ぐ | ☐ |
| 05 | OS・ソフトの更新が自動化され、未更新端末を把握しているか | 既知の穴を塞ぎ続けられる | ☐ |
| 06 | 管理者権限を持つ人が最小限で、普段は一般権限で作業しているか | 1台の感染が全社に広がらない | ☐ |
| 07 | 『感染したら誰が何をするか』の初動手順と連絡先が1枚にまとまっているか | 復旧までの期間と損害を最小化できる | ☐ |
| 08 | 取引先・委託先と情報を共有する際の規約・方法が決まっているか | サプライチェーン経由の被害を防ぐ | ☐ |
| 09 | 全従業員が年1回以上、標的型メールの訓練または教育を受けているか | 侵入の起点（メール）での被害率を下げる | ☐ |
| 10 | サイバー保険の加入有無と、補償範囲（事業中断・損害賠償）を把握しているか | 被害時の資金的ダメージを限定できる | ☐ |

## 診断の過程で気づいた点（セキュリティ以外）

- トップページに問い合わせ導線（フォーム）がない。問い合わせはメール・電話中心と推測

06 / HOW WE CAN HELP

# 当社で代行できる範囲

本レポートの指摘のうち、当社が対応できる項目です。相場の下限付近で、まとめて短期間に実施します。社内で対応される場合も、手順書の提供や確認（再診断）だけの依頼も可能です。

| # | 項目 | 当社の対応 | 期間 | 業者相場 |
|---|---|---|---|---|
| 01 | **Content-Security-Policy（スクリプト差し込み防止）** | CSPヘッダを段階導入（Report-Only→本番） | 15〜30分 | 〜1万円 |
| 02 | **公開サブドメイン（証明書履歴から）** | 不要なものは停止、必要なものはIP制限/認証 | 半日 | 3〜10万円 |
| 03 | **クリックジャッキング防止（X-Frame-Options）** | X-Frame-Options: SAMEORIGIN | 15分 | 〜1万円 |
| 04 | **HSTS（常時https強制）** | レスポンスヘッダに Strict-Transport-Security を追加 | 15分 | 〜1万円 |
| 05 | **X-Content-Type-Options** | nosniff を追加 | 15〜30分 | 〜1万円 |

PACKAGE ESTIMATE

**5 万円〜（税別）**

上記一時対策の一括実施。個別相場の合計（5〜14万円）の下限で提示。正式見積は無料。

CONTINUOUS MONITORING

**月 1.1 万円（税別）**

本診断を毎月自動実施し、点数の変化・新たな弱点・証明書/ドメイン期限を通知。年1回の報告書を稟議用に提供。

**その先の話**

セキュリティの土台が整うと、業務のクラウド化・AIによる自動化（問い合わせ対応、書類処理、営業事務）を安全に進められます。当社はもともと業務改革・マーケティングが本業です。土台が済んだ後の「攻め」の相談もお受けします。

**お問い合わせ**　株式会社ネットフィックス　sawakix@netfix.co.jp　https://netfix.co.jp

07 / METHOD & APPENDIX

# 調査方法・前提・生データ

### METHOD

- DNS公開レコード（SPF/DKIM/DMARC/MX/NS/DS/CAA/CNAME）
- TLS接続と証明書（443番のみ・通常の閲覧と同等）
- 公開Webページ（トップ・robots.txt・security.txt）のHTTP応答
- 公開データベース: 証明書透明性ログ（crt.sh）、Shodan InternetDB、Have I Been Pwned、Spamhaus DBL、OSV.dev、RDAP/WHOIS

### LIMITATIONS

- 侵入試行・脆弱性スキャン・負荷は行っていません（不正アクセス禁止法の圏外）
- 公開DBの情報は数日〜数週間の遅れがあります
- DKIMは一般的なセレクタ名のみ確認
- 点数は当社基準。安全性の保証・認証ではありません
- 高評価でも内部要因による事故は防げません

## 生データ

| 項目 | 値 |
|---|---|
| SPF | v=spf1 a:sv8029.xserver.jp include:_spf.google.com -all |
| DMARC | v=DMARC1; p=quarantine; rua=mailto:postmaster@netfix.co.jp |
| DKIM selectors | google |
| MX | 5 alt1.aspmx.l.google.com. \| 5 alt2.aspmx.l.google.com. \| 1 aspmx.l.google.com. \| 10 aspmx2.googlemail.com. \| 10 aspmx3.googlemail.com. |
| NS | 01.dnsv.jp. \| 02.dnsv.jp. \| 03.dnsv.jp. \| 04.dnsv.jp. |
| TLS | protocol: TLSv1.3<br>cipher: TLS_AES_256_GCM_SHA384<br>expires: 2027-01-01T06:03:20+00:00<br>days: 52<br>issuer: Let's Encrypt<br>sans: ['netfix.co.jp', 'www.netfix.co.jp']<br>legacy: [] |
| IP / ports | 183.181.88.30 (netfix.co.jp,www.netfix.co.jp): 25,80,443,993<br>172.217.78.26 (alt1.aspmx.l.google.com): 25<br>192.179.30.26 (alt2.aspmx.l.google.com): 25 |
| Subdomains (13) | blog.netfix.co.jp, c.netfix.co.jp, ichinen.netfix.co.jp, jcn.netfix.co.jp, lp.netfix.co.jp, m.netfix.co.jp, s.netfix.co.jp, shop.netfix.co.jp, support.netfix.co.jp, test.netfix.co.jp, u.netfix.co.jp, wine.netfix.co.jp, www.netfix.co.jp |
| Response headers | server: nginx<br>date: Tue, 10 Nov 2026 03:27:57 GMT<br>content-type: text/html; charset=UTF-8<br>transfer-encoding: chunked<br>connection: keep-alive<br>vary: Accept-Encoding<br>content-encoding: gzip |
| Software | — [] |