Webセキュリティ診断は
Webサイトの脆弱性や改ざんの有無を定期的に診断します

簡単利用	診断時の立ち会いやサーバー停止不要	
メール通知	問題発生時にメールでお知らせ	
結果はWeb		いつでも好きなときに結果を確認 ※PDFでダウンロードもできます。

ご利用料金

初期費用

Webセキュリティ診断 初期費用　不要

＋

インターネット接続サービス 初期費用

＋

月額利用料

基本契約	基本URL（1ドメイン）ごとに	5,500円（税込） ※同一ドメインであっても、100ページ・100パラメータを超えて診断する場合は、追加契約となります。
追加契約	追加URL（基本URLを除く1ドメイン）ごとに	4,400円（税込） ※追加契約で追加することができる追加URLの数は、最大4つまでとなります。

＋

インターネット接続サービス 月額利用料

＋

プロバイダサービス 月額利用料

注意事項

●Webセキュリティ診断をお申込みいただくお客さま名義での、フレッツ光、フレッツ・ADSL、電話サービスまたはISDNサービスの契約が必要です。診断対象となるWebコンテンツやプログラムはお客さま（契約者）が所有、管理していることが必要です。●月額利用料は、ご利用開始日の翌月から発生します（ご利用開始日と同月に解約した場合は、ご利用開始月の月額利用料が発生します）。●解約月の月額利用料は日割り計算いたしません。●本サービスは、診断対象URLにおいて全てのWebアプリケーションプログラムの脆弱性の検出及びすべての不正リンクURLの検出を保証するものではありません。●本サービスを提供することに伴い発生する損害及びお客さまの本サービスの利用により生じる結果については、いかなる責任も負いません。●お客さまのシステム構成や設定、ホームページの仕様等によっては、本サービスの一部が実施されない場合があります。●本サービスにより生成される診断結果は、診断実施時点のものであり、診断後に発見されるWebアプリケーションプログラムの脆弱性及び不正リンクURLについては加味されません。●診断対象のサイトの仕様変更やシステムの設定変更の影響によって診断対象に生じた変化については加味しません。●診断対象のサーバーにアクセスできない（サーバー停止、アクセス規制等を含みますが、これらに限られません。）場合は、診断することができません。●本サービスは、診断により発見された問題点について、いかなる対策方法の提示及び修繕や修理手配も行いません。●本サービスの利用規約は、予告なく変更となる場合があります。詳しくは、ホームページ（https://flets.com/web-security-shindan/）の最新の規約をご確認ください。●その他の事項に関しては、お問い合わせいただければメールにてご回答致します。

お問い合わせ

東日本電信電話株式会社
「Webセキュリティ診断」

0120-446556

受付時間：午前9時～午後5時
（土曜・日曜休日・年末年始
（12月29日～1月3日）を除く）

ホームページ　https://business.ntt-east.co.jp/service/web-security-shindan/　Webセキュリティ診断　検索

NTT 東日本

安全なWebサイトの運営をNTT東日本がサポートします

Webセキュリティ診断

攻撃を受けると会社はもちろん、利用者であるお客さまにも迷惑をかけてしまいかねません。

あなたの会社にWebサイトがある限り、関係ないでは済みません。

Webセキュリティ診断で「もしも」を防ぎませんか？

脆弱性や改ざんの有無をNTT東日本が定期的に診断します

2020年に報告のあった
Webサイト改ざん件数

1,261件

出典：JPCERTコーディネーションセンター「JPCERT/CCインシデント報告対応レポート（2020年10月1日～12月31日）」「図5 Webサイト改ざん件数の推移」をもとにNTT東日本が算出

多いと思うか、少ないと思うかはあなた次第！

情報漏えい（例）

個人情報が攻撃者に不正に取得された！

悪意のある操作により、アプリケーションが想定しないSQL文を実行させ、データベースシステムを不正に操作する攻撃

サーバーに格納されているファイルが抜き出された！

Webサイトのディレクトリへアクセスすることで、同じディレクトリに格納されているファイルを不正に閲覧・取得する攻撃

勝手にサーバーに潜り込まれた！

プログラムに与えるパラメータにOSに対する命令文（コマンド）を紛れ込ませて不正に操作する攻撃

会社の機密情報が抜き取られた！

「../」を利用してディレクトリを遡り、本来はアクセスが禁止されているディレクトリにアクセスする攻撃

成りすまし（例）

本物そっくりのサイトが作られてフィッシング詐欺に！

攻撃者が作成したスクリプトを脆弱なWebサイトを介して、ほかのユーザのブラウザ上で実行させる攻撃

掲示板に犯罪予告の書き込み!?

不正サイトにアクセスしたユーザに、脆弱性のあるWebサイトへ不正なスクリプトを送信させる攻撃

改ざん（例）

Webサイトを見たお客さまがウイルスに感染！

アプリケーションの脆弱性等をつき、公開されているホームページに不正なリンクを埋め込む等の攻撃

これらの脅威をWebセキュリティ診断で防ぎましょう

6つの脆弱性診断 ＋ 改ざん検出

SQLインジェクション脆弱性診断

データベースと連携しているWebサイトで、データの不正な操作・取得につながる可能性がある脆弱性の有無を診断

1回／月　診断範囲：最大100パラメータ

ディレクトリインデックス脆弱性診断

ディレクトリに格納されているファイルの不正な閲覧・取得につながる脆弱性の有無を診断

1回／月　診断範囲：1URL（最大100ページ）

OSコマンドインジェクション脆弱性診断

攻撃者から悪意のあるリクエスト（OSへの命令）の要求を受け、不正に操作されてしまう脆弱性の有無を診断

1回／月　診断範囲：最大100パラメータ

ディレクトリトラバーサル脆弱性診断

公開されているトップディレクトリを遡り、非公開のファイルやフォルダに不正な操作が実行されてしまう脆弱性の有無を診断

1回／月　診断範囲：最大100パラメータ

クロスサイトスクリプティング脆弱性診断

悪意のあるスクリプトの埋め込みにつながる可能性がある脆弱性の有無を診断

1回／月　診断範囲：最大100パラメータ

クロスサイトリクエストフォージェリ脆弱性診断

リクエストを十分に検証せず受け取り、正規のリクエストとして扱い不正に実行されてしまう脆弱性の有無を診断

1回／月　診断範囲：お客さまが事前に指定したページ（最大100ページ）

改ざん検出

不正なリンクを埋め込む等の改ざんの有無を診断

1回／日　診断範囲：最大100ページ

診断対象　基本契約及び追加契約で指定したURLを起点とし、そのリンク先にあるページ（同一ドメイン内）を、上記「診断範囲」に定める範囲でNTT東日本が任意に選定

診断対象外　1.ログイン等、認証が必要なページ　2.日本語ドメインのURL　3.一部の携帯サイト等PCからインターネット経由でアクセスできない場合　4.診断対象のサイトにアクセスするために特別な機器やソフトウェアを用いる場合　5.JavaやFlash等のクライアントアプリケーションと連携したページ　6.ファイルアップロード（multipart）等のリクエスト形式のページ　7.画像ファイル、動画ファイル、PDF、Flash、圧縮ファイル等　8.パラメータのないWebアプリケーション　9.その他、起点となるURLからたどることができないページ、または、形式がHTML、JavaScript、スタイルシート以外であるページ　10.お客さまが診断対象外として指定したページ

Webセキュリティ診断は簡単利用！
詳しくは裏面をチェック

●パラメータとは、Webコンテンツ及びプログラムに対し動作条件を与えるための情報を指します。●脆弱性診断について、同一URL内であっても診断範囲を超えるパラメータについては診断を行いません。●本サービスの実施により診断対象のお客さまの問い合わせページ、電子メール送信ページ、登録ページ、掲示板等の動的コンテンツにおいては、実際にデータの登録、送信等が行われる場合があります。登録されたデータの削除や送信された電子メールの削除は、お客さまの責任において行っていただきます。また、データの登録、送信等により生じる結果については、当社は一切責任を負いません。●改ざん検出について、診断範囲を超えるページについては診断を行いません。●改ざん検出は暦日単位で1日に1度、診断を行います。●正常に診断を終了できなかった場合、脆弱性診断、改ざん検出ともに当日中に1回再度診断を実施します。また、再度診断を行っても正常に終了できなかった場合は、その旨を電子メールにて通知します。●その他サービスの詳細な内容や提供条件については、ホームページ（https://business.ntt-east.co.jp/service/web-security-shindan/）をご確認ください。