NTT ExCパートナー

＼わずか3ヵ月で／ ※JPCERT/CC インシデント報告対応レポート［2024 年 1 月 1 日～ 2024 年 3 月 31 日］

6,000件以上※のセキュリティインシデントが発生！

セキュリティインシデントの

ダメージは甚大！

企業サイトは**定期的**に**診断**しましょう！

企業のウェブサイトでセキュリティインシデントが発生すると「**顧客情報や、個人情報の漏えい／改ざん／破壊**」「**非公開情報の取得によるサーバー乗っ取り、なりすまし**」「**悪性サイトへの誘導による詐欺や情報窃取の発生**」など甚大な影響をもたらします。
その結果、**ウェブサイト自体が機能停止して利益が減少**したり、**社会的信用が低下**したりするだけでなく、**ランサムウェアを広める原因**になるなどしてセキュリティインシデント拡大の加害者となる可能性もあります。

企業サイトでセキュリティインシデントが発生すると・・・

！ 企業データベース内の顧客情報･取引先情報の

漏えい／改ざん／破壊

！ 閲覧しているお客さまの

個人情報の窃取

！ 閲覧しているお客さま本人が

意図しない投稿、決済行為の発生

！ 悪性サイトへの不正誘導による

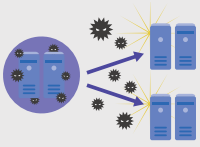
サポート詐欺や、情報窃取等の発生

！ セッションやログイン情報の窃取による

なりすまし・不正決済等の発生

！ 企業内サーバー／ネットワークへの

侵入口の構築



企業に甚大な悪影響が！

01 ウェブサイトの**機能停止**およびそれに伴う**利益の減少**

02 企業の**社会的信用の低下**

03 セキュリティ脅威**拡大の要因化**

セキュリティインシデント回避のためには定期的な診断が効果的！

NTT ExCパートナーのウェブセキュリティ診断

ウェブアプリケーション診断

ウェブアプリケーションに存在する問題点を検出します。

特徴	・信頼度が高く世界的にも活用されている OWASP アプリケーションセキュリティ検証標準に沿った 101 項目をチェック ・随時アップデートされる診断項目で、最新の脅威も検知 ・診断結果は情報処理安全確保支援士・CISSP・GPEN などのセキュリティのプロが分析。 対処すべき脅威の優先付けをするので、その後の対応方針を立てやすい
主な診断項目	・SQL インジェクション　・クロスサイト・スクリプティング ・OS コマンド・インジェクション　・セッションハイジャック ・クロスサイト・リクエスト・フォージェリ　・ディレクトリ・トラバーサル　・意図しないリダイレクト
期間	ご契約から 8 営業日～

※対象システムごとに金額は異なります。システムを調査したうえでお見積もりさせていただきます。
※詳細はウェブサイトをご確認ください。https://www.nttexc.co.jp/lp/web-security/

プラットフォーム診断／クラウドセキュリティ診断

プラットフォーム診断

・インターネット上に公開されているサーバーやネットワーク機器に対し、アクセス可能なポートを調査

・ポートスキャンで応答したポートに対し脆弱性スキャンを実施

クラウドセキュリティ診断

・クラウドサービス利用のセキュリティ設定に関する問題点を検出

・CIS ベンチマーク※ やクラウドベンダが提供するセキュリティのベストプラクティスに準拠した設定か否かを確認

※CIS ベンチマーク：CIS（Center of internet Security）が策定したサイバーセキュリティ防御を実装・管理するのに役立つガイドライン

診断実施の流れ

Step 01（無料）
診断対象の事前調査・お見積もり提示

セキュリティ技術者がお客さまのウェブサイトを巡回調査し、最適な診断プランとお見積もりをご提案いたします。

Step 02
ご契約

診断対象、診断内容、実施時期等を調整のうえ、ご発注いただきます。

Step 03
診断実施

経験豊富なセキュリティ技術者がお客さまのウェブサイトを診断します。

Step 04
診断結果のご報告

診断結果を報告書にてご報告いたします。報告会の開催も可能です。

お問い合わせフォーム
https://www.nttexc.co.jp/inquiry/solution/s014inp/

ウェブセキュリティ診断 特設ページ
https://www.nttexc.co.jp/lp/web-security/

株式会社NTT ExCパートナー ウェブセキュリティ診断事務局