CHUBU JIMUKI
co.,Ltd.

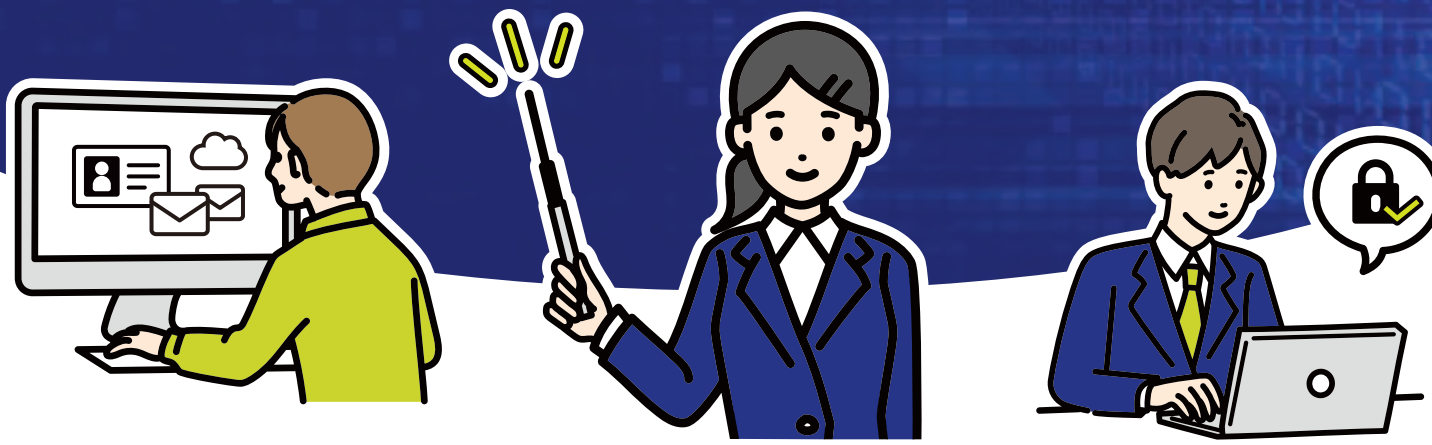
照~TE·RA·SU~ シリーズ

脆弱性診断サービス

“査”

セキュリティ上の弱点・問題点・欠陥を狙ったサイバー攻撃の増加

システムの脆弱性を狙い、webページの改ざんやデータの窃取と破壊、ウイルス感染といった被害が増加しています。ネットワークやOS、ミドルウェア、アプリケーションなどの脆弱性を診断し、セキュリティの現状を確認することで、悪意ある攻撃や情報漏えいなどのリスクを未然に防げます。



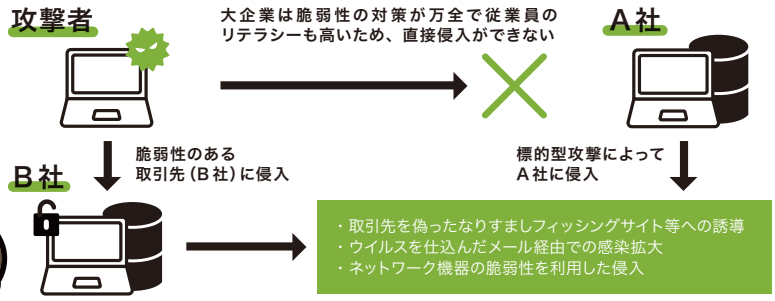
外部からサイバー攻撃をうけるリスクは、様々なシステムの脆弱性に隠れています。

- ソフトウェアの脆弱性
- ハードウェアの脆弱性
- ネットワーク脆弱性

セキュリティ対策の脆弱性を狙った攻撃の手法

取引先である企業を経由し不正侵入するサイバー攻撃

流通の中で関わった企業へと侵入して、本命である大企業や親会社へ攻撃を仕掛けるサイバー攻撃が増加しており、その脅威は年々着実に高まってきています。取引先を介してセキュリティ対策の不備をつく手法が「サプライチェーン攻撃」です。



サプライチェーン攻撃のしくみ

セキュリティに敏感な大企業は自社のセキュリティ構築に注力しています。自社の防御をどれだけ堅牢にしたとしても、取引先企業のどこかに穴があれば、そこから侵入され攻撃される可能性があります。
日本では、９割以上がいわゆる中小企業です。その大半はコストや人的な要因で十分なセキュリティ対策ができておらず、サイバー攻撃に対して非常に脆弱であるのが現状であるため、ターゲットとして中小企業が狙われています。

システムのセキュリティ強化には現状の脆弱性を把握することが重要です！

脆弱性診断サービスのご提案

お客様の状況に応じて、2つの手法で診断いたします。

脆弱性診断とペネトレーションテストのサービス内容

システム全体を網羅的に確認

脆弱性診断

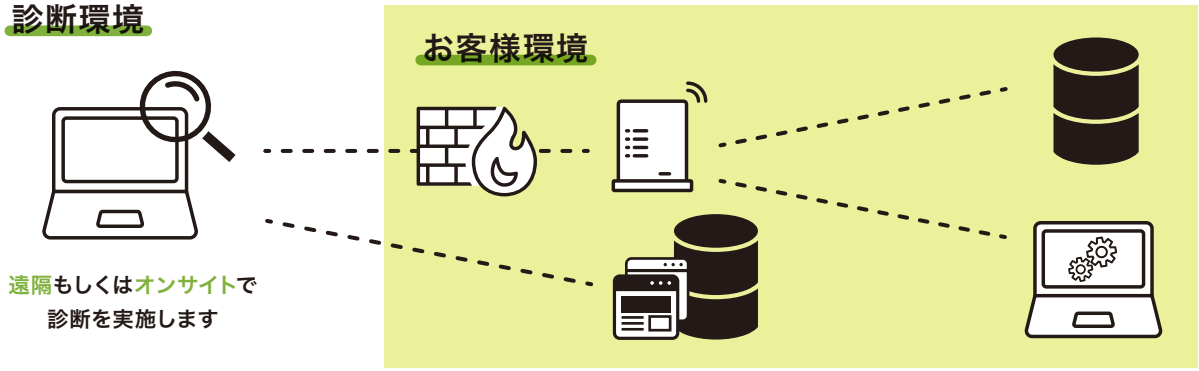
ツールもしくは人的な診断を行います。
特定のサーバ、ネットワーク機器に対する脆弱性を診断します。

現実的な攻撃シナリオを用いて攻撃耐性を確認

ペネトレーションテスト

シナリオを設定して対象のサーバ、ネットワーク機器に対して攻撃を行います。どこまで侵入できるのか、ウィルス感染した場合にどこまで感染するのか調査する方法です。

診断イメージ



診断の対象となるもの

- ネットワーク機器（主にルータ/ファイアウォール）
- 公開サーバ
- サーバ（アプリ・システムなど）

診断結果の報告と対策

検出した脆弱性に対して対策措置を実施することで、セキュリティレベル向上に役立てる事を目的として実施します。
診断後、対策措置を実施し、脆弱性を無くしていくことがサイバー攻撃などの脅威に対するセキュリティレベル向上に直結します。

脆弱性診断だけにとどまらず、結果に基づいて実施すべき対策を提示します。

脆弱性診断サービス“査”は、

システムに隠れている脆弱性を洗い出し、リスクを明確にすることで、未然に攻撃を防ぐためのセキュリティ対策をご提案いたします！

CHUBU JIMUKI co.,Ltd.
〒500-8309 岐阜県岐阜市都通 1 丁目 15 番地
TEL：058-251-7191（代表）
FAX：058-255-0011

■大垣支店
〒503-0854 岐阜県大垣市築捨町 5 丁目 69-1
TEL：(0584) 89-0711　FAX：(0584) 87-0145

■尾張支店
〒483-8227 愛知県江南市赤童子町良原 165 番地 1
TEL：(0587) 58-6688　FAX：(0587) 58-6707

■東濃支店
〒509-0222 岐阜県可児市羽崎 495-1
TEL：(0574) 62-8490　FAX：(0574) 62-8491

■多治見営業所
〒507-0042 岐阜県多治見市前畑町 2 丁目 13 番地フロイデ 1 階 事務所
TEL：(0572) 26-7702　FAX：(0572) 26-7703

はたらくを、かえる。未来が、かわる。