GUARDIAN NET

まずは

セキュリティ診断

しませんか？

対策の前に“現状把握”ー

自院のセキュリティリスクを知ることが、最適な対策への第一歩です。

実際に起きているサイバー攻撃の被害

ランサムウェアによる診療停止

ランサムウェアに感染し、
診療データが暗号化。
診療や予約システムが停止し、
業務がストップするケースも。

診療・予約システムが停止

情報漏洩による信用の失墜

患者情報の流出や
不正アクセスにより、
信用を失い、医院の存続に
影響を及ぼすリスクも。

患者情報の流出・不正アクセス

復旧費用
500万円超のケースも

システム復旧やデータ復元、
機器の再導入などにより、
500万円を超える費用が
発生するケースもあります。

復旧費用は
500万円超のケースも

サイバー攻撃は年々増加
歯科医院も「標的」に
なっています

まずは、
セキュリティの現状を知る
ことから始めましょう。

1 セキュリティ診断でわかること

専門的な診断で、院内のセキュリティ状況を多角的にチェックします。

PC管理	レントゲン	バックアップ	Wi-Fi	権限管理	ウイルス対策
PC・端末管理 OSやソフトの更新 状況など	レントゲン・医療機器 ネットワーク接続の 脆弱性確認	バックアップ データの保存状況 ・復旧手順の確認	院内ネットワーク 不正アクセスの リスク確認（Wi-Fi）	アカウント・権限管理 ユーザー権限や パスワード管理	ウイルス対策・全般 ウイルス対策ソフト 設定や運用状況

診断で現状を可視化。 無駄な投資を防ぎます。

2 診断結果から 本当に必要な対策が分かります

やみくもにすべてを導入するのではなく、本当に必要な対策だけをご案内いたします。

診断結果イメージ

総括
『危険度 高』レベルが４件、
『危険度 中』レベルが５件と
大きな脆弱性が発見されました。

危険度 ： 中
概要 リモート操作でTCP123番ポートに接続すると、 プログラム等のサービス実行状況を取得されることがあります。
脆弱性検出結果 TCPプロトコルを介して多くのサービスが 実行されていることが検出されました。
影響 実行されているサービスに脆弱性が存在する場合、リモート 操作によりサーバー情報の窃取・サービス運用妨害攻撃・ 悪意のあるプログラムを実行される等の可能性があります。
解決策 ファイアウォールなどでTCP123番ポートへのアクセスを適切に 制御する必要があります。具体的には信頼できるIPアドレスや ネットワークからのアクセスのみを許可し、不要なアクセスは 遮断するように設定します

やみくもに導入すると…

コストがかかる・運用が複雑になる・効果が不明確

診断結果に戻づく最適投資

必要な対策だけを導入

✅コストを最小化
✅運用負担を軽減
✅効果を最大化

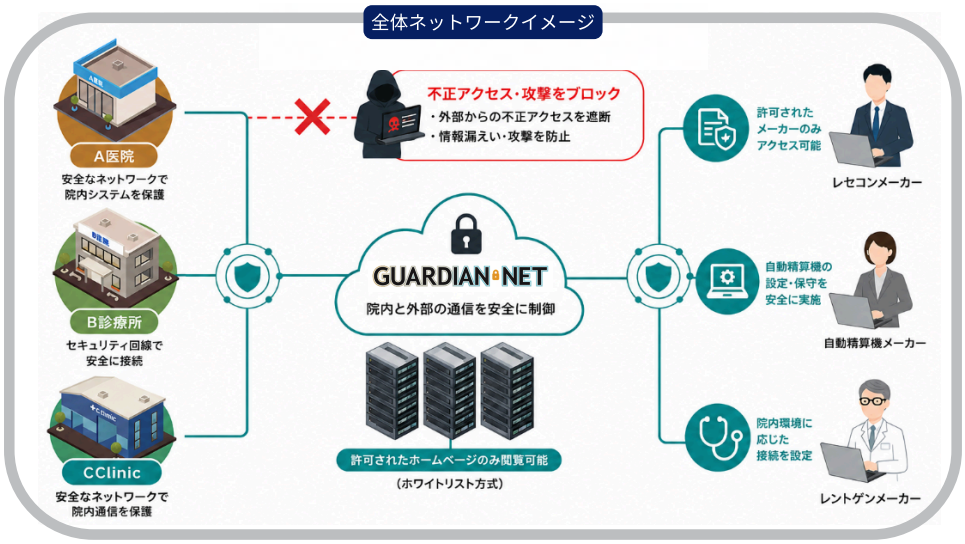
3 "GUARDIAN.NET"なら診断から導入・運用までワンストップでサポート

歯科医院さまのための
クラウド型セキュリティサービス

GUARDIAN NET
ガーディアンネット

STEP 1 お問合せ　STEP2 診断　STEP3 提案　STEP4 導入

何を導入すべきか迷わない。 診断から運用までお任せください。



※行政機関の通達に即したネットワークです

安心 １０年以上の公的クラウドサービス提供実績

安全 外から攻撃されない閉ざされたネットワーク

安価 個別のセキュリティ対策が不要

GUARDIAN.NETの特徴

各医院様は繋ぐだけ	クラウドで一括防御	24時間365日フル監視	安全な通信のみ許可	医院様の運用負担ゼロ
複雑な設定不要で簡単に導入可能	全ての医院様をクラウド上で厳重管理	常時監視を行い、脅威を即時探知・対応	不正なアクセスや通信を自動でブロック	手間なく安心して診療に集中できる

無駄投資ゼロ・運用負担ゼロ・専門知識ゼロ

まずは、セキュリティ診断で現在のリスクを可視化！

GUARDIAN NET

まずは！

セキュリティ診断受付中

大切な患者様と医院を守る為に
右記ＱＲよりご相談下さい

- 現状を把握したいかた
- リスクを知りたいかた
- 何から始めれば良いか迷っているかた

スマホで簡単アクセス！

販売元