サイバー攻撃対策通信

令和７年２月27日
令和６年度第６号
栃木県警察本部
警備部警備第一課

CAUTION CAUTION CAUTION CAUTION CAUTION

今、医療機関が狙われている

県内医療機関、ランサムウェア被害

2025年2月、県内の医療機関がサーバに不正アクセスされるサイバー攻撃を受けて、ランサムウェアによりデータが暗号化され、**患者などの個人情報が最大30万人分流出した可能性**があり、一時診療業務が停止するなど、深刻な影響を受けました。

なぜ医療機関が狙われるのか・・

- **資金力**があり**人命を優先**する（身代金要求に応じ易いと攻撃者が認識）
- **患者の個人情報や医療情報**など、情報資産価値が高い
- **外部機器や業者とネットワーク共有**していることが多く脆弱性が突かれ易い
- **セキュリティ対策に十分な予算や人材を確保できていない**

サイバー攻撃対策の重要ポイントは・・

病院のサイバー攻撃対策において最も重要なポイントは、

1　技術的対策の実施
- OSやソフトウェアの最新バージョンへのアップデート
- セキュリティソフト導入とファイアウォールの最適化
- データの暗号化とバックアップの定期的な実施

2　従業員教育の徹底
- セキュリティ意識の向上
- パスワードポリシーの策定と運用

3　早期検知システムの導入
- NDRなどを活用し、侵入後の脅威に対して早期検知や隔離・除去

4　インシデント対応計画の策定
- BCP（事業継続計画）の一部として、緊急時の対応等の整備

5　包括的な資産管理
- 医療IT/OTシステムと相互作用するあらゆる資産とアカウントのリスト化と管理

などが挙げられます。

厚生労働省のホームページに、
「医療分野のサイバーセキュリティ対策について」
が掲載されていますが、
今一度チェックリスト等確認し、
その運用に遺漏なきようお願いいたします。

厚労省　サイバー

TPCCAT
Tochigi Police Counter Cyber Attack Team

CAUTION CAUTION CAUTION CAUTION CAUTION

CAUTION CAUTION CAUTION CAUTION CAUTION

医療機関に対するランサムウェア攻撃は、世界的に増加しており、国内でも多くの機関が甚大な被害に遭っています。

～国内における主なランサムウェア攻撃発生事例～

岡山県の精神科医療センター（2024年５月）

被害　・電子カルテを含む病院情報システムが完全に機能停止
・最大約４万人分の患者情報が流出した可能性
・バックアップデータが攻撃者によって破壊され、復旧が困難に

原因　・ＶＰＮの脆弱性の放置

鹿児島県の病院（2024年３月）

被害　・画像管理サーバが正常に運用できなくなった
・診療記録のＰＤＦファイルの一部が暗号化された

原因　・認証なしでリモートデスクトップ接続可能
・画像管理サーバにウイルス対策ソフトが未設定

大阪府の総合病院（2022年10月）

被害　・基幹システムサーバの大部分が暗号化され、完全復旧まで約２か月を要し、経済的損失は数十億円

原因　・給食事業者のＶＰＮの脆弱性の放置（サプライチェーン攻撃）

徳島県の病院（2021年10月）

被害　・電子カルテなどの端末や関連サーバのデータが暗号化され、使用不能
・復旧に２か月以上要した

原因　・ＶＰＮの脆弱性の放置
・Windowsアップデート自動更新無効
・Windowsファイアウォールの無効化
・Windows Defenderの無効化
・サポート終了したWindows７の利用
・ドメインユーザが管理者グループに所属
・ベンダーとの契約書に脆弱性情報の通知に関する記述がない
・ウイルス対策ソフトが未稼働
・ログイン試行回数制限を設定せず
・認証用パスワードが最短５桁
・USBメモリの運用ポリシーなし

基本を怠った事業者が
被害に遭っています！
自組織のセキュリティ対策を再確認し
不備があれば
直ちに対策して下さい！！

CAUTION CAUTION CAUTION CAUTION CAUTION