2022 年 2 月 16 日

Venture Solution

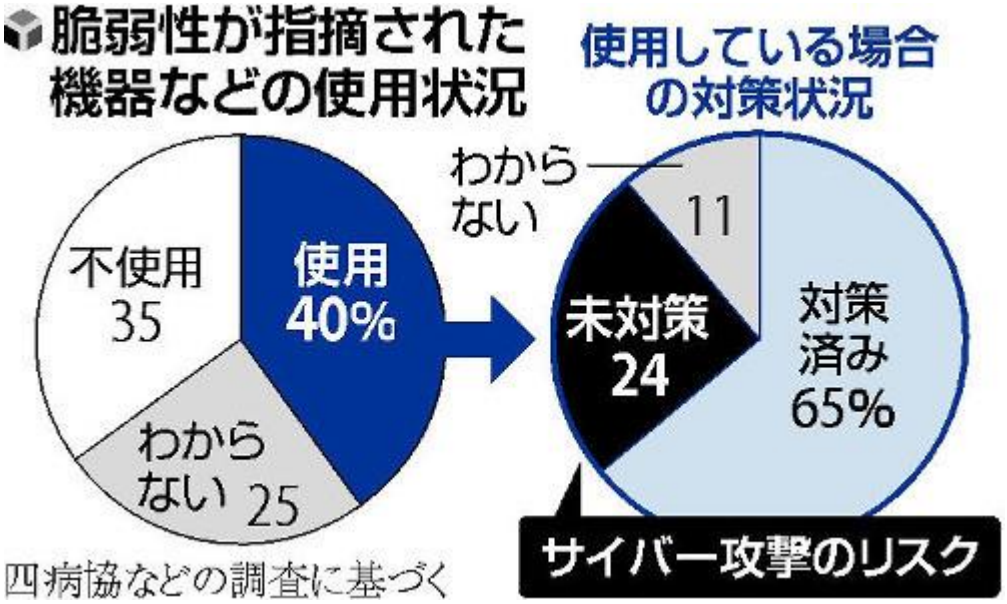
コラム記事

被害にあうリスクが高いと理解しつつも、人手不足により対策が追い付いていないケースが多いと報告されています。
特にほとんどの病院では電子カルテの導入を進めており、アナログ管理からデジタル管理へ切り替わっています。
ランサムウェアによるウイルス感染では、病院のシステムが停止し復旧にかなりの時間を要してしまう恐れがあるため、「感染したことがないから、まだ大丈夫」ではなく「感染を未然に防ぐ対策」をすぐに取れるよう意識・準備することが重要であると考えています。
そこで、病院に特化したセキュリティー対策に関する記事が掲載されておりましたのでご紹介いたします。

病院の１割、対サイバー攻撃「脆弱機器」を未対策のまま使用…９割「脅威感じる」が対策追い付かず

（読売新聞オンライン 2/16(水) 5:03 配信 より引用）

全国の病院を対象に実施されたサイバーセキュリティー調査で、約１割の病院がサイバー攻撃への脆弱（ぜいじゃく）性を指摘された機器などについて、適切な対応を取らないまま使用していることがわかった。ランサムウェアと呼ばれるウイルスで病院のシステムが停止する被害が相次ぐ中で、対策の遅れが明らかになった。



（写真：読売新聞）

（読売新聞オンラインより引用）

病院団体でつくる「四病院団体協議会」（四病協）と一般社団法人「医療ＩＳＡＣ（アイザック）」が緊急調査を行った。
1 月 31 日から、加盟する 5,596 病院を対象に調査を実施し、今月 10 日までの中間報告を取りまとめた。
回答を寄せたのは 476 病院。

国が、脆弱性を指摘した製品のうち、外部から病院のシステムに接続する際に使う「ＶＰＮ」などを使用していた病院は 40%あり、このうち、対策を取っていない病院は 24%だった。全体の約 1 割が、被害に遭うリスクが高い状態にあった。

「サイバー攻撃の脅威を感じる」と答えた病院が全体の 90%に達する一方で、セキュリティー予算については 46%が「十分でない」と回答。危機意識に対策が追いついていない実情が浮かんだ。

（写真：厚生労働省）（読売新聞オンラインより引用）

電子カルテシステムが被害に遭った病院では、オンラインで接続していたバックアップも含めて感染した事例もあり、復旧が長期化している。調査では、98％の病院でバックアップを取得していたが、ネットワークから遮断したオフラインで保管していたのは 47％にとどまった。

厚生労働省も 1 月下旬から、全国の病院に脆弱性が指摘された機器の使用状況や、バックアップの取り方に関する調査を実施している。調査結果を踏まえ、各病院に個別に改善を促す。

サイバー攻撃を受けているのは病院だけではありません。
ですが、記事にある通り院内で使用されている機器において脆弱性を理解しながらも、対策を打てていない病院が多く存在することも事実だと感じています。
病院および関連企業へのサイバー攻撃の報告事例は増え続けているため、脆弱性を理解するとともに必要な対策を
検討できるような情報共有や人材確保の必要性が高まっていると考えております。