医療分野のサイバーセキュリティ対策について

医療機関におけるITシステムの現状

近年、医療機関においても電子カルテ、診療予約システム等のITシステムの導入が進み、医療機関と患者の双方に様々なメリットをもたらしています。

しかしながら、新型コロナウイルスが感染拡大するなか、国際的に医療機関へのサイバー攻撃が増加しています。

海外の医療機関では、ランサムウェアと呼ばれるコンピュータ・ウイルスに感染し、院内システムの停止により患者の死亡へつながる事案も発生しています。

国内の医療機関もサイバー攻撃の標的となるおそれが高まっています。

重要情報の漏洩　重要情報の改ざん　医療システムの停止

↓

セキュリティリスクの増加

サイバーセキュリティの脅威

サイバーセキュリティの脅威となるサイバー攻撃の例をいくつか紹介します。

標的型メール攻撃

「標的型メール攻撃」とは、特定の個人や組織、情報を狙って、知人、取引先などを装いメールなどを送る攻撃です。

本物と区別がつきにくい文面で騙し、不正なサイトへの誘導やメールに添付されたファイルを開かせてコンピュータ・ウイルスに感染させるなどします。

安易に添付ファイルを開かない、相手方への事実確認などを行いましょう。

ランサムウェア

「ランサムウェア」とは、コンピュータ・ウイルスの一種で、感染するとコンピュータ内のデータを暗号化し、データ回復の為に「身代金」を要求します。

システムを常に最新に保ち、定期的にデータのバックアップをとり、復旧できる体制を整えましょう。

身代金を支払ってもデータが復元される保証はありません。

フィッシング攻撃

「フィッシング」とは、宅配の不在通知、通販サイトからの料金請求などを装って騙し、ＩＤ・パスワードやクレジットカード番号などを盗み取る手口のことです。

メールの本文やURLに不審な部分がないか、よく確認し、パスワード等の入力は、公式アプリやブックマークに登録している正規のアドレスから行いましょう。

ＤＤｏＳ攻撃

「DDoS（Distributed Denial of Service）攻撃」とは、複数のコンピュータから標的のサーバに大量のデータを送りつけて応答不能にし、サービスを停止させる攻撃です。

ファイアウォールなどDDoS対策機器の導入など、適切な対処方法を取ることで、リスクを低減できます。

ウェブサイトの改ざん

ID とパスワードの流出による不正アクセスや、サーバの脆弱性を突いて、ウェブサイトの情報を改ざんし、偽情報の表示やコンピュータ・ウイルスを拡散させるなどの被害が発生します。

ウェブサイトの脆弱性は定期的に確認し、脆弱性がある場合は、速やかに修正パッチ等を適用しましょう。

パスワード攻撃

予想しやすいパスワードを使用して攻撃する「辞書攻撃」やありそうな文字列などを総当たりで試みる「総当たり攻撃」など、様々な攻撃方法があります。

予想されにくいパスワードの使用と適切な管理、生体認証の導入、不正アクセスの検知など対策をとりましょう。

サイバー攻撃による被害発生の影響

サイバー攻撃により被害が発生した場合、様々な影響が考えられます。

患者のプライバシー侵害

患者の個人情報等、重要な情報が漏洩することによって、患者や社会からの信用を著しく失墜してしまいます。

診療業務の停止

サイバー攻撃により医療系のＩＴシステムが停止することによって、通常の診療業務が予期せず停止してしまう可能性があります。

インシデント対応における負荷

インシデントの対応に多くの時間を要する可能性があり、それが診療業務や経営への大きな負荷になってしまいます。

サイバーセキュリティ対策

サイバーセキュリティの脅威に対し、日頃の対策を心がけましょう。

メールの添付ファイル

業務でメールを使用する際には、例え取引先や知り合いからのメールでも、添付ファイルをむやみに開かないようにしましょう。

件名や内容が不自然ではないかを確認したり、送信者に対してメール送信の事実の有無を確認するなどして、標的型メール攻撃の被害防止に十分留意しましょう。

外部メディアの使用

例えインターネットに接続していない端末でも、USBメモリやSDカード等の外部メディアを媒介してウィルス感染するおそれがあります。

また、機密情報等を保存した外部メディアを紛失する等のリスクもあります。

使用する際は、組織のルールを遵守し、持ち出す情報も必要最低限にしましょう。

セキュリティソフトの導入

基本的なことですが、ファイアウォールやウィルス対策ソフトを導入しましょう。

ウィルス対策ソフトは、パターンファイルの更新をこまめに行い、定期的に端末等のファイルスキャンを実行することにより、気づかずにウィルスに感染していた場合でも、被害を最小限に食い止めることが期待できます。

不測事態発生時の連絡

不測事態が発生した場合、早急に組織内の担当部門に連絡し、担当者の指示に従いましょう。

決して自分だけで判断したり対応したりしないようにしてください。

また、予め組織内の担当部門の連絡先を把握しておくことも、発生した事案に円滑に組織的対応をする上で重要です。

ひと、くらし、みらいのために
厚生労働省
Ministry of Health, Labour and Welfare

厚生労働省ホームページ（医療分野のサイバーセキュリティ対策について）
https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html

サイバー犯罪被害防止6か条

①導入しようウィルス対策ソフト　④転ばぬ先のバックアップ
②ソフトは常に最新に　⑤使い回しダメ・ゼッタイ
③開けるな危険！不審メール　⑥悩む前にまず相談

岡山県警察本部
サイバー犯罪対策課
☎（０８６）２３４－０１１０
https://www.pref.okayama.jp/soshiki/331/