医療機関を取り巻く情報セキュリティ対策の現状

【お知らせ】
医療機関等にて情報セキュリティの教育研修を円滑に実施できるよう映像教材を公表しています。
医療機関等で働く皆様に是非意識して頂きたい、医療情報のセキュリティの基礎的な考えについて動画としてまとめました。
医療機関等におけるサイバー攻撃対策の一環としてご活用ください。

・医療機関等向けサイバーセキュリティ研修用動画（ショート版）
・医療機関等向けサイバーセキュリティ研修用動画（フル版）

情報セキュリティ対策はシステムを利用する全職員で対応すべき問題

例えば、普段使うパソコンが、ある日突然見たことのない画面に変わっていたら、あなたはどう対応しますか？

対応方法は把握されていますか？
院内で対応方法は構築されていますか？
情報システム部門に電話しますか？

原因は、あなた宛に届いたウイルスが添付されたメールを開いてしまったからかもしれません。もしくは、システムの脆弱性を狙って、外部の誰かが内部システムに侵入し、攻撃をしたのかもしれません。

最近ではこのような外部からの攻撃により、医療情報システムが停止し、診療ができなくなった事例も発生しています。いずれにせよ、病院の情報セキュリティ対策は情報システム部門だけの問題ではなく、システムの利用者である経営層、医師、コメディカル、事務スタッフ等の全てのシステム利用者の問題です。

「予防できる疾病（コンピューターウイルス）」は可能な限り予防し、発症（感染）してしまった時の対応を事前に検討し、訓練することが、情報セキュリティ対策においても重要です。

情報セキュリティインシデントとは何か

院内の情報化の進展により、医療機関は様々な情報システムの導入や院外ネットワークとの接続を行っています。院内における情報セキュリティ対策が不十分である場合、様々な情報セキュリティインシデントリスクの脅威にさらされている可能性があります。

例えば、医療機関における情報セキュリティインシデントとしては以下のようなことが考えられます。

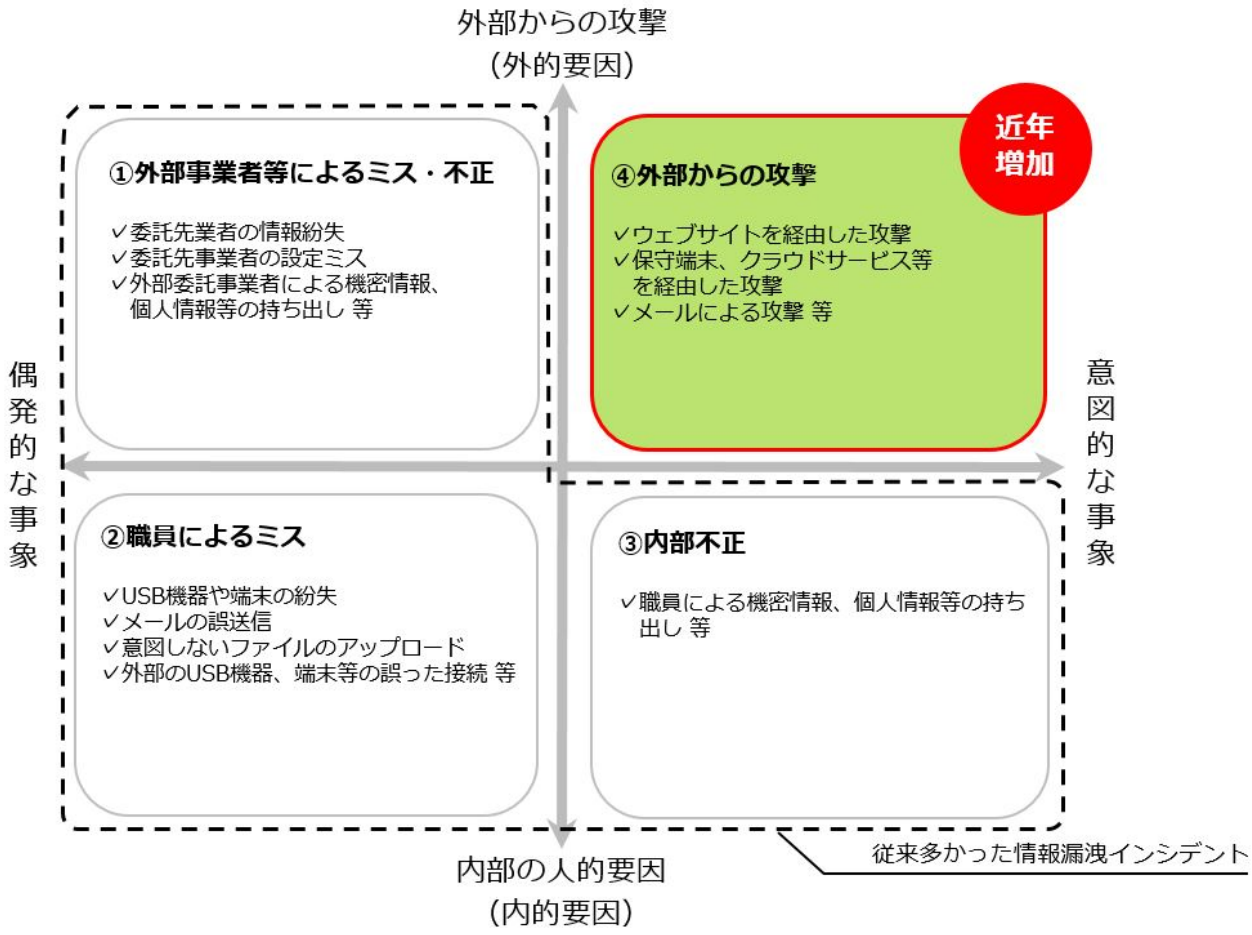
①外部事業者等によるミス・不正
診療系ネットワークはクローズドなネットワークであるが、クラウドサービス、保守事業者等との接続回線から侵害される可能性がある。侵害された場合、システム内にて、データの窃取や漏えい、破壊等の横断的侵害行為が行われる可能性がある
②職員によるミス
USB機器や端末等の紛失による情報漏えいの可能性がある
③内部不正

業務とは関係のない患者のデータ参照、機密情報・個人情報等の持ち出しが考えられ、情報流出の可能性がある

④外部からの攻撃

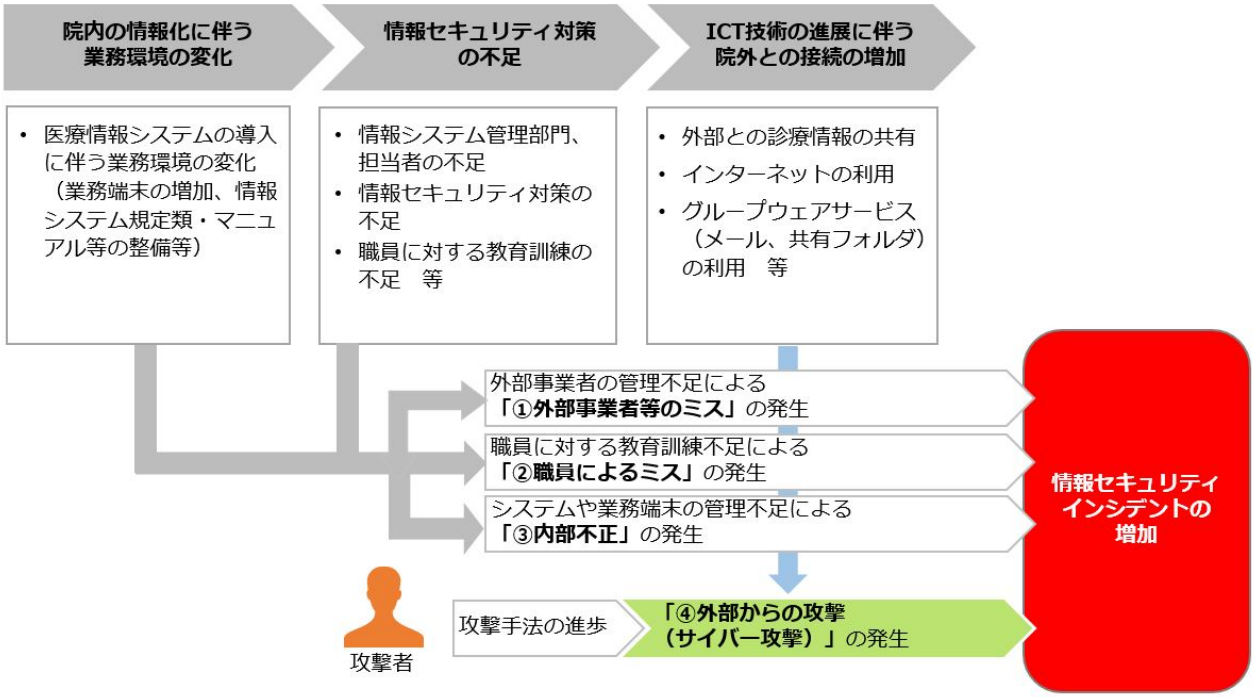
ランサムウェアと呼ばれるマルウェア「WannaCry」が代表的。感染すると端末ロックやファイル暗号化により端末が利用不能となる。また、感染した業務端末から、攻撃可能な端末等を検索し、自ら拡散する性質を持っていることから、他の業務端末にも感染が拡大する恐れがある

従来は、「職員によるミス」「内部不正」が多くみられましたが、近年は「外部からの攻撃」つまり「サイバー攻撃」が増加傾向となっています。



医療機関の情報化に伴う業務環境の変化に対して十分な対策がとれていないことや、攻撃者の手法の進歩により、情報セキュリティインシデントは増加傾向にあります。

医療機関における情報化の動向



情報セキュリティ対策は、情報システム部門の課題だけではなく、医療機関の事業継続や存続に影響する経営課題でもあります。

情報セキュリティ対策における構成

情報セキュリティ対策における構成は、「組織的対策」「人的対策」「技術的対策」「物理的対策」であり、患者への医療サービスの品質向上（医療安全対策）においても、同様の構成です。

情報セキュリティ対策は、患者への医療サービスの品質向上（医療安全）と同様に、各職種で対応する必要があり、「組織的対策」「人的対策」「技術的対策」「物理的対策」のうち、いずれかの対策が欠けても、全体の有効性は欠けた部分と同じく、最も低い水準となります。

情報セキュリティ対策の構成と対策例

組織的対策	• 情報システム部門の設置、体制強化 • 情報システム等に係る規定の策定　等
人的対策	• 情報システム部門との情報共有の強化 • 職員への教育訓練 • 外部委託先の管理　等
技術的対策	• ファイヤーウォール、ウイルス対策ソフトの導入 • 定期的なログの確認・分析　等
物理的対策	• 入退館（室）管理の実施 • 重要な端末等への盗難防止用チェーンの設置 • 端末等の覗き見防止の対策　等

これから対策を実施する場合

最初に講じる対策は、組織的対策となる「情報システム部門、または、担当者」の設置です。情報セキュリティは、専門領域であり組織的対策を病院内部で講じることが難しい場合、アウトソーシングサービスへの相談・委託を含めて、対策の検討を行うことが望ましいでしょう。

対策を実施済の場合

情報セキュリティ対策の対応ができている場合は、情報システム監査を受審することで、情報システム運用管理に関する継続的な管理を実施することが望ましいでしょう。

情報セキュリティ対策の必要性を理解し、「経営層」「情報システム部門」「システム利用者」について、自らが継続的に対策を講じることが必要不可欠であるといえます。

TOPへ戻る

ページの先頭へ戻る

- 医療情報連携ネットワークはなぜ必要？
  - 出発点は地域医療を良くしたいという思い
  - 医療情報連携ネットワークの導入効果
  - 利用者の声（導入効果）
- 医療情報連携ネットワークをどう作る？
  - 医療情報連携ネットワークの構築手順
  - 実施のポイント
  - 利用者の声（苦労した点、成功要因）
  - ガイドライン、書式例など
- 医療情報連携ネットワークの具体例を見る

- 医療情報連携ネットワークとは
- データで見る
- ピックアップ事例
- 事例を探す
- 構築手順
  - 構築手順について
  - Step1：計画
  - Step2：構築
  - Step3：運用
  - Step4：更改
- FAQ
- 用語集
- お役立ち情報
  - リンク集
  - 資料ダウンロード

プライバシーポリシー・免責事項 | お問い合わせ |