医業経営情報

REPORT

Available Information Report for Medical Management

医業経営

組織的・技術的
安全対策で守る

医療機関のサイバーセキュリティ対策

1 広がる医療機関へのサイバー攻撃
2 医療情報システムに関するガイドラインの概要
3 ランサムウェアによる被害実例
4 院内で取り組むべきサイバーセキュリティ対策

2022
9
SEP

税理士法人　森田会計事務所

1 | 広がる医療機関へのサイバー攻撃

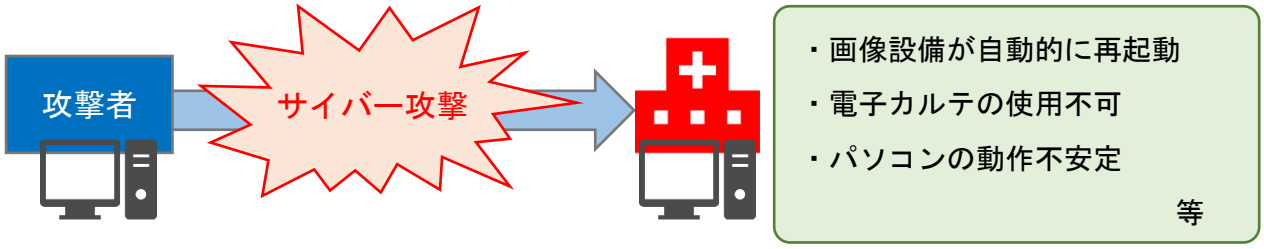
昨今、医療業界では電子カルテの導入等「医療機関のIT化」が進み、業務の効率化には欠かせないものとなっています。しかし、それに伴った情報セキュリティに関する事故は、医療機関自体の存続に大きく影響する経営課題となっており、サイバーセキュリティは医療機関の規模に関わらず、経営者にとって軽視できない分野です。

本レポートでは、医療機関のサイバー攻撃がどのようなものかに触れ、厚生労働省のサイバーセキュリティ対策に関する様々なガイドラインや、被害にあった医療機関の実例をみながら、今後医療機関が取り組むべきサイバーセキュリティについてご紹介します。

1 | 医療機関に対するサイバー攻撃

サイバー攻撃と一口に言っても、コンピュータへの不正アクセスによる情報流出や端末動作の不安定化等、その内容は様々です。具体的には、CTやレントゲン等で撮影した画像を保存することができなくなる、ランサムウェア攻撃により電子カルテが使用できなくなる等、診療に直接影響が出る事例があります。このように日本国内だけではなく、世界各国の医療機関でサイバー攻撃による被害が発生しています。

◆サイバー攻撃のイメージ



2 | ランサムウェアとは

ランサムウェアはRansom（身代金）とSoftware（ソフトウェア）を組み合わせた造語です。ランサムウェアに感染したコンピュータのロックや、内部ファイルを暗号化することによって使用不能にした後に、元に戻すことと引き換えに「身代金」を要求する悪意のあるソフトウェアです。また、昨今のランサムウェア攻撃の中には、コンピュータを使用不可にするだけではなく、情報を事前に盗み取った上、「身代金の支払いがなければ情報を暴露する」と脅迫する手法も存在しています。

◆ランサムウェアによる攻撃のイメージ

3 診療所の医療情報システムの管理体制

日本医師会総合政策研究機構では、2021年４月に医療機関における情報システムの管理体制の実態把握を目的とした全国調査を実施し、結果を公表しました。対象は病院約5,000施設と診療所約5,000施設で回収できたのは2,989施設、全体の30.4%となりました。

調査項目の「院内システムの院内外への接続状況について」への回答は、「電子カルテ」や「医事会計システム」等のシステムごとに集計されています。診療所の医事会計システムの接続状況について見てみると、「インターネットと接続している」と回答しているのが全体の42.6%であることがわかりました。また、診療所の電子カルテの接続状況についてみると、全体の26.4%が「インターネットと接続している」と回答しています。

インターネットと接続するということは外部ネットワークと接続されている状態であり、コンピュータ自体のセキュリティが万全であっても、場合によってはコンピュータが危険な状態にさらされ、外部へ情報が漏洩する可能性があります。

◆院内システムの院内外への接続状況（医事会計システム）

		全体	貴院内の他のシステムやインターネットとの接続はしていない	インターネットとは接続していないが、貴院内の他のシステムと接続している	貴院内の他のシステムとは接続していないが、インターネットと接続している	貴院内の他のシステムとインターネットの両方に接続している	このシステムは使っていない
全体		(2989)	654 21.9	1347 45.1	368 12.3	456 15.3	164 5.5
病床規模	診療所	(1400)	351 25.1	310 22.1	279 19.9	318 22.7	142 10.1
	病院　20～199床	(979)	232 23.7	547 55.9	79 8.1	105 10.7	16 1.6
	病院　200～499床	(463)	65 14.0	356 76.9	10 2.2	26 5.6	6 1.3
	病院　500床以上	(147)	6 4.1	134 91.2	0 0.0	7 4.8	0 0.0

出典：日本医師会総合政策研究機構　「医療機関の情報システムの管理体制に関する実態調査」

◆院内システムの院内外への接続状況（電子カルテシステム）

		全体	貴院内の他のシステムやインターネットとの接続はしていない	インターネットとは接続していないが、貴院内の他のシステムと接続している	貴院内の他のシステムとは接続していないが、インターネットと接続している	貴院内の他のシステムとインターネットの両方に接続している	このシステムは使っていない
全体		(2989)	205 6.9	1204 40.3	90 3.0	379 12.7	1111 37.2
病床規模	診療所	(1400)	136 9.7	319 22.8	77 5.5	293 20.9	575 41.1
	病院　20～199床	(979)	51 5.2	423 43.2	7 0.7	60 6.1	438 44.7
	病院　200～499床	(463)	14 3.0	327 70.6	6 1.3	20 4.3	96 20.7
	病院　500床以上	(147)	4 2.7	135 91.8	0 0.0	6 4.1	2 1.4

出典：日本医師会総合政策研究機構　「医療機関の情報システムの管理体制に関する実態調査」

また、診療所の情報システムの管理体制について見てみると、専任の担当部門または委員会等を設置している診療所の割合は全体の4.4%でした。ほとんどの診療所が、兼務の担当者や院長自らが管理している状態にあります。特に院長は経営や診療にも携わることが多いことから、情報システムの管理を積極的に行うことは困難であり、多くの診療所がサイバーセキュリティに関して十分な対策がされていないことがわかります。

◆情報システムの管理体制

		全体	専任の担当部門がある	専任の担当部門はないが、委員会等を設置している	専任の担当部門や委員会等はないが、専任の担当者がいる	専任の担当部門、委員会等や専任の担当者はいないが、兼務の担当者がいる	上記のような管理体制はなく、院長が自ら管理している
全体		2,989	617 20.6	244 8.2	191 6.4	993 33.2	944 31.6
病床規模	診療所	1,400	42 3.0	19 1.4	73 5.2	365 26.1	901 64.4
	病院　20～199床	979	201 20.5	161 16.4	82 8.4	495 50.6	40 4.1
	病院　200～499床	463	245 52.9	55 11.9	35 7.6	125 27.0	3 0.6
	病院　500床以上	147	129 87.8	9 6.1	1 0.7	8 5.4	0 0.0

出典：日本医師会総合政策研究機構　「医療機関の情報システムの管理体制に関する実態調査」

2 医療情報システムに関するガイドラインの概要

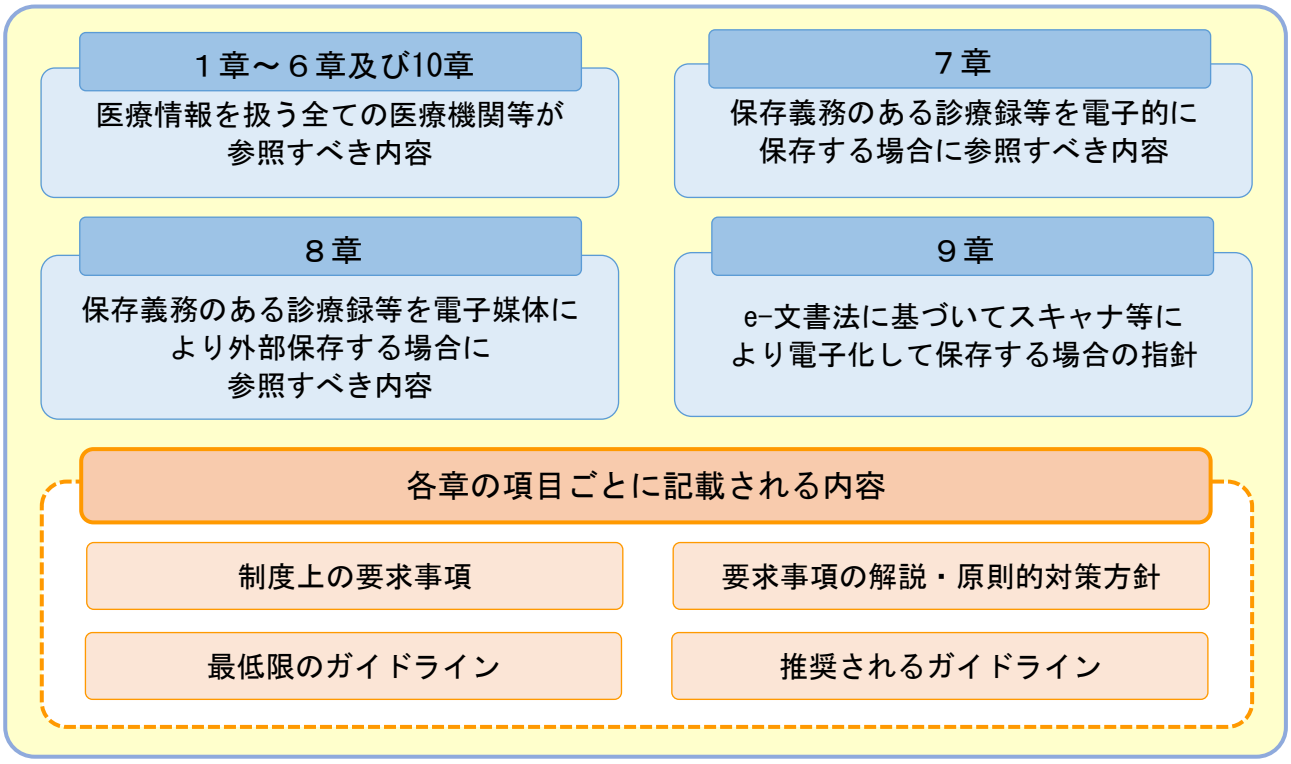
前章のとおり、日本国内はもちろんのこと、世界中でサイバー攻撃による被害が発生しています。総務省や経済産業省等の各省庁からサイバーセキュリティに対するガイドラインが公開されており、厚生労働省の「医療情報システムの安全管理に関するガイドライン第5.2版」（以下、ガイドライン）では、医療分野における電子情報の取り扱い方法をはじめセキュリティ上の対応等、様々な事項について記載されています。

1 ガイドラインの内容

ガイドラインは全10章で構成されています。１章から６章および10章は医療情報を扱う全ての医療機関等が参照すべき内容とし、７章は診療録等を電子保存する際に参照すべき内容、８章は診療録等を電子媒体により外部保存する際に参照すべき内容、９章はｅ-文書法に基づいてスキャナ等により電子保存する場合に参照すべき内容としています。

また、ガイドラインの中には、実行する際に「法律や指針等の要求に応えるべき最低限のガイドライン」に加え、「トラブル発生時の説明責任の観点から実施した方が理解を得やすく、推奨されるガイドライン」まで記載されています。

◆医療情報システムの安全管理に関するガイドライン　第5.2版



2　組織的安全管理対策と物理的安全管理対策

ガイドラインの中で、６章では医療情報システムの基本的な安全管理対策について記載されており、その中は「組織的」「物理的」「技術的」「人的」と区分けされています。

◆医療情報システムの安全管理に関するガイドライン　第6章

組織的 安全管理対策	物理的 安全管理対策	技術的 安全管理対策	人的 安全管理対策

「組織的」安全管理対策は、職員の責任と権限を明確にし、規程や手順を整備運用しながら、その実施状況を自己点検によって確認しなければなりません。具体的には医療情報システム安全管理責任者を設置するとともに、医療情報システム運用担当者を限定することが求められています。ただし、ガイドライン上では小規模医療機関等で役割が自明の場合は、明確な規程を定めなくとも良いとされています。

◆組織的安全管理対策（厚生労働省　医療情報システムの安全管理に関するガイドライン　第5.2版）

- 安全管理対策を講じるための組織体制の整備
- 安全管理対策を定める規程等の整備と規程等に従った運用
- 医療情報の取扱い台帳の整備
- 医療情報の安全管理対策の評価、見直し及び改善
- 情報や端末の外部持ち出しに関する規則等の整備
- 端末等を用いて外部から医療機関等のシステムにリモートアクセスする場合は、その端末等の管理規程
- 事故又は違反への対処

「物理的」安全管理対策は、医療情報システムを使用する際に、コンピュータ等を物理的な方法によって保護することです。具体的にはサーバーが保管されている場所には施錠をすること等が挙げられます。情報の種別、重要性と利用形態に応じていくつかのセキュリティ区画を定義した上で、以下の事項を考慮して、適切に管理する必要があります。

◆物理的安全管理対策（厚生労働省　医療情報システムの安全管理に関するガイドライン　第5.2版）

- 入退館（室）の管理（業務時間帯、深夜時間帯等の時間帯別に、入室権限を管理）
- 盗難、覗き見等の防止
- 機器、装置、情報媒体等の盗難や紛失防止も含めた物理的な保護及び措置

3 技術的安全管理対策と人的安全管理対策

残念ながら技術的安全管理対策のみで全ての脅威に対抗できる保証はありません。サイバーセキュリティは、先に述べた「組織的安全管理対策」や「物理的安全管理対策」等と組み合わせて対策することによってより強固なものとなります。しかし、その技術的安全管理対策の限界を的確に認識しつつ適用することにより、「技術的」な対策は強力な安全管理の手段となり得ます。

ガイドライン内では技術的な対策として下記の項目について詳細に解説しています。

◆技術的安全管理対策（厚生労働省　医療情報システムの安全管理に関するガイドライン　第5.2版）

- 利用者の識別・認証
- 情報の区分管理とアクセス権限の管理
- 外部のアプリケーションとの連携における認証・認可
- アクセスの記録（アクセスログという）
- 不正ソフトウェア対策
- ネットワーク上からの不正アクセス
- 医療等分野におけるIoT機器の利用

医療機関等は、情報の盗難や不正行為、情報設備の不正利用等のリスク軽減を図るため、人による誤りの防止を目的とした「人的」安全管理対策を策定する必要があります。

人的安全管理対策には守秘義務と違反時の罰則に関する規定や教育、訓練に関する事項が含まれています。

具体的には雇用契約に守秘・非開示に関する条項を含めることや、職員に対し「個人情報の安全管理」に関する教育訓練を定期的に実施すること、さらには退職後の個人情報保護規程を定めることが挙げられています。

ガイドラインでは医療情報システムに関連する者として、次の５種類を想定しています。

◆人的安全管理対策（厚生労働省　医療情報システムの安全管理に関するガイドライン　第5.2版）

- 医師、看護師等の業務で診療に関わる情報を取り扱い、法令上の守秘義務のある者
- 医事課職員、事務委託者等の医療機関等の事務の業務に携わり、雇用契約の下に医療情報を取り扱い、守秘義務を負う者
- システムの保守事業者等、医療機関等とは雇用契約を結ばずに医療機関等の業務に携わる者
- 見舞い客等の医療情報にアクセスする権限を有しない第三者
- 診療録等の外部保存の委託においてデータ管理業務に携わる者

3 ランサムウェアによる被害実例

前述のとおり、情報セキュリティをより強固なものにするべく、厚生労働省から医療情報システムに関する様々な事項についてのガイドラインが公開されています。しかし、依然として医療機関に対するサイバー攻撃は後を絶ちません。特にランサムウェアによる攻撃はすぐに復旧できるものではなく、多額の復旧費用や長期間の休診を要する場合もあります。本章では２つの実例をご紹介します。

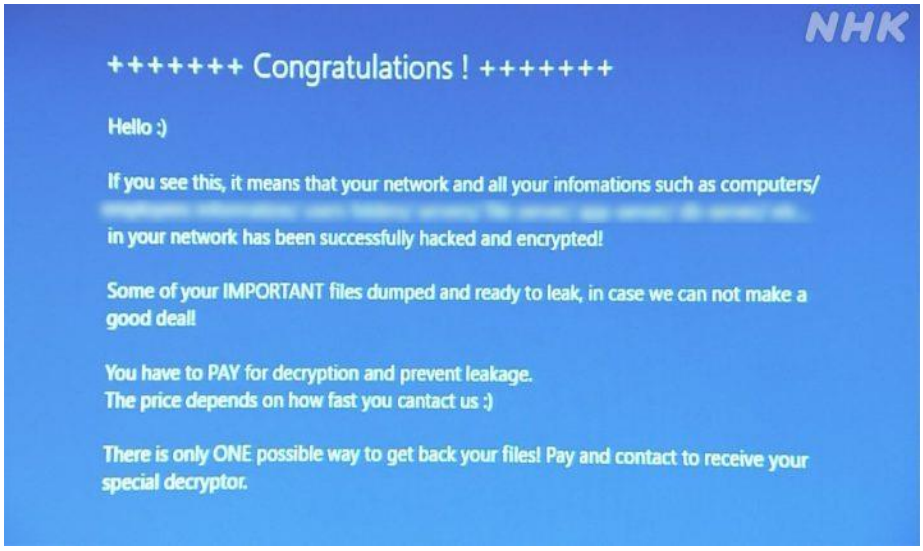
1 Kリハビリテーション病院・附属クリニックの実例

令和４年１月12日深夜に、Ａ県Ｋ市にある「Ｋリハビリテーション病院・附属クリニック」にて患者数万人分の電子カルテが閲覧できなくなる被害が発生しました。

スタッフが病院内にあるサーバーを確認すると、以下のような文章が送られており、電子カルテのデータを暗号化して身代金を要求するランサムウェアによる攻撃と認識されました。そこで病院は、警察への通報や厚生労働省への報告を行い、院内のインターネットがつながるパソコンを停止させて、患者への聞き取りによる紙カルテを再度作成し、手書き処方箋で診療を行う等の対応をしました。

今まで電子カルテを使用して患者情報に簡単にアクセスできていたものが紙カルテとなり、院内での患者情報の管理が複雑化してしまいました。サーバーの復旧後は紙カルテの情報を電子カルテに転記する作業があり、業務の負担が増加しているのは明らかです。

◆身代金を要求する内容のメール



出典：NHK サイカルjournal

2　T町立病院の実例

令和３年10月末、Ｔ県Ｔ町立病院がランサムウェア攻撃を受け、電子カルテの閲覧等ができなくなる等の大きな被害が生じました。

その後約２か月もの間、通常診療は停止してしまい、翌令和４年１月４日に再開されています。令和４年６月７日には一連の被害状況から再発防止策までを取りまとめた『Ｔ県Ｔ町立病院　コンピュータウイルス感染事案　有識者会議調査報告書』が公開されました。

今回の被害は、令和３年10月末に院内のプリンタから一斉に犯行声明が印刷されたことで発覚しました。ランサムウェア攻撃の被害を受け、電子カルテ等の患者情報を扱うサーバーのデータが暗号化され、使用不可能となってしまいました。被害を確認した後はネットワークを遮断し、救急患者や新規患者の受け入れを中止しました。さらには手術も延期せざるを得なくなる等、病院の運営は停止してしまいました。

◆T町立病院　コンピュータウイルス感染事案　有識者会議調査報告書より

令和3年10月31日未明、病院内に設置されていた複数台のプリンタが、一斉に犯行声明を印字し始めたことでインシデントが発覚した。Lockbit2.0によるランサムウェア（身代金要求型ウイルス）に感染し、患者の診察記録を預かる電子カルテ等の端末や関連するサーバーのデータが暗号化され、データが使用できない甚大な被害が生じた。侵入経路としては導入している仮想プライベートネットワーク（VirtualPrivateNetwork、以下「VPN」という。）装置の脆弱性を悪用して侵入したものと思われる。

ランサムウェア感染の確認後は、ネットワークの遮断や端末の停止等を行い、一時、救急や新規患者の受け入れを中止し、手術も可能な限り延期にする等、病院としての機能は事実上、停止する状態に陥った。

公開された調査報告書の中では、被害を確認してから診療を再開するまでの経過を取りまとめています。被害を確認した翌日には迅速に警察へ被害届を提出し、災害対策本部を設置して状況確認を行っています。同日にはＴ町長へ報告を行った後、記者会見を開きました。その後は、前述のＫリハビリテーション病院・附属クリニックと同様に紙媒体を用いた診療に切り替え、外来患者は予約診療のみとしました。12月上旬には季節性インフルエンザ予防接種を実施しましたが、サーバーの復旧作業中ということもあり、現場は非常に混乱しました。

令和３年11月以降はシステムの復旧に時間を要し、12月末には電子カルテのデータ復元を完了し、翌年１月４日に通常診療を再開する経過となりました。

次ページでは時系列順にいくつか抜粋しご紹介します。

◆T町立病院　コンピュータウイルス感染事案　有識者会議調査報告書(一部抜粋)

月日	時間	概要
令和３年 10月31日	未明	院内にある複数のプリンタから、データを窃取および暗号化した内容の文書の大量印刷を確認。
	８時55分	○○県警察本部へ相談。被害届として受理される。
	10時00分	災害対策本部を正式発足。医療提供状況の確認と各種連携の確認を行う。(BCPに基づき、紙ベースでの医療提供の実施等)
	10時46分	開設者であるＴ町長へ現状報告。
	16時00分	記者会見の実施。
11月１日		ネットワークを介しない印刷対応実施確認。 入院患者一覧表の作成やコピー機の設置等を行う。患者受け入れ方針の変更点確認等。
11月３日	16時00分	修復会社にてサーバー系統の調査復旧を試みる。
12月29日		電子カルテシステムのデータ復元を確認。
令和４年 １月４日		電子カルテシステムを再稼働し通常診療を再開。

報告書では様々な側面に対して課題を提示しています。「組織的な課題」としては、サイバー攻撃による事業継続リスクが存在する認識と、このリスクを回避するためのリソースの確保ができていなかったことをはじめ、情報システムの安全管理に関する備えがなかったことが挙げられています。Ｔ町立病院は１名の情報システム担当者のみで運営されていましたが、総務省が令和４年４月に公開した「公立病院の現状について」にあるように、全国的に公立病院の経営状況は良いとは言えず、Ｔ町立病院においても医療情報システムの安全管理を実現するリソースを割く余裕がないことが課題として挙げられました。

◆T町立病院　コンピュータウイルス感染事案　有識者会議調査報告書より(一部改変)

総務省が2022年４月に公開した「公立病院の現状について」にあるように、公立病院の経営状況は悪化の一途をたどっており、Ｔ町立病院のような200床未満(全体の54.1%)の医療機関は、一般的にIT部門を持っておらず、少しパソコンに詳しい庶務係がIT担当を一人で兼任しているような状況にある。仮にＴ町立病院が前述したようなリスク管理対象にサイバー攻撃を含めBCPを策定することになっても、救急救命センターのような高度な医療行為を担っていないため、医者と看護師の配分を調整しても人件費が膨らむ(医療機能の低下していく病院はベッド当たりの入院単価が下がることとなるので人件費が上がる)。このような状況下ではＴ町立病院においても医療情報システムの安全管理を実現するリソースを割く余裕は無く、サイバー攻撃リスクを盛り込んだBCP策定を理由に、IT担当者の増員を予算に含めても受け入れられないのは明白である。

4 院内で取り組むべきサイバーセキュリティ対策

1 スタッフへの研修によるセキュリティ強化

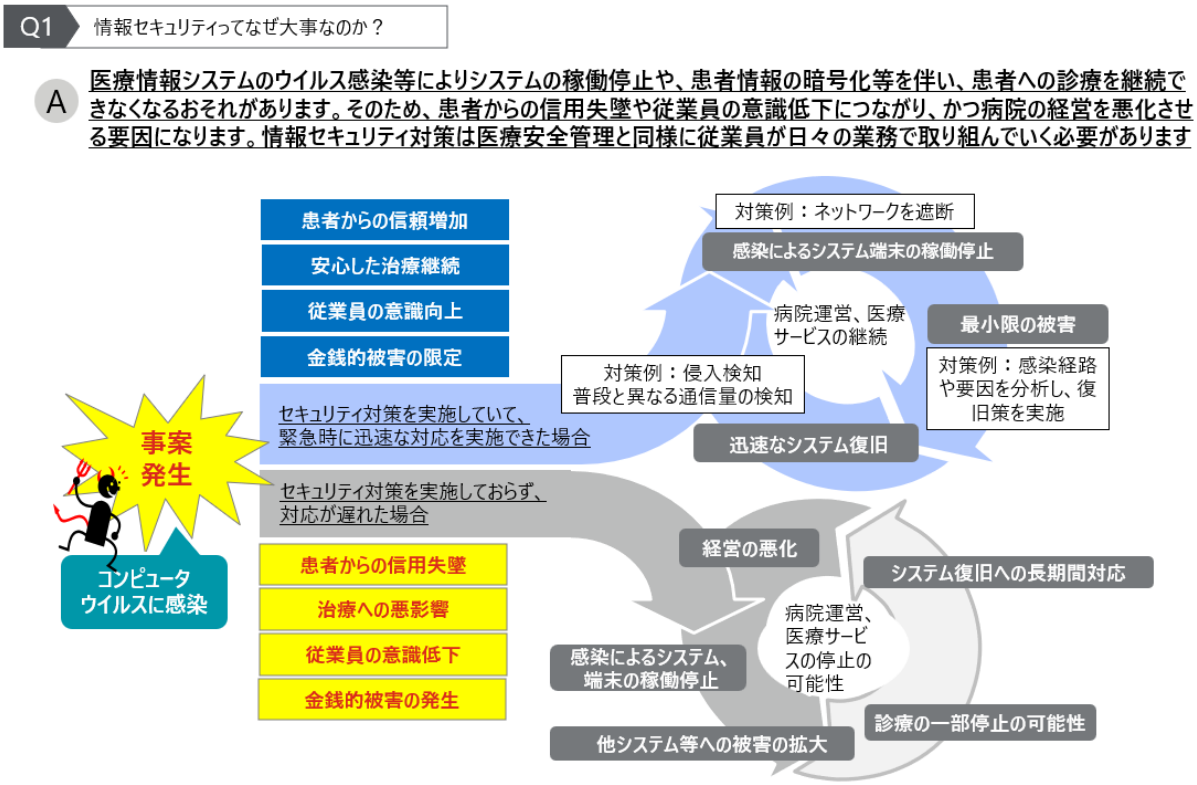
サイバー攻撃はいつ発生するかわかりません。また、院内のシステム管理者だけがサイバーセキュリティに対して知識を深めるだけで院内の情報を守り切るのは困難です。

また、サイバー攻撃被害の原因がスタッフにある可能性もあります。実際に個人情報をUSBメモリに入れて持ち出して紛失してしまい、トラブルになった事例もあります。

厚生労働省では、医療機関で働くスタッフのサイバーセキュリティに関する理解を深めるために、研修教材を作成しています。院内での情報利用については、全スタッフが共有しておくべきです。

情報セキュリティの重要性を再確認し、院内での情報セキュリティの強化に努めましょう。

◆情報セキュリティの重要性



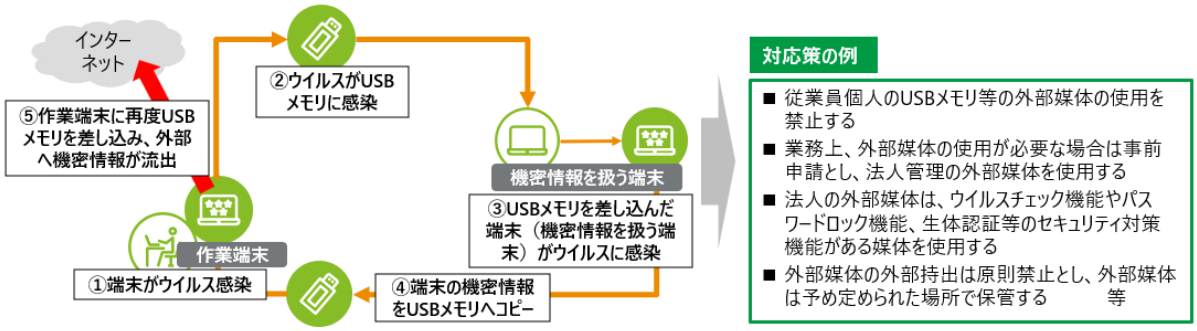
出典：厚生労働省　情報セキュリティ研修教材（医療従事者向け）

◆外部媒体のリスクについて

Q5 USB等を使うときに何に気をつければいいのか?

A **紛失防止のための取組だけでなく、外部媒体への保存は暗号化の実施、外部媒体自体にウイルスチェック機能やパスワード機能、生体認証等の対策を付与することが重要です**

事例	発生国	被害組織	内容
USB機器や端末の紛失	日本	A医学部付属病院	• 総合内科・総合診療科で患者約1万3千人分の個人情報を記録したUSBメモリを紛失した。持ち運びできる媒体への情報保存はマニュアルで禁止されていたが、医師はマニュアルの存在を知らなかった
		B市立病院	• 医師が、患者約330人分の手術記録を保存したUSBメモリーを紛失した • 病院は個人情報の外部への持ち出しは禁止しているが、無断で自宅に持ち帰っていた。情報の流出や悪用は確認されていないが、警察に遺失物届を提出した
		C医科大学病院	• 薬剤師が、糖尿病・内分泌・代謝内科を受診した患者3,835人の氏名や生年月日などの個人情報が入ったUSBメモリーを紛失した。情報の流出は確認されていないが、同病院は患者に文書で謝罪し、警察に遺失物届を提出した



出典：厚生労働省　情報セキュリティ研修教材（医療従事者向け）

◆マルウェアの理解と防御

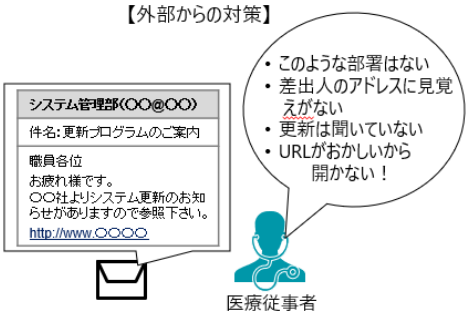
Q7 外部攻撃について何に気を付ければいいのか？

A **マルウェア対策は、職員の一人一人が情報セキュリティの必要性を理解し、自覚をもって取り組むことが重要です。自施設の情報システム部門や担当者に相談の上、情報セキュリティ対策を実施しましょう**

事例	被害組織	内容
外部からの標的型攻撃と想定（未特定）	T大学	• 内部メールサーバの管理画面の設定が変更されていることを発見し調査を行ったところ、業務端末がマルウェア（コンピュータウイルス）に感染し、同端末及び同メールサービスのサーバ等に保存されていた個人情報が流出した可能性があることが判明した • 流出した可能性のある情報は、システムを利用する職員、学生の個人情報で約36,300件であった • 同大学では、直ちに流出した可能性のある全てのパスワードの変更等の対応を実施し、情報セキュリティ対策の強化を実施した
	K研究所	• ウェブメールサーバへの不正アクセスにより、職員のメールアドレスから約2,000件の迷惑メールが送信された • 職員がウェブメールの管理者を騙ったメールに記載されていたサイトにアクセスしたためアカウント名、パスワードが奪取された

対応策の例

外部からの対策	■ 見知らぬ添付ファイル付きの電子メールは注意する（受信メールの信頼性を確認する、添付ファイルを開かない、安易にクリックしない等） ■ 外部記憶媒体（USBなど）からの感染を予防する	職員が心がける対策
アップデートの実施	■ パソコンOSのアップデートを行い、修正プログラムを適用する ■ セキュリティ対策ソフトを最新版に更新する ■ アプリケーション、ソフトを最新版に更新する	情報システム部門または担当者に確認の上、取るべき対策
インターネットセキュリティ対策	■ Windowsやウイルス対策ソフトに付いているパーソナルファイヤーウォールを有効にする ■ 第三者が無断で使用できないように、PC端末には、IDとパスワードを設定する	



出典：厚生労働省　情報セキュリティ研修教材（医療従事者向け）

2｜サイバーセキュリティ対策のチェックリスト

厚生労働省では『医療情報システムの安全管理に関するガイドライン』の中で、「経営層向け」「システム管理者向け」「医療従事者・一般の利用者向け」それぞれに対してサイバーセキュリティ対策チェックリストを作成しており、サイバー攻撃に対する認識を確認することができます。以下では「経営層向け」のチェックリストを一部抜粋します。

自院で実施できているか確認してみてください。

◆経営層向け　サイバーセキュリティ対策チェックリスト

	チェック項目
①	医療情報システムの安全管理に関する方針について以下の内容を含めて策定しているか ・理念（基本方針と管理目的の表明） ・医療情報システムで扱う情報の範囲 ・情報の取扱いや保存の方法及び期間 ・不要・不法なアクセスを防止するための利用者識別の方法 ・医療情報システムの安全管理責任者 ・苦情・質問の窓口
②	運用管理規程等において次の内容を定めているか ・医療機関等の体制 ・契約書・マニュアル等の文書の管理方法 ・リスクに対する予防措置、発生時の対応の方法 ・機器を用いる場合は機器の管理方法 ・端末等を用いて外部から医療機関等のシステムにリモートアクセスする場合はその情報端末等の管理方法 ・個人情報の記録媒体の管理（保管・授受等）の方法 ・患者等への説明と同意を得る方法 ・監査 ・苦情・質問の受付窓口
③	サイバーセキュリティに関する取組方針を常日頃から職員や外部委託先等に伝えてコミュニケーションを取っているか
④	法令上の守秘義務のある者以外の者を職員として採用するにあたって雇用契約に守秘・非開示に関する条項を含める等の安全管理対策を実施しているか
⑤	インシデント対応の専門チーム（CSIRT等）を設置しているか
⑥	経営者が責任を持って組織の内外へ説明ができるように、経営者への報告ルート、公表すべき内容やタイミング等を定めているか

出典：厚生労働省　経営層向け　サイバーセキュリティ対策チェックリスト

■参考資料

厚生労働省：医療情報システムの安全管理に関するガイドライン　第5.2版
情報セキュリティ研修教材（医療従事者向け）
情報セキュリティ研修教材（経営層向け）
医療情報システムの安全管理に関するガイドライン
医療機関のサイバーセキュリティ対策チェックリスト

NHK サイカルjournal：あなたの病院の「感染」対策は大丈夫？
～問われる医療機関のセキュリティー～

日本医師会総合政策研究機構：病院・診療所のサイバーセキュリティ：医療機関の情報システムの管理体制に関する実態調査から

徳島県つるぎ町立半田病院：コンピュータウイルス感染事案　有識者会議調査報告書

医業経営情報レポート

組織的・技術的安全対策で守る　医療機関のサイバーセキュリティ対策

【著 者】日本ビズアップ株式会社
【発 行】税理士法人　森田会計事務所
〒630-8247　奈良市油阪町456番地　第二森田ビル 4F
TEL 0742-22-3578　　FAX 0742-27-1681
