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

（参考資料　５）

医療における情報セキュリティに関する脅威やインシデント

Ministry of Health, Labour and Welfare of Japan

情報処理推進機構（IPA）「情報セキュリティ10大脅威 2021」

昨年順位	個人	順位	組織	昨年順位
1位	スマホ決済の不正利用	**1位**	ランサムウェアによる被害	5位
2位	フィッシングによる個人情報等の詐取	**2位**	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗・中傷・デマ	**3位**	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	**4位**	サプライチェーンの弱点を悪用した攻撃	4位
3位	クレジットカード情報の不正利用	**5位**	ビジネスメール詐欺による金銭被害	3位
4位	インターネットバンキングの不正利用	**6位**	内部不正による情報漏えい	2位
10位	インターネット上のサービスからの個人情報の窃取	**7位**	予期せぬIT基盤の障害に伴う業務停止	6位
9位	偽警告によるインターネット詐欺	**8位**	インターネット上のサービスへの不正ログイン	16位
6位	不正アプリによるスマートフォン利用者への被害	**9位**	不注意による情報漏えい等の被害	7位
8位	インターネット上のサービスへの不正ログイン	**10位**	脆弱性対策情報の公開に伴う悪用増加	14位

引用：https://www.ipa.go.jp/security/vuln/10threats2021.html

医療における情報セキュリティ インシデント事例（一部）

2015.11.27　菰野厚生病院（三重県）：医事システムの端末がウイルス感染。インターネット利用中に感染し、ウイルスが院内ネットワークを通じてサーバーに侵入。サポート終了したOS（Windows XP）を試用していたことも原因の一つ。

2017

2016.01.14　鳥取県立中央病院（鳥取県）：庁内LANパソコン１台が、外部からのウイルスメールによりコンピュータウイルスに感染し、保存されていた3,152個の電子ファイルがコンピュータウイルスにより、開くことができなくなった。

2017.08～2018.01　福島医大病院（福島県）：コンピューターウイルス感染により検査装置が不具合を起こし、患者へのコンピューター断層撮影(CT)などをやり直すトラブルが起きた。

2018

2018.10.16　宇陀市立病院（奈良県）：電子カルテを含む医療情報システムがコンピュータウイルスに感染し、一部のデータが暗号化され、患者カルテが参照できなくなった。外部と接続されていないはずの医療情報システムが外部と接続された状況になり、ウイルスの侵入・感染に至った可能性が高いとの指摘。

2019

2019.05.20　多摩北部医療センター（東京都）：職務用パソコン端末へ送信された不正アクセスを意図したメールの添付ファイルを開封した結果、マルウェアに感染し、メールボックス内に不正アクセスされ、メールボックス内の除法の一部が流出した。

2019.11.01　徳島大学病院（徳島県）：海外出張の際にパソコン及び業務用携帯電話の収められたカバンの盗難被害が発生した。当該パソコンに患者の症例情報（3,201件）等、業務用携帯電話に職員氏名・業務用電話番号（約1,000件）が保管されていた。

2020

2021

2021.04.30　千葉大学医学部附属病院（千葉県）：患者586名の個人情報を個人用パソコンに保存し、大学で許可されていないクラウドサービスを利用していたところ、宅配業者を装ったフィッシングメールによりクラウドサービス用ID・パスワードを盗み取られ、個人情報を閲覧できる状態になっていた。

2021.05.31　市立東大阪医療センター（大阪府）：医用画像参照システムに不正アクセスがあり、システムが利用できなくなった。

2021.10.31　つるぎ町立半田病院（徳島県）：電子カルテがランサムウェアに感染し、システムが利用できなくなった。

医療における情報セキュリティに関する脅威やインシデント

近年、「外的要因」かつ「意図的な事象」に脅威・インシデントの傾向が変化しつつある

外的要因

外部事業者等によるミス

・外部事業者の情報紛失
・外部事業者の設定ミス

等

(事例)
・外部事業者の設定ミスにより、患者70人分の個人情報が含まれたファイルがインターネットを経由しアクセス可能な状態となり、個人情報が漏洩する恐れがあった。

外部からの攻撃

・Webサイト、保守回線等を経由した攻撃
・ランサムウエアやマルウエアなど、システムの様々な脆弱性を利用した攻撃

等

近年、「外部からの攻撃」が増加傾向にあり、医療機関個々での単独対策には限界がある。

偶発的

意図的

職員によるミス

・USBメモリやPCの紛失・盗難
・FAXやメールの誤送信
・誤操作によるファイルのアップロード

等

(事例)
・医師が患者約330人分の手術記録を保存したUSBメモリを紛失した。
・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を保存したUSBメモリを紛失した。

内部不正

・職員による、機密情報、個人情報等の持ち出し
・委託事業者による機密情報、個人情報等の持ち出し

等

(事例)
・元職員が、在職中に患者の個人情報を持ち出し、新しく開設する介護事業所の案内状送付に利用した。

内的要因

参照：https://www.mhlw.go.jp/stf/seisakunitsuite/bunya/kenkou_iryou/iryou/johoka/cyber-security.html

海外のヘルスケア分野における情報セキュリティ インシデント事例 等

2016.02.15　アメリカ・ハリウッドにあるHollywood Presbyterian医療センターで、サイバー犯罪者による攻撃を受け、
病院のデータを人質にして、9000枚のビットコイン（約340万ドル相当）を要求された。
急を要する患者については救急車で移送が行われ、病院の職員は紙とペンで患者のカルテを記録し、各部門はファックスでやりとりをせざるを得なくなっており、病院のメールサーバーがダウンしたため、患者は検査結果を確認するために、病院に出向くことにもなった。

2020.09　ドイツ・デュッセルドルフ大学病院でランサムウェアによりシステムが停止が発生した。
同病院で救命処置を受ける予定だった患者を受け入れることができず、別の病院に搬送された。

2021.05　アイルランドの公的医療サービスを提供するHealth Service Executive（HSE）のシステムの一部が、
ランサムウェアグループContiによる攻撃で、停止した。これにより、一部の外来患者の予約がキャンセルされた。
なお、Contiは「Apache Log4j」の脆弱性を利用していた。

The health sector and in particular the vaccine rollout was a major focus for the NCSC, with the organisation's world-leading services protecting NHS, healthcare, and vaccine supplier IT systems from malicious domains billions of times.

（NCSC英国家サイバーセキュリティセンター 年次レビュー）

参照： https://www.ncsc.gov.uk/news/record-number-mitigated-incidents
https://japan.zdnet.com/article/35179996/