★福岡市医師会ホームページにバックナンバー掲載！
（ https://www.city.fukuoka.med.or.jp/jouhousitsu/ ）

No. ２５３

医療情報室レポート

２０２２年８月１日
福岡市医師会医療情報室
TEL092-852-1505・FAX092-852-1510
E-mail：j-kikaku@city. fukuoka. med. or. jp

特集：医療機関におけるサイバーセキュリティ対策

我々の生活様式や経済活動を大きく変容させた新型コロナウイルス（COVID-19）は世界中で猛威を振るい続け、国内では感染拡大の第7波の渦中にあるが、この混乱に乗じて国内の様々な企業や団体等においてサイバー攻撃の被害が増加してきている。

サイバー攻撃とはサーバーやパソコン等の情報端末に対し、ネットワークを利用してシステムやデータの破壊や窃取、改竄を行うものだが、令和3年に警察が検挙したサイバー攻撃関連の犯罪は前年比23.6%増の1万2,209件と過去最多を記録しており、警察庁に報告された国内の「ランサムウェア」による被害件数は146件（令和2年下半期は21件）と増加の一途を辿っている。

サイバー攻撃の被害は企業の規模や業界を問わず広範囲に及んでおり、令和3年10月には徳島県の病院が「ランサムウェア」によるサイバー攻撃を受け、電子カルテ等の基幹システムに障害が発生、新規の診療受付や救急患者の受入を一時停止して、通常診療の再開までに約2ヵ月の期間とシステム復旧に約2億円もの費用を要した。

医療業界もサイバー攻撃の標的に含まれており、医療機関におけるサイバーセキュリティ対策は喫緊の課題となっている。

今回は、医療機関におけるサイバーセキュリティ対策について考えてみる。

● 最近のサイバー攻撃の種類と被害事例

○ランサムウェア（身代金要求型不正プログラム）

サイバー攻撃における最近の動向として、データを暗号化して使用不能にし、元に戻すことと引き換えに身代金を要求する**「ランサムウェア」**と呼ばれる**マルウェア**（悪意のあるソフトウェア）による被害が増加している。

医療機関が**「ランサムウェア」**に感染し、電子カルテ等が使用不可となれば、診療に多大な影響が生じる。

主な感染経路はシステムメンテナンス等の際に院外から遠隔で接続時に使用する**「VPN（仮想施設網）装置」**の脆弱性を悪用したものが最も多い。令和3年10月に徳島県の病院が被害を受けたサイバー攻撃も、この装置が最新バージョンではなかったために外部からの侵入を許したことが原因である。

最近の医療機関における**「ランサムウェア」**への感染が疑われる事例は右記を参照。

<ランサムウェアへの感染が疑われる医療機関の事例>

発生年月	発生県など	概要
2021年10月	静岡県 病院(160床)	システムの一部に障害が発生し、診療を一部制限 (2022年2月に仮復旧)
2021年10月	徳島県 病院(120床)	電子カルテの患者約8万5,000人分のデータが閲覧不能 (2022年1月に通常診療再開)
2022年1月	愛知県 病院(279床)	電子カルテや医事会計システムに不具合が発生
2022年4月	大阪府 病院(92床)	電子カルテの患者数万人分のデータが閲覧不能 (2022年6月に復旧)
2022年5月	岐阜県 病院(60床)	電子カルテの患者約11万人分のデータが閲覧不能 (バックアップにより翌日には復旧)
2022年6月	徳島県 病院(90床)	電子カルテや院内LANシステムが使用不能 (バックアップにより同月末に復旧)

○「Emotet（エモテット）」（標的型メール攻撃）

近年増加しているサイバー攻撃として**「Emotet（エモテット）」**と呼ばれるマルウェアがある。主な攻撃手法は実在する組織や人物を名乗る**「なりすましメール」**を送信し、受信者が添付されたファイルを開くことで不正なプログラムがダウンロードされるものである。

「Emotet（エモテット）」に感染すると**パソコン等の端末内にあるメールアドレスや送受信履歴が窃取**され、メールがさらに拡散されて感染が広がることが特徴で、その手口は益々巧妙化しており対策が難しくなっている。

本会では実際に本会会員や福岡市医師会を騙った**「なりすましメール」**が送信されていることを確認しており、**不審な添付ファイルやURLには不用意にアクセスしない**よう注意が必要である。

● サイバー攻撃への対策

電子カルテ等の医療情報システム全般に関し、基礎となるガイドラインは厚生労働省による**「医療情報システムの安全管理に関するガイドライン」**となる。令和4年3月に改訂された第5.2版では**「ランサムウェア」**に関する対応が新たに盛り込まれており、年内には更なる改定が予定されている。自院でできるサイバー攻撃への対策等について次のとおりまとめた。

項目	内容
セキュリティ対策の強化	・ウイルス対策ソフトの導入、定期的なウイルススキャンの実施 ・医療情報を扱うシステムやソフトウェアは常に最新の状態にアップデートを行う
院内への周知と情報提供	・不審なメールや添付ファイルは絶対に開かないよう職員に周知 ・端末等がウイルスに感染した時はネットワークケーブルを切り離す等の初期対応を周知
ベンダーとの保守契約確認	・サイバー攻撃の発覚時、即座にベンダーによる対応が可能か保守契約内容を確認 (ベンダーの対応が不可の場合、調査や復旧が進まず、被害が拡大する可能性がある)
バックアップデータの管理	・バックアップデータは院内ネットワークから切り離したオフラインの媒体等に保管 (バックアップも使用不可となれば復旧まで多大な時間を要し、多額の費用がかかる)
BCP(事業継続計画)の策定	・自院に被害が起きた際でも診療を継続させるため、BCP(事業継続計画)を策定 ・策定後は対処手順が適切に機能するか平時から訓練を行い、常に改訂に取り組む

※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」などを参照

テーマ：医療機関におけるサイバーセキュリティ対策

● 損害への備え

医療機関がサイバー攻撃を受けた場合、原因究明やデータ復旧等様々な対応が必要となり、かつ多額の費用も発生する。また、情報漏洩による損害賠償請求を受ける可能性もあることから、医療機関にはサイバー攻撃発生による損害への備えが欠かせない。

福岡県医師会では会員医療機関に向け、サイバー攻撃や情報漏洩リスクへの対策として団体保険**「医療機関用サイバー保険」**を設けている。

また、日本医師会では、主にサイバー保険未加入の医療機関を対象にセキュリティ対策の基本的支援として**「サイバーセキュリティ支援制度」**を本年6月1日に創設している。

<医療機関用のサイバー保険について>

	福岡県医師会団体保険「医療機関用サイバー保険」	**日本医師会「サイバーセキュリティ支援制度」**
内容	サイバー攻撃や情報漏洩事故により発生した損害賠償責任や費用損害を補償	①日本医師会サイバーセキュリティ対応相談窓口(緊急相談窓口)の設置 TEL：0120-179-066　運営時間：9～21時(年中無休) ②セキュリティ対策強化に向けた無料サイト(※)の活用 ※Tokio Cyber Port((株)東京海上日動火災保険運営の情報提供サイト) ③日本医師会サイバー攻撃一時支援金・個人情報漏洩一時支援金制度
対象	福岡県医師会会員(別途加入手続きが必要)	日本医師会Ａ①会員(本制度のための新たな費用負担はなし)

● 最新情報の取得

日々変容し、進化し続けるサイバー攻撃の手口に対応するためには、最新情報を取得しつつ、対策を継続することが求められる。

最新のサイバー攻撃の動向や情報セキュリティに関して、情報収集を行うためのサイトを一例として紹介する。

<サイバー攻撃や情報セキュリティに関するサイト>

	団体名	**特色**	**URL**
1	独立行政法人 情報処理推進機構 (IPA)	システムやソフトの脆弱性に関する最新情報を発信	https://www.ipa.go.jp/
2	内閣サイバーセキュリティセンター (NISC)	情報セキュリティに関する冊子などを作成して発信	https://www.nisc.go.jp/
3	福岡県警 サイバー犯罪対策課	県内で発生したサイバー攻撃の最新手口を紹介	https://www.police.pref.fukuoka.jp/seian/cyber/index.html
4	Tokio Cyber Port ((株)東京海上日動火災保険)	日医「サイバーセキュリティ支援制度」の一部として紹介	https://tokiocyberport.tokiomarine-nichido.co.jp/cybersecurity/s/

● 改正個人情報保護法

本年4月1日、個人情報等の漏洩が判明した場合の法的義務等を新設した**「改正個人情報保護法」**が施行された。

主な改正内容は個人情報漏洩時に**「個人情報保護委員会への報告と本人への通知の義務化」**、個人情報の**「安全管理措置の公表の義務化」**等があり、法人に対する罰則規定も金額が**1億円に引き上げ**られた。患者の個人情報を取扱う医療機関でも漏洩時の対策等の検討が必要である。

＜「改正個人情報保護法」における主な改正内容＞

①個人情報保護委員会への報告と本人への通知の義務化

個人情報漏洩等が発生した場合、個人の権利利益を害する恐れが大きい事態については、**「個人情報保護委員会への報告」**と**「本人への通知」**を義務化

個人情報保護委員会への報告が必要となる事態
- ①要配慮個人情報の漏洩等
- ②財産的被害の恐れがある漏洩等
- ③不正の目的による恐れがある漏洩等
- ④1,000件を超える漏洩等

※①～④の恐れがある場合も対象

②安全管理措置の公表の義務化

個人情報の安全管理のために講じた措置の公表を義務化(安全管理に支障を及ぼす恐れがあるものを除き、ホームページ等で本人が知り得る状態に置くことが必要)

安全管理措置の一例
- ・個人情報の取扱いの基本的なルールを決める
- ・紙で管理の場合は鍵のかかる場所に保管
- ・パソコン等で管理の場合はファイルにパスワードを設定
- ・パソコンにセキュリティ対策ソフトを導入

※個人情報保護委員会ホームページをもとに作成

● 福岡市医師会の取組み

本会では会内に向けて、会員専用サイトに**「情報セキュリティ」**の特設ページを設け、**「Emotet（エモテット)」**に関する情報や、サイバー保険等のセキュリティ対策に向けた最新情報の発信に努めている。

また、本年9月には本会会員医療機関を対象に、**「福岡県警サイバー犯罪対策課」**による**「サイバー犯罪の現状と対策(仮)」**の講演と、福岡医師協同組合からは**「サイバー保険案内」**を予定しており、サイバーセキュリティ対策強化のため、会員の皆様をはじめ、会員医療機関に従事する皆様方には多数ご参加ください。（講演会詳細は会員専用サイト等にて後日案内予定）

【福岡市医師会会員の先生で、情報セキュリティに関してお困りのことがあれば、本会情報企画課（TEL 852-1505）までお問合せください。】

医療情報室の目

★情報の取扱いにおける危機意識の向上

サイバー攻撃は不特定多数にウイルスメールを送る「ばらまき型」から、最近は特定の企業や組織を狙って攻撃する「標的型」へと変化しており、攻撃の手口も巧妙化していくことで、その対策も益々難しくなってきている。

医療機関では患者の個人情報といった機微な情報を取扱うために、「ランサムウェア」による被害から電子カルテのデータが全て暗号化された場合、診療の継続は不可能となり、医療の提供に多大な影響が生じる。また、改正個人情報保護法の厳格化により個人情報保護委員会への報告義務が原則30日以内になったが、サイバー攻撃の被害回復に2ヵ月近くの時間を要することから、被害に遭うことで自動的に法令違反になる危険性もある。医療機関には万全のセキュリティ対策が求められるのだが、前述のサイバー保険への加入や対策ソフト導入、データのバックアップ体制の整備などには一定の費用負担が生じることから、安全な医療提供体制の維持のためには国による公的な財政支援も必要と考える。

情報セキュリティに精通した人材を院内で育成することも容易ではなく、また、どれほど技術的・物理的に強固なセキュリティ対策を行っても、受け取り側の判断を惑わす「Emotet」のような標的型のメール攻撃を受けた場合、サイバーセキュリティに関する知見が十分でなければ、不審なファイルを開いたり悪意のあるサイトに誘導されてしまう等、容易にネット上の脅威に晒されてしまう危険をはらんでいる。

医業経営には様々なリスクがあるが、サイバーセキュリティ対策も危機管理としての重要性は一層高まってきており、医療情報に携わる全ての医療従事者が危機管理への意識を向上させることが肝要である。

編 集　福岡市医師会：担当理事　牟田　浩実(情報企画・広報担当)・江口　　徹(地域医療担当)
※ご質問やお知りになりたい情報(テーマ)がありましたら医療情報室までご連絡ください。(事務局担当　情報企画課 上杉)
(TEL092-852-1505・FAX092-852-1510　E-mail：j-kikaku@city. fukuoka. med. or. jp)