福県医発第2535号(地)
令和３年12月９日

各 医 師 会 長　　殿

福 岡 県 医 師 会
会　長　松　田　峻一良
（公 印 省 略）

医療機関を標的としたサイバー攻撃（ランサムウェア）への対応について

さて近年、国内外の医療機関を標的としたランサムウェア（情報システムを使用不可の状態にした上で身代金を要求するウイルス）を利用したサイバー攻撃による被害が増加している状況にあり、その注意喚起については、本会より「医療機関を標的としたランサムウェアによるサイバー攻撃について」（令和３年７月28日付福県医発第1315号（地））及び「医療機関を標的としたサイバー攻撃への対応について」（令和３年11月９日付福県医発第2260号（地））にて貴会宛てご連絡したところです。

今般、日本医師会より昨今の状況を受けて、改めて下記の点について周知依頼がありました。

なお、日本医師会より、本通知に記載の内容については、サイバー攻撃の抜け道となり得ることから、悪用を防ぐため、基本的には医療機関従事者並びに医療機関と守秘義務契約を結んだベンダーのみに見せることができるものであり、一般には公開しないよう依頼がなされております。

つきましては、貴会におかれましても本件についてご了知いただくとともに、貴会会員への周知方につき、よろしくお願い申し上げます。

記

１）リモート接続等に利用される、SSL-VPN装置（特にFORTINET社製）の脆弱性が悪用される事例が増えていることから、機器を納品した事業者等への確認や機器の内容に更新がないか点検して早期に対応してください。

２）ランサムウェアを利用したサイバー攻撃により情報が失われる事案が発生していることから、「医療情報システムの安全管理に関するガイドライン第5.1版」の「7.2章　見読性の確保について」（バックアップの作成、バックアップからの閲覧の確保）及び「7.3章保存性の確保について」（バックアップおよび履歴の保存）を参考に、バックアップを作成してください。

小郡三井医師会より　　医療情報システム担当理事　栁　大三郎
会長　島田昇二郎

3）サイバー攻撃により医療情報システムに障害が発生した場合は、厚生労働省（下記連絡先）に連絡してください。

■厚生労働省　医政局研究開発振興課医療情報技術推進室

電話：03-3595-2430　メール：igishitsu@mhlw.go.jp

標的型メールを受信した場合等は、情報処理推進機構（IPA）に相談してください。

■情報処理推進機構（IPA）情報セキュリティ安心相談窓口

電話：03-5978-7509（平日日中のみ）　メール：anshin@ipa.go.jp

4）「医療機関のサイバーセキュリティ対策チェックリスト」及び「医療情報システム等の障害発生時の対応フローチャート」を活用いただき、対策に役立ててください。

「医療情報システムの安全管理に関するガイドライン　第5.1版」

https://www.mhlw.go.jp/stf/shingi/0000516275.html

（情シ　４９）
令和３年12月２日

都道府県医師会　担当理事　殿

日本医師会　常任理事
長島　公之
（公印省略）

医療機関を標的としたサイバー攻撃（ランサムウェア）への対応について(注意喚起)

平素より本会会務の運営に特段のご理解・ご支援を賜り厚く御礼申し上げます。

近年、国内外の医療機関を標的とした、ランサムウェア（情報システムを使用不可の状態にした上で身代金を要求するウイルス）を利用したサイバー攻撃による被害が増加している状況にあり、日本医師会では、令和３年７月６日「医療機関を標的としたランサムウェアによるサイバー攻撃について(注意喚起)」（情シ22号)、令和３年11月２日「医療機関を標的としたサイバー攻撃への対応について(注意喚起)」において、医療機関を標的としたランサムウェアによるサイバー攻撃に関する注意喚起を行ってまいりました。今回の事務連絡は、昨今の状況を受けて厚生労働省からの改めての周知依頼となります。

今回の事務連絡の内容は以下の４点です。

１）リモート接続等に利用される、SSL-VPN 装置（特に FORTINET 社製）の脆弱性が悪用される事例が増えていることから、機器を納品した事業者等への確認や機器の内容に更新がないか点検して早期に対応してください。

２）ランサムウェアを利用したサイバー攻撃により情報が失われる事案が発生していることから、「医療情報システムの安全管理に関するガイドライン第5.1 版」の「7.2 章 見読性の確保について」（バックアップの作成、バックアップからの閲覧の確保）及び「7.3 章 保存性の確保について」（バックアップおよび履歴の保存）を参考に、バックアップを作成してください。

３）サイバー攻撃により医療情報システムに障害が発生した場合は、厚生労働省（下記連絡先）に連絡してください。

■厚生労働省　医政局研究開発振興課医療情報技術推進室
TEL ： 03-3595-2430　MAIL: igishitsu@mhlw.go.jp

標的型メールを受信した場合等は、情報処理推進機構（IPA）に相談してください。

■情報処理推進機構(IPA)　情報セキュリティ安心相談窓口
電話　03-5978-7509（平日日中のみ）　メール　anshin@ipa.go.jp

４）「医療機関のサイバーセキュリティ対策チェックリスト」及び「医療情報システム等の障害発生時の対応フローチャート」を活用いただき、対策に役立ててください。
「医療情報システムの安全管理に関するガイドライン　第5.1版」
https://www.mhlw.go.jp/stf/shingi/0000516275.html

本内容は、基本的に医療機関従事者ならびに医療機関と守秘義務契約を結んだベンダーのみに見せることができます。ホームページの一般に公開されている部分には掲載しないようお願いいたします。

つきましては、貴会におかれましても、本件についてご了知いただくと共に、貴会管下の郡市区等医師会ならびに会員への周知方につき、是非、ご高配を賜りますようお願い申し上げます。

以上

【別添資料】
・令和3年11月26日付日医宛て厚生労働省医政局研究開発振興課名事務連絡 「医療機関を標的としたランサムウェアによるサイバー攻撃について」
・別添：「医療情報システムの安全管理に関するガイドライン 第5.1 版 抜粋」

また、必要に応じて、令和3年7月6日「医療機関を標的としたランサムウェアによるサイバー攻撃について(注意喚起)」(情シ22号)も参照ください。

＜ランサムウェア対策に参考となるサイトや資料＞
■IPAのランサムウェア対策特設ページ
https://www.ipa.go.jp/security/anshin/ransom_tokusetsu.html

■IPA ランサムウェアの脅威と対策～ランサムウェアによる被害を低減するために
https://www.ipa.go.jp/files/000057314.pdf
特に、6ページ　1.5.ランサムウェアの感染経路
8ページ　3.1.ランサムウェアに感染しないための対策
9ページ　3.2.ランサムウェアの感染に備えた対策

■IPA 事業継続を脅かす 新たなランサムウェア攻撃について
～「人手によるランサムウェア攻撃」と「二重の脅迫」～
https://www.ipa.go.jp/files/000084974.pdf
特に、5. 対策

事　務　連　絡
令和３年 11 月 26 日

公益社団法人日本医師会　殿

厚生労働省医政局研究開発振興課
医療情報技術推進室

医療機関を標的としたランサムウェアによるサイバー攻撃について
（再注意喚起）

近年、国内外の医療機関を標的とした、ランサムウェアを利用したサイバー攻撃による被害が増加していることから、令和３年６月 28 日付け「医療機関を標的としたランサムウェアによるサイバー攻撃について（注意喚起）」（厚生労働省政策統括官付サイバーセキュリティ担当参事官室、厚生労働省医政局研究開発振興課医療情報技術推進室、厚生労働省医薬・生活衛生局医療機器審査管理課、厚生労働省医薬・生活衛生局医薬安全対策課事務連絡）をもって注意喚起するとともに、令和３年 10 月 20 日付け「医療情報システムの安全管理に関するガイドライン」に関する「医療機関のサイバーセキュリティ対策チェックリスト」及び「医療情報システム等の障害発生時の対応フローチャート」について」（厚生労働省医政局研究開発振興課事務連絡）をもって「医療情報システムの安全管理に関するガイドライン 第 5.1 版」の別添として、「医療機関のサイバーセキュリティ対策チェックリスト」及び「医療情報システム等の障害発生時の対応フローチャート」を策定した旨通知いたしましたが、その後も医療機関に対するサイバー攻撃の事例が複数あり、医療機関の診療体制に大きな影響が出ているところです。

つきましては、再度、貴会員等関係者に注意喚起いただきますよう、よろしくお願いいたします。

特に、医療機関において、下記の点に注意いただくよう併せて周知をお願い申し上げます。

なお、参考までに、NISC から提供された FORTINET 社製品の脆弱性情報及び同ガイドラインの抜粋を添付いたします。

記

１．リモート接続するために利用される、SSL-VPN 装置（特に FORTINET 社製）の脆弱性を悪用し、医療機関のネットワークに不正侵入し、ランサムウェアに感染させる事例が複数発生していることから、対応策として、ソフトウエア、機器等に脆弱性がないか点検し、脆弱性を発見した場合は早急に対処すること。

２．最近、国内外の医療機関を標的とし、ランサムウェアを利用したサイバー攻撃により情報が失われる事案が発生していることから、このような場合に備えて、「医療情報システムの安全管理に関するガイドライン第 5.1 版」の「7.2 章　見読性の確保について」及び「7.3 章　保存性の確保について」を参考に、バックアップを作成すること。

３．サイバー攻撃により医療情報システムに障害が発生した場合は、「医療情報システムの安全管理に関するガイドライン第 5.1 版　6.10 章　C. 最低限のガイドライン　5」を参照して所管省庁等に連絡すること。また、標的型メールを受信した場合等は、情報処理推進機構（IPA）に相談されたい。

なお、医療機関等がサイバー攻撃を受けた際の厚生労働省の連絡先は、次のとおりである。

（医療機関等がサイバー攻撃を受けた際の厚生労働省連絡先）
医政局研究開発振興課医療情報技術推進室
TEL ： 03-3595-2430
MAIL: igishitsu@mhlw.go.jp

４．「医療機関のサイバーセキュリティ対策チェックリスト」及び「医療情報システム等の障害発生時の対応フローチャート」を活用いただき、対策に役立てていただくこと。

添付資料

医療情報システムの安全管理に関するガイドライン 第5.1版 抜粋

7.2. 見読性の確保について

A. 制度上の要求事項

必要に応じ電磁的記録に記録された事項を出力することにより、直ちに明瞭かつ整然とした形式で使用に係る電子計算機その他の機器に表示し、及び書面を作成できるようにすること。

（e-文書法省令　第4条第4項第1号）

①　見読性の確保

必要に応じ電磁的記録に記録された事項を出力することにより、直ちに明瞭かつ整然とした形式で使用に係る電子計算機その他の機器に表示し、及び書面を作成できるようにすること。

（ア）　情報の内容を必要に応じて肉眼で見読可能な状態に容易にできること。

（イ）　情報の内容を必要に応じて直ちに書面に表示できること。

（施行通知　第2　2（3）①）

「診療録等の記録の真正性、見読性及び保存性の確保の基準を満たさなければならないこと。」

（外部保存改正通知　第2　1（1））

B. 考え方

見読性とは、電子媒体に保存された内容を、「診療」、「患者への説明」、「監査」、「訴訟」等の要求に応じて、それぞれの目的に対し支障のない応答時間やスループット、操作方法で、肉眼で見読可能な状態にできることである。e-文書法の精神によれば、画面上での見読性が確保されていることが求められているが、要求によっては対象の情報の内容を直ちに書面に表示できることが求められることもあるため、必要に応じてこれに対応することを考慮する必要がある。

電子媒体に保存された情報は、紙に記録された情報と違い、以下の理由によりそのままでは見読できない場合がある。

- 電子媒体に格納された情報を見読可能なように画面に呼び出すために、何らかのアプリケーションが必要である。
- 記録が、他のデータベースやマスター等を参照する形で作成されることが多く、データの作成時点で採用したマスター等に依存しなければ、正しい記録として見読できない。
- 複数媒体に分かれて記録された情報の相互関係が、そのままでは一瞥して分かりに

くい。

そのため、電子媒体に保存された情報は、保存されたこれらに適切に対応することにより、紙の記録と同等といえる見読性を確保しなければならない。

また、何らかのシステム障害が発生した場合においても、診療に重大な支障がない最低限の見読性を確保する対策も考慮に含める必要がある。特に、災害等の非常時には、システムが完全に停止してしまうおそれもあるため、定期的なバックアップを実施して、診療録等に記載された患者情報を確認できるようにしておくことが望ましい。

ネットワークを通じて外部に保存する場合は、これらのことに適切に対応することに加えて、外部保存先の機関の事情により見読性が損なわれることを考慮に含めた十分な配慮が求められる。その際には、「4.2　委託と第三者提供における責任分界」を参考にしつつ、あらかじめ責任を明確化しておき、速やかな復旧が図られるように配慮しておく必要もある。

これらのことに配慮していても、万一、保存していた情報がき損した場合等は、可能な限り速やかな復旧に努め、「診療」、「患者への説明」、「監査」、「訴訟」等の要求に応える見読性の確保を図らなければならない。

C. 最低限のガイドライン

1. 情報の所在管理

   紙管理された情報を含め、各種媒体に分散管理された情報であっても、患者ごとの全ての情報の所在が日常的に管理されていること。

2. 見読化手段の管理

   電子媒体に保存された全ての情報とそれらの見読化手段を対応付けて管理すること。また、見読化手段である機器、ソフトウェア、関連情報等は常に整備された状態にすること。

3. 見読目的に応じた応答時間

   目的に応じて速やかに検索表示又は書面に表示できるようにすること。

4. システム障害対策としての冗長性の確保

   システムの一系統に障害が発生した場合でも、通常の診療等に差し支えない範囲で診療録等を見読可能とするため、システムの冗長化（障害の発生時にもシステム全体の機能を維持するため、平常時からサーバやネットワーク機器等の予備設備を準備し、運用すること）を行う又は代替的な見読化手段を用意すること。

D. 推奨されるガイドライン

【医療機関等に保存する場合】

1. バックアップサーバ

システムが停止した場合でも、バックアップサーバと汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読できるようにすること。

2. 見読性確保のための外部出力

システムが停止した場合でも、見読目的に該当する患者の一連の診療録等を汎用のブラウザ等で見読ができるように、見読性を確保した形式で外部ファイルへ出力できるようにすること。

3. 遠隔地のデータバックアップを使用した見読機能

大規模火災等の災害対策として、遠隔地に電子保存記録をバックアップするとともに、そのバックアップデータ等と汎用的なブラウザ等を用いて、日常診療に必要な最低限の診療録等を見読できるようにすること。

【ネットワークを通じて外部に保存する場合】

医療機関等に保存する場合の推奨されるガイドラインに加え、次の事項が必要となる。

4. 緊急に必要になることが予測される診療録等の見読性の確保

緊急に必要になることが予測される診療録等は、内部に保存するか、外部に保存しているものの複製又は同等の内容の情報を医療機関等の内部に保持すること。

5. 緊急に必要になるとまではいえない診療録等の見読性の確保

緊急に必要になるとまではいえない情報についても、ネットワークや外部保存を受託する事業者の障害等に対応できるような対策を実施しておくこと。

7.3. 保存性の確保について

A. 制度上の要求事項

電磁的記録に記録された事項について、保存すべき期間中において復元可能な状態で保存することができる措置を講じていること。

（e-文書法省令　第4条第4項第3号）

③　保存性の確保

電磁的記録に記録された事項について、保存すべき期間中において復元可能な状態で保存することができる措置を講じていること。

（施行通知　第2　2（3）③）

「診療録等の記録の真正性、見読性及び保存性の確保の基準を満たさなければならないこと。」

（外部保存改正通知　第2　1（1））

B. 考え方

保存性とは、記録された情報が法令等で定められた期間にわたって真正性を保ち、見読可能にできる状態で保存されることをいう。

診療録等の情報を電子的に保存する場合に、保存性を脅かす原因として、例えば下記のものが考えられる。

(1) コンピュータウイルスや不適切なソフトウェア等による情報の破壊及び混同等
(2) 不適切な保管・取扱いによる情報の滅失、破壊
(3) 記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取り
(4) 媒体・機器・ソフトウェアの不整合による情報の復元不能
(5) 障害等によるデータ保存時の不整合

これらの脅威をなくすために、それぞれの原因に対する技術面及び運用面での各種対策を施す必要がある。

(1) コンピュータウイルスや不適切なソフトウェア等による情報の破壊及び混同等

コンピュータウイルス又はバグ等によるソフトウェアの不適切な動作により、電子的に保存された診療録等の情報が破壊されるおそれがある。このため、コンピュータウイルスや不適切なソフトウェアによるこれらの情報へのアクセスを防止しなければならない。

また、情報を操作するソフトウェアが改ざんされていないこと、及び仕様のとおりに動作

していることを確認しなければならない。

さらに、保存されている情報が、改ざんされていない情報であることを確認できる仕組みを設けることが望ましい。

(2) 不適切な保管・取扱いによる情報の滅失、破壊

電子的な情報を保存している媒体が不適切に保管されている、あるいは情報を保存している機器が不適切な取扱いを受けているために情報が滅失してしまうか、破壊されてしまうことがある。このようなことが起こらないように、情報が保存されている媒体及び機器の適切な保管・取扱いが行われるように、技術面及び運用面での対策を施さなければならない。

使用する記録媒体や記録機器の環境条件を把握し、電子的な情報を保存している媒体や機器が置かれているサーバ室等の温度、湿度等の環境を適切に保持する必要がある。また、サーバ室等への入室は、許可された者以外が行うことができないような対策を施す必要がある。

また、万一、滅失であるか改ざん又は破壊であるかを問わず、情報が失われるような場合に備えて、定期的に診療録等の情報のバックアップを作成し、そのバックアップを履歴とともに管理し、復元できる仕組みを備える必要がある。この際に、バックアップから情報を復元する際の手順と、復元した情報を診療に用い、保存義務を満たす情報とする際の手順を明確にしておくことが望ましい。

(3) 記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取り

記録媒体、記録機器の劣化による読み取り不能又は不完全な読み取りにより、電子的に保存されている診療録等の情報が滅失してしまうか、破壊されてしまうことがある。これを防止するために、記録媒体や記録機器の劣化特性を考慮して、劣化が起こる前に新たな記録媒体や記録機器に複写する必要がある。

(4) 媒体・機器・ソフトウェアの不整合による情報の復元不能

媒体・機器・ソフトウェアの不整合により、電子的に保存されている診療録等の情報が復元できなくなることがある。具体的には、システム移行時にマスタデータベース、インデックスデータベースに不整合が生じること、機器・媒体の互換性がないことにより情報の復元が不完全となる又は読み取りができなくなること等である。このようなことが起こらないように、システム変更・移行時の業務計画を適切に作成する必要がある。

(5) 障害等によるデータ保存時の不整合

ネットワークを通じて外部に保存する場合、診療録等を転送している途中にシステムが停止したり、ネットワークに障害が発生したりして正しいデータが外部の委託先に保存されないことも起こり得る。その際は、再度、外部保存を委託する医療機関等からデータを転

送する必要が生じる。

そのため、委託する医療機関等は、医療機関等内部のデータを消去する等の場合には、外部保存を受託する事業者において、当該データが保存されたことを確認してから行う必要がある。

C. 最低限のガイドライン

【医療機関等に保存する場合】

1. コンピュータウイルスや不適切なソフトウェア等による情報の破壊、混同等の防止
   (1) いわゆるコンピュータウイルスを含む不適切なソフトウェアによる情報の破壊、混同等が起こらないように、システムで利用するソフトウェア、機器及び媒体を適切に管理すること。
2. 不適切な保管・取扱いによる情報の滅失、破壊の防止
   (1) 記録媒体及び記録機器の保管及び取扱いについて、運用管理規程を作成し、適切な保管及び取扱いを行うよう関係者に周知徹底するとともに、教育を実施すること。また、保管及び取扱いに関する作業履歴を残すこと。
   (2) システムが情報を保存する場所（内部、可搬媒体）を明示し、その場所ごとの保存可能容量（サイズ）、期間、リスク、レスポンス、バックアップ頻度、バックアップ方法等を明確にすること。これらを運用管理規程に定めて、その運用を関係者全員に周知徹底すること。
   (3) 記録媒体の保管場所やサーバの設置場所等には、許可された者以外が入室できないような対策を実施すること。
   (4) 電子的に保存された診療録等の情報に対するアクセス履歴を残すとともに、その履歴を適切に管理すること。
   (5) 各保存場所における情報がき損したときに、バックアップされたデータ等を用いてき損前の状態に戻せるようにすること。もし、き損前と同じ状態に戻せない場合には、き損された範囲が容易に分かるようにしておくこと。
3. 記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止
   (1) 記録媒体が劣化する前に、当該記録媒体に保存されている情報を新たな記録媒体又は記録機器に複写すること。記録媒体及び機器ごとに劣化が起こらずに正常に保存が行える期間を明確にするとともに、使用開始日、使用終了予定日を管理して、月に一回程度の頻度でチェックを行うこと。使用終了予定日が近づいた記録媒体又は記録機器は、そのデータを新しい記録媒体又は記録機器に複写すること。これらの一連の運用の流れを運用管理規程に定めるとともに、関係者に周知徹底すること。
4. 媒体・機器・ソフトウェアの不整合による情報の復元不能の防止
   (1) システム更新の際の移行を迅速に行えるように、診療録等のデータについて、標準

形式が存在する項目は標準形式で、標準形式が存在しない項目は変換が容易なデータ形式で、それぞれ出力及び入力できる機能を備えること。

(2) マスタデータベースの変更の際に、過去の診療録等の情報に対する内容の変更が起こらない機能を備えること。

【ネットワークを通じて医療機関等の外部に保存する場合】

医療機関等に保存する場合の最低限のガイドラインに加え、次の事項が必要となる。

5. データ形式及び転送プロトコルのバージョン管理と継続性の確保を行うこと

保存義務のある期間中に、データ形式や転送プロトコルがバージョンアップ又は変更されることが考えられる。その場合、外部保存を受託する事業者は、以前のデータ形式や転送プロトコルを使用している医療機関等が存在する間は対応を維持しなくてはならない。

6. ネットワークや外部保存を受託する事業者に設備の劣化対策の実施を求めること

ネットワークや外部保存を受託する事業者の設備の条件を考慮し、回線や設備が劣化した際にそれらを更新する等の対策を実施するよう求めること。

D. 推奨されるガイドライン

【医療機関等に保存する場合】

1. 不適切な保管・取扱いによる情報の滅失・破壊の防止

(1) 記録媒体、記録機器及びサーバは、許可された者しか入ることができない部屋に保管するとともに、その部屋の入退室の履歴を残し、保管及び取扱いに関する作業履歴と関連付けて保存すること。

(2) サーバ室には、許可された者以外が入室できないよう、鍵等の物理的な対策を施すこと。

(3) 診療録等のデータのバックアップを定期的に取得するとともに、その内容に対する改ざん等が行われていないことを検査する機能を備えること。

2. 記録媒体、設備の劣化による情報の読み取り不能又は不完全な読み取りの防止

診療録等の情報をハードディスク等の記録機器に保存する場合は、RAID-1 又は RAID-6 相当以上のディスク障害に対する対策を行うこと。

医療情報システムの安全管理に関するガイドライン 第5.1版 抜粋

6.10. 災害、サイバー攻撃等の非常時の対応（抜粋）

C. 最低限のガイドライン

5. コンピュータウイルスの感染などによるサイバー攻撃を受けた（疑い含む）場合や、サイバー攻撃により障害が発生し、個人情報の漏洩や医療提供体制に支障が生じる又はそのおそれがある事案であると判断された場合には、「医療機関等におけるサイバーセキュリティ対策の強化について」（医政総発1029 第1号 医政地発1029 第3号 医政研発1029 第1号 平成30年10月29日）に基づき、所管官庁への連絡等、必要な対応を行うほか、そのための体制を整備すること。また上記に関わらず、医療情報システムに障害が発生した場合も、必要に応じて所管官庁への連絡を行うこと。

厚生労働省連絡先

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

※ 独立行政法人等においては、各法人の情報セキュリティポリシー等に基づき所管課へ連絡すること。

なお、情報処理推進機構は、コンピュータウイルスや不正アクセスに関する技術的な相談を受け付ける窓口を開設している。標的型メールを受信した、Webサイトが何者かに改ざんされた、不正アクセスを受けた等のおそれがある場合は、下記連絡先に相談することが可能である。

連絡先 情報処理推進機構 情報セキュリティ安心相談窓口（03-5978-7509）