

「医療機関向けランサムウェア 対応検討ガイダンス」の制定背景・概要

(NPO) デジタル・フォレンジック研究会 理事/ 「医療」分科会主査
(一社) 医療ISAC 理事

江原悠介

1. ガイダンス制定の背景(1/3)

サイバー脅威は巧妙化・高度化しており、海外の医療機関が被害を受けていたランサムウェアの感染事例は国内にも見受けられる事態になり始めている。

直近でも、大阪の総合病院や徳島の総合病院が相次いでランサムウェア感染し、一部では患者診療の継続性に深刻な影響を及ぼす事態に至っていることはメディア報道の通りである。

■「医療機関向けランサムウェア対応検討ガイダンス」より

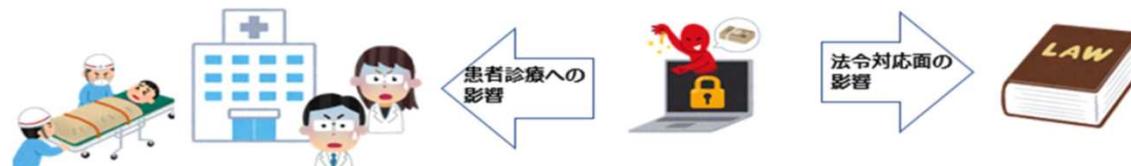
1. 本ガイダンス制定の背景(1/3)

ランサムウェアによるサイバー攻撃のリスクが急増するなか、その脅威は今や国内の医療機関にも及んでいる。実際に日本国内でもランサムウェアにより医療情報システムが利用不可となり、患者診療の継続性に影響を与える事案が報告されている。

法令上、病院は個人データの漏洩、滅失、毀損を防止するための必要かつ適切な安全管理措置を講じる義務を負っている。

さらに、電子カルテなどは、法的な保存期限を定められた法定保存文書であり、この文書が暗号化され復旧不可となることは、その病院にとって医師法・医療法等の各種法令違反となるおそれがある。また、電子カルテ等は、病院や医療従事者に対する民事訴訟が発生した場合においては自らを守る重要な証拠資料である。ランサムウェアによる被害は、病院において様々な不利益をもたらすといえる。

そのため、医療機関において、医療情報システムを標的とするランサムウェアへの備えは、患者診療や法令遵守を維持する上で喫緊の課題となっていると言える。



1. ガイダンス制定の背景(2/3)

医療機関におけるセキュリティは3省2ガイドラインを前提としているが、これらはいくまで紙媒体で管理していた患者情報を**電子的に管理する上で求められる諸要件**をまとめたものであり、**悪意ある外部の攻撃者によるサイバー脅威を想定した対策要件の整理**までには至っていない。

21年10月に厚生労働省から厚労省安全管理ガイドラインの別添資料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・「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」が公開され、さらに10月下旬の徳島の総合病院の事案を受け、厚労省から11月下旬に再注意喚起の事務連絡が行われている。

ただし、重要な点は、本連絡でフォーカスされるサイバー対策の前提となる別添資料群はいくまで**サイバー攻撃全般を想定した内容であり、ランサムウェア対策の観点からは補足すべきポイントが存在すること**と考えている。

■「医療機関向けランサムウェア対応検討ガイダンス」より

■「医療機関向けランサムウェア対応検討ガイダンス」より

2021/11/26:厚生労働省「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)」

1. 本ガイダンス制定の背景(2/3)

一方、国内の医療機関の多くでは、セキュリティ部門を持ち、専門性のある要員がランサムウェア対策に積極的に対応するだけの**経済的・人的リソースを持ち合わせない状況**でもある。

こうした状況を前提とせず、標準的なランサムウェア対策のベストプラクティスを提示しても、その対策の多さの前に、**医療機関として「どこから優先的に着手すべきなのか」「必須対策はどれで、推奨対策はどれなのか」という問いに直直する可能性が高い**と言える。

優先着手の必須対策は???

優先度は???



■厚労省安全管理GLの別添資料

医療情報システムの安全管理に関するガイドライン
医療機関のサイバーセキュリティ対策チェックリスト

近年、医療情報システムへのサイバー攻撃が数多く発生しており、医療情報の漏えいや、重要機密の複製・毀損が生じた事案も増加傾向にあり、医療機関を中心に、患者情報やサイバーセキュリティ対策の強化が求められています。

本チェックリストは、各医療機関において自らのサイバーセキュリティ対策の現状を把握することを目的に、そのチェック項目を整理したものであり、必ずしもすべての項目を実施している必要はなく、詳細は別途参照ください。

- 医療情報システムの安全管理に関するガイドライン(第1版) 本編
- オンライン診療の適切な実施に関する指針
- 電子処方箋の適切な実施に関する指針
- オンライン診療環境等、レセプトオンライン請求及び健康保険組合に対する社会保険手続に係る電子申請システムに係るセキュリティに関するガイドライン
- 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
- サイバーセキュリティ経営ガイドライン(第1版)
- 中小企業の情報セキュリティ対策ガイドライン(第1版)

なお、「医療情報システムの安全管理に関するガイドライン」の内部が、文書法、個人情報保護法等への対応を目的としたセキュリティ管理など多岐に亘る一方、本チェックリストは「医療情報システムの安全管理に関するガイドライン」のみを整理しているためチェックリストではない。幅広くサイバーセキュリティ対策に特化した内容となっていることにご留意ください。

サイバー攻撃全般を想定した資料



事務連絡
令和3年11月26日

一般社団法人日本病院会 殿

厚生労働省医政局研究開発部医務課
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部医務課医療情報技術推進室、厚生労働省医薬・生活衛生局医薬安全管理課、厚生労働省医薬・生活衛生局医薬安全管理課)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部医務課事務連絡」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」を確定した旨通知いたしました。その後、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があります。

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。

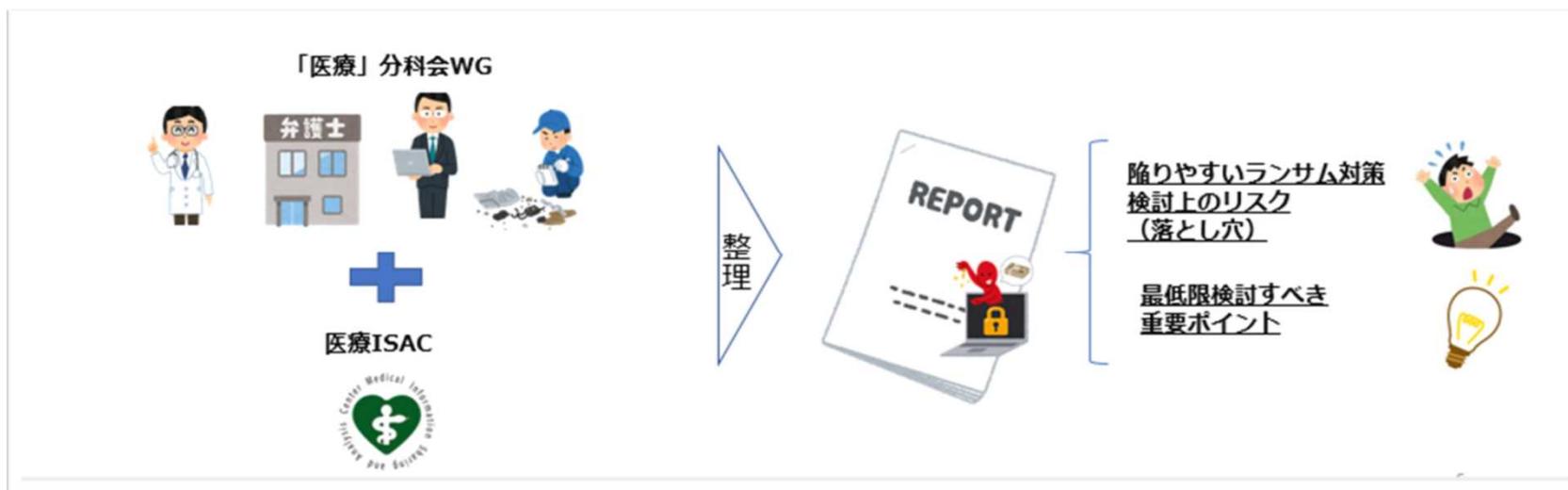
特に、医療機関において、下記の点に注意いただくよう併せて周知をお願いします。

1. ガイダンス制定の背景(3/3)

そのため、医療」分科会では、厚労省安全管理GLの別添のサイバーセキュリティ関連資料を基にして、**国内の医療機関が喫緊のリスクとして直面するランサムウェアに備える**べく、検討すべきポイントを医療ISACとの連携のもと整理し、ガイダンス（手引き）として公表することにした。

具体的には、ランサムウェアへの対応を検討する際に、**どのような陥りやすいリスク（落とし穴）があり、それを回避するため、どのような検討を最低限行うべきなのか**についてまとめている。

■「医療機関向けランサムウェア対応検討ガイダンス」より



2. ガイダンス概要 (1/5)

本ガイダンスで厚労省安全管理GL別添資料を基に、ランサムウェアという個別マルウェアへの対応を検討する上で重点的に考えるべき11件のポイントを、「**必須**」/「**推奨**」の2区分より整理している。

■「医療機関向けランサムウェア対応検討ガイダンス」より

3. ランサムウェア対応検討上のポイント

～3-1：＜落とし穴＞回避に向けた検討ポイント概要(1/2)

ランサムウェア対策を検討する上で**医療機関が陥りやすい＜落とし穴＞**、及びそれを回避するための検討ポイントの概要は以下の通り。



陥りやすい11の＜落とし穴＞

- ① バックアップデータまで暗号化されてしまった
- ② 冗長化して安心していたのに、待機系システムまで暗号化されてしまった
- ③ システム利用を優先する医師の声に負けて、ネットワークに繋いだら、ランサム感染範囲が拡大してしまった
- ④ セキュリティベンダーに調査・復旧を依頼する費用支出を避けるため、自前に対応したところ、被害範囲が拡大し、かえって復旧コストがかかることに
- ⑤ ネットワーク構成図からはデータの流れが把握できず、ランサムの感染拡大に関する机上調査では役に立たなかった
- ⑥ 感染端末のケーブルをとりあえず外したが、担当者が至急の作業があるとのことだったので、スタンドアロンで利用を許した
- ⑦ いつものシステムベンダーに復旧依頼までお願いしたが、調査・復旧が進まなかった
- ⑧ 診療系ネットワークは外部と繋がっていないので、調査範囲は非診療系のみにしたが、後日、診療系にまで被害が及んでいた
- ⑨ データ復旧上の身代金がそれほど高くなかったので払うことにしたが、想定通りの復旧に至らなかった
- ⑩ システム復旧のため、感染端末のバックアップを取り、リストアしたらまた感染検知が発生した
- ⑪ 身代金を払って安心していたら、患者の情報が結局暴露され、メディアや患者から問い合わせが続いた



落とし穴回避に向けた検討ポイント（概要）

- ▶ オフライン型の外部記憶媒体にバックアップデータを保管しているか **必須**
- ▶ コールドスタンバイ方式のシステム冗長化を採用しているか
- ▶ ランサムウェアの＜危なさ＞をしっかりと院内関係者に周知できているか **必須**
- ▶ ランサムウェアに備え、必要なサイバー保険に加入しているか
- ▶ システム間のデータの流れ、相互の接続状況の情報まで構成図に含まれているか
- ▶ 感染端末の取扱いは十分に理解されているか
- ▶ インシデントに対応できるセキュリティベンダーの目星をつけているか **必須**
- ▶ 診療系NWは安全という＜神話＞に依らない調査ができているか
- ▶ 身代金支払いに伴う様々なリスクが検討されているか **必須**
- ▶ 感染後の端末を感染前に戻すことの困難さを理解しているか
- ▶ ランサム被害に伴う情報暴露の対応の困難さは想像されているか

2. ガイダンス概要 (2/5)～バックアップ

「必須」区分とした項目のなかで、特に重要度の高い項目としては、**バックアップデータの管理方式の検討**になる。バックアップデータの取得・退避方法の検討はランサムウェアを想定した場合、最も重要なポイントの一つである。

■「医療機関向けランサムウェア対応検討ガイダンス」より

3. ランサムウェア対応検討上のポイント

～3-2：詳細その①：バックアップデータの管理(1/2)

経営層
管理責任者
一般利用層

関連する対策番号
0-1

サイバーセキュリティ体制整備と情報収集

医療情報システムがランサムウェアに感染した場合、システム内部のデータだけでなく、該当システムに搭載されるバックアップメディア (DAT、LTO、RDX等)、ネットワーク上のストレージ (NAS) 等、システム内外へ感染は容易に拡大する。

そのため、ランサムウェアに備えたバックアップデータは院内のシステム・ネットワーク内部でなく、物理的にそこから切り離された環境、例えば**オフラインの媒体での管理**が推奨される。

陥りやすい落とし穴

バックアップデータまで暗号化されてしまった

ベンダにはバックアップを定期的取得する指示しているので大丈夫ですよ！

ベンダはバックアップ取得先まで指示されていないため、NASに保管。ランサム感染でNASまで暗号化され、バックアップデータが使えない状態。

必須 検討すべきポイント

重要度の高い医療情報システムのバックアップは、院内システム・ネットワーク内部で管理するのではなく、物理的に切り離された環境で管理すること

■対応方針 (例)

→

オフラインの外部記憶媒体
バックアップデータの移行

重要度の非常に高い電子カルテシステムのデータは、不定期にでも、外部記憶媒体にバックアップし、オフラインで保管する運用とする

必須検討上のポイント

データの管理(2/2)

経営層
管理責任者
一般利用層

関連する対策番号
0-1

サイバーセキュリティ体制整備と情報収集

クラウド上にデータバックアップを保管することも一案である。クラウド上にデータコピーを行うバックアップ方式の場合、**ランサムウェアへコピーされ、そこで感染拡大をもたらすリスク**がある。バックアップへの**アクセス管理が十分でない場合**、外部のクラウド上のデータにウェアも存在する。バックアップを保管する場合は、**クラウド上のバックアップまで感染されないよう**が必要である。

クラウド上にデータバックアップ保管する運用において注意すべきポイント

クラウド

クラウドデータバックアップデータまでクラウド

クラウド

一般ユーザによる読み書きが可能
読み書き権限を悪用してデータを暗号化

クラウド上のバックアップデータを誰でも読み書き(操作)可能にしていたため、その権限を悪用され、クラウド上のデータに感染が拡大

バックアップ取得を行う時のみデータ同期を実行すること

クラウド上のバックアップデータには、少なくとも一般ユーザが読み書きできる権限を付与しないこと

2. ガイダンス概要 (3/5)～関係者へのランサム危険性の周知

同様に「必須」区分に該当するものは、バックアップ運用等の技術的対策ではなく、人的対策に関係するものである。これは医療機関固有の業務構造を前提とするため、**院長・理事長によるトップダウン型のガバナンスのもとで行われることが推奨**される。

■「医療機関向けランサムウェア対応検討ガイダンス」より

3. ランサムウェア対応検討上のポイント

～3-2：詳細その③：ランサムウェアの危険性の周知

経営層
管理責任者
一般利用者

関連する
対策番号： 0-1

サイバーセキュリティ体制整備と情報収集

ランサムウェアに感染した医療情報システムは院内ネットワークから切り離し、利用停止とする必要がある。ただ、患者診療を重視する現場の医療従事者にとっては診療の効率性・継続性を損なうことになるため、**通常の運用に戻すことが強く求められ、その結果、感染範囲が拡大するリスク**がある。特に二重脅迫型のランサムウェアの場合、患者情報が外部へ公開されてしまうことは、**医療従事者にとっては職務上の守秘義務の侵害**をもたらすことにもなり、また別のリスクが発生することになる。そのため、**ランサムウェアが通常のコンピュータウイルスとは異なる点を院長・理事長等の病院のトップマネジメント層のコミットのもとで、しっかり院内の医療従事者に周知・理解させ、本来であれば回避できた被害の拡大を防げる風土を醸成することが重要である。**

陥りやすい落とし穴

システム利用を優先する現場の声に負けて、ネットワークに繋いだら、ランサム感染範囲が拡大してしまった

なんで電カルが使えないんだ！
いまずく復旧させろ！

仕方ないからネットワークに繋ごうか、
多分大丈夫だろうし、

院内ネットワーク全体にランサム感染が拡大し、
大問題に発展

必須

検討すべきポイント

院長・理事長等のトップマネジメント層から、ランサムウェアの危険性・特殊性を院内の医療従事者へ周知し、院内IT担当者の復旧サポートの重要性を理解させるための教育的な仕組みを作ること

■対応方針（例）

院長

+

セキュリティ委員会

→

ランサムの脅威に関する現場への理解促進

院長・理事長の関与のもと、情報セキュリティ委員会等でランサムウェアの危険性を院内従事者へ周知する教育プログラムを作成。定期的なセキュリティ研修を通して院内の理解を醸成する。

2. ガイダンス概要 (4/5)～適切なベンダーとのコミュニケーション

セキュリティベンダーとの連携も重要である。セキュリティベンダーとの連携不全が原因で、院内のランサムウェア感染拡大を招いた事例もあるため、「餅は餅屋」という考えのもとで、**サイバー脅威の被害を受けた場合は即座にセキュリティベンダーと適時に連携するコミュニケーションパスを確保しておくことが必要**となる。

■「医療機関向けランサムウェア対応検討ガイドンス」より

3. ランサムウェア対応検討上のポイント

～3-2：詳細その⑦：セキュリティベンダーとの連携(1/2)

経営層
管理責任者
一般利用者

関連する：	2-1	原因調査（脳力）
対策番号	2-10	被害状況調査
	2-14	証拠保全の実施
	3-2	ベンダ/事業者へ依頼

保守契約を結んでいる医療情報システムのベンダーはあくまでシステムの専門家であり、セキュリティの専門家ではない可能性に留意すべきである。感染状況の調査や原因分析、復旧対応を行う際には、**専門性を持ったセキュリティベンダーに依頼を行う必要がある**。保守契約の中でのシステム復旧をセキュリティに精通しないベンダーに指示し続けることは、**かえって感染範囲を拡大させ、復旧の困難度を増大させるリスク**がある。よって、ケーブルを外した後は、**セキュリティベンダーを交えて復旧計画を検討の上、対応を図ることが推奨される**。

陥りやすい落とし穴



いつものシステムベンダーに被害復旧依頼までお願いしたが、調査・復旧が進まなかった

ウイルスに感染しておたくのシステムが使えない！保守契約あるんだから復旧させろ！

セキュリティベンダでないから分からないけど、ネットで調べて対応策を探さない！



結果、感染が院内ネットワーク全体へ拡大し、他のシステムまで暗号化されることに。

必須 検討すべきポイント



セキュリティに詳しくないシステムベンダーに無理に調査・復旧指示を行うのではなく、セキュリティインシデントに専門的に対応できるセキュリティベンダーと連携すること

■対応方針（例）

セキュリティベンダーの目星調査 → 119番 → 感染時には専門家にすぐに対応してもらえる連絡体制をとる

ランサムウェア感染の状況調査・証拠保全・復旧を行える専門的なセキュリティベンダーに平時から目星を付けておく。（転ばぬ先の杖）
それにより、感染発覚後に即座にセキュリティベンダーに依頼を行えるようになること。

8

2. ガイダンス概要 (5/5)～身代金支払い要否のリスク検討

ランサムウェア被害を最短で突破する方法、つまり身代金支払いについても様々なリスクが付随することは慎重に検討しなければならない。

■「医療機関向けランサムウェア対応検討ガイダンス」より

3. ランサムウェア対応検討上のポイント

～3-2：詳細その⑨：身代金支払いの検討(1/2)

経営層	関連する	2-12	方針指示
管理責任者	対策番号	3-1	復旧指示
一般利用者			

ランサムウェアに感染すると、暗号化を解除するために身代金を仮想通貨等で支払うように要求されるが、支払いを行っても**必ずしも復旧するとは限らない**点に注意すべきである。

また、身代金を支払う行為はサイバー攻撃集団という**反社勢力へ加担**するリスク、自分たちが**サイバー攻撃コミュニティへ「金払いの良いお客さん」であることを伝える**リスクが伴う。特に反社勢力への資金提供（身代金支払いと同等）が善管注意義務違反と判断された判例もあるため、**病院の経営陣の善管注意義務の問題**と捉え、弁護士にも相談の上、慎重に判断する必要がある。

陥りやすい落とし穴

データ復旧上の身代金がそれほど高くなかったので払うことにしたが、**想定通りの復旧に至らなかった**

急いでシステム復旧しないといけないから、今回は身代金支払って対応しよう

身代金を支払ったのにデータは半分も復旧せず、システムとして利用できない状況。さらに今度は別の部門システムが異なる攻撃集団によりランサムウェア攻撃を受け、以前より高い身代金を要求される事態に。

必須 検討すべきポイント

データ復旧等に向けた**対応の選択肢として、身代金を支払うという選択肢は存在するが、必ずしも想定する復旧には至らないリスクがある**。こうした検討は病院経営上の善管注意義務に直結する問題でもあるため、**専門家に相談して、慎重に対応方法を検討すること**

■対応方針（例）

データ復旧できないリスク

反社への加担の可能性

更なる攻撃のリスク

身代金を払うことには様々なリスクがあることをしっかり検討のうえ、対応方針を策定すること

25

3. まとめ

END