

---

# 医療機関向け ランサムウェア対応検討ガイドンス

特定非営利活動法人  
デジタル・フォレンジック研究会  
「医療」分科会

一般社団法人医療ISAC

# 目次

---

1. 本ガイドダンス制定の背景
2. 本ガイドダンスの位置付け
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
  - 3-2. 検討ポイント詳細
  - 3-3. ランサムウェア対応フローチャート

Appendix.

- ・用語集
- ・本ガイドダンス制定WG参加者リスト

---

## 1 .本ガイダンス制定の背景

# 1. 本ガイドンス制定の背景(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. 本ガイドンス制定の背景(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、医療機関としても「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」という問いに直面する可能性が高いと言える。

推奨策は???



優先着手の必須対策は???

# 1. 本ガイドンス制定の背景(3/3)

このような状況を受け、当研究会「医療」分科会では、サイバーセキュリティの専門家、デジタルフォレンジックサービスの専門家、弁護士、医師等の有志のもとでWGメンバーを結成し、（一社）医療ISACとの連携のもと、**セキュリティ面の経済的・人的リソースが十分でない状況下でランサムウェア対策を検討しようとする医療機関を想定読者として、ランサムウェア対応上の重要な検討ポイント**を整理の上、本ガイドンスにて取りまとめた。

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。



---

## 2.本ガイダンスの位置付け

## 2.本ガイドンスの位置付け(1/3)

本ガイドンスは、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（5.1版）」の別添資料として、21年10月に公開された「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」におけるサイバー攻撃全般を想定した対応策を元にしつつ、**ランサムウェアへの対応を検討する上で陥りやすい落とし穴、それを回避するための検討ポイントにフォーカスすることで、厚生労働省より公開された資料を補足することを目的**としている。

そのため、本ガイドンスとともに、厚生労働省の別添資料群もあわせて確認することが推奨される。

### ■厚労省安全管理GLの別添資料



サイバー攻撃全般を想定した資料

### 本ガイドンス



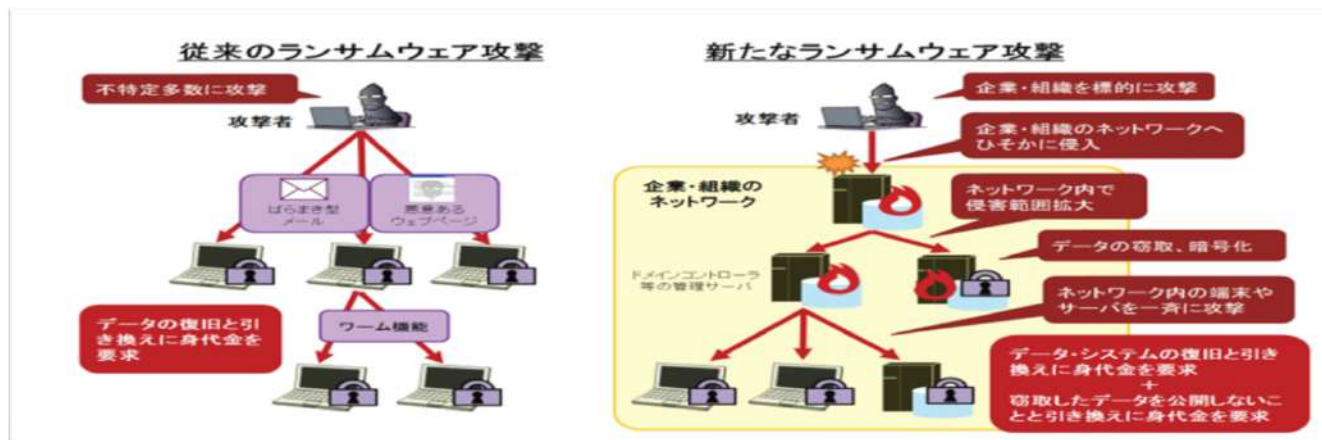
**ランサムウェアという  
特定のサイバーリスク  
にフォーカスした内容**



## 2.本ガイダンスの位置付け(2/3)

現在のランサムウェアはシステムを暗号化して、復旧の引き換えに身代金を要求する従来のパターンより、システムを暗号化するとともに、データを窃取し、その外部公開の停止と引き換えに身代金を要求する新たな攻撃パターン（二重脅迫型）が多い状況である。

そのため、本ガイダンスでは**従来のパターンのみでなく、この新たな二重脅迫型の攻撃パターンも含めた検討ポイント**を取りまとめている。



## 2.本ガイダンスの位置付け(3/3)

検討ポイントは**必須/推奨の二つの観点**で分類している。また、厚生労働省「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」上の**対策番号**と紐づけ、その**対策の検討・対応主体**として定義されている院内の関係者も把握できるようにしている。

医療機関にて本フローチャートに応じてランサムウェア対応を検討する際には、**各対策番号について、関係する院内の検討主体が主体となり、検討ポイントの内容を考慮のうえ、具体的な対応を考えることが推奨される。**

### 必須・推奨の考え方

必須

**ランサムウェア対応の際に、必ず検討すべき事項。**  
本事項の検討が十分でない場合、ランサムウェアに感染した場合、対応手続上、深刻なリスクを招く。

推奨

**【必須】ほどではないが、ランサムウェア対応の際に、検討することが強く推奨される事項。**  
本事項をしっかりと検討することで、ランサム対応の有効性を高めることができる。

### 関連する対策番号

「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」で示される対策のどこで、該当する検討を行うべきかを示している

例1) フローチャートの対策番号0-1で検討すべきポイント

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
----------	-----	---------------------

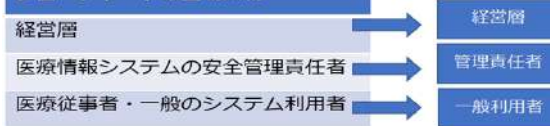
例2) フローチャートの対策番号1-2、及び2-6それぞれで検討すべきポイント

関連する対策番号	1-2	ケーブル等の切離
	2-6	被害拡大防止

### 関係する検討主体

「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」で示される対策の検討・対応主体が誰かを示している

#### フローチャートの登場人物



例1) 経営層が検討すべき対策

経営層
管理責任者
一般利用者

例2) 経営層、及び医療情報システムの安全管理責任者が検討すべき対策

経営層
管理責任者
一般利用者

## (参考) ランサムウェア感染被害イメージ

ランサムウェアに感染した場合の脅迫メッセージは様々な方式で表示される。不審なファイルをクリックすると直後に脅迫メッセージがポップアップで表示されたり、壁紙に強制指定される、プリンタから脅迫メッセージが記載された用紙が排出される等、ランサムウェアによってパターンは異なる。

(例1) Locky (データ暗号化ランサムウェア) に感染した場合、以下のようなポップアップが表示される



(例2) LOCKBIT (データ暗号化及び情報暴露型ランサムウェア) に感染した場合、以下のような画面が壁紙に強制指定される



---

### 3. ランサムウェア対応検討上のポイント

# 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、自前で対応したところ、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いでいないので、調査範囲は非診療系のみにしたら、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）

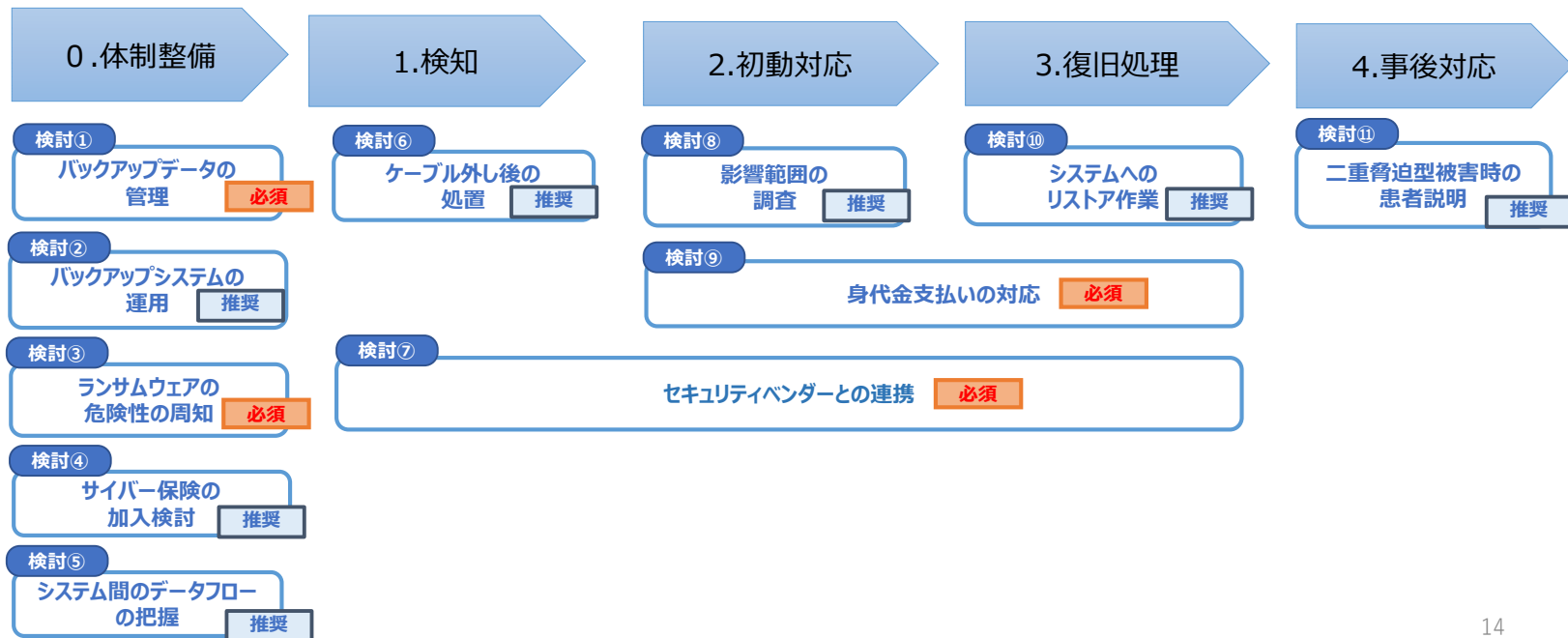
- ▶ オフライン型の外部記憶媒体にバックアップデータを保管しているか
- ▶ コールドスタンバイ方式のシステム冗長化を採用しているか
- ▶ ランサムウェアの＜危なさ＞をしっかりと院内関係者に周知できているか
- ▶ ランサムウェアに備え、必要なサイバー保険に加入しているか
- ▶ システム間のデータの流れ、相互の接続状況の情報まで構成図に含まれているか
- ▶ 感染端末の取扱いは十分に理解されているか
- ▶ インシデントに対応できるセキュリティベンダーの目星をつけているか
- ▶ 診療系NWは安全という＜神話＞に依らない調査ができているか
- ▶ 身代金支払いに伴う様々なリスクが検討され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

# 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(2/2)

＜落とし穴＞を回避するための検討ポイントを必須/推奨の2つの観点より分類し、厚生労働省「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」の時間区分に応じて以下の通り整理している。

各検討ポイントの詳細は次頁以降を参照。



# 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

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に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かったため、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に。



**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）



バックアップデータの移行

オフラインの外部記憶媒体

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

### 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(2/2)

経営層

管理責任者

一般利用者

関連する  
対策番号

0-1

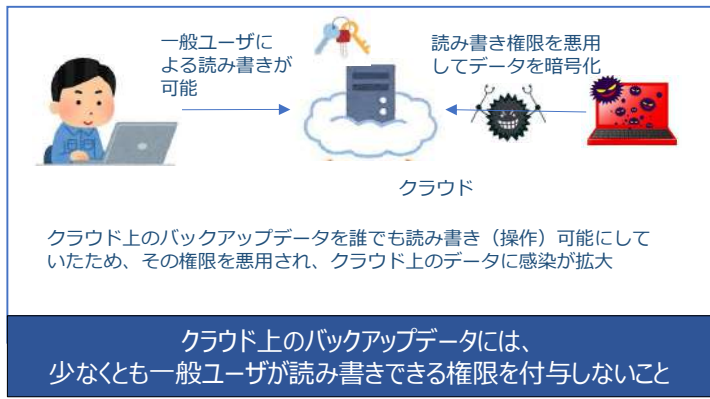
サイバーセキュリティ  
ディ体制整備と  
情報収集

オフライン媒体での管理以外にも、**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。ただし、院内システムと常に同期を取り、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、**ランサムウェアに感染したデータまでクラウド上へコピーされ、そこで感染拡大をもたらすリスク**がある。

また、クラウド上に保管したデータバックアップへの**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まで感染を拡大していくランサムウェアも存在する。

そのため、クラウド上にデータ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に運用方法をしっかり検討する**ことが必要である。

#### ■ランサムウェア対策として、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





# 3. ランサムウェア対応検討上のポイント

～3-2：詳細その②：バックアップシステムの運用

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  
ディ体制整備と  
情報収集

本番系（主系）の医療情報システム上のデータをリアルタイムで待機系（副系）システムと同期させ、稼働系が利用不可になるとともに待機系へ切り替える**ホットスタンバイ/ウォームスタンバイ方式**では、稼働系がランサムウェアに感染した場合、そのまま**待機系へも被害が及ぶため危険**である。

医療機関ではシステムの冗長化設計はホット/ウォームスタンバイ方式が多いが、通常時は待機系は停止させ、緊急時にのみ立ち上げるという**コールドスタンバイ方式の必要性**についてしっかり検討することが推奨される。

## 陥りやすい落とし穴



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



電カルはリアルタイム冗長化してます！稼働系が落ちてても、すぐに待機系に切り替わります！！

システム障害の観点で稼働系/待機系のリアルタイム同期していたため、稼働系のランサム感染がそのまま待機系に反映。両方とも使えない状態に。



## 推奨

## 検討すべきポイント



ランサムウェア被害によるネットワーク経由感染を考慮して、すぐに切り替わる**ホット/ウォームスタンバイ方式**でなく、**コールドスタンバイ方式**で待機系の運用を行うこと

## ■対応方針（例）



ランサムウェアの備えの観点より、異常時以外は稼働停止する**コールドスタンバイ方式**での待機系(バックアップ)システムの運用を検討すること

# 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！  
いますぐ復旧させろ！

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。

# 3. ランサムウェア対応検討上のポイント

～3-2：詳細その④：サイバー保険の加入検討

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場合に必要な調査・復旧費用は医療機関にとっては想定外の支出であり、それを回避するため、保守契約を結ぶシステムベンダーに対応を指示することで、事態の収束を図ろうとする傾向がある。

しかし、こうした目先の支出を避けようとする対応は、**結果的に感染範囲の拡大を招き、より大きな調査・復旧コストをもたらすリスク**が高い。

そのため、仮にランサムウェアに感染したとしても、費用面の懸念なく、適切な対応をタイムリーに行うことができるように、**サイバー保険に加入するという選択肢を検討**することは重要である。

陥りやすい落とし穴



セキュリティベンダに調査・復旧を依頼する費用支出を避けるため、自前で対応したところ、被害範囲が拡大し、かえって復旧コストがかかることに




ランサム感染後にベンダーに調査・復旧の見積を依頼したところ、通常のシステム保守の数倍のコストがかかることが判明

仕方がないので、システム保守ベンダーに保守契約の一環として復旧指示



感染がどんどん拡大し、結果、新規患者の受入れ停止をせざるを得ないほどの状況になり、謝罪会見へ

推奨 検討すべきポイント



ランサムウェアに感染した場合に備え、専門のセキュリティベンダーへの作業依頼、マスコミ等への広報費用、再発防止に向けた費用等をまかなうサイバー保険に加入すべきか否かを検討すること

## ■対応方針（例）



**ランサム感染に備え、自院に必要なサイバー保険を比較評価し、必要に応じて加入を行うこと**

# 3. ランサムウェア対応検討上のポイント

～3-2：詳細その⑤：システム間のデータフローの把握


経営層
管理責任者
一般利用者

関連する 対策番号	0-2	ネットワーク構成図 の作成（更新）
--------------	-----	----------------------

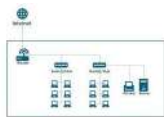
ネットワーク構成図はシステムを取り巻くネットワーク機器・ケーブル等の静態的な接続構成を記述するものだが、ランサムウェアへの備えの観点からは、院内の各システムがどのように相互接続しているのか、どの診療科・病棟のいずれの端末からどのシステムへアクセス可能になっているのか、といった**動的なデータフロー情報**のほうが重要となる。

そのため、ネットワーク構成図は、**院内の各システム・端末間の相互接続・データフローの状況**を含めて整理することが推奨される。

陥りやすい落とし穴



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




立派なネットワーク構成図をベンダ  
に作ってもらったので、大丈夫！

特定システムを取り巻く詳細なネット  
ワーク構成情報は把握できるが、院内全  
体のシステム間のデータの流れまでは含  
まれていなかったため、感染範囲の目途  
を付ける資料として役に立たなかった



推奨 検討すべきポイント



ネットワーク構成図には、院内の各システムがどのように相  
互接続しているのか、どの端末からどのシステムへアクセ  
ス可能になっているかという、データの流れ（フロー）に関  
する情報も含めること

## ■対応方針（例）



特定システムのネットワーク接続構成図のみにと  
どまらず、院内全体のシステム間の相互接続状況  
を可視化する目的でネットワーク構成図をベンダ  
協力のもとで作成すること

# 3. ランサムウェア対応検討上のポイント

～3-2：詳細その⑥：ケーブル外し後の処置

経営層
管理責任者
一般利用者


関連する 対策番号	1-2	ケーブル等の切断
	2-6	被害拡大防止

医療情報システムがランサムウェアに感染した場合、システムをネットワークケーブルから切り離しても未感染の機能の一部は利用可能である。

緊急時の作業等がある場合は思わず利用してしまう職員がいるかもしれないが、その行為はシステム内部のランサムウェアの感染経路や被害範囲の情報を抹消し、その後の対応を妨げるリスクがある。

そのため、ケーブルから外したシステムは一切操作せず、現状保全を確実にすることが重要である。

陥りやすい落とし穴



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




ランサムに感染したけど、ケーブル外したから、エクセルで残りの仕事やっつけてしまおう。

感染端末で色んな操作を行われたので、感染後のウイルスの動きの情報が掻き消されてしまい、被害範囲の調査に大きな影響が発生



推奨

検討すべきポイント



感染が発覚したシステムや端末からネットワークケーブルを外したあとは、可能なかぎり操作はせず、現状の保全を行うようにすること

## ■対応方針（例）



感染した端末のネットワークケーブルを外した後は、調査・復旧まで一切触らないように院内の医療従事者へ周知すること

# 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 対策番号	2-1	原因調査（協力）
	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すしかない！



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すぐに依頼を行えるようにすること。

# 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(2/2)

経営層
管理責任者
一般利用者

関連する 対策番号	2-1	原因調査（協力）
	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

当研究会では証拠保全等のデジタル・フォレンジック調査・解析サービスの専門企業をウェブサイトで紹介しているため、本サイトの情報を確認することが推奨される。また、経済産業省が主管する情報セキュリティサービス基準審査登録制度にてセキュリティサービス専門企業リストも参考となるため、あわせて確認することが望ましい。

## ■ 当研究会の紹介サイト

(URL)

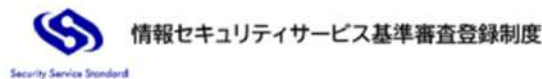
<https://idf-link.digitalforensic.jp/>

回体会員企業名	受付時間	対応地域	詳細
株式会社FRONTEO	平日09:00～18:00	日本（東京・名古屋にオフィスあり）、米国、台湾、中国、韓国	<a href="#">詳細</a>
株式会社ラック	24時間365日	日本 ※その他地域は要相談	<a href="#">詳細</a>
株式会社ディアイティ	平日09:00～18:00	全国	<a href="#">詳細</a>
アイフォレンセ日本データ復旧研究所 株式会社	平日09:00～18:00	日本（大阪にラボあり）日本国外は応相談	<a href="#">詳細</a>
株式会社くまなんピーシーネット	平日10:00～18:00	全国	<a href="#">詳細</a>

## ■ 情報セキュリティサービス基準審査登録制度

(URL)

<https://sss-erc.org/>



登録サービス種別
情報セキュリティ監査サービス
脆弱性診断サービス
デジタルフォレンジックサービス
セキュリティ監視・運用サービス

# 3. ランサムウェア対応検討上のポイント

～3-2：詳細その⑧：影響範囲の調査


経営層
管理責任者
一般利用者

関連する 対策番号	2-10	被害状況調査
--------------	------	--------

電子カルテシステム等が配置される診療系ネットワークは基本的に外部ネットワークと遮断したクローズド環境とされているが、ネットワーク構成図にも記載されずに、**知らぬ間に外部と繋がっていたり、院内のIT担当者でも把握していない抜け道が存在する可能性**がある。

そのため、**診療系ネットワークは安全という考えにとらわれ、調査範囲を不用意に狭めることは危険**である。ネットワーク全体を対象に、ランサムウェアの感染影響範囲を調査することが推奨される。

### 陥りやすい落とし穴



診療系ネットワークは外部と繋いでいないので、調査範囲は非診療系のみにしたら、後日、診療系にまで被害が及んでいたことが発覚

情報系から診療系は大丈夫だろう・・・




業者が持ち込んだUSBメモリにランサムウェアが混入しており、情報系のシステムでランサム感染が発生。  
診療系は独立したネットワークなので問題ないとして、調査範囲は情報系NWのみとした。

あれ！ここも??



実は業者のNW環境全体にランサム感染が発生していたことが後日発覚。同じ業者に診療系NWのシステムのリモート保守も委託していたため、業者のリモート保守用環境から診療系NWへ感染が拡大

### 推奨 検討すべきポイント



ランサムウェアは通常のセキュリティの考えでは安全とされていた防御壁もすり抜けてくるという考えに立って、影響範囲を広く深く調査すること

### ■対応方針（例）



**ランサムウェアは従来のセキュリティ上の防御をすり抜けてどんどん感染を拡大するコンピュータウイルスであるという認識を持つこと**



# 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

管理責任者

一般利用者

関連する  
対策番号

2-12

方針指示

3-1

復旧指示

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に、思ったより復旧に繋がらなかった



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**

# 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(2/2)

経営層
管理責任者
一般利用者

関連する 対策番号	2-12	方針指示
	3-1	復旧指示

ランサムウェアの種類によっては、暗号化されたデータを身代金を払わずとも、復号できる可能性がある。これらの復号ツールは**No More Ransomプロジェクト**という、欧州警察（ユーロポール）やセキュリティベンダが連携した取組のもとで、**無償提供**されている。（言語選択で日本語でサイト表示をすることも可能）

また、国内外のセキュリティベンダーでもランサムウェアの種類に応じた復号ツールを**無償公開しているケース**もある。

そのため、身代金の支払い検討をする前に、こうした**無償ツールを用いた復号化が出来ないか**についてまずは検証することが推奨される。

## ■ No More Ransomプロジェクト

(URL)

<https://www.nomoreransom.org/ja/index.html>



# 3. ランサムウェア対応検討上のポイント

～3-2：詳細その⑩：システムへのリストア作業


経営層
管理責任者
一般利用者

関連する 対策番号	3-3	再設定やバックアップ データのリストア等
--------------	-----	-------------------------


「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」はサイバー攻撃全般の対応手順に主眼を置いている。そのため、仮にランサムウェアからの復旧という具体的なケースにおいて、「3-3：再設定や再インストール、バックアップデータのリストア等」の手順に従い、**感染端末からバックアップを取得し、リストアを行った場合、再度ランサムウェアの感染が発生するリスク**がある。

ランサムウェアからの復旧時にシステムへのリストアを行う場合は、フォレンジック等による原因調査により把握した**感染日より前のバックアップ**を用いてリストア作業を行うことが推奨される。

陥りやすい落とし穴



**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**



ようやくランサムの駆除もできた！  
システムを復旧させよう！


厚労省が公表した資料に従って、バックアップを取って、リストア！



バックアップに混入していたランサムに再度感染することに。

推奨

検討すべきポイント



ランサムウェア感染からシステムを復旧する場合、バックアップとして取得しているデータ等が、**感染前のものであることを確認した上で、リストア作業**をすること

## ■対応方針（例）



バックアップデータが感染日より前の時点で取得されたことのチェック

**感染日より前に取得したバックアップを用いてリカバリを実施すること**

# 3. ランサムウェア対応検討上のポイント

～3-2：詳細その⑪：二重脅迫型被害時の情報公開

経営層

管理責任者

一般利用者

関連する  
対策番号

4-7

情報公開の検討

二重脅迫型のランサムウェアでは窃取した情報の公開（暴露）の停止と引き換えに身代金の要求が行われる。  
【その⑨：身代金支払い対応】でも説明した通り、**仮に身代金を払っても、こちらの要求が通る保証は一切ない。**  
**窃取された患者情報は公開（暴露）され、既に漏えいしてしまっているという認識**のもとで、情報が窃取された患者への情報開示・説明を幅広く行い、復旧に向けて、**患者も含めた関係組織の助力や理解を得る必要がある。**

## 陥りやすい落とし穴



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



とりあえず身代金は払ったから、患者情報は公開されないだろう。  
患者に不要な心配はかけられないから、情報開示は止めよう

約束を違え患者情報が公開され、ダークネットに流通。マスコミに気づかれ、謝罪会見を行う羽目に。



## 推奨

## 検討すべきポイント



身代金の支払いが患者情報の公開を防ぐ保証は一切ないため、被害が発生した場合は包み隠さず、患者も含めた関係者・関係組織に適時に状況開示をして、援助・理解をこそ得るようにすること

## ■対応方針（例）



二重脅迫ランサム感染



ランサム感染復旧へのご理解・ご協力をお願いします。



二重脅迫型のランサムウェア被害を受けた時点で、サイバー攻撃集団に情報は漏えいしており、アンコントロールになるため、被害を受けた患者には包み隠さず状況を説明し、理解を得ること。

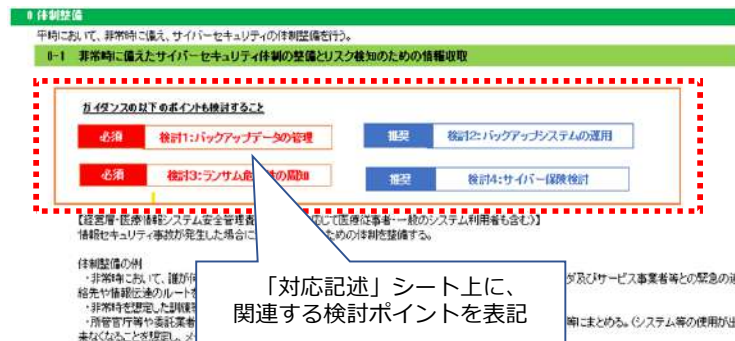
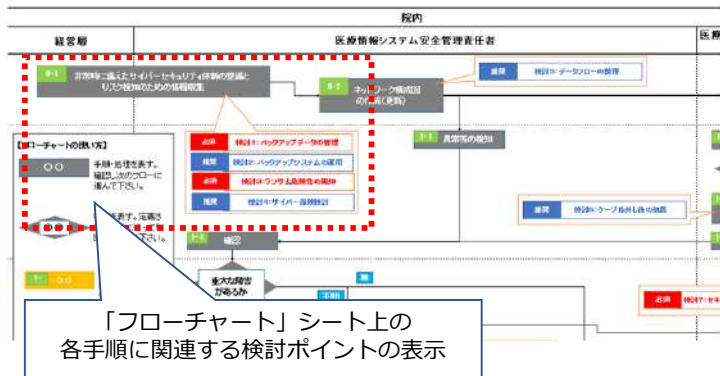
### 3. ランサムウェア対応検討上のポイント

#### ～3-3：ランサムウェア対応検討フローチャート

上述の各検討ポイントを、厚生労働省「医療情報システムの安全管理に関するガイダンス」別添資料「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」内の『フローチャート』シート・『対応記述』シートに埋め込み、ランサムウェア対応を検討するポイントを可視的に把握できる、**別紙「ランサムウェア対応上の検討ポイントを含めたフローチャート」**も整理した。

当該別紙を本ガイダンスの内容とともに利活用し、ランサムウェアへの対応を検討することが推奨される。

#### ■（別紙）ランサムウェア対応検討フローチャート



---

Appendix.

# Appendix : 用語集

本ガイドランスの用語の定義・補足は以下の通り。

対象頁	用語	定義・補足
p4	法定保存文書	医療に関する法令や関連規則により保存期間が定められている文書。 例えば、患者の診療録は医師法24条で5年間の保存が義務付けられている。また、保険医療機関及び保険医療養担当規則第9条では療養の給付の担当に関する帳簿及び書類その他の記録（例：手術記録、薬剤管理指導記録、退院時サマリー、診断書等）は3年間の保存が義務付けられる。
P6、p22	デジタルフォレンジック	インシデントレスポンス*や法的紛争・訴訟に際し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術。なお、インシデントレスポンスとは、コンピュータやネットワーク等の資源及び環境の不正使用、サービス妨害行為、データの破壊、意図しない情報の開示等、並びにそれらへ至るための行為（事象）等への対応等を指す
p11	ダークウェブ	インターネット空間に存在するが、通常のインターネット利用とは異なる特殊な設定・ツール等によりアクセスが可能となる領域
p15	DAT、LTO	Digital Audio Tape、Linear Tape-Openの略称。 カートリッジ交換式の磁気テープにデータ等をバックアップするための装置。
	RDX	Removable Disk Exchange systemの略称。リムーバブルディスクを使って、ドラッグ&ドロップ方式でバックアップ・復旧が可能な装置
	NAS	Network Attached Storageの略称。ネットワークに直接接続して使用するファイルサーバ。
p16	ホット/ウォーム/コールドスタンバイ	予備のバックアップシステムをどのような状態で準備するかを指す。本番系システムに問題が発生した場合、常に起動している待機系へ瞬時に切り替えることを可能にするホットスタンバイ方式、待機系の一部の機能を停止させているため多少切り替えに時間を要するウォームスタンバイ方式、待機系は原則停止させ、本番系に問題があり次第起動を行うコールドスタンバイ方式がある。
p18	サイバー保険	サイバー攻撃の被害を受けた際に必要となる原因調査・復旧対応費用、第三者への損害賠償費用・訴訟費用等を補填する保険サービス。費用補填の範囲は損保会社のメニュー・プログラムにより異なる。
p23	診療系ネットワーク	電子カルテ等、患者診療に不可欠なコアシステム群が接続している院内ネットワーク。診療に直接的な影響を及ぼさない業務システム、情報管理目的のシステムが接続する院内ネットワークと切り離され管理されることが多い。
p25	善管注意義務	院長や事務長等、該当者の能力・社会的地位などから考えて一般的に期待される注意義務を指す。この義務を怠り、何らかの問題が発生した場合、民法上過失があると判断され、損害賠償等の対象となる可能性がある。

# Appendix : 本ガイダンス制定WG参加者リスト

本ガイダンスは「医療」分科会WGに参画した以下のメンバーにより、医療ISACの支援のもとで検討・制定された。

氏名	所属
江原 悠介	医療分科会主査 PwCあらた有限責任監査法人 システム・プロセス・アシュアランス シニアマネージャー
緒方 健	医療分科会幹事 千葉大学医学部附属病院次世代医療構想センター 特任研究員
吉峯 耕平	医療分科会幹事 田辺総合法律事務所 パートナー弁護士
舟橋 信	(株)セキュリティ工学研究所 取締役、(株)FRONTEO 取締役
和田 則仁	湘南慶育病院 外科 部長
近藤 剛	有徳総合法律事務所 弁護士
松浦 洋一	(株)テリロジーワークス 取締役
深山 治	リーガレックス(同) 代表社員
下垣内 太	アイフォレンセ日本データ復旧研究所(株) 代表取締役
土方 恭子	宇田川・新城法律事務所 弁護士
佐藤 健太郎	早稲田大学大学院 経営管理研究科
山本 竹志	リソース・グローバル・プロフェッショナル・ジャパン(株)
松本 一弘	アクレスコ(株)
鈴木 文一郎	(株)ワイ・イー・シー 取締役
野村 政也	(株)ワイ・イー・シー 販売推進本部 販売推進部
梅澤 一巳	(株)ワイ・イー・シー 販売推進本部 販売推進グループ マネージャー
岡田 忠	鹿島情報技術研究所 主席研究員



