デジタル・フォレンジック研究会「医療」分科会
「医療機関向けランサムウェア対応検討ガイダンス」の解説

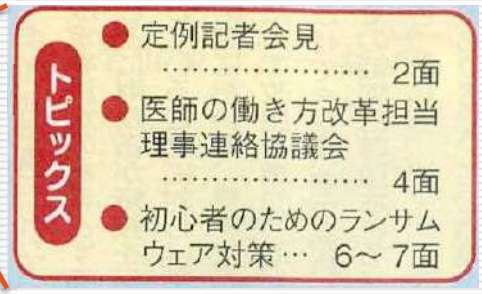
医療機関向けランサムウェア対応検討ガイダンス

ランサムウェアへの セキュリティ対応の臨床的側面

和田　則仁
デジタル・フォレンジック研究会 理事
湘南慶育病院外科 部長

2021年12月16日（木）19:50～20:15、Web開催

日本医師会による情報提供



出典：日医ニュース 第1447号 令和3年12月20日（日本医師会）

医療機関に求められる対策・対応の水準

各医療機関に最低限実施してもらいたい６カ条

1、安全性が担保できない私物パソコンやUSBメモリ等の外部記憶装置を接続しない。
2、職員に対する注意喚起とセキュリティ教育を継続的に行う。
3、院内で利用しているセキュリティ装置を提供元が推奨する最新の状態に必ず保つ。
4、セキュリティ装置に不必要な通信が通過する設定が施されていないか改めて確認をする。
5、業務・医療システムとそこへ接続するパソコン等はネットワーク（セグメント）を必ず分ける。
6、業務・医療システムが長期間にわたって脆弱な状態にならないようにする。

※上記の3～6はご利用の情報システムの保守事業者に確認・相談願います。

サイバー攻撃を受けた場合の対応方法

サイバー攻撃を受けた疑いがある場合、あるいは受けてしまった場合には、以下のようなご対応をお願いいたします。

○サイバー攻撃（コンピューターウイルスの感染等）を受けた疑いがある場合
被害の拡大を防ぐため、直ちにご利用の情報システムの保守事業者等に連絡して、指示を仰いで下さい。

○診療系情報システムの停止や個人情報の流出等の被害等が発生した場合
下記にご連絡願います。
▶厚生労働省医政局研究開発振興課医療情報技術推進室
☎03-3595-2430　✉igishitsu@mhlw.go.jp

なお、一般的な情報セキュリティ（主にウイルスや不正アクセス）に関する技術的な相談をしたい場合には、下記の相談窓口もご活用願います。
▶情報処理推進機構（IPA）情報セキュリティ安心相談窓口
https://www.ipa.go.jp/security/anshin/index.html
☎03-5978-7509（平日日中のみ）　✉anshin@ipa.go.jp

出典：鳴原祐輔「初心者のためのランサムウェア対策」日医ニュース 第1447号 令和3年12月20日（日本医師会）

カリフォルニア州の病院、ハッカーにビットコインで17,000ドルの身代金を支払う （2016年2月17日）

- ハリウッドPresbyterian医療センター
- ランサムウエア
- 「システム正常化の利益最大化のためにやむを得なかった」
- ハッキングによる健康被害の報告はない
- 患者データ流出は確認されていない

SECTIONS SEARCH **Chicago Tribune** SUBSCRIBE 4 weeks for 99¢

SUNDAY NOV. 16, 2017 SPORTS BREAKING MOST POPULAR OPINION SUBURBS ENTERTAINMENT BUSINESS ADVERTISING

News / Nation & W

California hospital paid $17,000 ransom in bitcoins to hackers

The Hollywood Presbyterian Medical Center in 2004. The hospital was recently the target of a ransomware extortion plot in which hackers seized control its computer systems and then demanded that directors pay in bitcoin to regain access. (Ricardo DeAratanha / Los Angeles Times)

By **Tribune news services - Contact Reporter**

FEBRUARY 17, 2016, 10:51 PM

A Los Angeles hospital paid a ransom of about $17,000 to hackers who infiltrated and disabled its computer network because paying was in the best interest of the hospital and the most efficient way to solve the problem, the medical center's chief executive said Wednesday.

"It is the beginning of a pandemic hitting health systems in the next few years."
Larry Whiteside, Jr. (CEO, Whiteside Security LLC)

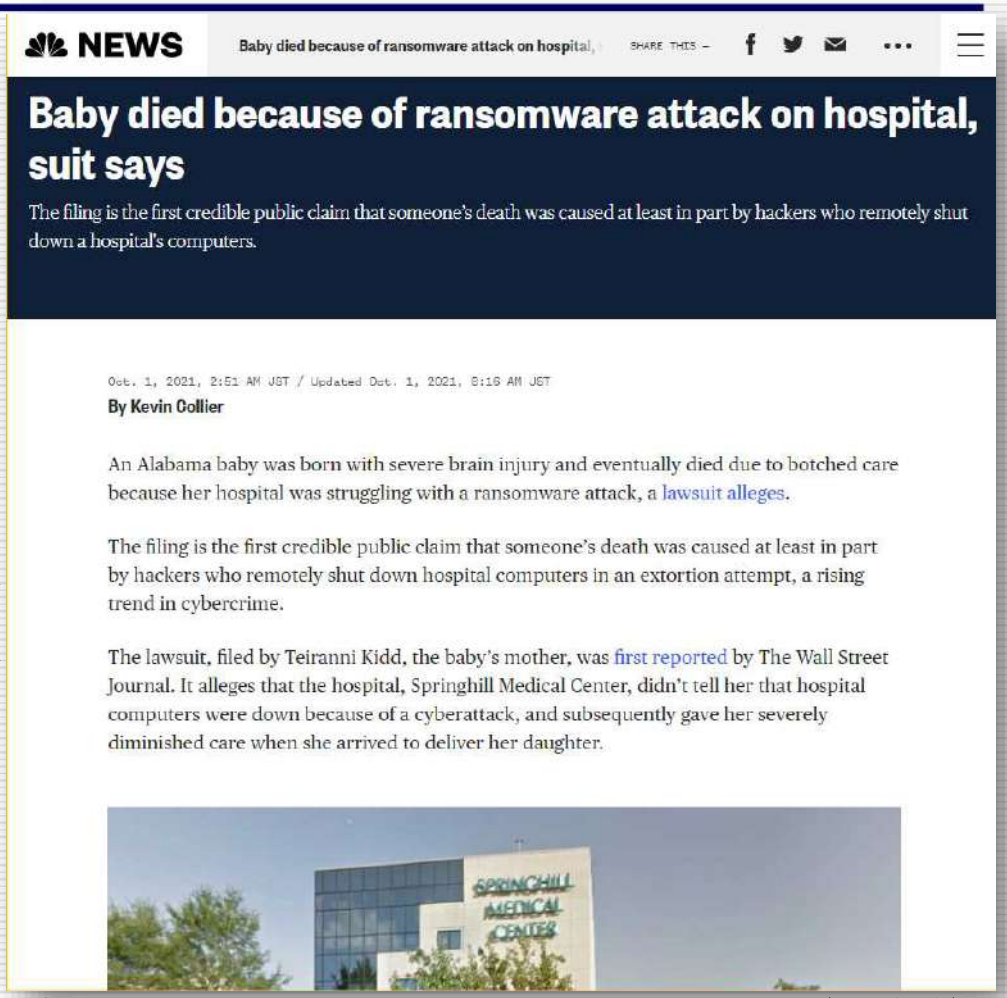
http://www.chicagotribune.com/news/nationworld/ct-california-hospital-ransom-hackers-20160217-story.html

Keio University 1858 CALAMVS GLADIO FORTIOR

ランサムウエアによるシステム障害で患者が死亡し訴訟

- ランサムウエアによるシステム障害で患者が死亡し訴訟となった初のケース。
- アラバマ州のSpringhill医療センターが、ランサムウェアによりシステムが停止していることを伝えず、妊婦に不適切なケアを行った。
- 医師や看護師は、胎児の首に臍帯が巻き付いていたことを示す複数の検査を見逃し、出産時に脳障害を起こし、９ヵ月後に死亡した。

注意義務違反、説明義務違反



NEWS Baby died because of ransomware attack on hospital, SHARE THIS –

Baby died because of ransomware attack on hospital, suit says

The filing is the first credible public claim that someone's death was caused at least in part by hackers who remotely shut down a hospital's computers.

Oct. 1, 2021, 2:51 AM JST / Updated Oct. 1, 2021, 8:16 AM JST

By Kevin Collier

An Alabama baby was born with severe brain injury and eventually died due to botched care because her hospital was struggling with a ransomware attack, a lawsuit alleges.

The filing is the first credible public claim that someone's death was caused at least in part by hackers who remotely shut down hospital computers in an extortion attempt, a rising trend in cybercrime.

The lawsuit, filed by Teiranni Kidd, the baby's mother, was first reported by The Wall Street Journal. It alleges that the hospital, Springhill Medical Center, didn't tell her that hospital computers were down because of a cyberattack, and subsequently gave her severely diminished care when she arrived to deliver her daughter.

https://www.nbcnews.com/news/baby-died-due-ransomware-attack-hospital-suit-claims-rcna2465 (2021/10/1)

WannaCry ransomware attack

- 2017年5月12日(金)から大規模なサイバー攻撃が開始
- 150か国の23万台以上のコンピュータに感染
- 日本：日立製作所、ＪＲ東日本、イオン、本田技研など
- 英国National Health Service (NHS) のシステムが感染
- 一部の病院で診察や手術の予約のキャンセル、救急車の受け入れ不能、画像診断・病理診断の停止
- 解除キー300ドル（3日後に2倍）払った形跡あり

NHSのシステム感染の事後検証

Source: S Ghafur, et al. NPJ Digit Med 2019;2:98.

Published online: 02 October 2019

NHSの電カルデータ
- WannaCry攻撃の-2週（4/28～5/4）
- WannaCry攻撃の-1週（5/5～5/11）
- WannaCry攻撃の週（5/12～5/18）
- WannaCry攻撃の+1週（5/19～5/25）
- WannaCry攻撃の+2週（5/26～6/1）

調査項目
- 総入院数
- 緊急入院
- 予定入院
- 日帰り入院
- 日帰り以外の予定入院
- 救急外来受診数
- 救急外来死亡数
- 外来予約数
- 外来受診者数
- 外来キャンセル数

WannaCry感染前後の全病院の活動状況

Mortality

Across all trusts, compared to the baseline week, there was no significant difference in the number of deaths in A&E. There was also no significant difference in deaths in A&E between infected and non-infected trust (0 deaths (−0.1 to 0.1).

Table 1. National activity counts in the weeks before, during, and after WannaCry

		Week					Total
		−2	−1	WannaCry week	+1	+2	April–June
Total admissions	総入院数	273,727	303,386	297,840	302,986	265,193	3,755,086
Emergency admissio	緊急入院	142,485	145,178	144,492	146,547	140,759	1,854,462
Elective admissions	予定入院	131,242	158,208	153,348	156,439	124,434	1,900,624
Day case admissions	日帰り入院	108,395	130,281	126,141	128,613	102,994	1,565,867
Elective admissions e	1泊以上予定入院	22,847	27,927	27,207	27,826	21,440	334,757
A&E attendances	救急外来受診数	373,542	374,710	365,833	371,676	375,949	4,806,543
Deaths in A&E	救急外来死亡数	340	360	310	303	339	4218
Outpatient appointm	外来予約数	1,878,032	2,323,146	2,272,223	2,272,220	1,704,802	27,449,176
Outpatient attendan	外来受診者数	1,485,163	1,836,566	1,779,498	1,786,203	1,336,314	21,539,339
Outpatient cancellati	外来キャンセル数	132,541	164,408	175,552	163,215	126,517	2,050,352

A&E accident and emergency

Source: S Ghafur, et al. NPJ Digit Med 2019;2:98.

ベースラインと比較した病院の活動示標

Table 2. Activity before, during, and after WannaCry across all trusts

	総入院数	緊急入院	予定入院	日帰り入院	1泊以上予定入院	救急外来受診数	救急外来死亡数	外来予約数	外来受診者	外来キャンセル数
Panel A: Point estimates and confidence intervals of difference in average daily activity per hospital in the weeks before, during, and after WannaCry across all trusts compared to baseline period										
−2	5.5	3	3.5	4.3	0.6	8.4	0	46	44.6	−3.6
	[1.9, 9.0]	[2.1, 3.8]	[0.4, 6.6]	[1.6, 7.0]	[−0.2, 1.3]	[6.3, 10.4]	[−0.0, 0.1]	[2.7, 89.3]	[11.5, 77.7]	[−10.6, 3.4]
−1	4.8	1.6	4.1	3.6	0.8	5.1	0	70.9	68.9	−3.5
	[1.4, 8.3]	[0.7, 2.4]	[1.1, 7.1]	[1.1, 6.2]	[0.1, 1.5]	[3.1, 7.2]	[0.0, 0.1]	[28.3, 113.4]	[36.4, 101.3]	[−10.3, 3.4]
WannaCry week	0.2	1.1	−0.3	−0.5	0.2	−3.2	0	26.3	21.1	4.4
	[−3.3, 3.7]	[0.2, 1.9]	[−3.3, 2.8]	[−3.0, 2.1]	[−0.5, 0.9]	[−5.3, −1.2]	[−0.0, 0.0]	[−16.3, 68.9]	[−11.4, 53.6]	[−2.5, 11.2]
+1	4.4	2.6	2.5	2.1	0.7	2.3	0	34.3	32.3	−4.2
	[1.0, 7.9]	[1.8, 3.5]	[−0.5, 5.5]	[−0.5, 4.6]	[0.0, 1.4]	[0.2, 4.3]	[−0.1, 0.0]	[−8.2, 76.9]	[−0.2, 64.8]	[−11.1, 2.7]
+2	−0.4	1.7	−2.3	−1.6	−0.8	10.6	0	−93.3	−74.8	−8.6
	[−3.9, 3.1]	[0.8, 2.5]	[−5.4, 0.8]	[−4.2, 1.1]	[−1.5, −0.1]	[8.6, 12.7]	[−0.0, 0.1]	[−136.8, −49.9]	[−108.0, −41.6]	[−15.6, −1.6]
N	17,882	17,299	15,790	13,096	15,070	13,832	13,832	17,114	17,114	17,114
Mean per trust per day	210	107.2	120.4	119.6	22.2	347.5	0.3	1603.9	1258.6	119.8
Panel B: Expected national activity during with and without WannaCry										
Predicted activity 予測値	296,718.9	143,798	151,903.5	126,568	26,964.8	365,833	310	2,285,402.3	1,790,122.8	176,435.8
Pred WannaCryがない WannaCr 場合の予測値 similar to	296,449.1	142,379.4	152,208	127,038.4	26,765.1	369,256.9	320.6	2,250,567.3	1,762,225.9	170,669.2
Estimated difference 差	269.8	1418.6	−304.5	−470.4	199.6	−3423.9	−10.6	34,834.9	27,896.8	5766.6
	[−4489, 5028.7]	[317.3, 2519.9]	[−3996.6, 3387.6]	[−3097, 2156.2]	[−611.8, 1011.1]	[−5592.3, −1255.5]	[−48, 26.8]	[−21525.2, 91195.1]	[−15100.2, 70893.9]	[−3316.6, 14849.9]

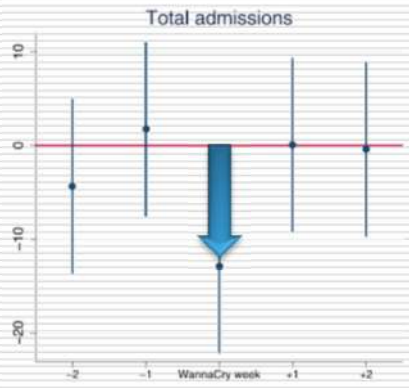
Panel A: The dependent variable is activity per trust per day. Point estimates reflect the average difference in daily activity across all hospitals in weeks before, during, and after WannaCry compared to the baseline, which is any other day between 1 April and 30 June 2017. Regression controls for day of week, bank holiday, and hospital fixed effects. 95% confidence intervals in squared brackets. Panel B: Expected activity is the predicted activity from the regression

A&E accident and emergency

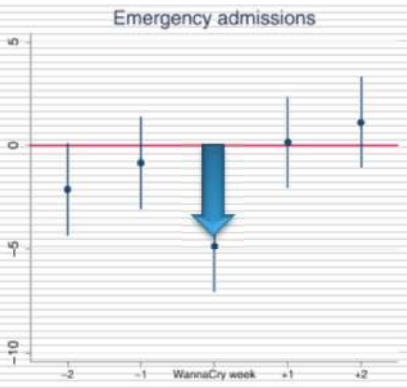
Source: S Ghafur, et al. NPJ Digit Med 2019;2:98.

感染した病院と、感染していない病院の比較

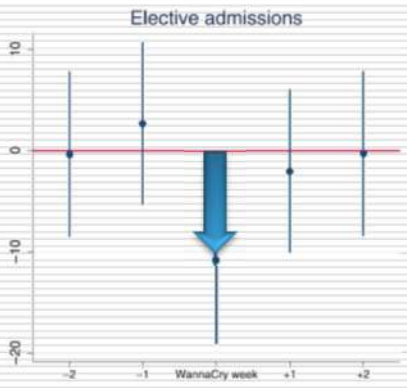
総入院数



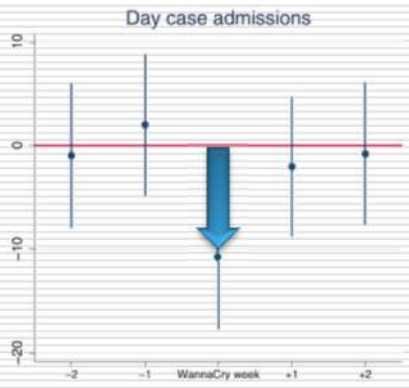
緊急入院



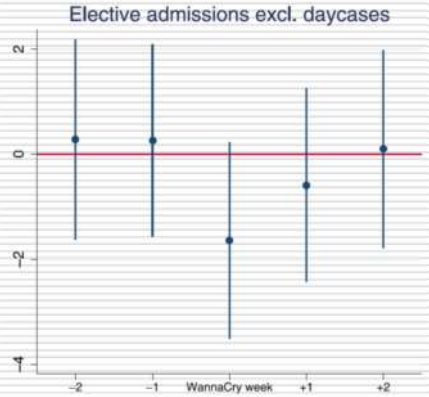
予定入院



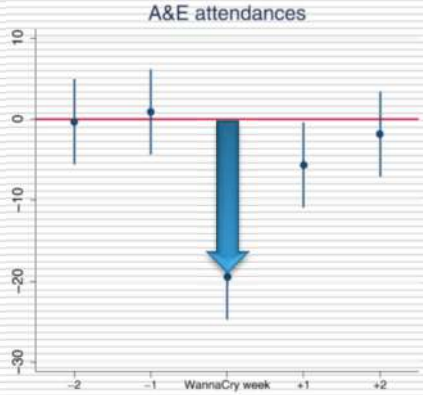
日帰り入院



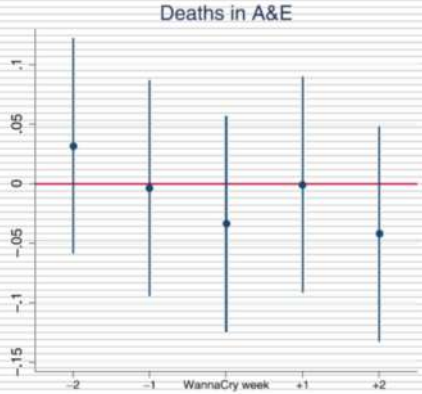
１泊以上予定入院



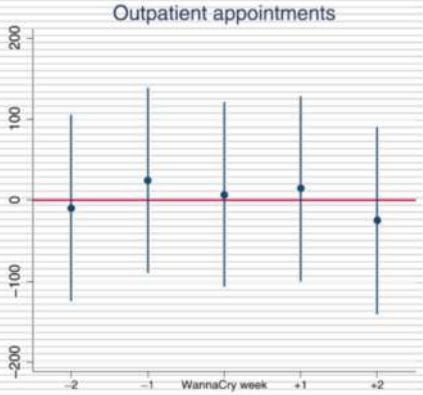
救急外来受診数



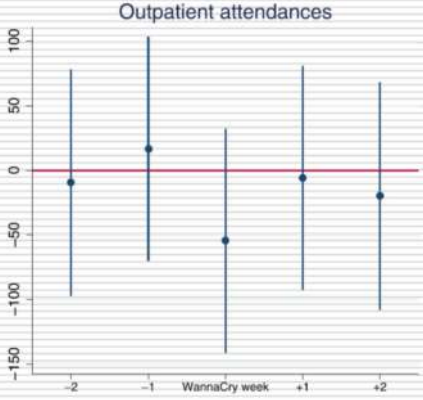
救急外来死亡数



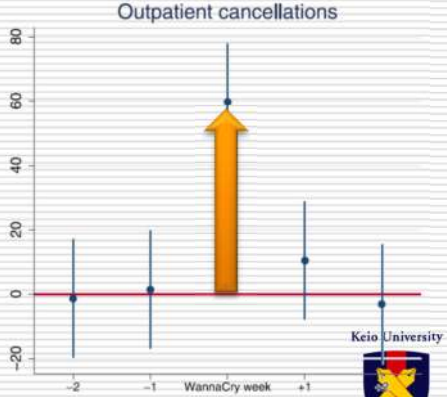
外来予約数



外来受診者数



外来キャンセル数



Source: S Ghafur, et al. NPJ Digit Med 2019;2:98.

感染した病院の活動低下による経済的損失の合計

Source: S Ghafur, et al. NPJ Digit Med 2019;2:98.

Table 3. Estimated impact of WannaCry on total activity during the WannaCry week

	At actually infected trust 感染病院の実績		If all trusts were i全ての病院が感染した場合	
	Activity difference	Costed difference	Activity difference	Costed difference
Total admissions 総入院数	−2935.6	−£4.0 m 6億円	−17,562.1	−£24 m
	[−5067.2, −803.9]	[−£6.6 m, −£1.5 m]	[−30,314.8, −4809.3]	[−£39.3 m, −£8.8 m
Emergency admi 緊急入院	−1066	−£2.1 m	−6386.6	−£12.6 m
	[−1558.5, −573.5]	[−£3.1 m, −£1.1 m]	[−9337.1, −3436.1]	[−£18.4 m, −£6.8 m]
Elective admissio 予定入院	−2175.6	−£1.9 m	−13,162.2	−£11.5 m
	[−3815.9, −535.3]	[−£3.5 m, −£0.3 m]	[−23,086.1, −3238.3]	[−£20.9 m, −£2.0 m]
Day case admissions 日帰り入院	−1857.7	−£1.2 m	−11,016.4	−£7.2 m
	[−3038.6, −676.7]	[−£2.0 m, −£0.4 m]	[−18,019.6, −4013.1]	[−£11.8 m, −£2.6 m]
Elective admissions excl. day cases 1泊以上予定入院	−315.8	−£0.7 m	−1907.7	−£4.2 m
	[−676.6, 45.1]	[−£1.5 m, £0.1 m]	[−4087.9, 272.4]	[−£9.1 m, £0.6 m]
A&E attendances 救急外来受診数	−3760.2	−£0.6 m 1億円	−20,648.6	−£3.3 m
	[−4781.7, −2738.7]	[−£0.8 m, −£0.4 m]	[−26,224.6, −15,072.6]	[−£4.1 m, −£2.4 m]
Outpatient appointments 外来予約数	3328.8	£0.2 m	9303.7	£0.9. m
	[−21,730.7, 28,388.3]	[−£2.3 m, £2.6 m]	[−140,860.5, 159,467.9]	[−£13.7 m, £15.5 m]
Outpatient atten 外来受診者数	−12,166.8	−£1.2 m	−71,860.0	−£7.0 m
	[−31,562.4, 7228.8]	[−£3.1 m, £0.7 m]	[−186,415.1, 42,695.2]	[−£18.2 m, £4.2 m
Outpatient cance 外来キャンセル数	13,534.4	£1.3 m 2億円	78,962	£7.7 m
	[9453.3, 17,615.4]	[£0.9 m, £1.7 m]	[54,791.4, 103,132.6]	[£5.3 m, £10.1 m]
Total financial im 経済的損失の合計		−£5.9 m 9億円		−£35.0 m 50億円
		[−£8.2 m, −£3.6 m]		[−£48.8 m, −£21.2 m]

医療機関向けランサムウェア対応検討ガイダンス

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。

医療情報システムへの依存度が高い

- 過去の情報の参照
- 診療支援
- 効率・迅速性
- 情報共有

- 最適ではない医療行為による合併症の増加
- 遅延による悪い結果
- 待ち時間の増加
- 因果関係は？

医療機関向けランサムウェア対応検討ガイダンス

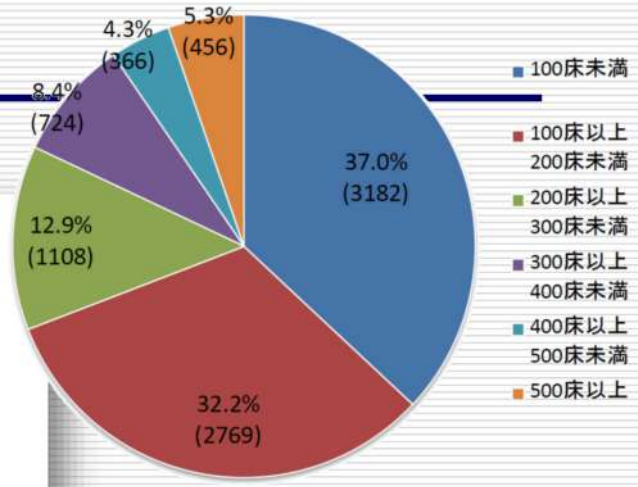
1．本ガイダンス制定の背景(2/3)

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。

5

病床規模別病院数（全国8,605病院）



医療施設調査(2011年)

病院の規模	大	⟷	小
依存度	大	⟷	小
影　響	大	⟷	小
リソース	大	⟷	小

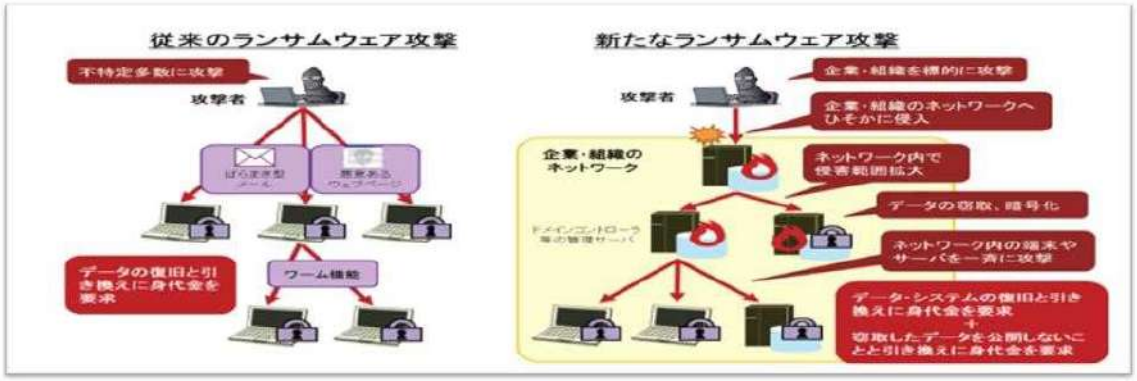
Keio University

医療機関向けランサムウェア対応検討ガイダンス

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。



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」より

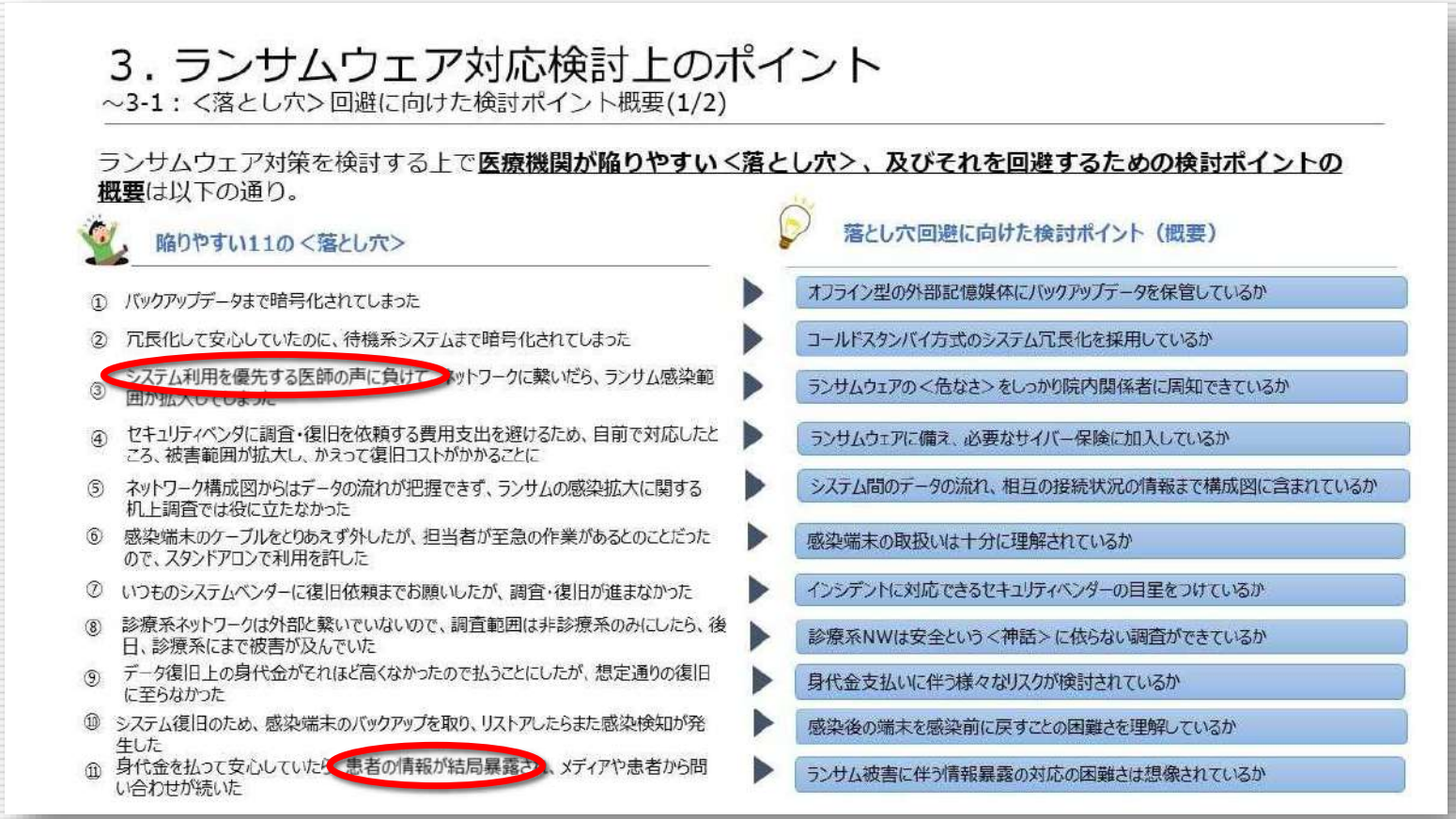
医療情報システムが
利用できない

システムダウンで
想定(経験)済み
当面の診療は可能

医療情報の公開

回復不能の被害
賠償

医療機関向けランサムウェア対応検討ガイダンス



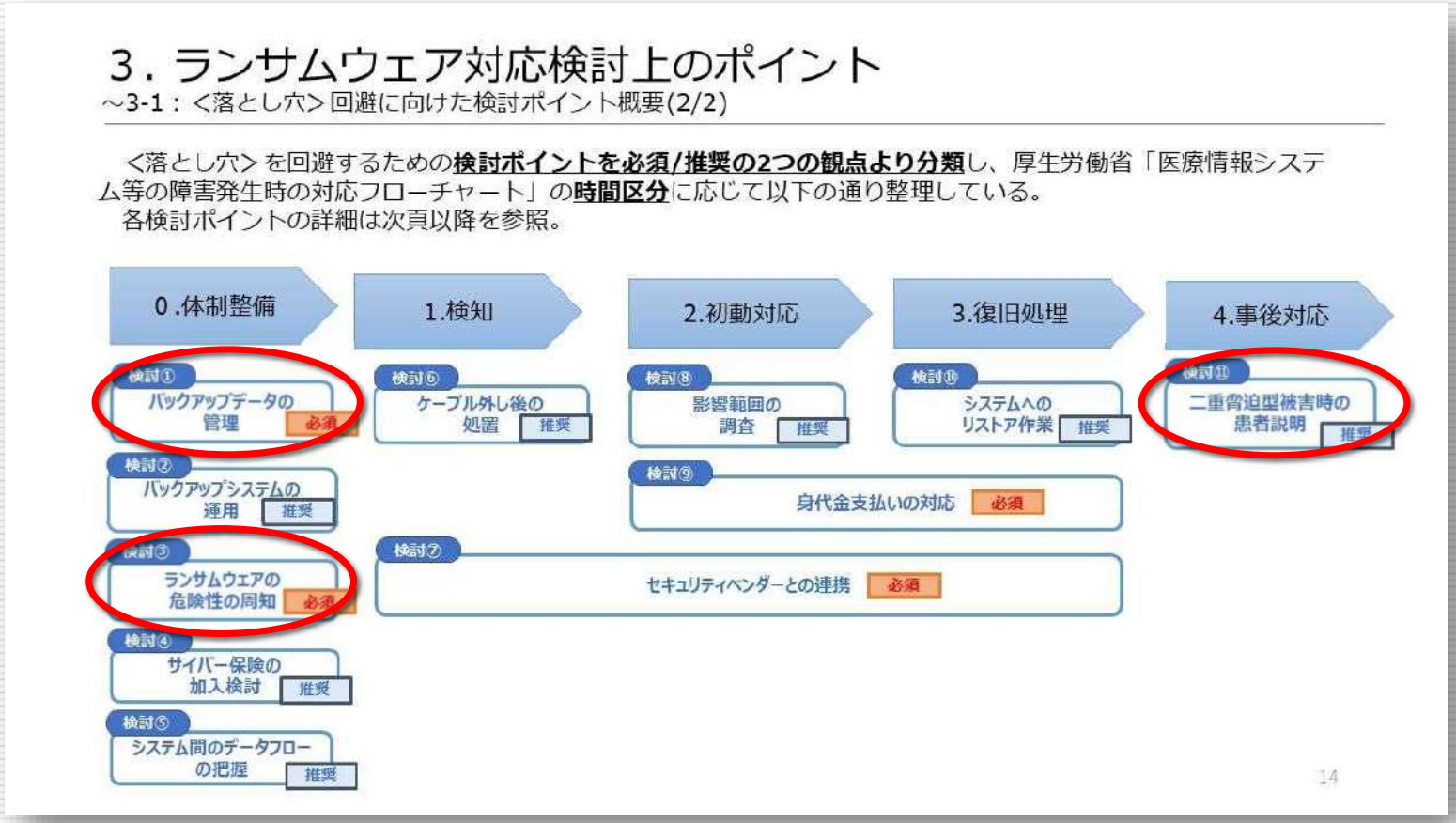
3．ランサムウェア対応検討上のポイント

～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>	落とし穴回避に向けた検討ポイント（概要）
① バックアップデータまで暗号化されてしまった	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
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	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
③ システム利用を優先する医師の声に負けて[illegible]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	ランサムウェアの<危なさ>をしっかり院内関係者に周知できているか
④ 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	ランサムウェアに備え、必要なサイバー保険に加入しているか
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	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
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	感染端末の取扱いは十分に理解されているか
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	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
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	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
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	身代金支払いに伴う様々なリスクが検討されているか
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	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
⑪ 身代金を払って安心していたら[illegible]患者の情報が結局暴露さ[illegible]、メディアや患者から問い合わせが続いた	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

医療機関向けランサムウェア対応検討ガイダンス



医療機関向けランサムウェア対応検討ガイダンス

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

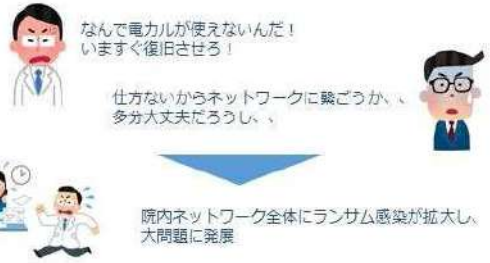
経営層
管理責任者
一般利用者

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



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・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。

18

医療機関向けランサムウェア対応検討ガイダンス

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となる調査・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）

保険カバー範囲


調査・復旧費用


広報費用


再発防止に向けた必要費用

・・・

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

19

医療機関向けランサムウェア対応検討ガイダンス

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 ケーブル等の切離
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）

端末した感染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

21

医療機関向けランサムウェア対応検討ガイダンス

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巨星調査

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。

22

Keio University
1858
CALAMVS GLADIO FORTIOR

医療機関向けランサムウェア対応検討ガイダンス

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

診療系は外部に一切繋がってません。だから情報系のシステムの感染なら、診療系は調べる必要はないです！

診療系/非診療系を切り離すネットワーク機器に脆弱性が存在。その脆弱性を悪用するランサムウェアれ、診療系NWへの感染が発生することに。

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

24

医療機関向けランサムウェア対応検討ガイダンス

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で払うことにしたが、想定通りの復旧に至らなかった

必須

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）

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

医療機関向けランサムウェア対応検討ガイダンス

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・説明を幅広に行い、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、情報開示は止めておこう

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、アンコントローラブルになるため、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。

28