「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

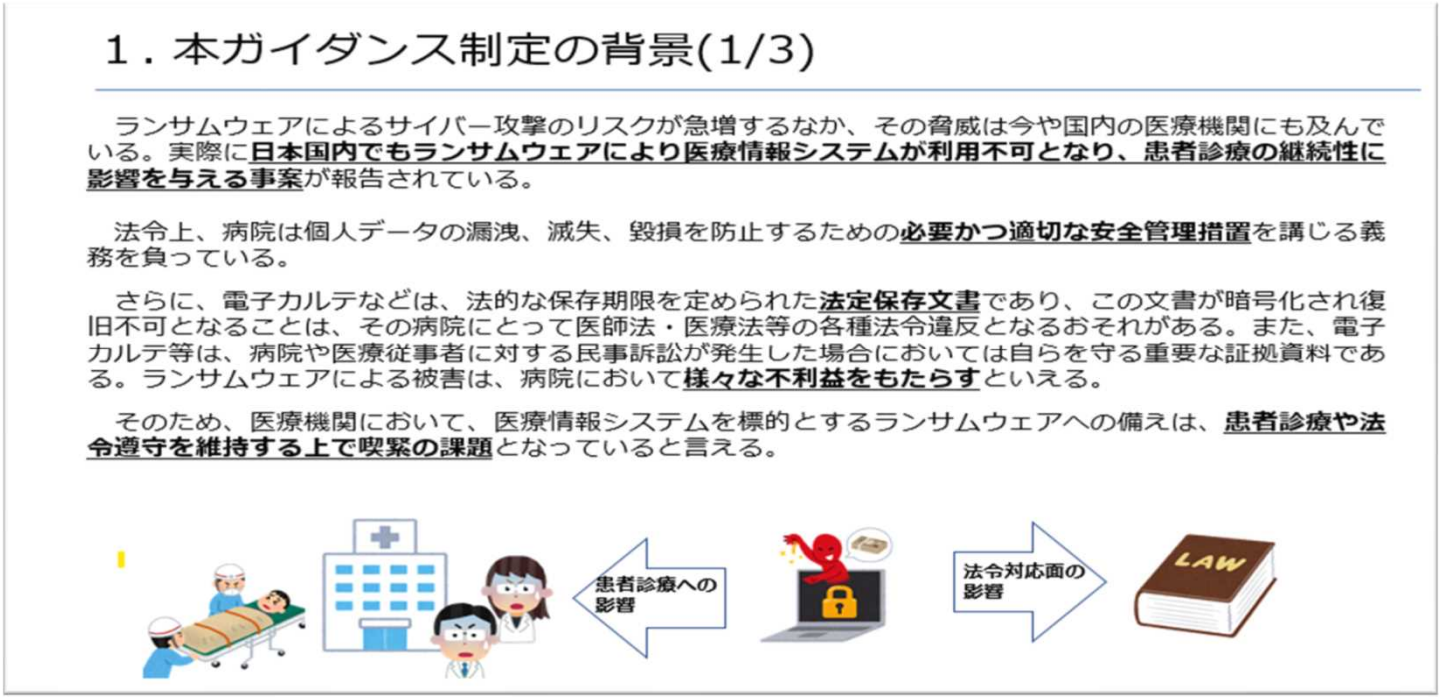
（NPO） デジタル・フォレンジック研究会 理事/「医療」分科会主査
（一社）医療ISAC 理事

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。

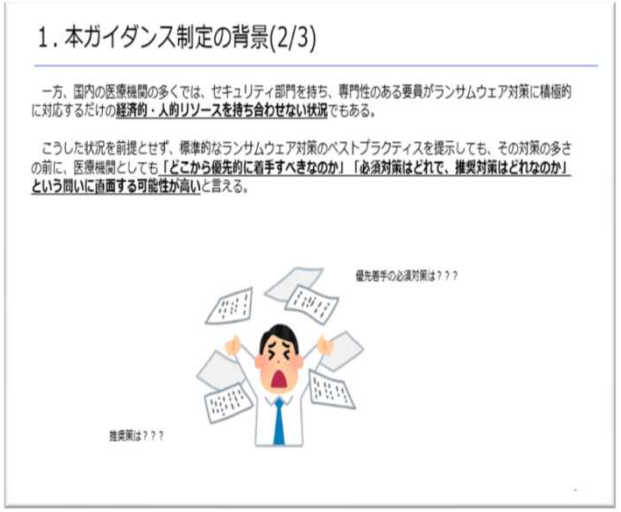
■「医療機関向けランサムウェア対応検討ガイダンス」より



1. ガイダンス制定の背景(2/3)

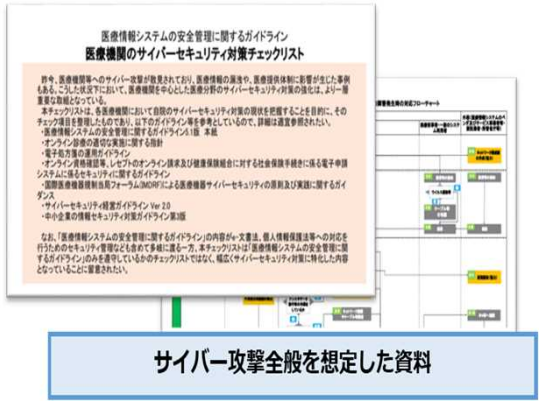
医療機関におけるセキュリティは3省2ガイドラインを前提としているが、これらはあくまで**紙媒体で管理していた患者情報を電子的に管理する上で求められる諸要件**をまとめたものであり、**悪意ある外部の攻撃者によるサイバー脅威を想定した対策要件の整理**までには至っていない。
21年10月に厚生労働省から厚労省安全管理ガイドラインの別添資料として医療機関のサイバーセキュリティ対策チェックリスト」・「医療情報システム等の障害発生時の対応フローチャート」が公開され、さらに10月下旬の徳島の総合病院の事案を受け、厚労省から11月下旬に再注意喚起の事務連絡が行われている。
ただし、重要な点は、本連絡でフォーカスされるサイバー対策の前提となる別添資料群はあくまで**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



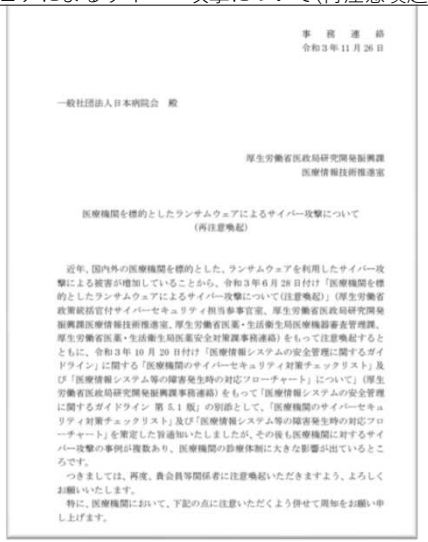
■「医療機関向けランサムウェア対応検討ガイダンス」より

■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

2021/11/26:厚労省「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. 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。

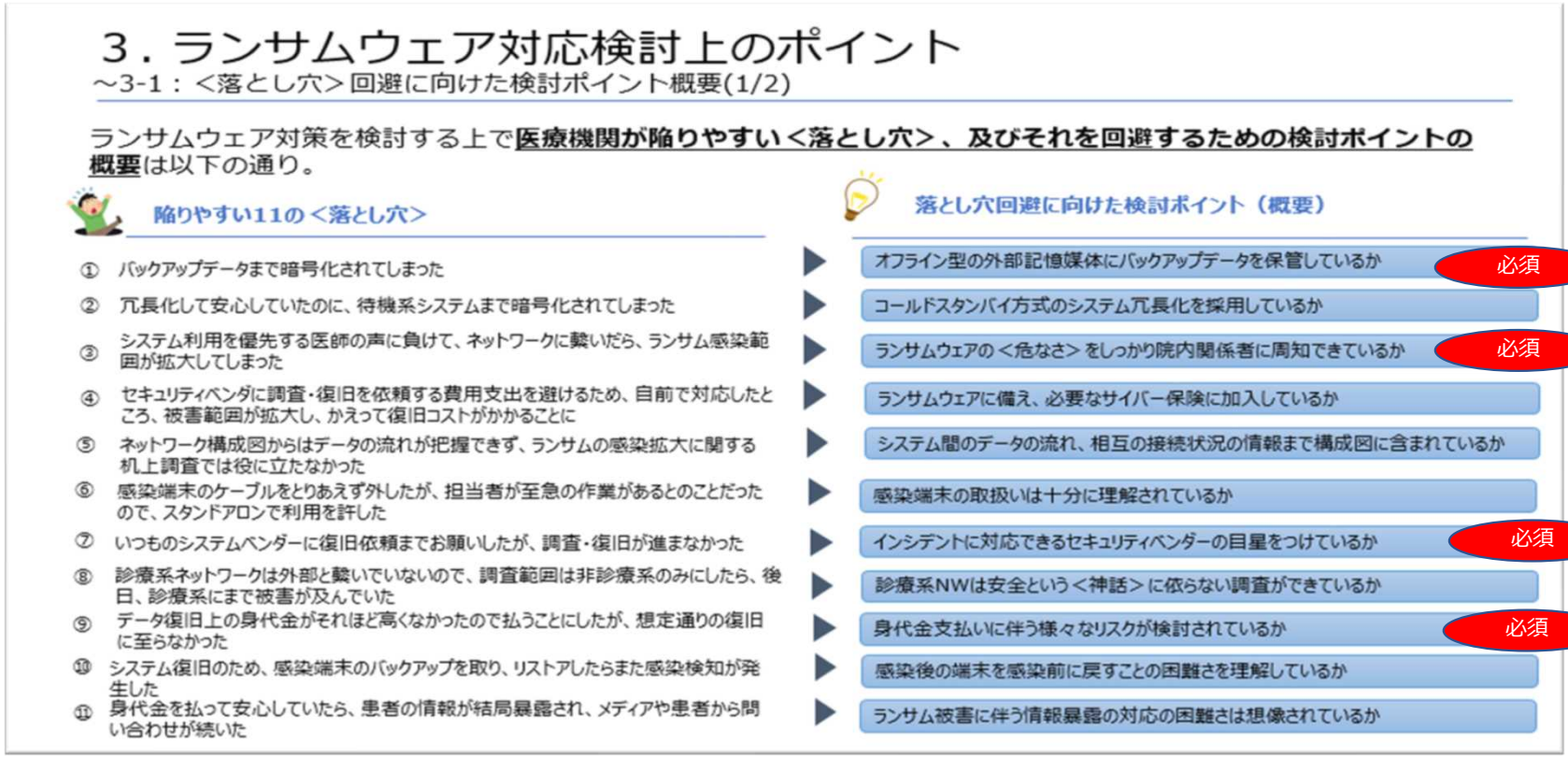
　具体的には、ランサムウェアへの対応を検討する際に、**どのような陥りやすいリスク（落とし穴）があり、それを回避するため、どのような検討を最低限行うべきなのか**についてまとめている。

■「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)

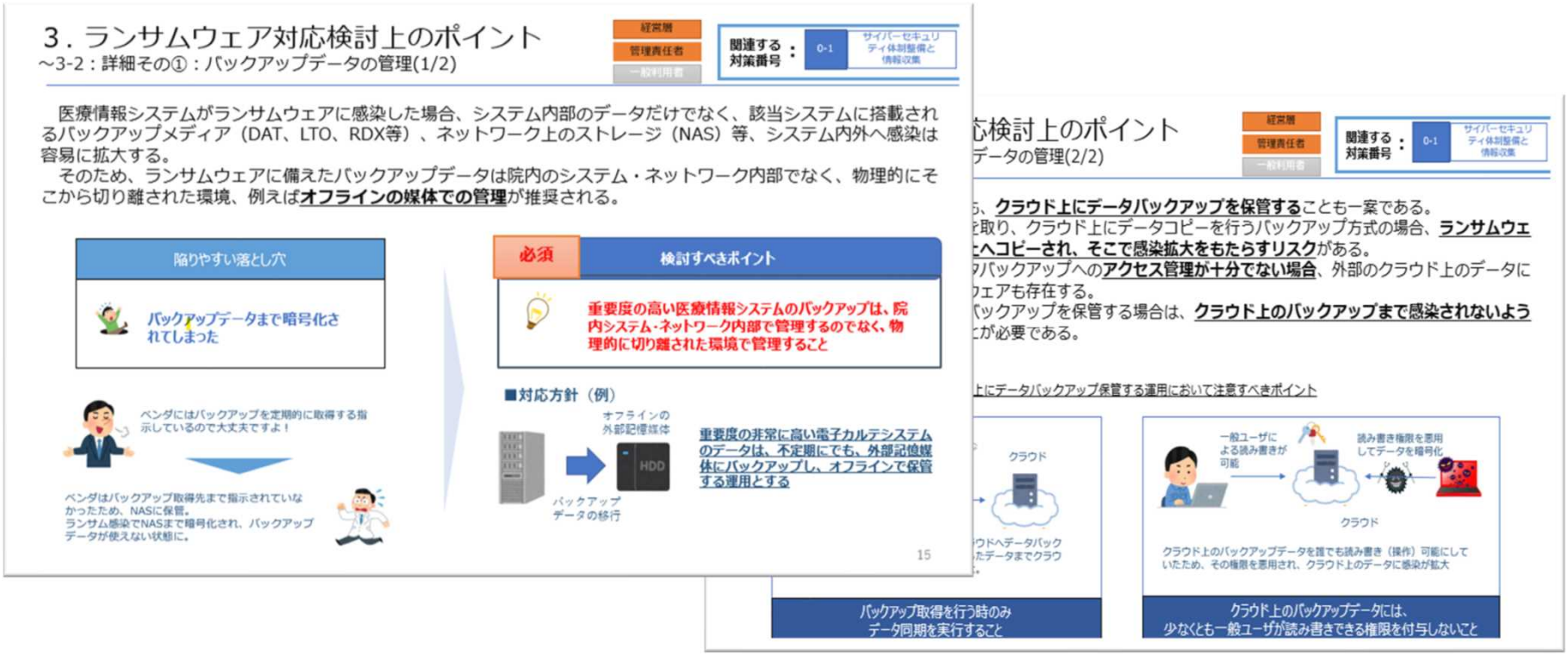
ランサムウェア対策を検討する上で**医療機関が陥りやすい＜落とし穴＞、及びそれを回避するための検討ポイントの概要**は以下の通り。

陥りやすい11の＜落とし穴＞	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	必須
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、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	必須
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	必須
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	必須
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、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	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。

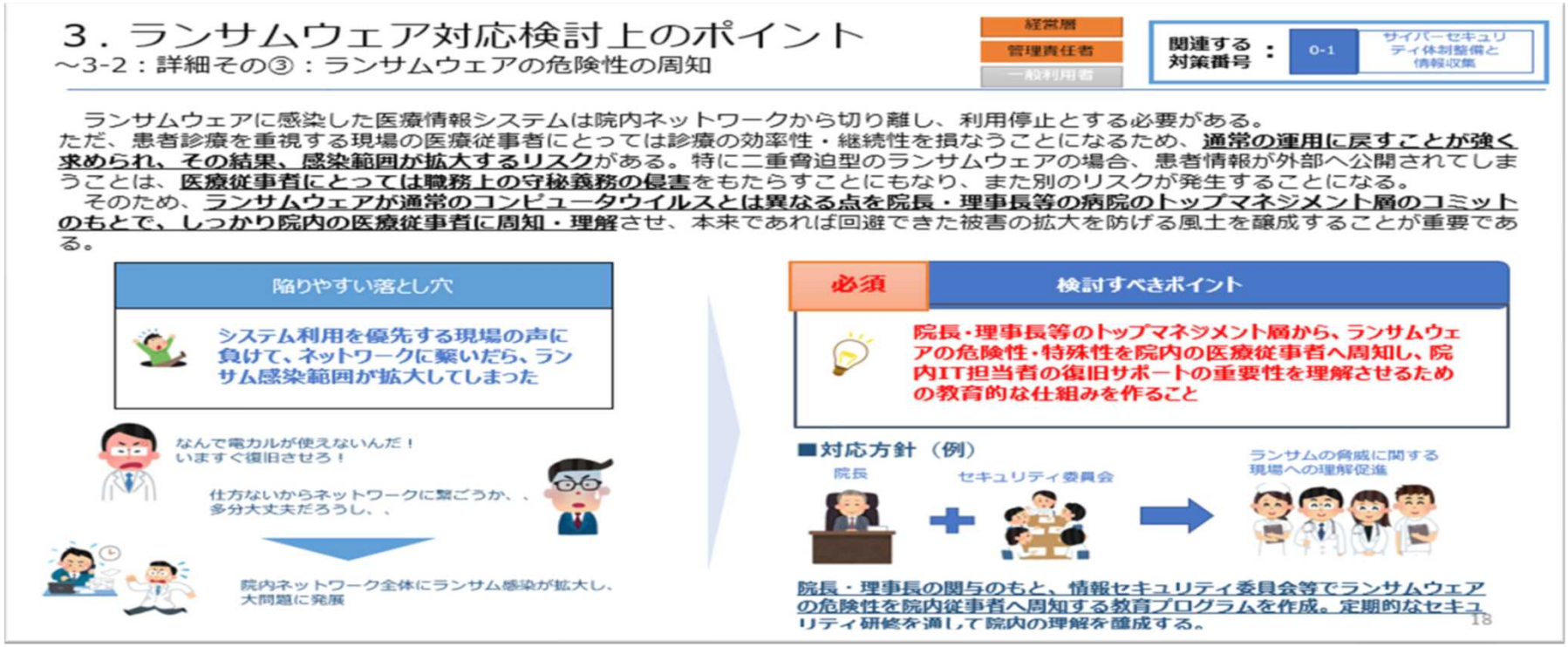
■「医療機関向けランサムウェア対応検討ガイダンス」より



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。

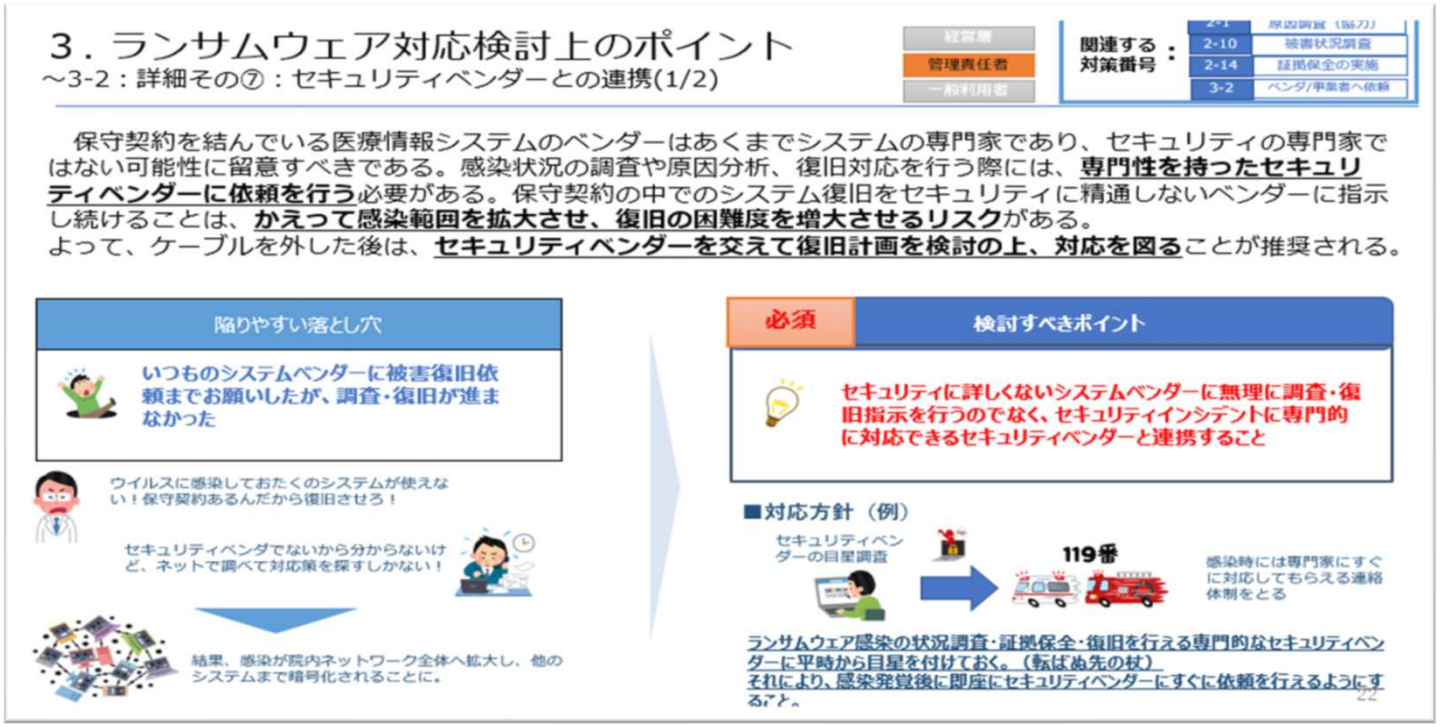
■「医療機関向けランサムウェア対応検討ガイダンス」より



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。

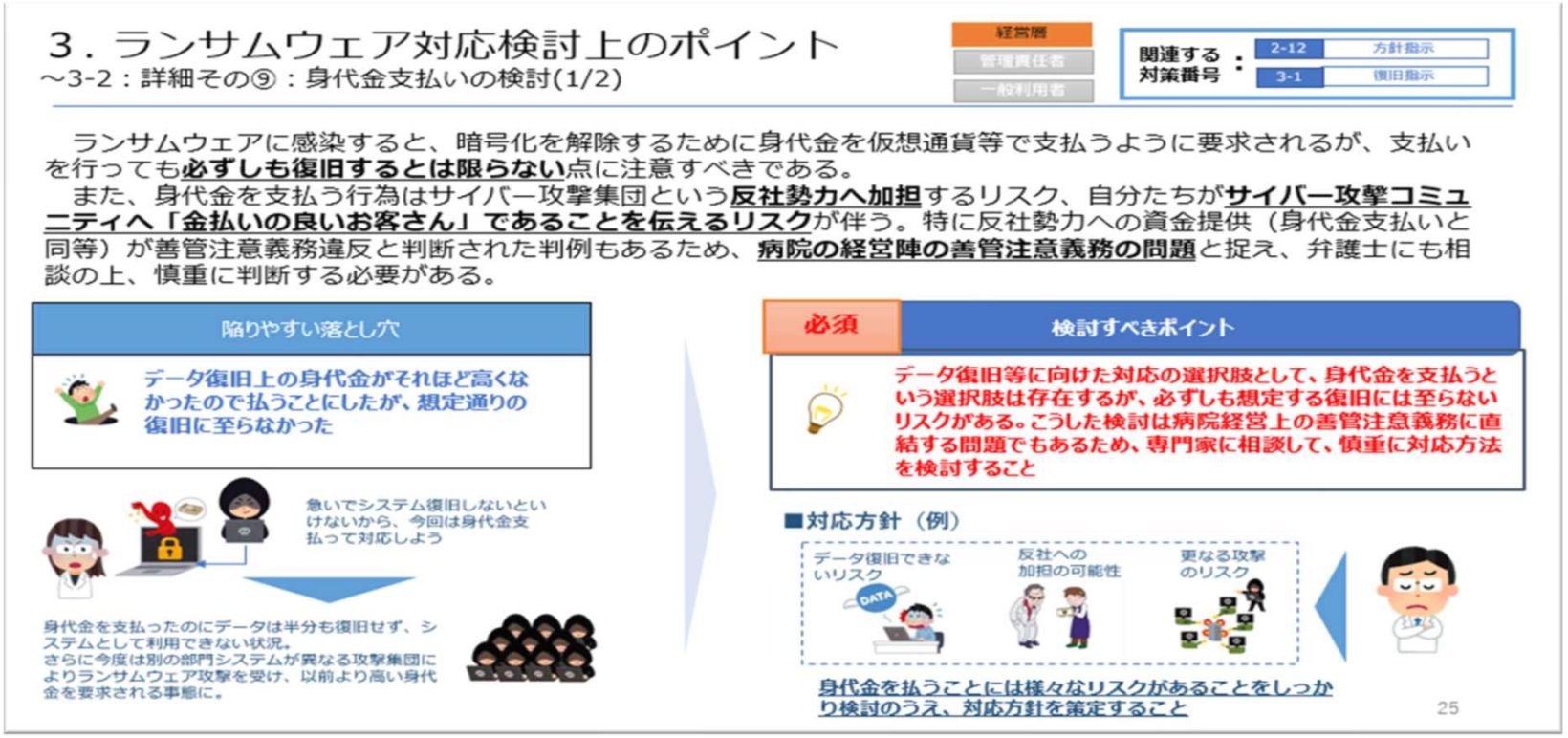
■「医療機関向けランサムウェア対応検討ガイダンス」より



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. まとめ

END