TLP:AMBER

Medical Cyber Security Council
医療サイバーセキュリティ協議会

MedCSCの活動概要

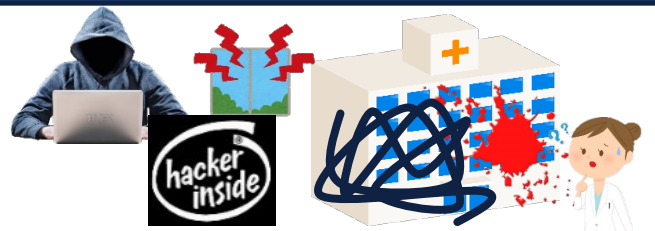
2022/5/16 UPDATE
医療サイバーセキュリティ協議会

TLP:AMBER

Medical Cyber Security Council
医療サイバーセキュリティ協議会

医療サイバーセキュリティ協議会(MEDICAL CYBER SECURITY COUNCIL: MEDCSC)の概要

「医療業界が自助努力によりのサイバー防衛力」を高め、実効的リスク低減を目指す会員共益型の一般社団法人
～病院・医療へのサプライヤーにより、**病院、医療サプライチェーンのサイバーセキュリティリスクの低減を目指す**～



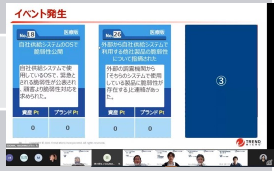
2023年電子処方箋試行、さらにリスク増

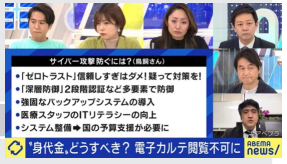
MDCSCの活動目標

- ①医療施設のサイバー対応改善
- ②医療業界のサイバーセキュリティ成熟度向上
- ③重要社会基盤としての医療業界の責務

活動拡大と社会関心増大

協議会の主な活動	内容
第1回座談会 2019/09	医療機器ベンダーサイバーセキュリティ座談会として発足 現状の課題と基本趣旨講演
第2回座談会 2019/12	現状の共有、講演、議論 医療機器ハッキングコンテストの提案
第3回協議会 2020/02	病院におけるセキュリティ対応状況の共有 初の病院での開催、病院見学会
第4回協議会 2020/10	講演：医療機器セキュリティのレギュレーション課題について 講演：病院でのサイバーセキュリティの取り組み紹介
第5回協議会 2021/02	講演：医療機器ベンダーSIRT(CSIRT/PSIRT)の運営紹介 提案：インシデント訓練について
第6回協議会 2021/05	演習：医療業界対象のインシデント訓練（ボードゲーム） 病院、SIer、HISベンダー、医療機器ベンダーの混成チームで病院で発生したサイバーインシデントの対処を行うシミュレーション訓練 https://mdcsc.jp/?p=227
第7回協議会 2021/09	討論：医療機器ベンダー視点のギャップと医療機関視点のギャップ
第8回協議会 2022/01	情報交換ワークショップ 講演：PKIの基礎と医療分野への適用（講演） 講演：3省ガイドラインの改訂の影響（講演）
第1回スピンオフ座談会 2022/02	TLP:REDによる病院、医療機器ベンダーの課題討論
第2回スピンオフ座談会 2022/3	医療機器ベンダーのあるべき姿について徹底議論





- リスク啓発
- サイバーBCP→マネジメント体制
- インシデント対応→セキュリティ運用体制、インテリジェンスの活用
- リスクアセスメント
- 応急的措置→改善ロードマップ

各医療施設の自律的成熟度向上を支援

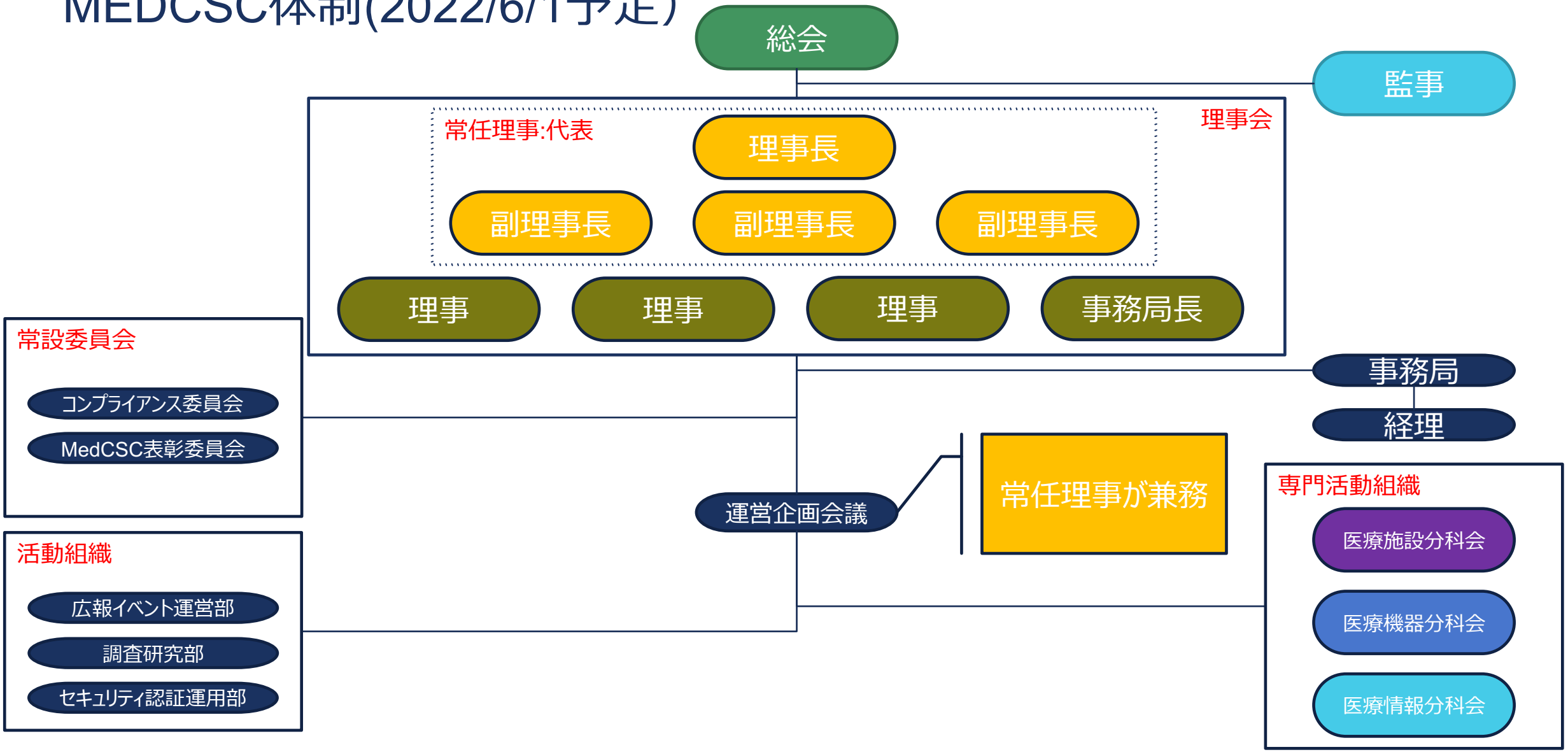
- セキュリティ人材育成
- 地域人材共有
- ガバナンス構築

医療業界全体のサイバー対応力の底上げ

- 非競争領域での連携
- 病院評価
- 外部開示

社会に対する開示・発信

MEDCSC体制(2022/6/1予定)



役員メンバー

理事長
村井勝

- 慶応大学医学部　名誉教授
- 元慶応大学病院病院長

副理事長（病院担当）
鳥飼幸太

- 群馬大学医学部付属病院　システム統合センター　副センター長

副理事長（政策担当）
松山征嗣

- トレンドマイクロ株式会社
- 医療機器サイバーセキュリティ協議会共同発起人

副理事長（戦略担当）
鈴木克明

- オリンパス株式会社
- 医療機器サイバーセキュリティ協議会共同発起人

活動理念

医療業界の全ステークホルダが連携して医療防衛を行う能力を身に着け、
サイバーリスク制御による医療の安心・安全と安定的提供の実現する

自助

- 医療業界の重要ステークホルダーのセキュリティレベル（組織、製品、サービス）向上の支援
- 医療施設の自発的サイバー対応レベルの向上の支援
  - セキュリティガバナンス構築、サイバーBCP、地域連携
- 医療機関へのサプライヤーによる製品・サービスのセキュリティ対応レベルの向上の支援
  - セキュリティ要求に対する責務

共助

- 医療・サプライチェーン一体となったリスクの実行的低減を目的とした活動と対応体制の構築、運営
  - セキュリティ情報交換ワークショップ
  - 情報発信と議論
- セキュリティオペレーションの支援
  - 環境変化への対応
  - 平時の脆弱性対応
  - 有事のインシデントレスポンス）

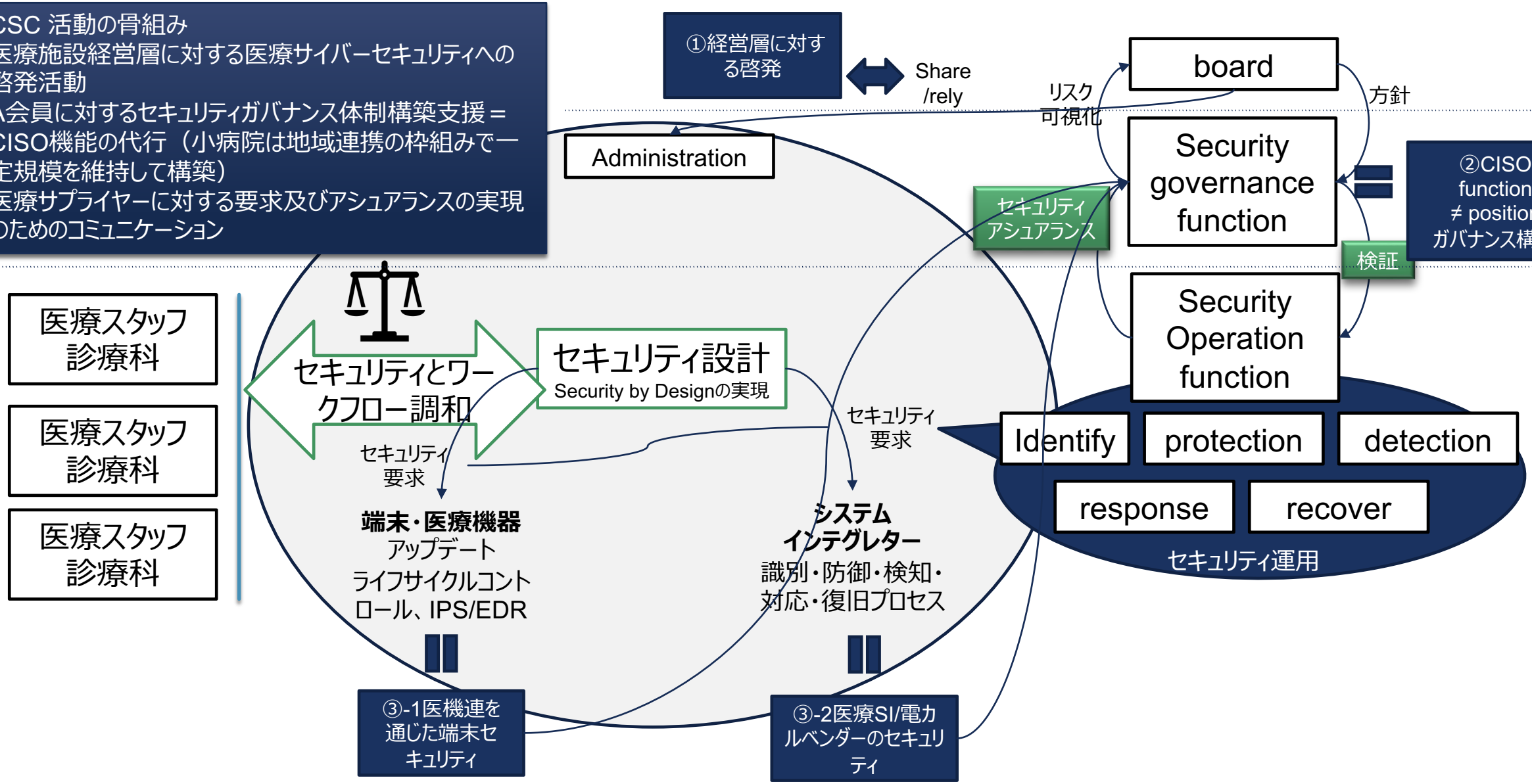
公助

- 医療のサイバーリスク対応に対する環境整備
  - 政府・官公庁との連携
- 医療セキュリティ人材不足の解消
  - セキュリティ人材（医療情報技師）育成

TLP:AMBER

Medical Cyber Security Council
医療サイバーセキュリティ協議会

MedCSC 活動の骨組み
① 医療施設経営層に対する医療サイバーセキュリティへの啓発活動
② A会員に対するセキュリティガバナンス体制構築支援＝CISO機能の代行（小病院は地域連携の枠組みで一定規模を維持して構築）
③ 医療サプライヤーに対する要求及びアシュアランスの実現のためのコミュニケーション



医療セキュリティ実現を考える上で基礎となる「組織・機能・資金」

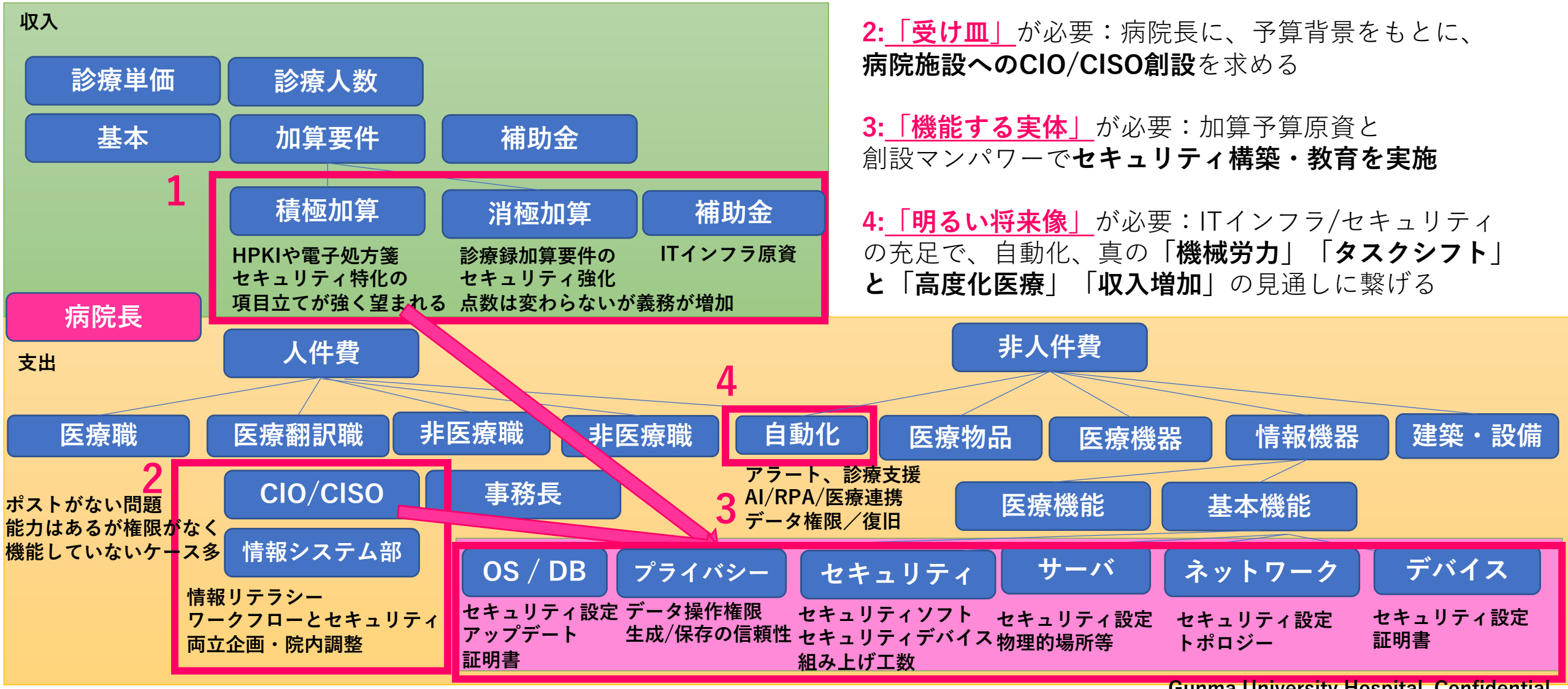
- 予算の流れとセキュリティ強化実施に不足している箇所/
- 病院長+医師系代議士へのアピールポイント

1:「真水の予算」が必要：診療報酬改定や補助金に、**セキュリティ加算やCISO加算、IT設備原資**を求める

2:「受け皿」が必要：病院長に、予算背景をもとに、**病院施設へのCIO/CISO創設**を求める

3:「機能する実体」が必要：加算予算原資と創設マンパワーで**セキュリティ構築・教育を実施**

4:「明るい将来像」が必要：ITインフラ/セキュリティの充足で、自動化、真の「**機械労力**」「**タスクシフト**」と「**高度化医療**」「**収入増加**」の見通しに繋げる



病院の医療セキュリティ化を阻む障壁

- 病院を稼働させながら「継ぎ足し続けた」ネットワーク機器の整理に踏み込む体力が必要

易

セキュリティリテラシーの共通化

院内端末運用の共通化

院内診療手順の共通化

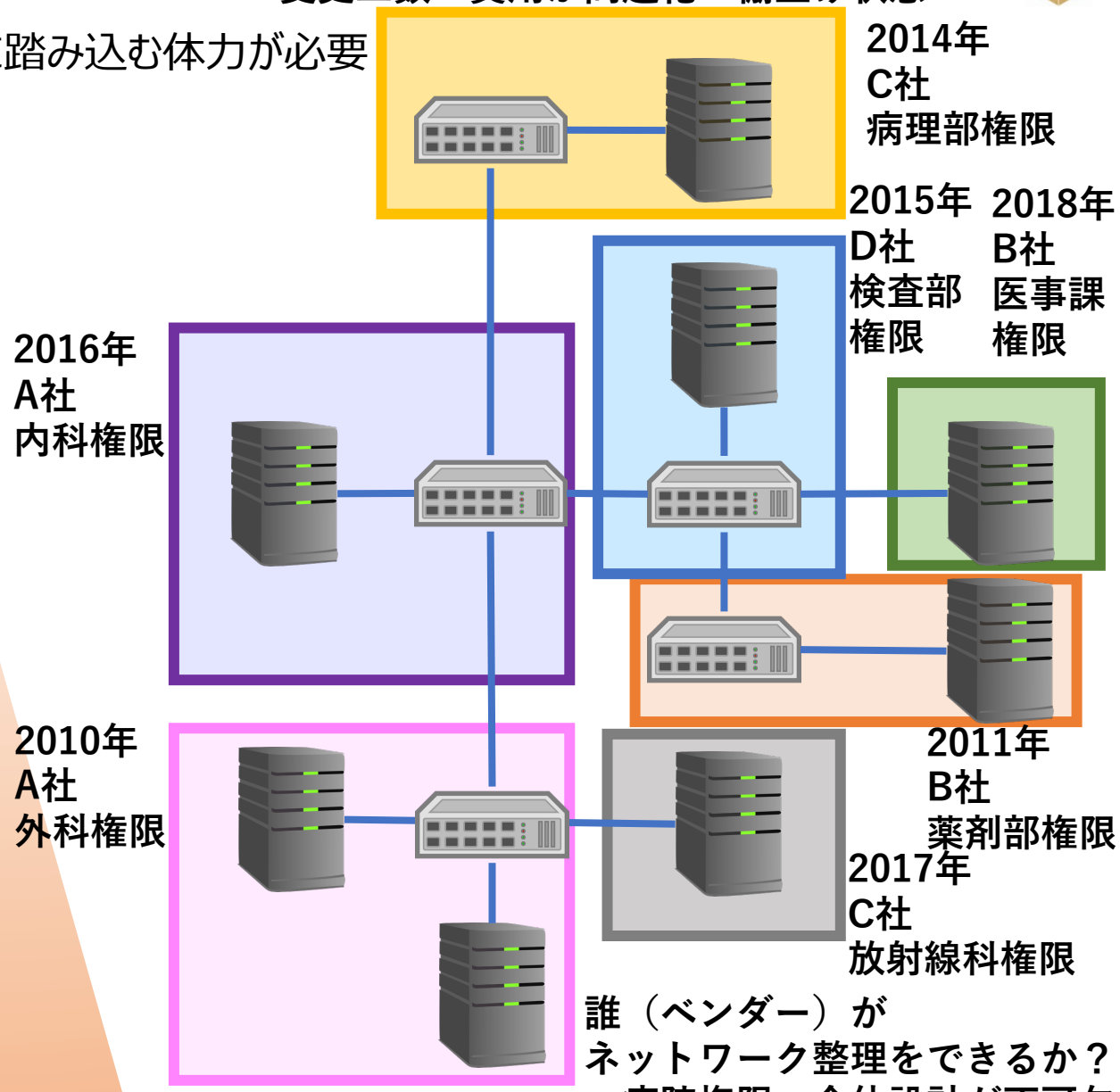
病院内の機器設置場所の整備

ネットワークインフラの整理

電源・建物設備

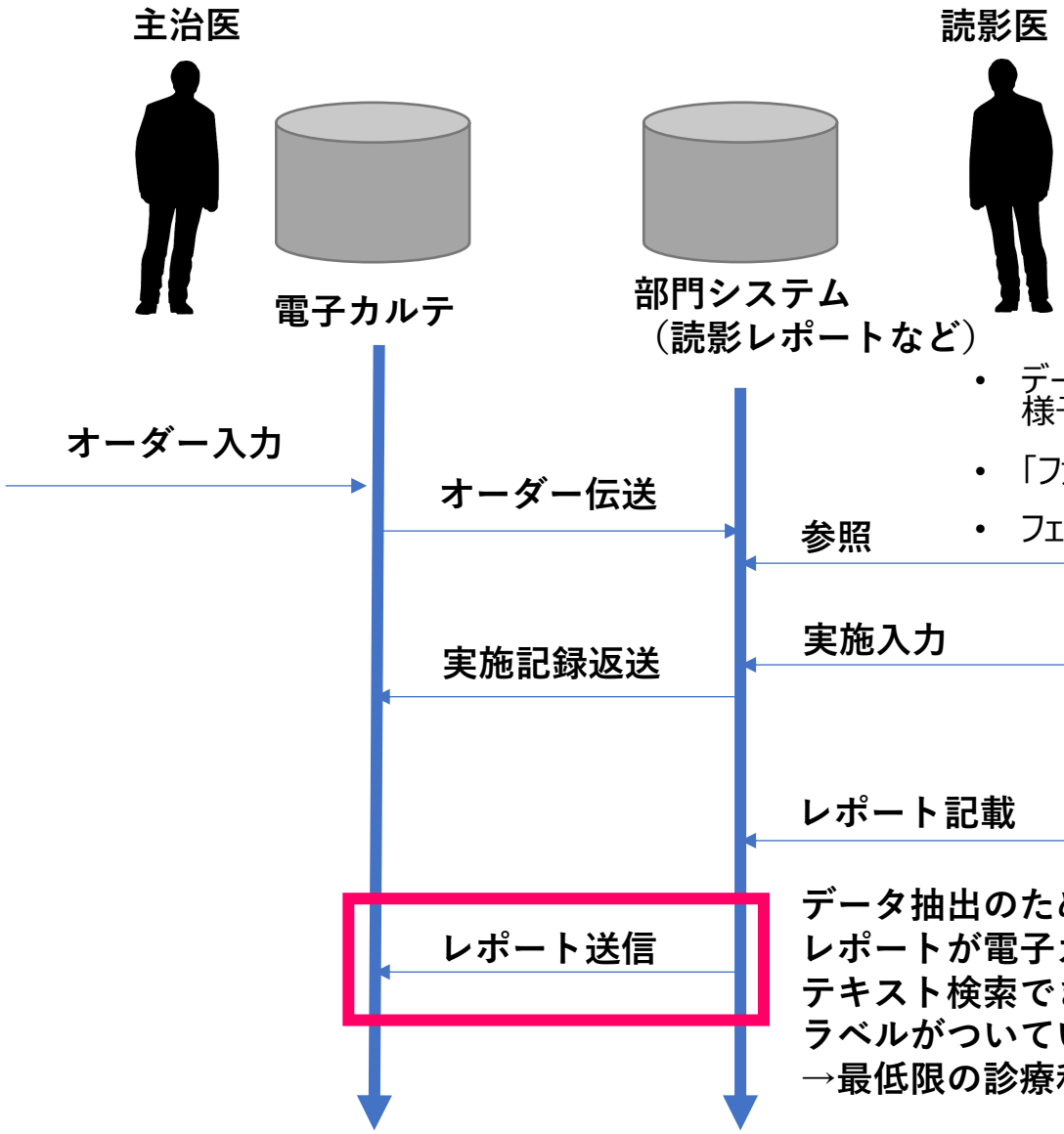
難

「継ぎ足しの」医療機器ネットワーク
変更工数・費用が問題化→棚上げ状態



誰（ベンダー）が
ネットワーク整理をできるか？
→病院権限・全体設計が不可欠

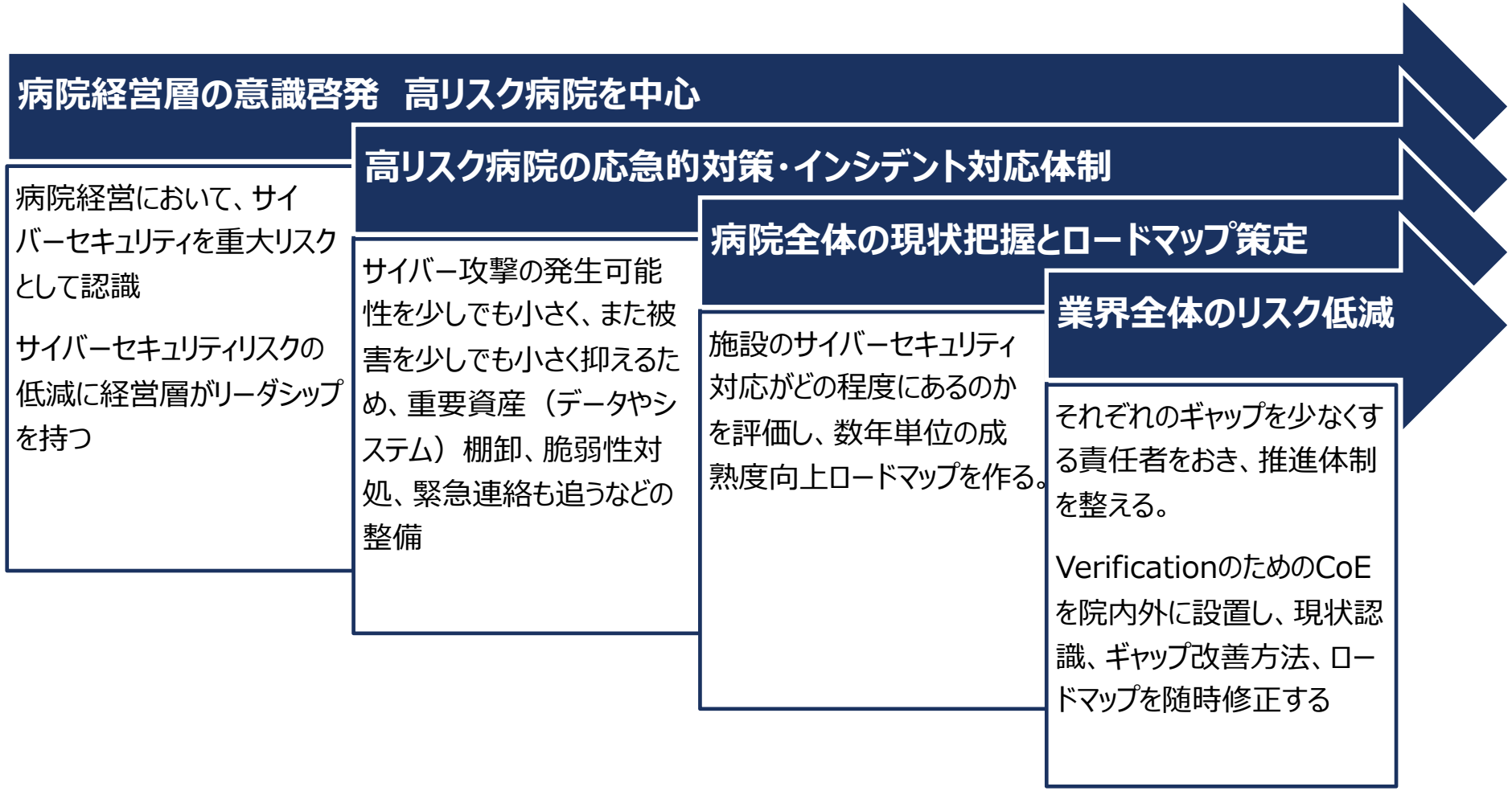
医療情報データサイエンスに関わる「ニワトリとタマゴ」問題



- データを利活用したい人の中で「誰かが接続してくれないかな」と様子見で待っている人多数
- 「ファーストペンギンになって損をしたくない」に囚われすぎて業界が停滞
- フェアな受益者負担の考え方は必要・重要

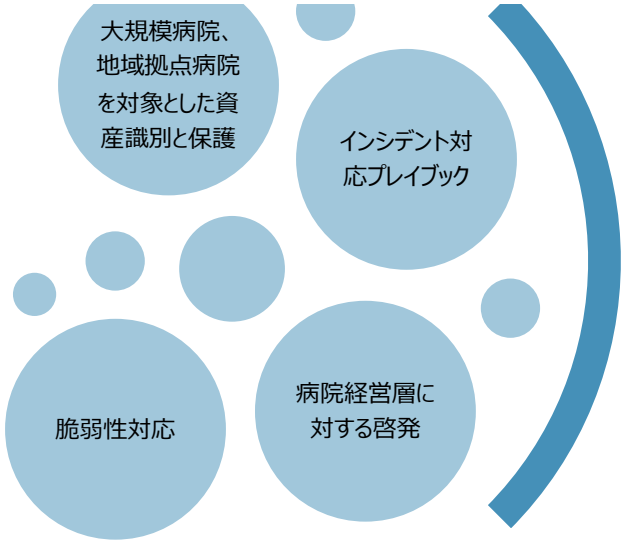
データ抽出のために追加工数を要するケース例
レポートが電子カルテでテキスト検索できるように送信されていない
テキスト検索できても、情報にラベルがついていない
ラベルがついていても独自
→最低限の診療利用のための整備では広範なデータ利活用に繋がらない

データ接続インフラが整って、データサイエンスの研究ができ、資金が獲得できる
資金があって、データ接続インフラを整えることができる　→ 誰が最初のキックを作る？



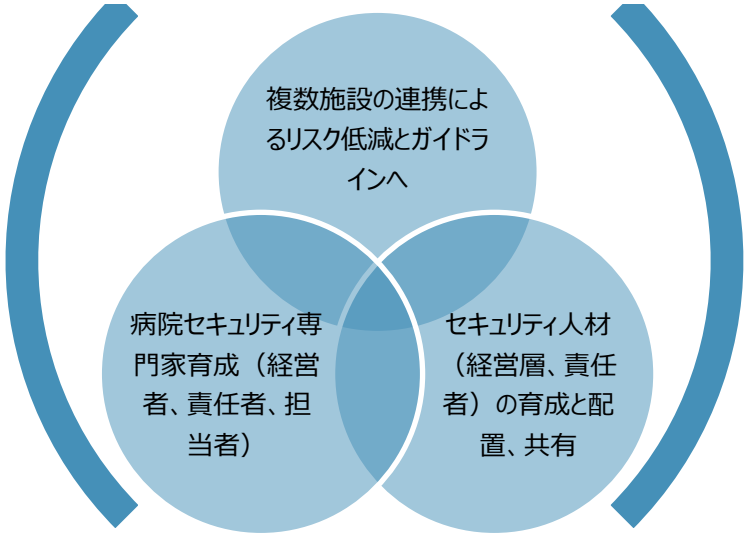
■※インシデント発生状況など施設によっては順序が入れ替わることもあります。

1年目



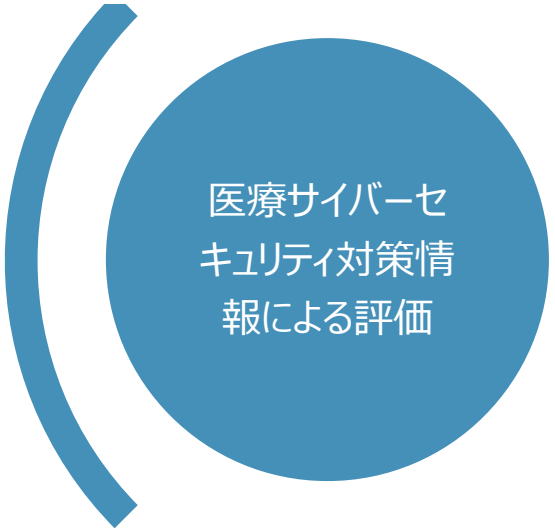
高リスク施設に対するリスク低減の実施

2年目



地域拠点病院まで対象を広げたサイバーセキュリティ成熟度向上

3年目以降



セキュリティガバナンス（院内、地域、サプライヤー）の構築

目的達成までのマイルストーン

医療業界のサイバーリスク低減

意識変革

- あるべき姿の発信
- 体制構築
- 経営陣のリーダシップとリソース確保
- MedCSC協議会、座談会の実施
- 教科書・書籍執筆
- 学会での講演、チュートリアル
- 医療施設で持つべきセキュリティ体制モデルの作成
- 病院経営層に対する直接的な重要リスク認識の語りかけ
- 協議会会員相互の共助関係構築
- 公助体制の構築（診療報酬）
- 医療業界向けサイバーセキュリティ保険の開発

医療施設の成熟度向上

- 推進体制
- リスク分析
- 戦略策定
- 実行評価
- 医療特有の問題対処ができるセキュリティ人材の育成
- セキュリティ責任者の設置と権限付与
- 実行責任者の獲得
- サイバーBCP及びインシデント対応体制の構築
- 病院のセキュリティ成熟ロードマップ策定支援
- 協議会による成熟度評価
- 病院経営層にセキュリティ知識を教育
- エンジニアに病院経営知識を教育
- 医療情報技師改良・育成

サプライチェーンガバナンス

- 啓発
- 医療施設・サプライヤーのコミュニケーション
- 対医療機器、サービス、電カルベンダー
- 対インテグレータ
- 医療の重要エンティティである責任を各業界団体で認識させる
- 医療サプライヤー連絡会の創設
- 協議会での情報共有ワークショップ
- 座談会による課題議論
- 医療施設で必要なセキュリティ要求の先取り対応
- SIerとして、医療施設のリスクコントロールを自発的に引き上げる
- 病院のセキュリティ要件ガイドライン作成

一般社団法人化について（定款案より抜粋）

- 2022/4現在、協議会は任意団体として31組織、60名が登録されている。
- 基本的には企業・団体による参画を原則とするが、理事会の決議に基づき個人の参加を認める場合もある
- 2022/6以降（登記後）、協議会会員は、会員資格の確認の連絡から2022/12末までに以下のいずれかの2023年度以降の属性、もしくは退会を申し出ることとする。申し出がない場合はB会員とする。
  - 執行部・協議会職員・・・協議会執行部・事務局、セキュリティ共助環境の構築、維持、運営、改善。会費の適切な運用と開示。
  - A会員・・・共助対象となる医療施設。協議会・講演、座談会などのイベントへの参加、医療機関のセキュリティ向上共助支援、見学会などへの参加。会費（協議会運営資金）の供出。
  - B会員・・・医療サプライヤー。共助の枠組みへの貢献、医療業界におけるセキュリティ動向や情報収集を目的とした医療機関以外の団体、協議会・講演・座談会などイベントへの参加。会費（協議会運営資金）の供出
  - 賛助会員・・・協議会の業務提携に基づく会員資格、協議会・講演・座談会などイベントへの参加、協議会運営資金の提供
  - オブザーバー・・・官公庁、他の任意団体による会員資格、協議会・講演・座談会などイベントへの参加、共助組織の適切な発展を目的とした様々な助言、支援、活動を要請
- このうち、執行部・協議会職員、賛助会員、オブザーバーは一般社団法人医療サイバーセキュリティ協議会の社員となる資格を有す。

会員種別	年会費	対象	権利・義務
執行部 協議会 職員	-----	協議会執行 理事 監事 顧問など	• セキュリティガバナンス構築支援提供 • Medical ISAC(仮称）の運営 • 協議会・座談会などの開催・運営
A会員	診療所 20,000円/年 200床未満 100,000円/年 400床未満 150,000円/年 400床以上 200,000円/年	医療機関 （共助対象）	• セキュリティガバナンス支援要請 • Medical ISAC（仮称）への参加 • 協議会・座談会・イベントへの参加
B会員	法人正会員 100,000円/年 個人正会員 5,000円/年	医療サプライヤーや 個人	• Medical ISAC（仮称）への参加義務 • 協議会・座談会・イベントへの参加
賛助会員	法人・個人賛助会員	協議会との 業務提携等に基づく 会員資格	• セキュリティ向上のためのISACへの参加 • 協議会・座談会・イベントへの参加
オブザーバー	理事会の決議による原則無償	官公庁/ 任意団体メンバー	• 執行部に準ずる