

# 一般社団法人医療サイバーセキュリティ協議会のご紹介

## Medical Cyber Security Council

# 一般社団法人医療サイバーセキュリティのご紹介

## 2022年度活動報告

- 2022年度は、一般社団法人としての医療サイバーセキュリティ協議会の初年度でした。実際に医療機関で医療事業停止を引き起こすサイバーインシデントが複数発生し、サイバーリスクは高い状態であった。地政学的にも、ロシア・中国・北朝鮮に対するサプライチェーン独立の流れもあり、サイバーリスクは依然高い状態を維持することが推測される。そのなかで、2022年度は、以下の活動を行なった。
  - 市中病院に対するサイバーアセスメントの実施（2022/6, 筑波記念病院様他）
  - サイバー保険製品開発に向けた話し合い（2022/7-8, SOMPO Japan他）
  - 病院に対するC-BCP(サイバー事業継続計画)雛形の展開（日本病院会）
  - 医療機関におけるサイバーセキュリティ人材（仮称：医療CISO）の育成に向けたフレームワークの構築・合意(医療情報学会@札幌にて2022/11)
  - 協議会を通じた会員に対するサイバーセキュリティケイパビリティ獲得支援活動(随時)
  - 厚生労働省の医療分野におけるサイバーセキュリティ情報共有の検討会、オンライン診療にかかるガイドライン改定研究班への参加など
- MedCSCは、医療機関のサイバーセキュリティ成熟度の向上、リスクの実効的な低減の支援を。サプライヤーに対しては、医療施設で動作しているシステム、機器、ソフトウェアのセキュリティアシュアランスを提供できるケイパビリティの獲得支援を行います。

## 2023 年度のMedCSC活動方針

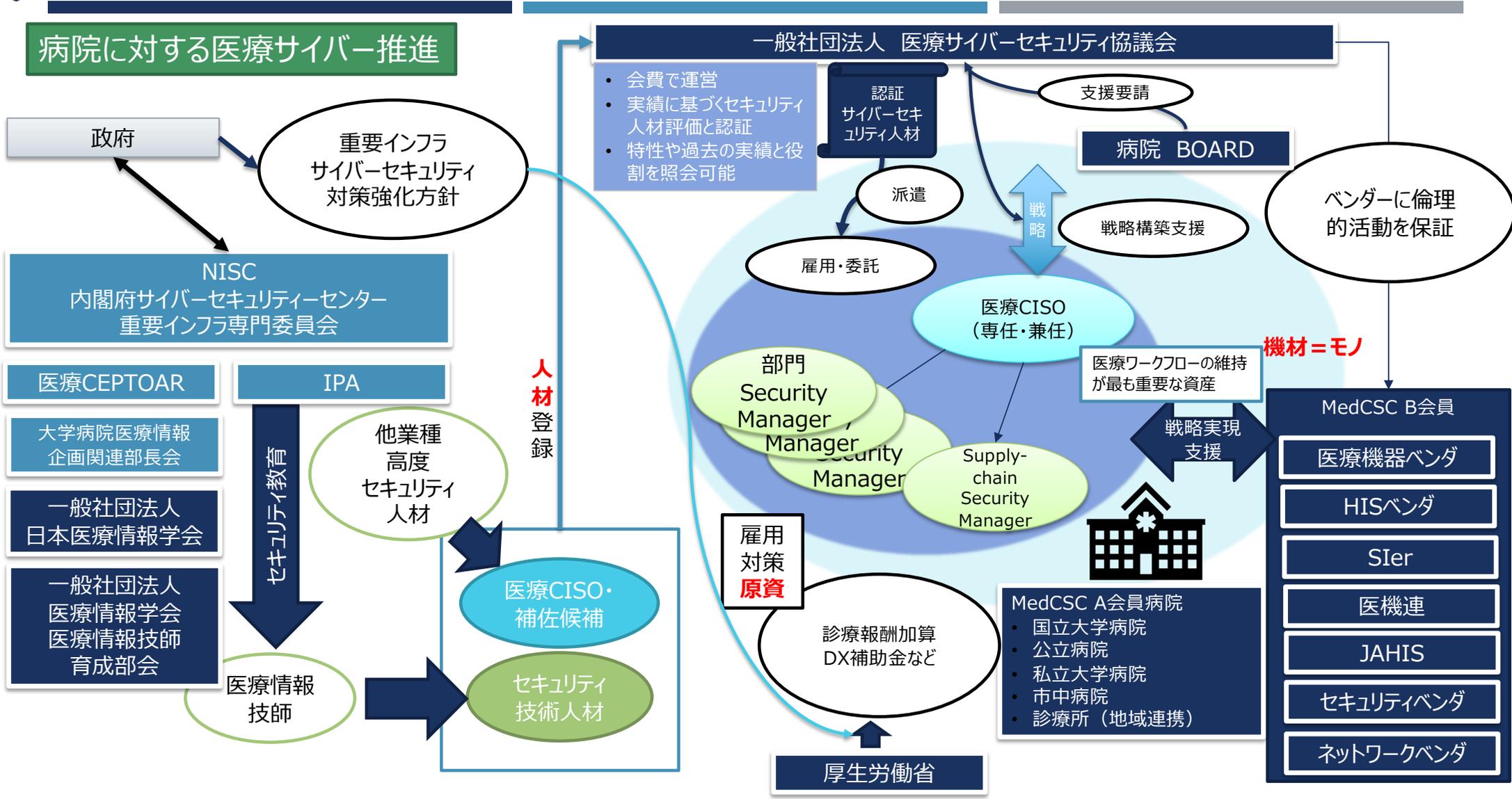
2023年度は、医療業界において、サイバーセキュリティ対策が進まない以下の3つの課題に直接対応していく。

1. 医療機関におけるセキュリティ人材育成と医療機関を中心としたサイバーセキュリティガバナンス構築
  - サイバーセキュリティで毀損される可能性のある資産は、ほとんどが医療機関のものであることから、医療機関自らがサイバーセキュリティ対応を行う必要がある。しかし、サイバーセキュリティ対応は専門知見が必要であり、まずは、医療機関側に立つCISOを育成することで医療機関を中心としたセキュリティガバナンスを構築する。
2. 医療機関、業者双方納得した導入と保守契約の実現による医療機関のサプライチェーンマネジメントの有効性向上
  - 医療機関が、導入するセキュリティ対策は限られた資産を合理的に配分する必要がある。リスク分析に基いた優先度に基づく分配がなされるべきである。また、医療システム、機器については、セキュリティ対策がどのようなリスクに対応するために機能しているかを明確にする必要がある。
3. リスクに応じたサイバーセキュリティ情報の展開と、リアクションのモニタリング
  - サイバーセキュリティに関連する情報が無造作に展開されている状態では、意味がなく、必要なアクションを翻訳して展開し、かつ、それらのアクションのモニタリングが必要となる。

## ①医療業界の人材不足

- 病院におけるサイバー攻撃被害が頻発、長期間（数日～1カ月以上）に及ぶ医療の停止被害が発生している
- 医療関係者のリスク認識は高まっても、対応がなかなか進まない
- ∴医療業界におけるサイバーセキュリティリソース不足
  - 人：内閣サイバーセキュリティセンター(NISC)、IPA、医療情報学会、大学病院医療情報企画関連部長会、奈良先端大学院大学門林Lab、医療サイバーセキュリティ協議会による人材育成構想の合意(2022/11)
    - 各県の急性期医療センターを対象にした50名（2年間）の指導的サイバーセキュリティ人材を育成（その後2年間で200名：各県の中核病院以上）を目標
    - NISC、IPA、門林Labにより、候補人材（医療情報技師＋他業界のセキュリティ人材）へサイバーセキュリティ教育コンテンツと日々のアップデート、資格化
    - 医療情報学会＋大学病院医療情報企画関連部長会：各病院でのサプライチェーンを含めたセキュリティガバナンスの構築（MedCSCが総合支援）
    - MedCSC：育成された人材登録と分配、ガバナンス、サイバーBCP構築、病院に対するサプライヤー協力の維持などのツール提供、現場支援
  - システム・医療機器：医機連とMedCSCにより議論開始(MedCSC)
    - 医機製販業らが医療機関におけるサイバーセキュリティ要求に応えるためのセキュリティアシュアランスを実現
  - お金：体制構築・人材・セキュリティ対策機器等に対する診療報酬の加算を厚労省に働きかけ
    - ガイドライン改訂と合わせて検討中

### 病院に対する医療サイバー推進



## ②医療機関と業者間の信頼関係を向上させる

病院にサイバーセキュリティ専門人材がCISOとして配置され、セキュリティガバナンスを構築していく中で、サイバー成熟度を上げるためにアセスメント、ロードマップなどの戦略を策定する必要がある

医療現場では、医療機関とベンダー間でのインシデント発生時に責任分解点が不明瞭であり、平時オペレーション（脆弱性ハンドリングやリスク評価）、有事オペレーションインシデントレスポンス（フォレンジックや復旧など）の実施が双方納得のもとでできていない

∴ サイバーセキュリティのオペレーションにおいて、双方が必要性及び優先度に納得できる保守契約を結ぶことができる必要がある

サイバーセキュリティにおける対策の必要性を論理的に表現し、双方で納得する必要がある。

セキュリティアシュアランスケース：必達条件（システムの可用性など）を達成するために必要な要件を木構造で表した論理式

論理式であるため、必要条件や達成のリスクなどを考慮して双方が法的に理解できる

ケースを全て書き出すことが困難であるので、ユーザグループを作ってケースのバージョンアップを行なっていく

ケースを構築できるノウハウをMedCSCがレクチャーし、多くの医療機関に対して実施し、アシュアランスケースを成熟させていく

### 医療ワークフローとセキュリティガバナンス

1. 医療施設のセキュリティアシュアランス構築≒CISO機能の構築、の支援・代行（小規模施設は地域連携の枠組みで一定規模を維持して構築）
2. システムオペレーションに対するセキュリティ要求 などセキュリティコミュニケーションの推進

① 経営層の与信

共有・信頼・委任

管理部門

リスク可視化

経営層

セキュリティガバナンス

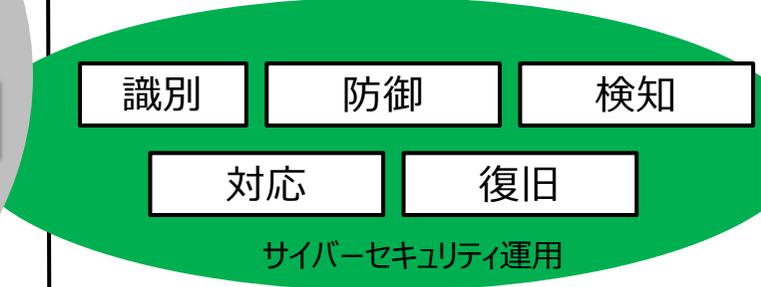
方針

検証

② セキュリティガバナンスの構築

セキュリティオペレーション

セキュリティアシュアランス



セキュリティ設計  
Security by Designの  
実現

セキュリティとワークフロー調和

セキュリティ要求

セキュリティ要求

医療ワークフロー上に調和実装

端末・医療機器  
アップデート  
ライフサイクルコントロール、IPS/EDR

システムインテグレーター  
識別・防御・検知・  
対応・復旧プロセス

医療スタッフ  
診療科

医療スタッフ  
診療科

医療スタッフ  
診療科

③-1 医療機器ベンダーを通じた納入システムセキュリティ

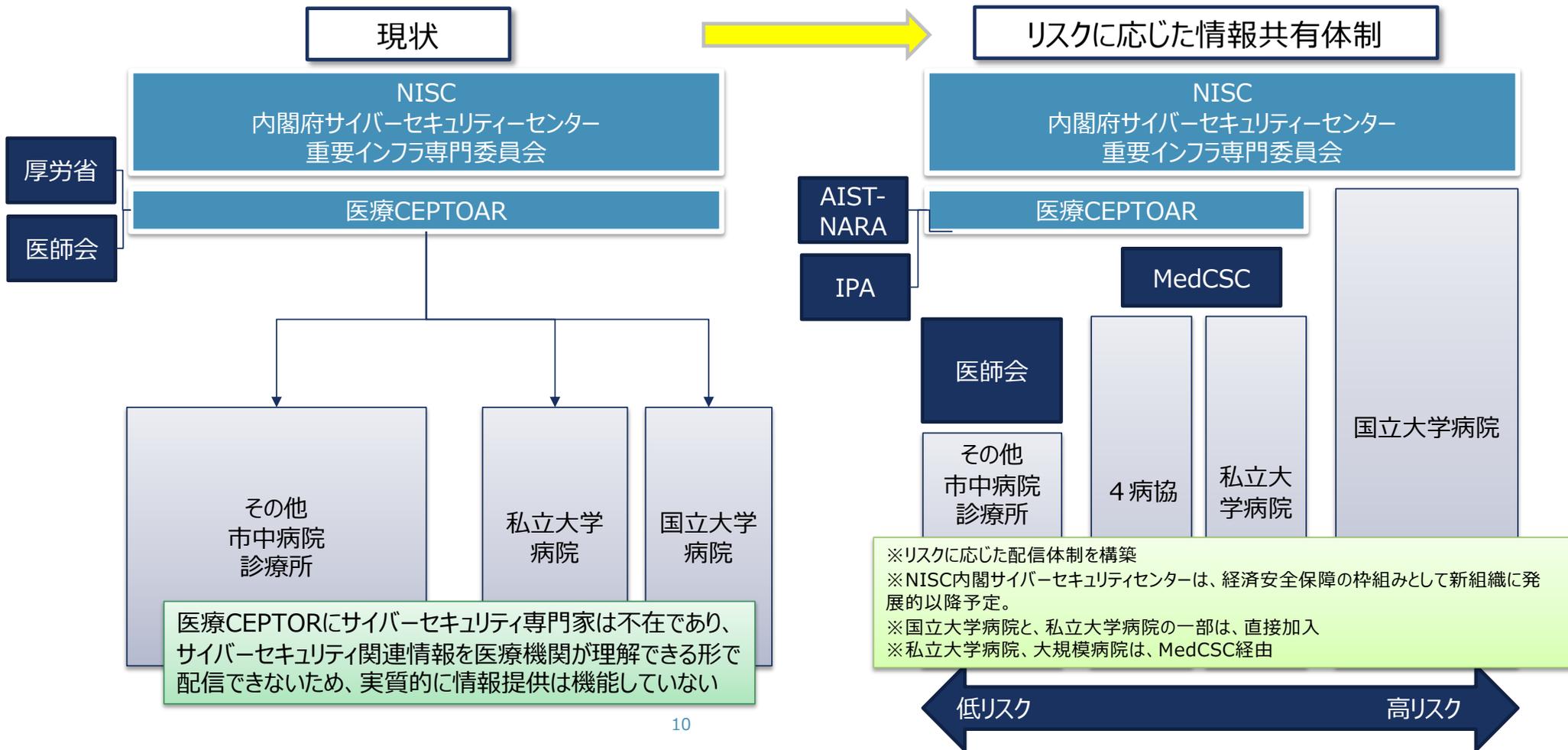
③-2 医療ネットワーク・SI/電カルベンダーを通じたシステムセキュリティ

- ・ インシデントレスポンス連携⇒合同インシデント訓練
- ・ リスクコミュニケーション（脆弱性、SBOMやTII）⇒情報交換ワークショップ、フラットなコミュニケーションの場
- ・ セキュリティアシュアランスツリー構築の協力⇒共助、ベストプラクティス共有

### ③適切な情報展開

- NISC サイバーセキュリティ協議会は、サイバーセキュリティ関連情報（「サイバー攻撃の被害が発生した」、「重大な脆弱性が発見され対応が必要」など）の共有を行なっている。医療業界に対しては、医療CEPTOAR（事務局が日本医師会）によって展開されている
  - 「医療機関側で素早くアクションが取れる形での情報共有」：当初は、重大な脆弱性について情報共有の際、展開された医療機関側でどういったアクションをとって良いかわからないなどの状況も発生したが、徐々に医療機関がどのようなアクションを取れば良いかという情報を付与して展開するなどやや改善されている。
  - 「モニタリングの必要性」：情報を受け取った医療機関が、アクションをとったか否か、どのようなアクションをとったかという情報をあつめ状況を可視化することも必要となる。
  - 「リスクに応じた情報展開の必要性」：サイバー攻撃により被害が発生した場合、急性期病院などはリスクが高い反面、診療所などは比較的风险が低い。そのため、リスクに応じた情報展開を行うことが可能な体制を作る必要がある
  
- リスクに応じた情報展開体制案：
  - 国公立大学病院は、NISCへ直接加入する
  - 大手私立大学病院・急性期・中核病院は適切な団体を通じて情報展開・アクションのモニタリングを行う
  - その他市中病院、診療所は上記の情報を参考にして医師会を通じて配信

# サイバーセキュリティ関連情報共有フローの改善



# 入会案内



## 会員資格と入会のご案内

- 一般社団法人医療サイバーセキュリティ協議会(MedCSC)の会員資格は4種類があります。
  - A/B会員は、協議会会員の相互共助により、サイバーセキュリティに関連する様々な支援を受けられます。
    - サイバーセキュリティに関する各種助言、相談
    - Cyber-BCP構築支援、サイバーリスクアセスメントテンプレート提供など
1. A会員:医療機関の法人もしくは個人

a.	診療所等	年会費	20,000 円
b.	200 床未満	年会費	100,000 円
c.	400 床未満	年会費	150,000 円
d.	400 床以上	年会費	200,000 円
  2. B会員:医療機関に対するサプライヤーの法人もしくは個人

a.	法人	年会費	100,000 円
b.	個人	年会費	5,000 円
  3. 賛助会員:協議会との業務提携等に基づく会員資格
    - ① 年会費は別途契約によって定める 資格:当協議会の趣旨に賛同して基金を拠出し、さまざまな活動において活動を共にする法人・個人
    - ② 特典:当協議会が参加するイベントへの参加、当協議会からの情報共有、グループワークサイトへの参加など
  4. オブザーバー:官公庁、任意団体のメンバー
- A会員およびB会員は、法人法上の社員となります。
  - 入会は、会員規約の巻末にある入会申込書を、[info@medcsc.org](mailto:info@medcsc.org)に送付してください。理事会での承認ののち、会費の振込が確認できた時点で入会完了となります。



<https://medcsc.org/>