TLP:AMBER+STRICT

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

MedCSC活動紹介

一般社団法人医療サイバーセキュリティ協議会

2023/6

TLP:AMBER+STRICT

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

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、サイバーリスクは以前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）
  - サイバー保険製品開発に向けた話し合い　（2022/7-8, SOMPO Japan）
  - 病院に対するC-BCP(サイバー事業継続計画)雛形の展開
  - 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(2022/11)
  - 協議会を通し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

- 会員数が見込みの50%にとどまる結果となっています。MedCSCの価値を広く周知して、継続的な活動としていきたい。

- 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。

TLP:AMBER+STRICT

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

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に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。

TLP:AMBER+STRICT

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

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

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

病院に対する医療サイバー推進

政府

重要インフラ
サイバーセキュリティ
対策強化方針

NISC
内閣府サイバーセキュリティーセンター
重要インフラ専門委員会

医療CEPTOAR

IPA

大学病院医療情報
企画関連部長会

一般社団法人
日本医療情報学会

一般社団法人
医療情報学会
医療情報技師
育成部会

セキュリティ教育

医療情報
技師

他業種
高度
セキュリティ
人材

人材登録

医療CISO・
補佐候補

セキュリティ
技術人材

一般社団法人　医療サイバーセキュリティ協議会

- 会費で運営
- 実績に基づくセキュリティ人材評価と認証
- 特性や過去の実績と役割を照会可能

認証
サイバーセキュリティ人材

派遣

雇用・委託

支援要請

病院　BOARD

戦略

戦略構築支援

ベンダーに倫理的活動を保証

医療CISO
（専任・兼任）

部門
Security
Manager

Security
Manager

Security
Manager

Supply-
chain
Security
Manager

機材＝モノ

戦略実現
支援

MedCSC B会員

- 医療機器ベンダ
- HISベンダ
- SIer
- 医機連
- JAHIS
- セキュリティベンダ
- ネットワークベンダ

雇用
対策
原資

サイバーセキュリティ
責任者・体制設置
加算

MedCSC A会員病院

- 国立大学病院
- 公立病院
- 私立大学病院
- 市中病院
- 診療所（地域連携）

厚生労働省

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、双方が必要性や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

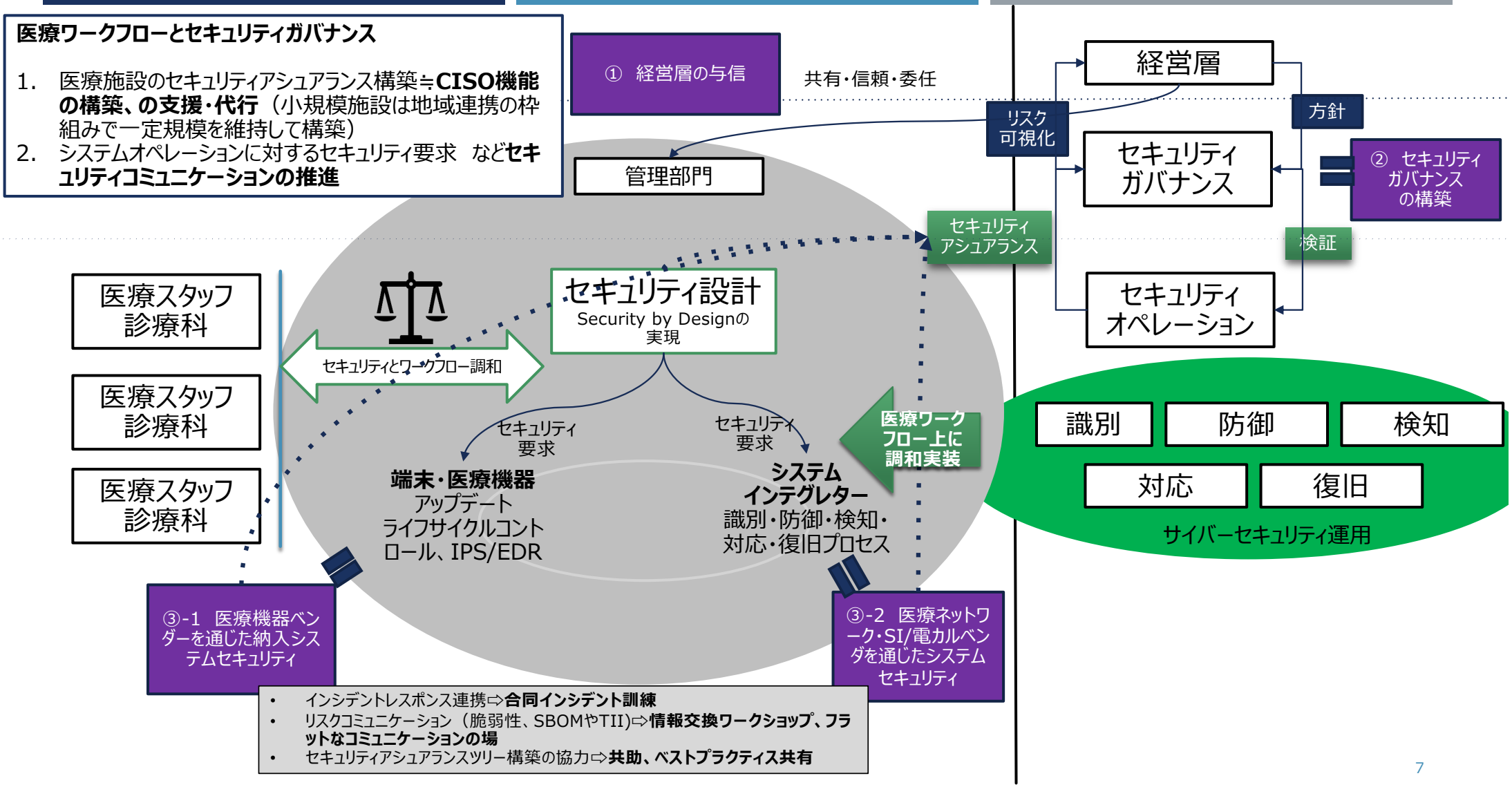
論理式であるため、必要条件や達成のリスクなどを考慮して双方が法的に理解できる

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**

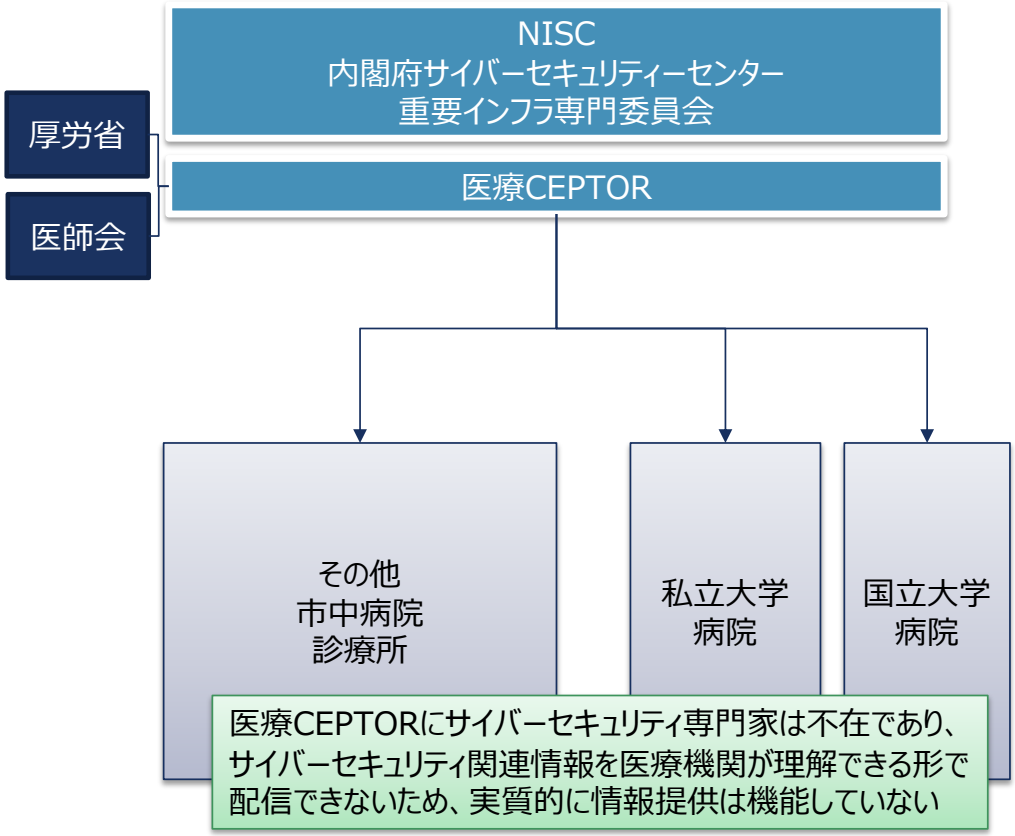


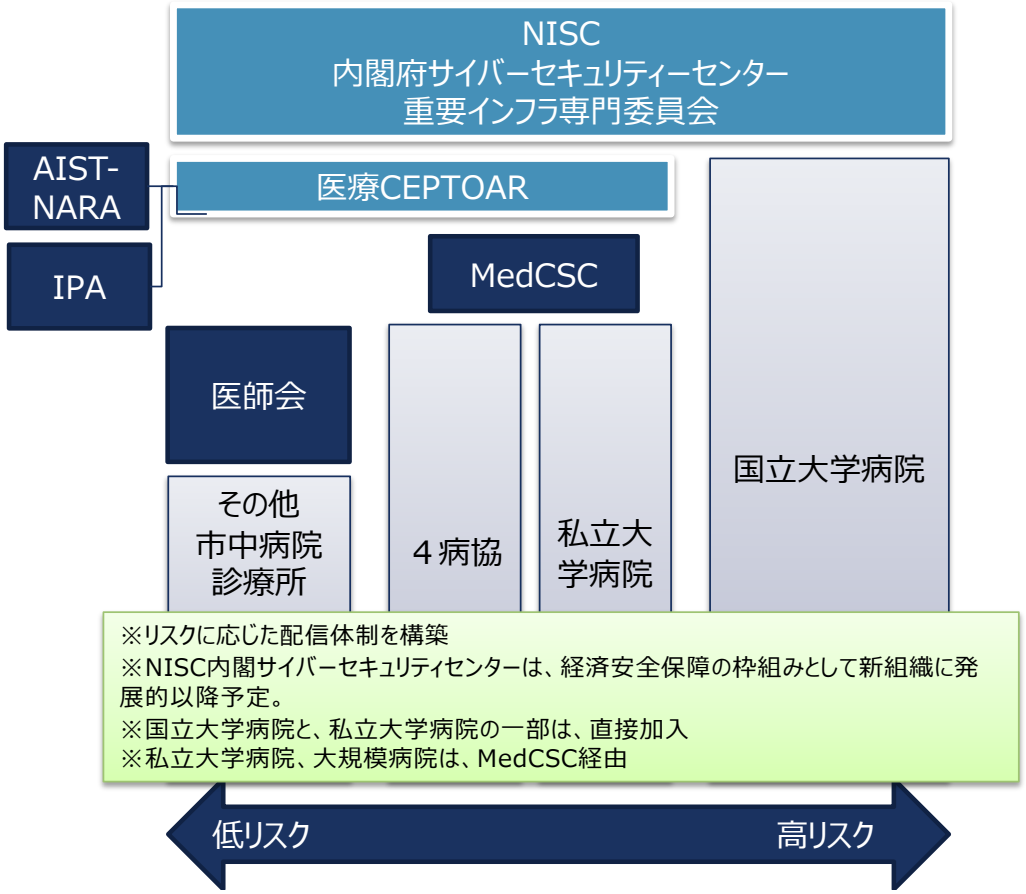
- インシデントレスポンス連携⇨**合同インシデント訓練**
- リスクコミュニケーション（脆弱性、SBOMやTII)⇨**情報交換ワークショップ、フラットなコミュニケーションの場**
- セキュリティアシュアランスツリー構築の協力⇨**共助、ベストプラクティス共有**

③適切な情報展開

現状、医療業界に対するサイバー情報は、NISCの医療CEPTAER
リスクに応じた情報展開が可能な体制を作る
リアクションモニターを行う

NISCからのサイバーセキュリティ関連情報提供のフローの改善

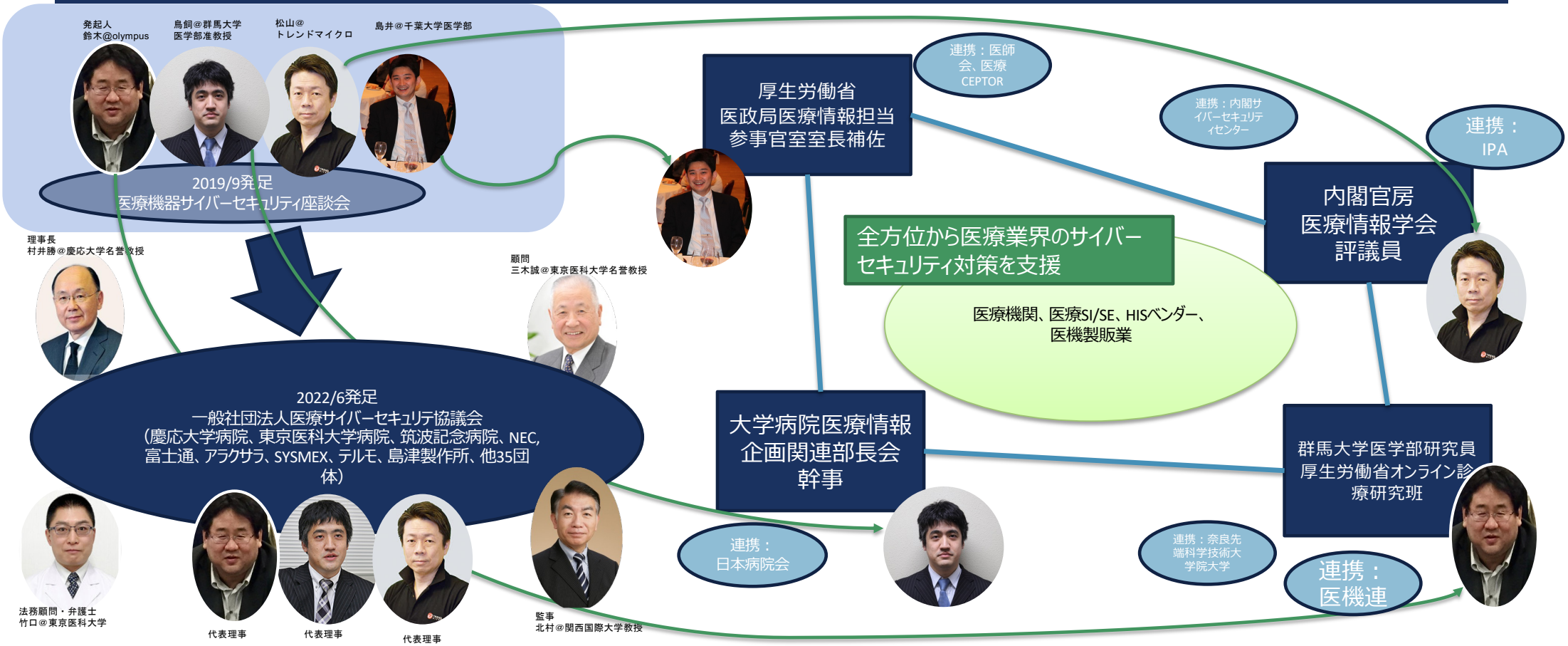




TLP:AMBER+STRICT

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

MedCSCの活動拡大



https://medcsc.org/