



医療ISAC セキュリティ民主化分科会



アジェンダ

1. 分科会概要
2. 年間活動スケジュール
3. 活動報告書イメージ
4. 想定課題と解決策案
5. セキュリティ民主化へのアプローチ
6. セキュリティ民主化構想

分科会概要

- ✓ 医療事業は重要インフラ事業に位置付けられておりサイバー攻撃による被害を受けると社会へ甚大な影響を及ぼすにも関わらず、医療機関のセキュリティ態勢は他業界と比較し十分に進められていません。
- ✓ 近年、規模の大きさに関わらず医療機関への攻撃は激化しており、加えて医療機関は医療情報連携ネットワークを通じて相互に接続されているため、医療業界全体のセキュリティを底上げしていくことが肝要です。
- ✓ そのためには一見、難解でかつ投資が高額で効果の見えにくいセキュリティを民主化し、全ての医療機関が高度なセキュリティを享受できる体制の検討等、意識と理解及び対策の底上げを図る活動を推進します

分科会名称	セキュリティ民主化分科会
活動内容	<ol style="list-style-type: none"> 1. 医療業界全体のセキュリティ体制強化 <ul style="list-style-type: none"> ✓ 現状の課題把握・仮説検証、施策立案、サービス企画 ✓ 概念実証とフィードバック・改善、既に提供されているサービスの把握と周知 2. サイバーセキュリティ教育・研修（MIST※、各業態で提供されているものも最大限活用） <ul style="list-style-type: none"> ✓ 経営層向け研修・訓練の企画・推進 ✓ 非IT人材向けの研修・訓練の企画・推進 3. 医療情報ベンダーや医療機器ベンダーを含めたサプライチェーンのセキュリティ強化 <ul style="list-style-type: none"> ✓ 取引先を含めたセキュリティ対策強化策の企画・推進
参加対象者	<p>セキュリティ対策に課題意識のある医療機関会員（一般診療所規模歓迎）、協力企業会員（医療情報ベンダー、医療機器ベンダー、セキュリティベンダー）、他 （協力企業会員の皆様においては、自社サービスの宣伝・販売目的ではなく、社会課題解決の主旨に賛同いただける企業のご参加を期待しております）</p>

※MIST:医療機関向けセキュリティ教育支援ポータル Medical Information Security Training <https://mist.mhlw.go.jp/>

年間活動スケジュール

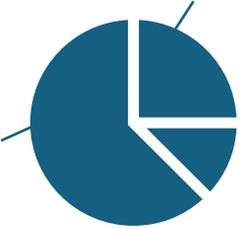
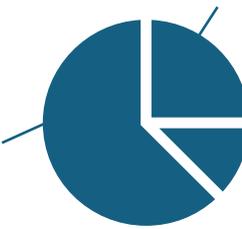
本日

		2025年										2026年		
		4	5	6	7	8	9	10	11	12	1	2	3	
マイルストーン		▼分科会概要説明					▼キックオフ	▼月次定例	▼月次定例	▼月次定例	▼月次定例	▼活動報告		
会員募集 セミナー・広報		会員募集												
		セミナー・広報企画					セミナー・広報企画							
立ち上げ準備		コアメンバー参加依頼												
分科会活動	1. セキュリティ体制強化	現状確認・アンケート					課題検証・分析				レポート作成	次年度企画		
	2. セキュリティ教育・研修						経営層教育企画				経営層教育コンテンツ開発			
	3. サプライチェーンのセキュリティ強化						委託先評価改善・分析				委託先評価の共通化・クラウド化検討			

活動報告書イメージ

- ✓ 2025年度の活動では、医療業界のセキュリティの現状課題および実施すべき施策を検証しレポートにまとめます。

活動報告書イメージ

調査内容	分科会参加者に対して、自身が所属する医療機関のセキュリティ上の課題と実施すべき施策を選択形式でアンケートを実施			
アンケート結果	<p>医療システムの課題</p> <p>25% : パスワードの使いまわし</p> <p>70% : 不十分な脆弱性管理</p> 	<p>人材の課題</p> <p>25% : 一般従業員のリテラシーの欠如</p> <p>70% : IT人材不足</p> 		
	<p>実施すべき施策</p>  <p>72% : セキュリティ啓発活動</p> <p>18% : 技術的対策の網羅</p>			

想定課題と解決策案

- ✓ 医療機関のサイバーセキュリティ態勢はサイバー攻撃の激化に伴い少しずつ進歩していますが、医療機関のサイバー攻撃による被害は高止まりしており、サイバー攻撃のリスクは依然として高い状況です。
- ✓ サイバーセキュリティのための予算・専門人材は不足しており十分な対策実現は難しいため、共助によりリソースを共有し業界全体で安価で効率的なセキュリティ態勢強化を実現し、規模を問わず医療提供に専念できる態勢整備を支援します。

想定課題	
1	規模によるセキュリティ体制の格差
2	サプライチェーン上のセキュリティホール
3	ボランティアによる取り組みの限界
4	医療機関へのサイバー攻撃の激化
5	医療機関ごとにセキュリティに係る規定・教育コンテンツを作成（標準化・共有化が劣後）
6	医療機関ごとにBCPを整備（業界全体でのサイバーBCPの欠如）
7	医療機関ではセキュリティ人材・予算が不足



解決策案

セキュリティの民主化

サイバーセキュリティ専門の共同組織を立ち上げ、リソースやサービスを共有し業界全体のセキュリティ態勢を強化する

セキュリティ民主化へのアプローチ

- ✓ 医療業界において、各医療機関とコンサル・セキュリティベンダー等が本分科会を通じてセキュリティ組織共同化の仮説検証を実施しサービスの共同化による効果を測定します。その結果を基に数社でセキュリティ組織を共同化し、その組織を共有することで医療業界全体のセキュリティの底上げを目指します。



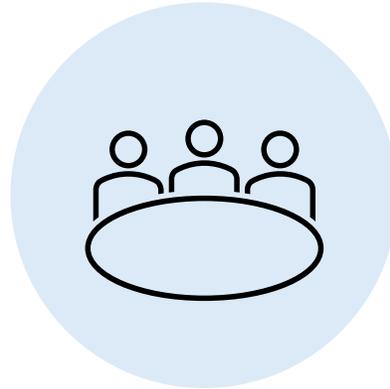
分科会立ち上げ

医療業界のセキュリティに課題を感じている方々を中心に分科会を立ち上げ



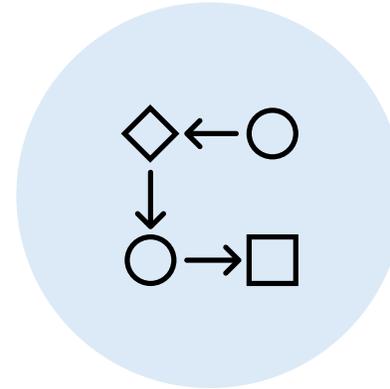
仮説検証

現状認識しているセキュリティの課題と解決案を医療機関とベンダーの両方の観点で検証を実施



スモールスタート

分科会の中で中心となる組織をいくつか対象に期間限定で共同組織を立ち上げて運用上の課題を抽出



検証・改善

スモールスタート時に抽出した課題を改善し、本番運用時のサービスメニューを確定、必要なリソースを算出し正式募集をかける



本番運用

セキュリティ組織を共同化（シェアードサービスの活用）し利用組織を医療業界全体へ拡大

本分科会による活動

共同組織へ引継ぎ

セキュリティ民主化構想

- ✓ サイバーセキュリティの共同組織を立ち上げて規定や各種社内報告資料、教育コンテンツ、訓練、各種セキュリティソリューションを共通化・シェアし、他業界における知見も活かし専門人材を共有することによりコストを低減し、「3ない」状態（人がいない、予算がない、知識がない）を解消しセキュリティが高められる仕組みを構築します。

