事業名	医療情報セキュリティ等対策経費

外部有識者のコメント

〇事業の課題や問題点

・医療機関へのサイバー攻撃への対応策として、１）階層別の研修及び初動対応支援、２）外部ネットワーク接続の俯瞰的把握及び安全性の検証・調査を行っている。
・リスクに備えるための重要な事業であるが、効果を検証するための適切なアウトカムが設定されていない。研修受講者数、セキュリティー対策の充実では、事業の効果が見えにくい。
・障害対応体制の整備は重要であり、本事業が自己点検の機会となりプラス面も多いが、中小規模の医療機関においては、医療情報システム安全管理責任者の配置が難しい状況もある。関心はあるが人員不足等により準備に時間を割くことができずに事業の活用を見送った例もある。

・サイバーセキュリティ対策調査事業において研修の受講者数がアウトカム、KPIとして設定されているが、受講者のターゲットを絞らず、漫然と受講者数を増やしても効果的とは言えないのではないか。
・セキュリティ安全責任者未配置の病院、サイバーセキュリティ確保事業の対象病院中辞退した病院こそ、リスクが大きいと思われ、この事業の中で、これらの病院を放置したままでよいのか。
・予算の執行率が低い。説明を聞いても十分と思われない。

・実際にインシデントが発生するかには偶発的な事象の影響が大きいためアウトカム指標として設定するのは困難である点は首肯できるが、問題の規模を正確に把握するためにも発生件数については適切に把握しておくべきである。
・セキュリティ対策・研修を進められるかについては病院側の事情も大きいことは事実だが、被害が発生した場合に想定される社会的問題の規模などを基準として効率的に対策が進められるよう、計画的に取り組むべきである。

・医療機関におけるサイバーセキュリティは非常に重要なテーマだが、資金面、人材・ノウハウの面で対応可能範囲が限定されている。各病院間の格差もあり、出来るだけその格差を埋め、安心出来る医療体制構築が必要である。

・サイバー攻撃によるダメージの代表的なものとして個人情報の漏洩と診療業務の滞りがあるとみられるが、後者は、周辺医療機関との連携が困難なへき地医療拠点病院等では、場合によって患者の生命等に差し障る事態となるおそれがある（資料01・５頁）。一方、医療情報システム安全管理責任者等は、とくに地方の医療機関において配置されない場合が相対的に多く（同８頁）、サイバー攻撃のダメージに対する脆弱性は、地方の医療機関にとって大きいとも考えられる。
・サイバーセキュリティ対策調査事業とサイバーセキュリティ確保事業は相互に連関させる方が良いように思われる。

・アウトカム指標が、本事業を行なっていくことで望む状況の達成に向けたマイルストーンになっていないと感じられる。昨年の執行率が46%と低い点についてその原因を把握し、本年以降の事業アクションの精査・どこにお金を使うかの再考が必要。

〇改善の手法や事業見直しの方向性

・事業成果を研修受講者数で成果を測ることが難しい。研修後にBCP策定に至った数を数値化し、研修の効果を測ることを検討できないか。研修内容の理解度、受講によるプラスの効果などの実態の把握ができるとよい。
・調査事業で行うリーダー育成の研修の成果が、確保事業の活用に生かせるとよい。
・規模や特性に応じたフォローができるとよい。現地調査の事前ヒアリングシートは詳細な内容になっていると想像するが（調査のための調査にならぬよう）、できるだけ簡略化して、システム担当者の負担を軽減し、活用しやすい事業となるよう改善を図る。
・現状では、医療機関におけるセキュリティ対策の公表は難しいとのことであるが、他の医療機関の好事例を知る機会にもなるため、検討を進めていただきたい。

・研修受講者数のみでなく、研修のターゲットを、まずはセキュリティ安全管理責任者に重点を置くべき。そのうえで、研修受講したセキュリティ安全管理者に院内での研修を義務付けてはどうか。
・300床以上の病院においてもセキュリティ安全管理責任者未設置の病院が20%以上、サイバーセキュリティ確保事業についても対象病院の30%程度が辞退という現況は深刻。かかる状況が生じている原因を確認のうえ、改善するための方策を検討してほしい。
・セキュリティ安全管理責任者未設置の病院については経営者層の研修に重点を置き、セキュリティ安全管理責任者を設置させるようすべきではないか。
・予算の積算を精緻に検討し、不要な予算は削減すべき。

・インシデントの発生について厚生労働省への報告を義務付ける、あるいは個人情報の漏洩が発生した場合に報告義務のある個人情報保護委員会との連携を取るなどの手段により被害発生を正確に把握することが求められる。

・サイバーセキュリティ研修に関して、受講人員が増えているのは良いことだが、実際に対応できる人材が増加しているかどうかが重要であり、そのレベルに達している人材を把握し、増加させることが重要。その人数をアウトカムに出来ないか。又、医療機関におけるサイバーセキュリティ事業について、現状を把握することがまず重要である。外部ネットワーク接続点を把握出来ている、その先の対応を行っている医療機関等ステージ管理を行い、それぞれのステージの医療機関を増加させる為の人員的なサポートを行うことが必要ではないか。それぞれのステージの医療機関数をアウトカムに出来ないか。

・研修受講者数に関する指標は、現状のものに加え、医療機関の機能別区分（同５頁）にもとづき、とりわけ脆弱性のみられる地方の医療機関を強化すべく設定するのも一案ではないかと考える。
・サイバーセキュリティ対策調査対策事業にスクリーニング機能をもたせ、研修で自機関のネットワークの全体像を把握できていない受講生を洗い出し、その所属する医療機関に、安全性の調査等を促す等、サイバーセキュリティ対策調査事業とサイバーセキュリティ確保事業を連関させてはどうか。

・研修の受講者数をKPIに置くだけでなく、研修を受けたことでこの事業の目的達成に向けてどのような効果があったのかがわかるアウトカムの設置があると良い。

〇その他（特筆すべき事項）

・階層別研修では、経営層にセキュリティ対策の重要性を理解してもらうよい機会になっている。セキュリティ対策にはどの程度行えば十分なのかの判断が難しい。経営者の判断材料として、安全レベルの提示があるとありがたいのではないか。
・IT系人材の人手不足は深刻で、視察先の病院でも採用に苦労しているという話を伺った。調査事業で行う研修を通じて、システム安全管理責任者になりうる人材の発掘ができるよう期待する。