とりまとめコメント

事業名　医療情報セキュリティ等対策経費

昨今、国内の医療機関を標的としたランサムウェアによるサイバー攻撃による被害が増加し、長期にわたり診療が停止した事例も複数発生している現状を踏まえると、関係者に対する各種研修の実施や、外部ネットワークとの接続の安全性の検証・検査、オフライン・バックアップ体制の整備など、医療機関のサイバーセキュリティ対策を充実させていくことは重要である。

そのためにも、まずはサイバー攻撃の現状をしっかりと把握する必要がある。関連のガイドラインの見直しなどにより、どの程度の数のインシデントが発生しているのかを的確に把握しておく必要がある。

各種の研修については、現在、受講者数総数をアウトカム指標としているが、経営層向けやシステム・セキュリティ管理者向けなど研修の種類が複数ある中で、ターゲットを細かく分けて受講者数を設定すべきである。特にシステム・セキュリティ管理者が重要となるので、その研修受講者数を把握していくことが重要である。また、例えば、研修後に受講者を講師とする院内研修を実施するなど、研修の効果がより広く浸透するような取組も検討すべきである。

研修受講者数の設定に際しては、この事業でどの程度の病院を対象にするかということを念頭に設定するほか、研修受講者の所属する病院数も指標として設定すべきである。

また、研修内容についても、最新の情報を取り入れつつ、各コースに相応しいものとするよう、不断の検証を行うべきである。

研修の効果については、例えば研修後にBCPの策定に至った施設数を把握するなど、一定の指標を設定することを検討すべきである。

外部ネットワークとの接続の安全性の検証・検査や、オフライン・バックアップ体制の整備については、医療機関のサイバーセキュリティを確保する観点から有効な取組であり、その状況を適切に把握するとともに、その進捗状況を指標として設定することが必要である。

これらの取組は、一斉に実施することが困難と思われるので、例えば、診療が停止した場合に地域医療に大きな影響が出る病院など、一定の優先順位を付けて取組を進めることも検討すべきである。

また、安全性の検証・検査の事前準備の負担や人員不足が原因で、検証・検査を辞退した医療機関があったことも踏まえ、事前準備の負担軽減や、研修受講者の活用など、医療機関が検証・検査を受けやすくするための方策も検討すべきである。

各種研修と医療機関に対する調査を関連させ、調査で判明した主な課題を研修内容に反映させるとともに、研修において自機関のネットワークの全体像の把握や安全性の調査を促すことを検討すべきである。

また、他の医療機関の参考となるよう、セキュリティ対策の好事例の積極的な収集・公表についても、検討するべきである。

本事業は重要な事業であるが、予算の執行率が低いことから、その原因を分析した上で、適切な予算規模となるよう精査を行うべきである。