

日本医師会サイバーセキュリティ支援制度の創設について

近年サイバー攻撃による被害は増加し、直近でも、医療機関を標的としたランサムウェア攻撃や Emotet をはじめとする標的型メール攻撃が多発化しており、地域の医療提供体制に影響を及ぼすケースも発生しております。そのため日本医師会ではサイバーセキュリティ支援制度を創設し、令和4年6月1日より運営を開始いたしました。

【制度の概要】

1. 制度の対象

日本医師会 A①会員 ※本制度のための新たな費用負担はございません。

2. 支援の内容

(1) 日本医師会サイバーセキュリティ対応相談窓口（緊急相談窓口）の設置（無料）

サイバーセキュリティに関連する日常の些細なセキュリティトラブルから重大トラブルまで幅広くご相談いただける相談窓口（年中無休・受付時間：9時～21時）を設置しました。本窓口は何度でもご利用が可能です。

(2) セキュリティ対策強化に向けた無料サイト（Tokio Cyber Port）の活用

東京海上日動火災保険株式会社が運営するサイバーセキュリティ情報発信ポータルサイト「Tokio Cyber Port」では、サイバーセキュリティに関する最新のニュースやコラム掲載、標的型攻撃メール訓練や各種マニュアル・テキストが提供されております。

(3) 日本医師会サイバー攻撃一時支援金・個人情報漏えい一時支援金制度

日本医師会 A①会員が開設・管理する医療機関において下記に該当する被害が発生した際に、初期対応を支援する費用として一時金をお支払いいたします。

（事由発生日：2022年6月1日以降）

① サイバー攻撃の被害を受けた場合

サイバー攻撃を受けた場合や、サイバー攻撃にて個人情報が漏えいした場合に初期対応を支援する費用として **10万円**のお支払い、加えてサイバー攻撃を受けた影響により、1日以上休業した場合には追加で **5万円**をお支払いします。一時支援金のお支払にあたっては、厚生労働省への届出を要件とします。

② サイバー攻撃に起因しない個人情報漏えいが発生した場合

初期対応を支援する費用として **5万円**をお支払いします。一時支援金の支払いにあたっては、個人情報保護委員会への再発防止策を講じた報告かつ、漏えいした本人へ通知することを要件とします。

※「(3)①サイバー攻撃の被害を受けた場合」につきましては、サイバー攻撃の影響で医療機関が1日以上休業した場合、追加の支援金をお支払いすることとしておりますが、休業の事実を確認するために、都道府県医師会または郡市区等医師会から休業証明書の発行を受けることを要件といたします。

※詳細につきましては【日本医師会メンバーズルーム内専用ページ】をご覧ください。

https://www.med.or.jp/japanese/members/info/cyber_shien.html