制度概要動画はこちら

医療機関を標的としたサイバー攻撃が多発する中、会員様をサポートする
日本医師会「サイバーセキュリティ支援制度」が始まっています。ぜひご活用ください。

その1 サイバーセキュリティ支援制度

サイバーセキュリティのご相談は、「サイ窓」にお電話を。

- ネットがつながらない
- セキュリティの診断をしてみたい
- パソコンが乗っ取られた
- サイバー攻撃を受けた

0120-179-066
年中無休 6時～21時／無料でご利用OK

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）

その2 サイバーセキュリティ支援制度

セキュリティ対策強化に向けた無料サイトをご活用ください。

Tokio Cyber Port powered by 東京海上日動

- サイバーセキュリティに関する最新記事の掲載
- 機関紙「Cyber Risk Journal」の提供
- 標的型攻撃メール訓練サービスのご提供
- 従業員実践テキストのご提供等

その3 サイバーセキュリティ支援制度

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

1. サイバー攻撃の被害を受けた場合 …10万円
   ①に加え、1日以上休業した場合は休業日数に応じて以下に記載の金額を追加でお支払いします。
   - 1日以上休業した場合 …10万円
   - 2日以上休業した場合 …20万円
   - 3日以上休業した場合 …30万円
2. サイバー攻撃に起因しない個人情報の漏洩が発生した場合 …5万円

サイバーセキュリティ支援制度について

【制度対象者】日本医師会A①会員

近年増加しているサイバー攻撃は今後もその傾向は続くと見込まれ、直近でも医療機関を標的としたランサムウェア攻撃※1 Emotet※2 をはじめとする標的型メール攻撃※3が多発化しています。医療提供体制に影響を及ぼすケースも発生していることから日本医師会としてもこの事態を深刻に受け止め、会員におけるサイバーセキュリティ対策の一助となるような基礎支援策から成る以下のサイバーセキュリティ支援制度を創設することとしました。

※1 マルウェア（コンピューターウイルスやスパイウェアなど、PCなどの端末に不利益をもたらす悪意のあるプログラムやソフトウェアの総称）の1種で、感染した端末は、保存されているデータが暗号化されて使用できない状態になってしまいます。そのデータを元に戻す対価や窃取した情報を漏洩しない対価として、身代金を要求されるケースが多いです。　※2 非常に高い感染力・拡散力を持つマルウェアの1種で、感染した端末内のメール情報（送受信者のアドレスや本文内容）が窃取されてしまいます。窃取された情報により、発信元などを偽装したEmotet付メールがばら撒かることで、さらに感染が拡大します。　※3 対象の組織から重要な情報を盗むことなどを目的として、知り合いや取引先のふりをして送られてくるメールで、Emotetなどのマルウェアが添付されていたり、有害なサイトに誘導するような内容になっています。

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）

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を設置しています。本窓口は無料で何度でもご利用いただけます。

1次対応

ネット接続の不具合やウイルス感染等の日常診療業務におけるトラブルに対して、初期のアドバイスやウイルス駆除、セキュリティ診断のリモートサポート等を行います。

●ご連絡先

0120-179-066

年中無休 6時~21時 ／無料で何度でもご利用可能です

2次対応

不正アクセスや情報漏えい等の高度な専門性を要する重大なトラブルに対して、より専門的な観点でのアドバイスを実施いたします。また会員様の要望に応じた専門事業者（フォレンジック事業者※、弁護士）のご紹介を行います。

※フォレンジック事業者とは、セキュリティ事故発生時に原因究明などのために、コンピュータに残された証拠を調査する専門事業者のことを指します。

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

サイバー攻撃の被害に遭わないためには、日頃からのサイバー攻撃に対する意識の向上や予防が非常に重要となります。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、本サービスの活用を推奨しています。

利用方法

下記URLまたは二次元コードからアクセスのうえ、会員登録いただくことでどなたでも無料でご利用いただけます。

Tokio Cyber Port　※一部サービスは有償となります。

https://tokiocyberport.tokiomarine-nichido.co.jp/-cybersecurity/s/

サービス提供内容例

- サイバーセキュリティに関する最新記事の掲載
- 機関紙「Cyber Risk Journal」の提供
- 標的型攻撃メール訓練サービスのご提供
- 従業員実践テキストのご提供等

各サービスの詳細等は左記URLへアクセスのうえご確認ください。

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・管理する医療機関および介護サービス施設・事業所において、サイバー攻撃の被害を受けた場合、もしくは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一時金をお支払いします。

①サイバー攻撃の被害を受けた場合のお支払い金額

●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…**10万円**をお支払いします。

●サイバー攻撃を受けた影響により、1日以上休業※1した場合…**休業した日数×10万円（最大30万円）**※2を追加でお支払いします。

一時支援金のお支払にあたっては、厚生労働省への届出もしくは日本医師会への届出を要件とします。

※1 休業の定義についてサイバー攻撃を受けたことにより、新規患者（初診料の算定対象）の診察業務を一切停止した場合も「休業」として補償対象とします（再診等その他の診察を実施していても休業と見なします）。
※2 事由発生日が2023年6月1日以降の場合の金額です。事由発生日が2022年6月1日~2023年5月31日の場合は一律5万円をお支払いします。

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のお支払い金額

●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。

※上記①、②ともに内部犯罪に起因した案件はお支払いの対象外となります。
※本制度の詳細は、メンバーズルーム内に掲載しておりますのでご確認ください。
なお、アクセスには日医会員専用ユーザーID、パスワードが必要です。

4 医療情報システム安全管理ガイドライン第6.0版に関するご支援策

医療情報システム安全管理ガイドライン第6.0版（含む立入検査対応）における独自の解説資料・動画等の公開および相談窓口を設置する予定です（令和5年10月以降予定）。詳細につきましては別途ご案内いたしますので、今しばらくお待ちください。

このご案内は概要の説明となります。詳しい内容については下記をご確認ください。

本制度の詳細について
日本医師会ホームページおよびメンバーズルームをご覧ください。

https://www.med.or.jp/doctor/sys/cybersecurity/001566.html

本制度全般に関するお問合せ先

日本医師会情報システム課

TEL 03-3942-6135　FAX 03-3946-6295

MAIL josys@po.med.or.jp