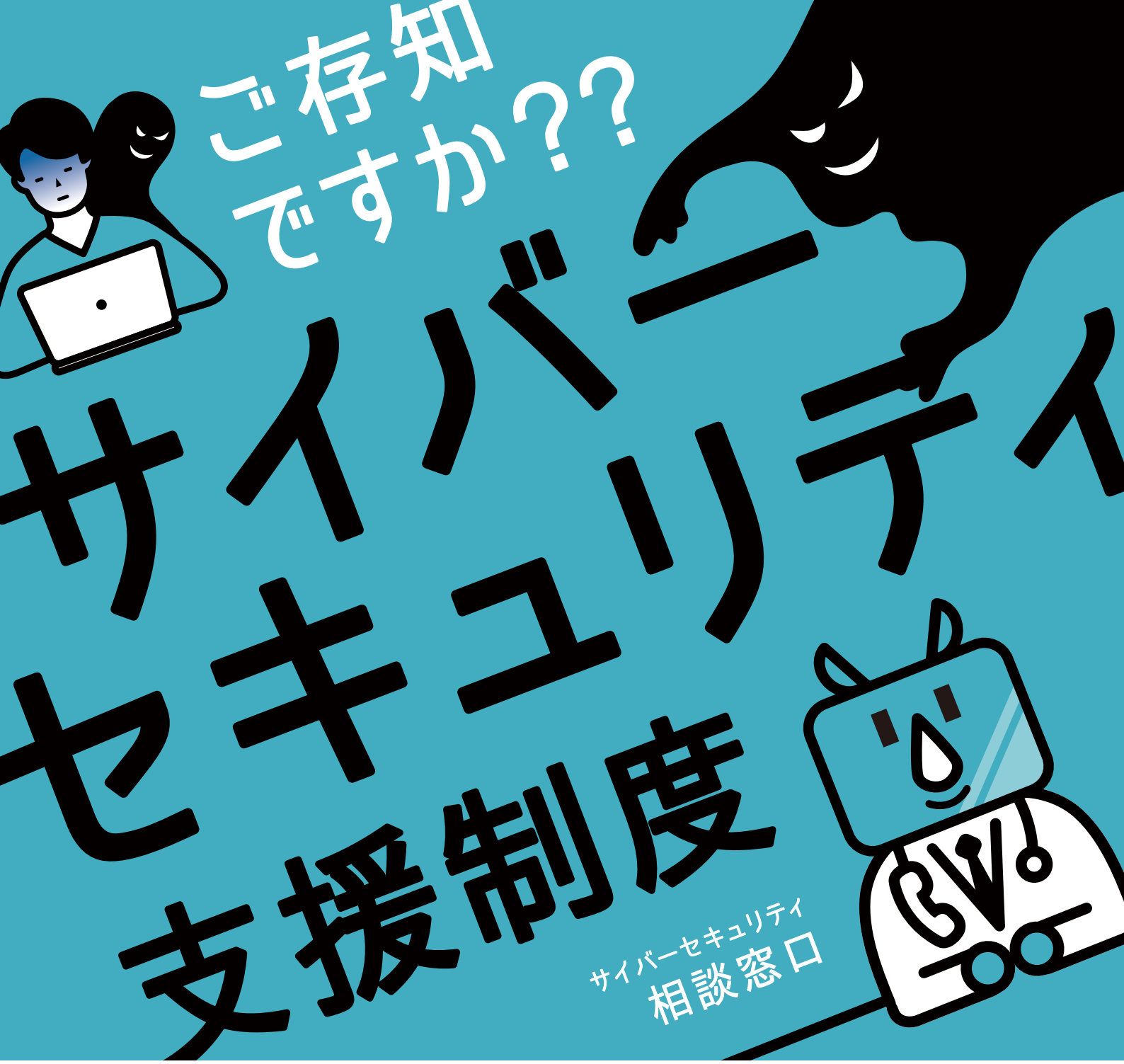

制度概要動画はこちら

医療機関等を標的としたサイバー攻撃や求められるセキュリティ対策について、
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」を、ぜひご活用ください。

その1

セキュリティトラブルのご相談は、「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

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

❶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

その4

「医療情報システムの安全管理に関するガイドライン」・「サイバーセキュリティ対策チェックリスト」に関するご支援策

1. 日本医師会セキュリティガイドライン相談窓口
   - 付随するセキュリティ対策の相談も可!

0120-339-199
平日9時~18時／無料でご利用OK

2. サイバーセキュリティ対策チェックリストの実践ガイド・セミナー動画提供
   - 今後対応が必要なセキュリティ対策や立入検査の備えに!

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Emotetをはじめとする標的型メール攻撃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 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）**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）。

こんなときに！ ①サイバー攻撃の被害事例

- ランサムウェア攻撃を受け、サーバーがダウンした
- ホームページに不正アクセスされ、内容を改ざんされた
- 偽の警告画面に記載された業者の電話番号に連絡し、リモート操作されてしまった

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。

こんなときに！ ②サイバー攻撃に起因しない個人情報漏えいの被害事例

- FAXの誤送信により患者の個人情報を漏えいしてしまった
- カルテを待合室に置き忘れ、別の患者が見てしまった
- 個人情報が含まれるUSBを紛失してしまった

4 「医療情報システムの安全管理に関するガイドライン」・「サイバーセキュリティ対策チェックリスト」に関するご支援策

① 日本医師会セキュリティガイドライン相談窓口

厚生労働省が策定している「医療情報システムの安全管理に関するガイドライン第6.0版」および「医療機関におけるサイバーセキュリティ対策チェックリスト」に関するご相談やそれらに付随するセキュリティ対策に関す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。

●窓口運営時間 平日9時～18時（土日、祝日、年末年始は休業） ●ご連絡先 TEL：0120-339-199

② 医療機関におけるサイバーセキュリティ対策チェックリストの実践ガイドおよびセミナー動画の提供

厚生労働省が策定している「医療機関におけるサイバーセキュリティ対策チェックリスト」について、医療機関等の皆様がチェックリストを用いた確認を効率的に実施いただくための解説資料・動画を無料で提供いたします。本資料・動画をご活用いただき、チェックリストで求められている項目を中心とした今後のセキュリティ対策および立入検査対策にもご活用ください。ご不明点やお困りごとがあれば、上記①「日本医師会セキュリティガイドライン相談窓口」へお問い合わせください。
※本資料・動画は、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。

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