



日本医師会 サイバーセキュリティ支援制度概要 および利用マニュアル

公益社団法人 日本医師会

2024年1月31日 改定

目次

1. サイバーセキュリティ支援制度の概要
2. サイバーセキュリティ支援制度の具体的な内容
3. 本制度に関するQ&A

1. サイバーセキュリティ支援制度の概要

1. サイバーセキュリティ支援制度の概要

1-1 制度創設の背景

近年サイバー攻撃による被害は増加し、今後もその傾向は続く見込まれています。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、医療提供体制に影響を及ぼすケースも発生しています。日本医師会としてもこの事態を深刻に受け止め、対応策を検討した結果、会員様の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サイバーセキュリティ支援制度を創設することといたしました。

(*)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。

(**)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れることで、さらに感染が拡大します。

(***)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。

1-2 制度の対象

日本医師会A①会員

1-3 制度の概要

下記5つの支援策で構成されています。各項目の詳細については次ページ以降を参照ください。

- 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）
- 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
- 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
- ④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
- ⑤日本医師会セキュリティガイドライン相談窓口

2. サイバーセキュリティ支援制度の具体的な内容

2. サイバーセキュリティ支援制度の具体的な内容

2-1 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いたします。本窓口は無料で何度でもご利用いただけます。

(1) 具体的なサービスご提供内容

■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。

■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) 窓口運営時間

年中無休 6時～21時

(3) ご連絡先

TEL : 0120-179-066

(4) 費用

無料（何度でもご利用可能です）

2. サイバーセキュリティ支援制度の具体的な内容

2-1 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）

（5）利用時の注意点等

- 相談窓口のご利用時には、電話口で日本医師会A①会員が開設・管理する医療機関または介護サービス施設・事業所であることを確認させていただきます。具体的には、A①会員名、医療機関名または介護サービス施設・事業所名、所在地、医籍番号（6桁）もしくは会員番号（10桁）を確認いたしますので、これらが分かるものをご用意のうえご連絡ください。
- A①会員本人に加え、職員の方からのお問合せも可能です。
- 都道府県医師会、郡市区等医師会の事務局の方からのお問合せも可能です。

2. サイバーセキュリティ支援制度の具体的な内容

2-2 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。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、日本医師会としても本サービスの活用を推奨します。

(1) 利用方法

下記URLよりもしくはQRコードよりアクセスのうえ、会員登録いただくことでどなたでもご利用いただけます。

<URL>

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



(2) サービス運営会社

東京海上日動火災保険株式会社

(3) 費用

無料（一部サービスは有償となります）

(4) サービス提供内容（一例）

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上記（1）のURLへアクセスのうえご確認ください。

2. サイバーセキュリティ支援制度の具体的な内容

2-3 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

日本医師会 A ①会員が開設・管理する医療機関または介護サービス施設・事業所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(*)）
本制度の詳細につきましては、制度規程（別紙）をご参照ください。

(*)以下の内容は事由発生日が2023年6月1日以降の場合となります。事由発生日が2022年6月1日～2023年5月31日までの場合は、P26(4-17)をご参照ください。

(1) お支払いする金額について

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10万円をお支払いします。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休業日数1日につき10万円（最大3日30万円限度）をお支払いします。

一時支援金のお支払にあたっては、厚生労働省または日本医師会への届出を要件とします。（詳細はP26(4-18)をご確認ください。）

(*) 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。

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。

2. サイバーセキュリティ支援制度の具体的な内容

2-3 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

(2) 支援金のご請求方法

一時支援金をご請求いただく際には、下記書類をご準備のうえ次頁(3)記載の事務局へご送付をお願いします。各資料のサンプルは別添資料をご参照ください。

【ご提出書類】

①サイバー攻撃を受けた場合

- ・厚生労働省への報告書の写または日本医師会への報告書
- ・サイバー攻撃一時支援金・個人情報漏えい一時支援金給付申請兼振込依頼書
- ・都道府県医師会もしくは郡市区等医師会作成の休業証明書（休業した場合のみ）

②サイバー攻撃によらない個人情報漏えいの場合

- ・個人情報保護委員会へ提出した報告資料の写
- ・サイバー攻撃一時支援金・個人情報漏えい一時支援金給付申請兼振込依頼書

(3) 請求回数について

1 医療機関または1介護サービス施設・事業所あたり年間1回までかついずれか一方のみのご請求となります。

サイバー攻撃一時支援金と個人情報漏えい一時支援金は重ねてお支払いいたしません。

(4) 各種書類の送付先

〒980-8799

日本郵便株式会社 仙台中央郵便局留め

日本医師会 サイバー攻撃一時支援金事務局 宛

* 送料は会員様にてご負担のうえ、上記送付先へ郵送願います。

2. サイバーセキュリティ支援制度の具体的な内容

2-3 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

(5) 支援金のお支払いスケジュール

支援金のお振込みスケジュールは以下の通りとなります。お支払いに必要な全ての書類が到着し、内容に問題ないことを確認のうえ、お振込みをさせていただきます。

- ①毎月1日～15日までに到着：当月末までに事務局お振込み手続き完了
- ②毎月16日～末日までに到着：翌月15日までに事務局お振込み手続き完了
- * 休日等によりご指定口座への着金日が月初や16日以降になる場合があります。

(6) お問い合わせ先

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事務局

TEL：0120-411-250

Mail：jma-cyber@qag.jp

運営時間：平日9時～18時（土日、祝日、年末年始は休業）

* メールでのお問い合わせの際は、件名を以下にしてくださいようお願いします。

メール件名：【日本医師会】【会員様名(医療機関名または介護サービス施設・事業所名)】一時支援金手続き希望

2. サイバーセキュリティ支援制度の具体的な内容

2-4 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

医療機関へのサイバー攻撃が相次ぐ状況を受け、2023年5月末、厚生労働省により「医療情報システムの安全管理に関するガイドライン」が第6.0版に改定されました。本改定に合わせて、「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」が作成され、医療機関が優先的に取り組むべき事項がまとめられています。また、医療機関において医療法に基づく立入検査の際には、本チェックリストを用いて、医療機関のセキュリティ対策状況の確認が行われます。このような背景により、日本医師会としても会員様のセキュリティ対策および立入検査対策の一助となるよう具体的な対応方法を示した実践ガイドおよびセミナー動画を作成いたしました。

(1) 実践ガイドおよびセミナー動画の掲載先

日本医師会サイバーセキュリティ支援制度（会員限定メンバーズルーム）

* アクセスするには日医会員用ユーザID、パスワードが必要です。

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



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

公益社団法人 日本医師会
2023年12月21日発行

はじめに

医療機関の経営者の皆様へ

医療機関等に対するサイバー攻撃は年々増加傾向にあり、その脅威が深刻化しています。医療機関等がサイバー攻撃の被害を受けると、医療提供体制の継続が困難となるばかりでなく、患者や医療従事者の健康、財産等に関する被害が生じ、その被害は計り知れないに及ぶ可能性があります。医療機関等の設備が医療情報システムに対してサイバーセキュリティ対策を講ずることによって、多発する**サイバー攻撃の被害の発生可能性を低減**できることが、これら一連の**トラブルから医療を守る**という大きなメリットがあります。

医療機関の設備がサイバーセキュリティ対策に適切に組み立てられ、万が一の被害を未然に防ぎ、患者や医療従事者の健康や財産の被害を防ぐことが、医療機関の経営者の責務です。本実践ガイドは、医療機関の経営者の方々に、サイバーセキュリティ対策の重要性を伝えるとともに、具体的な対策の方向性を示すことを目的としています。

ガイドライン及びチェックリストは、医療情報システムを安全に管理していくために必要な事項が記載されています。本実践ガイドは、本チェックリストを用いて、医療機関の設備の**サイバーセキュリティ対策の現状を確認**することができます。

本実践ガイドは、医療機関の経営者の方々に、サイバーセキュリティ対策の重要性を伝えるとともに、具体的な対策の方向性を示すことを目的としています。本実践ガイドは、医療機関の経営者の方々に、サイバーセキュリティ対策の重要性を伝えるとともに、具体的な対策の方向性を示すことを目的としています。

厚生労働省が作成した「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」もご参照の上、本実践ガイドに活用ください。



目次

サイバーセキュリティ対策チェック！

すべての項目に ☒ は付きますか？

5	1. 今和5年度中に達成できるように優先的に取り組みましょう	13-14
6	2. 今和6年度中に達成できるように取り組みましょう	15-16
7	3. 実践ガイドの使い方	17-18
8	4. 医療情報システムの管理・運用	19-26
9	5. インシデント発生に備えた対応	27-36
10	6. FAQ	37-39
11	7. 謝辞	40-45
12	8. 付録	46-53

* 立ち入り検査の際は、この冊子ではなく、医療機関の設備に設置したチェックリスト42Aのシリアル番号が記載された表紙が必要です。

(2) 費用 無料

2. サイバーセキュリティ支援制度の具体的な内容

2-5 日本医師会セキュリティガイドライン相談窓口（2023年10月31日～）

2023年5月末に改定された厚生労働省の「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」、本改定に合わせて作成された「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」およびそれら付随するセキュリティ対策に関する相談窓口を設置いたします。本窓口は無料で何度でもご利用いただけます。

(1) 具体的なサービスご提供内容

厚生労働省の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、日本医師会の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、それに付随するセキュリティ対策に関するご相談に対応します。

(2) 窓口運営時間

平日9時～18時（土日、祝日、年末年始は休業）

(3) ご連絡先

TEL：0120-339-199

(4) 費用

無料（何度でもご利用可能です）

(5) 利用時の注意点等

- 相談窓口のご利用時には、電話口で日本医師会A①会員が開設・管理する医療機関または介護サービス施設・事業所であることを確認させていただきます。具体的には、A①会員名、医療機関名または介護サービス施設・事業所名、所在地、医籍番号（6桁）もしくは会員番号（10桁）を確認いたしますので、これらが分かるものをご用意のうえご連絡ください。
- A①会員本人に加え、職員の方からのお問合せも可能です。
- 都道府県医師会、郡市区等医師会の事務局の方からのお問合せも可能です。

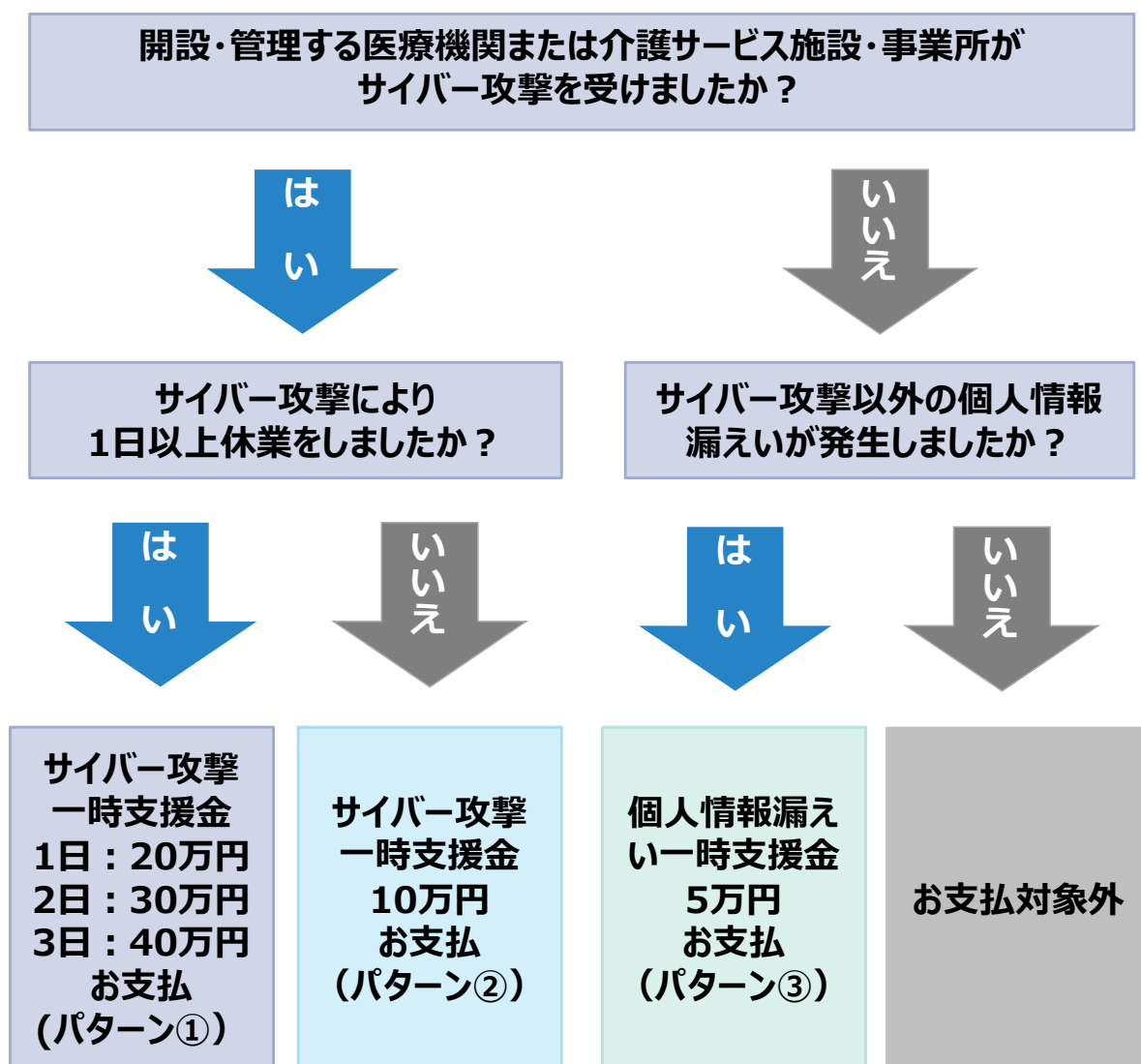
2. サイバーセキュリティ支援制度の具体的な内容

2-6 サイバーセキュリティー制度の変更点（2023年6月1日～）

2022年6月1日に創設した本制度は、2023年6月1日以降、順次以下の改定を行い、支援内容をさらに拡充しております。

No	対象の支援策	項目	2022年6月1日 ～2023年5月31日	2023年6月1日～
①	サイバーセキュリティ対応 相談窓口 (緊急電話相談窓口)	相談窓口の開局時間	9時～21時	6時～21時
②	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	サイバー攻撃一時支援金 のお支払要件	厚生労働省への報告	厚生労働省への報告もしくは 日本医師会への報告
③		一時支援金の対象施設	A①会員が開設・管理する 医療機関	A①会員が開設・管理する 医療機関または 介護サービス施設・事業所
④		サイバー攻撃一時支援金 (休業)のお支払額	1日以上休診：5万円	1日以上休診:10万円 2日以上休診:20万円 3日以上休診:30万円
⑤	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ご提供	実践ガイドや セミナー動画の提供	—	実践ガイド：2023年12月より、 セミナー動画：2024年1月より ご提供開始
⑥	日本医師会セキュリティガイドライン 相談窓口	ガイドラインに関する 相談窓口の設置	—	2023年10月31日より新設

一時支援金対象可否フローチャート



各種一時支援金のお支払いの要件、提出書類等についてはP9～P11をご参照ください。

一時金ご請求時の流れについて

サイバー攻撃 一時支援金

1日：20万円
2日：30万円
3日：40万円
お支払
(パターン①)

①サイバー攻撃の被害内容につき、所定の書式にて厚生労働省へ報告書を提出するまたは日本医師会宛の報告書を作成する
※日本医師会宛の場合は事前の提出は不要です

②1日以上休業した場合、都道府県医師会もしくは
郡市区等医師会へ休業証明書の作成を依頼する

③申請書兼振込依頼書を記入のうえ、
厚生労働省への報告書または日本医師会への報告書
と休業証明書とともに事務局へ郵送

サイバー攻撃 一時支援金 10万円 お支払 (パターン②)

①サイバー攻撃の被害内容につき、所定の書式にて厚生労働省へ報告書を提出するまたは日本医師会宛の報告書を作成する
※日本医師会宛の場合は事前の提出は不要です

②申請書兼振込依頼書を記入のうえ、厚生労働省への
報告書または日本医師会への報告書とともに事務局へ郵送

個人情報漏えい 一時支援金 5万円 お支払 (パターン③)

①個人情報保護委員会ホームページへアクセスし、
発生した事案の内容を専用フォームに入力し速報を行う。
(確報のために、報告内容をCSVファイルで保存する)

②上記①と同様の流れで、再発防止策の記入と、
漏えいした方本人への対応状況を記入した確報を行う。
確報の提出前にPDFファイルの出力を必ず行う。

③出力したPDFファイルを印刷し、
手書きで日付を追記する。

④申請書兼振込依頼書を記入のうえ、日付を追記した
個人情報保護委員会の報告書控とともに事務局へ郵送

3. 本制度に関するQ&A

3. 本制度に関するQ&A

目次

1. 制度全般

- 1-1 A①会員以外も所定の手続きをすれば、本制度を利用することはできますか。
- 1-2 日本医師会を退会した場合や、A①会員以外に会員区分を異動した場合、継続して本制度を利用することはできますか。
- 1-3 日本医師会にA①会員として入会した場合や、A①会員に会員区分を異動した場合、いつから本制度を利用することができますか。
- 1-4 2023年6月1日前後の変更点を教えてください。
- 1-5 本制度の利用に費用は発生しますか。

2. 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）

- 2-1 PC等の使い方やセットアップ等、PC操作に関する問い合わせも可能ですか。
- 2-2 電話以外にメール等での相談は可能ですか。
- 2-3 リモートサポートはどのように行うのでしょうか？
- 2-4 相談窓口で紹介された専門事業者に業務を依頼する場合の費用は自己負担ですか。
- 2-5 相談した内容は日本医師会に共有されますか。

3. 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

- 3-1 利用登録せずに利用する方法はありますか。（利用登録は必須ですか。）
- 3-2 利用登録を一括して日本医師会側で対応することはできますか。

3. 本制度に関するQ&A

目次

- 4. 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
 - 4-1 サイバー攻撃被害を厚生労働省へ届出した際の資料は何を用意すればいいですか。
 - 4-2 受け取った支援金の使途は決められていますか。
 - 4-3 支援金が振込まれた後に何か通知や連絡はきますか。
 - 4-4 保険会社が販売するサイバー攻撃用の保険との違いはありますか。
 - 4-5 サイバー攻撃一時支援金と個人情報漏えい一時支援金を両方受け取ることはできますか。
 - 4-6 サイバー攻撃一時支援金の支払い対象となる事例を教えてください。
 - 4-7 迷惑メールを受け取っただけでも厚生労働省へ届出すれば、サイバー攻撃一時支援金は受け取れますか。
 - 4-8 職員が個人情報記載された書類が入っているカバンを紛失した場合でも、個人情報漏えい一時支援金を受け取れますか。
 - 4-9 サイバー攻撃による休業証明書はどのように手配したらいいですか。
 - 4-10 サイバー攻撃を受けた報告書はどこまで記入する必要がありますか？
 - 4-11 個人情報保護委員会への提出資料はどこまで記入する必要がありますか？
 - 4-12 サイバー攻撃を受けた報告書を厚生労働省へ提出する際の送付先はどちらになりますか？
 - 4-13 個人情報保護委員会へ報告した内容を入手するにはどうしたらいいですか？
 - 4-14 受け取った一時支援金の税務処理について教えてください。
 - 4-15 一時金の申請期限はありますか？
 - 4-16 1年に1回の請求までとなっていますが、1年間とはいつからいつまででしょうか？
 - 4-17 サイバー攻撃を受けて1日以上休業した場合で、事由発生日が2023年5月31日以前の場合はいくら一時支援金が支払われますか？
 - 4-18 サイバー攻撃を受け一時金を申請する場合、厚生労働省へ報告書の提出は必須ですか。

3. 本制度に関するQ&A

目次

- 5. 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
 - 5-1 厚生労働省作成の「医療情報システムの安全管理に関するガイドライン」および「医療機関等におけるサイバーセキュリティ対策チェックリスト」の掲載場所はどこですか。
 - 5-2 厚生労働省作成の「医療機関等におけるサイバーセキュリティ対策チェックリスト」と日本医師会の「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」の違いは何ですか。
- 6. 日本医師会セキュリティガイドライン相談窓口
 - 6-1 厚生労働省の「医療情報システムの安全管理に関するガイドライン」を見ましたが、何から手を付けてよいかわかりません。このような場合も相談は可能ですか。
 - 6-2 電話以外にメール等での相談は可能ですか。
 - 6-3 相談窓口で紹介された専門事業者に業務を依頼する場合の費用は自己負担ですか。
 - 6-5 相談した内容は日本医師会に共有されますか。

3. 本制度に関するQ&A

1. 制度全般

1-1 A①会員以外も所定の手続きをすれば、本制度を利用することはできますか。

ご利用いただけません。

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）および、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はA①会員のみの制度となります。

尚、東京海上日動火災保険株式会社が運営する「Tokio Cyber Port」については、どなたでも会員登録すれば利用可能です。

1-2 日本医師会を退会した場合や、A①会員以外に会員区分を異動した場合、継続して本制度を利用することはできますか。

A①会員だった方が退会された場合は、退会年月日以降、A①会員からそれ以外の会員区分に異動した場合には、異動年月日以降は本制度を利用することはできません。

1-3 日本医師会にA①会員として入会した場合や、A①会員に会員区分を異動した場合、いつから本制度を利用することができますか。

入会の場合は、日本医師会への入会年月日から、A①会員への会員区分異動の場合は、異動年月日からご利用いただけます。

なお、日本医師会への入会手続きや異動手続きは、ご地元の郡市区等医師会、都道府県医師会それぞれの入会手続きを経たうえで行われるため、ご地元の郡市区等医師会に申請いただいてから手続き完了まで2～3カ月かかります。完了までの間であってもご利用いただくことができますが、手続き中である旨をご地元の医師会に確認させていただく場合があります。

1-4 2023年6月1日前後の変更点を教えてください。

P14をご確認ください。

1-5 本制度の利用に費用は発生しますか。

各制度のご利用に伴う費用は発生しません。ただし、サイバーセキュリティ対応相談窓口（緊急相談窓口）では、会員様のご要望において専門事業者をご紹介した場合で会員様と事業者との間でサービス委託料等が発生した場合は、全額会員様ご自身のご負担となります。

また、セキュリティ対策強化に向けた無料サイト（Tokio Cyber Port）につきましても、一部有償サービスがございます。

3. 本制度に関するQ&A

2. 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）

2-1 PC等の使い方やセットアップ等、PC操作に関する問い合わせも可能ですか。

一般的なPCの操作に関する問い合わせには対応しておりません。

また、相談窓口にて初期対応実施時にサイバー攻撃とは関係ない通信障害等であることが確認できた場合には、PCメーカーや通信事業者へのご連絡をご案内させていただきます。

2-2 電話以外にメール等での相談は可能ですか。

お電話のみでの対応となります。

2-3 リモートサポートはどのように行うのでしょうか？

相談窓口よりリモートサポートに必要な情報をお伝えし、オペレータが会員様と同じ画面を見ながらサポートを行います。

2-4 相談窓口で紹介された専門事業者に業務を依頼する場合の費用は自己負担ですか。

会員様ご自身で負担いただく形になります。

別途、ご自身でサイバー攻撃に対応する保険に加入されている場合には、そちらの保険で費用負担できる可能性がありますので、加入保険会社等にお問い合わせください。

2-5 相談した内容は日本医師会に共有されますか。

今後のサービス向上を目的に定期的に日本医師会に共有されます。

3. 本制度に関するQ&A

3. 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

3-1 利用登録せずに利用する方法はありますか。（利用登録は必須ですか。）

利用登録は必須ではなく、一部コンテンツは利用登録なしでも確認できますが、全てのコンテンツを利用するには利用登録が必要になります。ぜひ積極的にご登録いただき、今後のさらなるサイバーセキュリティ対策に関する意識向上や対策強化にお役立てください。

3-2 利用登録を一括して日本医師会側で対応することはできますか。

できません。

利用登録時にメールアドレス等の入力が必要となるため、会員様ご自身で利用登録いただく必要があります。

3. 本制度に関するQ&A

4. 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

4-1 サイバー攻撃被害を厚生労働省へ報告・届出した際の資料は何を用意すればいいですか。
厚生労働省へ電話にて報告・届出した場合には、別添資料「サイバー攻撃被害に関する厚生労働省への報告内容」を記入のうえご提出ください。

また、厚生労働省へメールで報告した場合には、当該メールを印刷したものを提出願います。

4-2 受け取った支援金の使途は決められていますか。

特に決められておりませんので、会員様のご判断で使途を決定ください。

4-3 支援金が振込まれた後に何か通知や連絡はきますか。

申請書にチェックを入れていただいた方法（電話もしくはメール）にてご連絡をいたします。

4-4 保険会社が販売するサイバー攻撃用の保険との違いはありますか。

保険会社にて販売している保険は、サイバー攻撃を受けた際に係る費用実費を補償する商品と理解をしています。（詳細は各保険会社にご確認ください）

本制度は、サイバー攻撃を受けた際に初期対応を支援する目的で、定額の一時金をお支払いするものになります。

4-5 サイバー攻撃一時支援金と個人情報漏えい一時支援金を両方受け取ることはできますか。

両方受け取ることはできません。

サイバー攻撃により個人情報が漏えいした場合は、サイバー攻撃一時支援金10万円をお支払いいたします。

4-6 サイバー攻撃一時支援金の支払い対象となる事例を教えてください。

以下のような事例がお支払いの対象となります。判断に迷われた場合は事務局までご連絡ください。

- ・メールに添付されていた添付ファイルを開いてしまい、Emotet等に感染した
- ・不正アクセス等によりホームページが改ざんされた。
- ・マルウェアに感染、電子カルテが使用できなくなった。

4-7 迷惑メールを受け取っただけでも厚生労働省へ届出すれば、サイバー攻撃一時支援金は受け取れますか。

迷惑メールの受信だけでは、サイバー攻撃を受けたかは判断できませんので、厚生労働省への報告・届出を行っても一時支援金を受け取ることはできません。

3. 本制度に関するQ&A

4. 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

4-8 職員が個人情報が記載された書類が入っているカバンを紛失した場合でも、個人情報漏えい一時支援金を受け取れますか。

個人情報保護委員会へ再発防止策を作成した報告書の提出と、漏えいした方本人への通知が確認できればお受け取り可能です。

4-9 サイバー攻撃による休業証明書はどのように手配したらいいですか。

別添資料「サイバー攻撃による休業証明書」に必要事項を記入のうえ、都道府県医師会もしくは郡市区等医師会の捺印を取り付け下さい。

4-10 サイバー攻撃を受けた報告書はどこまで記入する必要がありますか？

全ての項目について可能な限り詳細に記入のうえ、厚生労働省または日本医師会へご提出をお願いします。厚生労働省へ提出を行った場合は、その後、一時支援金請求時に写を本制度事務局まで送付ください。

4-11 個人情報保護委員会への提出資料はどこまで記入する必要がありますか？

全ての項目について記入をお願いします。尚、個人情報漏えい一時支援金のお支払いにあたっては、再発防止策の記入および漏えいした本人への対応（通知）が対応済みであることが条件となります。

4-12 サイバー攻撃を受けた報告書を厚生労働省へ提出する際の送付先はどちらになりますか？

厚生労働省の連絡先は下記の通りとなります。

〒100-8916

東京都千代田区霞が関 1 - 2 - 2 中央合同庁舎第 5 号館

医政局特定医薬品開発支援・医療情報担当参事官室

[TEL:03-6812-7837](tel:03-6812-7837) MAIL:igishitsu@mhlw.go.jp

4-13 個人情報保護委員会へ報告した内容を入手するにはどうしたらいいですか？

個人情報保護委員会のホームページから報告をする際に、「PDF出力」のボタンがありますので、そこから入手可能です。報告を提出してしまうと、PDFファイルの出力ができなくなるため、必ず提出前に出力するようお願いします。

一時支援金のご請求時には、PDFファイルを印刷したものに日付を追記のうえ、申請書兼振込依頼書とともに事務局へ送付をお願いします。

3. 本制度に関するQ&A

4. 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

4-14 受け取った一時支援金の税務処理について教えてください。

基本的に見舞金として申告した場合、非課税扱いになると考えられますが、各医療機関の会計処理により異なる可能性があるため、顧問税理士もしくは管轄の税務署にご相談下さい。

【国税HP】

<https://www.nta.go.jp/taxes/shiraberu/saigai/h30/0018008-045/09.htm>

【税についての相談窓口】

<https://www.nta.go.jp/taxes/shiraberu/shirabekata/9200.htm#a02>

4-15 一時金の申請期限はありますか？

申請期限はありません。尚、1医療機関あたり年間1回までのご請求となります。

4-16 1年に1回の請求までとなっていますが、1年間とはいつからいつまででしょうか？

2022年6月1日に制度が始まりますので、2022年6月1日～2023年5月31日までが1年間となります。その後、毎年6月1日～5月31日までの期間が1年間となります。

4-17 サイバー攻撃を受けて1日以上休業した場合で、事由発生日が2023年5月31日以前の場合はいくら一時支援金が支払われますか？

事由発生日が2022年6月1日～2023年5月31日までの期間である場合で1日以上休業した場合には、休業日数にかかわらず一時支援金15万円をお支払いします。詳細は以下をご確認ください。

【お支払いする金額について】

●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10万円をお支払いします。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。

4-18 サイバー攻撃を受け一時金を申請する場合、厚生労働省へ報告書の提出は必須ですか。

必須ではありませんが、厚生労働省への提出を推奨しております。制度改定により、2023年6月1日以降は日本医師会への報告書の提出のみでも一時金のお支払いは可能です。

3. 本制度に関するQ&A

5. 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

5-1 厚生労働省作成の「医療情報システムの安全管理に関するガイドライン」および「医療機関等におけるサイバーセキュリティ対策チェックリスト」の掲載場所はどこですか。

以下に掲載されていますので、ご確認ください。

【厚生労働省HP】

https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

5-2 厚生労働省作成の「医療機関等におけるサイバーセキュリティ対策チェックリスト」と日本医師会の「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」の違いは何ですか。

日本医師会の「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」では、厚生労働省の「医療機関等におけるサイバーセキュリティ対策チェックリスト」で求められているめられている項目を中心に、実践的かつ効率的に取り組んでいただけるよう具体的にわかりやすく記載するよう努めたものになります。厚生労働省のチェックリストもご参照の上、ぜひ積極的にご活用ください。

3. 本制度に関するQ&A

6. 日本医師会セキュリティガイドライン相談窓口

6-1 厚生労働省の「医療情報システムの安全管理に関するガイドライン」を見ましたが、何から手を付けてよいかわかりません。このような場合も相談は可能ですか

ご相談は可能ですが、まずチェックリスト項目にしたがって対応をお願いします。このチェックリストは、ガイドラインの記載内容のうち、医療機関の皆様が優先的に取り組むべき事項を抽出したものです。チェックリスト項目内でも、優先順位により対応時期が定められていますので、まずはそこから着手されることを推奨いたします。

日本医師会の「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」もご参照いただき、ご不明点がございましたらお気軽にご相談ください。

6-2 電話以外にメール等での相談は可能ですか。

お電話のみでの対応となります。

6-3 相談窓口で紹介された専門事業者に業務を依頼する場合の費用は自己負担ですか。

会員様ご自身で負担いただく形になります。

6-4 相談した内容は日本医師会に共有されますか。

今後のサービス向上を目的に定期的に日本医師会に共有されます。