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

2025年7月1日　改定

目次

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と見込まれています。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6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
⑥「医療情報システムの契約における当事者間の役割分担に関する確認表」に関する解説動画の提供（New 2025年7月～）

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。

（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(4-17) 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

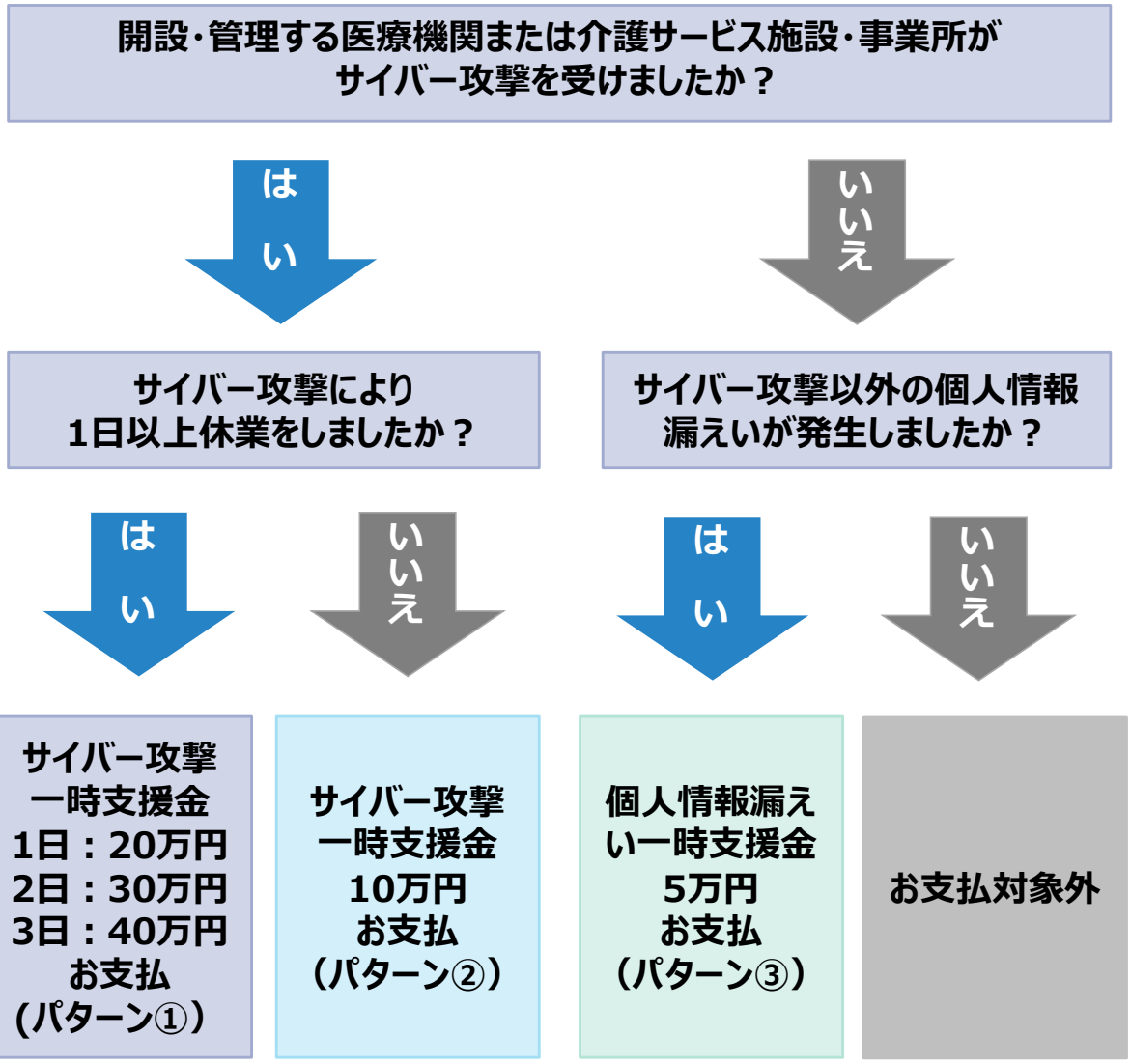
（5）支援金のお支払いスケジュール
支援金のお振込みスケジュールは以下の通りとなります。お支払いに必要な全ての書類が到着し、内容に問題ないことを確認のうえ、お振込みをさせていただきます。

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、件名を以下にしていただくようお願いします。
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

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写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写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もに事務局へ郵送

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おります。
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

（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月末の厚生労働省の「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」の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の実践ガイドおよびセミナー動画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。なお、2-6「医療情報システムの契約における当事者間の役割分担等に関する確認表」に関する解説動画についてのご相談も受け付けております

（1）具体的なサービスご提供内容
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、それらに付随するセキュリティ対策に関するガイドライン第6.0版に関する各種ご相談に対応します。また2-6「医療情報システムの契約における当事者間の役割分担等に関する確認表」に関する解説動画についての相談にも対応します。

（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 「医療情報システムの契約における当事者間の役割分担等に関する確認表」に関する解説動画の提供（2025年7月～）

医療機関とシステム事業者等における役割分担の整理と、契約による明文化に資することを目的に2024年6月に総務省、厚生労働省、経済産業者の３省連名で「医療情報システムの契約における当事者間の役割分担等に関する確認表」（以降、「役割分担確認表」と記載）が策定されました。「役割分担確認表」は2部で構成されており、Part1については、医療機関が、契約前に自ら行う情報セキュリティ対策がまとめられており、各種セキュリティ対策の実施や、現時点での対策状況を可視化することは、事業者との契約作業に関係なく非常に重要になるため、日本医師会としてもセキュリティ対策の一助となるよう、Part１について具体的な対応方法等を解説した動画を作成しました。

（1）「医療情報システムの契約における当事者間の役割分担等に関する確認表」
Part1解説動画の掲載先

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


医療情報システムの契約における当事者間の役割分担等に関する確認表

Part1 主に医療機関が実施する項目

（契約を締結する上で医療機関が主体となって、必要に応じてシステム関連事業者の協力を得ながら実施することが望ましい項目の例）

＊が付されている用語については、別添の「用語の解説」を適宜参照すること。

項番	項目	内容	初回確認（　/　）	完了日（日付）	備考欄
A	事業者選定・事業者管理				
1	事業者からの開示資料の確認	事業者から開示を受けたサービス仕様適合開示書**1等（MDS/SDS**2、MDS2**3等）を確認しているか。	はい・いいえ	（　/　）	
2	事業者管理	①事業者との契約・協働体制を把握・管理できているか。	はい・いいえ	（　/　）	
		②医療情報を第三者提供する場合の管理体制が整備されているか。	はい・いいえ	（　/　）	
B	医療機関の内部体制				
1	「医療情報システムの安全管理に関するガイドライン」の確認	「医療情報システムの安全管理に関するガイドライン」を確認したか。	はい・いいえ	（　/　）	
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」に基づく契約時での現状把握及びの対応	「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」を用いて、契約時に医療情報システムの現状把握及び対応を実施しているか。	はい・いいえ	（　/　）	
3	安全管理のための人的管理	① 医療情報を取り扱う職員に関して人的安全管理対策を実施しているか。	はい・いいえ	（　/　）	
		② 個人情報の安全管理に関する職員への教育・訓練を採用時及び定期的に実施し、教育・訓練の実施状況について定期的に経営層へ報告しているか。	はい・いいえ	（　/　）	
4	通常時における管理責任	医療情報システムの管理や運用を適切に行っているか。	はい・いいえ	（　/　）	
5	通常時における説明責任	① 医療情報システムの機能や運用につき、医療機関として状況を適切に把握し、必要に応じて患者等に説明ができるようになっているか。	はい・いいえ	（　/　）	
		② システム構築等を実施する際に、医療機関として状況を適切に把握し、必要に応じて事業者に説明ができるようになっているか。	はい・いいえ	（　/　）	
6	物理的リスクの対応	① 機器や記憶媒体を持ち出す際の紛失・盗難リスクの対応を行っているか。	はい・いいえ	（　/　）	
		② 施設への物理的侵入リスクの対応を行っているか。	はい・いいえ	（　/　）	
C	情報類の整備				
1	医療情報システムの運用ルール及び情報類の策定	医療情報システムの運用ルールを定め、明文化された情報類を整備しているか。必要に応じて情報類の見直しを行っているか。	はい・いいえ	（　/　）	
2	通常時における定期的な見直し、改善責任	医療情報システムの運用につき、適宜事業者からの情報提供を受け、定期的に見直し、必要な改善を行えるようになっているか。	はい・いいえ	（　/　）	
3	インシデント発生に備えた対応	BCP**4（事業継続計画）について、定期的な見直しや従業員への訓練・周知等を行っているか。	はい・いいえ	（　/　）	

３．本制度に関するQ&A

３．本制度に関するQ＆A

目次

３．本制度に関するQ＆A

目次

３．本制度に関するQ&A

目次

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　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となる情報をお伝えし、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ご提出願います。

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　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、そちらから入手可能です。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ので、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日に制度が開始しますので、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分かりません。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ご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。