

事務連絡
令和8年2月19日

各都道府県 衛生主管部（局） 御中

厚生労働省医政局
医療情報担当参事官室

「医療機関におけるサイバーセキュリティ確保事業」
の実施に係る支援対象病院の選定について（依頼）

日頃より厚生労働行政に対しご協力を賜り、厚く御礼申し上げます。

医療機関等におけるサイバーセキュリティ対策として特に迅速に対応いただきたい事項については、令和6年8月1日付事務連絡「医療機関等におけるサイバーセキュリティ対策の取組みについて（周知依頼）」をお示し、医療機関等に周知をお願いしているところです。

現在、病院におけるサイバーセキュリティの更なる確保のため、外部ネットワークとの接続の安全性の検証・検査や、オフライン・バックアップ体制の整備を支援する「医療機関におけるサイバーセキュリティ確保事業」を実施しています。令和7年度補正予算においては、サイバー攻撃に対する安全性をより一層強化するため、外部接続点が多数存在する医療機関に対して、その適正化まで事業対象を拡充し、維持管理支援等を行います。

つきましては、当該事業をより効果的なものとするため、地域の医療提供体制の実情を踏まえ、別記のとおり各都道府県において支援対象病院を選定していただくよう、ご協力の程よろしくお願ひいたします。

（照会先）

厚生労働省医政局医療情報担当参事官室

1 事業概要

事業名：令和8年度医療機関におけるサイバーセキュリティ確保事業

- 病院の外部接続点の適正化及び維持管理体制づくりの支援
- 上記適正化及び維持管理体制づくりに必要な設備購入・構築等に掛かる経費の補助※

※補助について

- ・適正化及び維持管理（外部接続点の集約等）の計画策定を受けた施設について、その実施に係る令和8年度内の費用の一部を補助します。補助金の支払いについては、令和9年3月10日（予定）までに設備購入・構築等に掛かる経費の支払いが済んでいることが条件となります。
- ・補助基準額（予定：今後交付要綱において正式決定）

400床以上病院 3,500千円 399床以下病院 2,000千円

補助額は、上記金額を補助上限とします（補助率10/10）

なお、補助基準額については、申請状況により予算の範囲内で減額又は増額する場合があります。

2 支援対象の医療機関

- 電子カルテシステムを導入している※
- ネットワーク構成図や機器管理台帳を作成している

上記2点を満たしている病院、314施設を対象とします。

※ 令和8年度中の電子カルテシステム更改を予定していないこと。

なお、「外部接続点の適正化及び維持管理体制づくり」の支援を受けず、設備購入・構築等に掛かる経費のみの申請は認められません。

3 支援対象病院の選定方法

- 各都道府県から該当する病院に連絡等を行い、支援対象病院を選定してください。
- 本年度の選定では、各都道府県に2枠（計94枠）を確保します。残りの220施設については、厚生労働省にて支援対象病院を選定いたします※。
- 各都道府県の判断において優先的に支援対象とする場合は、その旨お伝えください。
- 選定された支援対象病院が事業途中で辞退した場合は、次点の病院が支援対象病院として新たに選定される場合があります。

※順位選定の基準

- ・特定機能病院など地域における主要な診療機能を担う病院

- ・外部接続点の適正化の効果が大きいと想定される病院
- ・立入検査等においてセキュリティ対策が不十分と思われる病院
- ・令和6年度及び令和7年度の医療機関におけるサイバーセキュリティ確保事業に参加された病院

4 提出期限等

提出期限：令和8年3月27日（金）まで

なお、期限までの提出が困難な場合は、個別対応を検討いたしますので、照会先までご相談ください。

提出方法：別紙1「【様式】R8 サイバーセキュリティ確保事業支援対象病院リスト」により提出

提出先：厚生労働省医政局医療情報担当参事官室

なお、期限までの提出が困難な場合は、個別対応を検討いたしますので、照会先までご相談ください。

4 その他・補足情報

- 選定された支援対象病院への支援に関しては、当該事業の受託企業から直接支援対象病院に連絡等を行い、進めることとなります。（特に都道府県で対応していただくことはありません。）
- 補助金申請に関する詳細は今後発版予定の補助金交付要綱、補助金公募要領において明示します。
- （参考情報）「外部接続点の適正化、維持管理」の考え方
外部ネットワークとの通信接点を物理・論理的に最小化・一元化し、組織全体の通信に対し一律かつ適正な監視・制御を可能にすること。

| | |
|-----|--|
| 適正化 | 1. 物理的集約 管理対象となる物理的な接続インターフェース及び境界デバイスを削減し、管理密度を高める行為。 2. 論理的集約（制御・運用の適正化） 通信経路と権限をソフトウェア定義で一元化し、セキュリティポリシーの適用を自動化・均一化する行為。 |
|-----|--|

(別記)

| | |
|-------|---|
| 維持・管理 | 適正化された接続点の機能と可用性を継続的に担保し、動的な脅威や組織の変化に合わせてセキュリティ状態を常に最新化（アップデート）し続けるプロセス（技術的維持、運用管理） |
|-------|---|

以上