日医発第 1266 号（情シ）
令 和 5 年 10 月 11 日

都道府県医師会　担当理事　殿

公益社団法人　日本医師会
常任理事　長島　公之
（公印省略）

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

平素より本会会務の運営に特段のご理解・ご支援を賜り厚く御礼申し上げます。

近年、国内外の医療機関を標的とした、ランサムウェア（情報システムを使用不可の状態にした上で身代金を要求するウイルス）を利用したサイバー攻撃による被害が増加している状況にあり、日本医師会においても注意喚起を行ってまいりました。

ここ数年、10 月末に医療機関へのサイバー攻撃によって電子カルテの閲覧・利用ができなくなる等の事案が発生していることを踏まえ、厚生労働省よりサイバーセキュリティの注意喚起等に関して、本会宛に周知依頼が参りました。

医療機関におかれましては、別添 1～3 を参考にサイバーセキュリティ対策に取り組んでいただきたくお願い申し上げます。また、別添 4,5 の情報も併せてご活用ください。

なお、別添 4 に関しまして、8 月 25 日付け日医発第 968 号（情シ）「厚生労働省委託事業　令和 5 年度「医療情報セキュリティ研修及びサイバーセキュリティインシデント発生時初動対応支援・調査事業」について」にてお知らせしました「医療機関向けサイバーセキュリティ対策研修」について、リアルタイムで受講できなかった方への対応策の実施を日本医師会から強く要望した結果、一部アーカイブ配信が予定されている旨が記載されております。引き続き、広くアーカイブ配信されるよう求めてまいります。

つきましては、貴会におかれましても、本件についてご了知いただくと共に、貴会管下の郡市区等医師会ならびに会員への周知方につき、ご高配を賜りますようお願い申し上げます。

【別添資料】

- 【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）
- 別添 1：サイバーセキュリティ　9 の心得
- 別添 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
- 別添 3：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マニュアル
- 別添 4：令和 5 年度 医療情報セキュリティ研修
- 別添 5:【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強化について（注意喚起）

以上

事　務　連　絡
令和５年 10 月 10 日

公益社団法人　日本医師会　御中

厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室
厚生労働省政策統括官付サイバーセキュリティ担当参事官室

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）

日頃から厚生労働行政に対して御協力を賜り、厚く御礼申し上げます。

医療機関等においては、保有する医療情報の安全を確保するため、「医療情報システムの安全管理に関するガイドライン」等に沿って、必要な対策を講じていただいているところです。

一方、ここ数年、医療機関へのサイバー攻撃によって電子カルテの閲覧・利用ができなくなる等の事案が発生していることを踏まえ、別添１のとおり、医療機関において早急に取り組んでいただきたいセキュリティ対策等についてまとめましたので、管内、管下の医療機関に対し、院内掲示等でサイバーセキュリティに対する意識醸成に活用するよう周知ください。併せて、医療法第 25 条第１項に基づく立入検査において確認することとしている「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」（別添２）について、「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マニュアル」（別添３）を活用しながら、医療機関において対策が適切に講じられているか確認するよう要請ください。また、万が一、サイバー攻撃を受けた場合にも事業継続計画等により地域住民への医療提供体制に支障が出ることのないよう医療機関に対する注意喚起をお願いします。

さらに、医療機関向けセキュリティ教育支援ポータルサイトの研修コンテンツ（別添４）や、令和４年 11 月 10 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強化について（注意喚起）」（別添５）の情報もご活用下さい。

なお、別添５のランサムウェア特設ページについてはサイトが移動しておりますので下記 URL をご参照ください。

https://www.nisc.go.jp/tokusetsu/stopransomware/index.html

■医療機関等がサイバー攻撃を受けた場合等の厚生労働省連絡先
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
※迷惑メール防止のため、メールアドレスの一部を変えています。
「×」を「@」に置き換えてください。

■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（令和５年５月）
URL ： https://www.mhlw.go.jp/stf/shingi/0000516275_00006.html

別添１

他人事・過去の事だと思っていませんか!?

～ 10月31日に起きた過去のサイバーインシデントを未然に防ぐために！～

〈サイバーセキュリティ ９の心得〉

経営管理者（院長、医療情報システム安全管理責任者等）

1 アカウント整理と使用状況の棚卸し

- ☑ 不要なアカウントの削除
- ☑ アカウントのパスワード強度と管理状況

2 連絡先の整備

- ☑ 自組織内の緊急連絡先を整理
- ☑ ベンダー、保守契約先等の連絡先を整理

3 バックアップの実施状況の点検

- ☑ 計画通りにバックアップが実行されているか確認
- ☑ バックアップデータがネットワークから隔離されているか確認

医療情報システムの安全管理実務者

4 通信制御の確認

- ☑ 通信の整理が適切に行われているか確認
- ☑ 不要な通信先への制御（トラフィックコントロール）が行われているか確認
- ☑ 関係事業者とのネットワーク接続点が管理下にあるか確認

5 ログの確認

- ☑ 攻撃の兆候がないかを再確認

6 各種システムの更新

- ☑ ソフトウェアの更新が適切に行われているか確認
- ☑ セキュリティ対策ソフトが常に稼働しているか確認

医療従事者等

7 機器やデータの持ち出しルールの確認と順守

- ☑ 端末や外部記憶媒体の持ち出しについて、自組織内の安全基準等に沿った適切な対応

8 利用機器に関する対策

- ☑ 不正アクセスを防止するため、不正プログラム対策ソフトウェアは「常」に稼働
- ☑ 長期間使用しない場合は電源 OFF

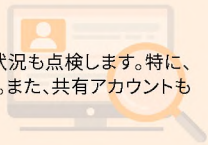
9 電子メールの確認

- ☑ 電子メールを確認する前に、以下の対策を実施する
  - ・利用機器のOS・アプリケーションに対する修正プログラムの適用
  - ・不正プログラム対策ソフトウェアなどの定義ファイルの更新
- ☑ アカウントのパスワード強度と管理状況

経営管理者（院長、医療情報システム安全管理責任者等）

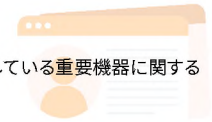
1 ✔アカウント整理と使用状況の棚卸し

- 現在使用中のアカウントを整理し、不要なアカウントを停止・削除します。同時に、使用中のアカウントのパスワード強度と管理状況も点検します。特に、弱いパスワード（数字やアルファベットだけなど）が使われている場合は、半年以内にパスワード変更が行われたかを確認します。また、共有アカウントも同様に整理し使用状況の棚卸を実施します。



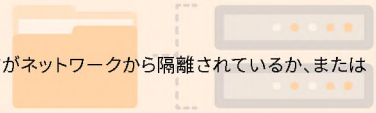
2 ✔連絡先の整備

- 各種・各方面（緊急時の連絡先として、SAJ・厚生労働省等）との連絡先、連絡担当者の整理を実施します。同様に、自組織で契約している重要機器に関する保守ベンダーやセキュリティベンダーとの連絡先も整理します。
  ※事案が発生した際に迅速かつ適切な対応を行うために、事前に対応策を策定します。



3 ✔バックアップの実施状況の点検

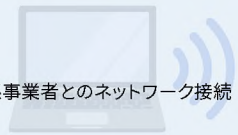
- 重要なシステムのバックアップが計画通りに行われているかを確認します。さらに、バックアップしたデータがネットワークから隔離されているか、または複数の方法でデータの保護が確保されているかも確確認します。



医療情報システムの安全管理実務者

4 ✔通信制御の確認

- 病院ネットワークにおける必要な通信の整理が適切に行われているかどうかを確認します。
  また、重要なシステムや通信制御を行っている機器のログが適切に保存され、運用されていることを確認します。さらに、関係事業者とのネットワーク接続点をすべて管理下においてください。

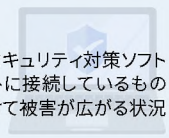


5 ✔ログの確認

- 攻撃の兆候がないかを再確認します。
  ※攻撃の兆候の例：管理者以外の認証の有無、または重要なシステムやネットワーク機器での管理外の設定変更などが発生していないかを確認します。

6 ✔各種システムの更新

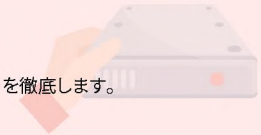
- バージョンアップやファームアップが適切に行われているかを確認します。特にインターネットに接続しているシステムに関しては、セキュリティ対策ソフトが常に稼働しているかを徹底的に確認し、導入されていない場合（セキュリティ対策ソフト等）は導入します。さらに、インターネットに接続しているもののセキュリティ対策が不十分な場合は、通信制御の可能性を検討し、システムの停止または縮退を検討します。（これにより攻撃を受けて被害が広がる状況を未然に防ぎます。）



医療従事者等

7 ✔機器やデータの持ち出しルールの確認と順守

- 端末や外部記憶媒体の持ち出しは、組織内の安全基準等に則った適切な対応（持ち出し・持ち込みに関する内規の遵守等）を徹底します。



8 ✔利用機器に関する対策

- 不正アクセスを防止するため、不正プログラム対策ソフトウェアを「常」に稼働し、また古いシステムが放置されているような場合は管理者に届出・相談してください。
- 長期間使用しない場合は電源を落とします。

9 ✔電子メールの確認

- 電子メールを確認する前に、利用機器のOS・アプリケーションに対する修正プログラムの適用や不正プログラム対策ソフトウェアなどの定義ファイルの更新などを実施します。
- 不審な添付ファイル・リンクを開かないようにします。不審な点があれば開封する前に、電話や別の手段で管理者に相談・確認します。

対策しても インシデントが発生してしまったら… 速やかに連絡を!

⚠インシデントかも…？

- ウイルスに感染してしまったなど、気になる点がございましたらご連絡ください。
- 厚生労働省へは医療機関等がサイバー攻撃を受けた（疑い含む）場合等にはご連絡ください。

〈派遣依頼方法〉

以下のいずれかの方法でご連絡ください

A 厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室にご連絡ください。

B 本事業の専用サイト「インシデントかも？」からご連絡ください。
https://mhlw-training.saj.or.jp/

QRコードはこちら

厚生労働省 厚生労働省委託事業

〈厚生労働省 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

Software Association of Japan

〈一般社団法人ソフトウェア協会〉
医療情報セキュリティ研修事務局
E-mail. mist-sajinfo@saj.or.jp

別添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

医療機関確認用

	チェック項目	確認結果 （日付）	備考
医療情報システムの有無	医療情報システムを導入、運用している。 （「いいえ」の場合、以下すべての項目は確認不要）	はい・いいえ （　/　）	

○　令和５年度中

*以下項目は令和５年度中にすべての項目で「はい」にマルが付くよう取り組んでください。

*２（２）及び２（３）については、事業者と契約していない場合には、記入不要です。

*1 回目の確認で「いいえ」の場合、令和５年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付）			備考
		１回目	目標日	２回目	
1 体制構築	（1）　医療情報システム安全管理責任者を設置している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**				
	（1）　サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（2）　リモートメンテナンス（保守）を利用している機器の有無を事業者等に確認した。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（3）　事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	サーバについて、以下を実施している。				
	（4）　利用者の職種･担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（5）　退職者や使用していないアカウント等､不要なアカウントを削除している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（6）　アクセスログを管理している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	ネットワーク機器について、以下を実施している。				
	（7）　セキュリティパッチ(最新ファームウェアや更新プログラム）を適用している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
	（8）　接続元制限を実施している。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	
3 インシデント発生に備えた対応	（1）　インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）への連絡体制図がある。	はい・いいえ （　/　）	（　/　）	はい・いいえ （　/　）	

- 各項目の考え方や確認方法等については、「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マニュアル～医療機関・事業者向け～」をご覧ください。
- 立入検査の際は、チェックリストに必要な事項が記入されているかを確認します。

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

医療機関確認用

○　参考項目（令和６年度中）

*以下項目について、令和６年度中にすべての項目で「はい」にマルが付くよう取り組んでください。

	チェック項目	確認結果（日付）			備考
		１回目	目標日	２回目	
2 医療情報システムの管理・運用	**サーバについて、以下を実施している。**				
	（７）　セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）	
	（９）　バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）	
	端末 PC について、以下を実施している。				
	（４）　利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）	
	（５）　退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）	
	（７）　セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）	
	（９）　バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）	
3 インシデント発生に備えた対応	（２）　インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）	
	（３）　サイバー攻撃を想定した事業継続計画（BCP）を策定、又は令和６年度中に策定予定である。	はい・いいえ（　/　）	（　/　）	はい・いいえ（　/　）	

● 各項目の考え方や確認方法等については、「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マニュアル～医療機関・事業者向け～」をご覧ください。

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

事業者確認用

○　令和５年度中

*以下項目は令和 5 年度中にすべての項目で「はい」にマルが付くよう取り組んでください。
*1 回目の確認で「いいえ」の場合、令和 5 年度中の対応目標日を記入してください。

	チェック項目	確認結果（日付）			備考
		1 回目	目標日	2 回目	
1 体制構築	（1） 事業者内に、医療情報システム等の提供に係る管理責任者を設置している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
2 医療情報システムの管理・運用	**医療情報システム全般について、以下を実施している。**				
	（2） リモートメンテナンス（保守）している機器の有無を確認した。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（3） 医療機関に製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出した。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	サーバについて、以下を実施している。				
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（6） アクセスログを管理している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	ネットワーク機器について、以下を実施している。				
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（8） 接続元制限を実施している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	

事業者名：＿＿＿＿＿＿＿＿＿＿＿＿＿＿

● 各項目の考え方や確認方法等については、「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マニュアル～医療機関・事業者向け～」をご覧ください。

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

事業者確認用

○　参考項目（令和６年度中）

*以下項目について、令和６年度中にすべての項目で「はい」にマルが付くよう取り組んでください。

	チェック項目	確認結果（日付）			備考
		1 回目	目標日	2 回目	
2 医療情報システムの管理・運用	**サーバについて、以下を実施している。**				
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	端末 PC について、以下を実施している。				
	（4） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（5） 退職者や使用していないアカウント等、不要なアカウントを削除している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（7） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	
	（9） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。	はい・いいえ（ / ）	（ / ）	はい・いいえ（ / ）	

● 各項目の考え方や確認方法等については、「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マニュアル～医療機関・事業者向け～」をご覧ください。

別添３

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マニュアル

～医療機関・事業者向け～

本マニュアルは、「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（以下「チェックリスト」という。）」をわかりやすく解説するものです。チェックリストを活用する際に、ご覧ください。

～はじめに～

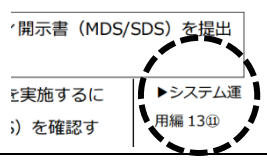
○　医療機関等に対するサイバー攻撃は近年増加傾向にあり、その脅威は日増しに高まっています。医療機関が適切な対策をとることで、こうしたサイバー攻撃等の情報セキュリティインシデントによる患者の医療情報の流出や、不正な利用を事前に防ぐことが重要です。医療情報システムは、効率的かつ正確に医療行為を行う上で重要な役割を果たしています。医療の継続性を支える観点からも、適切な管理の下、医療情報システムを利用することが求められています。

○　医療機関等におけるサイバーセキュリティ対策については、厚生労働省が作成している「医療情報システムの安全管理に関するガイドライン（以下「ガイドライン」という。）」を参照の上、適切な対応を行うこととしているところ、このうち、まずは医療機関が優先的に取り組むべき事項をチェックリストにまとめました。

本マニュアルは、医療機関におけるチェックリストを用いた確認の実行性を高めるために、サイバーセキュリティ対策に馴染みがない方にもご理解いただけるよう、チェック項目の考え方や確認方法、用語等についてなるべく平易な言葉で解説することを目指しました。

○　医療機関および医療情報システム・サービス事業者（以下「事業者」という。）は、本マニュアルを参照しつつチェックリストを活用して、日頃から実のあるサイバーセキュリティ対策を行って下さい。

目次

凡例		本マニュアルの「Ⅱ各チェック項目の解説」では、それぞれのチェック項目に紐づく「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」の該当箇所を右側に「▶」で示しています。

Ⅰ　チェックリストの使い方

1．チェックリストの用意

○　チェックリストを使用するにあたり、医療機関においては「医療機関確認用」、事業者においては「事業者確認用」を用いて確認してください。事業者と契約していない医療機関においては「事業者確認用」による確認は不要です。

○　医療機関は事業者に「事業者確認用」を送付し、対策の状況を確認するよう求めてください。複数の医療情報システムを利用している場合、システムを提供している事業者ごとに確認を求めてください。なお、事業者に対しても別途本取組について周知を行っていきます。

2．チェックリストの記入方法

○　各項目の実施状況を確認し、「はい」または「いいえ」にマルをつけて、確認した日付を記入してください。もし１回目の確認で「いいえ」の場合は、対策の実施にかかる令和５年度中の目標日を記入するようにしてください。チェックリストは紙媒体または電子媒体のどちらで使用して頂いても構いません。

○　医療機関は「医療機関確認用」について令和５年度中に全てのチェック項目で「はい」にマルがつくように、事業者と連携して取り組むようにしてください。

（※）　事業者と契約していない場合には、２（２）及び２（３）の記入は不要です。

○　複数の事業者と契約している場合、契約内容によっては「事業者確認用」の一部の項目の確認が不要になることもあります。「事業者確認用」には、事業者名を記入する欄を設けています。医療機関は各事業者から回収してください。

3．参考項目について

○　「医療機関確認用」、「事業者確認用」ともに、参考項目を設けています。参考項目については令和６年度中には全ての項目で「はい」にマルがつくよう取組を進めてください。

4．その他

○　チェックリストの確認結果は随時参照して、日頃の対策の実施に役立ててください。

○　少なくとも年に１回は、チェックリストを用いた点検を実施してください。

○　医療機関と直接契約関係にない事業者においては、「事業者確認用」の作成は不要です。

～立入検査時、チェックリストを確認します～

医療法に基づく立入検査では、病院、診療所および助産所においてサイバーセキュリティ確保のために必要な取組を行っているかを確認することとしています。

令和 5 年度は、「医療機関確認用」、「事業者確認用」の全ての項目について、１回目の確認の日付と回答等が記入されていることを確認します（※）。このうち、３（１）の連絡体制図は現物を確認しますので、立入検査までに作成してください。

参考項目は令和５年度の立入検査では確認しません。

日頃の確認に加え、立入検査前は改めてチェックリストを用いてサイバーセキュリティ対策の状況を確認しましょう。

なお、医療機関は事業者からチェックリストを回収しておきましょう。

（※） 事業者と契約していない場合には、「医療機関確認用」２（２）及び２（３）についての確認は求められません。

Ⅱ　各チェック項目の解説

医療情報システムの有無　　【医療機関確認用】

医療情報システムを導入、運用している。

本チェックリストが対象とする医療情報システムは、医療情報を保存するシステムだけではなく、医療情報を扱う情報システム全般を想定します（例：レセコン、電子カルテ、オーダリングシステム等）。これには、事業者により提供されるシステムだけでなく、医療機関等において自ら開発・構築されたシステムが含まれます。

本項目の「いいえ」にマルがつく場合、以下すべての項目は確認不要です。

▶概説編 2.3

1　体制構築　　【医療機関確認用・事業者確認用】

（1） 医療情報システム安全管理責任者を設置している。

医療機関等において、医療機関の経営層は安全管理を直接実行する医療情報システム安全管理責任者を設置する必要があります。医療情報システム安全管理責任者としての職務は、情報セキュリティ方針の策定及び教育・訓練を含む情報セキュリティ対策を推進することです。情報セキュリティ対策の実効性を確保するために、経営層が医療情報システム安全管理責任者に就くことが望ましいですが、医療機関の規模・組織等によっては企画管理者が兼務することもあります。

また、事業者においても医療情報システム等の提供に係る管理責任者を設置する必要があります。

（用語の解説）

企画管理者：医療機関において医療情報システムの安全管理の実務を担う担当者を指します。

▶経営管理編
3.1.2②
3.2

2　医療情報システムの管理・運用　【医療機関確認用・事業者確認用】

（用語の解説）

医療情報システム全般：サーバ、端末 PC、ネットワーク機器を指します。

サーバ：電子カルテサーバやレセコンサーバ等、ネットワーク上で情報やサービスを提供するコンピュータを指します。

ネットワーク機器：無線 LAN やルータ等を指します。

（1） サーバ、端末 PC、ネットワーク機器の台帳管理を行っている。（医療情報システム全般）

▶経営管理編 1.2.1＜管理責任＞②
▶企画管理編 9.1

医療情報システムで用いる情報機器等の安全性を確保するために、情報機器等の所在と、それらの使用可否の状態を適切に管理する必要があります。そのため、企画管理者は医療機関で所有する医療情報システムで用いる情報機器等について機器台帳を作成して管理を行い、情報機器等が利用に適した状況にあることを確認できるようにしてください。また、医療機関の経営層は定期的に管理状況に関する報告を受け、管理実態や責任の所在が明確になるよう、監督してください。台帳で管理する内容としては情報機器等の所在や利用者、ソフトウェアやサービスのバージョンなどが想定されます。

（用語の解説）

情報機器等の所在：実際の設置場所やネットワーク識別情報等を指します。

（補足）

サーバ、端末 PC、ネットワーク機器のうち、自身の医療機関で保有する医療情報システムについて台帳管理を行っていれば、「医療機関確認用」 2 （1）の「はい」にマルをつけてください。

●機器台帳の例

管理番号	メーカー	OS	ソフトウェア	ソフトウェアバージョン	IPアドレス	コンピュータ名	設置場所	利用者	登録日	状態	説明
001	A社	Win11	○○電子カルテ	2.0	192.168.○.○	Room1のPC１	Room1	a医師（○○科）	2020/12/1	稼働	
002	A社	Win11	○○電子カルテ	1.2	192.168.○.○	Room1のPC2	Room1	b医師（○○科）	2020/12/1	停止	メンテナンス
003	A社	Win8	○○電子カルテ	2.0	192.168.○.○	Room2のPC１	Room2	c医師（△△科）	2014/10/1	稼働	
004	B社	Win11	○○管理システム	5.0.1	192.168.○.○	Room3のPC１	Room3	a医師（○○科）、b医師（○○科）、c医師（△△科）	2021/8/1	稼働	

（２） リモートメンテナンス（保守）を利用している機器の有無を事業者に確認した。（医療情報システム全般）

リモートメンテナンス（保守）作業または保守環境に対するサイバー攻撃が想定されます。システム運用担当者は、このようなリスクに対応するために必要な措置を講じ、企画管理者に報告する必要があります。そのため、システム運用担当者は、２（１）で整理した情報をもとにリモートメンテナンスを利用している機器の有無を事業者に確認し、企画管理者へ報告してください。

なお、本項目は、事業者と契約していない場合には、チェックリストの記入は不要です。

（用語の解説）

システム運用担当者：医療機関において医療情報システムの実装・運用を担う担当者を指します。

▶企画管理編 9.1
▶システム運用編 10.1

（３） 事業者から製造業者/サービス事業者による医療情報セキュリティ開示書（MDS/SDS）を提出してもらう。（医療情報システム全般）

医療情報システムのセキュリティに関するリスク評価およびリスク管理を実施するにあたっては、事業者が作成する医療情報セキュリティ開示書（MDS/SDS）を確認することが有効です。企画管理者は事業者へ当該医療情報システムに関する MDS/SDS の有無を確認し、事業者から回収してください。

なお、本項目は、事業者と契約していない場合には、チェックリストの記入は不要です。

（用語の解説）

MDS/SDS：Manufacturer / Service Provider Disclosure Statement for Medical Information Security））：医療情報セキュリティ開示書（製造業者/サービス事業者による医療情報セキュリティ開示書の略称です。各製造業者/サービス事業者の医療情報システムのセキュリティ機能に関する説明の標準的記載方法（書式）を JIRA(一般社団法人 日本画像医療システム工業会)/JAHIS で定めた物で、製品/サービス説明の一部として製造業者/サービス事業者によって作成され、セキュリティマネジメントを実施する医療機関等を支援するため、医療機関等側において必要な対策の理解を容易にすることなどの用途に用いられることが想定されています。

▶概説編 4.5

（４） 利用者の職種・担当業務別の情報区分毎のアクセス利用権限を設定している。
（サーバ、端末 PC）

▶企画管理編 13④ 13.1.3

医療情報システムの利用権限は、医療従事者の資格や医療機関内の権限規程に応じて設定することが重要です。企画管理者は情報の種別、重要性と利用形態に応じて情報の区分管理を行い、その情報区分ごと、組織における利用者や利用者グループごとに利用権限を規定してください。利用者に付与した ID 等については、台帳を作成して一覧化することが望ましいです。台帳で管理する項目としては、所属部署・氏名・ユーザーID・権限等が想定されます。

なお、端末 PC については、令和５年度は参考項目としています。令和６年度中に対応できるよう取り組んでください。

●利用者 ID 台帳の例

No.	所属部署	性	名	電話番号	ユーザID	説明	権限	状態
001	システム管理	abc	def	****	abc@def	安全管理責任者	Admin	使用可
002	A科	efg	hij	****	efg@hij	使用者	User	使用可
003	A科	klm	nop	****	klm@nop	使用者/退職予定	User	使用可（23年３月まで）
004	B科	qrs	tuv	****	qrs@tuv	使用者	User	使用可
・	・	・	・	・	・	・	・	・

（５） 退職者や使用していないアカウント等、不要なアカウントを削除している。
（サーバ、端末 PC）

▶企画管理編 13⑦

企画管理者は２（４）で整理した情報を元に、退職者や使用していない ID 等が含まれていないかを確認してください。長期間使用されていない等の不要な ID は不正アクセスに利用されるリスクがありますので、速やかに削除してください。

なお、端末 PC については、令和５年度は参考項目としています。令和６年度中に対応できるよう取り組んでください。

（6） アクセスログを管理している。（サーバ）

医療情報システムが適切に運用されているかを確認するために、システム運用担当者は利用者のアクセスログを記録するとともに、企画管理者はそのログを定期的に確認してください。例えば不正アクセスがあった場合でも、その痕跡を発見して追跡する起点となることなどが期待されます。アクセスログは、少なくとも利用者のログイン時刻、アクセス時間及び操作内容が特定できるように記録することが必要です。

（補足）

アクセスログへのアクセス制限を行い、アクセスログの不当な削除／改ざん／追加等を防止する対策を併せて講じてください。

▶経営管理編 4.2
▶企画管理編 5.3
▶システム運用編 17①②

●アクセスログの例

ユーザーID	氏名	時刻	カテゴリ	操作情報
abc@def	abcdef	2023/5/16 8:30:00	管理メニュー	ログイン
abc@def	abcdef	2023/5/16 8:30:20	管理メニュー	起動
abc@def	abcdef	2023/5/16 8:31:00	入力メニュー	起動
abc@def	abcdef	2023/5/16 8:32:00	入力メニュー	カルテ入力
abc@def	abcdef	2023/5/17 12:30:00	管理メニュー	ログオフ
ghi@jkl	ghijkl	2023/5/17 8:40:00	管理メニュー	ログイン
ghi@jkl	ghijkl	2023/5/17 8:40:30	管理メニュー	起動
ghi@jkl	ghijkl	2023/5/17 8:45:00	管理メニュー	ログオフ
・	・	・	・	・

（７） セキュリティパッチ（最新ファームウェアや更新プログラム）を適用している。
（医療情報システム全般）

▶システム運用編 8③
8.1
8.2
13.2

不正ソフトウェアは、電子メール、ネットワーク、可搬媒体等を通して医療情報システム内に侵入する可能性があります。対策としては不正ソフトウェアのスキャン用ソフトウェアの導入が効果的であると考えられ、このソフトウェアを医療情報システム内の端末、サーバ、ネットワーク機器等に常駐させることにより、不正ソフトウェアの検出と除去が期待できます。

しかし、不正ソフトウェア対策のスキャン用ソフトウェアを導入し、適切に運用したとしても、全ての不正ソフトウェアが検出できるわけではありません。このため、システム運用担当者がまず実施すべき対策として、スキャン用ソフトウェアの導入に加えて、パターンファイルの更新を含め、セキュリティ・ホール（脆弱性）が報告されているソフトウェアへのセキュリティパッチを適用することが挙げられます。

なお、サーバと端末 PC については、令和 5 年度は参考項目としています。令和 6 年度中に対応できるよう取り組んでください。

（用語の解説）

パターンファイル：ウイルス対策ソフトがウイルスを発見するために使用するデータのこと。

（補足）

古い OS（Operating System の略。コンピュータを動作させるための基本的機能を提供するシステム全般のこと）を使用している等の理由で、動作確認ができずパッチが適用されていない場合がありますが、こうした機器がサイバー攻撃の対象になることがありますので、本項目を通じてシステム状況を確認することが重要です。

（８） 接続元制限を実施している。（ネットワーク）

外部ネットワークに接続する際には、ネットワークや機器等を適切に選定し、監視を行うことが必要です。特に、無線 LAN を使用する際は不正アクセス対策として適切な利用者以外に無線 LAN を利用されないようにすることが重要です。システム運用担当者は、例えば、ネットワーク機器に接続出来る MAC アドレスが限定すること等、不正アクセス対策を実施してください。

（用語の解説）

MAC アドレス：Media Access Control アドレスの略。LAN カードの中で、イーサネット（特に普及している LAN 規格）を使って通信を行うカードに割り振られた一意の番号。インターネットでは IP アドレス以外にも MAC アドレスを使用して通信を行っています。LAN カードは、製造会社が出荷製品に対して厳密に MAC アドレスを管理しているため、同一の MAC アドレスを持つ LAN カードが 2 つ以上存在することはありません。

（補足）

MAC アドレスによるアクセス制限の効果は限定的であることに留意する必要がありますので、追加の対策はガイドラインや事業者とも確認をお願いします。

▶システム運用編 13⑪

（９） バックグラウンドで動作している不要なソフトウェア及びサービスを停止している。（サーバ、端末 PC）

不正ソフトウェアは電子メール、ネットワーク等の様々な経路を利用して医療情報システム内に侵入する可能性があります。システム側の脆弱性を低減するため、まずは利用していないサービスや通信ポートを非活性化させることが重要です。システム運用担当者はプログラム一覧やタスクマネージャー等で不要なソフトウェアやサービスが作動していないかを確認し、不要なものがある場合は企画管理者に相談の上、対策を講じてください。

なお、サーバと端末 PC については、令和 5 年度は参考項目としています。令和 6 年度中に対応できるよう取り組んでください。

▶システム運用編 8.1

3　インシデント発生に備えた対応　【医療機関確認用】

（1）インシデント発生時における組織内と外部関係機関（事業者、厚生労働省、警察等）の連絡体制図がある。

▶経営管理編
3.4.2①
3.4.3①
▶企画管理編
12.3

医療機関の経営層は情報セキュリティインシデント発生に備え、事業者や外部有識者と非常時を想定した情報共有や支援に関する取決めや体制を整備するよう、企画管理者に指示することが重要です。企画管理者はサイバーインシデント発生時、速やかに情報共有等が行えるよう、緊急連絡網を明示した連絡体制図を作成して下さい。連絡体制図には施設内の連絡先に加え、事業者、情報セキュリティ事業者、外部有識者、都道府県警察の担当部署、厚生労働省や所管省庁等が明示されていることが想定されます。

このような連絡体制が整備されていることで、速やかな初動対応支援が可能となり被害拡大の防止につながります。

立入検査時は、連絡体制図が作成されていることを確認します。

（用語の解説）

CSIRT: 「Computer Security Incident Response Team」の略。コンピュータセキュリティにかかるイシデントに対処するための組織の総称。インシデント関連情報、脆弱性情報、攻撃予兆情報を常に収集、分析し、対応方針や手順の策定などの活動をする。

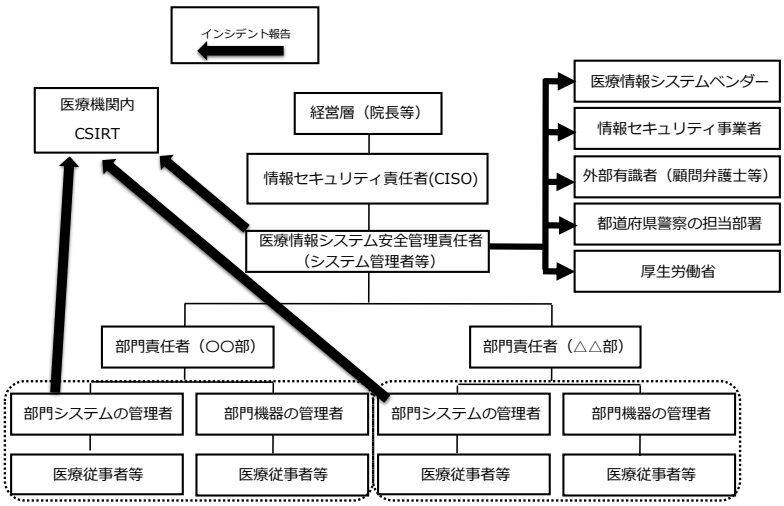
CISO: 「Chief Information Security Officer」の略。最高情報セキュリティ責任者。施設や組織における情報セキュリティを統括する責任者を指す

（補足）

サイバー攻撃を受けた疑いがある場合は、下記の厚生労働省の連絡先に御連絡ください。なお、いたずら防止のため、184 発信、公衆電話発信は受信不可としますので、医療機関の電話で御連絡願います。

【連絡先】厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室　03-6812-7837

●連絡体制図の例



（２）インシデント発生時に診療を継続するために必要な情報を検討し、データやシステムのバックアップの実施と復旧手順を確認している。

非常時でも、稼働が損なわれた医療情報システムを復旧できるよう、情報システムやデータ等のバックアップを適切に確保し、その復旧手順を整備・確認しておくことが求められます。企画管理者はバックアップを確保する際、重要なファイルについては、不正ソフトウェアの混入による影響が波及しないよう複数の方式で世代管理するよう設計し、システム運用担当者は手順に従いバックアップを確保してください。復旧手順の整備については、例えば、BCP に復旧手順を定めるなどの方法が挙げられます。

なお、令和５年度は参考項目としています。令和６年度中に対応できるよう取り組んでください。

（用語の解説）

世代管理：バックアップの一種で、最新データだけでなく、それ以前のデータもバックアップする方法を指します。例えば、３世代以上で管理する場合、日次でバックアップを行うならば、「3 世代以上」とは「３日以上」のバックアップを確保することになります。

（補足）

３世代目以降のバックアップはオフライン（物理的あるいは論理的に書き込み不可の状態）にする等の対策が望ましいです。

▶経営管理編
3.4.1
▶企画管理編
11.2
▶システム運用編
11.1
12.2
18.1

（３）サイバー攻撃を想定した事業継続計画（BCP）を策定、又は令和６年度中に策定予定である。

医療機関の経営層は企画管理者と連携して非常時における業務継続の可否の判断基準や継続する業務選定等の意思決定プロセスを検討し、サイバー攻撃を想定した BCP 等を整備することとしています。この BCP を整備しておくことにより、万が一サイバー攻撃を受けても重要業務が中断しない、または中断しても短い期間で再開することが期待できます。

なお、令和５年度は参考項目としています。令和６年度中に対応できるよう取り組んでください。

▶経営管理編
3.4.1
▶企画管理編
11.1

～参考資料～

◇[特集]　小規模医療機関等向けガイダンス

診療所や歯科診療所、薬局、訪問看護ステーション等の小規模医療機関等（以下「小規模医療機関等」という。）では、医療情報システムの安全管理を専任で対応する人材が十分に確保できないというケースも多くみられます。本ガイダンスは、小規模医療機関等において、ガイドラインに示されている安全管理対策を実施するために必要な内容の概略を簡易的に示しています。

◇[特集]　医療機関等におけるサイバーセキュリティ

本ガイダンスはサイバーセキュリティに関係する部分を要約し、サイバー攻撃の典型例など具体的な事例などもまとめています。チェックリストを用いた確認と併せて一読いただき、ぜひサイバーセキュリティに対する理解をさらに深めてください。

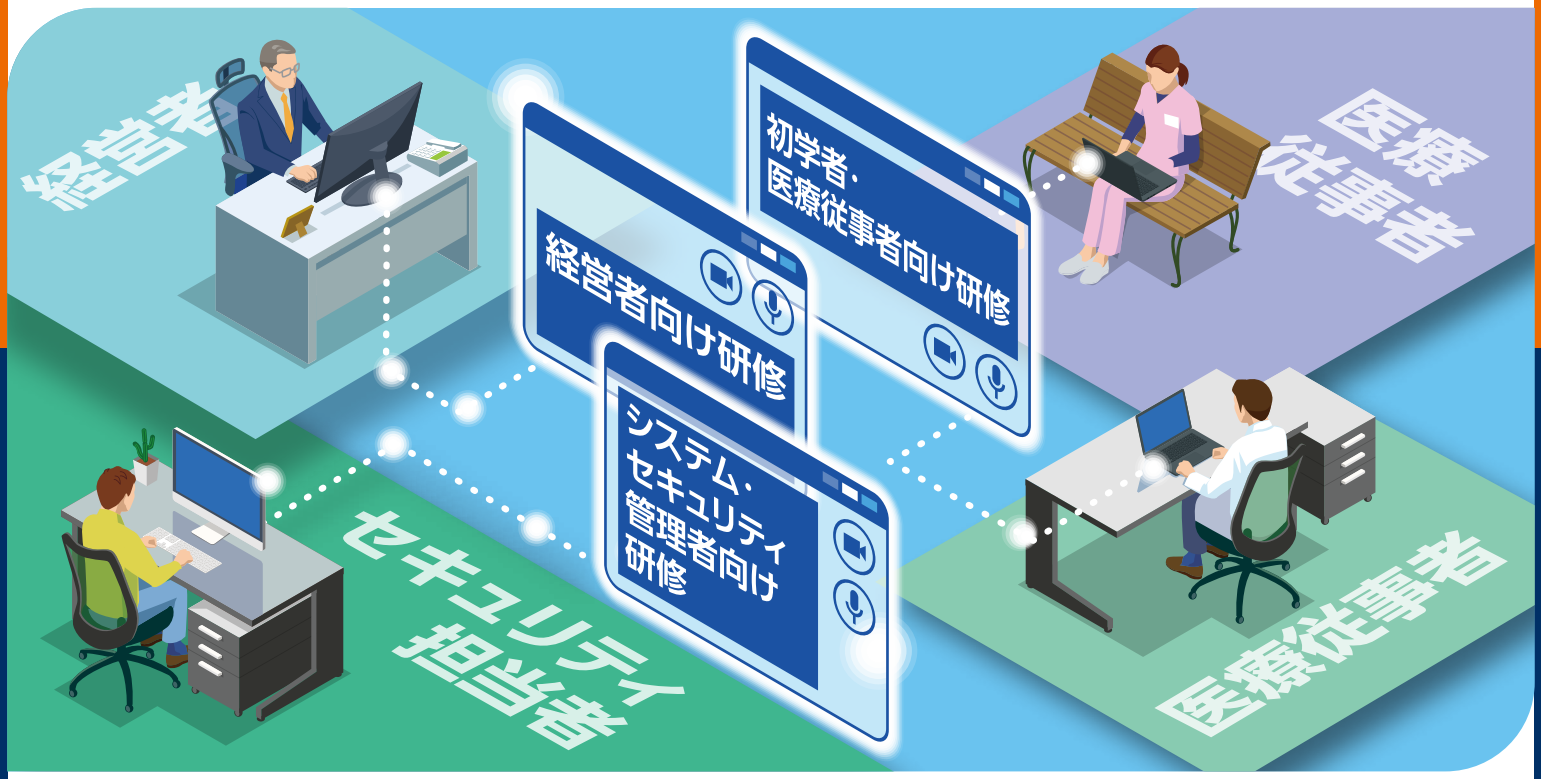
※　厚生労働省 HP「医療情報システムの安全管理に関するガイドライン第 6.0 版　特集」に掲載しています。

厚生労働省
Ministry of Health, Labour and Welfare

別添４

Software Association of Japan

令和5年度
医療情報セキュリティ研修



サイバーセキュリティ対策にかかる医療機関等向け研修について

近年、国内外の医療機関を標的とした、サイバーセキュリティインシデントが増加しており、我が国においても、世界各国と同様にリスクが高まっている状況にあります。昨年発生した「大阪府立病院機構　大阪急性期・総合医療センター」におけるランサムウェアよるインシデントにおいては、新規外来患者の受入の一時停止を招く被害となりました。こうした背景から医療機関のサイバーセキュリティ対策の徹底を図るべく、昨年度に引続き、医療機関のシステム・セキュリティ管理者や経営層等の階層別に研修を実施いたします。

開催概要

開催形式　オンライン開催

申込方法　医療機関向けセキュリティ教育支援ポータルサイト（MIST）よりお申込み下さい
https://mhlw-training.saj.or.jp/

対象
- 医療機関等の経営に携わる方
- 医療機関のシステム・セキュリティ等の管理者
- 医師、看護師、薬剤師等の医療従事者

研修の詳細と申込はこちら

● 本研修等に関するお問い合わせ先 ●

一般社団法人ソフトウェア協会 医療情報セキュリティ研修事務局　E-mail. mist-sajinfo@saj.or.jp

ひと、くらし、みらいのために
厚生労働省
Ministry of Health, Labour and Welfare

Software Association of Japan

研修一覧

サイバーセキュリティインシデントは、
ひとり、ひとりの日頃の意識にて防ぐことができます。
9月より研修開始、ぜひご参加ください。

研修の詳細と申込はこちら

研修種別	受講対象	実施方法	研修概要
導入研修 9月研修開始	医療機関等の従事者	オンライン	立入検査の項目に含まれたサイバーセキュリティの対応・対策に向けた医療機関におけるサイバーセキュリティチェックリストに基づいた研修
			2023年3月末に公開された大阪府立病院機構 大阪急性期・総合医療センターの「情報セキュリティインシデント調査委員会報告書」をベースにインシデントの内容、発生原因、対策、BCPの見直し等について学習
初学者等向け研修 10月研修開始	サイバーセキュリティの基礎知識を習得したい方	オンライン	サイバーセキュリティインシデントが身近であることを認識頂くとともに、システムや端末を使うにあたって、自分たちで今すぐできる備えなどについて学習
		ワークショップ	「今、実施しているセキュリティの工夫」「セキュリティの悩み」等をテーマにグループ単位で議論し情報共有を行う
経営者向け研修 10月研修開始	医療機関等の経営に携わる方	オンライン	つるぎ町立半田病院、大阪府立病院機構 大阪急性期・総合医療センター等のインシデント事例、経営者として必要なサイバーセキュリティの意識と知識について学習
		ワークショップ	「自組織の経営とセキュリティの考え方」「セキュリティでできていること、できていないこと」等をテーマにグループ単位で議論し情報共有を行う
		現地視察	大阪府立病院機構 大阪急性期・総合医療センターの視察およびインシデントの概要、ITガバナンスの重要性について学習
システム・セキュリティ管理者向け研修 10月研修開始	医療機関等のシステム・セキュリティ管理する方	オンライン	現在あるIT資産を活用したセキュリティ対策について学習Active Directory（AD）入門、認証・認可や特権管理の重要性などについて学習
		演習	インシデントレスポンス対応、マルウェアの感染体験やログ調査などの演習
		現地視察	大阪府立病院機構 大阪急性期・総合医療センターの視察およびインシデントの概要、インシデント対応の勘所について学習
e-learning	医療機関等の従事者	WEB	情報セキュリティの基礎、サイバー攻撃手法、インシデントレスポンス等の基本コンテンツ他、各研修の動画をアーカイブとして配信

※研修内容等については、変更される場合がございます。詳細は本事業のポータルサイト（MIST）をご確認ください。
※アーカイブ形式の実施を一部予定しております。

別添５

事　務　連　絡
令和４年 11 月 10 日

各都道府県衛生主管部（局）　御中

厚生労働省医政局特定医薬品開発支援・医療情報担当参事官室
厚生労働省政策統括官付サイバーセキュリティ担当参事官室

医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）

今般、大阪急性期・総合医療センター（以下「センター」という。）において、ランサムウェアによるサイバー攻撃事案が発生し、電子カルテの閲覧・利用ができなくなる等により、地域の医療提供体制に影響が出ているところです。医療機関を攻撃対象とする同種攻撃は近年増加傾向にあり、その脅威は日増しに高まっています。

厚生労働省では、センターに専門家チームを派遣して、原因の調査と復旧支援を行っていますが、攻撃の侵入経路は、医療機関自身のシステムではなく、院外の調理を委託していた事業者のシステムを経由したものである可能性が高いことが判っています。

医療機関においては、保有する医療情報の安全を確保するため、「医療情報システムの安全管理に関するガイドライン」（以下「ガイドライン」という。）等に基づき、必要な対策を講じていただいているところですが、今般のセンターにおける事案も踏まえると、医療機関自身のシステムにおけるサイバーセキュリティ対策に加え、サプライチェーンとの接続状況や、取引先システムのサイバーセキュリティ対策等をも俯瞰しつつ、必要な対策を講じていくことが求められています。

こうした状況を踏まえ、管内、管下の医療機関に対し、同種のサイバー攻撃に備え、令和３年６月 28 日付事務連絡「医療機関を標的としたランサムウェアによるサイバー攻撃（注意喚起）」（参考）に加え、下記の対策が適切に講じられているか確認を要請するとともに、万が一、サイバー攻撃を受けた場合にも事業継続計画等により地域住民への医療提供体制に支障が出来ることのないよう注意喚起をお願いします。

また、内閣サイバーセキュリティセンターにおいて、ランサムウェア対策に関する特設サイトを作成しているので、必要に応じてご活用下さい。

記

１　サプライチェーンリスク全体の確認

上記の通り、自組織のみならずサプライチェーン全体を俯瞰し、発生が予見されるリスクを医療機関等自身でコントロールできるようにする必要があることから、関係事業者のセキュリティ管理体制を確認した上で、関係事業者とのネットワーク接続点（特にインターネットとの接続点）をすべて管理下におき、脆弱性対策を実施する。

２　リスク低減のための措置

〇パスワードを複雑なものに変更し、使い回しをしない。不要なアカウントを削除しアクセス権限を確認する。多要素認証を利用し本人認証を強化する。

〇IoT 機器を含む情報資産の保有状況を把握する。

〇VPN 装置を含むインターネットとの接続を制御するゲートウェイ装置の脆弱性は、攻撃に悪用される可能性があるので、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。

〇悪用が既に報告されている脆弱性については、ログの確認やパスワードの変更など、開発元が推奨する対策が全て行われていることを確認する。

〇VPN 機器に対する管理インターフェースのインターネット上の適切なアクセス制限を実施する。

〇メールの添付ファイルを不用意に開かない、URL を不用意にクリックしないこと。不審メールは、連絡・相談を迅速に行い組織内に周知する。

３　インシデントの早期検知

〇サーバ等における各種ログを確認する。(例:大量のログイン失敗の形跡の有無)

〇通信の監視・分析やアクセスコントロールを再点検する。(例：不審なサイトへのアクセスの有無)

４　インシデント発生時の適切な対処・回復

〇サイバー攻撃を受け、システムに重大な障害が発生したことを想定した事業継続計画が策定する。

〇データ消失等に備えて、データのバックアップの実施及び復旧手順を確認する。

〇インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、外部関係機関への連絡体制や組織内連絡体制等を準備する。

〇インシデント発生時及びそのおそれがある場合には、速やかに厚生労働省等の関係機関に対し連絡する。

５　金銭の支払いに対する対応

厚生労働省としては、サイバー攻撃をしてきた者の要求に応じて金銭を支払うこ

とは、犯罪組織に対して支援を行うことと同義と認識しており、以下の観点により金銭の支払いは厳に慎むべきである。

〇金銭を支払ったからと言って、不正に抜き取られたデータの公開や販売を止めることができたり、暗号化されたデータが必ず復元されたりする保証がないこと。

〇一度、金銭を支払うと、再度、別の攻撃を受け、支払い要求を受ける可能性が増えること。

６　ランサムウェア特設ページ

https://security-portal.nisc.go.jp/stopransomware/

■医療機関等がサイバー攻撃を受けた場合等の厚生労働省連絡先

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

※迷惑メール防止のため、メールアドレスの一部を変えています。

「×」を「@」に置き換えてください。