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

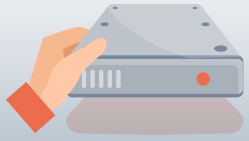
6 各種システムの更新

- ☑ 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

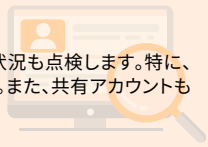
9 電子メールの確認

- ☑ 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）

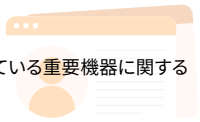
1 ✓アカウント整理と使用状況の棚卸し

- 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。



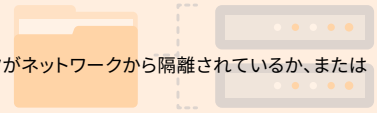
2 ✓連絡先の整備

- 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

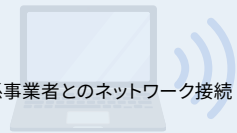
- 重要なシステムのバックアップが計画通りに行われているかを確認します。さらに、バックアップしたデータがネットワークから隔離されているか、または複数の方法でデータの保護が確保されているかも確認します。



医療情報システムの安全管理実務者

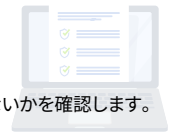
4 ✓通信制御の確認

- 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。



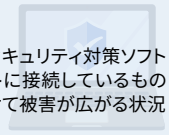
5 ✓ログの確認

- 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

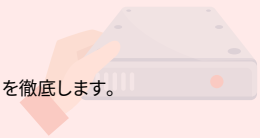
- バージョンアップやファームアップが適切に行われているかを確認します。特にインターネットに接続しているシステムに関しては、セキュリティ対策ソフトが常に稼働しているかを徹底的に確認し、導入されていない場合（セキュリティ対策ソフト等）は導入します。さらに、インターネットに接続しているものセキュリティ対策が不十分な場合は、通信制御の可能性を検討し、システムの停止または縮退を検討します。（これにより攻撃を受けて被害が広がる状況を未然に防ぎます。）



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